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**

DECLARATION OF MAURICE MASON IN SUPPORT OF PLAINTIFF'S EMERGENCY *EX PARTE* APPLICATION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Maurice Mason, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration in support of Microsoft's Emergency *Ex Parte* Application for Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or upon information and belief from my review of documents and evidence collected during Microsoft's investigation. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. I have been employed by Microsoft since August 2021. In my role with Microsoft's DCU, I assess technological security threats to Microsoft and the effect of such threats on

Microsoft's business and customers. My responsibilities include investigating cybercriminal operations that abuse Microsoft platforms and services, conducting technical, infrastructure, and financial analysis related to malware distribution and cybercrime-as-a-service operations, and supporting civil disruption actions and law enforcement referrals. I am familiar with Microsoft systems relevant to this matter, including Azure cloud services and Microsoft's code signing infrastructure.

3. Prior to my current role, I worked as a Senior Consultant on Microsoft's Incident Response Team, where I was a lead digital forensic analyst managing multiple incident response and threat-hunting engagements that included performing incident response and forensic analysis for Fortune 500, Fortune 100, and Fortune 50 companies. Prior to joining Microsoft, I held various positions, both in the private sector and in government, where I performed digital forensic analysis, including on malware and ransomware-related matters. A copy of my resume is attached to this declaration as **Exhibit 1**.

4. Since on or about June 2025, I have been investigating the structure and function of the criminal enterprise operated by the Defendants, referred to herein as the "Certificate Abuse Enterprise." The Certificate Abuse Enterprise is comprised of John Does 1–2, who are collectively known as "Fox Tempest Defendants," and John Does 3–4, who are collectively known as "Vanilla Tempest Defendants" (and together with Fox Tempest Defendants, the "Defendants"), and other cybercriminals. At a high level, the Certificate Abuse Enterprise's scheme involves (1) fraudulently obtaining code signing certificates from Microsoft's Artifact Signing service; (2) using the certificates to sign malware; (3) deploying the signed malware—which appears to be legitimate software—to gain unauthorized access to victim computers; and (4) exploiting that access to steal information, deploy ransomware, and extort victims.

CYBERCRIME AT ISSUE: MALWARE-SIGNING-AS-A-SERVICE

5. Code signing is 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. A code signing certificate is a digital credential issued by a trusted certificate authority (e.g., Microsoft or trusted third-party public key infrastructure providers) that allows a software publisher to apply a cryptographic signature to an executable file. This certificate verifies the identity of the publisher and enables computer operating systems to confirm that the file has not been altered or tampered with since it was signed.

6. As it pertains to Microsoft's Windows operating system, a valid digital signature permits software to satisfy the security mechanisms that the Windows operating system would otherwise apply or 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, allowing users to install the software unimpeded.

7. This dynamic is further strengthened 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.

8. With increasing frequency, sophisticated malicious cyber actors have subverted this critical trust mechanism in modern computing operating systems by obtaining or misusing valid signing certificates to mask dangerous malware as trusted software. This form of abuse has given rise to what is known as Malware-Signing-as-a-Service ("MSaaS"), a criminal service model in

which an operator provides fraudulently obtained code signing certificates from a certificate authority to malicious cyber actors for the purpose of signing malicious software. MSaaS operators also develop and maintain the infrastructure that enables their customers to upload malicious files and receive signed binaries, causing those files to appear as legitimately signed to operating systems and their applicable security controls. Accordingly, by deploying signed malware, threat actors are able to bypass or reduce security warnings, including UAC prompts, SmartScreen alerts, SAC, browser warnings, and certain antivirus detections.

9. Malicious cyber actors distribute signed malware through a combination of techniques including malicious advertising ("malvertising"), search engine optimization ("SEO") poisoning, and deceptive download pages leading victims to unknowingly download and execute malicious software. Malvertising involves the purchase and injection of malicious ads into legitimate online advertising streams such that a user on a legitimate website may be redirected to a malicious site or may trigger a download of the malware. SEO poisoning is the manipulation of search engine results (e.g., through specific keywords) such that malicious links appear near the top of search results, increasing the chance that a user will select them. Deceptive download pages are webpages designed to look like legitimate download sites for well-known software products, but instead distribute the malware once a user initiates the download.

10. Once executed, the signed malware is used by the actors to establish initial access, perform data collection, enable lateral movement, and facilitate follow-on activity, including the deployment of additional malware or ransomware. MSaaS lowers the barrier to entry for cyberattacks from both a technical and financial perspective, by allowing even malicious cyber actors without advanced technical skills to deploy malware that bypasses the security controls imposed by Microsoft and other technology companies. This model has proven lucrative for both

the MSaaS operators and the malicious cyber actors relying on their services, as it supports widespread malware distribution at scale.

11. In June 2025, Microsoft became aware of a cluster of MSaaS activity traceable to Fox Tempest Defendants. As a result, DCU began investigating Fox Tempest Defendants and the users of their service.

CERTIFICATE ABUSE ENTERPRISE DEFENDANTS

12. Based on our investigation, I believe that Fox Tempest Defendants are cybercriminals who enable the Certificate Abuse Enterprise. Since May 2025, Fox Tempest Defendants have run an illicit MSaaS operation that enables Vanilla Tempest Defendants as well as other cybercriminals, including those not named as defendants herein, to distribute malware at scale. Specifically, Fox Tempest Defendants fraudulently obtain code signing certificates from Microsoft's Artifact Signing service and sell them to Vanilla Tempest Defendants and other malicious cyber actors. DCU initiated its investigation into Fox Tempest Defendants in June 2025, shortly after the service was created and began to cause harm. Microsoft has directly observed Vanilla Tempest Defendants leveraging this capability to deliver malware that masquerades as trusted software and bypasses security controls.

13. John Doe 1 is a cybercriminal who has obtained unauthorized access to Microsoft's Artifact Signing service through fraudulent means in order to procure code signing certificates. John Doe 1 established, owns, and operates the technical infrastructure specifically designed and used by Fox Tempest Defendants to provide fraudulently obtained code signing certificates to Vanilla Tempest Defendants as well as other cybercriminals. Based on our investigation, John Doe 1 was responsible for the development and ongoing operation of the code signing service, maintained administrative access to the supporting infrastructure, and exercised technical control

over all components of the service, and upon information and belief, continues to facilitate the distribution of malware through the code signing service as of the date of this declaration.

14. John Doe 2, who operates under the alias "SamCodeSign," is a cybercriminal who serves as the customer-facing sales channel for Fox Tempest Defendants' MSaaS operation. John Doe 2 communicates directly with customers, including Vanilla Tempest Defendants, to market and sell access to fraudulently obtained code signing certificates. John Doe 2 operates the Telegram channel used by Fox Tempest Defendants to advertise and sell the code signing service. John Doe 2 actively solicits and collects cryptocurrency payments from Vanilla Tempest Defendants and other customers in exchange for such certificates and provides instructions to customers for access and use of the service. These communications and transactions are ongoing. During communications with a cooperating source supporting Microsoft's test purchase of certificates, John Doe 2 communicated in Russian and directed the source to a Google Form offering various purchase tiers for code signing. John Doe 2 processed payment for the service and provided instructions, which allowed me to successfully sign test software using a certificate and infrastructure offered by Fox Tempest Defendants.

15. Based on our investigation, I believe that John Does 3 and 4 are cybercriminals that Microsoft tracks under the designation "Vanilla Tempest," also known as "VICE SPIDER" and "Vice Society." Vanilla Tempest has been active since 2021 and is assessed by Microsoft to be a financially motivated cybercriminal group that conducts opportunistic ransomware and data-extortion campaigns targeting victims across multiple sectors. John Does 3 and 4 have purchased fraudulently obtained code signing certificates from Fox Tempest Defendants and have used those certificates to digitally sign malware. Using these certificates and Microsoft's branding without authorization, John Does 3 and 4 have disguised their malware as legitimate, trustworthy software,

including as a Microsoft product, to deploy the malware on the computers of unsuspecting victims without their knowledge or consent. Through this conduct, John Does 3 and 4 have: unlawfully accessed victims' computers and devices; exfiltrated and stolen personal and confidential information belonging to victims; deployed ransomware designed to encrypt victims' files and render their systems inoperable; and extorted victims by demanding payment in exchange for restoring access to, or suppressing disclosure of, their data. This criminal activity is ongoing and continues to cause irreparable harm to Microsoft and its customers.

FOX TEMPEST DEFENDANTS' MODUS OPERANDI

16. Based on our investigation, I have observed that Fox Tempest Defendants operate through a systematic, repeatable, and commercialized process designed to fraudulently obtain Microsoft code signing certificates and sell access to those certificates to Vanilla Tempest Defendants and other cybercriminals, for the purpose of signing malware and distributing the malware to victims. The specific methods and patterns of conduct employed by Fox Tempest Defendants are described below.

A. Creation of Fraudulent Microsoft Tenants to Obtain Access to Code Signing Certificates

17. Since May 2025, Fox Tempest Defendants have systematically established more than 580 fraudulent Microsoft tenants to gain unauthorized access to Microsoft's Artifact Signing service. Microsoft's "Artifact Signing," launched in 2024, is a fully managed, end-to-end code signing service intended to be used by software developers. 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. Artifact Signing employs a digest-signing methodology, consistent with

standard practices of certificate authorities for securing software distribution. Under this approach, only a cryptographic hash of the relevant file is transmitted to the signing service; the underlying file itself is not transmitted. Accordingly, the signing service does not have the ability to inspect the underlying code prior to executing the signing operation.

18. 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, a user could go 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. To activate an Azure subscription required for Artifact Signing, the user must click on a verification email sent by Microsoft, which confirms that the user controls the provided email address. A user must also agree to Microsoft's Terms of Use for Artifact Signing, a copy of which is attached to the Complaint as **Exhibit 1**.

19. 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 systems and processes that aim to prevent untrustworthy parties, including malicious cyber actors, from using Microsoft products and services. During this process, Microsoft requires the user to provide information such as the organization's legal name, business address, first name, last name, domain name, company website, and contact email addresses. Microsoft's entity verification system screens applicants across multiple sources to validate their identities and 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. Microsoft also leverages internal datasets, threat and fraud indicators, and third-party analysis in the validation process. For individual identity verification, Microsoft's verification system

leverages a third-party solution that provides the capabilities necessary to confirm the authenticity of the provided government-issued identification.

20. To activate Azure subscriptions associated with Artifact Signing, Fox Tempest Defendants have verified their email addresses by clicking a verification link sent by Microsoft. Fox Tempest Defendants have also used these email addresses as multi-factor authentication methods for their Azure accounts.

21. To bypass the Microsoft entity and identity validation systems and processes required to access Artifact Signing, Fox Tempest Defendants have employed a range of fraudulent techniques. Fox Tempest Defendants have exploited the partner sign-up process by registering new domains using fake names and contact information. They have also submitted fake government-issued identification documents, created fake shell companies and business registration documents, and in at least one instance, impersonated a legitimate company.

B. Development of Infrastructure to Run the MSaaS Operation

22. Fox Tempest Defendants have used two primary channels to distribute fraudulently obtained code signing certificates to the Vanilla Tempest Defendants and other cybercriminals.

23. First, Fox Tempest Defendants operate a website, signspace.cloud, to deliver their code signing service to Vanilla Tempest Defendants and other malicious cyber actors. The signspace.cloud website allows Vanilla Tempest Defendants and other customers to upload and sign their code using the certificates fraudulently obtained by Fox Tempest Defendants. After purchasing certificates, customers sign in to the website's user page where they upload their malicious code to be signed and download the signed malicious code with the certificate added. **Figure 1** is a screenshot of the login page to the signspace.cloud website. The website includes an

administrator panel that allows Fox Tempest Defendants to manage each customer's page and provide them with certificates.

