'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 229 | 13 DESEMBER 2024

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

General News

AS Berikan $5 Juta untuk Informasi Mengenai 'Peternakan IT' Korea Utara

Departemen Luar Negeri AS menawarkan hadiah hingga $5 juta bagi informasi yang dapat menghentikan aktivitas perusahaan proxy Korea Utara seperti Yanbian Silverstar di Tiongkok dan Volasys Silverstar di Rusia yang menghasilkan lebih dari $88 juta dalam enam tahun melalui pekerjaan IT ilegal. Kedua perusahaan ini merekrut pekerja Korea Utara sebagai tenaga lepas IT, menggunakan identitas curian warga AS untuk mendapatkan pekerjaan jarak jauh, kemudian mencuci uang hasilnya untuk mendukung program rudal nuklir Korea Utara yang dilarang PBB. Pada hari yang sama, Departemen Kehakiman mendakwa 14 pekerja "IT warriors" yang terlibat dalam pencurian identitas, penipuan, dan pencucian uang. Sebelumnya, pemerintah AS menyita sekitar $2,3 juta dalam beberapa aksi di 2022 dan 2023, termasuk 29 domain internet yang digunakan untuk memfasilitasi penipuan. Ancaman ini terus berkembang, dengan beberapa pekerja menggunakan keahlian coding mereka untuk memeras mantan pemberi kerja setelah dipecat. Terbaru, perusahaan KnowBe4 menjadi korban, merekrut aktor ancaman yang mencoba memasang malware meskipun proses perekrutan melibatkan pemeriksaan ketat. Kasus ini menyoroti bahaya yang terus berlanjut dari pekerja IT Korea Utara yang menyamar sebagai staf berbasis di AS.

Prioritas : 3. Important
Sumber : https://www.bleepingcomputer.com/news/security/us-offers-5-million-for-info-on-north-korean-it-worker-farms/

Kepolisian Spanyol Bongkar Jaringan 'Vishing' yang Menipu 10.000 Nasabah Bank

Kepolisian Spanyol, bekerja sama dengan pihak berwenang di Peru, berhasil membongkar jaringan besar penipuan suara (vishing) dan menangkap 83 pelaku di kedua negara. Sebanyak 35 pelaku ditangkap di berbagai kota di Spanyol, termasuk Madrid dan Barcelona, sementara 48 lainnya ditahan

di Peru, termasuk pemimpin jaringan tersebut. Dalam 29 penggerebekan simultan, polisi menyita uang tunai, ponsel, komputer, dan dokumen terkait. Jaringan ini menjalankan operasi panggilan palsu dari tiga call center dengan 50 agen, menggunakan teknologi pemalsuan nomor untuk menyamar sebagai bank resmi. Dengan database curian dan skrip manipulasi, mereka menipu korban untuk memberikan informasi sensitif seperti kode OTP dengan alasan ada aktivitas penarikan ATM yang mencurigakan. Kode ini diteruskan ke operator di dekat cabang bank untuk menarik uang tunai dengan sebagian hasil dikirim ke organisasi di Peru. Polisi mengingatkan publik bahwa bank tidak pernah meminta data pribadi atau kode OTP dan penting untuk selalu memverifikasi identitas agen sebelum memberikan informasi sensitif.

Prioritas : 3. Important
Sumber : https://www.bleepingcomputer.com/news/security/spain-busts-voice-phishing-ring-for-defrauding-10-000-bank-customers/

Breachs/Hacks/Leaks

Peretasan Byte Federal Ungkap Data 58 Ribu Pengguna

Perusahaan Bitcoin ATM asal AS, Byte Federal, mengalami peretasan pada November 2024 yang mengungkap data 58.000 pelanggan akibat kerentanan di GitLab. Byte Federal, operator ATM Bitcoin terbesar di AS dengan lebih dari 1.200 mesin di 42 negara bagian, mendeteksi pelanggaran ini setelah peretas mengakses server melalui celah keamanan di GitLab. Langkah darurat langsung dilakukan, termasuk menonaktifkan platform, mengisolasi peretas, dan mengamankan server yang terdampak. Meskipun tidak ada dana atau aset digital pelanggan yang dicuri, data sensitif seperti nama lengkap, alamat, nomor telepon, email, hingga SSN dan ID pemerintah terungkap, berpotensi memicu ancaman seperti serangan phishing atau pengambilalihan akun. Byte Federal telah memperbarui sistem keamanan internal, mengganti kata sandi, dan mencabut token akses, sementara investigasi forensik dengan bantuan ahli eksternal dan pihak berwenang masih berlangsung. Pelanggan disarankan untuk tetap waspada terhadap komunikasi mencurigakan, memantau laporan kredit, dan mengamankan kredensial login mereka. Dukungan tambahan disediakan melalui hotline dan email resmi perusahaan.

Prioritas : 3. Important
Sumber : https://www.bleepingcomputer.com/news/security/bitcoin-atm-firm-byte-federal-hacked-via-gitlab-flaw-58k-users-exposed/

Vulnerabilities

Kerentanan di Mobil Skoda & Volkswagen Buka Peluang Peretas Lacak Pengguna Secara Jarak Jauh

Peneliti keamanan siber menemukan kerentanan pada sistem infotainment beberapa model mobil Skoda dan Volkswagen yang memungkinkan peretas melacak lokasi pengguna dan mengakses data sensitif secara jarak jauh. PCAutomotive mengungkapkan 12 kelemahan pada Skoda Superb III 2022, khususnya pada unit infotainment MIB3 yang dapat disusupi malware untuk mengambil alih fungsi kendaraan tanpa otorisasi. Sekitar 1,4 juta kendaraan diperkirakan rentan terhadap serangan,

termasuk model dengan komponen aftermarket. Dengan hanya memanfaatkan koneksi Bluetooth dalam jarak 10 meter, peretas dapat melacak GPS, merekam suara, dan mengakses kontak telepon pemilik kendaraan. Volkswagen telah menanggapi laporan ini dengan memperbaiki kerentanan melalui program pengungkapan keamanan, memastikan tidak ada risiko bagi keselamatan pelanggan. Insiden ini menjadi pengingat pentingnya keamanan siber dalam kendaraan modern yang semakin kompleks dan terhubung. Industri otomotif perlu memperkuat protokol keamanan untuk melindungi privasi dan keselamatan pengguna secara menyeluruh.

Prioritas : 3. Important
Sumber : https://cybersecuritynews.com/vulnerabilities-skoda-volkswagen-cars/

Kerentanan di Facebook Messenger iOS Membuka Peluang Serangan Denial-of-Service Melalui Emoji

Penemuan baru tentang kerentanan di Facebook Messenger untuk iOS mengungkapkan celah serius yang dapat mengganggu panggilan grup melalui reaksi emoji. Kerentanan denial-of-service (DoS) ini teridentifikasi oleh Signal 11 Research pada versi 472.0.0 dan dianalisis lebih lanjut di versi 477.0.0, telah diperbaiki, namun dampaknya menyoroti risiko dari percakapan grup yang tidak terenkripsi. Messenger, yang digunakan oleh ratusan juta pengguna di seluruh dunia, memperkenalkan enkripsi ujung-ke-ujung (E2EE) untuk percakapan dan panggilan di Desember 2023. Namun, chat grup awalnya tidak memiliki E2EE yang memungkinkan fitur-fitur seperti reaksi emoji selama panggilan grup tidak tersedia dalam percakapan terenkripsi. Kerentanan ini disebabkan oleh pengiriman emoji reaksi tidak valid yang mengakibatkan aplikasi Messenger di perangkat iOS macet, memicu gangguan pada semua pengguna iOS dalam panggilan tersebut. Meta telah memperbaiki masalah ini di versi terbaru Messenger untuk iOS sehingga pengguna disarankan untuk memperbarui aplikasi mereka dan memanfaatkan E2EE untuk mengurangi risiko serupa yang terkait dengan fitur yang tidak terenkripsi.

Prioritas : 3. Important
Sumber : https://cybersecuritynews.com/vulnerabilities-skoda-volkswagen-cars/

Malware

Pumakit: Malware Rootkit Linux Baru yang Mengintai Secara Siluman

Malware rootkit baru bernama Pumakit ditemukan menginfeksi sistem Linux dengan teknik eskalasi hak istimewa yang canggih dan metode siluman untuk menyembunyikan keberadaannya. Elastic Security mendeteksi malware ini melalui unggahan file mencurigakan bernama 'cron' di VirusTotal pada 4 September 2024. Pumakit menggunakan proses infeksi multi-tahap, dimulai dengan dropper 'cron' yang memuat payload ke memori dan menginstal modul rootkit kernel 'puma.ko.' Modul ini dilengkapi Kitsune SO, rootkit userland yang menyisipkan diri ke proses menggunakan 'LD_PRELOAD' untuk mencegat sistem panggilan pengguna. Pumakit menargetkan kernel Linux sebelum versi 5.7, memanfaatkan fungsi 'kallsyms_lookup_name()' untuk mengubah perilaku sistem dan mengaitkan 18 syscall dengan 'ftrace' guna memperoleh akses root, mengeksekusi perintah, dan menyembunyikan aktivitas berbahaya. Rootkit ini menyembunyikan keberadaannya dari log kernel, alat sistem, dan

antivirus, serta dapat mengaburkan file, proses, dan koneksi jaringan tertentu. Kitsune SO juga bertugas berkomunikasi dengan server C2, menyampaikan perintah, dan mengirimkan informasi sistem kepada operator. Elastic Security telah merilis aturan YARA untuk membantu administrator mendeteksi serangan Pumakit.

Prioritas : 2. Urgent
Sumber : https://www.bleepingcomputer.com/news/security/new-stealthy-pumakit-linux-rootkit-malware-spotted-in-the-wild/

IOCONTROL: Malware Baru Menargetkan Infrastruktur Kritikal

Malware baru bernama IOCONTROL digunakan oleh aktor ancaman Iran untuk menyerang perangkat IoT dan sistem OT/SCADA di infrastruktur kritikal Amerika Serikat dan Israel. Malware ini dirancang modular sehingga mampu menyerang perangkat dari berbagai produsen seperti D-Link, Hikvision, dan Phoenix Contact. Menurut penelitian Claroty's Team82, IOCONTROL merupakan senjata siber yang dapat menyebabkan gangguan besar pada sistem seperti manajemen bahan bakar Orpak dan Gasboy. Aktor ancaman yang dikenal sebagai CyberAv3ngers mengklaim telah menginfeksi 200 stasiun pengisian bahan bakar, memungkinkan mereka mengendalikan pompa, terminal pembayaran, dan mencuri data. Malware ini menggunakan protokol MQTT untuk berkomunikasi dengan server C2, sementara konfigurasi dienkripsi dengan AES-256-CBC untuk meningkatkan keamanan. Selain itu, IOCONTROL mendukung berbagai fungsi, seperti pengumpulan informasi sistem, eksekusi perintah OS, dan penghapusan diri untuk menghindari deteksi.

Prioritas : 2. Urgent
Sumber : https://www.bleepingcomputer.com/news/security/new-iocontrol-malware-used-in-critical-infrastructure-attacks/

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