W3 May | EN | Story of the week: Code Signing Certificate on the Darkweb

medium.com/s2wlab/w3-may-en-story-of-the-week-code-signing-certificate-on-the-darkweb-94c7ec437001

Hyunmin Suh May 18, 2021

Hyunmin Suh

May 17, 2021

·

8 min read

Trust but verify

Co-Author: Denise Dasom Kim, Jungyeon Lim, YH Jeong **| S2W LAB Talon**

Executive Summary

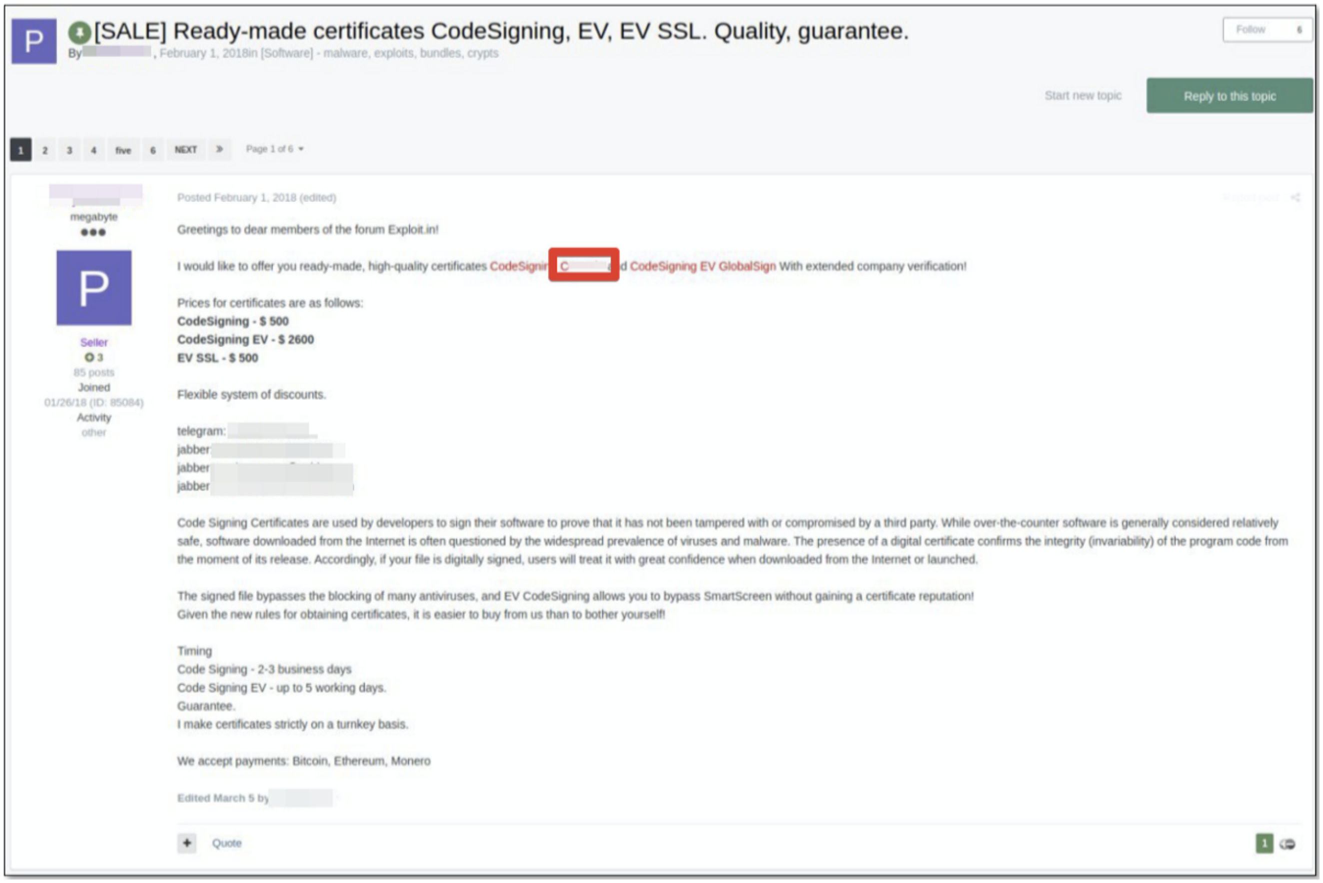
Code signing certificates have been used since Stuxnet incident (2011) as of today. Malware using code signing certificate is classified as highly reliable software and is less likely to be detected by Anti Virus (AV). It is known that attackers prefer code signed certificates as the most of current Internet and security systems are oriented toward trust and reputation dependent models.

Code signing certificates began to be sold on the dark web from around 2015 to 2016, and are mostly spotted on Russian speaking forums. Until recently, code signed certificates are being sold by various sellers on the forums and prices ranging from $400 to $3500 depending on the grade of the certificate.

It is important to consider the fact that this criminal ecosystem being active is that sellers have been constantly supplying certificates of legitimate companies, which can be seen that those of companies and developers' lack of security awareness and negligence of management provided the cause of hacking code signing certificates processing servers.

Most of the code signing certificate issues had already been a big issue in the past, so many people regard this issue as just an old case. However, attackers are still interested in code signing certificate servers and still being traded on the dark web or via hidden channels.

Code signing certificate sales posting in the dark web



[SALE] Ready-made certificates CodeSigning, EV, EV SSL. Quality, guarantee.

By[redacted], February 1, 2018in [Software] - malware, exploits, bundles, crypts

[redacted]
megabyte
Seller
3
85 posts
Joined
01/26/18 (ID: 85084)
Activity
other

Posted February 1, 2018 (edited)

Greetings to dear members of the forum Exploit.in!

I would like to offer you ready-made, high-quality certificates CodeSignin[redacted]d CodeSigning EV GlobalSign With extended company verification!

Prices for certificates are as follows:
CodeSigning - $ 500
CodeSigning EV - $ 2600
EV SSL - $ 500

Flexible system of discounts.

telegram: [redacted]
jabber [redacted]
jabber [redacted]
jabber [redacted]

Code Signing Certificates are used by developers to sign their software to prove that it has not been tampered with or compromised by a third party. While over-the-counter software is generally considered relatively safe, software downloaded from the Internet is often questioned by the widespread prevalence of viruses and malware. The presence of a digital certificate confirms the integrity (invariability) of the program code from the moment of its release. Accordingly, if your file is digitally signed, users will treat it with great confidence when downloaded from the Internet or launched.

The signed file bypasses the blocking of many antiviruses, and EV CodeSigning allows you to bypass SmartScreen without gaining a certificate reputation!
Given the new rules for obtaining certificates, it is easier to buy from us than to bother yourself!

