VENAFI®

Protect Your Machine Identities

Threat Bulletin:

Report Released about Chinese Hackers Who Are Stealing Code-Signing Certificates

These certificates are then used in attacks by other groups, including Chinese intelligence agencies

Report:
Burning Umbrella an Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers. By Tom Hegel, May 3, 2018

Article Summarizing Report:
Report: Chinese Actors Steal Code-Signing Certificates. By Jeremy Kirk, May 7, 2018

Venafi Case Study:
Global Technology Provider Secures Code-signing Certificates to Safeguard Its Brand

---

What's in the Report?
The report is based on research conducted by ProductWise, a security vendor. The research reveals that Chinese hackers are stealing legitimate code-signing certificates for use in malware attacks to make the malware code look legitimate. These hacker groups pool resources for use by other groups in attacks, including Chinese intelligence agencies.

Why is Code Signing Important?
When the company's code is signed using certificates, this confirms both the company as author and the integrity of the software. The company's customers expect products signed with the company's code-signing certificates to be secure—they must be able to rely on the brand to deliver safe products.

How Are Code-Signing Certificates Used in Attacks?
Attackers compromise code-signing certificates from legitimate organizations and use them to sign malicious code. Because the malicious code is signed with a stolen, legitimate certificate, it does not trigger any warnings by security controls, and unsuspecting users will trust that the application is safe to install and use.

How Do Hackers Get Code-Signing Certificates?
Hackers gain access to a network through traditional phishing and email scam methods and then look for storage devices that store code-signing certificates. When organizations use best-practices, code-signing certificates should remain secure. This is why hackers are targeting smaller organizations who may not use best-practices in their security infrastructure. In these smaller organizations, their code-signing keys and certificates are often stored on a local machine or network shared storage where they are easy to find.

How Can Venafi Help?
Venafi safeguards the code-signing key and certificate lifecycle from attack:

- Securing the request and issuance process for code-signing from abuse and attack
- Safely generating code-signing keys and requesting code-signing certificates
- Issuing keys and certificates according to approved workflow
- Logging all code-signing certificate requests
- Delivering all code-signing certificates only to authorized users

The protection provided by the Venafi Platform prevents attackers from manipulating the certificate request process to acquire a valid code-signing certificate. Venafi partners with CAs, including DigiCert, the leading issuer of enterprise code-signing certificates, to better secure the certificate issuance process.

For more information on how Venafi can secure code-signing certificates, read the case study: Global Technology Provider Secures Code-signing Certificates to Safeguard Its Brand

"We don't want to be the owner of a certificate that was used to sign malware. We need to secure our business and brand as a trusted technology and security company—and securing the certificate-signing process needs to be part of that effort…

People trust our brand—that trust is part of all of our product sales. To maintain this trust, we use Venafi as a gateway that imposes consistent, predictable key and certificate security across the enterprise."

Solution Architect, Global Technology Provider