
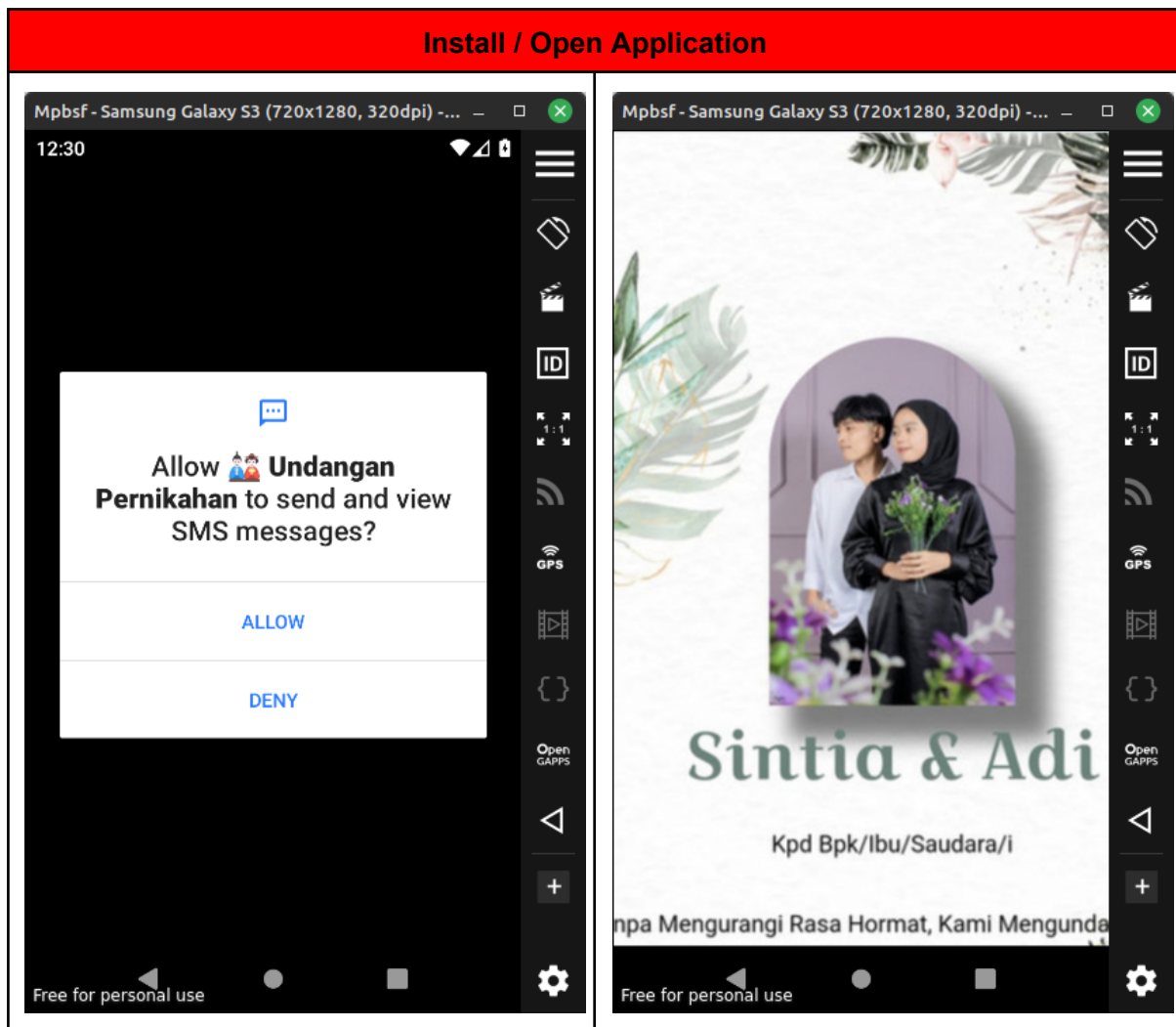


KELASTAMBAHkelastambah@gmail.com**ANALISIS^(v1.1) APLIKASI MALWARE UNDANGAN PERNIKAHAN****FILE INFORMATION**

File Name	UNDANGAN DARI SINTYA.apk
Size	5.53 MB (5799519)
MD5	dd8c96c00dafec64a609d501160753c9
SHA1	28c7e939761c9539e955a55a26668d3f34e3ee6e
SHA256	1ad75a0dcb204a7941d4de6024153d4c1fb07f4387dbfdbf63b2cec03690b329

