ARMY CYBER
INSTITUTE

Weekly Cyber Threat Report

16 Oct 17 – 6 Nov 2017

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.

EU Set to Declare Cyberattacks as "Acts of War," Allowing Collective Response.

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 response to malicious cyber activities" — which defines cyberattacks on any EU country as an act of war, potentially triggering a military retaliation – even including conventional arms – in response. In 2014, NATO updated its cyber defense policy, to make an explicit link between cyberattacks at a certain threshold and the invocation of a NATO's article 5 collective defense as part of the treaty. >> 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.

TECH TRENDS: Stories/Links

- **Flaw in IEEE P1735 Standard, Used to Encrypt IP.**
  >> Standard Exposes Intellectual Property.
- **Paradise Papers Revelations Around the World.**
  >> Major Data Breach Creates Huge Exposure.
- **Nepal Bank Latest Victim in Targeting SWIFT System.**
  >> Another SWIFT Attack.
- **$300 Million Worth of Etherium Locked Up!**
  >> Coders Hack Back to Block $300 Million Theft.
- **Hackers Launch Silence Trojan, Quietly Raid Millions!**
  >> New Banking Trojan Hits 10 Institutions.
- **Oracle Plasters 'Easily Exploitable' Backdoor in Identity Mgr.**
  >> A Perfect '10' Bug Score!
- **Samsung Works with U.S. Military to prototype 5G NW.**
  >> Military-Commercial Collaboration on 5G Network.
- **Critical Tor Flaw Leaks Users Real IP Address.**
  >> Tor Flaw.
- **Nanotube Fiber Antennas as Capable as Copper.**
  >> Nanotech Cyber Capabilities.
- **Faster Big-Data Analysis.**
  >> Speeding Up Big D Analysis by 100X.
- **Assessing the IoT Botnet: Reaper.**
  >> Reaper Botnet.
- **Sweden Mulls Introducing Digital 'Anti-Terror' Fences.**
  >> Creative Use of Cyber to Thwart Terrorists.
- **How Wireless Intruders Can Bypass NAC Controls.**
  >> New Technique Against Wireless.
- **U.S. Ports Lack Key Cyber Tools.**
  >> More Vulnerabilities in Maritime Critical Infrastructure.
- **Bootkit Ransomware Hops Down BadRabbit Hole in Japan.**
  >> Destructive Wiper Savages Japanese Businesses.
- **Disney-Branded Internet Filter Had 23 Vulnerabilities.**
  >> Parental Filter Leaves Parents Vulnerable.
- **Seagate Launches 1st HDD for AI-Enabled Surveillance.**
  >> Enhancing AI Enabled Surveillance.
- **BB CEO Promises to Break Customer Encryption if US Asks.**
  >> Breaking Encryption a Business Strategy?
- **FBI Unable to Break into Texas Church Gunman's Cellphone.**
  >> The Old Encryption-Law Enforcement Debate is Alive.
- **iPhone 7 Compromised Several Times at Hacker Event.**
  >> iPhone 7 Vulnerabilities.

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 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.