3-4-2019

Cyber Threat Report 04 March 2019

Patrick Bell
Army Cyber Institute

ARMY CYBER INSTITUTE AT WEST POINT

CYBER THREAT REPORT

March 4, 2019

Threat Actor Update

BabyShark Malware Targets US National Security Think Tanks

Palo Alto Networks Unit 42 notes the spear phishing emails with a malicious Excel macro document attached share similarities to past North Korean campaigns.

Stone Panda Hacks Norwegian and US companies

The Chinese state-sponsored threat actor APT10 infiltrated a Norwegian managed services provider, international apparel retailer, and a US-based law firm were targeted as part of an economic espionage campaign.

Microsoft Claims Russian Hackers Targeted European Think Tanks

Microsoft is confident attacks targeting Aspen Institute, German Marshall Fund, and German Council on Foreign Relations employees originated from APT28 Fancy Bear.

Chafer APT Targets Diplomats in Iran with Custom Malware

Kaspersky Lab believes the Iran-linked APT is waging a cyber-espionage operation against diplomats in Iran.

Threat Target Update

Supply Chain Attacks Spiked 78% in 2018

Symantec reported malicious actors are increasingly moving toward stealthier intrusions via websites and the software supply chain, exploiting vulnerabilities in commercial software and operating systems to launch cyberattacks.

88% of UK Businesses Breached in Last 12 Months

According to Carbon Black, attacks on UK businesses are growing in volume and sophistication. One-hundred percent of Government and Local Authority organizations reported being breached.

German critical infrastructure attacks rise sharply

In the second half of 2018, the BSI received more reports of IT security incidents by critical infrastructure companies than in all of 2017.

Catastrophic attack wipes servers and backups of VFEmail

A hacker wiped every server and backup server of webmail service provider VFEmail. The company is working to salvage user data.

US Government Contractors phished with online bidding

Anomali Labs have discovered a server hosting two separate phishing campaigns targeted government contractors seeking their PII through online bidding-themed phishing campaigns.

ACI Update

- **Learn about the lessons learned from ACI's Jack Voltaic 2.0 exercise in this GCN.com article.**
- **Read West Point Cyber Chair LTG(R) Rhett Hernandez's interview on the need for coalitions as the key to successful cyber defense.**
- **ACI outreach engaged with middle school students to discuss cryptography, cybersecurity, and inspire them to pursue studies in science, technology, engineering, and mathematics.**

Tech Sector Update

News involving key players, products, and technologies

- **QuadrigaCX cryptocurrency exchange customers may be out $190M after founder dies with passwords**
- **Apple agrees to store Russian data on local servers, strengthening government**
- **DigiCert and Utimaco collaborating with Microsoft to secure future of IoT from quantum computing threats**
- **Google under fire for hidden Nest microphone**
- **TikTok reaches $5.7M settlement with FTC over children's online privacy**

Regulation and Policy Update

News impacting the operational and regulatory environment

- **President Trump executive order supports research and commercialization of AI**
- **Congress considering exchange program for federal, industry, and academia cyber experts**
- **UK makes it illegal to view terrorist propaganda even once**
- **Duke Energy fined $10M for cybersecurity violations**
- **Senators want DHS to explore banning government use of foreign VPNs**
- **UK Parliament report will call for increased regulation of Facebook**

Contact Us

Army Cyber Institute at West Point
2101 New South Post Road West
Point, NY 10996
Phone: 845-938-3436
Web: https://cyber.army.mil
Email: threat.cyber@westpoint.edu

Compilation of cyber-related media reports for the purpose of promoting situational awareness in the government and is not subject to copyright protection. This is not vetted intelligence and does not represent the official position of the US Government or Department of Defense.