Welcome Chat as a secure messaging app? Nothing could be further from the truth

welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth

July 14, 2020

We discovered a new operation within a long-running cyber-espionage campaign in the Middle East. Targeting Android users via the malicious Welcome Chat app, the operation appears to have links to the malware named BadPatch, which MITRE links to the Gaza Hackers threat actor group known also as Molerats.

Our analysis shows that the Welcome Chat app allows spying upon its victims. However, it is not simple spyware. Welcome Chat is a functioning chat app that delivers the promised functionality along with its hidden espionage capacity.

We found this spyware being advertised to chat-hungry users (these apps are banned in some countries in the Middle East region) on a dedicated website (see Figure 1). The fact that the website is in Arabic conforms with the targeting of the whole campaign we believe this operation belongs to. The domain was registered in October 2019; we couldn't, however, determine when the website was launched.

Figure 1. The website of the malicious Welcome Chat app

The malicious website promotes the Welcome Chat app, claiming it's a secure chat platform that is available on the Google Play store. Both claims are false. In regard to the "secure" claim, nothing is further from the truth. Not only is Welcome Chat an espionage tool; on top of that, its operators left the data harvested from their victims freely available on the internet. And the app was never available on the official Android app store.

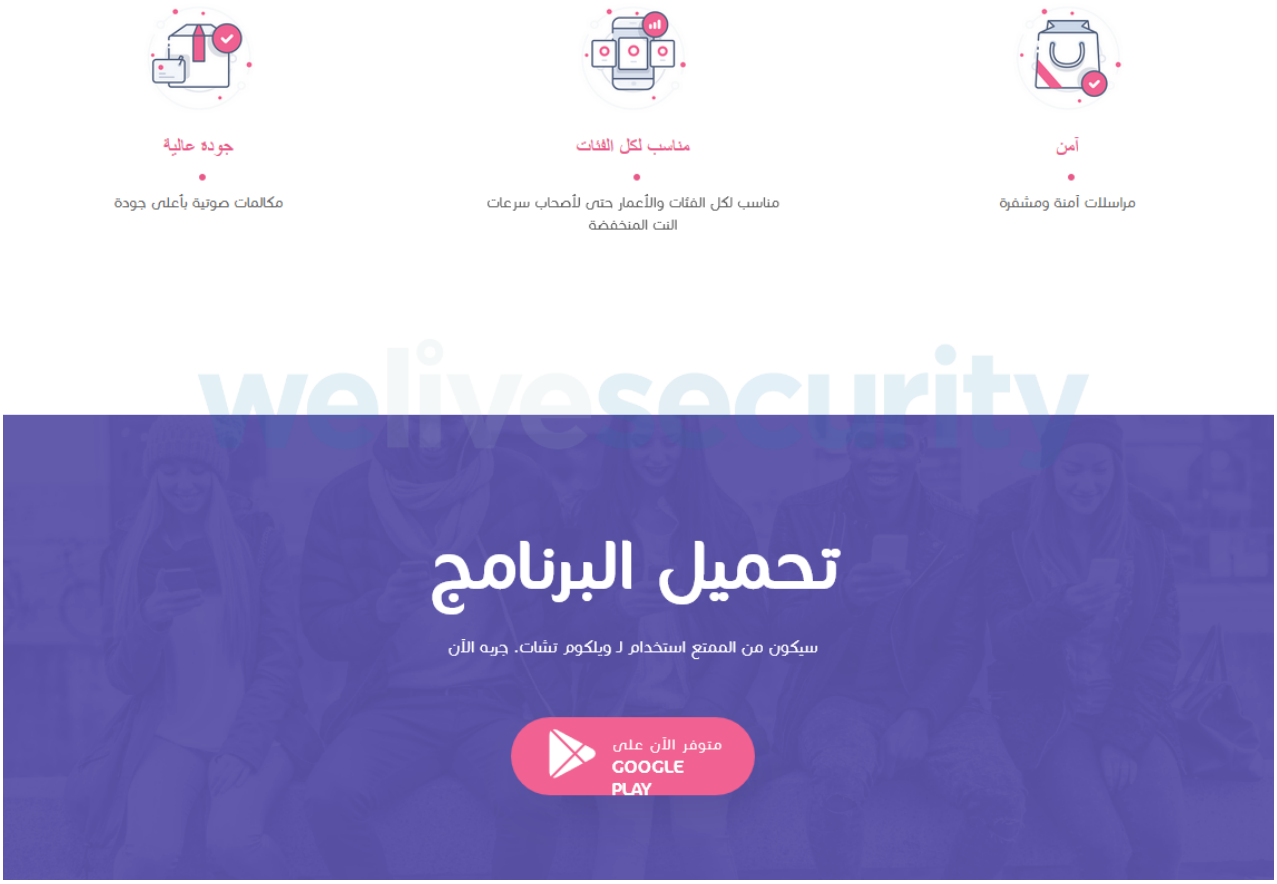

Figure 2. Despite the caption stating "High quality, secure and available on Google Play", the button leads to the installation file being downloaded directly from the malicious website

Functionality/Analysis

Once the user downloads the app, it needs the setting "Allow installing apps from unknown sources" to be activated since the app was not downloaded from the Play Store.

After installation, the malicious app will request the victim to allow permissions such as send and view SMS messages, access files, record audio, and access contacts and device location. Such an extensive list of intrusive permissions might normally make the victims suspicious – but with a messaging app, it's natural they are needed for the app to deliver the promised functionality.

