**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-10, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	)	Civil Action No: 1:20CV730 **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

DECLARATION OF PIERRE ("PETER") ANAMAN IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Pierre ("Peter") Anaman, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU") within the company's Corporate, External, and Legal Affairs ("CELA") department. I make this declaration in support of Microsoft's Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated and based on my review of records Microsoft maintains in the ordinary course of business. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. INTRODUCTION

2. In my role at Microsoft, I personally oversee, coordinate and participate in investigations into activity that jeopardizes the integrity of Microsoft's systems and the safety of customer data. Through this work, I became personally familiar with phishing schemes that are

designed to steal personally identifiable information and confidential information from Microsoft's customers, and the significant efforts Microsoft takes to protect against such harms. Before joining Microsoft, I was a Senior Internet Investigations Manager at the law firm Covington & Burling from 2000 through 2008. Before that, I was a Forensic Accounting Data Analyst Team Leader at PricewaterhouseCoopers from 1998 through 2000. I am a graduate of University of Surrey with a Bachelor of Science degree in Law and French and obtained a Postgraduate Legal Practice Course at the Law School called College of Law, Surrey, UK. I was a cadet officer in the Écoles Spéciale Militaires de Saint-Cyr, Coëtquidan, France and a Platoon Officer in the French Army. I have been employed by Microsoft since 2008.

II. OVERVIEW OF INVESTIGATION INTO DEFENDANTS

3. My declaration concerns sophisticated criminals engaged in a complex scheme to unlawfully obtain access to personal and confidential information of Microsoft customers. Specifically, it describes an online criminal network that sends phishing emails containing deceptive messages concerning the global COVID-19 pandemic or other socially engineered lures in order to induce targeted victims to click on malicious links in those emails. These phishing emails are designed to look like they come from an employer or other trusted source. Once the victims click on the malicious links, they are led to servers which present the victims with a malicious Web Application ("Web App").[1] The malicious Web App interacts with Microsoft's Office 365 services, as described more fully below. Having convinced the victims that the original phishing email was sent by a trusted source, the criminals then cause the victims to erroneously believe that the Web App also originates from the same trusted source and, most

[1] For clarity, the references here to a "Web App" do not relate to mobile apps. Rather, the Web App is software running on servers controlled by Defendants and which can interact with and obtain access to Microsoft Office 365 accounts.

importantly, is approved or published by Microsoft. As a result, targeted victims are deceived into clicking a button that grants the malicious Web App, and therefore the criminals, access to the victims' Office 365 account including the account contents, such as email, contacts, notes and material stored in the victims' OneDrive for Business cloud storage space and corporate SharePoint document management and storage system. The attacker may also be able to access and alter account settings as the attacker has full control over the account. Until the Web App is disabled or token revoked, the attacker will have continued access to the Office 365 account.

4. In this way, the attackers attempt to gain unauthorized access to Office 365 accounts of Microsoft's customers. Notably, as more fully described below, this scheme enables unauthorized access without explicitly requiring the victims to directly give up their login credentials at a fake website or similar interface. Rather, the victims input their credentials into legitimate Office 365 login pages that are not under the cybercriminals' control. In some instances, the victim may alternatively be asked to confirm the identity linked to their device in lieu of entering credentials. Thereafter, the cybercriminals utilize the malicious Web Apps to gain access based on the victims' previous entry of credentials. This highly deceptive scheme has the same practical effect as direct theft of credentials, except that the victims are not aware that they unintentionally provided cybercriminals access to their Office 365 account.

5. The precise identities and locations of the cybercriminals behind this unlawful scheme are generally unknown, but they targeted Microsoft customers across the globe including specifically in the area of Alexandria, in the Eastern District of Virginia. These cybercriminals are named as John Does 1 and 2 in this case (referred to here as "Defendants"). I investigated the infrastructure described in this declaration, including malicious internet domain names. During my investigation, I reviewed a publicly available database of information, called a

"WHOIS" database. The WHOIS database generally contains the names, mailing addresses, email addresses and similar contact information provided by parties when registering domain names. I determined that the Defendants registered internet domains using private registration services, which conceal the contact information ordinarily available in the WHOIS database. However, even with such information concealed, the private registration services assign Defendants arbitrary "proxy" email addresses associated with domain names and make those email addresses available in the public WHOIS database. The private registration services provide the proxy email addresses publicly for the purpose of enabling communication with Defendants regarding their domain names. I believe that the email addresses are the only known possible way of communicating the existence of this action specifically to the Defendants.

6. Microsoft commits tremendous resources to detecting and blocking threats to its customers and their accounts. In December 2019, Microsoft first detected early instances of the Defendants' malicious phishing and Web App scheme. I began collecting information regarding Defendants' creation and deployment of the malicious Web Apps and known attempts by the Web Apps to access Microsoft's cloud infrastructure. Based on patterns discovered at that time, Microsoft developed technical means to block the Defendants' activity and disabled the Web Apps that existed at that time. In this way, Microsoft was, thus far, able to protect its customers. However, recently Defendants have begun creating new malicious Web Apps. Defendants' activities pose a persistent risk. Defendants have sent millions of phishing emails. Defendants continue to evolve their tactics, now leveraging messages purporting to be about important COVID-19 issues, as discussed more fully below. Defendants have designed these COVID-19-themed phishing emails, like the previous emails, to deceive recipients to click on a link and thereafter grant access to their Office 365 accounts via new versions of the malicious Web Apps.

