

Cyber Threat Intelligence

The EV Code Signature Market for eCrime



<u>@Intrinsec</u>



<u>@Intrinsec</u>





<u>Blog</u>

<u>Website</u>

024 Intrinsec Inc. All rights reserved



# TLP: CLEAR

# PAP: CLEAR

# Table of contents

Key findi	ngs3
Introduc	tion
1 Asy	mmetric Cryptography and Code Signing 4
1.1	Public Key Cryptography
1.2	Certificates 4
1.3	Code Signing and Authenticode
2 The	Market
2.1	Benefits of Code Signing for Cybercrime7
2.2	Cybercrime Code Signing Market7
2.3	Process of Obtaining an EV Code Signing Certificate11
3 The	Malwares
3.1	CA Delivered Certificates
3.1.	1 QakBot and PikaBot December 2023 Campaign
3.1.	2 Grandoreiro Banker Impersonates a Closed Company 14
3.2	Stolen Certificates
3.2.	1 NVIDIA
3.2.	2 The Case of Kimsuky 16
3.3	Self-Signed Certificates
4 Acti	onable content
4.1	Indicators of compromise17
4.2	Recommendations
Sources.	



#### **TLP: CLEAR**

#### **PAP: CLEAR**

# 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.

© Intrinsec TLP : CLEAR Page **3** sur **17** 



#### **TLP: CLEAR**

PAP: CLEAR

# 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)

# Public key cryptography Encryption : Signing : CipherText = PublicKey(ClearText) Signature = PrivateKey(Hash(Text))



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.

> © Intrinsec TLP : CLEAR Page **4** sur **17**



#### **TLP: CLEAR**

PAP: CLEAR

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.

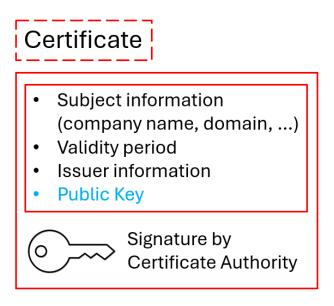


Figure 2: Contents of a certificate.

© Intrinsec TLP : CLEAR Page **5** sur **17** 



#### TLP: CLEAR

#### **PAP: CLEAR**

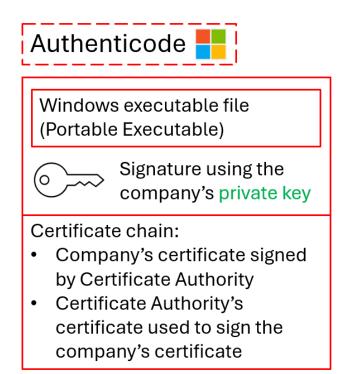
## 1.3 Code Signing and Authenticode

**Authenticode** is a code signing standard developed by Microsoft for signing Windows executable files, **Portable Executable** (PE). The PE format contains a structure called <u>Attribute Certificate Table</u> 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



*Figure 3: Authenticode: Windows' code signing mechanism.* 

© Intrinsec TLP : CLEAR Page **6** sur **17** 



#### **TLP: CLEAR**

#### **PAP: CLEAR**

# 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	•	8
Sign pre-Windows-10 Drivers	•	0
Instant Microsoft SmartScreen Reputation	⊘	0
Two-factor Authentication with USB Token or Cloud Signing Service	0	0
Available to Individuals Without a Registered Business	8	0
Trusted on Major Software Platforms	0	0

#### Figure 4: Benefits of code signing from <u>SSL.com</u>.

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

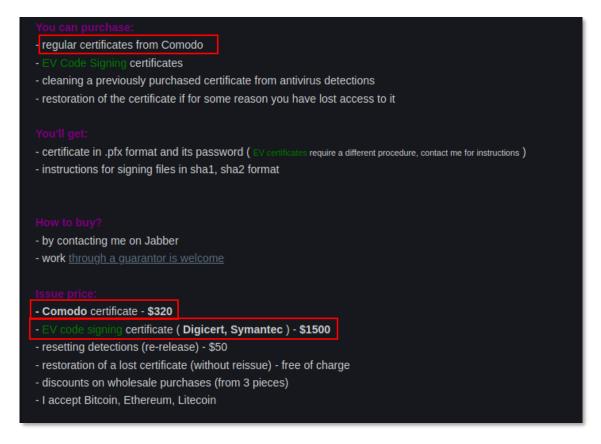
Most of the advertising seen on the forum concerns EV certificates. The sellers probably assume that registering for an OV certificate is easy enough so that one does not need to pay a dedicated service to access it. We did, however, see a couple of offers regarding **OV certificates**, their prices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

© Intrinsec TLP : CLEAR Page **7** sur **17** 



#### **TLP: CLEAR**

#### **PAP: CLEAR**



#### 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	PostedMarch 16, 2016 (edited)
Code signing guru	Currently 1 available (Thawte, for exe). I make to order, 2-4 working days.
	======================================

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.

