On the Eve of Code Signing Transformation

HITOMI KIMURA

JSAC2023 1.26.2023

Who am I

- Hitomi Kimura
  - Incident Response Analyst for EDR
  - Observing and Reporting new or noteworthy things of incidents
  - Work for Trend Micro in United States
  - Moved to United States in 2016
  - Interested in PKI

- Today's material will be available after blurred a part of screenshots.

2022 was a difficult year for code signing.

- Reports of valid signed driver abuse continued
- QAKBOT distributed valid signed Malicious Modules

Date	Threat Actor	Key Point of Abuse	Victim	Note
2022/5	AvosLocker Ransomware	Stop anti-virus from bringing in vulnerable code-signed driver(BYOVD)	Avast	Link
2022/7	QAKBOT	Multiple abused certificates may have been issued directly to the adversary	Microcompanies	Link
2022/8	Cuba Ransomware	Brought in code-signed driver with NVIDIA certificate and private key found in the LAPSUS leak to stop anti-virus	NVIDIA	Link
2022/8	A ransomware actor	Stop anti-virus from bringing in vulnerable code-signed driver(BYOVD)	Genshin Impact	Link
2022/9	Lazarus	Stop monitoring from bringing in vulnerable code-signed driver(BYOVD)	Dell	Link
2022/12	POORTRY & STONESTOP	Developer program account created and code-signed malicious drivers	Microsoft	Link1, Link2, Link3, Link4

Various Code Signing Abuse Scenarios (In the Wild)

SEQ	Compromised Part	Key Point of Abuse
1	Code-signed module	BYOVD(Bring Your Own Vulnerable Driver)
2	Supply Chain	Supply chain compromise introduced malicious code into continuous integration
3	Supply Chain	Developer program account created a code-signed malicious driver as a legitimate driver
4	Private key	Stolen or leak of legitimate certificates and private keys
5	Part of RA	Adversary is impersonating a real company owned by someone else for code signing certificates (Still under investigation)
6	Part of RA	Adversary prepares a company owned by them for code signing certificates
7	Algorithm	Created a fake certificate due to MD5 hash value collision

No CA Compromise was observed yet: WebPKI case around 2011 of a person taking control of the RA and getting certificates issued by the CA (e.g., Comodo, DigiNotar) has not yet been seen in code-signing certificates scene. But as of 2022, adversaries' motivation to obtain code-signed drivers has increased, and we can prospect that it will happen next time.

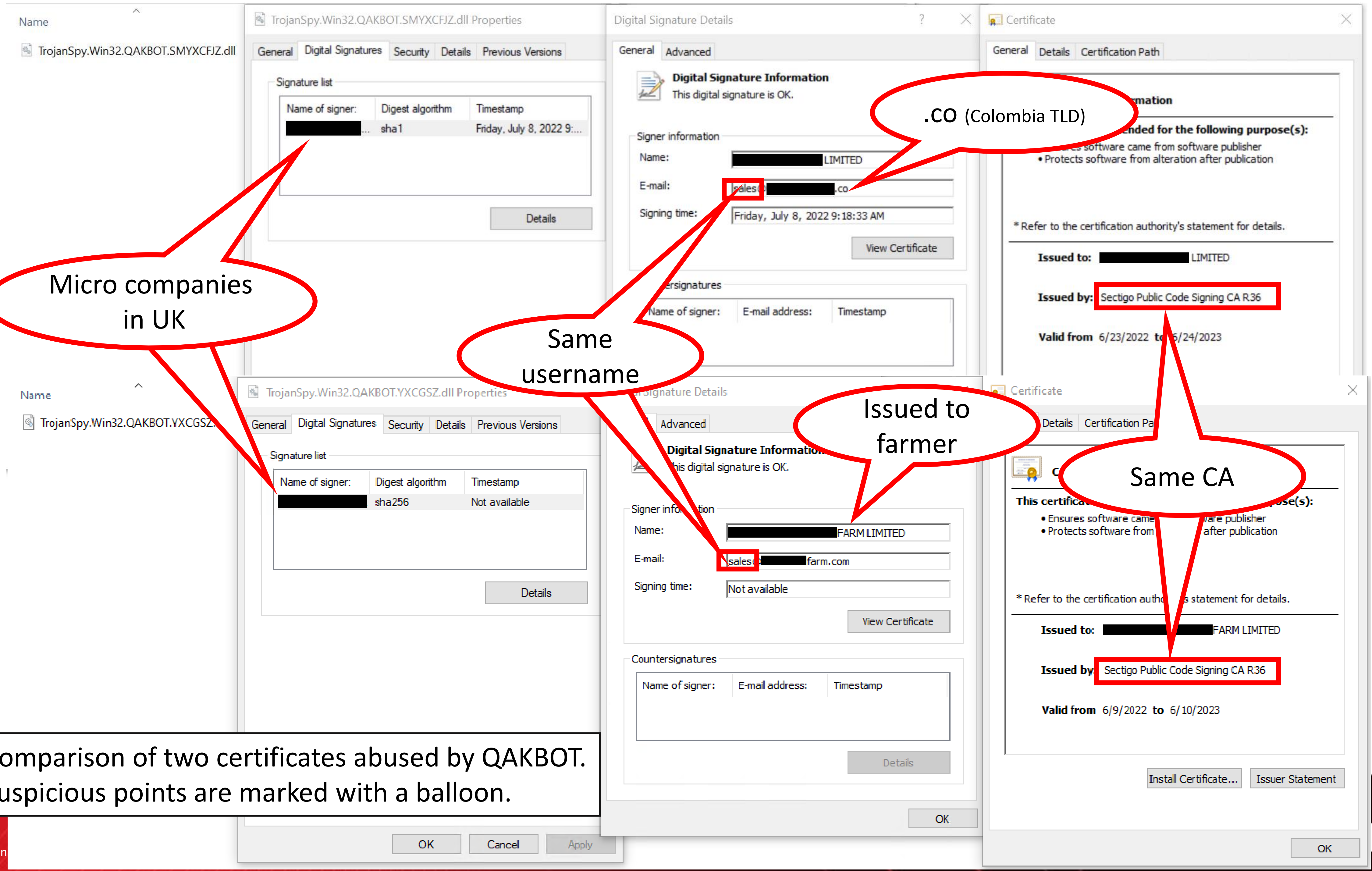
Points to be focused on (1)

