

# RSA® Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: AIR-RO4

## Using Large Scale Data to Provider Attacker Attribution for Unknown IOC's

Connect  Protect



**Dan Hubbard**

CTO OpenDNS, a Cisco company  
[@dhubbard858](https://twitter.com/dhubbard858)

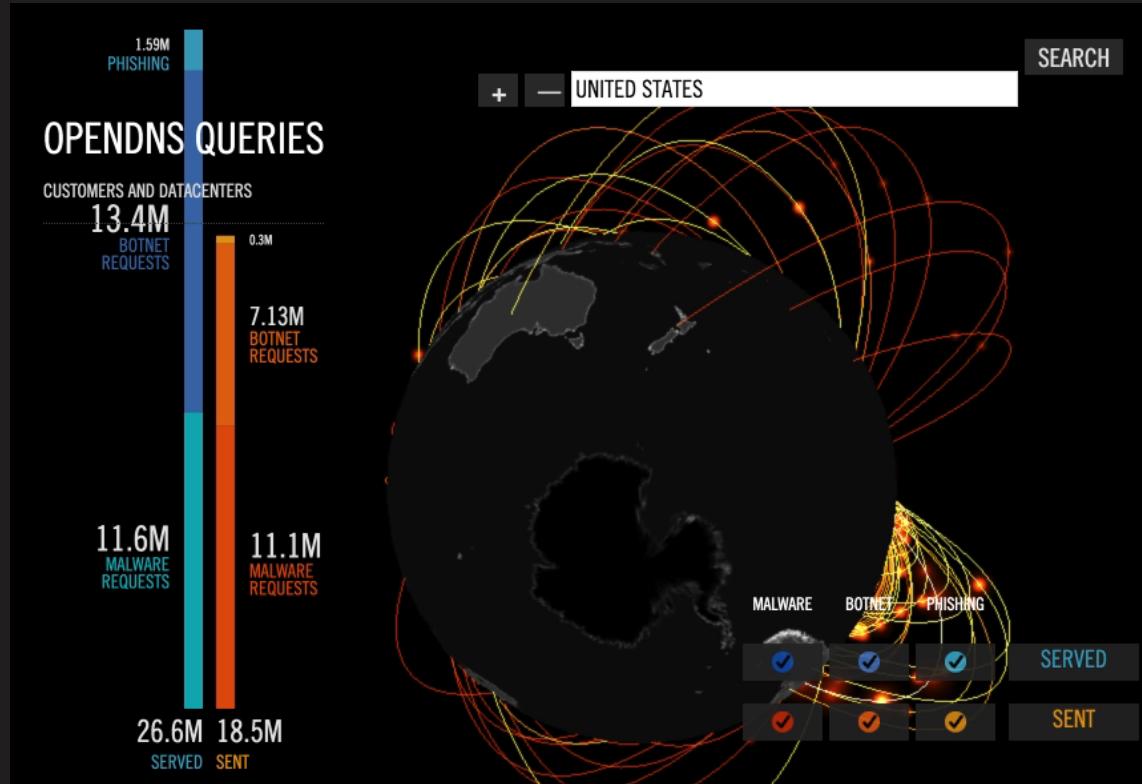
**Dhia Mahjoub**

Technical Leader, OpenDNS  
[@dhialite](https://twitter.com/dhialite)