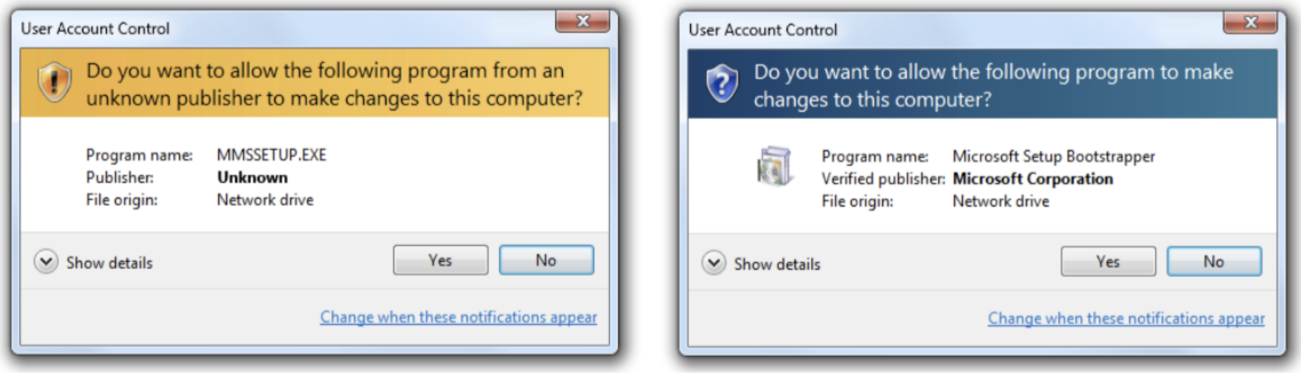
Timing
Code Signing - 2-3 business days
Code Signing EV - up to 5 working days.
Guarantee.
I make certificates strictly on a turnkey basis.

We accept payments: Bitcoin, Ethereum, Monero

Edited March 5 by [redacted]

According to the seller, it can issue a certificate of global brand C that issues SSL certificates. And the price ranges from $500 to $2600.

If you develop a software without code signing, the biggest difference is in the User Account Control (UAC) part when executing the software.



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: MMSSETUP.EXE
Publisher: **Unknown**
File origin: Network drive

User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Microsoft Setup Bootstrapper
Verified publisher: **Microsoft Corporation**
File origin: Network drive

Not Code Signed **Code Signed**

Image from SSL2BUY ()

CodeSigning vs SSL Certificate

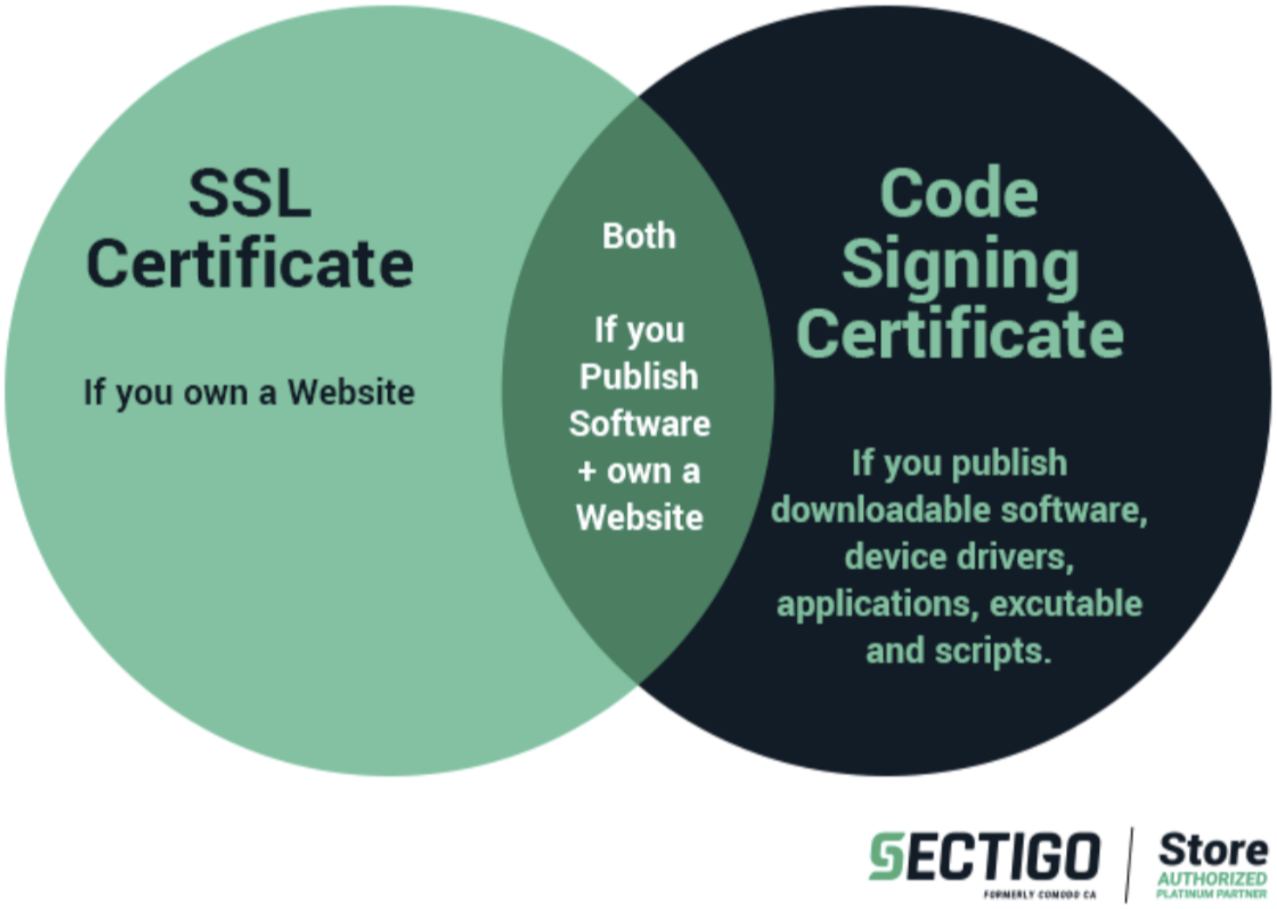

SSL Certificate
If you own a Website
Both
If you Publish Software + own a Website
Code Signing Certificate
If you publish downloadable software, device drivers, applications, excutable and scripts.
SECTIGO
FORMERLY COMODO CA
Store
AUTHORIZED
PLATINUM PARTNER

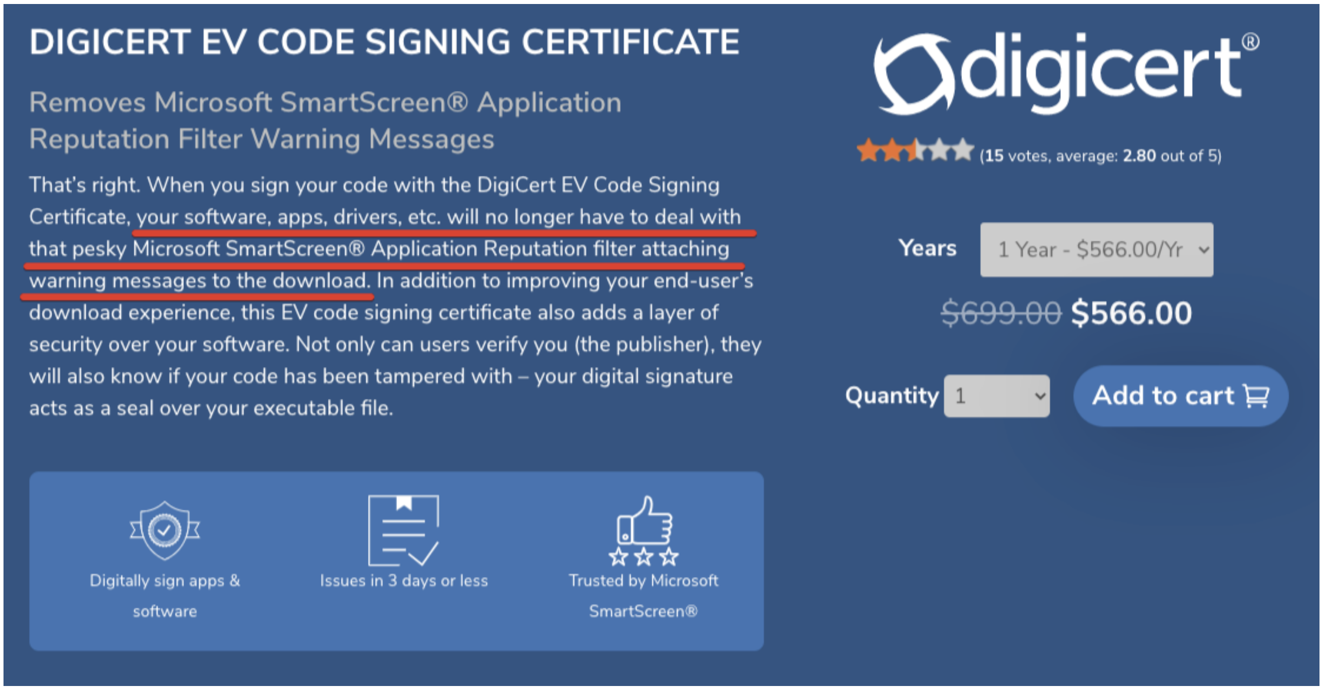
Image from SECTIGO store ()

