'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 140 | 07 Agustus 2023

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

General News

4 Hacker Ungkap Alasan RI Jadi Sasaran Empuk Kejahatan Siber

Berdasarkan laporan lanskap keamanan siber 2023 dari Ensign Infosecurity, grup penjahat siber Desorden, Dark Pink, dan Naikon menjadi kelompok yang perlu diantisipasi. Sebab, ketiganya punya kemampuan bahasa Melayu yang dapat mendukung serangan. Menurut Vice President of Advisory, Consulting Ensign InfoSecurity, Teo Xiang Zheng, Malaysia dan Indonesia sebenarnya memiliki kelompok penyerang yang sama. Jadi, Malaysia dan Indonesia memiliki Dark Pink, Lotus Blossom, dan Naikon. Adapun sektor-sektor favorit sasaran para hacker adalah pemerintahan, layanan finansial, asuransi, dan industri komersial. Seperti contohnya, serangkaian serangan siber yang dilakukan oleh Desorden menyebabkan industri komersial terpukul secara signifikan. Mereka membobol data dan melakukan serangan ransomware terhadap usaha kecil dan menengah. Di samping itu, Ensign juga mendapati dua kerentanan yang seringkali dieksploitasi di Indonesia, yakni satu kerentanan dari tahun 2006 dan satu lagi dari tahun 2017. Dua kerentanan yang dimaksud adalah CVE-2017-0199 yang merupakan Arbitrary Code Execution di Microsoft Office 2007 sampai 2016, pada Windows Vista SP2 hingga Windows 8.1, serta Windows Server 2008 SP2; dan CVE-2006-1540 yang merupakan Denial of Service and Arbitrary Code Execution pada Microsoft Office 2000 hingga 2003.

Prioritas : 1. Critical
Sumber : https://www.cnbcindonesia.com/tech/20230805183448-37-460501/4-hacker-ungkap-alasan-ri-jadi-sasaran-empuk-kejahatan-siber

Google Terus Memperingatkan Pengguna Untuk Mengaktifkan Fitur *Enhanced Safe Browsing*

Google terus mengirimkan notifikasi melalui Gmail mengenai peringatan untuk mengaktifkan fitur *enhanced safe broswing.* Fitur ini dirilis sejak tahun 2007 sebagai peningkatan dari fitur *safe browsing* standar Google yang memberi peringatan kepada pengguna saat mereka mengunjungi situs phishing dan malware yang dikenal. Perbedaan antara kedua fitur keamanan ini adalah bahwa Safe Browsing akan membandingkan situs yang dikunjungi dengan daftar domain yang disimpan secara lokal, sedangkan Enhanced Safe Browser akan memeriksa apakah situs tersebut berbahaya secara real-time melalui layanan *Google cloud*. Namun, penggunaan *Enhanced Safe Browsing* sedikit mengorbankan privasi, karena Chrome dan Gmail akan berbagi URL dengan Google untuk memeriksa apakah mereka berbahaya dan sementara mengaitkan informasi ini dengan akun Google yang sudah masuk. Meskipun tujuan di balik fitur ini dimengerti - melindungi pengguna dari ancaman online potensial - dorongan agresif Google untuk mengadopsinya menimbulkan masalah. Peringatan berulang ini mungkin dianggap mengganggu oleh beberapa pengguna, dan ada keprihatinan privasi terkait fitur ini. Meskipun manfaat yang dijanjikan, tidak semua pengguna mungkin nyaman menghubungkan akun Google mereka dengan Chrome atau data penjelajahan dengan akun Google mereka.

Prioritas : 1. Critical
Sumber : https://www.opp.today/news2/google-gmail-continuously-nagging-to-enable-enhanced-safe-browsing/3245/

Breachs/Hacks/Leaks

Kelompok Clop Ransomware Menggunakan Torrents Untuk Membocorkan Data MOVEit

Geng ransomware Clop telah mengubah taktiknya sekali lagi dan kini menggunakan torrent untuk bocorkan data yang dicuri dalam serangan MOVEit. Pada tanggal 27 Mei, Clop ransomware meluncurkan serangkaian serangan pencurian data, yang tidak disadari oleh korban mereka, MOVEit, hingga 14 Juni. Awalnya, kelompok ini mulai memeras korban dengan melepaskan file yang dicuri di situs bocoran data Tor. Namun, metode ini terbukti lambat dan tidak seberbahaya yang mereka harapkan, karena kecepatan unduhan yang lambat. Untuk mengatasi hal ini, mereka membuat situs clearweb untuk membocorkan data yang dicuri, tetapi situs-situs ini lebih mudah untuk dihancurkan. Sebagai solusi atas masalah ini, Clop kini mulai menggunakan torrent untuk mendistribusikan data yang dicuri dari serangan MOVEit. Peneliti keamanan Dominic Alvieri menemukan taktik baru ini dan mengidentifikasi torrent untuk dua puluh korban, termasuk Aon, K & L Gates, Putnam, Delaware Life,

Zurich Brazil, dan Heidelberg. Clop telah mendirikan situs Tor baru yang memberikan instruksi tentang cara menggunakan klien torrent untuk mengunduh data yang bocor, beserta daftar tautan untuk dua puluh korban. Jika metode baru ini terbukti berhasil bagi Clop, mereka kemungkinan akan terus menggunakan torrent untuk bocoran data. Ini merupakan pengaturan yang lebih mudah, tidak memerlukan situs web yang kompleks, dan memiliki potensi untuk distribusi data yang dicuri yang lebih luas. Coveware memperkirakan bahwa Clop bisa mendapatkan $75 hingga $100 juta dalam pembayaran tebusan, karena mereka telah meyakinkan sejumlah kecil perusahaan untuk membayar tuntutan tebusan yang besar. Dampak penggunaan torrent terhadap jumlah pembayaran masih harus dilihat, tetapi dengan pendapatan yang signifikan, mungkin tidak akan menjadi masalah bagi kelompok ransomware ini.

Prioritas : 3. Important
Sumber : https://securityaffairs.com/149213/apt/bluecharlie-changes-attack-infrastructure.html

Kelompok APT BlueCharlie Mengubah Infrastruktur Serangan Setelah Adanya Laporan Mengenai Aktivitas Mereka

Peneliti di Recorded Future melaporkan bahwa kelompok APT BlueCharlie (atau juga dikenals ebagai Callisto, COLDRIVER, Star Blizzard, SEABORGIUM, dan TA446) mengubah infrastruktur serangannya setelah ada laporan mengenai aktivitas mereka. BlueCharlie utamanya berfokus menargetkan perusahaan konsultan intelijen, lembaga pemerintah dan non-pemerintah, ahli hubungan internasional Rusia, dan warga negara Rusia yang berada di luar negeri. Namun, kini BlueBharlie membangun infrastruktur serangan baru mulai Maret 2023 dan memiliki 94 domain baru. Para peneliti merekomendasikan organisai untuk menerapkan *multi-factor authentication*, mengganti password secara berkala, serta terus melatih kesadaran keamanan pada pegawai, kontraktor, hingga vendor pihak ke-tiga untuk selalu waspada

Prioritas : 3. Important
Sumber : https://securityaffairs.com/149213/apt/bluecharlie-changes-attack-infrastructure.html

Vulnerabilities

Microsoft Memperbaiki Kerentanan Setelah Dikritik Oleh CEO Tenable

Pada 20 Maret 2023, melalui Coordinated Vulnerability Disclosure (CND), Tenable menginformasikan kepada Microsoft mengenai adanya kerentanan pada Power Platform Custom Connectors dengan menggunakan kode yang dimodifikasi. Kerentanan ini memungkinkan pelanggan dapat menulis kode untuk *customer connectors.* Isu mengenai hal ini menjadi besar setelah CEO Tenable, Amit Yoran, mempublikasi sebuah tulisan di LinkedIn mengenai kelalaian Microsoft dalam menangani hal ini, dan

baru menangani kerentanan pada 6 Juli 2023. Setelahnya, Tenable memeriksa bahwa kerentanan tersebut masih dapat dieksploitasi. Sehari setelah artikel yang ditulis Yoran, Microsoft segera merilis perbaikan kerentanan ini dengan mengungkapkan bahwa mereka mengutamakan keseimbangan antara keterlambatan *response* dengan kualitas dalam perbaikan kerentanan. Amit Yoran diketahui pernah menduduki jabatan Direktur Keamanan Siber Nasional pada Department of Homeland Security.

Prioritas : 3. Important
Sumber : https://therecord.media/microsoft-resolves-vulnerability-following-criticism

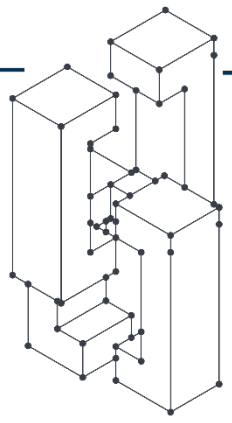
Malwares

Teknik Pencurian Data Dengan Memanfaatkan Malware pada Ponsel yang Dapat Mendeteksi Bunyi Ketukan Keyboard

Sebuah tim peneliti dari universitas-universitas Inggris telah melatih model pembelajaran mendalam yang dapat mencuri data dari ketukan tombol keyboard yang direkam menggunakan mikrofon dengan akurasi 95%. Saat Zoom digunakan untuk melatih algoritma klasifikasi suara, akurasi prediksi turun menjadi 93%, yang tetap sangat tinggi dan menjadi rekor untuk media tersebut. Serangan semacam ini sangat mempengaruhi keamanan data target, karena dapat membocorkan informasi sensitif seperti kata sandi, percakapan, pesan, atau informasi lainnya kepada pihak ketiga yang berniat jahat. Langkah pertama dari serangan ini adalah merekam ketukan tombol pada keyboard target, karena data tersebut diperlukan untuk melatih algoritma prediksi. Hal ini dapat dicapai melalui mikrofon yang berdekatan atau ponsel target yang mungkin telah terinfeksi malware yang memiliki akses ke mikrofonnya. Alternatifnya, ketukan tombol dapat direkam melalui panggilan Zoom di mana peserta rapat yang tidak sah membuat korelasi antara pesan yang diketik oleh target dan rekaman suaranya. Peneliti mengumpulkan data latihan dengan menekan 36 tombol pada MacBook Pro modern sebanyak 25 kali masing-masing dan merekam suara yang dihasilkan oleh setiap tekanan. Kemudian, mereka menghasilkan gelombang dan spektrogram dari rekaman yang memvisualisasikan perbedaan yang dapat diidentifikasi untuk setiap tombol dan melakukan langkah-langkah pemrosesan data tertentu untuk memperkaya sinyal yang dapat digunakan untuk mengidentifikasi ketukan tombol.

Prioritas : 2. Urgent
Sumber : https://technewsspace.com/a-new-algorithm-can-steal-data-by-analyzing-the-sound-of-keystrokes-with-up-to-95-accuracy/

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