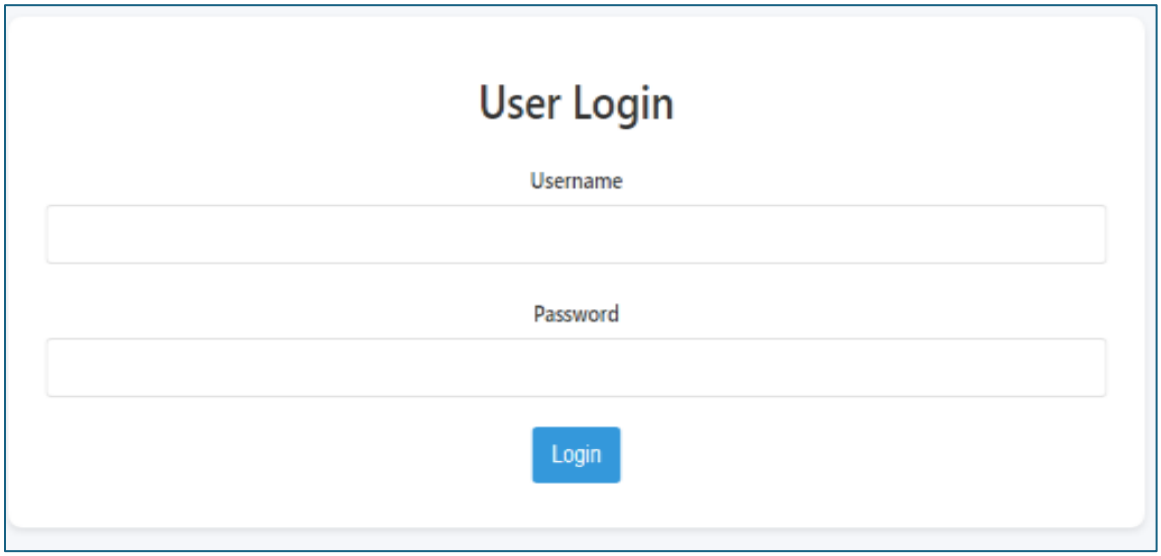


FIGURE 1

24. The domain name registrar[1] for signspace.cloud is GoDaddy.com LLC ("GoDaddy"), a company based in the United States. Aruba PEC SpA, a company based in Italy, is the registry[2] for the ".cloud" domain. The website is hosted by Freak Hosting, a company based in the United Kingdom, using servers located in Germany, and by Wavecom, a company based in Estonia, using servers located in Estonia. The known IP addresses associated with servers hosting Fox Tempest Defendants' signspace.cloud website are 31.59.58[.]9 and 38.180.163[.]50. Additional information on the signspace.cloud domain is attached to the Complaint as **Exhibit 2**. Upon information and belief, Fox Tempest Defendants maintain control of the signspace.cloud website and may continue to use it to operate their code signing service.

[1] 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.
[2] 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.

25. In the course of our investigation, I also identified a GitHub repository containing code that runs the signspace.cloud website and manages its back-end and front-end processes. The repository belongs to a GitHub user account that also controls multiple other repositories. These repositories include an additional contributor whose profile publicly identifies the individual as the person suspected to be John Doe 1. According to the GitHub logs I reviewed, this contributor's account created the repository for the code signing service. The logs also reveal that both the repository owner's account and the contributor's account share identical device cookies, client identifiers, and source IP addresses. Furthermore, the contributor accessed their GitHub account using the same IP addresses of the servers that host signspace.cloud.

26. Second, beginning in January 2026, Fox Tempest Defendants began using virtual machines[3] to operate their code signing service. The transition coincided with Microsoft's implementation of anti-fraud measures that 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 Microsoft's Remote Desktop Protocol and instruct them to follow specific steps to sign their code. Based on a cryptocurrency payment from Vanilla Tempest Defendants to SamCodeSign following the transition to virtual machines, I believe Vanilla Tempest Defendants are among the customers who have received such access and instructions. These virtual machines are hosted by RouterHosting LLC (d/b/a "Cloudzy"), a company registered in Cyprus and headquartered in Dubai, United Arab Emirates. DCU 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

[3] A virtual machine is a software-based emulation of a physical computer that runs an operating system and applications as an independent machine within another host computer.

addresses associated with the virtual machines is attached to the Complaint as **Appendix B**.

27. The shift from the signspace.cloud website to virtual machines demonstrates Fox Tempest Defendants' awareness of potential detection and their efforts to evade enforcement. In communications with a cooperating source during a test purchase, 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."[4]

C. Marketing and Sale of Code Signing Certificates

28. Fox Tempest Defendants use Telegram, a cloud-based instant messaging service, to communicate with customers and potential customers about the service. John Doe 2, known by the alias SamCodeSign, operates the Telegram channel for Fox Tempest Defendants and has sold access to the code signing service via an auction, conducted through Google Sheets, or via direct purchase through a Google Form.

29. Metadata from a Google Sheet used by SamCodeSign to manage the auction of code signing certificates indicated that the Gmail 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, linking these marketing operations to the fraudulent tenant creation.

VANILLA TEMPEST DEFENDANTS' ATTACK CHAIN

30. Vanilla Tempest Defendants rely on Fox Tempest Defendants' MSaaS infrastructure to create fraudulently signed code that enables their malicious software to bypass security controls and gain access to victim computers. The following paragraphs describe the step-

[4] 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.

by-step attack chain employed by the Vanilla Tempest Defendants, from the use of the code signing service through deployment of malware on victim computers.

A. Acquisition of Code signing Services

31. Vanilla Tempest Defendants and other cybercriminals purchase code signing certificates from Fox Tempest Defendants by making cryptocurrency payments to a wallet controlled by Fox Tempest Defendants. I identified five payments that occurred between June 2025 and January 2026 between wallets attributed by Chainalysis Reactor—a tool that traces and analyzes cryptocurrency transactions—to Vanilla Tempest Defendants (as senders) and SamCodeSign (as recipient), which I discuss in more detail below. Based on our investigation, I believe that Vanilla Tempest Defendants use the service with the knowledge that the certificates are fraudulently obtained through Microsoft's Artifact Signing service. Following payment, Fox Tempest Defendants provide Vanilla Tempest Defendants with access to their MSaaS infrastructure.

B. Signing of Oyster Malware

32. Once Vanilla Tempest Defendants obtain access to the code signing service, they use it to digitally sign their malware with certificates fraudulently obtained through Microsoft's Artifact Signing service. Microsoft has observed Vanilla Tempest Defendants signing malware known as "Oyster" (also known as "Broomstick" or "CleanupLoader") using certificates from Fox Tempest Defendants. **Figure 2** is a screenshot of a now-revoked certificate that Vanilla Tempest purchased from Fox Tempest Defendants to sign Oyster malware. Oyster malware enables malicious cyber actors to gather system information, extract credentials, issue commands, deploy additional malware (including ransomware), and ensure ongoing access to infected endpoints through the use of scheduled tasks.


Certificate
General
Details
Certificate Information
This certificate has been revoked by its certification authority.
Issued to: GALVIN & ASSOCIATES LLC
Issued by: Microsoft ID Verified CS EOC CA 01
Valid from 6/6/2025 to 6/9/2025
Install Certificate...
Issuer Statement
OK

FIGURE 2

33. Because the malware is signed with a valid certificate from Microsoft's Artifact Signing service, the Windows operating system recognizes the malware as legitimate software. This digital signature causes the operating system to suppress security warnings that would otherwise alert the user to the suspicious nature of the software, including Microsoft's SmartScreen filter and User Account Control prompts. In Windows 11, the SAC feature, which is designed to block unsigned or low-reputation software entirely, permits the signed malware to execute, rather than blocking its access, because it carries a valid digital signature.

C. Deployment of Signed Malware against Victims

34. 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.

35. Vanilla Tempest Defendants subsequently distribute the signed malware via malvertising, search engine optimization poisoning, and fake download sites.

36. In one of their campaigns, first observed by Microsoft in September 2025, Vanilla Tempest Defendants redirected victims searching for Microsoft Teams to attacker-controlled advertisements and fraudulent download pages. Vanilla Tempest Defendants 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®. **Figure 3** is a screenshot of a fake Microsoft Teams download site created by Vanilla Tempest Defendants.

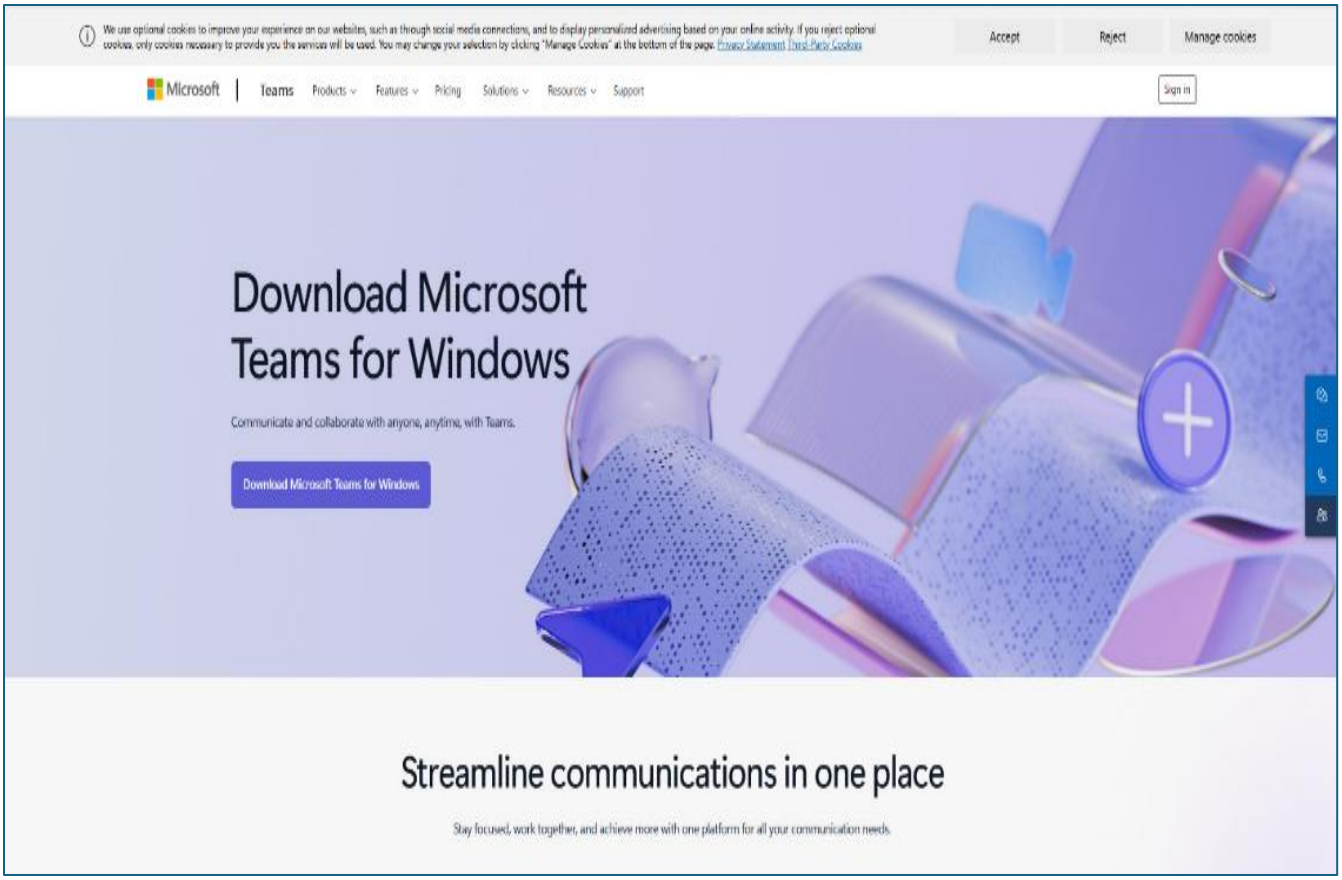


FIGURE 3

37. 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. Rhysida ransomware encrypts victims' files and renders their computers unusable, allowing Vanilla Tempest Defendants to extort victims by demanding payment in exchange for restoring access to their data. **Figure 4** depicts the attack chain, including the respective roles of the Fox Tempest and Vanilla Tempest Defendants in enabling it.

