NTT Security Holdings

# Broken Seals, Broken Trust:

## Flaws and Defences in the Certificate Ecosystem

Yuta Sawabe, Rintaro Koike

# Who am I?

NTT Security Holdings

Yuta Sawabe

Security Researcher @ NTT Security

Rintaro Koike

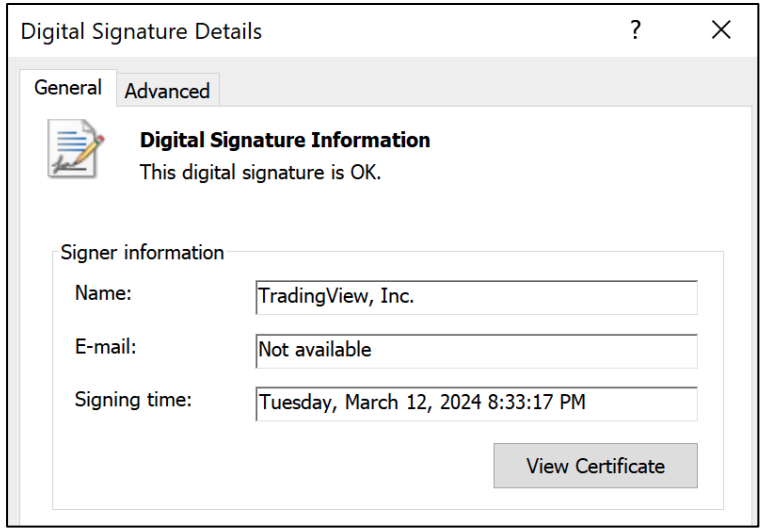
Security Researcher @ NTT Security
Threat Research, Malware Analysis
Researcher @ nao_sec

# Code-Signing Certificate

NTT Security Holdings

Commonly used for the following two main purposes:

- To identify the software publisher
- To verify if the software has been tampered with



# Abuse of Code-Signing Certificate

NTT Security Holdings

It is now common for malware and other 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

NTT Security Holdings

1. Stealing from organisations that already possess certificates

→ This was traditionally the most common method.

2. Purchasing certificates through alternative channels

→ 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**

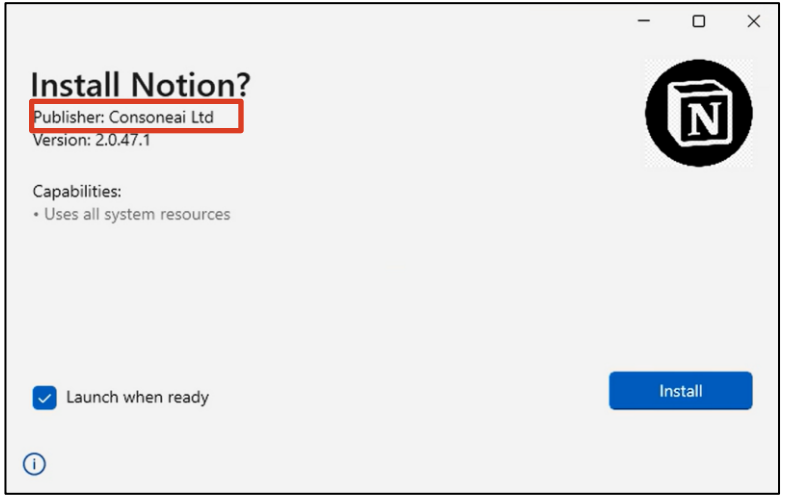
Digital code signing certificates are more expensive than credit cards or weapons.

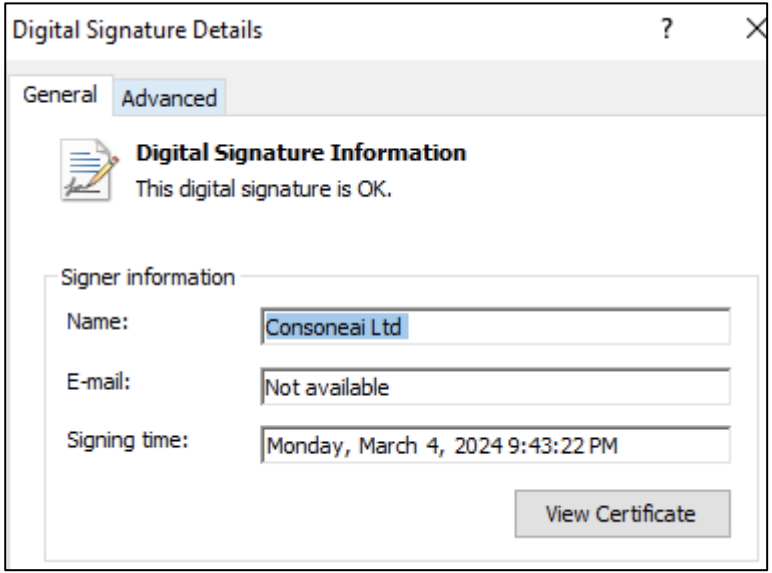
Written by **Charlie Osborne,** Contributing Writer
Oct. 31, 2017 at 5:00 a.m. PT

# Example: Malicious MSIX File

NTT Security Holdings

MSIX files must be signed with a valid code-signing certificate.
→ Vendors distributing MSIX files work in collaboration with certificates sellers.