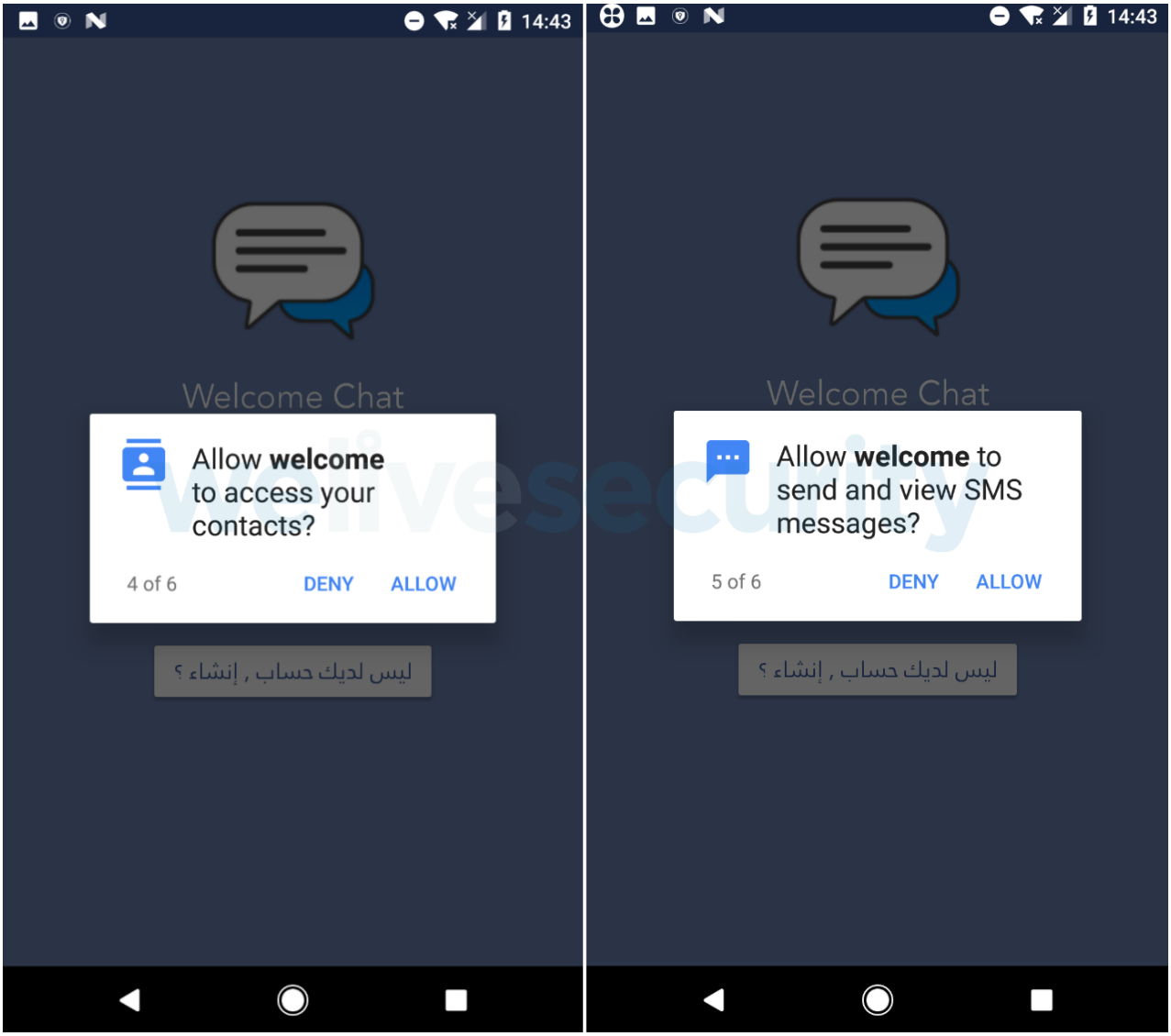

Figure 3. Permission requests by Welcome Chat spyware

In order to be able to communicate with other users of this app, the user needs to register and create a personal account (see Figure 4).

