Challenges in Inferring Domain Hijacking at Scale

Gautam Akiwate
DINR Workshop 2020

Mattijs Jonker, Raffaele Sommese, KC Claffy, Stefan Savage, Geoff Voelker
UC San Diego, University of Twente
Key Observation: DNS Configuration is Critical Infrastructure

Control over DNS Configuration == Full Domain Control

- Control over DNS Configuration allows:
  - Rerouting traffic
  - Compromise credentials
  - Steal/send email
  - Sign SSL Certificates
- Distinct from cache poisoning and protocol attacks
Threat Model: DNS Configuration vulnerable at a Registrar

- Registrars are extremely attractive targets
  - Registrant account compromise
    - Stolen Credentials
    - No 2FA or “on-change” notifications
    - Domain Shadowing
  - Entire Registrars compromised
    - Stolen EPP credentials can compromise all registrar customers
PCH.NET Attack

- Normal DNS Configuration

Authoritative Nameservers
- ns2.pch.net
- ns3.pch.net
- anyns.pch.net
- mail.pch.net

Krebs Article on DNS Hijacking Attacks
DHS Emergency Directive - January 2019
PCH.NET Attack

- On 2019-01-02

Authoritative Nameservers
- ns3.mmfasi.com
- ns4.mmfasi.com
- ns2.pch.net
- ns3.pch.net
- anyns.pch.net
PCH.NET Attack

- On 2019-01-02

Authoritative Nameservers:
- ns3.mmfasi.com
- ns4.mmfasi.com
- ns2.pch.net
- ns3.pch.net
- anyns.pch.net
## PCH.NET Attack: SSL Certificates Signed

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain</th>
<th>Certificate Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-01-02</td>
<td>mail.pch.net</td>
<td>C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA</td>
</tr>
<tr>
<td>2019-01-02</td>
<td>kerio.mail.pch.net</td>
<td>C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA</td>
</tr>
<tr>
<td>2019-01-02</td>
<td>mail.pch.net</td>
<td>C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA</td>
</tr>
<tr>
<td>2019-01-02</td>
<td>kerio.mail.pch.net</td>
<td>C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA</td>
</tr>
</tbody>
</table>
Identifying Domain Hijacking

Approach #1:

Define patterns that could highlight abusive activity?

**Domain:** [old nameservers] → [new nameservers] → [old nameservers]

**Nameserver:** [old IPs] → [new IPs] → [old IPs]
Identifying Domain Hijacking

Approach #1:
Define patterns that could highlight abusive activity?

**Domain:** [old nameservers] → [new nameservers] → [old nameservers]

**Nameserver:** [old IPs] → [new IPs] → [old IPs]

Not very effective.
Identifying Domain Hijacking

Approach #1:

Define patterns that could highlight abusive activity?

**Domain:** [old nameservers] → [new nameservers] → [old nameservers]

**Nameserver:** [old IPs] → [new IPs] → [old IPs]

Not very effective. Lot of false positives.
Identifying Domain Hijacking

Approach #2:

Focus on transitions in DNS Configuration

Supplement transitions in DNS configuration with data from other sources

Cluster the transitions based on features

Can we isolate features crucial for identifying DNS Hijacking?
Identify DNS Hijacking: Features

Example Transition: foo.com → new nameserver → ns1.bar.com

Additional Information
Identify DNS Hijacking: Features

Example Transition: foo.com → new nameserver → ns1.bar.com

Additional Information

foo.com → registration information → creation date, registrar, update date
bar.com → registration information → creation date, registrar, update date
Identify DNS Hijacking: Features

Example Transition: foo.com → new nameserver → ns1.bar.com

Additional Information
foo.com → registration information → creation date, registrar, update date
bar.com → registration information → creation date, registrar, update date
foo.com → other nameservers → [ns1.foo.com, ns2.foo.com]
Identify DNS Hijacking: Features

Example Transition: foo.com → new nameserver → ns1.bar.com

Additional Information
foo.com → registration information → creation date, registrar, update date
bar.com → registration information → creation date, registrar, update date
foo.com → other nameservers → [ns1.foo.com, ns2.foo.com]
ns1.bar.com → IP address → ASN, Geo, AS Rank
ns[1,2].foo.com → IP address → ASN, Geo, AS Rank
Identify DNS Hijacking: Features

Example Transition: foo.com → new nameserver → ns1.bar.com

Additional Information

- foo.com → registration information → creation date, registrar, update date
- bar.com → registration information → creation date, registrar, update date
- foo.com → other nameservers → [ns1.foo.com, ns2.foo.com]
- ns1.bar.com → IP address → ASN, Geo, AS Rank
- ns[1,2].foo.com → IP address → ASN, Geo, AS Rank
- foo.com → CT logs → new SSL certificates signed
Limitations
Limitations

● Transitions in DNS Configuration
  ○ Use of Zone Files (Coarse Granularity)
  ○ Domain Name Zone Alert (DNZA) / DNS Transparency
    ■ Improve granularity of detection
Limitations

- 150k-300k domains show changes daily
  - Data collection challenges
  - Rate limits (whois)

- Lot of other abuse that shows up in transition
  - Domains that change nameservers in lockstep multiple times
    - Machine generated domain names [gdcpmhznxxysjhtpt.xyz]

- Challenge to separate abusive domains from domain hijacking
Limitations

- Ground Truth
  - Limited Ground Truth
    - Few like PCH.NET discussed in news media
  - How can we be sure if it is a domain hijack?
Discussion

● **What other features?**
  ○ Domain Age [zone files | whois]
  ○ Registrar [whois]
  ○ ASN [pfx2as]
  ○ IP Geolocation [netacuity]
  ○ AS Rank [asrank]
  ○ SSL Certificates

● **What other data sources?**

● **Ground truth?**