29th ANNUAL FIRST CONFERENCE

SAN JUAN
PUERTO RICO
JUNE 11-16, 2017

FIGHTING PIRATES AND PRIVATEERS

WWW.FIRST.ORG

DNS is NOT Boring!
Using DNS to Expose and Thwart Attacks

Rod Rasmussen

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

DNS is NOT Boring!
Using DNS to Expose and Thwart Attacks

While almost every major organization in the world is being continuously attacked over the Internet from a wide variety of actors, tools, and methods, the vast majority of them are sitting on a gold mine of data that could expose and thwart those attacks and don't even know it. That data is in the very mundane task of resolving names to network addresses otherwise known as Domain Name Service (DNS).

DNS is NOT Boring!
Using DNS to Expose and Thwart Attacks

This session will explore how to dig data out of your organization’s DNS queries and responses, find activities like data exfiltration using DNS tunnels, malware activities, and other attacks leveraging the DNS, and provide some thoughts on how to use the organization’s DNS infrastructure itself to protect from these threats.

Agenda

Frame the issues

Talk about threats and mitigations

Review some real-world incidents

Get down-and-dirty with actual tools and data

Q&A (and requests)

Presenter – Rod Rasmussen

Principle, R2 Cyber

Formerly: 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

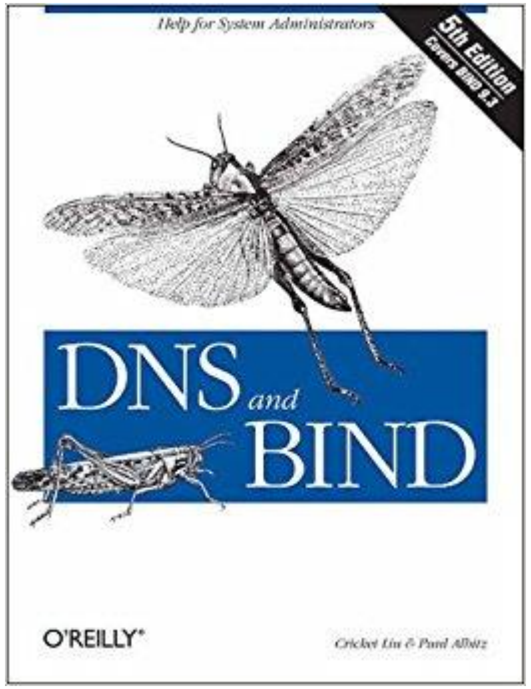
Forum of Incident Response and Security Teams (formerly FIRST Representative)

DNS-OARC

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

Who Knows how to Spell DNS?

If not – Buy this Book!



Help for System Administrators

5th Edition
Covers BIND 9.3

DNS and BIND

O'REILLY®

Cricket Liu & Paul Albitz

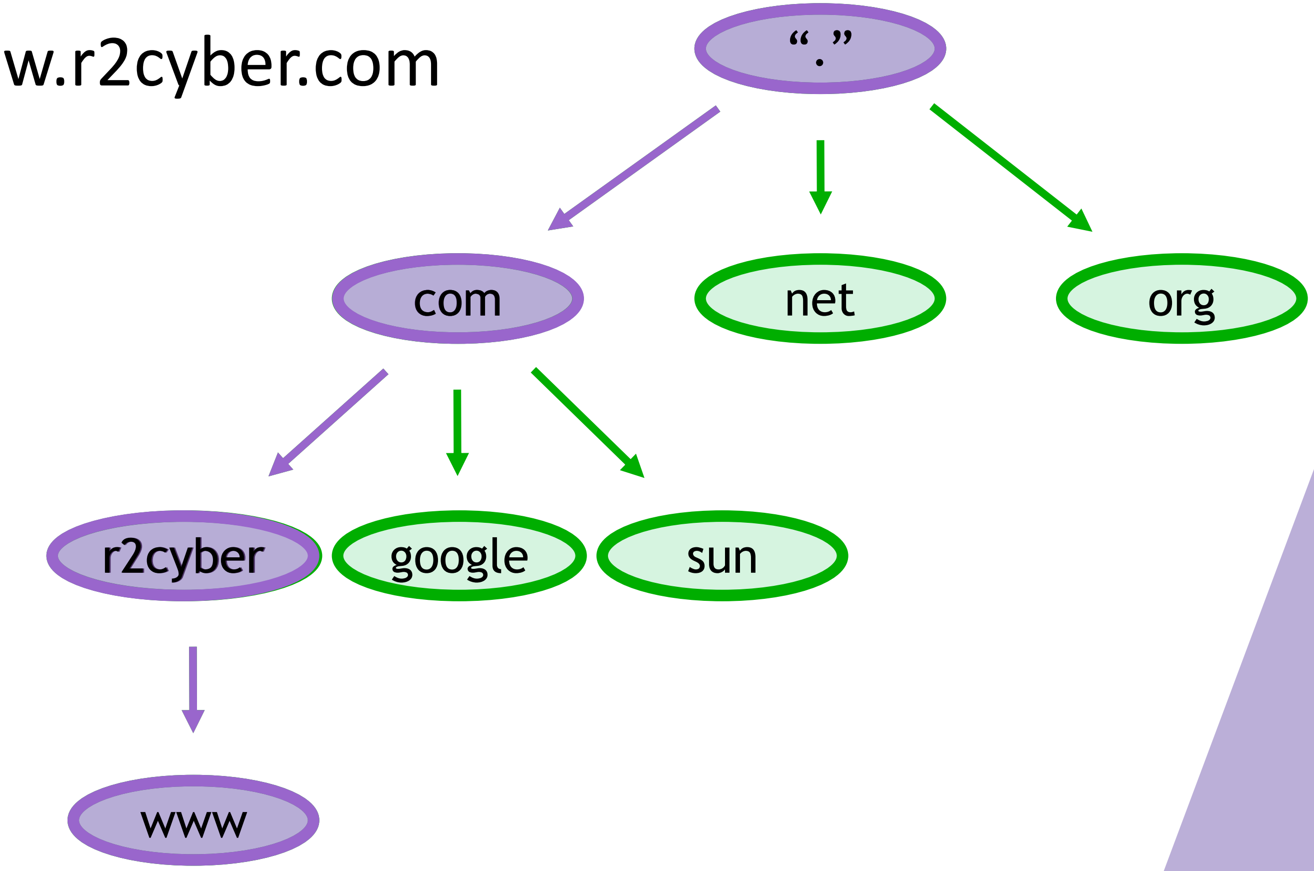
By this guy…

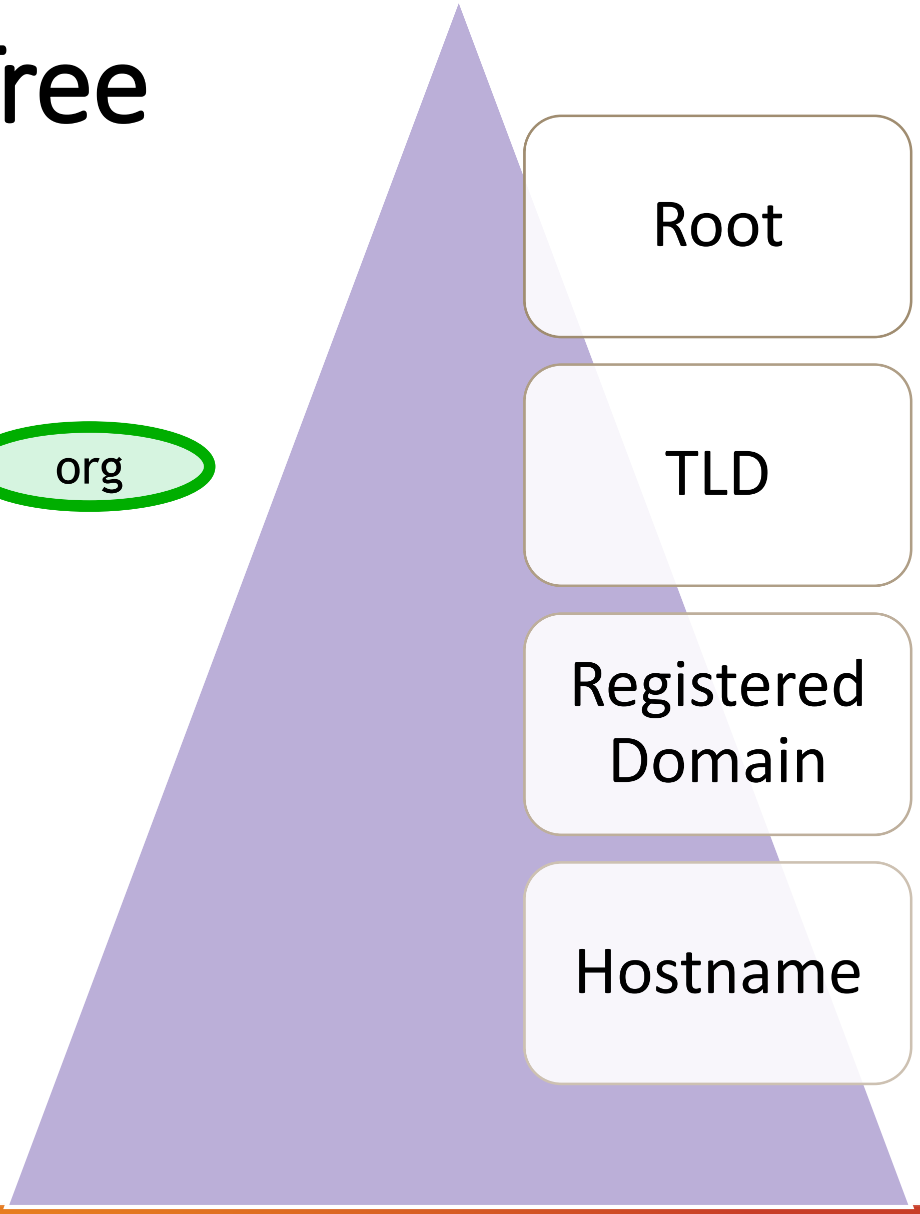
"Response Policy Zones are the first mechanism that lets us turn DNS servers from security targets into security tools.
- Cricket Liu, Chief DNS Architect

