Some URL shortener services distribute Android malware, including banking or SMS trojans

welivesecurity.com/2021/07/20/url-shortener-services-android-malware-banking-sms-trojans/

July 20, 2021

On iOS we have seen link shortener services pushing spam calendar files to victims' devices.

Lukas Stefanko
20 Jul 2021 - 02:00PM

On iOS we have seen link shortener services pushing spam calendar files to victims' devices.

We hope you already know that you shouldn't click on just any URLs. You might be sent one in a message; somebody might insert one under a social media post or you could be provided with one on basically any website. Users or websites providing these links might use URL shortener services. These are used to shorten long URLs, hide original domain names, view analytics about the devices of visitors, or in some cases even monetize their clicks.

Monetization means that when someone clicks on such a link, an advertisement, such as the examples in Figure 1, will be displayed that will generate revenue for the person who generated the shortened URL. The problem is that some of these link shortener services use aggressive advertising techniques such as scareware ads: informing users their devices are infected with dangerous malware, directing users to download dodgy apps from the Google Play store or to participate in shady surveys, delivering adult content, offering to start premium SMS service subscriptions, enabling browser notifications, and making dubious offers to win prizes.

We've even seen link shortener services pushing "calendar" files to iOS devices and distributing Android malware – indeed, we discovered one piece of malware we named Android/FakeAdBlocker, which downloads and executes additional payloads (such as banking trojans, SMS trojans, and aggressive adware) received from its C&C server.

Below we describe the iOS calendar-event-creating downloads and how to recover from them, before spending most of the blogpost on a detailed analysis of the distribution of Android/FakeAdBlocker and, based on our telemetry, its alarming number of detections. This analysis is mainly focused on the functionality of the adware payload and, since it can create spam calendar events, we have included a brief guide detailing how to automatically remove them and uninstall Android/FakeAdBlocker from compromised devices.

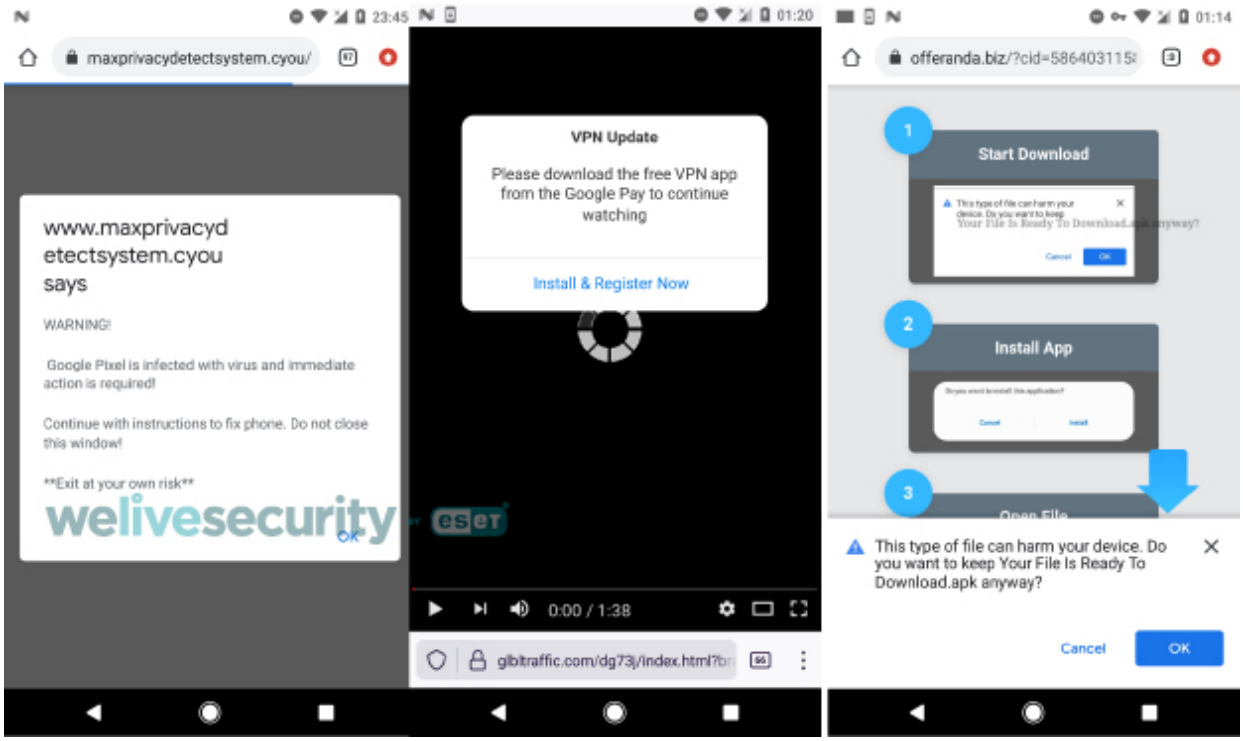


Figure 1. Examples of shady aggressive advertisements

Distribution

Content displayed to the victim from monetized link shorteners can differ based on the running operating system. For instance, if a victim clicked on the same link on a Windows device and on a mobile device, a different website would be displayed on each device. Besides websites, they could also offer an iOS device user to download an ICS calendar file, or an Android device user to download an Android app. Figure 2 outlines options we have seen in the campaign analyzed here.

Figure 2. Malware distribution process

While some advertisements and Android applications served by these monetized shortened links are legitimate, we observed that the majority lead to shady or unwanted behavior.

iOS targets

On iOS devices, besides flooding victims with unwanted ads, these websites can create events in victims' calendars by automatically downloading an ICS file. As the screenshots in Figure 3 show, victims must first tap the subscribe button to spam their calendars with these events. However, the calendar name "Click OK To Continue (sic)" is not revealing the true content of those calendar events and only misleads the victims into tapping the Subscribe and Done button.

These calendar events falsely inform victims that their devices are infected with malware, hoping to induce victims to click on the embedded links, which lead to more scareware advertisements.

