CyberSN

Pwn your career

Active Cyber Defenses

2023 Cyber Security Day

Dom Glavach, CISSP

Chief Security and Technology Officer

Whoami

Dom Glavach – IUP CS Alumni

- CISO, Research Fellow, *Red/Blue/Purple*
- Cyber Organization SME
- Cyber Diligence & Breach Assessment (M&E/PE Investments)
- 20+ Government Contactor
- AFCEA Cyber Committee Chair (embedded and vehicle security)
- DNS junkie, prefer IRC over chat and coach a little hockey

https://CyberSN.com/cybersecurity-career-center

Cyber Threat Landscape (reported)

- **9,334** New vulnerabilities in the last 90 days
  - *National Vulnerability Database*
- **40%** year to year increase of interactive attacks
  - *Crowdstrike*
- **1 in 3 breaches** were identified by an organization’s team or tools
  - *IBM Cost of a Data Breach Report*
- **Many many more**
  - *Phishing*
  - *Identity*
  - *Industry*
  - *Cloud vs on-premise*
  - *Time to discover*

Current Approaches

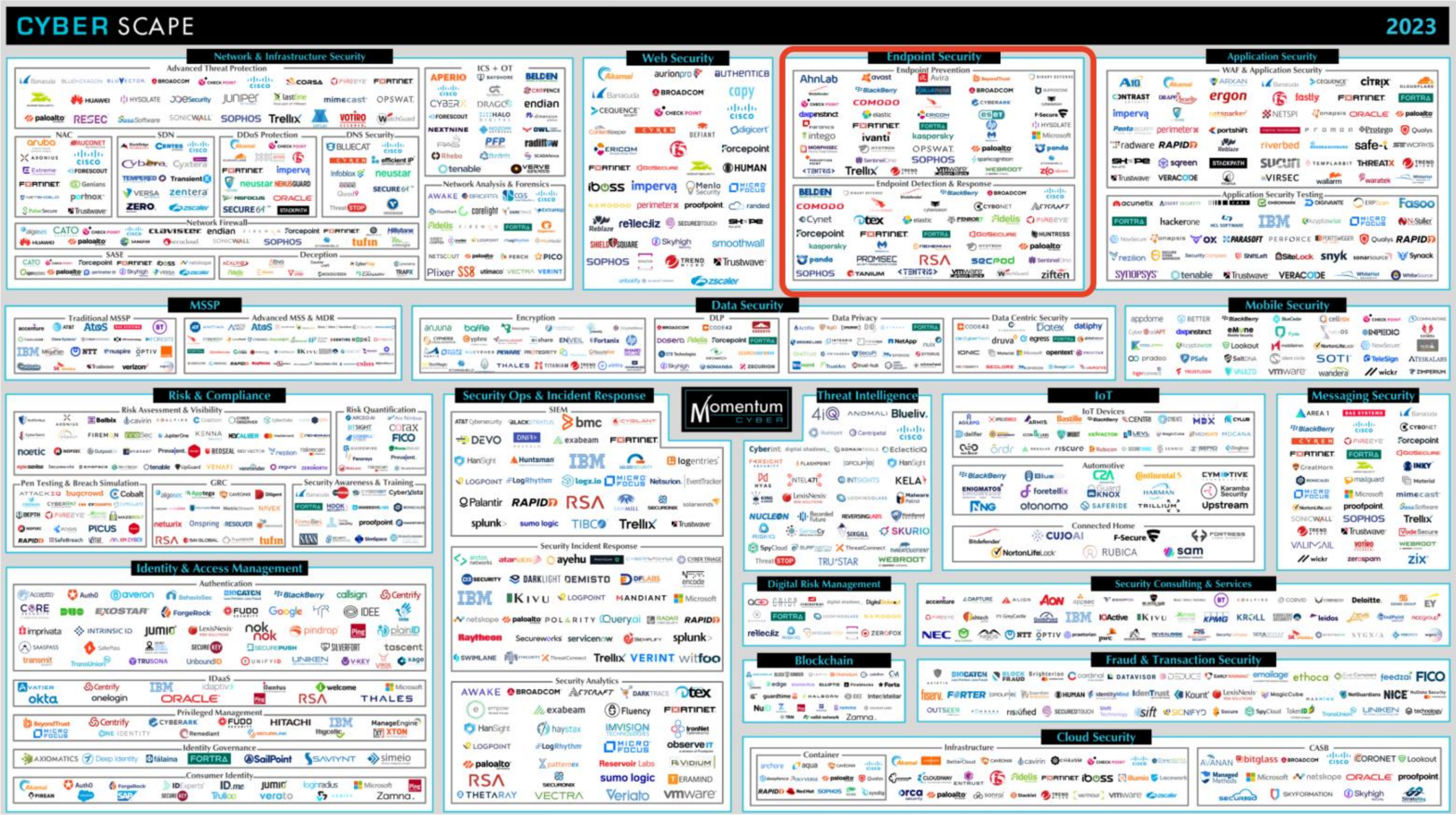
- Evolved over time as perimeters blurred
- Then
  - Patch
  - Defend
  - Detect
  - Respond
- Now
  - Hygiene
  - Identity
  - Visibility
  - Resilience
  - Reporting

Evolved and similar results

Product overcrowding

- Defense in Depth
  - Founding cyber principle
  - Not intended to become a purchasing strategy
- Complexity
  - Environment/Architecture
  - Regulatory Compliance
  - The People
- Cyber industry and organizations require solutions

Overcrowding



Momentum Cyber – Q1 2023 Cybersecurity Market Review

Adversaries

- Opportunistic
- Organized (sometimes)
- Innovative
  - LLM
  - Endless examples
- Cost effective *or lazy*
- Persistent and persistence
- Disruptive

"What keeps you up at night?"

Question?

Do you think adversaries can bypass cyber solutions?

Answer(s)

Depends on who we are asking…

While (yes)

- From our standpoint (attackers and defender) the answer is: **Yes**
  - Can we detect (discover) the evasion?
  - How long to respond and remediate?
  - How can we build resiliency?

- Better question
  - Can we find the threat before the incident?

- No silver bullets
  - Solutions, Visibility SOAR, IR, Pen Testing, Red Teaming
  - Pairing data, environment and people
    - Threat Hunting

Flash back

- Evolved over time as perimeters blurred
- Then
  - Patch
  - Defend
  - Detect
  - Respond
- Now
  - Hygiene
  - Identity
  - Visibility
  - Resilience
  - Reporting

Security Analyst Perspective

Threat Hunting

Threat hunting is a proactive and ongoing cybersecurity practice that aims to uncover hidden threats that may evade traditional security measures. Leveraging people expertise, data analysis, and continuous monitoring to identify and remediate (respond) potential cyber incidents before they can cause significant damage to an organization.

- Actively searching for advanced adversaries
    - Beacons, anomalies, tactics
    - Environment and activities
        - Point in time hunt example
- Beyond automations and solutions
    - *Can we find the threat before the incident?*

Attributes

- **Proactivity:** Proactive searching for any unusual or suspicious activities that may indicate a cyber threat.
- **Expertise:** Leverage knowledge, experience, and data to identify potential threats.
- **Continuous:** Continuously monitoring and searching rather than on an ad-hoc basis.
- **Data:** Analyze large volumes of data, including logs, network traffic, and endpoint information, to identify patterns, anomalies, and potential threats.
- **Indicators:** Indicators of compromise (IOCs) and indicators of attack that can be behavioral, technical, or contextual in nature.
- **Hypothesis-Driven:** Develop hypotheses based on the understanding of the organization's environment and the evolving threat landscape.
- **Collaborative:** Collaboration between different cybersecurity teams, incident responders, analysts, and leadership to share information and insights.
- **Evolving:** As threats evolve, threat hunting techniques and strategies must also adapt
- **Prescriptive:** Once a potential threat is identified, mitigate and initiate remediation measures.

