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

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

ARMY CYBER INSTITUTE

Weekly Threat Report

ACI – THREAT ANALYSIS CELL for 16 FEB 17 to 6 MAR 17

Army Holds 'Solariums' on Strategic Importance of Secure Software.

Item of Interest: Cybersecurity / Baseline Standards / Cyber Defense

The Army is grappling with the challenge of developing common software baselines, closing institutional gaps and creating a unity of effort across the entire department for software sustainment and development. Held at Aberdeen Proving Ground, the Software Solariums — the first of which was held in September and the second Feb. 2-3 — were about bringing stakeholders together from across the Army, joint force and contracting community to make some "way-ahead recommendations," said Maj. Gen. Bruce Crawford, commander of Army Communications and Electronics Command. >> Army Solariums.

Hard-to-Detect Fileless Attacks Target Banks, Other Organizations.

Item of Interest: Attack Techniques / Open Source Tools / Stealth

A wave of attacks that have recently affected banks and other enterprises used open-source penetration testing tools loaded directly into memory instead of traditional malware, making their detection much harder. Researchers from antivirus vendor Kaspersky Lab started investigating these attacks after the security team from an unnamed bank found Meterpreter in the random access memory (RAM) of a server that acted as the organization's Windows domain controller. >> New HackingTechnique Increases Stealth.

Google Project Zero: How We Cracked Samsung's DoD and NSA Certified Knox.

Item of Interest: Cybersecurity / Virtualization / Vulnerabilities.

Google's Project Zero hackers have detailed several high-severity flaws that undermined a core defense in Samsung's Knox platform that protects Galaxy handsets in the enterprise. Since launching Knox in 2013, the platform has been certified for internal use by UK and US government departments, including the US DoD and NSA. Given these certifications, defense-in-depth mechanisms should be rock solid. But according to Project Zero's Gal Beniamini, who last year tore apart Android's full disk encryption, a Knox hypervisor designed to protect the Linux kernel during runtime can be subverted multiple ways. >> Hypervisor Vulnerable.

Artificial Intelligence Giving Weapons Greater Autonomy.

Item of Interest: AI / Smart Weapons / Intellectual Property

Chinese researchers are making great strides toward advancing artificial intelligence and machine learning technologies that could eventually be incorporated into semiautonomous weapons like anti-ship cruise missiles, observers predict. Chinese companies such as Internet giant Baidu have been making steady progress on AI research, challenging American rivals such as Google and Microsoft. Some Chinese researchers working with U.S. companies have chosen to return home to work on indigenous research projects. >> AI Enabled Weapons.

Revealed: Web Servers Used by Disk-Nuking Shamoon Cyberweapon.

Item of Interest: Malware / Cyber Campaigns / Cyber Defense / Attack Techniques

A detailed analysis of the Shamoon malware – which is playing a huge role in the cyberwar between Saudi Arabia and Iran – has identified servers used to spread the software nasty. Shamoon surfaced in 2012 when it infected 30,000 workstations in the world's largest oil production firm, Saudi Aramco, wiped their hard drives, and put the giant into panic mode. Since then the malware has been refined, and attacks have continued on high-value Saudi government and industry targets as late as last month. >> Iran Cyber Campaign Continues.

Ukraine Charges Russia with New Cyber Attacks on Infrastructure.

Item of Interest: Cyber Threats / Critical Infrastructure / Cyber Campaigns

Ukraine on Wednesday accused Russian hackers of targeting its power grid, financial system and other infrastructure with a new type of virus that attacks industrial processes, the latest in a series of cyber offensives against the country. Oleksandr Tkachuk, Ukraine's security service chief of staff, said at a press conference that the attacks were orchestrated by the Russian security service with help from private software firms and criminal hackers, and looked like they were designed by the same people who created malware known as "Black Energy." >> Russian Cyber Campaign Continues.

TECH TRENDS:

VULNERABILITIES<LINKS

- Botnets Have Infiltrated the Twitter verse. >> Bots.
- Open-Source Attack Tools Open Pandora's Box. >> Malware for Free.
- Intel has a chip with 24 cores that costs $9k. >> Super Chip.
- The security impact of HTTPS interception in the wild. >> 10% of Connections Intercepted.
- Researchers transmit 10 bits with a single photon. >> Bits.
- Terahertz wireless could make space borne satellite links as fast as fib er-optic links. >> 100GBs per second.
- Protecting quantum computing networks against hacking threats. >> Quantum Security.
- Researchers bypass ASLR protection with simple Java code. >> Address Space Layout Randomizer Vulnerable.
- Police Using IoT to Detect Crime. >> Crimefighting Tool?
- Non-Secure IoT Devices Are Powerful Weapons. >> IoT as a Weapon System.
- Hologram Technology Is Finding Military Users. >> Holograms.
- New Ransomware could poison water supply. >> New ICS Attack.
- New Attack Threatens Android For Work Security. >> App in the Middle Attack.
- PC microphones helped steal hundreds of gigabytes of data from Ukraine firms. >> OP Bug Drop.
- Malware Attack on Polish Banks Uses Russian as False Flag. >> False Flag Cyber Attack.
- 25% of healthcare organizations using public cloud do not encrypt data. >> Health Data Vulnerable.
- Stolen Health Record Databases Sell for $500,000 in the Deep Web. >> Databases for Sale.

STATs of the WEEK

A fifth (20%) of Spam Emails Sent in 2016 Distributed Ransomware.

SOURCE:

Kaspersky Labs.