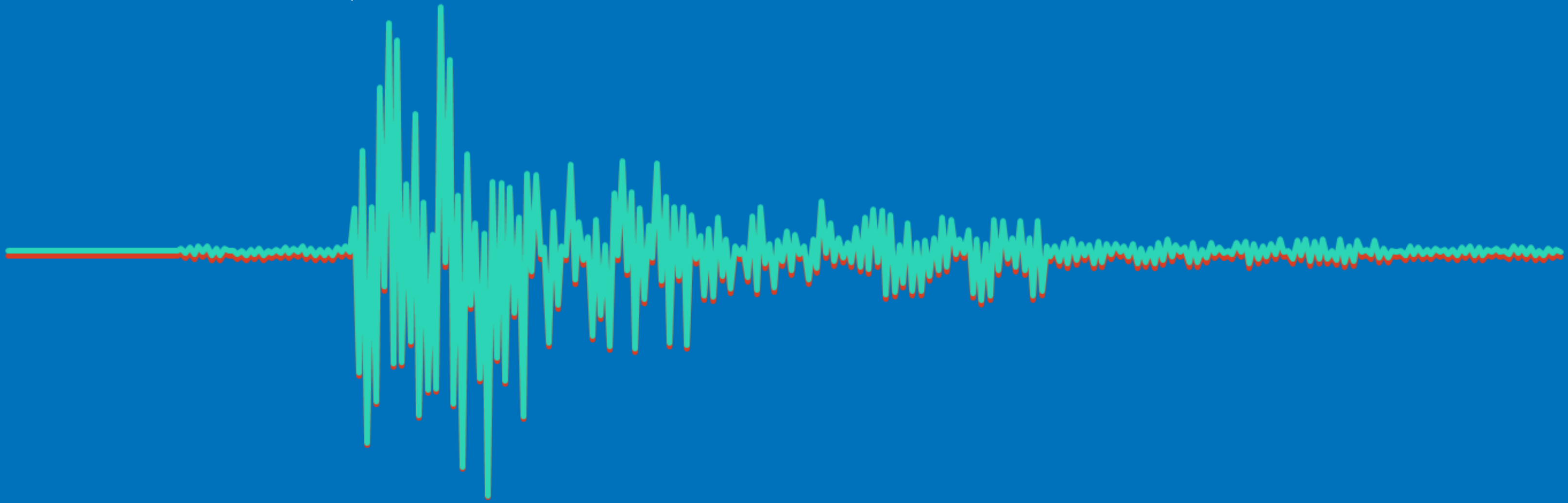
NTT Security Holdings



# P-wave of malicious code signing

Yuta Sawabe, Shogo Hayashi, Rintaro Koike

# Who am I?

Yuta Sawabe

Security Researcher @ NTT Security

Shogo Hayashi

Security Researcher @ NTT Security
EDR Log Analysis, Custom Signature Creation

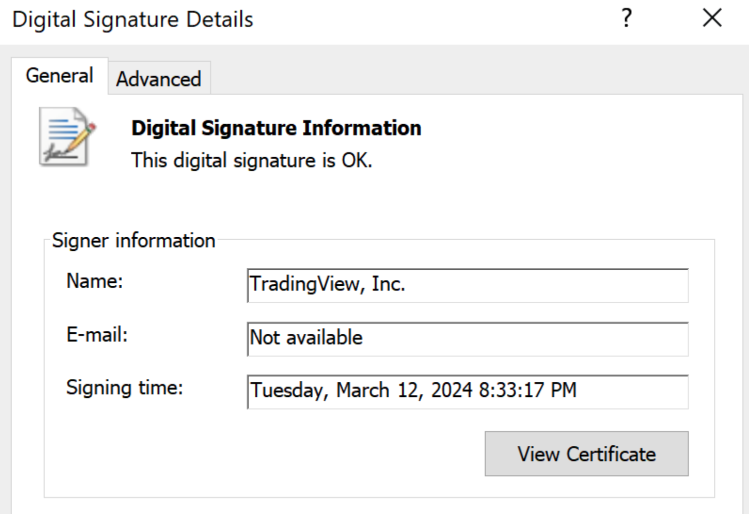
Rintaro Koike

Security Researcher @ NTT Security
Threat Research, Malware Analysis
Researcher @ nao_sec

# Code-Signing Certificate

Widely used for the following two main purposes:

- To indicate the software publisher
- To verify whether the software has been tampered with



**Digital Signature Information**

This digital signature is OK.

Signer information

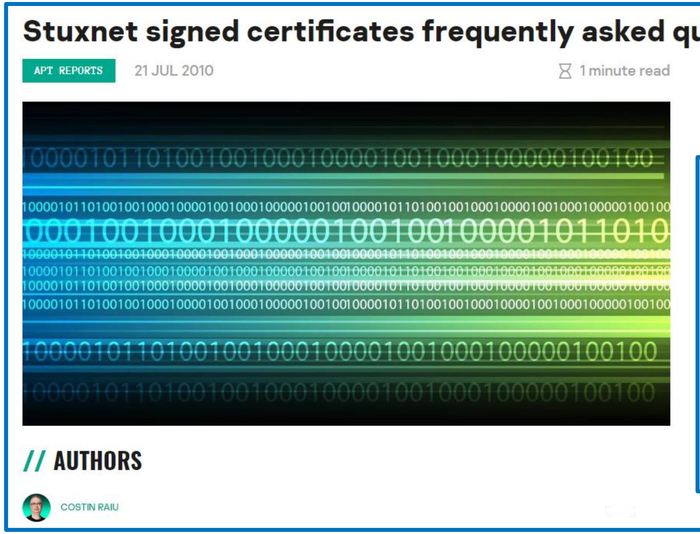
Name: TradingView, Inc.

E-mail: Not available

Signing time: Tuesday, March 12, 2024 8:33:17 PM

# Abuse of Code-Signing Certificate

It is no longer uncommon for malware or malicious files to be code-signed.



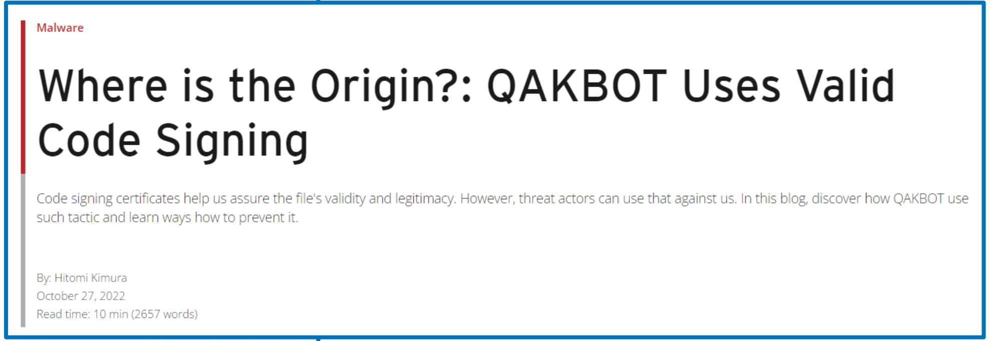
## Stuxnet signed certificates frequently asked questions

APT REPORTS 21 JUL 2010 1 minute read

GREAT WEBINARS

// AUTHORS

COSTIN RAIU



Malware

## Where is the Origin?: QAKBOT Uses Valid Code Signing

Code signing certificates help us assure the file's validity and legitimacy. However, threat actors can use that against us. In this blog, discover how QAKBOT use such tactic and learn ways how to prevent it.

By: Hitomi Kimura
October 27, 2022
Read time: 10 min (2657 words)

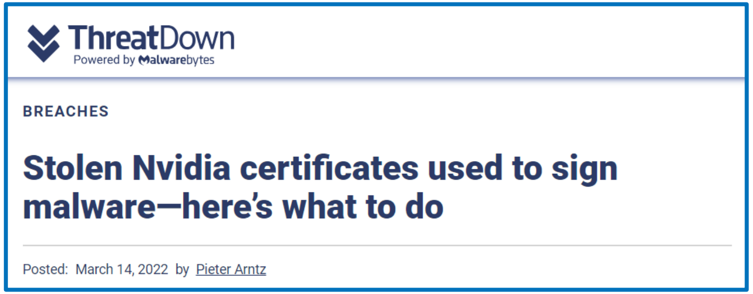
# How to Get Valid Certification

1. Stealing from organizations that already possess certificates

→ This was traditionally the most common method.

2. Purchasing certificates issued through various means

→ This method has surged in recent times.

