

Exposing Fox Tempest: A malware-signing service operation

By Microsoft Threat Intelligence

Published: 2026-05-19 · Archived: 2026-08-05 02:00:19 UTC

Fox Tempest is a financially motivated threat actor that operates a malware-signing-as-a-service (MSaaS) used by other cybercriminals to more effectively distribute malicious code, including ransomware. The threat actor abuses Microsoft Artifact Signing to generate short-lived, fraudulent code-signing certificates to appear legitimately signed, allowing malware to evade security controls.

Fox Tempest has created over a thousand certificates and established hundreds of Azure tenants and subscriptions to support its operations. Microsoft has revoked over one thousand code signing certificates attributed to Fox Tempest. In May 2026, Microsoft's Digital Crimes Unit (DCU), with support from industry partner [Resecurity](#), [disrupted Fox Tempest's MSaaS offering](#), targeting the infrastructure and access model that enables its broader criminal use.

Microsoft Threat Intelligence observed Fox Tempest's operations enabling the deployment of Rhysida [ransomware](#) by threat actors such as [Vanilla Tempest](#), as well as the distribution of other malware families including Oyster, [Lumma Stealer](#), and Vidar. The consistency, scale, and downstream impact of the resulting attack activity demonstrate that Fox Tempest is a vital operator within the broader cybercrime ecosystem.

In this blog, we examine how Fox Tempest's MSaaS operation functioned and how it enabled the delivery of trusted, signed malware across the cybercrime ecosystem. We also provide [Microsoft Defender](#) detections, indicators of compromise (IOCs), and mitigation recommendations to help organizations identify and disrupt similar activity.

Fox Tempest's role and impact

Fox Tempest doesn't directly target victims but instead provides supporting services that enable ransomware operations by other threat actors. Microsoft Threat Intelligence has tracked Fox Tempest since September 2025. Microsoft Threat Intelligence has linked the actor to various ransomware groups including Vanilla Tempest, [Storm-0501](#), [Storm-2561](#), and Storm-0249, who have all leveraged Fox Tempest-signed malware in active intrusions. Malware delivery in these attacks have included use of legitimate purchased advertisements, malvertising, and SEO poisoning.

Cryptocurrency analysis associated with Fox Tempest has identified clear links tying the actor to ransomware affiliates responsible for delivering several prominent ransomware families, including INC, Qilin, Akira, and others, with observed proceeds in the millions. Based on the scale of the MSaaS offering, Microsoft Threat Intelligence assesses that Fox Tempest is a well-resourced group handling infrastructure creation, customer relations, and financial transactions.

The downstream impact of these operations has resulted in attacks against a broad range of industry sectors, including healthcare, education, government, and financial services, impacting organizations globally including, but not limited to the United States, France, India, and China.

Fox Tempest's malware signing as a service infrastructure

Fox Tempest's MSaaS capability was available through the website *signspace[.]cloud*, a now defunct service that was disrupted by DCU, which enabled other threat actors to fraudulently obtain short-lived Microsoft-issued certificates that were valid for only 72 hours, obtained through [Artifact Signing](#) (previously named Azure Trusted Signing). This use of short-life certificates from a trusted source allowed malware and ransomware to masquerade as legitimate software (like AnyDesk, Teams, Putty, and Webex) to bypass security controls, significantly increasing the likelihood of execution and successful delivery. Fox Tempest offered this MSaaS capability to the ransomware ecosystem since at least May 2025.

To obtain legitimate signed certificates through Artifact Signing, the requestor must pass detailed [identify validation](#) processes in keeping with industry standard verifiable credentials (VC), which suggests the threat actor very likely used stolen identities based in the United States and Canada to masquerade as a legitimate entity and obtain the necessary digital credentials for signing. The SignSpace website was built on Artifact Signing and enabled secure file signing through an admin panel and user page, leveraging Azure subscriptions, certificates, and a structured database for managing users and files. A GitHub repository, called code-signing-service, included configuration files and technical details that directly linked it to the infrastructure behind *signspace[.]cloud*.