# Code-Signing Certificate Sellers

NTT Security Holdings

**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)**

# Price List Example

NTT Security Holdings

**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$*

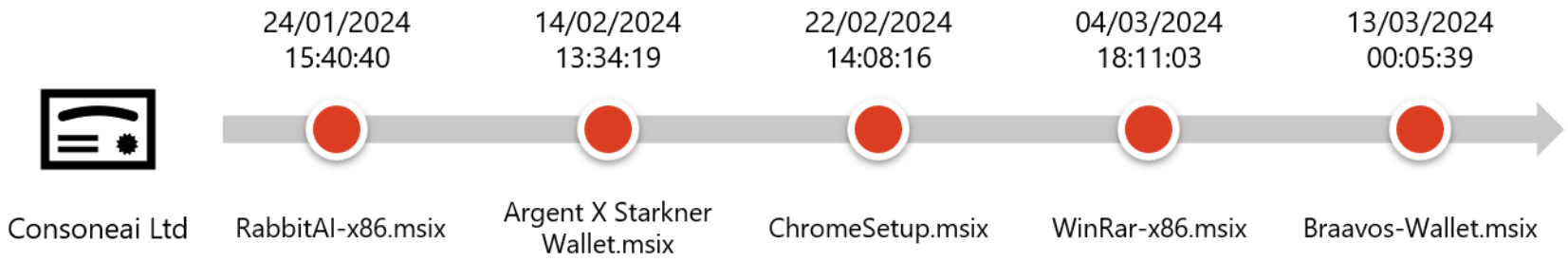
*(The pre-order is made on a full prepayment or deposit to the escrow, the period for obtaining a certificate is on average 3 - 14 days, the entire process of obtaining a certificate will be accompanied by a progress report)*

# Collecting MSIX Files

NTT Security Holdings

We tracked MSIX files submitted to online malware-sharing sites for over a year.

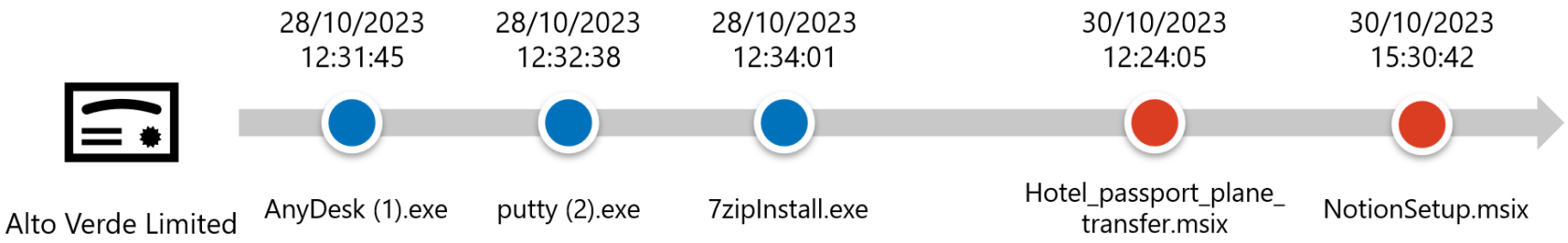
Most certificates were abused for several months.



# Notable Findings

NTT Security Holdings

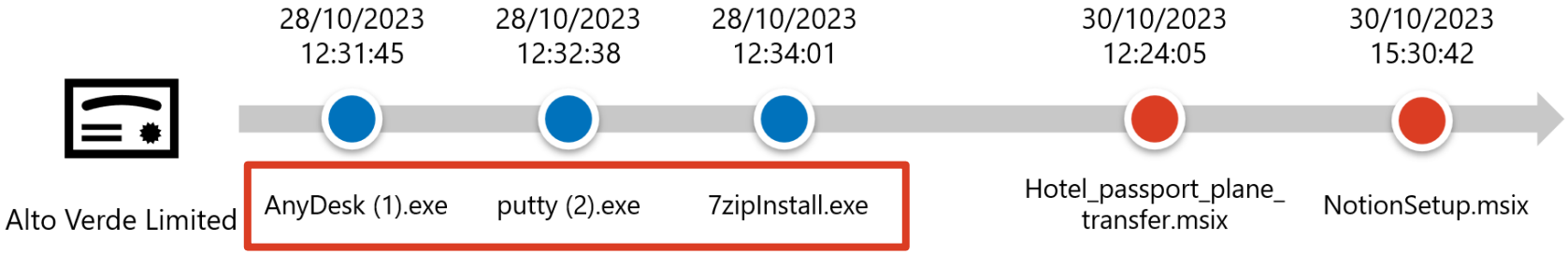
Legitimate files (“test samples”) appeared before the MSIX files.



# Notable Findings

NTT Security Holdings

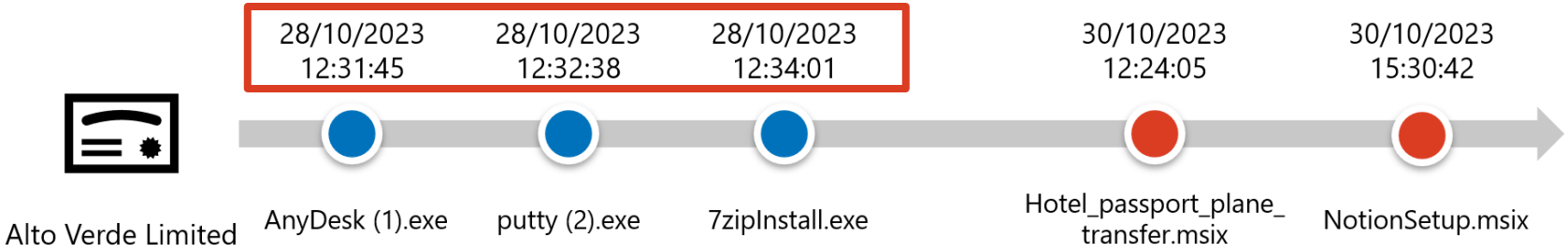
1. Legitimate files were signed with the same certificate as the MSIX files



