Warlock Ransomware: Old Actor, New Tricks?

The China-based actor behind the Warlock ransomware may not be a new player and has links to malicious activity dating as far back as 2019.

- Threat Intelligence
- 22 Oct 2025
- 5 Min Read

Share

The Warlock ransomware first appeared in June 2025 and made an impact weeks later, after attackers deploying it were discovered exploiting the ToolShell zero-day vulnerability in Microsoft SharePoint (CVE-2025-53770) on July 19, 2025.

Warlock is an unusual threat. Unlike many ransomware operations, which are headquartered in Russia or other countries in the Commonwealth of Independent States, Warlock appears to be used by a group based in China. And, while its name is new, its origins appear to date back much further, with links to a diverse range of activity.

ToolShell attacks

Warlock sprang to prominence following the ToolShell attacks. Prior to patching of this vulnerability, Microsoft said that three distinct actors, all of which it linked to China, had been exploiting it as a zero-day: Budworm (aka Linen Typhoon, APT27), Sheathminer (aka Violet Typhoon, APT31), and Storm-2603. Storm-2603 was using the exploit to deploy Warlock and another ransomware payload, LockBit. The new Warlock ransomware appears to be unrelated to an older ransomware threat named Warlock Dark Army.

Research published by CheckPoint on July 31 provided further details on Storm-2603's activities, noting that the group used multiple ransomware payloads and sometimes bundled them together. Payloads were often deployed using DLL sideloading, a popular tactic among Chinese groups. Another feature of its attacks was the use of a custom command and control (C&C) framework that appeared to be called ak47c2 by the attackers themselves.

Other vendors began sharing what they knew about the group. Palo Alto Unit 42 said what it called the Project AK47 toolkit used by Storm-2603 (which it calls CL-CRI-1040) included a backdoor, loaders that were deployed via DLL sideloading, and a ransomware payload called AK47/Anylock. The group also used the legitimate application 7zip (7z.exe) to sideload a loader named 7z.dll. The group had been recently linked to a ransomware site named Warlock Client. It too noted that the group had also been acting as a LockBit 3.0 affiliate.

Similar activity was uncovered by Symantec and Carbon Black in early August when an engineering company in the Middle East was attacked with Warlock. The attackers also used 7z.exe to sideload a loader named 7z.dll.

Most recently, Trend Micro published its own findings on Warlock, which suggested that the Warlock payload may simply be a rebrand of Anylock since it had observed Warlock appending encrypted files with the extension .x2anylock. Trend also threw more light on the LockBit connection, saying that the version of Warlock it analyzed appeared to be a modified version of the LockBit 3.0 payload.

Trend also noted that there may be a link to the now retired Black Basta ransomware operation, observing similarities in tactics, negotiation styles and victimology, suggesting "a possible offshoot or rebrand."

Trend's conclusion, that Warlock may be a rebrand of Anylock, is supported by findings from Symantec and Carbon Black. In an investigation into an attack against a U.S. firm in early August 2025, we found a ransomware payload attempting to encrypt files and appending the extensions .x2anylock, but the ransom note claimed the attack had been performed by Warlock. Again, the attackers sideloaded a malicious file named 7z.dll.

Links to earlier espionage attacks

While Warlock appears to be a rebrand of the older Anylock payload, some of the tools used in Warlock attacks suggest that the group behind Warlock has been active for a lot longer than previously known. In both Warlock attacks investigated by Symantec and Carbon Black in August 2025, the attackers deployed a

custom defense evasion tool, which was signed with a stolen digital certificate that appeared to come from a company or developer called coolschool (Serial: 4deb2644a5ad1488f98f6a8d6bca1fab).

This leveraged a vulnerable driver (SHA256: f6ee01303cf1d68015eee49f7dc7f26151a04ae642a47e49c70806931ce652d3) to try and disable security software on infected systems using the Bring Your Own Vulnerable Driver (BYOVD) technique. The driver was an old Baidu anti-virus driver dating from 2016 with an expired certificate. It was renamed googleapiutil64.sys, likely as a bid to make it appear less suspicious.

This coolschool stolen certificate appears to have been in use as far back as 2022, when it was used to sign Cobalt Strike and BYOVD-related malware uploaded to VirusTotal. In 2022, researchers at TeamT5 linked the stolen certificate to an APT group they dubbed CamoFei, who appeared to be Chinese threat actors that had been active since at least 2019. The group was involved in a diverse range of attacks, ranging from espionage, to denial-of-service, to ransomware. Its ransomware payload, known as CatB, had been signed with the same coolschool certificate.

Similar attacks continued until at least 2024. SentinelOne, which calls the group ChamelGang, said it had staged attacks against organizations in the U.S., Brazil, India, Russia, Taiwan and Japan. This included attacks on the Presidency of Brazil and the All-India Institute of Medical Sciences (AIIMS). Noting the group's targeting, SentinelOne commented on the blurring of the lines between espionage and cybercrime attacks, noting that in some cases, ransomware attacks could be used to misattribute or cover up evidence of espionage intrusions.

Emergent China cybercrime nexus

Although the toolset used by this group has evolved over time, the links to earlier attacks suggest that some, if not all the actors, behind Warlock may have been active since 2019. The diverse range of attacks the group has been involved in suggests they may be contractors, willing to sell their services to entities involved in espionage but also not above generating additional income from ransomware attacks. Indeed, it's involvement in ransomware may at times be useful to obfuscate or cover up espionage activities.

The involvement of Chinese espionage actors in ransomware is a growing phenomenon. In February of this year, Symantec and Carbon Black uncovered evidence of a Chinese espionage actor, seemingly moonlighting as an affiliate for RA World ransomware. The attackers behind Warlock appear to be a different breed, with cybercrime not a sideline, but one of the group's core activities.

Protection/Mitigation

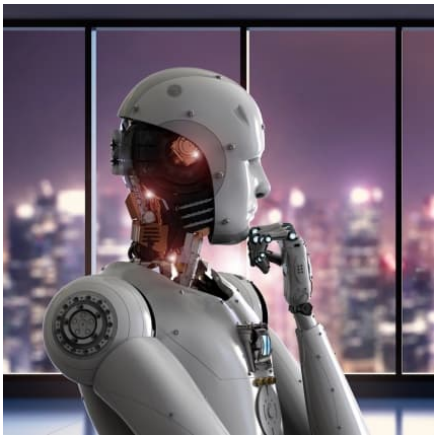
For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

9d52af33c05ea80f9bc47404b02ace4e16203dd81aef9021924885a6bff1d3c1 - Loader (7z.dll)
15649e4d246fe6d03dc75ecb4cabe5d1f8723519ed8dd3176e1a97325e827daf - Loader (7z.dll)
24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf - Curl Backdoor
f6ee01303cf1d68015eee49f7dc7f26151a04ae642a47e49c70806931ce652d3 - Vulnerable driver
edcf76600cd11ef7d6a5c319087041abc604e571239fe2dae4bca83688821a3a - LockBit 3.0
e23d5cb32a2d62314a8b26a205b634ee968f5a0500c190bc6edb55ec70285eb5 - Defense Evasion Tool
9f2434d5f8d042323cc7964520d99bda661bb23ce505cb03c8a07758bc9397a6 - Defense Evasion Tool
8ca7304846c69300237a8577fbeec2720ea9a4bd09cb7fe484a8d5efc79ad073 - Defense Evasion Tool
bba75dc056ef7f9c4ade39b32174c5980233fc1551c41aca9487019191764bac - Defense Evasion Tool
ca2c02f592d72cafc218f4edd1ea771f8d1458cb95c2c76c3e384e63cefd1fb6 - Warlock
6feb5361fd3abd3a7a733c30bfcc2b58fc774ac6aa91a468ce2e31dcffc9d4de - Warlock
2c9f0f324e9cca0481162cdc21ee9b60a7541941a33af99113d08bbd859d7473 - Warlock

About the Author



Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.

You might also enjoy