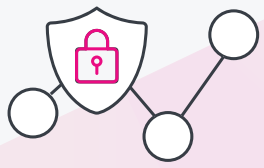
Top Cybersecurity Threat Detections With **Splunk and MITRE ATT&CK**

Classify, identify and assess threats with MITRE ATT&CK — monitor and respond with Splunk



splunk>

Table of Contents

Foreword

Cloud migrations and digital transformation are on the rise. To keep up, security leaders need to take a data-centric approach to securing their organization.

In this complex and unpredictable world, Splunk is foundational to keeping organizations like yours secure and resilient so you can detect and respond to threats faster, evolve with the needs of the business and innovate with confidence. Your organization's security and resilience depend upon your networks talking to each other, and your security tools analyzing all of your data and providing relevant insights.

To be resilient, we believe you need to be able to see your full infrastructure and all its data — at full fidelity. It's essential to creating security operations that are flexible enough to adapt to new threats, emerging technologies and ever-increasing data volumes.

You need faster detection and response techniques. You can do this by harnessing all of your data, automating processes that will identify new threats in record time and allowing your team to focus on their highest priorities.

This is how we improve our cyber resilience, which allows us to accelerate business growth, ensure privacy and compliance, and continue innovating.

We're invested in solving customer challenges in this evolving world by strengthening our security and observability offerings. This is why we've put together this list of MITRE ATT&CK tactics and corresponding threat detections and analytic stories from the Splunk threat research team (STRT) to combat the latest threats, so that you can stay resilient in the face of complexity and uncertainty.

Patrick Coughlin
VP, GTM Strategy & Specialization

As technologies evolve, cybercriminals have become even more sophisticated. Threat actors are constantly evolving their approach — from data encryption and exfiltration, to double extortion attacks that leak proprietary data if their demands aren't met.

If that wasn't bad enough, financially-motivated cybercrime is also on the rise, outpacing state-sponsored activity to account for more than 80% of interactive intrusions. This influx of malicious attacks is projected to cost organizations a hefty $10.5 trillion annually by 2025. Attackers are also taking advantage of vulnerabilities in supply chains, targeting the operational weaknesses of organizations and exploiting new attack surfaces opened up by cloud services.

To protect against these cyber threats, we need to reimagine and reinforce our security defenses, and be resilient in the face of ever-evolving threats. In this e-book, we examine some of the major threat tactics and techniques defined by the MITRE ATT&CK framework, and how security teams can be better prepared (and equipped) with the help of Splunk.

Enter MITRE ATT&CK

MITRE ATT&CK is a knowledge base of common tactics, techniques and procedures (TTPs) that documents the ways in which threat actors operate, ultimately serving as a playbook of TTPs seen and reported out in the wild. Organizations refer to MITRE ATT&CK to classify attacks, assess risk and improve their overall security posture to gain a better understanding of adversaries' behavior, so that they can identify and implement relevant threat detections.

In essence, ATT&CK is a standardized, easily accessible and globally acknowledged threat language that security specialists can look to for threat intelligence and to help bolster their security posture.

The MITRE ATT&CK framework can also help:

- Inform the security operations center (SOC) on how to prioritize alerts and detections.
- Identify and assess risks, control gaps and risk appetite.
- Provide a framework for security governance and maturity.
- Recommend new data sources based on quantifiable risk reduction.
- Sharpen a view of attack paths, improving a security team's knowledge and skills.

The nirvana solution: ATT&CK + Splunk

As threats evolve, so does the ATT&CK framework. To keep up with new and emerging threats, security teams need to adapt and update their threat detection and response capabilities at the same rate as their adversaries. Splunk Enterprise Security (ES), Splunk Security Essentials (SSE), and Splunk Enterprise Security Content Updates (ESCU) help organizations prepare for threats by mapping MITRE ATT&CK to Splunk's Analytic Stories — security guides that include narrative background on attack techniques and threats accompanied by Splunk searches, machine learning and security orchestration, automation and response (SOAR) playbooks.

