CYBER STASH

Crucial Cybersecurity Wisdom

Mastering the Art of Effective Adversary Threat Detection

eclipse

Preface

Welcome to the Future of Cybersecurity!

The realm of cybersecurity is in a state of perpetual flux. The adversaries we face continually adapt and evolve, employing increasingly sophisticated tactics to breach our digital fortresses. In response, defenders must also evolve, embracing a paradigm shift in threat detection.

This whitepaper challenges conventional wisdom, presenting a strategic framework that empowers organisations to fortify their defenses while optimising their resources.

Our journey begins by dispelling the misconception that effective behavioural detection demands exorbitant investments. Instead, we advocate a methodical shift in perspective, urging organisations to refocus their efforts on the Top 20 Most Common Adversary Techniques. These techniques are not mere abstractions but the frontline battlegrounds where real-world cyber threats unfold.

To guide you through this transformation, we have meticulously crafted a framework grounded in the core principles of Prevalence, Choke Points, and Actionability. We explore each of these facets to equip you with a holistic understanding of how to master threat detection in the digital age.

But we don't stop there. We also delve into real-world attack scenarios, demonstrating how the Top 20 detection rules would have detected known threats. These tangible examples underscore the practical relevance of our framework.

As we embark on this journey together, remember that you are not just reading words on a page; you are unlocking a vision for the future of cybersecurity. We invite you to explore, contemplate, and embrace the knowledge within these pages to fortify your defenses and outmanoeuvre the ever-evolving adversary.

Welcome to the future of cybersecurity, where efficacy and resource optimisation reign supreme, and where the defenders are poised to lead the way.

.

Unlock the full potential of your cybersecurity defense and embark on a journey of unparalleled protection. We extend a warm and wholehearted invitation for you to connect with us at https://www.cyberstash.com, where your peace of mind and security await. Let's fortify your defenses together.

The Discerning Nature of "20"

The choice of "20" was derived from a comprehensive review of numerous real-world attacks. It represents the outcome of a thorough evaluation, signifying the balance where monitoring techniques achieve maximum efficacy while optimising resources. This number remains adaptable, responsive to the dynamic threat landscape. Initially encompassing around 16 core techniques, the final count emerged from extensive analysis and alignment with established security paradigms, shaped by the collective knowledge of the security community.

Strategic Prioritisation: Prevalence, Choke Points, and Actionability

Our methodology for the selection of the Top 20 Techniques is underpinned by a holistic approach that considers three vital factors: Prevalence, Choke Points, and Actionability. This approach is in alignment with the mission of *The Center for Threat-Informed Defense*, an esteemed R&D organisation dedicated to advancing the state of the art and the state of the practice in threat-informed defense. These components provide the scaffolding for a framework that empowers defenders to tailor their detection tools and strategies to the most pertinent and influential techniques.

Prevalence: A Glimpse into Real-World Attacks

Prevalence, within the context of MITRE ATT&CK, denotes the frequency with which an attacker employs a specific technique over a defined period. This methodology provides us with the acumen to discern the techniques actively witnessed during cyber intrusions. Armed with this knowledge, defenders can adeptly hone their detection tools to concentrate on the techniques characterised by the highest frequency and contemporaneity. Prevalence metrics are informed by data culled from the Sightings Ecosystem, where each sighting embodies one or more ATT&CK techniques wielded by adversaries against, or in targeting, victim infrastructure.

Choke Points: Unveiling Attack Chain Vulnerabilities

Choke Points, within the realm of the MITRE ATT&CK framework, constitute specific techniques where multiple other techniques converge or diverge. These choke points wield a unique stature in the adversary's arsenal, as their elimination would fundamentally disrupt the execution of an attack. An in-depth analysis of choke points empowers defenders to pinpoint the critical techniques indispensable for the success of an attack. These techniques act as common denominators, even within otherwise disparate attack scenarios. For instance, T1047 (WMI) can serve as a choke point due to the multitude of other techniques that adversaries can execute after initiating WMI. Safeguarding against malicious WMI utilisation can profoundly restrict the potential attack paths available to adversaries.

Actionability: An Empowerment Avenue for Defenders

Actionability, in the MITRE ATT&CK context, encapsulates the defender's opportunity to detect or mitigate each ATT&CK technique, based on publicly available analytics and security controls. Comprehending the actionability of a technique is pivotal, for it enables defenders to respond to incidents with alacrity and effectiveness, potentially thwarting incidents altogether. Actionability is a pivotal cornerstone in the defender's toolkit, empowering them to take proactive measures in safeguarding their infrastructure.

The Top 20 Most Common Adversary Techniques

In the realm of cybersecurity, knowledge is power. To develop a deeper understanding of the Top 20 most frequently observed ATT&CK techniques, we must delve into each one and comprehend how adversaries employ them to infiltrate, compromise, and manoeuvre within victim environments. The following is a detailed breakdown of each of these techniques:

1. Command Line Interface / PowerShell (T1059)

This technique involves the execution of commands through the command line or PowerShell. Adversaries commonly use this technique to run malicious scripts or commands, exploiting the legitimate functionalities of these interfaces to avoid detection.

2. Valid Account Misuse (T1078)

In Valid Account Misuse, adversaries utilise legitimate accounts, often with elevated privileges, to move laterally within a network. This technique allows them to blend in with authorised user activity, making detection more challenging.

3. System Information Discovery (T1082)

Adversaries leverage System Information Discovery to gather data about the target system. This information helps them to identify vulnerabilities and weaknesses that can be exploited in subsequent stages of the attack.

4. Registry Run Keys (T1060)

The Registry Run Keys technique involves manipulating Windows Registry keys to maintain persistence. By adding malicious entries, adversaries ensure that their malware runs automatically at system startup.

5. Credential Dumping (T1003)

Credential Dumping is a pivotal technique for adversaries seeking access to sensitive information. They extract login credentials from compromised systems, enabling them to escalate privileges and move laterally.

6. Remote Services (T1021)

Adversaries exploit Remote Services to access and manipulate services on remote systems. By targeting services with known vulnerabilities, they can compromise systems and establish a foothold.

7. Process Injection (T1055)

Process Injection allows adversaries to inject malicious code into legitimate processes, evading traditional security measures. This technique is used to run malicious code within the context of a trusted process.

8. Scheduled Tasks (T1053)

Scheduled Tasks is a persistence technique that adversaries employ to maintain access to a compromised system. By creating scheduled tasks, they ensure that their malware or backdoor runs at specific intervals.

9. Signed Binary Proxy Execution (T1218)

In Signed Binary Proxy Execution, adversaries use signed binaries to proxy execution of malicious payloads. This technique helps them bypass application whitelisting and other security controls.

10. Boot/Logon Autostart Execution (esp. Shortcut Modification) (T1547)

This technique involves modifying shortcuts or autostart locations on a system to ensure the execution of malicious code during system boot or user logon.

11. Windows Management Instrumentation (WMI) (T1047)

Adversaries leverage Windows Management Instrumentation (WMI) to automate administrative tasks and execute code on remote systems. This technique provides extensive control over compromised systems.

12. Masquerading (T1036)

Masquerading is a technique where adversaries disguise malicious files or processes to appear as legitimate entities. This tactic aims to evade detection by security tools.

13. Hijack Execution Flow (T1574)

Hijack Execution Flow involves manipulating the flow of execution in a legitimate application to divert it toward malicious code. Adversaries use this technique to control the behavior of compromised applications.

14. Obfuscated Files or Information (T1027)

Adversaries often obfuscate their files or information to conceal their malicious intent. By employing various obfuscation techniques, they aim to evade detection by security tools.

15. Virtualisation/Sandbox Evasion (T1497)

Virtualisation/Sandbox Evasion is employed by adversaries to detect the presence of a virtualised environment or sandbox and modify their behavior to avoid detection.

16. Remote File Copy (T1544)

Adversaries employ Remote File Copy to transfer files from one system to another within a network. This technique facilitates lateral movement and the distribution of malicious payloads.

17. Disabling Security Tools (T1089)

This technique involves disabling or tampering with security tools and mechanisms on a victim's system. By deactivating security controls, adversaries can operate without interference.

18. Exploit Public Facing Application (T1190)

Adversaries seek to exploit vulnerabilities in public-facing applications to gain initial access to a network. These applications often serve as entry points for attackers.

19. Remote Access Software (e.g., RDP) (T1219)

Remote Access Software allows adversaries to access victim systems remotely. Commonly used tools like Remote Desktop Protocol (RDP) provide attackers with a means to control systems from a distance.

20. Webshells (T1505)

Webshells are malicious scripts or programs uploaded to a web server. They grant adversaries remote access and control over the compromised system through a web-based interface.

The Nuances of Hunting with the Top 20 Rules

When utilising the Top 20 rules for hunting, there are additional considerations to keep in mind. The rules, when employed for hunting, may need to be "relaxed." This implies detecting any use of the technique rather than solely searching for specific attacks, which might inadvertently lead to the overlooking of some threats. In the hunting context, the focus is not only on the presence of an attack but also on the techniques employed by adversaries. This dynamic approach ensures that while specific attack patterns may evolve, the focus on the most frequently observed techniques remains unwavering.

Special Consideration: Tailoring the Top 20 for Specialised Environments

Organisations operating in specialised attack surface areas, such as those involved in Operational Technology (OT) and Industrial Control Systems (ICS), may need to tailor the Top 20 framework to their specific requirements. These environments often entail specialised threats and vulnerabilities that necessitate a customised approach. For OT/ICS organisations, the Top 20 Techniques can serve as a foundational framework, but they should be augmented with industry-specific threat intelligence and expertise. Techniques and tactics unique to these environments should be integrated into the existing framework, ensuring a comprehensive approach to securing critical infrastructure.

Additionally, the concept of choke points becomes even more critical in OT/ICS environments. Identifying and defending against choke points specific to these industries can significantly enhance the security posture. Understanding the actionability of techniques within the context of OT/ICS is also paramount, as it enables rapid incident response and mitigation in a domain where downtime can have severe consequences.

In the grand tapestry of cybersecurity, the ability to adapt and tailor one's defenses is paramount. With this strategic framework and the Top 20 Techniques at their disposal, organisations can navigate the complex and ever-changing threat landscape with resilience and resource efficiency.

The Dynamic Top 20: A Synergy of Adaptability and Resource Efficiency

An important aspect to reiterate is that the Top 20 Most Common Adversary Techniques remain far from static. They are designed to evolve with the ever-changing threat landscape. The natural question is whether 21 techniques might surpass the efficacy of 20. While theoretically feasible, this should be predicated upon an assumption of unlimited resources. The crux of the matter lies in whether monitoring 21 techniques affords visibility into every attack. Thus far, experience has affirmed the efficacy of the Top 20, striking a balance between cost-efficiency and comprehensive coverage. This rationale prompts security teams to judiciously discern where to establish the boundary.

In conclusion, CyberStash advocates a strategic framework that is both dynamic and cost-efficient. We encourage cybersecurity teams to realign their focus onto the Top 20 most frequently observed ATT&CK techniques, thereby empowering them to enhance their security posture while wisely managing their resources. In the ever-evolving arena of cybersecurity, the wisdom lies in making informed decisions, concentrating on techniques of paramount importance, and embracing adaptability as the cornerstone of robust cybersecurity defenses. The cyber threat hunting perspective further reinforces the adaptability of this framework, emphasising the recognition of techniques over specific attacks, and aligning organisations with a dynamic, forward-thinking security posture.

For organisations operating within specialised attack surface areas, the framework remains adaptable, allowing for the integration of industry-specific considerations and expertise, ensuring comprehensive security in the face of evolving threats.

Examples of Real-World Attacks and Detection

In this section, we delve into real-world cyberattacks carried out by adversaries and explore how the Top 20 Most Common Adversary Techniques can be harnessed for effective detection. By examining these attack scenarios, we gain valuable insights into the practical application of the Top 20 detection rules and how they could have thwarted or alerted defenders to these threats. These examples serve as tangible demonstrations of the importance of adopting the right strategies and detection measures to bolster an organisation's cybersecurity defenses against ever-evolving adversaries.

Example 1: Volt Typhoon Targeting U.S. Critical Infrastructure with "Living off the Land" Techniques

Techniques Used:

- Execution: Command Line Interface / PowerShell (T1059)
- Persistence: Scheduled Tasks (T1053)
- Defense Evasion: Obfuscated Files or Information (T1027)

Detection with Top 20 Rules:

The Volt Typhoon threat group initiated malicious commands through the Command Line Interface and PowerShell (T1059). Continuous monitoring for unusual command line activities or PowerShell usage would have detected these actions.

To maintain persistence, the attackers utilised Scheduled Tasks (T1053) to ensure their malware runs at specific intervals. Detection rules targeting scheduled task creation and changes would have identified this technique.

In an attempt to evade detection, the adversaries obfuscated files and information (T1027). Detection rules focused on identifying obfuscation techniques and anomalies in file behavior would have been crucial for detecting this evasion strategy.

Example 2: Ransomware Attack Leveraging LockBit 3.0

Techniques Used:

- Execution: Command Line Interface / PowerShell (T1059)
- Credential Access: Credential Dumping (T1003)
- Defense Evasion: Obfuscated Files or Information (T1027)

Detection with Top 20 Rules:

The ransomware attacker initiated malicious commands through Command Line Interface and PowerShell (T1059) to execute the encryption process. Monitoring for suspicious command line activity or PowerShell usage could have detected these actions.

To gain elevated privileges, the attacker engaged in credential dumping (T1003) to obtain login credentials. Detection rules for credential access anomalies would have raised alarms.

The attacker attempted to evade detection by obfuscating files or information (T1027). Detection rules focused on identifying obfuscation techniques and anomalies in file or information behavior could have detected this evasion tactic.

Example 3: SolarWinds Supply Chain Attack

Techniques Used:

- Initial Access: Supply Chain Compromise
- Execution: Command Line Interface / PowerShell (T1059)
- Persistence: Scheduled Tasks (T1053)

Detection with Top 20 Rules:

The SolarWinds attack began with a sophisticated supply chain compromise. While supply chain attacks can be challenging to detect, monitoring for anomalies in the supply chain, especially in software updates, is crucial. While not covered explicitly in the Top 20 rules, it's essential to have visibility into the software supply chain.

Once inside the target networks, the adversaries used PowerShell for execution (T1059). The detection rule for PowerShell activity would have identified this unusual usage and raised alerts.

To maintain persistence, the attackers created scheduled tasks (Scheduled Tasks, T1053). Monitoring for scheduled task creation and changes would have helped detect this aspect of the attack.

Example 4: WannaCry Ransomware Attack

Techniques Used:

- Execution: EternalBlue (T1210)
- Defense Evasion: Obfuscated Files or Information (T1027)

Detection with Top 20 Rules:

The WannaCry ransomware attack exploited the EternalBlue vulnerability (EternalBlue, not explicitly in Top 20 but related) to propagate within networks. Organisations that had not applied the necessary patches might have detected the attack by monitoring for vulnerable systems or unusual SMB traffic.

The attackers obfuscated their ransomware code (Obfuscated Files or Information, T1027). Monitoring for signs of obfuscation within files would have raised alarms.

Example 5: NotPetya Ransomware Attack

Techniques Used:

- Execution: Command Line Interface / PowerShell (T1059)
- Credential Access: Credential Dumping (T1003)
- Defense Evasion: Obfuscated Files or Information (T1027)

Detection with Top 20 Rules:

The NotPetya ransomware attack began by leveraging the Command Line Interface and PowerShell (T1059) to execute its encryption process. Monitoring for unusual command line activity or PowerShell usage could have potentially detected these malicious actions.

As the attacker sought to escalate privileges, they engaged in credential dumping (T1003) to obtain login credentials. Detection rules focused on identifying anomalies in credential access could have alerted defenders to this suspicious activity.

To avoid detection, the attacker employed obfuscation techniques (T1027) to make their ransomware payload less conspicuous. Detection rules designed to spot obfuscation or anomalies in file behavior could have played a crucial role in identifying this evasion tactic.

CyberStash: Your Partner in Advanced Cybersecurity

CyberStash is your strategic ally, dedicated to a singular mission: to significantly reduce your business's vulnerability to the ever-escalating threat of cyberattacks. We don't just stop at preventing breaches; we take it a step further. Our vigilant approach ensures that we not only shield your organisation from threats but also respond with unmatched swiftness to detected threats, curtailing any potential damage before it can inflict irreparable harm on your day-to-day operations.

But what sets us apart isn't just our dedication to prevention and rapid response. It's our comprehensive solution – **eclipse.xdr**. Our robust Managed Detection and Response (MDR) Service is designed to empower your business, not only to withstand the dynamic challenges of the cyber threat landscape but also to thrive in it.

To gain a profound understanding of how **eclipse.xdr** can transform your cybersecurity posture, we extend to you a warm and wholehearted invitation to reach out to CyberStash. Our seasoned team is enthusiastic about offering you not only a complimentary presentation but also a comprehensive demonstration of the **eclipse.xdr** solution. This provides you with more than just insights; it affords you a hands-on experience, a firsthand look into the full spectrum of our capabilities.

Together, we can fortify your organisation against the ever-changing realm of cyber threats, ensuring your business is not just resilient but thriving in today's digital landscape.

https://www.cyberstash.com