Infoblox
CONTROL YOUR NETWORK

Current security trends impacting registrants and end users

Webinar of the new At-Large Capacity Building Program – October 2016

Agenda

- Malicious uses of the DNS to attack you, your networks, your people
- Where is the abuse showing up in the DNS ecosystem
- Some thoughts on dealing with these issues
- Q&A

Presenter – Rod Rasmussen

VP, Cybersecurity, Infoblox

IID founder, CTO

Co-chair Anti-Phishing Working Group’s Internet Policy Committee

Member of:

ICANN's Security and Stability Advisory Committee

Online Trust Alliance’s Steering Committee

FCC Communications Security, Reliability and Interoperability Council

Messaging Malware Mobile Anti-Abuse Working Group

Forum of Incident Response and Security Teams (FIRST Representative)

DNS-OARC

“Collaboration is the key to defeating online crime and creating a trusted, secure Internet."

DNS in the Focus of Attacks

- Attacks on the DNS infrastructure itself
  - Leveraging victims’ use of the DNS against them
- DNS as infrastructure for attacks
  - Malicious actors using DNS just like ”the good guys” to support attacks
- DNS as an attack vector
  - Using the DNS in unintended ways to attack victims

- Why: Targets and Motivations

Attacks on DNS Services and Operations

- Goal is to take your DNS infrastructure offline or corrupting operations
- Flooding/DDoS
  - Your DNS is the target
  - Reflective amplification using your infrastructure
    - Open recursive to large records
- Hijacking/Spoofing
- Vulnerability exploits
- Reconnaissance
  - Infrastructure
  - Spam enablement
  - Spear phishing

DNS Enables Delivery of Content & Services

- From annoying to unwanted to malicious
  - Unwanted offers & solicitations
  - Spamming, scams, gray market, jurisdictionally restricted activities
  - Criminal activities – phishing, malware, malvertising, data theft
  - State actors' malicious activities
- The same reasons everyone uses DNS in the first place
  - Consistent location naming
  - Names convey meaning
  - Resiliency in infrastructure

Various Spams/Scams/Unwanted Content

- Majority of “dodgy” domain registrations related to large-scale spamming
  - Enable e-mail, search engine results, evasion
- Services rely on “reputation” of domains and other infrastructure to make delivery decisions
  - Spam filtering, rankings, forwarding
- Schemes to circumvent local laws (e.g. pharma, gambling, pornography, restricted goods) typically use non-local infrastructure and providers to avoid easy shut-down.
  - An old problem, but down to a science now.
  - Shows conflict between a global resource (DNS) with extra-territorial provisioning and local laws

Malware Exploiting DNS

- Over 91% percent malware uses DNS
  - To gain command and control
  - To exfiltrate data
  - To redirect traffic
- Despite adversaries' reliance on DNS, few organizations are monitoring DNS
- Advanced attacks and data breaches persist and impact all sizes and types of organizations
- Average total cost of data breach ~$3.8M USD
- Consumers/users affected
- Difficult to report and mitigate at service providers

Source: Cisco 2016 Annual Security Report

Anthem.

SONY PICTURES

TARGET

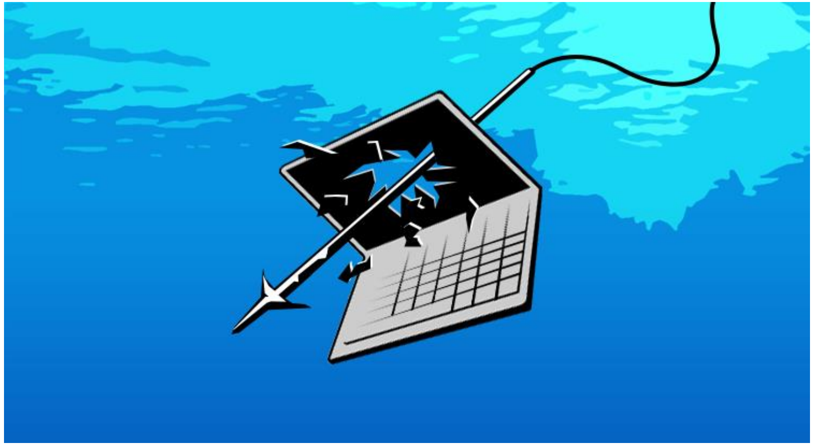
Ransomware Growing Exponentially

- Example of malware that leverages the DNS during all stages of the crime
  - Surveillance and targeting
  - Infection
  - Command and Control
  - Payoff
- Malware encrypts user data and blocks access
- Must pay ransom in Bitcoin or other untraceable method to unlock data
  - Usually will actually give you key, but not always
  - Targeting SMB’s and professionals who have high-value data
- FBI: Ransomware expected to be over $1 Billion crime in 2016
- Up from under $100 million in 2015
- Surveys show lack of awareness of the crime by most people, including employees of enterprises

