

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 ANSEMI IN SUPPORT OF
MICROSOFT'S EX PARTE MOTION TO SUPPLEMENT PRELIMINARY
INJUNCTION ORDER**

I, David Anselmi, declare as follows:

1. I am a Senior 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 specifically crafted to appear as if there is an issue with the targeted individual's account. 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). As can be seen in **Exhibit 1**, the Phosphorus defendants sometimes also disguise their command and control domains by using terms that make them appears to be related to online services, such as Microsoft's. For example, in the domains at **Exhibit 1**, the Phosphorus defendants have incorporated terms such as "mail" or account "login" or "identity-verification" 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's trademarks in its online services, such as Microsoft's "Outlook" or "Office 365" services and brands.

- b. Since the Preliminary Injunction Order, Microsoft has identified an additional eleven domains that the Phosphorus defendants have registered that follow the same patterns and are obviously 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 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 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 access their email. 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. 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:

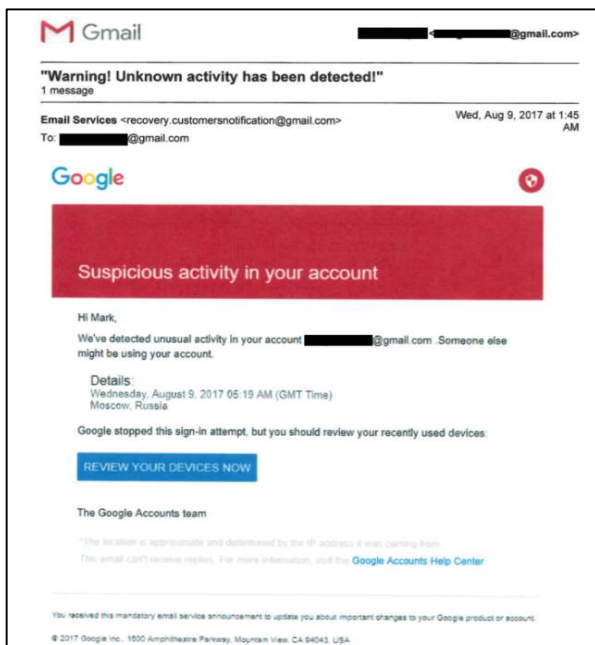


Figure 3

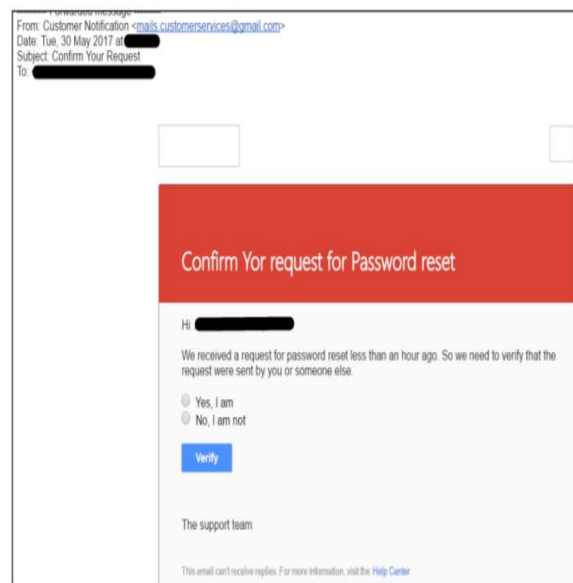


Figure 4

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:

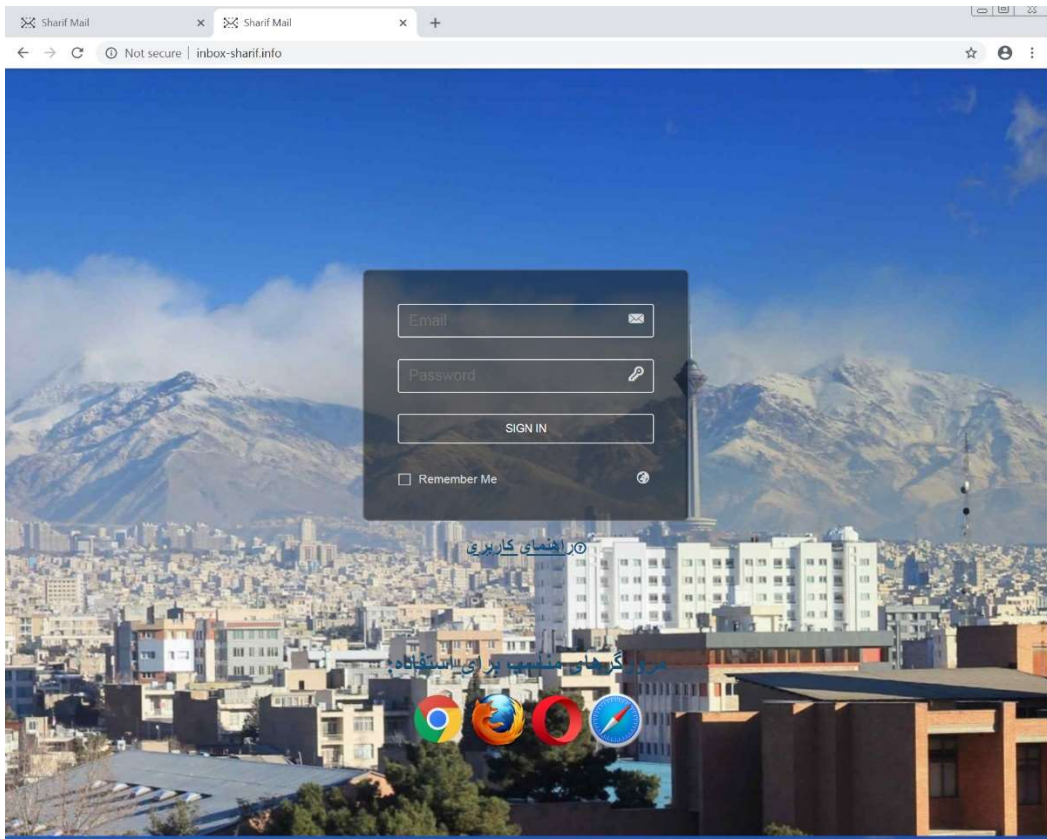


Figure 5

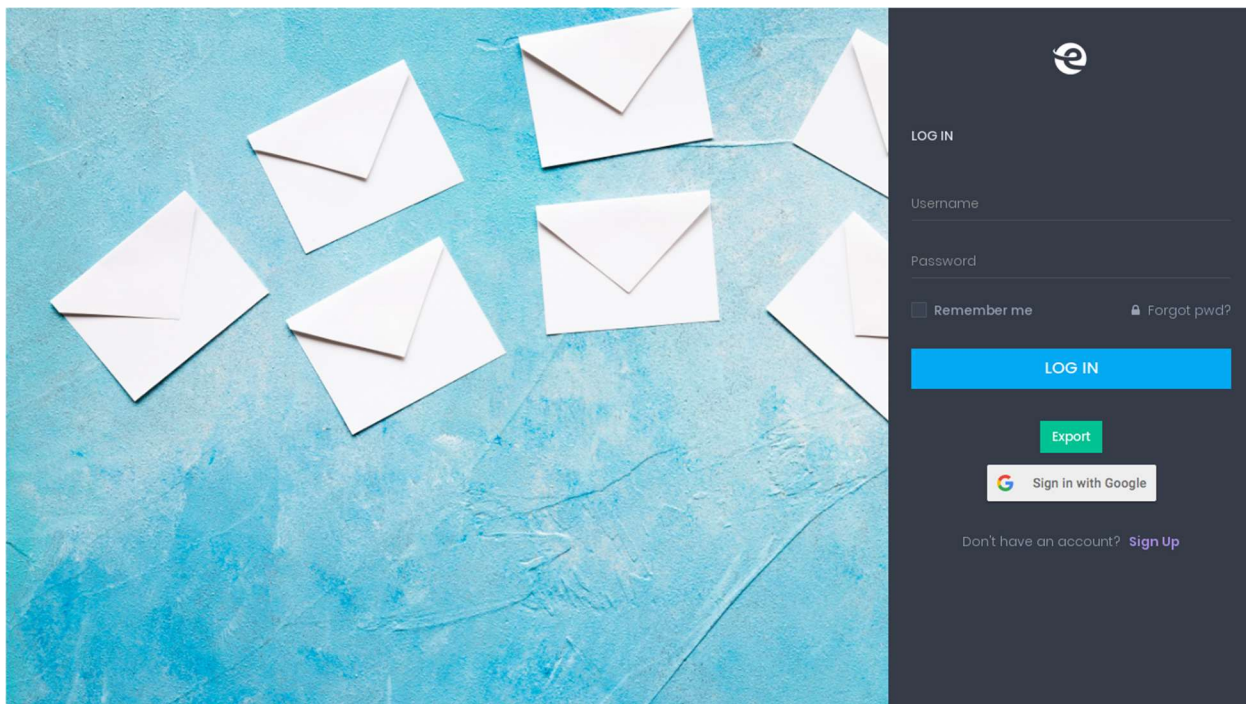


Figure 6

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.

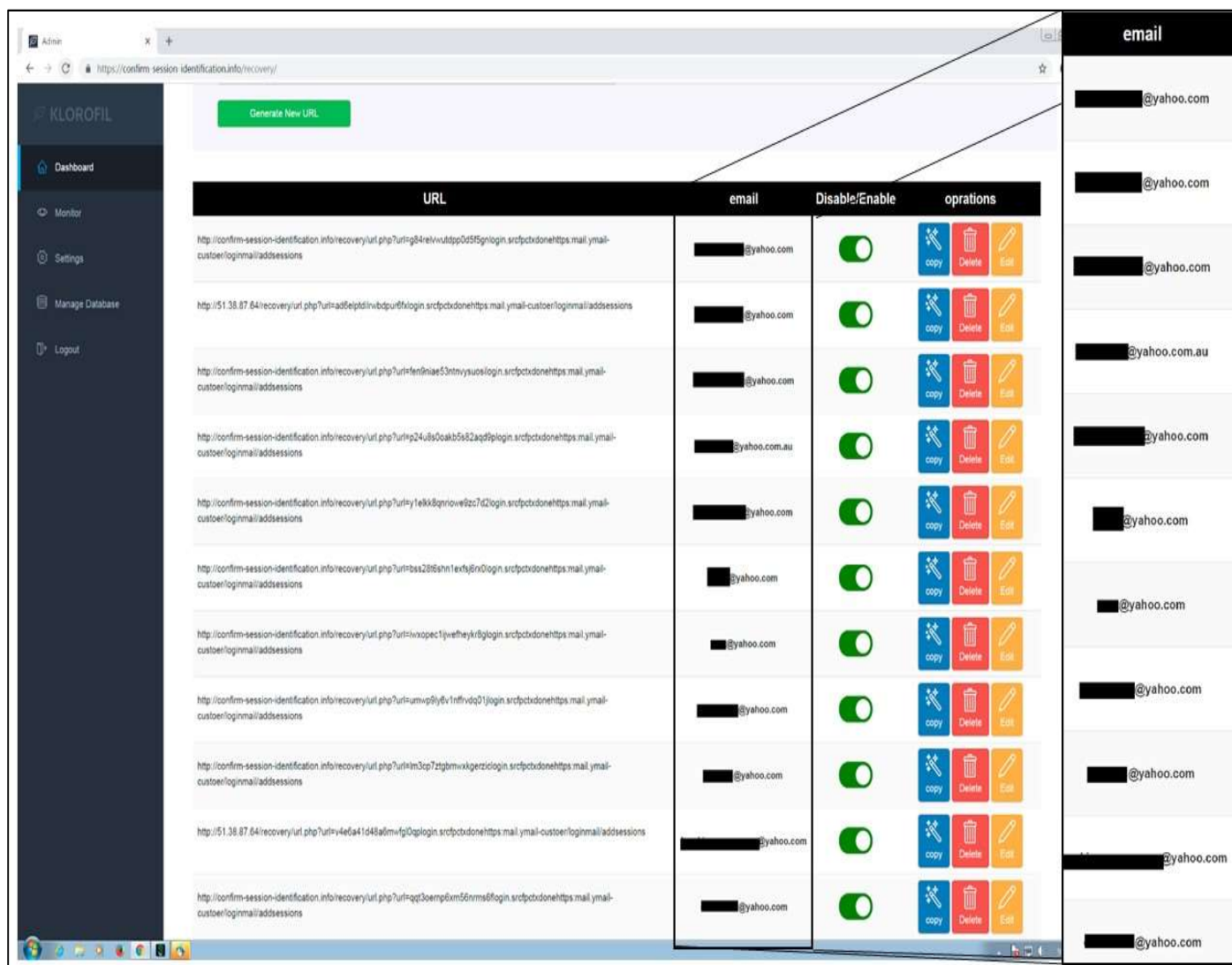
16. The Phosphorus defendants have targeted victims who are using Microsoft email services, and Microsoft investigators, by inspecting login history, have confirmed that Phosphorus defendants have intruded into those accounts potentially to steal information of Microsoft's users. **Figures 1 and 2** 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 CloudFlare 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 browser window with the address bar displaying <https://confirm-session-identification.info/recovery/>. The page has a dark sidebar with the 'KLOROFIL' logo and navigation links: Dashboard, Monitor, Settings, Manage Database, and Logout. The main content area features a green 'Generate New URL' button and a table with the following columns: URL, email, Disable/Enable, and operations.

URL	email	Disable/Enable	operations
http://confirm-session-identification.info/recovery/url.php?url=ing84relvvutdp05f5glogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://51.38.87.64/recovery/url.php?url=ad8eipdlinvbdpurlflogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=infen0iae53nrvysuoclogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=ip24u850akb562aqdlogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com.au	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=iy1ekkkgnr0ve7c7d2login.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=bsx28fahh1exty8rx0login.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=ixvopect1fwefheykrlogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=umwpg9lydv1nfrvdq0jlogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=im3cp7ztgbmwxkgerziclogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://51.38.87.64/recovery/url.php?url=iv4ed41648afmwfg0glogin.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit
http://confirm-session-identification.info/recovery/url.php?url=qq3oemp6xm56nms6login.srctpcxdonehttps.mail.ymail-customerloginmail/addresses	[redacted]@yahoo.com	<input checked="" type="checkbox"/>	copy, Delete, Edit

To the right of the table, a separate column labeled 'email' lists the email addresses for each row, all of which are redacted except for the domain part (e.g., @yahoo.com, @yahoo.com.au).

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
██████████@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
██████████@yandex.com

Email Password reporter
██████████

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 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. 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 14th day of May, 2019.

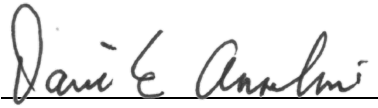

David E. Anselmi

EXHIBIT 1

APPENDIX A

.COM, .NET DOMAINS

Registry

c/o

VeriSign, Inc.

VeriSign Information Services, Inc.

12061 Bluemont Way

Reston, Virginia 20190

United States

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

.INFO DOMAINS

Registry

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

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

.WORLD DOMAINS

Registry

Binky Moon, LLC

Donuts Inc.

5808 Lake Washington Blvd. NE, Suite 300

Kirkland, WA 98033

United States

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
----------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------