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:

>> Russia Is Attacking U.S. Forces With Electronic Weapons In Syria Every Day. Electronic Attack!
>> Nigeria’s Internet Fraudsters Zero In On Corporate Email. BECs Keep Paying Off!
>> Russians Posing as ISIS Threaten Military Wives. Russian False Flag Cyber OPs.

his partner, but it also shed light on the symbiotic relationship between Russian intelligence and past anti-virus programs. His testimony in a U.S. court in Virginia helped lead to the conviction of

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

In 2013, Jurjis 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?
>> 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 country’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.
>> 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.

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