HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-01

ANDROID MALWARE TRIES TO TRICK YOU. HERE'S HOW TO SPOT IT

Malicious apps are common, and they can drive you nuts with ads or steal your personal information.

1. Background:

Android malware is often deceptive. A mobile app called Ads Blocker, for example, promised to remove pesky ads from your phone, which sometimes pop up to cover your screen just when you're about to access something important. But people quickly found the app was nothing less than malware that served up more ads, according to security researchers.

It is just one example of malware that can frustrate Android phone users, plaguing them with ads that the creators get paid to display, even when they are looking at unrelated apps. Malware often also harvests fake clicks on the ads, doubling up on the value for the makers.

Researchers say adware like Ads Blocker is the most common type of malware on Android devices. An adware infection can make your phone so frustrating to use that you want to hulk out and crush it, but Android malware can do worse things -- like stealing personal information from your phone.

Malware can be disorienting, getting in the way of how you normally use your phone and making you feel uneasy even if you are not sure what is causing the problem. It is also common. Malwarebytes says it found close to 200,000 total instances of malware on its customers' devices in May and then again in June.

2. How malware on your phone works

a. Mobile malware typically takes one of two approaches:

According to Adam Bauer, a security researcher for mobile security company Lookout a mobile malware typically takes one of two approaches. The first type of malware tricks you into granting permissions that let it access sensitive information. That is where the Ads Blocker app fits in, and many of the permissions it requested sound like something a real ad blocker would have needed. But they also let the app run constantly in the background and show users ads even when they were using unrelated apps.

The second type of malware exploits vulnerabilities in phones, gaining access to sensitive information by giving itself administrator privileges. That reduces the need to get users to click "OK" on permissions requests, making it easier for the malware to run without users noticing its presence on the device.

b. Signs of malware on your Android phone

If you notice these things happening, your phone might be infected:

- You are seeing ads constantly, regardless of which app you are using.
- You install an app, and then the icon immediately disappears.
- Your battery is draining much faster than usual.
- You see apps you do not recognize on your phone.

These are all worrying signs that mean you should investigate further.

c. Ransomware on Android phones

Another type of malware is ransomware. Victims typically see their files locked away where you cannot use them. Typically, a pop-up demands payment in Bitcoin to get them back. Most Android ransomware can only lock up files on external storage, such as photos, Bauer said.

d. What mobile malware can do to your phone

Besides making you miserable with constant ads, mobile malware can access private information. Common targets include:

- Your banking credentials
- Your device information
- Your phone number or email address
- Your contact lists

Hackers can use this information for a variety of malevolent tasks. They can commit identity theft with your banking credentials. The Anubis banking Trojan, for example, accomplishes this by tricking users into granting it the access to an Android phone's accessibility features. This, in turn, allows the malware to log every app that you launch and the text you enter, including passwords. After you grant the permission one time, the malware's activity is completely invisible on screen, with no sign anything malevolent is happening as you log into your accounts.

Hackers can also use malware to collect and sell your device and contact information, until you are flooded with robocalls, texts and more ads; and they can send links for more malware to everyone on your contacts list.

3. Recommendations

Military personnel and Civilian Human Resource are advised to follow these tips in on how to stop malware on your Android phone:

First, keep your phone's software updated. Security experts consistently rank a current OS and updated apps as one of the most important steps users can take to protect their devices and accounts. If you already have malware running on your phone, software updates from your phone-maker -- say Android 10 or the upcoming Android 11 -- can patch vulnerabilities and cut off the access the malicious software enjoyed. Updates can also keep malware from working in the first place.

Next, review what permissions your apps have. Does a game have the ability to send SMS messages? That is probably unnecessary and could be a red flag, Bauer said. Keep this in mind when installing apps in the future, too.

Removing apps you think are malicious can be tricky. At times you can just remove the app's permissions, delete the app and be done with it. Other malicious apps will give themselves administrator privileges, so they cannot just be deleted without extra steps. If you have trouble removing a specific app, you can try looking it up online to find what has worked for other people.

You can also consider installing antivirus apps. These services can sometimes slow your phone, and they do have heightened access to your phone in order to spot malicious behavior, so you have to choose one you trust. And you are likely to want to choose the paid option if you can, both to unlock all the best features and to avoid seeing even more ads.

Still, the apps can warn you about malware on your phone and offer you customer service when you need to deal with something nasty. At the very least, you can use a well-known program like Malwarebytes, Norton, Lookout or Bitdefender to scan your device if you think you already have malware installed.

Finally, you can get rid of or avoid Android apps downloaded from third-party app stores. These apps do not go through review by Google and can more easily sneak malicious software onto your phone. Google does not catch everything before it gets on your phone, as reports about malicious Android apps being removed show, but sticking to the official Google Play Store -- and having a direct outlet to report problems you encounter -- is a further line of defense.

4. Dissemination

The information provided is intended to increase the security awareness of AFP units' mobile smart phone users and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin in whole for educational, non-commercial purposes.

Reference:

https://www.cnet.com/tech/services-and-software/android-malware-tries-to-trick-you-heres-how-to-spot-it/