INTRINSEC
Innovative by design

Cyber Threat Intelligence

The EV Code Signature Market for eCrime

@Intrinsec @Intrinsec Blog Website

Table of contents

Key findings

- Code Signing Technology allows developers to digitally sign their programs, ensuring authenticity and integrity.
- This can be exploited by malicious actors to bypass security measures, gain privileges, and deceive users with seemingly legitimate certificates.
- The cybercrime market for EV certificates offers a wide range of services, including various certificate authorities and delivery methods.
- To obtain code signing certificates, resellers can register new companies, impersonate existing ones, or acquire then through theft.

Introduction

Code signing is a technology that allows software developers to attach a digital signature to their programs, proving that the code is authentic and has not been tampered with. Malicious actors exploit code signing to bypass security measures, gain administrative privileges, and enhance user trust by using legitimate-seeming certificates.

The cybercrime market for code signing certificates mainly focuses on EV certificates, with prices ranging from $2000 to $6000. The resellers can either register a new company or impersonate an existing company to get a valid certificate from a certificate authority.

Malware campaigns, such as QakBot and Grandoreiro, have used valid EV code signing certificates obtained through company impersonation or exploiting closed companies. Code signing certificates can also be obtained through theft, as seen in incidents like the theft of NVIDIA's code signing certificates by the Lapsus$ extortion group in early 2022.

1 Asymmetric Cryptography and Code Signing

1.1 Public Key Cryptography

Asymmetric cryptography relies on **key pairs**. Each key pair contains a public key and a private key. As the name suggests, the **private key is supposed to be kept private** and **the public key is supposed to be shared**.

In the **encryption** process, the public key is used by the sender to encrypt the message, and the private key is used by the receiver to decrypt the message. The only person that can read the message is the owner of the private key, thus usually the person that generated the key pair. This process ensures **confidentiality** of the communication.

In the **signature** process, the text to be signed is first hashed then the hash is signed using the private key. To check the signature's validity, one must compute the hash of the text and compare it to the "public key decrypted" signature. If the signature is valid, this process ensures:

- Data **integrity** (the message has not been modified)
- **Authenticity** (the message comes from the owner of the private key)
- **Non-repudiation** (the sender cannot deny that he sent the message)

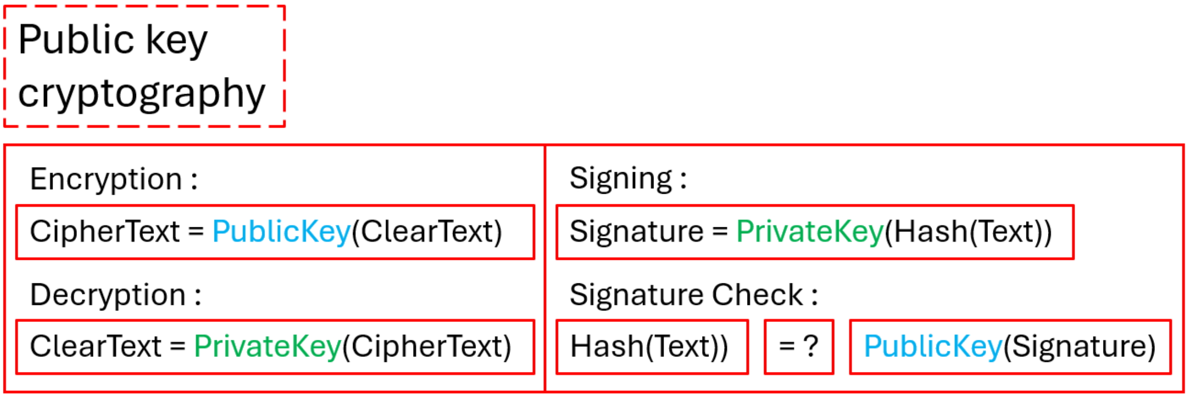


Figure 1: Encryption and signature in public key cryptography.

1.2 Certificates

Certificates are essential for securely **sharing public keys** and associating them with specific **identities**. They rely on **Certificate Authorities (CAs)**, trusted entities responsible for verifying the authenticity of certificate holders' identities and digitally signing certificates to validate them.

These CAs verify the subject's information and ensure the subject's possession of the private key by issuing a challenge. Once verified, the CA provides a certificate containing **the subject's information and their public key**. The CA then **signs** this data, and the signature is appended to the certificate, **certifying the authenticity** of all information within it.

Web browsers and operating systems maintain databases containing the root certificates of trusted Certificate Authorities. This allows them (web browsers and operating systems) to verify the validity of the CA's signatures, establishing trust in the certificates issued by those authorities.

This process involving the issuance, validation, and management of digital certificates by trusted Certificate Authorities, is a fundamental component of **Public Key Infrastructure** (PKI). The Public Key Infrastructure facilitates the transitivity of trust, meaning that trust in a root Certificate Authority (CA) extends to all certificates issued by that CA.

Non-repudiation remains true due to the presence of **revocation** mechanisms. Revocation enables the invalidation of compromised certificates and enhances the credibility of digital signatures.

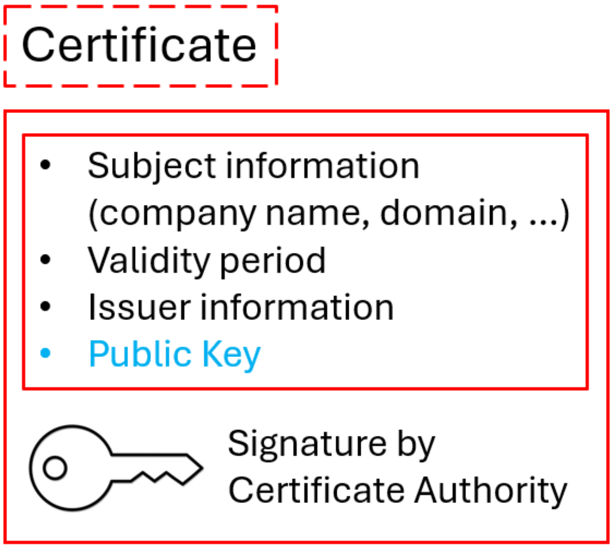

Certificate
Subject information (company name, domain, ...)
Validity period
Issuer information
Public Key
Signature by Certificate Authority

Figure 2: Contents of a certificate.

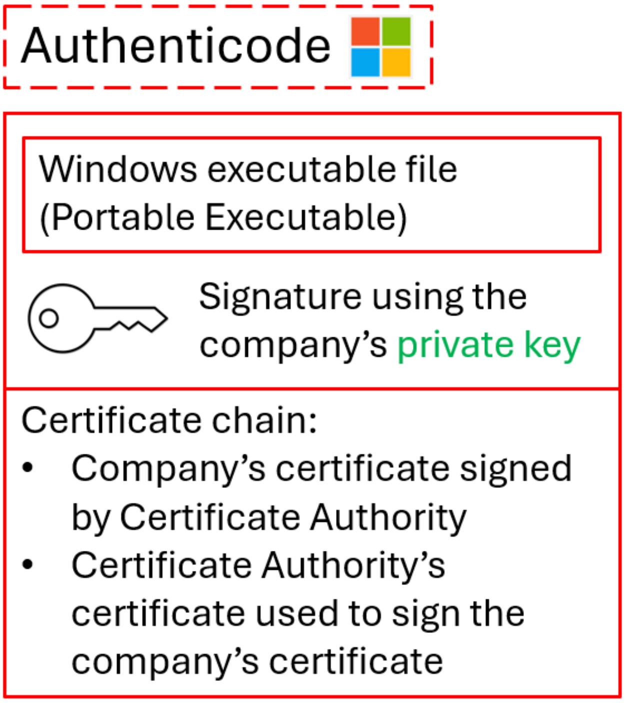
1.3 Code Signing and Authenticode

Authenticode is a code signing standard developed by Microsoft for signing Windows executable files, **Portable Executable** (PE). The PE format contains a structure called Attribute Certificate Table which is used to store certificates and signature-related data. This allows software vendors to securely verify the authenticity and integrity of their executable files, thereby establishing trust with end-users and safeguarding against tampering or malicious alterations.