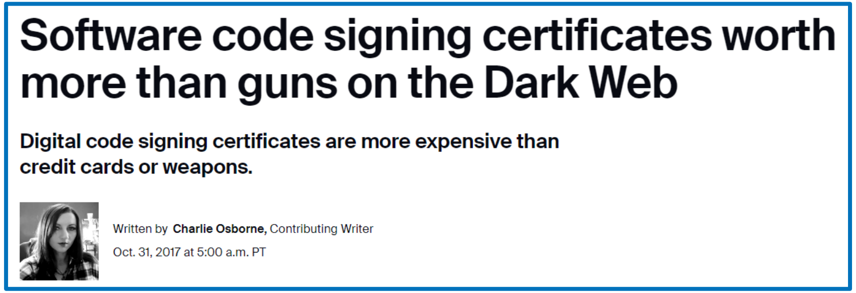


ThreatDown
Powered by Malwarebytes

BREACHES

**Stolen Nvidia certificates used to sign malware—here's what to do**

Posted: March 14, 2022 by Pieter Arntz



**Software code signing certificates worth more than guns on the Dark Web**

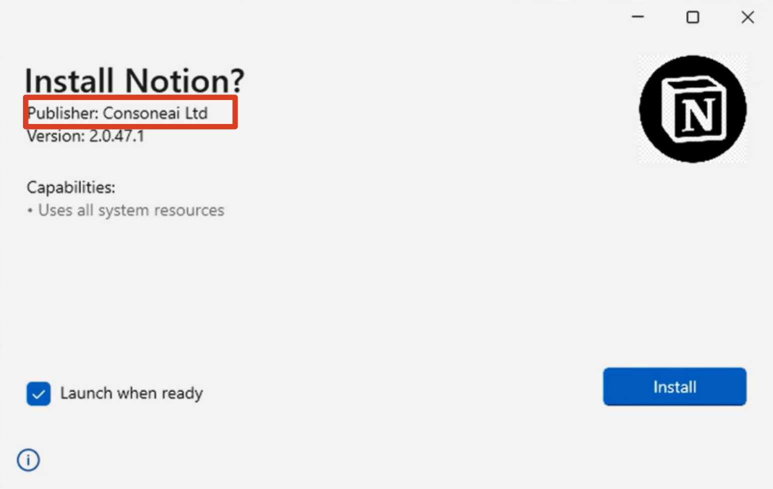
Digital code signing certificates are more expensive than credit cards or weapons.

Written by **Charlie Osborne,** Contributing Writer

Oct. 31, 2017 at 5:00 a.m. PT

# e.g., Malicious MSIX File

MSIX files must be signed with a valid code-signing certificate
→ Vendors providing MSIX files collaborate with code-signing certificates sellers



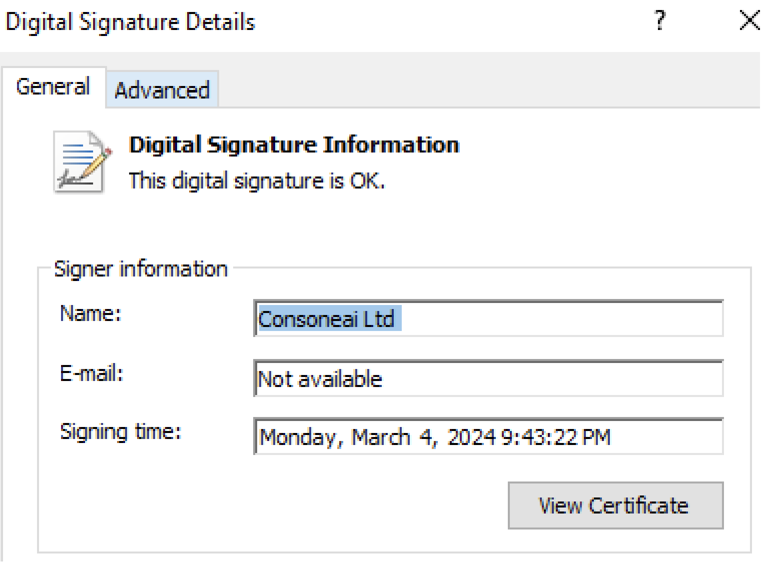
Install Notion?

Publisher: Consoneai Ltd

Version: 2.0.47.1

Capabilities:
- Uses all system resources

☑ Launch when ready



Digital Signature Details

**Digital Signature Information**

This digital signature is OK.

