IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

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:

FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5

DECLARATION OF CHRISTOPHER COY IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Christopher Coy, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU") Malware & Cloud Crimes Team. 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. 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 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 Engineer, responsible for assessing the quality and value of patents across a diverse set of technology areas in Microsoft's patent portfolio, and analyzing third-party patent

portfolios for acquisition, licensing, or litigation. Prior to that, while also employed by Microsoft, I worked as a Senior Security Program Manager responsible for development of Microsoft's corporate Security Development Lifecycle (SDL) security policy; and as a Software Design Engineer, I led multiple teams responsible for ensuring the quality of a variety of feature areas across Microsoft products, including Windows Phone, Windows 7, Xbox HD DVD, Operations Manager, and msn.com. Before joining Microsoft, I worked for Informix Corporation as a Software Engineer performing quality assurance test development for Informix database systems. In parallel to my Microsoft employment, I am also a United States Navy Reservist having served for 20 years as an Intelligence Officer and a qualified Information Warfare Officer, attaining the rank of Commander. I am a graduate of the University of Kansas, Lawrence, Kansas. I have been employed by Microsoft since March 1998.

3. I have investigated the structure and function of a spearphishing operation called "Bohrium" as well as the activities carried out through this operation, and an assessment of the impact on Microsoft's business and on users of the Internet. The Bohrium operation has caused, and continues to cause, extreme damage to Microsoft and other parties which, if allowed to continue, will be compounded as the case proceeds.

4. I have participated in the investigation of the infrastructure described in this declaration and have determined that the defendants have registered Internet domains using fictitious names and fictitious physical addresses. The defendants have registered domains using email addresses, by which they necessarily communicated with domain registrars in order to register the domains. I believe that the email addresses are the only known possible way of communicating the existence of this action specifically to the defendants. Because the identities of those behind the activity addressed in this declaration are uncertain, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: "Bohrium."

II. OVERVIEW OF INVESTIGATION INTO BOHRIUM AND CONCLUSIONS

5. My declaration concerns an organization that is engaged in sophisticated harmful activity on the Internet. The precise identities and locations of those behind the activity are generally unknown but have been linked by many in the security community to an Iranian group or groups.

6. Microsoft investigators have been monitoring and gathering information on an Iranian activity group, Bohrium, targeting the technology, transportation, government, and high education sectors in the Middle East, with a strong focus on the United Arab Emirates and Saudi Arabia. Bohrium was identified as a cluster of activity disparate from another Iranian cyber group now tracked by Microsoft as Curium. As of 2021, Microsoft observed Bohrium target Information Technology (IT) service providers, including several based in India. Bohrium likely targets the IT service providers to gain access to the customers that fit into their victim profile. Additionally, through its investigation, Microsoft has determined that Bohrium has affirmatively targeted Microsoft customers in the United States.

7. In the course of Microsoft's investigation, my team and I, (1) analyzed and created "signatures" (which can be thought of as digital fingerprints) for the malware and infrastructure used by Bohrium; (2) observed logins to Microsoft services from Bohrium-controlled infrastructure on the Internet; (3) matched reported Bohrium phishing email campaigns to registered domains; (4) monitored internet domain and IP address registrations associated with the Bohrium-controlled email addresses; (5) monitored other pertinent information, such as "Whois" record information regarding internet domains and IP addresses associated with Bohrium; (6) monitored infrastructure frequently utilized by Bohrium in order to identify new domains and confirm resolution settings to Internet Service Providers ("ISPs") often used by Bohrium; and (7) reviewed peer findings and public reporting on Bohrium.

8. The investigative team has developed methods to help us identify new domains registered by the Bohrium actors. Particular features of the Bohrium infrastructure have been identified and patterns of content, non-content, and technical features have been determined to be

exclusively and specifically associated with the Bohrium defendants. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Bohrium 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 Bohrium 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.

9. Based on our investigation and analysis, Microsoft has determined that Bohrium specializes in targeting, penetration, and stealing sensitive information from high-value computer networks connected to the Internet. Bohrium targets Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. **Figure 1** below demonstrates that over half of Bohrium's targets are in the Information & Technology and Government Agencies & Services sectors:

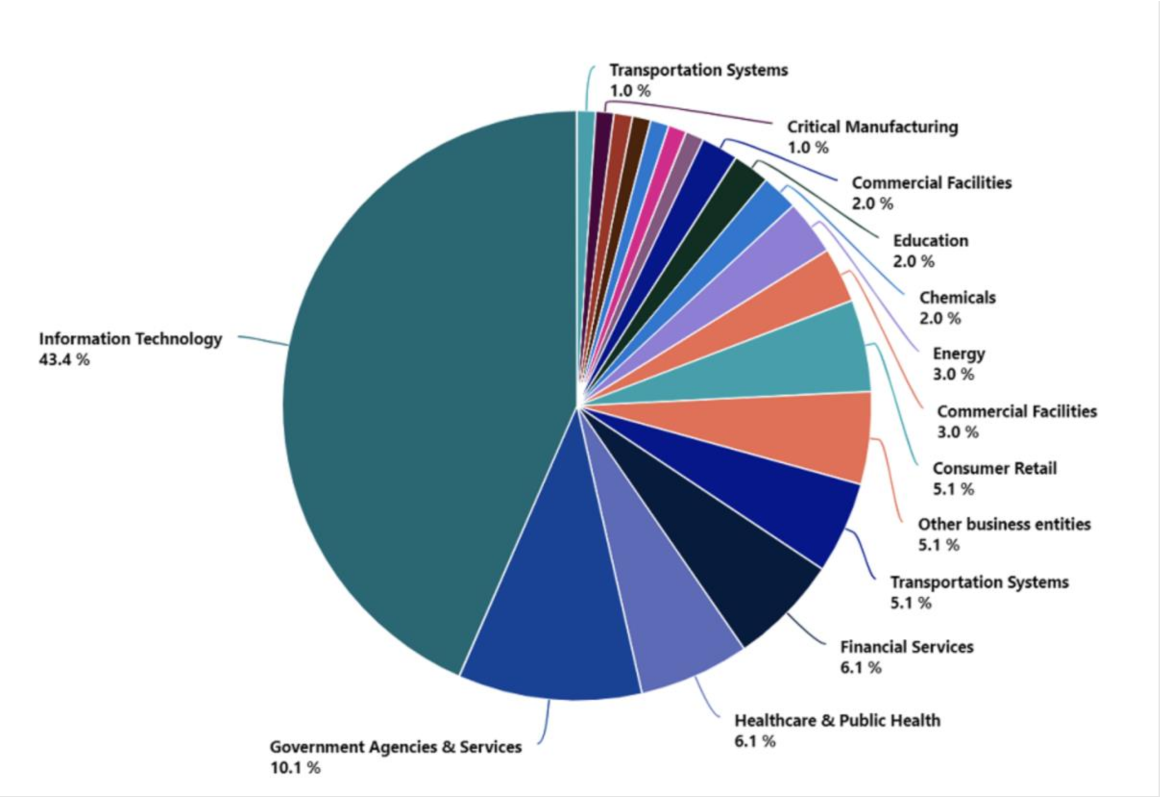


Figure 1 – Bohrium Targets by Sector

10. Bohrium's objectives appear to be obtaining credentials to accounts and sensitive communications from within the accounts. According to Microsoft's investigation, Bohrium remains active and poses a current threat today, and an ongoing threat into the future.

III. BOHRIUM'S METHOD OF COMPROMISING AND STEALING INFORMATION FROM VICTIMS

11. Bohrium leases virtual private services to browse, research, register, and administer domains and to handle the "command and control" infrastructure of their malware.

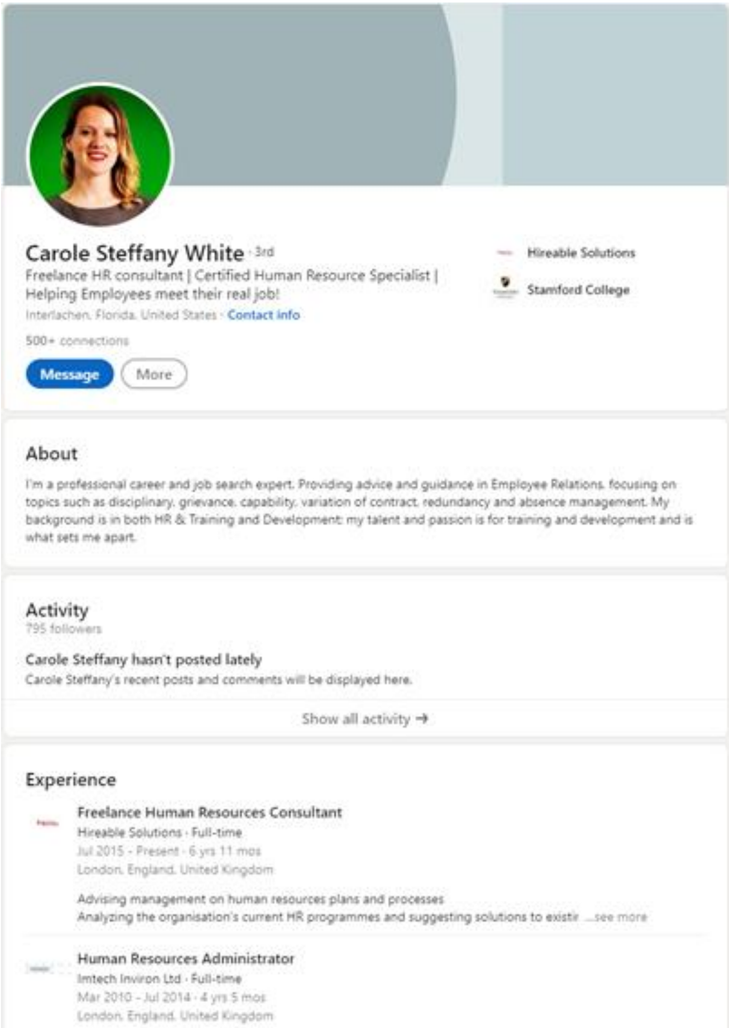
12. Upon information and belief, I understand that LinkedIn Corp. ("LinkedIn," a wholly-owned Microsoft subsidiary), a social media platform that is primarily used by its users for professional networking and career development, observed Bohrium using fictitious profiles (profiles with fictitious names and stock image profile photos) to engage with targeted individuals (legitimate users of the platform) for the purpose of collecting information the Bohrium operators can then use to engage in a tactic known as "spearphishing." Specifically, Bohrium creates fake profiles, where they purport to be a recruiting company with the goal of connecting with individuals in a specific industry, encouraging users to apply for a new employment opportunity, obtaining their personal information (such as an email address), using that email address to launch a spearphishing operation with the goal of having the targeted individual download Bohrium malware, and then infecting the user's computer with Bohrium malware.

