CYBERARK

SOLUTION BRIEF

SOLARWINDS BREACH: IDENTITY SECURITY BEST PRACTICES TO REDUCE RISK AND REGAIN CONTROL

INTRODUCTION

In December 2020[1], a supply chain attack trojanizing SolarWinds Orion business software updates was discovered to have impacted over 18,000 organizations. During the initial investigation, the attack revealed itself to be a part of a highly sophisticated global intrusion campaign utilizing a supply chain attack vector. The attackers were successful in infiltrating many high-profile organizations both public and private, through the use of extremely intelligent and evasive attack techniques. The use of compromised administrative privileged accounts and credentials was instrumental in the success of this attack.

HOW DOES PRIVILEGED ACCESS APPLY TO THE SOLARWINDS BREACH?

Once the attackers have an established foothold, they can attack any organization impacted by the SolarWinds breach by following well established steps in the attack chain by: 1) traversing the network looking for high-value targets, 2) gaining unauthorized access to privileged account credentials, and 3) using elevated privileges to steal confidential information. The SolarWinds breach and the resulting attacks on U.S. organizations exhibit all three of these tactics.[2] In light of this, it is worth noting that Identity Security solutions provide key capabilities to assist in 1) preventing credential theft, 2) stopping lateral and vertical movement within the network, 3) limiting privilege escalation and abuse and 4) enabling risk aware, adaptive Multi-Factor Authentication (MFA).

NEXT STEPS FOR IMPACTED ORGANIZATIONS TO TAKE

Organizations that may have been compromised by the SolarWinds breach should take steps to rapidly secure privileged access and to help mitigate and prevent the progression of the attack. Based on CyberArk's experience and expertise, the following steps are recommended to help provide organizations quick and effective controls to regain command and control over privileged access and credentials, which can be found in the CyberArk Security Fundamentals guide. Once the immediate tasks outlined below are completed, organizations must next focus on strengthening and enhancing already deployed controls.

IMMEDIATE REMEDIATION STEPS:

- Deploy a Privileged Access Management (PAM) solution or validate existing PAM deployment
- Run a CyberArk DNA scan to identify additional administrative accounts in the network
- Rotate credentials on a regular cadence
- Restrict access to Tier0 assets from a specific, hardened control point
- Isolate sessions when privileged credentials are used
- Detect backdoor account creation
- Deploy "least privilege" measures to endpoints and workstations (including those used to administer the PAM solution)

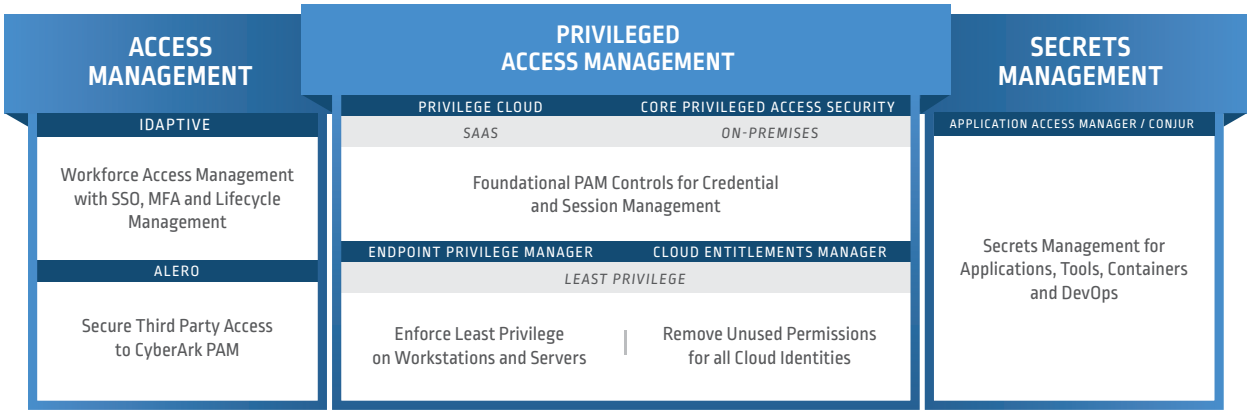
- Monitor for managed credential use outside the PAM solution
- Establish normal behavior patterns of existing users and elevate to stronger authentication on anomaly detection
- Enable risk aware, adaptive Multi-Factor Authentication (MFA) whenever possible

LONGER TERM STEPS:

- Follow CyberArk's Blueprint strategy for PAM success
- Deploy "least privilege" measures to servers and applications
- Secure application credentials and continuous integration/development (CI/CD) pipelines
- Configure Active Directory based on credential boundaries
- Identify all possible points of entry (i.e. VPN, SSO etc.) and implement adaptive MFA
- Replace antiquated authentication protocols such as RADIUS with more modern ones like SAML, OIDC, OAuth 2.0. with MFA implemented

CyberArk is ready and willing to help organizations follow this process to maximize security quickly and effectively. Partner with CyberArk to create a fast-tracked implementation of a targeted set of controls to shut down the privileged pathway. A comprehensive Identity Security program will help address the gaps and vulnerabilities that the attackers in the SolarWinds breach took advantage of such as gaining administrative access through compromised credentials, and the escalation of privileges and permissions. CyberArk delivers deep identity security controls and privileged remediation services that can buy you invaluable time in detecting attacks earlier, and preventing attackers from reaching their end goal of data theft or disruption. Click here to find out how CyberArk can help you secure privileged access today.

CYBERARK IDENTITY SECURITY PORTFOLIO



SECURITY FIRST APPROACH | AI-POWERED | FRICTIONLESS EXPERIENCE | EVERYWHERE

[1] Reuters, REFILE-EXCLUSIVE-U.S. Treasury breached by hackers backed by foreign government – sources, December 13th, 2020

[2] CRN News, Security: VMware Flaw Used To Hit Choice Targets In SolarWinds Hack: Report, December 18, 2020