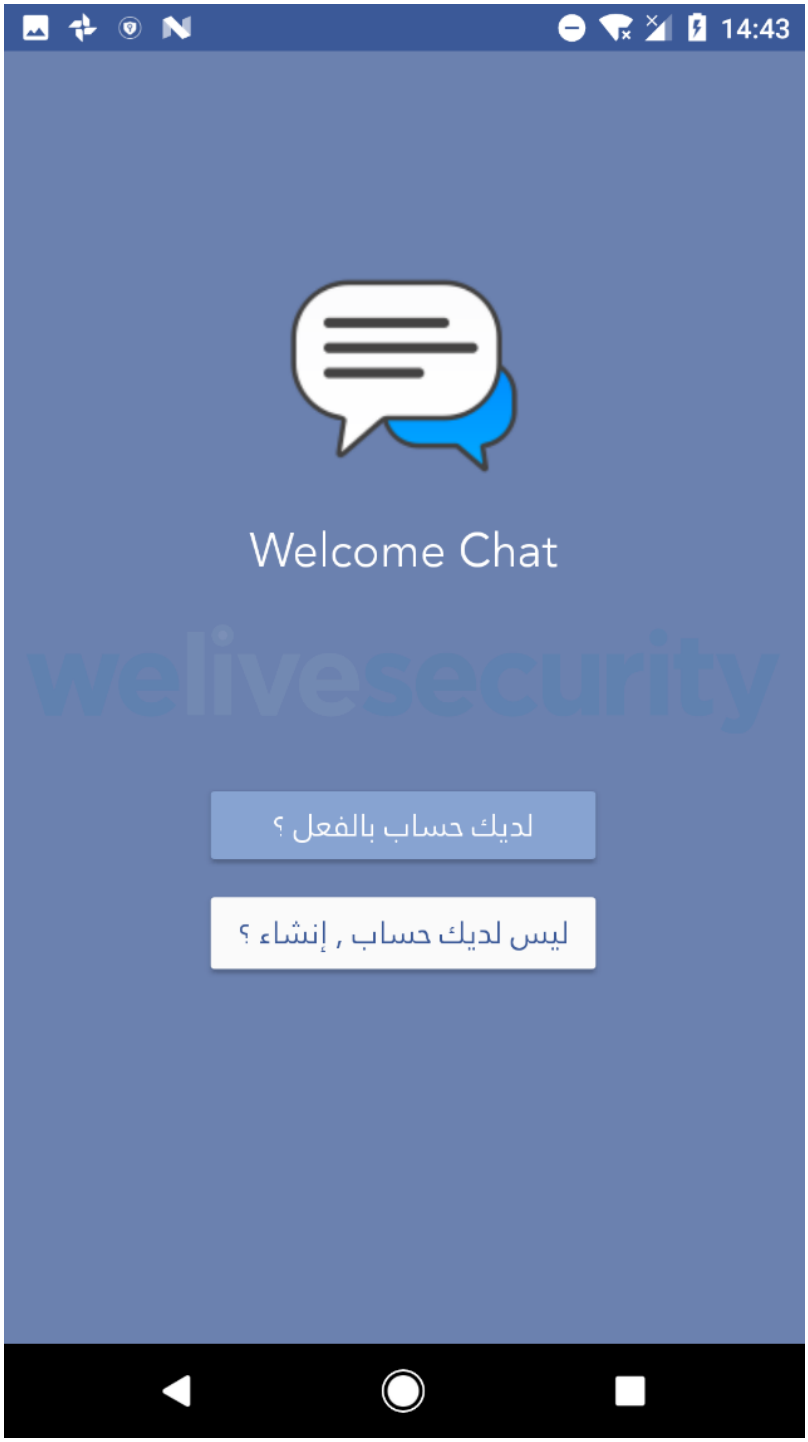

Figure 4. The Sign up/Login dialog of the Welcome Chat app

Immediately after receiving these permissions, Welcome Chat sends information about the device to its C&C and is ready to receive commands. It is designed to contact the C&C server every five minutes.

On top of its core espionage functionality – monitoring the chat communications of its users – the Welcome Chat app can perform the following malicious actions: exfiltrating sent and received SMS messages, call log history, contact list, user photos, recorded phone calls, the GPS location of the device, and device info.

Trojanized or attacker-developed chat app?

An interesting question arises with functional trojan apps: is the app an attacker-trojanized version of a clean app, or did the attackers develop a malicious app from scratch?

In both cases, it is easy for the attackers to spy on exchanged in-app messages as they would – naturally – have the authorization keys to the user database.

Despite the first option being typical for trojanized apps, we believe that in this particular case, the second explanation is more probable.

Typically, trojanized apps are created via a process of appending the malicious functionality to a legitimate app. The bad guys find and download a suitable app. After decompiling it, they add the malicious functionality and recompile the now-malicious-yet-still-functioning app to spread it among their desired audience.

There is a major question mark with this option: to this day, we have not been able to discover any clean version of the Welcome Chat app. Not only can it not be found on any of the Android markets we have on our radar; based on the binary matching algorithms in our sample classification systems, we haven't found any clean app with this same chat functionality. Of interest in this regard is that a clean version of Welcome Chat, without the espionage functionality, was uploaded to VirusTotal in mid-February 2020 (hash: 757bd41d5fa99e19200cee59a3fd1577741ccd82). The malicious version was first submitted to VirusTotal a week earlier.

This leads us to believe that the attackers developed the malicious chat app on their own. Creating a chat app for Android is not difficult; there are many detailed tutorials on the internet. With this approach, the attackers have better control over the compatibility of the app's malicious functionality with its legitimate functions, so they can ensure that the chat app will work.

Code analysis

The Welcome Chat espionage app seems to have targeted Arabic-speaking users: both the default website language and default in-app language are Arabic. However, based on debug logs left in the code, strings, class and unique variable names, we were able to determine that most of the malicious code was copied from publicly available open source code projects and code example snippets available on public forums.

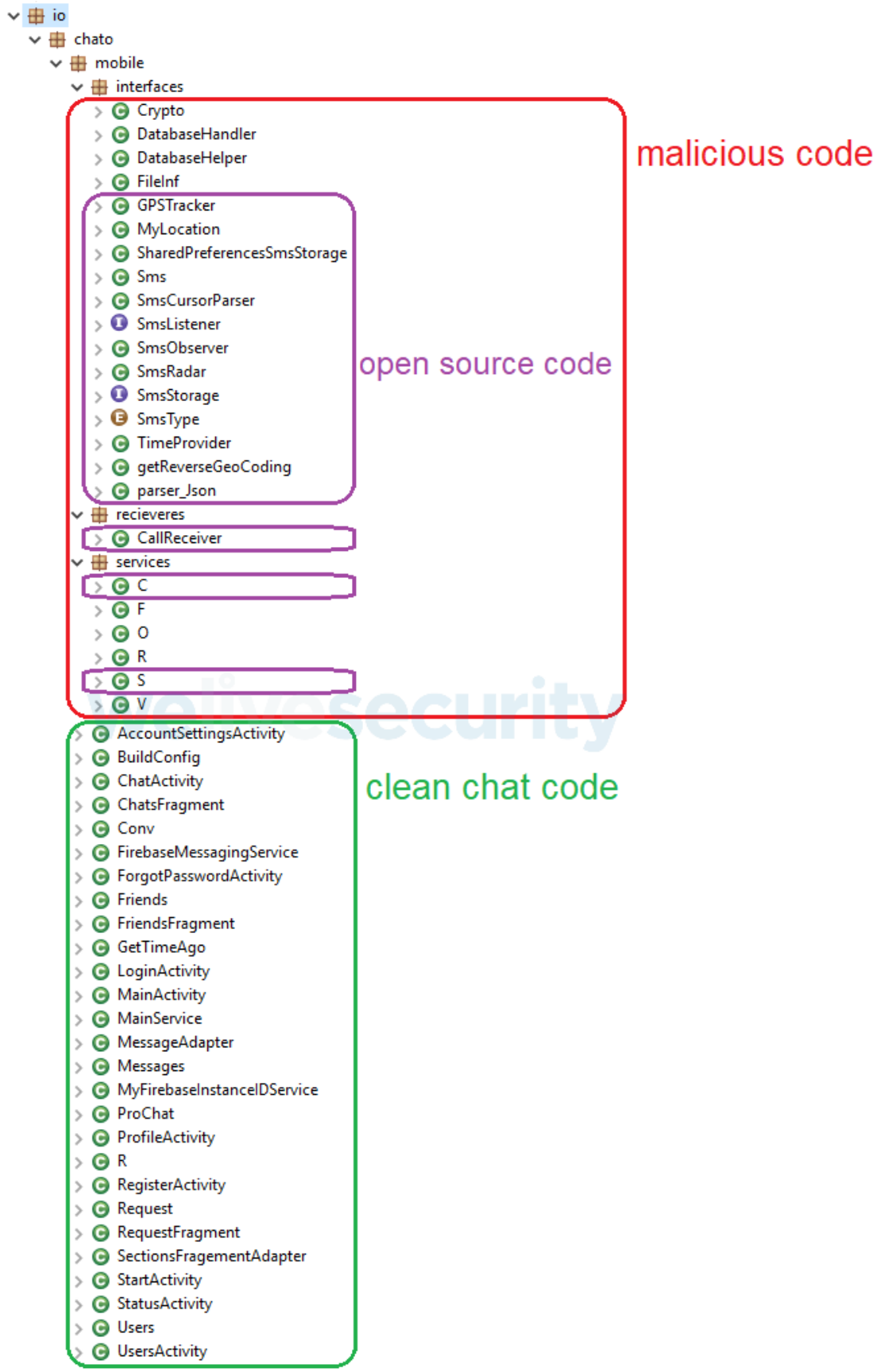

Figure 5. The developer used different pieces of open source code to create the malicious app

In some cases, the copied open source code is quite old – see Table 1. As a possible explanation, all the listed examples come at the very top among the results of simple googling for the respective functionalities.

Table 1. The origins of the malicious code

Functionality	Source	Age (years)
Call recording	open source, GitHub	8
SMS stealing	open source, GitHub	6
Google Maps coordinates	open source, Blogspot (plus other sources)	5
GEO tracking	open source, GitHub	8
GPS tracking	open source, GitHub	5

User data leak

The Welcome Chat app, including its infrastructure, was not built with security in mind. The app uploads all of the user's stolen data to the attacker-controlled server via unsecured HTTP.

Transmitted data is not encrypted and because of that, not only it is available to the attacker, it is freely accessible to anyone on the same network.

The database contains data such as name, email, phone number, device token, profile picture, messages and friends list – in fact, all the users' data except for the account passwords can be found uploaded to the unsecured server.

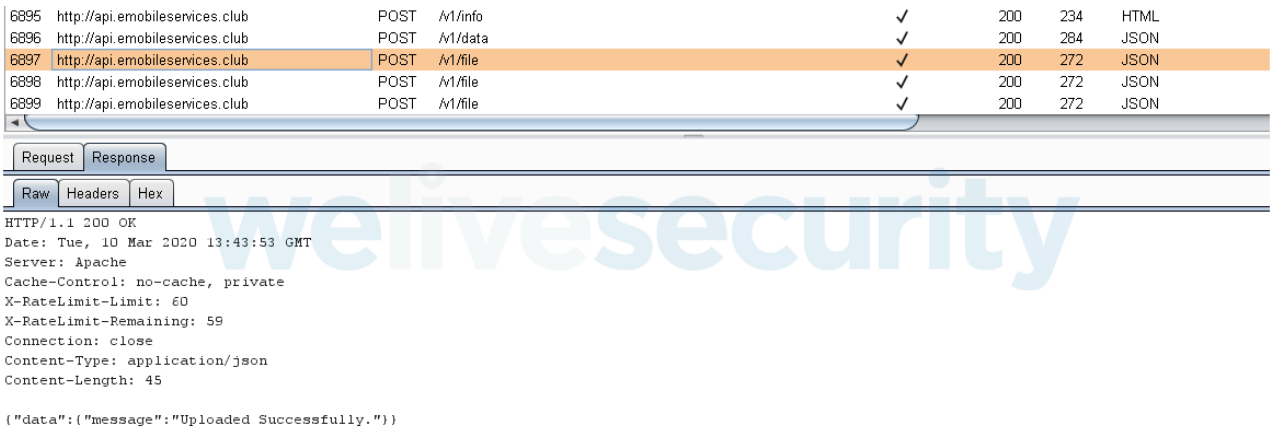

Figure 6. The victim's device uploads the user data to the app's server

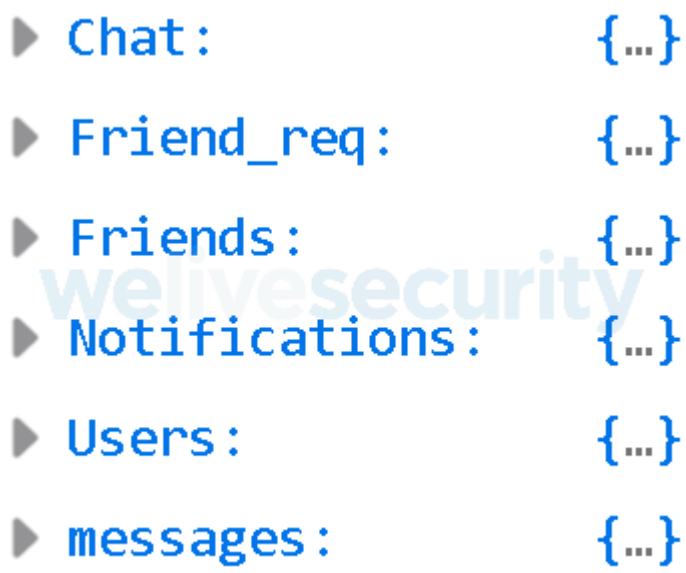

Figure 7. User database leak

Figure 8. Leaked user info

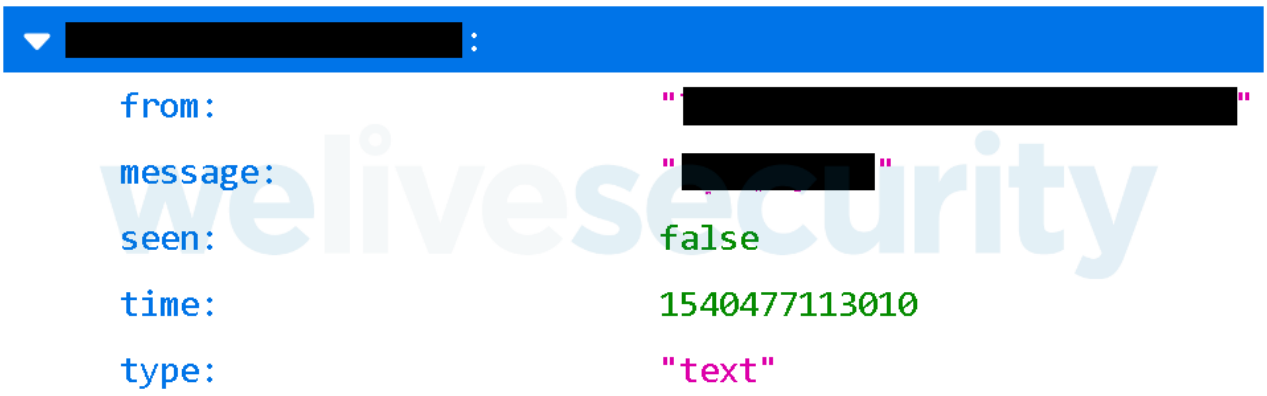

Figure 9. An example of an in-app message being freely accessible on the app's unsecured server

Once we discovered the sensitive information as being publicly accessible, we intensified our efforts to discover the developer of the legitimate chat app (i.e., the app the espionage tool was – eventually – a trojanized version of) to disclose the vulnerability to them. We

found neither the developer nor the app, convincing us that the app was built from the beginning as malicious. Naturally, we made no effort to reach out to the malicious actors behind the app.

Possible BadPatch connection

The Welcome Chat espionage app belongs to the very same Android malware family that we identified at the beginning of 2018. That malware used the same C&C server, pal4u.net, as the espionage campaign targeting the Middle East that was identified in late 2017 by Palo Alto Networks and named BadPatch. In late 2019, Fortinet described yet another espionage operation focused on Palestinian targets with the domain pal4u.net among its indicators of compromise.

For these reasons we believe that this campaign with new Android trojans comes from the threat actors behind the long-term BadPatch campaign.

Recommendation

While the Welcome Chat-based espionage operation seems to be narrowly targeted, we strongly recommend that users don't install any apps from outside the official Google Play store – unless it's a trusted source such as a website of an established security vendor or some reputable financial institution. On top of that, users should pay attention to what permissions their apps require and be suspicious of any apps that require permissions beyond their functionality – and, as a very basic security measure, run a reputable security app on their mobile devices.

Indicators of Compromise (IoCs)

Hash	ESET detection name
C60D7134B05B34AF08023155EAB3B38CEDE4BCCD	Android/Spy.Agent.ALY
C755D37D6692C650692F4C637AE83EF6BB9577FC	Android/Spy.Agent.ALY
89AB73D4AAF41CBCDBD0C8C7D6D85D21D93ED199	Android/Spy.Agent.ALY
2905F2F60D57FBF13D25828EF635CA1CCE81E757	Android/Spy.Agent.ALY

C&C: emobileservices.club

MITRE ATT&CK techniques

Tactic	ID	Name	Description

Tactic	ID	Name	Description
Initial Access	T1444	Masquerade as Legitimate Application	Welcome Chat impersonates a legitimate chat application.
Persistence	T1402	App Auto-Start at Device Boot	Welcome Chat listens for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts.
Discovery	T1426	System Information Discovery	Welcome Chat collects information about the device.
Collection	T1412	Capture SMS Messages	Welcome Chat exfiltrates sent and received SMS messages.
	T1430	Location Tracking	Welcome Chat spies on the device's location.
	T1433	Access Call Log	Welcome Chat exfiltrates call log history.
	T1432	Access Contact List	Welcome Chat exfiltrates the user contact list.
	T1429	Capture Audio	Welcome Chat records surrounding audio.
	T1533	Data from Local System	Welcome Chat steals user photos stored on device.
Command and Control	T1437	Standard Application Layer Protocol	Welcome Chat uploads exfiltrated data using the HTTP protocol.

Lukas Stefanko
14 Jul 2020 - 11:30AM

Newsletter