“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 13 DEC 16 to 19 DEC 16

Microsoft, Intel, Others Oppose China Plans to Get Access to Source Code

Item of Interest: Intellectual Property / Government Surveillance

Microsoft, Intel, and IBM are three of the most vocal companies that opposed China’s plans to access proprietary source code of software and technology products in order to make sure that they’re hacker proof or do not include backdoors. Twisting Big Tech's Arm.

AI & China: Neural Network Learns to Identify Criminals by Their Faces

Item of Interest: Artificial Intelligence / Privacy Rights / Government Surveillance

Thanks to the work of Xiaolin Wu and Xi Zhang from Shanghai Jiao Tong University in China. These guys have used a variety of machine-vision algorithms to study faces of criminals and non-criminals and then tested it to find out whether it could tell the difference. AI to Target Undesirables?

Putin Brings China's Great Firewall to Russia in Cybersecurity Pact

Item of Interest: Cyber Alliances / Government Surveillance

The Kremlin has joined forces with Chinese authorities to bring the internet and its users under greater state control. Russia has been working on incorporating elements of China’s Great Firewall into the “Red Web”, the country’s system of internet filtering and control, after unprecedented cyber collaboration between the countries. Cyber Alliances the New World Order?

North Korea Cyberattack Traced to City in China

Item of Interest: Advanced Persistent Threats / Critical Infrastructure / ICS-SCADA Systems

"It is our understanding the internal network of the military was hacked from an IP address in Shenyang," a military source told Yonhap. "The malicious code used in the hacking is similar to the code used in several computer breaches." A separate 2014 cyberattack that infiltrated multiple servers at Korea Hydro and Nuclear Power was also linked to an IP address in Shenyang, according to the report. Continuous Attacks Against Ally.

Cybersecurity Advice for the Nuclear Industry

Item of Interest: Critical Infrastructure / Cyber Defense / ICS-SCADA Systems

Less complexity, an active defense, transformative research, and institutionalized cybersecurity should be nuclear industry’s key priorities to stem the rising tide of cyber threats. ICS Experts Shoot Red Flare.

The Botnet That Broke the Internet Isn’t Going Away

Item of Interest: Botnets / Cyber Weapons / Malware / OCO

In just the past few weeks, Mirai disrupted internet service for more than 900,000 Deutsche Telekom customers in Germany, and infected almost 2,400 TalkTalk routers in the UK. This week, researchers published evidence that 80 models of Sony cameras are vulnerable to a Mirai takeover. Botnet Keeps Attacking. And Winning.

An Entire Anti-Drone Industry Is Emerging

Item of Interest: Counter Drone Tech / Cyber Defense / Emerging Technology

An entire anti-drone industry is emerging that will arm anti-drone people with anti-drone technology. These new tools will enable drone detection, tracking, identification, disabling, and even hacking and hijacking the drones as they fly. High Tech Cat and Mouse.

TECH TRENDS:

VULNERABILITIES<LINKS

- *North Korea’s “Super-Secure Red Star OS” Can Be Hacked.* >> Red Star OS.
- *Guessing Valid Credit Card Numbers in Six Seconds? Priceless!* >> Brute Force Wins Again!
- *Innovative Technique to Curtail Illegal Copying.* >> Optical Watermarking.
- *Engineers creates chip just 3 Atoms thick.* >> Nano-tech and Chips.
- *Technical Roadmap for Quantum Computing.* >> Quantum Road-map.
- *Printer Security So Bad, HP Inc. Will Sell Services to Fix It.* >> Glaring Gaps in Every Office.
- *China Chases Silicon Valley Talent Who Are Worried About Trump Presidency.* >> $1 Million Bonus!
- *New NIST Guide Helps Small Businesses Improve Cybersecurity.* >> Help for the Little Guy.
- *Cyberattacks to Get Much Worse, Former NSA Official Says.* >> Health Industry a Target.
- *Cybercriminals Spreading Malware Using Microsoft’s OneDrive.* >> Clever Attack Vector.
- *One-Fifth of Government Agencies Don't Encrypt Data.* >> 20% Fail Basic Cyber-Security Test.
- *Corporate Data Left Unprotected in the Wild.* >> Scores of Gaps in Security.
- *ThyssenKrupp Secrets Stolen in 'Massive' Cyber Attack.* >> German Industrial Giant Pwned!
- *Highly Sensitive Data of Explosives Company Leaked.* >> Explosive Leak.
- *Growing Sophistication of Cyber Attacks Requires Defense and Employee Training.* >> Training.
- *Why it's so hard to prosecute cyber-criminals.* Uphill.
- *Arkansas Sheriff Hit by Ransomware Pays Hackers.* >> Law Enforcement Targeted.

STATs of the WEEK

1. Ransomware spiked 6,000% in 2016 and most victims paid the hackers.

2. 91% of Cyber-Attacks Start with a Phishing Email.

SOURCE:

1. IBM.
2. US-CERT.

Web: http://cyber.army.mil
ThreatCellEmail: threat.cyber@usma.edu

Connect on LinkedIn
Visit our YouTube Channel
Follow us on Twitter
Friend us on Facebook