ResponderCon

SEPTEMBER 13, 2022

Successful DFIR From Preparation and Monitoring

INVESTIGATING THE ANATOMY OF A RANSOMWARE ATTACK

Dennis M. Allen

Director - Security Programs - Strategy & Risk

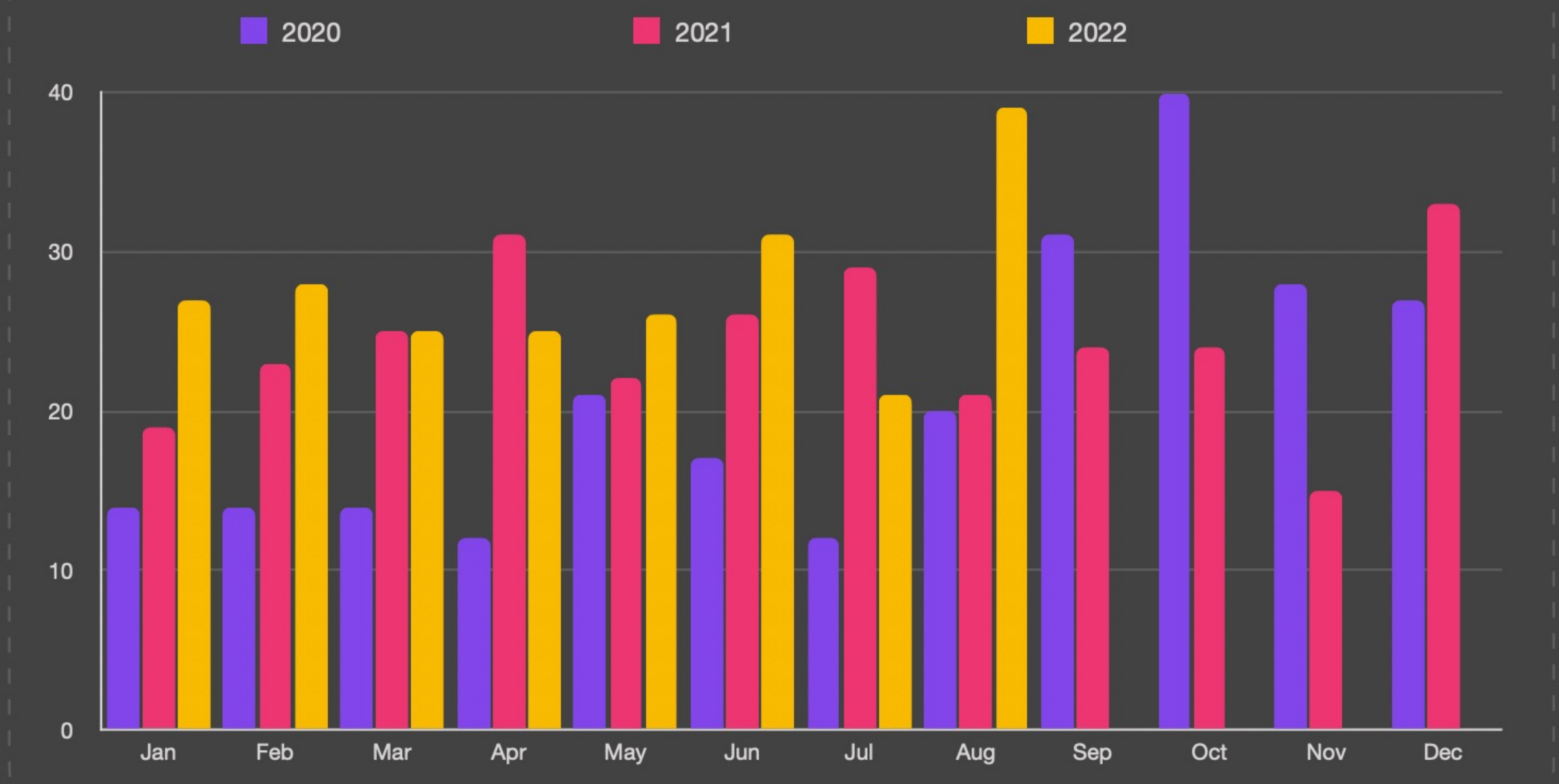
stratascale

An SHI Company

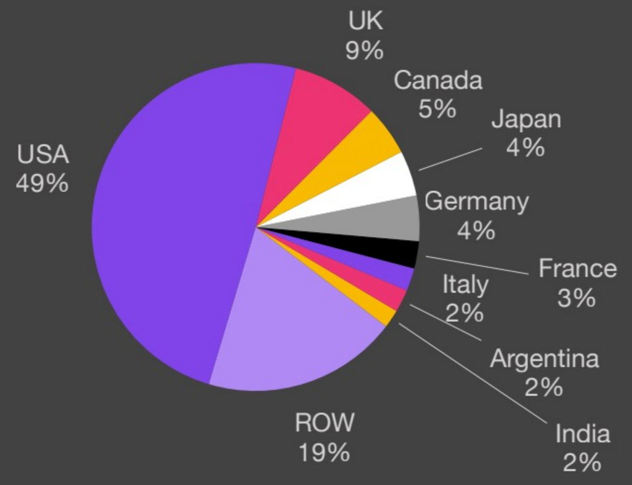
Agenda

- Ransomware landscape
- Ransomware preparation
- Scenario walk-through
- Wrap-up

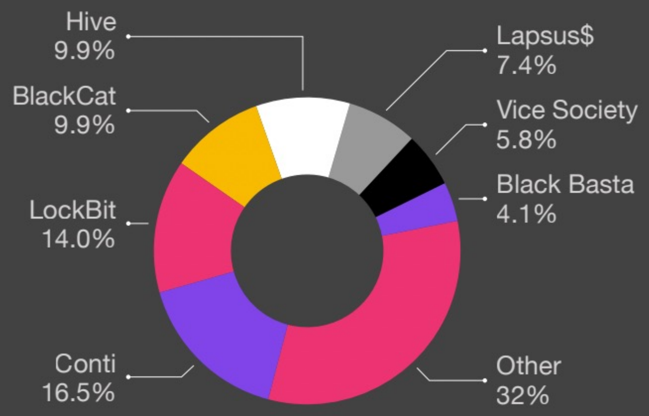
Ransomware Trend by Month



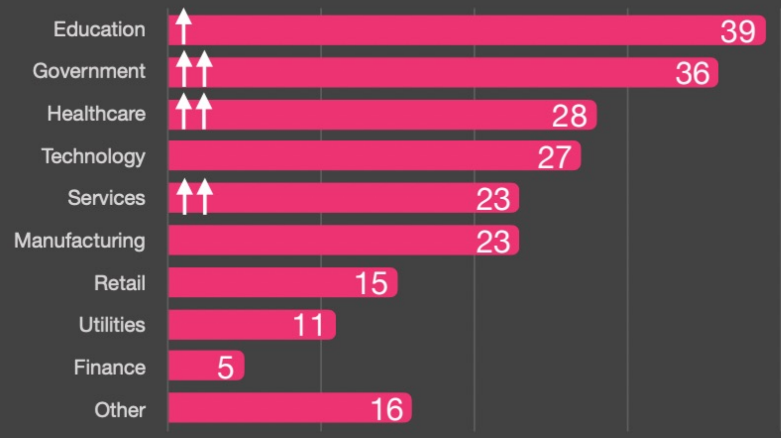
Ransomware by Country



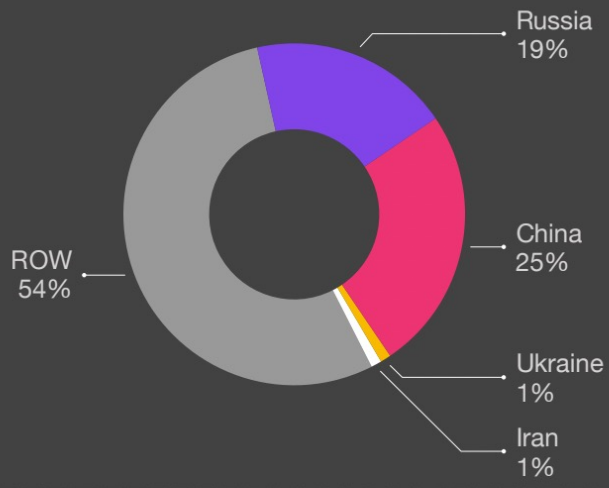
Ransomware by Variant



Ransomware by Industry



Ransomware Exfiltration Country



Key Trends

80% of all attacks use PowerShell

87% of attacks exfiltrate data

Average payout US $228,125k

+8% from Q1/22

Best Practices

- Prepare

  (Risk Strategy, Data Strategy, IR Plan, Insurance policies)

- Instrument

  (Technical and non-technical controls)