Most of the content of the PE file is hashed then signed using the vendor's key pair. The certificate of the vendor is included in the PE file as well as the certificate of the CA that signed the vendor's certificate, allowing the end user to verify the full **certificate chain**.

The certificate must be valid for **code signing** purposes (delivered by the CA as such), and there exists two types of code signing certificates:

- **Organisation Validated** (OV) certificates. The CA verifies the identity of the organisation applying for the certificate
- **Extended Validation** (EV) certificates. The CA performs additional checks on the organisation's legal identity, physical existence and operational status through government records



Authenticode

Windows executable file (Portable Executable)

Signature using the company's private key

Certificate chain:

- Company's certificate signed by Certificate Authority
- Certificate Authority's certificate used to sign the company's certificate

Figure 3: Authenticode: Windows' code signing mechanism.

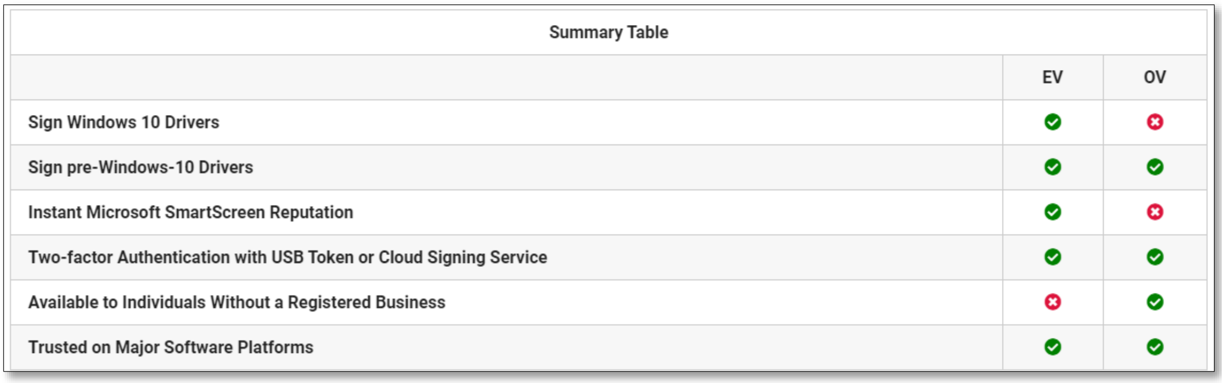
2 The Market

2.1 Benefits of Code Signing for Cybercrime

Code signing can be exploited for malicious purposes. Given the level of validation (OV or EV), signing the code can provide several benefits:

- Bypassing Microsoft **SmartScreen**
- Accessing **administrative** privileges
- Lower the **antivirus risk score**
- Improving the browser **Safe Browsing** score
- Enhancing **user trust**
- Signing **drivers**

Down below is an example from **SSL.com** showing the advertised benefits of code signing. The prices range from about **$100 to $500 per year**, depending on the number of files signed and the signing process used (Cloud/YubiKey).



Summary Table

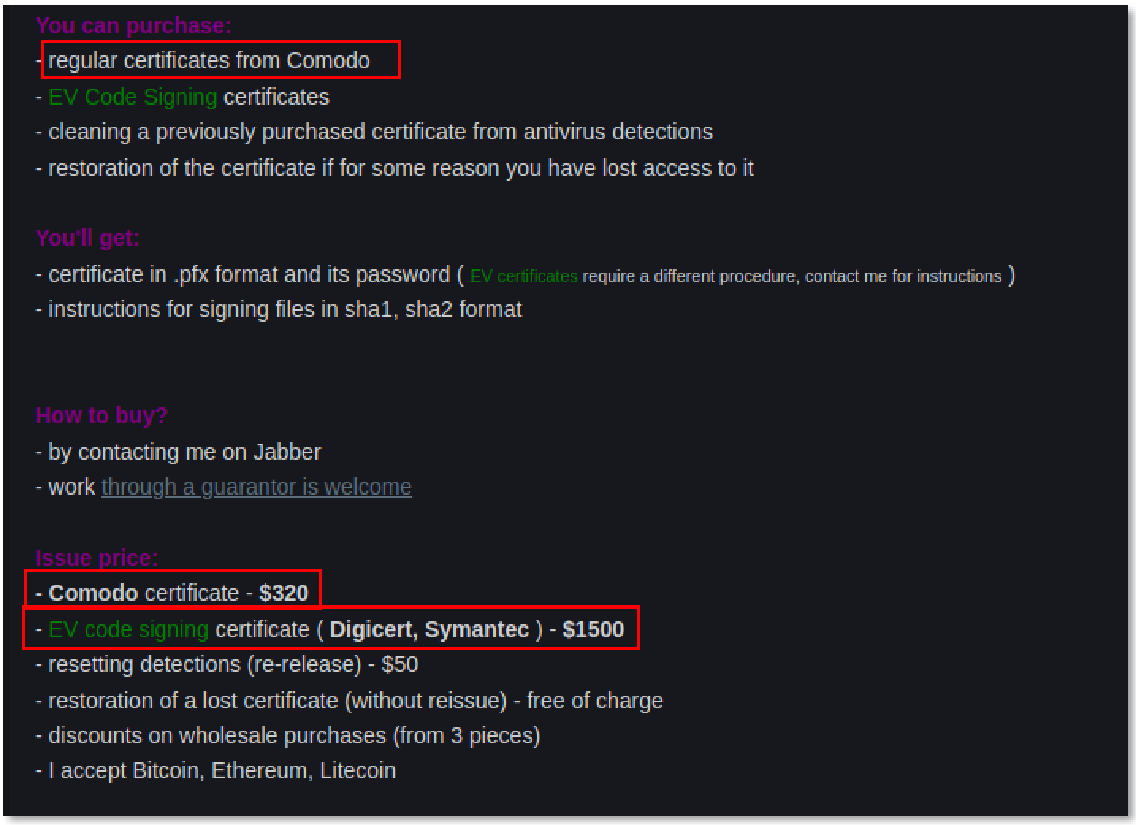
	EV	OV
Sign Windows 10 Drivers	✓	✗
Sign pre-Windows-10 Drivers	✓	✓
Instant Microsoft SmartScreen Reputation	✓	✗
Two-factor Authentication with USB Token or Cloud Signing Service	✓	✓
Available to Individuals Without a Registered Business	✗	✓
Trusted on Major Software Platforms	✓	✓

Figure 4: Benefits of code signing from SSL.com.

To take advantage of those benefits, malicious operators can try and sign their code using seemingly legitimate certificates delivered from CA. As our team monitors the underground cybercrime forums and marketplaces, we came upon multiple posts advertising code signing certificates sales. Here is an overview of the **code signing certificate market** on cybercrime forum **Exploit**.

2.2 Cybercrime Code Signing Market

Most of the advertising seen on the forum concerns EV certificates. The sellers probably assume that registering for an OV certificate is easy enough so that one does not need to pay a dedicated service to access it. We did, however, see a couple of offers regarding **OV certificates**, their prices were about **$300**.



