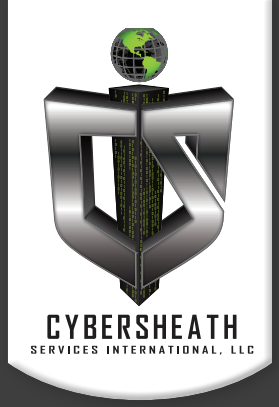

APT PRIVILEGED ACCOUNT EXPLOITATION

SECURING ORGANIZATIONS AGAINST ADVANCED, TARGETED ATTACKS

By CyberSheath Services International, LLC

Commissioned by Cyber-Ark Software

April 2013

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Companies of all sizes today face an unprecedented number of cyber attacks on their networks from organized, patient, and well-funded groups targeting specific information. Advanced, targeted attacks follow a common, multi-stage approach to breaching defenses, gathering and exfiltrating critical data.

Looking closely at the Advanced Persistent Threat (APT) attack pattern reveals that the theft, misuse, and exploitation of privileged accounts is a key tactic in each phase of the APT's methodology. A privileged account is any login ID on a system or application which has more privileges than a general user. Privileged accounts are normally used by system administrators to manage the system, as service accounts, or by applications to connect to one another. Privileged accounts are pervasive throughout any organization, with some studies indicating that they are more numerous than general user accounts.

Compromising privileged accounts is on the critical path to success for advanced attackers as they progress from network intrusion through lateral movement and ultimately to data theft. Nearly all of the most prominent reported data breaches of 2012 involved some form of credential theft or account misuse. Surprisingly, few solutions offered to CISO's and Security teams today focus on protecting privileged accounts and preventing their compromise.

In fact, many of the solutions marketed to CISO's presuppose privileged account compromise and lateral movement, operating on the premise that it's a foregone conclusion that the APT will steal and exploit valid privileged account credentials. Instead, the focus of defending networks and data is often geared towards reacting to constantly changing tactics in the form of zero day exploits, new malware and sophisticated spear phishing campaigns.

A CISO can spend a large portion of their budget on tools that try to predict attacker behavior that often at best simply rely on signatures from other previously known attacks. When these tools fail, as inevitably they will, CISO's are left with an incident to respond to and a steady diet of spend, remediate, and operate. So what's a CISO to do? Is there a way to get off the hamster wheel of incident response and begin to try and be proactive rather than reactive?

The answer is yes and the opportunity to do so resides in protecting, accounting for, and gaining real-time intelligence and visibility of privileged accounts through the use of security tools designed to effectively control credentials.

Privileged account credentials represent a known entity that if secured and controlled properly, could significantly disrupt the APT attack cycle. This concept of protecting privileged accounts to prevent data breach is acknowledged and endorsed by top cyber executives as well as government, commercial, and other subject matter experts as a matter of established best practice.

As a CISO, how can you afford to pass on the opportunity to measurably reduce successful APT attacks and concede ownership of the keys to your kingdom without attempting to protect them?

ADVANCED ATTACKS CONTINUOUSLY TARGET PRIVILEGED ACCOUNTS

CyberSheath conducted this descriptive benchmark study, representative of a non-statistical sample of 10 leaders in the cyber community, including 4 CISO's and 3 security operations center directors of U.S.-based organizations that collectively have annual revenue exceeding $40 billion dollars. With security oversight of more than 170,000 employees across the globe in the defense, financial, and technology sectors, these industry leaders oversee mature incident response programs and have experience defending against sophisticated, targeted threats. Additionally, former government executives with unique visibility to advanced persistent threat attack data across Department of Defense components were surveyed. Information gathered during research is sensitive and confidential and given the nature of the data, all respondents requested that their participation be anonymous.

Of those interviewed, each one confirmed that **the compromise of privileged accounts was a key stage in 100% of all advanced attacks.** With no uncertainty, every respondent agreed that credential theft and misuse is involved in every single targeted attack they respond to. In fact, the ability to takeover and utilize legitimate credentials during the attack, said one SOC Director of a Fortune 500 Company, was a reliable enough indicator toclassify an attack as APT. "Attackers use this because it's easy," said one former government executive charged with collecting and collating attack information across .com, .mil and .gov networks. "Hash passing and reuse is a high probability vector."

