New Threat Report Illustrates Need For Safe Enablement Of SaaS Applications

October 6, 2015

SANTA CLARA, Calif., Oct. 6, 2015 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, today announced the latest edition of its Application Usage and Threat Report (AUTR) completed by the Palo Alto Networks Unit 42 Threat Intelligence team.

Experience the interactive Multimedia News Release here: http://www.multivu.com/players/English/7049352-palo-alto-networks-autr/

The report, based on data from more than 7,000 enterprises worldwide, showcases real-world trends in enterprise application usage and critical developments in how attackers are attempting to infect organizations. It also offers practical recommendations for preventing cyberattacks.

Findings highlight the explosion in adoption of software as a service (SaaS) based applications, with the potential to introduce new security risks, or allow unauthorized access to sensitive data. Through the report, security organizations also gain insight into how long-standing and common attack vectors, such as email and executable files, continue to present challenges, as well as global application usage trends for high-risk categories, such as remote access applications.

KEY FINDINGS

- **SaaS-based applications explode in popularity** – The number of SaaS-based applications observed on enterprise networks has grown 46 percent from 2012 to 2015, and now includes more than 316 applications.
- **Email attachments continue their toxicity** – Over 40 percent of email attachments were found to be malicious.
- **Remote access application usage is widespread** – There are currently 79 unique remote access applications in use worldwide, which are commonly used by cyberattackers during the course of their operations.
- **Tragedies in the news or headline news turned into attack vectors** – On average, there was a six-hour gap between a breaking news story and when it was used to deliver a spear phishing or spam or Web attack.
- **Prominent adversary profiles exposed** – Three threat actors: Carbanak (Russia/Ukraine), Sandworm (Russia), and Shell Crew (China) have been identified as groups that are engaged in cyberespionage and cybercriminal activity targeting government and business organizations throughout Europe and North America.

QUOTE

"At Palo Alto Networks, we believe that the sharing of cyberthreat intelligence benefits society as a whole, and that belief is the motivation behind the publication of our annual Application Usage and Threat Report. The better informed cybersecurity professionals are about how attackers are exploiting applications to compromise networks, the more likely they will be able to identify attacks and take action to stop them before their networks are compromised."

- Ryan Olson, intelligence director, Unit 42 at Palo Alto Networks

RECOMMENDED ACTIONS

- With the increasing popularity of SaaS applications, security teams are cautioned to familiarize themselves with "shadow IT" – a trend occurring in enterprise networks in which users use SaaS and other applications without IT's knowledge or approval – and its potential to weaken security policies.
- Pervasiveness of malicious email attachments highlights the need for automated security measures that can automatically stop a disguised executable file mistakenly activated by an end user.
- The speed at which new threats are evolving is getting faster and faster. Automated attack tools help criminals to take advantage of new vulnerabilities in a matter of hours. Stopping these attacks requires automated advanced threat prevention measures that provide broad visibility and protection against known and unknown threats.

ABOUT THE AUTHOR

Source material for the report comes from real-world data provided by more than 7,000 enterprise organizations with the Palo Alto Networks security platform deployed. In total, the analysis done for the report included over 65 petabytes of data from WildFire™ and AutoFocus™ subscriptions. The 2015 AUTR is the 12th edition of the report.

To Learn More

- Download the 2015 Application Usage and Threat Report here.
- Access resources explaining the intersection of applications and threats here.
- Read the Palo Alto Networksblog for additional highlights from the report.

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_Inc_Logo

1

d0910651-5add-401b-ba9c-dea380f10b74.HR

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/new-threat-report-illustrates-need-for-safe-enablement-of-saas-applications-300154634.html

SOURCE Palo Alto Networks

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