GLOBAL COMMUNICATION SOLUTIONS PROVIDER

CASE STUDY

CYBERARK®

Company: Global Communication Solutions Provider - USA

Global Communication Solutions Provider Deploys CyberArk Privileged Access Manager Solution to Mitigate the Threat of Pass-the-Hash Attacks

Annual Revenue: $8.69 billion USD (2012)

Employees: 22,000 employees in 65 countries; Sales in 100 countries

CyberArk Product & Services:
CyberArk Privileged Access Manager Solution

Platforms: Windows servers and admin accounts

> "CyberArk makes the whole process painless to the end user. Their solution is extremely intuitive and easy to set up. The solution protects all of our admin and privileged accounts and enables us to tout our strengthened Smart Card security posture to all of our customers."

Security Solutions Architect at
Global Communication Solutions
Provider

CyberArk solution Highly Relevant Mitigation Steps to Combat Advanced Threats and Improve Privileged Access Security

CyberArk's customer, a publicly-traded provider of communication solutions and services to enterprises and governments, is well established as a proactive, security-aware organization. However, as a global business with access to sensitive customer information, the company is also frequently a target of increasingly sophisticated cyber-attacks.

ABOUT PASS-THE-HASH ATTACKS

One type of attack, in particular, began to incite significant concern across the organization—an advanced threat known as a Pass-the-Hash attack that targets Windows operating systems. These types of attacks generally involve cyber attackers who seek to capture account logon and password credentials on one machine and then use these credentials to authenticate to another machine. Usually, the credentials are present in hashed form—hence the name—and serve as an authenticator to access services on the network.

In this type of attack, the attacker obtains an endpoint in the network and then harvests the hashes. This approach is usually performed by a user with local administrative permissions. These can be obtained by various methods, including a stolen SAM Database, Dump LSASS.exe or other means. Hashes on endpoints may include the credentials for the active user, as well as those for network administrators or services that perform privileged actions on the endpoint (through remote access, for example).

Ultimately, the ability of an attacker to steal and use the hash of an administrative password presents a significant vulnerability. The attacker can continue to move from endpoint to endpoint, across the network, while executing commands with the appropriate, stolen privileged account.

THE CHALLENGE: SMART CARDS INCREASE THE RISK OF PASS-THE-HASH DAMAGE

For this global communications company, Pass-the-Hash attacks posed an immediate and troubling challenge. While the company was able to identify the existence of these types of attacks before a serious breach occurred (evidence of password theft and password cracking was clear and eminent), they struggled with the unique nature of a stolen hash. As a first step, the IT team opted to restrict access to their admin and privileged accounts by issuing Smart Cards. Unfortunately, this did not solve the problem, as vulnerabilities persisted within these Smart Card-enabled accounts.

Smart Cards, which are touted to prevent credential theft through multifactor authentication, actually exacerbate the problem. With Smart Cards, the passwords associated with each privileged account, by default, never expire and are never changed again. As a result, once the hash is stolen, the attacker can exploit it in perpetuity.

To truly combat Pass-the-Hash attacks against Smart Card-enabled admin accounts, the organization would need to deploy a custom solution that ensures admin and privileged passwords are automatically changed with some frequency to proactively protect against stolen credentials and abuse.

SOLUTION: CYBERARK PRIVILEGED ACCESS MANAGER SOLUTION TO THE RESCUE

Fortunately, the communications company simultaneously initiated a search for a password management solution to proactively manage all of their local, built-in privileged accounts. After reviewing multiple solutions, the company selected the CyberArk Privileged Access Manager Solution. The company chose CyberArk due to the robustness of the solution and its ability to restrict and protect privileged domain accounts.

Soon after deployment, however, members of the security solutions team were able to identify a more critical use case for the CyberArk solution. Out of the box, the solution also enabled the organization to limit the ability of administrators to inadvertently expose privileged credentials to higher risk computers and Pass-the-Hash cyber attackers. Through role-based access control, the organization can identify and manage Smart Card-enabled privileged accounts, assigning strong and rapidly changing passwords that prevent attackers from stealing credentials and authenticating across the network.

Moreover, the organization now controls, manages and logs the use of all privileged user credentials with the CyberArk solution. Looking ahead, the company plans to leverage the CyberArk Privileged Access Manager Solution to enforce other highly relevant mitigation steps, including:

- Unique password changes for every privileged user and service accounts (such as Windows Services, Scheduled Tasks, IIS App Pools and others) – this mitigates the dangers of password reuse.
- Automation of random and complex passwords.
- One-time password changes for privileged access – whenever a Windows domain admin uses a privileged credential, it is replaced with a new one. If the privileged credential is changed right after its usage, the window of opportunity for the attacker is very narrow.

Challenge

- Proactively protect and secure privileged accounts against Pass-the-Hash attacks.

Key Benefits

- Painless implementation and integration of CyberArk Privileged Access Manager Solution across all admin accounts.
- Increased Smart Card-enabled privileged access security.
- Elimination of privileged password theft/abuse and advanced Pass-the-Hash attacks.

RESULTS: INCREASING PRIVILEGED ACCESS MANAGER SECURITY, ELIMINATING PASS-THE-HASH AND IMPROVING SMART CARD SECURITY POSTURE

The CyberArk solution was easy to deploy. The process involved little coordination with other departments and, within days, the organization was able to begin creating policies, define them and apply them to protect their privileged accounts.

Since implementation, the organization has yet to have one single Pass-the-Hash attack or incident involving highly privileged accounts, and there have been no other indicators of future attacks. Moreover, the CyberArk solution has eliminated any and all abuses of privileged accounts across the customer's entire network.

"CyberArk makes the whole process painless to the end user. Their solution is extremely intuitive and easy to set up. The solution protects all of our admin and privileged accounts and enables us to tout our strengthened Smart Card security posture to all of our customers," remarks one of the company's Security Solutions Architects.

The organization continues to praise CyberArk as an easy tool that is "invisible to users" and "functionally solves a long term problem." Just as importantly, the company can now demonstrate to their customers that their Smart Card-enabled accounts are secure and protected from theft and abuse.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.