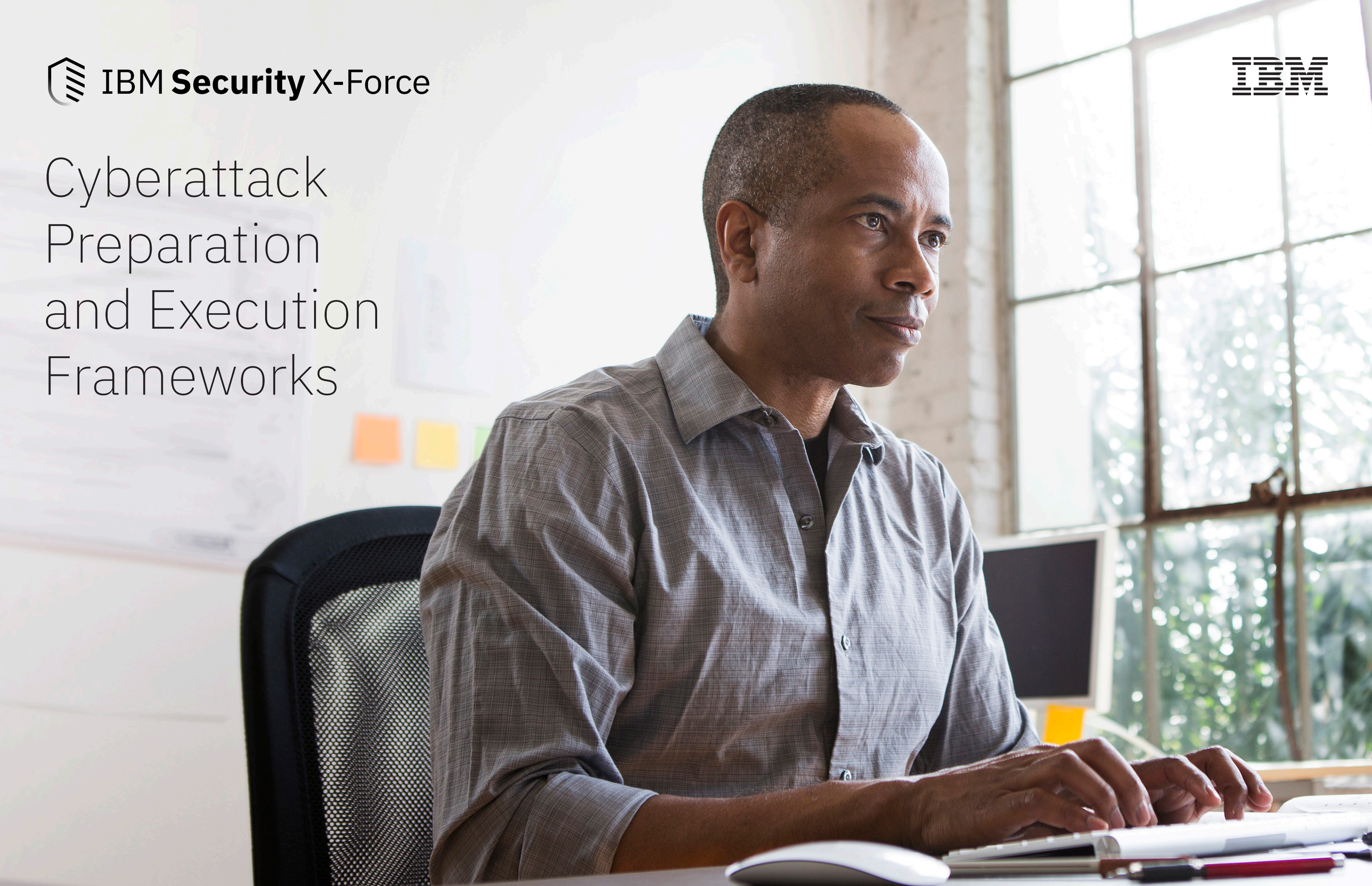
IBM **Security** X-Force

Cyberattack Preparation and Execution Frameworks



01

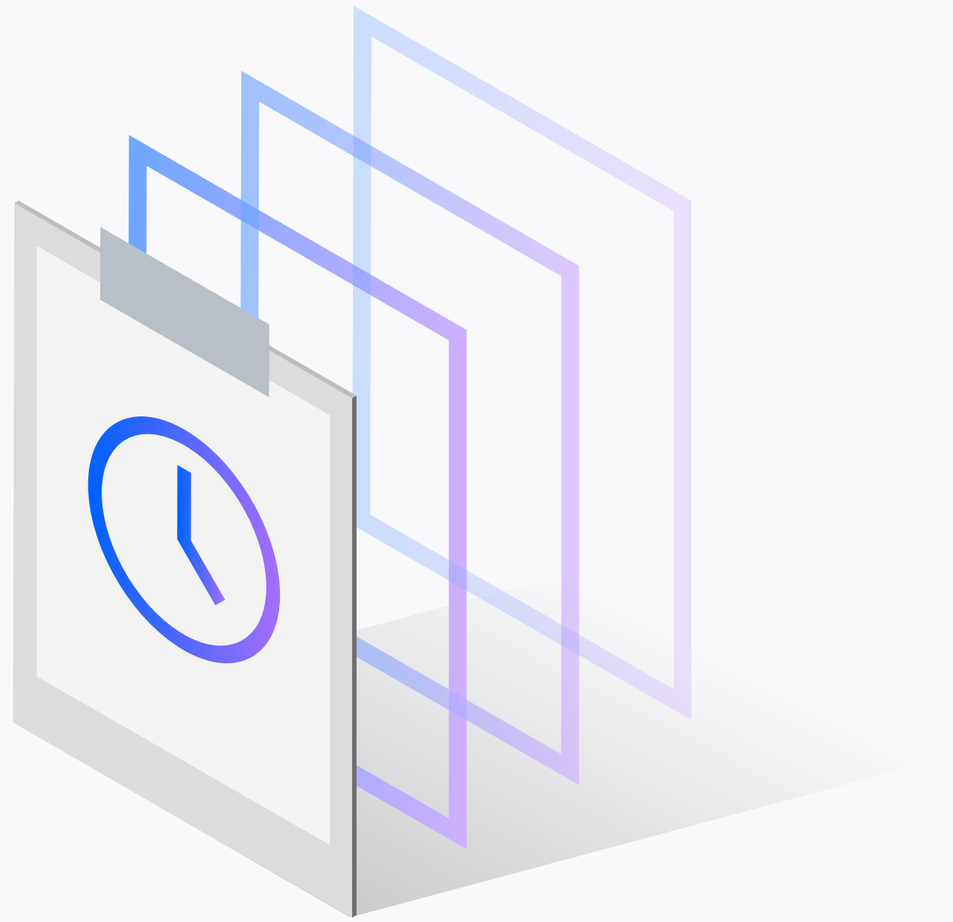
Overview

IBM Security X-Force cyberattack preparation and execution frameworks build upon the industry-standard conceptual approaches to analyzing a cyberattack. These industry-standard approaches include Lockheed Martin's Cyber Kill Chain*, Mandiant's Attack Lifecycle*, MITRE's ATT&CK*, and others. The X-Force cyberattack preparation and execution frameworks provide a logical flow representative of attacks today and they also incorporate phases not typically included in other frameworks. As attackers continue to increase in sophistication, X-Force believes these additional phases are increasingly relevant.

The X-Force attack preparation framework is a particularly important addition, as it is vital to understanding and responding to modern cyber incidents. The frameworks also incorporate the use of tactics that attackers employ to hide their attack planning, presence within a network and attribution to a specific country or group. The attacker may perform obfuscation tactics during both the cyberattack preparation and the cyberattack execution frameworks. These phases are identified as "operational security" and "defense evasion and monitoring" respectively.

Finally, the X-Force cyberattack preparation and execution frameworks recognize that some phases of an attack can occur simultaneously, sequentially, repeatedly or not at all, and an attacker may continuously modify the attack throughout the engagement. The X-Force frameworks capture the flexibility that is available to the attacker and present the feedback phase throughout the entire engagement.

These key features enhance the ability for threat researchers to analyze simple and sophisticated incidents and clearly communicate all known attacker tactics. The X-Force approach helps security teams inside and outside of IBM to understand the design and execution of a cyberattack in a detailed, organized manner. This approach enables teams to use that insight to better identify and respond to threats to their organization.



* Please see: Lockheed Cyber Kill Chain: **www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html**, Mandiant Attack Lifecycle: **www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf**, and MITRE ATT&CK: **https://attack.mitre.org/wiki/Main_Page**

02

X-Force Cyberattack Preparation and Execution Frameworks

Figure 1 is a schematic view of X-Force cyberattack preparation and execution frameworks. The graphic can be read from left to right, where the first part of the attack is the preparation framework. After undertaking the phases of the attack preparation, the attacker will launch the attack. Depending on the result, the attacker will either proceed to the phases in the cyberattack execution framework or will reassess the requirements needed for a successful attack. Once inside the execution framework, the attacker will attempt to complete some or all the phases necessary to try and meet the attacker's objective.

