2-2-2019

Cyber Threat Report 02 February 2019

Patrick Bell
Army Cyber Institute

ARMY CYBER INSTITUTE AT WEST POINT

CYBER THREAT REPORT

February 2, 2019

Threat Actor Update

Russians accused of hacking DNC after 2018 midterms

Attack attempt apparently unsuccessful, but bears similarities to APT29, the Russian hacking group "Cozy Bear."

FireEye links DNS hijacking campaign to Iran

The campaign has targeted dozens of government, telecom, and Internet infrastructure entities across the Middle East, North Africa, Europe, and North America.

Lazarus-affiliated tools used against Chilean interbank network

The malware toolkit, linked to the North Korean Advanced Persistent Threat group, continues targeting Latin American financial institutions.

DarkHydrus APT utilizes Google Drive in malware attack campaign

The APT group is utilizing Google Drive as its command-and-control server against targets in the Middle East according to 360TIC and Palo Alto Networks.

Threat Target Update

Ukranians hacked SEC for insider trading

New Jersey prosecutors allege two Ukrainians committed securities fraud conspiracy, wire fraud conspiracy, computer fraud conspiracy, wire fraud, and computer fraud.

German man releases private data of politicians and celebrities

The 20-year-old confessed to the biggest data hack in German history and claimed to have acted out of anger at his targets. No foreign intelligence involvement is suspected.

"Cyber incident" compromises Airbus personal data

Hackers acquired professional contact and IT identification details of Europe-based employees, but may have been targeting the firm's intellectual property.

Malware disrupts Tribune Publishing and Los Angeles Times

The attack, which debilitated printing operations, is believed to have originated outside of the US and can reportedly be traced to the Ryuk ransomware that took down a NC water utility in October.

Shipping industry targeted in "whaling" attacks

Pen Test Partners identifies business email compromise attacks are rampant against the shipping industry, which is known for its lax security standards.

ACI Update

- A Fifth Domain article quotes an ACI researcher on preventing cyber attacks through the use of Artificial Intelligence.
- The United States Military Academy's Cyber Policy Team wins innaugural Cyber 9/12 Strategy Challenge in Lille, France.
- The Army Cyber Institute welcomed Soldiers from the 335th Signal Command (Theater) Army Reserve Cyber Operations Group, formally beginning a mutually beneficial partnership.

Tech Sector Update

News involving key players, products, and technologies

- Apple rescinded Google and Facebook access to private iOS apps amid privacy scandal; since reinstated
- Ireland's data protection authority announces Twitter compliance investigation
- Fiat-Chrysler prepares for trial over failure to patch known cybersecurity holes in US cars
- Facebook to merge WhatsApp, Messenger, and Instagram messaging
- Amazon, Google, and Facebook spent more than $65 million lobbying Congress in 2018

Regulation and Policy Update

News impacting the operational and regulatory environment

- 2019 National Intelligence Strategy published with focus on Cyber Threat Intelligence
- Japanese government will try to hack its citizens' IoT devices
- France's Defense Secretary willing to use cyber weapons to respond and attack
- Many Europeans states considering Huawei bans
- National Counterintelligence and Security Center launches public awareness program to prepare US companies from cyber attacks.
- Vietnam's cybersecurity law takes effect, upsetting Internet freedom advocates

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.