- Certificate revocation might not work as we expect in case of code signing abuse
  - Better to revoke than not to revoke, that's for sure.
  - it is still unknown if the certificate will be revoked by Certificate Authority, even no compromise private keys.
  - The conditions may be affected to verify the current status for revocation, it is difficult to be confident that the risky drivers should not be loaded on all computers in the enterprise even if the certificate has been revoked.
  - Discussion in CABF: "Malware based revocation" (2022/6～2022/12, Voted but not merged yet)
    - It seems that the CAs are aiming for more practical operations, such as changing the "one business day" period for contacting subscribers to "24 hours" after confirming an incident.
    - The driver abuse and the SolarWinds case was also discussed, but details are not mentioned for the next case.
    - For this discussion, 2022/12/01 minutes is well worth reading.

Points to be focused on (2)

- Abuse of Certificate Issuance Process might be happening
  - One or a few stolen certificates being used in APT was a well-known scenario of code signing abuse
  - Around July 2022, the distribution of valid code-signed modules by QAKBOT was observed, and further investigation found the use of 7 certificates
  - A review of the contents of the abused certificate reveals some strange points, leading us to think that the adversary may have been issued the certificate directly from the CA, for example, by identity theft.

Dive into the Abused Certificates



Name

TrojanSpy.Win32.QAKBOT.SMYXCFJZ.dll

TrojanSpy.Win32.QAKBOT.SMYXCFJZ.dll Properties

General | Digital Signatures | Security | Details | Previous Versions

Signature list

Name of signer:	Digest algorithm	Timestamp
[redacted]...	sha1	Friday, July 8, 2022 9:...

Details

Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information

Name: [redacted]LIMITED

E-mail: sales@[redacted].co

Signing time: Friday, July 8, 2022 9:18:33 AM

View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp

Certificate

General | Details | Certification Path

...mation

...nded for the following purpose(s):
- ...s software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: [redacted]LIMITED

Issued by: Sectigo Public Code Signing CA R36

Valid from 6/23/2022 to 6/24/2023

Name

TrojanSpy.Win32.QAKBOT.YXCGSZ...

TrojanSpy.Win32.QAKBOT.YXCGSZ.dll Properties

General | Digital Signatures | Security | Details | Previous Versions

Signature list

Name of signer:	Digest algorithm	Timestamp
[redacted]	sha256	Not available

Details

OK | Cancel | Apply

...Signature Details

Advanced

Digital Signature Information
...his digital signature is OK.

Signer information

Name: [redacted]FARM LIMITED

E-mail: sales@[redacted]farm.com

Signing time: Not available

View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp

Details

OK

Certificate

Details | Certification Pa...

This certifica... ...ose(s):
- Ensures software came ... ...are publisher
- Protects software from ... after publication

* Refer to the certification autho... ...s statement for details.