You can purchase:
- regular certificates from Comodo
- EV Code Signing certificates
- cleaning a previously purchased certificate from antivirus detections
- restoration of the certificate if for some reason you have lost access to it

You'll get:
- certificate in .pfx format and its password (EV certificates require a different procedure, contact me for instructions)
- instructions for signing files in sha1, sha2 format

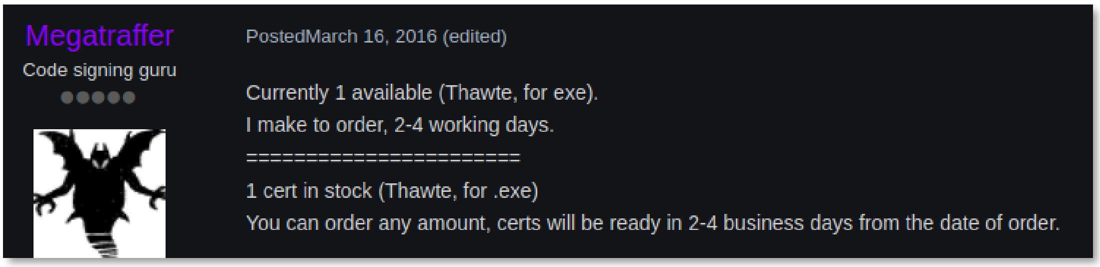
How to buy?
- by contacting me on Jabber
- work through a guarantor is welcome

Issue price:
- **Comodo** certificate - **$320**
- EV code signing certificate (**Digicert, Symantec**) - **$1500**
- resetting detections (re-release) - $50
- restoration of a lost certificate (without reissue) - free of charge
- discounts on wholesale purchases (from 3 pieces)
- I accept Bitcoin, Ethereum, Litecoin

Figure 5: Offer for both OV and EV certificates.

Regarding EV certificates, the prices range from **$2000 to $6000**, depending on several factors such as:

- If the **company name** needs to be custom-made.
- When the certificate needs to be ready by. It can go from **2-5 days up to 2 weeks**.
- Which CA will deliver the certificate (GlobalSign, Sectigo, SSL.com, Entrust, Comodo, …).
- How will the customer **access** the key pair (Cloud, sent USB, remote USB)



Megatraffer
Code signing guru

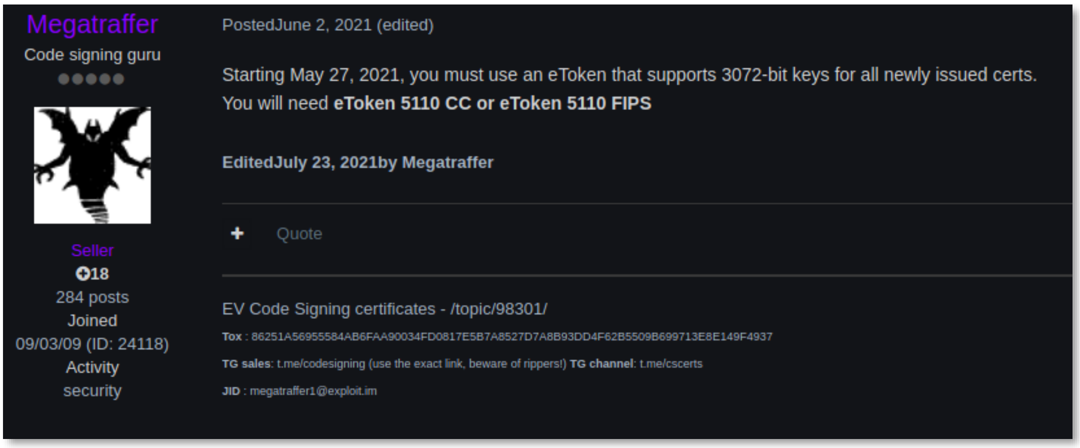
PostedMarch 16, 2016 (edited)

Currently 1 available (Thawte, for exe).
I make to order, 2-4 working days.
=======================
1 cert in stock (Thawte, for .exe)
You can order any amount, certs will be ready in 2-4 business days from the date of order.

Figure 6: Forum user advertising an order time of 2-4 business days for an EV certificate.

Cloud signing technology allows someone to sign their code using their EV certificate online, by **uploading** the file to the CA's website. However, this technology is not favoured by cybercriminals as the files are scanned by an **antivirus** as they are uploaded. In the case of malware, the user should then make their code **fully undetectable** (FUD) before uploading it to the cloud, and even then, the cloud would still have records of what has been uploaded.

If the user does not want to use the cloud service, they must use a **physical token**. The token can be ordered from the CA, and most of the forum services offer to deliver this token using a **private courier**. Some of the forum services even offer a remote USB service, in which the customer can connect to the physical token from the network.



Megatraffer
Code signing guru
Seller
18
284 posts
Joined
09/03/09 (ID: 24118)
Activity
security

PostedJune 2, 2021 (edited)

Starting May 27, 2021, you must use an eToken that supports 3072-bit keys for all newly issued certs. You will need **eToken 5110 CC or eToken 5110 FIPS**

EditedJuly 23, 2021by Megatraffer

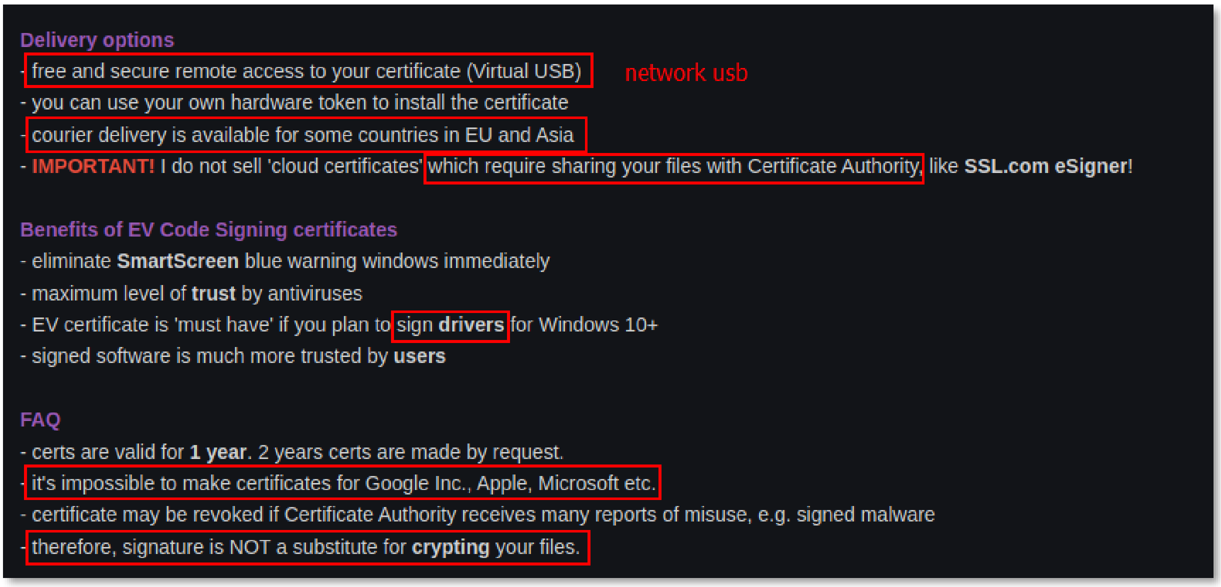
EV Code Signing certificates - /topic/98301/

Tox : 86251A56955584AB6FAA90034FD0817E5B7A8527D7A8B93DD4F62B5509B699713E8E149F4937

TG sales: t.me/codesigning (use the exact link, beware of rippers!) **TG channel**: t.me/cscerts

JID : megatraffer1@exploit.im

Figure 7: Physical token needed to use the certificates.



Delivery options

- free and secure remote access to your certificate (Virtual USB) network usb
- you can use your own hardware token to install the certificate
- courier delivery is available for some countries in EU and Asia
- **IMPORTANT!** I do not sell 'cloud certificates' which require sharing your files with Certificate Authority, like **SSL.com eSigner**!

Benefits of EV Code Signing certificates

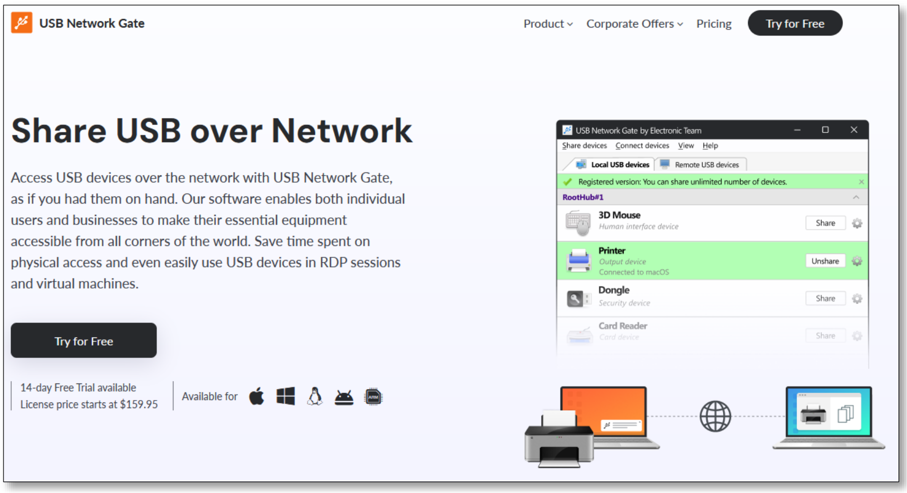
- eliminate **SmartScreen** blue warning windows immediately
- maximum level of **trust** by antiviruses
- EV certificate is 'must have' if you plan to sign **drivers** for Windows 10+
- signed software is much more trusted by **users**

FAQ

- certs are valid for **1 year**. 2 years certs are made by request.
- it's impossible to make certificates for Google Inc., Apple, Microsoft etc.
- certificate may be revoked if Certificate Authority receives many reports of misuse, e.g. signed malware
- therefore, signature is NOT a substitute for **crypting** your files.

Figure 8: EV code signing offer advertising courier delivery and remote access to the physical token.

Such “**USB over network**” technologies exist and are legitimate businesses. We found an example of such a business called USB Network Gate:



Share USB over Network

Access USB devices over the network with USB Network Gate, as if you had them on hand. Our software enables both individual users and businesses to make their essential equipment accessible from all corners of the world. Save time spent on physical access and even easily use USB devices in RDP sessions and virtual machines.

14-day Free Trial available
License price starts at $159.95

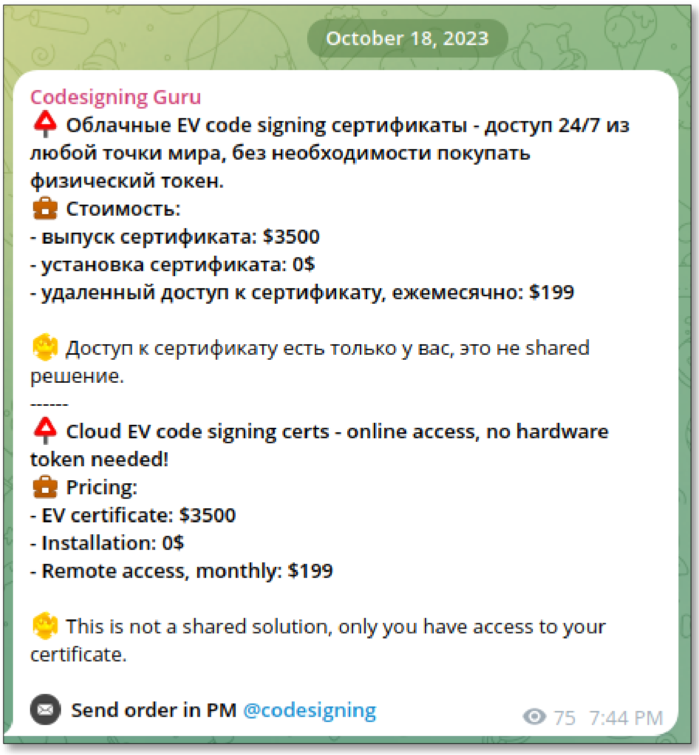
Available for

Registered version: You can share unlimited number of devices.

RootHub#1	
3D Mouse Human interface device	Share
Printer Output device Connected to macOS	Unshare
Dongle Security device	Share
Card Reader Card device	Share

Figure 9: Example of a USB over network technology.

These services are also advertised on **Telegram**, as shown in this capture offering both **cloud signing** and **remote access** to the physical token.



October 18, 2023

Codesigning Guru

🔺 **Облачные EV code signing сертификаты - доступ 24/7 из любой точки мира, без необходимости покупать физический токен.**
💼 **Стоимость:**
- выпуск сертификата: $3500
- установка сертификата: 0$
- удаленный доступ к сертификату, ежемесячно: $199

👌 Доступ к сертификату есть только у вас, это не shared решение.

🔺 **Cloud EV code signing certs - online access, no hardware token needed!**
💼 **Pricing:**
- EV certificate: $3500
- Installation: 0$
- Remote access, monthly: $199

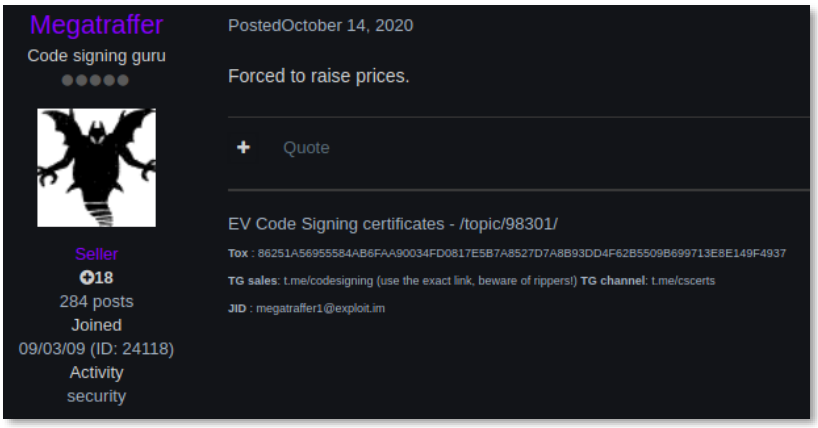
👌 This is not a shared solution, only you have access to your certificate.

✉ **Send order in PM** @codesigning

👁 75 7:44 PM

Figure 10: Telegram EV certificate service, advertising both cloud access and remote access.

These EV certificate resellers can be affected by the changes and hardening in security policies of CA. For example, this post shows that a vendor **increases their prices** due to the **higher complexity** of the screening by the CA.



Megatraffer
Code signing guru

Seller
18
284 posts
Joined
09/03/09 (ID: 24118)
Activity
security

PostedOctober 14, 2020

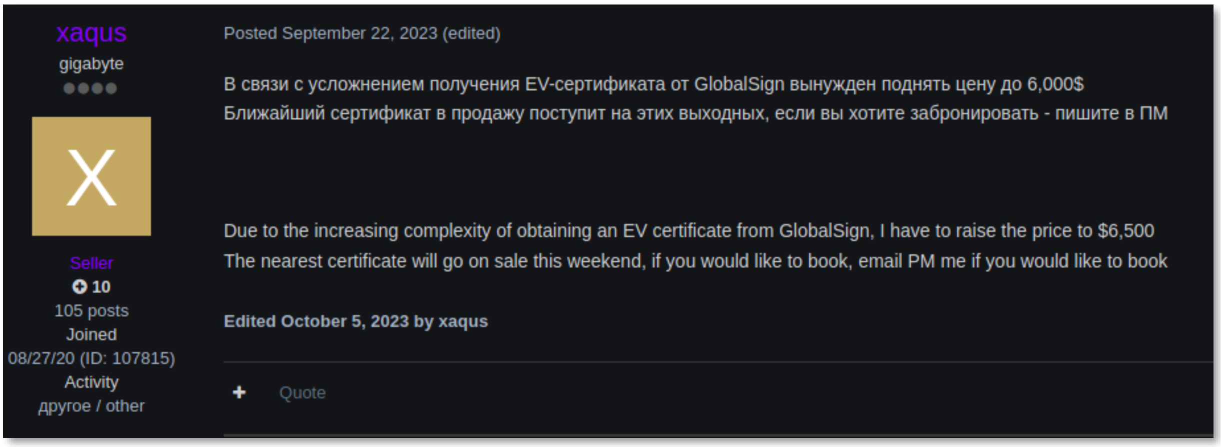
Forced to raise prices.