Infoblox

DNS Refresher – Directed Tree

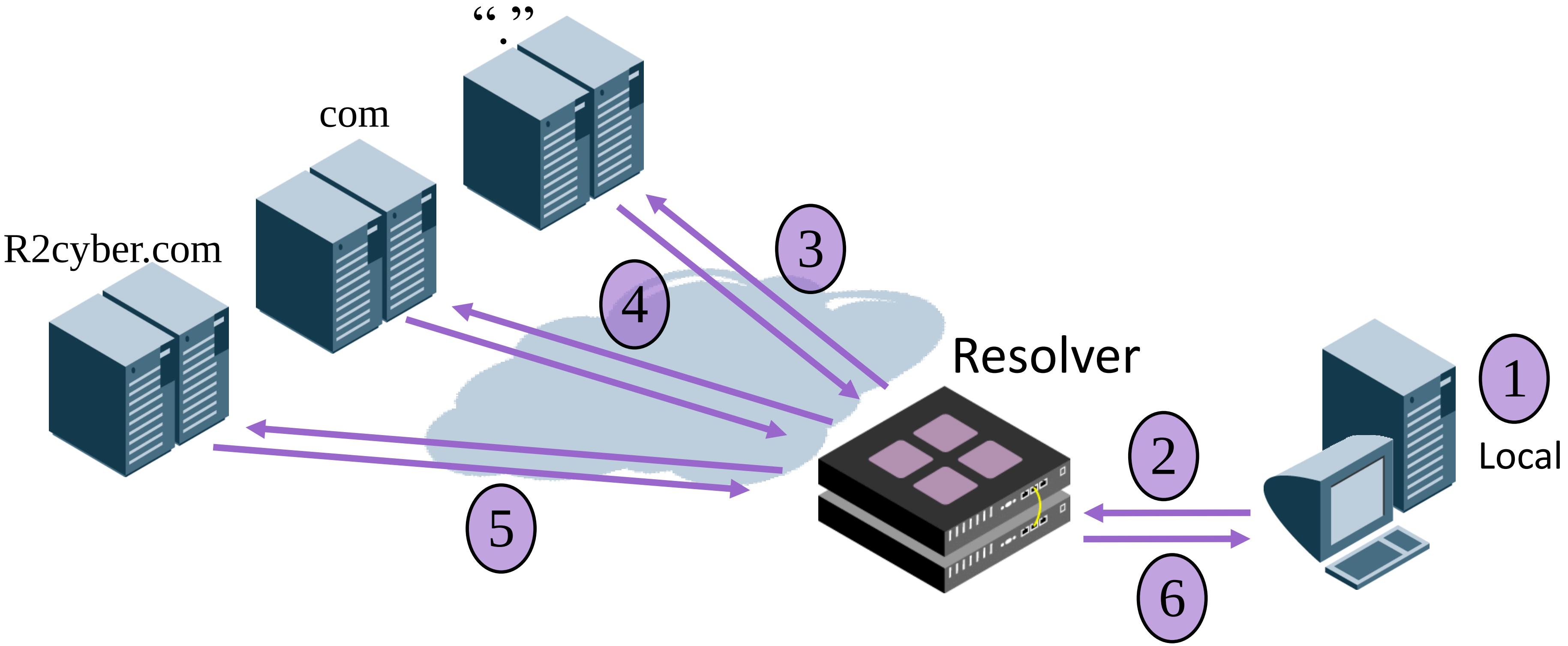
- www.r2cyber.com



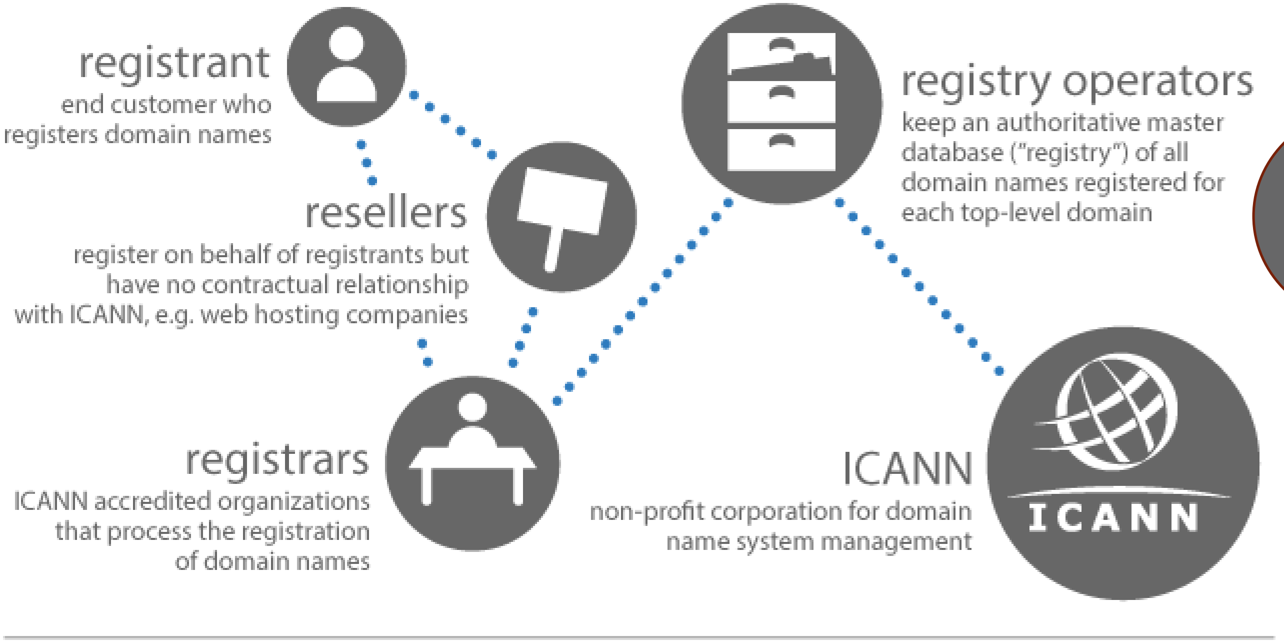


How DNS Resolution Works

- Resolution process
  - Client: “What is the IP address of www.r2cyber.com?”



And Some other Important Players



registrant
end customer who registers domain names

resellers
register on behalf of registrants but have no contractual relationship with ICANN, e.g. web hosting companies

registrars
ICANN accredited organizations that process the registration of domain names

registry operators
keep an authoritative master database ("registry") of all domain names registered for each top-level domain

ICANN
non-profit corporation for domain name system management

domain registry process

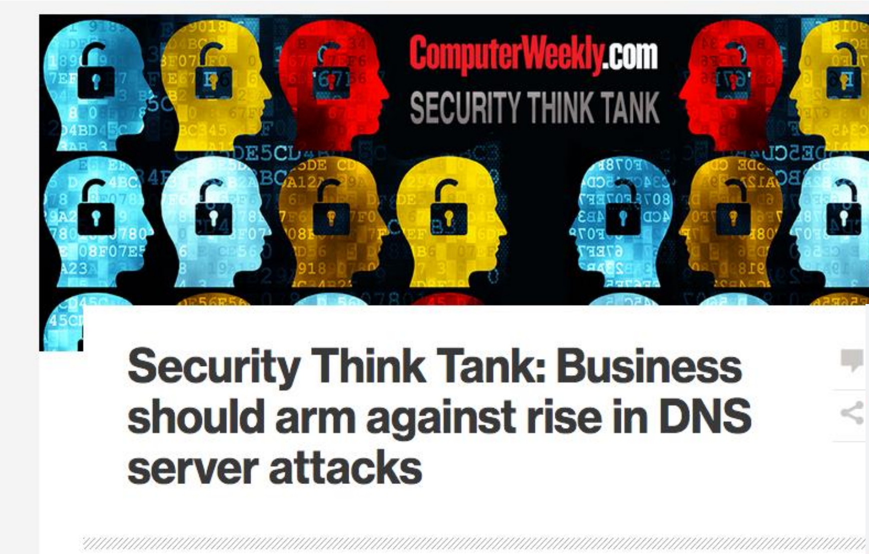
ccTLD Operator

individual country authorities
impose national laws, requirements and other attributes unique to a ccTLD

So No Big Deal, Right?

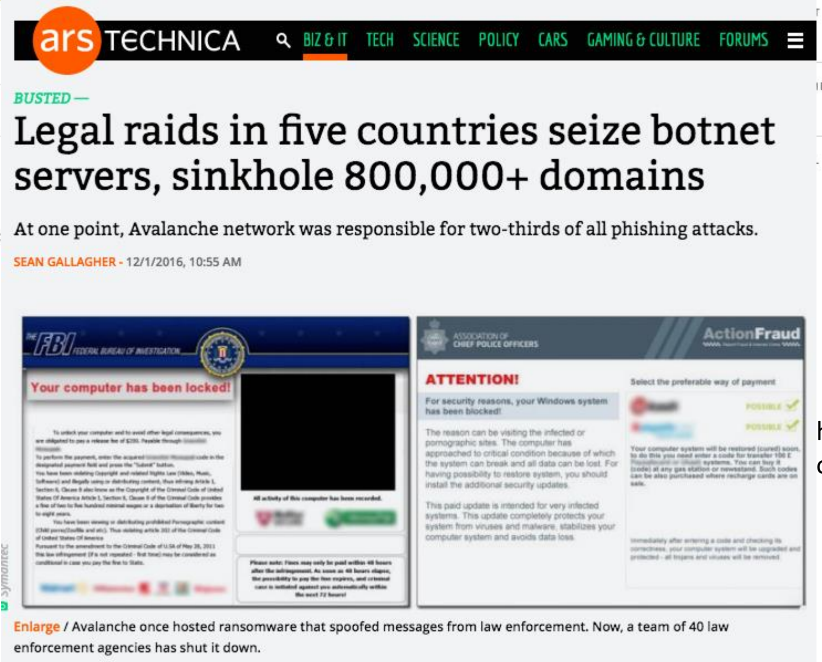
- DNS is a lights-on critical service connectivity service
- History shows it to be extremely resilient
- Been around a long time now
- Looks can be deceiving
  - People tend to take it for granted
  - Not thought of a security control
  - Cost center rather than strategic tool
    - Who’s using Godaddy for their corporate domains?

DNS Attacks of all sorts remain highly impactful



Security Think Tank: Business should arm against rise in DNS server attacks

http://www.computerweekly.com/opinion/Security-Think-Tank-Business-should-arm-against-rise-in-DNS-server-attacks


ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
FORUMS
THE FBI FEDERAL BUREAU OF INVESTIGATION
Your computer has been locked!
ASSOCIATION OF CHIEF POLICE OFFICERS
ActionFraud
ATTENTION!
For security reasons, your Windows system has been blocked!
Select the preferable way of payment
POSSIBLE
POSSIBLE
symantec

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

Enlarge / Avalanche once hosted ransomware that spoofed messages from law enforcement. Now, a team of 40 law enforcement agencies has shut it down.

https://arstechnica.com/security/2016/12/legal-raids-in-five-countries-seize-botnet-servers-sinkhole-800000-domains/

How Hackers Hijacked a Bank's Entire Online Operation

ANDY GREENBERG SECURITY 04.04.17 10:52 AM

HOW HACKERS HIJACKED A BANK'S ENTIRE ONLINE OPERATION

https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/

Large Attack Surface

- Servers, outsourced services, chains of reliance an opportunity for attack
  - Each point of the operational authoritative DNS infrastructure
  - Vulnerabilities in the recursive infrastructure
  - The provisioning and domain management ecosystem
- Little monitoring done by most organizations
  - DNS just works
  - DNS one of very few protocols with largely unimpeded flow between networks
- Few are thinking about Jiu-Jitsu – turning the tables on the attackers
  - If they are coming at you via DNS – you can turn that into intelligence and action

DNS-Related Attacks fall into Three Main Buckets

- Attacks of the DNS infrastructure itself
  - Including leveraging your DNS to attack others
- Use the DNS protocol as it was designed but for malicious purposes
- Exploit "valid" but creative unintended uses of DNS such as DNS tunnels

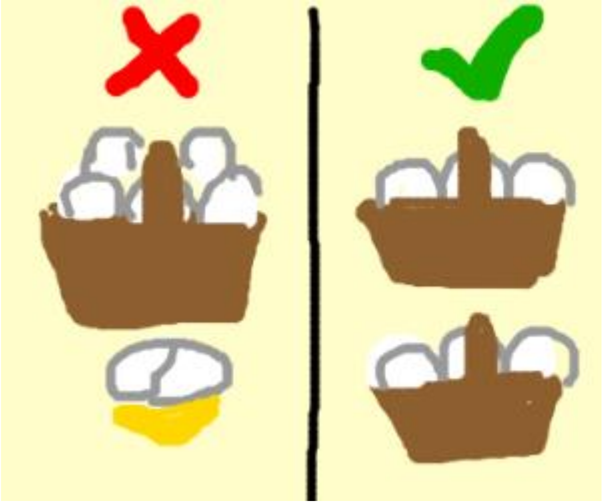
Attacks on DNS Services and Operations

- Goal is to take your DNS infrastructure offline or to impact operations
- Flooding/DDoS
  - Your DNS is the target
  - Reflective amplification using your infrastructure
- Hijacking
- Spoofing
- Vulnerability exploits/reconnaissance

Just a few quick thoughts on these issues

Dyn Attack – Did we all Relearn our Lessons?

- Massive interdependencies on someone else's DNS – could be 2-3 layers of services
- Did your own DNS go dark?
- What happened to diversity?
  - Internal vs. External
  - Multiple providers
  - DYI backups



Who’s your (Go)Daddy?

- Entire bank hijacked this year via hijacking
- What domain registrar are you using?
- What controls do you have in place (locking and change management at various levels)
  - Registries and registrars are outside your control – yet they are critical to your DNS infrastructure
- Domain “shadowing” a big deal these days – hijacking “light”

You ARE Employing anti-Spoofing, Right?

- Spoofing still a major problem
- BCP 38 & 84 as relevant now as ever and a bit easier to do

- Oh, and while I’m at it DNSSEC is getting a lot easier to provision – you should probably do it now if you haven’t already!

Don’t Forget E-mail

- SPF & DKIM work fairly well – solve some basic issues with spoofing of your domains in the e-mail stream
- DMARC actually works pretty darn well
  - Advance notice of campaigns against your customers/employees/constituents
  - Get ahold of IOC’s from bounced messages
  - Telemetry may tell you a lot about nature of those spoofing you for attacks
  - Great for detecting some spear-phishing campaigns
- These all require integration and maintenance in DNS

Bad Guys Use the DNS Too!

- Because they have to – just like us
- Obvious stuff like look-alike domains for phishing and dropping exploits
- Provisioning infrastructure – most botnets are SaaS platforms…
- Resiliency of campaigns - traditional firewalls block IP space
- Easy to stand-up new infrastructure with automation

Phishing via Malicious Domains is “in” Again

- Soon to be released APWG report will show around 40% of phishing attacks involve a fraudulently registered domain name
  - I’ve been crunching the data for weeks now!
  - Numbers way up
- Some domains being aged well over a year
  - Most attacks still on fresh domains, but cannot rely on age anymore
- IDN Homographic attacks still not a major issue
- Lots of data available on what attacks are out there!