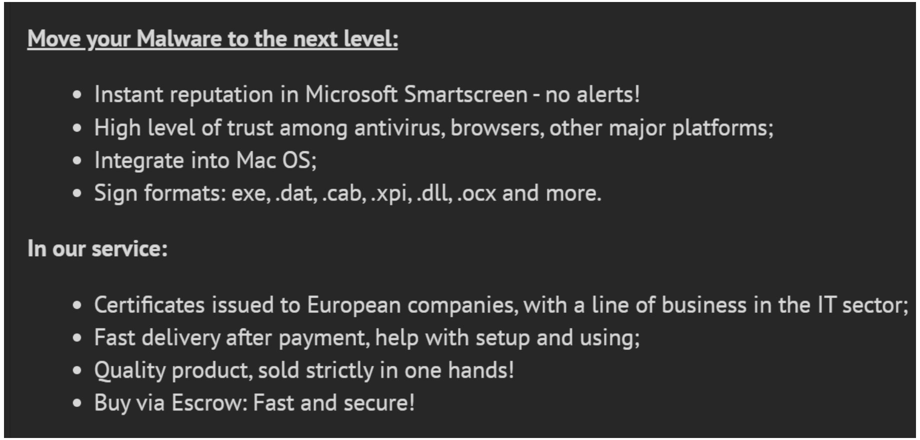
Signer information

Name: Consoneai Ltd

E-mail: Not available

Signing time: Monday, March 4, 2024 9:43:22 PM

# Code-Signing Certificate Sellers

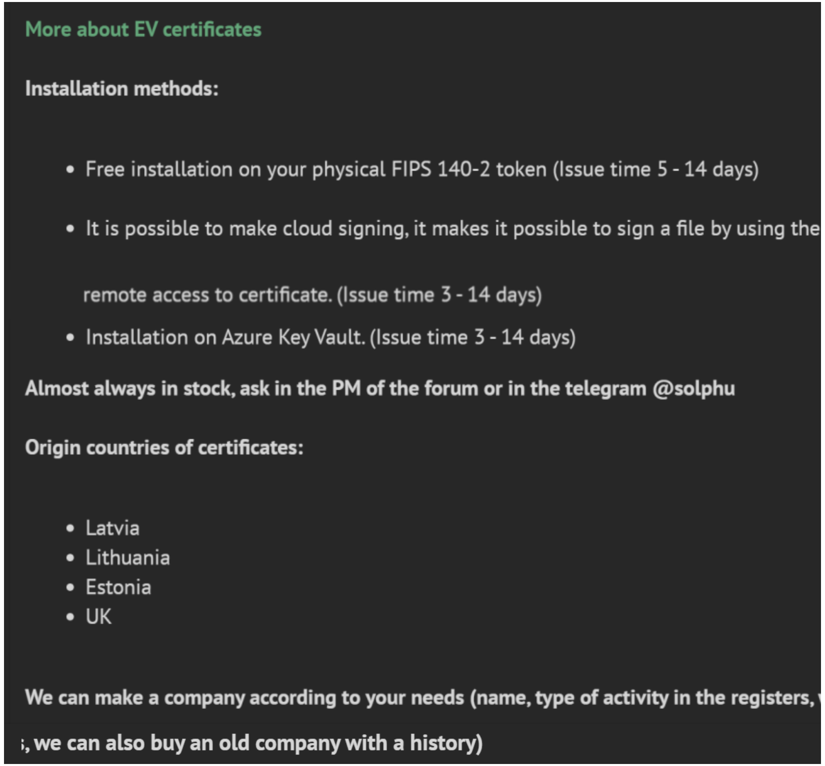


**Move your Malware to the next level:**

- 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**

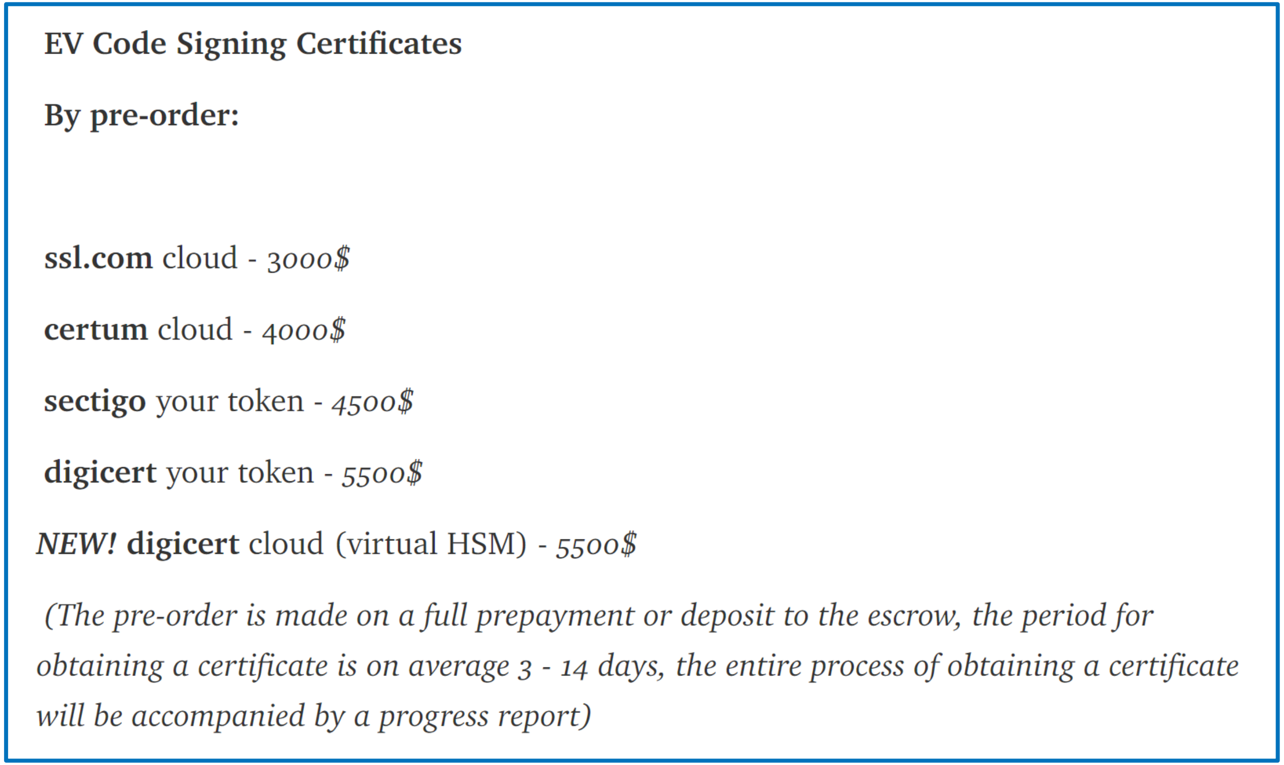
**Origin countries of certificates:**

- Latvia
- Lithuania
- Estonia
- UK

**We can make a company according to your needs (name, type of activity in the registers, v**

**, we can also buy an old company with a history)**

# Price List Example



**EV Code Signing Certificates**

**By pre-order:**

**ssl.com** cloud - *3000$*

**certum** cloud - *4000$*

**sectigo** your token - *4500$*

**digicert** your token - *5500$*

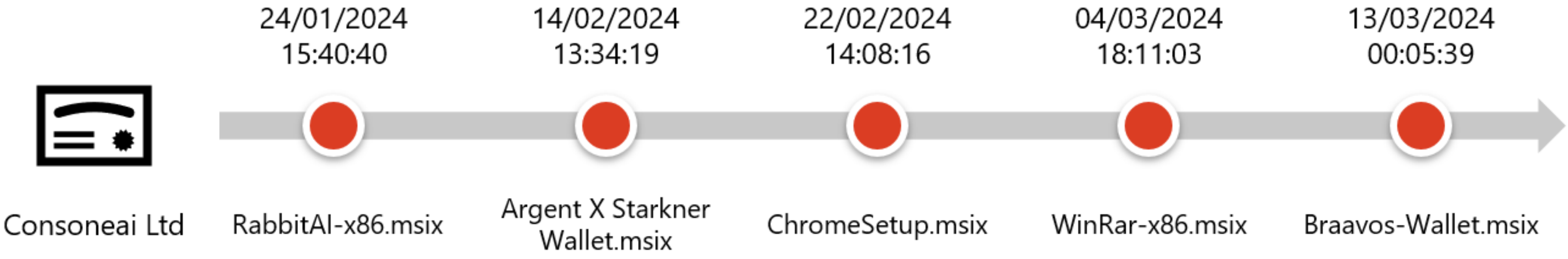
***NEW!*** **digicert** cloud (virtual HSM) - *5500$*

*(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)*

# Collecting MSIX Files

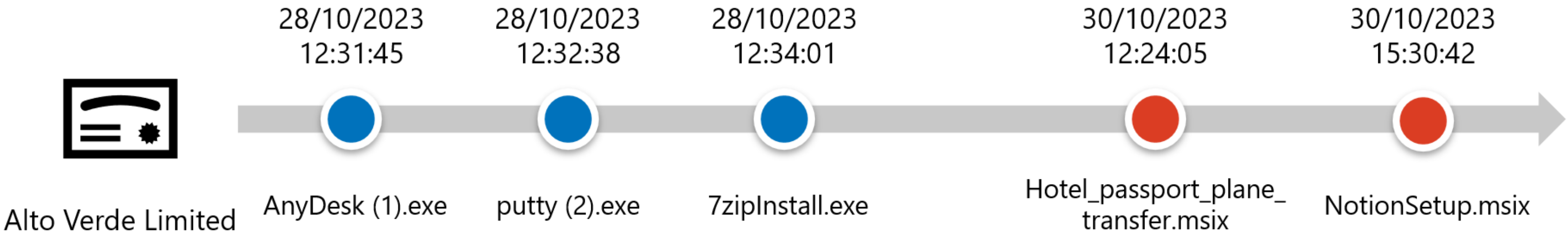
Investigated MSIX files submitted on online malware-sharing sites for over a year

A single certificate is abused for several months.