Most respondents conceded that APT compromise of privileged account credentials was "unavoidable"in their current environments, and had accepted this as an unanswered APT capability. Nearly all focused their security efforts on detection and containment after the fact. Few had implemented any advanced protections for privileged accounts, with most just employing the basics of password management and end user training.

When asked if providing greater protection, accountability, and intelligence around privileged accounts would influence the effectiveness of advanced attacks, ***every*** respondent confirmed that this would make a "significant" impact. One SOC Manager confirmed that removing the adversary's ability to compromise privileged accounts would "essentially stop their ability to move laterally throughout the network."

> **"IF AN ASSET IS SECURED SO THAT IT NEEDS A PRIVILEGED ACCOUNT TO ACCESS IT, THEN PROTECTING PRIVILEGED ACCOUNTS IS EFFECTIVE AGAINST APT ATTACKS ON THAT SYSTEM."**
>
> SOC Director, Fortune 1000 Company

Finally, when surveyed as to why their organizations had not implemented a program to protect privileged accounts, CISO's generally responded that privileged account protection strategies got lost in "boil the ocean" identity management discussions.

Identity management projects are often an albatross around the neck of a CIO. They ordinarily start out under the veil of improving the user experience and quickly devolve into expensive, complex and difficult to manage IT projects. Pragmatic CISO's wisely avoid being the champion for identity management. Unfortunately this often means that they miss an opportunity to get their privileged accounts under control.

APT PRIVILEGED ACCOUNT EXPLOITATION

Advanced Attacks Continuously Target Privileged Accounts [Continued]

Additionally, none of the CISO's we spoke with actually had operational responsibility for managing privileged accounts, which typically reside in Active Directory, owned, operated and managed by the IT delivery organization.

The CISO's and SOC Directors we interviewed all agreed that the compromise of privileged accounts severely complicates the detection, containment, and eradication phases of incident response. Organizations are usually very slow in detecting APT attacks where privileged accounts have been compromised, with some respondents reporting that breaches can remain undetected for months up to even years.

- **Privileged account use appears as normal traffic flow, and is not detected by traditional detection methods.** Additionally, detecting legitimate processes being used for illegitimate purposes are the equivalent of "finding a needle in a stack of needles."
- When a domain controller is compromised, an attacker can then create multiple accounts for future use.|
- Attacks that leverage a privileged account can delete logs, making analysis harder at best and requiring forensic analysis at worst. Time is money; forensics takes time and analysts are expensive.
- Attacks that leverage a privileged account can continue to bring in and install new malware and tools to evade detection and open more backdoors.

ATTACKS THAT LEVERAGE A PRIVILEGED ACCOUNT ARE MORE DIFFICULT TO DETECT, SHUT DOWN AND REMEDIATE.

- Capturing authentication logs from workstations/servers for analysis, especially in large enterprises, can require a tremendous amount of storage and processing power. Not logging or auditing privileged account use may make it very difficult to ever track the attack back to specific privileged account misuse. **SOC teams lack real-time intelligence concerning privileged account use provided by auditing and SIEM alerts.**
- Most organizations focus their monitoring efforts on what is going in/out of network, not what's going on within. Almost everyone can detect firewall activity, but how many can tell every host a domain admin has logged into?
- Attacks that leverage a privileged account mean that a security analyst can't necessarily look for a specific piece of malware or network traffic; every host that the compromised account had logged into is now suspect.

Advanced Attacks Continuously Target Privileged Accounts [Continued]

The costs of data breaches to a company can be exorbitant. A recent study by the Ponemon Institute shows that the average cost of a data breach event is $2.4 million over a two-year period, and that malicious or criminal attacks, the most expensive cause of data breaches, are often the culprit. In 2011, 37 percent of data breach cases involved malicious attack[1].

Protecting an organization's confidential data from exfiltration is ordinarily the most important goal of a security organization. Proprietary information, trade secrets, patent filings, classified documents, personally identifiable information, and new product designs are the crown jewels of an organization. It is often impossible to put a price tag on the information when it is compromised.

When data is stolen, companies may suffer loss of productivity, public embarrassment, loss of customer trust, legal action, unfavorable media coverage, customer turnover, and a decline in company's share price. Depending on the industry and type of data lost, laws requiring notifications to affected parties can also be a factor, as well as fines and penalties being levied.

The costs to eradicate attackers from a compromised network can also be extremely high. Most of the CISO's and SOC Managers we spoke to had experience responding to large-scale APT compromises of major networks. Many had been part of lengthy response efforts to remove well-entrenched adversaries from their network. In each of these major incident responses, the attackers had compromised core privileged accounts throughout the enterprise.

In these cases, all surveyed affirmed that taking corrective action to "clean" an entire organization that has an unknown amount of attacker controlled accounts is ***very painful to the users and very expensive.*** Some steps required during the remediation of these major incidents included:

- 100% Password Reset for all accounts
- Manually trying to remove admin rights from all accounts
- Manually attempting to give admin rights back when necessary
- Broken service accounts
- User downtime
- Decreased user confidence in the security team
- Perception of security team as being out of touch with business
- Thousands of man-hours of work from the Security Department, IT, and the Help Desk

ATTACKS THAT LEVERAGE A PRIVILEGED ACCOUNT ARE MORE DAMAGING AND EXPENSIVE.

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

HIGH PROFILE ATTACKS IN 2012 LEVERAGED PRIVILEGED ACCOUNTS

2012 brought many reports of data breach to the public's attention through increased media coverage and mandatory reporting regulations. Some events were caused by physical losses, such as lost backup tapes and laptops, while other, more high-profile incidents focused on customized malware such as Flame or Duqu, which were highly sophisticated campaigns designed to target specific government and industrial systems.

IN THE CUSTOMARY ATTACK TECHNIQUES OF THE APT, THE TARGETING AND THEFT OF LEGITIMATE CREDENTIALS IS ALWAYS PRESENT.

While those types of breaches are interesting to note, the most prevalent threatsactually facing large organizations today are still organized groups or nation states attempting to steal intellectual property and sensitive information, employing established and predictable attack methods.

CyberSheath researched 10 well-reported attacks over the last 12 months,all containing elements of privileged account exploitation, and examined how greater privileged account controlcould have played an important role in thwarting the APT. In each case, it was evident that attackers targeted the credentials of privileged users, and lacked essential credential protection, accountability, and intelligence processes to detect and stop the attacks before data was lost.

#1 SOUTH CAROLINA DEPARTMENT OF REVENUE

The personal data of nearly 4 million individuals and 700,000 businesses was exposed in the South Carolina Department of Revenue (DoR) data breach that began in August 2012. The public incident response report, authored by Mandiant who was contracted by the Department of Revenue to perform incident response confirmed that "all Windows user accounts" credentials were stolen and exploited by the attackers. Attackers moved laterally throughout 44 systems, and password hash dumping was used throughout the process.

Privileged Account Protection: If the South Carolina Department of Revenue had implemented a privileged accounts protection solution, the initial compromise and subsequent lateral movement and privilege escalation could possibly have been averted.

#2 RED OCTOBER

In October, 2012, Kaspersky Labs discovered a high-level cyber-espionage campaign that had successfully infiltrated computer networks at diplomatic, governmental and scientific research organizations for over five years, gathering data and intelligence from mobile devices, computer systems and network equipment.

The malware is known as Red October or Rocra, and is as complex as Flame and "much more sophisticated" than Night Dragon or Aurora. It is delivered by a Trojan and operates through extensive command and control. The amount of stolen data from victim organizations in 39 countries is estimated to be over five terabytes of information.

High Profile Attacks in 2012 Leveraged Privileged Accounts [Continued]

The infection mechanism of the malware associated with Red October begins with a spear phishing email delivering malicious software embedded in an excel file. After a user clicks and installs the main malware package, up to 30 additional modules are downloaded designed for reconnaissance, email stealing, persistence, spreading, and exfiltration.

One of those modules, known as MSHash, is a standalone executable used to dump cached domain password hashes, and locally stored sensitive information, such as LSA secrets. It uses direct disk access to bypass system registry ACLs.

Privileged Account Protection: Preventing an adversary's ability to move laterally throughout the network by protecting privileged accounts can drastically lower the damage done by targeted attacks. By decreasing the value of compromised passwords through the use of a comprehensive privileged account security solution, or eliminating cached login hashes, companies can drastically impact the APT attack cycle.

#3 UTAH DEPARTMENT OF HEALTH

On March 10, 2012, attackers illegally gained access to a Utah Department of Technology Services (DTS) computer server that stored Medicaid and Children's Health Insurance Program claims data.

The attackers began removing personal information from the server on March 30th, but it wasn't until three days later that DTS detected the breach and shut down the server. By that time, the Social Security numbers of 280,000 people, as well as less-sensitive personal information of another 500,000 people, had been stolen.

DTS stated that the adversaries had "exploited a default password on the user authentication layer of the system." The attackers were able to bypass multiple network, perimeter and application level security controls. DTS also reported that they had "sophisticated processes in place to totally secure all of the data on state computer servers, but this particular server hadn't been configured the same way."

Privileged Account Protection: Identifying critical systems and ensuring that they have access controls securely configured is an essential, if not foundational step in protecting company data. However, when companies have thousands of systems and the processes of asset management, system hardening, vulnerability management, and the implementation of access controls are done manually, serious oversight errors can occur. By automating access controls on all systems, databases, network devices, virtual environments, security appliances, business and web-based applications, through a systematic process with the right technology, an organization can ensure that all systems have proper access controls in place, that they are configured correctly, and that they are being reviewed regularly.

#4 THE UNIVERSITY OF GEORGIA

Full names, social security numbers and other sensitive information were exposed when two employees who had access to sensitive information had their account passwords reset by an intruder. The two accounts were then used by the hackers to gain access to the personal information.

High Profile Attacks in 2012 Leveraged Privileged Accounts [Continued]

Privileged Account Accountability: Password reset requests for privileged users is an auditable event that could indicate suspicious activity. Managing all privileged accounts with a comprehensive privileged account security solution eliminates the cloak of anonymity inherent in privileged and shared accounts, providing direct accountability to a specific user, even for shared accounts, and could have enabled the University to confirm in real time the validity of the password reset requests and possibly thwarted the attack.

#5 NASA JET PROPULSION LIBRARY (JPL)

In November 2011, JPL IT Security reported suspicious network activity involving Chinese-based IP addresses. Their review disclosed that the intruders had **compromised the accounts of the most privileged JPL users,** giving the intruders access to most of JPL's networks.

Privileged Account Intelligence: Deployment of a comprehensive privileged account security solution integrated with an existing Security Information and Event Management platform that provides real time privilege monitoring and alerting via a dashboard could have alerted NASA to this attack in advance. Additionally, by employing a session monitoring and recording solution, incident response teams could drill down through detailed forensics data to rapidly triage alerts and precisely identify the specific users and the activities they performed during a privileged session.

#6 TOYOTA

Shortly after his dismissal in August 2012 from Toyota's US manufacturing site, an IT contractor is said to have logged into the toyotasupplier.com website without authorization and spent hours downloading proprietary plans for parts, designs and pricing information. Although Toyota did not say what data it believes the contractor may have stolen, their attorneys have said that "If this information were disseminated to competitors or otherwise made public, it would be highly damaging to Toyota and its suppliers, causing immediate and irreparable damage." Toyota also alleges that the former programmer sabotaged at least 13 different web applications and removed security certificates from servers.

Privileged account Intelligence: A privileged accounts protection solution enables organizations to respond in real-time to threatening privileged activity, including the ability to block all privileged activity on resources that are currently threatened and terminate an active, malicious privileged session to disrupt the attack. With up to the minute situational awareness of privileged account activities, security teams may have been able to detect and avert the Toyota malicious behavior.

#7 SWISS NDB INTELLIGENCE SERVICE

In December of 2012, classified information shared by foreign governments may have been compromised in a large data theft by a senior IT technician for the NDB, Switzerland's intelligence service. Investigators believe the technician downloaded terabytesof classified material from the Swiss intelligence service's servers onto portable hard drives. The perpetrator was described as a "very talented" technician and senior enough to have "administrator rights," giving him unrestricted access to most or all of the NDB's networks.

High Profile Attacks in 2012 Leveraged Privileged Accounts [Continued]

Privileged Account Intelligence: The anomalous actions of administrators over long periods of time can be logged and monitored with a privileged accounts protection solution. In the case of the Swiss NDB, security teams may have been able to discover the actions of the rogue IT technician by analyzing login actions and subsequent behavior on target systems long before serious data theft may have occurred.

#8 SUBWAY

In September, 2012, two Romanian men plead guilty to participating in a campaign to illegally access the computers of hundreds of Subway restaurants in the U.S. and steal payment card data, resulting in more than 146,000 compromised payment cards and more than $10 million in losses. During the attacks, the men remotely scanned the internet to identify vulnerable point-of-sale systems, then logged onto the targeted POS systems over the internet by either guessing the passwords or password cracking. A lawsuit related to the case alleges that the PCAnywhere remote access program resident on the computers at most affected locations all had the same login credentials.

Privileged Account Protection: Widespread reuse of default or guessable passwords enables attackers to compromise numerous systems simultaneously and with little effort. Controlling internet accessible point of sales with unique and secure credentials can be accomplished with a privileged accounts protection solution.

#9 SAUDI ARAMCO

In August of 2012, a person with privileged access to the Saudi state-owned oil company Aramco's computers inserted the Shamoon virus on the company's network, stealing data and then erasing an estimated three quarters of all computers. After analyzing the code from the Aramco attack, security experts say that the event involved a company insider, or insiders, with privileged access to Aramco's network. Local administrator privileges were required to execute the payload.

Privileged Account Protection: In the Aramco case, damage may have been averted by closing network shares, disabling remote access, and most importantly, enforcing least privilege for all users.

#10 GLOBAL PAYMENTS

In April 2012, the credit and debit card processor Global Payments disclosed a breach of its systems that involved at least 1.5 million accounts. While the company has yet to release full details on the breach, one security analyst asserted that the "attackers took over an administrative account that was not protected sufficiently," breaking into the company's system "by answering the application's knowledge based authentication questions correctly."

High Profile Attacks in 2012 Leveraged Privileged Accounts [Continued]

Privileged Access Intelligence: Proper logging, monitoring, and alerting for changes to privileged account actions can warn security teams of the possibilities of malicious behavior. When this information is correlated in a SIEM with other administrative actions, the intelligence gathered can trigger notifications to the SOC analysts, initiating session monitoring, aiding in incident investigations, response, and forensics.

It's not just an exercise in hindsight analysis to point out that had these organizations employed a privileged account credential protection, accountability and intelligence strategy and solution, the breaches they experienced might never have occurred; rather it's a call to action for CISO's. It is clear that the absence of fundamental access control measures was a significant factor in many of the high profile attacks of 2012. In fact, according to Mandiant's M-Trends 2012 Report: "In 100% of the cases Mandiant responded to this year the attacker used valid credentials." Similarly, the 2012 Verizon Data Breach report indicates that exploitation of default or guessable credentials occurred in 55% of all known breaches. Use of stolen login credentials was present 40% of the time, and brute force and dictionary attacks represented 29%.

OTHER RESEARCH CONFIRMS: CONTROLLING PRIVILEGED ACCOUNTS PREVENTS ATTACKS

We at CyberSheath, and the security professionals we surveyed for this research, believe that taking control over privileged accounts can effectivelyprevent some cyber-attacks and significantly increase the time and financial investment requirements of the attackers. But don't just take our word for it. Almost every whitepaper or report about cyber-attack methodology lists controlling privileged accountsas a basic, foundational mitigating step in securing an enterprise from attack. Additionally, the fundamental concepts of access control and identity management specifically detailed in widely accepted frameworks adequately describe the risks and mitigating controls associated with privileged accounts. Examples include:

1. A recurring recommendation in the 2012 Verizon Data Breach Report to mitigate several attack methods is to "restrict user administrative rights."

2. The Australian Department of Defence Signals Directorate (DSD) won the SANS Institute's 2011 U.S. National Cyber security Innovation Award for its ground-breaking research in finding and implementing four key security controls that stop the spread of infection from targeted intrusions. The DSD asserted that at least 85% of their targeted cyber intrusions could be prevented by following the first four key mitigation actions listed in their 35 Strategies to Mitigate Targeted Cyber Intrusions. Of those four methods, two are directly related to controlling privileged use:

- Minimize the number of users with administrative privileges
- Use application whitelisting to help prevent malicious software and other unapproved programs from running

3. Microsoft's #1 and #2 mitigation recommendations to prevent Pass the Hash:

- Mitigation #1- Restrict and protect high privileged domain accounts - Restricts the ability of administrators to inadvertently expose privileged credentials to higher risk computers.
- Mitigation #2- Restrict and protect local accounts with administrative privileges - Restricts the ability of attackers to use local administrator accounts or their equivalents for lateral movement PtH attacks.

Additionally, the report confirmed that "Privileged Password Management tools and password vaults are effective mitigations against" Pass-the-Hash techniques[2].

[2]Microsoft: Mitigating Pass-the-Hash (PtH) and Other Credential Theft Techniques

Other Research Confirms: Controlling Privileged Accounts Prevents Attacks [Continued]

4. Controlling privileged account accessaligns directly with NIST 800-53, ISO 27001/27002, NERC CIP, PCI DSS, the SANS Top 20 Critical Controls, and other best practice standards to prevent APT privileged account compromise. Recurring recommendations of these frameworks include:

- Enforce Least Privilege
- Use multifactor authentication for access to privileged accounts
- Secure, manage, automatically change and log all activities associated with all types of Administrative/Privileged Passwords
- Increase password complexity
- Use a unique password for each local administrator account
- Reduce cached credential storage
- Remove local administrator rights from the majority of users
- Reduce the number of privileged domain-wide service accounts
- Log and monitor privileged account use
- Use two-factor authentication for critical systems
- Change default passwords on all network devices
- Change passwords on suspicion of misuse
- Employ technical means of enforcing password policies

CONCLUSION

- The importance of credential theft and exploitation in a successful APT attack can't be overstated. **When it comes to privileged accounts, CISO's have three primary responsibilities: implement protection, maintain accountability and utilize intelligence to maintain visibility.** Doing these three things may deny the APT an easy critical path to the compromise of a network. Given this well established pattern of attack and recycled tactics of the APT, Chief Information Security Officers have an opportunity to regain some previously lost ground in the battle to stop data exfiltration.

- With dozens of security tools on the market, CISO's are faced with the dilemma of where to apply their limited resources to mitigate these attacks in an effective manner. But a solution that provides protection, accountability and intelligence of privileged accounts is **one of the first security tools a CISO would want in their organization to stop targeted attacks.** Taking control of the keys to the kingdom, before augmenting with other protective measures, should be the earliest investment for a mature security organization. Organizations need to implement a privileged account protection, accountability and intelligence solution as a primary component of their security strategy.

- APT account compromise is not a foregone conclusion; properly controlling privileged credentials stops account compromise, privilege escalation, and lateral movement. **CISO's don't have to accept that credential theft and misuse is an inevitability** that they must endure and respond to. Measureable security gains can be had by concentrating on the hard work of privileged account protection.

- Privileged account management solutions can be had without the cost and complexity of enterprise identity management projects. It's not often that CISO's have an opportunity to leverage something they have complete control over, privileged identities, in the fight against the APT. Seize the day.

ABOUT CYBERSHEATH

Co-founded by a Chief Information Security Officer for a Fortune 500 company & Chief Executive Officer for an Inc. 500 company, CyberSheath applies business discipline to cyber security, enabling our customers to measure risk, meet compliance goals, prioritize investments, and improve overall security posture, all while saving money. We've built a global network of best-in-class partners that we leverage as a force multiplier to deliver pragmatic, end to end solutions for our customers. Having been in the trenches as security practitioners and business executives, CyberSheath goes beyond the WHAT (best practices) and delivers the HOW.

CONTACT

CyberSheath Services International, LLC
942 Seneca Road
Great Falls, VA 22066
www.cybersheath.com
1-855-384-8070