Malware Exploiting DNS

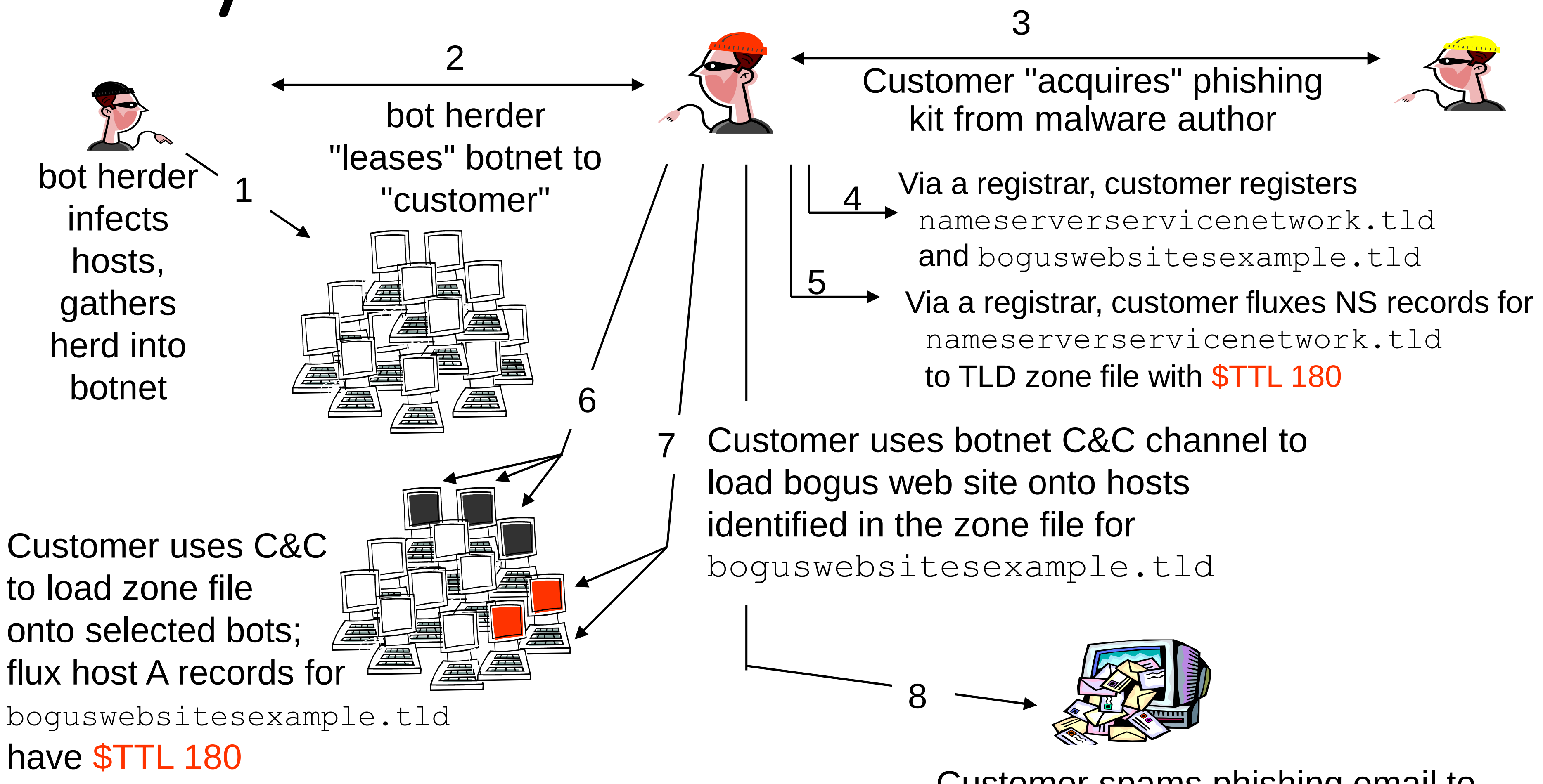
- Over 91% percent malware uses DNS*
  - To maintain command and control
  - To exfiltrate data
  - To redirect traffic
- Nearly all the crypto* stuff uses DNS based C&C
- Blow right through standard firewalls that are busy looking at IP addresses and other traffic
- Provisioning of DNS infrastructure for all sorts of criminal activity is highly automated and specialized

***Source:** Cisco 2016 Annual Security Report

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…

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 communications 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 website online
- 2016 – Registrar of last resort stood-up to sinkhole many DGA’s

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

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

Hiding in Plain Site

- Exfiltration via DNS growing - more botnet C&C via DNS signaling

DNS and Data Breach

- DNS tunnels are commonly used to send sensitive information out

- Data can be exfiltrated by embedding data directly in DNS queries

$7.6 M — Average material loss per breach incident

46% — % of survey respondents who have experienced DNS data exfiltration

45% — % of survey respondents who have experienced DNS tunneling

Source: *SC Magazine*, Dec 2014, “DNS attacks putting organizations at risk, survey finds”

Data Exfiltration Examples

A large developer of video games had malware inside the network that tried to exfiltrate data via DNS queries using spoofed addresses.

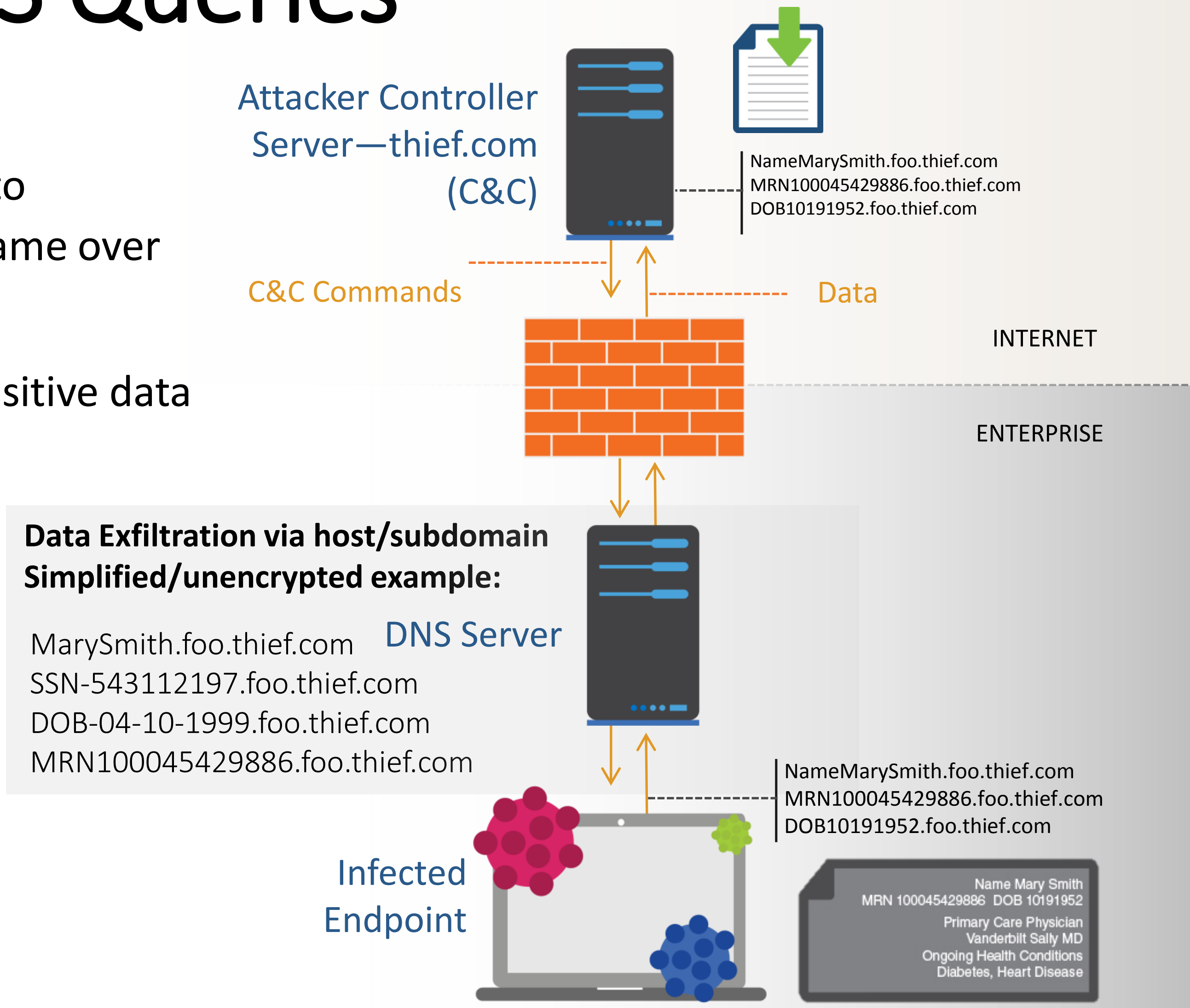
A large automaker's main concern is loss of intellectual property that could erode its competitive advantage, and the company is very keen on preventing it from happening via DNS.

A large bank failed an audit because of lack of protection for data over DNS.

A large insurance company is concerned about liability because it is aware that DNS is not protected.

Data Exfiltration via 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


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

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

Domain Shadowing

a Hybrid Attack

- 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
- Stealing *reputation*

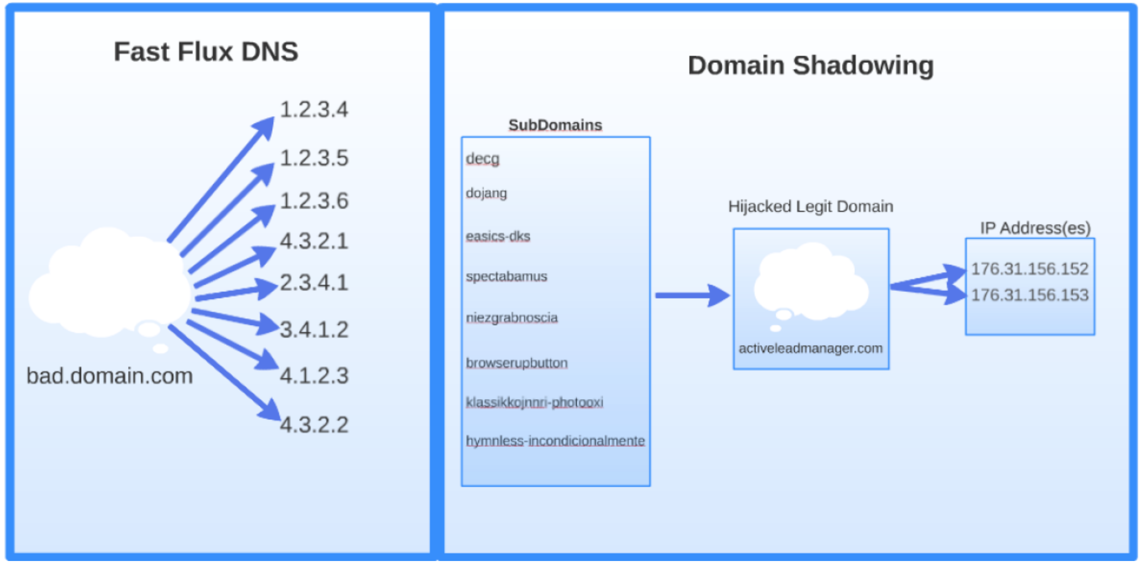


Image Source: Cisco Talos Group

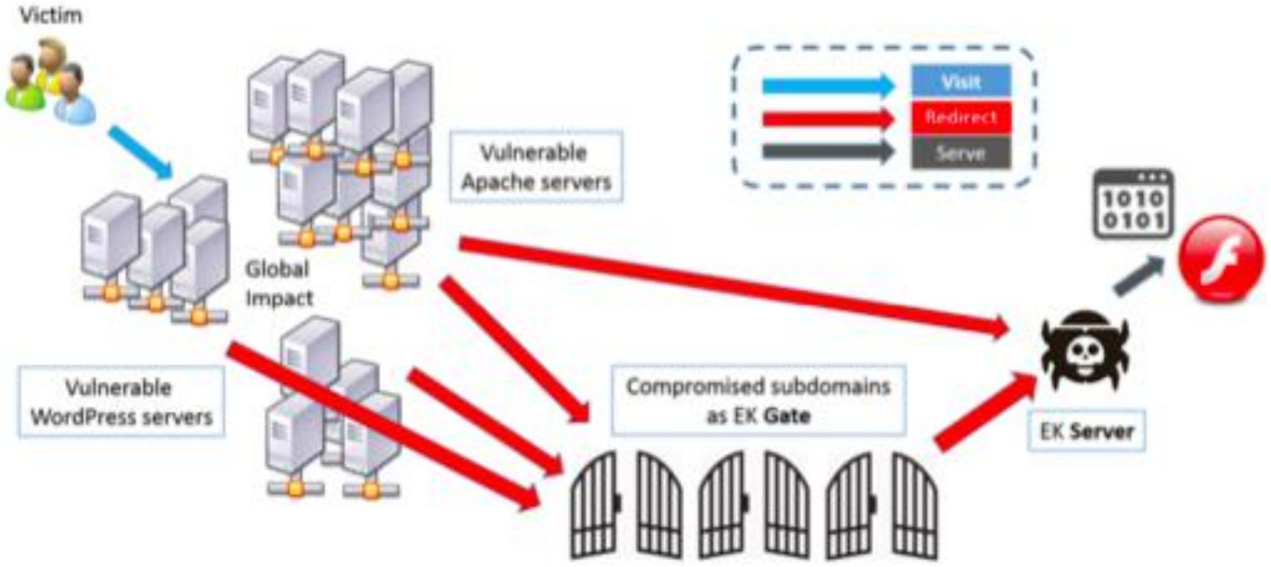

Victim
Global Impact
Vulnerable Apache servers
Vulnerable WordPress servers
Visit
Redirect
Serve
1010
0101
Compromised subdomains as EK Gate
EK Server

Image Source: Unit 42, Palo Alto Networks

OK, That’s Kinda Depressing – What do we do?

