'Cyber blitz.
www.idsirtii.or.id

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 238 | 22 DESEMBER 2023

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

General News

First American Menonaktifkan Sistem TI Setelah Terjadi Serangan Siber

First American Financial Corporation, perusahaan asuransi terbesar kedua di US menonaktifkan sistem IT-nya sebagai dampak dari serangan siber. “First American telah mengalami insiden keamanan siber. Sebagai tanggapannya, kami telah membuat sistem tertentu offline dan berupaya untuk kembali ke operasi bisnis normal sesegera mungkin,” kata perusahaan itu dalam sebuah pernyataan yang dipublikasikan di situs web yang didedikasikan untuk serangan siber tersebut. Didirikan pada tahun 1889, First American menyediakan layanan keuangan dan penyelesaian kepada pembeli dan penjual rumah, profesional real estate, dan pihak lain yang terlibat dalam transaksi properti residensial dan komersial.

Prioritas : **3. Important**
Sumber : https://www.bleepingcomputer.com/news/security/first-american-takes-it-systems-offline-after-cyberattack/

Penguras Crypto Mencuri $59 Juta Dari 63 Ribu Orang Melalui Iklan di Twitter

Iklan Google dan Twitter mempromosikan situs yang berisi penguras mata uang kripto bernama 'MS Drainer' yang telah mencuri $59 juta dari 63,210 korban selama sembilan bulan terakhir. Menurut analis ancaman blockchain di ScamSniffer , mereka menemukan lebih dari sepuluh ribu situs web phishing menggunakan drainer tersebut dari Maret 2023 hingga hari ini, dengan lonjakan aktivitas yang diamati pada bulan Mei, Juni, dan November. Pengguna dibawa ke situs web phishing yang tampak sah dan ditipu untuk menyetujui kontrak jahat, sehingga memungkinkan drainer untuk secara otomatis melakukan transaksi tidak sah dan mentransfer uang korban ke alamat dompet penyerang.

Prioritas : **3. Important**
Sumber : https://www.bleepingcomputer.com/news/security/crypto-drainer-steals-59-million-from-63k-people-in-twitter-ad-push/

Breach/Hacks/Leaks

Serangan Phishing Menggunakan Kelemahan Microsoft Office Lama Untuk Menyebarkan Malware Agen Tesla

Pelaku ancaman mengeksploitasi kerentanan Microsoft Office lama, yang dilacak sebagai CVE-2017-11882 (skor CVSS: 7.8), sebagai bagian dari kampanye phishing untuk menyebarkan malware Agen Tesla. Agen Tesla adalah spyware yang digunakan untuk memata-matai korban dengan mengumpulkan penekanan tombol, clipboard sistem, tangkapan layar, dan kredensial dari sistem yang terinfeksi. Untuk melakukan ini, spyware membuat thread dan fungsi pengatur waktu yang berbeda di fungsi utama. Para ahli pertama kali menemukan malware tersebut pada bulan Juni 2018, namun malware tersebut telah tersedia sejak tahun 2014, ketika mereka mengamati pelaku ancaman menyebarkannya melalui dokumen Microsoft Word yang berisi VBA Macro berbahaya yang dapat dijalankan secara otomatis. Setelah pengguna mengaktifkan makro, spyware akan diinstal pada mesin korban. Dalam kampanye baru-baru ini, penyerang mengirimkan pesan spam menggunakan kata-kata seperti “pesanan” dan “faktur” dalam upaya mengelabui penerima agar membuka dokumen Excel yang berbahaya.