APP INFORMATION

App Name	 Undangan Pernikahan
App Modify Date	2023:06:07 22:02:52
Minimal supported Android version	Oreo (8.0.0) - API level 26
Package Name	com.google.androidsmsteaT
Main Activity	Main Activity com.example.myapplication.MainActivity
Target SDK Min SDK	32 26
Android Version Name Android Version Code	1.0 1
Permissions	android.permission.INTERNET android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.READ_SMS



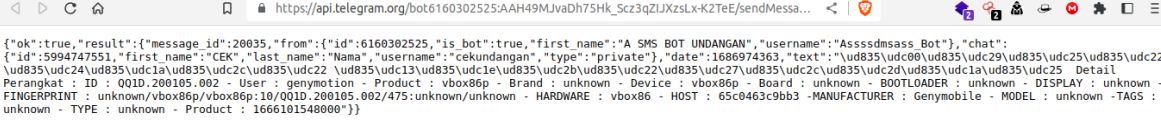
Isi dari aplikasi tersebut yang nampak hanya webview gambar yang diposting pada <https://postimages.org/> ['https://i.postimg.cc/DzRpNYpQ/Screenshot-20230310-140055-Chrome.jpg'].



Setelah di install, aplikasi tersebut berjalan dilatar belakang dan aplikasi tersebut tidak ada / nampak pada home / menu aplikasi. Hal ini menyebabkan banyak orang awam yang tidak mengetahui bahwa perangkatnya telah terinstall malware.

Aplikasi ini juga berjalan startup / otomatis berjalan ketika perangkat dihidupkan dari keadaan mati.

Aplikasi tersebut meng-collect data dan dikirim melalui bot telegram ke telegram pelaku.



```

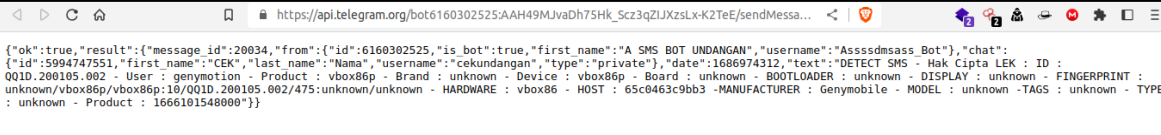
{"ok":true,"result":{"message_id":20035,"from":{"id":6160302525,"is_bot":true,"first_name":"A SMS BOT UNDANGAN","username":"Asssssdmsass_Bot"},"chat":{"id":5994747551,"first_name":"CEK","last_name":"Nama","username":"cekundangan","type":"private"},"date":1686974363,"text":"\ud835\udc00\ud835\udc29\ud835\udc25\ud835\udc22\ud835\udc24\ud835\udc1a\ud835\udc2c\ud835\udc22\ud835\udc13\ud835\udc1e\ud835\udc2b\ud835\udc22\ud835\udc27\ud835\udc2c\ud835\udc2d\ud835\udc1a\ud835\udc25 Detail Perangkat : ID : QQ1D.200105.002 - User : genymotion - Product : vbox86p - Brand : unknown - Device : vbox86p - Board : unknown - BOOTLOADER : unknown - DISPLAY : unknown - FINGERPRINT : unknown/vbox86p/vbox86p:10/QQ1D.200105.002/475:unknown/unknown - HARDWARE : vbox86 - HOST : 65c0463c9bb3 -MANUFACTURER : Genymobile - MODEL : unknown -TAGS : unknown - TYPE : unknown - Product : 1666101548000"}}

```

```

{"ok":true,"result":{"message_id":20056,"from":{"id":6160302525,"is_bot":true,"first_name":"A SMS BOT UNDANGAN","username":"Asssssdmsass_Bot"},"chat":{"id":5994747551,"first_name":"CEK","last_name":"Nama","username":"cekundangan","type":"private"},"date":1686975129,"text":"\ud835\udc00\ud835\udc29\ud835\udc25\ud835\udc22\ud835\udc24\ud835\udc1a\ud835\udc2c\ud835\udc22\ud835\udc13\ud835\udc1e\ud835\udc2b\ud835\udc22\ud835\udc27\ud835\udc2c\ud835\udc2d\ud835\udc1a\ud835\udc25 Detail Perangkat : ID : QQ1D.200105.002 - User : genymotion - Product : vbox86p - Brand : unknown - Device : vbox86p - Board : unknown - BOOTLOADER : unknown - DISPLAY : unknown - FINGERPRINT : unknown/vbox86p/vbox86p:10/QQ1D.200105.002/475:unknown/unknown - HARDWARE : vbox86 - HOST : 65c0463c9bb3 -MANUFACTURER : Genymobile - MODEL : unknown -TAGS : unknown - TYPE : unknown - Product : 1666101548000"}}

