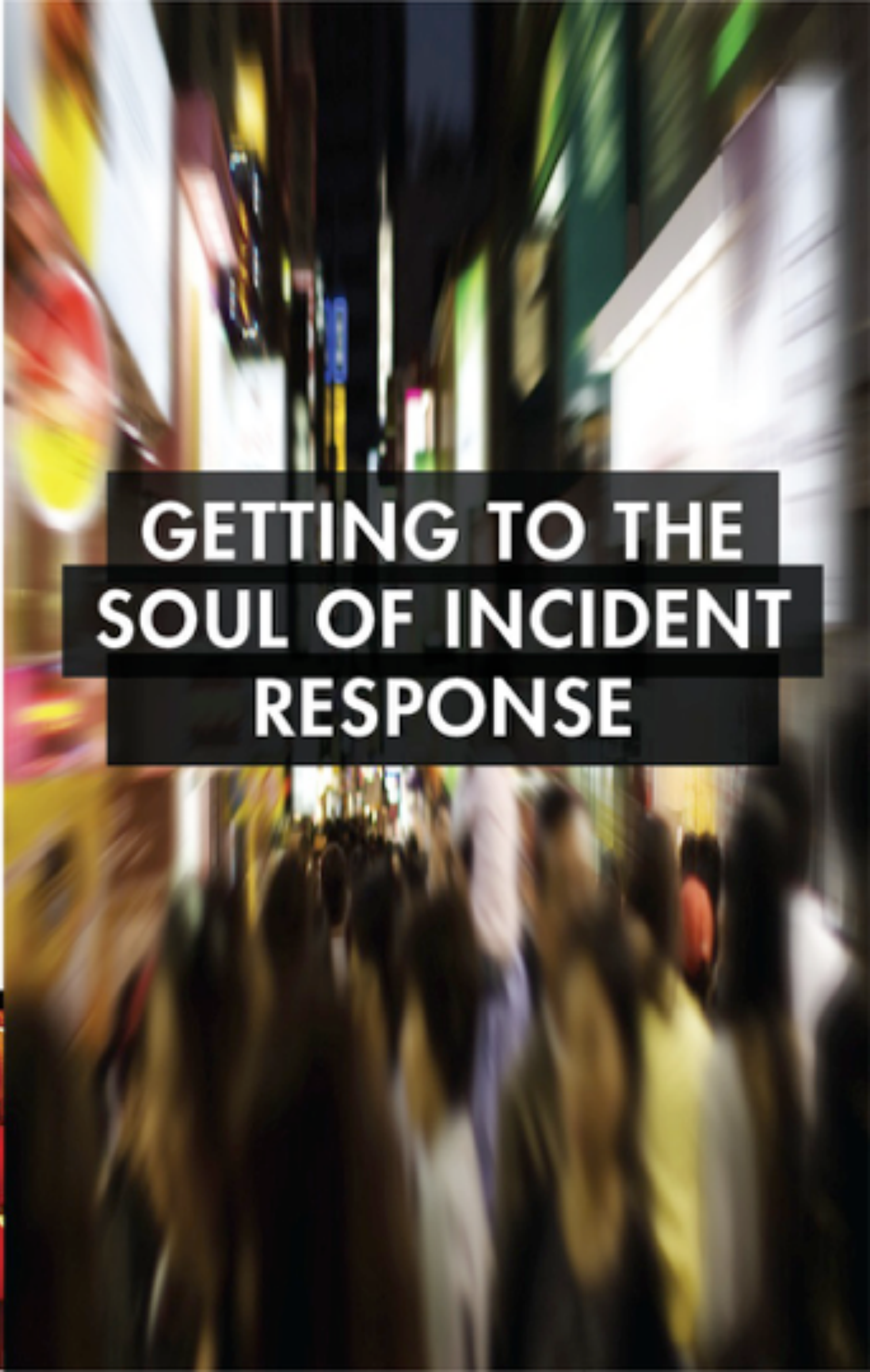
28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016



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.

(as a comic character from MIRcon)

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 source (shutting down criminal networks)

At the destination (defending your assets)

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)

PawnStorm
VolatileCedar
SaffronRose
Sofacy APT1
FlyingKitten
TerracottaVPN
DynamitePanda

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

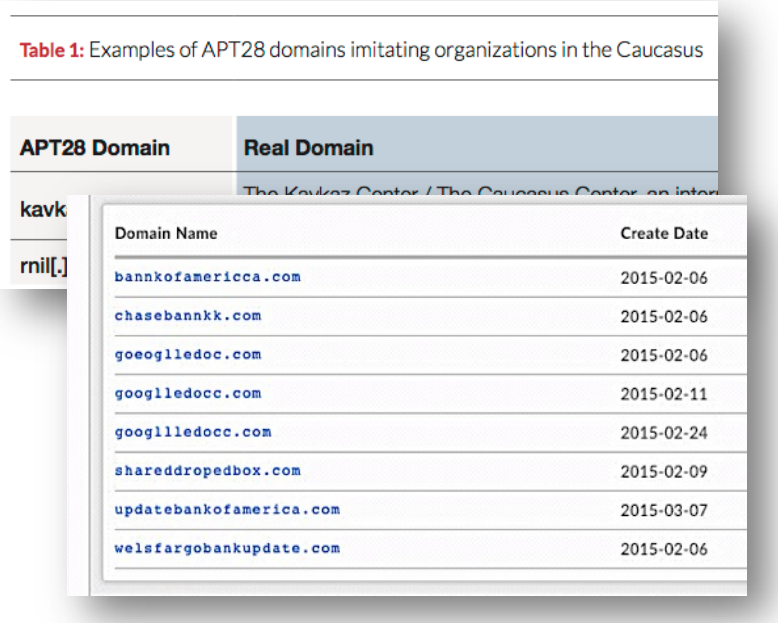


Table 1: Examples of APT28 domains imitating organizations in the Caucasus

APT28 Domain	Real Domain
kavk	The Kavkaz Center / The Caucasus Center, an inter
rnil[.]	

Domain Name	Create Date
bannkofamericca.com	2015-02-06
chasebannkk.com	2015-02-06
goeoglledoc.com	2015-02-06
googlledocc.com	2015-02-11
googllledocc.com	2015-02-24
shareddropedbox.com	2015-02-09
updatebankofamerica.com	2015-03-07
welsfargobankupdate.com	2015-02-06