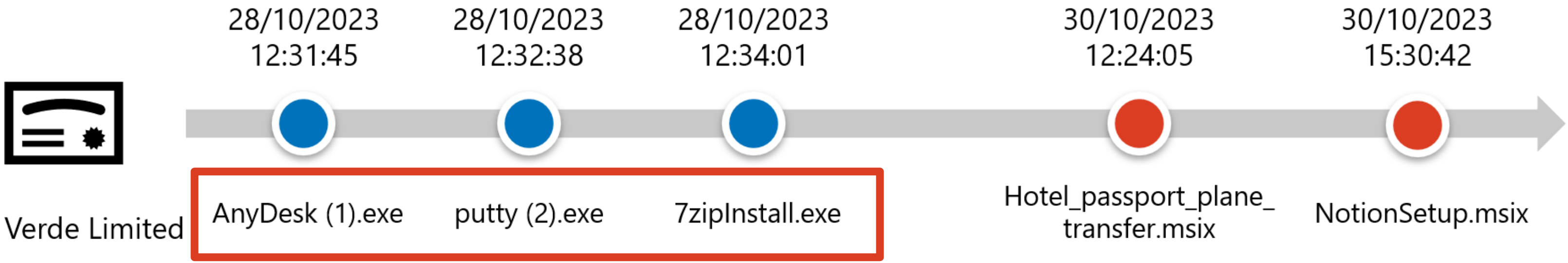
# Interesting Habit

Legitimate files (test samples) submitted before the MSIX files exist



# Interesting Habit

1. Legitimate Software files signed with a certificate



Alto Verde Limited

28/10/2023 12:31:45 AnyDesk (1).exe

28/10/2023 12:32:38 putty (2).exe

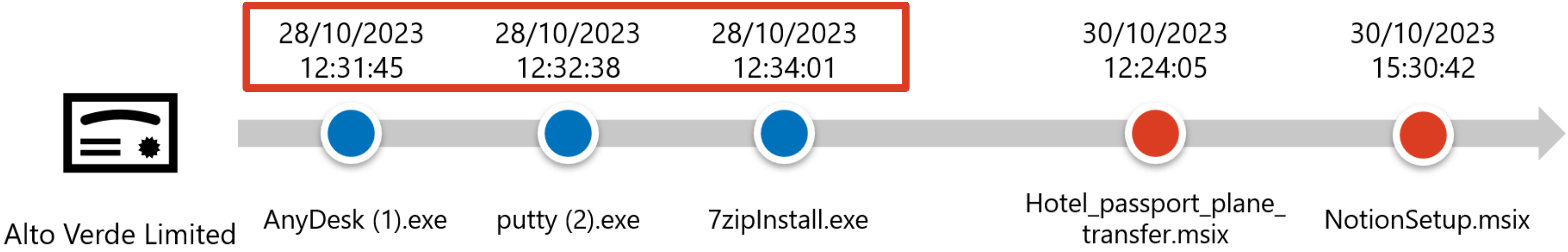
28/10/2023 12:34:01 7zipInstall.exe

30/10/2023 12:24:05 Hotel_passport_plane_transfer.msix

30/10/2023 15:30:42 NotionSetup.msix

# Interesting Habit

2. Submitted before the MSIX files



Alto Verde Limited

28/10/2023 12:31:45 AnyDesk (1).exe

28/10/2023 12:32:38 putty (2).exe

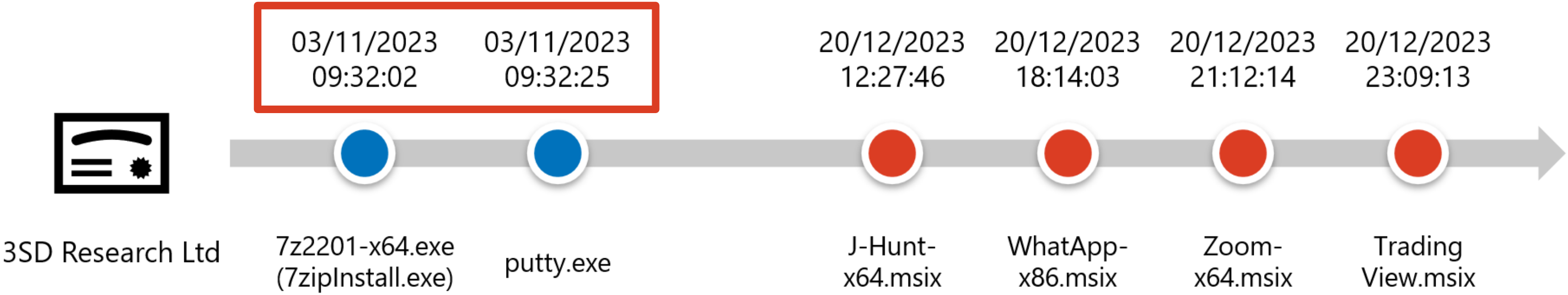
28/10/2023 12:34:01 7zipInstall.exe

30/10/2023 12:24:05 Hotel_passport_plane_transfer.msix

30/10/2023 15:30:42 NotionSetup.msix

# Interesting Habit

Sometimes submitted several months in advance



3SD Research Ltd

03/11/2023 09:32:02
7z2201-x64.exe (7zipInstall.exe)

03/11/2023 09:32:25
putty.exe

20/12/2023 12:27:46
J-Hunt-x64.msix

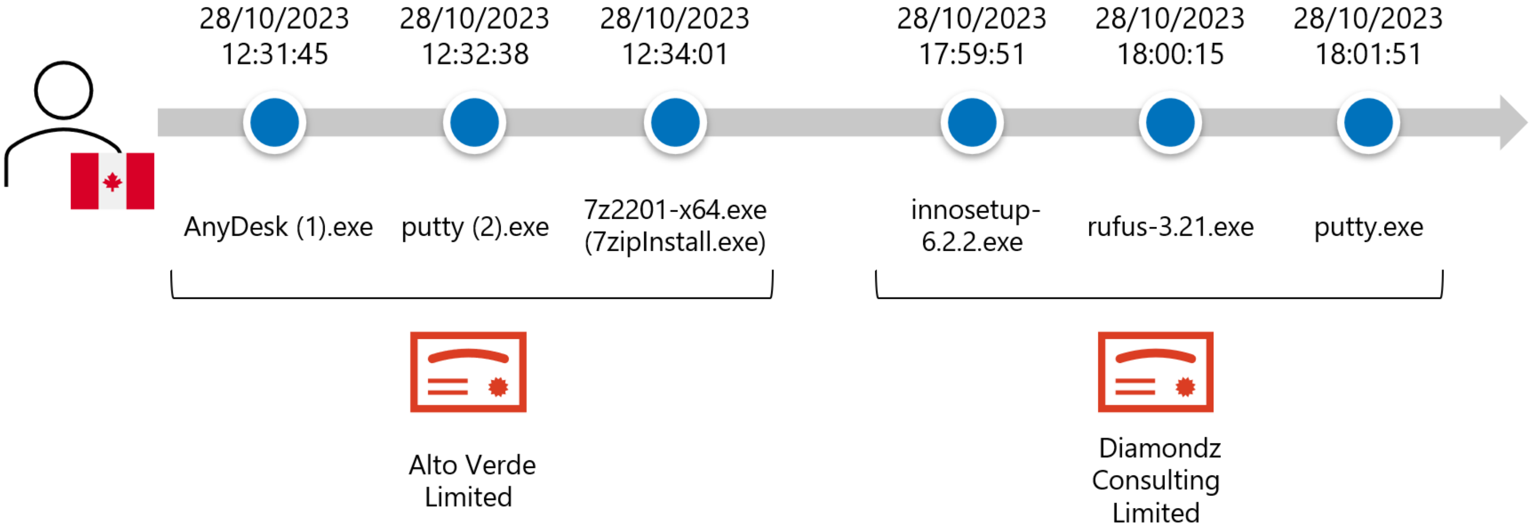
20/12/2023 18:14:03
WhatApp-x86.msix

20/12/2023 21:12:14
Zoom-x64.msix

20/12/2023 23:09:13
Trading View.msix

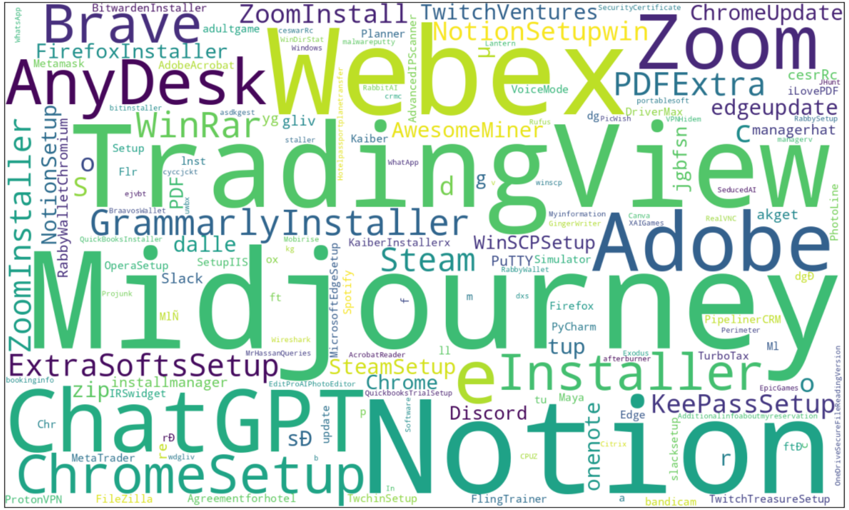
# Interesting Habit

3. The same uploader submits multiple test samples at the same time.



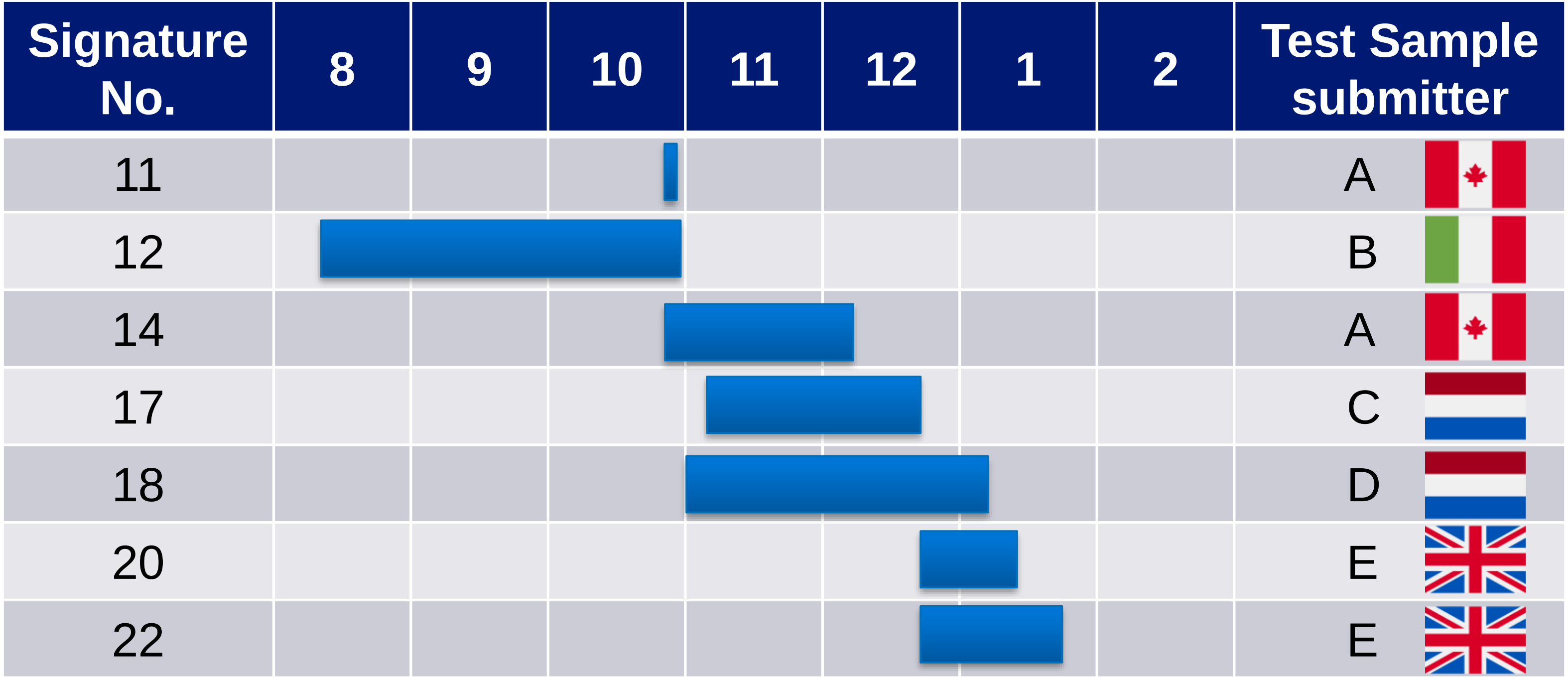
# Collecting MSIX & Test Samples

- Analyzed over 300 malicious MSIX files submitted by March 2024
- Discovered 24 certificates and 18 test samples