```



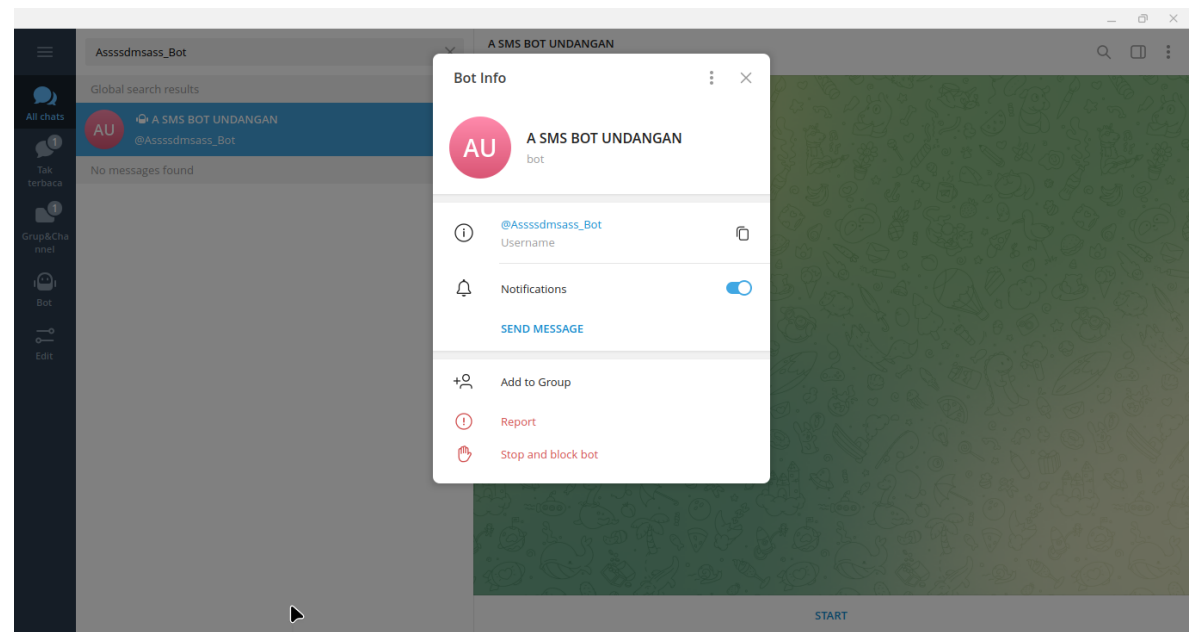
```

{"ok":true,"result":{"message_id":20034,"from":{"id":6160302525,"is_bot":true,"first_name":"A SMS BOT UNDANGAN","username":"Asssssdmsass_Bot"},"chat":{"id":5994747551,"first_name":"CEK","last_name":"Nama","username":"cekundangan","type":"private"},"date":1686974312,"text":"DETECT SMS - Hak Cipta LEK : ID : QQ1D.200105.002 - User : genymotion - Product : vbox86p - Brand : unknown - Device : vbox86p - Board : unknown - BOOTLOADER : unknown - DISPLAY : unknown - FINGERPRINT : unknown/vbox86p/vbox86p:10/QQ1D.200105.002/475:unknown/unknown - HARDWARE : vbox86 - HOST : 65c0463c9bb3 -MANUFACTURER : Genymobile - MODEL : unknown -TAGS : unknown - TYPE : unknown - Product : 1666101548000"}}

```

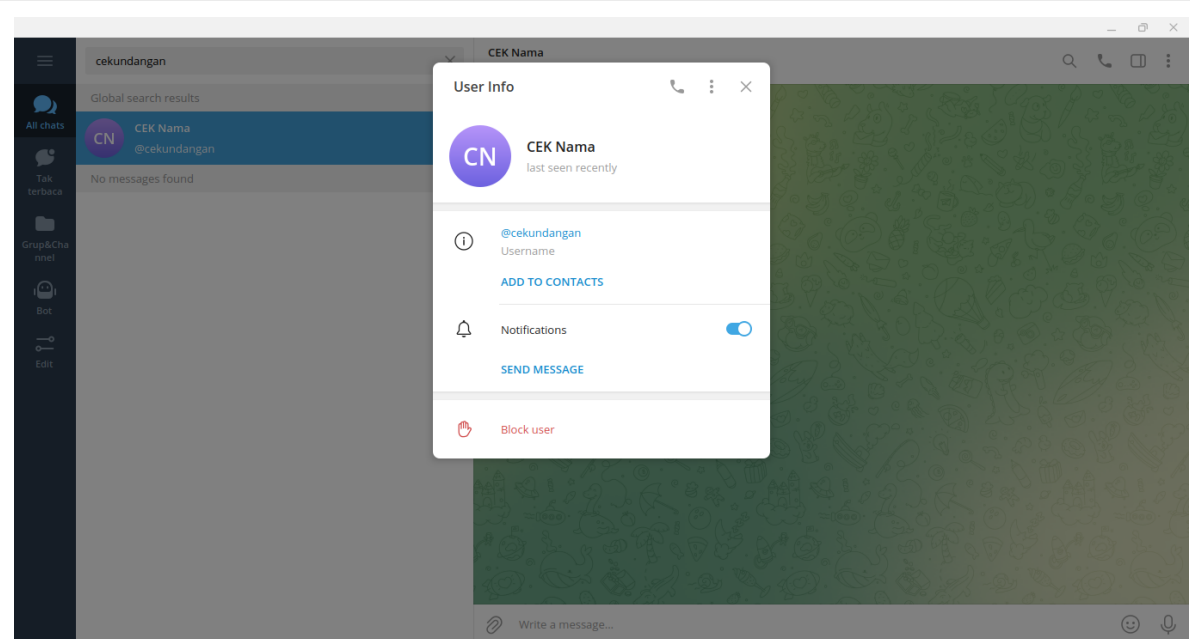
Informasi Bot Telegram Pelaku

```
{"ok":true,"result":{"id":6160302525,"is_bot":true,"first_name":"A SMS BOT UNDANGAN","username":"Assssdmsass_Bot","can_join_groups":true,"can_read_all_group_messages":false,"supports_inline_queries":false}}
```



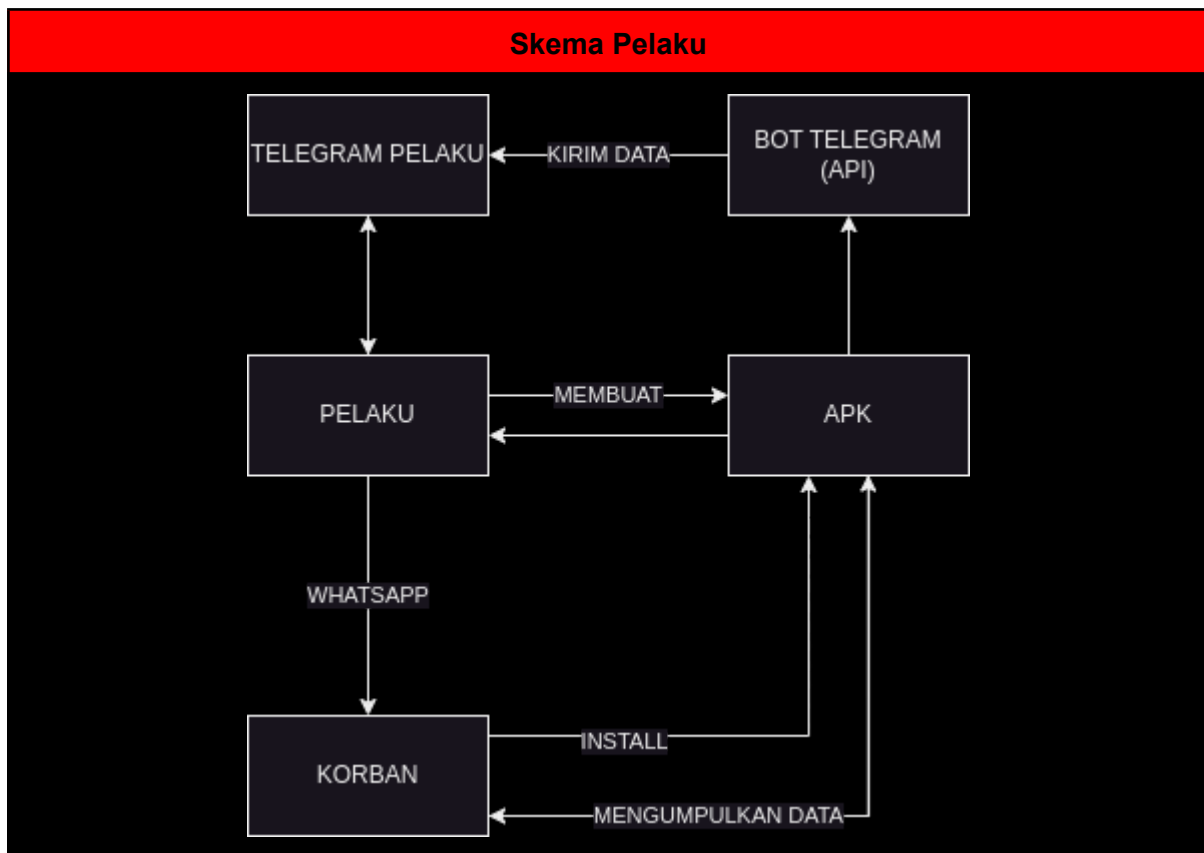
Informasi Telegram Pelaku

```
"id":5994747551,"first_name":"CEK","last_name":"Nama","username":"cekundangan"
```



Berikut adalah data yang dikirimkan kepada bot tersebut.

- **ID:** ID unik dari build sistem operasi Android dan unique device ID (IMEI, MEID or ESN).
- **User:** Nama pengguna atau profil yang digunakan.
- **Product:** Nama produk atau model perangkat.
- **Brand:** Nama merek perangkat.
- **Device:** Nama perangkat atau versi.
- **Board:** Nama board perangkat.
- **BOOTLOADER:** Versi bootloader perangkat.
- **DISPLAY:** Berisi informasi tentang display perangkat.
- **FINGERPRINT:** ID unik yang dibuat oleh sistem operasi berdasarkan beberapa informasi perangkat, termasuk versi sistem operasi, model perangkat, dll.
- **HARDWARE:** Jenis perangkat keras yang digunakan.
- **HOST:** Nama atau ID host tempat perangkat lunak di-build.
- **MANUFACTURER:** Informasi nama pabrikan atau produsen.
- **MODEL:** Model perangkat.
- **TAGS:** Berisi tag atau penanda tambahan untuk perangkat atau build.
- **TYPE:** Berisi informasi tambahan tentang jenis perangkat atau perangkat keras, , seperti smartphone, tablet, atau smartwatch.
- **Product:** ID produk lainnya atau timestamp, seperti nomor versi atau waktu dan tanggal kompilasi.



Penjelasan skema:

1. Pelaku menciptakan APK yang dirancang untuk mengumpulkan data korban. Ini melibatkan penulisan kode dan pengembangan aplikasi yang dapat mengekstrak informasi dari perangkat korban.
2. Setelah APK selesai dibuat, pelaku mengirimkan APK tersebut menggunakan WhatsApp kepada korban.
3. Korban menerima pesan dan mengunduh / menginstal APK.
4. Setelah APK di instal oleh korban, data korban dikumpulkan oleh APK tersebut.
5. APK menggunakan API bot Telegram untuk mengirimkan data yang dikumpulkan ke akun Telegram pelaku.
6. Pelaku menerima data korban yang dikirim oleh APK melalui bot Telegram.

Analisis Pelaku

Dari beberapa file serupa yang telah dianalisis, terungkap bahwa semua jejak mengarah pada satu bot telegram yang menjalankan operasi yang sama. Bot tersebut bertugas mengirim pesan ke satu akun telegram yang sama. Pelaku menggunakan berbagai aplikasi serupa sebagai sarana untuk mengumpulkan data korban, yang kemudian dikirimkan ke akun telegram yang telah disebutkan. Sasaran utama dari serangan ini adalah pengguna

WhatsApp. Agar dapat mencapai tujuannya, pelaku menggunakan berbagai nomor WhatsApp yang berbeda dan menggunakan aplikasi berbeda tapi serupa dalam melancarkan aksinya.

Selain mengirim data ke bot telegram, aplikasi tersebut juga berbahaya. Aplikasi tersebut dapat mencuri dan mendapatkan akses ke kredensial pengguna seperti nama pengguna dan kata sandi, melakukan eksplorasi terhadap jaringan dan sistem untuk mencari informasi target, mengumpulkan informasi pribadi seperti lokasi perangkat, informasi jaringan, dan pesan teks, berkomunikasi dengan server yang dikendalikan oleh penyerang untuk menerima instruksi dan mengirimkan data yang dikumpulkan, mengalihkan panggilan telepon dan pesan teks ke tujuan yang tidak sah melalui eksploitasi kerentanan jaringan, serta menyebabkan dampak negatif seperti penghapusan data perangkat, penipuan tagihan operator telekomunikasi, atau kegiatan jahat lainnya yang dapat menyebabkan kerugian finansial atau kerugian lainnya.

Analisis	
System Summary	<ul style="list-style-type: none">• Requests potentially dangerous permissions• Reads shares settings• Classification label
Data Obfuscation	<ul style="list-style-type: none">• Uses reflection
Persistence and Installation Behavior	<ul style="list-style-type: none">• Installs an application shortcut on the screen
Boot Survival	<ul style="list-style-type: none">• Installs a new wake lock (to get activate on phone screen on)
Hooking and other Techniques for Hiding and Protection	<ul style="list-style-type: none">• Uses Crypto APIs
Malware Analysis System Evasion	<ul style="list-style-type: none">• Accesses android OS build fields
Language, Device and Operating System Detection	<ul style="list-style-type: none">• Queries the unique device ID (IMEI, MEID or ESN)
Spreading	<ul style="list-style-type: none">• Accesses external storage location
Networking	<ul style="list-style-type: none">• Opens an internet connection• Checks an internet connection is available• Performs DNS lookups (Java API)

	<ul style="list-style-type: none"> • Uses HTTPS • Connects to IPs without corresponding DNS lookups • URLs found in memory or binary data • Performs DNS lookups • Uses secure TLS version for HTTPS connections
E-Banking Fraud	<ul style="list-style-type: none"> • Has functionality to add an overlay to other apps
Spam, unwanted Advertisements and Ransom Demands	<ul style="list-style-type: none"> • Sends SMS using SmsManager • Has permission to send SMS in the background
Operating System Destruction	<ul style="list-style-type: none"> • Lists and deletes files in the same context
Change of System Appearance	<ul style="list-style-type: none"> • May access the Android keyguard (lock screen) • Acquires a wake lock
Stealing of Sensitive Information	<ul style="list-style-type: none"> • Parses SMS data (e.g. originating address) • Has permission to receive SMS in the background • Has permission to read the SMS storage • Monitors incoming SMS • Reads boot loader settings of the device • Creates SMS data (e.g. PDU) • May take a camera picture
Remote Access Functionality	<ul style="list-style-type: none"> • Found parser code for incoming SMS (may be used to act on incoming SMS, BOT) • Found suspicious command strings (may be related to BOT commands)
Location Tracking	<ul style="list-style-type: none"> • Queries the phones location (GPS)
Analysis Advice	<ul style="list-style-type: none"> • Unable to instrument or execute APK, runtime error occurred • Unable to instrument or execute APK, no dynamic information has been logged
Compliance	<ul style="list-style-type: none"> • Uses secure TLS version for HTTPS connections

Mitre Attack	
Credential Access	<ul style="list-style-type: none"> • T1412 Capture SMS Messages
Discovery	<ul style="list-style-type: none"> • T1421 System Network Connections Discovery • T1430 Location Tracking • T1426 System Information Discovery
Collection	<ul style="list-style-type: none"> • T1430 Location Tracking • T1507 Network Information Discovery

	<ul style="list-style-type: none">• T1412 Capture SMS Messages
Command and Control	<ul style="list-style-type: none">• T1573 Encrypted Channel• T1095 Non-Application Layer Protocol• T1071 Application Layer Protocol
Network Effects	<ul style="list-style-type: none">• T1449 Exploit SS7 to Redirect Phone Calls/SMS
Impact	<ul style="list-style-type: none">• T1447 Delete Device Data• T1448 Carrier Billing Fraud

Berikut penjelasan tentang ancaman malware aplikasi tersebut.

1. Credential Access: Ancaman ini mengacu pada kemampuan malware untuk mencuri dan mendapatkan akses ke kredensial pengguna, seperti nama pengguna, kata sandi, atau informasi otentikasi lainnya. Hal ini dapat menyebabkan pencurian identitas, penyalahgunaan akun, atau akses tidak sah ke sistem dan layanan.

2. Discovery: Ancaman ini melibatkan upaya malware untuk mengeksplorasi jaringan dan sistem yang terinfeksi guna mendapatkan informasi lebih lanjut tentang targetnya. Ini termasuk pencarian dan pemetaan koneksi jaringan, melacak lokasi perangkat, serta mengumpulkan informasi sistem dan jaringan lainnya. Tujuan utama dari tahap ini adalah untuk memahami lingkungan target dan mengidentifikasi potensi sasaran yang rentan.

3. Collection: Ancaman ini mencakup proses pengumpulan informasi yang dilakukan oleh malware setelah berhasil masuk ke dalam sistem atau perangkat. Ini bisa mencakup pencurian informasi pribadi, termasuk pelacakan lokasi perangkat, pengumpulan informasi jaringan, dan pemantauan pesan teks (SMS). Informasi yang dikumpulkan dapat digunakan untuk kegiatan jahat seperti penipuan atau penyalahgunaan data.

4. Command and Control: Ancaman ini terkait dengan kemampuan malware untuk berkomunikasi dengan server yang dikendalikan oleh penyerang, yang disebut sebagai Command and Control (C2). Melalui saluran enkripsi atau protokol lapisan aplikasi, malware dapat menerima instruksi dan mengirimkan data yang dikumpulkan ke penyerang. Ini memungkinkan penyerang untuk mengendalikan malware dan memanfaatkannya untuk tujuan jahat.

5. Network Effects: Ancaman ini melibatkan eksploitasi kerentanan dalam jaringan telekomunikasi, seperti protokol SS7, untuk mengalihkan panggilan telepon atau pesan teks (SMS) ke tujuan yang tidak sah. Ini dapat dimanfaatkan untuk menyebabkan gangguan komunikasi, melakukan serangan phishing, atau mendapatkan akses ke informasi pribadi pengguna.

6. Impact: Ancaman ini mencakup dampak negatif yang dihasilkan oleh malware setelah berhasil melakukan serangan. Salah satu dampaknya adalah penghapusan data perangkat, dimana malware dapat menghapus informasi penting atau menghapus seluruh data dari perangkat. Ancaman lainnya adalah penipuan tagihan operator telekomunikasi, di mana malware dapat memanfaatkan layanan pembayaran operator untuk mendapatkan keuntungan finansial secara tidak sah.

Security vendors' analysis	
Security vendors	Malware
AhnLab-V3	PUP/Android.FLPprev.1174132
Antiy-AVL	Trojan/Generic.ASMalwAD.63
Avira (no cloud)	ANDROID/SpyAgent.YKY.Gen
Cynet	Malicious (score: 99)
DrWeb	Android.SmsSpy.888.origin
F-Secure	Malware.ANDROID/SpyAgent.YKY.Gen
Google	Detected
K7GW	Trojan (005a3c221)
Lionic	Trojan.AndroidOS.SmsThief.C!c
McAfee	Artemis!DD8C96C00DAF
Microsoft	Trojan:AndroidOS/Smsthief.F!MTB
Sophos	Andr/SMSSpy-FJ
Symantec Mobile Insight	AppRisk:Generisk
Alibaba	TrojanSpy:Android/Smsthief.2c1106f3
Avast-Mobile	Android:Evo-gen [Trj]
BitDefenderFalx	Android.Trojan.SmsSpy.AEF
Cyren	AndroidOS/ABRisk.OFXZ-4
ESET-NOD32	A Variant Of Android/Spy.SmsSpy.YA
Fortinet	Android/SmsSpy.YA!tr
Ikarus	Trojan-Spy.AndroidOS.SMSSpy
Kaspersky	HEUR:Trojan-Spy.AndroidOS.SmsThief.tw
MAX	Malware (ai Score=99)
McAfee-GW-Edition	Artemis!Trojan
NANO-Antivirus	Trojan.Android.SmsSpy.junlyr

Symantec	Trojan.Gen.MBT
Trustlook	Android.Malware.Spyware