

Microsoft disrupts Fox Tempest malware-signing-as-a-service platform tied to ransomware gangs

By Jonathan Greig

Published: 2026-05-19 · Archived: 2026-08-05 02:00:11 UTC

Microsoft said it took down a critical service that helped cybercriminals slip through defenses by making malware look like legitimate software.

The company unsealed a legal case in U.S. District Court on Tuesday detailing the disruption of Fox Tempest — a popular service that has operated since May 2025 and provides cybercriminals with code signing tools.

The group abused Microsoft's Artifact Signing, which is designed to verify that software is legitimate and hasn't been tampered with.

Steven Masada, assistant general counsel at Microsoft's Digital Crimes Unit, said cybercriminals used the service to deliver malware and enable ransomware, infecting thousands of machines and compromising networks worldwide.

"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," he said.

"Instead of forcing their way in, attackers could slip through the front door by masquerading as a welcomed guest."

Masada explained that 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.

Ransomware affiliates tied to large groups like Rhysida, INC, Qilin and Akira would upload their malware to the Fox Tempest site, have it legitimized and then create fake websites masquerading as real platforms to download safe software.

This use of short-life certificates from a trusted source allowed malware and ransomware to resemble legitimate software like AnyDesk, Teams, Putty and Webex to bypass security controls, significantly increasing the likelihood of execution and successful delivery.

Masada noted that they seized Fox Tempest's website, took hundreds of virtual machines offline and blocked access to a site hosting the underlying code. He said Microsoft obtained evidence showing cybercriminals complaining about the actions.

"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."

Fox Tempest's MSaaS

Microsoft called the scheme malware-signing-as-a-service (MSaaS) and said Fox Tempest is a well-resourced operation that had departments handling infrastructure creation, customer relations, and financial transactions.

Fox Tempest used Microsoft Artifact Signing to create short-lived, fraudulent code-signing certificates.

The group has created over a thousand certificates and established hundreds of Azure tenants and subscriptions to support its operations. Microsoft said it has revoked over 1,000 code signing certificates attributed to Fox Tempest.

Microsoft security officials saw ransomware actors use the service to distribute malware families including Oyster, Lumma Stealer and Vidar. Hackers delivered the signed malware through purchased advertisements and links made to look like legitimate websites.

Microsoft analyzed cryptocurrency payments showing Fox Tempest was paid millions of dollars by ransomware affiliates and the tool was used in attacks targeting a range of organizations in the U.S. China, France and India.

The scheme, which charged users thousands of dollars, is evidence of how the cybercriminal ecosystem is evolving as disruption operations continue, Masada said. Cybercriminals now rely on an array of services that allow them to scale attacks and slip past defenses.

While cybercriminals have long sold illicit code-signing certificates, Fox Tempest showed how this activity is now sold as a service at scale.

“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,” Masada said.

“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.”

Get more insights with the

Recorded Future

Intelligence Cloud.

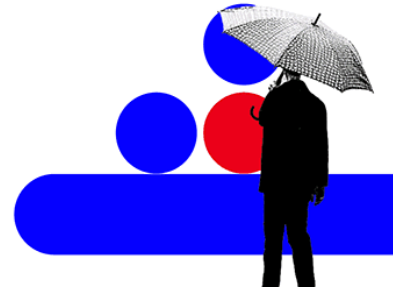
[Learn more.](#)



Know what matters.

Act first.

Get started



No previous article

No new articles



[Jonathan Greig](#)

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.

Source: <https://therecord.media/microsoft-disrupts-fox-tempest-malware-signing-service>