GETTING TO THE SOUL OF INCIDENT RESPONSE
Adversary Recon and Practical Defenses Using Domain and DNS OSINT

Tim Helming
Director, Product Management
DomainTools
Instruction Slide

• Please **do not delete** the title slide.
• You are **not required** to use this template.
• You are welcome to include your organization’s logo/brand on the presentation title page.
• You are also welcome to adjust the location of your logo as long as it does not overlap/touch the FIRST logo.
• Your slides must be reviewed prior to your presentation by the FIRST Program Chair and Committee.
Contents

• OSINT for adversary analysis—and why adversary analysis is useful
• Which OSINT sources are we talking about?
• Forensic Domain Mapping: Nexus Discovery and Expansion
• Attribution/Profiling/Analyzing. Without lurking on teh darkwebs (unless that’s your thing)
• Oh, snap, we’re breached. Now what?
• Continuous Security & Threat Hunting
So, me.

Been in the security game a long time. When I began...

- Started as a support guy at a firewall company
- Eventually ran product at the firewall company
- Now running product at DomainTools
- Musician, radio ham (WT1IM), motorcycle guy
Combating Cybercrime…

At the destination (defending your assets)

At the source (shutting down criminal networks)
Why do adversary analysis?

“Attribution is a proxy for risk.”

– Kevin Mandia
Why do adversary analysis?

“The pursuit of attribution, manifesting itself in adversary analysis, can be employed to improve an organization's resource allocation and security posture.”

– Josh Ray
VP, Verisign iDefense
Why do adversary analysis?

Adversary analysis ≠ positive attribution. A solid profile can speak volumes.

• Calculated vs opportunistic/scattershot attack
• Lone wolf vs connected network
• Scale of operations
• Nature of operations
• TT&Ps

...many of which can be discerned quickly, to help you triage indicators
Why do adversary analysis?

A solid profile (or positive attribution) enables multiple actions:

- Look for lateral movement
- Discover dwell time (more later)
- Monitor attackers
- Learn more via search (i.e. you now have a bunch more search terms)
Threat Actor OpSec and Patterns

It’s easier for everyone—including the bad guys—to follow patterns than to act randomly. Poor OpSec heightens their risk of exposure.

There are patterns evident in DNS/Whois OSINT that can be discerned...

...and anticipated

(...and others that can be red herrings)
Sources of OSINT

- **DNS** lookups (many sources of passive/massive DNS. Live lookups are fine but don’t scale)
- **Dig** (command line)
- **Whois** lookups (many web sources, or port 43 from command line)
- **MX records** (several web sources, command line also supports this)
- **Archive.org**’s Wayback Machine
- **Search engines** (there are a few of these too 😊)
- **Malware analysis** (we won’t be covering that today)
OSINT = Free?

Short answer
• Piecemeal: Yes
• At scale: No (typically)

Longer answer
• With some work, there are things you can do to automate collection/querying of OSINT in large(ish) volumes, but...
• Consider the domains-by-IP problem
• There are products that solve the scale/cross-indexing problem for you
Examples – introduction

Using a phishing attack, an APT, and an ad-hoc investigation of a DDoS service, we will see:

• Forensic domain mapping
• Techniques: “nexus discovery” and “expansion”
• Adversary analysis techniques
Profile your adversary with this one weird trick

**Scenario**
Google document phishing attack

**Goals**
profile threat and assess risk

**Begin with the domain**
GoeoglleDoc.com
Initial phish domain

Domain Name: GOEOGLLEDOC.COM
Registry Domain ID: 1901083053_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.wildwestdomains.com
Registrar URL: http://www.wildwestdomains.com
Update Date: 2015-02-06T06:16:00Z
Creation Date: 2015-02-06T06:16:00Z
Registrar Registration Expiration Date: 2016-02-06T06:16:00Z
Registrar: Wild West Domains, LLC
Registrar IANA ID: 440
Registrar Abuse Contact Email: abuse@wildwestdomains.com
Registrar Abuse Contact Phone: +1.480-624-2505
Reseller: WordPress.com
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Reginald C. Rodman
Registrant Organization:
Registrant Street: 12 Heath Hill
Registrant City: Brookline
Registrant State/Province: Massachusetts
Registrant Postal Code: 02043
Registrant Country: United States
Registrant Phone: +1.5169081197
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: procurement.alumatecsystem.com@gmail.com
Registry Admin ID:
Admin Name: Reginald C. Rodman
Admin Organization:
Admin Street: 12 Heath Hill
Admin City: Brookline
The magic of cross-indexed Whois databases....
Inferring Adversary Intent

Reginald C. Rodman: Busy Guy

This phone number connects to other domains, all registered to Reginald Rodman. Known as “Reverse Whois”

**TELEPHONE: 15169081197**

Administrative - Billing - Registrant - Technical

In the most current archive we have 9 domain records that match your reverse whois search

Click here to download the full list of domain names.

OSINT sources:
- commercial Whois data providers

**Strong inferences:**
- Targeting banks
- These domains registered within 3 days of each other
Use It!

Goals: profile threat and assess risk

Next Steps:

• Search for domains in network logs
• Proactively block access
• Study attacker’s infrastructure
• Monitor future registrations
What Makes a Good Nexus?

- **Uniqueness of the datapoint**
  - abuse@enom.com is NOT a good nexus
  - stealthreconx@gmail.com IS a good nexus

- **Smaller is (generally) better**
  - A hosting IP with 100K sites is not going to tell you much about your target domain
  - A single or low-count IP is more likely to indicate connection and affinity

- **A datapoint with semantic meaning is good**
  - “skydaddyhacks@aol.com” tells us something...
Example 2: APT 28 (FireEye report)

Table 1: Examples of APT28 domains imitating organizations in the Caucasus

<table>
<thead>
<tr>
<th>APT28 Domain</th>
<th>Real Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>kavkazcentr[].info</td>
<td>The Kavkaz Center / The Caucasus Center, an international Islamic news agency with coverage of Islamic issues, particularly Russia and Chechnya (kavkazcenter.com)</td>
</tr>
<tr>
<td>rmil[].am</td>
<td>Armenian military (mil.am)</td>
</tr>
</tbody>
</table>

“We have seen APT28 register at least two domains mimicking the domains of legitimate organizations in the Caucasus...One APT28 domain imitated a key Chechen-focused news website, while the other appeared to target members of the Armenian military by hosting a fake login page.” – Page 11, APT28 Report
OSINT sources:
- port 43
- passive DNS
- commercial providers
IP Expansion

Notice anything?

- googleproductupdate
- sry-yahoo
- update-windows
- ...etc

A pattern is clear...

OSINT sources:
- passive DNS
- commercial providers
Example 3: DDoS for sale

DDoS brokers abound.

Example: top10booters[.]com

We know this site is bad.  
*But can we learn more about its extended network? Its operator(s)*?
Seek Nexus…

- Registrant Name/Address: not interesting
- Registrant Email
  - 2 addresses look interesting (abuse@enom is not interesting)
- DNS
  - IP address: could be interesting (stay tuned)
  - MX: only interesting in that they *have* MX
  - NS: not interesting
Expansions: IP and email

Nexus: 185.30.165.39
- top10booters\.com
- darkbooter\.com
- darkbooter\.net
- fatal-mt2\.net
- hazebooter\.com
- hazebooter\.net
- icestresser\.com
- iddos\.co
- iddos\.net
- ionbooter\.com
- ipstressers\.com
- minecraftkings\.net
- pcgameguides\.net

Nexus: stealthreconx@gmail.com
- ddosninja\.com
- dimension\.li
- expuse\.in
- iddos\.co
- ionbooter\.com
- ituneshacks\.com
- newmicrosoftoffice\.com
- pcgameskeys\.net
- pickmypromdress\.com
- top10booters\.com
- xboxburn\.com
- xboxonecompetitions\.com
Attribution path

Top10booters[.]com

185.30.165.39  stealthreconx@gmail.com

22 likely-connected domains

6 unique, non-anonymous email addresses

10 not-obviously-fake human names

2 names with tight connections to top10booters

1 strong candidate for our attacker
Capitalize on “sIOPSec”

Sometimes, registrants initially register openly, add privacy later.

Oops! (example dotnetexplorer[.]info from Volatile Cedar)
Capitalize on “sIOPSec”

Corroborate via Wayback Machine or screenshot history tools
Apply It…
OSINT in Continuous Security

It’s not just for IR any more...

Looking Back
Forensics:
• Were these domains or IPs seen previously?
• Innocuous-looking traffic might have been evil

Today
Mitigation:
• Lock down against observed threats
• Find and lock down against expanded threat network

Looking Ahead
Prevention:
• Monitor new registrations by this actor
• Defend before attacks are launched
Oh, Snap—I’m Breached! Now What?

OK-stopped the leak. But...

How long have they been inside?
Where have they been sending my data?
Where might they try to send it next?

Use OSINT to expand

exfiltrationdomain.com
(nexus discovery) ->
(expansion) ->
pwnyoudomain.com
lulzdomain.com
wewinulosedomain.com
...etc
OSINT in Continuous Security and for Hunt Teams

1) Detect initial indicators, expand to connected assets
2) Review archives for earlier expanded threat
3) Monitor cybersquatters, repeat offender domain registrants
4) Proactively block new threat infrastructure
Summing Up

- **Adversary analysis is worthwhile,** especially for attention-getting threat indicators
- **Sources of OSINT abound**
- **Piecemeal lookups are free; at-scale typically is $**
- **Technique: nexus discovery and expansion**
  - **“Nexus:”** a data point that connects infrastructure
  - **“Expansion:”** the broader set of connected entities, expanded from the original one
- **These techniques have application across tenses of time**
Wrapping Up

Q&A
Thank You!

thelming@domaintools.com

@timheling