EV Code Signing certificates - /topic/98301/

Tox : 86251A56955584AB6FAA90034FD0817E5B7A8527D7A8B93DD4F62B5509B699713E8E149F4937

TG sales: t.me/codesigning (use the exact link, beware of rippers!) **TG channel**: t.me/cscerts

JID : megatraffer1@exploit.im



xaqus
gigabyte

Seller
10
105 posts
Joined
08/27/20 (ID: 107815)
Activity
другое / other

Posted September 22, 2023 (edited)

В связи с усложнением получения EV-сертификата от GlobalSign вынужден поднять цену до 6,000$
Ближайший сертификат в продажу поступит на этих выходных, если вы хотите забронировать - пишите в ПМ

Due to the increasing complexity of obtaining an EV certificate from GlobalSign, I have to raise the price to $6,500
The nearest certificate will go on sale this weekend, if you would like to book, email PM me if you would like to book

Edited October 5, 2023 by xaqus

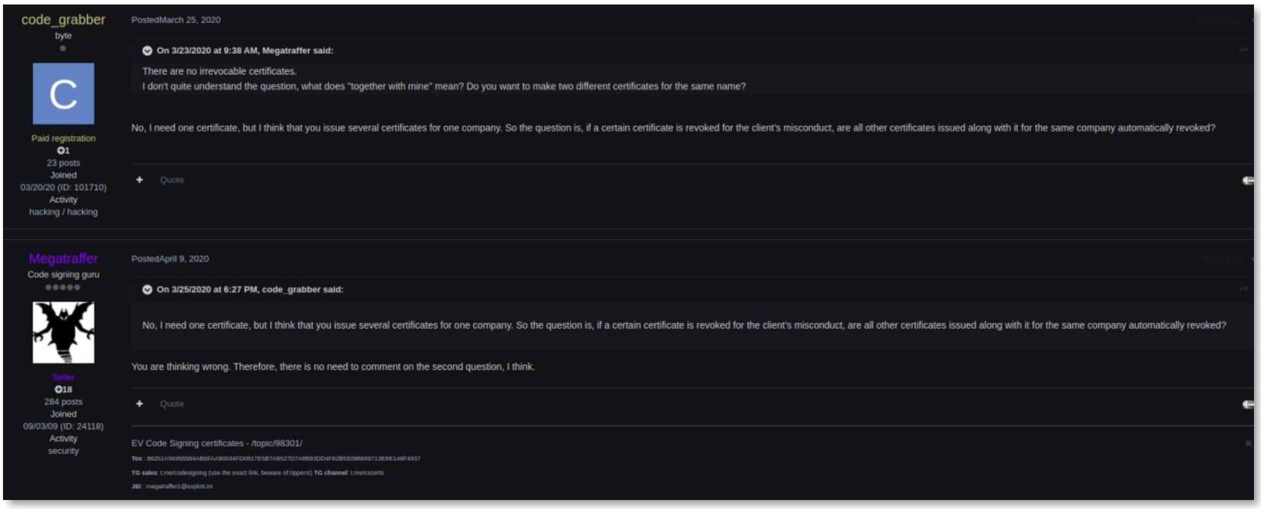
Figure 11: Variations in complexity for obtaining EV certificates results raising prices.

2.3 Process of Obtaining an EV Code Signing Certificate

One needs to have a company to register for an OV or EV code signing certificate. From our understanding, the certificate resellers either:

- **Impersonate** an **existing** company
- **Register** a **new** company

Considering the number of resellers and the volume of certificates sold, the second option seems more likely. We found a clue in one of the discussions, in which a customer asked the reseller if they re-used the company to deliver multiple certificates. A question to which the reseller answered that they do not do .



code_grabber
byte

Paid registration
1
23 posts
Joined
03/20/20 (ID: 101710)
Activity
hacking / hacking

PostedMarch 25, 2020

> **On 3/23/2020 at 9:38 AM, Megatraffer said:**
> There are no irrevocable certificates.
> I don't quite understand the question, what does "together with mine" mean? Do you want to make two different certificates for the same name?

No, I need one certificate, but I think that you issue several certificates for one company. So the question is, if a certain certificate is revoked for the client's misconduct, are all other certificates issued along with it for the same company automatically revoked?

Megatraffer
Code signing guru

Seller
18
284 posts
Joined
09/03/09 (ID: 24118)
Activity
security

PostedApril 9, 2020

> **On 3/25/2020 at 6:27 PM, code_grabber said:**
> No, I need one certificate, but I think that you issue several certificates for one company. So the question is, if a certain certificate is revoked for the client's misconduct, are all other certificates issued along with it for the same company automatically revoked?

You are thinking wrong. Therefore, there is no need to comment on the second question, I think.

EV Code Signing certificates - /topic/98301/

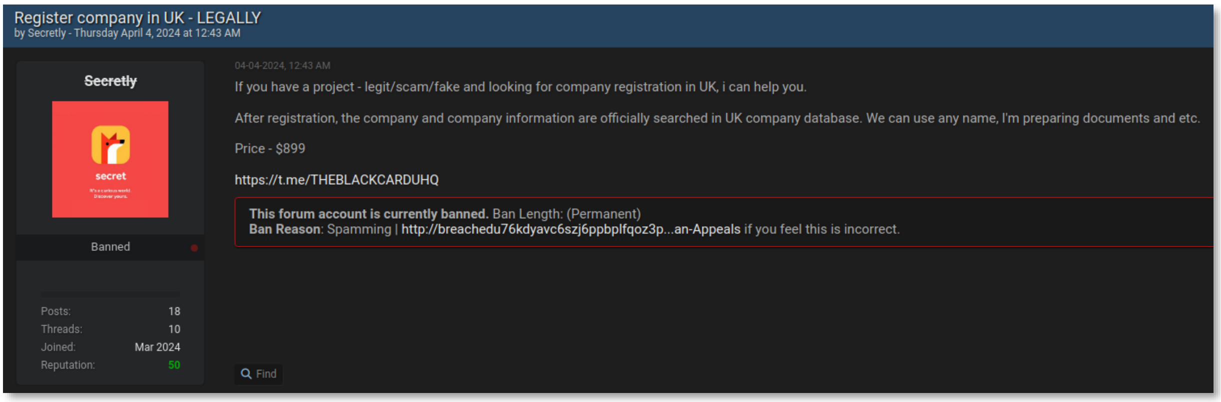
Tox : 86251A56955584AB6FAA90034FD0817E5B7A8527D7A8B93DD4F62B5509B689713E8E149F4937

TG sales: t.me/codesigning (use the exact link, beware of rippers!) **TG channel**: t.me/cscerts

JID : megatraffer1@exploit.im

Figure 12: Discussion in which the reseller claims not to use the same company for multiple certificates.

We are aware that such services to register companies exist. Here is an example on a different forum, of a user offering to **legally register a company in the UK** for $899.



Register company in UK - LEGALLY
by Secretly - Thursday April 4, 2024 at 12:43 AM

Secretly

Banned

Posts:	18
Threads:	10
Joined:	Mar 2024
Reputation:	50

04-04-2024, 12:43 AM

If you have a project - legit/scam/fake and looking for company registration in UK, i can help you.

After registration, the company and company information are officially searched in UK company database. We can use any name, I'm preparing documents and etc.

Price - $899

https://t.me/THEBLACKCARDUHQ

This forum account is currently banned. Ban Length: (Permanent)
Ban Reason: Spamming | **http://breachedu76kdyavc6szj6ppbplfqoz3p...an-Appeals** if you feel this is incorrect.

Figure 13: Service to register a company in the UK.

