certin
Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0079

Mobile Ransomware

Original Issue Date: December 15, 2016

Description

Ransomware has been in the news repeatedly over the past few years. Mobile ransomware is a form of malware that locks your computer or mobile device, encrypts your files and holding them ransom until you pay a fee to the cybercriminals who hold them hostage. People are tricked into accidentally downloading the malware through social networking schemes, assuming that they are downloading innocent content or critical services. Simplocker, Svpeng, Pletor, Stampado, Fusob, CryptoWall and TeslaCrypt are some examples of mobile ransomeware.

Once downloaded, ransomware displays a screen-wide message that demands money from you to release the device. After the payment is processed, often via Bitcoin, the ransomware will send you an unlock code or decrypt the data. Mobile devices are now more integrated into our day-to-day lives than our PCs, a ransomware attack can have a tremendous impact on us.

How mobile ransomware is distributed?

Mobile ransomware masquerades as a legitimate app in third party app stores, popular games, flash and video players or as a system update. One could also get hit with an attack by visiting pornographic websites, forums or clicking on a spam link in text messages.

How mobile ransomware works?

Once the malware is on the device, it contacts a server, which generates an encryption key unique to that device. The decryption key is stored on the attacker's server, and the victim gets the key only if they pay up. In a less sophisticated attack, there's an encryption key for the entire campaign, not for each device, in such a case, a security company may be able to crack the encryption.

What to do when your phone is infected with ransomware?

If you've already been infected, don't panic and don't pay the hacker. You can download ransomware Removal and other apps to remove ransomware Trojan viruses and unlock encrypted data. Paying the ransom gives you no guarantee that the online criminals at the other end of the transfer will give you the decryption key. And even if they do, you would be further funding their attacks and fuelling the never ending malicious cycle of cyber crime.

A factory reset the device may remove the trojan app. Unfortunately a factory reset results in all data on the device being erased. Since you won't be able to get into the settings, you'll need to initiate a factory reset a little differently depending on the phone manufacturer.

Sometimes it may not be possible to factory reset the device because the trojan app prevented them from doing so. In this case, you can try to reboot your device into safe mode. Once you're in safe mode, open the Application Manager and look for any app under the Downloaded tab that you don't recognize and delete it. Once you're all set, just turn off the phone or tablet as you normally do and turn it on to reboot it in its normal state. Hopefully the trojan app will be gone and your phone will be unlocked. You can always repeat the process and try again.

How to stay protected against mobile ransomware?

Users should take the following preventive measures:

- Back up data frequently through the backup software provided by the phone manufacturer.
- Keep the data backup disconnected from mobile devices. If you do get infected, you can easily wipe your mobile phone and restore it to remove any ransomware.
- Do not root/ jailbreak your device to override usage and/or access limitations.
- Install apps from Official App Stores only, i.e., Google Play/ Apple App/ Microsoft/ BlackBerry World etc.
- Do not install the app if suspicious permission rights are required. Many apps that while not technically malicious, do disclose far too much personal information without a legitimate reason.
- Disable "installation of apps from unknown sources" feature on Android devices.
- Enable the "Verify apps" features to check apps when you install them and periodically scan for potentially harmful apps on Android.
- Install anti-malware app.
- Install the latest patches for apps and operating system in use.
- Check and keep your anti-malware app and signatures are up-to-date to protect against new threats or older threats that haven't yet been fixed by OS or application updates.
- Enable "Safe Browsing" in Chrome/ "Fraudulent Website Warning" in Safari/ "SmartScreen" features in Internet Explorer to avoid visit known phishing and malicious sites.
- Enable blocking of pop-ups.
- Do not open any suspicious emails and its attachments.
- Do not click URL links or open attachments in SMS, MMS, instant messages, or emails from untrusted or suspicious origin.
- Refrain from visiting suspicious websites or downloading any files from them.

References

CIAD-2016-0061: Prevention of Ransomeware Infections
http://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0061

Avast
https://blog.avast.com/the-evolution-of-mobile-ransomware

Kaspersky
https://blog.kaspersky.com/mobile-ransomware-2016/12491/

Heimdal Security
https://heimdalsecurity.com/blog/ransomware-decryption-tools/

Digital Trends
http://www.digitaltrends.com/mobile/android-cyber-police-ransomware-news/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India