Traditional Security Tools ≠ DNS Security

- Traditional security tools often cannot detect attacks via DNS that threaten your enterprise network
    - Traditional firewalls IP-address centric
    - DLP and other breach tools don’t look at DNS for exfil
- DNS resolution is lights-on service – hard to hand off to security product
    - DPI on DNS? Not at scale
- Critical parts of infrastructure outside network and your operational and/or legal control

Instrumenting Your Network

- If you want to stop ”bad things” you have to look for them first!

- DNS logging at the resolver
- Passive DNS replication
- DNS Tap (dnstap.info)
- DPI techniques
- Log data and push into other analysis infrastructure
  - Custom database or analysis tools like ELK stack or Splunk
  - SIEM
  - Cloud to handle scale and allow for machine-learning
  - Build your own Passive DNS (PDNS) database!

DITL Yourself!

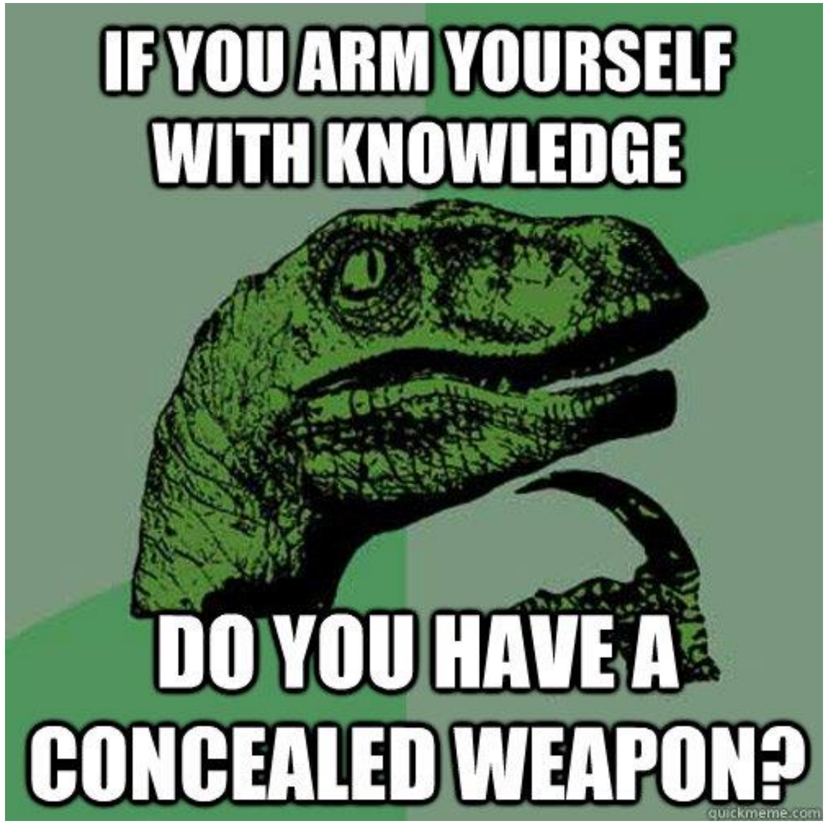
- Day-in-the-life-of-the Internet
- DNS-OARC does this at "Internet Scale" annually
- Baseline your typical day/week/mo.
- You don't know what's "weird" unless you know what's normal
- Keep stuff like PDNS around forever if possible

Lock Down DNS Channels

- Lots of people use different DNS servers than yours
  - Intentionally for “speed”
  - Their “free app” made the change for $$$ purposes
  - Off-network
  - Bad guy actions (remember DNS Changer?)
- You can use your network infrastructure to help
  - Redirect Port 53
  - Monitor for those hitting dodgy resolvers
  - Tricks available to determine if your users are circumventing your DNS
    - Cookies and/or embedded URLs with unique, tracked hostnames are your friend!

Arm Yourself with Knowledge

- Know what to look for, how severe it is, so you can react appropriately
- Lots of data on DNS reputation available
  - Open source
  - Commercial feeds
  - Sharing communities
- Can get data bundled in various solutions
- Mine your own data
  - Know what "normal" is
  - Look for suspicious activities
  - Know what is hitting "just you"!!!
- Pivot off known attack infrastructure to find more


IF YOU ARM YOURSELF WITH KNOWLEDGE
DO YOU HAVE A CONCEALED WEAPON?
quickmeme.com

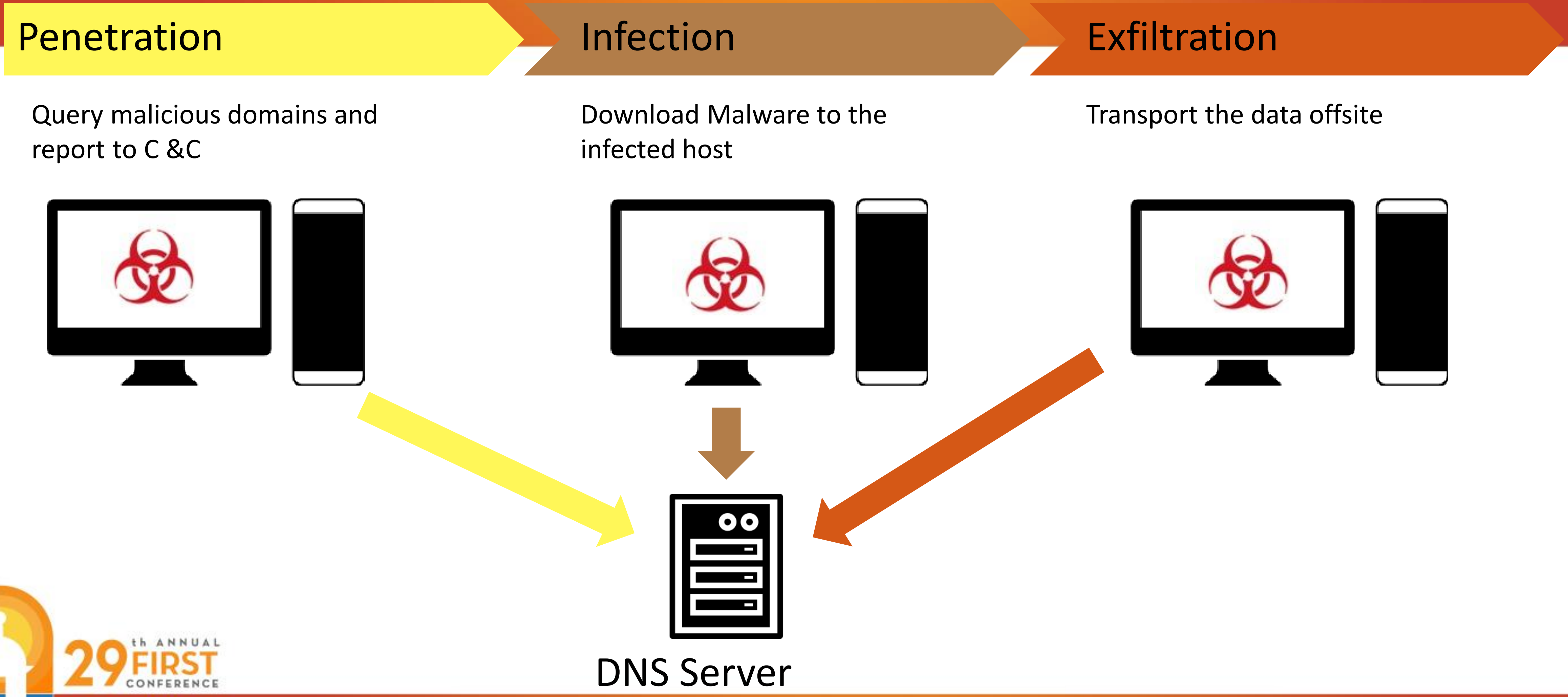
Applying Knowledge

- DNS Firewall to implement feeds and learnings in DNS resolution path
    - Lowest overhead, fastest response
- Next-gen Firewall can block via deep packet inspection (DPI)
- Some applications in IDS products
- Specialized in-line hardware also blocks via DPI
- SIEM analysis
- Query reputation systems to understand risk on per-hostname basis

- Depending on capabilities, can apply a machine learning model to discover new attacks

The Motion of Malware Through Networks

Malware uses DNS at every stage



Penetration

Query malicious domains and report to C &C

Infection

Download Malware to the infected host

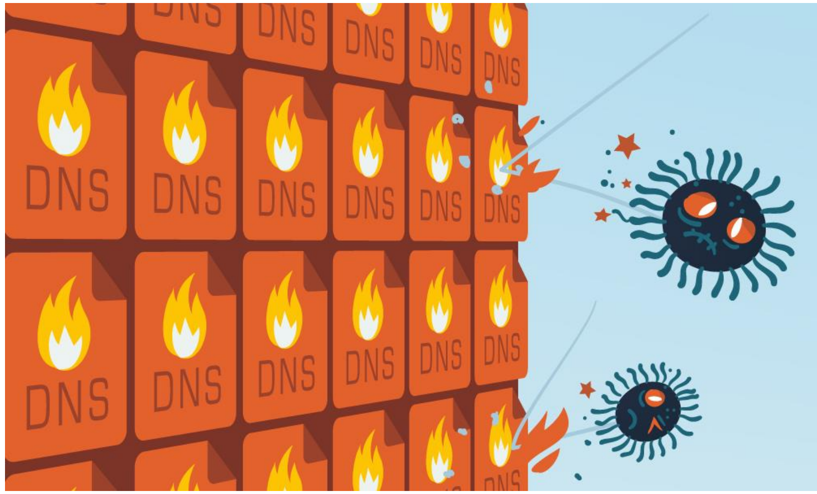
Exfiltration

Transport the data offsite

DNS Server

The Principles of a DNS Firewall

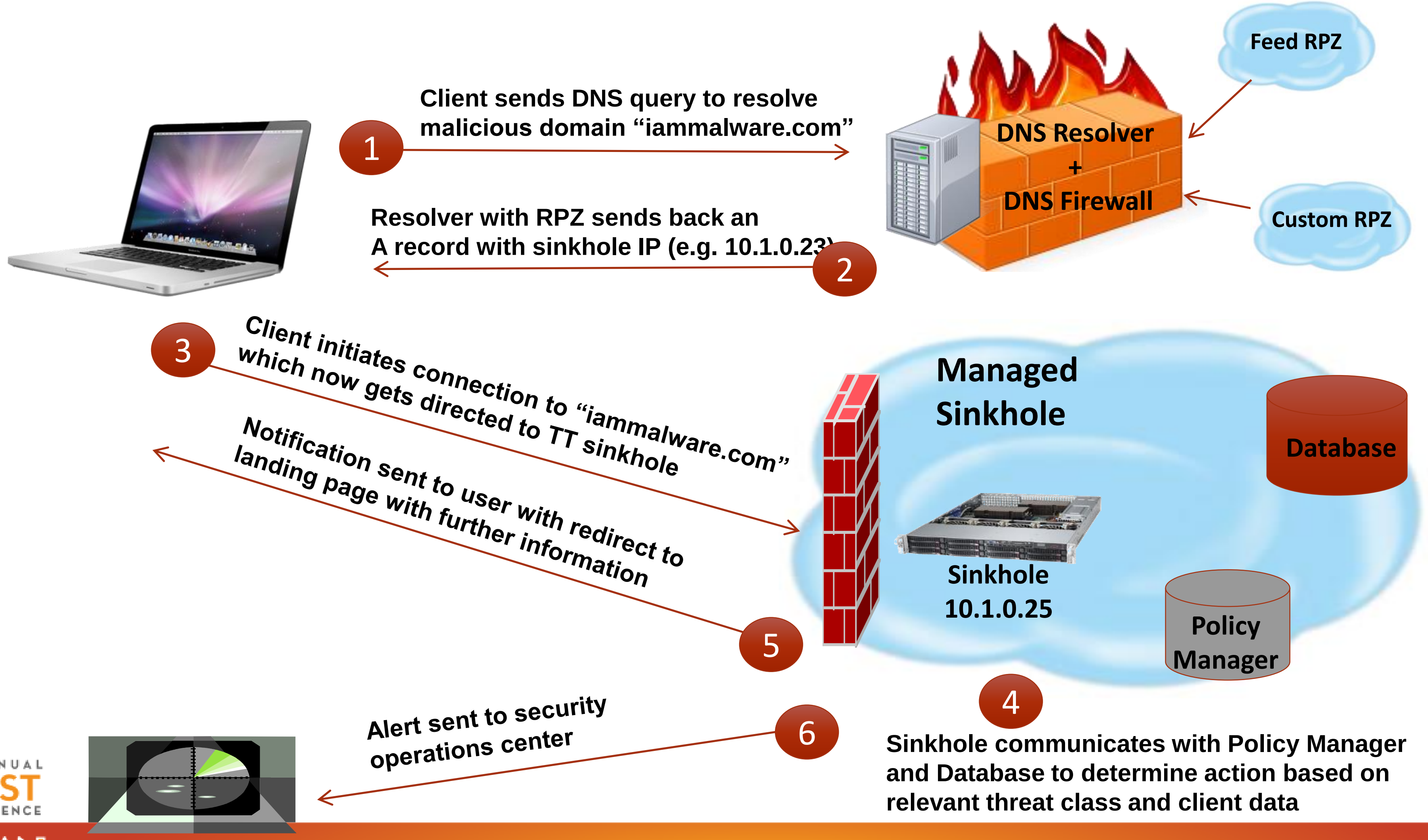
- Pre-load the cache with the responses you want to give and keep them there
  - Done regularly for various routing/internal uses
  - Many ways to get entries in there
- Can synthesize values or NX responses
- Monitor mode – log hits and watch activity
- Get lists of hostnames to block from somewhere
  - Develop lists in-house
  - Free (not quite as in beer)
  - Commercial services
- RPZs make this trivial, secure, and very scalable when using BIND



