UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Microsoft Corporation, a Washington State Corporation and Health-ISAC, Inc., a Florida non-profit organization,

Plaintiffs,

v.

Saad Fridi,

and

John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Case No.

FILED UNDER SEAL
PURSUANT TO LOCAL RULE 5

DECLARATION OF DEREK RICHARDSON IN SUPPORT OF PLAINTIFFS' *EX PARTE* APPLICATION FOR TEMPORARY RESTRAINING ORDER

I, Derek Richardson declares as follows:

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

2. Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software programs and hardware systems to individuals, businesses, and governments. Microsoft® is a provider of the Windows® computer operating system, and a variety of other software and services including Microsoft 365®, Outlook®, and Azure®. 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 worldwide symbols that are well-recognized within its channels of trade. To protect this goodwill, reputation, and strong branding, Microsoft has registered trademarks for the following products and services: Microsoft®, Windows®, Microsoft 365®, Office365®, Office®, Microsoft Office®, SharePoint®, OneDrive®, Outlook®, and Excel®, among other trademarks. The registrations for these trademarks are attached to the Complaint as **Appendix B**.

3. Microsoft's Digital Crimes Unit ("DCU") is a Microsoft team responsible for protecting Microsoft and its customers against cybercrime threats. DCU is an international team of technical, legal, and business experts that has been fighting cybercrime, protecting individuals and organizations, and safeguarding the integrity of Microsoft services since 2008.[1] One of DCU's responsibilities is to investigate cybersecurity threats and identify and attribute attacks, like it has done here with the Tycoon 2FA Defendants. DCU also collaborates with Microsoft Threat Intelligence ("MTI"), which is made up of thousands of world-class experts, security researchers, analysts, and threat hunters. MTI regularly publishes threat intelligence blogs alerting customers and the public of cybersecurity threats.[2] On average, there are approximately 600 million cyber or nation state attacks attempted against Microsoft customers daily. As part of my role with DCU, I identify the attackers or threat groups that pose the largest risk to Microsoft customers.

[1] *Microsoft Digital Crimes Unit*, Microsoft available at https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit (last accessed Feb. 17, 2026).

[2] *See* Microsoft, *Threat Intelligence Blog*, available https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/ (last accessed Feb. 17, 2026).

4. I joined Microsoft in 2013. In my role at Microsoft as part of DCU, I assess technological security threats to Microsoft and the effect of such threats on Microsoft's business and customers. Among my responsibilities is protecting Microsoft's online service assets from network-based attacks. I also investigate malware and participate in court-authorized countermeasures to neutralize and disrupt malware. For example, in my role as both an investigator and software engineer, I have personally participated in investigation and stopping malware families and other threats such as Lumma and RedVDS.

5. I obtained my Bachelor of Science in Business Administration from Hawaii Pacific University in 2006. I obtained my juris doctorate and MBA from Texas Tech University in 2013. I also obtained a graduate certificate in strategic studies and am SANS GIAC certified in Reverse Engineering Malware, Penetration Testing, Advanced Network Forensics and Window Forensics. Prior to entering the private sector, from 2001 to 2005, I served as Infantry Team Leader in the United States Marine Corps. I was responsible for leading a combat team in Iraq, including the historic liberation of Fallujah in the battle of Fallujah of 2004. Before joining Microsoft, I worked at Fiveby Solutions, Inc. which provides vendor services to Microsoft's DCU. A copy of my resume is attached to this declaration as **Exhibit 1**.

6. My declaration concerns the investigation into a foreign cybercriminal organization comprised of Defendant Saad Fridi and a series of unknown individuals—John Does 1-4—who are collectively known as "Tycoon 2FA Defendants." I investigated the structure and function of Tycoon 2FA Defendants' criminal organization, which I discuss in this declaration. I, along with my DCU colleagues, investigated Tycoon 2FA Defendants' victim targeting methodology, attack techniques, and the tools used to execute their cybercriminal attacks. My declaration also addresses the impact and harm that Tycoon 2FA Defendants cause Microsoft, its customers, and

the public, and the continuation of this irreparable harm if the Tycoon 2FA Defendants are permitted to carry out their cybercriminal activity. Finally, my declaration explains what I believe to be the most effective way of disrupting Tycoon 2FA Defendants' illegal activity.

CYBERCRIME AT ISSUE: PHISHING-AS-A-SERVICE

7. Phishing is the fraudulent practice of sending emails or other messages purporting to be from legitimate senders to induce recipients to reveal personal information, such as passwords or other credentials. It is a form of social engineering where the recipient-victim is convinced to interact with the correspondence (referred to as the "lure"). Tycoon 2FA Defendants manufacture, sell, and facilitate the deployment of pre-packaged sets of tools ("phishing kits") that enable other cybercriminals to launch phishing attacks with relative ease. These Tycoon 2FA phishing kits are advertised and promoted as being able to circumvent the security features of Microsoft products (and the security features of other companies such as Adobe, Google, GoDaddy), use Microsoft logos, and mimic the appearance of authentic communications to deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. When a phishing recipient clicks on a weaponized link, she effectively ushers the attacker through the front door of the victim's system negating the ability of Microsoft security to repel the attack.

8. Phishing is particularly pernicious because once the victim interacts with the lure and unknowingly provides their credentials to a cybercriminal, that cybercriminal has unfettered

access and can launch devasting ransomware and malware attacks. In 2024 alone the estimated financial impact of phishing attacks was more than $3.5 billion.[3]

9. I, along with other DCU investigators, investigate cybercrime campaigns like phishing-as-a-service ("PhaaS") that are perpetrated by threat actors targeting Microsoft and its customers. In this role, several DCU investigators including myself investigated Tycoon 2FA's PhaaS campaign.

10. As an experienced cybercriminal investigator, I am familiar with phishing. The intent of phishing typically includes stealing someone's account credentials, authorization tokens or causing the victim to reveal personal information (such as credit card numbers, bank information, or passwords) or sensitive business information for use in perpetrating additional cybercrimes.

11. The Phishing-as-a-Service or PhaaS kits are essentially "how to" or "do-it-yourself" manuals to assist Tycoon 2FA Defendants' cybercriminal customers in developing and executing attacks on email systems through phishing campaigns. Cybercriminals can buy the phishing kit that best serves their criminal objective, including selecting which companies they want to target (here, targeting Microsoft's enterprise customers). This declaration specifically concerns the phishing kits that are designed to lead victims to believe they are dealing with legitimate Microsoft products and therefore can be used to target Microsoft customers.

12. The Tycoon 2FA Defendants operate in a fashion similar to other threat actors that have been enjoined by U.S. federal courts such as the "RaccoonO365 Defendants" and the "Fake

[3] Microsoft, *Microsoft Digital Defense Report 2024*, at p. 34, available at https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf (Oct. 2024) ("2024 *MDDR*").

ONNX Defendants." Both sold do-it-yourself phishing kits and operated as a PhaaS. In November 2024, Microsoft filed a lawsuit in the Eastern District of Virginia and obtained injunctive relief effectively crippling Fake ONNX's cybercriminal operations. *See Microsoft Corporation and LF Projects LLC v. Abanoub Nady and John Does 1-4*, Civil Action No. 1:24-cv-2013-RDA (E.D. VA. Nov. 12, 2024) (Alston, J.). In August 2025, Microsoft filed a lawsuit in the Southern District of New York and obtained injunctive relief, effectively crippling RaccoonO365's cybercriminal operation. *Microsoft and Health-ISAC v. Joshua Ogundipe and John Does 1-4*, 1:25-cv-07111 (S.D.N.Y. Aug. 2025) (Rakoff, J.). I have spoken with members of DCU who were involved with the Fake ONNX investigation, and I am now familiar with that investigation. I participated in the RaccoonO365 investigation and therefore, am familiar with that investigation.

13. In Fall 2025, a Microsoft internal security team identified the Tycoon 2FA Defendants as the phishing operation that had the most significant adverse impact on Microsoft customers by volume of attacks. As a result, DCU began investigating Tycoon 2FA. Our investigation revealed that Tycoon 2FA has operated since Fall 2023 (one of the primary domains associated with the operation was purchased in July 2023 and the Telegram channel that Defendants use to connect with potential purchases was launched in October 2023). Since then, Tycoon 2FA has become more active, as its sophisticated, multi-layered redirection features are attractive for cybercriminals, compared to the standard one level of redirection common across other phishing kits. Redirection is the process by which an individual is taken to multiple website URLs before landing on the end domain. While redirection is a normal process, Tycoon 2FA uses it to add an extra layer of security and to prevent detection of their cybercriminal activity.