FIGURE 4

D. Microsoft's Disruption Efforts and Continuing Harm

38. In October 2025, Microsoft disrupted this Vanilla Tempest campaign by revoking more than 200 certificates that the Vanilla Tempest Defendants had fraudulently obtained and used in fake Microsoft Teams setup files to deliver the Oyster backdoor and deploy Rhysida ransomware.[5]

39. Despite this disruption, Vanilla Tempest Defendants have continued their criminal activity, including by using fake Microsoft Teams installers to deliver malware signed by fraudulently obtained certificates. Furthermore, Microsoft identified a Bitcoin payment from a cryptocurrency wallet attributed to Vanilla Tempest Defendants to a wallet attributed to SamCodeSign in January 2026, following the shift to virtual machine-based distribution infrastructure for the code signing service. These ongoing activities demonstrate that Vanilla

[5] *See generally* Microsoft Security Intelligence (@MsftSecIntel), *In early October 2025, Microsoft disrupted a Vanilla Tempest campaign by revoking over 200 certificates that the threat actor had*, X (formerly Twitter) (Oct. 15, 2025, 6:44 PM), https://x.com/MsftSecIntel/status/1978592789857251490 (detailing the Vanilla Tempest attack chain and Microsoft's disruption efforts).

Tempest Defendants' attacks are ongoing and will continue unless and until this Court grants the requested injunctive relief.

40. In total, 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 fraudulent tenants created by the Fox Tempest Defendants.

41. Based on our investigation, I believe that Fox Tempest Defendants, Vanilla Tempest Defendants, and other cybercriminals operate as parts of a single coordinated criminal operation, the Certificate Abuse Enterprise. Each group is dependent on the other to achieve their shared objective of deploying malware at scale to profit from impacted victims. Fox Tempest Defendants provide the underlying capability by systematically creating fraudulent Microsoft tenants, fraudulently procuring code signing certificates, and commercializing access to those certificates through their code signing infrastructure. Without customers to purchase and deploy the signed malware, Fox Tempest Defendants' operation would have no purpose and would not generate the revenue necessary to sustain the operation. Vanilla Tempest Defendants, in turn, rely entirely on Fox Tempest Defendants' fraudulent certificates to circumvent security controls inherent in computing operating systems and make their malware appear legitimate. Without access to these certificates, Vanilla Tempest Defendants could not execute their attack chain as effectively. Furthermore, repeated cryptocurrency payments occurring between the two groups from June 2025 to January 2026 demonstrate the continuing nature of the scheme.

TEST PURCHASES

42. Between February and March 2026, I, with the assistance of a cooperating source,[6] conducted two test purchases from Fox Tempest Defendants' code signing service.

43. To initiate the purchases, I worked with the cooperating source to communicate with SamCodeSign on Telegram, expressing an interest in purchasing certificates from the code signing service. SamCodeSign uses Telegram to advertise the Fox Tempest Defendants' code signing service. **Figure 5** is a screenshot of a Telegram message from SamCodeSign to members of the Telegram group marketing access to certificates obtained by Fox Tempest Defendants.

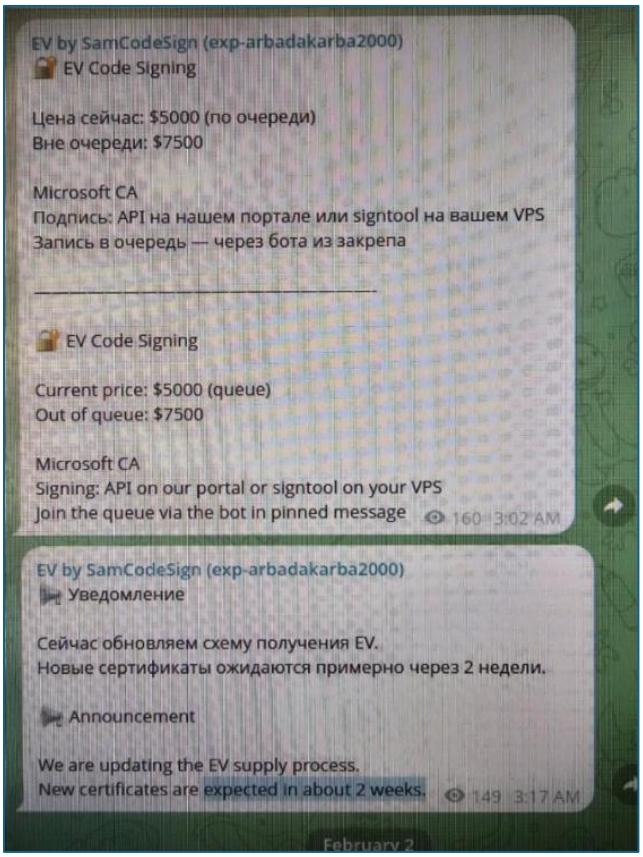


FIGURE 5

[6] The cooperating source is a security research firm that Microsoft has previously worked with on other disruption operations, and who has proven reliable and trustworthy in those operations, and who assisted in this matter with access to the Telegram channel used by SamCodeSign.

44. In the group, SamCodeSign directed customers to use a Google Form to select the purchase type, corresponding 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, provide contact information, and include any additional comments. **Figure 6** is a screenshot of the Google Form linked in the message from SamCodeSign.

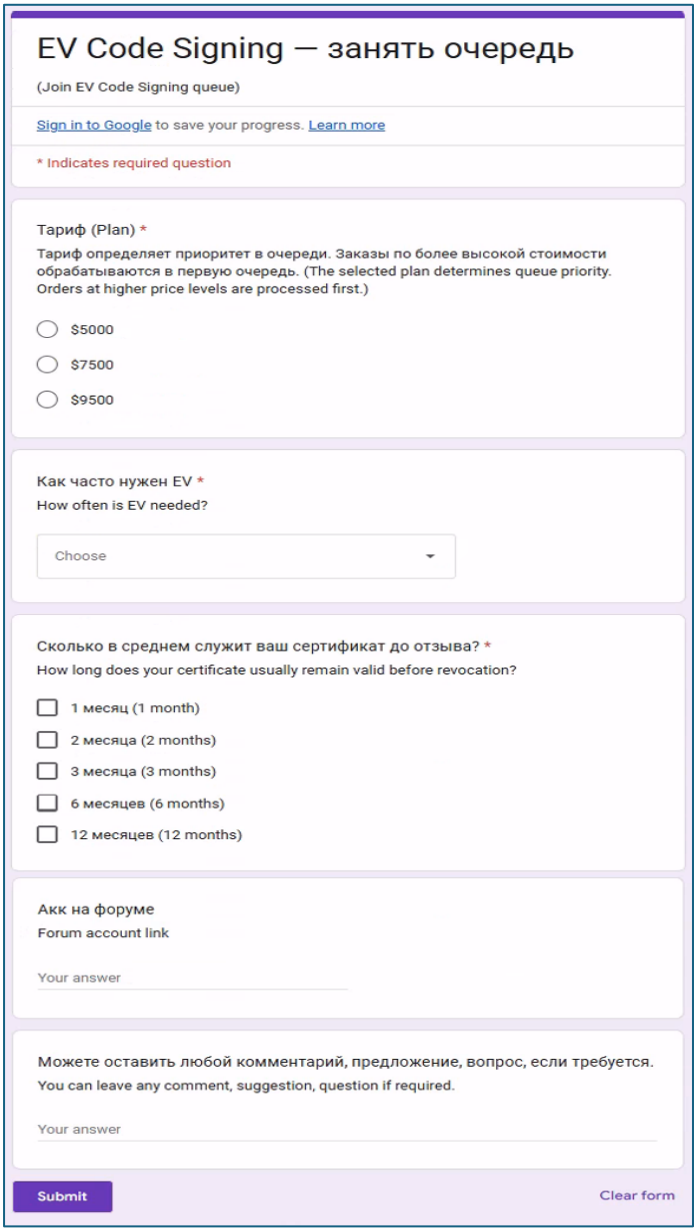


FIGURE 6

45. After the cooperating source completed the Google Form, SamCodeSign sent a direct message to the source on Telegram requesting payment via a Bitcoin address. **Figure 7** is a screenshot of the Telegram message from SamCodeSign providing the Bitcoin address.

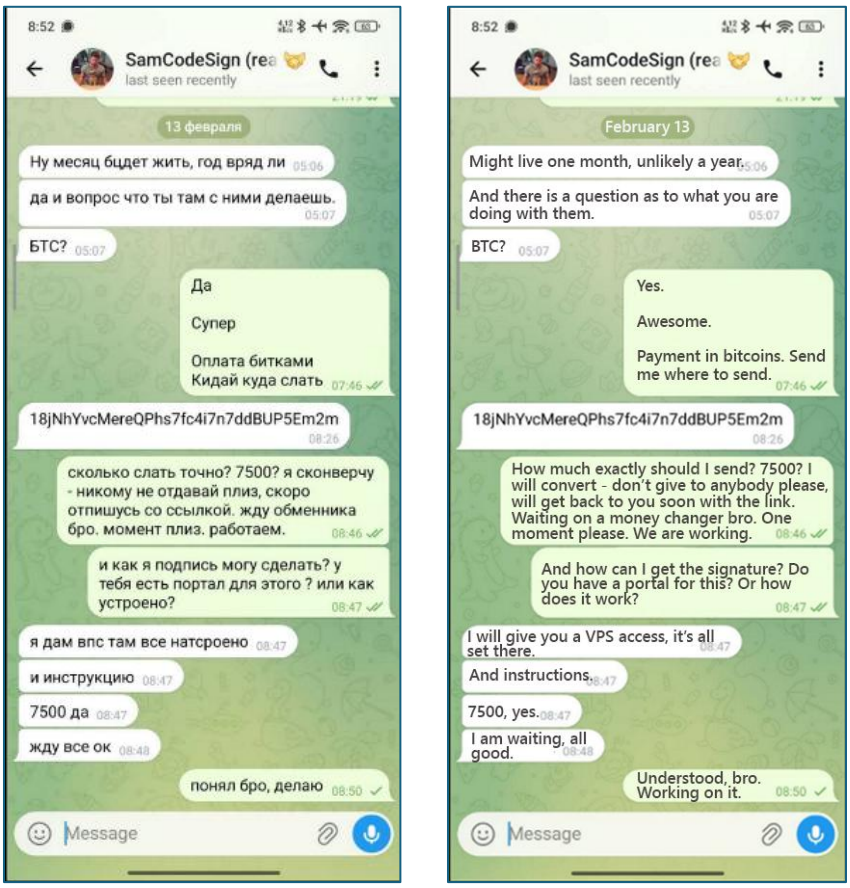


FIGURE 7

46. Following payment to the Bitcoin address, SamCodeSign sent information to access a virtual machine and complete the code signing process using the machine. **Figure 8** is a screenshot of the Telegram message from SamCodeSign providing information on obtaining access to the virtual machine and the code signing process. For the second test purchase, the cooperating source communicated with SamCodeSign directly to facilitate the purchase and I did not have to complete the Google Form. **Figure 9** is a screenshot of the Telegram message from SamCodeSign facilitating the second purchase.