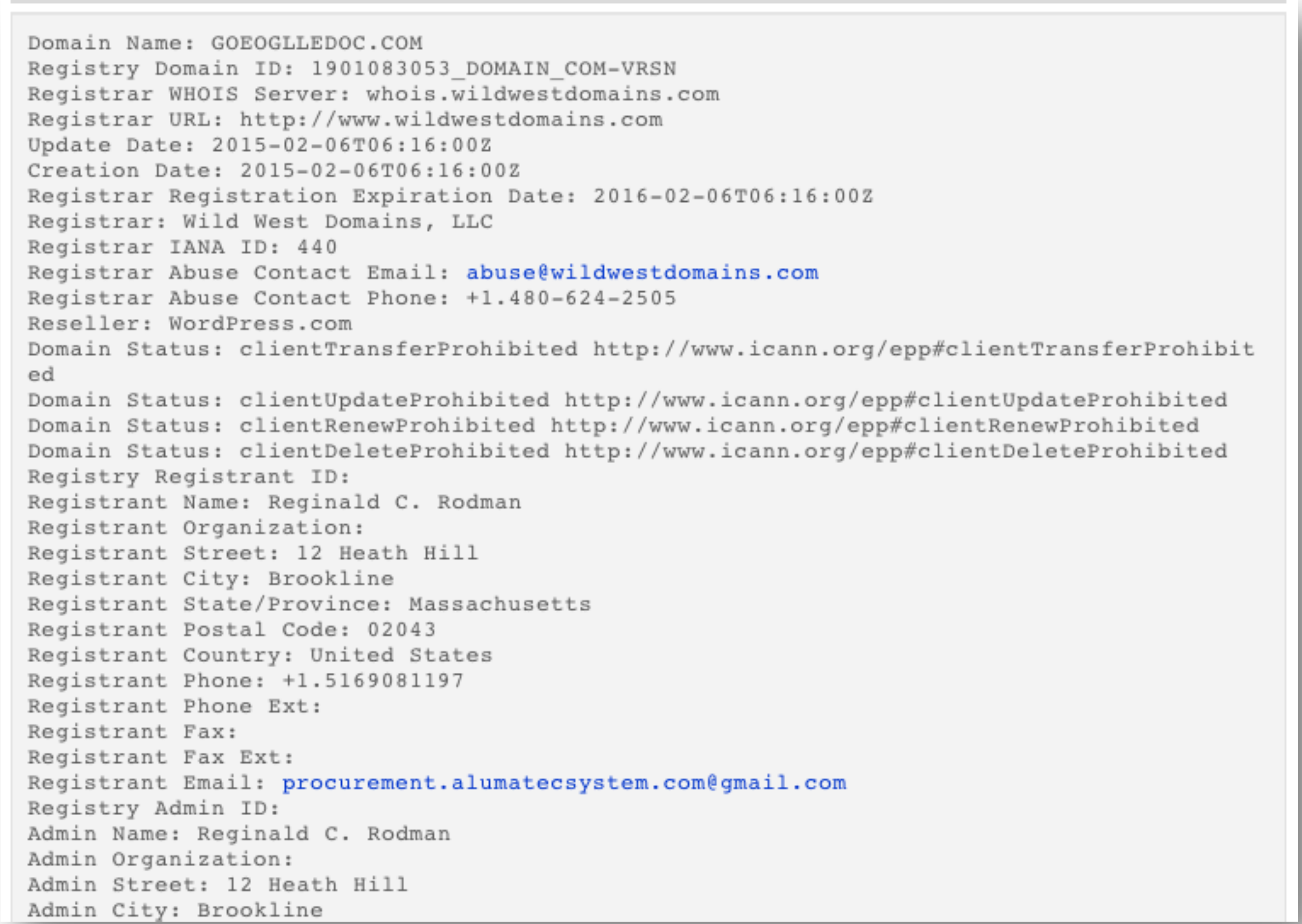
Profile your adversary with this one weird trick

Scenario
Google document phishing attack

Goals
profile threat and assess risk

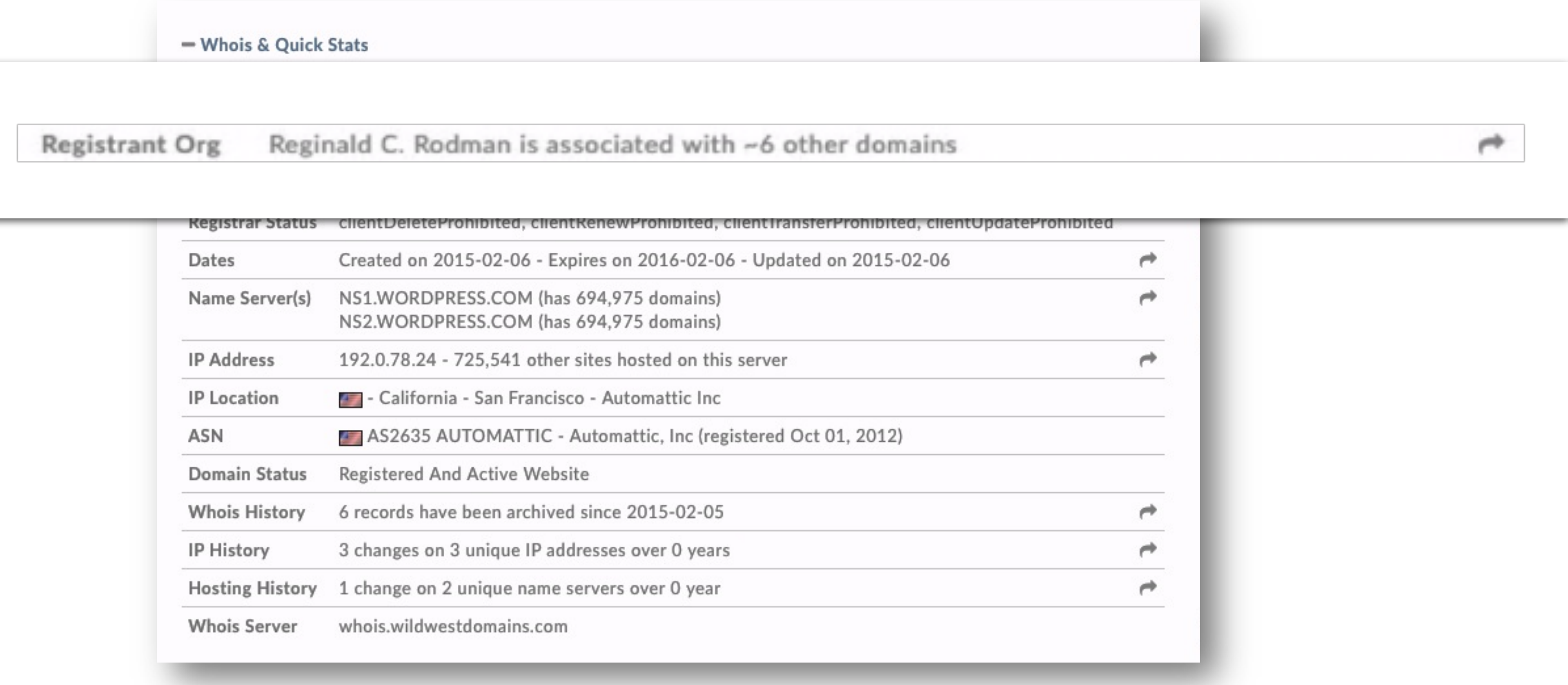
Begin with the domain
GoeoglleDoc.com

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#clientTransferProhibit
ed
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….



— Whois & Quick Stats

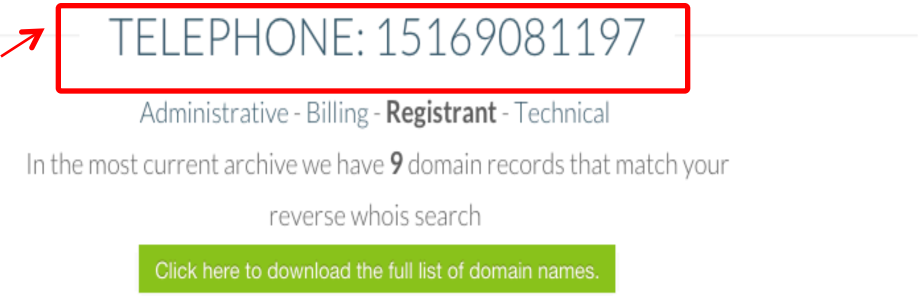
Registrant Org	Reginald C. Rodman is associated with ~6 other domains	↱

Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited	
Dates	Created on 2015-02-06 - Expires on 2016-02-06 - Updated on 2015-02-06	↱
Name Server(s)	NS1.WORDPRESS.COM (has 694,975 domains) NS2.WORDPRESS.COM (has 694,975 domains)	↱
IP Address	192.0.78.24 - 725,541 other sites hosted on this server	↱
IP Location	- California - San Francisco - Automattic Inc	
ASN	AS2635 AUTOMATTIC - Automattic, Inc (registered Oct 01, 2012)	
Domain Status	Registered And Active Website	
Whois History	6 records have been archived since 2015-02-05	↱
IP History	3 changes on 3 unique IP addresses over 0 years	↱
Hosting History	1 change on 2 unique name servers over 0 year	↱
Whois Server	whois.wildwestdomains.com	

