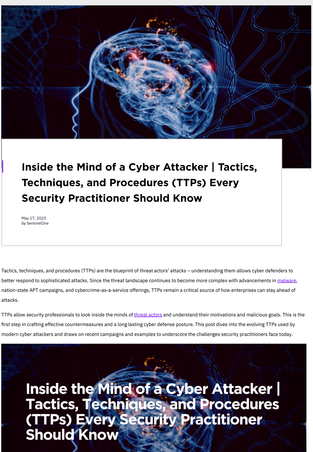

Inside the Mind of a Cyber Attacker | Tactics, Techniques, and Procedures (TTPs) Every Security Practitioner Should Know

May 17, 2023
by SentinelOne

Tactics, techniques, and procedures (TTPs) are the blueprint of threat actors' attacks – understanding them allows cyber defenders to better respond to sophisticated attacks. Since the threat landscape continues to become more complex with advancements in malware, nation-state APT campaigns, and cybercrime-as-a-service offerings, TTPs remain a critical source of how enterprises can stay ahead of attacks.

TTPs allow security professionals to look inside the minds of threat actors and understand their motivations and malicious goals. This is the first step in crafting effective countermeasures and a long lasting cyber defense posture. This post dives into the evolving TTPs used by modern cyber attackers and draws on recent campaigns and examples to underscore the challenges security practitioners face today.

Starting With Why | Peering Into the Motivations & Goals of Cyber Attackers

Understanding the motivations behind a cyberattack can greatly enhance the ability to effectively protect the organization. Breaking down the 'who', 'why' and 'what' of the attack can help defenders build a profile of the attackers including what they stand to gain in the event of a successful attack, how they are monetizing these gains, and how they are likely to strike again.

Based on their motivations and capabilities, there are six main reasons behind cyberattacks:

1. Financial Gain – Cybercriminals often seek to steal sensitive data, such as credit card information or intellectual property (IP), to sell on the dark web or to use in other criminal activities. Cybercriminals motivated by profit are typically indifferent to who their targets are and what they stand for. Examples of financially motivated attacks include banking trojans like Emotet and ransomware, such as the DarkSide attack on Colonial Pipeline and the rash of double-extortion attacks by Ransomware-as-a-Service gangs like LockBit.
2. Espionage – Nation-state actors and other advanced persistent threat (APT) groups often conduct cyber espionage campaigns to gather intelligence or steal IP for strategic purposes. They are usually funded or sponsored directly by the nation and target government-run organizations, opposing political entities, and large businesses. A well-known example of a cyber espionage campaign is the Stuxnet worm, which targeted Iranian nuclear facilities and more recently Metador, an unattributed threat actor targeting telcos, ISPs and universities.
3. Disruption – Some cyber attackers aim to cause disruption or destruction, either for ideological reasons or as a form of 'hacktivism'. The primary goal of hacktivists is to bring awareness to their cause through the exposure of secrets and sensitive information, or by taking down services or organizations deemed to be part of the opposition. Examples include the DDoS attacks carried out by Anonymous or the NotPetya ransomware attack, which caused significant damage to businesses worldwide. A more recent example of this art a mass scale is the AcidRain malware used to render Viasat KA-SAT modems inoperable in the first few months of the ongoing Russian-Ukrainian conflict.
4. Cyber Terrorism – Cyber terrorism models together two significant concerns – attacks using sophisticated technology, and traditional terrorism. Cyber terrorists are focused on attacking critical services to intentionally cause harm to further their political, economic, technical, or military agendas. They often target state services and essential industries to maximize destruction and disruption such as the WannaCryptor attack on the Iranian train system. Cyber terrorism also seems to intimate, coerce, or influence vulnerable audiences to see fear or force political changes.
5. Personal Causes – Unlike external threat actors that need to break into a targeted network, malicious insiders already have access rights into the environment and can work from within to get around the cybersecurity framework. Personal reasons such as revenge or retaliation are usually the motivation behind insider threats. Often in these cases, malicious insiders seek to steal and leak classified information or IP in the name of their personal cause.
6. Attention & Notoriety – Script kiddies are low-level, unskilled attackers that leverage tools and available kits designed by others to penetrate a targeted system. Motivating factors for script kiddies are usually quite simple – they seek attention, excitement, and chaos. Also, cyberhackers motivated by reputation and attention are known to actively seek targets that are widely known and required to disclose the attack rather than smaller, unknown ones.

Reading the Blueprints | How Tactics, Techniques, and Procedures (TTPs) Help Cyber Defenders

TTPs play an essential role in empowering security defenders to combat cyber threats effectively. By analyzing and understanding TTPs, defenders gain valuable insights into the behaviors and methodologies employed by adversaries. This accelerates the process for identifying potential attacks, developing proactive defense strategies, and implementing security measures specific to business and industry risks.

Organizations like NIST and MITRE categorize and catalog the behaviors of threat actors into tactics, techniques, and procedures; collectively known as TTPs. Tactics refer to the highest-level description of the behavior, techniques are descriptions that give the tactic context, and procedures describe the activities to give context of the technique. To break this down further:

- Tactics – These are the overarching strategies and goals behind an attack. They can be thought up as the 'why' to the tactical objectives and explain the reasons fueling the cyberattacker. Tactics are important for cyber defenders as they can be used to build the threat profile of the actor being investigated. Many threat actors and groups are recognizable by the use of specific tactics.
- Techniques – These are the methods that the threat actor uses to launch and engage in the attack to achieve their objective. Actors often use many techniques during their campaigns to facilitate initial compromise, move laterally within the compromised environment, exfiltrate data, and more. Techniques can be analyzed at every stage of the cyberattack, leaving behind a distinguishable digital footprint of the threat actor.
- Procedures – These are the step-by-step sequence of actions that make up the attack, including the tools and kits used by the threat actor. During forensic investigations for example, security analysts may perform file system analysis to reconstruct a procedure in order to build out a timeline of the attack. Analysts will also look for modifications to system files, find clues in event logs, and try to build a picture of what happened in each stage of the attack.

Being able to detect patterns and indicators of compromise through TTPs are instrumental in helping security professionals respond promptly to threats. It's also the trigger for critical improvements in policies and workflows that can stop similar threats in the future. TTPs serve as a foundation for threat intelligence leading to better risk mitigation and facilitating a more collective approach to cybersecurity.

Understanding How TTPs Work in Real-World Attacks

Both the frequency of cyber crime and their constant development continue to increase at staggering rates. Researchers estimate that the world will face 33 billion account breaches in 2023 alone and that attacks are now occurring once every 39 seconds. This section explores some of the most common TTPs used in modern threat campaigns and how they are leveraged in various types of real-world attacks.

Social Engineering

Social engineering is the psychological manipulation of individuals into divulging sensitive information or performing actions that compromise security. This tactic is often employed in phishing campaigns, such as the highly targeted spear-phishing attacks that have been linked to APT groups like APT29, also known as Cozy Bear, and APT28, also known as Sofacy or Fancy Bear. These campaigns often use highly convincing emails that appear to come from legitimate sources, luring victims into clicking malicious links or downloading malware-laden attachments.

Social engineering campaigns utilize various TTPs to manipulate human behavior and exploit vulnerabilities. Other than phishing, common TTPs associated with social engineering include:

- Pretexting – The attacker creates a plausible scenario or false identity to deceive the target, gaining their trust, and extracting sensitive information.
- Impersonation – Pretending to be someone else, such as a trusted colleague, authority figure, or service provider, to manipulate the target into providing sensitive data or performing certain actions.
- Water-holing – Compromising legitimate websites frequently visited by the target audience and injecting malicious code or links to infect visitors' devices.

Exploiting Vulnerabilities

Attackers often exploit known vulnerabilities in software and hardware to gain unauthorized access to systems or escalate privileges. One recent example is the exploitation of the Microsoft Exchange Server vulnerabilities, dubbed ProxyLogon and attributed to the HAFNIUM APT group. The group used these vulnerabilities to gain access to email accounts and deploy additional malware for further exploitation. Several TTPs are associated with vulnerability exploitation including:

- Scanning – Conducting network or system scans to identify potential vulnerabilities, such as open ports, unpatched software, or misconfigurations.
- Zero Day Exploits – Exploiting vulnerabilities that are unknown or have not yet been patched by the software vendor, giving attackers an advantage over defenders.
- Privilege Escalation – Exploiting vulnerabilities or misconfigurations to elevate privileges and gain higher-level access within a system or network.
- Remote Code Execution (RCE) – Exploiting vulnerabilities that allow an attacker to execute arbitrary code on a targeted system, providing full control over the compromised device.
- Denial-of-Service (DoS) Attacks – Overloading a system or network with excessive requests or malicious traffic to disrupt its availability and potentially expose vulnerabilities.

Living Off the Land

"Living off the land" (LotL) is a tactic where attackers use legitimate tools and processes already present on a victim's system to carry out their attacks, making it more difficult for security solutions to detect their activities. An example of this is the use of PowerShell, a powerful scripting language built into Windows, which has been used in various attacks, including the infamous Emotet banking trojan and the Ryuk ransomware. Threat actors are known to use these TTPs to achieve successful LotL:

- Windows Management Instrumentation (WMI) Abuse – Leveraging the WMI infrastructure to execute commands, retrieve information, or interact with systems, bypassing security controls.
- Scripting Language Abuse – Utilizing scripting languages like JavaScript, VBScript, AppleScript, or Python to execute malicious code or automate malicious activities.
- Fileless Malware – Deploying malware that resides only in memory, leveraging legitimate system processes or functionalities to carry out malicious activities without leaving traditional file-based traces.
- Masquerading – Disguising malicious files, processes, or commands with legitimate names, making them appear benign to evade detection.

Lateral Movement

Once attackers gain a foothold in a network, they often use lateral movement techniques to move between systems and escalate their privileges. In techniques like pass-the-hash or pass-the-ticket, an attacker uses stolen credentials or authentication tokens to move between systems.

One recent example is the SolarWinds supply chain attack, in which the threat actors used a combination of custom malware, stolen credentials, and legitimate tools to move laterally within the targeted networks, ultimately gaining access to sensitive data and systems. The following TTPs contribute to lateral movement:

- Remote Desktop Protocol (RDP) Hijacking – Unauthorized control or manipulation of remote desktop sessions to move laterally between systems.
- Credential Theft and Brute Force Attacks – Stealing or cracking credentials to impersonate legitimate users and move laterally within the network.
- Man-in-the-Middle (MiTM) Attacks – Intercepting network traffic and tampering with communication to gain unauthorized access or escalate privileges.
- Active Directory Exploitation – Exploiting weaknesses or misconfigurations within the Active Directory infrastructure to escalate privileges or gain unauthorized access to other systems or domains.

Data Exfiltration and Covering Tracks

After achieving their objectives, cyberattackers often exfiltrate the stolen data, using covert channels or encrypted communication to avoid detection. In some cases, attackers also take steps to cover their tracks and maintain persistence, such as deleting logs or using rootkits to hide their presence on compromised systems. A notable example of this is the DarkHotel APT group, known for its highly targeted attacks on luxury hotels, which utilized a combination of custom malware and sophisticated techniques to exfiltrate sensitive data and maintain a low profile within the compromised networks. To wipe away traces of their actions, attackers will often use a combination of these TTPs:

- Compression and Encryption – Compressing or encrypting stolen data to obfuscate its content and make it more difficult to detect or analyze.
- Protocol Tunneling – Encapsulating exfiltrated data within other network protocols, such as DNS or HTTP, to bypass security controls and avoid suspicion.
- Data Obfuscation – Modifying or obfuscating data formats or file extensions to make exfiltrated information appear as benign or unrelated files.
- Exfiltration Through Trusted Protocols – Utilizing commonly used protocols like FTP, SSH, or HTTP to transfer stolen data, blending it with legitimate network traffic to evade detection.
- Data Destruction – Deleting or wiping data traces after exfiltration to eliminate evidence and hinder forensic investigations.

Proactive Measures for Security Practitioners

While understanding the TTPs is integral to the development of threat intelligence and defense mechanisms, this alone can only win half the battle. Enterprises must also enforce excellent cyber hygiene protocols and strengthen their security strategy holistically.

Implement a Strong Security Framework

Adopting a robust security framework, such as the NIST Cybersecurity Framework or the CIS Critical Security Controls, can help organizations systematically identify and address potential weaknesses in their security posture. Regularly reviewing and updating these frameworks is crucial to staying ahead of evolving threats.

Continuous Security Training and Awareness

Regular security training and awareness programs for employees can help reduce the risk of successful social engineering attacks. Training should cover topics like phishing, password security, and the importance of reporting suspicious activities.

Patch Management and Vulnerability Scanning

Implementing a robust patch management process and conducting regular vulnerability scans can help organizations identify and address known vulnerabilities in their systems, reducing the attack surface for cyber attackers.

Network Segmentation and Zero Trust

Network segmentation and the implementation of a zero trust security model can help limit lateral movement within a network, making it more difficult for attackers to escalate privileges and access sensitive data.

Monitoring and Incident Response

Establishing a well-defined incident response process and investing in monitoring tools, such as Security Information and Event Management (SIEM) systems or Extended Detection and Response (XDR) solutions like SentinelOne Singularity, can help organizations quickly detect, respond to, and contain cyber threats.

Conclusion

Identifying attack vectors and new methods are key to staying steps ahead of cyber attackers. Real-life examples and recent APT campaigns have shown how TTPs analysis enriches security practitioners' repertoire, allowing them to gain valuable insights into the tactics and techniques they are working against.

Though threat actors will continue to upgrade their methods and innovate their processes, there are many ways enterprises can mitigate risk and harden their defenses. Establishing an effective response strategy and deep, continuous monitoring can help augment a business' in-house team's defenses with robust detection and response capabilities.

Enterprises worldwide have turned to SentinelOne's Singularity™ Platform to proactively resolve modern threats at machine speed. Learn how SentinelOne works to more effectively manage risk across user identities, endpoints, cloud workloads, IoT, and more. Contact us or book a demo today.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- MITRE Managed Services Evaluation | 4 Key Takeaways for MDR & DFIR Buyers
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls
- Advancing Security | The Age of AI & Machine Learning in Cybersecurity
- How to Modernize Vulnerability Management in Today's Evolving Threat Landscape

©2023 SentinelOne, All Rights Reserved.
Privacy Policy Master Subscription Agreement