Issued to: [redacted]FARM LIMITED

Issued by: Sectigo Public Code Signing CA R36

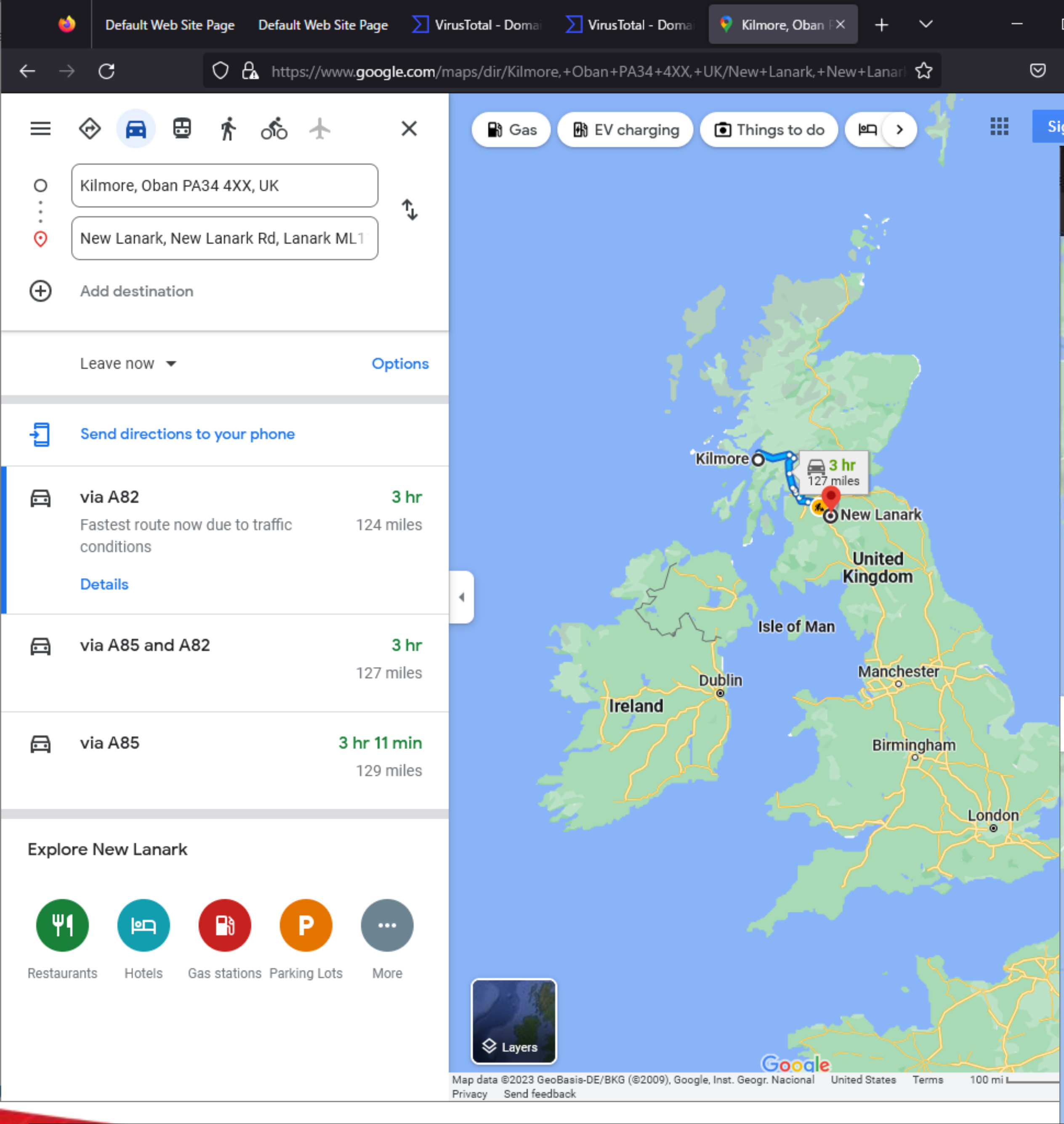
Valid from 6/9/2022 to 6/10/2023

Install Certificate... | Issuer Statement

OK

Comparison of two certificates abused by QAKBOT. Suspicious points are marked with a balloon.