# Notable Findings

NTT Security Holdings

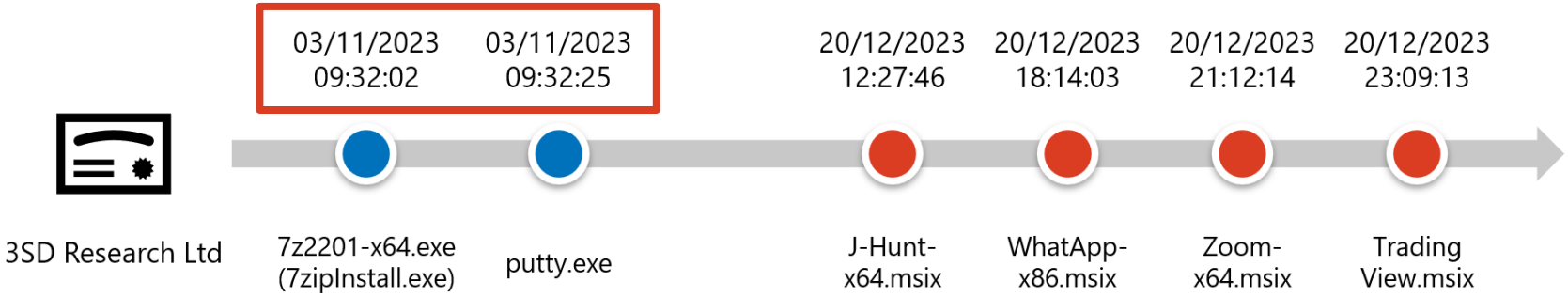
2. The test samples were submitted before the MSIX files



# Notable Findings

NTT Security Holdings

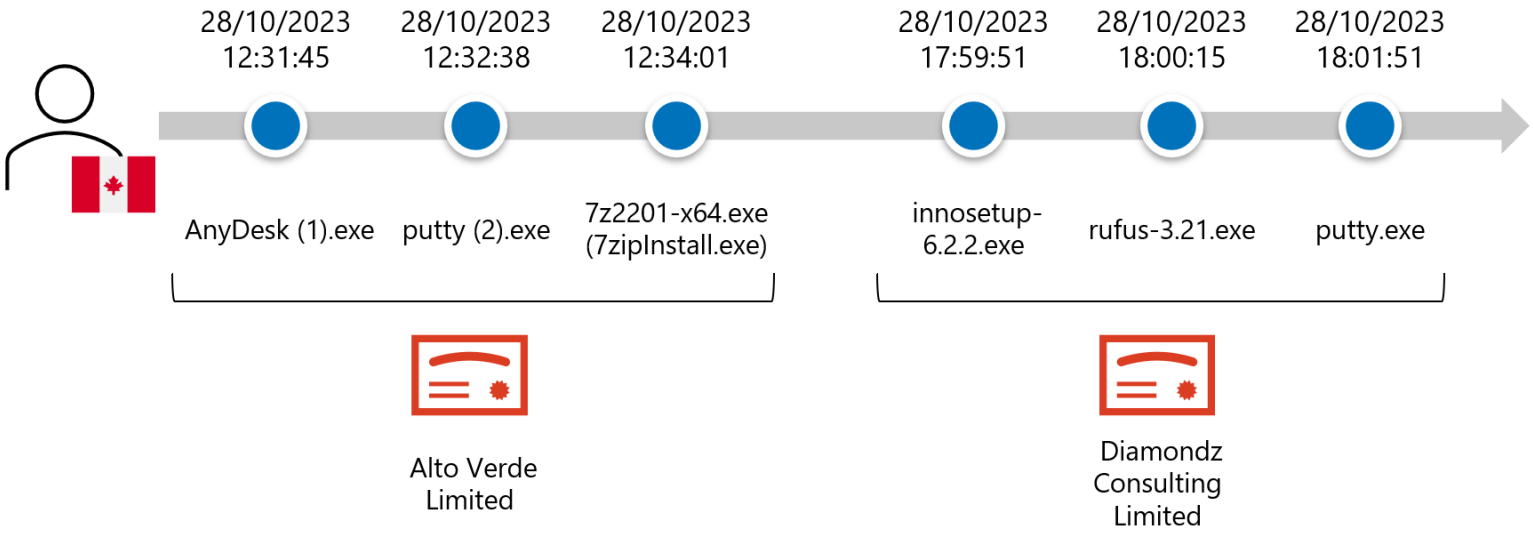
In some cases, they appeared earlier several months in advance



# Notable Findings

NTT Security Holdings

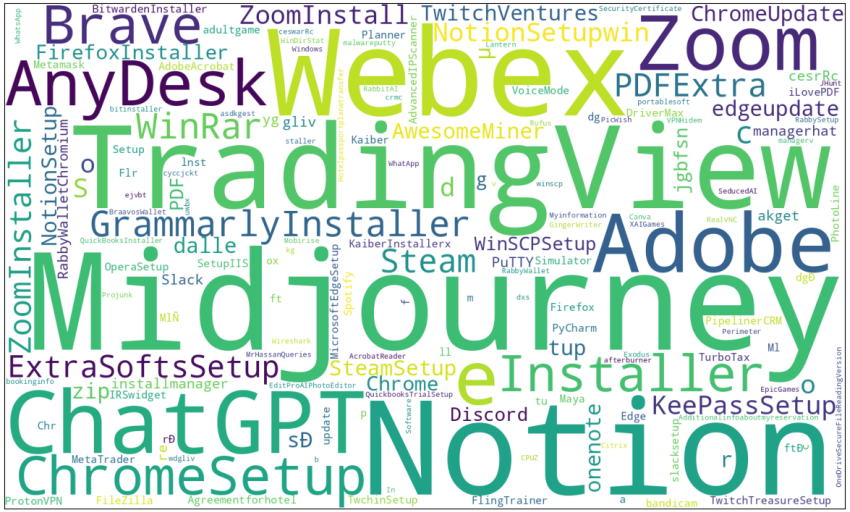
3. The same uploader submits multiple test samples at the same time.



# Collected MSIX & Test Samples

NTT Security Holdings

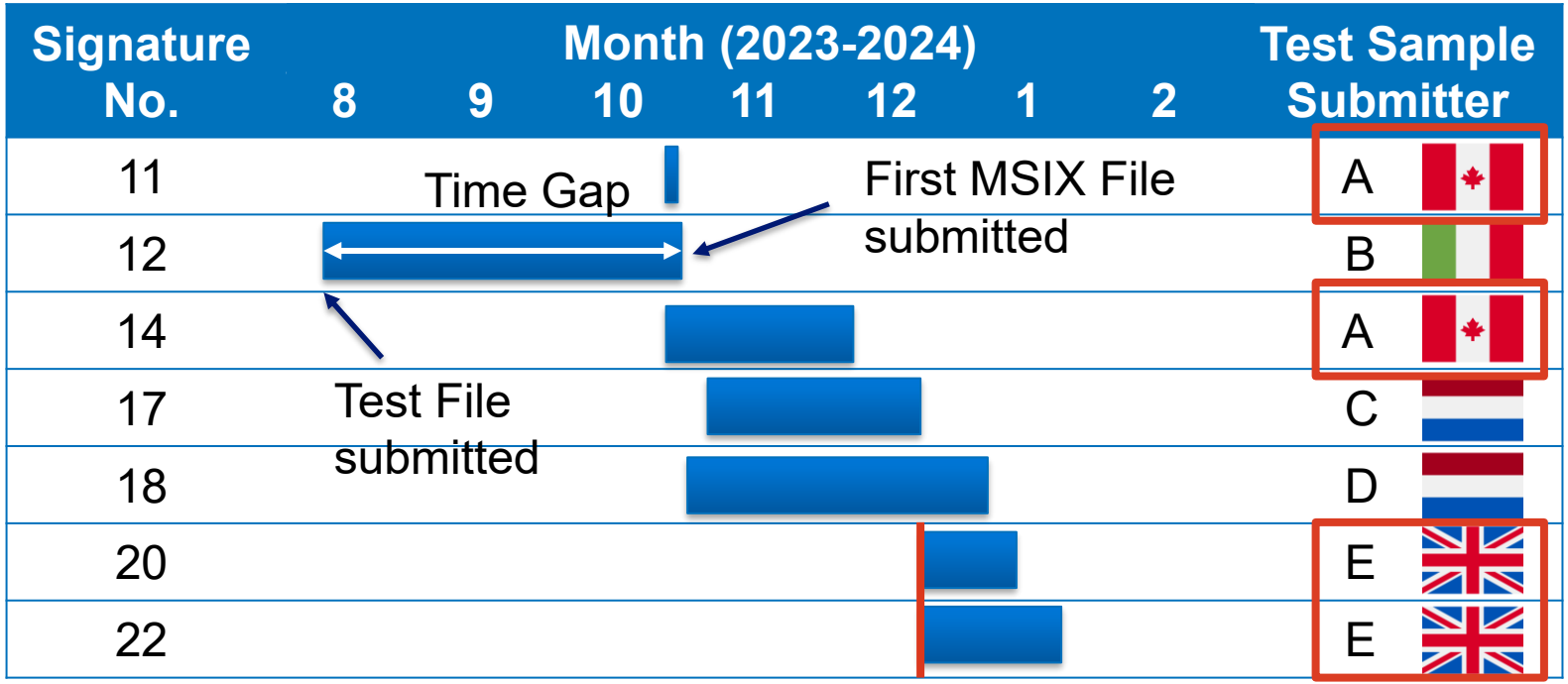
- We analyzed over 300 malicious MSIX files submitted by March 2024.
- From these, we identified 24 certificates and 18 test samples.