RPZ – Response Policy Zones

- “Most new domain names are malicious.
    - I am stunned by the simplicity and truth of that observation. Every day lots of new names are added to the global DNS, and most of them belong to scammers, spammers, e-criminals, and speculators…. Domains are cheap, domains are plentiful, and as a result most of them are dreck or worse.”
    - Paul Vixie
        - "Taking Back the DNS” July 30, 2010
        - http://www.circleid.com/posts/20100728_taking_back_the_dns/
- RPZ (Response Policy Zones) the result
- Any BIND resolver can easily implement large-scale domain block lists
    - Scalable: Several lists, different policies per list
    - Fast: Automatically updated with real-time data
- Many commercial DNS resolvers support them https://dnsrpz.info/
- DNS Policies now available in Microsoft Server 2016
    - Not quite as robust as RPZ, but can get the job done

Using a Managed Sinkhole with your DNS Firewall



1 Client sends DNS query to resolve malicious domain “iammalware.com”

2 Resolver with RPZ sends back an A record with sinkhole IP (e.g. 10.1.0.23)

3 Client initiates connection to “iammalware.com” which now gets directed to TT sinkhole

4 Sinkhole communicates with Policy Manager and Database to determine action based on relevant threat class and client data

5 Notification sent to user with redirect to landing page with further information

6 Alert sent to security operations center

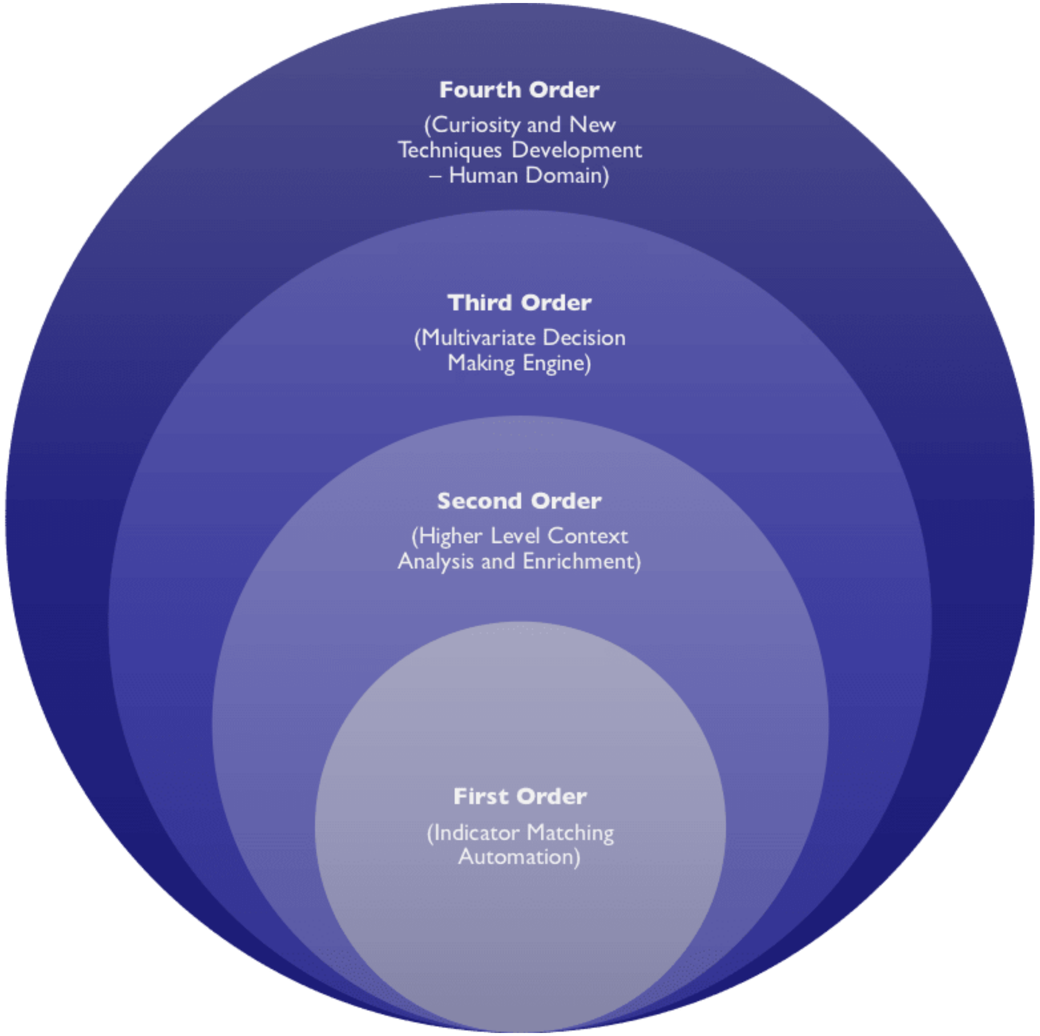
Don’t Forget about NXD

- NXDOMAIN – Non-Existent Domain responses can be a ”canary in the coalmine”
- Machines infected with DGA’s stick out very brightly
- Store them in your PDNS database (separate entry type)
  - Mine for patterns – can indicate DGA activities
  - If sent from a server authoritative for a tunneling domain, may indicate one-way data dump
- Pre-fetching and common typos may cause lots of noise here
- Bonus – alert you if part of your critical DNS infrastructure goes down

Turbo-Powering Your DNS Defenses

Threat Hunting Automation Maturity Model

- Framework I Saw at FIRST – This is Why You Come!
- Alex Pinto gave a great presentation on this on Monday
- Credit to Niddel and Alex for this one


Fourth Order
(Curiosity and New Techniques Development – Human Domain)
Third Order
(Multivariate Decision Making Engine)
Second Order
(Higher Level Context Analysis and Enrichment)
First Order
(Indicator Matching Automation)

Attributes of Interesting Data

- Known evil – categorized by reputation
- Meta data drivers to infer suspicious activities
  - Popularity of domain/hostname
  - Age of domain
  - Nameserver or hosting location reputation
  - Registrar reputation
  - TLD of domain
    - Some new gTLDs are cesspools (.top, .gdn, .bid)
- Fun with machine learning models

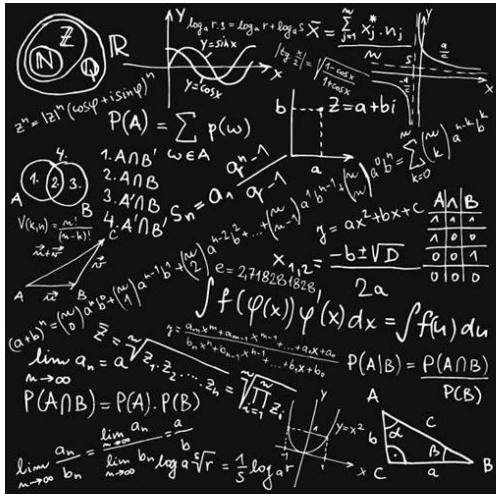
A Formula for Fast Flux

- 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

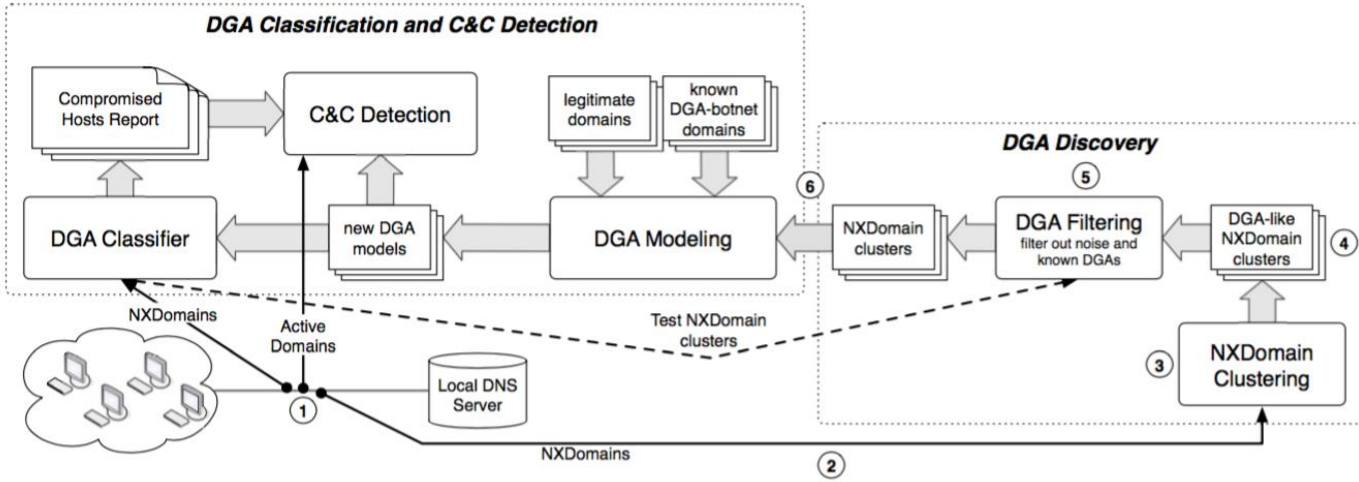


DGA Detection

- 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
    - Feeds available free and commercial
- 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
  - http://bit.ly/2dnEa4Y

Example from Research: Pleiades

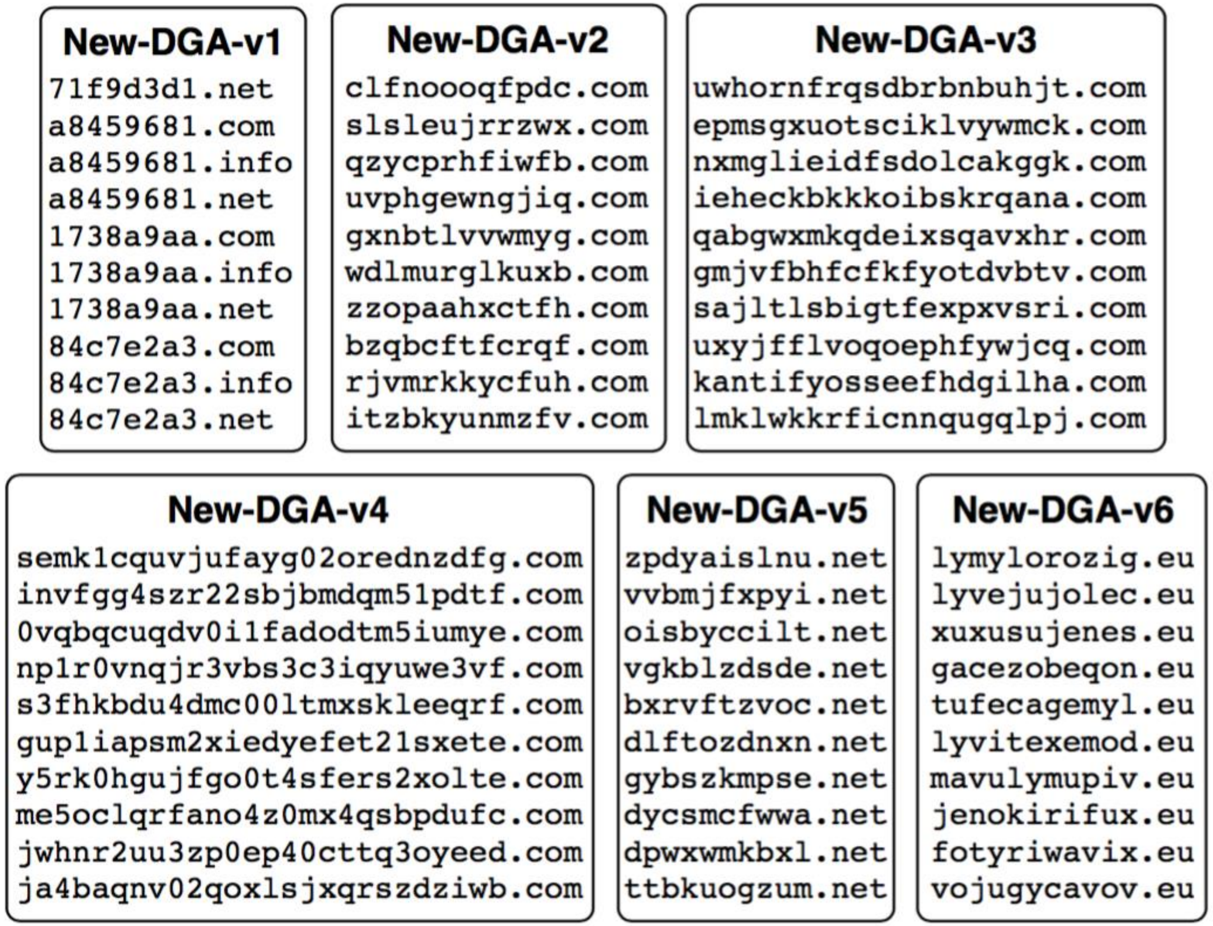
- **Pleiades**: a DGA-based botnet identification system
- Analyze streams of NXDomains at the recursive level
- Accurately detects and models (new and old) DGA-bots
- Our experimental results allowed us to discover six new DGA-based botnets
- HMM-based active C&C detector for new DGAs
    - Manos Antonakakis of GA Tech & Damballa



