2-14-2018

Cyber Threat Report 01 Feb - 14 Feb 2018

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

ARMY CYBER INSTITUTE

Bi-Weekly Cyber Threat Report

Feb 1st – Feb 14th, 2018

When Crypto-Mining Malware Hits a SCADA Network.

Items of Interest: ICS-SCADA / Advanced Persistent Threats / DCO

Stealthy crypto-mining is on track to surpass ransomware as cybercriminals' most favorite money-making option, and companies with computers and servers that run all day and night long are the preferred targets. This could be more than just a nuisance to the companies – it could seriously affect business operations and render some companies unable to operate for days and even weeks. In some instances, namely when the companies are part of critical infrastructure, the consequences may be more severe than in others.

>> Utility Servers a Goldmine.

73% of Firms Fail Cybersecurity Readiness Tests.

Items of Interest: Cybersecurity / Business Continuity

A staggering 73% of firms face major shortcomings in terms of cybersecurity readiness, according to a new report from specialist insurer Hiscox. Globally, almost half of the 4,500 businesses surveyed (45%) across the US, UK, Germany, Spain, and the Netherlands reported at least one cyber-attack in the past year. Of those, 66% suffered two or more attacks.

>> Wide Ranging Survey Delivers Bad News.

Researchers Showcase Automated Cyber Threat Anticipation System.

Items of Interest: Cyber Strategy / DCO / Response Actions

A group of researchers is trying to develop an automatic early warning system that should help defenders take preventative action before specific cyber attacks start unfolding. Their approach leverages the fact that preparation of cyber attacks often occurs in plain sight, discussed on online platforms and publicly accessible discussion forums.

>> Cyber Counter-Reconnassaince Platform.

Russian Hackers Hunt Hi-Tech Secrets, Exploiting US Weakness.

Items of Interest: Data Security / Third Party Access /

Russian cyberspies pursuing the secrets of military drones and other sensitive U.S. defense technology tricked key contract workers into exposing their email to theft, an Associated Press investigation has found. What ultimately may have been stolen is uncertain, but the hackers clearly exploited a national vulnerability in cybersecurity: poorly protected email and barely any direct notification to victims.

>> Iron Twilight Targets Key Personnel Inside Military-Industrial Complex.

Custom-Made Jihadi Encryption App Hides Messages in Images

Items of Interest: Terrorism / Tradecraft / Cyber Tactics

According to the technology outlet Motherboard, online developers aligned with the global jihadist movement have created a custom tool that allows users to hide encrypted messages inside images, a technique known as steganography. Although the app has been in the testing phases for weeks and its effectiveness is unclear, extremists have long proposed concealing sensitive correspondence through this form of cryptography.

>> "Muslim Crypt" Uses Steganography to Mask Terrorist Comms.

Please also see:

Brits Unveil New Technology Which Detects 94% of ISIS Videos. >> UK AI Program.

Nation's Top Spies Say Russia Continues to Target U.S. Political System

Items of Interest: Advanced Persistent Threats / Influence Operations / Cyber Strategy

The nation's top intelligence chiefs were united Tuesday in declaring that Russia is continuing efforts to disrupt the U.S. political system and is targeting the 2018 midterm election, following its successful operation to sow discord in the most recent presidential campaign.

>> Russia Intent on Undermining Next Election.

Please see also: "The United States is Under Attack." >> DNI Sounds Alarm.

TECH TRENDS:

Stories/Links

- Cryakl Ransomware Antidote Released.
  >> Get to Know Nomoreransom.org.
- House Bill to Boost Cyber Cooperation with Ukraine.
  >> Cyber Alliance?
- That Mega-Vulnerability Cisco Dropped Has an Exploit.
  >> CISCO ASA Software Targeted.
- 36 Indicted for Roles in Transnational Criminal Org.
  >> Infraud Organization: Cyber-Criminal Gang Broken.
- Hotspot VPN Security Flaw Puts 500M Users at Risk.
  >> Popular VPN Service Vulnerable.
- 2017 Smashed Records for Most Breaches, Exposure.
  >> Data Breach, Theft, and Exposure Trends Continue.
- Air Gapped Exfiltration with Noise, Light and Magnets.
  >> Cutting Edge Hacks for Exfiltration.
- Flaw in TLS/SSL Certificates Allows Covert Data Transfer.
  >> Certs Exposed During Handshake.
- 42% Popular Websites are Vulnerable to Cyberattack.
  >> 4600 Phishing Sites Use Legit Hosting Services.
- Hackers Crack Phone Location Tracking, with GPS Off.
  >> Numerous Data Sources Can Give You Away.
- Internet-Accessible ICS Nodes are increasing Yearly.
  >> Tens of Thousands of ICS Systems Accessible.
- Ultra-Reliable OpenVMS, had root for 30 years.
  >> Legacy System VMS, Not So Bulletproof.
- Tech Teams With Insurance for Cyber Policy Discounts.
  >> Apple, CISCO, and Allianz Support Businesses.
- Drones Emerge as New Dimension in Cyber War.
  >> Using Drones As An "Access" Platform.
- Galois to Develop Hardware Security Under DARPA.
  >> Hardware Security a Priority for DARPA.
- How to Hide Within a Social Network.
  >> Remove One, Add Many Technique Aids Concealment.
- What is Micro Segmentation?
  >> Granular Segmentation Improves Security.
- German Court: "Facebook Use of Personal Data Illegal."
  >> Ruling: FB Did Not Secure Informed Consent.
- Crypto Mining Site Hijacked Millions of Android phones
  >> Drive-By Mining Campaign Hits Android.

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