Public Safety Threat Report:

Defending Against the Top Threats to Public Safety

Disclosure Protocol: GREEN: Restricted to the community
Date of Writing: 05 January 2024

The Public Safety Threat Alliance (PSTA) threat intelligence team actively monitors and evaluates the threats to public safety. In this report, we examine the most common threats impacting public safety, the top tradecraft used against public safety networks, and the most useful defensive measures practitioners can take. Our team used both open and closed-sources as part of our investigation, including information from our ActiveEye Managed Detection and Response team, private and trusted vendors, and government reporting. We used numerous intelligence analytical techniques in the assessment of threat intelligence provided in this report.

Key Points

- There were **368** cyberattacks impacting public safety organizations in 2023, a **64%** increase over 2022.
- Europe public safety attacks eclipsed the U.S. in overall attacks, with the nation targeted by over half of all worldwide hacktivism.
- Ransomware attacks to U.S. public safety organizations increased **63%** in 2023 due to **157%** more extortion groups attacking the nation in 2023.
- **21%** of MITRE ATT&CK's 800 possible techniques and sub-techniques were likely to be employed against public safety networks.

Executive Summary

Attacks to public safety increased in 2023, eclipsing 2022 attack totals by over half. Municipal attacks doubled this year, mostly due to more frequent extortion and initial access broker activity. Successful public safety cyberattacks in Europe surpassed the United States for the first time this year driven primarily by hacktivism, of which Europe accounted for over half in the world. American emergency services felt the brunt of a **63%** increase in extortion activity over 2022. In addition, rare but impactful attacks to mission-critical services occurred in the U.S., showcasing the threat ransomware poses to public safety.

The PSTA Threat Intelligence team identified approximately 180 techniques which threat actors are most likely to employ against public safety networks. Several of these, such as credential abuse, vulnerability exploitation, hiding malware payloads, and attacking remote desktop protocol, are extremely prevalent, and therefore represent a heightened risk for public safety.

Defenders can employ a variety of detection techniques and mitigation strategies (described below in Appendix A and B) to combat the most common threats. Such strategies include implementing multi-factor authentication and patching known exploited vulnerabilities.

Background

Adversaries who attack public safety rely on a variety of tactics, techniques, and procedures (TTPs)[1] to compromise target networks, escalate privileges, execute code, and steal information. This report examines the TTPs most commonly employed during attacks, aligned to the MITRE Corporation's ATT&CK Framework.[2] The ATT&CK Framework categorizes TTPs along the attack chain,[3] allowing defenders to understand and mitigate adversary behavior.

Top Threats to Public Safety Networks

Public safety compromises were at an all-time high in 2023. We observed a total of **368** attacks impacting public safety organizations, a **64%** increase over last year (See Figure 1). Attacks against municipalities, police departments, and federal and military organizations all increased, with municipal entities seeing the largest growth at a **111%** increase (**167** total) over similar attacks observed in 2022. These municipal attacks were often wide-reaching and occasionally a first step in disrupting mission-critical systems like computer-aided dispatch (CAD).

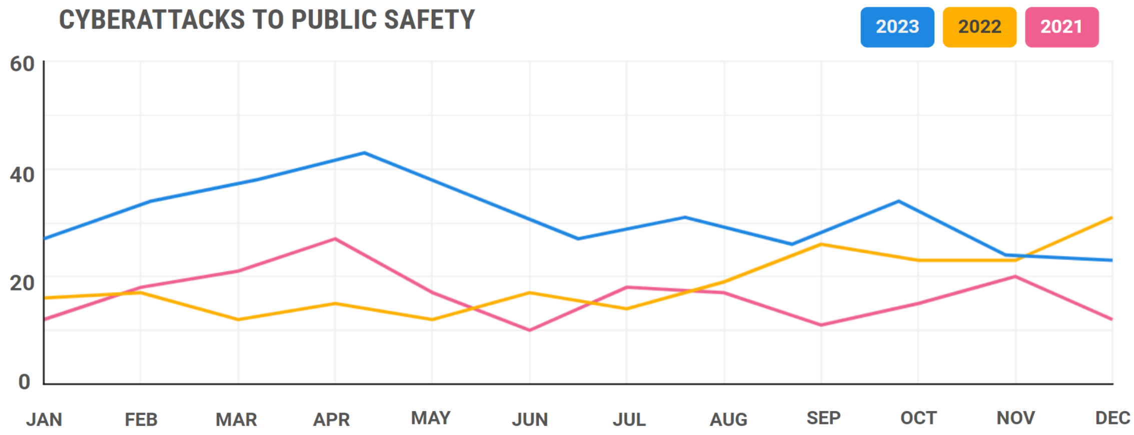


FIGURE 1: Comparison of 2021, 2022, and 2023 cyberattacks against public safety

[1] https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures
[2] https://attack.mitre.org/resources/
[3] https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

An array of adversaries targeted public safety, ranging from financially-motivated extortion groups to ideologically-driven hacktivists. The most prolific group attacking public safety in 2023 was the *LockBit*[4] syndicate with **29** attacks, a minor increase over the group's compromises observed the previous year. Across public safety, *LockBit* mostly attacks municipalities and police departments, likely due to these organizations' moderate size, connection to critical services, and sometimes constrained cybersecurity resources. Like all extortion syndicates, *LockBit* is opportunistic, striking victims who present the highest possibility of attack success and monetary payout.

European public safety cyberattacks exceeded the United States for the first time, with **140** compromises over **94** U.S. attacks, a **49%** difference. Growing hacktivism and initial-access-broker (IAB) activity helped to drive this increase (see Figure 2), with **58%** of ideologically-motivated attacks worldwide impacting European nations. Russia's ongoing war against Ukraine was the primary driver for this activity, generating regular, low-impact distributed-denial-of-service (DDoS) attacks. The top pro-Russian adversary, *NoName057(16)*, accounted for at least **50%** of all European hacktivism, but other groups such as *Anonymous Sudan* also conducted frequent DDoS attacks.

