Malware authors increasingly use legitimate certificates to bypass defences

Reference: Memo [190524-1] Date: 24/05/2019 - Version: 1.0
Keywords: digital certificates, digital infrastructure
Sources: publicly available information

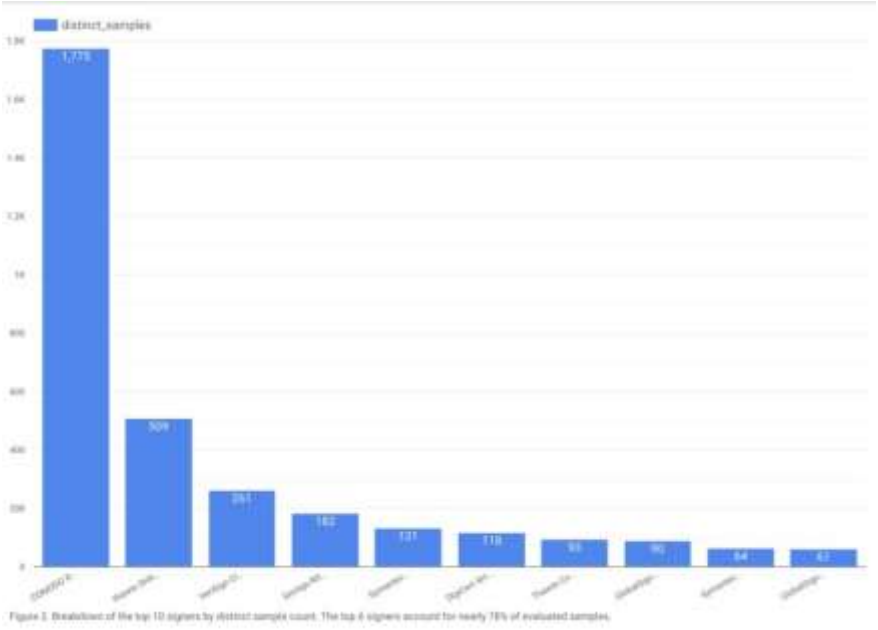
Key Points

- Malware authors increasingly use legitimate certificates to sign their code.
- Certificate authorities sometimes fail to verify the identities of people applying for code-signing certificates.
- Signing malware with legitimate certificates increases the chance of remaining undetected.

Summary

A recent study has found that malware is increasingly signed by legitimate certificates, obtained directly or indirectly from certificate authorities (CA) or their resellers. The study revealed that 3,815 signed malware samples were uploaded to VirusTotal scanning service over a period of one year. The researchers focussed on Windows Portable Executable (PE) files with more than fifteen detections. Certificates from Sectigo, Thawte, VeriSign, Symantec, DigiCert, GlobalSign, WoSign, Go Daddy, WoTrus, GDCA, Certum, E-Tugra, and Entrust were among the abused ones. This is in contrast with an earlier trend that if malware was signed, it was usually done with a stolen certificate. Most of the digital certificates used to sign malware samples found on VirusTotal in 2018 have been issued by the Certificate Authority (CA) Comodo CA (aka Sectigo).

There are also clear indications that the CA-s are fighting back by revoking certificates used by malicious actors.



Breakdown of the top 10 signers by distinct sample count. The top 6 signers account for nearly 78% of evaluated samples

Source: Chronicle Blog

Comments

Digital certificates cryptographically vouch for the trustworthiness of the software's publisher. They tell an operating system that the software is legitimate. Therefore, malware creators have long tried to use certificates to increase the chances of their creations to go undetected by anti-malware measures. Perhaps the first widely known use of certificates was by Stuxnet (2010), although it was not the first malware to try that. The creators of the famous nuclear-centrifuge-destroying cyber weapon used certificates stolen from JMicron and Realtek. In 2015, a powerful advanced persistent threat (APT) group dubbed Duqu deployed a sophisticated malware platform that attempted to infect the venues for some of high level P5+1 talks about the Iranian nuclear deal. Attackers used certificates from hardware manufacturers such as Foxconn, Realtek and Jmicron.

However, this particular research summarised in this Memo talks about certificates being legitimately obtained and used in malware propagation. Stolen certificates, provided that the CA and the owner knows that they have been stolen, usually get revoked. To avoid this, getting a valid certificate, vouched for by a trusted CA, is a much safer way of signing malware.

The ability of malicious actors to buy trust exposes inherent flaws of the current chain of security vouching. Here the CA-s would need to do more to make sure that whoever they sell their certificates to, do not plan to abuse their commercially obtained trust and use it for malicious purposes.