APCO International
Emerging Technology Forum

The Thanksgiving PSAP Cyber Attack: A Case Study

APCO International
Leaders in Public Safety Communications®

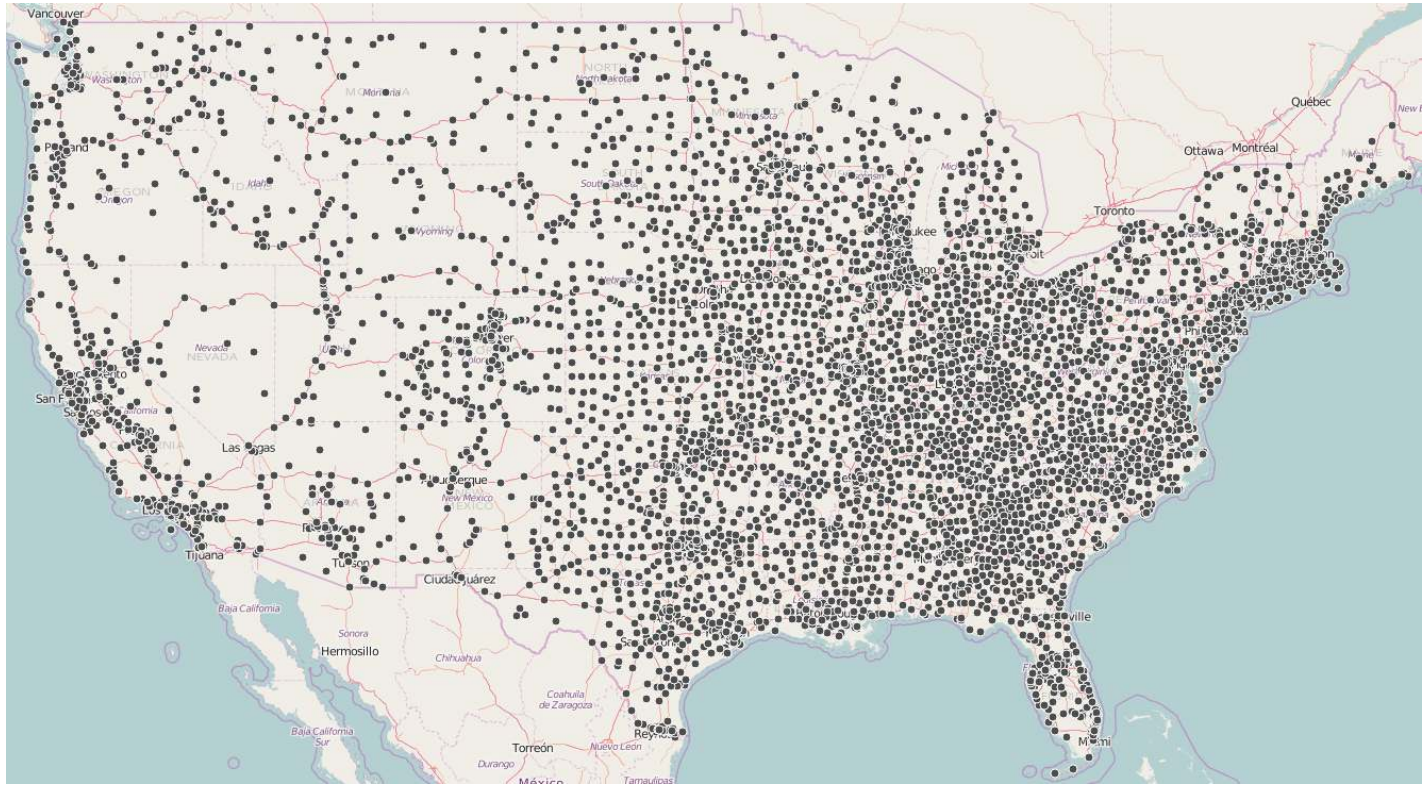
Timothy Lorello – President & CEO of SecuLore Solutions

Tim.Lorello@SecuLore.com

SECULORE™ SOLUTIONS

"Protecting Our Nation's Most Important Number: 9-1-1!"

Why Should You Care About Cybersecurity?



Source: ArcGIS Public Safety Answering Points (PSAPs) Story Map Based upon FCC PSAP Registry (01/15/2016)

Are cybersecurity concerns causing you delays in NG9-1-1 upgrades?

The First Line of Defense

5893 PSAPs
standing in front of
thousands of Police/Fire/EMS departments

Cyber Threats to Public Safety Are REAL

Ransomware payments for 2016 are expected to hit a **billion dollars**, according to the FBI.