The *signspace[.]cloud* service has two unique modeling groupings: the admin and the customers. The admin is responsible for maintaining the tooling, account creation, and infrastructure, while the customers provide files to be fraudulently code signed. Customers who accessed the service could upload malicious files to be signed using Fox Tempest-controlled certificates.

Below are examples of the *signspace[.]cloud* portal as seen by Fox Tempest’s customers:

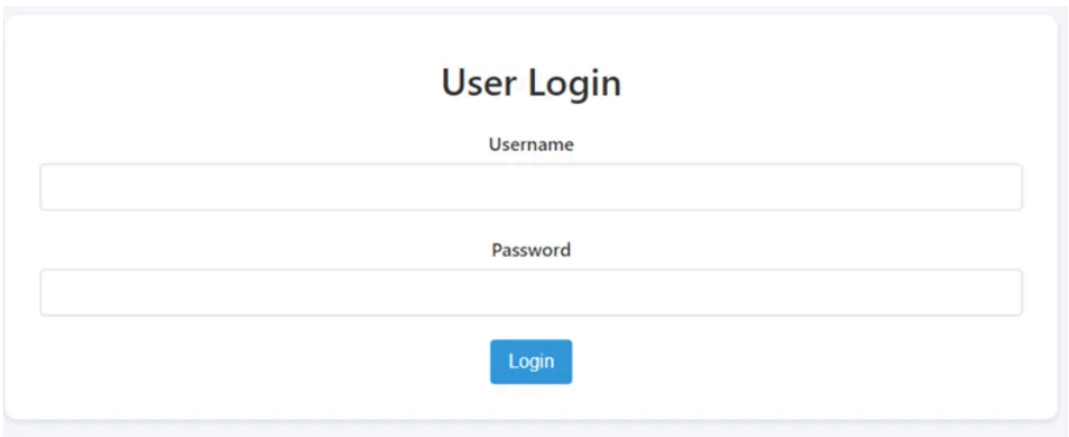


Figure 1. Fox Tempest’s SignSpace sign-in portal

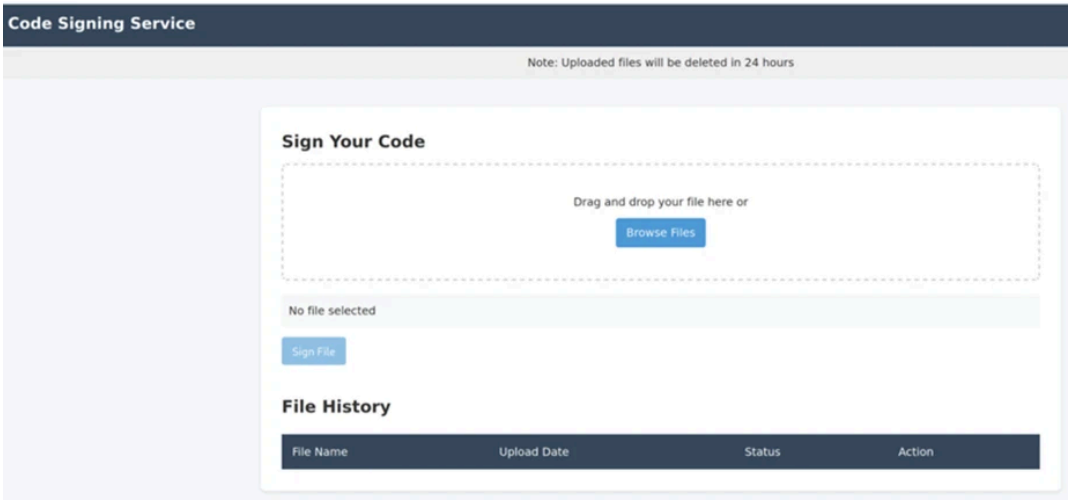


Figure 2. Fox Tempest’s SignSpace code signing service upload page

In February 2026, Microsoft Threat Intelligence observed a notable shift in Fox Tempest’s operational infrastructure. Fox Tempest transitioned to providing customers with pre-configured virtual machines (VMs) hosted on US-based virtual private server provider Cloudzy’s infrastructure, allowing threat actors to upload their malicious files directly to Fox Tempest-controlled environments and receive signed binaries in return. This infrastructure evolution reduced friction for customers, improved operational security for Fox Tempest, and further streamlined the delivery of malicious but trusted, signed malware at scale. Microsoft’s Digital Crimes Unit (DCU) disrupted this infrastructure and continues to partner with Cloudzy to identify and disrupt related infrastructure.

