
ICANN
ANNUAL GENERAL
63
BARCELONA
20–25 October 2018

Domain Name System Abuse
An Introduction

Agenda

- What is DNS Abuse? DNS Misuse?
- Examples of DNS Abuse or Misuse
- Evolving DNS Threat Landscape
- Abuse in an ICANN Context

What is DNS Abuse?

- No globally accepted definition exists, but definitional variants include
  - Cyber crime
  - Hacking
  - **Malicious conduct**
- Threats to the DNS fall under three categories:
  - *data corruption*, *denial of service*, and *privacy violations*.
- DNS Misuse is often distinguished from DNS Abuse
  - In the English language the terms “misuse” and “abuse” are often interchangeable, with abuse being the more severe. However we use the terms to differentiate between attacks that “misuse” the system and those that “abuse” the system itself. Both are equally bad.

Keep It Simple

In simpler terms “DNS abuse” refers to anything that attacks or abuses the DNS infrastructure,

or

DNS misuse refers to exploiting the DNS protocol or the domain name registration processes for malicious purposes.

Why Is the DNS a Target for Attacks

- Everyone uses the DNS to resolve user friendly names to Internet Protocol addresses
- Disrupt the DNS and you disrupt e-merchant transactions, government services, e-learning, or social engagement
- Exploit the DNS and you can trick, defraud or deceive users
- Vectors for exploitation
  - Maliciously register domain names
  - Hijack name resolution or name registration services
  - Corrupt DNS data

All of the operational elements of the DNS are targets for attacks

- Authoritative Name Servers host zone data
  - The set of "DNS data" that the registrant publishes
- Recursive Name Resolvers ("resolvers")
  - Systems that find answers to queries for DNS data
  - Caching resolvers find and store answers locally for "TTL" period of time
- Client or "stub" resolvers
  - Software in applications, mobile apps or operating systems that query the DNS and process responses

What elements of the DNS are targeted and how?

Target	Authoritative Name Server	Recursive Resolver	Stub Resolver
Access bandwidth	✓	✓	✓
Access network elements	✓	✓	✓
NS or device:			
Hardware	✓	✓	✓
OS software	✓	✓	✓
Name server software	✓	✓	
Cache		✓	✓
Application software			✓
Administration	✓	✓	✓
Configuration	✓	✓	✓

Agenda

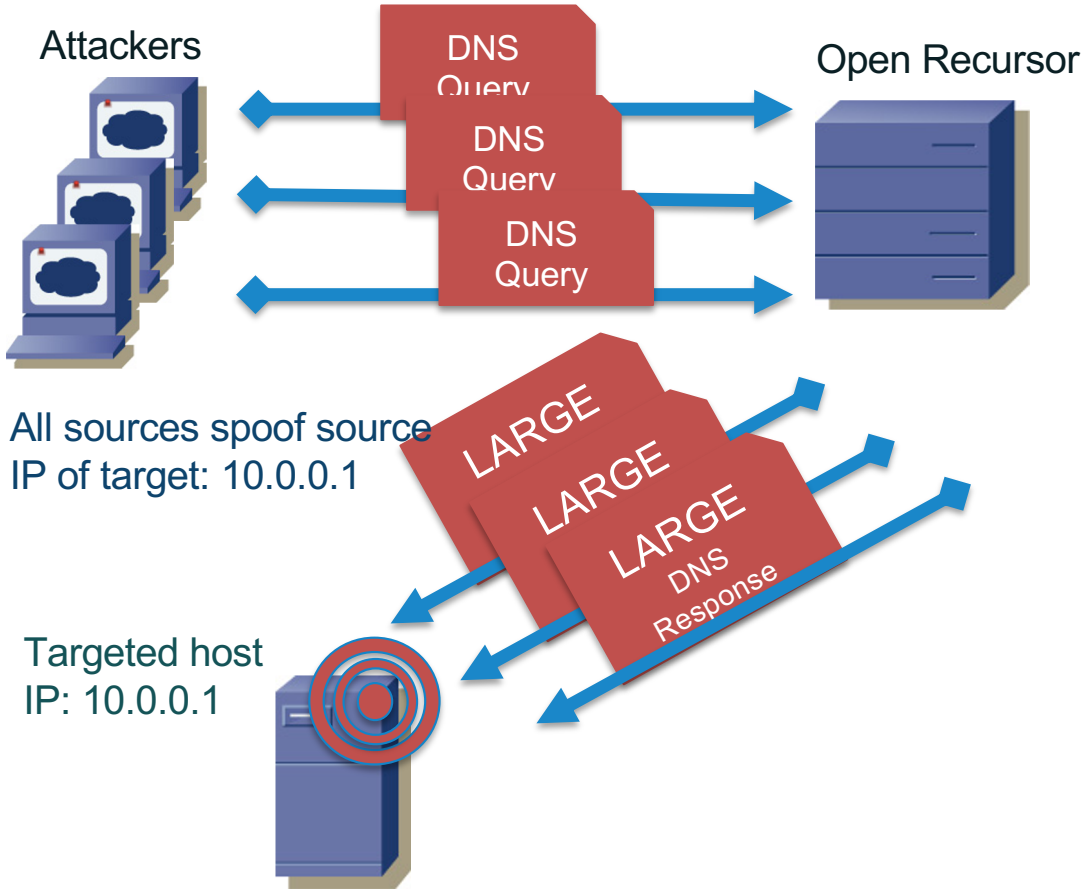
- What is DNS Abuse? DNS Misuse?
- Examples of DNS Abuse or Misuse
- Evolving DNS Threat Landscape
- Abuse in an ICANN Context

Attacks Against Name Servers or Recursors

- “Exploit to own” DOS attack
- Reflection attack
- Amplification attack
- Distributed Reflection and Amplification DOS attack
- (Host) Resource Depletion Attack
- Cache Poisoning or Exhaustion attacks
- DNS Man-in-the-Middle attack

