Know the Path of an Attack and Block it with Privileged Account Security

Table of Contents

Executive Summary

Organizations are struggling to stop advanced attacks from both external attackers and malicious internal users. These attacks target access to critical systems and valuable sensitive data. Advanced attacks accomplish this mission through a pattern of gaining access to accounts (i.e., local business user accounts) and using those to gain access to additional assets, accumulating privileges, and eventually reaching the target to complete the mission of the attack. Organizations must stop attacks in the midst of this lifecycle to help prevent successful cyber attacks and the ensuing damage they cause to the organization.

CyberArk's approach to stopping advanced attacks is to provide organizations with the capability to secure and monitor use of privileged accounts through a centralized privileged account security platform. This platform provides a comprehensive set of security controls including:

- **Protect credentials:** Organizations implement proactive controls that lock down privileged account passwords and SSH keys. By storing these credentials securely, restricting access to them, and automatically rotating them, organizations can reduce unauthorized use of privileged accounts.
- **Secure sessions:** Organizations secure and control privileged sessions with session isolation. This creates separation between an administrator's endpoint and critical assets, ensuring that malware on a user's endpoint cannot spread to a target asset. Session isolation also prevents privileged credentials from ever being seen by the user or reaching and being stored on a potentially compromised endpoint.
- **Enforce least privilege and endpoint protection:** Organizations limit administrative and super-user rights on servers and endpoints to mitigate intentional and accidental misuse of excessive privileges. Least privilege enforcement enables organizations to reduce the attack surface while also enabling users to remain productive by easily requesting elevated privileges when necessary. Organizations may also secure endpoints by closely controlling and monitoring applications via whitelist, blacklist, and "greylist" (restricting unknown applications).
- **Continuous monitoring:** Organizations implement continuous monitoring of all privileged account use, including live monitoring as well as behavioral analytics. Should an attacker manage to hijack a privileged account, continuous monitoring capabilities can help an organization detect the malicious behavior based on events or patterns of events that fall outside baselines generated specifically for the authorized user. Compromises can be addressed promptly by automatically rotating credentials or otherwise preventing continued unauthorized access to the affected privileged accounts.

This white paper explains how CyberArk's highly innovative and effective solutions help organizations to proactively mitigate the risk of cyber attacks and detect cyber attackers within the attack lifecycle before they complete their mission.

Modeling the Attack Lifecycle

Practically every organization is at risk of compromise from advanced attacks. These attacks are difficult to stop because advanced attacks use techniques that cannot readily be stopped using antivirus software and other signature-based tools. Or, if they are detected, it's too late to stop an attacker from exfiltrating data or disrupting business because detection occurs at the final stage of the attack lifecycle.

Safeguarding an organization from advanced attacks requires understanding attackers' techniques. Experts from CyberArk Research Labs used their experiences with real-world attacks to model the lifecycle of a typical attack. Figure 1 depicts this model.

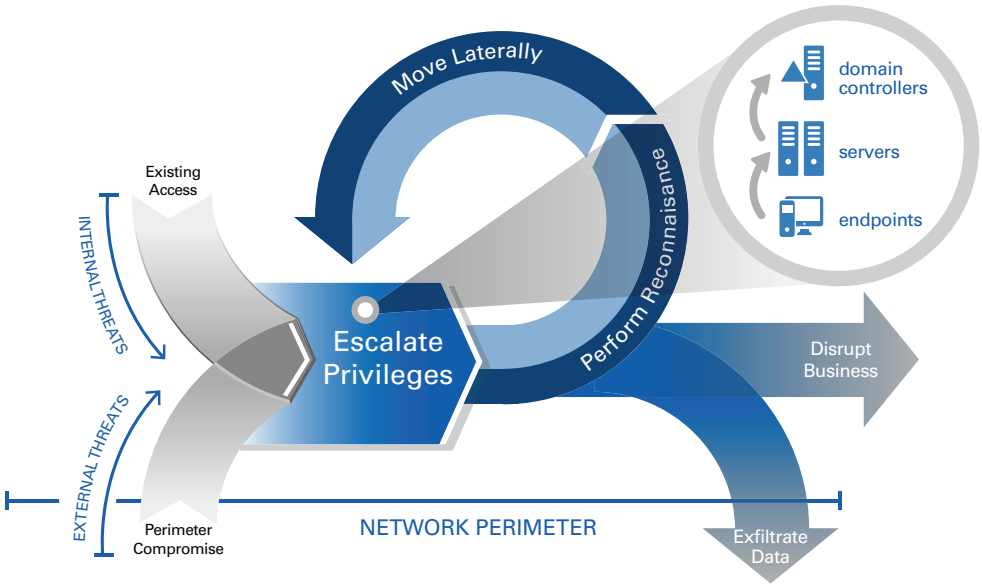

Figure 1: CyberArk's Attack Lifecycle Model

The attack lifecycle model has four steps:

Step 1: Acquire and use credentials with standard privileges within the organization's logical network perimeter.

Figure 1 displays two versions of step 1, one for external attackers and one for internal attackers. Step 1 is typically trivial for an internal attacker, such as an employee who already has access to an account. According to a recent study, insiders perform over 45 percent of data breaches.[1] For an external attacker, step 1 generally takes minimal effort, such as conducting a phishing attack. Once the attacker has successfully gained access to the network, step 1 is complete. Note that the remaining steps are the same for both internal and external attacks because at this stage, it doesn't matter whether an attacker originated from the inside or externally; they all use credentials to look like an insider.

Step 2: Escalate privileges if the attacker does not already have the necessary privileges.

There are many ways to escalate privileges, and they fall into two groups: increasing the privileges available to an existing account, and acquiring access to another account that has greater privileges. The former can potentially be achieved by exploiting operating system vulnerabilities or other weaknesses, while the latter usually occurs by gaining access to other account credentials that are not well secured.

1 Forrester Research, December 2014.
https://www.forrester.com/Despite+Scale+Of+Sony+Hack+Internal+Breaches+Most+Common/-/E-PRE7486

Step 3: Acquire access to the targeted assets.

Figure 1 represents this step as a loop with three sub steps:

- Step 3.1 is to perform reconnaissance using the escalated privileges. The purpose is to identify one or more accounts on one or more assets that should get the attacker closer to the goal.
- Step 3.2 is to select the next asset and account to target, hijack the account by stealing password hashes or other credentials with access to that asset, and then move laterally to that asset using the stolen credentials.
- Step 3.3 is to check if the targeted asset is now accessible. If it is not, the attacker will repeat steps 2 and 3 to further escalate privileges, perform additional reconnaissance, and make another lateral move. Steps 2 and 3 may be repeated many times before the targeted asset is reached.

Step 4: Leverage the access gained in order to accomplish the mission.

This can be carried out in a number of ways. Often attackers are seeking sensitive data such as credit card information, bank account numbers, healthcare information, personally identifiable information (PII), or intellectual property. In this case, the attacker may accomplish their mission by exfiltrating the targeted data to a location outside the organization. In other cases, attackers are attempting to disrupt business by causing physical harm or shutting down critical business systems and applications. Step 4 occurs when the attacker has gained privileged access to the target asset and is able to carry out their mission successfully.

Throughout the attack lifecycle, the attacker may use acquired privileges to disable, reconfigure, or otherwise prevent the organization's security controls from detecting and stopping the attack in progress.

Once step 4 has been completed, much of the damage has already been done. Even if an organization detects an incident at this stage, for example detecting in-progress data exfiltration, it may be too late to prevent damage. This is why it is so important for an organization to detect and stop attacks as early in the attack lifecycle as possible. On the other end of the lifecycle, it is nearly impossible for organizations to keep all attackers outside their perimeters, so even though perimeter security is important, organizations should not concentrate all resources on stopping attacks at step 1. Accordingly, organizations should focus on disrupting the attack lifecycle during steps 2 and 3. The rest of this paper provides recommendations for doing that.

Proactively Mitigating Attacks Exploiting Privileged Accounts

The attack lifecycle relies on gaining access to privileged accounts – accounts with higher privileges than standard user accounts, such as the ability to administer an asset's operating system, applications, and data. Privileged accounts are prized by advanced attackers, not only because each account can provide full access to a particular asset or application, but also because a single account often provides administrative privileges on multiple assets. This allows an attack to easily progress from asset to asset within an enterprise, compromising each asset along the way and eventually reaching the target asset and accessing its sensitive data and/or controls.

CyberArk's proactive approach to breaking the attack lifecycle is to make it much more difficult for advanced attackers to obtain the credentials of privileged accounts and to help reduce any unauthorized access that they do manage to acquire. Organizations may implement this approach through CyberArk's comprehensive Privileged Account Security solution built on a single integrated platform. This solution helps an organization secure credentials, isolate and control privileged sessions, enforce least privilege policies, and continuously monitor these sessions for unusual or suspicious behavior.

Characteristics of the CyberArk approach and its benefits for disrupting the attack lifecycle empower organizations to include the following:

- **Secure storage for privileged credentials.** All privileged account credentials, including passwords and SSH keys required by users and applications, may be strongly safeguarded in a secure vault, and access to credentials is usually granted via successful multifactor authentication. This makes them less susceptible to compromise than credentials that are stored insecurely on administrator laptops, typed in on malware-infected devices that capture keystrokes, hard-coded and embedded into application scripts, or otherwise exposed to more threats by being used from end user devices. The securing of privileged credentials is key to help organizations mitigate risk at every step in the attack lifecycle.
- **Automatic rotation of privileged credentials.** A major security challenge for organizations is frequently rotating privileged credentials throughout the enterprise, including administrative passwords and SSH keys for every piece of hardware and software. When credentials are infrequently rotated, they can be reused for an extended period of time until they are eventually (if ever) rotated. Former employees may be able to access accounts long after they have left an organization, and attackers can have access to an account for an extended period of time. By enabling automatic connections to target systems, the organization can establish strong, unique passwords for privileged accounts and rotate them regularly, without ever disclosing the passwords to users. The regular rotation of passwords can help prevent unauthorized credential access and reduce the risk of attack techniques such as "Pass-the-Hash" that leverage static password hashes stored on endpoints during and after authentication. An organization can significantly decrease the likelihood of an attacker successfully moving laterally throughout the organization by implementing unique privileged credentials that are regularly rotated.
- **Isolation and control of privileged account sessions.** Organizations often support a wide range of end users who require access to privileged credentials including temporary employees, contractors, and third party vendors. To help protect the critical assets that various individuals are accessing, organizations can secure privileged sessions by isolating session activity in a secure environment. Session isolation prevents malware from spreading to critical systems by ensuring that all privileged sessions take place through a secure proxy server that separates the end user machine from the target system. In addition, session isolation prevents the privileged credential from being exposed on the user's endpoint. Session isolation is an important security measure that helps mitigate the risk of attackers moving laterally to gain access to target assets because access is strictly controlled and monitored by the organization through the proxy server.
- **Policy restrictions on administrator actions and endpoint protection.** Although administrative accounts typically grant full access to an asset, an end-to-end privileged account security solution enables an organization to issue more granular privileges via policies. Examples include an organization providing only the necessary privileges to each user/asset combination (i.e., the principle of least privilege), specifying which commands each user can or cannot perform on each asset, controlling and monitoring which applications are permitted to run, and setting days of the week and times of the day when each user can have a privileged account session with each asset. On endpoints, an organization can remove local administrator permissions from the business user, dramatically reducing the risk of successful compromise of endpoints. These restrictions help organizations prevent progression of an attack early in the attack lifecycle - at the first compromised endpoint - by preventing an attacker from gaining elevated privileges, reducing the risk of users to intentionally or accidentally execute harmful commands, and assisting in controlling and monitoring applications on endpoints.

Limits on Lateral Movement

The CyberArk Solution can greatly reduce an attacker's ability to perform lateral movement within the organization's perimeter. The CyberArk Solution helps organizations limit the use of privileged accounts, which makes it much harder for attackers to navigate the network, gather data about its assets, and gain access to additional assets in an organization.

No matter how effective attack mitigation measures are, such as tightly locking down privileged credentials and isolating and controlling privileged account sessions, improper use of privileged credentials can still occur, whether accidental or intentional. A classic example is an administrator who misuses privileges to steal sensitive data. The next section of this white paper focuses on the importance of continuous monitoring, using data analytics, in breaking the attack lifecycle.

Continuously Monitoring Privileged Account Use for Attack Detection and Containment

When protecting against advanced attacks, a layered defense is a must-have. The next – and often last – layer of security is attack detection and containment. The goal for attack detection and containment measures is to find an attack in-progress, stop it from proceeding any further, and prevent continued access to the assets that were already compromised.

As previously discussed in this white paper, the earlier in the attack lifecycle that the attack can be detected, the sooner that security teams can respond and prevent further damage. One key to detecting attacks faster is to focus an organization's security analytics on a critical area – privileged account use – instead of trying to do analytics on everything at once. Privileged accounts are at the heart of the attack lifecycle, and most cyber attacks could not be completed without attackers first gaining access to privileged accounts[1]. By focusing on privileged account use, organizations can make great progress in detecting and stopping attacks, thereby limiting potential damage.

The CyberArk Solution is designed to carefully analyze privileged account usage using its self-learning analytics engine. The solution includes a complex combination of proprietary algorithms including both deterministic algorithms and on-going behavioral analytics on users and entities, such as endpoints and servers. The CyberArk Solution assigns a risk score to each security incident which indicates its relative severity as compared to other anomalous events, and alerts security teams of the incident.

Here are some basic examples of how the CyberArk Solution can enable an organization to detect suspicious activity involving privileged account use:

- A privileged user accesses a server containing sensitive data. Because this server is critical, the organization has locked down the privileged credentials that enable access to this server. It's important for organizations to monitor privileged account usage to ensure that the established controls work properly. By analyzing a combination of data inputs, the CyberArk Solution determines that this login attempt is malicious because the user did not properly request the privileged credential from the CyberArk Digital Vault before accessing the server. This activity generates a threat alert with an associated high risk score, so security teams are equipped with the intelligence needed to quickly respond. The security team can even respond to the attack by rotating the impacted credential to stop the user from continuing the suspected attack.
- An attacker manipulates Kerberos tickets in order to authenticate to various assets, all while appearing as an authorized user. Kerberos attacks are particularly difficult to detect because attackers look exactly like authorized users, so traditional endpoint monitoring solutions typically cannot detect these attacks. The CyberArk Solution monitors and conducts analytics on endpoint data as well as network traffic, which helps enable the solution to detect anomalies in Kerberos traffic. Therefore, the CyberArk Solution can help detect and alert on Kerberos attacks earlier in the attack lifecycle, enabling security teams to promptly respond to these potentially catastrophic attacks.

Once a security incident is detected, the next step that security teams must take is to respond to the threat. The CyberArk Solution offers an innovative feature for incident response when there is an indication of compromise. When the CyberArk analytics engine detects a suspected stolen privileged credential, the solution can automatically rotate the credential in the CyberArk Digital Vault. This helps prevent the compromised account from being used again by an attacker, such as to perform lateral moves between assets, while still allowing authorized administrators accessing the credential in the CyberArk Digital Vault to access and use the new credential.

1 CyberArk Threat Report: Privileged Account Exploits Shift the Front Lines of Cyber Security

Benefits of an Integrated Platform

There are two major approaches to privileged account security technology. The first is to have a single integrated platform, with all its components created and maintained by a single vendor. CyberArk Solutions are built on the CyberArk Shared Technology Platform which enables organizations to deploy a single infrastructure and expand the solution efficiently and cost-effectively to meet expanding business needs. A single infrastructure also offers administrators a single-pane-of-glass interface for centralized management and unified auditing and reporting.

The second approach is to have a multivendor solution, which has components from two or more vendors. These approaches can be hard to distinguish because portions of some solutions come from third parties, such as original equipment manufacturers (OEMs) and other partners. It is important to research any potential privileged account security product to determine the origin of each of its components.

Having a single integrated platform for privileged account security is superior to using a multivendor solution because an integrated solution is needed for an organization to achieve effective and efficient attack mitigation, detection, and containment. Multivendor solutions may not be integrated, and as a result, they are less capable at tracking an attacker across systems, identifying subtle deviations from expected patterns of behavior, and otherwise rapidly and accurately detecting and stopping advanced attacks. Other disadvantages of multivendor solutions may include diminished capabilities for centralized management and reporting, as well as a potential higher total cost of ownership.

Conclusion

The CyberArk Solution is designed to break the attack lifecycle in order to help prevent successful cyber attacks and the damage they cause to the organization, including potential financial loss and damage to the organization's brand and reputation. By focusing on privileged account security, the CyberArk Solution helps stop attackers before they can successfully accomplish their attack mission.

The CyberArk Solution protects enterprises from advanced attacks through a centralized privileged account security solution built on a single platform. To proactively protect and control access to privileged accounts, organizations can use the CyberArk Solution to store privileged credentials in a secure digital vault that regularly rotates them. The CyberArk Solution can also help enforce organizational policy restrictions to limit intentional or accidental misuse and isolate privileged account sessions to limit interactions between an administrator's endpoint and target assets.

In addition to reducing the risk of privileged account misuse, the CyberArk Solution offers fast detection for cases where misuse does occur. The solution continuously monitors privileged account usage to identify anomalous activity. Its self-learning analytics engine establishes baselines of normal activity and uses them to identify anomalous activity. The analytics engine can be used to detect both external and internal attackers attempting to use privileged accounts to gain unauthorized access to assets, steal account credentials, and perform other malicious actions. The CyberArk Solution can alert administrators when a compromise is detected and automatically rotate or disable credentials to prevent further access using the compromised credential.

Stolen, abused and misused privileged credentials are used in nearly all cyber attacks[2]. The CyberArk Solution can assist with stopping attackers before they gain access to their ultimate target by focusing on proactively protecting an organization's privileged accounts and continuously monitoring their usage for early detection. With the CyberArk Solution, an organization can better safeguard their sensitive assets and reduce damage to the organization caused by attempted cyber attacks.

2 CyberArk Threat Report: Privileged Account Exploits Shift the Front Lines of Cyber Security

About CyberArk

CyberArk is the only security company laser-focused on striking down targeted cyber threats; those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world's leading companies – including 40 of the Fortune 100 – to protect their highest-value information assets, infrastructure, and applications.

For additional information, visit **www.cyberark.com.**