



COMMUNICATIONS SECTOR COORDINATING COUNCIL

July 26, 2017

Matt Tooley
Vice President Broadband Technology, NCTA – The Internet & Television Association
& Co-Chair for the CSCC Cybersecurity Committee



Communications Sector Coordinating Council



- Help coordinate initiatives to improve the physical security and cybersecurity of sector assets
- Help to ease the flow of information within the sector, across sectors, and with designated Federal agencies; and
- Help to address issues related to response and recovery following an incident or event

BROADCASTING



There are more than 14,000 radio and 1,700 television broadcasting facilities in the United States, sending broadcasts through the air to a frequency network of transmitters.

CABLE



The cable industry is composed of approximately 7,791 cable systems that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service.

WIRELESS



Wireless technology consists of cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless and other commercial and private radio services.

WIRELIN



Over 1,000 companies offer wireline, facilities-based communications services in the United States. Wireline companies serve as the backbone of the Internet.

SATELLITE



Satellite communications systems deliver advanced data, voice, and video communications, transmitting data from one point on the Earth to another.

CSCC Industry Partners



3U TECHNOLOGIES
Underground, Underwater, Under-Ice



Cincinnati Bell
connecting what matters



Frontier



itta



Nsight
TELSERVICES



T-Mobile



AMERICAN CABLE
ASSOCIATION

43 Members as of
April 2017



JUNIPER
NETWORKS



NTA
THE RURAL
BROADBAND
ASSOCIATION



U.S. Cellular



AIB
Association for International Broadcasting



COMCAST
NBCUNIVERSAL



HARRIS



Level(3)
COMMUNICATIONS



NTT



USTEALCOM
THE BROADBAND ASSOCIATION



atis



Consolidated
communications



H HUBBARD
RADIO



NAB
NATIONAL ASSOCIATION OF BROADCASTERS



SIA
The Voice of the Satellite Industry



JTC
Utilities
Technology
Council



AT&T



COX
COMMUNICATIONS



HUGHES



ncta



Sprint



verizon



CableLabs



CSRA
Think Next. Now.



iconectiv



neustar



TDS



ViaSat



CenturyLink



ctia



INTERNET
SECURITY
ALLIANCE



NABA



TIA
ADVANCING GLOBAL COMMUNICATIONS



windstream
communications



Charter
COMMUNICATIONS



FairPoint
communications



iridium
Everywhere



CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

Enterprise-Level
Cybersecurity Risk
Management



CSRIC Cybersecurity Best
Practices - March 2015

WG 4

Executive Order 13636
February 2013



NIST Cybersecurity Framework
1.0 – February 2014



Critical Infrastructure
Cyber Community C³
Voluntary Program

CSCC Technical White Paper



Industry Technical White Paper

July 17, 2017

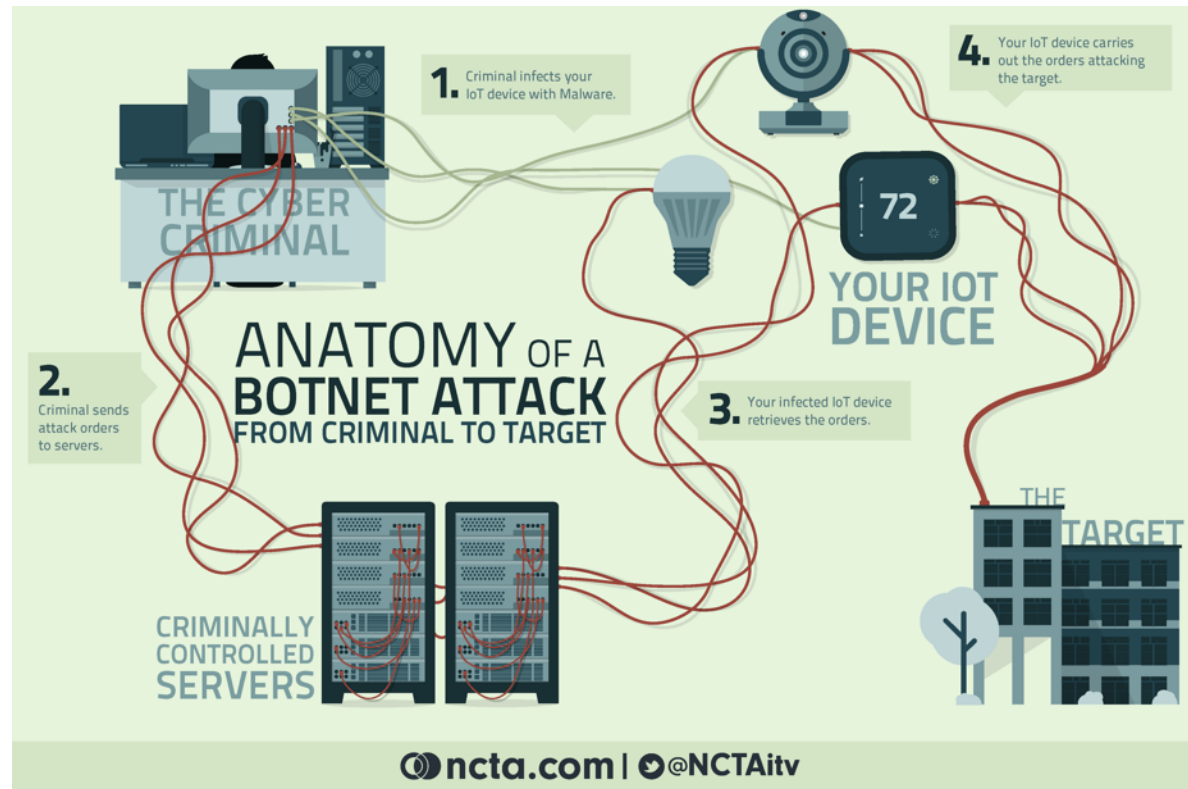
ABSTRACT

On May 11, 2017 President Trump signed Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, tasking the Department of Commerce and the Department of Homeland Security to lead an open and transparent process to identify ways to improve the resilience of the internet and communications ecosystem and reduce the threats perpetuated by botnets, particularly distributed denial of service attacks. In this technical white paper, the communications sector describes the botnet problem from the perspective of internet service providers (ISPs), identifies some challenges and opportunities, and then proposes several preliminary recommendations or actionable steps that ecosystem participants, including ISPs, should consider to mitigate the threats associated with botnets and automated attacks.

Communications Sector Coordinating Council

- Discusses botnets through the lens of ISPs
- Discusses what ISPs do today and some emerging solutions
- Makes nine preliminary recommendations for the internet ecosystem to help reduce the threats

Bots and Botnets



*Bot – a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator (aka bot master or bot herder).**

*Botnet – a network of internet-connected end-user computing devices infected with bot malware and are remotely controlled by third parties for nefarious purposes.**

* Both definitions are from Federal Communications Commission (FCC), Communications Security Reliability and Interoperability Council (CSRIC) III, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers*, (Mar. 2012)

Threats from Botnets

DDoS Attacks

Data Theft

Unauthorized
Network
Gateways

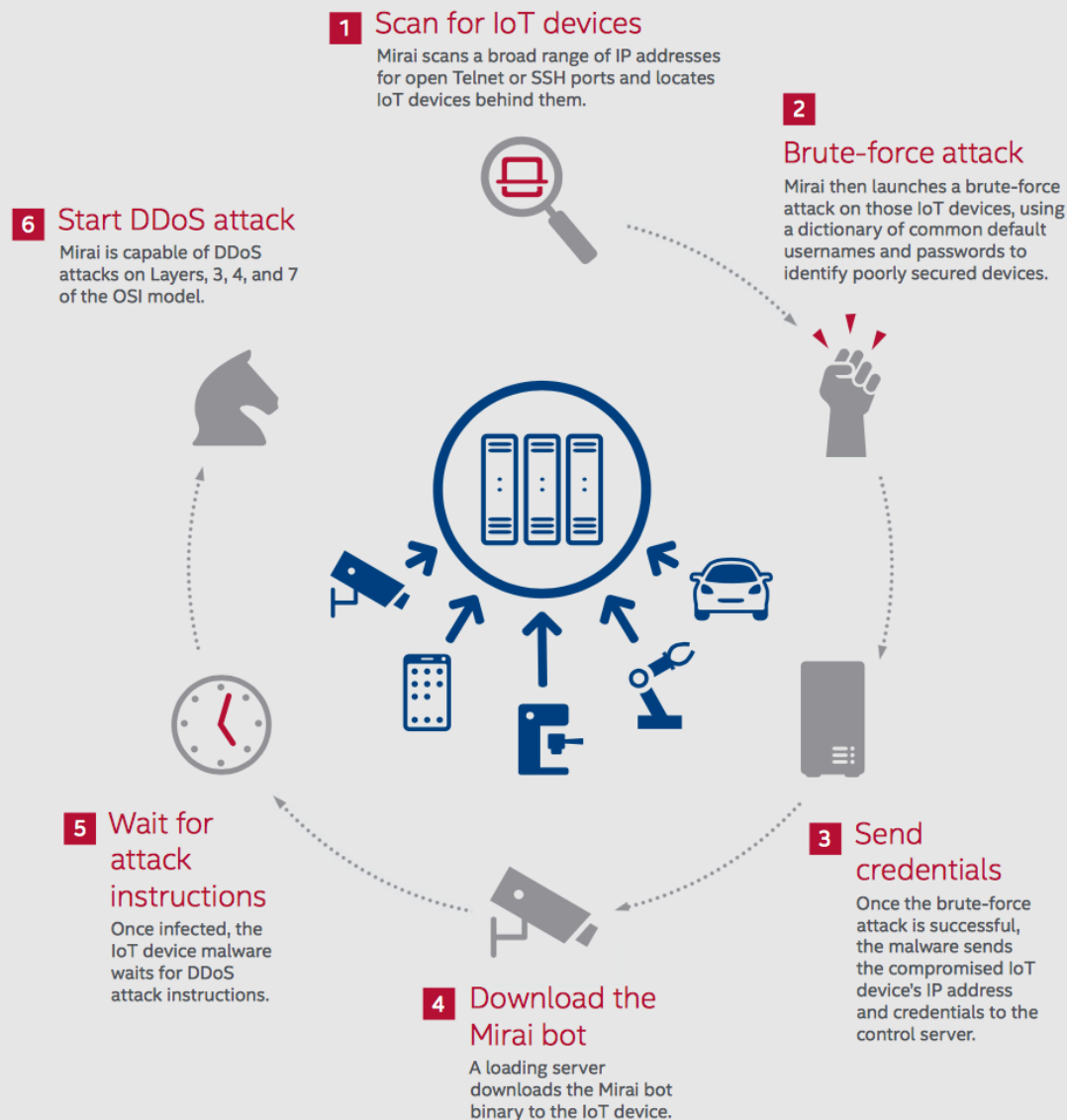
Illegal Content
Distribution

Processing
Theft

Click Fraud