Prioritas : **2. Urgent**
Sumber : https://securityaffairs.com/156246/cyber-crime/agent-tesla-phishing-cve-2017-11882.html

Vulnerabilities

Ivanti Menambal 12 Kerentanan Kritis Pada Produk Avalanche MDM

Ivanti memberi tahu pelanggan tentang 20 kerentanan yang telah diperbaiki dalam produk manajemen perangkat seluler perusahaan (MDM) Avalanche, termasuk lebih dari selusin kelemahan yang memiliki tingkat keparahan 'kritis'. Avalanche digunakan oleh banyak organisasi untuk mengelola perangkat seluler mereka, memastikan perangkat tersebut aman, dapat diakses, dan tersedia. Produk ini dapat digunakan untuk mengelola berbagai perangkat, mulai dari pemindai gudang hingga tablet di lantai ritel. Avalanche 6.4.2 yang baru dirilis menambal 20 kerentanan yang memengaruhi semua versi produk lokal yang didukung — versi 6.3.1 dan yang lebih baru — serta rilis yang lebih lama. “Setelah mengetahui kerentanannya, kami segera memobilisasi sumber daya untuk memperbaiki masalah dan kini tersedia perbaikan untuk semua versi yang terkena dampak,” kata Ivanti dalam postingan blognya .

Prioritas : **2. Urgent**
Sumber : https://www.securityweek.com/ivanti-patches-dozen-critical-vulnerabilities-in-avalanche-mdm-product/

Malwares

Malware JavaScript Baru Menargetkan 50.000+ Pengguna di Puluhan Bank di Seluruh Dunia

Malware JavaScript baru telah diamati mencoba mencuri kredensial akun perbankan online pengguna sebagai bagian dari kampanye yang menargetkan lebih dari 40 lembaga keuangan di seluruh dunia. Cluster aktivitas, yang menggunakan injeksi web JavaScript, diperkirakan telah menyebabkan setidaknya 50.000 sesi pengguna terinfeksi yang tersebar di Amerika Utara, Amerika Selatan, Eropa, dan Jepang. Rantai serangan dicirikan oleh penggunaan skrip yang dimuat dari server yang dikendalikan pelaku ancaman ("jscdnpack[.]com"), yang secara khusus menargetkan struktur halaman yang umum di beberapa bank. Diduga malware tersebut dikirimkan ke target dengan cara lain, misalnya melalui email phishing atau malvertising. Saat korban mengunjungi situs web bank, halaman login diubah untuk memasukkan JavaScript berbahaya yang mampu mengambil kredensial dan kata sandi satu kali (OTP). Naskahnya dikaburkan untuk menyembunyikan maksud sebenarnya.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/12/new-javascript-malware-targeted-50000.html

Trojan Android “Chameleon” Memiliki Kemampuan Melakukan Bypass Otentikasi Biometrik

Peneliti keamanan siber telah menemukan versi terbaru dari malware perbankan Android bernama Chameleon yang telah memperluas targetnya hingga mencakup pengguna di Inggris dan Italia. Chameleon sebelumnya didokumentasikan oleh Cyble pada bulan April 2023, mencatat bahwa itu telah digunakan untuk memilih pengguna di Australia dan Polandia setidaknya sejak bulan Januari. Seperti malware perbankan lainnya, malware ini diketahui menyalahgunakan izinnya pada layanan aksesibilitas Android untuk mengambil data sensitif dan melakukan serangan overlay. Temuan terbaru dari ThreatFabric menunjukkan bahwa trojan perbankan kini dikirimkan melalui Zombinder , dropper-as-a-service (DaaS) siap pakai yang dijual ke pelaku ancaman lain dan dapat digunakan untuk "mengikat" muatan berbahaya ke aplikasi yang sah. Tambahan baru lainnya adalah penggunaan API Android untuk mengganggu operasi biometrik perangkat target dengan secara diam-diam mengalihkan mekanisme otentikasi layar kunci ke PIN sehingga memungkinkan malware untuk "membuka kunci perangkat sesuka hati" menggunakan layanan aksesibilitas.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/12/new-chameleon-android-banking-trojan.html

Ditandatangani secara elektronik oleh:
DIREKTUR OPERASI KEAMANAN SIBER

Andi Yusuf, M.T.
Pembina Tk. I (IV/b)

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