SAFEnet



INSTALLAH AKU KAU KUMATA-MATAI

Melacak Asal dan Arah Aplikasi Penipuan Melalui APK

Laporan Penelitian

Installah Aku, Kau Kumata-matai

Melacak asal dan arah aplikasi penipuan melalui APK

SAFEnet

Oktober 2023

Installah Aku, Kau Kumata-matai

Melacak asal dan arah aplikasi penipuan melalui APK

Tim Peneliti:
Andreas Takimai (Peneliti Utama)
Abul Hasan Banimal
Ardy Wibisana

Penyelia & Penyunting:
Anton Muhajir

Desainer & Tata Letak:
Syaifullah

Oktober 2023

Penerbit
Southeast Asia Freedom of Expression Network (SAFEnet)
Jalan Gita Sura III Nomor 55 Peguyangan Kaja
Denpasar, Bali 80115

+62 811 9223375
info@safenet.or.id
@safenetvoice
safenet.or.id

Laporan ini menggunakan lisensi Creative Commons Attribution-NonCommercial 4.0 (CC BY-NC 4.0). Anda bebas untuk untuk mendistribusikan, mencampur ulang, mengadaptasi, dan membuat materi dalam media atau format apa pun hanya untuk tujuan nonkomersial, dan hanya selama atribusi diberikan kepada pencipta. Informasi lebih lanjut di https://creativecommons.org/licenses/by-nc/4.0/

DAFTAR ISI

Daftar Isi 1

1. Pengantar 2

2. Analisis 4

2.2 Analisis APK 9

2.2.1. Analisis dengan Virus Total 9

2.2.2. Pengecekan Aset APK 10

2.2.3. Pengecekan ponsel korban 13

2.2.3.1. Penelusuran manual pada perangkat 13

2.2.3.2. Penelusuran dengan alat analisis 14

2.3. Memahami cara APK 16

2.3.1 Pengakuan korban 16

2.3.2. Melalui pengecekan APK terpasang 16

2.3.3. Melalui simulasi 16

2.3.4. APK menyembunyikan diri 18

2.4. Melacak pelaku 20

2.4.1. Mesin pembuat APK 20

2.4.2. Telegram bot 21

2.4.3. Melacak alamat IP 22

2.5. Cara mencabut APK 24

3. Penutup 25

4. Catatan kaki 26

1. PENGANTAR

Satu tahun terakhir beredar metode baru serangan digital dalam bentuk pemancingan (*phishing*) melalui berkas dengan ekstensi APK (aplikasi). Berkas atau fail ini terutama dikirim ke platform percakapan WhatsApp. Demikian juga yang terjadi di berbagai grup WhatsApp beranggotakan orang-orang Papua. Secara berantai pengiriman itu terjadi dalam jangka waktu lima bulan sejak Mei hingga September 2023. Serangan ini masih terus terjadi, meskipun sudah tidak sesering lima bulan tersebut.

Beberapa pengguna WhatsApp langsung terpancing mengunduh dan membuka berkas aplikasi tersebut, tetapi ada juga yang tidak. Mereka yang membuka langsung kaget karena tiba-tiba tanpa sadar nomornya kemudian meneruskan pesan berisi aplikasi tersebut ke beberapa grup WhatsApp di mana dia ikut. Karena takut, ada yang menghapus aplikasi WhatsApp dan memasang (instal) ulang. Setelah itu, rasanya masalah sudah terselesaikan. Namun, korban yang tidak menyadari akan melanjutkan ke tahap berikut yaitu mengunjungi alamat web pengalihannya, lalu memasukkan nomor ponselnya di sana. Mereka pun jadi korban. Pada kasus lain (bukan orang Papua yang menjadi sasaran riset ini) salah satu korban harus kehilangan hingga Rp 1,4 miliar.[1] Uangnya hilang begitu saja. Ia terkejut karena mendapatkan notifikasi jika uangnya telah ditarik.

Modus penipuan dengan cara sama juga pernah terjadi akhir tahun lalu. Beberapa praktisi keamanan digital, seperti Nikko Enggaliano[2] dan Teguh Aprianto[3], telah menganalisis dan membongkar penipuan menggunakan APK tersebut. Berdasarkan temuan mereka, penipuan dilakukan dengan berpura-pura mengirim pesan kepada korban untuk melihat foto pengiriman paket J&T dan penipuan cek resi J&T. Menurut temuan mereka, APK dibangun langsung oleh pelaku dan terhubung dengan *server* milik pelaku. Sehingga, informasi yang didapat dari ponsel korban langsung dikirm ke *server* pelaku. Proses pembuatan APK tersebut juga tanpa layanan aplikasi lain, tetapi hanya disembunyikan atau di-*encode* dengan Base64. Tidak seperti dalam temuan ini di mana pelaku menggunakan Telegram bot untuk memodifikasi APK yang tersedia di laman terbuka dan menerima informasi tentang perangkat dan pesan singkat (SMS) di sana. Mereka memanfaatkan *tools* yang tersedia di Github dan mengubah penerimaan informasi melalui Telegram bot.



Berdasarkan temuan sementara, serangan melalui APK ini lebih banyak bermotif ekonomi. Pelaku akan mengincar uang korban terutama yang menggunakan aplikasi perbankan.[4] Meskipun demikian, serangan secara masif melalui grup-grup WhatsApp orang Papua tetap perlu diwaspadai dan diperiksa lebih lanjut. Untuk itulah kami melakukan pemeriksaan lebih mendalam terhadap serangan APK kepada orang-orang Papua tersebut.

Melalui pemeriksaan tersebut, kami ingin mencapai tiga hal. Pertama, menemukan metode dan korban serangan digital melalui APK terhadap orang-orang Papua. Kedua, mengetahui isi APK yang disebarluaskan melalui grup-grup Whatsapp orang Papua. Ketiga, memberi wawasan dan jawaban agar korban dapat menemukan dan mengatasi sendiri jika mengalami serangan termasuk memeriksa perangkatnya secara mandiri.



1.1. Metodologi

Untuk menjawab pertanyaan kunci, dari mana pengirim APK dan apa motifnya, peneliti mengidentifikasi melalui beberapa tahap, yaitu:

- Pertama, mengumpulkan data dari 13 grup milik orang Papua. Selain itu, langsung menemui korban dan mengekstrak data dari gawai.
- Kedua, mengidentifikasi sumber aplikasi dengan teknik *open source intelligent* (OSINT) untuk mencari tahu lebih banyak informasi.
- Ketiga, membandingkan dengan simulasi cara kerja dari pembahasan sumber lain mengenai hal terkait pada aplikasi yang sama. Pembahasan ini menggunakan metode yang tidak teknis guna memudahkan pembaca terutama agar dapat memahami orang awam dan mempraktikkan solusi secara mandiri.

1.2. Temuan

Setelah melakukan penyelidikan, ditemukan beberapa hal, yaitu:

- Aplikasi ini disebarkan dengan mengirimkan langsung dan ada juga yang meneruskan. Setiap aplikasi yang dikirim ada yang dibubuhi komentar pancingan. Ada juga kiriman pesan tanpa komentar, tetapi tidak dalam jumlah besar.
- Ada 19 aplikasi dengan nama berbeda yang dibagikan di berbagai grup milik orang Papua.
- Beberapa korban mengaku aplikasi tersebut terkirim dari perangkat korban tanpa dia ketahui ke beberapa grup yang ia tergabung.
- Telegram digunakan sebagai pembuat aplikasi penipuan dan pengintai tersebut.
- Aplikasi tersebut hanya menargetkan mengakses pesan ringkas (SMS) dan internet untuk mengintai aktivitas pengiriman SMS yang dilakukan pada perangkat.
- Melalui Telegram Bot pembuat dapat menerima setiap SMS yang masuk di ponsel korban.
- Pembuat menggunakan beberapa blog untuk mengalihkan korban saat melakukan klik. Alamat IP-nya teridentifikasi sering melakukan kejahatan maya.

2. ANALISIS

2.1. Penyebaran APK

Android Package Kit yang disingkat apk atau APK adalah format berkas (*file*) yang digunakan di sistem operasi Android. APK menjadi ekstensi pada sebuah berkas dengan nama namaberkas. apk. Sebagai perangkat lunak, berkas ini biasa digunakan untuk aplikasi baik maupun buruk. Dalam kasus penipuan, dia berisi aplikasi jahat untuk tujuan macam-macam, terutama mendapatkan data-data pribadi korban.

Penyebaran APK ini pula yang terjadi ke beberapa grup WhatsApp warga, mahasiswa, dan aktivis Papua. Misalnya grup warga Papua yang menjadi sasaran adalah grup *INFO KEJADIAN TERKINI, LINTAS INFORMASI TIMIKA, LINTAS INFORMASI TOLIKARA,* dan sebagainya. Sedangkan grup mahasiswa Papua sasarannya adalah grup *MAHASISWA PAPUA SE-DUNIA* dan beberapa grup paguyuban. Sedangkan pada grup aktivis Papua, APK ini menyasar grup dengan nama *Ruang Diskusi Papua, WEST PAPUA,* dan lain-lain. Secara keseluruhan, ada lebih dari 15 grup WhatsApp yang menjadi sasaran pengiriman. Namun, yang menjadi objek penelitian hanya 13 grup.

No	Nama APK	Tanggal Dikirim	Waktu	Grup Sasaran	Keterangan Pengiriman
1	DAFTAR-DJP	30-Mei-23	22:09	grup A	-
2	DAFTAR-DJP	30-Mei-23	21:55	grup A	-
3	DAFTAR-DJP	30-Mei-23	21:56	grup B	-
4	DAFTAR-DJP	30-Mei-23	22:09	grup B	-
5	DAFTAR-DJP	30-Mei-23		grup A	-
6	cek.bpjs.kesehatan	31-Mei-23		grup I	-
7	DAFTAR-DJP	31-Mei-23		grup A	-
8	DAFTAR-DJP	31-Mei-23		grup C	-
9	DAFTAR-DJP	31-Mei-23	2:08	grup K	-
10	DAFTAR-DJP	31-Mei-23		grup D	-
11	DAFTAR.DJP.MPAJAK_sign	31-Mei-23	10:36	grup H	-
12	DAFTAR.DJP.MPAJAK_sign	31-Mei-23	10:35	grup M	-
13	DAFTAR-DJP	1-Jun-23		grup D	-
14	CEK DATA	1-Jun-23		grup D	-
15	DAFTAR.DJP.MPAJAK_sign	1-Jun-23	21:42	grup A	-

16	DAFTAR.DJP.MPAJAK_sign	1-Jun-23	22:06	grup C	-
17	DAFTAR.DJP.MPAJAK_sign	1-Jun-23	21:54	grup I	-
18	DAFTAR.DJP.MPAJAK_sign	1-Jun-23		grup D	-
19	DAFTAR-DJP	1-Jun-23		grup F	-
20	DAFTAR-DJP	1-Jun-23		grup K	-
21	DAFTAR.DJP.MPAJAK_sign	2-Jun-23	12:05	grup E	-
22	DAFTAR.DJP.MPAJAK_sign	2-Jun-23		grup C	-
23	CEK DATA	2-Jun-23		grup D	-
24	DAFTAR.DJP.MPAJAK_sign	2-Jun-23	7:54	grup E	-
25	DAFTAR.DJP.MPAJAK_sign	2-Jun-23	8:06	grup F	-
26	DAFTAR.DJP.MPAJAK_sign	2-Jun-23	8:08	grup H	-
27	DAFTAR.DJP.MPAJAK_sign	2-Jun-23		grup I	-
28	DAFTAR.DJP.MPAJAK_sign	3-Jun-23		grup E	-
29	cek.bpjs.kesehatan	4-Jun-23	21:29	grup I	-
30	cek.bpjs.kesehatan	4-Jun-23	21:54	grup I	-
31	DAFTAR.DJP.MPAJAK_sign	5-Jun-23		grup D	-
32	DAFTAR.DJP.MPAJAK_sign	5-Jun-23		grup F	-
33	DAFTAR.DJP.MPAJAK_sign	5-Jun-23	11:15	grup F	-
34	DJP.Mpajak	6-Jun-23		grup M	-
35	DAFTAR.DJP.MPAJAK_sign	7-Jun-23		grup E	-
36	cek.bpjs.kesehatan	7-Jun-23		grup E	-
37	CEK DATA	8-Jun-23	17:26	grup A	-
38	DJP.Mpajak	8-Jun-23		grup L	Ini untuk pendaftaran kerja iya kk
39	DJP.Mpajak	8-Jun-23		grup A	-
40	DJP.Mpajak	8-Jun-23	19:57	grup I	Ini untuk pendaftaran kerja iya kk
41	DAFTAR.DJP.MPAJAK_sign	8-Jun-23		grup A	-
42	DJP.Mpajak	9-Jun-23		grup I	-
43	Cek Data	9-Jun-23		grup L	-
44	DAFTAR.DJP.MPAJAK_sign	9-Jun-23	19:50	grup A	-
45	DAFTAR.DJP.MPAJAK_sign	9-Jun-23	19:54	grup G	-
46	DAFTAR.DJP.MPAJAK_sign	9-Jun-23	19:55	grup I	-
47	DAFTAR.DJP.MPAJAK_sign	11-Jun-23		grup C	-
48	apk.djmpmpajak	12-Jun-23	13:25	grup F	-
49	CEK TIKET	19-Jun-23	20:12	grup A	-
50	CEK TIKET	19-Jun-23		grup C	-
51	undangan pernikahan	19-Jun-23		grup H	-
52	DJP.Mpajak-1	19-Jun-23		grup I	Ini untuk pendaftaran lowongan kerja
53	apk.djmpmpajak	19-Jun-23	23:11	grup A	-
54	apk.djmpmpajak	19-Jun-23	23:34	grup B	-
55	apk.djmpmpajak	19-Jun-23	23:10	grup F	-

57	undangan pernikahan	20-Jun-23	8:20	grup H	Ketua hadir di acara ini nanti
58	undangan pernikahan	20-Jun-23	6:26	grup H	-
59	DAFTAR-DJP-14	21-Jun-23	22:57	grup B	-
60	DAFTAR-DJP-14	21-Jun-23		grup H	-
61	CEK TIKET	21-Jun-23		grup L	-
62	cek.bpjs.kesehatan	21-Jun-23		grup C	-
63	DAFTAR.DJP.MPAJAK_sign	22-Jun-23		grup D	-
64	DAFTAR.DJP.MPAJAK_sign-4	22-Jun-23		grup H	-
65	INFO DATA	22-Jun-23		grup G	-
66	INFO DATA	22-Jun-23		grup M	-
67	DAFTAR.DJP.MPAJAK_sign-27	26-Jun-23	19:48	grup E	-
68	DAFTAR.DJP.MPAJAK_sign-31	26-Jun-23	18:45	grup E	-
69	DAFTAR.DJP.MPAJAK_sign-6	27-Jun-23	11:57	grup E	-
70	apk-13.djpmpajak	28-Jun-23	9:51	grup D	-
71	apk-13.djpmpajak	28-Jun-23	9:50	grup I	-
72	Lihat Foto Undangan Pernikahan	29-Jun-23		grup L	-
73	UNDANGAN PERNIKAHAN PDF	30-Jun-23		grup L	-
74	DJP.Mpajak	30-Jun-23		grup E	Ini untuk pendaftaran lowongan kerja online. Untuk daftar kerja djp
75	DJP.Mpajak	30-Jun-23		grup F	-
76	DJP.Mpajak	30-Jun-23		grup K	-
77	cek.bpjs.kesehatan	30-Jun-23		grup A	-
78	DJP.Mpajak	30-Jun-23		grup E	Ini untuk pendaftaran lowongan kerja online
79	LIHAT RINCIAN	5-Jul-23		grup J	-
80	DAFTAR.DJP.MPAJAK	5-Jul-23		grup J	-
81	DAFTAR.DJP-2.MPAJAK	7-Jul-23		grup B	Ini untuk pendaftaran lowongan kerja online
82	apk.djpmpajak	8-Jul-23		grup C	-
83	DAFTAR-DJP-13	10-Jul-23		grup H	-
84	DAFTAR.DJP-4.MPAJAK	13-Jul-23		grup L	-
85	CEK DATA	13-Jul-23		grup H	-
86	Daftar-2.DJP	14-Jul-23	13:06	grup I	-
87	CEK DATA	15-Jul-23		grup A	-
88	Cek Lokasi-4	15-Jul-23		grup E	-
89	cek.bpjs.kesehatan	2-Agu-23		grup A	-
90	Cek Lokasi-2	3-Agu-23		grup E	-
91	Lihat Foto Korban Tabrakan Lari	3-Agu-23		grup E	-
92	DAFTAR.DJP.MPAJAK	3-Agu-23		grup H	-
93	cek.bpjs.kesehatan	14-Agu-23		grup A	-
94	cek.bpjs.kesehatan	15-Agu-23		grup M	-

Tabel 1. Daftar penyebaran APK di dalam grup-grup milik orang Papua.

Secara berantai, pengiriman berkas berisi APK ini dilakukan bertubi-tubi sejak 30 Mei 2023 hingga 15 Agustus 2023. APK dikirim oleh nomor sama sebanyak 3 sampai 4 kali. Ada yang dikirim dalam jangka waktu beberapa hari, tetapi ada juga yang berbeda hanya dalam hitungan detik. Misalnya nomor 0812-XXX mengirim dua macam APK sebanyak 4 kali pada tanggal berbeda: 1, 8, dan 19 Juni 2023. Nomor 0813-ZZZ mengirim pada waktu berjarak 23 menitan. Ada yang mengirim hingga dua kali di grup sama. Ada yang hanya sekali di grup berbeda. Ada juga yang mengirim hingga 3 kali dan hanya berbeda beberapa menit bahkan detik antara pengiriman satu dengan yang lain oleh nomor sama. Pengiriman tersebut terjadi hampir setiap hari dan hanya pada saat itu dan setelahnya tidak dilakukan pengiriman lagi. Hanya beberapa nomor yang melakukan pengiriman ulang lagi di hari bahkan bulan berbeda.

Berikut ini merupakan pola pengiriman yang diambil dari beberapa pengirim.

NO	NAMA APK	PENGIRIM	TANGGAL DIKIRIM	WAKTU	GRUP SASARAN
42	DJP.Mpajak	0812-WWW	9-Jun-23		grup I
79	LIHAT RINCIAN	0812-WWW	5-Jul-23		grup J
37	CEK DATA	0812-XXX	8-Jun-23	17:26	grup A
49	CEK TIKET	0812-XXX	19-Jun-23	20:12	grup A
14	CEK DATA	0812-XXX	1-Jun-23		grup D
50	CEK TIKET	0812-XXX	19-Jun-23		grup C
87	CEK DATA	0812-YYY	15-Jul-23		grup A
89	cek.bpjs.kesehatan	0812-YYY	2-Agu-23		grup A
2	DAFTAR-DJP	0813-WWW	30-Mei-23	21:55	grup A
3	DAFTAR-DJP	0813-WWW	30-Mei-23	21:56	grup B
1	DAFTAR-DJP	0813-WWW	30-Mei-23	22:09	grup A
4	DAFTAR-DJP	0813-WWW	30-Mei-23	22:09	grup B
53	apk.djmpmpajak	0853-XXX	19-Jun-23	23:11	group A
54	apk.djmpmpajak	0853-XXX	19-Jun-23	23:34	group B
55	apk.djmpmpajak	0853-XXX	19-Jun-23	23:10	group F

Tabel 2. Pola pengiriman APK ke grup sasaran.

Dari semua APK yang bisa kami kumpulkan, ada 19 macam nama berkas APK yang diedarkan. Sebagian di antaranya hampir mirip dengan menggunakan nama DJP, tetapi nama berkas lain berbeda seperti, *'Cek Lokasi', 'Lihat Foto Korban Tabrak Lari', 'Undangan Pernikahan',* hingga *'Cek Data'.* Berbagai nama yang digunakan pada dasarnya memiliki kesamaan satu sama lain. Semua aplikasi tersebut dibuat dengan cara sama.

Aplikasi tersebut disebarkan sebanyak 94 kali dalam 13 grup orang Papua. Pengiriman dilakukan baik di dalam grup masyarakat, mahasiswa hingga aktivis Papua. Aplikasi dengan nama *'DAFTAR. DJP.MPAJAK_sign'* paling banyak dikirim

hingga mencapai 27 kali. Beberapa aplikasi lain, seperti *apk.djpmpajak*, *Daftar-2.DJP*, *Lihat Foto Korban Tabrakan Lari*, *LIHAT RINCIAN*, dan *UNDANGAN PERNIKAHAN PDF* dikirim hanya sekali.

NO	NAMA APK	JUMLAH PENGIRIMAN
1	DAFTAR.DJP.MPAJAK_sign	27
2	DAFTAR-DJP	16
3	DJP.Mpajak	10
4	cek.bpjs.kesehatan	9
5	CEK DATA	6
6	apk.djmpmpajak	4
7	CEK TIKET	3
8	Lihat Foto Undangan Pernikahan	3
9	undangan pernikahan	3
10	apk-13.djpmpajak	2
11	Cek Lokasi-2	2
12	DAFTAR.DJP-2.MPAJAK	2
13	DAFTAR.DJP.MPAJAK	2
14	INFO DATA	2
15	apk.djpmpajak	1
16	Daftar-2.DJP	1
17	Lihat Foto Korban Tabrakan Lari	1
18	LIHAT RINCIAN	1
19	UNDANGAN PERNIKAHAN PDF	1

Tabel 3. Tabel jumlah pengiriman APK



Pengiriman tersebut disertai pesan-pesan untuk memancing pengguna membuka. Berikut contoh komentar pancingan, *"ini untuk pendaftaran kerja ya kk"*, *"Ini untuk pendaftaran lowongan kerja"*, dan *"Ketua hadir di acara ini nanti"*.

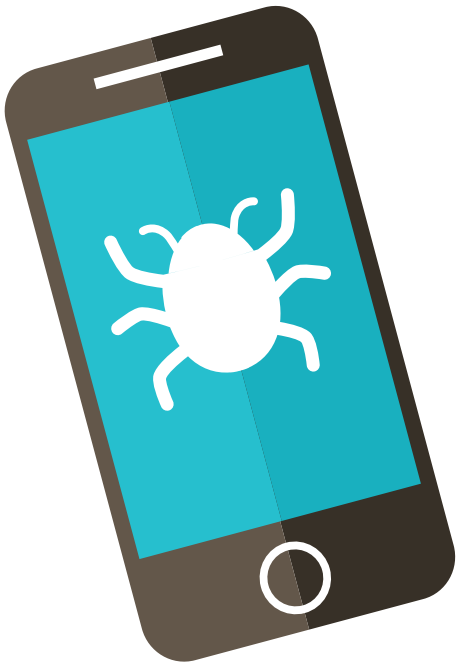


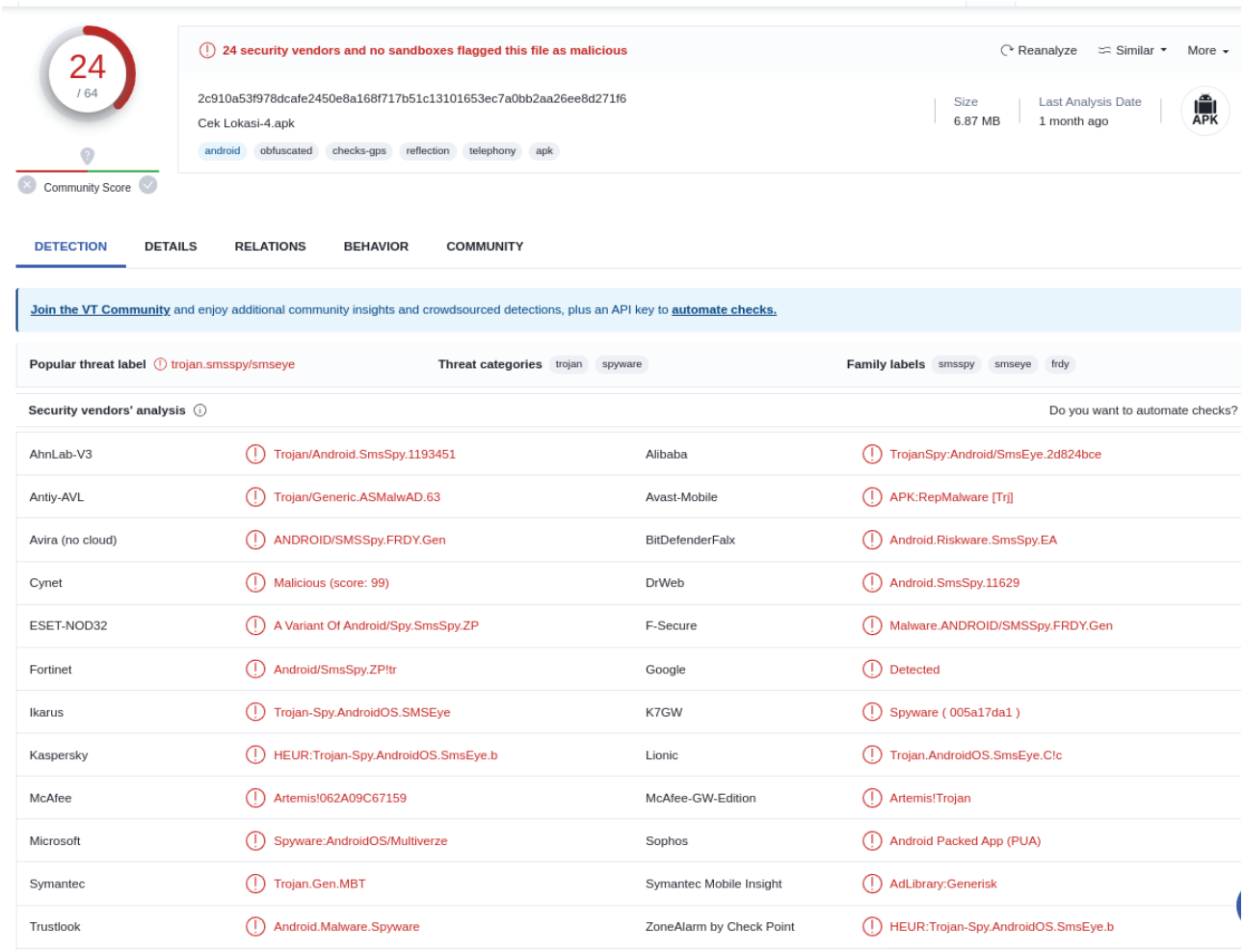
Gambar 1: Pengirim memberikan beragam balasan komentar di bawah aplikasi yang dikirim.

2.2. Analisis APK

2.2.1. Analisis dengan Virus Total

Untuk mengetahui virus apa saja yang ada di dalam aplikasi-aplikasi tersebut, kami menggunakan alat analisis bernama VirusTotal[5] dengan mengunggah file tersebut. Setelah mengunggah di sana, muncul puluhan virus berbahaya[6]. Rata-rata setiap aplikasi memiliki 20-25 virus (tulisan berwarna merah) yang muncul dari setiap analisis dengan VirusTotal.

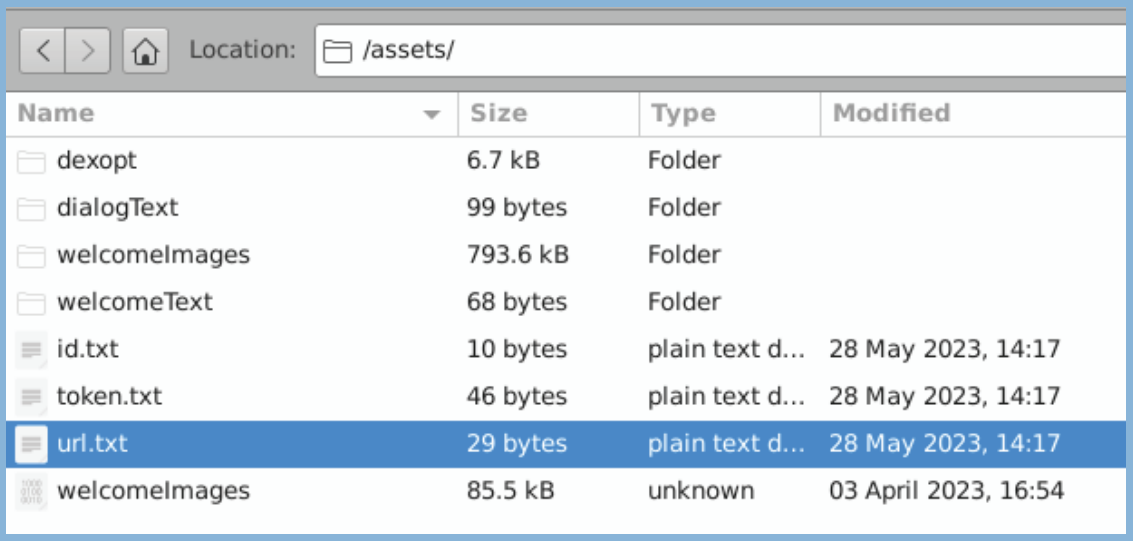




Gambar 2: Hasil analisis virus total menunjukan 24 macam virus yang terdeteksi.

2.2.2. Pengecekan Aset APK

Setelah APK tersebut dipasang, dia mengarahkan ke situs web tertentu untuk mengelabui korban. Untuk mengetahui situs web tersebut diarahkan ke mana, dibuka secara manual dengan mencari tempat pranala disimpan. Alamat pranala tersebut disimpan di dalam *folder asset* dengan nama fail pranala. Hal ini berlaku juga untuk mengumpulkan id dan token *(akan dibahas di bagian melacak pelaku)*.



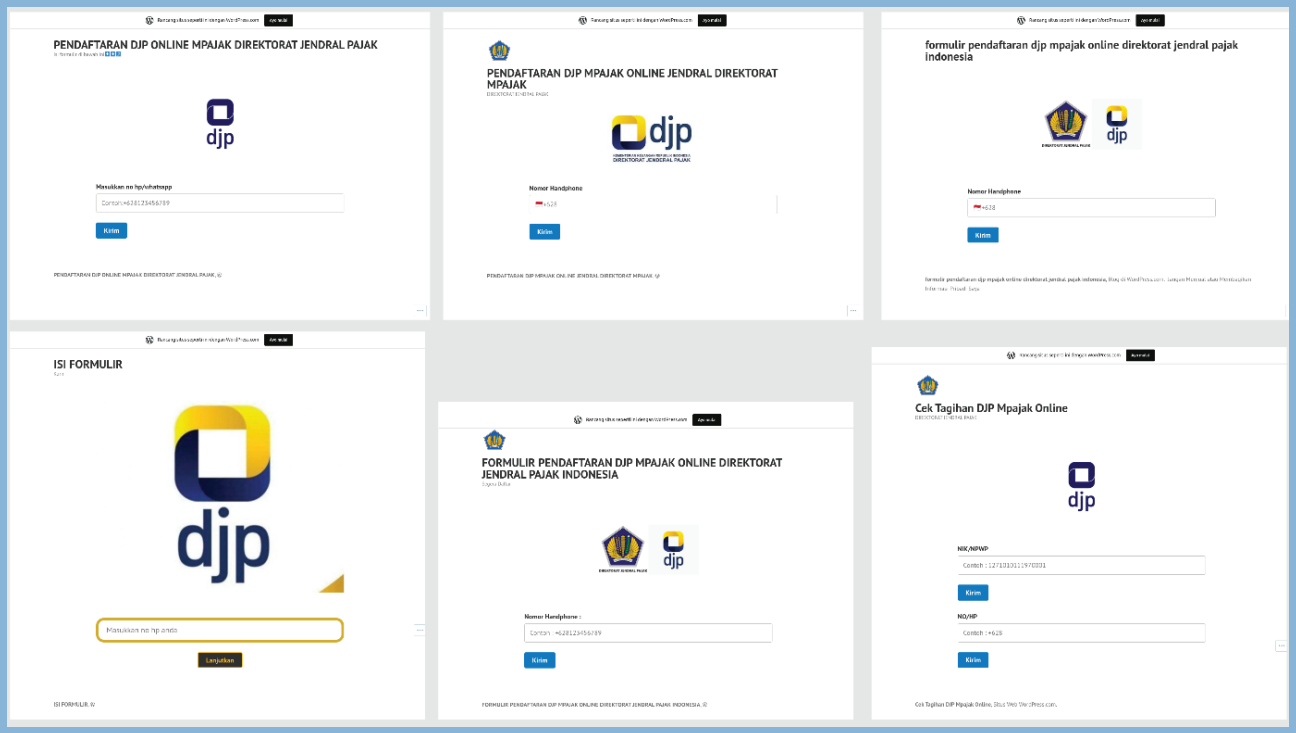
Gambar 3: Membuka folder assets yang menyimpan alamat url.

Setelah menelusuri, kami menemukan bahwa semua yang ada di dalam *folder* tersebut dikumpulkan seperti tabel berikut ini. Terlihat bahwa kebanyakan apk itu dibuat dari domain sama, tetapi nama subdomainnya berbeda. Selain itu juga, ada yang diubah hanya nama apk-nya. Misalnya *Cek Lokasi-2*, *Cek Lokasi-4*, *Lihat Foto Korban Tabrak Lari*, dan *Lihat Foto Undangan Pernikahan* memiliki nama alamat sama.

