4-4-2019

Cyber Threat Report 04 April 2019

Patrick Bell
Army Cyber Institute

CYBER THREAT REPORT

April 4, 2019

Threat Actor Update

Russia Regularly Spoofs Regional GPS

The Center for Advanced Defense (C4ADS) found spoofing of the global navigational satellite system regularly occurred near sensitive areas in Russia, Crimea, and Syria.

North Korean Hackers Behind $571M Crypto Heists

A UN report states the DPRK uses cyberspace "as an asymmetric means to carry out illicit and undercover operations in the field of cybercrime and sanctions evasion."

Chinese Hackers Target Universities to Steal Maritime Secrets

According to iDefense, Chinese hackers used spear phishing to target 27 universities around the world to gain access to maritime military research.

Microsoft Takes Down 99 Hacker-Controlled Websites

A judge granted an injunction allowing Microsoft to disrupt a network of sites the Iranian-linked group APT35 (Charming Kitten, Ajax Security Team, "Phosphorus") used to execute phishing attacks with fake Microsoft security warnings.

Secret Service Detain Chinese Woman with Malware at Mar-a-Lago

The woman bypassed layers of security with a thumb drive containing malware

Threat Target Update

Ransomware Strikes Norsk Hydro, 2 US-based Chemical Companies

LockerGogo, a malicious encryption program, likely infected a Norwegian aluminum company and US firms Hexion and Momentive costing tens of millions in lost business.

Top Navy Admiral Warns of Cyberattacks Against Brass

Chief of Naval Operations Adm. John Richardson said the cyber threat against its top brass led to last year's decision to stop publicly releasing promotion lists.

Hackers Hijacked ASUS Software Updates to Install Backdoors

Kaspersky Labs claims a sophisticated supply chain attack led approximately one million PCs to download and install spyware from the update servers of ASUS, the world's fifth largest computer maker. Three unnamed vendors may also be infected.

Albany, NY and Jackson County, GA suffer ransomware attacks

Link: Jackson County paid $400,000 to regain access to systems and data
Link: Albany: damage unknown, but most services available

Half of industrial control system networks have faced cyberattacks

According to Kaspersky Lab's *Threat Landscape for Industrial Automation Systems* report, almost one in two industrial systems display evidence of attackers attempting malicious activity--in most cases, detected by security software.

ACI Update

- **Dr. Erica Borghard co-authored "Chinese Hackers are Stealing U.S. Defense Secrets: Here is How to Stop Them" for The Council on Foreign Relations.**
- **ACI formalized partnership with 335th Signal Command.**
- **The 2019 International Conference on Cyber Conflict in the U.S. (CyCon U.S.) will explore Defending Forward. The Call for Papers is open now through 22 July 2019.**

Tech Sector Update

News involving key players, products, and technologies

- MySpace loses 50 million songs in failed server migration
- Boeing 737 Max crashes increase scrutiny on oversight and software quality assurance
- Aerodata outage cancels and delays US airlines
- Google fined $1.7B in Europe for antitrust violations in search ad brokering
- Lyft becomes 2019's first tech unicorn to go public, raising $2.34B in IPO
- NIST pushes new encryption protocols for quantum, connected devices

Regulation and Policy Update

News impacting the operational and regulatory environment

- White House increases DoD cyber budget request by $1.6B
- US threatens to reduce intelligence sharing if Germany does not ban Huawei
- Bipartisan IoT security standards bill introduced
- DHS plans no formal investigation into Russian electrical grid incursions
- US Supreme Court rejects Zappos appeal that would have limited liability from data breaches
- Chinese owner may be forced to sell Grindr due to US national security risks
- Executive Order on Coordinating National Resilience to Electromagnetic Pulses issued

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