- Practice

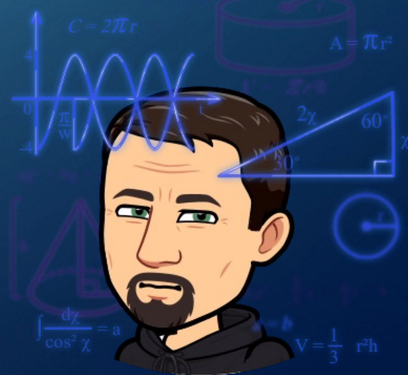
  (Validate RTO/RPO, TTX, Attack simulations)

- Improve

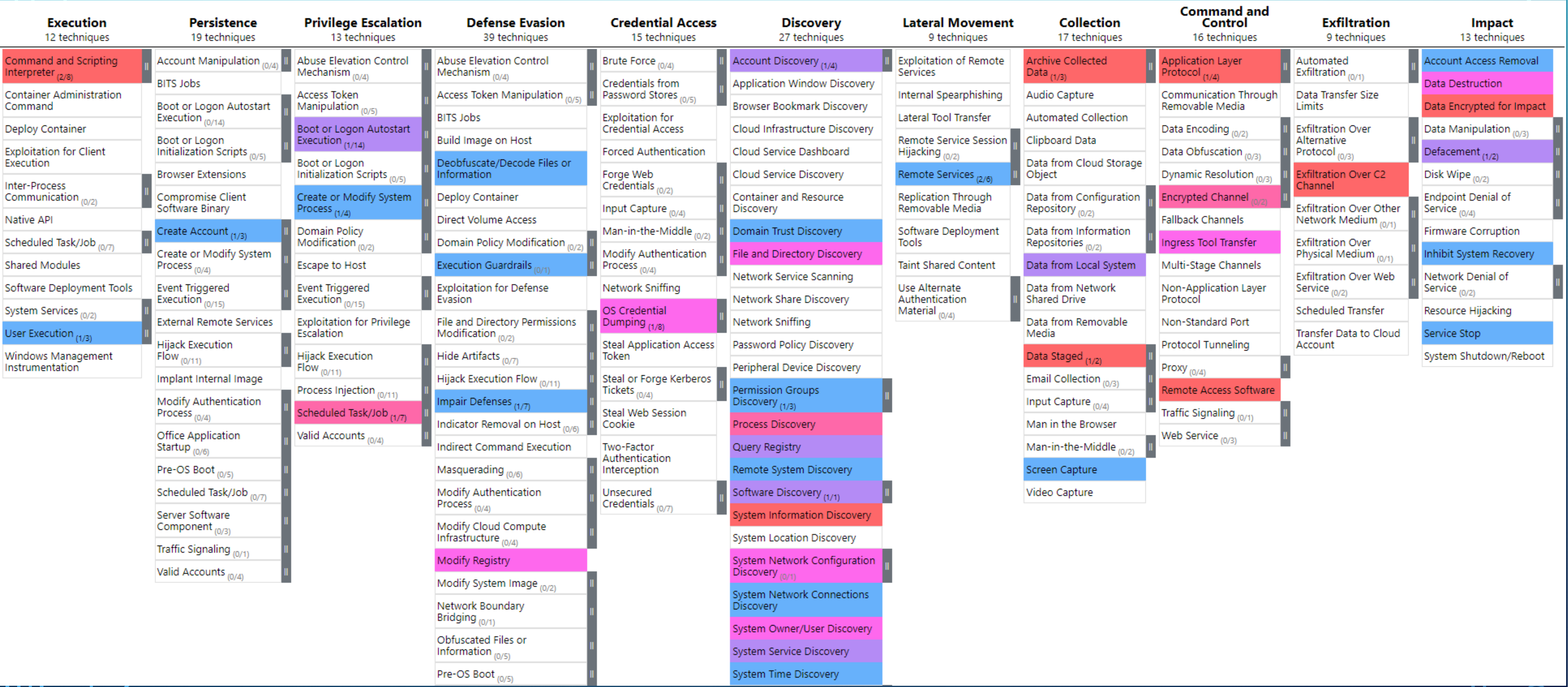
  (Playbooks, Policies, and other Procedures)

Ransomware IR Playbook

1. Identify
   - Most critical systems and data
   - Define Policies, and Procedures
2. Prepare
   - Security Awareness Training
   - Patch management
   - Verify Backups
   - Technical controls like network segmentation, MFA, etc.
3. Respond
   - Incident declaration/activation
   - Restore, rebuild, etc.
   - Pay?
4. Recover
   - Clean/Reset Passwords
   - Crisis communications



Ransomware TTP Mapping



Execution
12 techniques

- Command and Scripting Interpreter (2/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/7)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (1/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Internal Image
- Modify Authentication Process (0/4)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/7)
- Server Software Component (0/3)
- Traffic Signaling (0/1)
- Valid Accounts (0/4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (1/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (1/7)
- Valid Accounts (0/4)

Defense Evasion
39 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (1/7)
- Indicator Removal on Host (0/6)
- Indirect Command Execution
- Masquerading (0/6)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (0/5)
- Pre-OS Boot (0/5)

Credential Access
15 techniques

- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (1/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/7)

Discovery
27 techniques

- Account Discovery (1/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (1/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1/1)
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery (0/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (2/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Archive Collected Data (1/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (1/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

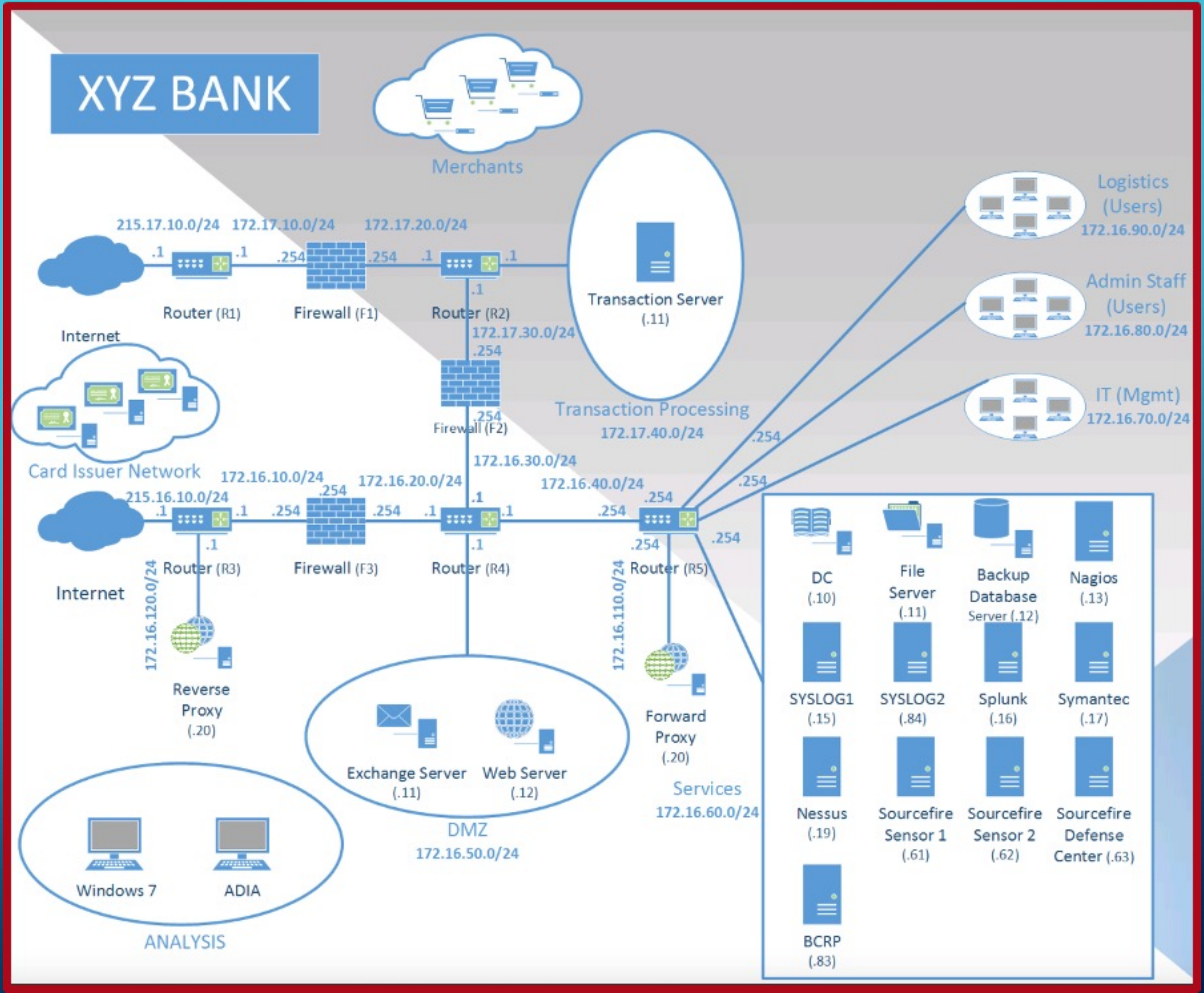
Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (1/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Image source: https://github.com/scythe-io/community-threats/blob/master/Ransomware_Top_TTPs/Ransomware_Top_TTPs_navigator.png

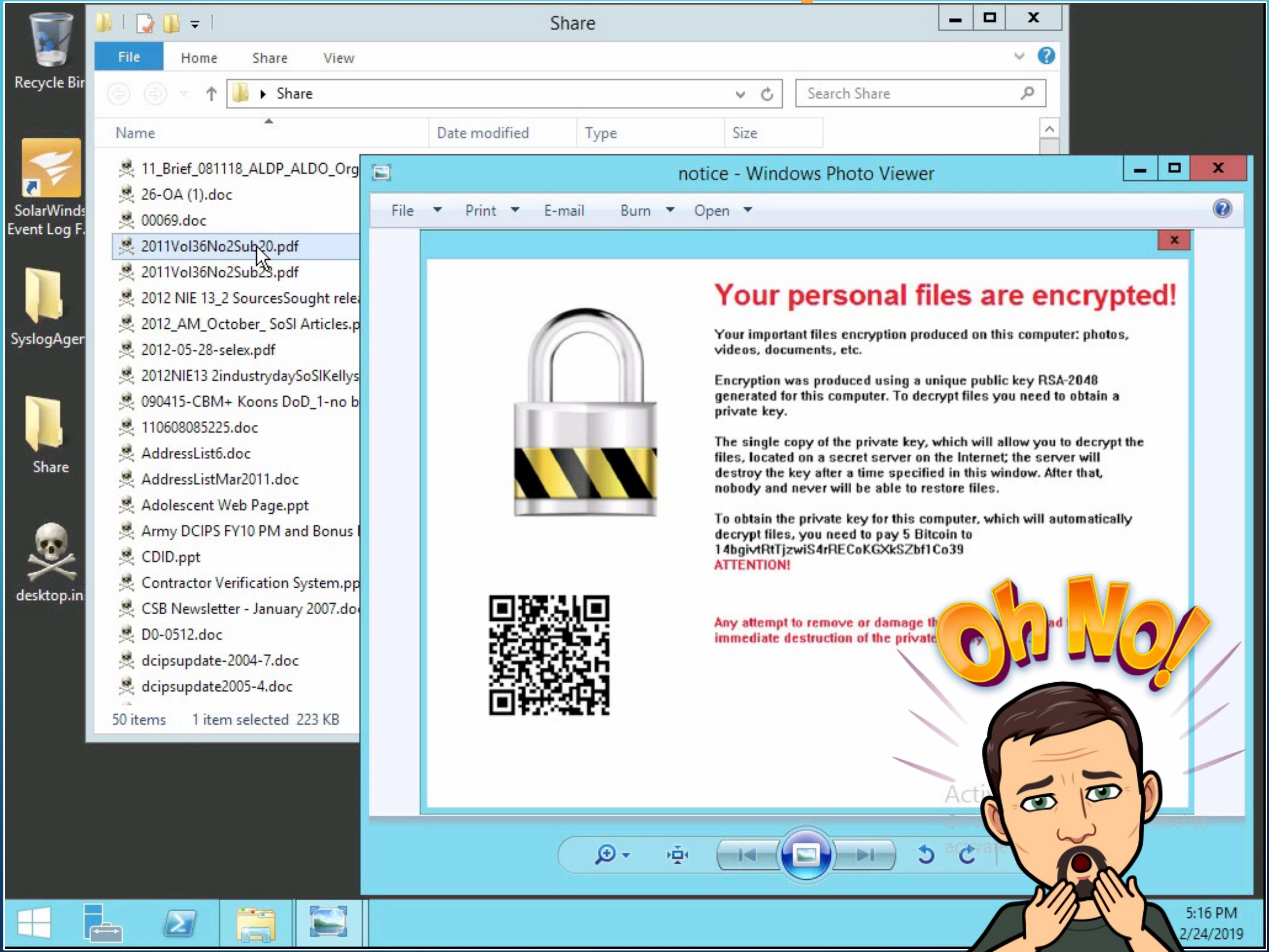


XYZ BANK
Merchants
Internet
215.17.10.0/24
172.17.10.0/24
172.17.20.0/24
.1
.1
.254
.254
.1
.1
Router (R1)
Firewall (F1)
Router (R2)
Transaction Server
(.11)
Transaction Processing
172.17.40.0/24
.1
172.17.30.0/24
.254
Firewall (F2)
.254
Internet
Card Issuer Network
Logistics
(Users)
172.16.90.0/24
Admin Staff
(Users)
172.16.80.0/24
IT (Mgmt)
172.16.70.0/24
.254
.254
.254
.254
172.16.30.0/24
172.16.40.0/24
172.16.10.0/24
172.16.20.0/24
215.16.10.0/24
.1
.1
.254
.254
.254
.1
.1
.1
.254
.254
Internet
Router (R3)
Firewall (F3)
Router (R4)
Router (R5)
.1
.1
172.16.120.0/24
Reverse
Proxy
(.20)
172.16.110.0/24
Forward
Proxy
(.20)
Services
172.16.60.0/24
Exchange Server
(.11)
Web Server
(.12)
DMZ
172.16.50.0/24
Windows 7
ADIA
ANALYSIS
DC
(.10)
File
Server
(.11)
Backup
Database
Server (.12)
Nagios
(.13)
SYSLOG1
(.15)
SYSLOG2
(.84)
Splunk
(.16)
Symantec
(.17)
Nessus
(.19)
Sourcefire
Sensor 1
(.61)
Sourcefire
Sensor 2
(.62)
Sourcefire
Defense
Center (.63)
BCRP
(.83)

Detection & Analysis

- User calls the help desk, believes they “accidentally” clicked on a phishing link sent from SANS

Detection & Analysis



11_Brief_081118_ALDP_ALDO_Org
26-OA (1).doc
00069.doc
2011Vol36No2Sub20.pdf
2011Vol36No2Sub23.pdf
2012 NIE 13_2 SourcesSought rele
2012_AM_October_ SoSI Articles.p
2012-05-28-selex.pdf
2012NIE13 2industrydaySoSIKellys
090415-CBM+ Koons DoD_1-no b
110608085225.doc
AddressList6.doc
AddressListMar2011.doc
Adolescent Web Page.ppt
Army DCIPS FY10 PM and Bonus
CDID.ppt
Contractor Verification System.pp
CSB Newsletter - January 2007.do
D0-0512.doc
dcipsupdate-2004-7.doc
dcipsupdate2005-4.doc

50 items 1 item selected 223 KB

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain a private key.

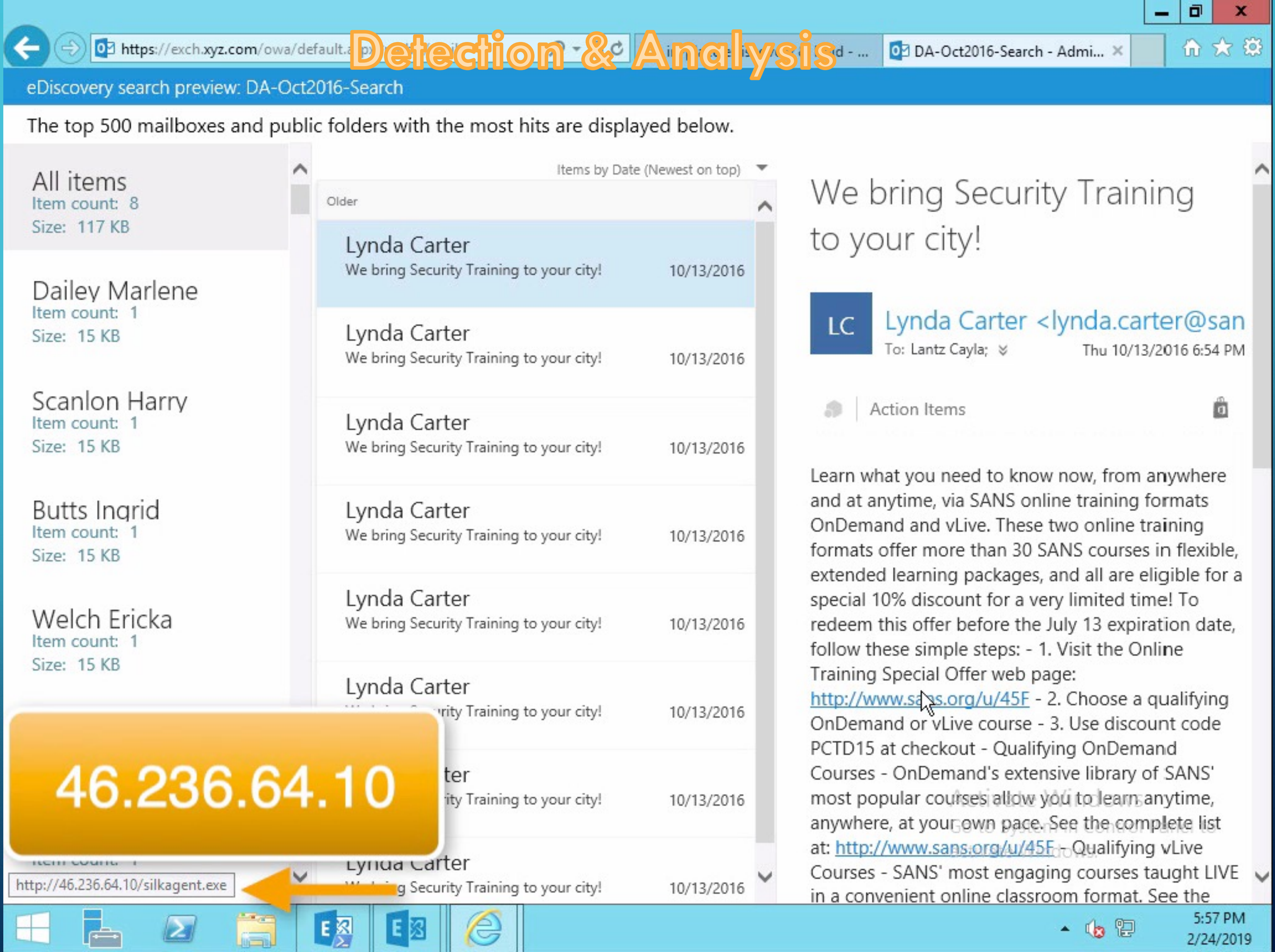
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 5 Bitcoin to
14bgivtRtTjzwiS4rRECoKGXkSZbf1Co39
ATTENTION!

Any attempt to remove or damage th ad
immediate destruction of the private

"It's not the plane,
It's the pilot."
-Maverick-

Detection & Analysis



https://exch.xyz.com/owa/default.aspx

DA-Oct2016-Search - Admi...

eDiscovery search preview: DA-Oct2016-Search

The top 500 mailboxes and public folders with the most hits are displayed below.

All items
Item count: 8
Size: 117 KB

Dailey Marlene
Item count: 1
Size: 15 KB

Scanlon Harry
Item count: 1
Size: 15 KB

Butts Ingrid
Item count: 1
Size: 15 KB

Welch Ericka
Item count: 1
Size: 15 KB

Item count: 1

Items by Date (Newest on top)

Older

Lynda Carter We bring Security Training to your city!	10/13/2016
Lynda Carter We bring Security Training to your city!	10/13/2016
Lynda Carter We bring Security Training to your city!	10/13/2016
Lynda Carter We bring Security Training to your city!	10/13/2016
Lynda Carter We bring Security Training to your city!	10/13/2016
Lynda Carter ...rity Training to your city!	10/13/2016
...ter ...ity Training to your city!	10/13/2016
Lynda Carter ...g Security Training to your city!	10/13/2016

We bring Security Training to your city!

LC Lynda Carter <lynda.carter@san
To: Lantz Cayla;
Thu 10/13/2016 6:54 PM

Action Items

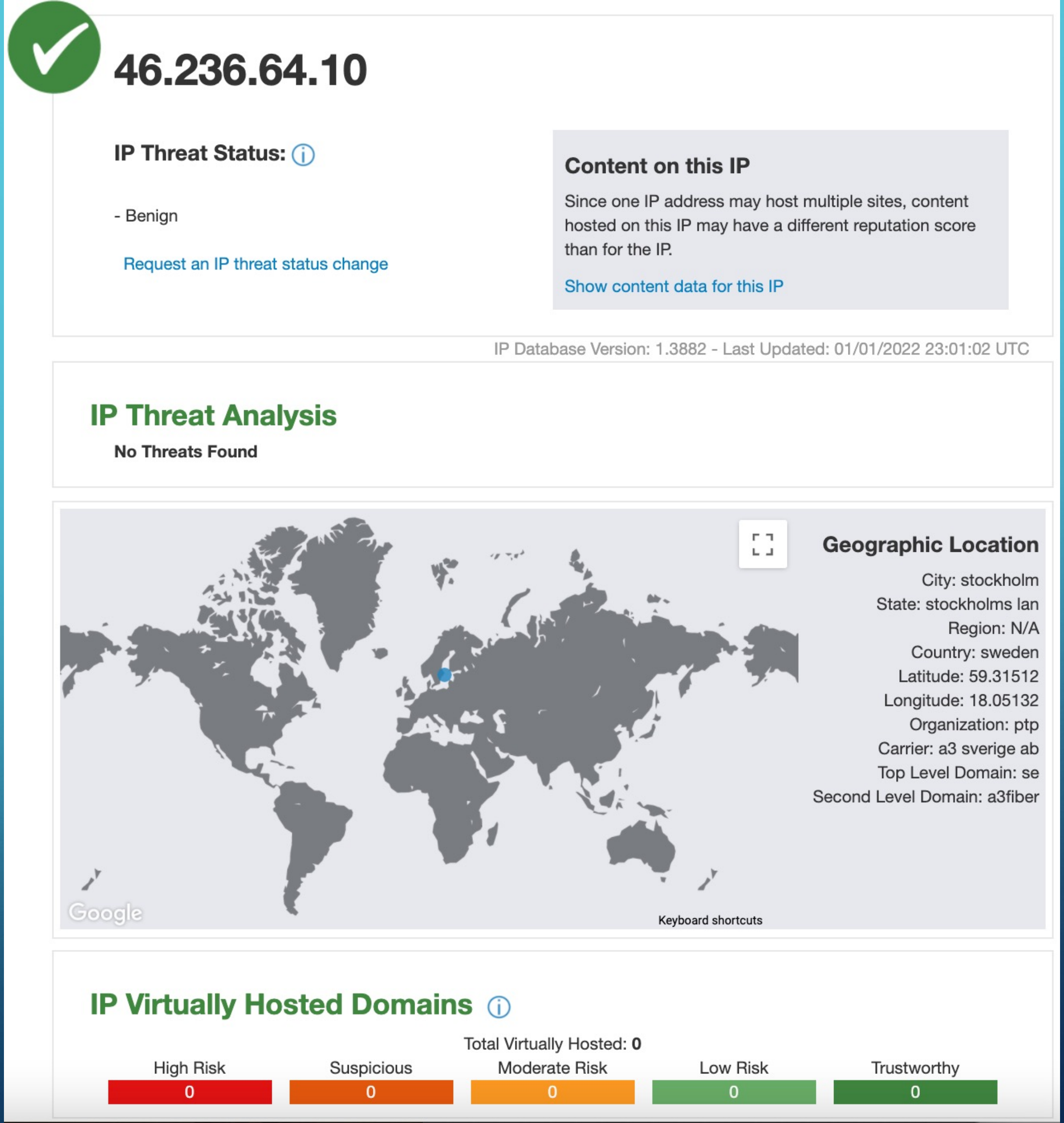
Learn what you need to know now, from anywhere and at anytime, via SANS online training formats OnDemand and vLive. These two online training formats offer more than 30 SANS courses in flexible, extended learning packages, and all are eligible for a special 10% discount for a very limited time! To redeem this offer before the July 13 expiration date, follow these simple steps: - 1. Visit the Online Training Special Offer web page: http://www.sans.org/u/45F - 2. Choose a qualifying OnDemand or vLive course - 3. Use discount code PCTD15 at checkout - Qualifying OnDemand Courses - OnDemand's extensive library of SANS' most popular courses allow you to learn anytime, anywhere, at your own pace. See the complete list at: http://www.sans.org/u/45F - Qualifying vLive Courses - SANS' most engaging courses taught LIVE in a convenient online classroom format. See the

http://46.236.64.10/silkagent.exe

46.236.64.10

5:57 PM
2/24/2019

Detection & Analysis



46.236.64.10

IP Threat Status: ⓘ

- Benign

Request an IP threat status change

Content on this IP

Since one IP address may host multiple sites, content hosted on this IP may have a different reputation score than for the IP.

