www.idsirtii.or.id

20 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 108

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	1
URGENT	2	0	0
IMPORTANT	1	2	0

General News

Malware BRATA pada Perangkat Android

Kemunculan BRATA dimulai pada tahun 2019 sebagai *banking trojan* yang mampu melakukan tangkapan layar, instalasi aplikasi baru, dan mematikan layar seolah perangkat tampak mati. Pelaku ancaman di balik *malware* BRATA telah mengembangkan taktik dan kemampuan *malware* dalam mencuri informasi. BRATA telah diperbarui dengan teknik *phising* baru, kelas baru untuk meminta izin tambahan pada perangkat, dan *payload* tambahan dari server C2. Izin tambahan dimaksudkan untuk memungkinkan BRATA mengirim dan menerima SMS, yang dapat membantu penyerang untuk mencuri kode *One-Time Password* (OTP) dan *Two Factor Authentication* (2FA).

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/android-wiping-brata-malware-is-evolving-into-a-persistent-threat/ >

Temuan Aplikasi Kamera Populer yang Mengandung *Malware* pada Android

Google telah menghapus aplikasi populer PIP Pic Camera Photo Editor dari *app store* setelah mengetahui bahwa aplikasi ini mengandung *malware* yang dapat merusak dan mencuri kredensial Facebook, termasuk *username* dan *password*. Selain itu, *malware* ini juga memungkinkan peretas nuntuk mencuri data pribadi dan mengirim pesan penipuan ke kontak pengguna. Menurut laporan, terdapat empat aplikasi lainya yang mengandung *malware* dan mampu menampilkan iklan yang tidak diinginkan serta menekan masa pakai baterai. Para ahli menyarankan pengguna yang telah/pernah menginstal aplikasi terkait untuk segera menghapusnya dan mengganti kredensial Facebook.

Prioritas: *2. Urgent*

< https://www.thesun.co.uk/tech/18937643/warning-urgent-malware-android-google/ >

Microsoft Defender Telah Tersedia di iOS, Android, dan macOS

Microsoft telah menyediakan perlindungan Microsoft Defender sama seperti pada sistem Windows pada platform iOS, Android, dan macOS. Layanan ini tersedia sebagai bagian dari Microsoft 365 yang dirancang untuk menawarkan perlindungan terhadap ancaman *online* serta ancaman lokal. Pada Windows dan macOS, Microsoft Defender bekerja bersama antivirus bawaan atau pihak ketiga sekaligus memberikan perlindungan *phising* di internet. Pada Android, Microsoft Defender menyertakan antivirusnya sendiri bersama pemindaian *malware* untuk aplikasi yang saat ini diinstal dan baru diunduh. Pada aplikasi iOS, Microsoft Defender menyediakan perlindungan web dan memungkinkan pengguna melihat status keamanan perangkat lain tempat aplikasi diinstal.

Prioritas: *3. Important*

< https://nairametrics.com/2022/06/19/microsoft-defender-now-available-on-ios-android-and-macos/ >

Breachs/Hacks/Leaks

Peretas Targetkan Duppies dan Berhasil Kuras Beberapa *Wallet*

Komunitas Duppies NFT baru baru ini meramaikan Twitter akibat peretasan yang terjadi pad akun resmi Twitter Duppies NFT. Beberapa *wallet* milik pengguna Duppies NFT telah terkuras setelah menglik tautan "*stealth mint*" yang diumumkan melalui pengumuman akun Twitter Duppies NFT. Melalui tautan ini, beberapa pengguna secara efektif telah menyerahkan kendali *wallet* NFT mereka. Tim Duppies telah menghubungi Twitter Support untuk meminta agar mereka menutup halaman tersebut sebagai bagian pencegahan agar tidak ada lagi masyarakat yang terjerumus dalam eksploitasi tersebut. Tim Duppies juga memberikan $DUST gratis ke akun acak yang membantu mereka melaporkan peretasan.

Prioritas: *3. Important*

< https://nftevening.com/hackers-target-duppies-nft-and-successfully-drain-multiple-wallets/ >

Jutaan Data Warga India Bocor di *Dark Web*

Sebanyak 6.162.450 data pribadi warga India telah diretas dan bocor di *dark web* sejak Sabtu lalu yang dipelopori oleh DragonForce. Data yang meliputi nama, nomor kontak, lokasi, dan informasi media sosial pengguna India menunjuukkan bahwa data tersebut diretas melalui server raksasa media sosial terkemuka. Diketahui pula kelompok ini telah melakukan peretasan pada situs web pelabuhan utama India dan layanan logistik milik swasta. DragonForce membuang seluruh basis data pelabuhan, serta nama dan nomor kontak semua pengendara layanan logistik di *dark web* sebagai bukti eksploitasinya. Peretasan terhadap informasi pribadi sudah menjadi perhatian utama dunia karena menimbulkan berbagai bentuk kejahatan lainnya, seperti pemerasan, penipuan, dan lain-lain.

Prioritas: *3. Important*

< https://www.freepressjournal.in/india/cyber-attack-continues-on-india-as-hackers-leak-data-of-lakhs-of-citizens-on-dark-web >

Vulnerabilities

Lebih Dari Selusin Kerentanan Ditemukan pada Siemens Industrial Network Management System

Peneliti keamanan siber telah mengungkapkan perincian terhadap 15 kerentanan keamanan pada Siemens SINEC Network Management System (NMS), dilacak sebagai CVE-2021-33722 hingga CVE-2021-33736 yang telah diatasi dalam versu V1.0 SP2 Update 1. Kerentanan dapat menimbulkan sejumlah risiko pada perangkat Siemens, diantaranya *denial-of service,* kebocoran kredensial, dan *remote code execution*. Hal ini memungkinkan penyerang untuk mengeksekusi kode arbitrer pada sistem dengan hak istimwa. Kerentanan utama, CVE-2021-33723, memungkinkan eskalasi hak istimewa ke akun administrator dan dapat digabungkan dengan CVE-2021-33722 yang memungkinkan eksekusi kode arbitrer melalui jarak jauh. Kerentanan lainnya, CVE-2021-33729 berkaitan dengan SQL *Injection* yang dapat dimanfaatkan penyerang dalam mengeksekusi perintah arbitrer di basis data lokal.

Prioritas: ***1. Critical***

< https://thehackernews.com/2022/06/over-dozen-flaws-found-in-siemens.html >