2-14-2018

Cyber Threat Report 01 Feb - 14 Feb 2018

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

Follow this and additional works at: https://digitalcommons.usmalibrary.org/aci_rp

Recommended Citation
https://digitalcommons.usmalibrary.org/aci_rp/13

This Article is brought to you for free and open access by the Army Cyber Institute at USMA Digital Commons. It has been accepted for inclusion in ACI Technical Reports by an authorized administrator of USMA Digital Commons. For more information, please contact nicholas.oliynyk@usma.edu.
Stealthy crypto-mining is on track to surpass ransomware as cybercriminals’ most favorite money-making option, and companies with computers and servers that run all day and night long are the preferred targets. This could be more than just a nuisance to the companies — it could seriously affect business operations and render some companies unable to operate for days and even weeks. In some instances, namely when the companies are part of critical infrastructure, the consequences may be more severe than in others.

**73% of Firms Fail Cybersecurity Readiness Tests.**

A staggering 73% of firms face major shortcomings in terms of cybersecurity readiness, according to a new report from specialist insurer Hiscox. Globally, almost half of the 4,500 businesses surveyed (45%) across the US, UK, Germany, Spain, and the Netherlands reported at least one cyber-attack in the past year. Of those, 66% suffered two or more attacks.

Researchers Showcase Automated Cyber Threat Anticipation System.

A group of researchers is trying to develop an automatic early warning system that should help defenders take preventative action before specific cyber attacks start unfolding. Their approach leverages the fact that preparation of cyber attacks often occurs in plain sight, discussed on online platforms and publicly accessible discussion forums.

**Russian Hackers Hunt Hi-Tech Secrets, Exploiting US Weakness.**

Russian cyber spies pursuing the secrets of military drones and other sensitive U.S. defense technology tricked key contract workers into exposing their email to theft, an Associated Press investigation has found. What ultimately may have been stolen is uncertain, but the hackers clearly exploited a national vulnerability in cybersecurity: poorly protected email and barely any direct notification to victims.

**Custom-Made Jihadi Encryption App Hides Messages in Images**

According to the technology outlet Motherboard, online developers aligned with the global jihadist movement have created a custom tool that allows users to hide encrypted messages inside images, a technique known as steganography. Although the app has been in the testing phases for weeks and its effectiveness is unclear, extremists have long proposed concealing sensitive correspondence through this form of cryptography.

**Nation’s Top Spies Say Russia Continues to Target U.S. Political System**

The nation’s top intelligence chiefs were united Tuesday in declaring that Russia is continuing efforts to disrupt the U.S. political system and is targeting the 2018 midterm election, following its successful operation to sow discord in the most recent presidential campaign.

**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