6-5-2017

Cyber Threat Reports 16 May - 05 June 2017

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

ARMY CYBER INSTITUTE

Weekly Cyber Threat Report

16 May '17 – 5 June '17

UK PM May's on London Terror Attack: 'Regulate' Internet Companies

Items of Interest: Cyber Policy / International Standards / Combatting Terror

British Prime Minister Theresa May's statement in response to the terror attacks that saw seven people murdered in London on Saturday night has again called for internet companies to make life harder for those who would discuss hateful and violent ideologies. "We cannot and must not pretend that things can continue as they are," the PM said, "and they need to change in four important ways."… >> **Regulate the Net.**

Chinese 'Fireball' Malware Infects 250m Systems Worldwide.

Items of Interest: Malware / Cybersecurity / DCO

A strain of Chinese browser-hijacking malware dubbed Fireball has infected 250 million computers. The malware takes over web browsers and turns them into zombies, security firm Check Point warns. Fireball is capable of executing any code on the infected machines, resulting in a wide range of actions from stealing credentials to dropping additional software nasties. >> **250 Million Systems Worldwide.**

China Cyber-Security Law Will Keep Citizens' Data Within the Great Firewall.

Items of Interest: Data Security / Intellectual Property / Cyber-Powers

China's new cyber-security laws, which come into effect on Thursday, may make it harder for foreign businesses to trade in the country. Under the regulations, data on Chinese citizens – including personal information, salary details and more – can only be kept within China. The law would also prevent the transmission of any economic, scientific or technological data overseas on either national security or public interest grounds, as defined by the Chinese government. The rules apply to any "network operator" – a term that encompasses social media companies and large internet firms – and mean that they need users' permission before transferring any data on them outside the country. The consequences for businesses that fail to comply with this new law are dire: a refused or revoked license can never be reversed. >> **China's Security.**

Insider Threat: Report Highlights Problems, Recommendations and Resources.

Items of Interest: Inside Threats / Threat Mitigation / DCO / Cybersecurity

Describing the insider threat challenges we faced, Mr. Eftekhari said this: "Critical Infrastructure leaders and policy makers are just now beginning to understand the potential for catastrophic digital and cyber-kinetic incidents at the hands of insider threats. As the authors point out, mitigating malicious and non-malicious insiders must be a top priority not only for our government, but for all private-sector organizations. This publication is a powerful asset for any organization looking to build or improve an insider threat mitigation program." >> **Insider Threat Categorized.**

SCADA Systems Plagued by Insecure Development and Slow Patching.

Items of Interest: ICS-SCADA Systems / Critical Infrastructure / Cybersecurity

SCADA systems are at the core of water treatment plants, gas pipelines, electrical power distribution systems, wind farms, expansive communication systems, and even civil defense sirens. Therefore, attacks on SCADA systems have the potential to impact a wide range of systems and numerous pieces of critical infrastructure." And HMIs are the most logical point of attack: if an HMI is compromised, attackers can do pretty much anything to the critical infrastructure it manages. >> **Breaking into SCADA through HMIs.**

TECH TRENDS: Stories/Links

- **The Cost of IoT hacks: 13% of revenue for smaller firms >> 13% of Revenue.**
- **Massive security breach at prominent Los Angeles clinic puts thousands at risk. >> Insider Exposes 15K Patients.**
- **The WannaCry Effect: Users Abandon Windows XP En-Masse. >> Windows XP Systems Culled.**
- **OneLogin Affected by Data Breach, Attacker May Have Decrypted Data. >> Access Manager Hacked.**
- **How Terrorists Slip Beheading Videos Past YouTube's Censors. >> Upload Knights.**
- **Messaging app Telegram centerpiece of IS social media strategy. >> Encrypted Comms Support Terror Plans.**
- **Defense contractor stored intelligence data in Amazon cloud unprotected. >> NGA Data Exposed By Contractor.**
- **Vulnerability affecting 1,000+ apps is exposing terabytes of data. >> Mobile App Vul: "HospitalGown".**
- **Cybercrime Costs to Reach $8 Trillion by 2022. >> $$$.**
- **Radio-controlled pacemakers aren't as hard to hack as you (may) think. >> Four Major Producers Vulnerable.**
- **New 'Judy' malware on Android may have infected 36 million devices. >> Android Malware: "Judy".**
- **Chrome Bug Lets Sites Record Audio and Video Without Indicating. >> Recording Behind the Scenes.**
- ***Hackers Came, but the French Were Prepared. >> Neutralizing Cyber Attacks.***
- **Subtitle Hack Puts Over 200M People at Risk of Remote Code Execution Attacks. >> 200 Million Video Streamers Vulnerable.**

Contact Us

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