Email spam

Attack process

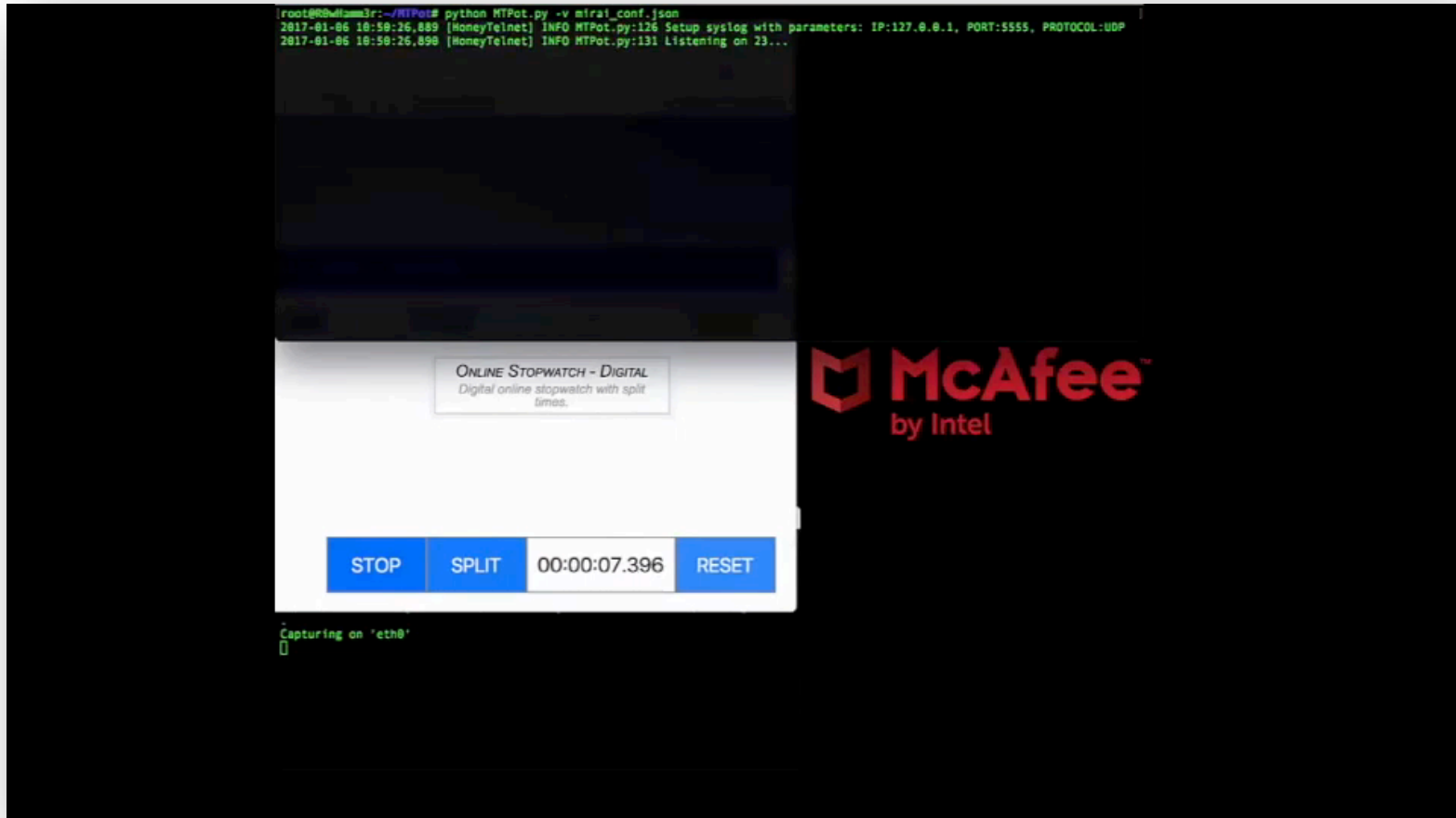


Mirai Botnet

- Level 3 Threat Research Labs observed >1M IoT devices participating in attacks
- Majority of infected devices were located in Taiwan, Brazil, and Columbia

A good case study to illustrate botnets through the lens of an ISP

Demonstration of Mirai Botnet Scanning



Source: McAfee on Youtube - <https://youtu.be/vnitAXYGmI0>

- Within 30 seconds attacks start hitting the honeypot
- Within 60 seconds Mirai hits the honeypot

Mirai Botnet Attacks

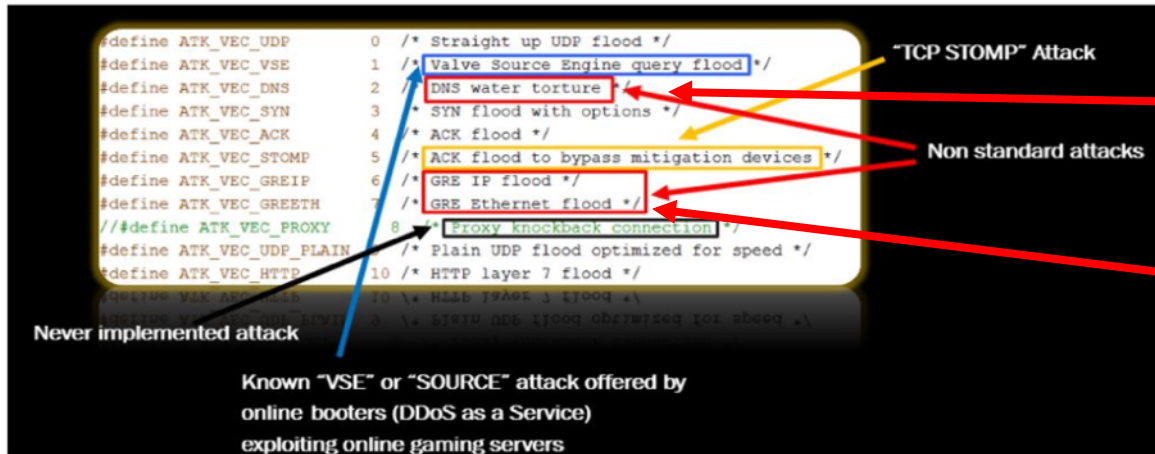


Figure 1: DDoS Attack Methods Source: F5 Labs - <https://f5.com/labs/articles/threat-intelligence/ddos/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-attack-on-ovh-22422>

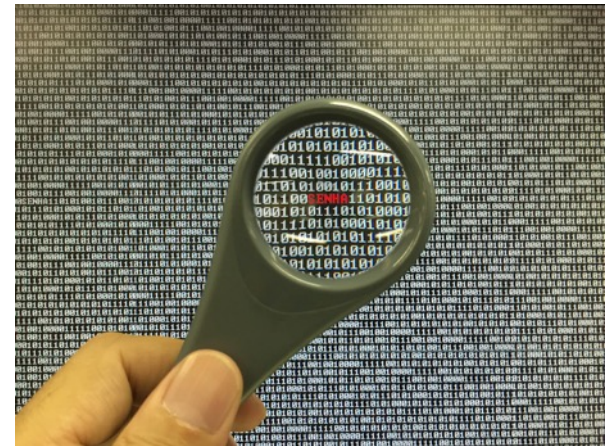
Primary Sources

- IoT devices – IP security cameras and their DVRs
- Majority of traffic originated from outside the U.S.



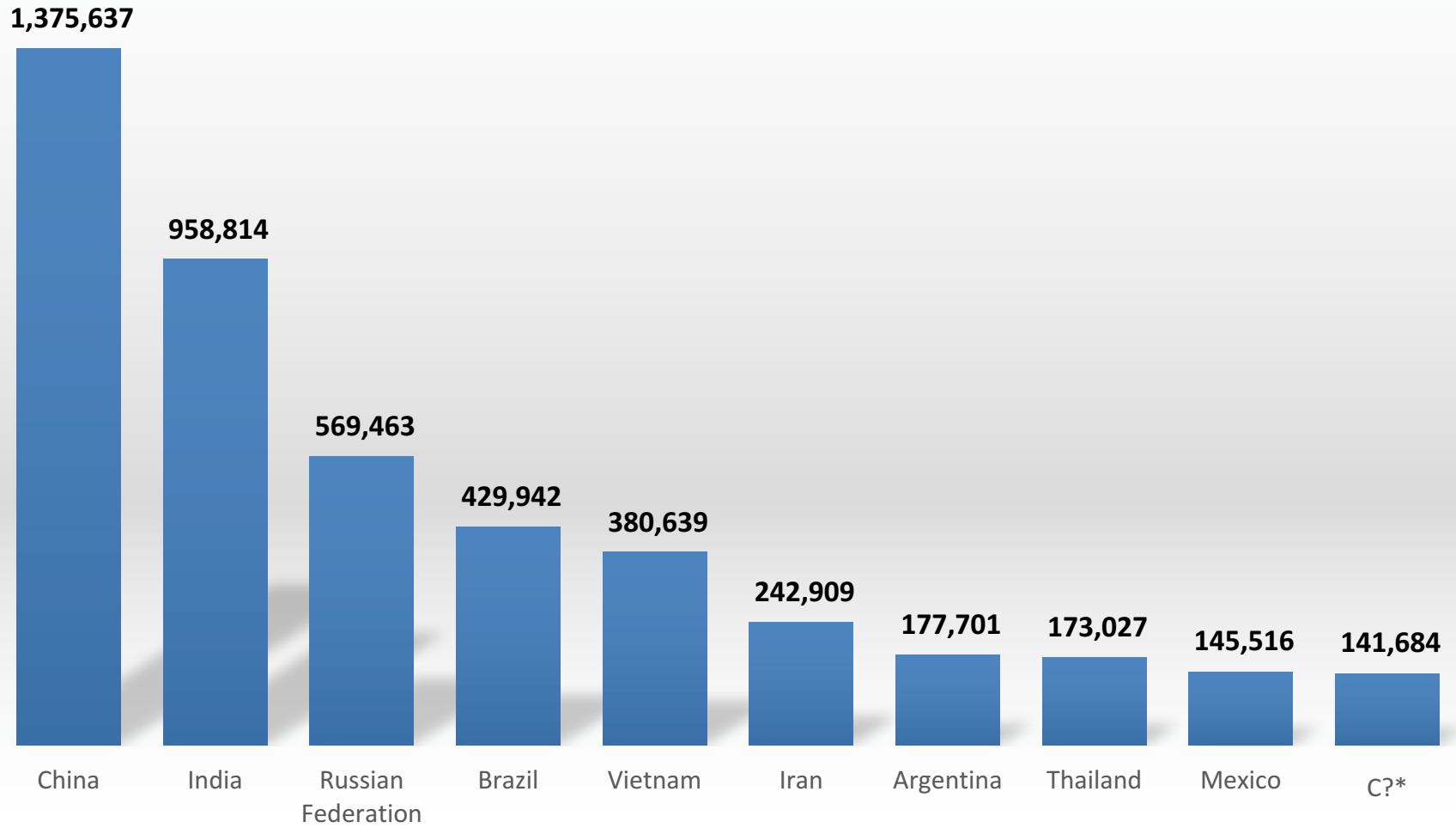
Botnet Attack Traffic

- Abuses UDP-based protocols
 - DNS/DNSSec, NTP, chargen, QOTD,SSDP
- Not limited to UDP protocols
 - Brobot used HTTP/HTTPS
 - IPv6 header extensions
- Growing trend to encrypt C&C traffic
- Vast majority of traffic originates from outside the U.S.



Top 10 Worst Botnet Countries

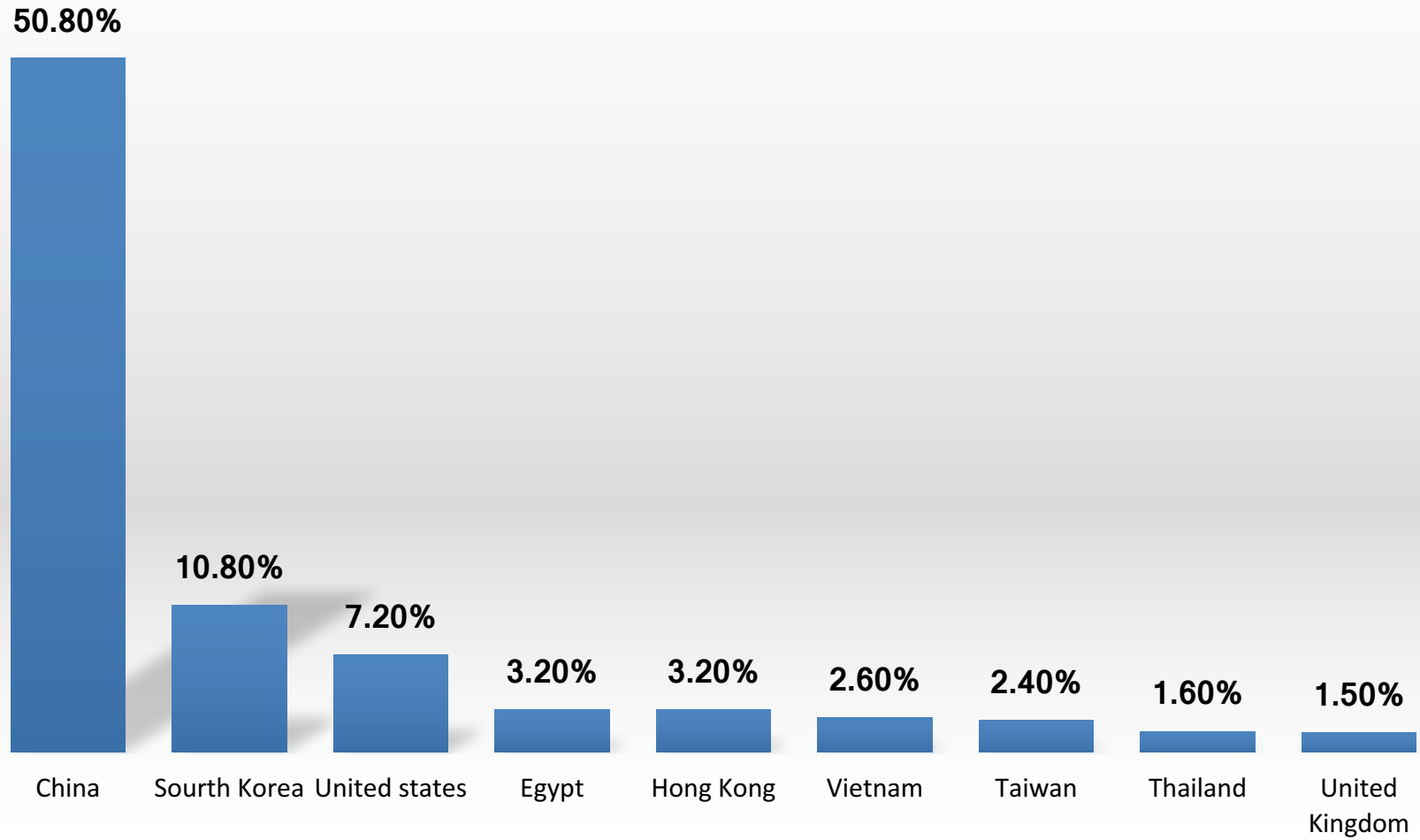
■ Number of Bots



Source: Spamhaus as of June 29, 2017. <https://www.spamhaus.org/statistics/botnet-cc/>

Top 10 Botnet Traffic Attacking Countries

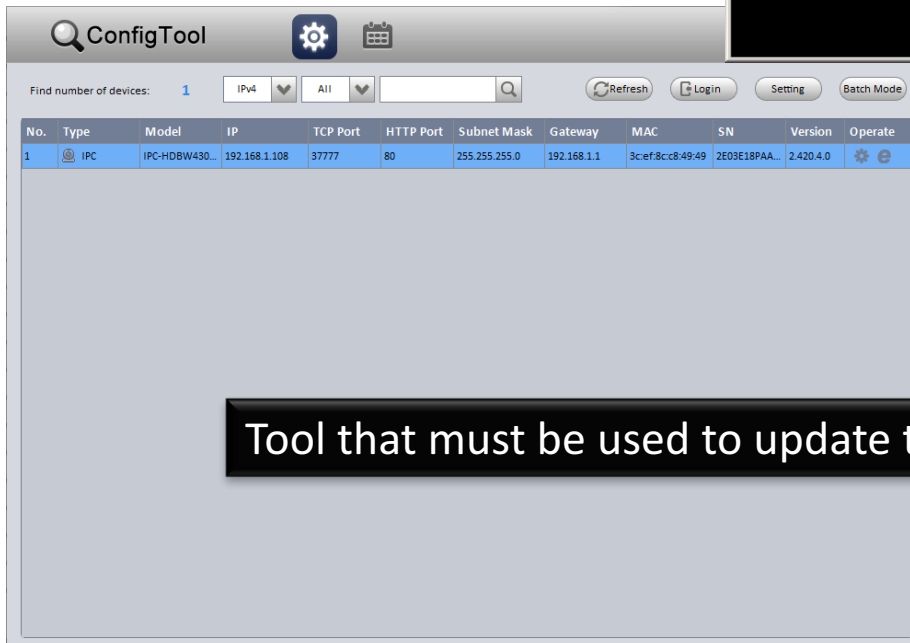
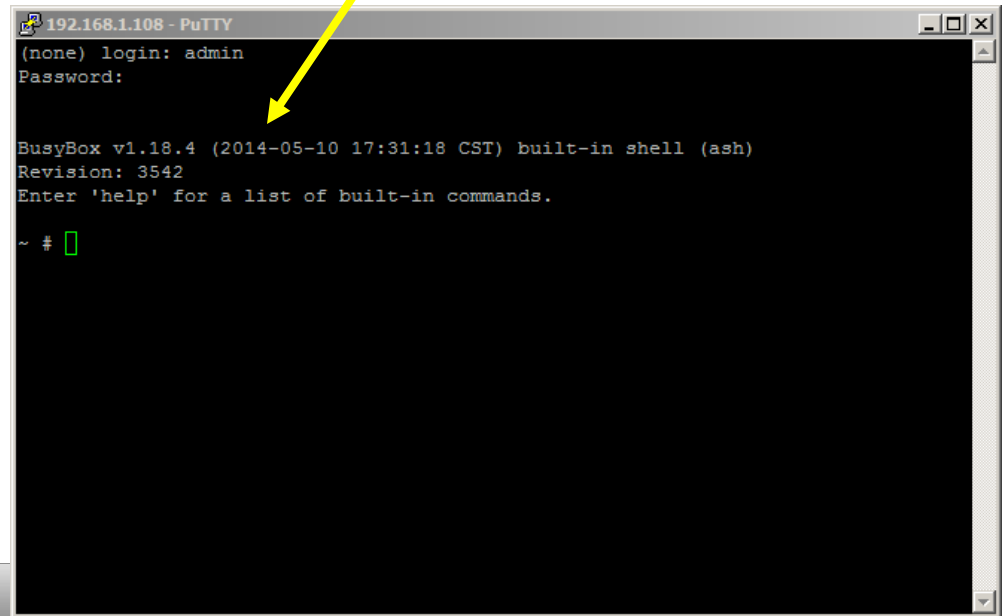
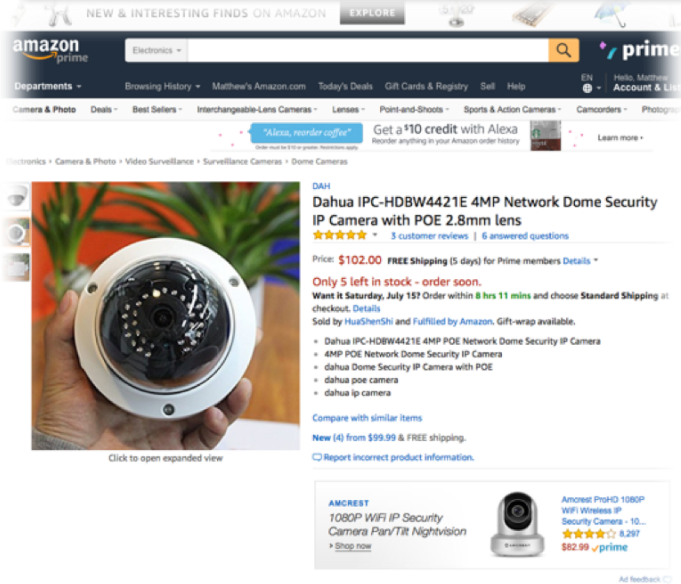
■ Percentage of botnet attack traffic



Source: Incapsula Global DDoS Threat Landscape Q1 2017. <https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html>

Purchased via Amazon in late 2016

Out of date software - 2014!!



Tool that must be used to update the software

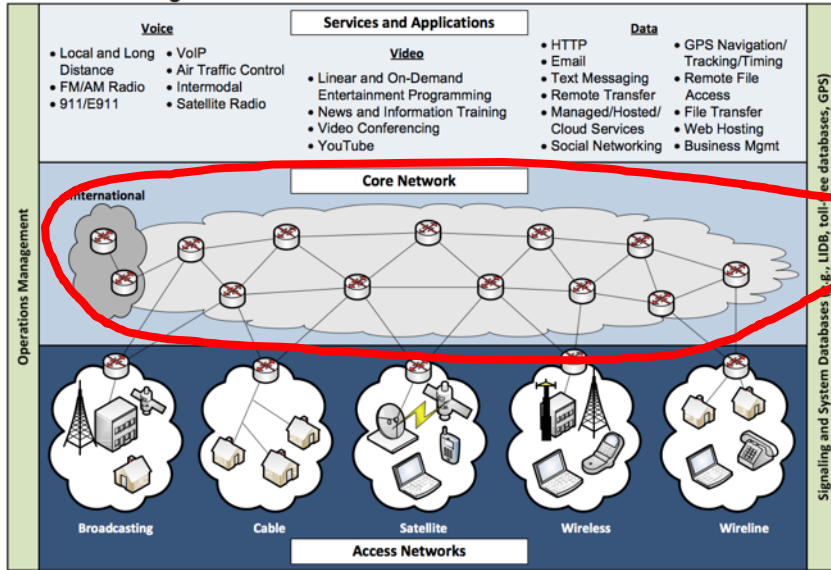
Tools & Techniques Used By ISPs

Identify	Identification of critical assets, Information Sharing
Detect	Packet Sampling, Signature Analysis, Heuristic/behavioral Analysis
Protect	ACLs, policing, black/sink holes, DDoS "scrubbers", BGP Flowspec, CDNs/anycast, end-user AV software, managed security service offerings to customers
Respond & Recover	Mitigate attack traffic, work with upstream provider(s) to filter; notify customers per ABC for ISPs

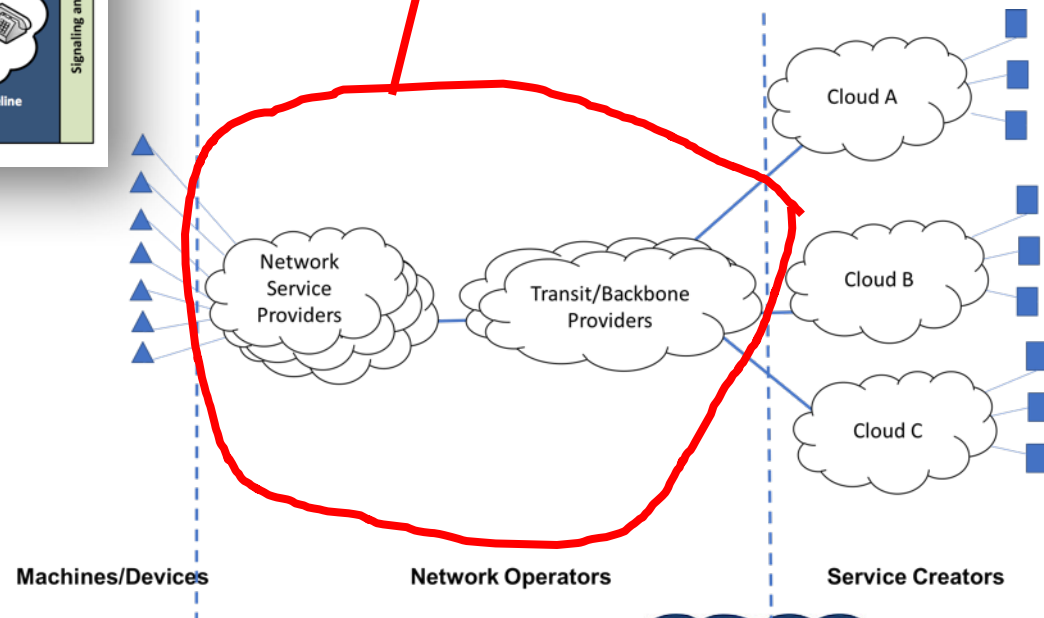


Identify: Critical Assets

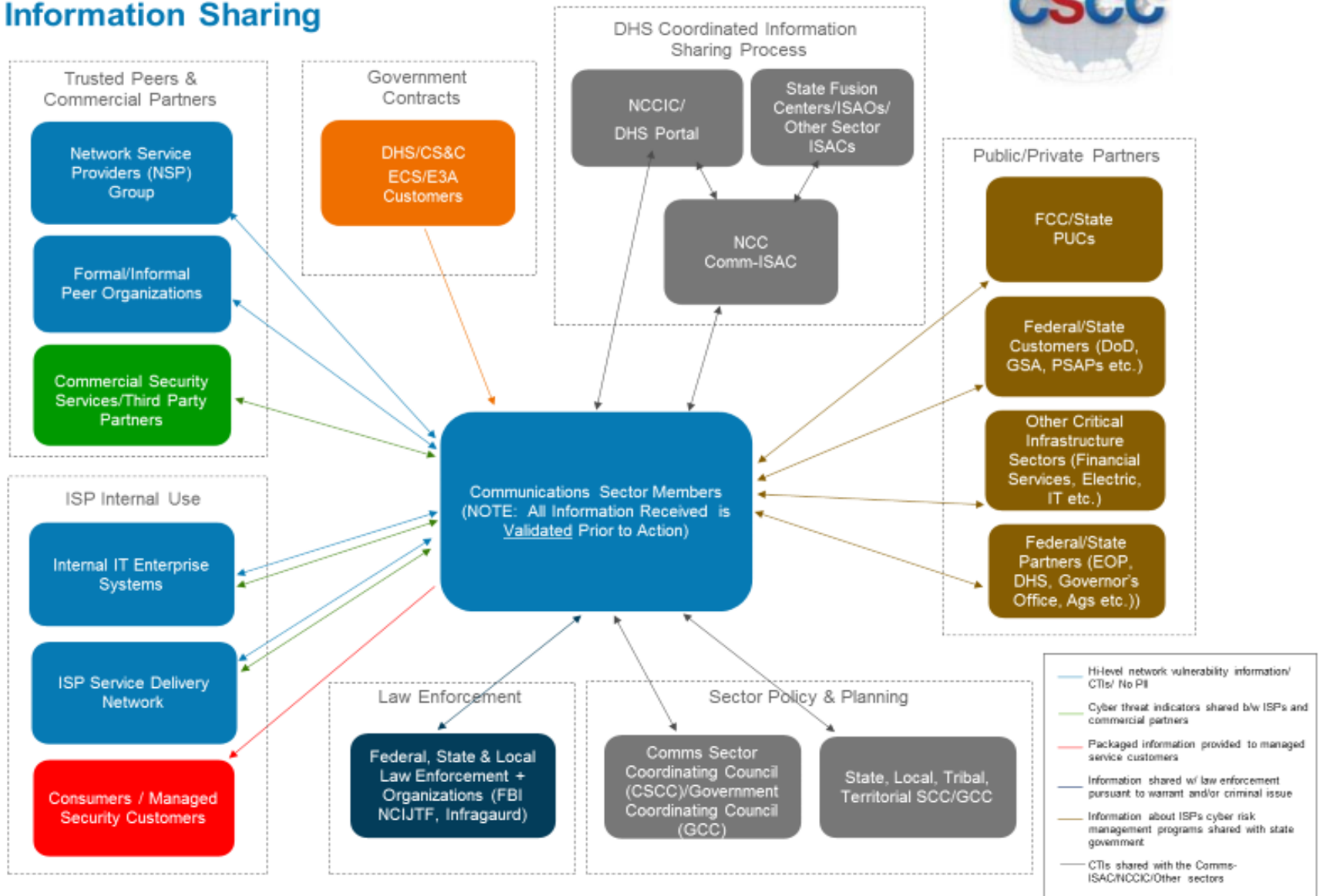
Figure 2-2: Communications Sector Architecture Model



