**New Report: Advanced Cyber Attacks Reliant on Privileged Credential Exploitation**

June 11, 2014 4:03 PM ET

*CyberSheath Analysis of 10 Benchmark Cyber-Attacks from 2013 Uncovers Stolen Privileged Credentials form the Basis of Each Attack*

**Newton, Mass. â€“ June 11, 2014 â€“**A new cyber-security report reveals that while new and sophisticated malware variants were continually developed to exploit systems in 2013, criminals, hacktivists and advanced attacks continue to do the most damage by exploiting privileged accounts. Compiled by CyberSheathâ€™s advanced security investigations team and commissioned by CyberArk, The Role of Privileged Accounts in High Profile Breaches, also includes a detailed case study covering a Fortune 500 companyâ€™s struggle with, and eventual remedy for, a dramatic reduction in recorded breaches.

Analysis of 10 of 2013â€™s most notable cyber attacks, including the NSA leak by insider Edward Snowden, point of sale (POS) breaches like the many attacks on retailers, the attack on the *New York Times* â€“ CyberSheath found that privileged accounts were on each attackerâ€™s critical path to success 100 percent of the time, regardless of the perimeter attack vector. The research uncovered that increased visibility and actionable intelligence on privileged accounts within an organizationâ€™s IT environment greatly increased the ability for those organizations to successfully detect and disrupt an attack.

Highlights from The Role of Privileged Accounts in High Profile Breaches report include:

- **A Case Study: The True Cost of a â€œDo-Nothingâ€Approach**
  The exploitation of privileged accounts detailed in this case study directly led to more than 200 compromised machines, more than 10,000 man hours of overtime, and a total breach cost exceeding $3 million dollars in a six-month span. This real-world example explores one organizationâ€™s privilege account problem and highlights lessons-learned throughout the remediation process.
- **High Profile Attacks in 2013 Leveraged Privileged Accounts**
  CyberSheath researched and analyzed 10 benchmark attacks throughout 2013, including the NSA leak, POS breaches, the attack on the *New York Times,* MacRumors, U.S. banking institutions, the Department Of Energy (DOE), South Korean banking and broadcast networks, the *Washington Post* and attacks revealed by Mandiantâ€™s APT1 report. Each of these attacks happened as a result of privileged account exploitation. The research showed that protecting, managing, and monitoring these accounts, organizations could have stopped these attacks before significant damage was done.
- **Strategic Takeaways For CISOs**
  Looking closely at the advanced attack patterns leveraged in these 10 benchmark breaches reveals that the theft, misuse, and exploitation of privileged accounts is a critical step in attack methodology. Key takeaways for CISOs from the CyberSheath report include:
    - The attacks that matter to business exploit privileged accounts 100 percent of the time.
    - Big company or small, organizations have more privileged accounts than they know about and the risk of exposure they represent makes them urgent priorities.
    - Protecting privileged accounts gives CISOs an opportunity to quantify risk reduction and deliver results that can be measured.
    - Privileged accounts represent a clear case for providing a return on investment and reduce risk.
    - Protecting privileged accounts is an opportunity to become a challenging target and take back ground in the fight against advanced threats.
    - Automated privileged account security solutions reduce human error, overhead and operational costs.

For a full copy of the report, please visit:
http://cyberark.com/contact/role-privileged-accounts-high-profile-breaches

**Supporting Quotes**

â€œAdvanced attacks follow a common, multi-stage approach to breaching defences, gathering and exfiltration critical data,â€said John Worrall, CMO, CyberArk. â€œItâ€™s clear that privileged access is required to gain access to target systems and move laterally from system to system. The faster the industry takes notice of the privileged connection to these attacks, the more quickly better defences can be mounted.â€

â€œCompanies of all sizes today face an unprecedented number of cyber-attacks from organized, patient and well-funded groups,â€said Eric Noonan, CEO, CyberSheath. â€œWeâ€™re starting to see CISOâ€™s shift from band aid point-solution purchases to integrated technologies built on intelligence-gathering features to combat advanced threats.â€

**About CyberArk**

CyberArk is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the worldâ€™s leading companies â€“ including 30 of the Fortune 100 and 17 of the worldâ€™s top 20 banks â€“ to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, MA. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com, read the company blog, http://www.cyberark.com/blog/, follow on Twitter @CyberArk or Facebook at https://www.facebook.com/CyberArk.

# # #

**Media inquiries:**

| | |
|---|---|
| Brian Merrill<br>fama PR (for CyberArk)<br>Phone: +1-617-986-5005<br>Email: cyberark@famapr.com | Eric Seymour<br>CyberArk<br>Phone: +1-617-796-3240<br>Email: eric.seymour@cyberark.com |

Wednesday, June 11, 2014 - 14:00