Below is an example of the Fox Tempest-provided VM environment as seen by customers:

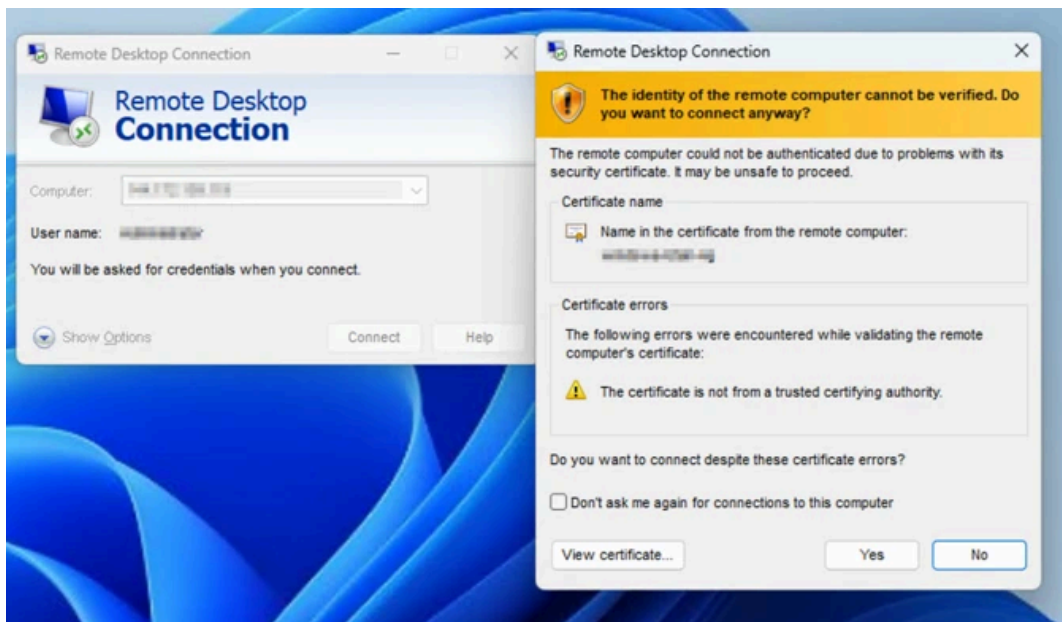


Figure 3. Accessing VM provided by Fox Tempest

Inside the VM, Fox Tempest provided files that are used to sign code:

- The first file, *metadata.json*, was a configuration file that pointed to an Azure-hosted endpoint which also included the signing account and certificate profile.
- The second file, *test.js*, is an example of a file provided by Fox Tempest that had been digitally signed to demonstrate their signing capabilities to customers.
- The third file, *PS code sample.txt*, contains the PowerShell script they used to sign customer-submitted files using certificates under Fox Tempest control.

