PRIMUS PARTNERS®

Quote by Devroop Dhar, Co-founder & CEO, Primus Partners

Published in CSO
November 03, 2025

Rhysida ransomware exploits Microsoft certificate to slip malware past defenses

The threat actor is weaponizing Microsoft's trusted signing system to deliver its OysterLoader malware through fake search ads.

Read on: https://www.csoonline.com/article/4083208/rhysida-ransomware-exploits-microsoft-certificate-to-slip-malware-past-defenses.html

Article Content: The Rhysida ransomware gang, known for targeting enterprises, has shifted to using malvertising campaigns to spread its malware. In its recent campaigns, the threat actor has impersonated fake download pages mimicking legitimate software such as Microsoft Teams, PuTTY and Zoom.

Rhysida group is deploying a malvertising technique to attack. The group purchases Bing search engine advertisements to put the links for convincing-looking, malicious landing pages for downloading software right in front of potential victims.

The ongoing malicious ad campaign has been delivering a malware called OysterLoader. An initial access tool (IAT), previously known as Broomstick and CleanUpLoader, is used to establish a foothold on a device so a second-stage persistent backdoor can be dropped on the system and establish long-term access, noted cybersecurity firm Expel.

Exploiting inherent trust

While the campaign begins through malvertising, Rhysida ransomware has deployed two strategies to evade detection or make it difficult to detect.

First, the group packages the malware. This technique is used to compress, encrypt, or obfuscate the function of the software, resulting in a low static detection rate when the malware is first seen.

Second, the Rhysida Ransomware group uses code-signing certificates by awarding their own malicious files a higher level of trust to appear legitimate. For this, the group is leveraging trusted signing from Microsoft.

“Microsoft Trusted Signing certificates are issued with a 72-hour validity period. After that, the certificates expire and need to be renewed. This short period makes the standard process of purchasing and reselling certificates infeasible. However, the Rhysida ransomware gang — or a supplier of theirs — has identified a means to abuse Microsoft’s Trusted Signing system, allowing them to sign files at scale,” Expel noted in its research.

“Signed binaries enjoy automatic trust inside Windows and many security tools, so they often pass through without scrutiny,” explained Amit Jaju, global partner/senior managing director – India at Ankura Consulting. “Real-time detection is tough because security controls traditionally treat signed files as safe. They even abused Microsoft’s Trusted Signing service, which led to over 200 certificates being revoked. By the time defenders catch on and revocations propagate, attackers have already moved to fresh certs. That time gap is their advantage.”

According to Expel’s latest analysis, Rhysida has dramatically increased its use of code-signing certificates. From merely seven certificates during its first Microsoft Teams malvertising campaign from May to September 2024, the second campaign, commencing June 2025, already has over 40 certificates. The dramatic increase in files and certificates indicates a higher operational tempo and resource investment, said the company.

Also, along with OysterLoader, the threat actor has used Latrodectus malware to get initial access to networks.

Identifying forensic signals

The campaigns that leverage trusted certificates undermine the trust model enterprises rely on. Signed malware bypasses app-allow lists, browser warnings, OS checks, and antivirus assumptions about signed code. When the file poses as Teams or PuTTY, employees don’t hesitate to download it as it looks normal.

“Once inside, the malware runs with fewer restrictions, grabs persistence, and brings in heavier payloads. It also complicates investigations because the usual red flags are missing. And since attackers piggyback on everyday software ecosystems, one endpoint foothold can turn into lateral movement and, eventually, ransomware fast,” added Jaju.

Experts say defenders must change their mindset. “We shouldn’t assume signed files are safe,” said Devroop Dhar, MD and co-founder at Primus Partners. “Start by checking where the installer came from, was it a vendor site or a sketchy search-ad link. These little details often tell the whole story. New or mismatched publisher names, or certificates issued unusually recently, should raise suspicion. On endpoints, look for rundll32, PowerShell, or msiexec process chains — not specific malware names, but recurring behavior patterns.”

Jaju added that defense now depends on behavioral analytics and proactive validation. “Use EDR that focuses on behavior instead of trust tags. pin certificates for mission-critical apps so only known-approved certs can run. Feed threat intelligence streams into detection pipelines so revocations and IOCs trigger action immediately. Add DNS controls and filtering to block fake download paths.”

Dhar emphasized that CISOs must treat signed malware and fake installers as part of today’s landscape. “The focus should shift to verification: where the file came from, who signed it, and what it did right after launch.” Both experts agree that the problem extends beyond individual organizations. Abuse of Microsoft’s trusted signing service exposes systemic cracks that demand tighter certificate vetting and stronger industry-wide oversight.