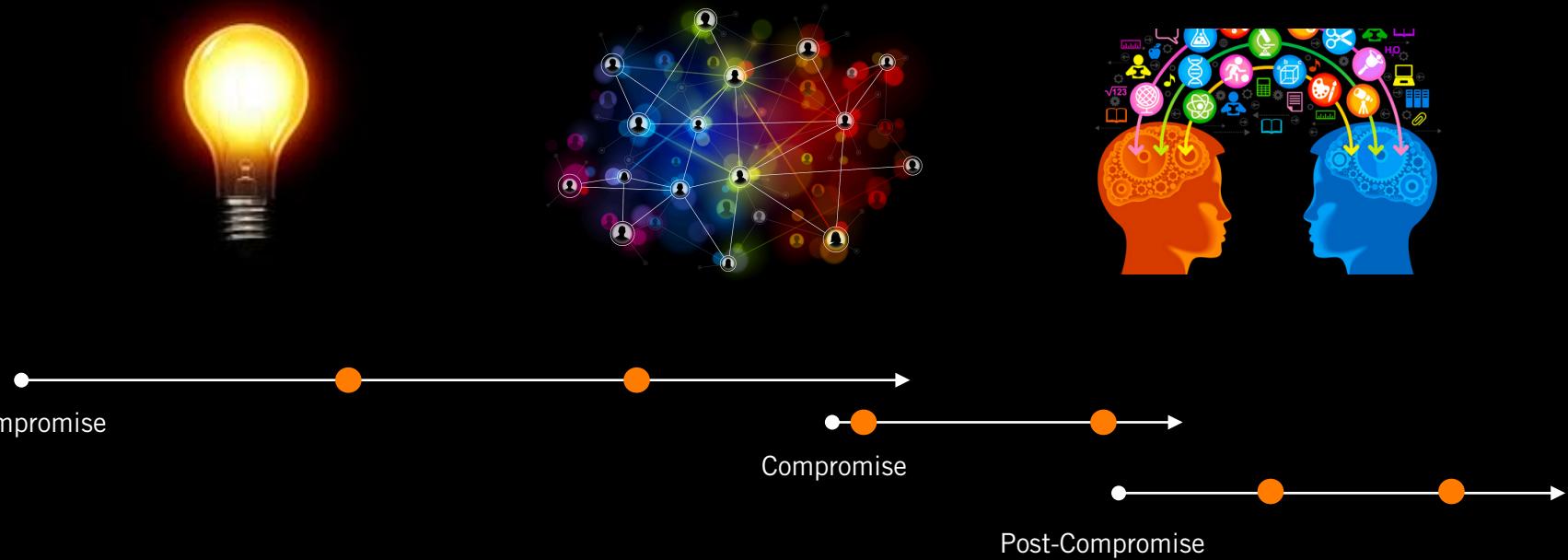
#RSAC

# Our Data



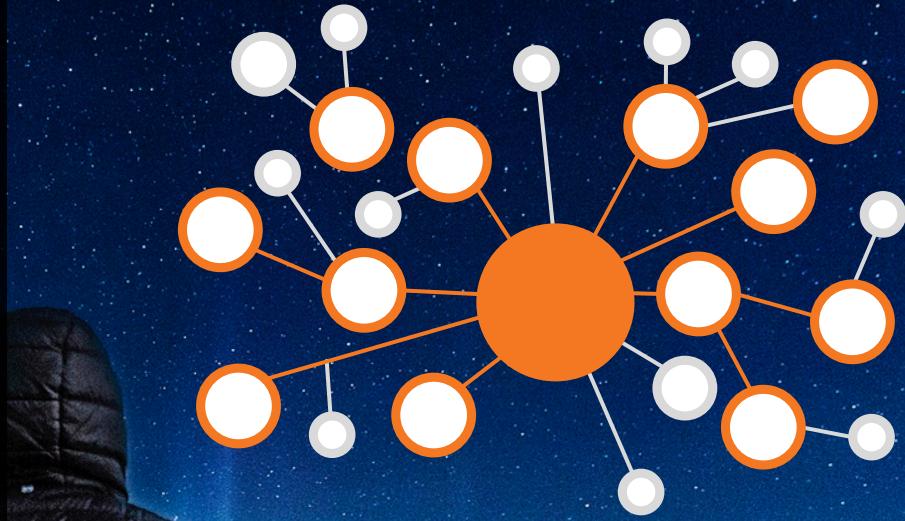
# Inferences of Guilt

---



# Inferences of Attribution

---



# Can we build security context around inferences?

---



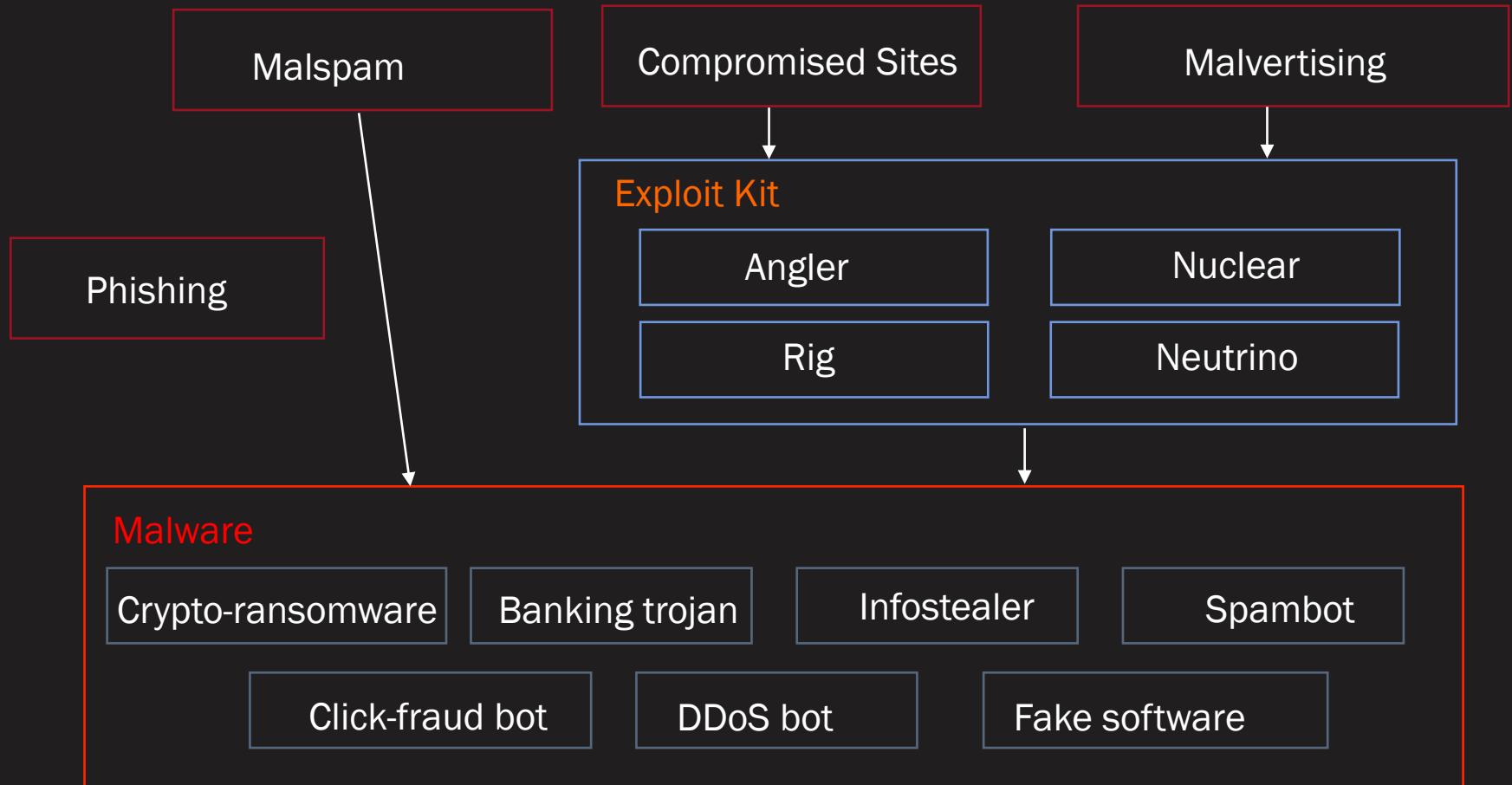
Decrease dwell time in response and enable focused hunting.

---



# Threat Landscape

---



# Acoustic Models

---

# SPRank

---

- **Challenge:** Build scalable detection models that are:
    - Generic to rapidly catch a large number of malware domains/IPs of various types
    - Specific to provide context and details about detected threats
  - Design detection that is immune to evasion and obfuscation by adversaries
  - Focus on below the recursive DNS layer
  - Inspect DNS query features that are harder to change at global scale
  - Assimilate DNS traffic patterns to sound waves
- ➔ Detect domains that show spike in traffic over a short time window (e.g. 1 hour)

# SPRank

springweirtransferrerrisque.communicationtrainingforathletes.com

INVESTIGATE

Visualize

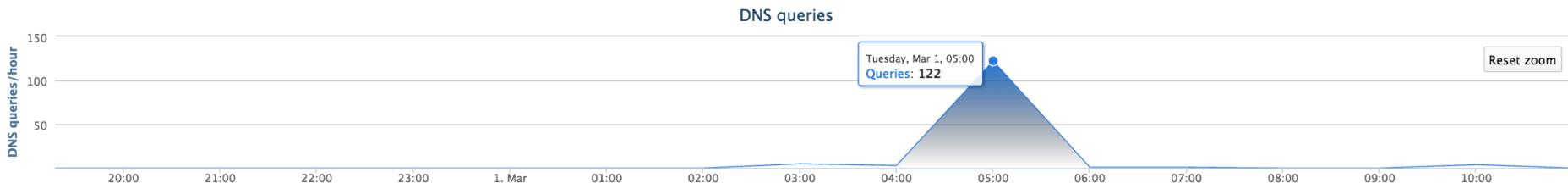
Search in Google

Search in VirusTotal

## DETAILS FOR SPRINGWEIRTRANSFERRERRISQUE.COMMUNICATIONTRAININGFORATHLETES.COM

One or more of the IP addresses that this domain resolves to are currently blocked by OpenDNS

This domain is currently in the OpenDNS Security Labs block list

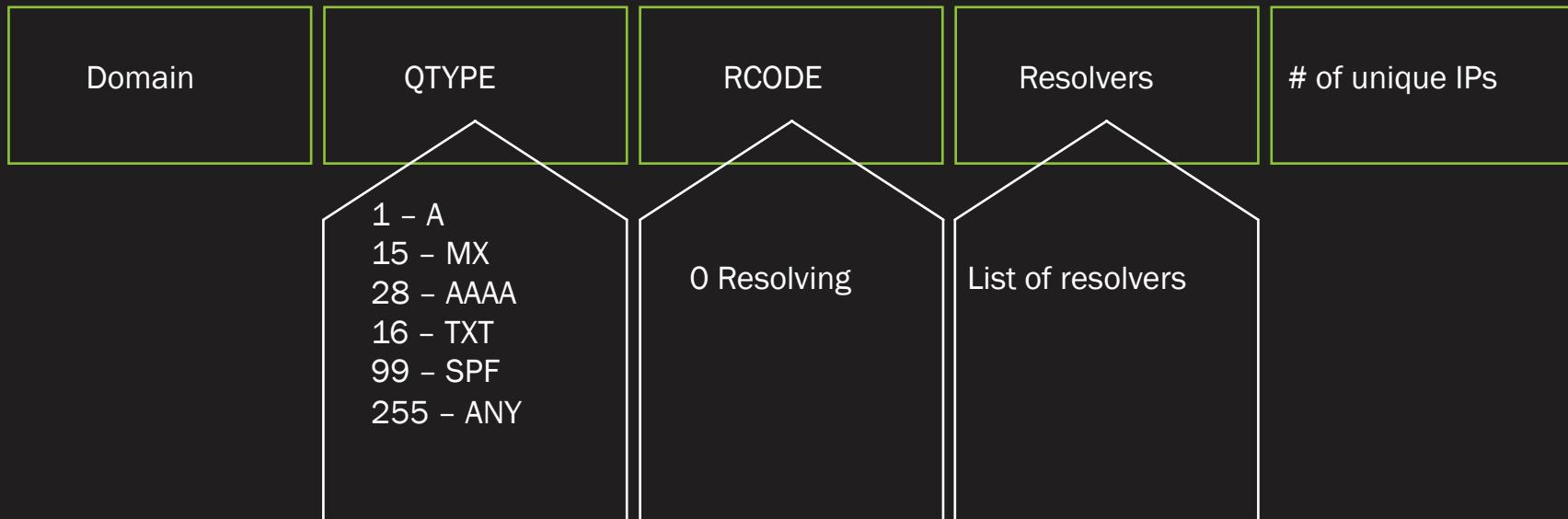


Dhia Mahjoub, Thomas Mathew, BruCon 2015, Flocon 2016, Kaspersky SAS 2016

United States ODNS-01010US0;62/202,662

# SPRank DNS Features

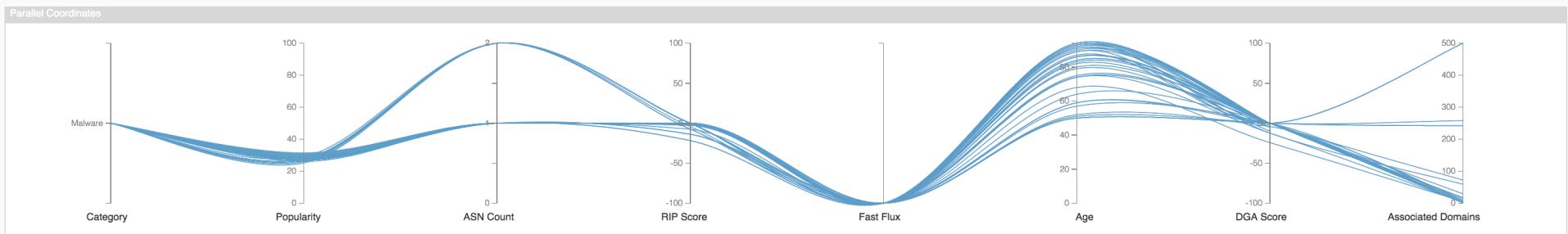
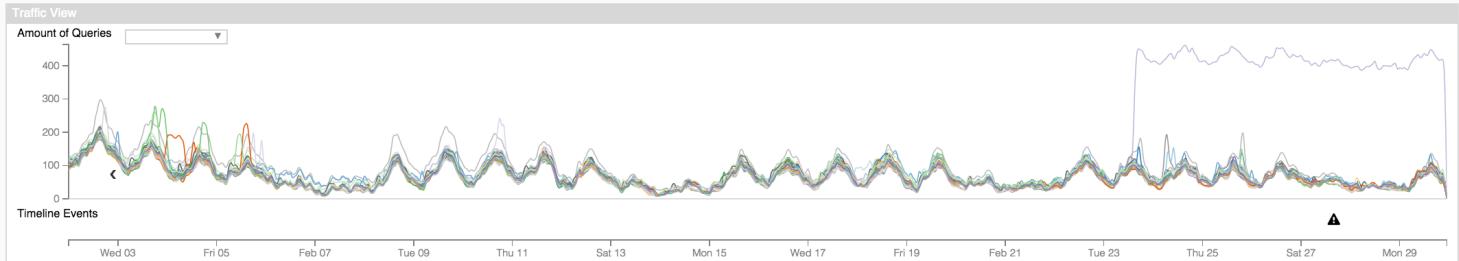
---



# SPRank DNS Features

---

springweirtransferrerisque.communicationtrainingforathletes.com. 3.0 121  
40.33 94 14 {((nyc),5),((ash),6),((yvr),4),((ams),2),((cdg),2),((yyz),13),((fra),33),  
((dfw),24),((lax),6),((pao),11),((mia),7),((syd),1),((sea),5),((lon),2)} {((1),114),  
((28),7)}



Keep Only Remove Export CSV Send To

<input type="checkbox"/> Domain	Category	Popularity	ASN Count	RIP Score	Fast Flux	Age	DGA Score	Associated Domains
aglobal.kz	Malware	27.65	1	-1.86	false	93.00	0.00	
amaisdecor.com.br	Malware	26.88	1	0.00	false	57.00	0.00	
americanfinance33.tk	Malware	26.04	2	-7.44	false	82.00	-5.18	
andreyantonenko.tk	Malware	25.13	2	0.00	false	50.00	0.00	
anoopvarier.in	Malware	27.65	1	-13.67	false	75.00	0.00	1
anton-petrov.su	Malware	27.65	1	-2.00	false	94.00	0.00	15
apbinary.tk	Malware	27.65	2	0.00	false	50.00	0.00	
apinside.it	Malware	27.65	1	-13.96	false	94.00	0.00	
apoption.tk	Malware	26.88	2	-0.47	false	59.00	0.00	
apps-hub.in	Malware	27.65	1	-7.52	false	92.00	0.00	72
apttrader.tk	Malware	26.04	2	0.00	false	50.00	0.00	
ariixhouse.nl	Malware	30.29	1	0.00	false	79.00	-9.72	
aveskamp.org	Malware	28.38	1	0.00	false	87.00	0.00	500
babylicious.ie	Malware	29.05	1	0.00	false	92.00	0.00	
cheapshirts.us	Malware	30.86	1	-2.59	false	93.00	0.00	17
chemiavskaja.com	Malware	27.65	1	-0.54	false	94.00	0.00	1

# SPRank Detections

---

Exploit kits

DGA

Phishing

Fast flux  
malware  
CnC

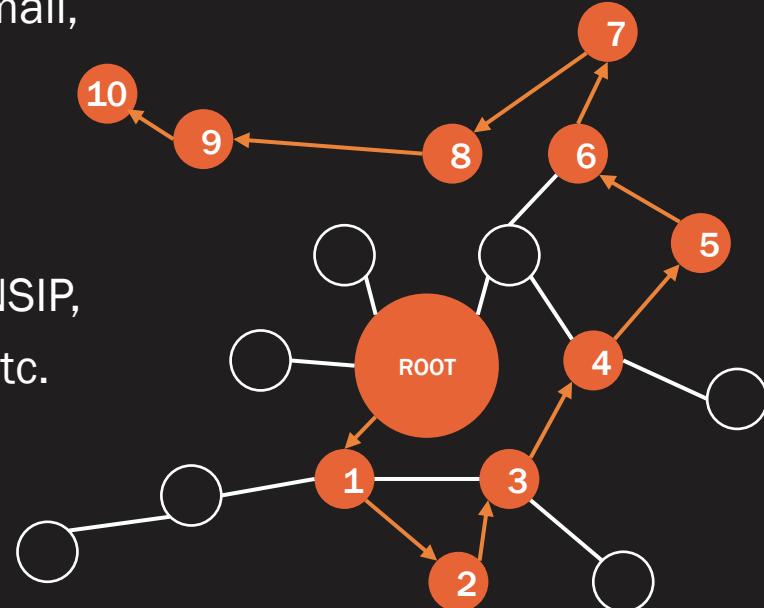
Crypto-  
ransomware  
CnC

## Enrich and Expand at Scale

---

# Expand Technical Threat Intelligence Knowledge

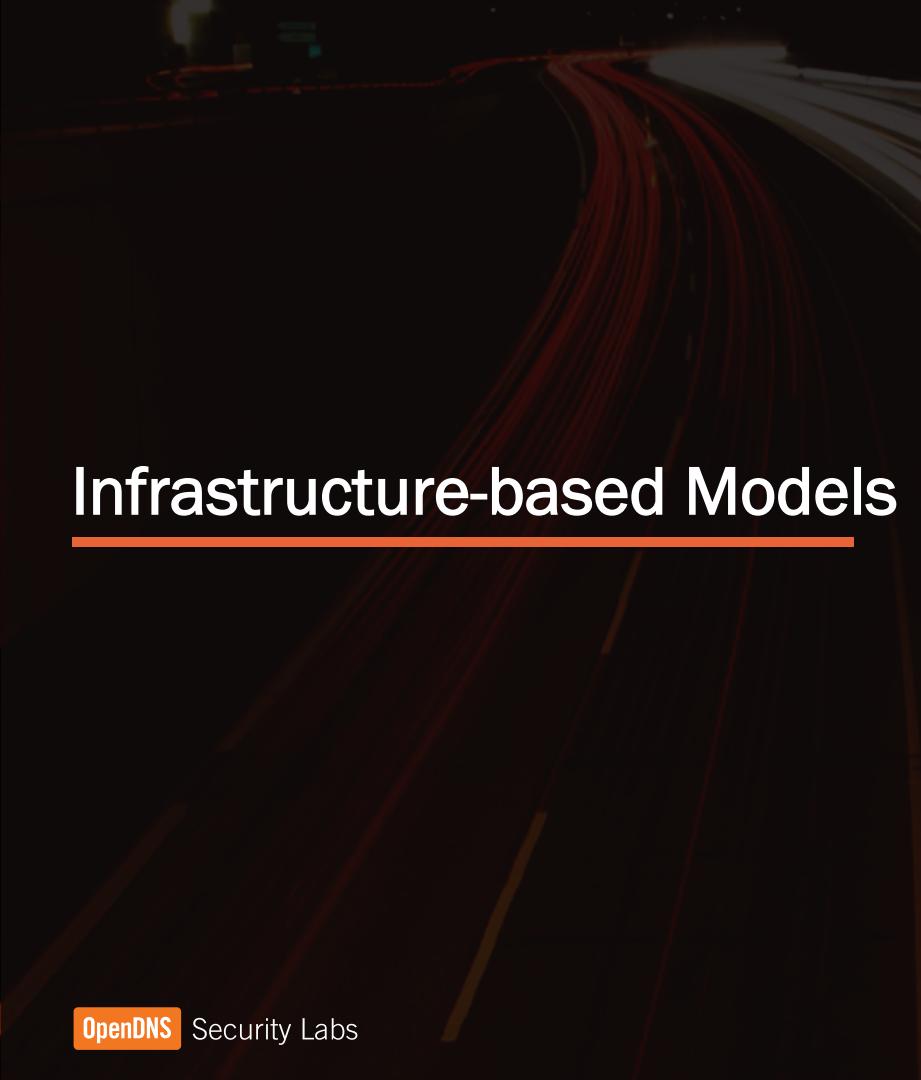
- Graph representation of IOCs and their relationships
- Node = IOC, e.g. domain, IP, domain whois email, IP whois email, ASN, prefix, hash, etc.
- Edge = bidirectional expansion relationship between IOCs , e.g. domain to IP, domain to NSIP, domain to whois email, hash to C2 domain, etc.



# Expand Technical Threat Intelligence Knowledge

---

- Start a search with a seed, e.g. SPRank, NLPRank, Fast flux, DGA, etc., sample analysis, proxy logs, threat reports, etc.
- **Warning:** Dilution of threat signal from hop to hop b/c of shared hosting IPs, sinkhole IPs, sinkholed domains, sinkhole NSs, samples that make noisy/smokescreen calls, etc.
- Human analyst or automatic scripts should apply efficient filters on edge traversal



# Infrastructure-based Models

---



# IOCs Related to Domain Registration and Hosting

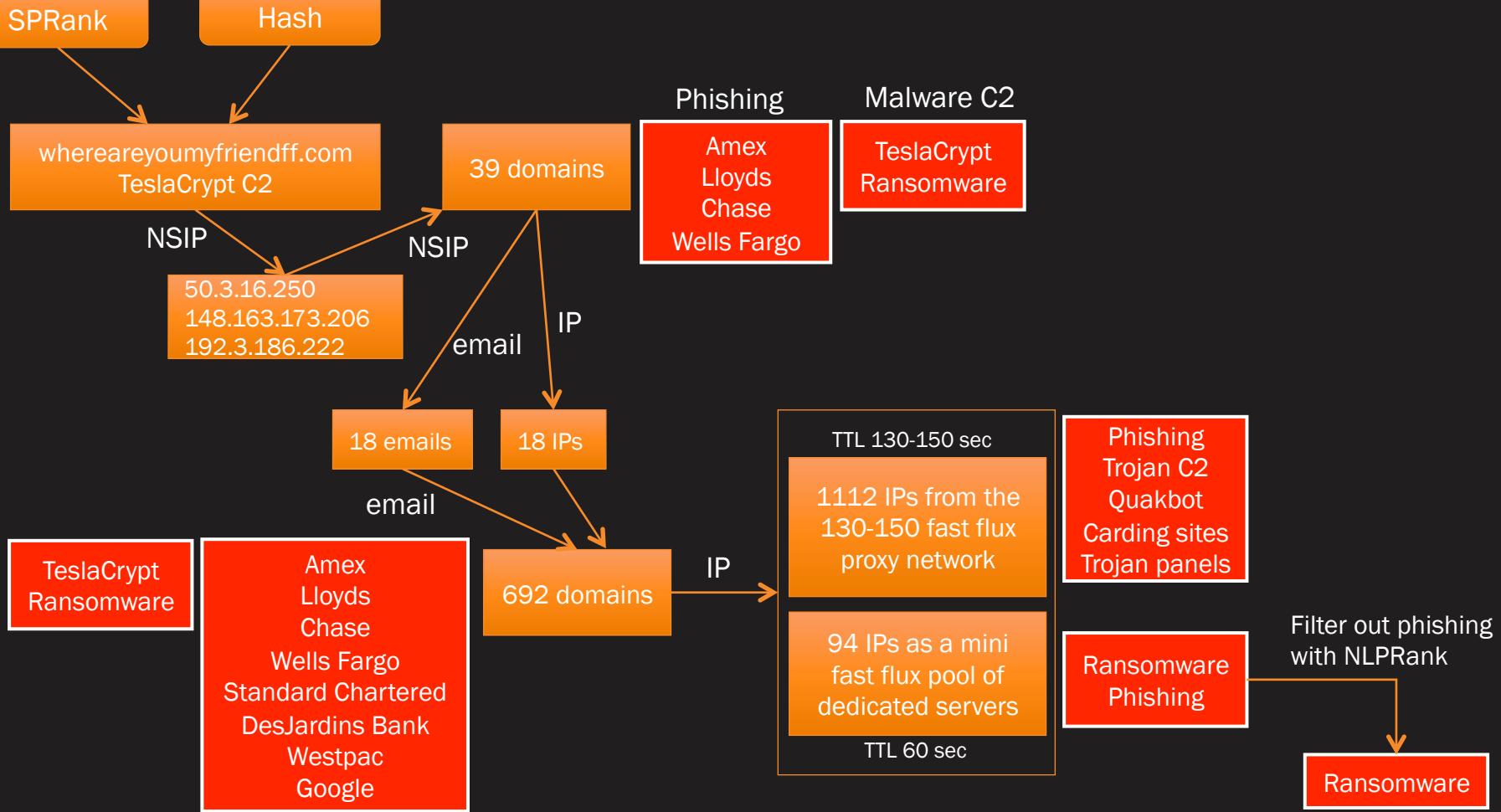
---

- Pivot around IPs
- Pivot around domain whois email
- Pivot around name servers
- Pivot around name server IPs
- Mine domains in /24 or smaller range, e.g. /29, /30
- Mine fast flux proxy networks

# Derive Tactical Intelligence from Technical IOCs

---

- **Goal:** From Technical IOCs, derive Tactical intelligence:
  - About hosting infrastructures and registration patterns
  - About malware campaign patterns:
    - Domain query patterns, pattern similarity, timing, correlation with other events
    - IP querying or hosting patterns
- **Objective of Tactical Intelligence:**
  - predictive IOC blocking,
  - understanding of crimeware TTPs for preventive measures, take-down operations



# TeslaCrypt example – Pool of Dedicated Fast Flux IPs

---

20	36352	AS-COLOCROSSING - ColoCrossing,US
14	16276	OVH OVH SAS,FR
8	50673	SERVERIUS-AS Serverius Holding B.V.,NL
5	8100	ASN-QUADRANET-GLOBAL - QuadraNet, Inc,US
5	62638	QUERY-FOUNDRY - Query Foundry, LLC,US
5	56694	DHUB Telecommunication Systems, LLC,RU
4	46664	VOLUMEDRIVE - VolumeDrive,US
4	201094	GMHOST Alexander Mulgin Serginovic,UA
3	63294	FEVVO - Fevvo, Inc,US

- Pool of VPS, VDS machines in ARIN and RIPE based hosting providers

# TeslaCrypt example – “130-150” Fast Flux Network

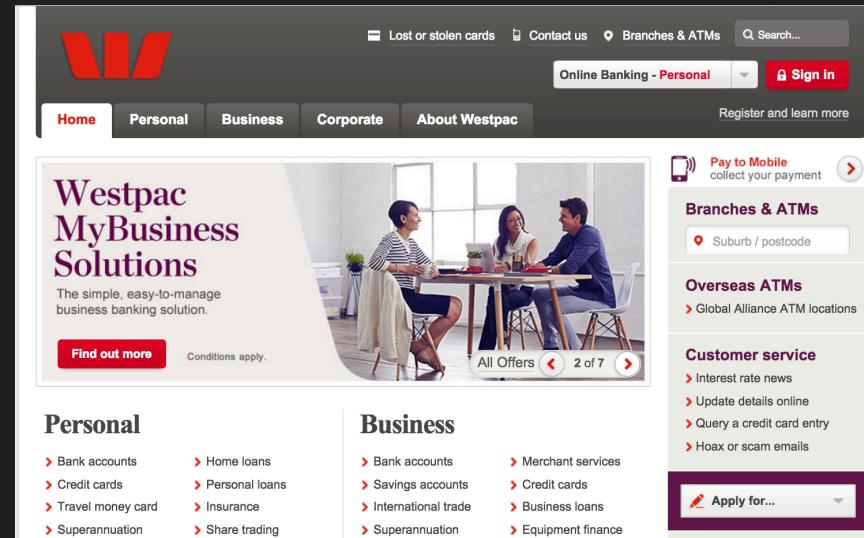
---

100	15895	KSNET-AS _Kyivstar_ PJSC,UA
83	8708	RCS-RDS RCS & RDS SA,RO
56	25229	VOLIA-AS Kyivski Telekomunikatsiyni Merezhi LLC,UA
37	13188	BANKINFORM-AS CONTENT DELIVERY NETWORK LTD,UA
24	34661	BREEZE-NETWORK TOV TRK _Briz_,UA
24	15377	FREGAT-AS ISP _Fregat_ Ltd.,UA
23	31272	WILDPARK-AS WildPark Co,UA
15	12714	TI-AS Net By Net Holding LLC,RU
14	6849	UKRTELNET PJSC UKRTELECOM,UA
13	6703	ALKAR-AS PRIVATE JOINT-STOCK COMPANY _FARLEP-INVEST_,RU

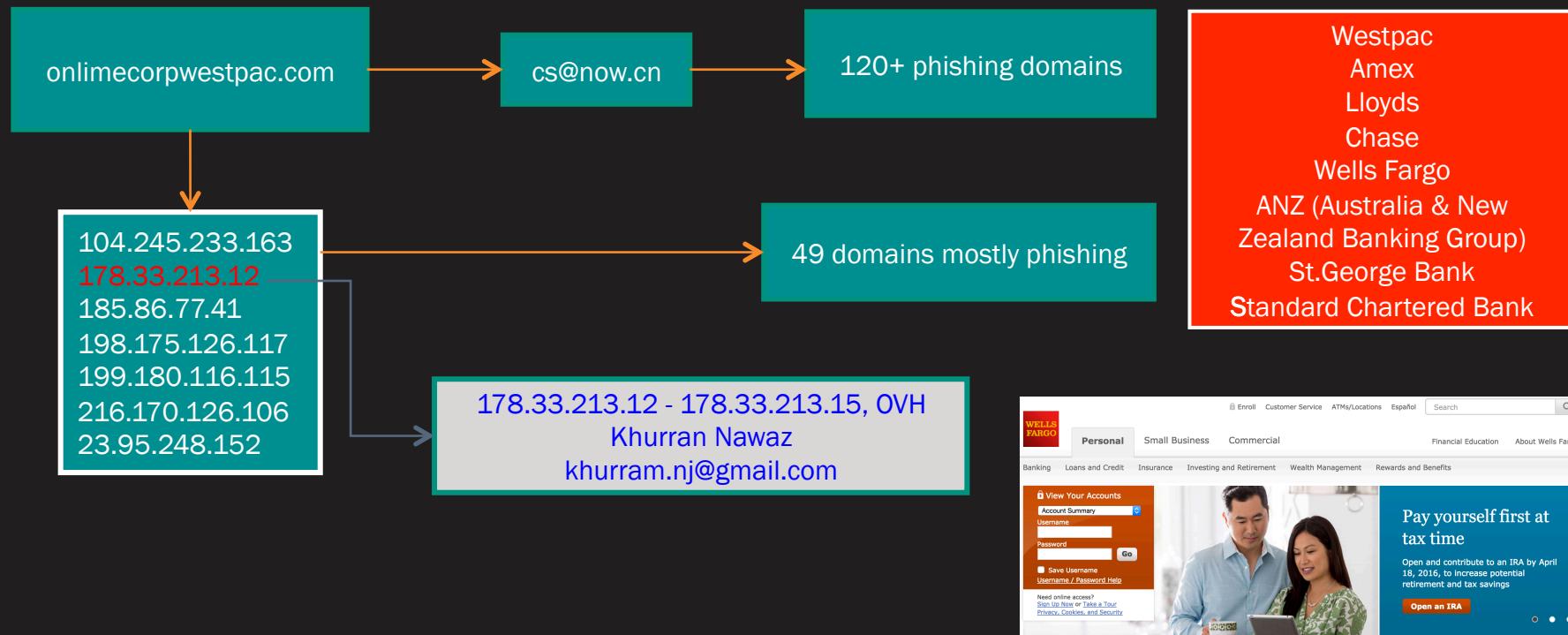
- A pool of IPs from the known fast flux proxy network with TTL 130-150
- 20k+ live compromised broadband, DSL, FIOS residential machines mainly in Ukraine, Russia

# Phishing (1)

- onlimecorpwestpac.com, a Westpac Bank phish
- Registered on Jan 5<sup>th</sup> 2016
- Spike on Jan 6<sup>th</sup>, 11pm, domain live for 6 days

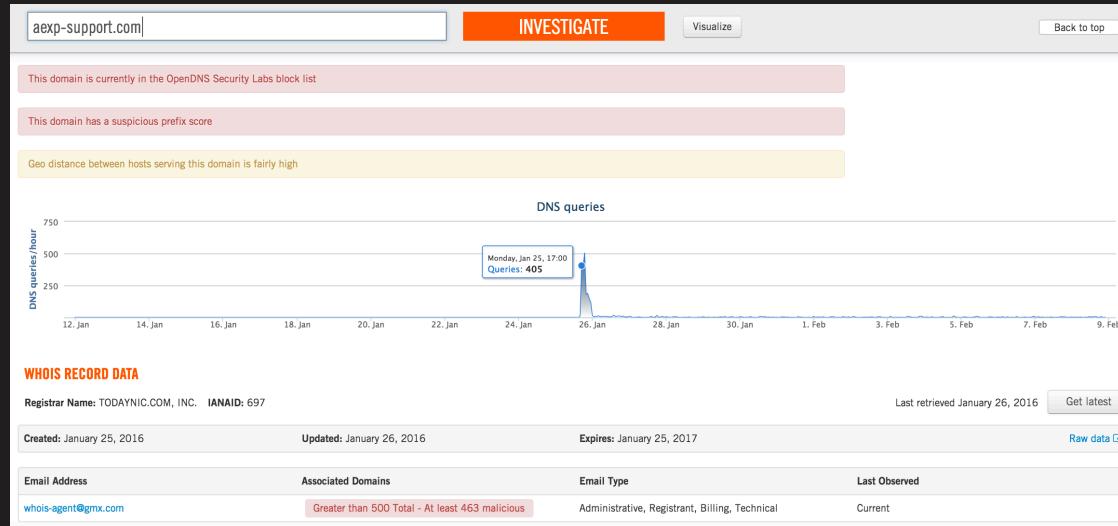


# Phishing (1)

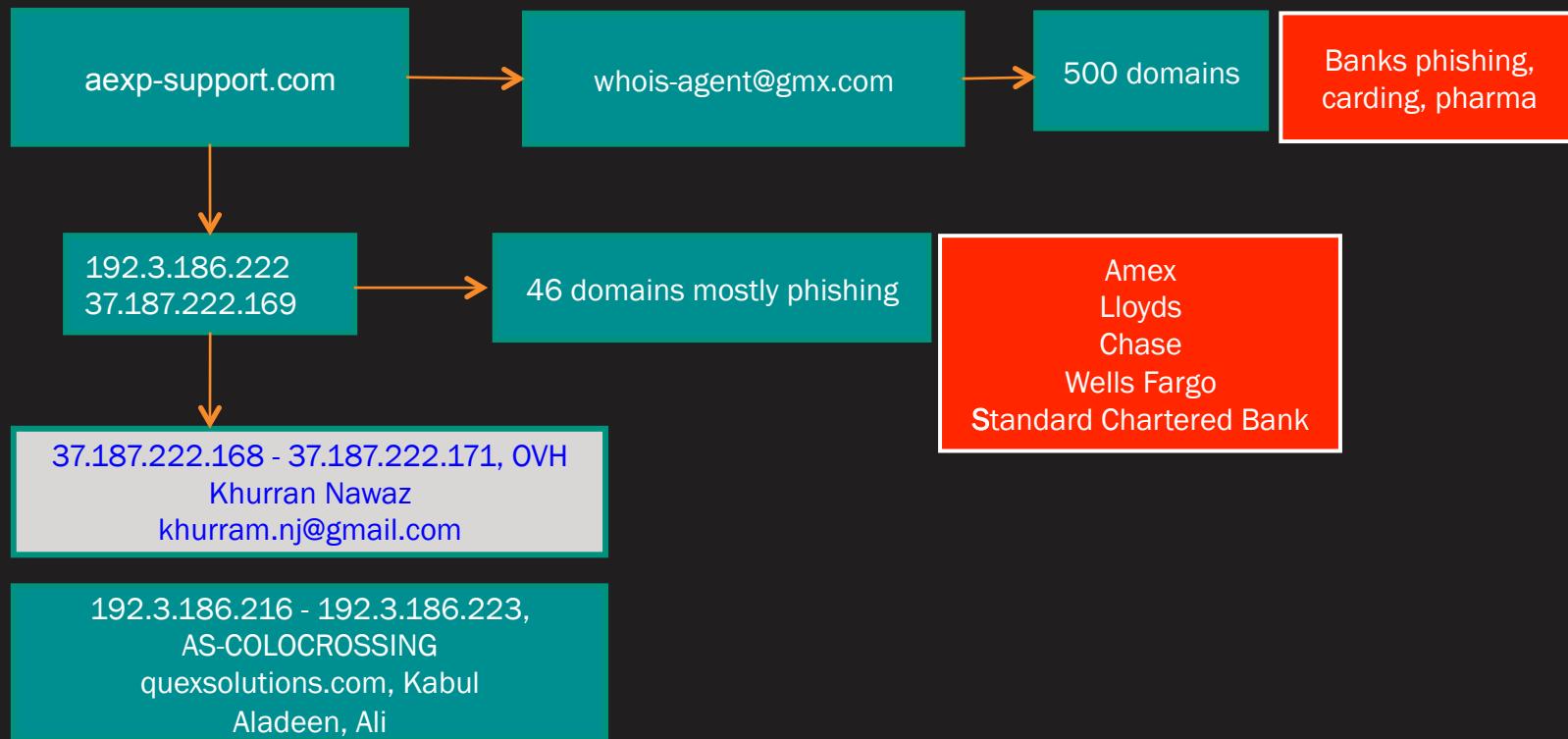


# Phishing (2)

- aexp-support.com, an Amex phish
- Registered on January 25<sup>th</sup> 2016
- Spike on Jan 25<sup>th</sup>, 4pm



# Phishing (2)



## Phishing (2)

---

- Same actor Khurran Nawaz, [khurram.nj@gmail.com](mailto:khurram.nj@gmail.com)
- Registered 2 separate IP ranges on OVH
- **178.33.213.12 - 178.33.213.15**
- **37.187.222.168 - 37.187.222.171**
- Serving domains for phishing campaigns against at least 9 banks in US, Canada, Australia and New Zealand

# Predictive Models

---

# IP Range Fingerprinting

---

- Introduced at Black Hat 2014
- Scan neighboring range for open services & versions, OS version
- Certain attack IPs share identical fingerprints
- If we detect first seed domains by acoustic or other model, then block similar IPs before they start hosting domains

➔ Map out IP space of Bulletproof hosting providers

# IP Range Fingerprinting

---

- iou2386yu.ey346uidhfjj.xyz
- 46.102.152.72, AS51852, <https://www.ghoster.com/>

46.102.152.97 2015-10-04 2015-10-05 1

46.102.152.72 2015-10-03 2015-10-05 2

46.102.152.91 2015-10-03 2015-10-04 1

46.102.152.52 2015-10-02 2015-10-04 2

46.102.152.46 2015-10-02 2015-10-04 2

- 5 IPs in the /24 range are hosting EK domains with similar pattern

# IP Range Fingerprinting

---

- The 5 IPs share the same fingerprint

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)

80/tcp open http nginx web server 1.2.1

Service Info: OS: Linux

- 4 more IPs in /24 have same fingerprint with no hosted domains at the time of discovery. However, they are set up in bulk to host EK domains in the next days. Indeed EK domains appeared shortly

46.102.152.115

46.102.152.123

46.102.152.143

46.102.152.150

## DEDICATED SERVERS

Intel Xeon CPUs & 1Gbits Port

Rapid Deployment - No Need to Wait!

Reliable Hardware & Network

CentOS, Debian, Ubuntu & Windows Server

Location Choice - Europe & USA



PayPal  Skrill  WebMoney Perfect Money  bitcoin  cashU  Litecoin SolidTrust PAY  CHECK ALL

cPanel Web Hosting

Linux VPS

Windows RDP VPS

Dedicated Servers

Domains

 CPANEL HOSTING

\$1.95 /mo.



- PHP, MySQL, Perl, Python, CGI, Ruby (RoR)
- SMTP, POP3/IMAP, Anti-spam/virus

 CPANEL RESELLER

\$24.95 /mo.



- UNLIMITED cPanels
- FREE Site Builder Software

### Top 6 Reasons

Why to Choose QHoster?



Web Hosting Provider Since 2004

# Malware Hosting Patterns

---

Domain  
Shadowing

Hoster  
Hopping

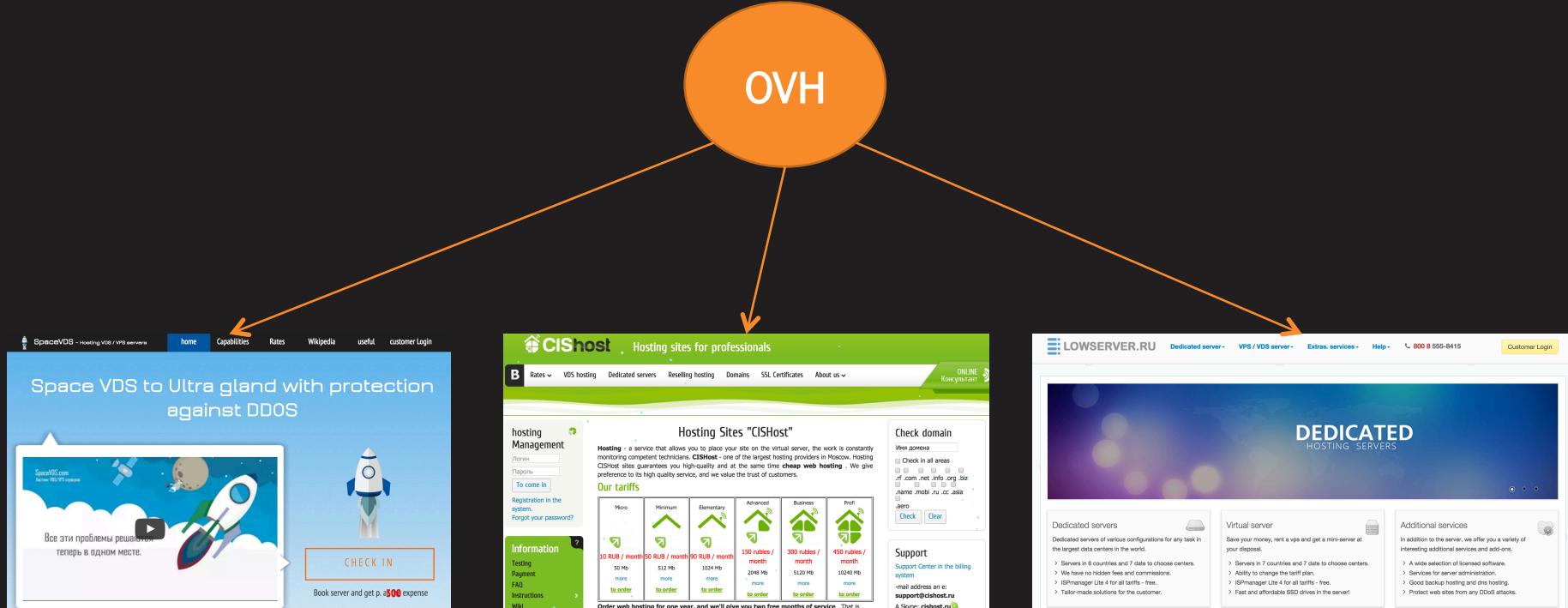
Abused  
Large  
Providers

Concentrated  
Hosting on  
Russian  
Speaking  
Providers

Register  
Offshore  
and  
Diversify IP  
space

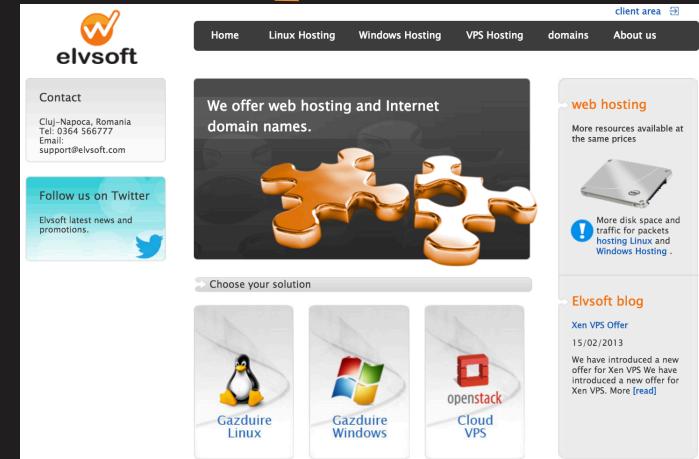
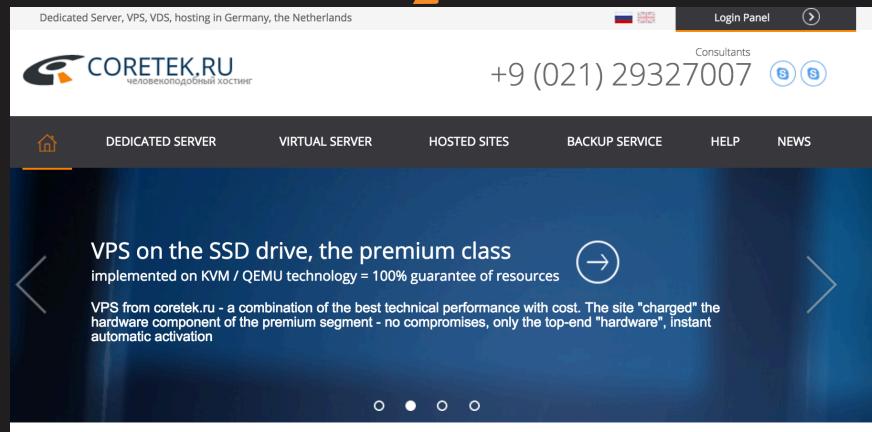
Multi-purpose  
Fast Flux  
Proxy  
Network

# RU Speaking Hosters under Large Providers



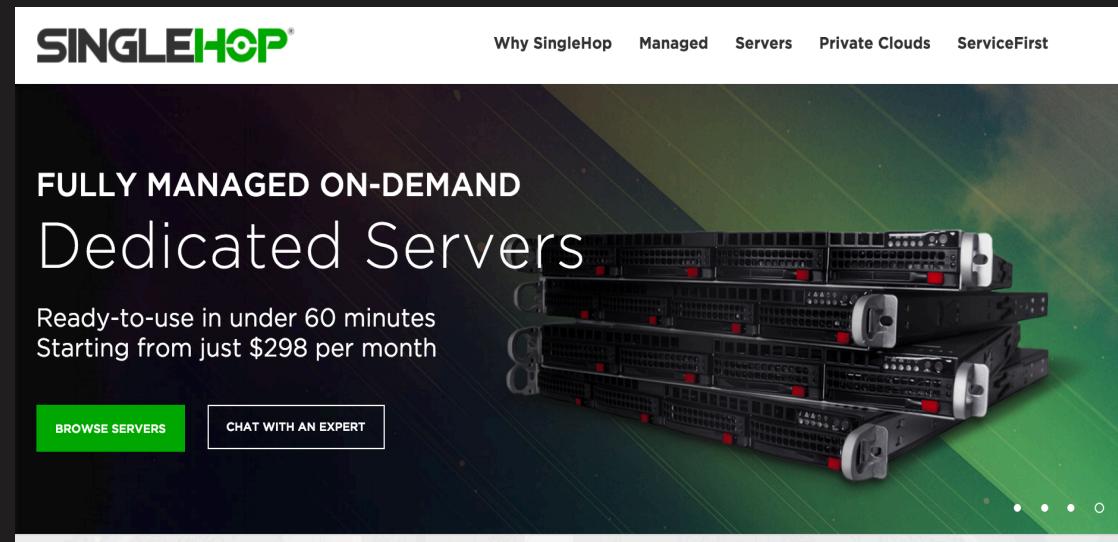
# RU Speaking Hosters under Large Providers

Leaseweb



# Hoster Hopping

- Large abused provider Singlehop : rogue ranges registered by same actor org: robert mcdono to host Angler:
  - 173.236.74.200/29
  - 69.175.20.72/29
  - 69.175.112.224/29
  - 184.154.47.96/29
  - 69.175.66.72/29



# Register Offshore and Diversify IP Space



KING SERVERS  
Dedicated Hosting



24x7 support



Email



Twitter



Sales: +7-800-775-3451



Chat with us, we are online!

Client Login

Register

RU

VPS Hosting

Dedicated Hosting

Fast Delivery Servers

Game hosting

Data backup

Resellers

Discounts

Reviews

## NETWORK OF DATA-CENTERS



- Data processing center Serverius Flevoland
- Data center in Netherlands



- Data processing center HE.net California
- Data center in USA



- Data processing center Telenet Moscow
- Data center in Russia

## SLA MONITORING



Our advantages

Discounts

Fast SSD with VDS

CDN

Network of Data-Centers

Microsoft software

VDS server  
VDS-USA-1G



VDS server  
SSD-RU-512



VDS server  
VDS-NL-2G



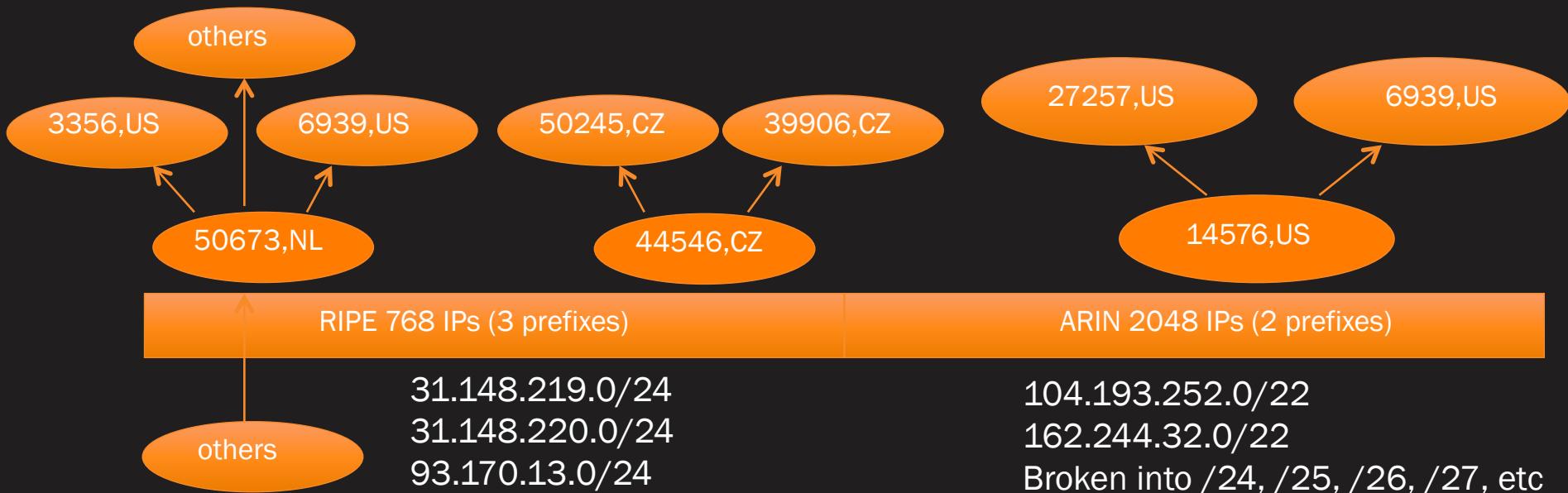
Prepay Promo: Get 1, 2 or 3 months FREE on 3, 6 or 12 month billing. [Chat now for details.](#)

x

# King Servers

- Hosting provider's business registered in **Anguilla**
- Hosting EK domains, malware, porn, insurance scam, fake software, pharma
- 2816 IPs: **2048** IPs in **ARIN** space, **768** IPs in **RIPE** space

# King Servers



# Creating Inferences from Malware Behavior

How can I expand a single behavior indicator to identify others and infer attribution

The screenshot shows a web-based malware analysis interface. At the top, there's a navigation bar with tabs: Behavioral Indicators, Network Activity, Processes, Artifacts, Registry Activity, and File Activity. Below the navigation bar is the ThreatGRID logo and the tagline "Malware Threat Intelligence Platform".

## Analysis Report

ID	01ba0f2d450e2ebc5f9bf8f582477b2c	Filename	56029-132-1327b_eiasus.exe
OS	2600.xpsp.080413-2111	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	2/17/16 15:33:52	Analyzed As	exe
Ended	2/17/16 16:05:52	SHA256	02b00f7615e1fd9091d947dad00dfe60528d9015b694374df2b5525ea6dd1301
Duration	0:32:00	SHA1	8e5c7e0b3a6bca03148976dd0231132416e8a422
Sandbox	phl-work-23 (pilot-d)	MD5	8a19930c553f653861495d5efe5f268b

### Warnings

- Executable Failed Integrity Check

## Behavioral Indicators

**Shadow Copy Deletion Detected**

Volume Shadow Copies are snapshots of portions of a file system used for backups and System Restore points. The 'vssadmin.exe' utility provides a way to remove these copies. Malware authors may delete these copies in order to make recovery and access to a target's original files more difficult.

This is especially true for ransomware varieties which encrypt files since these shadow copies may still contain the files in an unencrypted state.

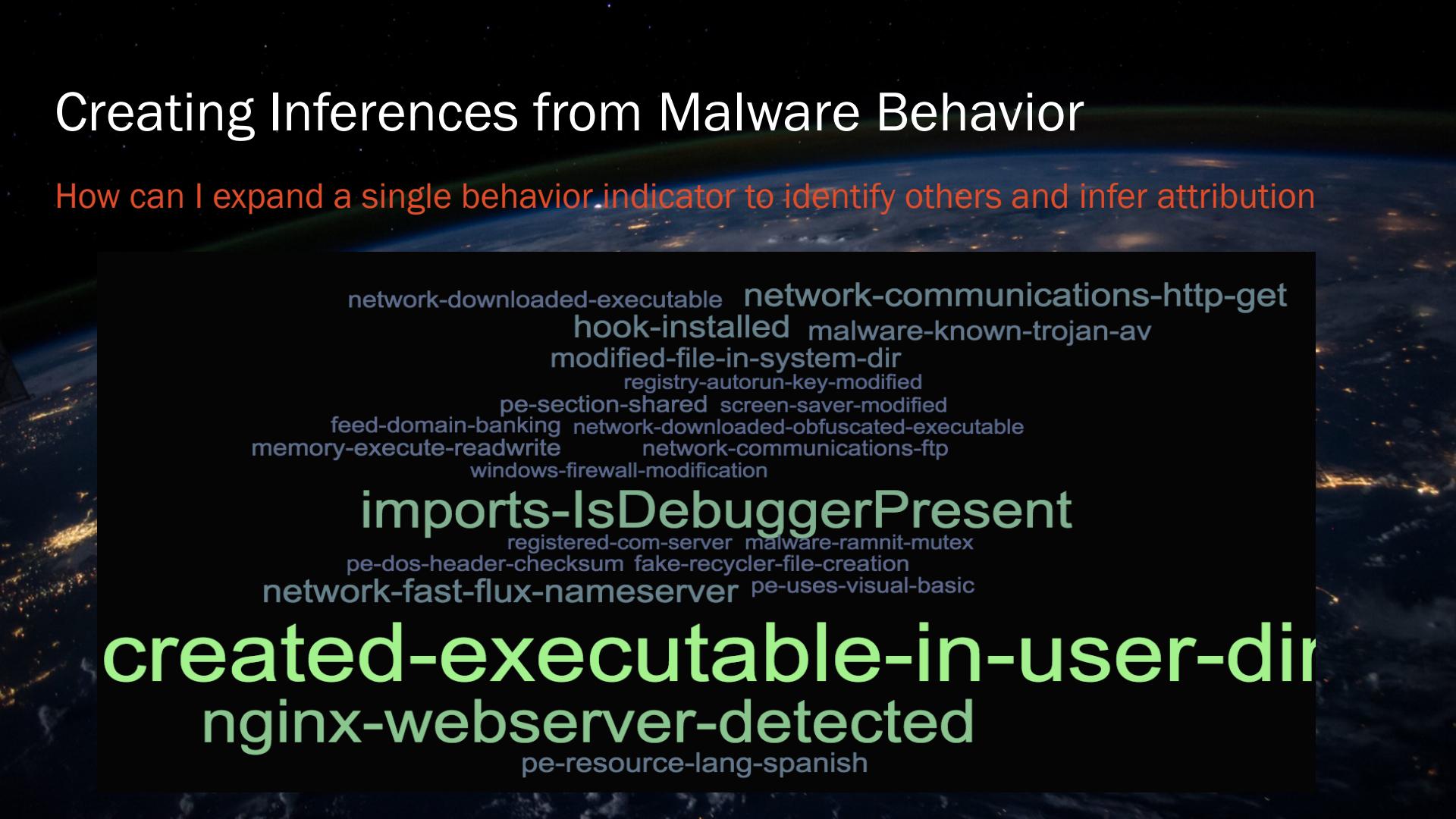
Severity: 100 Confidence: 100

Categories	Tags
weakening	crypto, ransomware, file, system

Command Line	Process Name	Process ID
vssadmin.exe Delete Shadows /All /Quiet	vssadmin.exe	1464 (vssadmin.exe)

# Creating Inferences from Malware Behavior

How can I expand a single behavior indicator to identify others and infer attribution



network-downloaded-executable network-communications-http-get  
hook-installed malware-known-trojan-av  
modified-file-in-system-dir  
registry-autorun-key-modified  
pe-section-shared screen-saver-modified  
feed-domain-banking network-downloaded-obfuscated-executable  
memory-execute-readwrite network-communications-ftp  
windows-firewall-modification

**imports-IsDebuggerPresent**

registered-com-server malware-ramnit-mutex  
pe-dos-header-checksum fake-recycler-file-creation  
network-fast-flux-nameserver pe-uses-visual-basic

**created-executable-in-user-dir**

**nginx-webserver-detected**

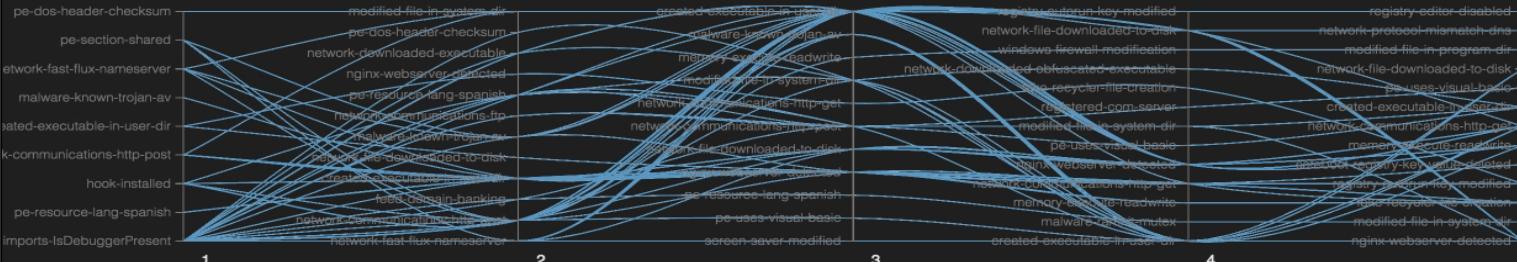
pe-resource-lang-spanish

# Creating Inferences from Malware Behavior

39 / 87 Elements Brushed

Traffic View PC View

Parallel Coordinates



Keep Only Remove Export CSV Send To

	name	1	2	3	4	5
1	b151d3eff7107676962c299a4b74def	imports-IsDebuggerPresent	feed-domain-banking	pe-resource-lang-spanish	malware-ramnit-mutex	modified-file-in-system-dir
2	0a4d0e5d0b69560414bbd20127bd81	pe-resource-lang-spanish	created-executable-in-user-dir	nginx-webserver-detected	memory-execute-readwrite	false-recycler-file-creation
3	62da7996891fa028572e529a36982e	hook-installed	created-executable-in-user-dir	nginx-webserver-detected	network-communications-https-post	false-recycler-file-creation
4	b993b711f953fa63000c31e75c4801	pe-resource-lang-spanish	created-executable-in-user-dir	nginx-webserver-detected	network-communications-https-post	false-recycler-file-creation
5	54ddb7b307b25ae5d3f2c46d04bb1	network-communications-http-post	created-executable-in-user-dir	nginx-webserver-detected	memory-execute-readwrite	fake-recycler-file-creation
6	5a3b2d276b1a2303e4bf1268a04b40	hook-installed	created-executable-in-user-dir	nginx-webserver-detected	network-communications-https-post	fake-recycler-file-creation
7	636bcc21be9534e96593ba6f641ac2e	network-communications-http-post	created-executable-in-user-dir	nginx-webserver-detected	network-communications-https-post	registry-autorun-key-modified
8	d0cdfd1dd56d708d3bf796493c6a535	created-executable-in-user-dir	network-file-downloaded-to-disk	nginx-webserver-detected	network-communications-https-post	safeboot-registry-key-value-deleted
9	5520d165361bdb5f87deb343e34dc8	network-communications-http-post	created-executable-in-user-dir	nginx-webserver-detected	memory-execute-readwrite	false-recycler-file-creation
10	044d8e3201a8c5e4a36b8af989349	network-communications-http-post	created-executable-in-user-dir	nginx-webserver-detected	network-communications-https-post	registry-autorun-key-modified
11	6662930532577d2df3fbe7bd7c8a997	hook-installed	network-communications-https-post	nginx-webserver-detected	network-communications-https-post	registry-autorun-key-modified
12	cdb37fb34d2562084d4223d944755f	malware-known-trojan-av	created-executable-in-user-dir	nginx-webserver-detected	memory-execute-readwrite	false-recycler-file-creation
13	fcc37a0a2d9635513bc904e273a0d3	pe-resource-lang-spanish	created-executable-in-user-dir	nginx-webserver-detected	network-communications-https-post	false-recycler-file-creation
14	098726bef3a1bea1c7f8a1a48849251	network-communications-http-post	created-executable-in-user-dir	nginx-webserver-detected	network-communications-https-post	registry-autorun-key-modified

# Creating Inferences from Malware Behavior



Now lets take each new hash based on behavior from the inferences graph the network indicators.

# Creating Inferences from Malware Behavior

OpenDNS Investigate

DOCUMENTATION DASHBOARD INVESTIGATE SUPPORT dan@opendns.com Sign Out

SEARCH PATTERN SEARCH

hb.net INVESTIGATE Visualize

THREAT SAMPLE (SHA256)  
**3b32b0c7c2262e91a39d0b9423ecf39abd05033da1021c317c9c24513fd0aa1b**

SHA1 25c0ca28174d6008bc2fd17dd2d2e7ad2103a9e3  
MD5 6aed2d44887d40d3683de406d56a3ba9

Search in Google  
Search in VirusTotal

Threat Score: **100**  
First Seen: Feb 23, 2016 20:30:01 UTC  
Full Sample Data from Threat Grid

BEHAVIORAL INDICATORS

Indicator	Confidence ⓘ	Severity ⓘ
Process Created a File in a Fake Recycle Bin folder	100	100
Shadow Copy Deletion Detected	100	100
Excessive Suspicious Activity Detected	100	90
Process Modified an Executable File	100	60
Process Modified File in a User Directory	80	70

# Creating Inferences from Malware Behavior

OpenGraphiti



Nodes

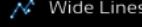


All



Activity

Edges

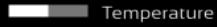


Wide Lines

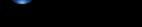


Activity

Physics



Temperature

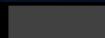


Filters

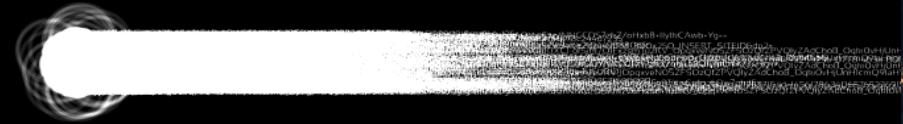
LOD Min/Max

Node LOD

Edge LOD



0 0



# How can you use inferences?

---





OpenDNS is  
now part of Cisco.



Dan Hubbard

@dhubbard858

Dhia Mahjoub

@dhialite