Mapping criminal infrastructures from “patient zero” using Whois

David Piscitello
Interisle Consulting Group
Massive data breaches – e.g., Target, Sony – were the result of a successful phishing attack.

Whois helps investigators learn what’s below the surface of breaches or other cyber attacks.
Patient zero

The first patient in an outbreak who is noticed by health authorities typically triggers a response or investigation.
From patient zero investigators gather information to map the progression of a disease outbreak.

• Who is patient zero?
• What are his symptoms?
• Where was he found?
• Where did he travel from and to?
• When did he travel?
• What threat does his condition pose?
Index domains are the “patient zeros” of cyber investigations

- **Who is** the domain holder?
  - Notify the breach victim
  - Pursue the cyber attacker

- Where and when were the domains registered?

- **What other domains have similar registration data?**

**Attacks often involve a conspiracy of domains... use index domain to identify that conspiracy**
How do first responders use Whois?

Criminal Abuse of Domain Names:
Bulk Registration and Contact Information Access

http://www.interisle.net/sub/CriminalDomainAbuse.pdf
CASE STUDY
CRIMINAL DOMAINS
IN .TOKYO

• Abuse activity in .TOKYO from December 12, 2018 through December 25, 2018

• 8,715 .TOKYO criminal abuse domain names

<table>
<thead>
<tr>
<th>Registrar</th>
<th>IANA ID</th>
<th>Criminal Abuse Domains Identified</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMO Internet, Inc. d/b/a Onamae.com</td>
<td>49</td>
<td>8,713</td>
<td>100.0</td>
</tr>
<tr>
<td>NameCheap, Inc.</td>
<td>1068</td>
<td>2</td>
<td>0.0</td>
</tr>
</tbody>
</table>

Nearly all of these were registered using a single registrar.
WHY THIS REGISTRAR?

- VERY CHEAP DOMAIN REGISTRATIONS
- CUSTOMERS CAN REGISTER IN VOLUME
- CUSTOMERS CAN GENERATE RANDOM LOOKING DOMAINS

1 ¥ = €0.0083

Web site will create random names

Customers can upload a file of names
Cheap domain names contribute to a criminal marketplace in which small investments can yield extraordinary returns.

1000s of domain names can be acquired for pennies per domain from registrars like GMO Internet.

Mailing lists can be purchased in the dark web or online.

Ransomware can be purchased as a service for €35.

Phishing kits can be downloaded for free from social media sites.

Online tutorials are available from YouTube.

Assuming a ransomware extortion fee of $200-500 USD, a ransomware attack is profitable with a handful of victims.

Even a single ransomware or phishing campaign is a lucrative enterprise.
IDENTIFYING CRIMINAL ACTORS: SEARCH AND PIVOT

• .TOKYO sample spans a “post-GDPR” time period
• Use historical and recent Whois records
• **Use** {registrant name, registrant organization, registrant email} **to**
  • SEARCH historical Whois databases
  • PIVOT to other databases or social media
• to identify the criminal actors
• Only some Whois records contain contact data
• Assume that criminals submit inaccurate or fraudulently composed data
WHAT DOES SEARCH-AND-PIVOT REVEALS?

• The harmful content or attack messages
• Where criminal actors host *infrastructure*, e.g.
  • Malware or ransomware executables
  • Phishing or financial fraud web pages
  • Political influence campaign material
  • Mail servers that send phishing lures
  • DNS servers that support DDoS attacks
• Other domain holders that may be part of a criminal enterprise
• Other Top-level domains in which the criminal actor has registered names
The suspect appears to have used GMO’s bulk registration tools to generate thousands of random-looking domains names in matters of minutes.

- GMO offered .TOKYO domains registrations at very low cost.
- The suspect provided a registrant address in Japan.
- The suspects targeted .TOKYO but not exclusively. .INFO, .CLUB, .ONLINE, .XYZ, .BIZ, .SPACE, and .WORK were also targeted.
- The suspect hosted Japanese phishing or malware at three hosting providers:
  - InterQ GMO Internet, Inc.
  - IDC Frontier, Inc.
  - Sakura Internet, Inc.
LET’S REVIEW:

JAPANESE SPAMMERS TARGETED JAPANESE USERS USING A JAPANESE REGISTRAR AND JAPANESE HOSTING OPERATORS
COMPLETE WHOIS RECORDS ARE ESSENTIAL IF FIRST RESPONDERS AND LAW ENFORCEMENT ARE TO IDENTIFY VICTIMS AND CRIMINAL ACTORS

BUT... DUE TO AN OVERLY BROAD INTERPRETATION OF THE EU GDPR

PUBLIC WHOIS IS NOW DARK
EU’S GDPR IS INTENDED TO PROTECT PERSONAL PRIVACY

Whois implementation protects Internet criminals or dark organizations
## Adverse Effects of ICANN Whois Policy

<table>
<thead>
<tr>
<th>Blanket redaction</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Inhibits searches to correlate domains or actors to attacks</td>
<td>No discrimination between EU data subjects and legal persons</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legitimate disclosure of non-public Whois is still not defined</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No policy for timely or predictable access</td>
<td>No accreditation frameworks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&quot;One size fits all&quot;</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Registries are redacting more data than is required by GDPR</td>
<td>Solution assumes all data protection laws will align with GDPR</td>
</tr>
</tbody>
</table>
EFFECT OF ICANN POLICY ON ACCESS TO HISTORICAL COMPLETE WHOIS RECORDS

Facts & Figures: Whois Policy Changes Impair Blocklisting Defenses
http://lnnk.in/@whoisimpedesblocklisting
WHEN PRIVACY REGULATION BLOCKS CRIMINAL INVESTIGATION CITIZENS ARE EXPOSED TO HARM AND LOSS

DATA PROTECTION REGULATIONS MUST ACCOMMODATE FIRST RESPONDER AND LAW ENFORCEMENT ACCESS TO CRITICAL INFORMATION

PRIVACY PROTECTION AND PUBLIC SAFETY: A DELICATE BALANCING ACT
Creative Commons

• Slide 2, 3: Lassa Fever investigation, Mike Blyth
  https://www.flickr.com/photos/blyth/

• Slide 3: Enzootic Plague investigation, CDC Global,
  https://www.flickr.com/photos/cdcglobal/

• Slide 4: World Map, Share reproductions,
  https://www.flickr.com/photos/shaireproductions/

• Slide 10: Computer Hackers,
  https://www.flickr.com/photos/121483302@N02/

• All other images from Pixabay Images