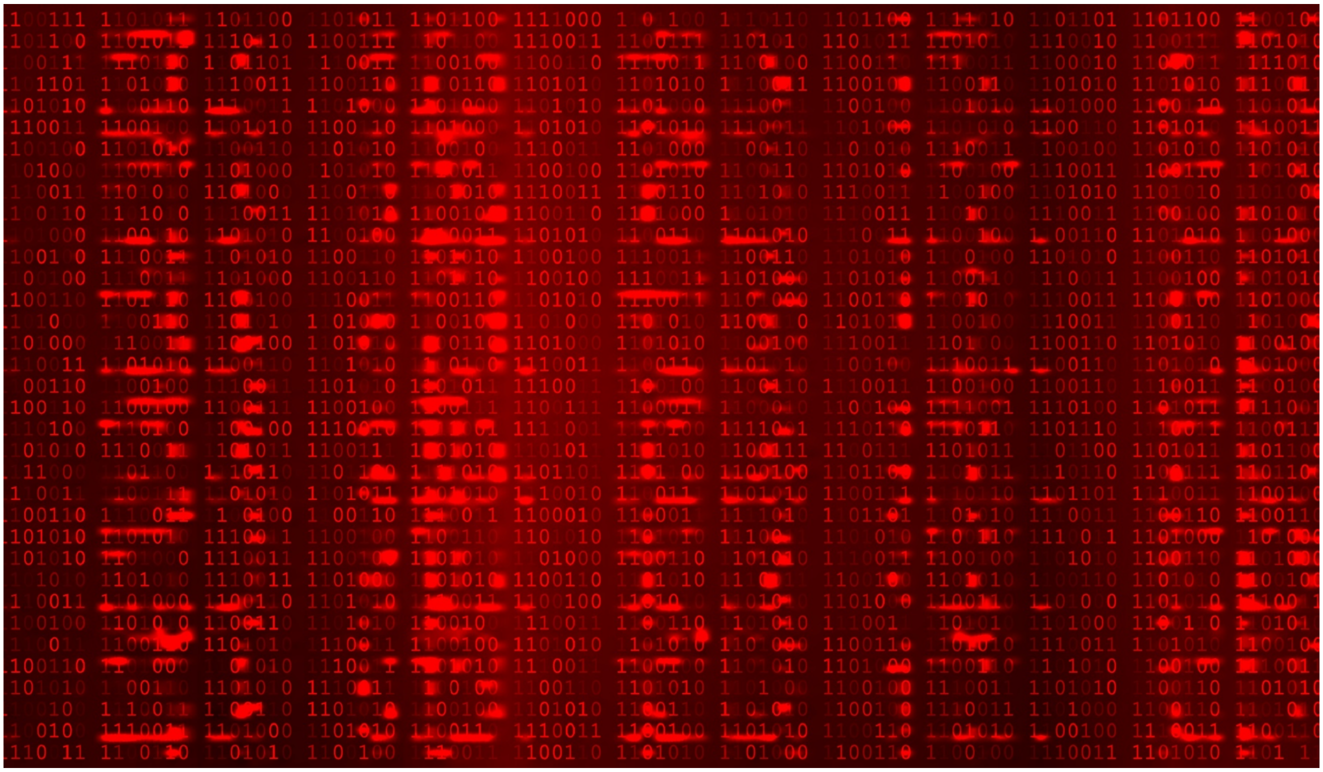
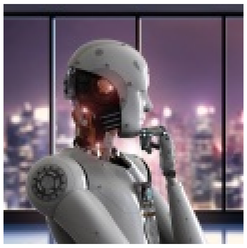
China-linked Espionage Tools Used in Ransomware Attacks

security.com/threat-intelligence/chinese-espionage-ransomware





Threat Hunter TeamSymantec

Tools that are usually associated with China-based espionage actors were recently deployed in an attack involving the RA World ransomware against an Asian software and services company.

During the attack in late 2024, the attacker deployed a distinct toolset that had previously been used by a China-linked actor in classic espionage attacks.

While tools associated with China-based espionage groups are often shared resources, many aren't publicly available and aren't usually associated with cybercrime activity.

Prior Espionage Attacks

In all the prior intrusions involving the toolset, the attacker appeared to be engaged in classic espionage, seemingly solely interested in maintaining a persistent presence on the targeted organizations by installing backdoors.

In July 2024, an attacker compromised the Foreign Ministry of a country in southeastern Europe. The attacker leveraged a legitimate Toshiba executable named toshdpdb.exe to sideload a malicious DLL named toshdpapi.dll. This DLL acts as a loader for a heavily obfuscated payload that is contained in a file called TosHdp.dat.

The payload is encrypted with the RC4 decryption key: 20240120@@@. Analysis of the decrypted payload revealed that it is a variant of PlugX (aka Korplug), a custom backdoor that is not publicly available malware and is only associated with China-linked espionage actors. To date, it has never been used by actors based in other countries. Features of this variant included encrypted strings, dynamic API resolution, and control flow flattening. Its configuration was encrypted using the RC4 key qwedfgx202211.

The PlugX plugins compilation timestamps for this variant were identical to those in the Thor PlugX variant, documented by Palo Alto, which was linked to Fireant (aka Mustang Panda, Earth Preta), a China-based espionage group.

The variant also has some similarities to the PlugX type 2 variant documented by Trend Micro, which has also been linked to Fireant. The configuration was encrypted using the same RC4 key (qwedfgx202211), and both variants had similar configuration structures.

Further espionage attacks involving the same PlugX variant followed. In August 2024, the attacker compromised the government of another southeastern European country. Also in August 2024, the attacker compromised a government ministry in a Southeast Asian country. In September 2024, they briefly compromised a telecoms operator in the region, and in January 2025, the attacker targeted a government ministry in another Southeast Asian country.

Ransomware Attack

In the midst of these apparent espionage attacks, in late November 2024, the same toolset was used in connection with a criminal extortion campaign against a medium-sized software and services company in South Asia.

While no infection vector was found, the attacker later claimed that the target’s network was compromised by exploiting a known vulnerability in Palo Alto’s PAN-OS (CVE-2024-0012) firewall software. The attacker then said administrative credentials were obtained from the company’s intranet before stealing Amazon S3 cloud credentials from its Veeam server, using them to steal data from its S3 buckets before encrypting computers.

The attacker leveraged the same Toshiba executable (toshdpdb.exe) to sideload the malicious DLL named toshdpapi.dll. This DLL acts as a loader, and when executed, it searches for a file named toshdp.dat in the current folder and decrypts it. The decrypted payload from the toshdp.dat file is the same PlugX variant observed in the prior espionage attacks.

Machines on the target's network were encrypted with the RA World ransomware. The attacker demanded a $2 million ransom, which would be reduced to $1 million if paid within three days.

Hypotheses

There is evidence to suggest that this attacker may have been involved in ransomware for some time. In a report on RA World attacks, Palo Alto said that it had found some links to Bronze Starlight (aka Emperor Dragonfly), a China-based actor that deploys different ransomware payloads. One of the tools used in this ransomware attack was a proxy tool called NPS, which was created by a China-based developer. This has previously been used by Bronze Starlight. SentinelOne, meanwhile, reported that Bronze Starlight had been involved in attacks involving the LockFile, AtomSilo, NightSky, and LockBit ransomware families.

It is unclear why an actor who appears to be linked to espionage operations is also mounting a ransomware attack. While this is not unusual for North Korean threat actors to engage in financially motivated attacks to subsidize their operations, there is no similar history for China-based espionage threat actors, and there is no obvious reason why they would pursue this strategy.

Another possibility is that the ransomware was used to cover up evidence of the intrusion or act as a decoy to draw attention away from the true nature of the espionage attacks. However, the ransomware deployment was not very effective at covering up the tools used in the intrusion, particularly those linking it back to prior espionage attacks. Secondly, the ransomware target was not a strategically significant organization and was something of an outlier compared to the espionage targets. It seems unusual that the attacker would go to such lengths to cover up the nature of their campaign. Finally, the attacker seemed to be serious about collecting a ransom from the victim and appeared to have spent time corresponding with them. This usually wouldn't be the case if the ransomware attack was simply a diversion.

The most likely scenario is that an actor, possibly one individual, was attempting to make some money on the side using their employer's toolkit.

Protection/Mitigation

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

Indicators of Compromise

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

7bae7f21bd4adf84eb3cc281fcc3d5fc3d1e47edd0dadd86587ce8ec63df1b8f — toshdpdb.exe (benign)

c1e6955acdefa9769a7ae0c1abf54a26e2158154dd6ec07cc71eb06c575193d5 — toshdpapi.dll

18127cfd08cc49be08714d29e09ec130dcc0b19b7fcddc22c71d28fd245eb1b1 — toshdpapi.dll

e177eb358f93ccc1ac4694feb0139e82c62d767388872d359d7c2ed0a05c2726 — toshdpapi.dll

6ac81aa8d3f9d86ad5a18ea42fa1829b055dd25f123f9ee90002d64d4ef7a394 — toshdp.dat

2707612939677e8ea4709ecb4f45953d4a136a9934b6d0c256917383cdaef813 — RA World

38a26fffbab5297e4229897654d2f67c6ee52b316c7ac4d4a1493d187b49ec25 — RA World

bb5740d2129663ae1c46b1ea1bdd0b8c423b6eb8f6e6f2b0b158a9e833496a01 — NPS Proxy Tool

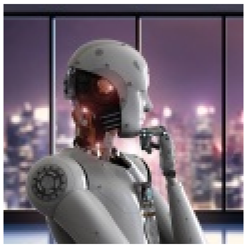
plugins.jetbrians[.]net — NPS Proxy C&C

police.tracksyscloud[.]com — PlugX C&C

caco.blueskyanalytics[.]net — PlugX download server

158.247.213[.]167 — NPS Proxy C&C

154.223.18[.]123 — PlugX download server



About the Author

Threat Hunter Team

Symantec

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