No	Nama APK	Alamat URL
1	cek.bpjs.kesehatan.apk	https://daftarbpjs.code.blog/
2	Cek Lokasi-2.apk	https://undangan799.code.blog/
3	Cek Lokasi-4.apk	https://undangan799.code.blog/
4	DAFTAR.DJP.MPAJAK	https://djp.design.blog/
5	DAFTAR.DJP.MPAJAK_sign.apk	https://djponlinepajak.art.blog/
6	DAFTAR.DJP-2.MPAJAK	https://djp.design.blog/
7	DAFTAR.DJP-4.MPAJAK	https://djp.design.blog/
8	Daftar-2.DJP	https://djp.data.blog/
9	DAFTAR-DJP-17.apk	https://djpmpajak.art.blog/
10	DJP.Mpajak.apk	https://djpmpajak.data.blog/
11	Lihat Foto Korban Tabrakan Lari.apk	https://undangan799.code.blog/
12	Lihat Foto Undangan Pernikahan.apk	https://undangan799.code.blog/
13	cek.bpjs.kesehatan.apk	https://daftarbpjs.code.blog/
14	DAFTAR.DJP.MPAJAK_sign.apk	https://djponlinepajak.art.blog/
15	DAFTAR-DJP-17.apk	https://djpmpajak.art.blog/
16	DJP.Mpajak.apk	https://djpmpajak.data.blog/
17	UNDANGAN PERNIKAHAN.apk	https://grabdalam.mfs.gg/Lanjutkannext
18	CEK DATA	https://cekdataanda.data.blog/
19	INFO DATA	https://newsupdatekeamanan.news.blog/

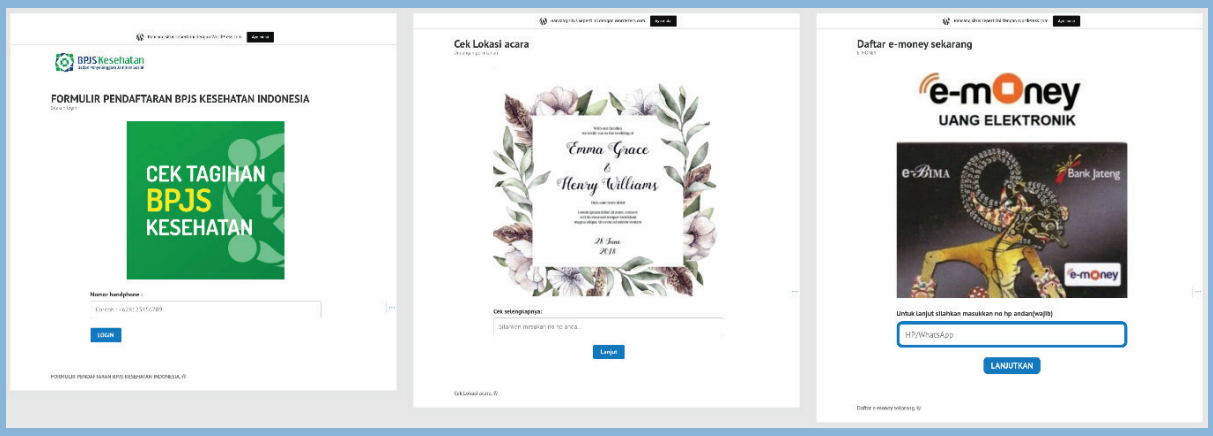
Tabel 3: Daftar website yang dimasukan ke dalam APK yang digunakan untuk mengumpulkan informasi lain.

Rata-rata, situs web tersebut memiliki ciri-ciri sama walaupun nama alamat domainnya berbeda-beda. Misalnya yang memiliki nama djp memiliki tampilan sama. Kebanyakan informasi yang diminta adalah nomor telepon atau WhatsApp, kecuali *djponlinepajak* yang meminta nomor induk kependudukan (NIK) atau nomor pokok wajib pajak (NPWP).



Gambar 4: Tampilan website yang digunakan untuk mengelabui korban

Tampilan situs web lain agak berbeda, tetapi memiliki struktur dan permintaan kontak yang sama.



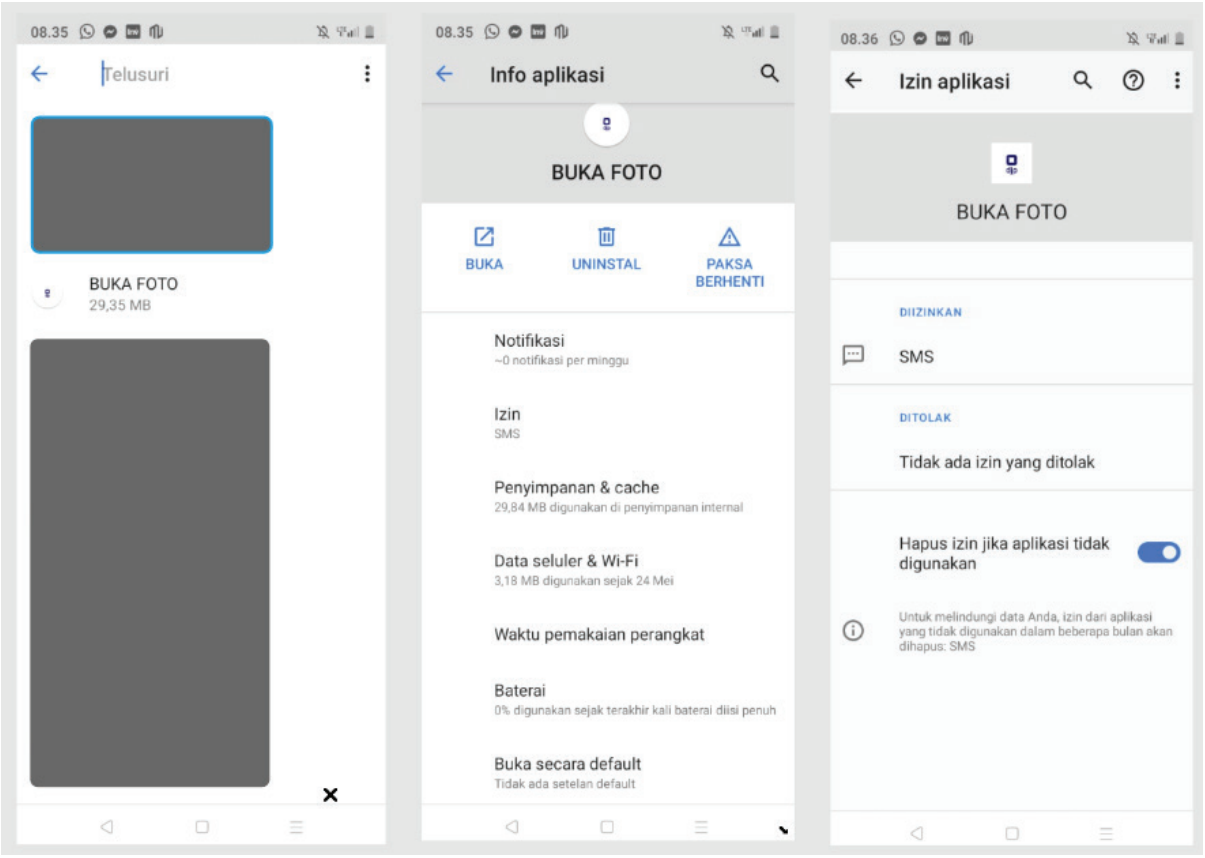
Gambar 5: Tampilan situs web untuk mengelabui korban dalam bentuk desktop

2.2.3. Pengecekan Ponsel Korban

2.2.3.1. Penelusuran Manual pada Perangkat

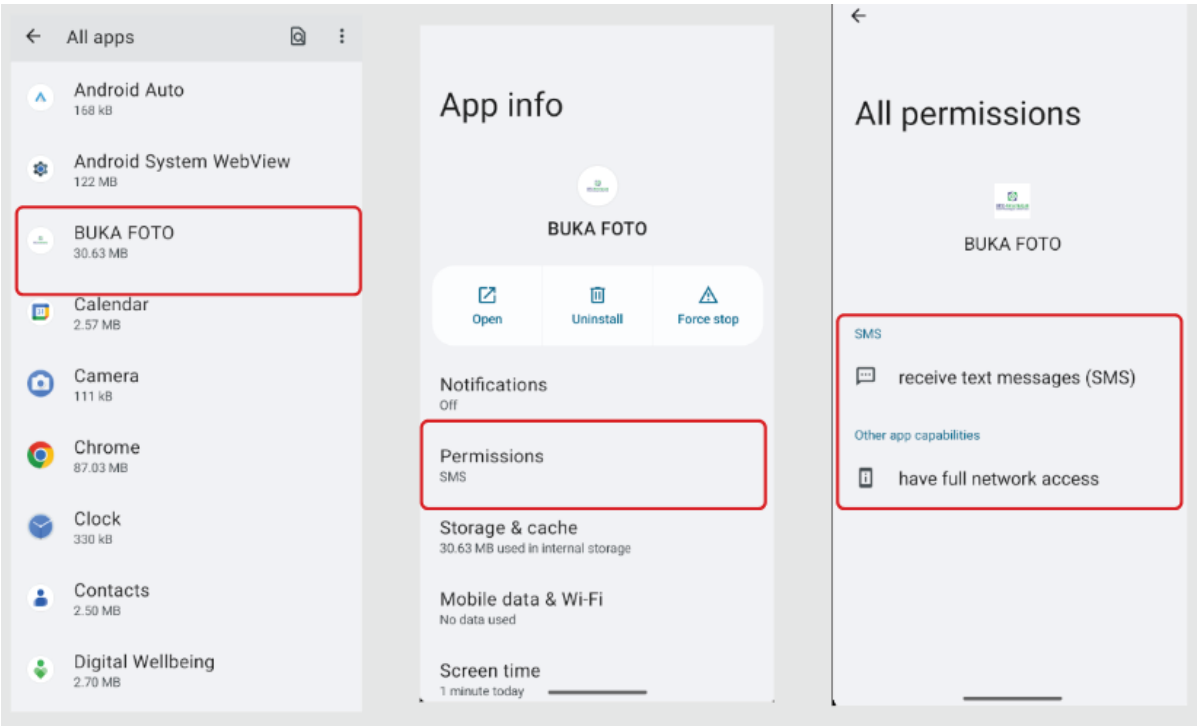
Tahap pertama setelah mencari layar utama tempat tumpukan aplikasi, tidak muncul apa-apa. Tidak ada yang aneh dan ponsel berjalan seperti biasa. Tahap kedua, langsung menelusuri Pengaturan *(Setting)* > Aplikasi *(Apps)* dan menemukan sesuatu yang berbeda dari biasanya. Muncul sebuah aplikasi dengan nama *'Buka Foto'.* Dari sini terlihat aplikasi tersebut aneh. Ternyata benar bahwa aplikasi tersebut merupakan APK yang terpasang setelah diklik korban. Hal tersebut dapat dilihat dari gambar aplikasi yang muncul mirip logo dalam situs web dan hanya logo dan tulisan *djp* di bawahnya pada APK tersebut. Setelah mengecek lebih lanjut, ada izin akses yang muncul yakni SMS.





Gambar 6: Pengecekan manual yang dilakukan pada salah satu korban

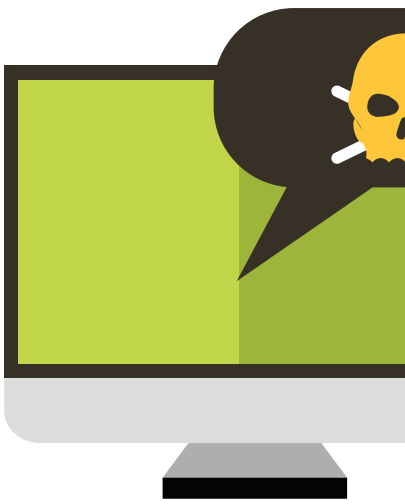
Untuk melakukan pembandingan, dilakukan pemasangan juga dengan simulator dan ditemukan sama bahwa ada dua hal yang dapat diakses, yakni akses SMS dan internet.

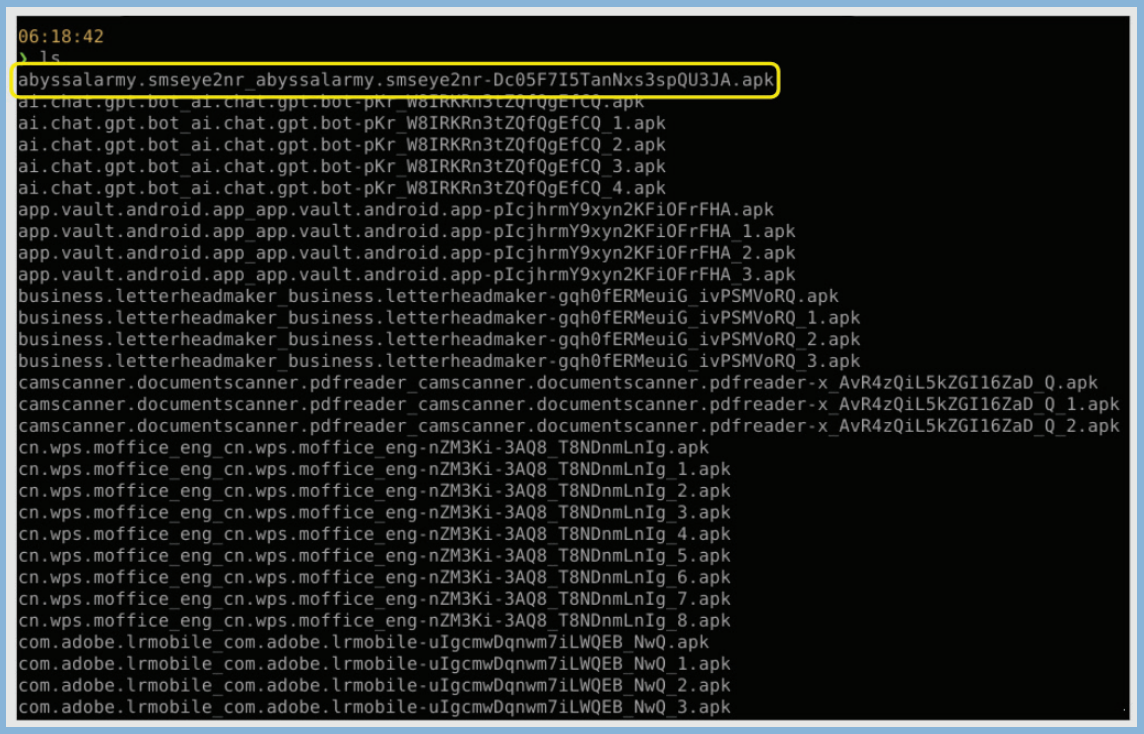


Gambar 7: Akses yang didapat setelah aplikasi dipasang.

2.2.3.2. Penelusuran dengan Alat Analisis

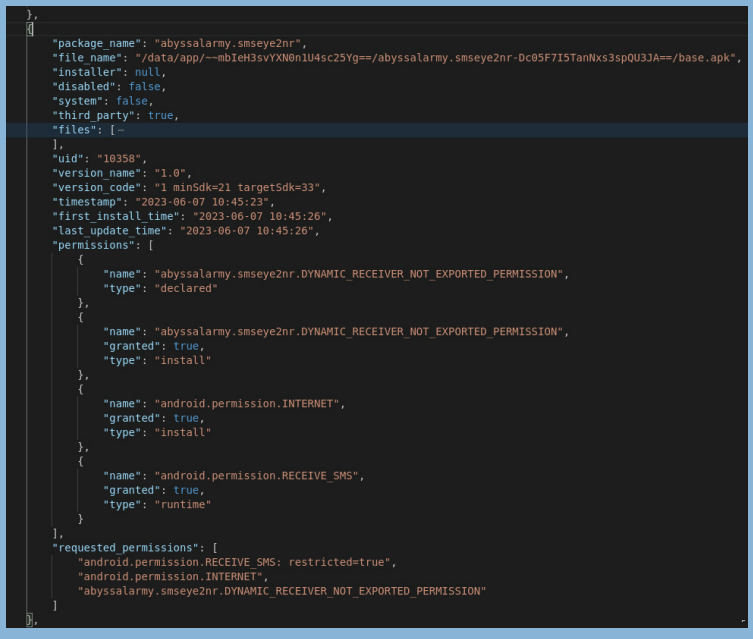
Selain secara manual, pemeriksaan dilakukan juga dengan mengumpulkan aplikasi terinstal dari ponsel korban. Hal itu dilakukan dengan menjalankan alat mvt-android. Setelah data ekstrak dikumpulkan, muncul salah satu aplikasi dengan nama yang aneh, yakni '*abyssalarmy.smseye2nr* ...'.





Gambar 8: Kumpulan aplikasi terinstal pada hp korban. Pada gambar kotak kuning muncul aplikasi yang mencurigakan.

Jika melihat hasil ekstrak, sama seperti pengecekan manual, aplikasi ini dapat mengakses SMS dan internet. Namun, ada yang berbeda di sini. File ekstrak ini menunjukan tiga hal yang dapat diakses, yakni SMS, internet, dan ada yang berbahasa agak teknis "... *DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION*"



Gambar 9: Perizinan akses pada apk hasil ekstrak.

2.3 Memahami Cara APK Bekerja

2.3.1. Pengakuan Korban

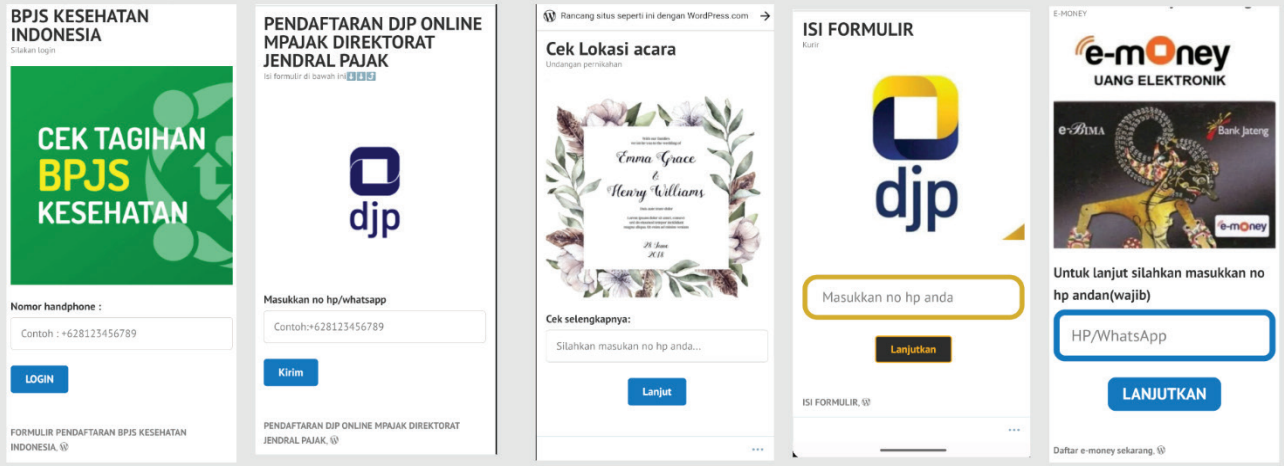
Berdasarkan wawancara, beberapa korban mengaku bahwa ketika aplikasi dipasang, aplikasi tersebut diteruskan begitu saja tanpa sepengetahuan korban di dalam grup WA yang dia ikut. Mereka kaget karena beberapa grup mengeluarkan mereka dengan alasan telah menyebarkan aplikasi yang mereka sudah ketahui bahwa itu berbahaya. Setelah mengetahui hal tersebut, satu-satunya solusi yang dilakukan adalah dengan mencopot dan memasang ulang kembali aplikasi WhatsApp.

Mereka merasa dengan melakukan itu masalah sudah selesai. Tetapi, APK tersebut baru terlihat jelas setelah dilakukan pengecekan manual dan diekstrak perangkatnya. Beberapa korban yang ditemui juga mengirimkan aplikasi tersebut di grup sasaran yang dikumpulkan.

2.3.2. Melalui Pengecekan APK Terpasang

Jika melakukan klik aplikasi tersebut, ia akan meminta izin untuk akses SMS. Setelahnya, ia akan mengarahkan ke situs web yang disediakan untuk mengisi beberapa informasi. Dalam mode ponsel, situs web tersebut akan tampil seperti gambar berikut. Tergantung mana yang diklik.

Setelah aplikasi meminta izin akses ke SMS (*android.permission.RECEIVE_SMS*) pada perangkat korban, pelaku akan mendapatkan informasi notifikasi jika APK tersebut telah diinstal bersama informasi mengenai perangkat, yakni tipe model dan manufaktur. Tujuan pengiriman informasi ini berbeda-beda, tetapi menggunakan



Gambar 10: Tampilan mode ponsel yang muncul setelah aplikasi tersebut dipasang pada perangkat.

format sama. Untuk notifikasi aplikasi terpasang dengan format: *"Notifikasi aplikasi diinstal + Nama Perangkat: ... "*. Demikian juga dengan ketika SMS masuk di ponsel korban: *"SMS dikirim oleh: ... + Isi sms"*. Kalimatnya beragam, tetapi pada intinya mengikuti pola seperti ini.

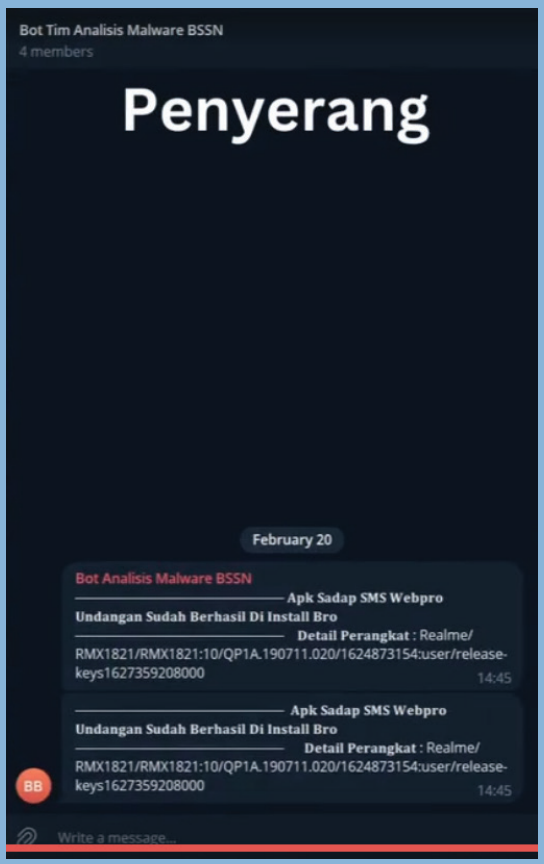
2.3.3. Melalui Simulasi

Untuk mengetahui langsung cara APK tersebut bekerja, ada simulasi oleh Badan Siber dan Sandi Negara (BSSN) melalui akun YouTube mereka[7]. Simulasi itu juga menunjukan bahwa APK tersebut jika

dijalankan ia dapat mengirimkan SMS dari ponsel korban dan dikirimkan ke Telegram bot pelaku. Informasi pertama yang dikirim kepada pelaku adalah informasi mengenai detail perangkat, baik dari merek hingga ID ponsel tersebut.