Protect the core network to ensure the delivery of services



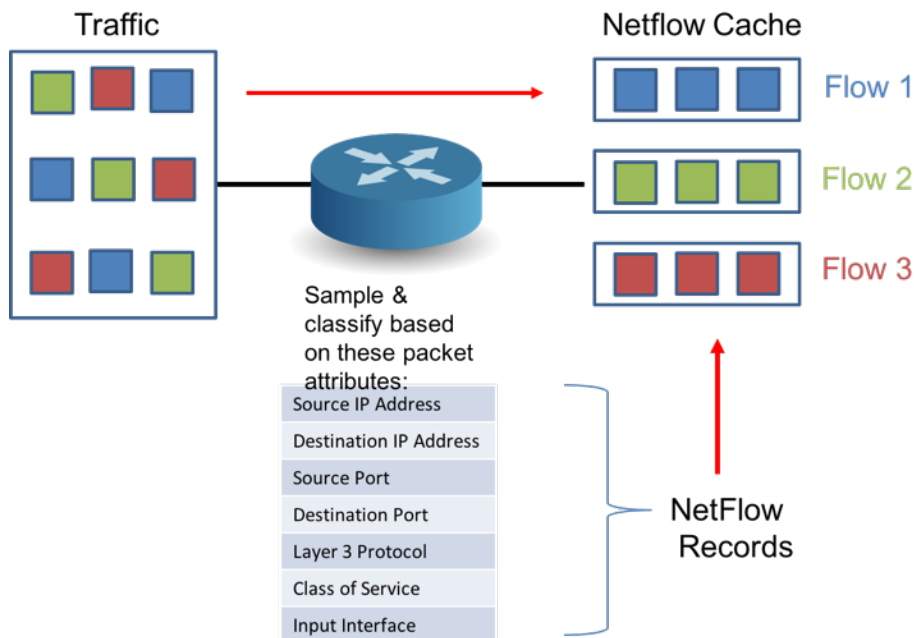
Notional Diagram Communications Sector Information Sharing



Identify - Information Sharing

Detect

- Packet Sampling
- Signature & Behavioral Analysis



SNORTOLOGY 101

THE ANATOMY OF A SNORT RULE

WHAT IS SNORT?

Snort is an open source network intrusion prevention system (IPS) by Cisco. It is capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching and matching, and detect a variety of attacks and probes. Snort can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging), or as a full-blown network intrusion prevention system.

LET'S BREAK IT DOWN

BASIC OUTLINE OF A SNORT RULE

```
[action][protocol][sourceIP][sourceport] -> [destIP][destport] ( [Rule options] )
```

RULE HEADER

The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information.

EXAMPLE

```
Rule Header  alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
Message      msg: "BROWSER-IE Microsoft Internet Explorer
              CacheSize exploit attempt";
Flow         flow: to_client,established;
Detection    file_data;
              content:"recordset"; offset:14; depth:9;
              content:".CacheSize"; distance:0; within:100;
              meta:/CacheSize/s*/s*/";
              byte_test:0,>,0x3fffffff,0,relative,string;
Metadata     policy max-detect-ips drop, service http;
References   reference:cve,2016-8077;
Classification  classtype: attempted-user;
Signature ID  sid:65535;rev:1;
```

RULE OPTIONS

alert Action to take (option) The first item in a rule is the rule action. The rule action tells Snort what to do when it finds a packet that matches the rule criteria (usually alert).

tcp Type of traffic (protocol) The next field in a rule is the protocol. There are four protocols that Snort currently analyzes for suspicious behavior - TCP, UDP, ICMP, and IP.

\$EXTERNAL_NET Source address(es) variable or literal

\$HTTP_PORTS Source port(s) variable or literal

-> Direction operator The direction operator -> indicates the orientation of the traffic to which the rule applies.