As can be seen from above diagram, the main difference between SSL certificate and code signing certificate is whether you own a website or you publish downloadable software, applications, etc.

If so, let’s have a look how the EV is different in the code signature.

Code Signing vs Code Signing EV

The code signing EV mentioned by seller means Extended Validation (EV) code signing certificates, which differs from the general code signing certificate in that the private key is stored in a separate hardware token in the case of EV. The most noticeable difference when running the software is that the Windows Smart Screen Filter warning does not appear when using EV code signing certificates.



DIGICERT EV CODE SIGNING CERTIFICATE

Removes Microsoft SmartScreen® Application Reputation Filter Warning Messages

That's right. When you sign your code with the DigiCert EV Code Signing Certificate, your software, apps, drivers, etc. will no longer have to deal with that pesky Microsoft SmartScreen® Application Reputation filter attaching warning messages to the download. In addition to improving your end-user's download experience, this EV code signing certificate also adds a layer of security over your software. Not only can users verify you (the publisher), they will also know if your code has been tampered with – your digital signature acts as a seal over your executable file.

(15 votes, average: 2.80 out of 5)

Years: 1 Year - $566.00/Yr

~~$699.00~~ $566.00

Quantity: 1

digicert®
Add to cart
Digitally sign apps & software
Issues in 3 days or less
Trusted by Microsoft SmartScreen®

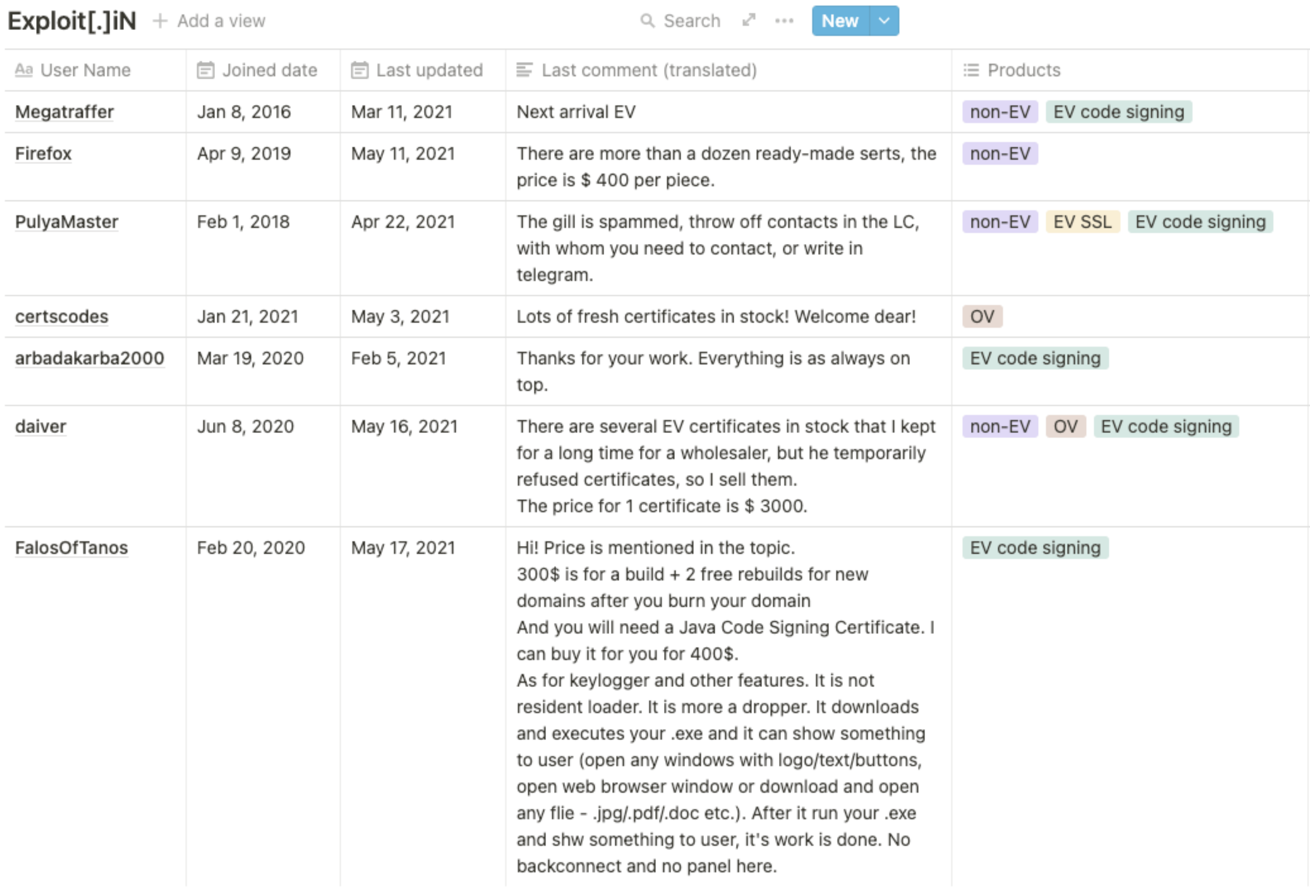
Image from Code Signing Store ()

Because of this, many cybercriminals use code signed certificate to increase the success rate of attacks when creating malwares.

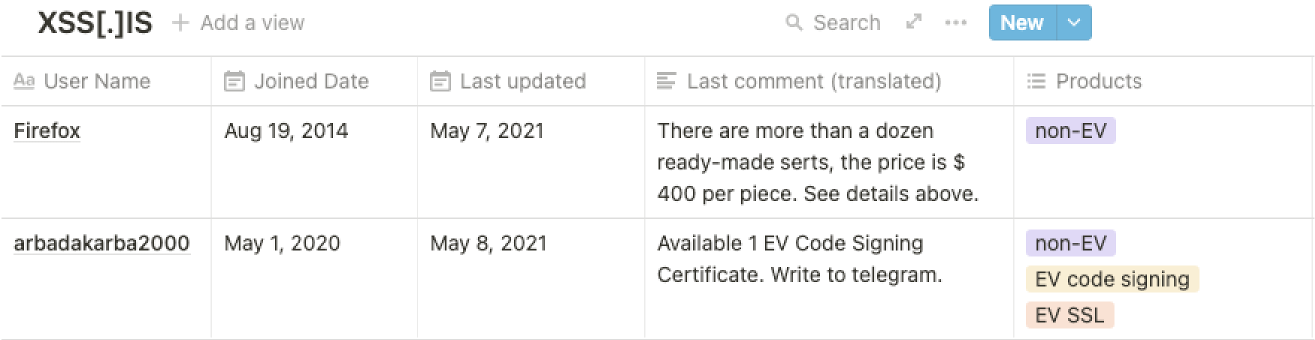
However, the certificate cannot be issued by anyone, it is required to submit documents such as business registration certificate, tax payment certificate, and etc. to authorities and go through examination process. Therefore, attackers directly steal the code sign certificate by compromising legitimate company's certification server, or purchase it from the dark web sellers.

Then, let's take a look at how many sellers are still active on the dark web forums.

Code Signing Certificate Sellers on the dark web



User Name	Joined date	Last updated	Last comment (translated)	Products
Megatraffer	Jan 8, 2016	Mar 11, 2021	Next arrival EV	non-EV EV code signing
Firefox	Apr 9, 2019	May 11, 2021	There are more than a dozen ready-made serts, the price is $ 400 per piece.	non-EV
PulyaMaster	Feb 1, 2018	Apr 22, 2021	The gill is spammed, throw off contacts in the LC, with whom you need to contact, or write in telegram.	non-EV EV SSL EV code signing
certscodes	Jan 21, 2021	May 3, 2021	Lots of fresh certificates in stock! Welcome dear!	OV
arbadakarba2000	Mar 19, 2020	Feb 5, 2021	Thanks for your work. Everything is as always on top.	EV code signing
daiver	Jun 8, 2020	May 16, 2021	There are several EV certificates in stock that I kept for a long time for a wholesaler, but he temporarily refused certificates, so I sell them. The price for 1 certificate is $ 3000.	non-EV OV EV code signing
FalosOfTanos	Feb 20, 2020	May 17, 2021	Hi! Price is mentioned in the topic. 300$ is for a build + 2 free rebuilds for new domains after you burn your domain And you will need a Java Code Signing Certificate. I can buy it for you for 400$. As for keylogger and other features. It is not resident loader. It is more a dropper. It downloads and executes your .exe and it can show something to user (open any windows with logo/text/buttons, open web browser window or download and open any flie - .jpg/.pdf/.doc etc.). After it run your .exe and shw something to user, it's work is done. No backconnect and no panel here.	EV code signing

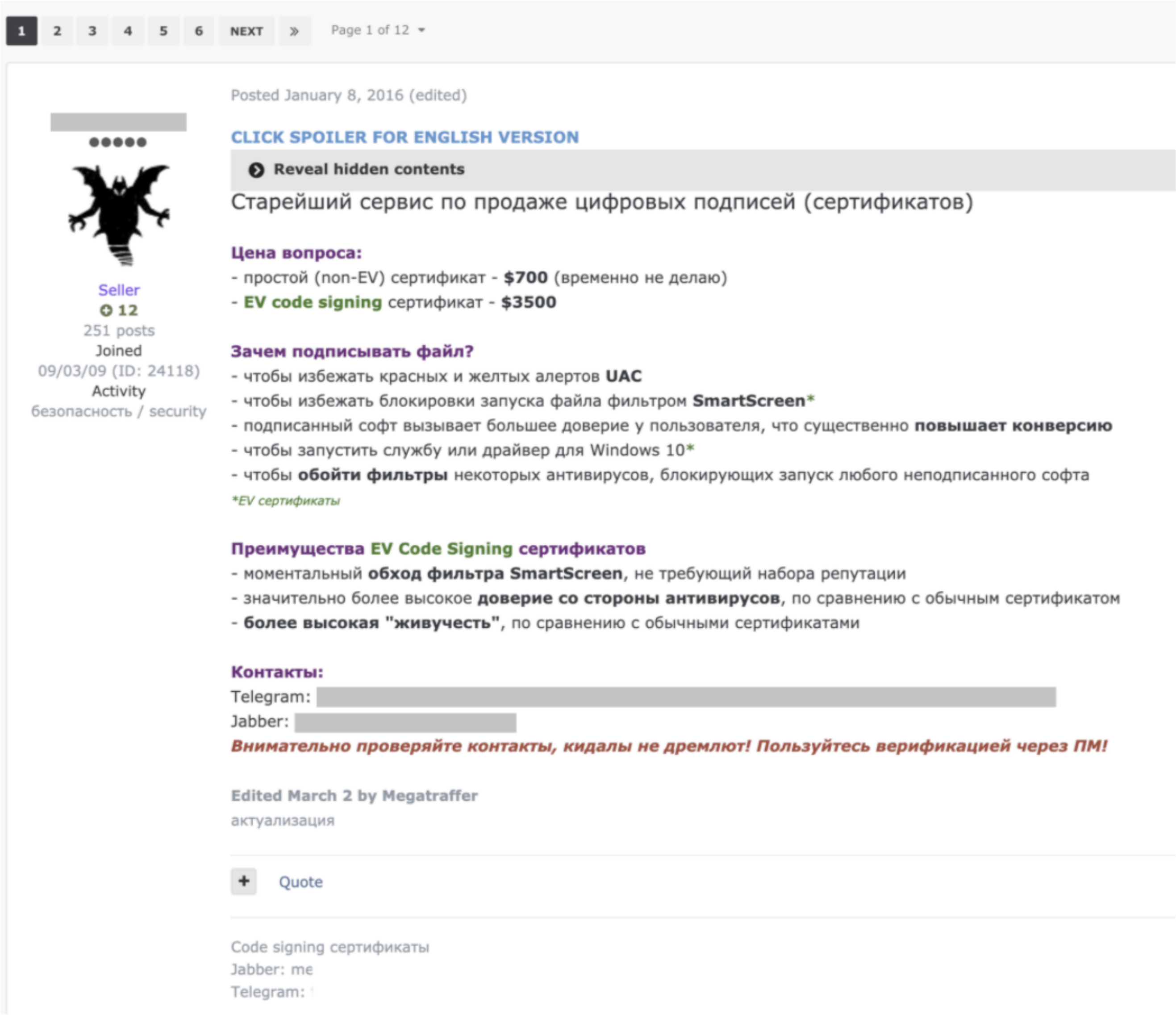


User Name	Joined Date	Last updated	Last comment (translated)	Products
Firefox	Aug 19, 2014	May 7, 2021	There are more than a dozen ready-made serts, the price is $ 400 per piece. See details above.	non-EV
arbadakarba2000	May 1, 2020	May 8, 2021	Available 1 EV Code Signing Certificate. Write to telegram.	non-EV EV code signing EV SSL

As can be seen from the table, users have been active from at least 2 months to 7 years. In this regard, code signing certificates can be seen as quite a popular product on the dark web.

Seller’s Posts in Exploit[.]iN Forum

> ### Megatraffer



[redacted]

●●●●●

Seller
⊕ 12
251 posts
Joined
09/03/09 (ID: 24118)
Activity
безопасность / security

Posted January 8, 2016 (edited)

CLICK SPOILER FOR ENGLISH VERSION

Старейший сервис по продаже цифровых подписей (сертификатов)

Цена вопроса:
- простой (non-EV) сертификат - **$700** (временно не делаю)
- **EV code signing** сертификат - **$3500**

Зачем подписывать файл?
- чтобы избежать красных и желтых алертов **UAC**
- чтобы избежать блокировки запуска файла фильтром **SmartScreen***
- подписанный софт вызывает большее доверие у пользователя, что существенно **повышает конверсию**
- чтобы запустить службу или драйвер для Windows 10*
- чтобы **обойти фильтры** некоторых антивирусов, блокирующих запуск любого неподписанного софта

**EV сертификаты*

Преимущества EV Code Signing сертификатов
- моментальный **обход фильтра SmartScreen**, не требующий набора репутации
- значительно более высокое **доверие со стороны антивирусов**, по сравнению с обычным сертификатом
- **более высокая "живучесть"**, по сравнению с обычными сертификатами

Контакты:
Telegram: [redacted]
Jabber: [redacted]
Внимательно проверяйте контакты, кидалы не дремлют! Пользуйтесь верификацией через ПМ!

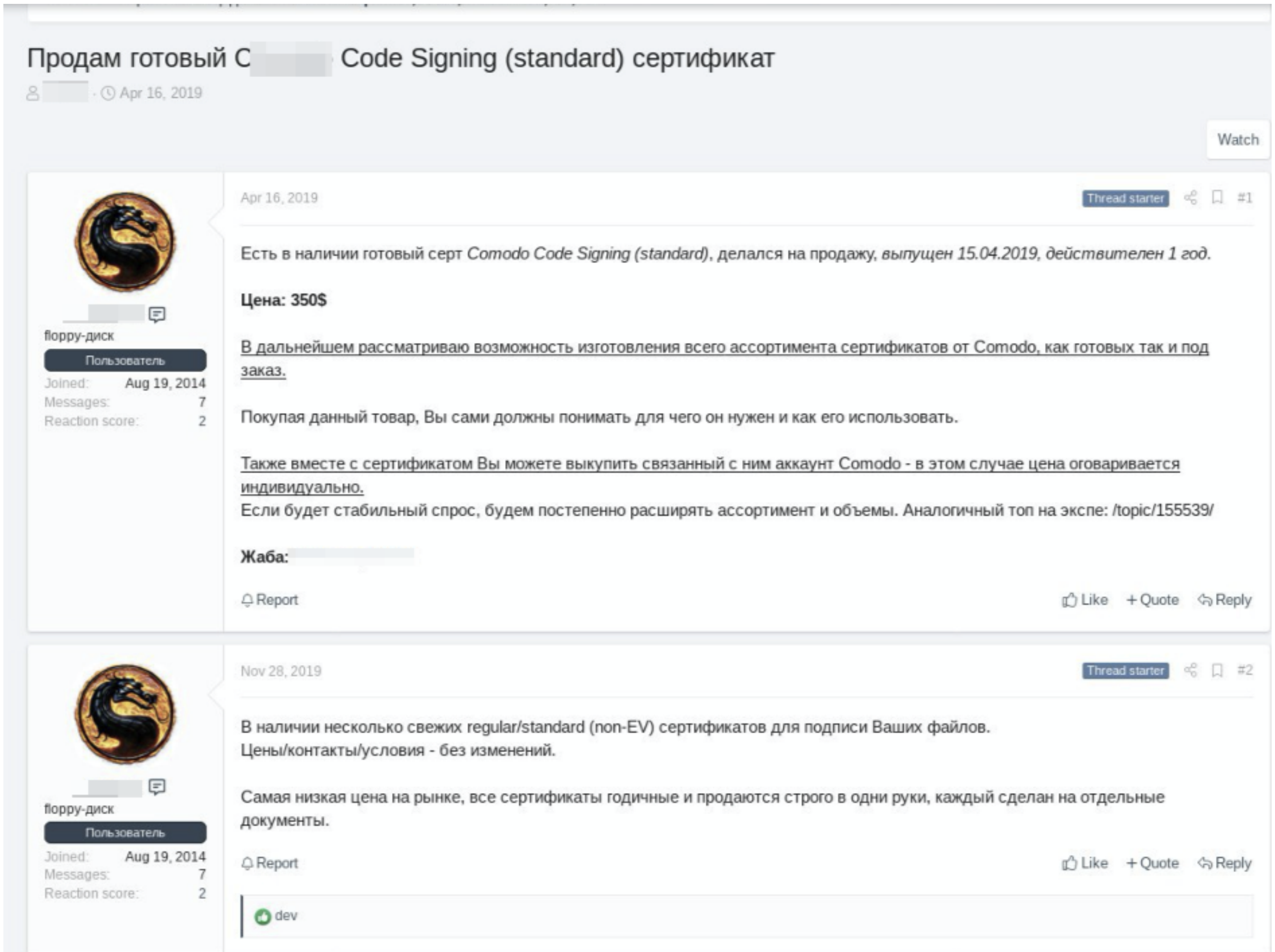
Edited March 2 by Megatraffer
актуализация

Code signing сертификаты
Jabber: me
Telegram:

Digital certificates for sale, from the oldest and most trusted service!🎖We offer:- regular (non-EV) code signing certificates- EV code signing certificatesPrice- non-EV certificate - $700- EV code signing certificate - $3500All certificates:- valid for 1 year, can also make them for 2 yearsWhy signing files?- to avoid red/yellow UAC warnings- to avoid SmartScreen alerts- signed software is much more trusted by users- some antiviruses block ALL unsigned software from being executedBenefits of EV Code Signing certificates- removes SmartScreen blue windows immediately- maximum level of trust by AVs- EV certificate is a 'must have' if you want to sign drivers for Windows 10Contact:***sanitized by s2wlabDouble-check contact details before sending money! Beware of scammers!

Seller’s Posts in XSS[.]IS Forum

> ### Firefox



Продам готовый С[redacted] Code Signing (standard) сертификат

[redacted] · Apr 16, 2019

Watch

[redacted]
floppy-диск
Пользователь
Joined: Aug 19, 2014
Messages: 7
Reaction score: 2

Apr 16, 2019 Thread starter #1

Есть в наличии готовый серт *Comodo Code Signing (standard)*, делался на продажу, *выпущен 15.04.2019, действителен 1 год.*

Цена: 350$

В дальнейшем рассматриваю возможность изготовления всего ассортимента сертификатов от Comodo, как готовых так и под заказ.

Покупая данный товар, Вы сами должны понимать для чего он нужен и как его использовать.

Также вместе с сертификатом Вы можете выкупить связанный с ним аккаунт Comodo - в этом случае цена оговаривается индивидуально.
Если будет стабильный спрос, будем постепенно расширять ассортимент и объемы. Аналогичный топ на экспе: /topic/155539/

Жаба: [redacted]

Report · Like · + Quote · Reply

[redacted]
floppy-диск
Пользователь
Joined: Aug 19, 2014
Messages: 7
Reaction score: 2

Nov 28, 2019 Thread starter #2

В наличии несколько свежих regular/standard (non-EV) сертификатов для подписи Ваших файлов.
Цены/контакты/условия - без изменений.

Самая низкая цена на рынке, все сертификаты годичные и продаются строго в одни руки, каждый сделан на отдельные документы.

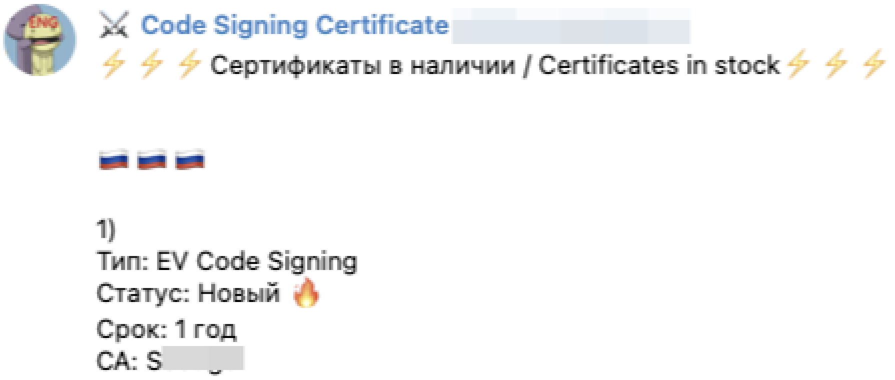
Report · Like · + Quote · Reply

dev

There is a ready-made C**** Code Signing certificate (standard), made for sale, released on 04/15/2019, valid for 1 year.Price: 350 $In the future, I am considering the possibility of manufacturing the entire range of certificates from C***, both ready-made and to order.When buying this product, you yourself must understand what it is for and how to use it.Also, along with the certificate, you can redeem the C**** account associated with it - in this case, the price is negotiated individually.If there is a stable demand, we will gradually expand the range and volumes. A similar top on the ex: / topic / 155539 /***sanitized by s2wlab

Seller’s Posts in Telegram

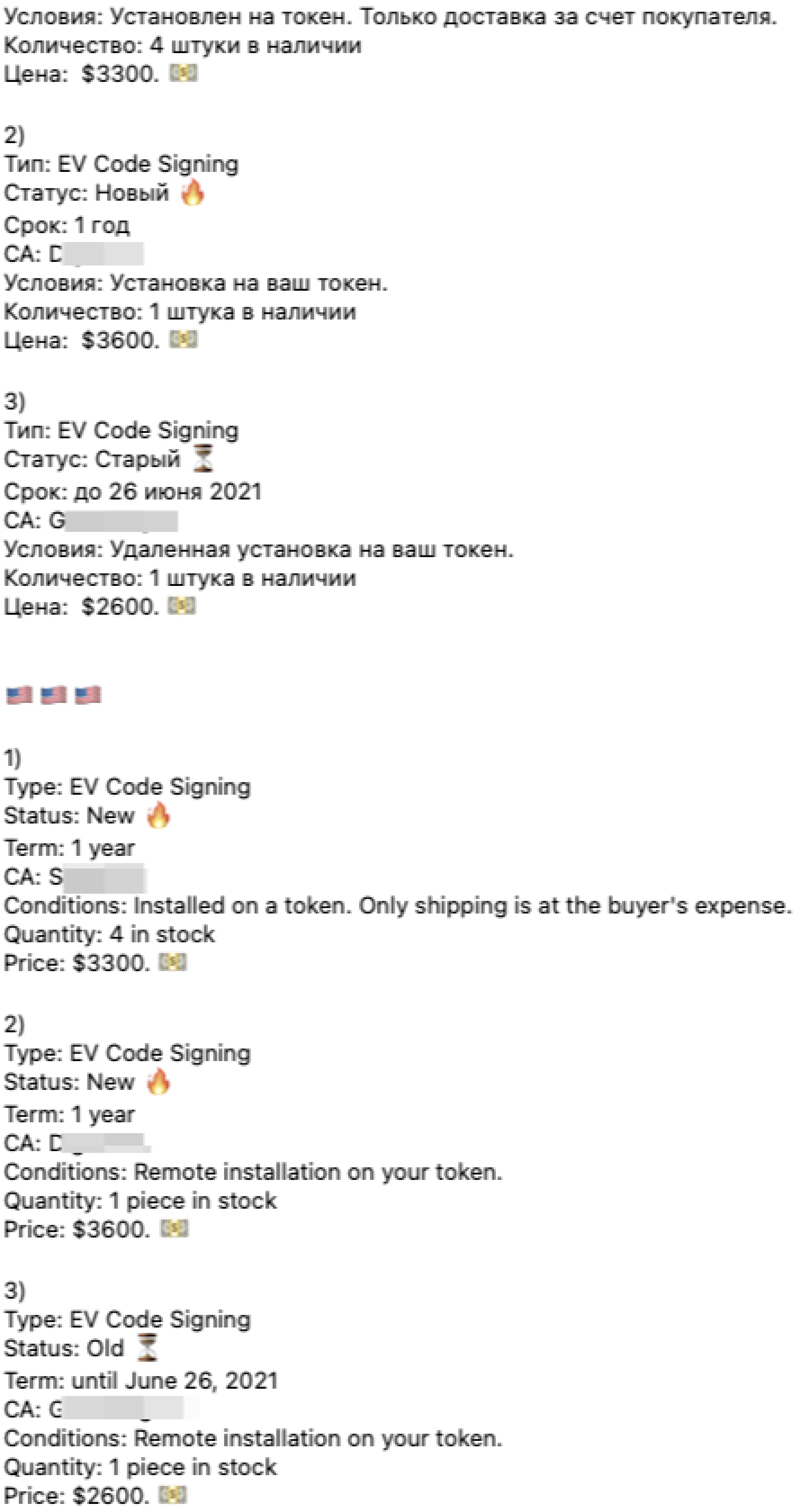
> SamCodeSign



⚔️ Code Signing Certificate [redacted]
⚡⚡⚡ Сертификаты в наличии / Certificates in stock ⚡⚡⚡

🇷🇺🇷🇺🇷🇺

1)
Тип: EV Code Signing
Статус: Новый 🔥
Срок: 1 год
CA: S[redacted]



Условия: Установлен на токен. Только доставка за счет покупателя.
Количество: 4 штуки в наличии
Цена: $3300. 💵

2)
Тип: EV Code Signing
Статус: Новый 🔥
Срок: 1 год
CA: D[redacted]
Условия: Установка на ваш токен.
Количество: 1 штука в наличии
Цена: $3600. 💵

3)
Тип: EV Code Signing
Статус: Старый ⏳
Срок: до 26 июня 2021
CA: G[redacted]
Условия: Удаленная установка на ваш токен.
Количество: 1 штука в наличии
Цена: $2600. 💵

🇺🇸 🇺🇸 🇺🇸

1)
Type: EV Code Signing
Status: New 🔥
Term: 1 year
CA: S[redacted]
Conditions: Installed on a token. Only shipping is at the buyer's expense.
Quantity: 4 in stock
Price: $3300. 💵

2)
Type: EV Code Signing
Status: New 🔥
Term: 1 year
CA: D[redacted]
Conditions: Remote installation on your token.
Quantity: 1 piece in stock
Price: $3600. 💵

3)
Type: EV Code Signing
Status: Old ⏳
Term: until June 26, 2021
CA: G[redacted]
Conditions: Remote installation on your token.
Quantity: 1 piece in stock
Price: $2600. 💵

```
⚡⚡⚡Сертификаты в наличии / Certificates in stock⚡⚡⚡

    🇺🇸🇺🇸🇺🇸1)Type: EV Code SigningStatus: New 🔥Term: 1 yearCA: S***Conditions:
Installed on a token. Only shipping is at the buyer's expense.Quantity: 4 in
stockPrice: $3300. 💵2)Type: EV Code SigningStatus: New 🔥Term: 1 yearCA:
D***Conditions: Remote installation on your token.Quantity: 1 piece in stockPrice:
$3600. 💵3)Type: EV Code SigningStatus: Old ⏳Term: until June 26, 2021CA:
G***Conditions: Remote installation on your token.Quantity: 1 piece in stockPrice:
$2600. 💵
```

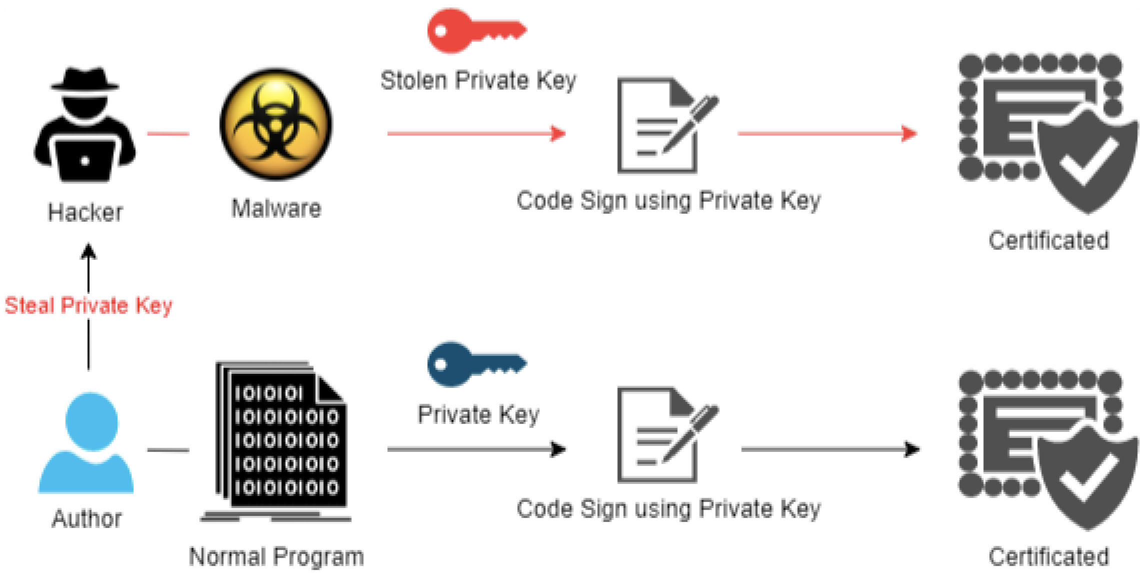
Conclusion

Malware signed with stolen certificates have been found constantly. As mentioned earlier, the reason why the criminal ecosystem is still active today is that there is an abundance of supply chains in which hackers constantly bringing legitimate companies' certificates.

It is difficult for general companies to cope with malicious code signed with legitimate companies certificates. Therefore, the most fundamental solution is to raise the security awareness of companies and developers for the code signing certificate server and manage them in cautious manner.

References to past cases related to code signing certificates

Case 1 : Private-Key Stolen

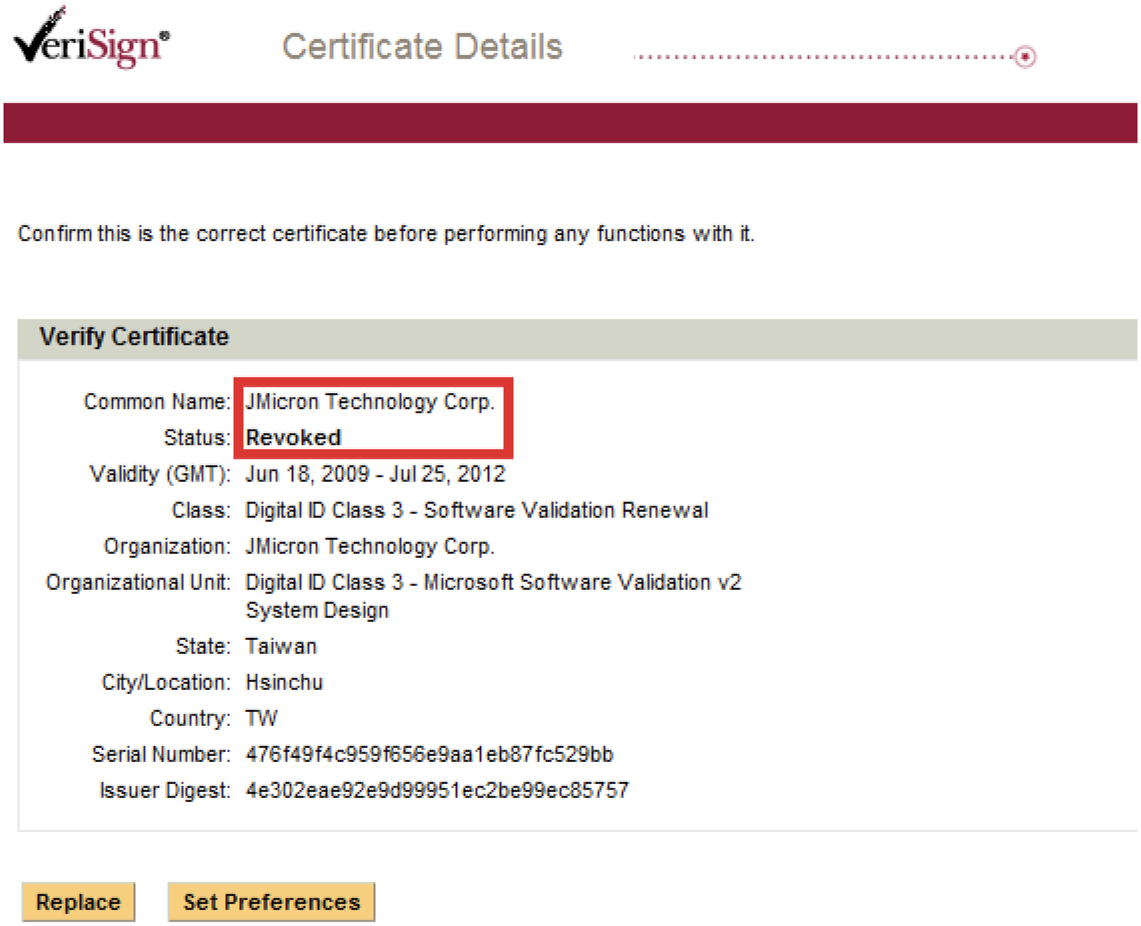


Stealing the private-key of a normal software developer, signing the malicious code they developed, and disguised as a legitimate program

Case 1–1. Stuxnet malware incident related

- Date of incident: January 2011
- Malware used: Trojan — Zeus

- Incidents explained: Use of stolen digital signatures by Realtek Semiconductor Corp. based in Taiwan



Confirm this is the correct certificate before performing any functions with it.

Verify Certificate

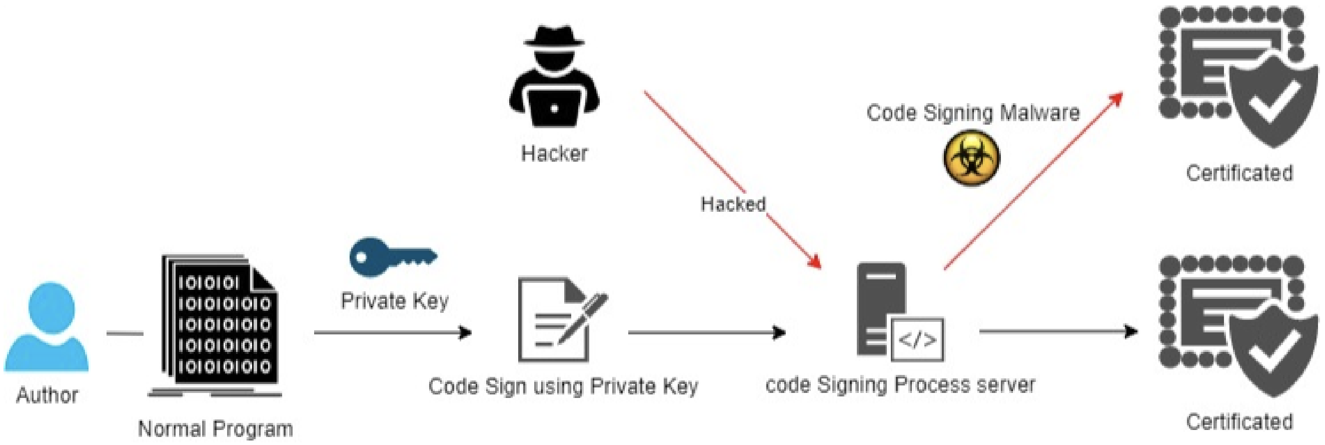
Common Name:	JMicron Technology Corp.
Status:	Revoked
Validity (GMT):	Jun 18, 2009 - Jul 25, 2012
Class:	Digital ID Class 3 - Software Validation Renewal
Organization:	JMicron Technology Corp.
Organizational Unit:	Digital ID Class 3 - Microsoft Software Validation v2 System Design
State:	Taiwan
City/Location:	Hsinchu
Country:	TW
Serial Number:	476f49f4c959f656e9aa1eb87fc529bb
Issuer Digest:	4e302eae92e9d99951ec2be99ec85757

Digital signature that was stolen at the time of incident (see the reference 13)
According to Kaspersky, JMicron and Realtek announced the possibility of infection with Zeus, a Trojan that steals digital signatures. They also provided that digital signatures stolen could not only be used by attackers on the stuxnet driver, but could also be sold on the black market.

Case 1–2. Sony Pictures hacking incident related

- Date of incident: November 2014
- Malware used: Destover Malware
- Incidents explained: Destover Malware signed by stolen sony certificate, and hijacked pfx file

Case 2 : Compromised Code Signing Process Server



Signing malicious codes of hackers by compromising the server that performs code signing process.

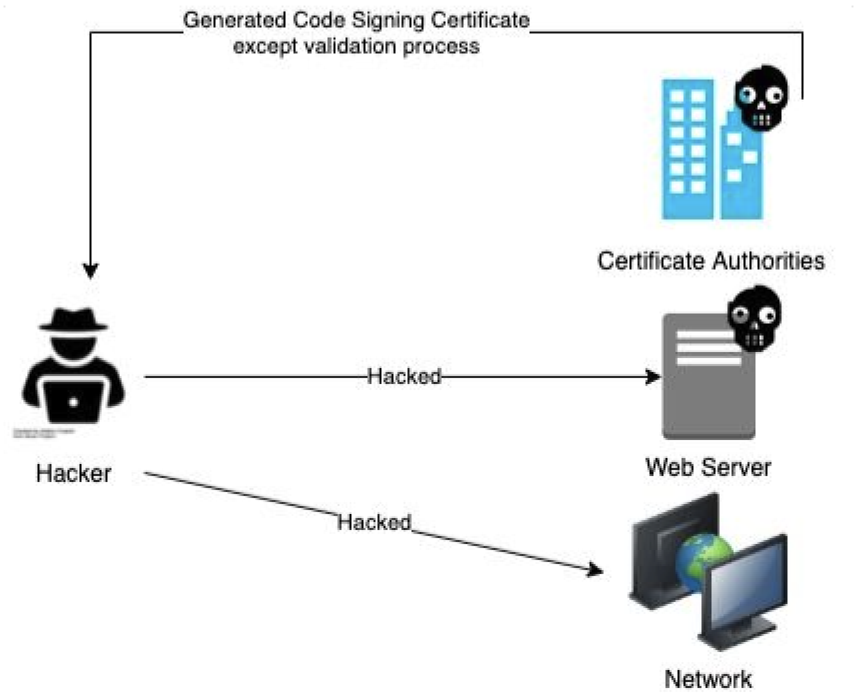
Case 2–1. Adobe hacking incident

- Date of incident: September 2012
- Malware used: pwdump7 v 7.1, myGeeksmail.dll
- Incidents explained: Attackers penetrated the network and reached a build server on which they requested a signature for two malicious utilities.

Case 2–2. Bit9 system hacking incident related

- Date of incident: February 2013
- Malware used: Trojan, Backdoor.Hikit
- Incidents explained:- Web Server hacked by SQL injection, and installed Backdoor.Hikit- Accessed to virtual machine that processes digital signature- 32 malicious file's been tampered

Case 3 : Direct Attack on Certificate Authority



Compromising the Certificate Authority (CA) that issues code signing certificate and manipulating them to issue code signing certificates for attacker

Case 3–1. Comodo Certificate Authority (CA) breached case

- Date of incident: March 2011
- Malware used:
- Incidents explained:- Create a new ID after hijacking a user account registered with RA in South Africa (), issuing 9 fake certificates- ComodoHacker gets a full access to the RA network then reverse engineered the DLL (TrustDll.dll) handling certification request- ComodoHacker post : - The username and password are hard-coded in the DLL file, allowing hackers to connect directly to the API used to sign certificates- Created its own CSR (Certificate Signing Request), then signed with the API already have an access to, and issued 9 fraudulent certificates for the CAs mentioned above

Case 3–2. DigiNotar Certificate Authority (CA) breached case

- Date of incident: August 2011
- Vulnerability used: Web server vulnerability
- Incidents explained:- Google's chrome team discovered that DigiNotar-issued certificate doesn't match 's internal list of certificates- Web server hacked → Office-Net hacked → Secure-Net hacked including CA server → Activated Remote Desktop protocol and connected
- More than 531 fraudulent certifications has been issued.
- DigiNotar — Bankrupted due to its hacking incident
- Attacker's note :

Reference

1. Issued for Abuse: Measuring the Underground Trade in Code Signing Certificates ()
2. The Use of Counterfeit Code Signing Certificates Is on the Rise ()
3. Understanding Code Signing Abuse in Malware Campaigns ()
4. The Real Story of Stuxnet ()
5. Case study of Stuxnet ()
6. 악성코드를 유포시키기 위한 코드서명 해킹 3가지 유형 ()
7. SONY PICTURES ENTERTAINMENT — EU Cyber Direct ()
8. Adobe Says Its Code Signing Infrastructure Has Been Hacked (?)
9. The Scary and Terrible Code Signing Problem You Don’t Know You Have ()
10. Microsoft, FireEye confirm SolarWinds supply chain attack ()
11. Hackers are selling legitimate code-signing certificates to evade malware detection ()
12. Stuxnet: Zero victims ()
13. Stuxnet signed certificates frequently asked questions ()
14. Stuxnet and stolen certificates ()
15. VB2018 paper: Since the hacking of Sony Pictures ()
16. Stolen Sony certificates used to digitally sign Destover Malware ()
17. ‘Destover’ malware now digitally signed by Sony certificates (updated) ()
18. Comodo-Fraud-Incident-2011–03–23 ()
19. SECURITY BREACH IN CA NETWORKS -COMODO, DIGINOTAR, GLOBALSIGN ()
20. All You Need to Know About the SolarWinds Attack ()
21. EP 3: DIGINOTAR, YOU ARE THE WEAKEST LINK, GOOD BYE! ()

CYBER THREAT INTELLIGENCE DIVISION
TALON