

Disrupting Fox Tempest: A cybercrime service that turned “verified” software into a pathway for ransomware

By Steven Masada

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

Every day, we decide what software to trust in seconds guided by simple labels such as “verified,” “secure,” and “safe to install.” The problem is that those signs can be manipulated.

Today, Microsoft unsealed a legal case in the US District Court for the Southern District of New York targeting a cybercrime service known as Fox Tempest, which, since May 2025, has enabled cybercriminals to disguise malware as legitimate software. The malware-signing-as-a-service (MSaaS) worked by fraudulently accessing and abusing code signing tools, such as Microsoft’s Artifact Signing, a system designed to verify that software is legitimate and hasn’t been tampered with. Cybercriminals used the service to deliver malware and enable ransomware and other attacks, infecting thousands of machines and compromising networks worldwide.

For the first time, Microsoft is taking public action against a powerful, but often unseen, enabler within the cybercrime ecosystem, targeting how cybercriminals prepare and employ techniques to optimize their rate of success. To disrupt the service, we seized Fox Tempest’s website *signspace[.]cloud*, took offline hundreds of the virtual machines running the operation, and blocked access to a site hosting the underlying code. This action builds upon [persistent internal efforts](#) to revoke fraudulently obtained code-signing certificates and enhance our defenses and employ new security features to detect and thwart such malicious activity. It’s already having an impact: cybercriminals are complaining about challenges accessing the current service.

Our impact extends beyond one actor. The lawsuit targets Fox Tempest’s infrastructure and also names [Vanilla Tempest](#) as a co-conspirator, a prominent ransomware group that used the service to [deploy malware](#) like Oyster, Lumma Stealer, and Vidar, and ransomware, including Rhysida, in multiple recent cyberattacks. Vanilla Tempest has targeted [schools](#), [hospitals](#), and other [critical organizations worldwide](#), while Rhysida, a highly evolved ransomware variant that both encrypts files and steals data, often used for double extortion, has been used by various actors in numerous high-profile attacks globally, including to steal and leak internal documents from the [British Library](#) and to disrupt operations at [Seattle-Tacoma International Airport](#). Microsoft’s investigation further linked Fox Tempest to various additional ransomware affiliates and families, including INC, Qilin, Akira, and others.

More broadly, this case points to how cybercrime is changing. What once required a single group to carry out an attack from start to finish is now broken into a modular ecosystem where services are bought and sold and work interchangeably with one another. Some services are inexpensive and widely used. Others, like Fox Tempest, are highly specialized and expensive because they remove friction or bypass obstacles that make attacks fail, making them both more reliable and harder to detect. As seen with Fox Tempest, when these services are combined with AI-powered tactics, attacks can scale more easily, reaching more people and becoming more convincing.

This kind of abuse isn't new, but it is evolving

Illicit [code-signing certificates](#) have been [sold and trafficked](#) for more than a decade. That includes its use by nation-state actors to target [critical infrastructure organizations](#) in Europe. What's changed is how this activity is marketed, packaged, and sold as a service, along with the scale at which it is now used across ransomware campaigns. Instead of buying certificates one-by-one, criminals upload their malware to a service that signs it for them.

What also makes this model notable is the level of investment. Unlike lower-cost services like [RedVDS](#), a cybercriminal infrastructure provider that costs as little as \$24 per month, which Microsoft disrupted earlier this year, Fox Tempest shows that more sophisticated actors are willing to pay thousands of dollars for advanced capabilities that make attacks easier to carry out, harder to detect, and more likely to succeed.

How Fox Tempest sold “legitimacy” at scale

Fox Tempest's business model was straightforward: sell fraudulent code-signing capability, let others package malware, and enable attacks downstream. The model has generated millions in proceeds, demonstrating significant financial profit.

Behind the scenes, the operators built access at scale. Using fabricated identities and impersonating legitimate organizations, they created hundreds of fraudulent Microsoft accounts to obtain real code-signing credentials in volume. Customers who paid for Fox Tempest's services could then upload malicious files via an online portal for them to be signed using Fox Tempest-controlled certificates. Cybercriminals paid thousands of dollars for the service, reflecting how valuable this capability was.

