PCH
Packet Clearing House

Briefing on Dec 2018 - Jan 2019 DNS/IMAP Prepositioning Attacks

Saturday May 11, 2019
ICANN DNS Symposium

Bill Woodcock
Executive Director
Packet Clearing House

References

Cisco/Talos:

https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://blog.talosintelligence.com/2019/04/seaturtle.html

DHS:

https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign
https://cyber.dhs.gov/blog/#why-cisa-issued-our-first-emergency-directive
https://cyber.dhs.gov/ed/19-01/

GCHQ:

https://www.ncsc.gov.uk/content/files/protected_files/article_files/Alert-DNS-hijacking.pdf

Mandiant/Fireeye:

https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

Ars Tech:

https://arstechnica.com/information-technology/2019/01/multiple-us-gov-domains-hit-in-serious-dns-hijacking-wave-dhs-warns/
https://arstechnica.com/information-technology/2019/01/a-dns-hijacking-wave-is-targeting-companies-at-an-almost-unprecedented-scale/

Targets

- Many national governments, mostly middle-eastern
- A few Internet critical infrastructure operators (IXPs and root & TLD nameservice)
- All military cyber-offense prepositioning

Timing

- Coincides with end-of-year shutdown of Middle Eastern governments for expat holiday travel.
- USG shutdown was coincidental.
- Timing was very effective

Structure of the Attack

DNS Hijack

- Registrar EPP credential found in spoils of an attack against a third party
- Registrar - Registrar Wholesaler - Registry
  - No due-diligence to determine whether change was authorized
- NS (but not DS) records changed four one-hour periods Dec 13, 14, and Jan 2
- Authoritative DNS proxy gives false answers to Comodo
- Other queries proxied using answers obtained from 8.8.8.8
- Comodo “domain validation” SSL certificate issued
  - No due-diligence to determine whether change was authorized
  - (priors used Let’s Encrypt, which *does* do DNSSEC validation)

IMAP Hijack

- SSL cert put into IMAP proxying infrastructure
- IMAP logins intercepted, credentials harvested
  - SMTP traffic in/out collaterally intercepted during hijack periods
- Mailboxes, vCards, vCals exfiltrated

Warning Signs

- DNSSEC-validating IMAP clients were unable to connect to mail server during brief hijack periods.

- Proxied inbound SMTP all came from a single source during the hijack windows, which meant that all inbound spam was also coming from single source, so that source immediately got graylisted and shut off.

- Hypothetically, inbound queries to authoritative DNS servers should have been more geographically concentrated during the hijack periods, but this didn’t stand out notably in the data.

Defenses

Actual:

- DNSSEC signing / DNSSEC validation
- Walking NS/DS delegation from the root
- Registry Lock
- IMAP server not reachable from the Internet
- More structural separation between services

Hypothetical:

- Cert pinning
- MDM to lock recursive resolver
- DANE authentication of the IMAP server

New Tool

Walking NS/DS delegation from the root

New Tool

Walking NS/DS delegation from the root

We began visually graphing DNS dependencies for domains we're responsible for, and it turns out that the status-quo for nearly all domains is very, very bad.

Anything critical needs to be registrar locked, registry locked, and DNSSEC signed, and that needs to be true for *every dependency*. Then you need to actually DNSSEC validate (ideally client-side) and use DANE to authenticate servers, not CA certs.

Thanks, and Questions?

Bill Woodcock
Executive Director
Packet Clearing House
woody@pch.net
+1 415 831 3103