3hours, approx. 200km away

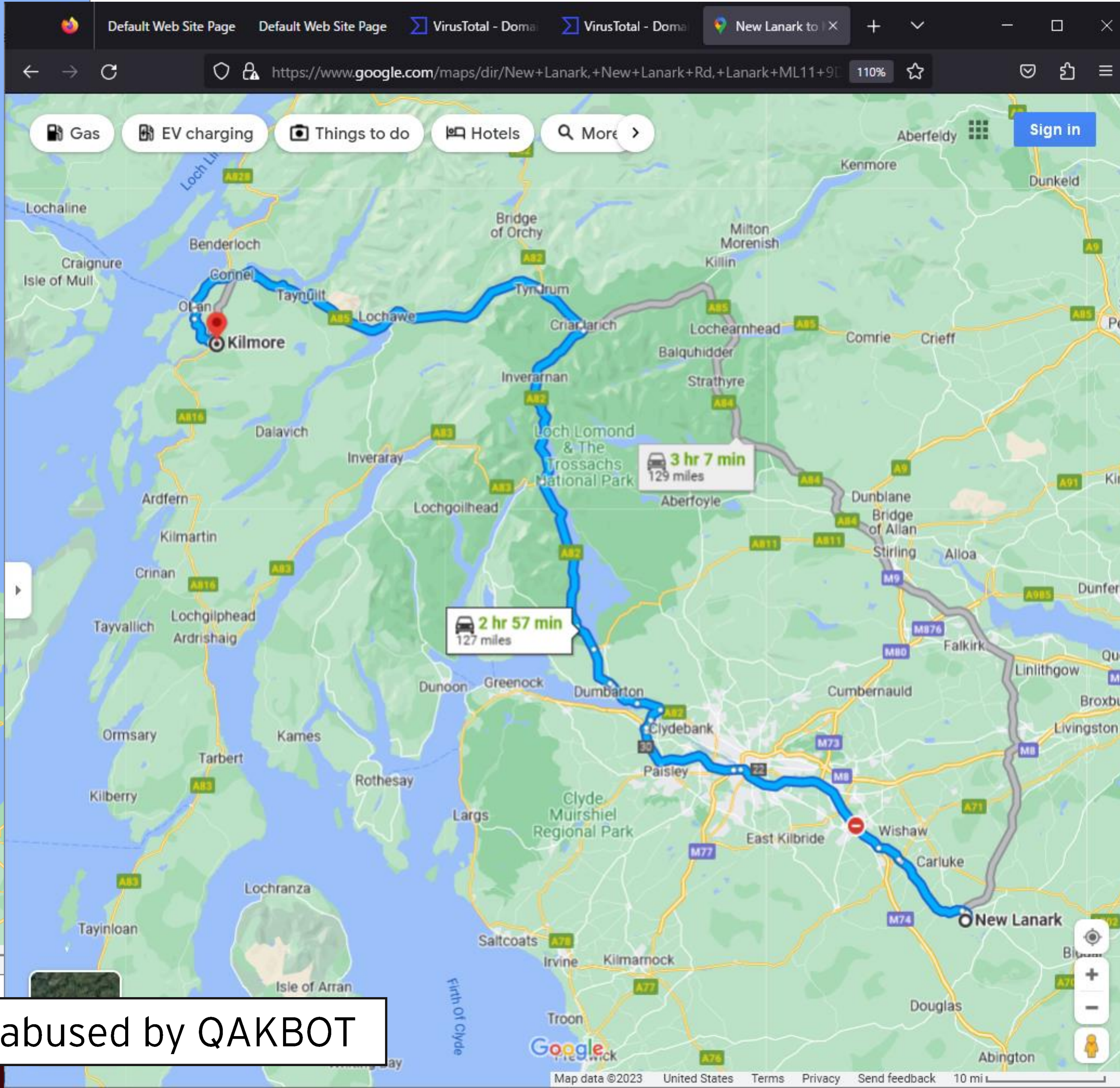


Kilmore, Oban PA34 4XX, UK

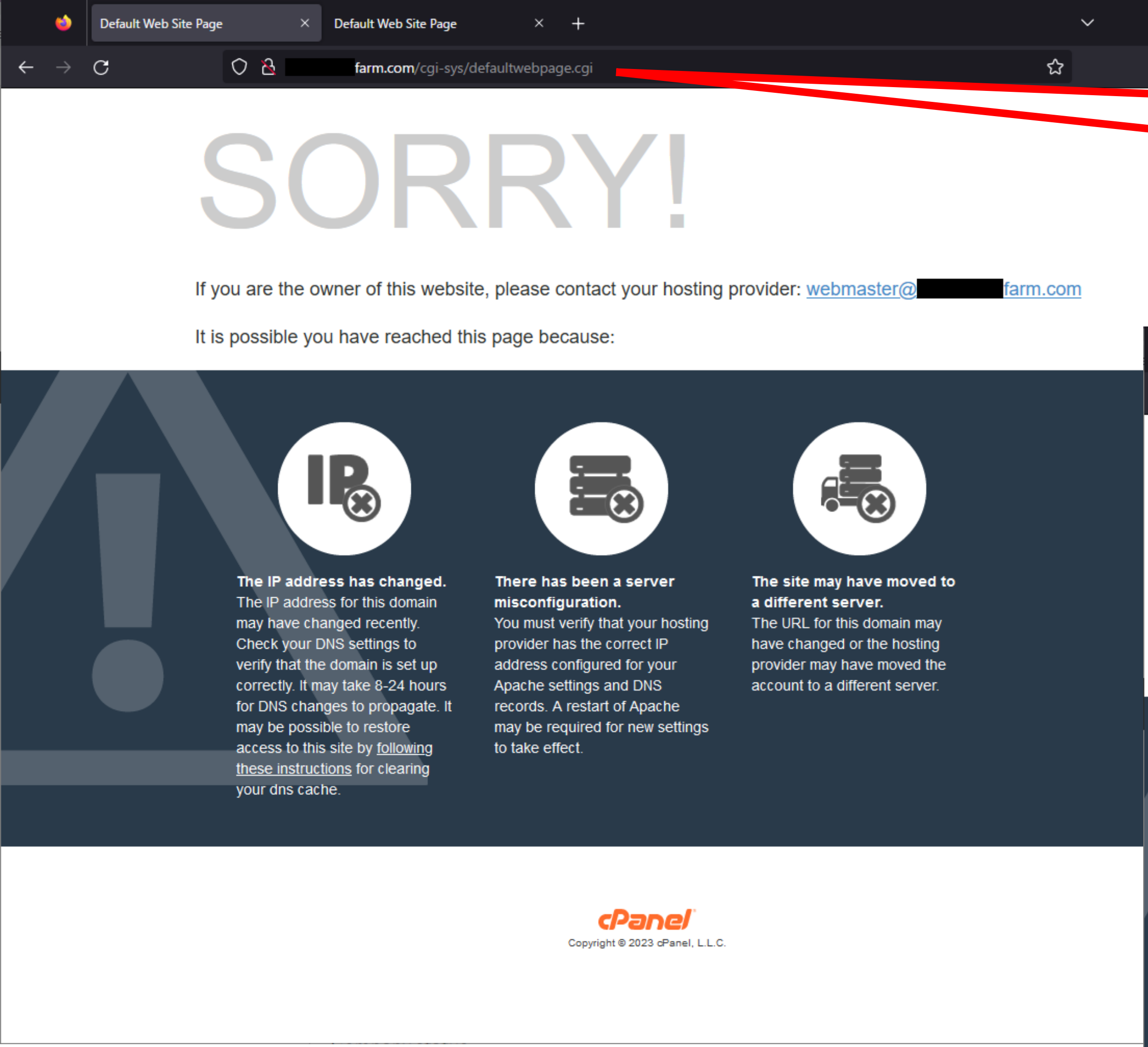
New Lanark, New Lanark Rd, Lanark ML1

via A82 Fastest route now due to traffic conditions	3 hr 124 miles
via A85 and A82	3 hr 127 miles
via A85	3 hr 11 min 129 miles

Explore New Lanark



How far apart are the two companies in the certificates abused by QAKBOT



[redacted]farm.com/cgi-sys/defaultwebpage.cgi

SORRY!