Statistical Features in Pleiades

- 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

Previously Unknown DGA’s Pleiades Found



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

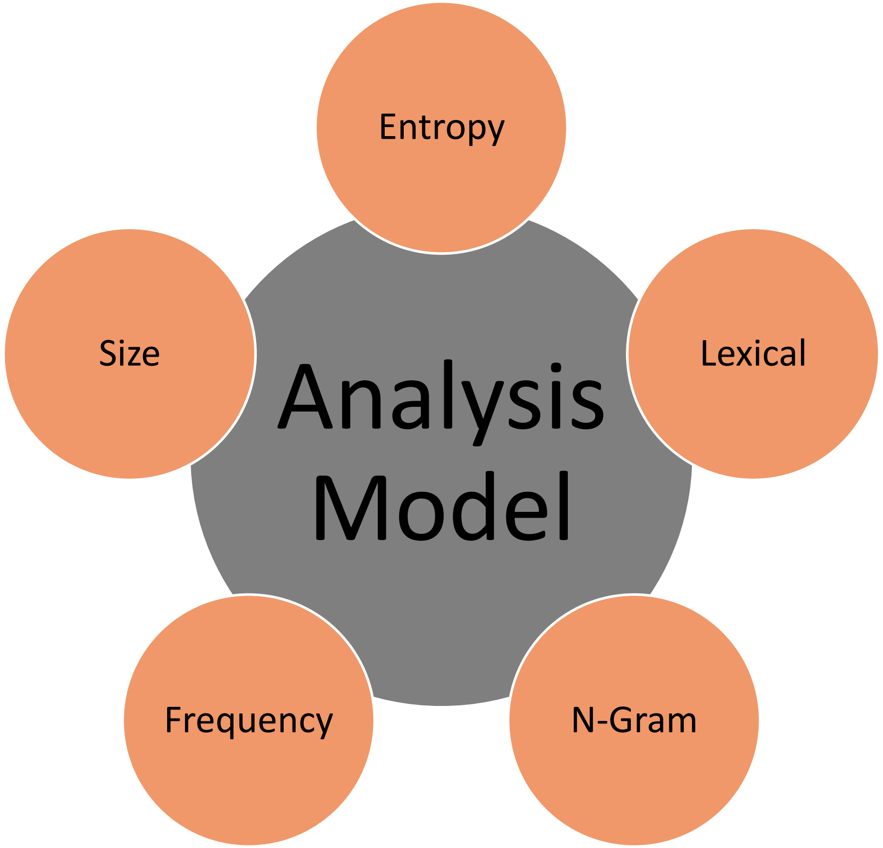
New-DGA-v4	New-DGA-v5	New-DGA-v6
semk1cquvjufayg02orednzdfg.com	zpdyaislnu.net	lymylorozig.eu
invfgg4szr22sbjbmdqm51pdtf.com	vvbmjfxpyi.net	lyvejujolec.eu
0vqbqcuqdv0i1fadodtm5iumye.com	oisbyccilt.net	xuxusujenes.eu
np1r0vnqjr3vbs3c3iqyuwe3vf.com	vgkblzdsde.net	gacezobeqon.eu
s3fhkbdu4dmc00ltmxskleeqrf.com	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.

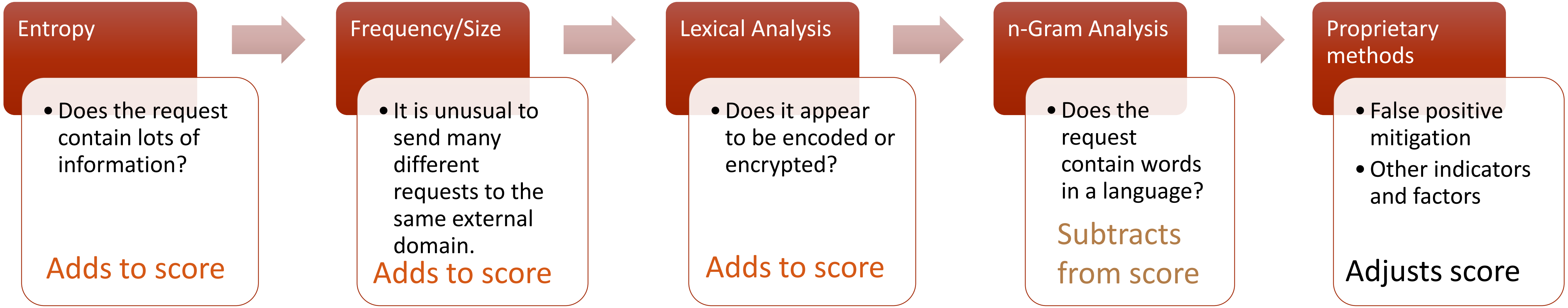
DNS Tunneling Detection With Machine Learning

Machine learning techniques can detect sophisticated data exfiltration techniques that don't have well-known signatures (including zero day)

1. Examine all DNS records (e.g.: TXT, A, AAAA)
2. Detects presence of data using lexical and temporal analysis
3. Certain attributes add to a threat score; others subtract from it
4. Final score classifies a request as exfiltration or not
5. If exfiltration is found, can automatically add destinations to RPZ feed or other protection data sets
6. Scales protection to other parts of the network
7. Use both sides of the DNS data resolution – many clients or a single client with many requests just as important as funky domains



How an Analytics Model Works



Entropy
- Does the request contain lots of information?

Adds to score

Frequency/Size
- It is unusual to send many different requests to the same external domain.

Adds to score

Lexical Analysis
- Does it appear to be encoded or encrypted?

Adds to score

n-Gram Analysis
- Does the request contain words in a language?

Subtracts from score

Proprietary methods
- False positive mitigation
- Other indicators and factors

Adjusts score

- Analytics algorithms are sophisticated and complex
- Simplifying greatly, certain attributes add to a threat score, others subtract from it
- All attributes are evaluated and weighted
- After all attributes are evaluated, a final score will classify a request as exfiltration or not
- If the finding is exfiltration, the destination DNS server is added to a special RPZ zone that contains the block, log, redirect policy

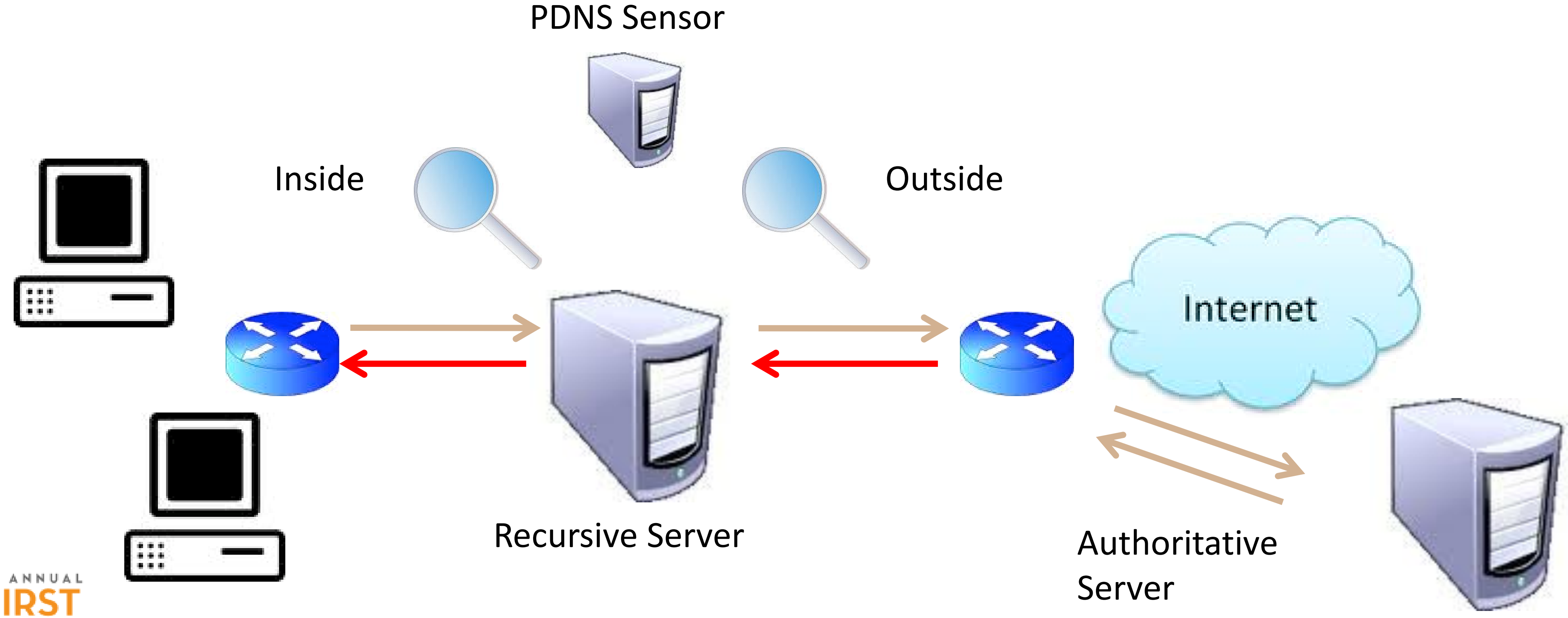
Detecting Domain Shadowing

- 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
- Newly seen hostnames on long-established domains
- Lots of these odd hostnames showing up at once
- Hosted at registrars with known domain shadowing problems
- Machine learning techniques again useful
- Careful to not run into advertising networks, CDN’s or some other legit infrastructure
  - White listing wise
- Should block the odd hosts, whitelist the main “legit” ones if popular

PDNS: Best Thing for Threat Research Since…

Inside vs. Outside

- Where do we monitor from?



Inside Monitoring

- Get all resolution attempts (minus stub caching)
  - Good for watching for volume spikes
  - Volume can be quickly overwhelming
- Know exact machine(s) making requests
  - Can track down infections to the source
  - Privacy concerns (ISPs)

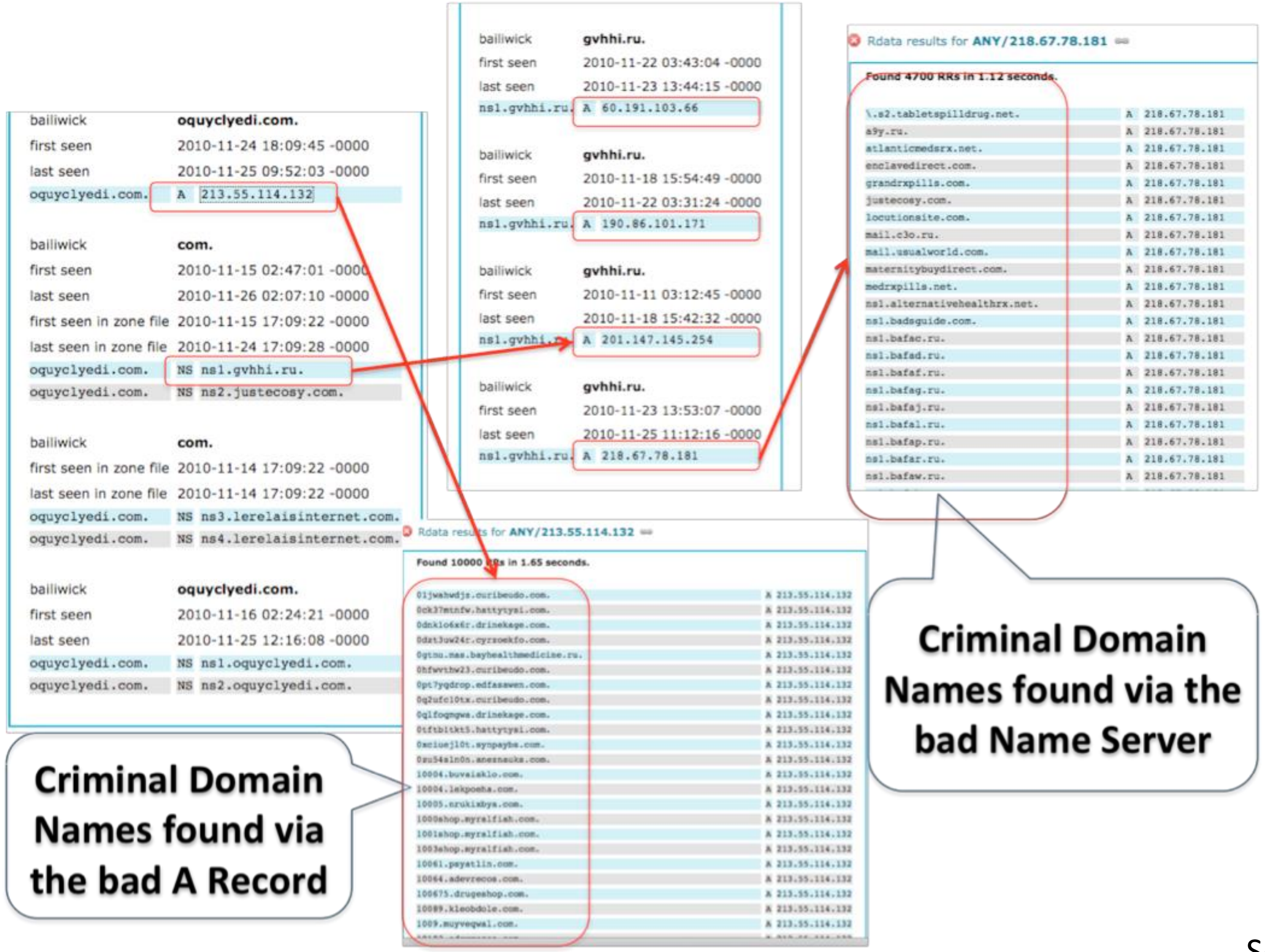
Outside Monitoring

- See aggregate numbers of resolutions for the organization, ISP etc.
  - Easier data management
  - Lose volume information to caching
- Privacy and internal security concerns largely handled

