Security Leftovers

By *Roy Schestowitz*
Created *10/10/2015 - 4:10pm*
Submitted by Roy Schestowitz on Saturday 10th of October 2015 04:10:27 PM Filed under Security [1]

- **Tor browser co-creator: Experian breach shows encryption may not be security panacea [2]**

  The Experian/T-Mobile hack may be more worrisome than Experian?s carefully worded description of it suggests, some security experts said Friday.

  One is the co-creator of the Tor secure browser, David Goldschlag, (now SVP of strategy at Pulse Secure). Goldschlag previously was head of mobile at McAfee, and also once worked at the NSA.

  I asked Goldschlag a simple question: ?After the Office of Personnel Management and Experian hacks, is there reason to fear that hackers now have the means to steal actual financial information (credit card numbers, etc.) from banks or insurers??

- **AV-TEST tests Linux security solutions against Linux and Windows threats [3]**

  To do so, it is often sufficient to copy files from a Linux environment to Windows.? it further adds. The most obvious mode of attack involves luring victims to install software or updates via third-party package sources. The team conducted test by running 16 different Anti-virus solutions and splitting test session into three distinct phases,

  The detection of Windows malware
  The detection of Linux malware and
  The test for false positives.

  Out of 16 antivirus solutions 8 detected between 95-99% of the 12,000 Windows threat used in the test: The Anti-virus solutions that helped in detection include Bitdefender, ESET, Avast, F-Secure, eScan, G Data, Sophos and Kaspersky Lab (server version).

- **Outlook.com had classic security blunder in authentication engine** [4]

  The cross-site request forgery vulnerability means that any user visiting a malicious page can have their accounts hijacked without further interaction.

  The since-patched hole existed in Microsoft Live.com and could have been spun into a dangerous worm, Wineberg says.

- **Meet the White Team, Makers of the Linux.Wifatch Viligante Malware** [5]

  However, Softpedia News noted that the Linux.Wifatch source code has not been released in its entirety. That?s likely because the White Team is worried that traditional cybercriminals would exploit the malware for more nefarious purposes. It also explains why it was a clandestine operation in which router owners weren?t aware their systems had been infected, even if it was only to defend them against black-hat attackers.

  Whether or not anyone appreciates the White Team?s form of vigilante security tactics, they may believe the work should serve as a warning to those who don?t follow basic data protection procedures, Hacked said. For example, there are still untold numbers of home routers that use default passwords and leave admin access wide open to malware and other threats.

- **Practical SHA-1 Collision Months, Not Years, Away** [6]

- **Search engine can find the VPN that NUCLEAR PLANT boss DIDN'T KNOW was there - report** [7]

  The nuclear industry is ignorant of its cybersecurity shortcomings, claimed a report released today, and despite understanding the consequences of an interruption to power generation and the related issues, cyber efforts to prevent such incidents are lacking.

  The report adds that search engines can "readily identify critical infrastructure components with" VPNs, some of which are power plants. It also adds that facility operators are "sometimes unaware of" them.

  Nuclear plants don't understand their cyber vulnerability, stated the Chatham House report, which found industrial, cultural and technical challenges affecting facilities worldwide. It specifically pointed to a "lack of executive-level awareness".

Security

Source URL: http://www.tuxmachines.org/node/80912

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://venturebeat.com/2015/10/03/tor-browser-co-creator-experian-breach-shows-encryption-may-not-be-security-panacea/
[3] http://news.thewindowsclub.com/av-test-tests-linux-security-solutions-linux-windows-threats-80379/
[4] http://www.theregister.co.uk/2015/10/09/hotmail_hijack_hole_earns_boffin_25k_double_bug_bounty_trouble/
[5] https://securityintelligence.com/news/meet-the-white-team-makers-of-the-linux-wifatch-viligante-malware/
[6] https://threatpost.com/practical-sha-1-collision-months-not-years-away/114979/
[7] http://www.theregister.co.uk/2015/10/05/nuclear_plants_cyber_denial_man_in_the_middle/