Phishing Still Popular and Evolving

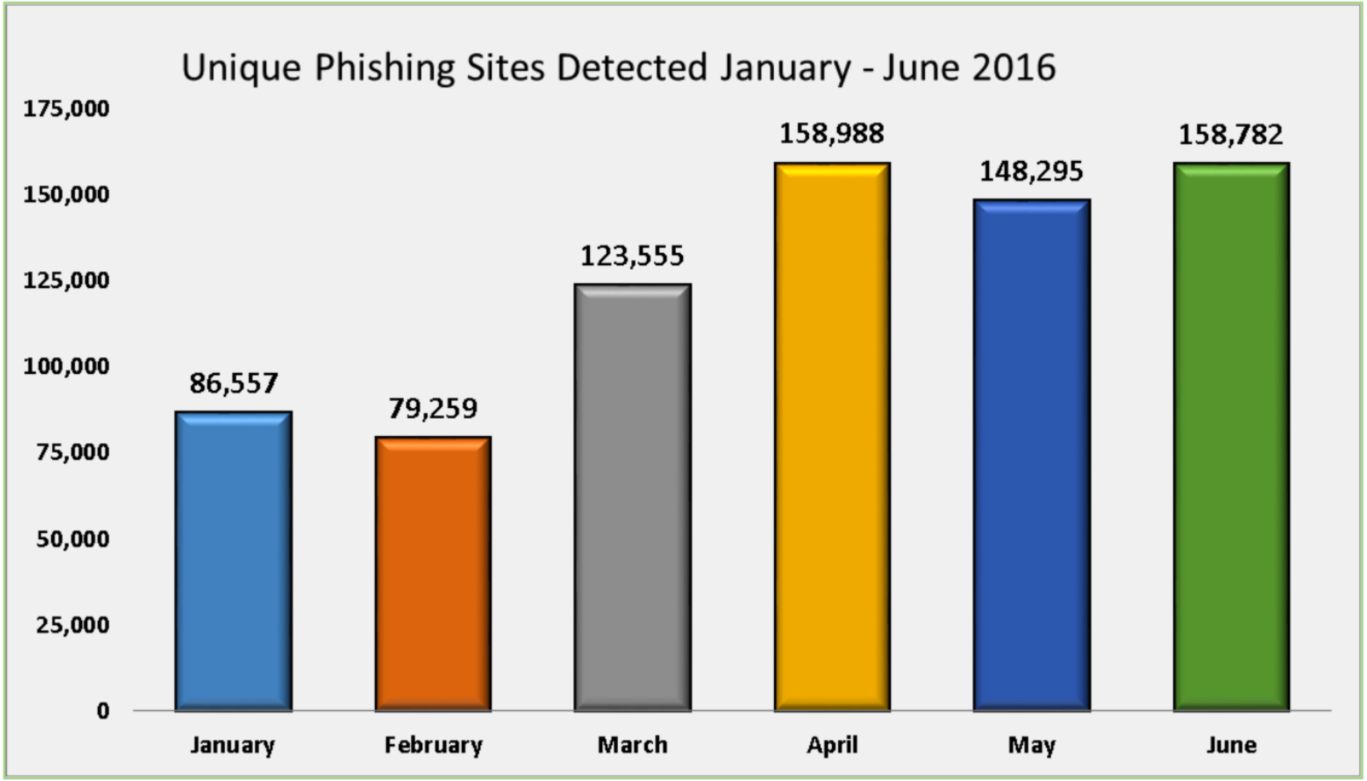
- 2,000– 5,000 sites detected daily
- Shift away from financial services towards retail, online services and other consumer-oriented businesses
- Access credentials to online services much more the target than credit cards
- 2015 Ponemon study results for US targets:
  - Cost to contain malware: $208,174
  - Cost of malware not contained: $338,098
  - Productivity losses from phishing: $1,819,923
  - Cost to contain credential compromises: $381,920
  - Cost of credential compromises not contained: $1,020,705
  - Total extrapolated cost: $3,768,820

Spear Phishing Taking a Huge Toll



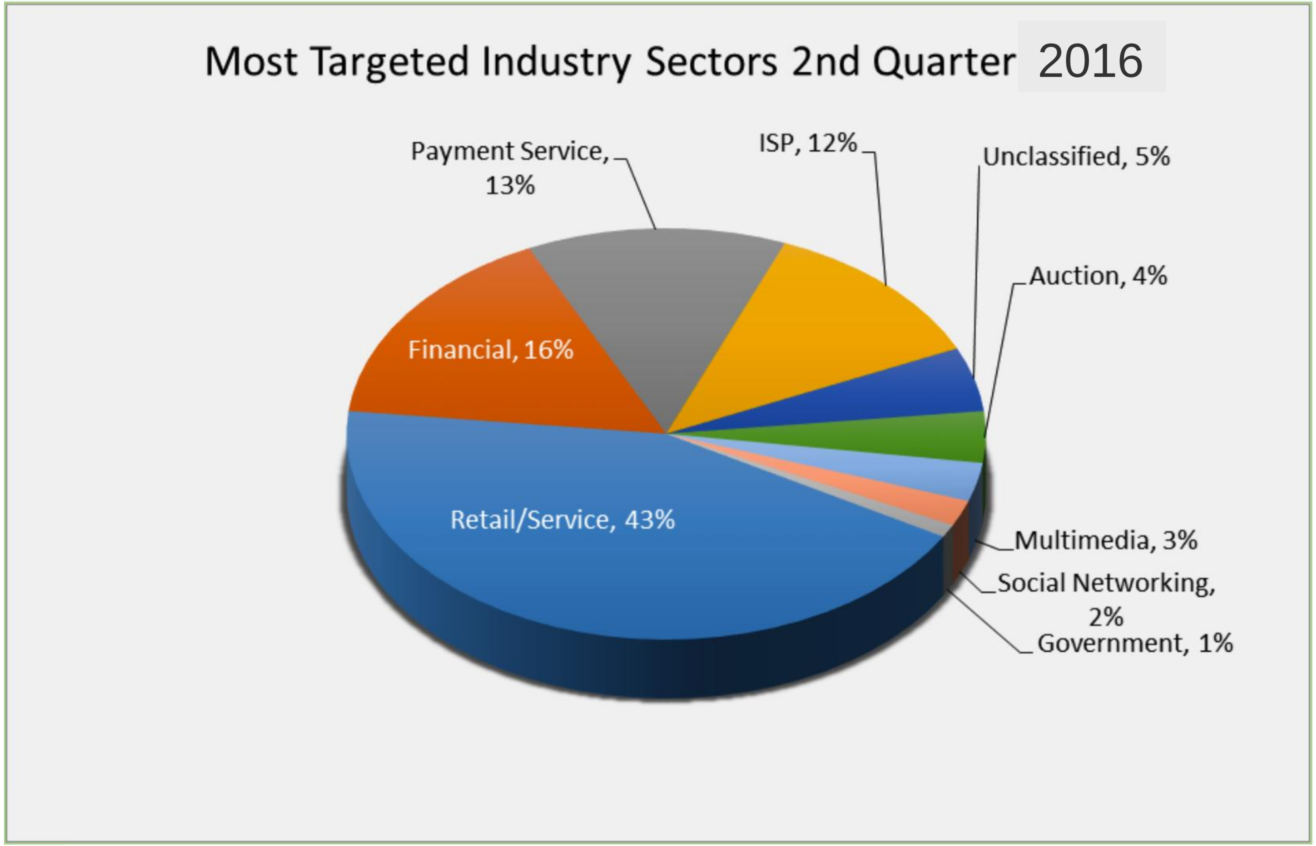
- FBI: $1.2B Lost to Business Email Scams (8/2015)
- FBI: $2.3 Billion Lost to CEO Email Scams (8/2016)
- Money transfers sent directly by victims
- CFO or controller victim of CEO or other impersonation
- Businesses usually not protected against losses
- Major impact including bankruptcies
- Easy to spoof domains for sending e-mail
  - Lack of email authentication in-place
  - Look-alike domains effective
- Easy to perform reconnaissance

Phishing on the Rise in 2016



Source: APWG 2Q 2016 Phishing Trends Report

Phishing Targets 2Q 2016



Source: APWG 2Q 2016 Phishing Trends Report

DNS Rarely Monitored and Usually Available

- Lights-on service – must work in order to use Internet
- Not seen as a traditional threat vector – it is a naming/location services protocol, isn’t supposed to carry data
- Tools for spotting suspicious activities on organizations’ networks usually not tuned for DNS
- Tools aren’t assigned to monitor actual DNS request/response data to look for transport/tunneling activities

DNS and Data Exfiltration

DNS tunneling attacks let infected endpoints or malicious insiders exfiltrate data.