2023 TOP EUROPEAN ATTACK SHIFTS

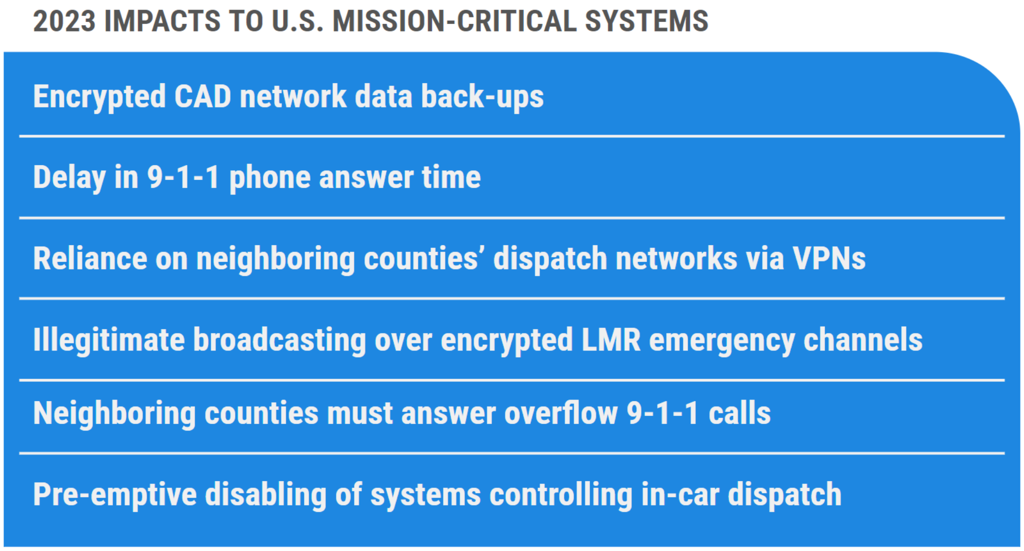
ACCESS BROKERS	11 → 22	+100%
HACKTIVISM	34 → 52	+53%
EXTORTION	37 → 45	+22%

FIGURE 2: Three largest attack categories changes for European cyberattack

Successful cyberattacks against United States public safety agencies increased **50%** this year **(61 → 94).** Extortion was the number one threat to U.S. emergency service organizations; in 2023, there were a total of **65** U.S. attacks involving ransomware and data extortion, a **63%** increase over 2022. Several factors contributed to the rise in extortion, but one of the most significant was an overall growth in the number of extortion syndicates operating today. In 2022, there were **7** attributed groups targeting the U.S., whereas in 2023 that grew to **18**. Some new groups, like *8Base*, conducted only a single compromise while others, such as *Rhysida*, targeted public safety in the U.S. with regularity.

[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

We have moderate confidence mission-critical systems are increasingly becoming impacted in public safety cyberattacks. Rare but disruptive attacks to mission-critical services in the United States were observed this year, primarily in association with ransomware attacks. In 2023, there were **16** reported cases of disruptions to land mobile radio (LMR), CAD, and 9-1-1 call handling systems. **81%** of these involved public safety entities in the United States. This is a **30%** increase compared to 2022. While successful attacks affected a range of systems, they primarily impacted dispatch operations (See Figure 3).


2023 IMPACTS TO U.S. MISSION-CRITICAL SYSTEMS

- Encrypted CAD network data back-ups
- Delay in 9-1-1 phone answer time
- Reliance on neighboring counties' dispatch networks via VPNs
- Illegitimate broadcasting over encrypted LMR emergency channels
- Neighboring counties must answer overflow 9-1-1 calls
- Pre-emptive disabling of systems controlling in-car dispatch

FIGURE 3: Observed disruptions to U.S. LMR, CAD, and 9-1-1 call handling systems in 2023

