3-16-2018

Cyber Threat Report 01 Mar - 16 Mar 2018

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

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

Recommended Citation

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.oliynyk@usma.edu.
Bi-Weekly Cyber Threat Report
Mar 1st – Mar 16th, 2018

Russian Cyber Activity Targeting Critical Infrastructure.

**Items of Interest: ICS-SCADA / Advanced Persistent Threats / DCO**

Since at least March 2016, Russian government cyber actors targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. Analysis by DHS and FBI, resulted in the identification of distinct indicators and behaviors related to this activity. Of note, the report Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group, released by Symantec on September 6, 2017, provides additional information about this ongoing campaign.

This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as “staging targets” throughout this alert. The threat actors used the staging targets’ networks as pivot points and malware repositories when targeting their final intended victims. >> U.S. CERT: Russian C.I. Campaign.

>> Please also see: Russian Hackers Use Updated Adobe Flash Tool. Dealer’s Choice Platform.

>> Please also see: Russian A-V Tester Guilty in Certifying Attack Code. Russian Running Illegal Textbed.

>> Russian Cyberspies Hacked Routers in Energy Sector Attacks. CISCO Routers Targeted.

>> Telegram Must Give FSB Encryption Keys: Russian Court. FSB Twists Tech’s Arm for Keys.

>> Keeping on Top of ICS-Focused Hacking Groups, Defenses. Review of ICS-SCADA APTs.

Chinese Hackers Hit U.S. Firms Linked to South China Sea.

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

Chinese hackers have launched a wave of attacks on mainly U.S. engineering and defense companies linked to the disputed South China Sea, the cybersecurity firm FireEye Inc. said. The suspected Chinese cyber-espionage group dubbed TEMP.Periscope appeared to be seeking information that would benefit the Chinese government, said FireEye, a U.S.-based provider network protection systems. The hackers have focused on U.S. maritime entities that were either linked or have clients operating in – the South China Sea, said Fred Plan, senior analyst at FireEye. >> Chinese Cyber Priorities.

>> WeChat Banned by Australian Government. >> Chinese Social Media App Found Faulty.


>> China Isn’t Being Honest With Its Vulnerabilities Database. >> Another Angle to Chinese State Cyber Efforts.

Iranian Threat Group Tactics.

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

From January 2018 to March 2018, through FireEye’s Dynamic Threat Intelligence, we observed attackers leveraging the latest code execution and persistence techniques to distribute malicious macro-based documents to individuals in Asia and the Middle East.

We attribute this activity to TEMP.Zagros (reported by Palo Alto Networks and Trend Micro as MuddyWater), an Iran-nexus actor that has been active since at least May 2017. This actor has engaged in prolific spear phishing of government and defense entities in Central and Southwest Asia. The spear phishing emails and attached malicious macro documents typically have geopolitical themes. When successfully executed, the malicious documents install a backdoor we track as POWERSTATS. >> Iranian Spear-Fishing Campaign.


New Developments in Cyber-Crime as a Service.

**Items of Interest: Cyber-Crime / Cyber Threats**

The neverending stream of high-profile, large scale data breaches has lawmakers searching for answers on how hackers are benefiting and how to stop them. At a hearing Thursday, the House Financial Services Subcommittee on Terrorism and Illicit Finance heard from experts about how to find and crack down on cybercriminals who are swiping and trading massive amounts of individuals’ compromised private information. >> Black TDS Provided Scalable SPAW Campaigns.


>> Cyber Threats are ‘Coming at Us From All Sides,’ FBI Director Says. >> FBI on Digital Warfare.

>> CryptoLurker Hacker Crew Skulk About Like Cyberspies, Earn $$$ Spy Tactics Used by Criminals.

Compilation of cyber-related media reports for the purpose of promoting situational awareness in the government and is not subject to copyright protection. This is not vetted intelligence and does not represent the official position of the US Government or Department of Defense.

© 2017 Army Cyber Institute

REV-01.01