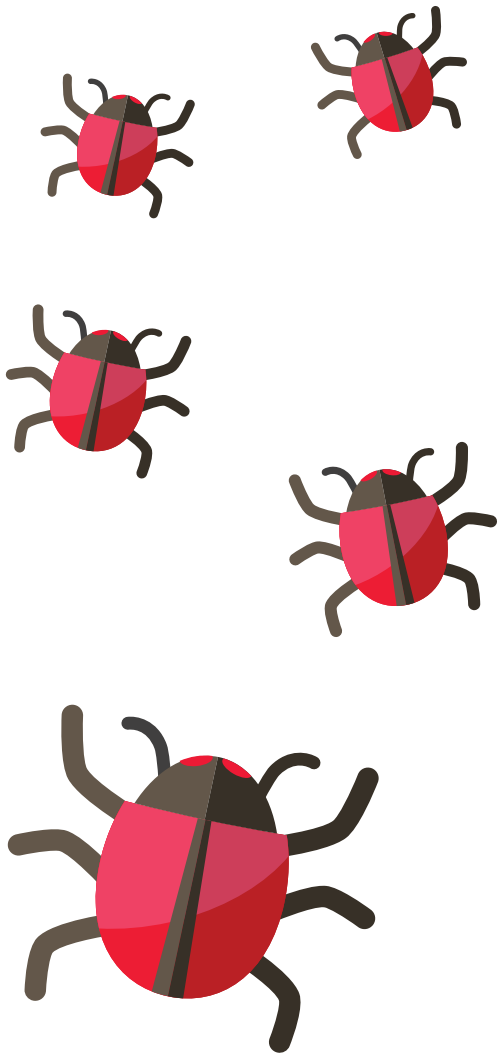
Berikut pesan yang didapat penyerang, *"Apk ... sudah berhasil di install Bro'* dan *'Detail perangkat: ... "*

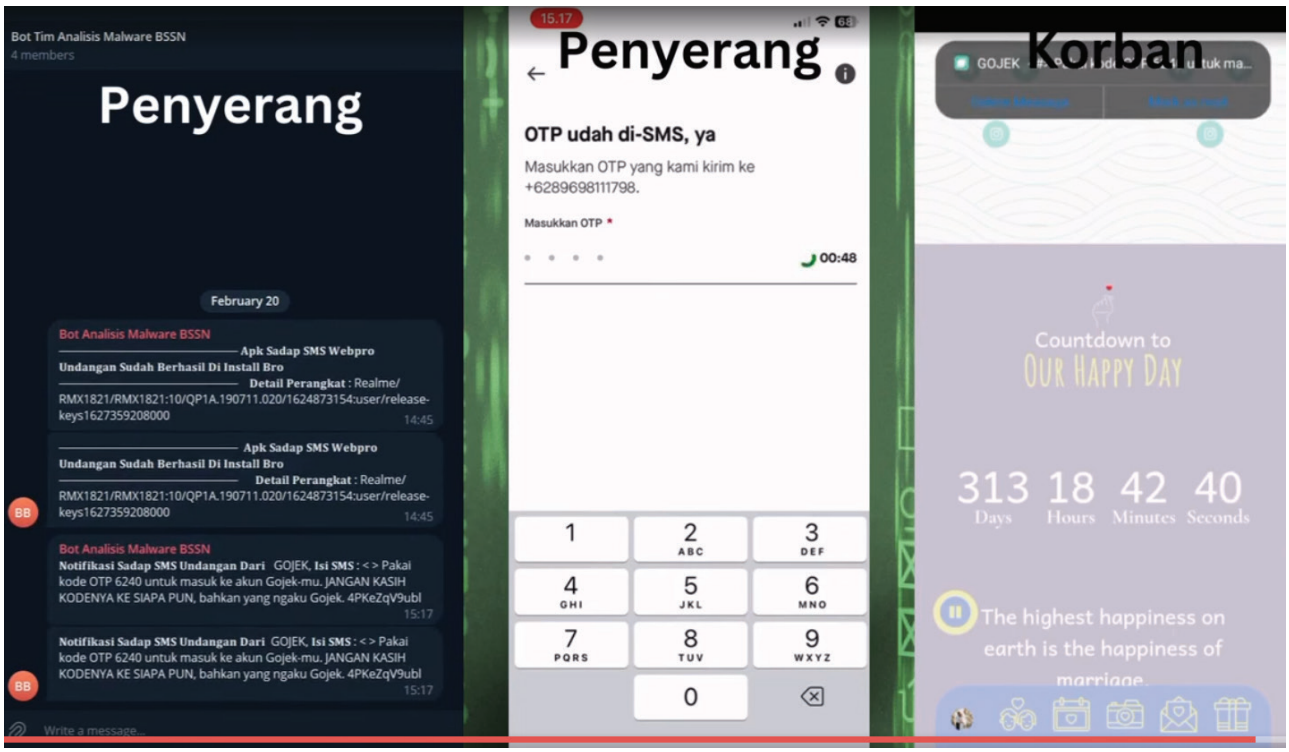
Isi pesan lengkapnya dapat dilihat pada gambar berikut ini:



Gambar 11: Simulasi BSSN akses yang didapat pelaku dari hp korban mengenai informasi detail perangkat.

Pada simulasi pengiriman kode sekali pakai atau *one time password* (OTP) Gojek pelaku langsung mendapat notifikasi kode tersebut dengan seluruh isi pesan.



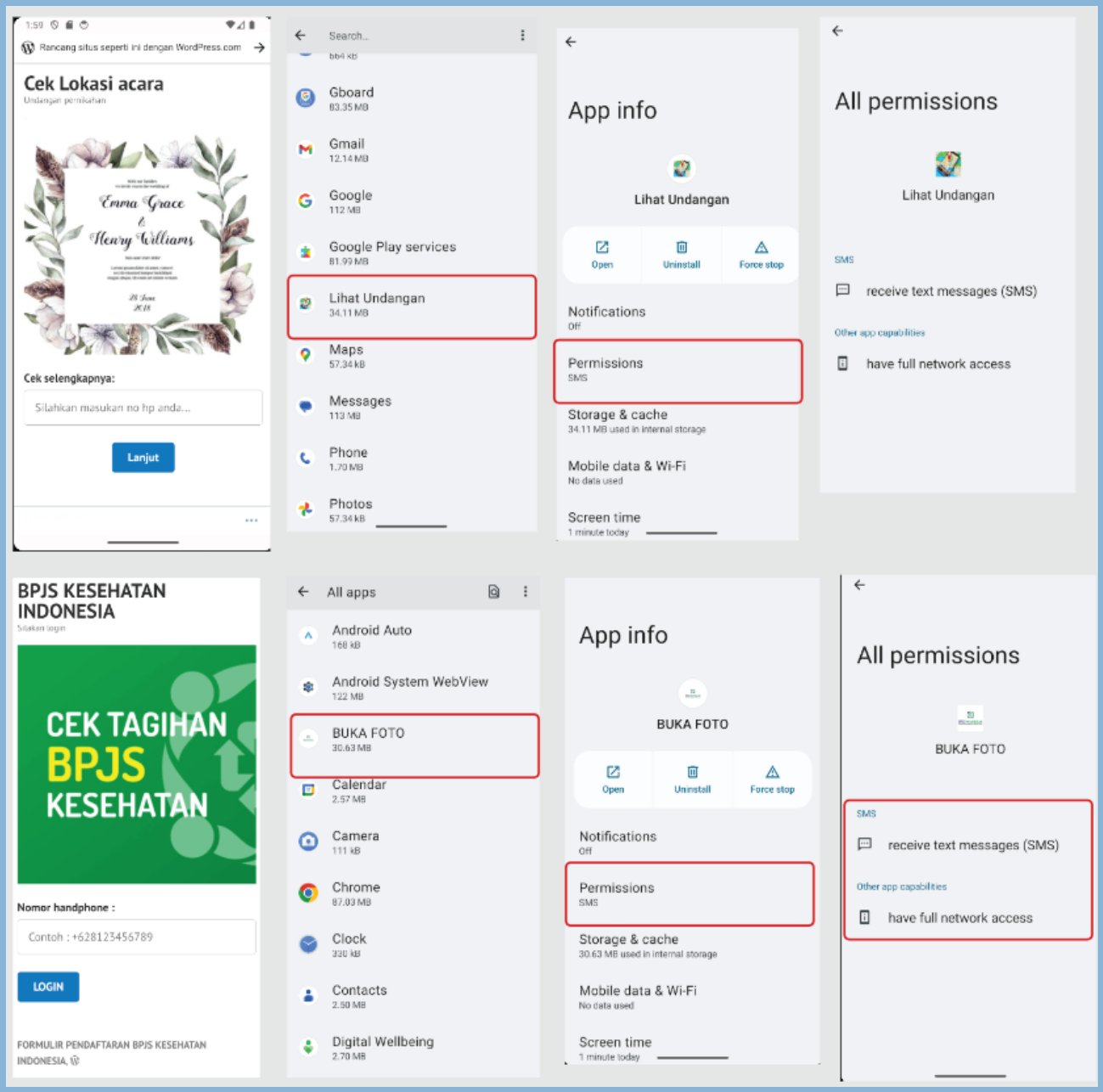


Gambar 12: Simulasi akses Gojek oleh penyerang untuk mendapat kode OTP.

Ketika pelaku mencoba masuk ke akun Gojek, ia akan menunggu beberapa detik untuk notifikasi SMS kode OTP masuk pada ponsel korban. Lebih cepat dari korban, pelaku menerima pesan: *"Notifikasi ... dari GOJEK, Isi SMS: <> ..."* (isi pesan lengkapnya dapat dilihat pada gambar di atas).

2.3.4. APK Menyembunyikan Diri

Rupanya setelah APK terpasang, ia menghilang begitu saja dari tumpukan aplikasi di laman bagian depan. Tidak dapat ditemukan satupun ciri-ciri APK tersebut terpasang di layar depan. Aplikasi ini hanya dapat ditelusuri dengan mengunjungi pengaturan bagian aplikasi. Hanya dengan cara demikian APK yang terinstal dapat ditemukan.



Gambar 13: APK hanya dapat terlihat melalui penelusuran pengaturan.

Nama yang muncul pada APK terpasang berbeda-beda. Ada yang bernama *Buka Foto* di bagian Semua Aplikasi *(All Apps)* dan Informasi Aplikasi *(App info)*. Namun, ada yang berbeda nama. Pada semua aplikasi muncul *Lihat Undangan* tetapi pada informasi aplikasi muncul dengan nama *Buka Foto*. Setelah dibuat simulasi secara virtual, beberapa yang muncul seperti gambar tabel berikut.

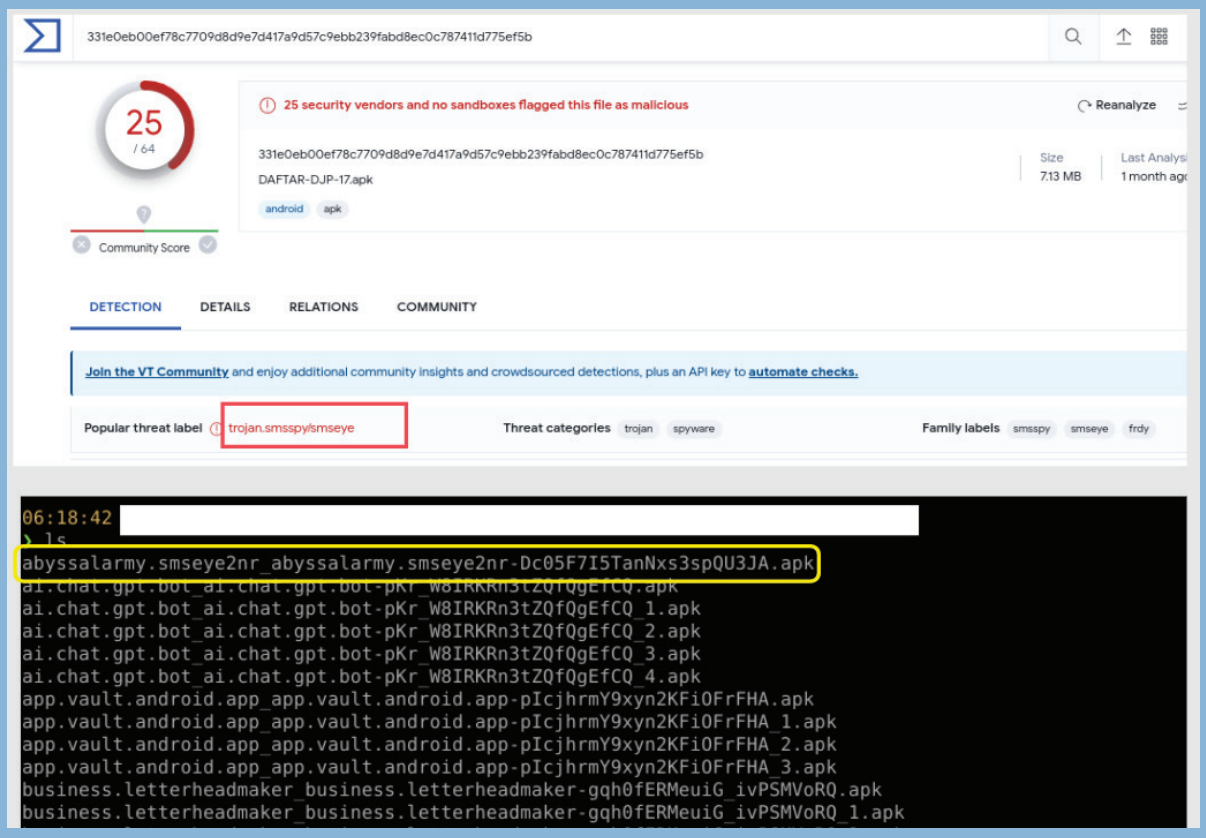
No	Nama APK	All Apps	App info
1	CEK DATA	Buka Foto	Buka Foto
2	cek.bpjs.kesehatan.apk	Buka Foto	Buka Foto

Gambar 14: Kumpulan nama APK yang terinstal pada perangkat.

2.4. Melacak Pelaku

2.4.1. Mesin Pembuat APK

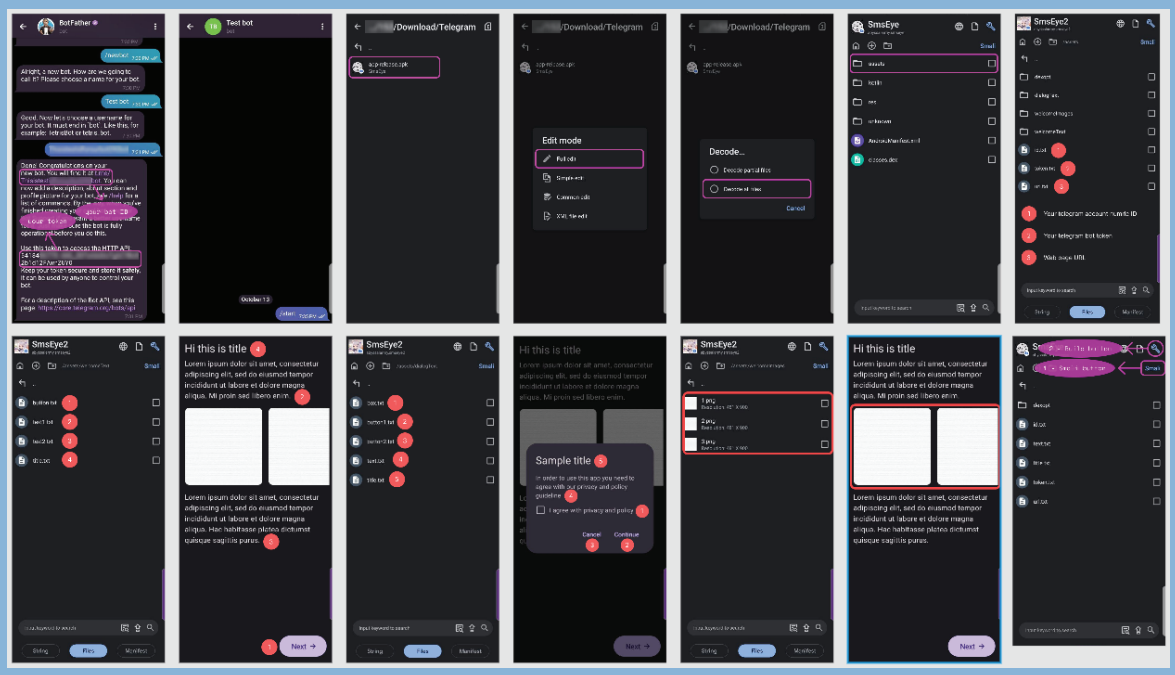
Untuk mengetahui bagaimana APK dibuat perlu menelusuri berdasarkan nama yang muncul dari beberapa pelacakan sebelumnya. Pada hasil analisis VirusTotal muncul label dengan nama *'smseye'* (gambar dengan lingkaran merah). Hal lain lebih spesifik juga muncul pada APK yang terinstal pada ponsel korban. Hasil ekstrak memberikan sebuah nama APK, yakni *'abbyssalarmy...'* (gambar dengan lingkaran kuning).



Gambar 15: Petunjuk untuk mengetahui sumber APK.

Setelah melakukan penelusuran dengan menggunakan nama *'smseye'* dan atau *'abbyssalarmy'*, ditemukan sebuah alat yang digunakan untuk membuat APK ini. Alat ini bernama Android SMS Spyware.

APK ini dibuat menggunakan bot Telegram. Hampir semua APK tersebut dibuat dengan smseye versi ke-2. Alat ini digunakan untuk membuat APK yang dapat memata-matai perangkat berbasis Android. Tahapan pembuatannya juga dijelaskan di sana, sehingga siapapun dapat membuatnya dengan cukup mudah.



Gambar 16: Tahapan pembuatan APK menggunakan bot telegram versi kedua.

2.4.2. Telegram Bot

Dari penelusuran lebih lanjut, didapatkan juga *ID* dan *Token* pelaku. Setelah menyingkirkan beberapa aplikasi bernama mirip, berkurang menjadi 12 APK. Nama APK tersebut berbeda, tetapi setelah mengecek alamat *url* beberapa memiliki nama subdomain sama. Kesamaan tersebut muncul juga dari ID dan Token telegram pelaku (yang diberi warna merah dan hijau menunjukan kesamaan ID dan Token). Berikut ini ID dan Token yang berhasil dikumpulkan.

No	Nama APK	Alamat URL	ID	Token
1	DJP.Mpajak.apk	https://djpmpajak.data.blog/	1906667239	5531871192:AAGd3nFCjJ1wyImJmFfSDdfLoUKUUluX6YY
2	cek.bpjs.kesehatan.apk	https://daftarbpjs.code.blog/	5690403779	6054401854:AAEN9slAsHIRVw-HCQssi0EaJ2y281AzTvg
3	UNDANGAN PERNIKAHAN.apk	https://grabdalam.mfs.gg/Lanjutkannext	5690403779	6039879654:AAFIXcSecTLNPhNHMhooQ1ddoZd498fCUac
4	CEK DATA	https://cekdataanda.data.blog/	5858717263	6299447822:AAG-idn_1gQDN59BZNZ1CPTGV9FCIlpvCuA
5	Cek Lokasi-2.apk	https://undangan799.code.blog/	5959990681	6129262865:AAFqEmLbsP1tzz4bHGS7b6-wWXhZE2Fh8Sk
6	Lihat Foto Korban Tabrakan Lari.apk	https://undangan799.code.blog/	5959990681	6129262865:AAFqEmLbsP1tzz4bHGS7b6-wWXhZE2Fh8Sk
7	Lihat Foto Undangan Pernikahan.apk	https://undangan799.code.blog/	5959990681	6129262865:AAFqEmLbsP1tzz4bHGS7b6-wWXhZE2Fh8Sk
8	INFO DATA	https://newsupdatekeamanan.news.blog/	6020337282	5971525992:AAGSzHfc3Ceix7B-0lqGd-nDtlvZufdGFWQ
9	DAFTAR-DJP-17.apk	https://djpmpajak.art.blog/	6180427060	6007814149:AAEGr8O5FKoWiQ1Mj_aEuFd93ipeTbwKEUw
10	DAFTAR.DJP.MPAJAK_sign.apk	https://djponlinepajak.art.blog/	6228019944	5687117035:AAGFhZd6GPcbTwmYd2wxmmGcWa4SVkAAfps
11	Daftar-2.DJP	https://djp.data.blog/	6291253639	6350581621:AAH7__LKBv57QNon2oZ5q_RIZpNXnST2lKM
12	DAFTAR.DJP.MPAJAK	https://djp.design.blog/	6325829447	6353317442:AAGOAvHK9l1HZ45YMaj4LElvwnCY7kdEgVA

Tabel 4: data pengumpulan id dan token pelaku.

Lebih lanjut, berdasarkan ID dan Token dapat dilakukan pencarian nama dan *username* akun *bot* yang digunakan. Setelah mencari menggunakan *token checker bot* dan *usif bot* di Telegram tidak ditemukan nama sebenarnya. Hanya nama samaran dan istilah-istilah yang tidak jelas. Rupanya pelaku menutup jejaknya dengan cara demikian.

Berikut ini nama-nama yang muncul setelah melakukan pencarian.

ID	Token	Nama Token	Username	Nama Id
1906667239	5531871192:AAGd3nFCjJ1wyImJmFfSDdfLoUKUUluX6YY	Telkomtselmania	@Tselappsrajabot	Dana Kaget
5690403779	6054401854:AAEN9slAsHIRVw-HCQssi0EaJ2y281AzTvg	Bemalu oy jangan majak bot Wang ni binatang	@Notifikasi123455bot	
5858717263	6299447822:AAG-idn_1gQDN59BZNZ1CPTGV9FCIlpvCuA	VERSI terbaru	@Versifjcjcfkrbot	
5959990681	6129262865:AAFqEmLbsP1tzz4bHGS7b6-wWXhZE2Fh8Sk	LUKI	@Fbfbfjfffbot	
6020337282	5971525992:AAGSzHfc3Ceix7B-0lqGd-nDtlvZufdGFWQ			
6180427060	6007814149:AAEGr8O5FKoWiQ1Mj_aEuFd93ipeTbwKEUw			DANA KAGET
6228019944	5687117035:AAGFhZd6GPcbTwmYd2wxmmGcWa4SVkAAfps	Patokaaaaa	@Qqqqqqhalobot	ropil
6291253639	6350581621:AAH7__LKBv57QNon2oZ5q_RIZpNXnST2lKM	Kntl13	@Lovelove123456bot	
6325829447	6353317442:AAGOAvHK9l1HZ45YMaj4LElvwnCY7kdEgVA	Riski,Aan, Jagong, Alan,Deris,Berill	@Pyopyo99bot	

Tabel 5: Username dan id yang muncul setelah melacak berdasarkan id dan token

2.4.3. Melacak Alamat IP

Untuk mengetahui lebih lanjut mengenai pembuat APK, perlu menelusuri alamat *url* untuk menemukan alamat protokol internet (IP address). Setelah melakukan penelusuran domain tersebut dengan menggunakan *DNSDumpster*[8] berikut ini kumpulan informasi alamat IP dari beberapa beberapa url yang digunakan.

No	Nama APK	Alamat URL	Alamat IP
1	CEK DATA	https://cekdataanda.data.blog/	192.0.78.24
2	Daftar-2.DJP	https://djp.data.blog/	192.0.78.25
3	DAFTAR.DJP.MPAJAK	https://djp.design.blog/	192.0.78.25
4	DJP.Mpajak.apk	https://djpmpajak.data.blog/	192.0.78.25
5	cek.bpjs.kesehatan.apk	https://daftarbpjs.code.blog/	192.0.78.30
6	DAFTAR-DJP-17.apk	https://djpmpajak.art.blog/	192.0.78.30
7	Lihat Foto Korban Tabrakan Lari.apk	https://undangan799.code.blog/	192.0.78.30
8	DAFTAR.DJP.MPAJAK_sign.apk	https://djponlinepajak.art.blog/	192.0.78.31
9	INFO DATA	https://newsupdatekeamanan.news.blog/	192.0.78.31

Tabel 6: Daftar nama APK dan lokasi penyimpanannya.

Untuk mengetahui alamat IP tersebut wajar atau tidak perlu mengecek ke AbuseIPDB[9]. Setelah melakukan pengecekan alamat IP tersebut, muncul informasi bahwa alamat tersebut pernah melakukan kejahatan dunia maya. Tidak hanya pemancingan tetapi dilaporkan jika mereka mengirim email spam, eksploitasi *host*, *phising*, dan lain-lain.

IP Abuse Reports for **192.0.78.24**:

This IP address has been reported a total of **13** times from 11 distinct sources. 192.0.78.24 was first reported on August 26th 2021, and the most recent report was **4 weeks ago**.

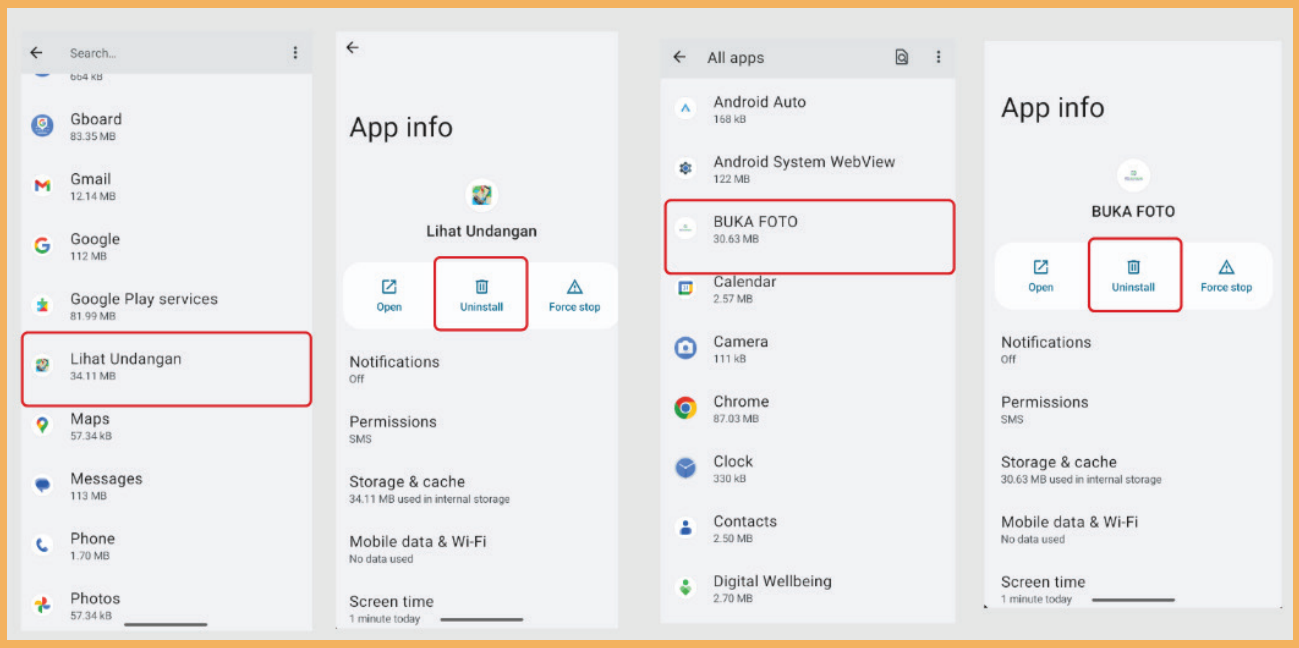
Old Reports: The most recent abuse report for this IP address is from **4 weeks ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	Date	Comment	Categories
DODDesertHawk	18 Aug 2023	publishing scam website exploited host trojan,ransware virus Malware	Phishing Exploited Host
oonux.net	15 Aug 2023	RouterOS: Scanning detected TCP 192.0.78.24:443 > x.x.x.x:60884	Port Scan
Nookie	22 Oct 2022	Phishing site	Phishing Email Spam Exploited Host
vicky	14 Oct 2022	info@onestopparkinglotcare.com - free estimate for Asphalt Repairs, Potholes,	Email Spam Spoofing
vicky	20 Sep 2022	info@onestopparkinglotcare.com	Email Spam Spoofing
ChillScanner	05 Jul 2022	2 probe(s) @ UDP(53)	Port Scan
Lotus Prime	26 Apr 2022	IP used for web phishing	Phishing
ISPLtd	24 Feb 2022	Feb 24 08:46:01 SRC=192.0.78.24 PROTO=TCP SPT=80 DPT=13213 SYN Feb 24 08:46:02 SRC=192.0.78.24 ... show more	Port Scan
marcel-knorr.de	24 Feb 2022	[MK-VM4] Blocked by UFW	Port Scan Brute-Force

Gambar 17: Laporan alamat IP berkaitan terlibat dalam kejahatan dunia maya.

2.5. Cara Mencabut APK

Agar tidak ada akses terhadap pelaku, korban harus memutuskan akses dari pelaku. Untuk itu, minimal korban perlu mencopot aplikasi tersebut. Untuk melakukannya, pergi ke *pengaturan (Settings)* kemudian ke Aplikasi dan cari nama aplikasi yang tampak sama seperti tabel di atas. Setelah itu, perlu menekan aplikasi tersebut dan menuju ke bagian tengah dengan nama *Hps Instalan (Uninstall)*.



Gambar 18: Petunjuk penghapusan aplikasi terinstal.

3. PENUTUP

Berdasarkan penelitian menggunakan metode gabungan, kami menemukan bahwa aplikasi yang disebarkan secara berantai di dalam grup Papua merupakan aplikasi penipuan berbahaya. Aplikasi tersebut dapat mengakses dan memantau percakapan SMS melalui Telegram. Setelah melakukan klik, APK tersebut diteruskan ke dalam grup di mana korban bergabung tanpa sepengetahuan korban. APK tersebut dibuat dengan menggunakan bot Telegram. Ketika APK terpasang dan diizinkan akses, penyerang dapat mengakses SMS dan internet untuk meneruskan ke Telegram pelaku.

Oleh karena itu, sangat berbahaya dan dapat merugikan korban sebab dapat berpotensi mengakses aplikasi untuk bertransaksi secara daring maupun mengakses percakapan melalui SMS. Saat dipasang ia dapat mengarahkan korban untuk memberikan informasi pribadi pada website tertentu yang dibuat pelaku dan diminta memasukkan nomor ponsel maupun NPWP dan atau NIK.

Setelah melakukan penelusuran berdasarkan pranala yang ditemukan bahwa alamat IP tersebut sering digunakan untuk melakukan berbagai kejahatan di dunia maya. Nama pembuat juga dibuat palsu agar tidak mudah diketahui oleh orang lain.

Meskipun tidak ada bukti bahwa serangan-serangan melalui APK ini terkait erat dengan ekspresi atau represi politik, tetap saja dia harus diwaspadai agar tidak semakin banyak warga, mahasiswa, dan aktivis Papua yang menjadi korban.

Untuk itu, kami merekomendasikan kepada korban agar segera melakukan pengecekan perangkat untuk minimal dengan menghapus APK tersebut jika sudah terpasang pada perangkat atau pernah merasa melakukan pemasangan APK tersebut. Dengan demikian, Anda akan terbebas dari pemantauan pelaku yang bersiap untuk mencuri informasi tentang percakapan Anda di gawai.

Tidak semua aplikasi yang ada di jagat maya adalah baik. Tidak semua APK dapat menguntungkan. Paling tidak, salah satu yang dapat dilakukan adalah melakukan penginstalan hanya melalui Google Playstore. Jangan pernah melakukan klik pada alamat tertentu ataupun aplikasi yang dibagikan melalui Whatsapp.

4. CATATAN KAKI

1 https://tekno.kompas.com/read/2023/07/07/10150007/korban-penipuan-file-apk-terkuras-rp-1-4-m-ini-ciri-ciri-modusnya-hati-hati?page=all

2 https://nikkoenggaliano.my.id/read.php?id=7

3 https://teguh.co/membongkar-modus-penipuan-aplikasi-kurir-dan-informasi-terduga-pelaku/

4 https://www.merdeka.com/peristiwa/483-orang-jadi-korban-penipuan-modus-link-phising-dan-apk-kerugian-rp12-miliar.html

5 https://www.virustotal.com/

6 https://www.virustotal.com/gui/file/340f5c9b2437524e44b28c6dc109352f46355b87c7b2912040e42945159c2231/detection

7 https://youtu.be/W98rn22grBs

8 https://dnsdumpster.com/

9 https://www.abuseipdb.com/


SAFEnet