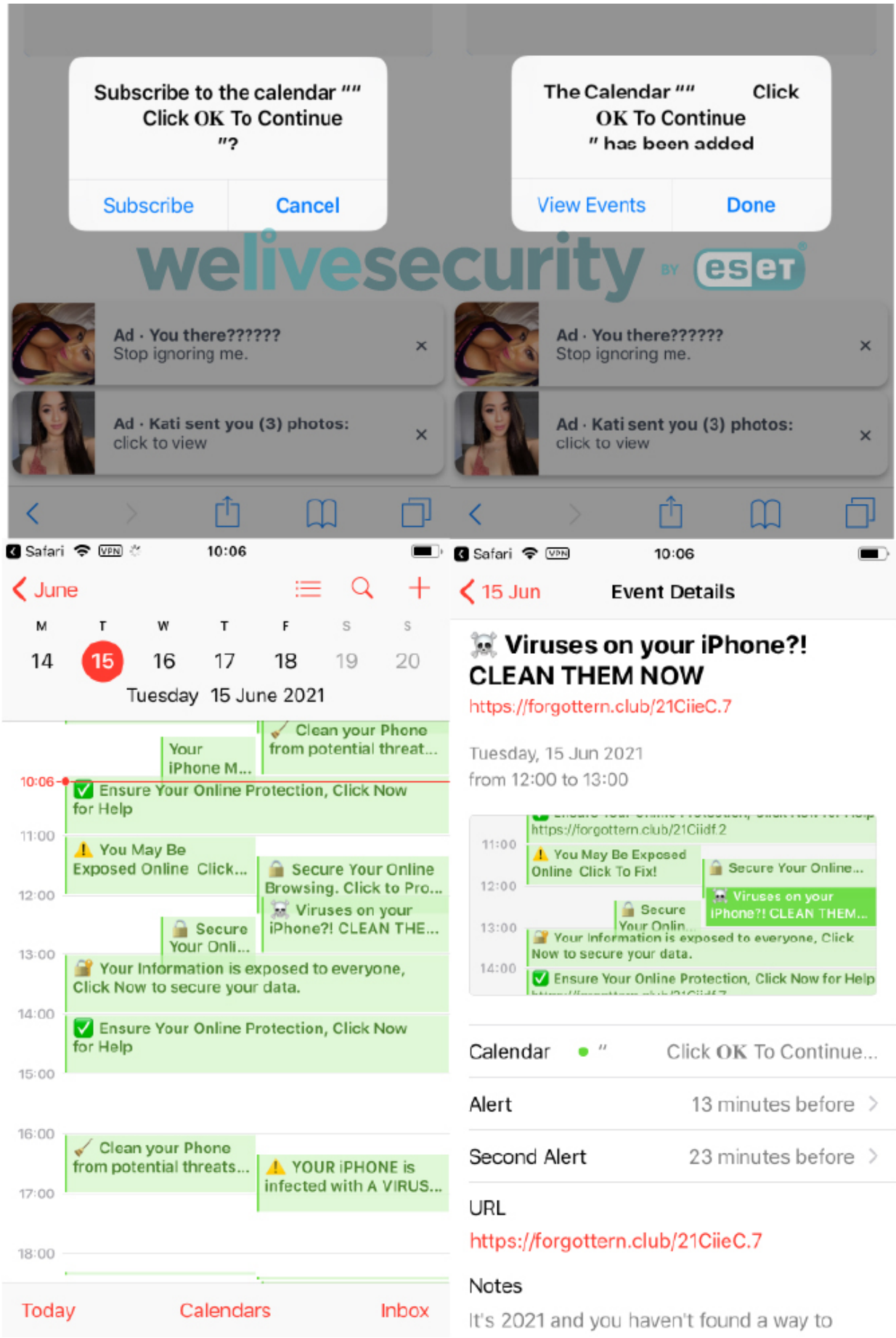


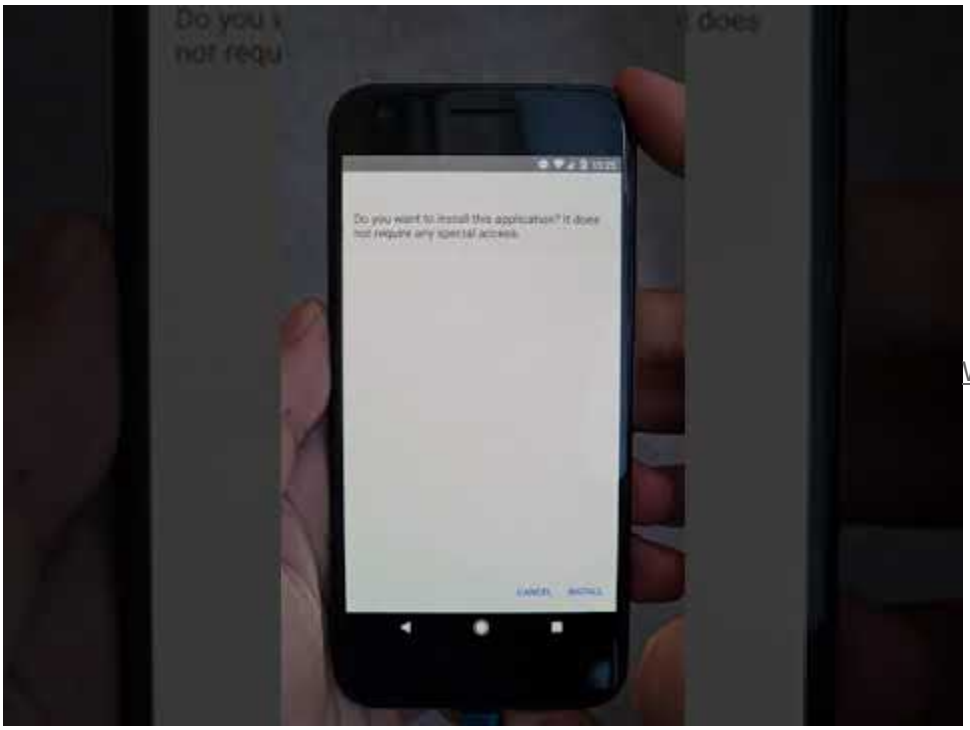
Figure 3. Scam website requests user to subscribe to calendar events on iOS platform

Android targets

For victims on Android devices, the situation is more dangerous because these scam websites might initially provide the victim with a malicious app to download and afterwards proceed with visiting or downloading the actual expected content searched for by the user.

There are two scenarios for Android users that we observed during our research. In the first one, when the victim wants to download an Android application other than from Google Play, there is a request to enable browser notifications from that website, followed by a request to download an application called adBLOCK app.apk. This might create the illusion that this adBLOCK app will block displayed advertisements in the future, but the opposite is true. This app has nothing to do with the legitimate adBLOCK application available from the official source.

When the user taps on the download button, the browser is redirected to a different website where the user is apparently offered an ad-blocking app named adBLOCK, but ends up downloading Android/FakeAdBlocker. In other words, the victim's tap or click is hijacked and used to download a malicious application. If the victim returns to the previous page and taps on the same download button, the correct legitimate file that the intended victim wanted is downloaded onto the device. You can watch one of the examples in the video below.

