

**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. 26-cv-03737(RA)

PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation (“Microsoft”) has filed a complaint for injunctive and other relief pursuant to: (1) the Racketeer Influenced and Corrupt Organizations Act (“RICO”), 18 U.S.C. § 1962(c)-(d); (2) the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(b) and 1030(a)(6); (3) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a), and 1125(c); and New York state common law claims of (4) breach of contract; (5) trespass to chattels; and (6) unjust enrichment. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 18 U.S.C. § 1964(a) (RICO), 15 U.S.C. § 1116(a) (the Lanham Act), 18 U.S.C. § 1030(g) (the Computer Fraud and Abuse Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

On May 8, 2026, the Court issued a Temporary Restraining Order (“TRO”) and Order to Show Cause (“OSC”) why an injunction should not be issued. On May 19, 2026, following Microsoft’s representation to the Court that the TRO has been executed, Microsoft duly served Defendants with the Summons, TRO, Order Extending TRO, Complaint, Emergency *Ex Parte* Application for Temporary Restraining Order and Order to Show Cause re Preliminary Injunction (“TRO Application”), and Memorandum of Law and Declarations in Support of the TRO Application. Defendants have not responded to the Court’s Order to show Cause or otherwise appeared in the action. Microsoft now moves for an Order for Preliminary Injunction seeking to keep in place the relief granted by the TRO.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and the memorandum filed in support of Microsoft’s TRO Application, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case pursuant to 28 U.S.C. § 1331 and 28 U.S.C. § 1367, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against John Does 1–2 (collectively “Fox Tempest Defendants”) and John Does 3–4 (collectively “Vanilla Tempest Defendants,” and together with Fox Tempest Defendants, the “Defendants”) pursuant to: (1) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)-(d); (2) the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(b) and 1030(a)(6); (3) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a), and 1125(c); and New York state common law claims of (4) breach of contract; (5) trespass to chattels; and (6) unjust enrichment.
2. There is good cause to believe that Defendants are members of a sophisticated

criminal enterprise that has systematically exploited Microsoft's code-signing technology to facilitate their unlawful conduct. 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, and have sold fraudulently obtained code signing certificates to Vanilla Tempest Defendants and other cybercriminals. Vanilla Tempest Defendants have used those certificates to digitally sign malware, disguising it as legitimate software, including representing them as Microsoft products, to deploy ransomware, steal sensitive information, and extort victims for financial gain.

3. There is good cause to believe that Fox Tempest Defendants supply their illicit code signing service by fraudulently creating Microsoft tenants designed to bypass Microsoft's identity validation requirements, 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.

4. There is good cause to believe that Defendants have distributed certificates to cybercriminals through two channels: (1) the website `signspace[.]cloud`, registered through GoDaddy.com, LLC ("GoDaddy") and (2) virtual machines hosted by RouterHosting LLC (d/b/a "Cloudzy").

5. There is good cause to believe that Defendants have engaged in and are likely to continue engaging in acts or practices that violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. §§ 1962, 1962(d)), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), and the Lanham Act (15 U.S.C. §§ 1114, 1125), and that also constitute breach of contract, trespass to chattels, and unjust enrichment, and Microsoft, therefore, is likely to prevail on the merits of this action.

6. Microsoft owns the registered trademarks Microsoft®, Windows®, Microsoft 365®, Microsoft Teams®, and Azure®, and numerous other trademarks used in connection with its services, software, and products.

7. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations. The evidence set forth in Microsoft's Memorandum of Law in support of its TRO Application and the accompanying declarations and supporting exhibits, demonstrate that Microsoft is likely to prevail on its claims that Defendants have engaged in violations of the foregoing law by:

- A. Fraudulently creating more than 580 Microsoft tenants using false identifying information to obtain access to Microsoft's Artifact Signing service and to generate code signing certificates;
- B. Selling and distributing fraudulently obtained code signing certificates to cybercriminals, including Vanilla Tempest Defendants, through Telegram, Google Forms, and other infrastructure they manage;
- C. Operating infrastructure specifically designed for the distribution of fraudulently obtained certificates, including the signspace[.]cloud website and virtual machines hosted by Cloudzy;
- D. Signing malware, including "Oyster" (also known as "Broomstick" or "CleanupLoader"), with fraudulently obtained certificates to bypass security features of the Windows operating system, including SmartScreen, User Account Control, and Smart App Control;
- E. Creating fraudulent installer files bearing the name "MSTeamsSetup.exe" and hosting them on malicious domains designed to mimic legitimate Microsoft Teams websites;
- F. Employing search engine optimization poisoning and malicious advertising campaigns to lure Microsoft's customers to malicious download sites;
- G. Deploying malware onto thousands of computers in the United States, including machines owned and operated by Microsoft, causing damage by collecting system information, stealing credentials, executing unauthorized commands, downloading additional malware, and deploying ransomware;

- H. Operating a Racketeering Enterprise by leveraging each other's work 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, (iii) sign and deploy malware on the computers of Microsoft and its customers, (iv) gain unauthorized access to victims' computers, and (v) engage in further malicious activities, including exfiltrating sensitive personal and financial information, deploying ransomware, and extorting victims for financial gain; and
- I. Infringing the protected marks of Microsoft for the purpose of causing confusion or mistake, whereby the victims of Defendants' attacks mistakenly associate such conduct with Microsoft.

8. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. Defendants' activities irreparably damage Microsoft's reputation, brands, and customer goodwill. If a customer stops using Microsoft's products because the customer, unaware of Defendants' deception, blames Microsoft for Defendants' malware or believes that Microsoft's products are not secure, Microsoft may not be able to convince the customer to return to Microsoft. In addition, Defendants' data theft and deployment of additional malware and ransomware harming Microsoft's customers and the public cannot be remedied after the fact.

9. There is good cause to believe that Defendants will continue to engage in such unlawful actions if not restrained from doing so by Order of this Court. Notwithstanding Microsoft's prior disruption efforts, including the revocation of more than 200 code-signing certificates in October 2025 and implementation of additional anti-fraud measures that introduced substantial friction into the `signspace[.]cloud` website, Defendants have persisted in their unlawful conduct and continued to engage in the criminal scheme described herein.

10. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the continued operation of Defendants' infrastructure, including the `signspace[.]cloud` website and the virtual machines hosted by Cloudzy

identified in **Exhibit 2** and **Appendix B** to the Complaint, respectively. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- A. Defendants are engaged in activities that directly violate United States law and harm Microsoft, its customers, and the public;
- B. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- C. Defendants are likely to relocate Internet infrastructure and migrate their code signing operations to new virtual machines and hosting providers, thereby permitting them to continue their illegal acts; and
- D. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

11. There is good cause to believe that Defendants have operated their criminal scheme through certain instrumentalities—specifically through the signspace[.]cloud website identified in **Exhibit 2** to the Complaint and the virtual machines hosted by Cloudzy identified in **Appendix B** to the Complaint.

12. There is good cause to believe that to halt the injury caused by Defendants, they must continue to be prohibited from fraudulently obtaining access to Microsoft's Artifact Signing service, prohibited from operating or using the signspace[.]cloud website or the virtual machines hosted by Cloudzy to distribute code signing certificates, and prohibited from using Microsoft's trademarks to perpetrate their unlawful scheme.

13. There is good cause to believe that to halt the injury caused by Defendants, the signspace[.]cloud domain identified in **Exhibit 2** to the Complaint must remain beyond the control of Defendants' criminal operation, and the virtual machines hosted by Cloudzy and identified in **Appendix B** to the Complaint must remain inaccessible to Defendants.

14. There is good cause to believe that Defendants have specifically directed their

activities to the Southern District of New York.

15. There is good cause to permit notice of the instant Preliminary Injunction Order by alternate means. The following means of service are authorized by law, satisfy due process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants concerning the instant order and this action: (1) transmission by email, facsimile, mail, and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the United States; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

16. Microsoft's counsel has certified that Microsoft served Defendants via the alternative methods of service authorized in the TRO as set forth below:

- A. Microsoft published notice of the Summons and Complaint and materials relating to Microsoft's application for issuance of a TRO and preliminary injunction on a publicly available website (www.noticeofpleadings.net/OpFauxSign);
- B. Microsoft announced publicly and through the media the issuance of the TRO;
- C. Any person using the Internet, including participants in Defendants' scheme, who visits [signspace\[.\]cloud](http://signspace[.]cloud), would be informed that the domain had been seized by Microsoft in connection with this action and would be provided with the link to the Notice of Pleadings website where the pleadings for this action may be accessed;
- D. Microsoft served Fox Tempest Defendants (John Does 1–2) by process server via their agent, the domain registrant for [signspace\[.\]cloud](http://signspace[.]cloud), Domains By Proxy, LLC;
- E. Microsoft served Fox Tempest Defendants (John Does 1–2) by mail via their agent, the domain registrant for [signspace\[.\]cloud](http://signspace[.]cloud), Domains By Proxy, LLC;

F. Microsoft served Defendants using the registrant emails associated with the signspace[.]cloud, Teams-download[.]buzz, Teams-install[.]run and Teams-download[.]top domains, which was found to be a reliable method of contacting the Defendants, and Microsoft confirmed via the “delivery receipt” and “read receipt” features on Microsoft Outlook that at least one email to each Defendant was successfully delivered (i.e., no bounce back).

17. Accordingly, there is good cause to believe Microsoft has complied with its obligations to serve and provide notice of this action to Defendants.

18. There is good cause to believe that Defendants have no legitimate interest in carrying out their criminal activities.

19. There is good cause to believe that the harm to Microsoft in denying the relief requested in its TRO Application outweighs any harm to any legitimate interest of Defendants (of which there is none) and that there is no undue burden to any third party.

PRELIMINARY INJUNCTION ORDER

IT IS THEREFORE ORDERED that Defendants, their representatives, and persons who are in active concert or participation with Defendants and the Certificate Abuse Enterprise, are restrained and enjoined during the pendency of this action from: (1) fraudulently creating Microsoft tenants or otherwise accessing Microsoft’s Artifact Signing service; (2) obtaining, selling, distributing, or otherwise trafficking in code signing certificates fraudulently obtained through Microsoft’s Artifact Signing service; (3) signing malware or any other unauthorized software using certificates obtained from Microsoft’s Artifact Signing service; (4) deploying malware on the computers of Microsoft, Microsoft’s customers, or any other person, including through deceptive distribution methods such as spoofed websites, malicious advertising campaigns, and search engine optimization poisoning; (5) capitalizing on the trademarks of Microsoft to fabricate legitimacy for their malware distribution scheme, including creating installer files or websites that bear or mimic Microsoft’s trademarks; (6) misappropriating that

which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (7) destroying the goodwill and reputation of Microsoft; (8) impersonating Microsoft, its systems, products, and services; (9) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, namely the signspace[.]cloud domain and the virtual machines hosted by Cloudzy identified in **Exhibit 2** and **Appendix B** to the Complaint, respectively, and through any other component or element of Defendants' illegal infrastructure at any location, including infrastructure Defendants may attempt to rebuild; and (10) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that Defendants, their representatives, and persons who are in active concert or participation with Defendants and the Certificate Abuse Enterprise are restrained and enjoined during the pendency of this action from: (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks Microsoft®, Windows®, Microsoft 365®, Microsoft Teams®, and Azure®, and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names, or service marks; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation, or description of Defendants or of their activities, whether by symbols, words, designs, or statements, which would damage or injure Microsoft or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products, or services are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products, or services as Microsoft's.

IT IS FURTHER ORDERED that, with respect to the signspace[.]cloud domain identified in **Exhibit 2** to the Complaint, GoDaddy, as the domain name registrar for signspace[.]cloud, shall take the following actions during the pendency of this action:

A. Maintain Microsoft's registrar of choice, MarkMonitor, Inc., as the registrar of record for signspace[.]cloud, and MarkMonitor, Inc. shall maintain Microsoft as the registrant for that domain.

B. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domain with the current registrar;

C. Ensure the domain remains active and continues to resolve in the manner set forth in this Order;

D. Prevent the transfer, modification, or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft.

E. Take all steps required to propagate the foregoing changes through the Domain Name System ("DNS"), including to the relevant domain registry.

F. Preserve all evidence that may be used to identify the Defendants using the domain.

G. With regard to the domain registries, registrars, and hosting providers for signspace[.]cloud located outside the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by Defendants to the citizens of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars, registrants,

or hosts to effectuate this request.

IT IS FURTHER ORDERED that, with respect to the virtual machines hosted by Cloudzy and identified in **Appendix B** to the Complaint, Cloudzy shall take the following actions during the pendency of this action:

A. Continue to disable Defendants' access to all virtual machines identified in **Appendix B** to the Complaint and preserve all data, files, logs, and records associated with those virtual machines, including but not limited to disk images, network traffic logs, access logs, billing records, account information, and any other records relating to Defendants' use of those virtual machines.

B. Continue to provide Microsoft with access to and control over all virtual machines identified in **Appendix B** to this Order, including all data and files stored on the virtual machines and metadata and account information associated with the virtual machines.

C. Continue to prevent Defendants from creating, accessing, or controlling any new virtual machines or other computing resources through Cloudzy's platform in connection with the activities prohibited by this Order.

D. Continue to take reasonable steps to work with Microsoft to ensure that Defendants cannot use Cloudzy's services to continue their code signing operations or to gain unauthorized access to computers, sign malware, or engage in any other activities prohibited by this Order.

IT IS FURTHER ORDERED that copies of this Preliminary Injunction Order may be served by any means authorized by law, including (1) transmission by email, facsimile, mail, and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration

and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the United States, and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent they provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS SO ORDERED.

Entered this 22 day of May, 2026.



UNITED STATES DISTRICT JUDGE