3 The Malwares

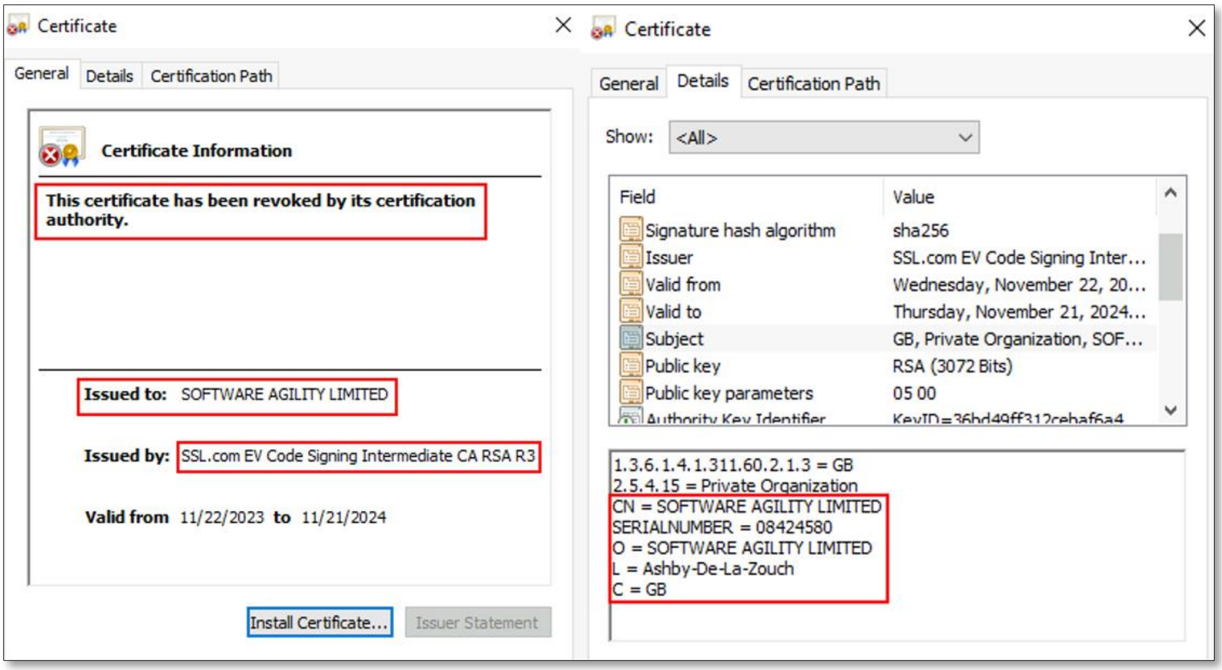
3.1 CA Delivered Certificates

Certificates delivered by CA used for malicious intents can come from either:

- An actual company that the malware operator **spoofs** to acquire a certificate
- A company **registered** by the malware operator/certificate reseller for the sole purpose of acquiring a code signing certificate

3.1.1 QakBot and PikaBot December 2023 Campaign

This QakBot campaign happened around December 15, 2023, and the samples were signed using an **EV code signing certificate** delivered by SSL.com on November 11, 2023, with subject "SOFTWARE AGILITY LIMITED". Since then, the certificate has been **revoked** by the issuer.



Certificate Information

This certificate has been revoked by its certification authority.

Issued to: SOFTWARE AGILITY LIMITED

Issued by: SSL.com EV Code Signing Intermediate CA RSA R3

Valid from 11/22/2023 **to** 11/21/2024

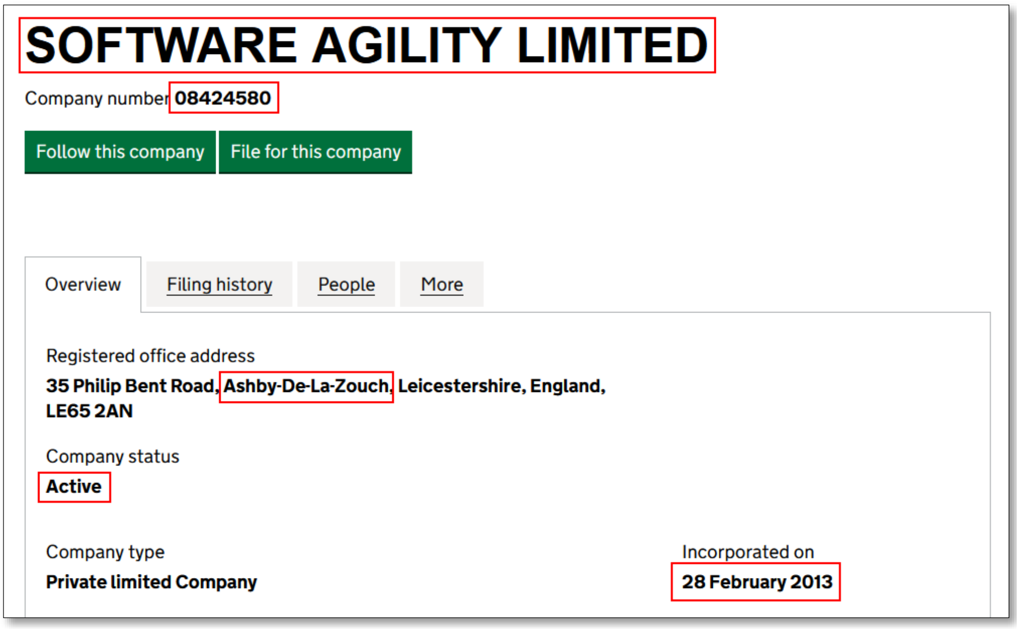
Show: <All>

Field	Value
Signature hash algorithm	sha256
Issuer	SSL.com EV Code Signing Inter...
Valid from	Wednesday, November 22, 20...
Valid to	Thursday, November 21, 2024...
Subject	GB, Private Organization, SOF...
Public key	RSA (3072 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=36bd49ff312cebaf6a4

```
1.3.6.1.4.1.311.60.2.1.3 = GB
2.5.4.15 = Private Organization
CN = SOFTWARE AGILITY LIMITED
SERIALNUMBER = 08424580
O = SOFTWARE AGILITY LIMITED
L = Ashby-De-La-Zouch
C = GB
```

Figure 14: Certificate used during December 2023 QakBot campaign (VirusTotal).

Using the UK company information service, we were able to find this company which was registered in February 2013. This company does not seem to have had much activity, which may suggest that it was **registered by an ill-intentioned person**. However, the fact that it was registered 10 years ago could also lead to assume that this was once a legitimate company that has been **spoofed** by the attackers, possibly using leaked data. QakBot has also been seen **dumping key pairs** from infected computers, which can be re-used for code signing if no physical token is needed.



SOFTWARE AGILITY LIMITED

Company number 08424580

Registered office address
35 Philip Bent Road, Ashby-De-La-Zouch, Leicestershire, England, LE65 2AN

Company status
Active

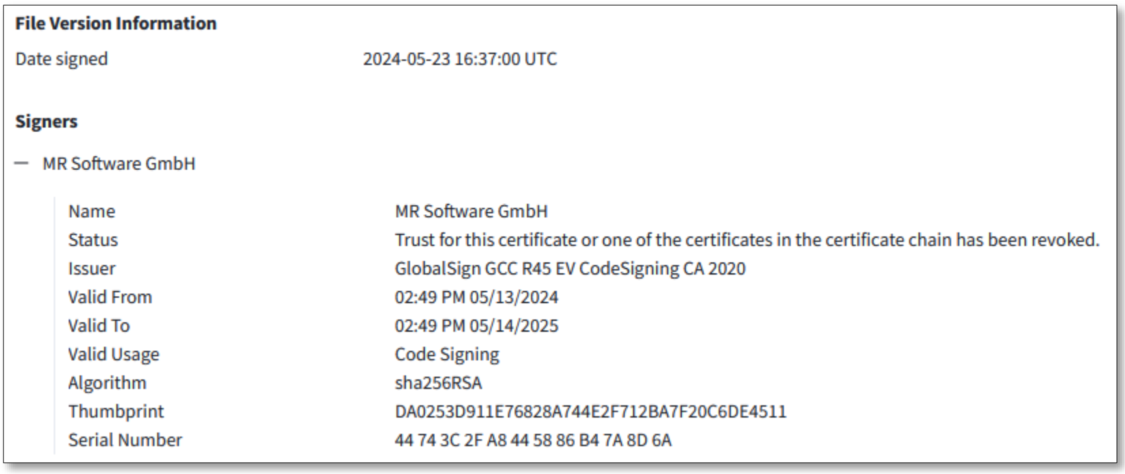
Company type
Private limited Company

Incorporated on
28 February 2013

Figure 15: Registration of the company subject of the certificate (Source).

