3-27-2017

Cyber Threat Reports 21 Mar - 27 Mar 2017

James Twist
Army Cyber Institute, contact.cyber@usma.edu

"Compilation of cyber-related media reports for the purpose of promoting situational awareness in the government." "This is not vetted intelligence."

NOTE: Please email: james.twist@usma.edu if you wish to be added or removed from the distribution list.

ARMY CYBER INSTITUTE

Weekly Threat Report

ACI–THREAT ANALYSIS CELL for 21 MAR17 to 27 MAR17

China's Evolving Cyber Warfare Strategies.

Item of Interest: Cyber Strategy / Advanced Persistent Threats

China's cyber capabilities are continuously evolving in parallel with the People's Liberation Army's (PLA) ongoing military reforms and modernization drives. As the PLA invests in the development of comprehensive cyber capabilities, the character of future conflicts in East Asia will increasingly reflect cyber-kinetic strategic interactions.

In a potential conflict with Taiwan, for example, the PLA may put a strategic premium on denying, disrupting, deceiving, or destroying Taiwan's Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. This would be followed by the deployment of the PLA's conventional air wings, precision ballistic missile strikes, and sea power projection platforms – all within the first hours of the conflict. >> Chinese Strategies.

DOD Scientists Say Microchips in Weapons Can Be Hacked.

Item of Interest: Hardware / Supply Chain / Cybersecurity

Most of the U.S. military's weapons systems were built without any effort to protect them from cyberattacks on hardware components, and there is evidence that some already have been fitted with digital backdoors, meaning an enemy could make them fail in a real conflict, Pentagon science advisers said.
>> Cyber Supply Chain.

Espionage Risk to US Heightened as China's Military Presses Domestic Tech Firms.

Item of Interest: Military-Civilian Cooperation / Innovation / Industrial Base

China is taking a page from the Pentagon's playbook under the Obama administration: it's partnering with tech companies to develop more cutting-edge weapons. But China's innovation-focused strategy could elevate the espionage risk to the U.S. Ironically, this new threat emerges as the Trump administration is expected to slow its outreach to the tech firms. >> Increased Espionage Threat?

Microsoft Modifies Windows OS for Chinese Government.

Item of Interest: Software / Cybersecurity / Advanced Persistent Threats / Intellectual Property

China has long been both a huge lure and a thorn in the side for Microsoft. Massive piracy of Windows XP, a decade-long effort to replace Windows entirely with a home-grown Linux variant called Red Flag and an OpenOffice variant called Red Office. But now Microsoft—in partnership with the state-owned China Electronics Technology Group (CETC)—is preparing to reboot its relationship with Beijing.
>> W10 Source Code Available to Chinese Government.

>> See also: ***US Military Going All-In on Windows 10.*** >> U.S. Military Fully Committed to W10.
>> Please see also: ***Windows 10 Keylogger: Microsoft is Tracking Everything You Type.*** W10 Keylogger.
>> Please See Also: ***Windows 10: DoubleAgent 0-day Hijacks Microsoft Tool to Turn A-V into Malware.*** A-V Tool Double Agent?

TECH TRENDS: Stories/ Links

- AV firms do need to stop breaking HTTPS. >> By-passing Encryption.
- 21% of Websites Still Use Insecure SHA-1 Certificates. >> SHA-1 Still Used in the Wild.
- Why Printers Still Pose a Security Threat. >> Printer Vulz.
- Another Challenge For IoT: Open Backdoors. >> IoT Backdoors.
- DDoS Protection: 14 Unique Ways to Protect Your Organisation. >> DDoS Defense.
- Achilles Heel of The Army Air & Missile Defense: the Network. >> Network Defense.
- MAC Randomization: A Massive Failure. >> Researchers Smash Privacy Technique.
- Zero-Day Facts of Life Revealed in RAND Study. >> 7 Year Shelf Life.
- Browser Fingerprinting Tech Works Across Different Browsers. >> 99% Accuracy.
- Preinstalled Malware Found on 38 Android Devices Delivered to Two Companies. >> Commercial Purchases & Supply Chain.
- Army moves toward fielding counter-UAS tools. >> UAS Defense.
- Behavior Analytics Will Leapfrog Security. >> Deep Learning Defensive Tools.
- Norway Says Cyber Attacks Came From Russia. >> Latest Russian Victim.
- Teaching Kids Cyber Skills. Cyber Nation.
- Microsoft Edge Hacked 5 Times at Pwn2Own. >> Browser Security.
- Banking Trojan Citadel Used to Steal $500M, Author Pleads Guilty. >> $500 Million Malware.

STATs of the WEEK

20% of websites are vulnerable due to use of SHA-1 encryption according to new research.

SOURCE: Venafi Labs