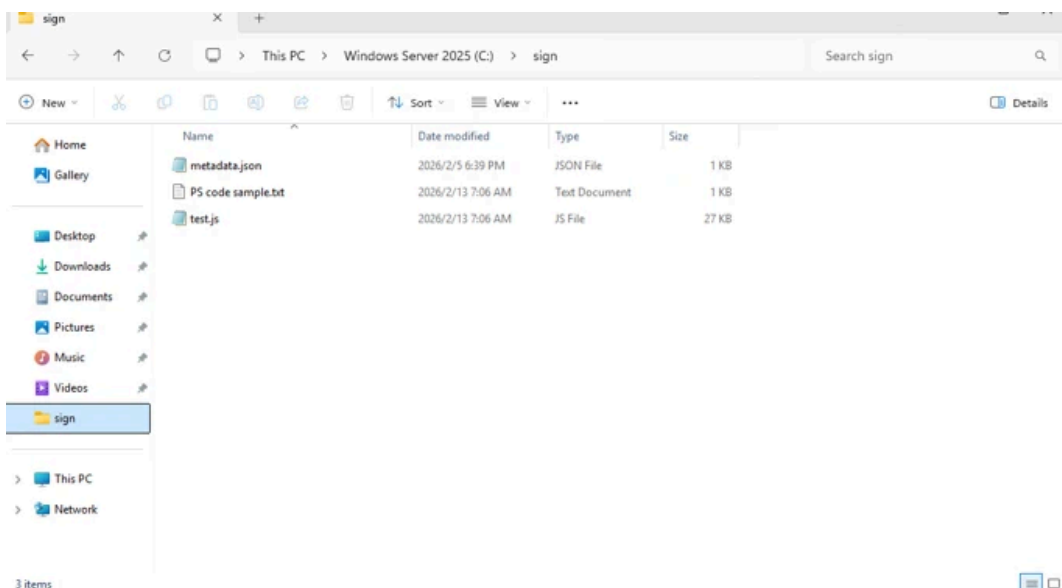


Figure 4. Fox Tempest provided files

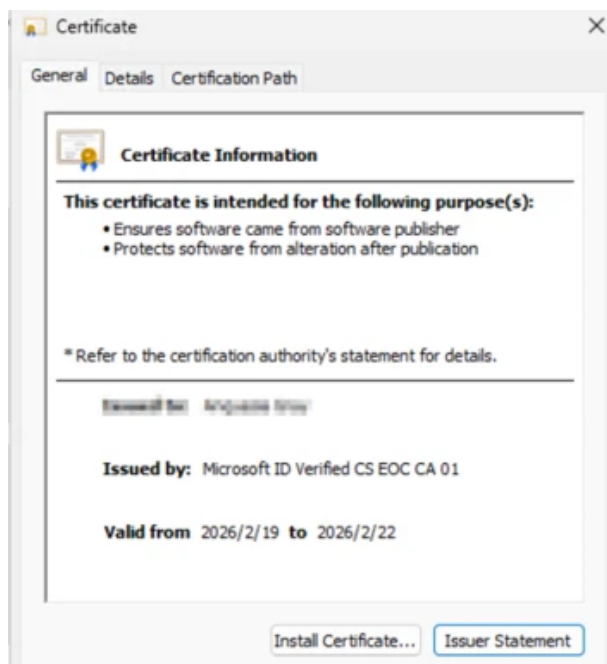


Figure 5. Fox Tempest provided certificate

Threat actors using Fox Tempest's MSaaS offering paid thousands of dollars to get their malicious code signed, as shown below with the Google Form detailing the service's pricing model. Actors filled out the form before being added to a queue to submit payment and gain access to a VM. The form (written in both English and Russian) asks the user to choose a selected plan from a price list of \$5000 USD, \$7500 USD, or \$9000 USD, with a mention that higher paying plans receive priority in the queue sequence.

EV Code Signing — занять очередь

(Join EV Code Signing queue)

[Sign in to Google](#) to save your progress. [Learn more](#)

* Indicates required question

Тариф (Plan) *

Тариф определяет приоритет в очереди. Заказы по более высокой стоимости обрабатываются в первую очередь. (The selected plan determines queue priority. Orders at higher price levels are processed first.)

☐ \$5000

☐ \$7500

☐ \$9500

Как часто нужен EV *

How often is EV needed?

Choose

Сколько в среднем служит ваш сертификат до отзыва? *

How long does your certificate usually remain valid before revocation?

☐ 1 месяц (1 month)

☐ 2 месяца (2 months)

☐ 3 месяца (3 months)

☐ 6 месяцев (6 months)

☐ 12 месяцев (12 months)

Акк на форуме

Forum account link

Your answer

Можете оставить любой комментарий, предложение, вопрос, если требуется.

You can leave any comment, suggestion, question if required.