These powerful components work together to help you detect, investigate and respond to signs of threats in your environment. Periodic updates help you continually uplevel your defenses. Analytic Stories are complements to traditional indicators of compromise (IOCs), which are lagging and often ephemeral. By the time you detect them, attackers have usually changed their URLs, IP addresses and other artifacts, making the IOCs obsolete. In contrast, ESCU helps you monitor for common/perennial adversary tactics and techniques. Once you've identified signs of these threats in your environment, you can use searches and playbooks to help you decide whether to investigate further.

MITRE ATT&CK use cases

Different applications for the MITRE ATT&CK taxonomy within Splunk

Below are some of the ways the ATT&CK framework can be applied within Splunk:

- **Mapping defense controls**
  Security teams can develop a clear understanding of defense tools, systems and strategies when they're referenced against the ATT&CK tactics and techniques and their associated threats. MITRE ATT&CK tags are easily applied to Splunk Enterprise Security correlation searches to annotate and provide a deeper understanding of the events.

- **Threat hunting**
  Security teams can map defenses to ATT&CK to identify critical gaps in their security infrastructure, which can help detect previously overlooked threat activity. Using Splunk Security Essentials and the MITRE ATT&CK map, threat hunters can identify gaps in coverage and then drive further development for detections, or generate ideas about new searches or use cases in order to plug existing holes.

- **Investigating**
  Incident response can refer to the ATT&CK framework to better address potential vulnerabilities, validating certain measures while detecting misconfigurations and other operational flaws.

- **Identifying threat actors and groups**
  Security teams can align malicious actors and groups with associated documented behaviors.

Meet Splunk's threat research team

None of this would be possible without the Splunk threat research team, who works tirelessly to enhance Splunk's security offerings with out-of-the-box use cases, detection searches and playbooks. Every two weeks, their research is bundled into a content release, and then shared with the Splunk community and beyond. This content ranges from threat detections to step-by-step guidelines and is accessible within Splunk. Gone are the days of writing custom searches and testing new detections — now, pre-packaged detections can be implemented to speed up investigations. This research is integral to the quick containment and remediation of a threat and helps free up time for security teams to focus on critical tasks.

Bottom line? Splunk's threat research helps security teams get the most out of their Splunk investment, seamlessly integrating and mapping threat detections to the MITRE ATT&CK framework for greater security coverage, and to also amplify certain security capabilities with expert knowledge and research around the latest threats and security trends.

The end goal of using MITRE ATT&CK in your Splunk environment is to provide further insight and value to your existing deployment against the backdrop of the ATT&CK framework. In the constantly changing world of security needs and detections, building this framework helps by basing current and future work on relevant, real-world applications.

MITRE ATT&CK Tactics

Ready to take your threat response to the next level? Below we break down the major MITRE ATT&CK threat tactics and techniques, along with examples of how to respond with Splunk.

Reconnaissance (TA0043)

Threat tactic: to gather information

Why these threats exist

Reconnaissance is exactly what it sounds like — an attack that's centered on gathering and sourcing information relevant to a target and their system(s) and/or organization. This can involve a whole host of techniques, including social engineering, network infiltration and physical surveillance. The sourced information usually includes details about the organization's infrastructure, as well as key staff and personnel. This information is leveraged by the threat actor to assist in other phases of the cyber kill chain — a series of steps, comparable to MITRE ATT&CK, that outlines an attack from reconnaissance to data exfiltration, as defined by the global security company Lockheed Martin.

How these threats are executed

The goal is for threat actors to obtain information about the victim's identity, as well as information about the networks they operate on, including administrative data and specifics regarding the organization's operations.

To do this, threat actors will often interact directly with the system through techniques like automated/port scanning, packet sniffing and ping sweeps. This is referred to as "active recon," and is generally faster and more accurate than a "passive" approach, where the attacker queries information over the internet — including public information services such as "Whois" queries, using tools like Wireshark and Shodan, or methods like OS fingerprinting.

In order to break down and address the potential stages of this tactic, the techniques identified by the MITRE ATT&CK framework include the initial collection of information, determining the network range of the target, finding access points and open ports, as well as mapping the organization's network. Essentially, these are all the steps that support the collection of source information, better informing the adversary to select or identify their target.