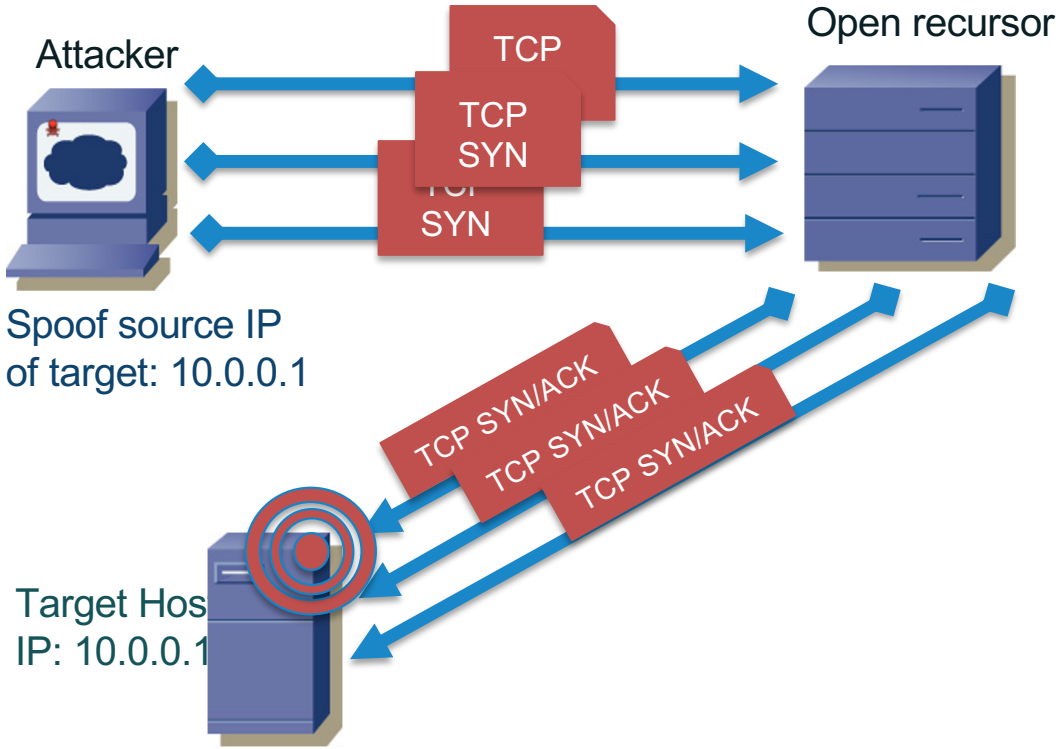
Let’s look at some examples

Distributed reflection and amplification attack (DDoS)



- Launch reflection and amplification attack from 1000s of origins
- Reflect through open recursor
- Deliver 1000s of large responses to target

(Host) Resource Depletion DOS attack



- Attacker sends flood of DNS messages over TCP from spoofed IP address of target
- Name server allocates resources for TCP connections until resources are exhausted
- Name resolution is degraded or interrupted

Solution/Defense Space

Most current solutions include a mix of “Provisioning” and smart “filtering” also called “scrubbing”.

Whether you do this in house or purchase services (or both) is often a question of available skills and resources.

Often defense needs to take place upstream of the attacked network either at the ISP or through cloud services.

Poisoning a Cache

- Attacker launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com with malicious data about ebay.com
- Vulnerable resolvers ad malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry

My Mac

What is the IPv4 address for loseweightfastnow.com

I'll cache this response… and update www.ebay.com

My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO *www.ebay.com is at 192.168.1.2*

ecrime name server

Solution/Defense Space

If you manage your own resolvers keep them private to your known users

Use modern DNS software and keep it up-to-date!

Most server software has built in features to make cache poisoning harder through randomization of source ports, query IDs and other solutions.

Treat your DNS software like any other critical network element and purchase relevant support services.

Use DNSSEC to sign your zones and validate your resolution process.

https://www.internetsociety.org/deploy360/dnssec/basics/

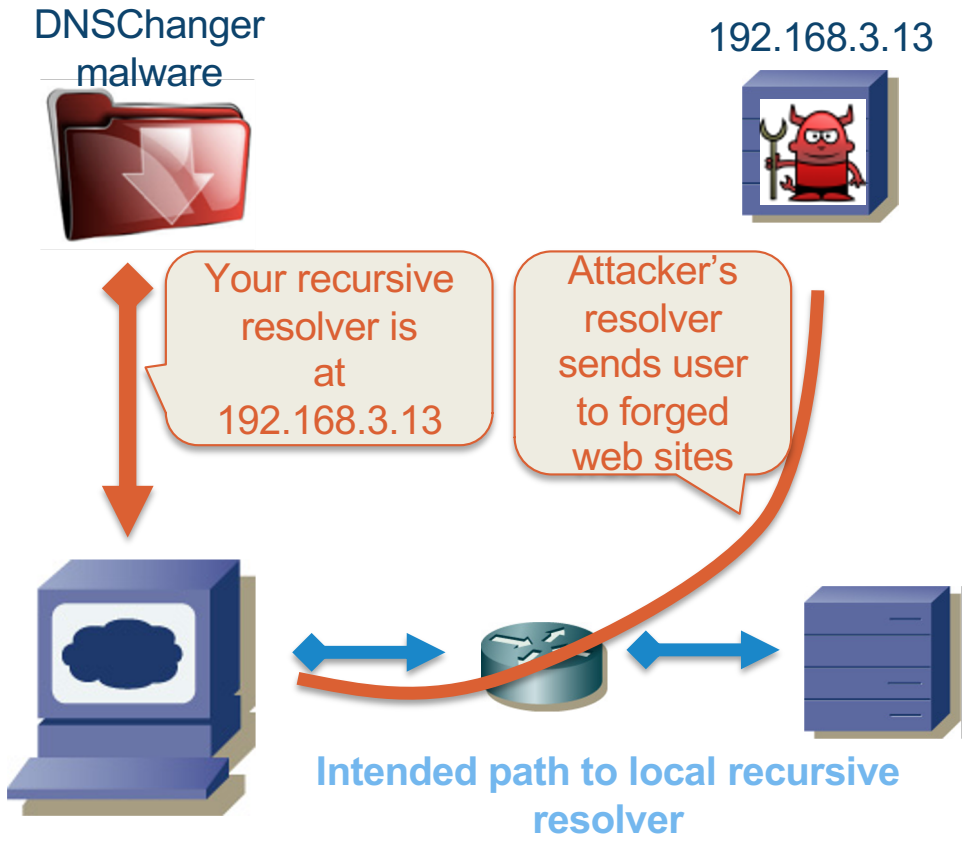
Poisoning a host (DNSChanger)

Attacker distributes DNS configuration altering malware via

- Spam, drive-by download…

DNSChanger malware

- Alters DNS configuration of infected PC
- Causes all requests to go to a malicious name server run by attackers
- Attacker updates malware to redirect web traffic to a destination of his choosing



https://www.fbi.gov/file-repository/dns-changer-malware.pdf

Solution/Defense Space

Issues like DNS changer are not really DNS issues but more generic network hygiene issues.