Your answer

Submit

Clear form

Figure 6. Google form used by Fox Tempest

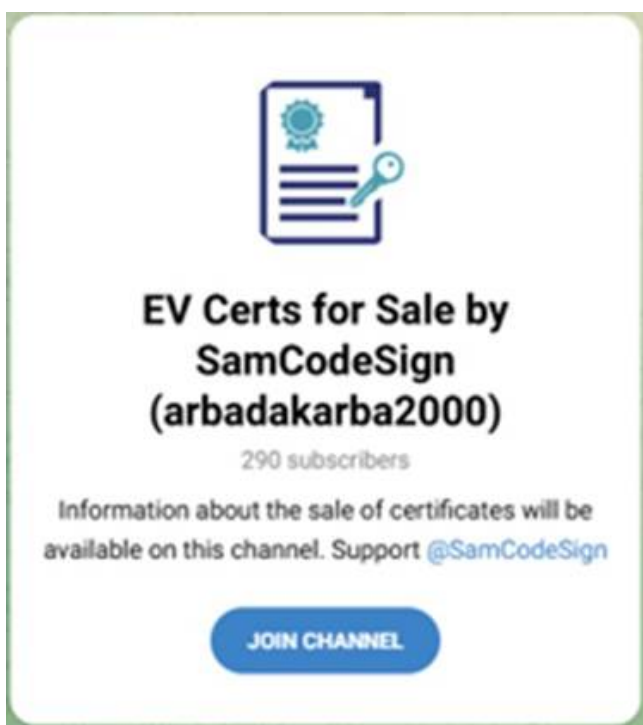


Figure 7. Telegram used by Fox Tempest

Fox Tempest engaged directly with customers using a Telegram channel, *EV Certs for Sale by SamCodeSign* under the user account *arbadakarba2000*. All signing activity occurred using a Fox Tempest-provided email address associated with a very small number of IP addresses.

Case study: Fox Tempest enables Vanilla Tempest attacks

Vanilla Tempest began using Fox Tempest's MSaaS service as early as June 2025. Through this service, Vanilla Tempest uploaded malicious payloads such as trojanized Microsoft Teams installers, which Fox Tempest would fraudulently signed to appear legitimate. Vanilla Tempest would then distribute these signed binaries through legitimately purchased advertisements that redirected users searching for Microsoft Teams to attacker-controlled advertisements and fraudulent download pages.

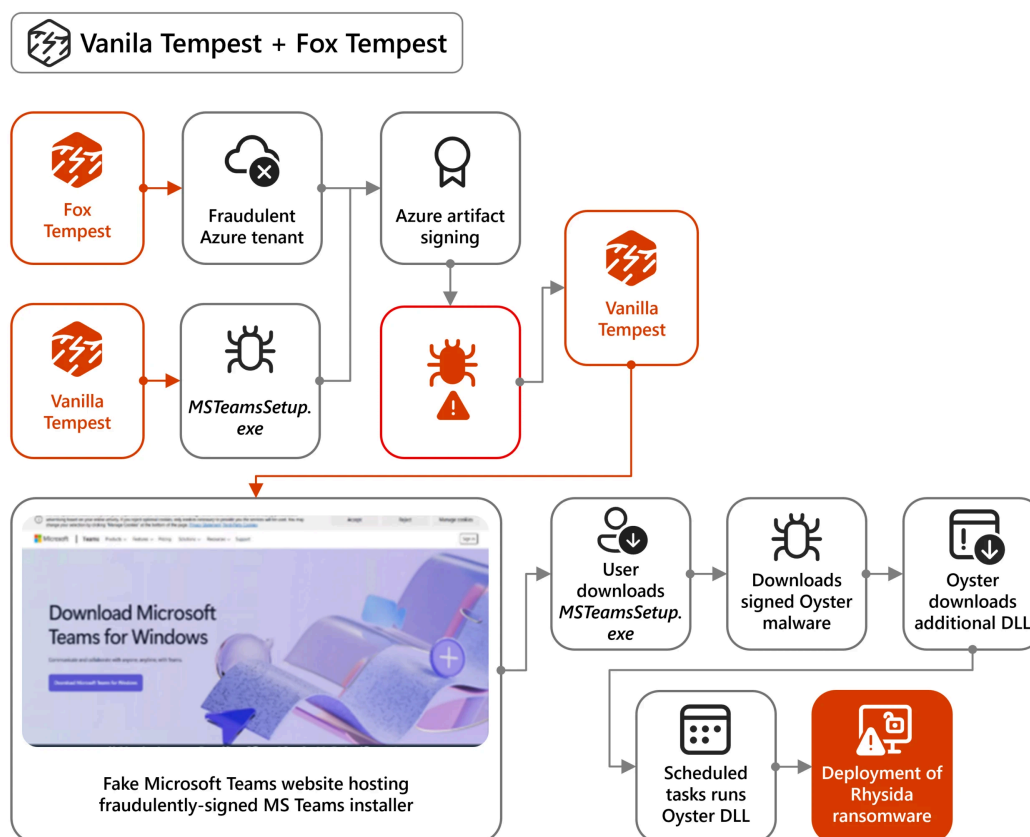


Figure 8. Vanilla Tempest and Fox Tempest attack chain

Victims were presented with a malicious *MSTeamsSetup.exe* in place of the legitimate client, reflecting a broader pattern of Vanilla Tempest frequently abusing trusted software brands to lure victims and establish initial access. Execution of the counterfeit installer resulted in the deployment of the Oyster backdoor (also known as Broomstick), a modular, multistage implant that establishes persistent remote access, initiates command-and-control (C2) communications, collects host-level information, and enables the delivery of additional payloads. By masquerading as a widely deployed enterprise collaboration tool hiding behind a fraudulently signed binary, Vanilla Tempest's Oyster payload was likely able to evade casual detection and blend into normal enterprise activity. In some observed cases, Vanilla Tempest also deployed Rhysida ransomware within victim environments using the same process.

Defending against Fox Tempest-enabled attacks

To defend against Fox Tempest tactics, techniques, and procedures (TTPs) and similar activity, Microsoft recommends the following mitigation measures:

- Read the [human-operated ransomware threat overview](#) for advice on developing a holistic security posture to prevent ransomware, including credential hygiene and hardening recommendations.
- Turn on [cloud-delivered protection](#) in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Turn on [Safe Links](#) and [Safe Attachments](#) in Microsoft Defender for Office 365.
- Encourage users to use Microsoft Edge and other web browsers that support [Microsoft Defender SmartScreen](#), which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that host malware.
- Turn on tenant-wide [tamper protection](#) features to prevent attackers from stopping security services or using antivirus exclusions. Without tamper protection, attackers could simply turn off Microsoft Defender Antivirus without the need to acquire higher privileges.

- Customers running Intune or Microsoft Defender for Endpoint Security Configuration can [enable `DisableLocalAdminMerge` to prevent modification of antivirus exclusions via GPO](#).
- In addition to tamper protection, you can also [enable and configure Microsoft Defender Antivirus always-on protection in Group Policy](#).
- If there is an issue with a device during roll out of various antivirus features, the device can be placed in [troubleshooting mode](#) to turn off tamper protection temporarily without impacting the wider organizational security policy.
- Microsoft Defender XDR customers can turn on [attack surface reduction rules](#) to prevent several of the infection vectors of this threat. These rules, which can be configured by any user, offer significant hardening against targeted attacks. In observed attacks, Microsoft customers who had the following rules turned on could mitigate the attack in the initial stages and prevent hands-on-keyboard activity:
 - [Use advanced protection against ransomware](#)