Common Threat Hunting Models

- **Intel-based Hunting:** Information from threat intelligence sources
  - IoCs, hash values, IP addresses, domain names and networks or host artifact
  - Threat Intelligence providers, CERTS, Information Sharing and Analysis Centers (ISACs)
  - Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII)

- **Hypothesis hunting:** Leverages frameworks, and global detection playbooks to identify advanced persistent threat groups and malware attacks
  - Attacker IoAs and TTPs
  - Searching threat actors based on the environment, domain and attack behaviors

- **Custom hunting:** Situational awareness and industry-based hunting methods.
  - Anomalies in the SIEM and EDR tools and is customizable based on environment requirements
  - Targeted attacks and geopolitical issues

Good Threat Hunters

- Curious
- Informed
- Collaborative

- Building a career
  - Security Analyst
  - Incident Response
  - Threat Intelligence

Artificial Intelligence impact?

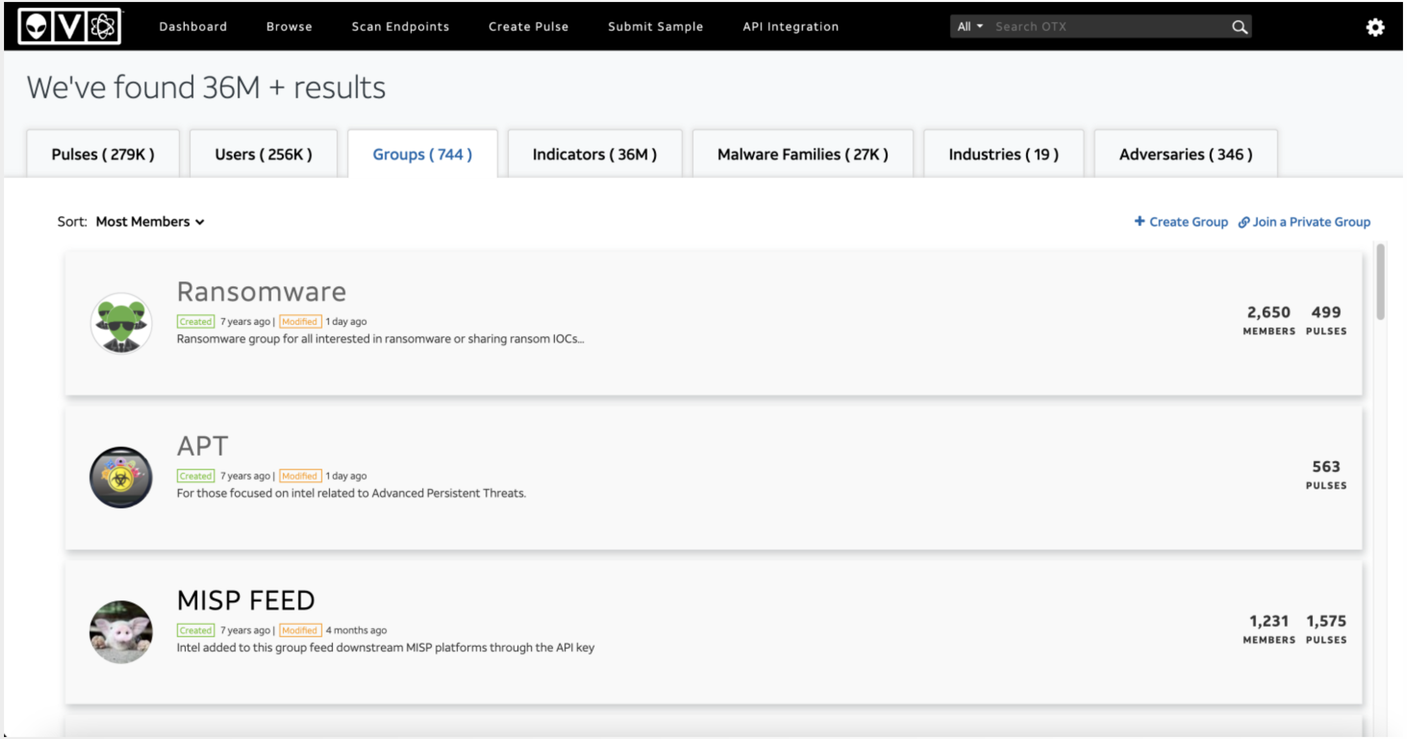
Available Tools & Resources

- **Threat Intelligence Feeds**
  - Knowing the trends
- **MITRE ATT&CK Framework**
  - Knowing the adversary
- **Velociraptor**
  - Intel-based and custom hunts
- **Real Intelligence Threat Analytics (RITA)**
  - Finding the adversary beacon
- **HTB Hunts**
  - CTF style hunting

Threat Intelligence Feeds

- **AlienVault – Open Threat Exchange**
  - Personal favorite – free access to over 20 million threat indicators and collaboration
  - **https://otx.alienvault.com/**
- **SANS Internet Storm Center**
  - Daily incident handler diaries summarize and analyze cyber events and new trends
  - **https://isc.sans.edu/**
- **VirusShare Malware Repository**
  - Repository of malware samples – excellent for research, forensics, and hunting
  - **https://virusshare.com/**
- URLhaus (Abuse.ch)
  - Tracks and share malware URLs
  - **https://urlhaus.abuse.ch/browse/**
- FBI InfraGard Portal
  - Information related to the 16 critical infrastructure of sectors.
  - **https://www.infragard.org/** - *Membership may vary*

AlienVault OTX



We've found 36M + results

Ransomware

Created 7 years ago | Modified 1 day ago

Ransomware group for all interested in ransomware or sharing ransom IOCs...

2,650 MEMBERS 499 PULSES

APT

Created 7 years ago | Modified 1 day ago

For those focused on intel related to Advanced Persistent Threats.

