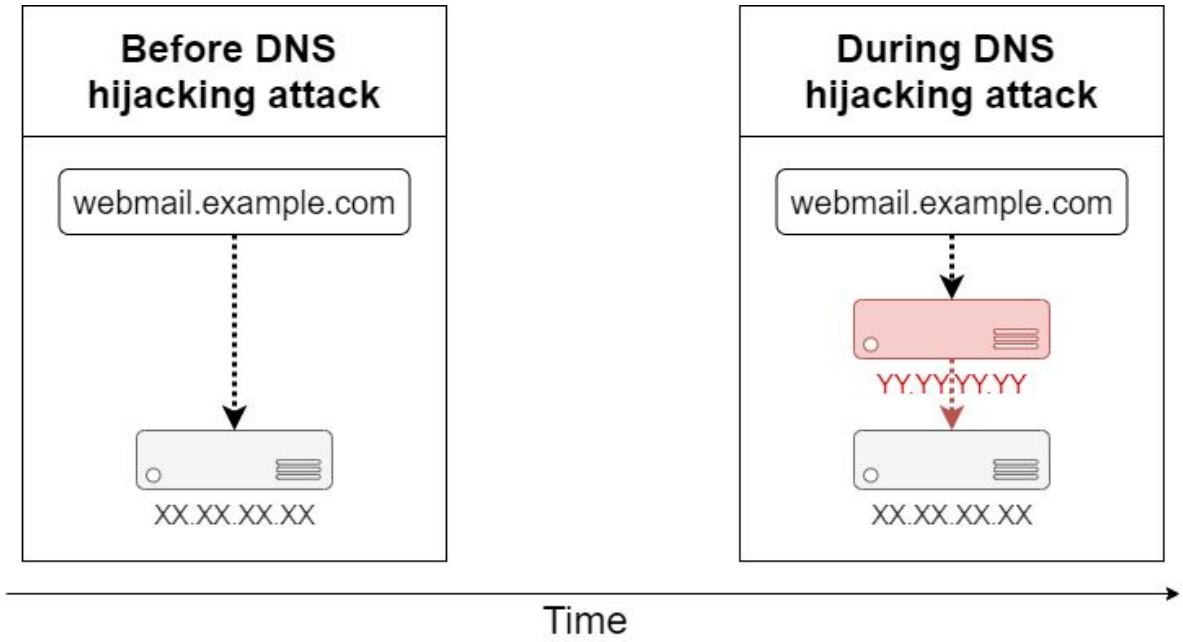
Large-scale Indirect DNS Hijacking Detection using HTTPS Scan Data

Thesis presentation for master in Security & Network Engineering

Student Niels Warnars
Supervisor C. Veenman (NCSC-NL)

Background

1. DNS records compromised at domain registrar
2. Traffic gets redirected to malicious (MitM) server, e.g. for credential harvesting



Current work / publications

- Analyses of previous hijacking incidents
  - Fox-IT (2017)
  - CrowdStrike / FireEye / Cisco Talos (2019)

- DNS hijacking detection by monitoring for DNS changes
  - Aimé, researcher at Kaspersky (2019)
  - Braun (2016)

Limitations

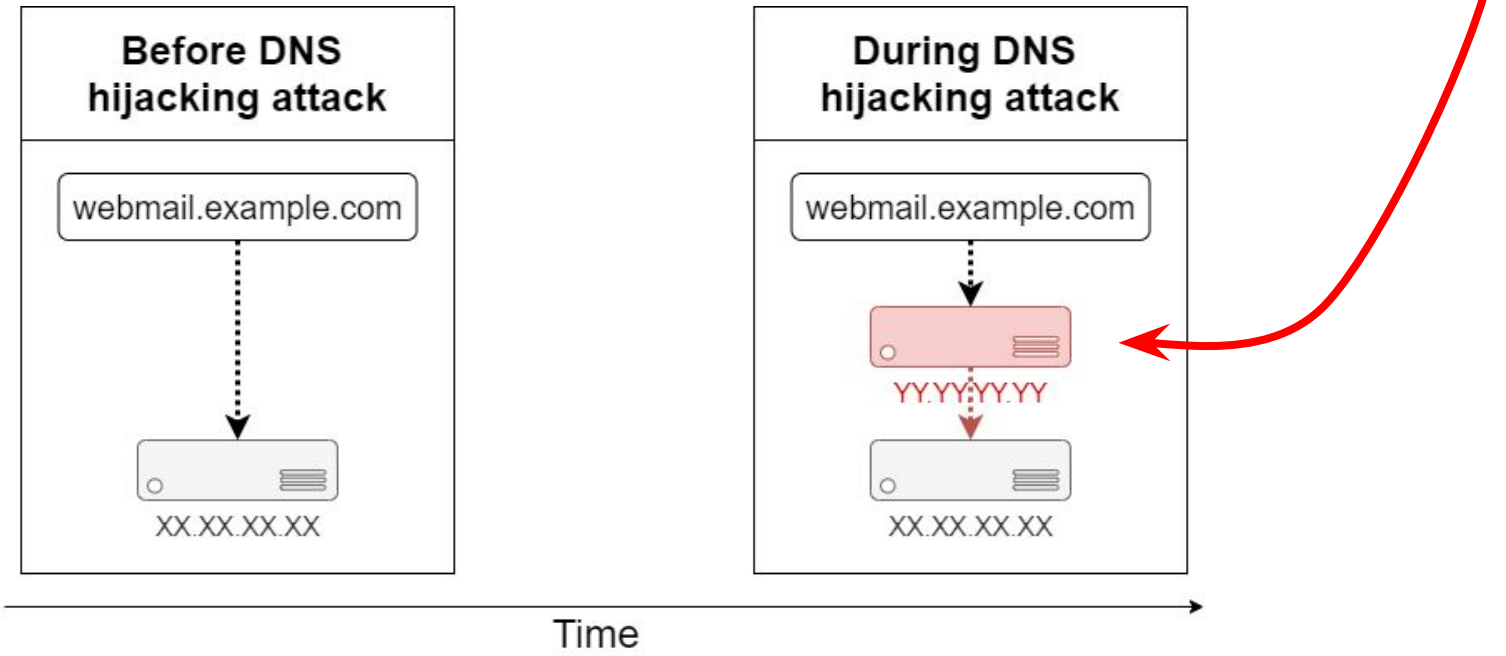
- Analyses of previous hijacking incidents:
  - No research method published by CrowdStrike / FireEye / Cisco Talos

