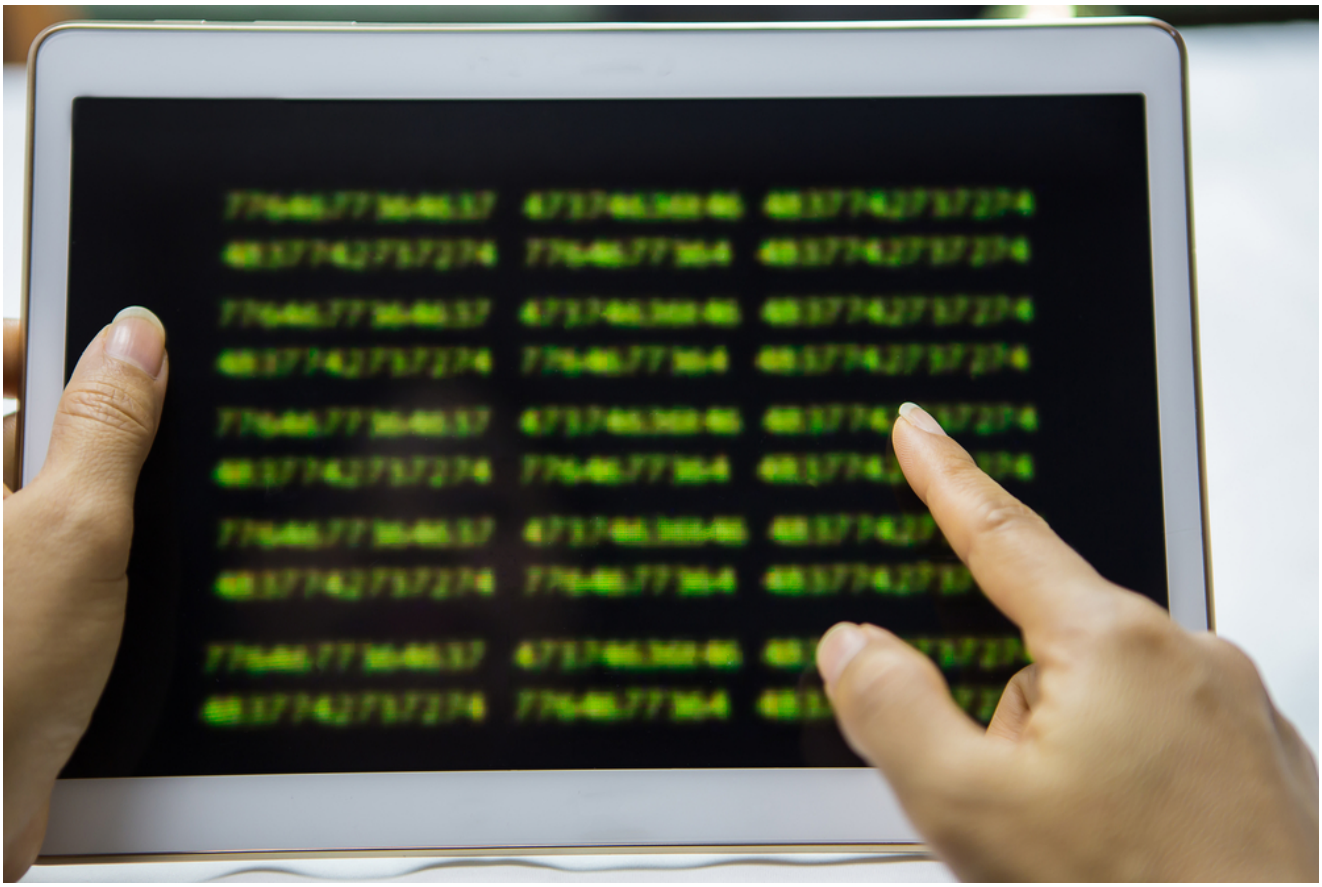
DoubleLocker: Innovative Android Ransomware

welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/

October 13, 2017



DoubleLocker can change the device's PIN, preventing victims from accessing their devices, and also encrypts the data it finds in them - a combination that has not been seen previously in the Android ecosystem.

ESET Research

13 Oct 2017 - 10:55AM

DoubleLocker can change the device's PIN, preventing victims from accessing their devices, and also encrypts the data it finds in them – a combination that has not been seen previously in the Android ecosystem.

