"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 7 MAR 17 to 20 MAR 17

NATO Warns Cyber Attacks Are a Threat to Democracy Itself.

Item of Interest: Cyber Warfare / Core Principles

NATO is showing concern about the impact of cyber-attacks, considering that they are a threat to individuals and organizations, but also to the fundamental nature of democracy. According to Jamie Shea, deputy assistant secretary general for emerging security challenges at NATO, cyber is facilitating more advanced and more effective psychological warfare, information operations, coercion and intimidation attacks, ZDNet reports. Shea added that "Now we worry about the future of democracy, stability, and health of the state's institutions. We are losing faith in the very instruments we've created to spur our economy and spur globalization," Shea said. >> Threat to Democracy?

Which Cyber Countermeasures Improve Security and Which Are a Waste of Money?

Item of Interest: Cybersecurity Strategy

If you want to know about which cyber defenses are most effective and which a waste of money and resources are, ask a hacker. And that's just what Nuix researchers did. "During Black Hat USA and DEF CON 24 in 2016, we conducted a survey of known hackers, professionally known as penetration testers, and asked about their attack methodologies, favorite exploits, and what defensive countermeasures they found to be the most and least effective. >> Effective Cybersecurity Choices.

Yahoo: 32 Million Accounts Accessed via Cookie Forging Attack.

Item of Interest: Hacking Techniques / Software Vulnerabilities / Leadership

Yahoo has said that an unauthorized third party accessed the company's proprietary code to learn how to forge certain cookies, which it said resulted in an intruder accessing approximately 32 million user accounts without a password. "We believe that some of this activity is connected to the same state-sponsored actor believed to be responsible for the 2014 security incident." >> What is Cookie Forging?

Hackers Drawn to Energy Sector's Lack of Sensors, Controls.

Item of Interest: Critical Infrastructure / Energy Sector / Cybersecurity / Defensive Strategy

Oil and gas companies, including some of the most celebrated industry names in the Houston area, are facing increasingly sophisticated hackers seeking to steal trade secrets and disrupt operations, according to a newspaper investigation. A stretch of the Gulf Coast near Houston features one of the largest concentrations of refineries, pipelines and chemical plants in the country, and cybersecurity experts say it's an alluring target for espionage and other cyberattacks. >> Energy Sector Vulnerable?

Undetectable Mac Malware Proton for Sale on the Dark Web.

Item of Interest: Malware / Cybercrime / Advanced Persistent Threats

Hackers are now selling malware for Mac devices straight out on the dark web. They claim the malware is undetectable and provides hackers with the ability to take full control over MacOS devices by evading antivirus software. Proton, as it has been named, the malware is a Remote Administration Tool that is currently being sold over Russian cybercrime message boards. >> Evasive R.A.T.!

StoneDrill Malware Supersedes Shamoon, Has Both Data Wiping and Spying Features.

Item of Interest: Malware / Detection & Mitigation / Offensive Cyberspace Operations

A new type of destructive malware was discovered by Kaspersky. Similar to infamous wiper Shamoon, StoneDrill will destroy everything that's on the infected computer. According to the announcement, StoneDrill features advanced anti-detection techniques and espionage tools. So far, it has targeted victims in the Middle East, but one target was also discovered in Europe. The malware was built in a similar style to the second version of Shamoon, but it was even worse, more sophisticated. As of right now, it's not known how StoneDrill is propagated. >> Sophisticated Cyber Weapon.

TECH TRENDS: Stories / Links

- Data Leak exposes 36K Boeing Employees. > Careless Email.
- Engineers Exfiltrate Data by Blinking Hard Drives' LEDs. > Emanations enable hacking.
- Necurs Botnet Gets Proxy Module with DDOS Capabilities. > Spambot weaponized?
- Cloudbleed: Websites Leaked Crypto Keys, Passwords, More Due to Cloudflare Bug. > Cloudbleed Vulnerability.
- Google Demonstrates First Ever SHA-1 Hash Collision. > SHA-1 Encryption Broken.
- The Devastating Impact of Healthcare Data Breaches. > Healthcare Data.
- Critical SQL Injection Vulnerability Found in NextGEN Gallery WordPress Plugin. > 1 Million Vulnerable Sites.
- Robots Vulnerable to Cyberattacks: Researchers. > Robot Cybersecurity Exposed.
- Millions of Smart Devices in Spain are Vulnerable to Attack. > 5.3 Million Devices Unsecure.
- New FCC Chairman: Net Neutrality Rules Were a 'Mistake' > Net Neutrality Going Away?
- vBulletin Hack Exposes 820,000 Accounts from 126 Forums. > One Hacker, 820K Accounts.
- Security Slip-ups in 1Password and Other Password Managers 'Extremely Worrying'. > Password Managers.
- The Cyber Security Landscape: A Frightening Picture. > CIT Report on Cybersecurity.
- BlackArch Linux Now Offers More Than 1700 Ethical Hacking Tools. > 1700+ Open Source Tools
- Yahoo Execs Knew About 2014 Data Breach As It Happened. > Executive Responsibilities?
- We Found a Hidden Backdoor in Chinese IOT Devices. > Chinese Backdoor.
- Fake Facebook Lite App Infected with Trojan to Steal User's Info. > FB Lite App Infected.

STATs of the WEEK

High Costs of Ransomware: Data from 1000+ businesses shows that:

1. About 85% of the infected businesses had their files forced offline for at least a week.
2. A third of cases had to suffer through these issues for a month or more.
3. 15% of the businesses targeted by this type of attacks never got their data back.

SOURCE: Report "Grim Reality of Ransomware"

Timico Cloud Services & Datto Business Solutions.