Proprietary Software Leftovers

By *Roy Schestowitz*
Created *29/08/2019 - 9:31am*
Submitted by Roy Schestowitz on Thursday 29th of August 2019 09:31:56 AM Filed under Microsoft [1] Software [2] Mac [3] Security [4]

- **BuyDRM launches Linux support for DRM [5]**

  BuyDRM has announced Linux support for its MultiKey Server, a multi-DRM software platform specifically designed for deployments in remote or limited connectivity environments.

- **Some airlines are banning Apple?s MacBook Pros even if they weren?t recalled [6]**

  In June, Apple recalled the 2015 MacBook Pro with Retina Display, sold between September 2015 and February 2017, because the battery ?may pose a fire safety risk,? and the FAA soon reminded airlines not to carry those laptops with defective batteries on board. But some airlines are now banning Apple laptops whether they?ve got a bad battery or not, as reported by Bloomberg.

- **More Airlines Ban MacBook Pros in Checked Luggage [7]**

  All 15-inch versions of Apple Inc.?s MacBook Pro must be carried in the cabin and switched off, Qantas said in a statement Wednesday. The rule went into effect Tuesday morning. Rival Virgin Australia Holdings Ltd. went further on Aug. 26, banning all Apple laptops from checked-in luggage.

- **Popular PDF app was quietly plonking malware onto Android phones [8]**

  The security smart folks note that the app itself doesn't appear to be a malicious one, but rather it contains a trojan that gathers spyware and other malware from a malicious server and then runs in on a victim's phone. This trojan, dubbed Necro.n appears to have been sneaked into the app through the use of a legit-looking advertising library package.

  As such, the developers of the app, which has received some 100 million downloads, might not even realise their software is causing their users a malware headache.

- **[Cracker] Claims He Can ?Turn Off 25,000 Cars? At The Push Of A Button [9]**

  Your car?s immobilizer is supposed to be used for good. If a crook steals your car, it's possible for you to connect to the immobilizer, which tracks the vehicle and allows you to stop anyone from turning on the engine. But with one particular immobilizer - the U.K.-made SmarTrack tool from Global Telemetrics - an easy-to-hack vulnerability meant it was simple for researchers at Pen Test Partners to turn on the immobilizer permanently, without the customer knowing a thing.

  To prove it was possible, the researchers from British cybersecurity company Pen Test Partners hacked the vehicle of one of their own employees, disabling his car whilst they were in the U.K. and he was in Greece, not long before he was due to head to a wedding.

- **French cyberpolice, Avast and FBI neutralise global 'botnet' [10] [iophk: Windows TCO]**

  French police have neutralised a [cracking] operation that had taken control of more than 850,000 computers, mainly in Latin America, while also managing to remove the malware from the infected devices.

  The agents went into action last spring after the Czech antivirus firm Avast alerted them to the software worm, called Retadup, that was being controlled by a server in the Paris region.

- **Putting an end to Retadup: A malicious worm that infected hundreds of thousands [11] [iophk: Windows TCO]**

  Retadup is a malicious worm affecting Windows machines throughout Latin America. Its objective is to achieve persistence on its victims? computers, to spread itself far and wide and to install additional malware payloads on infected machines. In the vast majority of cases, the installed payload is a piece of malware mining cryptocurrency on the malware authors? behalf. However, in some cases, we have also observed Retadup distributing the Stop ransomware and the Arkei password stealer.

- **Authorities free 850,000 machines from grasp of Retadup worm [12] [iophk: Windows TCO]**

  After gaining persistence, Retadup goes on to distribute secondary malware on infected machines. It most commonly delivers a Monero cryptomining program, but also has been observed spreading over malware programs including Stop ransomware and the Arkei password stealer, Avast reports.

  The vast majority of Retadup victims whose infections were neutralized in last month?s crackdown are based in Latin American countries. However, the law enforcement operation itself specifically targeted C2 infrastructure based in France and the U.S.

- **Report finds majority of 2019 ransomware attacks have targeted state and local governments [13] [iophk: Windows TCO]**

  The majority of ransomware attacks in the U.S. in 2019 have targeted state and local governments, a report published Wednesday by cybersecurity group Barracuda Networks found.

  The report counted a total of 55 ransomware attacks on U.S. state and local government entities between January and July of 2019. These attacks involve a malicious actor or group encrypting a network and asking for money, often in the form of bitcoin, to allow the user access.

- **Threat Spotlight: Government Ransomware Attacks [14] [iophk: this is disinformation which fails to steer potential victims away from Windows and towards GNU/Linux or one of the BSDs]**

  Barracuda researchers have identified more than 50 cities and towns attacked so far this year. The team?s recent analysis of hundreds of attacks across a broad set of targets revealed that government organizations are the intended victims of nearly two-thirds of all ransomware attacks. Local, county, and state governments have all been targets, including schools, libraries, courts, and other entities.

Here?s a closer look at state and local government ransomware attacks and solutions to help detect, block, and recover from them.

Microsoft Software Mac Security

Source URL: http://www.tuxmachines.org/node/127503

Links:
[1] http://www.tuxmachines.org/taxonomy/term/62
[2] http://www.tuxmachines.org/taxonomy/term/38
[3] http://www.tuxmachines.org/taxonomy/term/97
[4] http://www.tuxmachines.org/taxonomy/term/59
[5] https://www.rapidtvnews.com/2019082957132/buydrm-launches-linux-support-for-drm.html
[6] https://www.theverge.com/2019/8/28/20837532/apple-macbook-pro-recall-battery-airplane-airline-quantas-virgin-australia-checked-baggage
[7] https://www.bloomberg.com/news/articles/2019-08-28/apple-laptop-flight-restrictions-spread-as-qantas-imposes-limits
[8] https://www.theinquirer.net/inquirer/news/3080919/camscanner-pdf-android-malware
[9] https://www.forbes.com/sites/thomasbrewster/2019/08/25/hacker-claims-he-can-immobilize-25000-cars-at-the-push-of-a-button/
[10] https://www.france24.com/en/20190828-french-cyberpolice-fbi-avast-neutralize-global-botnet
[11] https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/
[12] https://www.scmagazine.com/home/security-news/authorities-free-850000-machines-from-grasp-of-retadup-worm/
[13] https://thehill.com/policy/cybersecurity/459049-report-finds-majority-of-2019-ransomware-attacks-have-targeted-state-and
[14] https://blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/