3.1.2 Grandoreiro Banker Impersonates a Closed Company

We found on VirusTotal a case of company **impersonation**. **Grandoreiro** is a banking trojan active in South America since at least 2019, and it was distributed recently, around May 23, 2024. It was signed by a valid EV code signing certificate of subject "**MR Software GmbH**" delivered by GlobalSign on May 13, 2024.



File Version Information

Date signed	2024-05-23 16:37:00 UTC

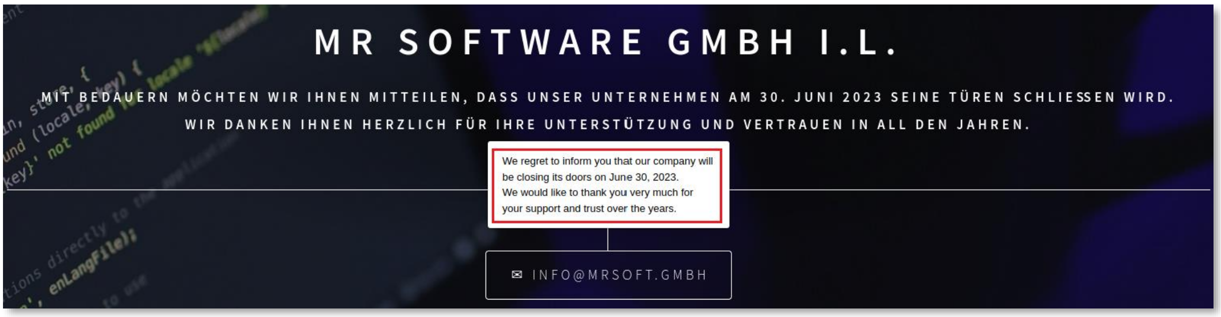
Signers

— MR Software GmbH

Name	MR Software GmbH
Status	Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Issuer	GlobalSign GCC R45 EV CodeSigning CA 2020
Valid From	02:49 PM 05/13/2024
Valid To	02:49 PM 05/14/2025
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	DA0253D911E76828A744E2F712BA7F20C6DE4511
Serial Number	44 74 3C 2F A8 44 58 86 B4 7A 8D 6A

Figure 16: Certificate used to sign Grandoreiro.

After looking up the company, we discovered that **the company has been closed since June 30**, 2023. This suggests that the person applying for the certificate probably exploited this fact to **impersonate** the company.



MR SOFTWARE GMBH I.L.

MIT BEDAUERN MÖCHTEN WIR IHNEN MITTEILEN, DASS UNSER UNTERNEHMEN AM 30. JUNI 2023 SEINE TÜREN SCHLIESSEN WIRD.
WIR DANKEN IHNEN HERZLICH FÜR IHRE UNTERSTÜTZUNG UND VERTRAUEN IN ALL DEN JAHREN.

We regret to inform you that our company will be closing its doors on June 30, 2023.
We would like to thank you very much for your support and trust over the years.

✉ INFO@MRSOFT.GMBH

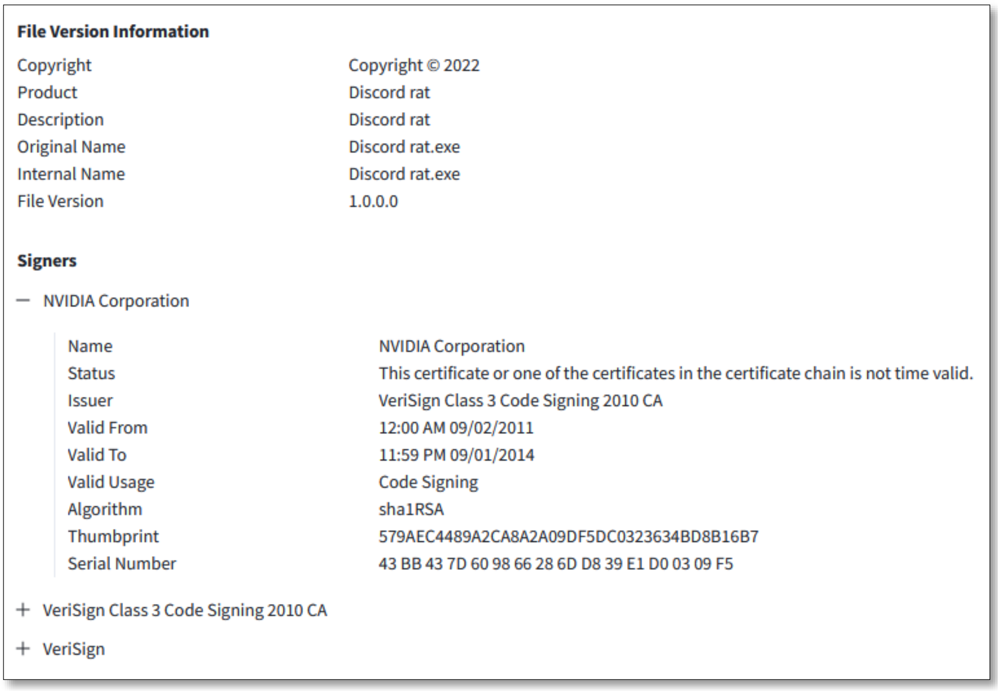
Figure 17: Closed company impersonated for a valid certificate (Source).

3.2 Stolen Certificates

3.2.1 NVIDIA

In early 2022, **NVIDIA** suffered a cyber-attack by the **Lapsus$ extorsion group** during which at least two code signing **certificates** were **stolen** (amongst other proprietary data). These valid certificates were later spread and used by threat actors to sign their malicious code.

Here is an example of the **Discord RAT signed** using one of NVIDIA's leaked certificates, uploaded to VirusTotal on May 9, 2024.



File Version Information

Copyright	Copyright © 2022
Product	Discord rat
Description	Discord rat
Original Name	Discord rat.exe
Internal Name	Discord rat.exe
File Version	1.0.0.0

Signers

— NVIDIA Corporation

Name	NVIDIA Corporation
Status	This certificate or one of the certificates in the certificate chain is not time valid.
Issuer	VeriSign Class 3 Code Signing 2010 CA
Valid From	12:00 AM 09/02/2011
Valid To	11:59 PM 09/01/2014
Valid Usage	Code Signing
Algorithm	sha1RSA
Thumbprint	579AEC4489A2CA8A2A09DF5DC0323634BD8B16B7
Serial Number	43 BB 43 7D 60 98 66 28 6D D8 39 E1 D0 03 09 F5

+ VeriSign Class 3 Code Signing 2010 CA

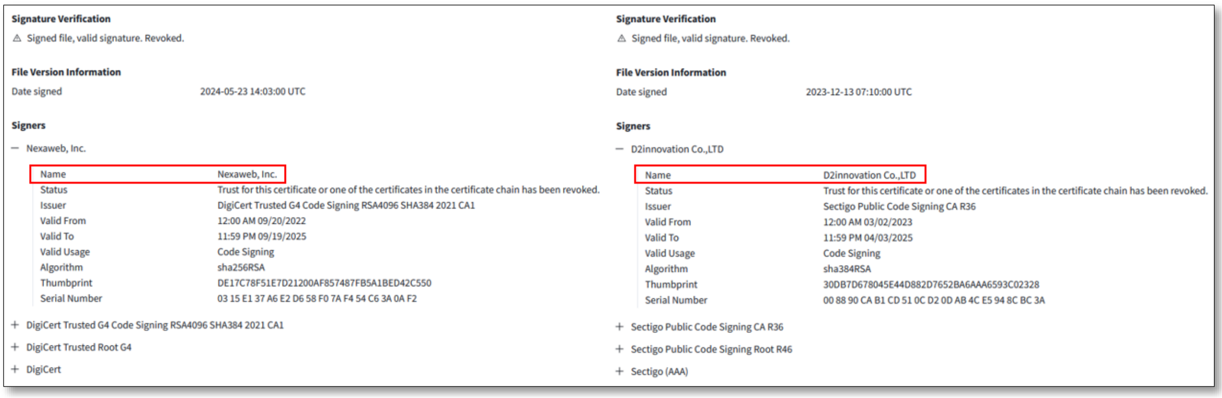
+ VeriSign

Figure 18: Discord RAT signed with NVIDIA's leaked certificate.

