CyberArk Releases Report Identifying New Patterns in Advanced Targeted Attacks

November 19, 2014 9:00 AM ET

Analysis of Firsthand Experiences of the World's Most Renowned Cybersecurity Forensics Teams Pinpoints Exploitation of Privileged Accounts as a "Signature" in Targeted Attacks

NEWTON, Mass.--(BUSINESS WIRE)--Nov. 19, 2014-- CyberArk (NASDAQ: CYBR), the company that protects organizations from cyber attacks that have made their way inside the network perimeter, today released a new report identifying the compromise and misuse of privileged accounts as a key signature common among advanced targeted cyber attacks.

Privileged Account Exploits Shift the Front Lines of Security, provides an expert's vantage point into emerging patterns in targeted attacks by analyzing the experiences of the world's most renowned threat investigators in remediating the most devastating breaches. Participants include:

- Cisco Talos Security Intelligence and Research Group
- Deloitte Financial Advisory Service LLP – Computer and Cyber Forensics Team
- Deloitte & Touche LLP – Cyber Risk Services
- Mandiant, a FireEye company
- RSA, The Security Division of EMC
- The Verizon RISK Team

"This coalition represents some of the smartest, most experienced and knowledgeable threat investigators in the world. By understanding the commonalities they're discovering across their investigations, we're gaining significant insights into attack patterns for targeted attacks," said Udi Mokady, CEO, CyberArk. "What the research discovered was the exploitation of privileged accounts occurs in almost every targeted attack, and is the primary reason why attacks are so hard to discover and stop. These accounts empower attackers to access secure networks and databases, destroy breach evidence, avoid detection and establish backdoors that make it nearly impossible to dislodge them from networks. Securing privileged accounts represents the new first line of defense in the on-going cyber-battle companies are fighting."

Privileged accounts which consist of IT administrative credentials, default and hardcoded passwords, application backdoors and more, provide attackers with an 'all access pass', enabling them to go where they want, traversing a network without hindrances. These accounts are also critical for attackers to hide their tracks and to exfiltrate data. Once attackers gain privileged access to critical applications and systems, they become exponentially more difficult to stop, heightening the risk of data loss and business damage.

Key findings of the report include:

- **Every Industry, Every Company is now a Target**: Cyber-attackers have broadened their targets, pursuing companies of all sizes, in all industries. This is often a means to an end: attackers are frequently after their supply chain partners. Threat investigators have traced attacks to non-traditional targets such trucking companies and all types of professional services firms, from management consultants and auditors to litigation attorneys, frequently as a key step in an attack on a business partner.
- **Perimeter Resistance is Futile:** Attackers will get inside of perimeter security and the most likely infection point is employees. Phishing attacks are the most common vector and are growing in sophistication, making employee log-ins far easier points of infiltration than network or software exploits.
- **Attackers Stay Hidden for Months or Years**: Most attacks have been ongoing for 200 days or more before initial detection. Monetary attacks have a much shorter time to detection – typically less than 30 days. Attackers can cover their tracks using privileged accounts to delete log data and other evidence.
- **Attackers Covet Privileged Access**: Privileged accounts are exploited in almost every targeted cyber attack. The

threat investigators claim that between 80-100 percent of all serious security incidents they've investigated featured the "signature" of compromised and exploited privileged accounts in the attack process.

- **Privileged Accounts Threat Vastly Underestimated**: The risk and security vulnerabilities presented by privileged accounts are much greater than most companies realize. Companies underestimate how many privileged accounts they have and on what systems they reside. CyberArk's research demonstrates that organizations today have at least three-to-four times as many privileged accounts as employees.
- **Attackers' Exploits of Privileged Accounts Increasingly Sophisticated**: Security investigators report a range of privileged account exploits – including repeated exploits in service accounts, to embedded devices in the Internet of Things to establishing multiple identities in Microsoft Active Directory to ensure redundant access points and backdoors.

To download a free copy of the report and accompanying infographic, please visit: http://www.cyberark.com/threat-report and http://www.cyberark.com/blog/cyber-threat-investigators-identify-signature-dangerous-cyber-attacks

About CyberArk

CyberArk (NASDAQ: CYBR) 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 world's leading companies – including more than 35 percent of the Fortune 100 and 17 of the world's top 20 banks – 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.

Forward-Looking Statements

This release may contain forward-looking statements, which express the current beliefs and expectations of our management. Such statements involve a number of known and unknown risks and uncertainties that could cause our future results, performance or achievements to differ significantly from the results, performance or achievements expressed or implied by such forward-looking statements. Important factors that could cause or contribute to such differences include risks relating to: changes in the new and rapidly evolving cyber threat landscape; our failure to effectively manage our growth; fluctuations in our quarterly results of operations; real or perceived shortcomings, defects or vulnerabilities in our solution or the failure of our solution to meet customers' needs; our inability to acquire new customers or sell additional products and services to existing customers; competition from IT security vendors and other factors discussed under the heading "Risk Factors" in the final prospectus for our initial public offering filed with the Securities and Exchange Commission on September 24, 2014. Forward-looking statements in this release are made pursuant to the safe harbor provisions contained in the Private Securities Litigation Reform Act of 1995. These forward-looking statements are made only as of the date hereof, and we undertake no obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise.

Source: CyberArk

Media Relations Contacts:
fama PR
Brian Merrill, +1 617-986-5005
cyberark@famapr.com

or
CyberArk
Eric Seymour, +1 617-796-3240
press@cyberark.com
or
Investor Relations Contact:
ICR
Staci Mortenson, +1 617-558-2132
IR@cyberark.com