コード署名 変革の前夜

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.

 ©2023 Trend Micro Inc.

2022年はコード署名受難の年でした

- 有効な署名付きドライバ悪用のレポートが続いた
- QAKBOTが有効な署名付き不正モジュールを配布

Date	Threat Actor	Key Point of Abuse	Victim	Note
2022/5	AvosLocker Ransomware	脆弱な署名ドライバを持ち込みアンチウイルスソフトを停止	Avast	Link
2022/7	QAKBOT	悪用された複数の証明書は攻撃者に直接発行されている可能性あり	Microcompanies	Link
2022/8	Cuba Ransomware	LAPSUSがリークしたNVIDIAの証明書と秘密鍵で署名したドライバを持ち込みアンチウイルスソフトを停止	NVIDIA	Link
2022/8	A ransomware actor	脆弱な署名ドライバを持ち込みアンチウイルスソフトを停止	Genshin Impact	Link
2022/9	Lazarus	脆弱な署名ドライバを持ち込みモニタリング機能を停止	Dell	Link
2022/12	POORTRY & STONESTOP	特定の開発者プログラムアカウントが不正なドライバを作成し署名を受けた	Microsoft	Link1, Link2, Link3, Link4

 ©2023 Trend Micro Inc.

多様なコード署名悪用のシナリオ(観測されたもの)

SEQ	Compromised Part	Key Point of Abuse
1	署名付きモジュール	脆弱な署名付きドライバの活用：BYOVD(Bring Your Own Vulnerable Driver)
2	サプライチェーン	サプライチェーンの危殆化で継続的インテグレーションの中に悪性コードが混入
3	サプライチェーン	開発者プログラムアカウントが不正なドライバを正規のドライバとして作成
4	秘密鍵	正規に発行された証明書と秘密鍵の盗難、リーク
5	RAの一部	攻撃者が他人が所有する実在の企業になりすまして証明書発行を受けている可能性がある。(まだ調査中)
6	RAの一部	攻撃者が会社を用意して証明書発行を受ける
7	アルゴリズム	MD5ハッシュ値の衝突による証明書の偽造

CAのCompromiseはまだない：2011年にWebPKIで起きた、攻撃者がRAを掌握してCAから発行を受ける事例(例: Comodo, DigiNotar)はコード署名証明書に対してはまだ見られないが、2022年現在ではドライバ署名を得ることへの攻撃者のモチベーションが高まっているため次があればそれは起こるだろうと予見される。

 ©2023 Trend Micro Inc.

改めて照らされる問題点①

- コード署名悪用ではおそらくみなさんの期待通り機能しない証明書失効
  - 失効しないよりしたほうがましであることは確かだが
  - 正規の証明書で署名された正規のモジュールが悪用されるシナリオでは
    秘密鍵が危殆化していないため(現行の運用では)証明書は失効されない可能性が高い
  - 仮に証明書が失効されたとしても、コンピュータ上での実行が
    証明書失効の検証によりブロックされるかどうかはコンディション次第
  - 「証明書失効されたモジュールが組織内のすべてのコンピュータで
    実行されないこと」を検証し自信を持つことが難しい
  - CABFでの「Malware based revocation」の議論 (2022/6～2022/12、可決されたが未マージ)
    - 失効事由確認後、CAからサブスクライバへの連絡が「1営業日」だったものを「24時間」へ変更するなどよりプラクティカルな運用を目指している様子
    - 署名ドライバの悪用やSolarWinds事例を例にどうするかも議論されたが次の事例で具体的にどうなるかの言及はなし
    - このテーマについて議論している2022/12/01の議事録は見ごたえあり

 ©2023 Trend Micro Inc.