- DNS hijacking detection by monitoring for DNS changes:
  - Only works by monitoring fixed list of domains
  - Only works in real time (unless passive DNS is used)

- Method wanted that:
  - works without predefined target list
  - uses readily available data sets (= internet-wide scans)
  - can be used to identify historic hijacking incidents

Research idea

- **Attempt to detect new attacker-controlled server with scan data**



Example: Hijacking case from November 2018

- **mail.petroleum.gov.eg**
- MitM server: 206.221.184.133

- Same page exposed by original targeted server

ssl.cert.serial:	301078028659410558591678396364699753741233
ssl.cert.notbefore:	2018-11-20 14:50:54
ssl.cert.notafter:	2019-02-18 14:50:54
ssl.cert.issuer:	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
ssl.cert.subject:	CN=mail.petroleum.gov.eg

http.status:	200
http.title:	Outlook Web App
http.html_hash:	31204603
http.robots_hash:	None
http.favicon.hash:	1768726119

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
request-id: 6f61e2e8-e44e-4659-b89a-52ec8ccb9595
Set-Cookie: ClientId=DFOQNXHKYFGBKUXIMYW; expires
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 27 Nov 2018 09:25:25 GMT
Content-Length: 56264
```

Sources:

- Hijacking case: CrowdStrike
- Scan data: Shodan

Research Questions

- *Can DNS hijacking attacks be detected indirectly by identifying the attacker-controlled MitM servers using internet-wide HTTPS scan data?*

- Sub questions:
  - *What properties characterise previously-documented DNS hijacking attacks?*
  - *How can internet-wide HTTPS scan data be filtered to potentially identify new attacker-controlled MitM servers?*
  - *How do different filtering methods compare with regard to coverage?*

Methodology

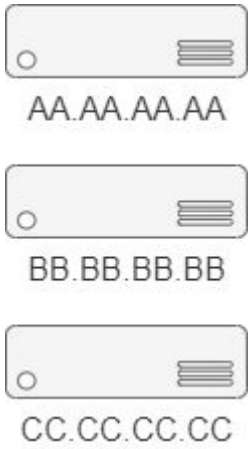
Parts of research

- Part 1: Analyse 50 hijacking incidents documented by Crowdstrike / Cisco
- Part 2: Design and implement detection system
- Part 3: Validate implementation by hunting for historic hijacking incidents

Construction of detection system

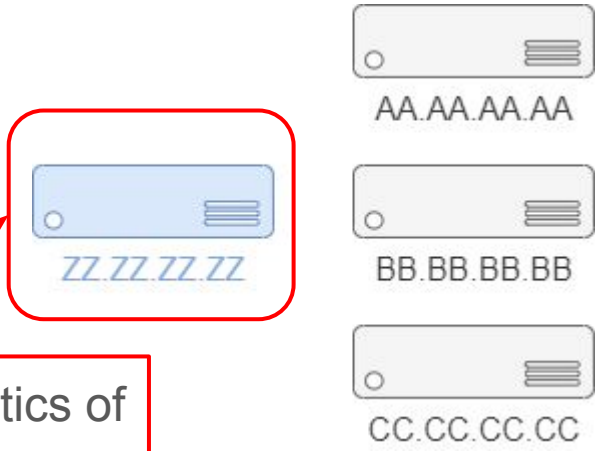
Base state

- Servers on 2020-10-19



Diff analysis

- New servers on 2020-11-02



Check for characteristics of DNS hijacking MitM server

Hunting for previous hijacking attacks

- Time period: Jan 2018 - Nov 2020 (= 73 scans)
- Data source: Rapid7

- Parsed / processed data:
  - 460 million certificates
  - 2.4 billion HTTP responses / HTML pages

Data sources

Data provider	**Data type**
crt.sh (CT Logs)	Historic certificates
RiskIQ	Historic certificates Historic passive DNS
VirusTotal	Historic passive DNS
Shodan	Historic scan records
Rapid7	Historic scan records

Data parsing/preprocessing for detection system

Certificates

- Only CA-issued certificates
- Only way to ensure integrity of subject alternative names

HTTP responses

1. Header hash
2. Body hash
3. Page structure hash

Results

Analysis of old hijacking incidents

Choice of hoster

- No clear pattern:
  - Legitimate hosters
  - Low-reputation hosting providers

Sources old hijacking cases:

- CrowdStrike / Cisco Talos

AS Name	AS Number	Count (total=26)
DigitalOcean, LLC	AS14061	9
Choopa, LLC	AS20473	6
myLoc managed IT AG	AS24961	2
DataShack, LC	AS33387	2
Zemlyaniy Dmitro Leonidovich	AS42159	2
BelCloud Hosting Corporation	AS44901	2
ReliableSite.Net LLC	AS23470	1
Linode, LLC	AS63949	1
KANARTEL	AS33788	1

Analysis of old hijacking incidents

ASN / Country difference of MitM server relative to targeted server

- Different ASN: 50 / 50 cases
- Different country: 45 / 50 cases

