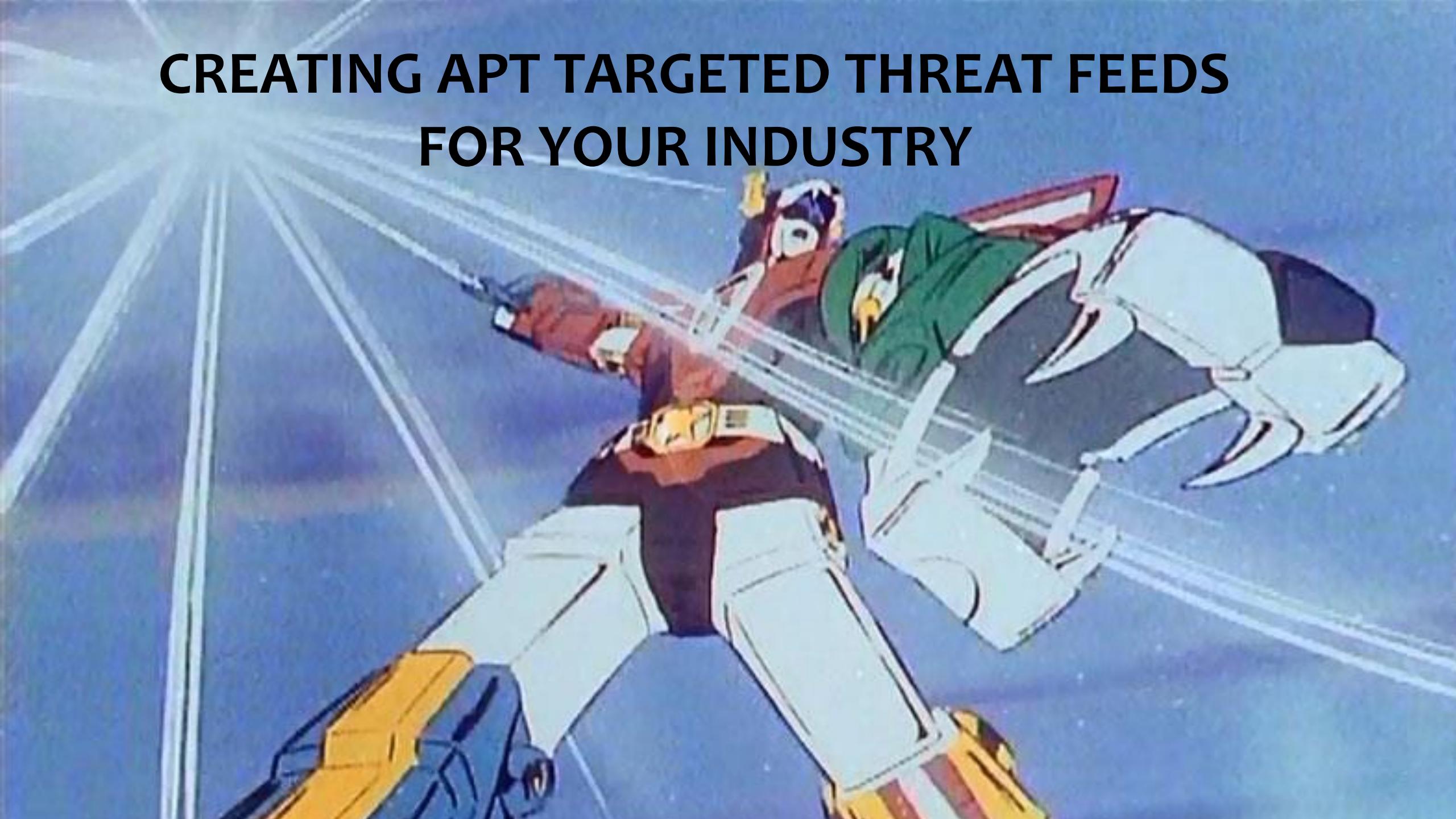
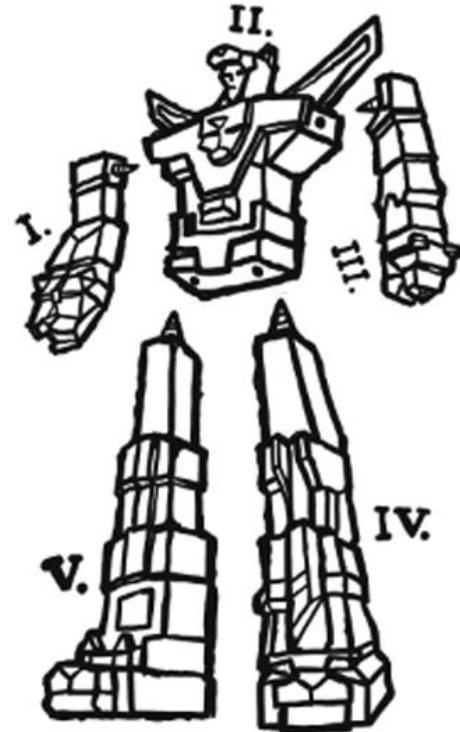


# **CREATING APT TARGETED THREAT FEEDS FOR YOUR INDUSTRY**



# Circle City Con 7.0 Apocalypse

Keith Chapman | CTIA  
Senior Security Analyst  
Belcan LLC  
[kchapman@belcan.com](mailto:kchapman@belcan.com)



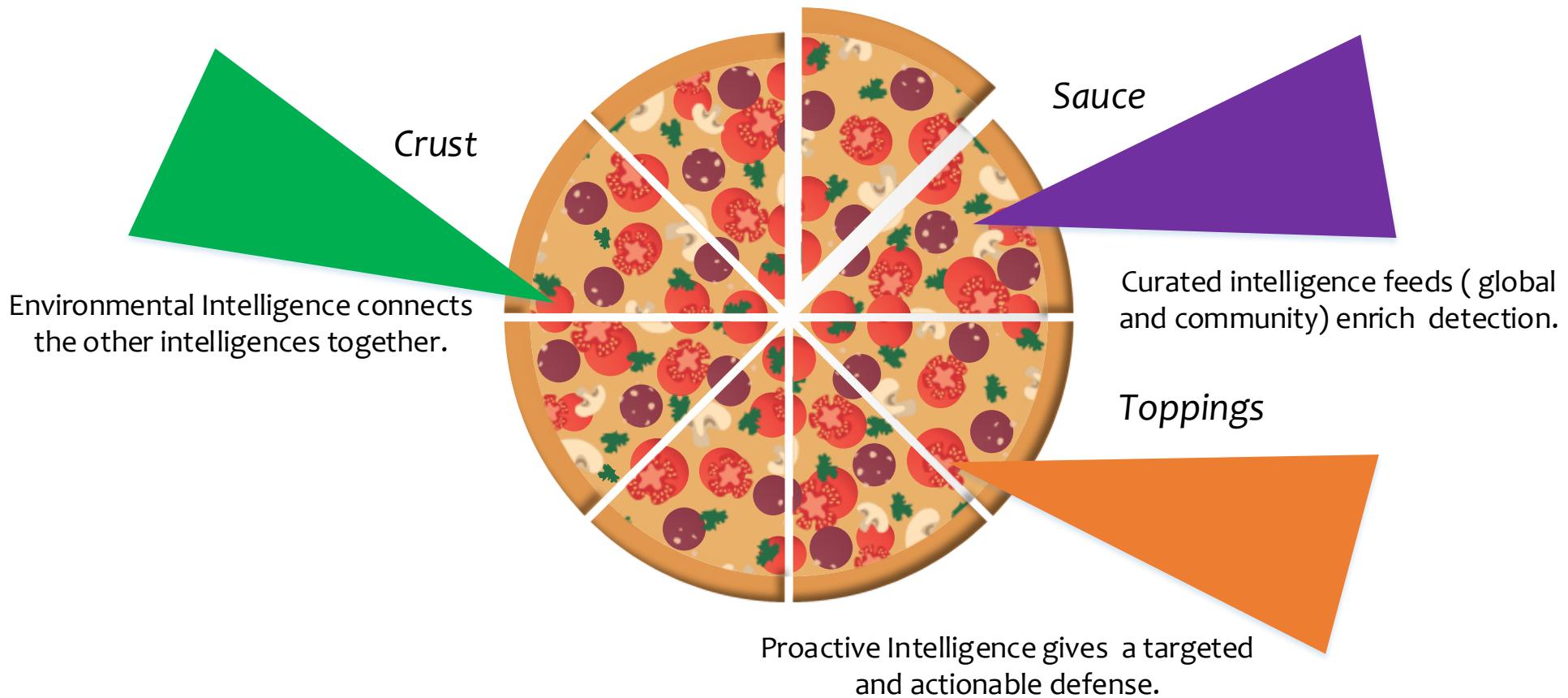
---

J O I N,   o r   D I E.



*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



# Advanced

# Persistent

# Threats



DEEPPANDA



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

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



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. <sup>[1]</sup>
Enterprise	T1132	Data Encoding	An APT19 HTTP malware variant used Base64 to encode communications to the C2 server. <sup>[4]</sup>
Enterprise	T1140	Deobfuscate/Decode Files or Information	An APT19 HTTP malware variant decrypts strings using single-byte XOR keys. <sup>[4]</sup>
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. <sup>[4]</sup>
Enterprise	T1189	Drive-by Compromise	APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets. <sup>[4]</sup>
Enterprise	T1143	Hidden Window	APT19 used <code>-W Hidden</code> to conceal PowerShell windows by setting the WindowStyle parameter to hidden. <sup>[1]</sup>
Enterprise	T1031	Modify Existing Service	An APT19 Port 22 malware variant registers itself as a service. <sup>[4]</sup>
Enterprise	T1112	Modify Registry	APT19 uses a Port 22 malware variant to modify several Registry keys. <sup>[4]</sup>
Enterprise	T1027	Obfuscated Files or Information	APT19 used Base64 to obfuscate commands and the payload. <sup>[1]</sup>
Enterprise	T1086	PowerShell	APT19 used PowerShell commands to execute payloads. <sup>[1]</sup>
Enterprise	T1060	Registry Run Keys / Startup Entries	An APT19 HTTP malware variant establishes persistence by setting the Registry key

# 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	<p>Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist.</p> <p>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.<sup>[3][4]</sup></p>
Exploit Protection	<p>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.<sup>[5][6]</sup></p>
Restrict Web-Based Content	<p>For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.</p> <p>Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.</p>
Update Software	<p>Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on.</p>

