Palo Alto Networks Uncovers New Source of Cyberthreats Targeting Businesses

July 22, 2014

Research pinpoints how "419" scammers have evolved to get around traditional enterprise safeguards

SANTA CLARA, Calif., July 22, 2014 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, today revealed that cyber criminals in Nigeria have evolved common malware campaigns to infiltrate businesses that have not previously been their primary targets.

419 Evolution, a new report released today from Unit 42, the Palo Alto Networks threat intelligence team, explains how Nigeria-based scammers are now using the same tools more sophisticated criminal and espionage groups often deploy to steal business-critical data from enterprises.

Nigerian criminals are infamous for running easily-spotted "419" phishing scams that attempt to collect credit card details or personal information from individuals, but over the past few years have expanded their skills to target businesses using more advanced techniques. Palo Alto Networks researchers discovered these activities and techniques, code-named Silver Spaniel, using WildFire, which rapidly analyzes cyberthreats in a cloud-based, virtual sandbox environment.

Key research takeaways:

- Among other techniques, Nigerian criminals use Remote Administration Tools (RATs) available through underground forums, including commercial RATs such as NetWire, that provide complete control over infected systems
- Attacks similar to Silver Spaniel in the past may have come from Eastern Europe or a hostile espionage group; businesses haven't traditionally dedicated resources to these potentially impactful spammers from Nigeria
- Traditional Antivirus programs and legacy firewalls are ineffective because Silver Spaniel attacks are specifically designed to evade those technologies

Quote:

- "These Silver Spaniel malware activities originate in Nigeria and employ tactics, techniques and procedures similar to one another. The actors don't show a high level of technical acumen, but represent a growing threat to businesses that have not previously been their primary targets." -- Ryan Olson, Unit 42 Intelligence Director, Palo Alto Networks

To protect against the NetWire RAT, Palo Alto Networks has released a free tool to decrypt and decode command and control traffic and reveal data stolen by Silver Spaniel attackers, available at https://github.com/pan-unit42/public_tools.

Palo Alto Networks Launches A New Era In Threat Intelligence

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 focuses on the technical aspects of attacks, as well as the context in which they are launched, helping all members of the business community, from CEOs to security practitioners, better understand who is executing attacks and why.

To learn more:

- Download 419 Evolution, the latest research report from Unit 42
- Visit the Unit 42 homepage and read the Unit 42 blog for additional insights from the threat intelligence team
- Visit Palo Alto Networks at Booth #227 at **Black Hat USA 2014**, August 5-7, and hear from Unit 42 threat intelligence experts directly

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.

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/20130508/SF04701LOGO

SOURCE Palo Alto Networks

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