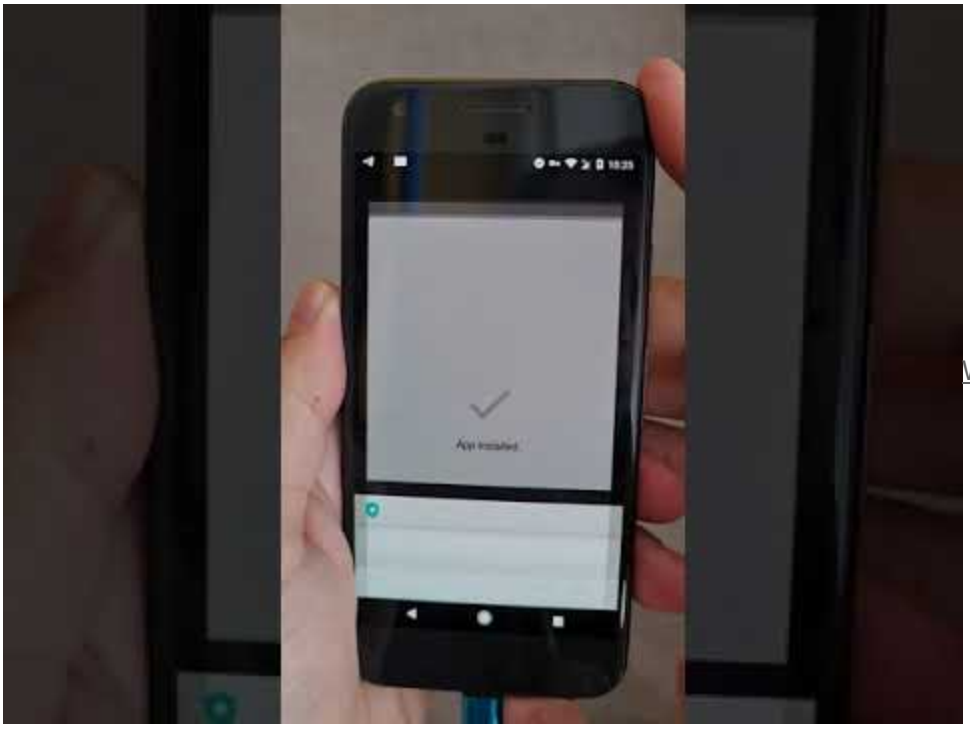


Watch Video At:

https://youtu.be/ps2QS0Oquos

In the second Android scenario, when the victims want to proceed with downloading the requested file, they are shown a web page describing the steps to download and install an application with the name Your File Is Ready To Download.apk. This name is obviously

misleading; the name of the app is trying to make the user think that what is being downloaded is the app or a file they wanted to access. You can see the demonstration in the video below.



Watch Video At:

https://youtu.be/iogUoGf1RxY

In both cases, a scareware advertisement or the same Android/FakeAdBlocker trojan is delivered via a URL shortener service. Such services employ the Paid to click (PTC) business model and act as intermediaries between customers and advertisers. The advertiser pays for displaying ads on the PTC website, where part of that payment goes to the party that created the shortened link. As stated on one of these link shortening websites in the privacy policy section, these ads are via their advertising partners and they are not responsible for delivered content or visited websites.

One of the URL shortener services states in its terms of service that users should not create shortened links to transmit files that contain viruses, spyware, adware, trojans or other harmful code. To the contrary, we have observed that their ad partners are doing it.

Telemetry

Based on our detection data, Android/FakeAdBlocker was spotted for the first time in September 2019. Since then, we have been detecting it under various threat names. From the beginning of this year till July 1st, we have seen more than 150,000 instances of this threat being downloaded to Android devices.

Figure 4. ESET detection telemetry for Android/FakeAdBlocker

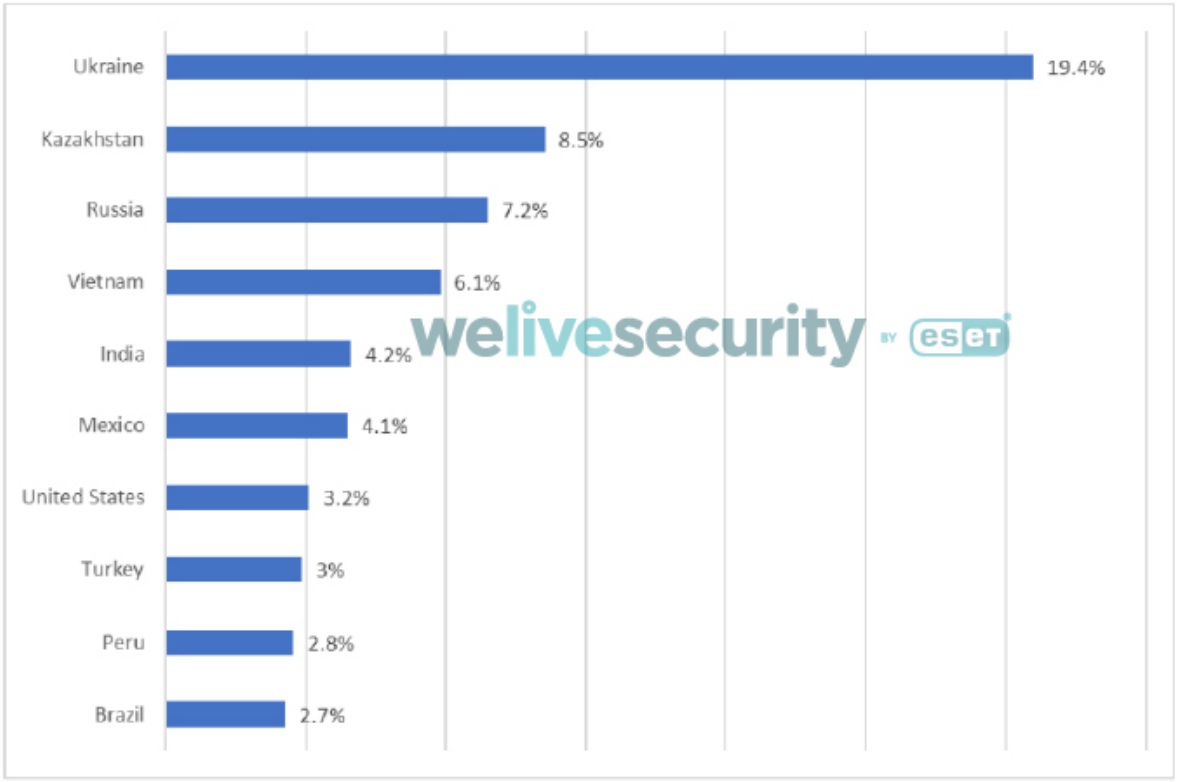


Figure 5. Top ten countries by proportion of Android/FakeAdBlocker detections (January 1st – July 1st 2021)

Android/FakeAdBlocker analysis

After downloading and installing Android/FakeAdBlocker, the user might realize that, as seen in Figure 6, it has a white blank icon and, in some cases, even has no app name.