How to detect and respond with Splunk

Splunk Threat Detection: Attacker Tools on Endpoint

- **Splunk Analytic Story**
  Monitor for Unauthorized Software, XMRig, SamSam Ransomware, Unusual Processes
- **MITRE ATT&CK Tactics**
  Reconnaissance, Credential Access, Defense Evasion
- **MITRE ATT&CK Techniques**
  Match Legitimate Name or Location, Masquerading, OS Credential Dumping, Active Scanning
- **Kill Chain Phase**
  Installation, Command & Control, Actions on Objectives
- **How it works**
  This threat detection looks for the execution of commonly used attacker tools on an endpoint.

Execution (TA0002)

Threat tactic: to run malicious code

Why these threats exist

Threat execution refers to the techniques used by an attacker to run or control malicious code on a local or remote system. Techniques that run malicious code are often paired with a number of other tactics, like infiltrating a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does remote system discovery.

How these threats are executed

Adversaries may abuse command and script interpreters to execute commands, like PowerShell, AppleScript, Unix, Windows and Python. These interfaces and languages allow users to interact with computer systems, and are a common feature across many different platforms. Attackers can use them to discover information, execute code, open windows, send keystrokes and interact with almost any open application locally or remotely. Some command shells allow attackers full access to almost any aspect of the target's system.

Containers are another way for attackers to run code and control systems. By abusing a container administration service, they can control an environment's containers remotely. And deploying a container into an environment allows them to run code and evade defenses from the inside.

Another execution tactic includes abusing task scheduling to facilitate initial or recurring execution of malicious code at a specified date and time. Adversaries may also deploy malicious payloads via shared modules or gain access to third-party software suites installed within an enterprise network. They also abuse system services or daemons to execute commands or programs and by using social engineering to lure a user to take specific actions, like clicking on a bogus link or downloading a malicious file.

How to detect and respond with Splunk

Splunk Threat Detection: Linux Decode Base64 to Shell

- **Splunk Analytic Story**
  Linux Living Off the Land
- **MITRE ATT&CK Tactics**
  Defense Evasion, Execution
- **MITRE ATT&CK Techniques**
  Obfuscated Files or Information, Unix Shell
- **Kill Chain Phase**
  Delivery, Exploitation
- **How it works**
  This threat identification searches for base64 being decoded and passed to a Linux shell. Base64 encoding is often abused and used to carry confusing malicious payloads disguised as legitimate code.

Persistence (TA0003)

Threat tactic: to maintain a foothold

Why these threats exist

Once a threat actor gets into a target's systems, persistence invariably pays off — trumping almost every other tactic in an attacker's playbook. To successfully maintain their foothold, the attacker must preempt any number of interruptions that could cut off their access, including system restarts or updated credentials. This tactic covers access, action or configuration changes that allow the perpetrator to move laterally (and, above all, covertly) within the compromised account or system, replacing or hijacking legitimate code with their own.

How these threats are executed

One technique adversaries use to maintain access is account manipulation. They may modify credentials or permission groups and then perform iterative password updates to bypass password duration policies. They may also add and grant account credentials, modify secure socket shell (SSH) authorized keys or register devices to accounts they control.

They also use scripts that are automatically executed at boot or logon initialization to establish persistence. Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

Adversaries can also create a new account to maintain access to victim systems, whether it's a local, domain or cloud account. They also modify system-level processes to repeatedly execute malicious payloads using launch agents, system services, Windows services and launch daemons.

How to detect and respond with Splunk

Splunk Threat Detection: O365 Added Service Principal

- **Splunk Analytic Stories**
  Office 365 Detections, Cloud Federated Credential Abuse
- **MITRE ATT&CK Tactics**
  Persistence
- **MITRE ATT&CK Techniques**
  Cloud Account, Create Account
- **Kill Chain Phase**
  Exploitation
- **How it works**
  This threat detection identifies the creation of a new setting by alerting about a specific correlating event. Though the creation of a new federation is not necessarily malicious, the event needs to be followed closely, as it could indicate credential abuse.

Privilege Escalation (TA0004)

Threat tactic: to gain higher-level permissions

Why these threats exist

After bad actors enter and explore a network with unprivileged access, sometimes they have to go even further and get elevated permissions to fulfill their objectives. The techniques they use to gain those permissions are grouped under privilege escalation. Common approaches involve taking advantage of system weaknesses, misconfigurations and vulnerabilities.

