MESSAGING MALWARE MOBILE

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

M^{3}AAWG
MESSAGING MALWARE MOBILE

M^{3}AAWG Training Video Series

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

(more than 2.25 hours of training)

This is Segment 2 of 6

The complete series is available at: https://www.m3aawg.org/activities/maawg-training-series-videos

Segment 1 **Top SP Security Essential Techniques** **(about 20 minutes)**	**Segment 2** **Types of Malware Problems ISPs Encounter** **(about 20 minutes)**	**Segment 3** **Understanding the Threat:** **A Cyber-Criminal's Work Day & Cyber-Criminal Behavior Drivers** **(about 30 minutes)**
Segment 4 **Turning Point** **(about 12 minutes)**	**Segment 5** **Remediating Violated Customers** **(about 35 minutes)**	**Segment 6** **U.S. FCC's Anti-Botnet Code of Conduct (ABCs for ISPs)** **Overview &** **Code on a Shoestring Budget** **(about 20 minutes)**

M3AAWG
MESSAGING MALWARE MOBILE

Types of Malware Problems ISPs Encounter

Segment 2 of 6

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

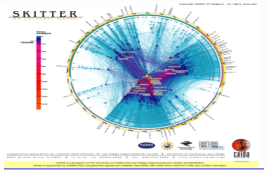
M3AAWG
MESSAGING MALWARE MOBILE

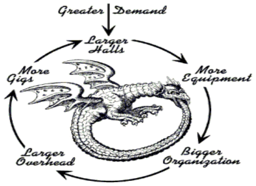
Barry Greene has over 30 years industry experience including having served as president of the ISC (Internet Systems Consortium). He is a pioneer in service provider security and operational security reaction teams.

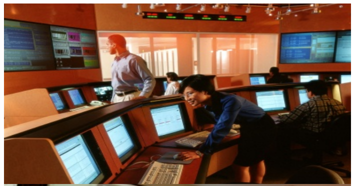
Barry is currently a participant on the U.S. Federal Communications Commission's (FCC's) Communications Security, Reliability and Interoperability Council (CSRIC).

Top SP Security Essential Techniques

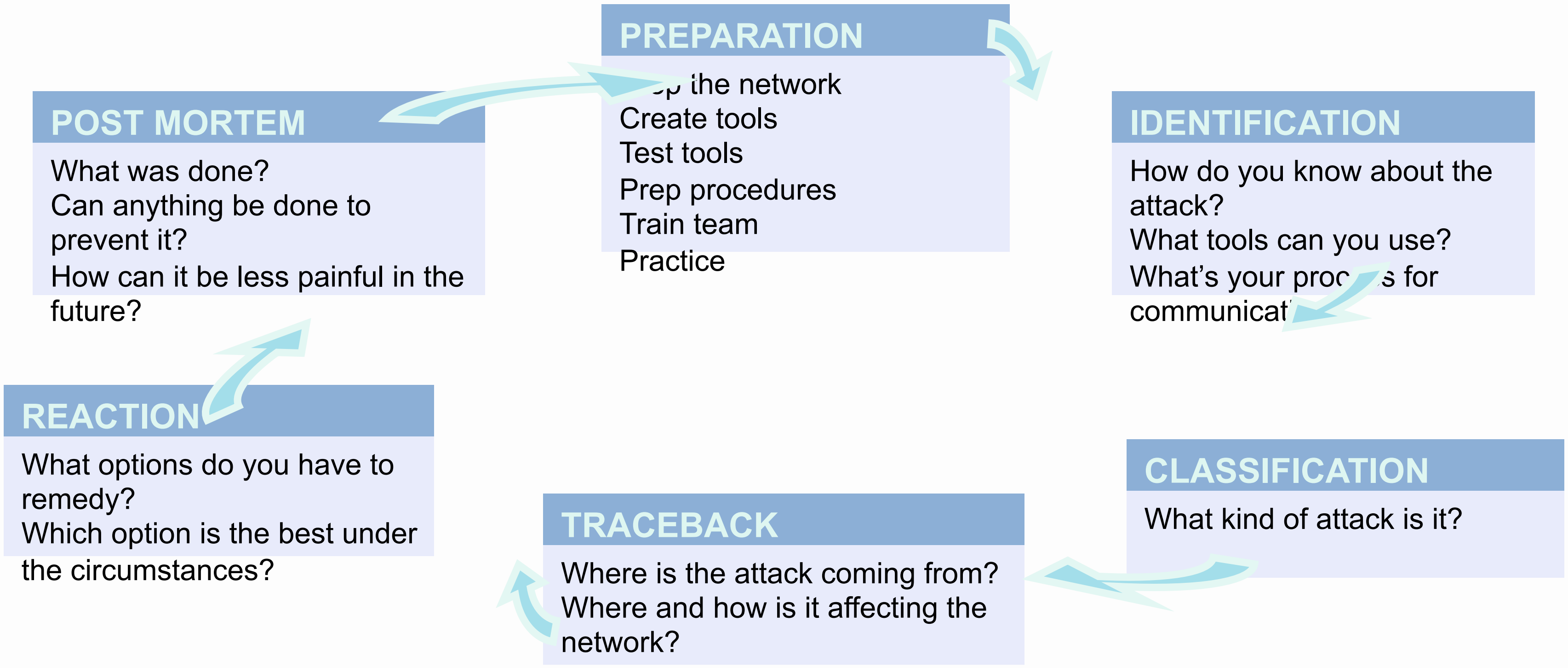
The Executive Summary







SP Security in the NOC - Prepare



PREPARATION

Map the network
Create tools
Test tools
Prep procedures
Train team
Practice

IDENTIFICATION

How do you know about the attack?
What tools can you use?
What's your process for communication?

