'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 152 | 23 AGUSTUS 2023

OVERVIEW	Critical	Urgent	Important
General News	0	1	1
Breachs/Hacks/Leaks	0	1	2
Vulnerabilities	1	0	0
Malwares	1	1	0

General News

Apple Merilis *Security Update* untuk Mengatasi CVE-2023-23529

Apple telah meluncurkan pembaruan untuk kerentanan WebKit pada iPhone dan Mac yang dieksploitasi oleh *threat actor*. Kerentanan tersebut dilacak sebagai CVE-2023-23529 yang dapat dieksploitasi oleh *threat actor* dengan mengirimkan *url* berbahaya untuk masuk ke sistem iPhone, iPad, dan Mac. Pembaruan keamanan tersedia pada iPhone iOS 16.3.1, iPadOS 16.3.1, dan MacOS Ventura 13.2.1.

Prioritas : 3. Important
Sumber : https://www.bitdefender.com/blog/hotforsecurity/apple-patches-first-zero-day-flaw-reported-in-2023-on-ios-and-macos/

Puluhan *Adware* Android Terdeteksi Beredar pada Google Play Store

Perusahaan keamanan McAfee mendeteksi beberapa aplikasi yang mengandung *malware* pada Google Play Store. Sebanyak 43 aplikasi terdeteksi di mana telah diunduh lebih dari 2,5 juta pengguna. Sebagian besar aplikasi yang mengandung *malware* merupakan aplikasi *streaming* media dan berita. *Malware* yang terkandung dalam aplikasi tersebut merupakan *adware* yang dapat mengonsumsi daya baterai, data internet, penipuan *online*, atau menjadi pintu bagi serangan lebih lanjut.

Prioritas : 2. Urgent
Sumber : https://techno.okezone.com/read/2023/08/22/54/2869196/puluhan-aplikasi-berisi-malware-ditemukan-di-google-play-store-ini-cara-mengeceknya

Breachs/Hacks/Leaks

Gang Ransomware Akira Menargetkan Pengguna Cisco VPN

Peneliti keamanan siber Sophos mengamati aktivitas Gang Ransomware Akira yang menargetkan produk Cisco VPN untuk mendapatkan akses ke jaringan korban. Akira menargetkan organisasi yang menggunakan Cisco VPN tanpa menerapkan MFA. Akira terdeteksi menggunakan aplikasi *remote access* RusDesk yang sah untuk melakukan mekanisme *persistence* pada jaringan korban.

Prioritas : 2. Urgent
Sumber : https://securityaffairs.com/149770/malware/akira-ransomware-cisco-vpn.html

Gang Ransomware Snatch Menyerang Departemen Pertahanan Afrika Selatan

Gang Ransomware Snatch telah menambahkan Departemen Pertahanan Afrika Selatan ke dalam daftar korbannya. Snatch mengklaim telah mengambil data kontrak militer, data panggilan internal, dan data pribadi dengan ukuran 1,6 TB. Snatch melakukan *reboot* perangkat korban dan mengatur dalam *safe mode* untuk menghindari deteksi perimeter keamanan.

Prioritas : 3. Important
Sumber : https://securityaffairs.com/149760/cyber-crime/snatch-ransomware-department-of-defence-south-africa.html

Kelompok Peretas Ukraina "Cyber Resistance" Mengklaim Berhasil Meretas Parlemen Rusia

Sebuah kelompok peretas asal Ukraina yang menyebut diri mereka sebagai Cyber Resistance mengklaim telah berhasil meretas akun email seorang politisi senior Rusia, Alexander Babakov. Kelompok ini telah mempublikasikan 11 GB email yang diduga milik Babakov, yang merupakan wakil ketua parlemen Rusia, dengan tuduhan bahwa dokumen-dokumen tersebut membuktikan keterlibatannya dalam pencucian uang dan penghindaran sanksi.

Prioritas : 3. Important
Sumber : https://therecord.media/ukrainian-hackers-claim-to-leak-emails-of-russia-duma-deputy?&web_view=true

Vulnerabilities

Tim CSIRT India (CERT-In) Mendeteksi Kerentanan Baru pada Chrome

Tim CERT-In (India) mendeteksi adanya kerentanan pada browser Chrome dan telah memperingatkan pada situs resminya. Kerentanan pada Chrome tersebut memungkinkan *threat actor* melakukan *bypass security restrictions, execute arbitrary code, disclose sensitive information*, dan menyebabkan *denial of service* (DoS). Pengguna Chrome disarankan untuk melakukan pembaruan ke versi terbaru Chrome 116.0.5845.96 untuk Mac dan Linux serta Chrome 116.0.5845.96/.97 untuk Windows PC.

Prioritas : 1. Critical

Sumber : https://www.deccanherald.com/technology/gadgets/new-security-vulnerabilities-detected-on-chrome-warns-cert-in-2654658

Malwares

Malware-as-a-Service XLoader MacOS Menyamar sebagai Aplikasi OfficeNote

Peneliti keamanan SentinelOne mendeteksi aktivitas *malware* baru pada perangkat Apple MacOS. *Malware* tersebut disebut dengan XLoader yang menyamar sebagai aplikasi OfficeNote.dmg. XLoader merupakan *Malware-as-a-Service* (MaaS) yang dapat digunakan untuk mencuri informasi dan sebagai *keylogger* untuk dijual kepada *threat actor* lain. Dengan penyamaran sebagai aplikasi OfficeNote maka diindikasikan target dari XLoader merupakan pengguna di lingkungan pekerjaan.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/08/new-variant-of-xloader-macos-malware.html

Carderbee Menargetkan Organisasi di Aisa Menggunakan PlugX

Tim Threat Hunter Symantec melacak aktivitas serangan Carderbee. Aktivitas serangan tersebut memanfaatkan versi trojan dari perangkat lunak resmi yang disebut Cobra DocGuard Client. Aplikasi Cobra DocGuard merupakan aplikasi yang dikembangkan oleh Perusahaan China EsafeNet. Aplikasi tersebut dimanfaatkan untuk mengirimkan *backdoor* PlugX atau Korplug. Malware ditandatangani menggunakan sertifikat Microsoft yang sah dengan tujuan untuk menghindari deteksi. Aktivitas serangan Carderbee ditemukan di Hong Kong dan wilayah Asia.

Prioritas : 1. Critical
Sumber : https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse

KONTAK KAMI

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

@Id_SIRTII (+62) 21 7883 3610 bantuan70@bssn.go.id