Palo Alto Networks Unit 42 Uncovers New Cyberattacks Targeting Government and Military Networks in Southeast Asia

June 16, 2015

Findings Indicate Potentially State-sponsored Adversary Operating Over Three Years

SANTA CLARA, Calif., June 16, 2015 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, today shared research that uncovers a series of potentially state-sponsored cyberattacks targeting government and military organizations in countries throughout Southeast Asia.

Discovered by the Palo Alto Networks Unit 42 threat intelligence team and dubbed "Operation Lotus Blossom", the attacks appear to be an attempt to gain inside information on the operation of nation-states throughout the region. The campaign dates as far back as three years and involves targets in Hong Kong, Taiwan, Vietnam, the Philippines and Indonesia.

Over 50 separate attacks have been identified in Operation Lotus Blossom. They all use a custom-built Trojan, named "Elise" to deliver highly targeted spear phishing emails and gain an initial foothold on targeted systems. Unit 42 believes the Elise malware was developed to specifically meet the unique needs of the operation, but also is being used in other non-related attacks by the adversary.

The attacks, which display the use of custom-built tools, extensive resources, and persistence across multiple years, suggest a well funded and organized team is behind them. Given these variables and the nature of the targets, Unit 42 believes the motivation for the attacks is cyber espionage and the actors behind them are associated with or sponsored by a nation-state with strong interests in the regional affairs of Southeast Asia.

QUOTE

- "The Trojan backdoor and vulnerability exploits used in Operation Lotus Blossom aren't cutting-edge by today's standards, but these types of attacks can be detrimental if they are successful and give attackers access to sensitive data. The fact that older vulnerabilities are still being used tells us that until organizations adopt a prevention-based mindset and take steps to improve cyber hygiene, cyberattackers will continue to use legacy methods because they still work well."
  - Ryan Olson, intelligence director, Unit 42, Palo Alto Networks

The Unit 42 team discovered the Lotus Blossom campaign using the recently announced Palo Alto NetworksAutoFocus service, which allowed the team's security analysts to correlate and interrogate security events from over 6,000 WildFire subscribers and other threat intelligence sources. These attacks are automatically prevented for all Palo Alto Networks Threat Prevention and WildFire subscribers. Others are encouraged to check their networks for signs of intrusion and add relevant indicators to their security controls, all of which are detailed in the full report.

Recommendations

- **Read more details of the Lotus Blossom attacks on the Unit 42 blog**: http://researchcenter.paloaltonetworks.com/2015/06/operation-lotus-blossom/
- **Access the complete report here, including all Indicators of Compromise (IOCs):** https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html
- **Subscribe to Unit 42 research and analysis updates**: https://www.paloaltonetworks.com/threat-research.html
- **Learn more about AutoFocus:** http://media.paloaltonetworks.com/lp/autofocus/?ts=autofocus
- **Learn more about WildFire**: https://www.paloaltonetworks.com/products/technologies/wildfire.html

About Unit 42
Unit 42 is the Palo Alto Networks threat intelligence team and is made up of accomplished cybersecurity researchers and industry experts. The team 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 around the world. The Unit 42 team is available to consult with Palo Alto Networks customers on security concerns, others in the security industry, and for follow-up questions on their research.

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/20150527/218856LOGO

SOURCE Palo Alto Networks

Brittany Stagnaro, Americas PR & AR Manager, 408-425-6302, bstagnaro@paloaltonetworks.com; Tim Whitman, Voce Communications, 617-721-5994, twhitman@vocecomm.com