UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington State Corporation, Plaintiff, v. John Doe 1, John Doe 2, a/k/a SamCodeSign, a/k/a "Fox Tempest," and John Does 3–4, a/k/a "Vanilla Tempest," Defendants.	Civil Action No. **FILED UNDER SEAL**

COMPLAINT

Plaintiff Microsoft Corporation ("Microsoft"), by its attorneys, brings this action against John Does 1–2 (collectively "Fox Tempest Defendants") and John Does 3–4 (collectively "Vanilla Tempest Defendants," and together with the Fox Tempest Defendants, "Defendants"). Defendants engage in a fraudulent scheme to obtain and use code signing certificates to deceive victims into downloading dangerous malware under the false belief that it is trusted software. Through this scheme, Defendants steal sensitive information from and perpetrate ransomware attacks against Microsoft's customers and the public at large. Microsoft asserts claims based on (i) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)–(d); (ii) the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(6) & 1030(b); (iii) the Lanham Act, §§ 1114(1), 1125(a), & 1125(c); (iv) breach of contract; (v) common law trespass to chattels; and (vi) unjust enrichment.

Microsoft alleges as follows:

NATURE OF THE ACTION

1. Code signing is intended to serve as a critical trust mechanism in modern computing environments, providing cryptographic verification of both the origin and the integrity of software so that users and operating systems may reliably distinguish legitimate programs from malicious ones. With increasing frequency, however, sophisticated threat actors have subverted this very mechanism, obtaining or misusing valid signing certificates to mask dangerous malware as trusted software. This abuse is not limited to an isolated occurrence affecting a single entity; rather, it is a pervasive, industry-wide threat that has impacted the most sophisticated and security-conscious enterprises.

2. The exploitation of code signing infrastructure to disguise malware as trustworthy software is neither a recent development nor an isolated occurrence. Over the past decade, it has grown into a systemic problem affecting every part of the global software supply chain, evolving in both scale and sophistication as malicious cyber actors have refined their methods to circumvent robust defenses implemented by software companies. Researchers have documented both the prevalence of digitally signed malware and a fundamental shift in the underlying threat landscape—from stealing private keys from software vendors to directly procuring new certificates from certificate authorities under false or impersonated identities.[1]

3. Both organized criminal groups and state-sponsored actors have engaged in this practice on an industrial scale, using fraudulently obtained certificates to sign ransomware,

[1] *See* Kristián Kozák et al., *Issued for Abuse: Measuring the Underground Trade in Code Signing Certificates*, Proc. 17th Workshop on Econ. Info. Sec. 14 (2018), https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/06/WEIS_2018_paper_14.pdf; Aaron Walton, *Code-signing certificate abuse in the Black Basta chat leaks (and how to fight back)*, Expel (Mar. 18, 2025), https://expel.com/blog/code-signing-certificate-abuse-in-the-black-basta-chat-leaks-and-how-to-fight-back/.

infostealers, backdoors, and post-exploitation tools used to target individuals, enterprises, and government institutions.[2] These malicious binaries ultimately reach their victims through distribution mechanisms such as malicious advertising, search engine optimization poisoning, and trojanized installers hosted on fake download sites.[3] Fueled by a mature and organized underground market in which code signing certificates are bought, sold, and replenished as criminal commodities, these incidents reflect a pervasive, industry-wide problem that has undermined the public-key infrastructure on which modern computing depends. The conduct at issue in this action exemplifies and exacerbates this deliberate and ongoing pattern of code signing abuse.

4. To combat this escalating threat and to hold accountable those who perpetuate it, Microsoft brings this action against Defendants who, along with others not named as defendants, are members of an organized criminal enterprise (hereinafter the "Certificate Abuse Enterprise") that has systematically exploited Microsoft's code signing technology to facilitate their unlawful conduct, causing substantial and far-reaching harm to Microsoft, its customers, and the public.

5. To carry out their Certificate Abuse Enterprise, Fox Tempest Defendants have exploited Microsoft's Artifact Signing service to fraudulently obtain code signing certificates and sell them to Vanilla Tempest Defendants. Vanilla Tempest Defendants then disguise dangerous malware, including ransomware loaders and information-stealing programs, as legitimate software

[2] *See, e.g.*, Walton, s*upra*, note 1; Rob Wright, *Iranian State Hackers Use SSL.com Certificates to Sign Malware*, Dark Reading (Sept. 26, 2025), https://www.darkreading.com/vulnerabilities-threats/iranian-hackers-ssl-certificates-sign-malware.

[3] *See, e.g.*, Walton, s*upra*, note 1 (documenting delivery of code-signed malware through malicious advertisements impersonating the messaging application Slack); AhnLab Security Emergency Response Center, *Infostealer with Abnormal Certificate Being Distributed* (Sept. 26, 2023), https://asec.ahnlab.com/en/57553/ (documenting distribution of LummaC2 and RecordBreaker infostealers through SEO-poisoned pages); Brian Donohue & Jason Killam, *Certified evil: Investigating signed malicious binaries*, Red Canary (July 31, 2024) https://redcanary.com/blog/threat-detection/code-signing-certificates/ (analyzing a code-signed loader masquerading as a Microsoft Teams installer delivered from a non-Microsoft domain).

by signing the malware with these certificates that brand the software as trusted by Microsoft, packaging it to appear as legitimate Microsoft products, and employing malicious advertising campaigns and search engine optimization poisoning techniques. These efforts trick victims into downloading the malware onto their devices, allowing Vanilla Tempest Defendants to steal their information, deploy ransomware, and extort them for financial gain.

6. Microsoft released Artifact Signing in November 2024. Microsoft's investigation has found that since May 2025, Fox Tempest Defendants have created more than 580 fraudulent Microsoft tenants to obtain access to Microsoft's Artifact Signing service, a managed code signing solution used by software developers.[4] Vanilla Tempest Defendants and other cybercriminals have used the fraudulently obtained certificates from Fox Tempest Defendants to impact thousands of customer machines in the United States.

7. The Certificate Abuse Enterprise has financially benefited from their criminal scheme: Fox Tempest Defendants through the sale of fraudulently obtained code signing certificates and Vanilla Tempest Defendants through ransomware attacks, data theft, and extortion campaigns launched with the assistance of malware signed by such certificates. Microsoft confirmed this scheme through two test purchases in which a cooperating source joined a Telegram group chat operated by John Doe 2, completed a Google Form to select a code signing service, corresponded with John Doe 2 about the service, and paid John Doe 2 in Bitcoin. Following the payment, John Doe 2 provided credentials and instructions to access a virtual machine, where a Microsoft investigator successfully signed test software with a certificate controlled by Fox Tempest Defendants.

[4] A Microsoft "tenant" refers to a dedicated cloud environment in which user accounts, data, and applications can be centrally managed.

8. Defendants' conduct has caused and will continue to cause substantial, irreparable injury to Microsoft, its customers, and the public. Microsoft seeks injunctive relief and other equitable relief and damages against Defendants.

PARTIES

9. Microsoft is a corporation duly organized under the laws of the state of Washington, with its headquarters and principal place of business in Redmond, Washington. Microsoft's Digital Crimes Unit ("DCU") is the Microsoft division responsible for protecting Microsoft and its customers against cybercrime threats. DCU is an international team of technical, legal, and business experts that have been fighting cybercrime, protecting individuals and organizations, and safeguarding the integrity of Microsoft services since 2008.[5] One of DCU's responsibilities is to investigate cybersecurity threats and identify and attribute attacks, as it has done here with the Defendants. DCU also collaborates with MSTIC, the Microsoft Threat Intelligence Center, which is comprised of thousands of world-class experts, security researchers, analysts, and threat hunters. MSTIC publishes a threat intelligence blog alerting customers and the public of cybersecurity threats.

10. Defendant John Doe 1 is a cybercriminal who obtains unauthorized access to Microsoft's Artifact Signing service through fraudulent means to acquire code signing certificates. Upon information and belief, John Doe 1 owns and operates Fox Tempest Defendants' infrastructure specifically designed and used for the purpose of providing fraudulently obtained code signing certificates to other malicious cyber actors.

[5] *See* Steven Masada*, Defending the Gates: How a Global Coalition Disrupted Tycoon 2FA, a Major Driver of Initial Access and Large-Scale Online Impersonation*, Microsoft (Mar. 4, 2026), https://blogs.microsoft.com/on-the-issues/2026/03/04/how-a-global-coalition-disrupted-tycoon; Steven Masada, *Disrupting Lumma Stealer: Microsoft Leads Global Action Against Favored Cybercrime Tool*, Microsoft (May 21, 2025), https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/.

11. Defendant John Doe 2, also known by the alias "SamCodeSign," is a cybercriminal who communicates with other malicious cyber actors, including Vanilla Tempest Defendants, to market and sell access to fraudulently obtained code signing certificates on behalf of Fox Tempest Defendants. John Doe 2 solicits and collects payments from Vanilla Tempest Defendants and other malicious cyber actors in exchange for such certificates.

12. Upon information and belief, Defendants John Doe 3 and John Doe 4 are cybercriminals that Microsoft tracks under the designation "Vanilla Tempest" and are also known as "VICE SPIDER" and "Vice Society," who have purchased fraudulently obtained code signing certificates from Fox Tempest Defendants and used those certificates to digitally sign malware. Using the certificates and Microsoft's branding without authorization, John Does 3 and 4 have disguised the malware as legitimate, trustworthy software, including representing the malware as Microsoft products, to more easily deploy the malware onto the computers of unsuspecting victims without their consent. Through the foregoing conduct, John Does 3 and 4 have unlawfully accessed victims' computers and devices, exfiltrated and stolen the personal and confidential information of victims, deployed ransomware designed to encrypt victims' files and systems, and extorted victims by demanding payment in exchange for restoring access to, or suppressing, their data. This criminal activity is ongoing and continues to cause irreparable harm to Microsoft and its customers.