Keep software patched

Have a password management process in place. (i.e. remove “default” passwords on all devices)

Monitor your network traffic, including DNS traffic, for unusual behaviors.

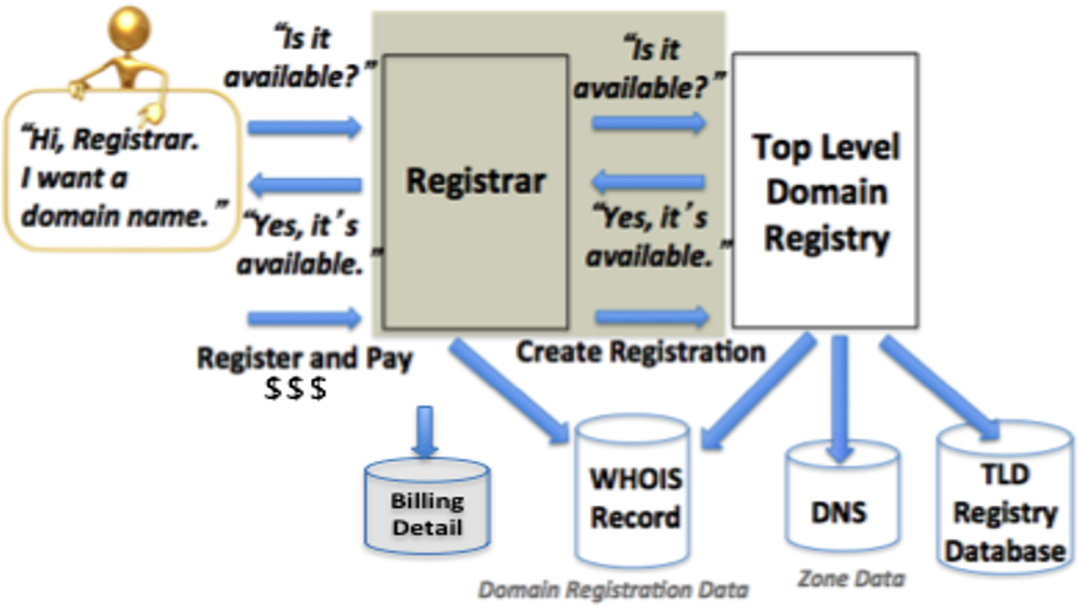
Give your staff training on computer/network hygiene and avoiding risks on line. (Phishing, Malware, etc. etc.)

DNS protocol and registration system misuse

- Domain name registration hijacking, DNS hijacking
- DNS protocol as a Covert Exfiltration Channel
- DNS protocol as a Covert Malware Channel
- Fast Flux

Let's look at some examples

Domain name registrations are sweet targets for attacks



How to register a gTLD domain:

1. Choose a string e.g., `example`
2. Visit a registrar to check string availability
3. Pay a fee to register the name
4. Submit registration information

Registrar and registries manage:

- "string" + TLD (managed in registry DB)
- Contacts, DNS (managed in Whois)
- DNS, status (managed in Whois DBs)
- Payment information

Process is automated, rapidly provisioned.
Correspondence is largely email
Inexpensive registrations are plentiful…
Good for consumers, good for attackers, too

Why do attackers and criminals register domain names?

Register names, sometimes in volume to host

- Phishing (fraud) pages
- Ransomware payment web pages
- Malware distribution sites
- Scam sites (advance fee fraud, reshipping etc.)
- Counterfeit goods sites
- Illegal pharmaceutical or piracy sites

Domain names also play roles in criminal DNS Infrastructures

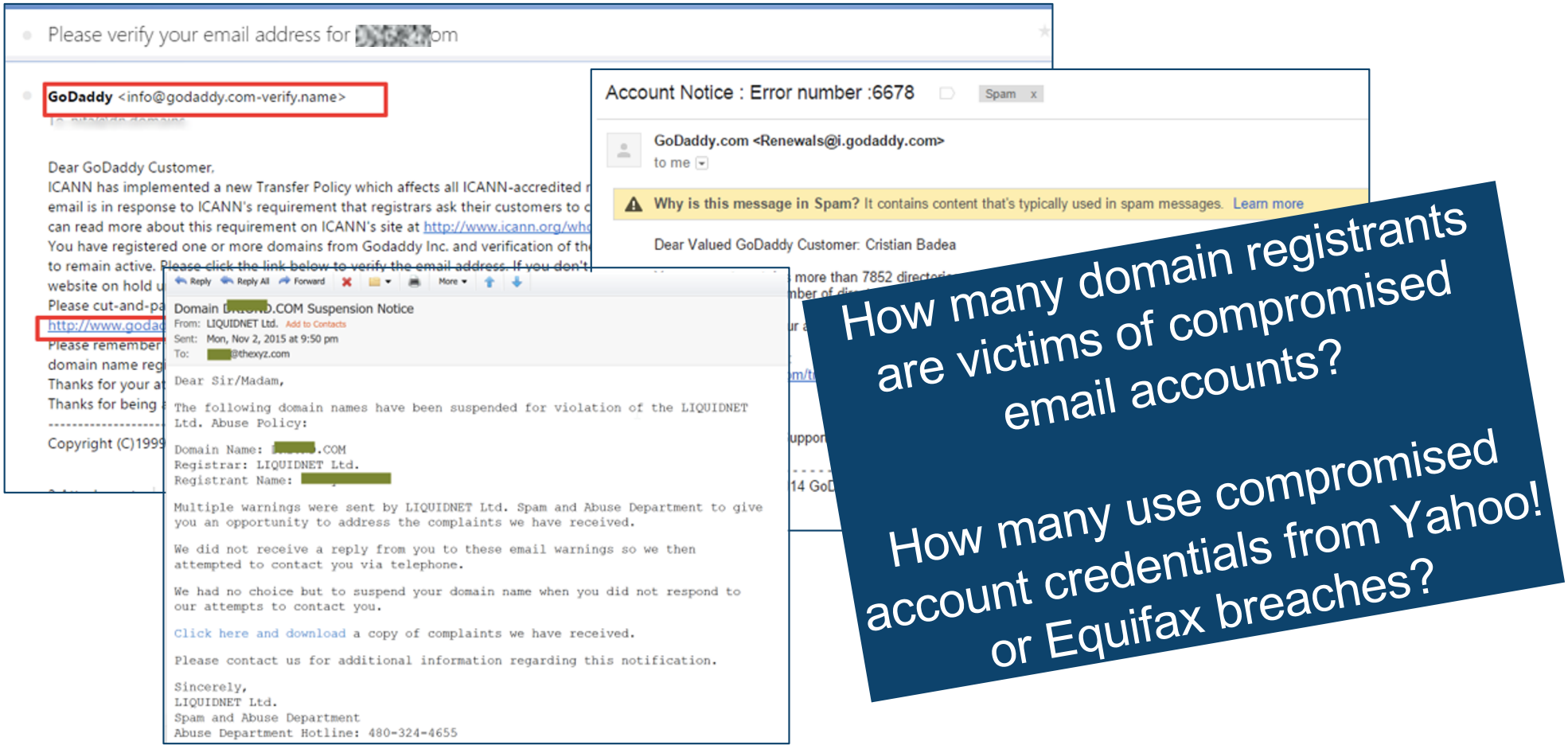
- Name server names for ecrime name resolution
- Names for command-control administration for botnet

