RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HTA-W14

EARLY DETECTION OF MALICIOUS ACTIVITY – HOW WELL DO YOU KNOW YOUR DNS?

Merike Käo

CTO
Farsight Security
merike@fsi.io

Talking Points

- Three Decades of DNS Evolution
- Malicious Activity Utilizing DNS
- New Vectors: IDN / IPv6 / IoT
- Using DNS Information As Threat Intelligence
- Conclusions

How To Apply Information From Today

- Next week
  - Identify who ‘owns’ DNS in your environment
  - Include both brand protection and infrastructure components
- Over next 3 months
  - Perform an assessment of your DNS infrastructure
    - Know ALL registered domains; are those registrations protected with multifactor auth?
    - Get a baseline: determine where queries and responses are going (i.e. what's "normal?”)
- Within 6 months
  - Implement techniques to detect and mitigate DNS abuse for malicious activity
    - Hijacking, Data Exfiltration, DDoS
    - Actively manage DNS traffic on the network

THREE DECADES OF DNS EVOLUTION

“ Let’s Put Everything In The DNS ”

A Brief History Of DNS

- ARPANET utilized a central file (HOSTS.TXT)
  - Contained names to address mapping
  - Maintained by SRI's NIC (Stanford Research Institute's Network Information Center)
- Changes emailed to NIC
- Administrators downloaded HOSTS.TXT file
- Growth created problems with scalability, name collisions & consistency
- DNS created in 1983 by Paul Mockapetris (RFCs 882 and 883)
- DNS attained its *modern* form in 1987 (RFCs 1034 and 1035)

What Is DNS?

- Globally distributed, loosely coherent, dynamic database
- Mapping names to IP addresses
  - RFC 1034: DNS concepts and facilities.
  - RFC 1035: DNS implementation and protocol specification.
- Comprised of three components
  - A “name space”
  - Servers making that name space available
  - Resolvers (clients) which query the servers about the name space
- Both UDP and TCP are used

DNS Looks Simple

Recursive Server

Primary/Secondary Servers

Q1: www.farsighsecurity.com. / A?

Q2: www.farsightsecurity.com./A

R2: com./NS

Authoritative ROOT

Q3: www.farsightsecurity.com./A

R3: farsightsecurity.com./NS

Authoritative COM

Q4: www.farsightsecurity.com./A

R4: www.farsightsecurity.com./A

Authoritative farsightsecurity

R1: www.farsightsecurity.com./A

FARSIGHT SECURITY

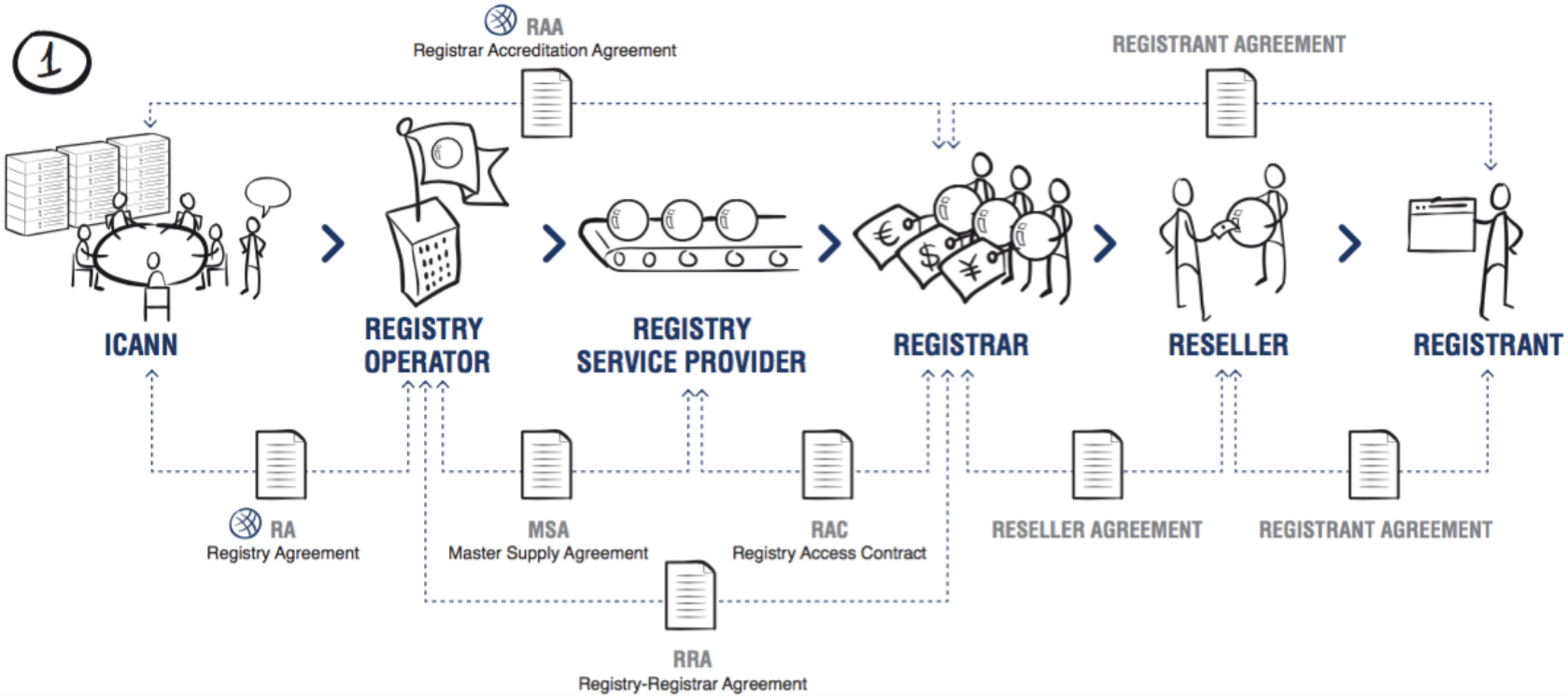
DNS In Reality….Not So Simple

- Presentation at IETF DNS Operations meeting (3/20/18)
  - https://datatracker.ietf.org/meeting/101/materials/slides-101-dnsop-sessa-the-dns-camel-01
- Raised issues of increased DNS standards complexity
  - 185 RFCs / 2781 pages of text
  - Unexpected interaction of features
- Complexity decreases quality and security
  - Malicious actors can take advantage of the complexity

DNS Security

- You (mostly) have control over your DNS infrastructure
  - Domain management
  - Recursive DNS resolver settings
- What aspects are not under your control?
  - Do you know when someone else is using your domain?
  - Do you know when someone is redirecting DNS traffic from your site?
- Have you ever thought about who you register your domain with?
  - Authentication practices for domain management

Who Protects Your Domain Registration?



