'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 232 | 18 DESEMBER 2024

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

General News

Bitter APT Menargetkan Sektor Pertahanan Turki dengan Malware WmRAT dan MiyaRAT

Kelompok spionase siber yang diduga berasal dari Asia Selatan, yang dikenal sebagai Bitter, dilaporkan menargetkan sektor pertahanan di Turki dengan dua malware yang disebut sebagai WmRAT dan MiyaRAT. Serangan tersebut melibatkan penggunaan aliran data alternatif dalam arsip RAR untuk mengirimkan file pintasan (LNK) yang membuat tugas terjadwal di mesin target untuk menarik lebih banyak payload. Bitter, yang juga dikenal sebagai TA397, APT-C-08, APT-Q-37, Hazy Tiger, dan Orange Yali, telah aktif sejak 2013 dan sebelumnya menargetkan negara-negara seperti Cina, Pakistan, India, Arab Saudi, dan Bangladesh dengan malware seperti BitterRAT, ArtraDownloader, dan ZxxZ. Mereka juga terlibat dalam serangan siber yang menyebar malware Android seperti PWNDROID2 dan Dracarys. Pada bulan Februari 2024, Bitter melakukan serangan spear-phishing terhadap sebuah lembaga pemerintah Tiongkok yang tidak disebutkan namanya. Serangan ini melibatkan pengiriman trojan yang dapat mencuri data dan mengendalikan perangkat dari jarak jauh. Serangan ini menunjukkan bahwa Bitter memiliki fokus di Asia.

Prioritas : 1. Important
Sumber : https://thehackernews.com/2024/12/bitter-apt-targets-turkish-defense.html

Breachs/Hacks/Leaks

5 Juta Detail Kartu Pembayaran Dicuri Sebagai Pengingat untuk Memantau Pengeluaran Natal

Sebuah kebocoran data yang melibatkan 5 juta kartu pembayaran telah terjadi di Amerika Serikat. Tim keamanan Leakd.com menemukan bahwa 5 terabyte tangkapan layar yang berisi rincian sensitif telah terbuka di sebuah penyimpanan cloud Amazon S3 yang dapat diakses secara bebas. Pihak yang

bertanggung jawab atas kebocoran tersebut belum diketahui, tetapi tampaknya ini adalah hasil dari operasi phishing yang menargetkan kartu kredit dan debit. Informasi yang bocor terdiri dari tangkapan layar yang diambil dari komputer para korban yang mengisi rincian mereka di situs web yang menawarkan hadiah liburan dengan potongan harga besar. Meskipun belum diketahui siapa yang berada di balik kebocoran tersebut, tim Penyalahgunaan AWS telah memulai investigasi berdasarkan informasi yang diberikan oleh Leakd. Kebocoran ini menunjukkan pentingnya mengawasi pengeluaran selama musim liburan untuk melindungi diri dari penipuan online.

Prioritas : 1. Important

Sumber : https://www.malwarebytes.com/blog/news/2024/12/5-million-payment-card-details-stolen-in-painful-reminder-to-monitor-christmas-spending

Email Data Breach Ledger Palsu Baru Mencoba Mencuri Dompet Kripto

Sebuah kampanye phishing baru telah muncul menerobos sebagai pemberitahuan data breach dari perangkat keras dompet kripto, Ledger. Para penjahat mencoba mencuri frasa pemulihan pengguna yang digunakan untuk mengakses dan mencuri mata uang kripto. Ledger adalah dompet kripto yang aman yang menggunakan frasa pemulihan 24 kata untuk melindungi dana pengguna. Phishing Ledger telah menjadi masalah dalam beberapa waktu terakhir, dengan penjahat mencoba mencuri frasa pemulihan atau menjalankan perangkat lunak palsu untuk mencuri informasi pribadi. Setelah pelanggaran data yang terjadi pada 2020, kampanye ini semakin meningkat dengan penipuan email palsu berpura-pura sebagai pemberitahuan pelanggaran data terbaru. Email-email ini berjanji untuk memperbarui keamanan dengan meminta pengguna untuk memverifikasi frasa pemulihan mereka. Penting untuk diingat bahwa frasa pemulihan harus disimpan secara offline dan tidak pernah dibagikan kepada siapa pun.

Prioritas : 2. Urgent

Sumber : https://www.bleepingcomputer.com/news/security/new-fake-ledger-data-breach-emails-try-to-steal-crypto-wallets/

Vulnerabilities

NVIDIA Rilis Perbaikan untuk Masalah Performa Game dengan NVIDIA App Baru

NVIDIA telah berbagi perbaikan sementara untuk masalah performa game yang terkait dengan NVIDIA App yang baru diluncurkan. Masalah ini terjadi ketika opsi Game Filters diaktifkan dalam aplikasi, yang mengakibatkan penurunan performa game hingga 15%. NVIDIA merekomendasikan untuk menonaktifkan opsi Game Filters dan melakukan restart game sebagai solusinya. Masalah ini telah diakui oleh perusahaan dan mereka sedang menyelidikinya. Banyak pengguna melaporkan bahwa aplikasi ini mengurangi performa game di PC mereka ketika Game Filters atau Photo Mode diaktifkan, bahkan setelah menonaktifkan overlay dan filter lainnya. Beberapa pengguna terpaksa menghapus aplikasi ini karena masalah yang ditimbulkannya. Namun, ada juga yang mengatakan bahwa setelah menghapus aplikasi tersebut, masalah performa yang terjadi pada game mereka dapat teratasi. Hal

ini menunjukkan bahwa ada masalah yang perlu diperbaiki pada aplikasi tersebut, namun NVIDIA memberikan solusi sementara dengan menonaktifkan opsi Game Filters sebagai jalan keluarnya.

Prioritas : 2. Urgent
Sumber : https://www.bleepingcomputer.com/news/software/nvidia-shares-fix-for-game-performance-issues-with-new-nvidia-app/

CVE-2024-55661: Kerentanan RCE Ditemukan di Alat Pemantauan Pulsa Laravel

Celah keamanan telah ditemukan di Laravel Pulse, yang dapat memungkinkan pengguna yang diautentikasi mengambil alih server dan mengeksekusi kode sewenang-wenang. Kerentanan ini terletak di metode remember() dari properti RemembersQueries di komponen Livewire. Kerentanan ini dapat dieksploitasi untuk mengeksekusi pemanggilan fungsi atau metode statis di dalam aplikasi. Pengguna yang memiliki akses ke dasbor Pulse dapat memanfaatkan kelemahan ini untuk mengeksekusi perintah sistem, membaca file sensitif, atau bahkan mengendalikan server. Kerentanan ini memiliki dampak yang signifikan dan membutuhkan beberapa kriteria untuk berhasil dieksploitasi. Penemuan dan pelaporan kerentanan ini dilakukan oleh Jeremy Angele.

Prioritas : 1. Important
Sumber : https://securityonline.info/cve-2024-55661-rce-vulnerability-discovered-in-laravel-pulse-monitoring-tool/?&web_view=true

Malwares

Peretas Menggunakan File Microsoft MSC untuk Menyebarkan Backdoor dalam Serangan Pakistan

Sebuah serangan phishing baru yang menargetkan Pakistan menggunakan iming-iming pajak dan memanfaatkan file Microsoft MSC untuk menyebarkan pintu belakang yang disamarkan. Serangan ini diduga dimulai dengan tautan atau lampiran email phishing, tetapi tidak ada informasi yang diketahui mengenai email aslinya. Serangan ini menggunakan file MSC, yang merupakan file konsol Microsoft, untuk menjalankan kode berbahaya. File ini menyamar sebagai file PDF dengan ekstensi ganda (.pdf.msc) dan menggunakan Microsoft Management Console (MMC) untuk menjalankan kode JavaScript yang tersemat. Kode ini memuat file DLL ("DismCore.dll") di latar belakang sambil menampilkan file umpan. Salah satu dokumen yang digunakan dalam serangan ini berjudul "Pengurangan Pajak, Rabat dan Kredit 2024" dan terkait dengan Dewan Federal Pakistan. Serangan ini menunjukkan penyalahgunaan file MSC yang telah diberi nama kode GrimResource.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2024/12/hackers-use-microsoft-msc-files-to.html

Penyerang Mengeksploitasi Microsoft Teams dan AnyDesk untuk Menyebarkan Malware DarkGate

Baru-baru ini, penyerang telah menggunakan rekayasa sosial melalui panggilan Microsoft Teams untuk menyebarkan malware bernama DarkGate. Mereka berpura-pura menjadi klien pengguna dan mendapatkan akses jarak jauh ke sistem korban. Meskipun gagal menginstal aplikasi Microsoft Remote Support, penyerang berhasil menginstruksikan korban untuk mengunduh AnyDesk, sebuah alat yang biasanya digunakan untuk akses jarak jauh. Serangan dimulai dengan pemboman kotak masuk email target dengan ribuan email, di mana penyerang kemudian berpura-pura sebagai karyawan pemasok eksternal. Setelah itu, mereka memerintahkan korban untuk menginstal AnyDesk, yang kemudian disalahgunakan untuk mengirimkan pencuri kredensial dan malware DarkGate. DarkGate adalah trojan akses jarak jauh yang telah berevolusi menjadi penawaran malware-as-a-service (MaaS) dengan pelanggan yang dikontrol dengan ketat. Malware ini memiliki kemampuan mencuri kredensial, keylogging, penangkapan layar, perekaman audio, dan desktop jarak jauh. Kampanye DarkGate telah aktif sejak tahun 2018.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2024/12/attackers-exploit-microsoft-teams-and.html

Ditandatangani secara elektronik oleh:
DIREKTUR OPERASI KEAMANAN SIBER

Andi Yusuf, M.T.
Pembina Utama Muda (IV/c)

KONTAK KAMI

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

@Id_SIRTII (+62) 811 1065 2018 bantuan70@bssn.go.id