13. As a preliminary step, Bohrium acquires the infrastructure that it needs to carry out the operation. The first step of the Bohrium operation involves acquiring infrastructure to use in connection with their operation, such as acquiring Virtual Private Servers ("VPSs") and registering domain names, so that Bohrium is able to host its content. My investigation has identified Bohrium registering recruitment-themed domains such as elecresearch[.]org or penspen[.]org to use in connection with the spearphishing operation. I have also tracked linkedinz[.]me and discovered that this domain was registered to Roshan Sijin, which is a fictitious persona that Bohrium also

used to create a fake LinkedIn profile.[1] Bohrium has also consistently used, as part of its infrastructure, two threat-actor specific custom domains masquerading as HR and talent agencies: (1) sh-url[.]link and (2) enerflex[.]org. I have also identified Microsoft-impersonation domains (domains impersonating a Microsoft product or service), such as microsoftdefender[.]info, sharepointfile[.]com, outlookdelivery[.]com, and microsoftsecure[.]org, which also constitutes the Bohrium infrastructure. These domains represent a subset of Bohrium-controlled domains; a full list of domains that I have identified as associated with the Bohrium malware is listed in **Exhibit 1** to my declaration.

14. After acquiring necessary infrastructure, Bohrium creates fictitious social media accounts to contact legitimate users who work at companies the Bohrium actors wish to target. I have observed these fake profiles claim to work on behalf of companies like Freelance HR Recruiters, ApplyTalents, or Mid East Hiring, which are United Kingdom-based recruiting companies that specialize in hiring for Middle East-based employers. **FIGURE 2** is an image of a profile for Carole Steffany White, an individual who purports to work with Freelance HR Recruiters and claims to "help employees meet their real job."

[1] This profile does not belong to a legitimate user; rather it is entirely made up. On information and belief, LinkedIn disabled this profile upon completion of the investigation.



Carole Steffany White · 3rd

Freelance HR consultant | Certified Human Resource Specialist | Helping Employees meet their real job!

Interlachen, Florida, United States · Contact info

500+ connections

Hireable Solutions

Stamford College

About

I'm a professional career and job search expert. Providing advice and guidance in Employee Relations, focusing on topics such as disciplinary, grievance, capability, variation of contract, redundancy and absence management. My background is in both HR & Training and Development: my talent and passion is for training and development and is what sets me apart.

Activity

795 followers

Carole Steffany hasn't posted lately

Carole Steffany's recent posts and comments will be displayed here.

Experience

Freelance Human Resources Consultant
Hireable Solutions · Full-time
Jul 2015 - Present · 6 yrs 11 mos
London, England, United Kingdom

Advising management on human resources plans and processes
Analyzing the organisation's current HR programmes and suggesting solutions to existir ...see more

Human Resources Administrator
Imtech Inviron Ltd · Full-time
Mar 2010 - Jul 2014 · 4 yrs 5 mos
London, England, United Kingdom

Figure 2 – Fictitious Profile Posing as a Recruiting Company

15. I have observed that the Bohrium operators utilize the fictitious recruitment-themed profiles to target individuals located in the Middle East who are employed in the maritime, shipping, and information technology sectors. Bohrium operators will interact with the targeted individuals under the guise of offering new employment and developing a professional rapport. The Bohrium operators will then request the target's email address (*i.e.*, under the guise of a promise to send recruiting materials), so that Bohrium actors can engage in future conversations with the targeted individuals off of the LinkedIn platform.