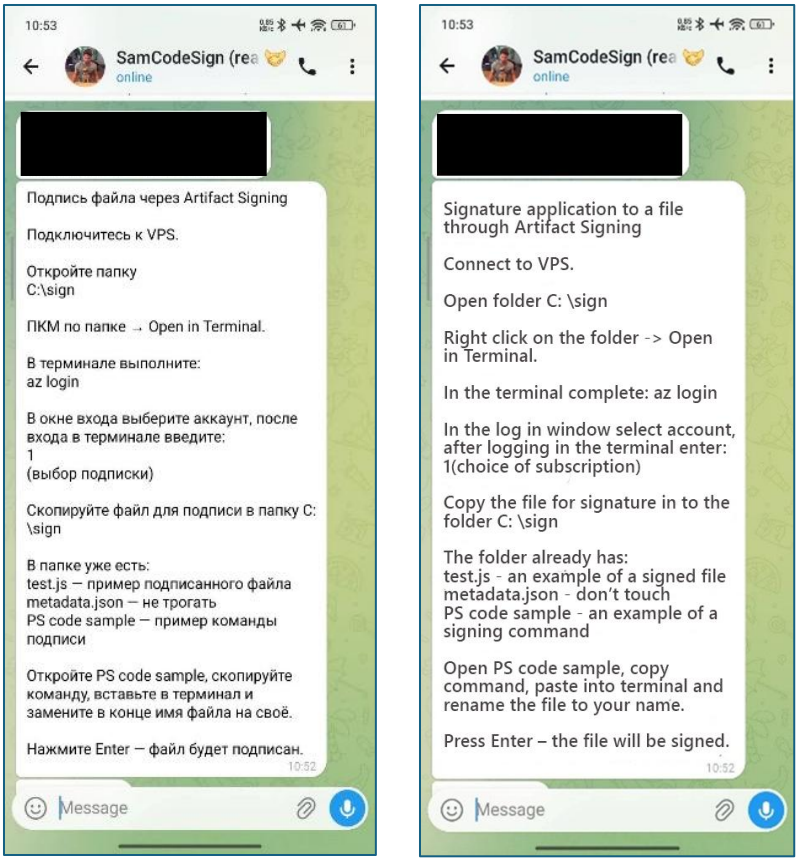


FIGURE 8

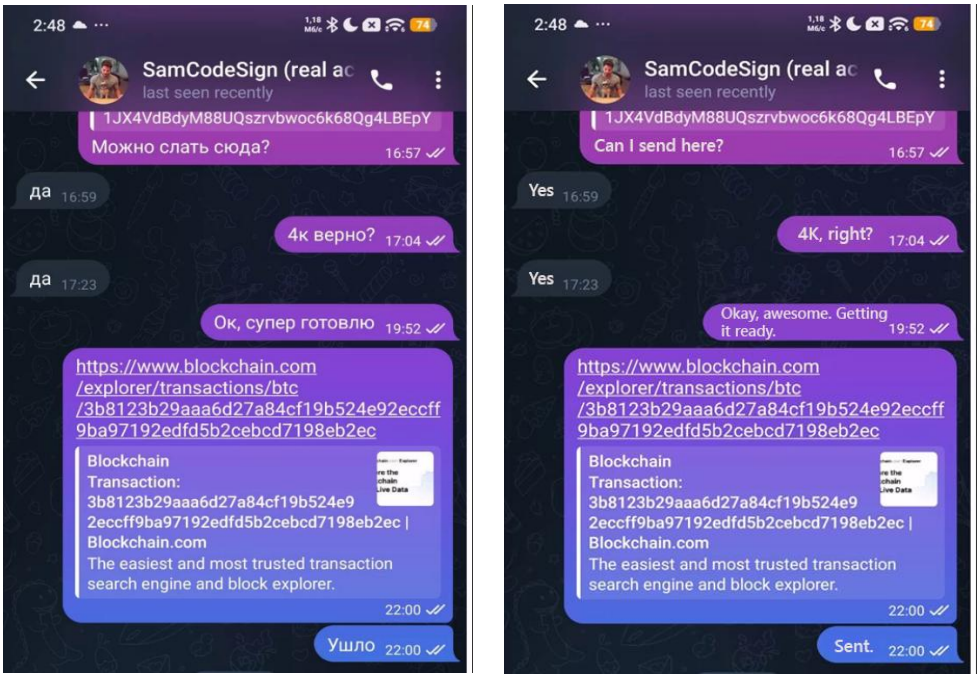


FIGURE 9

47. During the course of the messages with SamCodeSign, the cooperating source asked SamCodeSign whether the signspace.cloud website belonged to him, to which SamCodeSign responded affirmatively. In the message, 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." **Figure 10** is a screenshot of this message from SamCodeSign.

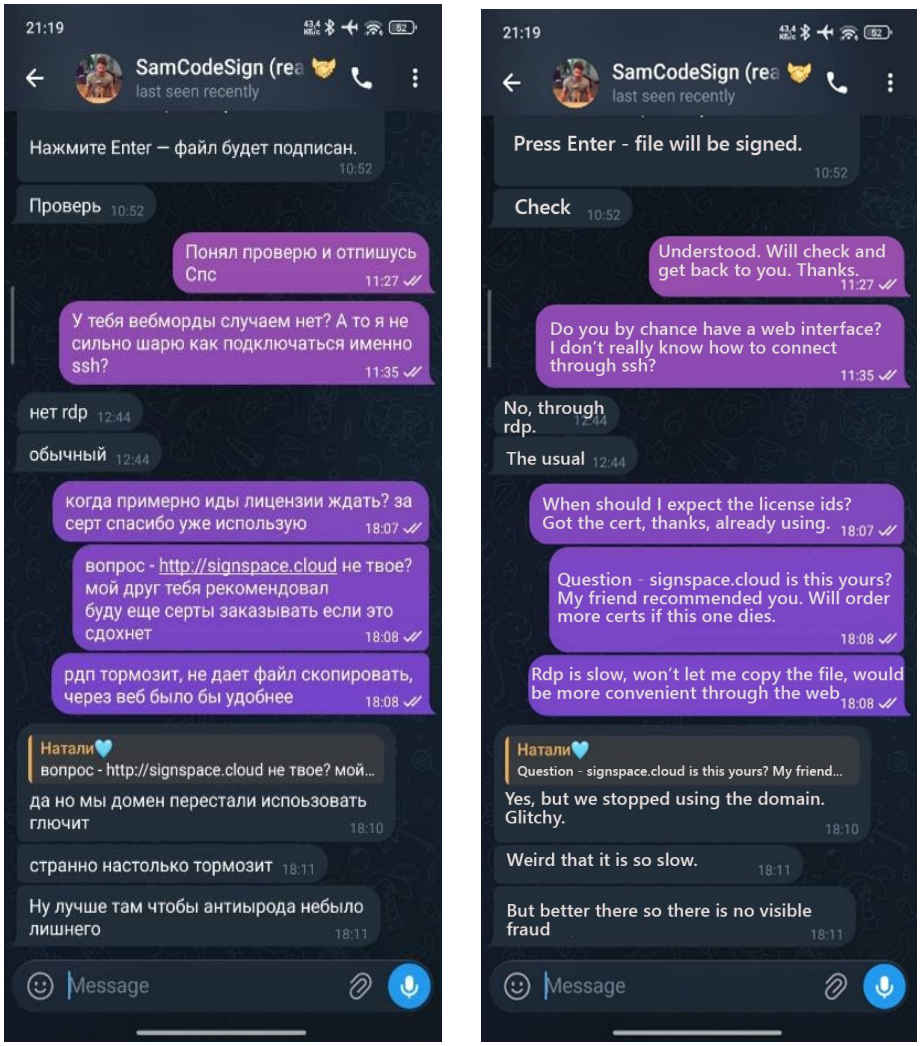


FIGURE 10

48. In each test purchase, I used the credentials that SamCodeSign provided to remotely access the virtual machine to conduct the code signing. **Figure 11** is a screenshot of the remote

desktop connection process to access the virtual machine. **Figure 12** is a screenshot of the desktop of the virtual machine upon logging in.

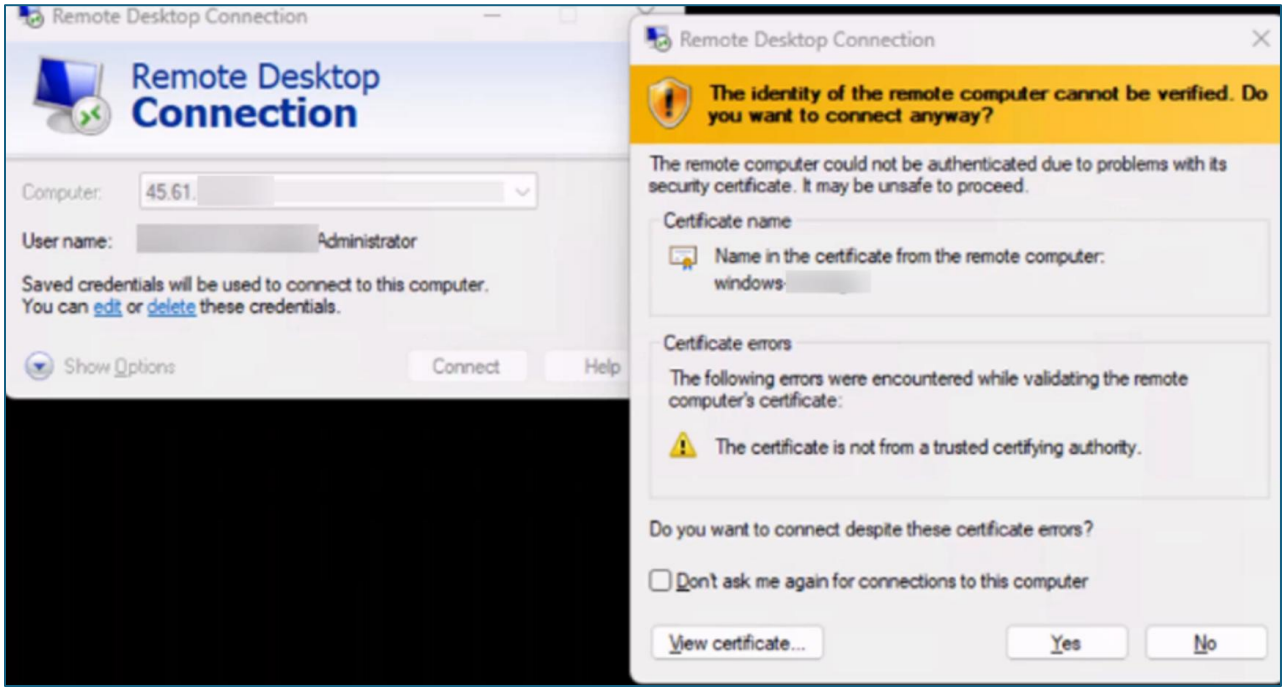


FIGURE 11

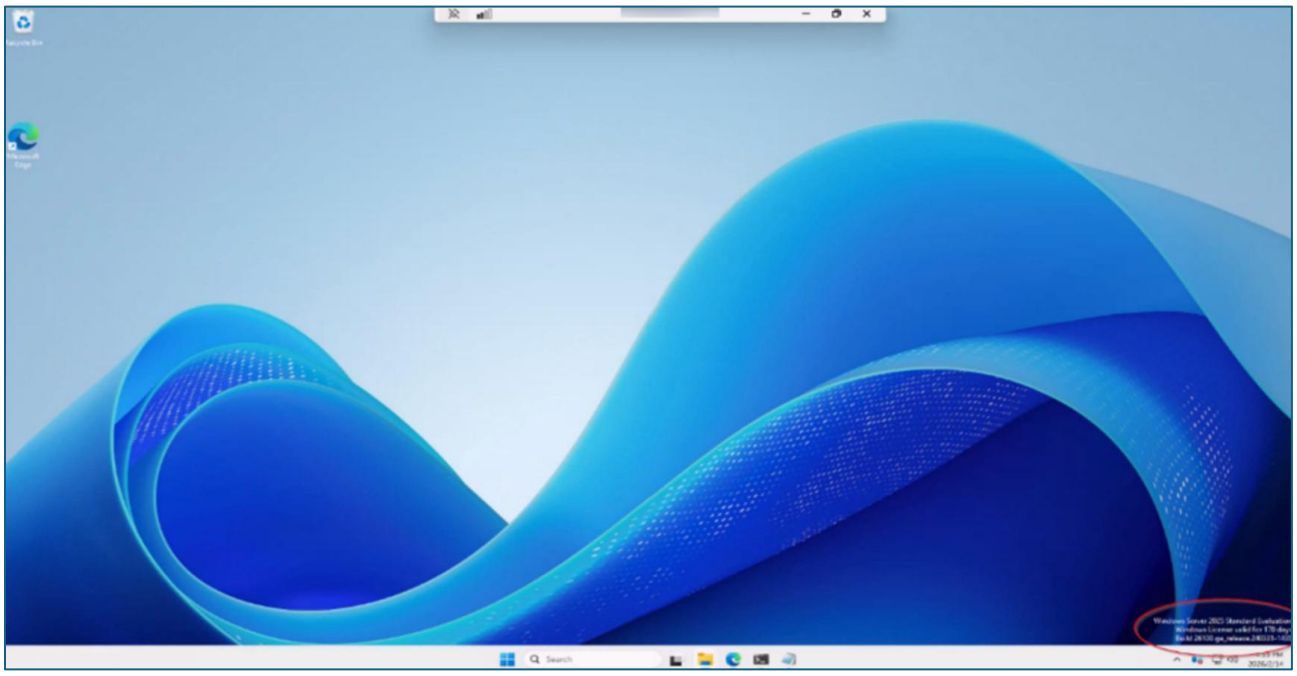


FIGURE 12

49. Upon remotely accessing the machine, I identified an accessible folder (C:\sign) containing three files: metadata.json, test.js, and PS code sample.txt. **Figure 13** is a screenshot of this folder.

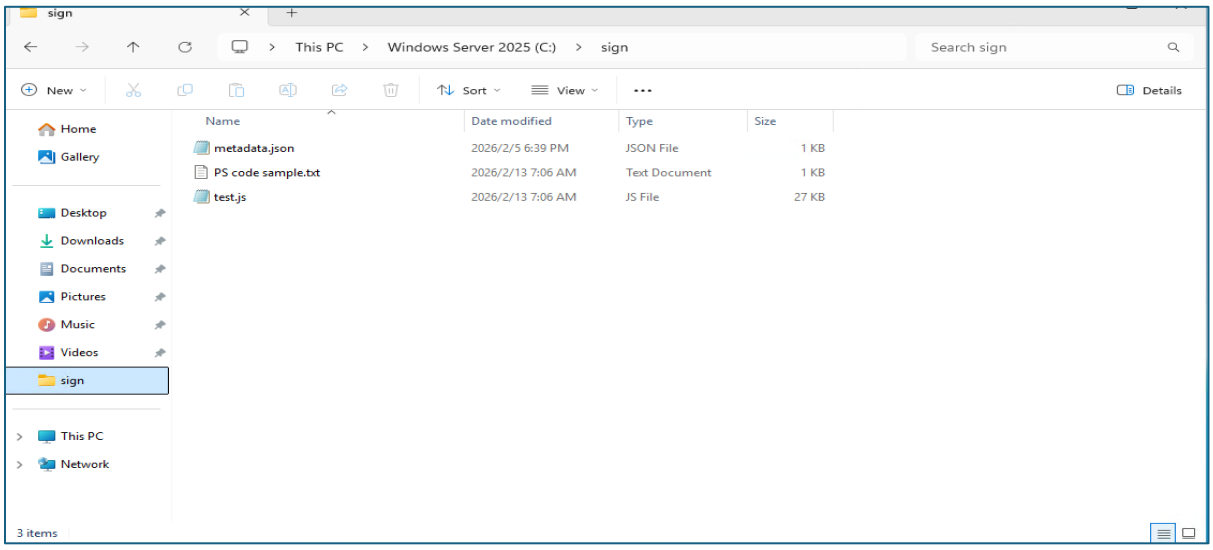


FIGURE 13

50. 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. **Figure 14** is a screenshot of the contents of the file.

FIGURE 14

51. 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. **Figure 15** is a screenshot of the certificate for the test file.

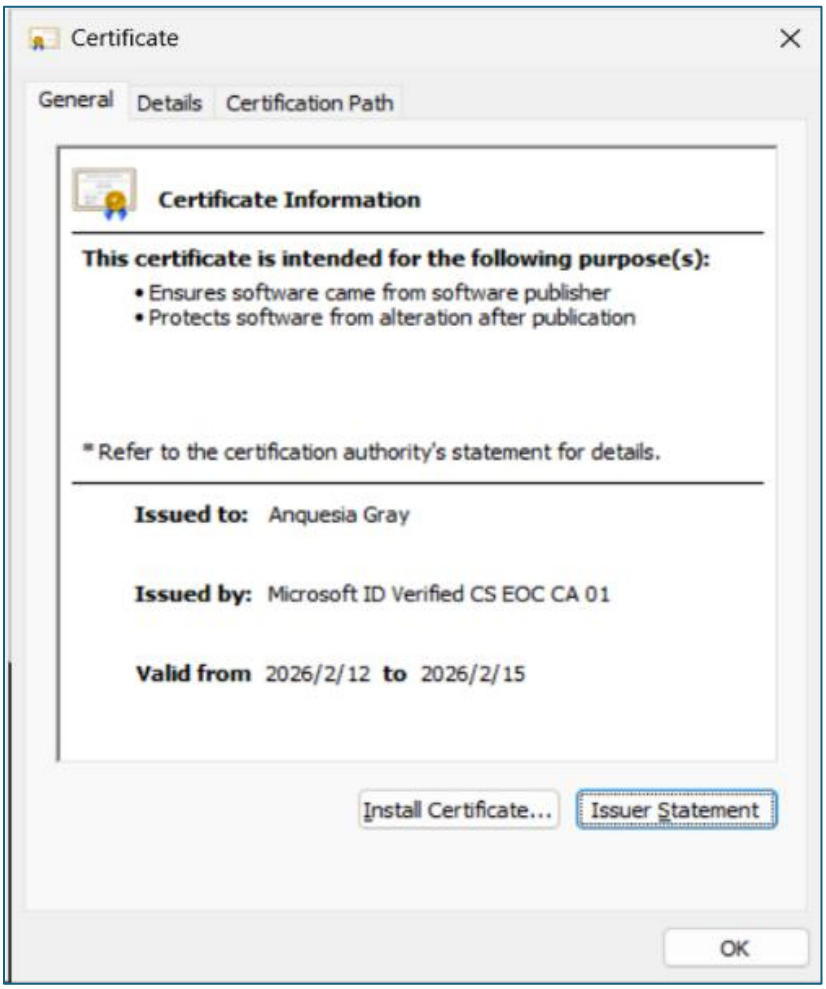


FIGURE 15

52. 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 command shown in **Figure 16** uses Microsoft's signtool.exe command to sign files digitally using SHA-256 hashing, an Azure code signing library, and metadata specified in the configuration file. The signature is timestamped via Microsoft's timestamping service (timestamp.acs.microsoft.com) to ensure validity.

```
& "C:\Program Files (x86)\Windows Kits\10\bin\10.0.26100.0\x64\signtool.exe" sign /v /debug /fd SHA256 /tr "http://timestamp.acs.microsoft.com" /td SHA256 /dlib
"C:\Users\Administrator\AppData\Local\Microsoft\MicrosoftArtifactSigningClientTools\Azure.CodeSigning.Dlib.dll" /dmdf "C:\sign\metadata.json" "test.js"
```

FIGURE 16

53. Using the virtual machine, I signed a file. First, I authenticated to the appropriate Azure account using the "az login" command within a terminal.

54. Second, in the login window, I was prompted to choose which subscription to use and selected the only available subscription associated with the tenant. *See* **Figures 17** and **18**.

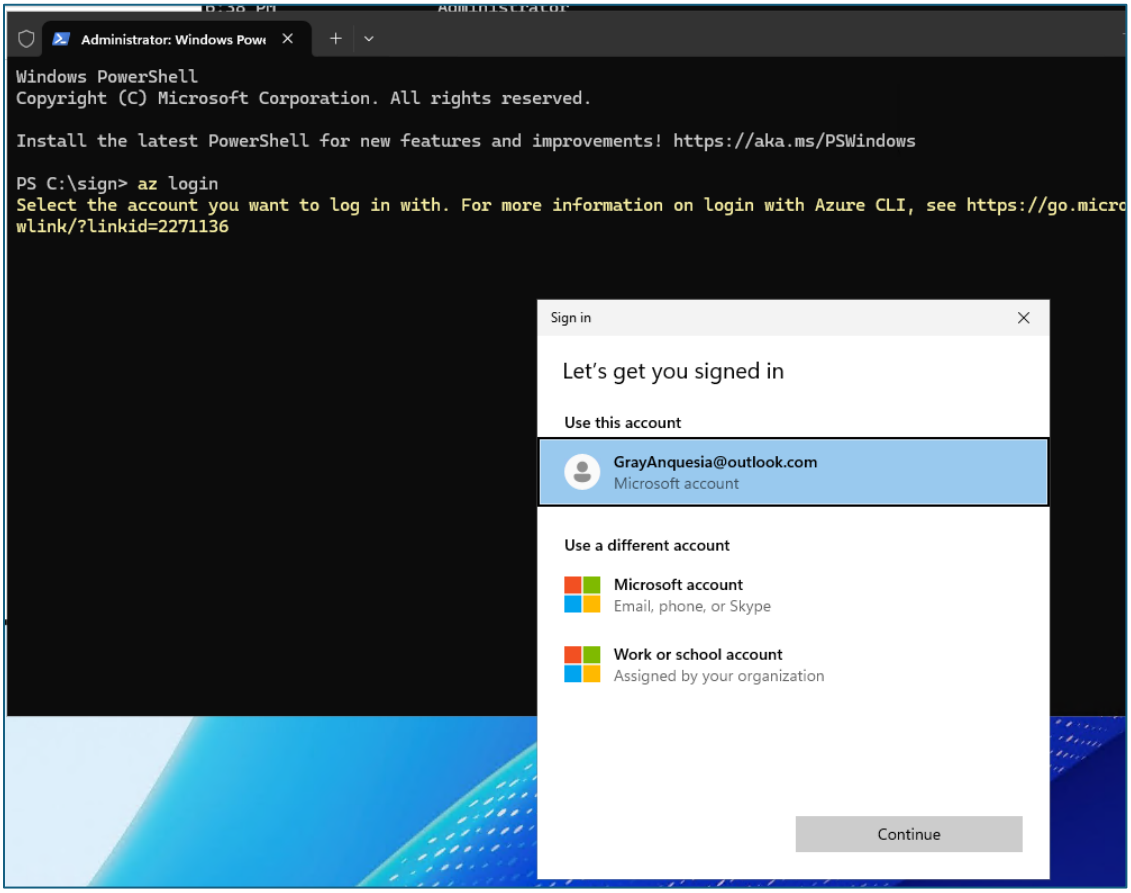


FIGURE 17

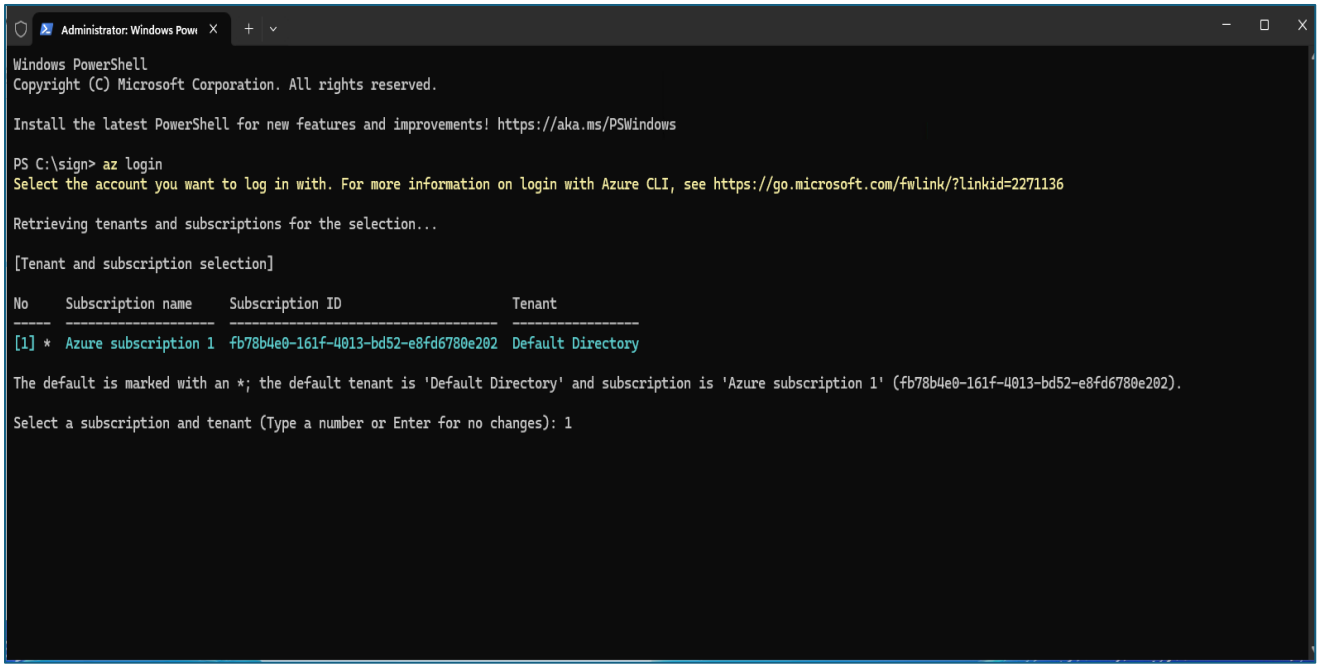


FIGURE 18

55. Third, I copied a test file into the C:\sign folder, which contained the configuration file and the sample containing the signing command. *See* **Figure 19**.

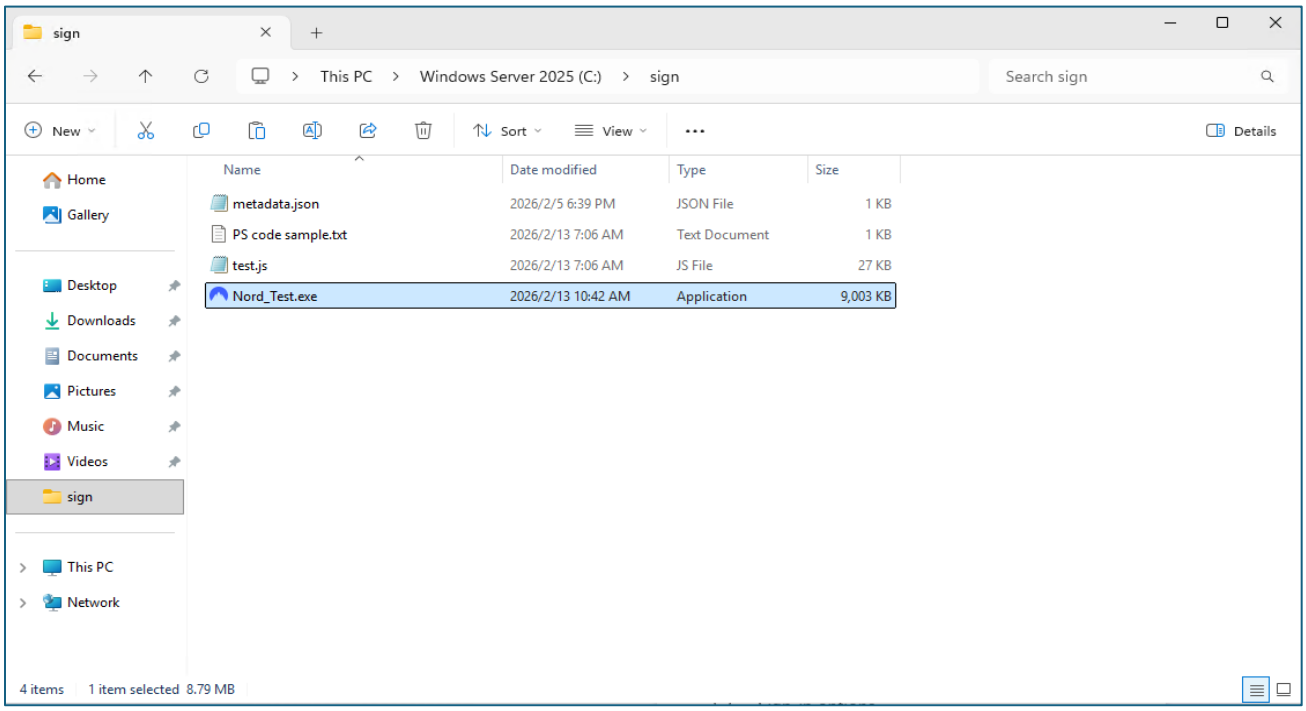


FIGURE 19

56. Fourth, I executed the signing command from the code sample file. *See* **Figure 20**.

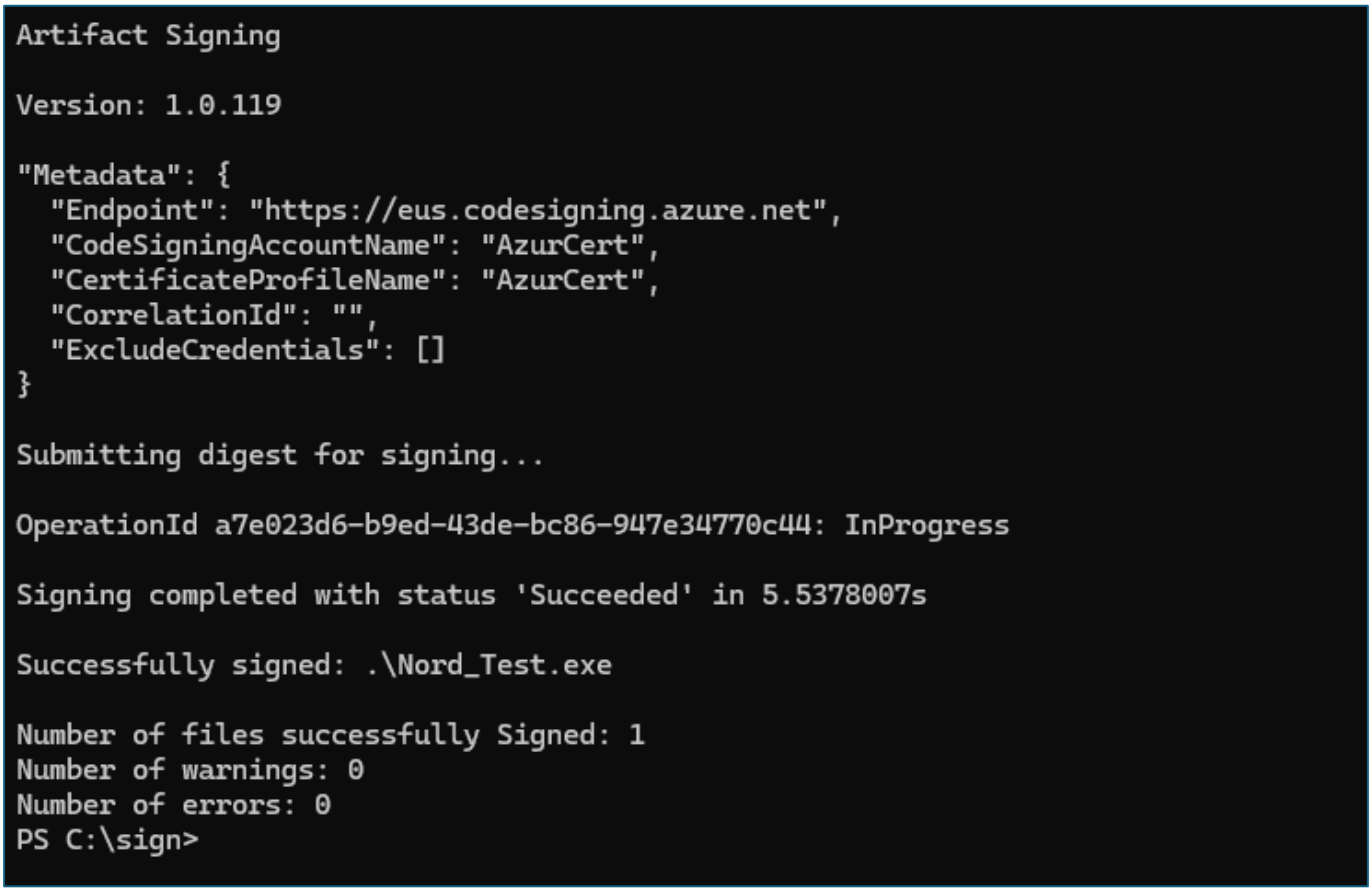


FIGURE 20

57. Upon execution, the test file was successfully signed with the certificate provided by the Fox Tempest Defendants. **Figure 21** is a screenshot of the original certificate for the test file before executing the signing command. **Figure 22** is a screenshot showing the certificate for the test file after executing the signing command, which changed the certificate issuer to Microsoft.

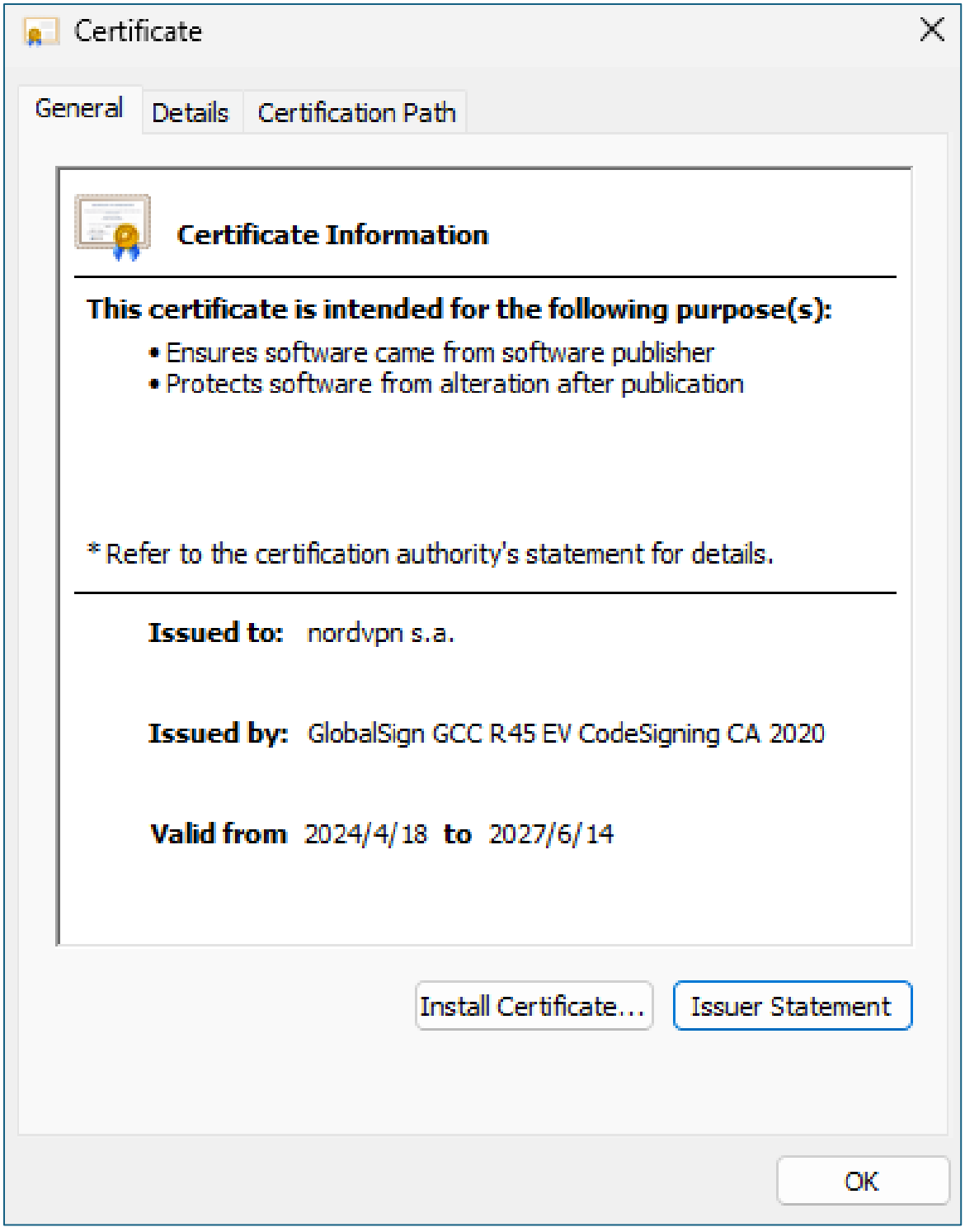

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued to: nordvpn s.a.
Issued by: GlobalSign GCC R45 EV CodeSigning CA 2020
Valid from 2024/4/18 to 2027/6/14
Install Certificate...
Issuer Statement
OK

FIGURE 21

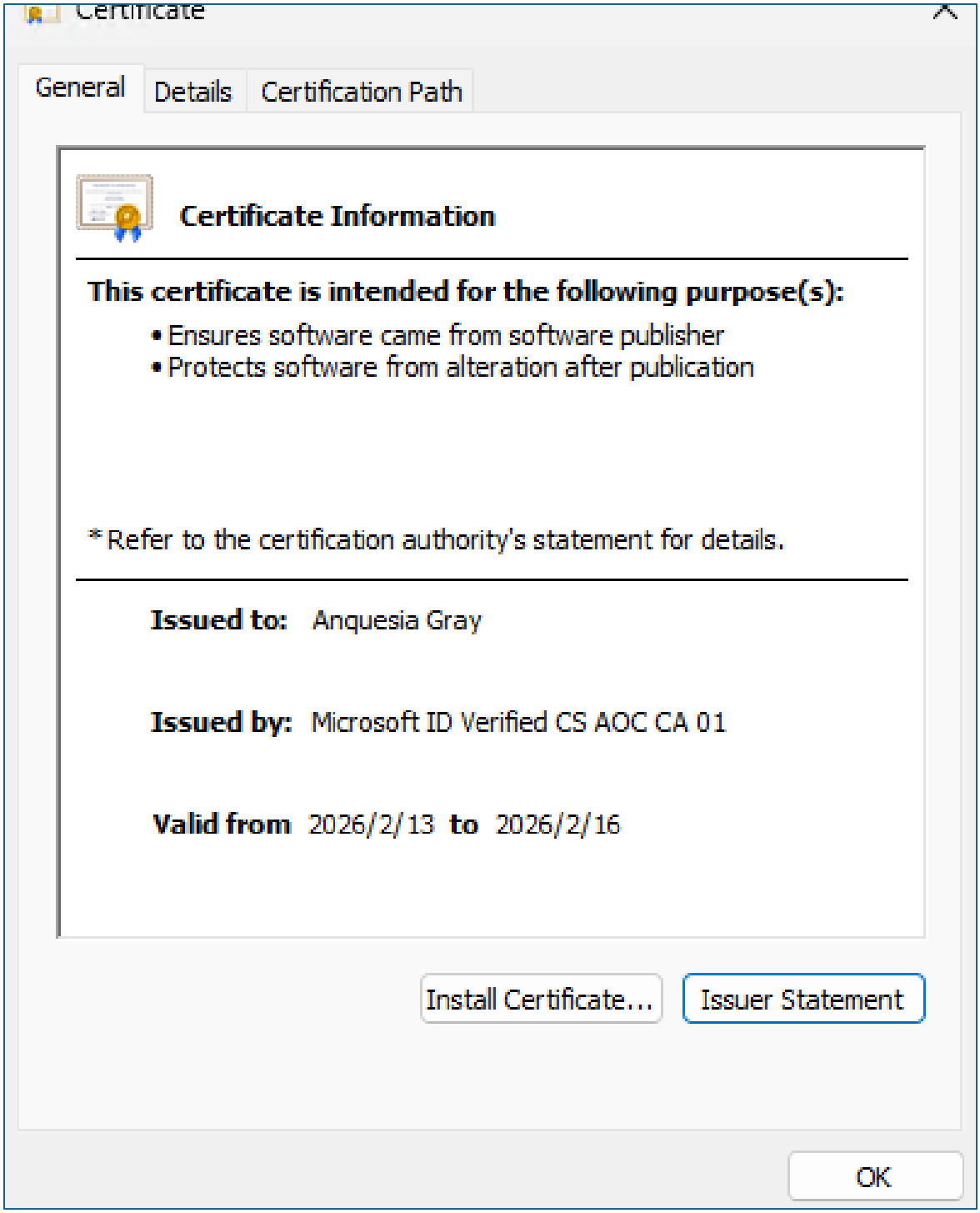

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued to: Anquesia Gray
Issued by: Microsoft ID Verified CS AOC CA 01
Valid from 2026/2/13 to 2026/2/16
Install Certificate...
Issuer Statement
OK

FIGURE 22

58. During the first test purchase, I collected information on the Microsoft tenant and subscription used by the Fox Tempest Defendants to facilitate the code signing process. **Figure 23** shows the TenantID 6d4ee6bc-fd52-4d56-b576-fc238704cdd9 and Subscription ID fb78b4e0-161f-4013-bd52-e8fd6780e202.

FIGURE 23

59. My review of the AzurCert records for this subscription number showed that eight certificates were created with this subscription. *See* **Figure 24**.

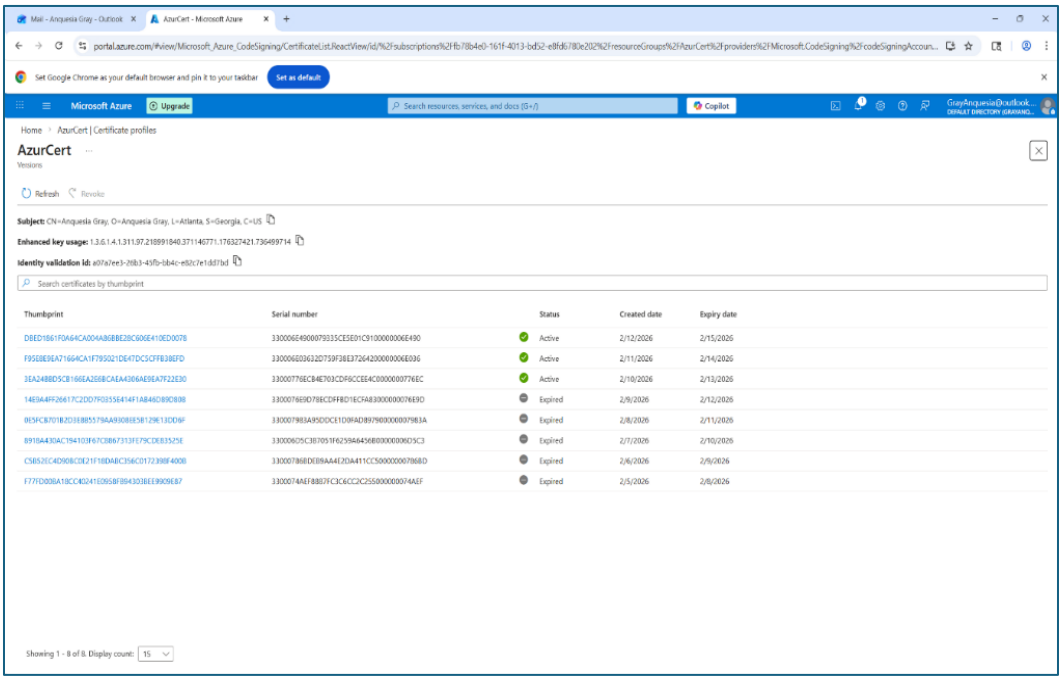


FIGURE 24

60. Based on our investigation, I believe the virtual machines contain critical evidence concerning the Certificate Abuse Enterprise's operations. Such evidence could include configuration files and access logs showing who operated the infrastructure and their locations, malware samples and signing artifacts demonstrating the use of fraudulently obtained certificates, and financial and account records. This information is essential to identifying and attributing conduct to the John Doe Defendants, uncovering additional victims, and supporting Microsoft's claims in this action.

CRYPTOCURRENCY PAYMENT AND FINANCIAL TRACING

61. Fox Tempest Defendants required payment in cryptocurrency for their certificate signing services. As part of the test purchases, SamCodeSign provided the following Bitcoin addresses for payment: 18jNhYvcMereQPhs7fc4i7n7ddBUP5Em2m and 1JX4VdBdyM88UQszr vbwoc6k68Qg4LBEpY. *See* **Figures 7** and **9** above for screenshots of messages from SamCodeSign including these Bitcoin addresses. I executed payment to these addresses in exchange for the certificates. **Figure 25** illustrates the payment to these wallets.

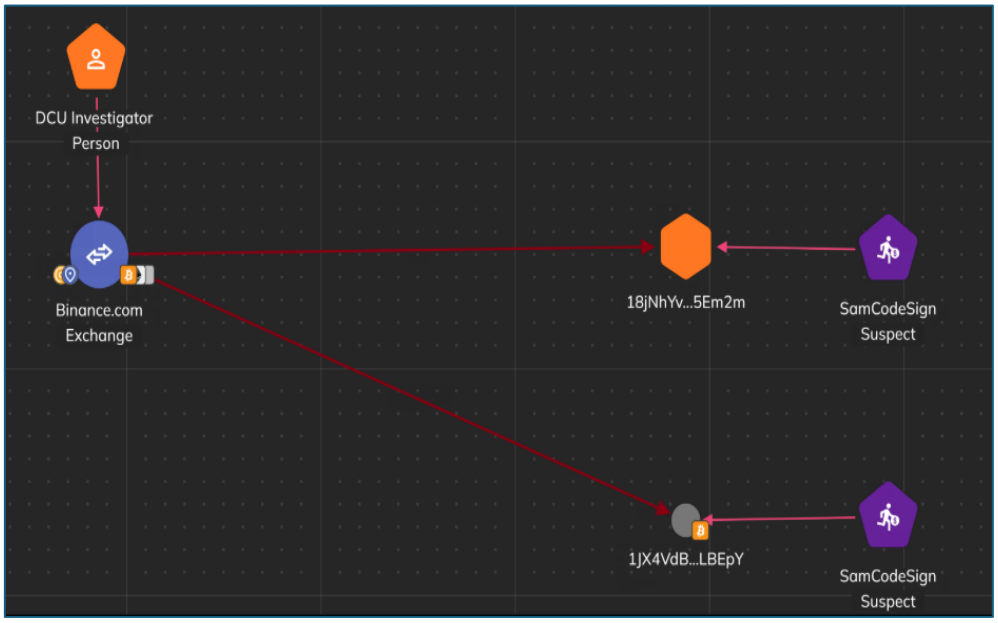


FIGURE 25

62. Using the information provided by Fox Tempest Defendants, open-source intelligence, and Chainalysis Reactor, I conducted a comprehensive review of the transactions associated with the test purchases. Chainalysis Reactor groups cryptocurrency addresses controlled by the same entity and ties those clusters to specific real-world entities based on information gleaned 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.

63. The analysis I produced using Chainalysis Reactor shows that my payments were routed through multiple intermediate cryptocurrency wallet addresses. In both transactions, the funds first passed through intermediary Bitcoin wallet addresses bc1q6tlttm9sg5uh9uv4grr8tsuvsx k367haj5xkxw and bc1qvwxqg6jzlhky0cm6zf5my92c5qymx8rcw9u6nk. Further analysis revealed that the funds were ultimately transferred to a Bybit-associated wallet (1ApiPC2e4FpQnDdTpcVPsn3fPyUBob783t). This wallet has been active since October 2, 2024, and has processed approximately $774,825.58 in total transaction volume. **Figure 26** illustrates the flow of Microsoft's payment to these wallets.

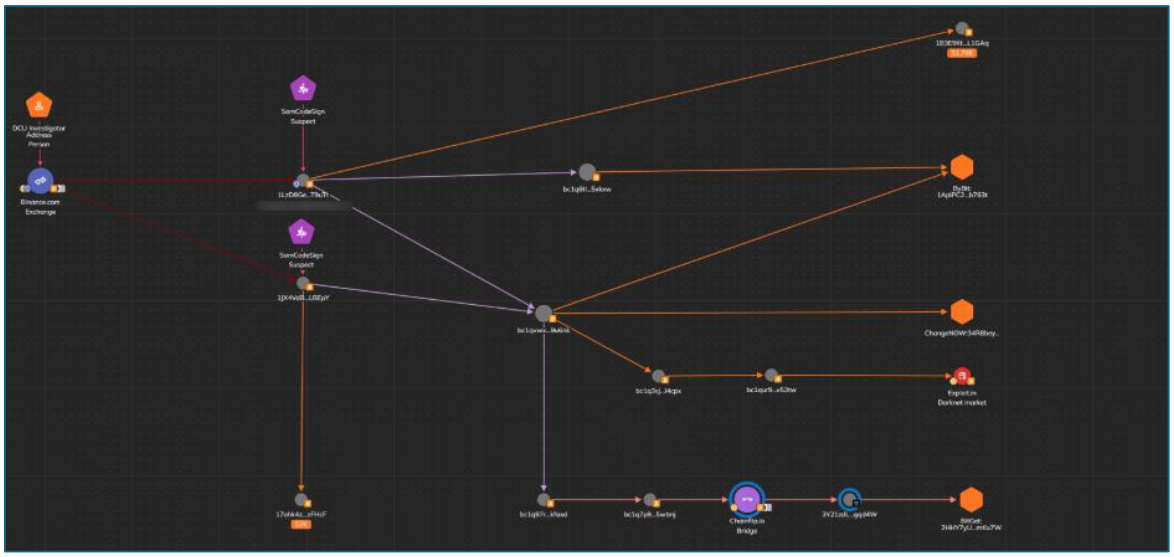


FIGURE 26

64. Additional analysis indicates that five payments from June 2025 to January 2026 were made from two Bitcoin wallets attributed in Chainalysis Reactor to Vanilla Tempest Defendants (identified in **Figure 27** as "Rhysida ransomware"). These wallets conducted indirect transactions with other wallets leading to a wallet attributed to SamCodeSign, further linking the activity to Fox Tempest Defendants. **Figure 27** illustrates the flow of payments between these wallets.

FIGURE 27

DEFENDANTS TARGET VICTIMS LOCATED IN NEW YORK

65. Microsoft has identified thousands of customer machines in the United States that have been impacted by malware signed with certificates originating from Fox Tempest Defendants' operations.

66. A significant portion of this activity is directed at New York-based organizations and individuals. More than 10,000 customer machines located in the State of New York have been impacted by such malware. Of these machines, more than 4,000 are located within the Southern District of New York.

HARM TO MICROSOFT AND ITS CUSTOMERS

67. The Defendants targeted Microsoft, its customers, and the public to advance their financially motivated cybercrimes. The Defendants have caused and continue to cause irreparable injury to Microsoft, its customers, and the public. Defendants' activities irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill. More than a dozen machines owned and operated by Microsoft have also been impacted by malware signed by certificates obtained from Fox Tempest Defendants.

68. The Defendants' criminal acts directly harm Microsoft's reputation and goodwill that it has obtained through its extensive branding efforts.

69. 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®, Microsoft Teams®, and Azure®. Microsoft has invested substantial resources in developing high-quality, effective, and trusted products and services. Because of 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 represents significant goodwill that has been established through decades of use in the United States and globally. To protect this goodwill, reputation, and strong branding, Microsoft has registered

hundreds of trademarks with the United States Patent and Trademark Office, including the Microsoft®, Windows®, Microsoft 365®, Microsoft Teams®, and Azure® marks. The registrations for these trademarks are attached to the Complaint as **Appendix A**.

70. The certificates found in Vanilla Tempest Defendants' malware display the Microsoft® trademark, creating an association with Microsoft, its products, and services. Further, Vanilla Tempest Defendants use the mark Microsoft Teams® on websites designed to mimic the appearance of an authentic website where a user could obtain the Microsoft Teams software to deceive victims into downloading the malicious software from the website.

71. Customers expect certain quality from Microsoft. To that end, Microsoft places restrictions on how its branding can be used. When products attributed to Microsoft are used in connection with cybercrime, customers will mistakenly believe Microsoft is responsible for the attack. Customers subjected to the negative effects of Defendants' activities 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 Defendants' malware or believes that Microsoft's products are not secure (because customers are unaware of Defendants' deception), it may be costly or impossible to convince the customer to return to Microsoft.

72. Microsoft has invested significant resources totaling more than $1,500,000 to address and attempt to remediate the harm caused by the Defendants' crimes. Specifically, Microsoft has spent more than 8,000 investigative hours investigating the Defendants and their infrastructure to remediate and prevent future attacks. In addition, Microsoft has expended

significant effort revoking certificates that Defendants fraudulently obtained and used to perpetrate attacks as well as taking steps to prevent Defendants from obtaining certificates going forward.

DISRUPTING DEFENDANTS' ILLEGAL ACTIVITY

73. Through this lawsuit, Microsoft is requesting judicial authorization to direct the domain name registrar for the signspace.cloud domain and the provider of the virtual machine infrastructure used by the Defendants to take actions that would disrupt this scheme. The internet domain and virtual machine infrastructure relied upon by the Certificate Abuse Enterprise are the most vulnerable parts of their operation. Without access to the signspace.cloud domain, registered through GoDaddy, and the virtual machines hosted by Cloudzy, Fox Tempest Defendants would not be able to provide fraudulently obtained code signing certificates to their customers, and Vanilla Tempest Defendants would not be able to digitally sign their malware.

74. The steps set forth in the proposed *ex parte* temporary restraining order ("Proposed Order"), which will be carried out upon entry of the requested Proposed Order, will immediately prevent the Defendants from operating the Certificate Abuse Enterprise. For instance, the redirection of the signspace.cloud domain and disabling of Fox Tempest Defendants' virtual machine infrastructure will directly disrupt their operation, preventing Vanilla Tempest Defendants and other cybercriminals from using these mechanisms to sign additional malware with fraudulently obtained certificates, thus mitigating risk and injury to Microsoft and its customers.

75. I believe that the virtual machine data that Microsoft will receive from Cloudzy upon entry of the Proposed Order will contain categories of evidence, as discussed above, that are uniquely probative of the Certificate Abuse Enterprise and that cannot be reconstructed from Microsoft's own telemetry or from other sources. This information is essential to identifying and

attributing conduct to the John Doe Defendants, uncovering additional victims, and supporting Microsoft's claims in this action.

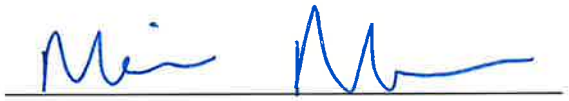
76. It is critical that these actions be shielded from anyone associated with the Certificate Abuse Enterprise until the takedown of their infrastructure is complete and the virtual machine data has been preserved. If Fox Tempest Defendants become aware of these efforts before they are completed, there is a substantial risk that they will relocate the infrastructure to alternative providers and that they will wipe, encrypt, or migrate the contents of the Cloudzy-hosted virtual machines before that data can be preserved. Fox Tempest Defendants have already demonstrated the capability and willingness to take such action, having previously transitioned their infrastructure after Microsoft's anti-fraud activity impaired the functioning of the signspace.cloud website.

77. I believe that the steps described in the Proposed Order are appropriate and necessary to suspend the ongoing harm caused by the Certificate Abuse Enterprise to Microsoft, its customers, and the public. The Defendants' scheme is specifically designed to circumvent technical mitigation efforts, making it impossible for Microsoft to curb the resulting harms through technical means alone. While the Defendants may attempt to establish new infrastructure, judicial relief will immediately halt the ongoing harm from their current operations, preserve critical evidence of their criminal activity, and impose significant costs and delays that will disrupt their ability to reconstitute their scheme. In the absence of judicial relief, the Defendants will be able to continue using this infrastructure to fraudulently obtain certificates and sign malware, exposing additional victims to the Certificate Abuse Enterprise's malicious activities. Moreover, Microsoft will continue to monitor for new infrastructure and can seek additional relief as necessary.

78. For all of these reasons, I believe the only way to mitigate injury and disrupt the Certificate Abuse Enterprise's infrastructure is to take the steps described in the Proposed Order prior to providing notice to the Defendants.

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

Executed May 4th, 2026 in New York, New York



Maurice Mason
Principal Investigator, Digital Crimes Unit
Microsoft Corporation