How to detect and remove malware Agent Smith on Android

Agent Smith targets Android mobile operating systems, replacing installed applications with malicious versions without users' knowledge.

A new type of malware targeting smartphones has infected about 25 million devices (15 million of them are in India). This malicious software is called Agent Smith. Agent Smith targets Android mobile operating systems, replacing installed applications with malicious versions without users' knowledge.

Today's article will show you how to detect, prevent and protect your Android device from Agent Smith malware.

Agent Smith - New malware appeared on Android device

What is malware Agent Smith?

Agent Smith is a modular malware, exploits a variety of Android vulnerabilities, to replace existing legitimate applications with a malicious phishing version. Malicious apps do not steal data. Instead, replaced applications display a large amount of ads for users or credit theft from the device to pay for the displayed ads.

Agent Smith has the same name as a character from the famous Matrix movie. Check Point's team believes that the methods used by the malware are similar to those used by Agent Smith in this cult series.

According to Jonathan Shimonovich, head of Check Point Software Technologies' mobile device threat research, malware attacks user-installed applications silently, making it difficult for Android users. towel in self-defense against such threats.

Furthermore, Agent Smith has infected a large number of devices. India is the most attacked country. Check Point's research shows that about 15 million devices are contaminated with Agent Smith. The second country is Bangladesh, with about 2.5 million devices becoming victims of this malware. There are more than 300,000 cases of Agent Smith infections in the United States and about 137,000 cases in the UK.

Country	Total Devices	Total Infection Event Count
India	15,230,123	2,017,873,249
Bangladesh	2,539,913	208,026,886
Pakistan	1,686,216	94,296,907
Indonesia	572,025	67,685,983
Nepal	469,274	44,961,341
US	302,852	19,327,093
Nigeria	287,167	21,278,498
Hungary	282,826	7,856,064
Saudi Arabia	245,698	18,616,259
Myanmar	234,338	9,729,572

How does Agent Smith malware work?

Check Point Research believes Agent Smith malware comes from a Chinese company, created to help Chinese Android developers publish and promote applications in foreign markets.

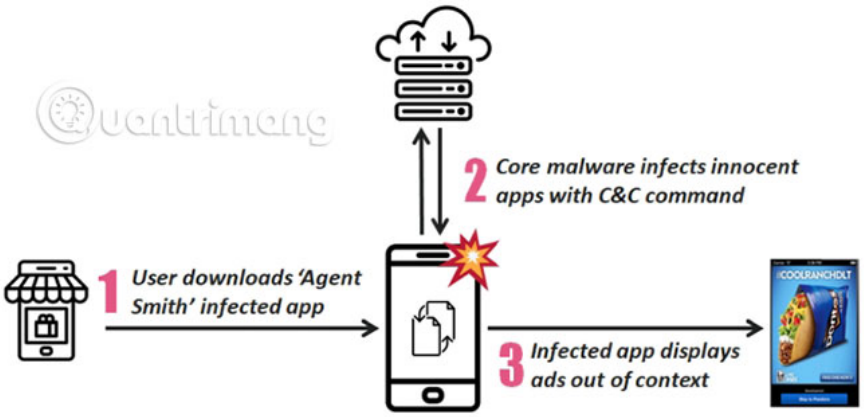
Malware first appeared on a third-party app store. 9Apps. This third-party app store is aimed at Indian, Arabic and Indonesian users (which explains why the number of devices infected with Agent Smith is so large). That's one of the reasons you should avoid downloading Android apps from third-party app stores.

Agent Smith malware works in three phases.

1. A dropper application (a type of malware developed to launch the virus, takes the form of a free smartphone application), for example, to install the malicious software voluntarily. The original Dropper contains malicious files encrypted and often takes the form of image, game or "adult" applications, almost inactive.

2. Dropper decodes and installs malicious files. Malware uses Google Updater, Google Update for U or 'com.google.vending' to disguise its activity.

3. The main malware creates a list of installed applications. If an application matches its 'prey' list, it will 'patch' the target application with a malicious advertising module, replacing the original as if it were a single application update. simple.



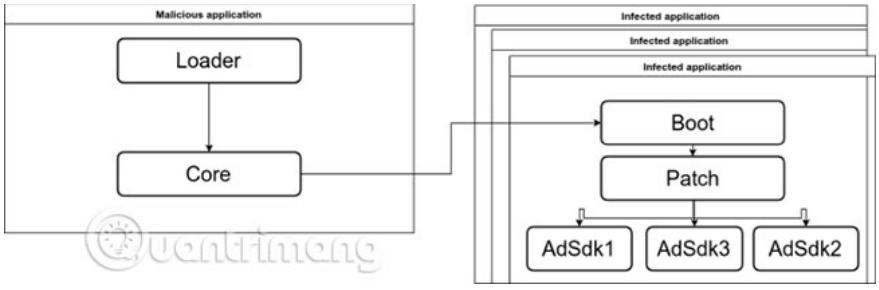
The 'prey' list includes WhatsApp, Opera, SwiftKey, Flipkart, Truecaller, etc.

Interestingly, Agent Smith incorporates several Android vulnerabilities, including Janus, Bundle and Man-in-the-Disk. The combination creates a 3-stage infection process, allowing malware distributors to build botnets that make money (through advertising). Check Point's team believes that Agent Smith may be the first campaign to integrate and weaponize all the vulnerabilities together, making the malware extremely dangerous.

Malware Module Agent Smith

Agent Smith malware uses a modular structure to infect targets, including:

1. Loader
2. Core
3. Boot
4. Patch
5. AdSDK
6. Updater



Dropper is a legitimate application that is repackaged to contain a malicious Loader module. Loader extracts and runs the Core module, in turn communicating with the C&C server of the malware. After that, the C&C server will send the list of prey. If any suitable application is found, the malware will use the vulnerability to transmit the Boot module into the repackaged application.

The next time the infected application launches, the Boot module runs the Patch module, uses the AdSDK module to introduce the ad and starts generating revenue.

Another interesting element of Agent Smith is that it does not stop at a malicious application. If Agent Smith finds multiple matches in the prey list, it replaces each application with the malicious version.

Agent Smith also released malicious updates for repackaged applications, continuing to infect and serve many new advertising packages.

Delete Agent Smith applications from Google Play

The main infection point of Agent Smith is a third-party app store, 9Apps. However, it is almost impossible to touch Google Play. Check Point has discovered 11 applications on Google Play Store that contain a set of malicious, inactive files related to Agent Smith. Agent Smith's Google Play versions use a slightly different spread technique but with the same goal.

Check Point reported malicious applications to Google and all were removed from Google Play Store.

How to detect and delete Agent Smith from Android

You can recognize Agent Smith quite easily. If your frequently used applications suddenly start creating too large amounts of advertising, it is a sure sign that something is wrong. Ads that "serve" malware are difficult or impossible to escape (this is another sign to note). But because Agent Smith acted almost silently in making advertisements, it was extremely difficult to recognize very small changes on the application.

1. How to detect malicious apps on Android

Please note that applications that suddenly display a huge amount of advertising are not 'exclusive' identifiers of Agent Smith. Other types of Android malware also serve ads to increase revenue. Therefore, your device may have been infected with another type of Android malware.

If you suspect something is wrong, you should use antivirus software to scan your device.

The first suggestion is Malwarebytes Security, the Android version of the excellent anti-malware tool. Download Malwarebytes Security and scan the entire system. It will summarize and remove any malicious applications available on your device.

Download Malwarebytes Security (Free, subscription available).

Reference more article: Top best antivirus application for Android phones for more details!

Wish you find the right choice!