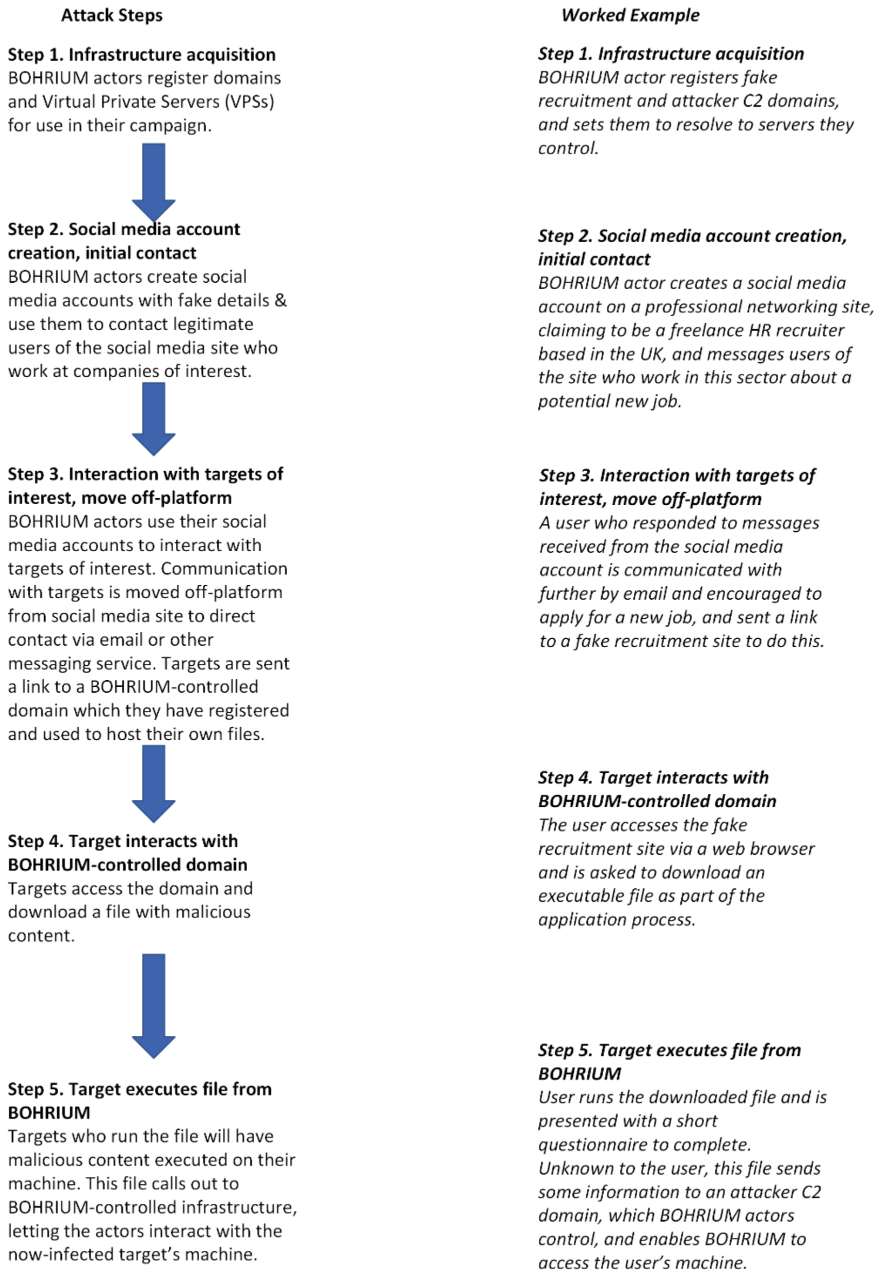
16. Using the target's email, Bohrium will continue to engage in off-platform communications by sending the target an email with a link to a Bohrium-controlled domain. For

example, individuals are sent a link to the Bohrium-controlled elecresearch[.]org so that the target can begin the job application process. Because the link's nefarious origins are concealed, the target believes the email is legitimate and unsuspectingly clicks on the link. In a typical spearphsihing attack, the malware is sent to the targeted individual via an email or link that is specifically crafted to appear as if it was sent from a reputable email provider (e.g., Gmail based email addresses have been associated with Bohrium) and is tailored to the targeted individual. As described, *infra* at ¶ 19, by gathering information about the targeted individuals from social media and other public sources, Bohrium is able to package the spearphishing email in a way that gives the email credibility to the target. For example, Bohrium will disseminate a poll on social media platforms asking users to identify the types of software the user is most likely to download. This poll is designed to collect actionable intelligence from these targets to determine which types of applications a target would most likely respond to. The threat actor would then be in a better position to design malware and phishing techniques of greater effectiveness. This makes it more likely that the target interacts with the Bohrium-controlled domain (the goal of the spearphish).

17. Once the target opens the email link and interacts with the Bohrium-controlled domain, the target unknowingly downloads a file with malicious content. For example, when a user accesses elecresearch[.]org, the user is asked to download a file as part of the application process. Once downloaded, this malicious file calls out to Bohrium-controlled infrastructure, alerting the Bohrium actors and allowing them to interact with the now-infected target machine. Here, when the user opens the downloaded file, the user is asked to complete a short questionnaire. The user thinks they are providing personal information in response to a job posting, but unknown to the user, the information is actually being sent back to the Bohrium-controlled attacker C2 domain. This allows and enables Bohrium to access and control the user's device and execute the malicious content on the victims' devices.

18. **Figure 3** is a flow chart that depicts the attack steps described herein that the Bohrium defendants complete in connection with their criminal enterprise to infect victims'

computers with the Bohrium malware. The left column of **Figure 3** describes the five-step attack. The right column of the same figure denominated "worked example" describes the same five-step attack plan but uses evidence that I have gathered in connection with my investigation.



Attack Steps

Step 1. Infrastructure acquisition
BOHRIUM actors register domains and Virtual Private Servers (VPSs) for use in their campaign.

Step 2. Social media account creation, initial contact
BOHRIUM actors create social media accounts with fake details & use them to contact legitimate users of the social media site who work at companies of interest.

Step 3. Interaction with targets of interest, move off-platform
BOHRIUM actors use their social media accounts to interact with targets of interest. Communication with targets is moved off-platform from social media site to direct contact via email or other messaging service. Targets are sent a link to a BOHRIUM-controlled domain which they have registered and used to host their own files.

Step 4. Target interacts with BOHRIUM-controlled domain
Targets access the domain and download a file with malicious content.

Step 5. Target executes file from BOHRIUM
Targets who run the file will have malicious content executed on their machine. This file calls out to BOHRIUM-controlled infrastructure, letting the actors interact with the now-infected target's machine.

Worked Example

Step 1. Infrastructure acquisition
BOHRIUM actor registers fake recruitment and attacker C2 domains, and sets them to resolve to servers they control.

Step 2. Social media account creation, initial contact
BOHRIUM actor creates a social media account on a professional networking site, claiming to be a freelance HR recruiter based in the UK, and messages users of the site who work in this sector about a potential new job.

Step 3. Interaction with targets of interest, move off-platform
A user who responded to messages received from the social media account is communicated with further by email and encouraged to apply for a new job, and sent a link to a fake recruitment site to do this.

Step 4. Target interacts with BOHRIUM-controlled domain
The user accesses the fake recruitment site via a web browser and is asked to download an executable file as part of the application process.

Step 5. Target executes file from BOHRIUM
User runs the downloaded file and is presented with a short questionnaire to complete. Unknown to the user, this file sends some information to an attacker C2 domain, which BOHRIUM actors control, and enables BOHRIUM to access the user's machine.

Figure 3 – Attack Steps and Worked Example of Bohrium Operation

19. Bohrium has engaged in several tactics in creating the spearphishing email to maximize its efficacy in tricking the target. In several instances, Bohrium has utilized brand impersonation domains, in which Bohrium has registered domains which impersonate legitimate companies. In these instances, Bohrium has been observed using these domains to spearphish targets by pretending to be from the impersonated company and tricking the target into believing they are receiving legitimate communications from the impersonated company. Some examples of this include sharepointfile[.]com, outlookdelivery[.]com, microsoftdefender[.]info, and microsoftsecure[.]org (impersonating Microsoft). Bohrium also registers domains that are themed around providing technical/online services, likely in an attempt to disguise any observed network traffic to these domains as legitimate. In some instances, these domains have impersonated specific companies like Microsoft; but in other cases, the domains are more generally themed around the provisions of cloud services, online services, or technical updates. These technical domains have been used for the command and control of the Bohrium malware implant. Finally, Bohrium has been observed as registering domains themed around generic recruitment and/or interviewing themes. Given that the targets are first identified and lured via fake recruiting, the recruitment-themed emails have been observed to gain traction with this category of targets. As with the other Bohrium domains, the recruitment/interviewing themed domains are also used as part of a spearphishing campaign against targets of interest.

20. The domains also have the benefit of being inconspicuous so as not to attract attention from network administrators when they are reviewing network traffic logs. All of these types of domains may be referred to as "command and control domains," and the associated computer infrastructure may be referred to as "command and control infrastructure."

21. Through research and investigation, Microsoft has determined that Bohrium currently uses the domains identified in Appendix A of the complaint, also attached as **Exhibit 1** to this declaration, in its command and control infrastructure. As part of my investigation, I performed lookups of these domains in a publicly accessible "Whois" database, which contains

contact information regarding the registrants of these domains and technical details about the domains. Information in **Exhibit 1** is generated from the publicly available Whois registration data.

22. The spearphishing emails often include links to websites that Bohrium has set up in advance and that it controls. When a victim clicks on the link in the email, their computer connects to the Bohrium-controlled website. However, the victim is presented with a copy of a legitimate login page for the webmail provider for which the victim is a subscriber so that the victim is not alerted to the spearphish. By clicking on the links contained within these spearfishing emails, the targeted user will be connected to a Bohrium-controlled website which will attempt to induce the victim to enter their account credentials. Bohrium spearphishes targets with emails that contain a link to an actor-controlled site intended to coerce the victim into inputting credentials or download malicious software ("malware") onto the victim machine.

23. Once the malware, an implant tracked by Microsoft under the name "C5", is on the victim machine, it collects clipboard data, keystrokes, and screenshots of the active window on the desktop, and then compresses and encrypts this data before writing it to a temporary file and exfiltrating these back to Bohrium's command and control infrastructure. This data is then exfiltrated to the command and control server, generally via HTTPS, although C5 can also support ICMP and HTTP protocols. In addition to the C5 implant, Bohrium has also been observed using a custom .NET password stealer on victim machines, and then attempting to move laterally within victim networks using supplied credentials. The presence of these two malware implants can be identified by the following signatures:

- Hacktool:Win32/C5Client.A!dha
- Hacktool:Win32/PasswordImporter.A!dha

24. Whilst Bohrium has been observed researching a small number of public exploits, including downloading proof-of-concept code from GitHub for the widely-used Proxylogon exploit, they have not been observed using any zero-day exploits.

25. I have determined that the bulk of Bohrium activities can be classified according to the following ATTACK framework techniques:

Tactic	ID	Technique	Description
Establish Accounts	T1585	T1585.001 Social Media Accounts T1858.002 Email Accounts	Bohrium establishes fictitious social media and email accounts
Acquire Infrastructure	T1583	T1583.001 Domains T1583.003 Virtual Private Servers T1583.006 WebServices	Bohrium acquires domains, VPS, and web services to establish the malware infrastructure
Phishing	T1566	T1566.002 Spearphishing Link T1566.003 Spearphishing via Service	Bohrium engages in phishing by utilizing spearphishing links. Bohrium also engages in spearphishing through services
User Execution	T1204	T1204.001 Malicious Link T1204.002 Malicious File	Sending of malicious files and malicious links
Scheduled Task/Job	T1053	T1053.005 Scheduled Task	Scheduled Task
Input Capture	T1056	T1056.001 Keylogging	Keylogging
Obtain Credentials	T1555	T1555.003 Credentials from Web Browsers	Obtain Credentials from password stored and web browsers
Valid Accounts	T1078	T1078.003 Local Accounts T1078.004 Cloud Accounts	T1078.003 Local Accounts T1078.004 Cloud Accounts

26. I have concluded that Bohrium uses leased Virtual Private Servers ("VPS") for part of their infrastructure. These are generally used for browsing/research, registration, administration of domains, and handling command and control infrastructure for their malware. In my experience, there are multiple benefits of using a VPS such as increased website reliability, improved website performance, allowing users to allocate resources as they wish, installing only the operating system and software that a user specifically intends to use, and allowing the user to configure and maintain the virtual server at the user's own discretion. Between September and December 2021, one email account used by Bohrium was observed attempting to lease

infrastructure from at least five VPS providers. The leased infrastructure can be actively used by Bohrium for months at a time.

27. Once the Bohrium malware exfiltrates data back to Bohrium's command and control infrastructure, Bohrium is able to use this data to gain access to the victims' Microsoft Office 365 accounts using the stolen credentials. Once Bohrium has access to these Microsoft Office accounts, Bohrium uses this access to steal information from these accounts. To protect Office 365 users, Microsoft regularly issues Nation State Notifications ("NSNs") to inform victims of this unlawful access activity. Through our tracking of Bohrium, Microsoft has observed that in some instances, Bohrium has repeatedly targeted or attempted to target the same organization or individual over a period of months or even longer.