14. In November 2024, Tycoon 2FA Defendants published a number of videos that provided step-by-step instruction on how the Tycoon 2FA phishing kit operated. Videos such as

the “How To Add Telegram API Key And Chat ID-VEED.mp4” which was published on veed[.]io on November 13, 2024, have led to Tycoon 2FA’s increased popularity with cybercriminals. As other phishing kit operations are taken down or enjoined, phishing kits like Tycoon 2FA fill the void, as they offer similar kits[4] and features to those that are no longer available to cybercriminals.

15. These phishing kits are particularly problematic as they facilitate “adversary-in-the-middle” (“AiTM”) attacks whereby the attacker establishes a permanent presence in a victim’s system with the ability to intercept communications.[5]

16. PhaaS lowers the barrier to entry for cybercrime from a technical skillset perspective, by allowing even novices to launch effective phishing attacks. PhaaS also offers anonymity to the attackers as the service provider (the developer of the Tycoon 2FA-branded kits) handles the technical aspects of the phishing campaigns and advertises these support services as a selling point. Additionally, PhaaS lowers the barrier to entry from a financial perspective as cybercriminals no longer need to expend significant financial resources to develop and scale their infrastructure. This model has proven lucrative, as it enables widespread phishing activities. The ease of use and availability of these services makes it an attractive option for potential cybercriminals. The Tycoon 2FA Defendants’ “phishing operation” provides the gateway and

[4] While Tycoon 2FA kits are similar to other phishing kits, several key differences are that Tycoon 2FA offers a more sophisticated, multi-level redirection, the domains are provided as part of the kit, and purchasers have to use third-party mass mailing tools instead of having it integrated as part of the offering.

[5] The Tycoon 2FA-branded phishing kit allows cyber criminals to infiltrate the systems of Microsoft customers undetected and collect the usernames and passwords of the users of the infiltrated network. This is known as AiTM, which is a form of cyberattack where the malicious actor intercepts communications between two parties without their knowledge. It is particularly common for AiTM attacks to leverage PhaaS platforms given the high volume of phishing emails that these phishing kits make possible. This enables these criminals to then enter the system using these purloined credentials and remain undetected. Microsoft has identified AiTM attacks as one of the Top 5 PhaaS models by volume. 2024 MDDR at 34-35.

know-how for would-be cybercriminals to attack Microsoft customers and steal their personal and confidential business information. For more seasoned cybercriminals, PhaaS kits, such as the Tycoon 2FA kit, allows for low-cost scaling of a small-scale cyber operations into a larger, more widespread operation.

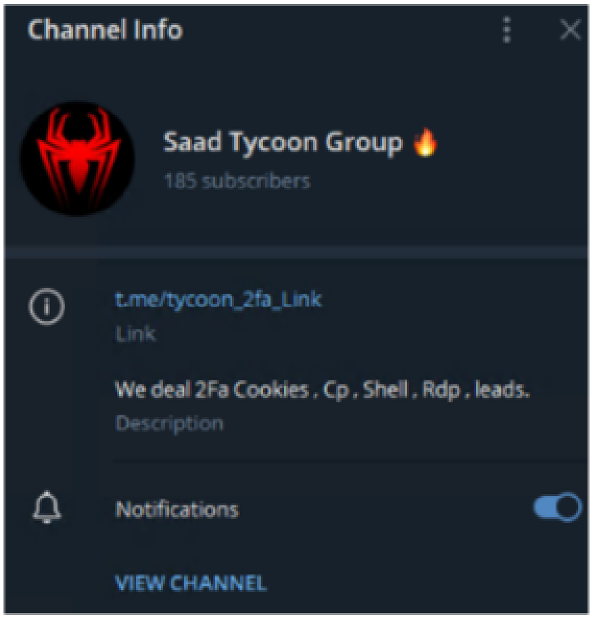
THE TYCOON 2FA DEFENDANTS

17. Tycoon 2FA Defendants are cybercriminals that manufacture and sell Tycoon 2FA phishing kits and provide PhaaS to other cybercriminals. Other downstream cybercriminals purchase the Tycoon 2FA-branded phishing kits from the Tycoon 2FA Defendants and launch phishing attacks against many organizations across various industries. By August 2025, internal Microsoft telemetry revealed that 62 percent of the phishing attacks blocked by Microsoft involved the use of the Tycoon 2FA kit. Tycoon 2FA Defendants boast that their kits include multiple phishing templates (including, for example, Outlook, Excel, 365, SharePoint, Word, Adobe, GoDaddy), multiple distribution methods for the phishing emails (PDF attachments, QR codes, links included in the email), anti-detection features (including antibot detection and IP blocking), reverse proxy through the use of Cloudflare workers' deployment[6], credential/session cookie delivery, and end-user analytics (the ability to track the effectiveness of a particular phishing campaign). Through these offerings, the Tycoon 2FA platform is designed for large-scale credential theft operations.

18. DCU investigated the Tycoon 2FA Defendants and identified Defendant Saad Fridi as an individual involved in the criminal organization. In October 2023, Tycoon 2FA launched their Telegram Channel, titled "Saad Tycoon Group." *See* **Figure 1X**. A Microsoft security

[6] Cloudflare Workers can be used to hide the IP addresses of the actual malicious servers: https://developers.cloudflare.com/workers/

researcher who was able to access the Telegram Channel observed communications from an individual with the username "@SaaadFridi" and a potential customer discussing purchasing a 2FA kit. *See* **Figure 2**.



Saad Tycoon Group 🔥

185 subscribers

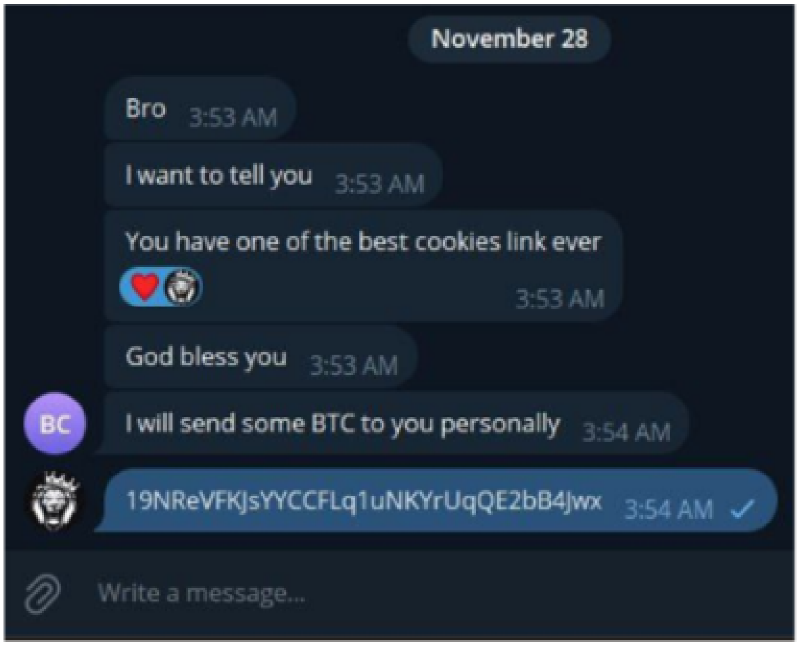
t.me/tycoon_2fa_Link

Link

We deal 2Fa Cookies , Cp , Shell , Rdp , leads.

Description

Figure 1



November 28

Bro 3:53 AM

I want to tell you 3:53 AM

You have one of the best cookies link ever 3:53 AM

God bless you 3:53 AM

BC I will send some BTC to you personally 3:54 AM

19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx 3:54 AM ✓

Figure 2

19. Using this information, we used the username information to observe other posts by the same user, leading us to conclude that he was the operator of the Telegram channel. Additionally, we were able to use the November 2024 Veed videos posted by Tycoon 2FA to obtain further telemetry regarding the identity of the individual responsible for the Tycoon 2FA kit and channel. We then combined open-source intelligence (OSINT) with Microsoft internal telemetry which revealed several emails addresses associated with the same user: saad.fridi110[@]hotmail[.]co[.]uk,saadfridi381[@]outlook[.]com, and saad.fridi381[@]gmail[.]com. This allowed us to determine the identity of Saad Fridi, who is believed to reside in Pakistan. Using other publicly available social media, we were able to further validate Fridi's identity, including through analysis of his cryptocurrency wallets.

20. To support this phishing operation, Tycoon 2FA Defendants established and operated a vast network of internet domains (also known as web addresses), which are used to identify a website and allow users on the internet to access a particular website. Unlike some phishing kits where cybercriminals are required to purchase their own domains to use in connection with their phishing, the Tycoon 2FA kit provides purchasers with pre-registered domains that are embedded in the templates from the control panel. The Tycoon 2FA users choose which domains they want to include in each of their templates that they download from the control panel. Tycoon 2FA users send emails to trick victims into clicking on malicious links in the emails which redirect to a Tycoon 2FA-controlled webpage and then unknowingly provide their credentials to Defendants. The identity of the website domains used by Tycoon 2FA Defendants to support their phishing operation are set forth at **Appendix A** to this Complaint and constitute Tycoon 2FA Defendants' technical infrastructure. Microsoft has identified 330 domains associated with Tycoon 2FA.

