QWACs in the internet ecosystem

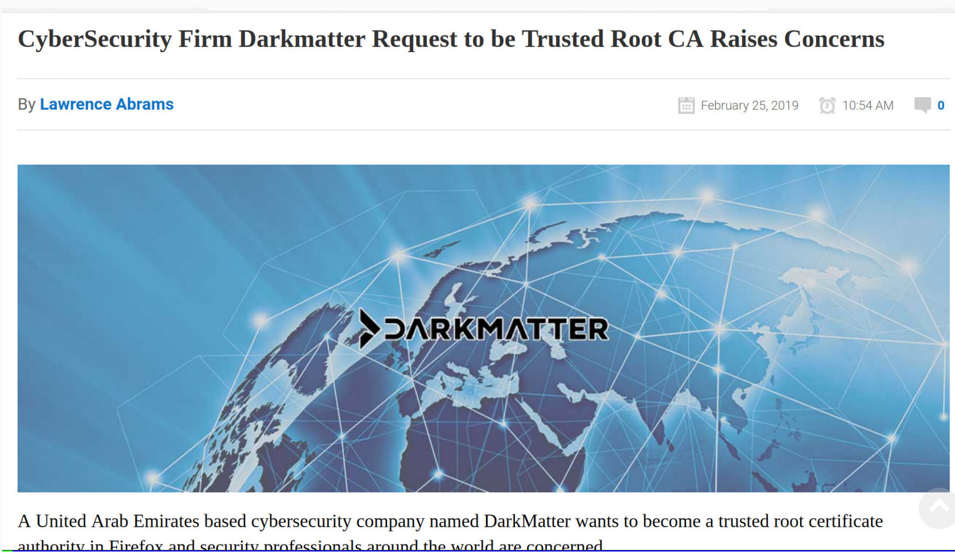
Tanja Lange [1] Benjamin Beurdouche [2]

May 10, 2022

[1] Eindhoven University of Technology

[2] Mozilla Paris

Big issues: Governance and trust



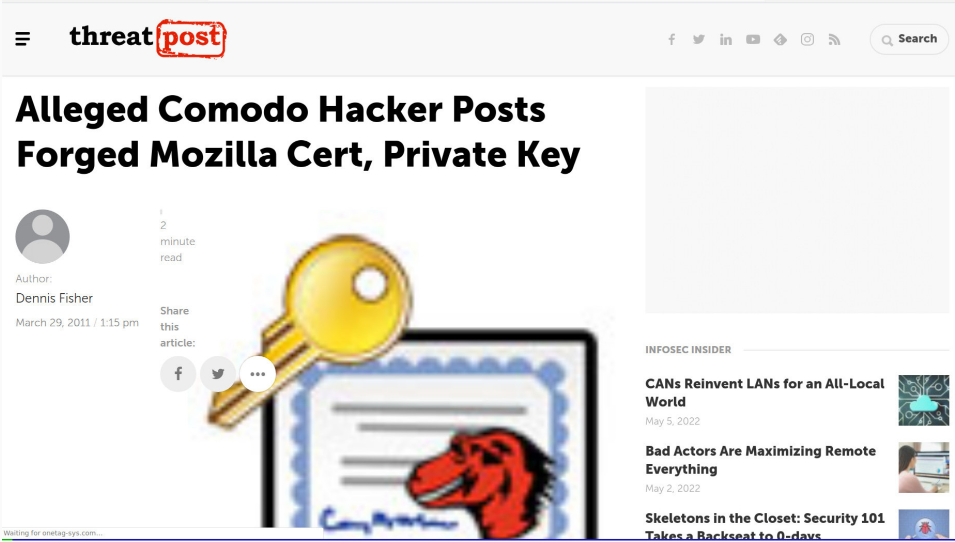
CyberSecurity Firm Darkmatter Request to be Trusted Root CA Raises Concerns

By **Lawrence Abrams** February 25, 2019 10:54 AM 0

A United Arab Emirates based cybersecurity company named DarkMatter wants to become a trusted root certificate authority in Firefox and security professionals around the world are concerned.

`https://www.bleepingcomputer.com/news/security/cybersecurity-firm-darkmatter-request-to-be-trusted-root-ca-raises-concerns/`

. . . and (sadly) for good reasons . . .