28. Bohrium relies on and uses a range of Microsoft services to support their malicious activities, including the creation and use of email accounts for spearphishing targets and signing up for other services, such as VPS registration. I have observed that Bohrium often uses Azure-based services for hosting its malicious content. In doing so, Bohrium relies on the Microsoft brand and trademark to perpetrate its spearphishing and malware attacks. Bohrium's use of Microsoft services, its brand, and trademarks deceives and confuses victims into thinking that the spearphishing is email is *not compromised* because the domain is Microsoft's and incorporates Microsoft's trademarks and branded material. For example, researchers or other parties who are looking for malicious activities or accidentally browse to this domain may not understand that there is any malicious activity associated with it because it displays what appears to be legitimate Microsoft content. Similarly, when the domain is being used for malicious purposes to target victims, the victim will be completely unaware of this fact because they are tricked into believing that the link is a legitimate Microsoft website and that the site is trustworthy, when in fact it is malicious and actively delivering malware.

29. Bohrium's use of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links or otherwise interacting with webpages that they believe

are associated with and owned by Microsoft. As noted above, by tricking victims into clicking on the fraudulent links and providing their credentials, the Bohrium defendants are then able to log into the victim's account. Additionally, the Bohrium defendants can read sensitive and personal emails within the account, create new inbox rules including auto-forwarding, access the victim's contact list, send additional spearphishing emails to the victim's contacts, and hide traces of this malicious activity in the victim account by deleting emails. 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 these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands. By specifically targeting Microsoft's Windows operating system and utilizing registry and file paths containing Microsoft's trademarks, in order to deceive users and carry out the fraudulent scheme, the Bohrium defendants infringe Microsoft's trademarks and deceptively use those trademarks in the context of Microsoft's Windows operating system.

IV. BOHRIUM HAS ATTACKED MANY MICROSOFT CUSTOMERS IN THE UNITED STATES AND AROUND THE WORLD

30. Through its investigation, Microsoft has determined that Bohrium has affirmatively targeted Microsoft customers in the United States. Additionally, Bohrium has been most active in targeting individuals who resided in the United Arab Emirates. As can be seen below in **Figure 4**, two-thirds of Bohrium activity are directed towards the United Arab Emirates. India also is a prominent target, accounting for approximately twenty percent of Bohrium malware activity.

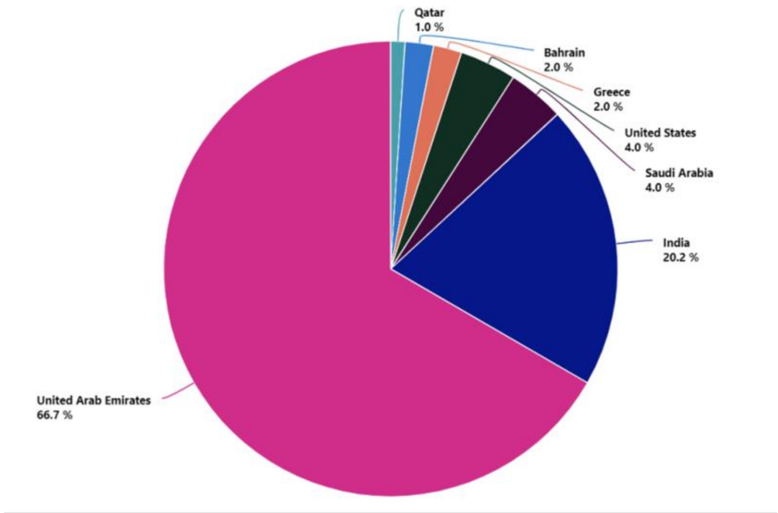


Figure 4 - Breakdown of Bohrium Targets by Country

V. BOHRIUM CAUSES IRREPARABLE HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

31. Microsoft® is a provider of the Windows® operating system, the Hotmail®, Outlook®, and MSN® email and messaging services and the Office 365® and Azure® cloud-based business and productivity suite of services, as well as a variety of other hardware products, software, and services, including under the Surface®, Xbox®, and HoloLens® brands and trademarks. 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®, Windows®, Hotmail®, Outlook®, Office 365®, MSN®, Azure®, Surface®, Xbox®, and HoloLens® marks.

32. The activities carried out by the Bohrium defendants, described above, injure

Microsoft and its reputation, brand, and goodwill because users of compromised computers and accounts are likely to incorrectly believe that Microsoft is the source of problems caused by the Bohrium defendants. Microsoft is similarly injured because the Bohrium defendants direct their intrusions to Microsoft customer accounts hosted on Microsoft's servers and to Microsoft's Windows operating system running on customers' computers. Microsoft and its customers must bear this extraordinary burden. Microsoft must respond to customer service issues caused by the Bohrium defendants and must expend substantial resources dealing with the injury and confusion. Microsoft has had to expend substantial resources in an attempt to assist its customers and to prevent the misperception that Microsoft is the source of damage caused by the Bohrium defendants. For example, Microsoft must expend resources to block the malware discussed above, and block attempts by Bohrium to compromise user accounts.

33. Once customers' accounts are compromised by Bohrium or their computers are infected, they may be unaware of that fact and may not have the technical resources to solve the problem, allowing their computers to be misused indefinitely.

34. In such circumstances, technical attempts to remedy the problem may be insufficient and the injury caused to customers will continue. The injury caused by the Bohrium defendants extends far beyond Microsoft to other consumers and providers of email services and internet infrastructure and to all computer users, each of whom is at risk.

35. Based on my experience assessing computer threats and the impact on business, I conclude that customers may incorrectly attribute the negative impact of the Bohrium defendants to Microsoft. Further, based on my experience, I therefore conclude that there is a serious risk that customers may move from Microsoft's products and services because of the Bohrium defendants and their activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

36. Microsoft and its customers are injured when the malware used by the Bohrium defendants is maliciously introduced onto users' computers. The installation of the malware by

deceiving consumers and without Microsoft's authorization is an intrusion into the Microsoft Windows operating system, without Microsoft's authorization.

37. Among other things, the Bohrium defendants install and run software without the customers' or Microsoft's knowledge or consent, to support the Bohrium infrastructure and to steam information. The Bohrium defendants specifically target the Windows operating system. For example, as discussed, they write particular entries to the registry of the Windows operating system, without the consent of Microsoft or its customers, and manipulate and store data in Windows registry and file paths that contain Microsoft's trademarks. The Bohrium defendants collect and transmit personal information, including the contents of communications and files, and other personal and sensitive information from users' accounts and computers. Microsoft's customers may be incorrectly led to believe that Microsoft is the source of such issues. This causes injury to Microsoft.

VI. TRANSFERRING CONTROL OF THE HARMFUL BOHRIUM DOMAINS WITHOUT FIRST INFORMING THE DEFENDANTS IS THE ONLY WAY TO PREVENT THE INJURY

38. Bohrium's illegal activities will not be easy to disrupt. Evidence indicates that Bohrium is sophisticated, well-resourced, organized, patient, and persistent. Bohrium specializes in targeting organizations producing and storing sensitive data by gathering extensive information about their employees through publicly available information, posing a fictitious recruiting company promising to recruit for employment the targeted individuals, and then using that information to fashion phishing attacks intended to trick those employees into compromising their credentials. Bohrium disguises its activities by using the names and trademarks of Microsoft and other legitimate and trusted companies.

39. A vulnerable point in Bohrium's operations are the Internet domains through which Bohrium obtains victim credentials, logs into compromised accounts, reviews sensitive information from victim accounts and controls malware on victim computers that targets Microsoft's Windows operating system. A core active subset of these is listed in **Exhibit 1** to this

declaration. These Bohrium registered domains incorporate brands and trademarks that are owned by Microsoft. In order to protect Microsoft's customers, which are being targeted by malware distributed or potentially distributed through such domains, these domains must be seized, and their possession transferred to Microsoft.

40. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby significantly cut off the means by which the Bohrium defendants collect victim credentials or control malware on victim computers. In other words, any time a user clicks on a link in a spearphishing email and provides their username and password, instead of this information going to the Bohrium defendants, the information will be sent to a Microsoft-controlled, secure server. The same holds true for any victim machines that have been infected with malware used by Bohrium. Granting Microsoft possession of these domains will allow Microsoft to significantly cut off communications between infected computers and the servers currently controlled by Bohrium. Hence, the victim machines will no longer be communicating with the Bohrium defendants' command and control servers, and Microsoft can work with the appropriate authorities to assist with victim notifications. While it is not possible to rule out the possibility that the Bohrium defendants could use fallback mechanisms to evade the requested relief, redirecting this core, active subset of Bohrium domains will directly disrupt current Bohrium infrastructure, mitigating risk and injury to Microsoft and its customers.

41. The requested relief will also enable Microsoft to assist its customers who have had their credentials compromised by the Bohrium defendants. Microsoft will be able to identify domains and IP addresses associated with customers whose credentials have been compromised going forward. Microsoft, working in collaboration with the relevant webmail service providers that provide services to the owners of the compromised accounts, can notify them that their credentials have been compromised and assist them in setting up two-factor or multi-factor authentication and other security measures in attempts to prevent the credentials from being compromised again in the future.

42. 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 Bohrium's ability to compromise additional accounts, to identify new potential victims to target and to infect victim machines with malware. In the absence of such action, the Bohrium defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to Bohrium.

43. Bohrium's techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in Bohrium's active infrastructure become known to the security community, Bohrium abandons or decreases use of that infrastructure and moves to new infrastructure that is used to continue the Bohrium defendants' efforts to compromise accounts of new victims. For this reason, providing notice to the Bohrium defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Bohrium 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, providing notice to the Bohrium 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 threat actors such as Bohrium, I believe the Bohrium 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.

44. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by threat 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 all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Bohrium infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

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 26 day of May, 2022, in Alexandria, Virginia.

Christopher Coy