On Server Monitoring

- Had been impractical (performance of DNS concerns), but capabilities are improving
- May be required with future adoption of dprive
  - New IETF standards for encrypting DNS traffic

Mapping Criminal Infrastructure



```
bailiwick              oquyclyedi.com.
first seen             2010-11-24 18:09:45 -0000
last seen              2010-11-25 09:52:03 -0000
oquyclyedi.com.        A  213.55.114.132

bailiwick              com.
first seen             2010-11-15 02:47:01 -0000
last seen              2010-11-26 02:07:10 -0000
first seen in zone file 2010-11-15 17:09:22 -0000
last seen in zone file 2010-11-24 17:09:28 -0000
oquyclyedi.com.        NS ns1.gvhhi.ru.
oquyclyedi.com.        NS ns2.justecosy.com.

bailiwick              com.
first seen in zone file 2010-11-14 17:09:22 -0000
last seen in zone file 2010-11-14 17:09:22 -0000
oquyclyedi.com.        NS ns3.lerelaisinternet.com.
oquyclyedi.com.        NS ns4.lerelaisinternet.com.

bailiwick              oquyclyedi.com.
first seen             2010-11-16 02:24:21 -0000
last seen              2010-11-25 12:16:08 -0000
oquyclyedi.com.        NS ns1.oquyclyedi.com.
oquyclyedi.com.        NS ns2.oquyclyedi.com.
```

```
bailiwick      gvhhi.ru.
first seen     2010-11-22 03:43:04 -0000
last seen      2010-11-23 13:44:15 -0000
ns1.gvhhi.ru.  A  60.191.103.66

bailiwick      gvhhi.ru.
first seen     2010-11-18 15:54:49 -0000
last seen      2010-11-22 03:31:24 -0000
ns1.gvhhi.ru.  A  190.86.101.171

bailiwick      gvhhi.ru.
first seen     2010-11-11 03:12:45 -0000
last seen      2010-11-18 15:42:32 -0000
ns1.gvhhi.ru.  A  201.147.145.254

bailiwick      gvhhi.ru.
first seen     2010-11-23 13:53:07 -0000
last seen      2010-11-25 11:12:16 -0000
ns1.gvhhi.ru.  A  218.67.78.181
```

```
Rdata results for ANY/213.55.114.132

Found 10000 RRs in 1.65 seconds.

01jwahwdjs.curibeudo.com.            A 213.55.114.132
0ck37mtnfw.hattytysi.com.            A 213.55.114.132
0dnklo6x6r.drinekage.com.            A 213.55.114.132
0dzt3uw24r.cyrzoekfo.com.            A 213.55.114.132
0gtnu.mas.bayhealthmedicine.ru.      A 213.55.114.132
0hfwvthw23.curibeudo.com.            A 213.55.114.132
0pt7ygdrop.edfasawen.com.            A 213.55.114.132
0q2ufcl0tx.curibeudo.com.            A 213.55.114.132
0qlfogngwa.drinekage.com.            A 213.55.114.132
0tftbltkt5.hattytysi.com.            A 213.55.114.132
0xciuej10t.synpayba.com.             A 213.55.114.132
0zu54sln0n.aneznauka.com.            A 213.55.114.132
10004.buvaiaklo.com.                 A 213.55.114.132
10004.lekpoeha.com.                  A 213.55.114.132
10005.nrukixbya.com.                 A 213.55.114.132
1000shop.myralfiah.com.              A 213.55.114.132
1001shop.myralfiah.com.              A 213.55.114.132
1003shop.myralfiah.com.              A 213.55.114.132
10061.payatlin.com.                  A 213.55.114.132
10064.adevrecos.com.                 A 213.55.114.132
100675.drugeshop.com.                A 213.55.114.132
10089.kleobdole.com.                 A 213.55.114.132
1009.muyveqwal.com.                  A 213.55.114.132
```

```
Rdata results for ANY/218.67.78.181

Found 4700 RRs in 1.12 seconds.

\.s2.tabletspilldrug.net.            A 218.67.78.181
a9y.ru.                              A 218.67.78.181
atlanticmedsrx.net.                  A 218.67.78.181
enclavedirect.com.                   A 218.67.78.181
grandrxpills.com.                    A 218.67.78.181
justecosy.com.                       A 218.67.78.181
locutionsite.com.                    A 218.67.78.181
mail.c3o.ru.                         A 218.67.78.181
mail.usualworld.com.                 A 218.67.78.181
maternitybuydirect.com.              A 218.67.78.181
medrxpills.net.                      A 218.67.78.181
ns1.alternativehealthrx.net.         A 218.67.78.181
ns1.badsguide.com.                   A 218.67.78.181
ns1.bafac.ru.                        A 218.67.78.181
ns1.bafad.ru.                        A 218.67.78.181
ns1.bafaf.ru.                        A 218.67.78.181
ns1.bafag.ru.                        A 218.67.78.181
ns1.bafaj.ru.                        A 218.67.78.181
ns1.bafal.ru.                        A 218.67.78.181
ns1.bafap.ru.                        A 218.67.78.181
ns1.bafar.ru.                        A 218.67.78.181
ns1.bafaw.ru.                        A 218.67.78.181
```

Criminal Domain Names found via the bad A Record

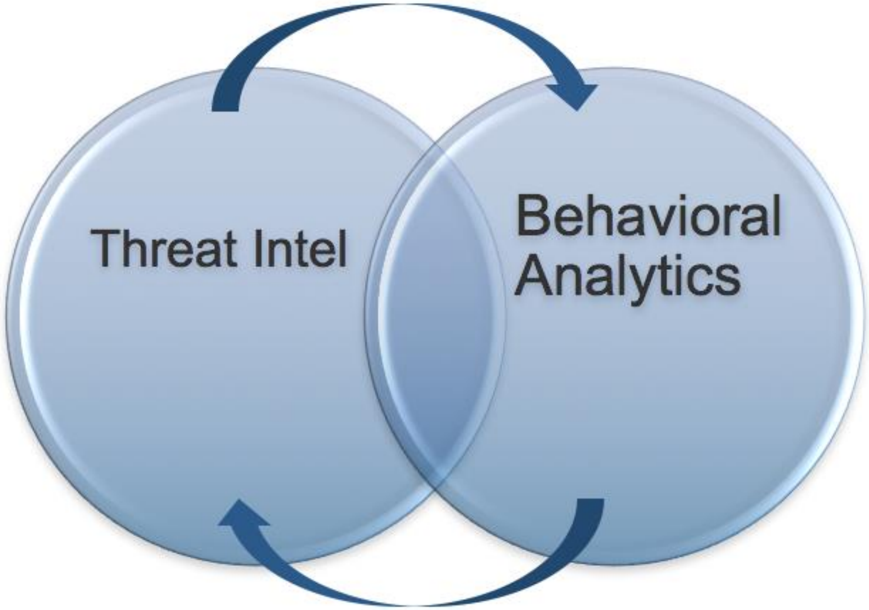
Criminal Domain Names found via the bad Name Server

Source: ISC

Combine Techniques for Protection against Known and Unknown Threats

Threat Data

- Regular threat feeds are about known threats
- Constantly updated
- Tailored for high detection, low false positives
- Cover malware, phishing, ransomware, more
- Internal alerts
- DNS telemetry (PDNS DB)



Behavioral Analytics

- Detects threats by how the endpoint is acting
- Surfaces unknown threats
- Can take threat data and refine it
- Threat feeds can be adjusted based on findings

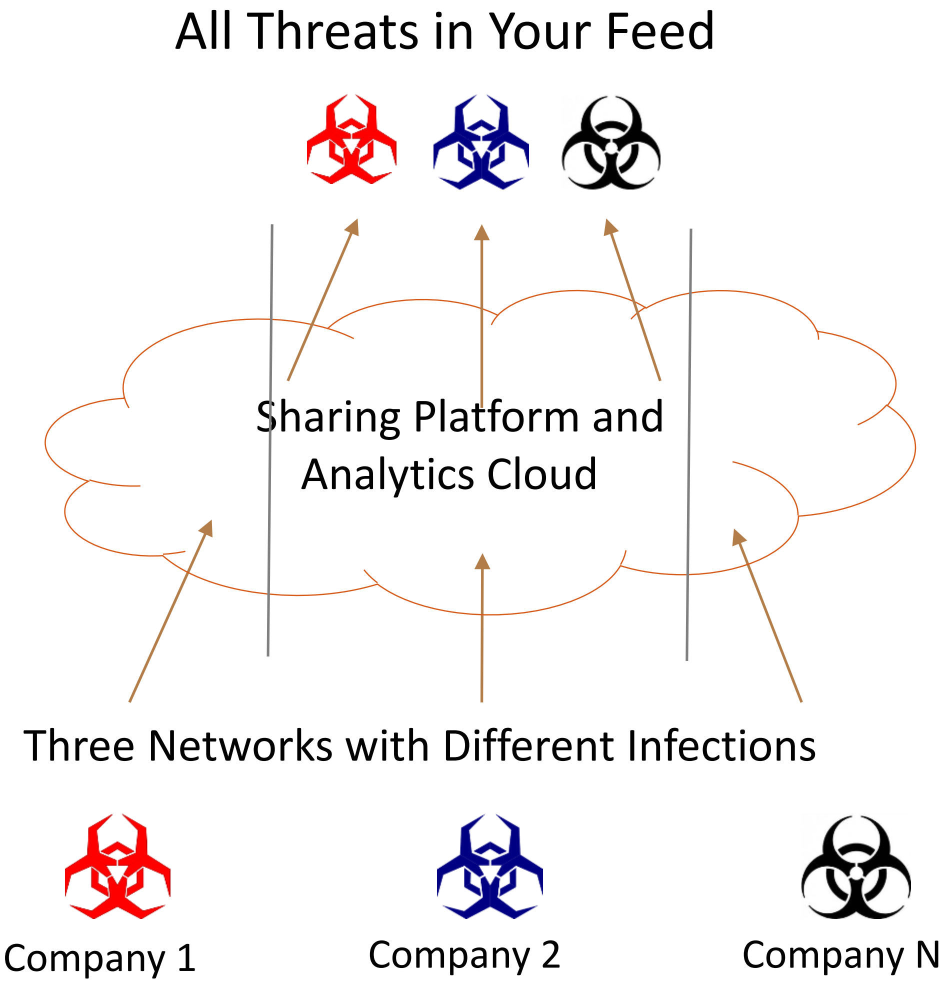
Threat Intelligence + Behavioral Analytics = Most Complete Protection

Engage Your Threat Intelligence Team

- Constantly bring in new threat data from around the Internet
- Expand reported threat data into infrastructure of malicious actors’
  - DNS configurations, whois, SSL Certs, SSH fingerprints – a host of techniques
  - Use infrastructure metadata (Passive DNS, zone files, hosting data) to find fresh malicious Internet presences
  - Track fast-flux infrastructure
- Reverse binaries and perform other malware analysis
  - Constantly update DGA data
  - Command & Control data
- Feed into your DNS Firewall continuously

Sharing Effect: 1 + 1 = 3

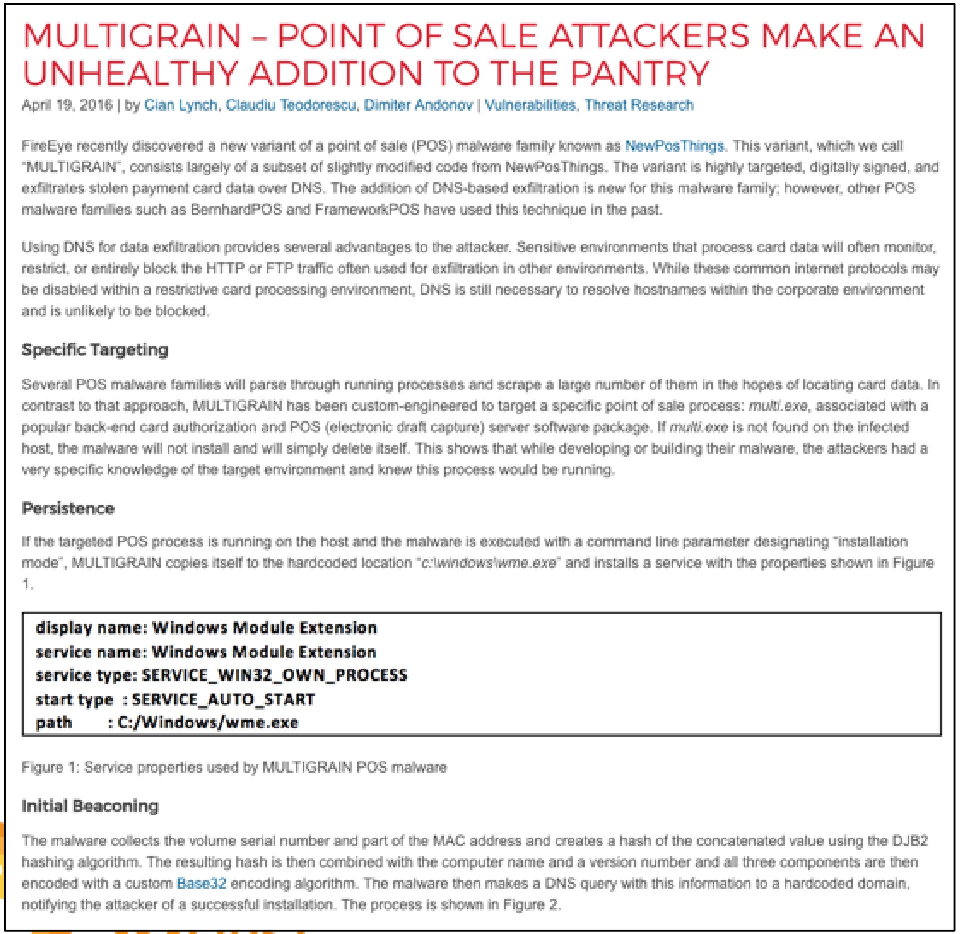
Protect against Threats Found in Sharing Partners' Networks


All Threats in Your Feed
Sharing Platform and Analytics Cloud
Three Networks with Different Infections
Company 1
Company 2
Company N

- Partners can contribute non-sensitive threat data
- You can protect yourself from all discovered threats against anyone else
- Sharing of raw, anonymized data can create a better analytics pool

Case study: Threat Intelligence Process

1. TTP's identified, by internal team or others



MULTIGRAIN – POINT OF SALE ATTACKERS MAKE AN UNHEALTHY ADDITION TO THE PANTRY

April 19, 2016 | by Cian Lynch, Claudiu Teodorescu, Dimiter Andonov | Vulnerabilities, Threat Research

FireEye recently discovered a new variant of a point of sale (POS) malware family known as NewPosThings. This variant, which we call "MULTIGRAIN", consists largely of a subset of slightly modified code from NewPosThings. The variant is highly targeted, digitally signed, and exfiltrates stolen payment card data over DNS. The addition of DNS-based exfiltration is new for this malware family; however, other POS malware families such as BernhardPOS and FrameworkPOS have used this technique in the past.

Using DNS for data exfiltration provides several advantages to the attacker. Sensitive environments that process card data will often monitor, restrict, or entirely block the HTTP or FTP traffic often used for exfiltration in other environments. While these common internet protocols may be disabled within a restrictive card processing environment, DNS is still necessary to resolve hostnames within the corporate environment and is unlikely to be blocked.

Specific Targeting

Several POS malware families will parse through running processes and scrape a large number of them in the hopes of locating card data. In contrast to that approach, MULTIGRAIN has been custom-engineered to target a specific point of sale process: *multi.exe*, associated with a popular back-end card authorization and POS (electronic draft capture) server software package. If *multi.exe* is not found on the infected host, the malware will not install and will simply delete itself. This shows that while developing or building their malware, the attackers had a very specific knowledge of the target environment and knew this process would be running.

Persistence

If the targeted POS process is running on the host and the malware is executed with a command line parameter designating "installation mode", MULTIGRAIN copies itself to the hardcoded location "*c:\windows\wme.exe*" and installs a service with the properties shown in Figure 1.

```
display name: Windows Module Extension
service name: Windows Module Extension
service type: SERVICE_WIN32_OWN_PROCESS
start type  : SERVICE_AUTO_START
path        : C:/Windows/wme.exe
```

Figure 1: Service properties used by MULTIGRAIN POS malware

Initial Beaconing

The malware collects the volume serial number and part of the MAC address and creates a hash of the concatenated value using the DJB2 hashing algorithm. The resulting hash is then combined with the computer name and a version number and all three components are then encoded with a custom Base32 encoding algorithm. The malware then makes a DNS query with this information to a hardcoded domain, notifying the attacker of a successful installation. The process is shown in Figure 2.

https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html

2. Internal team performs research to find threat indicators and adds them to detection data sets and protection feeds

For long-lasting attacks, automate on-going collection of indicators

Multigrain threat indicators

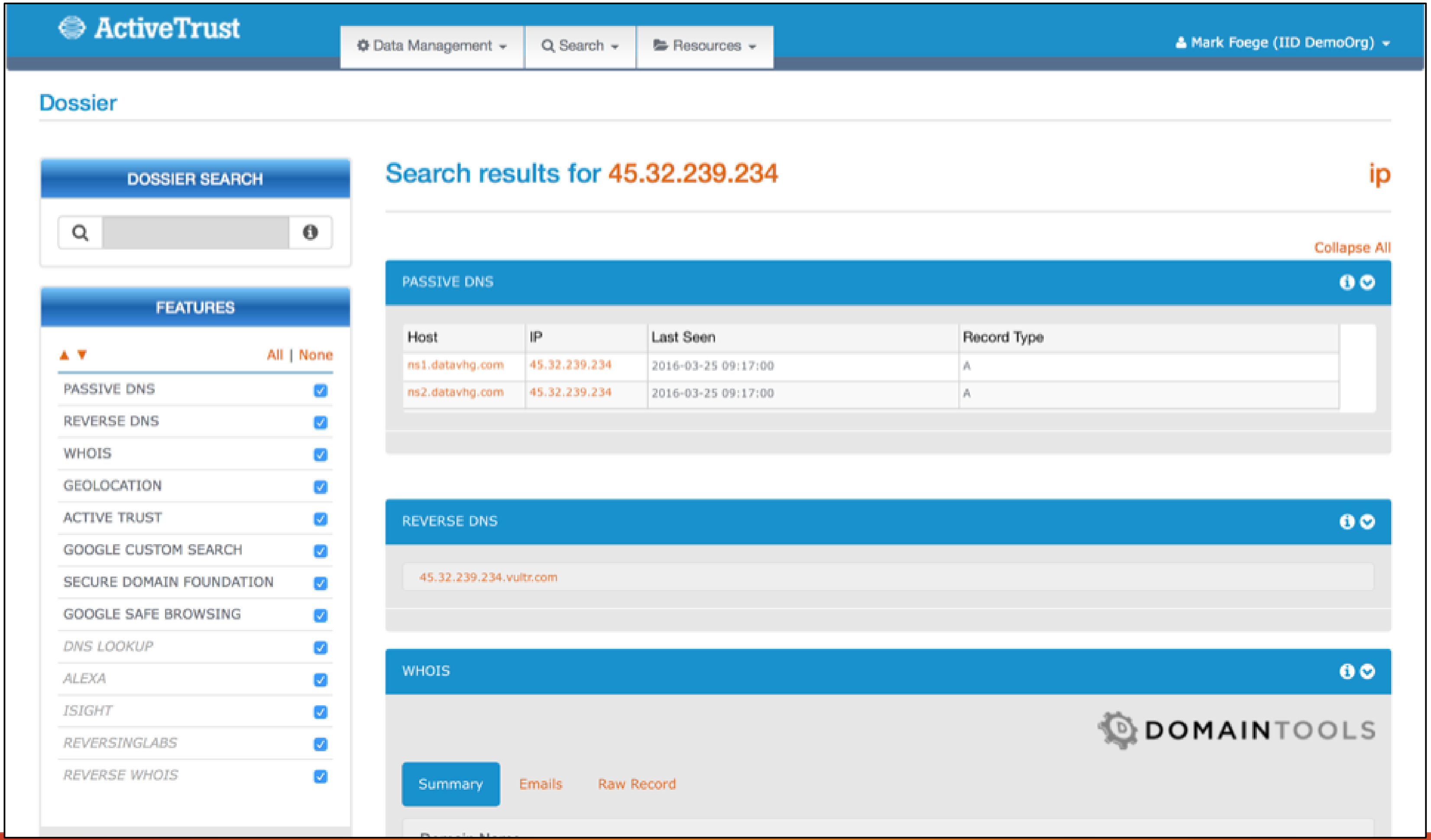
45.32.239.234

datavhg.com

dojfgj.com

Case study: Threat Intelligence Process

3. Customer gets a DNS Firewall hit on an indicator:
use your tools to find out more about it



Dossier

DOSSIER SEARCH

FEATURES

All | None

- PASSIVE DNS ☑
- REVERSE DNS ☑
- WHOIS ☑
- GEOLOCATION ☑
- ACTIVE TRUST ☑
- GOOGLE CUSTOM SEARCH ☑
- SECURE DOMAIN FOUNDATION ☑
- GOOGLE SAFE BROWSING ☑
- *DNS LOOKUP* ☑
- *ALEXA* ☑
- *ISIGHT* ☑
- *REVERSINGLABS* ☑
- *REVERSE WHOIS* ☑

Search results for 45.32.239.234 ip

Collapse All

PASSIVE DNS

Host	IP	Last Seen	Record Type
ns1.datavhg.com	45.32.239.234	2016-03-25 09:17:00	A
ns2.datavhg.com	45.32.239.234	2016-03-25 09:17:00	A

REVERSE DNS

45.32.239.234.vultr.com

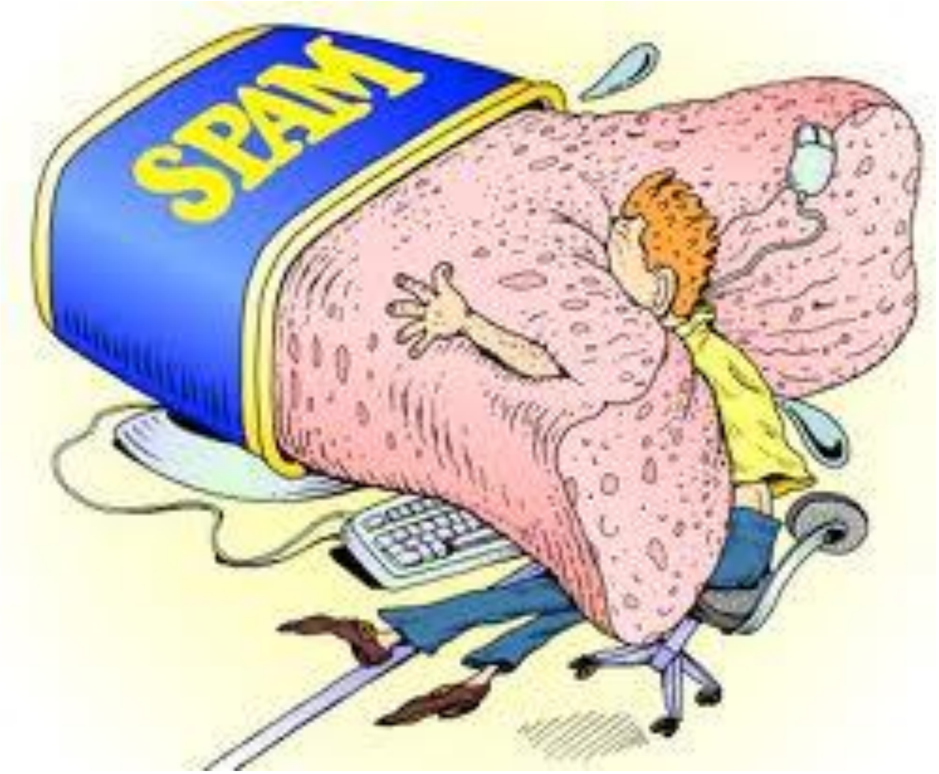
WHOIS

Let’s Play with Some Useful Tools!

- Infoblox TIDE
- DomainTools Iris
- Farsight DNSDB
- RiskIQ PassiveTotal
- Cisco Umbrella Investigate
- Zetalytics Zone Cruncher
- Deteque (Spamhaus) PDNS Research Portal
- BFK Passive DNS Replication

Thanks to all the vendors who gave me access to their commercial products!

Hey, I just got some…



Summary

- DNS is a critical infrastructure asset which is a constant target of attack but most still take for granted
- DNS is fundamental to the operation of malware and data exfiltration – a continuously exploited blind spot
- Many vendors and open source tools provide a range of solutions to protect DNS, disrupt malware and prevent data exfiltration
- DNS Firewalls are powerful security devices for network and user defense and breach detection
- Passive DNS is a super-effective threat research tool
- Use DNS Jiu-Jitsu to turn your hum-drum DNS infrastructure into a turbo-charged, malware crushing, network protection leviathan!

FIRST
Improving Security Together

DNS is NOT Boring!
Using DNS to Expose and Thwart Attacks

Rod Rasmussen

Thank You!

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO