Attacker Profiles and Motivations

In *The Art of War*, Sun Tzu teaches "know thy enemy, know thy self. A thousand battles, a thousand victories" (translated in various forms) to instill the importance of understanding the strengths, weaknesses, strategies, and tactics of your adversary as well as you know your own. Of course, in modern cyber warfare a thousand battles can occur in a matter of seconds, and a single victory by your enemy can imperil your entire organization. Thus, knowing your enemies – including their means and motivations – is more important than ever.

In the relatively innocuous "good ol' days" of *hackers* and *script kiddies*, the primary motivation for a cyberattack was notoriety, and the attack objective was typically limited to defacing or "owning" a website to cause inconvenience and/or embarrassment to the victim.

Key Terms

The term *hacker* was originally used to refer to anyone with highly specialized computing skills, without connoting good or bad purposes. However, common misuse of the term has redefined a hacker as someone who circumvents computer security with malicious intent, such as a cybercriminal, cyberterrorist, or hacktivist, cracker, and/or black hat.

A *script kiddie* is someone with limited hacking and/or programming skills who uses malicious programs (malware) written by others to attack a computer or network.

Modern cyberattacks are perpetrated by far more sophisticated and dangerous adversaries, motivated by far more sinister purposes:

Cybercriminals. Acting independently or as part of a criminal organization, cybercriminals commit acts of data theft, embezzlement, fraud, and/or extortion for financial gain. According to the RAND Corporation, "In certain respects, the black market [for cybercrime] can be more profitable than the illegal drug trade,"[1] and by many estimates, cybercrime is now a US$1 trillion industry.

State-affiliated groups. Sponsored by or affiliated with nation-states, these organizations have the resources to launch very sophisticated and persistent attacks, have great technical depth and focus, and are well funded. They often have military and/or strategic objectives such as the ability to disable or destroy critical infrastructure, including power grids, water supplies,

[1] Lillian Ablon, Martin Libicki, and Andrea Golay. "Markets for Cybercrime Tools and Stolen Data." RAND Corporation, National Security Research Division. Accessed January 16, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

transportation systems, emergency response, and medical and industrial systems. The Center for Strategic and International Studies reports that "At the nation-state level, Russia, Iran, and North Korea are using coercive cyberattacks to increase their sphere of influence, while China, Russia and Iran have conducted reconnaissance of networks critical to the operation of the U.S. power grid and other critical infrastructure without penalty."[2]

Cybercrime vendors. Capitalizing on the service model of cloud computing, many threat actors now rent or sell their malware and exploits – including *business email compromise (BEC)* and ransomware – as cybercrime-as-a-service (CCaaS) offerings on the dark web. Vendors profit from the purchase or rental of their services and potentially earn a commission from the attacks themselves. Additional services often include mix-and-match bundles, collection services, volume discounts, and 24-hour support.

Hacktivists. Motivated by political or social causes, hacktivist groups (such as Anonymous) typically execute denial-of-service (DoS) attacks against a target organization by defacing their websites or flooding their networks with traffic.

Cyberterrorists. Terrorist organizations use the internet to recruit, train, instruct, and communicate, and to spread fear and panic to advance their ideologies. Unlike other threat actors, cyberterrorists are largely indiscriminate in their attacks, and their objectives include physical harm, death, and destruction.

Key Terms

Business email compromise (BEC) is the unauthorized use of email leading to financial fraud. BEC techniques including spamming and phishing, among others.

External threat actors – including organized crime, state-affiliated groups, activists, former employees, and other unaffiliated or otherwise unknown attackers – account for the majority of data breaches. Internal actors were involved in 34 percent of reported data breaches.[3]

Modern cyberattack strategy

Modern cyberattack strategy has evolved from a direct attack against a high-value server or asset ("shock and awe") to a patient, multistep process that blends exploits, malware, stealth, and evasion in a coordinated network attack ("low and slow").

[2] Zheng, Denise E. "Global Forecast 2016: Disrupting the Cyber Status Quo." Center for Strategic and International Studies. November 16, 2015. https://www.csis.org/analysis/disrupting-cyber-status-quo.

[3] "Verizon 2021 Data Breach Investigations Report." Verizon Enterprise Solutions. Accessed January 16, 2022. https://verizon.com/dbir/.

The Cyber-Attack Lifecycle (see Figure 1-1) illustrates the sequence of events that an attacker goes through to infiltrate a network and exfiltrate (or steal) valuable data. Blocking of just one step breaks the chain and can effectively defend an organization's network and data against an attack.