Source: https://newgtlds.icann.org/en/announcements-and-media/infographics/dns-industry-responsibilities

Understanding Resource Records

Common Record Types

A	Map host to an IPv4 address
AAAA	Map host to an IPv6 address
NS	Defines the name servers that are used for the zones
PTR	Defines a domain name that is associated with an IP address
TXT	Used for communicating arbitrary and unformatted text
MX	Defines mail exchange server that is associated to a domain name

Other Record Types

SOA	Provides information about the start of authority (aka APEX)
DS	Indicates that the delegated zone is digitally signed
SRV	Service location (IP address and port information)
NSEC3	Provides authenticated denial of existence
HINFO	Specifies type of CPU and OS of host
CNAME	Define an alias for a domain name

DNS – Also Used For Email Security

- SPF (Sender Policy Framework)
  - SPF records are typically defined using the TXT record type
  - SPF record type is deprecated
  - Specifies a list of authorized host names/IP addresses that mail can originate from for a given domain name
- DKIM (Domain Keys Identified Mail)
  - Requires addition of public keys into DNS
    - Inserted directly into zone as a TXT record
    - Or, it will be a CNAME pointing to the key in your provider's DNS
  - Validates via cryptographic authentication that organization delivering email the right to do so
- DMARC (Domain-based Message Authentication, Reporting and Conformance)
  - DMARC policies are published in a DNST XT RR

Record Types Seen In A Day

- Observations validate that common RR types are seen more often
- The more interesting information is in the lesser utilized RR types
- Could they be used for malicious activity?

Observations	% of Obs	Record Type & Code
16,964,386	57.27%	A (1)
9,460,957	31.94%	SOA (6)
1,745,213	5.89%	CNAME (5)
714,677	2.41%	NS (2)
259,468	0.88%	PTR (12)
204,785	0.69%	MX (15)
149,771	0.51%	TXT (16)
100,424	0.34%	AAAA (28)
18,140	0.06%	NULL (10)
2,393	0.01%	SRV (33)
440	<0.01%	SPF (99)
77	<0.01%	WKS (11)
59	<0.01%	<UNKNOWN>(1169)
7	<0.01%	DNAME (39)
4	<0.01%	LOC (29)
3	<0.01%	HINFO (13)
1	<0.01%	<UNKNOWN>(4652)
1	<0.01%	<UNKNOWN>(4097)
1	<0.01%	RP (17)
29,620,807	**100.00%**	

DNS Response Codes

- When a DNS query is made, it succeeds or fails
- The status is returned as a ‘DNS response code’
  - **$ dig google.com**

    [...]

    ;; ->>HEADER<<- opcode: QUERY, **status: NOERROR** [etc]

    google.com. 180 IN A 216.58.193.110

    NOERROR == normal successful completion status code
  - **$ dig asasdjasjnasfjnasfnkafs.com**

    [...]

    ;; ->>HEADER<<- opcode: QUERY, **status: NXDOMAIN** [etc]

    NXDOMAIN == domain does not exist

MALICIOUS ACTIVITY UTILIZING DNS

Everything Old Is New Again

Criminals Love DNS

- DNS is often a neglected network service
  - Configure it and it just works
  - As long as no users complain all is good
  - Cost center rather than strategic tool
- Cybercrime utilizing DNS is increasing
- Noone is watching and it's a rich target
  - Expired reputable domains being re-registered for abuse
  - Old applications still querying for FQDNs associated with old companies
  - Look-alike domains that are difficult to detect

DNS Abuse Is Becoming "Trendy"

BUSTED —

Legal raids in five countries seize botnet servers, sinkhole 800,000+ domains

At one point, Avalanche network was responsible for two-thirds of all phishing attacks.

SEAN GALLAGHER - 12/1/2016, 10:55 AM

Brazilians whacked: Crooks hijack bank's DNS to fleece victims

Usernames, passwords swiped for hours, malwar
dropped on PCs

By Iain Thomson in San Francisco 5 Apr 2017 at 07:33 27 SHAR

Dell forgot to renew PC data recovery domain, so a squatter bought it

Days later it served malware, but the only visible damage was to Dell's reputation

By Simon Sharwood, APAC Editor 26 Oct 2017 at 05:04 56 SHARE

Dell forgot to re-register a domain name that many PCs it has sold use to do fresh installs of their operating systems. The act of omission was spotted by a third-party who stands accused of using it to spread malware.

SECURITY

LinkedIn DNS hijacked, site offline

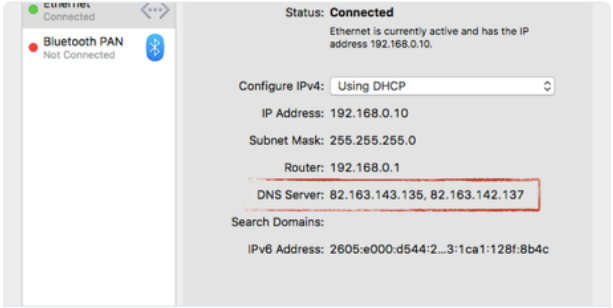
Be patient ... we've dealt with hacks before says business hub