Given the risk posed by Defendants reconstituting their operations, including use of existing infrastructure to carry out further attacks on Microsoft's Office 365 services and customers, and attempts to put in place new infrastructure, it is necessary to seek immediate relief in this action.

7. I recently investigated the existing domain names and IP address infrastructure that Defendants prepared for the Web App attacks discussed in this declaration. I reviewed the functionality of this infrastructure in relation to Defendants' Web Apps. I also investigated the network traffic associated to the infrastructure that provided insights on how the domain names were being used in the attack. Further, I reviewed internal server logs to identify how the infrastructure was being used to register OAuth 2.0 Web Apps. In addition to using domain names that attempted to impersonate Microsoft Office, the Defendants used Web App names that attempted to impersonate legitimate Microsoft services. During my investigation, I monitored the Defendants' domain names and IP addresses, and investigated email addresses and other "WHOIS" record information regarding those domain names and IP addresses.

8. Based on my investigation and analysis, I determined that Defendants attempted to target Microsoft customers in both the private and public sectors, including businesses in different industries. Defendants frequently targeted the C-suite, senior managers, and regional leaders of a variety of businesses and organizations.

9. Defendants' acts indicate that their objective is to obtain unlawful access to Office 365 accounts and obtain sensitive communications from within the accounts. According to my investigation, Defendants pose a current and ongoing threat to Microsoft and the security of its customers.

III. MICROSOFT'S OFFICE 365 SERVICES AND PROTECTION MEASURES

10. Office 365 is an online service that provides access to Microsoft's Office software on a subscription basis. Customers purchase a subscription to Office 365 that may provide

access to both cloud and locally stored versions of the software. Use of Office 365 requires an online account.

11. Microsoft goes to great lengths to protect customer accounts. In particular, Microsoft engineered Office 365 to prevent spam, viruses and malware from even reaching Office 365 users. For example, Microsoft built multiple spam filters into Office 365 accounts, so customers' email addresses are protected from the moment the first message is received. Microsoft uses multiple anti-malware engines to detect potentially dangerous software sent to users. Microsoft also offers Office 365 Advanced Threat Protection, which helps protect a user's mailbox against new, sophisticated attacks in real time. In addition to stopping phishing attempts before they reach users, Microsoft also investigates phishing attacks to identify and stop the criminals behind these malicious attacks.

12. Microsoft also enables integration of Web App functionality into Office 365 and other cloud services. In general, Web Apps are widely used in organizations to drive productivity, create efficiencies, and increase security in a distributed network. Microsoft takes many measures to monitor and block malicious Web Apps, based on telemetry indicating atypical behavior. However, in cases where threat groups suddenly and massively scale their activity, and move quickly to adapt their activities to evade Microsoft's defensive mechanisms, additional measures, such as the relief requested in this action, are necessary to mitigate injury and to protect Microsoft and its customers. In this case, as discussed in detail below, in order to ensure protection against Defendants' malicious Web Apps, it is necessary to supplement Microsoft's defensive efforts and to proactively disable Defendants' existing malicious infrastructure.

13. I reach this conclusion based on my own investigation of Defendants' activities.

Through various investigative techniques, including those summarized above, Microsoft uncovered Defendants' COVID-19-themed phishing and malicious Web App scheme aimed at Microsoft Office 365 users. I participated in the investigation of Defendants' scheme and am personally familiar with the details of Microsoft's investigation.

IV. DEFENDANTS USE DECEPTIVE COVID-19 MESSAGES AND MALICIOUS WEB APPS IN AN ATTEMPT TO COMPROMISE OFFICE 365 ACCOUNTS

Phishing Attacks

14. Phishing is a broad term that encompasses many different activities. The most well-known phishing schemes fall under the umbrella of social engineering attacks. Generally, these schemes involve an individual or online criminal network creating spoofed emails that purport to be from legitimate and trusted businesses, agencies, or individuals.

15. In a typical scenario, phishing emails are designed to lead recipients to fake websites that trick users into divulging sensitive information, such as financial account data, login credentials, and other personally identifiable information. Criminals operating the fake websites harvest personal information and then use such information to unlawfully access peoples' accounts for illicit gain. Cybercriminals also sell stolen personal information to other criminals who use the information to inflict further harm on the victims or for further illicit purposes.

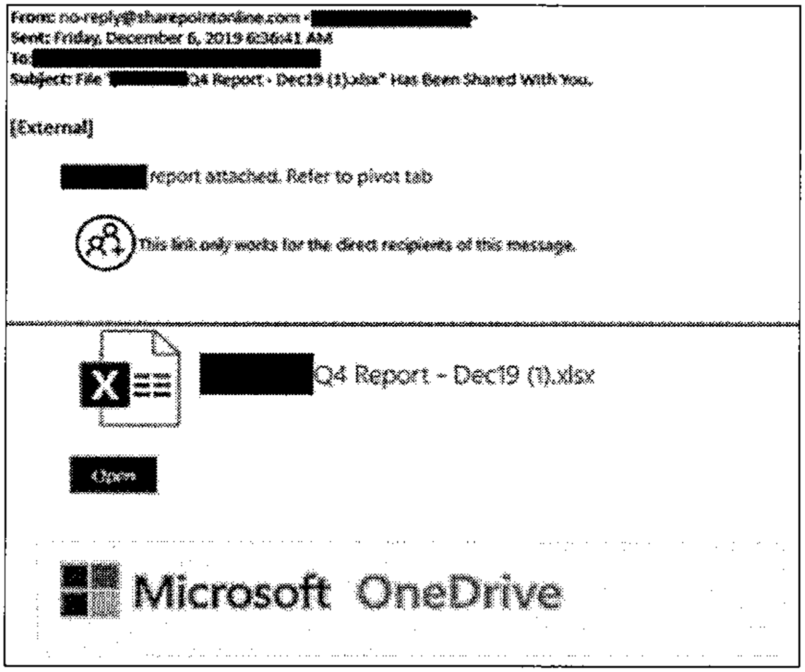
Defendants Send COVID-19 Themed Phishing Emails To Lure Victims