Hijacking (theft) is another way that attackers acquire domain names

Why pay if you can crack?

- Attacker gains control of a domain registrar or registry customer account
  - Social engineering
  - Phishing attack
  - Data breach
- Attacker modifies/adds name server record for domain
  - NS record that is published in TLD zone associates domain's name server with IP address of attacker's host
- Attacker publishes "attack" zone data
  - Resource records in zone data support phishing, fraud, or defacement sites, spam mail exchanges, VoIP servers…

Criminals exploit registrar email correspondence (Phishing)



Solution/Defense Space

Defend your own DNS by using a registrar with security features

- Two-factor authentication
- DNS name locking services
- Support for DNSSEC

Other factors: Dedicated support lines, escalation paths, clear anti-abuse policies…

DNS is a critical element of your network. So, when purchasing do the same due diligence you would as when purchasing other critical services.

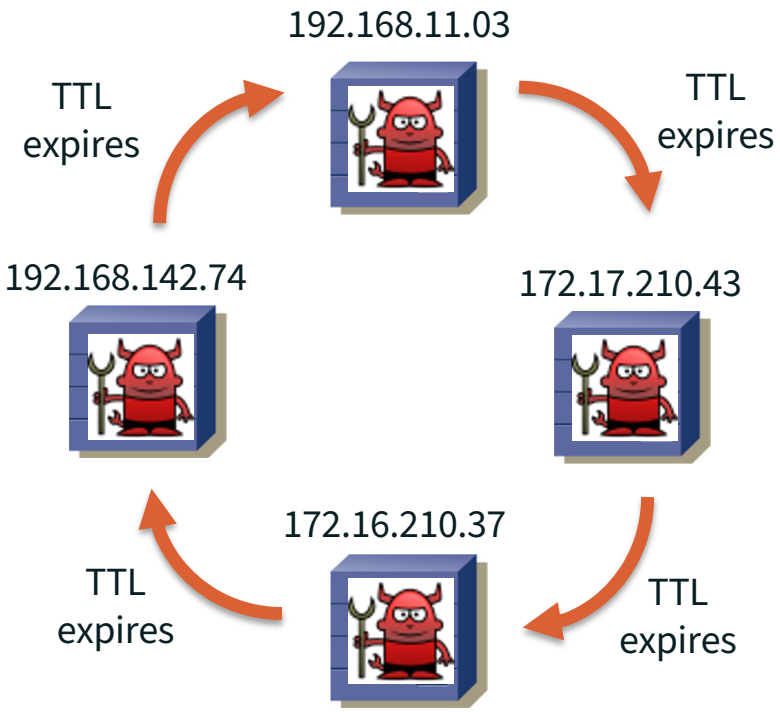
Using the DNS to evade, obfuscate, and make networks agile

Fast flux

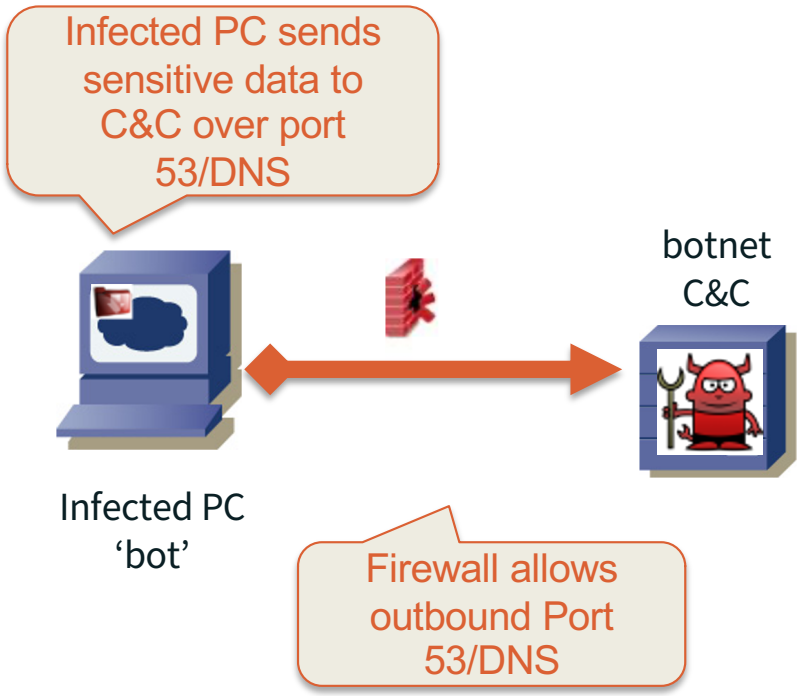
- Attacker associates IP address with a web proxy or name server for short time to live (TTL)
- Attacker changes IP of host or name server at low TTL frequency to thwart investigators