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

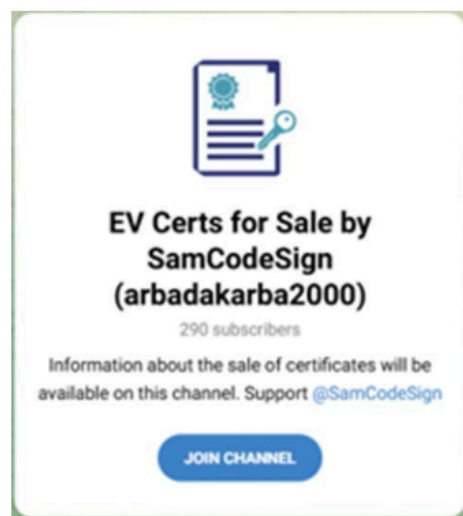
Можете оставить любой комментарий, предложение, вопрос, если требуется.

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

Your answer

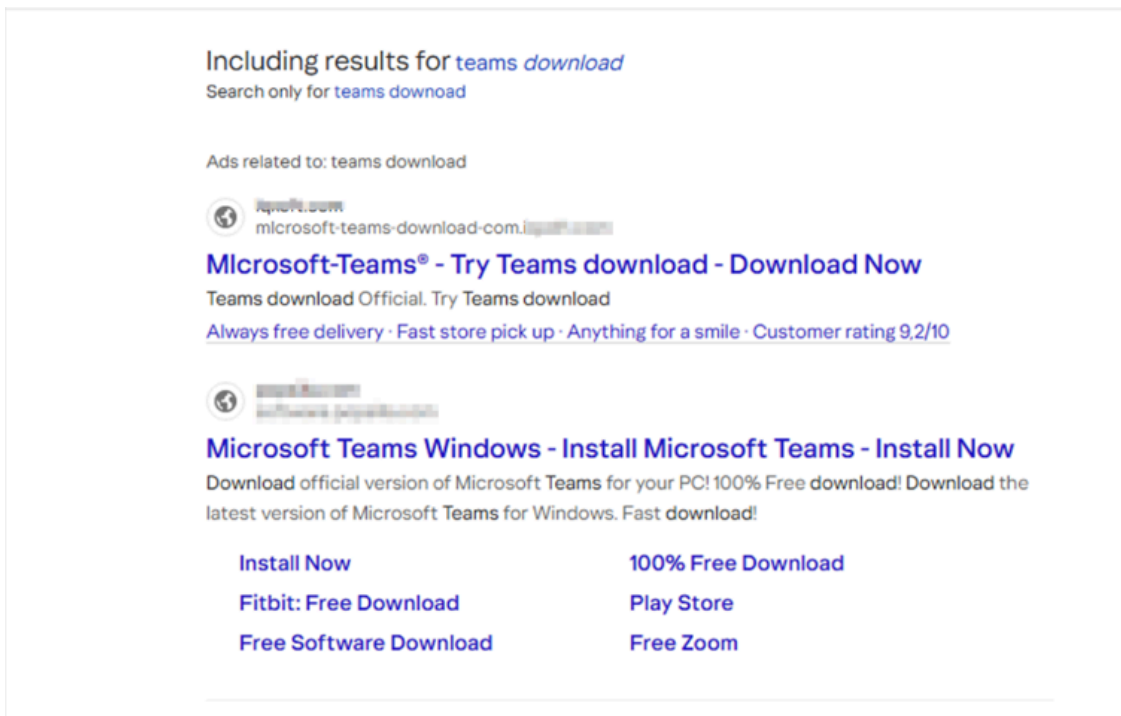
Submit

Clear form

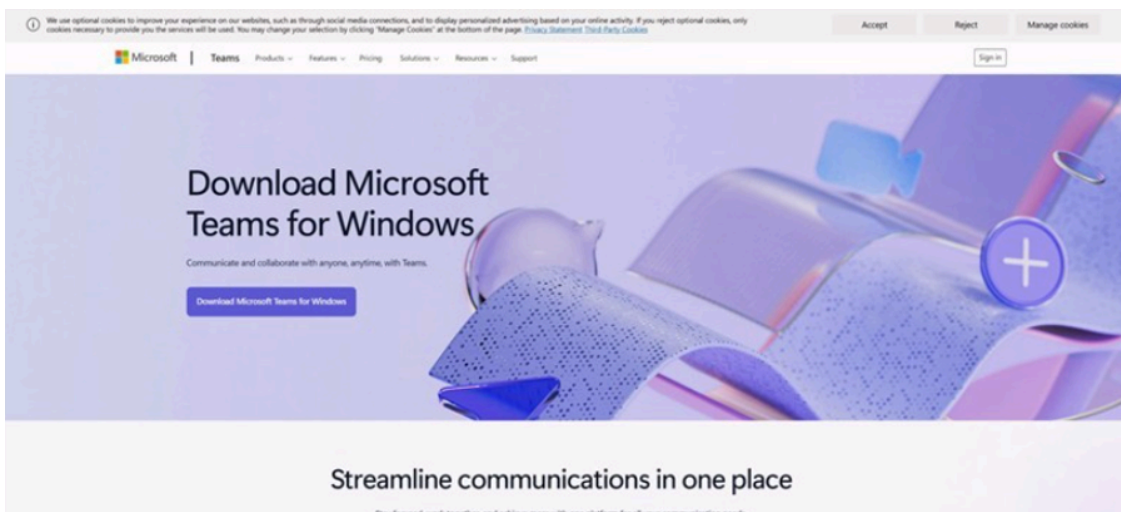


Fox Tempest’s pricing model form and Telegram channel where you could purchase the service. The more you pay, the quicker you get access to the service.

