Palo Alto Networks Delivers Industry-First Capabilities to Prevent Credential Theft and Abuse

February 7, 2017

New Capabilities Delivered in Palo Alto Networks Next-Generation Security Platform Operating System, PAN-OS 8.0

SANTA CLARA, Calif., Feb. 7, 2017 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, today announced advancements to its Next-Generation Security Platform that provide customer organizations with the ability to prevent the theft and abuse of stolen credentials, one of the most common methods cyber adversaries use to successfully compromise and maneuver within an organization to steal valuable assets.

The majority of breaches involve password theft at some stage of the attack lifecycle. According to the 2016 Verizon Data Breach Incident Report (DBIR), nearly two-thirds of the breaches analyzed were, in some part, the result of stolen credentials. Because the vast majority of organizations continue to use simple password-based credentials as the primary means of enabling user access to systems, it is often easier for an attacker to steal passwords than it is to find and hack a vulnerable system or successfully bypass malware detection and threat prevention technologies.

Traditional approaches to stopping credential phishing are rudimentary, manual, limited, and rely primarily on educating employees and classifying a phishing site before someone encounters it. If the organization's security products miss a new phishing site, the only recourse is hoping the user doesn't proceed to enter his or her credentials. Further, password-only-based approaches to authentication remain very common due to the traditional complexities of implementing multi-factor authentication, leaving many applications exposed to simple credential abuse-based access by attackers.

Palo Alto Networks now delivers the industry's first multi-method, scalable and automated approach designed to prevent credential-based attacks. These capabilities, delivered from the next-generation firewall, prevent the theft and abuse of stolen credentials and complement additional malware and threat prevention and secure application enablement functionality, to extend customer organizations' ability to prevent cyber breaches.

Among the more than 70 new features introduced to the Next-Generation Security Platform as part of PAN-OS® security operating system version 8.0, credential theft prevention feature highlights include:

- **Automatically identify and block phishing sites** by sending suspicious links from emails to the WildFire™ service for enhanced machine learning-based analysis. If the site is determined to be phishing, PAN-DB will automatically update the phishing URL category, block the site, and prevent users from accessing it.
- **Prevent users from submitting credentials to phishing sites;** by integrating with User-ID™ technology, the firewall can recognize the movement of enterprise credentials in the traffic. If a user unknowingly attempts to transmit a username and password to an unauthorized site, policies within the firewall can alert or drop the traffic and stop the transmission of corporate credentials.
- **Prevent the use of stolen credentials by** providing a policy-based multi-factor authentication framework natively in the next-generation firewall. This unique capability makes it easy to enforce multi-factor authentication from the firewall to stop cyber adversaries from moving laterally in a network and accessing sensitive resources with the help of stolen credentials or compromised endpoints. This is achieved by working at the network level in conjunction with authentication and identity management frameworks, such as single sign-on and multi-factor authentication, and integrating with a number of next-generation identity access management vendors, including Okta®, Ping Identity® and Duo Security, as well as policy enforcement tools. In addition to simplifying the overall administrative overhead, with this new centralized policy-based approach in PAN-OS 8.0, administrators will now be able to protect internal and custom applications with multi-factor authentication, a step that is often impossible to deploy with today's existing tools.

Additional threat prevention, management and hardware highlights are also available with the introduction of PAN-OS 8.0. See these related press releases:

- Palo Alto Networks Extends Safe Application Enablement and Breach Prevention From the Network to the Cloud with Enhancements to Its Next-Generation Security Platform
- Palo Alto Networks Raises Bar with New Threat Prevention Capabilities for Its Next-Generation Security Platform
- Palo Alto Networks Expands Range of Next-Generation Firewall Devices with New Hardware and Virtual Appliances

QUOTES

- "Palo Alto Networks routinely delivers features, like credential theft protection, that address the common cybersecurity challenges IT teams face on a daily basis. It's this continued focus on delivering real-world value that keeps the Palo Alto Networks Next-Generation Security Platform relevant with our customers, and we anticipate they will have a positive reaction to the new innovations announced today."

- Mike McGlynn, vice president, Security Solutions, World Wide Technology, Inc.

- "Credential theft has been a challenge for countless organizations around the world. Palo Alto Networks is bringing to market a unique approach to intercepting the problem at the network level. When this feature is tightly integrated with identity access management solutions, organizations can make significant progress towards ending credential theft."

- Jeff Wilson, senior research director, Cybersecurity Technology, IHS Markit

- "We have too often seen headlines that highlight credential theft as one of the primary methods cyber adversaries use to gain access to networks, systems and assets. For years, there has been an absence of an effective and scalable way for organizations to address this challenge. We are pleased to introduce these unique and industry-leading capabilities as part of our Next-Generation Security Platform and to deliver yet another innovation among many designed to help organizations prevent cyber breaches."

- Lee Klarich, executive vice president, Product Management, Palo Alto Networks

AVAILABILITY

- PAN-OS 8.0 is now available globally to customers of Palo Alto Networks with a current support contract.

To learn more about the Palo Alto Networks Next-Generation Security Platform, visit: https://www.paloaltonetworks.com/products/platforms.html.

Find out more about the new features in PAN-OS 8.0 and new devices:

- **What's New in PAN-OS 8.0**
- **Credential Theft and Abuse Prevention**
- **Register to Attend Palo Alto Networks Colossal Security Event**
- **Palo Alto Networks Next-Generation Security Platform**
- **Blog: Announcing PAN-OS 8.0 - Our Biggest Launch Yet**

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com.

Palo Alto Networks,the Palo Alto Networks logo and PAN-OS are trademarks of Palo Alto Networks,Inc.in the United States and in jurisdiction throughout the world.All other trademarks,trade names or service marks used or mentioned herein belong to their respective owners.

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/palo-alto-networks-delivers-industry-first-capabilities-to-prevent-credential-theft-and-abuse-300403206.html

SOURCE Palo Alto Networks, Inc.

Brittany Stagnaro, Palo Alto Networks, 408-425-6302, bstagnaro@paloaltonetworks.com