Show content data for this IP

IP Database Version: 1.3882 - Last Updated: 01/01/2022 23:01:02 UTC

IP Threat Analysis

No Threats Found

Geographic Location

City: stockholm
State: stockholms lan
Region: N/A
Country: sweden
Latitude: 59.31512
Longitude: 18.05132
Organization: ptp
Carrier: a3 sverige ab
Top Level Domain: se
Second Level Domain: a3fiber

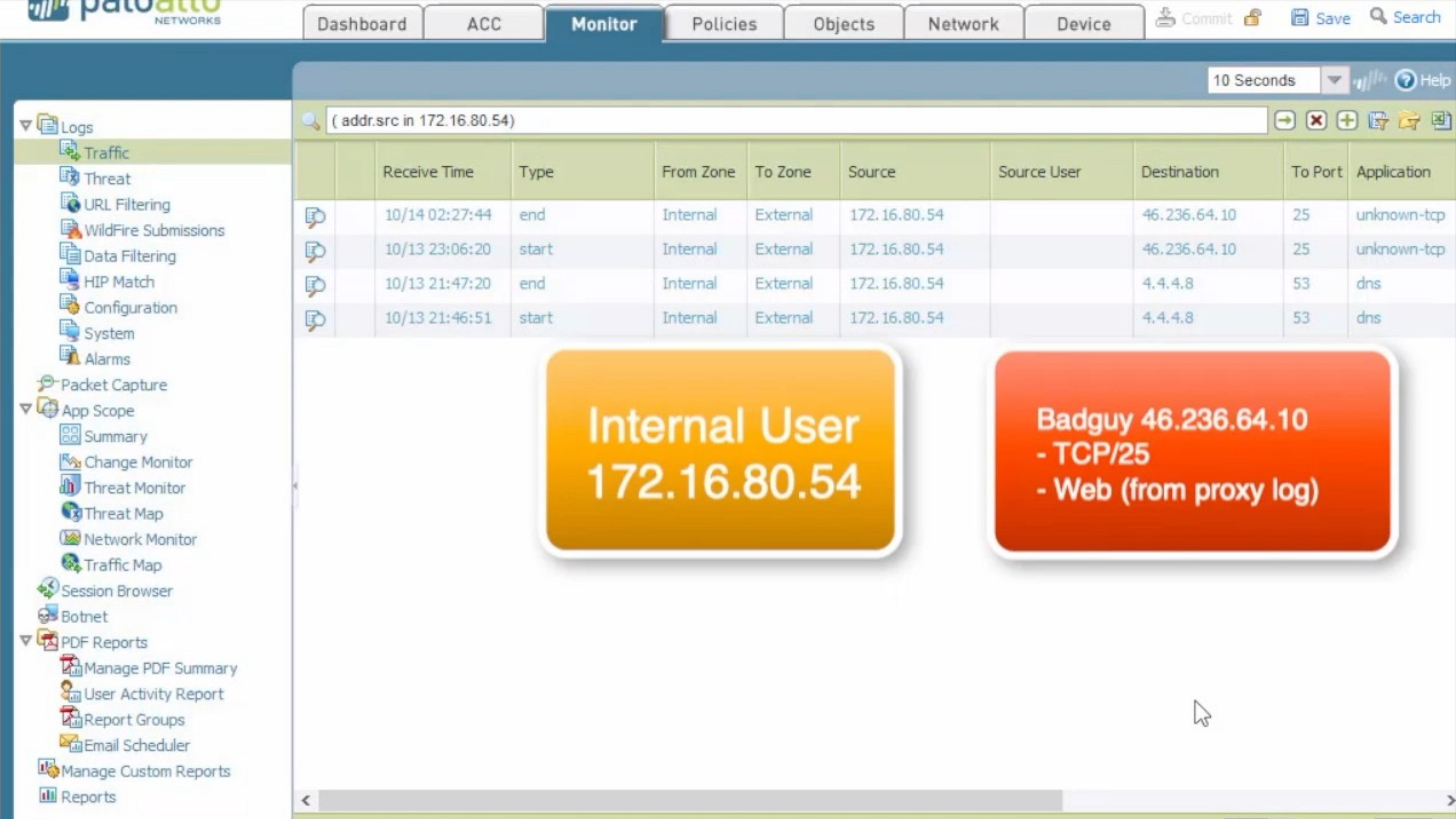
IP Virtually Hosted Domains ⓘ

Total Virtually Hosted: **0**

High Risk	Suspicious	Moderate Risk	Low Risk	Trustworthy
0	0	0	0	0

Detection & Analysis – What we know so far

- Phishing email sent from lynda.carter@sans.edu (not .org)
- Phishing email with a malicious link to 46.236.64.10 instead of the sans.org link
- 8 Users received the email
- 1 User (172.16.80.54) visited the link in the phishing email
- 172.16.80.54 is also connecting to 46.236.64.10 on TCP Port 25
- Finland IP is not a “known bad” address



(addr.src in 172.16.80.54)

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
10/14 02:27:44	end	Internal	External	172.16.80.54		46.236.64.10	25	unknown-tcp
10/13 23:06:20	start	Internal	External	172.16.80.54		46.236.64.10	25	unknown-tcp
10/13 21:47:20	end	Internal	External	172.16.80.54		4.4.4.8	53	dns
10/13 21:46:51	start	Internal	External	172.16.80.54		4.4.4.8	53	dns

Internal User
172.16.80.54

Badguy 46.236.64.10
- TCP/25
- Web (from proxy log)

Question Time

What is ***<u>your</u>*** biggest concern?

Detection & Analysis – What we know so far

- Phishing email sent from lynda.carter@sans.edu (not .org)
- Phishing email with a malicious link to 46.236.64.10 instead of the sans.org link
- 8 Users received the email
- 1 User (172.16.80.54) visited the link in the phishing email
- 172.16.80.54 is also connecting to 46.236.64.10 on TCP Port 25
- Finland IP is not a ”known bad” address

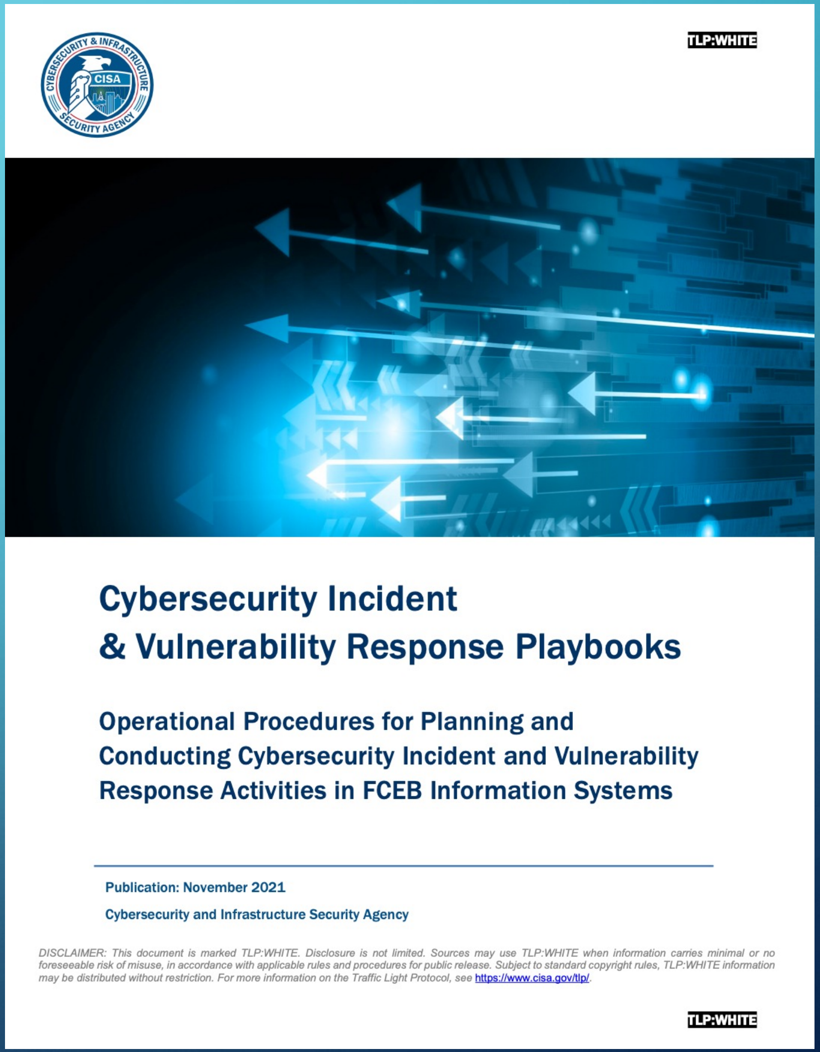
- Two other internal hosts are connected to the Badguy IP: 172.16.60.11 & 172.16.110.20
- 172.16.60.11 is a critical Transaction Server
- When accessing the Transaction Server, it automatically reboots
- Network Monitoring tools demonstrate that the Transaction Server is offline

Detection & Analysis

- Have we identified the root cause?
- Have we identified the full extent of the incident?
- What internal departments or groups should get involved?
- What other analysis should be done?
- What 3rd Parties need to be contacted?

Incident Response Plan

- Let’s take a look…



TLP:WHITE

Cybersecurity Incident & Vulnerability Response Playbooks

Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems

Publication: November 2021

Cybersecurity and Infrastructure Security Agency

DISCLAIMER: This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/.