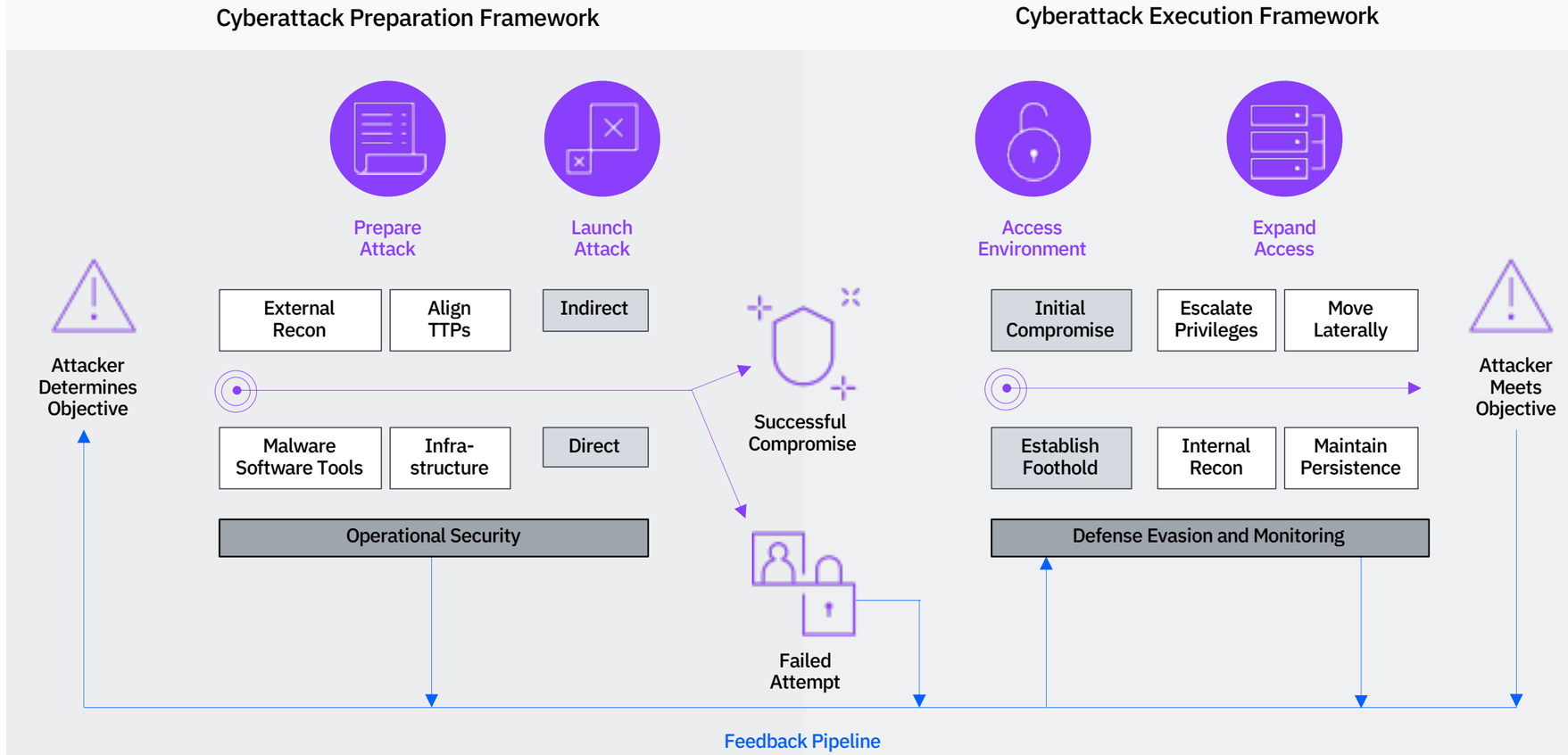


Figure 1: X-Force cyberattack preparation and execution frameworks

03

Key Needs Addressed by the Frameworks

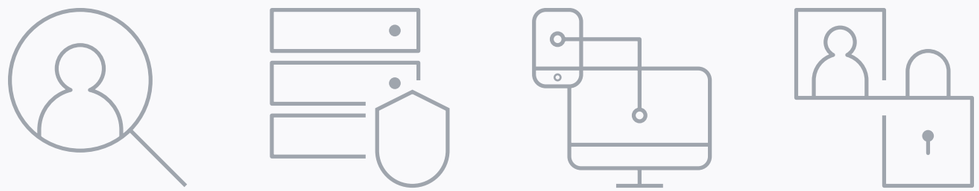
The X-Force cyberattack preparation and execution frameworks characterize threat data and communicate threat intelligence. These frameworks explain the full range of activities that occur prior to and during an actual compromise. This process provides incident responders and threat intelligence analysts with a model they can use to track data, conduct peer review research, and communicate analysis with greater clarity and consistency. The X-Force cyberattack preparation and execution frameworks also provide clients with an easy and efficient way to compare different cyberattack threat vectors relevant to their industries.

The X-Force cyberattack preparation framework addresses the following key needs:

- **Analysis and Response.** Provides an intuitive framework to analyze the cyberattack planning process and respond to observable instances of malicious activity
- **Clarity of Communication.** Provides a model that allows threat researchers to communicate analyses clearly and consistently to customers of various knowledge levels and perspectives
- **Increased Flexibility.** Creates a framework that has the flexibility to respond to various attacks perpetrated by known and unknown cyber-threat groups and attack tactics

The X-Force cyberattack execution framework addresses the following key needs:

- **Analysis.** Provides a model that allows researchers to group data in a structured manner and supports additional trending and predictive analysis
- **Informed Decision-Making.** Provides an intuitive framework to analyze a single detected instance of malicious activity and establishes this activity as a pivot point for expeditious decision-making and response planning
- **Increased Flexibility.** Offers a framework that has the flexibility to respond to various known and unknown cyber-threat groups and attack types
- **Clarity of Communication.** Provides an adaptable model for communicating attack components on a generalized or detailed level to customers of various knowledge levels and perspectives



