www.idsirtii.or.id

30 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 224

OVERVIEW

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

General News

Tim AI dan Keamanan Siber BRIN Ciptakan Aplikasi Pengenal Wicara untuk Medis

Badan Riset dan Inovasi Nasional (BRIN) menciptakan aplikasi Sistem Pengenal Wicara untuk Pendiktean Medis (SPWPM). Sistem tersebut membantu para dokter menulis laporan diagnosis, memeriksa, dan memberikan konsultasi kepada pasien, secara langsung. Riset ini dimonitor dan dievaluasi langsung oleh Pusat Layanan Teknologi (Pusyantek) BRIN. Sistem tersebut hasil kerja sama tim perekayasa Pusat Riset Kecerdasan Artifisial dan Keamanan Siber- BRIN dengan PT Dua Empat Tujuh (Solusi247) dan Rumah Sakit Jantung dan Pembuluh Darah Harapan Kita. tim riset kecerdasan buatan dan keamanan siber BRIN telah menggeluti teknologi pengenalan wicara sejak 2010.

Prioritas: *3. Important*

< https://cyberthreat.id/read/14904/Tim-AI-dan-Keamanan-Siber-BRIN-Ciptakan-Aplikasi-Pengenal-Wicara-untuk-Medis >

Serangan Ransomware Baru di Ukraina Diduga Berasal Dari Sandworm

Serangan ransomware yang menargetkan organisasi di Ukraina dikaitkan dengan kelompok peretas dari Rusia yang terkenal, Sandworm. Perusahaan perangkat lunak Slovakia ESET yang pertama kali mendeteksi gelombang serangan ini, mengatakan ransomware yang mereka beri nama RansomBoggs telah ditemukan di jaringan beberapa organisasi Ukraina. Ransomware ini diketahui menggunakan skrip PowerShell untuk menyebarkan *payload* RansomBoggs bernama POWERGAP. Diketahui sebelumnya POWERGAP juga digunakan dalam mendistribusikan malware CaddyWiper dalam serangan terhadap organisasi Ukraina pada bulan Maret. RansomBoggs mengenkripsi file menggunakan AES-256 dalam mode CBC menggunakan kunci acak dan menambahkan ekstensi .chsch ke semua ekstensi file terenkripsi. Ransomware ini juga memberikan catatan tebusan dari James P. Sullivan, karakter utama film Monsters Inc.

Prioritas: *3. Important*

< https://www.bleepingcomputer.com/news/security/new-ransomware-attacks-in-ukraine-linked-to-russian-sandworm-hackers/ >

Breachs/Hacks/Leaks

Challenge TikTok "*Invisible Body*" Dimanfaatkan Untuk Mendistribusikan Malware

Peretas saat ini sedang memanfaatkan *Challenge* TikTok yang sedang tren bernama '*Inivsible Challenge*' untuk menyebarkan malware di ribuan perangkat yang memiliki kemampuan untuk mencuri kata sandi, akun Discord, dan, *cryptocurrency wallet*. *Challenge* TikTok sedang tren ini merupakan tantangan yang dibuat dimana pengguna Tiktok dapat merekam dirinya menggunakan filter yang membuat seakan-akan badan menjadi tidak terlihat atau tembus pandang. Nama filter Tiktok tersebut adalah "*Invisible Body*". Peretas memanfaatkan tren ini dengan membuat video mengklaim bahwa mereka dapat menghapus efek dari filter "*Invisible Body*" menggunakan *software* khusus sehingga dapat mengekspos badan pembuat video, tetapi *Software* ini berisi malware "WASP Stealer". Diketahui video tersebut telah ditonton lebih dari 1 juta kali.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/tiktok-invisible-body-challenge-exploited-to-push-malware/ >

Ransomware Trigona Meluncurkan Situs Negosiasi

Ransomware yang sebelumnya belum memiliki nama telah menamai dirinya dengan nama “Trigona”. Mereka telah aktif selama beberapa waktu kebelakang. Pada awal tahun ini telah didapatkan sampel dari ransomware tersebut dimana mereka belum memiliki nama sebagai identitas dan korban diarahkan melakukan negosiasi melalui email. Pada akhir Oktober 2022 tim dari MalwareHunterTeam, mendapatkan sampel ransomware ini dan diketahui bahwa mereka telah meluncurkan situs negosiasi pada TOR dan resmi menamakan diri mereka 'Trigona' dengan logo yang memperlihatkan seseorang dengan kostum lebah. Saat mengenkripsi file, Trigona akan mengenkripsi semua file di perangkat kecuali yang ada di folder tertentu, seperti folder Windows dan Program Files. Selain itu, ransomware akan mengganti nama file terenkripsi untuk menggunakan ekstensi ._locked. Ditandai dengan mereka telah meluncurkan situs pada TOR, menjadi tanda bahwa mereka akan meningkatkan serangannya. Akhir-akhir ini diketahui bahwa terdapat korban baru dari perusahaan real estate di Jerman.

Prioritas: *1. Important*

< https://www.bleepingcomputer.com/news/security/trigona-ransomware-spotted-in-increasing-attacks-worldwide/>

Aplikasi Android Berbahaya Mencuri Nomor Telepon Pengguna

Aplikasi SMS pada android Symoo dengan jumlah 100.00 unduhan di Play Store mengklaim dirinya sebagai aplikasi SMS yang memudahkan pengguna. Akan tetapi aplikasi ini merupakan aplikasi berbahaya. Aplikasi ini akan meminta izin akses untuk mengirim dan membaca SMS, pada tampilan awal aplikasi ini akan meminta pengguna untuk memasukkan nomor telepon mereka. Setelah proses itu, aplikasi akan berhenti berjalan dan pengguna akan menerima SMS yang berisi kode OTP pembuatan akun baru pada berbagai *platform* dimana mereka merasa tidak pernah membuat akun tersebut. Diketahui bahwa aplikasi ini mencuri nomor telepon pengguna untuk membuat akun pada berbagai aplikasi dan *platform* untuk dijual. Dari penelusuran yang dilakukan diketahui Symoo terhubung dengan aplikasi “*Virtual Number*” penjual layanan sewa nomor telepon, dimana pengguna dapat menyewa nomor dengan harga kurang dari 50 sen untuk membuat akun pada berbagai aplikasi.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/malicious-android-app-found-powering-account-creation-service/ >

Vulnerabilities

Acer Telah Memperbaiki Kerentanan Pada UEFI

Acer telah memperbaiki kerentanan dengan kategori *High* yang berdampak pada beberapa model laptop yang dapat memungkinkan penyerang untuk menonaktifkan UEFI Secure Boot pada sistem yang ditargetkan. Fitur keamanan Secure Boot merupakan fitur yang dapat memblokir bootloader sistem operasi yang tidak tepercaya pada perangkat komputer untuk mencegah aplikasi berbahaya seperti rootkit dan bootkit dimuat selama proses startup. Dilaporkan oleh peneliti malware ESET Martin Smolar, kerentanan ini didefinisikan sebagai CVE-2022-4020 telah ditemukan pada driver HQSwSmiDxe DXE pada beberapa perangkat Notebook Acer. Penyerang dapat menyalahgunakan kerentanan ini tanpa memerlukan interaksi pengguna untuk mengubah pengaturan UEFI Secure Boot dengan memodifikasi variabel NVRAM BootOrderSecureBootDisable dan menonaktifkan Secure Boot. Laptop Acer yang terkena dampak meliputi Acer Aspire A315-22, A115-21, A315-22G, Extensa EX215-21, dan EX215-21G. Pengguna perangkat tersebut dapat mengunduh pembaruan BIOS dari situs web dukungan perusahaan.

Prioritas: *2. Urgent*

<https://www.bleepingcomputer.com/news/security/acer-fixes-uefi-bugs-that-can-be-used-to-disable-secure-boot/ >

KONTAK KAMI

bantuan70@bssn.go.id

(021) 788 33610

Jl. Harsono RM No. 70
Kel. Ragunan, Kec. Ps. Minggu
Jakarta Selatan, 12550

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