Venafi

The Rise of Code Signing as a Major Attack Vector

Extensive research has found that compromised code signing certificates used in supply chain attacks are the primary goal of Chinese threat actors APT41, also known as Winnti Group.

Recent analysis shows that this group spent the last decade honing attack methods to compromise code signing keys and certificates in "low value" targets like gaming and adware organizations. These certificates are then used in a wide variety of targeted cyberespionage attacks in the software, hardware, media, healthcare, high-tech and telecommunications sectors.

INDUSTRIES TARGETED

Code Signing and Threat Actors

Malicious code that uses a legitimate code signing certificate from a trusted developer will not only allow adversaries to execute code on a secured system, but also enable the malicious code to go unnoticed.

APT41

APT41 has been observed using at least 46 different code families and tools. The most relevant tools are highlighted here:

1 CHINA CHOPPER: One of APT41's primary weapons; used as a backdoor; includes a loader, dynamic-link library (DLL), and a rootkit; also used often by APT17.

2 HIGHNOON.BIN: Modified version of Windows DLL apphelp.dll, used for persistence.

3 HIGHNOON.LITE: Standalone, non-persistent version of HIGHNOON, can download and execute memory-resident modules after C2 authentication.

4 PHOTO: DLL backdoor that conducts system reconnaissance.

5 COLDJAVA: Backdoor that inserts shellcode and Black Coffee variant into the Windows registry.

6 BLACK COFFEE: Has multiple capabilities; from reverse shell, file enumeration, and deletion to C2 communication through legitimate websites, and obfuscating traffic.

7 CHINA CHOPPER: Code injection web shell that can execute Microsoft .NET code within HTTP POST commands.

8 SOGU: Backdoor.

9 JUMPALL: Malware dropper which is known to have dropped variants of HIGHNOON, ZXSHELL, and SOGU.

10 HOMEUNIX: Launcher for download plugins used by many other Chinese espionage groups such as APT1, APT10, APT17, APT18, and APT20.

11 LIFEBOAT: Backdoor, communicates with C2 server via HTTP.

12 ZXSHELL: Backdoor.

14 POTROAST: Backdoor.

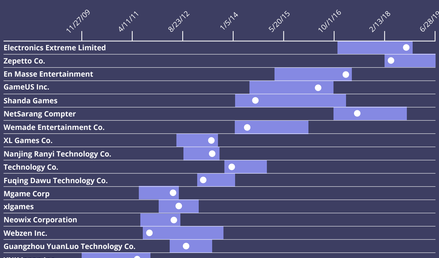
14 SWEET-CANDLE: Downloader that can download and execute payload from C2 server.4

Modus Operandi: The Anatomy of an APT41 Attack

APT41 specifically targets the production environment of software development companies.

They then use their access to the production environments to get gain access to higher level targets by compromising the supply chain of the initial victim, injecting malicious code into legitimate commercial software that is then distributed to organizations who use the software.

Observed use of code signing certificates from FireEye report



Which Industries Does APT41 Target?

The group has been observed targeting the following sectors:

- Software development
- Hardware manufacturers
- Telecommunication
- Media
- Video game
- Non-profit organizations
- Universities
- Think tanks
- Retail
- Travel services
- Virtual currencies
- Healthcare
- Biomedical and pharmaceutical
- Foreign governments
- Aviation
- Pro-democracy politicians and activists

The primary targets for these attacks have been in the United States and east Asia. However, Germany, Indonesia, the Russian Federation, South Korea, China, Sweden, Thailand, Turkey, Japan and Hong Kong have also been targeted as well as organizations in other countries.

APT41

APT41 is reported to be responsible for several high-profile supply-chain attacks against the software industry which lead to the distribution of trojanized software to more victims:

- **2014** — Online games distributed by a Southeast Asian video game distributor
- **March 2017** — CCleaner Utility
- **June 2017** — Netsarang software packages (aka ShadowPad)
- **June-November 2018** — ASUS Live Update utility (aka ShadowHammer)
- **July 2018** — Southeast Asian video game distributor
- **March 2019** — Games and development application in Asia trojanized with a backdoor
- **February 2020** — South Korea and Taiwan video game developers backdoored
- **January 2021** — Attacks on Russian game developers
- **March 2021** — Operation "ColumnTK" big airline heist
- **April 2021** — Major Mongolian CA backdoored

Conclusion: Protecting Software Development Pipelines

Security and development teams may want to use the following controls as a checklist for evaluation of security best practices for software development and build environments.

Control 1 Restrict administrative access to CI/CD tools.

Control 2 Only accept commits signed with a developer GPG key.

Control 3 Automation access keys expire automatically.

Control 4 Reduce automation access to read-only.

Control 5 Only dependencies from trusted registries can be used.

Control 6 Any critical or high-severity vulnerability breaks the build.

Control 7 Store artifacts in a repository in development, stage and production.

Control 8 Validate artifact digest.

Control 9 Pull-requests require two reviewers and a passing build to be merged.

Control 10 Artifacts in higher repositories are signed.

Control 11 Available container images don't have high or critical vulnerabilities.

Control 12 Validate artifact signatures and digests.

Control 13 Scan deployed images in production.

Control 14 Validate Kubernetes resource manifests.

Control 15 Ensure build environments are ephemeral and immutable.

Get the full details on these industry-recommended software security controls and the potential exposures they limit at
https://github.com/Venafi/blueprint-securesoftwarepipeline#readme