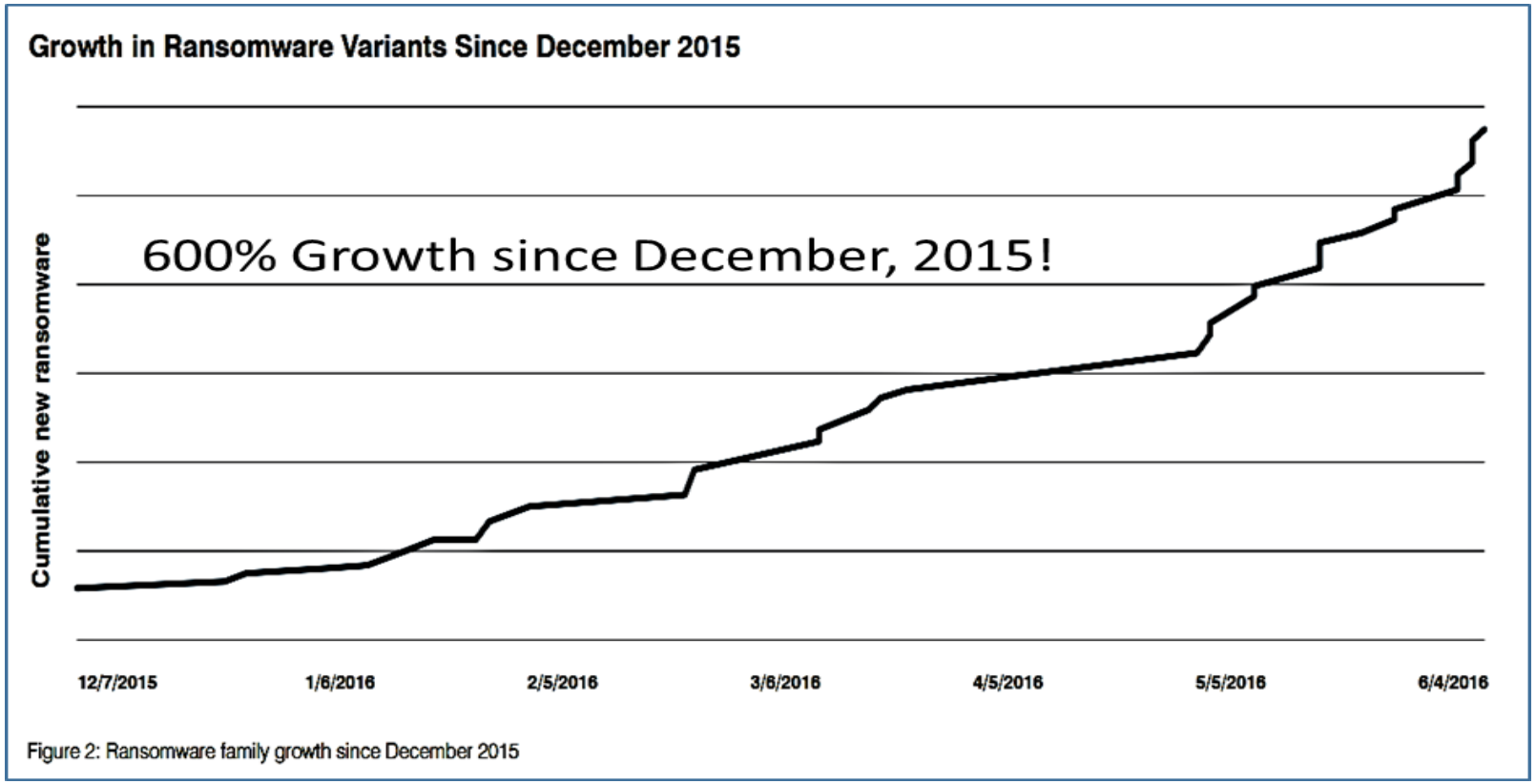


Figure 2: Ransomware family growth since December 2015

Why attack?

- Extortion

"Since 2013, hackers have hit [police] departments in at least seven states…."

States feeling the effects:

Alabama	Massachusetts
Illinois	New Hampshire
Maine	Tennessee
New Jersey	

States Feeling the Effect – More Than Seven! [1]

Collinsville [Alabama] Police Department Hit by Ransomware Trojan (6/2014)

Virus Wipes Out [New Hampshire] Police Department's Computers (6/2014)

Cyber attack temporarily shut down Newark [New Jersey] police computer systems (6/2014)

Dickson [Tennessee] Sheriff's Office pays ransom to cyber criminals (11/2014)

Suburban Chicago [Illinois] PD Forced To Pay A Hacker $500 Ransom For Its Own Files (2/2015)

Tewksbury [Massachusetts] Police Department Pays $500 Bitcoin Ransom to Hackers (4/2015)

Bitcoin ransom paid for Lincoln County [Maine] police data blocked by computer virus (4/2015)

States Feeling the Effect – More Than Seven! [2]

Janesville [Wisconsin] computer systems hit by virus, likely 'ransomware' (1/2016)

[Arizona] Superior Court Attacked By Ransomware (2/2016)

Melrose [Massachusetts] Police Pay 1 Bitcoin to Get Rid of Ransomware (2/2016)

Medfield [Massachusetts] paid hackers a $300 ransom to 'unlock' the town network (2/2016)

City of Durham [North Carolina] avoids ransomware threat by backing up data (2/2016)

Alto [Texas] city office battles ransomware issue (3/2016)

Ransomware virus infects Pinal County [Arizona] Attorney's Office case files (5/2016)

Hackers hit upstate [New York] municipalities with ransomware (5/2016)

Hackers hit Larimer County [Colorado], services impacted (6/2016)

Town of Palm Beach [Florida] fights ransomware attack on 911 system (6/2016)

Virus hits Prior Lake [Minnesota] server; resident data not likely breached (6/2016)

States Feeling the Effect – More Than Seven! [3]

Woodbury County [Iowa] Ransomware Attack Leaves Thousands of Files Compromised (7/2016)

Wadena City [Minnesota] computers infected with virus (7/2016)

[Florida] City of Sarasota's system hacked by ransomware, data held hostage (8/2016)

City takes swift action after ransomware infects Honolulu [Hawaii] Fire Department computers (9/2016)

Crow Wing County [Minnesota] Board: Back up or pay up: County fights against ransomware (9/2016)

Springfield [Tennessee] City Hall recovers from ransomware attack (9/2016)

Palmhurst [Texas] Police Department Avoids Data Loss (9/2016)

Mount Holly Springs [Pennsylvania] police fall victim to cyber attack (10/2016)

Ransomware Result: Free Ticket to Ride in San Francisco [California] (11/2016)

Ransomware targets Howard County [Indiana] government (11/2016)

Madison Co. [Indiana] government servers fall victim to hackers, ransomware (11/2016)

[Arkansas] sheriff's office hit by ransomware pays hackers (12/2016)

Mount Pleasant [South Carolina] Police Department hit with ransomware cyberattack (12/2016)

Case Study: The Thanksgiving PSAP Attack

- Employee system was compromised via email phishing campaign
  - Email phishing campaign was conducted against multiple email addresses
  - Anti-virus software stopped approximately 38% of attacks seen
  - One employee was tricked into opening an offensive document, infecting the machine
    - The workstation reached out for malicious malware – believe it was stopped
    - Mamba ransomware later encrypted drive, destroying remaining evidence

- Web Server was compromised
  - Attacker used known vulnerabilities against WebLogic server
  - Delivered "Mamba" ransomware to over 100 servers and workstations
    - Mamba does full-drive encryption, disabling entire system
    - Mamba looks for and encrypts all shared storage drives as well

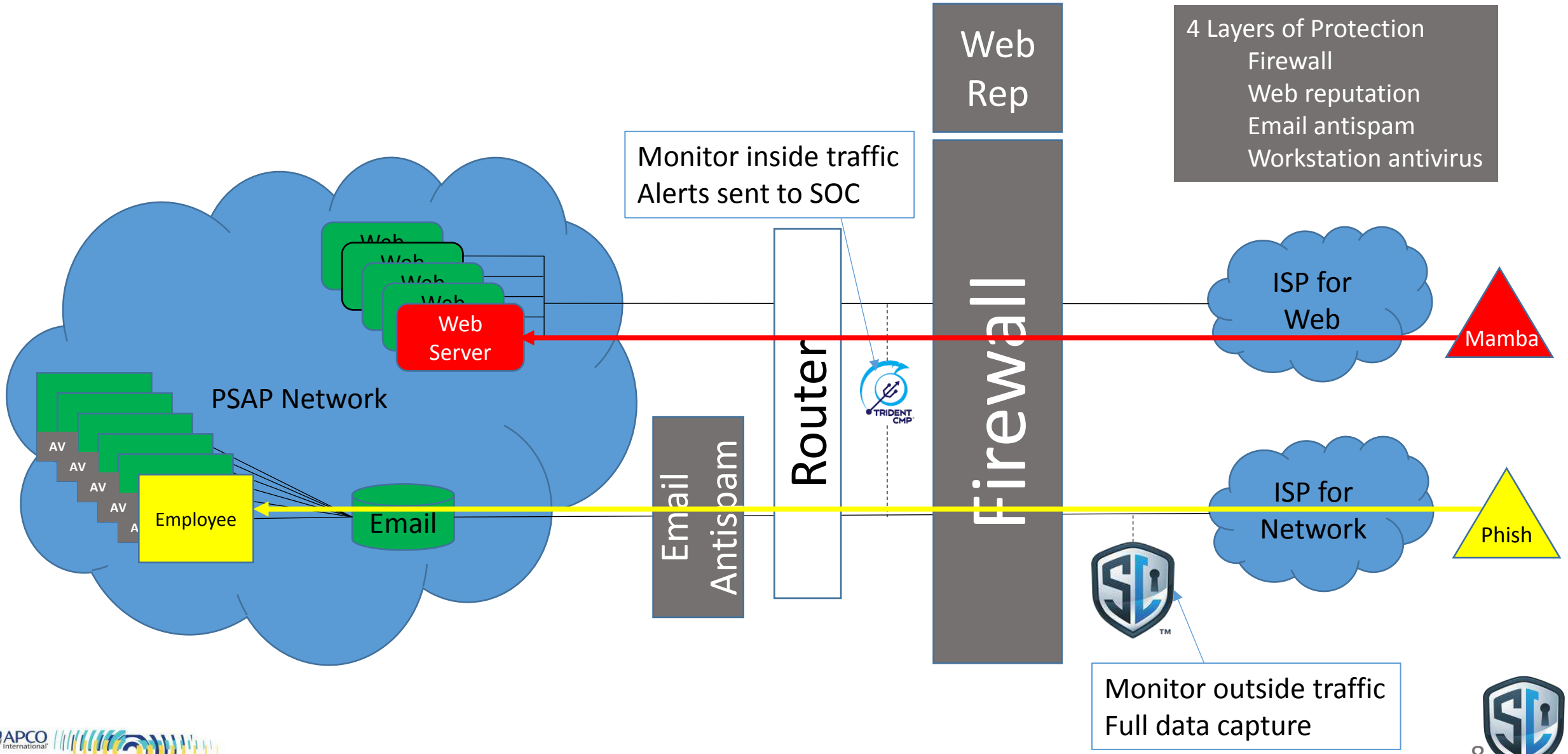
- Small data transfer occurred with Russian Server
  - Seen shortly after email phishing attack
  - Not related to ransomware attack (or was it)

- Remote process execution console (psexecsvc.exe) detected on various servers
  - Not related to ransomware attack (or was it)

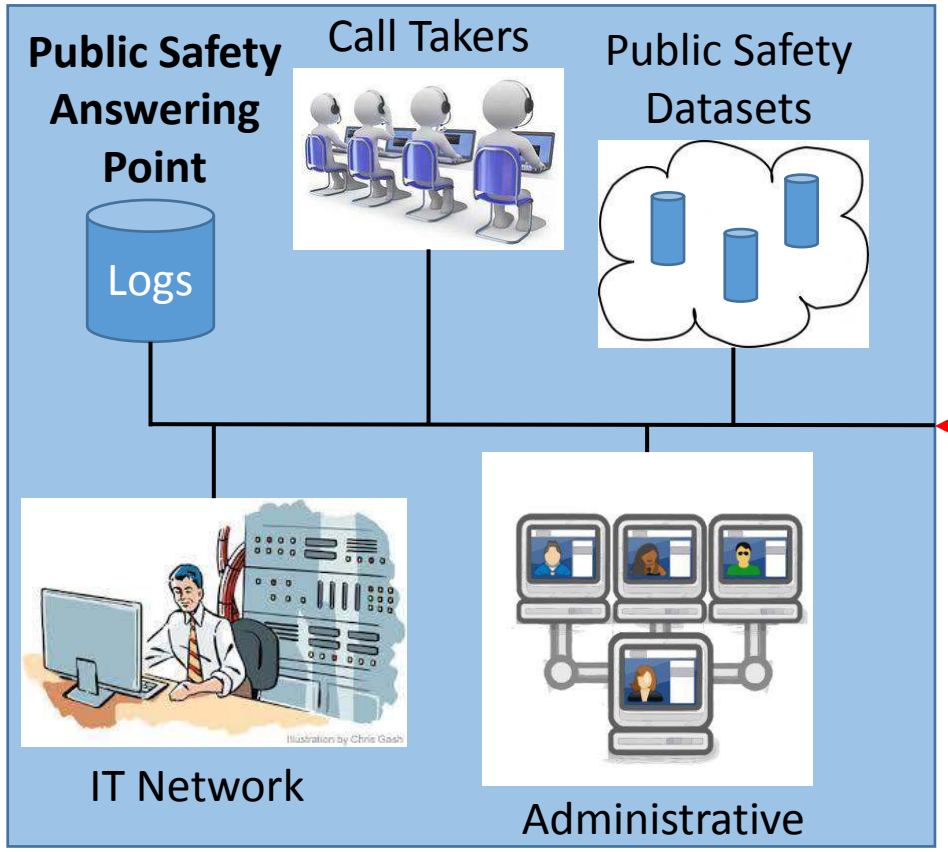
- Adware/malware seen on multiple systems
  - Not suspected of malicious activity (but confusing)

Five separate malicious activities
Attack spanned 44 hours
IT team wrestled for 3½ days
3 months later, still recovering

PSAP Network Protections in Place



Ransomware: It Starts with Finding a Way In



Attacker may:

1) Probe the network
2) Send continuous interrogations
3) Send continuous phishing attacks

An email attack, intended to cause the victim to make a selection installs malware on the victim's machine

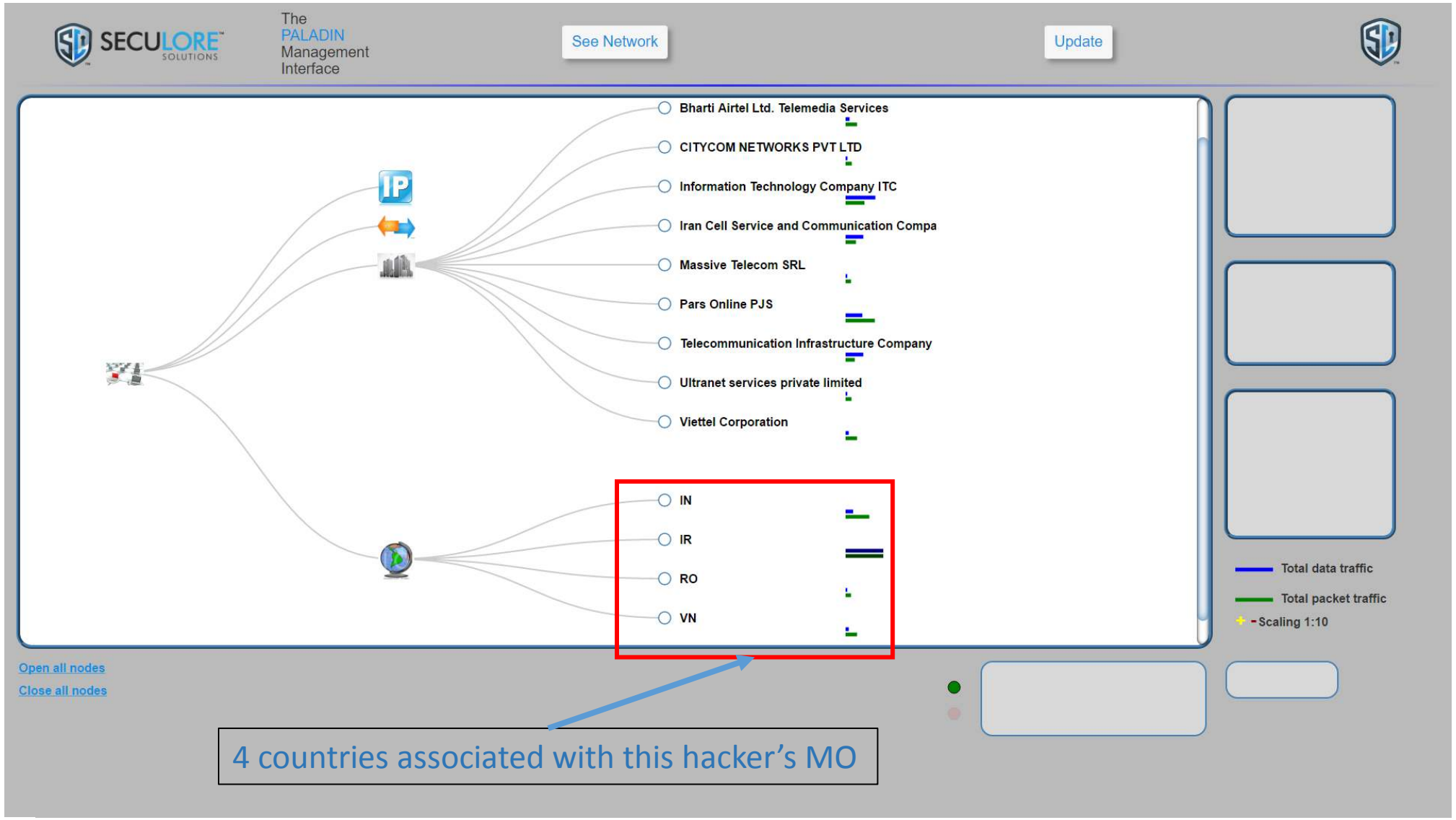
Network Provider

Hacker rents an exploit kit

"Command and Control" server

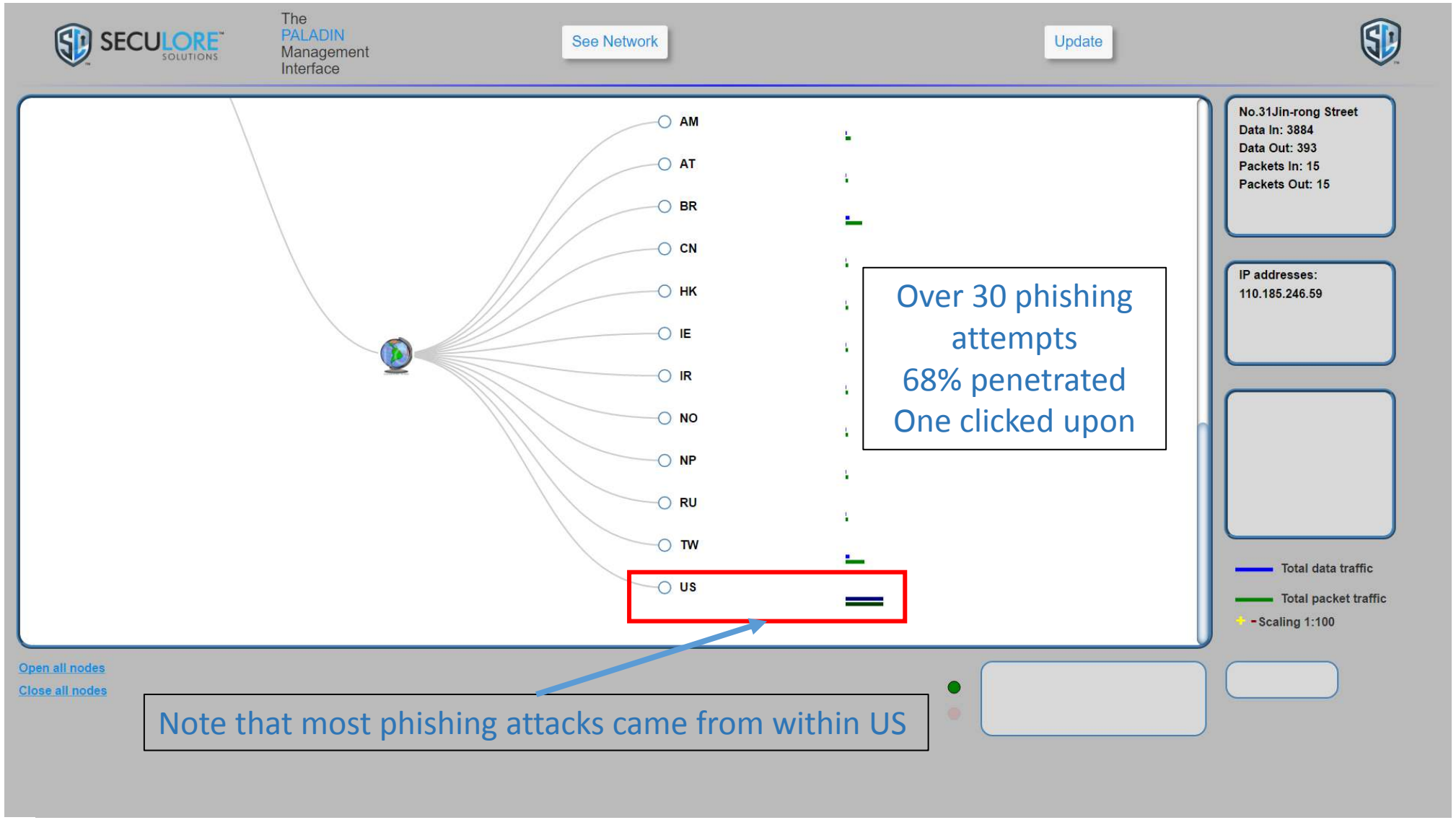
Case Study: The Scan – The Fake – The Strike

Step One
The Scan



Case Study: The Scan – The Fake – The Strike

Step Two
The Fake



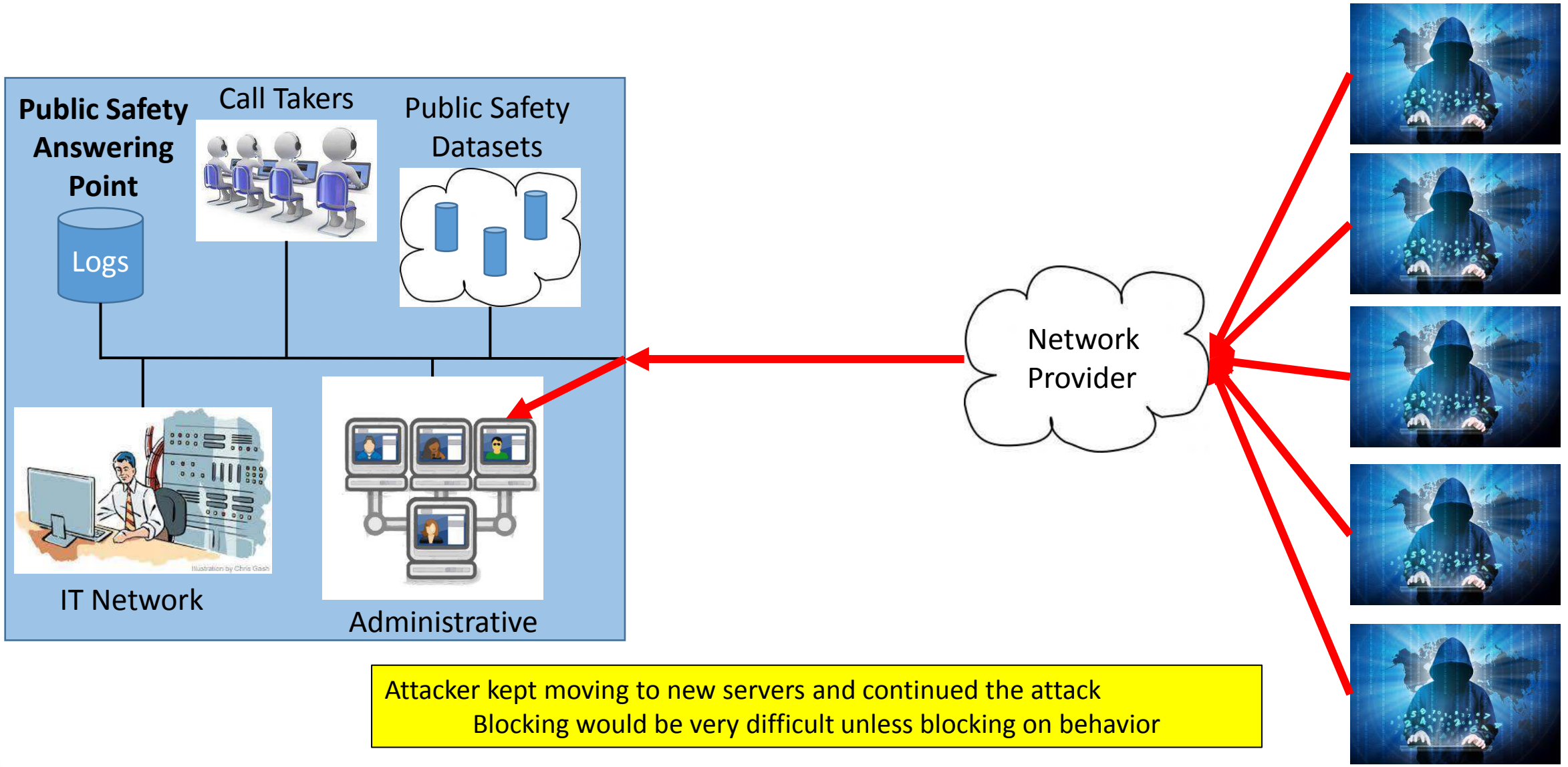
Case Study: The Scan – The Fake – The Strike

Step Three
The Strike

Time	WebLogic Attack	Brief Description	Attacker Information
11/24-07:34	Tor Exit Node Detected	Source IP = 185.129.62.63	Copenhagen, Denmark
11/24-07:34	Vulnerability found	css.jsp	
11/24-07:38	Active Directory info	"C:\temp\com.csv" uploaded to attacker	
11/24-07:39	Possible target list	"list.txt" downloaded to target	
	Mamba ransomware loaded	"output.zip" downloaded to target	
11/24-08:02	Status being checked	Source IP = 46.166.148.176	<Unknown City>, Netherlands
11/24-08:10	Status being checked	Source IP = 176.126.252.12	<Unknown City>, Romania
11/24-08:12	Status being checked	Source IP = 81.7.13.181	<Unknown City>, Germany
11/24-08:34	Status being checked	Source IP = 176.10.99.207	<Unknown City>, Switzerland
11/24-08:36	Status being checked	Source IP = 168.1.6.51	Sydney, Australia
11/24-08:37	Status being checked	Source IP = 193.90.12.90	Oslo, Norway
11/24-08:46	Status being checked	Source IP = 199.68.196.124	San Jose, United States
11/24-08:55	Status being checked	Source IP = 37.130.227.133	<Unknown City>, United Kingdom
11/24-11:41	Status being checked	Source IP = 173.208.213.114	Kansas City, United States
11/24-12:09	Status being checked	Source IP = 176.31.7.241	<Unknown City>, France
11/24-12:29	Status being checked	"log_file.txt" Mamba file uploaded to attacker	
11/24-13:33	Status being checked	Source IP = 171.25.193.78	<Unknown City>, Sweden
11/24-13:57	Status being checked	Source IP = 37.187.129.166	<Unknown City>, France
11/24-14:21	Status being checked	Source IP = 216.244.66.231	Seattle, United States
11/24-14:35	779 bytes FTP'd to attacker	Source IP = 37.187.129.166	<Unknown City>, France
11/24-14:38	Last interaction detected	SecuLore monitoring removed	

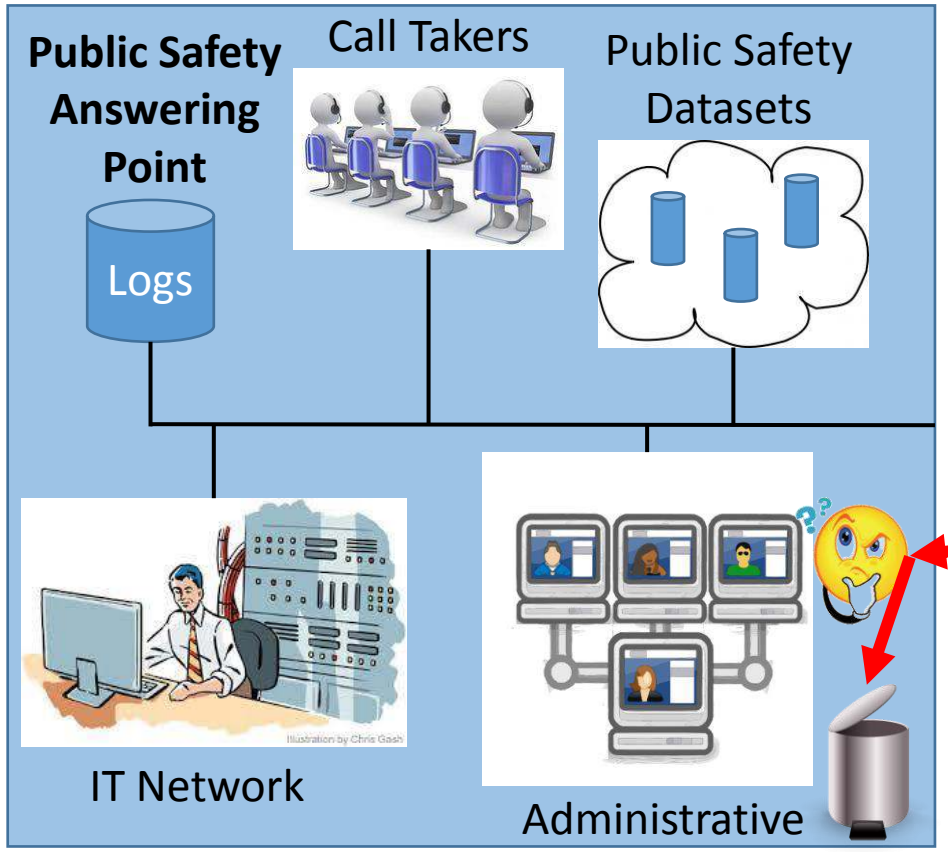
The attacker origin automatically moved (courtesy of The Onion Router (TOR)

A Polymorphic Attack Vector



Attacker kept moving to new servers and continued the attack
Blocking would be very difficult unless blocking on behavior

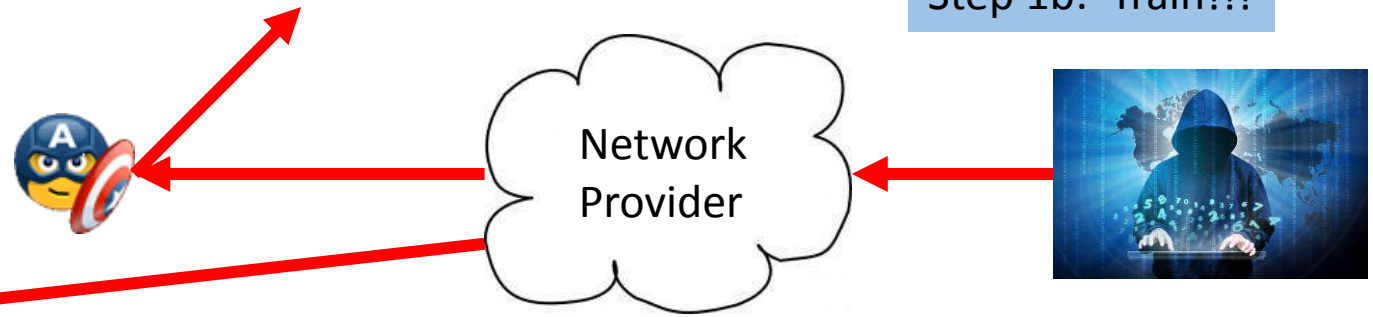
Thwarting a Ransomware Attack (1/6)



Step 1: Identification

Step 1a: Deflect!!!

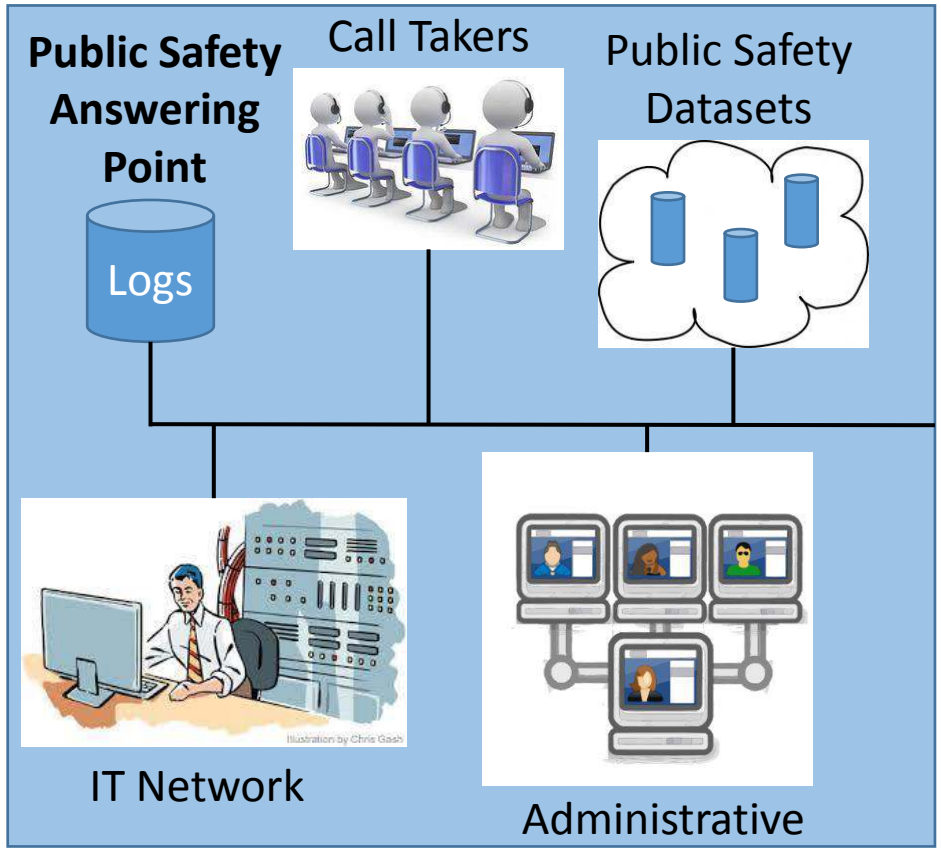
Step 1b: Train!!!



Attacker may:

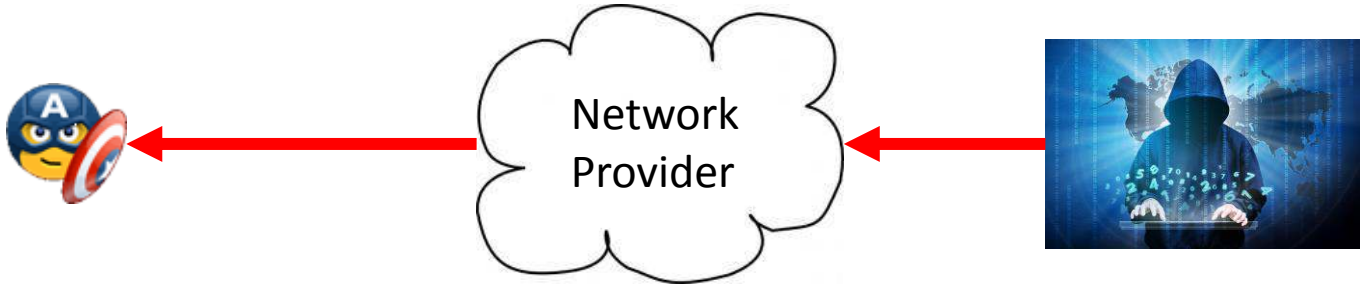
1) Probe the network
2) Send continuous interrogations
3) Send continuous phishing attacks

Thwarting a Ransomware Attack (2/6)



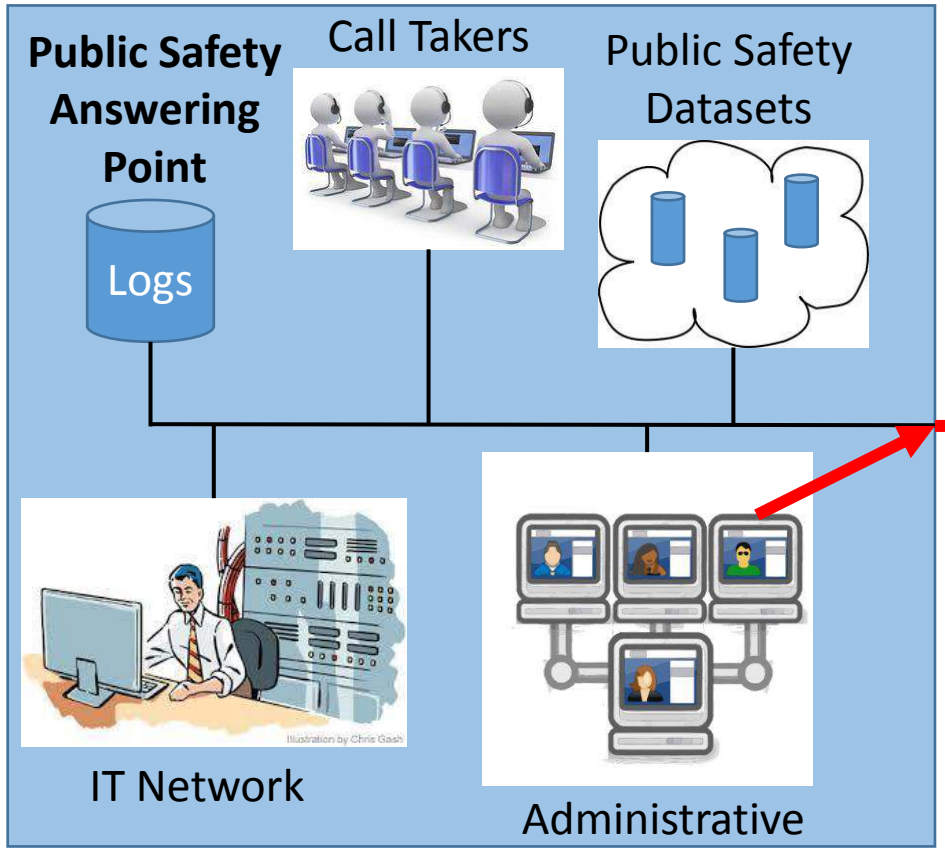
Step 2: Exploitation

Step 2a: Blocking



Stop the exploit from reaching the intended target

Thwarting a Ransomware Attack (3/6)



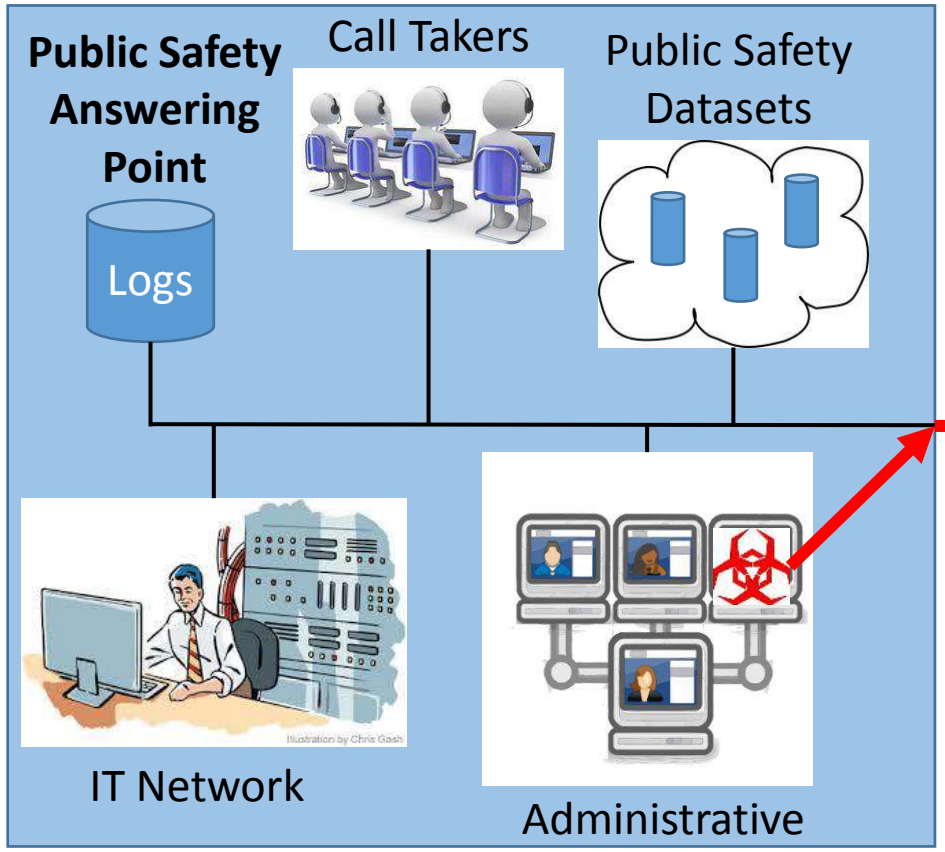
Prevent ransomware retrieval
"HQ" are known bad actors

Step 3: Retrieve Ransomware

Step 3a: Stop retrieval

Network Provider

Thwarting a Ransomware Attack (4/6)



Prevent key exchange
Look for bad behavior

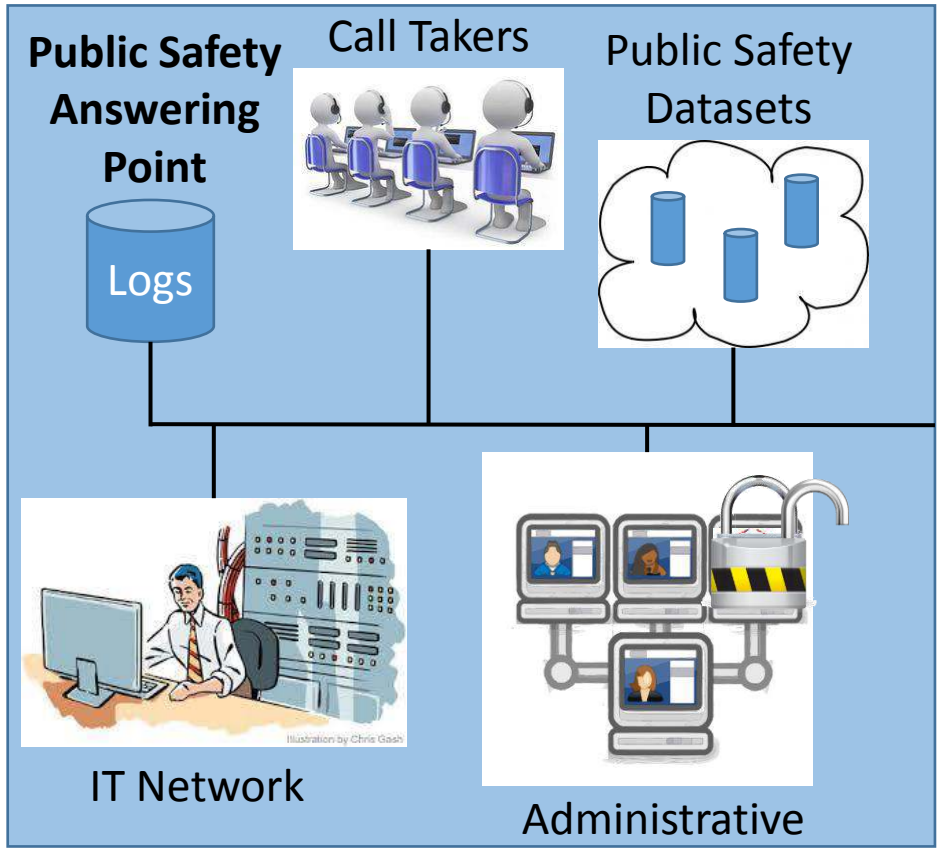
Step 4: Key exchange

Step 4a: Stop key exchange

Network Provider

Have an End Point Security system that scrubs the malware

Thwarting a Ransomware Attack (5/6)



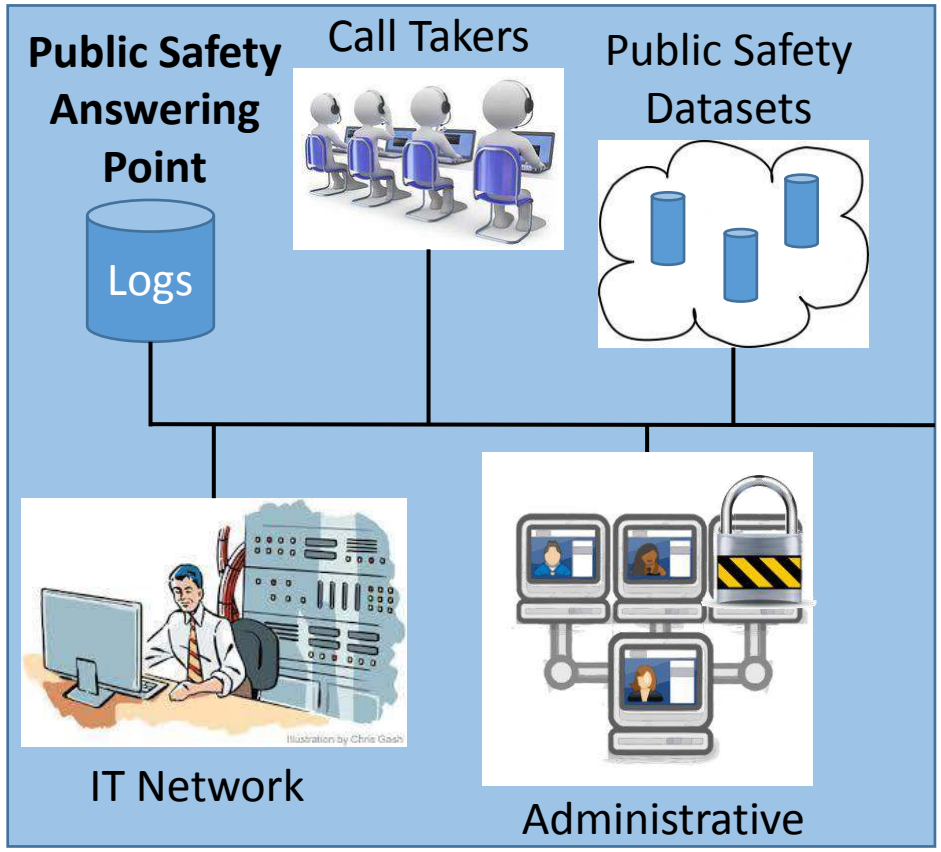
Step 5: Encryption

Step 5a: Stop encryption

Network Provider

Remove encryption tools from systems
Protect common exploit directories
Capture keys and unlock files

Thwarting a Ransomware Attack (6/6)



Don't pay the ransom!

Step 6: Extortion

Step 6a: Deny extortion

Do not contact the hacker

Network Provider

Restore system from good backups

Morals of the Story

Patch Your Systems (vendors too!)

Train Your Staff

Keep complete/regular backups

Let Your IT Staff Show Their Abilities!

Monitor – Visualize - Protect

Questions?

SECULORE™ SOLUTIONS

“Protecting Our Nation’s Most Important Number: 9-1-1!”

The Thanksgiving PSAP Cyber Attack: A Case Study

Timothy Lorello – President & CEO

Tim.Lorello@SecuLore.com

(410) 703-3523