Double (fast) flux

- Apply fast flux technique to both web proxy and name server



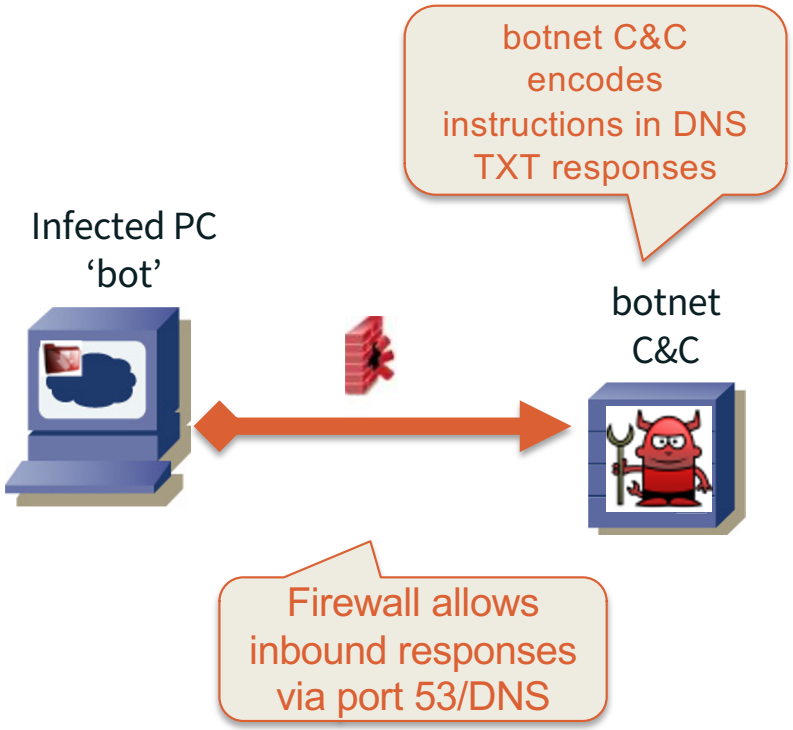
DNS as a Covert Exfiltration Channel



- DNS messages manipulated to forward sensitive data from infected PC *through firewall* to botnet command and control (C&C)
- Proof of concept: exfiltrate results of SQL injection attacks

https://www.forcepoint.com/blog/security-labs/udpos-exfiltrating-credit-card-data-dns

DNS as a Covert Malware Channel



- Malware on infected PC performs TXT lookups to botnet C&C
- TXT responses contain instructions for bot
- Examples in wild:
  - Feederbot
  - Morto

https://www.techrepublic.com/blog/it-security/morto-not-your-average-creepy-crawly-worm/

Agenda

- What is DNS Abuse? DNS Misuse?
- Examples of DNS Abuse or Misuse
- Evolving DNS Threat Landscape
- Abuse in an ICANN Context

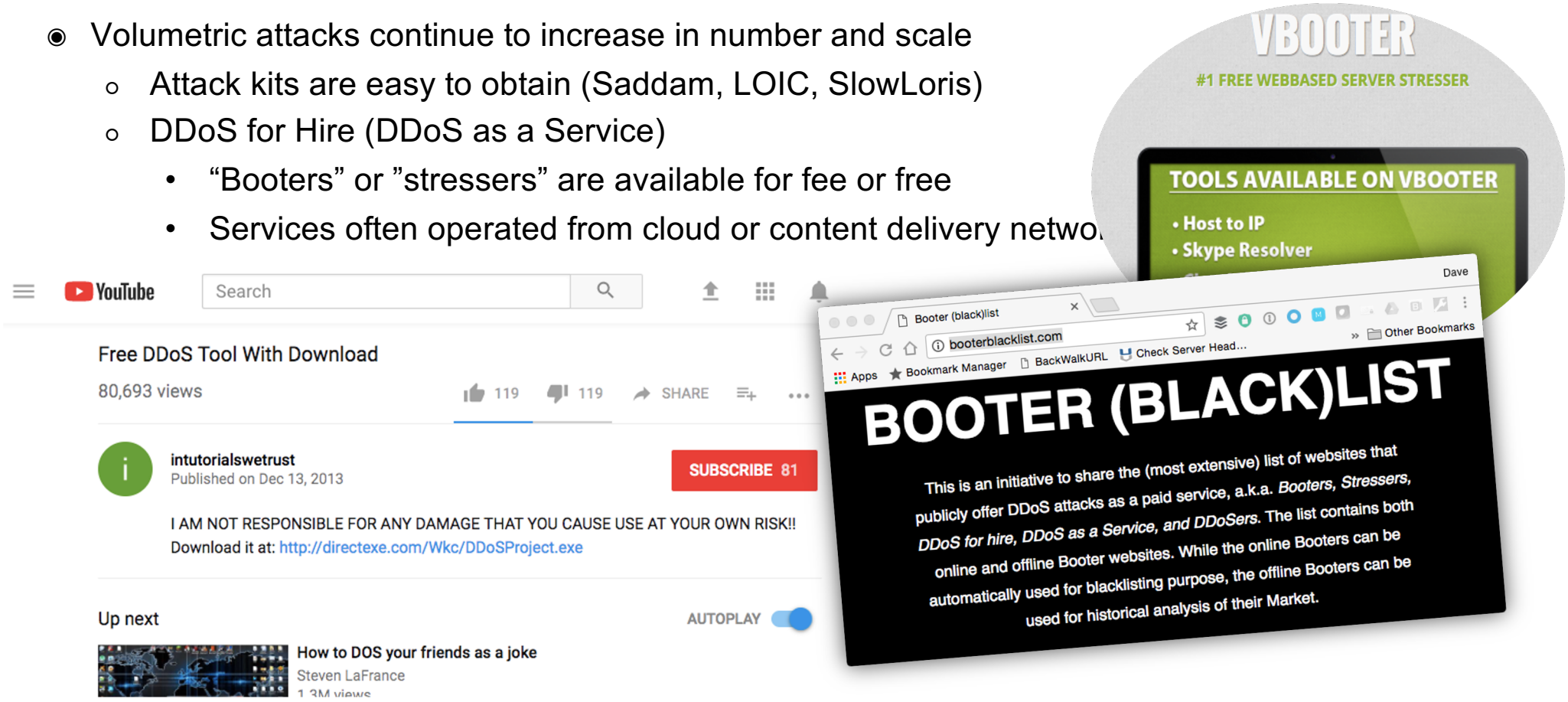
The outlook gets grimmer and grimmer, every day…

- More and better botnets
  - DDoS as a Service?
  - Fast-flux, double-flux redux!
  - Spam as a cloud service
  - Example: Avalanche malware and DNS hosting infrastructure
- Internet of Vulnerable Things
  - Botnet recruitment to next level
  - Example: Mirai malware capable of IP, TCP, UDP, DNS volumetric attacks
- DNS: “Ignition key” or “kill switch” for emerging class of attacks?
  - Example: Wannacry, Wannacrypt

https://www.flickr.com/photos/roach/

Do you really wannacry? DDoS Kits and Services

- Volumetric attacks continue to increase in number and scale
  - Attack kits are easy to obtain (Saddam, LOIC, SlowLoris)
  - DDoS for Hire (DDoS as a Service)
    - “Booters” or ”stressers” are available for fee or free
    - Services often operated from cloud or content delivery netwo

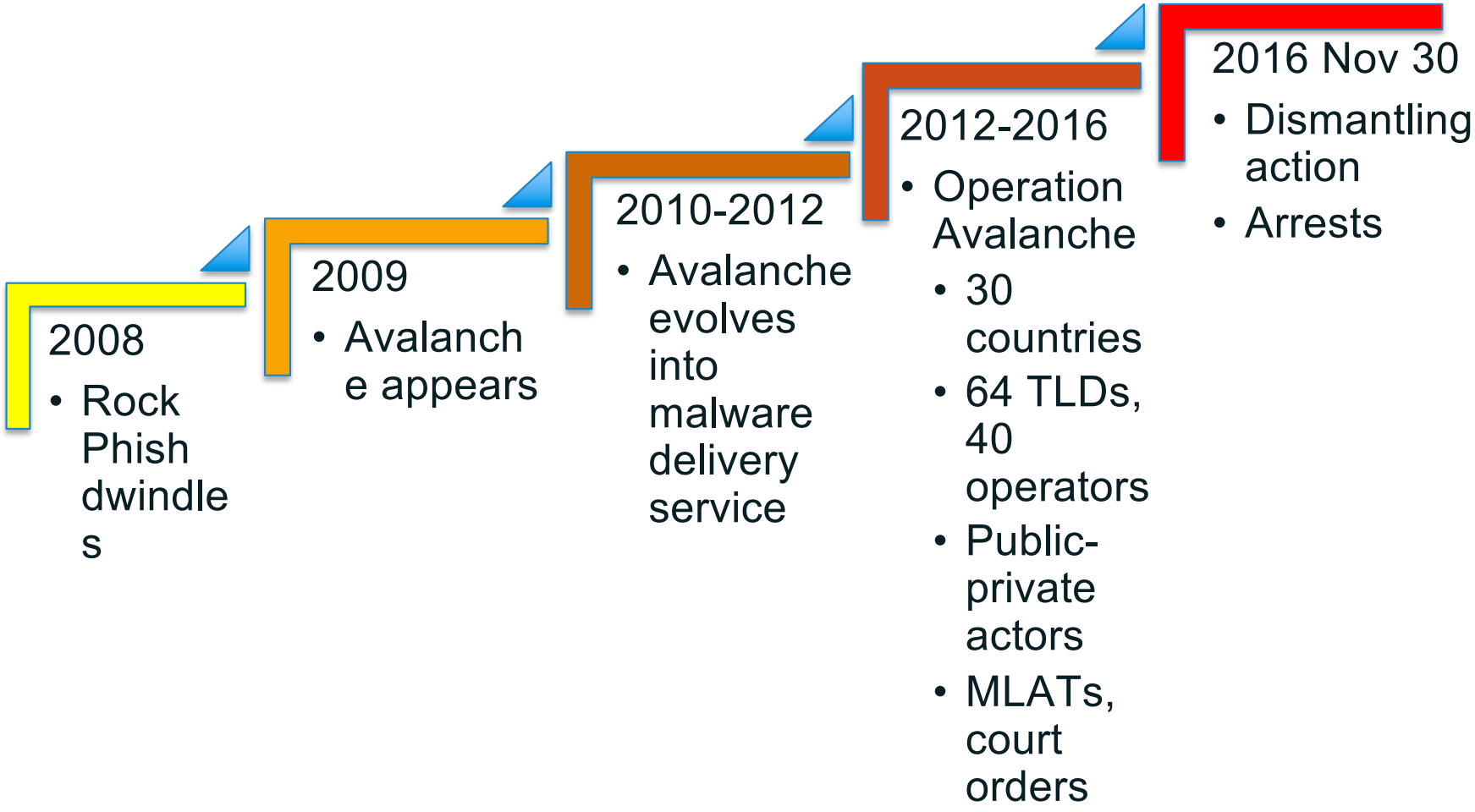


Avalanche malware and DNS hosting infrastructure

- Criminal malware and DNS hosting infrastructure
  - Evolved from botnet to malware delivery service
  - Bulletproof hosting used double fast-flux
  - Predominantly used for financial fraud attacks
- Avalanche offered a “cloud customer experience”
  - Criminal domain registrations
  - Access to a C2 server and service assets (bots)
  - Choice of Malware: 20 families available

Andromeda	Nymaim	Carberp	KBot / Bolek	Panda Banker
CoreBot	Ranbyus (.tw)	Doc-Downloader	Rovnix	Dofoil
Slempo	GOZI2	Teslacrypt	GozNym	Trusteer App
KINS	URLZone	Marcher	VawtrakMatsnu	Xswkit

