ARMY CYBER INSTITUTE

Bi-Weekly Cyber Threat Report

August 29 – September 11, 2017

U.S. Government Cybersecurity Lags Behind Fast Food Joints, Say Analysts.

Items of Interest: Critical Infrastructure / Cyber Strategy

The American federal government and countless state and local governments throughout the U.S. are more vulnerable to cyberattacks than your local McDonald's. A new study ranking the cybersecurity of 18 industries "paints a grim picture" with the U.S. government 16th when it comes to protecting its computer systems and data from hackers. "Meeting the information security posture of the fast food industry should not be a lofty goal when it comes to the federal government," said Alex Heid, a hacker and Chief Research Officer at cybersecurity consulting firm SecurityScorecard.

>> Government 16th Out of 18 Industries in Cybersecurity.

Chinese Internet Users Forced to Reveal Real Names When Posting Online.

Items of Interest: Cyber Strategy / Cyber Defense

Remaining anonymous while browsing the web in China is a concept that's pretty much dead, as the country has just released new regulations that would require Internet users to reveal their real names when posting comments online. Until now, users were forced to disclose their identity when connecting to a number of popular services like WeChat, Weibo, and use mobile phone numbers, but with this new set of rules, forums and smaller services would have to enforce the same requirement as well.

>> Chinese State Security Grows More Powerful.

UK Infrastructure Failing to Meet the Most Basic Cybersecurity Standards.

Items of Interest: Critical Infrastructure / Cyber Preparedness

More than a third of national critical infrastructure organizations have not met basic cybersecurity standards issued by the UK government, according to Freedom of Information requests by Corero Network Security.

>> 40% of UK Critical Infrastructure Organizations Not Compliant.

Cyber Criminals Target UK Universities to Steal Missile Secrets and Personal Data.

Items of Interest: Intellectual Property / Data Security

Cyber gangs are targeting British universities to get hold of research into their technological advances, it has been reported. The number of cybersecurity breaches at tertiary institutions has doubled in the past year as gangs exploit weak defenses to steal sensitive information for foreign states.

>> Oxford and Other Prominent Universities Give Up Defense Tech.

Security Researchers: Hackers Have Infiltrated U.S. and EU Energy Companies.

Items of Interest: Critical Infrastructure / APTs / Defense Industrial Base

Phishing, watering holes and malware are being used to steal credentials which could be used to tamper with energy supplies. Over two dozen energy companies and utility providers in the US and Europe have been attacked as part of a cyber espionage campaign which looks to infiltrate the control systems of power supply systems.

>> APT Dragonfly / Energetic Bear / Crouching Yeti is Back!

>> CrashOverRide_Dragos Cybersecurity Report.

Facebook Uncovers $100G in Fake Ad Spending Tied to Russians During 2016 Election.

Items of Interest: Cyber Campaigns and Tactics / Threat Analysis

"In reviewing the ads buys, we have found approximately $100,000 in ad spending from June of 2015 to May of 2017 — associated with roughly 3,000 ads — that was connected to about 470 inauthentic accounts and Pages in violation of our policies," Alex Stamos, Chief Security Officer at Facebook wrote in a post. "Our analysis suggests these accounts and Pages were affiliated with one another and likely operated out of Russia."

>> New Efforts to Stop the Trolls.

TECH TRENDS:

Stories/Links

- Titan Security: How Google Combats Hardware Backdoors.
  >> Hardware Root of Trust.
- Feds Outline Technical Evidence Against WannaCry Researcher
  >> Furthering Attribution.
- Leak of 1,700+ valid IOT passwords makes IoT mess worse.
  >> Massive List Opens Door to 1700 Different Devices.
- Intel AI Accelerator Capable of Trillion Ops Per Second Per Watt.
  >> Neural Compute Engine.
- India shut off the internet in an attempt to maintain order.
  >> 50 Million in the Dark for 5 Days.
- DARPA Looks Beyond Moore's Law.
  >> NextGen Chip Architectures.
- Gazing at Gazer. ESET Analyzes White Bear APT.
  >> ESET_Malware Analysis of Turla's Backdoor.
- Multiple Vulz Affect Rockwell Switches Used in C.I.
  >> CERT Advisory_Rockwell Switches.
- Serious Flaws Found in Westermo Industrial Routers.
  >> Industrial Routers Used in Manufacturing Have Serious Holes.
- Apache Struts Stuffed: Hackers Can Inject Code Into Servers.
  >> Open Source Framework for Developing Apps Wide Open.
- China's Cybersecurity Law Grants 'Unprecedented' Control.
  >> Rock and a Hard Place: Lose Your IP or Access to Huge Market.
- Multiple Bootloader Bugs in Major Chipset Vendors' Code.
  >> Attackers Inside Smartphone's Boot Code.
- Massive Computer Hacking and Telecommunications Fraud.
  >> Elaborate Telecommunications Fraud.
- What Are the Most Important Programming Languages?
  >> Most Prominent Languages for Developers.
- CMU Software Leader Nominated for Pentagon Weapons Testing.
  >> New Focus on Cybersecurity for USG?
- Robot Learns to Follow Orders Like Alexa.
  >> Advancements in Robotics.

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

Compilation of cyber-related media reports for the purpose of promoting situational awareness in the government and is not subject to copyright protection. This is not vetted intelligence and does not represent the official position of the US Government or Department of Defense.

© 2017 Army Cyber Institute