ARMY CYBER INSTITUTE

Cyber Threat Report

December 1 – December 31st, 2017

Cyber Weapons Making Nuclear Deterrence Trickier.

Items of Interest: Cyber Weapons / Critical Infrastructure

Advances in cyber-weapons and counter-space capabilities are creating new pressures on concepts of nuclear deterrence as traditionally construed. As a result, there exists a real and growing possibility of rapid and unintended escalation of any U.S.-Russia crisis or conflict. >> Digital Complexities Muck with Deterrence Models.

(Another) Massive Leak Exposes Data on 123 Million US Households.

Items of Interest: Data Security / Data Confluence / Big Data

The cloud-based data repository from marketing analytics company Alteryx exposed a wide range of personal details about virtually every American household, according to researchers at cybersecurity company UpGuard. The leak put consumers at risk for a range of nefarious activities, from spamming to identity theft, the researchers warned. >> Cloud-Based Marketing Repository Gives Us All Away.

Russia To Build Own Internet Directory, Citing US Info War.

Items of Interest: Cyber Strategy / Cyber Defense

The Russian government will build an "independent internet in the event of global internet malfunctions," the Russian news site RT reported on Tuesday. More precisely, Moscow intends to create an alternative to the global Domain Name System, or DNS, the directory that helps the browser on your computer or smartphone connect to the website server that you're trying to reach. The Russians cited national security concerns, but the real reason may have more to do with Moscow's own plans for offensive cyber operations. >> Nation-State Network Segmentation.

Chinese Security Firm A Front for Advanced Hacking Operations.

Items of Interest: Cyber Policy

Three men who worked for an Internet security firm in China have been indicted on federal charges for hacking into at least three multinational corporations. The malware has been tied to the Chinese government. >> New Front in IP Fight.

Russia Targeted 200 journalists Using Classic KGB Tactics.

Items of Interest: Cyber Threat Tactics / Information Warfare

The AP identified journalists as the third-largest group on a hacking hit list obtained from cybersecurity firm Secureworks, after diplomatic personnel and U.S. Democrats. >> Russia's Multi-Faceted Information Warfare Campaign.

SOCOM Commander: U.S. Needs More Offensive Cyber Weapons.

Items of Interest: Offensive Cyberspace Operations / Cyber Strategy

"While defending is paramount, arguably the greatest space for advancement is in the realm of attack and exploit," said Gen. Raymond A. Thomas III. "We have the technology, we just have to embrace … [cyber] as an essential weapon in our arsenal." he said during remarks at a conference in Virginia. "The limiting factor for cyber effectiveness continues to revolve around policy and process," he said. >> More Punch Needed in U.S. Cyber Arsenal.

The COOLEST Hacks of 2017. >> Surprising, Lesser Known Hacks To Know.

The 10 Most Important Tech Stories of 2017. >> Big Trends in Tech.

TECH TRENDS:

Stories/Links

- What do Gaming Companies Have to Do with DDoS Attacks?
  >> Links Between On-Line Gaming and DDoS Attacks.
- MS Issues ER Update to Address Critical Vul.
  >> Remote Code Execution Vul in Malware Protection Engine.
- Secure Apps Exposed by Flaws in Base Program Languages.
  >> Programming Languages Security Compared.
- Bitcoin Boom is Boon for Extremists.
  >> Profiting From Digital Obscuration to Avoid the Law.
- Thank Kim Jong Un for Your Crypto Gains.
  >> NK's Role in Cryptocurrency Fluctuation.
- Ransomware Attacks North Carolina County.
  >> The New Battleground?
- Major Intel ME Firmware Flaw Lets Attackers Get God Mode.
  >> Buffer Overflow Flaw on Chip's Firmware.
- Hacker Ends Mission After Bricking 10 Million Devices.
  >> "The Janitor", Brickerbot, and a Stark Warning on IoT.
- Facebook Using AI to Spot Terrorist Content.
  >> AI Blocking Content.
- Anonymization Beaten with a Dash of SQL.
  >> The Lesson: Don't release Anonymized Data.
- Profiting From Data Hidden Within Plain Sight.
  >> The Many Uses of Data & Why It's Re-sold.
- Britain Warns Russia It's Ready to Retaliate to Cyber Attacks.
  >> GB Claims Full Spectrum of OCO Options Available.
- US Capital's Surveillance Network Hijacked by Romanians.
  >> When A City Loses Its Surveillance Network.
- This Android Malware Can Overheat and Warp Your Phone.
  >> Loapi Malware Can Physically Damage Device.
- US Short of Options to Punish North Korea for Cyber Attack.
  >> Few Cyber Options for Dealing With Cyber Adversary?
- Air-Gapped ICS Network Pwned in Demo.
  >> New Technique for Hacking Air-Gapped SCADA.

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

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