## 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

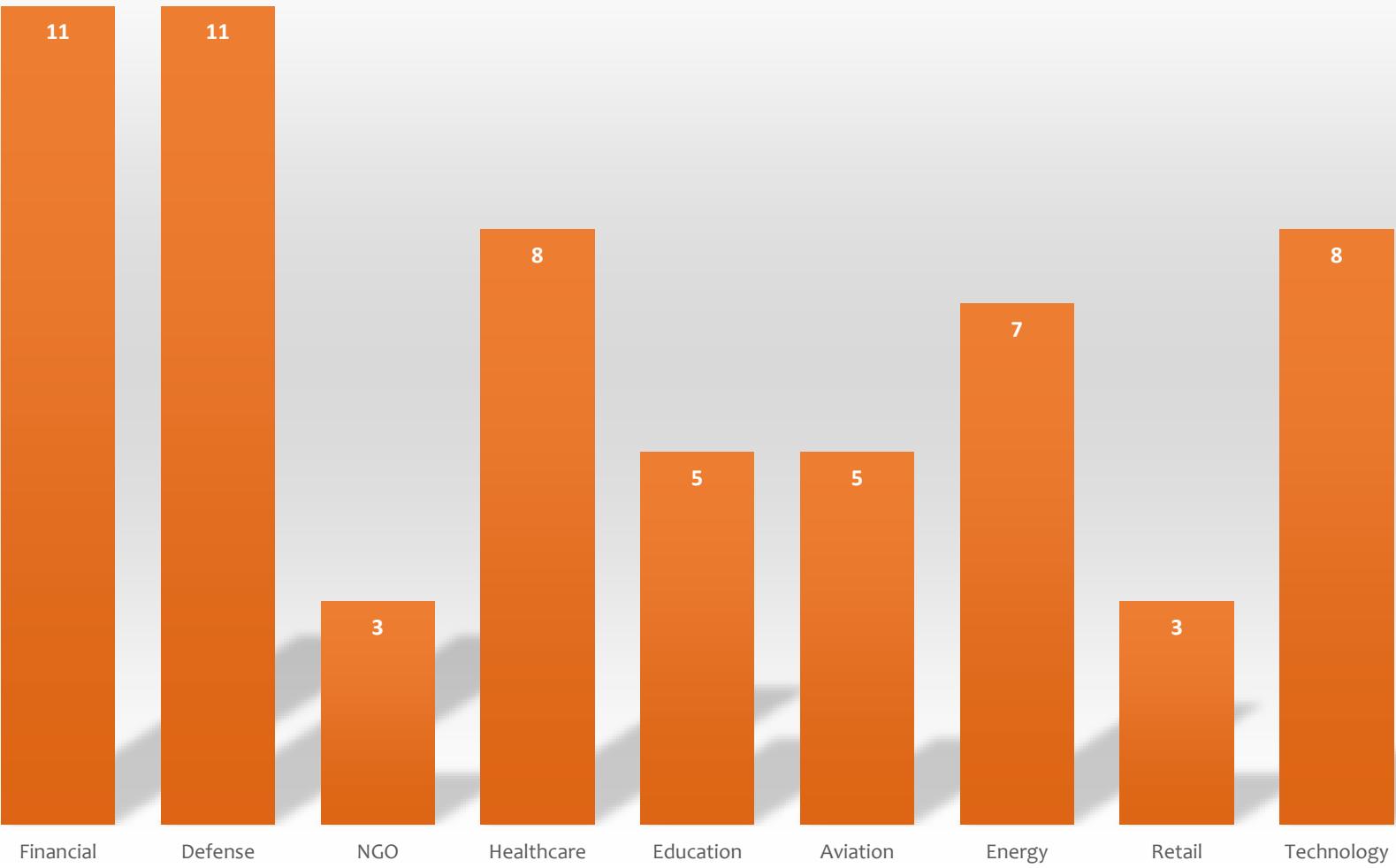
1. Adair, S., Moran, N. (2012, May 15). Cyber Espionage & Strategic Web Compromises – Trusted Websites Serving Dangerous Results. Retrieved March 13, 2018.
2. Lassalle, D., et al. (2017, November 6). OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, 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
Groups	Financial	Defense	NGO	Healthcare	Education	Aviation	Energy	Retail	Technology
1 admin@338									
2 APT12									
3 APT17									
4 APT18									
5 APT19									
6 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

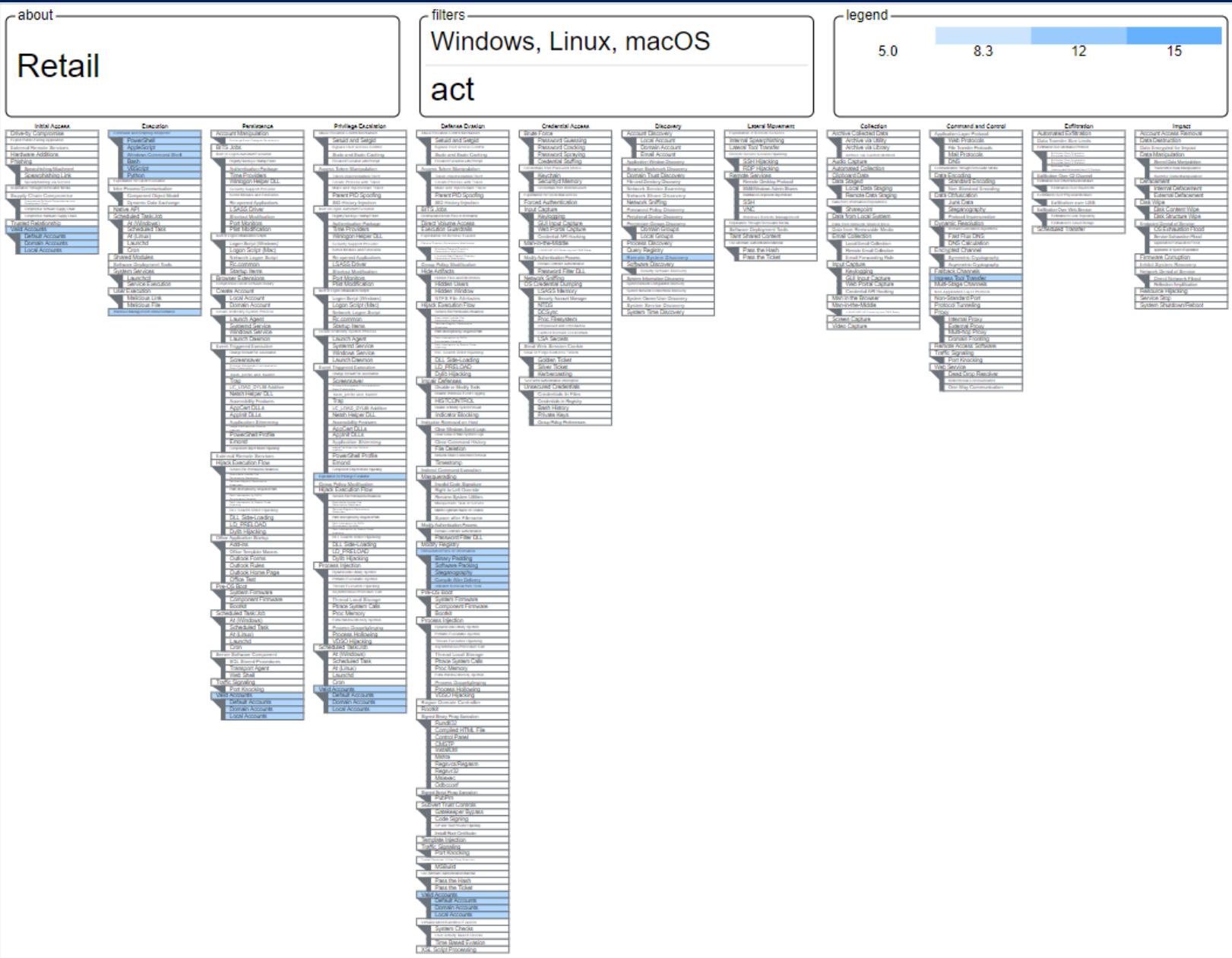


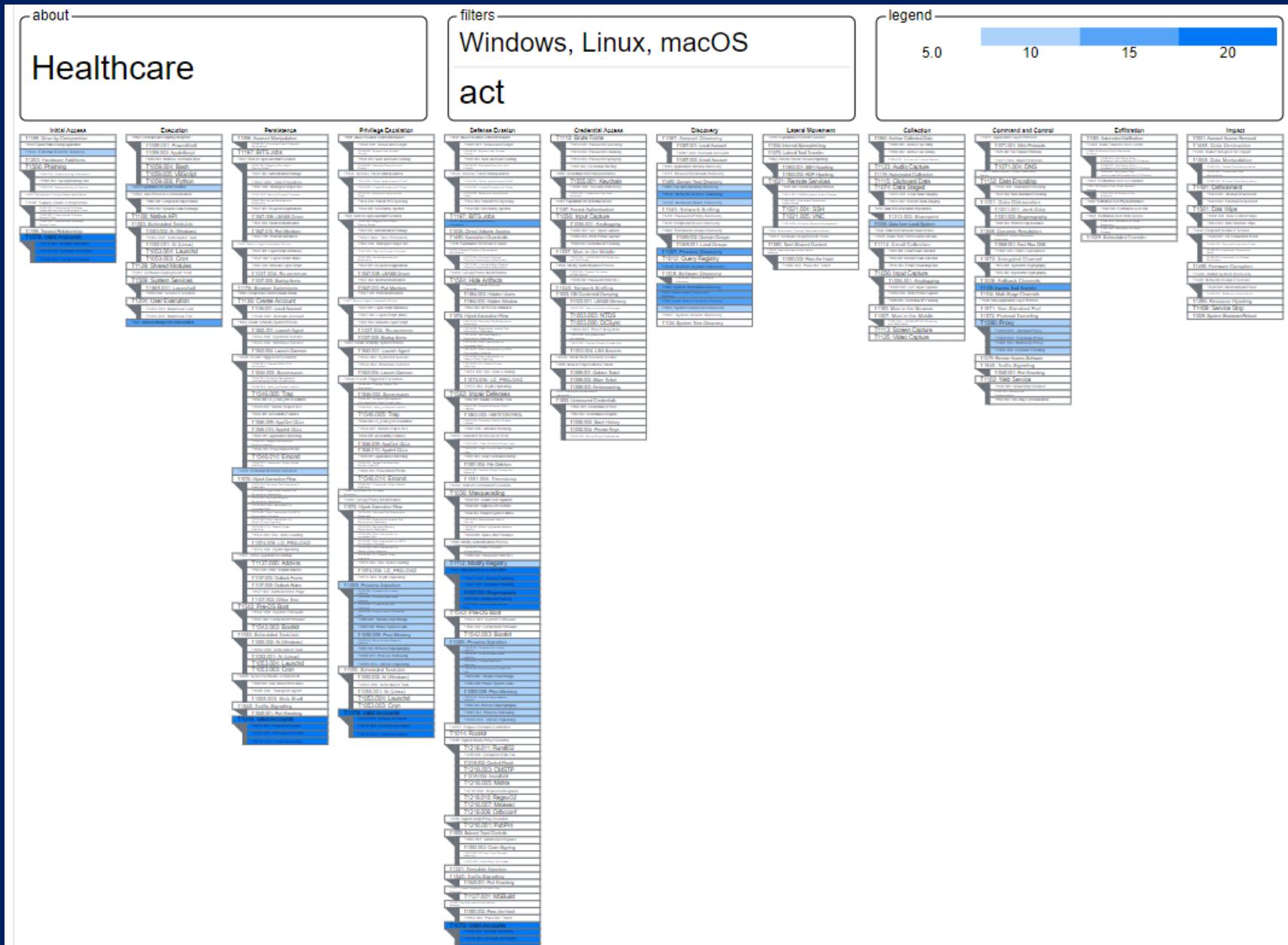


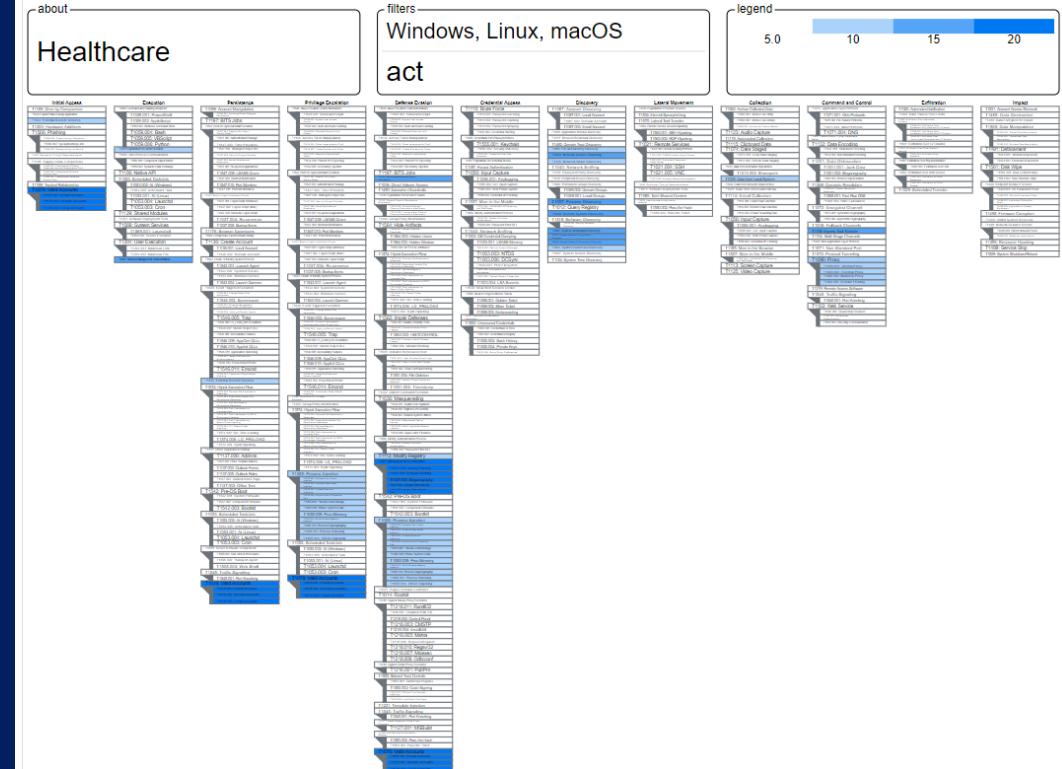
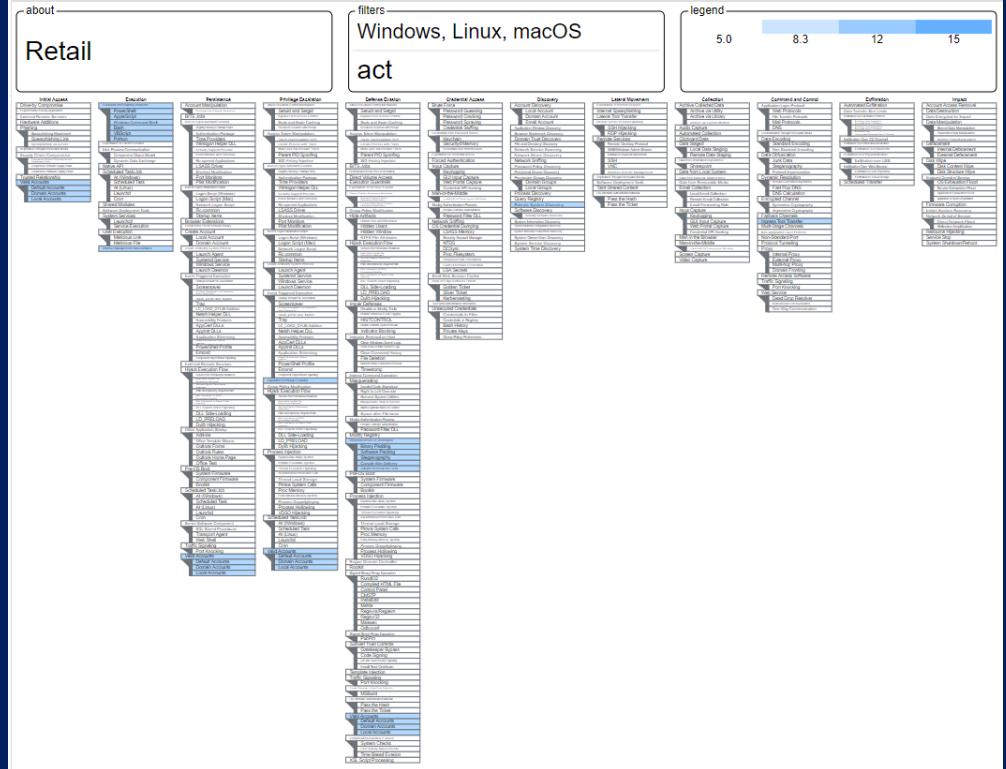
- Research APT groups that target your industry.
- Make a heat map using MITRE ATT&CK tools to see which techniques were most likely.
- A single color may work better than stop light protocol colors.
- Assign scores to each APT group and layer them.
- Place focus on the beginning of the kill chain before 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.



Aviation				filters				score gradient			
				stages: act platforms: Windows, Linux, macOS				5  30			
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	bash profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Application Discovery	AppleScript	Audio Capture	Common User Port	Automated Exfiltration	Account Access Removal
Exploit Public-Racing	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window	Automated Collection	Communication Through	Data Compressed	Data Destruction	
External Remote Services	CommandLine Interceptor	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark	Cloud Content Object Model	Connection Proxy	Data Encrypted	Data Encrypted for Impact	
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Browser User Account	Credential Dumping	Domain Trust Discovery	Clipboard Data	Data from Information	Data Transfer Size Limits	Defacement	
Supply Chain Compromise	Component Object Model	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web	File and Directory	File System Local System	Filesystem Cryptographic	Exfiltration Over Alternative	Disk Content Wine	
Supply Chain Attachment	Control Panel Items	Application Shimming	Browser User Account	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shares	Data Breeding	Exfiltration Over Command	Disk Structure Wine
SupplyChain Link	Dynamic Data Exchange	Authentication Package	CMSTP	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable	Data Circulation	Exfiltration Over Offer	Endpoint Denial of Service
Supply Chain via Service	Execution through API	BITS Jobs	Dll Hijacking	Compiled HTML File	Forced Authentication	Network Setting	Pass the Ticket	Data Staged	Domain Printing	Exfiltration Over Physical	Firmware Corruption
Trust Relationship	Execution	Booklet	Dll Hijacking	Compiled After Delivery	Expiration for Credential	Network Setting	Passport Policy Discovery	Remote Desktop Protocol	Email Collection	Document Generation	Scheduled Transfer
Valid Accounts	Graphical User Interface	Browser Extensions	Download	Component Firmware	Component Object Model	Hosts	Passport Policy Discovery	Remote File Copy	Input Capture	Failure Channels	Network Denial of Service
Initial Access	Logon UI	Component Firmware	Downloads	Container Persistence	Container Persistence	Hotkey	Passport Policy Discovery	Remote Services	Man in the Browser	Multi-hop Proxy	Resource Hijacking
Launchers	LogonUI	Component Object Model	Downloads	Container Persistence	Container Persistence	Process	Passport Policy Discovery	Remote Services	Man in the Browser	Multi-Step Channels	Runtime Data Manipulation
Local Job Scheduling	Create Account	Hooking	DCShadow	Container Persistence	Container Persistence	Protocol	Passport Policy Discovery	Remote Services	Man in the Browser	Multi-Stage Channels	Service Stop
LSASS Driver	Logon UI	Container Persistence	Container Persistence	Container Persistence	Container Persistence	Protocol	Passport Policy Discovery	Remote Services	Man in the Browser	Multi-User Communication	Stored Data Manipulation
Mount	Dll Hijacking	Launch Daemon	Daemons	Container Persistence	Container Persistence	Protocol	Passport Policy Discovery	Windows Admin Shares	Port Knocking	Multi-layer Encryption	System Shutdown/Reboot
PowerShell	Emulator	New Service	DLL Side-Loading	Private Keys	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote Access Tools	Port Knocking	Temporary Data
Regexec/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol Application Layer	
Regsvr32	WMI Automation	Path Interception	Execution Guards	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol Cryptographic	
Rundl32	Windows Management	Path Modification	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Scheduled Task	Hooking	Port Interception	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Trap	Port Monitors	Port Modification	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Trusted Developer Utilities	Login Item	Port Monitors	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
User Execution	Logon Scripts	Void Accounts	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Windows Management	LSASS Driver	Web Shell	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Windows Remote	Modify Existing Service	Indicator Blocking	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
XSL Script Processing	Ntapi Helper DLL	Indicator Removal From	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
New Service	New Service	Indicator Removal on Host	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Office Application Startup	Office Application Startup	Indicator Removal	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Path Interception	Path Interception	Install Root Certificate	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Port Knocking	Port Modification	Install Root Certificate	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Port Monitors	Port Modification	Launchd	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
PowerShell Profile	PowerShell Profile	LC_MAIN Hijacking	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Rc_common	Rc_common	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Re-opened Applications	Re-opened Applications	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Revolvment Access	Revolvment Access	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
ScreenSaver	ScreenSaver	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Security Support Provider	Security Support Provider	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Server Software	Server Software	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Software Recovery	Software Recovery	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Setup and Setup	Setup and Setup	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Shortcut Modification	Shortcut Modification	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Systematic Prinzipal	Systematic Prinzipal	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Startup Items	Startup Items	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
System Firmware	System Firmware	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
System Services	System Services	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Time Providers	Time Providers	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Trap	Trap	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Valid Accounts	Valid Accounts	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Web Shell	Web Shell	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Windows Management	Windows Management	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	
Winlogon Helper DLL	Winlogon Helper DLL	Memory Dumping	Execution Guards and	Passport Filter DLL	Passport Filter DLL	Protocol	Passport Policy Discovery	Windows Admin Shares	Remote File Copy	Protocol File Application	