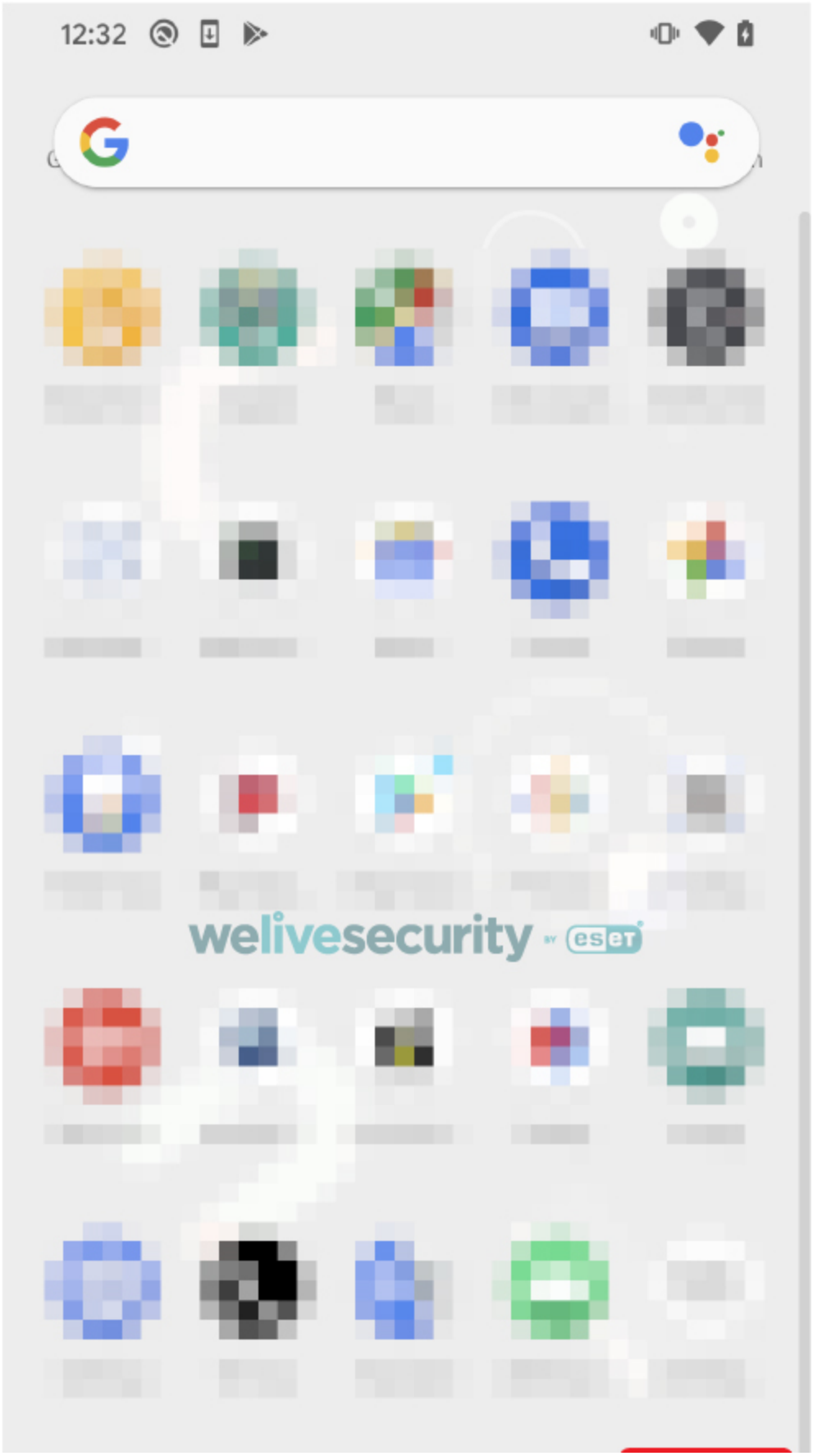


Figure 6. App icon of Android/FakeAdBlocker

After its initial launch, this malware decodes a base64-encoded file with a .dat extension that is stored in the APK's assets. This file contains C&C server information and its internal variables.

Figure 7. Decoded config file from APK assets

From its C&C server it will request another configuration file. This has a binary payload embedded, which is then extracted and dynamically loaded.

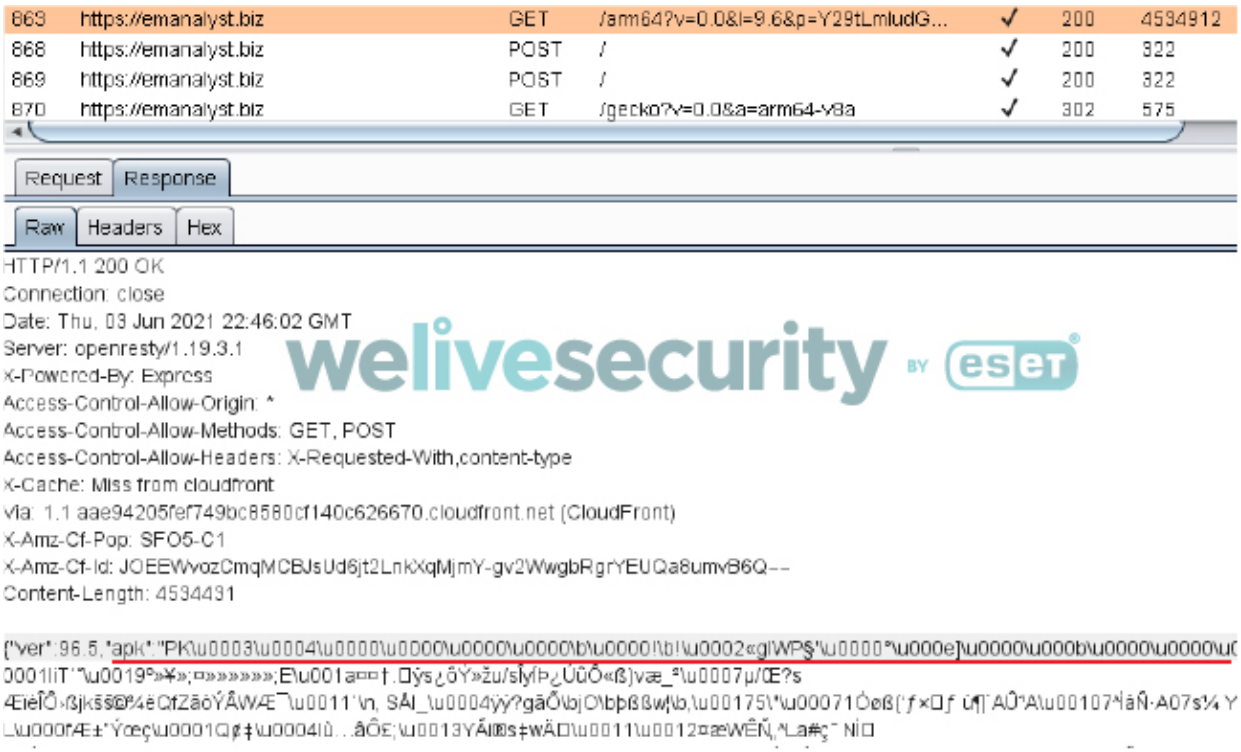


Figure 8. Android/FakeAdBlocker downloads an additional payload

For most of the examples we have observed, the this payload was responsible for displaying out-of-context ads. However, in hundreds of cases, different malicious payloads were downloaded and executed. Based on our telemetry, the C&C server returned different payloads based on the location of the device. The Cerberus banking trojan was