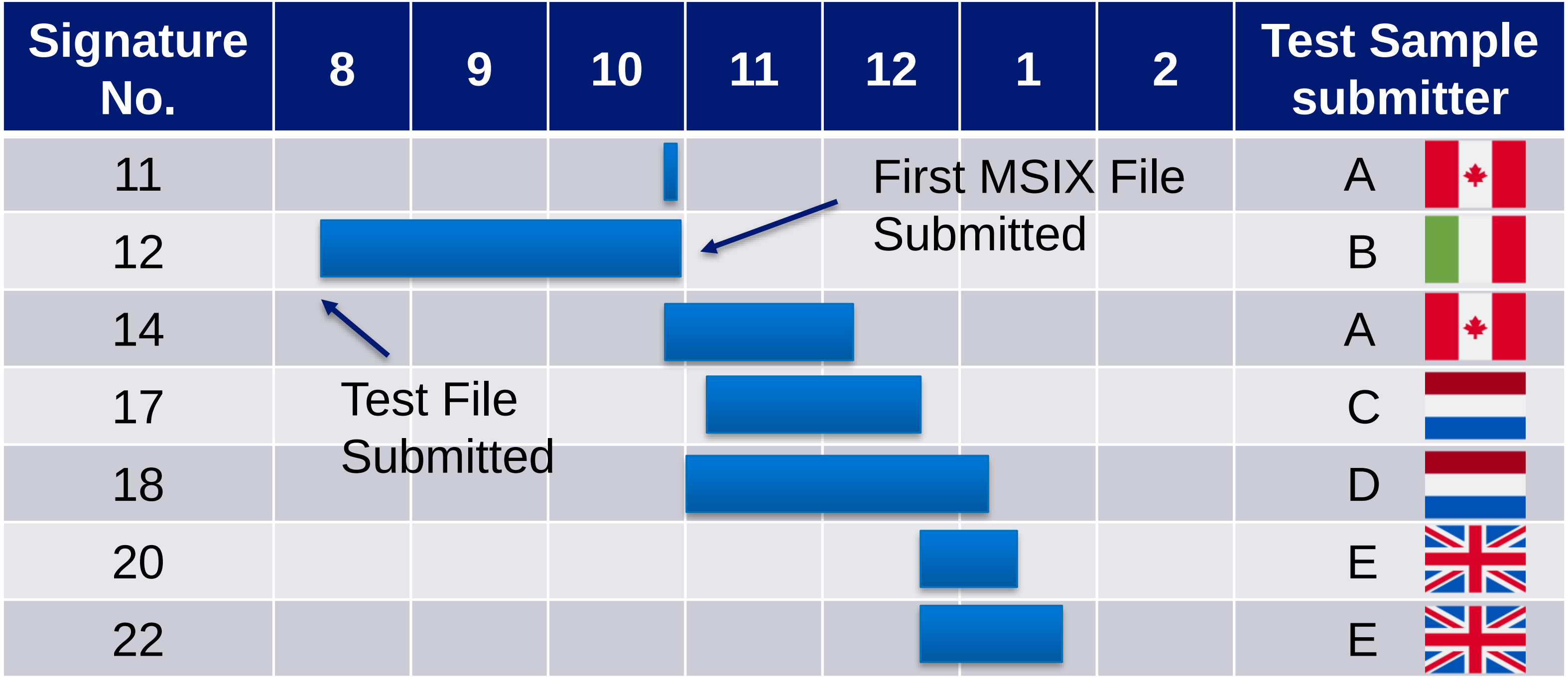
| Legitime Software | # Test Samples |
|---|---:|
| Putty | 6 |
| 7-zip | 3 |
| Rufus | 2 |
| AnyDesk | 1 |
| Inno Setup | 1 |
| Others | 5 |

# Test Samples (Until Mar 2024)



| Signature No. | 8 | 9 | 10 | 11 | 12 | 1 | 2 | Test Sample submitter |
|---|---|---|---|---|---|---|---|---|
| 11 | | | ■ | | | | | A 🇨🇦 |
| 12 | ■ | ■ | ■ | | | | | B 🇮🇹 |
| 14 | | | ■ | ■ | ■ | | | A 🇨🇦 |
| 17 | | | | ■ | ■ | | | C 🇳🇱 |
| 18 | | | | ■ | ■ | ■ | | D 🇳🇱 |
| 20 | | | | | ■ | ■ | | E 🇬🇧 |
| 22 | | | | | ■ | ■ | | E 🇬🇧 |

# Test Samples (Until Mar 2024)

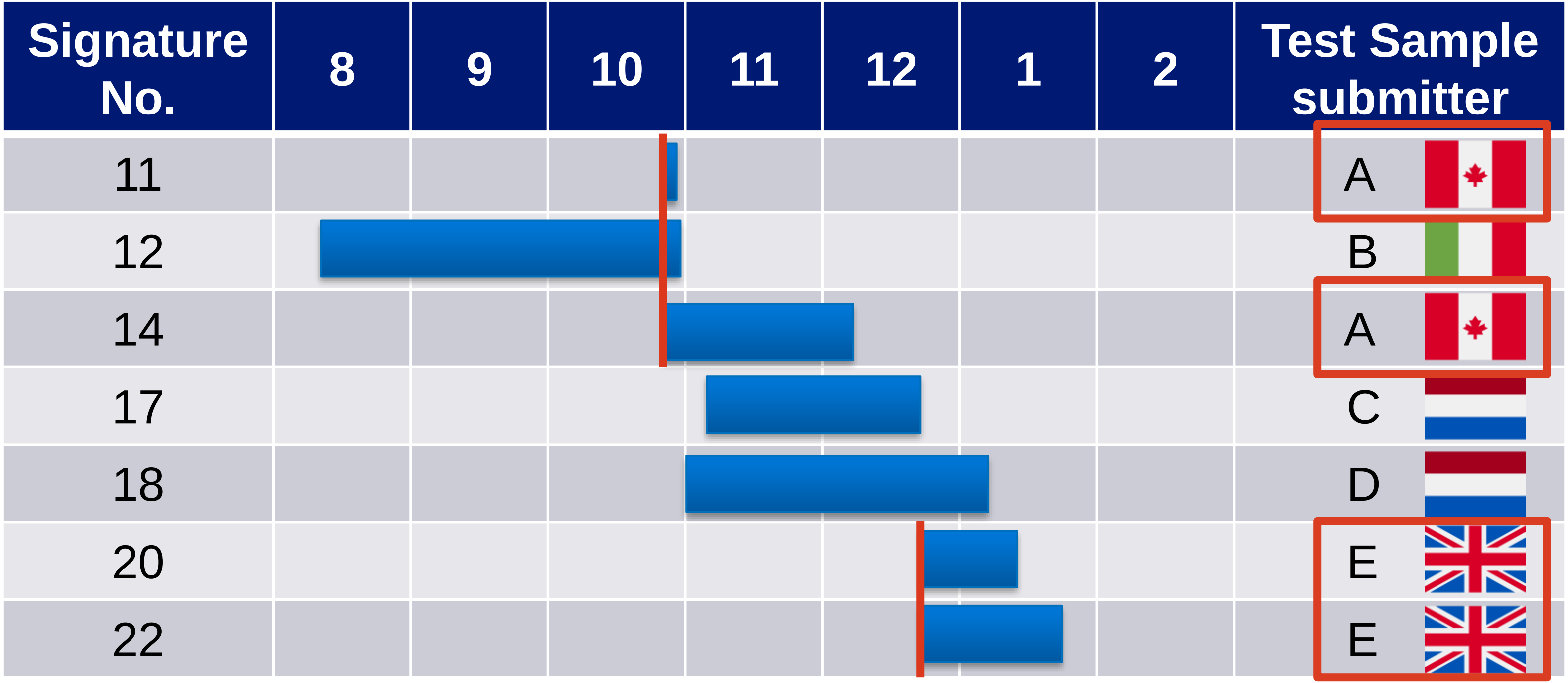


| Signature No. | 8 | 9 | 10 | 11 | 12 | 1 | 2 | Test Sample submitter |
|---|---|---|---|---|---|---|---|---|
| 11 | | | ■ | | | | | A 🇨🇦 |
| 12 | ■ | ■ | ■ | | | | | B 🇮🇹 |
| 14 | | | ■ | ■ | ■ | | | A 🇨🇦 |
| 17 | | | | ■ | ■ | | | C 🇳🇱 |
| 18 | | | | ■ | ■ | ■ | | D 🇳🇱 |
| 20 | | | | | ■ | ■ | | E 🇬🇧 |
| 22 | | | | | ■ | ■ | | E 🇬🇧 |

First MSIX File Submitted

Test File Submitted

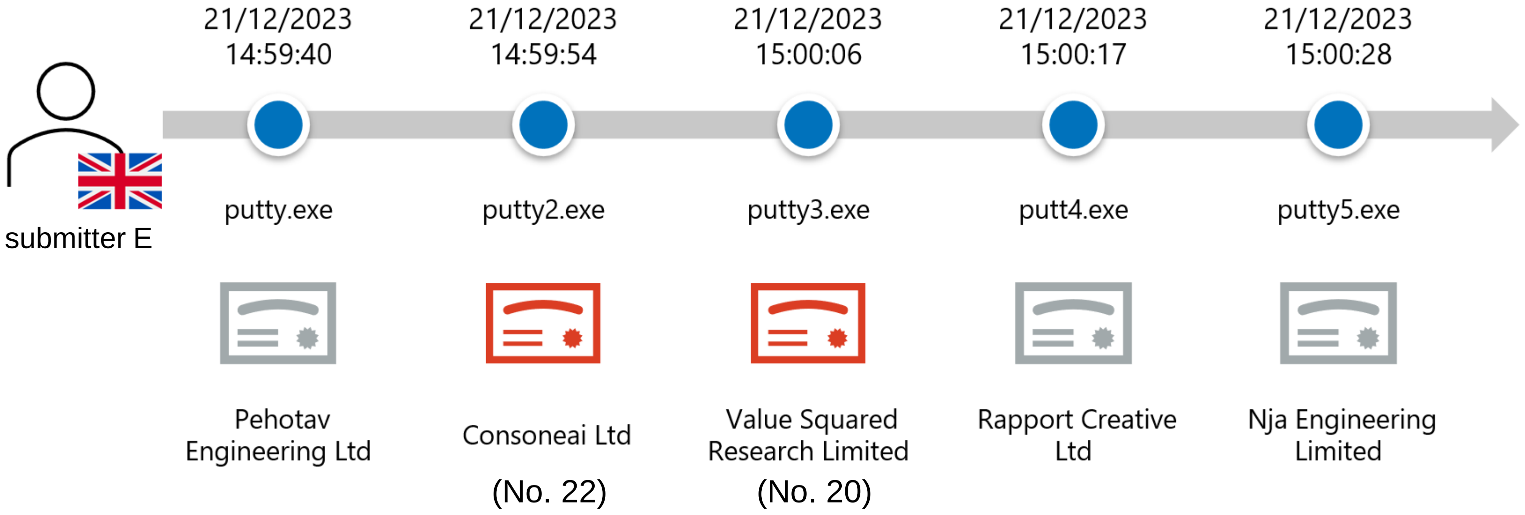
# Test Samples (Until Mar 2024)



| Signature No. | 8 | 9 | 10 | 11 | 12 | 1 | 2 | Test Sample submitter |
|---|---|---|---|---|---|---|---|---|
| 11 | | | ▇ | | | | | A 🇨🇦 |
| 12 | ▇ | ▇ | ▇ | | | | | B 🇮🇹 |
| 14 | | | ▇ | ▇ | ▇ | | | A 🇨🇦 |
| 17 | | | | ▇ | ▇ | | | C 🇳🇱 |
| 18 | | | | ▇ | ▇ | ▇ | | D 🇳🇱 |
| 20 | | | | | ▇ | ▇ | | E 🇬🇧 |
| 22 | | | | | ▇ | ▇ | | E 🇬🇧 |

# Hypothesis: Future Sight

Certificates that may be abused in the future can be identified from test samples.



submitter E

21/12/2023 14:59:40
putty.exe
Pehotav Engineering Ltd

21/12/2023 14:59:54
putty2.exe
Consoneai Ltd
(No. 22)

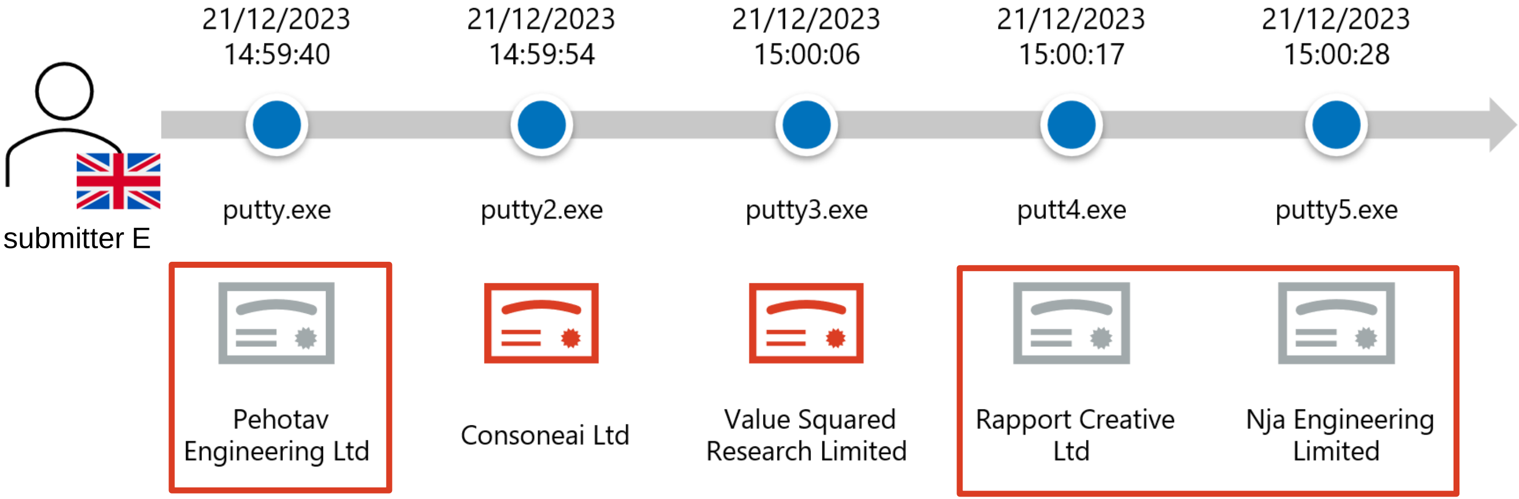
21/12/2023 15:00:06
putty3.exe
Value Squared Research Limited
(No. 20)

21/12/2023 15:00:17
putt4.exe
Rapport Creative Ltd

21/12/2023 15:00:28
putty5.exe
Nja Engineering Limited

# Hypothesis: Future Sight

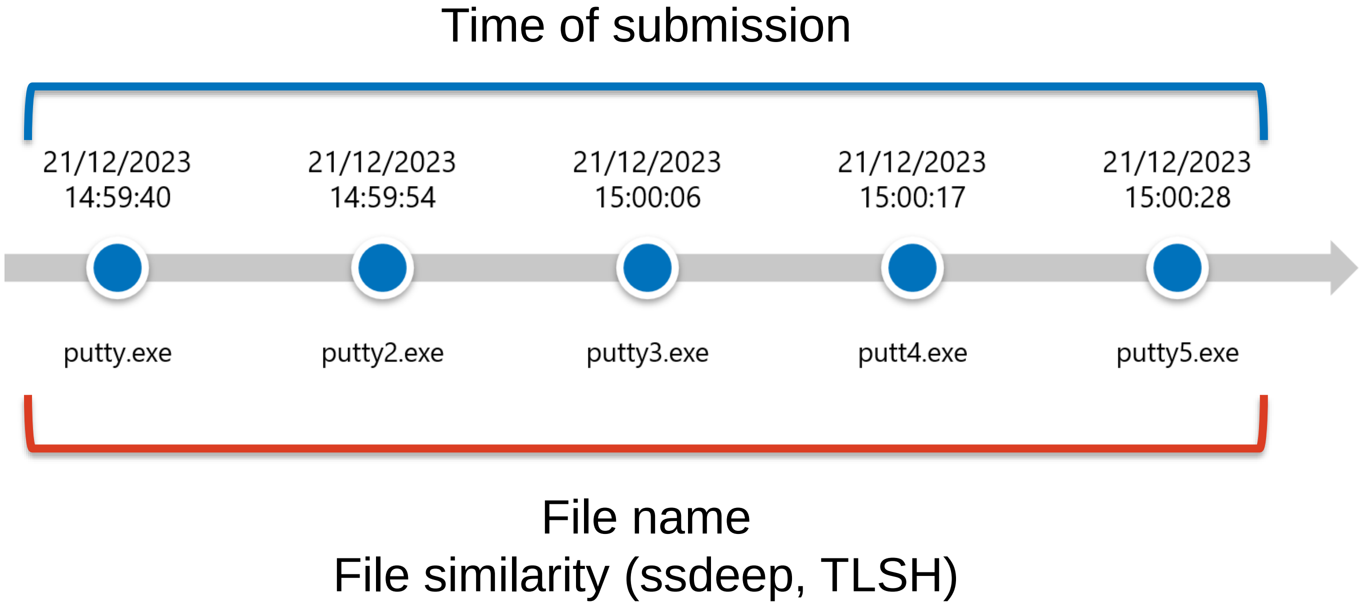
Certificates that may be abused in the future can be predicted from test samples



