Cyber Threat Report 16 Jan - 31 Jan 2018

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

Follow this and additional works at: https://digitalcommons.usmalibrary.org/aci_rp

Recommended Citation
https://digitalcommons.usmalibrary.org/aci_rp/19

This Article is brought to you for free and open access by the Army Cyber Institute at USMA Digital Commons. It has been accepted for inclusion in ACI Technical Reports by an authorized administrator of USMA Digital Commons. For more information, please contact nicholas.oljnyk@usma.edu.
Russian Cyber-Spies Are Carrying Out Some Pretty Clever Hacks.

**Items of Interest: Advanced Persistent Threats / Tradecraft / OCO**

According to a 29-page report ESET published yesterday, Turla hackers have been using benign-looking Flash Player installers to deliver their code. At first analysis, even if victims downloaded the files from sketchy sources, the file would connect to the actual Adobe domains and IP addresses to download and install the necessary files. In spite of the legitimate-looking web traffic, employees at these embassies and consulates received a new backdoor trojan named Mosquito. The attacks with the Mosquito backdoor have taken place since July 2016 and allowed the Turla group to siphon off important documents and infect the victim with additional malware. >> Russian APT Uses Adobe Flash Player to Install Malware.

Hackers Could Blow Up Factories Using Smartphone Apps.

**Items of Interest: Critical Infrastructure / ICS-SCADA / Software Security**

Two security researchers, Alexander Bolshev of IOActive and Ivan Yushkevich of Embedi, spent last year examining 34 apps from companies including Siemens and Schneider Electric. They found a total of 147 security holes in the apps, which were chosen at random from the Google Play Store. Bolshev declined to say which companies were the worst offenders or reveal the flaws in specific apps, but he said only two of the 34 had none at all. Some of the vulnerabilities the researchers discovered would allow hackers to interfere with data flowing between an app and the machine or process it's linked to. So an engineer could be tricked into thinking that, say, a machine is running at a safe temperature when in fact it's overheating. >> Critical Infrastructure Vulnerable Through Reliance on Apps.

‘Terabyte of Death’ Cyberattack Looms Against DoD.

**Items of Interest: Cyber Strategy / DCO / Cyber Threats**

‘Terabyte of Death’ Attack: A Matter of When, Not If. A few years ago, getting a 1-gigabyte or 2-gigabyte attack at the internet access point was a big deal, he said. “Now, we get 600-gig attacks on the internet access points and unique, different ways of attacking that we hadn’t thought of before,” he added. The Defense Department is fortified against even larger attacks, he said. “There’s now, we would call it the ‘terabyte of death’ – there is a terabyte of death that is looming outside the door,” he said. “We’re prepared for it, so we know it’s coming.” He noted, “It’s just a matter of time before it hits us.” >> DISA Directors Stark Warning.

Triton Exploited Zero-Day Flaw to Target Industrial Systems.

**Items of Interest: Critical Infrastructure / Malware Analysis**

The Triton Trojan which targeted core industrial systems in the Middle East last year exploited a zero-day flaw in Triconex controllers to carry out its attack. Triton was first detected in the wild in August 2017 and hit the spotlight in December after the malware was used in an attempt to close down industrial systems in the Middle East.

Researchers from FireEye’s Mandiant said Triton was able to manipulate emergency shutdown systems at an unnamed critical infrastructure firm in the region. The malware is one of only a handful of known examples which have been developed for the purpose of attacking companies in the core industrial sector, including oil, gas, and electricity. >> Triton 0 Day Explained.

Cybercriminals Stole $172 Billion from 978 Million Consumers Last Year.

**Items of Interest: Cyber Crime / Economics / Vulnerability Analysis**

Consumers are confident they’re safe online, but hackers have proven otherwise, stealing $172 billion from 978 million consumers in 20 countries in the past year, according to the 2017 Norton Cyber Security Insights Report. >> A Study in CyberCrime.

China’s Communist Party Extends Reach into Foreign Companies.

**Items of Interest: Cyber Strategy / Advanced Persistent Threats**

American and European companies involved in joint ventures with state-owned Chinese firms have been asked in recent months to give internal Communist Party cells an explicit role in decision-making, executives say. >> Ominous Encroachment.