itworldcanada.com

Understanding Android Malware Families: ransomware and scareware (Article 3) | IT World Canada Blog

Gurdip Kaur and Arash Habibi Lashkari

8-11 minutes

Ransomware is malicious software used by individuals to encrypt documents on computers or digital devices.

How they work

Perpetrators demand a ransom from the owner of a device to access the victim's documents; once in, criminals install ransomware on their mobile phone or computer. When the owner clicks on a malicious link in an email, text message or website, their document is automatically locked (otherwise known as a crypto locker).

In case you missed it:

Understanding Android Malware Families – the foundations (Article 1)

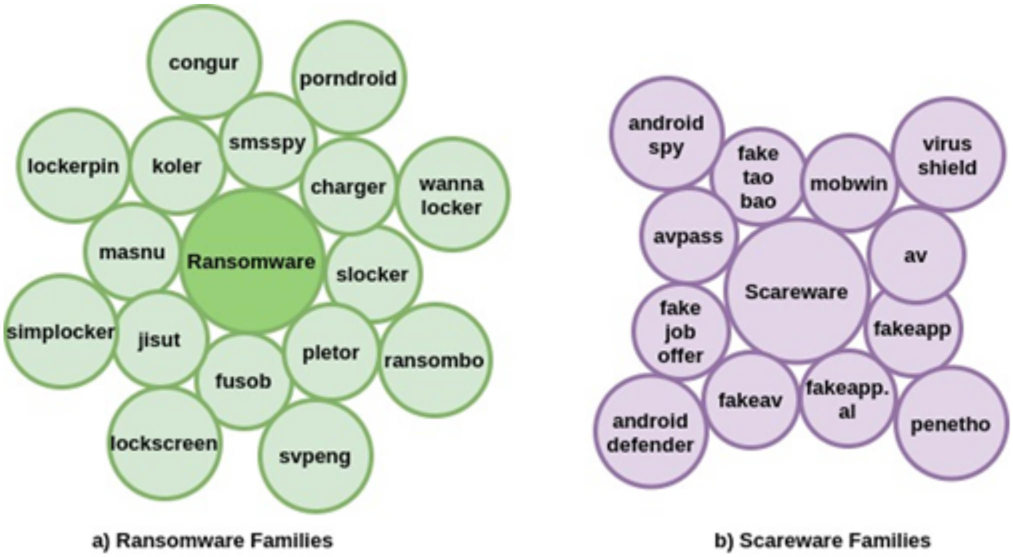
Understanding Android Malware Families – the trojan: an impersonator in the background (Article 2)

On the other hand, scareware is malicious software that criminals convince users to purchase or download. Bad actors coax victims into believing that they may harm their device if they don't download or buy malicious software. Scareware is often initiated through pop-up advertising and takes advantage of attackers' social engineering tactics to coax users into installing fake anti-virus software.

Here, we've analyzed and provided results for several ransomware and scareware families.

The malicious behaviour of ransomware and scareware families

Common ransomware activities include sending text messages, enabling GPS, browsing the Internet and clicking on compromised pop-up advertisements. Additionally, ransomware families can set a four-digit PIN to lock the smartphone, save images, documents, and videos in both the compromised device's external and internal storage. In the worst scenario, they can disable the SIM card on the victim's device.



a) Ransomware Families

b) Scareware Families

Ransomware vs Scareware

All the ransomware families collect sensitive data from mobile phones and interact with hardware settings to fetch which Android operating system version is installed on a device. All, except Fusob and Jisut browse the Internet to download malicious files on compromised devices. Additionally, Congur and SmsSpy family communicate via a command-and-control server.

Looking into scareware families, Avpass is the only family that interacts with anti-virus solutions installed on a device. All the scareware families browse the Internet to display pop-up advertisements and download fake software to victims' phones. Mobwin and FakeApp families collect sensitive information from the device and interact with hardware settings. Further, FakeApp communicates with remote command-and-control servers.

Both ransomware and scareware families perform some common activities: LockerPin (a ransomware family) bears a close resemblance to FakeTaoBao (a scareware family). PornDroid (a ransomware family) and FakeApp (a scareware family) also share similarities.

COVID-19 reshapes ransomware and scareware attack landscape

Ransomware attributed to 2.47 per cent of all Android malware attacks in 2019. Many targeted professional services, especially within the healthcare and the public sectors. Further, the number of ransom attacks continues to grow, especially during the pandemic, along with the prices demanded. According to Coveware, large company's payments grew significantly in 2020. Users also installed 20,708 new mobile ransomware Trojans last year.

Trends in ransom attacks during the pandemic

Attackers commonly circulate fake COVID tracking apps via hyperlinks within spam emails. After the fake app is downloaded, it installs malware to steal users' data and capture device information. Beyond fake apps, attackers use COVID-based themes to search people who infected with the virus. Victims are then coaxed to deposit a fee and provide their bank card details.

During the pandemic, ransomware grew 72 per cent, while mobile vulnerabilities grew by 50 per cent. At the beginning of May 2020, The Canadian Centre for Cyber Security in Ottawa took down over 1,500 COVID-19-themed fraudulent sites or email addresses aimed at Canadians since the start of the year. In August 2020, ransomware attackers targeted well-known Canadian real-estate companies, who stole personal HR, finance, and payroll information from the company's website and demanded an unspecified ransom. In one of the most popular WannaCry ransomware attacks in May 2017, over 200,000 computers were infected across 150 countries, resulting in financial damage in the millions.

Ransomware and scareware: an unholy marriage

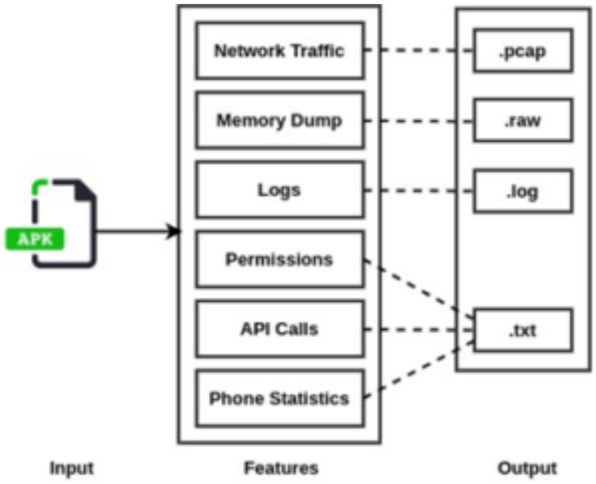
Scareware attacks are no less severe and predominant than ransomware attacks. In this case, criminals leverage people's fear of the pandemic to coax them into fake money-making ventures. As a result, panicky victims proved easy prey by sharing sensitive information.

With mobile ransomware schemes, bad actors send encrypted notes to users' mobile phones or tablets, notifying them that their device is locked and inaccessible, even if the user restarts it. Attackers typically exploit the "SYSTEM_ALERT_WINDOW" Android permission to display an overlay window on victims' mobile screens.

Scareware notifications try to convince people that their mobile device has been affected to encourage users to pay relatively steep fees for fake anti-virus solutions. Not surprisingly, these "anti-virus solutions" are only available to download from untrustworthy third-party app stores. Duped individuals provide their credit card, opening the door for attackers to steal their identity and carry out malicious activities; these include hijacking the victim's device and encrypting documents and personal data on the device.

Clearly, there's a close relationship between scareware and ransomware: Scammers use fake, downloaded anti-virus software to pave the way for the ransomware attack.

Technical features used to detect scareware and ransomware



In the *CCCS-CIC-AndMal-2020, CIC-InvesAndMal2019*, and *CIC-AndMal2017* datasets, the following features are extracted from APK files in the appropriate output format to detect ransomware and scareware malware families. Figure 2 summarizes the technical features extracted from input files and the output format used to store them.

1. *Network traffic:* Network traffic features describe the data transmitted and received between other devices in the network. It indicates foreground and background network usage. Network traffic features include the total number of packets sent and received; it is stored in .pcap files.
2. *Memory dump:* Memory dumps represent interactions of malware with memory. They can be in the form of fetching data from memory, storing data into memory, and using memory to execute some instructions while the malware is running in the background. Memory dumps also contain information related to shared memory pages between two different processes. It's stored in .raw files.
3. *Logs:* Log messages provide information about errors, warnings, and debugging data to analyze what activities took place on an Android device. (stored in .log files).
4. *Permissions:* This feature specifies the permissions used by the malware families. For example, ransomware displays a ransom alert by accessing SYSTEM_ALERT_WINDOW permission. (stored in .txt files).
5. *API calls:* Application Programming Interface (API) features delineate the communication between two applications. API calls extracted from the malware APKs include inter-process communication, device information, connection to a database,

accessing GPS, and sending text messages. (stored in .txt files).

6. *Phone statistics:* Phone statistics provide details about the amount of data used by various applications. In addition, battery statistics are also used because ransomware and scareware drain the battery faster, just like Android malware. (stored in .txt files).

How to protect your device

1. Avoid clicking on suspicious links in email, text messages and advertisements.
2. Do not install apps from third-party stores.
3. Never disclose personal information when purchasing something online from a source that you don’t trust.
4. Be cautious of messages or notifications on your device telling you to download software – It may be a scam.

Finally, how to remove ransomware from your phone

If the ransomware has encrypted the files on your device, it can’t be decrypted without a decryption key as it’s available only to the attacker. Nevertheless, if files are not encrypted but the device has been locked by ransomware, here are steps you can take to remove ransomware from your phone:

- Step 1: Reboot the phone in safe mode to remove locker malware. Safe mode prevents third-party apps from running. Assuming that the ransomware comes via a third-party source, it can’t execute.
- Step 2: After rebooting the device in safe mode, uninstall the suspicious locker ransomware app.

- Step 3: If these first two steps fail, perform a factory reset of the device that will delete all apps and data on the device.