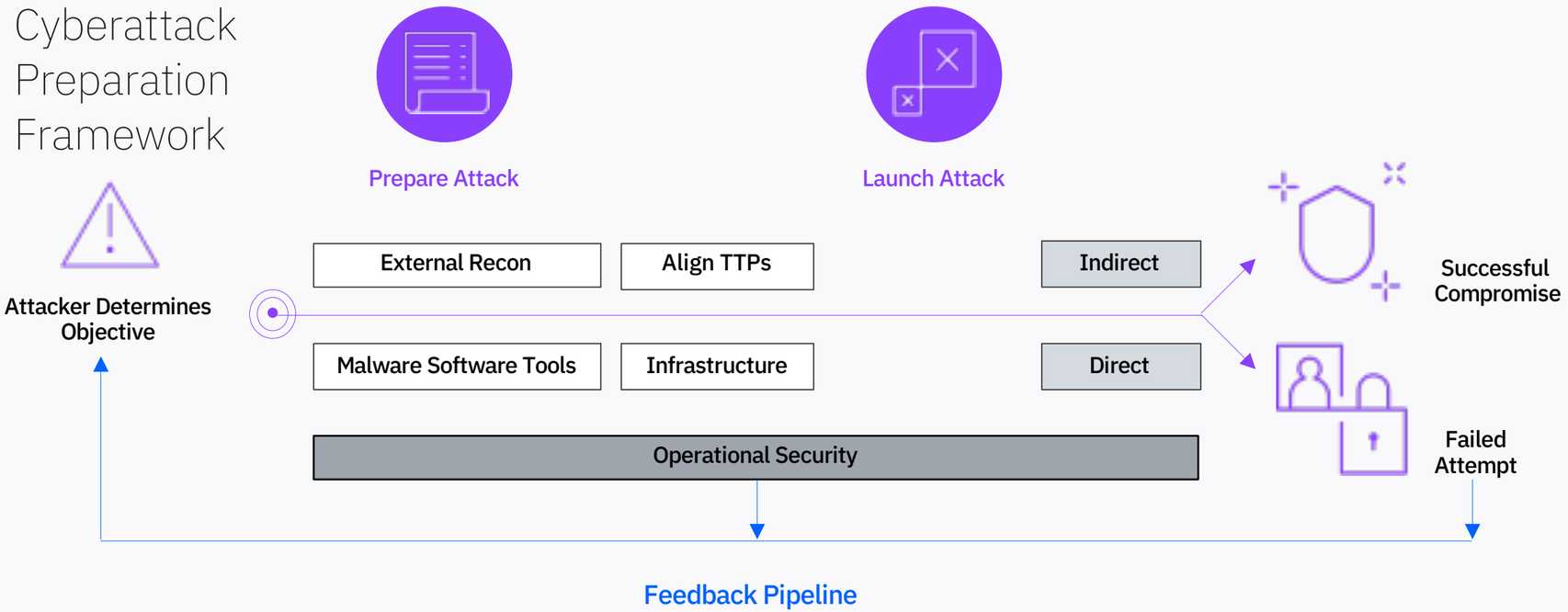
04

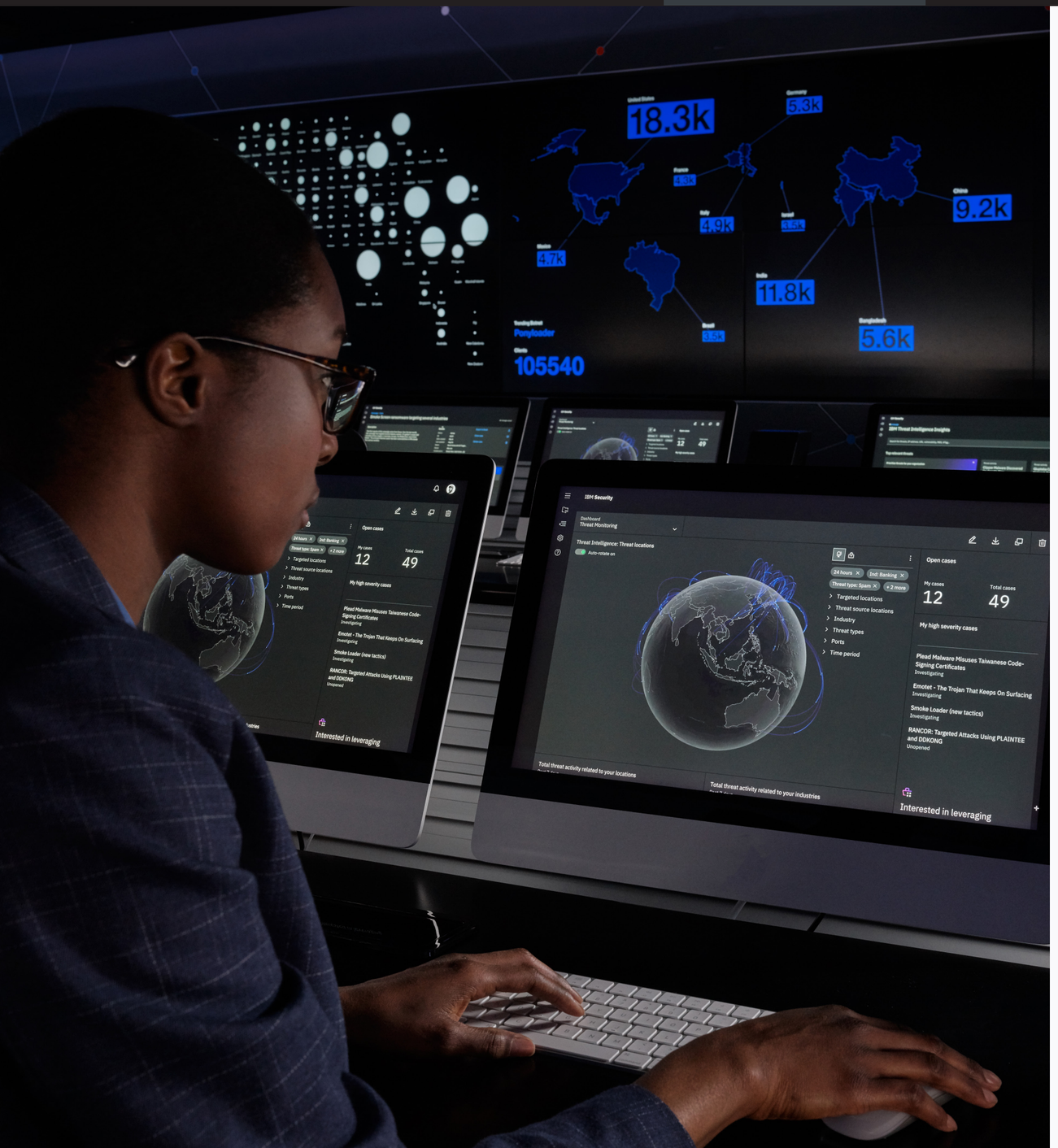
Phases of the X-Force Cyberattack Preparation Framework

The X-Force cyberattack preparation framework includes the phases that an attacker initially takes to determine a target and to prepare an attack. These phases occur before the attacker gains initial foothold.

The X-Force cyberattack preparation framework consists of eight phases, beginning with the determine objective phase and ending with the launch attack phase, where the attacker determines whether the attack resulted in a successful compromise or not. Between those initial and final phases, the attacker has several options to design an attack and may use any combination of the prepare attack phases. Upon determining the success or failure of the launch attack phase, the attacker will either move on to the execution framework in the case of a success, or revise, change, or cancel the attack plan in the case of a failure.

While many of the preparatory framework phases may be undetectable to a victim or defender, there are often opportunities to track attackers' online footprints and thwart attacks before they occur.





04

Phases of the X-Force Cyberattack Preparation Framework

Determine objective

During the determine objective phase, the attacker identifies the target, determines any attack requirements, and creates an initial attack plan. Additionally, the attacker may identify the strategic and tactical targets that are required to meet the attack's overall objective.

Strategic targets are those targets that inform the overall goals of the attack, often by determining whether an industry or company possesses the targeted objective, such as sensitive data or financial information.

Tactical targets are informed by the tasks required to complete the attack and govern how the attacker will achieve the strategic target. For example, tactical targets may consist of each specific avenue of infection into the target and each follow-on task that helps the attacker complete the objective.

Finally, attackers may outline an initial plan, including the tactics, tools and different requirements that are needed. As the attacker moves through the rest of the cyberattack preparation framework phases, the initial plan often changes.

IBM

04

Phases of the X-Force Cyberattack Preparation Framework

Defending the Network

