Palo Alto Networks Shines Spotlight on Malware Attack Vectors in Key Industries

December 10, 2014

Especially in education, high tech and healthcare industries, Kuluoz malware family persists

SANTA CLARA, Calif., Dec. 10, 2014 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, today unveiled new analysis of malware trends affecting thousands of organizations in major industries throughout the world. Among the findings, which were released today as part of the new Unit 42 Threat Landscape Review, is the persistence of the Kuluoz or Asprox malware family, which accounted for a majority of malware attack sessions affecting industries as varied as healthcare, retail and financial services.

The Unit 42 Threat Landscape Review is a recurring report examining how organizations in different industries are affected by malware. Research was performed by Unit 42, the Palo Alto Networks threat intelligence team, and included data from WildFire™, which is a key component of the Palo Alto Networks threat intelligence cloud that helps identify threats from applications by executing them in a virtual environment.

QUOTE:

- "The trends we observe in the Threat Landscape Review indicate that malware attacks against industries such as finance, healthcare and critical infrastructure occur over similar channels but in significantly different proportions. It is essential that information security practitioners, from management to governance to enablement and execution, stay current on trends and malware distribution patterns and take a prevention-centric approach to securing their organizations."
  – Ryan Olson, Intelligence Director, Unit 42, Palo Alto Networks

Among the key findings from the Fall 2014 Threat Landscape Review:

- All verticals saw e-mail (SMTP) and HTTP as the primary channels for malware delivery, but the percentages for each industry vary significantly, indicating that these industries have different threat profiles. Retail and wholesale organizations received almost 28 percent over the web channel, while hospitality organizations received just two percent over the same channel. Organizations need visibility into the types of traffic traversing their networks so they can quickly identify and prevent threats.
- Malware was delivered in over 50 distinct applications, 87 percent of which were delivered over e-mail and 11.8 percent through web browsing (HTTP). While these two channels account for the majority of malware attacks, it is important that organizations are able to identify malware in any application allowed in their network.
- Over 90 percent of unique malware samples were delivered in just one or two attacks. Most of these files are part of overarching malware families, but by deploying distinct files just once or twice attackers can evade many antivirus programs. Practitioners need to consider security that can identify and stop attacks at multiple stages in the attack kill chain.
- One malware family, known as Kuluoz or Asprox, was responsible for about 80 percent of all attack sessions recorded during October 2014, impacting nearly 2,000 different organizations. This malware has plagued Internet users for years, despite multiple attempts to disrupt its infrastructure.

Organizations can receive a customized version of the analysis provided in the Threat Landscape Review by requesting an Enterprise Risk Report, which helps organizations understand how their networks compare to those of their industry peers regarding malware attacks.

Enterprise Security Platform
To protect organizations from cyber threats and malware like the kind analyzed in this Threat Landscape Review, the Palo Alto Networks Enterprise Security Platform offers a unique preventative approach with three essential components – next-generation firewall, advanced endpoint protection and threat intelligence cloud – to secure computing environments, prevent known and unknown threats, and safely enable an increasingly complex and rapidly growing number of applications.

To learn more

- **Download the Unit 42 Threat Landscape Review:** www.paloaltonetworks.com/resources/research/threat-landscape-review.html
- **Request a customized Enterprise Risk Report (ERR) for your organization:** http://go.paloaltonetworks.com/err
- **Visit Unit 42, the Palo Alto Networks threat intelligence team, for new research, updates and confirmed speaking appearances:** https://www.paloaltonetworks.com/threat-research.html
- **Subscribe to regular research and analysis from the Unit 42 blog:** http://researchcenter.paloaltonetworks.com/unit42/

About Unit 42
Unit 42, the Palo Alto Networks threat intelligence team, is made up of accomplished cybersecurity researchers and industry experts. Unit 42 gathers, researches and analyzes up-to-the-minute threat intelligence, sharing insights with Palo Alto Networks customers, partners and the broader

community to better protect organizations. Unit 42 team leads regularly appear at industry conferences throughout the world.

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.

Logo - http://photos.prnewswire.com/prnh/20130508/SF04701LOGO

SOURCE Palo Alto Networks

Jennifer Jasper-Smith, Head of Corporate Communications, Palo Alto Networks, 408-638-3280, jjsmith@paloaltonetworks.com, or Tim Whitman, Voce Communications, 617-721-5994, twhitman@vocecomm.com