Even though the certificate expired in 2014, **Windows will still recognise the signature** as valid for loading the **drivers**.

3.2.2 The Case of Kimsuky

Kimsuky is an **Advanced Persistent Threat** allegedly from **North Korea** that targets South Korean critical entities such as critical infrastructure, industry, and government bodies for espionage purposes. This APT is known for resorting to code signing certificates. Here are two examples of **Kimsuky malware** signed using possibly **stolen certificates** belonging to one South Korean company and one American company.



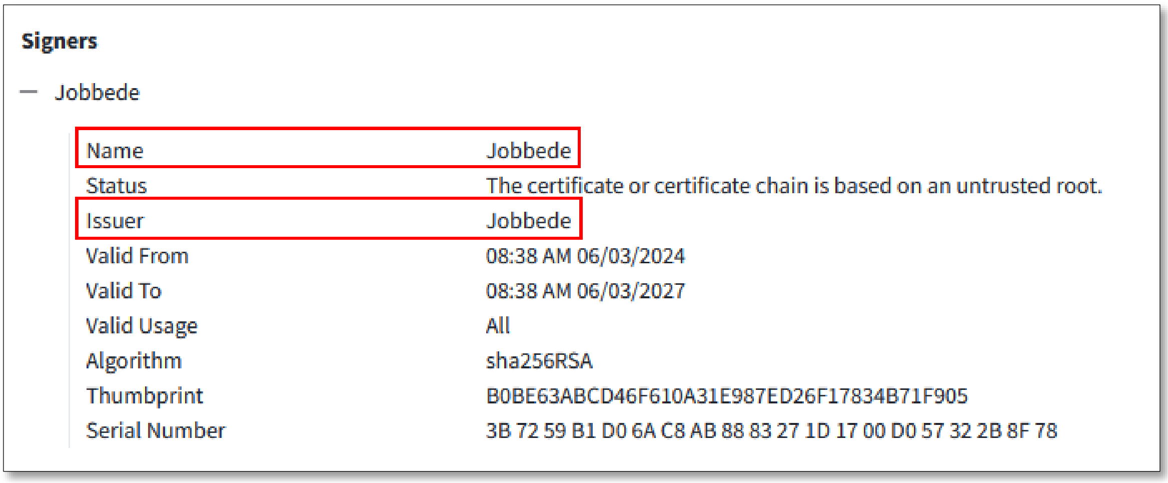
```
Signature Verification
⚠ Signed file, valid signature. Revoked.

File Version Information
Date signed                2024-05-23 14:03:00 UTC

Signers
— Nexaweb, Inc.
    Name             Nexaweb, Inc.
    Status           Trust for this certificate or one of the certificates in the certificate chain has been revoked.
    Issuer           DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
    Valid From       12:00 AM 09/20/2022
    Valid To         11:59 PM 09/19/2025
    Valid Usage      Code Signing
    Algorithm        sha256RSA
    Thumbprint       DE17C78F51E7D21200AF857487FB5A1BED42C550
    Serial Number    03 15 E1 37 A6 E2 D6 58 F0 7A F4 54 C6 3A 0A F2

+ DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
+ DigiCert Trusted Root G4
+ DigiCert
```

```
Signature Verification
⚠ Signed file, valid signature. Revoked.

File Version Information
Date signed                2023-12-13 07:10:00 UTC

Signers
— D2innovation Co.,LTD
    Name             D2innovation Co.,LTD
    Status           Trust for this certificate or one of the certificates in the certificate chain has been revoked.
    Issuer           Sectigo Public Code Signing CA R36
    Valid From       12:00 AM 03/02/2023
    Valid To         11:59 PM 04/03/2025
    Valid Usage      Code Signing
    Algorithm        sha384RSA
    Thumbprint       30DB7D678045E44D882D7652BA6AAA6593C02328
    Serial Number    00 88 90 CA B1 CD 51 0C D2 0D AB 4C E5 94 8C BC 3A

+ Sectigo Public Code Signing CA R36
+ Sectigo Public Code Signing Root R46
+ Sectigo (AAA)
```

Figure 19: Kimsuky malwares signed using possibly stolen certificates. Left. Right.

3.3 Self-Signed Certificates

Even though they are not very effective at bypassing malware protection systems, **self-signed certificates** are widely used in malware as a form of **social engineering**. They are **free** and can fool users into believing that the malware they are running is from a legitimate software vendor. Here is an example of a **FormBook/XLoader** (a popular RAT targeting Windows computers) sample distributed by **GuLoader** that was signed using a self-signed certificate.



```
Signers
— Jobbede
    Name             Jobbede
    Status           The certificate or certificate chain is based on an untrusted root.
    Issuer           Jobbede
    Valid From       08:38 AM 06/03/2024
    Valid To         08:38 AM 06/03/2027
    Valid Usage      All
    Algorithm        sha256RSA
    Thumbprint       B0BE63ABCD46F610A31E987ED26F17834B71F905
    Serial Number    3B 72 59 B1 D0 6A C8 AB 88 83 27 1D 17 00 D0 57 32 2B 8F 78
```

Figure 20: Example of a self-signed certificate used to sign FormBook (VirusTotal).

4 Actionable content

4.1 Indicators of compromise

Value	Type	Description
faca8b6f046dad8f0e27a75fa2dc5477d3ccf44adced64481ef1b0dd968b4b0e	SHA-256	Kimsuky – ZIP - “Job Description (LM HR Division II).zip”
cca1705d7a85fe45dce9faec5790d498427b3fa8e546d7d7b57f18a925fdfa5d	SHA-256	Kimsuky – EXE - “Job Description (LM HR Division II).pdf .scr”
ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca	SHA-256	Kimsuky - EXE
93a98b919aec23411ae62dba8d0d22f939da45dec19db2b4e7293124d8f1507f	SHA-256	QakBot - MSI
bd4f77fab5f0b23d7bdd4fc59eda4ea29888c049acbae9293b02ea9bb90c2947	SHA-256	Grandoreiro - MSI
dd2d5f3f85924ec11cbd69da21bd0b25c5c8034aad3d9490c96e39f20b966d4f	SHA-256	GuLoader / FormBook - EXE
3f10da079f9a101c55635d8bd1a091afa18d59b7076a2fee91775ac8fbe2d684	SHA-256	Discord RAT – EXE

4.2 Recommendations

- Implement strict policies about application vendor whitelisting and blacklisting
- Conduct thorough certificate validation
- Educate and train employees to detect unsigned code and malicious signers
- As far as Advertisers are concerned, avoid using first Google search results which contain the tag “Ad”. Use instead the first “organic” search result to initiate downloads from the official website of the searched software name
- Implement certificate revocation checking
- Use reputation-based threat intelligence for malicious certificates
- Use sandboxing and isolation techniques for unknown executables

Sources

- ➢ https://squiblydoo.blog/2024/05/13/impostor-certs/
- ➢ https://www.reversinglabs.com/blog/digital-certificates-impersonated-executives-as-certificate-identity-fronts
- ➢ https://www.trendmicro.com/en_us/research/22/j/where-is-the-origin-qakbot-uses-valid-code-signing-.html
- ➢ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537361(v=vs.85)