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

# Submission Timeline (Up to Mar 2024)

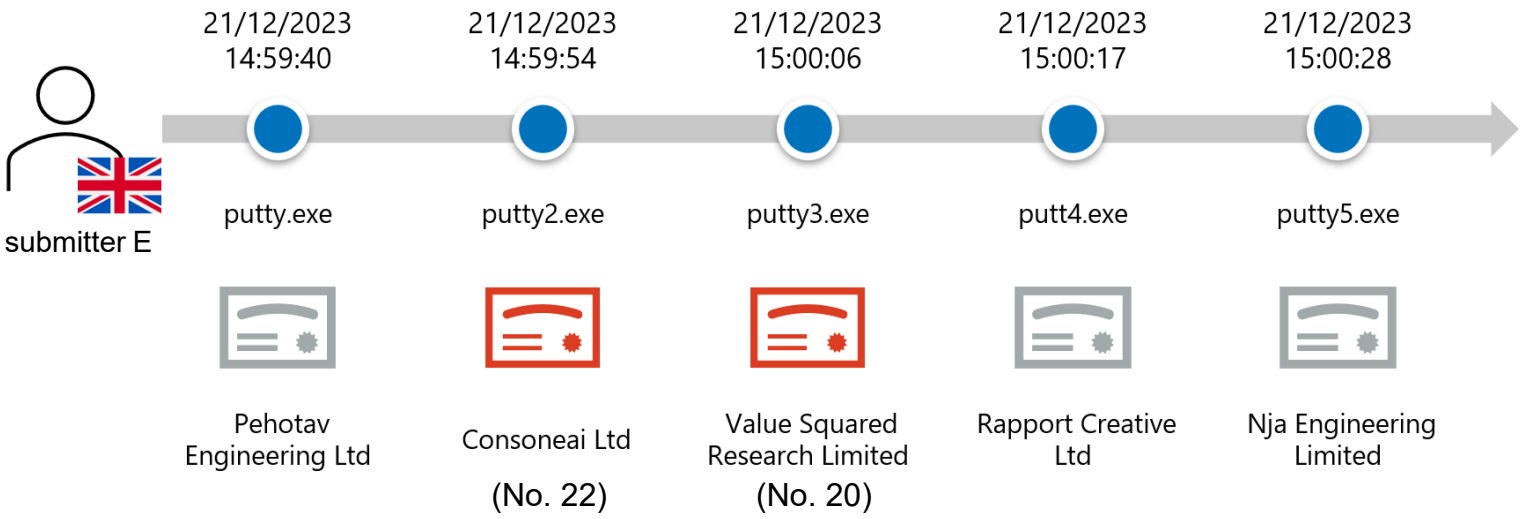
NTT Security Holdings



# Hypothesis: Future Sight

NTT Security Holdings

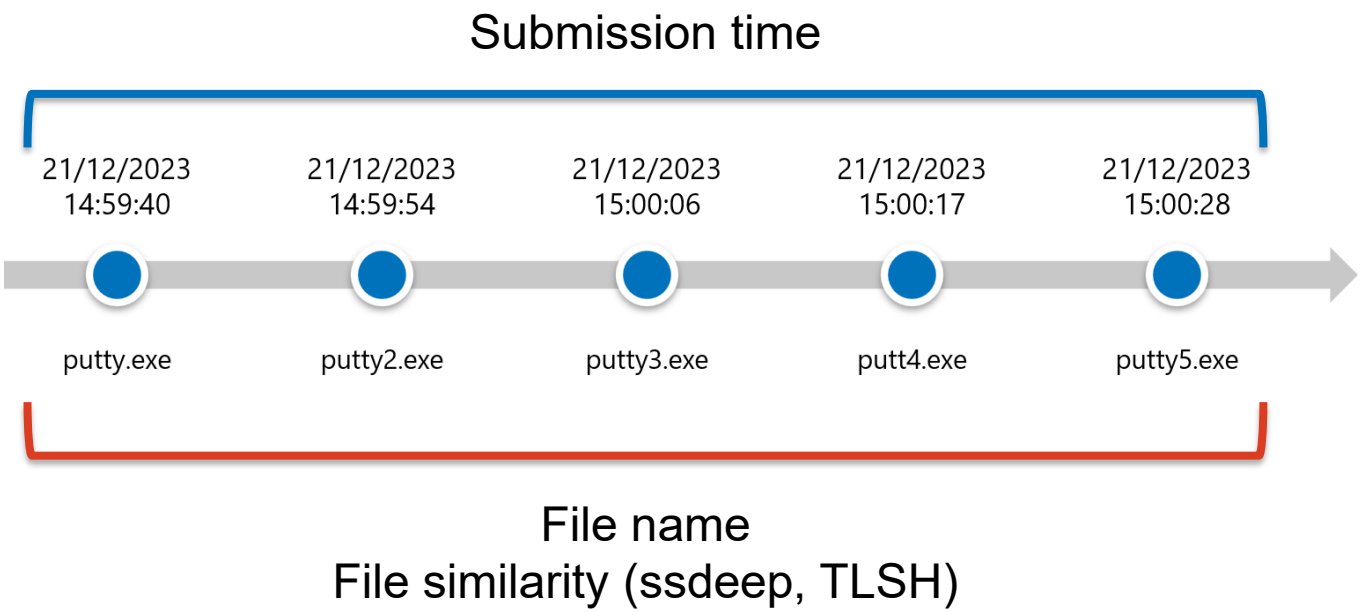
Test samples can be used to identify certificates that may be abused in the future.