Expected to be exploited in future attacks

# Find Test Sample

Attackers are likely to use similar test samples



Time of submission

21/12/2023 14:59:40 putty.exe

21/12/2023 14:59:54 putty2.exe

21/12/2023 15:00:06 putty3.exe

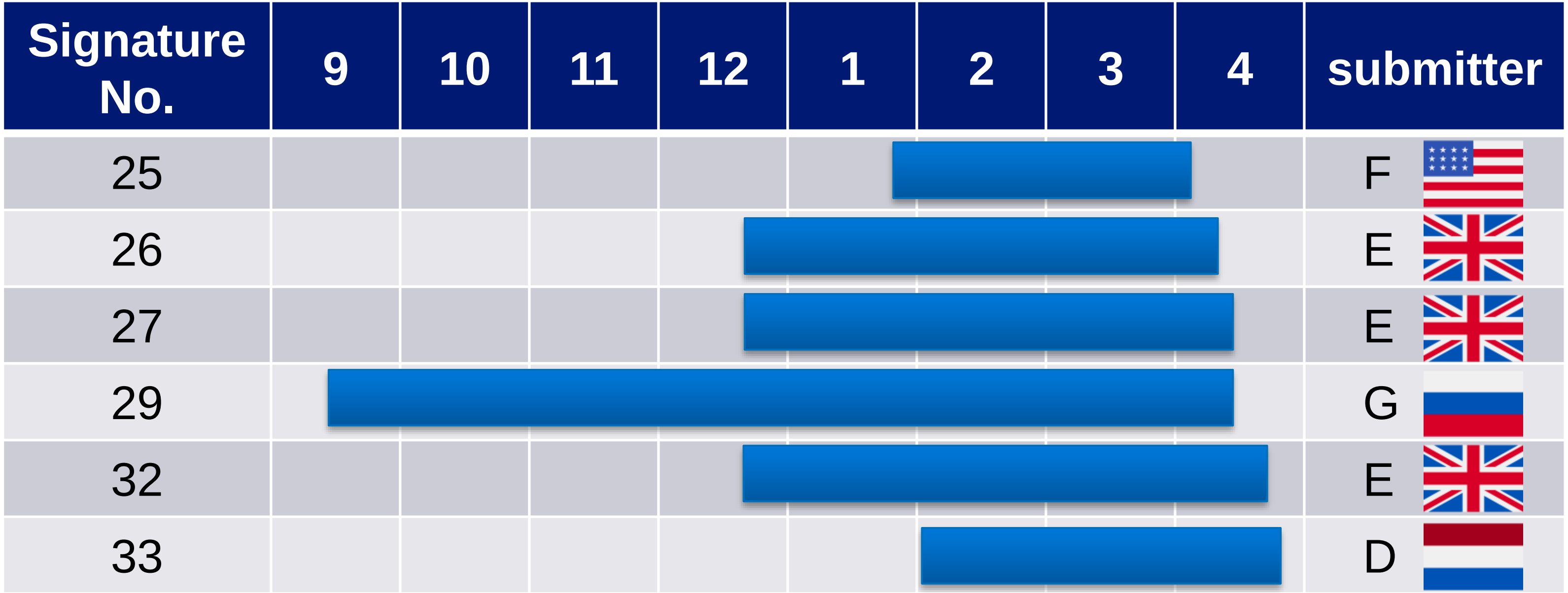
21/12/2023 15:00:17 putt4.exe

21/12/2023 15:00:28 putty5.exe

File name
File similarity (ssdeep, TLSH)

# Test Samples (Apr 2024)

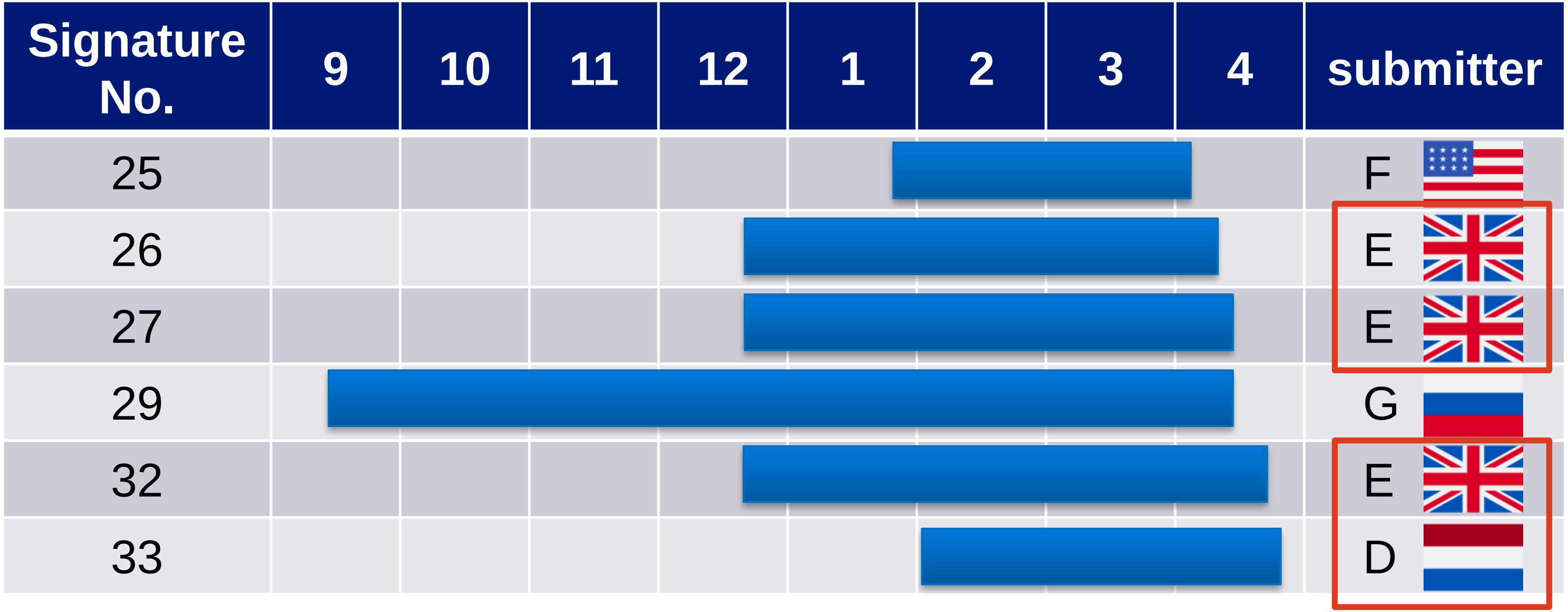
Discovered 10 new certificates in April 2024



| Signature No. | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | submitter |
|---|---|---|---|---|---|---|---|---|---|
| 25 | | | | | ■ | ■ | ■ | ■ | F 🇺🇸 |
| 26 | | | | ■ | ■ | ■ | ■ | ■ | E 🇬🇧 |
| 27 | | | | ■ | ■ | ■ | ■ | ■ | E 🇬🇧 |
| 29 | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | G 🇷🇺 |
| 32 | | | | ■ | ■ | ■ | ■ | ■ | E 🇬🇧 |
| 33 | | | | | | ■ | ■ | ■ | D 🇳🇱 |

