2024 DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

P-WAVE OF MALICIOUS CODE SIGNING

Yuta Sawabe, Shogo Hayashi & Rintaro Koike

NTT Security Holdings, Japan

yuta.sawabe@security.ntt
syogo.hayashi@security.ntt
rintaro.koike@security.ntt

ABSTRACT

These days, regardless of being related to APT or crime, many pieces of malware and malicious files are code signed. This is largely due to the existence of code-signing certificate sellers that play a role in the ecosystem. Instead of preparing code-signing certificates themselves, attackers can simply buy them.

We took a serious look at the interesting behaviour of code-signing certificate sellers. Prior to selling the certificates to their customers, they had signed benign software using the certificates and posted the signed software to online malware scanning services to test whether the certificates were judged as expected (not only valid, but also benign). Such inspections occurred long before the certificates were sold and abused by attackers.

We collected the files posted by these sellers and harvested code-signing certificate information that could be abused in the future. This was a kind of experiment to predict the future – and we succeeded in predicting future abuse cases. This could be an effective approach against code-signed malware and malicious files.

In this paper we will first introduce the code-signing certificate sellers and their ecosystem. Then, we will illustrate their interesting inspections with a detailed timeline. Finally, we will present the approach we have developed and evaluate its effectiveness.

CURRENT STATUS OF CODE-SIGNED MALWARE

Many of the software applications we use daily, such as web browsers, word processors and communication tools, are code signed. A code-signing certificate ensures the legitimacy of software, verifies that it has not been tampered with, and that it maintains its security and integrity. However, it is not uncommon for malware and malicious files to be code signed these days [1]. As shown in Table 1, there are two major types of code-signing abuse.

1	Threat actors use leaked or stolen code-signing certificates from some entity
2	Threat actors use code-signing certificates issued in some way

Table 1: Types of code-signing certificate abuse.

Traditionally, malware with code signing has generally pointed to the abuse of stolen certificates (Type 1 in Table 1). For example, it was reported in 2010 [2] that Stuxnet was signed with a stolen code-signing certificate. It was also reported in 2022 that the LAPSUS$ ransomware group stole code-signing certificates from *NVIDIA* and used those certificates to sign malware [3].

Nowadays, however, code-signed malware is also used in cases of widespread and high-frequency attacks, i.e. spray-and-play attacks. These attacks tend to use certificates in the manner described in Type 2 of Table 1. As one example, *Trend Micro* published a blog post about QAKBOT certificates in 2022 [4]. In the article, the researchers raise the possibility that QAKBOT obtained code-signing certificates from official certificate authorities (CAs) in some way. In addition, there have been a number of studies on the fraudulent obtaining of code-signing certificates, and it is known that code-signing certificates are traded on dark markets used by attackers [5] [6].

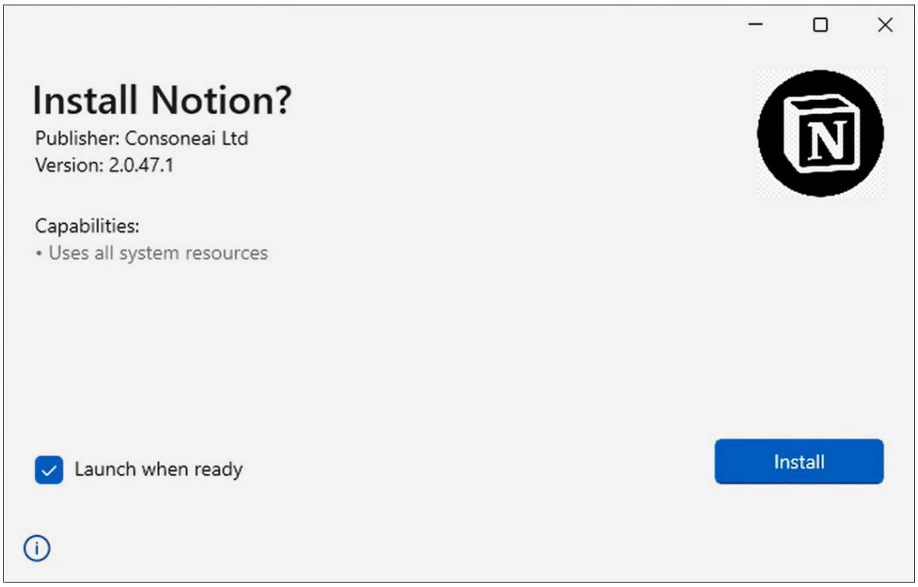
Thus, code-signed malware and malicious files are now being used not only in sophisticated state-sponsored cyber attacks, but also in financially motivated and other spray-and-play attacks in which anyone can be targeted, and the reliability of code-signing certificates is declining. We should not feel safe just because certain software is ‘code signed’. However, it is not practical for users to judge whether the code-signing certificates are trustworthy or not, or whether there is a possibility of theft. We need to seriously discuss the abuse of code-signing certificates.

ATTACK CAMPAIGNS USING CODE-SIGNED MALICIOUS FILES

Over the past year or so, one of the most common attacks abusing code signing has been with MSIX files. Two main sellers (BatLoader and FakeBat) provide weaponized MSIX files on the dark market, and many attack campaigns have been observed utilizing them [7] [8]. An MSIX file is required to be signed with a valid code-signing certificate in order to work [9]. Therefore, sellers dealing in weaponized MSIX files must obtain code-signing certificates in some way. Figure 1 shows an example of a malicious MSIX file.

Most attacks using malicious MSIX files have similar attack flows. Attackers mimic websites that distribute well-known software applications and set up advertising networks to reach those fake websites. In many cases, *Google* pay-per-click advertisements are leveraged, which appear as sponsored links when users search for names of the software in the search engine [10]. Figure 2 shows a malicious advertisement displayed in the *Google Search* results page.

