DDoS
History, Trends, Call for Action

Merike Kaeo, CTO
merike@fsi.io

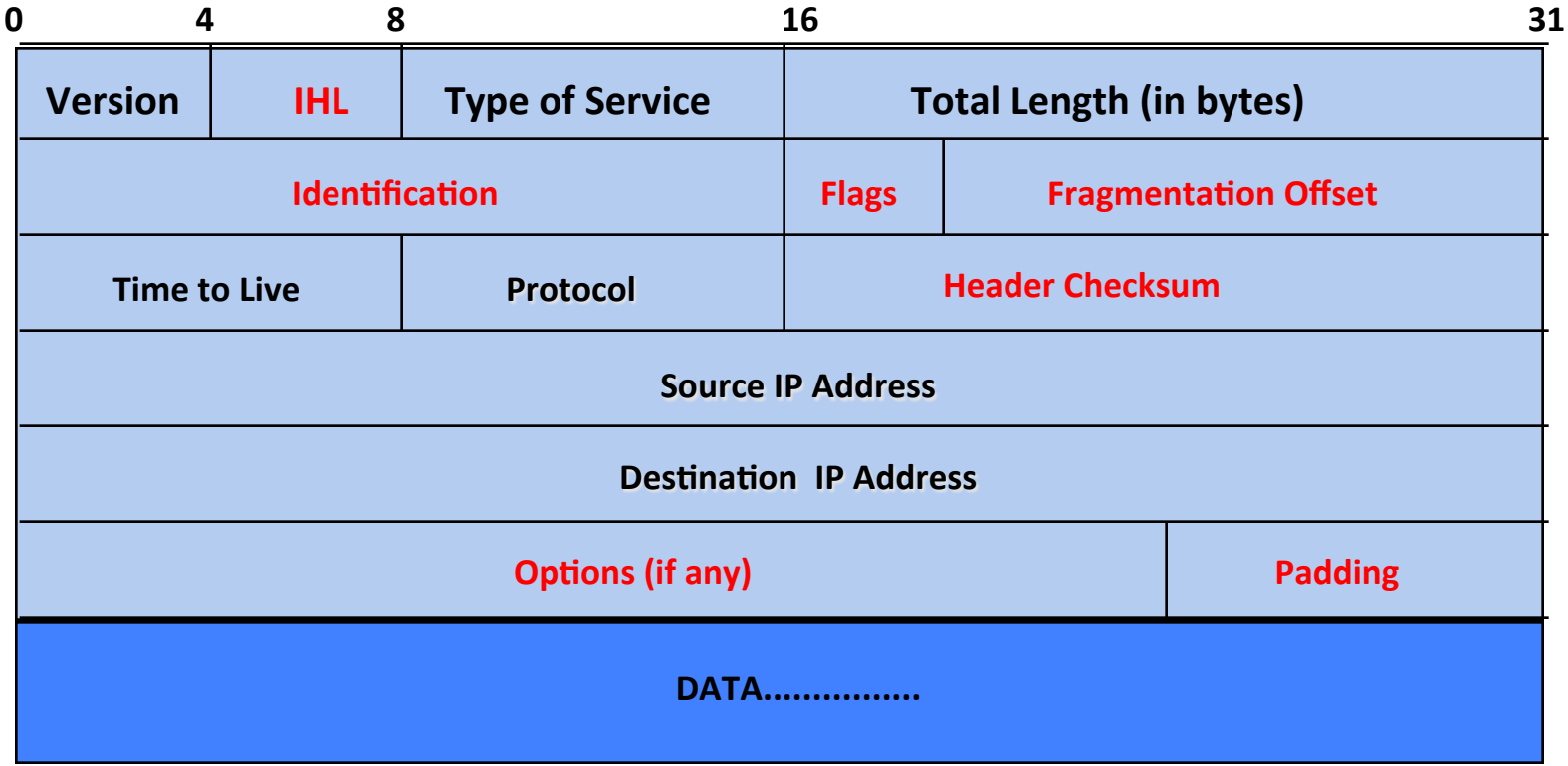
FARSIGHT SECURITY

DISCUSSION POINTS

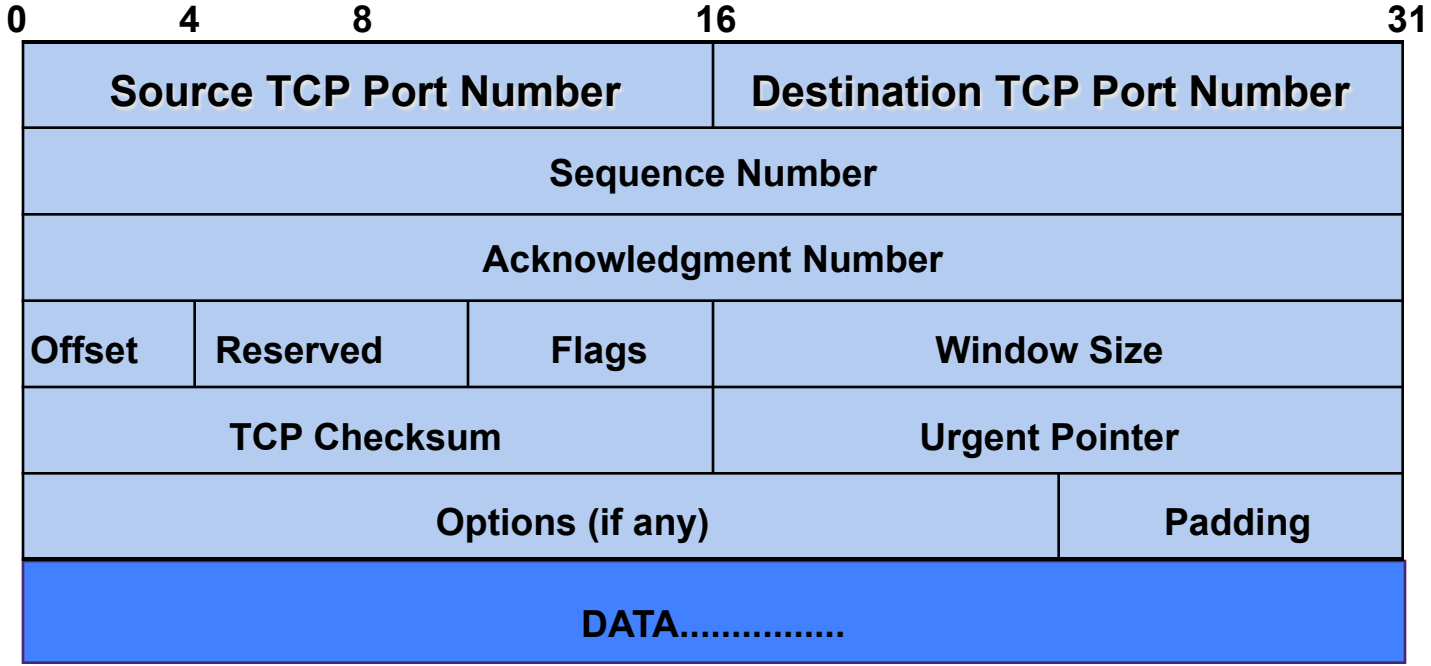
- DoS/DDoS – A Historical View
- Trends in Recent Years
- Mitigation Techniques
- Our Collective Responsibility

IPv4 BASICS

20 octets + options: 13 fields, including 3 flag bits



TCP HEADER



FLAGS:

- URG: indicates urgent data in data stream
- ACK: acknowledgement of earlier packet
- PSH: flush packet and not queue for later delivery
- RST: reset connection due to error or other interruption
- SYN: used during session establishment to synchronize sequence numbers
- FIN: used to tear down a session

IN DDoS EVERYTHING IS FAIR GAME

Internet Layer: basic communication, addressing and routing (IP, ICMP)
Transport Layer: handles communication among programs on a network (UDP, TCP)
Application Layer: end-user applications (NTP, DNS, FTP, etc.)

