CYBER THREAT REPORT

June 7, 2019

Threat Actor Update

Russia leads as countries begin migration from Windows to Linux

Russia, China, and South Korea are all migrating from Windows to Linux. Russia and China cite security concerns while South Korea cites cost reduction.

Leverage playbooks to anticipate and identify threat techniques

Unit 42 researchers released a new web tool to visualize adversary activities by mapping MITRE's ATT&CK techniques to kill-chain stages to help defenders understand APT activity.

Russian hackers breach three U.S. anti-virus companies

ADVIntel researchers asses the Fxmsp group to be a credible threat that is offering to sell sensitive proprietary data and network access for $300,000.

China repurposes NSA Hacking Tools

A Symantec research report suspects that Chinese intelligence discovered NSA developed malicious code on their networks and retooled it for Chinese operations.

Inside look at Iranian hacking group

A data dump, analyzed by Palo Alto Networks, exposes source code of Iranian threat group.

Threat Target Update

UK Government shares intel on malicious activity with 16 NATO Allies

Britain's foreign secretary Jeremy Hunt says for the past 18 months, Russia has carried out a new global campaign targeting critical infrastructure of foreign nations and the UK .

Rising threat of insecure code

New ICIT report from Rob Roy argues that software security is a national security concern.

Researchers find aircraft landing systems vulnerable to wireless attack

A paper written by students from Northeastern University shows their research into confirmed vulnerabilities in aircraft landing technology.

Whaling attacks on the rise as executives found to be top targets

Verizon's 2019 Data Breach report highlights threats to c-level executives. (Email required to download report).

Rising ransomware costs in Baltimore

Baltimore refused to pay the $76,000 ransom and faces recovery costs of over $18 million.

Personal Security

LINK: Top phishing subject lines
LINK: Personal web data removal workbook

ACI Update

- **Jack Voltaic 2.0 Critical Infrastructure research results presented at the Joint Engineer Training Conference and Expo**
- **Dr. Erica Borghard's article on Israel's kinetic response to Hamas cyber attack**
- **The 2019 International Conference on Cyber Conflict in the U.S. (CyCon US) 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

- Equifax first company to suffer financial downgrade due to cyber attack
- Huawei summary and what the future holds
- Big tech may face antitrust investigation from House Judiciary
- Amazon debuts delivery drone and claims to be operational in months
- China's tech sector cools down amid slowing demand due to trade war
- CrossFit leads movement to delete Facebook

Regulation and Policy Update

News impacting the operational and regulatory environment

- Executive Order to increase federal cyber workforce
- US telcos banned from using foreign gear by Executive Order
- Bipartisan bill to reduce counterintelligence threats to supply chain
- CCDCOE introduces Cyber Law Interactive Toolkit
- House election security bill reintroduced
- GDPR lessons learned this year
- Solarium Commission: new cyber policy tiger team

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