# 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. <sup>[4]</sup> 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. <sup>[1] [2]</sup> 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. <sup>[3]</sup>

## Detection

Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services.<sup>[37]</sup> 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 can also 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>

Event Actions    Customer    Input Filter    Global Actions    Sync Actions    Administration    Audit

REST client

List Events    Add Event    Import from...   

Search Attributes    View Proposals    Events with proposals    View delegation requests    Export Automation

## Events

	<input type="button" value="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
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		1340	Threat Actor Sofacy	<input type="button" value="Up:green"/> <input type="button" value="APT"/> <input type="button" value="misr-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	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	Synovus Financial	Belcan, US		787	Threat Actor Sofacy	<input type="button" value="Up:white"/> <input type="button" value="osint:source-type='blog-post'"/> <input type="button" value="APT"/>	28	dberberich@belcan.com	2018-08-07	Sofacy Group's Parallel Attacks	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		714	Microsoft Activity Group actor STRONTIUM Threat Actor Sofacy	<input type="button" value="APT"/> <input type="button" value="Threat Type:APT"/> <input type="button" value="Up:white"/> <input type="button" value="osint:source-type='blog-post'"/>	97	dberberich@belcan.com	2018-02-21	A Slice of 2017 Sofacy Activity by Kaspersky	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		874		<input type="button" value="APT"/> <input type="button" value="type:OSINT"/> <input type="button" value="osint:source-type='blog-post'"/> <input type="button" value="Up:white"/>	63	dberberich@belcan.com	2017-09-14	OSINT Phantom of the Opera: New KASPERAGENT Malware Campaign by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		1109	Threat Actor Sofacy	<input type="button" value="Up:white"/> <input type="button" value="osint:source-type='blog-post'"/> <input type="button" value="type:OSINT"/> <input type="button" value="Threat:Sofacy/APT28"/> <input type="button" value="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	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		732	Threat Actor Sofacy	<input type="button" value="Up:white"/> <input type="button" value="osint:source-type='blog-post'"/> <input type="button" value="APT"/> <input type="button" value="Threat:Sofacy/APT28"/>	127	dberberich@belcan.com	2017-11-02	OSINT Fancy Bear Pens the Worst Blog Posts Ever by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		711	Threat Actor Sofacy	<input type="button" value="admirably-scale-information-credibility='?'"/> <input type="button" value="admirably-scale-source-reliability='?'"/> <input type="button" value="osint:source-type='blog-post'"/> <input type="button" value="Up:white"/> <input type="button" value="APT"/> <input type="button" value="Threat:Sofacy/APT28"/>	117	dberberich@belcan.com	2017-07-21	Finding Nemo(hosts) from Sofacy by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		1142	Intrusion Set APT28 Threat Actor Sofacy Microsoft Activity Group actor STRONTIUM	<input type="button" value="Threat:Sofacy/APT28"/> <input type="button" value="Threat Type:APT"/> <input type="button" value="Up:white"/> <input type="button" value="osint:source-type='blog-post'"/> <input type="button" value="APT"/>	10	dberberich@belcan.com	2018-01-11	OSINT Doping Doping Domains - Possible Fancy Bear Domains Spoofing Anti-Doping and Olympic Organizations by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		820		<input type="button" value="type:OSINT"/> <input type="button" value="Up:white"/> <input type="button" value="APT"/>	71	dberberich@belcan.com	2014-09-10	OSINT The Path to Mass-Producing Cyber Attacks by FireEye	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		1100	Tool NanHaiShu	<input type="button" value="APT"/> <input type="button" value="Up:white"/> <input type="button" value="osint:source-type='blog-post'"/>	757	dberberich@belcan.com	2017-10-16	OSINT Leviathan: Espionage actor spearphishes maritime and defense targets	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		689		<input type="button" value="type:OSINT"/> <input type="button" value="Up:white"/> <input type="button" value="APT"/>	114	dberberich@belcan.com	2011-09-22	OSINT Trend Micro Exposes LURID APT	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US		104		<input type="button" value="type:OSINT"/> <input type="button" value="Up:white"/> <input type="button" value="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	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Page 1 of 1, showing 12 records out of 12 total, starting on record 1, ending on 12

Download CSV | PDF | Key

Belcan MISP - Powered by MISP 2.4.10 - Another quality product from the Global Information Security Team! - 2018-11-21 10:57:34

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						

Event Actions    Customer    Input Filter    Global Actions    Sync Actions    Administration    Audit

REST client

List Events    Add Event    Import from...  
My Events    Org Events

Enter value to search    Filter

**Events**

< previous    next >

Published	Org	Owner org	ID	Clusters	Tags	#Attr.	Email	Date	Info	Distribution	Actions
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	1340	Threat Actor Sofacy	ip:green APT misic-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	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	Synovus Financial	Belcan, US	787	Threat Actor Sofacy	tip:white osint:source-type="blog-post" APT	28	dberberich@belcan.com	2018-06-07	Sofacy Group's Parallel Attacks	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	714	Microsoft Activity Group actor STRONTIUM Threat Actor Sofacy	APT Threat Type:APT tip:white osint:source-type="blog-post"	97	dberberich@belcan.com	2018-02-21	A Slice of 2017 Sofacy Activity by Kaspersky	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	874		APT type:OSINT osint:source-type="blog-post" tip:white	63	dberberich@belcan.com	2017-06-14	OSINT Phantom of the Opera: New KASPERAGENT Malware Campaign by ThreatConnect	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	1109	Threat Actor Sofacy	tip: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	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	732	Threat Actor Sofacy	tip: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	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	711	Threat Actor Sofacy	admirably-scale-information-credibility="3" admirably-scale-source-reliability="4" osint:source-type="blog-post" tip:white APT Threat:Sofacy/APT28	117	dberberich@belcan.com	2017-07-21	Finding Nemo(hosts) from Sofacy by ThreatConnect	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	1142	Intrusion Set APT28 Threat Actor Sofacy Microsoft Activity Group actor STRONTIUM	Threat:Sofacy/APT28 Threat Type:APT tip:white osint:source-type="blog-post" APT	10	dberberich@belcan.com	2018-01-11	OSINT Doping Doping Domains - Possible Fancy Bear Domains Spoofing Anti-Doping and Olympic Organizations by ThreatConnect	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	820		type:OSINT tip:white APT	71	dberberich@belcan.com	2014-09-10	OSINT The Path to Mass-Producing Cyber Attacks by FireEye	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	1100	Tool NanHaiShu	APT tip:white osint:source-type="blog-post"	757	dberberich@belcan.com	2017-10-16	OSINT Leviathan: Espionage actor spearphishes maritime and defense targets	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	689		type:OSINT tip:white APT	114	dberberich@belcan.com	2011-09-22	OSINT Trend Micro Exposes LURID APT	Organisation	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	CthulhuSPRL.be	Belcan, US	104		type:OSINT tip: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	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Page 1 of 1, showing 12 records out of 12 total, starting on record 1, ending on 12

< previous    next >

Download CSV/JSON

Belcan MISP - Powered by MISP 2.4.10 - Another quality product from the Global Information Security Team! - 2018-11-21 10:57:34

## Expansion based on shared nameserver with a lot of Sofacy domains

Event ID	1340
UUID	5534e822-0e78-4eea-aea8-4ac3950d210b <a href="#">+</a>
Creator org	CthulhuSPRL.be
Owner org	Belcan, US
Email	dberberich@belcan.com
Tags	<a href="#">tip:green</a> <a href="#">APT</a> <a href="#">misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28"</a> <a href="#">+ +</a>
Date	2015-04-20
Threat Level	Medium
Analysis	Completed
Distribution	Your organisation only <a href="#">+ ↗</a>
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. <a href="#">↗</a>

[- Pivots](#) [- Galaxy](#) [+ Event graph](#) [+ Correlation graph](#) [+ ATT&CK matrix](#) [- Attributes](#) [- Discussion](#)

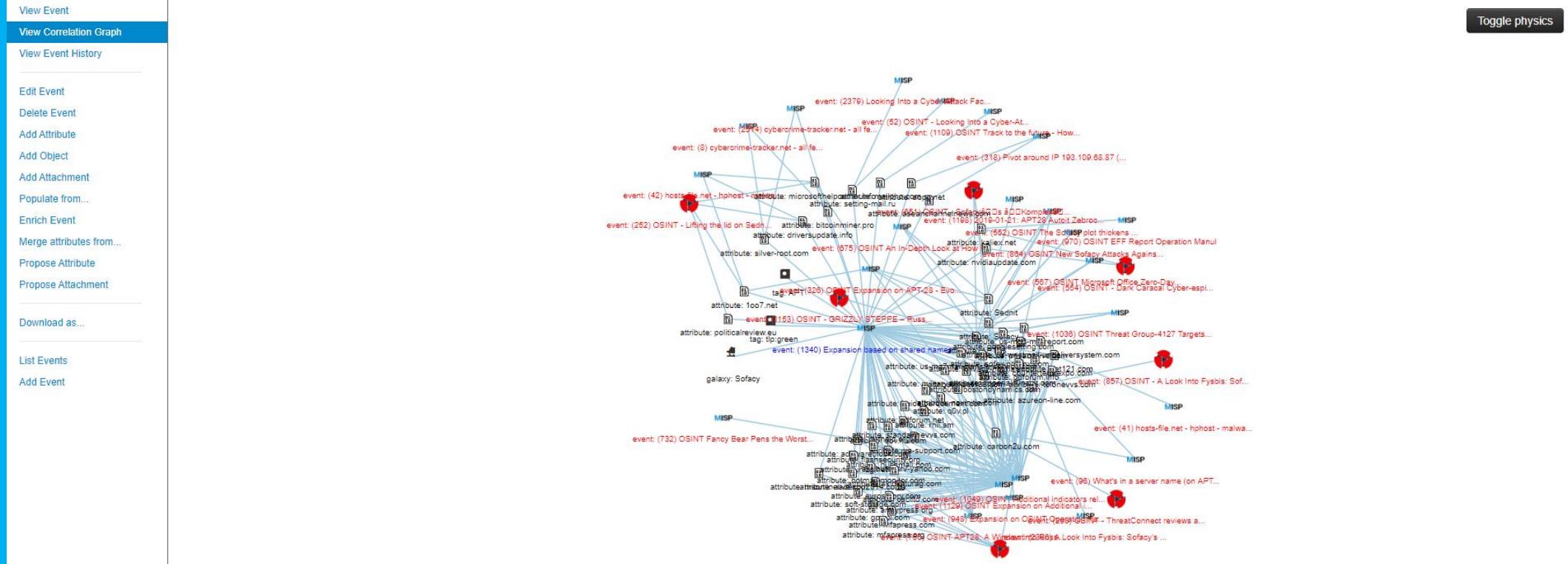
[x 1340: Expans...](#)

## Related Events

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

Show (19 more)

CthulhuSPRL.be



Event Actions    Related    Input Filters    Global Actions    Sync Actions    Administration    Audit

Logout

**List Events**

Add Event  
Import from...  
REST client

**List Attributes**

Search Attributes

**View Proposals**  
Events with proposals

**View delegation requests**

**Export Automation**

## Events

← previous    next →

**Filters:** Tag: APT X    My Events    Org Events

Published	Org	Owner org	ID	Clusters	Tags	#Att.	Email	Date	Info	Distribution	Actions
✓	ChihusSPRL.be	Belcan, US	1040	Threat Actor Sofacy Q	tip:green APT miss-galaxy.malicious-enterprise-attack-intrusion-set--APT28	1532	dberberich@belcan.com	2015-04-20	Expansion based on shared nameserver with a lot of Sofacy domains	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	Synovia Financial	Belcan, US	737	Threat Actor Sofacy Q	tip:white osint:source-type="blog-post" APT	28	dberberich@belcan.com	2016-03-07	Sofacy Group's Parallel Attacks	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	714	Microsoft Activity Group actor Threat Actor Sofacy Q	APT Threat:Type:APT tip:white osint:source-type="blog-post"	97	dberberich@belcan.com	2016-02-21	A Slice of 2017 Sofacy Activity by Kaspersky	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	874		APT type:OSINT osint:source-type="blog-post" tip:white	63	dberberich@belcan.com	2017-06-14	OSINT Phantom of the Opera: New KASPERAGENT Malware Campaign by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	1109	Threat Actor Sofacy Q	tip:white osint:source-type="blog-post" Threat:Sofacy/APT28 APT	181	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: ThreatConnect)	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	732	Threat Actor Sofacy Q	tip:white osint:source-type="blog-post" APT Threat:Sofacy/APT28	127	dberberich@belcan.com	2017-11-22	OSINT Fancy Bear Pens the Worst Blog Posts Ever by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	711	Threat Actor Sofacy Q	admiralty-scale-information-operationality>2< admiralty-scale-source-reliability>2< osint:source-type="blog-post" tip:white APT Threat:Sofacy/APT28	117	dberberich@belcan.com	2017-07-21	Finding Name/host(s) from Sofacy by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	1142	Intrusion Set Threat Actor Sofacy Q Microsoft Activity Group actor STRONTIUM Q	Threat:Sofacy/APT28 Threat:Type:APT tip:white osint:source-type="blog-post" APT	10	dberberich@belcan.com	2018-01-11	OSINT Doping Doping Domains - Possible Fancy Bear Domains Spoofing Anti-Doping and Olympic Organizations by ThreatConnect	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	820		type:OSINT tip:white APT	71	dberberich@belcan.com	2014-09-10	OSINT The Path to Mass-Producing Cyber Attacks by FireEye	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	1100	Tool Manbaishi Q	APT tip:white osint:source-type="blog-post"	767	dberberich@belcan.com	2017-10-10	OSINT Leviathan: Espionage actor spearheads maritime and defense targets	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	689		type:OSINT tip:white APT	114	dberberich@belcan.com	2011-09-22	OSINT Trend Micro Exposes LURID APT	Organisation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	ChihusSPRL.be	Belcan, US	104		type:OSINT tip: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	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Page 1 of 1, showing 12 records out of 12 total, starting on record 1, ending on 12

← previous    next →

Download CSV/PDF

Belcan MISP - Powered by MISP 2.6.11 - Another quality product from the Global Information Security Team - 2018-11-21 11:04:07

Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit

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 [X](#) [My Events](#) [Org Events](#) [Filter](#) Enter value to search

Published	Org	Owner org	ID	Clusters	Tags	#Attr.	Email	Date	Info	Distribution	Actions
<input checked="" type="checkbox"/>	Belcan, US	Belcan, US	2515		<a href="#">osint:source-type="block-or-filter-list"</a>	12948	dberberich@belcan.com	2019-11-14	Phishank online valid phishing feed	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	Belcan, US	Belcan, US	1008		<a href="#">osint:source-type="block-or-filter-list"</a>	246773	dberberich@belcan.com	2019-10-31	URLHaus Malware URLs feed	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	Belcan, US	Belcan, US	43		<a href="#">osint:source-type="block-or-filter-list"</a>	17772	dberberich@belcan.com	2019-10-31	OpenPhish url list feed	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	Belcan, US	Belcan, US	42			299930	dberberich@belcan.com	2019-10-31	hosts-file.net - hphost - malwarebytes - EMD classification ONLY feed	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	Belcan, US	Belcan, US	41			189144	dberberich@belcan.com	2019-10-31	hosts-file.net - hphost - malwarebytes feed	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	Belcan, US	Belcan, US	12		<a href="#">osint:source-type="block-or-filter-list"</a>	34077	dberberich@belcan.com	2019-10-31	Phishank online valid phishing feed	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	 Belcan, US	Belcan, US	579		<a href="#">circl:incident-classification="phishing"</a> <a href="#">tip:white</a>	321	dberberich@belcan.com	2019-02-07	Phishing collection (via URLabuse service)	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	DIGITALSIDE.IT	Belcan, US	1502		<a href="#">tip:white</a> <a href="#">type:OSINT</a> <a href="#">source:DigitalSide.IT</a> <a href="#">source:urlhaus.abuse.ch</a>	29	dberberich@belcan.com	2019-11-12	DigitalSide Malware report: MD5: 7022ba30e28ad3c6e8a256b8b5f79996	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	 Belcan, US	Belcan, US	31		<a href="#">circl:incident-classification="phishing"</a> <a href="#">tip:white</a>	85222	dberberich@belcan.com	2019-10-04	Processed phishank list 2019-10	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	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	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>
<input checked="" type="checkbox"/>	ESET	Belcan, US	1268	Threat Actor <a href="#">APT 29</a> <a href="#">Attack Pattern</a> <a href="#">Spearphishing Attachment - T1193</a> <a href="#">Execution through API - T1106</a> <a href="#">Execution through Module</a> <a href="#">Load - T1120</a> <a href="#">PowerShell - T1086</a> <a href="#">RunDLL2 - T1088</a> <a href="#">Scripting - T1054</a> <a href="#">Service Execution - T1035</a> <a href="#">Valid Accounts - T1078</a> <a href="#">Deobfuscate/Decode Files or Information - T1140</a> <a href="#">File Deletion - T1107</a> <a href="#">Modify Registry - T1112</a> <a href="#">Obfuscated Files or Information - T1027</a> <a href="#">Registry Run Keys / Startup Folder - T1060</a> <a href="#">Scheduled Task - T1063</a> <a href="#">Software Packing - T1045</a>	101	dberberich@belcan.com	2019-10-07	Operation Ghost - White Paper	Organisation	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Details</a>	

[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    Business    Input Filters    Global Actions    Sync Actions    Administration    Audit

Drive - T1038 Q ≡  
 • Data from Removable Media - T1026 Q ≡  
 • Exfiltration Over Command and Control Channel - T1041 Q ≡  
 • Fallback Channels - T1088 Q ≡  
 • File and Directory Discovery - T1083 Q ≡  
 • Network Share Discovery - T1135 Q ≡  
 • Process Discovery - T1097 Q ≡  
 • Standard Application Layer Protocol - T1071 Q ≡  
 • System Network Connections Discovery - T1049 Q ≡  
 • Windows Admin Stores - T1077 Q ≡

**Belcan, US** 157 Attack Pattern 56 dberberich@belcan.com 2019-10-07 SUPPLY CHAIN ATTACKS Organisation

• Exploit Public-Facing Application - T1190 Q ≡  
 • Valid Accounts - T1078 Q ≡  
 • Spearphishing Attachment - T1193 Q ≡  
 • Spearphishing Link - T1192 Q ≡  
 • Account Manipulation - T1098 Q ≡  
 • Create Account - T1136 Q ≡  
 • Application Deployment: Software - T1017 Q ≡  
 Tool  
 • Wmiexec Q ≡  
 • Mimikatz Q ≡  
 • CertMig Q ≡  
 • NsScan Q ≡  
 • ProcDump Q ≡  
 Malpedia  
 • Mimikatz Q ≡  
 Enterprise Attack - Tool  
 • Mimikatz - S0002 Q ≡  
 Tool  
 • Mimikatz Q ≡  
 • Mimikatz - 50002 Q ≡

✓ **EUROLEA** Belcan, US 451 Attack Pattern 19 doebach@belcan.com 2019-05-10 Targeted phishing - PDF documents / phanks Organisation

• Spearphishing Attachment - T1193 Q ≡  
 • Spearphishing Link - T1192 Q ≡

✓ **Belcan, US** 60 Attack Pattern 2 dberberich@belcan.com 2019-05-29 Sector 04 Driver's Increased Activity in 2019 Organisation

• type:OSINT  
 • osint\_lifetime="perpetual"  
 • osint\_certainty="50"  
 • tip:white  
 • osint\_source-type="technical-report"  
 • workflow.todo="expansion"

• type:OSINT  
 • osint\_lifetime="perpetual"  
 • osint\_certainty="50"  
 • tip:white  
 • osint\_source-type="technical-report"  
 • workflow.todo="expansion"

Download CSV/PDF

Belcan MISP - Powered by MISP 2.8.11a - Another quality product from the Global Information Security Team - 2019-10-21 11:04:50

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 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 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 timestamp 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 timestamp 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 timestamp 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

**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: cn8Kmx1YRX8SP1stpkSATi18Tb11A1leJzDFJyZg
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: cn8KmxiYRX8Sp1stpkSATi18Tb11AileJzDFJyZg" \
-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}}
```

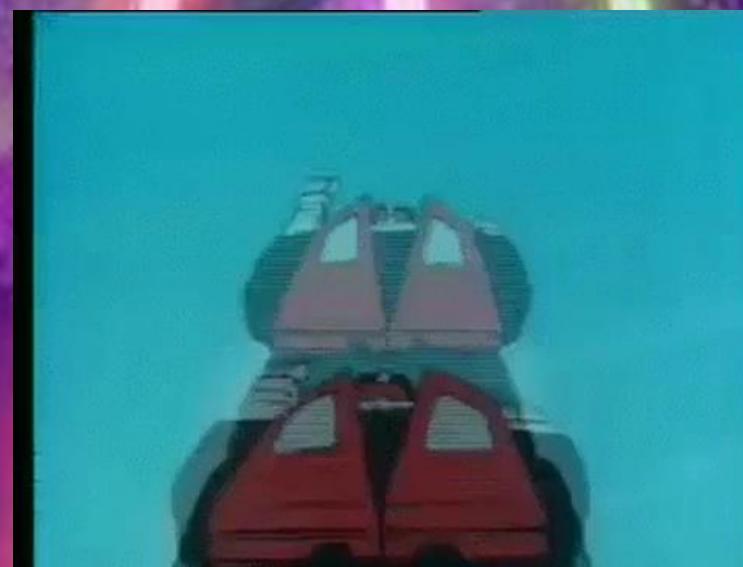
Download: GnuPG key Belcan MISP -- Powered by MISP 2.4.118 -- Another quality product from the Global Information Security Team! - 2019-11-21 12:37:52

e.commiii.skyppee.comweb.pkumedia.combbs.pkumedia.com  
stnet.comhostsvcnet.cometcrem.netmovieultimate.comnewfilmts.comfastdataexchange.orgliveweatherview.comanalyticsb  
yticstest.netlifeofmentalserice.commeteost.comrighttoppregnantpower.comkiteim.orgadobe-flash-  
es.orggeneralsecurityscan.comglobalresearching.orglvueton.comaudiwheel.comonline-  
comfsportal.netnetcorpscanprotect.commvbando.netmvtband.netviters.orgtreepastwillingmoment.comsendmevideo.orgsate  
panorama.comppcodecs.comencoder-  
kwmdmediacodecs.compostlkwarn.comshcserv.comversiontask.comwebcdelivery.commiopc.orgsecurityprotectingcorp.com  
rpind.comappexsrv.netadobeupgradeflash.comhttps://google.com.account-  
word.ga/security/signinoptions/passwordgoogle.com.account-  
word.ga80.255.12.231accounts.google.com.securitymail.gqsecuritymail.gq95.153.32.52smtrelayhost.comuzbekistan-  
comluminate-yahoo.comcc-yahoo-  
gopecmember.comcdncloudflare.com45645647.com57567547454.comciscohelpcenter.comintelsupportcenter.comintelsuppo  
ethighcomission.orgautoupdater.orgsecurityupdatereport.commozilla-  
ns.commozillapugins.comwincodec.comsecurityls.comwindowsdefenderupdater.comwindowschecker.netterms-  
e.comsyslowwindows.comkenlynton.comfastcontech.commslinux-update.comweb-privacy-  
ian.com645547657668787.comandroid-soft.netlive-  
gs.comprivatenewstoday.comservicetransferemail.comadawareblock.comaccess-apple-login-account.gqfileshelpprotut.gares  
word-com.gaaccount-activity-verification-login.gafileshelpprotut.gqrestore-login-account.gqaccount-verify-confirmation-info-  
gafilestore.gqreview-quilogin.gaaccount-verify-comfirmation-info-login.gqgoldsecurity.gasecure-bankofamerica-login-  
gaaccountlogin-inc.gainfo-apple-login-security.gqsecure-bankofamerica-login-com.gqaccountverify-disableinfo-login.gqjp-  
gqsecure-login-helpid-locked.gqalert-new-login-com.galocked-service-security.gasecure-management-login-account-index-  
ass.gqapple-realertlogin.gqllogin-bancochile-cl.gasecure-mobile-login1.gqappleid-login-appleid.gallogin-pap-web-access.gasecu  
login.gaappleid-manageaccountloginupdated.gallogin-recovery.gqsecure1-client-login.gqappleidcustomer-servicess-com-  
ccount.gallogin-sec-apple-secure-account-updated.gasecure1-login-apps.gqappleidcustomer-servicess-com-loginaccount.gqlog  
e1-mobile.gasecure5647login-com.gabrowsersecurity.gallogin-unlock-account.gasecurity-login-information.gqchange-  
word.gallogin-update unlock gasecuritycenter.gacleararea.customerlogin.com.galloginapps.info.gaservice account home

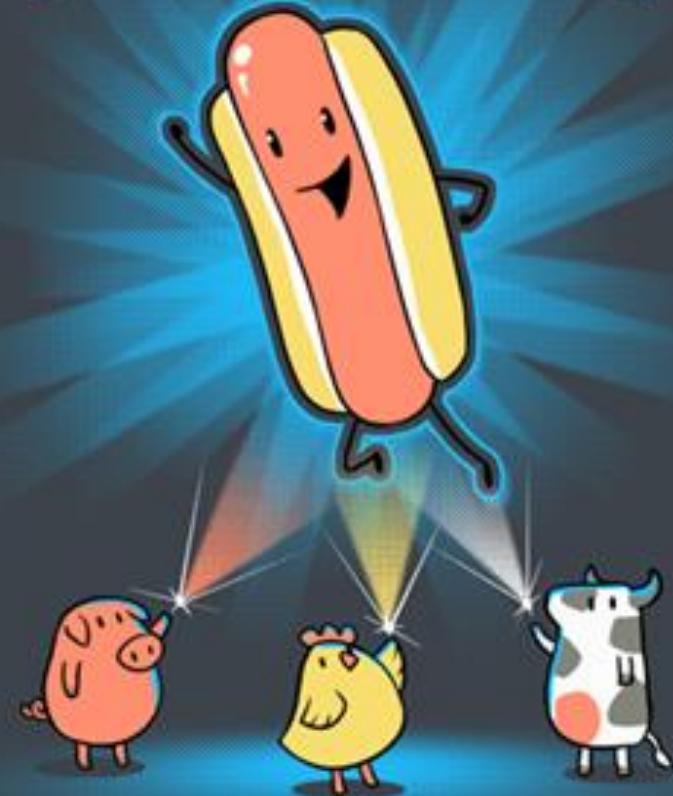
# Threat Intelligence Lifecycle



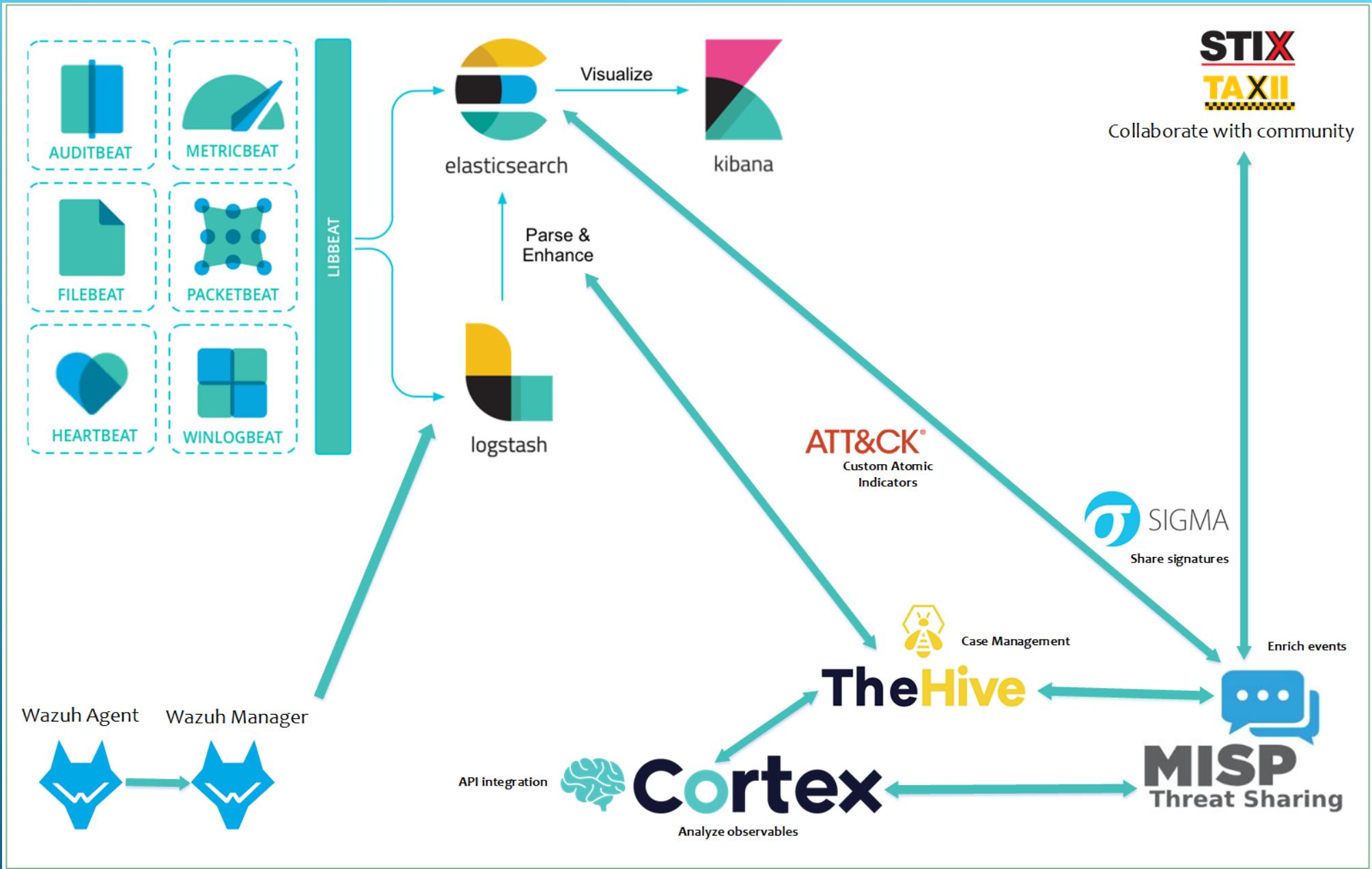
# How can this be scaled?



BY YOUR POWERS

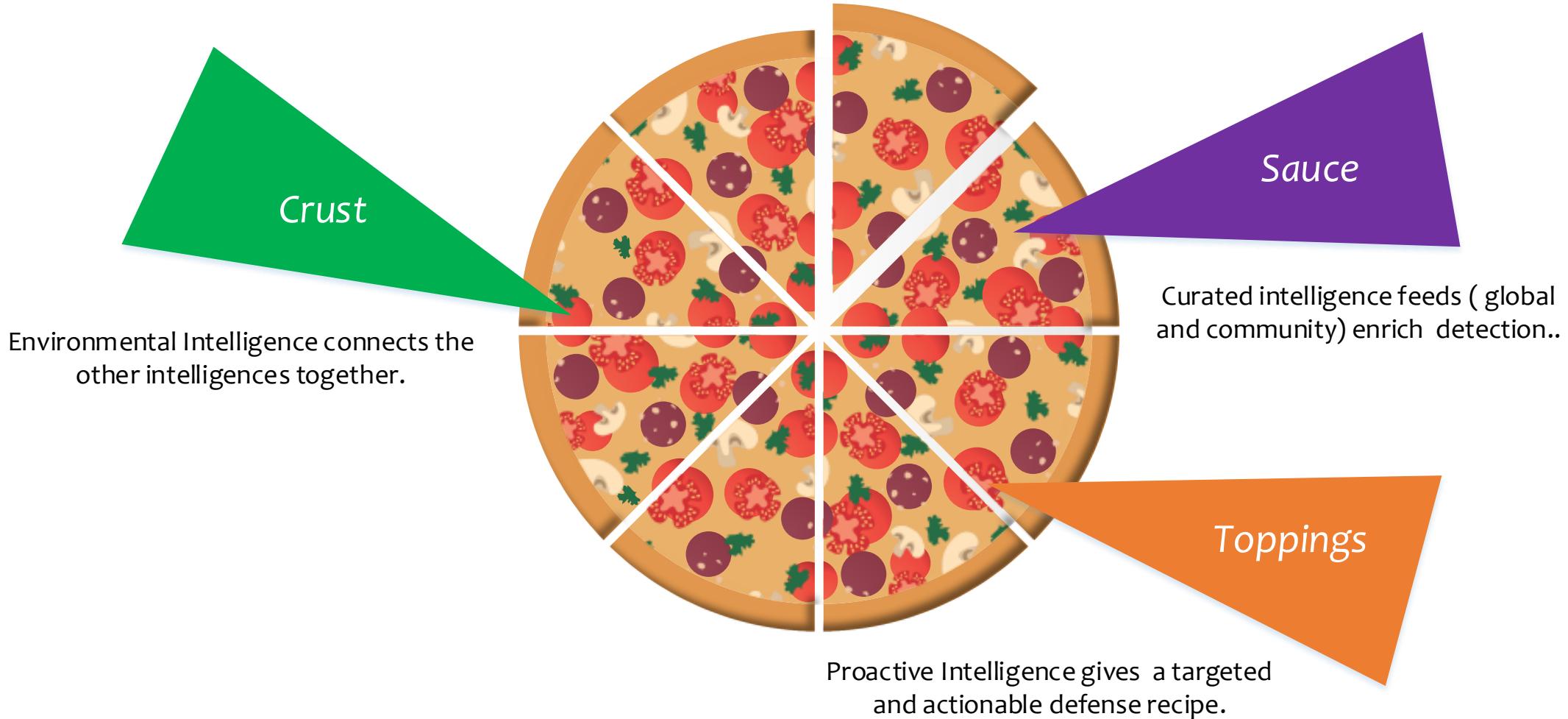


COMBINED!



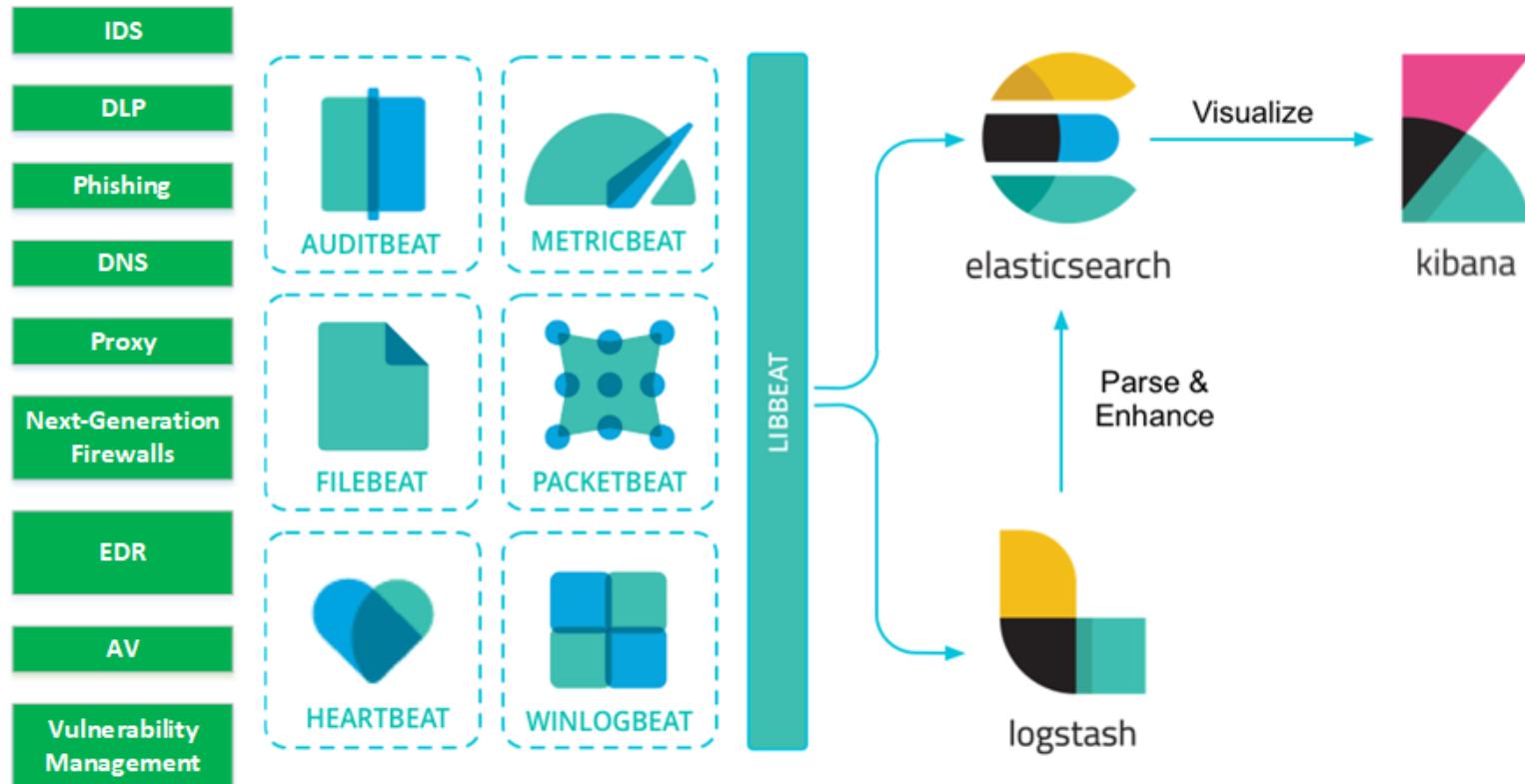
# Synergetic Intelligence Automation

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



## Environmental Intelligence

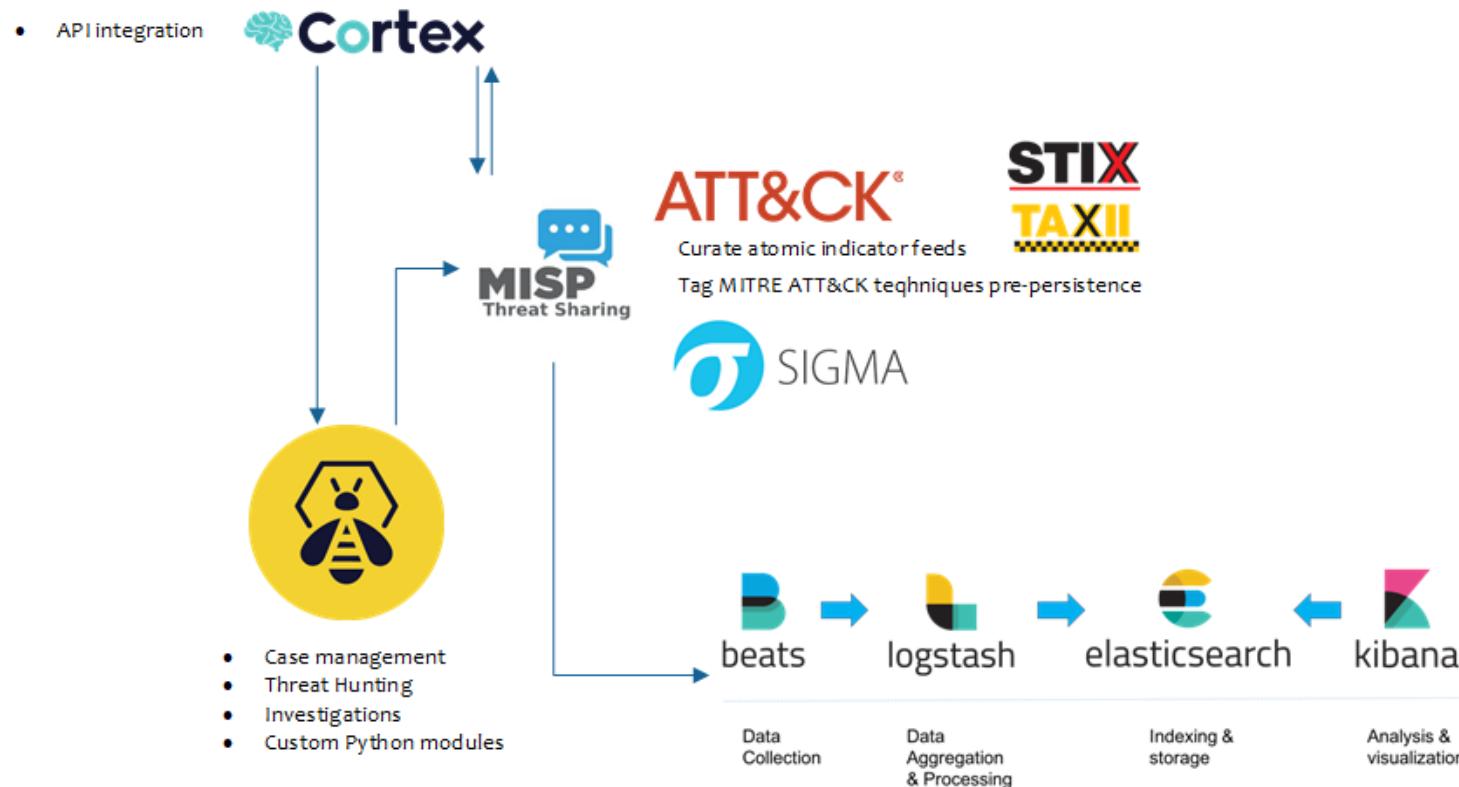
High value log sources are chosen for their visibility and relevance to use cases.  
Machine learning is leveraged to produce alerts based on anomalous behavior.



- 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

**whenitmatters.**

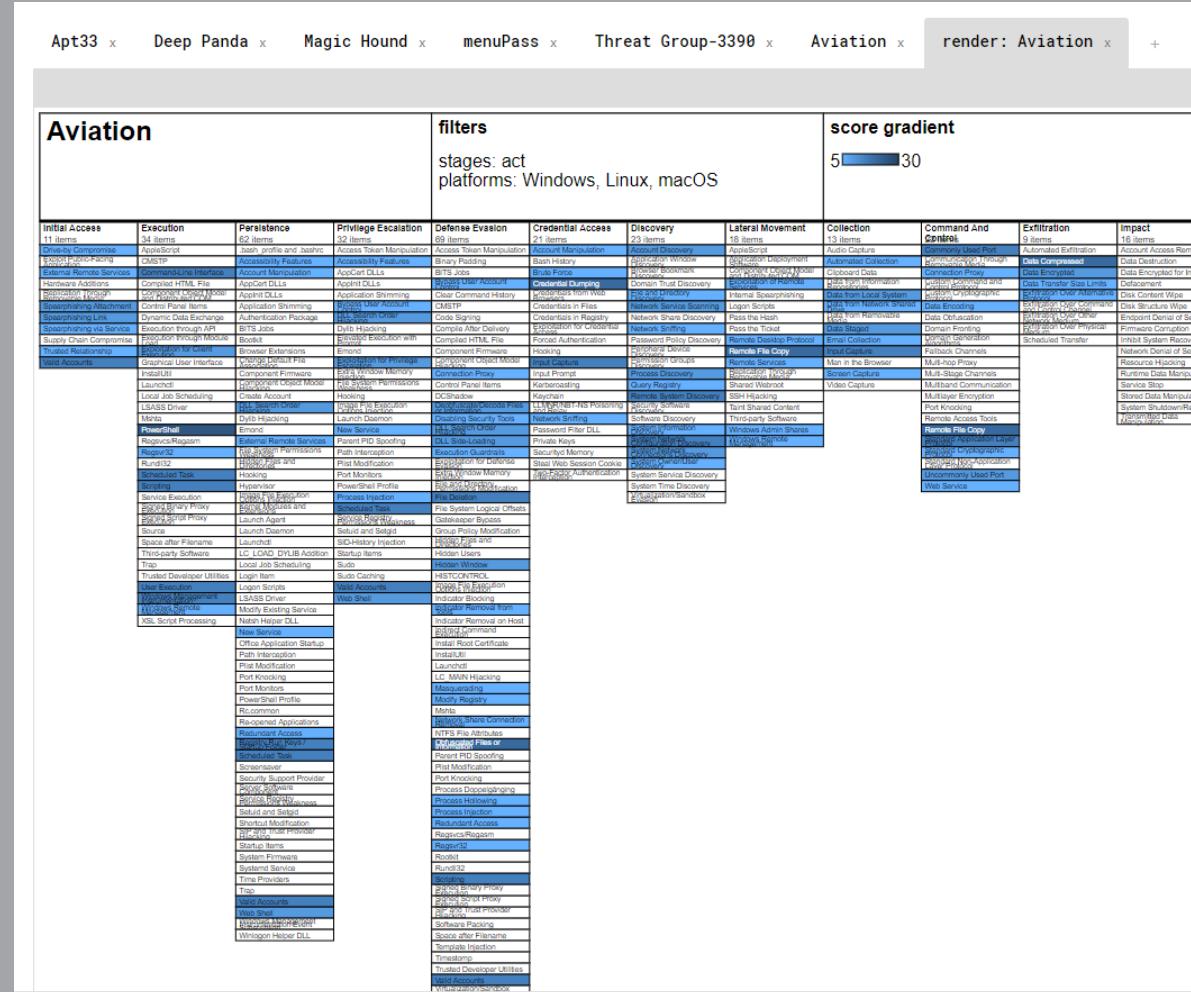


<https://github.com/MISP/MISP>

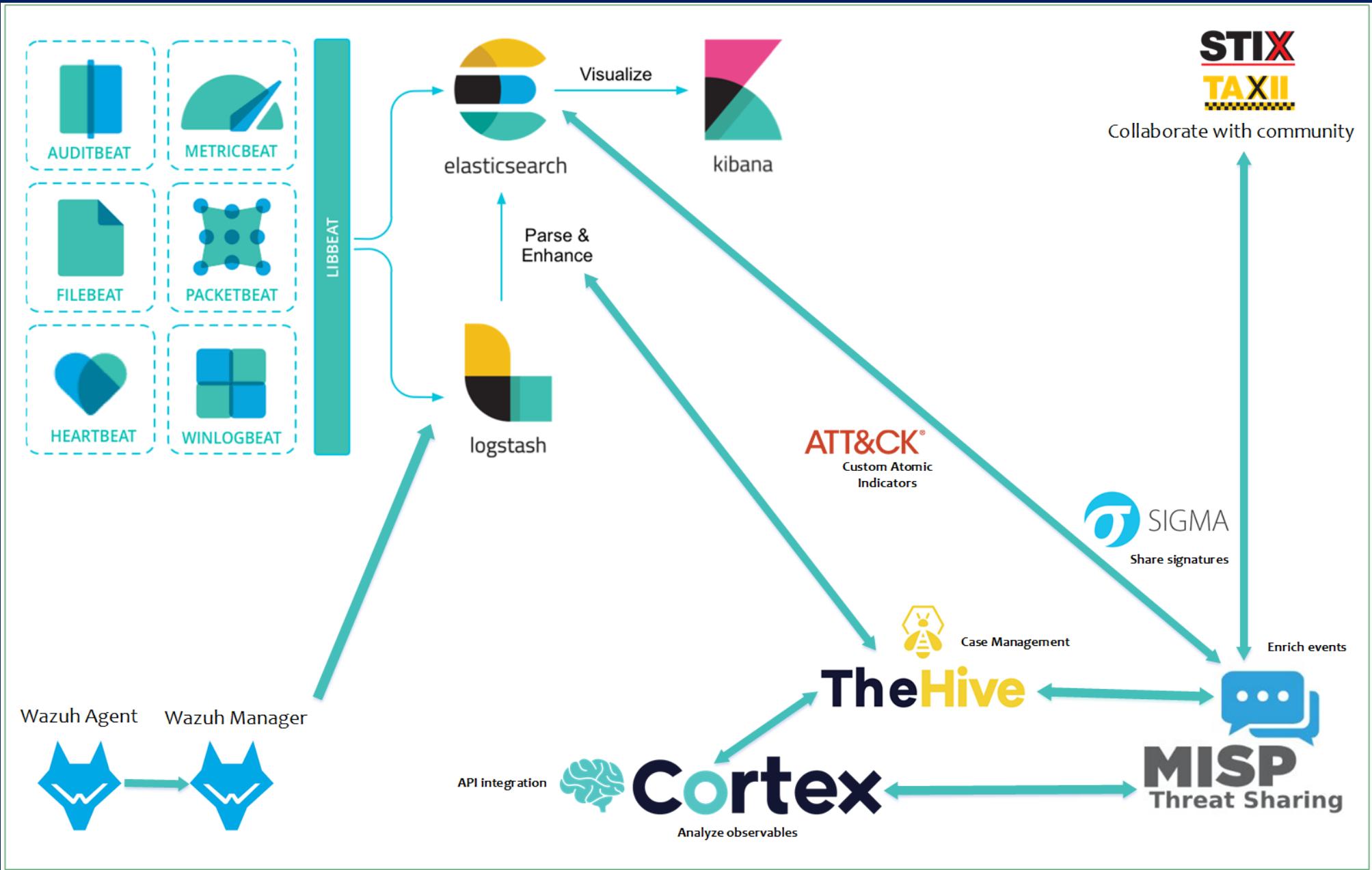
A	B	C	D	E	F	G	H	I	J
Groups	Financial	Defense	NGO	Healthcare	Education	Aviation	Energy	Retail	Technology
2 admin@338									
3 APT12									
4 APT17									
5 APT18									
6 APT19									
7 APT33									
8 APT38									
9 APT41									
10 Carbanak									
11 Charming Kitten									
12 Cobalt 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®



- 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.



**Keith Chapman | CTIA**  
Senior Security Analyst  
Belcan LLC  
[kchapman@belcan.com](mailto:kchapman@belcan.com)

