Palo Alto Networks Research Shows Real-Time Apps and FTP are Preferred Targets for Malware

March 25, 2013

Modern Malware Review Shows Traditional Antivirus Struggles To Detect Malware that Actively Avoids Detection

SANTA CLARA, Calif., March 25, 2013 /PRNewswire/ -- Palo Alto Networks™ (NYSE: PANW), the network security company, today announced its inaugural publication of the Modern Malware Review, an analysis of new and evasive malware in live enterprise networks. The review's findings show that traditional antivirus solutions are not identifying the vast majority of malware infecting networks via real-time applications such as web browsing. The Modern Malware Review is the first industry report to examine the behavior of unknown malware throughout its entire lifecycle, beginning when it enters the network, how it behaves once it is on the infected device and finally the outgoing traffic it generates. Key findings include:

- 94 percent of the fully undetected malware found on networks was delivered via web browsing or web proxies.
- 70 percent of malware left identifiers in their traffic or payload that can be used by security teams for detection.
- 40 percent of seemingly unique malware are actually repackaged versions of the same code.
- FTP is a highly-effective method for introducing malware to a network. 95 percent of malware delivered via FTP went undetected by antivirus solutions for more than 30 days.
- Modern malware is highly adept at remaining undetected on a host device. The review identified 30 different techniques for evading security and more than half of all malware behaviors were focused on remaining undetected.

"It's not enough to simply detect malware out there that is evading traditional security. Enterprises should come to expect more comprehensive prevention from their vendors," said Wade Williamson, senior research analyst, Palo Alto Networks. "That's what the Modern Malware Review is signaling – analyzing undetected malware in real networks has enabled us to arm IT security teams with actionable information for reducing their exposure against threats they might have otherwise missed."

The review provides recommended policies that can help security managers better protect their networks against malware attacks. For example, by knowing that the majority of malware is simply relocated and repackaged versions of the same code, such as Zeus botnets, security teams can use a variety of indicators to identify it and create security policies that can automatically block it.

"Security managers are bombarded almost daily with alerts about the latest malware threats, and manually examining each threat to develop policy to stop it would overwhelm any security team," said Phil Cummings, security administrator, Health Information Technology Services of Nova Scotia. "Reports like Palo Alto Networks' Modern Malware Review provide the kind of real-world data and actionable policy recommendations that make my job easier."

The Modern Malware Review analyzes malware collected by Palo Alto Networks between October and December 2012 via its WildFire malware analysis service. The review identified 26,000 different malware samples on networks that had gone completely undetected by their antivirus solutions.

To download the Modern Malware Review, please visit: http://www.paloaltonetworks.com/mmr.

About Palo Alto Networks
Palo Alto Networks is the network security company. Its innovative platform allows 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 11,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.

SOURCE Palo Alto Networks

Mike Haro, Director of Corporate Communications, Palo Alto Networks, 408-438-8628, mharo@paloaltonetworks.com; or Tim Whitman, Voce Communications, 617-897-8255, twhitman@vocecomm.com