11-6-2017

Cyber Threat Report 17 Oct - 06 Nov 2017

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/20

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.
Tor’s Next-Gen Onion System Works to Keep Servers Hidden.

**Items of Interest: Tradecraft / Dark Web**
Tor is unveiling its next-gen sites, with the focus on strengthening security. By using new encryption algorithms, improved authentication, and a redesigned directory, Tor claims its next-gen design will keep an onion address completely private. In the past, its network could learn about your onions, which could have resulted in info leaks and cyberattacks. Just this year, news emerged that a hacker had knocked out about a fifth of the Tor network (over 10,000 “secret” sites in total). "All in all, the new system is a well needed improvement that fixes many shortcomings of the old design, and builds a solid foundation for future onion work," writes Tor.

>> Next Gen Onion Keeps Servers in the Dark.

How Much Do Criminals Pay for Certificates on the Dark Web?

**Items of Interest: Cyber-Crime / Cyber-security / Tactics**
The Cyber Security Research Institute (CSRI) conducted a six-month investigation into the sale of digital code signing certificates on the dark web. The research uncovered code signing certificates readily available for purchase on the dark web, selling for up to $1,200 – making them more expensive than counterfeit U.S. passports, stolen credit cards and even handguns. “We’ve known for a number of years that cyber criminals actively seek code signing certificates to distribute malware through computers,” said Peter Warren, chairman of the CSRI. “The proof that there is now a significant criminal market for certificates throws our whole authentication system for the Internet into doubt and points to an urgent need for the deployment of technology systems to counter the misuse of digital certificates.”

>> Cyber criminals Neutralizing Cyber Security.
See also: Hackers abusing digital certs smuggle malware past security scanners. >> Dark Certs.

Canadians Suffer Dozens of Successful State-Sponsored Cyber-Attacks.

**Items of Interest: Cyber Defense / Cyber Strategy**
“While cyber incidents and breaches still occur, they are becoming less frequent,” says Public Safety Canada’s latest evaluation of the effectiveness of the government’s 2010 cyber security strategy. The government will shortly announce an updated cyber strategy after conducting a national consultation. >> Canadians Getting Hit Hard.


**Items of Interest: Cyber Policy / Alliances / International Relations**
In Response to Russian interference in the electoral campaigns in Germany, France, and the Netherlands, and the North Korean WannaCry attack on the U.K. health services EU governments are planning to sign a declaration – officially titled “The framework on a joint EU diplomatic strategy.” The government will shortly announce an updated cyber strategy after conducting a national consultation. >> Authorization for Collective Military Response Debated.

Russian Influence Reached 126 Million Through Facebook Alone.

**Items of Interest: Influence Campaigns / Weaponized Information**
Russian agents intending to sow discord among American citizens disseminated inflammatory posts that reached 126 million users on Facebook, published more than 131,000 messages on Twitter and uploaded over 1,000 videos to Google’s YouTube service, according to copies of prepared remarks from the companies that were obtained by The NY Times.

>> Cyber Reach.

Sowbug: Cyber Espionage Group Targets South American & Southeast Asian Governments.

**Items of Interest: Threat Actors / Diplomacy / Cyber Espionage**
Symantec has identified a previously unknown group called Sowbug that has been conducting highly targeted cyber-attacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates.

>> New SOWBUG APT Rips Into South America.