Palo Alto Networks Research Shines Spotlight on Cyber Threats Hiding in Plain Sight

June 2, 2014

Report Details How Traditional Exploit Techniques Used In Innovative Ways Can Mask Dangerous Threat Activity

SANTA CLARA, Calif., June 2, 2014 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, today revealed new research on how attackers exploit commonly-used business applications to bypass security controls -- and provides helpful insight into how business leaders and security practitioners need to reassess and strengthen their security posture.

To view the multimedia assets associated with this release, please click: http://www.multivu.com/mnr/7049351-palo-alto-networks-research-cyber-threats-plain-sight

The findings are based on analysis of traffic data collected from 5,500 network assessments and billions of threat logs over a 12-month span and are revealed in the 2014 edition of the Palo Alto Networks Application Usage and Threat Report. The report provides the industry's most detailed assessment of the relationship between advanced cyber threats and the applications running on enterprise networks worldwide.

Key takeaways:

- Common sharing applications such as e-mail, social media, and video remain favored vehicles for delivering attacks but are often the start of multi-phased attacks rather than the focus of threat activity.
- 99 percent of all malware logs were generated by a single threat using UDP; attackers also use applications like FTP, RDP, SSL, and NetBIOS to mask their activities.
- 34 percent of applications observed can use SSL encryption; many network administrators are unaware of what applications on their networks use unpatched versions of OpenSSL, which can leave them exposed to vulnerabilities such as Heartbleed.

Quote:

- "Our research shows an inextricable link between commonly-used enterprise applications and cyber threats. Most significant network breaches start with an application such as e-mail delivering an exploit. Then, once on the network, attackers use other applications or services to continue their malicious activity – in essence, hiding in plain sight. Knowing how cyber criminals exploit applications will help enterprises make more informed decisions when it comes to protecting their organizations from attacks."
  -- Matt Keil, senior research analyst, Palo Alto Networks

In addition to the findings, the report includes actionable intelligence that security teams can use to better protect their networks, such as:

- **Deploy a balanced safe enablement policy for common sharing applications -** key to the success of this recommendation is documentation of the policies, education of users, and periodically updating the policy.
- **Effectively control unknown traffic -** every network has unknown traffic: small in volume, averaging only 10 percent of bandwidth we observed, but high in risk. Controlling unknown UDP/TCP will quickly eliminate a significant volume of malware.
- **Determine and selectively decrypt applications that use SSL -** selective decryption, in conjunction with enablement policies outlined above, can help businesses uncover and eliminate potential hiding places for cyber threats.

To learn more:

- Download the 2014 Application Usage and Threat Report
- Access interactive tools and video providing explaining the intersection of applications and threats
- Read the Palo Alto Networks blog for additional highlights from the report

ABOUT PALO ALTO NETWORKS
Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.

Palo_Alto_Networks

Palo_Alto_Networks 1To view the multimedia assets associated with this release, please click: http://www.multivu.com/mnr/7049351-palo-alto-networks-research-cyber-threats-plain-sight

SOURCE Palo Alto Networks

Jennifer Jasper-Smith, Head of Corporate Communications, Palo Alto Networks, 408-638-3280, jjsmith@paloaltonetworks.com; or Tiffany Curci, Voce Communications, 208-725-2062, tcurci@vocecomm.com