Security: SKS, YouTube, Malware and More

By *Roy Schestowitz*
Created *04/07/2019 - 3:42pm*
Submitted by Roy Schestowitz on Thursday 4th of July 2019 03:42:29 PM Filed under Security [1]

- **Impact of SKS keyserver poisoning on Gentoo [2]**

  The SKS keyserver network has been a victim of certificate poisoning attack lately. The OpenPGP verification used for repository syncing is protected against the attack. However, our users can be affected when using GnuPG directly. In this post, we would like to shortly summarize what the attack is, what we did to protect Gentoo against it and what can you do to protect your system.

  The certificate poisoning attack abuses three facts: that OpenPGP keys can contain unlimited number of signatures, that anyone can append signatures to any key and that there is no way to distinguish a legitimate signature from garbage. The attackers are appending a large number of garbage signatures to keys stored on SKS keyservers, causing them to become very large and cause severe performance issues in GnuPG clients that fetch them.

  The attackers have poisoned the keys of a few high ranking OpenPGP people on the SKS keyservers, including one Gentoo developer. Furthermore, the current expectation is that the problem won?t be fixed any time soon, so it seems plausible that more keys may be affected in the future. We recommend users not to fetch or refresh keys from SKS keyserver network (this includes aliases such as keys.gnupg.net) for the time being. GnuPG upstream is already working on client-side countermeasures and they can be expected to enter Gentoo as soon as they are released.

- **YouTube's latest ban? Infosec instructional videos are outlawed [3]**

  Google's video-sharing site YouTube has started to ban videos that show users how to get past software restrictions and provide instructions on information security.

- **Youtube's ban on "hacking techniques" threatens to shut down all of infosec Youtube [4]**

  Youtube banning security disclosures doesn't make products more secure, nor will it prevent attackers from exploiting defects -- but it will mean that users will be the last to know that they've been trusting the wrong companies, and that developers will keep on making the same stupid mistakes...forever.

- **TN men use Bluetooth-enabled tablet to steal cars [5]**

  During the interrogation, one of the accused ?a car mechanic- said he bought a Bluetooth-enabled tablet online used by car showroom staff to access the vehicles.

- **Kaspersky reinforce collaboration with INTERPOL in the fight against cybercrime [6]**

  This cooperation strengthens the existing relationship between the two organizations, ensuring information and technology sharing can support INTERPOL in cybercrime-related investigations. Within the new agreement, Kaspersky will share information about its cyberthreat research and provide the necessary tools to assist with full digital forensics, aimed at strengthening efforts on the prevention of cyberattacks.

- **China Is Forcing Tourists to Install Text-Stealing Malware at its Border [7]**

  The malware downloads a tourist?s text messages, calendar entries, and phone logs, as well as scans the device for over 70,000 different files.

- **Chinese border guards reportedly install spy apps on tourists' Android phones [8]**

  Border guards reportedly took tourists' phones and secretly installed an app on them which could extract emails, texts and contacts, along with information about the handset; basically a mother-load of privacy-sapping stuff.

  There are reports that in some cases Android phones are returned to those entering the region with an app called F?ng c?i installed. Apple's iPhones don't appear to come back with the app, but they could have been scanned by border control guards in a separate area after travellers were forced to hand them over.

- **China Snares Tourists? Phones in Surveillance Dragnet by Adding Secret App [9]**

  The app gathers personal data from phones, including text messages and contacts. It also checks whether devices are carrying pictures, videos, documents and audio files that match any of more than 73,000 items included on a list stored within the app?s code.

Security

Source URL: http://www.tuxmachines.org/node/125534

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.gentoo.org/news/2019/07/03/sks-key-poisoning.html
[3] https://www.itwire.com/security/youtube-s-latest-ban-infosec-instructional-videos-are-outlawed.html
[4] https://boingboing.net/2019/07/03/nobus-r-us.html
[5] https://www.deccanherald.com/city/bengaluru-crime/tn-men-use-bluetooth-enabled-tablet-to-steal-cars-744639.html
[6] https://www.deccanchronicle.com/technology/in-other-news/030719/kaspersky-reinforce-collaboration-with-interpol-in-the-fight-against-c.html
[7] https://www.vice.com/en_us/article/7xgame/at-chinese-border-tourists-forced-to-install-a-text-stealing-piece-of-malware
[8] https://www.theinquirer.net/inquirer/news/3078354/chinese-border-surveillance-android-phones
[9] https://www.nytimes.com/2019/07/02/technology/china-xinjiang-app.html