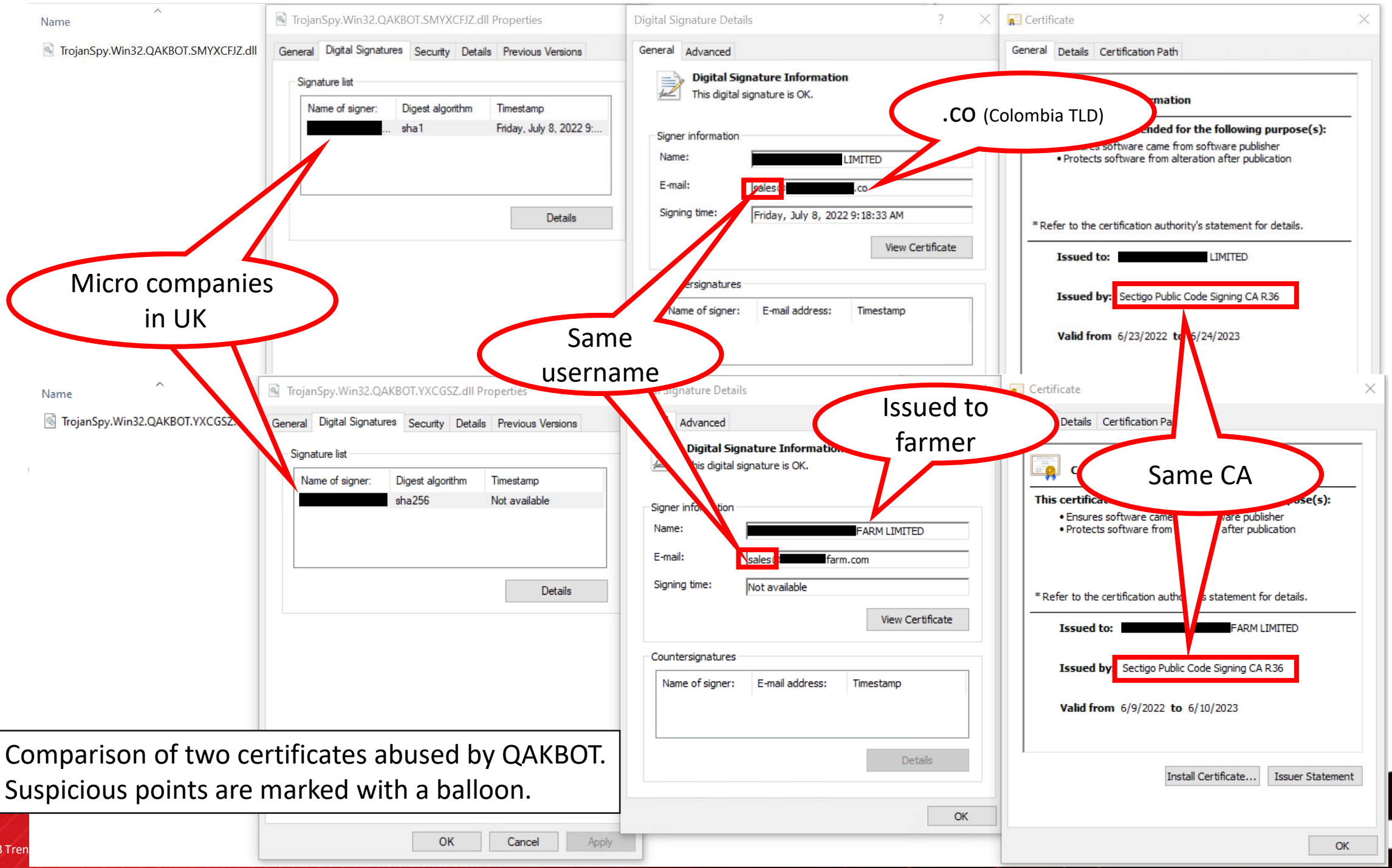
改めて照らされる問題点②

- 証明書発行プロセスの悪用が疑われる
  - 1枚かごく少数の盗まれた証明書をAPTで使われるのが
    コード署名悪用のよく知られるシナリオだったが…
  - 2022年7月ごろ、QAKBOTによる有効な署名付きモジュールの
    配布が確認され、詳しく調べると7枚の証明書利用を確認した
  - 悪用された証明書の内容を確認すると奇妙な点があり、
    攻撃者が身分証を偽るなどしてCAから直接証明書発行を
    受けている可能性を考えさせる

 ©2023 Trend Micro Inc.