Alleged Comodo Hacker Posts Forged Mozilla Cert, Private Key

2 minute read

Author:
Dennis Fisher
March 29, 2011 / 1:15 pm

Share this article:

INFOSEC INSIDER

CANs Reinvent LANs for an All-Local World
May 5, 2022

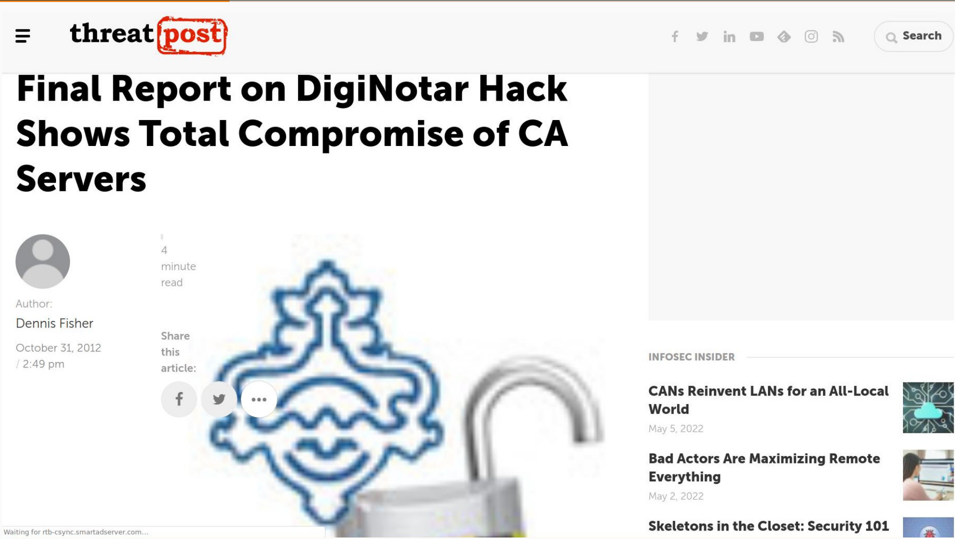
Bad Actors Are Maximizing Remote Everything
May 2, 2022

Skeletons in the Closet: Security 101 Takes a Backseat to 0-days

Waiting for onetag-sys.com...

https://threatpost.com/alleged-comodo-hacker-posts-forged-mozilla-cert-private-key-032911/75077/

. . . also in the Netherlands



Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

Author:
Dennis Fisher

October 31, 2012 / 2:49 pm

4 minute read

INFOSEC INSIDER

CANs Reinvent LANs for an All-Local World
May 5, 2022

Bad Actors Are Maximizing Remote Everything
May 2, 2022

Skeletons in the Closet: Security 101

`https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/`

Comment on flaws with implementation model

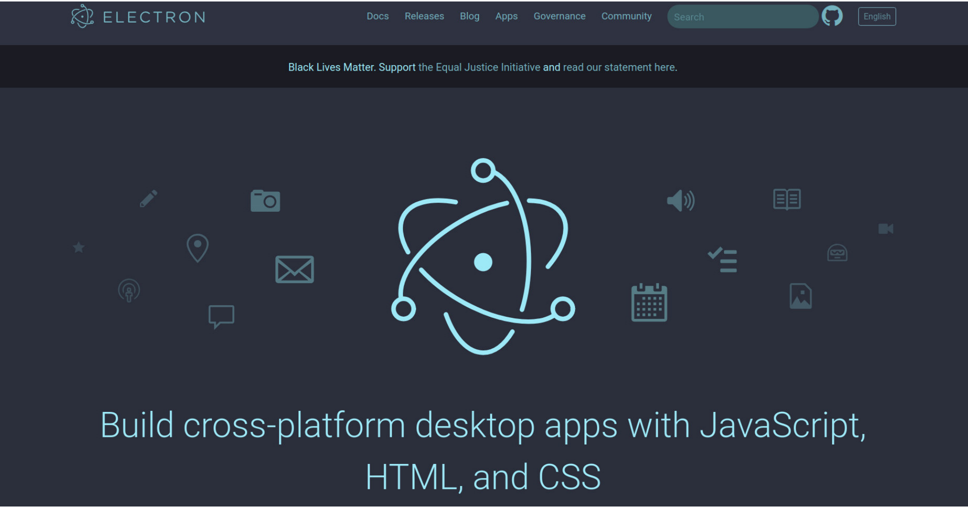
I was asked to comment on

> *(QWACs) [..] which – owing to flaws with its technical implementation model – has not gained popularity in the web ecosystem.*

Disclaimer: I don't know why adoption is low but can speculate.

- QWACs run into same problem as EV certificates.
- What do they show? (Is Strip inc. based in Kentucky?)
- Do users actually check?
- Backwards compatibility requires maintaining two versions. This opens a new attack avenue.
- Web pages, browsers, and TLS ecosystem do not match model of what is authenticated.