By Richard Chirgwin, 20th June 2013 Follow 1,877 followers

Objective-See
@objective_see

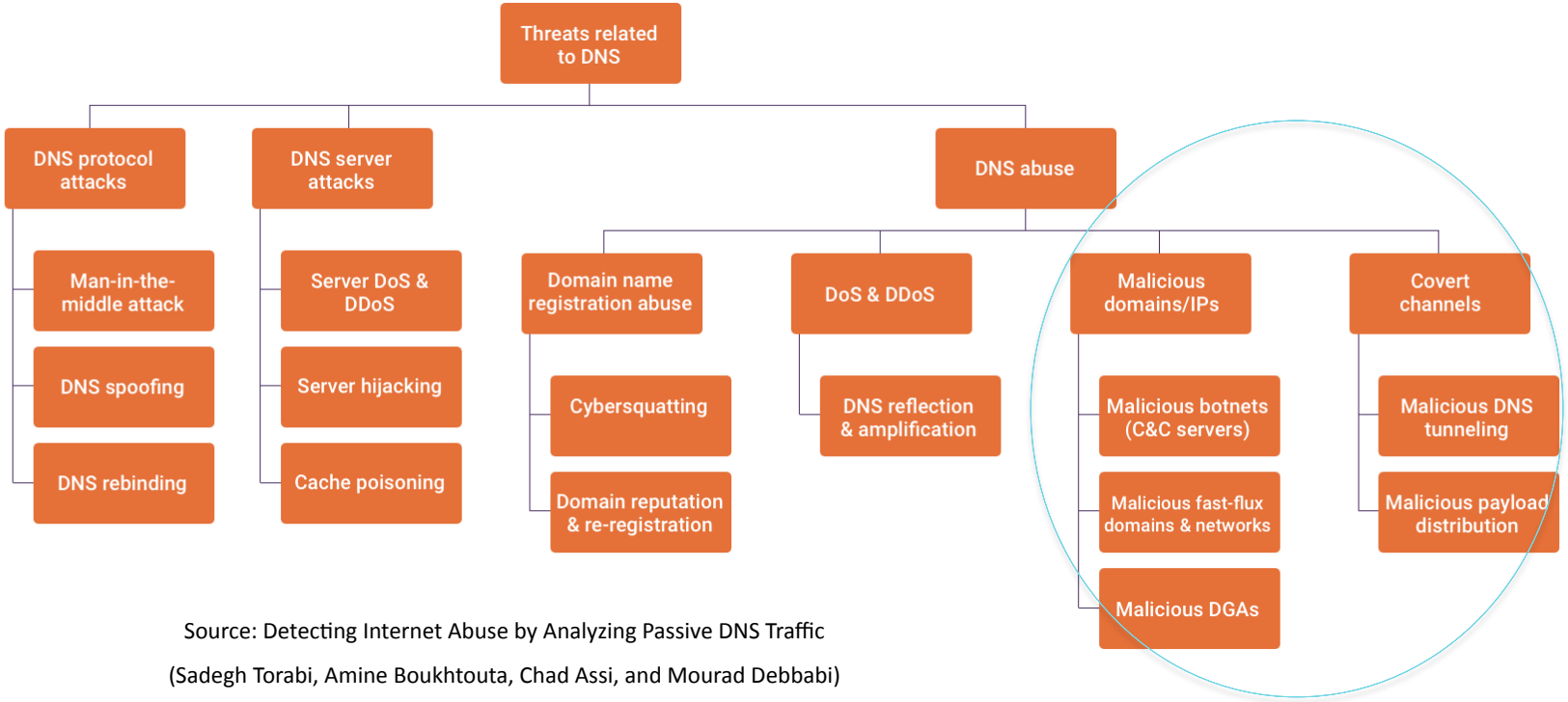
OMG do we have the 1st macOS malware of 2018 and can I name it!? OSX/MaMi is undetected by AV (src: VT) infecting Macs around the world - persistently installs new root cert & hijacks DNS settings: objective-see.com/blog/blog_0x26…
mahalo to a good friend for the ping

3:43 AM - Jan 12, 2018



Ay MaMi
Analyzing a New macOS DNS Hijacker: OSX/MaMi
objective-see.com

DNS Threats



Source: Detecting Internet Abuse by Analyzing Passive DNS Traffic

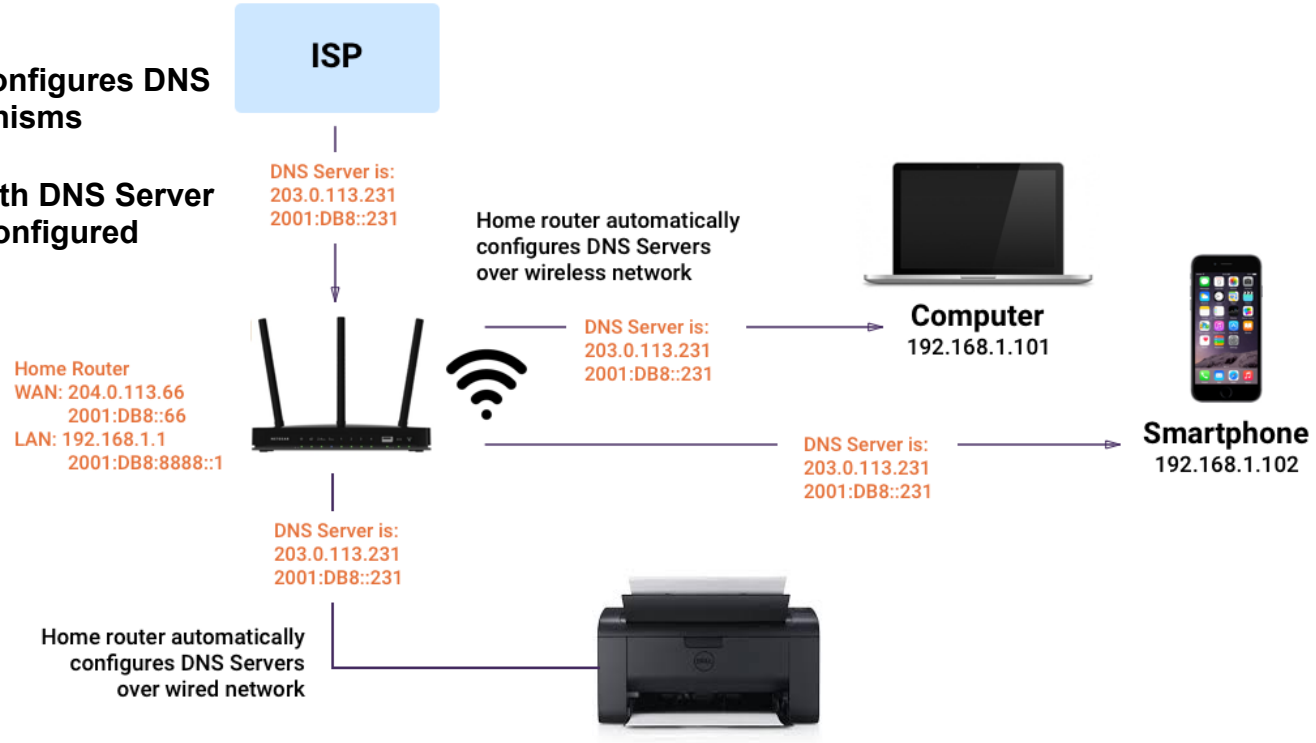
(Sadegh Torabi, Amine Boukhtouta, Chad Assi, and Mourad Debbabi)

Recursive DNS Server Configuration

Service provider automatically configures DNS Servers using automated mechanisms

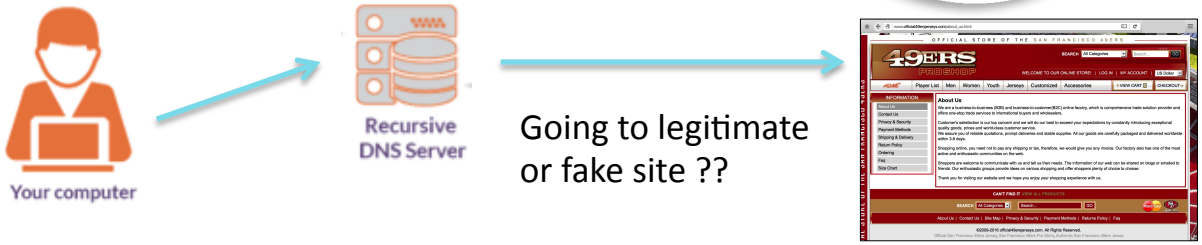
OR

Service provider provides you with DNS Server IP addresses that get statically configured



Do You Know Where Your Queries Are Going?

- DNS Hijacking
  - Ongoing threat
  - Not easy to detect
- DNS Changer (aka Ghostclick)
- OSX/MaMi – 2018
  - Malware distributed as unsigned Mach-O 64-bit binary
  - Installs a new root certificate and hijacks DNS servers
  - Adds two DNS servers to infected hosts
    - 82.163.143.135
    - 82.163.142.137



Why Do Criminals Register Domain Names?

- Often done at high volumes
  - Phishing sites
  - Ransomware payment web pages
  - Malware distribution sites
  - Counterfeit goods sites
  - Illegal pharmaceutical or piracy sites
- Domain names also part of criminal DNS infrastructure
  - Server names for eCrime name resolution
  - Names for command-control botnet administration

New gTLD Statistics

Current Statistics *(Updated monthly)*

Application Statistics: Overview (as of 28 February 2018)	
Total Applications Submitted	***1930***
Completed New gTLD Program (gTLD Delegated** - introduced into Internet)	1230
Application Withdrawn	610
Applications that Will Not Proceed/Not Approved	54
Currently Proceeding through New gTLD Program*	36

- Some Top Level Domains are more often used for abusive activities
- Economics plays a role
- Criminals use gTLDs rationally and adapt as necessary

Source: https://newgtlds.icann.org/en/program-status/statistics

Domain Generating Algorithms (DGA)

- What are they?
  - Ability to create hundreds or thousands of domains according to a specified "recipe"
  - Designed for resiliency
  - Good guys need to register or block ALL DGA generated names
  - Bad guy only needs to be able to register one to retain/regain control of botnet.
- What are they used for?
  - Botnet Command and Control

Sample Confiker DGA Domains (04-11-18)

aaaacs.ws.
aabrqn.ws.
aafwpu.ws.
aagfeu.ws.
aalmbn.ws.
aangnd.ws.
aasugq.ws.
aavzig.ws.
aaylgt.ws.
abbmfu.ws.
abfhve.ws.
abufyj.ws.
abumoh.ws.
abzztv.ws.
acenmj.ws.
acixby.ws.
acjbip.ws.
ackxsz.ws.
acwftw.ws.
adghbp.ws.
adnvzi.ws.
aebmpv.ws.
aegtcp.ws.

aekaus.ws.
aembux.ws.
aeodjm.ws.
aepjrr.ws.
afcwte.ws.
afdxgh.ws.
agdyba.ws.
agnvna.ws.
ahcgaq.ws.
ahellc.ws.
ahetum.ws.
ahftbc.ws.
ahgijz.ws.
ahijux.ws.
ahlhoz.ws.
ahmnop.ws.
ahnjdx.ws.
ahoiuw.ws.
aierkc.ws.
aiitru.ws.
aixrqi.ws.
ajgfkx.ws.
ajlvkm.ws.

ajmoyv.ws.
ajpjlc.ws.
ajtajz.ws.
ajxpss.ws.
akftnk.ws.
akpamg.ws.
akpgtb.ws.
akucsd.ws.
akudby.ws.
akurgu.ws.
akxnnk.ws.
akzsvw.ws.
alckzx.ws.
alhmfi.ws.
aljvwp.ws.
alwjns.ws.
alzeic.ws.
ambpqw.ws.
amiodi.ws.
amlxhm.ws.
amqogt.ws.
amsbkt.ws.
amuhnr.ws.

anefct.ws.
anirsx.ws.
anpwvv.ws.
anrwts.ws.
anwbbs.ws.
aoavxt.ws.
aoiyyb.ws.
aonrgc.ws.
aosokx.ws.
apcxkp.ws.
apiyip.ws.
apnguu.ws.
aprawe.ws.
apwscz.ws.
apxnws.ws.
aqdtaw.ws.
aqntlz.ws.
arcnza.ws.
arfpfj.ws.
argapq.ws.
arosoh.ws.
arvjqo.ws.
asbzdv.ws.

asdbfd.ws.
asgfqb.ws.
aslooq.ws.
aswfrd.ws.
asxhyk.ws.
atbxfd.ws.
atfjqd.ws.
atijcr.ws.
atinwa.ws.
atjiuc.ws.
atmfjw.ws.
atqxwq.ws.
atvzwp.ws.
atzrfb.ws.
aucoiq.ws.
audxic.ws.
aufoqx.ws.
aufswl.ws.
autece.ws.
auuuul.ws.
auvhnu.ws.
avbenr.ws.
avdanb.ws.
.

avdxal.ws.
avhtle.ws.
awbuec.ws.
awdyok.ws.
awgtga.ws.
awjilu.ws.
awlaga.ws.
awpqdo.ws.
awregw.ws.
awrvqk.ws.
awuwjr.ws.
axaasj.ws.
axdfbp.ws.
axesap.ws.
axgvph.ws.
axlrxp.ws.
axmayt.ws.
axqwkx.ws.
axukxc.ws.
axwaqx.ws.
ayezrv.ws.
ayhqsd.ws.
ayingi.ws.

ayjlmb.ws.
aykrdn.ws.
ayrvao.ws.
ayugfe.ws.
azavsp.ws.
azawnt.ws.
azcobo.ws.
azeeua.ws.
azlwkx.ws.
azozce.ws.
aztfie.ws.
azvfpx.ws.
azzzzv.ws.
badoqh.ws.
baquud.ws.
baxpcz.ws.
bazlaz.ws.
bbbbdm.ws.
bbcied.ws.
bbciwo.ws.
bbfhme.ws.
bbjmbp.ws.
bbkqfi.ws.