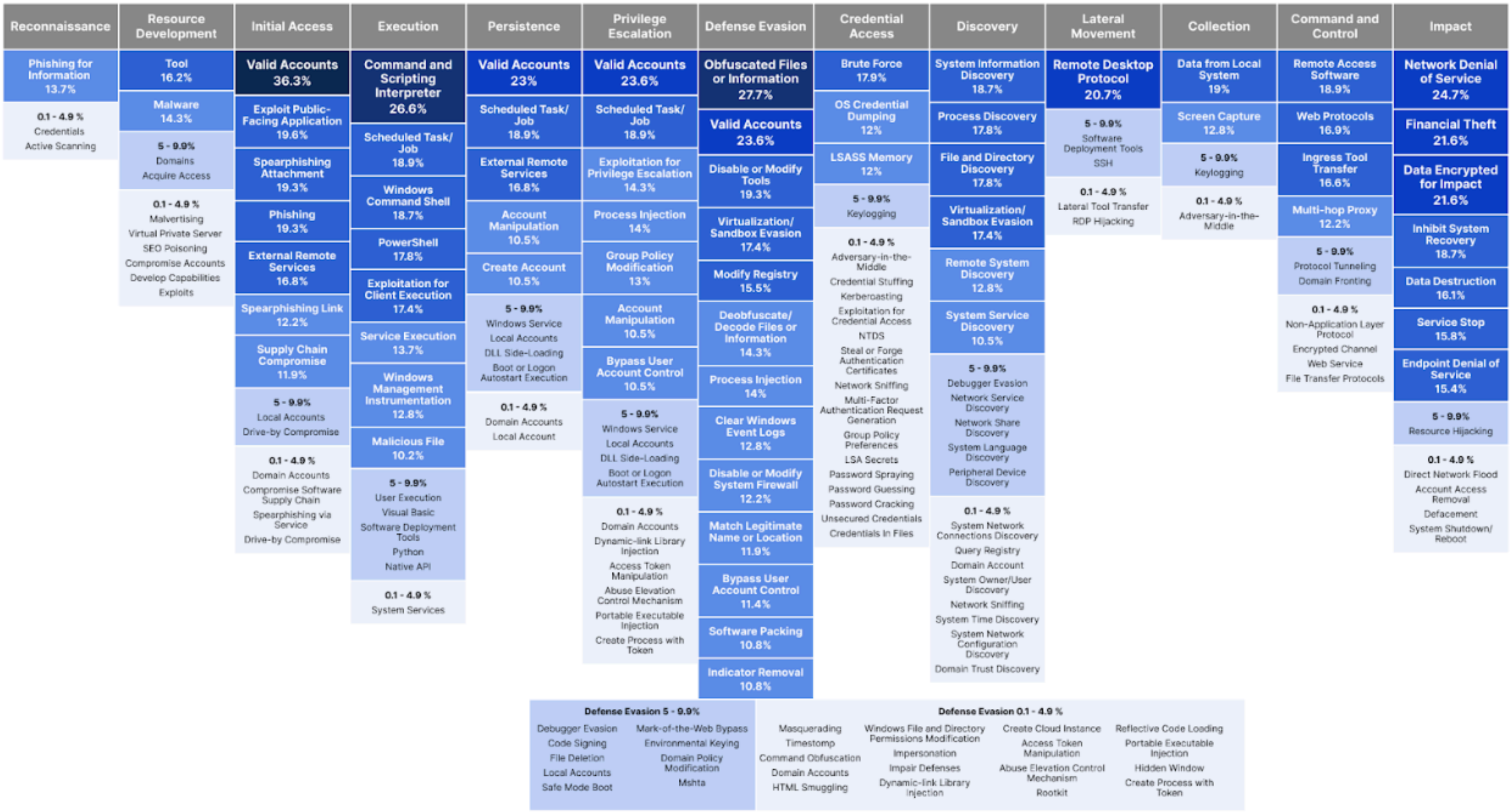
The 2023 Public Safety Attack Chain

There are over 800 techniques and sub-techniques[5] that adversaries can use to conduct cyberattacks as described in the MITRE ATT&CK Framework. However, only **21%** of these techniques are likely to be used in most attacks to public safety (See Figure 4). Some of these, such as Valid Accounts[6] or Command & Scripting Interpreter,[7] are assessed as extremely likely due to their popularity with top public safety threat actors. The below TTPs are the methods by which most adversaries will attempt to compromise and impact public safety organizations.

[5] https://attack.mitre.org/

[6] https://attack.mitre.org/techniques/T1078/

[7] https://attack.mitre.org/techniques/T1059/



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
Phishing for Information 13.7%	Tool 16.2%	Valid Accounts 36.3%	Command and Scripting Interpreter 26.6%	Valid Accounts 23%	Valid Accounts 23.6%	Obfuscated Files or Information 27.7%	Brute Force 17.9%	System Information Discovery 18.7%	Remote Desktop Protocol 20.7%	Data from Local System 19%	Remote Access Software 18.9%	Network Denial of Service 24.7%
0.1 - 4.9 % Credentials Active Scanning	Malware 14.3%	Exploit Public-Facing Application 19.6%	Scheduled Task/ Job 18.9%	Scheduled Task/ Job 18.9%	Scheduled Task/ Job 18.9%	Valid Accounts 23.6%	OS Credential Dumping 12%	Process Discovery 17.8%	5 - 9.9% Software Deployment Tools SSH	Screen Capture 12.8%	Web Protocols 16.9%	Financial Theft 21.6%
	5 - 9.9% Domains Acquire Access	Spearphishing Attachment 19.3%	Windows Command Shell 18.7%	External Remote Services 16.8%	Exploitation for Privilege Escalation 14.3%	Disable or Modify Tools 19.3%	LSASS Memory 12%	File and Directory Discovery 17.8%	0.1 - 4.9 % Lateral Tool Transfer RDP Hijacking	5 - 9.9% Keylogging	Ingress Tool Transfer 16.6%	Data Encrypted for Impact 21.6%
	0.1 - 4.9 % Malvertising Virtual Private Server SEO Poisoning Compromise Accounts Develop Capabilities Exploits	Phishing 19.3%	PowerShell 17.8%	Account Manipulation 10.5%	Process Injection 14%	Virtualization/ Sandbox Evasion 17.4%	5 - 9.9% Keylogging	Virtualization/ Sandbox Evasion 17.4%		0.1 - 4.9 % Adversary-in-the-Middle	Multi-hop Proxy 12.2%	Inhibit System Recovery 18.7%
		External Remote Services 16.8%	Exploitation for Client Execution 17.4%	Create Account 10.5%	Group Policy Modification 13%	Modify Registry 15.5%	0.1 - 4.9 % Adversary-in-the-Middle Credential Stuffing Kerberoasting Exploitation for Credential Access NTDS Steal or Forge Authentication Certificates Network Sniffing Multi-Factor Authentication Request Generation Group Policy Preferences LSA Secrets Password Spraying Password Guessing Password Cracking Unsecured Credentials Credentials In Files	Remote System Discovery 12.8%			5 - 9.9% Protocol Tunneling Domain Fronting	Data Destruction 16.1%
		Spearphishing Link 12.2%	Service Execution 13.7%	5 - 9.9% Windows Service Local Accounts DLL Side-Loading Boot or Logon Autostart Execution	Account Manipulation 10.5%	Deobfuscate/ Decode Files or Information 14.3%		System Service Discovery 10.5%			0.1 - 4.9 % Non-Application Layer Protocol Encrypted Channel Web Service File Transfer Protocols	Service Stop 15.8%
		Supply Chain Compromise 11.9%	Windows Management Instrumentation 12.8%	0.1 - 4.9 % Domain Accounts Local Account	Bypass User Account Control 10.5%	Process Injection 14%		5 - 9.9% Debugger Evasion Network Service Discovery Network Share Discovery System Language Discovery Peripheral Device Discovery				Endpoint Denial of Service 15.4%
		5 - 9.9% Local Accounts Drive-by Compromise	Malicious File 10.2%		5 - 9.9% Windows Service Local Accounts DLL Side-Loading Boot or Logon Autostart Execution	Clear Windows Event Logs 12.8%		0.1 - 4.9 % System Network Connections Discovery Query Registry Domain Account System Owner/User Discovery Network Sniffing System Time Discovery System Network Configuration Discovery Domain Trust Discovery				5 - 9.9% Resource Hijacking
		0.1 - 4.9 % Domain Accounts Compromise Software Supply Chain Spearphishing via Service Drive-by Compromise	5 - 9.9% User Execution Visual Basic Software Deployment Tools Python Native API		0.1 - 4.9 % Domain Accounts Dynamic-link Library Injection Access Token Manipulation Abuse Elevation Control Mechanism Portable Executable Injection Create Process with Token	Disable or Modify System Firewall 12.2%						0.1 - 4.9 % Direct Network Flood Account Access Removal Defacement System Shutdown/ Reboot
			0.1 - 4.9 % System Services			Match Legitimate Name or Location 11.9%						
						Bypass User Account Control 11.4%						
						Software Packing 10.8%						
						Indicator Removal 10.8%						

