RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

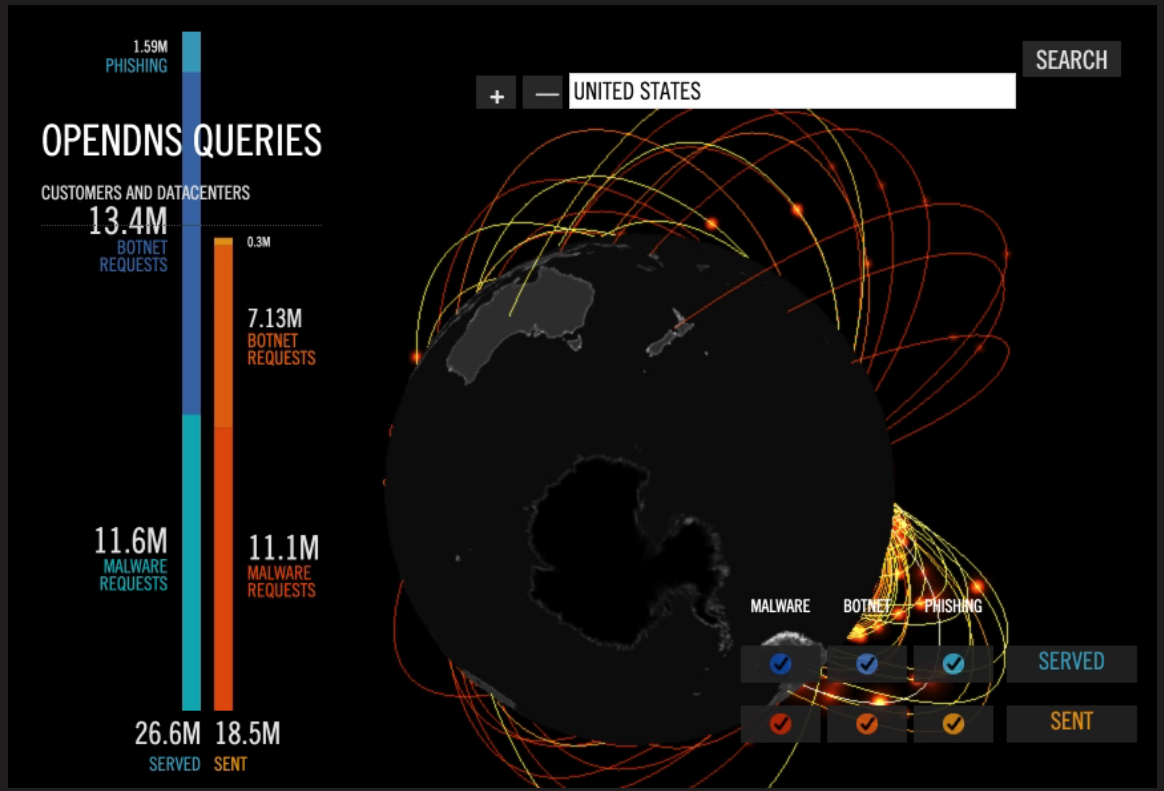
SESSION ID: AIR-RO4

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

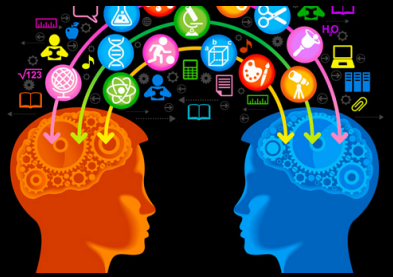
Dan Hubbard
CTO OpenDNS, a Cisco company
@dhubbard858

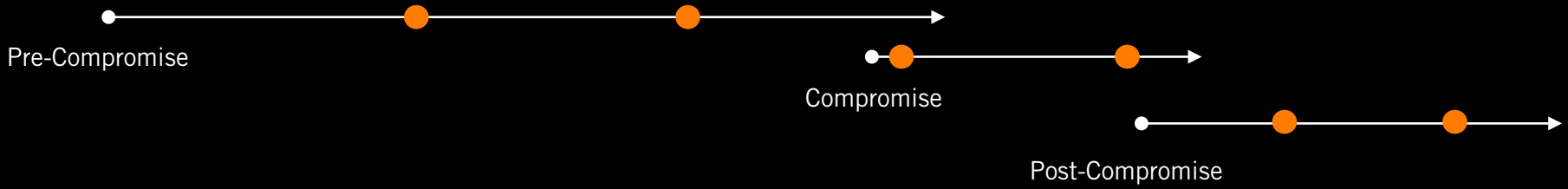
Dhia Mahjoub
Technical Leader, OpenDNS
@dhialite

Our Data


1.59M
PHISHING
OPENDNS QUERIES
CUSTOMERS AND DATACENTERS
13.4M
BOTNET
REQUESTS
0.3M
7.13M
BOTNET
REQUESTS
11.6M
MALWARE
REQUESTS
11.1M
MALWARE
REQUESTS
26.6M
SERVED
18.5M
SENT
SEARCH
UNITED STATES
MALWARE
BOTNET
PHISHING
SERVED
SENT

Inferences of Guilt



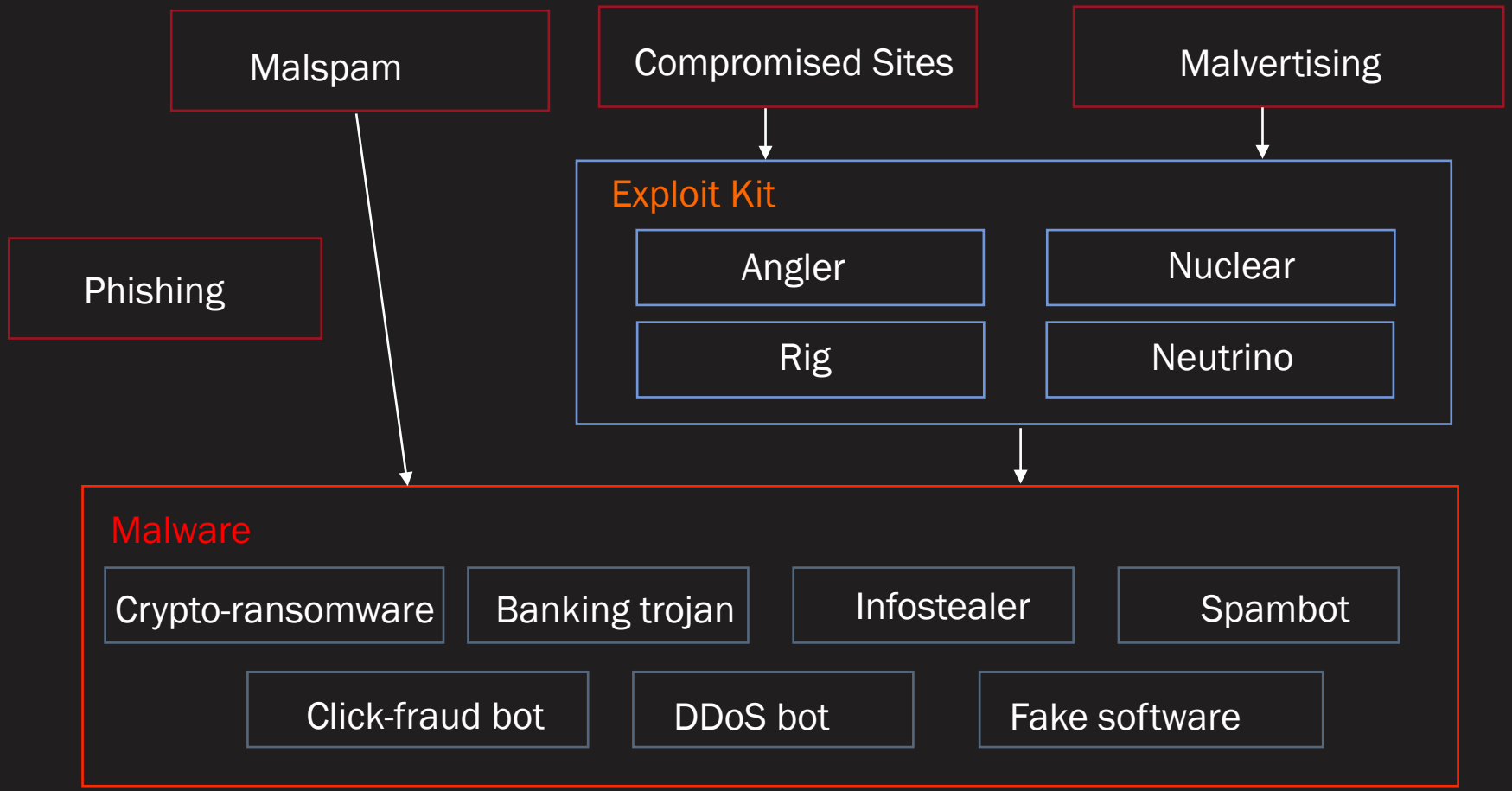


Inferences of Attribution

Can we build security context around inferences?

Decrease dwell time in response and enable focused hunting.

Threat Landscape


Malspam
Compromised Sites
Malvertising
Exploit Kit
Angler
Nuclear
Rig
Neutrino
Phishing
Malware
Crypto-ransomware
Banking trojan
Infostealer
Spambot
Click-fraud bot
DDoS bot
Fake software

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

springweirtransferrerisque.communicationtrainingforathletes.com INVESTIGATE

Visualize

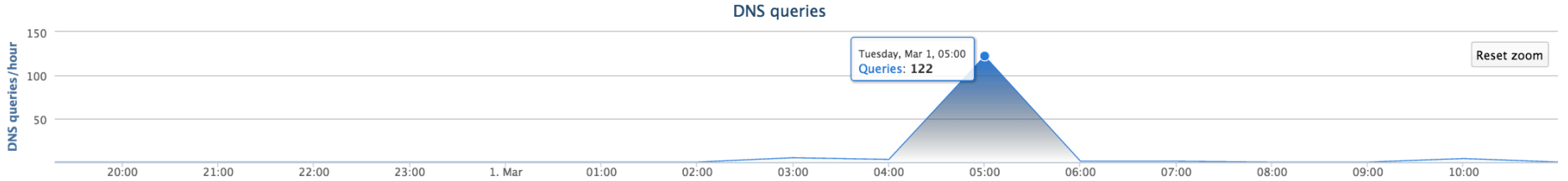
DETAILS FOR SPRINGWEIRTRANSFERRERISQUE.COMMUNICATIONTRAININGFORATHLETES.COM

Search in Google

Search in VirusTotal

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

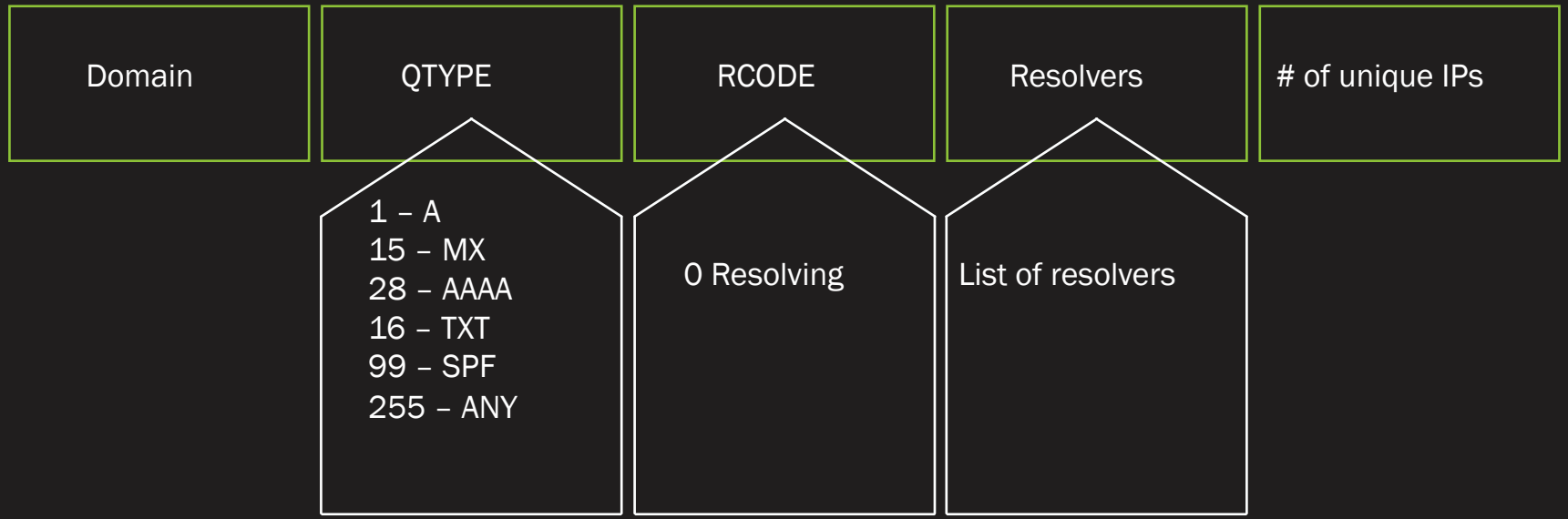
This domain is currently in the OpenDNS Security Labs block list



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

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

SPRank DNS Features

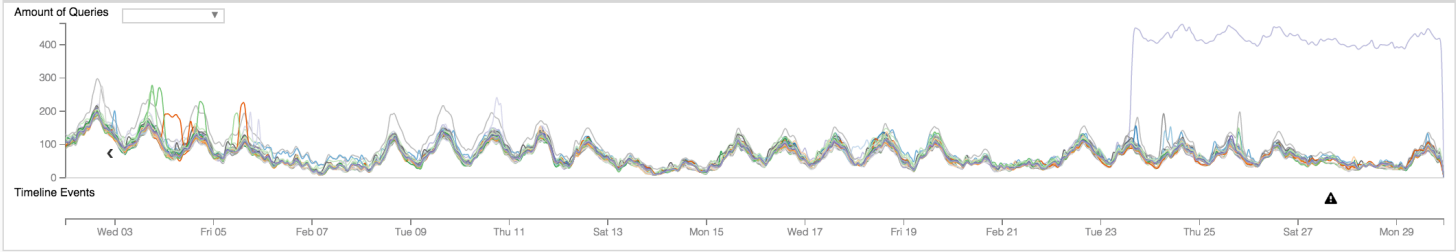


SPRank DNS Features

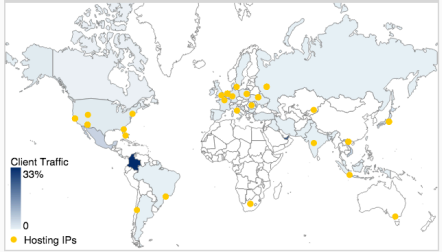
springweirtransferrerisque.communicationtrainingforathletes.com. 3.0 121 40.33 94 14 {((nyc),5),((ash),6),((yvr),4),((ams),2),((cdg),2),((yyz),13),((fra),33),((dfw),24),((lax),6),((pao),11),((mia),7),((syd),1),((sea),5),((lon),2)} {((1),114),((28),7)}

Traffic View | PC View

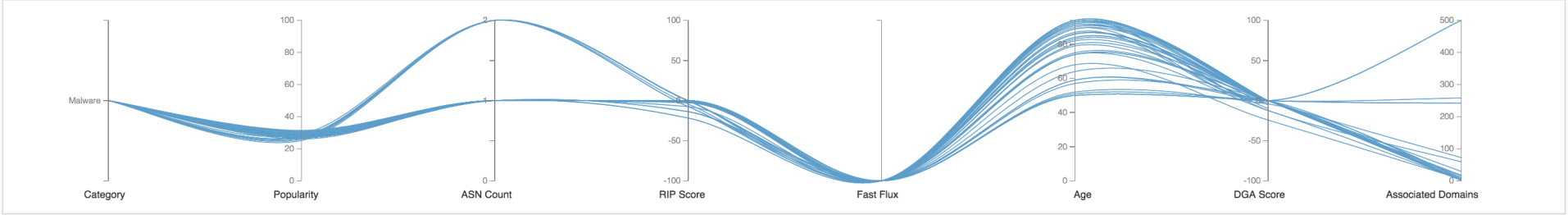
Traffic View



World View



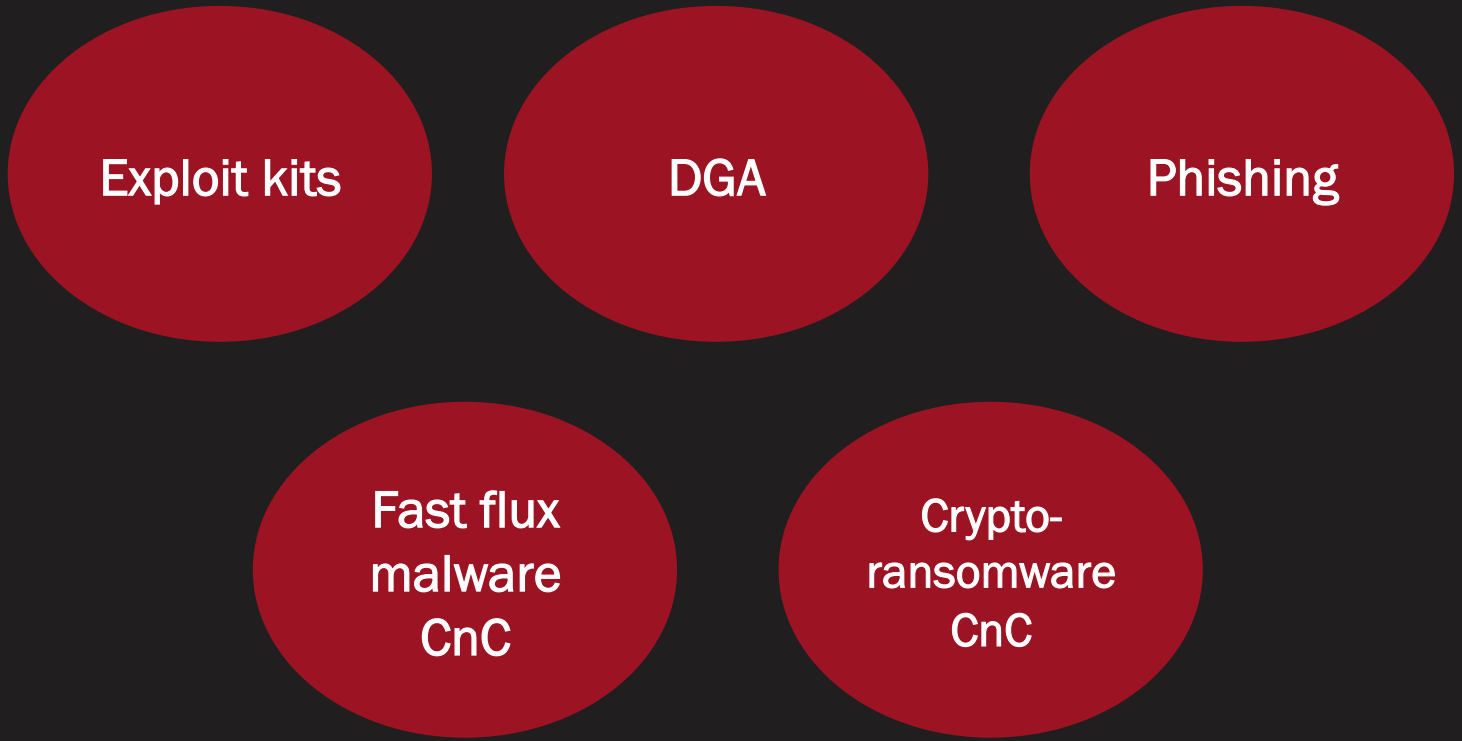
Parallel Coordinates



Keep Only | Remove | Export CSV | Send To

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	5
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
aptrader.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
cherniavskaia.com	Malware	27.65	1	-0.54	false	94.00	0.00	1

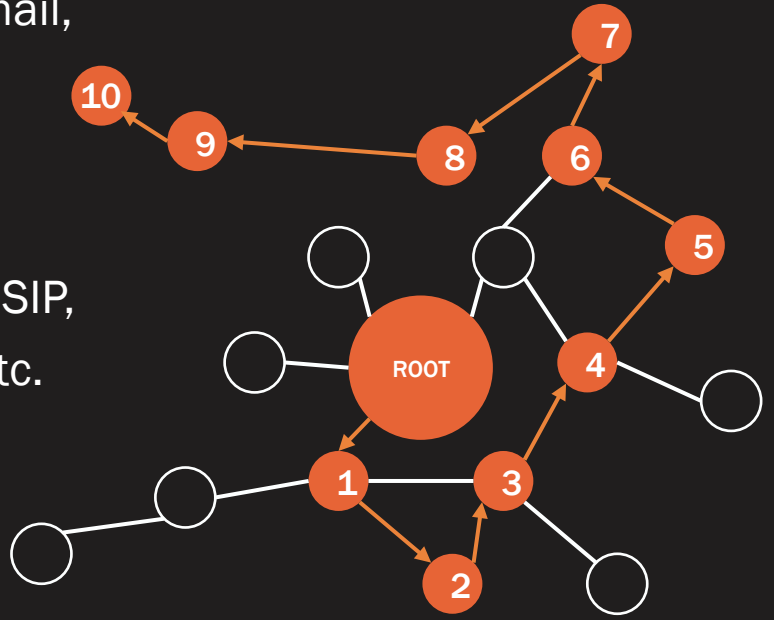
SPRank Detections



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

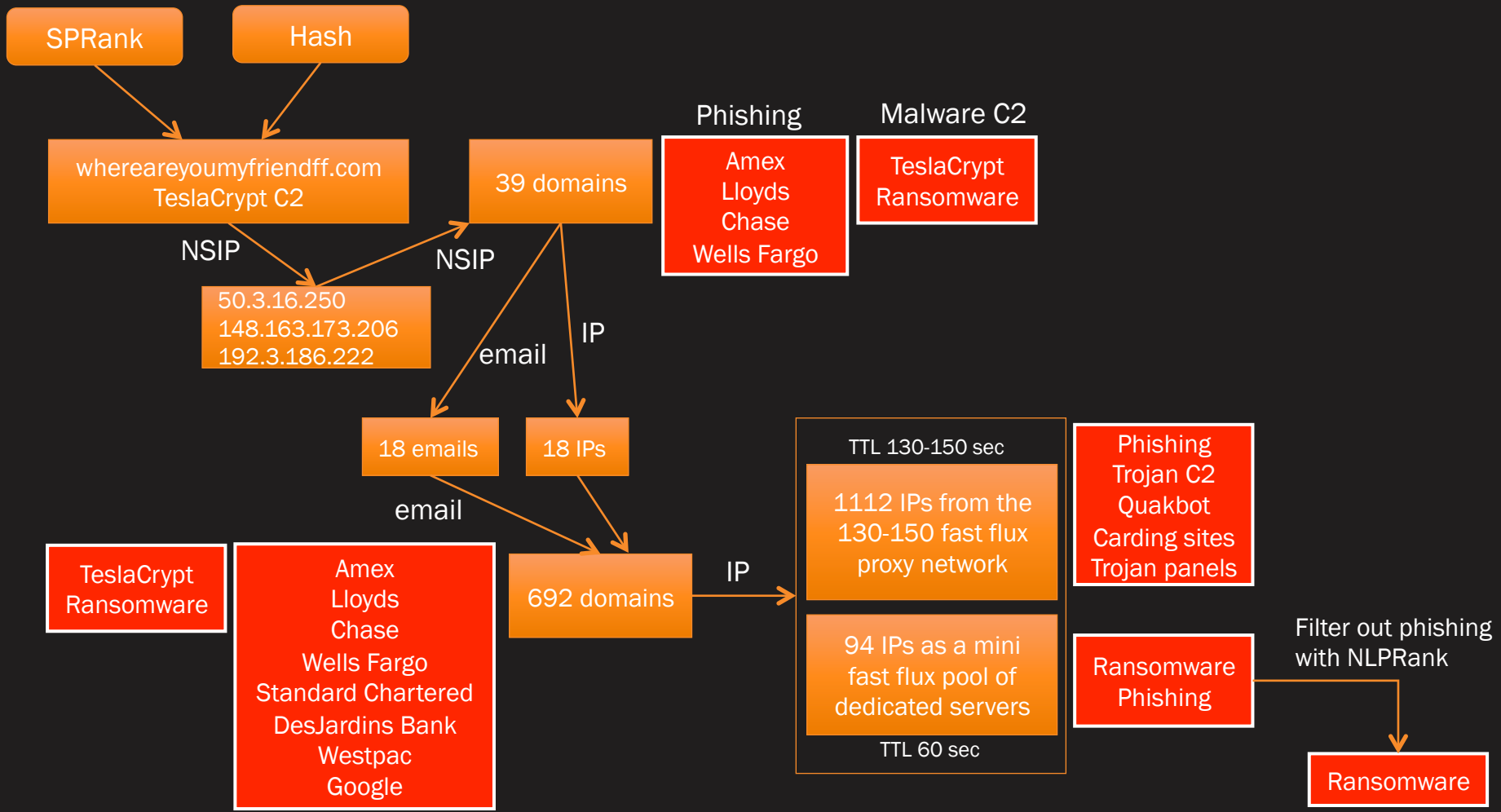
IOCs Related to Domain Registration and Hosting

- 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


SPRank
Hash
wheareyoumyfriendff.com
TeslaCrypt C2
NSIP
NSIP
50.3.16.250
148.163.173.206
192.3.186.222
39 domains
email
IP
Phishing
Amex
Lloyds
Chase
Wells Fargo
Malware C2
TeslaCrypt
Ransomware
18 emails
18 IPs
email
TeslaCrypt
Ransomware
Amex
Lloyds
Chase
Wells Fargo
Standard Chartered
DesJardins Bank
Westpac
Google
692 domains
IP
TTL 130-150 sec
1112 IPs from the
130-150 fast flux
proxy network
94 IPs as a mini
fast flux pool of
dedicated servers
TTL 60 sec
Phishing
Trojan C2
Quakbot
Carding sites
Trojan panels
Ransomware
Phishing
Filter out phishing
with NLPRank
Ransomware

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

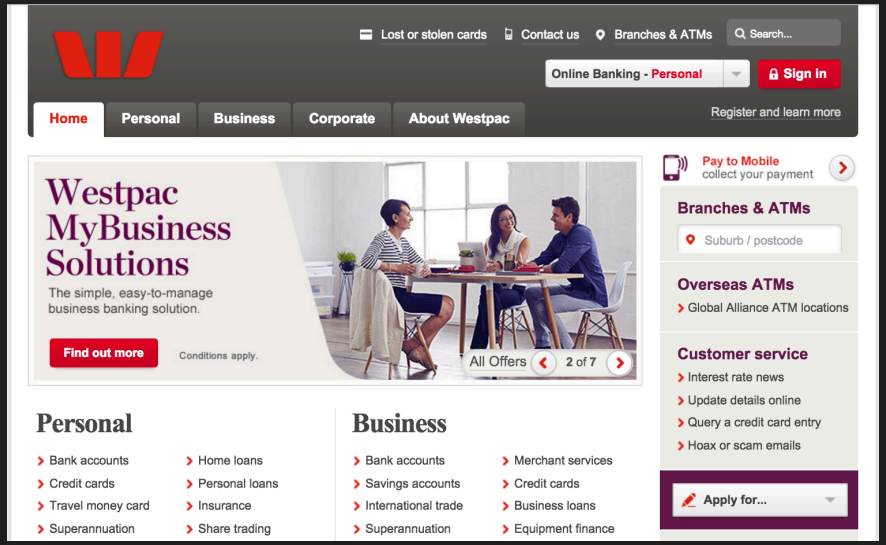
TeslaCrypt example – “130-150” Fast Flux Network

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 5th 2016
- Spike on Jan 6th, 11pm, domain live for 6 days



Phishing (1)

onlimecorpwestpac.com

cs@now.cn

120+ phishing domains

Westpac
Amex
Lloyds
Chase
Wells Fargo
ANZ (Australia & New Zealand Banking Group)
St.George Bank
Standard Chartered Bank

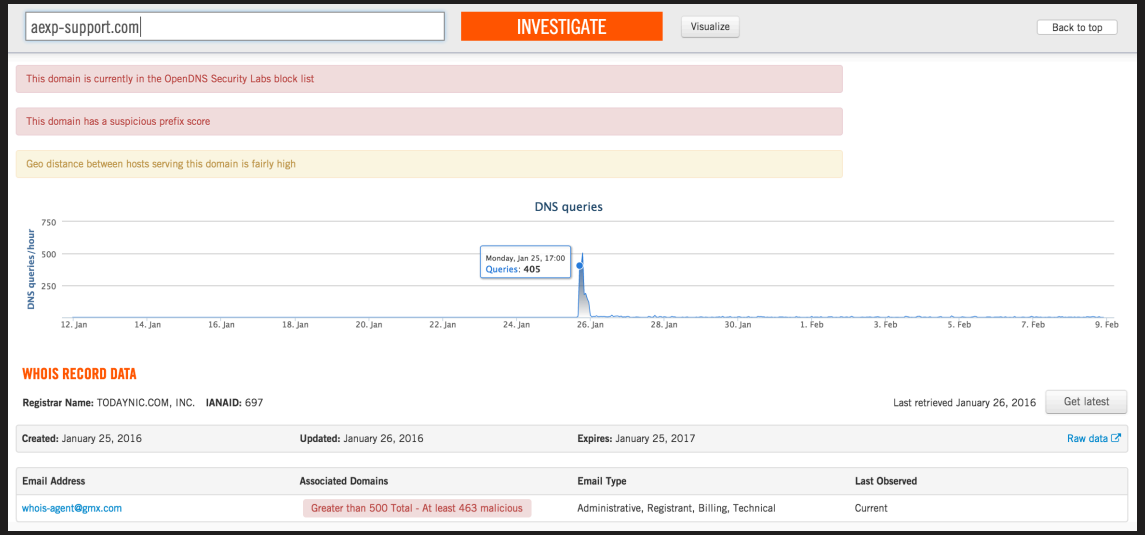
104.245.233.163
178.33.213.12
185.86.77.41
198.175.126.117
199.180.116.115
216.170.126.106
23.95.248.152

49 domains mostly phishing

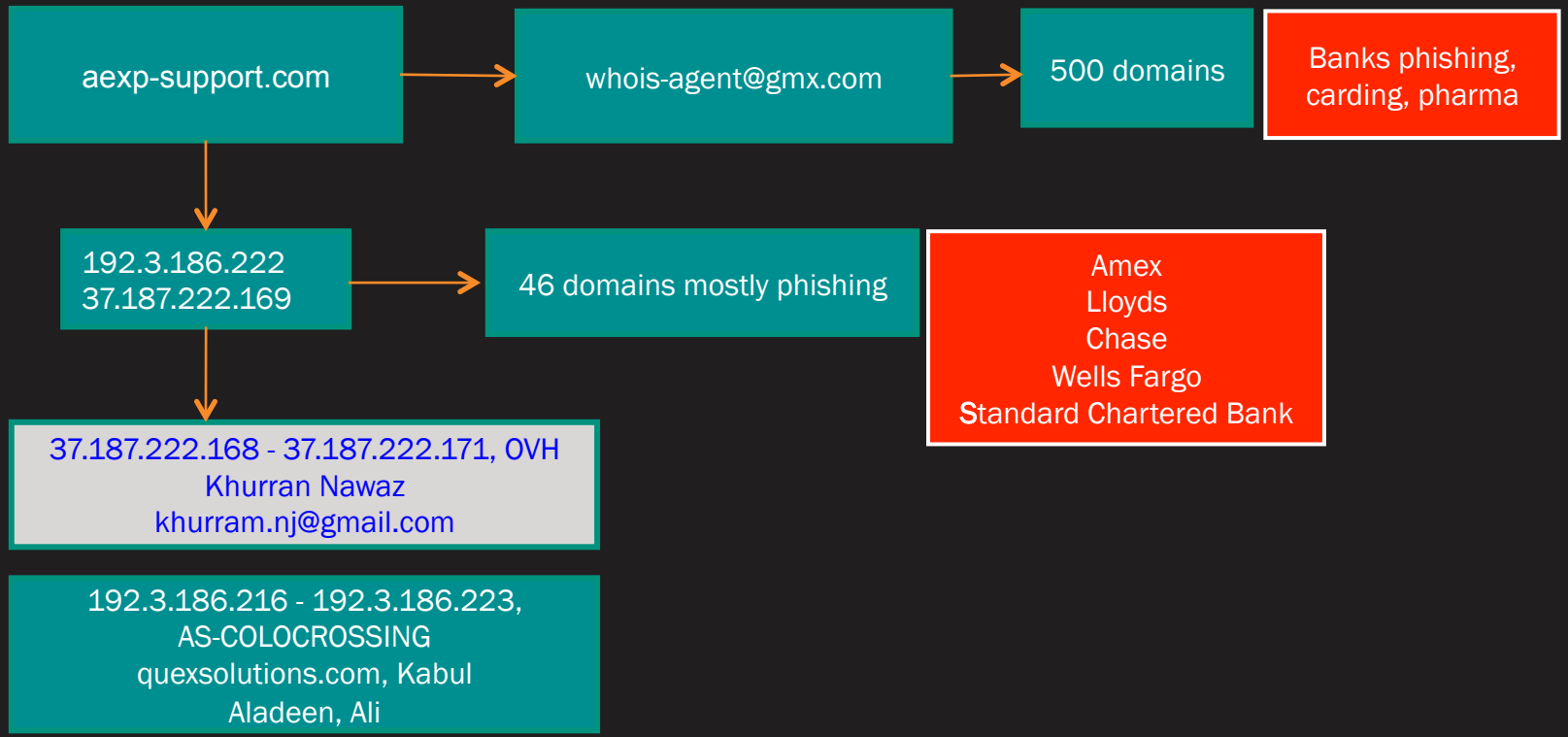
178.33.213.12 - 178.33.213.15, OVH
Khurran Nawaz
khurram.nj@gmail.com

Phishing (2)

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



Phishing (2)


aexp-support.com
whois-agent@gmx.com
500 domains
Banks phishing, carding, pharma
192.3.186.222
37.187.222.169
46 domains mostly phishing
Amex
Lloyds
Chase
Wells Fargo
Standard Chartered Bank
37.187.222.168 - 37.187.222.171, OVH
Khurran Nawaz
khurram.nj@gmail.com
192.3.186.216 - 192.3.186.223,
AS-COLOCROSSING
quexsolutions.com, Kabul
Aladeen, Ali

Phishing (2)

- Same actor Khurran Nawaz, 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.qhoster.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

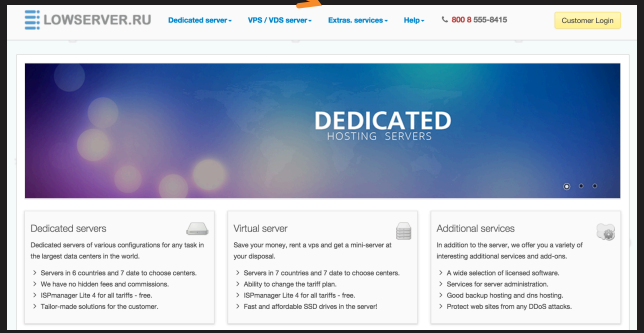
46.102.152.115
46.102.152.123
46.102.152.143
46.102.152.150


QHoster
Quality Hosting Matters
Need Help? Contact Us
Select Language
HOME
CREATE ACCOUNT
CUSTOMER LOGIN
NEED ADVICE? CHAT LIVE!
SKYPE
877-423-1155
800-610-5080
CPANEL WEB HOSTING
CPANEL RESELLER HOSTING
VIRTUAL SERVERS (VPS)
DEDICATED SERVERS
DOMAINS
SSL CERTIFICATES
4
PROMOTIONS
DEDICATED SERVERS
Intel Xeon CPUs & 1Gbits Port
save 20%
Rapid Deployment - No Need to Wait!
Reliable Hardware & Network
CentOS, Debian, Ubuntu & Windows Server
Location Choice - Europe & USA
regularly $212.44
$169.95/mo.
ORDER DEDICATED SERVER
PayPal
NETELLER
Skrill
Payza
WebMoney
Perfect Money
bitcoin
Ukash
cashU
litecoin
SolidTrustPay
paysafecard
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)
CPANEL RESELLER
$24.95/mo.
UNLIMITED cPanels
Top 6 Reasons
Why to Choose QHoster?
2004
Web Hosting Provider Since 2004

Malware Hosting Patterns

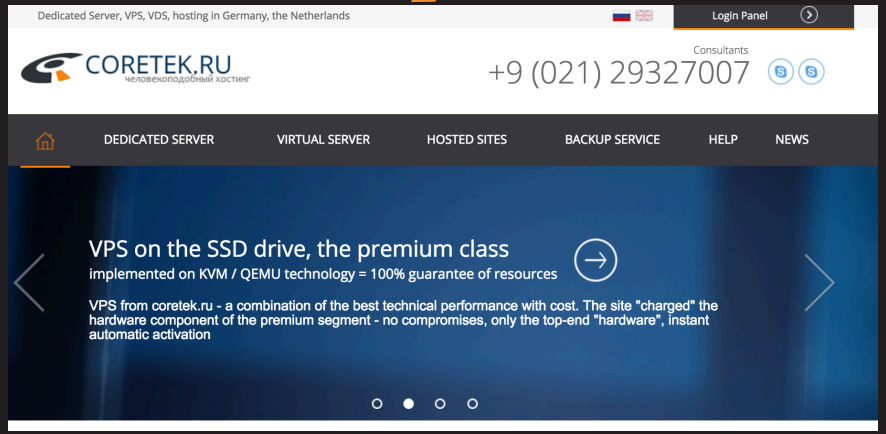

Domain Shadowing
Hoster Hopping
Abused Large Providers
Concentrated Hosting on Russian Speaking Providers
Register Offshore and Diversify IP space
Multi-purpose Fast Flux Proxy Network

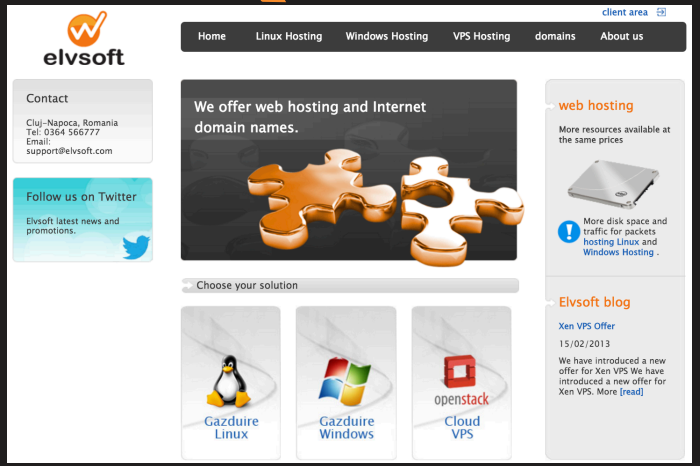
RU Speaking Hosters under Large Providers



RU Speaking Hosters under Large Providers

Leaseweb

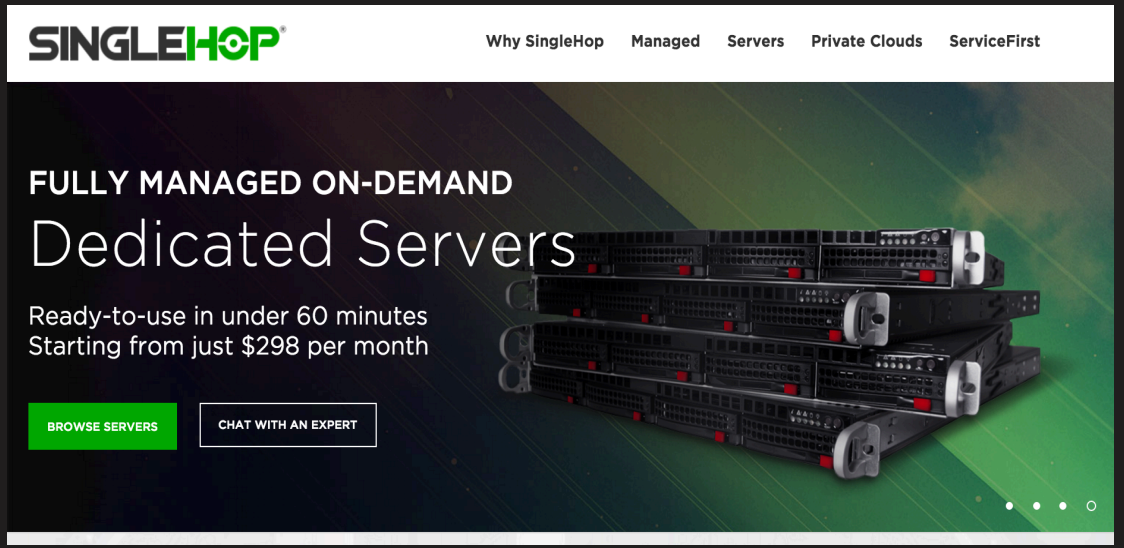




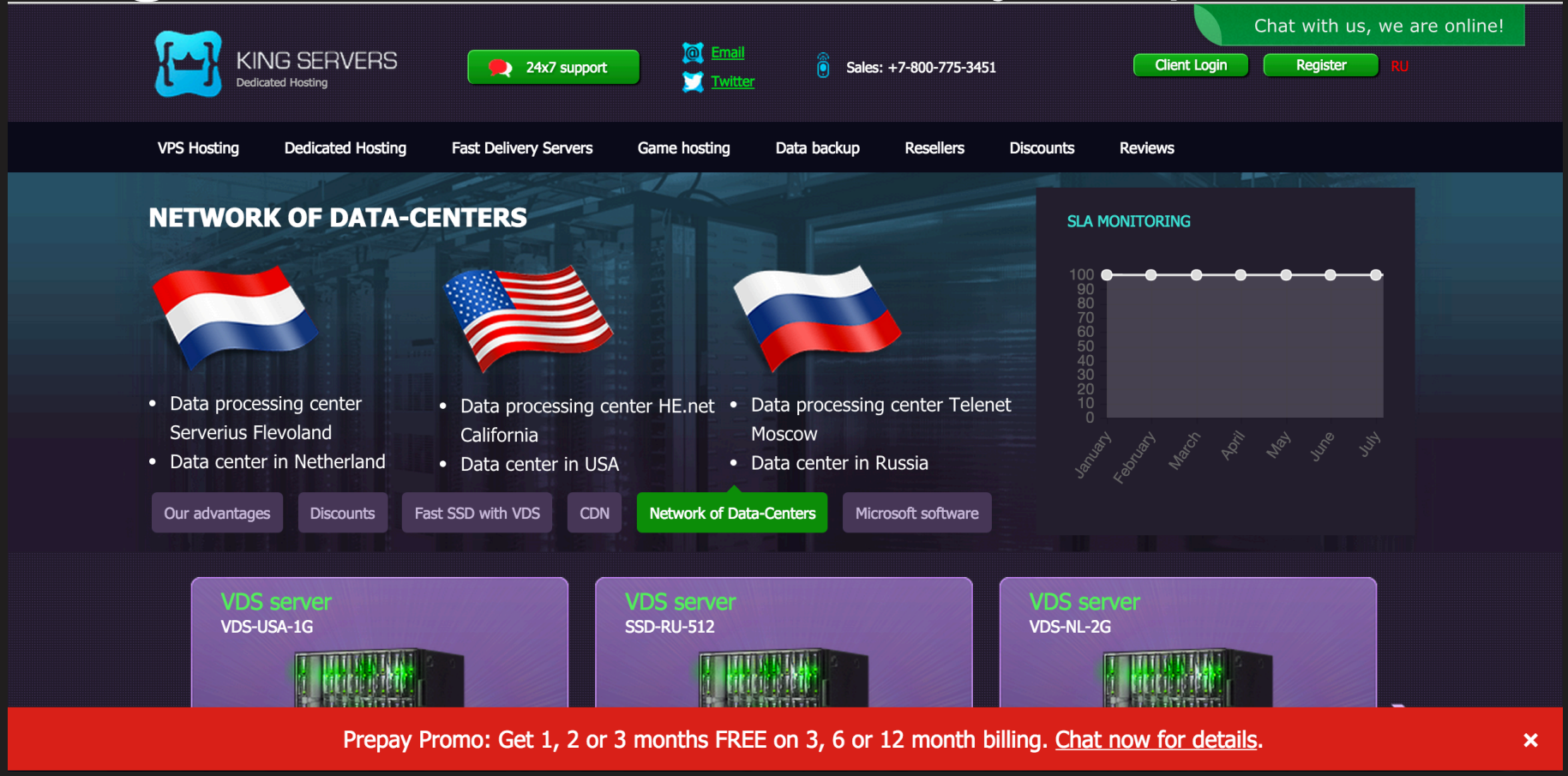
Hoster Hopping

- 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



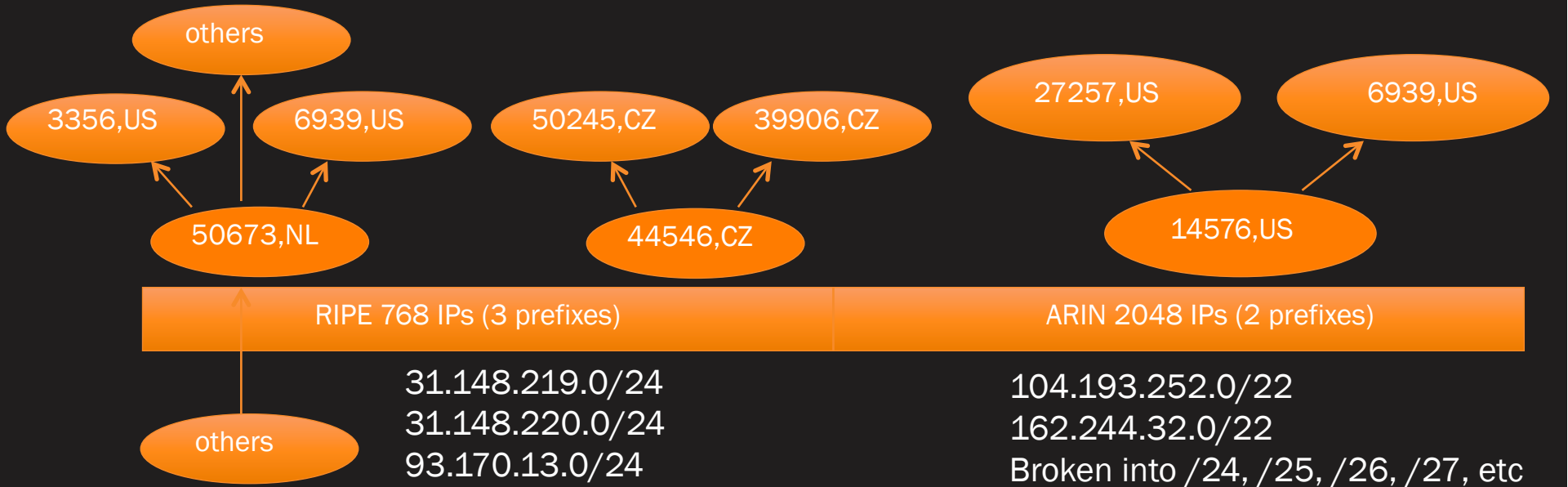
Register Offshore and Diversify IP Space



King Servers

- 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

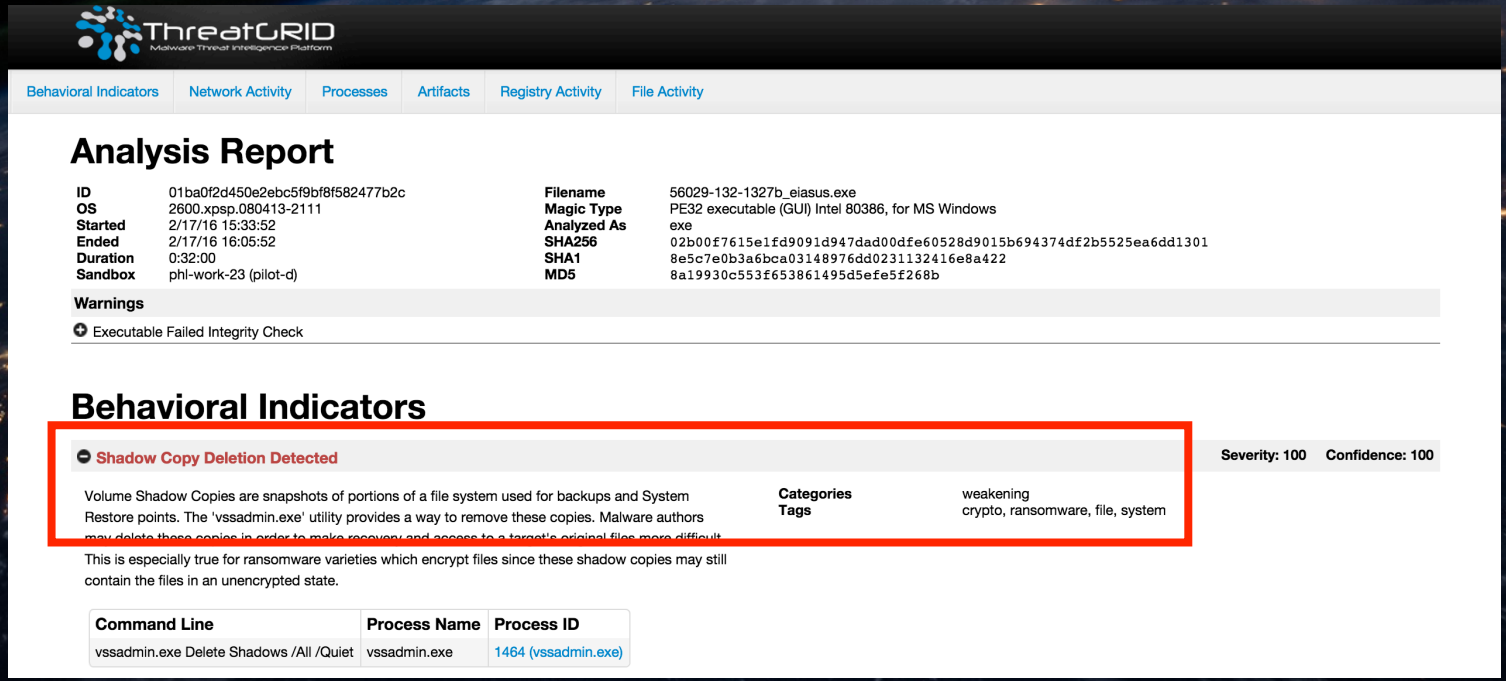


31.148.219.0/24
31.148.220.0/24
93.170.13.0/24

104.193.252.0/22
162.244.32.0/22
Broken into /24, /25, /26, /27, etc

Creating Inferences from Malware Behavior

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



Creating Inferences from Malware Behavior

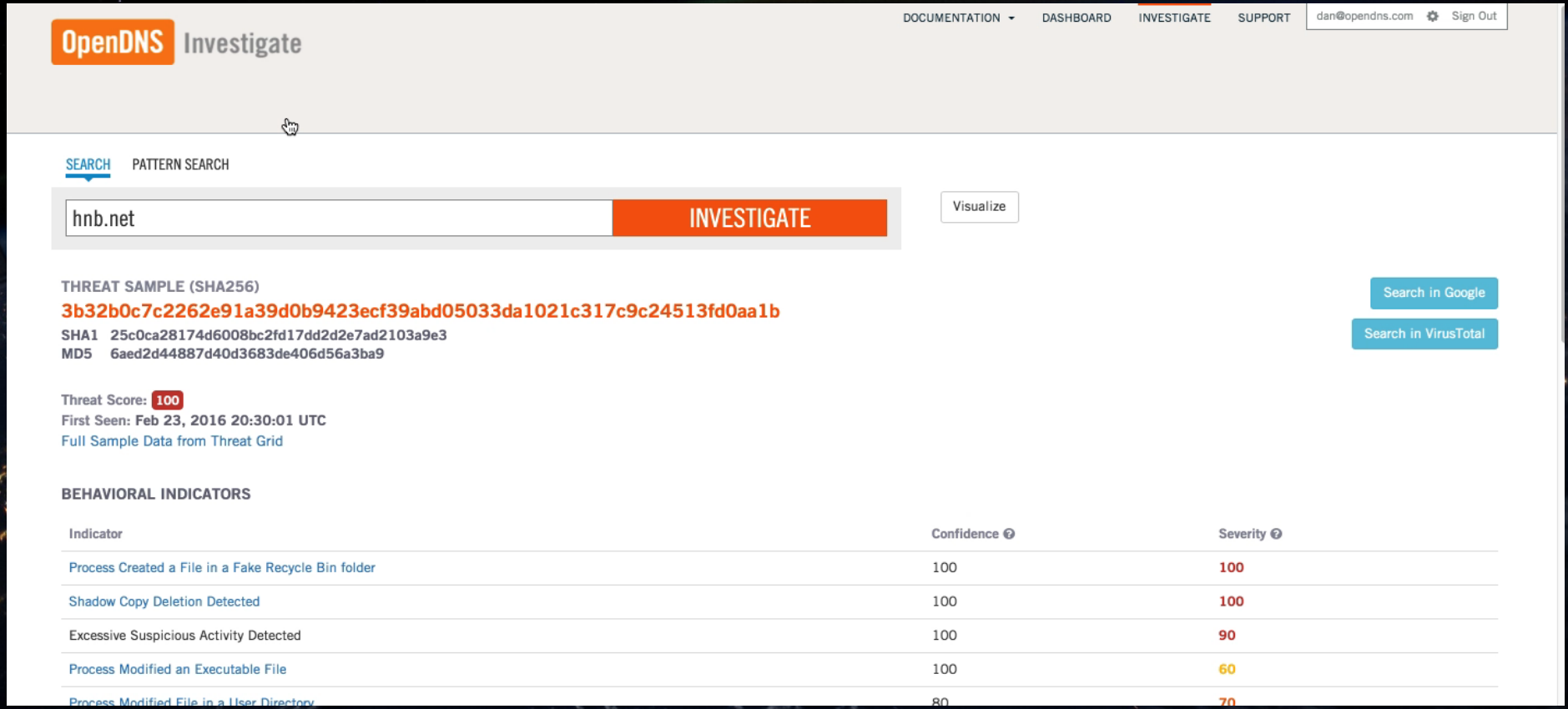
How can I expand a single behavior indicator to identify others and infer attribution

Creating Inferences from Malware Behavior

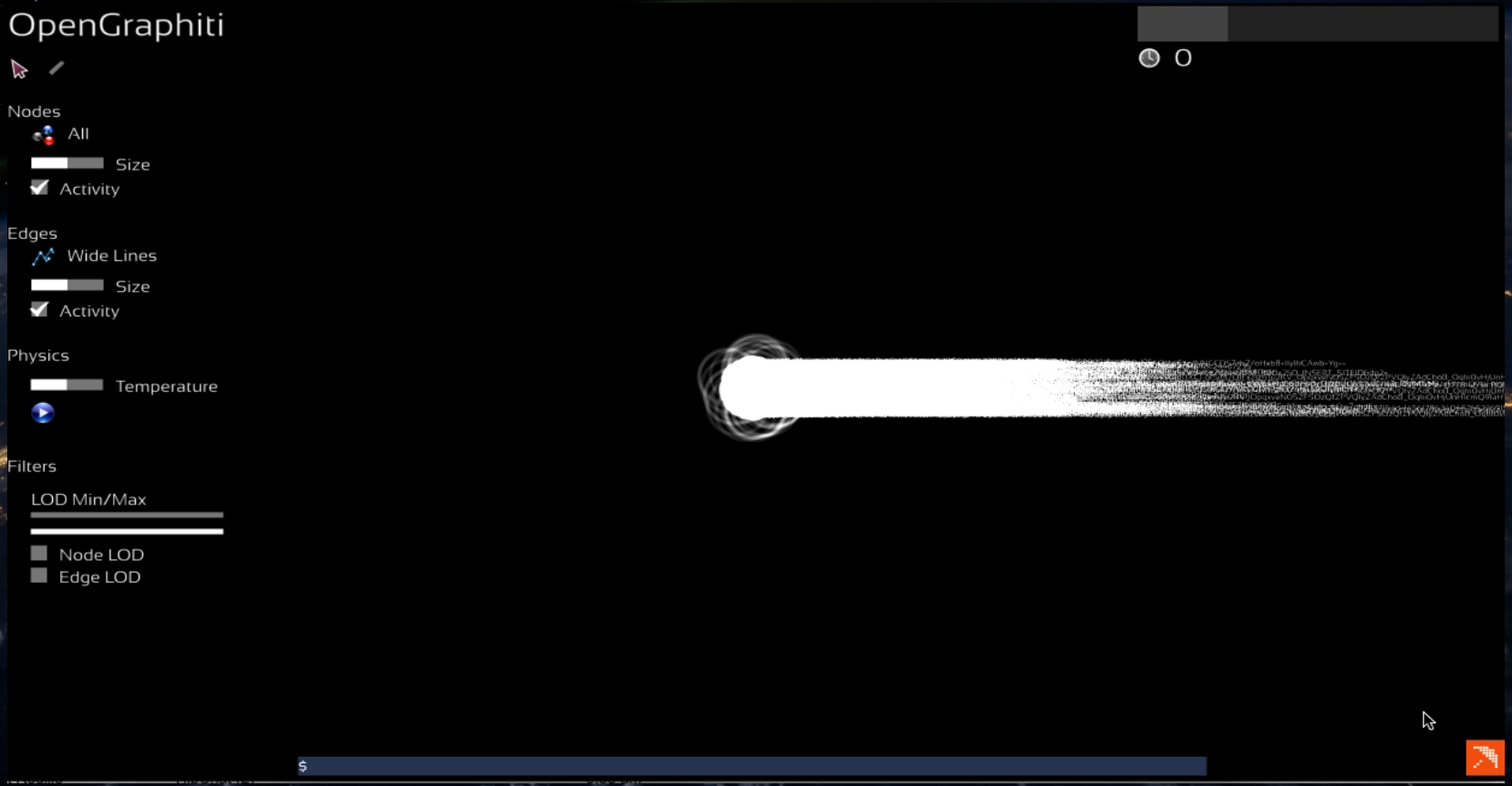
Creating Inferences from Malware Behavior

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

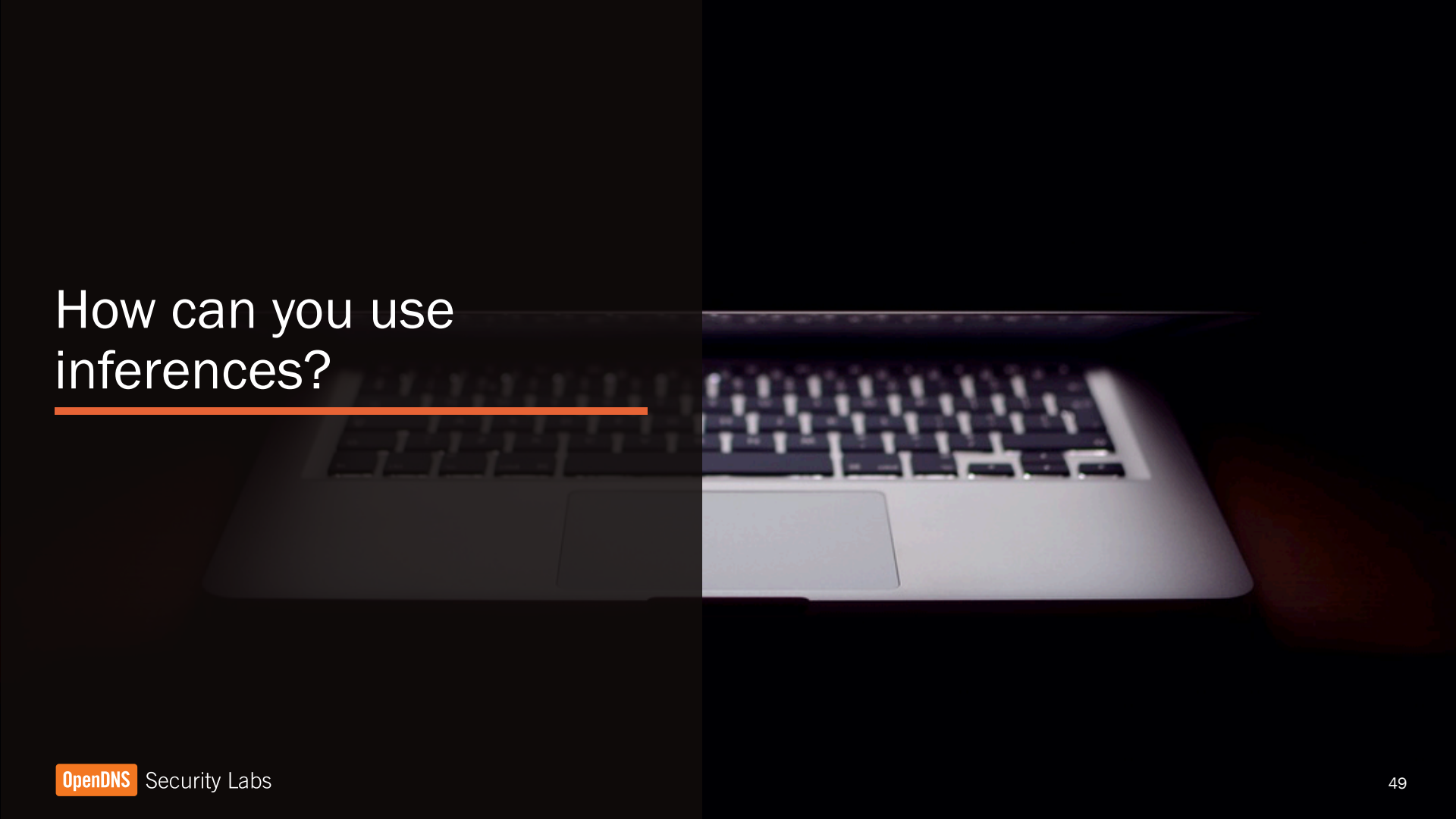
Creating Inferences from Malware Behavior



Creating Inferences from Malware Behavior



How can you use inferences?



OpenDNS is
now part of Cisco.

Dan Hubbard

@dhubbard858

Dhia Mahjoub

@dhialite