Avalanche Timeline



Attackers operate at Internet pace

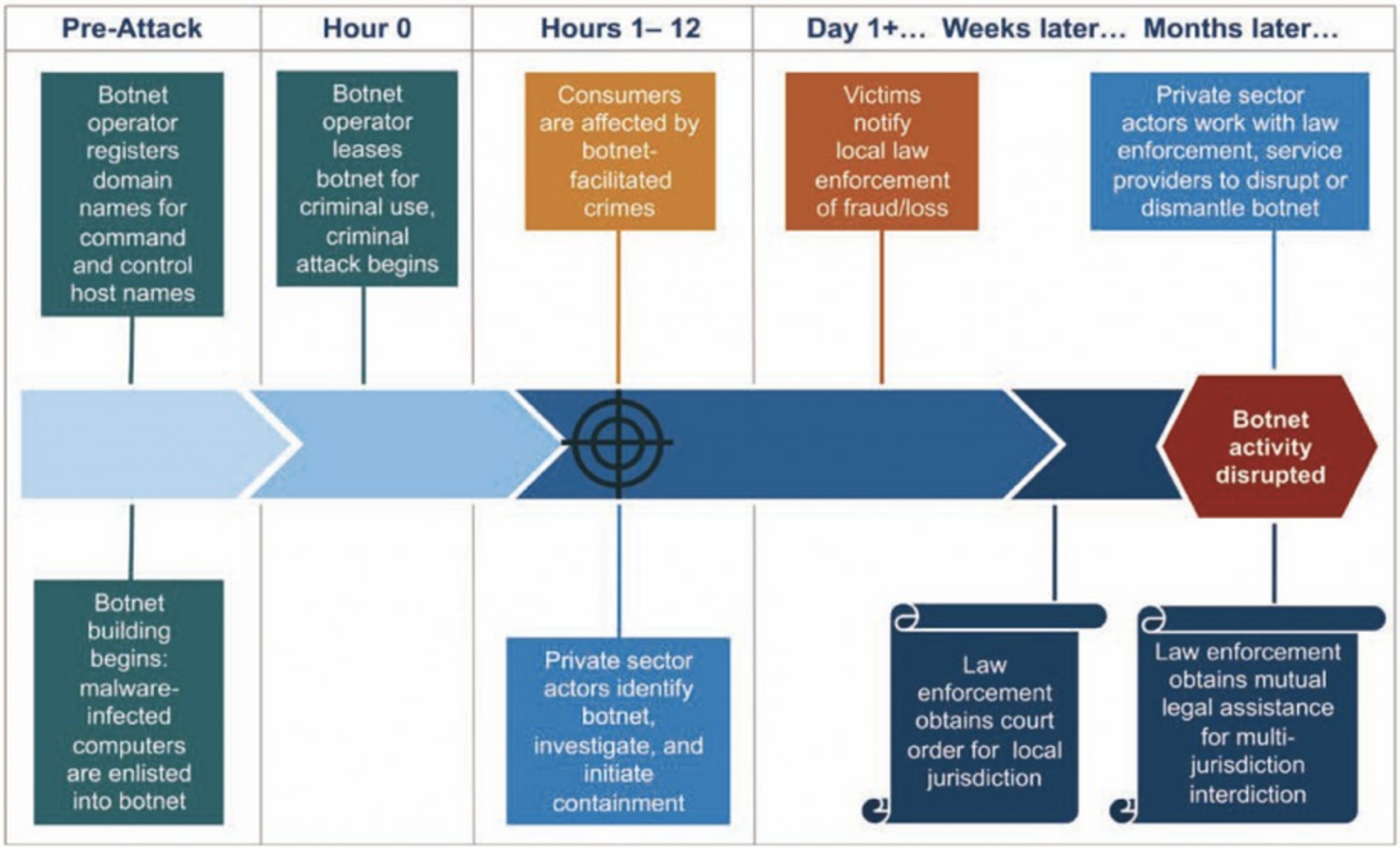


Figure 2. Representative Timeline for A Botnet-Enabled Criminal Attack

Avalanche Outcome

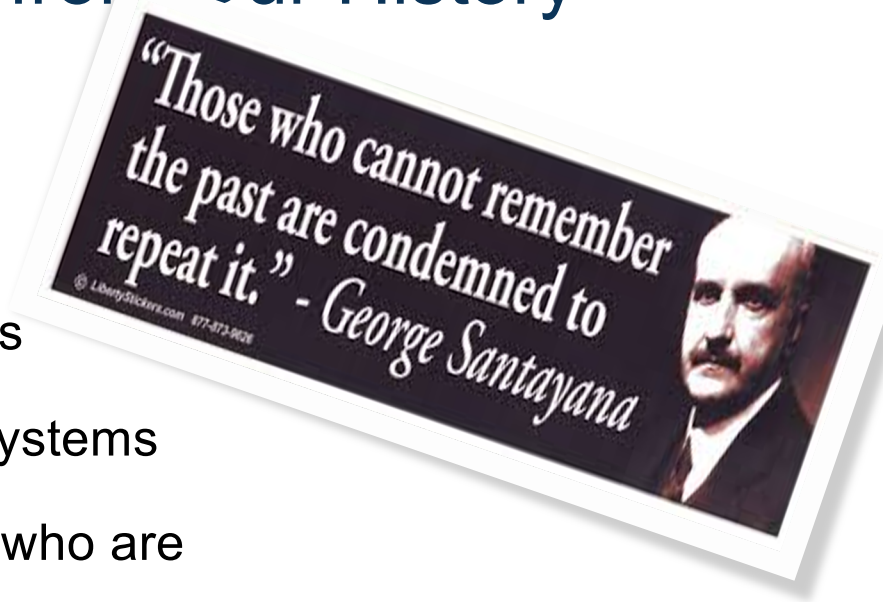
Avalanche Outcome

Andromeda was a direct follow up to Avalanche

https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

Mirai: A Lesson in Not Learning from Our History

History shows that we introduce new attack vectors with each new technology wave



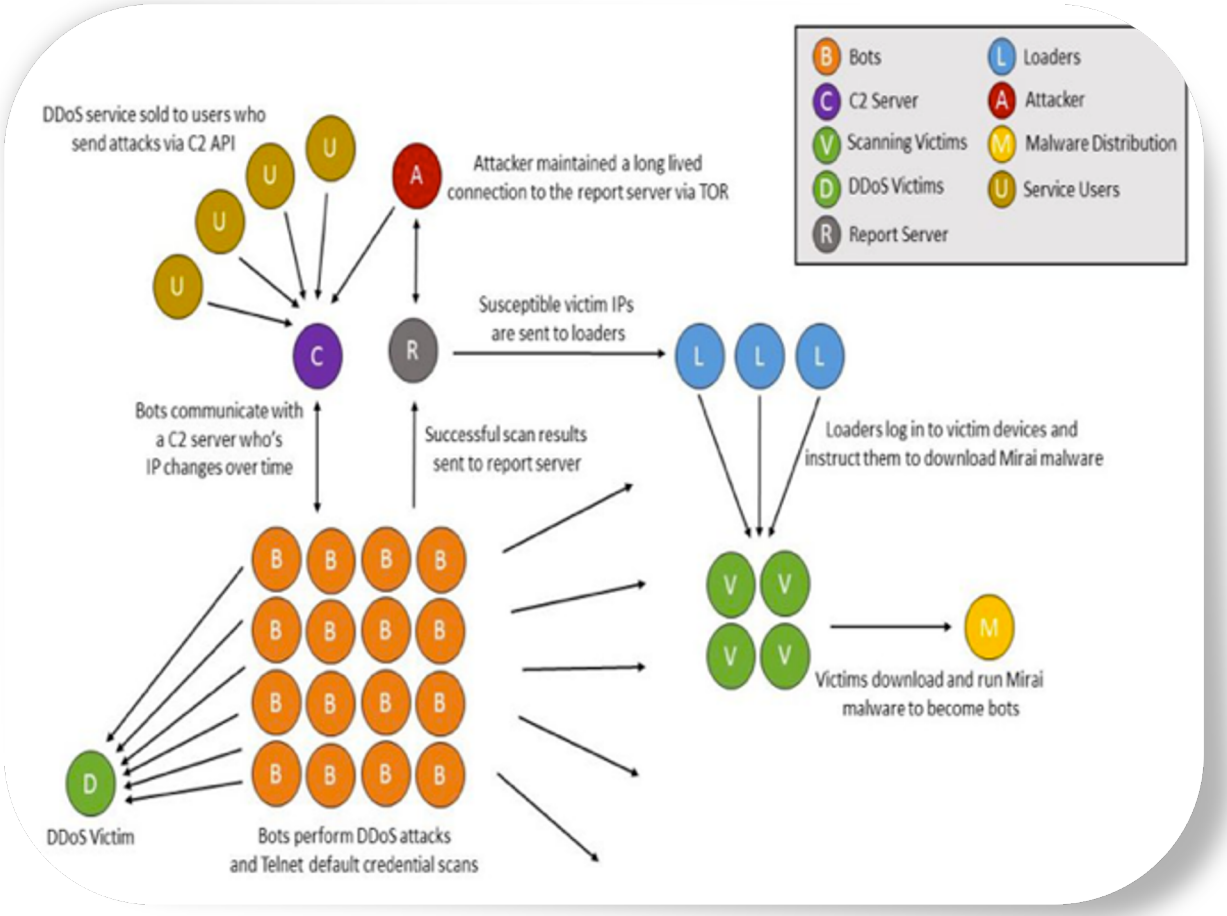
- New/custom OSs, streamlined software, apps
- Modifications to general purpose operating systems
- New actors: a new generation of developers who are *unfamiliar with vulnerability history*
- New actors fall prey to errors of prior generations of developers, e.g.,
  - Lax configurations
  - Little consideration for security or data protection

Mirai: Example of Exploitation of Known Vulnerabilities

"Vulnerable IoT devices are subsumed into the Mirai botnet by continuous automated scanning for and exploitation of **well-known,hardcoded administrative credentials** present in the relevant IoT devices.

These vulnerable embedded systems are typically listening for inbound telnet access on TCP/23 and TCP/2323."

Roland Dobbins, Arbor Networks



http://blog.level3.com/security/grinch-stole-iot/
https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/

Warning bells Mirai rings for us all

- Mirai characteristics expose many IoT security issues
  - A botnet that is largely comprised of IoT devices
  - The compromised devices use plain text channels that have long been regarded as unsecured and removed from use in previous waves of technology
  - The default credentials for these services are known and shared
  - The devices can be re-purposed for many kinds of attacks
- An IoT-populated botnet: DDOS as a service to a new level

Wannacry, Wannacrypt Ransomware

January 16: US CERT SMB Vulnerability Advisory

February 10: First infection report

March 14: Microsoft Patch

March 27: Wave #2

May 12: Wave #3

May 13
Researcher discovers and sinkholes unregistered C&C domain

May 13
New Wannacry variant

May 14: Researchers discover and sinkhole second unregistered C&C domain

Kill Switch?

- Malware author may have outwitted himself while attempting to protect code against analysis
  - Suspected intention was to have malware detect sandbox (analysis)
  - Instead, malware on infected computers attempted to connect to Command-Control server
- By registering the domains for sinkholing purposes, the researcher “unknowingly killed the malware”
  - https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

IF my ransomware fails to connect to the C2 then it’s safe to *encrypt* the victim system

ELSE IF

my ransomware does connect to the C2 then exit process to avoid analysis

That’s right… I think… yeah… Ok… coffee

https://www.flickr.com/photos/striatic/

Agenda

- What is DNS Abuse? DNS Misuse?
- Examples of DNS Abuse or Misuse
- Evolving DNS Threat Landscape
- Abuse in an ICANN Context

DNS Abuse in the ICANN policy world

https://www.flickr.com/photos/mypublicjournal/

- ICANN discussions often *touch* on issues relating to “abuse”
  - Deliberations are often heated or controversial
- Topics with highest heat map at ICANN 60
  - Whois accuracy
  - GDPR
  - Public safety
  - Reporting abuse

Government Advisory Committee on DNS Abuse

Beijing GAC communique, April 2013

- **Mitigating abusive activity**—Registry operators will ensure that terms of use for registrants include prohibitions against the **distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law**.
  - https://www.icann.org/en/system/files/correspondence/gac-to-board-18apr13-en.pdf

Hyderabad GAC communique, November 2016

- The GAC would like to remind ICANN that the list of Security Threats in the New gTLD Safeguards is not meant to be exhaustive. In fact, the Security checks Safeguard applicable to all New gTLDs refers to “security threats such as phishing, pharming, malware, and botnets” (emphasis added), which does not exclude other relevant threats. Please describe what analysis and reporting is conducted regarding other relevant threats not listed above, including **spam**?
  - https://www.icann.org/en/system/files/correspondence/gac-to-icann-08nov16-en.pdf

Public Safety Working Group

- Working group reports to and advises GAC on matters of abuse, public safety or public interest policy
- Law enforcement and invited cybersecurity SMEs
- Issues that the PSWG considers
  - GDPR
  - Whois accuracy
  - Carrier Grade Network Address Translation (CGN)
  - Fast Flux
  - DNS Abuse

Consideration of DNS abuse in contractual agreements

Registry base agreement

Specification 6 (4):

- Abuse PoC, malicious use of orphan glue records

Specification 11 (3):

- Registry Operator agrees to perform the following specific public interest commitments…

https://www.icann.org/resources/pages/registries/registries-agreements-en

Registrar Accreditation Agreement (RAA13)

Section 3.18:

- Abuse Point of Contact,
- Duty to investigate reports of abuse: “reasonable and prompt steps to investigate and respond appropriately to any reports of abuse”
- Publish procedures for receipt, handling, and tracking of abuse reports

Section 2.2:

- Abuse/Infringement Point of Contact for Privacy/Proxy Provider
- Publish process or facilities to report abuse of a domain name registration managed by the P/P Provider

- https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

Engage with ICANN

Thank You and Questions

Visit **icann.org**
Email: john.crain@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann