ARMY CYBER INSTITUTE

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 Testbed.

>> 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 Austrailian Government. >> Chinese Social Media App Found Faulty.

>> Cyber-Espionage Group Steals Data From UK Government Contractor. >> Chinese Campaign Examined.

>> 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 Attacks Spark Concerns About Iranian Cyber Threat. Iranian Aggressor Ramping Up.

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 Provides Scalable SPAM Campaigns.

>> Want to Reduce Cybercrime? Undermine Black Market, Experts Say. >> Follow The Money.

>> 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.

TECH TRENDS:

Stories/Links

- Cyber Threats to the Aviation Industry.
  >> Vulnerabilities in the Aviation Industry.
- Six Vulnerabilities Impacting ManageEngine Products.
  >> Widely Owned Business Software Has 6 Zero Days.
- Senators Want Dumber Tech for Energy Grid Cybersecurity.
  >> What is the Right Approach to C.I. Problem?
- The Myth of the Hacker Proof Voting Machine.
  >> Remote Access to Voting Machines Discovered.
- Google's Efforts to Clean-up Its Content.
  >> Google's Efforts to Keep Content Clean.
- MAC OS Malware Increases by 270%.
  >> MAC Malware on the Rise.
- AMD Confirms Processor Flaws Found by CTS Labs.
  >> Many AMD Processor Flaws Confirmed.
- Get Ready for New Updates to Guard Against Spectre.
  >> MicroCode Solution to Chip Flaw.
- Defending Military Vehicles Against Cyberattacks.
  >> Prevention and Detection Strategies.
- Inside the Army's Cyber 'Shark Tank'.
  >> Army's Cyber Forge.
- New Attack Bypasses Microsoft's Code Integrity Guard.
  >> MS Code Integrity Guard Can Be Subverted.
- Synopsys Adds New Algorithms to Protect IoT SoCs.
  >> New Defense for System on Chips.
- Feds Bust CEO Selling Custom Blackberries to Drug Cartel.
  >> Designer Stealth Phones.
- Exim Vul Opens 400,000 Servers to Remote Code Execution.
  >> Exim Mail Transfer Agent Holes.
- Researchers Bypass W10 Lock With Cortana Commands.
  >> Cortana Lets Bad Guys in the Back.
- British Military Spends More on Computers Than Weapons.
  >> Harbinger for the Future?
- Cyber-Attacks Becoming No. 1 Business Risk.
  >> Study Cites 9 Billion Attacks, 12 Thousand Vulz.
- Malware Authors Turn to DNS Protocol as a Covert Channel.
  >> Hackers Use DNS for C&C Technique.
- DDoS Attack Exceeds 1.7 Terabits per Second.
  >> Largest Ever DDoS Attack Recorded.
- Backdooring Connected Cars for Covert Remote Control.
  >> "The Bicho" Hardware Backdoor for Cars.
- New LTE Attacks open users to Snooping, Spoofing.
  >> Ten New Attacks for 4G LTE.
- Critical Vuln in Pivotal Framework's Data Parts Plugged.
  >> Web App Platform Has Some Gaps.

Contact Us

Army Cyber Institute at West Point
2101 New South Post Road
West Point, NY 10996
Phone: 845-938-3436
Web: www.cyber.army.mil
Email: threat.cyber@usma.edu