6-18-2018

Cyber Threat Report 01 June - 18 June 2018

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

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

Recommended Citation
https://digitalcommons.usmalibrary.org/aci_rp/15

This Article is brought to you for free and open access by the Army Cyber Institute at USMA Digital Commons. It has been accepted for inclusion in ACI Technical Reports by an authorized administrator of USMA Digital Commons. For more information, please contact nicholas.olijnyk@usma.edu.
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.

>> Vpfilter 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 Satellite & 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 Satellites Infected.

>> 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-to-thieves” didn’t just happen to small businesses. Google and Facebook fell victim to a scheme from a suspect in Lithuania. FBI Bust!

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

Contact Us

Army Cyber Institute at West Point
2101 New South Post Road
West Point, NY 10996
Phone: 845-938-4346
Web: www.cyber.army.mil
Email: threat.cyber@usma.edu

Linkedin  Youtube  Twitter  Facebook

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

REV-01.01