Preinstalled Malware Targeting Mobile Users

blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

March 10, 2017

Check Point mobile threat researchers recently detected a severe infection in 36 Android devices belonging to a large telecommunications company and a multinational technology company. While this is not unusual, one detail of the attacks stands out. In all instances, the malware was not downloaded to the device as a result of the users' use, it arrived with it.

According to the findings, the malware were already present on the devices even before the users received them. The malicious apps were not part of the official ROM supplied by the vendor, and were added somewhere along the supply chain. Six of the malware instances were added by a malicious actor to the device's ROM using system privileges, meaning they couldn't be removed by the user and the device had to be re-flashed.

Below are two examples of the malware installation. The research team was able to determine when the manufacturer finished installing the system applications on the device, when the malware was installed, and when the user first received the device.

A malicious adnet found in 6 mobile devices, APK com.google.googlesearch:

Loki malware, APK com.androidhelper.sdk:

Most of the malware found to be pre-installed on the devices were info-stealers and rough ad networks, and one of them was Slocker, a mobile ransomware. Slocker uses the AES encryption algorithm to encrypt all files on the device and demand ransom in return for their decryption key. Slocker uses Tor for its C&C communications.

The most notable rough adnet which targeted the devices is the Loki Malware. This complex malware operates by using several different components; each has its own functionality and role in achieving the malware's malicious goal. The malware displays illegitimate advertisements to generate revenue. As part of its operation, the malware steals data about the device and installs itself to system, allowing it to take full control of the device and achieve persistency.

The risk of pre-installed malware

As a general rule, users should avoid risky websites and download apps only from official and trusted app stores. However, following these guidelines is not enough to ensure their security. Pre-installed malware compromise the security even of the most careful users. In addition, a user who receives a device already containing malware will not be able to notice any change in the device's activity which often occur once a malware is installed.

The discovery of the pre-installed malware raises some alarming issues regarding mobile security. Users could receive devices which contain backdoors or are rooted without their knowledge. To protect themselves from regular and pre-installed malware, users should implement advanced security measures capable of identifying and blocking any abnormality in the device's behavior.

Appendix 1 – list of malware APKs, Shas, and Affected devices

com.fone.player1	Galaxy Note 2 LG G4	d99f490802f767201e8d507def4360319ce12ddf46765ca1b1168d64041f20f

com.lu.compass	Galaxy S7 Galaxy S4	f901fd1fc2ce079a18c619e1192b14dcc164c97da3286031ee542dabe0b4cd8c
com.kandian.hdtogoapp	Galaxy Note 4 Galaxy Note 8.0	b4e70118905659cd9b2c948ce59eba2c4431149d8eb8f043796806262d9a625b
com.sds.android.ttpod	Galaxy Note 2 Xiaomi Mi 4i	936e7af60845c4a90b8ce033734da67d080b4f4f0ca9c319755c4a179d54bf1b
com.baycode.mop	Galaxy A5	39c6bab80cc157bfe540bdee9ce2440b3b363e830bc7adaab9fc37075fb26fb1
com.kandian.hdtogoapp	Galaxy S4	998ab3d91cbc4f1b02ea6095f833bfed9d4f610eea83c51c56ce9979a2469aea
com.iflytek.ringdiyclient	ZTE x500	e9a30767e69dccb1b980eae42601dff857a394c7abdfe93a18e8739fa218d14b
com.android.deketv	Galaxy A5	01b8cb51464b07775ff5f45207d26d8d9f4a3b6863c110b56076b446bda03a8a
com.changba	Galaxy S4 Galaxy Note 3 Galaxy S4 Galaxy Note Edge Galaxy Note 4	a07745f05913e122ec19eba9848af6dfda88533d67b7ec17d11c1562245cbed1
com.example.loader	Galaxy Tab S2	e4e97090e9fd6cc3d321cee5799efd1806b5d8a9dea7c4872044057eb1c486ff
com.armorforandroid.security	Galaxy Tab 2	947574e790b1370e2a6b5f4738c8411c63bdca09a7455dd9297215bd161cd591
com.android.ys.services	Oppo N3 vivo X6 plus	0d8bf3cf5b58d9ba280f093430259538b6340b24e805058f3d85381d215ca778
com.mobogenie.daemon	Galaxy S4	0038f450d7f1df75bf5890cf22299b0c99cc0bea8d66e6d25528cb01992a436b
com.google.googlesearch	5 Asus Zenfone 2 LenovoS90	217eee3a83f33b658fb03fddfadd0e2eb34781d5dd243203da21f6cb335ef1b4
com.skymobi.mopoplay.appstore	LenovoS90	3032bb3d90eea6de2ba58ac7ceddead702cc3aeca7792b27508e540f0d1a60be
com.example.loader	OppoR7 plus	1cb5a37bd866e92b993ecbbcc4a2478c717eeb93839049ef0953b0c6ba89434e
com.yongfu.wenjianjiaguanli	Xiaomi Redmi	e5656c1d96158ee7e1a94f08bca1213686a05266e37fb2efb5443b84250ea29d
air.fyzb3	Galaxy Note 4	c4eac5d13e58fb7d32a123105683a293f70456ffe43bb640a50fde22fe1334a2
com.ddev.downloader.v2	Galaxy Note 5	92ae2083a8495cc5b0a0a82f0bdeb53877170d2615ce93bd8081172af9e60f8f
com.mojang.minecraftpe	Galaxy Note Edge	fbe9c495f86a291a0abe67ad36712475ff0674d319334dbd7a2c3aa10ff0f429
com.androidhelper.sdk	Lenovo A850	b0f6d2fc8176356124e502426d7aa7448490556ef68a2f31a78f4dd8af9d1750

NOTE: UPDATE MARCH 13, 2017- Some clarification was made. Number of devices from 38 to 36. Nexus machines were removed. Galaxy Note 8 was changed to Galaxy Note 8.0