ARMY CYBER INSTITUTE

Bi-Weekly Cyber Threat Report

April 15 – April 24, 2017

Kremlin-Linked Hacker Crew's Tactics Exposed.

Items of Interest: Cyber Tactics / Advanced Persistent Threats

Security researchers have published more intel on the tactics of the infamous Russian government-linked hacker crew blamed for compromising the Democratic National Committee (DNC) during last year's US election. A report by SecureWorks' Counter Threat Unit offers an analysis of the connection between the APT 28 crew and Russia's Main Intelligence Directorate (GRU) as well as a look at the comprehensive toolkits the cyber spies have put together. SecureWorks' report also documents attacks by APT 28 on a wide range of targets ranging from individuals in Russia and former Soviet states, current and former military and government personnel and organizations in the US and Europe, authors and journalists.

>> APT 28 Tactics.

Kaspersky Autopsies Cyber Crimes. Identifies Distinct Tradecraft of Lazarus Crew.

Items of Interest: Cyber Crime / Tradecraft

The hacking group blamed for the infamous $81m cyber-heist against the Central Bank of Bangladesh last year has been targeting a far wider range of organizations than previously thought. The so-called Lazarus cyber-espionage and sabotage crew has also been busy attacking casinos, software developers for investment companies and crypto-currency businesses as well as bank around the world, according to researchers from Kaspersky Lab. During the forensic analysis of artefacts left by the group in South-East Asian and European banks, Kaspersky Lab has reached a deep understanding of what malicious tools the group uses and how it operates. Knowledge of the hackers' tradecraft has helped to interrupt at least two other operations aimed at stealing a large amount of money from financial institutions.

>> Lazarus Cyber-Crime Team.

France Has a 'Fourth Army' of Young Hackers for Cyber Warfare

Items of Interest: Cyber Strategy / Cyber Warfare / Cyber Skills

They have done what they were asked to do. Analyze, identify and then develop a code that wipes it out," says Patrice, a French military officer testing potential recruits at a cyber defense center in western France. The exercise was one of dozens held across the country between March 20 and 31, involving 240 people from 12 elite technology colleges, part of a plan to create an army of talented cyber spies to counter digital destabilization efforts. Officials want them to be ready to face cyber warfare that could target civil infrastructure such as water, electricity, telecommunications and transport. They will also be expected to protect French democracy itself…

>> French Cyber Talent and Recruitment Campaign.

TECH TRENDS: Stories/Links

- **Researchers to Present New Vulnerabilities in Amsterdam. >> Zero Days and Femtocells.**
- **Facial Recognition on Galaxy S8 Can Be Bypassed with Photos. >> Bad Bio-metrics.**
- **Bank CEO Warns Tech Users: 'You have no idea what you agreed to". >> Bank Passcodes Given Away?**
- **Turn Threat Data Into Threat Intelligence. >> When Threat Data Goes Bad.**
- **Entrepreneur Vows To Publish Browsing History of U.S. Representatives. >> Bidding for Hackers?**
- **Fake WordPress Plugin Opens Sites to Attackers. >> World's Largest Blogging Platform Vulnerable.**
- **Dissecting One of APT29's Fileless WMI and PowerShell Backdoors. >> "Living Off the Land".**
- **Britain Bombarded With High Level Cyber Attacks. >> Britain Under Fire.**
- **Deep Learning Technologies. >> Micromote Design.**
- **Point-and-Pwn Tool for Posers Dumbs Down Ransomware Spreading. >> Cyber Arms Proliferation.**
- **Germany Creates Separate Military Wing for Cyber Command. >> Separate Cyber Service.**
- **A Better Way to Organize the Internet: Content-Centric Networking. >> NextGen Networking?**
- **Quantum Key System To Make Mobile Transactions More Secure. >> Light Based Encryption.**
- **Toward Printable, Sensor-Laden "Skin" for Robots. >> Flexible, Printable Electronics.**

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

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