

Security Data Analytics as a Guide for Intruder Hunting

**Bruce Roton : CISSP, CISM, CEH, CISA, CGEIT, ISO27001, CSSGB
Sr. Director, Security Solutions Architecture**



Disclaimer:

The purpose of this presentation is solely educational.

The content and opinions contained in this presentation are attributable to me solely in my personal capacity, and are neither endorsed by nor reflect the opinions of my employer, Level 3 Communications.

Section 1: Initiating an Intruder Hunting Program

Bruce Roton

CISSP, CISM, CEH, CISA, CGEIT, ISO27001, CSSGB, CCSFP

Sr. Director, Security Solutions Architecture, Level 3 Communications



What is Intruder Hunting

- **Intruder Hunting is a process for aggressive intruder detection and eviction, focused on specific targeted assets.**
- The basic components of the program include:
 - Program Charter and Job Descriptions for team
 - Establish and Implement Security Baselines and Standards
 - Target Selection (**Huntscape**) based on Risk Evaluation and Evidence Assessment
 - Monitoring Targets and setting Intruder Traps (Intruder Herding)
 - Identify and Report on Intrusions and Intrusion Attempts
 - Eviction and Remediation
- Must include **Recovery Point Plans** for target systems.
- Must include a **“Reporting Trust Plan”** (discussed later)

Information Security Management System (ISMS)

Initiation

- Pick a Standard Framework (ISO27001, NIST-800, PCI, etc...)
- Senior Management buy in is essential
- Allocate resources and fund the program (or fail)
- Define the goals, objectives, and charter (AKA Policy Statement)
- Identify your practice areas and assess your maturity (CMM).

Practice

- Data Classification and Valuation
- Data Discovery and Isolation
- Create an Incidence Response Policy and Program
- Define the Charter for the Intruder Hunting Program
- Define process for monitoring, measuring and reporting on progress, with a “Continuous Improvement Plan”

Intruder Hunting and the Organizational Structure

- Red Team versus Blue team Considerations
 - Intruder Hunting is an aggressor sport, so Red Team skills are more suited to the job. Not the only option, just better.
- Required skills
 - Risk Management and Assessment
 - Penetration Testing Methodology
 - Computer Forensics Tools and Methodology
- Specialized SOC function utilizing resources from the Forensics, Audit, and VM/Pen-test Teams
- Leader reports to highest ranking Security Leader (Director of Security Operations or the CISO) with dotted line reporting to Chief Legal Officer
- **Who does your CISO report to? Is your organizational structure creating a conflict of interest?**



Security Controls Baseline and Validation

- Basic “blocking and tackling” (Firewalls, IPS, Endpoint Sec, system logging, vulnerability scanning, and traffic monitoring)
- Regular Penetration Testing (**change testers/vendors regularly**), and use **External Counsel for all Assessments and Pen Tests**
- Expand standard controls for Target Systems: Data Analytics
 - User account monitoring
 - Memory, Disk, Processes, Services, and Network Monitoring
 - Full Log Monitoring and Analysis
 - Configuration Change Monitoring (processes, ports, serviced, files)
- All validation assessments should be driven by Data Classification
- **Define 3-4 classes of data, no more.** Examples:
 - **Public** – Any access
 - **Company Confidential** – Employee info, Marketing, Pricing, etc
 - **Compliance Sensitive** – PII, Financial, Health, ect
 - **Critical** – Operations flow, critical IP, business damaging, business terminating.

Section 2: Defining the HuntScape

Bruce Roton

CISSP, CISM, CEH, CISA, CGEIT, ISO27001, CSSGB, CCSFP

Sr. Director, Security Solutions Architecture, Level 3 Communications

Scope of the Intruder Hunting Program

- Define the scope of the Intruder Hunting program based on Company Resources, Assets, and Risk.
- Do you have the internal resources to operate an IH program?
 - Do you need external resources, or training? Maybe a two week crash course is enough to get started.
- How many assets do you have? If many high-risk targets, consider periodic target rotation. Rotation times should be less than 6 weeks.
- **Document your Risk Assessment findings as a Coarse Guidance System for Targeting.**
- **Use OSINT and Industry Peer groups for Target Fine Tuning**
 - Industry vertical Breach Reports
 - Researcher blogs and reports shouldn't be overlooked
 - Peer groups should be formed or tapped if already existing (industry and geo)
 - Local and federal law enforcement relationships should be maintained
- **Use a Threat Intelligence Program for In-Flight Course Corrections**

Using Risk Assessment Models

- Use Standardized Risk Assessment Frameworks (they're FREE - *mostly*)
 - And, they provide consistent risk treatment (thus the term "standardized")
- **NIST 800-30 Guide for Conducting Risk Assessments**
 - THE FUNDAMENTALS
 - RISK MANAGEMENT PROCESS
 - RISK ASSESSMENT
 - KEY RISK CONCEPTS
 - APPLICATION OF RISK ASSESSMENTS
 - THE PROCESS
 - PREPARING FOR THE RISK ASSESSMENT
 - CONDUCTING THE RISK ASSESSMENT
 - COMMUNICATING AND SHARING RISK ASSESSMENT INFORMATION
 - MAINTAINING THE RISK ASSESSMENT
- **ISO 27005 Information Security Risk Management (ISRM)**
 - Overview of the ISRM Process
 - Context Establishment
 - Information Security Risk Assessment (ISRA)
 - Information Security Risk Treatment
 - Information security Risk Acceptance
 - Information security Risk Communication
 - Information security Risk Monitoring and Review

Who is Larry?

Larry is a bright, outgoing, entrepreneurial kind of person. When in college, Larry was in the top of his class and earned a degree in biology, specializing in molecular chemistry. Everyone expected Larry to go on to medical school, but Larry decided on another path after getting his Master's degree. Larry graduated with honors in spite of occasional reprimands from his University for organizing environmental protests and his two arrests for involvement in unlawful Greenpeace activities.

Pease identify the most probable current situation for Larry now that he is 10 yrs out of college.