13. Based on its investigation of the foregoing conduct, including its test purchase of the code signing services, Microsoft alleges that Defendants are responsible for the conduct alleged here and that Microsoft's injuries were proximately caused by Defendants. Microsoft will endeavor to amend this Complaint to allege Defendants' true names and capacities when and if ascertained. [redacted]

Microsoft will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

14. Upon information and belief, the actions and omissions alleged to have been committed by John Does 1–4 were actions and omissions that each of them authorized, controlled, directed, or had the ability to authorize, control, or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, and aided and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

15. Third-party GoDaddy.com LLC ("GoDaddy") is the domain name registrar that registered the domain used by Fox Tempest Defendants to operate their illicit code signing service and is based in the United States.

16. Third-party RouterHosting LLC (d/b/a "Cloudzy") is the host of virtual machines located in the United States that are used by Fox Tempest Defendants to operate their illicit code signing service and is headquartered in Dubai, United Arab Emirates.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, because this action arises out of Defendants' violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has supplemental subject

matter jurisdiction over Microsoft's claims for breach of contract, trespass to chattels, and unjust enrichment pursuant to 28 U.S.C. § 1367.

18. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b), because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district.

19. Venue is also proper in this Court under 28 U.S.C. § 1391(c), because Defendants are subject to personal jurisdiction in the Southern District of New York. Defendants engage in conduct availing themselves of the privilege of conducting business in the State of New York, and use instrumentalities located in the State of New York and the Southern District of New York to carry out acts alleged herein. Defendants direct a significant amount of their cybercriminal activity to New York organizations and individuals. Specifically, more than 10,000 customer machines compromised by Defendants' malware are located in the State of New York. Of these New York machines, more than 4,000 are located within the Southern District of New York.

FACTUAL BACKGROUND

Microsoft's Services and Reputation

20. Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software and hardware systems to individuals, businesses, and governments. Microsoft is the provider of the Windows® computer operating system, and a variety of other software and services including Microsoft 365®, OneDrive®, and Azure®. Microsoft has invested substantial resources in developing high-quality, effective, and trusted 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

is one of the most well-known and trusted names in computing. The Microsoft brand enjoys extraordinary recognition and fame among consumers and it represents significant goodwill that has been established through decades of use in the United States and globally. Microsoft has registered hundreds of trademarks with the United States Patent and Trademark Office—including the Microsoft®, Windows®, Microsoft 365®, Microsoft Teams®, and Azure®—to help Microsoft safeguard its brands and their associated goodwill. Copies of the trademark registration for these trademarks are available as **Appendix A** to this Complaint.

21. Since late 2024, Microsoft has offered a cloud-based software service known as "Artifact Signing," a fully managed, end-to-end code signing service for developers, which is integrated with Microsoft's Azure cloud computing platform. Code signing is a method used to secure software applications against tampering and identity falsification. Digital signatures generated through code signing verify that the underlying code has not been modified and identify the entity that signed the application through the associated code signing certificate. Artifact Signing utilizes digest signing, a standard practice of certificate authorities to secure software distribution, whereby only a cryptographic hash of the file is transmitted to the service, not the file itself. As a result, the service cannot inspect the underlying code prior to signing.

22. Certificates obtained through Microsoft's Artifact Signing service display the Microsoft® trademark and identify Microsoft as the issuing certificate authority when an end user of the software signed by such certificates views the software's properties.

23. Software that carries a valid digital signature, such as a signature from an Artifact Signing certificate, is treated by the Windows operating system as authenticated and trustworthy. Specifically, a valid digital signature permits software to satisfy the security mechanisms that the operating system would otherwise present to the user of the device, including Microsoft's

SmartScreen filter and User Account Control ("UAC") components. These mechanisms are designed to warn users before they install or execute software from unverified or unknown sources. When a valid digital signature is present, however, the operating system suppresses these warnings.

24. This dynamic is further strengthened specifically in Windows 11, which introduces Smart App Control ("SAC"), a security feature that applies a default-deny approach to application execution. Unlike traditional warnings that a user may choose to disregard, SAC is designed to block unsigned or low-reputation software entirely, preventing its execution regardless of the user's intent. A valid digital signature is a prerequisite for the software to receive authorization to download at all.

25. Artifact Signing streamlines the code signing process for legitimate pre-vetted users by automating certificate management, providing security for certificate and key storage, and integrating with developer tools and pipelines. The service handles the creation, protection, and automatic rotation of code signing certificates on behalf of its users. These certificates are stored and protected within hardware modules that meet FIPS 140-2 Level 3 standards, and the certificates themselves are renewed daily and valid for only 72 hours to reduce the impact of signing misuse and abuse.[6]

26. To use Artifact Signing, a user must first sign up for an Azure subscription and tenant. Users may obtain an Azure subscription through Microsoft's standard onboarding process or, alternatively, through a process offered by partnering domain registrars, which creates a Microsoft Entra ID tenant and allows the user to obtain an Azure subscription under that tenant.

[6] *See* Microsoft, *Artifact Signing*, Microsoft Azure, https://azure.microsoft.com/en-us/products/artifact-signing (last visited Apr. 27, 2026); Microsoft, *Artifact Signing Certificate Management*, Microsoft Learn (last updated Jan. 8, 2026), https://learn.microsoft.com/en-us/azure/artifact-signing/concept-certificate-management.

After obtaining an Azure subscription, the user can set up and run the service through the Azure Portal. The process begins with registering the Artifact Signing resource provider, which enables signing functionality within the user's Azure tenant. The user then creates a signing account, the logical container for managing identity validations and certificate profiles. Then, the user can create certificate profiles to manage the certificates used for code signing.

27. However, before a user may request or issue any code signing certificates, the user must complete a mandatory entity and identity validation process. As part of this process, Microsoft leverages a set of internal entity and identity validation systems and processes that aim to prevent untrustworthy parties, including malicious cyber actors, such as Defendants, from using Microsoft products and services. During this process, Microsoft requires the user to provide information such as the entity's legal name, registered business address, primary contact's first and last name, domain name, company website, street address, city, ZIP or postal code, and contact email addresses. Microsoft's entity verification system screens applicants across a myriad of sources to validate their identity and indicia of trustworthiness, including by verifying that the organization's name and address match official business registration records and confirm ownership of the user's domain and email address. To perform these validations, Microsoft also leverages internal datasets, threat and fraud indicators, partnerships with subject-matter experts, and third-party analysis. For individual identity verification, Microsoft's verification system integrates with a third-party company that provides the capabilities necessary to confirm the authenticity of the provided government-issued identification.

28. All users of the Artifact Signing service are bound by Microsoft's Terms of Use for Artifact Signing ("Terms of Use"), a contract that governs access to and use of the service. A copy of the Terms of Use is available as **Exhibit 1** to this Complaint.

29. Under the Terms of Use, users make a series of representations and warranties to Microsoft and to any party who may rely on a certificate issued to them. Users represent and warrant the following, among other things:

- "[A]ll the Submitted Information and all representations [user] makes to Microsoft in any Services[7] applications are accurate."
- "[User] will inform Microsoft if the Submitted Information or the representations it made to Microsoft in any Services application changed or is no longer valid."
- "[T]he Submitted Information (including the email address of [user's] personnel who submitted such information, if applicable) has not been and will not be used for any unlawful purpose."
- "[User] will use the Services exclusively for authorized and legal purposes consistent with this [Terms of Use]."

30. Additionally, the Terms of Use require the user to "immediately investigate" any incident that could "reasonably compromise the trust status of the Services" and submit a report to Microsoft with the causes of the incident and proposed cures. The user is also obligated to "respond to all reports of malicious activity (including viruses, Phishing, Malware, Potentially Unwanted Applications, instances of fraud, or otherwise inaccurate information provided in acquisition of any signature, and applications and activities that, regardless of intent, cause harm to the Services or any related platforms or technologies or to Microsoft's assets or reputation[])]."

31. Users must agree to use Artifact Signing in accordance with the Code of Conduct, which includes the following:

[7] The "Services" refer to Artifact Signing.

- "[User] may not use the Services to (or to assist any third party to): (i) do anything illegal; (ii) engage in any activity that exploits, harms, or threatens to harm anyone; (iii) help others send unsolicited bulk email, postings, or instant messages; (iv) publicly display inappropriate images; (v) engage in false or misleading activity; (vi) engage in activity that harms the Services or others; (vii) infringe on or misappropriate the rights of others …."

32. The Terms of Use further require users to defend, indemnify, and hold Microsoft harmless from any claims that, if true as alleged, would reflect a breach of the Terms of Use or that relate in any way to the subscriber's use of the service.

Fox Tempest Defendants' Abuse of Artifact Signing

33. Starting in May 2025, Fox Tempest Defendants have operated an illicit code signing service for Vanilla Tempest Defendants and other cybercriminals. By selling access to code signing certificates fraudulently obtained through Microsoft's Artifact Signing service, Fox Tempest Defendants enable Vanilla Tempest Defendants to disguise their malware as legitimate software. This deception causes victims' Windows operating systems to recognize the malware as trustworthy, bypassing security features that would otherwise flag or block the malicious code.

A. Fox Tempest Defendants' Deceptive Activity to Obtain Certificates

34. Fox Tempest Defendants supply their illicit code signing service by fraudulently creating Microsoft tenants designed to bypass Microsoft's entity and identity validation requirements for Artifact Signing. To date, Fox Tempest Defendants have created more than 580 fraudulent Microsoft tenants and used them to obtain access to Microsoft's Artifact Signing service and generate the code signing certificates they sell to Vanilla Tempest Defendants and other cybercriminals.

35. To bypass the entity and identity validation process necessary to set up Artifact Signing, Fox Tempest Defendants have employed a range of fraudulent techniques, including exploiting the partner sign-up process by registering new domains using fake names and contact information, submitting fake government identification, and creating fraudulent shell companies or business registration documents to circumvent Microsoft's entity and identity validation requirements. In at least one instance, Fox Tempest Defendants impersonated a legitimate company to gain access to Artifact Signing.

B. Distribution of the Certificates to Vanilla Tempest Defendants

36. Fox Tempest Defendants use Telegram, a cloud-based instant messaging service, to communicate with customers and potential customers about the service. *See* **Figure 1**. John Doe 2, who goes by the alias "SamCodeSign," operates the Telegram group for Fox Tempest Defendants. SamCodeSign has sold access to the code signing service via an auction, conducted through Google Sheets, or via direct purchase through a Google Form.