Microsoft Defender detections

[Microsoft Defender](#) customers can refer to the list of applicable detections below. Microsoft Defender coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Tactic	Observed activity	Microsoft Defender coverage
Persistence	Threat actors distributed malware families including using Fox Tempest-signed binaries	Microsoft Defender Antivirus – Trojan:Win64/OysterLoader – Trojan:Win64/Oyster – Trojan:Win32/Malcert – Trojan:Win32/LummaStealer – Trojan:Win32/Vidar – Backdoor:Win32/Spyder – Trojan:Win32/Malgent – Trojan:Win64/Tedy – Trojan:Python/MuddyWater – Trojan:Win64/Fragtor Microsoft Defender for Endpoint – Vanilla Tempest activity group – User account created under suspicious circumstances – New group added suspiciously – New local admin added using Net commands – ‘LummaStealer’ malware was prevented – ‘Malcert’ malware was prevented – ‘Vidar’ malware was prevented
Impact	Analysis of Fox Tempest MSaaS identified links to the enablement of several ransomware families	Microsoft Defender Antivirus – Ransom:Win64/Rhysida – Ransom:Win64/Inc – Ransom:Win32/Qilin – Ransom:Win32/BlackByte Microsoft Defender for Endpoint – Ransomware-linked threat actor detected

		– ‘BlackByte’ ransomware was prevented – ‘INC’ ransomware was prevented – ‘Qilin’ ransomware was prevented – ‘Rhysida’ ransomware was prevented – A file or network connection related to a ransomware-linked emerging threat activity group detected
--	--	---

Microsoft Security Copilot

[Microsoft Security Copilot](#) is [embedded in Microsoft Defender](#) and provides security teams with AI-powered capabilities to summarize incidents, analyze files and scripts, summarize identities, use guided responses, and generate device summaries, hunting queries, and incident reports.

Customers can also [deploy AI agents](#), including the following [Microsoft Security Copilot agents](#), to perform security tasks efficiently:

- [Threat Intelligence Briefing agent](#)
- [Phishing Triage agent](#)
- [Threat Hunting agent](#)
- [Dynamic Threat Detection agent](#)

Security Copilot is also available as a [standalone experience](#) where customers can perform specific security-related tasks, such as incident investigation, user analysis, and vulnerability impact assessment. In addition, Security Copilot offers [developer scenarios](#) that allow customers to build, test, publish, and integrate AI agents and plugins to meet unique security needs.

Threat intelligence reports

Microsoft Defender XDR customers can use the following [threat analytics](#) reports in the Defender portal (requires license for at least one Defender XDR product) to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender XDR threat analytics

- [Actor profile: Fox Tempest](#)
- [Actor profile: Vanilla Tempest](#)
- [Threat Overview profile: Human-operated ransomware](#)
- [Activity profile: Vanilla Tempest leverages fake Microsoft Teams setup to deliver Oyster backdoor](#)

Microsoft Security Copilot customers can also use the [Microsoft Security Copilot integration](#) in Microsoft Defender Threat Intelligence, either in the Security Copilot standalone portal or in the [embedded experience](#) in the Microsoft Defender portal to get more information about this threat actor.

Indicators of compromise

Indicator	Type	Description	First seen	Last seen
-----------	------	-------------	------------	-----------

<i>signspace[.]cloud</i>	Domain	Attacker-controlled domain hosting MSaaS	2025-05-29	20:05
dc0acb01e3086ea8a9cb144a5f97810d291020ce	SignerSha-1	Certificate	2026-03-18	20:05
7e6d9dac619c04ae1b3c8c0906123e752ed66d63	SignerSha-1	Certificate	2026-03-21	20:05
f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc	SHA-256	File hash	2026-03-19	20:05
11af4566539ad3224e968194c7a9ad7b596460d8f6e423fc62d1ea5fc0724326	SHA-256	File hash	2026-03-21	20:05
f0a6b89ec7eee83274cd484cea526b970a3ef28038799b0a5774bb33c5793b55	SHA-256	File hash	2026-03-12	20:04

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the [Microsoft Threat Intelligence Blog](#).

To get notified about new publications and to join discussions on social media, follow us on [LinkedIn](#), [X \(formerly Twitter\)](#), and [Bluesky](#). To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the [Microsoft Threat Intelligence podcast](#).

Source: <https://www.microsoft.com/en-us/security/blog/2026/05/19/exposing-fox-tempest-a-malware-signing-service-operation/>