- Operators should understand fundamental networking behaviors
- Know which devices are communicating and what they are supposed to send and receive

ATTACK MOTIVATIONS

- Greed
- Prank
- Notoriety
- Revenge
- Ignorance
- State Sponsored

WHY DO THESE ATTACKS OCCUR

- Protocols have flaws
- Implementations have bugs
- Implementations have poor default settings
- Operators main focus is transiting customer traffic
- End users are IoT operators but not network engineers
- If someone floods traffic, how do you NOT cause collateral damage to legitimate traffic?

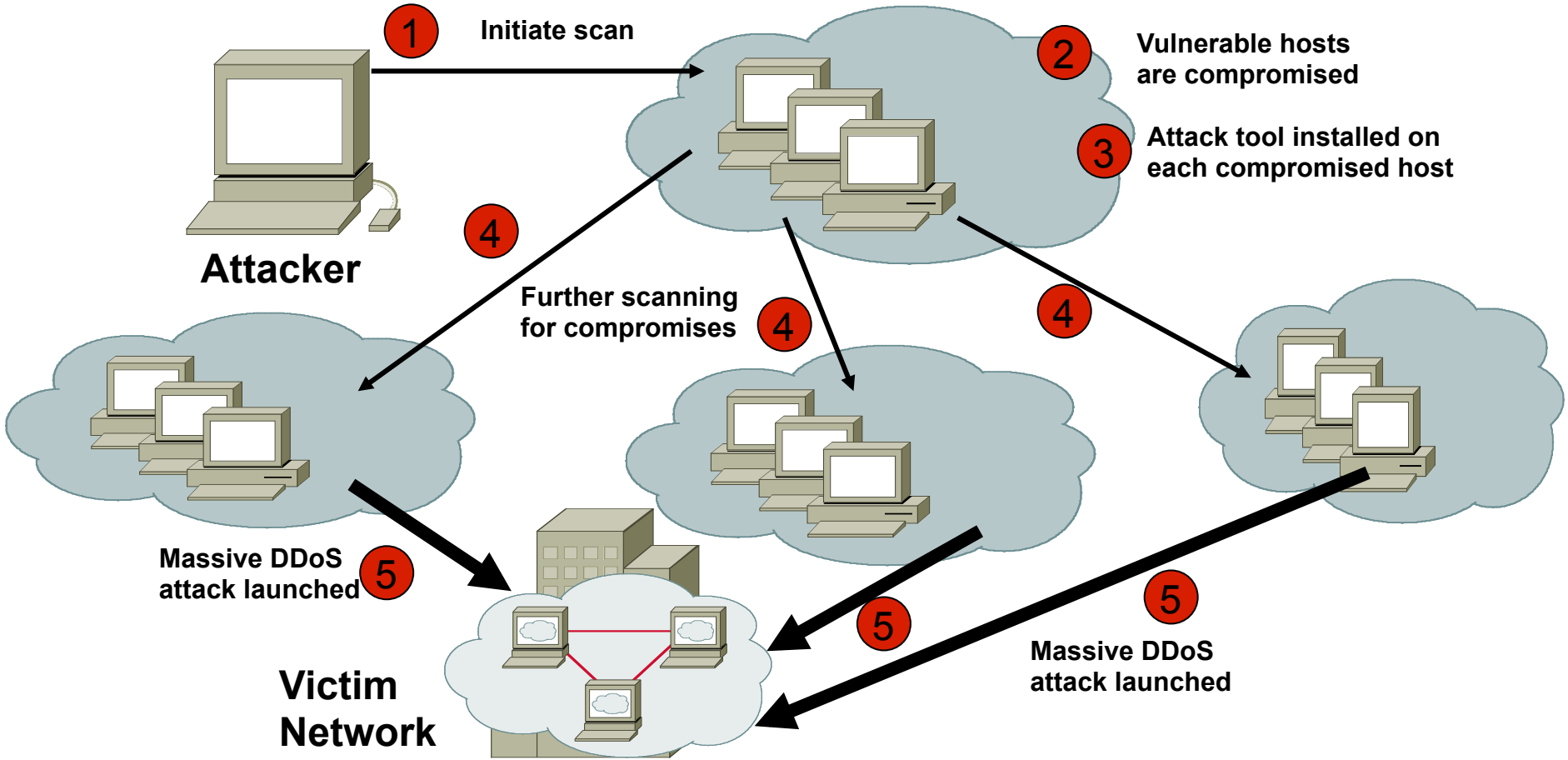
HISTORICAL VIEW: DoS

- Single Machine and relatively unsophisticated
- Ping of Death (1996)
  - Attacker sends ping packet larger than 65,536 bytes
  - Fragmentation would result larger reassembled packet
  - Many operating systems didn’t know how to handle oversized packets and would freeze or reboot
- Land.c (1997)
  - Attacker sends TCP SYN spoofed packet where source and destination IPs and ports are identical
  - When target machine tries to reply, it enters a loop, and repeatedly sends replies to itself eventually causing victim to crash

HISTORICAL VIEW: DoS

- Smurf (1999)
  - Large number of ICMP messages sent using target spoofed source IP address and destination IP broadcast address
  - All machines listening on broadcast address will send replies to target resulting in too many packets to process
- Fraggle
  - Variation of SMURF attack using UDP port 7 (echo) and port 23 (chargen) instead of ICMP
- Teardrop
  - Fragments sent with overlapping fragment offsets and receivers couldn’t process reassembled packets

HISTORICAL VIEW: DDoS



HISTORICAL VIEW: DDoS

- Multiple Machines used to orchestrate attack
- Distributed and automated
- Trinoo (1999)
  - https://staff.washington.edu/dittrich/misc/trinoo.analysis.txt
  - The attacker(s) control one or more "master" servers, each of which can control many "daemons". The daemons are all instructed to coordinate a packet based attack against one or more victim systems.
  - Specific ports are used in communications
  - Utilizes UDP and 'ICMP Port Unreachable' messages

