"Compilation of cyber-related media reports for the purpose of promoting situational awareness in the government. This is not a vetted intelligence product."

NOTE: Please email james.twist@usma.mil if you wish to be added or removed from the distribution list.

ARMY CYBER INSTITUTE

WEEKLY THREAT REPORT

ACI– THREAT ANALYSIS CELL for 18 NOV to 12 DEC 16

Japan Investigating Defense Network Break-In

Item of Interest: Defensive Cyberspace Operations / Critical Infrastructure / Advanced Persistent Threats

Japanese defense officials are investigating a reported penetration of the country's high-speed Defense Information Infrastructure (DII) network. The attacks, which Bloomberg attributes to a possible state-based actor, took place in September but have only now come to light. The DII network is shared by the country's Defense Ministry and its Self-Defense Forces, and according to the South China Morning Post, that allowed the intruders to also penetrate the Ground Self-Defense Force. Japanese SDF Network Breached.

Firefox 0-day in the Wild is Being Used to Attack Tor Users

Item of Interest: Anonymity / Exploits/ Privacy

There's a zero-day exploit in the wild that's being used to execute malicious code on the computers of people using Tor and possibly other users of the Firefox browser, officials of the anonymity service confirmed Tuesday. It included several hundred lines of JavaScript and an introduction that warned: "This is an [sic] JavaScript exploit actively used against Tor Browser NOW." Tor cofounder Roger Dingledine quickly confirmed the previously unknown vulnerability and said engineers from Mozilla were in the process of developing a patch. Tor 0 Day.

EU Police Agency Blames Human Error for Data Security Breach

Item of Interest: Cybersecurity / Data Security

Over 700 pages of confidential police files on 54 European terrorist cases were left unencrypted and exposed online, it has emerged. According to Zembla, the confidential files were taken home by the staff member and put on a personal Iomega storage device that was connected to the Internet without a password, potentially allowing anyone to download the files if they were discovered. Europol Terror Data Breach.

China Cybersecurity Firm Linked With Country's Intel Agency For Espionage

Item of Interest: Government Surveillance / Privacy Rights / Advanced Persistent Threats

Boyusec is working with China's intelligence services and military to doctor security products for spying, says Pentagon report. The Washington Free Beacon quotes the Pentagon as saying the products are doctored by Boyusec before being loaded into Chinese-manufactured computer and telephone equipment. Boyusec and Huawei Technologies, the country's telecom company which is reportedly close to its military, have teamed up for cyber espionage operations, according to the Pentagon. Chinese State Cyber Efforts.

San Francisco Metro System Hacked, Everyone Getting Free Rides

Item of Interest: Hacking / Transportation / Critical Infrastructure

A transit hack resulted in passengers getting free rides on San Francisco's light-rail trains after ticket machines had to be taken offline over the weekend. Passengers enjoyed the Muni Metro freebies Friday night and all day Saturday, reported the San Francisco Chronicle, as San Francisco Municipal Transportation Agency officials struggled to get the systems running again. Transportation Hack.

San Francisco Muni Hacker Gets Hacked Back

Item of Interest: Hacking Back / Response Actions

Revenge is sweet, but irony is sweeter. Apparently, the hacker who infiltrated San Francisco's Muni transportation system late last week fell victim to his own horrible personal cyber hygiene. According to Brian Krebs, a separate individual infiltrated the Muni hacker's own email using nothing more than the ransom note provided by the hacker. And he pulled it off using the oldest trick in the book. Hack-Back.

TECH TRENDS:

VULNERABILITIES<LINKS

- Hackers Hunting Hackers. Exploit Kit Backdoors.
- 48% of Organizations Have Suffered Ransomware Attacks. Ransomware Plague.
- ATM Skimming Hit NY Hospitals. Unguarded.
- Mirai botnet attacks thousands of home routers. Mirai Botnet.
- A new way to anonymize data might actually work. Polymorphic Encryption.
- Keygen Websites Spreading Gatak Backdoor Trojan. Watering Holes.
- "Vindows" Ransomware Uses Fake Microsoft Support. Old Trick Updated.
- Hackers Breach Kuwaiti Parliament Site on Election Da. Information OPs against Kuwait.
- Technology takes over flight of attacking drones. Counter Drone Technology.
- DNA Tech Secures Microchips. Fingerprinting Technology.
- 130,000 Navy Sailors Hacked. Sailor's Data Exposed.
- Huawei Facing a Major Problem in the US. Chinese State Sponsored Tech Company?
- It took 4 years to bring down avalanche. Cyber Crime Bust.
- Hackers waste Xbox, PS4, Pixel, with USB Zapr. Handheld Cyber Weapon.
- These Are the Hacking Powers the Federal Government Will Have under New Rule Change. Rule 41.
- Cyberattacks Strike Saudi Arabia Aviation Agency. Saudis Hit by Cyberattack.

STATs of the WEEK

1. **In 2015, there were 2,260 confirmed data breaches.**
2. **DDOS attacks vs small businesses cost an average of $52K per event**

SOURCE:
1. 2016 Verizon Data Breach Report
2. Kaspersky Labs