Once signed, their malware appeared legitimate. Attackers then distributed the signed malware through tactics such as search manipulation and malicious ads, where users are more likely to trust what they encounter. AI then helped generate and refine these campaigns to reach a broader audience.

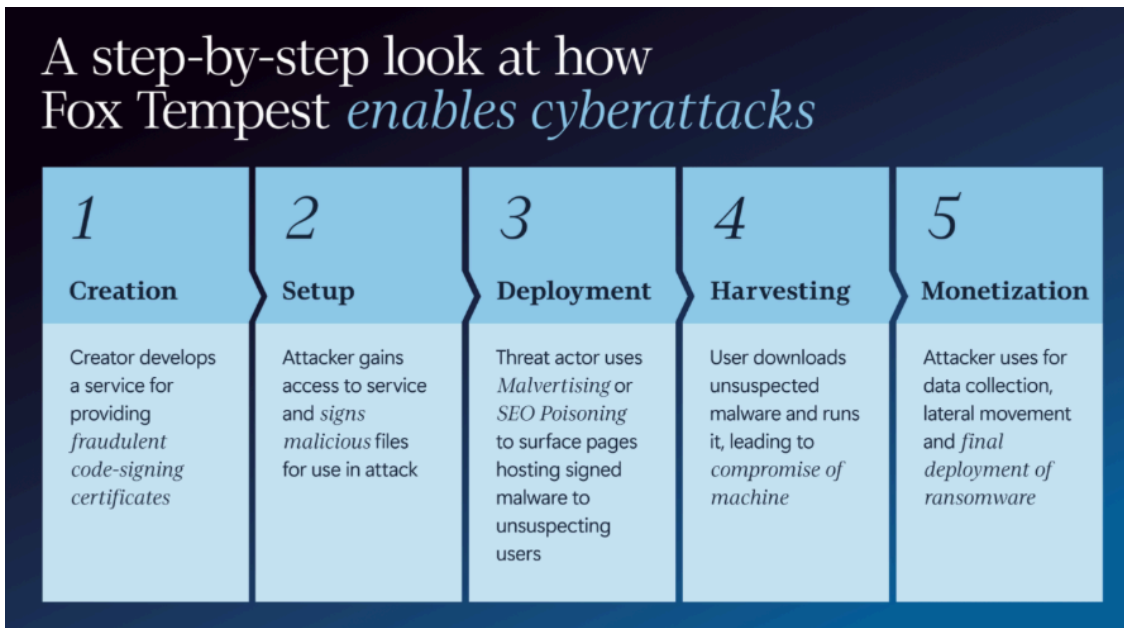


How code-signed malware appears in search results.



