'Cyber blitz.
www.idsirtii.or.id

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 141 | 08 Agustus 2023

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

General News

FBI Memperingatkan Pengguna Terhadap Pencurian NFT Oleh Malware

Biro Investigasi Federal (FBI) telah mengeluarkan peringatan tentang peningkatan yang mengkhawatirkan dalam penipuan keuangan yang menargetkan pengguna aktif di dalam komunitas Token Non-Fungible (NFT). Para penjahat siber berpura-pura menjadi pengembang NFT yang sah dan menggunakan taktik canggih untuk menipu korban yang tidak curiga. Dalam skema penipuan ini, para penjahat entah mendapatkan akses yang tidak sah ke akun media sosial pengembang NFT atau membuat akun yang hampir identik untuk mempromosikan perilisan NFT baru. Untuk memikat korban, mereka menggunakan taktik yang menciptakan perasaan mendesak yang palsu, dengan menggunakan frase seperti "persediaan terbatas" dan mempromosikan perilisan NFT sebagai "kejutan" atau pencetakan yang sebelumnya tidak diumumkan."

Prioritas : 2. Urgent
Sumber : https://www.hackread.com/fbi-warns-nft-theft-malicious-developers/

Ajang dan Arena Olahraga Alami Peningkatan Ancaman Siber

Microsoft merilis laporan Cyber Signals edisi kelima – menyoroti ancaman terhadap arena besar, pertandingan olahraga, dan perhelatan hiburan, berdasarkan pembelajaran serta telemetri yang diperoleh ketika memberikan dukungan keamanan siber bagi sejumlah fasilitas infrastruktur penting selama Negara Qatar menjadi tuan rumah FIFA World Cup 2022. Ancaman keamanan siber terhadap perhelatan dan arena berskala besar sangat beragam dan kompleks. Ancaman ini membutuhkan

kewaspadaan dan kolaborasi yang konstan di antara para pemangku kepentingan untuk mencegah dan memitigasi eskalasi yang mungkin terjadi. Dengan nilai pasar olahraga global mencapai lebih dari USD600 miliar, tim olahraga, penyelenggara liga utama, asosiasi olahraga global, serta pengunjung menyimpan banyak informasi berharga yang diinginkan oleh penjahat siber. Microsoft Defender Experts for Hunting melakukan penilaian risiko awal dengan mempertimbangkan profil pelaku ancaman siber, sekaligus taktik, teknik, dan prosedur mereka, serta inteligensi global lainnya dari telemetri. Mereka mengaku telah menganalisis lebih dari 634,4 juta upaya otentikasi seraya memberikan pertahanan keamanan siber untuk fasilitas dan organisasi di Qatar sepanjang November dan Desember 2022.

Prioritas : 3. Important
Sumber : https://www.medcom.id/teknologi/news-teknologi/Wb7zZy2N-ajang-dan-arena-olahraga-alami-peningkatan-ancaman-siber

Breachs/Hacks/Leaks

Kebocoran Data Pemerintah Jepang Mungkin Disebabkan oleh Oknum Internal Yang Pro-China

NHK menemukan bahwa pusat keamanan siber pemerintah Jepang menggunakan sistem email yang disediakan oleh perusahaan AS yang dilaporkan diretas oleh kelompok yang diduga mendukung China. Pusat tersebut sedang menyelidiki pelanggaran dalam sistem tersebut. Pusat Keamanan Siber Kabinet mengatakan pada Jumat bahwa pada bulan Juni mereka mendeteksi masalah dengan sistem email tersebut. Hasil penyelidikannya menemukan bahwa beberapa data terkait email yang dikirim dan diterima antara awal Oktober tahun lalu dan pertengahan Juni kemungkinan telah bocor. Perusahaan keamanan siber Mandiant menyatakan bahwa badan pemerintah dan organisasi lain di seluruh dunia yang menggunakan sistem email dari perusahaan AS ini telah menjadi target sejak sekitar Oktober tahun lalu, dengan mengeksploitasi apa yang disebut "kerentanan nol-hari". Kelompok yang diduga sebagai pelaku adalah UNC4841. Mereka diyakini melakukan kampanye siber-espionase yang mendukung China. Dikatakan bahwa tujuan dari para peretas yang diduga adalah untuk mengumpulkan informasi terklasifikasi. Pemerintah Jepang sedang menyelidiki apakah kelompok ini terlibat dalam pelanggaran di Pusat Keamanan Siber Kabinet.

