GovCERT.HK

Weekly IT Security News Bulletin, 2017-W52

25 December – 31 December 2017

Headlines

Loapi Trojan - a Swiss Army knife for Android attackers

- An Android Trojan called Loapi was found being capable of performing various malicious activities, including disseminating advertisements, launching distributed denial-of-service (DDoS) attacks and mining cryptocurrencies. The malware is distributed via advertising campaigns where users are redirected to attackers' websites to download malicious files disguised as antivirus solutions or adult content apps.

- After installing the malicious app, users are asked to grant device administrator permissions to the app in a loop, which will not exit until users give the rights. The malware also checks if the device is rooted for future use of the root privileges. Any attempts to revoke the granted permissions by users will trigger the app to lock the screen, close the window with device manager settings, and prompt the threatening message: "Phone data will (be) wiped. Are you sure?"

- Loapi adopts a modular architecture which makes it multifunctional. Its central command and control server instructs the list of modules to be downloaded and launched and the domains where the modules can be got. The known available modules include the advertisement module, SMS module, web crawling module, proxy module (for DDoS attacks), and the module for mining Monero cryptocurrency.

Advice

- Download and install mobile apps only from official app stores and grant only necessary permissions to the apps.

- Install and run update anti-malware software on your Android device.

- Back up your phone data regularly.

- Do not root your mobile device to undermine its access control, which may allow malware to do more harm.

Sources

- Kaspersky
- Malwarebytes

Browser login managers exploited by web trackers

- Princeton University's Center for Information Technology Policy discovered that 1,110 of the world's top 1 million popular websites were embedded with web tracking scripts capturing visitors' email addresses by exploiting a long-known vulnerability in browsers' built-in login managers.

- The login manager, also known as password manager, saves and automatically fills in username and password at the login form of web applications. The form auto-filling can take place without user interaction and even visibility of the form at most major browsers. Such vulnerability enables a website script to retrieve the saved credentials without user awareness by injecting an invisible login form with the username and password fields, which will trigger the auto-filling.

- The university research team found that the web tracking scripts extract the email address from the username field, create a hash and tie the hash with the site visitor's advertising profile, reflecting a privacy threat in addition to a security vulnerability. The team advises web publishers to isolate login forms on a separate subdomain to prevent form auto-filling on non-login pages. Users are advised to install ad blockers or tracking protection extensions against tracking by invasive third-party scripts. For browser vendors, users should be allowed to disable the auto-filling.

Advice

- Website owners are advised to isolate login forms on a separate subdomain to avoid cross-site scripting attacks to steal the form information.

- Users should not save their credentials at the browser and should disable form auto-filling if the browser allows.

- Users may install ad blockers or tracking protection extensions for better privacy protection.

Sources

- Freedom to Tinker
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. Debian

https://www.debian.org/security/2017/dsa-4073
https://www.debian.org/security/2017/dsa-4074

2. F5 Traffix SDC

https://support.f5.com/csp/article/K73337338

3. Huawei Products

http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171222-01-cryptography-en
http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171222-01-windows-en
http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171227-01-h323-en

4. IBM Products

https://www.ibm.com/blogs/psirt/ibm-security-bulletin-6/
https://www-01.ibm.com/support/docview.wss?uid=swg22009537

5. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2017-12/msg00087.html
https://lists.opensuse.org/opensuse-security-announce/2017-12/msg00090.html

6. SUSE

https://www.suse.com/support/update/announcement/2017/suse-su-20173411-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20173428-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20173435-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20173436-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20173440-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20173441-1/

Sources of product vulnerability information:

Debian
F5
Huawei
IBM
openSUSE
SUSE

Contacts:

cert@govcert.gov.hk