BADAN SIBER DAN SANDI NEGARA

TLP: Clear

# IMBAUAN KEAMANAN

# 2023

## *Juice Jacking*

Waspadai Serangan *Juice Jacking* Ketika Pelaksanaan Mudik

**16 April 2023**

# DAFTAR ISI

# Pendahuluan

Dalam menyongsong Hari Raya Idul Fitri, kegiatan mudik sangat identik melekat pada masyarakat di Indonesia, terutama di kota-kota besar. Pada tahun 2023 ini, Kementerian Perhubungan memperkirakan 123,8 juta orang melaksanakan mudik dimana angka ini meningkat 14,2 persen dibandingkan pada tahun 2022.

Ketika menggunakan moda transportasi umum, keamanan merupakan aspek yang harus dijaga oleh masing-masing pribadi. Baik keamanan fisik maupun keamanan pada barang bawaan, termasuk barang elektronik.

Ketika menggunakan handphone, perlu diwaspadai dalam melakukan pengisian daya pada *power adapter* di tempat umum. Apabila tidak hati-hati, kita dapat terkena dampak serangan *Juice Jacking.*

# Penjelasan

Obyek yang terdampak kerentanan ini adalah perangkat mobile yang menggunakan sistem operasi berikut:

| Produk | Versi Terdampak |
|---|---|
| Windows | • Tidak ada versi khusus |
| iOS | • Tidak ada versi khusus |
| Android | • Tidak ada versi khusus |

***Juice Jacking*** sering digunakan oleh peretas untuk mencuri data korbannya. Teknik ini mulai dikenal dan marak sejak tahun 2011 lalu dan meningkat di waktu-waktu tertentu seperti waktu mudik lebaran, natal dan tahun baru, maupun pekan libur sekolah di mana banyak masyarakat berada di fasilitas umum dengan jangka waktu yang lumayan lama. Seiring perkembangan teknologi dan meningkatnya kebutuhan masyarakat dalam menggunakan perangkat teknologi yang dapat memudahkan pekerjaan maka banyak produsen teknologi yang pada akhirnya memproduksi perangkat mobile sebagai jawaban atas tantangan global saat ini. Selain memiliki kelebihan, perangkat mobile juga memiliki beberapa kelemahan yang salah satunya adalah keterbatasan ketersediaan daya. Semakin lama digunakan dan semakin banyaknya aplikasi yang dijalankan di dalam satu perangkat mobile, semakin banyak pula daya yang dibutuhkan.

sumber: https://idcloudhost.com/apa-itu-juice-jacking-dan-cara-mencegahnya/

sumber: https://dmifinance.in/blog-details.php?headline-everything-you-need-to-know-about-juice-jacking-a-new-way-to-steal-your-data

**D**ampaknya adalah daya perangkat akan cepat habis, sementara fasilitas pengisian daya juga tidak banyak tersedia di tempat umum. Melihat fenomena ini tingginya kebutuhan pengguna akan perangkat mobile, beberapa produsen teknologi atau tempat umum mulai menyediakan fasilitas ataupun ruang khusus untuk pengisian daya yang dapat digunakan masyarakat secara bebas untuk mengisi daya perangkatnya. Hal ini kemudian dimanfaatkan peretas untuk mencuri data korban dengan menjalankan teknik *Juice Jacking* pada fasilitas umum yang seringnya masyarakat tidak sadar bahwa perangkatnya sedang diretas. lantas, sebenarnya apa itu J*uice Jacking* ? dan bagaimana cara mencegah dan mengihndari serangan *Juice Jacking* ? berikut penjelasan tentang *Juice Jacking* yang perlu diketahui bagi para pelaku perjalanan atau pengguna fasilitas umum yang sedang atau akan berpergian.

## *Juice Jacking* ? Apakah Seberbahaya Itu ?

***J**uice Jacking* merupakan salah satu Teknik yang digunakan peretas untuk mengambil data korban yang tersimpan di perangkat ponsel/tablet/perangkat portable lainnya milik korban melalui kabel pengisian daya yang dipasang pada fasilitas umum yang telah dimodifikasi oleh peretas. Biasanya, *Juice Jacking* terdapat pada fasilitas pengisian daya yang sudah menyediakan kabel atau *port* USB siap pakai untuk publik. Tidak hanya untuk perangkat ponsel, tetapi juga mendukung berbagai perangkat elektronik lainnya seperti laptop/tablet maupun perangkat *mobile* lainnya.

Teknik ini mulai berkembang sejak tahun 2011, semenjak para peneliti memberikan solusi untuk membuat tempat pengisian daya yang terbuka untuk publik. Pada awalnya, tidak ada serangan apapun terkait solusi ini sampai dengan salah satu pengguna menggunakan fasilitas pengisian daya dan perangkatnya memunculkan notifikasi peringatan keamanan yang kemudian dikenal sebagai *Juice Jacking*.

*Juice Jacking* merupakan salah satu serangan siber yang menyebarkan *malware* dalam jumlah yang banyak pada perangkat *mobile* secara diam-diam untuk menyalin data pribadi milik pengguna menggunakan *port* USB sebagai koneksi datanya. Secara lebih spesifik, *Juice Jacking* menyerang korban dengan menggunakan kabel atau *port* sebagai jalan bagi peretas untuk masuk dan mengakses data pribadi korban selama proses pengisian daya.

Lalu, apakah *Juice Jacking* berbahaya ? maka jawabannya adalah, **iya**. Pengguna biasanya tidak akan menyadari bahwa perangkatnya sudah diretas, karena *malware* yang disisipkan oleh peretas sudah diatur untuk melakukan pencurian data secara diam-diam atau yang sering dikenal dengan jalur *backdoor*. Sehingga, dari sisi pengguna tidak merasakan adanya keanehan ketika serangan *Juice Jacking* ini sedang berlangsung.

## Bagaimana Cara Kerja *Juice Jacking*?

**B**aik perangkat korban maupun perangkat peretas memiliki kesamaan yaitu jenis aliran yang melewati kabel yang sama. Kemudian ketika perangkat korban tersambung dengan kabel USB, maka transfer daya pun terjalin. Selama masa pengisian daya, *port* USB terbuka dan hal ini lah yang dimanfaatkan peretas untuk mengeksploitasi perangkat korban guna mendapatkan informasi sensitif yang dibutuhkannya.

*Juice Jacking* dapat langsung diterapkan karena tidak ada peringatan yang akan dimunculkan perangkat korban ketika kabel USB dihubungkan. Beberapa celah lainnya seperti mode transfer data otomatis yang diaktifkan korban sehingga membuat notifikasi peringatan tidak muncul ketika perangkat baru akan dihubungkan membuat teknik ini semakin tidak terdeteksi aktivitasnya. Oleh karena itu, penting bagi masyarakat untuk mengaktifkan fitur-fitur keamanan dasar pada perangkat pribadi agar dapat terhindar dari serangan *Juice Jacking* ini. Selain itu, masyarakat juga diimbau untuk menerapkan beberapa saran pencegahan agar terhindar dari serangan *Juice Jacking*. Lalu apa yang dapat dilakukan masyarakat, berikut merupakan saran pencegahan yang dapat diterapkan masyarakat saat sedang berpergian atau berada di tempat umum:

# Panduan Mitigasi

Hindari pengisian daya menggunakan *port* USB di tempat publik, gunakan stop kontak listrik arus AC sebagai gantinya.

Membawa pengisi daya dan *powerbank* pribadi maupun baterai eksternal ketika perjalanan.

Lebih diutamakan untuk membawa kabel pengisi daya dengan tipe *charging-only* untuk menghindari pengiriman data saat dilakukan pengisian daya.

Ketika menyambungkan perangkat ke *port* USB dan muncul notifikasi yang meminta untuk memilih ”Bagikan Data” atau ”Hanya Isi", selalu pilih ”Hanya Isi”.

# REFERENSI


- "Juice Jacking" https://www.wallofsheep.com/pages/juice (diakses April 16, 2023)
- "FBI warns against public phone charging stations at airports and hotels, citing malware risk" https://www.houstonchronicle.com/news/houston-texas/article/fbi-warns-against-using-public-charging-stations-17895735.php (diakses April 16, 2023)
- "Juice Jacking: The Dangers of Public USB Charging Stations" https://www.fcc.gov/juice-jacking-dangers-public-usb-charging-stations (diakses April 16, 2023)
- "Awas! FBI Sarankan Hindari Ngecas HP di Bandara-Mal" https://travel.detik.com/travel-news/d-6675756/awas-fbi-sarankan-hindari-ngecas-hp-di-bandara-mal (diakses April 16, 2023)
- "Mengenal Juice Jacking dan Cara Mencegahnya" https://idcloudhost.com/apa-itu-juice-jacking-dan-cara-mencegahnya/ (diakses April 16, 2023)
- "Juice Jacking, Ancaman Keamanan Data Melalui Kabel Pengisian Daya" https://voi.id/teknologi/271676/juice-jacking-ancaman-keamanan-data-melalui-kabel-pengisian-daya (diakses April 16, 2023)
- "Jangan Asal Ngecas HP di Tempat Umum, Bahaya Juice Jacking" https://www.cnbcindonesia.com/tech/20230413080357-37-429464/jangan-asal-ngecas-hp-di-tempat-umum-bahaya-juice-jacking (diakses April 16, 2023)
- "Serangan cyber melalui juice jacking, apa itu jacking ?" https://fcom.co.id/serangan-cyber-melalui-juice-jacking-apa-itu-jacking- (diakses April 16, 2023)

# INFORMASI DOKUMEN

## KETENTUAN PENGGUNAAN DOKUMEN

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

## RIWAYAT DOKUMEN

| VERSI DOKUMEN | TANGGAL RILIS |
|---|---|
| 1.0 | 16 APRIL 2023 |

## KONTAK KAMI

DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

Jl. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550

(021) 788 33610

bantuan70@bssn.go.id


BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
BHINNEKA TUNGGAL IKA
STHANA PAROKSHARTA BHAKTI