

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

**BRIEF IN SUPPORT OF MICROSOFT’S MOTION FOR PROTECTIVE ORDER
TEMPORARILY SEALING DOCUMENTS**

Microsoft submits the following memorandum in support of its Motion for a Protective Order Sealing Documents.

BACKGROUND

Microsoft has filed an *Ex Parte* Motion for Second Supplemental Preliminary Injunction Order (“Second Supplemental Preliminary Injunction Motion”) to prevent the activities of John Doe Defendants 1 and 2 (collectively “Defendants”) who are engaged in harmful and malicious Internet activities directed at Microsoft, its customers, and the general public. In the Second Supplemental Preliminary Injunction Motion, Microsoft seeks ex parte relief to disable the recently registered domains set forth in **Appendix A** to the Proposed Order. That will cease the irreparable harm resulting from Defendants’ conduct. Microsoft seeks relief under seal, with respect to the portion of the Order disabling the domains in **Appendix A** to the Proposed Order, because advance public disclosure or notice

of that requested relief would allow Defendants to evade such relief and further prosecution of this action, thereby perpetuating the irreparable harm at issue. The reasons for Microsoft's request are set forth in detail in the Second Supplemental Preliminary Injunction Motion filed concurrently herewith. Therefore, Microsoft requests that the *Ex Parte* Motion for Second Supplemental Preliminary Injunction Order and associated pleadings be sealed pending execution of the ex parte relief sought in Microsoft's Second Supplemental Preliminary Injunction Order, in particular disabling of the domains set forth in **Appendix A** to the Proposed Order. Microsoft's requested sealing order is narrowly tailored to impose the least restriction on the public's right of access to information as possible. Microsoft requests that all sealed documents be immediately unsealed upon execution of the portion of the Order disabling the domains set forth in **Appendix A** to the Proposed Order. As soon as that relief is executed, all papers will be made available on the public docket.

ARGUMENT

The right of access to court records is not absolute. *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597-98 (1978). Although both common law and the First Amendment afford the public a qualified right of access to judicial proceedings, *In re Fort Totten Metrorail Cases*, 960 F. Supp. 2d 2, 5 (D.C. Cir. 2013), the D.C. Circuit has expressed doubts about whether the First Amendment right of access applies outside of the criminal context. *SEC v. Am. Int'l Grp.*, 712 F.3d 1, 5 (D.C. Cir. 2013); *Ctr. for Nat'l Sec. Studies v. DOJ*, 331 F.3d 918, 935 (D.C. Cir. 2003); *In re Reporters Comm. for Freedom of the Press*, 773 F.2d 1325, 1337 (D.C. Cir. 1985) (Scalia, J.) (doubting that the benefits of open criminal trials inure to civil suits between private parties).

Competing interests may outweigh the public’s common law right of access to judicial records. *United States v. Hubbard*, 650 F.2d 293, 317–22 (D.C. Cir. 1980). Indeed, “[a] district court has authority to seal and unseal documents as part of its ‘supervisory power over its own records and files.’” *United States v. Ring*, 47 F. Supp. 3d 38, 40 (D.D.C. 2014) (quoting *Nixon v. Warner Commc’ns, Inc.*, 435 U.S. 589, 598 (1978)); *In re Nat’l Broad. Co.*, 653 F.2d 609, 613 (D.C. Cir. 1981) (“Because of the difficulties inherent in formulating a broad yet clear rule to govern the variety of situations in which the right of access must be reconciled with legitimate countervailing public or private interests, the decision as to access is one which rests in the sound discretion of the trial court.”).

Under D.C. Circuit law, the district court should weigh the following when presented with a motion to seal or unseal: “(1) the need for public access to the documents at issue; (2) the extent of previous public access to the documents; (3) the fact that someone has objected to disclosure, and the identity of that person; (4) the strength of any property and privacy interests asserted; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced during the judicial proceedings.” *Hubbard*, 650 F.2d at 317-22; *Metlife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 666 (D.C. Cir. 2017) (Garland, C.J.) (“[T]he Hubbard test has consistently served as our lodestar because it ensures that we fully account for the various public and private interests at stake.”).

The Federal Rules of Civil Procedure also recognize the important public and judicial interest in protecting confidential business information. *See* Fed. R. Civ. P. 26(c)(1)(G) (empowering courts to order “that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way”). Likewise, Supreme Court and D.C. Circuit authority recognize the necessity of non-public ex parte

proceedings. *See Granny Goose Foods, Inc. v. Teamsters*, 415 U.S. 423, 439, 94 S. Ct. 1113 (1974) (“Ex parte temporary restraining orders are no doubt necessary in certain circumstances...”); *Carroll v. President and Com’rs of Princess Anne*, 393 U.S. 175, 180 (1968) (“There is a place in our jurisprudence for ex parte issuance, without notice, of temporary restraining orders.”); *Omar v. Harvey*, 2006 WL 286861, at *1 (D.D.C. Feb. 6, 2006) (holding that an ex parte restraining order is appropriate where plaintiff demonstrates notice would render fruitless further prosecution of the action); *Council on American-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 75 (D.D.C. Nov. 3, 2009) (noting that ex parte restraining orders may be appropriate in circumstances where notice is impossible).

In this case, Microsoft’s rights and interests in protecting its ability to obtain ex parte temporary relief, and the necessity of sealing its pleadings in order to effectively disable the domains in **Appendix A** to the Proposed Order, is paramount over any competing public interest to *immediate* access to the information Microsoft requests be sealed. If Microsoft’s papers are not sealed, the relief sought would very likely be rendered fruitless, and there is a substantial risk Defendants would destroy evidence. Defendants are highly-sophisticated cybercriminals. They access Microsoft’s services without authorization; hack into high-value computer networks; install malware on the networks to gain and maintain long-term, surreptitious access to that network; and locate and exfiltrate sensitive information off of the networks. *See* Supplemental Preliminary Injunction Motion, filed contemporaneously herewith. If Defendants knew Microsoft sought the relief set forth in the Supplemental Preliminary Injunction Motion, they could quickly adapt the command and control infrastructure used to secretly establish themselves on a victim’s network. Declaration of David Anselmi In Support Of Microsoft’s *Ex Parte* Motion for Second Supplemental Preliminary Injunction Order (“Anselmi Decl.”) ¶¶ 32-34, set forth in **Exhibit 1** to

this Brief. Given Microsoft's actions against Defendants in this case, even disclosing that Microsoft has filed a Second Supplemental Preliminary Injunction Motion gives Defendants the opportunity to change their command and control infrastructure, set forth at **Appendix A** to the Proposed Order.

Additionally, evidence shows that when the Phosphorus defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury caused to their victims, making it more difficult for their victims to adequately assess the damage or take steps to mitigate that injury going forward. *Id.* ¶ 33. For example, once Defendants become aware that domains in Phosphorus' active infrastructure become known to the security community, they abandon that infrastructure and move to new infrastructure that is used to continue their efforts to intrude upon the computers of existing victims and new victims. *Id.* In the last five years, Microsoft has brought similar cases against John Doe defendants who have been conducting illegal activities through identifiable but movable infrastructures on the Internet very similar to that used by Phosphorus. Declaration of Gabriel M. Ramsey In Support Of Motion For Protective Order Temporarily Sealing Documents ("Ramsey Decl.") ¶ 5, set forth at **Exhibit 2** to this Brief. In four of those cases, the defendants immediately attempted to either destroy evidence or move their command and control infrastructure upon detecting the legal action being taken against them. *Id.* This underscores the risk that the Defendants in this case will take similar steps to destroy evidence and move their command and control infrastructure in **Appendix A** if they are given notice of the Second Supplemental Preliminary Injunction Motion. *Id.* ¶ 6.

The harm that would be caused by the public filing of Microsoft's Second Supplemental Preliminary Injunction Motion would far outweigh the public's right to access that information.

There is no need for the public to have immediate access to the Second Supplemental Preliminary Injunction Motion and supporting documents while Microsoft is seeking ex parte relief with respect to the domains in **Appendix A** to the Proposed Order, which will only be effective if these materials remain under seal. Applying the balancing test set forth in governing law demonstrates that Microsoft's interest in obtaining effective relief outweigh any immediate public right to disclosure.

Microsoft only seeks to seal such information for a limited period of time, until after effective ex parte temporary relief has been obtained, disabling the domains in **Appendix A** to the Proposed Order. After such point, sealing will no longer be necessary, and Microsoft will immediately commence efforts to provide Defendants notice of future hearings and service of related pleadings—at which point, all documents will be unsealed and the public will be given full access to these proceedings. Microsoft, upon execution of the ex parte relief disabling the domains in **Appendix A** to the Proposed Order, will file with the Clerk of the Court a Notice that the temporary restraining order has been executed. The Clerk of the Court may then file all documents related to this request on the public docket.

Should, however, the Court decide not to grant the ex parte relief Microsoft requests, Microsoft asks that such materials remain sealed for an indefinite period, as public disclosure or notice absent the ex parte relief requested would facilitate Defendants' harmful and malicious Internet activities.

Given the limited period of sealing as an alternative that balances the public interest in access with Microsoft's important interests in maintaining these materials under seal for a brief period of time, granting the instant request to seal is warranted and consistent with the legal framework for addressing this issue.

Dated: July 18, 2019

Respectfully submitted,

/s/ Gabriel M. Ramsey

Gabriel M. Ramsey (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com

Julia R. Milewski (D.C. Bar No. 1008678)
Justin D. Kingsolver (D.C. Bar. No. 1033806)
Matthew B. Welling (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
jkingsolver@crowell.com
mwelling@crowell.com

Richard Domingues Boscovich (*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.

EXHIBIT 1

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**DECLARATION OF DAVID ANSELMi IN SUPPORT OF
MICROSOFT'S EX PARTE MOTION TO SUPPLEMENT PRELIMINARY
INJUNCTION ORDER**

I, David Anselmi, declare as follows:

1. I am a Principal Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Microsoft's Ex Parte Motion to Supplement Preliminary Injunction Order. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my current role at Microsoft, I assess technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft's customer-facing online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting Microsoft's corporate resources from network-based attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager

performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 years reserve), attaining the rank of Lieutenant Colonel. I have been employed by Microsoft since February 1997.

I. OVERVIEW OF INVESTIGATION INTO PHOSPHORUS AND CONCLUSIONS

3. My declaration concerns an organization that is engaged in systematic criminal activity on the Internet. Because the identities of the individuals behind the activity addressed in this declaration are unknown, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: “Phosphorus.” Others in the security community who have researched this group of actors refer to the group by other names, including “APT 35,” “Charming Kitten,” and “Ajax Security Team.” The defendants have been linked to an Iranian hacking group or groups. I have investigated the infrastructure described in this declaration and have determined that the defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. Defendants have registered domains using functioning email addresses by which they communicated with domain registrars in order to complete the registration process.

4. Microsoft investigators have been monitoring and gathering information on the Phosphorus defendants. In the course of such investigation, I have been working with and directing a team that (1) engaged in the analysis and creation of “signatures” (which can be thought of as digital fingerprints) for the infrastructure used by the Phosphorus defendants, (2) discovered login activity into Microsoft services from Phosphorus-controlled infrastructure on the Internet, (3) matched reported Phosphorus phishing email campaigns to registered domains, (4) monitored domain registrations associated with the Phosphorus-controlled email addresses and other pertinent WHOIS record information, (5) monitored infrastructure frequently utilized by the Phosphorus defendants in order to identify new domains being registered by the Phosphorus defendants, (6) have confirmed resolution settings to particular Internet service

providers (ISPs) which have frequently been used by the Phosphorus defendants in the past, and (7) reviewed peer findings and public reporting on the Phosphorus defendants.

5. As alluded in paragraph 4 (1), the investigative team has developed methods to help us identify new domains registered by the Phosphorus actors. Particular features of the Phosphorus infrastructure have been identified and patterns of content, non-content, and technical features have been determined to be exclusively and specifically associated with the Phosphorus defendants. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Phosphorus domain. Each such domain is manually reviewed in detail by one or more subject matter experts as necessary to ascertain whether it is, in fact, a Phosphorus domain. Based on this analysis, we have identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the defendants.

6. Based on our investigation and analysis, Microsoft has determined that the Phosphorus defendants specialize in targeting and stealing credentials of prominent users of the Internet. The Phosphorus defendants target Microsoft and non-Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. Based on our research, the Phosphorus defendants have targeted Microsoft customers, political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East.

7. The Phosphorus defendants' objectives appear to be obtaining account credentials to later retrieve sensitive communications within the accounts. We believe that the Phosphorus defendants have been active since 2013 and continue to pose a threat today and into the future.

II. PHOSPHORUS' METHOD OF COMPROMISING AND STEALING INFORMATION FROM VICTIMS

8. The Phosphorus defendants typically attempt to compromise the personal (not work) accounts of the targeted individuals through a technique known as "spear phishing."

Spear phishing attacks are conducted in the following fashion: after researching a victim organization, the spear phisher will identify individuals associated with that organization through gathering publicly available information and by social engineering. The spear phisher will then initiate communications with the victim by using names, companies, and/or contents that are familiar to the victim. The ensuing communications exchanges are used to social engineer information, identify additional targets, entice a target into opening up a malicious attachment, and more. Microsoft has observed fake social networking profiles being created by Phosphorus defendants which would obviously present significant leverage in carrying out such an attack.

9. Another technique utilized by the Phosphorus defendants is to send a targeted individual an email specifically crafted to appear as if there is an issue with the targeted individual's account. Phishing emails often use generic domain names that appear to be tied to account activity and that require input of credentials for authentication. For example, domains such as service-accountrecovery.com. The Phosphorus defendants send the targeted individual an email citing an account problem as mentioned above, and which instructs the recipient to proceed to a (fake) website where they should login to remedy the situation. Through research and investigation:

a. Microsoft has determined that the Phosphorous defendants have used domains cited in **Exhibit 1** to this declaration (also attached as **Appendix A** to the Proposed Order). Sometimes, the Phosphorus defendants have created domains including Microsoft (or other) product names. At other times, as is presently the case, the defendants disguise their command and control domains by using terms that make them appears to be related to online services. In the domains at **Exhibit 1**, the Phosphorus defendants have incorporated terms such as "mail" or account "login" and "supports" and similar terms. The purpose of these formulations is to create the appearance of legitimate online services and to ultimately present content on the pages that mimic login pages that infringe Microsoft trademarks, such as Microsoft's "Outlook" or "Office 365" services and brands, or other confusing content.

b. Since the Preliminary Injunction Order and subsequent Supplemental

Injunction Order, Microsoft has identified an additional six domains that the Phosphorous defendants have registered that follow the same patterns and are no doubt intended to be leveraged in phishing attacks. These domains are listed in **Exhibit 1** and are also reflected in **Appendix A** to the Proposed Order.

10. The Phosphorus defendants create these domains with the purpose of ultimately including on the websites content that infringes Microsoft or other trademarks and with the purpose of confusing victims into clicking on links controlled by the Phosphorus defendants. When the user clicks on the links, they are taken to deceptive web pages that induce the victim to type in their Microsoft or other credentials, at which point the Phosphorus defendants obtain access to those credentials. This will result in the threat actors being able to log into the victim's account and gain access to whatever content is available on the legitimate service, which may include their email, address information, phone numbers, billing information, etc. Where available, the Phosphorus defendants can also download a copy of the victim's address book to be used for future targeting of additional intended victims. Not having safe emails impacts Microsoft's brands and services. Having personal information stolen by attackers impacts a customer's trust in the services being provided. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises for which they work, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

11. The Phosphorus defendants send these emails from a variety of online email services. As discussed above, there are domains created by the Phosphorus defendants with the ultimate goal of mimicking Microsoft brands, and those domains are clearly designed to be included in spear phishing emails as links to websites that the Phosphorus defendants have set up in advance and which they control. When a victim clicks on the link in the email, his or her computer is connected with the Phosphorus-controlled website. The victim is then presented a copy of a webpage that appears to be a login page for a webmail provider of which the victim is

a subscriber. In fact, this is a fake login page that is designed to induce the user to type in their webmail credentials. If the victim enters the correct credentials, at that point the Phosphorus actors obtain the user's credentials and can thereafter access the user's webmail account to steal email content and other information.

12. **Figures 1 and 2** below show copies of such webpages created by the Phosphorus defendants, designed to look like legitimate Microsoft Outlook login pages:



Figure 1



Figure 2

13. Phosphorus targets other brands beyond Microsoft and purport to be password reset or account login pages of other companies. For example, the Phosphorus defendants use fake emails instructing users to click links and type in credentials, fake “Verify” buttons prompting users to type their credentials into fraudulent login pages and fake “Sign in” pages instructing users to enter their user name and password. All of these methods are designed to induce users to type in credentials. As seen above with respect to the fake Microsoft login pages inviting users to type in their Microsoft Outlook “User name” and “Password,” this scheme is typical of the Phosphorus defendants’ activities. **Figures 3** through **4** are further examples of this tactic:

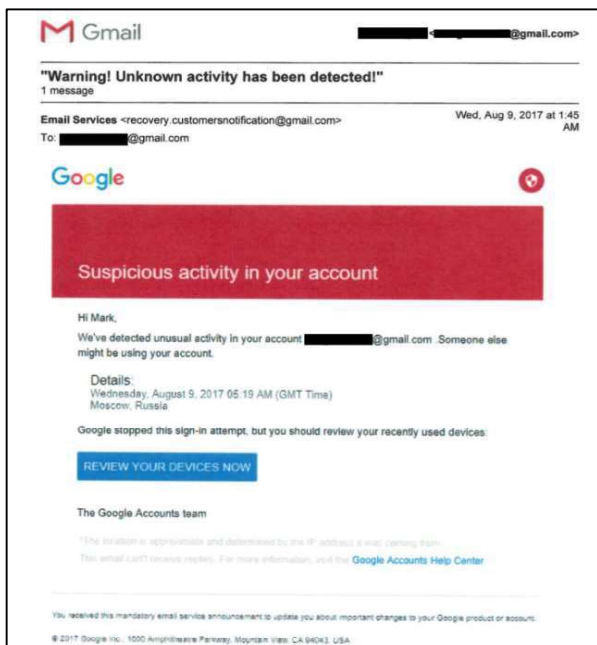


Figure 3

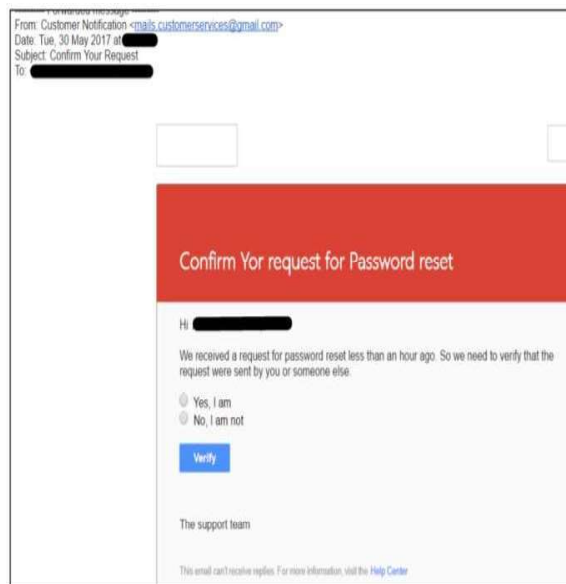


Figure 4

14. Defendants continue to target Microsoft and its users with new content. **Figures 5** and **6** are two recent examples of Defendants’ efforts to prompt users to type their credentials into fraudulent login pages:

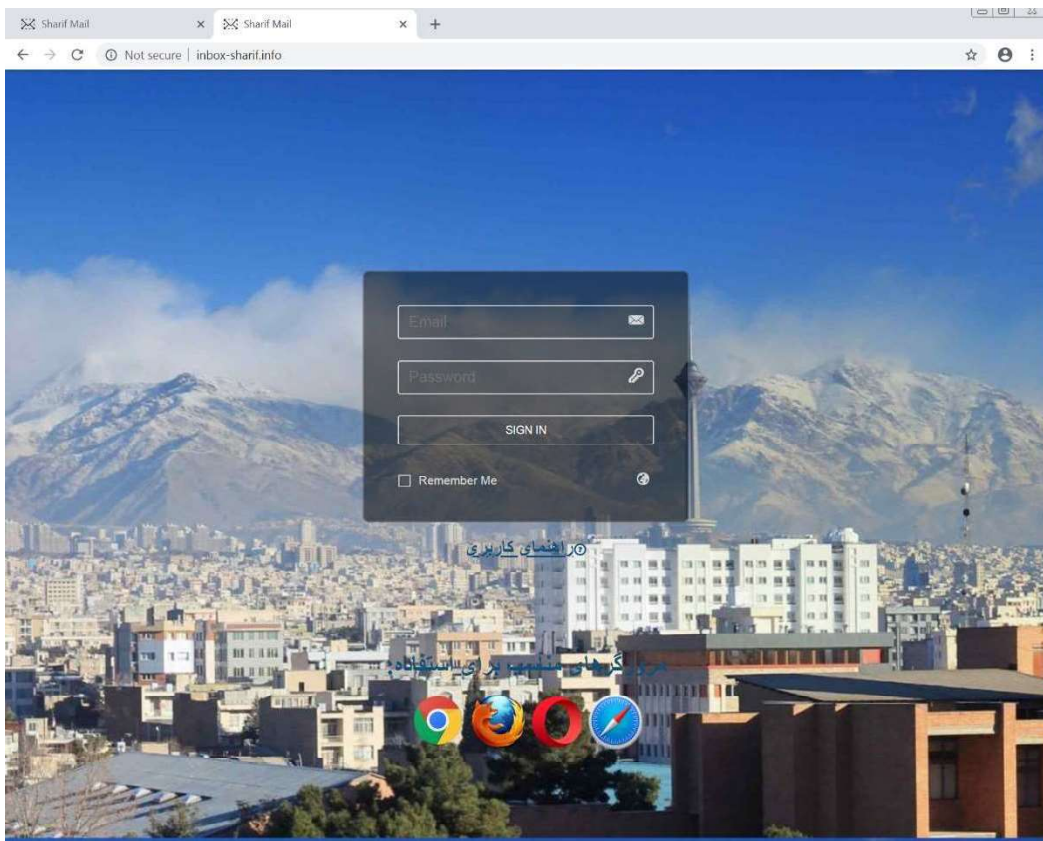


Figure 5

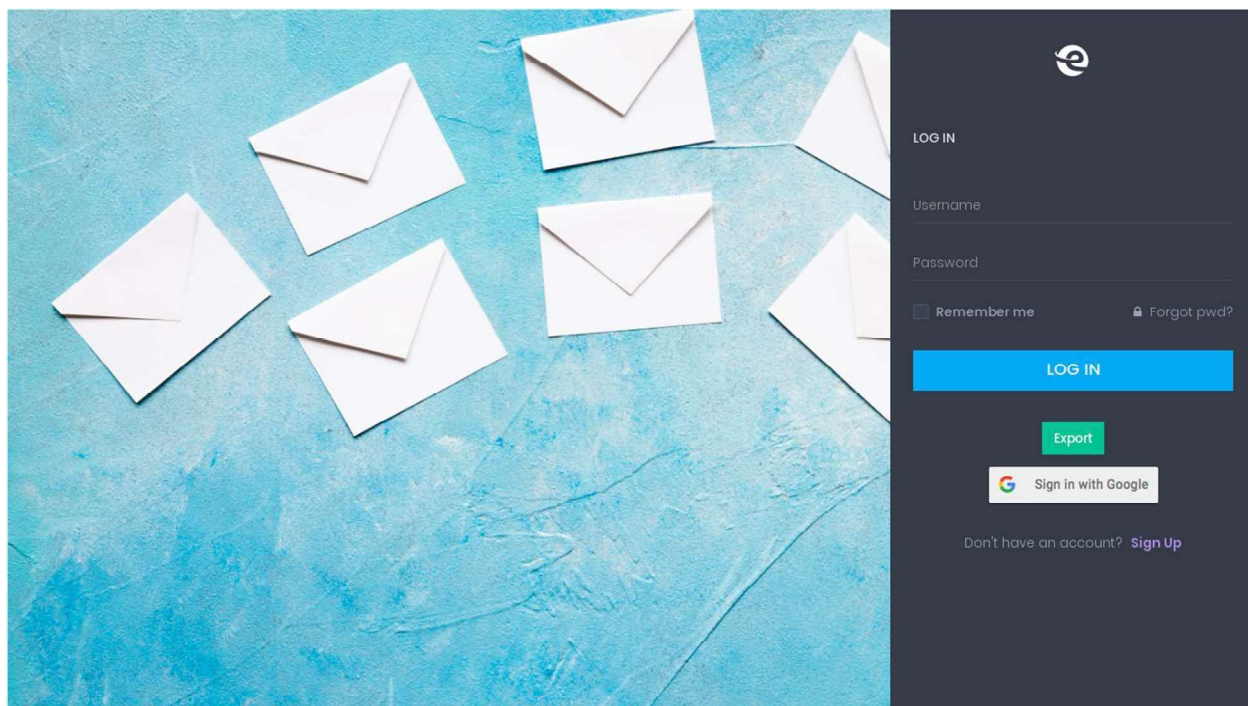


Figure 6

15. Upon successful compromise of a victim account, the Phosphorus defendants will not only be able to log into the account and review the victim's emails, but may also delete the spear phishing email that they previously sent to the user in an attempt to obfuscate their activities.

16. The Phosphorus defendants have targeted victims who are using Microsoft email services, and Microsoft investigators, by inspecting login history, have confirmed that Phosphorus defendants have intruded into those accounts potentially to steal information of Microsoft's users. **Figures 1 and 2** above demonstrate the Phosphorus defendants targeting users of Microsoft's Outlook email services.

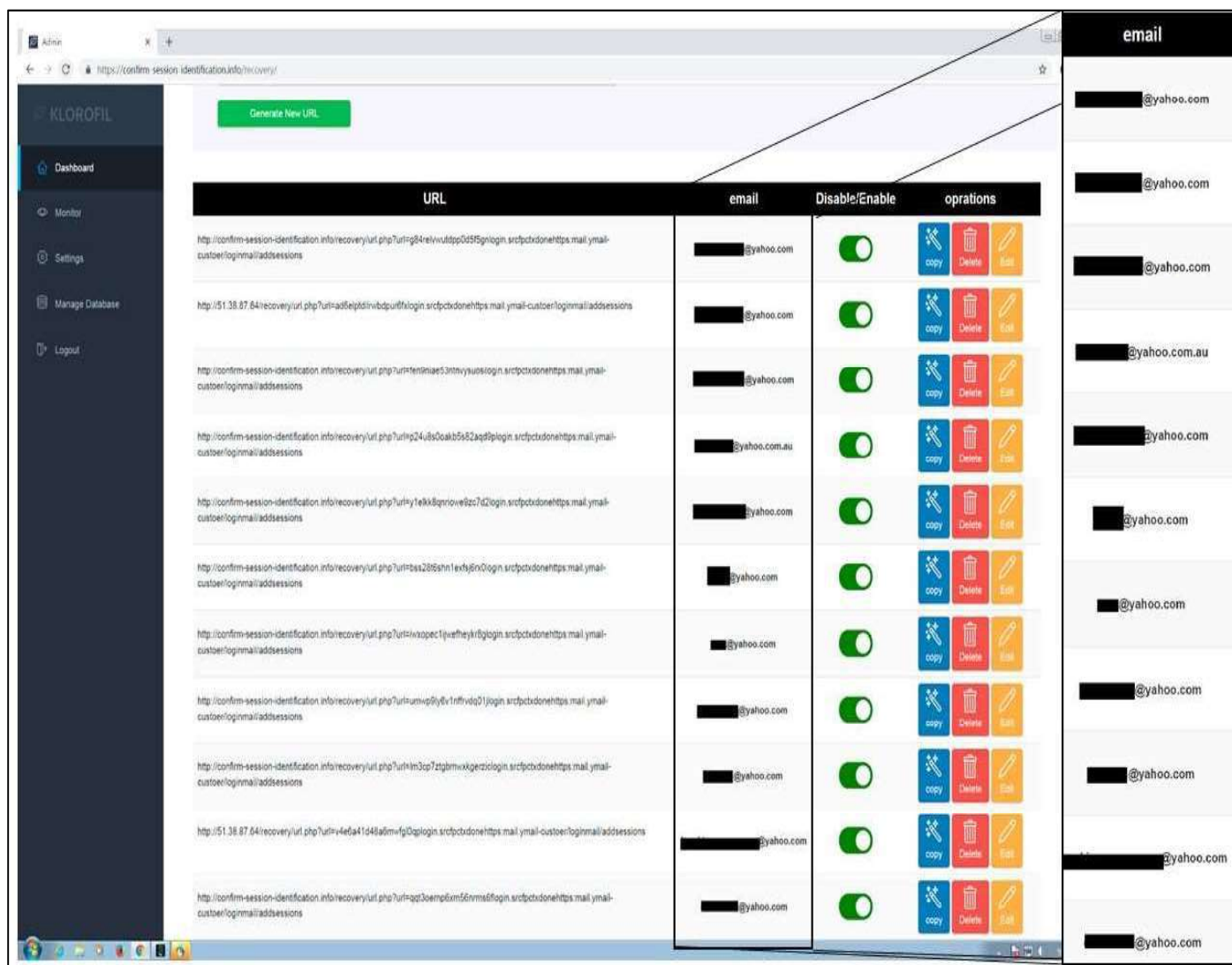
17. Microsoft investigators were also able to locate the control panel used by the Phosphorus defendants to create links sent to intended victims as well as to track successfully compromised victims who clicked on those links, typed in their credentials and had those credentials stolen by the defendants. Microsoft analysts identified the Phosphorus domain confirm-session-identification.info which led to discovery of the control panel URL. This control panel was accessed by a URL that was open and required no authentication. The control panel that the Phosphorus defendants used to monitor and control their access to victim accounts was present on the domain: confirm-session-identification.info. The domain confirm-session-identification.info was registered on 10/17/2018 as seen in the WHOIS record from a commonly used domain research tool called Domaintools.com. This record is reflected in **Figure 7**:

```
Domain Name: CONFIRM-SESSION-IDENTIFICATION.INFO
Registry Domain ID: D503300000240279653-LRMS
Registrar WHOIS Server:
Registrar URL: https://www.onlinenic.com
Updated Date:
Creation Date: 2018-10-17T11:27:08Z
Registry Expiry Date: 2019-10-17T11:27:08Z
Registrar: Registration Expiration Date:
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Domain ID Shield Service CO., Limited
Registrant State/Province: Hong Kong
Registrant Country: CN
Name Server: NS1.DNS-DIY.NET
Name Server: NS2.DNS-DIY.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/

The Registrar of Record identified in this output may have an RDDS service that can be queried for addit
```

Figure 7

18. The domain confirm-session-identification.info resolved to IP address 190.2.154.35 (Netherlands) from October 18th – 20th, 2018 and then moved to IP address 104.27.134.98 (US). The control panel below was obtained from the confirm-session-identification.info domain, when hosted on 104.27.134.98, on 11/04/2018. When visiting the URL <http://confirm-session-identification.info/recovery/> on 11/04/2018 the control panel did not require authentication to view its contents. Upon visiting this URL on 11/04/2018, we confirmed that the Phosphorus defendants use a unique ID (URL) for each targeted user. A redacted list of the users targeted can be seen in the email column in **Figure 8** below.



The screenshot shows a web application interface for 'KLOROFIL'. On the left is a sidebar with navigation links: Dashboard, Monitor, Settings, Manage Database, and Logout. The main content area displays a table with the following columns: URL, email, Disable/Enable, and operations. The table lists ten targeted users, each with a unique URL and a redacted email address. The 'Disable/Enable' column contains toggle switches, all of which are currently turned on. The 'operations' column contains three icons: a blue 'copy' icon, a red 'Delete' icon, and an orange 'Edit' icon. To the right of the table, there is a separate column labeled 'email' which lists the redacted email addresses for each user.

URL	email	Disable/Enable	operations
http://confirm-session-identification.info/recovery/url.php?url=84eivvutpp0d5f9nlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://51.38.87.64/recovery/url.php?url=a88eipktrivbdpurlfthlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=ntentiaes5.3ntvnyuswlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=924u83oakb562aqd8plogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com.au	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=ky1ekkl8pnrove9z07d2login.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=bsx286ahn1exy8n0ogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=ixvsopect1@efhejkrlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=umwq8y8v1nfrvqd01login.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=im3cp7ztgbrmxxkgerziclogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://51.38.87.64/recovery/url.php?url=y4ed941648a8m=fg0d8login.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit
http://confirm-session-identification.info/recovery/url.php?url=qp3oempx6m56nm6flogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy Delete Edit

Figure 8

19. The Phosphorus defendants' email panel has a "Monitor" screen for tracking compromised users. As seen in the screenshot below (**Figure 9**), there is at least one victim observed at the time of accessing the unauthenticated email panel:

Target Email	Auth Type	Auth Result	Date and Time	password/code
[REDACTED]@yahoo.com			2018-10-25 01:56:36	

User Agent	IP	country	city
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36	38.122.191.174	United States	America/New_York

Figure 9

20. Additionally, the settings tab (**Figure 10**) shows that when users' credentials are compromised, the credentials stolen from Microsoft users and others are emailed to the Yahoo account soup_mctavish@yahoo.com with the subject line "Yahoo-Pishing." Note here that the Phosphorus defendants misspelled "Phishing."

Admin

https://confirm-session-identification.info/recovery/setting_page.php

KLOROFIL

- Dashboard
- Monitor
- Settings**
- Manage Database
- Logout

Email Name reporter

[REDACTED]@yandex.com

Email Password reporter

[REDACTED]

Reporter Name

Yahoo-Pishing

Email Name Reiciver

soup_mctavish@yahoo.com

Reporter Subject

Yahoo-Pishing

Redirect Page

http://www.yahoo.com

save

Figure 10

21. The Phosphorus defendants also intrude upon and cause injury to Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers. In particular, the Phosphorus defendants have sent deceptive email messages to victims, such as those discussed above, which include links to websites from which the defendants install malicious software onto the victims' computers. The defendants refer to the malicious software as "Stealer." Stealer, once installed, can record what the victim types on their keyboard, take screenshots of what is on the victim's computer screen, steal login credentials for instant messaging account (including information about victims' Microsoft-owned "Skype" messaging accounts), email accounts, and other credentials. The Stealer software is installed from, and stolen information may be transferred to, defendants using command and control domains such as those reflected in **Exhibit 1**.

22. The installation of this malicious software damages the victim's computer and the Windows operating system on the victim's computer. During the infection of a victim's computer, the malicious Stealer software makes changes at the deepest and most sensitive levels of the computer's Windows operating system. The consequences of these changes are that the user's version of Windows is essentially adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users. For example, the defendants create registry key paths bearing the Microsoft "Windows" trademark, within the Microsoft operating system, including, among others:

"C:\WINDOWS\system32\rundll32.exe" "C:\ Documents and Settings\{USER}\ApplicationData\IntelRapidStart\AppTransferWiz.dll",#110

23. Further, as seen in **Figure 11** below, the Phosphorus defendants include metadata within the Stealer malicious software that expressly misrepresents that the software is created by "Microsoft" and that the software is a "Process for Windows."

File Version Information	
Copyright	Copyright © 2013
Product	Process for Windows
Description	Process for Windows
Original Name	Stealer.exe
Internal Name	Stealer.exe
File Version	1.0.0.0
Comments	Process for Windows

ExifTool File Metadata ⓘ	
AssemblyVersion	1.0.0.0
CharacterSet	Unicode
CodeSize	224256
Comments	Process for Windows
CompanyName	Microsoft
EntryPoint	0x38b1e
FileDescription	Process for Windows
FileFlagsMask	0x003f
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.0.0.0
FileVersionNumber	1.0.0.0
ImageFileCharacteristics	Executable, 32-bit
ImageVersion	0.0
InitializedDataSize	2048
InternalName	Stealer.exe
LanguageCode	Neutral
LegalCopyright	Copyright 2013
LinkerVersion	11.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0

Figure 11

III. PHOSPHORUS HAS ATTACKED MANY MICROSOFT CUSTOMERS IN THE DISTRICT OF COLUMBIA AND AROUND THE WORLD

24. Through its investigation, Microsoft has determined that the Phosphorus defendants have targeted Microsoft customers in the District of Columbia and continue to target our customers throughout the United States on multiple occasions.

IV. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

25. Phosphorus irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system and Outlook, Hotmail, OneDrive and Office 365 email and cloud services, as well as a variety of other software and services. Microsoft is the owner of the “Microsoft,” “Windows,” “Outlook,” “Windows Live,” “Hotmail,” “OneDrive” and “Office 365” trademarks. Microsoft has invested substantial resources in developing high-quality products and services. Microsoft has also invested, through its subsidiaries, in high value brands and services such as the “LinkedIn” brand and service. Due to the high quality and effectiveness of Microsoft’s products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and service and its brand, including the trademarks listed above.

26. Microsoft’s customers whose email accounts are compromised through the defendants’ credential theft are damaged by these activities. Similarly, Microsoft’s customers whose computers are infected with the malicious Stealer software are damaged by changes to Windows, which alter the normal and approved settings and functions of the user’s operating system, destabilize it, and enable unauthorized monitoring of the user and theft of user data.

27. In effect, once infected, altered and controlled by the Stealer software, the Windows operating system ceases to operate normally and is now a tool of deception and theft aimed at the owner of the infected computer. Yet they still bear the Microsoft Windows trademark. This is obviously meant to mislead Microsoft’s customers, and it causes extreme damage to Microsoft’s brands and trademarks.

28. Customers are usually unaware of the fact that their email accounts are compromised, that their computers are infected, that they are being monitored by the defendants

or that sensitive information is being stolen from them. Even if aware of an account intrusion or an infection of their computer, users often lack the technical resources or skills to resolve the problem, allowing their accounts and computers to be misused indefinitely, as manual steps to change account credentials or remove the malicious software may be difficult for ordinary users. They may be futile to a degree too where the Phosphorus defendants have software installed to observe the victim's activities and attempts to remediate the intrusion. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. This demonstrates the extreme problems that the activities of the Phosphorus defendants cause for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the defendants' intrusion into accounts and computers.

29. The activities of the Phosphorus defendants injure Microsoft and its reputation, brand, and goodwill. Users subject to the negative effects of the Phosphorus defendants' spear phishing emails sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. There is a great risk that Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

V. DISRUPTING PHOSPHORUS' ILLEGAL ACTIVITIES

30. The Phosphorus defendants' illegal activities will not be easy to disrupt. Evidence indicates that the Phosphorus defendants are highly sophisticated, well-resourced, organized, and patient. The Phosphorus defendants specialize in targeting individuals in organizations holding sensitive data, by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their credentials, and disguising its activities using the names and trademarks of Microsoft and other legitimate companies.

31. The most vulnerable point in the Phosphorus defendants' operations are a number of Internet domains through which the Phosphorus defendants obtain victim credentials, log into compromised accounts, and review sensitive information from victim accounts. A set of these is attached as **Exhibit 1** to this Declaration. Although not the case in **Exhibit 1**, similar domains have incorporated trademarks owned by Microsoft. Where domains have incorporated other companies' trademarks, those companies have been informed of and have no objection to Microsoft's proposal to take possession of the domains. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Phosphorus defendants collect victim credentials. In other words, any time a user clicks on a link in a spear phishing email and provides their username and password, that information will be prevented from going to the defendants at the Phosphorus domains, because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of defendants. While it is not possible to rule out the possibility that the Phosphorus defendants could use fall back mechanisms to evade the requested relief, redirecting this core subset of Phosphorus domains will directly disrupt current Phosphorus infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest, in protecting customers of other web services companies who have consented to the relief sought in this action.

32. I believe that the most effective way to suspend the injury caused to Microsoft, its consumers, and the public, is to take the steps described in the Second Supplemental Injunction Order ("Proposed Order"). This relief will significantly hinder the Phosphorus defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Phosphorus defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to the Phosphorus defendants' malicious activities. This can already be seen by effect of the Court's prior orders in this case. Executing the Court's previous Temporary Restraining Order and Preliminary Injunction Order, Microsoft cut communications between Defendants' existing command and

control infrastructure and the victim computers and networks that Defendants attacked and from which Defendants had been stealing information.

33. The Phosphorus defendants' techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in the Phosphorus defendants' active infrastructure become known to the security community, the defendants abandon that infrastructure and move to new infrastructure that is used to continue the Phosphorus defendants' efforts to compromise accounts of new victims. For this reason, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Phosphorus defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason as well, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft. Piecemeal requests to disable these domains, informal dispute resolution or notice to the defendants prior to redirecting the domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous intrusions such as those carried out by the Phosphorus defendants, and prior investigations and legal actions involving such intrusions and actors, I believe that the Phosphorus defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

34. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by actors carrying out intrusions such as those in this case, but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to

continue their operations and destroying or concealing evidence of their operations. For example, after public reports on this actor group were made available, the control panel cited in **Figures 8** through **10** was updated to require authentication. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Phosphorus infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

35. One of the basic questions faced by Microsoft's investigators in the course of their investigation into Phosphorus is determining whether or not a domain misusing a Microsoft trademark is actually associated with illegal activity being conducted by the Defendants. Fortunately, such a determination can be reliably made based upon what we know about Phosphorus and how they operate their criminal infrastructure.

36. First, the Defendants typically use a small set of distinctive malware, and this malware can be identified and distinguished from other types of malware based on several specific forensic factors. The specific types of malware known to be used by Defendants are listed in **Exhibit 2** to this Declaration. The presence of this distinctive malware therefore serves as a reliable indicator that Defendants are involved. In other words, if the malware used in a new attack matches the distinctive malware known to have been used by the Defendants in past attacks, it indicates that the actors behind the new attack are the Defendants. Further, in the future, if new malware variants or families are used by Phosphorus, Phosphorus may be identified based on the similarity of such new malware to previously used malware and previously used modes of deploying such malware.

37. Because Phosphorus malware is reasonably distinctive, domains that are used to deliver the Phosphorus malware to targeted victims and domains that are used to communicate with Phosphorus malware already installed on victim networks are strongly implicated as Phosphorus domains. For example, phishing e-mails that deliver Phosphorus malware in the form of weaponized documents or other attachments may come from or contain links back to particular domains. Other phishing e-mails include links to domains that Defendants have set up in advance as websites designed to download Phosphorus malware to the user's computer and

infect it. Once installed on a computer, Phosphorus malware is programmed to connect to and communicate with a particular set of domains after it successfully infects a victim network. In any of these cases, the Internet domains associated with the Phosphorus attack are strongly implicated as Phosphorus domains.

38. Second, Microsoft has identified patterns in the registration information provided by Defendants when registering the domains that they use in their illegal activities. The factors considered include information required to be submitted during the domain registration process and includes information such as: “name,” e-mail address, address and phone number provided by the registrant, the hosting service designated, the name servers used, and the IP address associated with the domain. Basic registration information associated with Domains registered by Defendants in the past, including the more recent domains registered by Defendants, is included in Exhibit 2. If the registration information associated with a newly identified domain closely matches the pattern associated with domains registered by the Defendants in the past, it is a strong indicator that the Defendants are behind the registration of the new domain. Further, in the future, if new information is used by Defendants, but registration patterns are similar to previously used registration patterns, this too will permit Phosphorus domains to be reliably identified.

39. Third, Microsoft considers the specific tactics used during a new attack. For example, Phosphorus Defendants often send phishing e-mails to victims in which the e-mail purports to be a notification from Microsoft to the recipient regarding an unauthorized access to the recipients Microsoft account, and requesting that the recipient reset his or her account credentials. If the victim clicks on the embedded “Change Password” button in the phishing email, the victim will be connected to a Phosphorus-controlled website which will attempt to induce the victim to enter his account credentials. Other tactics favored by the Phosphorus Defendants include particular deployments of remote code execution through browser drive-by, remote code execution through malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on. Where the

tactics used in a new attack match the tactics observed to be favored by Phosphorus Defendants in past attacks, it is an indication that the Phosphorus Defendants are behind the new attack. Consequently, a domain can be linked to the Phosphorus Defendants by observing the tactics used in attacks involving that domain. Further, in the future, if the details, code and mode of execution change, but the general tactics are consistent with prior tactics of Phosphorus, this too will permit Phosphorus domains to be identified.

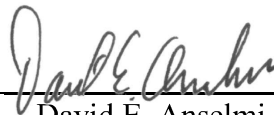
40. Fourth, the Phosphorus Defendants tend to target a particular type of victim and attempt to steal particular types of information. Therefore, Microsoft can use information about the intended victim to help determine whether or not Defendants are involved in the new attack. For example, Phosphorus continues to target Microsoft customers who are political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. Where an Internet domain is associated with an attack on these particular types of targets, it is a factor that is consistent with the known activity and objectives of the Defendants. Further, in the future, if the targeted individuals or institutions are consistent with prior tactics of Phosphorus, this too will permit Phosphorus domains to be identified.

41. Fifth, the Phosphorus Defendants have used Microsoft trademarked brands or slight misspellings of those brands in the names of the domains that they register for their illegal activity, or generalized versions suggestive of Microsoft's services. Defendants use this "blending" technique to disguise the illegal nature of their conduct from the intended target. Thus, use of Microsoft trademarks, brand names or slight misspellings or confusing variations of those trademarks or brand names in the domain name, or generalized versions of indicators of Microsoft's services, is an indicator that the domain is associated with Phosphorus. The list of known and likely trademarks, brands and variants used by Phosphorus is set forth at Exhibit 2.

42. Microsoft considers many factors associated with a domain including those described above and listed in Exhibit 2 to make a balanced determination of whether or not a domain is being used by the Phosphorus Defendants.

43. Defendants continue to register domains to carry out attacks on Microsoft's technology and customers, in particular, using Microsoft's trademarks, brands and other deceptive means, despite the court's previous orders to cease that activity and despite the prior relief which removed previously used domains from Defendants' control. Given Defendants' apparent willingness to violate the court's orders on an ongoing basis, and the ease and speed with which Defendants can register Microsoft-related domains to continue their attacks, an ongoing process is needed to efficiently and quickly curtail such activities as soon as Defendants register domains for their attacks. Without such a process, Defendants will be able to continue their malicious and illegal activities, and will continue to cause irreparable injury to Microsoft, its customers and the public. Without such a process, Defendants will not be deterred from engaging in such illegal and harmful activities. I have reviewed the process set forth in Microsoft's *Ex Parte* Motion for Second Supplemental Preliminary Injunction Order submitted with this declaration. Based on my experience and background, I conclude as a technical and practical matter that the process set forth in the proposed order would enable Microsoft and the Court to effectively and efficiently enforce the Court's prior and ongoing orders and stop the irreparable harm caused by Defendants' illegal activities on an ongoing basis. I also reach this conclusion on the basis that this same expedited process is in place, and ongoing, with respect to a separate matter in the Eastern District of Virginia, addressing a different threat actor group. The process has been effective in that matter. Thus, I conclude that it would be effective in the instant matter as well.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 17th day of July 2019, in Redmond, Washington.



David E. Anselmi

EXHIBIT 1

APPENDIX A**.COM DOMAINS****Registry**

c/o

VeriSign, Inc.

VeriSign Information Services, Inc.

12061 Bluemont Way

Reston, Virginia 20190

United States

mail-files.com	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: bd04d6f1eec84a9ba600d7c0c6f0325f.protect@whoisguard.com
logins-signin.com	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: be7e7649fbab44d5becff2c72e436f84.protect@whoisguard.com
supports-email.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491

	Registrant Fax Ext: Registrant Email: whoisprivacy@domainidshield.com onlinenic-enduser@onlinenic.com
loginacount.com	Registrant Organization: frederik Registrant State/Province: hessen Registrant Country: DE Registrant Email: Contact holder at https://www.domainidshield.com/gdpr onlinenic-enduser@onlinenic.com

.ORG DOMAINS**Registry****Public Interest Registry (PIR)****1775 Wiehle Avenue****Suite 200****Reston Virginia 20190****United States**

account-verify.org	Registrant Organization: delijapp Registrant State/Province: hb Registrant Country: AF onlinenic-enduser@onlinenic.com
--------------------	---

.INFO DOMAINS**Registry****Afilias, Inc.****300 Welsh Road****Building 3, Suite 105****Horsham, PA 19044****United States**

share-doc.info	Registrant Organization: Schroeder co. Registrant State/Province: NC Registrant Country: AF onlinenic-enduser@onlinenic.com
----------------	--

EXHIBIT 2

I. Criteria Indicating Phosphorus Domains

Delivers malicious software, code, commands, exploits and/or “backdoor” functionality previously associated with Phosphorus, including but not limited to: Stealer malware, or similar code or functionality deployed in a manner previously associated with Phosphorus.	Associated with remote code execution through browser drive-by or malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on, escalation of privileges, DLL file backdoor, credential stealing functionality, SSL tunnel, and/or functionality to deliver code or functions to “air gapped” USB devices, deployed in a manner previously associated with Phosphorus or similar code or functionality.
Domain registration information	Use of cryptocurrency to purchase services
Name servers	Start of Authority (SOA) records
Resolves to IP of past Phosphorus domain, command and control server or similar infrastructure	Resolves to IP used in past Phosphorus malware delivery or credential harvesting domains or credential harvesting domains
Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Phosphorus.	Used to deceive, target, obtain information from, and/or communicate commands or code to recipients that may possess or be able to provide sensitive information or trade secrets of persons, entities or networks related to the defense, critical infrastructure or high technology sectors, journalists, political advisors or organizations, government bodies, diplomatic institutions, religious organizations, universities, and/or military forces and installations.
SSL Cert Issuer_DN	SSL Cert Subject_DN
Host	Registrar
Domains similar to previously used domains	Victims being targeted similar to past targets

II. Known And Likely Microsoft Trademarks and Brands Used By Phosphorus

While Defendants may use any Microsoft marks, brands or confusingly similar indicators, Defendants have already exploited or are likely to exploit the following: “365,” “Azure,” “Bing,” “Excel,” “Exchange,” “Healthvault,” “Hotmail,” “LinkedIn,” “Live,” “Messenger,” “Microsoft,” “Minecraft,” “MSDN,” “MSFT,” “MS,” “MSN,” “.NET,” “O365,” “Office,” “OneDrive,” “Outlook,” “OWA,” “Passport,” “PowerPoint,” “SharePoint,” “Skype,” “Surface,” “Visio,” “Win,” “Windows,” and “Xbox.”

While Defendants may use any keyword, in combination with Microsoft marks, brands or confusingly similar indicators, or with other keywords, we believe following are the most likely keywords to be used, along with intentional misspellings:

365	analytic	care	click	continue
64	app	cares	cloud	control
access	are	center	com	corp
account	assist	centr	component	corporate
accounts	auth	centre	config	corporation
activities	authenticate	certificate	confirm	crc
adapter	authorizes	cfg	confirmation	credentials
adviser	broadcast	change	connect	customer
agency	bulletin	check	consumer	daily
american	cache	checksum	content	data

dc	http	my	redirect	support
delivery	id	mymail	reply	sync
department	identification	net	reserve	sys
departrment	identifier	network	review	system
dev	identify	news	scan	team
docs	identity	notification	search	technology
document	inbox	onlihe	sec	telecom
download	info	online	secure	telegram
drivadptrwin	intel	options	securing	tellekom
drive	intelligence	page	security	terms
driver	ipv4	panel	sell	test
drivers	ipv6	passport	send	tests
drv	issue	password	server	tools
edit	link	pc	service	transfer
elite	log	permission	servicing	trust
email	login	plus	session	trusted
expo	magic	podcast	set	update
file	mail	policy	setting	updater
fix	mailbox	politics	settings	updates
forum	management	press	share	upgrade
general	manager	privacy	sharing	user
getupdate	me	product	shop	users
getupdt	media	profile	signal	verification
global	meeting	progress	signin	verify
gov	member	protect	site	wear
help	message	protected	speak	web
here	mfa	provider	srv	webmail
home	mobile	ready	statistic	world
host	module	recognized	status	you
hotfix	monitor	recovery	store	your

III. Phosphorus Domains Registered By Defendants To Date

yahoo-verification.org	Registrant: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 109 First Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94988 Registrant Country: BA Registrant Phone: +1.4038493301 Registrant Fax: +1.4038493302 Registrant Email: domainadmin@yahoo-verification.org
support-services.com	Registrant Name: hash crypt Registrant Organization: hashcrypt Registrant Street: nbcj hjf,m Registrant City: losangles Registrant State/Province: Alabama Registrant Postal Code: 35004 Registrant Country: US Registrant Phone: +1.09876543567 Registrant Email: hashcrypt@protonmail.com
verification-live.com	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation

	Registrant Street: AS8068 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, Registrant City: toronto Registrant State/Province: toronto Registrant Postal Code: 64043 Registrant Country: UM Registrant Phone: +1.6509234001 Registrant Fax: +1.6509234002 Registrant Email: test9179@porotonmail.com
com-mailbox.com	Registrant Name: Priview Service Registrant Organization: mish Registrant Street: No 885, Azar st Registrant City: Dubai Registrant State/Province: Dubai Registrant Postal Code: 98120 Registrant Country: AE Registrant Phone: +97.3218526 Registrant Fax: +97.3218526 Registrant Email: domain.seller2017@yandex.com
com-myaccuants.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: co5940551458104@domainidshield.com
notification-accountservice.com	Registrant Name: mosa alnarjani Registrant Organization: Registrant Street: baqdad, alqusair st , no 246 Registrant City: baqdad Registrant State/Province: baqdad Registrant Postal Code: 548996 Registrant Country: IQ Registrant Phone: +964.7730061463 Registrant Email: meisam.bayat.sector@gmail.com
accounts-web-mail.com	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: US Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com

customer-certificate.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
session-users-activities.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
user-profile-credentials.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
verify-linke.com	Registrant Name: sora bara Registrant Organization: narabara Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 7482957439 Registrant Country: BI Registrant Phone: +1.234124323 Registrant Fax: +1.2129876243 Registrant Email: test9179@protonmail.com
support-services.net	Registrant Name: Support Services Inc. Registrant Organization: Support Services Inc. Registrant Street: 1901 Amphitheatre Parkway Registrant City: Mountain View Registrant State/Province: 64043 Registrant Postal Code: 64043 Registrant Country: US Registrant Phone: +1.6509234001 Registrant Fax: +1.6509188572 Registrant Email: test9179@protonmail.com
verify-linkedin.net	Registrant Name: sora bara Registrant Organization: none

	Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 748295743 Registrant Country: BI Registrant Phone: +75.234124323 Registrant Fax: +86.12124321 Registrant Email: dnsadmin@verify-linkedin.com
yahoo-verification.net	Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: BA Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
yahoo-verify.net	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 701 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 98089 Registrant Country: BI Registrant Phone: +1.4083893300 Registrant Fax: +1.4083893301 Registrant Email: domainadmin@yahoo-verify.net
outlook-verify.net	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: One Microsoft Way, Redmond, WA, 98052, US Registrant City: Washington Registrant State/Province: canada Registrant Postal Code: 7482957439 Registrant Country: US Registrant Phone: +1.234124323 Registrant Phone Ext: Registrant Fax: +1.2129876243 Registrant Fax Ext: Registrant Email: supportiveemail@protonmail.com
com-users.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: co5806503530204@domainidshield.com
verify-account.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL

	TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
telegram.net	Registrant Name: NS-CLOUD-B1.GOOGLedomains.COM Registrant Organization: Domains By Proxy, LLC Registrant Street: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant City: Arizona Registrant State/Province: Arizona Registrant Postal Code: 0056 Registrant Country: US Registrant Phone: +1.4806242505 Registrant Fax: +1.4806242506 Registrant Email: verdonew@protonmail.com
account-verify.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
myaccount-services.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
com-identifier-servicelog.name	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: https://www.name.com/contact-domain-whois/com-identifier-servicelog.name abuse@name.com

microsoft-update.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
outlook-livecom.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
update-microsoft.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
documentsfilesharing.cloud	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: documentsfilesharing.cloud@protecteddomainservices.com
com-microsoftonline.club	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
confirm-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK Registrant Email: onlinenic-enduser@onlinenic.com
session-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong

	Registrant Country: CN onlinenic-enduser@onlinenic.com
confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
document-share.info	Registrant Organization: Martini Registrant State/Province: Tashkent Registrant Country: UZ onlinenic-enduser@onlinenic.com
broadcast-news.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
webemail.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-identifier-servicelog.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
documentsharing.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: AF onlinenic-enduser@onlinenic.com
notification-accountservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identifier-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
documentofficupdate.info	Registrant Organization: William Brown Registrant State/Province: VA Registrant Country: US onlinenic-enduser@onlinenic.com
recoveryusercustomer.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
serverbroadcast.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
account-profile-users.info	Registrant Organization: arsalan co.

	Registrant State/Province: Louisiana Registrant Country: US onlinenic-enduser@onlinenic.com
account-service-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
accounts-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-accountidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-privacy-help.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-sessionidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-useraccount.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirmation-users-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-session-identification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
continue-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customer-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customers-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com

elitemaildelivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
email-delivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
message-serviceprovider.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notificationapp.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recognized-activity.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: VA onlinenic-enduser@onlinenic.com
recover-customers-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-recovery-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-continue.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-mail-customers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-verify-user.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
shop-sellwear.info	Registrant Organization: maryam s32 Registrant State/Province: tersite Registrant Country: US onlinenic-enduser@onlinenic.com
supportmailservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
terms-service-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
user-activity-issues.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
useridentity-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
users-issue-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
verify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
login-gov.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-signal-agency.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notifications-center.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
identifier-services-sessions.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
session-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
customer-managers.info	Registrant Organization: Home Registrant State/Province: TX

	Registrant Country: US onlinenic-enduser@onlinenic.com
confirmation-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-session-confirmation.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-managers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-services-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-session-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
sessions-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
download-teamspeak.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-issue-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
microsoft-upgrade.mobi	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
broadcastnews.pro	Registrant State/Province: UT Registrant Country: US abuse@name.com
mobile-messengerplus.network	Registrant Name: Cave Detector Registrant Organization: Masqat Co Registrant Street: No 64, Lion St Registrant City: Masqat Registrant State/Province: Masqat Registrant Postal Code: 85641 Registrant Country: OM Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: cave.detector@yandex.com
sessions-identifier-memberemailid.network	Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domain Protection Services, Inc. Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: CO Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar: Name.com, Inc. Registrar IANA ID: 625 Registrar Abuse Contact Email: abuse@name.com Registrar Abuse Contact Phone: +7.202492374
scribdinc.com	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201

	Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: https://www.name.com/contact-domain-whois/scribdinc.com abuse@name.com
telagram.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: whoisprivacy@domainidshield.com
bahaius.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
customers-reminder.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com

identity-verification-service.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
inbox-drive.info	Registration Name: Jennifer J. Bradley Registration Organization: roseron co Registration Street: 2811 Maple Avenue Registration City: Modesto Registration State/Province: CA Registration Postal Code: 95354 Registration Country: US Registration Phone: +1.251548796 Registration Phone Ext: Registration Fax: +1.251548796 Registration Fax Ext: Registration Email: amanda.cristiani15@gmail.com
inbox-sharif.info	Registration Name: Jennifer J. Bradley Registration Organization: roseron co Registration Street: 2811 Maple Avenue Registration City: Modesto Registration State/Province: CA Registration Postal Code: 95354 Registration Country: AF Registration Phone: +1.2564158796 Registration Phone Ext: Registration Fax: +1.2564158796 Registration Fax Ext: Registration Email: amanda.cristiani15@gmail.com
magic-delivery.info	Registration Name: William Brown Registration Organization: will co Registration Street: 410 Coulter Lane Registration City: Richmond Registration State/Province: VA Registration Postal Code: 23226 Registration Country: VA Registration Phone: +1.8042873632 Registration Phone Ext: Registration Fax: +1.8042873632

	Registration Fax Ext: Registration Email: williambrown.wl.br@gmail.com
recovery-services.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
verification-services.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
youridentityactivity.world	Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domain Protection Services, Inc. Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: CO Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY abuse@name.com

EXHIBIT 2

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

**DECLARATION OF GABRIEL M. RAMSEY IN SUPPORT OF MOTION FOR
PROTECTIVE ORDER TEMPORARILY SEALING DOCUMENTS**

I, Gabriel M. Ramsey, declare as follow:

1. I am an attorney admitted to practice in the State of California and the District of Columbia. I am a partner at the law firm of Crowell & Moring LLP (“Crowell”), counsel of record for the Plaintiff in this matter, Microsoft Corporation (“Microsoft”). I make this declaration in support of Microsoft’s Motion for Protective Order Temporarily Sealing Documents. I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would testify to the following under oath.

2. This case arises out of the harmful and malicious Internet activities of Defendants John Does 1 and 2 (collectively “Defendants”). I am informed and on that basis believe that Defendants are sophisticated cybercriminals who specialize in stealing sensitive information from computer networks. I am informed and on that basis believe that Defendants make and have continued to make unauthorized access to Microsoft’s services and software, hack into a target’s

computer network, and in particular Microsoft's software, install malware on those networks giving them long-term and surreptitious access to those networks, and then locate and exfiltrate sensitive information from them.

3. I am informed and believe that, for reasons explained in detail in the declaration of David Anselmi In Support Of Microsoft's *Ex Parte* Motion For Second Supplemental Preliminary Injunction Order, filed contemporaneously herewith, permitting Defendants to learn of these proceedings prior to execution of the temporary *ex parte* relief sought in Microsoft's Motion For Second Supplemental Preliminary Injunction Order—in particular the portion to disable the domains in Appendix A to that Order—would preclude Microsoft's ability to obtain effective relief against Defendants. This is because Defendants are highly sophisticated cybercriminals capable of quickly adapting the command and control infrastructure used to perpetrate Defendants' unlawful conduct in order to overcome Microsoft's remediation efforts and can and have done so repeatedly.

4. I am informed and believe that, absent a protective order, there is a substantial risk that Defendants will learn of these proceedings before the temporary *ex parte* relief to disable the domains in Appendix A to the Second Supplemental Preliminary Injunction Order can be effected and will take steps to evade the relief sought.

5. Over the past nine years, I, on behalf of Microsoft, have been involved with prosecuting twelve similar cases. These cases all involved similar litigation strategies and claims and have involved John Doe defendants conducting illegal activities through identifiable but movable online command and control infrastructures similar to that used by Phosphorus. In several of those cases, I personally observed that defendants also immediately took action to attempt to defy and evade the court's order as soon as they detected legal action being taken against them.

6. Thus, given Defendants' defiance of this Court's injunctive orders and my past experience with cases with very similar circumstances as those here, it is my belief that even

disclosing that Microsoft has requested a Second Supplemental Preliminary Injunctive Order to disable the domains at Appendix A to that order gives Defendants the opportunity to adapt the command and control infrastructure so that they can continue to perpetrate their unlawful conduct. For this reason, Microsoft respectfully requests that all documents filed in connection with the Second Supplemental Preliminary Injunction be temporarily sealed.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 17th day of July 2019, in San Francisco, California.

A handwritten signature in black ink, appearing to read 'Gabriel M. Ramsey', is positioned above a horizontal line.

Gabriel M. Ramsey

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

**ORDER GRANTING MICROSOFT'S MOTION FOR A PROTECTIVE ORDER
TEMPORARILY SEALING DOCUMENTS**

Before the Court is Microsoft's Motion for a Protective Order Temporarily Sealing Documents. Upon consideration of the Motion, the pleadings filed herein, and the arguments of counsel, the Court finding that the arguments of applicable rules and District of Columbia Circuit precedent are satisfied, that the requested order is the least restrictive means available to protect the interests of Microsoft and the public, and that there is a compelling need to enter a temporary sealing order,

Accordingly, **IT IS HEREBY ORDERED** that the following documents be filed and maintained UNDER SEAL in accordance with Fed. R. Civ. P. 26(c)(1) and Local Civil Rule 5, pending execution of the *ex parte* relief requested in Microsoft's Motion for Second Supplemental Preliminary Injunction Order filed contemporaneous with this Motion:

1. The instant Motion for Protective Order Temporarily Sealing Documents and accompanying documents, including the Brief in support of this Motion;

2. The declaration of Gabriel M. Ramsey in Support of Motion for Protective Order Sealing Documents;
3. Microsoft's *Ex Parte* Motion For Second Supplemental Preliminary Injunction Order and accompanying documents;
4. The Declaration of David Anselmi in Support of Microsoft's *Ex Parte* Motion For Second Supplemental Preliminary Injunction Order and attachments thereto;
5. The Declaration of Hon. Faith Hochberg (Ret.) and attachments thereto;
6. [Proposed] Second Supplemental Preliminary Injunction Order and accompanying documents.

IT IS FURTHER ORDERED that, immediately upon execution of the *ex parte* relief disabling the domains set forth at Appendix A, sought in Microsoft's Motion for Second Supplemental Preliminary Injunction Order, Microsoft shall file with the Clerk of the Court a Notice that the Second Supplemental Preliminary Injunction Order has been executed, and the Clerk of the Court upon receiving such Notice shall file the foregoing documents on the public docket. Microsoft shall be permitted to disclose any such material as deemed necessary to commence its efforts to provide Defendants notice of any further hearings and service of pleadings associated with Microsoft's Motion for Second Supplemental Preliminary Injunction Order.

IT IS SO ORDERED.

Entered this ____ day of July, 2019

Amy Berman Jackson
United States District Judge

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

**MICROSOFT’S MOTION FOR HEARING ON ITS *EX PARTE* MOTION FOR
SECOND SUPPLEMENTAL PRELIMINARY INJUNCTION ORDER**

PLEASE TAKE NOTICE that should the Court find it appropriate to hear oral argument on Microsoft’s *Ex Parte* Motion for Second Supplemental Preliminary Injunction Order, Microsoft respectfully requests oral argument to be set for Friday, July 26, 2019 at 10:00 a.m., or as soon as the matter may be heard.

Dated: July 18, 2019

Respectfully submitted,

/s/ Gabriel M. Ramsey

Gabriel M. Ramsey (*pro hac vice*)

CROWELL & MORING LLP

3 Embarcadero Center, 26th Floor

San Francisco, CA 94111

Telephone: (415) 986-2800

Fax: (415) 986-2827

gramsey@crowell.com

Julia R. Milewski (D.C. Bar No. 1008678)

Justin D. Kingsolver (D.C. Bar. No.

1033806)

Matthew B. Welling (*pro hac vice*)

CROWELL & MORING LLP

1001 Pennsylvania Avenue NW

Washington DC 20004-2595

Telephone: (202) 624-2500

Fax: (202) 628-5116

jmilewski@crowell.com

jkingsolver@crowell.com

mwelling@crowell.com

Richard Domingues Boscovich (*pro hac vice*)

MICROSOFT CORPORATION

One Microsoft Way

Redmond, WA 98052-6399

Telephone: (425) 704-0867

Fax: (425) 936-7329

rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

**MICROSOFT’S *EX PARTE* MOTION FOR SECOND SUPPLEMENTAL
PRELIMINARY INJUNCTION ORDER**

Plaintiff Microsoft Corporation (“Microsoft”), by counsel, pursuant to Federal Rule of Civil Procedure 65(a) and (c), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1116, & 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), the common law, and the All Writs Act, (28 U.S.C. § 1651), respectfully moves the Court for a Second Supplemental Preliminary Injunction Order.

As discussed in Microsoft’s brief in support of this *Ex Parte* Motion for Second Supplemental Preliminary Injunction Order contemporaneously filed and for the same reasons set forth in Microsoft’s Application for an *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction (“TRO Application”), Microsoft originally filed a list of domains on March 19, 2019, filed the first supplement to the list of domains on May 15, 2019, and requests that it be permitted to file this second supplemental list of domains and

subsequently transfer control to Microsoft with the additional new domains being used by Defendants set forth in **Appendix A** to the Proposed Order filed concurrently with this Motion.

As set forth more fully in Microsoft's brief, recent evidence shows that Defendants are again rebuilding Phosphorus' command and control infrastructure in defiance of the Court's authority by bringing on line new domains, which Defendants are using in the same illegal manner and for the same illegal purposes described in the TRO Application. As was the case with the majority of the domains addressed in the Court's TRO, the new domains also abuse Microsoft's trademarks and brands in order to disguise their illegal purpose. Microsoft also respectfully submits that a streamlined procedure is advisable to efficiently and quickly supplement the list of domains subject to the Court's order as soon as Defendants activate the new domains. As set forth more fully in Microsoft's brief, Microsoft requests that the Court appoint a Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to manage this process and relieve the burden on the Court.

The requested relief is necessary to halt the Phosphorus operation that is causing irreparable injury to Microsoft and its customers. Microsoft respectfully requests that the Court grant this Motion.

Dated: July 18, 2019

Respectfully submitted,

/s/ Gabriel M. Ramsey

Gabriel M. Ramsey (*pro hac vice*)

CROWELL & MORING LLP

3 Embarcadero Center, 26th Floor

San Francisco, CA 94111

Telephone: (415) 986-2800

Fax: (415) 986-2827

gramsey@crowell.com

Julia R. Milewski (D.C. Bar No. 1008678)

Justin D. Kingsolver (D.C. Bar. No.

1033806)

Matthew B. Welling (*pro hac vice*)

CROWELL & MORING LLP

1001 Pennsylvania Avenue NW

Washington DC 20004-2595

Telephone: (202) 624-2500

Fax: (202) 628-5116

jmilewski@crowell.com

jkingsolver@crowell.com

mwelling@crowell.com

Richard Domingues Boscovich (*pro hac vice*)

MICROSOFT CORPORATION

One Microsoft Way

Redmond, WA 98052-6399

Telephone: (425) 704-0867

Fax: (425) 936-7329

rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

**BRIEF IN SUPPORT OF MICROSOFT’S *EX PARTE* MOTION FOR SECOND
SUPPLEMENTAL PRELIMINARY INJUNCTION ORDER**

Plaintiff Microsoft Corporation (“Microsoft”) seeks an *Ex Parte* Second Supplemental Preliminary Injunction Order to address Defendants’ continuing efforts to rebuild Phosphorus’ command and control infrastructure and continue their illegal activities in open defiance of both this Court’s Preliminary Injunction Order dated April 12, 2019 and Supplemental Preliminary Injunction Order dated May 22, 2019. Microsoft expresses its appreciation for the continued attention of the Court to this ongoing cyber-security matter given Defendants’ continued defiance of this Court’s orders.

Microsoft incorporates by reference herein the arguments and evidence set forth in its Brief In Support Of Microsoft’s Application for an *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction (“TRO Application”), Dkt. No. 3-1, and in its prior Brief in Support of Microsoft’s *Ex Parte* Motion to Supplement Preliminary Injunction Order, Dkt. No. 19-6. As discussed in Microsoft’s TRO Application, the domains used in Phosphorus’ command and control infrastructure are critical to Phosphorus’ operation. The most

effective way to disable Phosphorus' operation is to disable the Internet domains used by John Does 1-2 ("Defendants").

I. BACKGROUND

On March 15, 2019, the Court granted an Emergency *Ex Parte* Temporary Restraining Order ("TRO") tailored to halt the illegal activities and the growth of the Phosphorus operation. Dkt. 11. Through the Phosphorus operation, Defendants lure victims into clicking on links embedded in personalized e-mails thereby compromising their computers, computer networks and accounts hosted on Microsoft's servers, all with the goal of stealing the victims' sensitive data. Defendants cause great harm to Microsoft by damaging the products that Microsoft licenses to its customers. Further, by exploiting Microsoft's famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, Defendants cause Microsoft irreparable reputational and other harms for which no monetary recourse is available.

As explained in Microsoft's TRO Application, Defendants conduct their illegal operations by using an online command and control infrastructure consisting of a set of websites and domains. Dkt. No. 3-1 at 2. These domains are used both to break into computers and networks of the organizations that Phosphorus targets, control the reconnaissance of those networks, and, ultimately, exfiltrate sensitive information from them. To disable this command and control infrastructure, this Court ordered that these Phosphorus-controlled Internet domains, listed in the **Appendix A** be redirected to secure Microsoft servers. Dkt. 14. On April 12, 2019, the Court converted the TRO into a Preliminary Injunction. Dkt. No. 18. On May 22, 2019, Microsoft moved, and was granted, a supplemental preliminary injunction to capture a supplemental Appendix A with additional domains. Dkt. 21.

Executing the Court's Temporary Restraining Order and Preliminary Injunction Orders,

Microsoft cut communications between Defendants’ existing command and control infrastructure and the victim computers and networks that Defendants attacked and from which Defendants had been stealing information. Declaration of David Anselmi In Support Of Microsoft’s Motion for Second Supplemental Preliminary Injunction Order (“Anselmi Decl.”) ¶ 32, attached as **Exhibit 1** to this Brief. This effectively stymied Defendants’ efforts to exploit the computers and networks they had targeted or already broken into.

However, Defendants, who are evidently resourceful and well-funded, continue to try to maintain and reestablish new command and control domains and other command and control infrastructure so that they can continue their illegal activities. Indeed, this probability was foreseen by the Court in issuing its TRO. And as foreseen, following the execution of the TRO and Preliminary Injunction, Defendants openly defied this Court and started to rebuild their command and control infrastructure by adding new Internet domains to Phosphorus’ command and control infrastructure. *Id.* ¶¶ 9, 14. This Court then issued a Supplemental Preliminary Injunction Order allowing Microsoft to redirect 11 new Phosphorus-controlled domains to Microsoft secure servers. Dkt. 21. Yet, Defendants continue to defy this Court’s orders. Consequently, Microsoft is asking the Court to allow it to redirect six new Phosphorus-controlled domains to Microsoft secure servers. Anselmi Decl. ¶ 9. This will disrupt Defendants’ recent illegal activity. A list of the new domains used by Defendants is provided in the **Appendix A** to the Proposed Order filed concurrently with this brief.

In addition, Microsoft respectfully submits that a streamlined procedure is advisable to efficiently and quickly supplement the list of domains subject to the Court’s order as soon as Defendants activate the new domains. As set forth more fully in Microsoft’s brief, Microsoft recommends that the Court appoint a Court Monitor, pursuant to Federal Rule of Civil Procedure

53, to manage this process and relieve the burden on the Court.

II. ARGUMENT

A. **There Is Good Cause to Supplement the Preliminary Injunction Order**

Microsoft seeks to again supplement the Preliminary Injunction Order by including the domains in **Appendix A** to the Proposed Order submitted with this motion to the prior list of domains transferred to Microsoft pursuant to the Court's prior injunctive relief. This will allow Microsoft to disrupt Defendants more recent illegal activity. Such supplemental relief has been granted in prior cases when defendants began using new domains after the court granted a temporary restraining order. *See Microsoft Corp. v. John Does 1-8*, Case No. 1:14-cv-00811-LOG-TCB (E.D. Va. 2014) (O'Grady, J.) at Dkt. No. 32 (disabling the "Shylock" botnet).

Here, absent the requested relief, Microsoft and its customers will continue to be irreparably harmed for the reasons detailed in Microsoft's prior submissions. Microsoft is likely to succeed on the merits, because the domains at issue in this motion are used for the same unlawful purposes and in the same unlawful manner set forth in Microsoft's previous motion for TRO and Preliminary Injunction. Anselmi Decl. ¶¶ 9, 14. Thus, pursuant to Federal Rule of Civil Procedure 65, disabling the additional six domains at issue is necessary to prevent harm to Microsoft and its customers.

With respect to this Second Supplemental Preliminary Injunction Order, ex parte relief is essential. If notice is given prior to issuance of the requested relief, it is likely that Defendants will be able to quickly mount an alternate command and control structure because Defendants have the technical sophistication and ability to move their malicious infrastructure. Anselmi Decl. ¶¶ 33, 34. Thus, providing notice of the requested ex parte relief will undoubtedly facilitate efforts by Defendants to continue to operate Phosphorus. Rule 65 of the Federal Rules of Civil Procedure permits ex parte injunctive relief where the moving party sets forth facts that

show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70*, 415 U.S. 423, 438–39 (1974) (“Ex parte temporary restraining orders are no doubt necessary in certain circumstances....”). It is well established that ex parte relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 73–74 (D.D.C. 2009) (granting ex parte TRO); *In re BAE Sys. PLC Derivative Litig.*, No. 07-1646, 2008 WL 458575, at *1 (D.D.C. Feb. 5, 2008) (granting ex parte TRO to enjoin party from selling U.S.-based assets allegedly acquired with bribe payments); *AT&T Broadband v. Tech Commc’ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming ex parte search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice was given); *Allscripts Misys, LLC v. Am. Dig. Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting ex parte TRO where “Defendant may dissipate the funds and/or take action to render it difficult to recover funds”); *Crosby v. Petromed, Inc.*, No. CV-09-5055, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as “notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs....”); *Little Tor Auto Ctr. v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (ex parte TRO appropriate where contraband “may be destroyed as soon as notice is given”).

As before in this matter, immediately upon execution of the Second Supplemental Preliminary Injunction Order and disablement of the additional domains, Microsoft will provide robust notice to Defendants. Microsoft will provide Defendants the documents associated with this motion and the Court’s order, by sending them to all of Defendants’ contact information

associated with the subject domains, thus providing notice and an opportunity to appear and contest the requested relief, if Defendants so choose.

B. An Ongoing Process Is Needed to Efficiency and Effectively Curtail Defendants' Efforts to Rebuild Phosphorus' Command and Control Infrastructure.

Microsoft seeks to supplement the Preliminary Injunction Order by establishing a streamlined procedure, assisted by a court-appointed monitor, to respond to new malicious domains registered by Defendants in violation of the injunction, as set forth more fully in the Second Supplemental Injunction Order submitted with this motion.

Defendants are persistent in their activities and are likely to attempt to maintain, rebuild, and even grow, their capabilities again and again. Microsoft will, as it has up until now, monitor Defendants' activities, identify new Phosphorus command and control domains associated with Microsoft trademarks or brands ("Phosphorus Domains") as they are activated, and will seek additional supplemental relief from the Court. Consequently, Microsoft and the Court face the prospect that enforcing the Court's order will require multiple ongoing rounds of amendments to the list of command and control domains subject to the Court's preliminary injunction order and multiple new proceedings. Failing this sustained effort, Defendants will continue their malicious and illegal activities, causing irreparable injury to Microsoft, its customers and the public.

Anselmi Decl. ¶ 32.

However, Microsoft acknowledges the burden that such a sustained effort will place on the Court. Microsoft therefore respectfully submits that a streamlined procedure is advisable to efficiently and effectively supplement the list of domains subject to the Court's order as soon as Defendants activate the new domains. In brief, Microsoft requests that the Court appoint a Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to manage this process and relieve the burden on the Court. The availability of a Court Monitor to oversee this process also increases

the effectiveness of the Court's prior injunctive orders, as it will enable a more prompt, continuous response to Defendants' continued violation of the orders. The Court Monitor will make determinations on any disputes between Microsoft, any Defendant, registry or other third party, regarding disabling of Phosphorus Domains set forth in the Proposed Order. The Court Monitor will further determine (based on evidence submitted by Microsoft) whether additional domains are in fact being used by Defendants as part of Phosphorus and may order that such new domains be added to the list of domains subject to the Court's injunctive orders. The Court Monitor will also monitor Defendants' compliance with the Court's orders.

Under Federal Rule of Civil Procedure 53(a)(1)(C), a court may appoint a court monitor to "address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge of the district." A court monitor is necessary here. For the Court to rule on continuous, repeated, potentially frequent motions to amend the Preliminary Injunction Order every time Defendants register and use new Phosphorus Domains leveraging Microsoft trademarks would impose an undue burden on the Court's limited time and resources. This is especially the case considering the ease and speed with which Defendants are currently registering Microsoft-related domains to continue their attacks. Further, the ability of a court monitor to make determinations on such matters will increase the effectiveness of the Court's existing injunctions and permit enforcement of Defendants' compliance on an ongoing basis. Courts have frequently made use of court-appointed monitors and other masters in cases such as this one, where ongoing compliance with the court's orders is at issue and supervision would be too time-consuming or difficult for the court to undertake without assistance. *See e.g., Ohio Valley Envtl. Coal. v. Fola Coal Co., LLC*, No. 2:13-21588, 2016 U.S. Dist. LEXIS 73904, at *50 (S.D. W. Va. June 7, 2016) ("Appointing a special master is proper in this case because

the proposed injunctive relief includes complex analysis and implementation of environmental engineering plans and monitoring to correct [defendant's] violations.”); Order, *Microsoft Corp. v. John Does 1-2*, Civil Action No. 1:16-cv-993 (E.D. Va. Dec. 6, 2016) (appointing a court monitor to resolve disputes relating to “Strontium Domains”); *Schaefer Fan Co. v. J & D Mfg., Inc.*, 265 F.3d 1282 (Fed. Cir. 2001) (appointing special master to resolve disputes and issue decisions regarding compliance with settlement agreement); *Evans v. Fenty*, 701 F. Supp. 2d 126, 129 (D.D.C. 2010) (Special Masters assisted court by making findings and recommendations that addressed defendants’ compliance and options for curing identified deficiencies); *see also* 18 U.S.C. § 1836(b)(2)(D) (providing that special masters may be appointed to locate and isolate trade secret information from other property).

As the first step in the streamlined process in the Second Supplemental Injunction Order, Microsoft will monitor Defendants’ activities and will identify new Microsoft related Phosphorus Domains as Defendants activate them. Making an accurate identification is crucial, and Microsoft will base its conclusions on a set of criteria developed over the course of its lengthy investigation into Defendants and Phosphorus. Anselmi Decl. ¶35. The following are factors Microsoft considers within its framework:

1. ***Presence of Distinctive Malware:*** Defendants typically use a relatively small set of distinctive malware that can be distinguished from other types of malware. *Id.* ¶ 36. The specific types of malware known to be used by Defendants are listed in Exhibit 2 to David Anselmi’s Declaration. If the malware used in a new attack matches or is a similar variant of the distinctive malware used by the Defendants in past attacks, it indicates that the actors behind the new attack are the Defendants. *Id.* at ¶37. Because Phosphorus malware is reasonably distinctive, domains that are used to deliver the Phosphorus malware to targeted victims or communicate with the Phosphorus malware already installed on victims’ networks are strongly implicated as Phosphorus domains. *Id.* The presence of this distinctive malware therefore serves as a reliable indicator that Defendants are using the Internet domain at issue. *Id.*
2. ***Pattern in Domain Registration:*** If the registration information associated with a newly identified Internet domain closely matches the pattern associated with the

domains registered by the Defendants in the past, it is a strong indicator that the Defendants are behind the registration of the new domain. *Id.* ¶38. Microsoft has identified patterns in the registration information provided by Defendants when registering the domains used in their illegal activities. *Id.* Microsoft considers such things as the e-mail address and phone number provided by the registrant, the hosting service designated, the name servers used, the IP address(es) and other technical details associated with the domain. *Id.* Exemplary registration information associated with Internet domains registered by Defendants in the past is included in Appendix A to the Proposed Order filed concurrently with this brief.

3. ***Tactics Used During a New Attack:*** Where the tactics used in a new attack match the tactics favored by Phosphorus Defendants in past attacks, it is an indication that the Defendants are behind the new attack. *Id.* ¶ 39. For example, Phosphorus Defendants often send phishing e-mails to victims in which the e-mail purports to be a notification from Microsoft regarding an unauthorized access to the recipients' Microsoft account, and requesting that she or he reset the account credentials. *Id.* ¶ 13. If the victim clicks on the embedded "Change Password" button in the phishing e-mail, the victim will be connected to a Phosphorus-controlled website which will attempt to induce the victim to enter his account credentials. *Id.* Other tactics favored by the Phosphorus Defendants include remote code execution through browser drive-by, remote code execution through malicious attachments, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on. *Id.*
4. ***Specific Targeted Victims:*** The Phosphorus Defendants tend to target a particular type of victim and attempt to steal particular types of information. *Id.* ¶ 40. Therefore, Microsoft can use information about the intended victim to help determine whether or not Defendants are involved in the new attack. *Id.* For example, Phosphorus continues to target political dissidents, activist leaders, religious organizations, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. *Id.* Where an Internet domain is associated with an attack on these particular types of targets, it is a factor that is consistent with the known activity and objectives of the Defendants.
5. ***Use of Microsoft Marks and Brands or Confusingly Similar Variants:*** The use of Microsoft trademarks and brand names or slight misspellings or variants of those trademarks or brand names in the domain name, alone or in combination with other terms, or generalized versions suggestive of Microsoft's services, is an indicator that the domain is associated with Phosphorus. The Phosphorus Defendants have used Microsoft trademarked brands or slight misspellings of those brands in the names of the domains that they register for their illegal activity. *Id.* ¶ 41. Defendants may also use generalized versions of terms that are suggestive of Microsoft's services, but do not specifically use a trademark, but nonetheless target Microsoft services and users. *Id.* Defendants use this technique to disguise the illegal nature of their conduct from the intended target.

Id. By studying the ways in which the Defendants have incorporated Microsoft's trademarks and brand names, or generalized versions of indicators of Microsoft's services, into domain names that Defendants have used in the past, Microsoft is able to identify domain names that Defendants use in the future. *Id.* ¶ 16.

Under Microsoft's proposal, when Microsoft determines that Defendants have activated a new Microsoft related Phosphorus Domain, the disposition of that domain, which is alleged to meet the articulated criteria to constitute Microsoft related Phosphorus Domains, and domains that are alleged to be Phosphorus Domains based on new criteria, Microsoft shall submit a written motion to the Court Monitor seeking a declaration that such domains are Phosphorus Domains. The Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Phosphorus Domains, again, subject to the right to judicial review.

Microsoft believes this process will reduce the burden on the Court, better ensure enforcement of the Court's orders, provide for efficient reaction against Defendants as they attempt to activate new domains for illegal ends, and provide an adequate mechanism for registries, third-parties, or Defendants to challenge the substance and process concerning enforcement of the injunction. Thus, the appointment of a court monitor in this case is appropriate under Federal Rule of Civil Procedure 53(a)(1)(C).

If the Court is amenable to appointment of a Court Monitor to oversee ongoing enforcement of the injunction, Microsoft respectfully requests the Court's recommendations concerning potential candidates for this role. In order to assist the Court, Microsoft proposes Hon. Faith Hochberg (Ret.) to serve as the Court Monitor. Judge Hochberg has relevant legal and technical expertise and has served in the capacity as a neutral special master in prior matters, including specifically matters involving cybercrime, having been appointed a Court Monitor in a similar prior matter. *See Microsoft Corp. v. John Does 1-2*, Civil Action No. 1:16-cv-993 (E.D.

Va. Dec. 6, 2016). Any Court Monitor must establish that there are no conflicts of interest and provide an affidavit “disclosing whether there is any ground for disqualification under 28 U.S.C. § 455.” A declaration of the foregoing candidate for the role of Court Monitor, including current curriculum vitae, is submitted concurrently with this motion, for the Court’s consideration. *See* Declaration of Hon. Faith Hochberg, attached as **Exhibit 2** to this Brief.

III. CONCLUSION

For the reasons set forth in this brief, the Anselmi Declaration submitted with this brief, and based on the evidence submitted with the prior Application for TRO and Preliminary Injunction, Microsoft respectfully requests that the Court grant Microsoft’s Motion for Second Supplemental Preliminary Injunction Order.

Dated: July 18, 2019

Respectfully submitted,

/s/ Gabriel M. Ramsey

Gabriel M. Ramsey (*pro hac vice*)

CROWELL & MORING LLP

3 Embarcadero Center, 26th Floor

San Francisco, CA 94111

Telephone: (415) 986-2800

Fax: (415) 986-2827

gramsey@crowell.com

Julia R. Milewski (D.C. Bar No. 1008678)

Justin D. Kingsolver (D.C. Bar. No. 1033806)

Matthew B. Welling (*pro hac vice*)

CROWELL & MORING LLP

1001 Pennsylvania Avenue NW

Washington DC 20004-2595

Telephone: (202) 624-2500

Fax: (202) 628-5116

jmilewski@crowell.com

jkingsolver@crowell.com

mwelling@crowell.com

Richard Domingues Boscovich (*pro hac vice*)

MICROSOFT CORPORATION

One Microsoft Way

Redmond, WA 98052-6399

Telephone: (425) 704-0867

Fax: (425) 936-7329

rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.

EXHIBIT 1

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**DECLARATION OF DAVID ANSELMi IN SUPPORT OF
MICROSOFT'S EX PARTE MOTION TO SUPPLEMENT PRELIMINARY
INJUNCTION ORDER**

I, David Anselmi, declare as follows:

1. I am a Principal Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Microsoft's Ex Parte Motion to Supplement Preliminary Injunction Order. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my current role at Microsoft, I assess technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft's customer-facing online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting Microsoft's corporate resources from network-based attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager

performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 years reserve), attaining the rank of Lieutenant Colonel. I have been employed by Microsoft since February 1997.

I. OVERVIEW OF INVESTIGATION INTO PHOSPHORUS AND CONCLUSIONS

3. My declaration concerns an organization that is engaged in systematic criminal activity on the Internet. Because the identities of the individuals behind the activity addressed in this declaration are unknown, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: “Phosphorus.” Others in the security community who have researched this group of actors refer to the group by other names, including “APT 35,” “Charming Kitten,” and “Ajax Security Team.” The defendants have been linked to an Iranian hacking group or groups. I have investigated the infrastructure described in this declaration and have determined that the defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. Defendants have registered domains using functioning email addresses by which they communicated with domain registrars in order to complete the registration process.

4. Microsoft investigators have been monitoring and gathering information on the Phosphorus defendants. In the course of such investigation, I have been working with and directing a team that (1) engaged in the analysis and creation of “signatures” (which can be thought of as digital fingerprints) for the infrastructure used by the Phosphorus defendants, (2) discovered login activity into Microsoft services from Phosphorus-controlled infrastructure on the Internet, (3) matched reported Phosphorus phishing email campaigns to registered domains, (4) monitored domain registrations associated with the Phosphorus-controlled email addresses and other pertinent WHOIS record information, (5) monitored infrastructure frequently utilized by the Phosphorus defendants in order to identify new domains being registered by the Phosphorus defendants, (6) have confirmed resolution settings to particular Internet service

providers (ISPs) which have frequently been used by the Phosphorus defendants in the past, and (7) reviewed peer findings and public reporting on the Phosphorus defendants.

5. As alluded in paragraph 4 (1), the investigative team has developed methods to help us identify new domains registered by the Phosphorus actors. Particular features of the Phosphorus infrastructure have been identified and patterns of content, non-content, and technical features have been determined to be exclusively and specifically associated with the Phosphorus defendants. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Phosphorus domain. Each such domain is manually reviewed in detail by one or more subject matter experts as necessary to ascertain whether it is, in fact, a Phosphorus domain. Based on this analysis, we have identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the defendants.

6. Based on our investigation and analysis, Microsoft has determined that the Phosphorus defendants specialize in targeting and stealing credentials of prominent users of the Internet. The Phosphorus defendants target Microsoft and non-Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. Based on our research, the Phosphorus defendants have targeted Microsoft customers, political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East.

7. The Phosphorus defendants' objectives appear to be obtaining account credentials to later retrieve sensitive communications within the accounts. We believe that the Phosphorus defendants have been active since 2013 and continue to pose a threat today and into the future.

II. PHOSPHORUS' METHOD OF COMPROMISING AND STEALING INFORMATION FROM VICTIMS

8. The Phosphorus defendants typically attempt to compromise the personal (not work) accounts of the targeted individuals through a technique known as "spear phishing."

Spear phishing attacks are conducted in the following fashion: after researching a victim organization, the spear phisher will identify individuals associated with that organization through gathering publicly available information and by social engineering. The spear phisher will then initiate communications with the victim by using names, companies, and/or contents that are familiar to the victim. The ensuing communications exchanges are used to social engineer information, identify additional targets, entice a target into opening up a malicious attachment, and more. Microsoft has observed fake social networking profiles being created by Phosphorus defendants which would obviously present significant leverage in carrying out such an attack.

9. Another technique utilized by the Phosphorus defendants is to send a targeted individual an email specifically crafted to appear as if there is an issue with the targeted individual's account. Phishing emails often use generic domain names that appear to be tied to account activity and that require input of credentials for authentication. For example, domains such as service-accountrecovery.com. The Phosphorus defendants send the targeted individual an email citing an account problem as mentioned above, and which instructs the recipient to proceed to a (fake) website where they should login to remedy the situation. Through research and investigation:

a. Microsoft has determined that the Phosphorous defendants have used domains cited in **Exhibit 1** to this declaration (also attached as **Appendix A** to the Proposed Order). Sometimes, the Phosphorus defendants have created domains including Microsoft (or other) product names. At other times, as is presently the case, the defendants disguise their command and control domains by using terms that make them appears to be related to online services. In the domains at **Exhibit 1**, the Phosphorus defendants have incorporated terms such as "mail" or account "login" and "supports" and similar terms. The purpose of these formulations is to create the appearance of legitimate online services and to ultimately present content on the pages that mimic login pages that infringe Microsoft trademarks, such as Microsoft's "Outlook" or "Office 365" services and brands, or other confusing content.

b. Since the Preliminary Injunction Order and subsequent Supplemental

Injunction Order, Microsoft has identified an additional six domains that the Phosphorous defendants have registered that follow the same patterns and are no doubt intended to be leveraged in phishing attacks. These domains are listed in **Exhibit 1** and are also reflected in **Appendix A** to the Proposed Order.

10. The Phosphorus defendants create these domains with the purpose of ultimately including on the websites content that infringes Microsoft or other trademarks and with the purpose of confusing victims into clicking on links controlled by the Phosphorus defendants. When the user clicks on the links, they are taken to deceptive web pages that induce the victim to type in their Microsoft or other credentials, at which point the Phosphorus defendants obtain access to those credentials. This will result in the threat actors being able to log into the victim's account and gain access to whatever content is available on the legitimate service, which may include their email, address information, phone numbers, billing information, etc. Where available, the Phosphorus defendants can also download a copy of the victim's address book to be used for future targeting of additional intended victims. Not having safe emails impacts Microsoft's brands and services. Having personal information stolen by attackers impacts a customer's trust in the services being provided. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises for which they work, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

11. The Phosphorus defendants send these emails from a variety of online email services. As discussed above, there are domains created by the Phosphorus defendants with the ultimate goal of mimicking Microsoft brands, and those domains are clearly designed to be included in spear phishing emails as links to websites that the Phosphorus defendants have set up in advance and which they control. When a victim clicks on the link in the email, his or her computer is connected with the Phosphorus-controlled website. The victim is then presented a copy of a webpage that appears to be a login page for a webmail provider of which the victim is

a subscriber. In fact, this is a fake login page that is designed to induce the user to type in their webmail credentials. If the victim enters the correct credentials, at that point the Phosphorus actors obtain the user's credentials and can thereafter access the user's webmail account to steal email content and other information.

12. **Figures 1 and 2** below show copies of such webpages created by the Phosphorus defendants, designed to look like legitimate Microsoft Outlook login pages:



Figure 1

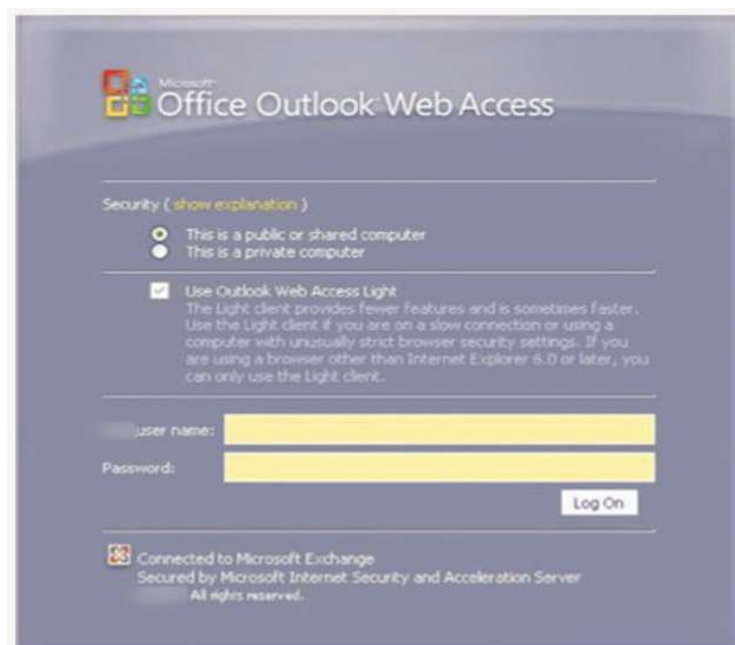


Figure 2

13. Phosphorus targets other brands beyond Microsoft and purport to be password reset or account login pages of other companies. For example, the Phosphorus defendants use fake emails instructing users to click links and type in credentials, fake “Verify” buttons prompting users to type their credentials into fraudulent login pages and fake “Sign in” pages instructing users to enter their user name and password. All of these methods are designed to induce users to type in credentials. As seen above with respect to the fake Microsoft login pages inviting users to type in their Microsoft Outlook “User name” and “Password,” this scheme is typical of the Phosphorus defendants’ activities. **Figures 3** through **4** are further examples of this tactic:

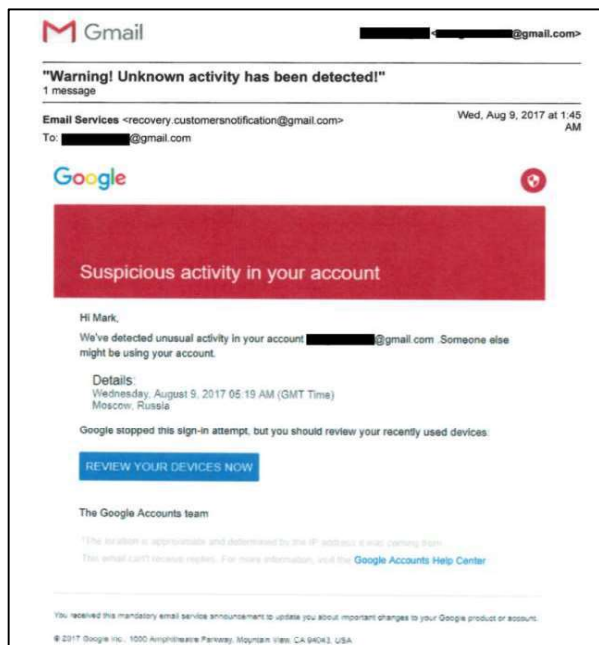


Figure 3

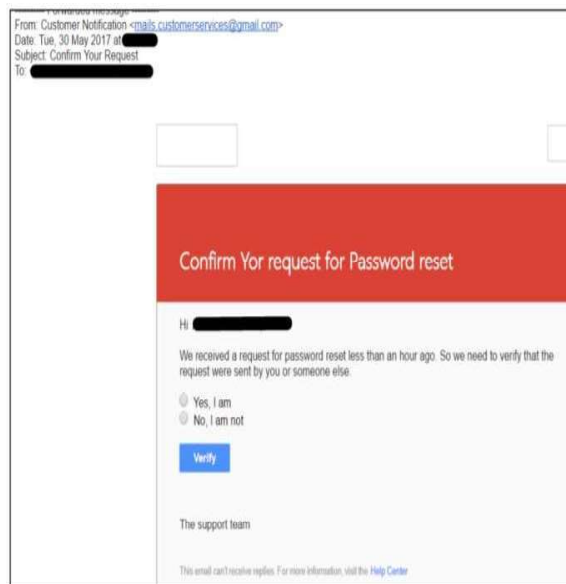


Figure 4

14. Defendants continue to target Microsoft and its users with new content. **Figures 5** and **6** are two recent examples of Defendants’ efforts to prompt users to type their credentials into fraudulent login pages:

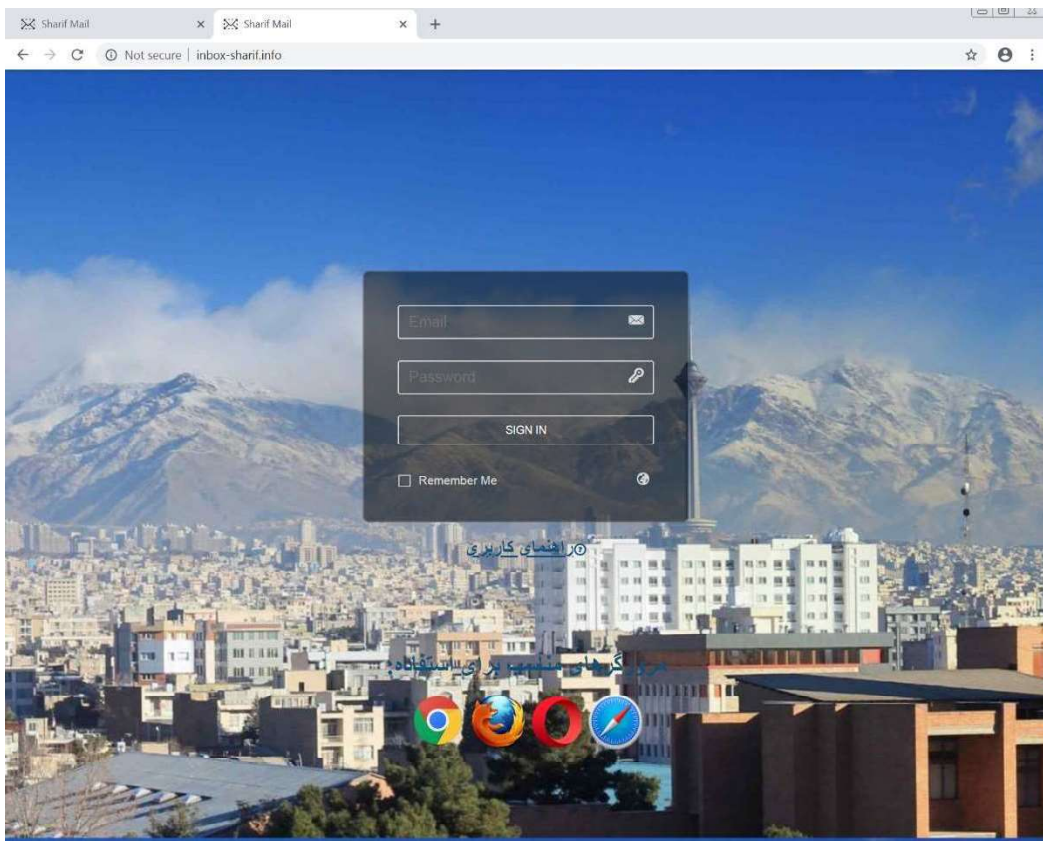


Figure 5

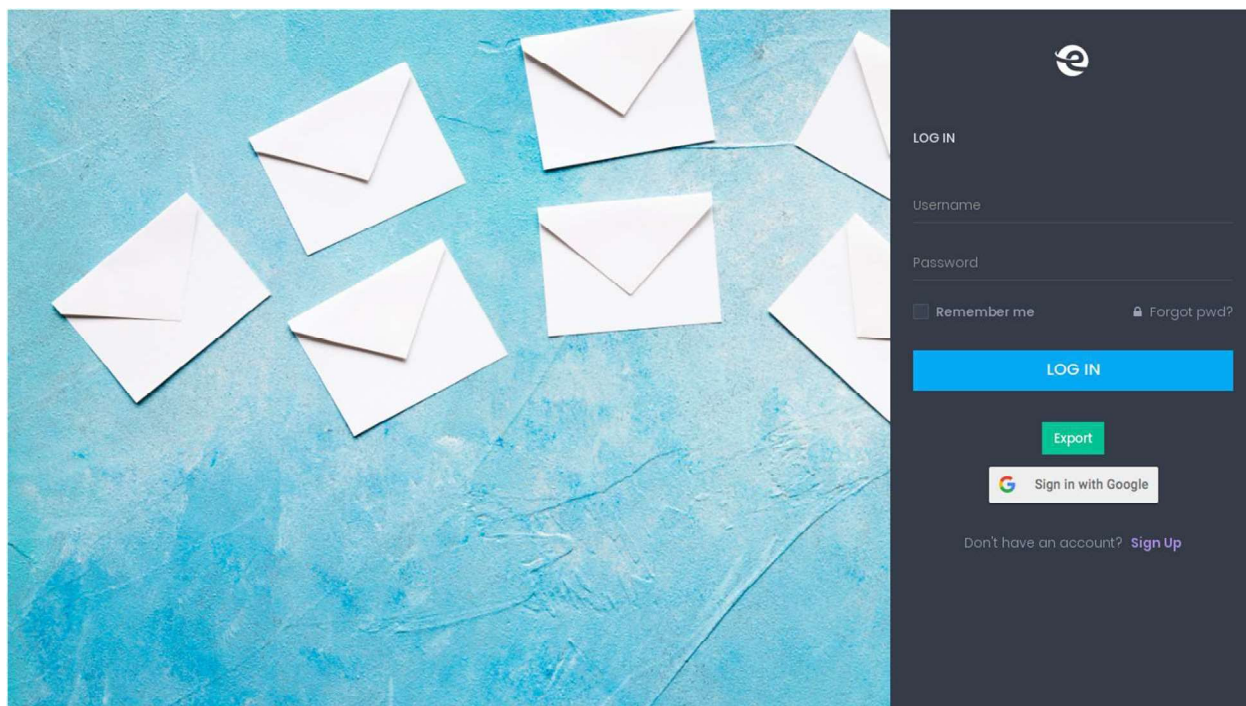


Figure 6

15. Upon successful compromise of a victim account, the Phosphorus defendants will not only be able to log into the account and review the victim's emails, but may also delete the spear phishing email that they previously sent to the user in an attempt to obfuscate their activities.

16. The Phosphorus defendants have targeted victims who are using Microsoft email services, and Microsoft investigators, by inspecting login history, have confirmed that Phosphorus defendants have intruded into those accounts potentially to steal information of Microsoft's users. **Figures 1 and 2** above demonstrate the Phosphorus defendants targeting users of Microsoft's Outlook email services.

17. Microsoft investigators were also able to locate the control panel used by the Phosphorus defendants to create links sent to intended victims as well as to track successfully compromised victims who clicked on those links, typed in their credentials and had those credentials stolen by the defendants. Microsoft analysts identified the Phosphorus domain confirm-session-identification.info which led to discovery of the control panel URL. This control panel was accessed by a URL that was open and required no authentication. The control panel that the Phosphorus defendants used to monitor and control their access to victim accounts was present on the domain: confirm-session-identification.info. The domain confirm-session-identification.info was registered on 10/17/2018 as seen in the WHOIS record from a commonly used domain research tool called Domaintools.com. This record is reflected in **Figure 7**:

```
Domain Name: CONFIRM-SESSION-IDENTIFICATION.INFO
Registry Domain ID: D503300000240279653-LRMS
Registrar WHOIS Server:
Registrar URL: https://www.onlinenic.com
Updated Date:
Creation Date: 2018-10-17T11:27:08Z
Registry Expiry Date: 2019-10-17T11:27:08Z
Registrar: Registration Expiration Date:
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Domain ID Shield Service CO., Limited
Registrant State/Province: Hong Kong
Registrant Country: CN
Name Server: NS1.DNS-DIY.NET
Name Server: NS2.DNS-DIY.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/

The Registrar of Record identified in this output may have an RDDS service that can be queried for addit
```

Figure 7

18. The domain confirm-session-identification.info resolved to IP address 190.2.154.35 (Netherlands) from October 18th – 20th, 2018 and then moved to IP address 104.27.134.98 (US). The control panel below was obtained from the confirm-session-identification.info domain, when hosted on 104.27.134.98, on 11/04/2018. When visiting the URL <http://confirm-session-identification.info/recovery/> on 11/04/2018 the control panel did not require authentication to view its contents. Upon visiting this URL on 11/04/2018, we confirmed that the Phosphorus defendants use a unique ID (URL) for each targeted user. A redacted list of the users targeted can be seen in the email column in **Figure 8** below.

URL	email	Disable/Enable	operations
http://confirm-session-identification.info/recovery/url.php?url=84eivvutpp0d5f9nlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://51.38.87.64/recovery/url.php?url=a88eipktrivbdpurlflogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=ntentiaes5.3ntvnyuswlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=hp24u83oakb562aqdlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com.au	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=ky1ekkkqprrove7c72login.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=bsx286ahn1exy8n0ogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=ixvsopect1(wehfykrlblogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=umwq8y8v1nfrvqd01login.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=lm3cp7ztgbrmxxkgerziclogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://51.38.87.64/recovery/url.php?url=y4ed941648a6m=fg0qlogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit
http://confirm-session-identification.info/recovery/url.php?url=qp3oempx6m56nm6flogin.srctpxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	☒	copy delete edit

Figure 8

19. The Phosphorus defendants' email panel has a "Monitor" screen for tracking compromised users. As seen in the screenshot below (**Figure 9**), there is at least one victim observed at the time of accessing the unauthenticated email panel:

Target Email	Auth Type	Auth Result	Date and Time	password/code
[REDACTED]@yahoo.com			2018-10-25 01:56:36	

User Agent	IP	country	city
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36	38.122.191.174	United States	America/New_York

Figure 9

20. Additionally, the settings tab (**Figure 10**) shows that when users' credentials are compromised, the credentials stolen from Microsoft users and others are emailed to the Yahoo account soup_mctavish@yahoo.com with the subject line "Yahoo-Pishing." Note here that the Phosphorus defendants misspelled "Phishing."

Admin

https://confirm-session-identification.info/recovery/setting_page.php

KLOROFIL

- Dashboard
- Monitor
- Settings**
- Manage Database
- Logout

Email Name reporter

[REDACTED]@yandex.com

Email Password reporter

[REDACTED]

Reporter Name

Yahoo-Pishing

Email Name Reiciver

soup_mctavish@yahoo.com

Reporter Subject

Yahoo-Pishing

Redirect Page

http://www.yahoo.com

save

Figure 10

21. The Phosphorus defendants also intrude upon and cause injury to Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers. In particular, the Phosphorus defendants have sent deceptive email messages to victims, such as those discussed above, which include links to websites from which the defendants install malicious software onto the victims' computers. The defendants refer to the malicious software as "Stealer." Stealer, once installed, can record what the victim types on their keyboard, take screenshots of what is on the victim's computer screen, steal login credentials for instant messaging account (including information about victims' Microsoft-owned "Skype" messaging accounts), email accounts, and other credentials. The Stealer software is installed from, and stolen information may be transferred to, defendants using command and control domains such as those reflected in **Exhibit 1**.

22. The installation of this malicious software damages the victim's computer and the Windows operating system on the victim's computer. During the infection of a victim's computer, the malicious Stealer software makes changes at the deepest and most sensitive levels of the computer's Windows operating system. The consequences of these changes are that the user's version of Windows is essentially adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users. For example, the defendants create registry key paths bearing the Microsoft "Windows" trademark, within the Microsoft operating system, including, among others:

"C:\WINDOWS\system32\rundll32.exe" "C:\ Documents and Settings\{USER}\ApplicationData\IntelRapidStart\AppTransferWiz.dll",#110

23. Further, as seen in **Figure 11** below, the Phosphorus defendants include metadata within the Stealer malicious software that expressly misrepresents that the software is created by "Microsoft" and that the software is a "Process for Windows."

File Version Information	
Copyright	Copyright © 2013
Product	Process for Windows
Description	Process for Windows
Original Name	Stealer.exe
Internal Name	Stealer.exe
File Version	1.0.0.0
Comments	Process for Windows

ExifTool File Metadata ⓘ	
AssemblyVersion	1.0.0.0
CharacterSet	Unicode
CodeSize	224256
Comments	Process for Windows
CompanyName	Microsoft
EntryPoint	0x38b1e
FileDescription	Process for Windows
FileFlagsMask	0x003f
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.0.0.0
FileVersionNumber	1.0.0.0
ImageFileCharacteristics	Executable, 32-bit
ImageVersion	0.0
InitializedDataSize	2048
InternalName	Stealer.exe
LanguageCode	Neutral
LegalCopyright	Copyright 2013
LinkerVersion	11.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0

Figure 11

III. PHOSPHORUS HAS ATTACKED MANY MICROSOFT CUSTOMERS IN THE DISTRICT OF COLUMBIA AND AROUND THE WORLD

24. Through its investigation, Microsoft has determined that the Phosphorus defendants have targeted Microsoft customers in the District of Columbia and continue to target our customers throughout the United States on multiple occasions.

IV. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

25. Phosphorus irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system and Outlook, Hotmail, OneDrive and Office 365 email and cloud services, as well as a variety of other software and services. Microsoft is the owner of the “Microsoft,” “Windows,” “Outlook,” “Windows Live,” “Hotmail,” “OneDrive” and “Office 365” trademarks. Microsoft has invested substantial resources in developing high-quality products and services. Microsoft has also invested, through its subsidiaries, in high value brands and services such as the “LinkedIn” brand and service. Due to the high quality and effectiveness of Microsoft’s products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and service and its brand, including the trademarks listed above.

26. Microsoft’s customers whose email accounts are compromised through the defendants’ credential theft are damaged by these activities. Similarly, Microsoft’s customers whose computers are infected with the malicious Stealer software are damaged by changes to Windows, which alter the normal and approved settings and functions of the user’s operating system, destabilize it, and enable unauthorized monitoring of the user and theft of user data.

27. In effect, once infected, altered and controlled by the Stealer software, the Windows operating system ceases to operate normally and is now a tool of deception and theft aimed at the owner of the infected computer. Yet they still bear the Microsoft Windows trademark. This is obviously meant to mislead Microsoft’s customers, and it causes extreme damage to Microsoft’s brands and trademarks.

28. Customers are usually unaware of the fact that their email accounts are compromised, that their computers are infected, that they are being monitored by the defendants

or that sensitive information is being stolen from them. Even if aware of an account intrusion or an infection of their computer, users often lack the technical resources or skills to resolve the problem, allowing their accounts and computers to be misused indefinitely, as manual steps to change account credentials or remove the malicious software may be difficult for ordinary users. They may be futile to a degree too where the Phosphorus defendants have software installed to observe the victim's activities and attempts to remediate the intrusion. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. This demonstrates the extreme problems that the activities of the Phosphorus defendants cause for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the defendants' intrusion into accounts and computers.

29. The activities of the Phosphorus defendants injure Microsoft and its reputation, brand, and goodwill. Users subject to the negative effects of the Phosphorus defendants' spear phishing emails sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. There is a great risk that Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

V. DISRUPTING PHOSPHORUS' ILLEGAL ACTIVITIES

30. The Phosphorus defendants' illegal activities will not be easy to disrupt. Evidence indicates that the Phosphorus defendants are highly sophisticated, well-resourced, organized, and patient. The Phosphorus defendants specialize in targeting individuals in organizations holding sensitive data, by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their credentials, and disguising its activities using the names and trademarks of Microsoft and other legitimate companies.

31. The most vulnerable point in the Phosphorus defendants' operations are a number of Internet domains through which the Phosphorus defendants obtain victim credentials, log into compromised accounts, and review sensitive information from victim accounts. A set of these is attached as **Exhibit 1** to this Declaration. Although not the case in **Exhibit 1**, similar domains have incorporated trademarks owned by Microsoft. Where domains have incorporated other companies' trademarks, those companies have been informed of and have no objection to Microsoft's proposal to take possession of the domains. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Phosphorus defendants collect victim credentials. In other words, any time a user clicks on a link in a spear phishing email and provides their username and password, that information will be prevented from going to the defendants at the Phosphorus domains, because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of defendants. While it is not possible to rule out the possibility that the Phosphorus defendants could use fall back mechanisms to evade the requested relief, redirecting this core subset of Phosphorus domains will directly disrupt current Phosphorus infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest, in protecting customers of other web services companies who have consented to the relief sought in this action.

32. I believe that the most effective way to suspend the injury caused to Microsoft, its consumers, and the public, is to take the steps described in the Second Supplemental Injunction Order ("Proposed Order"). This relief will significantly hinder the Phosphorus defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Phosphorus defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to the Phosphorus defendants' malicious activities. This can already be seen by effect of the Court's prior orders in this case. Executing the Court's previous Temporary Restraining Order and Preliminary Injunction Order, Microsoft cut communications between Defendants' existing command and

control infrastructure and the victim computers and networks that Defendants attacked and from which Defendants had been stealing information.

33. The Phosphorus defendants' techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in the Phosphorus defendants' active infrastructure become known to the security community, the defendants abandon that infrastructure and move to new infrastructure that is used to continue the Phosphorus defendants' efforts to compromise accounts of new victims. For this reason, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Phosphorus defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason as well, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft. Piecemeal requests to disable these domains, informal dispute resolution or notice to the defendants prior to redirecting the domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous intrusions such as those carried out by the Phosphorus defendants, and prior investigations and legal actions involving such intrusions and actors, I believe that the Phosphorus defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

34. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by actors carrying out intrusions such as those in this case, but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to

continue their operations and destroying or concealing evidence of their operations. For example, after public reports on this actor group were made available, the control panel cited in **Figures 8** through **10** was updated to require authentication. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Phosphorus infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

35. One of the basic questions faced by Microsoft's investigators in the course of their investigation into Phosphorus is determining whether or not a domain misusing a Microsoft trademark is actually associated with illegal activity being conducted by the Defendants. Fortunately, such a determination can be reliably made based upon what we know about Phosphorus and how they operate their criminal infrastructure.

36. First, the Defendants typically use a small set of distinctive malware, and this malware can be identified and distinguished from other types of malware based on several specific forensic factors. The specific types of malware known to be used by Defendants are listed in **Exhibit 2** to this Declaration. The presence of this distinctive malware therefore serves as a reliable indicator that Defendants are involved. In other words, if the malware used in a new attack matches the distinctive malware known to have been used by the Defendants in past attacks, it indicates that the actors behind the new attack are the Defendants. Further, in the future, if new malware variants or families are used by Phosphorus, Phosphorus may be identified based on the similarity of such new malware to previously used malware and previously used modes of deploying such malware.

