CyberArk Labs: New Research Examines Real-World Networks’ Exposure to Credential Theft Attacks and Complete Network Compromise

November 10, 2015 8:31 AM ET

Research Provides Insights into Cyber Attacks that Abuse Hijacked Privileged Credentials to Compromise Enterprise Security

NEWTON, Mass. & PETACH TIKVAH, Israel--(BUSINESS WIRE)--Nov. 10, 2015-- CyberArk (NASDAQ: CYBR), the company that protects organizations from cyber attacks that have made their way inside the network perimeter, today released new research from CyberArk Labs. The research found that, on average, 40 percent of network machines can provide cyber attackers with credentials enabling them to start an attack which could compromise an organization’s entire network.

The report, “Analyzing Real-World Exposure to Windows Credential Theft Attacks,” explores data from more than 50 networks to identify the prevalence and risk of what are referred to as “highly threatening machines.” These machines are Windows-based workstations or servers that hold sufficiently privileged credentials that enable the attacker to compromise other machines and privileged accounts, culminating in a broad network compromise. In fact, 88 percent of the networks scanned were found to be significantly susceptible to compromise through privileged account credential theft or abuse.

“In a given network, there are typically a number of highly threatening machines that can give an attacker the credentials needed to completely compromise the majority of Windows hosts on the network,” said Andrey Dulkin, director of cyber innovation at CyberArk Labs. “We’ve seen similar credential theft methods as the basis for major attacks across a number of organizations. Identifying these machines and securing the associated privileged credentials against theft and exploitation is a critical step in securing against advanced cyber attacks.”

In this research, CyberArk Labs details:

- Various credential abuse methods – including Pass-the-Hash, Overpass-the-Hash and other Kerberos attacks;
- The types of privileged accounts that pose the most danger to organizations – such as privileged user accounts and privileged service accounts;
- The effectiveness of specific mitigation strategies that can significantly lower the risk across different network types.

Research from CyberArk Labs focuses on targeted attacks against organizational networks – the methods, tools and techniques employed by cyber attackers, as well as methods and techniques to detect and mitigate such attacks.

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 world’s leading companies – including 40 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, Mass. 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.

View source version on businesswire.com: http://www.businesswire.com/news/home/20151110005354/en/

Source: CyberArk

Media Relations:
fama PR
Brian Merrill, +1-617-986-5005
cyberark@famapr.com
or
CyberArk
Liz Campbell, +1-617-558-2191
press@cyberark.com
or
Investor Relations:
CyberArk
Erica Smith, +1-617-630-6426
ir@cyberark.com