Attackers have recently used DNS tunneling in cases involving the theft of **millions of accounts.**[1]

46%

of large businesses have experienced DNS exfiltration.[2]

$3.8 M

Average consolidated cost of a data breach[3]

Goal of Malicious Actors

- Hacktivism
- Espionage
- Financial gain

Data Targets

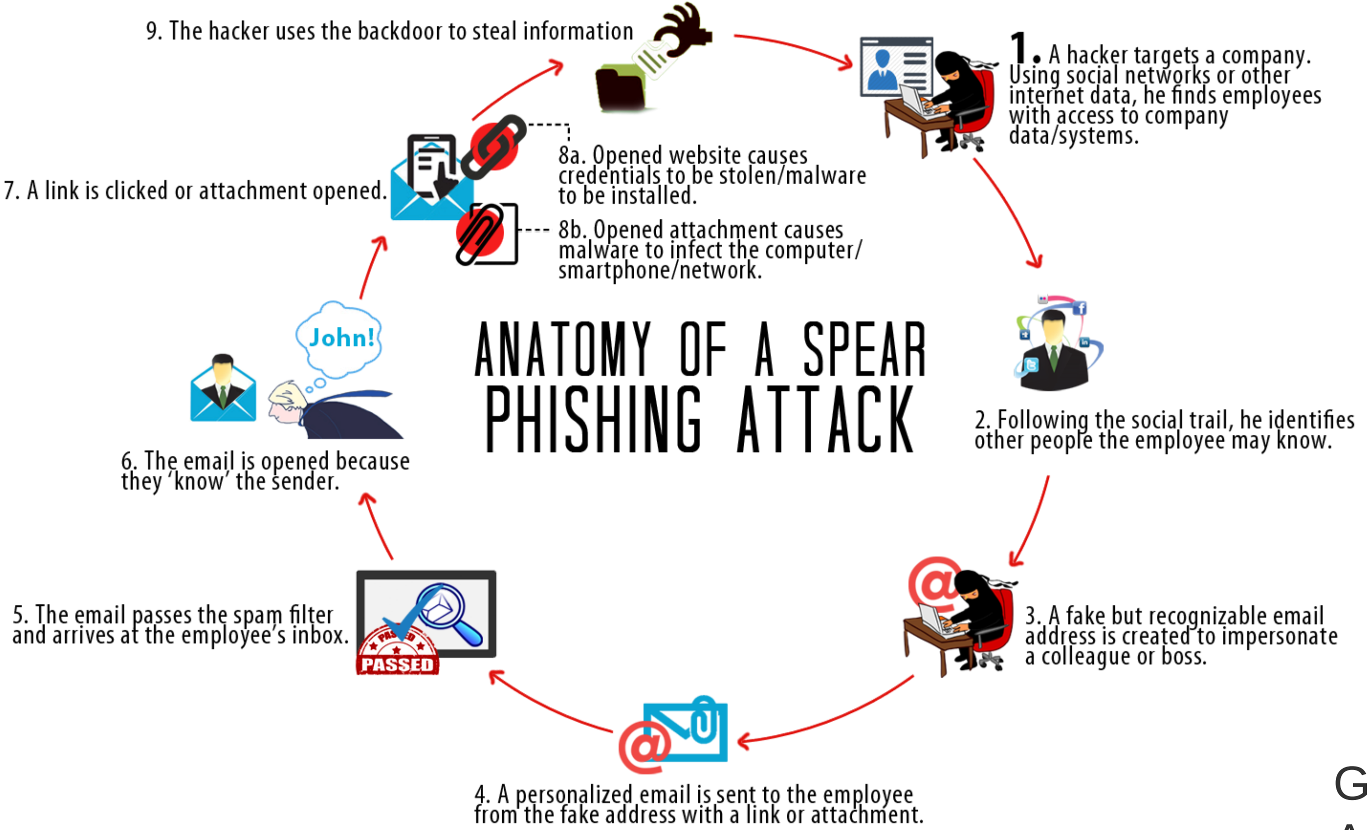
- Regulated data
- PII (personally identifiable information)
- Intellectual property
- Company financials, payroll data

1. *SANS Institute paper referencing Ed Skoudis as speaker at RSA Conference,* June 2012
2. *DNS attacks putting organizations at risk, survey finds, SC Magazine,* December 23, 2014
3. Ponemon Institute, 2015 Cost of Data Breach Study

- How: Techniques of DNS Abuse

Obtaining DNS Resources

- Buy them
  - Stolen payment credentials or accounts
  - Alternate currencies
  - FREE!!!
  - Use a compromised registrar account
  - Dodgy resellers
- Steal them
  - Compromise websites
  - Compromise DNS operator
  - Compromise Registrar account
    - Typically poor password management issues
    - Rare to see direct attacks on registrar infrastructure other than brute-force logins



ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/ smartphone/network.

