6-18-2018

Cyber Threat Report 01 June - 18 June 2018

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

ARMY CYBER INSTITUTE

Bi-Weekly Cyber Threat Report

June 1st – June 18th, 2018.

Startup Working On Contentious Pentagon AI Project Was Hacked.

Items of Interest: Russia / Artificial Intelligence

A lawsuit filed by former employee Amy Liu this month alleges that Clarifai's computer systems were compromised by one or more people in Russia, potentially exposing technology used by the US military to an adversary. The lawsuit says Clarifai learned of the breach last November, but that Clarifai's CEO and other executives did not promptly report it to the Pentagon. Tech Company Does Not Disclose Russian Hack.

>> Vpnfilter Malware Infecting 500,000 Devices Is Worse Than We Thought. Russian Malware.

>> In World Cup Russia, Our Wi-Fi Networks Will Log On To You! 20% of Wi-Fi Spots Wide Open.

Chinese Hacking Campaign Hacks Into Satelite & Defense Companies.

Items of Interest: APTs/ Cyber Strategy / Espionage

A sophisticated hacking campaign launched from computers in China burrowed deeply into satellite operators, defense contractors and telecommunications companies in the United States and southeast Asia, security researchers at Symantec Corp said on Tuesday. Symantec said the effort appeared to be driven by national espionage goals, such as the interception of military & civilian comms. Computers Controlling Satelites Infected.

>> FB Gave Huawei Special Access To User Data. Special Access Arrangement in Place Since 2010.

>> Chinese Hackers Carry Out Country Level Watering Hole Attack. Central Asian DB is Bait.

>> Hidden Cobra Strikes Again With Custom Rat, Smb Malware. Joanap & Brambul Examined.

>> NK Use MS, Apple, Samsung Tech in Attacks. Loopholes Give Adversary Cutting Edge Tech.

FBI Busts International Email Fraud Ring That Stole Millions.

Items of Interest: Cyber Crime / Law Enforcement

The FBI announced 74 arrests across seven countries in a major email fraud bust on Monday. The alleged email scammers, spread across seven countries, would target midsize businesses, looking to trick employees who had access to company finances. This "cyber-enabled financial fraud" which originated in Nigeria, fools victims into believing they're sending money to business partners, while they're really giving thousands of dollars away to thieves. It doesn't just happen to small businesses. Google and Facebook fell victim to a $100 million scam thanks to an scheme from a suspect in Lithuania. FBI Bust!

>> Atlanta's Huge Cyberattack Worse Than First Thought. 1/3 of Software Programs Unusable.

>> Cybercrooks Are Switching To Telegram. Underground Criminal Marketplaces in Decline.

>> Cryptomining Malware Digs Into Nearly 20% Of Organizations Worldwide. Coinhive.

A Cyber War Is Already Raging, May Lead To 'Armageddon' If Banks Get Hit.

Items of Interest: Critical Infrastructure / Cyber Defense

US and European authorities are concerned about a possible "armageddon" event caused by a successful cyber attack on western banks. A successfully coordinated attack on a too-big-to-fail bank could have "cataclysmic" consequences for the global financial system and deal significant damage to the national security of the west, experts said.

>> DOD Wants 'Internet Isolation' To Secure Pentagon Networks. What is Internet Isolation?

>> Gov Says 'Matter of Time' Until Airliner Hacked. Airplanes the Next Front in Cyber Battle?

>> Holes Punched In Hull Of Maritime Security. Industry Can Be Disrupted.

>> US Govt Mulls Snatching Back Control Of ICANN. Two Yeard Old Decision Under Review.

>> A 'Human In The Loop' Can't Control AI. Ex-Navy Sec Says Safeguards Must Be Built-In.

>> We Need A Better Plan To Deter Hacker Attacks Says US. State: We Need Cyber Detterence.

>> New Battlefield? Integrating Cyber & Electronic Warfare. Future of War or Blurring the Lines?

>> Live In Florida? FL More Likely To Be Hit Than Other States. Florida at Highest Risk for Attack.

>> Cyber Threats To The Midterm Elections. Experts Agree We Are Vulnerable.

>> DLA to Reduce Risks by Slashing App Footprint. DLA Aims to Protect Supply Chain.

>> Hackers Find 65 Bugs in the Pentagon's Travel Management System. DTS Full of Holes.

>> SS7 Routing-Protocol Breach Of US Cellular Carrier Exposed Customer Data. SS7 Exploited.

>> The Bleak State Of Federal Government Cybersecurity. OMB Says 70 Agencies at Risk.

>> US Senator To Pentagon: Encrypt Your Websites. 3 Year Old Deadline Completely Forgotten.

TECH TRENDS:

Stories/Links

- Vietnamese Law Forces Tech Firms to Store Data on Users.
  >> Data To Be Housed In-Country.
- Apple Will Fix Favorite L.E. iPhone Cracking Method.
  >> iPhone Lightning Port to Close Automatically in 1 Hour.
- Malware Analysis Report: N. Korean Trojan: TYPEFRAME.
  >> NK Trojan Examined in Detail.
- 92 Million Users of DNA Testing Firm MyHeritage Exposed.
  >> Israeli Genealogy Site Compromised.
- 26 Million Ticketfly Users' Data Stolen.
  >> Personal Data of 26 Million Taken.
- Critical Flaws Expose ABB Door Systems to Attacks.
  >> Intercoms, Fingerprint Readers, Access Keypads Exposed.
- Marine Corps Wooing Experienced Cyber Members.
  >> Marine Corps Adapts.
- How Employee Behavior Impacts Cybersecurity.
  >> Behavior Sabotages Cyber Security.
- Apple's Plans to Bring Artificial Intelligence to Your Phone.
  >> Hand held AI?
- The Zip Slip Vulnerability – What You Need To Know.
  >> Malware Uses Path Traversal to Wipe Out Files.
- Researchers "Discover 'Holy Grail' Of Machine Learning".
  >> Application of General AI to Machine Learning.
- 1 Of 3 Companies Say Paying Hackers Worth The Risk.
  >> Short Term View Hurts Cybersecurity.
- Microsoft to Buy Coding Site Github for $7.5 Billion.
  >> Open Source Coding Platform Goes to MS.
- Google Groups/G Suite Expose Internal Emails.
  >> 31% of Organizations Misconfigure SYSADMIN Controls.
- An Acoustic Attack Can Bluescreen Windows Computers.
  >> New Attack Vector: Sound Cards?
- Amazon Shareholders: Stop Sharing Facial Recognition.
  >> Rekognition Vs. Privacy Rights.
- Flaws In IBM Qradar Allow Remote Command Execution.
  >> Enterprise Security Product Has Some Flaws.
- An Average Data Breach Will Cost An Enterprise $1.23M.
  >> The Case for Increased IT Budgets.
- Efail Flaws Can Leak Plaintext In PGP & S/MIME.
  >> Bugs Unfixed for 10 Years Leave Gaping Holes.
- Chrome, Firefox Iframe Exploit Can Steal Fb Profile.
  >> Side Channel Attack Can Steal FB Profile.
- Gravityrat: Two-Year Evolution of an APT Targeting India.
  >> Evolution of a Remote Access Tool.
- New Hacking Tool Accesses DVRs and Their Video Feeds.
  >> getDVR_Credentials.
- Exploit Pack V10.07 Released 38.000+ Exploits + Zero-Days.
  >> Exploit Pack Complete with 0 Days For Sale.
- Big Telecoms Stop Sale of Customer Data Following Misuse.
  >> Several Third Party Companies Found at Fault.

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