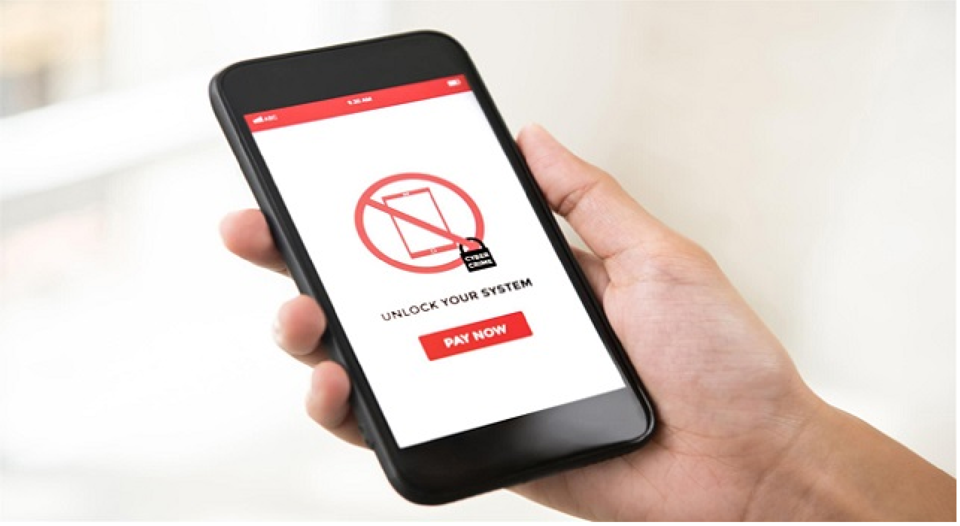
SLocker Mobile Ransomware Starts Mimicking WannaCry

blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/

July 5, 2017



Updated July 6 3:00 AM CDT to clarify statement about Slocker variant being notable as an Android file-encrypting ransomware.

Early last month, a new variant of mobile ransomware SLocker (detected by Trend Micro as ANDROIDOS_SLOCKER.OPST) was detected, copying the GUI of the now-infamous WannaCry. The SLocker family is one of the oldest mobile lock screen and file-encrypting ransomware and used to impersonate law enforcement agencies to convince victims to pay their ransom. After laying low for a few years, it had a sudden resurgence last May. This particular SLocker variant is notable for being an Android file-encrypting ransomware, and the first mobile ransomware to capitalize on the success of the previous WannaCry outbreak.

While this SLocker variant is notable for being able to encrypt files on mobile, it was quite short-lived. Shortly after details about the ransomware surfaced, decrypt tools were published. And before long, more variants were found. Five days after its initial detection, a suspect supposedly responsible for the ransomware was arrested by the Chinese police. Luckily, due to the limited transmission channels (it was spread mostly through forums like QQ groups and Bulletin Board Systems), the number of victims was very low.

Figure 1. Timeline for this ransomware sample

Figure 1. Timeline for this ransomware sample

The original sample captured by Trend Micro was named “王者荣耀辅助” (King of Glory Auxiliary), which was disguised as a cheating tool for the game King of Glory. When installed, it has a similar appearance to WannaCry, which has already inspired a few imitators.

Figure 2. The first mobile ransomware we’ve seen mimicking WannaCry

This ransomware disguises itself as game guides, video players, and so on in order to lure users into installing it. When installed for the first time, its icon looks like a normal game guide or cheating tool. Once the ransomware runs, the app will change the icon and name, along with the wallpaper of the infected device.

The ransomware announces a disabled activity alias for “com.android.tencent.zdevs.bah.MainActivity”. It then changes its icon by disabling the original activity and enabling the alias.

Figure 3. After running, the ransomware icon and name changes

Figure 3. After running, the ransomware icon and name changes

How the Ransomware Encrypts Files

When the ransomware is installed, it will check whether it has been run before. If it is not, it will generate a random number and store it in SharedPreferences, which is where persistent application data is saved. Then it will locate the device's external storage directory and start a new thread.

The thread will first go through the external storage directory to find files that meet specific requirements:

- The lowercase paths for target files must not contain "/.", "android", "com." and "miad".
- With the external storage as the root directory, target files should be in directories whose directory level is smaller than 3 or the lowercase file paths contain "baidunetdisk", "download" or "dcim".
- File name must contain "." and the byte length of the encrypted file name should be less than 251
- The file must be larger than 10 KB and smaller than 50 MB

We see that the ransomware avoids encrypting system files, focuses on downloaded files and pictures, and will only encrypt files that have suffixes (text files, pictures, videos). When a file that meets all the requirements is found, the thread will use ExecutorService (a way for Java to run asynchronous tasks) to run a new task.

Figure 4. Snippet showing the start of a new task

Figure 4. Snippet showing the start of a new task

The new task will use a method named "getsss" to generate a cipher based on the previously generated random number. This method computes the MD5 of the random number and selects 16 characters as a string from the hexadecimal representation of the MD5. After the string is generated, the ransomware will feed it to SecretKeySpec to construct the final key for AES before using AES to encrypt files.

*Figure 5. Snippet showing the "*getsss*" method*

Once the file has been encrypted, a suffix will be added to the file name. The suffix contains a QQ number and the random number used to generate the cipher.

Figure 6. Sample of encrypted file name

Figure 6. Sample of encrypted file name

The ransomware presents victims with three options to pay the ransom, but in the sample we analyzed, all three led to same QR code that asks the victims to pay via QQ (a popular Chinese mobile payment service). If victims refuse to pay after three days, then the ransom price will be raised. It threatens to delete all files after a week.

Figure 7. Payment options for the ransomware

Figure 7. Payment options for the ransomware

The ransomware tells victims that a decrypt key will be sent after the ransom has been paid. Through our analysis, we found that if victims input the key and click the Decrypt button, the ransomware will compare the key input with the value in MainActivity.m. But after tracking MainActivity.m, we found that the value is actually the previously mentioned random number plus 520.

Figure 8. Snippet showing the value is the random number plus 520

Figure 8. Snippet showing the value is the random number plus 520

Take the instance we are running as an example: the random number is 10049252. So the decrypting key should be 10049772 (10049252 + 520). Using that as the key and clicking on the Decrypt button will decrypt the files.

Figure 9. Decryption screen of mobile ransomware

Figure 9. Decryption screen of mobile ransomware

Numerous New Variants Emerge

After the initial ransomware was exposed, more and more variants appeared. While some variants changed the method for generating the decrypt key, the user can still decrypt the files if they figure out the new formula:

Figure 10. While the original used (random number + 520), these variations are similar but use other formulas

Some pack themselves to avoid static detection:

Solutions and Recommendations

Compared to the ransomware we’ve seen before, this ransomware is relatively simple. It is actually quite easy for a security engineer to reverse the ransomware and find a way to decrypt files. However, the proliferation of new variants so quickly after the first one shows that these malicious actors are not slowing down. Even though a suspect was caught, more advanced ransomware may be just around the corner.

To help you keep the information on your mobile device safe, here are some tips to protect you from ransomware:

- Only install apps downloaded from legitimate app stores such as Google Play
- Be careful about permissions an app asks for, especially permissions that allow the app to read/write on external storage
- Back up your data regularly—either on another secure device or on cloud storage
- Install comprehensive antivirus solutions. Mobile security solutions such as Trend Micro™ Mobile Security blocks threats from app stores before they can be installed and cause damage to devices, while Trend Micro™ Maximum Security offers in-depth protection for multiple devices and proactively secures them from the threat of ransomware.

Indicators of Compromise (IOCS)

SHA256	Package	Application Name
200d8f98c326fc65f3a11dc5ff1951051c12991cc0996273eeb9b71b27bc294d	com.android.tencent.zdevs.bah	王者荣耀辅助
2ffd539d462847bebcdff658a83f74ca7f039946bbc6c6247be2fc62dc0e4060	com.android.tencent.zdevs.bah	千变语音
36f40d5a11d886a2280c57859cd5f22de2d78c87dcdb52ea601089745eeee494	com.android.tencent.zdevs.bah	王者荣耀前瞻版
c347e09b1489c5b8061828526f4ce778fda8ef7fb835255914eb3c9268a265bf	com.android.tencent.zdevs.bah	千变语音秀
cb0a18bcc8a2c9a966d3f585771db8b2e627a7b4427a889191a93b3a1b261ba3	com.android.tencent.zdevs.bah	主流影视大全

Ransomware

A new variant of mobile ransomware SLocker was detected. It copies the GUI of the now-infamous WannaCry. It's one of the first Android file-encrypting ransomware, and the first mobile ransomware to capitalize on the success of the WannaCry outbreak.

By: Ford Quin July 05, 2017 Read time: (words)

Content added to Folio