16. Defendants send phishing emails to Microsoft's customers who are using its Office 365 email service. Defendants design these emails in a manner that deceptively impersonates legitimate communications originating from Microsoft's SharePoint or OneDrive for Business cloud storage services. For example, in these emails, Defendants leverage the presence of the "Microsoft" and "OneDrive" trademarks, and the presence of the term

"SharePoint" in the "From" email address to convince recipients that this is a legitimate communication from Microsoft. Further, Defendants send phishing emails from email addresses that contain references to companies or entities associated with the recipient, such as the name of their employer. Defendants may send phishing emails from compromised accounts of parties, such as employers or colleagues, within the recipient's trusted network.

17. Defendants also include in the phishing emails other deceptive content, usually what appears to be a link to "Open" a Microsoft Excel document. In fact, as detailed further below, this icon in the email is a malicious link that begins the process of Defendants attempting to obtain access to the victims' Office 365 accounts. Because victims are usually familiar and experienced with the legitimate file-share method using OneDrive for Business or SharePoint, and because the email appears to originate from a trusted entity (such as an employer) and contains typical data that might appear in a legitimate file-sharing email, the victims are tricked into clicking the malicious link.

18. When Defendants first began carrying out this scheme, the phishing emails contained deceptive themes associated with generic business activity. For example, the malicious Excel link would be named in a manner that uses information suggesting it is associated with a trusted entity and business terms such as "Q4 Report – Dec19." An example of an earlier phishing email is reproduced as **Figure 1**:



From: no-reply@sharepointonline.com <[redacted]>
Sent: Friday, December 6, 2019 6:36:41 AM
To: [redacted]
Subject: File "[redacted]Q4 Report - Dec19 (1).xlsx" Has Been Shared With You.

[External]

[redacted] report attached. Refer to pivot tab

This link only works for the direct recipients of this message.

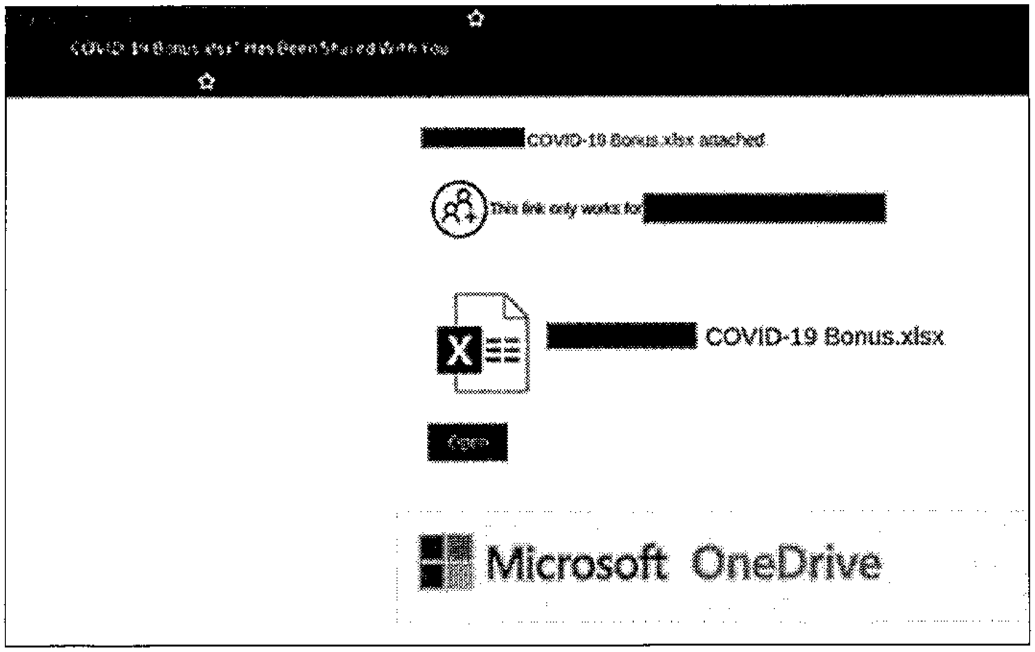
[redacted]Q4 Report - Dec19 (1).xlsx

Figure 1

19. I redacted Figure 1, replacing original text with black boxes, to protect personal information of the victim individual and company involved. In Figure 1, the first black box in the "From" line is the email address of the sender that is typically a compromised user whose account is used to send the phishing email. The second black box from the top, in the "To" line, is the email address of the recipient and person being targeted. The third, fourth and fifth black boxes in the "Subject" line and body of the email are strings from the domain name of the victim email address without the Top-Level Domain (TLD). For example, "victimstring" from "victim[@]victimstring.TLD".