37. Because Phosphorus malware is reasonably distinctive, domains that are used to deliver the Phosphorus malware to targeted victims and domains that are used to communicate with Phosphorus malware already installed on victim networks are strongly implicated as Phosphorus domains. For example, phishing e-mails that deliver Phosphorus malware in the form of weaponized documents or other attachments may come from or contain links back to particular domains. Other phishing e-mails include links to domains that Defendants have set up in advance as websites designed to download Phosphorus malware to the user's computer and

infect it. Once installed on a computer, Phosphorus malware is programmed to connect to and communicate with a particular set of domains after it successfully infects a victim network. In any of these cases, the Internet domains associated with the Phosphorus attack are strongly implicated as Phosphorus domains.

38. Second, Microsoft has identified patterns in the registration information provided by Defendants when registering the domains that they use in their illegal activities. The factors considered include information required to be submitted during the domain registration process and includes information such as: “name,” e-mail address, address and phone number provided by the registrant, the hosting service designated, the name servers used, and the IP address associated with the domain. Basic registration information associated with Domains registered by Defendants in the past, including the more recent domains registered by Defendants, is included in Exhibit 2. If the registration information associated with a newly identified domain closely matches the pattern associated with domains registered by the Defendants in the past, it is a strong indicator that the Defendants are behind the registration of the new domain. Further, in the future, if new information is used by Defendants, but registration patterns are similar to previously used registration patterns, this too will permit Phosphorus domains to be reliably identified.

39. Third, Microsoft considers the specific tactics used during a new attack. For example, Phosphorus Defendants often send phishing e-mails to victims in which the e-mail purports to be a notification from Microsoft to the recipient regarding an unauthorized access to the recipients Microsoft account, and requesting that the recipient reset his or her account credentials. If the victim clicks on the embedded “Change Password” button in the phishing email, the victim will be connected to a Phosphorus-controlled website which will attempt to induce the victim to enter his account credentials. Other tactics favored by the Phosphorus Defendants include particular deployments of remote code execution through browser drive-by, remote code execution through malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on. Where the

tactics used in a new attack match the tactics observed to be favored by Phosphorus Defendants in past attacks, it is an indication that the Phosphorus Defendants are behind the new attack. Consequently, a domain can be linked to the Phosphorus Defendants by observing the tactics used in attacks involving that domain. Further, in the future, if the details, code and mode of execution change, but the general tactics are consistent with prior tactics of Phosphorus, this too will permit Phosphorus domains to be identified.

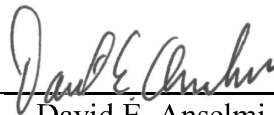
40. Fourth, the Phosphorus Defendants tend to target a particular type of victim and attempt to steal particular types of information. Therefore, Microsoft can use information about the intended victim to help determine whether or not Defendants are involved in the new attack. For example, Phosphorus continues to target Microsoft customers who are political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. Where an Internet domain is associated with an attack on these particular types of targets, it is a factor that is consistent with the known activity and objectives of the Defendants. Further, in the future, if the targeted individuals or institutions are consistent with prior tactics of Phosphorus, this too will permit Phosphorus domains to be identified.

41. Fifth, the Phosphorus Defendants have used Microsoft trademarked brands or slight misspellings of those brands in the names of the domains that they register for their illegal activity, or generalized versions suggestive of Microsoft's services. Defendants use this "blending" technique to disguise the illegal nature of their conduct from the intended target. Thus, use of Microsoft trademarks, brand names or slight misspellings or confusing variations of those trademarks or brand names in the domain name, or generalized versions of indicators of Microsoft's services, is an indicator that the domain is associated with Phosphorus. The list of known and likely trademarks, brands and variants used by Phosphorus is set forth at Exhibit 2.

42. Microsoft considers many factors associated with a domain including those described above and listed in Exhibit 2 to make a balanced determination of whether or not a domain is being used by the Phosphorus Defendants.

43. Defendants continue to register domains to carry out attacks on Microsoft's technology and customers, in particular, using Microsoft's trademarks, brands and other deceptive means, despite the court's previous orders to cease that activity and despite the prior relief which removed previously used domains from Defendants' control. Given Defendants' apparent willingness to violate the court's orders on an ongoing basis, and the ease and speed with which Defendants can register Microsoft-related domains to continue their attacks, an ongoing process is needed to efficiently and quickly curtail such activities as soon as Defendants register domains for their attacks. Without such a process, Defendants will be able to continue their malicious and illegal activities, and will continue to cause irreparable injury to Microsoft, its customers and the public. Without such a process, Defendants will not be deterred from engaging in such illegal and harmful activities. I have reviewed the process set forth in Microsoft's *Ex Parte* Motion for Second Supplemental Preliminary Injunction Order submitted with this declaration. Based on my experience and background, I conclude as a technical and practical matter that the process set forth in the proposed order would enable Microsoft and the Court to effectively and efficiently enforce the Court's prior and ongoing orders and stop the irreparable harm caused by Defendants' illegal activities on an ongoing basis. I also reach this conclusion on the basis that this same expedited process is in place, and ongoing, with respect to a separate matter in the Eastern District of Virginia, addressing a different threat actor group. The process has been effective in that matter. Thus, I conclude that it would be effective in the instant matter as well.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 17th day of July 2019, in Redmond, Washington.



David E. Anselmi

EXHIBIT 1

APPENDIX A**.COM DOMAINS****Registry**

c/o

VeriSign, Inc.**VeriSign Information Services, Inc.****12061 Bluemont Way****Reston, Virginia 20190****United States**

mail-files.com	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: bd04d6f1eec84a9ba600d7c0c6f0325f.protect@whoisguard.com
logins-signin.com	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: be7e7649fbab44d5becff2c72e436f84.protect@whoisguard.com
supports-email.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491

	Registrant Fax Ext: Registrant Email: whoisprivacy@domainidshield.com onlinenic-enduser@onlinenic.com
loginacount.com	Registrant Organization: frederik Registrant State/Province: hessen Registrant Country: DE Registrant Email: Contact holder at https://www.domainidshield.com/gdpr onlinenic-enduser@onlinenic.com

.ORG DOMAINS**Registry****Public Interest Registry (PIR)****1775 Wiehle Avenue****Suite 200****Reston Virginia 20190****United States**

account-verify.org	Registrant Organization: delijapp Registrant State/Province: hb Registrant Country: AF onlinenic-enduser@onlinenic.com
--------------------	---

.INFO DOMAINS**Registry****Afilias, Inc.****300 Welsh Road****Building 3, Suite 105****Horsham, PA 19044****United States**

share-doc.info	Registrant Organization: Schroeder co. Registrant State/Province: NC Registrant Country: AF onlinenic-enduser@onlinenic.com
----------------	--

EXHIBIT 2

I. Criteria Indicating Phosphorus Domains

Delivers malicious software, code, commands, exploits and/or “backdoor” functionality previously associated with Phosphorus, including but not limited to: Stealer malware, or similar code or functionality deployed in a manner previously associated with Phosphorus.	Associated with remote code execution through browser drive-by or malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on, escalation of privileges, DLL file backdoor, credential stealing functionality, SSL tunnel, and/or functionality to deliver code or functions to “air gapped” USB devices, deployed in a manner previously associated with Phosphorus or similar code or functionality.
Domain registration information	Use of cryptocurrency to purchase services
Name servers	Start of Authority (SOA) records
Resolves to IP of past Phosphorus domain, command and control server or similar infrastructure	Resolves to IP used in past Phosphorus malware delivery or credential harvesting domains or credential harvesting domains
Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Phosphorus.	Used to deceive, target, obtain information from, and/or communicate commands or code to recipients that may possess or be able to provide sensitive information or trade secrets of persons, entities or networks related to the defense, critical infrastructure or high technology sectors, journalists, political advisors or organizations, government bodies, diplomatic institutions, religious organizations, universities, and/or military forces and installations.
SSL Cert Issuer_DN	SSL Cert Subject_DN
Host	Registrar
Domains similar to previously used domains	Victims being targeted similar to past targets

II. Known And Likely Microsoft Trademarks and Brands Used By Phosphorus

While Defendants may use any Microsoft marks, brands or confusingly similar indicators, Defendants have already exploited or are likely to exploit the following: “365,” “Azure,” “Bing,” “Excel,” “Exchange,” “Healthvault,” “Hotmail,” “LinkedIn,” “Live,” “Messenger,” “Microsoft,” “Minecraft,” “MSDN,” “MSFT,” “MS,” “MSN,” “.NET,” “O365,” “Office,” “OneDrive,” “Outlook,” “OWA,” “Passport,” “PowerPoint,” “SharePoint,” “Skype,” “Surface,” “Visio,” “Win,” “Windows,” and “Xbox.”

While Defendants may use any keyword, in combination with Microsoft marks, brands or confusingly similar indicators, or with other keywords, we believe following are the most likely keywords to be used, along with intentional misspellings:

365	analytic	care	click	continue
64	app	cares	cloud	control
access	are	center	com	corp
account	assist	centr	component	corporate
accounts	auth	centre	config	corporation
activities	authenticate	certificate	confirm	crc
adapter	authorizes	cfg	confirmation	credentials
adviser	broadcast	change	connect	customer
agency	bulletin	check	consumer	daily
american	cache	checksum	content	data

dc	http	my	redirect	support
delivery	id	mymail	reply	sync
department	identification	net	reserve	sys
departrment	identifier	network	review	system
dev	identify	news	scan	team
docs	identity	notification	search	technology
document	inbox	onlihe	sec	telecom
download	info	online	secure	telegram
drivadptrwin	intel	options	securing	tellekom
drive	intelligence	page	security	terms
driver	ipv4	panel	sell	test
drivers	ipv6	passport	send	tests
drv	issue	password	server	tools
edit	link	pc	service	transfer
elite	log	permission	servicing	trust
email	login	plus	session	trusted
expo	magic	podcast	set	update
file	mail	policy	setting	updater
fix	mailbox	politics	settings	updates
forum	management	press	share	upgrade
general	manager	privacy	sharing	user
getupdate	me	product	shop	users
getupdt	media	profile	signal	verification
global	meeting	progress	signin	verify
gov	member	protect	site	wear
help	message	protected	speak	web
here	mfa	provider	srv	webmail
home	mobile	ready	statistic	world
host	module	recognized	status	you
hotfix	monitor	recovery	store	your

III. Phosphorus Domains Registered By Defendants To Date

yahoo-verification.org	Registrant: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 109 First Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94988 Registrant Country: BA Registrant Phone: +1.4038493301 Registrant Fax: +1.4038493302 Registrant Email: domainadmin@yahoo-verification.org
support-services.com	Registrant Name: hash crypt Registrant Organization: hashcrypt Registrant Street: nbcj hjf,m Registrant City: losangles Registrant State/Province: Alabama Registrant Postal Code: 35004 Registrant Country: US Registrant Phone: +1.09876543567 Registrant Email: hashcrypt@protonmail.com
verification-live.com	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation

	Registrant Street: AS8068 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, Registrant City: toronto Registrant State/Province: toronto Registrant Postal Code: 64043 Registrant Country: UM Registrant Phone: +1.6509234001 Registrant Fax: +1.6509234002 Registrant Email: test9179@porotonmail.com
com-mailbox.com	Registrant Name: Priview Service Registrant Organization: mish Registrant Street: No 885, Azar st Registrant City: Dubai Registrant State/Province: Dubai Registrant Postal Code: 98120 Registrant Country: AE Registrant Phone: +97.3218526 Registrant Fax: +97.3218526 Registrant Email: domain.seller2017@yandex.com
com-myaccuants.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: co5940551458104@domainidshield.com
notification-accountservice.com	Registrant Name: mosa alnarjani Registrant Organization: Registrant Street: baqdad, alqusair st , no 246 Registrant City: baqdad Registrant State/Province: baqdad Registrant Postal Code: 548996 Registrant Country: IQ Registrant Phone: +964.7730061463 Registrant Email: meisam.bayat.sector@gmail.com
accounts-web-mail.com	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: US Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com

customer-certificate.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
session-users-activities.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
user-profile-credentials.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
verify-linke.com	Registrant Name: sora bara Registrant Organization: narabara Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 7482957439 Registrant Country: BI Registrant Phone: +1.234124323 Registrant Fax: +1.2129876243 Registrant Email: test9179@protonmail.com
support-services.net	Registrant Name: Support Services Inc. Registrant Organization: Support Services Inc. Registrant Street: 1901 Amphitheatre Parkway Registrant City: Mountain View Registrant State/Province: 64043 Registrant Postal Code: 64043 Registrant Country: US Registrant Phone: +1.6509234001 Registrant Fax: +1.6509188572 Registrant Email: test9179@protonmail.com
verify-linkedin.net	Registrant Name: sora bara Registrant Organization: none

	Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 748295743 Registrant Country: BI Registrant Phone: +75.234124323 Registrant Fax: +86.12124321 Registrant Email: dnsadmin@verify-linkedin.com
yahoo-verification.net	Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: BA Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
yahoo-verify.net	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 701 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 98089 Registrant Country: BI Registrant Phone: +1.4083893300 Registrant Fax: +1.4083893301 Registrant Email: domainadmin@yahoo-verify.net
outlook-verify.net	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: One Microsoft Way, Redmond, WA, 98052, US Registrant City: Washington Registrant State/Province: canada Registrant Postal Code: 7482957439 Registrant Country: US Registrant Phone: +1.234124323 Registrant Phone Ext: Registrant Fax: +1.2129876243 Registrant Fax Ext: Registrant Email: supportiveemail@protonmail.com
com-users.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: co5806503530204@domainidshield.com
verify-account.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL

	TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
telegram.net	Registrant Name: NS-CLOUD-B1.GOOGLedomains.COM Registrant Organization: Domains By Proxy, LLC Registrant Street: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant City: Arizona Registrant State/Province: Arizona Registrant Postal Code: 0056 Registrant Country: US Registrant Phone: +1.4806242505 Registrant Fax: +1.4806242506 Registrant Email: verdonew@protonmail.com
account-verify.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
myaccount-services.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
com-identifier-servicelog.name	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: https://www.name.com/contact-domain-whois/com-identifier-servicelog.name abuse@name.com

microsoft-update.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
outlook-livecom.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
update-microsoft.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
documentsfilesharing.cloud	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: documentsfilesharing.cloud@protecteddomainservices.com
com-microsoftonline.club	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
confirm-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK Registrant Email: onlinenic-enduser@onlinenic.com
session-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong

	Registrant Country: CN onlinenic-enduser@onlinenic.com
confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
document-share.info	Registrant Organization: Martini Registrant State/Province: Tashkent Registrant Country: UZ onlinenic-enduser@onlinenic.com
broadcast-news.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
webemail.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-identifier-servicelog.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
documentsharing.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: AF onlinenic-enduser@onlinenic.com
notification-accountservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identifier-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
documentofficupdate.info	Registrant Organization: William Brown Registrant State/Province: VA Registrant Country: US onlinenic-enduser@onlinenic.com
recoveryusercustomer.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
serverbroadcast.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
account-profile-users.info	Registrant Organization: arsalan co.

	Registrant State/Province: Louisiana Registrant Country: US onlinenic-enduser@onlinenic.com
account-service-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
accounts-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-accountidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-privacy-help.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-sessionidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-useraccount.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirmation-users-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-session-identification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
continue-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customer-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customers-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com

elitemaildelivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
email-delivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
message-serviceprovider.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notificationapp.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recognized-activity.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: VA onlinenic-enduser@onlinenic.com
recover-customers-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-recovery-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-continue.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-mail-customers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-verify-user.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
shop-sellwear.info	Registrant Organization: maryam s32 Registrant State/Province: tersite Registrant Country: US onlinenic-enduser@onlinenic.com
supportmailservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
terms-service-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
user-activity-issues.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
useridentity-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
users-issue-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
verify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
login-gov.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-signal-agency.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notifications-center.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
identifier-services-sessions.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
session-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
customer-managers.info	Registrant Organization: Home Registrant State/Province: TX

	Registrant Country: US onlinenic-enduser@onlinenic.com
confirmation-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-session-confirmation.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-managers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-services-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-session-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
sessions-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
download-teamspeak.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-issue-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
microsoft-upgrade.mobi	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
broadcastnews.pro	Registrant State/Province: UT Registrant Country: US abuse@name.com
mobile-messengerplus.network	Registrant Name: Cave Detector Registrant Organization: Masqat Co Registrant Street: No 64, Lion St Registrant City: Masqat Registrant State/Province: Masqat Registrant Postal Code: 85641 Registrant Country: OM Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: cave.detector@yandex.com
sessions-identifier-memberemailid.network	Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domain Protection Services, Inc. Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: CO Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar: Name.com, Inc. Registrar IANA ID: 625 Registrar Abuse Contact Email: abuse@name.com Registrar Abuse Contact Phone: +7.202492374
scribdinc.com	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201

	Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: https://www.name.com/contact-domain-whois/scribdinc.com abuse@name.com
telagram.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: whoisprivacy@domainidshield.com
bahaius.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
customers-reminder.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com

identity-verification-service.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
inbox-drive.info	Registration Name: Jennifer J. Bradley Registration Organization: roseron co Registration Street: 2811 Maple Avenue Registration City: Modesto Registration State/Province: CA Registration Postal Code: 95354 Registration Country: US Registration Phone: +1.251548796 Registration Phone Ext: Registration Fax: +1.251548796 Registration Fax Ext: Registration Email: amanda.cristiani15@gmail.com
inbox-sharif.info	Registration Name: Jennifer J. Bradley Registration Organization: roseron co Registration Street: 2811 Maple Avenue Registration City: Modesto Registration State/Province: CA Registration Postal Code: 95354 Registration Country: AF Registration Phone: +1.2564158796 Registration Phone Ext: Registration Fax: +1.2564158796 Registration Fax Ext: Registration Email: amanda.cristiani15@gmail.com
magic-delivery.info	Registration Name: William Brown Registration Organization: will co Registration Street: 410 Coulter Lane Registration City: Richmond Registration State/Province: VA Registration Postal Code: 23226 Registration Country: VA Registration Phone: +1.8042873632 Registration Phone Ext: Registration Fax: +1.8042873632

	Registration Fax Ext: Registration Email: williambrown.wl.br@gmail.com
recovery-services.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
verification-services.info	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
youridentityactivity.world	Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domain Protection Services, Inc. Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: CO Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY abuse@name.com

EXHIBIT 2

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

DECLARATION OF HONORABLE FAITH HOCHBERG (RET.)

I, Faith Hochberg, declare as follows:

1. I currently serve as an independent mediator and arbitrator of complex cases. I was formerly U.S. District Judge for the District of New Jersey from 1999 through 2015. Prior to my service as a federal judge, I was the U.S. Attorney for the District of New Jersey, among other roles. Attached hereto as Exhibit A is a true and correct copy of my current curricula vitae. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. I understand that the parties and the court in the above-referenced case are considering the possibility of appointing me as Court Monitor for limited purposes to be defined by the court. Pursuant to that understanding and Rule 53(b)(3), I hereby aver that there are no grounds for my disqualification under 28 U.S.C. § 455 with respect to the above referenced case.

3. I have no personal bias or prejudice concerning the above-referenced parties, or personal knowledge of disputed evidentiary facts concerning the proceeding.

4. I have not served as a lawyer in the matter in controversy and have not worked with another lawyer that, during such association, worked as a lawyer concerning the matter, judged the matter, or have been a material witness in the matter.

5. I have not served in governmental employment and in such capacity participated as counsel, adviser, or material witness concerning the proceeding or expressed an opinion concerning the merits of the particular case in controversy.

6. I do not, individually or as a fiduciary, have a financial interest in the subject matter in controversy or in a party to the proceeding, or any other interest that could be substantially affected by the outcome of the proceeding. My spouse and any minor child residing in my household do not have a financial interest in the subject matter in controversy or in a party to the proceeding, or any other interest that could be substantially affected by the outcome of the proceeding.