How these threats are executed

By taking advantage of the vulnerabilities that already exist in the target's system, adversaries can gain elevated access such as SYSTEM/root level or local administrator status, a user account with admin-like access, or a user account with access to a specific system or to perform a specific function. The techniques used to gain higher-level permissions often overlap with persistence techniques, as features that let a hacker persist can also execute in an elevated context.

Threat actors can circumvent mechanisms designed to control elevated privileges using various methods to take advantage of built-in control mechanisms in order to escalate privileges on a system. Some of those methods include: abusing configurations where an application has the user identity and group identity set in order to get code running in a different (and possibly more privileged) user's context, bypassing user account control (UAC) mechanisms, and performing sudo caching and/or using the sudoers file.

Adversaries may also modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. By configuring system settings, they can automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges. Other techniques include tampering with system-level processes to repeatedly execute malicious payloads, modifying the configuration settings of a domain and using system mechanisms that trigger execution based on specific events.

How to detect and respond with Splunk

Splunk Threat Detection: Azure AD Successful PowerShell Authentication

- **Splunk Analytic Stories**
  Azure Active Directory Account Takeover
- **MITRE ATT&CK Tactics**
  Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **MITRE ATT&CK Techniques**
  Valid Accounts, Cloud Accounts
- **Kill Chain Phase**
  Exploitation
- **How it works**
  This threat detection identifies a successful authentication event against an Azure AD tenant using PowerShell commandlets. This behavior is uncommon for regular, non-administrative users. After compromising an account in Azure AD, attackers and red teams alike will perform enumeration and discovery techniques. One method of executing these techniques is leveraging the native PowerShell modules.

Defense Evasion (TA0005)

Threat tactic: to avoid being detected

Why these threats exist

Defense evasion is an enterprise tactic to avoid detection throughout the different stages of an attack. This covers a broad range of techniques, like uninstalling or disabling the target's security software, and obfuscating or encrypting data and scripts. To evade detection, threat actors will also leverage and abuse trusted processes to hide and masquerade their malware.

How these threats are executed

Bad actors try to evade detection in different ways, depending on the stage and type of attack. They exploit any and all vulnerabilities in the victim's environment, abuse credentials, modify permissions and attributes, hijack operating systems, inject code and hinder or disable security tools and other defensive mechanisms. Along the way, they do everything they can to hide and delete evidence of their presence and behavior in the target's environment.

To evade defenses, adversaries modify settings, access and other components of the victim's environment. By modifying the configuration settings of a domain, they can gain access to a centralized way to manage how computers and accounts can act and interact with each other on the network. By modifying access tokens, they can operate as different users or system security contexts to perform actions and bypass access controls. They also modify and impair defensive mechanisms like firewalls and antivirus protection, as well as other detections that could reveal their activity.

In addition to modifying permissions and attributes, adversaries try to hide evidence of their behavior by abusing features of operating systems and by masquerading by manipulating the features of their artifacts to make them appear legitimate. Threat actors may also abuse utilities that allow for command execution to bypass security restrictions, executing their own malicious payloads by hijacking the way operating systems run programs — and that's only the start.

How to detect and respond with Splunk

Splunk Threat Detection: Circle CI Disable Security Job

- **Splunk Analytic Story**
  Dev Sec Ops
- **MITRE ATT&CK Tactics**
  Persistence
- **MITRE ATT&CK Techniques**
  Compromise Client Software Binary
- **Kill Chain Phase**
  Actions on Objectives
- **How it works**
  This threat detection looks for CircleCI jobs on the build phase that have been disabled and provides the analyst with the job name, the user which disabled the CI job. This action would be done by an attacker to avoid defenses or disrupt services.

Credential Access (TA0006)

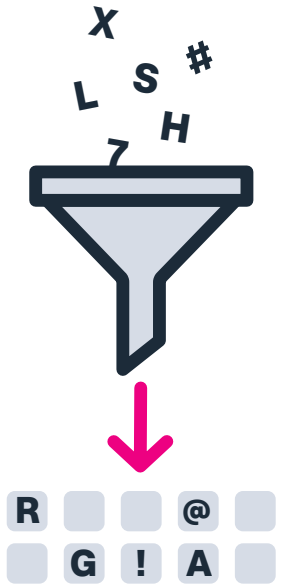
Threat tactic: to steal account details

Why these threats exist

Credential access consists of techniques for stealing account details like usernames and passwords. There are many techniques used to get credentials, including keylogging and credential dumping. In addition to being extremely effective, this type of attack is much harder to find than other types of initial access techniques because it will look like the legitimate use of a user account. This is an extremely cheap and efficient attack to gain access to user accounts and information.