563 PULSES

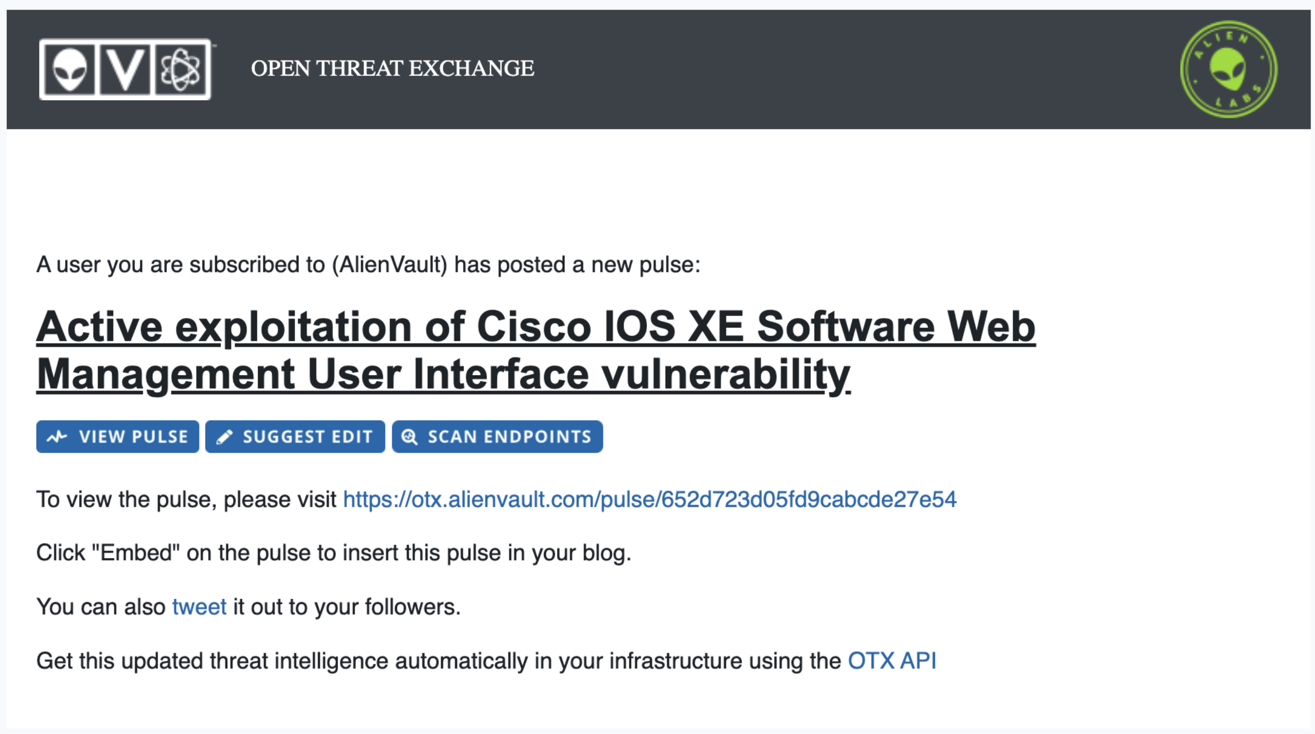
MISP FEED

Created 7 years ago | Modified 4 months ago

Intel added to this group feed downstream MISP platforms through the API key

1,231 MEMBERS 1,575 PULSES

AlienVault OTX Pulses



A user you are subscribed to (AlienVault) has posted a new pulse:

Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability

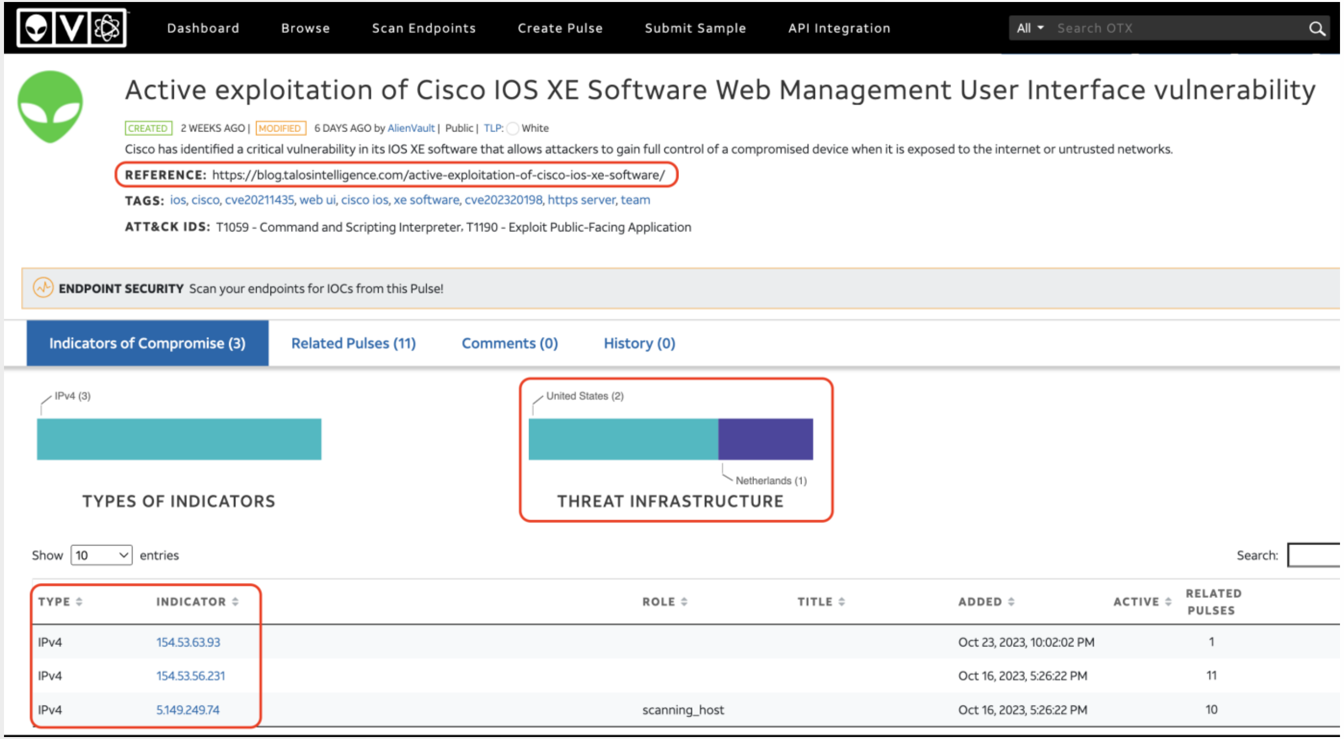
To view the pulse, please visit https://otx.alienvault.com/pulse/652d723d05fd9cabcde27e54

Click "Embed" on the pulse to insert this pulse in your blog.

You can also tweet it out to your followers.

Get this updated threat intelligence automatically in your infrastructure using the OTX API

AlienVault OTX Pulses Details



Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability

CREATED 2 WEEKS AGO | MODIFIED 6 DAYS AGO by AlienVault | Public | TLP: ○ White

Cisco has identified a critical vulnerability in its IOS XE software that allows attackers to gain full control of a compromised device when it is exposed to the internet or untrusted networks.

REFERENCE: https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

TAGS: ios, cisco, cve20211435, web ui, cisco ios, xe software, cve202320198, https server, team

ATT&CK IDS: T1059 - Command and Scripting Interpreter, T1190 - Exploit Public-Facing Application