Certificates on MitM servers (or in CT logs)

- New DV certificate: At least 40 / 50 cases
- Stolen certificate: At least 22 / 50 cases

HTTP responses on MitM servers

- Full cloning / proxying: At least 24 / 50 cases

Note: Not in all cases data was available in Shodan / RiskIQ

Detection system - Basis for filters

1. Newly initialised server
2. Newly issued DV cert for existing domain

3. New Autonomous System for existing domain
4. New country of hosting for existing domain

5. Fully proxied / cloned HTTP responses

Detection system - Statistics

Data set	Count
2020-10-19 scan - IPs with CA-issued cert	25.529.372
2020-11-02 scan - IPs with CA-issued cert	25.665.581

Filter step	Count
Filter (step 1) - New servers	2.612.405
Filter (step 2) - Step 1 + New DV certs	602.648
Filter (step 3) - Step 2 + Existing fully qualified domain names ● Also takes into account wildcard certificate matches	114.210

Detection system - Statistics

Filter step (+= New ASN for existing domain)	**Count**
Filter (step 4a) - Step 3 + new ASN ● Only ASNs under matching FQDN / wildcard domain	24.800
Diff (step 4b) - Step 3 + new ASN ● **ASNs under second-level domain**	**14.955**

Trade-off between risk of false positives and count reduction

Detection system - Statistics

Filter step (+= Previously observed HTTP responses)	**Count**
Filter (step 5a) - Step 4b + page hash	4297
Filter (step 5b) - Step 4b + page structure	6113
Filter (step 5c) - Step 4b + headers + page hash	2999
Filter (step 5d) - Step 4b + headers + page structure	**4423**

→ Filter on combination of observed headers and page structure

- Results of other filtering methods insignificant

Detection system - Statistics

Filter step (+= Country / high-risk ASN filter)	**Count**
Filter (step 6a) - Step 5d + change of country	1363
Filter (step 6b) - Step 5d + high-risk AS	813
Filter (step 6c) - Step 5d + change of country + high-risk AS	343

High-risk Autonomous Systems:

- 213 small low-reputation ASs
- 7 large legitimate ASs

Detection system - Statistics

Filter step (+= OWA portal)	**Count**
Diff (step 7a - base case) - Step 5d + OWA server	58
Diff (step 7a.1) - OWA server + change of country	3
Diff (step 7a.2) - OWA server + high-risk AS	0
Diff (step 7a.3) - OWA server + change of country + high-risk AS	0

Hunting for previous hijacking attacks

- Timeframe: Jan. 2018 - Nov. 2020

- Manual review Outlook Web Access:
  - Suspicious hits: 233
  - True positives: 0

Hunting for previous hijacking attacks

[[Two newly identified hijacking attacks redacted for confidentiality reasons]]

Discussion

- Hard to differentiate between new legitimate and new malicious servers
  - → Large amount of false positives without heavy filtering
    - → Heavy filtering creates risk of more missed cases

- Coverage gaps due to:
  - Scan interval of two weeks
  - Virtual / shared hosting
  - Wildcard certificates

Conclusion

Can DNS hijacking attacks potentially be detected indirectly by identifying the attacker-controlled MitM servers using internet-wide HTTPS scan data?

- Characteristics:
  - Strong indicator: New server with new DV-certificate for existing domain
  - Strong indicator: Different Autonomous System
  - Strong indicator: Fully proxied HTTP responses
  - Weak indicator: Different country of hosting

- Limited filter algorithm (with restrictions) potentially possible, not practical
  - Managed to identify a few targeted organisations with additional target filtering

Future Work

- High-risk target identification for hijacking monitoring
- Real world detection using Certificate Transparency