ARMY CYBER INSTITUTE

Bi-Weekly Cyber Threat Report

Sept 17 – Oct 2, 2017

DHS Reviewing Report Russia-Linked Hackers Targeted U.S. Energy.

Items of Interest: Strategy / Advanced Persistent Threats / Critical Infrastructure

The Department of Homeland Security (DHS) is reviewing a report by a leading cybersecurity company that identifies a sophisticated hacking campaign targeting the U.S. energy sector. Symantec on Wednesday attributed the campaign to a hacker group codenamed "Dragonfly," which has been linked by others to the Russian government. A DHS spokesman confirmed to The Hill that the department is examining the report, though he noted that there is no sign of a public safety threat at this time. "DHS is aware of the report and is reviewing it. At this time there is no indication of a threat to public safety," DHS spokesman Scott McConnell said.
>> APT Dragonfly 2.0 Campaign Against Energy Sector.

Other Developments with Russian Cyber Actors.

Five things to know about the Kaspersky-Russia controversy. >> Kaspersky in the Spotlight.
HP Enterprise let Russia scrutinize Cyber defense system used by Pentagon. >> ArcSight Internals.
Russian-Born Cybercriminal Sentenced to Over Nine Years in Prison. >> The Tverdokhlebov Case.
Russian National & Bitcoin Exchange Indicted For Alleged Money Laundering. >> The Vinnick Case.
Inside the Investigation and Trial of Roman Seleznev. >> The Seleznev Case.

Advent of "Destruction of Service" Attacks; Scale and Impact of Threats Grow.

Items of Interest: Cyber Crime / Threat Techniques / DCO

The Cisco® 2017 Midyear Cybersecurity Report (MCR) uncovers the rapid evolution of threats and the increasing magnitude of attacks and forecasts potential "destruction of service" (DeOS) attacks. These could eliminate organizations' backups and safety nets, required to restore systems and data after an attack. Also, with the advent of the Internet of Things (IoT), key industries are bringing more operations online, increasing attack surfaces and the potential scale and impact of these threats. >> https://engage2demand.cisco.com/cisco_2017_midyear_cybersecurity_report
FedEx: TNT NotPetya infection blew a $300m hole in our numbers. >> Huge Financial Impact.

Equifax Leaks Personal Info of 143 Million US Consumers.

Items of Interest: Cyber Security / Data Theft / Response Actions

One of the largest security breaches ever has come to light today as Equifax revealed attackers used an exploit on its website to access records for 143 million US citizens The oldest of the three major US credit bureaus, it maintains information on over 800 million people for credit and insurance reports. Equifax says the breach lasted from mid-May through July 29th when it was detected. The criminals had access to information that could allow them to create or take over accounts for many of the people impacted since they have names, addresses, birth dates, social security numbers and "in some cases" driver's license numbers.
>> The Beginning of the Story.

Different Aspects to the Story:

Three Equifax Managers Sold Stock Before Cyber Hack Revealed. >> Unethical Conduct?
Equifax data hack is spreading around the world. >> Global Impact.
Equifax was reportedly hacked almost five months before its first disclosed date. >> 5 Months.
Equifax's disastrous Struts patching blunder: THOUSANDS of other orgs did it too. >> 3,054 Orgs.
For weeks, Equifax customer service has been directing victims to phishing site. >> Botched.

Data and Intellectual Property Theft Running Rampant.

Portuguese Engineer Conspires to Export Technology to Iran. >> Optics with Military Applications.
New Zealand Man Conspires to Export Sensitive Parts to China. >> Accelerometers Used in Missiles.
Two Iranians Charged in Hacking of Vermont Software Company. >> Projectile Design.
Hacks of Disney & Netflix Show I-P and Company Secrets are in jeopardy. >> Cyber Extortion.
Operation Wilted Tulip – Exposing a Cyber Espionage Apparatus. >>
http://www.clearskysec.com/wpcontent/uploads/2017/07/Operation_Wilted_Tulip.pdf
CCleaner supply chain malware targeted tech giants. >> High Profile Tech Targeted for I-P Theft.
Chinese national pleads guilty to $100m Microsoft piracy racket. >> Bootleg Pirates.
Deloitte Gets Hacked: What We Know So Far. >> Cyber Security Firm's Has Client's Plans Stolen.

TECH TRENDS: Stories/Links

- **Infrared Signals In Cameras Lets Malware Jump Air Gaps.**
  >> aIR-Jumper weaves Crypto into Infrared.
- **Facebook Hit by €1.2m Fine in Spain for Breaking Privacy Laws.**
  >> FB Faces Scrutiny in Europe.
- **Syringe Infusion Vulnerable to Remote Attackers.**
  >> High Severity Flaws Found in Medicine Delivery Device.
- **'Blueborne': New, Unpatchable Bluetooth Vul Affects Billions.**
  >> 2 Billion Devices Vulnerable to Bluetooth Flaw.
- **Designing for Safety and Security in a Connected System.**
  >> Plan for Embedded Security.
- **D-Link Router Riddled With 0-day Flaws.**
  >> 10 Separate 0 Days in the Same Router!
- **Integrating Military Technologies into Automotive Apps.**
  >> The Future is Lidar.
- **DARPA Rolls Out Electronics Resurgence Initiative.**
  >> DARPA's Innovation Pathway for the NextGen Electronics.
- **Video Nasty Lets VMware Guests Run Code on Host.**
  >> 3 Separate Bugs in Virtual Machines.
- **DOE Invests $50 Mil to improve Critical infrastructure.**
  >> Is It Enough to Improve Energy Infrastructure?
- **Devs Use "Malicious" Modules in Official Python Repository.**
  >> Multiple Code Packages Uploaded to PyPI.
- **Dormant, Sensor Awakes After it IDs a Signal of Interest.**
  >> 0 Stand-By Power Has Many Uses.
- **BEC Attacks More Lucrative than Ransomware Over 3 Years.**
  >> Business Email Compromise: Criminal Riches for the Taking.
- **El Paso-Based Production Company Employee Sentenced.**
  >> Insider SYSADMIN Shuts Down Factory.
- **Attackers Can Use HVAC to C2 Malware on Air-Gapped NW.**
  >> Got HVAC?
- **AI Slurps Millions of Passwords to Know Ones You Use Next.**
  >> Machine Learning Password Cracker.

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

LinkedIn YouTube