CLASSIFICATION

What kind of attack is it?

TRACEBACK

Where is the attack coming from?
Where and how is it affecting the network?

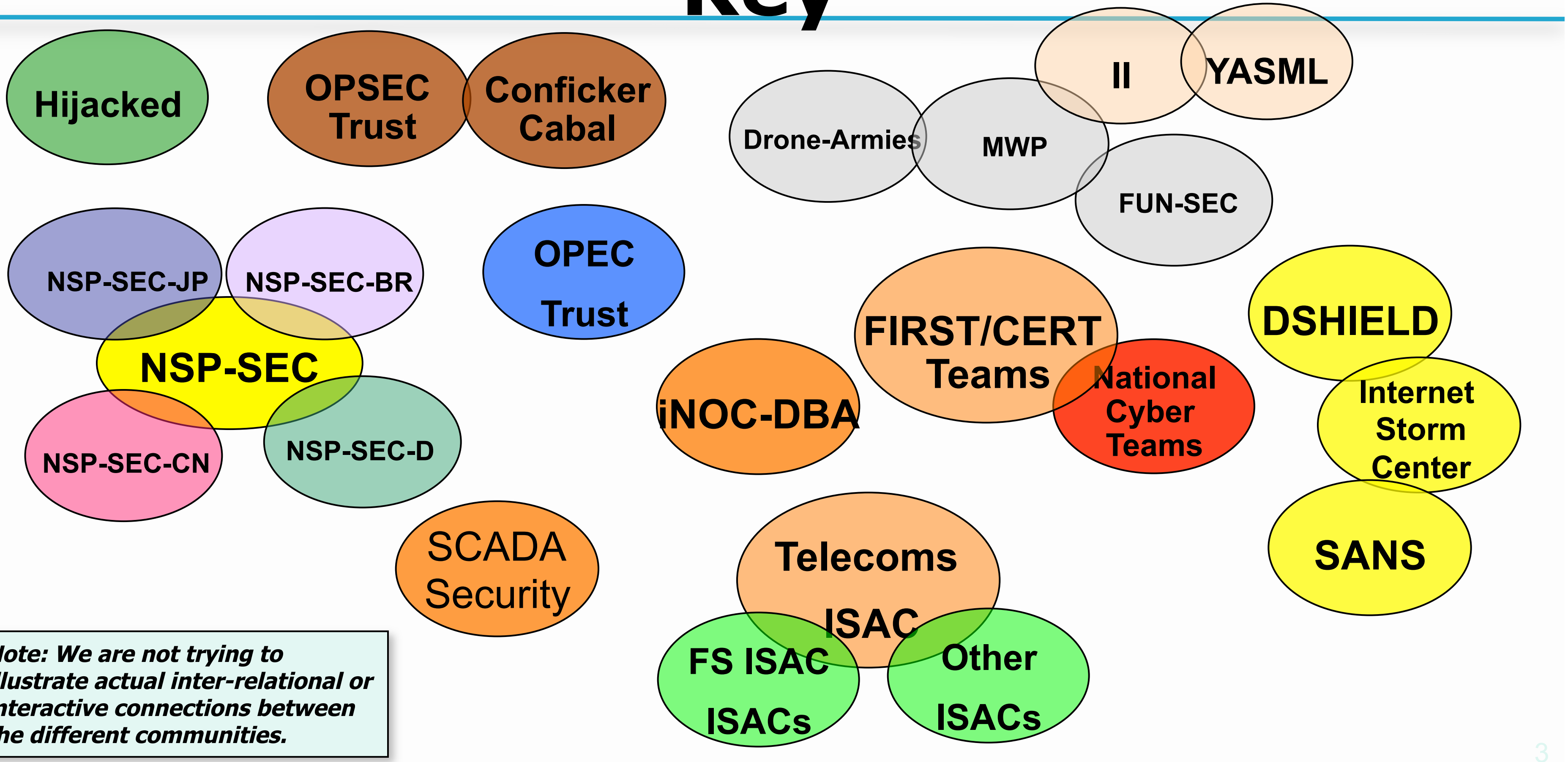
REACTION

What options do you have to remedy?
Which option is the best under the circumstances?

POST MORTEM

What was done?
Can anything be done to prevent it?
How can it be less painful in the future?