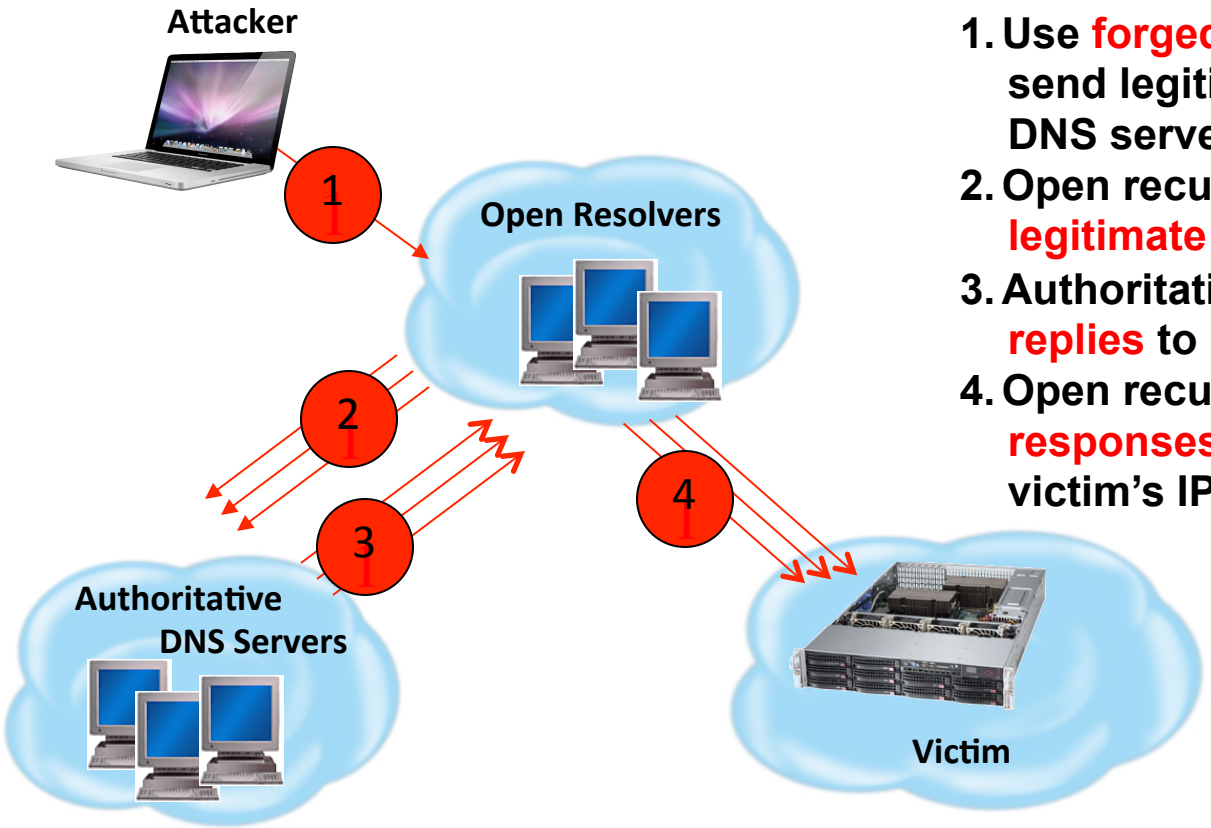
HISTORICAL VIEW: DDoS

- TFN (Tribal Flood Network) (1999)
  - More sophisticated tool that can cause ICMP flood, SYN flood, UDP flood and SMURT-style attacks
  - Communications between attack infrastructures uses ICMP echo and echo-reply packets
  - IP Identification and payload of ICMP echo-reply identify type of attack
  - IP address can be spoofed
- TFN2K (1999/2000)
  - Newer variant of TFN and doesn’t use specific ports
- Stacheldraht (2000)
  - Combines features of Trinoo and original TFN tool
  - It can encrypt communications

THE UNKNOWN – HOW CAN IT HARM YOU?

- Estonia Example (May 2007)
  - Creating ***trust***
    - TC-FIRST
    - Global Operation Security Teams
  - Cross functional meetings
  - Known roles due to e-voting (2005)
  - Government ***facilitated*** communication and tactics
  - Openness with ***information sharing*** was critical
  - A variety of attacks used including Botnet for Hire

DrDoS: DISTRIBUTED REFLECTOR ATTACKS



1. Use **forged IP address** of intended victim to send legitimate queries to open recursive DNS servers.
2. Open recursive DNS servers send **legitimate queries** to authoritative servers.
3. Authoritative servers send back **legitimate replies** to recursive DNS servers.
4. Open recursive DNS server **legitimate responses create massive DDoS attack** to victim's IP address.

DrDoS: NTP

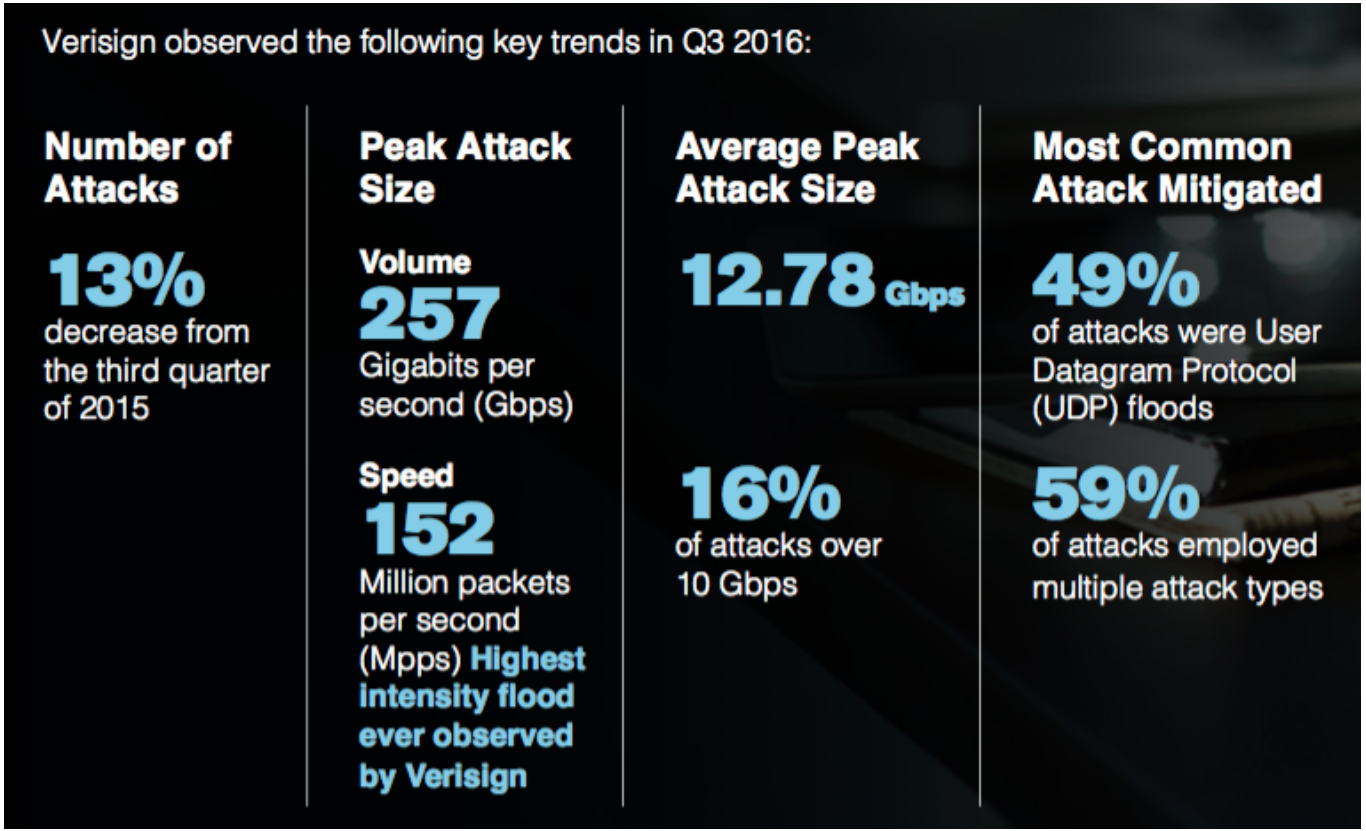
- Feb 2014 – 400Gbps
- NTP includes set of commands for monitoring
- When NTP server receives a ‘monlist’ command it will reply with list of last 600 assets that have interacted with that server
- Amplification of up to factor of 200X
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211

AMPLIFICATION HELL

Protocol	BAF *all*	BAF 50%	BAF 10%	PAF *all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	3.84	Request client statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

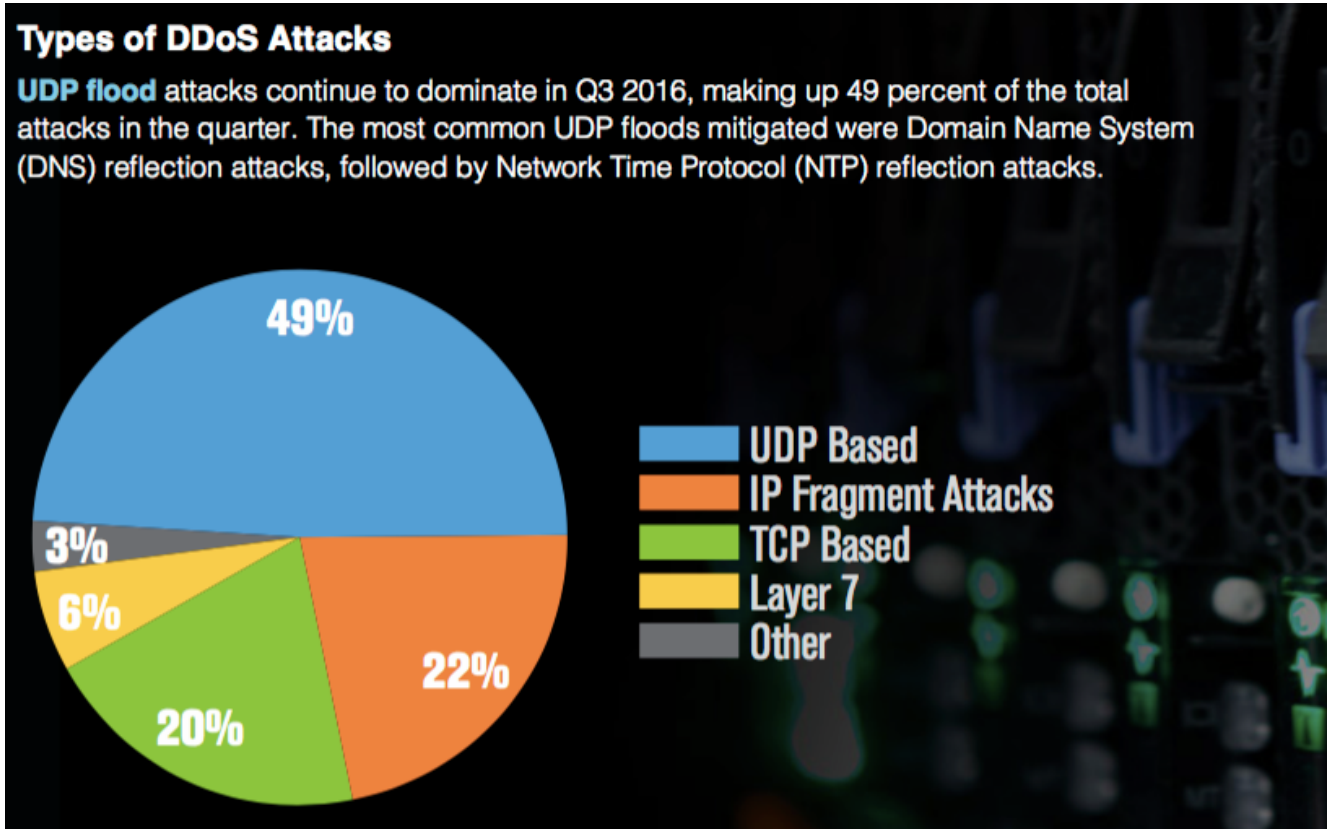
- Abusing Network Protocols for DDoS by Christian Rossow
- BAF: BW amplification factor
- PAF: Packet amplification factor
- Presented at NDSS 2014
- http://www.christian-rossow.de/articles/Amplification_DDoS.php

RECENT TRENDS: SOME STATISTICS



Source: Verisign DDoS Trends Report Q3 2016

RECENT TRENDS: ATTACK TYPES



Source: Verisign DDoS Trends Report Q3 2016

RECENT TRENDS: ATTACK TYPES

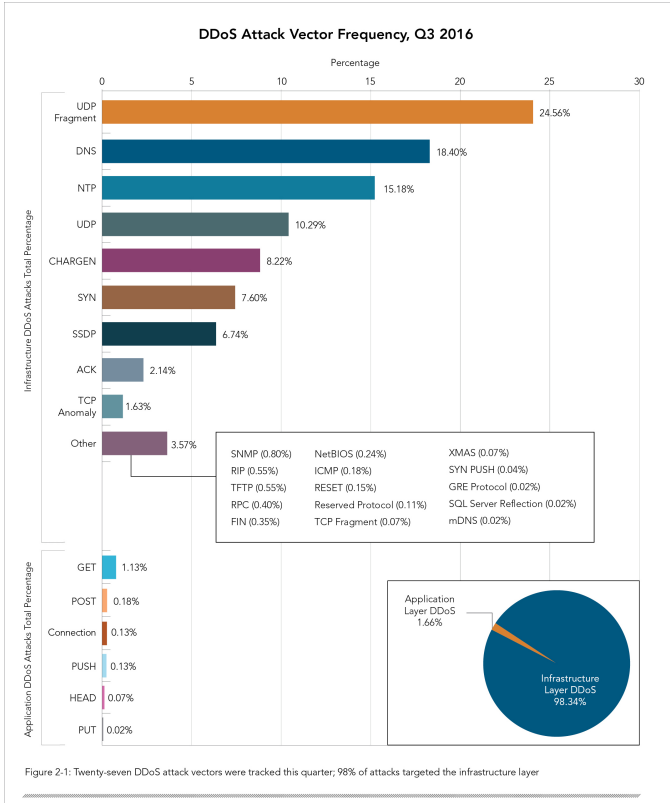


Figure 2-1: Twenty-seven DDoS attack vectors were tracked this quarter; 98% of attacks targeted the infrastructure layer

- UDP fragmentation and DNS reflection continue to be largest portion of DDoS attacks
- NTP and SYN floods still popular

Source: Akamai's [State of the Internet] Security Report Q3 2016

RECENT TRENDS: NTP

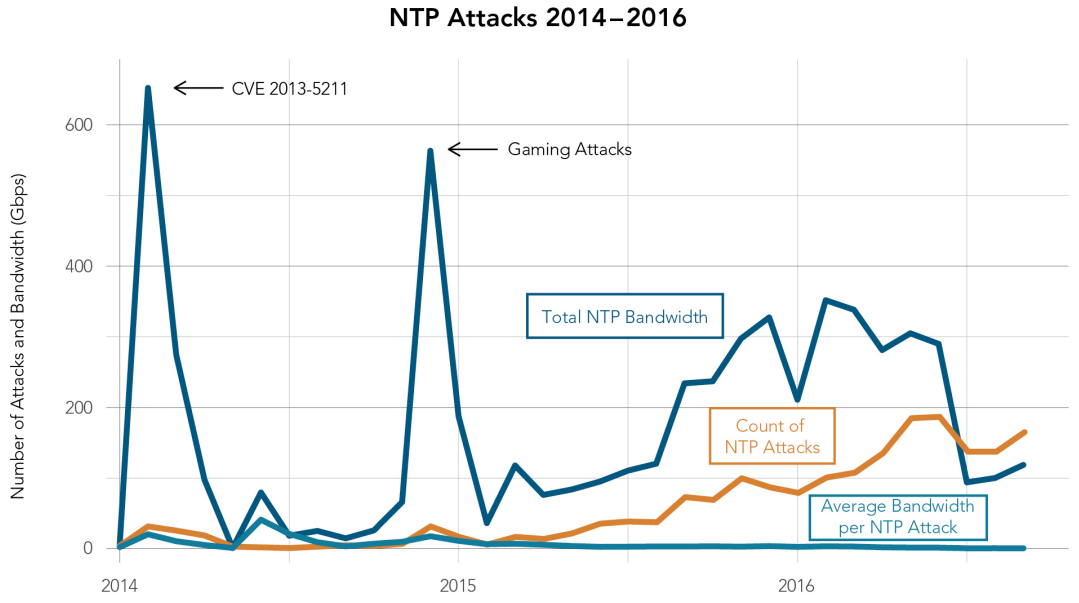


Figure 2-3: The release of the NTP monlist vulnerability caused a huge spike in NTP attack traffic, followed by a concentrated attack on gaming companies in December 2014

- Large spike in 2014 in NTP traffic when vulnerability discovered and sharing information about pools of vulnerable servers
- Large pool of stable but rarely patched systems exist which make for long tail
- Increase in number of botnets using NTP reflection attacks but seem to be pivoting to other protocols

Source: Akamai's [State of the Internet] Security Report Q3 2016

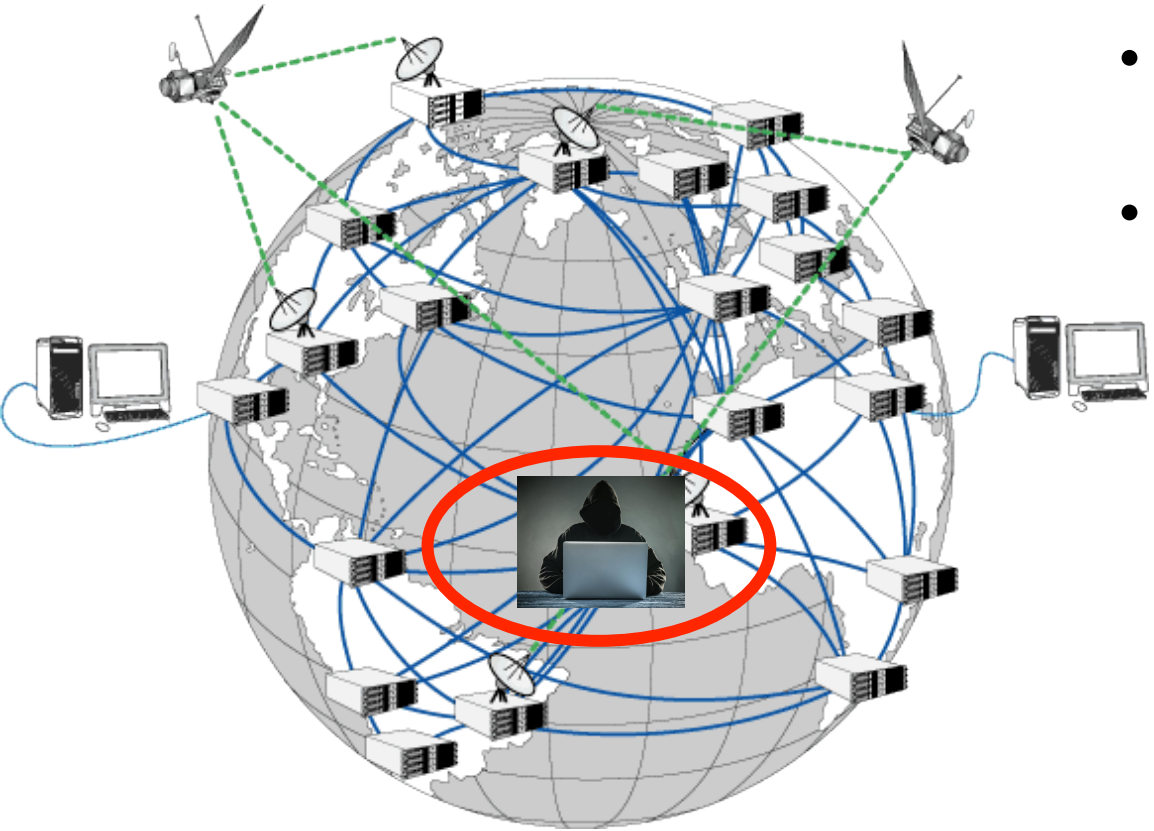
CONTINUING TRENDS

- Attackers will continue to try and change tactics to stay under detection
  - Packet size variations
  - Time of day variations
  - More utilization of encryption
- The bandwidth available for malicious intent will continue to increase
- The number of devices available for exploitation will continue to increase

MIRAI BotNet

- Brian Krebs's website saw 623Gbps Sept 2016
- Dyn was targeted but most heavily on Oct 21, 2016 with possibly over 1Tbps traffic
- Allegedly used to attack telecommunications infrastructure in Liberia with 500Gbps traffic
- Exploits the use of default username and passwords as well as Telnet (other variants exist) in IoT devices

THE NEW NORMAL



- Adhoc Mesh Networks
- Prevalent use of Tunneled Protocols
- “There’s an App for That”

A PERIOD OF RAPID CHANGE

- Intelligent, interconnected devices are continuing to be connected to the global Internet
- Data is accumulating faster than it can be organized or effectively protected
- The complexity of the Internet ecosystem creates a rich environment exploitable by activists, criminals, and nation states
- Data will continue be stolen or modified using subtle, persistent, directed attacks

DO YOU UTILIZE IPv6?

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

IPv6 CIDR Report

Status Summary

Table History

Date	Prefixes	CIDR Aggregated
06-09-16	32388	22859
07-09-16	32474	22892
08-09-16	32521	22935
09-09-16	32546	23001
10-09-16	32592	23015
11-09-16	32613	23007
12-09-16	32605	23003
13-09-16	32588	23003

This report is generated from an analysis of the BGP routing table within AS2.0 (APNIC), and was produced at Tue Sep 13 05:45:24 2016 AEST.

Status Summary

Table History

Date	Prefixes	CIDR Aggregated
08-01-17	34823	24375
09-01-17	34828	24377
10-01-17	34813	24394
11-01-17	35051	24481
12-01-17	35198	24420
13-01-17	35180	24466
14-01-17	35254	24465
15-01-17	35264	24465

This report is generated from an analysis of the BGP routing table within AS2.0 (APNIC), and was produced at Sun Jan 15 08:45:23 2017 AEST.

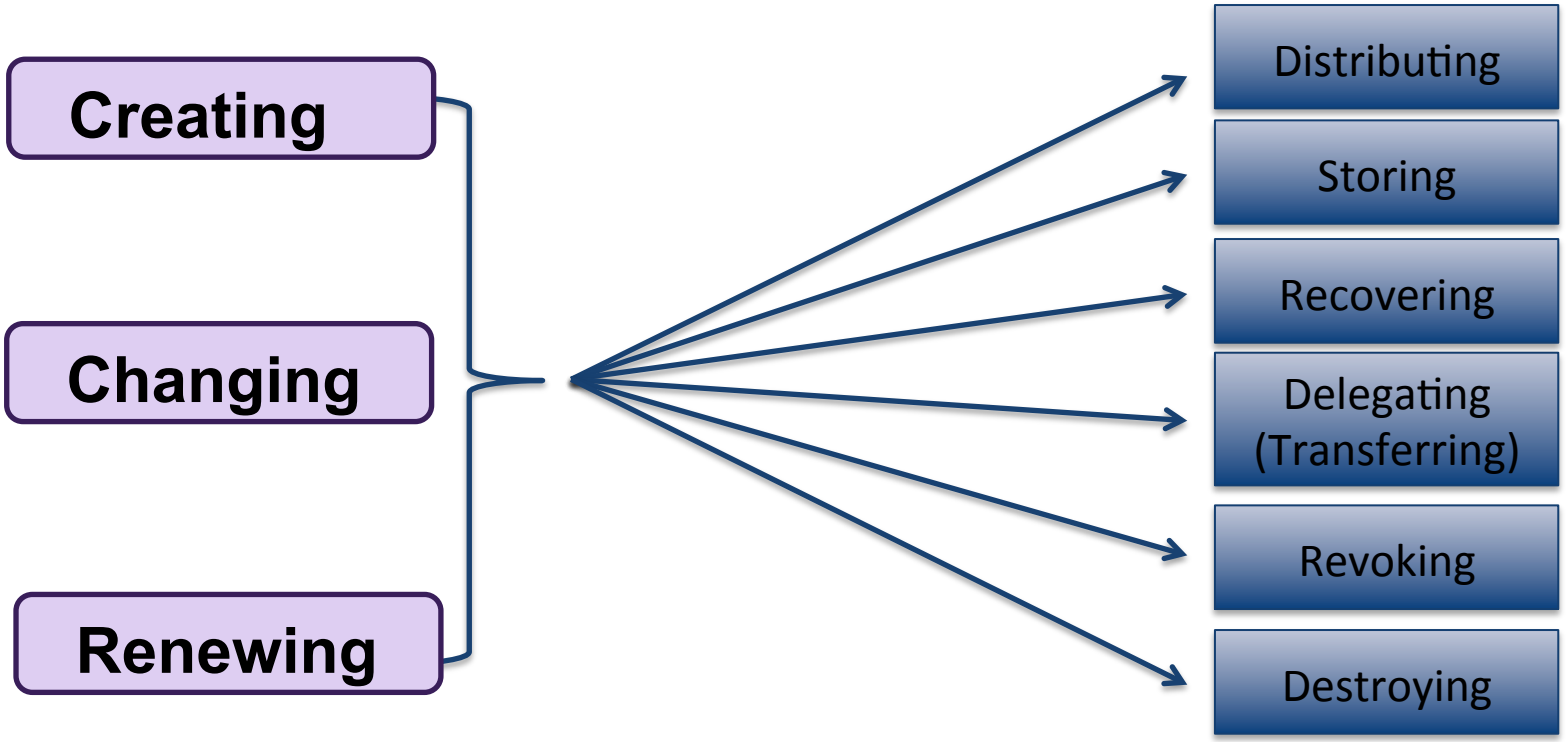
GENERAL GOOD HYGIENE

- Have Sufficient BW to Absorb Attack
- Filter Unwanted Traffic
- Rate Limit
- Effective Logging and Alerting Mechanisms
- Log, Collect and Correlate Attack Data
  - SHARE DATA with trusted folks
- Create and Maintain Redundancy of Infrastructure
- Pay Attention to Credential Management Lifecycle
- Define Minimum Security Feature Set From Vendors

CREDENTIAL COMPROMISE IS DDoS ENABLER

- Being victim of a phishing attack
- Laptop gets stolen
- Sharing your password with another person
- Re-using same password on many systems
- Spyware on your computer installed a keylogger
- Storing your private key in an easily accessed file
- Sending credentials in cleartext emails
- Unpatched security vulnerabilities are exploited

CREDENTIAL MANAGEMENT LIFECYCLE



- Know ALL credentials used in your environment
- Encourage multi-factor authentication

MITIGATION: DNS RECURSIVE RESOLVERS

- Ensure no unmanaged open recursive resolvers exist
  - Equipment vendors need to ship default as closed
  - BCPs should not show recursive resolver configurations as open
- Test to determine whether you have unmanaged open recursive resolvers in your environment
  - http://www.thinkbroadband.com/tools/dnscheck.html
  - http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl

MITIGATION: IP ADDRESS SPOOFING

- Everyone needs to play their part with source address validation efforts
- ISPs need to do ingress filters
  - BCP38(RFC2827) / BCP84 (RFC3704)
- Enterprises/SMBs need to implement egress filters
- Equipment vendors need to have better defaults

MITIGATION: TEST FOR KNOWN DDoS VECTORS

- Determine whether you allow IP address spoofing
  - https://spoofer.caida.org
  - https://www.nanog.org/sites/default/files/20161018_Kristoff_Security_Track_v1.pdf
- Determine whether you are susceptible to the NTP MODE 6 and MONLIST MODE 7 responses
  - http://openntpproject.org
- Determine whether you have unmanaged open recursive resolvers in your environment
  - http://www.thinkbroadband.com/tools/dnscheck.html
  - http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl

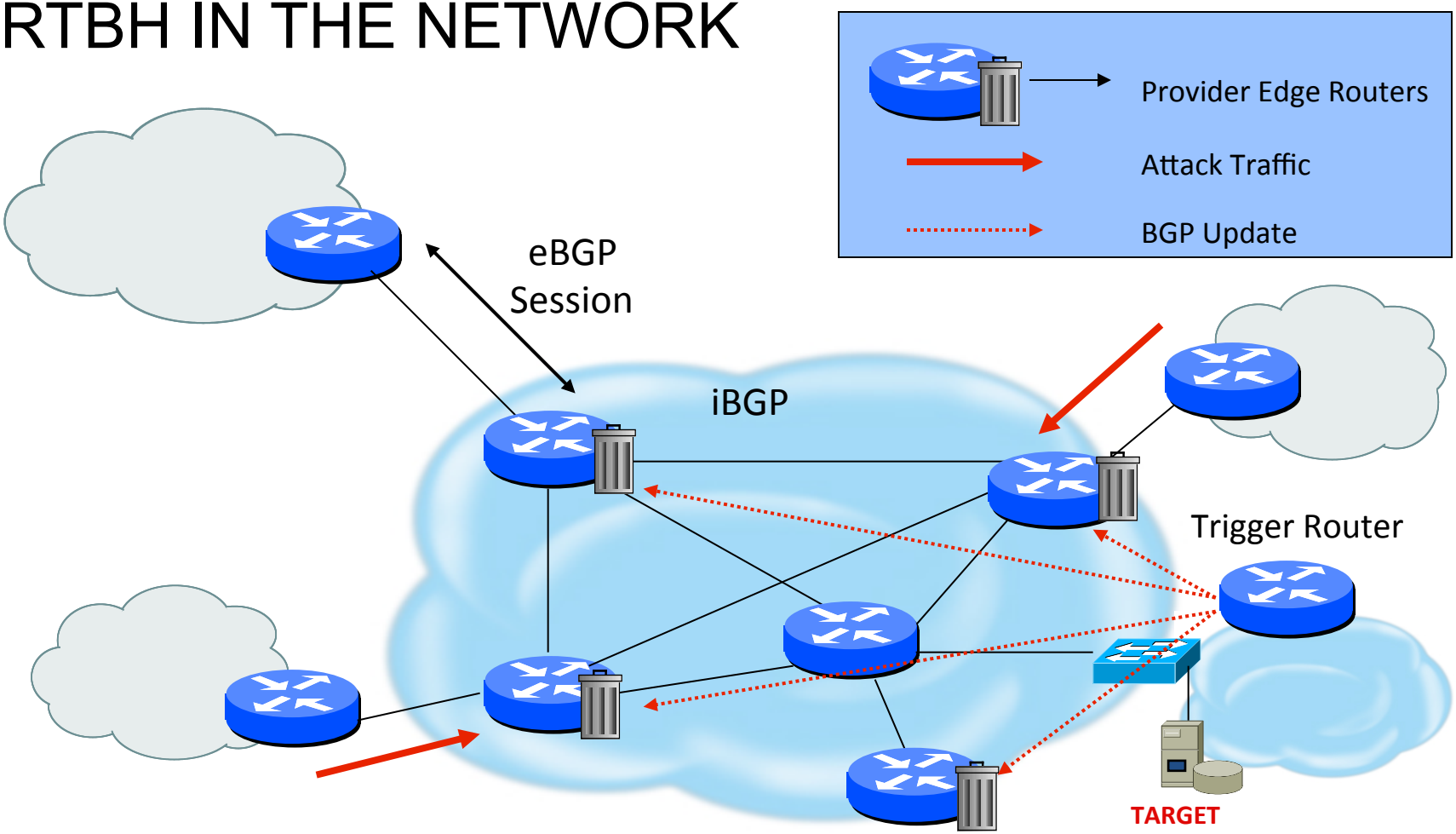
MITIGATION HOMEWORK

- Experience from using uRPF
  - Draft-savola-bcp84-urpf-experiences-03.txt
- Securing the Edge (SAC004 – Oct 2002)
  - https://www.icann.org/en/system/files/files/sac-004-en.pdf
- Advisory on DDoS Attacks Leveraging DNS Infrastructure (SAC065 – Feb 2014)
  - https://www.icann.org/en/system/files/files/sac-065-en.pdf
- RIPE Anti-Spoofing Task Force How-To (May 2008)
  - http://www.ripe.net/ripe/docs/ripe-431
- Team CYMRU Configuration Templates
  - http://www.team-cymru.org/templates.html

MITIGATION: UTILIZING RTBH

- Use BGP routing protocol to trigger network wide response to an attack flow
- Simple static route and BGP allows ISP to trigger network wide black holes as fast as iBGP can update network
- Unicast RPF allows for the black hole to include any packet whose source or destination address match the prefix
- Effective against spoofed and valid source IP address

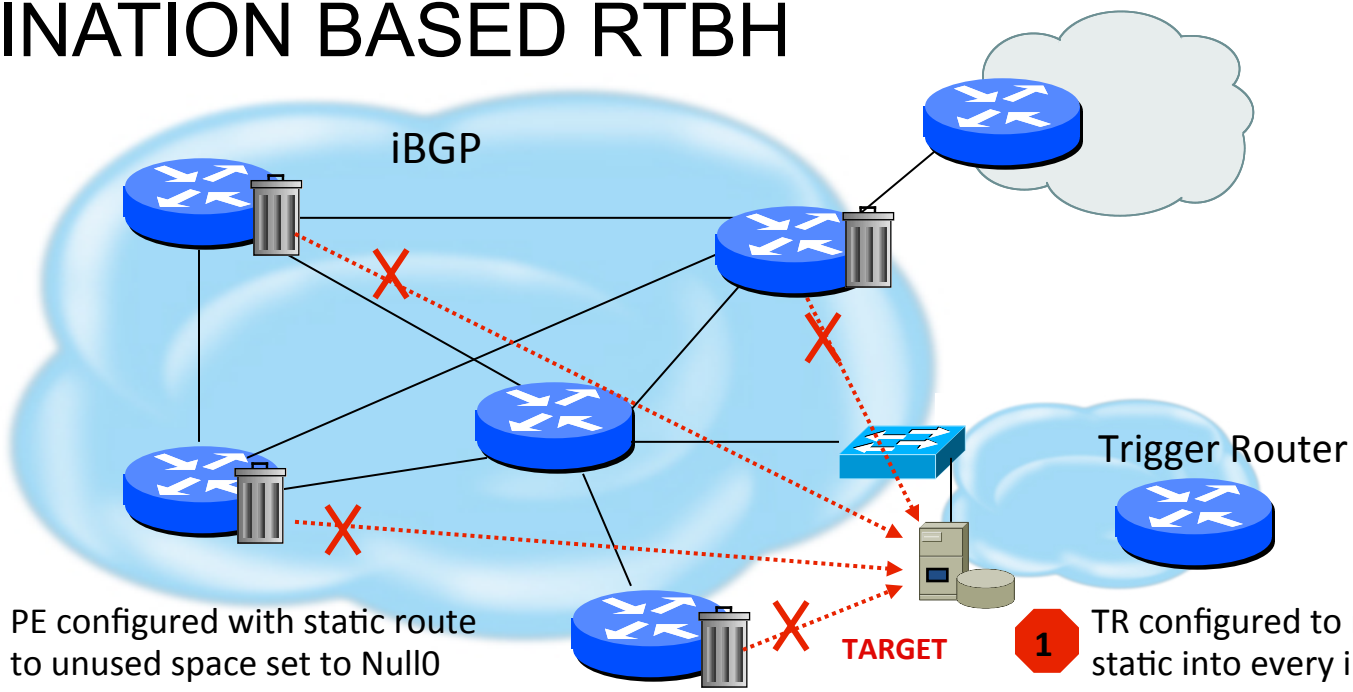
RTBH IN THE NETWORK



DESTINATION BASED RTBH

Steps:

1. **Preparation**
2. **Trigger**
3. **Withdrawal**



1. PE configured with static route to unused space set to Null0 (192.0.2.6/32 set to Null0)
2. Receives iBGP update which states next hop for target is 192.0.2.6/32
3. Installs new (valid) route to target

NOTE: All traffic to the target is dropped, even legitimate traffic

1. TR configured to redistribute static into every iBGP peer
2. Add static route which sets next hop to target destination (192.0.2.6)
3. Manually remove static route which causes BGP route withdrawl

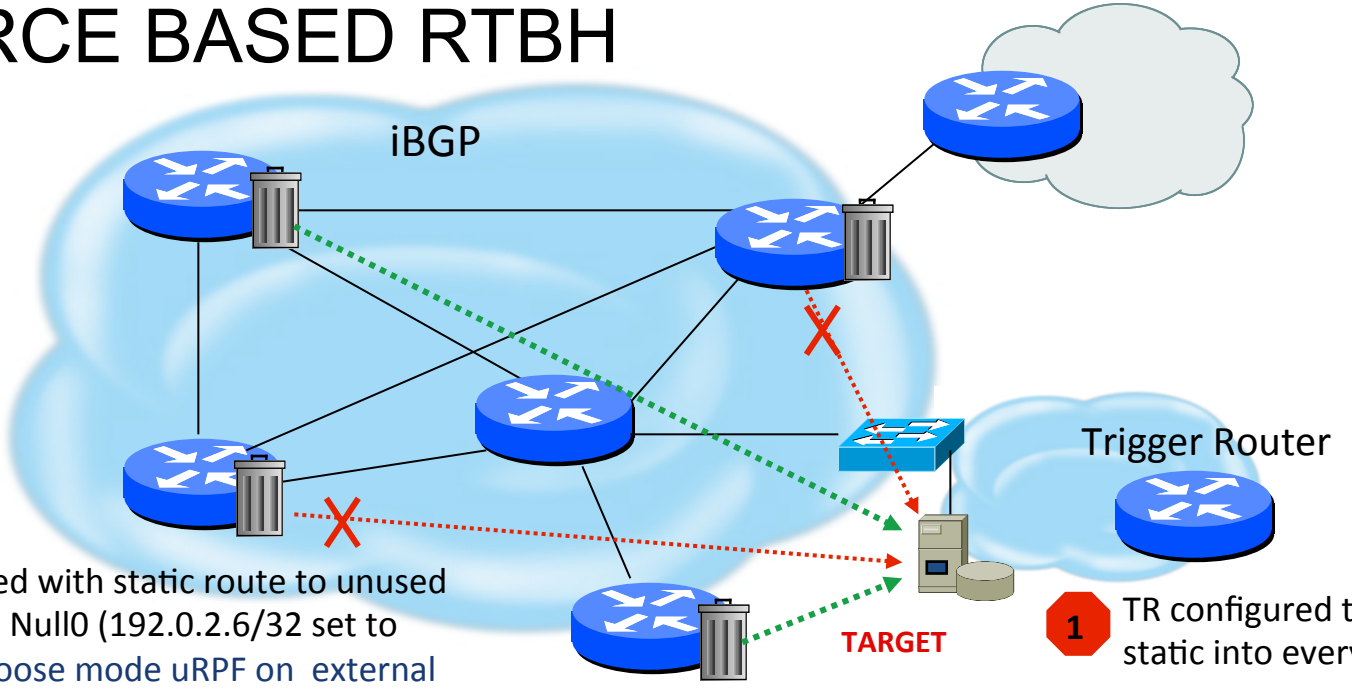
SOURCE BASED RTBH

- Ability to drop packets at network edge based on specific source IP address
- Permits legitimate traffic from reaching target destination
- Depends on Unicast RPF
- Packet dropped if:
  - Router has no entry for source IP address
  - Source IP address entry points to Null0

SOURCE BASED RTBH

Steps:

1. **Preparation**
2. **Trigger**
3. **Withdrawal**



1. PE configured with static route to unused space set to Null0 (192.0.2.6/32 set to Null0) and loose mode uRPF on external interfaces
2. Receives iBGP update which states next hop for target is 192.0.2.6/32. All traffic from source IP will fail loose uRPF check.
3. Installs new (valid) route to target

NOTE: Only traffic from the attack sources get dropped

1. TR configured to redistribute static into every iBGP peer
2. Add static route which sets next hop to target destination (192.0.2.6)
3. Manually remove static route which causes BGP route withdrawal

SHARING - CRIMINALS HAVE NO BARRIERS

- Websites advertise Botnets and malware for hire
- Vulnerabilities and Exploits are traded on open market
- There are no enforced rules for NOT sharing
- Social media is making sharing more efficient

Choose Custom Botnet

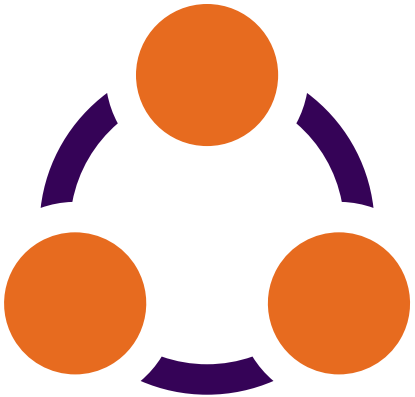
- Number of Hosts
- Geographic Region
- Bandwidth
- Duration
- etc

CONTINUE TO INCREASE SHARING

- Initial Step – Build Trust Thru Networking
- Start by sharing for specific use cases that don’t impact privacy and personally identifiable information (PII)
  - SSH Brute Force Attacks
  - DNS/SMTP/NTP Amplification Attacks
  - Passive DNS Information
- Investigate how to share data that may impact privacy/PII and what can be anonymized but still be useful
  - SPAM / Phishing details

GLOBAL EFFORTS FOR ACTION

- **DNS-OARC**: DNS System Security
- **FIRST**: Vulnerability management
- **ISACs**: Specialized Interest Groups
- **M3AAWG** / **APWG**: Anti SPAM, Phishing and Crime
- **NSP-SEC**: Big Backbone Providers and IP Based Remediation
- **OPSEC-Trust**: Situational Awareness



BEING PART OF THE SOLUTION

- RoutingManifesto.org/manrs
- Use ONLY cryptographically protected protocols (this implies integrity and non-repudiation and possibly confidentiality)
- Change ALL default usernames and credentials
- Keep up with vulnerabilities and patch/upgrade in a timely manner
- Share what you can and help cross-functional education


QUESTIONS ?