Palo Alto Networks Research Shows New Twist On Old Cyberattack Method Targeting Mobile Devices

December 7, 2015

White Paper from Unit 42 Explains How Cyberattackers Use Malware to Execute BackStab Attacks, Particularly Against iOS Devices

SANTA CLARA, Calif., Dec. 7, 2015 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, today revealed details of a new "BackStab" attack used to steal private information from mobile device backup files stored on a victim's computer. A white paper from the company's Unit 42 threat intelligence team explains how cyberattackers are using malware to remotely infiltrate computers and execute BackStab attacks in an unprecedented fashion.

Used to capture text messages, photos, geographic location data, and almost any other type of information stored on a mobile device in their possession, BackStab has been employed by law enforcement and cyberattackers alike. The Unit 42 white paper shows how BackStab attacks have evolved to leverage malware for remote access and why Apple® iOS devices have been a primary target for attacks, as the default settings in iTunes® store unencrypted backup files in fixed locations and automatically sync devices when they are connected to a user's computer.

Quote

- "Cybersecurity teams must realize, just because an attack technique is well-known, that doesn't mean it's no longer a threat. While conducting our research into BackStab attacks, we gathered over 600 malware samples from 30 countries around the world that were used to conduct remote BackStab attacks."
  - Ryan Olson, director of threat intelligence, Unit 42, Palo Alto Networks

Recommendations

- iOS users should encrypt their local backups or use the iCloud backup system and choose a secure password.
- Users should upgrade iOS devices to the latest version, which creates encrypted backups by default.
- When connecting an iOS device to an untrusted computer or charger via a USB cable, users should not click the "Trust" button when the dialog box is displayed.

Download the white paper at:
https://www.paloaltonetworks.com/resources/research/unit42-backstab-mobile-backup-data-under-attack-from-malware.html
Subscribe to Unit 42 research updates at
http://researchcenter.paloaltonetworks.com/unit42/
Learn more about Unit 42, the Palo Alto Networks threat intelligence team, at https://www.paloaltonetworks.com/threat-research.html

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 and the Palo Alto Networks logo 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.

Logo - http://photos.prnewswire.com/prnh/20150527/218856LOGO

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/palo-alto-networks-research-shows-new-twist-on-old-cyberattack-method-targeting-mobile-devices-300188627.html

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