bbphml.ws.
bbtqpt.ws.
bccmhy.ws.
bcgbwa.ws.
bcoygo.ws.
bcrrve.ws.
bczwql.ws.
bdauyq.ws.
bdjwjf.ws.
bdmbga.ws.
bdmsca.ws.
bdnnei.ws.
bdxvzj.ws.
bekfdi.ws.
bewmhi.ws.
bexmvn.ws.
bfnlud.ws.
bfwizf.ws.
bgfmvw.ws.
bggnuu.ws.
bgmwee.ws.
bgqfwg.ws.
bgrebt.ws.
.

bgthuv.ws.
bguczj.ws.
bgzhlm.ws.
bhfxgu.ws.
bhgebt.ws.
bhjcue.ws.
bhkylj.ws.
bhnbja.ws.
bhsdwc.ws.
bijitm.ws.
bijnep.ws.
bintgz.ws.
biptmt.ws.
biqtmy.ws.
bisijg.ws.
bizpys.ws.
bjcwgl.ws.
bjkqch.ws.
bjkvvt.ws.
bjmkcv.ws.
bjpilp.ws.
bjusmt.ws.
bjyxtg.ws.

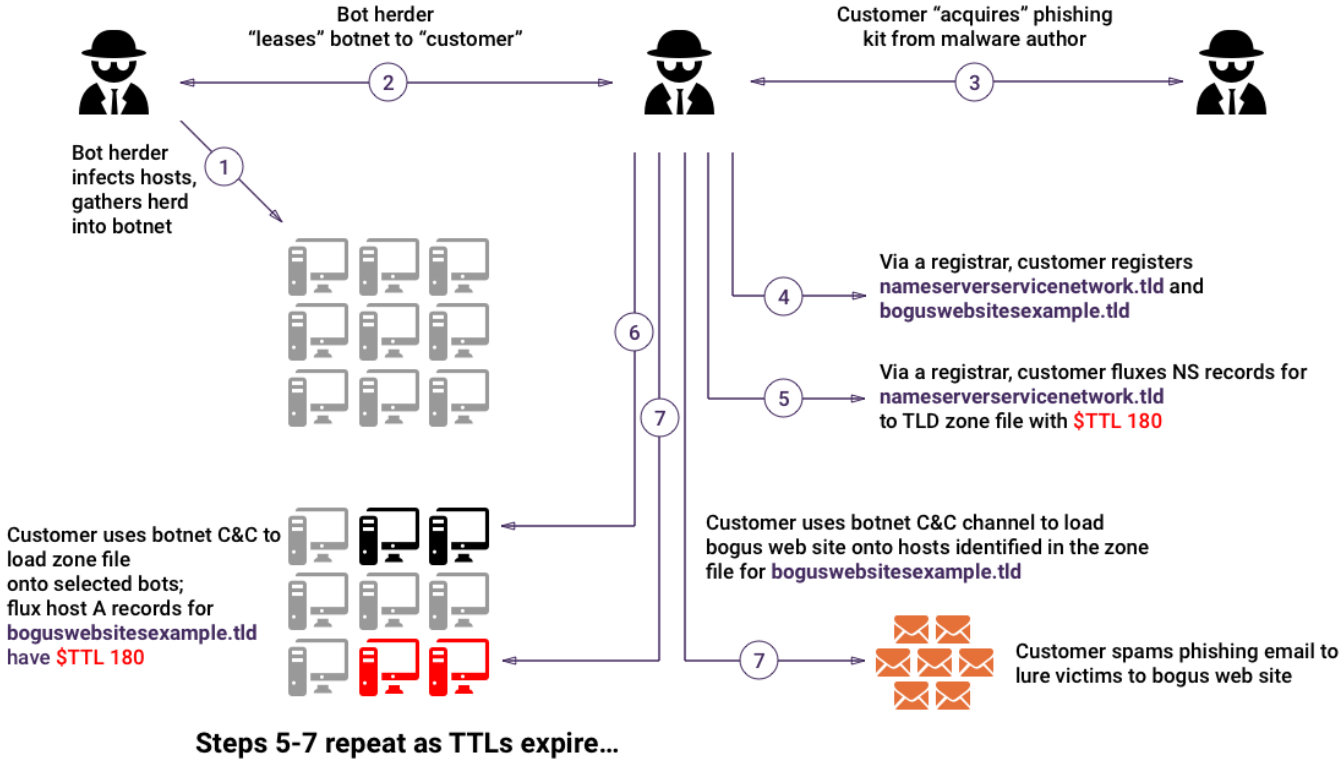
.....

Sample snaphot of a Confiker sinkhole yielded total of **6,267 domains**

xekepw.ws.
xeonqu.ws.
xeyzdy.ws.
xezofq.ws.
xffqvb.ws.
xfmmgo.ws.
xfvjel.ws.
xgaqyr.ws.
xgdsrv.ws.
xgekap.ws.
xgflti.ws.
xhawsk.ws.
xheami.ws.
xhesbo.ws.
xhgezo.ws.
xhgvkr.ws.
xhiutg.ws.
xhxgzn.ws.
xhzism.ws.
xhztdx.ws.
xicnrj.ws.
xikvzz.ws.
xiodhf.ws.

Fast Flux

- IP addresses are swapped at high frequency, using a combination of round-robin IP addresses and a very short TTL
- Enables botnets to hide behind rapidy shifting network of compromised hosts, acting as proxies.



DNS As Covert Malware Channel

- Malware on infected computer does TXT lookups to botnet C&C
- TXT responses contain instructions for bot
- Examples
  - Feederbot
  - Morto

NEW VECTORS: IDN / IPV6 / IOT

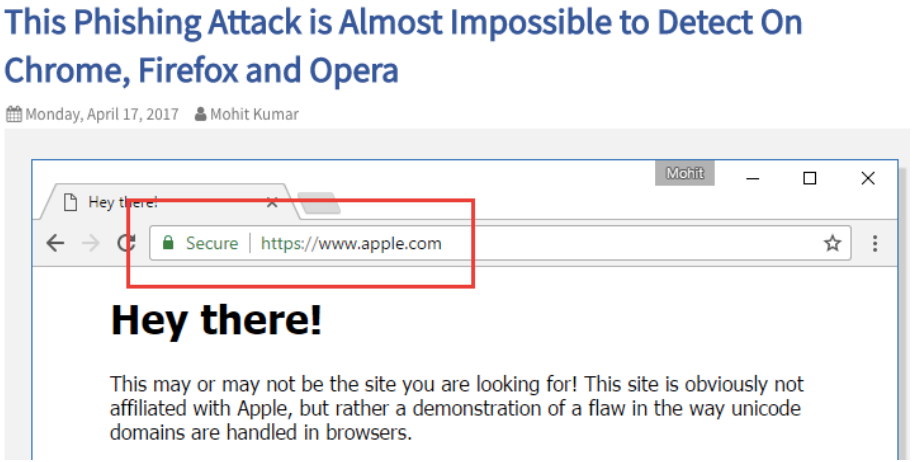
DNS Is Fundamentally Everywhere

International Domain Names (IDNs)

- Most TLDs use Roman or Latin letters, numbers and/or hyphens
- IDNs meet needs of other languages
  - Arabic
  - Chinese
  - Cyrillic (Russian)
  - Indian (Gangla, Devanagari, Gujarati, Gurmukhi, Tamil, Telugu)
  - Katakana (Japanese), etc.
- IDNs get represented in two ways
  - U-label (using the international character set, such as 中信)
  - A-label (ASCII-encoded form, such as xn—fiq64b)

IDN Homographs

- Different letters or characters might look alike
  - Uppercase “I” and lowercase “l”
  - Letter “O” and number “0”
- Characters from different alphabets or scripts may appear indistinguishable from one another to the human eye
  - Individually they are known as *homoglyphs*
  - In the context of the words that contain them they constitute *homographs*



IDN Homograph Attacks

Things are not always what they appear to be!

- Bad actors figured out they can register IDNs and target sites using homoglyphs (or sometimes homographs)
- Hard to discern difference with human eye

Example Punycode to rendered Unicode IDNs:

Unicode 0+0430

xn--frsight-2fg.com --> farsight.com

xn--80ak6aa92e.com --> appıe.com

All Cyrillic characters

IDN Abuse Research

- Examined 125 brand names and monitored IDN homographs in real time
  - https://www.farsightsecurity.com/2018/01/17/mschiffm-touched_by_an_idn/
- In 3 month period observed 116,113 homographs
- Large number seems disturbing and needs further investigation
  - No assumption made of intent against domains or domain owners
- Did find some live phishing sites
  - Companies were contacted to alert them of suspected phishing sites
  - Demonstrates that threat of IDN homograph impersonation is both real and actively being exploited

Suspicious IDNs

- Major brands
- gTLDs
- ccTLDs
- Led to questions of who creates policy and enforces IETF recommendations and ICANN guidelines

CREDIT SUISSE

```
xn--crditsuisse-cbb.at.          -->    créditsuisse.at.
xn--crditsuisse-cbb.ch.          -->    créditsuisse.ch.
xn--crditsuisse-cbb.com.         -->    créditsuisse.com.
xn--crditsuisse-cbb.de.          -->    créditsuisse.de.
xn--crditsuisse-cbb.dk.          -->    créditsuisse.dk.
xn--crditsuisse-cbb.eu.          -->    créditsuisse.eu.
xn--crditsuisse-cbb.net.         -->    créditsuisse.net.
xn--crdit-suisse-ceb.at.         -->    crédit-suisse.at.
xn--crdit-suisse-ceb.ch.         -->    crédit-suisse.ch.
xn--crdit-suisse-ceb.com.        -->    crédit-suisse.com.
xn--crdit-suisse-ceb.de.         -->    crédit-suisse.de.
xn--crdit-suisse-ceb.dk.         -->    crédit-suisse.dk.
xn--crdit-suisse-ceb.net.        -->    crédit-suisse.net.
xn--credit-sisse-klb.com.        -->    credit-süisse.com.
```

EBAY

```
xn--bay-ema.com.                 -->    êbay.com.
xn--eby-fla.com.                 -->    ebáy.com.
xn--eby-bla.com.                 -->    ebày.com.
xn--eby-hsb.com.                 -->    ebɑy.com.
xn--eby-jla.com.                 -->    ebây.com.
xn--80aj7b8a.com.                -->    eьay.com.
```

Suspicious IDNs

MISC: LUXURY BRANDS

```
www.xn--gucc-tpa.com.          -->      www.guccì.com.
xn--gucc-tpa.com.              -->      guccì.com.
xn--herms-7ra.com.             -->      hermès.com.
www.xn--herms-7ra.fr.          -->      www.hermès.fr.
www.xn--lousvuitton-qcb.com.   -->      www.louísvuitton.com.
```

MISC: SOCIAL PLATFORMS

```
xn--nstagram-11a.com.          -->      ınstagram.com.
xn--nstagram-skb.com.          -->      ınstagram.com.
www.xn--nstagram-skb.com.      -->      www.ınstagram.com.
xn--istagram-7pb.com.          -->      iṇstagram.com.
www.xn--imgu-t4a.com.          -->      www.imguŕ.com.
xn--imgr-sra.com.              -->      imgúr.com.
xn--whatspp-lwa.com.           -->      whatsápp.com.
xn--whtspp-cxcc.com.           -->      whatsapp.com.
```

How Well Do You Understand IPv6 ?

- It *is* similar to IPv4…..but NOT
- IPv4 and IPv6 interface addressing nuances
  - Which IPv6 address used to source traffic?
  - When is IPv4 address used vs IPv6 address for a dual-stacked host?
  - Where are special transition addresses used?
- More IPv6 nuances
  - Every mobile device is a /64
  - Extension headers
  - Path MTU Discovery
  - Fragmentation

Using DNS For IPv6 Related Investigations

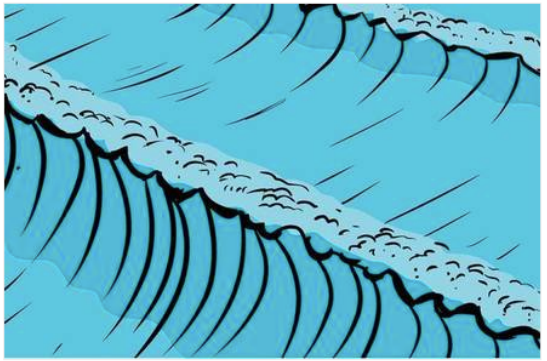
- Correlate domains seen in IPv4 and in IPv6
- Investigate same domains seen in IPv4 and IPv6
- Investigate domains seen separately from IPv4 vs IPv6 addresses

Passive DNS can be used to correlate IPv4 and IPv6 related information

It's begun: 'First' IPv6 denial-of-service attack puts IT bods on notice

Internet engineers warn this is only the beginning

By Kieren McCarthy in San Francisco 3 Mar 2018 at 09:30 59 SHARE ▼



DNS Abuse – IoT

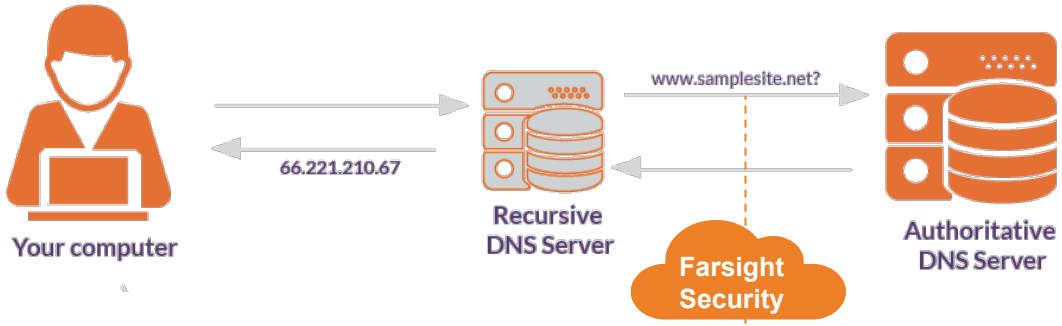
- Billions of devices available for DNS exploitation
  - Hijacking
  - Spoofing
  - Data Exfiltration
- Some DNS attacks ARE meant to disrupt
  - Reflective amplification attacks
  - Vulnerability exploits
- Are DNS concerns included in IoT security discussions?

USING DNS INFORMATION AS THREAT INTELLIGENCE

DNS Observations in Realtime for Timely Action

DNS Observations

- What is observed
  - Cache miss DNS traffic collected ABOVE large recursive resolvers
  - Largely avoids issues with potential PII
- Where this data can be used
  - By analysts, in the SOC, in the NOC, by LEOs and three letter agencies, by brand property specialists, by anti-spam/anti-phishing organizations, etc.



Why Speed Matters

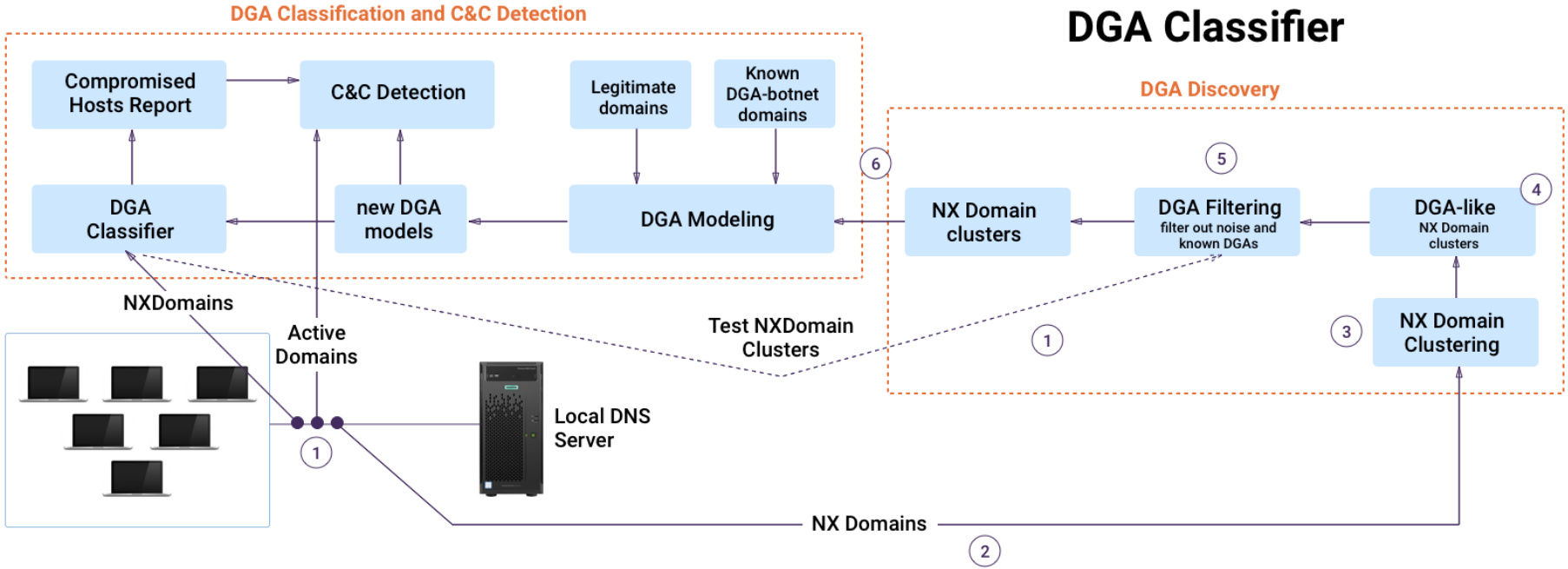
- Criminal infrastructure improvements
  - Scalability
  - Automation
  - Impact
- Need to quickly identify suspicious DNS behavior
  - Authoritative name server changes
  - DNS Errors and NXDOMAIN
  - Newly observed domains (most used for SPAM and Phishing scams)
- What can be detected and act as early warning?

DNS Observations As Added Intelligence

- Passive DNS Data
  - Ability to see what's what (if you have clues about where to look)
  - Detecting covert malware channels thru TXT records
- DNS Changes
  - Watch for changes (classic example: substitution of hostile NS's)
- DNS Errors
  - Operational monitoring: why is my nameserver returning SERVFAIL?
- NXDOMAIN
  - Can reveal hostile probes (pre-attack reconnaisance), common typos ripe for brand/typosquatting, intelligence on DGAs, RPZ-redefined names

Pleiades: DGA-Based Botnet Identification

Early Malware Detection Utilizing NXDOMAIN data



Source: M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, and D. Dagon, "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware," 21st USENIX Security Symposium, 2012.

Newly Observed Domains / Hosts

- Newly observed domains and hostnames provide early warning on newly active domains

- NOD: Newly Observed Domains
  - newly observed effective SLDs
  - e.g. *azure-app.cloudapp.net*
  - March 2018 avg: >2 NODs / sec, or **>150K NODs / day**
- NOH: Newly Observed Hosts
  - newly observed FQDNs
  - e.g. *lb5.azure-app.cloudapp.net*
  - March 2018 avg: >150 NOHs / sec, or **>12M NOHs / day**

Newly Observed Domain Name Blocking

- Most new domains (<24 hours) are used for malicious activity
- Most new domains do not yet have any reputation
- NOD as Streams
  - Newly active vs newly observed
- NOD as Feeds
  - RPZ (DNS Firewall)
  - RHSBL (for SPAM Assassin)
- Various Intervals Useful
  - 5m, 10m, 30min, 1hr, 6hr, 12hr, 24hr

IDNs and Look-Alike Domains

Query #2: RRset: www.xn--ytimes-vt7b.com ANY [Adv]

Returned 2 RRsets in 1082 ms at 2018-04-14 06:10:53 — Print | JSON | CSV | Text

#1, first seen: 2018-01-18 09:17:17, last seen: 2018-04-04 00:12:04	count: 17	bailiwick: xn--ytimes-vt7b.com.
www.xn--ytimes-vt7b.com (www.nytimes.com.)	A	216.250.120.114
#2, first seen: 2018-01-18 09:17:17, last seen: 2018-04-03 21:44:15	count: 12	bailiwick: xn--ytimes-vt7b.com.
www.xn--ytimes-vt7b.com. (www.nytimes.com.)	AAAA	2607:f1c0:1000:2038:9abe:6181:8851:e032

Query #7: RRset: www.xn--conbase-ww4c.com ANY [Adv]

Returned 3 RRsets in 1894 ms at 2018-04-14 06:20:27 — Print | JSON | CSV | Text

#1, first seen: 2018-03-09 02:05:37, last seen: 2018-04-13 20:30:58	count: 392	bailiwick: xn--conbase-ww4c.com.
www.xn--conbase-ww4c.com (www.coinbase.com.)	A	104.27.168.12
	A	104.27.169.12
#2, first seen: 2018-03-08 12:57:35, last seen: 2018-03-08 12:57:52	count: 5	bailiwick: xn--conbase-ww4c.com.
www.xn--conbase-ww4c.com. (www.coinbase.com.)	CNAME	xn--conbase-ww4c.com. (coinbase.com.)
#3, first seen: 2018-03-09 02:05:37, last seen: 2018-04-13 20:30:58	count: 95	bailiwick: xn--conbase-ww4c.com.
www.xn--conbase-ww4c.com. (www.coinbase.com.)	AAAA	2400:cb00:2048:1::681b:a80c
	AAAA	2400:cb00:2048:1::681b:a90c

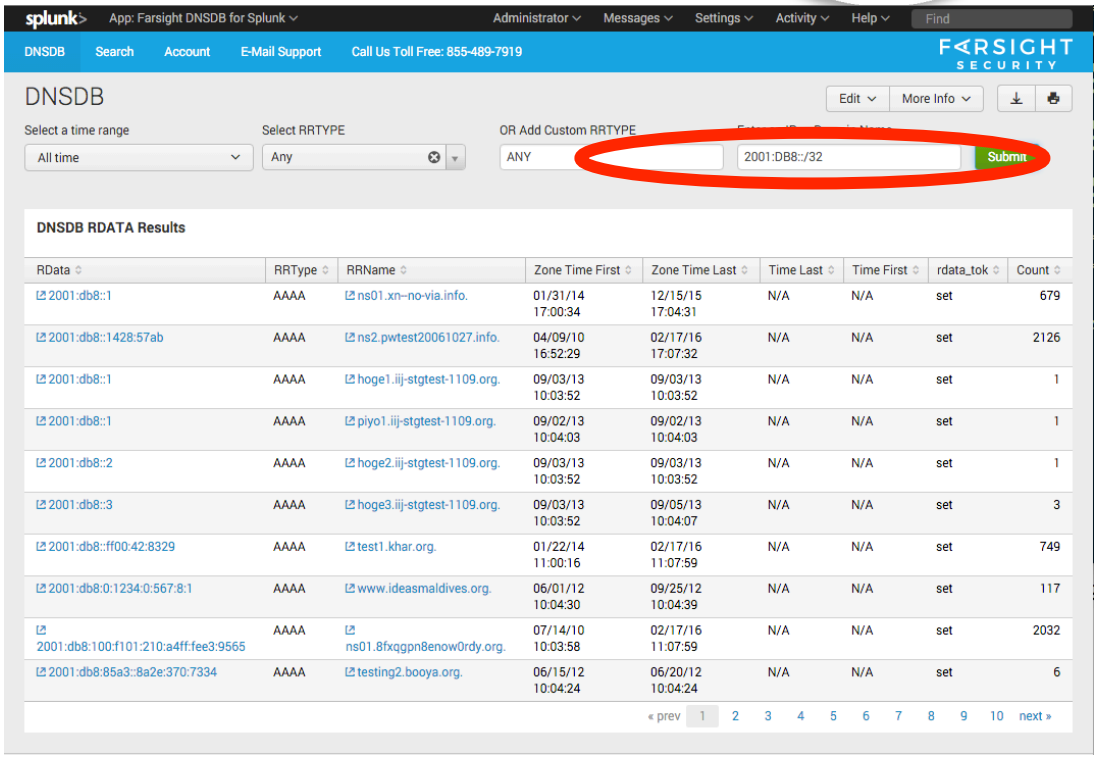
Query #13: RRset: www.xn--yutub-3we2d.ga ANY [Adv]

Returned 2 RRsets in 2697 ms at 2018-04-14 06:28:18 — Print | JSON | CSV | Text

#1, first seen: 2018-03-26 20:51:16, last seen: 2018-04-06 20:30:15	count: 147	bailiwick: xn--yutub-3we2d.ga.
www.xn--yutub-3we2d.ga (www.youtube.ga.)	A	104.24.100.193
	A	104.24.101.193
#2, first seen: 2018-03-26 20:51:17, last seen: 2018-04-11 07:25:34	count: 40	bailiwick: xn--yutub-3we2d.ga.
www.xn--yutub-3we2d.ga. (www.youtube.ga.)	AAAA	2400:cb00:2048:1::6818:64c1
	AAAA	2400:cb00:2048:1::6818:65c1

Integrating pDNS Into Existing Tools

- Why do we see RDATA for 2001:DB8::/32?
- Use existing tools to injest passive DNS information as added threat intelligence
  - Maltego
  - Splunk
  - Anomali
  - DomainTools



Last Thoughts

- Know which domains you use and what can potentially be abused
  - Do pay attention to security practices of registries and registrars
  - Investigate how prevalent IDN registrations are for your brands
  - Collaboration needed between legal, operational and security teams
- Utilize mechanisms to determine changes in DNS traffic patterns
  - Use real time feeds for faster action
  - Use historical information for detailed investigations
- Utilize mechanisms to block unknown malicious domains