www.idsirtii.or.id

22 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 218

OVERVIEW

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

General News

Malware Infostealer Aurora Semakin Diadopsi oleh Cybergangs

Penjahat dunia maya atau *cybergangs* semakin beralih ke pencuri informasi berbasis Go baru bernama 'Aurora' untuk mencuri informasi sensitif dari *browser* dan aplikasi mata uang kripto, mengekstraksi data langsung dari *disk*, dan memuat *payload* tambahan. Menurut firma keamanan siber SEKOIA, setidaknya tujuh *cybergang* terkenal dengan aktivitas signifikan telah mengadopsi Aurora secara eksklusif, atau bersama dengan Redline dan Raccoon, dua keluarga *malware* pencuri informasi lainnya. Alasan peningkatan popularitas Aurora ini adalah tingkat deteksi yang rendah dan status yang tidak diketahui secara umum, membuat infeksinya cenderung tidak terdeteksi. Secara bersamaan, Aurora juga menawarkan fitur pencurian data tingkat lanjut dan mungkin stabilitas infrastruktur dan fungsional.

Prioritas: ***2. Urgent***

<https://www.bleepingcomputer.com/news/security/aurora-infostealer-malware-increasingly-adopted-by-cybergangs/>

Breachs/Hacks/Leaks

Bjorka Jual Data PeduliLindungi, Kemenkes Sebut Tidak Ada Kebocoran

Peretas (*hacker*) Bjorka menjual 3,2 miliar data yang diklaim dari aplikasi PeduliLindungi US$ 100 ribu atau sekitar Rp 1,5 miliar di forum Breached.to. Namun, Kementerian Kesehatan (Kemenkes) menyebutkan bahwa tidak ada kebocoran data. “Sudah dicek. Tidak ada kebocoran data ya,” kata Juru Bicara Kemenkes Mohammad Syahril kepada Katadata.co.id, Senin (21/11). Pekan lalu, BSSN mengungkapkan bahwa *stakeholder* terkait tengah melakukan investigasi. Pihak terkait yang dimaksud yakni BSSN, Kementerian Kesehatan (Kemenkes), Kementerian Komunikasi dan Informatika (Kominfo), dan PT Telkom. Langkah-langkah teknis yang dilakukan di antaranya validasi data-data yang dipublikasikan oleh *threat actor* dengan data yang ada pada aplikasi PeduliLindungi, mengakuisisi *log firewall*, *imaging virtual machine*, dan *snapshot* aplikasi di server aplikasi PeduliLindungi.

Prioritas: ***1. Critical***

<https://katadata.co.id/desysetyowati/digital/637b61b24cca0/bjorka-jual-data-pedulilindungi-kemenkes-sebut-tidak-ada-kebocoran>

Kelompok Ransomware Daixin Mencuri 5 Juta Data Penumpang dan Karyawan AirAsia

Kelompok kejahatan dunia maya yang disebut Tim Daixin telah membocorkan data sampel milik AirAsia di portal kebocoran datanya. Perkembangan tersebut terjadi lebih dari seminggu setelah perusahaan menjadi korban serangan *ransomware* pada 11 dan 12 November, menurut DataBreaches.net. Pelaku ancaman diduga mengklaim telah memperoleh data pribadi terkait dengan lima juta penumpang unik dan seluruh karyawannya. Sampel yang diunggah ke situs bocoran mengungkapkan informasi penumpang dan ID pemesanan serta data pribadi terkait staf perusahaan. Seorang juru bicara pelaku ancaman mengatakan kepada DataBreaches.net bahwa serangan lebih lanjut tidak dilakukan karena langkah-langkah keamanan AirAsia yang buruk. Korban lain dari kelompok kriminal termasuk Rumah Sakit Fitzgibbon, Trib Total Media, International GmbH, dan OakBend Medical.

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/11/daixin-ransomware-gang-steals-5-million.html >

Ribuan Kunci API Algolia Dapat Mengekspos Data Pengguna

Lebih dari 1500 aplikasi telah ditemukan membocorkan kunci API & ID Aplikasi Algolia, berpotensi mengungkap data pengguna. Peneliti keamanan di CloudSEK berbagi data dengan *Infosecurity* sebelum dipublikasikan, menambahkan bahwa 32 dari aplikasi di atas ditemukan memiliki *hardcode* rahasia penting Admin dan sejauh ini tim telah mengidentifikasi 57 kunci admin yang unik. *Application Programming Interface* (API) Algolia memungkinkan pengembang menerapkan pencarian, penemuan, dan rekomendasi dalam situs web, aplikasi seluler, dan suara. Solusi ini digunakan oleh sekitar 11.000 perusahaan di seluruh dunia, termasuk Stripe, Slack, Medium, dan Zendesk, untuk mengelola 1,5 triliun permintaan pencarian yang dilaporkan setiap tahun. Kunci API admin dapat digunakan untuk mengakses berbagai Kunci API Algolia yang telah ditentukan sebelumnya, termasuk kunci API khusus Penelusuran, kunci API Pemantauan, kunci API Penggunaan, dan kunci API Analytics.

Prioritas: ***3. Important***

< https://www.infosecurity-magazine.com/news/algolia-api-keys-could-be-exploited/ >

Vulnerabilities

Kode PoC Diterbitkan Untuk *High-Severity* macOS *Sandbox Escape Vulnerability*

Seorang peneliti keamanan telah menerbitkan detail dan kode *proof-of-concept* (PoC) untuk kerentanan macOS yang dapat dieksploitasi untuk keluar dari *sandbox* dan mengeksekusi kode di dalam Terminal. Dilacak sebagai CVE-2022-26696 (skor CVSS 7,8), kerentanan keamanan telah diidentifikasi dan dilaporkan tahun lalu, dengan tambalan tersedia sejak rilis macOS Monterey 12.4 pada bulan Mei. Dalam imbauannya, Apple mencatat bahwa kerentanan tersebut memungkinkan proses *sandbox* untuk menghindari pembatasan *sandbox*, dan sanitasi lingkungan yang lebih baik menyelesaikan masalah tersebut. Eksploitasi kerentanan yang berhasil akan mengharuskan penyerang untuk dapat mengeksekusi *low-privileged code* pada sistem target. Penyerang yang dapat mengeksploitasi kerentanan ini dapat "meningkatkan hak istimewa dan mengeksekusi kode arbitrer dalam konteks pengguna saat ini.

Prioritas: ***2. Urgent***

<https://www.securityweek.com/poc-code-published-high-severity-macos-sandbox-escape-vulnerability?&web_view=true >

Google Mengidentifikasi 34 Versi Cracked dari Alat Peretasan Cobalt Strike Populer

Google Cloud minggu lalu mengungkapkan bahwa mereka mengidentifikasi 34 versi rilis yang diretas dari alat Cobalt Strike, yang paling awal dikirim pada November 2012. Versi, mulai dari 1.44 hingga 4.7, menambahkan hingga total 275 file JAR unik, menurut temuan dari tim Google Cloud Threat Intelligence (GCTI). Versi terbaru Cobalt Strike adalah versi 4.7.2. Cobalt Strike, dikembangkan oleh Fortra (née HelpSystems), adalah kerangka kerja populer yang digunakan oleh Red Team untuk mensimulasikan skenario serangan dan menguji ketahanan pertahanan dunia maya. Ini terdiri dari Server Tim yang bertindak sebagai hub *Command-and-Control* (C2) untuk menyita perangkat yang terinfeksi dari jarak jauh dan stager yang dirancang untuk mengirimkan muatan tahap berikutnya yang disebut Beacon, implan berfitur lengkap yang melaporkan kembali ke server C2. Mengingat rangkaian fiturnya yang luas, versi *software* ilegalnya semakin dipersenjatai oleh banyak *threat actor* untuk memajukan aktivitas pasca-eksploitasi mereka.

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/11/google-identifies-34-cracked-versions.html?&web_view=true >