www.idsirtii.or.id

16 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 214

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	1	0	0
URGENT	0	0	3
IMPORTANT	1	1	0

General News

Kampanye *Phishing* Menargetkan Bank BRI Menggunakan SMS *Stealer*

Baru-baru ini, Cyble Research and Intelligence Labs (CRIL) mengidentifikasi kampanye *phishing* yang menargetkan Bank Rakyat Indonesia (BRI). Kampanye ini dimulai dengan serangan *phishing* kemudian mengambil OTP dari perangkat yang terinfeksi menggunakan *malware* Android. Situs *phishing* yang teridentifikasi meniru bank BRI ini memikat korban untuk mengirimkan kredensial perbankan dengan menawarkan tarif rendah pada setiap transaksi. Setelah mengirimkan kredensial pengguna, situs *phishing* meminta korban untuk mengunduh file APK yang merupakan SMS *stealer.* Oleh karena itu, para nasabah direkomendasikan untuk mengunduh perangkat lunak hanya dari toko resmi. Selain itu, pengguna juga dapat mengaktifkan 2FA seperti biometrik. Langkah lainnya yang dapat dilakukan adalah dengan berhati-hati dalam membuka tautan apapun yang diterima melalui SMS ataupun *email.*

Prioritas: *1. Critical*

< https://www.latimes.com/business/technology/story/2022-11-11/ransomware-gangs-shift-tactics-making-crimes-harder-to-track?&web_view=true >

Layani Penerbangan Tamu VVIP KTT G20 Bali, AirNav Optimalkan Berbagai Sistem Aplikasi dan Inovasi

AirNav Indonesia mencatatkan pergerakan lalu lintas penerbangan di ruang udara Bali terus meningkat seiring berakhirnya perhelatan Internasional Konferensi Tingkat Tinggi (KTT) Presidensi G20 Indonesia 2022, namun AirNav menjamin akan terus memberikan layanan navigasi penerbangan yang terbaik dan seoptimal mungkin. AirNav juga mengoptimalkan berbagai sistem aplikasi dan inovasi yang dimiliki, yakni CHRONOS, aplikasi pengaturan *slot time* penerbangan; *Ground Delay Program* (GDP) guna mengurangi *holding* pesawat di udara dan efisiensi bahan bakar pesawat; Nav-Earth, yang bekerjasama dengan BMKG guna mengetahui kondisi cuaca ter-*update*; E-FFORT, sistem pengaduan keadaan kondisi keselamatan penerbangan dan publikasi Aeronautical Information Publication (AIP); serta Notice To Airmen (NOTAM) ke para pengguna jasa navigasi penerbangan.

Prioritas: *3. Important*

< https://bali.tribunnews.com/2022/11/15/layani-penerbangan-tamu-vvip-ktt-g20-bali-airnav-optimalkan-berbagai-sistem-aplikasi-dan-inovasi= >

Breachs/Hacks/Leaks

Whoosh Mengonfirmasi Adanya *Data Breach* Setelah Peretas Menjual 7,2 Juta Catatan Pengguna

Layanan The Russion Scooter-Sharing telah mengonfirmasi adanya *data breach* setelah diketahui basis data yang berisikan 7,2 juta data pelanggan dijual di forum peretasan. Basis data tersebut juga berisikan sebagian detail yang berkaitan dengan kartu pembayaran milik pengguna. Penjual juga mengklaim bahwa data yang dicuri termasuk 3.000.000 kode promo yang dapat digunakan orang untuk menyewa skuter Whoosh tanpa membayar. Berkaitan dengan hal tersebut, Whoosh telah memberi tahu penggunanya bahwa mereka telah bekerja sama dengan otoritas penegak hukum untuk mengambil semua tindakan guna menghentikan distribusi data.

Prioritas: *3. Important*

< https://www.bleepingcomputer.com/news/security/whoosh-confirms-data-breach-after-hackers-sell-72m-user-records/?&web_view=true >

Vulnerabilities

Aktivitas DTrack Menargetkan Eropa dan Amerika Latin

DTrack adalah *backdoor* yang digunakan oleh grup Lazarus. Awalnya ditemukan pada Tahun 2019 dan tetap digunakan selama tiga tahun. DTrack memungkinkan penjahat untuk mengunggah, mengunduh, memulai, atau menghapus file di *host* korban. Di antara file yang diunduh dan dieksekusi terdapat *keylogger*, pembuat tangkapan layar, dan modul untuk mengumpulkan informasi sistem korban. DTrack sendiri tidak banyak berubah selama ini. Meski demikian, ada beberapa modifikasi menarik, Dtrack menyembunyikan dirinya di dalam program yang terlihat seperti program sah yang dapat dieksekusi dan ada beberapa tahap dekripsi sebelum muatan *malware* dimulai. *Backdoor* DTrack terus digunakan secara aktif oleh grup Lazarus. Modifikasi cara *malware* dikemas menunjukkan bahwa Lazarus masih melihat DTrack sebagai aset penting. Hal ini juga dapat dilihat dari aktivitas DTrack yang telah meluas ke Eropa dan Amerika Latin.

Prioritas: *2. Urgent*

< https://securelist.com/dtrack-targeting-europe-latin-america/107798/?web_view=true >

Kemampuan Baru Typhon Reborn *Crypto Miner*

Pada awal Agustus 2022, Cyble Research Labs menemukan *crypto miner* bernama Typhon Stealer. Tak lama kemudian, mereka merilis versi terbaru yang disebut Typhon Reborn. Kedua versi tersebut memiliki kemampuan untuk mencuri *crypto wallet,* dan menghindari produk antivirus. Versi baru ini telah meningkatkan teknik anti analisis dan lebih banyak fitur berbahaya. Typhon Reborn dirilis dengan beberapa fitur baru dan opsi yang dapat dikonfigurasi. Penulis juga menghapus beberapa fitur yang ada, termasuk kemampuan *keylogging* serta fitur pencurian *clipboard* dan *crypto mining*. Keylogging dan *crypto mining code* biasanya mudah dideteksi di platform analisis. Peneliti berspekulasi bahwa penghapusan fitur ini adalah untuk menurunkan kemungkinan pendeteksian antivirus.

Prioritas: *2. Urgent*

< https://unit42.paloaltonetworks.com/typhon-reborn-stealer/?web_view=true >

Peneliti Melaporkan *Critical* SQLi dan *Access Flaws* pada Layanan Zendesk Analytics

Peneliti keamanan siber telah mengungkapkan detail kelemahan yang sekarang sudah ditambal di Zendesk Explore yang dapat dieksploitasi oleh penyerang untuk mendapatkan akses tidak sah ke informasi dari akun pelanggan yang mengaktifkan fitur tersebut. Perusahaan keamanan siber mengatakan tidak ada bukti yang menunjukkan bahwa masalah tersebut dieksploitasi secara aktif dalam serangan dunia nyata sehingga tidak ada tindakan yang diperlukan dari pihak pelanggan. Kerentanan terkait dengan SQL *Injection* di API GraphQL-nya yang dapat disalahgunakan untuk mengekstraksi semua informasi yang disimpan dalam *database* termasuk alamat email.

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/11/researchers-reported-critical-sqli-and.html?&web_view=true >