

OpenDNS

FloCon 2016
January 11-14, 2016
Daytona Beach, FL

New DNS Traffic Analysis Techniques to Identify Global Internet Threats

Dhia Mahjoub and Thomas Mathew
January 12th, 2016

OpenDNS is
now part of Cisco.



Dhia Mahjoub



**Technical Leader at OpenDNS
PhD Graph Theory Applied on Sensor Networks
Focus: Security, Graphs & Data Analysis**

Thomas Mathew



**Security Researcher at OpenDNS
Background: Machine Learning
Focus: Time Series and Data Analysis**

Agenda



OpenDNS Global Network & Types of DNS Traffic

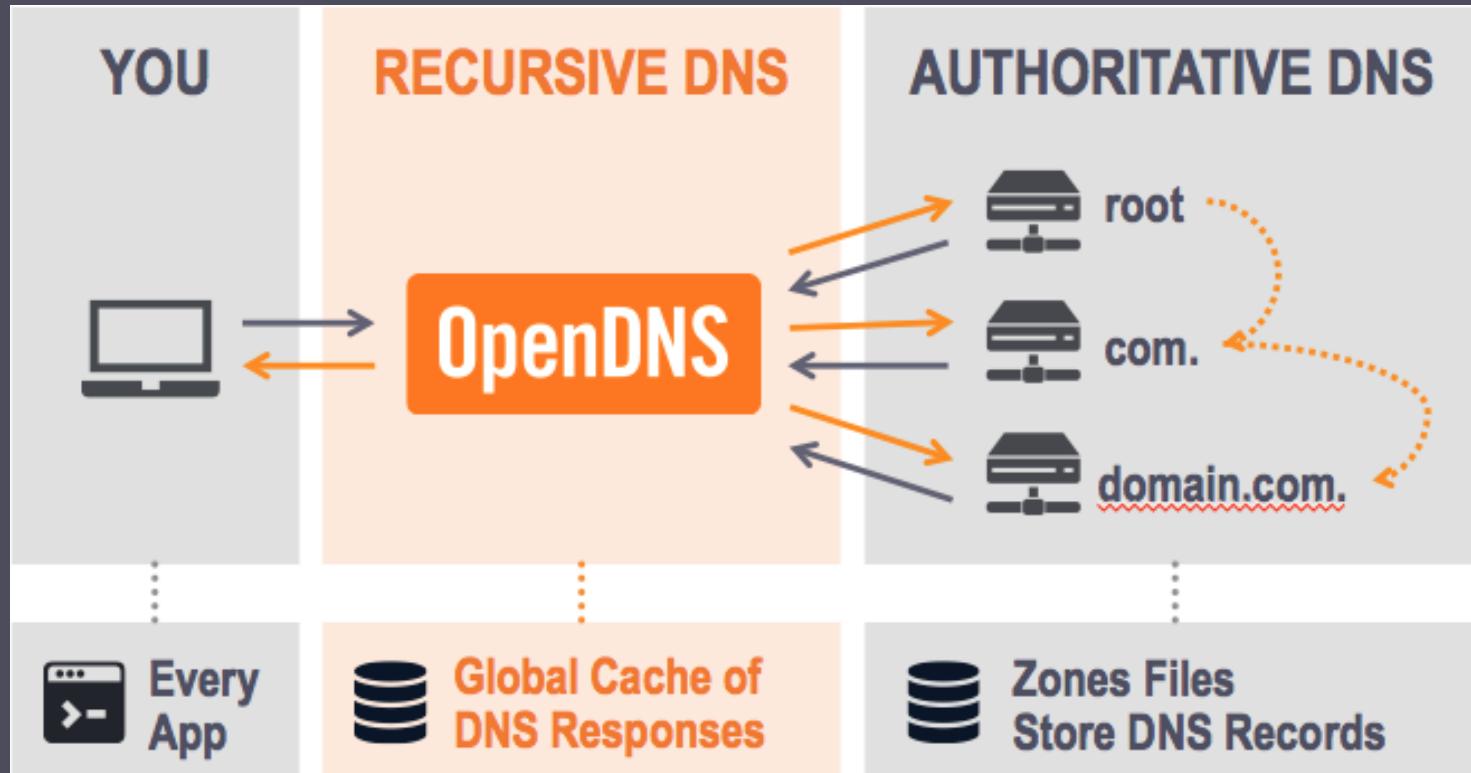
- Threat Landscape
- DNS Traffic Analysis Techniques
- Results and Recorded Suspicious Hosting Patterns
- Graph Analytics
- Conclusion

OpenDNS' Network Map



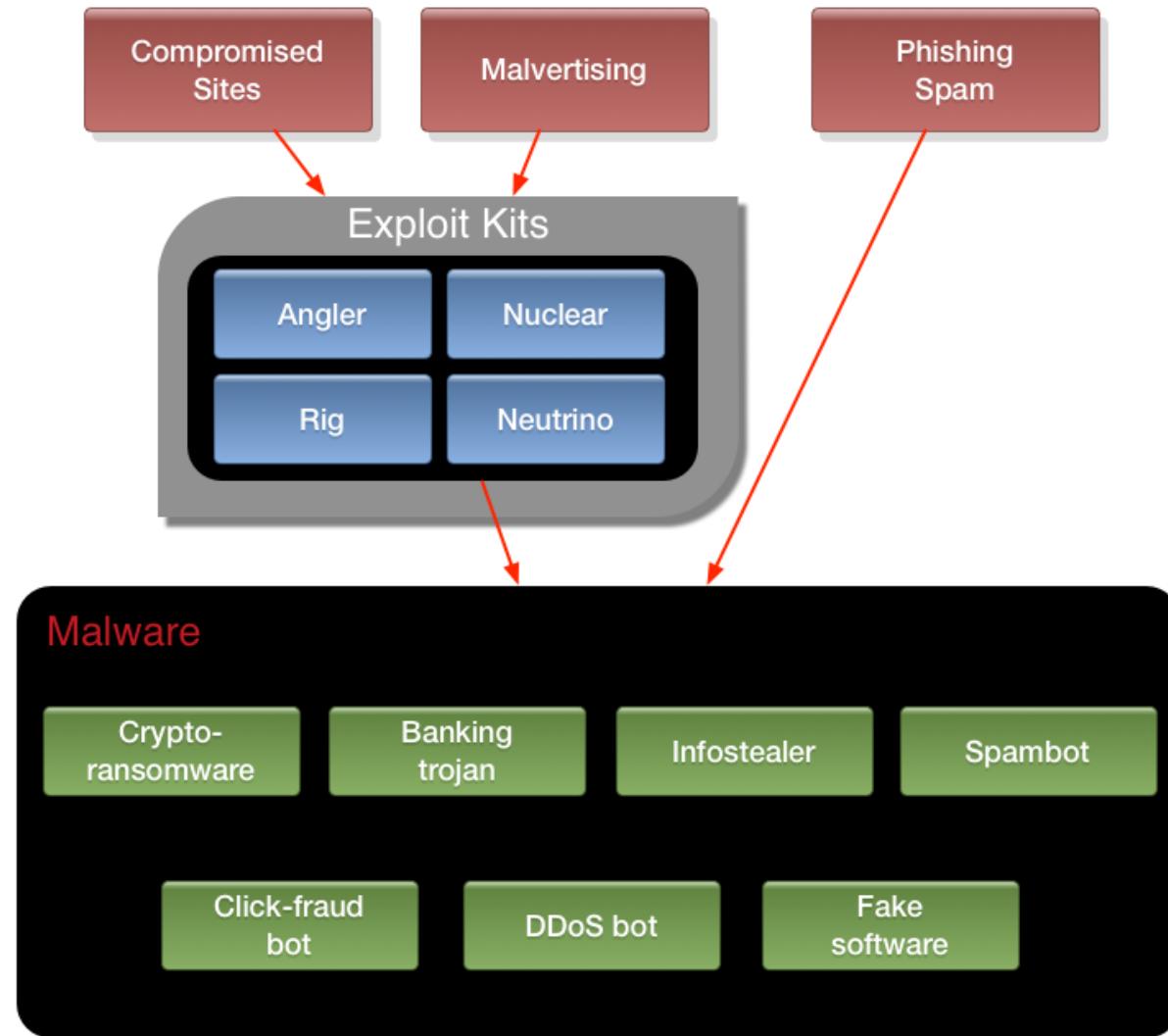
<https://www.opendns.com/data-center-locations/>

Where is OpenDNS in the network?

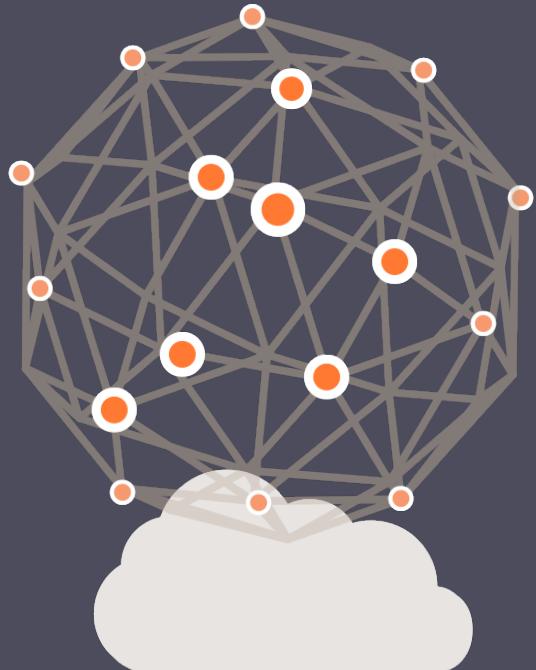


The background image shows an aerial view of a dense urban area during a golden hour sunset. The city is covered in a thick, hazy layer of orange and yellow light, with many skyscrapers and buildings visible through the mist. The overall atmosphere is mysterious and vast.

Threat Landscape



Some Security Graph Metrics



- 70+ Billion DNS queries per day
- Sample Authlogs:
 - ~46M nodes per day
 - ~174M edges per day

The background image shows an aerial view of a city skyline during a golden hour. The sky is filled with warm, orange and yellow clouds. Below, the city's buildings are visible through a layer of fog or low-hanging clouds, creating a hazy, atmospheric effect.

DNS Traffic Analysis Techniques

DNS Data – Authoritative Data

- Authoritative Data captures changes in DNS mappings:
- Can reconstruct all the domains mapping to an IP for a given time window and vice-versa
- Reconstruct data regarding name servers

DNS Data – Authoritative Data

- Authoritative Data helpful in catching ‘noisy’ domains
 - Fast flux, domains with bad IP, prefix reputation
- Noisy domains change mappings frequently e.g. Fast Flux

Domain Reputation

- We have noticed relying on domain reputation breaks on identifying certain groups of threat
 - Nxdomains, client behavior related domains
- Devised for an internet of 10 years ago
- Malicious domains move quickly from IP to IP
- Compromised domains
- Price of domain and subdomain have gotten cheaper

Signals

- Hypothesis: DNS query patterns are a signal that is harder to control
- **Refined Hypothesis:** DNS query patterns can be used to help identify Exploit kit domains

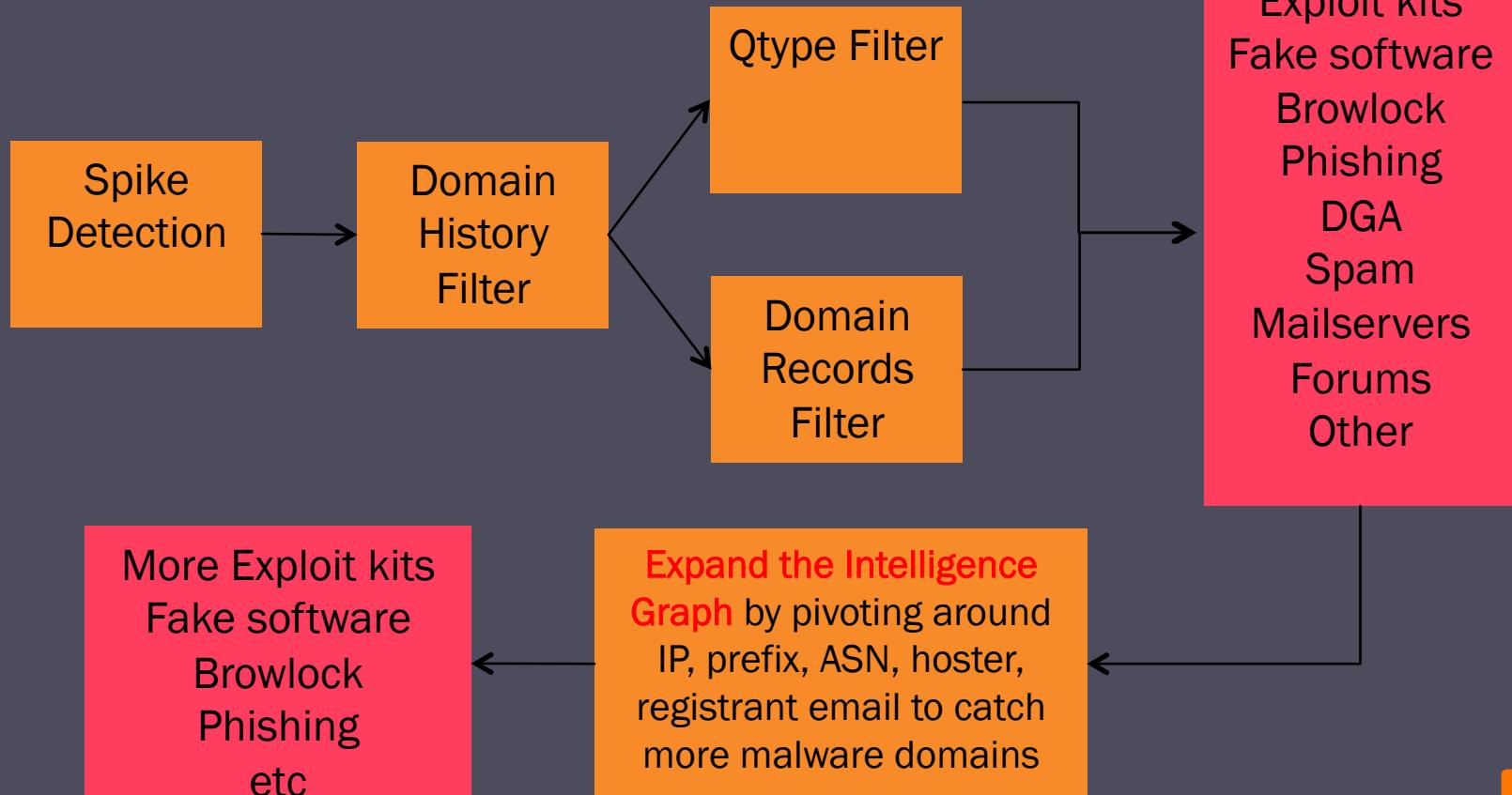
Signals (cont'd)

- Inherent vs. acquired/assigned features
- Lexical, DGA setup, hosting, registration can be changed
- Traffic patterns that emerge globally from clients querying malware domains are harder to obfuscate, change
- Defeat malware domains by tracking their features for which evasion at global scale is not easy

Traffic Patterns

- Create system to detect abrupt changes in query patterns
- Query pattern data is below the recursive layer
- Data includes: *Timestamp, Client IP, Domain queried, Resolver queried, Qtype, etc.*

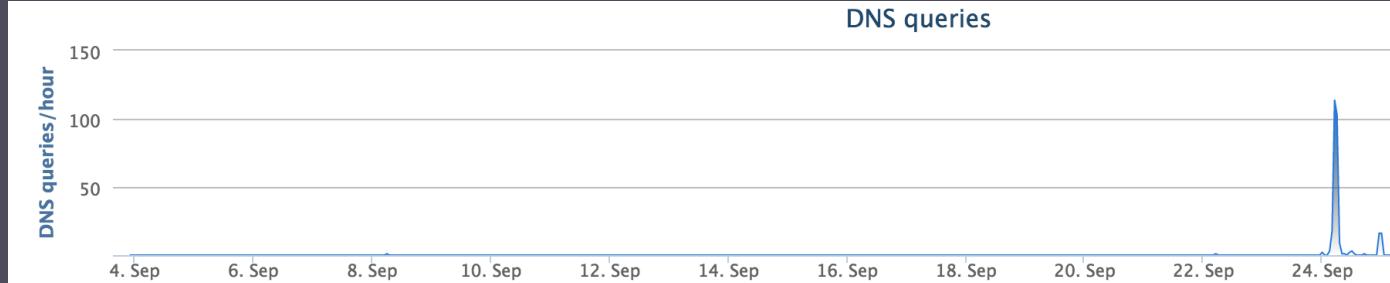
Detection System Components



Spike Detection

- Signal we look for is a **spike**
- Spike defined as a **jump in traffic over a two hour window**
 - Use predetermined threshold. Helps filter out google, facebook, etc
- Use a MapReduce job to calculate domains that spike
 - Output 50-100k domains each hour
- 50-100k domains is too much for manual inspection
- Domains that spike can have past history
- Mail servers, blogs, victimized domains, etc

Signals (cont'd)



Qtype Filter

- The amount of noise indicates we need more features
- Look at past history, DNS Qtypes, all existing DNS records of a domain, unique IPs, unique resolvers, etc.
- Partition based on Qtypes:
 - 1 – A Record
 - 15 – MX Record
 - 16 – TXT Record
 - 99 – SPF Record
 - 255 – ANY Record

Qtype Partition Results

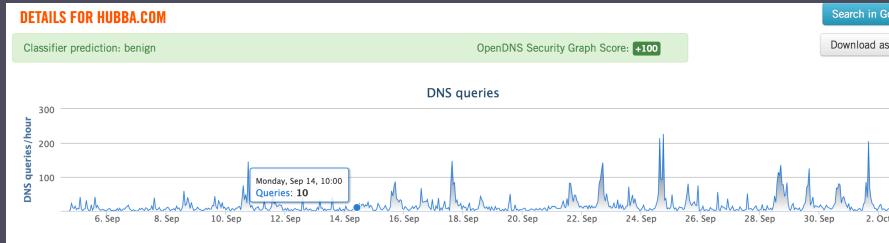
- Partition spikes based on their qtype distribution
 - i.e. A record only, A record and MX record, etc

$$\sum_{n=1}^5 nC5$$

- Interesting patterns begin to emerge
 - Only see 18 out of the 40 possible combinations
 - 75% or greater are A records only
 - Many combinations never appear ie only qtype 99
 - Behavior of domains can be associated with partition

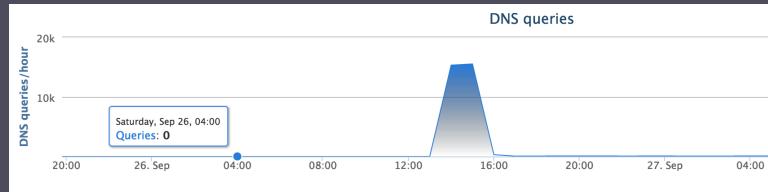
Qtype Partition Results

- Qtype of (1,15) associated with legitimate mail servers
 - Two types of distributions
 - 50/50 or 99/1 split between qtypes
 - ~4%
- Periodicity emergent in benign domains



Qtype Partition Results

- Qtype of (1,15,16,99,255) associated with legitimate mail and spam
 - Spam usually correlated with extremely high jumps
 - ~ 2.0% of all domains
 - demdeetz.xyz



Domain History Filter

- Past query history can be used to help remove benign domains and zero in on EMD ones
- Eliminate all domains with more than X consecutive non-zero hours of traffic
- Based on current EK domains' traffic patterns, only keep domains that feature Y consecutive most recent non-zero hours of traffic

Domain History Filter – benign with history

Enter domain name, ASN, IP address, or email address

100div.ru

INVESTIGATE

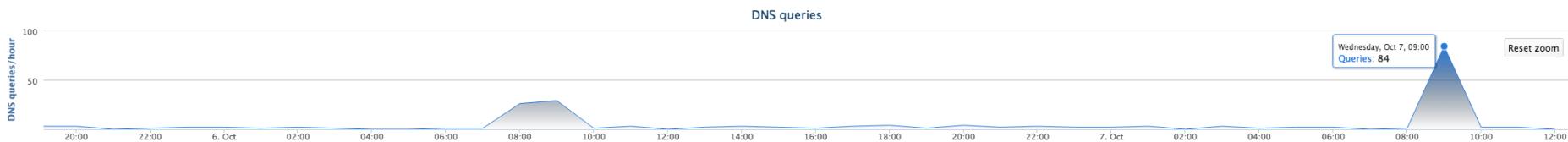
100div.ru 100sv.ru 1000001.ru 100doors.ru 100reg.ru 100big.ru 1001hr.ru 100pro.ru 101.ru
100prud.ru

DETAILS FOR 100DIV.RU

Search in Google

Download as CSV

This domain has appeared in the OpenDNS Security Labs block list



WHOIS RECORD DATA

Registrar Name: REGRU-RU IANAID: 729

Last retrieved October 7, 2015

Get latest

Created: March 11, 2014

Updated: -

Expires: March 11, 2016

Raw data ↗

Nameserver

ns2.beget.ru.

Associated Domains

350 Total - 3 malicious

Last Observed

Current

ns1.beget.ru.

350 Total - 3 malicious

Current

Domain History Filter – Nuclear EK

Enter domain name, ASN, IP address, or email address

INVESTIGATE[mdjnebdhdsbhss.tk](#) [mdjnebdhdsbhss.ml](#) [mdjnebdhdsbhss.cf](#) [mdjnebdhdsbhss.ga](#)[Search in Google](#)[Download as CSV](#)

DETAILS FOR MDJNEBDHDSBHSS.TK

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

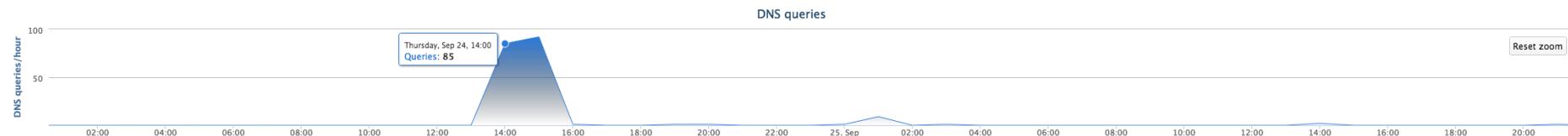
This domain is currently in the OpenDNS Security Labs block list

This domain is associated with the following type of threat: Exploit Kit

Classifier prediction: suspicious

OpenDNS Security Graph Score: **-98**

This domain may have been created using a domain generation algorithm (DGA)



WHOIS RECORD DATA

Registrar Name: - IANAID: -

Last retrieved October 7, 2015

[Get latest](#)

Nameserver	Associated Domains	Last Observed
ns01.freenom.com	Greater than 500 Total - At least 40 malicious	Current
ns02.freenom.com	Greater than 500 Total - At least 40 malicious	Current
ns04.freenom.com	Greater than 500 Total - At least 39 malicious	Current
ns03.freenom.com	Greater than 500 Total - At least 40 malicious	Current

Domain Records Filter

- Check for all DNS records available for a domain
- The existence/non-existence of certain records helps narrow down the purpose of a domain.
- Partition based on DNS records:
 - A
 - MX
 - TXT
 - CNAME
 - NS, specific name servers, indicative of compromise or malware

Random Forest

- Use random forest for classification
 - Example of ensemble learning using boosting. Boosting refers to process reducing bias from a set of weak estimators
 - Scalable via parallelization
- Use random forest on simple 2 class problem:
 - Exploit Kit/Non-Exploit Kit
 - In reality problem is multiclass: Spam, Exploit Kit, etc
 - For simplicity focus on binary problem

Random Forest (cont'd)

- Input:
 - Spike data
 - Time series data
- Output:
 - Classified domains
- Use Sklearn random forest library
- Challenges related to selecting features and tuning random forest parameters

Random Forest (cont'd)

- Features contain a mixture of continuous, discrete, and categorical variables.
 - Challenge for most estimators. Random forest handles this problem better than most estimators
- Continuous: Ratio of query counts to unique IPs
- Discrete: Query counts
- Categorical: QType Distribution
- Features include:
 - Number of unique IPs
 - Distribution of QTypes
 - Distribution of RCodes

Random Forest (cont'd)

- Have to tune various hyperparameters:
 - Number of features to decide split
 - Number of trees to create
 - Gini vs Entropy
- Gini measure used for deciding when to create splits
 - We chose Gini because it generalizes better to continuous data. Majority of our data is continuous
- Building deeper trees = longer training time
- We decided to use $\text{sqrt}(\text{number of features})$ to determine the max number of features used to generate split

Random Forest (cont'd)

- Created a training set of 1k exploit kits and 2k non-exploit kits.
- Ran through with a 10 fold cross validation
- Successful in minimizing false positives:
 - One challenge was handling Chinese gambling sites which have close to identical behavior to exploit kit domains.
 - Difference is only apparent after examining lexical structure of domain name
- AOC = .93
 - Significantly better than random

Results

Detected Threats

- Exploit kits: Angler Nuclear, Neutrino
- DGA
- Fake software, Chrome extensions
- Browlock
- Phishing

Detected Threats – Recorded Hosting Patterns

- Compromised domains – Domain shadowing
- Domain shadowing with multiple IP resolutions
- Register offshore and diversify IP space
- Large abused hosting providers (Hetzner, Leaseweb, Digital Ocean)
- Shady hosters within larger hosting providers (Vultr)

Compromised domains – Domain shadowing

- Compromised domains – Domain shadowing serving Angler, RIG, malvertising
- Spike domain can have GoDaddy name servers and still be a non EK, e.g. Chinese lottery, casino sites, spam
- Difference is: EK domains have traffic from multiple IPs spread across several resolvers
- Traffic to spam, casino sites comes from a single IP

Angler versus Spam

- **Exploit kit:** you.b4ubucketit.com. 0.0 45 45.0 40 11
{((ams),13),((cdg),1),((fra),3),((otp),1),((mia),6),((lon),6),((nyc),1),((sin),3),((pao),1),((wrw),3),((hkg),7)} {((1),45)}
- **Spam:** www.tzd.tcai006.net. 0.0 26 26.0 1 1 {((lon),26)} {((1),26)}
- 46.30.43.20, AS35415, Webzilla, <https://eurobyte.ru/>

Enter domain name, ASN, IP address, or email address

you.b4ubucketit.com

INVESTIGATE

b4ubucketit.com yourbuckets.com b4upetit.com b4ubuyit.com b4uburyit.com b4uburryit.com b4ubuildit.com
you-bag.com b4utxit.com b4uboxit.com

DETAILS FOR YOU.B4UBUCKETIT.COM

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

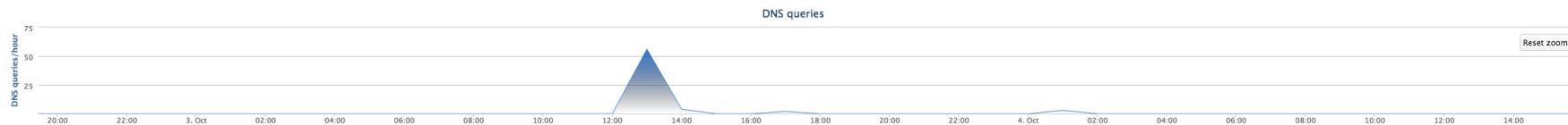
Search in Google

Download as CSV

This domain is currently in the OpenDNS Security Labs block list

Classifier prediction: suspicious

OpenDNS Security Graph Score: -99



WHOIS RECORD DATA

Registrar Name: GODADDY.COM, LLC IANALID: 146

Last retrieved July 17, 2015

Get latest

Created: July 5, 2010

Updated: July 6, 2015

Expires: July 5, 2017

Raw data ↗

Email Address

Associated Domains

Email Type

Last Observed

gap@pallottaco.com

88 Total - 84 malicious

Administrative, Registrant, Technical

Current

Show past data

Showing 1 of 2 Results

Namserver

Associated Domains

Last Observed

ns12.domaincontrol.com

Greater than 500 Total

Current

ns11.domaincontrol.com

Greater than 500 Total

Current



Services Rewards Help & support CHAT ONLINE REGISTER LOGIN

Shared Hosting CMS-Hosting VIP-hosting VDS / VPS

RATES VIRTUAL HOSTING

2 GB 4GB 6 GB 10 GB

159 ₽ PER MONTH 299 ₽ PER MONTH 399 ₽ PER MONTH 599 ₽ PER MONTH

TO ORDER TO ORDER TO ORDER TO ORDER

All rates include the SSD-drives, an unlimited number of sites and the MySQL database

Domain shadowing on multiple hosting IPs

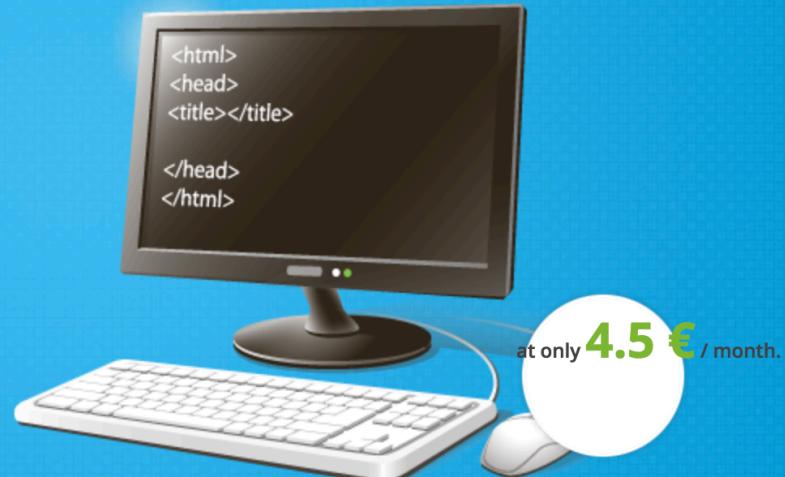
- odksooj.mit.academy. 3600 IN A 217.172.190.160
odksooj.mit.academy. 3600 IN A 85.25.102.30
- 217.172.190.160, AS8972, PLUSERVER-AS, <https://vps-server.ru/>
- 85.25.102.30, AS8972, PLUSERVER-AS, <https://vps-server.ru/>
- The range 217.172.190.158-160 is hosting similar EK domains
- 217.172.190.159 hosts vbnxkjd.governmentcontracting411.com which also resolves to 178.162.194.172
- 178.162.194.172, AS16265/AS28753, <http://www.hostlife.net/>
- The range 178.162.194.169-172 is also hosting similar EK domains

HOSTING

RELIABLE HOSTING FOR YOUR WEBSITE

**Hosting your sites on a fast SAS and SSD drive!
Discounts on hosting for 6 and 12 months!**

- Unlimited traffic for VIP tariff
- Instant account activation
- Databases fast SSD drive!
- Tested for Joomla, WP, Drupal
- You can select the version of PHP (5.3, 5.4, 5.5, 5.6 ...)

[READ MORE >](#)[BUY >](#)



380 (44) 392-01-34



RUS



USD



CUSTOMER LOGIN

[Register](#) | [Forgot your password?](#)

Ваш логин

Ваш пароль

* OK



HOSTING AND SERVERS

WEBSITE DEVELOPMENT

SSL

DOMAINS

ABOUT COMPANY

SUPPORTS

CONTACTS

DEDICATED SERVER

- 100% hardware resources
- PU and operating systems to choose from
- Manage the DNS
- Dedicated connection
- Administration
- Remote backup 50 GB



from 53.1 \$

Details



Write to us, we are online!

Another EK

- 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 similar pattern EK domains

Another EK

- 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 the /24 range have same fingerprint and are very likely set up to host EK domains in the next couple days, **and they did !**

46.102.152.115

46.102.152.123

46.102.152.143

46.102.152.150

Register Business Offshore and Diversify IP Space

- Qhoster, <https://www.ghoster.com/>
- Hosting provider's business registered in Belize
- Hosting EK domains, phishing in addition to ordinary content
- IP space in both ARIN and RIPE



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

regularly \$212.44
\$169.95/mo.

save
20%

ORDER DEDICATED SERVER



[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/TMAP Anti-spam/virus

CPanel RESELLER

\$24.95
/mo.



- UNLIMITED cPanels
- FREE Site Builder Software

Top 6 Reasons

Why to Choose QHoster?



2004 Web Hosting Provider Since 2004

OpenDNS

Register Business Offshore and Diversify IP Space

 KING SERVERS
Dedicated Hosting

 24x7 support

 Email
 Twitter

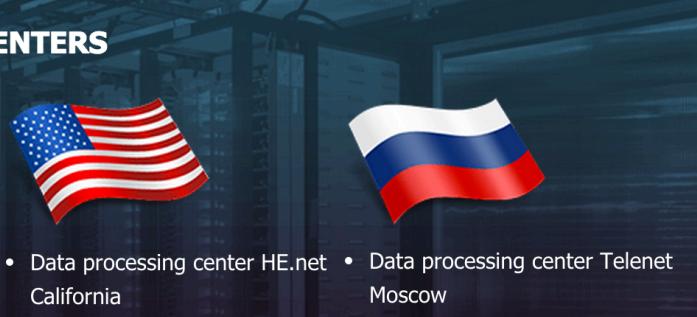
 Sales: +7-800-775-3451

 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 USA
- • Data processing center HE.net California
- Data processing center Telenet Moscow
- Data center in Russia

SLA MONITORING



Month	SLA Value
January	100
February	100
March	100
April	100
May	100
June	100
July	100

[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



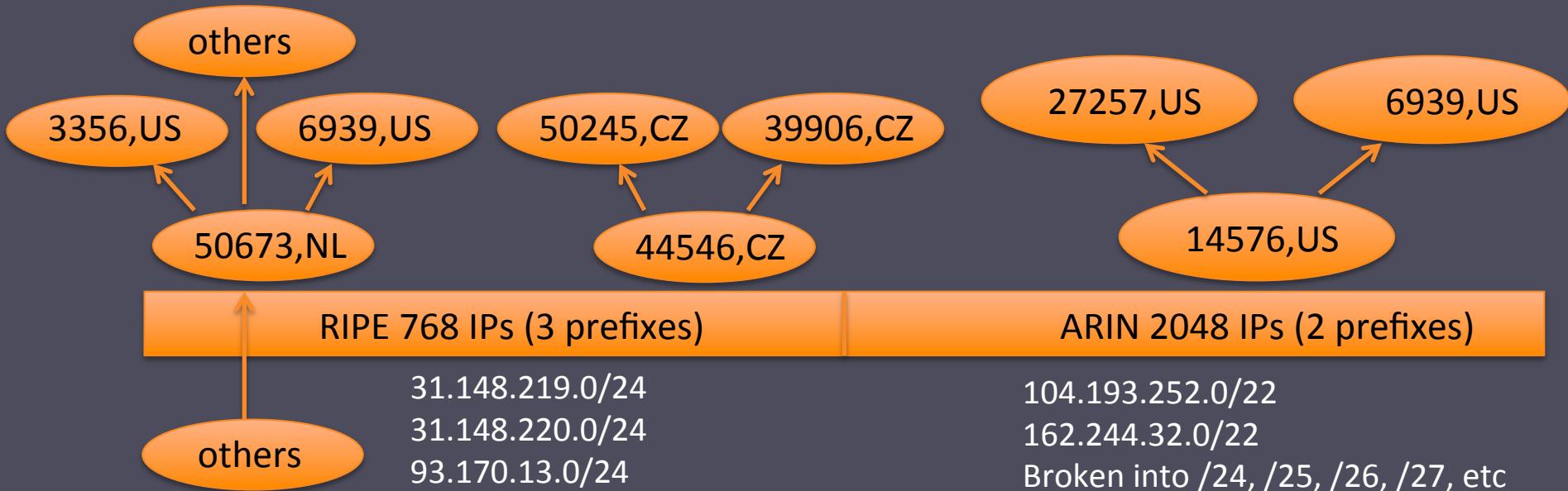
Prepay Promo: Get 1, 2 or 3 months FREE on 3, 6 or 12 month billing. [Chat now for details.](#)



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



Nuclear

- fegshsjdkasdhhasbaad.ga
- 188.226.215.37, AS200130, <https://www.digitalocean.com/>
- 400+ Nuclear domains on that IP between Sep 24 and Oct 8
- A domain's lifetime is less than 1 day

Nuclear – Abused Large Hosting Providers

- Previous pattern, name server domains registered with compromised email cavalliere.job@gmail.com and landing domains are registered as free domains under freenom
- Name servers hosted on [Digital Ocean](#) and [AS-Choopa/Vultr](#)
- Landing domains hosted on various ASNs, most notably AS-Choopa/Vultr
- New pattern: Nameservers are freenom's own name servers, and landing domains are hosted mainly on Vultr or Digital Ocean
- Digital ocean has 9 ASNs. The smaller ones are the most abused: AS202018, AS202109, AS200130

Previous pattern

Recent pattern

EK landing domains **registered for free** through freenom

Idem

EK landing domains hosted on various ASNs, most notably AS-Choopa/**Vultr**

EK landing domains hosted on various ASNs, mainly AS-Choopa/**Vultr**, **DigitalOcean**
Digital ocean has 9 ASNs. The smaller ones are the most abused: **AS202018**, **AS202109**, **AS200130**

Use **dedicated name servers** registered with **compromised email**
16 name servers registered with same email -> **Can pivot around email or name servers to blacklist EK domains**

Use of **freenom's name servers**: ns01-04.freenom.com
-> **Not possible to automatically pivot around name servers w/o weeding out FPs**

Name servers hosted on various ASNs, mainly AS-Choopa/**Vultr**, **DigitalOcean**
-> **Can block name server IPs**

freenom's name servers hosted on **Amazon** and **Google** ASNs
-> **Not reliable to block Amazon and Google IPs w/o FPs**

Vultr – Shady Hoster within larger hosting providers

- Vultr is a child company of AS-Choopa (AS20473) created to compete with Digital Ocean in the affordable VPS market
- IP space is 65,000 large in North America, Europe, Asia/Pacific
- Its cost-effectiveness made it an attractive platform for criminals to host Exploit kits, phishing and other gray content
- <https://labs.opendns.com/2015/09/14/phishing-spiking-and-bad-hosting/>

DGA - 1

nxsabpxvqdac86.com. 0.0 49 49.0 5 5 {((chi),12),((yvr),19),((lax),5),((ash),6),((dfw),7)} {((1),49)}

lofefstnlktbpk.com. 0.0 49 49.0 5 5 {((chi),12),((yvr),20),((lax),5),((ash),5),((dfw),7)} {((1),49)}

yeydhmuwhamfssagka.com. 0.0 48 48.0 5 5 {((chi),12),((yvr),19),((lax),5),((ash),6),((dfw),6)} {((1),48)}

xrgxhcueshoedxt.com. 0.0 48 48.0 5 5 {((chi),12),((yvr),19),((lax),5),((ash),5),((dfw),7)} {((1),48)}

uotsljmfuxd58.com. 0.0 48 48.0 5 5 {((chi),12),((yvr),19),((lax),5),((ash),5),((dfw),7)} {((1),48)}

sycfdptbswdf3.com. 0.0 48 48.0 5 5 {((ash),6),((chi),12),((yvr),19),((dfw),6),((lax),5)} {((1),48)}

pojrcpqajhcuqq4b.com. 0.0 48 48.0 5 5 {((chi),12),((yvr),19),((lax),5),((ash),5),((dfw),7)} {((1),48)}

odmwooyyfoysnc.com. 0.0 48 48.0 5 5 {((chi),12),((yvr),19),((lax),5),((ash),6),((dfw),6)} {((1),48)}

jcdbrovrumwouoo.com. 0.0 48 48.0 5 5 {((chi),12),((yvr),20),((lax),5),((ash),5),((dfw),6)} {((1),48)}

dsiahpklfbfbwqc3.com. 0.0 48 48.0 5 5 {((chi),12),((yvr),19),((lax),5),((ash),5),((dfw),7)} {((1),48)}

DGA - 1

- 22 DGA domains sharing identical spike features (volume, number of IPs, number of resolvers, resolver distribution)
- Subsequent hours' traffic patterns are also identical

Fake software

- flnhzjwdjqrwjqm.gangsta12.ru. 0.0 55 55.0 41 6
{((ams),7),((cdg),3),((fra),23),((wrw),5),((mia),13),((lon),4)} {((1),55)}
- 82.118.16.114, AS15626, ITLAS ITL Company
- 9 IPs in the vicinity are hosting same fake SW
- 82.118.16.107 - 82.118.16.115
- SoftwareBundler:Win32/LoadArcher.A

Fake software

 <https://www.virustotal.com/en/ip-address/82.118.16.114/information/>

Community Statistics Documentation FAQ About English Join our community Sign in

2015-10-04 forest-pad-deeplv.ru
2015-10-04 gangsta12.ru
2015-10-04 hdedmk25pb.ru
2015-10-04 ijnabxsewxe.p.magicbaseball.ru

[More](#)

⚠ Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset.**

8/65	2015-10-05 00:11:36	http://ozfdxubybugvp.anybodyloudly.ru/start_page.exe
5/65	2015-10-05 00:09:59	http://iophanti.magicbaseball.ru/nethost.exe
6/65	2015-10-05 00:03:01	http://iospecqutzuhm.stringglow.ru/start_page.exe
6/65	2015-10-05 00:01:14	http://ijnabxsewxe.p.magicbaseball.ru/start_page.exe
7/65	2015-10-05 00:00:18	http://lkjumbeuqzmlp.29rgio29kh.ru/start_page.exe
8/65	2015-10-04 23:50:34	http://ktjaupfepzep.anybodyloudly.ru/chrome_extension.exe
3/65	2015-10-04 23:03:51	http://stringglow.ru/
1/65	2015-10-04 23:03:44	http://forest-pad-deeplv.ru/
1/65	2015-10-04 23:02:32	http://hdedmk25pb.ru/
3/65	2015-10-04 23:02:05	http://9wko968ccy.ru/

[More](#)

⬇ Latest detected files that were downloaded from this IP address

Latest files that are **detected by at least one antivirus solution and were downloaded by VirusTotal from the IP address provided.**

40/57	2015-10-05 00:11:39	2a70b91e2b80b2f6d24edaddf0089754813b5face65768457239f8ca80c5c9aa
34/56	2015-10-05 00:10:02	9425e7ef719ff9bd6c5e64db65ed6236cd547678bcd3eaf6b94e1aec8abc1b3
41/57	2015-10-04 23:50:38	020b850d513fd7bdb7ed4f8178d07984070eb69a1f3504c4dc639fef0c9def09
35/57	2015-10-04 21:08:53	706ed6c471ce806e96ebadb77ba53869e2f297e0ccdd67a193d5b52d5a1df2739

Phishing

american-express-1v3a.com

american-express-4dw3.com

american-express-d34s.com

american-express-d3s1.com

american-express-f34s.com

american-express-s2a3.com

american-express-s3d2.com

american-express-s43d.com

american-express-s4a2.com

american-express-sn35.com

Enter domain name, ASN, IP address, or email address

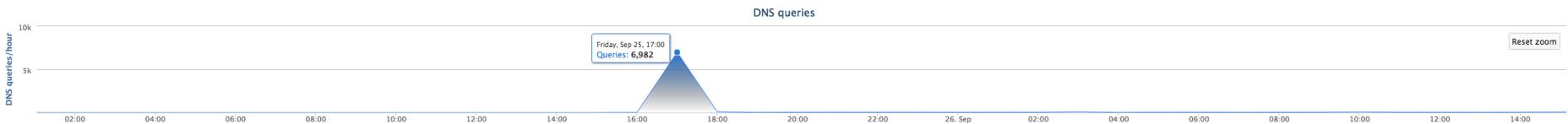
INVESTIGATE

american-express-1v3a.com american-express-3b1v3a.com american-express-1f06.com american-express-c6v9.com
american-express-n4q9.com american-express-s2a3.com american-express-4dw3.com american-express-w4gs.com
american-express-rfsa.com american-express-d3s1.com

DETAILS FOR AMERICAN-EXPRESS-1V3A.COM

[Search in Google](#)[Download as CSV](#)

This domain is currently in the OpenDNS Security Labs block list



WHOIS RECORD DATA

Registrar Name: Todaynic.com, Inc. IANAID: 697

Last retrieved September 25, 2015

[Get latest](#)

Created: September 25, 2015

Updated: September 25, 2015

Expires: September 25, 2016

[Raw data](#)

Email Address

whois-protect@hotmail.com

Associated Domains

98 Total - 95 malicious

Email Type

Administrative, Registrant, Billing, Technical

Last Observed

Current

Nameserver

dns2.555mir.ru

Associated Domains

21 Total - 18 malicious

Last Observed

Current

dns1.555mir.ru

21 Total - 18 malicious

Current

[Show more WHOIS data ▾](#)

DOMAIN TAGGING

Period	Category	URL
Sep 29, 2015 - Current	Phishing	http://american-express-1v3a.comamericanexpress/
Sep 29, 2015 - Current	Malware	
Sep 25, 2015 - Current	Phishing	http://american-express-1v3a.comamericanexpress/
Sep 25, 2015 - Current	Malware	

Phishing

- american-express-1v3a.com. 4.0 1351 337.75 487
16 {((nyc),78),((ash),87),((chi),173),((yvr),60),((ams),69),
((cdg),60),((yyz),17),((sin),262),((fra),18),((lax),37),((dfw),137),
((wrw),1),((pao),4),((mia),75),((syd),14),((lon),259)} {{{(1),1350},
((255),1)}

Phishing

- Hosting IPs:

- 149.210.234.215, AS20857

- 162.218.89.142, AS36352

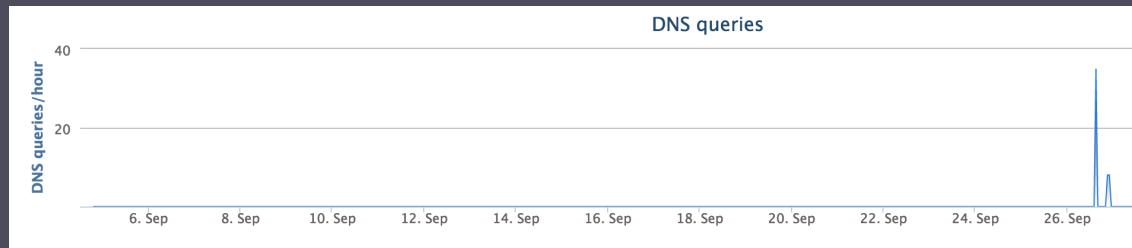
- 91.108.83.213, AS31400

- 93.189.42.13, AS41853

- Pivot around IPs and registrant emails, we find a lot more phishing sites for banks, e.g. Nova Scotia Bank, Royal Bank of Canada, and carding sites:
- www.scotiasupport.com, rbcrooyalbanksolution.com
- prvtzone.cc, mcduck.cc, mrbin.tw

Some FPs

- Some possible false positives (xard38.ooawaiidaddict.net, uclfgji.kieyopowertochange.net)
- Chinese SEO
- Pinyin + IP distribution

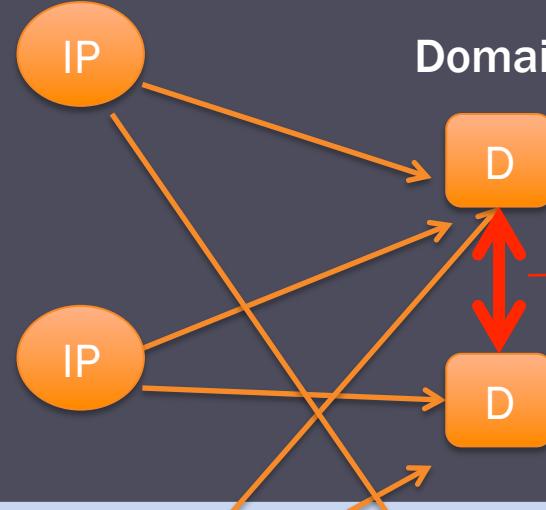


Graph Analytics

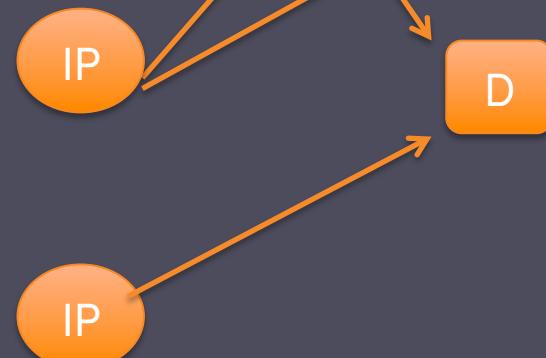
Time window

Client IPs

Domains



Edge in the co-occurrence
graph



Use Cases:

- Domains sharing same theme, e.g. security sites, hacking, carding sites
 - Visited by users with related interest
- Example: www.cert.org

CO-OCCURRENCES

podone.noxsolutions.com (86.55) dzone.com (8.33) searchsecurity.techtarget.com (5.12)

RELATED DOMAINS

www.bluesnews.com (6) seclists.org (6) www.biologynews.net (5) www.astrobio.net (4) www.boingboing.net (4) isc.sans.edu (4)
feeds.feedburner.com (3) www.freebsd.org (3)

- Botnet CnC domains, e.g. DGAs
- Infection chains: compromised sites -> Exploit kit landing domains

Co-occurring (Related) Domains

- Hourly job
- output is a 1.5 GB json file
- Number of Edges: 61,280,656
- Number of Vertices: 2,207,680
- 100luimg.361lu.com. {"ucsec1.ucweb.com":3.0,"d2.avgc.us":3.0,"home.1100lu.info":4.0}

Graph Analytics

- Find connected components
- Calculate density of every component
- Density=Nb. of edges / Nb. of vertices
- Number of Connected Components: 85421
- Distribution of nodes per component follows power-law

Component Distribution

```
In [59]: d_table.topk('DENSITY', k=50).print_rows(num_rows=50, num_columns=50)
```

component_id	COUNT	EDGE	DENSITY
7511	1907334	121647228	31.8893355857
2951	1350	73956	27.3911111111
148259	56	1280	11.4285714286
144924	106	1660	7.83018867925
95490	2640	36768	6.96363636364
385564	30	408	6.8
80013	78	1048	6.71794871795
36758	30	380	6.33333333333
109292	134	1672	6.23880597015
411980	104	1192	5.73076923077
307675	24	260	5.41666666667
123948	58	612	5.27586206897
385816	36	376	5.22222222222
385844	26	268	5.15384615385
207245	126	1288	5.11111111111
162841	84	856	5.09523809524
205820	152	1544	5.07894736842
276429	28	284	5.07142857143
93746	1998	20212	5.05805805806
331628	36	364	5.05555555556
20550	86	864	5.02325581395
115877	22	220	5.0
116691	2000	20000	5.0

Results

```
In [82]: v[v.apply(lambda x: x['component_id'] == 346812)].print_rows(num_rows=200, num_columns=200)
```

_id	in_degree	out_degree	total_degree	component_id
bbulotjtlego.biz.	0	10	10	346812
ckbbtxxbuvrj.biz	8	0	8	346812
csdmslkjmldl.biz.	0	10	10	346812
dcwxqrqjimmm.biz.	0	10	10	346812
dfijehkkjbvu.biz.	0	10	10	346812
dsjjjoonmqmf.biz.	0	10	10	346812
enmlmsiiyikp.biz.	0	10	10	346812
fgodsyitsrsd.biz.	0	10	10	346812
fslfvccstqgvt.biz	10	0	10	346812
jcbnobcdkbuv.biz.	0	6	6	346812
jppxtqnytmnn.biz	6	0	6	346812
jppxtqnytmmn.biz.	0	6	6	346812
khiullewpcpt.biz.	0	10	10	346812
khjnvkxqjihg.biz.	0	10	10	346812
qqyukmtjlcck.biz.	0	10	10	346812
scurvvkgewx.biz.	0	10	10	346812
bbyrrwpinxcd.biz.	0	10	10	346812
bnmjrssqskdj.biz	10	0	10	346812
bnmjrssqskdj.biz.	0	10	10	346812

```
In [84]: v[v.apply(lambda x: x['component_id'] == 385816)].print_rows(num_rows=200, num_columns=200)
```

_id	in_degree	out_degree	total_degree	component_id
mail3.tpmix.info	10	0	10	385816
mail12.tpmix.info.	0	11	11	385816
mail15.tpmix.info	9	0	9	385816
mail18.tpmix.info	12	0	12	385816
mail11.tpmix.info.	0	8	8	385816
mail15.tpmix.info.	0	9	9	385816
mail16.tpmix.info	10	0	10	385816
mail16.tpmix.info.	0	10	10	385816
mail17.tpmix.info	9	0	9	385816
mail14.tpmix.info.	0	11	11	385816
mail15.tpmix.info.	0	10	10	385816

- Detection of DGAs, spam domains, etc.

Conclusion

- Developed a more holistic view into DNS to detect threats
- Use traffic patterns below the recursive and combine it with pivoting around hosting infrastructures for more efficient threat detection
- Use traffic-based models to extract seeds from the large DNS data set
- Use graph analytics to explore communities of related threat domains

We are hiring!

OpenDNS

OpenDNS is
now part of Cisco.



Thomas Mathew and Dhia Mahjoub

tmathew@opendns.com

dhia@opendns.com
@DhiaLite