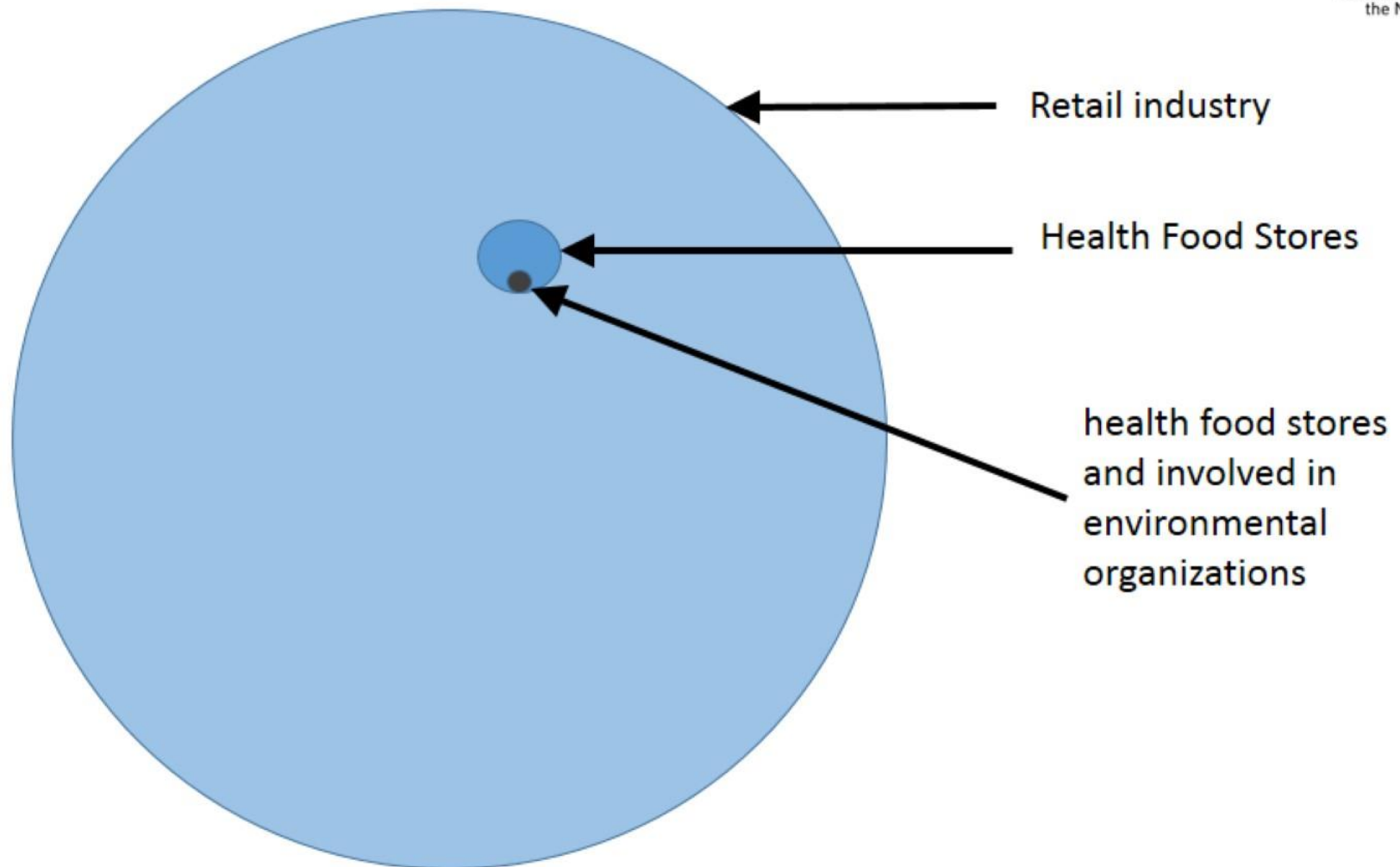
1. Larry is a director at a hardware manufacturer.
2. Larry owns a chain of health food stores and is involved in environmental organizations.
3. Larry is a sales person for a health insurer.
4. Larry works in the retail industry.

What are the Bad Guys After?

- You have 10 assets that you gauge to be of equal value.
- The last four times the company had an intrusion attempt, the intruders were targeting asset number 3.
- What is the probability the next intruder will most desire access to asset number 3? (90%, 75%, 50%, 25%, 10%)
- Did you consider the following?
 - Is asset number 3 simply the first target that intruders are likely to encounter after breaching external defenses?
 - Is asset number 3 simply the least well defended?
 - Is all of this just a coincidence that would become evident with a larger sample size over multiple organizations with similar assets?
 - Why are you making assessments of the desires of strangers?
- The two logic flaws here are called “Belief in Small Numbers”, and “the Availability Error”

Thanks to Amos Tversky and Daniel Kahneman for their work in the psychology of judgment and decision-making in situations of uncertainty, as well as behavioral economics.

Representative Error



Again, thanks to Amos Tversky and Daniel Kahneman for their work in the psychology of judgment and decision-making, as well as behavioral economics.

There are only 4 types of value

1. Use Value: Utility and availability risk
2. Confidentiality Value: Regulatory risk, litigation risk, and loss of competitive advantage associated with exclusive use
3. Integrity Value: Reliability in the accuracy of data (Regulatory risk litigation risk, process failure, and operational inefficiency)
4. Reputational Value: Damage to public and partner trust

Risk Scenario analysis and scoring against assets

- First, understand the value proposition of your potential adversaries.
- Can they make money from you? (Extortion, direct access to digital cash, resell of data, use you for other attacks, national competitive advantage)
- Are you critical infrastructure? (Cyber warfare, battlefield preparation, active destruction campaign, operational intelligence and intellectual property theft)
- Political, environmental, financial practices and affiliations.
- Some people just want to watch the world burn. (Digital Arsonists)

Backup Critical Servers to off-line, rotating storage

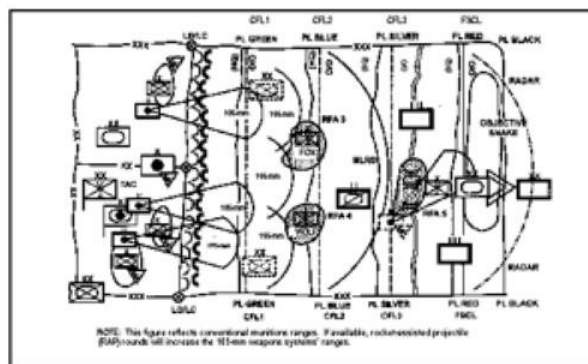


Understanding the “Kill Chain” and its Variants

- Originally a military combat term. An integrated process **requiring continuous integrity for success.**

F2T2EA

- Find: Locate the target.
- Fix: Fix their location; or make it difficult for them to move.
- Track: Monitor their movement.
- Target: Select an appropriate weapon or asset to use on the target to create desired effects.
- Engage: Apply the weapon to the target.
- Assess: Evaluate effects of the attack, and any intelligence gathered at the location.



The Evolved Attack Event Chain

It has been said that defenders have to get it right all the time, while attackers only have to get it right once to succeed. Not as true today as it was 10 years ago!

0. Presales Monetization
1. Reconnaissance and discovery
2. Attack strategy and exploit development
3. Initial intrusion (establishing a beachhead)
4. Gain Persistence
5. Target acquisition (locating the valuables)
6. Creation of an exfiltration path
7. Capture, encryption, and exfiltration.
8. Monetization

Detectable Functions

- Scanning/Recon
- Phishing
- Malware download
- Lateral Movement
- C2 Comms



Section 3: Automated and Manual Analysis Datasets & Collection of Data and Data Reduction Rules

Bruce Roton

CISSP, CISM, CEH, CISA, CGEIT, ISO27001, CSSGB, CCSFP

Sr. Director, Security Solutions Architecture, Level 3 Communications



Data Scientist: A person employed to analyze and interpret complex digital data, such as the using statistical analysis complex cross-correlation rulesets, in order to assist a business in its security decision-making.

- “To the extent possible, all decisions should be evidence based.”

But do not forget...

- “Evidence evaluated and interpreted in the absence of scientific methodology spawns myth and monsters.” In other words, intuition is not your friend.
- “The ignorance of, or denial of reality does not alter reality. It simply renders one less empowered to deal with reality.”
- “If you don't know where you are going, you'll end up someplace else.”

You Can't Write Rules to Look For Suspicious, Until Define Suspicious in the Context of Your Environment

- Are rare outbound blocked packets corrected behavior?
- **What is the normal behavior of my target system? Is it doing something outside of that behavior model? How would I know if it was?**
- What heuristics can I create based on my network behavior?
- Should that server ever communicate with anyone outside this network?
- **Where is Data-XXX supposed to live and have you seen it anywhere else?**
- Exactly who should be accessing those data stores?
- Should Fill in the blank type of data be traversing your network?
- Do you have a business partner in Ukraine?
- **Are there a few systems that are perfectly patched? Did you do that?**
- Should that comms channel really be encrypted?
- Why is there a Telnet session running on port 25?
- Are you old enough to be talking to me? Consider Domain ages
- **Are bad guys testing exfiltration path strategy on “expendable” asset**

Where Do You Start?

- **Buy tools or DIY with the free stuff (DIY focus here!)**
- Understand the technologies (Manual and Automated Big Data Analysis)
 - DNS Monitoring and Analysis (A)
 - Network Monitoring and Analysis (A)
 - Reconnaissance Monitoring (A?)
 - Intruder Traps and Honey Pots (A??)
 - Log Monitoring and Analysis (A?)
 - Memory Monitoring and Analysis (M/A??)
 - Disk Monitoring and Analysis (M/A??)
 - Searching the Registry for persistence (M/A??)
 - Processes and System Services Monitoring (M/A??)
 - Deriving Threat Intelligence to refine and focus the HuntScape (BD Automation)



Targeting With DNS Data Analytics

- Multiple Approaches to identify Malicious Domains:
 - Check for comms with IPs that don't have related nslookup queries. May be legit, or may be old-school hacker fixed IP.
 - Develop white list for server based nslookup queries. Note that some servers should never make DNS queries.
 - Identify Fast-flux domains - Malware related domains tend to have a short TTL with constantly changing destination IP addresses for a single DNS domain name
 - Track create dates and domain history
 - Track associated IP range ownership over time.



- **Catches the obvious**
 - Abuse (iTunes and web-radio) and Misuse (P2P and Gaming)
- **Catches the less obvious**
 - Communications to restricted or suspicious locations
 - Unexpected/Banned protocols and Encrypted channels
- **Can catch the true outliers (a bit more work/storage)**
 - Rare Communications and slow but regular communications
 - New behaviors and connections
- **Data Mining for Traffic Signatures**
 - Packet size within sequence: fingerprint potential malware download
 - Conversation timing: Associating packet delta with specific malware
 - Flags and window size: Fingerprinting systems and malware

$$3987^{12} + 4365^{12} = 4472^{12}$$

- There are two sides to every equation (**although they may not actually be equal**). You've identified all the potential targets, but it is still helpful to know WHO is targeting your organization.
- What type of reconnaissance are they running against you?
 - Direct Scanning? What's the "volume", "quality", and "specificity" of the scan?
 - Web and Application crawling? Look for TTPs, efficiency, "volume".
 - Metadata hunting? What can they collect and how will it influence targeting? Would you even notice the collection of this data?
 - There is always more than one way to get to a target. **1729** Did the attacker discover a path to the target you hadn't thought of?
 - Can you spot an attacker making any attempt to appear as part of your legitimate communications ecosystem?
 - Social Media? Are employees being targeted? What might the attacker find? Passwords, Corp Info, relationships, systems and defenses? (Highly manual analysis today.)

Advanced Honeypots and Tar Pits

- Modern honeypots have changed
 - Multi context (Related Server Systems, not single server)
 - Active appearance (Logs, Files, Users, etc)
 - Moderately Self Defending
- Best defense against a determined adversary
- Used to delay and distract
- System context switching is needed for intruder redirection.
- Ideal for forensics data collection
- **Advanced heuristics can be used to identify attacker and goals;**
 - Target selection
 - Attack technique
 - Malware usage
 - Keystroke behavior (error rate, type rate, command use and rate, command frequency, etc)



- **What we can see in memory**

- Processes (Path/Process Name, Version, Date/Time, Parent, MD5)
- Dynamic Libraries (Path, Version, Linked Process, MD5)
- System Drivers (Path, Version, Linked Process, MD5)
- File Versions (For cross reference back to disk file)
- Descriptions (For cross reference back to disk file)

- **Examination tools**

- Process Explorer
- Process Monitor
- Winhex
- Microsoft Windows Executables (wmic, tasklist)
- **Volatility**

- **Specialized tools for firmware (Used for malware persistence)**

- Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images. Binwalk uses the libmagic library, so it is compatible with magic signatures created for the Unix file utility.



Disk Monitoring and Analysis

- **What we can see on the Hard Drive / Disk**

- Registry Keys (Focused on Startup Locations)
- OS area of the File System (Files and Directories)
- Dates and Times
- File Version
- Startup Locations



- **Examination tools**

- Regedit
- **FTK Imager**
- **The Sleuth Kit**
- **Autopsy**
- **PTK Forensics** (add on to Autopsy)
- HashKeeper
- Xplico
- Windows Registry Recovery
- Winhex
- Microsoft Windows Executables (wmic, at, find, findstr, reg)



A Deeper Look at Disk Files and Analysis Rules

- System files in atypical directories or Subtle deviations in file names
- Persistent Locations (Services, RunKeys, Active Install Keys, etc.)
- Network indicators and new listening ports *** **System Services**
- Command Line Arguments (net use, netsh, cmd/c, -pass= and -pw=)
- Registry Modifications (Regadd, Regdelete)
- **Static Analysis Indicators of Compromise**
 - Compile Date – Does it match the date on a verified system?
 - Create Date – When was the file created on the file system?
 - PE Version Number –What’s the version number of the file?
 - MD5 Hash – Not just a matching, but one that matches a known good system.
 - PE Section Hash – Can you find a match to known malware?
 - Strings–Are there any clear text strings that can be used as indicators?
- **Tools to use during Static Analysis**
 - PE (portable executable) Tools (PE Investigator, PEID, PEView, StudPE)
 - WinHex (Review \$MFT, Registry,PE File strings)
 - SysInternals (Strings)

Kali Linux: So Many Tools in One Place!

- Information Gathering
- Vulnerability Analysis
- Exploitation Tools
- Wireless Attacks
- **Forensics Tools**
- Web Applications
- Stress Testing
- **Sniffing & Spoofing**
- **Password Attacks**
- **Maintaining Access**
- Hardware Hacking
- **Reverse Engineering**
- Reporting Tools



- **Binwalk**
- bulk-extractor
- Capstone
- chntpw
- Cuckoo
- dc3dd
- ddrescue
- DFF
- diStorm3
- Dumpzilla
- extundelete
- Foremost
- Galleta
- Guymager
- iPhone Backup Analyzer
- p0f
- pdf-parser
- pdfid
- pdgmail
- peepdf
- RegRipper
- **Volatility**
- Xplico

Can you leverage these techniques to create automated collection and normalize the data for analysis?

Common Persistent Locations in the Registry

- **Services**

- HKEY\SYSTEM\CurrentControlSet\services

- **Run Keys**

- HKEY\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

- **Winlogon**

- HKEY\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
- HKEY\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
- HKEY\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

- **Startup Folder**

- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

System Process Evaluation

Highly manual method – Can this be automated?

Windows Task Manager

File Options View Help

Applications Processes Services Performance Networking Users

Image Name	User Name	CPU	Memory (Private Wor...	Description
vmware-vmx.exe	roton.bruce	00	26,252 K	VMware Workstation VMX
vmware-usbarbitrator64.exe	SYSTEM	00	3,012 K	VMware USB Arbitration Service
vmware-unity-helper.exe *32	roton.bruce	00	10,800 K	VMware Unity Helper
vmware-authd.exe *32	SYSTEM	00	4,332 K	VMware Authorization Service
vmplayer.exe *32	roton.bruce	00	35,744 K	VMware Player
vmnetdhcp.exe *32	SYSTEM	00	7,788 K	VMware VMnet DHCP service
vmnat.exe *32	SYSTEM	00	1,992 K	VMware NAT Service
unsecapp.exe	SYSTEM	00	1,748 K	Sink to receive asynchronous callbacks for WMI client application
unsecapp.exe	SYSTEM	00	1,440 K	Sink to receive asynchronous callbacks for WMI client application
UdMapi.exe *32	roton.bruce	00	13,156 K	Skype for Business
TrGUI.exe *32	roton.bruce	00	20,000 K	Skype for Business
TracSrvWrapper.exe *32	SYSTEM	00		
taskmgr.exe	roton.bruce	00		
taskhost.exe	roton.bruce	00		
taskeng.exe	roton.bruce	00		
System Idle Process	SYSTEM	97		
System	SYSTEM	00		
svchost.exe	NETWORK SERVICE	00		
svchost.exe	LOCAL SERVICE	00		
svchost.exe	LOCAL SERVICE	00	2,920 K	Host Process for Windows Services
svchost.exe	LOCAL SERVICE	00	1,632 K	Host Process for Windows Services
svchost.exe	SYSTEM	00	4,852 K	Host Process for Windows Services
svchost.exe	LOCAL SERVICE	00	8,552 K	Host Process for Windows Services
svchost.exe	LOCAL SERVICE	00	3,584 K	Host Process for Windows Services
svchost.exe	NETWORK SERVICE	00	13,268 K	Host Process for Windows Services
svchost.exe	SYSTEM	00	14,608 K	Host Process for Windows Services
svchost.exe	LOCAL SERVICE	00	14,216 K	Host Process for Windows Services

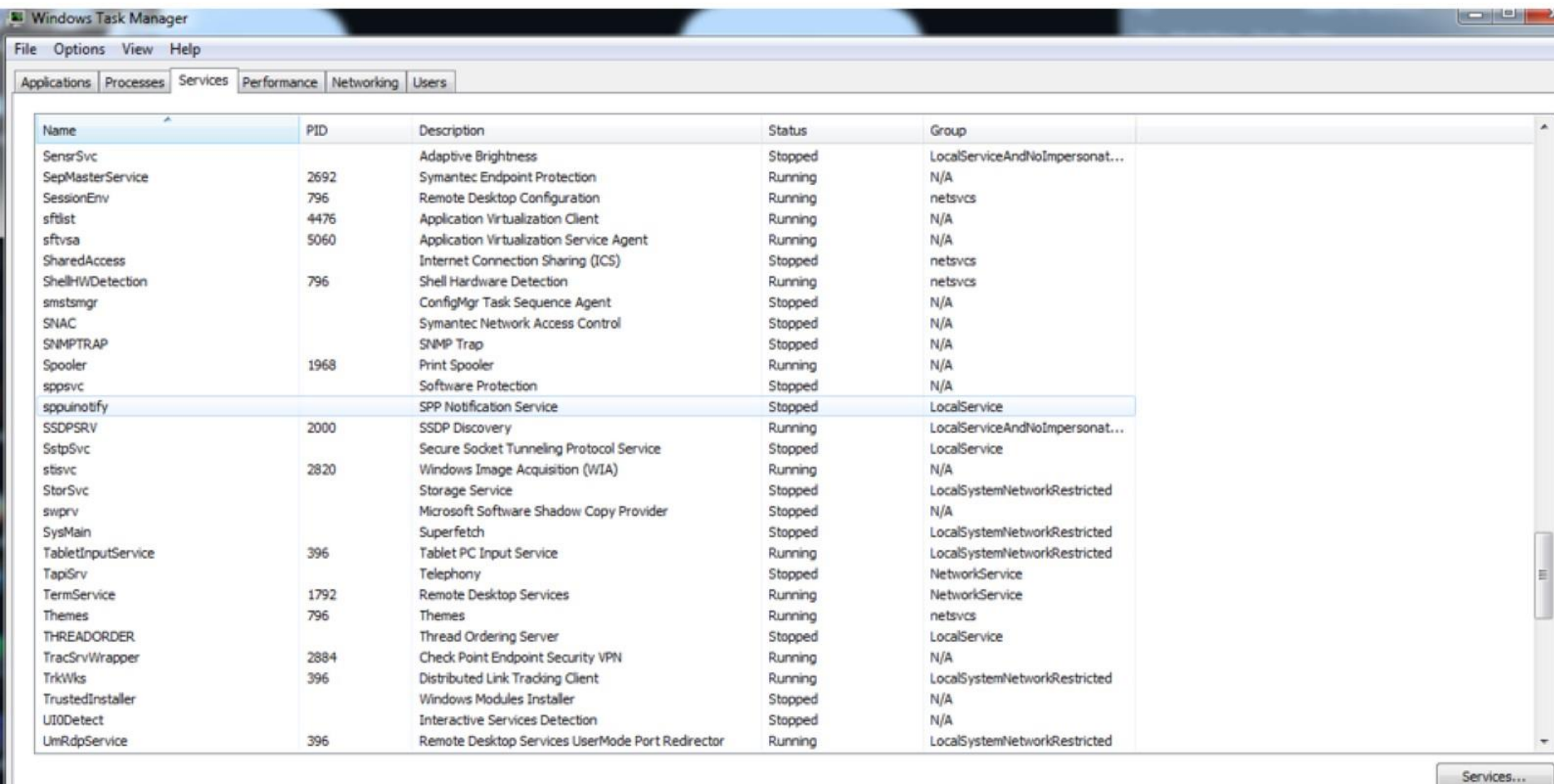
Show processes from all users

Processes: 126 CPU Usage: 3% Physical Memory: 37%

Check Properties of Processes by:

- Click on Properties / Detail
- Click Go to Service(s)
- Create Dump File (if needed)

System Services in Windows Management



The screenshot shows the Windows Task Manager application with the 'Services' tab selected. The Services console displays a list of system services. The columns are Name, PID, Description, Status, and Group. The service 'SPP Notification Service' (sppuotify) is highlighted in blue.

Name	PID	Description	Status	Group
SensrSvc		Adaptive Brightness	Stopped	LocalServiceAndNoImpersonat...
SepMasterService	2692	Symantec Endpoint Protection	Running	N/A
SessionEnv	796	Remote Desktop Configuration	Running	netsvcs
sftlist	4476	Application Virtualization Client	Running	N/A
sftvsa	5060	Application Virtualization Service Agent	Running	N/A
SharedAccess		Internet Connection Sharing (ICS)	Stopped	netsvcs
ShellHWDetection	796	Shell Hardware Detection	Running	netsvcs
smstsmgr		ConfigMgr Task Sequence Agent	Stopped	N/A
SNAC		Symantec Network Access Control	Stopped	N/A
SNMPTRAP		SNMP Trap	Stopped	N/A
Spooler	1968	Print Spooler	Running	N/A
sppsvc		Software Protection	Stopped	N/A
sppuotify		SPP Notification Service	Stopped	LocalService
SSDPSRV	2000	SSDP Discovery	Running	LocalServiceAndNoImpersonat...
SstpSvc		Secure Socket Tunneling Protocol Service	Stopped	LocalService
stisvc	2820	Windows Image Acquisition (WIA)	Running	N/A
StorSvc		Storage Service	Stopped	LocalSystemNetworkRestricted
swprv		Microsoft Software Shadow Copy Provider	Stopped	N/A
SysMain		Superfetch	Stopped	LocalSystemNetworkRestricted
TabletInputService	396	Tablet PC Input Service	Running	LocalSystemNetworkRestricted
TapSrv		Telephony	Stopped	NetworkService
TermService	1792	Remote Desktop Services	Running	NetworkService
Themes	796	Themes	Running	netsvcs
THREADORDER		Thread Ordering Server	Stopped	LocalService
TracSrvWrapper	2884	Check Point Endpoint Security VPN	Running	N/A
TrkWks	396	Distributed Link Tracking Client	Running	LocalSystemNetworkRestricted
TrustedInstaller		Windows Modules Installer	Stopped	N/A
UI0Detect		Interactive Services Detection	Stopped	N/A
UmRdpService	396	Remote Desktop Services UserMode Port Redirector	Running	LocalSystemNetworkRestricted

Now that you have the process to service link, you can record the PID and link to open ports and EXE file.

Making the Link: Process - Service - Listening Port

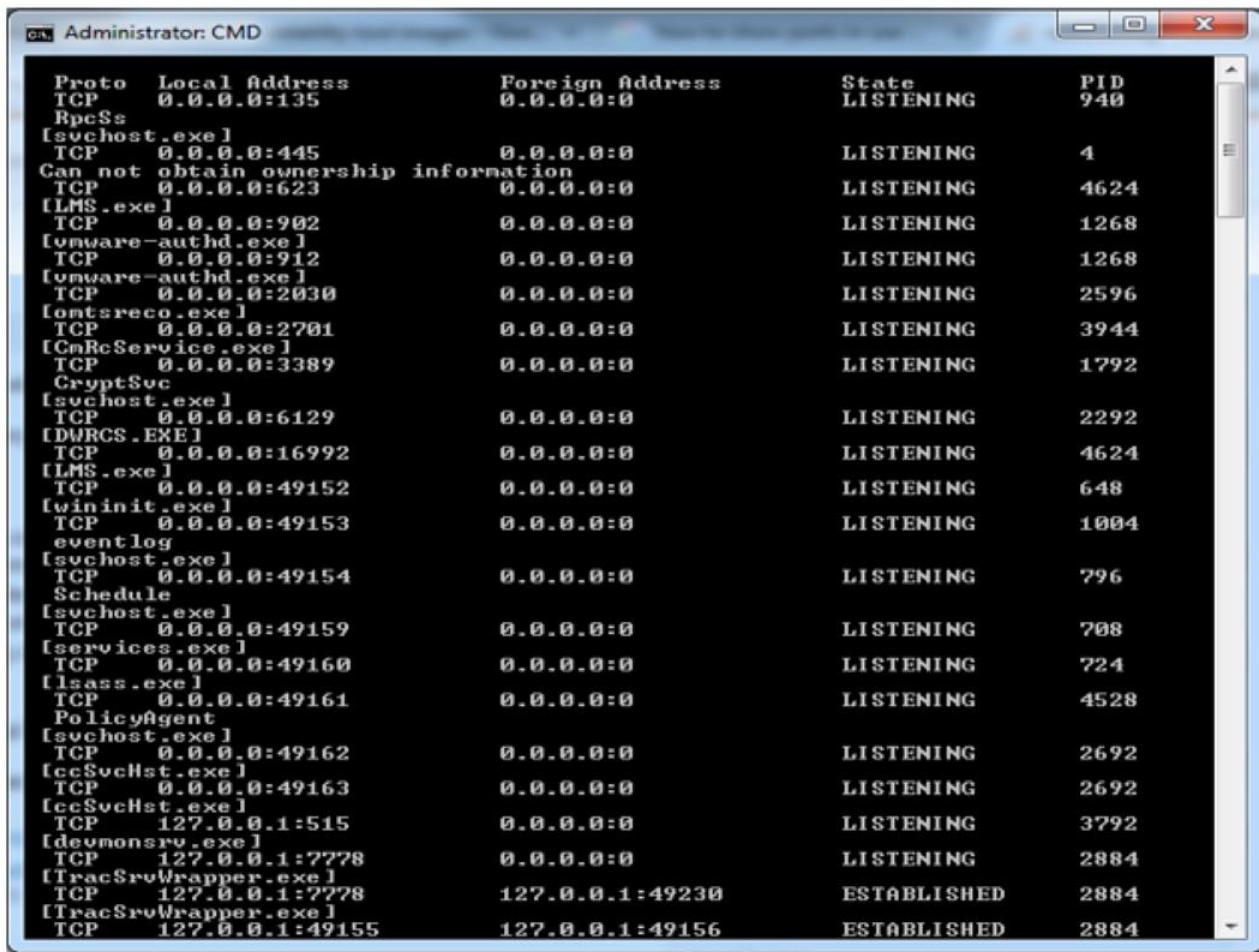
- Execute CMD.EXE as Administrator
- Netstat -anbo

-a Displays all connections and listening ports.

-b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed.

-n Displays addresses and port numbers in numerical form.

-o Displays the owning process ID associated with each connection.



Log Monitoring and Analysis

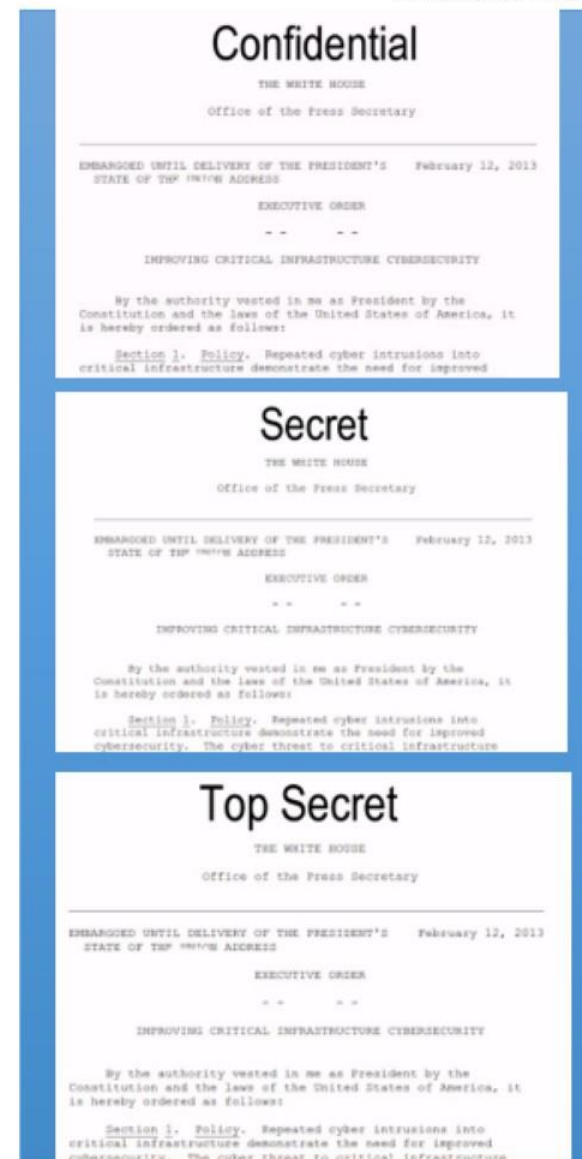
- New users
- Changes in user privileges
- **Processes Privilege changes**
- Service starts and stops
- Software installs
- **Gaps in time**
- Network protocol errors
- Memory errors
- **Abnormal process termination**
- Log statistics (log file versions, sizes, last updated, create date, etc)
- Typos and editing errors (Hacker may manually alter the file)



Steganography Based Compromise Detection



- Targeting with
- Stego traps simplified
 - Step 1: Pick multiple locations of increasing sensitivity within the network
 - Step 2: Use a Stego tool to create invisible digital watermarks at differing levels
 - Step 3: Create custom IPS signatures for the watermarks and watch for them on Egress points
- Note the obvious issues with encrypted channels and pre-transit encryption.
- Tool options: StegoMagic, Steghide, Staanote, Cloak, DataStash, S-tools, Steganos Security Suite, Playmaker, Wbstego, Stegspy, etc



Section 4: Deriving Threat Intelligence from Reduced and Correlated Data Sets

Bruce Roton

CISSP, CISM, CEH, CISA, CGEIT, ISO27001, CSSGB, CCSFP

Sr. Director, Security Solutions Architecture, Level 3 Communications



Threat Intelligence: Critical Information supporting the timely focus of human and technological resources

- Optimal solution should identify or quantify
 - Who is the Threat Actor (IP, Geo, Name, Organization, etc)
 - What is the Intent or Attack Type
 - What systems are potentially compromised
 - What Tools, Techniques, and Processes (TTP) are typically used by this attacker
 - What is the best defense against this adversary

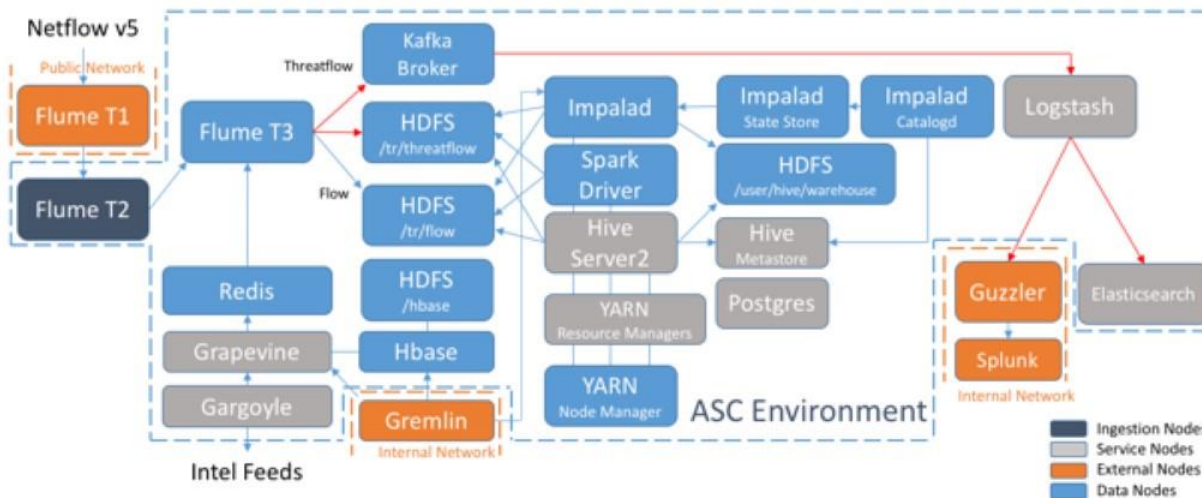
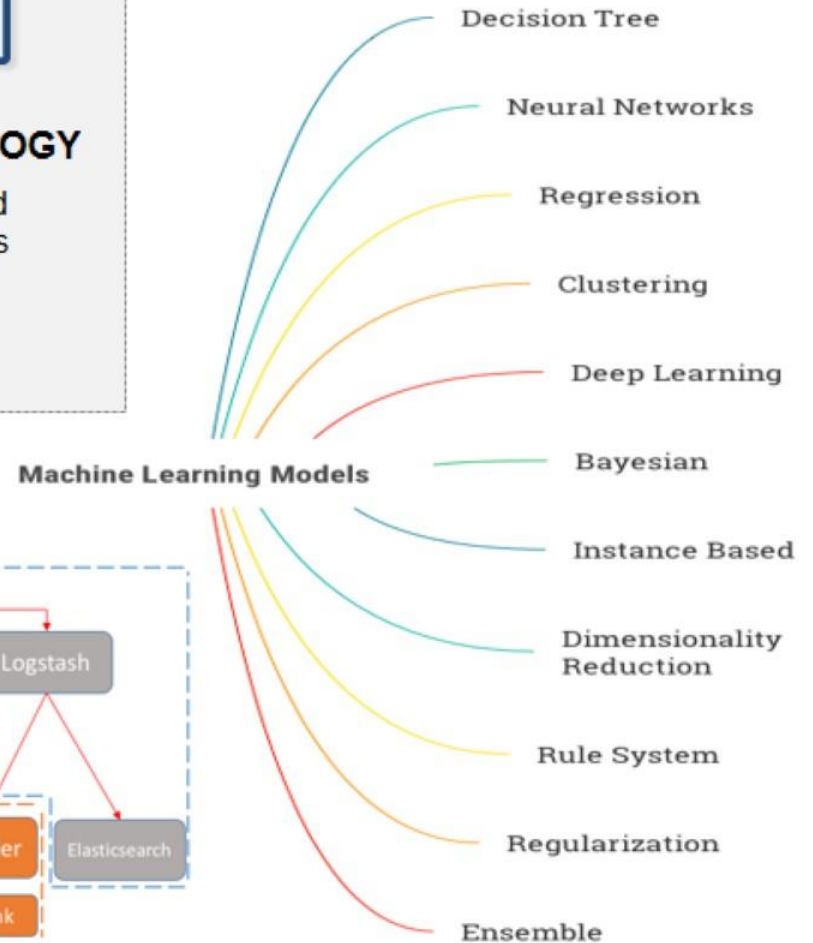
The next Section is a detailed look at a Threat Intelligence Program using Level 3 as an example.

Threat Intelligence Data

- Level 3 analyzes approximately 95B sampled NetFlow records per day from the Internet infrastructure.
- NetFlow data is correlated against the following categories of sources:
 - Public and Private sources
 - Crowdsourced intelligence
 - Researcher Honeypots
 - Personal researchers Intel
 - Commercial and free-to-use lists
 - Level 3 proprietary sources
 - NetFlow Data (95B rec/day)
 - DNS resolution analysis (360M rec/day)
 - Level 3 honeypots
 - Configuration Logs
 - Malware Tracking
 - C2 Tracking (over 5K per day)
 - OSINT research
 - Algorithmic risk views
 - Manual security analysis



Threat Intelligence Infrastructure



Actionable Threat Intelligence

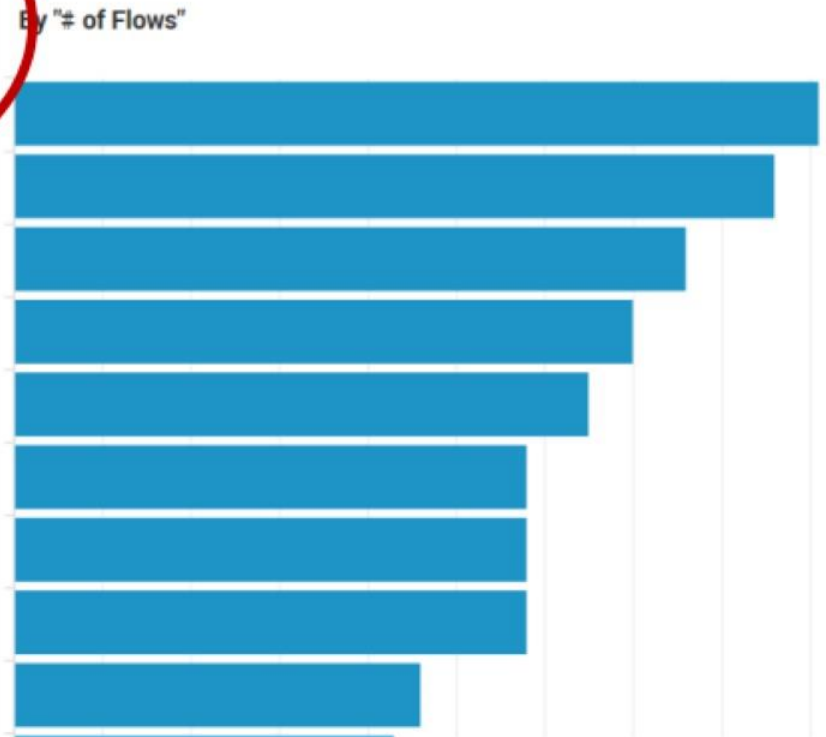
Top 10 Pairs by IPs

Top 10

Sort by # of Flows
Sort by # of Flows
Sort by Volume in MB
Sort by Duration in Hours

Pair	Countries	# of Flows	Volume in MB	Time	Hours
Pair-1	United States - United States	91	0.033	04/15/16 12:00:26:PM	4.17
Pair-2	United States - United States	86	0.040	04/15/16 12:05:00:PM	3.89
Pair-3	United States - United States	76	0.031	04/15/16 12:38:20:PM	3.41
Pair-4	United States - United States	70	0.027	04/15/16 12:07:14:PM	4.07
Pair-5	United States - United States	65	0.027	04/15/16 12:02:43:PM	4.13
Pair-6	United States - United States	58	0.027	04/15/16 12:37:57:PM	3.47
Pair-7	United States - United States	58	0.026	04/15/16 12:00:42:PM	4.17

This is where the story is told!



Section 5: Operationalizing Intruder Hunting

Bruce Roton

CISSP, CISM, CEH, CISA, CGEIT, ISO27001, CSSGB, CCSFP

Sr. Director, Security Solutions Architecture, Level 3 Communications



When Do You Report an Intrusion?

- “When to Report” can be complicated, but it needs to be well scripted and documented.
- Chief Legal Officer (or acting Counsel) is first on the list and part of the process for information dissemination.
- Are you sure there was an intrusion or is it just suspected?
- Has data been compromised or exfiltrated?
- Will further delay help gain intruder intel? At what possible cost?
- Can you report without being forced into action? (**Reporting Trust**)
- Is production being affected?
- Are partners being affected?
- Can you establish a Recovery Point?
- **Sometimes misinformation and incomplete information is worse than no information. Like yelling “fire” in a theater.**

To Whom Do You Report an Intrusion?

AKA: Who you gonna call?



- This can also be complicated, but needs to be well scripted and documented.
- Chief Legal Officer (or acting Counsel) is first on the list and part of the process for information dissemination.
- Are there potential legal, compliance issues, or PR ramifications?
- Do system owners need to take actions? (system rebuild, data restore, account rebuilds/resets)
- Will there be downtime or production impacts during the eviction?
- Are partners affected? Did the intrusion originate from a partner?
- Are user accounts compromised?
 - How critical are they?
 - Can they be reset simultaneously?
- Will law enforcement need to be notified? What about Shareholders?

Establishing “Need to Know” Protocol

- Executives need to know: (This includes Legal)
 - Business Financial Impact (Financial damage and loss)
 - Regulatory Compliance Impact (Do you have a Chief Compliance Officer?)
 - Litigation Impact (Potential for legal action against the organization)
 - Assurance that corrective action has been taken to prevent a similar intrusion
 - They DO NOT need the technical details of the intrusion (**Reporting Trust**)
- System Owners need to know:
 - What systems were impacted, and the nature of any damages you have detected
 - What recovery processes need to be followed to restore normal operations
 - Corrective actions they need to apply to prevent a similar incident in the future
- Network, Security, and Infrastructure
 - Corrective actions they need to apply to prevent a similar incident in the future
 - New processes and procedures
- End Users (as little as possible)

Knowing When to “Raise the Black”

Raise it too soon and they might run. Raise it too late and they might panic and start shooting. Men will be lost and you may be forced to sink the prize.



Consider the below (In this order).

1. What is the current state of the damage or loss?
2. Do you know the depth and breadth of the intrusion?
- 3. Has the intruder set traps or landmines for you to trigger during eviction?**
4. Do you understand how they got in?
5. Are you confident that you can expel them completely and block re-entry?
6. Do you understand the intruder's target, value proposition, and game-plan?
- 7. Is there value in monitoring?** Can you learn about the intruder's TTPs (Tools, Techniques and Processes). Is that information likely to be helpful in future attacks, or in identifying potential targets?

The Eviction Process

- First, Eviction needs to be a well documented standardized process.
- Second, don't make this "Killing James Bond". Take the Scott Evil approach.
- Document all known inhabited systems
- Identify any Persistence Methods used by the Intruder (RATs or Backdoors for re-entry).
- Identify original method of intrusion and point of entry if possible.
- Identify signaling to intruder and consider false signaling during eviction process
- Develop plan for malware removal
 - Are system rebuilds necessary?
 - Will reboots or downtime be required?
 - Test plan for post-eviction system cleanliness monitoring. (Configuration and Behavioral)
 - Ideally, quarantine system with controlled communications for the first 72 hours. Suggestion: Use a "portable Firewall" with customer ruleset inline on the system's physical network connection. Turn up only those comms required, and log everything.

If You are Thinking of Counter Attack, Remember:

You are NOT Batman



- Batman isn't running a business.
- Batman has a secret identity.
- Batman doesn't have a public facing Internet presence.
- Batman has billions of \$s and nearly infinite informational resources.
- Batman has a high ranking local law enforcement friend who will violate the law to protect Batman.
- Batman isn't afraid of being fined or doing prison time.
- Batman actually WANTS to start a war with organized criminals.
- **BATMAN ISN'T REAL!!!**

NONE of the above applies to YOU!

- If you are thinking retaliatory strike... Let's talk about your LEGAL options (Takedown requests, Malware uploads, Logic Bombs, destructive payloads, counter hacking, etc)