Inferring Adversary Intent

Reginald C. Rodman: Busy Guy

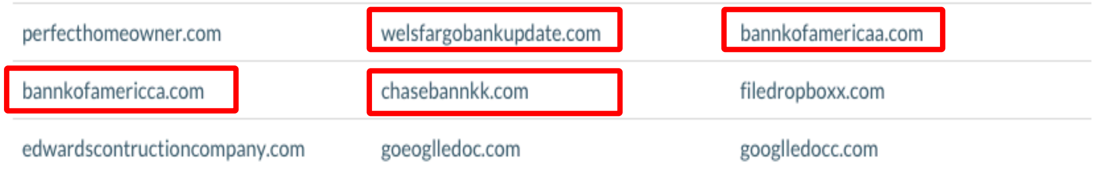
This phone number connects to other domains, all registered to Reginald Rodman. Known as "Reverse Whois"



TELEPHONE: 15169081197

Administrative - Billing - **Registrant** - Technical

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



perfecthomeowner.com	welsfargobankupdate.com	bannkofamericaa.com
bannkofamericca.com	chasebannkk.com	filedropboxx.com
edwardscontructioncompany.com	goeoglledoc.com	googlledocc.com

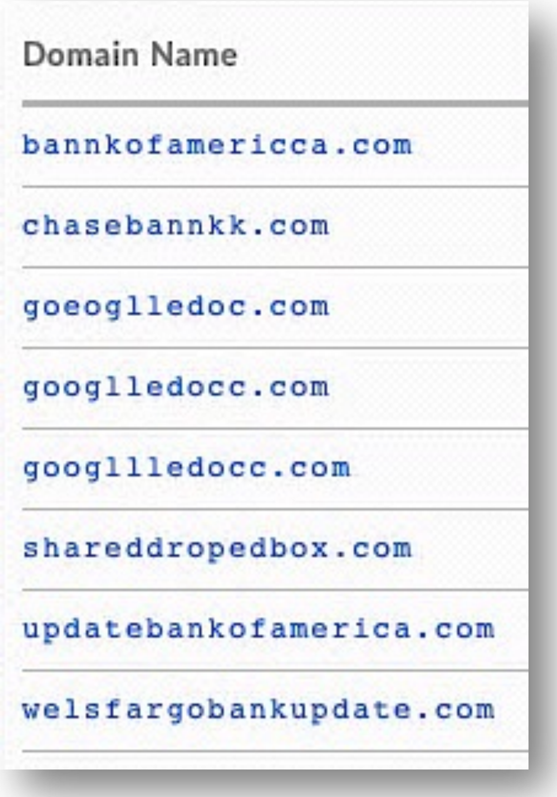
OSINT sources:

- commercial Whois data providers

Strong inferences:

- Targeting banks
- These domains registered within 3 days of each other

Use It!



Domain Name
bannkofamericca.com
chasebannkk.com
goeoglledoc.com
googlledocc.com
googllledocc.com
shareddropedbox.com
updatebankofamerica.com
welsfargobankupdate.com

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)

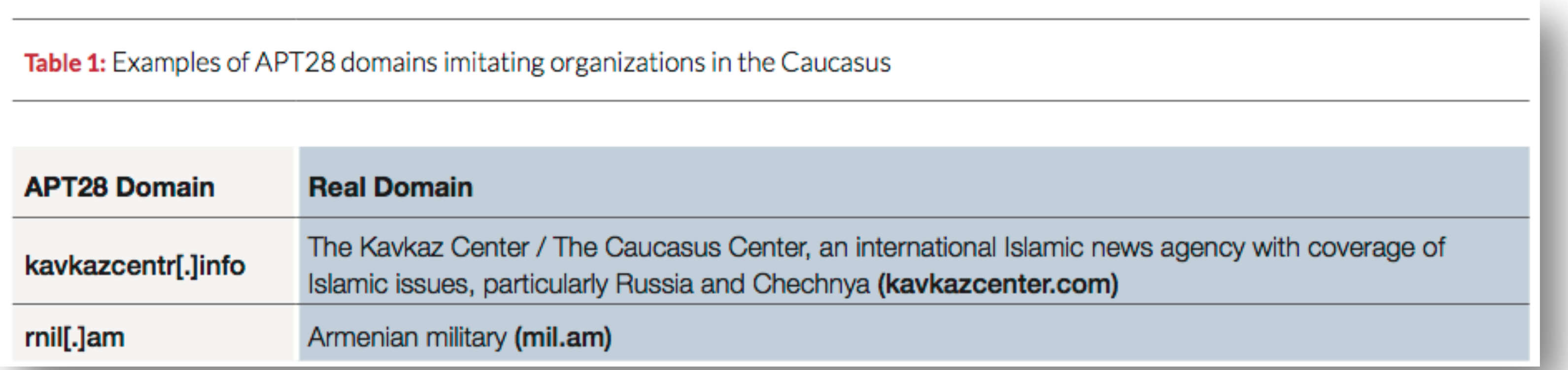


Table 1: Examples of APT28 domains imitating organizations in the Caucasus

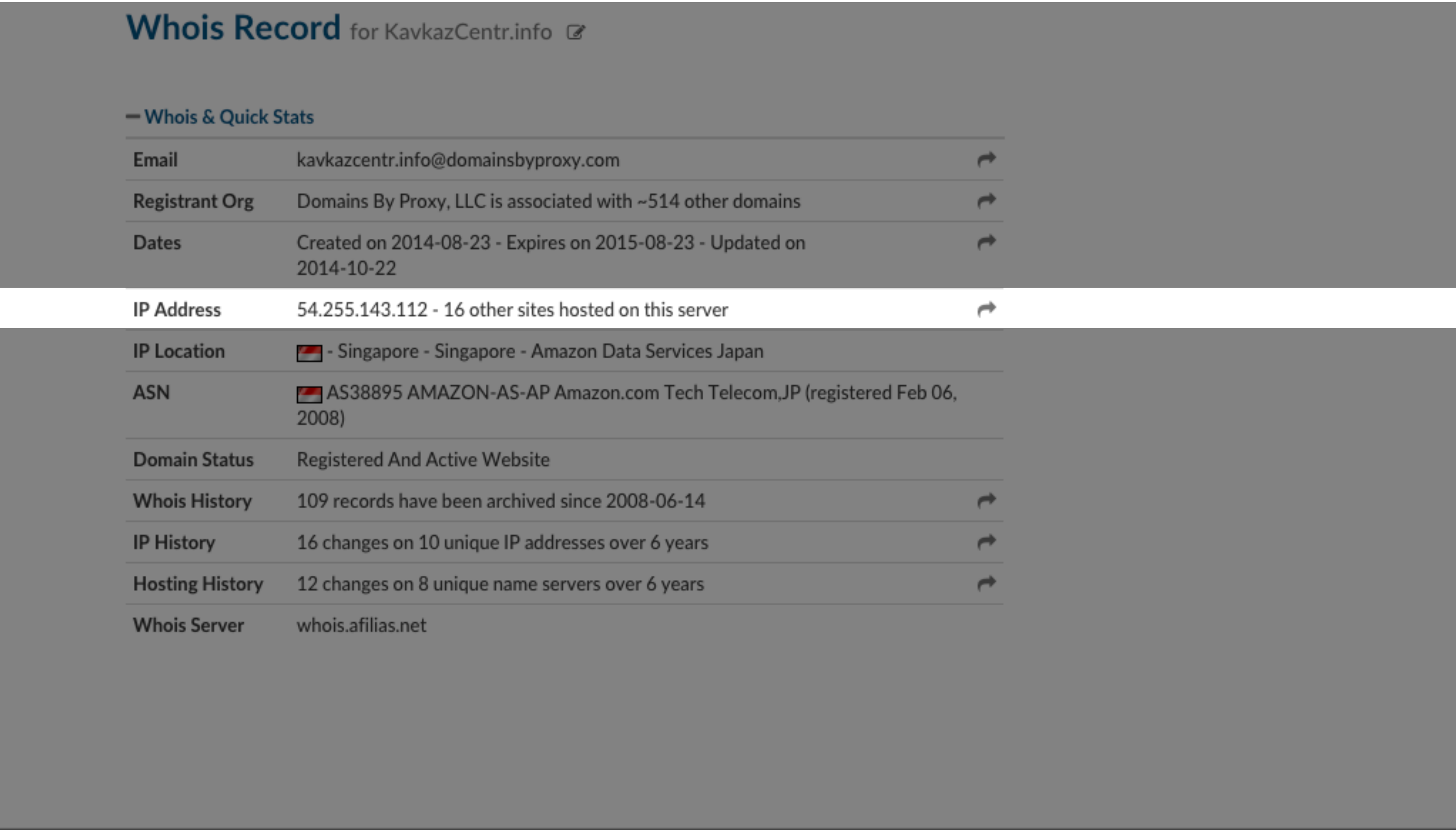
APT28 Domain	Real Domain
kavkazcentr[.]info	The Kavkaz Center / The Caucasus Center, an international Islamic news agency with coverage of Islamic issues, particularly Russia and Chechnya **(kavkazcenter.com)**
rnil[.]am	Armenian military **(mil.am)**

"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

IP Nexus

OSINT sources:

- port 43
- passive DNS
- commercial providers



Whois Record for KavkazCentr.info

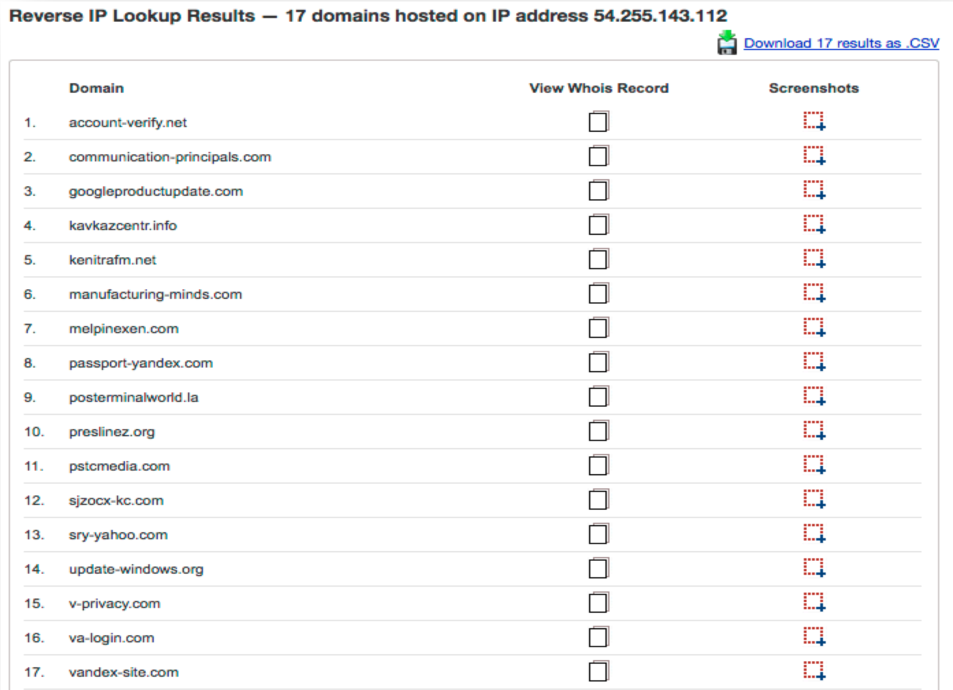
— Whois & Quick Stats

Email	kavkazcentr.info@domainsbyproxy.com
Registrant Org	Domains By Proxy, LLC is associated with ~514 other domains
Dates	Created on 2014-08-23 - Expires on 2015-08-23 - Updated on 2014-10-22
IP Address	54.255.143.112 - 16 other sites hosted on this server
IP Location	- Singapore - Singapore - Amazon Data Services Japan
ASN	AS38895 AMAZON-AS-AP Amazon.com Tech Telecom,JP (registered Feb 06, 2008)
Domain Status	Registered And Active Website
Whois History	109 records have been archived since 2008-06-14
IP History	16 changes on 10 unique IP addresses over 6 years
Hosting History	12 changes on 8 unique name servers over 6 years
Whois Server	whois.afilias.net

IP Expansion

OSINT sources:

- passive DNS
- commercial providers



Reverse IP Lookup Results — 17 domains hosted on IP address 54.255.143.112

Download 17 results as .CSV

	Domain	View Whois Record	Screenshots
1.	account-verify.net	□	□
2.	communication-principals.com	□	□
3.	googleproductupdate.com	□	□
4.	kavkazcentr.info	□	□
5.	kenitrafm.net	□	□
6.	manufacturing-minds.com	□	□
7.	melpinexen.com	□	□
8.	passport-yandex.com	□	□
9.	posterminalworld.la	□	□
10.	preslinez.org	□	□
11.	pstcmedia.com	□	□
12.	sjzocx-kc.com	□	□
13.	sry-yahoo.com	□	□
14.	update-windows.org	□	□
15.	v-privacy.com	□	□
16.	va-login.com	□	□
17.	vandex-site.com	□	□

Notice anything?

- googleproductupdate
- sry-yahoo
- update-windows
- …etc

A pattern is clear…

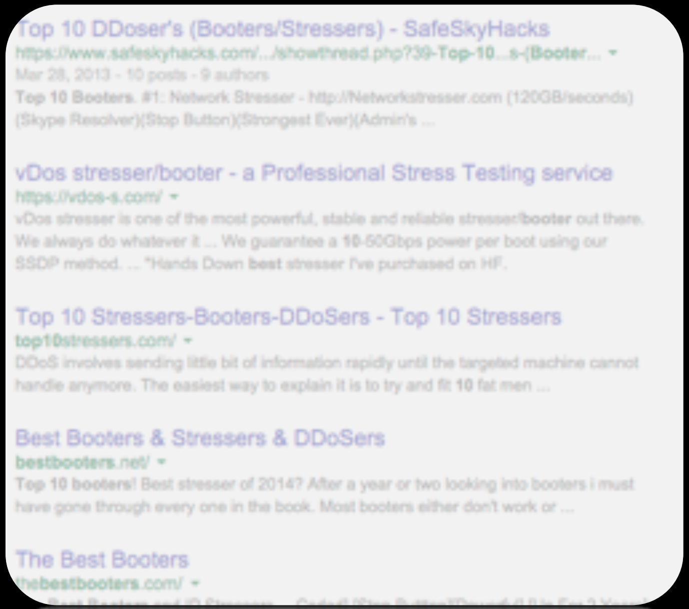
Example 3: DDoS for sale

DDoS brokers abound.

Example: top10booters[.]com

We know this site is bad.

But can we learn more about its extended network? Its operator(s)?



Top 10 DDoser's (Booters/Stressers) - SafeSkyHacks
https://www.safeskyhacks.com/.../showthread.php?39-Top-10...s-(Booter...
Mar 28, 2013 - 10 posts - 9 authors
Top 10 Booters. #1: Network Stresser - http://Networkstresser.com (120GB/seconds) (Skype Resolver)(Stop Button)(Strongest Ever)(Admin's ...

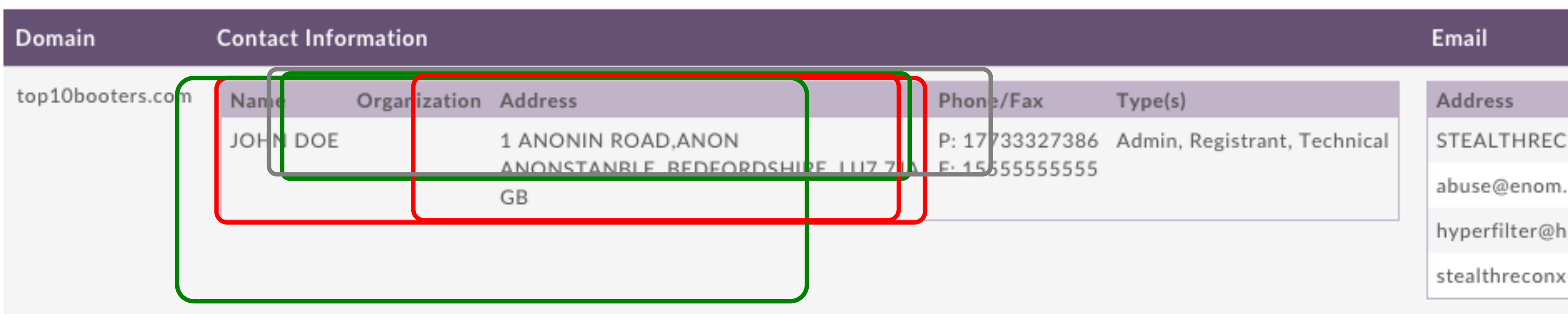
vDos stresser/booter - a Professional Stress Testing service
https://vdos-s.com/
vDos stresser is one of the most powerful, stable and reliable stresser/**booter** out there. We always do whatever it ... We guarantee a **10**-50Gbps power per boot using our SSDP method. ... "Hands Down **best** stresser I've purchased on HF.

Top 10 Stressers-Booters-DDoSers - Top 10 Stressers
top10stressers.com/
DDoS involves sending little bit of information rapidly until the targeted machine cannot handle anymore. The easiest way to explain it is to try and fit **10** fat men ...

Best Booters & Stressers & DDoSers
bestbooters.net/
Top 10 booters! Best stresser of 2014? After a year or two looking into booters i must have gone through every one in the book. Most booters either don't work or ...

The Best Booters
thebestbooters.com/

Seek Nexus…



Domain	Contact Information					Email
	Name	Organization	Address	Phone/Fax	Type(s)	Address
top10booters.com	JOHN DOE		1 ANONIN ROAD,ANON ANONSTANBLE, BEDFORDSHIRE, LU7 7JA GB	P: 17733327386 F: 15555555555	Admin, Registrant, Technical	STEALTHREC abuse@enom. hyperfilter@h stealthreconx

- 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

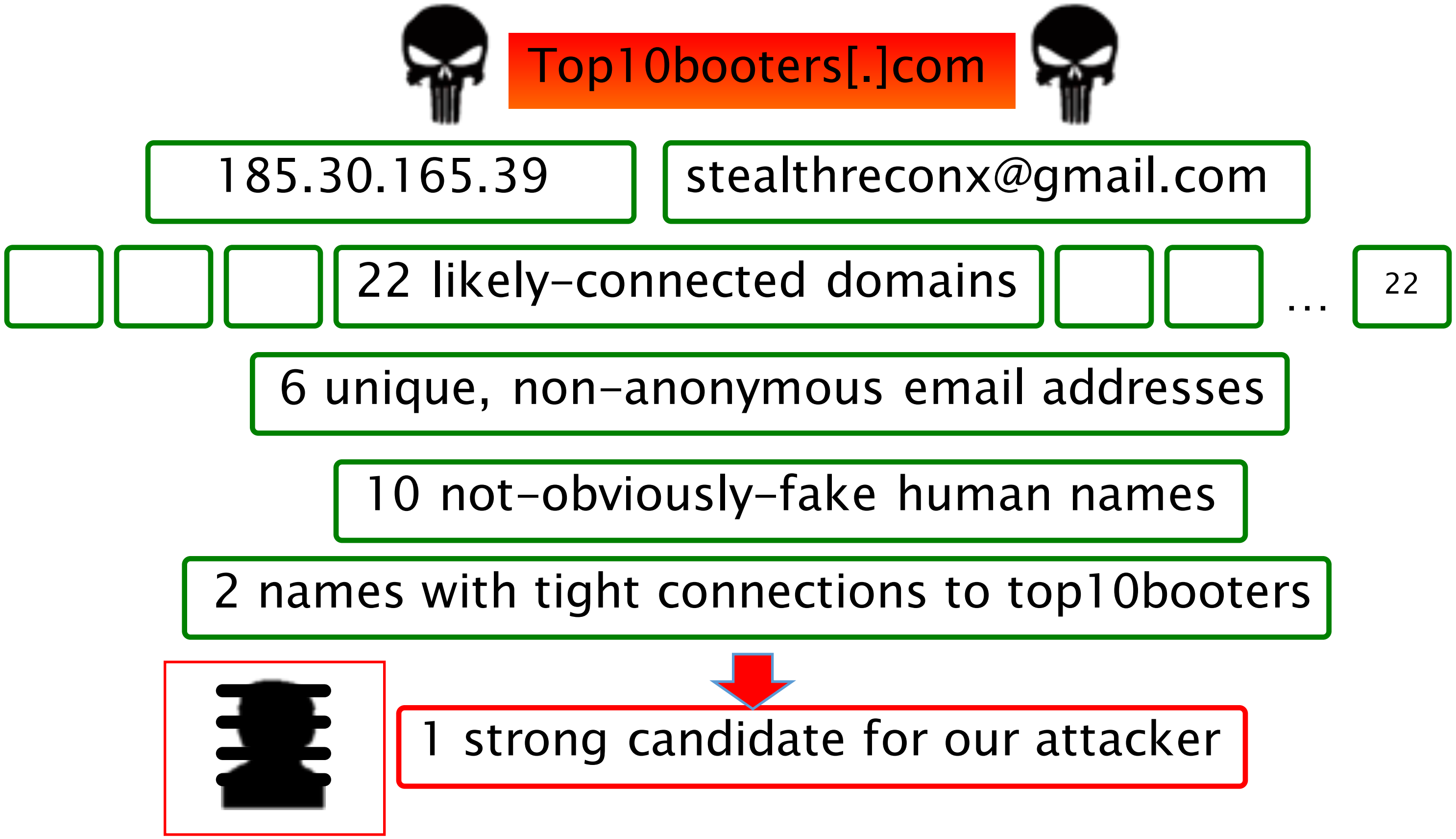
Nexus: 185.30.165.39

- **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 … 22

6 unique, non-anonymous email addresses

10 not-obviously-fake human names

2 names with tight connections to top10booters

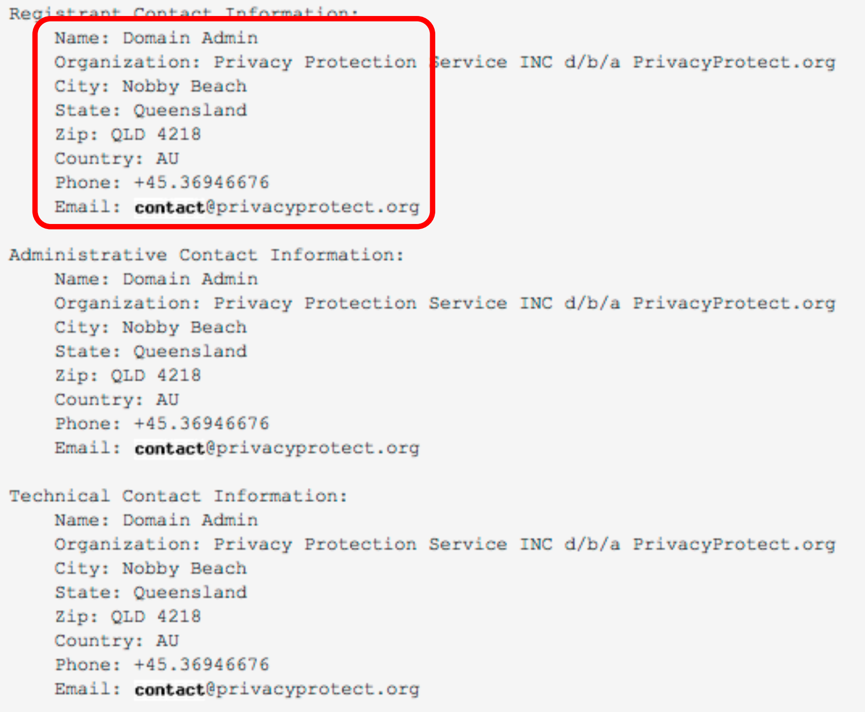
1 strong candidate for our attacker

Capitalize on “sIOPSec”

Sometimes, registrants initially register openly, add privacy later.

Oops! *(example* **`dotnetexplorer[.]info`** *from Volatile Cedar)*

Today:

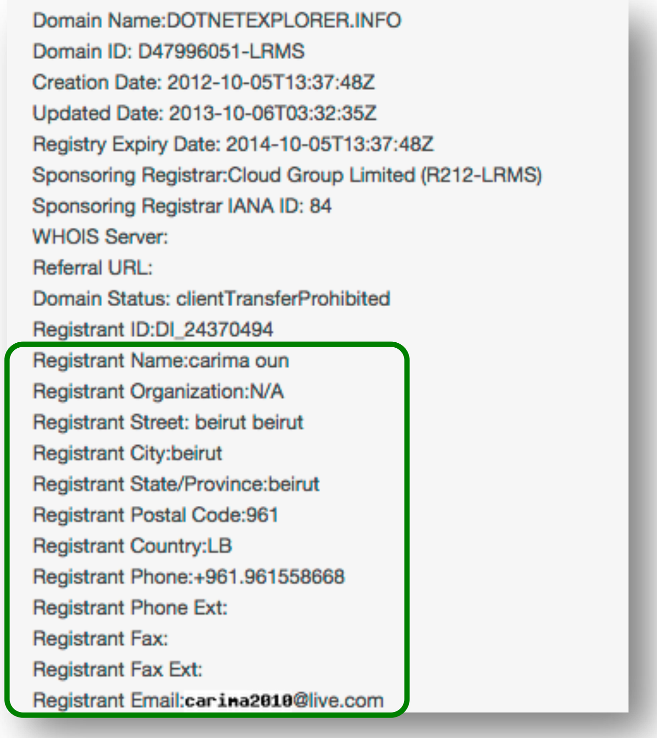


```
Registrant Contact Information:
    Name: Domain Admin
    Organization: Privacy Protection Service INC d/b/a PrivacyProtect.org
    City: Nobby Beach
    State: Queensland
    Zip: QLD 4218
    Country: AU
    Phone: +45.36946676
    Email: contact@privacyprotect.org

Administrative Contact Information:
    Name: Domain Admin
    Organization: Privacy Protection Service INC d/b/a PrivacyProtect.org
    City: Nobby Beach
    State: Queensland
    Zip: QLD 4218
    Country: AU
    Phone: +45.36946676
    Email: contact@privacyprotect.org

Technical Contact Information:
    Name: Domain Admin
    Organization: Privacy Protection Service INC d/b/a PrivacyProtect.org
    City: Nobby Beach
    State: Queensland
    Zip: QLD 4218
    Country: AU
    Phone: +45.36946676
    Email: contact@privacyprotect.org
```

Earlier:

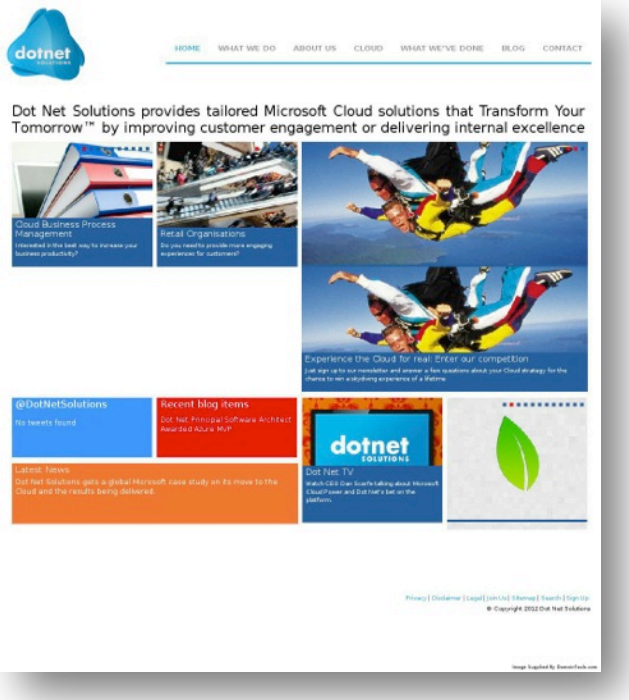


```
Domain Name:DOTNETEXPLORER.INFO
Domain ID: D47996051-LRMS
Creation Date: 2012-10-05T13:37:48Z
Updated Date: 2013-10-06T03:32:35Z
Registry Expiry Date: 2014-10-05T13:37:48Z
Sponsoring Registrar:Cloud Group Limited (R212-LRMS)
Sponsoring Registrar IANA ID: 84
WHOIS Server:
Referral URL:
Domain Status: clientTransferProhibited
Registrant ID:DI_24370494
Registrant Name:carima oun
Registrant Organization:N/A
Registrant Street: beirut beirut
Registrant City:beirut
Registrant State/Province:beirut
Registrant Postal Code:961
Registrant Country:LB
Registrant Phone:+961.961558668
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:carima2010@live.com
```

Capitalize on “sIOPSec”

Corroborate via Wayback Machine or screenshot history tools

Today:



Dot Net Solutions provides tailored Microsoft Cloud solutions that Transform Your Tomorrow™ by improving customer engagement or delivering internal excellence

Cloud Business Process Management
Interested in the best way to increase your business productivity?

Retail Organisations
Do you need to provide more engaging experiences for customers?

Experience the Cloud for real: Enter our competition
Just sign up to our newsletter and answer a few questions about your Cloud strategy for the chance to win a skydiving experience of a lifetime

@DotNetSolutions
No tweets found

Recent blog items
Dot Net Principal Software Architect Awarded Azure MVP

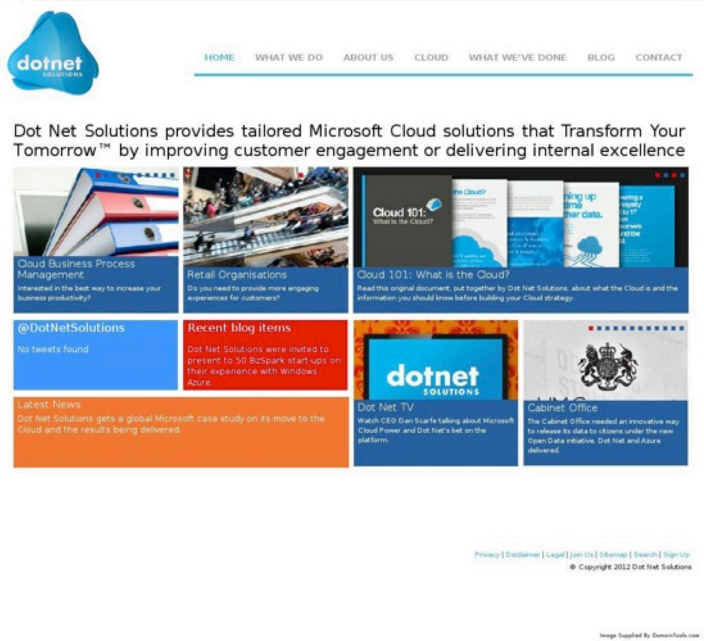
Latest News
Dot Net Solutions gets a global Microsoft case study on its move to the Cloud and the results being delivered.

Dot Net TV
Watch CEO Dan Scarfe talking about Microsoft Cloud Power and Dot Net's bet on the platform.

Privacy | Disclaimer | Legal | Join Us | Sitemap | Search | Sign Up
© Copyright 2012 Dot Net Solutions

Image Supplied By DomainTools.com

Earlier:



Dot Net Solutions provides tailored Microsoft Cloud solutions that Transform Your Tomorrow™ by improving customer engagement or delivering internal excellence

Cloud Business Process Management
Interested in the best way to increase your business productivity?

Retail Organisations
Do you need to provide more engaging experiences for customers?

Cloud 101: What is the Cloud?
Read this original document, put together by Dot Net Solutions, about what the Cloud is and the information you should know before building your Cloud strategy.

@DotNetSolutions
No tweets found

Recent blog items
Dot Net Solutions were invited to present to 50 BizSpark start-ups on their experience with Windows Azure.

Latest News
Dot Net Solutions gets a global Microsoft case study on its move to the Cloud and the results being delivered.

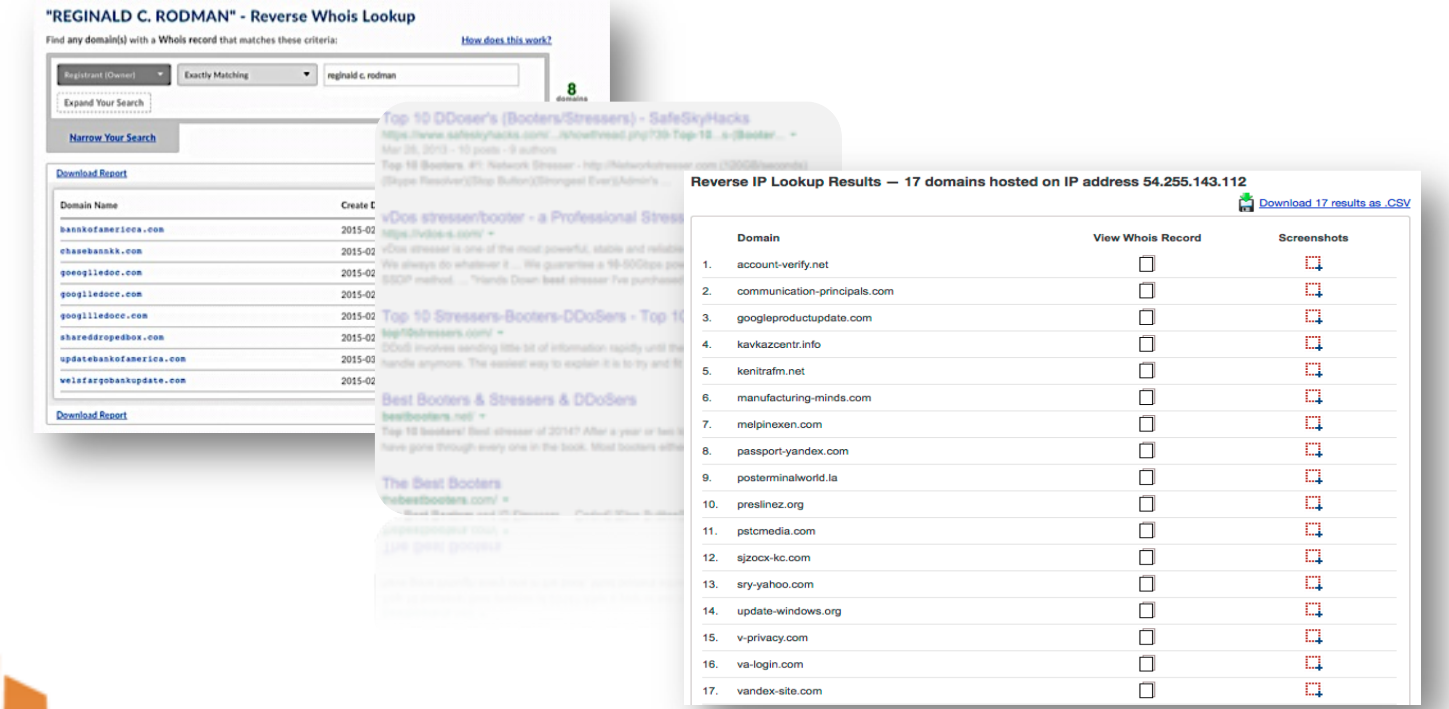
Dot Net TV
Watch CEO Dan Scarfe talking about Microsoft Cloud Power and Dot Net's bet on the platform.

Cabinet Office
The Cabinet Office needed an innovative way to release its data to citizens under the new Open Data initiative. Dot Net and Azure delivered.

Privacy | Disclaimer | Legal | Join Us | Sitemap | Search | Sign Up
© Copyright 2012 Dot Net Solutions

Image Supplied By DomainTools.com

Apply It…



"REGINALD C. RODMAN" - Reverse Whois Lookup

Find any domain(s) with a Whois record that matches these criteria:

How does this work?

Registrant (Owner) | Exactly Matching | reginald c. rodman

8 domains

Expand Your Search

Narrow Your Search

Download Report

Domain Name	Create D
bannkofamericca.com	2015-02
chasebannkk.com	2015-02
goeoglledoc.com	2015-02
googlledocc.com	2015-02
googllledocc.com	2015-02
shareddropedbox.com	2015-02
updatebankofamerica.com	2015-03
welsfargobankupdate.com	2015-02

Download Report

Top 10 DDoser's (Booters/Stressers) - SafeSkyHacks
https://www.safeskyhacks.com/.../showthread.php?39-Top-10...s-(Booter... ▾
Mar 26, 2013 - 10 posts - 9 authors
Top 10 Booters. #1: Network Stresser - http://Networkstresser.com (120GB/seconds) (Skype Resolver)(Stop Button)(Strongest Ever)(Admin's ...

vDos stresser/booter - a Professional Stress
https://vdos-s.com/ ▾
vDos stresser is one of the most powerful, stable and reliable
We always do whatever it ... We guarantee a 10-50Gbps pow
SSDP method, ... "Hands Down best stresser I've purchased

Top 10 Stressers-Booters-DDoSers - Top 10
top10stressers.com/ ▾
DDoS involves sending little bit of information rapidly until the
handle anymore. The easiest way to explain it is to try and fit

Best Booters & Stressers & DDoSers
bestbooters.net/ ▾
Top 10 booters! Best stresser of 2014? After a year or two
have gone through every one in the book. Most booters eithe

The Best Booters
thebestbooters.com/ ▾

Reverse IP Lookup Results — 17 domains hosted on IP address 54.255.143.112

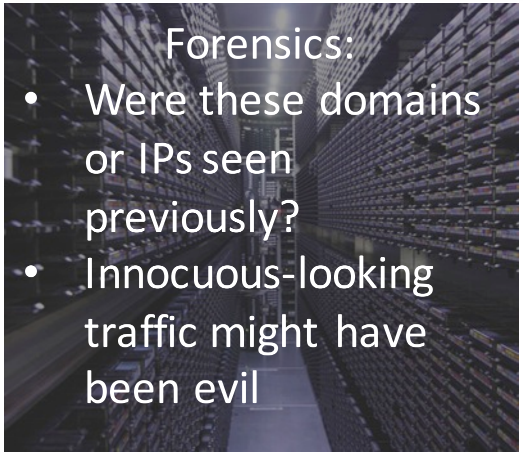
Download 17 results as .CSV

	Domain	View Whois Record	Screenshots
1.	account-verify.net	□	⬚
2.	communication-principals.com	□	⬚
3.	googleproductupdate.com	□	⬚
4.	kavkazcentr.info	□	⬚
5.	kenitrafm.net	□	⬚
6.	manufacturing-minds.com	□	⬚
7.	melpinexen.com	□	⬚
8.	passport-yandex.com	□	⬚
9.	posterminalworld.la	□	⬚
10.	preslinez.org	□	⬚
11.	pstcmedia.com	□	⬚
12.	sjzocx-kc.com	□	⬚
13.	sry-yahoo.com	□	⬚
14.	update-windows.org	□	⬚
15.	v-privacy.com	□	⬚
16.	va-login.com	□	⬚
17.	yandex-site.com	□	⬚

OSINT in Continuous Security

It’s not just for IR any more…

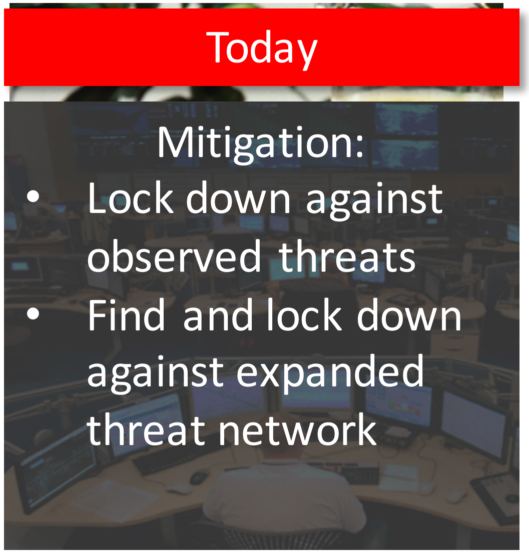
Looking Back



Forensics:

- Were these domains or IPs seen previously?
- Innocuous-looking traffic might have been evil

Today



Mitigation:

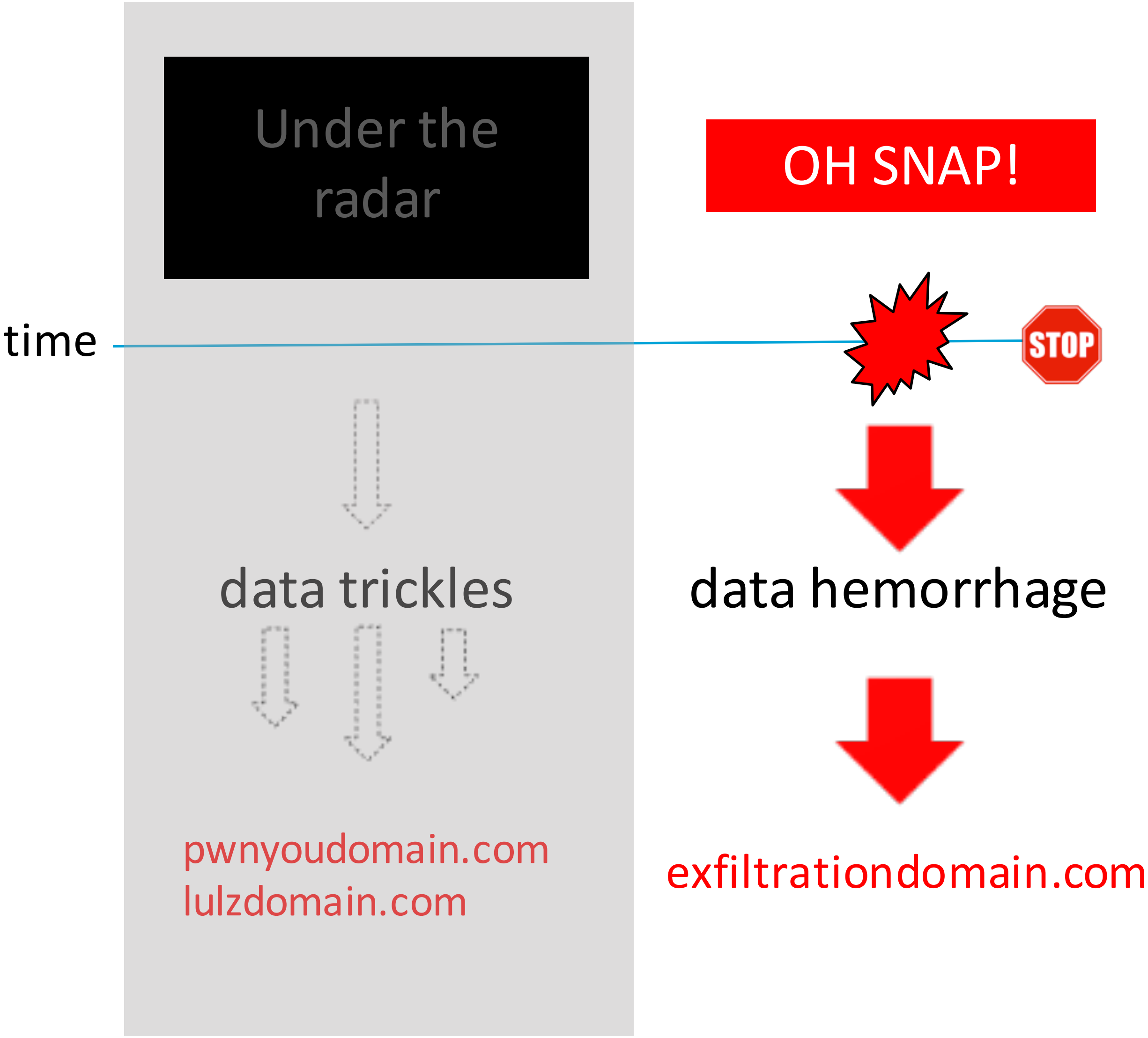
- Lock down against observed threats
- Find and lock down against expanded threat network

Looking Ahead

Prevention:

- Monitor new registrations by this actor
- Defend before attacks are launched

Oh, **Snap**—I’m Breached! Now What?



Under the radar

time

data trickles

pwnyoudomain.com
lulzdomain.com

OH SNAP!

data hemorrhage

exfiltrationdomain.com

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?

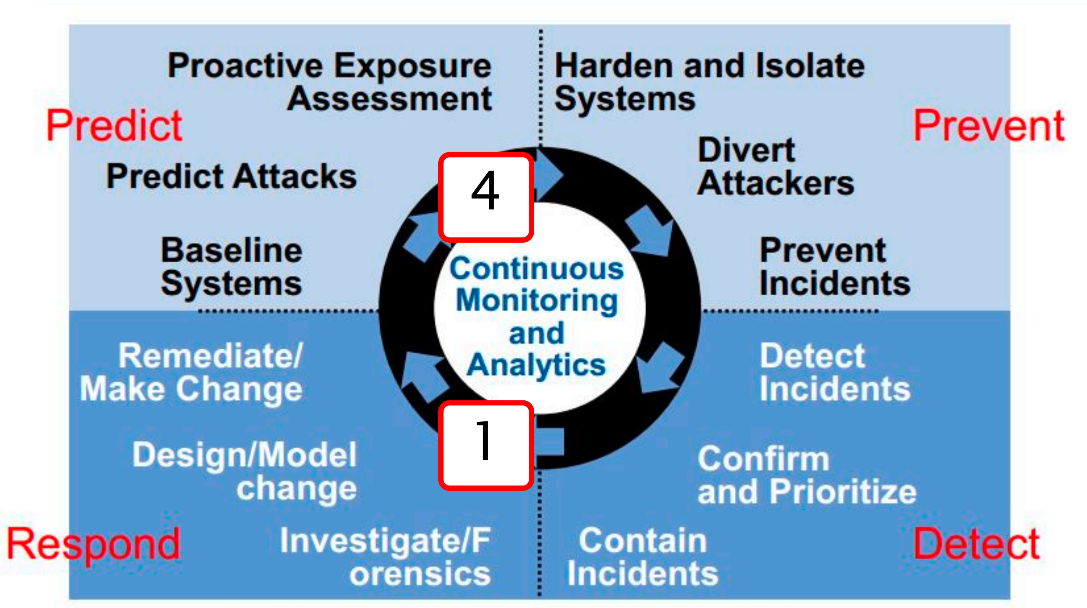
Use OSINT to expand

exfiltrationdomain.com
(nexus discovery) ->
(expansion) ->
pwnyoudomain.com
lulzdomain.com
wewinulosedomain.com
…etc

OSINT in Continuous Security and for Hunt Teams

3

2



dicators,
ted assets

s for earlier
panded threat

squatters,
omain

ock new threat

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

@timhelming