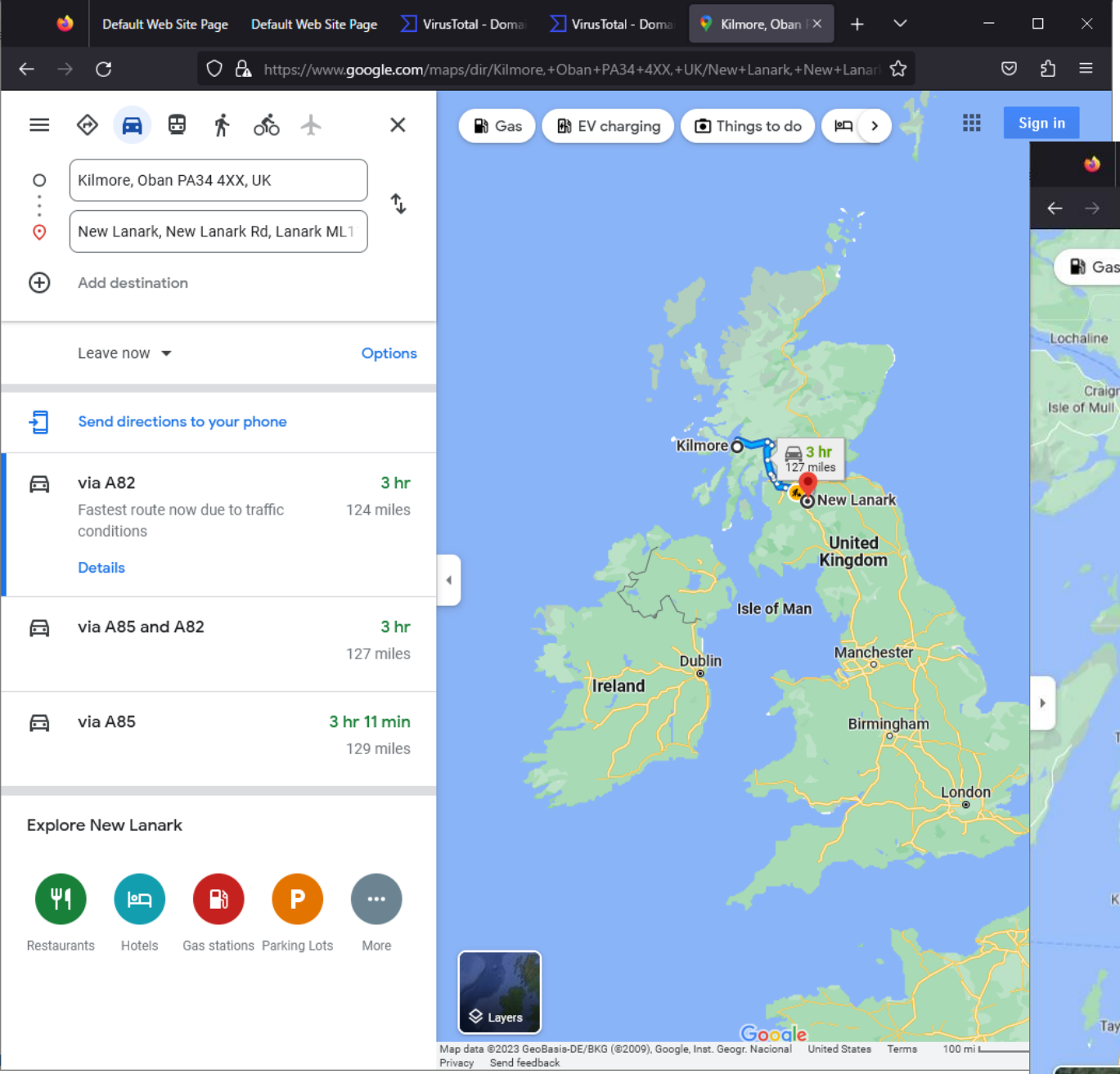
Dive into Abused Certificates