© Intrinsec TLP : CLEAR Page **8** sur **17** 



#### **TLP: CLEAR**

#### PAP: CLEAR

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.





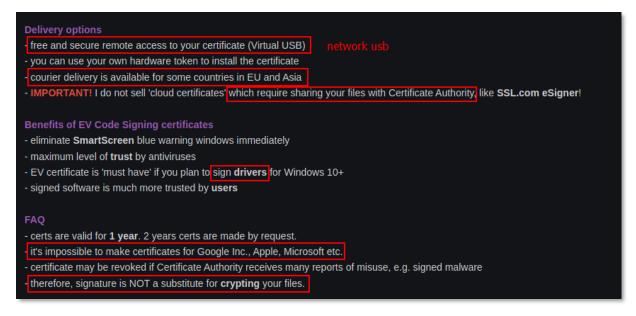


Figure 8: EV code signing offer advertising courier delivery and remote access to the physical token.

© Intrinsec TLP : CLEAR Page **9** sur **17** 



#### TLP: CLEAR

**PAP: CLEAR** 

INTRI

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

USB Network Gate	Product - Corporate Offers - Pricing Try for Free			
Share USB over Network	■ 11:53 Nortonin & Gone by Clemanic Feam,     -     -     -     -       Start centrals: Contract Backins: You     -     -     -     -       ✓ Log and SB4 devices:     -     -     -     -     -       ✓ Log and reference from them calmented for some them calmented number of devices:     -     -     -     -       ✓ Registrations:     -     -     -     -     -     -     -			
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	Retronative Constant			
and virtual machines.	Control environment     Control device     Con			
14 day Free Trial available License price starts at \$159.95				

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.



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.

© Intrinsec TLP : CLEAR Page **10** sur **17** 



#### **TLP: CLEAR**

#### **PAP: CLEAR**

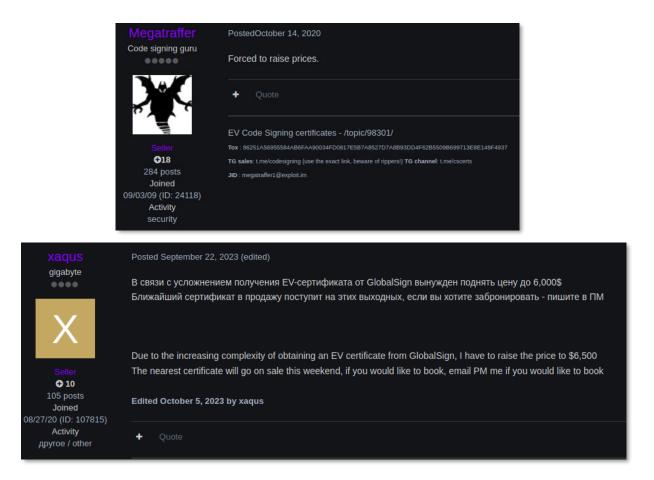


Figure 11: Variations in complexity for obtaining EV certificates results raising prices.

#### 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 .

© Intrinsec TLP : CLEAR Page **11** sur **17** 



#### TLP: CLEAR

#### PAP: CLEAR

code_grabber	PostedMarch 25, 2020	ł
	😋 On 3/23/2020 at 9:38 AM, Megatraffer said:	
С	There are no interocable 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?	
Paid registration 01 23 posts	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?	
Joined 03/20/20 (ID: 101710) Activity hacking / hacking		e
Megatraffer Code signing guru		ļ
0000 3411119 9410	On 3/25/2020 at 8:27 PM, code. grabber said:	1
X	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?	
Seller	You are thinking wrong. Therefore, there is no need to comment on the second question, I think.	
●18 284 posts Joined 09/03/09 (ID: 24118)		e
Activity security		
	To Guide curveColorging (cur the curve) of report) To diverse it noticents 20 regarding (curve) curve) in the curve of report (curve) curve curve of the curve	

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 by Secretly - Thursday April	UK - LEGALLY 124 at 12:43 AM
Secretly	04-04-2024, 12-23 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
Banned	This forum account is currently banned. Ban Length: (Permanent) Ban Reason: Spamming   http://breachedu76kdyavc6sz]6ppbplfqoz3pan-Appeals if you feel this is incorrect.
Posts: Threads:	18 10 224 96 Q Find

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

© Intrinsec TLP : CLEAR Page **12** sur **17** 



#### **TLP: CLEAR**

#### **PAP: CLEAR**

# 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	× 🛺 Certificate	
General Details Certification Path	General Details Certification Path	
Certificate Information	Show: <all></all>	
This certificate has been revoked by its certification authority.  Issued to: SOFTWARE AGILITY LIMITED	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	•
Issued by: SSL.com EV Code Signing Intermediate CA RSA R3 Valid from 11/22/2023 to 11/21/2024	I.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	· _
Install Certificate Issuer Statement		

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.

© Intrinsec TLP : CLEAR Page **13** sur **17** 



#### TLP: CLEAR

**PAP: CLEAR** 

	<b>WARE</b>	AGILIT	Y LIMIT	ED	
Follow this c		his company			
Overview	Filing history	People More			
-	office address ent Road. Ashby-D	e-La-Zouch, Leicester	shire. England,		
LE65 2AN Company st					
Active Company ty	/pe			Incorporated on	
	ited Company			28 February 2013	

Figure 15: Registration of the company subject of the certificate (<u>Source</u>).

#### 3.1.2 Grandoreiro Banker Impersonates a Closed Company

We found on <u>VirusTotal</u> 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 \	/ersion Information	
Date	signed	2024-05-23 16:37:00 UTC
Sign	ers	
— м	R 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.

© Intrinsec TLP : CLEAR Page **14** sur **17** 



#### **TLP: CLEAR**

**PAP: CLEAR** 



Figure 17: Closed company impersonated for a valid certificate (<u>Source</u>).

# 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 <u>VirusTotal</u> on May 9, 2024.

Convictor	Committee 2002				
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					
<ul> <li>NVIDIA Corporation</li> </ul>					
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	2 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**.

© Intrinsec TLP : CLEAR Page **15** sur **17** 



#### **TLP: CLEAR**

#### **PAP: CLEAR**

#### 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. Revok	ed.		nature Verification Signed file, valid signature. Revoked.	
File Version Information Date signed	2024-05-23 14:03:00 UTC		e Version Information te signed	2023-12-13 07:10:00 UTC
Signers — Nexaweb, Inc.			ners D2innovation Co.,LTD	
Name	Nexaweb, Inc.		Name	D2innovation Co.,LTD
Status	Trust for this certificate or one of the certificates in the certificate chain has been revoked.		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		Issuer	Sectigo Public Code Signing CA R36
Valid From	12:00 AM 09/20/2022		Valid From	12:00 AM 03/02/2023
Valid To	11:59 PM 09/19/2025		Valid To	11:59 PM 04/03/2025
Valid Usage	Code Signing		Valid Usage	Code Signing
Algorithm	sha256RSA		Algorithm	sha384RSA
Thumbprint	DE17C78F51E7D21200AF857487FB5A1BED42C550		Thumbprint	30DB7D678045E44D882D7652BA6AAA6593C02328
Serial Number	03 15 E1 37 A6 E2 D6 58 F0 7A F4 54 C6 3A 0A F2		Serial Number	00 88 90 CA B1 CD 51 0C D2 0D AB 4C E5 94 8C BC 3A
+ DigiCert Trusted G4 Code Signing	RSA4096 SHA384 2021 CA1	+	Sectigo Public Code Signing CA R36	
+ DigiCert Trusted Root G4		+	Sectigo Public Code Signing Root R46	
+ DigiCert		+	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.

ers	
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).

© Intrinsec TLP : CLEAR Page **16** sur **17** 



#### **TLP: CLEAR**

**PAP: CLEAR** 

# 4 Actionable content

#### 4.1 Indicators of compromise

Value	Туре	Description
faca8b6f046dad8f0e27a75fa2dc5477d3ccf44ad	SHA-256	Kimsuky – ZIP - "Job Description (LM HR
ced64481ef1b0dd968b4b0e		Division II).zip"
cca1705d7a85fe45dce9faec5790d498427b3fa8	SHA-256	Kimsuky – EXE - "Job Description (LM HR
e546d7d7b57f18a925fdfa5d		Division II).pdf .scr"
ff3718ae6bd59ad479e375c602a81811718dfb26	SHA-256	Kimsuky - EXE
69c2d1de497f02baf7b4adca		
93a98b919aec23411ae62dba8d0d22f939da45d	SHA-256	QakBot - MSI
ec19db2b4e7293124d8f1507f		
bd4f77fab5f0b23d7bdd4fc59eda4ea29888c049	SHA-256	Grandoreiro - MSI
acbae9293b02ea9bb90c2947		
dd2d5f3f85924ec11cbd69da21bd0b25c5c8034	SHA-256	GuLoader / FormBook - EXE
aad3d9490c96e39f20b966d4f		
3f10da079f9a101c55635d8bd1a091afa18d59b7	SHA-256	Discord RAT – EXE
076a2fee91775ac8fbe2d684		

#### 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-ascertificate-identity-fronts
- https://www.trendmicro.com/en\_us/research/22/j/where-is-the-origin-qakbot-uses-validcode-signing-.html
- https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/iedeveloper/platform-apis/ms537361(v=vs.85)

© Intrinsec TLP : CLEAR Page **17** sur **17**