20. Recently, as Defendants have renewed their efforts to target Microsoft and its customers, Defendants have created phishing emails containing deceptive themes associated with COVID-19. For example, Defendants now name the malicious Excel link in a manner suggesting it is associated with a trusted entity and use terms such as "COVID-19 Bonus". An

example of such a COVID-19 related phishing email is reproduced as **Figure 2**:



"COVID-19 Bonus.xlsx" Has Been Shared With You

[redacted] COVID-19 Bonus.xlsx attached.

This link only works for [redacted]

[redacted] COVID-19 Bonus.xlsx

Figure 2

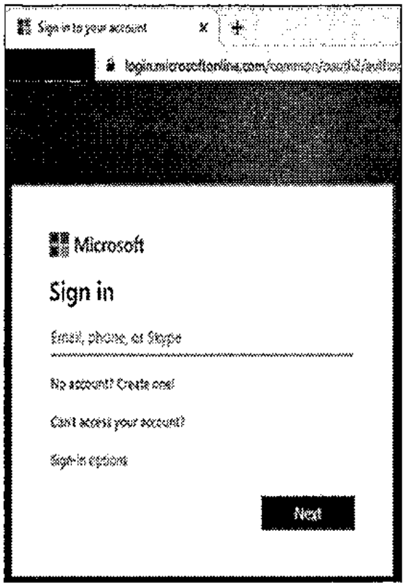
21. I redacted Figure 2, replacing original text with red boxes, to protect personal information of the victim individual and company involved. In Figure 2, the first red box is the email of the sender that is typically a compromised user whose account is used to send the phishing email. The third and fifth red boxes from the top are the email addresses of the recipient and person being targeted. The second, fourth and sixth red boxes from the top are strings from the domain of the victim email address without the Top-Level Domain (TLD). For example, "victimstring" from "victim[@]victimstring.TLD".

22. The scale of these phishing attacks is immense. In just one week, Defendants sent phishing emails to millions of Office 365 users. The scale of Defendants' attempts to reach potential victims and Defendants' ability to continuously create and deploy new malicious Web Apps from existing infrastructure, discussed below, demonstrates the substantial ongoing risk

posed by Defendants.

Defendants Attempt To Access Office 365 Through Malicious Web Apps

23. After Defendants socially engineer the victim to click the link in the body of the email, the victim is then prompted to sign into Microsoft's legitimate Office 365 portal at login.microsoftonline.com. The login portal presented to the victim at this point is reflected at **Figure 3** below, where the victim enters their user name, and at **Figure 4**, where the victim enters their password:



Sign in to your account

login.microsoftonline.com/common/oauth2/autho

Microsoft

Sign in

Email, phone, or Skype

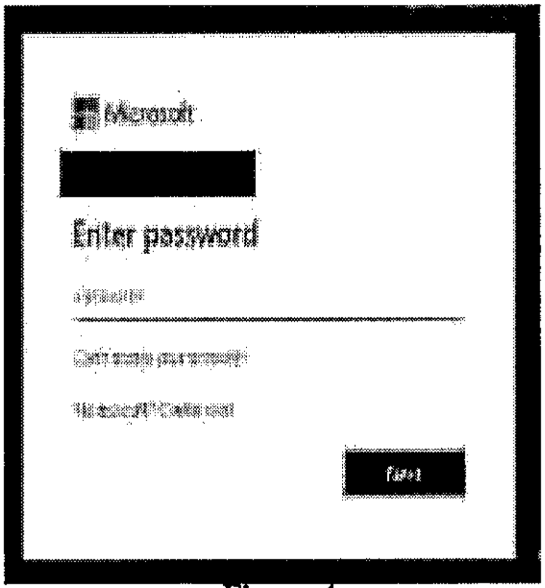
No account? Create one!

Can't access your account?

Sign-in options

Next

Figure 3



Microsoft

[redacted]

Enter password

[illegible]

[illegible]

[illegible]

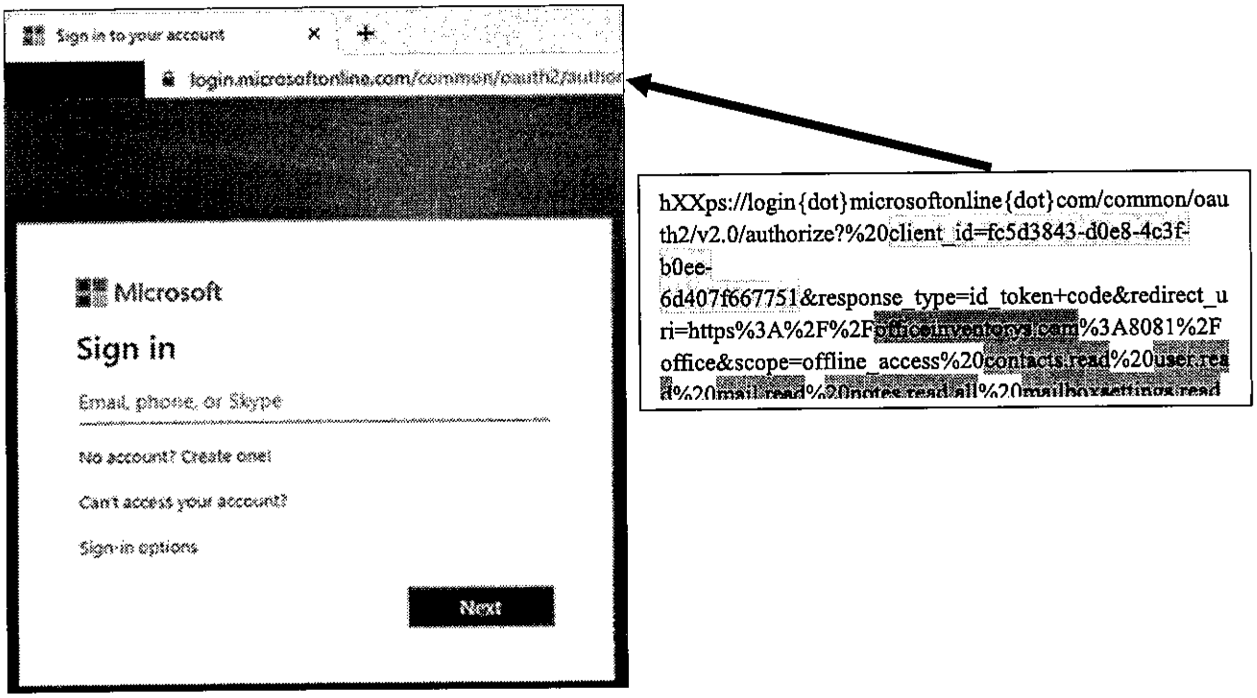
[illegible]