Reconnaissance. Like common criminals, attackers meticulously plan their cyberattacks. They research, identify, and select targets, often extracting public information from targeted employees' social media profiles or from corporate websites, which can be useful for social engineering and phishing schemes. Attackers will also use various tools to scan for network vulnerabilities, services, and applications that they can exploit, such as:

Network analyzers (also known as packet analyzers, protocol analyzers, or packet sniffers) are used to monitor and capture raw network traffic (packets). Examples include tcpdump and Wireshark (formerly Ethereal).

Network vulnerability scanners typically consist of a suite of tools including password crackers, port scanners, and vulnerability scanners and are used to probe a network for vulnerabilities (including configuration errors) that can be exploited. Examples include Nessus and SAINT.

Password crackers are used to perform brute-force dictionary attacks against password hashes. Examples include John the Ripper and THC Hydra.

Port scanners are used to probe for open TCP or UDP (including ICMP) ports on an endpoint. Examples include Nmap ("network mapper") and Nessus.

Web application vulnerability scanners are used to scan web applications for vulnerabilities such as cross-site scripting, SQL injection, and directory traversal. Examples include Burp Suite and OWASP Zed Attack Proxy (ZAP).

Wi-Fi vulnerability scanners are used to scan wireless networks for vulnerabilities (including open and misconfigured access points), to capture wireless network traffic and to crack wireless passwords. Examples include Aircrack-ng and Wifite.

Breaking the Cyber-Attack Lifecycle at this phase of an attack begins with proactive and effective end-user security awareness training that focuses on topics such as social engineering techniques (for example, phishing, piggybacking, and shoulder surfing), social media (for example, safety and privacy issues), and organizational security policies (for example, password requirements, remote access, and physical security). Another important countermeasure is continuous monitoring and inspection of network traffic flows to detect and prevent unauthorized port and vulnerability scans, host sweeps, and other suspicious activity. Effective change and configuration management processes help to ensure that newly

deployed applications and endpoints are properly configured (for example, disabling unneeded ports and services) and maintained.

Weaponization. Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message. Or, for highly targeted attacks, attackers may customize deliverables to match the specific interests of an individual within the target organization.

Breaking the Cyber-Attack Lifecycle at this phase of an attack is challenging because weaponization typically occurs within the attacker's network. However, analysis of artifacts (both malware and weaponizer) can provide important threat intelligence to enable effective zero-day protection when delivery (the next step) is attempted.

Delivery. Attackers next attempt to deliver their weaponized payload to a target endpoint, for example, via email, instant messaging (IM), drive-by download (an end user's web browser is redirected to a webpage that automatically downloads malware to the endpoint in the background), or infected file share.

Breaking the Cyber-Attack Lifecycle at this phase of an attack requires visibility into all network traffic (including remote and mobile devices) to effectively block malicious or risky websites, applications, and IP addresses, and preventing known and unknown malware and exploits.

Exploitation. After a weaponized payload is delivered to a target endpoint, it must be triggered. An end user may unwittingly trigger an exploit, for example, by clicking a malicious link or opening an infected attachment in an email, or an attacker may remotely trigger an exploit against a known server vulnerability on the target network.

Breaking the Cyber-Attack Lifecycle at this phase of an attack, as during the Reconnaissance phase, begins with proactive and effective end-user security awareness training that focuses on topics such as malware prevention and email security. Other important security countermeasures include vulnerability and patch management; malware detection and prevention; threat intelligence (including known and unknown threats); blocking risky, unauthorized, or unneeded applications and services; managing file or directory permissions and root or administrator privileges; and logging and monitoring network activity.

Installation. Next, an attacker will escalate privileges on the compromised endpoint, for example, by establishing remote shell access and installing rootkits or other malware. With remote shell access, the attacker has control of the endpoint and can execute commands in privileged mode from a command-line interface (CLI) as if physically sitting in front of the endpoint. The attacker will then move laterally across the target's network, executing attack code, identifying other targets of opportunity, and compromising additional endpoints to establish persistence.

The key to breaking the Cyber-Attack Lifecycle at this phase of an attack is to limit or restrict the attackers' lateral movement within the network. Use network segmentation and a Zero Trust model that monitors and inspects all traffic between zones or segments, and granular control of applications that are allowed on the network.

Command and Control. Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered. Communication is essential to an attack because it enables the attacker to remotely direct the attack and execute the attack objectives. C2 traffic must therefore be resilient and stealthy for an attack to succeed. Attack communication traffic is usually hidden with various techniques and tools including:

Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption.

Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic.

Port evasion using network anonymizers or port hopping to traverse over any available open ports.

Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult.

DNS tunneling is used for C2 communications, as well as data infiltration (for example, sending malicious code, commands, or binary files to a victim) and data exfiltration.

Breaking the Cyber-Attack Lifecycle at this phase of an attack requires inspection of all network traffic (including encrypted communications), blocking of outbound C2 communications with anti-C2 signatures (along with file and data pattern uploads), blocking of all outbound communications to known malicious URLs and IP addresses, blocking of novel attack techniques that employ port evasion methods, prevention of the use of anonymizers and proxies on the network, monitoring of DNS for malicious domains and countering with DNS sinkholing or DNS poisoning, and redirection of malicious outbound communications to honeypots to identify or block compromised endpoints and analyze attack traffic.

Actions on the Objective. Attackers often have multiple, different attack objectives including data theft; destruction or modification of critical systems, networks, and data; and denial-of-service (DoS). This last stage of the Cyber-Attack Lifecycle can also be used by an attacker to advance the early stages of the Cyber-Attack Lifecycle against another target. The 2018 Verizon *Data Breach Investigations Report* (DBIR) describes this strategy as a secondary motive in which "[web applications] are compromised to aid and abet in the attack of another victim."[4] For example, an attacker may compromise a company's extranet to breach a business partner that is the primary target. According to the DBIR, in 2014 there were 23,244 "incidents where web applications were compromised with a secondary motive." The attacker pivots the attack against the initial victim network to a different victim network, thus making the initial victim an unwitting accomplice."

[4] "11[4] "Verizon 2021 Data Breach Investigations Report." Verizon Enterprise Solutions. Accessed January 16, 2022. https://verizon.com/dbir/..

MITRE ATT&CK framework

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework is a comprehensive matrix of tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objective, and assess an organization's risk. Organizations can use the framework to identify security gaps and prioritize mitigations based on risk.

MITRE started ATT&CK in 2013 to document the TTPs that advanced persistent threats (APTs) use against enterprise networks. It was created out of a need to describe adversary TTPs that would be used by a MITRE research project called FMX. The objective of FMX was to investigate how endpoint telemetry data and analytics could help improve post-intrusion detection of attackers operating within enterprise networks. The ATT&CK framework was used as the basis for testing the efficacy of the sensors and analytics under FMX and served as the common language both offense and defense could use to improve over time.

MITRE ATT&CK now has three iterations:

- **ATT&CK for Enterprise:** Focuses on adversarial behavior in Windows, Mac, Linux, and cloud environments.
- **ATT&CK for Mobile:** Focuses on adversarial behavior on iOS and Android operating systems.
- **Pre-ATT&CK:** Focuses on “pre-exploit” adversarial behavior. Pre-ATT&CK is included as part of the ATT&CK for Enterprise matrix.

Techniques represent “how” an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. The MITRE ATT&CK matrix contains a set of techniques used by adversaries to accomplish a specific objective. Those objectives are categorized as tactics in the ATT&CK Matrix. The Enterprise ATT&CK matrix is a superset of the Windows, MacOS, and Linux matrices. MITRE regularly updates the techniques discovered in the wild by both cybersecurity researchers and hackers alike. As of 2022, there are 218 techniques defined in the Enterprise model.

Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique. For example, an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets.

Tactics represent the “why” of an ATT&CK technique or sub-technique. Adversarial tactics represent the attacker's goal or the reason for performing an action. For example, an adversary may want to achieve credential access.

Tactics are listed in Table 1-1.

Table 1-1

MITRE Tactics

Tactic	The attacker is trying to:
Reconnaissance	Gather information they can use to plan future operations
Resource Development	Establish resources they can use to support operations
Initial Access	Get into your network
Execution	Run malicious code
Persistence	Maintain their foothold
Privilege Escalation	Gain higher-level permissions
Defense Evasion	Avoid being detected
Credential Access	Steal account names and passwords
Discovery	Figure out your environment
Lateral Movement	Move through your environment
Collection	Gather data of interest to their goal
Command and Control	Communicate with compromised systems to control them
Exfiltration	Steal data
Impact	Manipulate, interrupt, or destroy your systems and data

Procedures are the specific implementation the adversary uses for techniques or sub-techniques. For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim. Procedures are categorized in the ATT&CK framework as techniques observed in the wild in the “Procedure Examples" section of technique pages.

Sub-techniques and procedures describe different things in ATT&CK. Sub-techniques are used to categorize behavior and procedures are used to describe in-the-wild use of techniques. Furthermore, since procedures are specific implementations of techniques and sub-techniques, they may include several additional behaviors in how they are performed. For example, an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim is a procedure implementation containing several (sub)techniques covering PowerShell, Credential Dumping and Process Injection used against LSASS.