4-10-2017

Cyber Threat Reports 28 Mar - 10 Apr 2017

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

Follow this and additional works at: https://digitalcommons.usmalibrary.org/aci_rp

ARMY CYBER INSTITUTE

Weekly Cyber Threat Report

March 28 – April 10, 2017

China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon.
Items of Interest: Cyber Strategy / Military Technology / A.P.T.s

When the United States Air Force wanted help making military robots more perceptive, it turned to a Boston-based artificial intelligence start-up called Neurala. But when Neurala needed money, it got little response from the American military. So Neurala turned to China, landing an undisclosed sum from an investment firm backed by a state-run Chinese company. >> Tech4Sale?

Researchers Present Early Warning System for Mass Cyber-Attacks.
Items of Interest: DCO / Cyber Tactics / Malware Markers

A new type of DDoS attack, called amplification attack, was found to be the source of many outages. An international team of researchers (Germany, Japan) has developed a special kind of digital bait for distributed attacks where 21 honeypot traps were laid out, enabling the researchers to document more than 1.5 million attacks. They attached secret digital markers to the attack codes they discovered in the digital wilderness, and could trace the source of the attacks. The different phases of attacks helped develop an early warning system from the data. >> Malware Markers.

IBM: 4 Billion Records Leaked in '16, 10K New Vulnerabilities.
Items of Interest: Data Security / Network Security

Cyber-criminals are getting bolder and bolder, a new report shows, indicating that the number of records breached in 2016 increased 556% compared to the previous year, hitting 4 billion. According to IBM's 2017 X-Force Threat Intelligence Index, on top of the 4 billion records that ended up on the Internet last year, there were also 10,000 software vulnerabilities documented. That is the highest single-year number in the 20 years it has published its report. >> Continuing Trend of Data Leaks.

FBI Cyber Division Warns the Healthcare Industry of FTP Attacks.
Items of Interest: Critical Infrastructure / Hacking Techniques / Cyber-security

The Cyber Division of the U.S. Federal Bureau of Investigation (FBI) warns the healthcare industry that malicious actors are actively targeting File Transfer Protocol (FTP) servers of medical and dental facilities that allow anonymous access. The attackers aim to steal protected health information (PHI) and personally identifiable information (PII) and use them for criminal purposes. >> Healthcare Industry Targeted.

Everything Wrong With the Web Today, According to its Inventor.
Items of Interest: Privacy Rights / Social Media / Data Security

Berners-Lee isn't particularly pleased with the way things have gone with his creation. He has previously and loudly pointed out the problems with the modern web. Here's what the web's inventor thinks is wrong with the web today. >> Data Sharing and the Stratified Internet.

TECH TRENDS: Stories/Links

- Be afraid: China is on the Path to Global Technology Dominance. >> Chinese Cyber Dominance?

- Farmers are Hacking Their Tractors So They Can Actually Fix Them. >> Right to Repair.

- Malware 'disguised as Siemens Software Drills into 10 Industrial Plants'. >> 10 Separate Plants Infected.

- FCC Moves to Crack Down on Scam Robocalls. >> Robocall Strike Force?

- Massive Gift Card Fraud Bot Discovered, 1,000 Customer Websites Attacked. >> GiftGhostBot.

- Java and Flash top list of most outdated programs on users' PCs. >> Most Outdated Software.

- U.S. Charges Russian FSB Officers & Criminals for Hacking Yahoo, Millions of Accounts. >> Indictment.

- New brain-inspired cybersecurity system detects 'bad apples' 100 times faster. >> Neuromorphic Cyber Microscope.

- Department of Labor hacked, possible identity theft of 170,000 Idaho job-seekers. >> Many States at Risk.

- A New Way to Spot Malicious Apps. >> Fairplay.

- LastPass Working on Fix for Newly Discovered Bug. >> Password Manager Vulnerability.

- Congress votes to repeal internet privacy rules. >> Telecom Victory.

- Hacking Attack Woke Up Dallas With Emergency Sirens. >> New Infrastructure Hack?

STAT of the Week:
Hacked Sites Up By 32% in 2016 Over 2015, Says Google. Website Security.

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

LinkedIn   YouTube   Twitter   Facebook

REV-01.01