Security: Windows Back Doors, China Plans to Create a Technology Security Management System and More

By *Roy Schestowitz*
Created *09/06/2019 - 8:45pm*
Submitted by Roy Schestowitz on Sunday 9th of June 2019 08:45:21 PM Filed under Security [1]

- **Report: No ?Eternal Blue? Exploit Found in Baltimore City Ransomware [2]**

  > But according to Joe Stewart, a seasoned malware analyst now consulting with security firm Armor, the malicious software used in the Baltimore attack does not contain any Eternal Blue exploit code. Stewart said he obtained a sample of the malware that he was able to confirm was connected to the Baltimore incident.

- **China Plans to Create a Technology Security Management System [3]**

  > The National Development and Reform Commission has been tasked with setting up the list system which aims to ?more effectively forestall and defuse national security risks,? Xinhua reported on Saturday. Details on the measures will be provided in the near future, according to the news agency.

- **BGP event sends European mobile traffic through China Telecom for 2 hours [4]**

  > The incident started around 9:43am UTC on Thursday (2:43am California time). That's when AS21217, the autonomous system belonging to Switzerland-based data center colocation company Safe Host, improperly updated its routers to advertise it was the proper path to reach what eventually would become more than 70,000 Internet routes comprising an estimated 368 million IP addresses. China Telecom's AS4134, which struck a network peering arrangement

with Safe Host in 2017, almost immediately echoed those routes rather than dropping them, as proper BGP filtering practices dictate. In short order, a large number of big networks that connect to China Telecom began following the route.

The result: much of the traffic destined for telecommunications providers using the affected IP addresses passed through China Telecom equipment before either being sent to their final stop or being dropped during long waits caused by the roundabout paths. [...]

- **Fortune 500 company Tech Data leaks 264GB of private data [5]**

  While the card numbers were obfuscated, the data wasn't encrypted, and it's possible there's more than this: going through an entire 264GB file is somewhat time-consuming, after all. The site did say the sample its reporters saw contained "tens of thousands of customers," and it was a fraction of the larger database.

  This data was kept on a server for support agents to look at for troubleshooting purposes, but the company had neglected to put a password on it - meaning anybody with access to a web browser could look at the logs at will.

- **An Open Source Program Aims to Help Idaho Shore Up Cyberdefenses [6]**

  The mitigation of phishing is a top priority for Idaho, said ITS Administrator Jeff Weak. Phishing is the practice of sending emails that appear to be from a reputable source but hide malware links or try to convince users to reveal personal or system information.

  ?Phishing, in general, that?s our biggest threat because we can stop a lot of the payload of most malware coming through. We have multiple layers of detection going through our email system so it will strip out virtually anything that looks out of place,? Weak said. ?Where that gets tricky is in hyperlinks and things of that nature that look natural to an email or if it?s embedded into another link inside of a Word document, for example.?

  Idaho is currently in its second year of mandated cybersecurity training for state employees, he said. The learning modules, provided by KnowBe4, include a phishing course. One goal is to educate personnel on differentiating emails that make it past current cyberdefenses and into their inboxes.

- **Malicious Actors Create ?Frankenstein Monsters? by Combining Open Source Components [7] [Ed: TechNadu has somehow managed to blame security issues in Windows (which is insecure by design) on "open source"; amazing spin]**

  Examples of these open source and freely available components include a tool that leverages

MSBuild to execute a PowerShell command, another GitHub hosted project called Fruityc2 that is used to build stagers, the ?PowerShell Empire?, and an article to help the attackers detect whether their software is running in a virtual machine or not. The reason for using open source tools is not only because they are free and readily available, but also because they feature higher operational security and make the malicious activities and the group behind them harder to detect. Custom tools on the other side leave unique traces, as they are developed by specific groups of hackers.

- **Checkmarx Makes SCA Market Waves with Enhanced Open Source Security Offering [8]**

Security

Source URL: http://www.tuxmachines.org/node/124695

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/
[3] https://www.bloomberg.com/news/articles/2019-06-08/china-to-limit-some-tech-exports-global-times-editor-hu-says
[4] https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/
[5] https://www.theinquirer.net/inquirer/news/3077063/tech-data-breach
[6] https://www.govtech.com/security/An-Open-Source-Program-Aims-to-Help-Idaho-Shore-Up-Cyberdefenses.html
[7] https://www.technadu.com/malicious-actors-frankenstein-monsters-combining-open-source-components/69598/
[8] https://www.businesswire.com/news/home/20190604005174/en/Checkmarx-SCA-Market-Waves-Enhanced-Open-Source