5-17-2018

# Cyber Threat Report 01 May - 16 May 2018

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

# ARMY CYBER INSTITUTE

## Bi-Weekly Cyber Threat Report

**May 1st – May 16th, 2018.**

## How China Acquires 'the Crown Jewels' of U.S. Technology

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

ATop's product was potentially groundbreaking — an automated designer capable of making microchips that could power anything from smartphones to high-tech weapons systems. It's the type of product that a U.S. government report had recently cited as "critical to defense systems and U.S. military strength." And the source of the money behind the buyer, Avatar, was an eye-opener: Its board chairman and sole officer was a Chinese steel magnate whose Hong Kong-based company was a major shareholder. The Price of NextGen Software Acquired by Rivals.

Please Also See:

>> Actor Advertises Japanese PII on Chinese Underground. Japanese PII Up for Grabs.
>> Chinese Behind a Decade of Hacks on Software Companies. China's Cyber Campaign Revealed.
>> NK Hackers Stole Data From 17 Countries in Ongoing Cyberattack. Scope of NK Threat.

## Trial Exposes Links Between Cybercriminals & Russian Government.

***Items of Interest: Cyber-Crime / Offensive Cyberspace Operations / Russia***

In 2013, Jurijs Martisevs says, he was contacted by Russian law enforcement. The agents from the Federal Security Service, or FSB, told him the U.S. government was seeking information on him, Martisevs testified. But he said the Russians did not want to hand him over — they wanted his help. At the time, Martisevs was helping run a service based overseas that helped hackers get past anti-virus programs. His testimony in a U.S. court in Virginia helped lead to the conviction of his partner, but it also shed light on the symbiotic relationship between Russian intelligence and the criminal underworld. Russian State Sponsored Cyber Activities.

Please Also See:

>> Russia Is Attacking U.S. Forces With Electronic Weapons In Syria Every Day. Electronic Attack!
>> Kaspersky Lab to Move Core Infrastructure to Switzerland. Transparency or Tradecraft?
>> Beware: Russians Impersonating LoJack Security to Hack Computers. Implant Loaders.
>> Russians Posing as ISIS Threaten Military Wives. Russian False Flag Cyber OPs.
>> Nigeria's Internet Fraudsters Zero In On Corporate Email. BECs Keep Paying Off!
>> Reno Man Pleads Guilty To 8K Fraudulent Accounts With Stolen IDs. One Thief, Many Victims.
>> Europe Continues to Be a Cybercrime Hub. Europe Sees 30% Year on Year Increase.

## Drawing 'Red Lines' for Threats Against the Grid.

***Items of Interest: Critical Infrastructure / DCO / ICS-SCADA***

Congress should step in if the White House doesn't deliver firm guidelines on the federal responses to cyberattacks on the county's electrical systems, said a member of the Senate Energy Committee. "If the executive branch won't create a cyber doctrine, Congress will," Sen. Martin Heinrich (D-N.M.) said during a panel on energy security. Malicious cyber actors must understand where the "red lines" are for the U.S. power grid, he said. Key Questions Raised.

Please Also See:

>> Cybercriminals Expose Oil & Gas While Industry Turns A Blind Eye. CI Left Unguarded.
>> Flaws in Critical-Infrastructure Software Could Spell Catastrophe. Energy Sector Issues.
>> Tennessee: Ukraine Computer Involved in Tennessee Elections Attack. Election Confusion.
>> Why Hackers Love Healthcare. How Hackers Evaluate Targets.
>> White House Sheds Cyber Coordinator Role. Streamlining the NSC.

## Spies Are Going After US Supply Chains, Intel Agencies Say.

***Items of Interest: Supply Chains / Cyber Strategy***

"The most critical CI threats cut across these threat actors: influence operations, critical infrastructure, supply chain, and espionage. Regional actors such as Iran, North Korea, and nonstate actors such as terrorist groups, transnational criminal organizations, and hackers/hacktivists are growing in intent and capability," William Evanina, who leads the National CI Security Center, told the Senate Intelligence Committee. Next Big Spy Battle?

Please Also See:

>> DHS Flexes Muscle with Cybersecurity Strategy. Consequences For Not Meeting Standards.
>> Only 9% of Millennials are Interested in a Cybersecurity Career. Skills Gap Getting Bigger.
>> Senate Wants More Cyber Intelligence. Leaders Seeking Automated Analysis.

## TECH TRENDS:

### *Stories/Links*

- Well-Trained Staff Is Your Best Defense Vs. IoT Cyberattacks
  >> It's About the People!
- Crabby Ransomware Nests in Compromised Websites.
  >> Gandcrab Ransomware.
- Justice Dept. & F.B.I. Investigating Cambridge Analytica.
  >> The Fall of a Political Data Sharing Firm.
- 25% of Businesses Hit with Cryptojacking in the Cloud.
  >> Big Numbers Lead to Big Questions in Cloud Security.
- DISA Discusses Next Steps for CAC Replacement, Encore III.
  >> NextGen Enterprise Security Imminent.
- Google & Internet Archive Top Choices for ISIS Propaganda.
  >> Study in Repositories Used by Terrorists.
- Google and Microsoft Reveal New Spectre Attack.
  >> New Variants Target Processors.
  >> Side Channel Vulnerabilities Alert.
- Optically Tunable Microwave Antennas for 5G Applications.
  >> Optically Induced Plasmas Tune Radiation & Frequency.
- TheMoon Botnet Leverages a 0-Day to Target GPON Routers.
  >> 250,000 Routers Targeted & Vulnerable.
- High-End Router Company DrayTek Admits to 0 Day Vul.
  >> 28 Models Found With Flaws.
- Comcast is Leaking Data From Customers' Wireless Routers.
  >> Internet Activation Service Found Lacking.
- Is Telegram Secure? French Terror Arrest Raises New ?'s.
  >> Doubts About Security.
- ZipperDown Vulnerability May Impact 10% of All iOS Apps.
  >> Researchers Claim 16,000 Apps Affected.
- Chrome, Firefox Targeted by 'Vega Stealer' Malware.
  >> Malware Targets Sensitive Data Stored in Browsers.
- Microsoft's Azure Green-lit For Use by US Spies.
  >> Azure Passes Important Test.
- Large Cryptojacking Campaign Targets Drupal Websites.
  >> 300 Sites Targeted for Old Content Mgmt System.
- Open-Source Vuls Plague Enterprise Codebase Systems.
  >> Summary: Open Source Security & Risk Analysis Report.
- New PowerShell Backdoor Discovered.
  >> PRB-Backdoor.
- FB Suspended 200 Apps in Data Misuse Investigation.
  >> Data Misuse in Social Media.
- Ticketmaster to Trial Facial Recognition Tech at Live Venues.
  >> Corporate Profits Vs. Privacy Rights in the Digital Age.
- Hide and Seek IoT Botnet Resurfaces with Persistence.
  >> Persistent Botnets.
- New Rowhammer Attack Can Hijack Computers Remotely.
  >> The Art & Science of Bit-Flipping DRAM Chips.
- 8.7B Identity Records on Surface, Deep, Dark Webs in 2017.
  >> Data Aggregation: The Really Bad Kind.


### 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