If you are the owner of this website, please contact your hosting provider: webmaster@[redacted]farm.com

It is possible you have reached this page because:

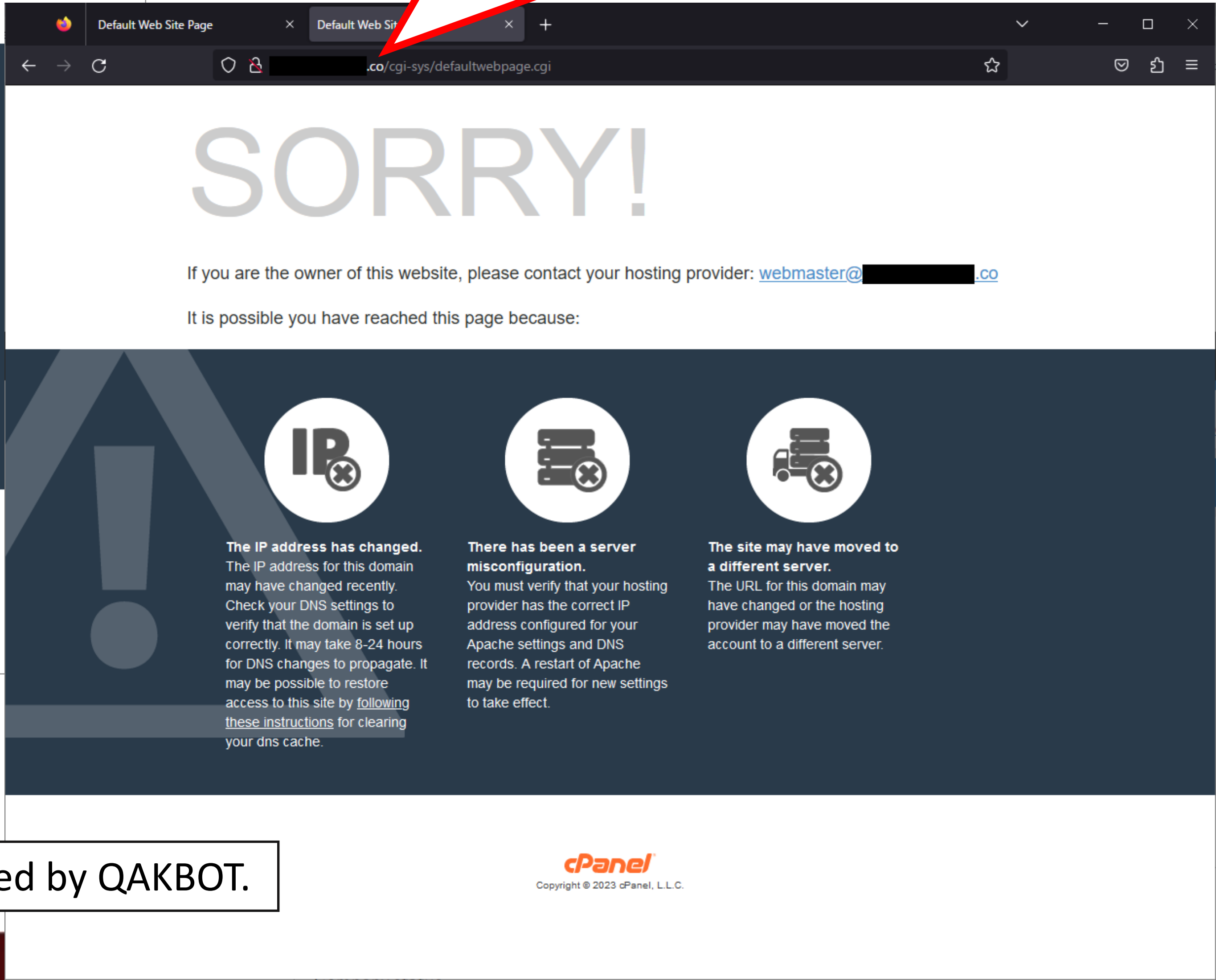
The IP address has changed. The IP address for this domain may have changed recently. Check your DNS settings to verify that the domain is set up correctly. It may take 8-24 hours for DNS changes to propagate. It may be possible to restore access to this site by following these instructions for clearing your dns cache.