# Hunting for Predictive Test Sample

NTT Security Holdings

Attackers are likely to use similar test samples



# Submission Timeline (Apr 2024)

NTT Security Holdings

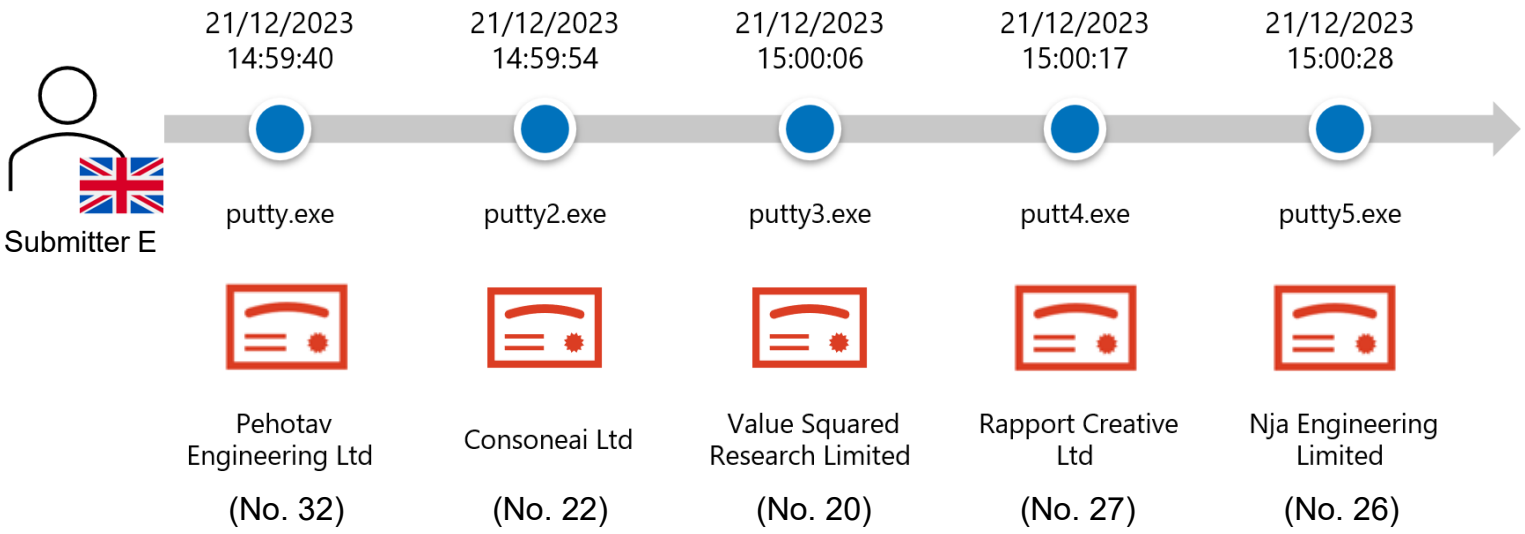
10 new certificates were discovered during April 2024

| Signature No. | Month (2023-2024) 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | Test Sample Submitter |
|---|---|---|---|---|---|---|---|---|---|
| 25 | | | | | | | | | F |
| 26 | | | | | | | | | E |
| 27 | | | | | | | | | E |
| 29 | | | | | | | | | G |
| 32 | | | | | | | | | E |
| 33 | | | | | | | | | D |

# Hypothesis: Future Sight

NTT Security Holdings

As predeicted, certificates identified from test samples were later abused.



# Insight

NTT Security Holdings

- AV detection testing through test samples
  - Test samples with different certificates are submitted in rapid succession.
  - Certificates often have similar issue dates and are submitted soon after issuance.
  - This demonstrates to to buyers that AV detection is avoided and certificates are not reused.

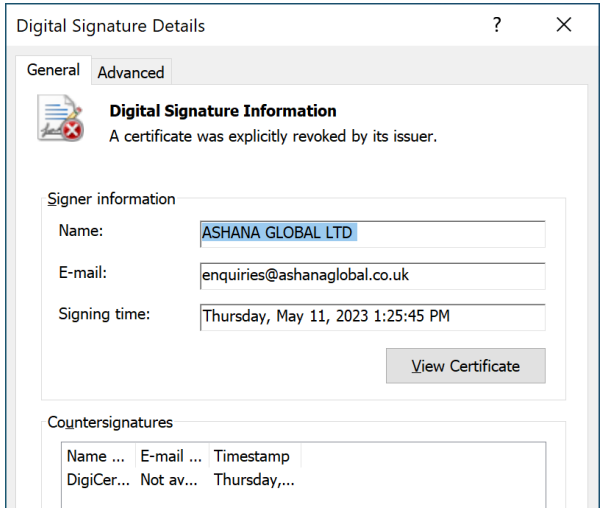
- The average gap between test sample and MSIX file submissions is **75.3 days**.
  - Vendors pre-generate and pool certificates in advance.
  - Multiple certificates are issued together but used at different times.

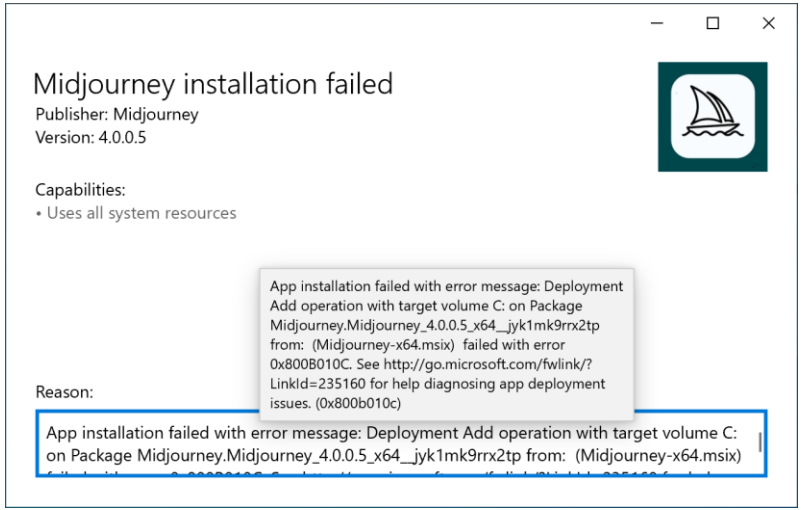
- Implication : Longer gaps make prediction and revocation more likely.

# Revocation of Malicious Certificates

NTT Security Holdings

When a certificate is revoked and added to the CRL, MSIX installation will fail.



