CRIMSON PUBLISHERS
Wings to the Research

Forensic Science & Addiction Research

ISSN 2578-0042

Mini Review

Ransomware on Android devices

Monika Choudhary*, Pavol Zavarsky and Dale Lindskog

Department of Information System Security Management, Concordia University of Edmonton, Canada

***Corresponding author:** Monika Choudhary, Department of Information System Security Management, Concordia University of Edmonton, Edmonton, T5B 4E4, Canada

Submission: February 09, 2018; **Published:** February 16, 2018

Abstract

Ransomware is a form of malicious code or malware that infects a computer and spreads rapidly to encrypt the data or to lock the device. This malware makes the data inaccessible to the users and the attackers demand payment from the user in order to decrypt and make files accessible to the user. The payment is often requested in Bitcoin or other untraceable currency. Individuals both at work and at home are at risk of these and similar attacks by hackers. Ransomware is expected to expand more as a common threat and profitable business for attackers in future. Recent events show a huge rise in Android-based mobile ransomware attacks. Ransomware viruses now exploit using the names of authorities including the FBI, USA Cyber Crime Investigation agency, and The ICE Cyber Crime Center. These locker type of ransomware make fake claims by portraying themselves as these agencies and then, warns the device users to pay some amount of money as fine for violation of law.

Mini Review

Some of the famous malicious payloads used are

Privilege escalation: Once the whole application gets downloaded, then on opening the app it will ask for administrative rights. Now, if the user clicks on activate button, then the application takes the privileges of device administrator, and this makes difficult to remove the malicious application from the device. In the recent versions of ransomware attacks, the activation window is overlaid with a malicious window pretending to be an Update patch installation. So, somehow the application tries to obtain the administrator privileges in order to lock the victim's device or to set a new PIN for lock screen of the device.

Remote control: Earlier ransomware packages communicate with a website via HTTPS to get encryption keys. An application which tries to make a secure HTTP request to a suspicious target is a clear hint of malevolent purposes. Now, the new variants have started to use XMPP communication in order to communicate with command and control server. These communications look like normal instant message communications, which makes the ransomware more difficult to get detected with anti-malware software. XMPP communications channel is used by the new Simplocker variants. Its variant uses an external Android library to communicate with the command and control network through a legitimate messaging relay server. And these messages can be encrypted using Transport Layer Security (TLS). The messages were received from the command and control network by the operators of the scheme via Tor. All communications to C&C server are done through port numbers 443, 80 and 123.

Information collection: Few ransomware applications collect information like IMEI number, call logs, contacts, profile, history bookmarks, SMS, the list of accounts in account service, phone state, GPS location of phone, and IP address. Some of the ransomware even check the tasks running in the device. Simplocker family contacts Command and control server and sends the information found on the mobile device to the attacker.

Encryption used: Crypto ransomware like Simplocker and Pletor uses AES encryption scheme in order to encrypt the data present in SD card. It usually searches for particular type of files and then encrypts them.

Permissions used: All apps which are installed by users require some permissions to be granted so that they can function. But malicious applications ask for permissions which are not for the functioning of app for but the mischievous purposes. All the permission requests which don't seem to be in accordance with app services can be taken seriously and may not be granted. Highly malicious apps can ask for some more permissions which can be used for these malicious purposes. These kinds of permissions are being used by an attacker so that the removal of these applications gets more difficult. Table 1 below mentions the kind of permissions which make the ransomware much more malicious.

Table 1: Some common permissions ransomware seeks from users.

S. No.	Permission
1	KILL_BACKGROUND_PROCESSES
2	DISABLE_KEYGAURD
3	USES_POLICY_FORCE_LOCK
4	BIND_DEVICE_ADMIN
5	FACTORY_TEST

An app uses KILL_ BACKGROUND_PROCESSES to stop the antivirus processing running in order to prevent ransomware from detection. FACTORY_TEST is used to run an app as manufacturer test application using root user privileges. BIND_DEVICE_ADMIN ensures that only the system can interact with application. These kind of permissions makes it difficult removal the ransomware apps from Android devices.

Phases of Ransomware in Android

Whenever an android device is infected with ransomware, then first of all it will try to gain an administrative privilege by simply asking for it or by tricking the user for installing patch updates. After gaining administrative access, it will ask for some permissions, which are required by app in order to perform its necessary tasks. But, we have seen from our analysis that, an app asking for irrelevant permissions with respect to the nature of that app is always for malicious purposes. Once, the permissions has been granted to the app, it will start gathering personal information from victim's device and then it contacts command and control server. It will send this information to the attacker and these messages are usually encrypted with transport layer security (Figure 1).

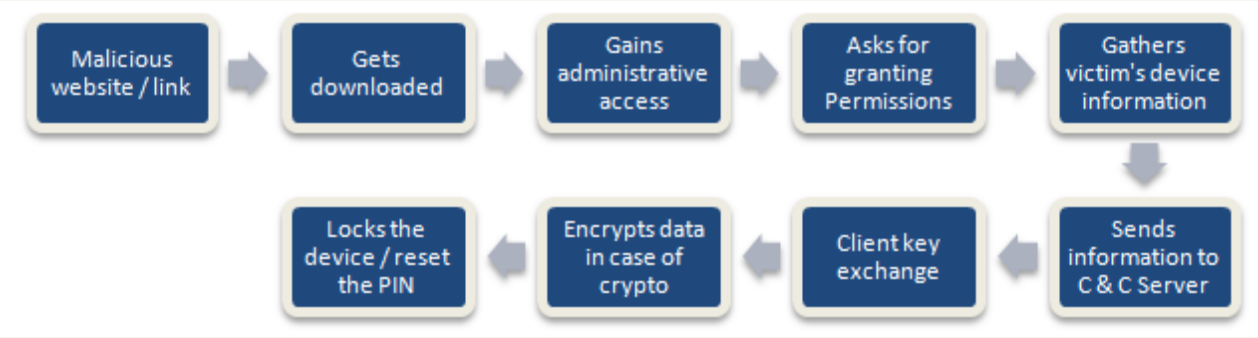

Figure 1: Life cycle of android ransomware.

It will obtain a private key from command and control server in case of crypto ransomware. Using this key it will encrypt the selected data present in Android device. After completing encryption, it will ask the user the victim to pay ransom by showing an alert. But in case of locker ransomware, it will reset the PIN of the Android device and then asks for ransom to restore access to the device.

Ransomware Detection

Packer detection

An algorithm may be developed to detect AndroidManifest.xml file before it being installed on the device of the user. Apktool is one such tool that can be used to extract AndroidManifest.xml and source code from the application.

Requested permissions

Checking permissions and do not granting permissions which looks suspicious for an application. Giving user an option to grant only necessary permissions for an application at the time of installation can solve many problems.

Conclusion

Recent ransomware attacks show that a significant number of ransomware families show similar characteristics. And by paying close attention to the Android Manifest file and ransomware permissions of an app can help a user in detecting underlying intentions of that app and save themselves from ransomware attack on their android devices.