4-16-2018

Cyber Threat Report 01 Apr - 16 Apr 2018

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

ARMY CYBER INSTITUTE

Bi-Weekly Cyber Threat Report

Apr 1st – Apr 16th, 2018

Recent Russian Cyber Activities and Developments.

Items of Interest: Advanced Persistent Threats / DCO

Robotics, artificial intelligence, and a willingness to strike the enemy's non-military targets will figure in the country's future strategies. Russia will be increasing investment in these areas, as well as space and information warfare, Russian Army Gen. Valery Gerasimov told members of the Russian Military Academy of the General Staff last Saturday. In the event of war, Russia would consider economic and non-military government targets fair game, he said. Non-Military Targets Fair Game?

>> Russians Mass-Exploit Routers in Homes and Gov. Russian Owned Routers?
>> Texas Democrats Note Interference from Russians. Interferance Continues.
>> What New Russian Weapon Took Out This Ukranian Drone? Jamming Efforts.
>> US Election Cybersecurity Funding Gets a Boost of $380 Million. $ for Security.
>> Could Enemies Sabotage Undersea Cables Linking the World? What's the Angle?
>> Russian Government Hacks Itself. Roskomnadzor Flap Hinders Millions.
>> NATO Strengthens Its Cyber Stance. NATO Collective Cyber Defense.

Chinese Cyber Threat Activities.

Items of Interest: Cyber Strategy / Advanced Persistent Threats

Intrusions Focus on the Engineering and Maritime Sector. Since early 2018, FireEye has been tracking an ongoing wave of intrusions targeting engineering and maritime entities connected to South China Sea issues. Chinese Strategic Objectives.

>> The U.S. and China Race to Develop 5G Networks. 5G Race.
>> China's New Frontiers in Dystopian Tech. China's Use of Facial Recognition.
>> Agencies Have 1-Year Deadline to ID Cyber Workforce Shortages. Cyber Shortages.
>> U.S. and China Play Chicken on Trade. How is Cyber Impacted?
>> Secretary Ross Announces Activation of ZTE Denial Order. ZTE Gear Banned.
>> Federal Agency Data Under Siege. Disturbing Study on Government Data.

Facebook Admits Public Data of its 2.2 Billion Users Compromised.

Items of Interest: Cyber Threats / Data Security

Facebook dropped another bombshell on its users by admitting that all of its 2.2 billion users should assume malicious third-party scrapers have compromised their public profile information. 2.2 Billion Users.

>> FB Logs Call and Texts Users Make & Receive On Their Phones. Opting Out.
>> FB Announces Changes to Combat Election Meddling. FB Efforts to Stop Russians.
>> FTC Confirms Probe into Facebook Data Misuse Scandal. Data Use or Misuse?
>> It's not just FB. Thousands of Companies Are Spying on You. Extent of Data Sharing.
>> FB Starts Checking Photos/Videos, Blocks Millions of Fake Accounts. ID Check.

A Cyberattack Hobbles Atlanta, and Security Experts Shudder.

Items of Interest: Cyber Threats / Critical Infrastructure

On March 22, computers in the Atlanta City Government were shut down by ransomware, causing outages on internal and public facing applications, including billing information, city payroll, and court-related information. Although computer networks for the Atlanta Police Department, 9-1-1 systems, and fire-rescue have not been affected, the portions of the network related to the court systems have, forcing police to write out reports by hand. The threat actor demanded $51,000 in Bitcoin to release the data. The ransom has not been paid. Atlanta Systems Brought Low.

>> Baltimore 911 Dispatch System Hacked. Baltimore Infrastructure Attacked.
>> SAMSAM Ransomware Hits Colorado's DoT. Colorado Hit By Ransomware.
>> US Gas Pipelines Hit by Cyber-Attack. Infrastructure Attack vs. Pipelines.
>> After Alert On Hacks, Bigger Push To Protect Power Grid. PJM Protects Grid.

TECH TRENDS:

Stories/Links

- Top Evasion & Exfiltration Techniques Used by Attackers.
  >> Attacker Techniques.
- Iran-linked Hackers Adopt New Data Exfiltration Methods.
  >> Iranian Data Exfil Measures.
- Thousands of Servers Found Leaking Passwords and Keys.
  >> 2300 Servers Exposing Credentials.
- Hacker 'Guccifer 2.0' Reportedly Confirmed Russian Agent.
  >> VPN Mistake Exposes Hacker to Scrutiny.
- 'R2D2' Stops Disk-Wipe Malware Before It Executes.
  >> R2D2 = Reactive Redundancy for Data Destruction.
- Stingray Spying: 5G Will Protect Vs. Surveillance Attacks.
  >> To 5G or Not to 5G?
- Frmr Israeli Spy & Team of Elite Hackers Form C-S Firm.
  >> Mossad Chief Starts New Cybersecurity Firm: XM Cyber.
- Why the Military Takes 3-D Printer Cybersecurity Seriously.
  >> What Could Go Wrong With a 3D Printer?
- AVCrypt Ransomware Attempts to Eradicate Your Antivirus.
  >> How AV Crypt Subverts Firewalls.
- GoScanSSH Malware Avoids Gov. and Military Servers.
  >> GoScan SSH Targets Vulnerable Linux Systems.
- Intel CPUs Vulnerable to New 'BranchScope' Attack.
  >> Another Attack Targets CPUs.
- Arkansas Man Sentenced for Developing Prolific Malware.
  >> NanoCore RAT and Net Seal Malware Developer Busted.
- Former IT Employee of Railroad Sentenced to Prison.
  >> Insider Damages Railroad Network.
- Trusted Boot: Ensuring Embedded Computing Systems.
  >> A Strategy for Protecting Embedded Systems.
- Why You Shouldn't Trust a Stranger's VPN.
  >> WebRTC Flaw Leaves VPNs Vulnerable.
- IoT Smartphone Apps Making Life Easy for Online Criminals.
  >> 80% of Apps Tested Vulnerable, Some have 15 Bugs.
- Congressional IT Workers Not Vetted.
  >> Unauthorized Access Revealed by IG.
- Your Monthly Data Breach Report for April 2018.
  >> April 2018: A Month Like Any Other.
- Legacy Tech a Threat to EU's Telecom Infrastructure.
  >> Legacy Tech Poses Challenge to Telecom Industry.
- Fake Software Update Abuses NetSupport RAT.
  >> Fake Updates Spreads RAT.
- Thousands of Hacked Sites Infecting Visitors with Malware.
  >> Banking Malware Lurking on Unprotected Sites.
- U.K. Reveals Its First Major Cyber-Attack Was Against IS.
  >> British Cyber Campaign Vs. ISIS Revealed.

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