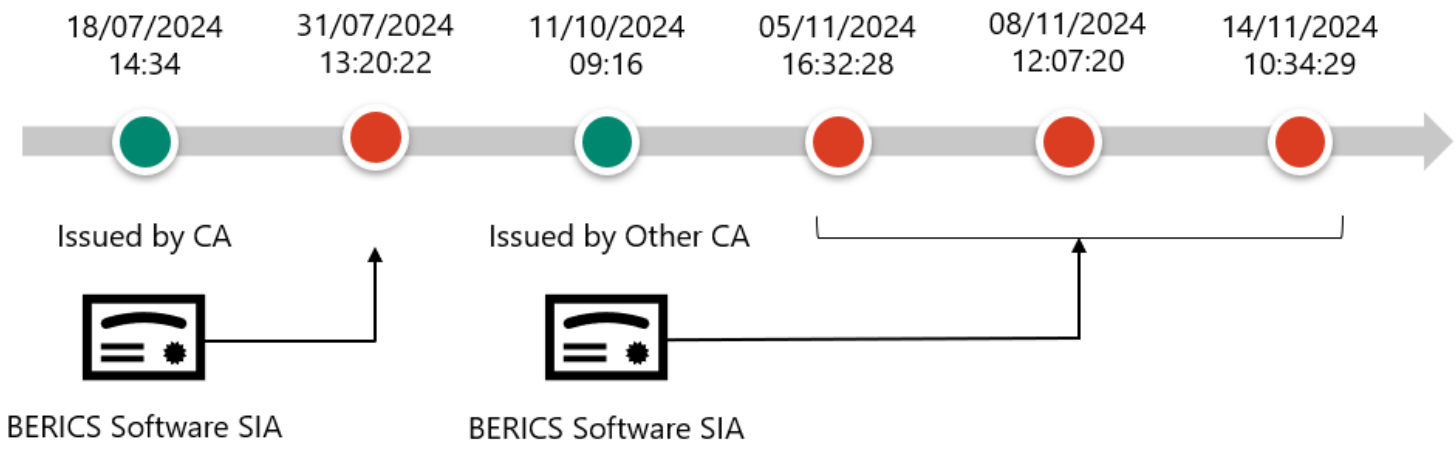



# Zombie Certificates

NTT Security Holdings

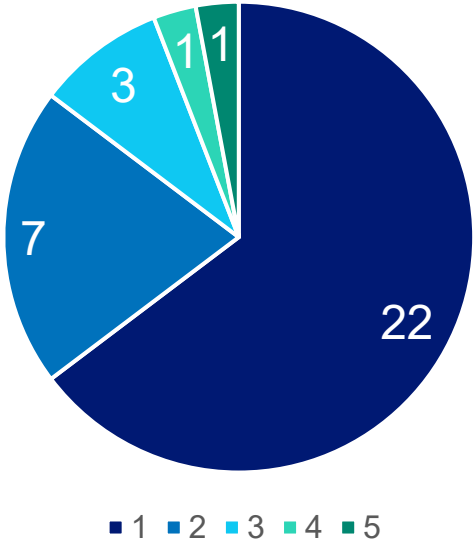
The same company was impersonated to obtain certificates from multiple CAs.

→ Zombie certificates reappear when CAs don’t coordinate on abuse.



# Common Traits on Abused Certification

NTT Security Holdings




## All Abused Certificates

- Validity Period: 1 year
- Signer: a legitimate company
- Company registered for over 3 years

## Most Frequently Used CA

- Country : GB
- Registered with Companies House

# How to Get Certification

NTT Security Holdings

## ❌ Certificate Theft

- Unlikely due to common traits across certificates
- Very few files signed other than MSIX and test files

## ❌ Shell Companies

- Unlikely, as most companies were registered over 3 years
- Their websites are legitimate, with SSL certificates from different CAs
- High cost of creating shell companies from scratch

## ✅ Company Impersonation

- OV certificates can be obtained with just a public link proving the company's existence
- Identity verification can be circumvented via SMS