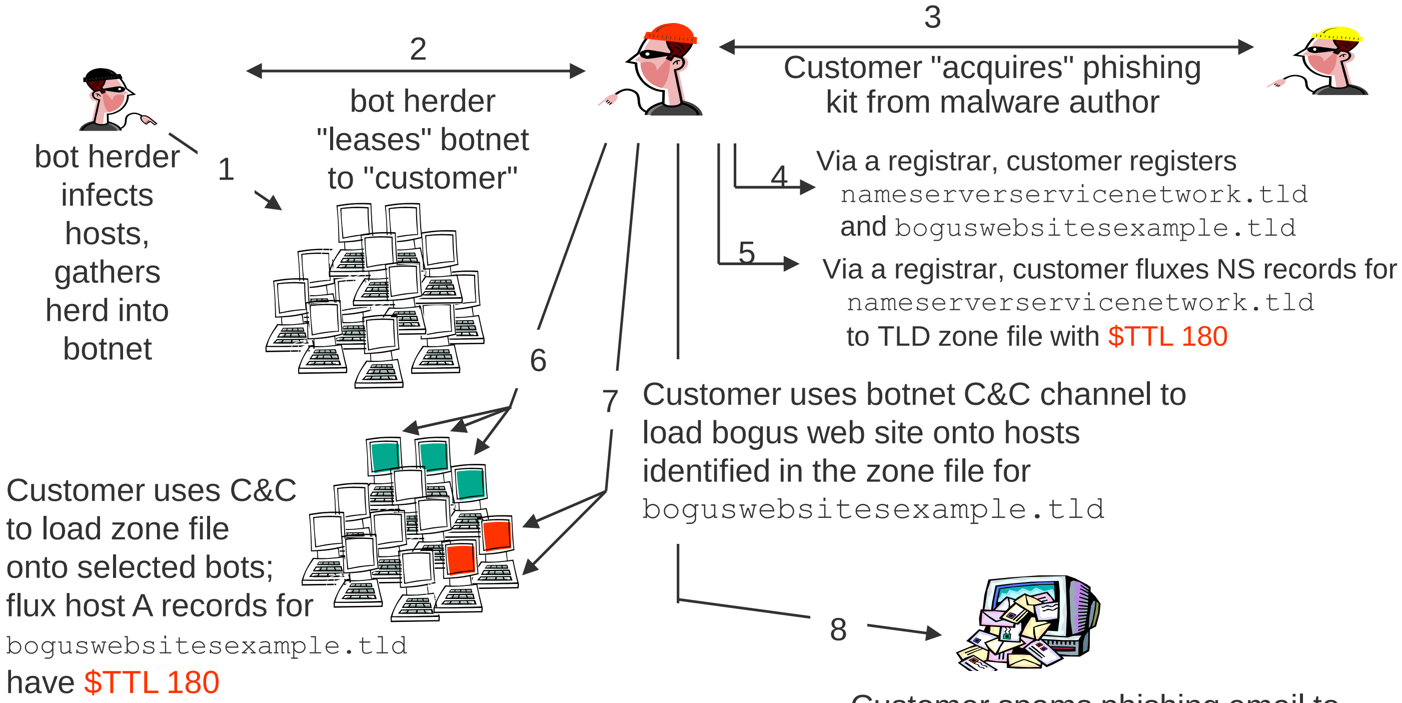
9. The hacker uses the backdoor to steal information

Graphic Credit: AstralD

Fast Flux Variations on a Theme…

- Basic fast flux hosting
  - IP addresses of illegal web sites are fluxed using the authoritative nameserver for the domain
- Name Server (NS) fluxing
  - IP addresses of DNS name servers are fluxed at the registrar
- Double flux
  - IP addresses of web sites *and* name servers are fluxed
- CDN networks use this technique too
  - False positives abound when just looking at basic flux data

Anatomy of a Fast Flux Attack



1 bot herder infects hosts, gathers herd into botnet

2 bot herder "leases" botnet to "customer"

3 Customer "acquires" phishing kit from malware author

4 Via a registrar, customer registers `nameserverservicenetwork.tld` and `boguswebsitesexample.tld`

5 Via a registrar, customer fluxes NS records for `nameserverservicenetwork.tld` to TLD zone file with $TTL 180

6 Customer uses C&C to load zone file onto selected bots; flux host A records for `boguswebsitesexample.tld` have $TTL 180

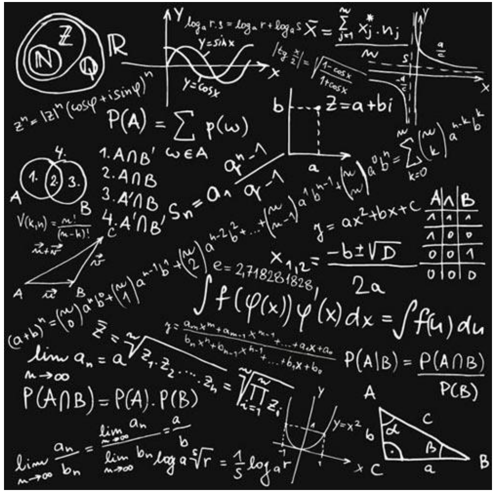
7 Customer uses botnet C&C channel to load bogus web site onto hosts identified in the zone file for `boguswebsitesexample.tld`

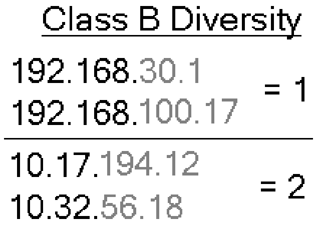
8 Customer spams phishing email to lure victims to bogus web site

STEPS 5-7 repeat as TTLs expire…

A Formula for Fast Flux

- Source: SANS institute
- Time-To-Live (TTL) < 1800 Seconds
- >4 ‘A’ Records (Address code used for storing IP addresses associated with a domain name)
- >4 ‘NS’ Records (Authoritative name server code which specifies a hostname where DNS information may be found)
- >2 Class B Networks in ‘A’ Record Result Set
- >2 Class B Networks in ‘NS’ Record Result Set
- Result Set Changes after TTL + 1 Sec





Class B Diversity

192.168.30.1
192.168.100.17 = 1

10.17.194.12
10.32.56.18 = 2

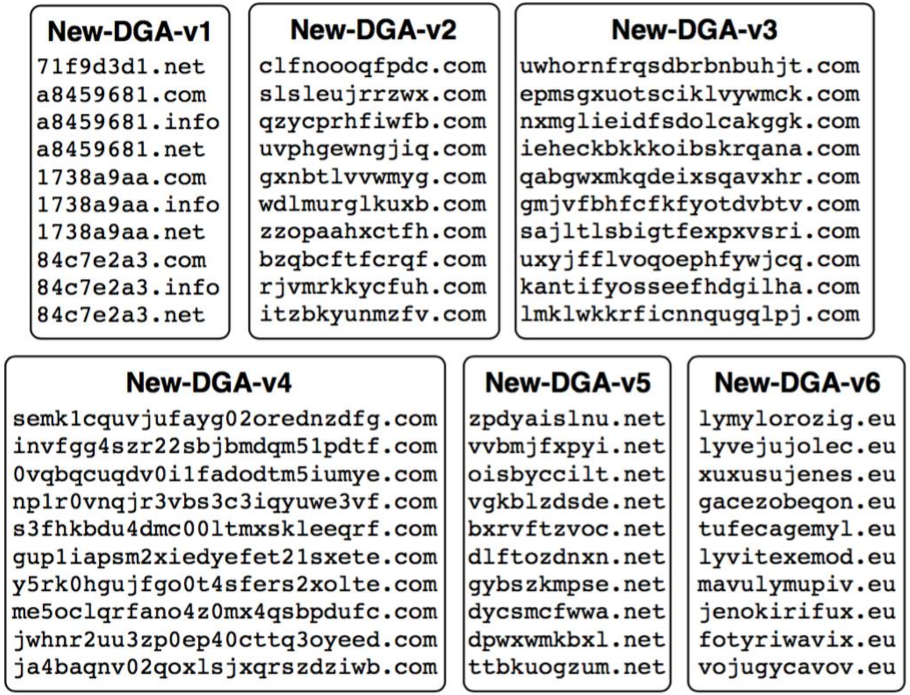
Domain Generation Algorithms (DGAs)

- To avoid losing botnet control due to server take-over, botnet authors often use the DNS for establishing communications
- Since domains can be shut-down, create an algorithm that changes the domain used for comms regularly
- You can generate hundreds or thousands of domains to make it impossible to pre-register them all – just need one to work
- Very noisy though – malware tries to reach many NX-domains every day as algorithm changes.
- Look very “odd” since characters used are generated mathematically and typically end up not being anything like natural language
- If you have the malware, you can reverse it to get the algorithm

DGA History

- Early 2008 – Kraken one of the first malware families to use a DGA
- Mid 2008 – World’s largest botnet “Srizbi” uses DGA algorithm
  - FireEye sinkholes for two weeks to keep out of criminal hands - abandoned
- Late 2008 – Conficker first discovered
  - Sinkhole efforts successful but malware authors escalate to creating over 250,000 potential domains per day in 2009.
- 2010 – Texas A&M University researchers publish paper on detecting DGA domain names
- 2012 – Georgia Tech and Damballa release whitepapers on new DGA use and detection methods using machine learning
- 2015 – DGA tracker websites online

Samples of DGA's from the Past



New-DGA-v1	New-DGA-v2	New-DGA-v3
71f9d3d1.net	clfnoooqfpdc.com	uwhornfrqsdbrbnbuhjt.com
a8459681.com	slsleujrrzwx.com	epmsgxuotsciklvywmck.com
a8459681.info	qzycprhfiwfb.com	nxmglieidfsdolcakggk.com
a8459681.net	uvphgewngjiq.com	ieheckbkkkoibskrqana.com
1738a9aa.com	gxnbtlvvwmyg.com	qabgwxmkqdeixsqavxhr.com
1738a9aa.info	wdlmurglkuxb.com	gmjvfbhfcfkfyotdvbtv.com
1738a9aa.net	zzopaahxctfh.com	sajltlsbigtfexpxvsri.com
84c7e2a3.com	bzqbcftfcrqf.com	uxyjfflvoqoephfywjcq.com
84c7e2a3.info	rjvmrkkycfuh.com	kantifyosseefhdgilha.com
84c7e2a3.net	itzbkyunmzfv.com	lmklwkkrficnnqugqlpj.com

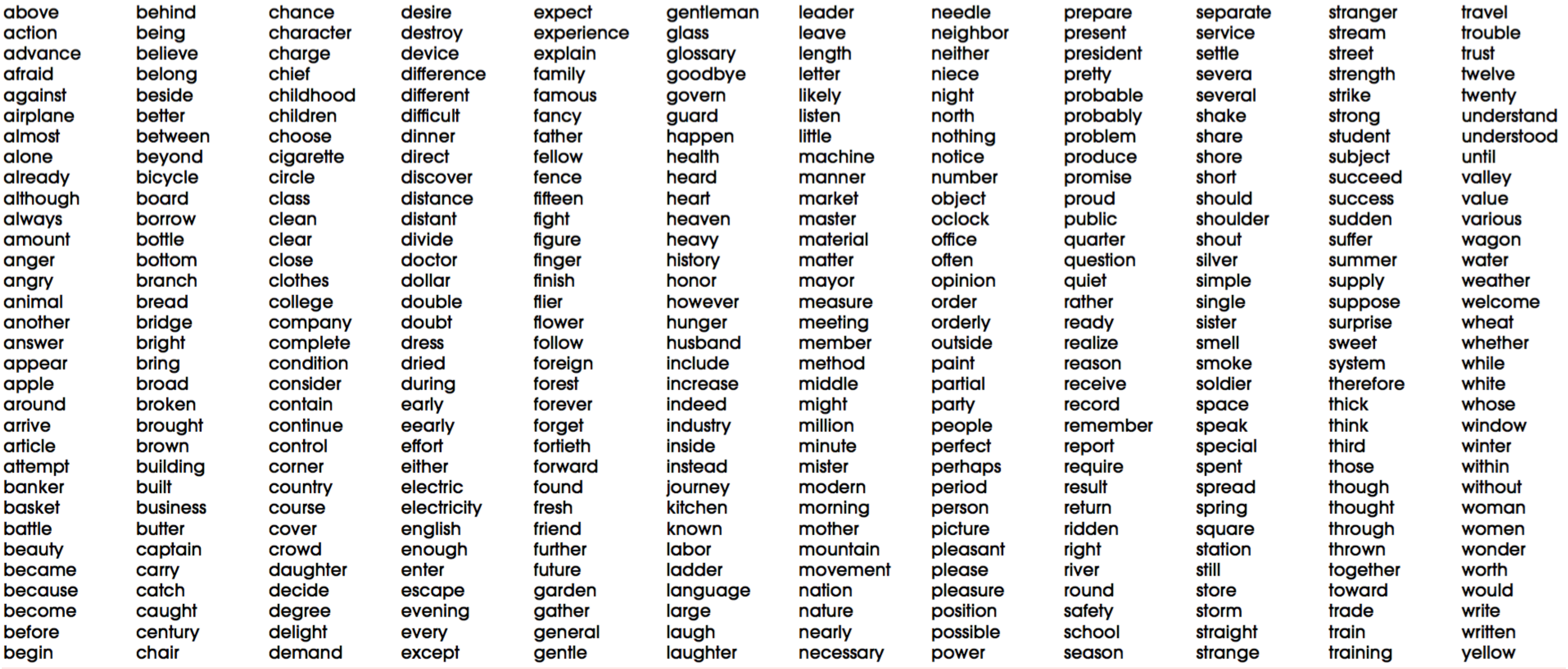
New-DGA-v4	New-DGA-v5	New-DGA-v6
semk1cquvjufayg02orednzdfg.com	zpdyaislnu.net	lymylorozig.eu
invfgg4szr22sbjbmdqm51pdtf.com	vvbmjfxpyi.net	lyvejujolec.eu
0vqbqcuqdv0i1fadodtm5iumye.com	oisbyccilt.net	xuxusujenes.eu
np1r0vnqjr3vbs3c3iqyuwe3vf.com	vgkblzdsde.net	gacezobeqon.eu
s3fhkbdu4dmc00ltmxskleeqrf.com	bxrvftzvoc.net	tufecagemyl.eu
gup1iapsm2xiedyefet21sxete.com	dlftozdnxn.net	lyvitexemod.eu
y5rk0hgujfgo0t4sfers2xolte.com	gybszkmpse.net	mavulymupiv.eu
me5oclqrfano4z0mx4qsbpdufc.com	dycsmcfwwa.net	jenokirifux.eu
jwhnr2uu3zp0ep40cttq3oyeed.com	dpwxwmkbxl.net	fotyriwavix.eu
ja4baqnv02qoxlsjxqrszdziwb.com	ttbkuogzum.net	vojugycavov.eu

Some of them were malware related: New-DGA-v1 was EnviServ.A and New-DGA-v6 was Simba-F, while others were not active any more.

Sophisticated DGA Example

- Recent Crowdstrike analysis of an advanced DGA-based malware (http://bit.ly/1fa2wLb)
- All variants of family contain identical 384-word list of common English words, decrypted at run time
- Domain names created by concatenating two pseudo-randomly selected words and appending ".net" to the end
- Objective: Get around standard machine-learning techniques employed by the security industry
- Bad result for domain holders: collisions with legitimate domains
  - Can lead to unintended DDoS of real websites/domains by bots
  - May have your domain black listed

DGA Dictionary



above
action
advance
afraid
against
airplane
almost
alone
already
although
always
amount
anger
angry
animal
another
answer
appear
apple
around
arrive
article
attempt
banker
basket
battle
beauty
became
because
become
before
begin

behind
being
believe
belong
beside
better
between
beyond
bicycle
board
borrow
bottle
bottom
branch
bread
bridge
bright
bring
broad
broken
brought
brown
building
built
business
butter
captain
carry
catch
caught
century
chair

chance
character
charge
chief
childhood
children
choose
cigarette
circle
class
clean
clear
close
clothes
college
company
complete
condition
consider
contain
continue
control
corner
country
course
cover
crowd
daughter
decide
degree
delight
demand

desire
destroy
device
difference
different
difficult
dinner
direct
discover
distance
distant
divide
doctor
dollar
double
doubt
dress
dried
during
early
eearly
effort
either
electric
electricity
english
enough
enter
escape
evening
every
except

expect
experience
explain
family
famous
fancy
father
fellow
fence
fifteen
fight
figure
finger
finish
flier
flower
follow
foreign
forest
forever
forget
fortieth
forward
found
fresh
friend
further
future
garden
gather
general
gentle

gentleman
glass
glossary
goodbye
govern
guard
happen
health
heard
heart
heaven
heavy
history
honor
however
hunger
husband
include
increase
indeed
industry
inside
instead
journey
kitchen
known
labor
ladder
language
large
laugh
laughter

leader
leave
length
letter
likely
listen
little
machine
manner
market
master
material
matter
mayor
measure
meeting
member
method
middle
might
million
minute
mister
modern
morning
mother
mountain
movement
nation
nature
nearly
necessary

needle
neighbor
neither
niece
night
north
nothing
notice
number
object
oclock
office
often
opinion
order
orderly
outside
paint
partial
party
people
perfect
perhaps
period
person
picture
pleasant
please
pleasure
position
possible
power

prepare
present
president
pretty
probable
probably
problem
produce
promise
proud
public
quarter
question
quiet
rather
ready
realize
reason
receive
record
remember
report
require
result
return
ridden
right
river
round
safety
school
season

separate
service
settle
severa
several
shake
share
shore
short
should
shoulder
shout
silver
simple
single
sister
smell
smoke
soldier
space
speak
special
spent
spread
spring
square
station
still
store
storm
straight
strange

stranger
stream
street
strength
strike
strong
student
subject
succeed
success
sudden
suffer
summer
supply
suppose
surprise
sweet
system
therefore
thick
think
third
those
though
thought
through
thrown
together
toward
trade
train
training

travel
trouble
trust
twelve
twenty
understand
understood
until
valley
value
various
wagon
water
weather
welcome
wheat
whether
while
white
whose
window
winter
within
without
woman
women
wonder
worth
would
write
written
yellow

DGA Detection

- Tried-and-true method: reverse the malware
  - 100% accurate
  - Know what to block/alert on when
  - Can anticipate false positive issues (collisions with legit domains)
  - Requires the malware and reverse-engineering capabilities
  - Data being shared by many security researchers/companies
- Machine learning analysis on large amounts of resolution data
  - Passive DNS replication most popular method
  - Analysis of enterprise DNS resolution can work since you have both sides of the resolution – question (questioner) and answer

Statistical Features used to Find DGA’s

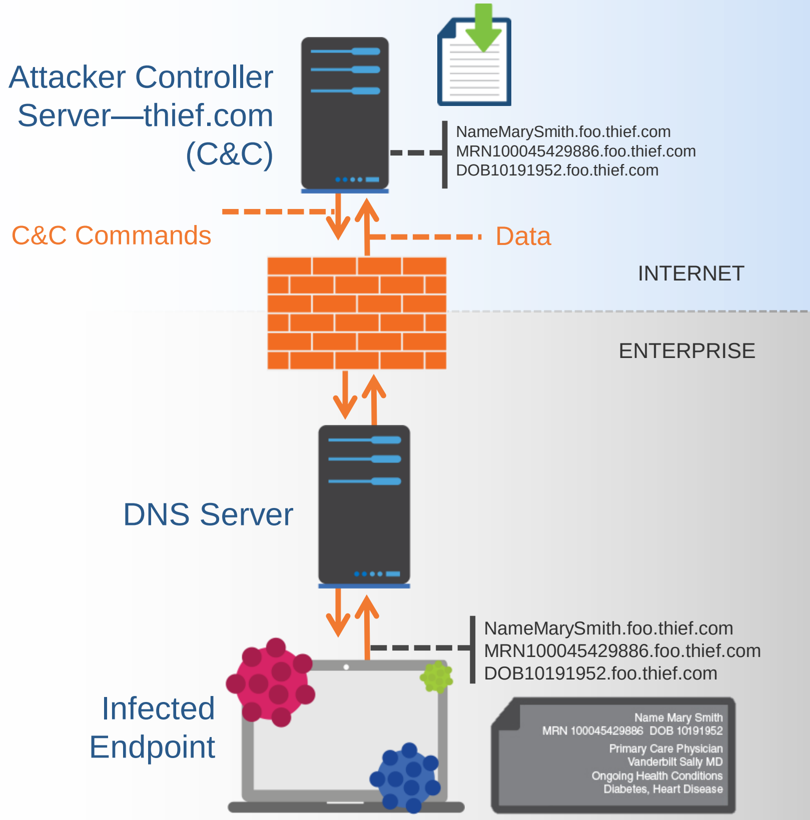
- Group NXDomains per asset with cardinality α
- *n*-gramFeatures
  - Frequency distribution of *n*-grams across domain
- Entropy-based features
  - Entropy of character distribution for separate domain levels, from the domains in the set
- Structural Domain Features
  - Summarizes NXDomains structure
    - Length
    - # of unique TLDs
    - # domain levels

Data Exfiltration over DNS Queries

- Sophisticated attack that anyone can use – built into different types of malware kits (FrameworkPOS, Game over Zeus)
- Infected endpoint gets access to file containing sensitive data
- It encrypts and converts info into encoded format
- Text is broken into chunks and sent via DNS using hostname.subdomain or TXT records
- Exfiltrated data is reconstructed at the other end
- Can use spoofed addresses to avoid detection

Data Exfiltration via host/subdomain
Simplified/unencrypted example:

MarySmith.foo.thief.com
SSN-543112197.foo.thief.com
DOB-04-10-1999.foo.thief.com
MRN100045429886.foo.thief.com



Attacker Controller Server—thief.com (C&C)

NameMarySmith.foo.thief.com
MRN100045429886.foo.thief.com
DOB10191952.foo.thief.com

C&C Commands

Data

INTERNET

ENTERPRISE

DNS Server

Infected Endpoint

NameMarySmith.foo.thief.com
MRN100045429886.foo.thief.com
DOB10191952.foo.thief.com

Name Mary Smith
MRN 100045429886 DOB 10191952
Primary Care Physician
Vanderbilt Sally MD
Ongoing Health Conditions
Diabetes, Heart Disease

Domain Shadowing

- Abuse legitimate domain's good reputation
- Break into registrar or DNS management account
- Insert "evil" hostnames but leave main domain and www alone
- Used primarily for exploit kits (EKs) that probe victim computers for vulnerabilities on their web browser and download malicious payload

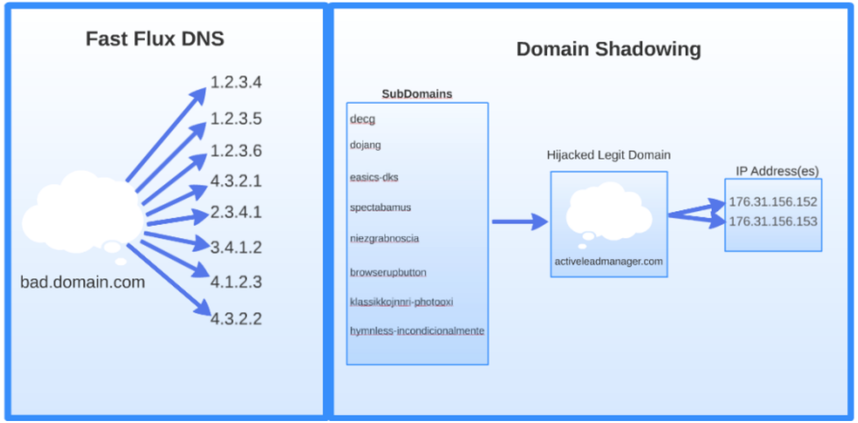
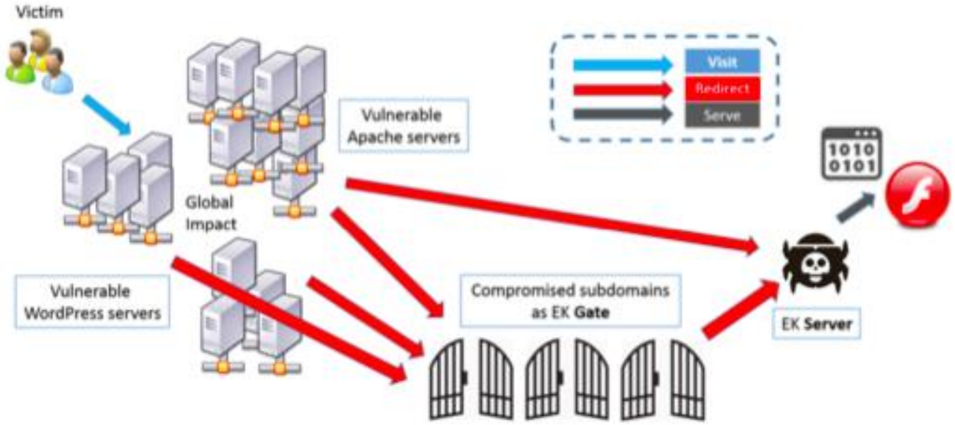


Image Source: Cisco Talos Group



Victim
Vulnerable Apache servers
Global Impact
Vulnerable WordPress servers
Visit
Redirect
Serve
Compromised subdomains as EK Gate
EK Server
1010
0101

Image Source: Unit 42, Palo Alto Networks

Detecting Domain Shadowing

- Look at third level hostnames
  - Will be weird, not “www” or “mail” under the main domain
  - Will point to different, often dodgy, IP space than main website does
- Lots of newly seen hostnames on long-established domains
- Hosted at registrars with known domain shadowing problems
  - Highly automated domain control panels (API’s preferred) to allow management of many domains at once
- Careful to not run into advertising networks, CDN’s or some other legit infrastructure
  - White listing is a fundamental and a core value
- Should block/mitigate the bad hosts, whitelist the “legit” ones

- Where: Tracking Abuse Across the DNS Ecosystem

Spamhaus Top 10 Lists

- https://www.spamhaus.org/statistics/tlds/
- Report relative “badness” by reporting on domains observed acting poorly (spamming, malware, abuse) relative to ”good” domains.
- (Db/Dt)*log(Db)
  - Db = bad domains seen
  - Dt = total domains seen
- Data available for registries and registrars
- Consistent over time until new campaigns come in
- Domains in this data are in active use, showing up in mail feeds and related DNS traffic.
  - Registrars and registries have more “parked” domains – index looks at domains one may actually see in use

October 18: Spamhaus Most Abused TLD’s

TLD	Index	Domains Seen	Bad Domains	% Bad
.science	9.30	41,333	36,582	88.5
.top	7.29	545,391	314,287	57.6
.stream	6.52	10,760	7,823	72.7
.gdn	5.71	19,503	11,879	60.9
.download	5.71	14,196	8,919	62.8
.biz	4.86	87,018	39,914	45.9
.click	3.78	10,691	4,769	44.6
.accountant	3.30	2,861	1,316	46.0
.win	2.83	63,802	18,366	28.8
.link	2.80	25,642	7,996	31.2

October 18: Spamhaus Most Abused Registrars

Registrar	Index	Domains Seen	Bad Domains	% Bad
Alpnames	9.24	209,916	161,725	77.0
Nanjing Imperisosus	8.32	4,118	4,118	100.0
Domainers Choice	6.51	1,928	1,688	87.6
GMO	6.08	249,416	128,829	51.7
Mijn Internetoplossing	4.45	3,041	1,805	59.4
101Domain	4.28	3,299	1,875	56.8
Moniker	2.65	7,845	2,639	33.6
URL Solutions	2.49	1,982	746	37.6
Dotname Korea	2.44	1,274	501	39.3
Netowl	2.43	4,277	1,432	33.5

SURBL – Current Most Abused TLD’s

SURBL: a collection of URI DNSBL lists of hostnames, typically web site domains, that appear in unsolicited messages

TLD	Domains	TLD	Domains
486,894	com	26153	link
277,654	top	24840	us
163,008	net	22599	click
10,1017	biz	19933	download
78,355	org	18883	xyz
64,877	info	15878	trade
55,766	win	15310	bid
5,4723	gdn	14103	science
51255	racing	12383	pw
38567	ru	11193	accountant

http://www.surbl.org/tld

SURBL Observations

- .top a consistent problem over time
- TLD programs matter
  - .info has low abuse overall despite low price promo (free at 1+1)
  - .xyz also free at 1+1 but has high abuse rate
- Price can matter
  - Problems with .work disappeared after price at GoDaddy went from $0.50 to $3.99
  - No abuse on high priced domains like .xxx and .porn despite natural fit for some sorts of abuse for those TLDs

APWG Global Phishing Survey 2015

- Results from unpublished research
- Rod Rasmussen & Greg Aaron researchers
- APWG phishing data for 2015
- APAC (Anti-Phishing Association of China) phishing data for 2015
- Tracks phishing only – other abuse has different patterns

2015 GPS Top-Line Totals

- Total “Attacks”: 227,445
- Total Domains used for phishing: 160,296
- Total Malicious domains used for phishing: 50,563 (32%)
- Total TLD’s used for phishing: 355
- Total TLD’s with malicious registrations: 135
- Total new gTLD’s used for phishing: 119
- Total new gTLD’s with maliciuos registrations: 64

2015 GPS Interesting Observations

- Domain shadowing at-scale
- Malicious registrations increasing
  - Over 30% from around 20% in past
- Some new gTLDs quite problematic
- Abuse following domain price
- Increasing use of URL shorteners
- Abuse clustering among some operators of new gTLDs

2015 GPS Key Statistics

	2015	2014	2013	2012
Phishing domain names	**160,296**	183,222	135,848	153,952
Attacks	**227,445**	247,713	188,323	216,938
TLDs used	**355**	272	210	207
IP-based phish (unique IPs)	**2,807**	5,412	2,463	3,845
Maliciously registered domains	**50,563**	49,932	35,004	13,545
IDNs	275	215	160	205

2015 GPS Highest Attacks Scores

TLD	TLD Location	# Unique Phishing Attacks	Score: Attacks / 10,000 domains
ly	Libya	2,066	232.7
im	Isle of Man (DUM est.)	269	78.9
do	Dominican Republic	194	76.9
by	Belarus	220	71.0
ph	Philippines (DUM est.)	469	70.3
ve	Venezuela (DUM est.)	414	65.7
pk	Pakistan	245	42.6
th	Thailand	251	38.8
cl	Chile	1,667	33.2
cf	Central African Republic	933	28.7
am	Armenia	78	27.9
ng	Nigeria	106	26.8
ge	Georgia (DUM est.)	69	25.8
gq	Equatorial Guinea	444	25.4
id	Indonesia	436	25.2

Minimum 25 attacks,
25K DUM
com = 10.1, avg. 7.3

2015 GPS Highest Phish Domains Scores

TLD	TLD Location	Unique Domain Names used for phishing 2015	Score: Phishing domains per 10,000 domains 2015
ve	Venezuela (DUM est.)	385	61.1
by	Belarus	158	51.0
pk	Pakistan	170	29.5
th	Thailand	184	28.4
cf	Central African Republic	802	24.7
gq	Equatorial Guinea	379	21.7
cl	Chile	1,086	21.6
ge	Georgia (DUM est.)	54	20.2
ng	Nigeria	77	19.5
ml	Mali	351	18.0
ma	Morocco	106	17.8
ga	Gabon	502	17.4
pe	Peru	156	16.8
do	Dominican Republic	42	16.7
ph	Philippines (DUM est.)	107	16.0

Minimum 25 attacks,
25K DUM
com = 7.4, avg. 5.2

2015 GPS Highest Malicious Domains

TLD	TLD Location	# Total Malicious Domains Registered 2015	Malicious registrations score/10,000 domains in registry
ve	Venezuela (DUM est.)	274	43.5
cf	Central African Republic	797	24.5
gq	Equatorial Guinea	378	21.6
ga	Gabon	467	16.2
ml	Mali	314	16.1
cc	Cocos (Keeling) Islands	3,069	12.0
pw	Palau	933	9.1
party	new gTLD	144	6.6
science	new gTLD	212	6.3
top	new gTLD	505	5.2
asia	generic TLD	79	3.3
date	new gTLD	30	2.7
com	generic TLD	34,782	2.7
win	new gTLD	130	2.3
link	new gTLD	38	2.1

Minimum 25 attacks,
25K DUM
com = 2.5, avg. 0.1

Abusive Domain Registration Observations

- Low/no cost domains are most abused
  - Bad guys’ resources limited too – stolen or not
  - Changes in abusive registrations follow domain price promotions (registrar and registry)
- Active anti-abuse programs make a difference but not a guarantee of a registrar or registry to have low/no abuse
- Continue to have issues with registrars in Asia
- Abusive resellers (potential vetting issues) a primary abuse driver
- Some new gTLDs doing very well, others struggling mightily
  - Some correlation of back-end operators with struggling TLDs

Protecting Yourself

- Lock down your domains with your registrar and DNS provider
- Use e-mail authentication in your DNS
- Implement DNSSEC if you have a business
- Use technology and services to protect you from abusive domains
  - Networks/businesses
    - Adequate security on network (look into a DNS Firewall)
    - Anti-spam solutions tuned to abusive domains
    - User education programs including spear phishing
    - Watch for data exfiltration via the DNS from your network
  - Individuals
    - Browser filters/blocker
    - ”Clean” DNS services
    - Personal anti-spam
    - Stop, Think, Connect!

Some Policy Questions to Consider

- Are we tracking, measuring, and reporting abuse consistently?
  - Differences in methods, categories, observations
  - If measuring domain name related abuse, are we parsing things properly? (abusively registered vs. abused)
  - Consistency and transparency on data for contracted parties
- Where are we with protection mechanisms for domain name registrants?
  - See SAC 040 and SAC 044
- What are appropriate measures for serial patterns of large-scale abusive registrations that remain uncorrected over many months or years?
- Are there ways to incent or assist industry participants (including registries and registrars) to share information on abuse patterns?
- Are there ways to foster creation of easier mechanisms for reporting and responding to reports of sophisticated attacks?

Thank You!

Infoblox®