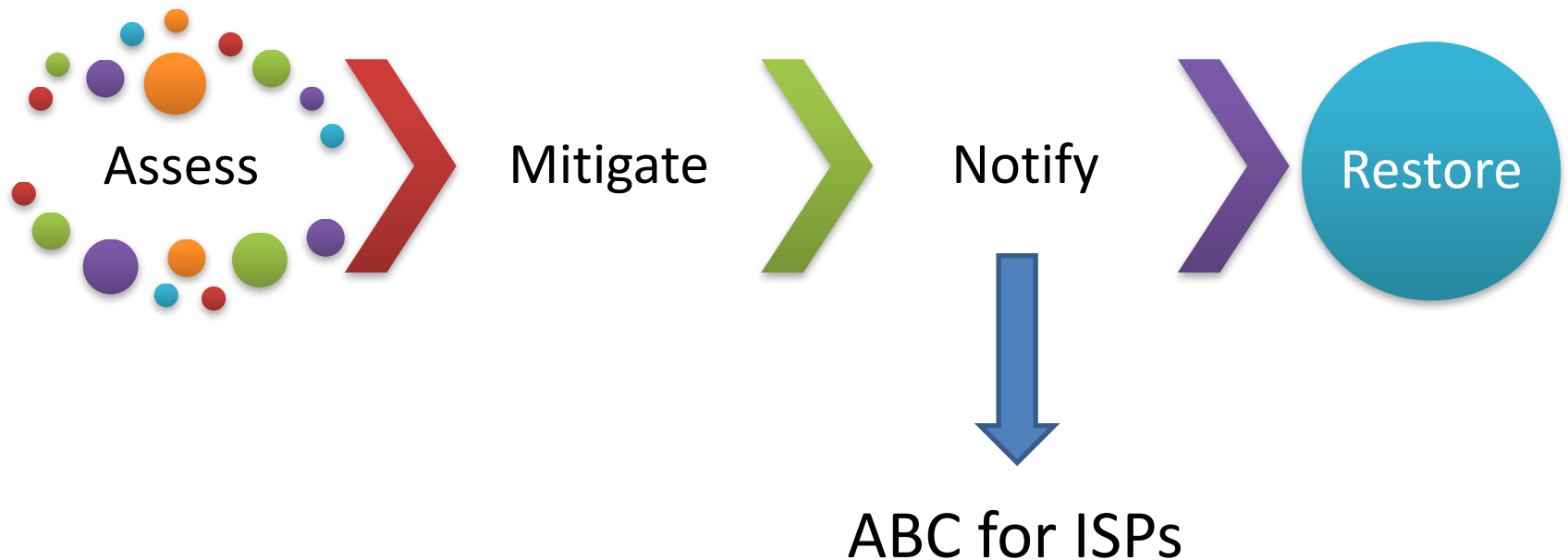
\$HOME_NET Destination address(es) variable or literal

any Destination port(s) variable or literal

Protect

Techniques	Description
Access Control Lists (ACLs)	Typically in a router/switch and is applied to the IP address and/or port, can be applied to domain names
Traffic Policing	Slowing down of malicious traffic
Black Holes	Silently drop packets from a source or to a destination, often done at the router
Sinkholes (DNS, sinkhole routing)	Used to redirect attacks to a server to capture attack traffic for analysis
BGP Flow Spec	Block traffic on the router that matches five-tuple
DDoS Scrubbers	Diverting victims traffic through a system that looks for traffic that matches malicious traffic patterns, and drops it
Content Delivery Networks/Anycast	Geographically distributing the content across multiple hosts
End-user Anti-virus Software	Desktop software that looks for malware
Managed Security Service Offerings	Network based firewalls, secure VPN, web/email security

Respond & Recover



Emerging Solutions - Technical

- Application of Machine Learning for Detection
 - Example – Applying AI to detect bots using domain generation algorithm
- Fingerprinting of encrypted C&C traffic
- Creating tarpits from dark IP address blocks
- Software Defined Networks (SDNs)

```
uqhucsontf[.]com  
myypqmvzkgnr[.]com  
ocufxskoiegqvv[.]com  
uflhdvsnjmfgcp[.]so  
otopshphtnhml[.]net  
aiygrmsryphqlkfcd[.]su  
etfxkiqtriteysf[.]pw  
crigtwrtdtxbcmsgjkmx[.]tv  
cجيoboxmxhsmrclrhxxl[.]im  
soqikjyliunjqaciqlg[.]tj  
jrguloma[.]biz  
anlxcceqeflidpwyhobm[.]jir
```

Emerging Solutions - Collaborative

- IETF DDoS Open Threat Signaling (DOTS)
 - Protocol for the real-time exchange of telemetry between DDoS mitigation platforms
 - Supports requests for DDoS mitigation and status updates network-to-network
- M3AAWG DDoS API
 - Application Program Interface to share identified sources (source IP addresses) of DDoS attack traffic
 - Allows network operators to share the source IP address for inbound IP flows in anonymous fashion with the network from which the flow emanates

Challenges & Opportunities

	Challenge	Opportunity
Botnet Takedowns	Requires lots of resources & coordination	More law enforcement & streamlining of international processes
Actionable Threat Information	Stale information in particular IP addresses	DHS AIS, IETF DOTs, M3AAWG DDoS API
Network Address Translation (NAT)	Identifying devices behind NAT routers	Reduce the need for NAT in home routers with IPv6
Off-Net Traffic	Overwhelming majority of botnet traffic originates from outside the U.S.	Inclusion in peering/transit agreements for availability and scrubbing to filter malicious traffic
End-User Notifications	Reaching the accountable party and notifying. IoT makes this worse	Following best practices and standards that include methods for device identification

Challenges & Opportunities

	Challenge	Opportunity
Fast Flux DNS	Botnets rapidly changing the IP addresses associated with the domain names for C&C servers	Broader use of the SSAC recommendations; Use of machine learning
Insecure IoT Devices	IoT devices shipping with known vulnerabilities	<ul style="list-style-type: none">• Applying principles of least privilege into the design of IoT devices• Use of network isolation/filtering by IoT devices to keep IoT traffic from doing harm to others
Amplification Attacks	Source address spoofing	Broader implementation of source address validation techniques (i.e. BCP 38/84, MANRS)
Network-to-Network Coordinated Network Management	Sources of ground truth for botnets; heterogeneous network architectures; C&C servers operating with shared services	More close, trusted collaboration and communications between stakeholders

Preliminary Recommendations

Attack Mitigation	End-Point Prevention
Encourage continued migration to all IPv6	End-points including IoT devices should follow security best practices and standards
Sharing of <u>actionable</u> cyber threat information	Ensure end-points are running up-to-date software
Pre-negotiated provisions for traffic filtering in transit and peering agreements	IoT devices should use network isolation and/or network-based filtering techniques for any communications to cloud-based services.
Streamline law enforcement process for botnet takedowns	
Adapt & apply machine learning for botnet detection	

Still need to discuss best practices & capabilities for all segments of the internet ecosystem

ADDRESSING BOTNETS IS A SHARED RESPONSIBILITY

Everyone Plays a Role

Anti-virus and security vendors, application and operating system developers, device manufacturers, domain registrars and registries, end users, Internet service and cloud service providers, IT departments, public-private partnerships, search engines, website owners and others

Employ relevant technologies and practices across lifecycle phases

PREVENT

DETECT

NOTIFY

REMEDiate

RECOVER

Educate and empower customers

Share information, lessons learned and resources

Thanks!

Matt Tooley
Email: mtooley@ncta.com