21. The remaining identities of the Tycoon 2FA cybercriminal organization are unknown or uncertain because Defendants take great measures to hide their identity. For example, Defendant Fridi allocates a set of domains to each user and users do not have access to the phishing domains of other Tycoon 2FA purchasers. Additionally, the kit offers multi-level redirection (meaning that when a victim clicks on the link they are taken to multiple webpages, including legitimate ones, before landing on the fake login page) and technical countermeasures to thwart security investigators. Nonetheless we have identified specific functions or responsibilities of these individuals who collectively carry out Tycoon 2FA's cybercrime operation.

22. Based on my investigation, I am informed and believe that John Doe 1 provides technical and administrative support for Tycoon 2FA Defendants criminal phishing organization, including facilitating the sale and promotion of the Tycoon 2FA kits.

23. Based on my investigation, I am informed and believe that John Doe 2 provides financial assistance for the Tycoon 2FA Defendants' criminal phishing organization and the technical infrastructure, including managing and facilitating the cryptocurrency payments from the purchase of the Tycoon 2FA phishing kits.

24. Based on my investigation, I am informed and believe that John Doe 3 and John Doe 4 are cybercriminals who purchased and used the Tycoon 2FA phishing kits to carry out phishing attacks. Although the exact number of purchasers is unknown and not ascertainable, given the number of attacks and attempted attacks where the Tycoon 2FA phishing kit was used and the cryptocurrency analysis conducted, I estimate the Tycoon 2FA criminal organization has hundreds if not thousands of members.

25. The Tycoon 2FA Defendants each have specialized roles within the cybercriminal organization. Each Tycoon 2FA Defendant cooperates and colludes in the sale, distribution,

deployment of the phishing kits, the control of the phishing operation, the provision of domains as part of the phishing kit, the provision of technical support to cybercriminal customers, the multi-tier subscription of phishing operation services, circumvention of technical security measures to gain access to victim computers and information, and the unauthorized use and dissemination of Microsoft's intellectual property. Their ongoing association with and reliance on each other's specialized role and contribution allows the Tycoon 2FA Defendants to function as a single unit within a unitary operational structure. Based on my investigation, I conclude this allows the Tycoon 2FA Defendants to scale their operation and increase the profits from their criminal activity. Because the creator, sellers, and distributors of the Tycoon 2FA-branded phishing kits work collectively with the cybercriminal customers, they are able to expand the scope and reach of the Tycoon 2FA Defendants' phishing operation.

<u>TYCOON 2FA DEFENDANTS' MODUS OPERANDI: PHISHING</u>

26. Tycoon 2FA Defendants develop phishing kits for their cybercriminal customers to purchase and use for the customers' cybercrime operations. These customers who purchase the all-in-one, do-it-yourself kits become part of the Tycoon 2FA Defendants' criminal operation when they, in turn, use and deploy the Tycoon 2FA-branding phishing kits to conduct their own cybercrimes directed at Microsoft and its customers. The Tycoon 2FA-branded phishing kits allow the cybercriminal customer to infiltrate the systems of Microsoft customers undetected and steal credentials belonging to users of the infiltrated network through deceit. The cybercriminal customers then use these stolen credentials to access and infiltrate the victim's network. The cybercriminal customers take on what is known as an Attacker in the Middle ("AiTM") role, whereby the cybercriminal customer positions itself between communications directed to and from Microsoft customers. **Figure 3** demonstrates how cybercriminal customers become part of the

Tycoon 2FA Defendants criminal organization as they buy the phishing kit, deploy the kit, and engage in phishing attacks (in collaboration with other, existing Tycoon 2FA Defendants) against a victim.

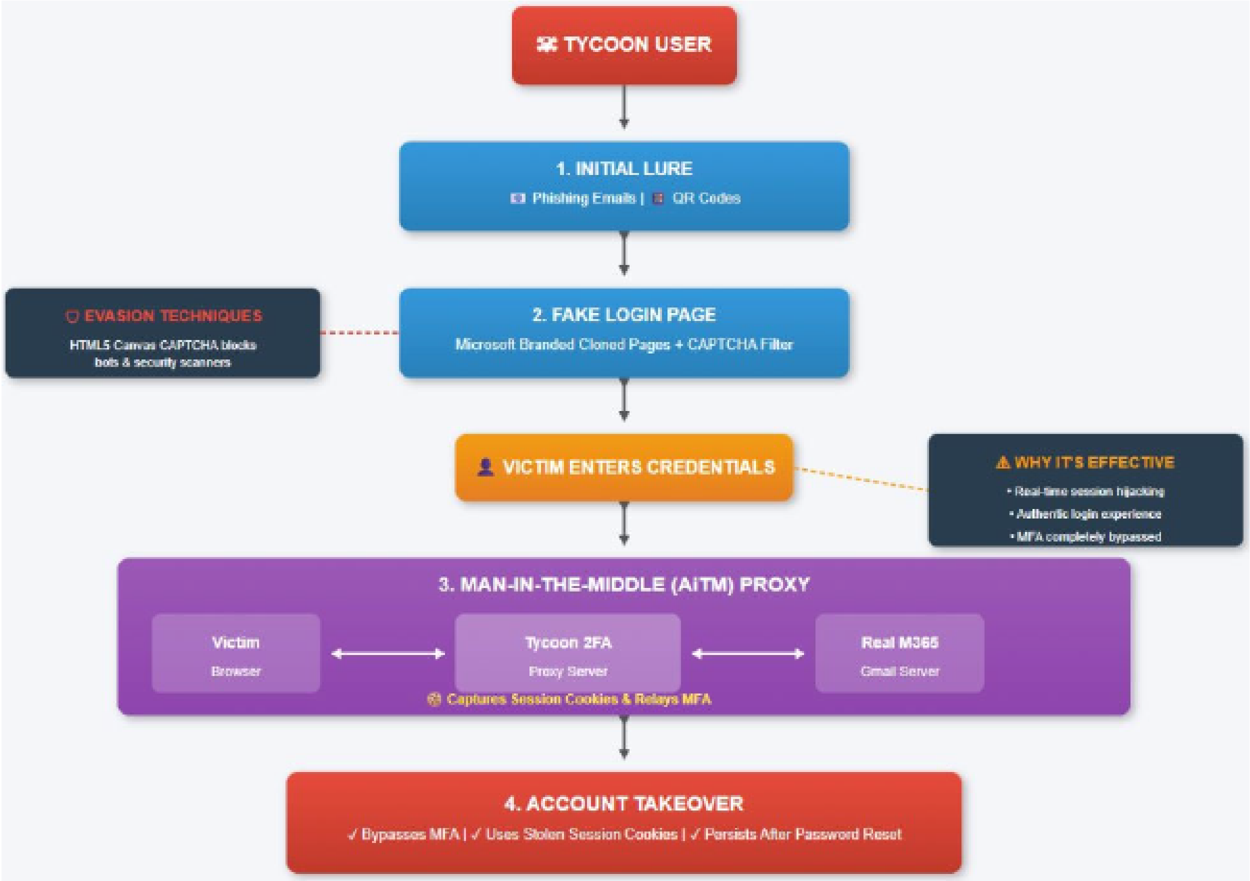

TYCOON USER
1. INITIAL LURE
Phishing Emails | QR Codes
EVASION TECHNIQUES
HTML5 Canvas CAPTCHA blocks bots & security scanners
2. FAKE LOGIN PAGE
Microsoft Branded Cloned Pages + CAPTCHA Filter
VICTIM ENTERS CREDENTIALS
⚠ WHY IT'S EFFECTIVE
• Real-time session hijacking
• Authentic login experience
• MFA completely bypassed
3. MAN-IN-THE-MIDDLE (AiTM) PROXY
Victim
Browser
Tycoon 2FA
Proxy Server
Real M365
Gmail Server
Captures Session Cookies & Relays MFA
4. ACCOUNT TAKEOVER
✓ Bypasses MFA | ✓ Uses Stolen Session Cookies | ✓ Persists After Password Reset

Figure 3[7]

[7] As described in greater detail herein (*see infra* ¶¶ XX), an AiTM attack flow follows the following steps:

1. **Phishing Email (initial lure)**: Attacker sends a phishing email to the victim.
2. **Multiple Redirects leading to fake login page:** When the victim clicks on the link in the email, the domain is redirected 3-4 times before landing on the fake login page. These redirects act as a defensive countermeasure to further avoid detection. On the fake login page the victim enters his or her real Microsoft credentials.
3. **Man-in-the-Middle (AiTM) proxy:** These credentials are relayed to Microsoft's server, which causes a 2FA (two-factor authentication) or MFA (multi-factor authentication)

27. When a phishing victim is deceived to visit a website to enter his or her credentials, Tycoon 2FA Defendants lie in wait to collect those credentials in order to subsequently access his or her accounts to further their cybercrime.

TYCOON 2FA DEFENDANTS ATTACK CHAIN

Step 1: Development and Sale of Tycoon 2FA -Branded Phishing Kits

28. The phishing kits designed, developed, and sold by the Tycoon 2FA Defendants are specifically intended to allow customers a do-it-yourself toolkit to phish Microsoft customers (as well as customers of Adobe, Google, GoDaddy) and use the ill-gotten credentials to infiltrate Microsoft systems. Specifically, these kits are customized using Microsoft logos to mimic the appearance of authentic communications to deceive victims into thinking that the email communication they receive, the files they are directed to open, or links to websites used to enter their personal credentials are authentic and Microsoft-approved. Tycoon 2FA phishing kits are marketed as being able to target Microsoft's product suites, such as Microsoft 365 and Office 365.[8] These malicious phishing kits support credentials theft, information exfiltration, and subsequent

prompt to be issued to the victim. When the victim enters the 2FA/MFA code, the authenticated session cookie is captured by Defendants.

4. **Account Takeover**: Defendants now possess the victim's authenticated session cookie, allowing them to access all Microsoft accounts associated with that credential, without having to do further 2FA/MFA.
5. **Data Exfiltration**: Defendants retrieve harvested credentials from the control panel. Because Defendants have access to the victims' accounts, they can conduct further exploitations (viewing files, downloading documents, changing account settings).

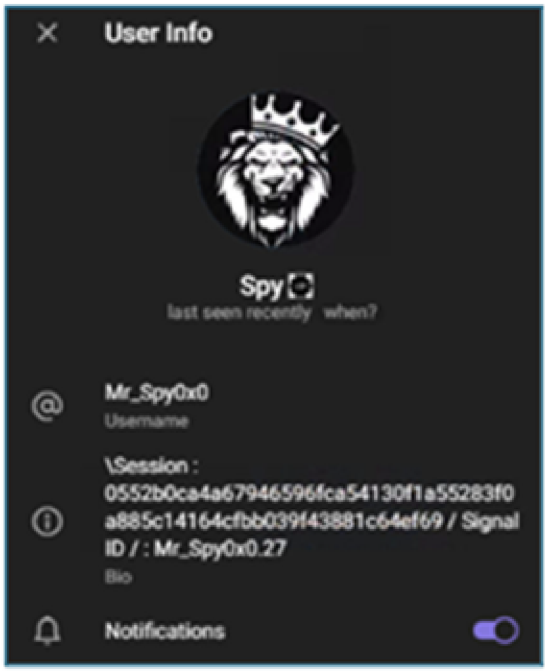
[8] Microsoft 365 and Office 365 are product families of productivity software, collaboration and cloud-based services owned by Microsoft. Microsoft 365 and Office 365 includes Microsoft Office, which is a bundle of productivity applications that contains, among other things: a word processor (Word), a spreadsheet program (Excel), a presentation program (PowerPoint), and an email client (Outlook). Microsoft Azure, or just Azure, is the cloud computing platform developed by Microsoft. It offers management, access and development of applications and services to individuals, companies, and governments through its global infrastructure. These products facilitate the electronic communications of Microsoft's customers.

end-user attacks which include business email compromise, ransomware, and financial fraud. Tycoon 2FA Defendants are able to execute these end-user attacks more readily when they can access a victim's Microsoft's account, which serves as a gateway to other computer applications, and where these applications are connected by a global Microsoft network infrastructure. Indeed, following a successful phish, users of the Tycoon 2FA kit are able to download a text file that they can then use to simultaneously log into all of the victim's Microsoft accounts that share credentials. These are selling points of the phishing kits, and Tycoon 2FA Defendants advertise the kits' abilities to break into Microsoft systems. While the kits are marketed based on their ability to break into Microsoft systems, this is not an instance where the kits are able to successfully exploit any Microsoft defenses or vulnerabilities. Rather, victims are tricked by the phishing to provide their credentials willingly, believing they are interfacing with legitimate Microsoft products allowing the attacker to enter through the front door of the victim's system.

29. The Tycoon 2FA-branded phishing kits are promoted through Telegram Messenger, a secure, cloud-based messaging platform. It is known for its end-to-end encryption. Tycoon 2FA Defendants previously set up Telegram accounts and "channels" (a thread that allows the administrator of the channel to post information to a larger audience) to facilitate private communications between the Tycoon 2FA Defendants and potential customers interested in buying the phishing kits.[9] *See* **Figure 4** for a screenshot of the Telegram profile of Mr._Spy0x0,

[9] In 2024, Sekoia, a security research company published an article which revealed operational details of Tycoon 2FA, *See* Sekoia TDR and Quentin Bourge, Quentin Bourge, *Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit*, Sekoia, available at https://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/#88b42268-54a7-49a0-9ff6-3f3d363c41ea (Mar. 25, 2024). Following that, Defendant Fridi shut down his Telegram channel. Now, Defendant Fridi requires potential purchasers to communicate with him via Telegram direct messages and will not sell his phishing kits unless the potential customer is referred to Defendant Fridi and is vetted through the trusted referral.

which, based on my investigation, is the account associated with Defendant Fridi and responsible for administering the Telegram channel used by the Tycoon 2FA Defendants.



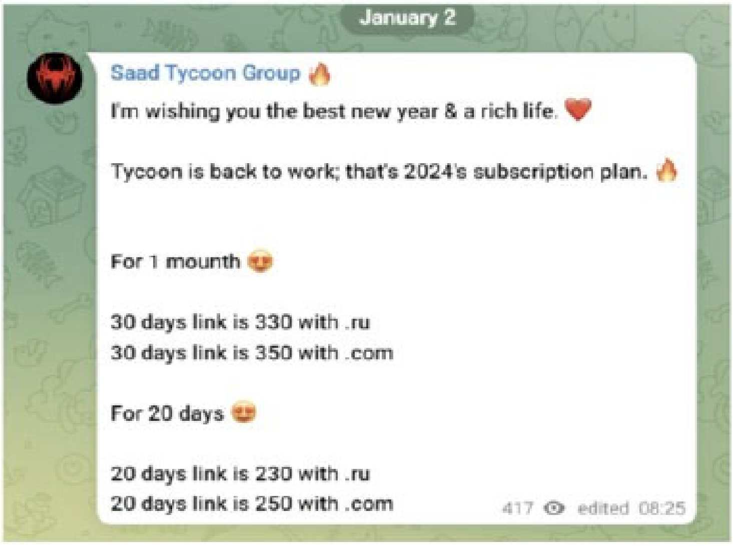
Spy
last seen recently when?

Mr_Spy0x0
Username

\Session : 0552b0ca4a67946596fca54130f1a55283f0 a885c14164cfbb039f43881c64ef69 / Signal ID / : Mr_Spy0x0.27
Bio

Figure 4

30. The phishing kits are offered as a monthly subscription, with different package options ranging in price based on the number and type of domains provided as well as distinct package features, similar to the way the software subscription services offer different-priced subscription tiers. For example, **Figure 5** is a screenshot of a Telegram message offering different plans based on subscription duration and type of domain offered. As shown in the screenshot, Tycoon 2FA Defendants charge more for a kit that includes .com domains (administered by a U.S. based registry) compared to .ru domains (Russia-based domains).



January 2

Saad Tycoon Group 🔥

I'm wishing you the best new year & a rich life. ❤️

Tycoon is back to work; that's 2024's subscription plan. 🔥

For 1 mounth 😍

30 days link is 330 with .ru
30 days link is 350 with .com

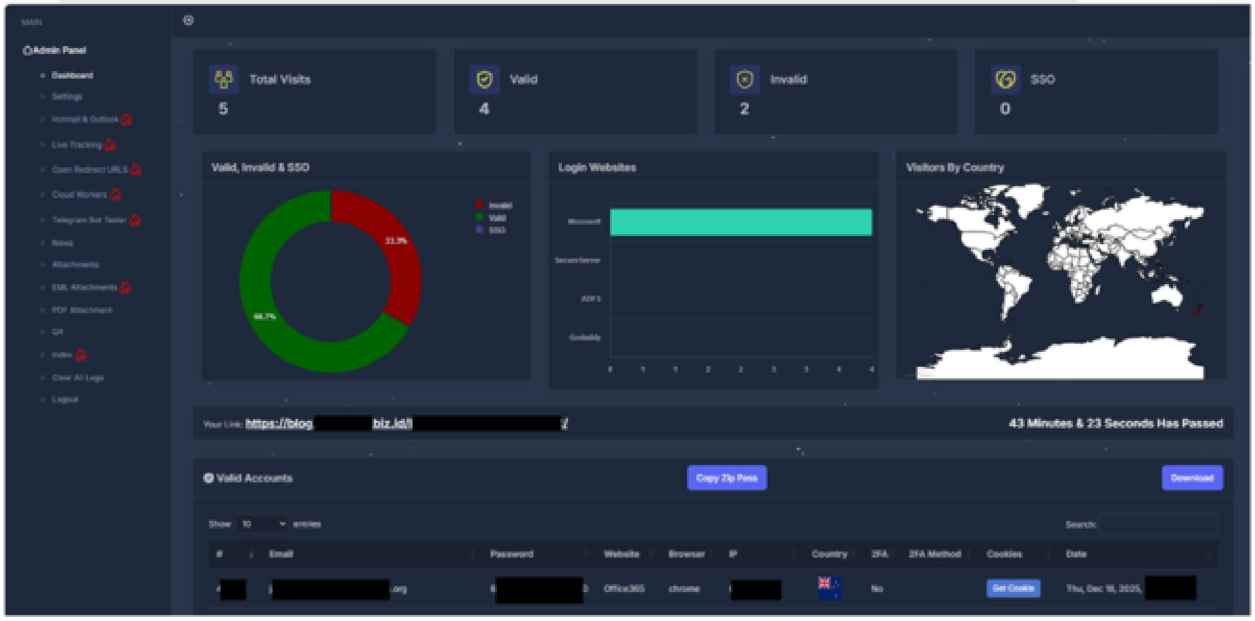
For 20 days 😍

20 days link is 230 with .ru
20 days link is 250 with .com

417 edited 08:25

Figure 5

31. The purchase of a subscription also grants access to the control panel or dashboard. From this dashboard, users can select and customize the pre-configured templates for their phishing campaigns, track recipients of phishing emails, track whether a phishing attack has been successful, track stolen credentials, and measure other metrics that the customer can use to assess the success of its cybercriminal activity. Defendant Fridi and the John Doe Defendants are responsible for the administration of the phishing kits (John Does 1 and 2), manage this dashboard using domains that Microsoft has been able to track back to Defendant Fridi. **Figure 6** is an image of the control panel to which a buyer has access.



Your Link: https://blog.[redacted]biz.id/l[redacted]/

43 Minutes & 23 Seconds Has Passed

Valid Accounts

Show 10 entries

Search:

#	Email	Password	Website	Browser	IP	Country	2FA	2FA Method	Cookies	Date
[redacted]	[redacted].org	[redacted]	Office365	chrome	[redacted]	🇳🇿	No		Get Cookie	Thu, Dec 18, 2025, [redacted]

Figure 6 (Control Panel)

32. The Tycoon 2FA Defendants accept payment via various cryptocurrency including Bitcoin (BTC) and Tether (USDT, a cryptocurrency tied to the United States Dollar), Ethereum, Tron, and LiteCoin. Using cryptocurrency adds a layer of anonymity. Tycoon 2FA Defendants accept payment through multiple cryptocurrencies to broaden its potential customer base.

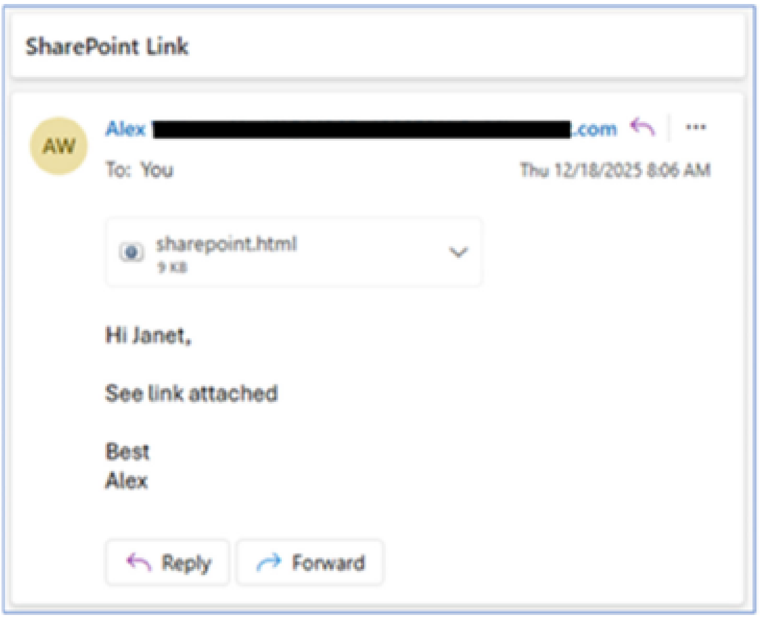
Step Two: Using the Kit to Conduct Phishing Attacks

33. In November 2025, I was involved in a test buy, where DCU purchased a subscription to the Tycoon 2FA phishing kit. Because Defendant Fridi closed his Telegram channel and because Fridi no longer sells to unvetted purchasers, we relied on a security research company that had previously purchased a Tycoon 2FA kit for security research purposes to purchase a subscription to Tycoon 2FA on Microsoft's behalf. For the price of $350, DCU was able to purchase a month subscription to the Tycoon 2FA phishing kit. DCU, via the security research source, which we paid to the cryptocurrency wallet information provided by Defendants. To allow for ongoing investigation, we have renewed the subscription so that DCU could retain access to the infrastructure through the time of filing.

34. Once payment was processed, we were granted access to the control panel, where we were able to customize the template for the phishing email, select the domain to use with the phishing email, and avoid detection by selecting certain countermeasures. Tycoon 2FA Defendants can ensure greater efficacy of their phishing attacks by tailoring the template to the target. For example, the email can emphasize that the attached document requires "urgent" attention. With minimal effort, Tycoon 2FA Defendants can customize the phishing lures to target a myriad of victims across various industries.

35. Following the test buy, DCU conducted a controlled phishing attack against a dummy account controlled by DCU. I thereby gained insight regarding the steps the Tycoon 2FA Defendants take to obscure their identity and conceal their cybercrimes. This also allowed us to see what a phishing victim would experience.

36. To effectuate the dummy purchase, we downloaded the template and sent a phishing email to the dummy account. Then, as the controller of the dummy account, we clicked on the phishing link. We were redirected multiple times before I was taken to a login screen that mimicked a Microsoft login screen. We entered the dummy account's credentials and was taken to a real Microsoft webpage, completing the deception. To the unsuspecting victim, they would not have been able to detect the multi-layered redirection or the technical measures that Tycoon 2FA Defendants have adopted to avoid detection. We then logged back into the control panel and was presented with a text file containing the phished credentials I had just effectively stolen. This allowed us to log into all the Microsoft services and products associated with the phished credentials. This process is captured through **Figures 7-14**.



SharePoint Link

Alex [redacted].com

To: You

Thu 12/18/2025 8:06 AM

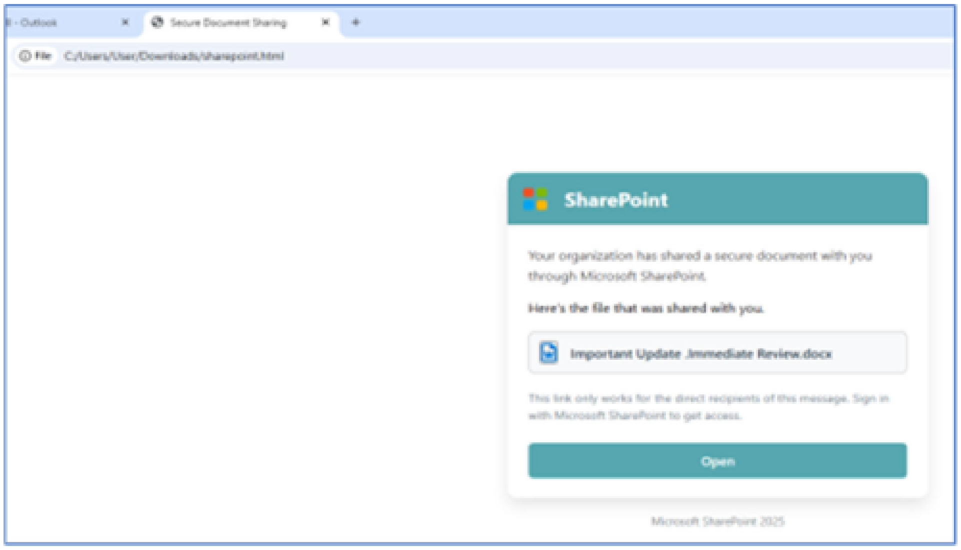
sharepoint.html
9 KB

Hi Janet,

See link attached

Best
Alex

Figure 7



C:/Users/User/Downloads/sharepoint.html

SharePoint

Your organization has shared a secure document with you through Microsoft SharePoint.

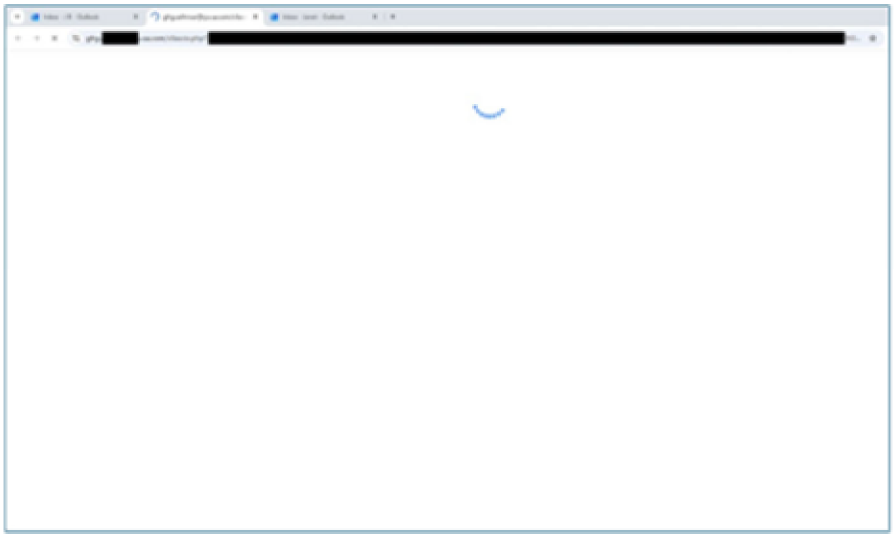
Here's the file that was shared with you.

Important Update .Immediate Review.docx

This link only works for the direct recipients of this message. Sign in with Microsoft SharePoint to get access.

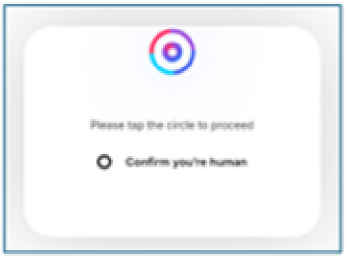
Microsoft SharePoint 2025

Figure 8



[redacted] [redacted]

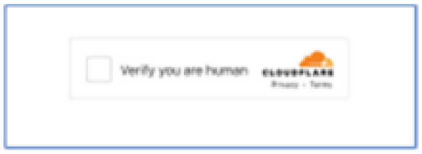
Figure 9



Please tap the circle to proceed

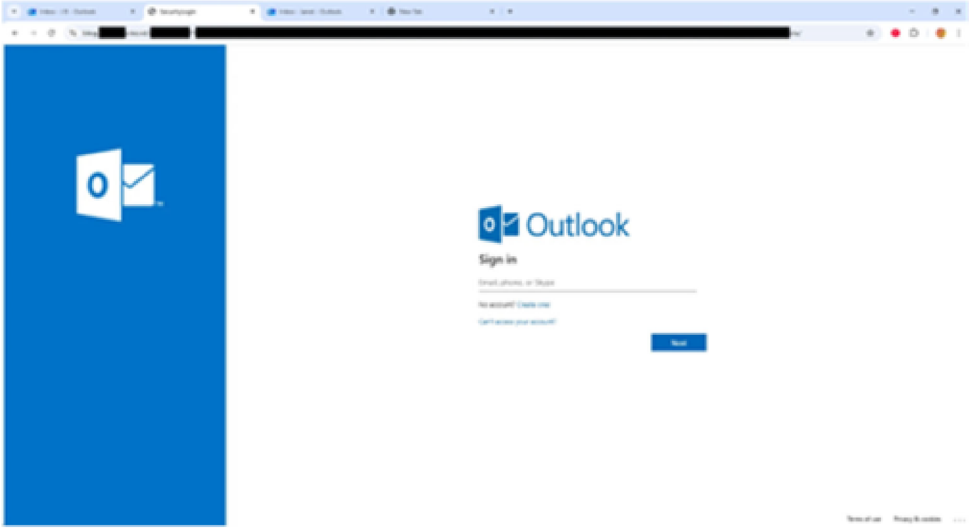
○ Confirm you're human

Figure 10



□ Verify you are human

Figure 11



[redacted] [redacted] [redacted]

Outlook

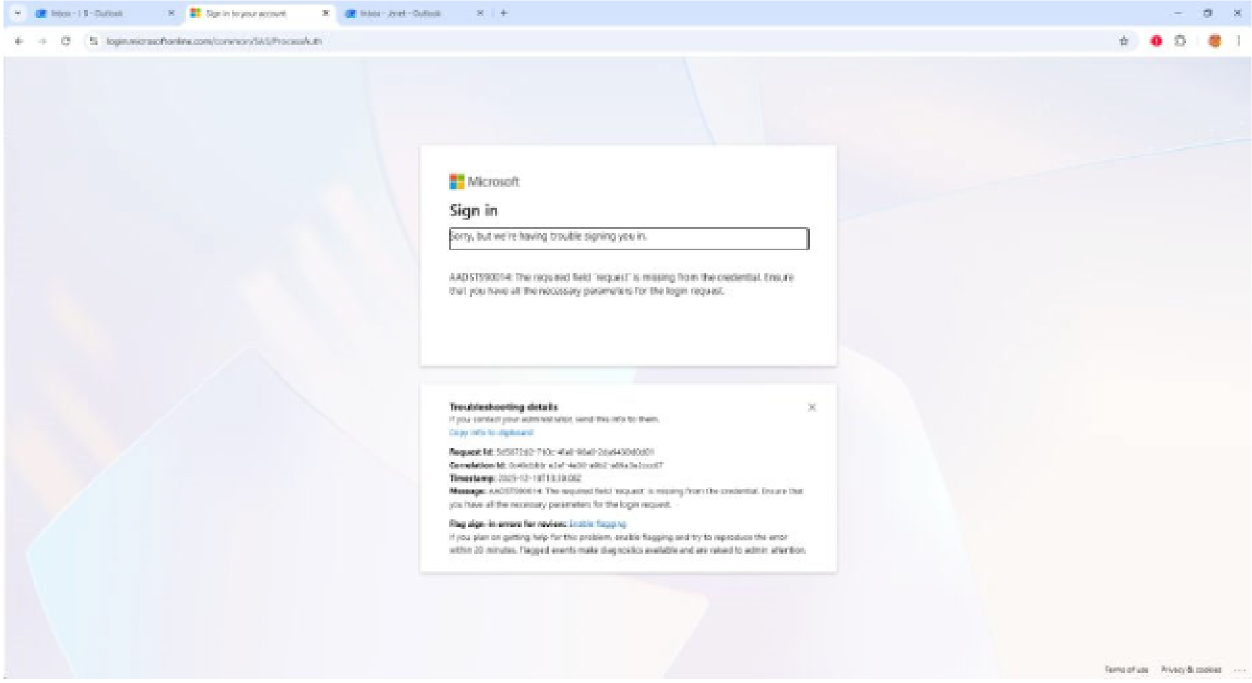
Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Figure 12



login.microsoftonline.com/common/SAS/ProcessAuth

Microsoft

Sign in

Sorry, but we're having trouble signing you in.

AADSTS90014: The required field 'request' is missing from the credential. Ensure that you have all the necessary parameters for the login request.

Troubleshooting details

If you contact your administrator, send this info to them.

Copy info to clipboard

Request Id: [illegible]

Correlation Id: [illegible]

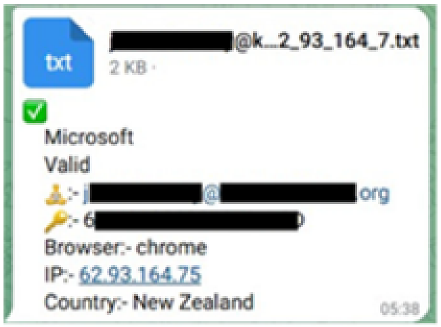
Timestamp: [illegible]

Message: AADSTS90014: The required field 'request' is missing from the credential. Ensure that you have all the necessary parameters for the login request.

Flag sign-in errors for review: Enable flagging

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

Figure 13



[redacted]@k...2_93_164_7.txt
2 KB ·

✅
Microsoft
Valid
🧘:- [redacted]@[redacted].org
🔑:- [redacted]
Browser:- chrome
IP:- 62.93.164.75
Country:- New Zealand
05:38

Figure 14

37. At this point the cybercriminal has access to all of the victim's connected Microsoft accounts and can use this access to commit further cybercrimes, such as information theft, business email compromise, or subsequent malware and ransomware attacks.

38. The Tycoon 2FA Defendants use legitimate Cloudflare infrastructure to further evade detection. Cloudflare is a company that provides legitimate network services and security features to protect websites from various online cyberthreats. The Cloudflare infrastructure hosts the phishing site and powers the redirection of the domains when the victim clicks on the link in the phishing emails.

39. Tycoon 2FA Defendants misuse Cloudflare's services to obscure the location of the phishing infrastructure and to avoid detection by automated security scanning systems that are designed to detect and block phishing websites. Defendants use these Cloudflare services to avoid detection. This enhances the success rate of the phishing attacks and makes it more difficult for the cybercriminal operation to be discovered and shut down. Tycoon 2FA Defendants use two

main Cloudflare services: reverse proxying[10] and a CAPTCHA[11] service to authenticate that a website link is clicked by a human (rather than by an automated process).

(a) *Reverse IP proxying*. Cloudflare provides an IP proxy feature that acts like a middleman to protect the privacy of domain owners. An IP proxy allows its users to have an intermediary to protect the privacy of the domain by shielding it from public view. When used by the Tycoon 2FA Defendants, this prevents security researchers or law enforcement from being able to identify the real IP address associated with the infrastructure. This allows Tycoon 2FA Defendants to hide their location, making it more difficult for their infrastructure to be taken down.

(b) *CAPTCHA*. CAPTCHAs allow a website to discern if it is interacting with a human user rather than a bot. Ordinally, CAPTCHAS are designed to protect consumers; Tycoon 2FA Defendants, however, use a CAPTCHA feature to prevent email security programs that would deploy automated programs (bots) to check if an email has malicious content or links to malicious websites. By using the CAPTCHAS (whether those that are offered as part of the kit or if the Tycoon 2FA user configures a Cloudflare one), Tycoon 2FA Defendants can block security scanning bots from running the scan of the websites controlled by Tycoon 2FA Defendants and exposing them as fraudulent. This prevents the websites controlled by 2FA Defendants from being flagged as "malicious" or "suspicious," which further ensures success of the phishing attack.

ATTRIBUTION TO THE TYCOON 2FA DEFENDANTS

[10] IP proxying is where a proxy server acts as an intermediary between the user and the web server. Proxy servers use a different IP address on behalf of the user, concealing the user's real address from web servers.

[11] CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) has been widely used as a means of protection against bots. It is a type of challenge – response test used to determine whether the user trying to access a website is human in order to deter bot attacks and spam.

40. Microsoft investigated the online infrastructure used in the Tycoon 2FA Defendants' phishing campaign described in this declaration. I determined that Defendants have registered 330 Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. The Tycoon 2FA Defendants registered domains using email addresses by which they communicated with domain registrars to complete the registration process.

41. Cybercriminals, such as the Tycoon 2FA Defendants, are known to hide their identities to evade capture by law enforcement and continue their cybercrime.

42. During the investigation, DCU identified "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Defendants. By identifying these signatures, DCU determined that the domains identified in **Appendix A** belong to and are used by the Tycoon 2FA Defendants. Specifically, we used the following indicators in my assessment: domain registration patterns, phishing URL patterns and components based on known Tycoon 2FA domains, the time period during which the domain was registered, analysis of WHOIS data, indicators from the Microsoft email detonation/protection system, domain resolution patterns, and open-source threat detection rules. Additionally, DCU collaborated with Proofpoint, a leading cybersecurity company that protects organizations by securing email systems and enterprise applications from cyber threats. I was able to use the domain information provided by Proofpoint to validate DCU's investigation and confirm which domains comprise Tycoon 2FA's technical infrastructure.

43. These features when taken together provide a high level of confidence that a given domain is a Tycoon 2FA domain. Each such domain is manually reviewed in detail by one or more subject matter experts at DCU as necessary to ascertain whether it is in fact a Tycoon 2FA

domain. Based on this analysis, we 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 Tycoon 2FA Defendants. At times, other researchers in the security community independently identify Tycoon 2FA domains and associated IP addresses, and these reports may be used to further validate Microsoft's analysis. These high-confidence domains are identified in **Appendix A**.

44. Additionally, we used the cryptocurrency account information provided to me by Tycoon 2FA Defendants to conduct a further financial analysis of the transactions and the cryptocurrency wallets used by Tycoon 2FA Defendants. We conducted this analysis using the information Tycoon 2FA Defendants provided to me, open-source information, and Chainalysis Reactor, a tool that facilitates the tracing of cryptocurrency funds.

45. Chainalysis Reactor groups cryptocurrency addresses that are controlled by the same entity and then ties those clusters to specific real-world entities based on information gleaned from other sources. Those sources amass information regarding cryptocurrency addresses through test transactions, open source-intelligence (OSINT), collecting and verifying evidence from third parties that have conducted transactions with entities on the blockchain, and exchanging information with law enforcement agencies.

46. I was able to conclude that this account (which was provided to me in connection with my purchase of the Tycoon 2FA kit), 1ADgVTV4fnS6WkKHvEprNPEkHnKP79VaUJ, (Bitcoin Network). Over a two-month period between November 3, 2025 and January 4, 2026, there were approximately 120 deposits totalling $28,000 USD into the wallet. DCU observed this account cashing out to the KuCoin wallet 38NN661R2apWs83kHTfG44AV6VVcS8vvRh. Since May 2025, approximately $200,000 have been deposited in the same wallet. Using the $350

subscription fee as a benchmark, this represents between 500-600 subscriptions since May 2025. Given that each subscription allows endless phishing during the month-long terms, this cryptocurrency analysis demonstrates the widespread attack potential. Additionally, based on my investigation, I identified other cryptocurrency accounts associated with Defendant Fridi, suggesting that he has diversified his wallets to avoid detection. Using this information as well as information that Fridi self-published about cryptocurrency wallets he purportedly owned, I was able to track payments to Fridi dating back to the outset of his Tycoon 2FA operation. This has allowed me to observe his cryptocurrency activity and track the growth of Tycoon 2FA's operation.

DEFENDANTS TARGET VICTIMS LOCATED IN NEW YORK

47. The Tycoon 2FA Defendants have targeted numerous healthcare organizations and companies in the education sector. As shown in the heatmap (**Figure 15**), a significant portion of this activity is directed at New York-based organizations and individuals. Specifically, at least 623 Microsoft customers located in the State of New York were successfully phished by Defendants using the Tycoon 2FA phishing kit (a successful phish means that individuals of the customer entity provided credentials to Defendants after receiving a phishing email).[12] Of these 623 New York customers, 596 are located within the Southern District of New York. *See* **Figure 16.** Furthermore, of the 92 co-Plaintiff Health-ISAC organizations that were successfully phished by Defendants, 2 are in the SDNY.

[12] Microsoft collaborated with SpyCloud, a leading identity threat protection company that provided this victim data in the form of phished credentials attributed to Tycoon 2FA. Once Microsoft completed the test purchase and conducted a dummy phish, we were able to observe what a Tycoon 2FA harvested credential looked like. We matched this with the SpyCloud data and were able to confirm which of the harvested credentials matched the Tycoon 2FA format. This allowed us to ascertain the total number of victims located in the United State and in New York.

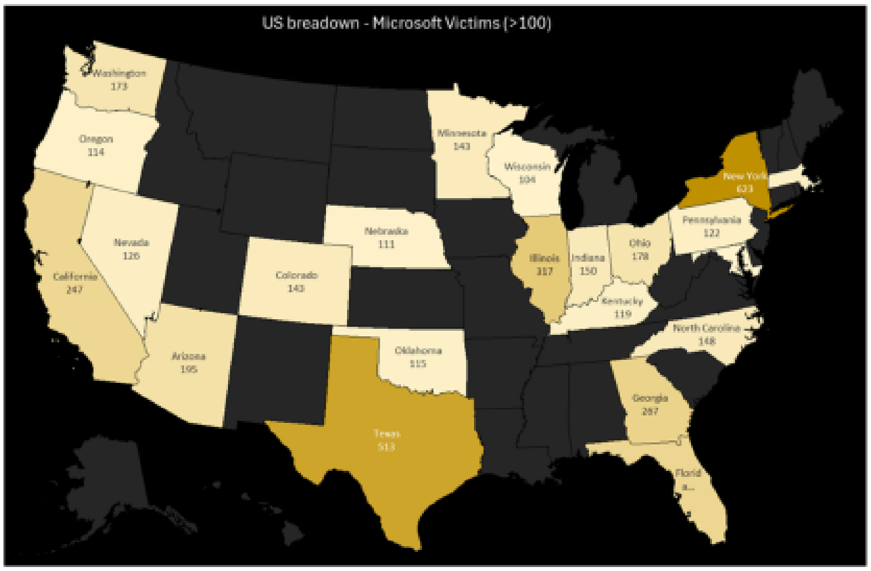


Figure 15

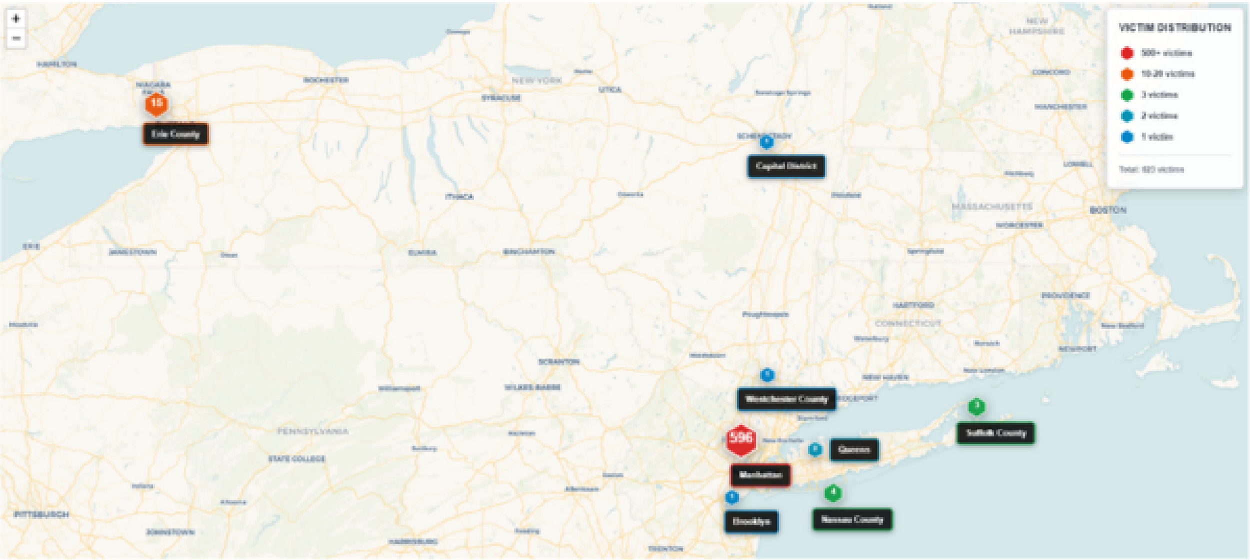


FIGURE 16

48. Since 2023, Tycoon 2FA Defendants have been responsible at least 96,000 individual, successfully phished credentials globally and at least 55,000 credentials in the United States (this number is not limited to Microsoft customers and represents instances where a victim was phished using the Tycoon 2FA phishing kit and were deceived to provide login credentials). 87% of the credentials phished are for enterprise accounts (e.g., employee work emails).

49. Most of Defendants' victims are entities that operate in the healthcare, real estate, financial, banking, and education sectors, targeting American companies across crucial, data-rich sectors. *See* **Figure 17** (sector breakdown of victims).

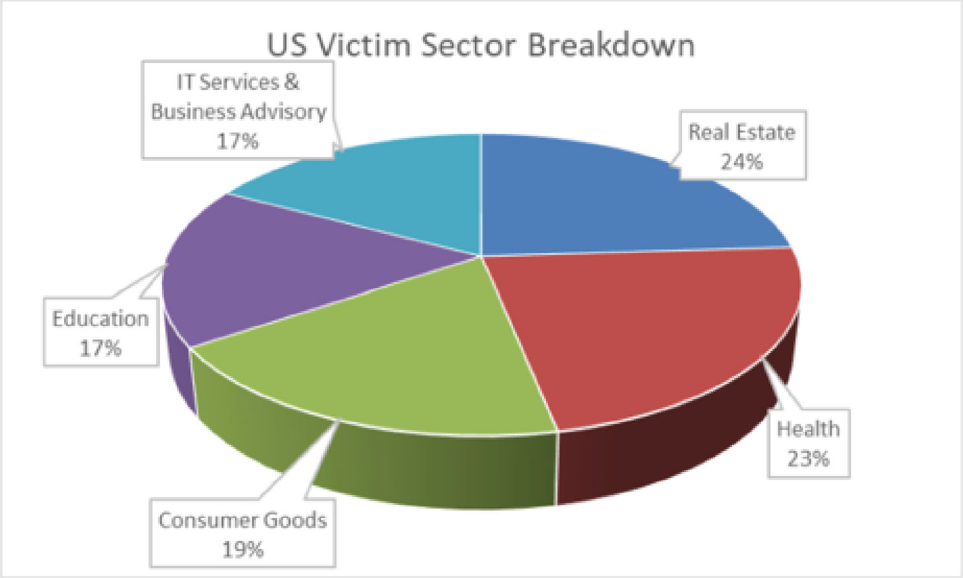


FIGURE 17

HARM TO MICROSOFT AND ITS CUSTOMERS

50. Tycoon 2FA Defendants targeted Microsoft, its customers, and the public to advance their financially motivated cybercrimes. The Tycoon 2FA Defendants have caused and continue to cause irreparable injury to Microsoft, its customers, and the public. The Tycoon 2FA Defendants' activities irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill.

51. The Tycoon 2FA Defendants' criminal acts directly harm Microsoft's reputation and goodwill it has obtained through its extensive branding efforts.

52. Tycoon 2FA-branded phishing kits are customized using Microsoft logos to mimic the appearance of authentic communications to deceive victims into thinking the email communication they receive, the files they are directed to open, or links to websites used to enter

their personal credentials are authentic and Microsoft-approved. Thus, each time a phishing kit is sold, it is done with the express purpose of hacking into Microsoft's products and systems that Microsoft has expended significant resources to build and protect.

53. Tycoon 2FA Defendants use Microsoft systems and programs, such as Outlook, Microsoft 365, and Office 365 to further deceive victims. Because the login pages that Tycoon 2FA Defendants use include the Microsoft name and logo, the victim will be completely unaware of the threat and will believe that the link is to a legitimate Microsoft webpage and therefore trustworthy when in fact it is malicious. In doing so, Tycoon 2FA Defendants exploit brand recognition Microsoft has cultivated and trust Microsoft has built with its customers.

54. Customers expect certain quality from Microsoft. To that end, Microsoft places restrictions on how its branding can be used. When "Microsoft" systems and products are used in connection with cybercrime, customers will mistakenly believe Microsoft is responsible for the attack. Customers subjected to the negative effects of Defendants' phishing attacks sometimes incorrectly believe Microsoft is the source of the problem and thus will 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. If a customer leaves Microsoft due to improperly blaming Microsoft for a phishing attack or believes that Microsoft's systems and products are not secure (because customers are unaware of Tycoon 2FA Defendants' deception), it may be costly or impossible to convince the customer to return to Microsoft. Additionally, because a successful phishing attack can be the precursor to other cybercriminal attacks, an organization that is later subject to a malware or ransomware attack that occurred because the cybercriminal gained network access through the phishing may incorrectly blame Microsoft for these attacks.

55. Microsoft has invested significant resources in excess of $5,000 to address and attempt to remediate the harm caused by Tycoon 2FA Defendants' crimes. Specifically, Microsoft has spent at least $925,000 and over 5,000 investigative hours investigating the Tycoon 2FA Defendants and their infrastructure.

DISRUPTING TYCOON 2FA'S ILLEGAL ACTIVITY

56. The Defendants' internet domains, used to execute their phishing campaigns, are the most vulnerable part of their operational infrastructure. These domains are attached as **Appendix A** to my declaration. These domains have been used in phishing emails directed at users of Microsoft's email services and enterprise platforms.

57. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers and thereby cut off the way the Tycoon 2FA Defendants phish and collect sensitive personal and business information from victims. In other words, any time a user clicks on a link in a phishing email and provides his or her username and password, that information will no longer be captured by Tycoon 2FA Defendants because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of the Tycoon 2FA Defendants.

58. Redirecting these Tycoon 2FA domains will directly disrupt Defendants' 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.

59. I believe the most effective way to suspend the injury caused to Microsoft, its customers, including Health-ISAC and the public, is to take the steps described in the Proposed Order. This relief will significantly hinder the Tycoon 2FA 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 Tycoon 2FA's malicious activities.

60. The Tycoon 2FA Defendants' techniques are designed to avoid technical mitigation efforts, eliminating the ability to curb the injury purely through technical means. For example, once domains in the Tycoon 2FA 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.

61. For this reason, providing notice to the Tycoon 2FA Defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Tycoon 2FA 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.

62. In my experience, if Tycoon 2FA Defendants were to learn of Microsoft's impending action and request for relief, Defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure.

63. 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.

64. For all of these reasons I believe the only way to mitigate injury and disrupt the most recent, active Tycoon 2FA infrastructure is to redirect the domains at issue to Microsoft prior to providing notice to the Defendants.

I declare under penalty of perjury under the laws of the United States that the forgoing is true and correct to the best of my knowledge.

Executed February 24, 2026 in New York, New York.

Derek Richardson
Investigator, Digital Crimes Unit
Microsoft Corporation