Aggressive Collaboration is the Key



Hijacked

OPSEC Trust

Conficker Cabal

Drone-Armies

MWP

II

YASML

FUN-SEC

NSP-SEC-JP

NSP-SEC-BR

NSP-SEC

NSP-SEC-CN

NSP-SEC-D

OPEC Trust

FIRST/CERT Teams

National Cyber Teams

iNOC-DBA

DSHIELD

Internet Storm Center

SANS

SCADA Security

Telecoms ISAC

FS ISAC

ISACs

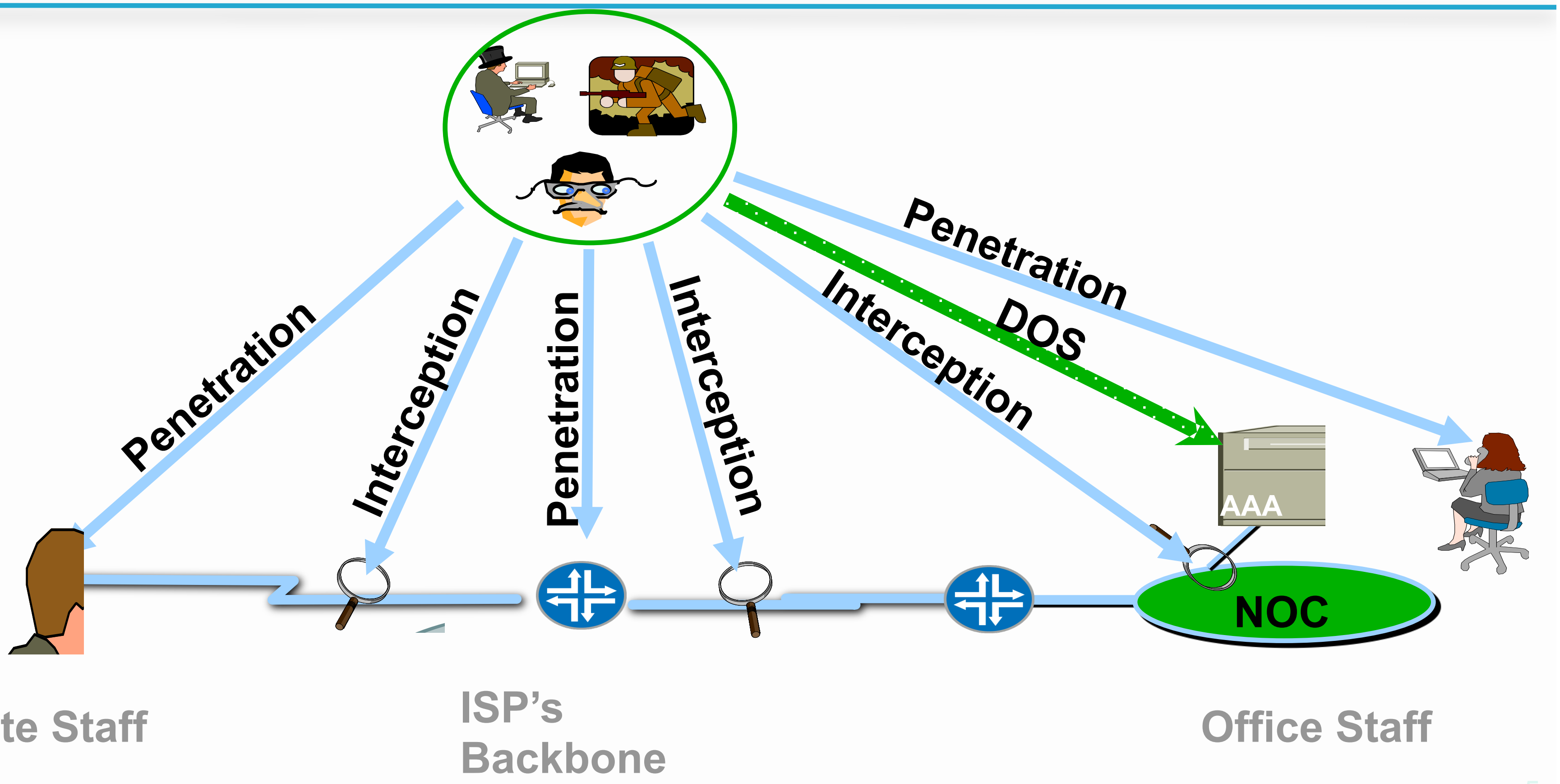
Other ISACs

Note: We are not trying to illustrate actual inter-relational or interactive connections between the different communities.

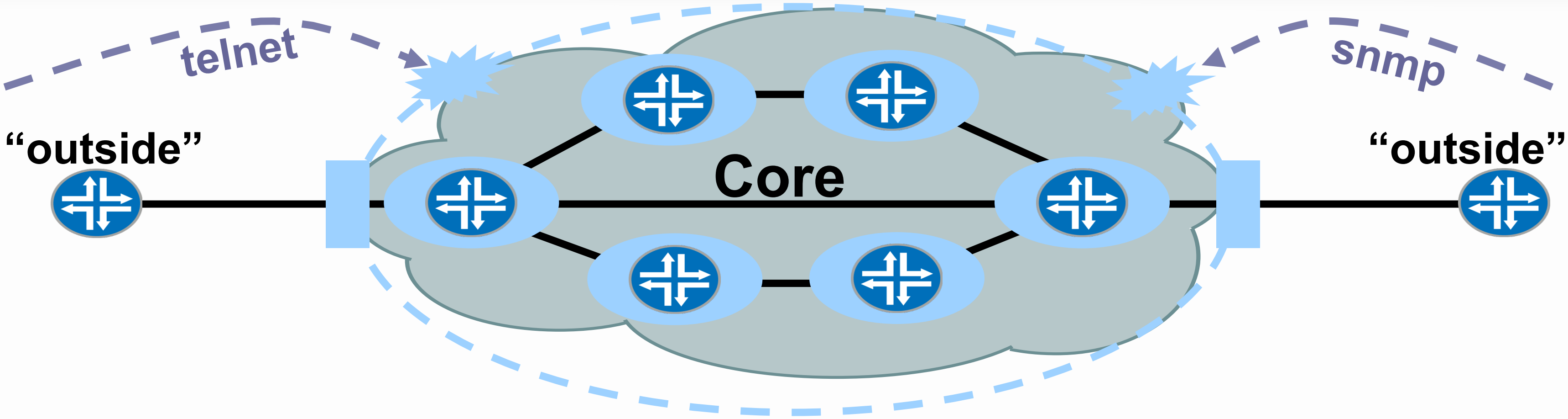
iNOC DBA Hotline

- INOC-DBA: *Inter-NOC Dial-By-ASN*
- The iNOC Hotline was used to get directly to their peers.
- Numbering system based on the Internet:
  - ASnumber:phone
  - 109:100 is Barry’s house.
- SIP Based VoIP system, managed by www.pch.net

Point Protection

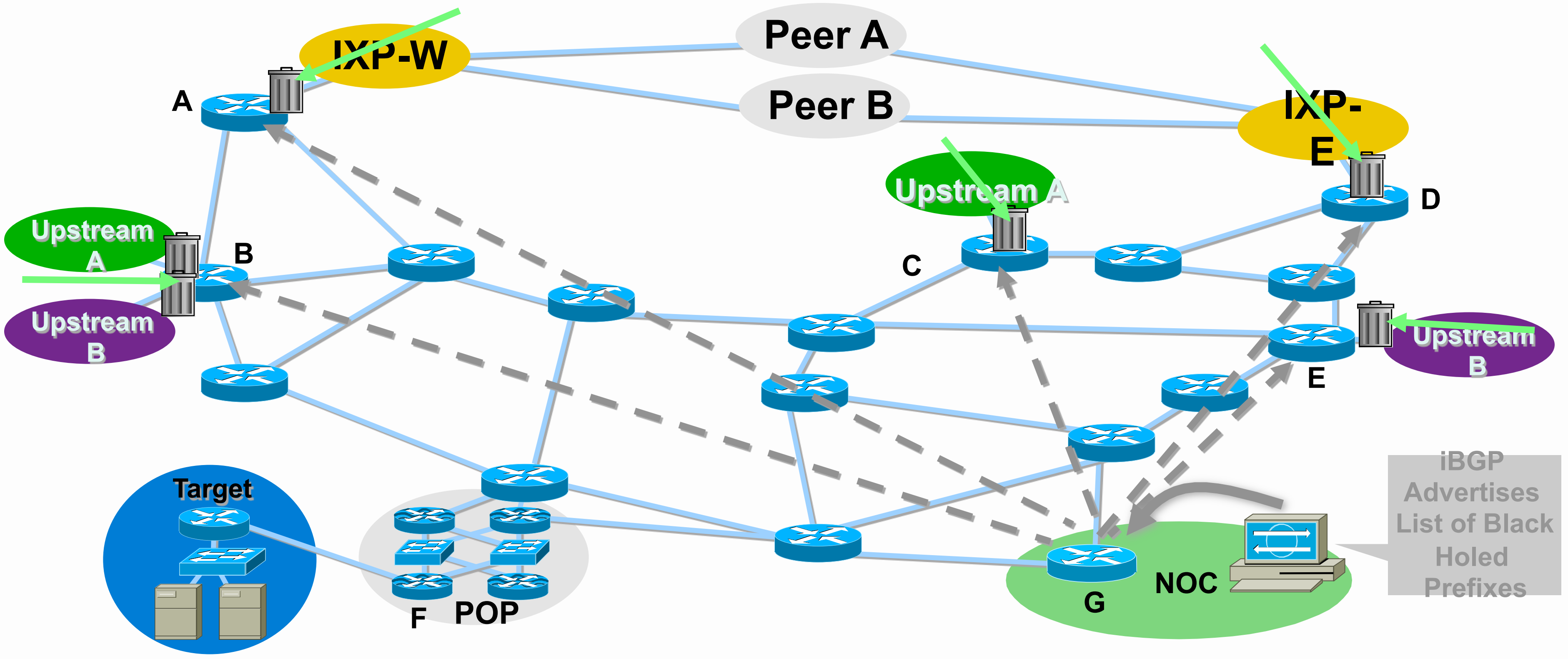


Edge Protection



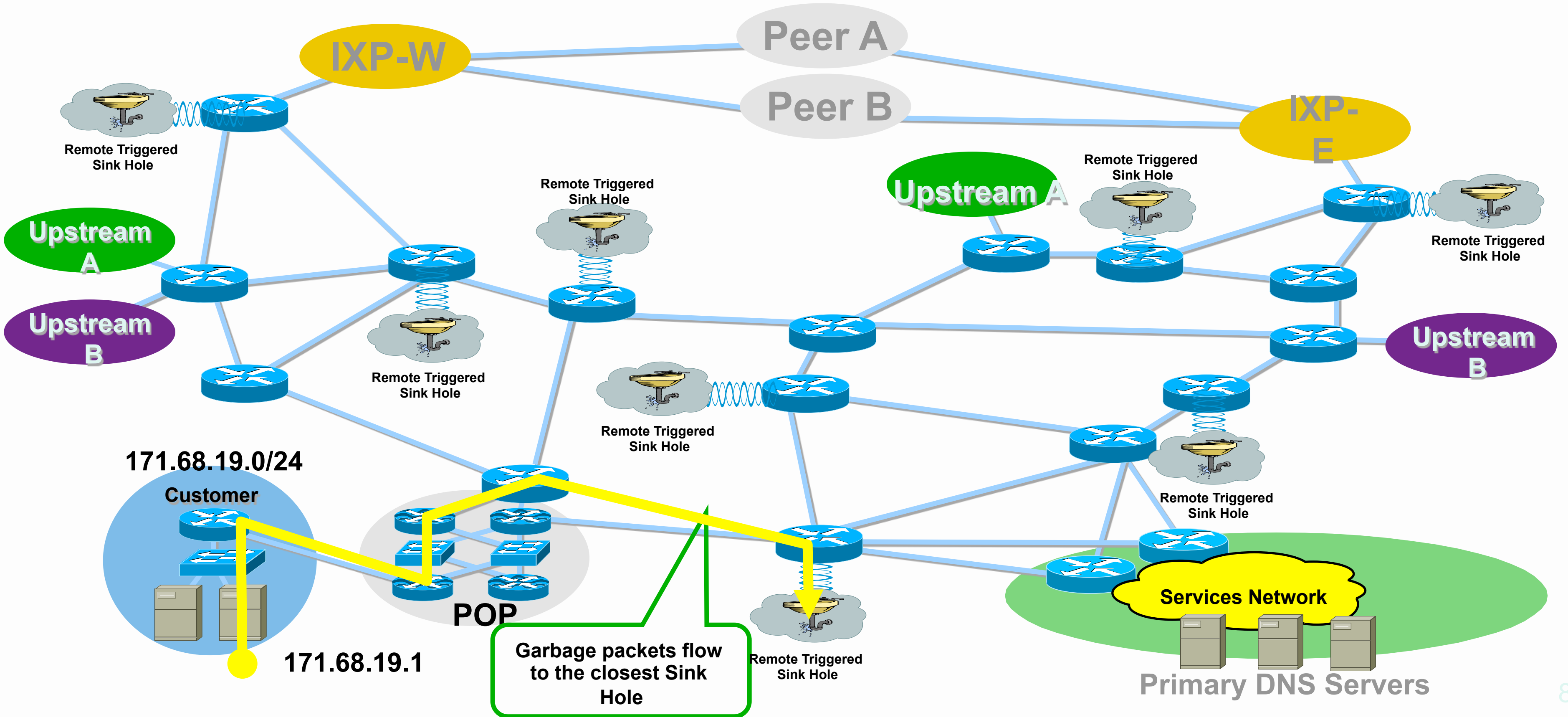
- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Destination Based RTBH



iBGP Advertises List of Black Holed Prefixes

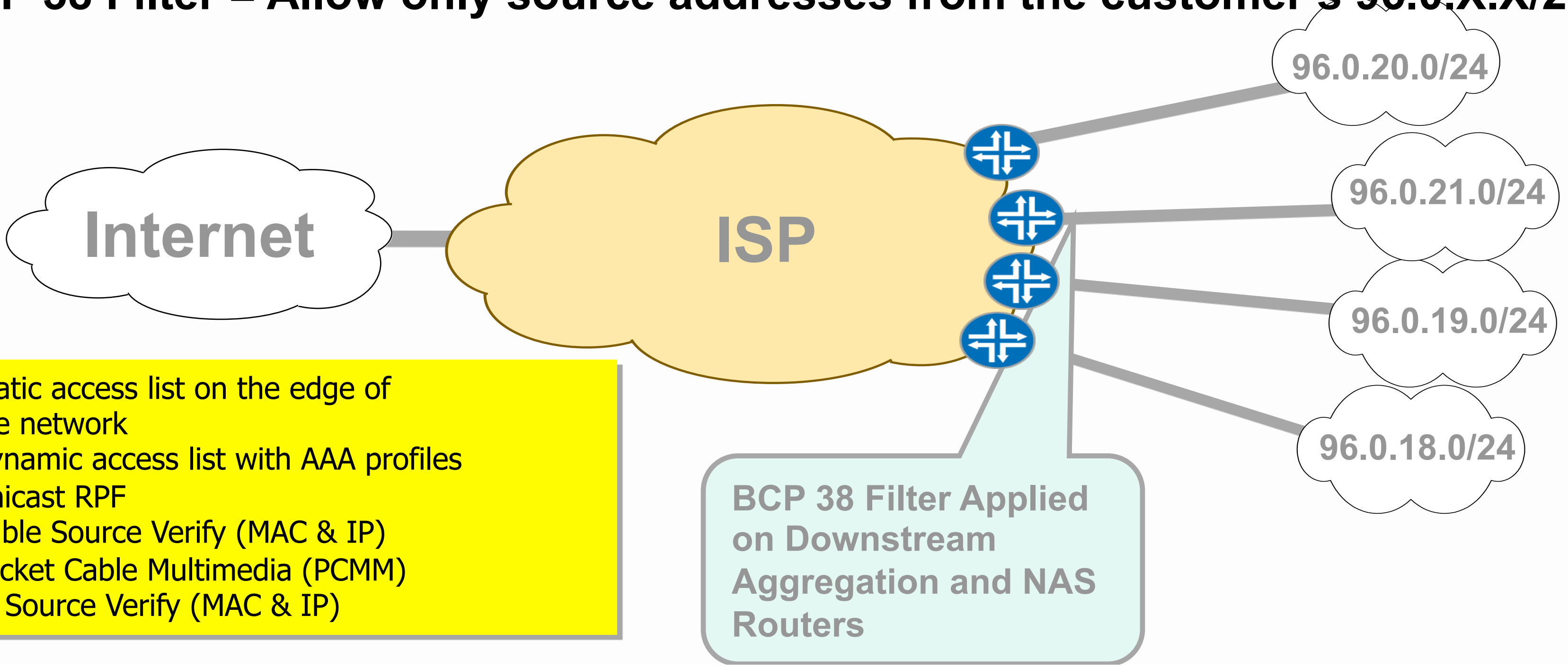
Sink Holes


IXP-W
Peer A
Peer B
IXP-E
Remote Triggered Sink Hole
Upstream A
Upstream B
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Upstream A
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Upstream B
Remote Triggered Sink Hole
Remote Triggered Sink Hole
171.68.19.0/24
Customer
POP
171.68.19.1
Remote Triggered Sink Hole
Services Network
Primary DNS Servers

Garbage packets flow to the closest Sink Hole

BCP 38 Ingress Packet Filtering

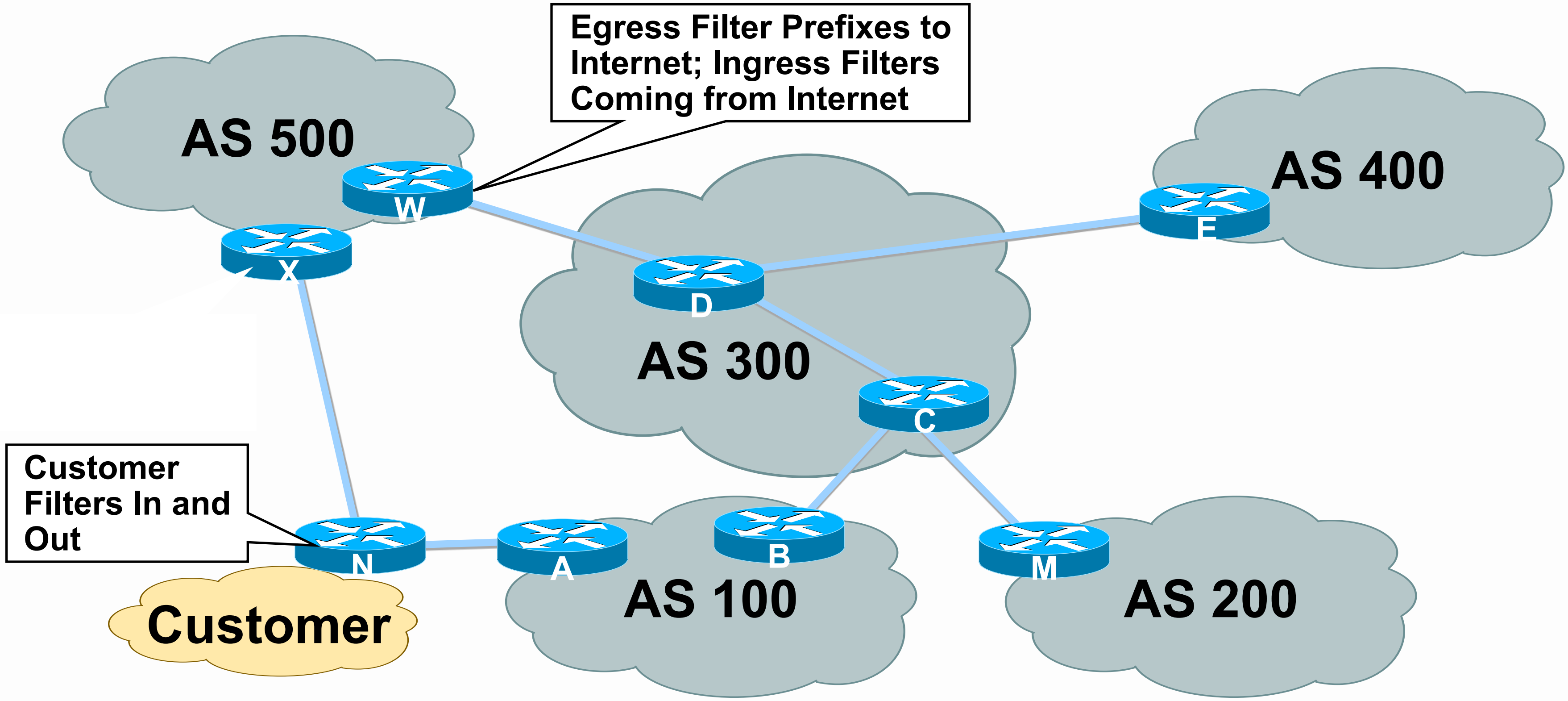
ISP's Customer Allocation Block: 96.0.0.0/19
BCP 38 Filter = Allow only source addresses from the customer's 96.0.X.X/24



BCP 38 Filter Applied on Downstream Aggregation and NAS Routers

- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Cable Source Verify (MAC & IP)
- Packet Cable Multimedia (PCMM)
- IP Source Verify (MAC & IP)

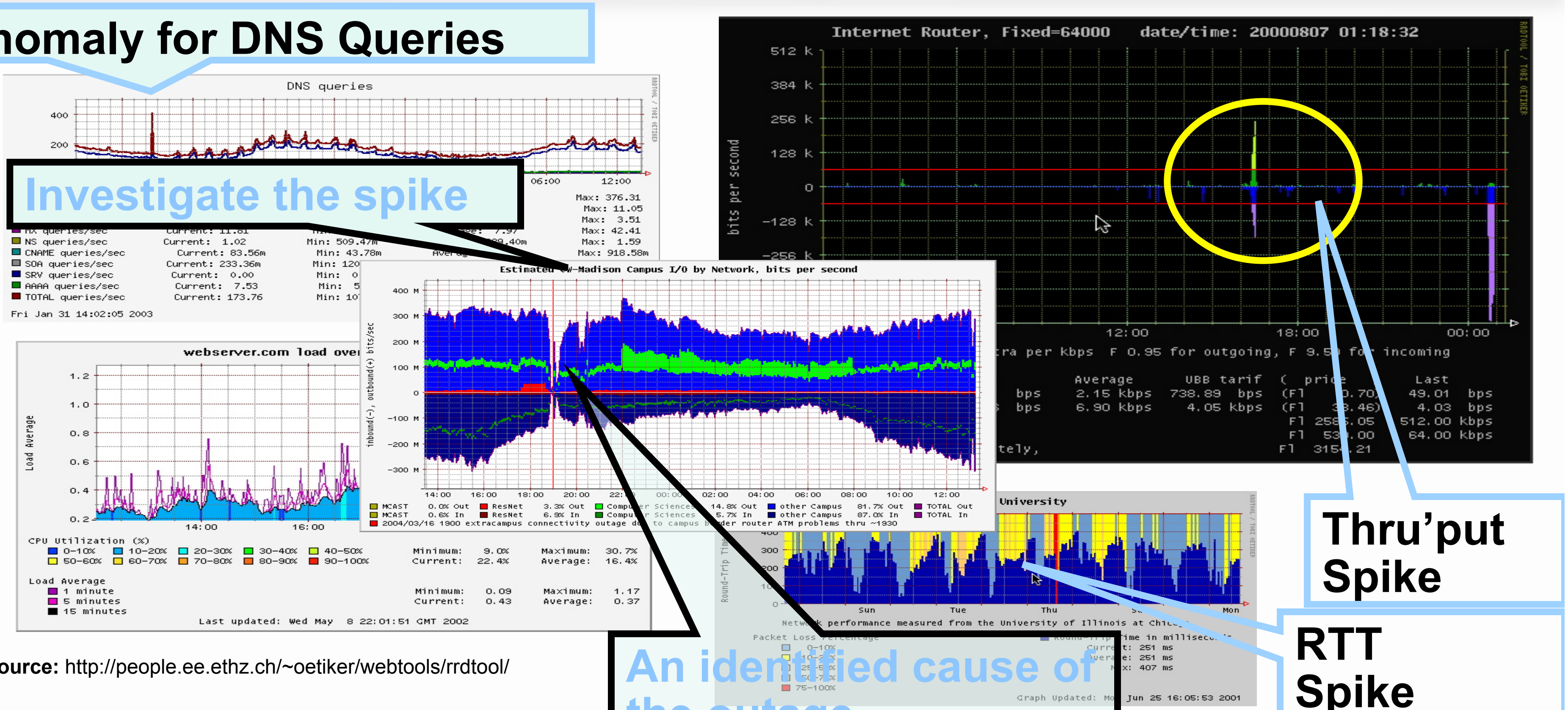
BGP Prefix Filtering



Egress Filter Prefixes to Internet; Ingress Filters Coming from Internet

Customer Filters In and Out

Total Visibility



Anomaly for DNS Queries

Investigate the spike

An identified cause of the outage

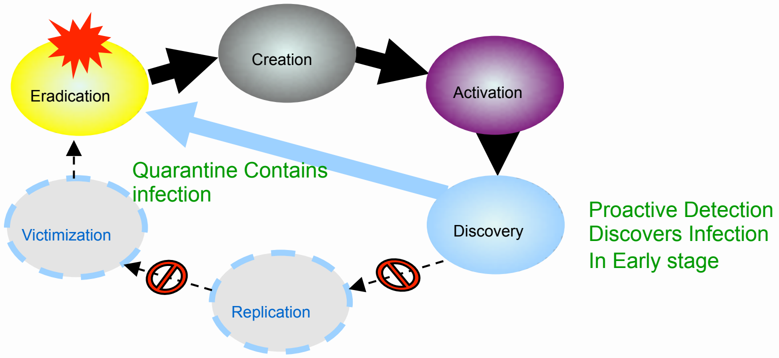
Thru'put Spike

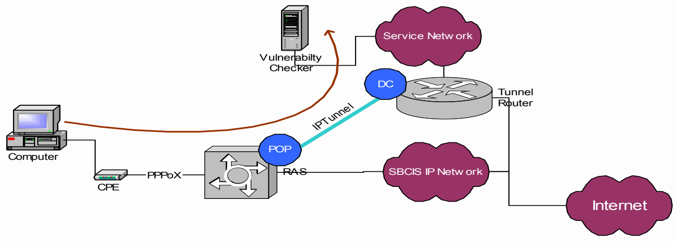
RTT Spike

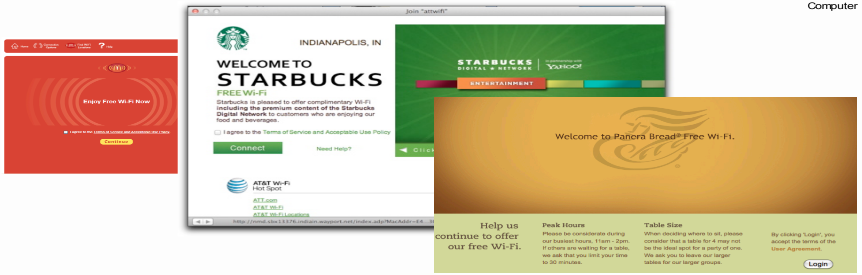
Source: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

Remediating Violated Customers

- We have enough experience in the industry to move remediation of violated customers to a normal part of the business.
- Leaving violated customers on your network puts your whole operation at risk.


Eradication
Creation
Activation
Quarantine Contains infection
Victimization
Discovery
Proactive Detection Discovers Infection In Early stage
Replication





Enjoy Free Wi-Fi Now

□ I agree to the Terms of Service and Acceptable Use Policy.

Continue

Join "attwifi"

INDIANAPOLIS, IN

WELCOME TO STARBUCKS

FREE Wi-Fi

Starbucks is pleased to offer complimentary Wi-Fi **including the premium content of the Starbucks Digital Network** to customers who are enjoying our food and beverages.

□ I agree to the Terms of Service and Acceptable Use Policy

Connect

Need Help?

STARBUCKS DIGITAL ★ NETWORK | in partnership with YAHOO!

ENTERTAINMENT

AT&T Wi-Fi Hot Spot

ATT.com
AT&T Wi-Fi
AT&T Wi-Fi Locations

http://nmd.sbx13376.indiain.wayport.net/index.adp?MacAddr=E4...3

Welcome to Panera Bread® Free Wi-Fi.

Help us continue to offer our free Wi-Fi.

Peak Hours
Please be considerate during our busiest hours, 11am - 2pm. If others are waiting for a table, we ask that you limit your time to 30 minutes.

Table Size
When deciding where to sit, please consider that a table for 4 may not be the ideal spot for a party of one. We ask you to leave our larger tables for our larger groups.

By clicking 'Login', you accept the terms of the User Agreement.

Login

MESSAGING MALWARE MOBILE

Bot Mitigation for ISPs – Link to Materials

http://confluence.senki.org/display/SPSec/MAAWG+26+-+Workshop

M3AAWG
MESSAGING MALWARE MOBILE

This has been the second of six video segments

View the entire

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

from the public training video pages on the M3AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Barry Raveendran Greene
for developing and presenting the material in this series
and allowing M3AAWG to videotape it for professionals worldwide.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG
MESSAGING MALWARE MOBILE

For information about M^{3}AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form