There has been a server misconfiguration. You must verify that your hosting provider has the correct IP address configured for your Apache settings and DNS records. A restart of Apache may be required for new settings to take effect.

The site may have moved to a different server. The URL for this domain may have changed or the hosting provider may have moved the account to a different server.

cPanel
Copyright © 2023 cPanel, L.L.C.

Using the same default page with different domain names, and no hosted any contents



[redacted].co/cgi-sys/defaultwebpage.cgi

SORRY!

If you are the owner of this website, please contact your hosting provider: webmaster@[redacted].co

It is possible you have reached this page because:

The IP address has changed. The IP address for this domain may have changed recently. Check your DNS settings to verify that the domain is set up correctly. It may take 8-24 hours for DNS changes to propagate. It may be possible to restore access to this site by following these instructions for clearing your dns cache.

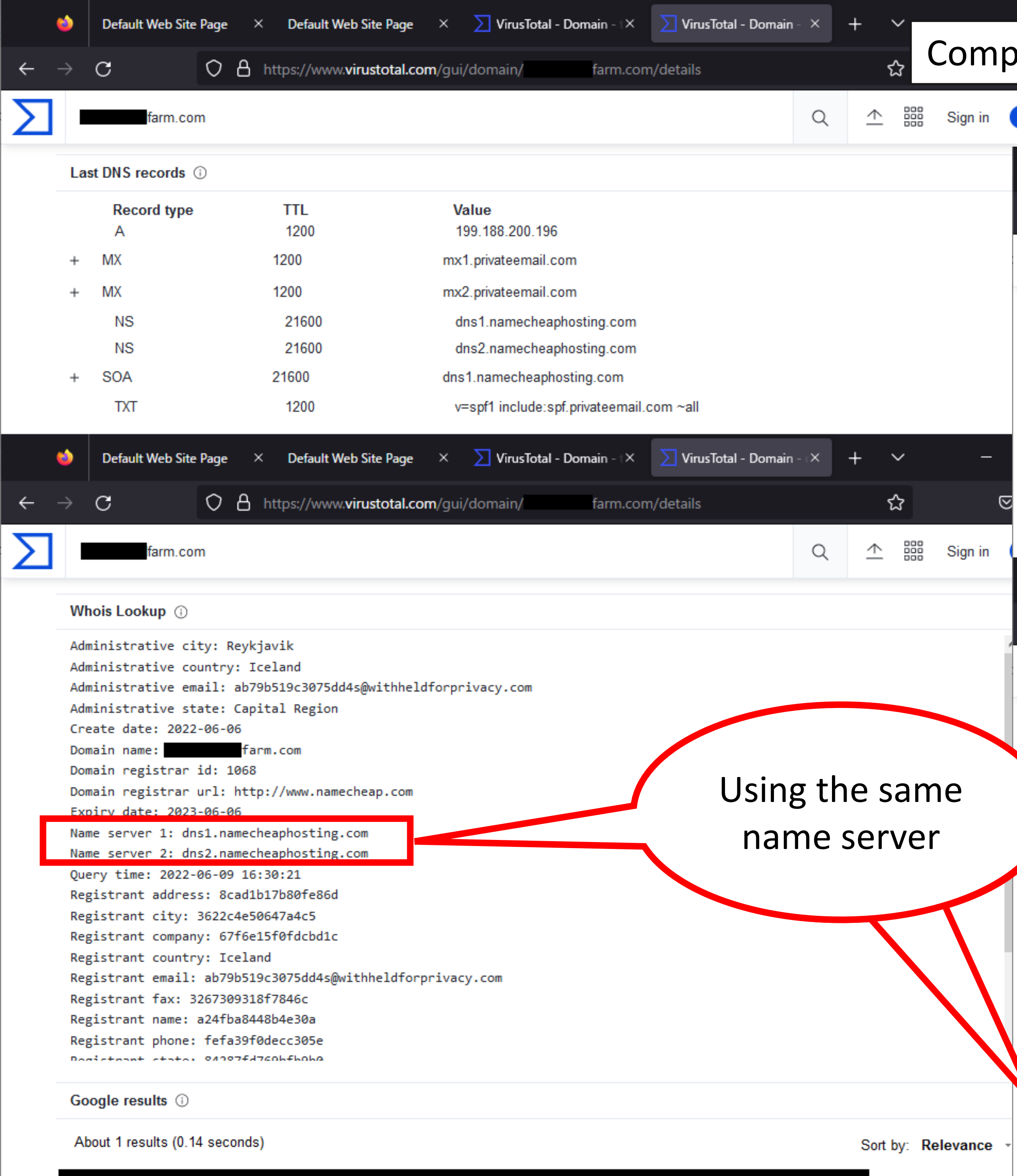
There has been a server misconfiguration. You must verify that your hosting provider has the correct IP address configured for your Apache settings and DNS records. A restart of Apache may be required for new settings to take effect.

The site may have moved to a different server. The URL for this domain may have changed or the hosting provider may have moved the account to a different server.

cPanel
Copyright © 2023 cPanel, L.L.C.

Comparison of two domain name in the certificates abused by QAKBOT.

Comparison of two domain name in the certificates abused by QAKBOT.



Last DNS records

Record type	TTL	Value
A	1200	199.188.200.196
+ MX	1200	mx1.privateemail.com
+ MX	1200	mx2.privateemail.com
NS	21600	dns1.namecheaphosting.com
NS	21600	dns2.namecheaphosting.com
+ SOA	21600	dns1.namecheaphosting.com
TXT	1200	v=spf1 include:spf.privateemail.com ~all

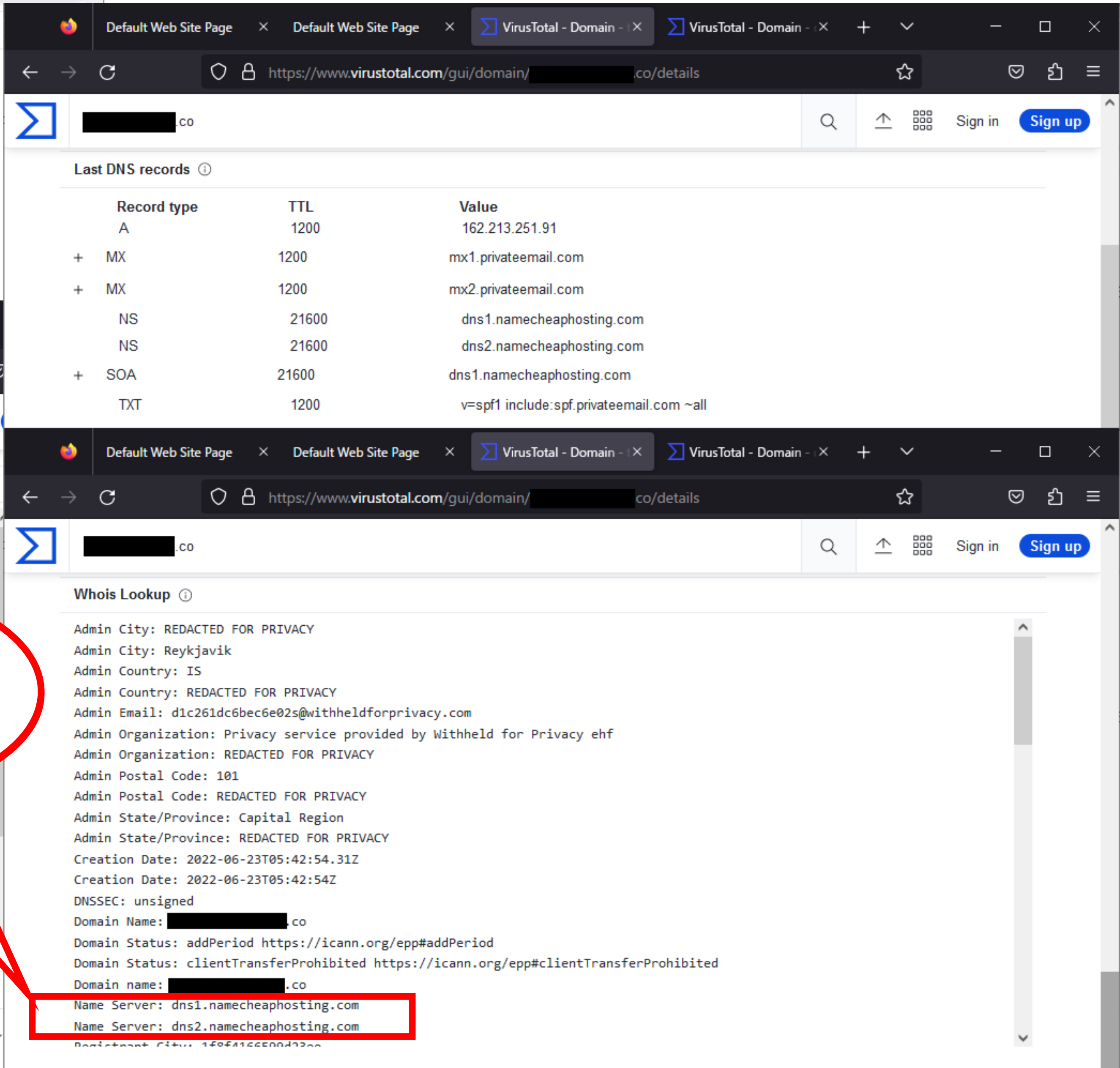
Whois Lookup

```
Administrative city: Reykjavik
Administrative country: Iceland
Administrative email: ab79b519c3075dd4s@withheldforprivacy.com
Administrative state: Capital Region
Create date: 2022-06-06
Domain name: [redacted]farm.com
Domain registrar id: 1068
Domain registrar url: http://www.namecheap.com
Expiry date: 2023-06-06
Name server 1: dns1.namecheaphosting.com
Name server 2: dns2.namecheaphosting.com
Query time: 2022-06-09 16:30:21
Registrant address: 8cad1b17b80fe86d
Registrant city: 3622c4e50647a4c5
Registrant company: 67f6e15f0fdcbd1c
Registrant country: Iceland
Registrant email: ab79b519c3075dd4s@withheldforprivacy.com
Registrant fax: 3267309318f7846c
Registrant name: a24fba8448b4e30a
Registrant phone: fefa39f0decc305e
Registrant state: 84287fd760bfb0b0
```

Google results

About 1 results (0.14 seconds)

Sort by: Relevance



Last DNS records

Record type	TTL	Value
A	1200	162.213.251.91
+ MX	1200	mx1.privateemail.com
+ MX	1200	mx2.privateemail.com
NS	21600	dns1.namecheaphosting.com
NS	21600	dns2.namecheaphosting.com
+ SOA	21600	dns1.namecheaphosting.com
TXT	1200	v=spf1 include:spf.privateemail.com ~all

Whois Lookup

```
Admin City: REDACTED FOR PRIVACY
Admin City: Reykjavik
Admin Country: IS
Admin Country: REDACTED FOR PRIVACY
Admin Email: d1c261dc6bec6e02s@withheldforprivacy.com
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Organization: REDACTED FOR PRIVACY
Admin Postal Code: 101
Admin Postal Code: REDACTED FOR PRIVACY
Admin State/Province: Capital Region
Admin State/Province: REDACTED FOR PRIVACY
Creation Date: 2022-06-23T05:42:54.31Z
Creation Date: 2022-06-23T05:42:54Z
DNSSEC: unsigned
Domain Name: [redacted].co
Domain Status: addPeriod https://icann.org/epp#addPeriod
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain name: [redacted].co
Name Server: dns1.namecheaphosting.com
Name Server: dns2.namecheaphosting.com
Registrant City: 1f8f4166500d23ee
```

Using the same name server

Abuse of Certificate Issuance Process might be happening

- At least, the applicants for the two certificates in this example are most likely to be the same.
- Other possibilities include, for example, a scenario in which a local software development company was contracted to develop a system for these two companies, received a code signing certificate on their behalf, and then had them stolen.
- But seems weird that they are interested in code signing but not hosting a website.
- Currently, still under investigation.

Revisit the History of abuse code signing

Date	Threat Actor	Key Point of Abuse	Victim	Note
2010	Stuxnet	Use the private keys stolen by famous companies	Realteck, JMicron	Link
2012	Flame	Collision of MD5 hash values by an unknown method.	Microsoft	Link1, Link2
2013	Zbot, Qakbot	Reported that they have functions for dumping certificates and private keys in PKCS#12	?	Link
2014	Destover	Private key was stolen and subsequently used to sign malware.	Sony Pictures Entertainment	Link
2015	menuPass	Leaked private key was used to sign malware.	HackingTeam	Link
2019	Nefilim Ransomware	Signed with a certificate of unknown origin Using a module(Similar to QAKBOT case)	A healthcare company	Link
2020	Robinhood Ransomware	Loading unsigned driver with BYOVD to stops process	GIGABYTE	Link

And then to 2022…

Now, transformation is expected

- Abuse is not easy, but it continues to show that it can be done if you try hard enough.
- Abuse of code-signed drivers has become a sweet spot for adversaries. The mood(I feel) has changed in 2022, especially as ransomware actors see the benefit of stopping security products such as anti-virus software as huge.
- PKI has been undergoing a lot of hardship for a long time, but the threats that have hit the code signing in the last few years have been really painful.
- We can expect that the abuse of code signing for PKI will continue, and we are on the eve of a transformation, but it might not be midnight yet.

Future

- If CT(Certificate Transparency) were also introduced into the process of issuing code signing certificates, the problems that WebPKI overcame earlier could be addressed, but there is no indication that this is being discussed at this time.
- After CABF CSBR "Malware based revocation" changes, the operation regarding revocation may change and should be monitored. However, there is no change in the difficulty of revocation verification.
- Regarding the method of private key theft/leakage or an attacker receiving certificate issuance, a hardware token will be required to issue code signing certificates starting in 2023/6, which may reduce abuse compared to the current method where the private key can be stored in the PKCS#12 file.
- “Application Store" is attractive from a security perspective, but platforms will become more powerful.
- New mechanisms for code integrity are beginning to be introduced. They should be a part of countermeasure of supply chain compromise, but the coverage is not yet wide enough.
  - Binary Transparency
  - sigstore
- This trend may lead to a transformation from traditional code signing with PKI to enabling verification of artifacts that are included in the supply chain to ensure integrity...

HITOMI KIMURA

Contact me anytime if you have questions!