1-2017

Cyber Threat Reports 20 Dec 2016 - 15 Jan 2017

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

"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 20 DEC 16 to 15 JAN 17

US Government Subcontractor Leaks Confidential Military Personnel Data.

Item of Interest: Data Breaches / Cyber-Security / Data Security

A Pentagon subcontractor has exposed reams of highly sensitive details belonging to active military healthcare professionals online, some of which hold top-secret security clearances. Potomac Healthcare Solutions, a subcontractor brought on board to supply healthcare professionals to the US government and military organizations through its Washington, DC.-based contractor Booz Allen Hamilton, was the source of the data leak. Chris Vickery, lead security researcher of the MacKeeper Security Center, who found the data, told ZDNet in an email that Potomac's own insecure server was the source of the leak. >> Yet Another Govt. Data Leak.

Ransomworm: The Next Level of Cybersecurity Nastiness

Item of Interest: Malware / Cybercrime / Defensive Cyber-space Operations.

As if holding your data hostage and seeking cash payment weren't harsh enough, security experts foresee the next stage of ransomware to be even worse. Scott Millis, CTO at mobile security company Cyber adAPT, expects ransomware to spin out of control in the year ahead. That is an astounding statement when you consider that there were more than 4,000 ransomware attacks daily in 2016, according to Symantec's Security Response group. Corey Nachreiner, CTO at WatchGuard Technologies, predicts that 2017 will see the first ever ransomworm, causing ransomware to spread even faster. >> Evolution of Malware.

Half of Businesses Fell Victim to Cyber Ransom Attacks in 2016.

Item of Interest: Digital Economy / Intellectual Property

Nearly half of businesses report that they were the subject of a cyber-ransom campaign in 2016, according to Radware's Global Application and Network Security Report 2016-2017. Data loss topped the list of IT professionals' cyber-attack concerns, the report found, with 27% of tech leaders reporting this as their greatest worry. It was followed by service outage (19%), reputation loss (16%), and customer or partner loss (9%). Malware or bot attacks hit half of all organizations surveyed in the last year. One reason for the pervasive attacks? The Internet of Things (IoT). Some 55% of respondents reported that IoT ecosystems had complicated their cybersecurity detection measures, as they create more vulnerabilities. >> Economic Subversion?

Can Government Really Fix the Internet of Things Mess?

Item of Interest: IoT / Cyber Policy / Network Security

The private sector often views government as the problem, not the solution. But, in the view of a growing number of experts, the opposite is true when it comes to addressing the rampant and increasing security risks of the Internet of Things (IoT). While it is not a unanimous view, there is general agreement that the blessings the IoT brings to modern life are being undermined by its curses – and that the market will not correct those curses. >> IoT Vulnerability.

US Electricity Grid Faces 'Imminent Danger' from Cyberattacks, Energy Department Warns.

Item of Interest: Critical Infrastructure / DCO / ICS-SCADA

The U.S. Energy Department says the electricity system "faces imminent danger" from cyber-attacks, which are growing more frequent and sophisticated. Grid operators say they are already on top of the problem. In the department's landmark Quadrennial Energy Review, it warned that a widespread power outage caused by a cyber-attack could undermine "critical defense infrastructure" as well as much of the economy and place at risk the health and safety of millions of citizens. The report comes amid increased concern over cybersecurity risks as U.S. intelligence agencies say Russian hacking was aimed at influencing the 2016 presidential election. >> US Preparedness Against Cyber-attack.

TECH TRENDS:

VULNERABILITIES<LINKS

- Android tops 2016 vulnerability list, with 523 bugs. >> *Most Vulnerable Software.*
- FBI probes FDIC hack linked to China's military. >> China Hacking Continues.
- Criminals pose as job applicants to infect networks. >> Social Engineering Vs. HR.
- *Russia to convicted criminal hackers: "Work with us Or jail!" Russian Cyber Recruiting.*
- *Hackers could turn your smart meter into a bomb. >> Bold Claim.*
- *FTC fines D-Link for shoddy security in router. >> Culpability for Poor Security?*
- *'Hacktivists' increasingly target local and state government computers. >>* State & Local Cyber Defense.
- FBI's CMS Hacked by Cyber Zeist. >> FBI Breached?
- FBI Hack Most Likely a Hoax, CMS Maker Says. >> Fake News or PR?
- Spy chief says Germany needs ability to counter cyberattacks. >> Cyber Arms Race?
- US Government Warns Hackers Could Stop Pacemakers and Kill Patients. >> Bio-Hacking?
- Shifu banking trojan evolves and expands. >> Shifu.
- *Los Angeles College pays hackers $28G ransom. >>* $$$.
- *Juniper warns: Borked upgrade opens root on firewalls. >>* Root Access to Firewalls.
- Windows 10 privacy controls: Just a little snooping – or the max? >> Is Privacy Dead?
- *Get ready for the rise of spymail. >>* Heuristics

STATs of the WEEK

There will be a projected shortfall of 1.5 million cybersecurity professionals by 2020.

SOURCE:

Multiple. Michael Brown (Former) CEO of Symantec, and (ISC) Global Information Security Workforce Study.