Targeted Attacks and the Privileged Pivot

Barak Feldman
National Director, CyberArk

Robert Jett
PNW Account Manager, CyberArk
South Korea Blames North Korea for Cyber Attack

Last month’s mysterious cyber attack that caused several banks and television stations in South Korea to go offline was executed by North Korea’s intelligence agency, according to official investigators based in Seoul.

The findings were revealed in the Korea Herald today as South Korea’s Ministry of Science, ICT and Future Planning connected the attacks to North Korea’s Reconnaissance General Bureau.

On March 20, the computer systems of local banks and Korean television stations KBS, YTN, and MBC went offline.

Cyber Attacks: A Daily Event, Overwhelming Coverage

ChineSE Hackers Target New York Times in Four-Month Cyberattack

Fast Feed

Swiss Spy Agency Warns CIA, MI6 Over 'Massive' Secret Data Theft

Summary: Switzerland’s national security agency warns that a huge amount of secret, counter-terrorist data may have been leaked by no other than a disgruntled ‘administrator-level’ employee.
Regardless of where they started, they all became insiders!
Privileged Accounts Create a Huge Attack Surface

- Privileged accounts exist in every connected device, database, application, industrial controller and more!

- Typically a ~3X ratio of privileged accounts to employees
The One Thing Attackers Need to Succeed!

Privileged Accounts – “Keys to the IT Kingdom”
Privileged Credentials are Everywhere

Privileged Accounts

Routers, Firewalls, Hypervisors, Databases, Applications

INDUSTRIAL CONTROL SYSTEMS
Power Plants, Factory Floors

Routers, Firewalls, Servers, Databases, Applications

ON-PREMISE DATA CENTER

WiFi Routers, Smart TVs

Cloud

Laptops, Tablets, Smartphones

ENDPOINTS
Privileged Credentials are Everywhere

Organizations typically have 3-4x more Privileged Accounts than employees
Hijacked Credentials Put the Attacker in Control

Compromised Privileged Accounts

Enable attackers to:

• Bypass security controls & monitoring
• Access all of the data on the device
• Disrupt normal operation of the device
• Cause physical damage
Proactive Protection, Detection & Response

Proactive protection
- Only authorized users
- Individual accountability
- Limit scope of privilege

Targeted detection
- Continuous monitoring
- Malicious behavior
- High risk behavior
- Alerting

Real-time response
- Session termination
- Full forensics record of activity
Privileged Account Security – Now a Critical Security Layer
Solving The Privileged Account Security Problem

Threats
- Advanced Threat
- Insider Threats
- Securing the Hybrid Cloud
- Securing Application Credentials
- Securing Shared Admin Accounts
- Sharing Sensitive Information

Audit & Compliance
- Control & Accountability for Privileged Users
- Monitor & Record Privileged Activity
- Compliance Reporting
- Remote User Access Control
- Auditing Secure File Transfer

Industrial Controls/SCADA
- Securing and Monitoring Shared Admin Accounts for ICS Systems
- Controlling and Monitoring Remote Vendors
- Smart Grid Security
The Privilege Escalation Cycle

1. Breach

2. RETRIEVAL
   - Gain access to credentials location
   - Retrieve credentials

3. USAGE
   - Use credentials

Goal
Primary Recommendations

Restrict Lateral Movement

• Assign a UNIQUE password on every endpoint for built-ins
• Establish Credential Boundaries on Domain; One-Time Passwords

Isolate High Value Assets

• Ensure users can not access sensitive assets directly from their endpoint
• Do not allow users or their machines to know a password (keyloggers, malware, etc.)

Monitor Behavior

• Look for changes in behavior for common privileged accounts and sensitive assets, especially indicators of credential theft
• Enable reactive countermeasures
Credential Boundaries

*See MSFT Whitepaper: Mitigating Pass the Hash Attacks and Other Credential Theft Version 2

**Tier 0** – Forest admins: Direct or indirect administrative control of the Active Directory forest, domains, or domain controllers

**Tier 1** – Server admins: Direct or indirect administrative control over a single or multiple servers

**Tier 2** – Workstation Admins: Direct or indirect administrative control over a single or multiple devices
Strategic Best Practices Summary

Session Recording & Desktop Isolation

• Isolate High value assets and create a new layer of security using proxy server.
• Leverage Universal connectors and native access to enforce PIV cards and role based accounts.
• Record all privileged activity without the use of an agent

Password Management

• Change passwords to built-in accounts to a unique value per end point
• Frequently change passwords to minimize the risk of credential (hash) theft

Privileged Analytics and Anomalies

• Watch for anomalous behavior of privileged accounts and bypass of controls to limit and stop events in progress.

Least Privilege Access and App Controls

• Reduce a large number of privileged users from desktops and servers by using a least privileged escalation model in Windows desktops/Servers and Unix/Linux.
What to do now – Getting Started

Identify
• Run free assessment tools to find out where privileged accounts exist and how they are being used/misused

Change
• Identify top 3-5 data center technologies and high Value assets and Isolate and change the built-in backdoor ids on each to a unique random password

Isolate
• Identify what systems/information an ‘attacker’ would target and assign priority
• Prevent end users from accessing these devices directly moving forward and do not disclose passwords
CyberArk Maturity Model – Levels of Control

Level 1: Password Management
Level 2: Session Isolation
Level 3: Least Privilege
Level 4: Behavioral Analytics

More Mature

Role Based Access
PIV/2FA
Primary Recommendations

Reduce Attack Surface
- Establish Role based access and Least Privilege Models
- Randomize Built-in Backdoor Admin Passwords

Credential Theft
- Isolate Passwords of Critical Assets

Lateral Movement
- Monitor Privileged Behavior

Enterprise Password Vault (EPV) and Viewfinity (OPM)
- Privileged Session Manager (PSM)
- Privileged Threat Analytics (PTA)
Extra Slides
How to Measure Success – Wide & Deep

Breadth of Coverage

<table>
<thead>
<tr>
<th>Tier 0 Win</th>
<th>Tier 1 Unix</th>
<th>Workstations</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Change</td>
<td>Pwd Change</td>
<td>Pwd Change</td>
<td>Pwd Change</td>
</tr>
<tr>
<td>Session Iso</td>
<td>Session Iso</td>
<td>Session Iso</td>
<td>Session Iso</td>
</tr>
<tr>
<td>Least Priv</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emb Creds</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Depth of Control
As defenses evolve, attackers adapt and innovate. In 2014 we observed new and emerging techniques at each stage of the attack lifecycle. These are a few highlights.

**Hiding Webshell**
Attackers continued to use novel techniques to deploy and hide web-based malware. Mandiant saw several stealthy techniques, including the following:
- Shells planted on servers that used SSL encryption to evade network monitoring
- Single-line "eval" shells embedded in legitimate web pages
- Server configuration files that were modified to load malicious DLLs

**Leveraging WMI and PowerShell**
Attacks are increasing WMI and PowerShell to create powerful built-in command tools to maintain presence, gather data, and more.

**Hijacking the VPN**
Mandiant witnessed more cases in which attackers successfully gained access to victims' VPNs than in any prior year.

**Malicious Security Packages**
Attacks took advantage of Windows security package extensibility to load backdoors and password loggers.

**Maintain Presence**

**Move Laterally**

---

**Initial Compromise**

**Establish Foothold**

**Escalate Privileges**

**Internal Recon**

**Com Mist**

---

** Plaintext Passwords**
Attackers used recompiled variants of the Mimikatz utility to steal plaintext passwords from memory while evading anti-virus detection.

**Kerberos Attacks**
After gaining domain administrator privileges, attackers used the Kerberos golden ticket attack to authenticate as any privileged account—even after domain password resets.
The Anunak/Carbanak Attacks
The Anunak/Carbanak Attacks

Access a single server

1. ACCESS
   - Phishing regular employees

2. RETRIEVAL
   - Tech support
   - A limited administrative access (e.g. tech support)

3. USAGE
   - Access a single server
The Anunak/Carbanak Attacks

Hijack domain admin credentials

Access the AD and compromise all domain accounts

Access a server

Domain admin

52 ATMs
The Anunak/Carbanak Attacks

Hijack credentials of banking system admins

Access email, workflow and banking servers

Install software to monitor activity (photo, video, etc.)

Enable remote access to servers

Transactions:
- Bank accounts
- E-currency
- Mobile prepaids
Who are the attackers?

Does attribution help mitigation?
CyberArk Contacts:

Rob Jett
Robert.jett@cyberark.com
(510) 717-9910

Barak Feldman
Barak.Feldman@cyberark.com