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

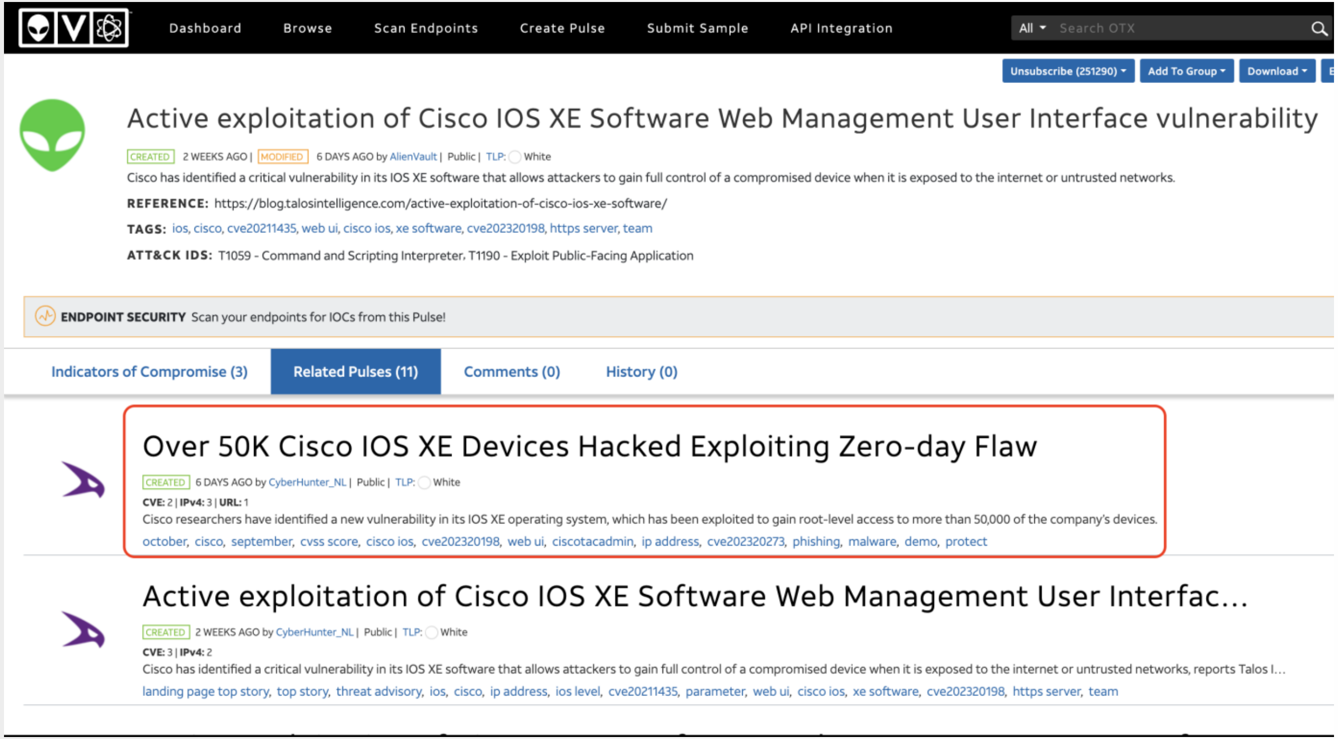
Show 10 entries

Search:

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
IPv4	154.53.63.93			Oct 23, 2023, 10:02:02 PM		1
IPv4	154.53.56.231			Oct 16, 2023, 5:26:22 PM		11
IPv4	5.149.249.74	scanning_host		Oct 16, 2023, 5:26:22 PM		10

©2023 CyberSN

AlienVault OTX Pulses Evolution



Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability

CREATED 2 WEEKS AGO | MODIFIED 6 DAYS AGO by AlienVault | Public | TLP: ○ White

Cisco has identified a critical vulnerability in its IOS XE software that allows attackers to gain full control of a compromised device when it is exposed to the internet or untrusted networks.

REFERENCE: https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

TAGS: ios, cisco, cve20211435, web ui, cisco ios, xe software, cve202320198, https server, team

ATT&CK IDS: T1059 - Command and Scripting Interpreter, T1190 - Exploit Public-Facing Application

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

Indicators of Compromise (3) | Related Pulses (11) | Comments (0) | History (0)

Over 50K Cisco IOS XE Devices Hacked Exploiting Zero-day Flaw

CREATED 6 DAYS AGO by CyberHunter_NL | Public | TLP: ○ White

CVE: 2 | **IPv4:** 3 | **URL:** 1

Cisco researchers have identified a new vulnerability in its IOS XE operating system, which has been exploited to gain root-level access to more than 50,000 of the company's devices.

october, cisco, september, cvss score, cisco ios, cve202320198, web ui, ciscotacadmin, ip address, cve202320273, phishing, malware, demo, protect

Active exploitation of Cisco IOS XE Software Web Management User Interfac...

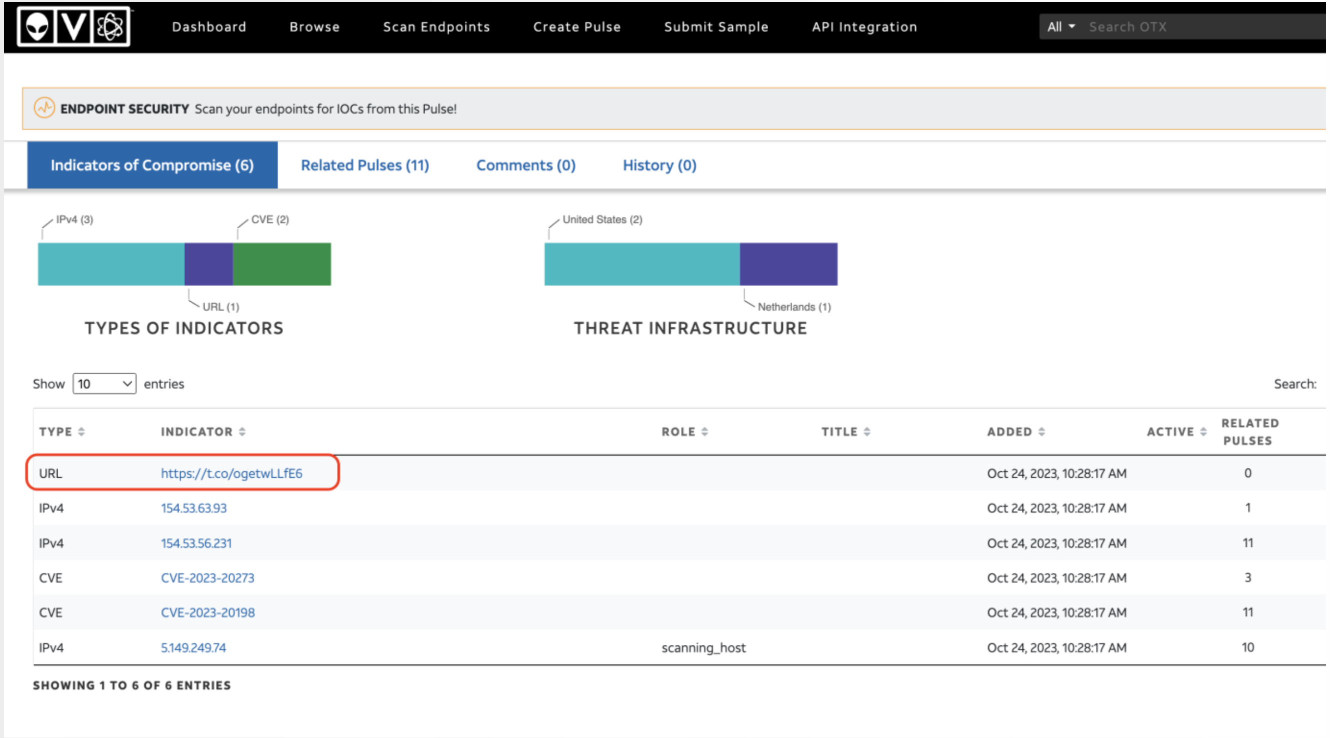
CREATED 2 WEEKS AGO by CyberHunter_NL | Public | TLP: ○ White

CVE: 3 | **IPv4:** 2

Cisco has identified a critical vulnerability in its IOS XE software that allows attackers to gain full control of a compromised device when it is exposed to the internet or untrusted networks, reports Talos I...

landing page top story, top story, threat advisory, ios, cisco, ip address, ios level, cve20211435, parameter, web ui, cisco ios, xe software, cve202320198, https server, team

AlienVault OTX Pulses Evolution Details



TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
URL	https://t.co/ogetwLLfE6			Oct 24, 2023, 10:28:17 AM		0
IPv4	154.53.63.93			Oct 24, 2023, 10:28:17 AM		1
IPv4	154.53.56.231			Oct 24, 2023, 10:28:17 AM		11
CVE	CVE-2023-20273			Oct 24, 2023, 10:28:17 AM		3
CVE	CVE-2023-20198			Oct 24, 2023, 10:28:17 AM		11
IPv4	5.149.249.74	scanning_host		Oct 24, 2023, 10:28:17 AM		10

