



Palo Alto Networks Reveals - for the First Time - Data on Applications Attackers Most Often Target

February 21, 2013

Data Shows Social Networking and Filesharing Threat Activity Pales in Comparison to Business Critical Apps

SANTA CLARA, Calif., Feb. 21, 2013 /PRNewswire/ -- Palo Alto Networks (NYSE: PANW), the network security company, today released its Application Usage and Threat Report. This 10th edition of the report is the first version to compile and correlate data on application usage and threat activity. Based on analysis of network traffic of more than 3,000 organizations between May and December 2012, the report is the network security industry's most comprehensive examination of application usage and threats. The report's findings include:

- **Social, video, and filesharing are not the top threat sources.** While 339 social networking, video, and filesharing applications represent 20 percent of network bandwidth use, they account for less than 1 percent of threat logs.
- **Exploits continue to target enterprises' most valued assets via commonly used business applications.** Of the 1,395 applications studied, 9 business critical applications were responsible for 82 percent of all exploit logs.
- **Malware hides inside custom applications.** Custom or unknown applications are the leading type of traffic associated with malware communications, accounting for 55 percent of malware logs, yet they are consuming less than 2 percent of network bandwidth.
- **SSL is used as both a security mechanism and a masking agent.** 356 applications use SSL in some way. SSL by itself represented 5 percent of all bandwidth and the 6th highest volume of malware logs. HTTP proxy, used both as a security component and to evade controls, exhibited the 7th highest volume of malware logs.

"Correlating threats with specific applications allows security teams to directly see and control risks in their networks," said René Bonvanie, chief marketing officer at Palo Alto Networks. "We are empowering our customers with the knowledge they need to implement comprehensive security policies and practices to better secure their networks with minimal impact on day-to-day operation."

"The volume of exploits targeting business critical applications was stunning and serves as a data center security wake-up call," said Matt Keil, senior research analyst at Palo Alto Networks and author of the report. "These threats will continue to afflict organizations until they isolate and protect their business applications by bringing threat prevention deeper into the network."

The report categorizes applications into 3 categories: personal applications, business applications, and custom or unknown applications.

- Personal applications include social networking applications (Facebook, Pinterest, Tumblr, and Twitter), filesharing (BitTorrent, Box, Dropbox, Putlocker, Skydrive, and YouSendit), and video (YouTube, Netflix, and Hulu Networks).
- Business applications include Microsoft SQL Server, Microsoft Active Directory, SMB, Microsoft RPC, and other commonly used enterprise applications.
- Custom or unknown applications are defined as either TCP or UDP based applications that are custom (internal to the organization), unrecognized commercially available, or a threat.

Application and Threat Information

Information on the nearly 1,600 applications that are identified by Palo Alto Networks can be found in Applopedia, part of the company's Application and Threat Research Center. Visit the online resource to find the latest news, commentary, and discoveries on applications and threats at <http://researchcenter.paloaltonetworks.com>.

To download the Application Usage and Threat Report (February 2013), please visit: <http://www.paloaltonetworks.com/autr>.

To explore the data from this report using our interactive data visualization tool, please visit: <http://researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization/>

About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its innovative platform enables enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks platform is its next-generation firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks products are used by more than 10,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, "The Network Security Company," the Palo Alto Networks Logo, App-ID, GlobalProtect, and WildFire are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.

SOURCE Palo Alto Networks

Mike Haro, Director of Corporate Communications, Palo Alto Networks, +1-408-438-8628, mharo@paloaltonetworks.com