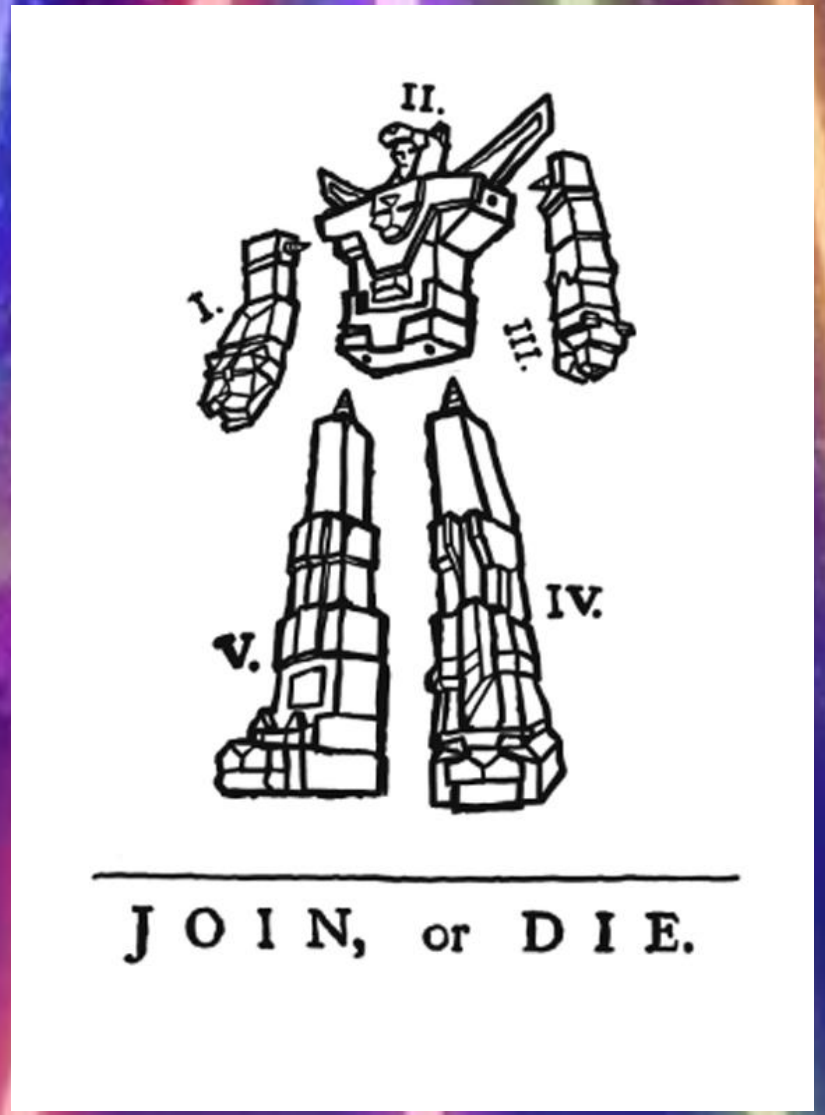
CREATING APT TARGETED THREAT FEEDS FOR YOUR INDUSTRY

Circle City Con 7.0 Apocalypse

Keith Chapman | CTIA
Senior Security Analyst
Belcan LLC
kchapman@belcan.com



My goal with this talk is to
share a method of getting more context
from threat feeds
and to use them in a way
that enriches what is important to you.

Defensive Pizza

Crust

Environmental Intelligence connects the other intelligences together.

Sauce

Curated intelligence feeds (global and community) enrich detection.

Toppings

Proactive Intelligence gives a targeted and actionable defense.

Advanced

Persistent

Threats

Adversary		Category or Nation-State
	SPIDER	ECRIME
	CHOLLIMA	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA)
	JACKAL	HACKTIVIST
	TIGER	INDIA
	KITTEN	IRAN
	LEOPARD	PAKISTAN
	PANDA	PEOPLE'S REPUBLIC OF CHINA
	BEAR	RUSSIAN FEDERATION
	CRANE	SOUTH KOREA
	BUFFALO	VIETNAM

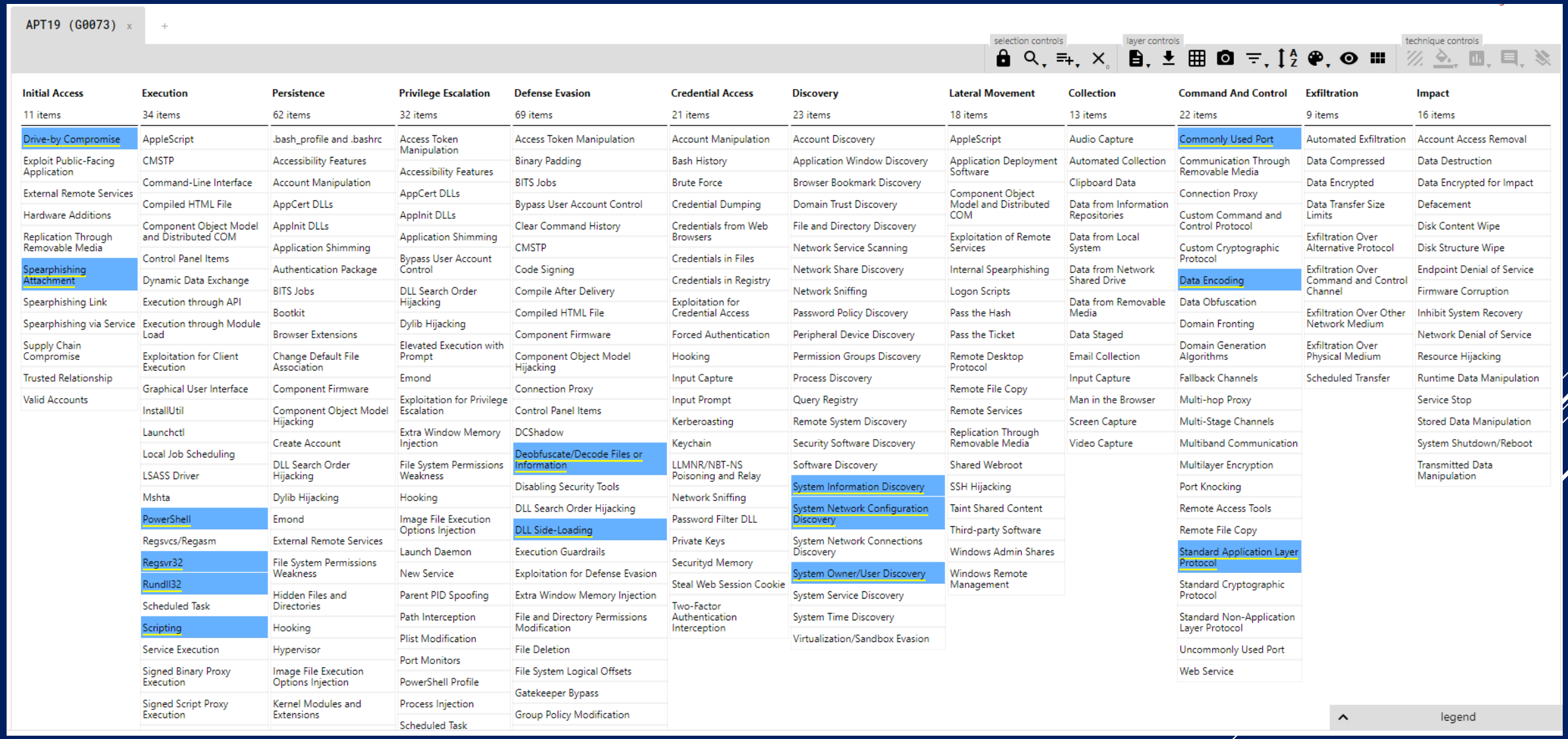
Image: CrowdStrike

You have around 20 minutes to contain a Russian APT attack

https://www.zdnet.com/article/you-have-around-20-minutes-to-contain-a-russian-apt-attack/

ATT&CK®

- MITRE ATT&CK is a knowledge base of adversary tactics and techniques based on real-world observations.
- Tactics are what attackers are trying to achieve.
- A technique is a specific behavior to achieve a goal and is often a single step in a string of activities employed to complete the attacker's overall mission.


APT19 (G0073)
selection controls
layer controls
technique controls
Initial Access
11 items
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
34 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Persistence
62 items
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
Emond
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Kernel Modules and Extensions
Privilege Escalation
32 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Parent PID Spoofing
Path Interception
Plist Modification
Port Monitors
PowerShell Profile
Process Injection
Scheduled Task
Defense Evasion
69 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Connection Proxy
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File and Directory Permissions Modification
File Deletion
File System Logical Offsets
Gatekeeper Bypass
Group Policy Modification
Credential Access
21 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Steal Web Session Cookie
Two-Factor Authentication Interception
Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark 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
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion
Lateral Movement
18 items
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Command And Control
22 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service
Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer
Impact
16 items
Account Access Removal
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
System Shutdown/Reboot
Transmitted Data Manipulation
legend

APT19

APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. [1] Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same. [2] [3] [4]

ID: G0073

Associated Groups: Codoso, C0d0so0, Codoso Team, Sunshop Group

Contributors: FS-ISAC, Darren Spruell

Version: 1.2

Created: 17 October 2018

Last Modified: 11 October 2019

Associated Group Descriptions

Name	Description
Codoso	[4]
C0d0so0	[4]
Codoso Team	[3]
Sunshop Group	[6]

Techniques Used

ATT&CK® Navi

Domain	ID	Name	Use
Enterprise	T1043	Commonly Used Port	APT19 used TCP port 80 for C2.[1]
Enterprise	T1132	Data Encoding	An APT19 HTTP malware variant used Base64 to encode communications to the C2 server.[4]
Enterprise	T1140	Deobfuscate/Decode Files or Information	An APT19 HTTP malware variant decrypts strings using single-byte XOR keys.[4]
Enterprise	T1073	DLL Side-Loading	APT19 launched an HTTP malware variant and a Port 22 malware variant using a legitimate executable that loaded the malicious DLL.[4]
Enterprise	T1189	Drive-by Compromise	APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets.[4]
Enterprise	T1143	Hidden Window	APT19 used `-W Hidden` to conceal PowerShell windows by setting the WindowStyle parameter to hidden.[1]
Enterprise	T1031	Modify Existing Service	An APT19 Port 22 malware variant registers itself as a service.[4]
Enterprise	T1112	Modify Registry	APT19 uses a Port 22 malware variant to modify several Registry keys.[4]
Enterprise	T1027	Obfuscated Files or Information	APT19 used Base64 to obfuscate commands and the payload.[1]
Enterprise	T1086	PowerShell	APT19 used PowerShell commands to execute payloads.[1]
Enterprise	T1060	Registry Run Keys / Startup	An APT19 HTTP malware variant establishes persistence by setting the Registry key [4]

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring application access tokens.

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring. [1]

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
    - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
    - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

ID: T1189

Tactic: Initial Access

Platform: Windows, Linux, macOS, SaaS

Permissions Required: User

Data Sources: Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)

Version: 1.1

Created: 18 April 2018

Last Modified: 11 October 2019

Mitigations

Mitigation	Description
Application Isolation and Sandboxing	Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist for these types of systems.[3][4]
Exploit Protection	Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. Many of these protections depend on the architecture and target application binary for compatibility.[5][6]
Restrict Web-Based Content	For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.
Update Software	Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on.

Detection

Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters. They can also do reputation-based analytics on websites and their requested resources such as how old a domain is, who it's registered to, if it's on a known bad list, or how many other users have connected to it before.

Network intrusion detection systems, sometimes with SSL/TLS MITM inspection, can be used to look for known malicious scripts (recon, heap spray, and browser identification scripts have been frequently reused), common script obfuscation, and exploit code.

Detecting compromise based on the drive-by exploit from a legitimate website may be difficult. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of browser processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic that may indicate additional tools transferred to the system.

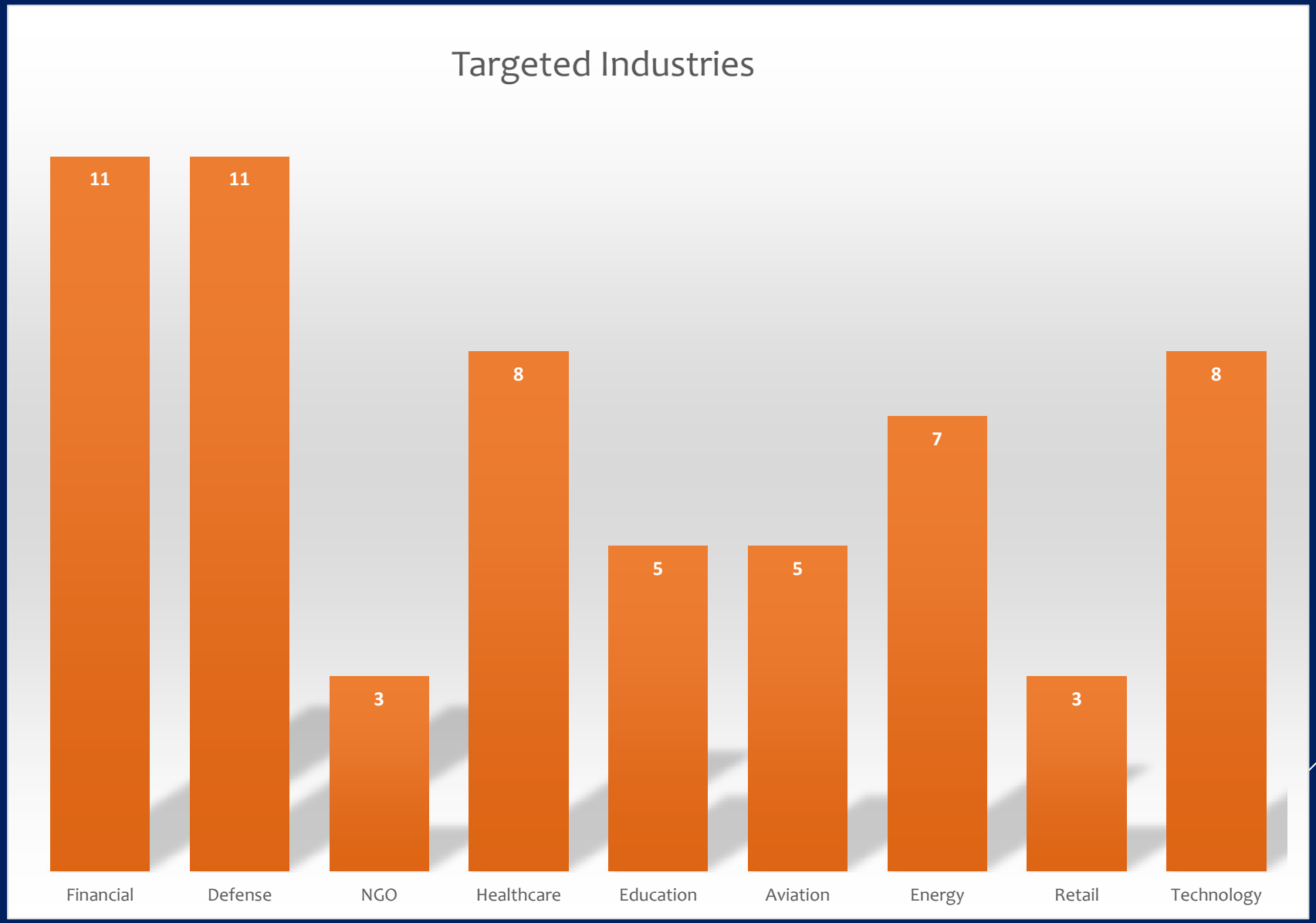
References

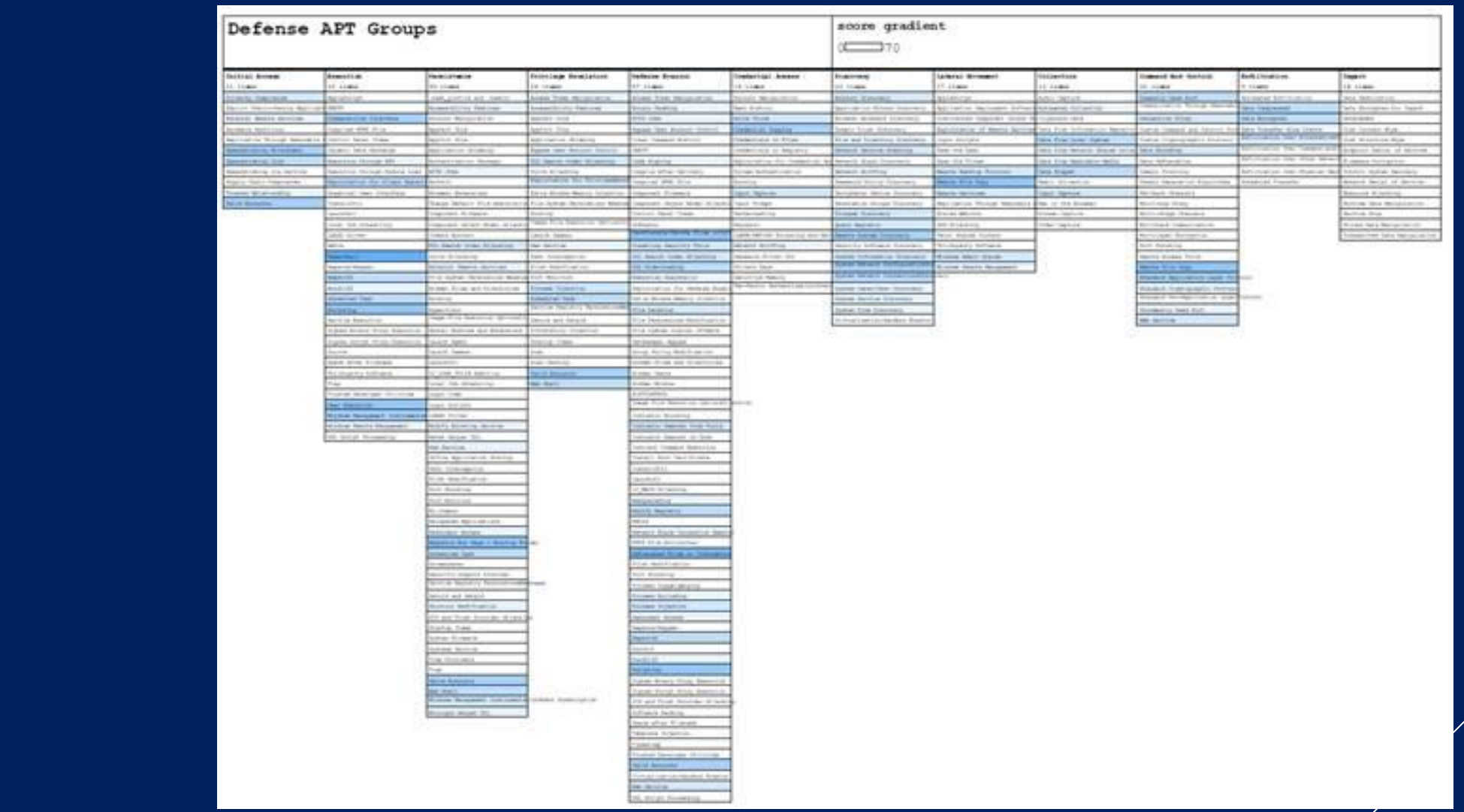
1. Adair, S., Moran, N. (2012, May 15). Cyber Espionage & Strategic Web Compromises – Trusted Websites Serving Dangerous Results. Retrieved March 13, 2018.
2. Lassalle, D., et al. (2017, November 6). OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society. Retrieved November 6, 2017.
3. Cowan, C. (2017, March 23). Strengthening the Microsoft Edge Sandbox. Retrieved March 12, 2018.
4. Goodin, D. (2017, March 17). Virtual machine escape fetches $105,000 at Pwn2Own hacking contest - updated. Retrieved March 12, 2018.
5. Nunez, N. (2017, August 9). Moving Beyond EMET II – Windows Defender Exploit Guard. Retrieved March 12, 2018.
6. Wikipedia. (2018, January 11). Control-flow integrity. Retrieved March 12, 2018.
7. FireEye. (2018, February 20). APT37 (Reaper): The Overlooked North Korean Actor. Retrieved March 1, 2018.
8. Trend Micro. (2017, February 27). RATANKBA: Delving into Large-scale Watering Holes against Enterprises. Retrieved May 22, 2018.
9. US-CERT. (2018, March 16). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved June 6, 2018.
10. DiMaggio, J. (2016, April 28). Tick cyberespionage group zeros in on Japan. Retrieved July 16, 2018.

- Select the APT groups that target your industry.

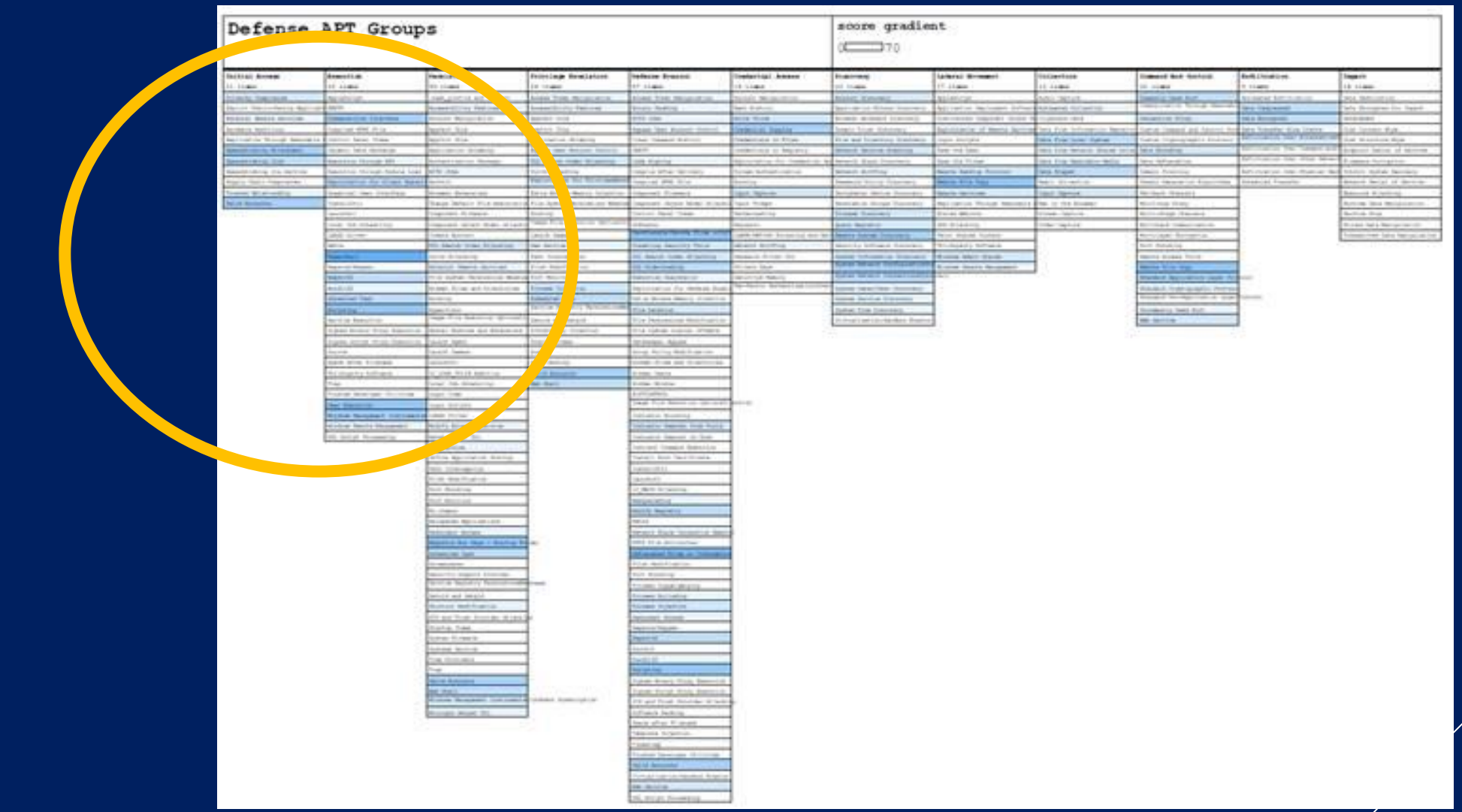
	A	B	C	D	E	F	G	H	I	J
1	Groups	*Financial*	*Defense*	*NGO*	*Healthcare*	*Education*	*Aviation*	*Energy*	*Retail*	*Technology*
2	admin@338									
3	APT12									
4	APT17									
5	APT18									
6	APT19									
7	APT33									
8	APT38									
9	APT41									
10	Carbanak									
11	Charming Kitten									
12	Cobalt Group									
13	Deep Panda									
14	Dragonfly									
15	Dragonfly 2.0									
16	Elderwood									
17	FIN4									
18	FIN5									
19	FIN6									
20	FIN7									
21	FIN8									
22	Gallmaker									
23	GCMAN									
24	Honeybee									
25	Leviathan									
26	Magic Hound									
27	menuPass									
28	MuddyWater									
29	OilRig									
30	Orangeworm									
31	Silence									
32	Silver Terrier									
33	Stone Pencil									
34	Threat Group-3390									
35	Thrip									
36	Tropic Trooper									
37	Turla									

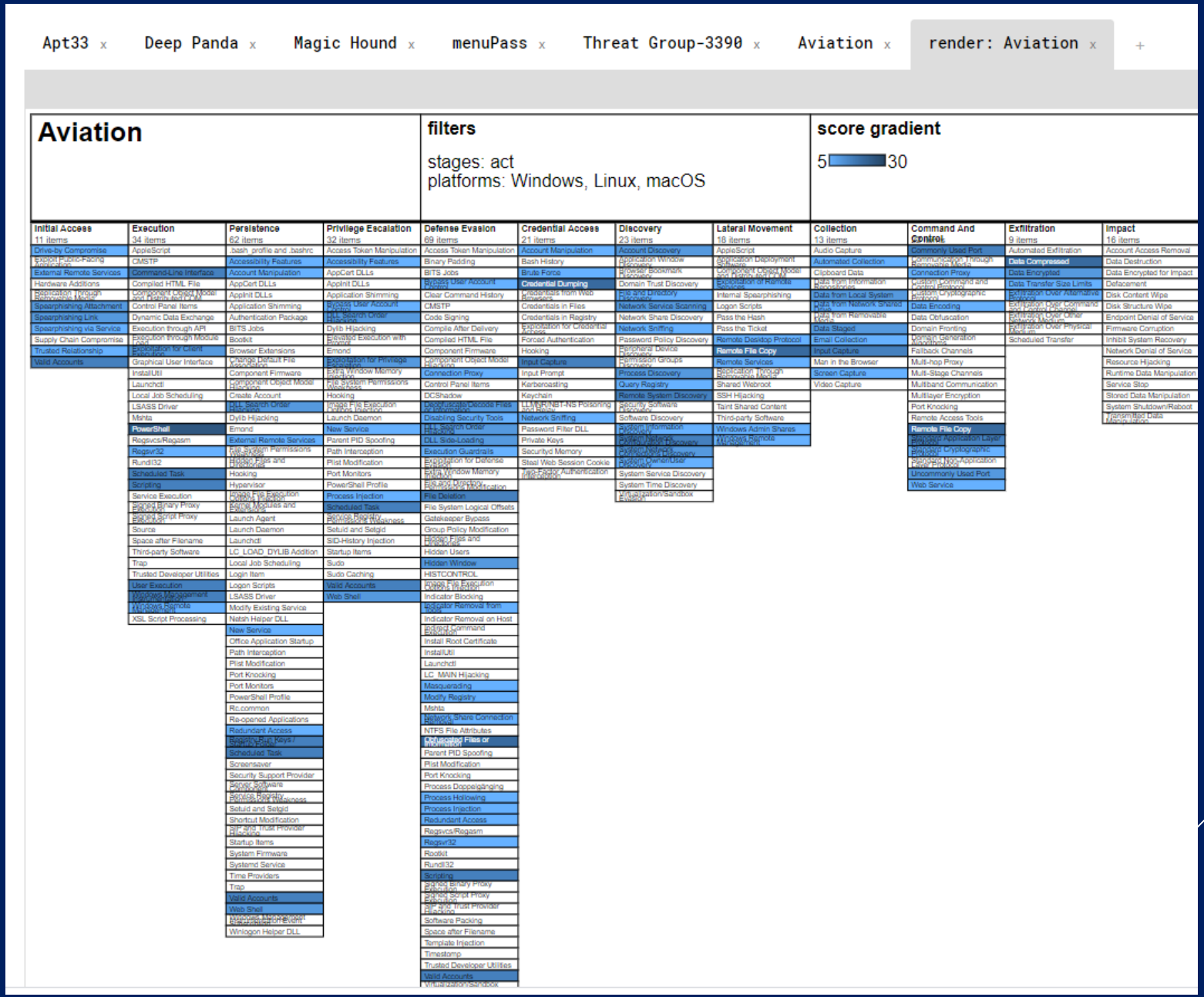
https://attack.mitre.org/beta/groups/


Targeted Industries
11
11
3
8
5
5
7
3
8
Financial
Defense
NGO
Healthcare
Education
Aviation
Energy
Retail
Technology


Defense APT Groups
score gradient
0
70

- Research APT groups that target your industry.
- Make a heat map using MITRE ATT&CK tools to see which techniques were most likely.
- A single color may work better than stop light protocol colors.
- Assign scores to each APT group and layer them.
- Place focus on the beginning of the kill chain before persistence.
- Identify log sources of the highest scoring techniques.
- Examine log sources to see what gaps are present.
- Search for tags of the techniques in MISP to produce a weighted feeds.
- Feeds can be enriched by Cortex analyzers.
- Export enriched feeds to SIEM.
- Automate by a cURL command.


Defense APT Groups
score gradient
0
70


Apt33
Deep Panda
Magic Hound
menuPass
Threat Group-3390
Aviation
render: Aviation
Aviation
filters
stages: act
platforms: Windows, Linux, macOS
score gradient
5
30
Initial Access
11 items
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
34 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Source
Space after Filename
Third-party Software
Trap
Trusted Developer Utilities
User Execution
Windows Management Instrumentation
Windows Remote Management
XSL Script Processing
Persistence
62 items
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
Emond
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Kernel Modules and Extensions
Launch Agent
Launch Daemon
Launchctl
LC_LOAD_DYLIB Addition
Local Job Scheduling
Login Item
Logon Scripts
LSASS Driver
Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup
Path Interception
Plist Modification
Port Knocking
Port Monitors
PowerShell Profile
Rc.common
Re-opened Applications
Redundant Access
Registry Run Keys / Startup Folder
Scheduled Task
Screensaver
Security Support Provider
Server Software Component
Service Registry Permissions Weakness
Setuid and Setgid
Shortcut Modification
SIP and Trust Provider Hijacking
Startup Items
System Firmware
Systemd Service
Time Providers
Trap
Valid Accounts
Web Shell
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL
Privilege Escalation
32 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Parent PID Spoofing
Path Interception
Plist Modification
Port Monitors
PowerShell Profile
Process Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
SID-History Injection
Startup Items
Sudo
Sudo Caching
Valid Accounts
Web Shell
Defense Evasion
69 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Connection Proxy
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File and Directory Permissions Modification
File Deletion
File System Logical Offsets
Gatekeeper Bypass
Group Policy Modification
Hidden Files and Directories
Hidden Users
Hidden Window
HISTCONTROL
Image File Execution Options Injection
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Indirect Command Execution
Install Root Certificate
InstallUtil
Launchctl
LC_MAIN Hijacking
Masquerading
Modify Registry
Mshta
Network Share Connection Removal
NTFS File Attributes
Obfuscated Files or Information
Parent PID Spoofing
Plist Modification
Port Knocking
Process Doppelgänging
Process Hollowing
Process Injection
Redundant Access
Regsvcs/Regasm
Regsvr32
Rootkit
Rundll32
Scripting
Signed Binary Proxy Execution
Signed Script Proxy Execution
SIP and Trust Provider Hijacking
Software Packing
Space after Filename
Template Injection
Timestomp
Trusted Developer Utilities
Valid Accounts
Virtualization/Sandbox Evasion
Credential Access
21 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Steal Web Session Cookie
Two-Factor Authentication Interception
Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark 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
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion
Lateral Movement
18 items
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Command And Control
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service
Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer
Impact
16 items
Account Access Removal
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
System Shutdown/Reboot
Transmitted Data Manipulation

about

Retail

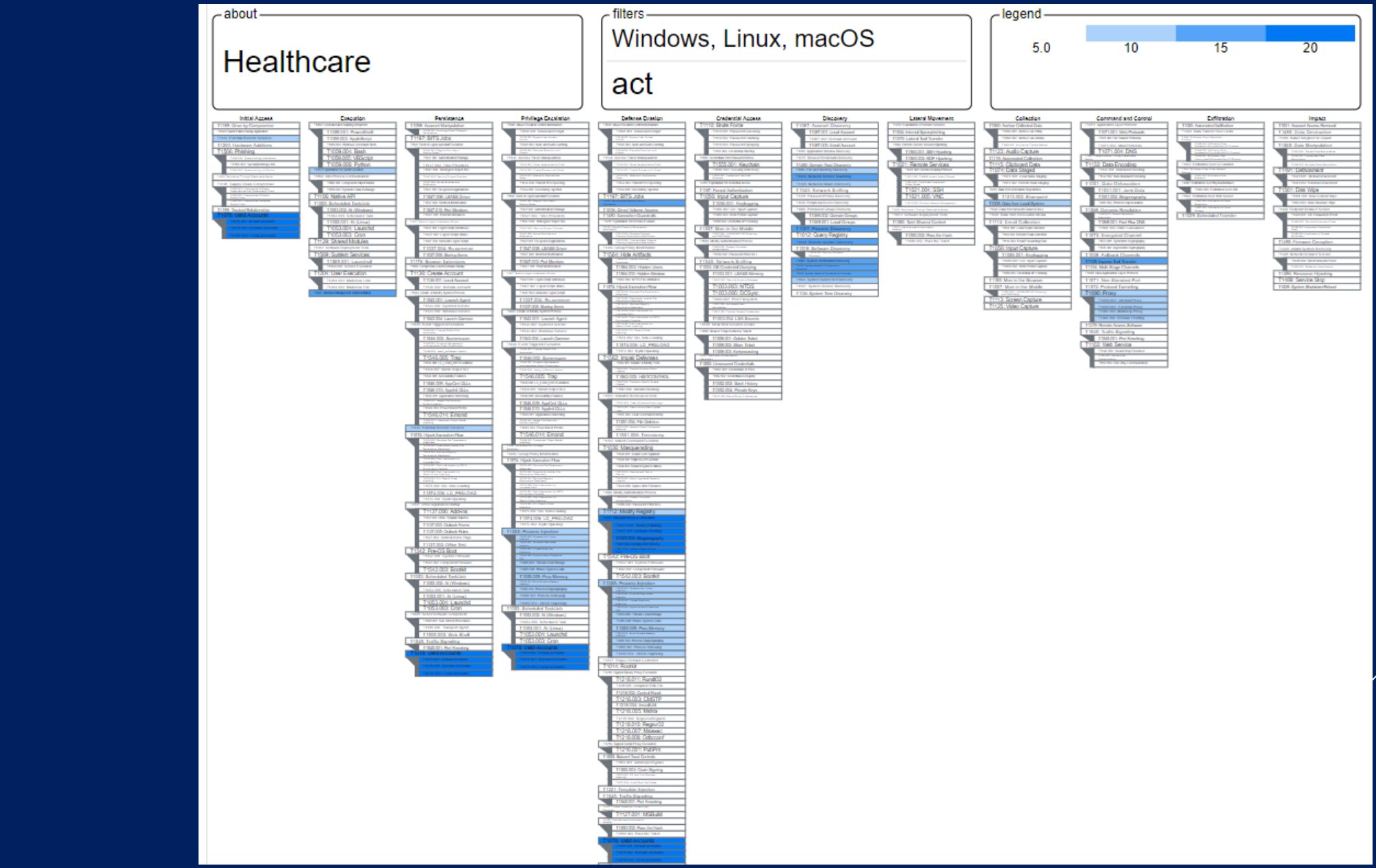
filters

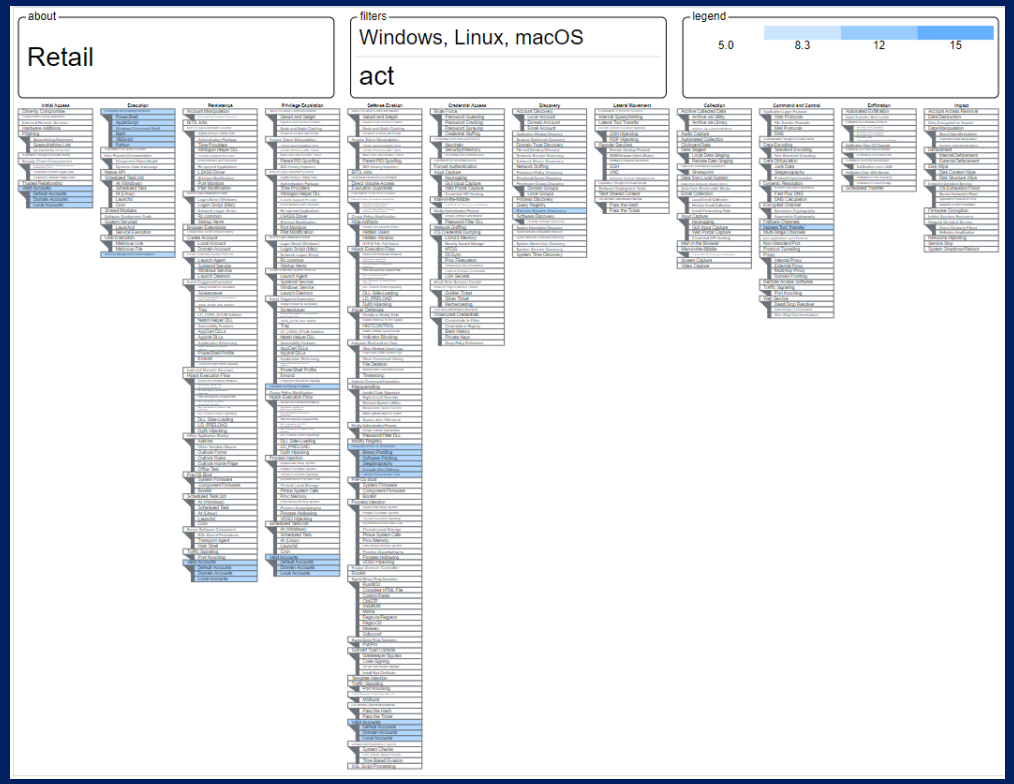
Windows, Linux, macOS

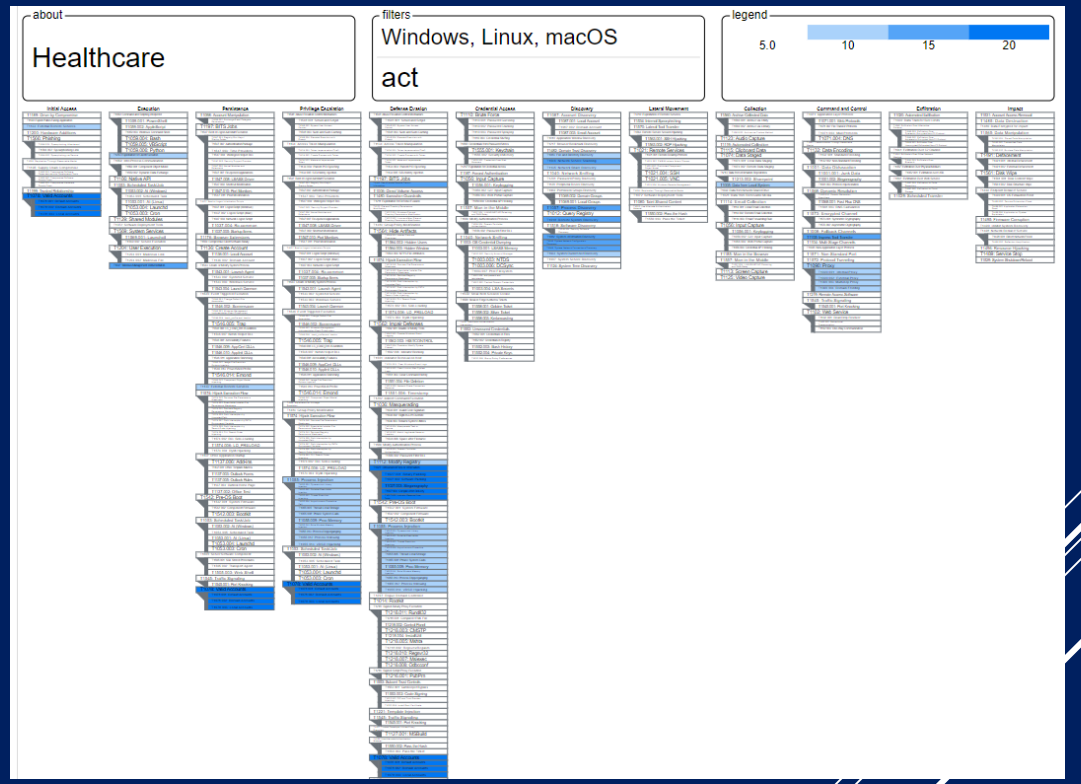
act

legend

5.0 8.3 12 15


about
Healthcare
filters
Windows, Linux, macOS
act
legend
5.0
10
15
20
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact


about
Retail
filters
Windows, Linux, macOS
act
legend
5.0
8.3
12
15


about
Healthcare
filters
Windows, Linux, macOS
act
legend
5.0
10
15
20

Valid Accounts

Sub-techniques (4)

ID	Name
T1078.001	Default Accounts
T1078.002	Domain Accounts
T1078.003	Local Accounts
T1078.004	Cloud Accounts

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise. [1]

Mitigations

Mitigation	Description
Application Developer Guidance	Ensure that applications do not store sensitive data or credentials insecurely. (e.g. plaintext credentials in code, published credentials in repositories, or credentials in public cloud storage).
Password Policies	Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. [4] When possible, applications that use SSH keys should be updated periodically and properly secured.
Privileged Account Management	Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. [1] [2] These audits should also include if default accounts have been enabled, or if new local accounts are created that have not be authorized. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. [3]

Detection

Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services. [37] Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

Perform regular audits of domain and local system accounts to detect accounts that may have been created by an adversary for persistence. Checks on these accounts could also include whether default accounts such as Guest have been activated. These audits should also include checks on any appliances and applications for default credentials or SSH keys, and if any are discovered, they should be updated immediately.

What is a threat intelligence platform?

•A threat intelligence platform or TIP facilitates the collection, aggregation and correlation of threat data from multiple sources in real time.

•This helps analysts identify threats that are relevant to their organization.

- Traditionally sharing threat data is a manual process: through email, spreadsheets or a ticketing portal.

- This approach does not scale.

- However, the use of APIs allow for the automation of actions without direct user involvement.

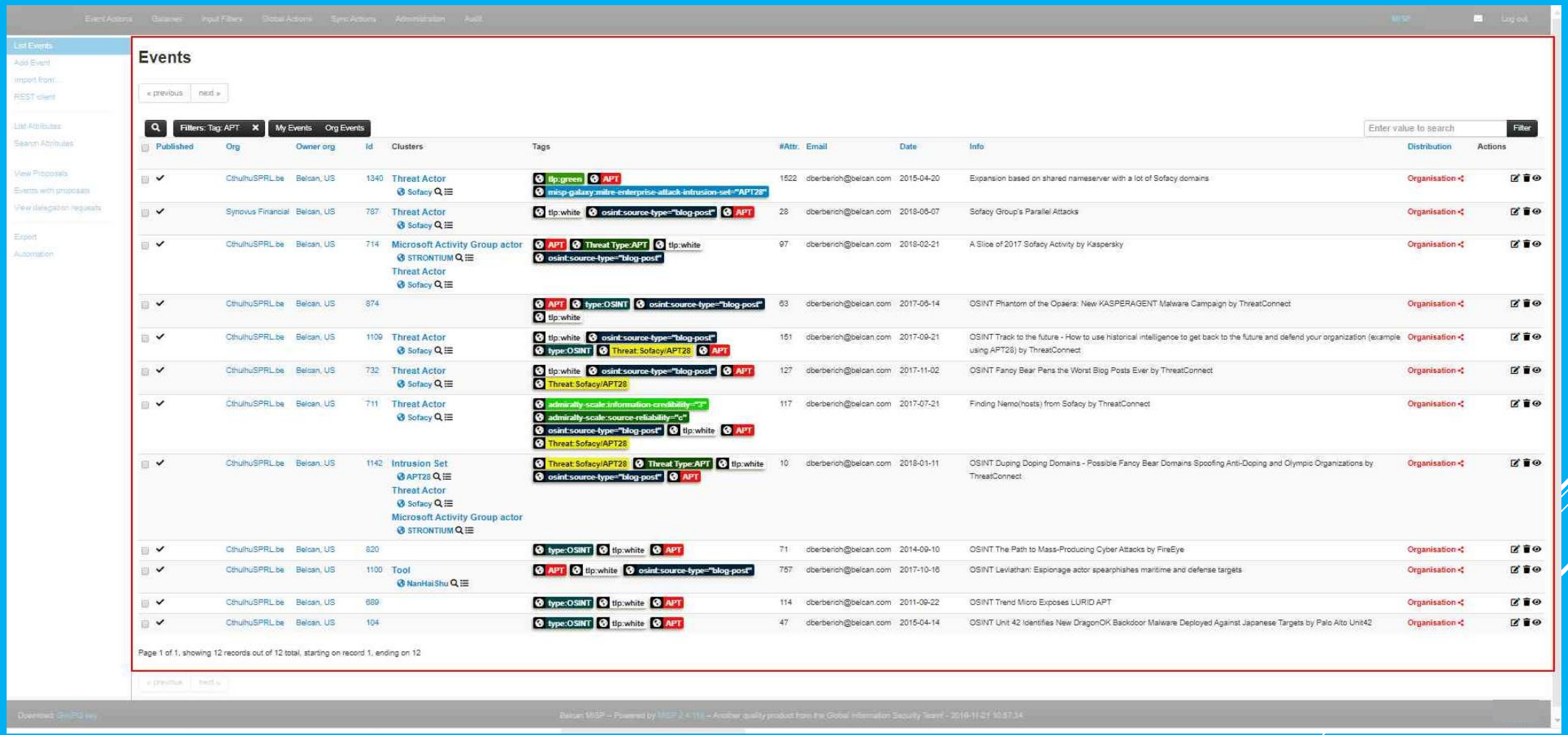
- The TIP makes it easier to share threat intelligence with other stakeholders.

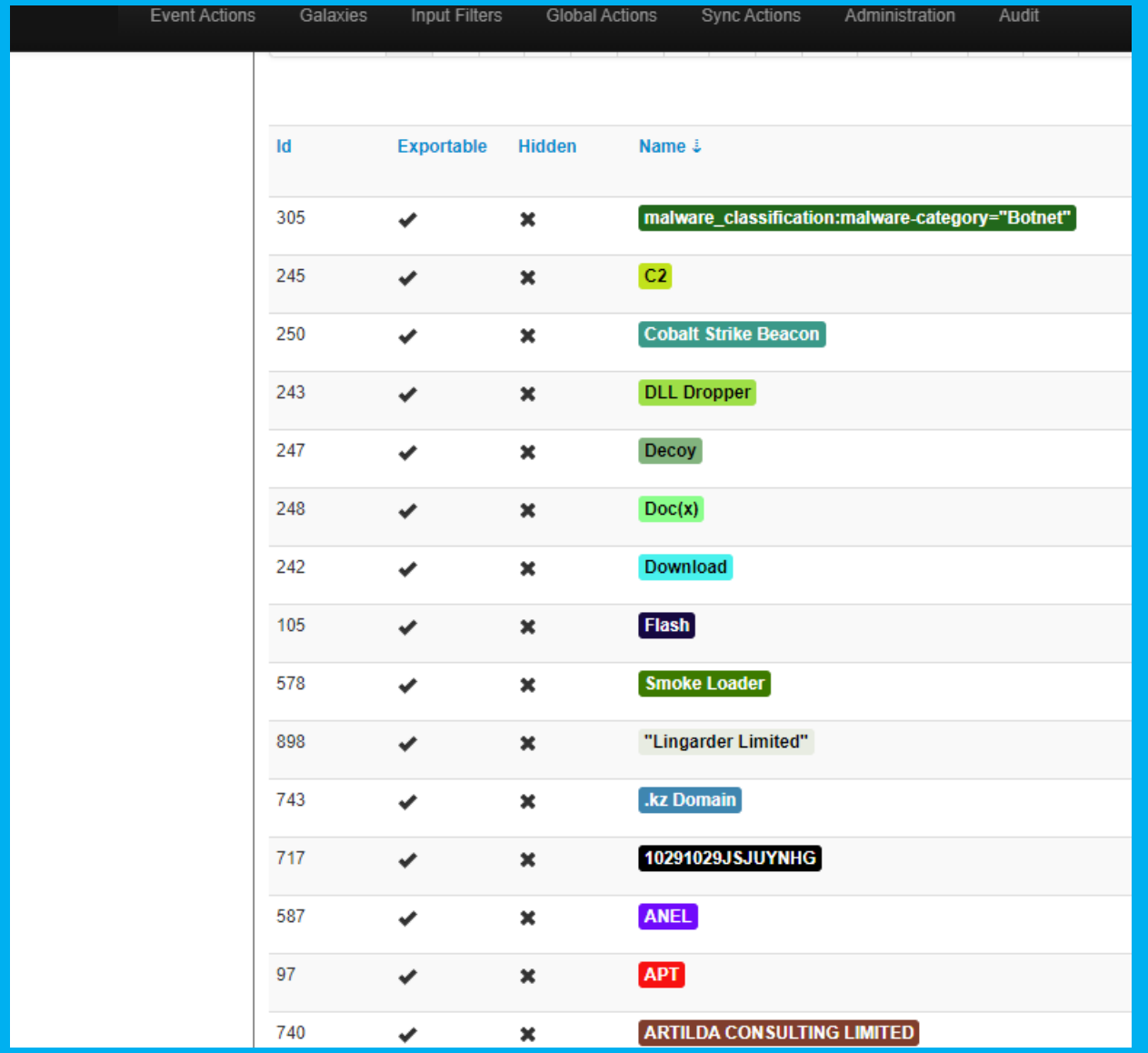
- The data that is collected can be used to enrich and contextualize other alerts in your security stack.

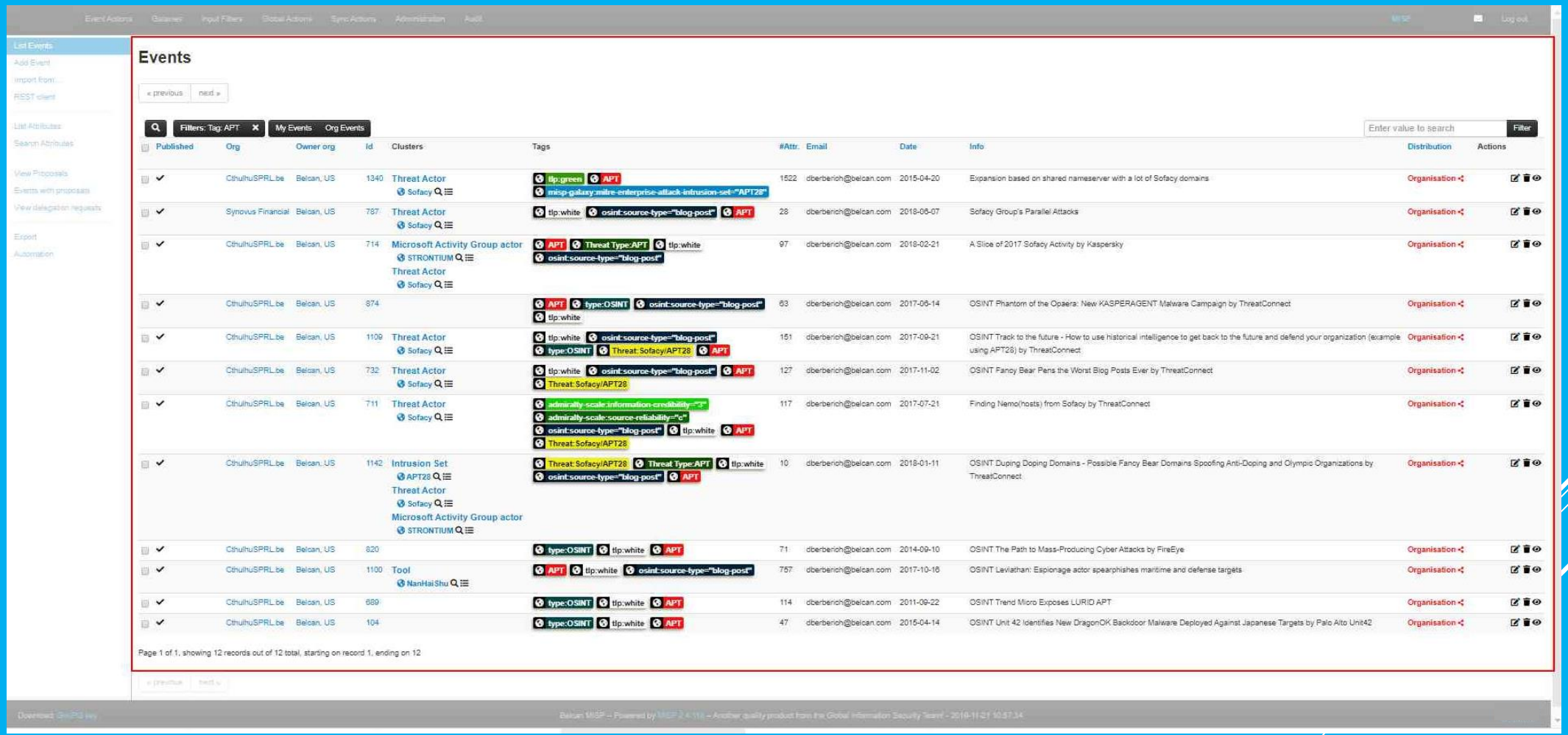
- TIPs use APIs to generate Whois information, reverse IP lookup, name servers, domain blocklists, etc.

- The TIP automatically analyzes the content of threat indicators to identify a threat actor's tactics, techniques and procedures (TTPs).

https://github.com/MISP/MISP


Events
Filters: Tag: APT
My Events
Org Events
Enter value to search
Filter
Published
Org
Owner org
Id
Clusters
Tags
#Attr.
Email
Date
Info
Distribution
Actions
CthulhuSPRL.be
Belcan, US
1340
Threat Actor
Sofacy
tlp:green
APT
misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28"
1522
dberberich@belcan.com
2015-04-20
Expansion based on shared nameserver with a lot of Sofacy domains
Organisation
Synovus Financial
787
tlp:white
osint:source-type="blog-post"
28
2018-06-07
Sofacy Group's Parallel Attacks
714
Microsoft Activity Group actor
STRONTIUM
Threat Actor
Threat Type:APT
97
2018-02-21
A Slice of 2017 Sofacy Activity by Kaspersky
874
type:OSINT
63
2017-06-14
OSINT Phantom of the Opaera: New KASPERAGENT Malware Campaign by ThreatConnect
1109
151
2017-09-21
OSINT Track to the future - How to use historical intelligence to get back to the future and defend your organization (example using APT28) by ThreatConnect
732
Threat: Sofacy/APT28
127
2017-11-02
OSINT Fancy Bear Pens the Worst Blog Posts Ever by ThreatConnect
711
admiralty-scale:information-credibility="3"
admiralty-scale:source-reliability="c"
117
2017-07-21
Finding Nemo(hosts) from Sofacy by ThreatConnect
1142
Intrusion Set
APT28
10
2018-01-11
OSINT Duping Doping Domains - Possible Fancy Bear Domains Spoofing Anti-Doping and Olympic Organizations by ThreatConnect
820
71
2014-09-10
OSINT The Path to Mass-Producing Cyber Attacks by FireEye
1100
Tool
NanHaiShu
757
2017-10-16
OSINT Leviathan: Espionage actor spearphishes maritime and defense targets
689
114
2011-09-22
OSINT Trend Micro Exposes LURID APT
104
47
2015-04-14
OSINT Unit 42 Identifies New DragonOK Backdoor Malware Deployed Against Japanese Targets by Palo Alto Unit42
Page 1 of 1, showing 12 records out of 12 total, starting on record 1, ending on 12


Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
Id
Exportable
Hidden
Name
305
malware_classification:malware-category="Botnet"
245
C2
250
Cobalt Strike Beacon
243
DLL Dropper
247
Decoy
248
Doc(x)
242
Download
105
Flash
578
Smoke Loader
898
"Lingarder Limited"
743
.kz Domain
717
10291029JSJUYNHG
587
ANEL
97
APT
740
ARTILDA CONSULTING LIMITED


Events
« previous
next »
Filters: Tag: APT
My Events
Org Events
Enter value to search
Filter
Published
Org
Owner org
Id
Clusters
Tags
#Attr.
Email
Date
Info
Distribution
Actions
CthulhuSPRL.be Belcan, US 1340 Threat Actor Sofacy tlp:green APT misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28" 1522 dberberich@belcan.com 2015-04-20 Expansion based on shared nameserver with a lot of Sofacy domains Organisation
Synovus Financial Belcan, US 787 Threat Actor Sofacy tlp:white osint:source-type="blog-post" APT 28 dberberich@belcan.com 2018-06-07 Sofacy Group's Parallel Attacks Organisation
CthulhuSPRL.be Belcan, US 714 Microsoft Activity Group actor STRONTIUM Threat Actor Sofacy APT Threat Type:APT tlp:white osint:source-type="blog-post" 97 dberberich@belcan.com 2018-02-21 A Slice of 2017 Sofacy Activity by Kaspersky Organisation
CthulhuSPRL.be Belcan, US 874 APT type:OSINT osint:source-type="blog-post" tlp:white 63 dberberich@belcan.com 2017-06-14 OSINT Phantom of the Opaera: New KASPERAGENT Malware Campaign by ThreatConnect Organisation
CthulhuSPRL.be Belcan, US 1109 Threat Actor Sofacy tlp:white osint:source-type="blog-post" type:OSINT Threat:Sofacy/APT28 APT 151 dberberich@belcan.com 2017-09-21 OSINT Track to the future - How to use historical intelligence to get back to the future and defend your organization (example using APT28) by ThreatConnect Organisation
CthulhuSPRL.be Belcan, US 732 Threat Actor Sofacy tlp:white osint:source-type="blog-post" APT Threat:Sofacy/APT28 127 dberberich@belcan.com 2017-11-02 OSINT Fancy Bear Pens the Worst Blog Posts Ever by ThreatConnect Organisation
CthulhuSPRL.be Belcan, US 711 Threat Actor Sofacy admiralty-scale:information-credibility="2" admiralty-scale:source-reliability="c" osint:source-type="blog-post" tlp:white APT Threat:Sofacy/APT28 117 dberberich@belcan.com 2017-07-21 Finding Nemo(hosts) from Sofacy by ThreatConnect Organisation
CthulhuSPRL.be Belcan, US 1142 Intrusion Set APT28 Threat Actor Sofacy Microsoft Activity Group actor STRONTIUM Threat:Sofacy/APT28 Threat Type:APT tlp:white osint:source-type="blog-post" APT 10 dberberich@belcan.com 2018-01-11 OSINT Duping Doping Domains - Possible Fancy Bear Domains Spoofing Anti-Doping and Olympic Organizations by ThreatConnect Organisation
CthulhuSPRL.be Belcan, US 820 type:OSINT tlp:white APT 71 dberberich@belcan.com 2014-09-10 OSINT The Path to Mass-Producing Cyber Attacks by FireEye Organisation
CthulhuSPRL.be Belcan, US 1100 Tool NanHaiShu APT tlp:white osint:source-type="blog-post" 757 dberberich@belcan.com 2017-10-16 OSINT Leviathan: Espionage actor spearphishes maritime and defense targets Organisation
CthulhuSPRL.be Belcan, US 689 type:OSINT tlp:white APT 114 dberberich@belcan.com 2011-09-22 OSINT Trend Micro Exposes LURID APT Organisation
CthulhuSPRL.be Belcan, US 104 type:OSINT tlp:white APT 47 dberberich@belcan.com 2015-04-14 OSINT Unit 42 Identifies New DragonOK Backdoor Malware Deployed Against Japanese Targets by Palo Alto Unit42 Organisation
Page 1 of 1, showing 12 records out of 12 total, starting on record 1, ending on 12

CthulhuSPRL.be

Expansion based on shared nameserver with a lot of Sofacy domains

Event ID	1340
UUID	5534e822-0e78-4eea-aea8-4ac3950d210b +
Creator org	CthulhuSPRL.be
Owner org	Belcan, US
Email	dberberich@belcan.com
Tags	tlp:green x APT x misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28" x + +
Date	2015-04-20
Threat Level	Medium
Analysis	Completed
Distribution	Your organisation only
Info	Expansion based on shared nameserver with a lot of Sofacy domains
Published	Yes (2019-10-31 16:33:30)
#Attributes	1522 (202 Objects)
First recorded change	2017-02-22 05:04:34
Last change	2018-07-25 07:29:31
Modification map	
Sightings	0 (0) - restricted to own organisation only.

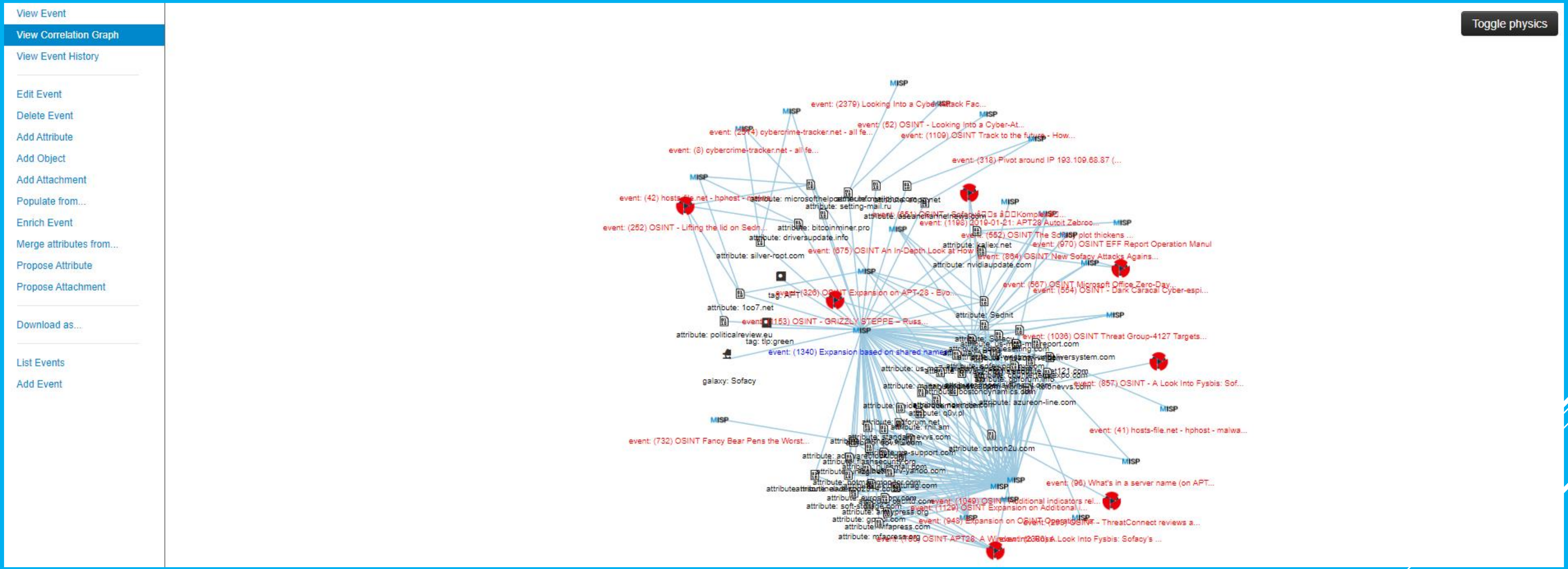
− Pivots − Galaxy + Event graph + Correlation graph + ATT&CK matrix − Attributes − Discussion

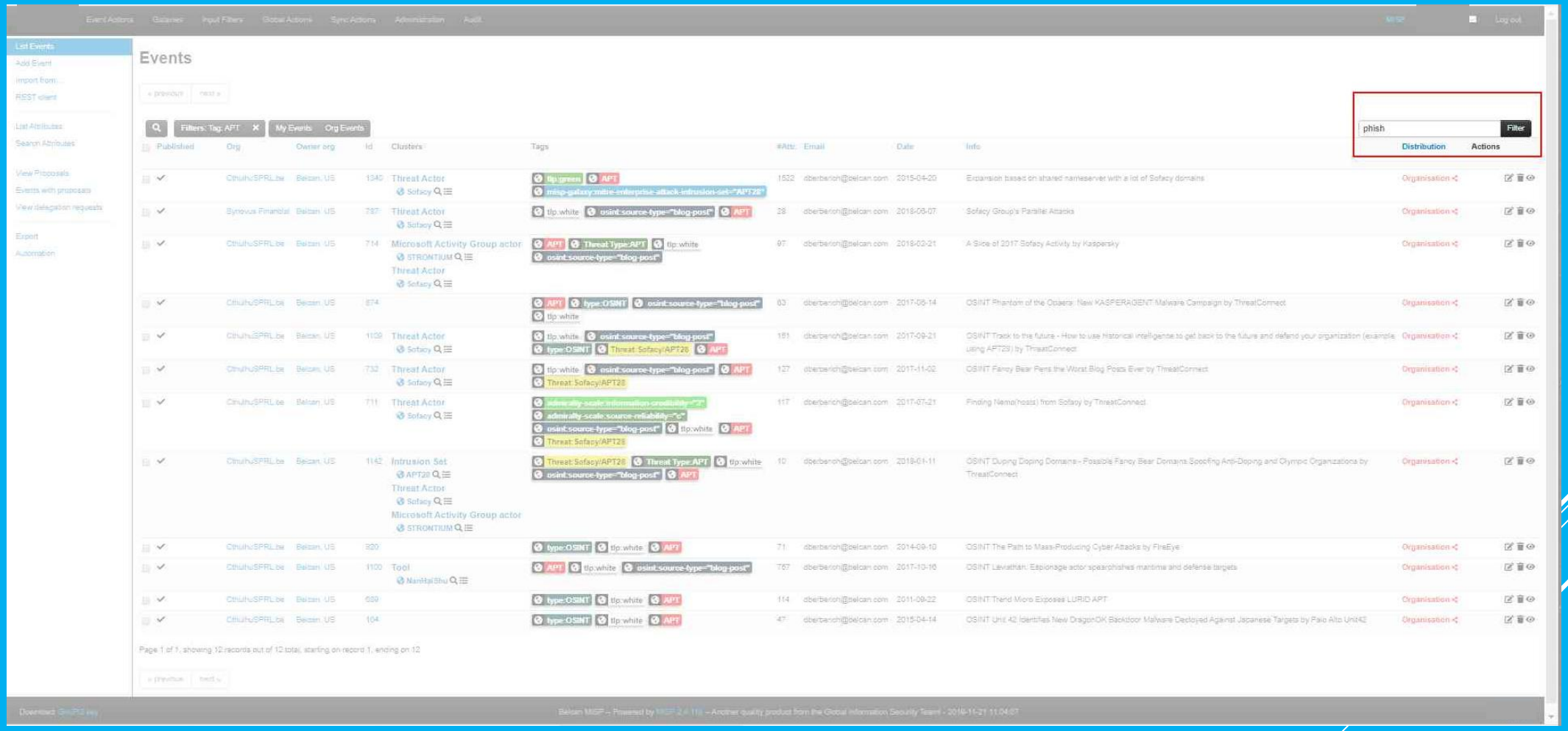
1340: Expans...

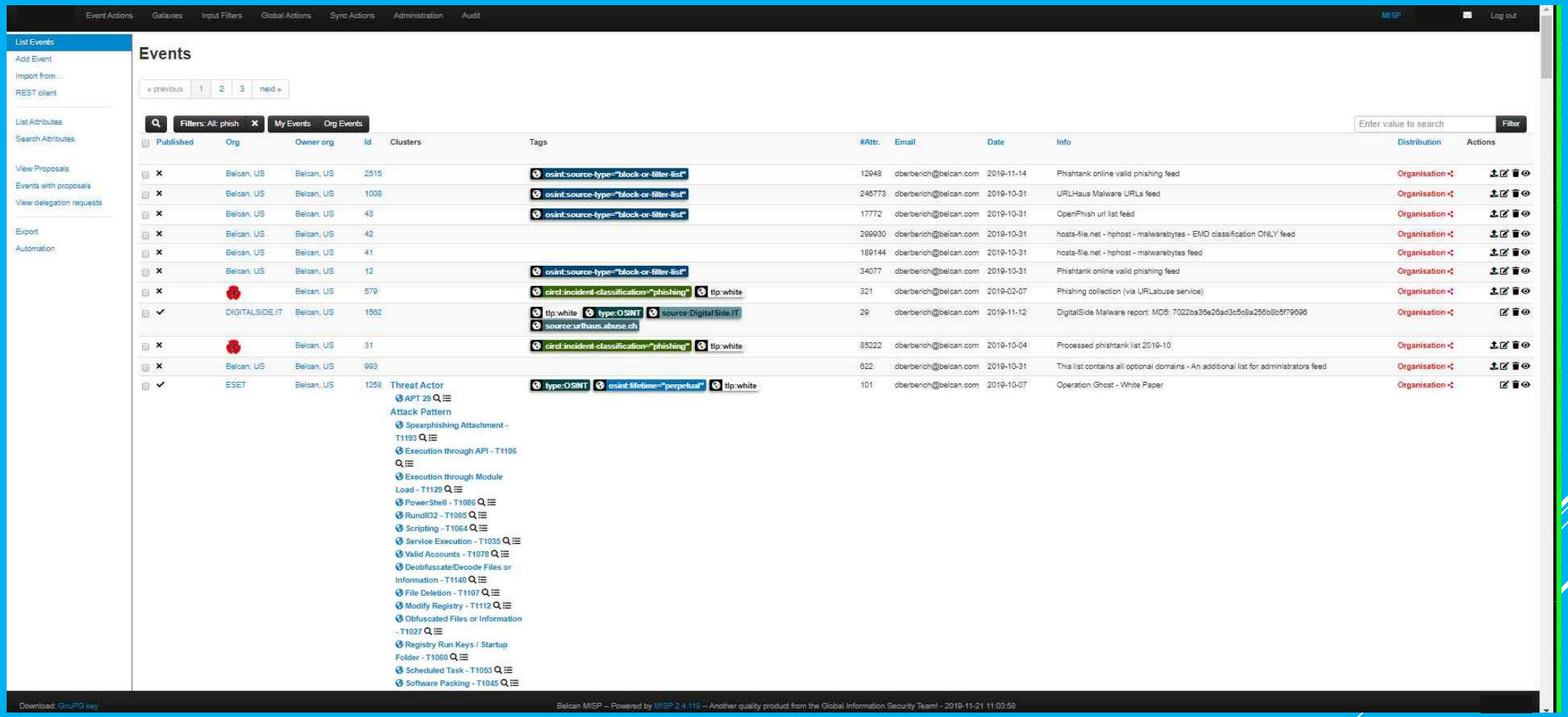
Related Events

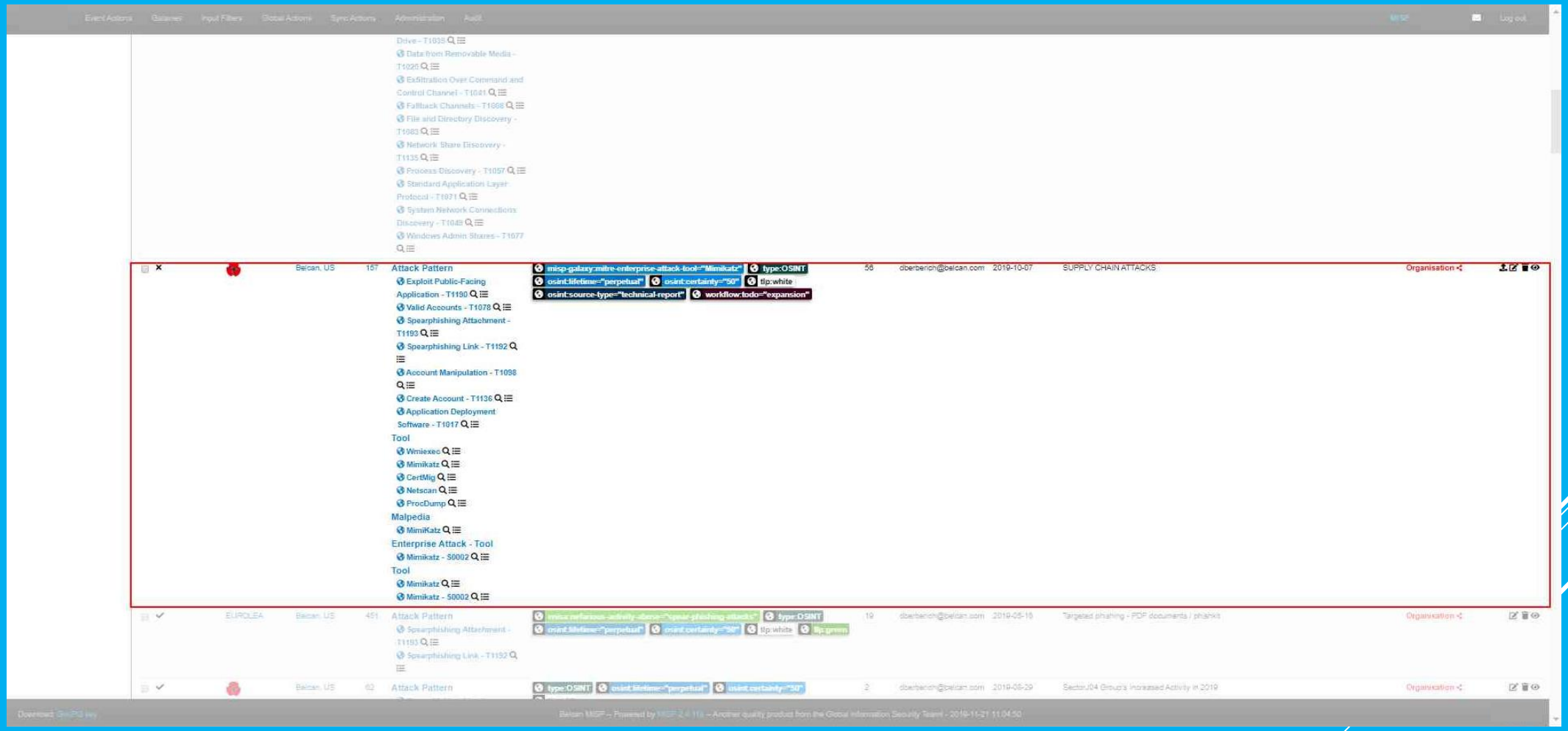
- Bel... US cybercrime-tracker.net - all feed 2019-11-14 2
- Bel... US cybercrime-tracker.net - all feed 2019-10-31 2
- Bel... US hosts-file.net - hphost - malwarebytes feed 2019-10-31 1
- Bel... US hosts-file.net - hphost - malwarebytes - EMD classification ONLY feed 2019-10-31 3
- VK-Intel 2019-01-21: APT28 Autoit Zebrocy Progression 2019-01-21 1
- OSINT - Dark Caracal Cyber-espionage at a Global Scale 2018-01-25 2
- Cth... OSINT Fancy Bear Pens the Worst Blog Posts Ever by ThreatConnect 2017-11-02 1
- Cth... OSINT Track to the future - How to use historical intelligence to get back to the... 2017-09-21 1
- OSINT - GRIZZLY STEPPE – Russian Malicious Cyber Activity 2016-12-29 1
- OSINT - Lifting the lid on Sednit: A closer look at the software it uses 2016-10-25 4

Show (19 more)


View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Populate from...
Enrich Event
Merge attributes from...
Propose Attribute
Propose Attachment
Download as...
List Events
Add Event
Toggle physics
event: (8) cybercrime-tracker.net - all fe...
event: (318) Pivot around IP 193.109.68.87 (...
event: (252) OSINT - Lifting the lid on Sedn...
event: (970) OSINT EFF Report Operation Manul
attribute: driversupdate.info
attribute: silver-root.com
attribute: nvidiaupdate.com
attribute: 1oo7.net
attribute: Sednit
attribute: politicalreview.eu
tag: tlp:green
event: (1340) Expansion based on shared names
event: (1036) OSINT Threat Group-4127 Targets...
galaxy: Sofacy
attribute: azureon-line.com
event: (41) hosts-file.net - hphost - malwa...
event: (732) OSINT Fancy Bear Pens the Worst...
attribute: carbon2u.com
event: (96) What's in a server name (on APT...


Events
phish
Filter
Distribution
Actions


Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Log out
List Events
Add Event
Import from...
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation
Events
« previous
1
2
3
next »
Filters: All: phish
My Events
Org Events
Enter value to search
Filter
Published
Org
Owner org
Id
Clusters
Tags
#Attr.
Email
Date
Info
Distribution
Actions
Belcan, US
Belcan, US
2515
osint:source-type="block-or-filter-list"
12948
dberberich@belcan.com
2019-11-14
Phishtank online valid phishing feed
Organisation
Belcan, US
Belcan, US
1008
osint:source-type="block-or-filter-list"
246773
dberberich@belcan.com
2019-10-31
URLHaus Malware URLs feed
Organisation
Belcan, US
Belcan, US
43
osint:source-type="block-or-filter-list"
17772
dberberich@belcan.com
2019-10-31
OpenPhish url list feed
Organisation
Belcan, US
Belcan, US
42
299930
dberberich@belcan.com
2019-10-31
hosts-file.net - hphost - malwarebytes - EMD classification ONLY feed
Organisation
Belcan, US
Belcan, US
41
189144
dberberich@belcan.com
2019-10-31
hosts-file.net - hphost - malwarebytes feed
Organisation
Belcan, US
Belcan, US
12
osint:source-type="block-or-filter-list"
34077
dberberich@belcan.com
2019-10-31
Phishtank online valid phishing feed
Organisation
Belcan, US
579
circl:incident-classification="phishing"
tlp:white
321
dberberich@belcan.com
2019-02-07
Phishing collection (via URLabuse service)
Organisation
DIGITALSIDE.IT
Belcan, US
1562
tlp:white
type:OSINT
source:Digital Side.IT
source:urlhaus.abuse.ch
29
dberberich@belcan.com
2019-11-12
DigitalSide Malware report: MD5: 7022ba36e26ad3c5c8a256b8b5f79696
Organisation
Belcan, US
31
circl:incident-classification="phishing"
tlp:white
85222
dberberich@belcan.com
2019-10-04
Processed phishtank list 2019-10
Organisation
Belcan, US
Belcan, US
993
622
dberberich@belcan.com
2019-10-31
This list contains all optional domains - An additional list for administrators feed
Organisation
ESET
Belcan, US
1258
Threat Actor
APT 29
Attack Pattern
Spearphishing Attachment - T1193
Execution through API - T1106
Execution through Module Load - T1129
PowerShell - T1086
Rundll32 - T1085
Scripting - T1064
Service Execution - T1035
Valid Accounts - T1078
Deobfuscate/Decode Files or Information - T1140
File Deletion - T1107
Modify Registry - T1112
Obfuscated Files or Information - T1027
Registry Run Keys / Startup Folder - T1060
Scheduled Task - T1053
Software Packing - T1045
type:OSINT
osint:lifetime="perpetual"
tlp:white
101
dberberich@belcan.com
2019-10-07
Operation Ghost - White Paper
Organisation
Download: GnuPG key
Belcan MISP -- Powered by MISP 2.4.118 -- Another quality product from the Global Information Security Team! - 2019-11-21 11:03:58


Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
Log out
Drive - T1035
Data from Removable Media - T1025
Exfiltration Over Command and Control Channel - T1041
Fallback Channels - T1008
File and Directory Discovery - T1083
Network Share Discovery - T1135
Process Discovery - T1057
Standard Application Layer Protocol - T1071
System Network Connections Discovery - T1049
Windows Admin Shares - T1077
Belcan, US
157
Attack Pattern
Exploit Public-Facing Application - T1190
Valid Accounts - T1078
Spearphishing Attachment - T1193
Spearphishing Link - T1192
Account Manipulation - T1098
Create Account - T1136
Application Deployment Software - T1017
Tool
Wmiexec
Mimikatz
CertMig
Netscan
ProcDump
Malpedia
MimiKatz
Enterprise Attack - Tool
Mimikatz - S0002
Tool
Mimikatz
Mimikatz - S0002
misp-galaxy:mitre-enterprise-attack-tool="Mimikatz"
type:OSINT
osint:lifetime="perpetual"
osint:certainty="50"
tlp:white
osint:source-type="technical-report"
workflow:todo="expansion"
58
dberbenich@belcan.com
2019-10-07
SUPPLY CHAIN ATTACKS
Organisation
EUROLEA
Belcan, US
451
Attack Pattern
Spearphishing Attachment - T1193
Spearphishing Link - T1192
type:OSINT
tlp:white
19
dberbenich@belcan.com
2019-05-16
Targeted phishing - PDF documents / phishkit
Organisation
Belcan, US
62
Attack Pattern
type:OSINT
2
dberbenich@belcan.com
2019-05-29
Sector.j04 Group's Increased Activity in 2019
Organisation

TLP:WHITE

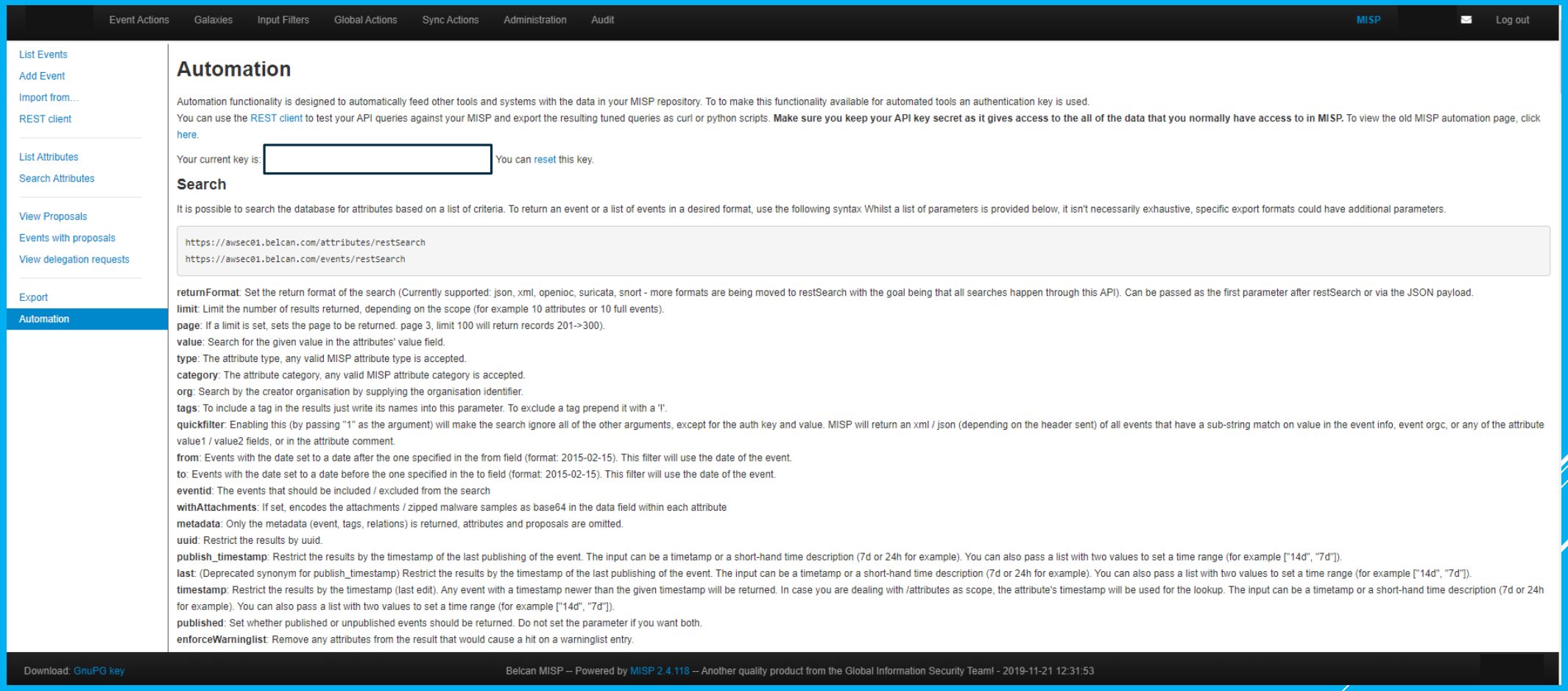
SUPPLY CHAIN ATTACKS

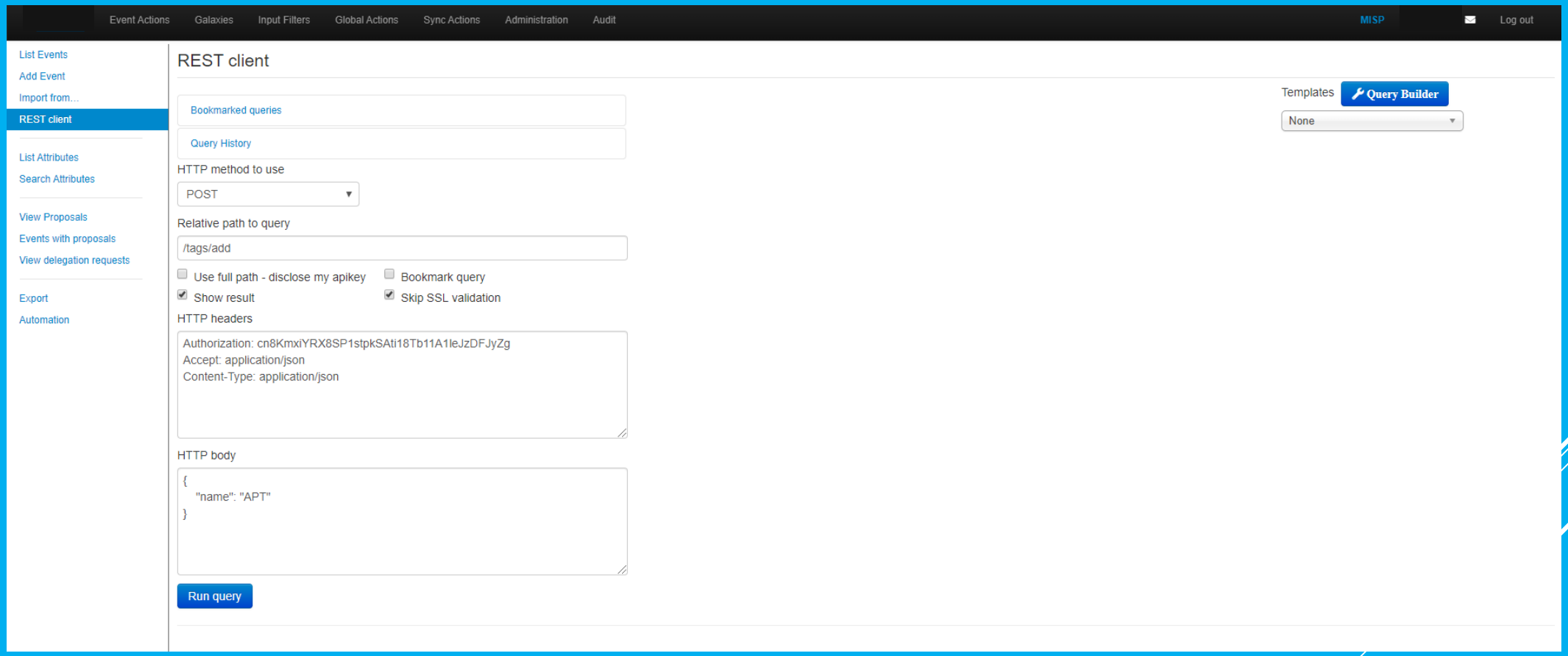
THREATS TARGETING SERVICE PROVIDERS AND DESIGN OFFICES

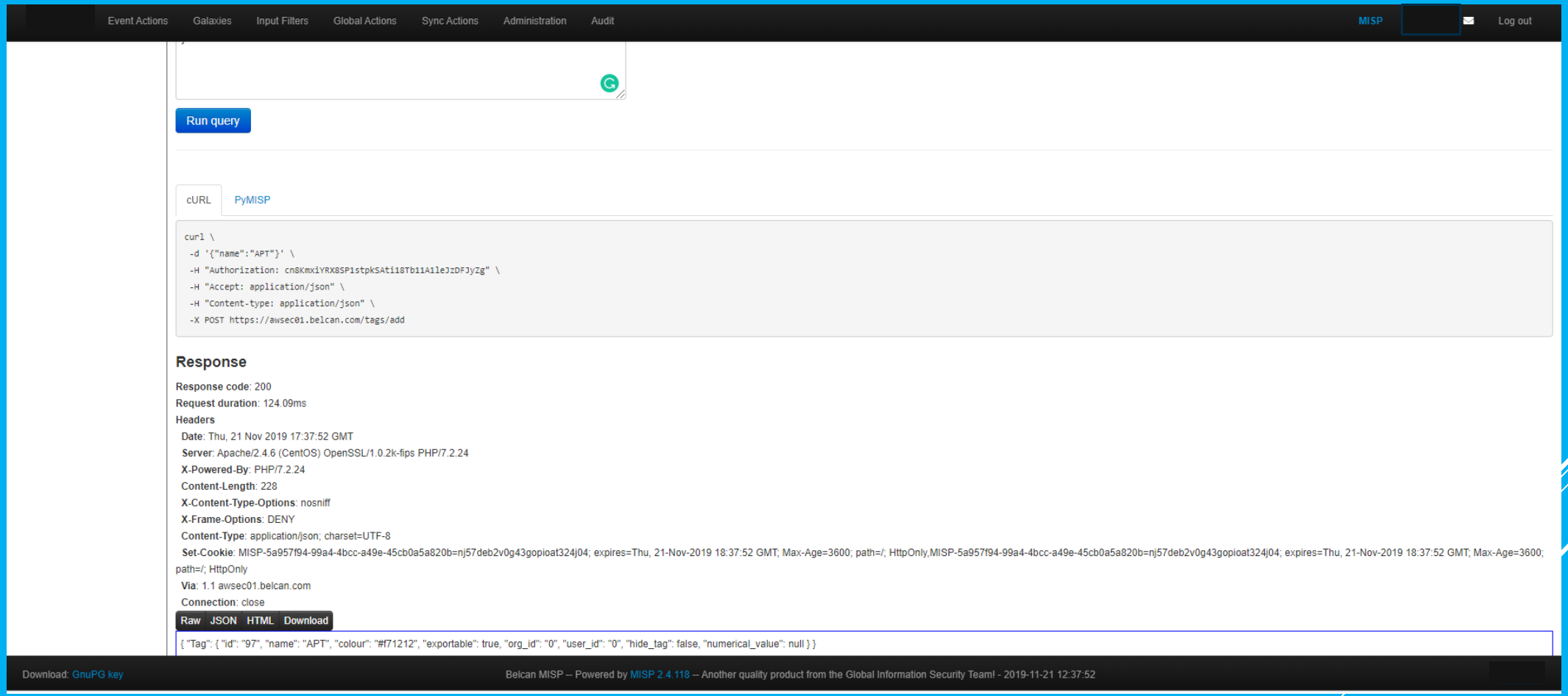
Version 1.0

October 7th 2019

TLP:WHITE

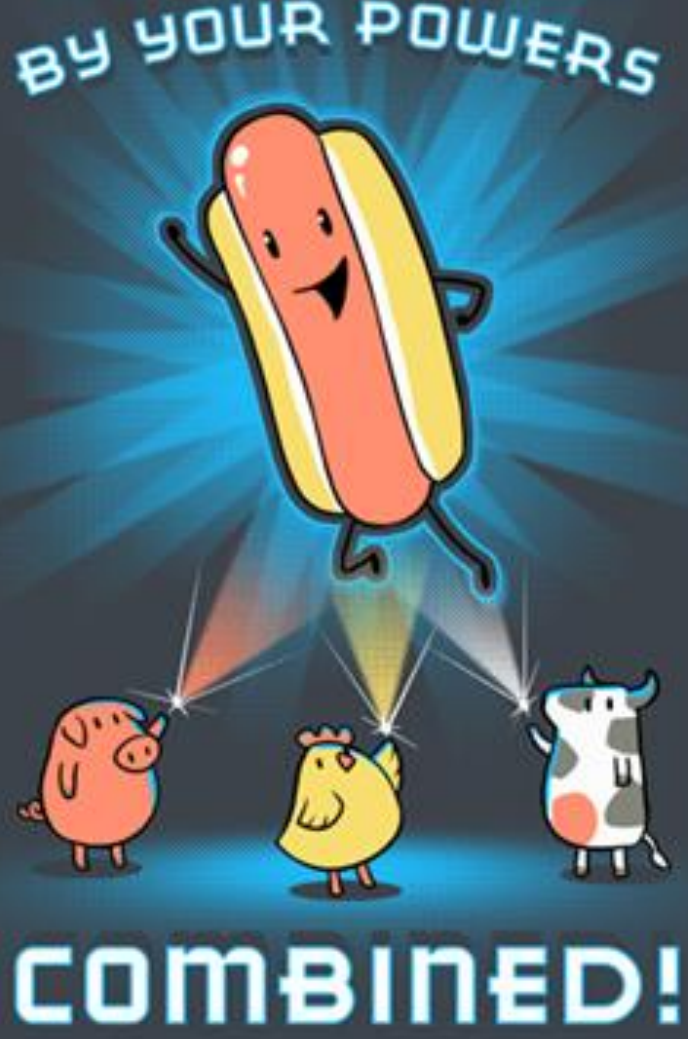

Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Log out
List Events
Add Event
Import from...
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation
Automation
Automation functionality is designed to automatically feed other tools and systems with the data in your MISP repository. To to make this functionality available for automated tools an authentication key is used.
You can use the REST client to test your API queries against your MISP and export the resulting tuned queries as curl or python scripts. Make sure you keep your API key secret as it gives access to the all of the data that you normally have access to in MISP. To view the old MISP automation page, click here.
Your current key is:
You can reset this key.
Search
It is possible to search the database for attributes based on a list of criteria. To return an event or a list of events in a desired format, use the following syntax Whilst a list of parameters is provided below, it isn't necessarily exhaustive, specific export formats could have additional parameters.
https://awsec01.belcan.com/attributes/restSearch
https://awsec01.belcan.com/events/restSearch
returnFormat: Set the return format of the search (Currently supported: json, xml, openioc, suricata, snort - more formats are being moved to restSearch with the goal being that all searches happen through this API). Can be passed as the first parameter after restSearch or via the JSON payload.
limit: Limit the number of results returned, depending on the scope (for example 10 attributes or 10 full events).
page: If a limit is set, sets the page to be returned. page 3, limit 100 will return records 201->300).
value: Search for the given value in the attributes' value field.
type: The attribute type, any valid MISP attribute type is accepted.
category: The attribute category, any valid MISP attribute category is accepted.
org: Search by the creator organisation by supplying the organisation identifier.
tags: To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'.
quickfilter: Enabling this (by passing "1" as the argument) will make the search ignore all of the other arguments, except for the auth key and value. MISP will return an xml / json (depending on the header sent) of all events that have a sub-string match on value in the event info, event orgc, or any of the attribute value1 / value2 fields, or in the attribute comment.
from: Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.
to: Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.
eventid: The events that should be included / excluded from the search
withAttachments: If set, encodes the attachments / zipped malware samples as base64 in the data field within each attribute
metadata: Only the metadata (event, tags, relations) is returned, attributes and proposals are omitted.
uuid: Restrict the results by uuid.
publish_timestamp: Restrict the results by the timestamp of the last publishing of the event. The input can be a timetamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
last: (Deprecated synonym for publish_timestamp) Restrict the results by the timestamp of the last publishing of the event. The input can be a timetamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
timestamp: Restrict the results by the timestamp (last edit). Any event with a timestamp newer than the given timestamp will be returned. In case you are dealing with /attributes as scope, the attribute's timestamp will be used for the lookup. The input can be a timetamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
published: Set whether published or unpublished events should be returned. Do not set the parameter if you want both.
enforceWarninglist: Remove any attributes from the result that would cause a hit on a warninglist entry.
Download: GnuPG key
Belcan MISP -- Powered by MISP 2.4.118 -- Another quality product from the Global Information Security Team! - 2019-11-21 12:31:53

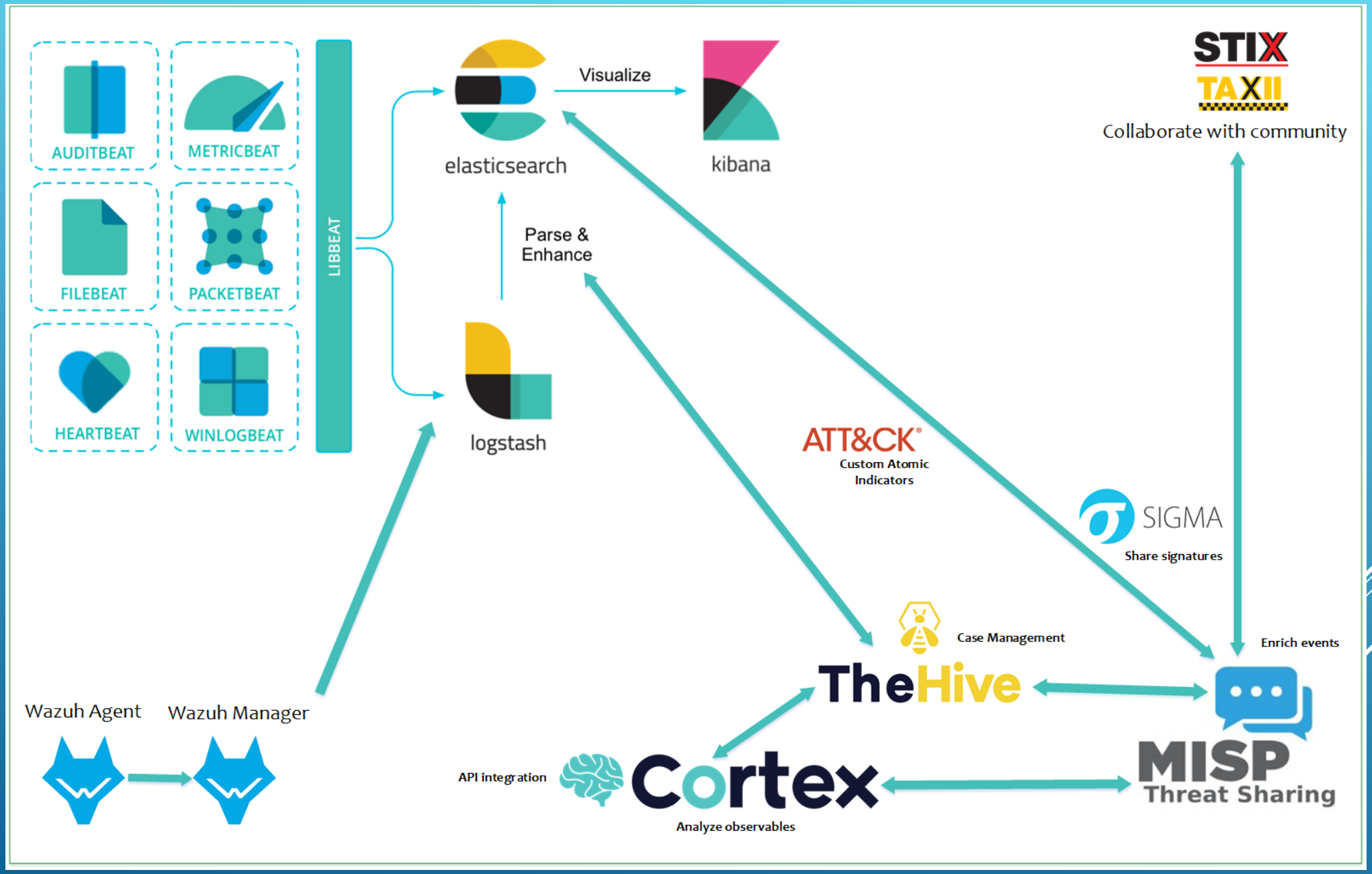

Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Log out
List Events
Add Event
Import from...
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation
REST client
Bookmarked queries
Query History
Templates
Query Builder
None
HTTP method to use
POST
Relative path to query
/tags/add
Use full path - disclose my apikey
Bookmark query
Show result
Skip SSL validation
HTTP headers
Authorization: cn8KmxiYRX8SP1stpkSAti18Tb11A1leJzDFJyZg
Accept: application/json
Content-Type: application/json
HTTP body
{
"name": "APT"
}
Run query


Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Log out
Run query
cURL
PyMISP
curl \
-d '{"name":"APT"}' \
-H "Authorization: cn8KmxiYRX8SP1stpkSAti18Tb11A1leJzDFJyZg" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://awsec01.belcan.com/tags/add
Response
Response code: 200
Request duration: 124.09ms
Headers
Date: Thu, 21 Nov 2019 17:37:52 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.24
X-Powered-By: PHP/7.2.24
Content-Length: 228
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: application/json; charset=UTF-8
Set-Cookie: MISP-5a957f94-99a4-4bcc-a49e-45cb0a5a820b=nj57deb2v0g43gopioat324j04; expires=Thu, 21-Nov-2019 18:37:52 GMT; Max-Age=3600; path=/; HttpOnly,MISP-5a957f94-99a4-4bcc-a49e-45cb0a5a820b=nj57deb2v0g43gopioat324j04; expires=Thu, 21-Nov-2019 18:37:52 GMT; Max-Age=3600; path=/; HttpOnly
Via: 1.1 awsec01.belcan.com
Connection: close
Raw
JSON
HTML
Download
{ "Tag": { "id": "97", "name": "APT", "colour": "#f71212", "exportable": true, "org_id": "0", "user_id": "0", "hide_tag": false, "numerical_value": null } }
Download: GnuPG key
Belcan MISP -- Powered by MISP 2.4.118 -- Another quality product from the Global Information Security Team! - 2019-11-21 12:37:52

mofa.mozjlla.comacer.moafee.comdel.moafee.comjnt.moafee.compcg.moafee.comsslc.moafee.comat.moafee.comlw.moafee.comks.moafee.comoa.moafee.comxxpp.moafee.comhp.moafee.comgumm.mozjlla.commsn.moafee.comphi.crabdance.com98.126.91.66113.66.248.60113.65.22.148113.65.41.28113.65.43.42113.66.12.112113.68.108.62113.68.110.239113.68.111.111113.68.168.73113.68.171.67ndbssh.com58.217.168.205222.95.171.17858.217.169.95www.ghostale.comwww.ycbackap.comasp.skyppee.comfacebook.skyppee.compop.skyppee.commail.skyppee.commil.skyppee.comweb.pktmedia.combbs.pktmedia.com nethostnet.comhostsvcnet.cometcrem.netmovieultimate.comnewfilmts.comfastdataexchange.orgliveweatherview.comanalyticsbar.organalyticstest.netlifeofmentalservice.commeteost.comrighttopregnantpower.comkiteim.orgadobe-flash-updates.orggeneralsecurityscan.comglobalresearching.orglvueton.comaudiwheel.comonline-reggi.comfsportal.netnetcorpscanprotect.commvband.netmvtband.netviters.orgtreepastwillingmoment.comsendmevideo.orgsatellitedeluxpanorama.comppcodecs.comencoder-info.tkwmdmediacodecs.compostlkwarn.comshcserv.comversiontask.comwebcdelivery.commiropc.orgsecurityprotectingcorp.comuniquecorpind.comappexsrv.netadobeupgradeflash.comhttps://google.com.account-password.ga/security/signinoptions/passwordgoogle.com.account-password.ga80.255.12.231accounts.google.com.securitymail.gqsecuritymail.gq95.153.32.52smtprelayhost.comuzbekistan-mfa.comluminate-yahoo.comcc-yahoo-inc.orgopecmember.comcdncloudflare.com45645647.com57567547454.comciscohelpcenter.comintelsupportcenter.comintelsupportcenter.nethighcomission.orgautoupdater.orgsecurityupdatereport.commozilla-

How can this be scaled?


BY YOUR POWERS
COMBINED!


AUDITBEAT
METRICBEAT
FILEBEAT
PACKETBEAT
HEARTBEAT
WINLOGBEAT
LIBBEAT
elasticsearch
Visualize
kibana
STIX
TAXII
Collaborate with community
Parse &
Enhance
logstash
ATT&CK
Custom Atomic
Indicators
SIGMA
Share signatures
Case Management
Enrich events
TheHive
Wazuh Agent
Wazuh Manager
API integration
Cortex
Analyze observables
MISP
Threat Sharing

Synergetic Intelligence Automation

A *fusion* of anomaly based detection, shared intelligence feeds and counterintelligence derived from deception technology.

Crust

Environmental Intelligence connects the other intelligences together.

Sauce

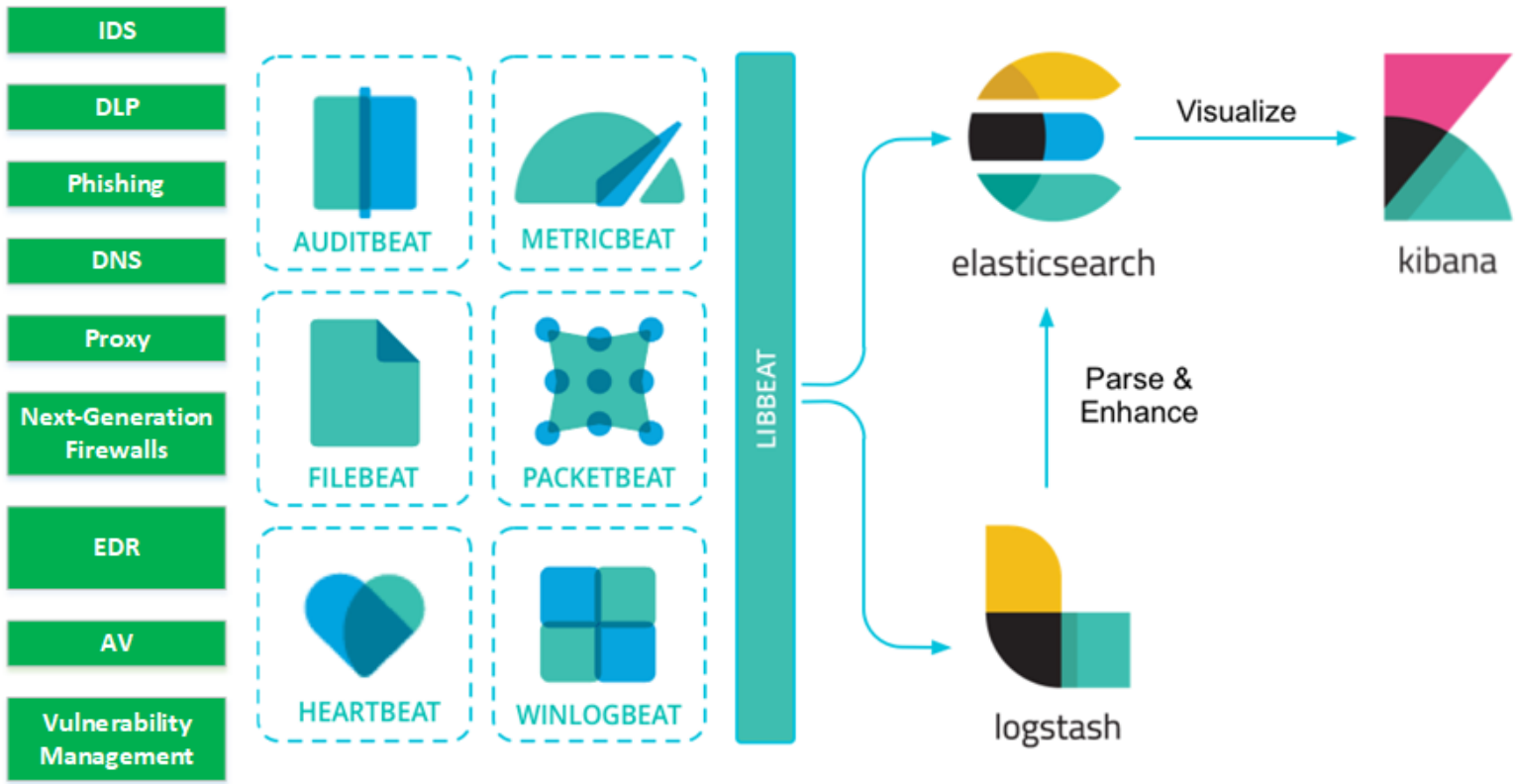
Curated intelligence feeds (global and community) enrich detection..

Toppings

Proactive Intelligence gives a targeted and actionable defense recipe.

Environmental Intelligence

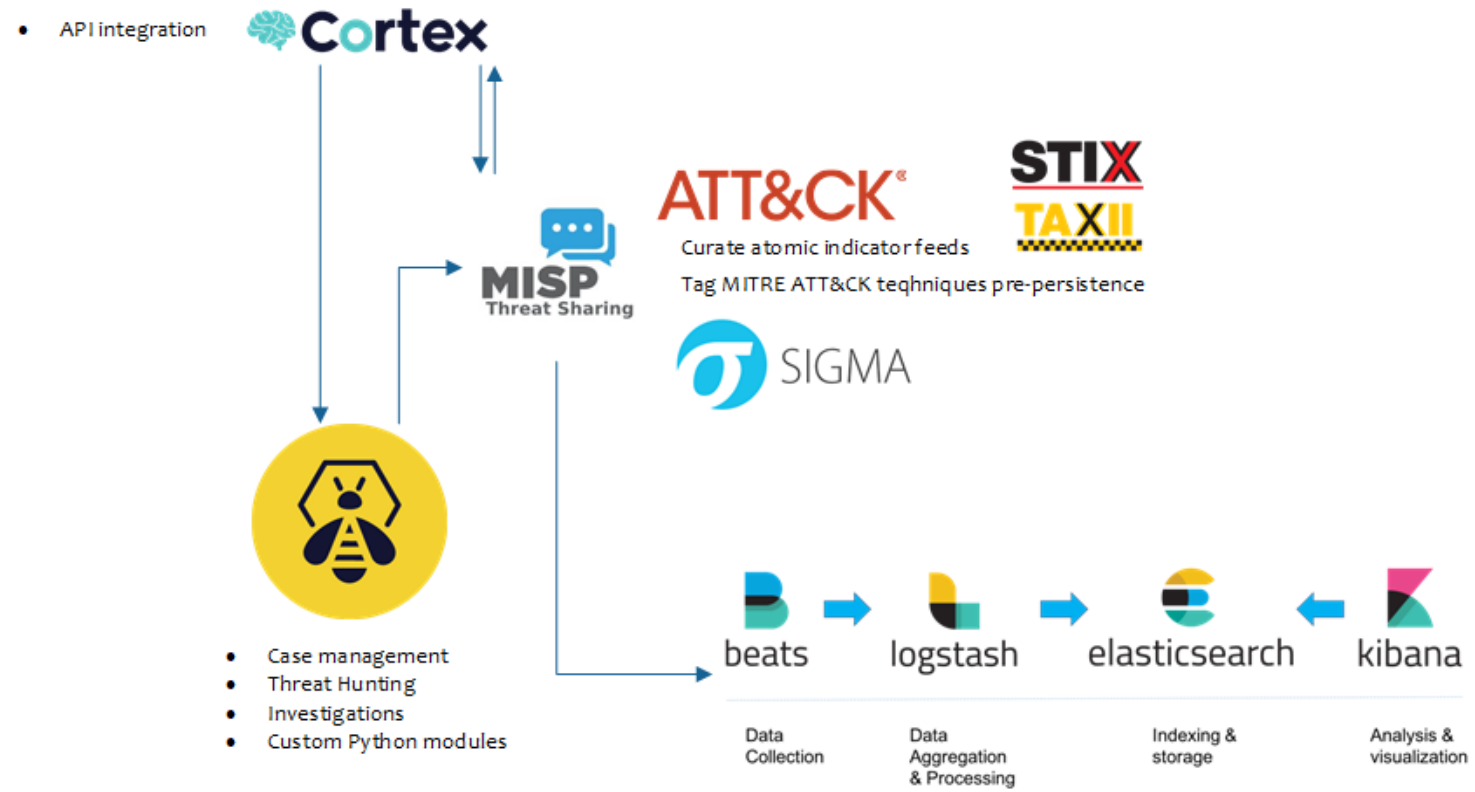
High value log sources are chosen for their visibility and relevance to use cases.
Machine learning is leveraged to produce alerts based on anomalous behavior.



- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation and Response (SOAR)

Curated Intelligence

This community shared intelligence is collected and curated to enrich the security stack with leading indicators of compromise to give added context to attacks.



Proactive Intelligence

This counterintelligence is real-time. Active defense makes attacks more difficult for attackers.

Select your token

Web bug / URL token

Alert when a URL is visited

DNS token

Alert when a hostname is requested

Unique email address

Alert when an email is sent to a unique address

Custom Image Web bug

Alert when an image you uploaded is viewed

Microsoft Word Document

Get alerted when a document is opened in Microsoft Word

Acrobat Reader PDF Document

Get alerted when a PDF document is opened in Acrobat Reader

Windows Folder

Be notified when a Windows Folder is browsed in Windows Explorer

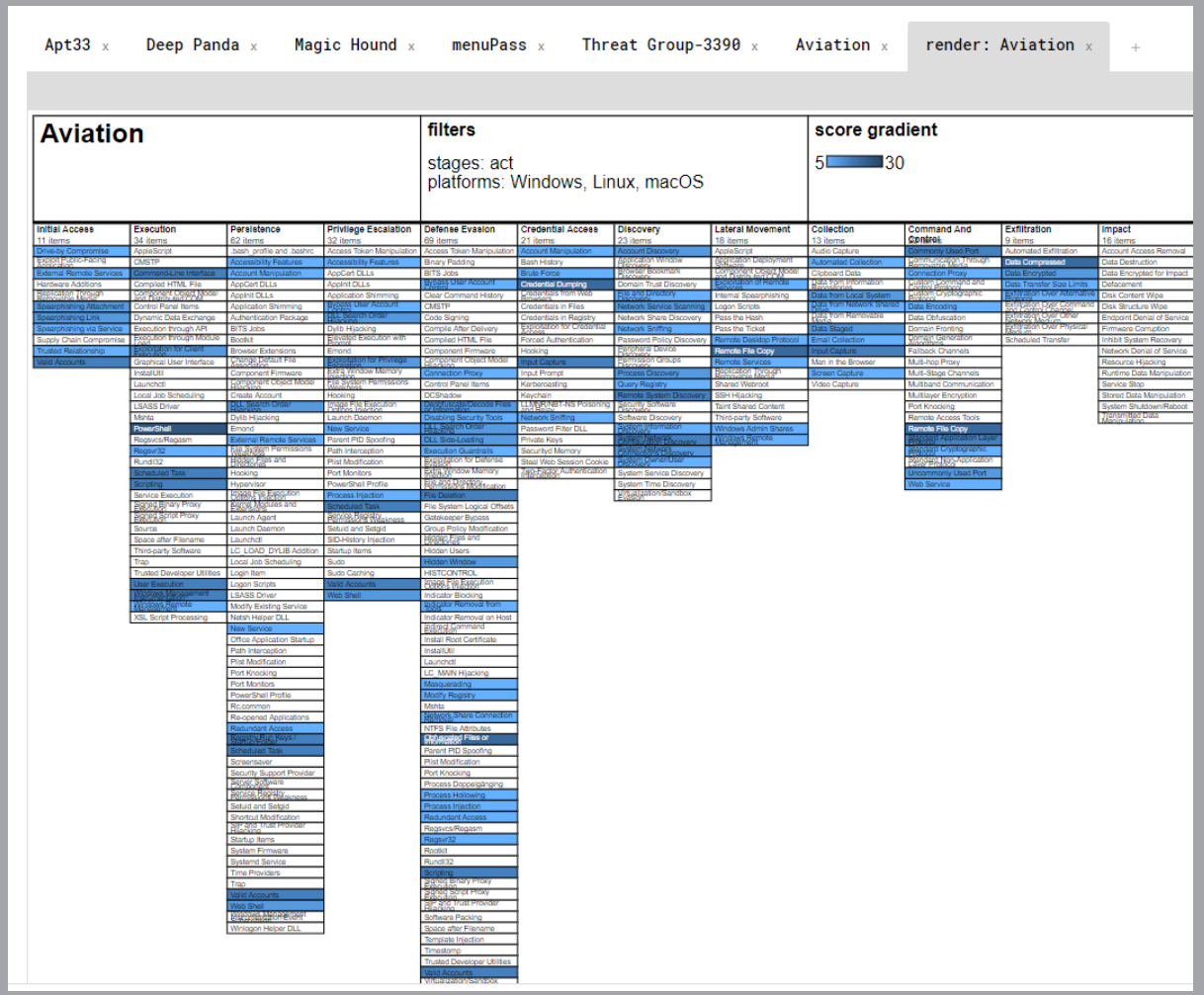
When it matters.

https://github.com/MISP/MISP

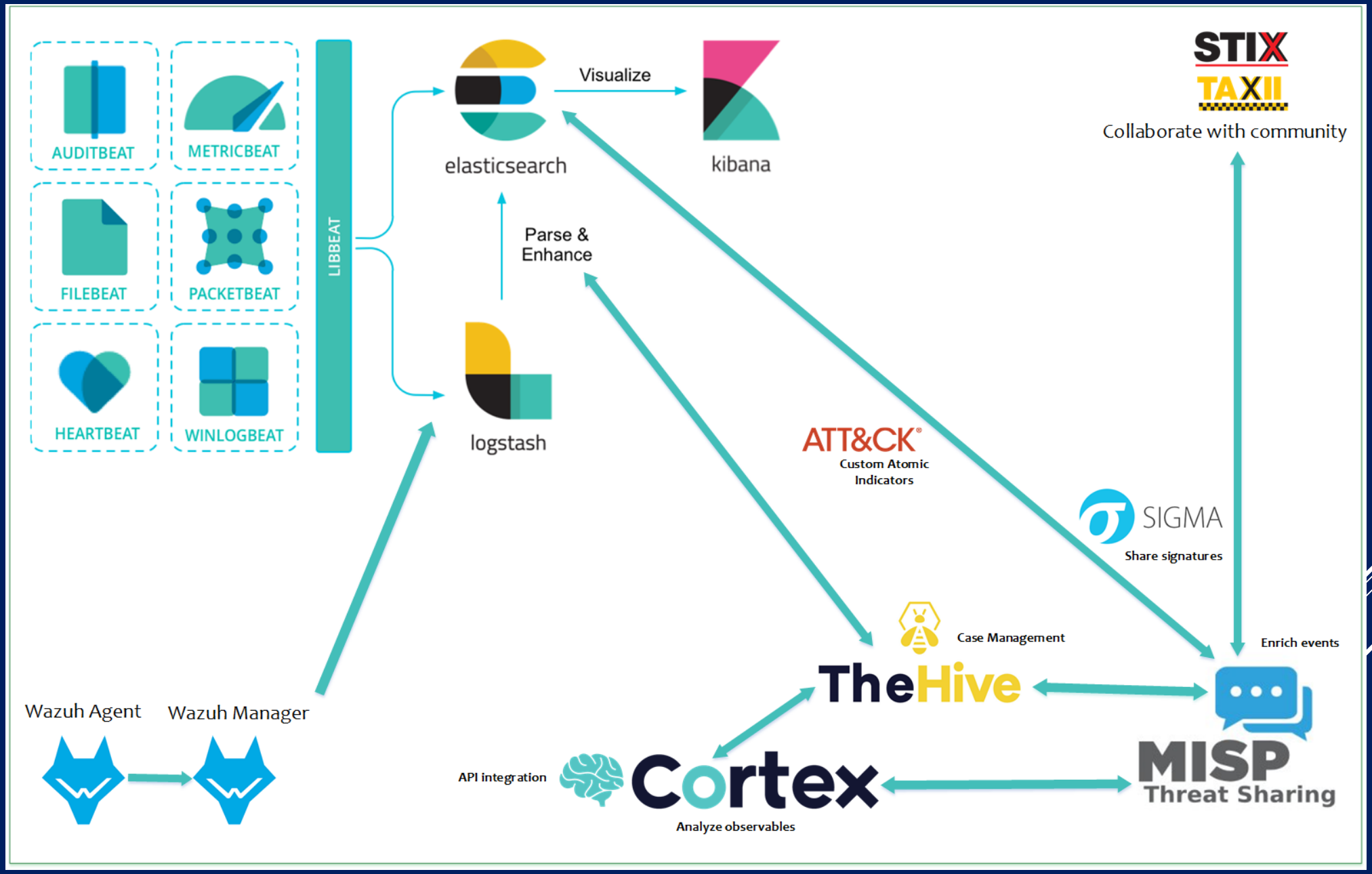
	A	B	C	D	E	F	G	H	I	J
1	Groups	*Financial*	*Defense*	*NGO*	*Healthcare*	*Education*	*Aviation*	*Energy*	*Retail*	*Technology*
2	admin@338									
3	APT12									
4	APT17									
5	APT18									
6	APT19									
7	APT33									
8	APT38									
9	APT41									
10	Carbanak									
11	Charming Kitten									
12	Cobalt Group									
13	Deep Panda									
14	Dragonfly									
15	Dragonfly 2.0									
16	Elderwood									
17	FIN4									
18	FIN5									
19	FIN6									
20	FIN7									
21	FIN8									
22	Gallmaker									
23	GCMAN									
24	Honeybee									
25	Leviathan									
26	Magic Hound									
27	menuPass									
28	MuddyWater									
29	OilRig									
30	Orangeworm									
31	Silence									
32	Silver Terrier									
33	Stone Pencil									
34	Threat Group-3390									
35	Thrip									
36	Tropic Trooper									
37	Turla									

https://attack.mitre.org/beta/groups/

ATT&CK®


Apt33
Deep Panda
Magic Hound
menuPass
Threat Group-3390
Aviation
render: Aviation
Aviation
filters
stages: act
platforms: Windows, Linux, macOS
score gradient
5
30
Initial Access
11 items
Execution
34 items
Persistence
62 items
Privilege Escalation
32 items
Defense Evasion
69 items
Credential Access
21 items
Discovery
23 items
Lateral Movement
18 items
Collection
13 items
Command And Control
Exfiltration
9 items
Impact
16 items

- Research APT groups that target your industry.
- Make a heat map using MITRE ATT&CK tools to see which techniques were most likely.
- A single color may work better than stop light protocol colors.
- Assign scores to each APT group and layer them.
- Place focus on the beginning of the kill chain before persistence.
- Identify log sources of the highest scoring techniques.
- Examine log sources to see what gaps are present.
- Search for tags of the techniques in MISP to produce a weighted feeds.
- Feeds can be enriched by Cortex analyzers.
- Export enriched feeds to SIEM.
- Automate by a cURL command.
- Python can also be integrated.


AUDITBEAT
METRICBEAT
FILEBEAT
PACKETBEAT
HEARTBEAT
WINLOGBEAT
LIBBEAT
elasticsearch
Visualize
kibana
logstash
Parse &
Enhance
STIX
TAXII
Collaborate with community
ATT&CK
Custom Atomic
Indicators
SIGMA
Share signatures
Case Management
Enrich events
TheHive
Wazuh Agent
Wazuh Manager
API integration
Cortex
Analyze observables
MISP
Threat Sharing

https://github.com/S1lv3rL10n/Talks

Keith Chapman | CTIA
Senior Security Analyst
Belcan LLC
kchapman@belcan.com