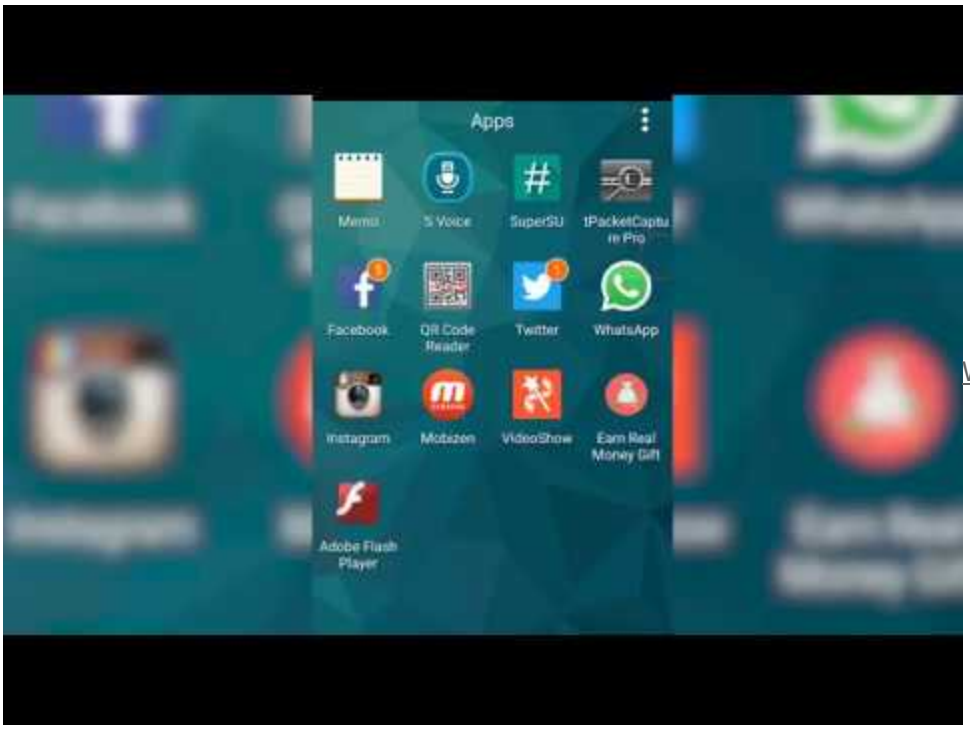
ESET researchers have spotted the first-ever ransomware misusing Android accessibility services. On top of encrypting data, it also locks the device.

Detected by ESET products as Android/DoubleLocker.A, the ransomware is based on the foundations of a particular banking Trojan, known for misusing accessibility services of the Android operating system. However, DoubleLocker doesn't have the functions related to harvesting users' banking credentials and wiping out their accounts. Instead, it has received two powerful tools for extorting money from its victims.

DoubleLocker can change the device's PIN, preventing victims from accessing their devices, and also encrypts the data it finds in them – a combination that has not been seen previously in the Android ecosystem.

"Given its banking malware roots, DoubleLocker may well be turned into what could be called ransom-bankers. Two-stage malware that first tries to wipe your bank or PayPal account and subsequently locks your device and data to request a ransom… Speculation aside, we spotted a test version of such a ransom-banker in the wild as long ago as May, 2017," comments Lukáš Štefanko, the ESET malware researcher who discovered DoubleLocker.

Distribution



Watch Video At:

https://youtu.be/odSWGPLEqt0

DoubleLocker spreads in the very same way as its banking parent does. It is distributed mostly as a fake Adobe Flash Player through compromised websites.

Once launched, the app requests activation of the malware's accessibility service, named "Google Play Service". After the malware obtains the accessibility permissions, it uses them to activate device administrator rights and set itself as the default Home application, in both cases without the user's consent.

"Setting itself as a default home app – a launcher – is a trick that improves the malware's persistence. Whenever the user clicks on the home button, the ransomware gets activated and the device gets locked again. Thanks to using the accessibility service, the user doesn't know that they launch malware by hitting Home," explains Štefanko.

Locking both device and data

DoubleLocker, once executed on the device, creates two reasons for the victims to pay.

First, it changes the device's PIN, effectively blocking the victim from using it. The new PIN is set to a random value which the attackes neither store nor send anywhere, so it's impossible for the user or a security expert to recover it. After the ransom is paid, the attacker can remotely reset the PIN and unlock the device.

Second, DoubleLocker encrypts all files from the device's primary storage directory. It utilizes the AES encryption algorithm, appending the extension ".cryeye". "The encryption is implemented properly, which means that, unfortunately, there is no way to recover the files without receiving the encryption key from the attackers," says Štefanko.

The ransom has been set to 0.0130 BTC (approximately USD 54 at time of writing) and the message highlights that it must be paid within 24 hours. However, if the ransom is not paid, the data will remain encrypted and will not be deleted.

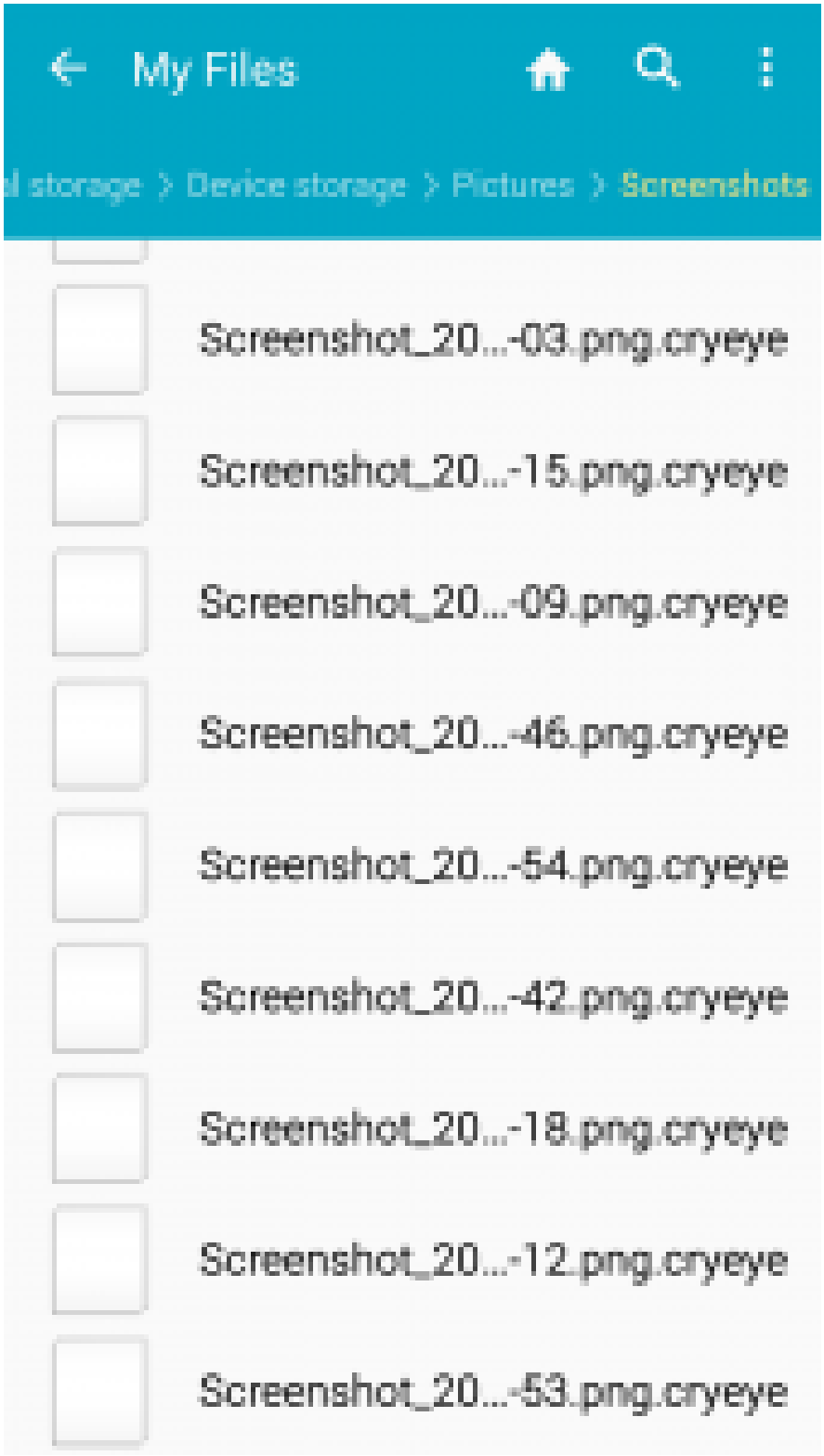


Figure 1: Encrypted files on a device compromised by with DoubleLocker

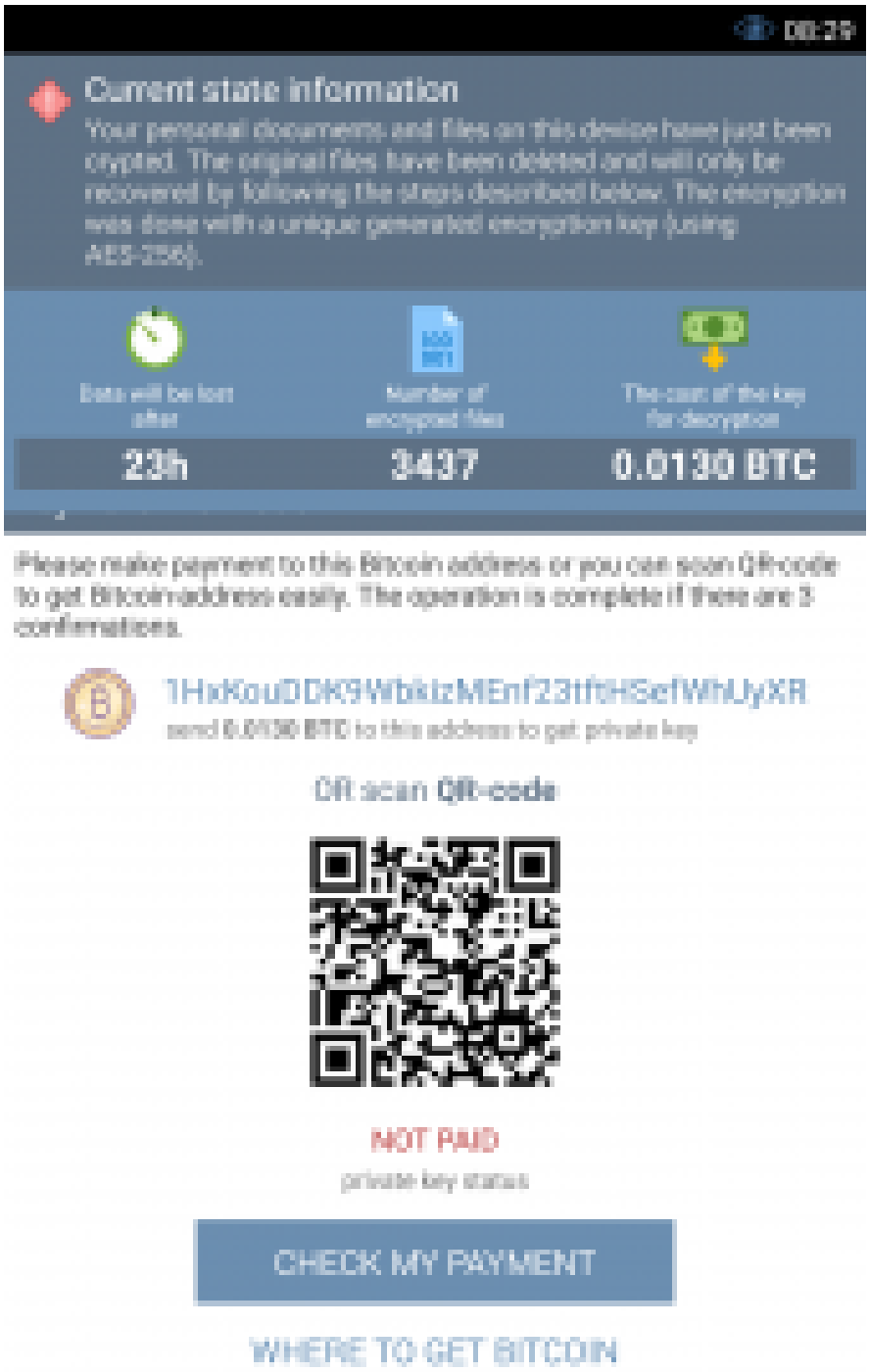


Figure 2: A part of the DoubleLocker ransom message

How to get rid of it?

In the ransom note, the user is warned against removing or otherwise blocking DoubleLocker: “Without [the software], you will never be able to get your original files back”.

To prevent unwanted removal of the “software”, the crooks even recommend disabling the user’s antivirus software.

“Such advice is irrelevant: all those with a quality security solution installed on their devices are safe from DoubleLocker,” explains Štefanko.

The only viable option to clean the device of the DoubleLocker ransomware is via a factory reset.

For rooted devices, however, there is a method to get past the PIN lock without a factory reset. For the method to work, the device needed to be in the debugging mode before the ransomware got activated.

If this condition is met, then the user can connect to the device by ADB and remove the system file where the PIN is stored by Android. This operation unlocks the screen so that the user can access their device. Then, working in safe mode, the user can deactivate device administrator rights for the malware and uninstall it. In some cases, a device reboot is needed.

As for the data stored on the device, there is no way to recover it, as mentioned earlier.

“DoubleLocker serves as just another reason for mobile users to have a quality security solution installed, and to back up their data on a regular basis,” concludes Štefanko.

Hash:

01d962f809ae061d1895cf71db9eeb07900929b8

13 Oct 2017 - 10:55AM