itworldcanada.com

Understanding Android Malware Families: Adware and Backdoor (Article 5) | IT World Canada Blog

Gurdip Kaur and Arash Habibi Lashkari

7-9 minutes

It is interesting to mention that backdoors can be linked with adware. Attackers use advertisement malware to lure the users in the first step. Once the user clicks the advertisement, a backdoor is installed on his device in the second step. Figure 1 shows the timeline of famous adware and backdoor families captured and analyzed in our Android malware dataset, named CCCS-CIC-AndMal-2020, published by the Canadian Institute for Cybersecurity (CIC) in collaboration with Canadian Centre for Cyber Security (CCCS) in 2020.

It is interesting to mention that the dataset contains 48 adware and 11 backdoor families captured between 2007 and 2018. For simplicity, Figure 1 presents malware families between 2011 and 2018 only. Most of the adware samples available in the dataset are captured between 2014 and 2016. Further, shedun is the largest adware family in the dataset and contains 19,036 samples. It is followed by zdtad adware family with 5,694 samples.

Behaviour exhibited by adware and backdoor families

To understand the behaviour exhibited by adware and backdoor families, we divided the functions performed by these families into different categories and then identified what type of activities are performed by each malware family. To make it easy to read, Figure 2 presents the behaviour exhibited by adware and backdoor families.

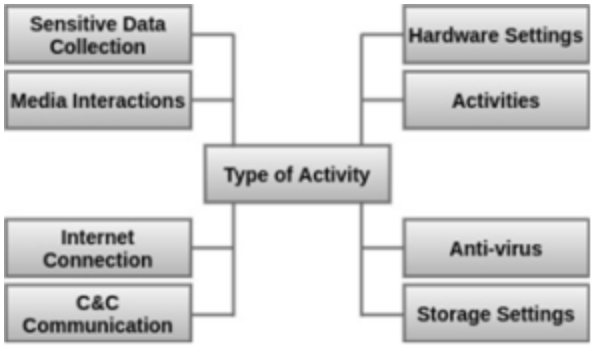

Figure 2: Type of activities performed by malware

Sensitive data collection: Adware families collect user contacts, send/receive spam emails, steal banking credentials, and collect personal information such as phone number, email address, app accounts, and browser history. Moreover, sending and receiving text messages is the most common function of many adware and backdoor families.

Media interactions: There is rare media interaction by adware families. However, androrat and dendroid backdoor families have major interactions with media that include making calls, collecting call history, taking over a phone's camera, collecting images, recording audio and hijacking the device's microphone.

Access to hardware settings: Most of the adware families collect phone information, such as phone status, IMEI number, phone ID, and location of the device. Some backdoor families kmin, moavt, levida, and droidkungfu also collect phone information.

Activities: A few adware families such as admogo, baiduprotect, dianle, and adend block, delete, and use phone applications or root the device. Appad, mobclick, and adend perform multiple functions. Appad accesses databases and executes queries, opens files and writes into them, starts services, registers receiver, and creates threads for inter-process communication, accesses cipher keys and updates the message digest, and gets device ID and verifies from device information whether a debugger is connected or not. In addition to all the aforementioned activities, mobclick sends broadcast messages whilst adend mainly initiates new activities. Some backdoor families, including kapuser, moavt and levida reboot the device repeatedly while hiddad, pyls and androrat access root level privileges.

Connecting to the internet: The majority of adware families steal network information (WiFi, IP, DNS), access malicious websites, and install malicious apps on compromised devices. Apparently, adware families display ads / notifications or warnings on the phone's screen. They also show URLs and shortcuts. Many backdoor families also steal network information and install malicious apps covertly.

Communication with command-and-control servers: A couple of adware and backdoor families communicate with the command-and-control server.

Uninstall anti-virus or avoid detection: Adware and backdoor families rarely uninstall anti-virus solutions installed on the target device and avoid getting detected by it.

Altering storage settings: Many adware families modify, collect, and access files and storage settings on the device. Some

backdoor families use external data and create memory guarded regions in the storage media

Technical features that can detect Adware and Backdoor:

Based on the results of our Android dataset (CCCS-CIC-AndMal-2020), the following technical features are very helpful to detect adware and backdoor:

1. **Memory features:** Memory features define activities performed by malware by utilizing memory.
2. **API features:** Application Programming Interface (API) features delineate the communication between two applications. Whenever a user browses some information in a browser, checks weather forecast, sets a timer, or uses Twitter on phone, he is using an Android API in the background.
3. **Network features:** Network features describe the data transmitted and received between other devices in the network. It indicates foreground and background network usage.
4. **Logcat features:** Logcat features write log messages corresponding to a function performed by malware.

Adware families undergo massive changes in memory while executing on a device. These families utilize private memory allocation and shared memory pages with other processes. This indicates that adware samples communicate with other processes while running on an infected device. These families also use API features to send notifications and warnings. Network features are used to send and receive packets between different processes. Finally, logcat features store the logs of activities performed by

adware families. Same is the scenario for backdoor families. However, memory features outweigh other features in detecting the presence of adware and backdoor families.

Preventive measures to protect your device

Adware shows pop-up messages to reveal its presence on the smartphone. It becomes fairly easy to detect adware on a phone. However, backdoor remains hidden from the user and performs malicious activities in a covert manner. Following key points can be considered to get rid of adware and backdoor on a smartphone:

Anti-virus scan: It is the easiest way to detect any vulnerability on the device. Anti-virus scan will display a list of vulnerabilities identified on the phone.

Identify fake apps: Keep a check on the apps installed without your permission. Uninstall them immediately.

Update firmware: Regularly update the firmware to avoid any vulnerabilities. Check for any update available in the settings and install the patch.

Control apps permissions: Do not agree to the unnecessary permissions requested by an app.

Do not click on links: Adware pops up malicious links but do not click on such links as it may lead to downloading malicious apps or malware on your device.

Conclusion

This article brings forward the fundamentals of adware and backdoor malware families. It comes equipped with malicious

behavior exhibited by these families on the target device. We established imperative indicators of compromise that points to the fact that the phone is infected by adware and backdoor families. Based on our public dataset on Android malware, named CCCS-CIC-AndMal-2020, we open on the technical features that are very useful to detect these families. Finally, the article introduces preventive measures to protect the device. The last article of the UAMF series will dig into PUA and file-infector malware families.