# Test Samples (Apr 2024)

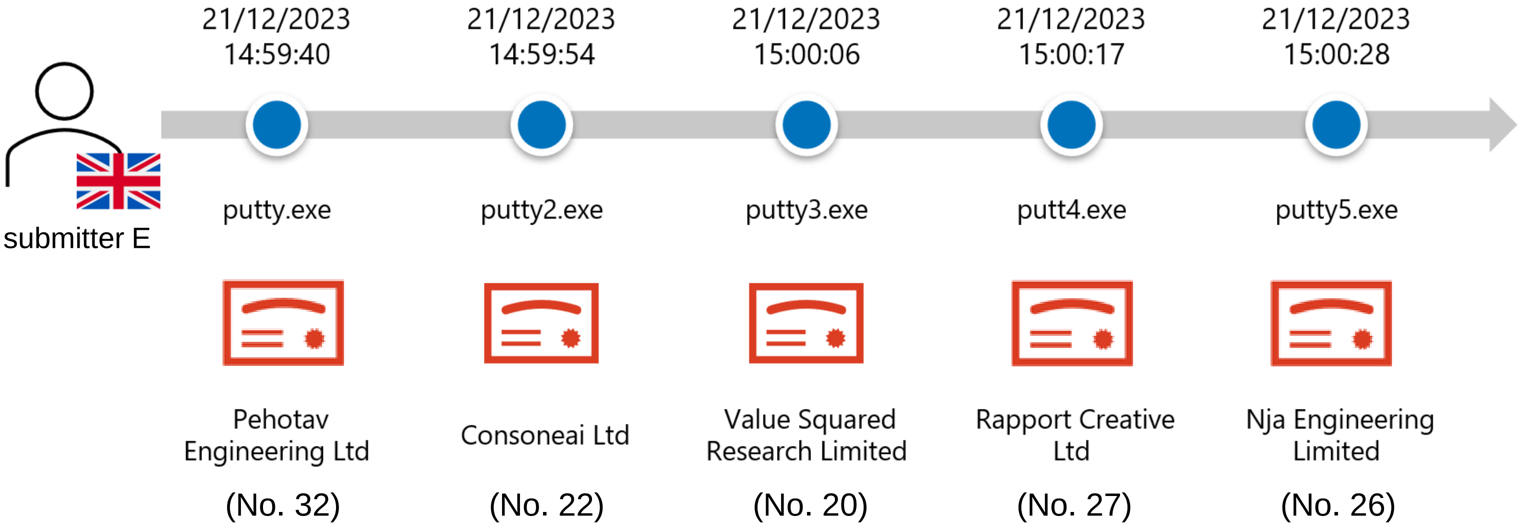
Discovered 10 new certificates in April 2024



| Signature No. | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | submitter |
|---|---|---|---|---|---|---|---|---|---|
| 25 | | | | | | | | | F 🇺🇸 |
| 26 | | | | | | | | | E 🇬🇧 |
| 27 | | | | | | | | | E 🇬🇧 |
| 29 | | | | | | | | | G 🇷🇺 |
| 32 | | | | | | | | | E 🇬🇧 |
| 33 | | | | | | | | | D 🇳🇱 |

# Hypothesis: Future Sight

Predicted certificates were abused as expected



submitter E

| 21/12/2023 14:59:40 | 21/12/2023 14:59:54 | 21/12/2023 15:00:06 | 21/12/2023 15:00:17 | 21/12/2023 15:00:28 |
|---|---|---|---|---|
| putty.exe | putty2.exe | putty3.exe | putt4.exe | putty5.exe |
| Pehotav Engineering Ltd | Consoneai Ltd | Value Squared Research Limited | Rapport Creative Ltd | Nja Engineering Limited |
| (No. 32) | (No. 22) | (No. 20) | (No. 27) | (No. 26) |

# Insight

- Certificate vendors submit test samples for detection testing
  - Test samples with different certificates are submitted in quick succession
  - Certificates have similar start times and are submitted soon after creation
  - Proves to buyers that AV detection is avoided, and certificates aren't reused

# Insight

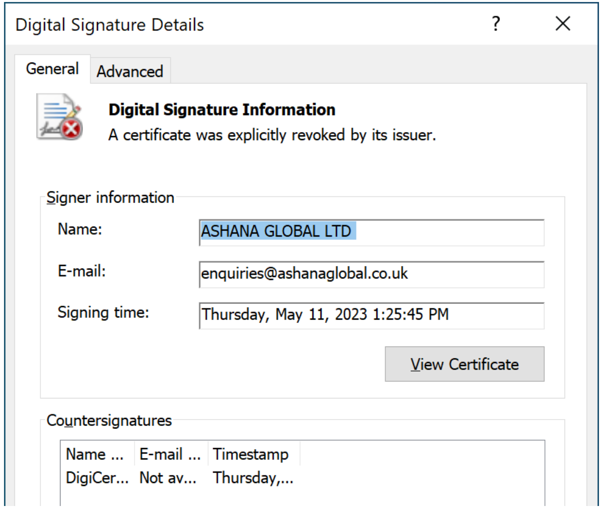
- Certificate vendors submit test samples for detection testing
  - Test samples with different certificates are submitted in quick succession
  - Certificates have similar start times and are submitted soon after creation
  - Proves to buyers that AV detection is avoided, and certificates aren't reused
- The average time gap between test samples and malicious files is 75.3 days
  - Vendors pre-create and pool certificates
  - Multiple certificates are created together, but used at different times

# Insight

- Certificate vendors submit test samples for detection testing
  - Test samples with different certificates are submitted in quick succession
  - Certificates have similar start times and are submitted soon after creation
  - Proves to buyers that AV detection is avoided, and certificates aren't reused
- The average time gap between test samples and malicious files is 75.3 days
  - Vendors pre-create and pool certificates
  - Multiple certificates are created together, but used at different times
- Longer gaps between test sample submits and abuse increase the chance of predicting and revoking certificates

# Revocation of Malicious Certificates

Revoked certificates are listed in the CRL, causing MSIX installation to fail



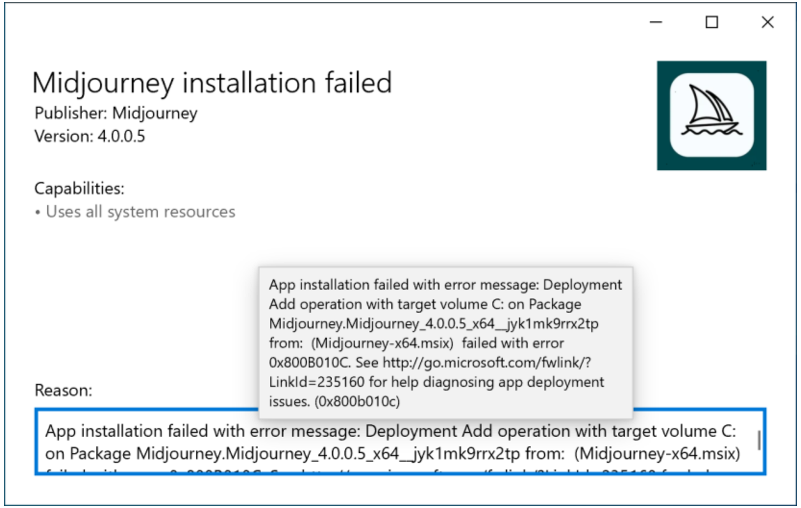
**Digital Signature Information**
A certificate was explicitly revoked by its issuer.

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,... |



Midjourney installation failed
Publisher: Midjourney
Version: 4.0.0.5

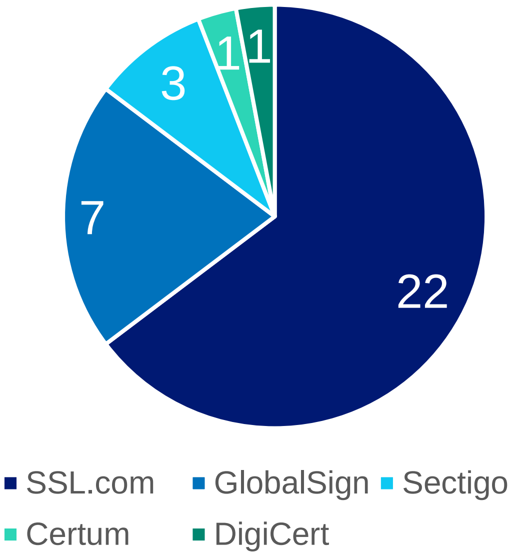
Capabilities:
- Uses all system resources

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)

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)

# Characteristics on Abused Certification



- Certificate validity: 1 year
- Signer: legitimate company
- Company has been registered for over 3 years

- Country code: GB
- Registered with Companies House

# How to Get Certification

- Certificate theft
  - Unlikely due to common characteristics between certificates
  - Few files signed other than MSIX and test files

# How to Get Certification

- Certificate theft
  - Unlikely due to common characteristics between certificates
  - Few files signed other than MSIX and test files
- Establishing a shell company
  - Unlikely due to over 3 years since registration
  - The website is real, and the SSL certificate is issued by a different CA
  - Creating a shell company from scratch is too costly

# How to Get Certification

- Certificate theft
    - Unlikely due to common characteristics between certificates
    - Few files signed other than MSIX and test files
- Establishing a shell company
    - Unlikely due to over 3 years since registration
    - The website is real, and the SSL certificate is issued by a different CA
    - Creating a shell company from scratch is too costly
- Impersonating a legitimate company
    - OV certificate requirements can be bypassed with a link proving the company’s existence
    - Identity verification can be circumvented via SMS, suggesting weak authentication processes

# Migration

- Certificates already abused: Report to the CA and revoke them
- Certificates predicted to be abused: Restrict execution of signed files (Group Policy > AppLocker)

# Responsible Disclosure

We report each abused certificate to the CA as soon as it is identified.

# Wrap-Up

- Uncovered attacks using MSIX and their ecosystem
- Proposed a method to predict certificates likely to be abused months in advance by analyzing vendors' testing activities
- Vendors are likely impersonating legitimate companies to obtain certificates

# Thank you!