How these threats are executed

In a large-scale credential stuffing attack, the attacker will set up a bot that's able to automatically log into multiple user accounts simultaneously, all the while faking different IP addresses. The stolen credentials will then be run against a long list of websites, checking for successful logins, personally identifiable information, credit cards or other valuable data from the compromised accounts. By running this process in parallel across multiple channels, the need to repeatedly log into a single service is reduced. Account information is also retained for future use, including phishing attacks or other transactions enabled by the compromised service.



How to detect and respond with Splunk

Splunk Threat Detection: 0365 Disable MFA

- **Splunk Analytic Story**
  Office 365 Detections
- **MITRE ATT&CK Tactics**
  Credential Access, Defense Evasion, Persistence
- **MITRE ATT&CK Techniques**
  Modify Authentication Process
- **Kill Chain Phase**
  Exploitation
- **How it works**
  This threat detection identifies when multifactor authentication has been disabled, what entity performed the action and against what user.

Discovery (TA0007)

Threat tactic: to figure out your environment

Why these threats exist

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help hackers observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

How these threats are executed

Cyber adversaries are better than ever at infiltrating systems. And once they gain access to a company's network, hackers often stay in the shadows to conduct reconnaissance. They silently watch and learn how to exploit security weaknesses like default settings to achieve their objectives by surprise. In the MITRE ATT&CK framework, this digital prowling is known as "discovery."

Smart businesses can blunt the impact of a breach by denying intruders this opportunity to get oriented. Many business leaders are familiar with attackers' common methods for breaching systems. Understanding this discovery phase of a cyberattack can make you more prepared to counter such activities and downstream consequences. The actions to take are tactical but they can make all the difference by enabling businesses to stay on strategy and sustain operations.

How to detect and respond with Splunk

Splunk Threat Detection: Windows AdFind Exe

- **Splunk Analytic Story**
  NOBELIUM Group, Domain Trust Discovery
- **MITRE ATT&CK Tactics**
  Discovery
- **MITRE ATT&CK Techniques**
  Remote System Discovery
- **Kill Chain Phase**
  Exploitation
- **How it works**
  This threat detection looks for the execution of adfind.exe with command-line arguments that it uses by default. Specifically the filter or search functions.

Collection (TA0009)

Threat tactic: to source data relevant to the target

Why these threats exist

No matter how cunning, threat actors can't go at it alone; to successfully conduct an attack, they need to tap into — or, more aptly, collect — key information as part of their threat campaign. This tactic is known as "collection," and involves a number of techniques around the sourcing of sensitive information and/or proprietary data. Eventually, the data collected is exfiltrated and leveraged by the attacker during other phases of the attack. Common target sources include drive types, browsers, audio, video and email, with collection methods ranging from screenshots to keyboard input.

How these threats are executed

There are infinite ways for a threat actor to collect digital (or physical) sensitive and personal information to support their operations. This can look like tapping into browsers, audio devices, hacking into email accounts, stealing login credentials and more. Once the attacker has gained access to the target's system, they can then target vulnerabilities and move laterally across the network as a means for collecting and relaying data to and from the compromised system.

How to detect and respond with Splunk

Splunk Threat Detection: Anomalous Usage of 7zip

- **Splunk Analytic Story**
  Cobalt Strike, NOBELIUM Group
- **MITRE ATT&CK Tactics**
  Collection
- **MITRE ATT&CK Techniques**
  Archive Via Utility, Archive Collected Data
- **Kill Chain Phase**
  Exploitation
- **How it works**
  The threat detection identifies a 7z.exe spawned from Rundll32.exe or Dllhost.exe. It's assumed that the adversary has brought in 7z.exe and 7z.dll. Additional coverage may be required to identify the behavior of renamed instances of 7z.exe.

Lateral Movement (TA0008)

Threat tactic: to move through your environment

Why these threats exist

At this stage, the threat actor is attempting to quickly (yet thoroughly) move through your environment. And they aim to cover the most ground by any means possible once they have infiltrated the victim's network.

In order to carry out their mission, bad actors need to explore the network to locate and gain access to their target. In this stage, they apply numerous techniques aimed at entering and controlling remote systems, so achieving their malicious objectives often involves cycling through multiple systems and accounts through lateral movement to install remote access tools. To accomplish this mission, they'll often use legitimate credentials with native network and operating system tools to stealthily cover their whereabouts.

How these threats are executed

Bad actors rely on a variety of techniques to stealthily move themselves across an environment. Once they've infiltrated a network, they may exploit a software vulnerability — often a flaw in a program, service or within the operating system software itself — to gain unauthorized entry into other internal systems.

Adversaries may also use internal spear phishing techniques to gain access to additional information or exploit other users within the same organization who already have access to accounts or systems within the environment. In this case, they often try to trick an unsuspecting person into clicking on a malicious link or downloading an infected attachment, which serves as a springboard for lateral movement to other parts of the network.

Bad actors can alternatively hijack users' pre-existing sessions to move laterally throughout a network, subsequently using valid credentials to log into a service specifically designed to accept remote connections. They may also use alternate authentication material, such as password hashes, Kerberos tickets and application access tokens, to bypass normal system access controls and move laterally.

How to detect and respond with Splunk

Splunk Threat Detection: Mimikatz PassTheTicket CommandLine Parameters

- **Splunk Analytic Story**
  Active Directory Kerberos Attacks
- **MITRE ATT&CK Tactics**
  Defense Evasion, Lateral Movement
- **MITRE ATT&CK Techniques**
  Use Alternate Authentication Material, Pass the Ticket
- **Kill Chain Phase**
  Exploitation
- **How it works**
  The following analytic looks for the use of Mimikatz command line parameters used to execute "PassTheTicket" attacks. Red teams and adversaries alike may use the pass the ticket technique by taking advantage of stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls.

Command and Control (TA0011)

Threat tactic: to control compromised systems

Why these threats exist

In the command and control phase, malicious attackers attempt to communicate with the very systems that they infected and compromised. Their objective is to take complete control of their targets and use their targets for nefarious purposes, often through phishing attacks, vulnerable software or security holes in browser plug-ins.

Once threat actors infect a device or system on the network, they employ a series of techniques to communicate with the compromised systems within a victim network. It's also not uncommon in this phase for adversaries to mimic normal traffic levels by using application layer protocols to avoid triggering security alerts, evade network filtering and generally dodge any other unwanted scrutiny.

How these threats are executed

The goal of this phase is to establish communication between the infected machine and the attacker's server to deliver a set of instructions aimed at taking complete control of the entire network or system. Once attackers successfully compromise a device, the infected computer then carries out commands from their command server to connect to as many devices as possible.

However, as they infect an entire network, adversaries also have to cover their tracks, which compels them to use a host of stealth techniques that mask command and control activities. One of these techniques is embedding commands in the traffic between the client and server of application layer protocols, such as web, file transfer, mail and DNS protocols, to blend in with existing traffic. Another includes communication via removable media, where adversaries can execute command and control functions on potentially disconnected networks using devices like USB drives to transfer commands between compromised systems.

Adversaries may also discreetly take over a network by simply adding junk data to protocol traffic, using steganography or impersonating legitimate protocols. Also, rather than relying on any inherent protections, they could employ a known encryption algorithm to conceal command and control traffic.

How to detect and respond with Splunk

Splunk Threat Detection: TOR Traffic

- **Splunk Analytic Story**
  Prohibited Traffic Allowed or Protocol Mismatch, Ransomware, Command and Control
- **MITRE ATT&CK Tactics**
  Command and Control
- **MITRE ATT&CK Techniques**
  Application Layer Protocol, Web Protocols
- **Kill Chain Phase**
  Command and Control
- **How it works**
  This threat detection looks for network traffic identified as The Onion Router (TOR), a benign anonymity network that can be abused by malicious attackers for a variety of nefarious purposes.

Exfiltration (TA0010)

Threat tactic: to steal proprietary data

Why these threats exist

In the exfiltration stage, adversaries employ a variety of sophisticated methods to steal data from your network. Once they've collected all the desired data, adversaries often find creative ways to stealthily package it, including compression and encryption techniques, to avoid detection as they lift it from your network. Some of their tactics for absconding with data under the radar have included transferring it over their command and control channels or putting size limits on the transmission.

How these threats are executed

Adversaries have a variety of tricks up their sleeves for exfiltrating sensitive data from an organization. One of the means is by using automated processes after the "collection" phase that transfers it out of the system. Another tactic bad actors use includes moving it in fixed size chunks or limited packet sizes below certain thresholds, as opposed to whole files, so as to avoid triggering various network transfer and security alerts.

Threat actors could alternatively rely on existing, legitimate external web services to exfiltrate data, as popular web services often tend to provide a significant amount of cover simply because the targeted organization was likely already using the services prior to the attack.

Adversaries may also attempt to exfiltrate data via a physical medium, such as a removable USB drive, external hard drive, cell phone, MP3 player or other common storage device, which would then become the final exfiltration point before the hackers altogether removed the data from the targeted system. They may also pilfer data via scheduled transfers performed only at certain times of the day or at certain intervals, which provide a perfect foil by blending into normal traffic patterns.

How to detect and respond with Splunk

Splunk Threat Detection: Windows PowerShell Connect to Internet With Hidden Window

- **Splunk Analytic Story**
  Log4Shell CVE-2021-44228, Malicious PowerShell, HAFNIUM Group
- **MITRE ATT&CK Tactics**
  Exfiltration
- **MITRE ATT&CK Techniques**
  Automated Exfiltration
- **Kill Chain Phase**
  Exploitation
- **How it works**
  This threat detection identifies PowerShell commands using the WindowStyle parameter to hide the window on the compromised endpoint. This combination of command-line options is suspicious because it overrides the default PowerShell execution policy, attempts to hide its activity from the user and connects to the internet.

Impact (TA0040)

Threat tactic: to manipulate, interrupt or destroy your systems and data

Why these threats exist

In this phase, the adversary is actively trying to manipulate, interrupt or destroy targeted systems and data. The impact phase consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact include destroying or tampering with data. In some cases, business processes might appear intact and running smoothly on the surface — however, in reality, attackers may have covertly altered them to access, steal or compromise data; conduct cyberespionage, and otherwise cause disruptions and wreak havoc on targeted systems.

How these threats are executed

AAltogether, the impact stage consists of a wide range of techniques that adversaries use to disrupt, compromise, destroy and manipulate the integrity and availability of network operations, processes and systems, devices and data, as well as the surrounding environment. These techniques are particularly dangerous as they can result in instantaneous disruption to processes, or may result in more long-term damage to the environment or systems.

Among their techniques, adversaries may interrupt system and network resources by blocking, deleting or locking down access to accounts, or by manipulating credentials to gain unauthorized access and removing access by legitimate users.

Adversaries can also aim to destroy data and files — either on specific systems or en masse — to interrupt systems, services and network resources as well as overwrite files on local and remote drives to render stored data irrecoverable. This includes manipulating data by inserting, deleting or changing it in an attempt to influence external outcomes, hide activity or affect a business process or decision.

Destruction can also include defacement of both internal and external content and web properties, which can in turn cause loss of revenue, credibility in the marketplace and reputation. To that end, adversaries may execute denial of service attacks that degrade or altogether block the availability of websites, email services, DNS and web-based applications by choking the system with traffic and causing it to crash.

How to detect and respond with Splunk

Splunk Threat Detection: Ransomware Notes Bulk Creation

- **Splunk Analytic Story**
  Clop Ransomware, DarkSide Ransomware, BlackMatter Ransomware
- **MITRE ATT&CK Tactics**
  Impact
- **MITRE ATT&CK Techniques**
  Data Encrypted for Impact
- **Kill Chain Phase**
  Exploitation
- **How it works**
  This threat detection identifies a large number of instances of ransomware notes to the infected machine. This behavior is a good indication of whether the ransomware note filename is new for the security industry or the ransomware note filename is not in your ransomware lookup table list for monitoring.

Ready to kickstart your security operations?

Check out Splunk Security Essentials, and start solving hundreds of different security challenges for free.

Learn More

splunk>

22-26440-Splunk-Cybersecurity Threat Detections with Splunk _ Mitre ATT_CK_SS-107