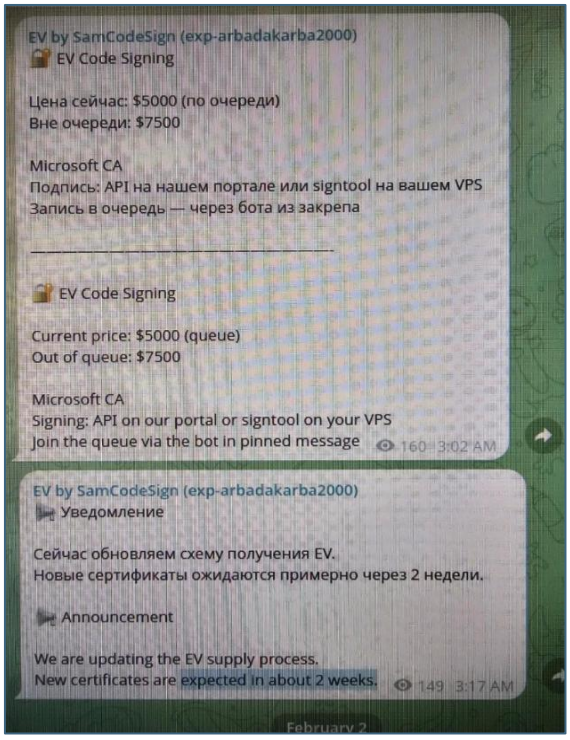

FIGURE 1 – Screenshot of Messages from SamCodeSign to the Group Chat

37. Metadata from a Google Sheet used by SamCodeSign indicated that the account gacermalkin@gmail.com is the owner of the document. This is the same email address used as a technical contact email address for more than 200 Microsoft tenants that John Doe 1 created to access Microsoft's Artifact Signing service.

38. Defendants have used two channels to distribute certificates to cybercriminals, including Vanilla Tempest Defendants: (1) the website, signspace.cloud, and (2) virtual machines hosted by Cloudzy, a company registered in Cyprus and headquartered in Dubai, United Arab Emirates.

39. **Signspace.cloud.** Fox Tempest Defendants operate a website, signspace.cloud, to deliver their code signing service to cybercriminals. The website allows customers to upload and sign their code using the certificates obtained by Fox Tempest Defendants.

40. After purchasing certificates from Fox Tempest Defendants, cybercriminal customers, like Vanilla Tempest Defendants, sign in to the website's user page where they upload their malicious code to be signed and download the digitally signed malicious code. *See* **Figure 2**.

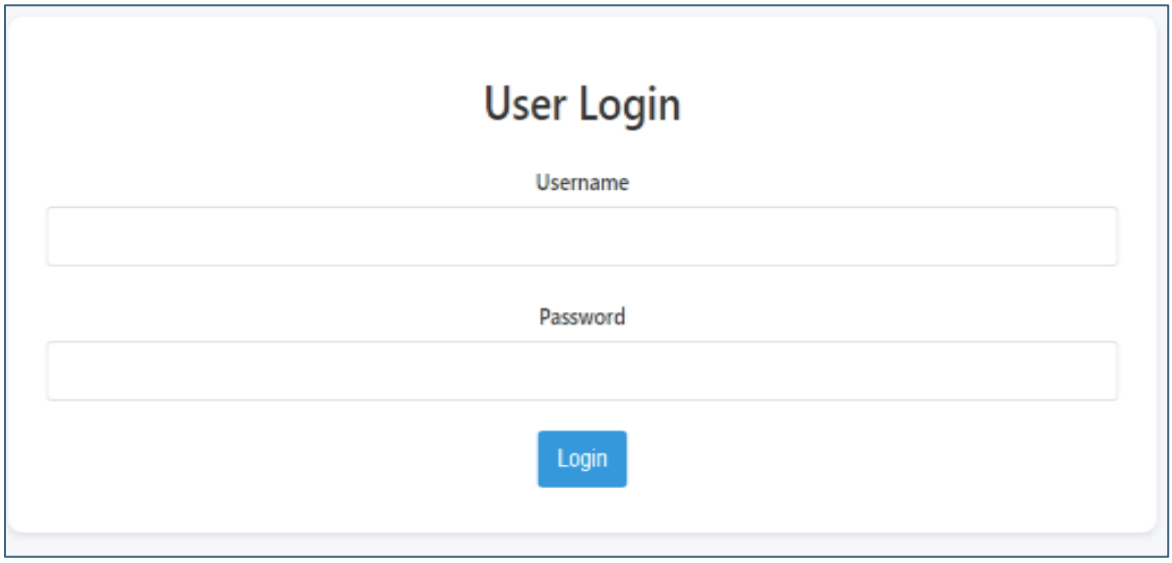

FIGURE 2 – Screenshot of User Login Page on signspace.cloud

41. The signspace.cloud website includes an administrator panel that allows Fox Tempest Defendants to manage each user's page and provide them with access to code signing certificates.

42. The signspace.cloud website uses code stored in a repository on GitHub. The GitHub repository contains code that runs the website and manages its back-end and front-end processes. Additionally, the repository includes a configuration file for a web application identified as the "Code Signing Service." Additional files included within the repository are associated with application database configuration, authentication and authorization settings, file-upload handling logic, user and role-based access controls, Azure cloud service credentials, and application-level operational parameters.

43. The repository is owned by a GitHub user account. This account also owns other repositories, which include an additional contributor whose profile publicly identifies the individual as the person suspected to be John Doe 1. GitHub logs show that this contributor's account created the repository for the code signing service. The logs further show that the repository owner's account and the contributor's account have used identical device cookies, client identifiers, and source IP addresses. Additionally, the contributor accessed their GitHub account using the same IP addresses of the servers that host signspace.cloud.

44. The domain name registrar[8] for signspace.cloud is GoDaddy, a company based in the United States. Aruba PEC SpA, a company based in Italy, is the registry[9] for the ".cloud" domain. The website is hosted by Freak Hosting, a company based in the United Kingdom, using servers located in Germany. Wavecom, a company based in Estonia, also provides hosting services

[8] A "domain name registrar" is an entity accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") and authorized to register domain names on behalf of end users.
[9] A "domain name registry" is the entity designated to operate the authoritative database for a given top-level domain ("TLD"), including maintaining the central registry of domain names within that TLD.

for the website using servers located in Estonia. The known IP addresses associated with servers hosting the signspace.cloud website are 31.59.58[.]9 and 38.180.163[.]50. Additional information on the signspace.cloud domain is provided as **Exhibit 2** to this Complaint. Upon information and belief, Fox Tempest Defendants maintain control of the signspace.cloud website and may continue to use it to further their criminal purpose.

45. **Virtual Machines.** In January 2026, Fox Tempest Defendants began leveraging virtual machines to operate their code signing service. Upon information and belief, Fox Tempest Defendants transitioned to this infrastructure because Microsoft's anti-fraud measures introduced substantial friction into the signspace.cloud website, impairing its ability to provide the code signing service. Fox Tempest Defendants provide customers with access to these virtual machines through Remote Desktop Protocol, a network communications protocol, and instruct them to follow specific steps to sign their code. Upon information and belief, Vanilla Tempest Defendants are among the customers who have received such access and instructions. These machines are hosted by Cloudzy. Microsoft has identified 149 virtual machines hosted by Cloudzy in connection with Fox Tempest Defendants' operations. Based on the IP addresses associated with the virtual machines, the servers hosting the virtual machines are located in the United States. A full list of the known host names and IP addresses associated with the virtual machines is provided as **Appendix B** to this Complaint.

C. Test Purchase of the Service

46. From February to March 2026, Microsoft, with assistance from a cooperating source, anonymously conducted two test purchases of the code signing service from John Doe 2, "SamCodeSign." These test purchases allowed DCU investigators to observe first-hand how Fox Tempest Defendants operate the service, the information a purchaser is provided, and the instructions given by SamCodeSign to connect to the service and sign the test software created by

Microsoft. Additionally, the test purchases allowed DCU to identify cryptocurrency wallets used by Fox Tempest Defendants.

47. As part of the first test purchase, the source filled out the Google Form available in the Telegram group. The Google Form asked the source to select the purchase type, which corresponds to how quickly the certificates will be provided (Standard for $5,000, Priority for $7,500, or Expedited for $9,500). The Google Form also requests that the purchaser specify how frequently they will need certificates and include any additional comments. *See* **Figure 3**.

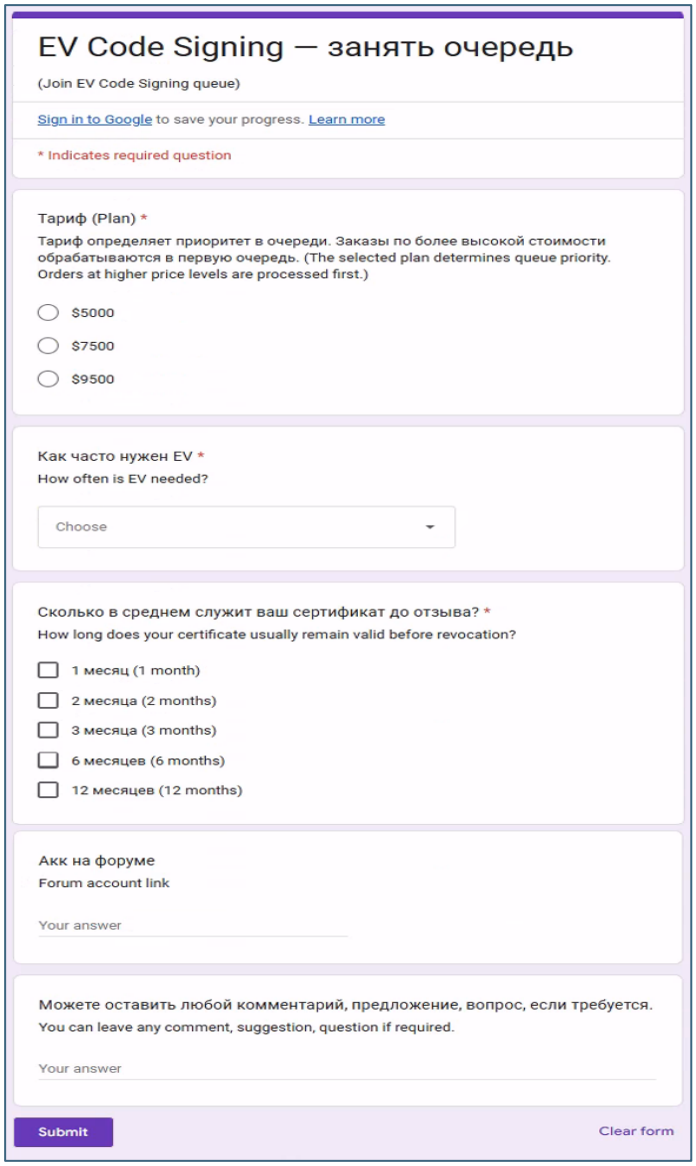

FIGURE 3 – Screenshot of Google Form for Code Signing Service

48. After the source completed the Google Form, SamCodeSign sent a direct message to the source and requested payment to a Bitcoin wallet. *See* **Figure 4**.[10] Following payment by the source, SamCodeSign sent instructions to access the virtual machine—including details such as the username, password, and IP address—and to complete the code signing process using the machine. *See* **Figure 5**.

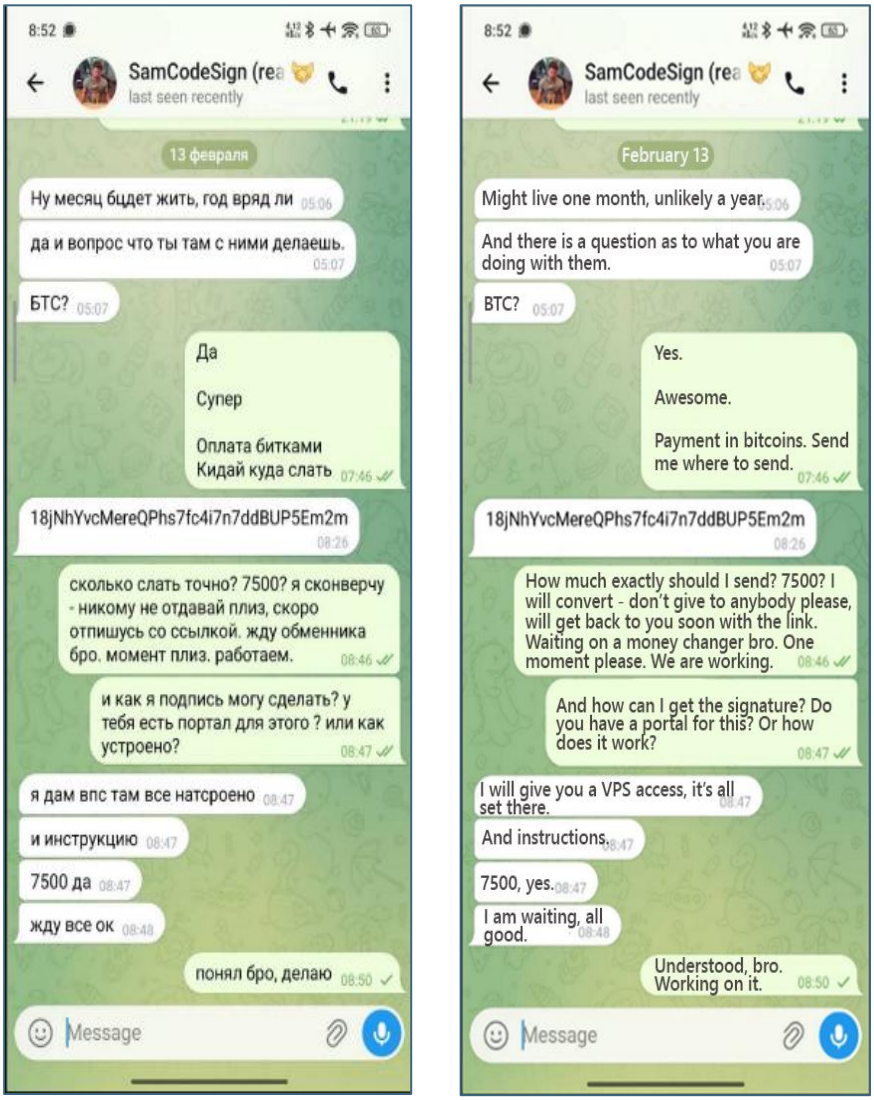

FIGURE 4 – Screenshot of Messages with SamCodeSign on Bitcoin Payment

[10] Unless otherwise indicated, communications with SamCodeSign were originally in Russian and have been translated into English by a fluent native speaker. These communications are included in substance and in part.

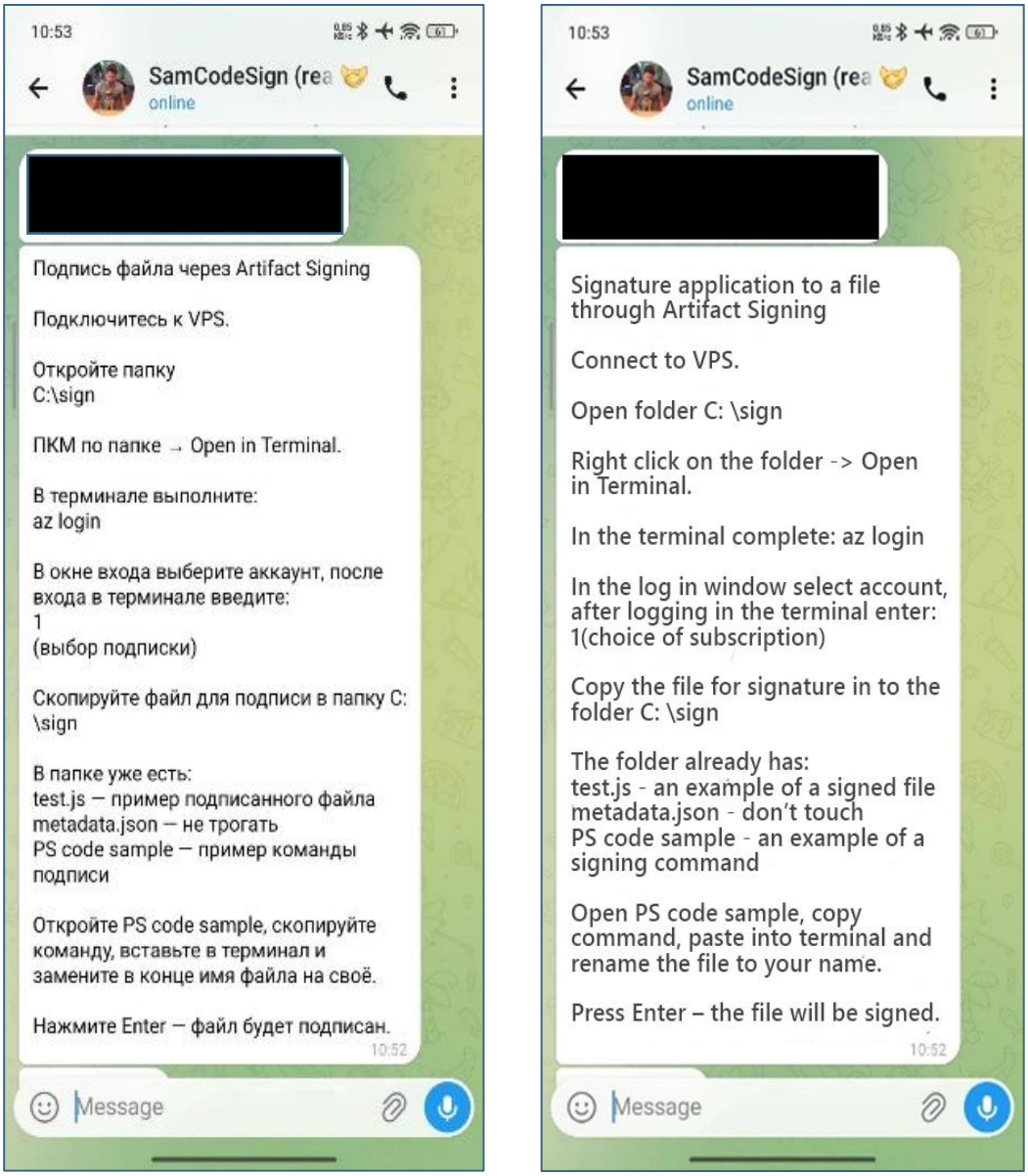

FIGURE 5 – Screenshot of Messages with SamCodeSign on Access to Code Signing Service

49. During the course of these communications, the source asked SamCodeSign whether the signspace.cloud website belonged to him, to which he responded affirmatively. SamCodeSign explained that Fox Tempest Defendants had stopped using the website because it had become too slow, and that it was preferable to use Remote Desktop Protocol "so there won't be visible fraud." *See* **Figure 6**.

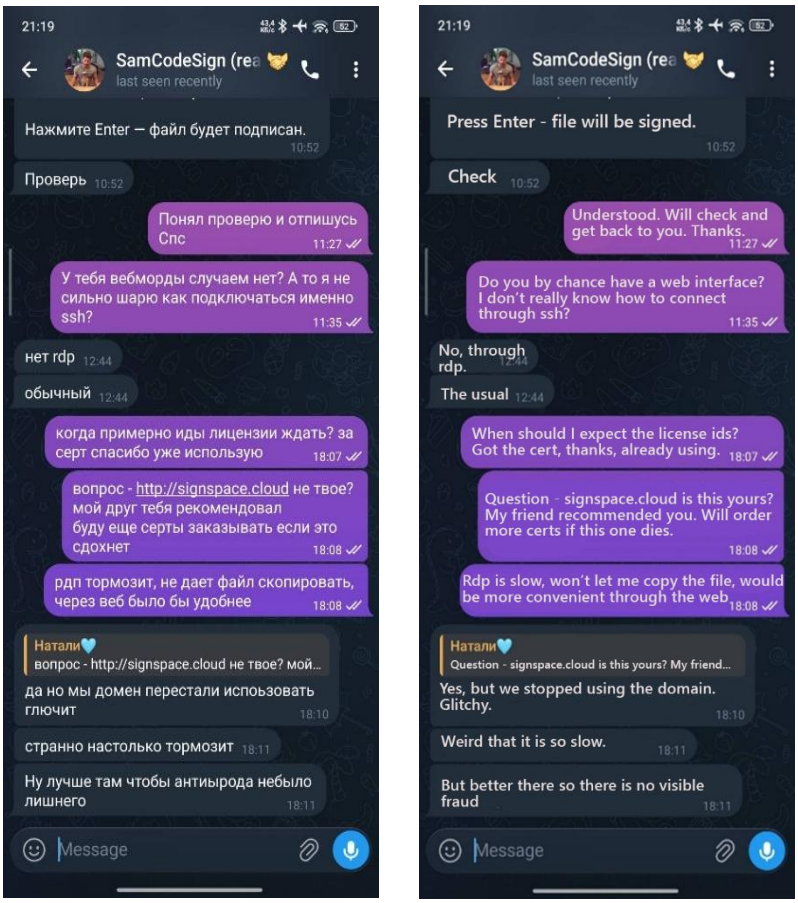

FIGURE 6 – Screenshot of Messages with SamCodeSign on signspace.cloud

50. A DCU investigator was able to log into the virtual machine using the credentials provided by SamCodeSign. Upon remotely accessing the machine, the investigator identified an accessible folder (C:\sign) containing three files: metadata.json, test.js, and PS code sample.txt.

51. The first file, metadata.json, was a configuration file pointing to an Azure-hosted code signing endpoint (eus.codesigning.azure.net). This file identified "AzurCert" as both the signing account and certificate profile. The second file, test.js, was an example of a file that had been digitally signed by Fox Tempest Defendants, provided to demonstrate their signing capabilities to prospective customers. The third file, PS code sample.txt, contained the code used to apply digital signatures to customer-supplied files using certificates controlled by Fox Tempest

Defendants. Specifically, the code used Microsoft's signtool.exe command to sign files digitally using the code signing account and the settings in the configuration file.

52. The investigator was able to successfully sign a test file using the infrastructure present on the virtual machine. The signing process operated as follows:

- First, the investigator authenticated to the appropriate Azure account using the "az login" command.
- Then, after signing into the account, the investigator was prompted to choose which subscription to use and selected the only available subscription associated with the tenant.
- Next, the investigator copied a test file into the C:\sign folder, which contained the configuration file and the sample containing the signing command.
- The investigator then executed the signing command from the code sample file, substituting the test file's name. Upon execution, the test file was successfully signed with the certificate controlled by Fox Tempest Defendants. *See* **Figure 7**.

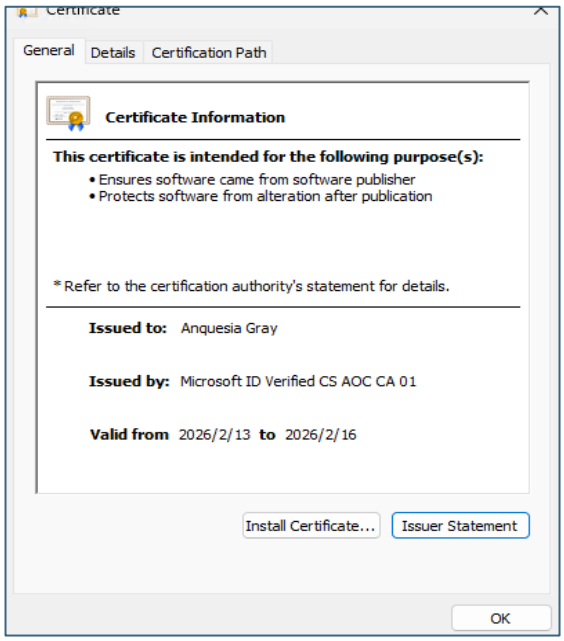

FIGURE 7 – Screenshot of Certificate Used to Sign Test File

53. During the test purchase, DCU investigators collected information on the Microsoft tenant and subscription used by Fox Tempest Defendants to facilitate the code signing. *See* **Figure 8**.

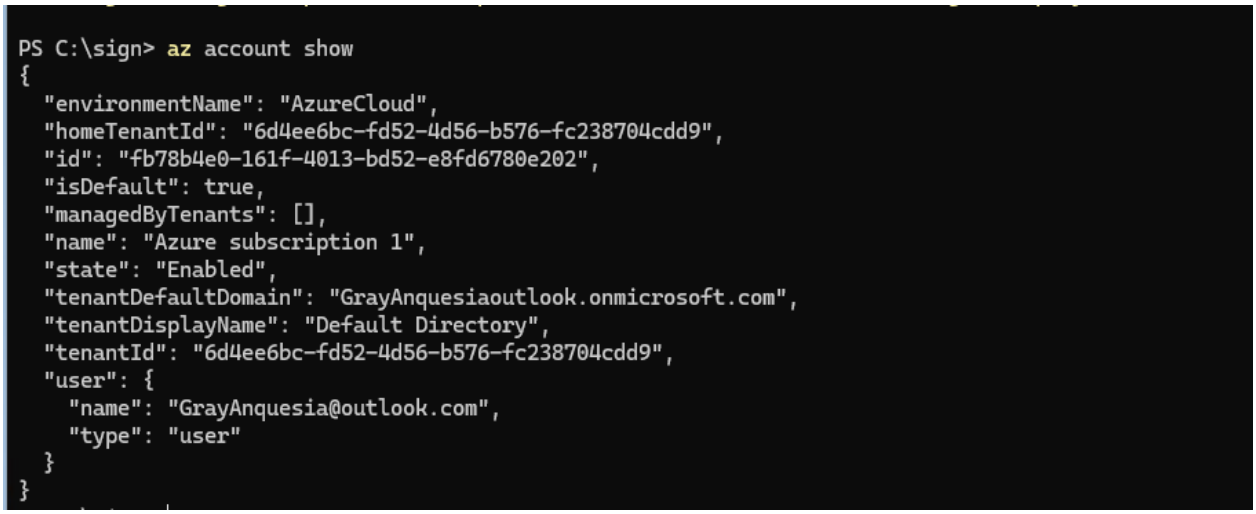

FIGURE 8 – Screenshot of Subscription and Tenant Information from Virtual Machine

Defendants' Attack Chain

54. Vanilla Tempest Defendants purchase code signing certificates from Fox Tempest Defendants by making cryptocurrency payments to a wallet controlled by Fox Tempest Defendants. Microsoft identified five payments occurring between June 2025 and January 2026 between wallets attributed by Chainalysis Reactor[11] to Vanilla Tempest Defendants (as senders) and to SamCodeSign (as recipient). Upon information and belief, Vanilla Tempest Defendants use the service with the knowledge that the certificates are fraudulently obtained. Vanilla Tempest Defendants then commence attacks on victims using the signed malware.

[11] Chainalysis Reactor is a tool used by investigators to trace and analyze cryptocurrency transactions. The tool groups cryptocurrency addresses controlled by the same entity and ties them to entities based on information from other sources. Those sources amass information on cryptocurrency addresses through: test transactions, open-source intelligence, evidence from third parties that have conducted other transactions with such entities, and information from law enforcement agencies.

55. Microsoft has observed Vanilla Tempest Defendants signing "Oyster" (also known as "Broomstick" or "CleanupLoader") malware using certificates from Fox Tempest Defendants. Vanilla Tempest Defendants program Oyster malware to collect system information, steal credentials, execute commands, download additional malware (including ransomware), and maintain persistence on infected machines by creating scheduled tasks. Vanilla Tempest Defendants frequently disguise Oyster malware as popular software including Microsoft Teams.

56. In furtherance of their scheme to deploy malware signed by the certificates purchased from Fox Tempest Defendants, John Does 3–4 created fraudulent installer files bearing the name "MSTeamsSetup.exe" and hosted them on malicious domains designed to mimic legitimate Microsoft Teams websites, including, among others, "teams-download[.]buzz," "teams-install[.]run," and "teams-download[.]top." The websites displayed Microsoft's logo, format, and trademarks, Microsoft® and Microsoft Teams®. Further, John Does 3–4 employed search engine optimization poisoning to lure Microsoft's customers to these malicious download sites. *See* **Figure 9**.

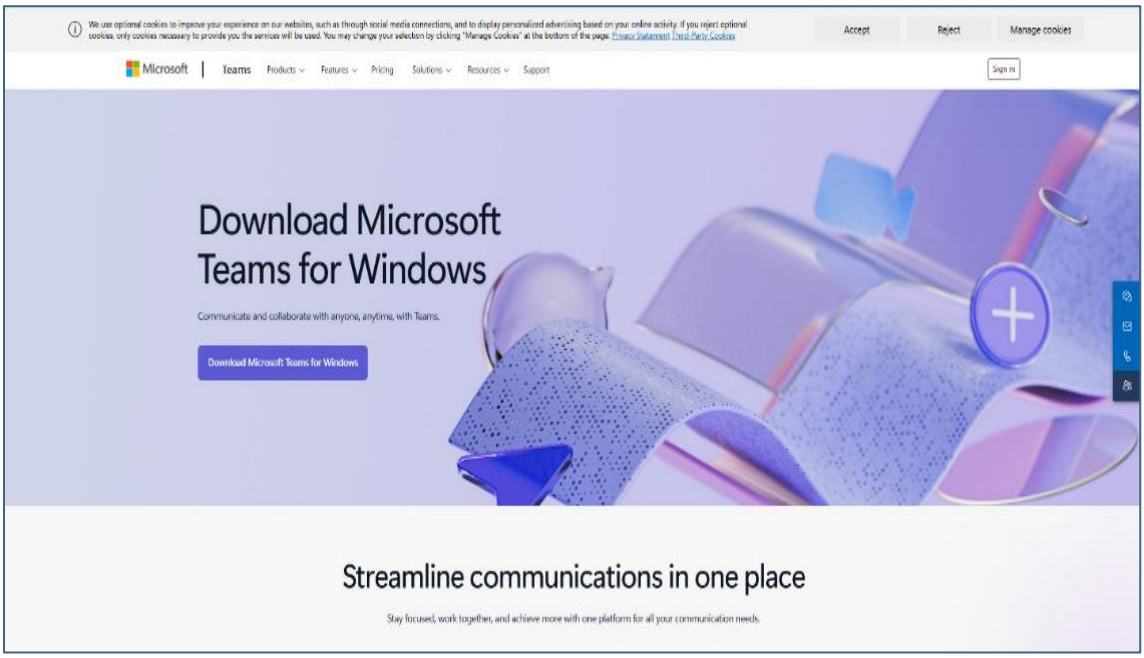

FIGURE 9 – Screenshot of Download Site Created by Vanilla Tempest Defendants

57. When unsuspecting victims executed the falsely named Microsoft Teams installer files, those files delivered a malicious loader, which in turn installed the fraudulently signed Oyster malware and ultimately deployed Rhysida ransomware. Because the Oyster malware was signed by a certificate from Microsoft's Artifact Signing service, the Windows operating system initially recognized the malware as legitimate software, when it would otherwise be flagged as suspicious or blocked entirely by security controls in the Windows operating system. **Figure 10** is a screenshot of a now-revoked certificate that Vanilla Tempest purchased from Fox Tempest Defendants to sign Oyster malware.

FIGURE 10 – Screenshot of Certificate Purchased by Vanilla Tempest Defendants

58. In October 2025, Microsoft disrupted this instance of criminal activity by revoking more than 200 code signing certificates that John Does 3–4 had fraudulently obtained and used in furtherance of the scheme described above. **Figure 11** illustrates this attack chain.

FIGURE 11 – Vanilla Tempest Defendants' Attack Chain

59. Notwithstanding Microsoft's disruption efforts, Vanilla Tempest Defendants have persisted in their unlawful conduct. Vanilla Tempest Defendants have continued to engage in the criminal scheme described herein, including by deploying fake Microsoft Teams installers containing malware signed with fraudulently obtained certificates. In January 2026, Vanilla Tempest Defendants made a Bitcoin payment from a cryptocurrency wallet attributed to them to a wallet attributed to SamCodeSign, coinciding with Fox Tempest Defendants' transition to virtual machine-based distribution infrastructure for their illicit code signing service.

60. Microsoft has identified thousands of customer machines, including more than a dozen machines owned and operated by Microsoft, in the United States that have been impacted by malware signed with certificates originating from the tenants created by Fox Tempest Defendants.

The Defendants' Racketeering Enterprise

61. Fox Tempest Defendants, Vanilla Tempest Defendants, and other cybercriminals exploiting the certificates obtained by the Fox Tempest Defendants together constitute a group,

the Certificate Abuse Enterprise, that is engaged in a common and continuous course of criminal conduct, as part of an ongoing organization and functioning as a continuing unit.

62. The Certificate Abuse Enterprise causes substantial harm to Microsoft, its customers, and the public. Fox Tempest Defendants and the malicious cyber actors who use their service, including Vanilla Tempest Defendants, cooperate and collude in the procurement and distribution of code signing certificates, signing and deployment of malware on victim computers, and exploitation of victims by stealing their information, deploying ransomware, and extorting them for financial gain.

63. The relationships among Fox Tempest Defendants and Vanilla Tempest Defendants are systematic and ongoing, enabling them to collectively pursue the criminal purpose of the Certificate Abuse Enterprise. As **Chart 1** below demonstrates, Fox Tempest Defendants and Vanilla Tempest Defendants each have specialized and indispensable roles in the Certificate Abuse Enterprise, on which the success and furtherance of the Certificate Abuse Enterprise is entirely dependent. Namely, the Fox Tempest Defendants and Vanilla Tempest Defendants leverage each other's criminal expertise and support to: (i) fraudulently obtain code signing certificates from Microsoft's Artifact Signing service through identity fraud and misrepresentation, (ii) sell and distribute those certificates to cybercriminals, knowing and intending they will use the certificates to facilitate unauthorized access to computers, (iii) sign and deploy malware onto the computers of unsuspecting Microsoft customers, (iv) gain unauthorized access to victim computers, and (v) engage in further malicious activities, including exfiltrating sensitive personal and financial information, deploying ransomware, and extorting victims for financial gain.

Defendants	Function
John Doe 1 (Fox Tempest Defendant)	Serves as an enabler of the Certificate Abuse Enterprise's malware deployment scheme. Fraudulently creates Microsoft tenants to obtain access to Microsoft's Artifact Signing service, acquires code signing certificates, develops technical solutions to successfully sign malware with fraudulently obtained code signing certificates, and maintains infrastructure to deliver the certificates to Vanilla Tempest Defendants.
John Doe 2 (Fox Tempest Defendant)	Serves as an enabler of the Certificate Abuse Enterprise's malware deployment scheme. Upon information and belief, markets and sells access to fraudulently obtained code signing certificates to Vanilla Tempest Defendants with the knowledge that they will be used to sign malware intended for deployment on victim computers. Solicits and collects cryptocurrency payments on behalf of Fox Tempest Defendants and provides credentials and instructions to Vanilla Tempest Defendants for accessing the code signing certificates and related infrastructure.
John Does 3–4 (Vanilla Tempest Defendants)	Serve as the executors of the Certificate Abuse Enterprise's malware deployment scheme. Purchase, via cryptocurrency payment, fraudulently obtained code signing certificates from Fox Tempest Defendants, use them to sign malware, and deploy the signed malware onto victims' computers through deceptive distribution methods, including malicious advertising campaigns, search engine optimization poisoning, and spoofed websites designed to mimic legitimate software download pages. Once deployed, the malware grants Vanilla Tempest Defendants unauthorized access to end users' computers, enabling them to exfiltrate sensitive personal and financial information, deploy ransomware, and extort victims.

CHART 1 – Defendants' Division of Labor

64. The Certificate Abuse Enterprise's criminal scheme is entirely predicated on the deployment of malware onto the computers of Microsoft's end users. Without valid code signing certificates, malware distributed by Vanilla Tempest Defendants would be flagged as suspicious or blocked entirely by security controls in the Windows operating system. Fox Tempest Defendants' fraudulent acquisition and distribution of certificates is therefore essential to the Certificate Abuse Enterprise's ability to deceive end users and gain unauthorized access to their computers. Similarly, without Vanilla Tempest Defendants' development, distribution, and deployment of malware, the certificates sold by Fox Tempest Defendants would not themselves

victimize computers or devices and generate the financial returns underpinning the Certificate Abuse Enterprise. Therefore, the Certificate Abuse Enterprise operates as an integrated criminal enterprise in which each group of Defendants depends on and cooperates with the other to accomplish the objective of defrauding victims by obtaining unauthorized access to their computers.

65. Repeated cryptocurrency payments occurring between Defendants from June 2025 to January 2026 demonstrate the continuing nature of the Certificate Abuse Enterprise.

66. Upon information and belief, Defendants have knowingly, and with intent to defraud, conspired with one another to perpetrate cyberattacks against victims using malware signed with code signing certificates fraudulently obtained from Microsoft's Artifact Signing service. These acts are continuing and will continue unless and until this Court grants Microsoft's request for a temporary restraining order.

67. Each of the foregoing illegal acts perpetrated by the Certificate Abuse Enterprise was conducted using cryptocurrency exchanges whereby funds are transferred via the internet—an instrumentality of interstate commerce, and/or interstate and/or foreign wires as described herein and therefore affected interstate commerce.

Harm to Microsoft and Microsoft's Customers

68. Defendants' actions have inflicted direct and severe harm on Microsoft. By creating more than 580 fraudulent Artifact Signing tenants using false information, Fox Tempest Defendants have undermined the integrity of Microsoft's Artifact Signing service and damaged Microsoft's reputation and the goodwill of its associated trademarks. The Artifact Signing service is designed to provide a secure, verified chain of trust between software developers, Microsoft, and end users. Defendants knowingly circumvented verification procedures by creating accounts with false identifying information, using the resulting certificates to sign malware in violation of

the Artifact Signing service's Terms of Use, and draining Microsoft's valuable computing resources. This conduct deceives Microsoft customers into believing that malicious software is legitimate and trustworthy, thereby harming the value of Microsoft's Artifact Signing service and damaging the goodwill associated with its trademarks. Furthermore, malware signed using certificates that the Fox Tempest Defendants fraudulently obtained has impacted machines owned and operated by Microsoft.

69. Vanilla Tempest Defendants' conduct has caused similar reputational harm through their abuse of Microsoft's brands more broadly. John Does 3–4 leveraged falsely named Microsoft Teams setup files hosted on domains designed to mimic Microsoft's registered marks and domains. Similar to the abuse of the Artifact Signing service, when Microsoft customers download what they believe to be legitimate Microsoft software and instead receive malware, those customers associate the resulting harm with Microsoft and its products, causing further damage to Microsoft's brands and the goodwill associated therewith.

70. Microsoft has expended significant resources to investigate the abuse of its Artifact Signing service, identify and disable the fraudulent tenants created by Fox Tempest Defendants, implement live monitoring, revoke the certificates used to sign malware, and complete other mitigations being announced publicly in connection with this action. Additionally, Microsoft has investigated and remediated damage caused to more than a dozen of its machines by malware signed by certificates originating from Fox Tempest Defendants. Microsoft has also addressed the harm resulting from the abuse of its Microsoft Teams® brand. In October 2025 alone, Microsoft investigated and revoked more than 200 certificates that John Does 3–4 fraudulently obtained and used to perpetrate attacks. Microsoft has expended significant resources—more than $1,500,000 and 8,000 investigative hours—to investigate and track the Defendants' illegal activities and to

counter and remediate the damage caused by Defendants and other members of the Certificate Abuse Enterprise to Microsoft and its customers.

71. Defendants' actions have inflicted direct and severe harm on Microsoft's customers. Microsoft has identified thousands of customer machines in the United States that have been impacted by malware signed with certificates originating from the fraudulent tenants created by Fox Tempest Defendants. Customers who have been compromised by Oyster malware face a multitude of severe consequences. These malware programs are designed to collect system information, steal credentials, execute commands, download additional malware, and maintain persistence on infected machines.

72. As a result of these compromises, impacted customers have experienced substantial financial, reputational, and emotional harm, including the theft of sensitive business, personal, and financial information, the theft of credentials that can be used for further intrusions, the deployment of ransomware that encrypts their files and renders their computers unusable, the extortion by Vanilla Tempest Defendants, and significant operational downtime.

73. The Certificate Abuse Enterprise has financially benefited from this criminal scheme, to wit, Fox Tempest Defendants have profited through the sale of fraudulently obtained certificates and Vanilla Tempest Defendants have profited through ransomware attacks, data theft, and extortion campaigns enabled by the malware signed by such certificates.

COUNT I
Violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)
(All Defendants)

74. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 73 above.

75. Beginning in June 2025 and continuing up through the filing of this Complaint, Fox Tempest Defendants and Vanilla Tempest Defendants were and are associated in fact with the Certificate Abuse Enterprise and have conducted its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce.

76. The Certificate Abuse Enterprise is an association-in-fact enterprise consisting of Fox Tempest Defendants, Vanilla Tempest Defendants, and other cybercriminals who function as a continuing unit for the common purpose of fraudulently obtaining code signing certificates from Microsoft's Artifact Signing service and using those certificates to deploy signed malware onto the computers of Microsoft's customers to steal sensitive information, deploy ransomware, and extort victims.

77. The members of the Certificate Abuse Enterprise each play distinct but interdependent roles in the Certificate Abuse Enterprise's criminal scheme. Fox Tempest Defendants serve as enablers by fraudulently creating Microsoft tenants, obtaining code signing certificates, and selling them to Vanilla Tempest Defendants and other cybercriminals. Vanilla Tempest Defendants and other cybercriminals serve as executors by purchasing certificates, signing malware, and deploying it onto victims' computers through deceptive distribution methods. The Certificate Abuse Enterprise operates as an integrated criminal unit in which each group depends on the other to accomplish the Certificate Abuse Enterprise's objectives.

78. Defendants conduct their affairs through a pattern of racketeering activity affecting interstate and foreign commerce involving numerous predicate acts, including violations of (i) the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C.§ 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

79. Vanilla Tempest Defendants violated 18 U.S.C. § 1030(a)(5)(A) each time they intentionally caused damage without authorization to Microsoft's customers' protected computers by deploying malware signed with fraudulently obtained certificates provided by Fox Tempest Defendants. Vanilla Tempest Defendants' malware infected customer machines in the United States, causing damage to those protected computers by collecting system information, stealing credentials, executing unauthorized commands, downloading additional malware, and/or deploying ransomware. Fox Tempest Defendants aided and abetted each violation of 18 U.S.C. § 1030(a)(5)(A) by knowingly providing the code signing certificates and means of signing malware to Vanilla Tempest Defendants, enabling their malware to be successfully deployed onto victims' computers.

80. Fox Tempest Defendants committed a violation of 18 U.S.C. § 1343 each time they created a new tenant by knowingly, and with the intent to defraud, submitting false identifying information to Microsoft's entity and identity validation systems to fraudulently obtain code signing certificates. Vanilla Tempest Defendants aided and abetted these violations through repeated cryptocurrency payments to Fox Tempest Defendants, enabling their continuous and fraudulent procurement of code signing certificates.

81. In violation of 18 U.S.C. § 1343, Vanilla Tempest Defendants knowingly, and with the intent to defraud, used the internet to distribute malware disguised as legitimate software, operated spoofed websites mimicking Microsoft Teams and other software products, and employed search engine optimization poisoning that deceived Microsoft's customers.

82. Altogether, the successful completion of these predicate acts is a result of coordinated and continuous activity by the Certificate Abuse Enterprise. Fox Tempest Defendants have created more than 580 fraudulent Microsoft tenants to deliver code signing certificates to

Vanilla Tempest Defendants and other cybercriminals. In turn, Vanilla Tempest Defendants and other cybercriminals have used the certificates to deploy malware that has impacted thousands of customer machines in the United States, including more than a dozen machines owned and operated by Microsoft.

83. Microsoft has been and continues to be directly injured by Defendants' conduct. As a proximate result of Defendants' pattern of racketeering activity, Microsoft has suffered reputational harm and damage to trademark goodwill, harm to the integrity of its Artifact Signing service, damage to Microsoft-owned machines impacted by signed malware, and significant expenditure of resources to investigate and remediate Defendants' illegal activities. But for the alleged pattern of racketeering activity, Microsoft would not have incurred these harms.

84. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT II
Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d)
(All Defendants)

85. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 84 above.

86. Beginning in June 2025 and continuing up through the filing of this Complaint, Fox Tempest Defendants and Vanilla Tempest Defendants conspired to associate in fact with the Certificate Abuse Enterprise and conduct its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. As part of the Certificate Abuse Enterprise, Fox Tempest Defendants and Vanilla Tempest Defendants further conspired together and with each other to engage in an unlawful pattern of racketeering activity involving numerous predicate acts of violations of (i) the Computer Fraud and Abuse Act (18 U.S.C.

§ 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), and (ii) wire fraud (18 U.S.C. § 1343), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(B).

87. The members of the Certificate Abuse Enterprise conspired for the common purpose of defrauding victims through the deployment of malware signed with code signing certificates fraudulently obtained from Microsoft's Artifact Signing service.

88. Microsoft has been and continues to be directly injured by Defendants' conduct. But for the alleged conspiracy to conduct a pattern of racketeering activity, Microsoft would not have incurred harm.

89. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT III
Conspiracy to Damage a Computer Without Authorization in Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(b)
(All Defendants)

90. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 89 above.

91. Defendants conspired with each other and other cybercriminals to commit offenses under 18 U.S.C. § 1030(a)(5)(A), which prohibits knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer.

92. Fox Tempest Defendants conspired with Vanilla Tempest Defendants and other cybercriminals by intentionally providing fraudulently obtained code signing certificates with the knowledge that such certificates would be used to sign malware for deployment onto the protected computers of Microsoft's customers. Fox Tempest Defendants marketed their code signing service

to cybercriminals, sold certificates knowing they would be used to sign malware, and provided technical support and infrastructure to facilitate the deployment of signed malware.

93. Vanilla Tempest Defendants conspired with Fox Tempest Defendants by purchasing code signing certificates from Fox Tempest Defendants, using those certificates to sign malware, and deploying the signed malware onto the protected computers of Microsoft and its customers.

94. As a result of the conspiracy and the overt acts taken in furtherance thereof, Defendants intentionally caused damage without authorization to protected computers in the United States, including more than a dozen owned and operated by Microsoft. The malware deployed by Defendants caused damage by collecting system information, stealing credentials, executing unauthorized commands, downloading additional malware, and deploying ransomware that encrypted victims' files and rendered their computers unusable.

95. Defendants' conduct involved interstate and/or foreign communications.

96. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000. Microsoft has expended significant resources totaling more than $1,500,000 to investigate Defendants' illegal activities, remediate the damage caused by Defendants to Microsoft's protected computers, and revoke fraudulently obtained certificates.

97. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT IV
Trafficking in Passwords or Similar Information with Intent to Defraud in Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(6)
(John Doe 1, John Doe 2)

98. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 97 above.

99. Fox Tempest Defendants knowingly, and with intent to defraud, trafficked in code signing certificates by fraudulently creating more than 580 Microsoft tenants, obtaining access to Microsoft's Artifact Signing service through those fraudulent tenants, generating code signing certificates, and selling those certificates to cybercriminals. Fox Tempest Defendants marketed and sold the certificates through Telegram, Google Forms, and managed Google Sheets, and collected cryptocurrency payments in exchange for providing access to the fraudulently obtained certificates.

100. Fox Tempest Defendants operated infrastructure specifically designed for providing fraudulently obtained code signing certificates to cybercriminals, including the signspace.cloud website and virtual machines hosted by Cloudzy.

101. The code signing certificates constitute "passwords or similar information" within the meaning of § 1030(a)(6) because, like passwords, when presented to a computer's authorization mechanisms, they enable Vanilla Tempest Defendants' malware to bypass security controls that would otherwise prevent unauthorized access.

102. The code signing certificates distributed by Fox Tempest Defendants provided Vanilla Tempest Defendants access to computers without authorization as the malware signed with those certificates caused the Windows operating system to treat the malware as legitimate software when software without such certificates would be flagged as suspicious or blocked entirely by Windows security features.

103. Fox Tempest Defendants' trafficking affected interstate and foreign commerce because they sold certificates to cybercriminals located outside the United States and the certificates were used to sign malware that was deployed on protected computers throughout the United States.

104. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000. Microsoft has expended significant resources totaling more than $1,500,000 to investigate Defendants' illegal activities, revoke fraudulently obtained certificates, and remediate the damage caused by Defendants to Microsoft.

105. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

COUNT V
Trademark Infringement Under the Lanham Act, 15 U.S.C. § 1114(1)
(All Defendants)

106. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 105 above.

107. Microsoft has the exclusive rights to use each of its inherently distinctive, federally registered trademarks in United States commerce, and Microsoft's ownership of and exclusive rights in and to the trademarks predate any rights that Defendants could establish in and to any mark that consists of one of the trademarks in whole and/or in part.

108. Defendants have made unauthorized use of Microsoft's trademarks, and specifically the Microsoft® and Microsoft Teams® marks. Fox Tempest Defendants have fraudulently obtained code signing certificates bearing the Microsoft® mark through Microsoft's Artifact Signing service and knowingly supplied those certificates to Vanilla Tempest Defendants for use in signing malware disguised as legitimate Microsoft Teams® software. Vanilla Tempest Defendants, in turn, have hosted fraudulent websites displaying Microsoft's trademarks and logos, distributed malware through those sites using file names and branding designed to mimic Microsoft Teams® software, and signed that malware with certificates bearing Microsoft's name—

all to create the false impression that the malware is authentic, trustworthy software originating from or endorsed by Microsoft. Through this conduct, Defendants have caused, and are likely to continue to cause, consumer confusion, mistake, and deception as to the origin, sponsorship, or approval of the malware.

109. Fox Tempest Defendants have intentionally enabled this infringement by knowingly providing certificates for signing malware bearing Microsoft's trademark, marketing their services to Vanilla Tempest Defendants and other cybercriminals, and collecting payment for services that facilitate ongoing infringement.

110. Microsoft has not consented to Defendants' use of its trademarks for any purpose, and Defendants' use of the trademarks is without permission from Microsoft.

111. Defendants were aware of Microsoft's rights in and to its trademarks before and when Defendants began using the trademarks and have undertaken these actions willfully and with the intent to cause confusion, mistake, and deception among consumers and members of the public.

112. Defendants adopted and use the trademarks in furtherance of their willful and deliberate plan to trade upon the extensive consumer goodwill, reputation, and commercial success of trusted products that Microsoft offers under its trademarks.

113. Defendants' acts and conduct complained of herein constitute trademark infringement in violation of 15 U.S.C. § 1114(1).

114. Based on the irreparable harm that Microsoft has suffered, and continues to suffer, as a result of Defendants' actions, Microsoft seeks injunctive relief and compensatory and treble damages in an amount to be proven at trial.

COUNT VI
False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a)
(All Defendants)

115. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 114 above.

116. Microsoft's trademarks are distinctive marks that are uniquely associated with Microsoft and exclusively identify Microsoft's businesses, products, and services.

117. Defendants have made unauthorized use of Microsoft's trademarks, and specifically the Microsoft® and Microsoft Teams® marks. Fox Tempest Defendants have fraudulently obtained code signing certificates bearing the Microsoft® mark through Microsoft's Artifact Signing service and knowingly supplied those certificates to Vanilla Tempest Defendants for use in signing malware disguised as legitimate Microsoft Teams® software. Vanilla Tempest Defendants, in turn, have hosted fraudulent websites displaying Microsoft's trademarks and logos, distributed malware through those sites using file names and branding designed to mimic Microsoft Teams® software, and signed that malware with certificates bearing Microsoft's name—all to create a false association with Microsoft, its products, and services.

118. Fox Tempest Defendants have intentionally enabled this false designation by knowingly providing certificates for signing malware bearing Microsoft's trademark, marketing their services to Vanilla Tempest Defendants and other cybercriminals, and collecting payment for services that facilitate ongoing false designation.

119. Defendants' actions and fraudulent conduct are likely to cause significant consumer confusion and to deceive consumers as to the affiliation, connection, approval, sponsorship, or association of Microsoft with Defendants.

120. Defendants' actions and fraudulent conduct thus constitute unfair competition, false endorsement, false association, and/or false designation of origin in violation of the Lanham Act, 15 U.S.C. § 1125(a).

121. Based on the irreparable harm that Microsoft has suffered, and continues to suffer, as a result of Defendants' actions, Microsoft seeks injunctive relief and compensatory and treble damages in an amount to be proven at trial.

COUNT VII
Trademark Dilution Under the Lanham Act, 15 U.S.C. § 1125(c)
(All Defendants)

122. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 121 above.

123. Microsoft has the exclusive rights to use its trademarks in commerce on and in connection with its businesses, products, and services.

124. Microsoft's trademarks are inherently distinctive and famous, and Microsoft's ownership of and exclusive rights in and to the trademarks predate any rights that Defendants could establish in and to any mark that consists of one of Microsoft's trademarks in whole and/or in part.

125. Microsoft's trademarks were famous before Defendants began using the trademarks.

126. Microsoft has not consented to Defendants' use of its trademarks for any purpose.

127. Defendants' use of Microsoft's famous trademarks, including the marks Microsoft® and Microsoft Teams®, in connection with the distribution of malware dilutes the distinctive quality of Microsoft's famous trademarks by tarnishment. Fox Tempest Defendants have fraudulently obtained code signing certificates bearing the Microsoft® mark through Microsoft's

Artifact Signing service and knowingly supplied those certificates to Vanilla Tempest Defendants for use in signing malware disguised as legitimate Microsoft Teams® software. Vanilla Tempest Defendants, in turn, have hosted fraudulent websites displaying Microsoft's trademarks and logos, distributed malware through those sites using file names and branding designed to mimic Microsoft Teams® software, and signed that malware with certificates bearing Microsoft's name. Defendants' conduct significantly harms the reputation of Microsoft's trademarks and diminishes Microsoft's ability to indicate the superior quality of products and services offered under its famous trademarks.

128. Fox Tempest Defendants have intentionally enabled this dilution by knowingly providing certificates for signing malware bearing Microsoft's trademark, marketing their services to Vanilla Tempest and other cybercriminals, and collecting payment for services that facilitate ongoing dilution.

129. Defendants use Microsoft's trademarks in commerce as part of their willful and deliberate scheme to trade upon and profit from the extensive consumer goodwill, reputation, commercial success, and fame of goods and services offered under Microsoft's distinctive and famous trademarks.

130. Defendants' use of Microsoft's trademarks, as alleged herein, dilutes Microsoft's famous trademarks in violation of 15 U.S.C. § 1125(c).

131. Based on the irreparable harm that Microsoft has suffered, and continues to suffer, as a result of Defendants' actions, Microsoft seeks injunctive relief and compensatory and treble damages in an amount to be proven at trial.

COUNT VIII
Breach of Contract
(John Doe 1, John Doe 2)

132. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 131 above.

133. Users of Microsoft's Artifact Signing service are bound by Microsoft's Terms of Use for Artifact Signing, a contract that governs access to and use of the service. By creating these tenants and accessing the Artifact Signing service, John Does 1–2 accepted and became bound by Microsoft's Terms of Use.

134. John Does 1–2 materially breached the Terms of Use by, among other things: (a) submitting false and fraudulent information to Microsoft in connection with the service, including fake identifying information and fraudulent business registration documents; (b) using the service for unlawful purposes, including to facilitate the sale of code signing certificates to cybercriminals; (c) engaging in illegal activity, false or misleading activity, and activity that harms Microsoft and others; (d) enabling access to the service by unauthorized third parties; and (e) failing to investigate malicious activity of which they had awareness.

135. As a direct and proximate result of breaches by John Does 1–2, Microsoft has been damaged in an amount to be proven at trial, including the costs of investigating the activities of John Does 1–2 and revoking fraudulently obtained certificates.

136. Microsoft seeks compensatory damages in an amount to be proven at trial.

COUNT IX
Trespass to Chattels
(John Doe 1, John Doe 2)

137. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 136 above.

138. John Does 1–2 used Microsoft's Artifact Signing service and computer networks, without authorization, with the intent to obtain code signing certificates through fraudulent means and to cause injury to Microsoft's property.

139. The activities of John Does 1–2 resulted in unauthorized access to Microsoft's Artifact Signing service, a proprietary Microsoft cloud-based code signing platform. John Does 1–2 fraudulently created more than 580 Microsoft tenants using false identifying information and used those tenants to access Microsoft's Artifact Signing service without authorization and obtain code signing certificates to which they were not entitled.

140. John Does 1–2 intentionally caused this conduct, and this conduct was unlawful and unauthorized.

141. Defendants' actions have caused injury to Microsoft by interfering with Microsoft's possessory interests in its property. Specifically, John Does 1–2 consumed Microsoft's computing resources without authorization by fraudulently accessing the Artifact Signing service and utilizing Microsoft's cloud infrastructure to generate code signing certificates. John Does 1–2 also deprived Microsoft of the use and value of its code signing certificates by obtaining them through fraud and distributing them to third parties for use in signing malware, thereby rendering those certificates untrustworthy and requiring Microsoft to revoke them.

142. Microsoft seeks compensatory and punitive damages in an amount to be proven at trial.

COUNT X
Unjust Enrichment
(John Doe 3, John Doe 4)

143. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 142 above.

144. The acts of John Does 3–4 complained of herein constitute unjust enrichment of John Does 3–4 at Microsoft's expense, in violation of the common law.

145. John Does 3–4 used, without authorization or license, Microsoft's Artifact Signing service and code signing certificates to sign malware and facilitate unlawful conduct to the benefit of John Does 3–4.

146. John Does 3–4 profited unjustly from their unauthorized use of Microsoft's code signing certificates. Through ransomware attacks, data theft, and extortion campaigns launched with the assistance of malware signed by fraudulently obtained certificates, John Does 3–4 have financially benefited from their criminal scheme at Microsoft's expense.

147. Upon information and belief, John Does 3–4 had an appreciation and knowledge of the benefit they derived from their unauthorized use of Microsoft's code signing certificates.

148. Retention by John Does 3–4 of the profits they derived from their malfeasance would be inequitable and unjust.

149. Microsoft seeks compensatory damages in an amount to be proven at trial, including, without limitation, disgorgement of the ill-gotten profits gained by John Does 3–4.

REQUEST FOR RELIEF

WHEREFORE, Microsoft respectfully requests that the Court enter judgment in its favor and against Defendants as follows:

1. Awarding judgment in favor of Microsoft and against Defendants, for Microsoft's actual damages from Defendants' activity complained of herein and for any injuries complained of herein, including but not limited to, interests and costs, in an amount to be proven at trial.

2. Declaring that Defendants' conduct has been willful, and that Defendants have acted with fraud, malice, and oppression.

3. Issuing a temporary restraining order and preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injuries complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activities complained of herein or from causing any of the injuries complained of herein.

4. Issuing a preliminary and permanent injunction giving Microsoft control over the domain and virtual machines used by Defendants to cause injury and access to all data stored on or associated with the virtual machines, and enjoining Defendants from using such instrumentalities.

5. Entering judgment disgorging Vanilla Tempest Defendants' profits.

6. Entering judgment awarding enhanced, exemplary, and special damages in an amount to be proven at trial.

7. Entering judgment awarding attorney's fees and costs.

8. Awarding such other relief that the Court deems just and proper.

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: May 4, 2026

Respectfully submitted,

MAYER BROWN LLP

Adam S. Hickey
David J. Lizmi
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
Tel: (212) 506-2500
Fax: (212) 262-1910
Email: *ahickey@mayerbrown.com*
dlizmi@mayerbrown.com

Sasha L. Keck
Christina Luk (*pro hac vice* forthcoming)
Aaron J. Futerman (*pro hac vice* forthcoming)
Tanner L. Wilburn (*pro hac vice* forthcoming)
MAYER BROWN LLP
1999 K Street NW
Washington, DC 20006
Tel: (202) 263-3000
Fax: (202) 263-3300
Email: *skeck@mayerbrown.com*
cluk@mayerbrown.com
afuterman@mayerbrown.com
twilburn@mayerbrown.com

Attorneys for Plaintiff Microsoft Corporation