When a user clicks on a download link on a fake software distribution website created by an attacker, a malicious MSIX file is downloaded. If the user executes the MSIX file, they are infected with malware.



Install Notion?

Publisher: Consoneai Ltd

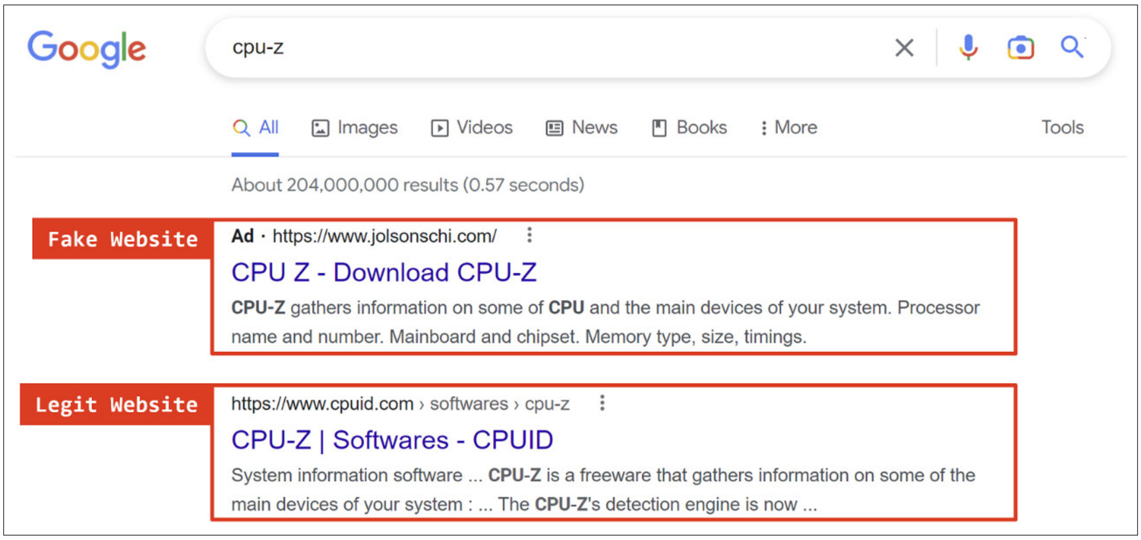
Version: 2.0.47.1

Capabilities:

- Uses all system resources

☑ Launch when ready

Figure 1: Example of malicious MSIX file.



cpu-z

About 204,000,000 results (0.57 seconds)

Ad · https://www.jolsonschi.com/

CPU Z - Download CPU-Z

CPU-Z gathers information on some of **CPU** and the main devices of your system. Processor name and number. Mainboard and chipset. Memory type, size, timings.

https://www.cpuid.com › softwares › cpu-z

CPU-Z | Softwares - CPUID

System information software ... **CPU-Z** is a freeware that gathers information on some of the main devices of your system : ... The **CPU-Z**'s detection engine is now ...

Figure 2: Malicious advertisement displayed in Google Search results page.

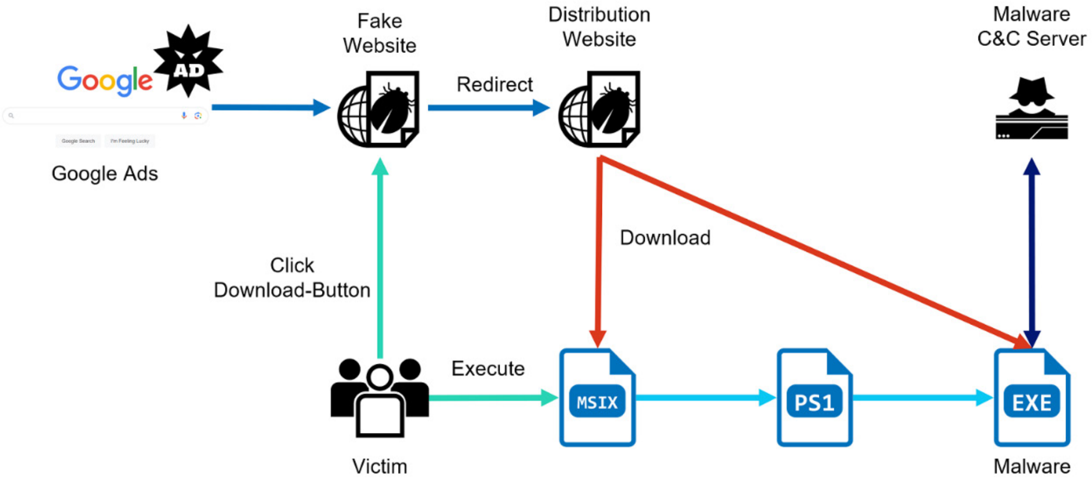
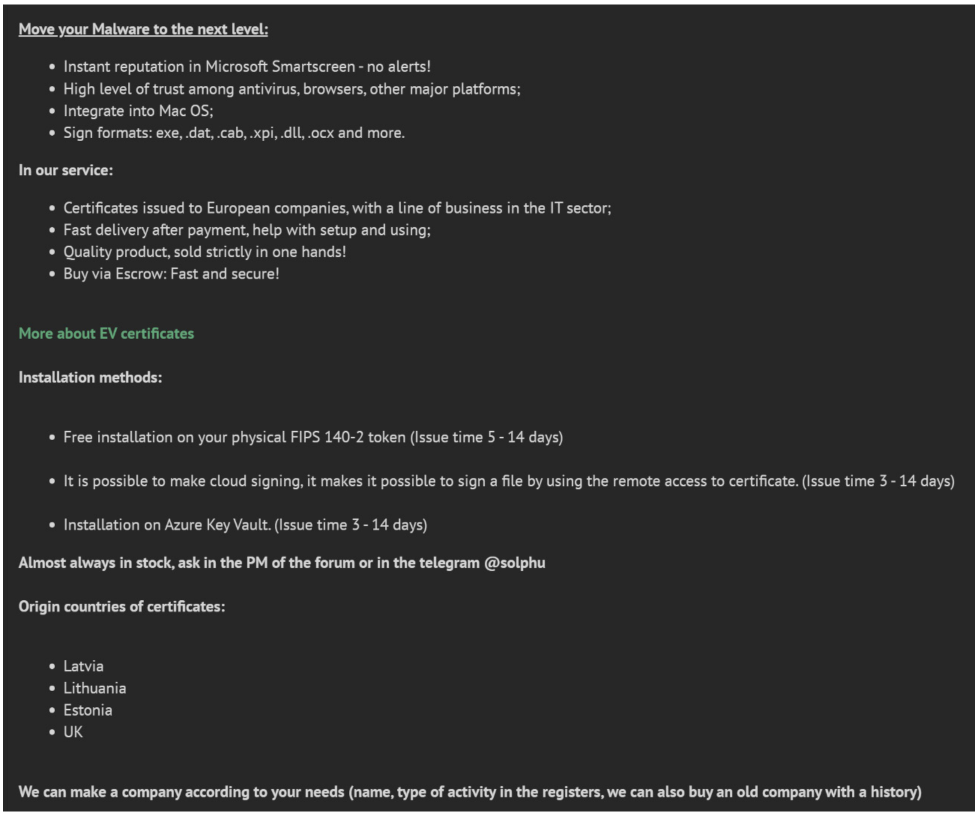