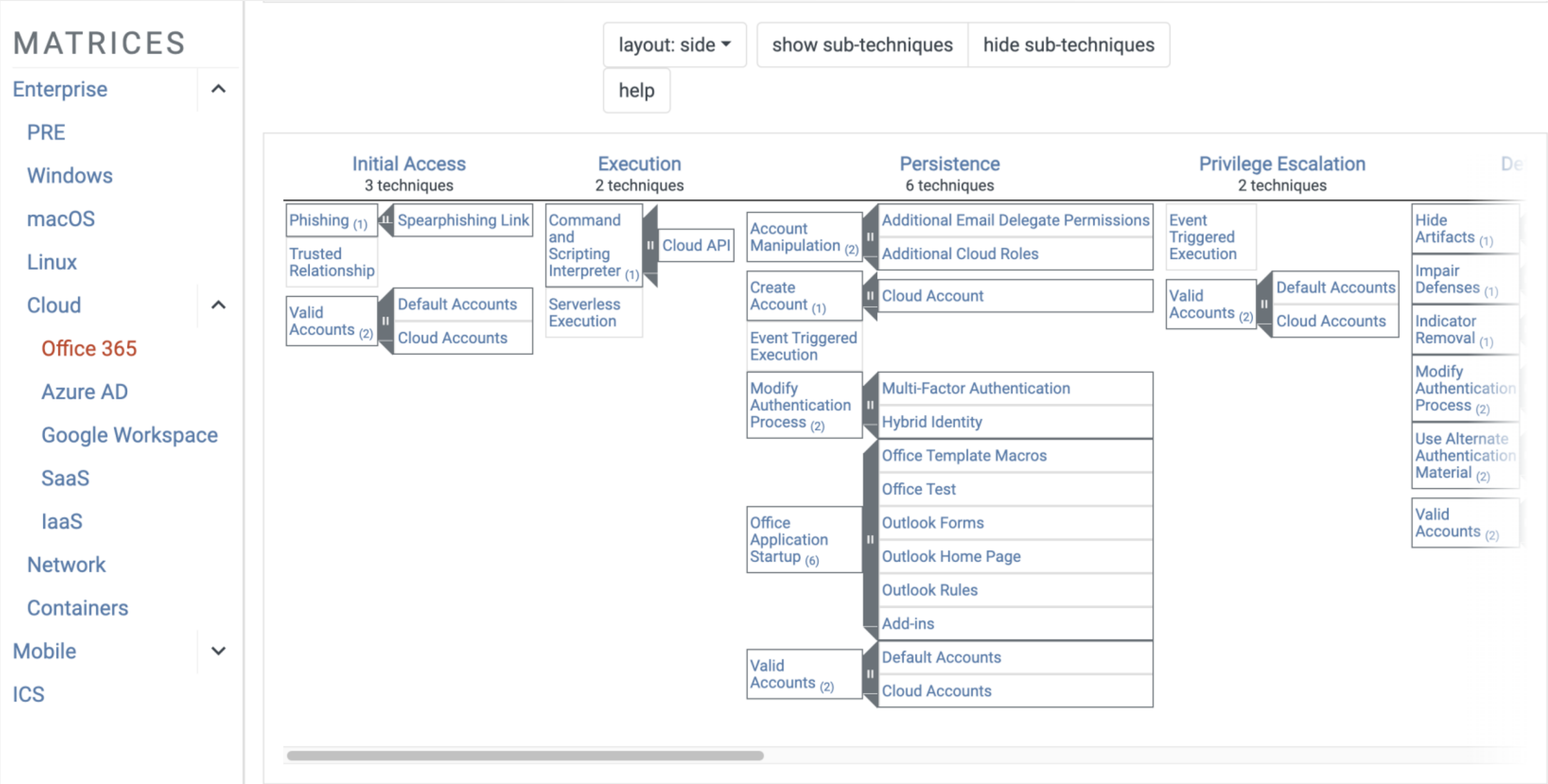
SHOWING 1 TO 6 OF 6 ENTRIES

MITRE ATT&CK Framework

- ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework
  - Version 14 is being released today (10/31/2023)
  - **https://attack.mitre.org/**

- Starting points
  - **https://attack.mitre.org/matrices/enterprise/**
  - **https://attack.mitre.org/tactics/enterprise/**

MITRE ATT&CK Framework – Office 365 Matrix



Initial Access 3 techniques

- Phishing (1)
  - Spearphishing Link
- Trusted Relationship
- Valid Accounts (2)
  - Default Accounts
  - Cloud Accounts

Execution 2 techniques

- Command and Scripting Interpreter (1)
  - Cloud API
- Serverless Execution

Persistence 6 techniques

- Account Manipulation (2)
  - Additional Email Delegate Permissions
  - Additional Cloud Roles
- Create Account (1)
  - Cloud Account
- Event Triggered Execution
- Modify Authentication Process (2)
  - Multi-Factor Authentication
  - Hybrid Identity
- Office Application Startup (6)
  - Office Template Macros
  - Office Test
  - Outlook Forms
  - Outlook Home Page
  - Outlook Rules
  - Add-ins
- Valid Accounts (2)
  - Default Accounts
  - Cloud Accounts

Privilege Escalation 2 techniques

- Event Triggered Execution
- Valid Accounts (2)
  - Default Accounts
  - Cloud Accounts

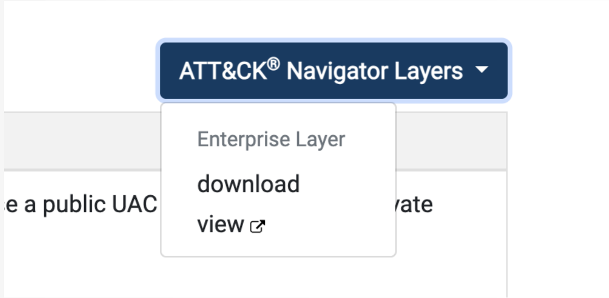
De

- Hide Artifacts (1)
- Impair Defenses (1)
- Indicator Removal (1)
- Modify Authentication Process (2)
- Use Alternate Authentication Material (2)
- Valid Accounts (2)

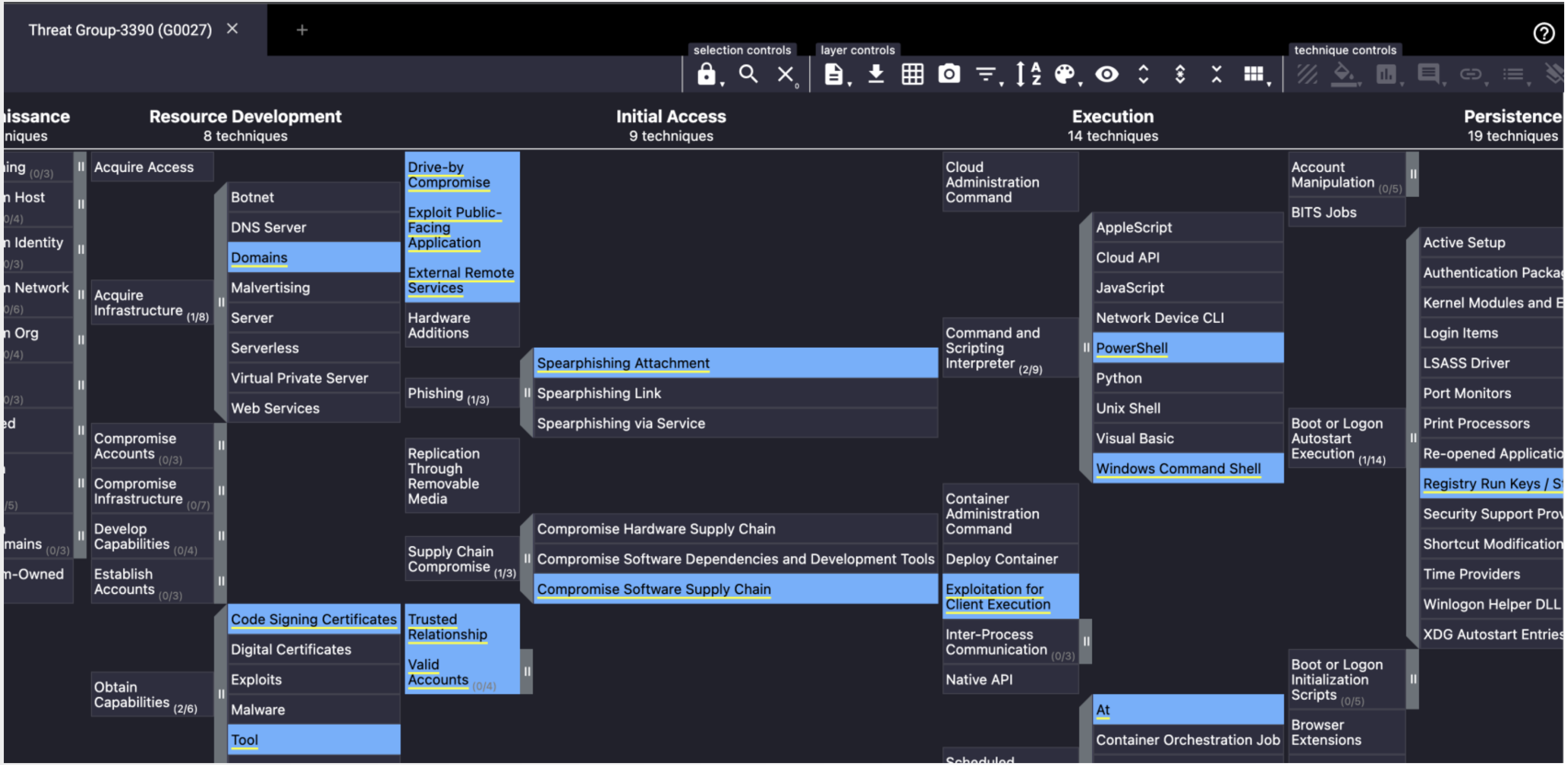
Explore more: **https://attack.mitre.org/matrices/enterprise/cloud/office365/**

MITRE ATT&CK Navigator

- ATT&CK Interactive navigator
    - Web-based tool for annotating and exploring ATT&CK matrices.
    - Visualize defense coverage, red team planning and more
    - https://mitre-attack.github.io/attack-navigator/
    - Quick sample of comparing two adversary groups
        - **https://youtu.be/78RIsFqo9pM**
    - Also available within the browsable framework



MITRE ATT&CK Navigator – Threat Group 3390



...issance
...niques

- ...ing (0/3)
- ...n Host (0/4)
- ...n Identity (0/3)
- ...n Network (0/6)
- ...n Org (0/4)
- (0/3)
- ...ed
- (/5)
- ...mains (0/3)
- ...n-Owned

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (1/8)
  - Botnet
  - DNS Server
  - Domains
  - Malvertising
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (2/6)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
  - Compromise Hardware Supply Chain
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
- Trusted Relationship
- Valid Accounts (0/4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (2/9)
  - AppleScript
  - Cloud API
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled...
  - At
  - Container Orchestration Job

Persistence
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
  - Active Setup
  - Authentication Packa...
  - Kernel Modules and E...
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applicatio...
  - Registry Run Keys / S...
  - Security Support Prov...
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions

Velociraptor

- Inspired by Google Rapid Response and OSQuery.
- Hunting endpoint activity
  - Agent-based tool
  - Web Interface and API
  - Velociraptor Query Language (VQL)
  - Strong community support and well documented
  - Other DFIR applications

- Starting point
  - **https://docs.velociraptor.app/**

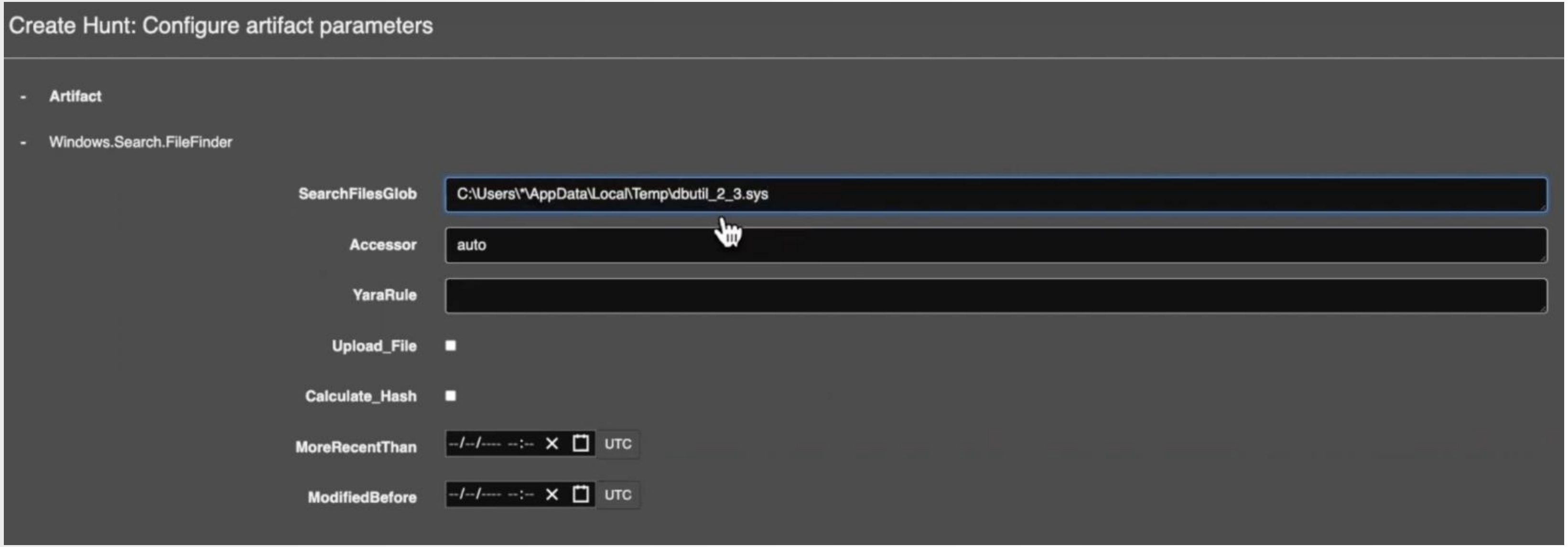
Velociraptor Hunting

- From basic to complex endpoint hunting
  - Simple file search
  - Complex VQL queries
  - Search the Artifact Exchange
    - MacOS.Application.Firefox.History – Reads firefox history
    - MacOS.UnifiedLogHunter – Live hunting of unified logs

- Labs
  - Server VM
  - Various OS Clients

- Training
  - https://docs.velociraptor.app/training/

Velociraptor – Basic Hunt

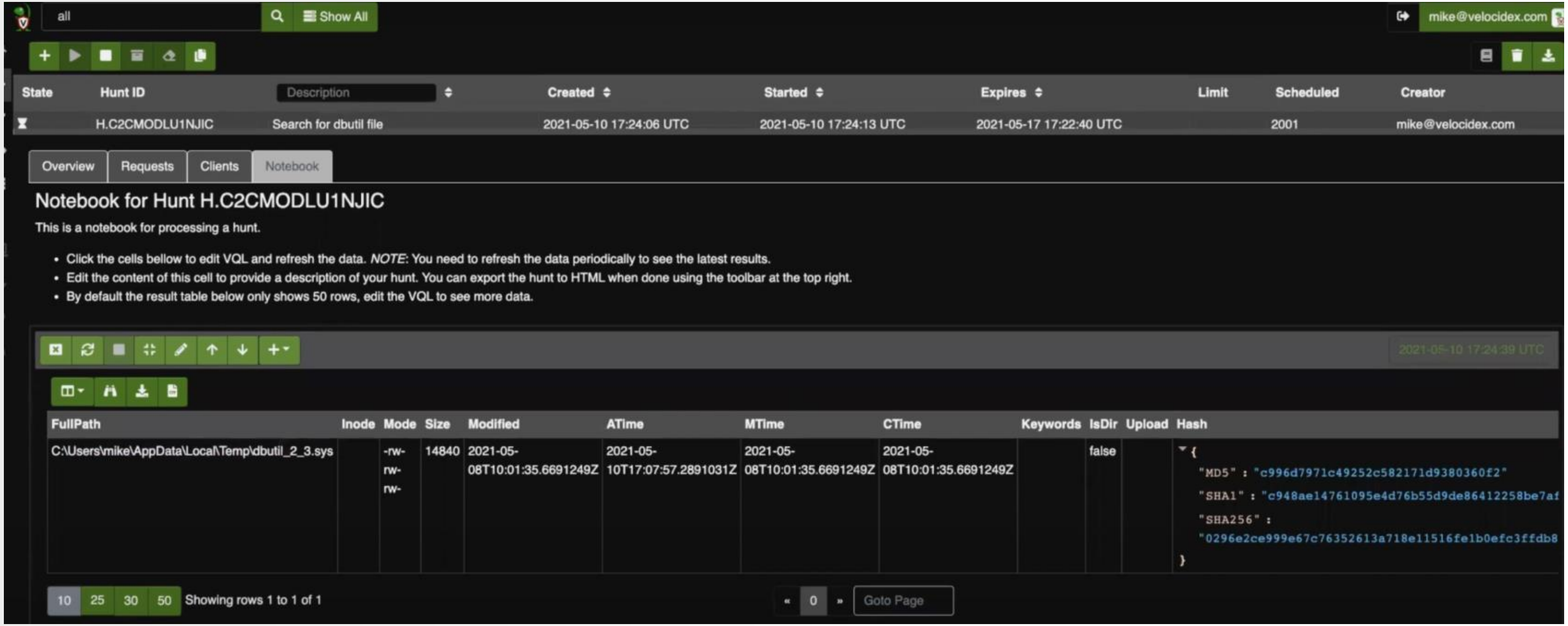


Create Hunt: Configure artifact parameters

- Artifact
- Windows.Search.FileFinder

SearchFilesGlob	C:\Users\*\AppData\Local\Temp\dbutil_2_3.sys
Accessor	auto
YaraRule	
Upload_File	□
Calculate_Hash	□
MoreRecentThan	--/--/---- --:-- UTC
ModifiedBefore	--/--/---- --:-- UTC

Velociraptor – Basic Hunt Results



State	Hunt ID	Description	Created	Started	Expires	Limit	Scheduled	Creator
⧗	H.C2CMODLU1NJIC	Search for dbutil file	2021-05-10 17:24:06 UTC	2021-05-10 17:24:13 UTC	2021-05-17 17:22:40 UTC		2001	mike@velocidex.com

Notebook for Hunt H.C2CMODLU1NJIC

This is a notebook for processing a hunt.

- Click the cells bellow to edit VQL and refresh the data. *NOTE*: You need to refresh the data periodically to see the latest results.
- Edit the content of this cell to provide a description of your hunt. You can export the hunt to HTML when done using the toolbar at the top right.
- By default the result table below only shows 50 rows, edit the VQL to see more data.

FullPath	Inode	Mode	Size	Modified	ATime	MTime	CTime	Keywords	IsDir	Upload	Hash

C:\Users\mike\AppData\Local\Temp\dbutil_2_3.sys		-rw-rw-rw-	14840	2021-05-08T10:01:35.6691249Z	2021-05-10T17:07:57.2891031Z	2021-05-08T10:01:35.6691249Z	2021-05-08T10:01:35.6691249Z		false		{
											"MD5" : "c996d7971c49252c582171d9380360f2"
											"SHA1" : "c948ae14761095e4d76b55d9de86412258be7af
											"SHA256" :
											"0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8
											}

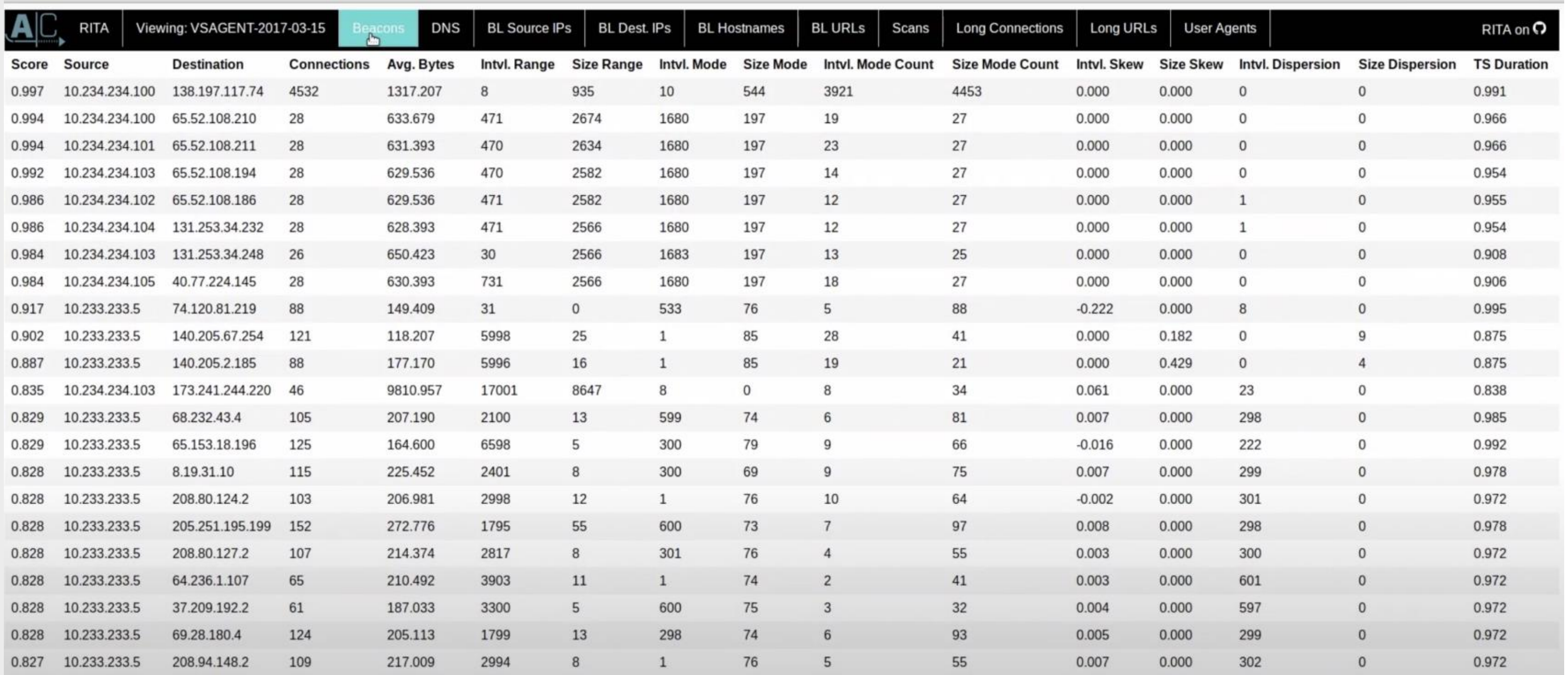
Showing rows 1 to 1 of 1

RITA

- Real Intelligence Threat Analytics
  - Zeek logs or PCAPs for analysis
  - Beacon hunting using behavior-based analytics
  - DNS Tunnelling and User-Agents
  - Web Interface and CLI

- Starting point
  - https://www.activecountermeasures.com/free-tools/adhd/
    - Active Defense Harbinger Distribution
    - RITA

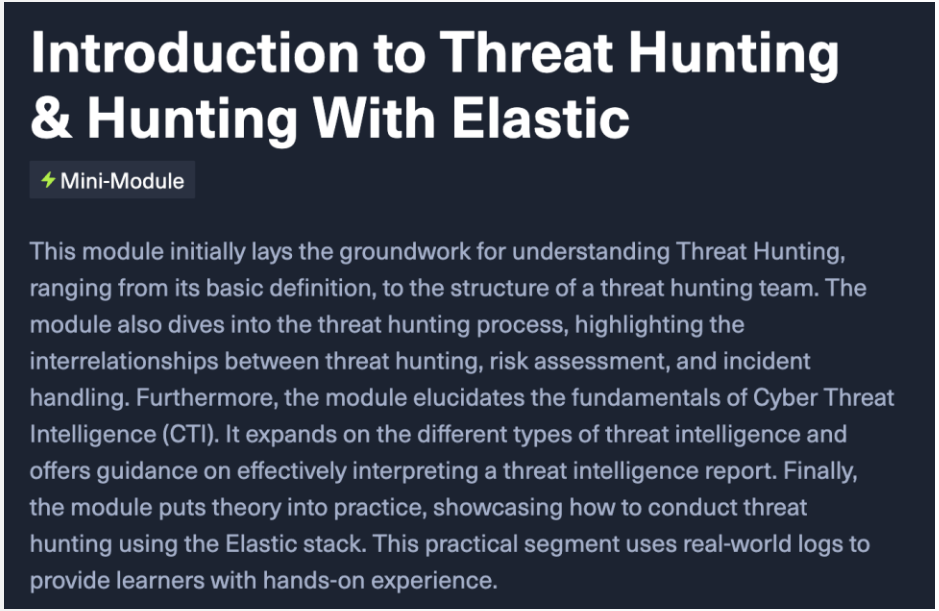
RITA Beacon Search



Score	Source	Destination	Connections	Avg. Bytes	Intvl. Range	Size Range	Intvl. Mode	Size Mode	Intvl. Mode Count	Size Mode Count	Intvl. Skew	Size Skew	Intvl. Dispersion	Size Dispersion	TS Duration
0.997	10.234.234.100	138.197.117.74	4532	1317.207	8	935	10	544	3921	4453	0.000	0.000	0	0	0.991
0.994	10.234.234.100	65.52.108.210	28	633.679	471	2674	1680	197	19	27	0.000	0.000	0	0	0.966
0.994	10.234.234.101	65.52.108.211	28	631.393	470	2634	1680	197	23	27	0.000	0.000	0	0	0.966
0.992	10.234.234.103	65.52.108.194	28	629.536	470	2582	1680	197	14	27	0.000	0.000	0	0	0.954
0.986	10.234.234.102	65.52.108.186	28	629.536	471	2582	1680	197	12	27	0.000	0.000	1	0	0.955
0.986	10.234.234.104	131.253.34.232	28	628.393	471	2566	1680	197	12	27	0.000	0.000	1	0	0.954
0.984	10.234.234.103	131.253.34.248	26	650.423	30	2566	1683	197	13	25	0.000	0.000	0	0	0.908
0.984	10.234.234.105	40.77.224.145	28	630.393	731	2566	1680	197	18	27	0.000	0.000	0	0	0.906
0.917	10.233.233.5	74.120.81.219	88	149.409	31	0	533	76	5	88	-0.222	0.000	8	0	0.995
0.902	10.233.233.5	140.205.67.254	121	118.207	5998	25	1	85	28	41	0.000	0.182	0	9	0.875
0.887	10.233.233.5	140.205.2.185	88	177.170	5996	16	1	85	19	21	0.000	0.429	0	4	0.875
0.835	10.234.234.103	173.241.244.220	46	9810.957	17001	8647	8	0	8	34	0.061	0.000	23	0	0.838
0.829	10.233.233.5	68.232.43.4	105	207.190	2100	13	599	74	6	81	0.007	0.000	298	0	0.985
0.829	10.233.233.5	65.153.18.196	125	164.600	6598	5	300	79	9	66	-0.016	0.000	222	0	0.992
0.828	10.233.233.5	8.19.31.10	115	225.452	2401	8	300	69	9	75	0.007	0.000	299	0	0.978
0.828	10.233.233.5	208.80.124.2	103	206.981	2998	12	1	76	10	64	-0.002	0.000	301	0	0.972
0.828	10.233.233.5	205.251.195.199	152	272.776	1795	55	600	73	7	97	0.008	0.000	298	0	0.978
0.828	10.233.233.5	208.80.127.2	107	214.374	2817	8	301	76	4	55	0.003	0.000	300	0	0.972
0.828	10.233.233.5	64.236.1.107	65	210.492	3903	11	1	74	2	41	0.003	0.000	601	0	0.972
0.828	10.233.233.5	37.209.192.2	61	187.033	3300	5	600	75	3	32	0.004	0.000	597	0	0.972
0.828	10.233.233.5	69.28.180.4	124	205.113	1799	13	298	74	6	93	0.005	0.000	299	0	0.972
0.827	10.233.233.5	208.94.148.2	109	217.009	2994	8	1	76	5	55	0.007	0.000	302	0	0.972

HackTheBox Threat Hunting

- Practical threat hunting module
  - https://academy.hackthebox.com/course/preview/introduction-to-threat-hunting--hunting-with-elastic



Introduction to Threat Hunting & Hunting With Elastic

This module initially lays the groundwork for understanding Threat Hunting, ranging from its basic definition, to the structure of a threat hunting team. The module also dives into the threat hunting process, highlighting the interrelationships between threat hunting, risk assessment, and incident handling. Furthermore, the module elucidates the fundamentals of Cyber Threat Intelligence (CTI). It expands on the different types of threat intelligence and offers guidance on effectively interpreting a threat intelligence report. Finally, the module puts theory into practice, showcasing how to conduct threat hunting using the Elastic stack. This practical segment uses real-world logs to provide learners with hands-on experience.

Additional Resources

- **https://www.crowdstrike.com/resources/reports/threat-hunting-report/**
  - Kerberoasting
- **https://attack.mitre.org/resources/related-projects/**
  - GitHub Repo
  - CASCADE
- **https://github.com/ThreatHuntingProject/hunter**
  - Threat Hunting Project
  - Complete threat hunting and analysis docker image
- **https://www.activecountermeasures.com/free-tools/**
  - Free hunting tools
- **https://www.activecountermeasures.com/hunt-training/**
  - **Free** Threat Hunting training – December 1, 2023 (6 hours)

CyberSN

Pwn your career

Thank you