downloaded to devices in Turkey, Poland, Spain, Greece and Italy. It was disguised as Chrome, Android Update, Adobe Flash Player, Update Android, or Google Guncelleme app (guencelleme is Turkish for “update” so the name of the app is Google Update). In Greece we have also seen the Ginp banking trojan being downloaded. The same malware family variant of SMS trojan was distributed in the Middle East. Besides these trojans, Bitdefender Labs also identified the TeaBot (also known as Anatsa) banking trojan being downloaded as a payload by Android/FakeAdBlocker. Payloads are downloaded to external media storage in the files subdirectory of the parent app package name using various app names. A list of payload APK names is included in the *IoCs* section.

The emerging fact that the C&C server can at any time distribute different malicious payloads makes this threat unpredictable. Since all aforementioned trojans have already been analyzed, we will continue with the analysis of the adware payload that was distributed to more than 99% of the victims. The adware payload bears many code similarities with the downloader so we are classifying both in the same Android/FakeAdBlocker malware family.

Although the payloads download in the background, the victim is informed about actions happening on the mobile device by the activity displayed saying file is being downloaded. Once everything is set up, the Android/FakeAdBlocker adware payload asks the victim for permission to draw over other apps, which will later result in it creating fake notifications to display advertisements in the foreground, and for permission to access the calendar.

Figure 9. Activity shown after start

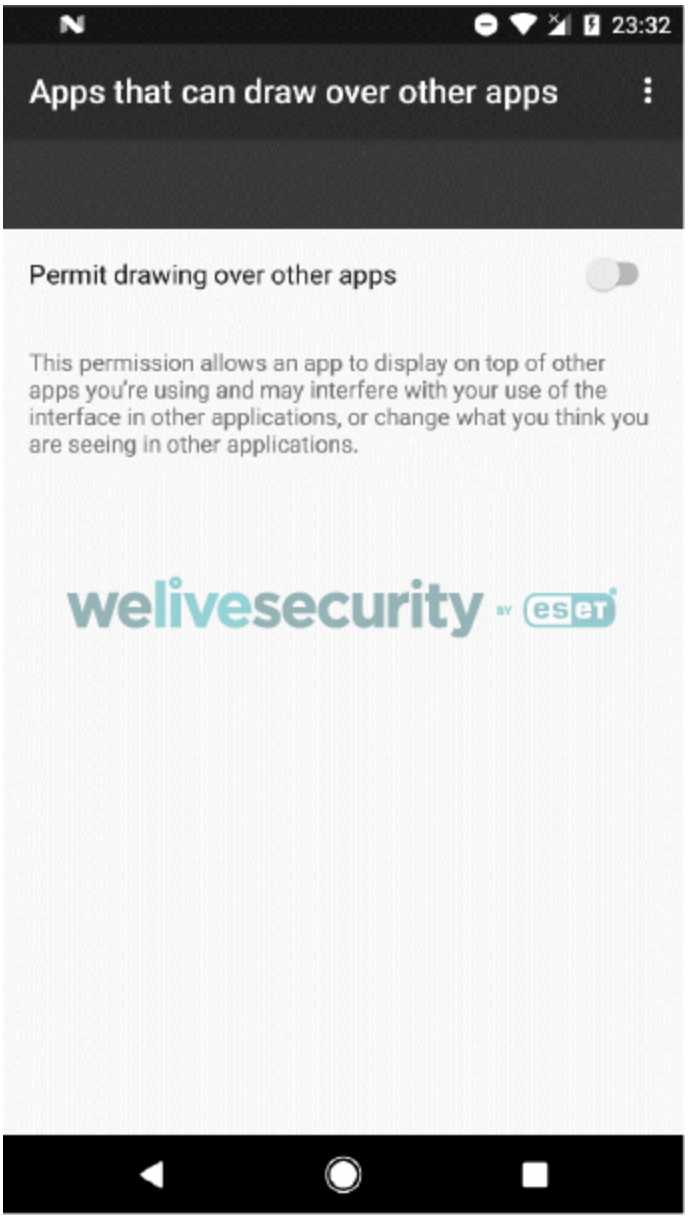


Figure 10. Permission request to control what is displayed in foreground

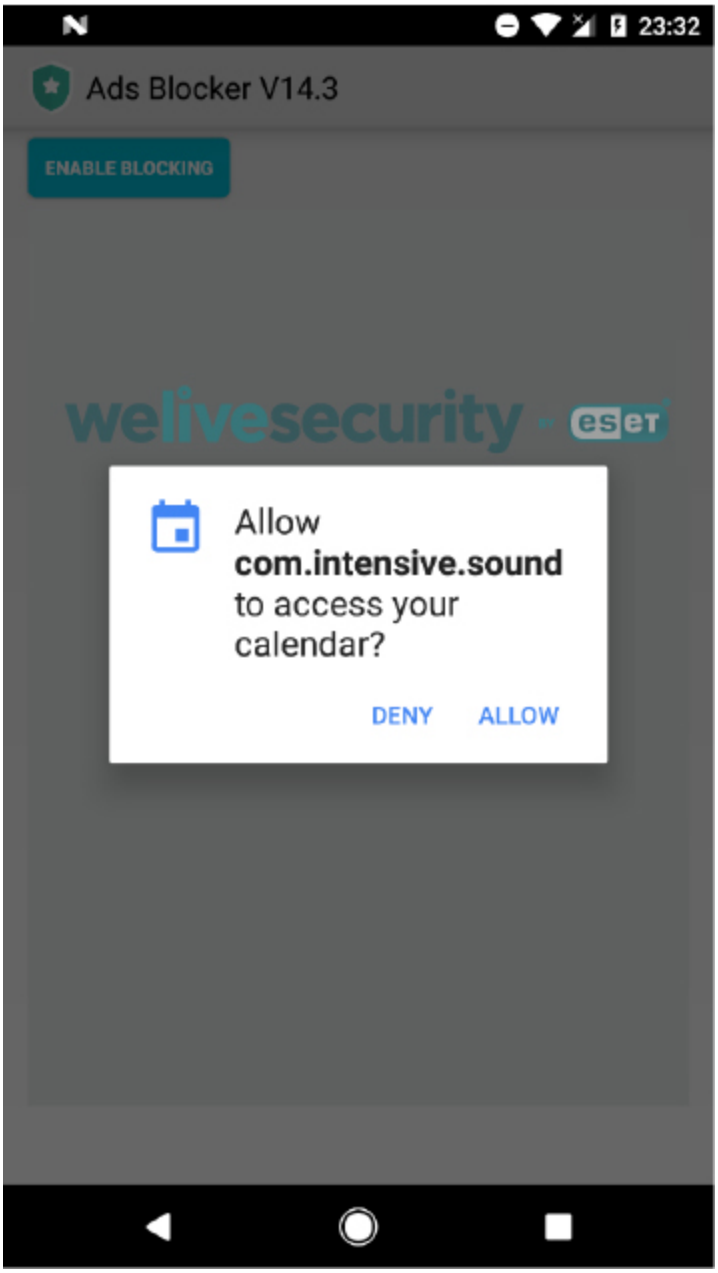


Figure 11. Permission request to edit calendar events

After all permissions are enabled, the payload silently starts to create events in Google Calendar for upcoming months.

Figure 12. Scareware calendar events created by malware (above) and detail (below)

It creates eighteen events happening every day, each of them lasts 10 minutes. Their names and descriptions suggest that the victim's smartphone is infected, user data is exposed online or that a virus protection app is expired. Descriptions of each event include a link that leads the victim to visit a scareware advertisement website. That website again claims the device has been infected and offers the user to download shady cleaner applications from Google Play.

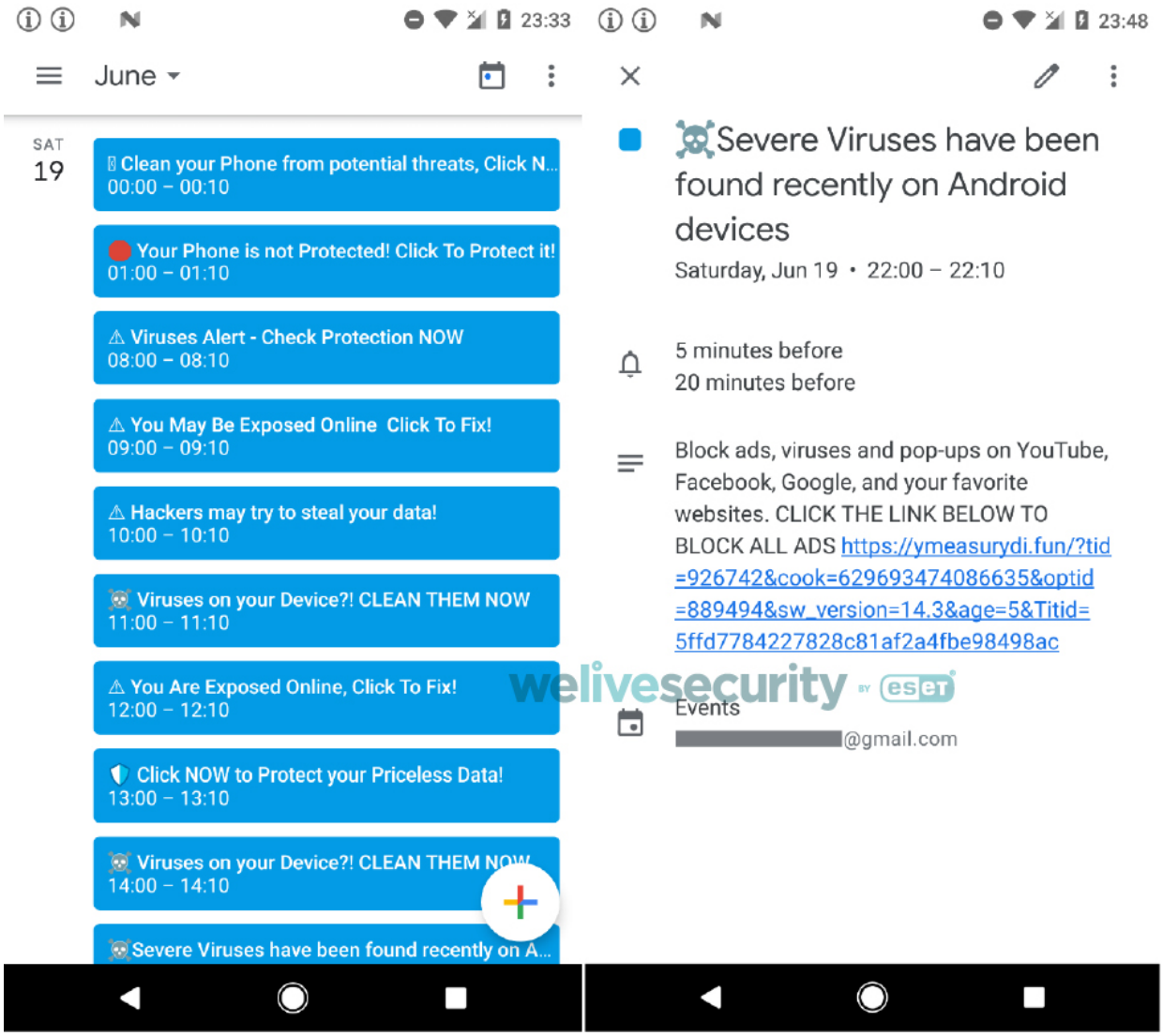


Figure 13. Titles and descriptions of the events (left) and the reminder displayed by one of them (right)

All the event title names and their descriptions can be found the malware's code. Here are all scareware event texts created by the malware, verbatim. If you find one of these in your Google Calendar, you are or were most likely a victim of this threat.

⚠ Hackers may try to steal your data!
Block ads, viruses and pop-ups on YouTube, Facebook, Google, and your favorite websites. CLICK THE LINK BELOW TO BLOCK ALL ADS

⚠ YOUR Device can be infected with A VIRUS ⚠
Block ads, viruses and pop-ups on YouTube, Facebook, Google, and your favorite websites. CLICK THE LINK BELOW TO BLOCK ALL ADS

☠Severe Viruses have been found recently on Android devices
Block ads, viruses and pop-ups on YouTube, Facebook, Google, and your favorite websites. CLICK THE LINK BELOW TO BLOCK ALL ADS

🛑 *Your Phone is not Protected ?! Click To Protect it!*
It's 2021 and you haven't found a way to protect your Device? Click below to fix this!

⚠ *Android Virus Protection Expired ?! Renew for 2021*
We have all heard stories about people who got exposed to malware and expose their data at risk. Don't be silly, protect yourself now by clicking below!

⚠ *You May Be Exposed Online Click To Fix!*
Hackers can check where you live by checking your device's IP while you are at home. Protect yourself by installing a VPN. Protect your self by clicking below.

✔️ *Clear Your Device from Malicious Attacks!*
Your Device is not invincible from viruses. Make sure that it is free from infection and prevent future attacks. Click the link below to start scanning!

⚠ *Viruses Alert – Check Protection NOW*
Hackers and practically anyone who want it can check where you live by breaking into your device. Protect your self by clicking below.

☠️ *Viruses on your Device?! CLEAN THEM NOW*
It's 2021 and you haven't found a way to protect your Device? Click below to fix this!

🛡️ *Click NOW to Protect your Priceless Data!*
Your identity and other important information can be easily stolen online without the right protection. VPN can effectively avoid that from happening. Click below to avail of that needed protection.

⚠ *You Are Exposed Online, Click To Fix!*
Hackers can check where you live by checking your device's IP while you are at home. Protect yourself by installing a VPN. Protect your self by clicking below.

🧹 *Clean your Phone from potential threats, Click Now.*
Going online exposes you to various risks including hacking and other fraudulent activities. VPN will protect you from these attacks. Make your online browsing secured by clicking the link below.

🛑 *Your Phone is not Protected! Click To Protect it!*
It's 2021 and you haven't found a way to protect your iPhone? Click below to fix this!

⚠ *YOUR Device can be infected with A VIRUS* ⚠
Block ads, viruses and pop-ups on YouTube, Facebook, Google, and your favorite websites. CLICK THE LINK BELOW TO BLOCK ALL ADS

⚠ You May Be Exposed Online Click To Fix!
Hackers can check where you live by checking your device's IP while you are at home. Protect yourself by installing a VPN. Protect your self by clicking below.

☠Severe Viruses have been found recently on Android devices
Block ads, viruses and pop-ups on YouTube, Facebook, Google, and your favorite websites. CLICK THE LINK BELOW TO BLOCK ALL ADS

☠ Viruses on your Device?! CLEAN THEM NOW
It's 2021 and you haven't found a way to protect your Device? Click below to fix this!

⚠ Android Virus Protection Expired ?! Renew for 2021
We have all heard stories about people who got exposed to malware and expose their data at risk. Don't be silly, protect yourself now by clicking below!

Besides flooding the calendar with scam events, Android/FakeAdBlocker also randomly displays full screen advertisements within the mobile browser, pops up scareware notifications and adult advertisements, and displays a Messenger-like "bubble" in the foreground mimicking a received message with a scammy text next to it.

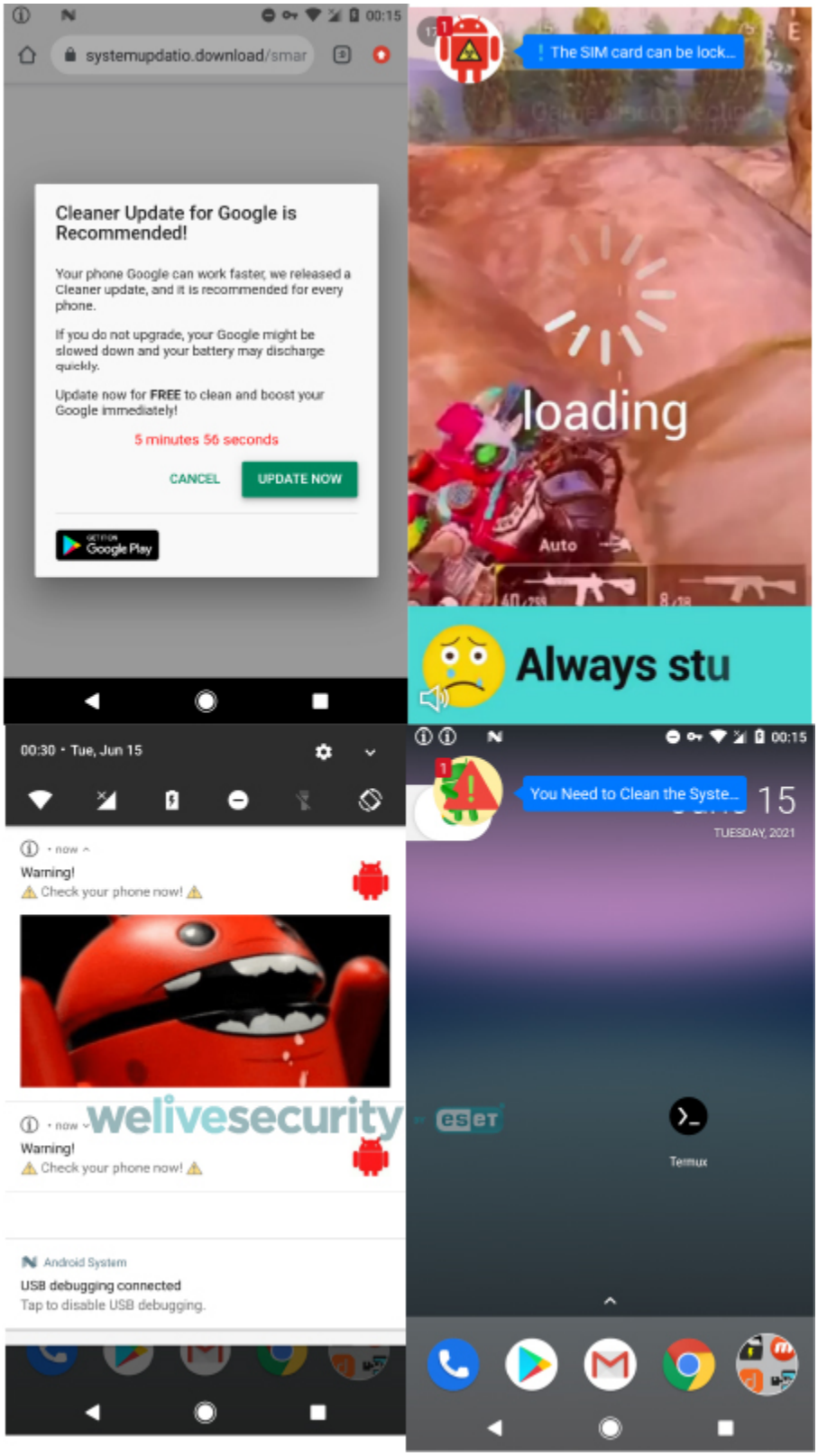


Figure 14. Examples of displayed scareware ads

Clicking on any of these would lead the user to a website with further scareware content that suggests that the victim install cleaners or virus removers from Google Play. We have already written about similar shady apps impersonating security software in 2018.

Uninstall process

To identify and remove Android/FakeAdBlocker, including its dynamically loaded adware payload, you need to first find it among your installed applications, by going to Settings -> Apps. Because the malware doesn't have an icon or an app name (see Figure 15), it should be easy to spot. Once located, tap it once to select it and then tap on Uninstall button and confirm the request to remove the threat.

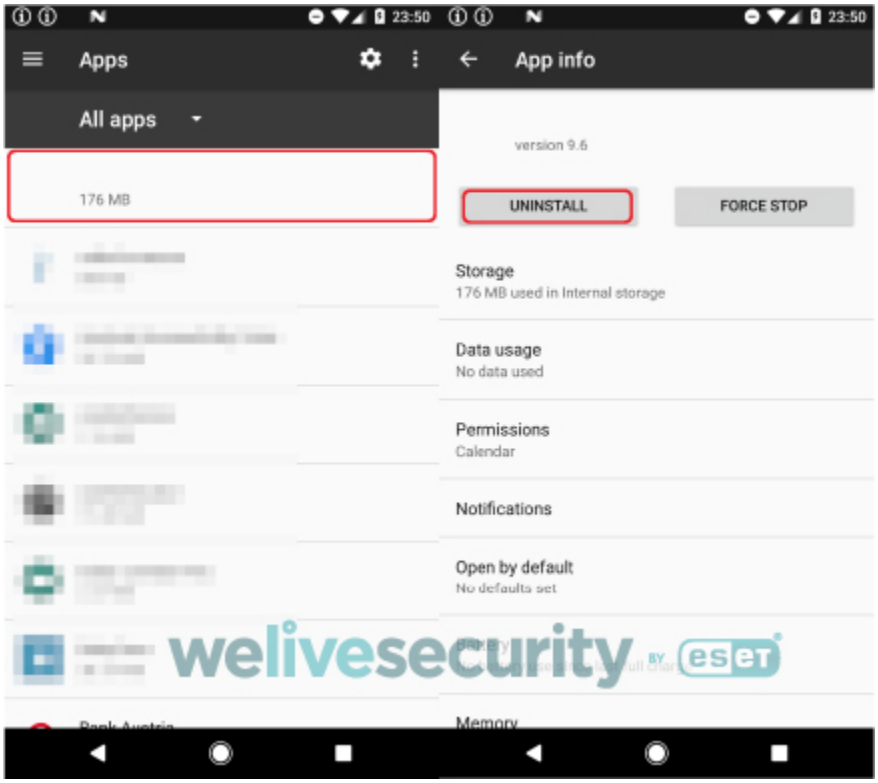


Figure 15. Manual uninstallation of malware

How to automatically remove spam events

Uninstalling Android/FakeAdBlocker will not remove the spam events it created in your calendar. You can remove them manually; however, it would be a tedious job. This task can also be done automatically, using an app. During our tests we successfully removed all these events using a free app available from the Google Play store called Calendar Cleanup. A problem with this app is that it removes only past events. Because of that, to remove upcoming events, temporarily change the current time and date in the settings of the device to be the day after the last spam event created by the malware. That would make all these events expired and Calendar Cleanup can then automatically remove them all.

It is important to state that this app removes all events, not just the ones created by the malware. Because of that, you should carefully select the targeted range of days.

Once the job is done, make sure to reset the current time and date.

Conclusion

Based on our telemetry, it appears that many users tend to download Android apps from outside of Google Play, which might lead them to download malicious apps delivered through aggressive advertising practices that are used to generate revenue for their authors. We identified and demonstrated this vector of distribution in the videos above. Android/FakeAdBlocker downloads malicious payloads provided by its operator's C&C server; in most cases, after launch these hide themselves from user view, deliver unwanted scareware or adult content advertisements and create spam calendar events for upcoming months. Trusting these scareware ads might cost their victims money either by sending premium rate SMS messages, subscribing to unnecessary services, or downloading additional and often malicious applications. Besides these scenarios, we identified various Android banking trojans and SMS trojans being downloaded and executed.

IoCs

Hash	Detection name
B0B027011102B8FD5EA5502D23D02058A1BFF1B9	Android/FakeAdBlocker.A
E51634ED17D4010398A1B47B1CF3521C3EEC2030	Android/FakeAdBlocker.B
696BC1E536DDBD61C1A6D197AC239F11A2B0C851	Android/FakeAdBlocker.C

C&Cs

emanalyst[.]biz
mmunitedaw[.]info
ommunite[.]top
rycovernmen[.]club
ransociatelyf[.]info
schemics[.]club
omeoneha[.]online
sityinition[.]top
fceptthis[.]biz
oftongueid[.]online
honeiwillre[.]biz
eaconhop[.]online
ssedonthep[.]biz
fjobiwouldli[.]biz
offeranda[.]biz

File paths of downloaded payloads

/storage/emulated/0/Android/data/com.intensive.sound/files/Download/updateandroid.apk
/storage/emulated/0/Android/data/com.intensive.sound/files/Download/Chrome05.12.11.apk
/storage/emulated/0/Android/data/com.intensive.sound/files/Download/XXX_Player.apk
/storage/emulated/0/Android/data/com.confidential.pottery/files/Download/Google_Update.apk
/storage/emulated/0/Android/data/com.confidential.pottery/files/Download/System.apk
/storage/emulated/0/Android/data/com.confidential.pottery/files/Download/Android-Update.5.1.apk
/storage/emulated/0/Android/data/com.cold.toothbrush/files/Download/Android_Update.apk
/storage/emulated/0/Android/data/com.cold.toothbrush/files/Download/chromeUpdate.apk
/storage/emulated/0/Android/data/com.cold.toothbrush/files/Download/FreeDownloadVideo.apk
/storage/emulated/0/Android/data/com.anaconda.brave/files/Download/MediaPlayer.apk
/storage/emulated/0/Android/data/com.anaconda.brave/files/Download/GoogleChrome.apk
/storage/emulated/0/Android/data/com.dusty.bird/files/Download/Player.apk

MITRE ATT&CK techniques

This table was built using *version 9* of the ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1476	Deliver Malicious App via Other Means	Android/FakeAdBlocker can be downloaded from third-party websites.
T1444	Masquerade as Legitimate Application	Android/FakeAdBlocker impersonates legitimate AdBlock app.	
Persistence	T1402	Broadcast Receivers	Android/FakeAdBlocker listens for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts.
T1541	Foreground Persistence	Android/FakeAdBlocker displays transparent notifications and pop-up advertisements.	
Defense Evasion	T1407	Download New Code at Runtime	Android/FakeAdBlocker downloads and executes an APK filefiles from a malicious adversary server.

Tactic	ID	Name	Description
T1406	Obfuscated Files or Information	Android/FakeAdBlocker stores base64-encoded file in assets containing config file with C&C server.	
T1508	Suppress Application Icon	Android/FakeAdBlocker's icon is hidden from its victim's view.	
Collection	T1435	Access Calendar Entries	Android/FakeAdBlocker creates scareware events in calendar.
Command And Control	T1437	Standard Application Layer Protocol	Android/FakeAdBlocker communicates with C&C via HTTPS.
Impact	T1472	Generate Fraudulent Advertising Revenue	Android/FakeAdBlocker generates revenue by automatically displaying ads.

20 Jul 2021 - 02:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion