IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, 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 5.1**

DECLARATION OF SEAN ENSZ IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Sean Ensz, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration in support of Microsoft's Application for an Emergency *Ex Parte* 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.

2. I have been employed by Microsoft since July 2018. In my role at Microsoft, I work as a Digital Crimes Unit Principal Investigator, and I investigate significant transnational cybercrime and nation state incidents and develop threat intelligence to disrupt malicious cyber operations. Prior to joining Microsoft in 2018, I served as the Information Assurance Manager at Devon Energy and spent ten years in information technology at the University of Oklahoma conducting and managing forensic investigations and incident response teams. A true and correct

copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

3. My declaration concerns the investigation into a Russia-based cybercriminal organization comprised of unknown individuals collectively known as “Star Blizzard” that is systematically and persistently engaging in cyberattacks that include developing infrastructure and capabilities to conduct spear phishing attacks to facilitate cybercrime, as detailed below. I discuss Star Blizzard’s victim targeting methodology, techniques, tools used to execute their techniques, and harm to Microsoft, its customers, and the public.

I. CYBERCRIME AT ISSUE: SPEAR PHISHING CAMPAIGNS

4. I, along with other Microsoft investigators, investigate cybercrime campaigns like spear phishing, that are perpetrated by threat actors that target Microsoft and its customers. In this function, Microsoft identified and investigated Star Blizzard’s spear phishing campaign.

5. As a Principal Investigator experienced in investigating cybercrimes, I have observed threat actors often use a social engineering tactic called phishing. Phishing attacks use deceptive emails tailored to use deceptive language to elicit fear or urgency by the recipient, to trick them into interacting with the email, such as clicking on a link or opening a file. The intent of phishing typically includes installing malware, stealing someone’s account credentials, or to reveal personal information (such as credit card numbers, bank information, or passwords). These emails often include links to websites that appear legitimate but are in fact, controlled by threat actors as part of their operation to steal information. Files attached in phishing emails may be infected with malicious computer software (“malware”) or include hyperlinks to threat actor-controlled websites. Threat actors use this tactic on a grand scale called campaigns, which are repeated, persistent attempts to target multiple victims to achieve their objective.

6. A spear phishing campaign is a type of attack where phishing emails are tailored to

a specific group, organization, or person, to increase the likelihood of stealing their target's credentials and data by convincing them of the email's legitimacy. This often includes: (i) using local language for the subject, body, and sender's name to make it harder for users to identify email as a spear phishing attempt; (ii) email topics that correspond to the recipient's responsibilities in the organization, e.g., sending academic or policy papers; or (iii) using compromised or impersonated email accounts to send spear phishing emails that appear legitimate and from a known sender.

7. Threat actors, particularly foreign criminal organizations or groups associated with foreign governments, use spear phishing to engage in information gathering, online influence, and espionage.

II. **STAR BLIZZARD DEFENDANTS**

Foreign Cybercriminals

8. My declaration concerns the investigation into the persistent spear phishing campaigns by the Star Blizzard Defendants – hostile cybercriminals believed to be operating from Russia. The identities of the cybercriminals behind the activities addressed in this declaration are uncertain and are collectively identified by the threat actor name that Microsoft has assigned to this group: "Star Blizzard." The Star Blizzard Defendants are formerly known as SEABORGIUM and also known in the cybersecurity community as the Callisto Group, COLDRIVER, and BlueCharlie.

Motivation and Targeted Victims

9. The Star Blizzard Defendants' primary objectives are information gathering, cyber influence, and cybercrime.

10. Since the beginning of 2022, Microsoft has observed the Star Blizzard Defendants' campaigns target over 30 organizations, in addition to personal accounts of people of interest. The Star Blizzard Defendants primarily target NATO countries, particularly the United States and the United Kingdom, and other countries in the Baltics, the Nordics, and Eastern Europe. Such targeting has included the government sector of Ukraine in the months leading up to the invasion by Russia, and organizations involved in supporting roles for the war in Ukraine. Despite some targeting of these organizations, Microsoft assesses that Ukraine is likely not a primary focus for this actor (as the Star Blizzard Defendants have also targets organization and individuals that work to oppose the Russian government and are adverse to Russia's interests or global and domestic policy beyond its invasion of Ukraine); however, it is most likely a reactive focus area for the actor and one of many diverse targets.

11. Within the target countries like the U.S., the Star Blizzard Defendants primarily focuses cyber operations on individuals working in defense and intelligence consulting companies, non-governmental organizations (NGOs) and intergovernmental organizations (IGOs), governmental policy think tanks, and higher education. The Star Blizzard Defendants have a high interest in targeting personal email accounts as well, with 30% of Microsoft's victim notifications related to the Star Blizzard Defendants' activities being delivered to Microsoft consumer email accounts. The Star Blizzard Defendants have also been observed targeting former intelligence officials, experts in Russian affairs, and Russian citizens abroad in the U.S.

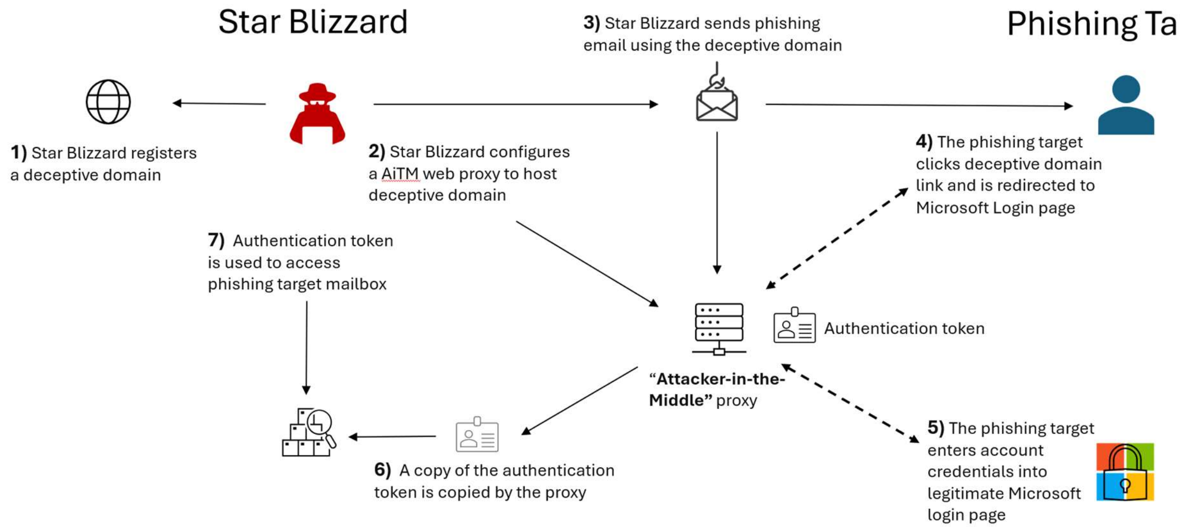
12. Since 2023, Microsoft has observed the Star Blizzard Defendants' campaigns continue to target NGOs, think tanks, government employees, and personal accounts belonging to current and former military and intelligence officials and policy advisors. The individuals targeted by these attacks predominately reside in the U.S., in and around the Washington, DC area.

13. The identified spear phishing campaigns are methodically crafted using email addresses that appear legitimate by representing a person known to the target using subject lines and imbedded or attached documents to lure the recipient into opening. In some cases, previously compromised accounts, known to the spear phishing target, are directly used by the Defendants to increase the likelihood of success.

14. Microsoft has identified 82 customers that have been targeted by the Star Blizzard Defendants since January 2023, at a rate of about once per week. This rate indicates the level of care used by Star Blizzard to identify targets, craft custom spear phishing emails, and develop the infrastructure needed to facilitate credential theft, and cull the target's mailbox sensitive documents and known contacts to develop additional targets if the target is compromised.

III. INVESTIGATING THE ATTACK CHAIN

15. Microsoft's investigation has established the Defendants have developed the following steps to successfully spear phish targets, Defendants: i) registers deceptive domains, ii) configures a AiTM web proxy to host deceptive domain, iii) sends phishing email using the deceptive domain deliver malicious content through a link to Microsoft's personal cloud storage platform, OneDrive, or by adding a malicious URL in the body of an email or PDF file attachment, iv) steals their credentials, and v) culls mailboxes to exfiltrate sensitive data and contacts. The Star Blizzard Defendants have successfully compromised organizations and people of interest in persistent spear phishing campaigns, infrequently changing their procedures and tactics. **Figure 1** is a visual representation of the Star Blizzard attack chain.


Star Blizzard
3) Star Blizzard sends phishing email using the deceptive domain
Phishing Target
1) Star Blizzard registers a deceptive domain
2) Star Blizzard configures a AiTM web proxy to host deceptive domain
4) The phishing target clicks deceptive domain link and is redirected to Microsoft Login page
7) Authentication token is used to access phishing target mailbox
Authentication token
"Attacker-in-the-Middle" proxy
5) The phishing target enters account credentials into legitimate Microsoft login page
6) A copy of the authentication token is copied by the proxy

"Attacker-in-the-Middle" is a network proxy allows an attacker to eavesdrop when a user enters their account password on a legitimate website, such as Microsoft's authentication website, to steal the account credential.

Figure 1

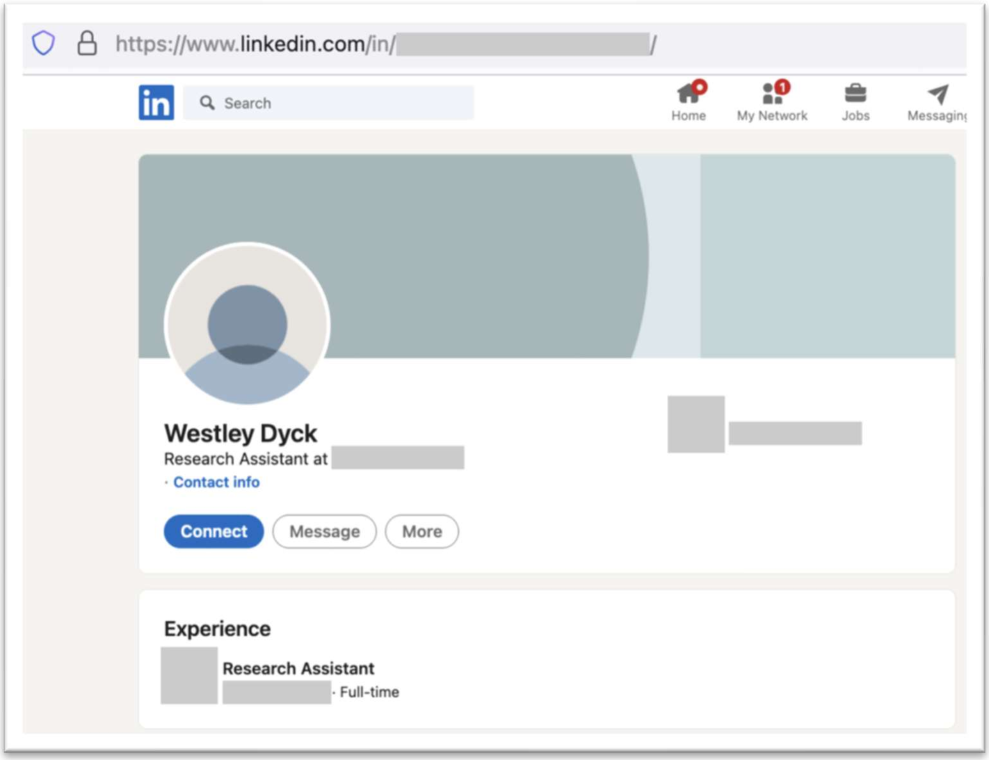
<u>Attack Step 1: Impersonation and Establishing Contact</u>

16. Before starting a campaign, the Star Blizzard Defendants often conducts reconnaissance of target individuals, with a focus on identifying legitimate contacts in the target's social network or sphere of influence.

17. Based on some of the impersonation and targeting observed, we suspect that the Star Blizzard Defendants use social media platforms, personal directories, and general open-source intelligence (OSINT) to supplement their reconnaissance efforts. The Star Blizzard Defendants often use their target's social networks through contact impersonation, rapport building, and additional spear phishing to deepen their intrusion.

18. In coordination with Microsoft's Microsoft Threat Intelligence Center (MSTIC), and partnership with LinkedIn, Microsoft observed fraudulent profiles attributed to the Star Blizzard Defendants being used sporadically for conducting reconnaissance of employees from

specific organizations of interest. **Figure 2** below is an example profile used by the Star Blizzard Defendants to conduct industry-specific reconnaissance. In accordance with their policies, LinkedIn terminated any account (including the one shown below) identified as conducting inauthentic or fraudulent behavior.



https://www.linkedin.com/in/[redacted]/

Westley Dyck

Research Assistant at [redacted]

· Contact info

[redacted] [redacted]

Experience

[redacted] Research Assistant

[redacted] · Full-time

Figure 2[1]

19. Defendants also register new email accounts at various consumer email providers, with the email address or alias configured to match legitimate aliases or names of impersonated

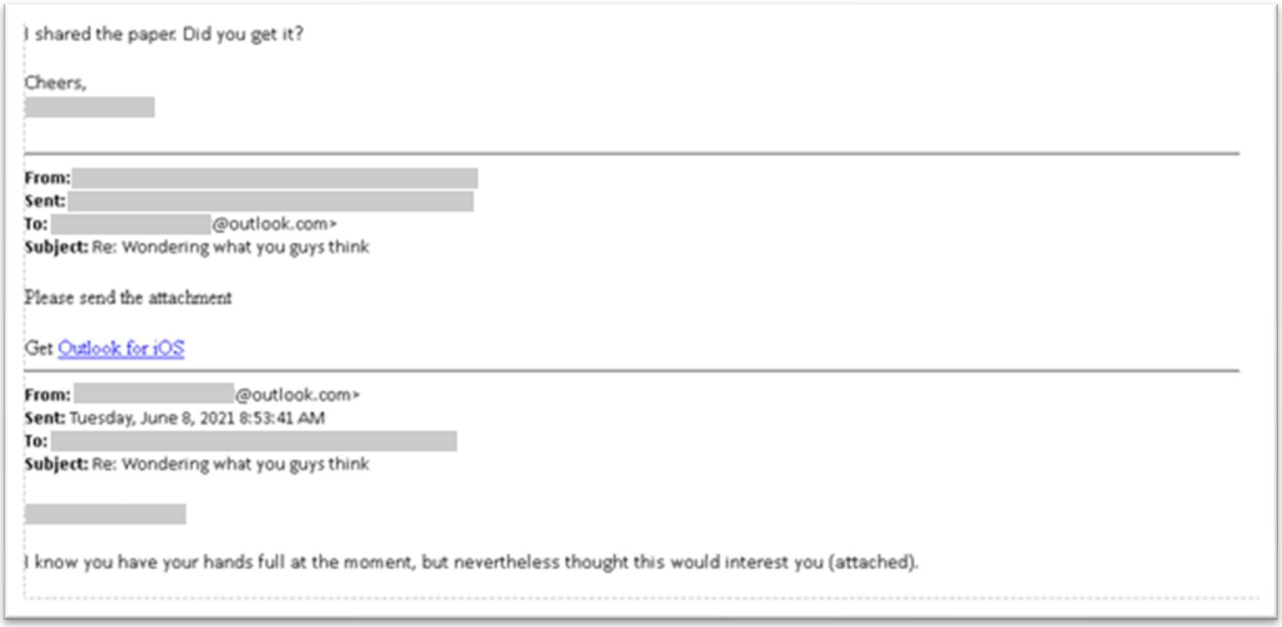
[1] Identifying information contained within this figure and others figures included in this declaration have been redacted for privacy of the targets and victims of the Star Blizzard Defendants.

individuals. For example, attached to this declaration is **Exhibit 2**[2] which are true and correct copies of threat research reports by the Cybersecurity and Infrastructure Security Agency (CISA) discussing the Star Blizzard Defendants' various tactics and techniques. It outlines several tactics, including the registration of consumer email accounts matching the names of individuals they are impersonating to conduct spear-phishing activity.

20. While the creation of new consumer accounts is common, we have also observed Defendants returning to and reusing historical accounts that match the industry of the ultimate target. In one case, we observed the Star Blizzard Defendants returning to an account it had not used in a year, indicating potential tracking and reusing of accounts if relevant to targets' industry.

21. After registering new accounts, the Star Blizzard Defendants proceed to establish contact with their target. In cases of personal or consumer targeting, Microsoft has mostly observed the actor starting the conversation with a benign email message, typically exchanging pleasantries before referencing a non-existent attachment while highlighting a topic of interest to the target. It is likely that this additional step helps the actor establish rapport and avoid suspicion, resulting in further interaction. If the target replies, the Star Blizzard Defendants proceed to send a weaponized email. **Figure 3** below is an example email showing the multi-email approach and rapport building frequently used by Defendants.

[2] Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a.



I shared the paper. Did you get it?

Cheers,
[redacted]

From: [redacted]
Sent: [redacted]
To: [redacted]@outlook.com>
Subject: Re: Wondering what you guys think

Please send the attachment

Get Outlook for iOS

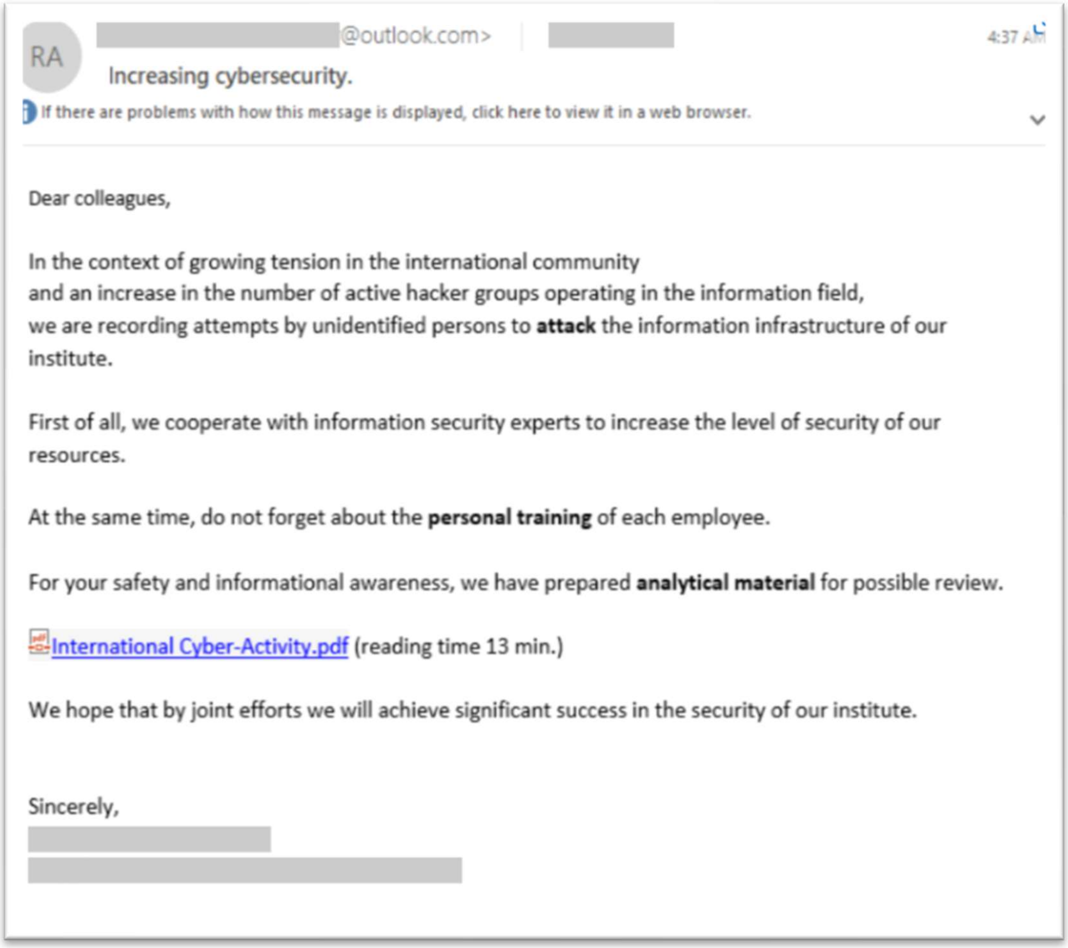
From: [redacted]@outlook.com>
Sent: Tuesday, June 8, 2021 8:53:41 AM
To: [redacted]
Subject: Re: Wondering what you guys think

[redacted]

I know you have your hands full at the moment, but nevertheless thought this would interest you (attached).

Figure 3

22. Microsoft has documented several cases where the Star Blizzard Defendants focus on a more organizational approach to spear phishing. In these cases, they use an authoritative approach in their social engineering (psychological manipulation to trick users into making security mistakes or giving away sensitive information) and typically goes to directly sending malicious content. **Figure 4** is an example of a spear phishing email where a Star Blizzard Defendant impersonates the lead of an organization and emails select members of the organization with a cybersecurity themed lure.



[redacted]@outlook.com> [redacted] 4:37 AM

Increasing cybersecurity.

If there are problems with how this message is displayed, click here to view it in a web browser.

Dear colleagues,

In the context of growing tension in the international community
and an increase in the number of active hacker groups operating in the information field,
we are recording attempts by unidentified persons to **attack** the information infrastructure of our institute.

First of all, we cooperate with information security experts to increase the level of security of our resources.

At the same time, do not forget about the **personal training** of each employee.

For your safety and informational awareness, we have prepared **analytical material** for possible review.

International Cyber-Activity.pdf (reading time 13 min.)

We hope that by joint efforts we will achieve significant success in the security of our institute.

Sincerely,
[redacted]

Figure 4

23. These examples serve to demonstrate the actors' capability to be dynamic and to adapt their social engineering approach to gain the trust of their victims.

<u>Attack Step 2: Deliver Malicious Content</u>

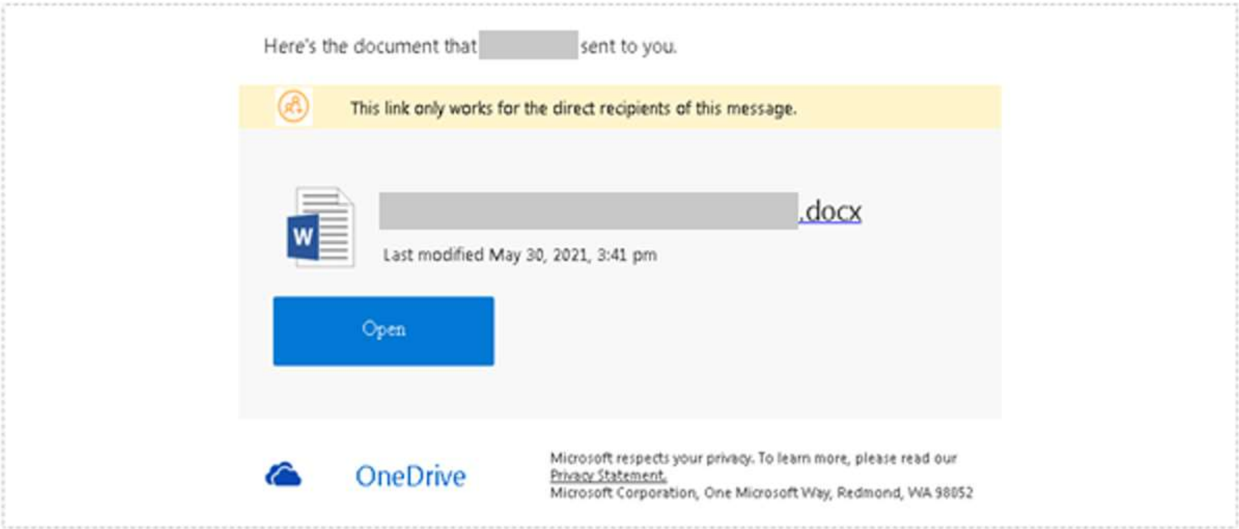
24. Microsoft investigation into the Star Blizzard Defendants' activities identified several variations in the way that the Star Blizzard Defendants delivers a link that directs targets to their credential stealing infrastructure.

Delivery Method #1 - Malicious Uniform Resource Locator (URL) in an Email

25. In the simplest case, the Star Blizzard Defendants directly add a URL to the body of their phishing email. A URL (Uniform Resource Locator) is a unique identifier used to locate a resource on the Internet. It is also referred to as a web address.

26. Occasionally, Defendants use URL shorteners which shortens the link to sometimes hide the website domain and make it look random. The Star Blizzard Defendants also use open redirects to obfuscate their web address from the security tools. Open redirect is a cyber exploit that occurs when a website redirects a user to a different, often malicious URL. This redirection is typically achieved through a crafted hyperlink supplied by Defendants, exploiting the trust users have in the genuine website.

27. The email varies between fake personal correspondence with a hyperlinked text and fake file sharing emails that imitate a range of platforms. **Figure 5** is an example of a follow-up email impersonating a OneDrive share. The link embedded takes the user to Defendant controlled infrastructure.



Here's the document that [redacted] sent to you.

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

[redacted].docx

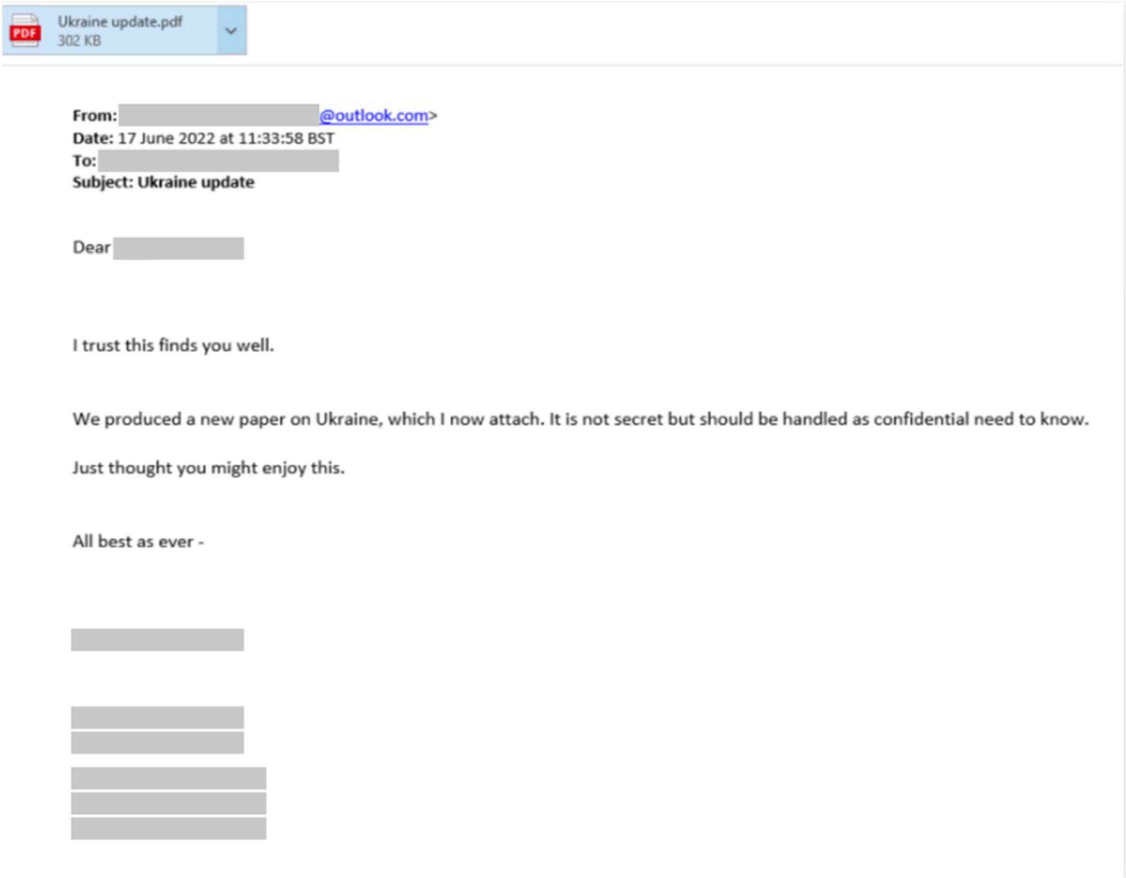
Last modified May 30, 2021, 3:41 pm

Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Figure 5

Delivery Method #2 - PDF File Attachment Contains Malicious URL

28. Microsoft has observed an increase in the use of attachments in the Star Blizzard Defendants' spear phishing campaigns. These attachments typically imitate a file or document hosting service, including OneDrive, and request the user to open the document by clicking a button. **Figure 6** and **Figure 7** are examples of a spear phishing email using the war in Ukraine as a ruse with the Star Blizzard Defendants directly attaching a PDF file to the email. Once a recipient downloads and attempts to open the attached, PDF file, the file appears to be a failed preview, redirecting the users to click a link which takes the user to Star Blizzard-controlled infrastructure.



Ukraine update.pdf
302 KB

From: [redacted]@outlook.com>
Date: 17 June 2022 at 11:33:58 BST
To: [redacted]
Subject: Ukraine update

Dear [redacted]

I trust this finds you well.

We produced a new paper on Ukraine, which I now attach. It is not secret but should be handled as confidential need to know.

Just thought you might enjoy this.

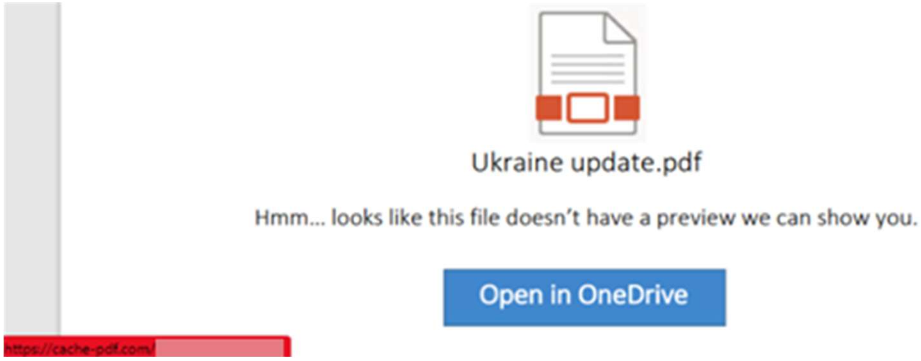
All best as ever -

[redacted]

[redacted]

[redacted]

Figure 6



Ukraine update.pdf

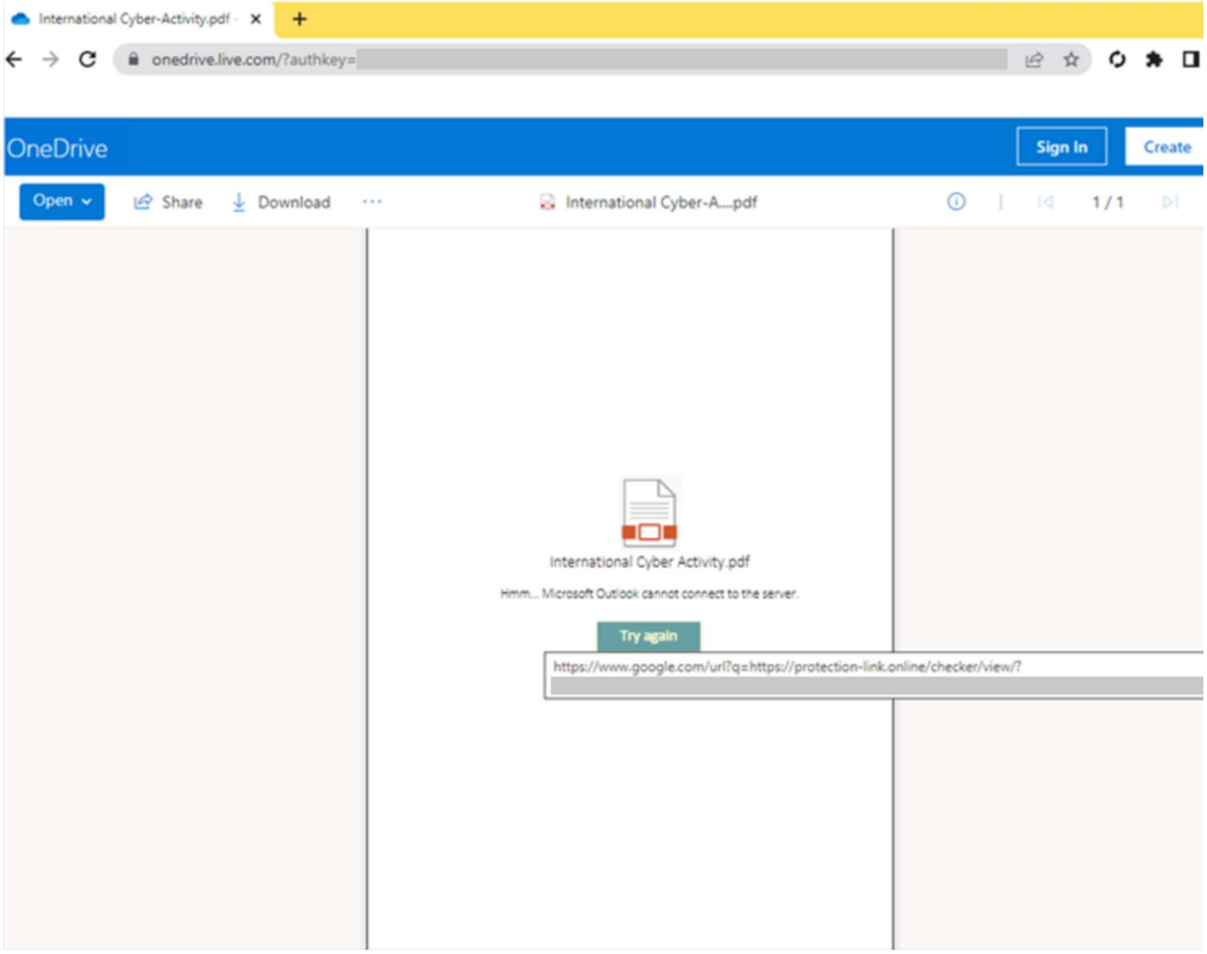
Hmm... looks like this file doesn't have a preview we can show you.

https://cache-pdf.com/[redacted]

Figure 7

Delivery Method #3 - OneDrive Link to PDF File Containing a Malicious URL

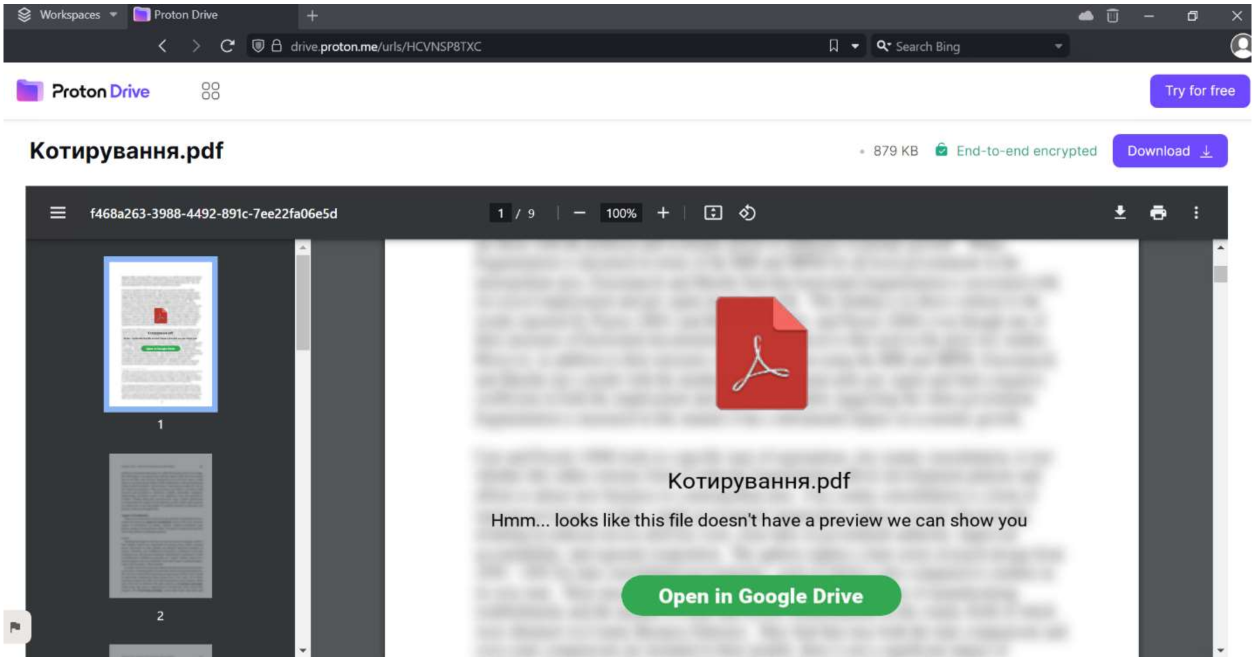
29. The Star Blizzard Defendants abuse OneDrive or other file sharing platform to host PDF files that contain a link to the malicious URL. This activity does not represent any security issues or vulnerabilities on the OneDrive platform. The Star Blizzard Defendants include a OneDrive link in the body of the email that when clicked directs the user to a PDF file hosted within a Star Blizzard-controlled OneDrive account. As seen in the previous example, the victim is presented with what appears to be a failed preview message, enticing the target to click the link to be directed to the credential-stealing infrastructure. Occasionally, the Star Blizzard Defendants makes use of open redirects within the PDF file to further disguise their operational infrastructure. In the example below, Defendants use a Google URL for redirection. **Figure 8** is an example of a document hosted on OneDrive that uses a Google redirect link to send users to Star Blizzard-controlled infrastructure. **Figure 9** is an example of another file sharing platform, Proton Drive, also being impersonated by the Star Blizzard Defendants.


International Cyber-Activity.pdf -
onedrive.live.com/?authkey=[redacted]
OneDrive
Sign In
Create
Open
Share
Download
···
International Cyber-A....pdf
1 / 1
International Cyber Activity.pdf
Try again

Hmm... Microsoft Outlook cannot connect to the server.

https://www.google.com/url?q=https://protection-link.online/checker/view/?
[redacted]

Figure 8



Котирування.pdf

Котирування.pdf

Hmm... looks like this file doesn't have a preview we can show you

Figure 9

Attack Step 3: Capture Credentials and Exfiltrate Data

30. Based on Microsoft's investigations, regardless of the method of delivery, when the target clicks the URL, the target is directed to a Star Blizzard-controlled virtual server hosting a phishing proxy framework. A proxy or proxy server acts as a go-between a user and the Internet, offering privacy, access, and security. Threat actors exploit proxy servers by using it to hide their activities.

31. The Star Blizzard Defendants often use a malicious proxy framework Evilginx, which is an advanced phishing tool that act as "man-in-the-middle" attack. This type of attack intercepts network communications between a user's browser and a legitimate website, stealthily capturing login credentials and authentication cookies, even if the account uses two-factor authentication (2FA). This is what allows the Star Blizzard Defendants to re-access the target's account at later time without requiring the target to perform the similar activity of clicking on a controlled link and inputting in credentials). This process is depicted in **Figure 10.**

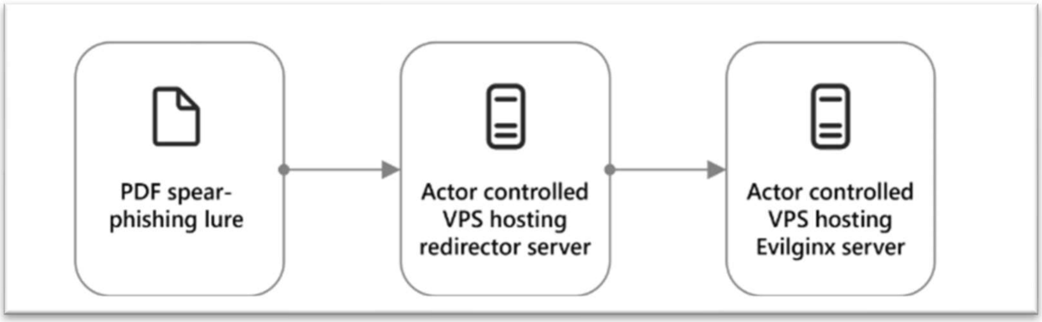

PDF spear-phishing lure
Actor controlled VPS hosting redirector server
Actor controlled VPS hosting Evilginx server

Figure 10

32. On occasion, Microsoft has observed attempts by the Star Blizzard Defendants to evade automated browsing and detonation by fingerprinting browsing behavior. In automated browsing, security systems use automated tools to visit websites. "Detonation" is when those security systems open files to see if they are harmful (like scanning them to see if they have a virus). Just like a fingerprint is unique, every browser and user have a unique "fingerprint" based on how users browse the Internet. The Star Blizzard Defendants can recognize when a security tool is checking their malicious website or file and limit malicious activity to avoid raising any alarms.

33. Once the target is redirected to the final page, the target is prompted to enter their credentials, by proxying the connect to the sign-in page for a legitimate provider and intercepting any credentials and authentication tokens. After credentials are captured or authentication tokens copied, the target is redirected to a website or document to complete the interaction to prevent tipping off the target that a phishing attack occurred. **Figure 11** is an example of a cloned phishing portal used by the Star Blizzard Defendants to directly impersonate a victim organization.

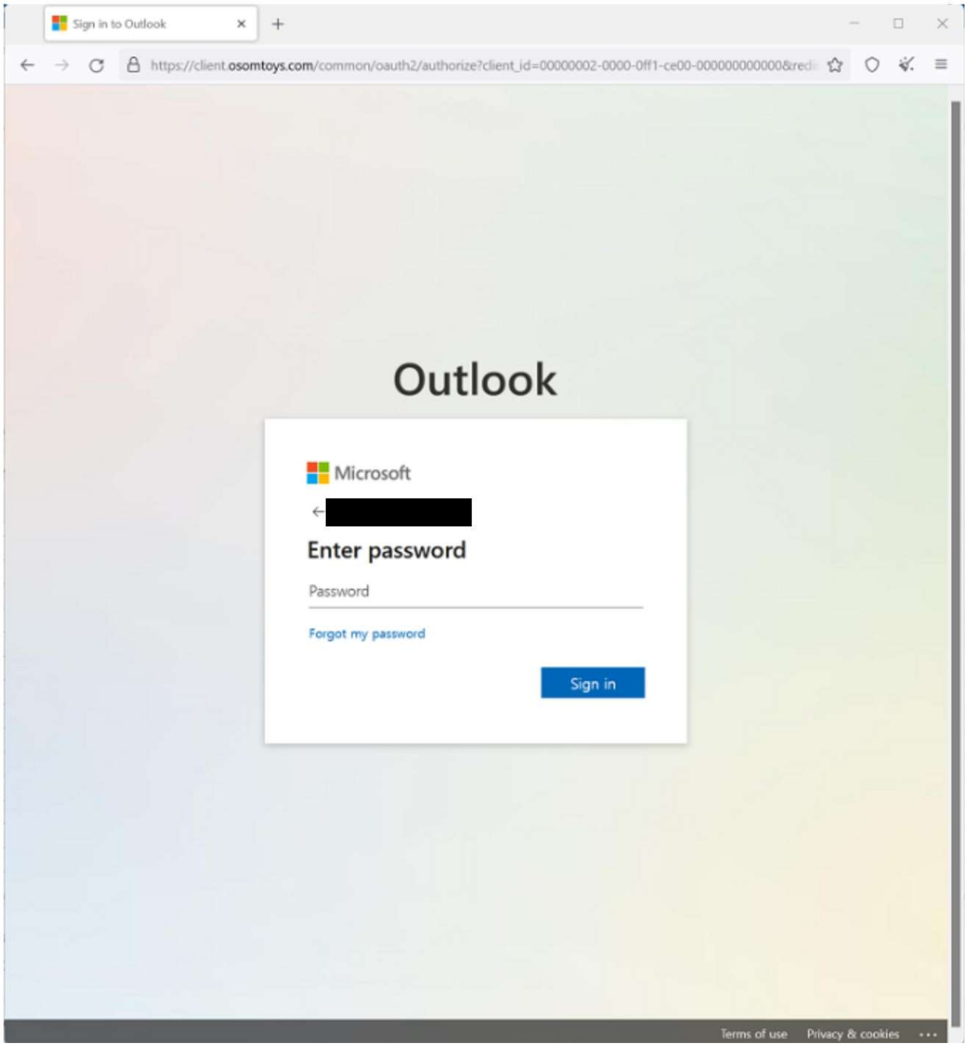


Figure 11

<u>Attack Step 4: Use Credentials and Exfiltrated Data</u>

34. Our investigation showed that the Star Blizzard Defendants use stolen credentials and replayed authentication tokens to directly sign in to victim email accounts. We have confirmed that Defendants regularly engage in the following activities:

a. **Exfiltration of intelligence data**: Defendants access exfiltrate emails, attachments, and contact lists from the inbox of victims. This includes both the ability to view the sensitive data within the email inbox and to download contact lists, emails, and any attachments to those emails.

b. **Setup of persistent data collection**: In limited cases, the Star Blizzard Defendants set up forwarding rules from victim inboxes to Star Blizzard-controlled dead drop accounts where the actor has long-term access to collected data. On more than one occasion, we have observed that the Star Blizzard Defendants were able to access mailing list data for sensitive groups, such as those frequented by former intelligence officials, and maintain a collection of information from the mailing list for targeting and exfiltration.

c. **Access to people of interest**: There have been several cases where the Star Blizzard Defendants used their impersonation accounts to facilitate dialog with specific people of interest and, as a result, were included in conversations, sometimes unwittingly, involving multiple parties. The nature of the conversations identified during investigations by Microsoft demonstrates potentially sensitive information being shared that could provide intelligence value.

35. Based on the specific victimology, documents stolen, conversations fostered, and sustained collection observed, we assess that data theft is likely a key motivation of the Star Blizzard Defendants.

IV. INVESTIGATING THE STAR BLIZZARD INTERNET INFRASTRUCTURE

36. Microsoft investigated the online infrastructure used in the Star Blizzard Defendants' spear phishing campaign described in this declaration. We determined that Defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. The Star Blizzard

Defendants have registered domains using functioning email addresses by which they communicated with domain registrars in order to complete the registration process.

37. Cybercriminals like the Star Blizzard Defendants are known to obfuscate their identities to evade capture by law enforcement and continue their cybercrime, which in this instance, is to engage in spear phishing activities to steal personal information and exfiltrate sensitive data.

38. In the course of the investigation, Microsoft (1) engaged in the analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Defendants, (2) discovered login activity into Microsoft services from Star Blizzard-controlled infrastructure on the Internet, (3) matched reported Star Blizzard spear phishing campaigns to registered domains, (4) monitored domain registrations associated with the Star Blizzard-controlled email addresses and other pertinent WHOIS record information, (5) monitored infrastructure frequently utilized by the Star Blizzard defendants in order to identify new domains being registered by the Star Blizzard defendants, (6) has confirmed resolution settings to particular proxy systems hosted on Virtual Private Servers (VPSs) which have frequently been used by the Star Blizzard defendants in the past, and (7) reviewed peer findings and public reporting.

39. For example, among other factors, Microsoft monitors and utilizes features specifically used by the Defendants, dates associated with the domain (registration etc.), particular abuse types or infrastructure providers previously seen carried out by the Star Blizzard Defendants, re-use of technical infrastructure previously used by the Defendants (specific Internet Protocol (IP) addresses and similar technical features associated with the domain or its operation), particular patterns of domain naming conventions that are known to be associated with the Defendants.

40. Our investigation found that the Star Blizzard Defendants register custom deceptive domains name that mimics a known website or cloud service may help the spear phishing link appear legitimate if securitized by the recipient. They use bespoke domains sparingly to reduce the likelihood an email security gateway or desktop security software will block the use of the link. By using a custom domain name, the Star Blizzard Defendants control when and how it delivered material and allows control of the Domain Name Service (DNS)[3] settings for redirection to Star Blizzard-controlled IP addresses and proxies and filters which computers are redirected through the proxy. The Star Blizzard Defendants use these domains/IP addresses as infrastructure to deliver a custom-built weaponized PDF or files to lure for the victim into opening and providing their credentials to copy authentication tokens.

41. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Star Blizzard 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 Star Blizzard 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 Star Blizzard Defendants. At times, other researchers in the security community independently identify Star Blizzard domains and associated IP addresses, and these reports may be used to further validate Microsoft's analysis.

[3] The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like Microsoft.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. https://www.cloudflare.com/learning/dns/what-is-dns/.

42. Our investigation and analysis note that the Star Blizzard Defendants have attempted to obfuscate their identities by using email marketing platforms to hide true email sender addresses and privacy-focused DNS providers to obscure IP addresses.

43. The Star Blizzard Defendants also use server-side scripts, which performs a filtering capability, in an attempt to ensure that the only successful connection made to the backend AiTM proxy is the intended target, and not cyber security researchers/analysts/network defenders, by running software code that automates processes on network servers that are operated by Defendants. The Star Blizzard Defendants also use virtual private servers (VPS) and cloud-based file-sharing platforms.

V. DEFENDANTS ATTACKED MICROSOFT CUSTOMERS IN THE DC METROPOLITAN AREA

44. Through its investigation, Microsoft has determined that, through the attacks described in this declaration, the Star Blizzard Defendants have affirmatively targeted Microsoft customers in the D.C. metropolitan area.

45. Microsoft recently investigated the recent IP addresses used by the accounts known to be targeted by Star Blizzard's spear phishing activities. Technology exists to determine the geographic location of IP addresses, alone or in association with domains. Using such technology, I determined the geographical location of these IP addresses collected during the sample period. I plotted such IP addresses on maps of the District of Columbia (DC) metropolitan area (including the Northern Virginia area and parts of Maryland), to represent the location of the relevant activity.

46. As can be seen below, in **Figure 12**, the Star Blizzard Defendants have directed their spear phishing activity toward defense and intelligence consulting companies, non-

governmental organizations (NGOs) and intergovernmental organizations (IGOs), think tanks, and higher education in the District of Columbia.

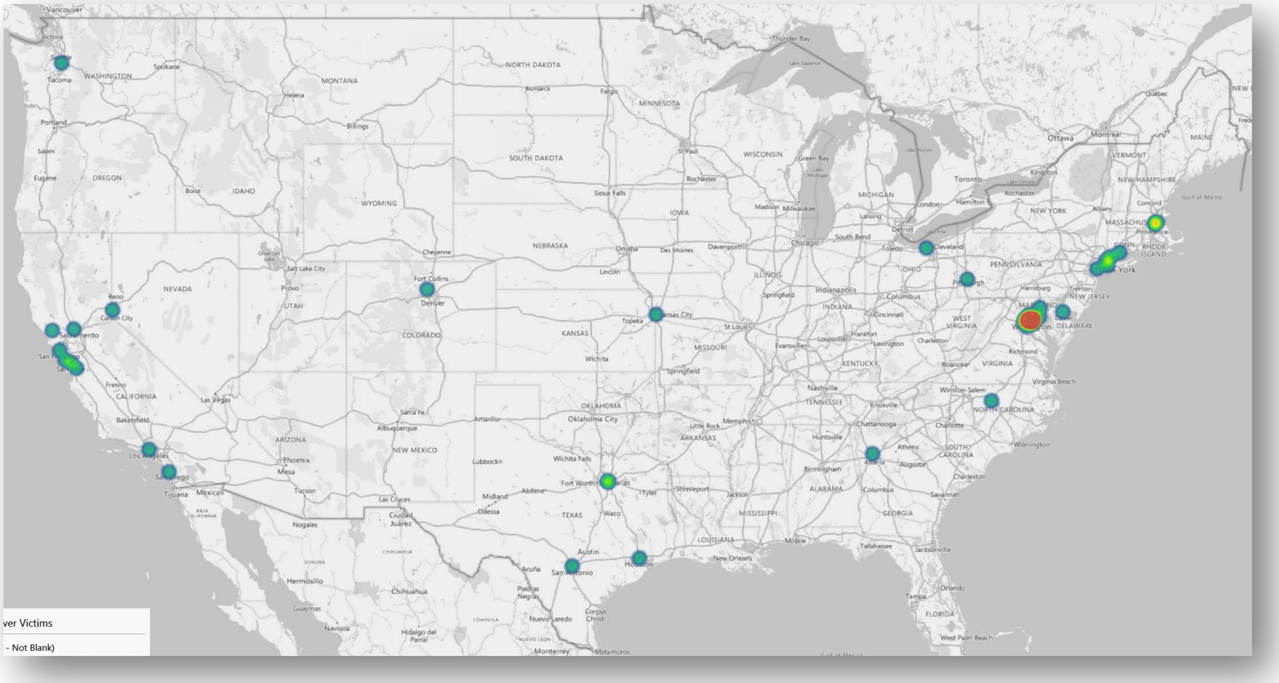


Figure 12

VI. HARM TO MICROSOFT AND ITS CUSTOMERS

47. The Star Blizzard Defendants' activities irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system and Outlook, Hotmail, OneDrive and Office 365 email and cloud services, as well as a variety of other software and services. Microsoft is the owner of the "Microsoft," "Windows," "Office," and "Outlook" trademarks. Trademark registrations infringed by Defendants are attached to the Complaint as **Appendix B.** 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, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and service and its brand, including the trademarks listed above. Microsoft has invested significant resources in excess of $5,000 to address the harm caused by the Star Blizzard Defendants' activities. Specifically, Microsoft has expended approximately $1,000,000, which represents the Microsoft personnel involved in efforts to investigate the Star Blizzard Defendants and their infrastructure.

48. Microsoft's customers who receive malicious spear phishing emails in their Outlook, Hotmail or Office 365 email addresses are damaged by the Star Blizzard Defendants' activities. Customers whose email accounts are compromised through the Defendants' credential theft are damaged by these activities.

49. Customers are usually unaware of the fact that they are being targeted, that their email accounts are compromised, that they are being monitored by the Star Blizzard Defendants or that sensitive information is being stolen from them. Even if aware of an account intrusion, users often lack the technical resources or skills to resolve the problem, allowing their accounts to be misused indefinitely, as manual steps to change account credentials or remove the Star Blizzard Defendants' access may be difficult for ordinary users.

50. This demonstrates the extreme problems that the activities of the Star Blizzard Defendants cause for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the defendants' intrusion into accounts and computers.

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

52. For customers in defense and intelligence consulting companies, non-governmental organizations (NGOs) and intergovernmental organizations (IGOs), think tanks, politicians, and higher education, the Star Blizzard Defendants' credential theft and exfiltration of data can be particularly damaging. Invasion of privacy, exfiltration of sensitive data, impersonation, reputational damage, ease of influence operations that may impact a targeted victim's career and how the public perceive their efforts, which may affect a victim's professional career.

53. Attached to this declaration as **Exhibit 3** is a true and correct copy of an article discussing Star Blizzard's activities expanding further to include defense-industrial targets, as well as U.S. Department of Energy facilities.[4]

VII. DISRUPTING STAR BLIZZARD'S ILLEGAL ACTIVITY

54. The most vulnerable point in the Defendants' operations are several Internet domains through which the Star Blizzard Defendants use AiTM proxies to obtain victim authentication tokens, replay those tokens to compromise accounts, and access sensitive

[4] Russian FSB accused of spear-phishing campaign against UK, US and allies, https://www.cshub.com/attacks/news/russian-fsb-accused-of-spear-phishing-campaign-against-uk-us-and-allies

information from victim accounts. A set of these is attached as **Appendix A** to the Complaint. These domains have been used in spear phishing emails directed at users of Microsoft's email services and exploit other Microsoft platforms like OneDrive.

55. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Star Blizzard Defendants collect victim credentials. In other words, any time a user clicks on a link in a spear phishing email and provides their username and password, that information will be prevented from going to the Defendants at the Star Blizzard-controlled domains, because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of the Star Blizzard Defendants.

56. Redirecting these Star Blizzard domains will directly disrupt current infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest, in protecting customers of other web services companies who have consented to the relief sought in this action.

57. I believe that the most effective way to suspend the injury caused to Microsoft, its consumers, and the public, is to take the steps described in the Proposed Order. This relief will significantly hinder the Star Blizzard Defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to Star Blizzard's malicious activities.

58. The Star Blizzard Defendants' techniques are designed to resist technical mitigation efforts, eliminating the ability to curb the injury purely through technical means. For example, once domains in the Star Blizzard Defendants' active infrastructure become known to the security

community, the Defendants abandon that infrastructure and move to new infrastructure that is used to continue Defendants' efforts to compromise accounts of new victims.

59. For this reason, providing notice to the Star Blizzard Defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason, as well, providing notice to the Star Blizzard 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.

60. Based on my experience observing the operation of numerous intrusions such as those carried out by the Star Blizzard Defendants, prior investigations, and legal actions involving such intrusions and actors, I believe that Defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

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

62. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Star Blizzard 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 that the foregoing is true and correct to the best of my knowledge.

Executed September 24, 2024, in Washington D.C.

Respectfully submitted,

____

Sean Ensz

Principal Investigator, Digital Crimes Unit
Microsoft Corporation

SEAN ENSZ

EXPERTISE

Investigations / Forensics

Incident Response

E-Discovery

Network Security

Program Development

CERTIFICATIONS

CISSP – ISC2 #44830
GSEC - GIAC
EnCE – Guidance Software
ACE- Access Data
RHCE 4 - RedHat, Inc

EDUCATION

BACHELOR OF SCIENCE
Oklahoma State University
2001

CONTACT

405.234.7715

saensz@gmail.com

PROFILE

Senior cyber security professional with 25 years of investigations, computer forensics, and incident response experience.

EXPERIENCE

Senior Investigator

Microsoft Digital Crimes Uni | 2021 - Present

Primary Responsibilities Include

- Investigating high impact cloud-based cybercrime incidents for potential criminal referral
- Developing Business Email Compromise Threat Intelligence on transnational organized crime gangs
- Disruption of Nation State infrastructure

SSIRP Crisis Lead

Microsoft Security Response Center | 2018 - 2021

Primary Responsibilities Include

- Managing cross-company security incident response that have significant impact to customers, Microsoft operations, and brand
- Managing incidents that include 0-day product vulnerabilities, cloud service vulnerabilities, privacy breaches, and criminal or nation state intrusions
- Coordinating with company stakeholders that include CELA, DCU, Issues Management, and Customer Support

Digital Security Manager

Devon Energy Corporation | 2014 - 2018

Primary Responsibilities Include

- Leading a 15-member security team
- Leading the Devon Cyber Incident Response Team (DCIRT)
- Conducting Insider Threat investigations
- Overseeing $4.1 million annual operating budget
- Managing Security Operations of Next-Gen Firewalls, Email Security Gateways, Endpoint Security, and Authentication Services
- Managing Physical Security video and card access systems
- Managing vendor relationships

SEAN ENSZ

TRAINING

SANS

SEC401 - Security Essentials
SEC504 – Incident Handling
SEC564 – Red Team Operations
LEG523 – Law of Investigations
MGT535 – IR Team Management

FORENSICS

NW3C – Basic Data Recovery
NW3C – Advanced Data Recovery
EnCase – Incident Responses & Forensic Analysis
EnCase – EnCase Enterprise
ACCESS DATA – FTK Bootcamp

INCIDENT RESPONSE

CERT/SEI – Incident Handling Fundamentals
CERT/SEI – Advanced Incident Handling

IT

RedHat – RHCE Rapid Track Course
Cisco - Introduction to Networking Technologies and ICND

Director of Information Security

University of Oklahoma | 2013- 2014

Primary Responsibilities

- ○ Representing Information Security functions to the Chief Information Office and various campus executive committees
- ○ Leading 10-member security team; including 2 managers
- ○ Managing budget and priorities for Incident Response, Computer Forensics, E-Discovery, and Risk Management functions
- ○ Overseeing enterprise-wide information security programs
- ○ Developing IT security related policy, process, and best practices
- ○ Establishing and executing the university's strategic security initiatives

Accomplishments

- ○ Established tri-campus security governance advisory council
- ○ Advocated $2.4 million next-gen network security architecture
- ○ Developed new campus-wide security risk management program

Principal Forensic Investigator

University of Oklahoma | 2004- 2013

Primary Responsibilities

- ○ Conducting digital investigations for Human Resources, Sexual Misconduct Office, and Law Enforcement assistance
- ○ Managing the OU Cyber Forensics Lab that maintained forensics capability for hard disk, mobile device, and network log analysis for IT and Police usage
- ○ Coordinating E-discovery efforts: preserve, collect, and analyze electronic stored information in preparation for civil litigation
- ○ Investigating network intrusions into campus system and data breaches and communicating findings to IT and campus leadership
- ○ Designing and implementing network monitoring tools to assistant in Incident Response and digital investigations
- ○ Team Lead for 6-person Investigations and Incident Response team

Accomplishments

- ○ Established OU Cyber Forensics Lab used by IT Security, OU Police, and Norman Police
- ○ Established the university's E-Discovery program in conjunction with the Office of Legal Counsel

SEAN ENSZ

TOOLS EXPERIENCE

Encase - Guidance Software

Forensics ToolKit - Access Data

Cellebrite UFED - Cellebrite

Office 365 Governance & Compliance - Microsoft

Maltego - Paterva

Qradar SIEM - IBM

Moloch Network Analysis - Open Source

Command Line Linux Tools - Open Souce

Police Investigator (*1999-2003)*

Police Officer (*1998-1999)*

Dispatcher (*1995-1998)*

Oklahoma State University Police Department | 1995- 2003

Primary Responsibilities

- Investigating computer crimes and other criminal violations as a State Commissioned Police Officer
- Conducting computer forensic investigations involving child pornography, network intrusions, credit card fraud, and intellectual property theft
- Investigating other criminal violations involving rape, narcotics, property theft, and fraud
- Providing investigative assistance to Federal Bureau of Investigations, Oklahoma State Bureau of Investigations, and Stillwater Police Dept

Accomplishments

- Established the OSUPD computer forensics lab
- Lead the investigation into the State's first successful prosecution of a digital copyright law violation

ADDITIONAL EXPERIENCE

Computer Forensics Adjunct Professor - Part Time

Redlands Community College / 2005 – 2007

Network Security Specialist

Oklahoma State University / 2003 – 2004

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY </>

Menu

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

SHARE:

CYBERSECURITY ADVISORY

Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns

Release Date: December 07, 2023 **Alert Code:** AA23-341A

RELATED TOPICS: NATION-STATE CYBER ACTORS </topics/cyber-threats-and-advisories/nation-state-cyber-actors>, CYBER THREATS AND ADVISORIES </topics/cyber-threats-and-advisories>, MALWARE, PHISHING, AND RANSOMWARE </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

The Russia-based actor is targeting organizations and individuals in the UK and other geographical areas of interest.

OVERVIEW

The Russia-based actor Star Blizzard (formerly known as SEABORGIUM, also known as Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie) continues to successfully use spear-phishing attacks against targeted organizations and individuals in the UK, and other geographical areas of interest, for information-gathering activity.

The UK National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the US National Security Agency (NSA), the US Cyber National Mission Force (CNMF), the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ) assess that Star Blizzard is almost certainly subordinate to the Russian Federal Security Service (FSB) Centre 18.

Industry has previously published details of Star Blizzard. This advisory draws on that body of information <https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/>.

This advisory raises awareness of the spear-phishing techniques Star Blizzard uses to target individuals and organizations. This activity is continuing through 2023.

To download a PDF version of this advisory, see Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns <https://www.ncsc.gov.uk/files/advisory-russian-fsb-cyber-actor-star-blizzard-continues-worldwide-spear-sphishing-campaigns.pdf>.

TARGETING PROFILE

Since 2019, Star Blizzard has targeted sectors including academia, defense, governmental organizations, NGOs, think tanks and politicians.

Targets in the UK and US appear to have been most affected by Star Blizzard activity, however activity has also been observed against targets in other NATO countries, and countries neighboring Russia.

During 2022, Star Blizzard activity appeared to expand further, to include defense-industrial targets, as well as US Department of Energy facilities.

OUTLINE OF THE ATTACKS

The activity is typical of spear-phishing campaigns, where an actor targets a specific individual or group using information known to be of interest to the targets. In a spear-phishing campaign, an actor perceives their target to have direct access to information of interest, be an access vector to another target, or both.

Research and Preparation

Using open-source resources to conduct reconnaissance, including social media and professional networking platforms, Star Blizzard identifies hooks to engage their target. They take the time to research their interests and identify their real-world social or professional contacts [T1589 <https://attack.mitre.org/versions/v14/techniques/t1589/>], [T1593 <https://attack.mitre.org/versions/v14/techniques/t1593/>].

Star Blizzard creates email accounts impersonating known contacts of their targets to help appear legitimate. They also create fake social media or networking profiles that impersonate respected experts [T1585.001 <https://attack.mitre.org/versions/v14/techniques/t1585/001/>] and have used supposed conference or event invitations as lures.

Star Blizzard uses webmail addresses from different providers, including Outlook, Gmail, Yahoo and Proton mail in their initial approach [T1585.002 <https://attack.mitre.org/versions/v14/techniques/t1585/002/>], impersonating known contacts of the target or well-known names in the target's field of interest or sector.

To appear authentic, the actor also creates malicious domains resembling legitimate organizations [T1583.001 <https://attack.mitre.org/versions/v14/techniques/t1583/001/>].

Microsoft Threat Intelligence Center (MSTIC) provides a list of observed Indicators of Compromise (IOCs) in their SEABORGIUM blog, but this is not exhaustive.

Preference for Personal Email Addresses

Star Blizzard has predominantly sent spear-phishing emails to targets' personal email addresses, although they have also used targets' corporate or business email addresses. The actors may intentionally use personal emails to circumvent security controls in place on corporate networks.

Building a Rapport

Having taken the time to research their targets' interests and contacts to create a believable approach, Star Blizzard now starts to build trust. They often begin by establishing benign contact on a topic they hope will engage their targets. There is often some correspondence between attacker and target, sometimes over an extended period, as the attacker builds rapport.

Delivery of Malicious Link

Once trust is established, the attacker uses typical phishing tradecraft and shares a link [T1566.002 <https://attack.mitre.org/versions/v14/techniques/t1566/002/>], apparently to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials.

The malicious link may be a URL in an email message, or the actor may embed a link in a document [T1566.001 <https://attack.mitre.org/versions/v14/techniques/t1566/001/>] on OneDrive, Google Drive, or other file-sharing platforms <https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/>.

Star Blizzard uses the open-source framework EvilGinx in their spear- phishing activity, which allows them to harvest credentials and session cookies to successfully bypass the use of two-factor authentication [T1539 <https://attack.mitre.org/versions/v14/techniques/t1539/>], [T1550.004 <https://attack.mitre.org/versions/v14/techniques/t1550/004/>].

Exploitation and Further Activity

Whichever delivery method is used, once the target clicks on the malicious URL, they are directed to an actor-controlled server that mirrors the sign-in page for a legitimate service. Any credentials entered at this point are now compromised.

Star Blizzard then uses the stolen credentials to log in to a target's email account [T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>], where they are known to access and steal emails and attachments from the victim's inbox [T1114.002 <https://attack.mitre.org/versions/v14/techniques/t1114/002/>]. They have also set up mail-forwarding rules, giving them ongoing visibility of victim correspondence [T1114.003 <https://attack.mitre.org/versions/v14/techniques/t1114/003/>].

The actor has also used their access to a victim email account to access mailing‑list data and a victim's contacts list, which they then use for follow- on targeting. They have also used compromised email accounts for further phishing activity [T1586.002 <https://attack.mitre.org/versions/v14/techniques/t1586/002/>].

CONCLUSION

Spear-phishing is an established technique used by many actors, and Star Blizzard uses it successfully, evolving the technique to maintain their success.

Individuals and organizations from previously targeted sectors should be vigilant of the techniques described in this advisory.

In the UK you can report related suspicious activity to the NCSC <https://report.ncsc.gov.uk/>.

Information on effective defense against spear-phishing is included in the Mitigations section below.

MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® <https://attack.mitre.org/versions/v14/matrices/enterprise/> framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Reconnaissance	T1593 <https://attack.mitre.org/versions/v14/techniques/t1593/>	Search Open Websites/Domains	Star Blizzard uses open-source resear and social media to identify information about victims use in targeting.
Reconnaissance	T1589 <https://attack.mitre.org/versions/v14/techniques/t1589/>	Gather Victim Identity Information	Star Blizzard uses online data sets and open-source resources to gather information about their targets.
Resource Development	T1585.001 <https://attack.mitre.org/versions/v14/techniques/t1585/001/>	Establish Accounts: Social Media Accounts	Star Blizzard has been observed establishing fraudulent profiles on professional networking sites to condu reconnaissan
Resource Development	T1585.002 <https://attack.mitre.org/versions/v14/techniques/t1585/002/>	Establish Accounts: Email Accounts	Star Blizzard registers consumer em accounts matching the names of individuals th are impersonatin to conduct spear-phishin activity.

Tactic	ID	Technique	Procedure
Resource Development	T1583.001 <https://attack.mitre.org/versions/v14/techniques/t1583/001/>	Acquire Infrastructure: Domains	Star Blizzard registers domains to ho their phishing framework.
Resource Development	T1586.002 <https://attack.mitre.org/versions/v14/techniques/t1586/002/>	Compromise Accounts: Email Accounts	Star Blizzard has been observed usir compromised victim email accounts to conduct spea phishing activity again contacts of th original victim
Initial Access	T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>	Valid Accounts	Star Blizzard uses compromised credentials, captured from fake log-in pages, to log i to valid victim user accounts
Initial Access	T1566.001 <https://attack.mitre.org/versions/v14/techniques/t1566/001/>	Phishing: Spear-phishing Attachment	Star Blizzard uses maliciou links embedd in email attachments t direct victims their credenti stealing sites
Initial Access	T1566.002 <https://attack.mitre.org/versions/v14/techniques/t1566/002/>	Phishing: Spear-phishing Link	Star Blizzard sends spear-phishing ema with maliciou links directly t credential-stealing sites or to documer hosted on a fi sharing site, which then direct victims credential-stealing sites

Tactic	ID	Technique	Procedure
Defense Evasion	T1550.004 <https://attack.mitre.org/versions/v14/techniques/t1550/004/>	Use Alternate Authentication Material: Web Session Cookie	Star Blizzard bypasses mul factor authenticatio on victim ema accounts by using session cookies stolen using EvilGinx
Credential Access	T1539 <https://attack.mitre.org/versions/v14/techniques/t1539/>	Steal Web Session Cookie	Star Blizzard uses EvilGinx steal the session cooki of victims directed to th fake log-in domains.
Collection	T1114.002 <https://attack.mitre.org/versions/v14/techniques/t1114/002/>	Email Collection: Remote Email Collection	Star Blizzard interacts directly with externally facing Exchange services, Offi 365 and Goog Workspace to access email and steal information using compromised credentials or access tokens
Collection	T1114.003 <https://attack.mitre.org/versions/v14/techniques/t1114/003/>	Email Collection: Email Forwarding Rule	Star Blizzard abuses email-forwarding rules to monit the activities a victim, steal information, and maintain persistent access to victim's email even after compromised credentials ar reset.

MITIGATIONS

A number of mitigations will be useful in defending against the activity described in this advisory.

- **Use strong passwords. Use a separate password for email accounts and avoid password re-use across multiple services.** See NCSC guidance: Top Tips for Staying Secure Online <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email>.
- **Use multi-factor authentication** (2-factor authentication/two-step authentication) to reduce the impact of password compromises. See NCSC guidance: Multi-factor Authentication for Online Services <https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services> and Setting Up 2-Step Verification (2SV) <https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv>.
- **Protect your devices and networks by keeping them up to date:** Use the latest supported versions, apply security updates promptly, use anti-virus and scan regularly to guard against known malware threats. See NCSC guidance: Device Security Guidance <https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software>.
- **Exercise vigilance.** Spear-phishing emails are tailored to avoid suspicion. You may recognize the sender's name, but has the email come from an address that you recognize? Would you expect contact from this person's webmail address rather than their corporate email address? Has the suspicious email come to your personal/webmail address rather than your corporate one? Can you verify that the email is legitimate via another means? See NCSC guidance: Phishing attacks: Defending Your Organization <https://www.ncsc.gov.uk/guidance/phishing> and Internet Crime Complaint Center(IC3) | Industry Alerts <https://www.ic3.gov/home/industryalerts>.
- **Enable your email providers' automated email scanning features.** These are turned on by default for consumer mail providers. See NCSC guidance: Telling Users to "Avoid Clicking Bad Links" Still Isn't Working <https://www.ncsc.gov.uk/blog-post/telling-users-to-avoid-clicking-bad-links-still-isnt-working>.
- **Disable mail-forwarding.** Attackers have been observed to set up mail-forwarding rules to maintain visibility of target emails. If you cannot disable mail-forwarding, then monitor settings regularly to ensure that a forwarding rule has not been set up by an external malicious actor.

DISCLAIMER

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Tags

Topics: Nation-State Cyber Actors </topics/cyber-threats-and-advisories/nation-state-cyber-actors>, Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Malware, Phishing, and Ransomware </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

MITRE ATT&CK TTP: Collection (TA0009), Credential Access (TA0006), Defense Evasion (TA0005), Initial Access (TA0001), Reconnaissance (TA0043), Resource Development (TA0042)

Co-Sealers and Partners: Federal Bureau of Investigation, International, National Security Agency

Nation-State Actor: Russia

Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

Related Advisories

SEP 05, 2024 CYBERSECURITY ADVISORY | AA24-249A

Russian Military Cyber Actors Target US and Global Critical Infrastructure </news-events/cybersecurity-advisories/aa24-249a>

AUG 29, 2024 CYBERSECURITY ADVISORY | AA24-242A

#StopRansomware: RansomHub Ransomware </news-events/cybersecurity-advisories/aa24-242a>

AUG 28, 2024 CYBERSECURITY ADVISORY | AA24-241A

Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations </news-events/cybersecurity-advisories/aa24-241a>

JUL 25, 2024 CYBERSECURITY ADVISORY | AA24-207A

North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs </news-events/cybersecurity-advisories/aa24-207a>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools> **News & Events** </news-events>

Careers </careers> **About** </about>

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

Equal Opportunity & Accessibility </oedia>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Filter Categories +

Russian FSB accused of spear-phishing campaign against UK, US and allies

Star Blizzard threat actor is “almost certainly” subordinate to the Russian Federal Security Service Centre 18

Add bookmark

Michael Hill
12/08/2023

The Russia-based actor Star Blizzard (formerly known as SEABORGIUM) continues to successfully use spear-phishing attacks against targeted organizations and individuals in the UK and US, as well as other geographical areas of interest, for information-gathering activity. That's according to an international cyber security advisory from multiple governments which states that Star Blizzard (also known as Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie) is almost certainly subordinate to the Russian Federal Security Service (FSB) Centre 18.

Star Blizzard has targeted sectors including academia, governmental organizations, NGOs, think tanks and politicians since 2019. Targets in the UK and US appear to have been most affected by Star Blizzard activity, however activity has also been observed against targets in other NATO countries and neighboring Russia, the advisory read. More recently, Star Blizzard activity appeared to expand further to include defense-industrial targets, as well as US Department of Energy facilities.

The UK Foreign Office has summoned the Russian ambassador and sanctioned a Russian intelligence officer along with a second member of the Star Blizzard group, according to *Sky News*. The UK government said the malicious cyber activity is an attempt to interfere in UK politics and democratic processes.

Star Blizzard conducts reconnaissance and impersonates contacts of their targets

Using open-source resources to conduct reconnaissance, including social media and professional networking platforms, Star Blizzard identifies hooks to engage targets, the advisory stated. “They take the time to research their interests and identify their real-world social or professional contacts.”

The threat actor creates email accounts impersonating known contacts of their targets to help appear legitimate. “They also create fake social media or networking profiles that impersonate respected experts and have used supposed conference or event invitations as lures.” Star Blizzard uses webmail addresses from different providers including Outlook, Gmail, Yahoo and Proton mail in their initial approach.

Personal email addresses targeted with spear-phishing

Star Blizzard has predominantly sent spear-phishing emails to targets' personal email addresses, although they have also used targets' corporate or business email addresses, the government said. “The actors may intentionally use personal emails to circumvent security controls in place on corporate networks.”

Having researched their targets' interests and contacts to create a believable approach, Star Blizzard then starts to build trust with potential victims. “They often begin by establishing benign contact on a topic they hope will engage their targets. There is often some correspondence between attacker and target, sometimes over an extended period, as the attacker builds rapport.”

Once trust is established, the attacker uses typical phishing tradecraft and shares a link, apparently to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials. “The malicious link may be a URL in an email message, or the actor may embed a link in a document on OneDrive, Google Drive or other file-sharing platforms.”

Threat actor uses open-source framework to harvest credentials and session cookies

Star Blizzard uses the open-source framework EvilGinx to harvest credentials and session cookies, successfully bypassing the use of two-factor authentication (2FA). Once the target clicks on the malicious URL, they are directed to an actor-controlled server that mirrors the sign-in page for a legitimate service. Any credentials entered at this point are now compromised.

"Star Blizzard then uses the stolen credentials to log in to a target's email account, where they are known to access and steal emails and attachments from the victim's inbox. They have also set up mail-forwarding rules, giving them ongoing visibility of victim correspondence."

Furthermore, the actor has used their access to a victim email account to access mailing-list data and a victim's contacts list, which they then use for follow-on targeting. They have also used compromised email accounts for further phishing activity.

A number of mitigations will be useful in defending against the activity, the advisory stated. These include:

- Using multi-factor authentication (MFA) to reduce the impact of password compromises.
- Protecting devices and networks by keeping them up to date.
- Enabling email providers' automated email scanning features.
- Disabling mail-forwarding.

Revelations of Russian state-sponsored activity are no surprise

The revelations detailing alleged Russian state-sponsored attempts to influence democratic processes should come as no surprise, commented Chris Morgan, senior cyber threat intelligence analyst at cyber security firm ReliaQuest. "For several years, multiple Western countries have accused Russia of attempting to conduct espionage against its adversaries, sowing disinformation and otherwise seeking to undermine democratic processes. Such covert activities also allow Russia to extract sensitive information, maintain persistence within systems of organizations of strategic interest and obtain intelligence to guide Russian foreign policy."

The attribution to StarBlizzard is also not unexpected, Morgan said. "The group has previously used domain impersonation to facilitate theft of credentials, while regularly rotating their infrastructure to avoid detection. Despite being agile and sophisticated, such APT groups continue to use rudimentary techniques – largely because they work."

Tags: Cyber Attack Phishing Cyber Security Incident

Comments

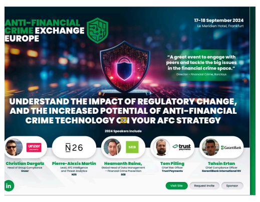
You must Login or Subscribe to comment.

Upcoming Events

Anti-Financial Crime Exchange Europe 2024

September 19-20
Frankfurt, Germany

Register Now | View Agenda | View Event


ANTI-FINANCIAL CRIME EXCHANGE EUROPE
UNDERSTAND THE IMPACT OF REGULATORY CHANGE, AND THE INCREASED POTENTIAL OF ANTI-FINANCIAL CRIME TECHNOLOGY ON YOUR AFC STRATEGY

OT Cybersecurity Summit

October 28 - 29, 2024
Norris Conference Center, Houston CityCentre, TX

Register Now | View Agenda | View Event

Automotive Cyber Security Europe 2024 | Automotive IQ

11 - 14 November 2024
The Westin Grand Frankfurt, Germany

Register Now | View Agenda | View Event

Digital Identity Week

09 - 10 September, 2025
Sydney, Australia

Register Now | View Agenda | View Event

DIGITAL IDENTITY WEEK
11-13 June 2024 | Melbourne, Australia
The one-stop-shop for organisations involved in authenticating human identity

MORE EVENTS

Follow Us

Latest Webinars

Preventing financial and reputational risk with process intelligence

👁 2024-05-23

🕓 11:00 AM - 12:00 PM EDT

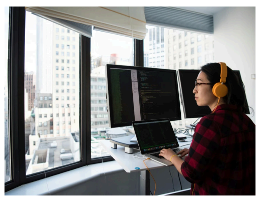
Learn how to manage risk stemming from poorly controlled processes in a collaborative way

Building high-performing development teams: Harnessing tools, processes & AI

👁 2024-05-02

🕓 11:00 AM - 12:00 PM EDT

Discover how to enhance your development team's efficiency through advanced tools, Agile methodologi...



Building cyber resilience

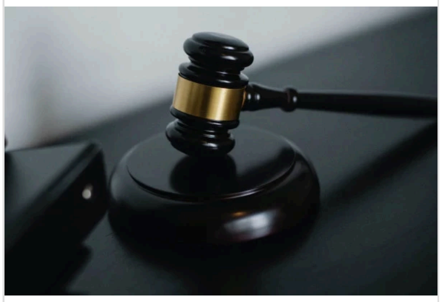
👁 2024-04-24

🕓 11:30 AM - 12:30 PM SGT

Why it's essential that technology seamlessly connects IT, security, risk and the business

MORE WEBINARS

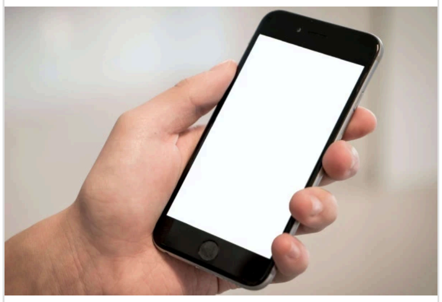
RECOMMENDED



IOTW: Victoria Court recordings exposed in suspected ransomware attack

🕓 2024-01-05

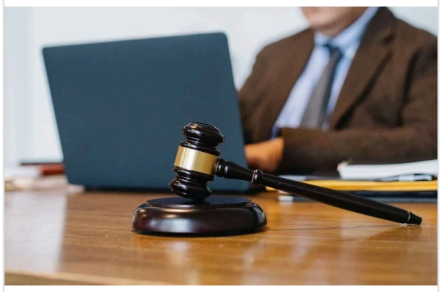
By Michael Hill



IOTW: Russia-linked cyber attack targets Ukraine's biggest phone operator

🕓 2023-12-15

By Michael Hill



BEC attacks on law firms spike as cyber criminals bypass MFA

🕓 2023-12-07

By Michael Hill

IOTW: Data breach exposes sensitive information of Canadian Government employees

🕓 2023-11-24

By Michael Hill

Cyber Security Hub, a division of IQPC