Often, the goal for network defenders is to protect a network from compromise completely. And although this goal may not always be possible, there are opportunities to recognize or disrupt a potential attack during the attack planning preparation. For example, defenders can closely monitor for unusual browsing of their public domains or hunt for signs that employee authentication credentials are posted on the web. Although these factors may not provide conclusive evidence of a pending attack, they can provide an avenue for further research and monitoring.

PREPARE ATTACK STAGE

The phases contained within the prepare attack stage include all the known methods that attackers use to get from their target selection to launching their attack. These phases don't need to happen sequentially and often; depending upon how the attack progresses, the steps may occur simultaneously and through multiple iterations. In some cases, these steps can be skipped entirely.

External Reconnaissance

During the external reconnaissance phase, the attacker will determine a target and will research the organization with a focus on exploitable access points. The attacker may research the organization's employees, subsidiaries, customers and partners, and may search for any credential information that can be used to infiltrate the organization through its authorized users. The attacker also may use publicly available employee information to identify users who have greater access and prepare to compromise those users' credentials if possible. The attacker will also try to map the network footprint internally and in cloud-hosted environments with which the target organization works.

Align TTPs to Target

During the align TTPs to target phase, the attacker determines the available tactics, techniques and procedures (TTPs) that are most likely to succeed against the target. For example, data obtained in the previous phases of the attack preparation could be used to build a credible phishing message or determine if there are any options to gain third-party access through a partner. The attacker may also determine what part, or parts, of the network must be compromised to achieve the attack's objective. Additionally during this phase the attacker may determine which malware and software tools are best suited to expand access once the initial host is compromised. It's worth noting that some attackers may opt to skip using malicious tools at any stage and instead leverage existing operating system commands to penetrate the network. Malware can be introduced at any point and changed or mutated throughout the attack phases.

04

Phases of the X-Force Cyberattack Preparation Framework

Defending the Network

Often an attacker's actions to prepare the attack infrastructure are observable. In some cases, attackers will reuse network infrastructure that they have used in the past, and defenders can then monitor known malicious C2 networks for possible reuse. In addition, defenders can monitor suspicious domain registrations. Finally, defenders can educate employees on the dangers of interacting with online personas and provide guidance on appropriate response and reporting requirements if an employee is approached through social media or email by a person whom they don't know personally.

Prepare Attack Infrastructure

During the prepare attack infrastructure phase, the attacker may build a command and control (C2) network and might develop procedures to obfuscate any observable traces that could lead back to the attacker's own resources. Once the attack occurs, the malware will attempt to reach back to the established C2 infrastructure after which the attacker can access and control the malware and the compromised hosts. Typically, to build the malicious C2 infrastructure and communication resources, the attacker will buy, register or gain illegal ownership of servers, Secure Sockets Layer (SSL) certificates, web service accounts, such as social media or email, and possibly other network resources to operate a high-availability C2.

Attackers typically use proxies or virtual private networks (VPNs) to secure their communications and obfuscate their locations and identities. In addition, depending on the target, attackers may develop new personas or impersonate real people; they may use other social-engineering schemes to make their tactics seem like legitimate activities. For example, attackers may be able to create a more believable phishing message by befriending a target online before delivering malware. Fake online personas can be created using various methods, including the creation of new email addresses, setup of social media accounts, joining or creating fake web pages for organizations, and registering for conferences.

04

Phases of the X-Force Cyberattack Preparation Framework

Defending the Network

Attackers often purchase or reuse existing malware to prepare an attack, and this activity may be observable. Defenders can monitor the dark web for indications that an attacker is procuring malware. During the testing phase, careless attackers may accidentally release their attack components or parts of them “in the wild,” which may be caught by detection programs and thus enable examination ahead of the actual launch of an attack.

Prepare Malware and Software Tools

The prepare malware and software tools phase begins after the attacker defines the general requirements of the attack; however, the tools and malware may be adjusted as needed as more information is gleaned during the other prepare attack phases. When preparing the attack toolset, attackers can use malware or they can repurpose software tools that have legitimate purposes. Attackers may develop new malware, may reuse or purchase previously developed custom tools, or might repurpose publicly available malware, such as backdoors or credential stealers. Similarly, attackers can procure an exploit for a known vulnerability or can secure a zero-day exploit that would reduce the risk of an attack being detected. This process may fool operating system control and malware detection applications into believing the code is from a trusted source and subsequently allow the code to run. These exploits and tools may be used later, during the launch attack phase, and after a successful compromise, to accomplish the attackers’ objectives.

Once the malware and tools are ready, attackers may test their function before directing the attack at a target. Tests may include building backdoors that connect back to the attackers’ test C2 networks, scanning malware with several antivirus engines to assess detectability, sending phishing emails to the attackers’ own addresses, or using a virtual machine to verify that the attacks work as expected.

04

Phases of the X-Force Cyberattack Preparation Framework

CONTINUOUS ATTACK PREPARATION STAGE

Within the X-Force cyberattack preparation framework, there are two phases considered part of the continuous attack preparation stage as the attacker will conduct these phases throughout the entire framework. The two continuous attack phases are operational security, which includes efforts to evade detection by the victim or by other outside observers, and the feedback cycle, in which the attacker reassesses and revises the attack plan.

Operational Security

The operational security phase represents all the actions attackers take to hide their attack preparations from the victims or cybersecurity defenders. Attackers, particularly savvy attackers, likely will be concerned about the potential that their targets may discover the operation or that the attackers' identities will be discovered. Attackers can try to protect their critical information from outside observation by hiding the true network addresses that are used for reconnaissance searches, malware purchases, network infrastructure purchases or other online activities. Attackers can also seek to protect their malware tools by obfuscating code, keeping malware samples away from online code and sample repositories, or creating a staged ecosystem of backdoors whereby some tools are held back from all but the most sensitive targets.

Feedback Cycle

The feedback cycle phase is a continuous process in which attackers likely will review the information that has been gleaned during the previous phases and assess the tools that are available to review, and revise the attack preparation. Knowledge gained in any of the phases can inform decisions made anywhere else in the entire cyberattack framework, which means this phase is always present in attacks.

LAUNCH ATTACK

Once an attacker has completed some or all the prior phases of the X-Force cyberattack preparation lifecycle, the attacker will launch an attack against the target either directly or indirectly.

04

Phases of the X-Force Cyberattack Preparation Framework

Direct Attack Types:

- Using stolen credentials
- Access computer at target location
- Phishing email with malicious file
- Phishing email with domain attached

Indirect Attack Types:

- Infect a work laptop while connected to home network
- Compromise a website
- Compromise an advertisement on a website
- “Trojanize” online code

Direct Attack

To gain access to the target network through a direct attack, the attacker could use several tactics. An attacker can remotely access a network using stolen credentials, or try to physically access computers at the target location for direct access to the network. An attacker could also send a general phishing email with a malicious file or domain attached, hoping that the target will open it. More specifically, a phishing email can be tailored to one or more of the users at the target to provide a more believable disguise. Instead of focusing on the targeted network’s users, the attacker could also choose to exploit a server directly. Attacks can take almost an unlimited number of shapes and can be as diverse as domain name system (DNS) poisoning, email credential theft or a self-propagating worm that comes from an external network.

Indirect Attack

To compromise a network, the attacker can attempt to gain access with an indirect attack. For example, the attacker may infect a work laptop while it’s connected to a home network. Another option is to compromise a website or an advertisement on a website, in the hope that users from the targeted organization might visit the website and inadvertently drop malware to their endpoint. Finally, the attacker could “Trojanize” an online code by hiding malicious code in an otherwise legitimate application, web page, file or code base.

DEFINE ATTACK AS SUCCESSFUL OR FAILED

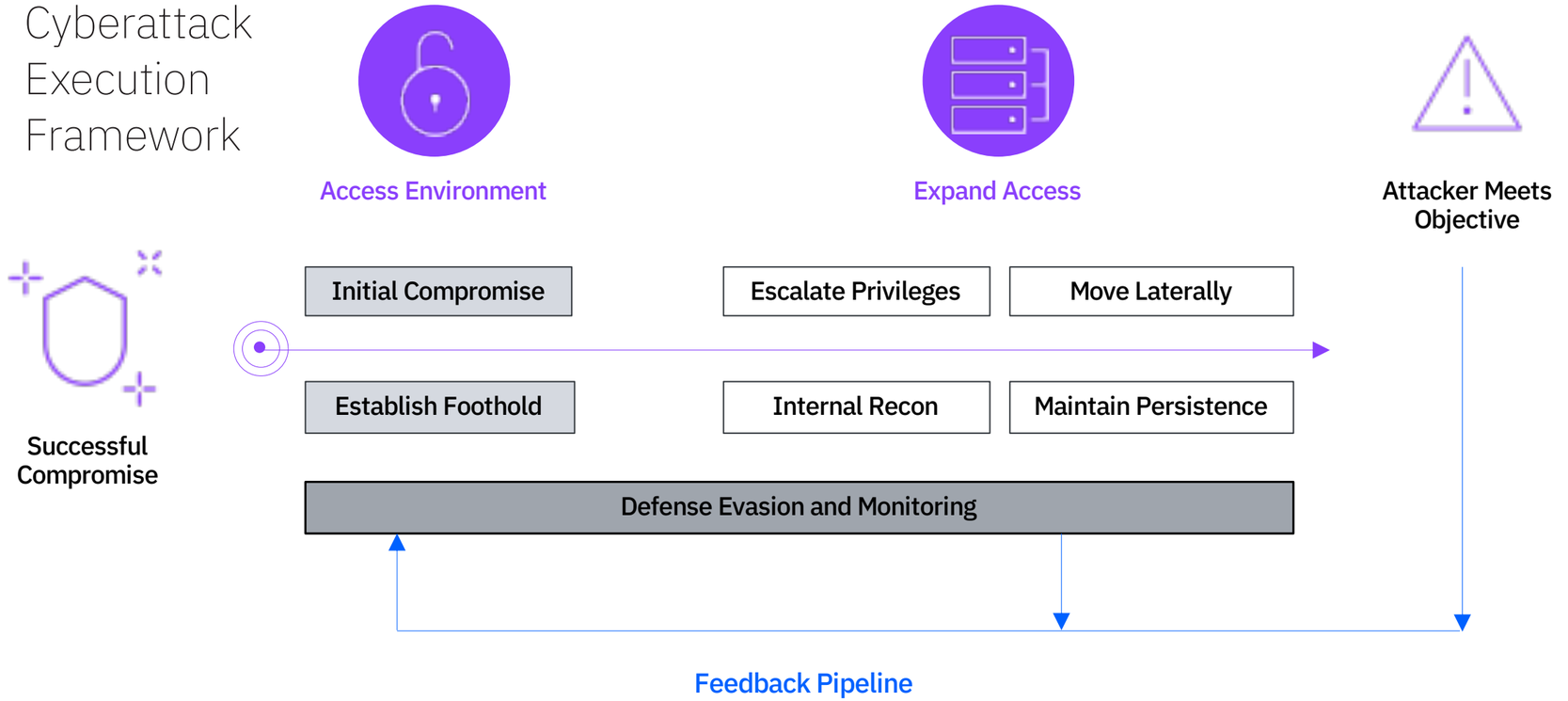
Finally, after an attack is launched, the attacker will determine whether the attack resulted in a successful compromise. If the attack fails, either completely or in part, the attacker may choose to return to one of the preparatory phases. The attacker could decide to alter aspects of the attack to increase the likelihood of success, leaving most of the attack intact. Or, particularly in the event of failure, the attacker may choose to move on to another, less protected target.

If the attack succeeds, the attacker will typically begin the phases of the X-Force cyberattack execution framework, using the access gained in the preparation framework.

05

Phases of the X-Force Cyberattack Execution Framework

The X-Force cyberattack execution framework includes the phases that occur after the attacker moves through the key phases of the X-Force cyberattack preparation framework, and successfully gains access to at least one host within a network, or has logged in to one or more user accounts. The X-Force cyberattack execution framework consists of eight distinct phases divided into three stages. Depending on the tools used and the attacker's objective, the phases of the attack framework can occur autonomously, by automating scripts and event-based instructions and configuration, or manually. Each method has its own advantages and disadvantages. For example, autonomous malware can spread through networks more quickly, while manual attacks can allow for more targeted and stealthier campaigns. Either type of attack tactic, whether autonomous or manual, can be modeled within this attack framework.



05

Phases of the X-Force Cyberattack Execution Framework

- The first two phases are part of the access environment stage. The initial compromise occurs after the attacker launches a successful attack and is a required first step in the cyberattack execution framework
- The second phase, establish foothold, occurs once an attacker gains access to a network. This phase is an initial requirement for the attacker to move on to any subsequent phases
- The next stage, expand access, includes four phases: escalate privileges, move laterally, internal reconnaissance and maintain persistence. These phases can occur simultaneously and through multiple iterations to accomplish the attack objectives. The attacker may choose to disregard some phases within the expand access stage or may not have the technological knowledge to accomplish all the phases
- Two phases, defense evasion and monitoring and feedback cycle, are included in the continuous attack stage because they occur throughout the entire span of malicious activity
- Defense evasion and monitoring include operational security measures and the attacker's TTPs for avoiding security tools, and frequently indicates a group's skill level
- The feedback cycle is when the attacker determines that there's a need to return to a previous phase described in the attack framework to further the same—or even new—mission objectives
- Finally, upon completion of the phases required for the specific attack, the attacker will execute their objective by completing the aims of the mission

IBM

05

Phases of the X-Force Cyberattack Execution Framework

Access Environment Stage

Once the attack is determined as successful, the attacker will have conducted the initial compromise and likely work quickly to establish foothold.

Initial Compromise

The initial compromise is the necessary first phase of the X-Force cyberattack framework and occurs after the attacker completes a successful launch attack phase as part of the preparatory steps. An initial compromise commences when the attacker has gained access to at least one host on the network or has logged into one user's account.

Tactics Used to Conduct the Initial Compromise Include:

- **Phishing or spear phishing:** A fraudulent email or electronic communication that targets a specific user or a specific industry to lure the user into revealing personal or confidential information, prompting them to click a link, or enticing the target to download a legitimate-looking attachment with hidden malware, which the attacker will use for illicit purposes.
- **Web compromise:** The general term used when attackers inject malicious code onto legitimate websites or web applications. Two examples are malvertising in which malicious code is injected into advertisements, and watering hole attacks in which a drive-by download is implanted into a web page that's frequented by a specific crowd of people.

05

Phases of the X-Force Cyberattack Execution Framework

Establish Foothold

During the establish foothold phase, the attacker ensures continued access to, and control of, at least one host or user account within the network. An attacker will aim to install a backdoor or to maintain another stealthy foothold in the network to remotely control the infected computer using an established C2 infrastructure.

From the foothold, the attacker can establish the outbound communication link to the C2 network. The communication between the victim and the attacker's command and control server is often encoded or encrypted in multiple layers, and its destination is obfuscated to prevent identification.

Tactics Used to Establish Foothold Include:

- **Backdoor:** Refers to any means that the attacker uses to access a host that bypasses the host's typical security and authentication mechanisms.
- **User account access:** Attackers may gain access to a user's online account, for example, remote access credentials, social network credentials or email credentials, to directly achieve their objective or pivot to other network resources.

Defending the Network

Although the hope is to protect a network from compromise completely, this expectation is rarely the case, and business leaders should operate under the assumption that their network is at risk of compromise. Therefore, the goal should be to prevent the attackers from reaching their objectives—either by defending the network internally or using an outside service provider. A defender's role in disrupting the attack begins with the initial compromise and establish foothold phases, where it's important to implement strong endpoint detection and mitigation strategies. Defenders should educate employees on common techniques that are used to compromise a network initially, such as spear phishing. In addition, defenders can closely monitor all network traffic, implement restrictions on any installation to prevent automatic malware installation, and filter against known exploits and malicious websites.

05

Phases of the X-Force Cyberattack Execution Framework

Defending the Network

A complex or advanced attack often requires the attacker to spend a lot of time and effort in the expand access stage. This stage provides an opportunity for a well-prepared defender to observe and counteract the attacker's actions that are taken within these phases. Defenders can restrict installation processes, enable strong access controls, and monitor all traffic within and leaving the network. Because these steps happen within the victim network—before the final objective is achieved— they represent the best opportunity that a defender has to prevent harm from occurring.

Options to Expand Access:

- Escalating privileges
- Moving laterally
- Performing internal reconnaissance
- Maintaining persistence

Expand Access Stage

The phases contained within the expand access stage include all the methods that attackers use to get from their initial compromises to the execution of their objectives. These phases don't need to happen sequentially; often, the phases will occur simultaneously and through multiple iterations. In some cases, such as an email account compromise, these phases can be skipped entirely.

Once attackers gain initial access to the network, they will attempt to gain further insight and expand access on the victim's network. Their options to expand access are through escalating privileges, moving laterally, performing internal reconnaissance, or maintaining persistence.

05

Phases of the X-Force Cyberattack Execution Framework

Escalate Privileges

During the escalate privileges phase, the attacker gains access to more resources within the compromised network. This access can include obtaining additional credential information, typically by obtaining usernames and passwords of users with greater access, stealing public key infrastructure (PKI) certificates, or accessing privileged accounts or computers. Although intruders will often try to gain administrator or full-system access, gaining credentials for a user who has more access than the initial intrusion host, and which helps adversaries achieve their goals, would also be considered an escalation of privilege.

Tactics Used to Escalate Privileges Include:

- Credential dumping: This term describes any tool that obtains username and password information from the operating system. Examples of credential dumping tools include Mimikatz and Windows Credential Editor (WCE).
- Pass the hash: A password hash is a one-way algorithm that provides a unique identifier for a plaintext password without revealing the password itself. A “pass-the-hash” attack occurs when the attacker will bypass authentication that requires the plaintext password by using stolen hashes.

05

Phases of the X-Force Cyberattack Execution Framework

Move Laterally

During the move laterally phase, the attacker moves to additional hosts on the network or additional networks— in the case of affiliated companies, merger targets, or third-party providers. This phase can use different tactics, or sometimes the same tactics— stolen credentials—as in the escalate privilege phase. The attacker will attempt to gain access to additional hosts to obtain data that wasn't initially available on the intrusion host, or to gain access to additional hosts for theft or destructive goals.

Tactics Used to Move Laterally Include:

- **Remote access:** Often a company will allow its users to connect to the network remotely. In these cases, attackers can use stolen credentials to access the network remotely, gain user-grade access, and disguise their activities as those of a legitimate user.
- **Schedule tasks:** This Windows feature allows the user to schedule programs or scripts to be executed at a certain time. The attacker can use this feature to execute code on start-up; for example, to establish persistence, or schedule an event at a certain date and time in the future. In addition, scheduled tasks can be exploited to remotely run malicious or destructive commands on additional hosts connected through the same network.
- **Net use command:** This command allows the attacker to configure connections to other resources that are mapped on the network and add connections to the network.
- **PsExec or PowerShell:** Both these Windows tools can allow the attacker remote command execution.

05

Phases of the X-Force Cyberattack Execution Framework

Escalate Privileges

During the escalate privileges phase, the attacker gains access to more resources within the compromised network. This access can include obtaining additional credential information, typically by obtaining usernames and passwords of users with greater access, stealing public key infrastructure (PKI) certificates, or accessing privileged accounts or computers. Although intruders will often try to gain administrator or full-system access, gaining credentials for a user who has more access than the initial intrusion host, and which helps adversaries achieve their goals, would also be considered an escalation of privilege.

Tactics Used to Escalate Privileges Include:

- **Credential dumping:** This term describes any tool that obtains username and password information from the operating system. Examples of credential dumping tools include Mimikatz and Windows Credential Editor (WCE).
- **Pass the hash:** A password hash is a one-way algorithm that provides a unique identifier for a plaintext password without revealing the password itself. A “pass-the-hash” attack occurs when the attacker will bypass authentication that requires the plaintext password by using stolen hashes.
- **Corrupt internal application or system:** Depending on the system configuration and applications available, the attacker may be able to inject commands or overwrite code to escalate permission levels remotely.

IBM

05

Phases of the X-Force Cyberattack Execution Framework

Internal Reconnaissance

Once attackers enter a network, they may collect additional information about the internal network through the internal reconnaissance phase. Intruders can gather information about users and groups on the network, see access levels used, and identify available files or databases. Intruders must establish what information they have access to and what data they may still need to accomplish their mission. Typically, attackers can accomplish internal reconnaissance using commands inherent to the operating system, but they can also use external tools, such as port scanners.

Tactics Used for Internal Reconnaissance Include:

- **System, account and application enumeration:** Malicious actors can use built-in commands or application features to identify whether a username exists in the system and then use brute-force techniques to determine the corresponding passwords.
- **Port scans:** Port scans or port scanners are tools used by the attacker to query the network for open ports to determine if there are any firewalls protecting the network. This reconnaissance tool can identify vulnerable access points.
- **File browsing:** An attacker will browse documents on the host computer and shared drives to find data of interest.
- **Service tickets:** Service tickets can be accessed through credential dumping tools and can give the attacker access to a specific resource.

05

Phases of the X-Force Cyberattack Execution Framework

Maintain Persistence

In the maintain persistence phase, attackers complete actions to strengthen and maintain their foothold, ensuring continued outside access throughout the environment. Attackers accomplish this goal by securing redundant and overlapping access to the network in case the system is restarted, an access point fails, or stolen credentials are denied. Often the attacker will place the initial backdoor in a registry location that ensures it will run each time the host is restarted to establish persistence immediately upon host compromise.

Tactics Used to Maintain Persistence Include:

- **Backdoor:** The attacker will use additional backdoors, described in the establish foothold phase, to increase redundancy, so that if one access point is removed or interrupted, the attacker still retains control using other entry points.
- **VPN abuse:** Attackers will use an authorized user's PKI or VPN credentials to remove the requirement to enter the system through a backdoor. This method may also help attackers hide within the network by disguising their traffic as that of a legitimate user's activity.
- **Webshell:** A webshell is a malicious script uploaded to a web server that gives the attacker the ability to remotely control the host.

IBM

05

Phases of the X-Force Cyberattack Execution Framework

Continuous Attack Stage

Within the X-Force cyberattack execution framework, there are two phases that are designated under the continuous attack stage—and the attacker will execute these phases during the entire intrusion. Defense evasion and monitoring include efforts to evade detection by the victim or defenders and the feedback cycle includes opportunities to reassess goals and tactics once inside a network.

Because a victim environment should be largely unknown to attackers, and can change depending on the defender's actions, attackers must be flexible as they react to the dynamic environment.

Defending the Network

Attackers use defense evasion and monitoring tactics to complicate the ability for defenders to find and remove attackers' foothold on the network. Defenders should closely monitor all network traffic, monitor endpoints and frequently search for any type of anomalous behavior. In addition, defenders should be cognizant of—and be prepared to react to— multiple attacker avenues of entry into the network. Removing multiple backdoors or reimaging a set of infected hosts may not completely remove attackers' access to the network.

05

Phases of the X-Force Cyberattack Execution Framework

Defense Evasion and Monitoring

The defense evasion and monitoring phase encompasses tactics attackers use to hide evidence of their network footprint. Unlike other phases described in the attack framework, defense evasion and monitoring can be conducted individually or as a combination of all other attack execution phases. This phase may include hiding malicious code within legitimate processes, log deletion or log destruction, clearing command history, packing, and encrypting and encoding communication and commands. In addition, some actors will practice “false flag” operations, which occur when the attacker attempts to use tactics employed by other threat actors to infer attribution that will pin the attack on another group. Attackers accomplish this tactic subtly by using a foreign language or by adjusting time stamps to suggest that the attack came from a different country; or more overtly, attackers will publicly self-identify with a false alias.

Some actors will respond if they perceive that they’re being identified by endpoint threat detection or incident response teams. In these cases, the intruders may monitor incident responders and their systems, try to disable any detection programs or try to remove their malware from the network before incident responders identify it. Finally, the attackers may maintain well hidden entry points in the network to enable future intrusions.

Tactics Used for Defense Evasion Include:

- **Rootkit:** This malicious computer software is designed to disguise its presence, and the presence of other malicious programs, by injecting into and modifying the operating system application programming interface (API) to fool antivirus programs.
- **Cryptography and steganography:** Cryptography refers to the masking of data or communications into text that’s unreadable without the key. Steganography, on the other hand, is the process of concealing data within data so that the existence of the message is hidden; for example, hiding data within an image, audio or video file.
- **Masquerading:** Masquerading occurs when the attacker places malicious code in a known trusted location and disguises it by naming it a trusted or common name that will bypass endpoint detection systems.

Tactics Attackers Use to Hide Network Footprint:

- Hiding malicious code within legitimate processes
- Log deletion
- Log destruction
- Clearing command history
- Packing
- Encrypting and encoding communications
- Encrypting and encoding commands
- “False flag”
- Using a foreign language
- Publicly self-identify with a false alias

05

Phases of the X-Force Cyberattack Execution Framework

Feedback Cycle

During the feedback cycle, the attacker likely will review the intrusion and compare results with the mission objective, and the attacker may return to and improve upon any phase of the attack. Based on information that's gleaned during all the other phases, the attacker may change tactics during the attack or for subsequent attacks. For instance, if a victim attempts to remove the attacker's access from the environment, the attacker may revise TTPs and enhance malware capabilities to reinsert access points into the same network—or for future attacks against other victims.

Execute Objective

By completing some or all the phases described in the X-Force cyberattack framework, the attacker hopes to complete the mission of the intrusion. Objectives vary depending upon whether the attacker has state-sponsorship, or may depend upon the attacker's motivation. An attacker seeking to perform espionage, for example, may consider data theft or reconnaissance as the principal goal. Other attacker objectives include destructive or disruptive cyberattacks, financial theft, ideological messaging, and nation state "soft power" influence campaigns.

Defending the Network

From a defender's perspective, the goal is to detect the attacker prior to this final phase. However, even if the attacker reaches this phase, the defender can minimize the impact of compromised data by restricting application control and using a data loss prevention tool to enforce strict data transfer controls. In addition, defenders can monitor egressing network traffic to stop outbound command and control communications.

IBM

06

Supplemental Information

Contributions by:
Jonathan Wrolstad, Alexandrea Berninger;
X-Force Threat Intelligence Production Team

X-Force Contact Information
To learn more about IBM Security X-Force incident response and threat intelligence services, please contact your IBM representative or IBM Business Partner, or visit www.ibm.com/security/services/xforce-incident-response-and-intelligence.

If you are experiencing a security breach, please contact IBM X-Force Incident Responders at:
1-888-241-9812 (US and Canada)
(001) 312-212-8034 (Outside the US and Canada)

© Copyright IBM Corporation 2021
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America February 2021

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, and PowerShell are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.