Figure 4

24. Once the Microsoft identity platform recognizes the credentials, the Defendants leverage an industry standard technical facility used by Microsoft known as "OAuth 2.0" to request access to victims' Office 365 accounts and to deceive victims into providing such access. The following describes the process by which Defendants misuse OAuth 2.0 to obtain access to victims' Office 365 accounts.

25. The first step in Defendants' misuse of OAuth 2.0 involves processing information contained within the URL that the Defendants used in the phishing email to take the

victim to the legitimate Office 365 portal. That URL contains additional information that defines the level of access requested by the malicious Web App and to be granted by the unsuspecting user. As seen in **Figure 5** the malicious URL contains several elements, highlighted below:



hXXps://login{dot}microsoftonline{dot}com/common/oauth2/v2.0/authorize?%20client_id=fc5d3843-d0e8-4c3f-b0ee-6d407f667751&response_type=id_token+code&redirect_uri=https%3A%2F%2Fofficeinventorys.com%3A8081%2Foffice&scope=offline_access%20contacts.read%20user.read%20mail.read%20notes.read.all%20mailboxsettings.read

Figure 5

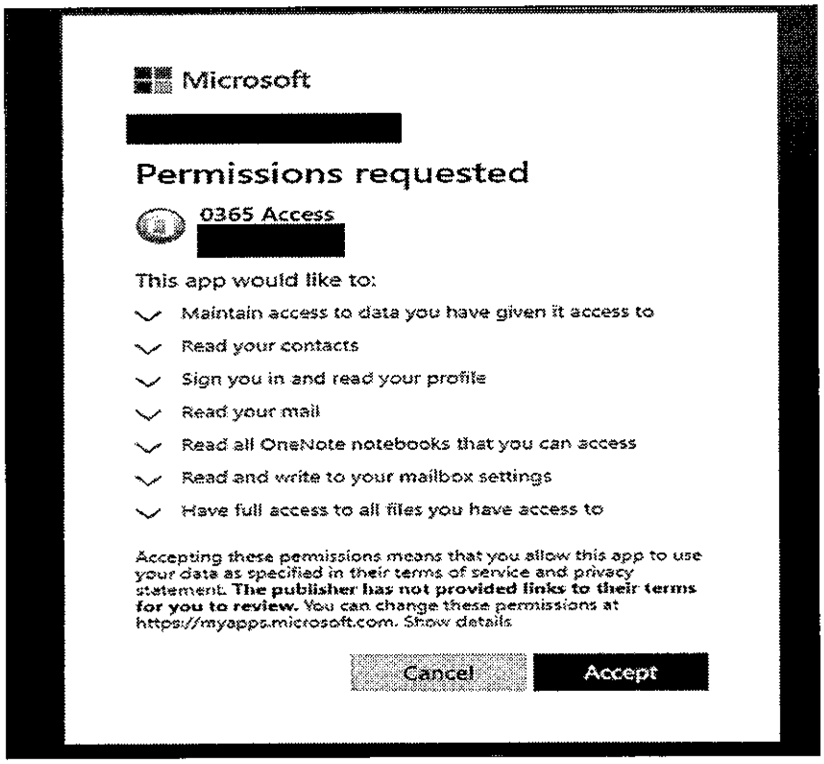
26. First, the malicious URL contains a parameter called **"client_id"** (highlighted in yellow above). The "client_id" is an identifier which is processed by the OAuth 2.0 facility to identify the Defendants' malicious Web App.

27. Second, the malicious URL contains a domain name, in this case **"officeinventorys.com"** (highlighted in green above). That is a domain name controlled by Defendants and one of the domain names that is the subject of this action. The Defendants' malicious Web App is hosted on servers associated with this domain name. In addition, once the user is deceived into accepting the Web App, authorization codes and/or tokens are sent to the servers associated with this domain name.

28. Third, the malicious URL contains other access parameters that operate as

instructions regarding what Office 365 resources to access. Highlighted in blue in the example above are parameters that define the level of access to Office 365 "**mail,**" "**contacts,**" "**files**" and "**notes.**" Further, the parameters define access to "**read**" those resources and to "**write**" (*i.e.* make changes to) Office 365 mailbox settings and files. Access is only granted once the unsuspecting user accepts an OAuth 2.0 request, as discussed further below.

29. Upon login, the Defendants cause the OAuth 2.0 facility to use the "client_id" and the access parameters noted above to produce a deceptive user interface that displays the name of the malicious Web App and displays a list of access levels for which the malicious Web App is requesting consent. Defendants leverage this user interface in a manner that deceptively presents the trademark "Microsoft" and the deceptive formulation "0365," designed to look like the genuine Office 365. The deceptive Web App user interface, which the victim still believes to be an authorized process associated with a trusted entity (such as an employer), requests the victim to grant the following permissions regarding Office 365 access: read contacts, read user profile, read user emails, modify mailbox settings (i.e. forwarding rules) and all files. An example of a deceptive Web App user interface is shown at **Figure 6**.



Microsoft

[redacted]

Permissions requested

0365 Access

[redacted]

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Figure 6

30. I redacted Figure 6, replacing original text with black boxes, to protect personal information of the victim individual and company involved. In Figure 6, the upper most black box would show the email address of the victim. The lower black box would show the domain name or the name of the app publisher associated to the malicious Web App.

31. After the user clicks "Accept," the OAuth 2.0 system generates an authorization code which is subsequently redeemed for one or more authentication tokens for that victim. This authentication token effectively serves the same function as the victim's credentials, communicating to the OAuth 2.0 system that the victim is authorized to have access to Office 365 account. In this way, the attacker is able to access the compromised Office 365 accounts by enabling the malicious Web App to gain access to the account in accordance with designated access parameters indicated in the graphical user interface depicted in Figure 6.

32. In this way, Defendants deceive victims to not only log into Office 365 and generate needed OAuth 2.0 tokens, but to further click on the "Accept" button, providing Defendants unauthorized access to defined resources within the Office 365 account. In this case, the victim will have granted access to all of the resources set forth above in Figure 6. Once Defendants deceive the victim into clicking "Accept," the OAuth 2.0 facility sends the previously generated OAuth 2.0 token and associated permissions to the Defendants' malicious Web App located at the Defendants' malicious domain name ("officeinventorys.com" in the example above). Once the malicious Web App receives the OAuth 2.0 token and associated permissions, this enables the Defendants to use the malicious Web App to make API calls to access the victim's Office 365 account. In accessing Microsoft's Office 365 servers in this way, Defendants are accessing, without valid authorization, computers that can be used in interstate

commerce.

33. If Defendants were able to successfully access the content of Office 365 accounts pursuant to this phishing attack, it would be possible for them to carry out activities such as sending deceptive emails from the compromised user, monitoring communications and transactions in order to carry out wire fraud or other forms of fraud, or simply stealing further financial credentials, account credentials or other valuable information that may be available. It is both the potential risk of Defendants' access to Microsoft's server resources, in general, and the potential risk of these further illegal activities that render the relief requested in this matter urgent and critical. All of the activities described above cause and threaten to cause serious injury to Microsoft and its customers.

V. DEFENDANTS' HARMFUL DOMAIN NAMES USED TO CARRY OUT ATTACKS AGAINST MICROSOFT OFFICE 365 ACCOUNTS

34. As discussed, Defendants use various domain names to host and deliver malicious Web Apps. Defendants have also registered domain names to prepare for other illegal activities, such as attempts to access the content of victims' emails. The following are domain names that Defendants are currently leveraging in their infrastructure, each of which is a .COM top-level domain (TLD) operated by Verisign as the Internet Corporation for Assigned Names and Numbers (ICANN) accredited registry within the Eastern District of Virginia.

Domain Names	Domain Registry	Registry Operator	Registry Location	Domain Registrar	Registrar Location
officeinventorys.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officehnoc.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officesuited.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officemtr.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officesuitesoft.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States

mailitdaemon.com	.COM	Verisign	VA, United States	GoDaddy.com, LLC	AZ, United States

35. As can be seen, many of these domain names are masquerades of Microsoft's Office products and services, such as "officeinventorys.com", "officesuitesoft.com", and "officehnoc.com". This is consistent with the deceptive nature of the fraud targeting Office 365. These domain names are used to create malicious Web Apps, consistent with their deceptive theme. Defendants also registered the domain name "mailitdaemon.com," which has been and is used to receive mail forwarded by Office 365 accounts successfully compromised by Defendants. In this domain name, Defendants use generic nomenclature seen in regular network administration, such as "mail," "IT" (information technology) and "daemon" (a process used in an email server).

36. These domain names used by Defendants are identified in Appendix A to the Complaint and attached as **Exhibit 1** to this declaration. As part of my investigation, I queried for these domain names in a publicly accessible "WHOIS" database, which contains available contact information regarding the registrants of these domain names, domain name registrars, and domain name web host. Information in Exhibit 1 is generated from the publicly available WHOIS registration data. Exhibit 1 includes, for each domain name, the available public contact information for Defendants and contact information for the relevant third-party domain registry, Verisign, Inc., as well as the contact for the relevant domain registrars.

VI. DEFENDANTS' CYBERCRIME SCHEME RELIES ON TRADEMARK INFRINGEMENT

37. In several different ways, Defendants deceive victims and disguise their malicious scheme by unauthorized reproduction of Microsoft's trademarks and brands. For example, as seen above and in **Exhibit 1**, Defendants have registered domain names that leverage the term "office" associated with Microsoft's "Office 365" trademark, brand and services. Additionally,

in the malicious phishing emails and Web App, Defendants reproduce the trademarks "Microsoft," the Microsoft corporate logo, "Office 365," "OneDrive," and "SharePoint," as well as confusingly similar variants such as "0365."

38. Further, Defendants have developed a technique where a victim clicking on a malicious link in a phishing email is first connected to the legitimate "microsoftonline.com" domain name. The victim clicks on the link, in reliance on deceptive information contained in the phishing email that causes the victim to mistakenly believe they are connecting to resources of a trusted entity such as an employer. This technique deceives and confuses victims into thinking the link is not part of a malicious scheme because the domain name is owned by Microsoft and incorporates Microsoft's trademarks and branded material. Yet, unknown to the victim, the Defendants are delivering a malicious Web App that is not in fact affiliated with Microsoft or any other trusted entity. In these ways, Defendants' activities deceptively use Microsoft's trademarks and brands. Defendants' use of Microsoft trademarks and brands is meant to confuse Microsoft's customers into clicking on malicious links and clicking "Accept" in the deceptive Web App user interface, which they mistakenly believe are sponsored by Microsoft or trusted entities.

VII. DEFENDANTS ATTACKED MANY MICROSOFT CUSTOMERS IN THE EASTERN DISTRICT OF VIRGINIA AND AROUND THE WORLD

39. Through my investigation, I determined that Defendants affirmatively targeted Microsoft customers in Virginia, including the Eastern District of Virginia, and throughout the United States and the world.

40. I recently investigated the location of potential victims, which Defendants attempted to target through the scheme set forth above. Such targeted entities are located, among other places, in Alexandria, Arlington, Chantilly, McLean, Falls Church, Herndon and

Reston. I plotted the locations of these targeted potential victims on maps of Virginia to represent the locations to which Defendants have directed their relevant activity, in **Figure 7**.

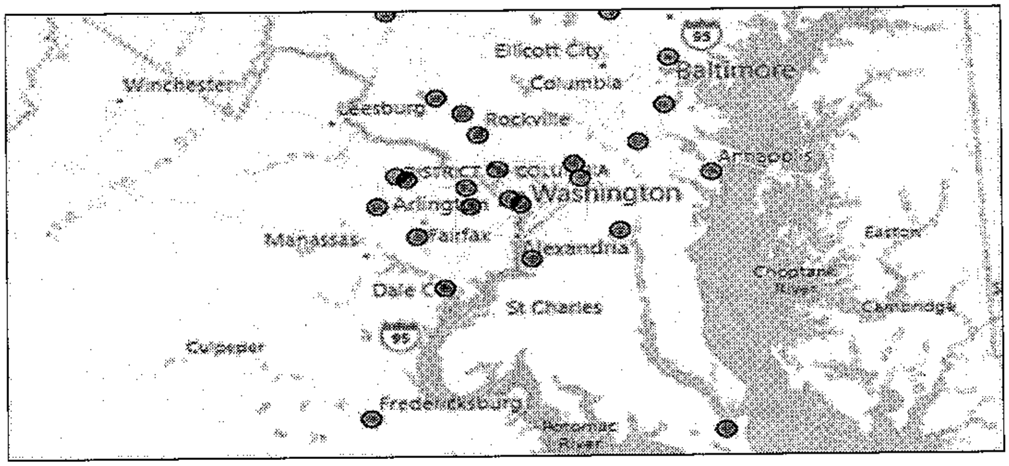


Figure 7

VIII. <u>HARM TO MICROSOFT</u>

41. Microsoft® is a provider of the Office 365,® OneDrive,® and SharePoint® cloud-based business and productivity suite of services, all offered under those trademarks and in connection with the Microsoft mark and the Microsoft corporate logo. Microsoft has invested substantial resources in developing high-quality products and services. 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, 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 services and its brand, including the Microsoft, Office 365, OneDrive and SharePoint trademarks.

42. As described in detail, Defendants use these trademarks, brands and confusingly similar variants in phishing emails and web interfaces presented to Microsoft's customers and

potential victims. Defendants' use of Microsoft trademarks and brands is meant to confuse and does cause confusion among Microsoft's customers and recipients of these communications, as those parties incorrectly perceive a relationship between Microsoft and the malicious activities of Defendants.

43. All of these activities cause injury to Microsoft. 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 they work for, may incorrectly attribute Defendants' malicious activities and the result of those activities, to Microsoft's products and services, should Defendants be able to carry out future attacks. Therefore, Defendants' activities dilute and tarnish the value of these Microsoft trademarks and brands. The activities carried out by Defendants, described above, injure Microsoft and its reputation, brand and goodwill because victims targeted by this scheme are likely to incorrectly believe that Microsoft is the source of problems caused by Defendants.

44. Microsoft is similarly injured because Defendants direct their attempted intrusions to accounts hosted on Microsoft's servers. Microsoft must bear this extraordinary burden. Microsoft must develop technical countermeasures and defenses, to suppress Defendants' activities, respond to customer service issues caused by Defendants and must expend substantial resources dealing with the injury and confusion. Microsoft has had to expend substantial resources to resist the ongoing attempted attacks on its infrastructure, products, services, and customers. Given that Defendants are continuing their targeting of Microsoft, and that such will be ongoing, this poses severe risk of injury to Microsoft, in that it ultimately threatens Microsoft's brands and customer relationships.

45. Based on my experience assessing computer threats and the impact on business, I

conclude that customers may incorrectly attribute the negative impact of Defendants to Microsoft. Further, based on my experience, I therefore conclude that if permitted to continue unabated, there is a serious risk that Defendants may interfere with Microsoft's customer relationships.

IX. TRANSFERRING CONTROL OF DEFENDANTS' HARMFUL DOMAIN NAMES WITHOUT FIRST INFORMING THE DEFENDANTS IS THE ONLY WAY TO PREVENT ONGOING INJURY

46. Defendants' illegal activities will not be easy to disrupt. Evidence indicates that Defendants are persistent, sophisticated, pose an immediate risk and are determined to attempt to overcome Microsoft's technical mitigation steps to date.

47. The vulnerable point in Defendants' operations are the internet domain names through which Defendants host and deploy malicious Web Apps and register those apps. Defendants' malicious infrastructure is set forth in **Exhibit 1** to this declaration.

48. Granting Microsoft possession of these domain names will enable Microsoft to cut off the existing means by which Defendants can deploy malicious Web Apps or facilitate unauthorized access to Microsoft's Office 365 services. Giving Microsoft possession of Defendants' active domain names will directly disrupt Defendants' infrastructure, mitigating risk and injury to Microsoft and its customers.

49. Based on my prior experience with similar operations and malicious technical infrastructure, I conclude that the only way to suspend the injury caused to Microsoft, its customers, and the public, is to take the steps described in the Proposed Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder Defendants' ability to compromise additional accounts, to identify new potential victims to target and to attempt to exfiltrate valuable information from Microsoft's servers. In the absence of such action, Defendants will be able to continue using

this infrastructure to target new accounts, exposing potential new victims to Defendants.

50. Defendants' techniques are designed to resist technical mitigation efforts, eliminating straightforward technical means to curb the injury being caused. For this reason, providing notice to Defendants in advance of redirection of the domain names at issue would render attempts to disable the infrastructure futile. Further, when 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. Based on my experience observing the operation of numerous threat actors such as Defendants, I believe Defendants would attempt to conceal the extent of their operations and minimize the extent of the victimization to their targets and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

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 29th day of June, 2020, in Seattle, Washington.

Peter Anaman

Peter Anaman

<u>**EXHIBIT 1**</u>

<u>**.COM DOMAINS**</u> ***<u>Registry</u>*** **Verisign, Inc.** **Verisign Information Services, Inc.** **Verisign Global Registry Services** **12061 Bluemont Way** **Reston Virginia 20190** **United States**	
OFFICEINVENTORYS.COM	***<u>Registrar</u>*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officeinventorys.com Registry Domain ID: 2502955959_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-03-13T16:12:21.00Z Registrar Registration Expiration Date: 2021-03-13T16:12:21.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: 649712c9fae543dbb1aea0fd78c804ed.protect@whoisguard.com Registry Admin ID:

	Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: 649712c9fae543dbb1aea0fd78c804ed.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: 649712c9fae543dbb1aea0fd78c804ed.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T11:42:28.55Z <<<
OFFICESUITESOFT.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officesuitesoft.com Registry Domain ID: 2497852670_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-02-28T04:39:59.00Z Registrar Registration Expiration Date: 2021-02-28T04:39:59.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107

	Reseller: NAMECHEAP INC Domain Status: clientHold https://icann.org/epp#clientHold Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: 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: 361349b7019e4ffeaa8189520398802e.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: 361349b7019e4ffeaa8189520398802e.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: 361349b7019e4ffeaa8189520398802e.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System:

	http://wdprs.internic.net/
OFFICEHNOC.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officehnoc.com Registry Domain ID: 2482044724_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-01-19T15:18:12.00Z Registrar Registration Expiration Date: 2021-01-19T15:18:12.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: cc9604648d71460288ef63ae22744aa5.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: cc9604648d71460288ef63ae22744aa5.protect@whoisguard.com

	Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: cc9604648d71460288ef63ae22744aa5.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T12:23:12.95Z <<<
OFFICESUITED.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officesuited.com Registry Domain ID: 2466161464_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2019-12-11T20:07:57.00Z Registrar Registration Expiration Date: 2020-12-11T20:07:57.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: 32d1ef4e2c624df59f656fc1399745c4.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: 32d1ef4e2c624df59f656fc1399745c4.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: 32d1ef4e2c624df59f656fc1399745c4.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T17:23:43.56Z <<<
OFFICEMTR.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officemtr.com Registry Domain ID: 2460235581_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z

	Creation Date: 2019-11-27T01:01:50.00Z Registrar Registration Expiration Date: 2020-11-27T01:01:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: ca357c245790440db15de36d422c3d18.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: ca357c245790440db15de36d422c3d18.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext:

	Tech Email: ca357c245790440db15de36d422c3d18.protect@whoisguard.com Name Server: pdns1.registrar-servers.com Name Server: pdns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T21:24:09.71Z <<<
MAILITDAEMON.COM	**GoDaddy.com, LLC** **14455 North Hayden Rd., Ste. 219** **Scottsdale, AZ 85260** Domain Name: mailitdaemon.com Registry Domain ID: 2466584834_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2019-12-13T04:09:33Z Creation Date: 2019-12-13T04:09:32Z Registrar Registration Expiration Date: 2020-12-13T04:09:32Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: mailitdaemon.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com

	Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: mailitdaemon.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: mailitdaemon.com@domainsbyproxy.com Name Server: NS17.DOMAINCONTROL.COM Name Server: NS18.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-17T09:00:00Z <<<