New Report Connects Privileged Account Exploitation to Advanced Cyber Attacks

April 24, 2013 4:32 PM ET

CyberSheath Releases APT Privileged Account Exploitation Research Report; Finds Properly Secured Privileged Accounts Reduces APT Exposure

NEWTON, Mass. - April 24, 2013 - Organizations can significantly reduce the threat of targeted attacks by proactively securing privileged accounts, according the first APT Privileged Account Exploitation research report. Compiled by CyberSheath's advanced security investigations team and commissioned by CyberArk, the report reveals that the theft, misuse and exploitation of privileged accounts is a key tactic in each phase of an Advanced Persistent Threat (APT) attack cycle.

CyberSheath's APT Privileged Account Exploitation report compiles interviews with leading CISOs and security professionals at organizations that collectively have more than $40 billion in annual revenues and more than 170,000 employees around the globe. CyberSheath combined these interviews with the analysis of several high-profile cyber attacks and related industry research from the past year to detail how privileged accounts are increasingly being used in advanced and targeted attacks to compromise organizations and steal data.

Key Findings of the APT Privileged Account Exploitation Research Report

- **The Compromise of Privileged Accounts was a Crucial Factor in 100 Percent of Advanced Attacks:** CyberSheath found that the absence of fundamental access control measures was a crucial factor in all of the recent high-profile attacks that were examined, including the South Carolina Department of Revenue, The University of Georgia, the NASA Jet Propulsion Library, Red October, Utah Department of Health, Toyota, The Swiss NDB Intelligence Service, Saudi Aramco, and Global Payments.
- **Attacks That Use Privileged Accounts are More Difficult to Detect, Shut Down and Remediate:** Attacks that leverage privileged accounts can delete logs to make forensic analysis more difficult and can be used to install new malware to evade detection and open more doors. In addition, privileged account use appears as normal traffic flow and is not detected by traditional means. Finding illicit privileged account use among legitimate processes is like finding a needle in a stack of needles.
- **Attacks That Exploit Privileged Accounts are More Damaging and Expensive:** Eradicating attackers from a compromised network can be extremely expensive and painful. In addition to the high-costs associated with data breaches (the average cost of a data breach is $2.4M over a two year period[1]), the efforts to remove well-entrenched attackers from a network requires multiple remediation steps that can take thousands of man-hours of work.
- **Properly Secured Privileged Accounts Can Significantly Reduce APT Exposure:** Locking down privileged accounts and preventing their use in APTs moves up the kill chain and helps thwart attack progression at the delivery stage, as opposed to the command and control stage.

Best Practices for Preventing APT Privileged Account Compromise

- Isolate, monitor and control every access point to all critical business systems
- Change default passwords on all servers, databases, applications and network devices
- Remove hard-coded passwords from scripts, configuration files and applications
- Employ technical means of automatically enforcing enterprise password policies
- Control access by enforcing least privilege
- Use multifactor authentication for access to privileged accounts
- Increase password complexity
- Use a unique password for each local administrator account
- Remove local administrator rights from the majority of users
- Reduce the number of privileged domain-wide service accounts

- Automatically change passwords on a periodic basis and immediately upon suspicion of misuse
- Monitor and record all activities associated with administrative and privileged accounts
- Implement tamper-proof logging, auditing, and alerting on privileged access

A full copy of the report can be accessed **here**.

Supporting Quotes:

"The theft and exploitation of privileged accounts is a critical and devastating part of the APT attack cycle. These accounts provide wide ranging access in the enterprise and enable attackers to easily simulate normal business traffic, making infiltrations extremely difficult to detect. Our examination showed that almost every major cyber-incident in the past couple of years involved privileged accounts. The protection, accountability and management of privileged accounts are the very first steps organizations need to take to stop targeted attacks."
- Eric Noonan, CEO, CyberSheath

"Privileged accounts have typically been viewed as the powerful IT administrator or super-user accounts. This old notion ignores the reality that the use of privileged accounts has expanded significantly throughout the enterprise. Privileged accounts also include default and hardcoded passwords, as well as application backdoors. These accounts exist everywhere - in servers, network devices, applications and more. Security needs to start with identifying and securing every one of these powerful accounts and automating the controls around them. Cyber-attackers know these weak spots exist and will do anything to gain access. By cutting off the means for attackers to travel freely and hide their tracks, organizations can reduce the APT threat."
- John Worrall, CMO, CyberArk

Twitter: **@CyberArk**
Free Privileged Account Security Risk Assessment: **http://www.cyberark.com/discover-dna**
Webinar: CyberArk will be holding a Webinar on these findings on May 29th, 2013. Register to attend **here**.

About CyberArk
CyberArkÂ® Software is a global information security company that specializes in protecting and managing privileged users, sessions, applications and sensitive information to improve compliance, productivity and protect organizations against insider threats and advanced external threats. With its award-winning **Privileged Identity Management**, **Privileged Session Management** and**Sensitive Information Management** Suites, organizations can more effectively manage and govern data center access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments. CyberArk works with more than 1,200 customers, including more than 40 percent of the Fortune 100. Headquartered in Newton, Mass., CyberArk has offices and authorized partners in North America, Europe and Asia Pacific. For more information, please visit **www.cyberark.com**.

[1] Ponemon Institute, 2011 U.S. Cost of a Data Breach Study

Wednesday, April 24, 2013 - 12:00