What is Code-Signed malware and how to avoid this malware?

Code signing is a method of using certificate-based digital signatures for a software for the operating system and users to determine its safety. What is code-signed malware and how does it work?

Code signing is a method of using certificate-based digital signatures for a software for the operating system and users to determine its safety. Only the right software can use its corresponding digital signature.

Users can download, install software safely and developers protect their product reputation with Code signing. However, hackers and malware distributors are using that exact system to malicious code through antivirus software and other security programs. So what is Code-signed malware and how does it work?

1. Remove root malware (malware) on Windows 10 computers
2. Top 10 most dangerous malware types with bank accounts
3. Learn about polymorphic malware and super polymorphism

What is Code Signed malware?

When the software is digitally signed, it has an official digital signature. The Certificate Authority certifies a software to identify software that is legitimate and safe to use.

Users will not have to worry because the operating system will check the certificate and verify the digital signature. For example, Windows uses a certificate chain that contains all the certificates needed to ensure legitimate software.

The certificate chain contains all the certificates needed to certify the object identified by the last certificate. In fact, it includes the end certificate, the intermediate CA certificate, and the root CA certificate trusted by all parties in the chain. Each intermediate CA certificate in the string contains a certificate issued by the CA on it. The root CA issues the certificate for itself.

When the system works, you can trust the software, Code signing system and CA. Malware is malicious, unreliable and has no access to the Certificate Authority or Code signing.

Hacker steals certificates from the Certificate Authority

Antivirus software knows malware is malicious because it adversely affects your system. It activates alerts, users reporting incidents and antivirus software can create malware signatures to protect other computers using the same antivirus engine.

However, if malware creators can sign malicious code using official digital letters, the process will not happen. Instead, Code-singed malware can penetrate the system by official means because your anti-virus software and operating system do not detect anything dangerous.

According to Trend Micro's research, the entire malware market is focused on supporting Code-signed malware development and distribution. Malware operators have access to valid credentials used to sign malicious code. The following table shows the number of malware using Code signing to evade antivirus software since April 2018.

Type	Number of software	Signed (overall downloads)	Number of software	Signed (browser-only downloads)
Trojan	22,413	59.9%	12,827	81.3%
Dropper	43,423	85.6%	33,820	95.4%
Ransomware	563	44.4%	313	68.7%
Bot	1,092	1.5%	268	2.2%
Worm	201	5.5%	57	12.3%
Spyware	80	21.2%	40	25.0%
Banker	1,719	1.2%	272	1.8%
FakeAV	987	2.8%	446	4.5%
Adware	29,345	43.1%	8,792	91.8%
PUP	31,018	76.0%	21,792	79.6%
Undefined	60,609	65.1%	42,614	71.3%
Benign (total)	43,601	30.7%	30,346	32.1%
Unknown (total)	1,626,901	38.4%	1,227,241	42.1%
Malicious (total)	191,450	66%	121,241	81%

Trend Micro's research also shows that about 66% of malware has digital signatures. In addition, there are specific types of malware that have many digital signature versions such as Trojans, droppers and ransomware.

Where does the Code signing certificate come from?

Malware distributors and developers have two ways to create code-signed malware. They steal certificates from the Certificate Authority by directly or redeeming or forging a legitimate organization and requesting certificates from CA.

As you can see, CA is not the only place hackers target. Distributors who have access to legal certificates can sell trusted digital signature certificates to malware developers and distributors.

A Masaryk University security research team in the Czech Republic and the Maryland Cybersecurity Center found four organizations selling Microsoft Authenticode certificates to anonymous buyers. When a malware developer has a Microsoft Authenticode certificate, they can sign any malware that can be via certificate and Code signing protection.

In some cases, instead of stealing certificates, hackers will hack into the server to build the software. When the new software version is released, it will have a legitimate certificate, hackers take advantage of this process to add malicious code.

Example of Code-signed malware

So, what does Code-signed malware look like? Here are three examples of this type of malware.

1. **Stuxnet malware** : This malicious software destroys Iran's nuclear program using two stealing certificates and 4 zero-day vulnerabilities. These certificates are stolen from the companies JMicron and Realtek. Stuxnet uses stolen certificates to avoid the need for a new Windows introduction, but all drivers require verification.
2. **Asus server breach:** Between June and November 2018, hackers hacked into an Asus server that companies use to push software updates to users. Research at Kaspersky Lab revealed that about 500,000 Windows devices received this malicious update before being detected. Without stealing the certificate, these hackers sign the Asus digital certificate for their malware before the software server distributes the system update.
3. **Flame malware: The** variant of the malware module Flame targets Middle Eastern countries, using fraudulent certificates to avoid detection. Flame developers have used a weak encryption algorithm to sign fake digital certificates signing, making it appear as if Microsoft signed them. Unlike Stuxnet for destructive purposes, Flame is a spy tool, looking for PDF files, AutoCAD, text files and other important industrial documents.

How to avoid Code-signed malware?

This malware uses Code signing to avoid anti-virus software and detection systems, so it is extremely difficult to protect against Code-signed malware. Always updating antivirus software, the system is necessary, avoid clicking on unknown links and carefully check where the link comes from before following it. Refer to the article Risks from malware and prevention.