7. Neither I nor my spouse, nor a person within a third degree of relationship to either of us, nor the spouse of such a person: (i) is a party to the proceeding, or an officer, director, or trustee of a party, (ii) is acting as a lawyer in the proceeding, (iii) is known to have an interest that could be substantially affected by the outcome of the proceeding, (iv) is to my knowledge likely to be a material witness in the proceeding.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 15th day of July, 2019 in New York, New York.


Hon. Faith Hochberg (Ret.)

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5.1**

[PROPOSED] SECOND SUPPLEMENTAL INJUNCTION ORDER

The Court, having considered the pleadings and declaration in support of Microsoft Corporation's ("Microsoft") Motion for Second Supplemental Preliminary Injunction Order, hereby orders that (i) the terms of the Preliminary Injunction Order ("Preliminary Injunction Order"), Dkt. 18, shall apply to the additional domains set forth in the **Appendix A** to this order established by Defendants in violation of this court's order and (ii) appoint a Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to manage this process and relieve the burden on the Court.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, memorandum, and all other pleadings and papers relevant to Microsoft's Motion for Second Supplemental Preliminary Injunction Order and Microsoft's original motion for Temporary Restraining Order and Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

I. The Defendants were served with notice of the Preliminary Injunction.

II. After receiving notice of the Preliminary Injunction, the Defendants have continued to engage in the conduct enjoined by the Preliminary Injunction Order, and therefore continue to violate the Preliminary Injunction Order. In particular, Defendants have intentionally and without authorization, continued and attempted to access and send malicious software, code, and instructions to protected computers, operating systems, and networks of Microsoft and its customers, attacking such computers, systems and networks, and exfiltrating information from those computers, systems and networks, using new domains.

III. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Preliminary Injunction Order, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for such prohibited and unlawful purposes.

IV. There is good cause to believe that, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of domains for purposes enjoined by the Preliminary Injunction Order, immediate and irreparable harm will result to Microsoft, Microsoft's customers and to the public, from the Defendants' ongoing violations.

V. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the Court's inherent equitable authority, good cause and the interests of justice require that this Order be Granted.

SECOND SUPPLEMENTAL PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, the terms of the Preliminary Injunction Order shall be supplemented and shall be enforced against Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, as follows:

- 1.** With respect to any currently registered Internet domains set forth in **Appendix**

A, the domain registries shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain shall be redirected to secure servers by changing the authoritative name servers to NS151.microsoftinternetsafety.net and NS152.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Injunction;

D. The WHOIS registrant, administrative, billing and technical contact and

identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System (“DNS”), including domain registrars.

IT IS FURTHER ORDERED that “Phosphorus Domains” are domains which are determined to meet the following two criteria:

Criteria 1: The domains are used by the Defendants to break into computers and networks of the organizations that Phosphorus targets, or control the reconnaissance of those networks, or, ultimately, exfiltrate sensitive information from them, or are otherwise used by the Defendants to carry out the activities and purposes prohibited by the Preliminary Injunction. A domain is determined to be a Phosphorus Domain by comparing the activities and patterns associated with that domain with known confirmed Phosphorus Domains. The following factors concerning the domain will be used in this analysis:

Delivers malicious software, code, commands, exploits and/or “backdoor” functionality previously associated with Phosphorus, including but not limited to: Stealer malware, or similar code or functionality deployed in a manner previously associated with Phosphorus.	Associated with remote code execution through browser drive-by or malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on, escalation of privileges, DLL file backdoor, credential stealing functionality, SSL tunnel, and/or functionality to deliver code or functions to “air gapped” USB devices, deployed in a manner
--	--

	previously associated with Phosphorus or similar code or functionality.
Domain registration information	Use of cryptocurrency to purchase services
Name servers	Start of Authority (SOA) records
Resolves to IP of past Phosphorus domain, command and control server or similar infrastructure	Resolves to IP used in past Phosphorus malware delivery or credential harvesting domains or credential harvesting domains
Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Phosphorus.	Used to deceive, target, obtain information from, and/or communicate commands or code to recipients that may possess or be able to provide sensitive information or trade secrets of persons, entities or networks related to the defense, critical infrastructure or high technology sectors, journalists, political advisors or organizations, government bodies, diplomatic institutions, religious organizations, universities, and/or military forces and installations.
SSL Cert Issuer_DN	SSL Cert Subject_DN
Host	Registrar
Domains similar to previously used domains	Victims being targeted similar to past targets

Criteria 2: The domains (a) use and infringe Microsoft’s trademarks, trade names or service marks or confusingly similar variants, or (b) use any false or deceptive designation, representation or description, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers, or (c) suggest in any way that Defendants’ activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or pass off Defendants’ activities, products or services as Microsoft’s. Such trademarks and brands shall include, but are not limited to the following trademarks, brands and/or confusingly similar variants: While Defendants may use any Microsoft marks, brands or confusingly similar indicators, Defendants have already exploited or are likely to exploit the following: “365,” “Azure,” “Bing,” “Excel,” “Exchange,” “Healthvault,” “Hotmail,” “LinkedIn,” “Live,” “Messenger,” “Microsoft,” “Minecraft,” “MSDN,” “MSFT,” “MS,” “MSN,” “.NET,” “O365,” “Office,” “OneDrive,” “Outlook,” “OWA,” “Passport,” “PowerPoint,”

“SharePoint,” “Skype,” “Surface,” “Visio,” “Win,” “Windows,” and “Xbox.” Also, Criteria 2 is met where defendants use generalized versions of terms that are suggestive of Microsoft’s services, but do not specifically use a trademark.

IT IS FURTHER ORDERED that the following processes shall be used to determine whether a domain is a Phosphorus Domain and to determine the disposition of such domains. With respect to domains alleged to meet the criteria to constitute Phosphorus Domains, and domains that are alleged to be Phosphorus Domains based on new criteria not listed in this Order, Microsoft shall submit a written motion to the Court Monitor seeking a declaration that such domains are Phosphorus Domains. The Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Phosphorus Domains, as set forth further below.

IT IS FURTHER ORDERED that, pursuant to Federal Rule of Civil Procedure 53(a)(1)(C) and the court’s inherent equitable powers, Hon. Faith Hochberg (Ret.) is appointed to serve as Court Monitor in order to make determinations on disputes regarding whether particular domains are Phosphorus Domains, to make determinations and orders regarding whether particular domains are Phosphorus Domains, and to monitor Defendants’ compliance with the Preliminary Injunction. Prior to being appointed, the Court Monitor must file an affidavit “disclosing whether there is any ground for disqualification under 28 U.S.C. § 455.” Fed. R. Civ. P. 53(b)(3); *see also* Fed. R. Civ. P. 53(a)(2) (discussing grounds for disqualification). Filed concurrently with this Order is the affidavit submitted to the court by the Court Monitor. The following sets forth the terms of the appointment of the Court Monitor:

- 1. Duties:** The duties of the Court Monitor shall include the following:
 - A. Carrying out all responsibilities and tasks specifically assigned to the

Court Monitor in this Order;

B. Resolving objections submitted by domain registries, Defendants or other third parties, to Microsoft's determinations that domains constitute Phosphorus Domains and, with respect to motions submitted by Microsoft that particular domains constitute Phosphorus Domains, making determinations whether such domains are or are not Phosphorus Domains;

C. Otherwise facilitating the Parties' or third parties' resolution of disputes concerning compliance with obligations under this Order or any orders issued by the Court Monitor, and recommending appropriate action by the court in the event an issue cannot be resolved by the Parties or third parties with the Court Monitor's assistance;

D. Investigating matters related to the Court Monitor's duties, and enforcing orders related to the matters set forth in this Order

E. Monitoring and reporting on Defendants' compliance with their obligations under the Preliminary Injunction and this Order;

F. The Court Monitor shall have all authority provided under Federal Rule of Civil Procedure 53(c).

2. Orders Regarding Phosphorus Domains: The Court Monitor shall resolve objections and shall make determinations and issue orders whether domains are Phosphorus Domains, pursuant to the terms set forth in the Preliminary Injunction, this Order and pursuant to the following process:

A. Upon receipt of a written objection from any domain registries, Defendants or any other third parties contesting any determinations by Microsoft that particular domains constitute Phosphorus Domains, or upon receipt of a written motion from Microsoft for a finding that particular domains constitute Phosphorus Domains, the Court Monitor shall take

and hear evidence whether a domain is a Phosphorus Domain, pursuant to the standards set forth in Rule 65 of the Federal Rules of Civil Procedure. Any party opposing such objection or motion shall submit to the Court Monitor and serve on all parties an opposition or other response within twenty four (24) hours of receipt of service of the objection or motion. The Court Monitor shall issue a written ruling on the objection or motion no later than two (2) days after receipt of the opposition or other response. Any party may seek and the Court Monitor may order provisional relief, including redirection of domains or other temporary disposition of domains, while any objection or motion is pending. A form of order which may be used by the Special Master is attached as **Appendix B**.

B. It is the express purpose of this order to afford prompt and efficient relief and disposition of Phosphorus Domains. Accordingly, in furtherance of this purpose, all objections, motions and responses shall be embodied and communicated between the Court Monitor, parties and third parties in electronic form, by electronic mail or such other means as may be reasonably specified by the Court Monitor. Also in furtherance of this purpose, hearings shall be telephonic or in another expedited form as may be reasonably specified by the Court Monitor.

C. The Court Monitor's determinations regarding any objection or any motion shall be embodied in a written order, which shall be served on all Parties and relevant third parties (including domain registries and/or registrars).

D. The Court Monitor is authorized to order the Parties and third parties to comply with such orders (pursuant to 28 U.S.C. § 1651(a)), subject to the Parties' and third parties' right to judicial review, as set forth herein.

E. If no Party or third party objects to the Court Monitor's orders and

determinations pursuant to the judicial review provisions herein, then the Court Monitor's orders and determinations need not be filed on the docket. However, at the time the Court Monitor submits his or her periodic reports to the court, as set forth below, the Monitor shall separately list in summary form his or her uncontested orders and determinations.

3. Judicial Review: Judicial review of the Court Monitor's orders, reports or recommendations, shall be carried out as follows:

A. If any Party or third party desires to object to any order or decision made by the Court Monitor, the Party shall notify the Court Monitor within one business day of receipt of service of the order or decision, and thereupon the Court Monitor shall promptly file on the court's docket the written order setting forth the Monitor's decision or conditions pursuant to Federal Rule of Civil Procedure 53(d). The Party or third party shall then object to the Court Monitor's order in the manner prescribed in this Order.

B. The Parties and third parties may file objections to, or a motion to adopt or modify, the Court Monitor's order, report, or recommendations no later than 10 calendar days after the order is filed on the docket. The court will review these objections under the standards set forth in Federal Rule of Civil Procedure 53(f).

C. Any party may seek and the Court may order provisional relief, including redirection of domains or other temporary disposition of domains, while any objection or motion is pending.

D. The orders, reports and recommendations of the Court Monitor may be introduced as evidence in accordance with the Federal Rules of Evidence.

E. Before a Party or third party seeks relief from the court for alleged noncompliance with any court order that is based upon the Court Monitor's report or

recommendations, the Party or third party shall: (i) promptly notify the other Parties or third party and the Court Monitor in writing; (ii) permit the Party or third party who is alleged to be in noncompliance five business days to provide the Court Monitor and the other parties with a written response to the notice, which either shows that the party is in compliance, or proposes a plan to cure the noncompliance; and (iii) provide the Court Monitor and parties an opportunity to resolve the issue through discussion. The Court Monitor shall attempt to resolve any such issue of noncompliance as expeditiously as possible.

4. Recordkeeping: The Court Monitor shall maintain records of, but need not file those orders, reports and recommendations which are uncontested by the Parties or third parties and for which judicial review is not sought. The Court Monitor shall file on the court's docket all written orders, reports and recommendations for which judicial review is sought, along with any evidence that the Court Monitor believes will assist the court in reviewing the order, report, or recommendation. The Court Monitor shall preserve any documents the Monitor receives from the Parties.

5. Periodic Reporting: The Court Monitor shall provide periodic reports to the court and to the Parties concerning the status of Defendants' compliance with this Order and other orders of the court or the Court Monitor, including progress, any barriers to compliance, and potential areas of noncompliance. The periodic reports shall also include a summary of all uncontested orders and determinations and a listing of ex parte communications. The Court Monitor shall file a report with the court under this provision at least once every 120 days.

6. Access to Information: The Court Monitor shall have access to individuals and non-privileged information, documents, and materials under the control of the Parties or third parties that the Monitor requires to perform his or her duties under this Order, subject to the

terms of judicial review set forth herein. The Court Monitor may communicate with a Party's or a third party's counsel or staff on an *ex parte* basis if reasonably necessary to carry out the Court Monitor's duties under this Order. The Court Monitor may communicate with the court on an *ex parte* basis concerning non-substantive matters such as scheduling or the status of the Court Monitor's work. The Court Monitor may communicate with the court on an *ex parte* basis concerning substantive matters with 24 hours written notice to the Parties and any relevant third party. The Court Monitor shall document all *ex parte* oral communications with a Party's or third party's counsel or staff in a written memorandum to file summarizing the substance of the communications, the participants to the communication, the date and time of the communication and the purpose of the *ex parte* communication. At the time the Court Monitor submits his or her periodic reports to the court, the Monitor shall separately list his or her *ex parte* communications with the Parties.

7. Engagement of Staff and Consultants: The Court Monitor may, consistent with a budget to be approved by the court, hire staff or expert consultants to assist the Court Monitor in performing his or her duties. The Court Monitor will provide the Parties advance written notice of his or her intention to hire a particular consultant, and such notice will include a resume and a description of duties of the consultant.

8. Compensation, and Expenses: Microsoft shall fund the Court Monitor's work pursuant to invoices submitted by the Court Monitor. The Court Monitor shall incur only such fees and expenses as may be reasonably necessary to fulfill the Court Monitor's duties under this Order, or such other orders as the court may issue. Every 120 days, in connection with reports of communications set forth above, the Court Monitor shall submit to the court an itemized statement of fees and expenses paid in connection with the Court Monitor's duties, which the

court will inspect for regularity and reasonableness.

9. Other Provisions: As an agent and officer of the court, the Court Monitor and those working at his or her direction shall enjoy the same protections from being compelled to give testimony and from liability for damages as those enjoyed by other federal judicial adjuncts performing similar functions. Nevertheless, any Party or non-party may request that the court direct the Court Monitor to disclose documents or other information reasonably necessary to an investigation or the litigation of legal claims in another judicial forum that are reasonably related to the Court Monitor's work under this Order. The Court shall not order the Court Monitor to disclose any information without providing the Parties notice and an opportunity to be heard. As required by Rule 53(b)(2) of the Federal Rules of Civil Procedure, the court directs the Court Monitor to proceed with all reasonable diligence. The Court Monitor shall be discharged or replaced only upon an order of the Court. The parties, their successors in office, agents, and employees will observe faithfully the requirements of this Order and cooperate fully with the Court Monitor, and any staff or expert consultant employed by the Court Monitor, in the performance of their duties.

10. Retention of Jurisdiction: The Court will retain jurisdiction to enforce and modify this Order until such time as the Court finds that Microsoft does not seek further determinations regarding any additional Phosphorus Domains or that Defendants establish, by a preponderance of the evidence, that there is no risk of continued use of Phosphorus Domains in violation of the Preliminary Injunction. Under no circumstances will the court's jurisdiction to modify or enforce this Order lapse before January 1, 2030.

IT IS FURTHER ORDERED that copies of this Order and all other pleadings and documents in this action, including orders, determinations, reports and recommendations of the

Court Monitor, may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatory to such treaties.

IT IS SO ORDERED

Entered this __ day of July, 2019

Amy Berman Jackson
United States District Judge

APPENDIX A

Appendix A**.COM DOMAINS****Registry**

c/o

VeriSign, Inc.

VeriSign Information Services, Inc.

12061 Bluemont Way

Reston, Virginia 20190

United States

mail-files.com	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: bd04d6f1eec84a9ba600d7c0c6f0325f.protect@whoisguard.com
logins-signin.com	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: be7e7649fbab44d5becff2c72e436f84.protect@whoisguard.com
supports-email.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491

	Registrant Fax Ext: Registrant Email: whoisprivacy@domainidshield.com onlinenic-enduser@onlinenic.com
loginacount.com	Registrant Organization: frederik Registrant State/Province: hessen Registrant Country: DE Registrant Email: Contact holder at https://www.domainidshield.com/gdpr onlinenic-enduser@onlinenic.com

.ORG DOMAINS**Registry****Public Interest Registry (PIR)****1775 Wiehle Avenue****Suite 200****Reston Virginia 20190****United States**

account-verify.org	Registrant Organization: delijapp Registrant State/Province: hb Registrant Country: AF onlinenic-enduser@onlinenic.com
--------------------	---

.INFO DOMAINS**Registry****Afilias, Inc.****300 Welsh Road****Building 3, Suite 105****Horsham, PA 19044****United States**

share-doc.info	Registrant Organization: Schroeder co. Registrant State/Province: NC Registrant Country: AF onlinenic-enduser@onlinenic.com
----------------	--

APPENDIX B

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:19-cv-00716-ABJ

[PROPOSED] ORDER SUPPLEMENTING THE INJUNCTION

The Court Monitor, having considered the pleadings and declaration in support of Plaintiff Microsoft Corporation's ("Microsoft") Motion To Supplement The Injunction, orders that the terms of the Preliminary Injunction Order ("Preliminary Injunction Order"), Dkt. 18, shall apply to the domains set forth in Appendix A to this order.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, memorandum, and all other pleadings and papers relevant to Microsoft's request to enforce and supplement the Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. The Defendants were served with notice of the Injunction.
2. After receiving notice of the Injunction, the Defendants have continued to engage in the conduct enjoined by the Injunction, and therefore continue to violate the Injunction. In particular, the Defendants have intentionally and without authorization, continued and attempted to access and send malicious software, code, and instructions to protected computers, operating systems, and networks of Microsoft and its customers, attacking such computers, systems and networks, and exfiltrating information from those computers, systems and networks, using new

domains, at Appendix A, which are (1) “using and infringing Microsoft’s trademarks,” (2) are “using in connection with Defendants’ activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers,” (3) “suggest[] ... that Defendants’ activities, products or services come from or are somehow sponsored or affiliated with Microsoft, and/or (4) are “passing off Defendants’ activities, products or services as Microsoft’s.” This conduct is prohibited by the Permanent Injunction, Docket 18 at p. 7.

3. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Injunction, using the domains at Appendix A, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of those domains for such prohibited and unlawful purposes.

4. There is good cause to believe that, unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of the domains at Appendix A for purposes enjoined by the Injunction, on an ongoing basis, immediate and irreparable harm will result to Microsoft, Microsoft’s customers and to the public, from the Defendants’ ongoing violations.

5. The domains at Appendix A have been shown by Microsoft to be “Phosphorus Domains,” pursuant to the terms of the Injunction.

6. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 53(a)(1)(C), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the court’s inherent equitable authority, good cause and the interests of justice require that this Order be Granted.

INJUNCTION

IT IS THEREFORE ORDERED that, the terms of the Injunction shall be supplemented and shall be enforced against the Defendants, Defendants’ representatives, and persons who are in active concert or participation with Defendants, as follows:

1. With respect to the Phosphorus Domains set forth at Appendix A, the domain registries listed in Appendix A. (the “domain registries”) shall take the following actions:

A. Within five (5) business days of receipt of this Order shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domains under its control, the domain registries for the domains, or their administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domains to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has permanent control over the hosting and administration of the domains in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registries or registrars of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domains shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domains;

C. The domains shall be redirected to secure servers by changing the authoritative name servers to NS151.microsoftinternetsafety.net and NS152.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Injunction;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation

One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domains by Defendants and prevent transfer or control of the domains to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System (“DNS”), including domain registrars.

IT IS SO ORDERED

Entered this ____ day of _____, ____

Hon. Faith S. Hochberg
United States District Judge (Ret.)