Prioritas : 3. Important
Sumber : https://www3.nhk.or.jp/nhkworld/en/news/20230805_09/

Vulnerabilities

Shadowserver Memperingatkan Kerentanan Kritikal pada Perangkat Citrix Yang Tengah Aktif Dieksploitasi

Shadowserver dan mitra-mitra terpercaya telah mengamati tiga kampanye berbahaya yang berbeda yang telah mengeksploitasi CVE-2023-3519, sebuah kerentanan injeksi kode yang dinilai kritis dengan skor CVSS 9.8 pada Citrix NetScaler ADC dan NetScaler Gateway. Pada 18 Juli 2023, Citrix merilis CTX561482 Buletin Keamanan Citrix ADC dan Citrix Gateway berisi imbauan dan perbaikan pada CVE-2023-3519, CVE-2023-3466, dan CVE-2023-3467. Serangan awal pada CVE-2023-3519 telah didokumentasikan dengan baik oleh CISA pada 20 Juli 2023 dalam dokulem laporan Cybersecurity Advisory Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells. Untuk membantu National CSIRTs dalam mengidentifikasi organisasi, Shadowserver telah menyediakan laporan identifikasi perangkat dan laporan kerentanan HTTP, yang dapat bermanfaat bagi organisasi untuk mengidentifikasi perangkat Citric Netscaler/Gateway yang terdampak. Dalam laporan itu juga disebutkan bahwa perangkat yang terdampak dan belum dilakukan patching sejak 20 Juli 2023, dipastikan sudah compromised.

Prioritas : 1. Critical
Sumber : https://www.shadowserver.org/news/technical-summary-of-observed-citrix-cve-2023-3519-incidents/

Malwares

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

Sebuah kampanye malware baru telah diamati menggunakan file konfigurasi OpenBullet yang berbahaya untuk menargetkan penjahat siber yang kurang berpengalaman dengan tujuan mengirimkan *remote access trojan* (RAT) yang mampu mencuri informasi sensitif. Perusahaan mitigasi bot, Kasada, mengatakan bahwa aktivitas ini dirancang untuk "mengeksploitasi jaringan kriminal yang tepercaya," menggambarkannya sebagai contoh dari pelaku ancaman canggih yang memangsa hacker pemula. OpenBullet adalah alat pengujian penetrasi open-source yang sah yang digunakan untuk mengotomatisasi serangan stuffing kredensial. Alat ini mengambil file konfigurasi yang disesuaikan dengan situs web tertentu dan dapat menggabungkannya dengan daftar kata sandi yang diperoleh melalui cara lain untuk mencatat upaya yang berhasil.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/08/new-malware-campaign-targets.html

Malware Jenis Baru: SkidMap pada Linux Menargetkan Kerentanan Redis Servers

Server Redis yang rentan tengah ditargetkan oleh sebuah malware baru bernama SkidMap yang dibuat untuk menargetkan pengguna Linux. Peneliti dari Trustwave menyatakan bahwa malwaren ini dapat beradaptasi dengan sistem yang ia infeksi. Beberapa distribusi Linux yang menjadi target SkidMap termasuk Alibaba, Anolis, openEuler, EulerOS, Stream, CentOS, RedHat, dan Rocky. SkidMap pertama kali diungkapkan oleh Trend Micro pada September 2019 sebagai botnet penambang kripto dengan kemampuan untuk memuat modul kernel berbahaya yang dapat menyembunyikan aktivitasnya serta memantau proses penambangan. Para operator malware ini juga ditemukan menyamarkan alamat IP *command & control* (C2) cadangan mereka di rantai blok Bitcoin, yang mengingatkan pada malware botnet lain yang dikenal sebagai Glupteba. Rantai serangan terbaru yang didokumentasikan oleh Trustwave melibatkan server Redis yang lemah keamanannya untuk mendistribusikan skrip *shell dropper* yang dirancang untuk mendistribusikan binary ELF yang menyamar sebagai berkas gambar GIF.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/08/new-skidmap-redis-malware-variant.html

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) 21 7883 3610 bantuan70@bssn.go.id