MUST READ Code Signing certificates becoming popular cybercrime commodity

Code Signing certificates becoming popular cybercrime commodity

October 9, 2015 By Pierluigi Paganini

Learn what Certificates as a Service stand for, discover why Code Signing certificates are a precious commodity and find out how to protect yourself online.

A recent phenomenon tracked by IBM Security X-Force researchers is the CaaS (Certificates as a

service). Cybercriminals would use the Dark Web for selling high-grade code certificates -which have obtained from trusted certificate authorities- to anyone that is interested in purchasing th

Sales of code signing certificates have increased considerably over the past few months, accord to X-Force researchers who have also provided some best practice guides on checking for truste certificates.

Talking about certificates

Why were certificates created? Their purpose is to generate trust and validation in software of c run on the machines. Using certificates, we can be safe about things like that a file has arrived f a valid source, it is not tampered with and its origin is open so we can validate its publisher.

Who issues the certificates and to whom are they granted? They are issued by the certificate authorities (CAs) and are granted to companies that generate code, protocols or software so th can sign their code and indicate its legitimacy and originality.

Talking about the importance of the certificates

ges, assur

they are genuine and issued from a trusted publisher. Users would receive alerts in an attempt to install files that are not accompanied with a valid certificate.

This is why cybercriminals aim to use certificates for legitimizing the malware code they make.

Cybercriminals using signed malware

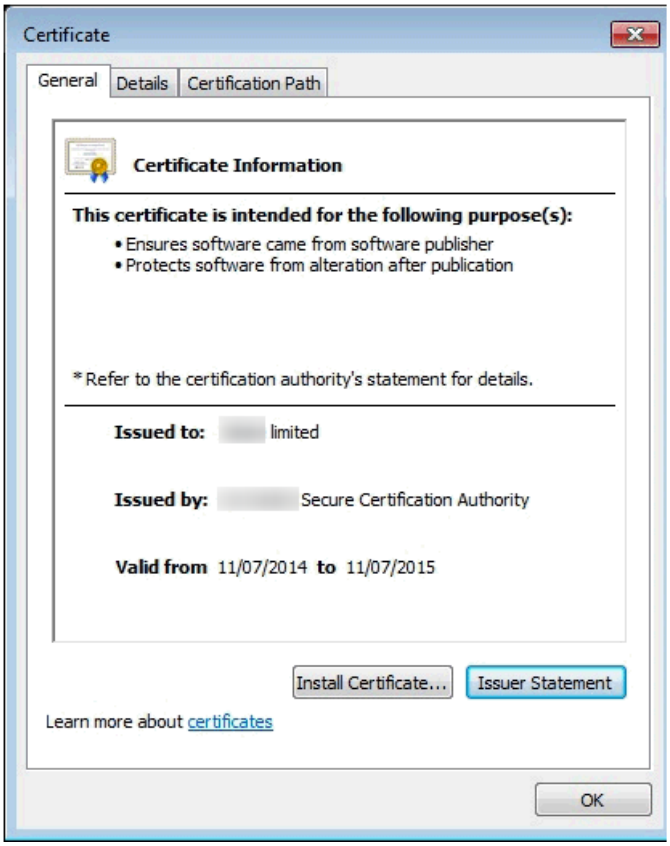
When cybercriminal create malicious code, their purpose is to make it appear as legitimate as possible. This is done by using signing certificates to sign their code.

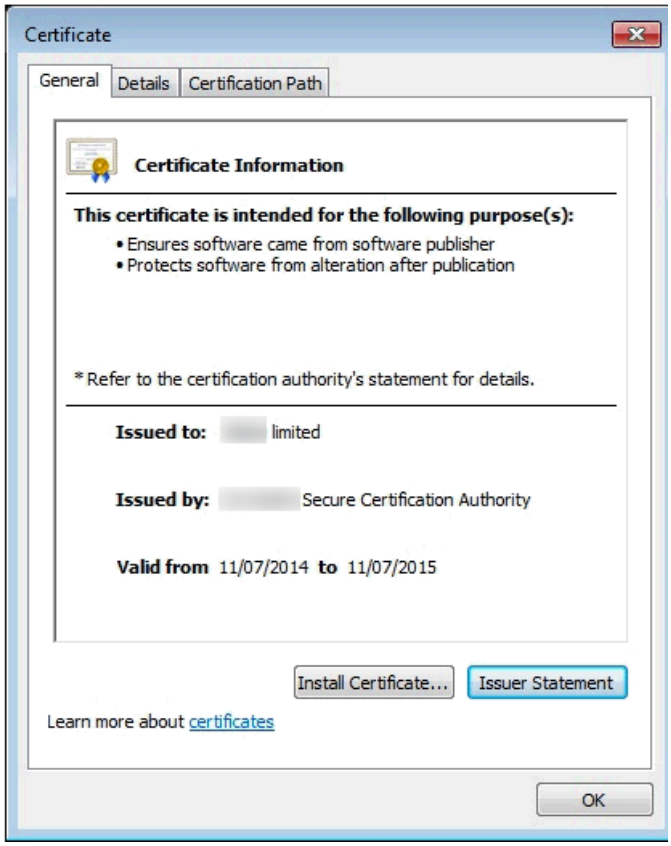
By stealing private keys of certificates using Trojan horses or by compromising the certificate key builder of software vendors, cybercriminals manage to get access to code signing certificates.

Suspicious certificates

When the researchers discovered that fraudsters used valid certificated, the first thing that came to their mind is that they somehow manage to acquire them directly from the certificate's issuer. What they did next is that they contacted the certificate owner, advised that it has been stolen and offered up to cybercriminals.

It is quite possible that cybercriminals would use certificates to register dummy corporations and then issue bank accounts, checks etc. It can be rather difficult to separate legitimate from dummy companies and this is due to the fact that cybercriminals take all the required steps for making it appear as authentic.





Recommendations

New measures of verification that will keep intruders away and not block code from legitimate vendors are needed.

Here's what you can do:

- Keep your operating system and the installed browsers fully updated.
- Do not add any new CAs to the root certificates zone (unless you are a security professional).
- Ban any files issued by unknown developers.
- Check the validity of the certificates and verify additional attributes like the certificate's hash sum.
- Keep a list of trusted certificates and update it regularly (a task for system administrators).
- Deploy endpoint security solutions

Written by: Ali Qamar, Founder/Chief Editor at SecurityGladiators.com

Author Bio:

Ali Qamar is an Internet security research enthusiast who enjoys "deep" research to dig out modern discoveries in the security industry. He is the founder and chief editor at Security Gladiators*, an ultimate source for cyber security. To be frank and honest, Ali started working online as a freelancer and still shares the knowledge for a living. He is passionate about sharing the knowledge with people, and always try to give only the best. Follow Ali on Twitter @AliQammar57*

Edited by Pierluigi Paganini

(Security Affairs – signing certificates , cybercrime)

Certificates as a service | code certificates | Cybercrime | Dark Web | malware | PKI | underground

Breaking News | Cyber Crime | Hacking | Malware

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Kemoge - Malicious Android Adware Infects Devices worldwide

NEXT ARTICLE
Who is behind the hack of Uber's driver database?

YOU MIGHT ALSO LIKE

Bad actors target entities worldwide via Cisco WebVPN

October 9, 2015 By Pierluigi Paganini

Who is behind the hack of Uber’s driver database?

October 9, 2015 By Pierluigi Paganini