Alternative: Standalone app



Black Lives Matter. Support the Equal Justice Initiative and read our statement here.

Build cross-platform desktop apps with JavaScript, HTML, and CSS

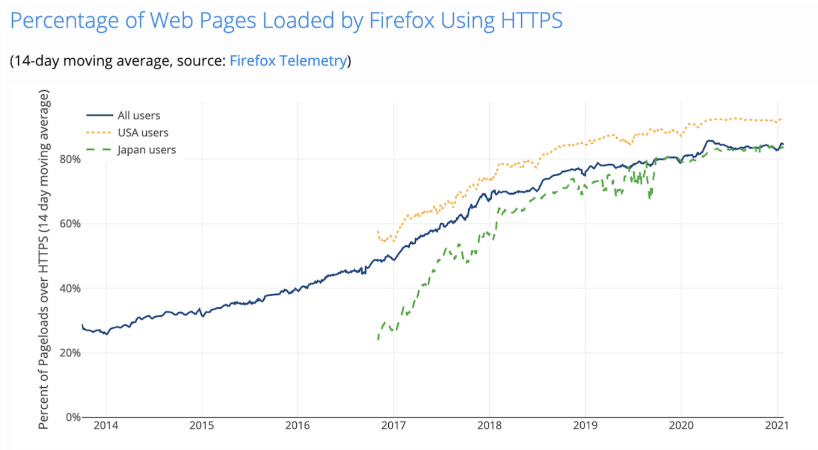
But more effort to develop, higher barrier to adoption, and divergence from normal web ecosystem.

Part 2.

Overview

- Browser CA root stores provide the **authentication** for Transport Layer Security (TLS), upon which modern web security (HTTPS) is built.
- The security of the internet is **under increasing attacks** from state actors globally, which want to man-in-the-middle web traffic. (Kazakhstan, Mauritius, India)
- Proposed regulation on electronic identification in Europe (i.e. eIDAS) would **mandate browsers to trust** TSPs authorised by each member state.

TLS Adoption



Percentage of Web Pages Loaded by Firefox Using HTTPS

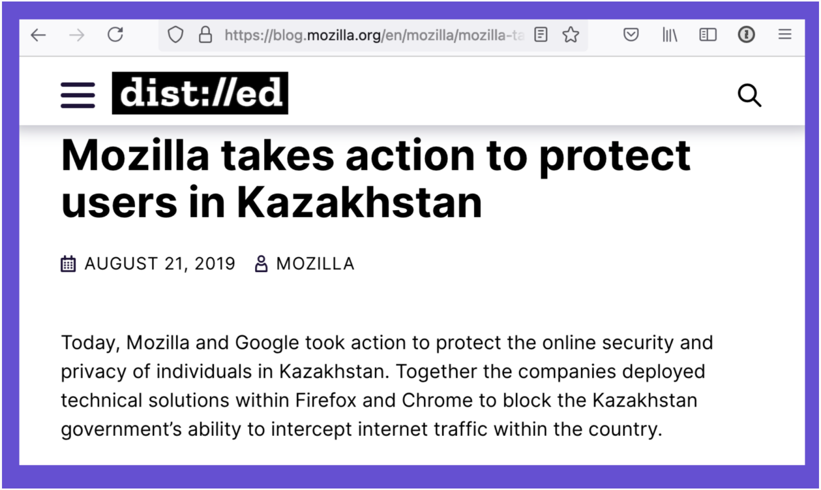
(14-day moving average, source: Firefox Telemetry)

Certificate Authorities & Root Store Programs

1. CAs grant websites the ability to authenticate servers, using a certificate issued by the CA. Commonly used for HTTPS.
2. Browser Root Store programs define and enforce rules for trusting Certificate Authorities.
   - Each browser maintains a list of CAs that satisfy extensive audit and policy criteria.
   - When CAs fail to follow the rules, data (e.g. bank account passwords, CCNs) is at risk.

CA root stores are operated publicly and discussion is open.

Internet is under attack by malicious actors



Mozilla takes action to protect users in Kazakhstan

AUGUST 21, 2019 MOZILLA

Today, Mozilla and Google took action to protect the online security and privacy of individuals in Kazakhstan. Together the companies deployed technical solutions within Firefox and Chrome to block the Kazakhstan government's ability to intercept internet traffic within the country.

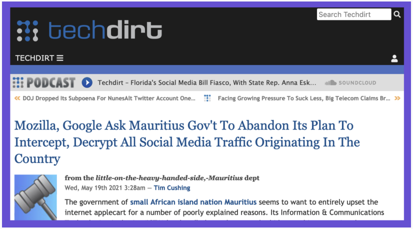
Mozilla's concerns with Article 45: direct risk to users globally

Automatically recognizing root certificates from the member states (as eIDAS mandated TSPs) is a security risk to users, both from mismanagement and misuse:

1. Especially in the context of man-in-the-middle attacks.
2. Each member state will establish its own list of qualified CAs, introducing multiple points of failure.
3. Browsers will lack transparency into what standard a CA has met and will lack rapid recourse if a TSP acts maliciously.
4. Nothing requiring that the corresponding standards meet baseline requirements for security or be maintained and improved.

Mozilla’s concerns with Article 45: setting a harmful precedent

Browsers will be unable to push back on proposals like we saw in Mauritius when the EU has set the norm that these approaches are acceptable.



Techdirt – Florida's Social Media Bill Fiasco, With State Rep. Anna Esk...

« DOJ Dropped Its Subpoena For NunesAlt Twitter Account One... Facing Growing Pressure To Suck Less, Big Telecom Claims Br... »

Mozilla, Google Ask Mauritius Gov't To Abandon Its Plan To Intercept, Decrypt All Social Media Traffic Originating In The Country

from the *little-on-the-heavy-handed-side,-Mauritius* dept

Wed, May 19th 2021 3:28am — Tim Cushing

The government of small African island nation Mauritius seems to want to entirely upset the internet applecart for a number of poorly explained reasons. Its Information & Communications

While the stated intent is different, the technical details of what the EU and Mauritius are proposing are the same.

The state of TSPs in the Mozilla Root Store

Many TSPs are already trusted Root CAs (April 2022):

- 22 QWAC TSPs included
- 4 QWAC TSPs removed (2 - ongoing/systemic problems; 2 - CA's decision)
- 7 QWAC TSPs in root inclusion process
- 1 QWAC TSP had their root inclusion request denied
- 4 QWAC TSPs withdrew their request
- 20 QWAC TSPs have not applied for inclusion

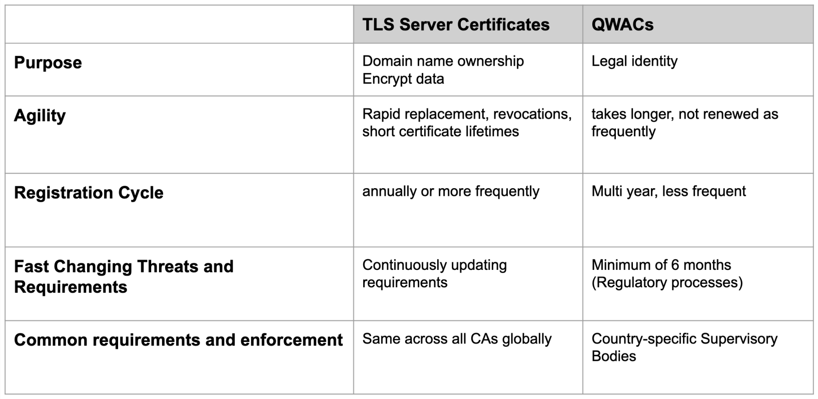
Conclusions

Our main concern is for the security and privacy of internet users. **We think that mandatory trust of TSPs outside the normal root store processes will lead to many security issues.**

Independently from the value of QWACS,
We can define technical solutions that don't regress the security benefits gained over the last decades by being separate from TLS and the Root Store processes.

Thank you!

Comparison of QWACs and TLS Server Certificates



	TLS Server Certificates	QWACs
Purpose	Domain name ownership Encrypt data	Legal identity
Agility	Rapid replacement, revocations, short certificate lifetimes	takes longer, not renewed as frequently
Registration Cycle	annually or more frequently	Multi year, less frequent
Fast Changing Threats and Requirements	Continuously updating requirements	Minimum of 6 months (Regulatory processes)
Common requirements and enforcement	Same across all CAs globally	Country-specific Supervisory Bodies

Mozilla's concerns with Article 45: UX in the address bar

Browsers have removed EV information from the address bar because:

- Organizational identity information provided in a certificate may be misleading. EV certs are used on Phishing sites.
- Research has found that EV indicators in the address bar do not provide value and security benefits, and only create more noise that consumers ignore.
- Different types of SSL/TLS certificates all serve a single purpose: to encrypt the communication between a browser and web site. Anything else is a marketing gimmick to charge customers more.