# Example: CA Verification Process in UK

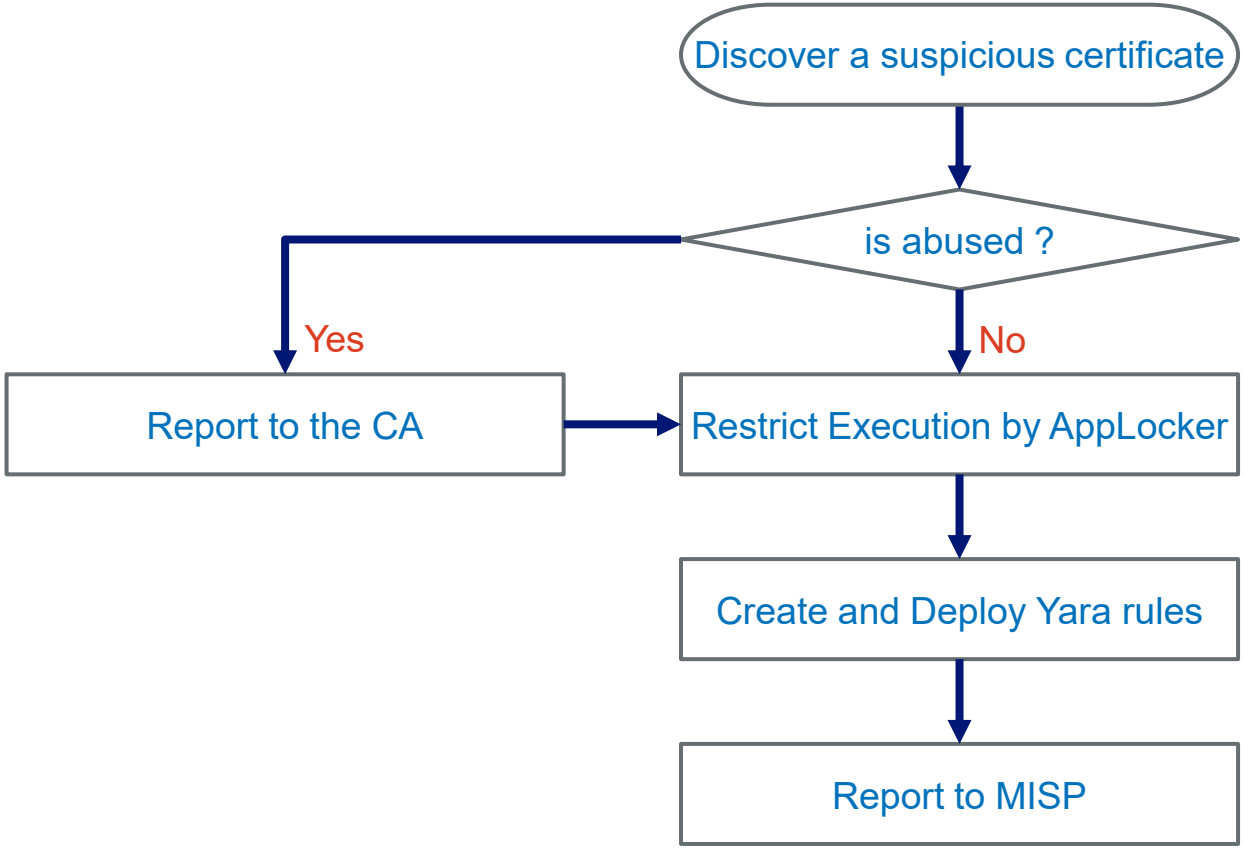
NTT Security Holdings

| Step | CA's Check | Attacker's Bypass |
|---|---|---|
| 1. Organaisation Validation | Verify legal existence via public databases (e.g., Companies House) | Submit fake company registration details |
| 2. Domain Control Validation | Send a validation code to the domain administrator's email | Register a similar domain and control email |
| 3. Callback Process | Make an automated phone call to verify the applicant's number | Use a fake phone number for verification |

ReversingLabs, "Digital Certificates - Models for Trust and Targets for Misuse", https://www.reversinglabs.com/blog/digital-certificates-impersonated-executives-as-certificate-identity-fronts

# Mitigation Flowchart

NTT Security Holdings



# Report to the CA

NTT Security Holdings

Report malicious certificates to the CA to initiate renovation.

- certReport
  - https://github.com/Squiblydoo/certReport
  - A tool to assist with reporting to the CA

README

## CertReport

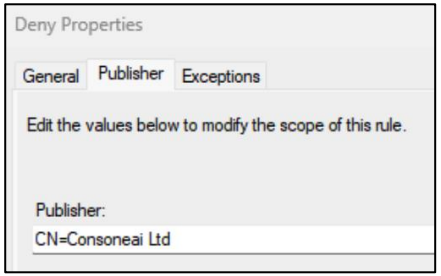
This tool is intended to reduce the load of effort required to report authenticode certificates. It is intended to take the smallest amount of effort from the reporter, but provide the certificate authority with most the information they need to make a decision. When possible, it is recommended to augment the report with your own findings to help the certificate provider know what suspicious indicators you found.

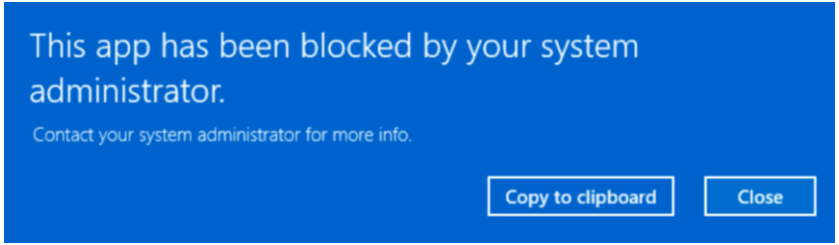
# Restrict Execution

NTT Security Holdings

Restrict execution of files signed with potentially abusive certificates

- AppLocker
- WDAC (Windows Defender Application Control)
- App Control for Business



# Create and Deploy YARA Rules

NTT Security Holdings

Use YARA rules to investigate and respond to certificate abuse

- If exploitation is confirmed
  - Collect IoCs related to malicious files or malware
- If exploitation is not yet confirmed
  - Monitor for signs of abuse
  - Report the exploitation to the CA when observed

```
import "vt"
import "pe"

rule Blacklist_Certificates
{
    condition:
        for any tag in vt.metadata.tags : ( tag == "signed" ) and
        (
            pe.signatures[0].subject contains "Consoneai Ltd" or
            pe.signatures[0].subject contains "Alto Verde Limited" or
            pe.signatures[0].subject contains "3SD Research Ltd" or
            ...
        )
}
```

# Manage in MISP

NTT Security Holdings

## MISP's authenticode-signerinfo object

| Object attribute | MISP attribute type | Description |
|---|---|---|
| content-type | text | Content type |
| digest-base64 | text | Signature created by the signing certificate's private key |
| digest_algorithm | text | Algorithm used to hash the file |
| encryption_algorithm | text | Algorithm used to encrypt the digest |
| issuer | text | Issuer of the certificate |
| program-name | text | Program name |
| serial-number | text | Serial number of the certificate |
| signature_algorithm | text | Signature algorithm |
| text | text | Free text description of the signer info |
| url | url | Url |
| version | text | Version of the certificate |

# Wrap-Up

NTT Security Holdings

| Flaw | Defence |
|---|---|
| Impersonation of organaisations | Stricter identity verification by CAs |
| Overlooked test samples | Use test samples to predict abuse |
| Zombie certificates (revoked but reused) | Improve CA revocation processes |
| Implicit trust in signed malicious files | Apply Applocker and YARA rules |
| Poor IoC management and sharing | Share IoCs via platforms like MISP |

# Thank you!