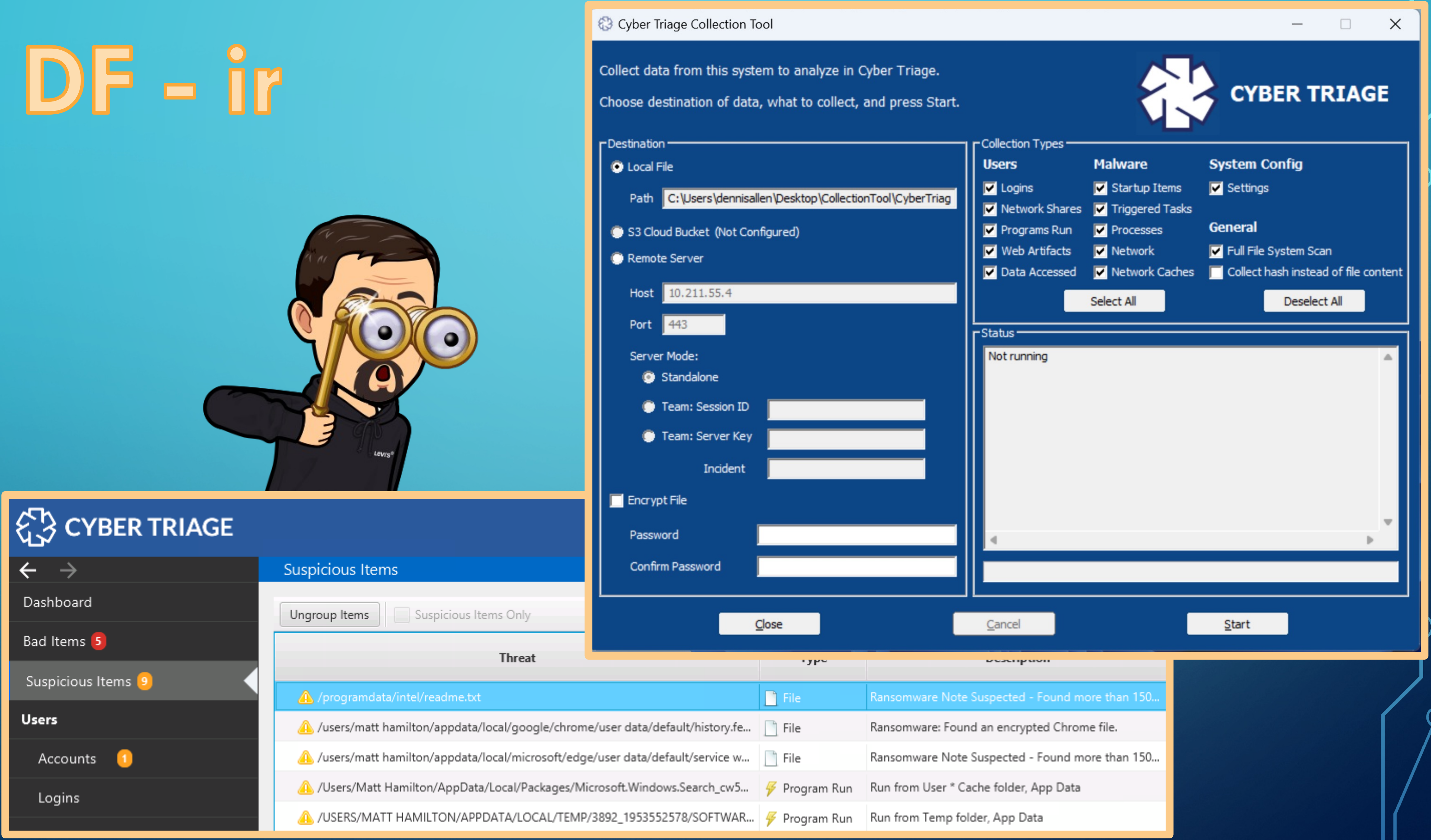
TLP:WHITE

https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen

Question Time

- What activities need to be prioritized?
- **WHAT BUSINESS PROCESS IS IMPACTED THE MOST?**
- How much is 5 Bitcoin? Does that impact your decision?
- What tools are available to aid next steps?
- What 3rd Parties need to be engaged (if any)?

DF - ir



Cyber Triage Collection Tool

Collect data from this system to analyze in Cyber Triage.

Choose destination of data, what to collect, and press Start.

Destination

● Local File

Path: C:\Users\dennisallen\Desktop\CollectionTool\CyberTriag

○ S3 Cloud Bucket (Not Configured)

○ Remote Server

Host: 10.211.55.4

Port: 443

Server Mode:

● Standalone

○ Team: Session ID

○ Team: Server Key

Incident

□ Encrypt File

Password

Confirm Password

Collection Types

Users
- ☑ Logins
- ☑ Network Shares
- ☑ Programs Run
- ☑ Web Artifacts
- ☑ Data Accessed

Malware
- ☑ Startup Items
- ☑ Triggered Tasks
- ☑ Processes
- ☑ Network
- ☑ Network Caches

System Config
- ☑ Settings

General
- ☑ Full File System Scan
- □ Collect hash instead of file content

Status

Not running

Threat	Type	Description
/programdata/intel/readme.txt	File	Ransomware Note Suspected - Found more than 150...
/users/matt hamilton/appdata/local/google/chrome/user data/default/history.fe...	File	Ransomware: Found an encrypted Chrome file.
/users/matt hamilton/appdata/local/microsoft/edge/user data/default/service w...	File	Ransomware Note Suspected - Found more than 150...
/Users/Matt Hamilton/AppData/Local/Packages/Microsoft.Windows.Search_cw5...	Program Run	Run from User * Cache folder, App Data
/USERS/MATT HAMILTON/APPDATA/LOCAL/TEMP/3892_1953552578/SOFTWAR...	Program Run	Run from Temp folder, App Data

Image source: https://www.cybertriage.com/features/ransomware/

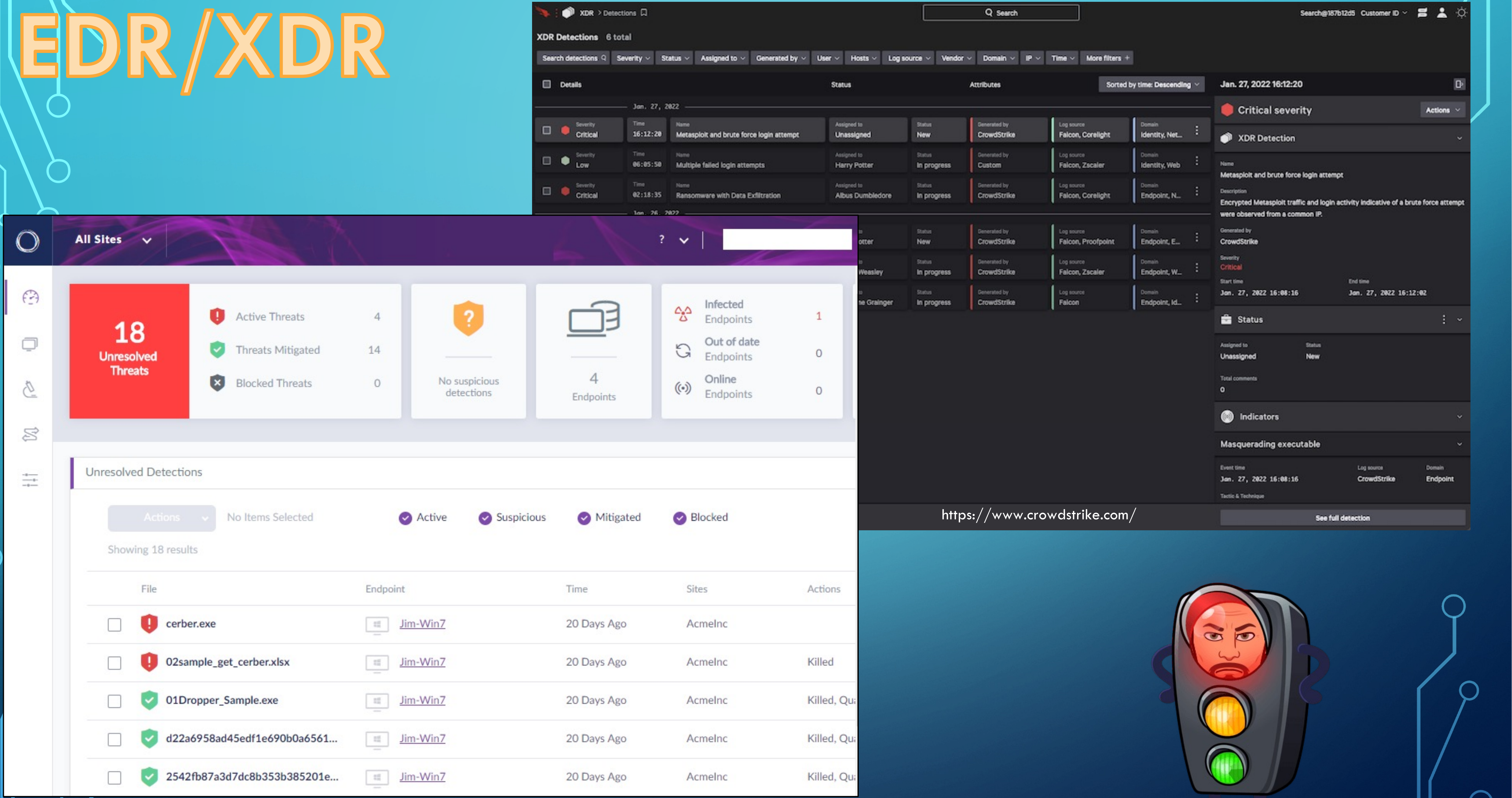
Other Windows IOCs

- Domain Admins being changed
- Local Admins being changed
- Local Users created or deleted
- New Services or Applications
- Suspicious RDP Logins

- New Services or Applications
- Password resets
- Changes to scheduled tasks
- Security Event Logs being cleared
- Unknown PowerShell script execution

https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance

EDR/XDR



XDR > Detections

Search

Search@187b12d5 Customer ID

XDR Detections 6 total

Search detections | Severity | Status | Assigned to | Generated by | User | Hosts | Log source | Vendor | Domain | IP | Time | More filters +

Details | Status | Attributes | Sorted by time: Descending

Jan. 27, 2022

Severity	Time	Name	Assigned to	Status	Generated by	Log source	Domain
Critical	16:12:20	Metasploit and brute force login attempt	Unassigned	New	CrowdStrike	Falcon, Corelight	Identity, Net...
Low	06:05:50	Multiple failed login attempts	Harry Potter	In progress	Custom	Falcon, Zscaler	Identity, Web
Critical	02:18:35	Ransomware with Data Exfiltration	Albus Dumbledore	In progress	CrowdStrike	Falcon, Corelight	Endpoint, N...

Jan. 26, 2022

Severity	Time	Name	Assigned to	Status	Generated by	Log source	Domain
			otter	New	CrowdStrike	Falcon, Proofpoint	Endpoint, E...
			Weasley	In progress	CrowdStrike	Falcon, Zscaler	Endpoint, W...
			e Grainger	In progress	CrowdStrike	Falcon	Endpoint, Id...

Jan. 27, 2022 16:12:20

Critical severity — Actions

XDR Detection

Name
Metasploit and brute force login attempt

Description
Encrypted Metasploit traffic and login activity indicative of a brute force attempt were observed from a common IP.

Generated by
CrowdStrike

Severity
Critical

Start time: Jan. 27, 2022 16:08:16
End time: Jan. 27, 2022 16:12:02

Status

Assigned to: Unassigned
Status: New

Total comments
0

Indicators

Masquerading executable

Event time: Jan. 27, 2022 16:08:16
Log source: CrowdStrike
Domain: Endpoint

Tactic & Technique

See full detection

https://www.crowdstrike.com/

All Sites

18 Unresolved Threats

Active Threats	4
Threats Mitigated	14
Blocked Threats	0

No suspicious detections

4 Endpoints

Infected Endpoints	1
Out of date Endpoints	0
Online Endpoints	0

Unresolved Detections

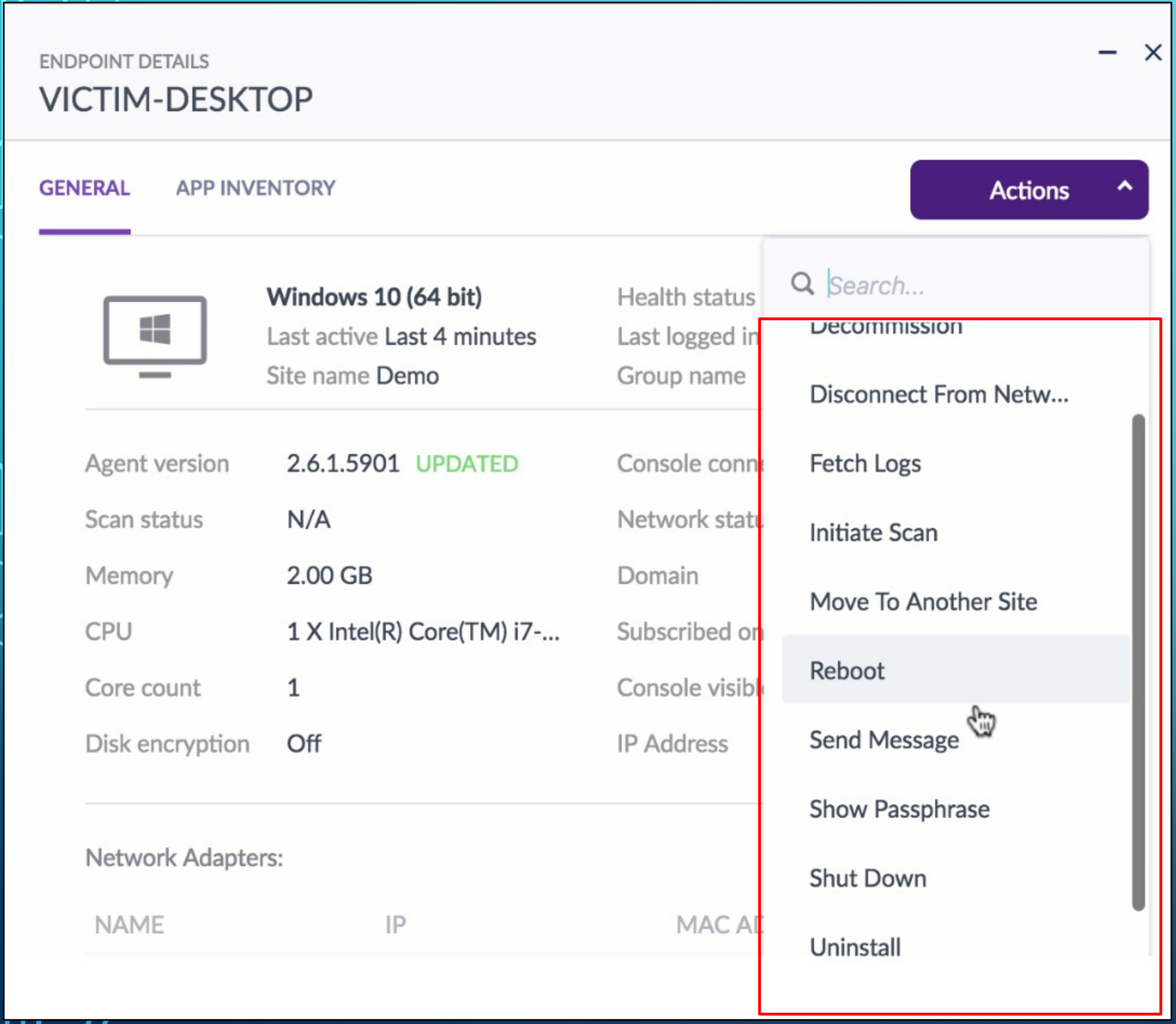
Actions | No Items Selected | ✓ Active | ✓ Suspicious | ✓ Mitigated | ✓ Blocked

Showing 18 results

	File	Endpoint	Time	Sites	Actions
□	cerber.exe	Jim-Win7	20 Days Ago	AcmeInc	
□	02sample_get_cerber.xlsx	Jim-Win7	20 Days Ago	AcmeInc	Killed
□	01Dropper_Sample.exe	Jim-Win7	20 Days Ago	AcmeInc	Killed, Qu
□	d22a6958ad45edf1e690b0a6561...	Jim-Win7	20 Days Ago	AcmeInc	Killed, Qu
□	2542fb87a3d7dc8b353b385201e...	Jim-Win7	20 Days Ago	AcmeInc	Killed, Qu

https://www.sentinelone.com/

EDR/XDR



ENDPOINT DETAILS

VICTIM-DESKTOP

Windows 10 (64 bit)

Last active Last 4 minutes

Site name Demo

Health status

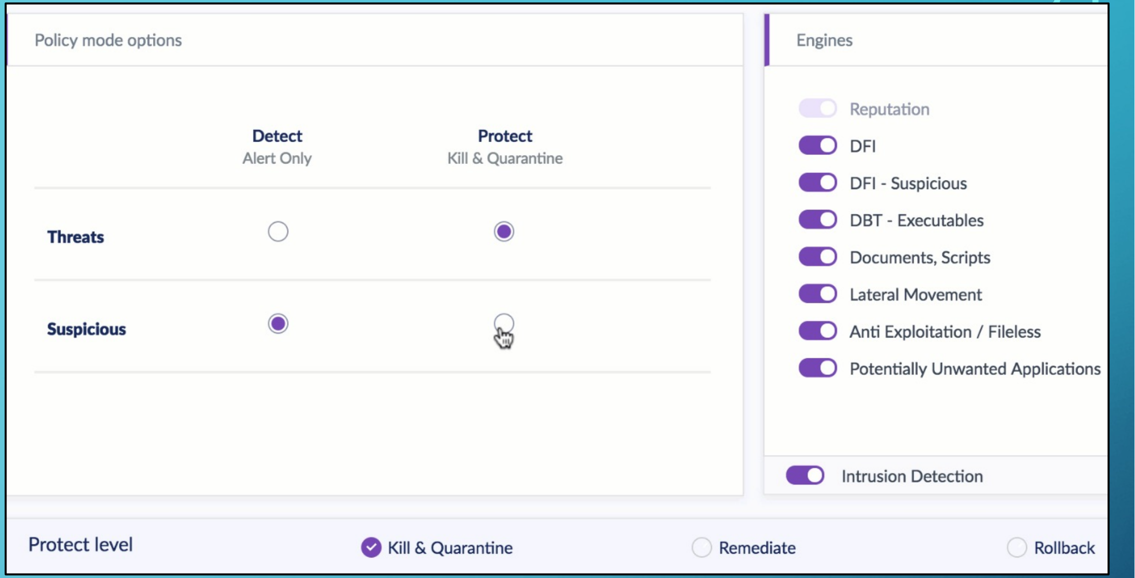
Last logged in

Group name

Agent version	2.6.1.5901 UPDATED	Console conn
Scan status	N/A	Network statu
Memory	2.00 GB	Domain
CPU	1 X Intel(R) Core(TM) i7-...	Subscribed on
Core count	1	Console visibl
Disk encryption	Off	IP Address

Network Adapters:

NAME	IP	MAC AD



Policy mode options

	Detect Alert Only	Protect Kill & Quarantine
Threats	○	●
Suspicious	●	○

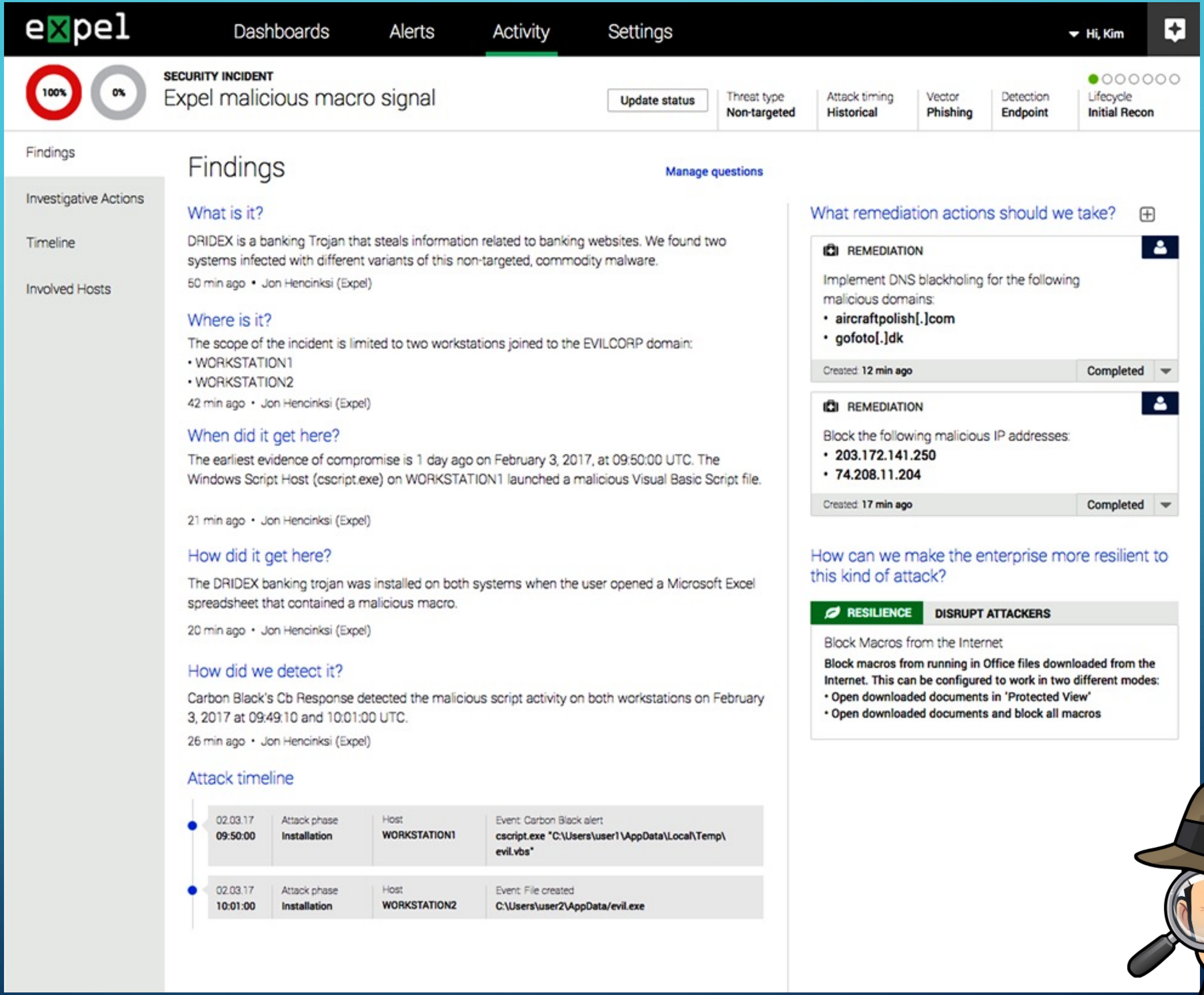
Engines

- Reputation
- DFI
- DFI - Suspicious
- DBT - Executables
- Documents, Scripts
- Lateral Movement
- Anti Exploitation / Fileless
- Potentially Unwanted Applications
- Intrusion Detection

Protect level ☑ Kill & Quarantine ○ Remediate ○ Rollback

https://www.sentinelone.com/

MDR



SECURITY INCIDENT

Expel malicious macro signal

Update status

Threat type	Attack timing	Vector	Detection	Lifecycle
Non-targeted	Historical	Phishing	Endpoint	Initial Recon

Findings

Manage questions

What is it?

DRIDEX is a banking Trojan that steals information related to banking websites. We found two systems infected with different variants of this non-targeted, commodity malware.

50 min ago • Jon Hencinksi (Expel)

Where is it?

The scope of the incident is limited to two workstations joined to the EVILCORP domain:

- WORKSTATION1
- WORKSTATION2

42 min ago • Jon Hencinksi (Expel)

When did it get here?

The earliest evidence of compromise is 1 day ago on February 3, 2017, at 09:50:00 UTC. The Windows Script Host (cscript.exe) on WORKSTATION1 launched a malicious Visual Basic Script file.

21 min ago • Jon Hencinksi (Expel)

How did it get here?

The DRIDEX banking trojan was installed on both systems when the user opened a Microsoft Excel spreadsheet that contained a malicious macro.

20 min ago • Jon Hencinksi (Expel)

How did we detect it?

Carbon Black's Cb Response detected the malicious script activity on both workstations on February 3, 2017 at 09:49:10 and 10:01:00 UTC.

26 min ago • Jon Hencinksi (Expel)

Attack timeline

02.03.17 09:50:00	Attack phase Installation	Host WORKSTATION1	Event: Carbon Black alert cscript.exe "C:\Users\user1\AppData\Local\Temp\evil.vbs"
02.03.17 10:01:00	Attack phase Installation	Host WORKSTATION2	Event: File created C:\Users\user2\AppData/evil.exe

What remediation actions should we take?

REMEDIATION

Implement DNS blackholing for the following malicious domains:

- aircraftpolish[.]com
- gofoto[.]dk

Created: 12 min ago Completed

REMEDIATION

Block the following malicious IP addresses:

- 203.172.141.250
- 74.208.11.204

Created: 17 min ago Completed

How can we make the enterprise more resilient to this kind of attack?

RESILIENCE DISRUPT ATTACKERS

Block Macros from the Internet

Block macros from running in Office files downloaded from the Internet. This can be configured to work in two different modes:

- **Open downloaded documents in 'Protected View'**
- **Open downloaded documents and block all macros**

https://expel.com/

Post-Incident Activity

- What should be done to improve security posture?
- What board involvement, notifications, or reporting is required?
- Is remedial training required for one or more employees?
- Are any HR actions required?
- What 3rd Parties need to be engaged (if any)?
  - Law Enforcement, Compliance Regulators, Insurance Carrier, ?-ISAC
- COMMUNICATIONS PLAN

Wrap-up

- What went well for XYZ Bank?
- What could XYZ bank have done better?
- What changes does XYZ bank need to make?
- Any other observations or action items?

Contact Info

Dennis M. Allen

Director - Security Programs - Strategy & Risk

stratascale

An SHI Company

https://www.linkedin.com/in/dennis-m-allen