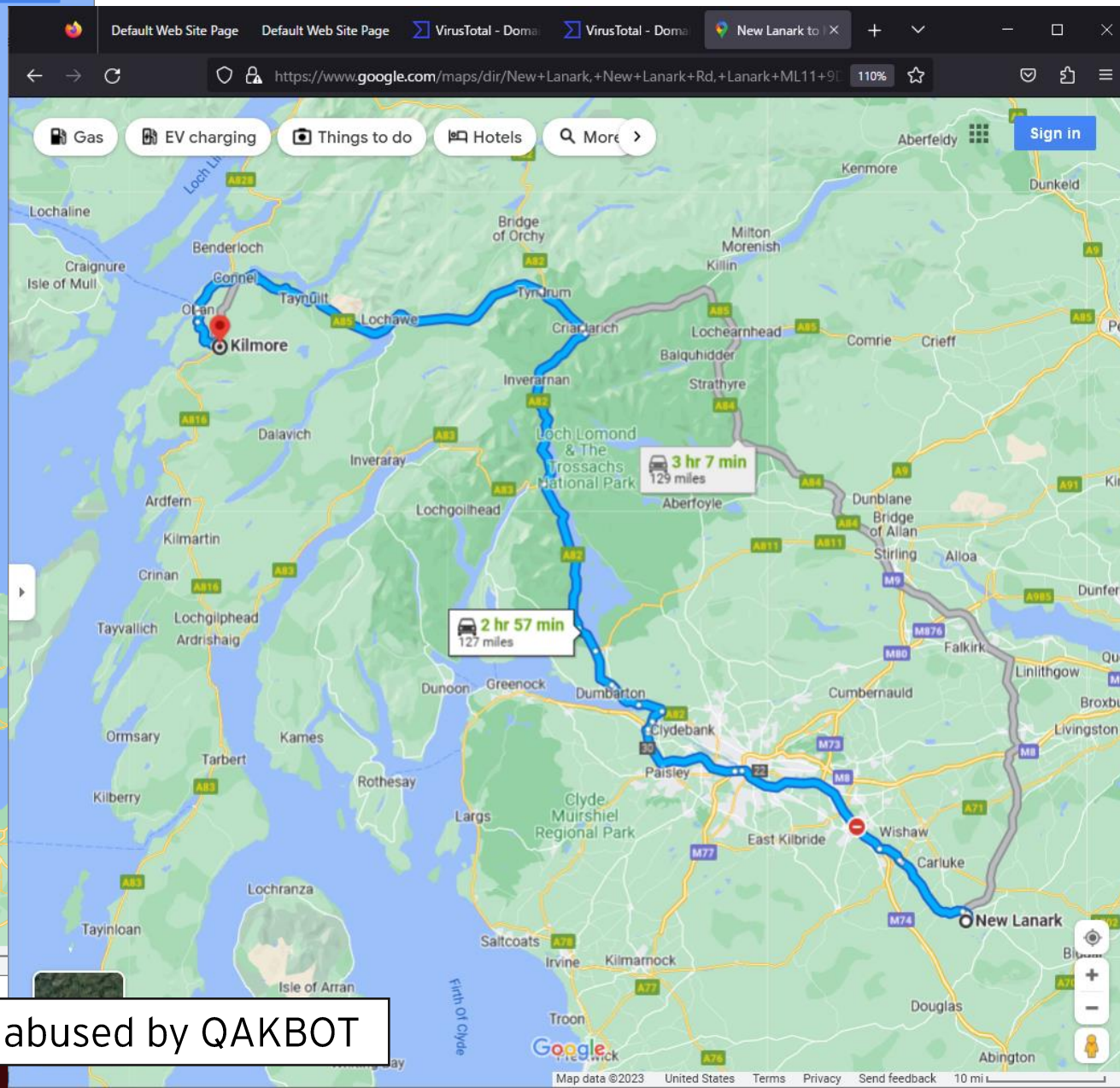
TREND MICRO



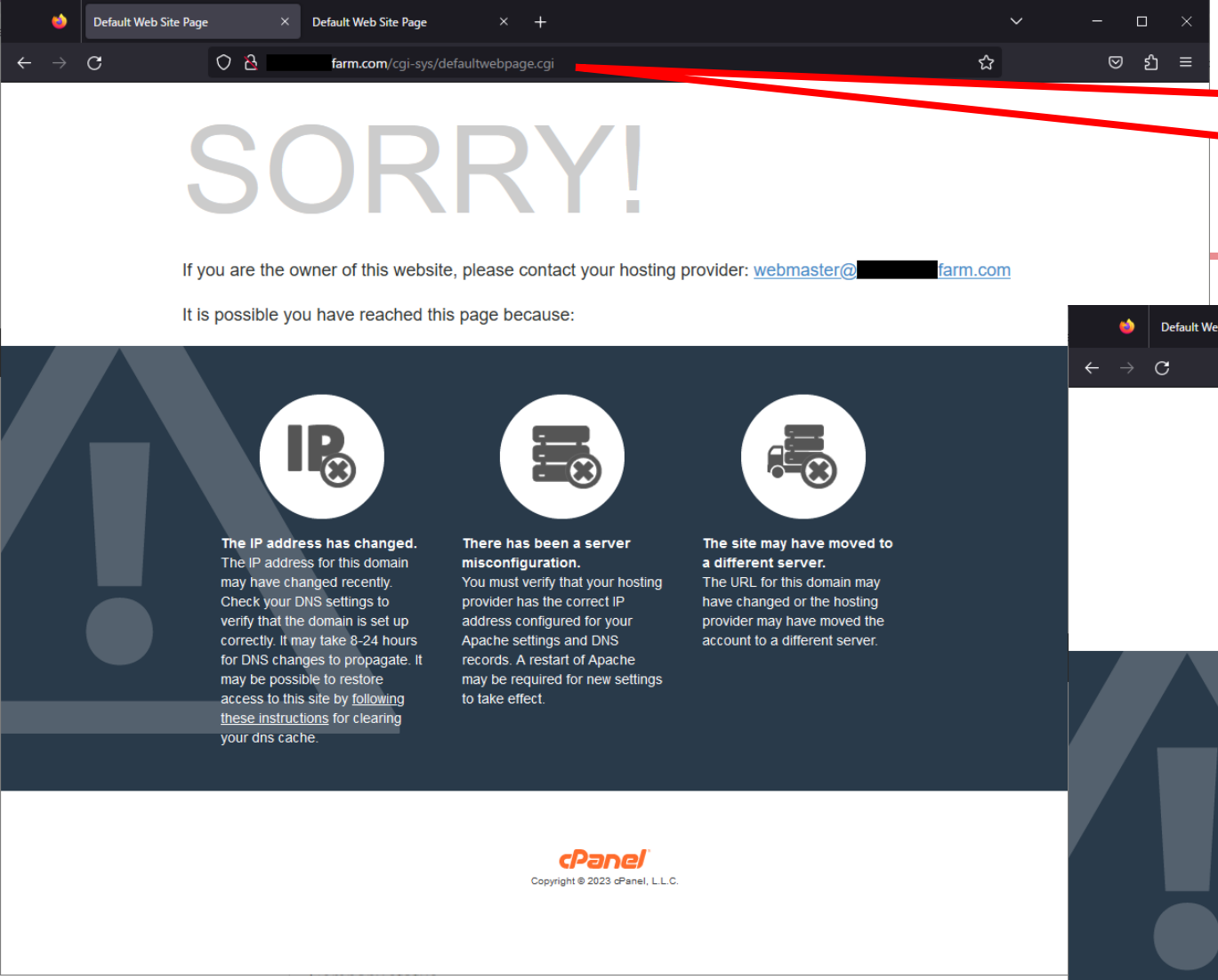
Comparison of two certificates abused by QAKBOT.
Suspicious points are marked with a balloon.

3hours, approx. 200km away

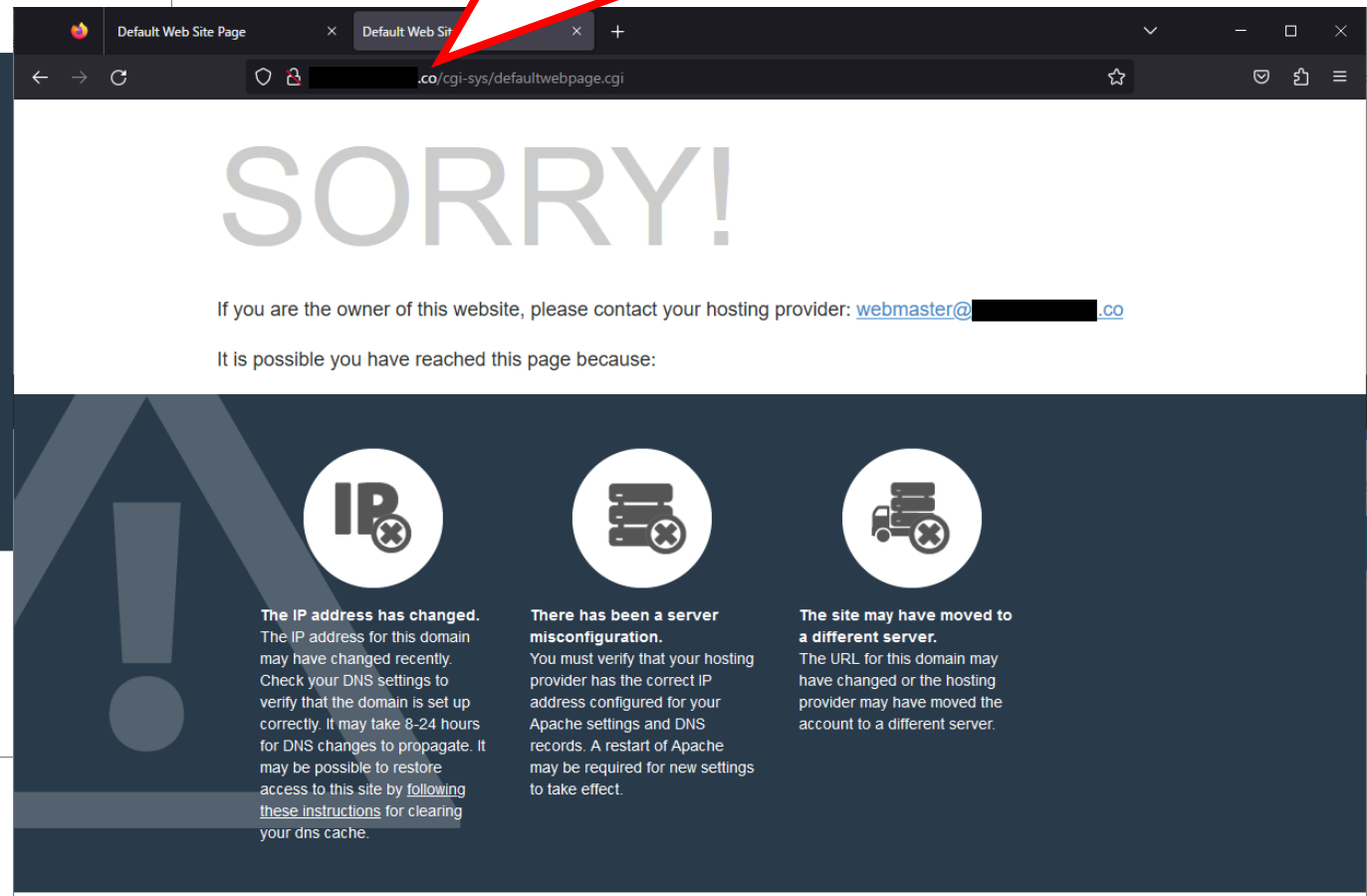




How far apart are the two companies in the certificates abused by QAKBOT



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



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

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

Default Web Site Page | Default Web Site Page | VirusTotal - Domain - | VirusTotal - Domain -

https://www.virustotal.com/gui/domain/[redacted]farm.com/details

[redacted]farm.com

Sign in | Sign up

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

Default Web Site Page | Default Web Site Page | VirusTotal - Domain - | VirusTotal - Domain -

https://www.virustotal.com/gui/domain/[redacted]farm.com/details

[redacted]farm.com

Sign in

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
```

Google results

About 1 results (0.14 seconds)

Sort by: Relevance

Using the same name server

Default Web Site Page | Default Web Site Page | VirusTotal - Domain - | VirusTotal - Domain -

https://www.virustotal.com/gui/domain/[redacted]co/details

[redacted].co

Sign in | Sign up

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

Default Web Site Page | Default Web Site Page | VirusTotal - Domain - | VirusTotal - Domain -

https://www.virustotal.com/gui/domain/[redacted]co/details

[redacted].co

Sign in | Sign up

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
```

証明書発行プロセスの悪用が疑われる

- 今回例示した2つの証明書の申請者は同じある可能性が高い
- 他の可能性として例えば、地域のソフトウェア開発会社がこの2つの会社のシステム開発を請け負って代わりにコード署名証明書の発行を受けた後それを盗難されたシナリオが考えられるが、コード署名に興味があるのにWebサイトをホストしていないのは奇妙に思える
- 現在調査中

 ©2023 Trend Micro Inc.

Revisit the History of abuse code signing

Date	Threat Actor	Key Point of Abuse	Victim	Note
2010	Stuxnet	有名企業から盗難された秘密鍵の使用	Realteck, JMicron	Link
2012	Flame	未知の探索手法による MD5ハッシュ値の衝突	Microsoft	Link1, Link2
2013	Zbot, Qakbot	PKCS#12形式で証明書と秘密鍵を ダンプする機能ありとレポート	?	Link
2014	Destover	秘密鍵が盗難されその後 マルウェア署名に利用された	Sony Pictures Entertainment	Link
2015	menuPass	リークされた秘密鍵が マルウェア署名に利用された	HackingTeam	Link
2019	Nefilim Ransomware	出所不明の証明書で署名された モジュールを使用	A healthcare company	Link
2020	Robinhood Ransomware	脆弱な署名ドライバで未署名ドライバ を読み込みプロセス停止	GIGABYTE	Link

そして2022年へ・・・

 ©2023 Trend Micro Inc.

いま変革が求められている

- 悪用は簡単ではないが、頑張ればできてしまうことが示され続けている
- 署名付きドライバのAbuseは攻撃者にとってスイートスポットになっている。特にランサムウェアアクターはアンチウイルスソフトなどのセキュリティ製品を停止させるベネフィットを大きくとらえていると想像させる。2022年でムードが変わったと感じる。
- PKIはずっと受難続きだが、その中でもここ数年のコード署名を襲う脅威は本当に苦しいものばかり
- Abuseはこれからも続くことが予見され、変革の前夜だがまだ全然夜が明ける気配がない

今後の展望

- コード署名証明書の発行プロセスにもCTが導入されればWebPKIが先に乗り越えてきた問題には対処できるようになるが、現在のところ検討されている様子はない
- CABF CSBRが「Malware based revocation」の変更を取り込んだ後、失効に関する運用が変化する可能性があるため要観察。しかし失効検証が難しい点には変化はない
- 秘密鍵の盗難・リークや攻撃者が証明書発行を受ける方法での悪用については、2023/6からコード署名証明書の発行にはハードウェアトークンが必須となるため、秘密鍵ごとPKCS#12ファイルに保管できる現在よりは悪用が減る可能性はある
- 「ストア方式」は安全確保の面で魅力があるがプラットフォームの力が強くなる
- サプライチェーンの危殆化への備えも含め、コードインテグリティについて新しい仕組みが導入され始めているが適用範囲はまだ広くない
  - Binary Transparency
  - sigstore
- この流れが、従来型のPKIによるコード署名からサプライチェーン全体で登場するアーティファクトの検証を可能にしインテグリティを確保するという方向性への変革の萌芽となるか

HITOMI KIMURA

Contact me anytime if you have questions!

©2023 Trend Micro Inc.