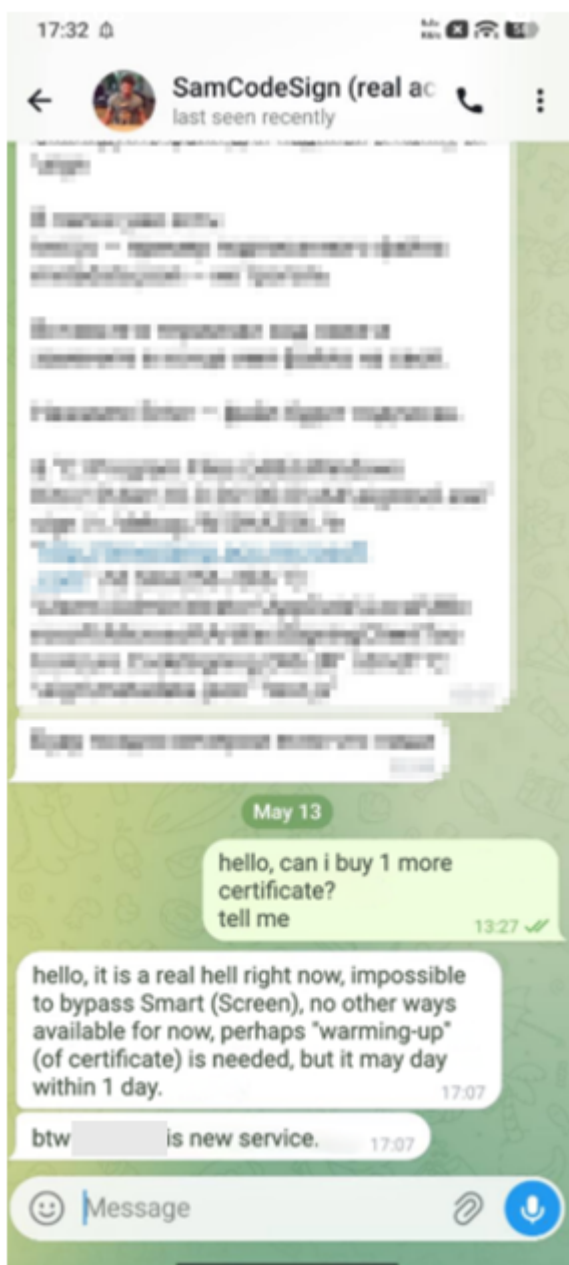
Fake Microsoft Teams download page and delivery mechanism for disguised code-signed malware

That changed the odds. Malicious software that should have been blocked or flagged by antivirus and other safeguards was more likely to be opened, allowed to run, or pass security checks—essentially allowing malware to hide in plain sight. Instead of forcing their way in, attackers could slip through the front door by masquerading as a welcomed guest.



An overview of malware-signing-as-a-service.

As Microsoft disabled fraudulent accounts, revoked fraudulently obtained certificates and introduced enhanced protections, the Fox Tempest operators continually adapted. In February 2026, they ultimately shifted to networks of third-party-hosted virtual machines to maintain and scale operations. That kind of rapid change is part of the model: these services evolve quickly in response to pressure and friction. In fact, Microsoft has observed further adaptations in response to our layered disruption efforts, with Fox Tempest attempting to shift operations and customers to another code-signing service.



Fox Tempest’s response to the disruptive efforts—translated from Russian by a third-party partner

In addition to seizing the core infrastructure behind the operation and degrading its ability to function at scale, we have taken further steps to prevent similar abuse, removing fraudulent accounts, strengthening verification, and limiting how this type of access can be reused. More technical details on the operation and the steps we’re taking to prevent similar abuse are available in this [Microsoft Threat Intelligence blog](#).

Cutting off a critical enabler of cybercrime

This action wasn’t about stopping one actor. It sought to strategically neutralize a vital service that many attackers, particularly ransomware groups, rely on. When legitimate code signing services are weaponized, everything downstream gets easier: malware looks legitimate, security warnings are less likely to trigger, and attacks are more likely to succeed. Degrading that capability adds friction and forces a reset. The success rates of attacks decrease, and attackers have to rebuild, find new ways in, and accept more risk with each attempt—driving up both the cost and the time required to operate.

Importantly, disruption actions don't happen in isolation and are never one-and-done. Collaboration is critical, as different organizations and sectors have visibility into different parts of the cybercrime ecosystem. In this case, we are working closely with cybersecurity company [Resecurity](#), whose insights help us better understand how Fox Tempest operates. We are also collaborating closely with [Europol's European Cybercrime Centre](#) (EC3) and the [Federal Bureau of Investigation](#) (FBI). As we've seen in previous efforts, we expect actors to try to rebuild. Collectively, we will continue to take action and keep the pressure on. That also means strengthening the code signing ecosystem through intelligence sharing and partnering with other code signing services, so it's harder for malicious actors to regain that ground in the first place.

When attackers can make malicious software look legitimate, it undermines how people and systems decide what's safe. Disrupting that capability is key to raising the cost of cybercrime. As threats evolve, the Microsoft Digital Crimes Unit will continue working with partners across industry and law enforcement to persistently identify and cut off the services that enable them.

For more than a decade, the Microsoft Digital Crimes Unit (DCU) has persistently disrupted cybercrime and nation-state threats targeting people, organizations, and critical infrastructure. Explore major disruptions—and the ongoing cases and operations behind them here: [Disrupting cyberthreats since 2008](#) | [Microsoft](#)

Tags: [Microsoft Digital Crimes Unit](#), [The Digital Crimes Unit](#)

Source: <https://blogs.microsoft.com/on-the-issues/2026/05/19/disrupting-fox-tempest-a-cybercrime-service/>