Figure 3: Attack flow using malicious MSIX file.

CODE-SIGNING CERTIFICATE SELLERS ON DARK MARKETS

We have been researching malicious MSXI files since February 2023, when their use began to emerge. Our investigation revealed that two sellers deal with weaponization services of MSIX files and provide code signing as an optional service. However, the sellers of MSIX file weaponization services do not obtain the code-signing certificates themselves. It is presumed that they purchase code-signing certificates from sellers offering such certificates on the dark market [11]. For example, according to an *eSentire* report, 'Afron', which sells BatLoader, is associated with a code-signing certificate seller called 'arbadakarba2000' [12]. Similarly, 'Eugenfest', which sells FakeBat, has a relationship with a seller called 'Balamut Service'.

Figure 4 shows a posting made by Balamut Service on the dark market. It notes that the purpose of signing malware is to bypass *Windows SmartScreen* and browser security mechanisms. In addition, the Baltic States (Latvia, Lithuania and Estonia) and the United Kingdom are listed as the origin countries of certificates.



Move your Malware to the next level:

- Instant reputation in Microsoft Smartscreen - no alerts!
- High level of trust among antivirus, browsers, other major platforms;
- Integrate into Mac OS;
- Sign formats: exe, .dat, .cab, .xpi, .dll, .ocx and more.

In our service:

- Certificates issued to European companies, with a line of business in the IT sector;
- Fast delivery after payment, help with setup and using;
- Quality product, sold strictly in one hands!
- Buy via Escrow: Fast and secure!

More about EV certificates

Installation methods:

- Free installation on your physical FIPS 140-2 token (Issue time 5 - 14 days)
- It is possible to make cloud signing, it makes it possible to sign a file by using the remote access to certificate. (Issue time 3 - 14 days)
- Installation on Azure Key Vault. (Issue time 3 - 14 days)

Almost always in stock, ask in the PM of the forum or in the telegram @solphu

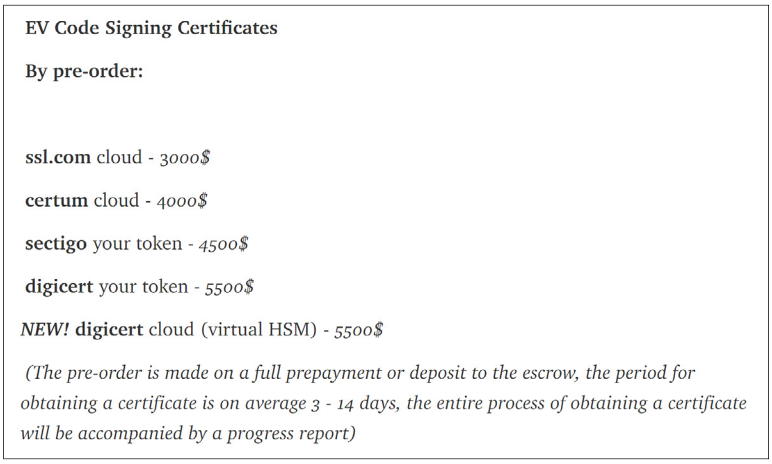
Origin countries of certificates:

- Latvia
- Lithuania
- Estonia
- UK

We can make a company according to your needs (name, type of activity in the registers, we can also buy an old company with a history)

Figure 4: Balamut Service advertisement posted on the dark market.

There is also more detailed information on Balamut Service's website. It mentions that they can issue Organization Validation (OV) and Extended Validation (EV) code-signing certificates from various public CAs. It is interesting to note that there are price differences depending on the types of certificates and the authorities. In addition to code-signing certificates, Balamut Service also provides Know Your Customer (KYC) verification services for its clients.



EV Code Signing Certificates

By pre-order:

ssl.com cloud - *3000$*

certum cloud - *4000$*

sectigo your token - *4500$*

digicert your token - *5500$*

***NEW!* digicert** cloud (virtual HSM) - *5500$*

(The pre-order is made on a full prepayment or deposit to the escrow, the period for obtaining a certificate is on average 3 - 14 days, the entire process of obtaining a certificate will be accompanied by a progress report)

Figure 5: Balamut Service price list (partial excerpt).

VERIFICATION PROCESS USING AN ONLINE FILE ANALYSIS SERVICE

We have been tracking attack campaigns using malicious MSIX files since the early days. In this process, we have continuously examined MSIX files submitted on an online file analysis service, specifically examining the certificates used by attackers. The certificate file (AppxSignature.p7x) and EXE file included in an MSIX file are code signed. In an attack campaign using MSIX files, attackers purchase certificates from the code-signing certificate sellers described in the previous section and distribute MSIX files signed with these valid certificates.

Figure 6 shows the timeline of an MSIX file that is code signed with a certain certificate. The time in the timeline indicates when the samples were uploaded to the online file analysis service. Typically, attackers rarely post malicious MSIX files to the online file analysis service, and many samples are assumed to have been submitted by the victims of attack campaigns. In other words, we can assume that the time of the submission of the samples corresponds roughly to the time when the attackers distributed the MSIX files in their attack campaigns. The timeline shows that the attackers use a single certificate to create multiple malicious MSIX files and deploy attack campaigns every few months to distribute these malicious files. Additionally, the file names cover a wide range of topics including cryptocurrency, AI devices and browser updates, indicating that the threat actors are trying to lure users into installing the MSIX files through various deceptive ways.

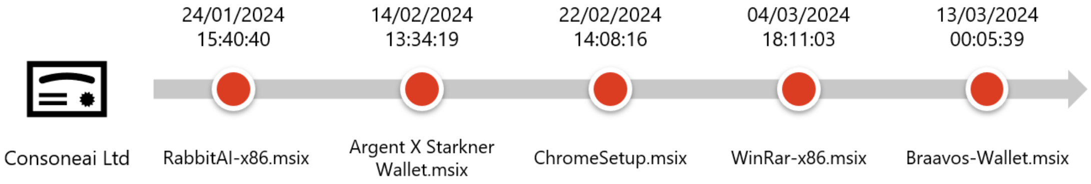


Figure 6: Timeline of signed malicious MSIX files.

We found that strange contributors had uploaded legitimate files signed with the same code-signing certificate as the malicious files. Moreover, these signed legitimate files were uploaded prior to the malicious MSIX files. The certificates used in attack campaigns with malicious MSIX files are, with a few exceptions, newly created certificates. Normally, searches for misused certificates on the online file analysis service will only return malicious MSIX files and related files contained within the packages. However, we found that, for some certificates, legitimate files were posted prior to the malicious MSIX files. Figure 7 shows the timelines of code-signed files with two certificates along with the time of their posting to the online file analysis service. The blue circles represent legitimate files signed by attackers, and the red circles represent the malicious MSIX files. As can be seen, the legitimate files were submitted before the malicious MSIX files. In this paper, we refer to a known legitimate file to which an attacker has applied their own certificate, and which was uploaded prior to a malicious MSIX file as a 'test sample'.

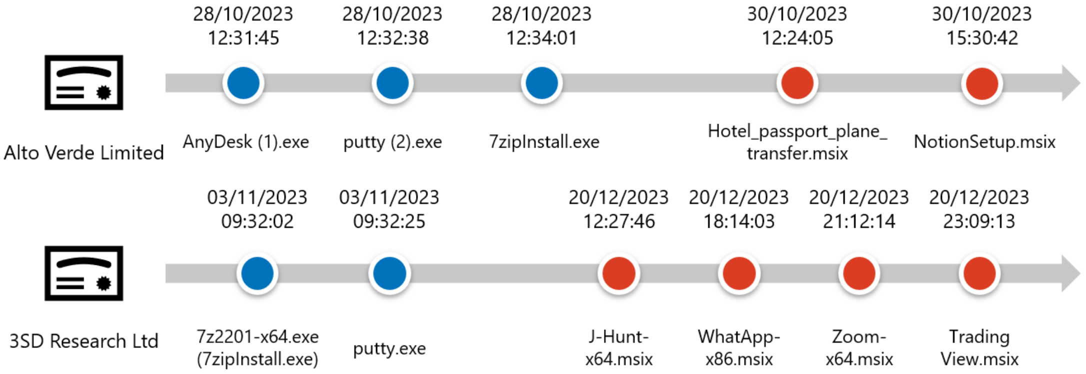


Figure 7: Test samples with code signing.

We assume that these strange samples were submitted by sellers offering certificates. We believe that the sellers upload some test samples they have created to the online file analysis service in order to verify in advance that the certificates are judged as valid and not malicious by security vendors. The fact that there have been cases of such submitters posting multiple test samples with different certificates, and that there is a time gap between submission of the test samples and submission of the malicious MSIX files, make it highly plausible that these submitters are the sellers of code-signing certificates. In addition, the time gap between submissions of signed legitimate files and malicious MSIX files range from a few days to several months. This time gap is the number of days between when a certificate seller creates a certificate and when an attacker purchases and abuses that certificate.

We examined over 300 malicious MSIX files submitted between February 2023 and March 2024 and collected 24 unique code-signing certificates. Table 2 shows, for each certificate, the earliest submission time of an MSIX file or a test sample (if any) using that certificate, and the information about the submitter who first submitted the test sample.

Signature	First MSIX submission	Test sample submitted	Test sample submission	Time from MSIX to test (days)	Time from signature to test sample (days)	Test sample submitter	Uploader country code
1	27/02/2023 22:08						
2	23/05/2023 09:09						
3	08/07/2023 20:05						
4	03/08/2023 14:34						
5	05/08/2023 07:05						
6	28/11/2023 23:06						
7	09/09/2023 07:20						
8	14/09/2023 08:42						
9	18/09/2023 20:51						
10	11/10/2023 07:07						
11	30/10/2023 12:24	✓	28/10/2023 21:31	1.6	23.5	A	CA
12	31/10/2023 05:52	✓	21/8/2023 16:55	70.5	52.1	B	IT
13	08/11/2023 17:31						
14	04/12/2023 11:18	✓	29/10/2023 2:59	36.4	23.6	A	CA
15	08/12/2023 16:22						
16	14/12/2023 20:34						
17	20/12/2023 12:27	✓	3/11/2023 18:32	46.8	0.5	C	NL
18	30/12/2023 22:10	✓	1/11/2023 20:26	59.1	1.1	D	NL
19	09/01/2024 22:40						
20	11/01/2024 19:27	✓	22/12/2023 0:00	20.8	7.3	E	GB
21	17/01/2024 15:14						
22	24/01/2024 15:40	✓	21/12/2023 23:59	33.7	7.1	E	GB
23	01/03/2024 22:12						
24	17/03/2024 16:10						

Table 2: List of abused certificates (February 2023 – March 2024).

More than half of the collected certificates had no test samples, and most of the files with earliest submission time were MSIX files or related samples. For some certificates, other signed malicious files other than MSIX were posted before malicious MSIX files were posted. It is possible that the certificates used in other attacks were diverted to the attack campaign using MSIX files. On the other hand, for certificates for which test samples were uploaded, the time gap between the submission of the test samples and the MSIX files ranged roughly from a few days to several months. We also confirmed the cases where the submitters who posted the test samples for multiple certificates were the same. This means that these submitters have control over multiple certificates, which lends weight to the theory that they are sellers offering code-signing certificates. We have not identified any cases of these submitters submitting MSIX files, which implies that there is a clear separation of roles between certificate sellers and attackers who distribute MSIX files.

FUTURE PREDICTION APPROACH LEVERAGING CERTIFICATE VALIDATION PROCESSES

This section describes a new approach to future prediction that utilizes certificates.

Through our investigations of the certificates applied to a number of MSIX files, we have uncovered the existence of submitters who uploaded test samples. In some of these cases, we identified that multiple test samples were uploaded by the same submitter. Figure 8 shows timelines of the test samples submitted by 'Submitter A' and 'Submitter E' in Table 2.

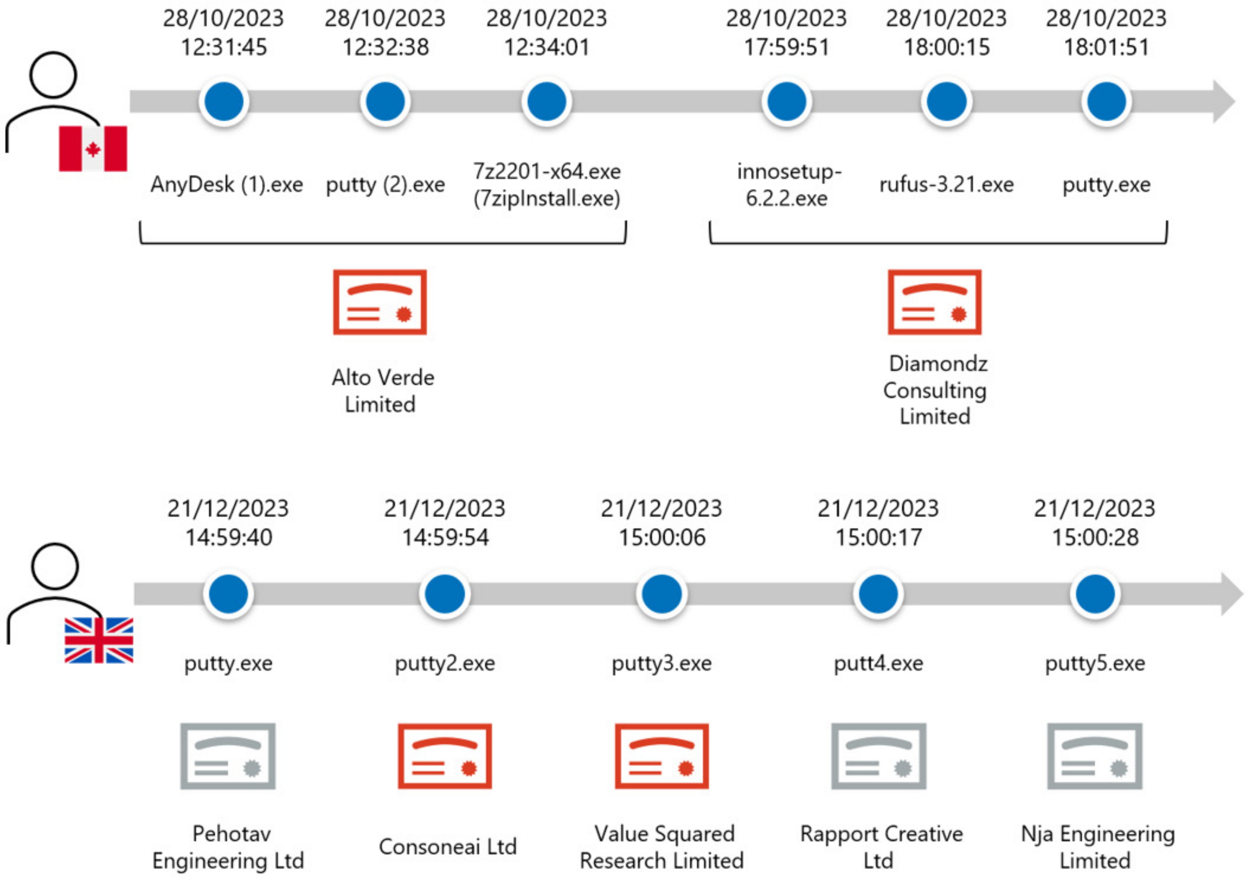


Figure 8: Submitters posting multiple test samples.

Submitter A posted multiple code-signed legitimate files using two different certificates. Submitter E submitted some test samples with several different certificates, including abused certificates, applied to a legitimate *Putty* file. Furthermore, the test samples were submitted consecutively over a short period of time, the certificate expiration times are close, and the file names are similar. All of these facts strongly support the theory that Submitter A and Submitter E are the sellers providing the code-signing certificates used in the attack campaign. The three grey certificates had not been used in attack campaign abusing MSIX files up to March 2024. However, it is highly possible that these certificates could be exploited in future attack campaigns. Therefore, we have speculated that it may be possible to predict in advance which certificates will be abused.

Our approach is an attempt to leverage test samples to predict which certificates are likely to be abused in the future. We focus on the submitters who first uploaded the test samples and investigate the files submitted by them later. During this investigation process, if we can find a sample with an unknown certificate for a known legitimate file, it means that this certificate is likely to be abused.

However, it would be difficult to investigate all the posted samples to see if they were posted by known attackers. Fortunately, as far as we have investigated, the type of legitimate files used in certificate validations are limited, and the same legitimate files are often used repeatedly. Therefore, we can implement our approach by limiting the number of target files by file names and similarity hashing to a practically available number of samples.

To evaluate the effectiveness of our approach, we performed additional research on the malicious MSIX files posted in April 2024 to verify whether we could predict which certificates would be exploited. The additional investigation confirmed that 10 new code-signing certificates were abused, as shown in Table 3.

Signature	First MSIX submission	Test sample submitted	Test sample submission	Time from MSIX to test (days)	Time from signature to test sample (days)	Test sample uploader	Uploader country code
25	03/04/2024 18:42	✓	01/30/2024 23:19	63.8	4.2	F	US
26	12/04/2024 13:30	✓	22/12/2023 00:00	112.6	1.3	E	GB
27	16/04/2024 17:41	✓	22/12/2023 00:00	116.7	1.3	E	GB
28	18/04/2024 18:35						
29	19/04/2024 20:54	✓	09/19/2023 19:31	213.1	6.6	G	RU
30	22/04/2024 20:54						
31	23/04/2024 15:16						
32	24/04/2024 12:55	✓	21/12/2023 23:59	124.5	1.2	E	GB
33	24/04/2024 19:32	✓	05/02/2024 22:05	78.9	10.5	D	NL
34	27/04/2024 07:59						

Table 3: List of abused certificates (April 2024).

Regarding the newly discovered code-signing certificates, there were six certificates for which test samples existed, four of which were submitted by previously known submitters. This implies that the abuse of these certificates is predictable using our approach. In fact, regarding the certificates used by Submitter E, the three previously unused certificates are now included in the list of newly abused certificates (certificates 26, 27 and 32 in Table 3).

In addition, focusing on the gap in posting times between the test samples and the MSIX files, we see that they tend to be greater than those of the certificates used before March. This suggests that code-signing certificate sellers are selling attackers certificates that they have created and stored in large numbers in advance, rather than creating certificates upon receipt of orders. This is likely because the process of issuing a valid certificate takes several days to several weeks – as shown in the certificate price list in Figure 5 – so they must prepare the certificates in advance. The larger the time gap between the creation of a valid certificate by a seller and the distribution of malicious MSIX files, the more likely our future prediction approach will be effective in preparing defences against attacks. In other words, if our approach can find a suspicious certificate before malicious MSIX files are distributed, we can report the fact to the certificate authority and ask them to revoke the certificates obtained fraudulently. If the certificate has been revoked, when the victim launches the malicious MSIX file the certificate verification will fail, and the file will not be executed. Furthermore, if the certificate sellers create certificates before selling them, we could even invalidate these certificates before attackers purchase them from the sellers.

We have continuously investigated new malicious MSIX files created daily and kept up with the attack campaigns. Our predictive approach helps to anticipate attackers' actions and prevent damage by disrupting and breaking attack chains.

CHARACTERISTICS OF ISSUED CERTIFICATES

We collected and analysed over 300 malicious MSIX files and were able to obtain 34 unique signer names.

CA	Subject country code	Total
Certum	EE	1
DigiCert	CA	1
GlobalSign	GB	1
	PL	4
	RU	2
Sectigo	CN	1
	GB	2
SSL.com	CN	2
	GB	18
	PL	1
	SE	1
Total		34

Table 4: Exploited CA list.

We investigated these signer names and the certificate authorities that issued the certificates and found that there was a total of five CAs, of which *SSL.com* was by far the most common. The country code listed in the subject of the certificate issued by SSL.com was Great Britain (GB), and the signer name was a company registered with Companies House [13]. From the malware distributed and PowerShell code, malicious MSIX files with these certificates are suspected to be linked to a threat actor called Eugenfest, which sells FakeBat. Given that the subject of the certificates sold by certificate seller Balamut Service includes Great Britain, this reconfirms the connection between Eugenfest and Balamut Service.

The next most observed CA was *GlobalSign*. All the certificates issued by this CA were EV certificates. In addition, the username of the email address listed in the signer name was 'admin', and our research of the domains revealed that web servers with no content existed on a particular hosting service. This suggests that these certificates may have been obtained by the same person. The certificates with 34 unique signer names have the following points in common:

- The certificate is valid for one year.
- The signer is a real name registered with a public agency such as Companies House.
- The signer is a Private Limited Company and has been incorporated for at least three years.

PROCEDURES FOR CERTIFICATES ISSUANCE AND POTENTIAL TACTICS

How do code-signing certificate sellers obtain certificates? We will consider this based on the certificates issued by SSL.com, the most commonly observed CA.

First, we discuss the possibility of certificate theft. As noted in the previous section, the certificates have many similarities. We believe that if the certificates had been stolen, many of these similarities would not exist. Moreover, some of the organizations listed as the signer have their own websites, and their certificates were issued from different CAs. Based on this, it is unlikely that the certificates were stolen.

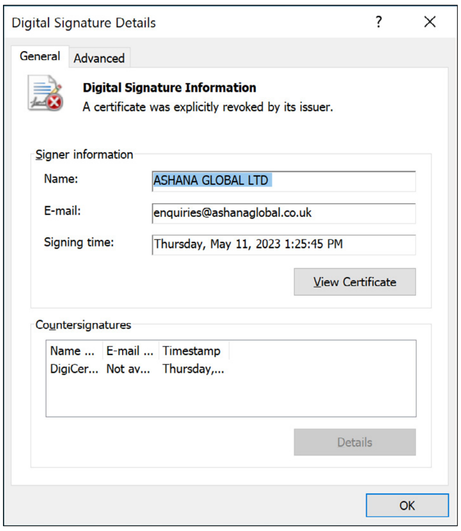
Next, we consider the possibility of a certificate seller establishing a bogus company to obtain a certificate. The companies registered with Companies House have been incorporated for more than three years and all have different incorporation dates. As noted above, some organizations are engaged in business activities. Considering the time and effort required for a seller to incorporate a bogus company from scratch and apply to *SSL.com* for the issuance of a certificate, this seems very unlikely.

Finally, we consider the possibility that a certificate seller impersonates a legitimate company to obtain certificates. Based on the signer information and certificate policy requirements, these abused certificates appear to be OV certificates. *SSL.com*'s validation requirements for OV certificates [14] require a link to publicly certify one's own organization. All organizations listed in the signer field we observed are registered with Companies House, so they meet this requirement. In addition, if the company has been incorporated for less than three years, an applicant's government-issued ID is also required, but the signers we observed do not have this requirement. Although phone authentication is required for identity verification, SMS authentication is also approved. In conclusion, we believe that it is highly probable that the abused certificates were obtained by a certificate seller impersonating a legitimate company.

REVOCATION OF CERTIFICATES TO PREVENT ABUSE

Regarding the code certificates that we confirmed to have been misused through our investigation, we share the related information with the CAs that issued them, and encourage revoking these certificates. When a certificate is revoked, the information of the revoked certificate is listed in and shared by the Certificate Revocation List (CRL). When a user handles a file signed by a certificate that has already been revoked, the user is notified that the certificate has been invalidated.

For example, when we check the properties of an MSIX file signed with a revoked certificate in *Windows Explorer*, we can see that the certificate has been revoked, as shown in Figure 9.



Digital Signature Information
A certificate was explicitly revoked by its issuer.

Signer information

Name: ASHANA GLOBAL LTD

E-mail: enquiries@ashanaglobal.co.uk

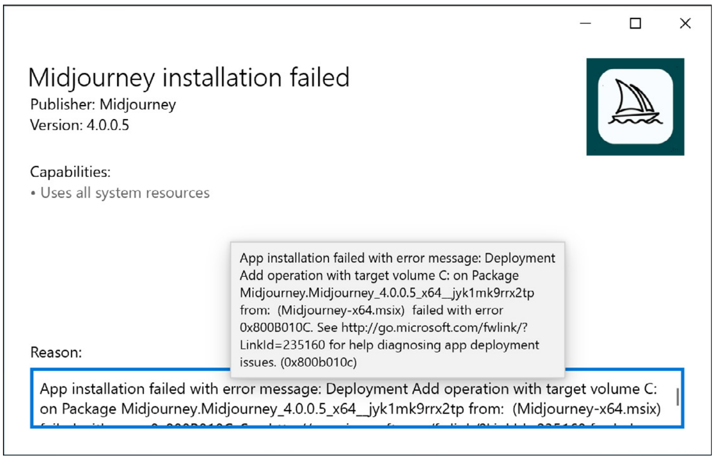
Signing time: Thursday, May 11, 2023 1:25:45 PM

Countersignatures

Name ...	E-mail ...	Timestamp
DigiCer...	Not av...	Thursday,...

Figure 9: Properties of a revoked certificate in Windows Explorer.

If the certificate has been revoked, the installation of an MSIX file cannot proceed, although there is a difference in the message displayed in *Windows* 10 and 11. In the case of *Windows 10*, the error message contains an error code of '0x800B010C', which indicates that the certificate has been revoked [15]. Therefore, the revocation of such abused certificates has certain effects in order to prevent the execution of signed malicious files.



Midjourney installation failed

Publisher: Midjourney

Version: 4.0.0.5

Capabilities:

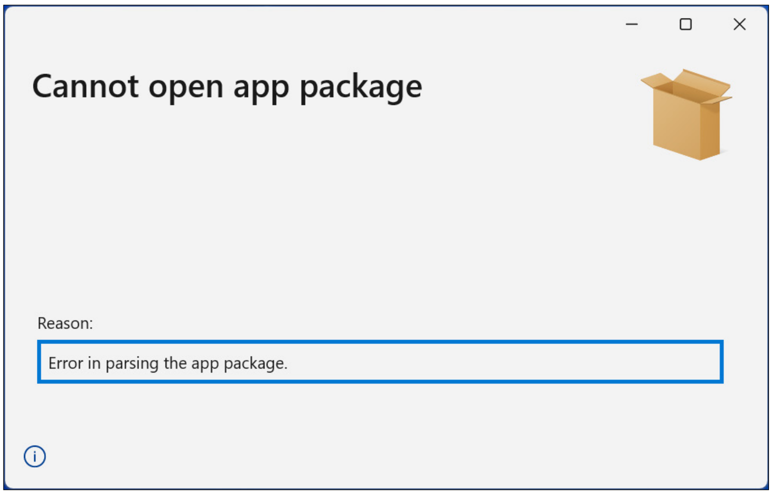
• Uses all system resources

Reason:

App installation failed with error message: Deployment Add operation with target volume C: on Package Midjourney.Midjourney_4.0.0.5_x64__jyk1mk9rrx2tp from: (Midjourney-x64.msix) failed with error 0x800B010C. See http://go.microsoft.com/fwlink/?LinkId=235160 for help diagnosing app deployment issues. (0x800b010c)

App installation failed with error message: Deployment Add operation with target volume C: on Package Midjourney.Midjourney_4.0.0.5_x64__jyk1mk9rrx2tp from: (Midjourney-x64.msix)

Figure 10: Opening an MSIX file with a revoked certificate in Windows 10.



Cannot open app package

Reason:

Error in parsing the app package.

Figure 11: Opening an MSIX file with a revoked certificate in Windows 11.

CONCLUSION

In this paper, we focused on the sellers behind the abuse of code-signing certificates used in malware and malicious files and proposed a method to predict future abuse cases by leveraging their habitual work.

Our approach has successfully predicted code-signing certificates that will be exploited in the coming months and has shown to be an effective method for the defence of entities. Sometimes, it can be beneficial for defence to focus on the habitual behaviour of threat actors and their associates.

We expect to encounter more and more code-signed malware and malicious files in the future. It is important to take a proactive approach to defeat these threats.

REFERENCES

[1] MITRE. Subvert Trust Controls: Code Signing. https://attack.mitre.org/techniques/T1553/002/.

[2] Raiu, C. Stuxnet signed certificates frequently asked questions. Securelist. 21 July 2010. https://securelist.com/stuxnet-signed-certificates-frequently-asked-questions/29725/.

[3] Arntz, P. Stolen Nvidia certificates used to sign malware—here's what to do. ThreatDown. 14 March 2022. https://www.threatdown.com/blog/stolen-nvidia-certificates-used-to-sign-malware-heres-what-to-do/.

[4] Kimura, H. Where is the Origin?: QAKBOT Uses Valid Code Signing. Trend Micro. 27 October 2022. https://www.trendmicro.com/en_us/research/22/j/where-is-the-origin-qakbot-uses-valid-code-signing-.html.

[5] Kim, D.; Kwon, B. J.; Dumitraş, T. Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI. CCS 2017. https://dl.acm.org/doi/10.1145/3133956.3133958.

[6] Kozák, K.; Kim, D.; Kwon, B. J.; Dumitraş, T. Issued for Abuse: Measuring the Underground Trade in Code Signing Certificates. WEIS 2018. https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/06/WEIS_2018_paper_14.pdf.

[7] Microsoft. Financially motivated threat actors misusing App Installer. 28 December 2023. https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/.

[8] Lambert, T.; Bohlmann, T.; Johns, C.; Lee, F. MSIX installer malware delivery on the rise across multiple campaigns. Red Canary. 12 January 2024. https://redcanary.com/blog/threat-intelligence/msix-installers/.

[9] Microsoft. Sign a Windows 10 app package. https://learn.microsoft.com/en-us/windows/msix/package/signing-package-overview.

[10] Segura, J. FakeBat campaign continues, now also targeting VMware users. ThreatDown. 17 April 2024. https://www.threatdown.com/blog/fakebat-campaign-continues-now-also-targeting-vmware-users/.

[11] eSentire. Unraveling BatLoader and FakeBat. https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/eSentire-Unraveling_BatLoader_and_FakeBat.pdf.

[12] Suh, H. W3 May | EN | Story of the week: Code Signing Certificate on the Darkweb. S2W. 17 May 2021. https://medium.com/s2wblog/w3-may-en-story-of-the-week-code-signing-certificate-on-the-darkweb-94c7ec437001.

[13] GOV.UK. Companies House. https://www.gov.uk/government/organisations/companies-house.

[14] SSL.com. What Are The Requirements for SSL.com OV and IV Certificates? https://www.ssl.com/faqs/ssl-ov-validation-requirements/.

[15] Microsoft. COM Error Codes (Security and Setup). https://learn.microsoft.com/en-us/windows/win32/com/com-error-codes-4.

APPENDIX (CERTIFICATES LIST)

Signature	Signer's name	Signature valid from
1	ASHANA GLOBAL LTD	15/02/2023 00:00
2	IMPERIOUS TECHNOLOGIES LIMITED	19/05/2023 15:32
3	SOTUL SOLUTIONS LIMITED	21/03/2023 00:00
4	STECH CONSULTANCY LIMITED	03/04/2023 01:35
5	Zhuzhou ZHUOER-TECH Co., Ltd.	12/04/2023 00:00
6	LEGION LLC	30/10/2023 14:13
7	EVRIM CONSULTANCY LIMITED	30/05/2023 21:25
8	WILLOW PHOTONICS LIMITED	30/05/2023 21:24
9	Fodere Titanium Limited	18/09/2023 09:45
10	Futurity Designs Ltd	21/09/2023 07:37
11	Alto Verde Limited	05/10/2023 10:18
12	LLC HORN	30/06/2023 13:43
13	Videra Services Ltd	10/08/2023 18:18
14	Diamondz Consulting Limited	05/10/2023 13:32
15	3D Tech Syd AB	21/11/2023 08:45
16	BCF SOFTWARE Sp. z o.o.	06/12/2023 15:43
17	3SD Research Ltd	03/11/2023 05:35

Signature	Signer’s name	Signature valid from
18	DMP UTI Limited	31/10/2023 18:48
19	CERAM Sp. z o.o.	08/01/2024 13:59
20	Value Squared Research Limited	14/12/2023 17:53
21	SOFT MICK LTD	27/12/2023 13:40
22	Consoneai Ltd	14/12/2023 22:52
23	SOFTWARE BYTES LTD	22/01/2024 15:43
24	Hunan Kangcai Business Services Partnership Enterprise (Limited)	02/02/2024 15:32
25	GREEN ENTERPRISE SP Z O O	26/01/2024 17:32
26	Nja Engineering Limited	20/12/2023 17:31
27	Rapport Creative Ltd	20/12/2023 17:39
28	Signed Software	07/06/2022 00:00
29	ExpoWave Technology OÜ	13/09/2023 05:31
30	Sichuan Mingchuang Sealing Technology Co., Ltd.	12/12/2023 12:28
31	SOFTWARE SP Z O O	07/03/2024 09:41
32	Pehotav Engineering Ltd	20/12/2023 18:48
33	QRC Holdings Limited	26/01/2024 10:04
34	KENSO SOFTWARE sp. z o.o.	22/04/2024 13:20