Defense Evasion 5 - 9.9%

Debugger Evasion
Code Signing
File Deletion
Local Accounts
Safe Mode Boot
Mark-of-the-Web Bypass
Environmental Keying
Domain Policy Modification
Mshta

Defense Evasion 0.1 - 4.9 %

Masquerading
Timestomp
Command Obfuscation
Domain Accounts
HTML Smuggling
Windows File and Directory Permissions Modification
Impersonation
Impair Defenses
Dynamic-link Library Injection
Create Cloud Instance
Access Token Manipulation
Abuse Elevation Control Mechanism
Rootkit
Reflective Code Loading
Portable Executable Injection
Hidden Window
Create Process with Token

FIGURE 4: Public safety heat map of most likely tradecraft

The above TTPs may be viewed as a left-to-right ‘attack chain,’ where a given adversary will start conducting reconnaissance, access a target public safety network, attempt to discover more about the location of sensitive files and servers, move to new systems and environments, erase evidence, and finally, perform the originally intended goal of the attack, whether that is ransomware delivery, data theft, or selling the access to another adversary.

Defending Against the Most Likely Threats

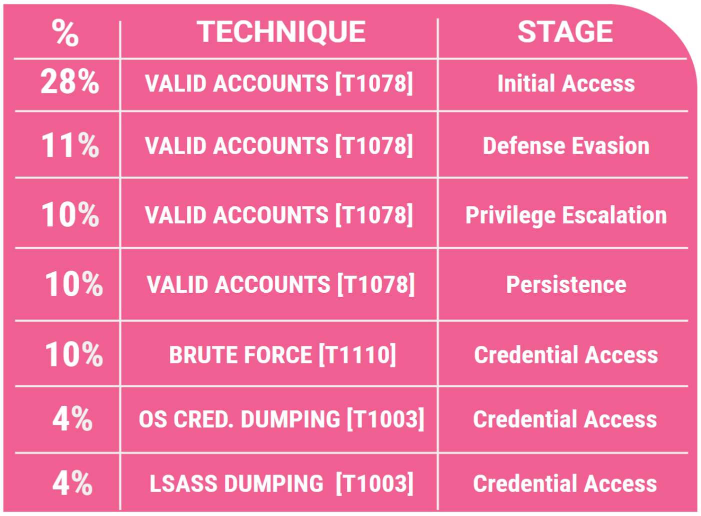
Some TTPs are so prevalent in public safety attacks, they deserve special consideration from defenders. Threat actors, including extortion syndicates, use these techniques to access target systems, operate under the radar, move laterally across victim networks, and execute commands and malware.

> *For a full checklist of* ***detections*** *and* ***mitigation*** *recommendations associated with the top tradecraft, please see Appendix A: Detection Methods for Top Tradecraft and Appendix B: 2023 Defender Checklist.*

Credential Abuse

The use of valid accounts by threat actors was the most common factor in public safety attacks this year. Threat actors leveraged techniques like Brute Force,[8] Valid Accounts,[9] and OS Credential Dumping[10] employed across the attack chain to accomplish varying objectives (See Figure 5). Adversaries also employed credential dumping tools to assist in credential access; *LockBit*, *Play*,[11] *BlackCat*, *Cuba*, and *Akira* syndicates all were observed using Mimikatz,[12] a tool known for stealing Windows logins.

WHAT PERCENTAGE OF THREAT ACTORS ABUSED CREDENTIALS?



%	TECHNIQUE	STAGE
28%	VALID ACCOUNTS [T1078]	Initial Access
11%	VALID ACCOUNTS [T1078]	Defense Evasion
10%	VALID ACCOUNTS [T1078]	Privilege Escalation
10%	VALID ACCOUNTS [T1078]	Persistence
10%	BRUTE FORCE [T1110]	Credential Access
4%	OS CRED. DUMPING [T1003]	Credential Access
4%	LSASS DUMPING [T1003]	Credential Access

FIGURE 5: Percentage of adversaries which leveraged top credential abuse TTPs

[8] https://attack.mitre.org/techniques/T1110/
[9] https://attack.mitre.org/techniques/T1078/
[10] https://attack.mitre.org/techniques/T1003/
[11] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
[12] https://attack.mitre.org/software/S0002/

Defenders should enforce multi-factor authentication (MFA) for as many services as possible, prioritizing privileged accounts and services such as remote connections like virtual private networks (VPNs) or remote access software (RAS). **29%** percent of attributed threat actors, including *LockBit*, used legitimate credentials to access target environments, while another **11%** leveraged them to evade detection from security monitoring solutions. MFA helps to counter such tradecraft, forcing attackers to rely on less convenient attack methods.

Organizations should require that all default passwords are changed, prioritizing externally-facing services and applications. Additionally, all hardware, software, and firmware for internal and external networks should be changed. Default accounts are frequently easier to brute-force, which is a tactic at least **10%** of public safety attackers leverage, including the *Royal*[13] and *CL0P*[14] extortion syndicates, as well as IABs like *mont4na*, who was responsible for **5** compromises this year.

Credentials ought to be both strong and unique. Practitioners should ensure credentials are not reused across the IT environment and that passwords have a length of 15 characters or more. This is because simple passwords take less time to guess or brute-force, and reused credentials make it easier for adversaries who successfully compromised credentials to move across victim networks and access new systems.

The above recommendations are especially important for administrator accounts; public safety attackers often target high-privileged accounts to access and control new environments. Roughly **2%** of all 2023 alerts from our ActiveEye Managed Detection team resulted in FortiGate firewall administrator accounts being disabled due to consecutive failed login attempts.

The Public Safety Threat Alliance offers Dark Web Monitoring for PSTA members at no cost. Dark Web Monitoring allows PSTA members to be alerted when possibly compromised credentials associated with defender domains are identified on criminal forums, marketplaces, and messaging platforms, supporting a well-rounded defense and alerting strategy.

Command & Scripting Interpreter

Attackers often misuse command shells in victim environments to execute arbitrary commands and install malware. Most command shells are built-in. This means threat actors like *LockBit*, *NoEscape*,[15] and *Snatch*[16] who targeted Windows Command Shell did so as a means of "living off the land,"[17] allowing them to potentially evade security alerts and mitigations after achieving initial access (See Figure 6).

[13] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

[14] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

[15] https://www.hhs.gov/sites/default/files/noescape-ransomware-analyst-note-tlpclear.pdf

[16] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a

[17] https://www.malwarebytes.com/blog/business/2023/04/living-off-the-land-lotl-attacks-detecting-ransomware-gangs-hiding-in-plain-sight

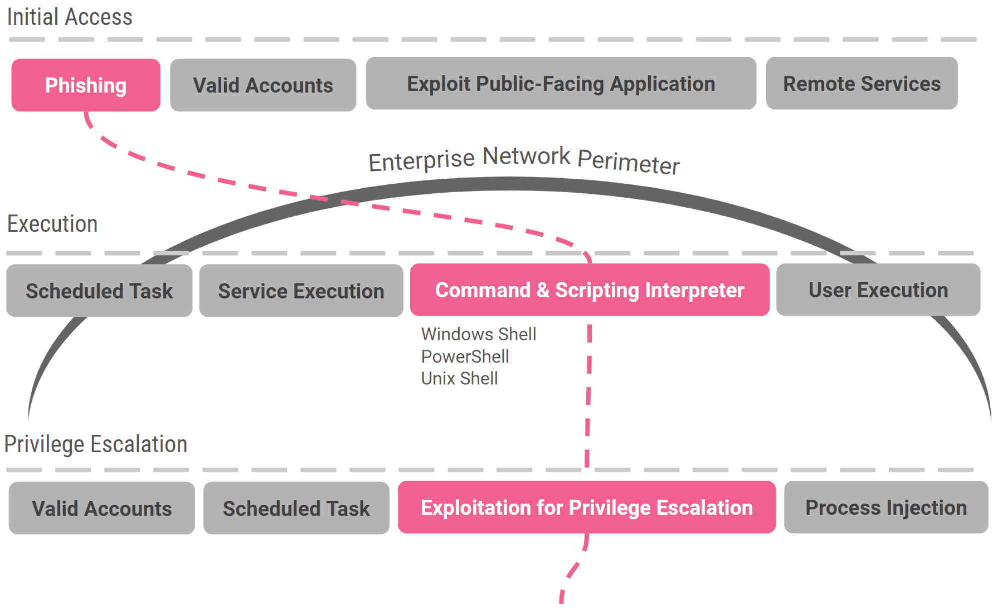


FIGURE 6: Example scenario showcasing command shell abuse following initial access

Organizations should use application control mechanisms to restrict dangerous command shell language elements, such as those employed to execute files or Windows APIs. Application code signing can assist defenders to prevent unwanted code execution by only permitting the execution of signed scripts. **13%** of all attributed threat actors, most of them aggressive extortion groups, use some form of command and scripting interpreter to execute dangerous files or commands.

If PowerShell is not necessary, disable the use of PowerShell following a review to assess the impact to the environment. **7%** of adversaries employ PowerShell as a powerful tool to discover sensitive information and execute code. Known PowerShell users include sophisticated and aggressive groups such as *LockBit* and other extortion syndicates, as well as most nation-state APTs who target public safety. In addition, **8%** of all 2023 alerts from our ActiveEye Managed Detection team involved activity in the execution phase[18] of attacks, under which PowerShell falls.

If it is required for business purposes, restrict PowerShell use to only administrator accounts or Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution. PowerShell Constrained Language mode can also be used to restrict access to dangerous language elements.

Obfuscated Files or Information

Most extortion groups who target public safety, as well as many nation-state APTs who conduct campaigns against government and military organizations, try to make malicious executables harder

[18] https://attack.mitre.org/tactics/TA0002/

to identify by compressing, archiving, or encrypting them.[19] For example, the *Medusa* group uses the Themida[20] trojan to protect payloads against reverse engineering.[21]

Defenders can leverage Microsoft Defender Antivirus to enable the 'Block execution of potentially obfuscated scripts' attack surface rule in audit or enforcement mode. The Antimalware Scan Interface (AMSI) on Windows 10 and 11 can also help. This recommendation is because **12%** of attributed public safety adversaries used this TTP as a regular part of their tradecraft. In addition, Obfuscated Files or Information ranked as Red Canary's 4th most common TTP in 2023,[22] showcasing its wide usage.

Other defensive measures, such as regular audits of fileless storage for abnormal or malicious data can be effective, but require a regular time investment which may not be feasible for most defenders who must prioritize which security measures provide the most benefit for the resources invested.

Remote Desktop Protocol

The use of the remote desktop protocol (RDP) is the most commonly observed method of lateral movement by threat actors who target public safety. Valid credentials are often used in conjunction with RDP to laterally move across assets in an organization. Over **10%** of observed threat actors targeting public safety used RDP as a means of lateral movement. These groups include *LockBit, Akira, BlackCat, Royal, and Rhysida*. The post-exploitation framework Cobalt Strike[23] is also often used as a means to move laterally using RDP.

Lateral movement allows threat actors to move deeper into a target environment in the hopes of discovering sensitive data as well as other assets. Extortion groups, like *LockBit*, look to move laterally as a means of maximizing their impact when they detonate their ransomware. Lateral movement also allows threat actors to avoid detection and maintain access within a target environment. Even if a threat actor's initial method of access is discovered and burned, a threat actor can still retain access due to their ability to burrow deeper in that environment with lateral movement.

Defenders should monitor for Windows event 4624 Logon Type 10. This event only occurs when a user accesses another system using RDP applications such Remote Desktop[24] or Terminal Services[25]. Also, monitor for network traffic connections over port 3389. This port is used to facilitate RDP

[19] https://attack.mitre.org/techniques/T1027/
[20] https://www.malwarebytes.com/blog/detections/trojan-malpack-themida
[21] https://research.nccgroup.com/2023/11/13/dont-throw-a-hissy-fit-defend-against-medusa/
[22] https://redcanary.com/threat-detection-report/techniques/obfuscated-files-information/
[23] https://www.sentinelone.com/cybersecurity-101/what-is-cobalt-strike/
[24] https://support.microsoft.com/en-us/windows/how-to-use-remote-desktop-5fe128d5-8fb1-7a23-3b8a-41e636865e8c
[25] https://www.pcmag.com/encyclopedia/term/terminal-services

connections. Defenders should also monitor newly created process such as mstsc.exe[26], which creates connections to RDP servers or other remote systems via valid accounts.

There are several mitigation strategies defenders can take to help thwart the use of RDP by threat actors within their organization. First and foremost, disable the use of RDP if it is not necessary for day to day operations. Disabling and removing unused applications and features is a means to reduce an organization's attack surface. If RDP is a necessary service, make sure to audit who is able to use this service. Remove unnecessary users and groups who do not need access to RDP. Since valid accounts can be used to facilitate RDP connections, it is important to use MFA as a means for authentication for remote logins.

Exploit Public-Facing Application

Vulnerability exploitation is a top initial access method. Adversaries often prioritize critical flaws which enable unauthenticated remote code execution (See Figure 7). Such flaws include the infamous Log4Shell,[27] legacy vulnerabilities, as well as more recent vulnerabilities such as CVE-2023-3519,[28] which allowed attackers to implant webshells on target networks.

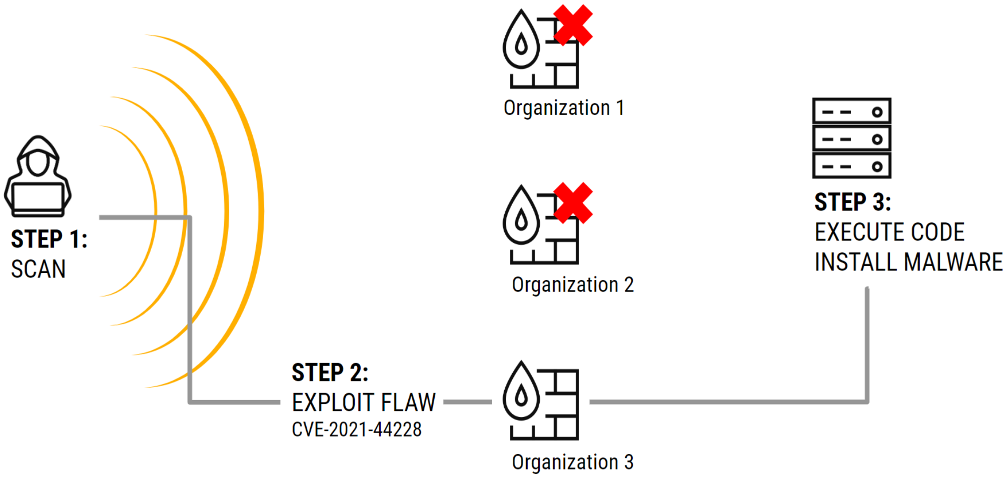


FIGURE 7: Example scenario of opportunistic vulnerability exploitation

Defenders should ensure that external-facing systems and services are patched regularly, prioritizing the exploited vulnerabilities listed in the United States Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities Catalog.[29] At least **10%** of public safety attackers, including the top extortion syndicates and IABs like *Kristina* and *mont4na*, targeted the same or similar flaws.

[26] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/mstsc

[27] https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[28] https://nvd.nist.gov/vuln/detail/CVE-2023-3519

[29] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Organizations should also make certain systems connected to the internet are not exploitable via services such as RDP or VPNs, which are frequently targeted for vulnerability exploitation. If these services must be available, ensure devices are properly configured and that security features are enabled. Ensure that ports are closed after vendor maintenance. As recently as 07 December 2023, adversaries used unpatched vulnerabilities to attack U.S. water suppliers and disrupt the water supply of an Irish municipality,[30] showcasing how exposed flaws can lead to disruptions for public safety organizations.

Maintaining up-to-date asset inventories can help defenders to identify internet-connected systems which might be exploited. An inventory of all organizational assets with an IP address (including IPv6), updated at least monthly, is recommended. Oftentimes, such assets are exploited without organizational knowledge, meaning services or systems existed unintentionally on the network perimeter. *CL0P* made headlines this year exploiting zero-day flaws in internet-connected instances of the MOVEit[31] file transfer service and SysAid[32] IT service automation software, of which instances organizations may or may not have been aware.

[30] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[31] https://www.cisa.gov/news-events/alerts/2023/06/07/cisa-and-fbi-release-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability

[32] https://therecord.media/clop-ransomware-gang-targets-new-zero-day

Appendix A: Detection Methods for Top Tradecraft

The following are detection methods for the top five observed tradecraft used by threat actors who target public safety entities. The detection methods are extrapolated from the MITRE ATT&CK framework and are broadly based so they are not tied to a specific security application or solution.

Helpful Security Tools for Detection:

- **Security Information and Event Manager (SIEM)**: Centralized log management application with the ability to set up alerts based on specific criteria available within logs
  - Helps Detect: Valid Accounts (T1078), Command and Scripting Interpreter (T1059), Remote Services: Remote Desktop Protocol (T1021.001), Phishing (T1566), Exploit Public-Facing Application (T1190)
- **Intrusion Detection System (IDS):** Monitors network traffic and reports suspicious and anomalous activity based on signatures
  - Helps Detect: Remote Services: Remote Desktop Protocol (T1021.001), Phishing (T1566), Exploit Public-Facing Application (T1190)
- **Endpoint Detection and Response (EDR)**: Monitors endpoints for cyber threats including malware, ransomware, and suspicious activity
  - Helps Detect: Valid Accounts (T1078), Command and Scripting Interpreter (T1059), Remote Services: Remote Desktop Protocol (T1021.001), Phishing (T1566), Exploit Public-Facing Application (T1190)

Valid Accounts (T1078)[33]

Data Source	Data Component	Detects
Logon Session	Logon Session Creation	Monitor for newly constructed logon behavior that may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. 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).
Logon Session	Logon Session Metadata	Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. 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.

[33] https://attack.mitre.org/techniques/T1078/

User Account	User Account Authentication	Monitor for an attempt by a user that may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Command and Scripting Interpreter (T1059)[34]

Data Source	Data Component	Detects
Command	Command Execution	Monitor command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script. Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used.
Module	Module Load	Monitor for events associated with scripting execution, such as the loading of modules associated with scripting languages (ex: JScript.dll or vbscript.dll).
Process	Process Creation	Monitor log files for process execution through command-line and scripting activities. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools. Also monitor for loading of modules associated with specific languages.
Process	Process Metadata	Monitor contextual data about a running process, which may include information such as environment variables, image name, user/owner, or other information that may reveal abuse of system features.
Script	Script Execution	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

[34] https://attack.mitre.org/techniques/T1059/

Obfuscated Files or Information (T1027)[35]

Data Source	Data Component	Detects
Command	Command Execution	Monitor executed commands and arguments for indicators of obfuscation and potentially suspicious syntax such as uninterpreted escape characters (e.g., ^). Also monitor command-lines for syntax-specific signs of obfuscation, such as variations of arguments associated with encoding.
File	File Creation	Detection of file obfuscation is difficult unless artifacts are left behind by the obfuscation process that are uniquely detectable with a signature. If detection of the obfuscation itself is not possible, it may be possible to detect the malicious activity that caused the obfuscated file (for example, the method that was used to write, read, or modify the file on the file system).
Module	Module Load	Monitoring module loads, especially those not explicitly included in import tables, may highlight obfuscated code functionality. Dynamic malware analysis may also expose signs of code obfuscation.
Process	Process Creation	Monitor for newly executed processes that may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.
Script	Script Execution	Monitor executed scripts for indicators of obfuscation and potentially suspicious command syntax, such as uninterpreted escape characters (e.g., ^). Also monitor commands within scripts for syntax-specific signs of obfuscation, such as encoded or otherwise unreadable blobs of characters.
Windows Registry	Key Creation	Monitor for the creation of Registry values that may highlight storage of malicious data such as commands or payloads.
WMI	WMI Creation	Monitor for the creation of WMI Objects and values that may

[35] https://attack.mitre.org/techniques/T1027/

		highlight storage of malicious data such as commands or payloads.

Remote Services: Remote Desktop Protocol (T1021.001)[36]

Data Source	Data Component	Detects
Logon Session	Logon Session Creation	Monitor for user accounts logged into systems associated with RDP (ex: Windows EID 4624 Logon Type 10). Other factors, such as access patterns (ex: multiple systems over a relatively short period of time) and activity that occurs after a remote login, may indicate suspicious or malicious behavior with RDP. Monitoring logon and logoff events for hosts on the network is very important for situational awareness. This information can be used as an indicator of unusual activity as well as to corroborate activity seen elsewhere.
Logon Session	Logon Session Metadata	Monitor authentication logs and analyze for unusual access patterns. A remote desktop logon, through RDP, may be typical of a system administrator or IT support, but only from select workstations. Monitoring remote desktop logons and comparing to known/approved originating systems can detect lateral movement of an adversary.
Network Traffic	Network Connection Creation	Monitor for newly constructed network connections (typically over port 3389) that may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Other factors, such as access patterns and activity that occurs after a remote login, may indicate suspicious or malicious behavior with RDP.
Network Traffic	Network Traffic Flow	Monitor network traffic for uncommon data flows that may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP).
Process	Process Creation	Monitor for newly executed processes (such as mstsc.exe) that may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions that spawn additional processes as the logged-on user.

[36] https://attack.mitre.org/techniques/T1021/001/

Phishing (T1566)[37]

Data Source	Data Component	Detects
Application Log	Application Log Content	Monitor for third-party application logging, messaging, and/or other artifacts that may send phishing messages to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[14][15] URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.
File	File Creation	Monitor for newly constructed files from phishing messages to gain access to victim systems.
Network Traffic	Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.
Network Traffic	Network Traffic Content	Monitor and analyze SSL/TLS traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.

Exploit Public-Facing Application (T1190)[38]

Data Source	Data Component	Detects
Application Log	Application Log Content	Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always

[37] https://attack.mitre.org/techniques/T1566/
[38] https://attack.mitre.org/techniques/T1190/

		succeed or may cause the exploited process to become unstable or crash. Web Application Firewalls may detect improper inputs attempting exploitation.
Network	Network Traffic Content	Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

Appendix B: 2023 Defender Checklist

The defender checklist is a set of recommendations organizations should implement to better protect themselves against the top observed tradecraft used by threat actors targeting public safety entities. The below recommendations are compiled from CISA's cybersecurity performance goals. The MITRE ATT&CK ID mitigated by the recommendation, cost and complexity of implementation are also provided within the recommendations.

- ☐ **Enforce Multi-Factor Authentication**
  Valid Accounts [T1078], Brute Force [T1110], Remote Services - Remote Desktop Protocol (T1021.001)
  Cost: $$ Complexity: Medium
  Organizations implement MFA for access to assets using the strongest available method for that asset. All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

- ☐ **Minimum Password Strength**
  Brute Force [T1110]
  Cost: $ Complexity: Low
  Organizations have a system-enforced policy that requires a minimum password length of 15 or more characters for all password-protected IT assets when technically feasible. Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.

- ☐ **Unique Credentials**
  Valid Accounts [T1078], Brute Force [T1110]
  Cost: $$ Complexity: Medium
  Organizations provision unique and separate credentials for similar services and asset access on IT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have passwords that are unique from all member user accounts.

- ☐ **No Exploitable Service on the Internet**
  Exploitation of Public-Facing Application [T1190], Remote Services - Remote Desktop Protocol (T1021.001)
  Cost: $ Complexity: Low
  Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented

to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.

□ **Asset Inventory**
Exploitation of Public-Facing Application [T1190]
Cost: $ Complexity: Medium
Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6). This inventory is updated on a recurring basis, no less than monthly for IT.

□ **Mitigating Known Vulnerabilities**
Exploitation of Public-Facing Application [T1190]
Cost: $ Complexity: Low
All known exploited vulnerabilities (listed in CISA's Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.

□ **Disable Macros by Default**
Phishing - Spearphishing Attachment [T1566.001]
Cost: $ Complexity: Low
A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.

□ **Email Security**
Phishing [T1566]
Cost: $ Complexity: Low
On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domain Based Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies.

□ **Change Default Passwords**
Valid Accounts - Default Accounts [T1078.001]
Cost: $ Complexity: Medium
Enforce an organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network.

In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices.

☐ **Revoking Credentials for Departing Employees**
Valid Accounts [T1078]
Cost: $ Complexity: Low
A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.

☐ **Separating User and Privileged Accounts**
Valid Accounts [T1078]
Cost: $ Complexity: Low
No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.

☐ **Detection of Unsuccessful (Automated) Login Attempts**
Brute Force [T1110]
Cost: $ Complexity: Low
All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis.

For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.

☐ **Use Antivirus Solutions**
Obfuscated Files or Information [T1027]
Cost: $$ Complexity: Low
Those running Microsoft Defender Antivirus can enable the "Block execution of potentially obfuscated scripts" attack surface reduction rule in either audit or enforcement mode. Enforcement and audit events are logged as event ID 1121 and 1122 in the Windows Defender (Operational) event log, respectively. An ID field with a value of 5beb7efe-fd9a-4556-801d-275e5ffc04cc will indicate that the obfuscation rule was fired.

Antivirus can also be used to automatically detect and quarantine suspicious files. Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10+ to analyze commands after being processed/interpreted.

☐ **Enforce Execution Prevention**
Command and Scripting Interpreter [T1059]
Cost: $$ Complexity: Medium
Use application control where appropriate. For example, PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., Add-Type).

☐ **Restrict PowerShell Usage**
Command and Scripting Interpreter: PowerShell [T1059.001]
Cost: $$ Complexity: Medium
It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions.Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.

When PowerShell is necessary, consider restricting PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.PowerShell JEA (Just Enough Administration) may also be used to sandbox administration and limit what commands admins/users can execute through remote PowerShell sessions.

☐ **Secure Sensitive Data**
OS Credential Dumping [T1003]
Cost: $$ Complexity: Medium
Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.

☐ **Log Collection**
Impair Defenses [T1562]
Cost: $$ Complexity: Medium
Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging.

☐ **System Backups**
Data Encrypted for Impact [T1486], Data Destruction [T1485]

Cost: $$ Complexity: Medium

All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year.

Appendix C: Assessment and Response Standard Operating Procedures

Levels of Analytic Confidence

High Confidence	**Moderate Confidence**	**Low Confidence**
Generally indicates judgments based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and still carries a risk of being wrong.	Generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.	Generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed.

Appendix D: Traffic Light Protocol for Disclosure

As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light Protocol (TLP), based upon the CISA Traffic Light Protocol guidance, which helps all members submit and leverage insights while being respectful of the submitting agency's preferences.

TLP:RED

RED: Restricted to the immediate PSTA participants only

- **When should it be used?** Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.
- **How may it be shared?** Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.

TLP:GREEN

GREEN: Restricted to the community

- **When should it be used?** Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
- **How may it be shared?** Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

TLP:AMBER

TLP:AMBER +STRICT

AMBER: Restricted to participants' organizations

- **When should it be used?** Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
- **How may it be shared?** Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. TLP: AMBER+STRICT Restricts sharing to the organization only.

TLP:CLEAR

CLEAR: Disclosure is not limited

- **When should it be used?** Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- **How may it be shared?** Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction.