'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 151 | 22 AGUSTUS 2023

OVERVIEW	Critical	Urgent	Important
General News	0	0	1
Breachs/Hacks/Leaks	0	0	1
Vulnerabilities	3	0	0
Malwares	0	2	0

General News

Generasi Z Rentan Terhadap Bahaya Internet

Perusahaan keamanan siber Kaspersky telah memberikan peringatan kepada orang tua di Indonesia untuk tetap waspada terhadap risiko penggunaan internet saat anak-anak berada di usia sekolah. Kaspersky mengungkapkan bahwa Gen Z merupakan kelompok yang terlalu banyak berbagi *(oversharing)*. Mereka memiliki pengetahuan terkait keamanan internet namun paling rentan terhadap penipuan. Terdapat sekitar 55 % dari survei mengaku bahwa mereka telah memasukkan informasi pribadi seperti nama, tanggal lahir, dan alamat atau lokasi pada sosial media. Mayoritas dari mereka (72 %) tidak dapat mengidentifikasi kemungkinan *phishing* dan 26 % mengaku telah menjadi korban *phishing*.

Prioritas : 3. Important
Sumber : https://www.viva.co.id/digital/digilife/1629560-bahaya-internet-untuk-anak-anak

Breachs/Hacks/Leaks

Gang Ransomware BlackCat/ALPHV Menginfeksi Perusahaan Jam Tangan Seiko

Gang Ransomware BlackCat/ALPHV menambahkan Perusahaan Jam Tangan Seiko Jepang dalam daftar korbannya. Dalam sebuah posting, BlackCat mengklaim memiliki data rencana produksi, data paspor karyawan, data rencana peluncuran model baru, dan hasil uji laboratorium. Sebelumnya pada tanggal 10 Agustus 2023, Perusahaan mengungkapkan bahwa telah terjadi pelanggaran data oleh pihak ketiga yang tidak berwenang untuk melakukan akses pada sebagian infrastruktur TI dan mengakses atau mengambil data.

Prioritas : 3. Important

Sumber : https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/

Vulnerabilities

Kerentanan *Zero Day* dengan Kemungkinan Dampak Kritikal pada Ivanti Sentry

Perusahaan perangkat lunak TI Ivanti memberikan peringatan kepada pengguna Ivanti Sentry terkait dengan adanya *zero day*. Kerentanan yang dilacak sebagai CVE-2023-38035 dengan kemungkinan dampak kritikal memungkinkan penyerang yang tidak terautentikasi dapat mengakses ke API konfigurasi portal admin yang diekspos melalui port 8443. Port 8443 terekspos karena digunakan oleh MobileIron Configuration Service (MICS). Kerentanan tersebut berdampak pada Ivanti Sentry versi 9.18 dan sebelumnya. Pengguna Ivanti Sentry direkomendasikan untuk tidak mengekspos MICS ke internet dan membatasi akses ke jaringan manajemen internal.

Prioritas : 1. Critical
Sumber : https://www.bleepingcomputer.com/news/security/ivanti-warns-of-new-actively-exploited-mobileiron-zero-day-bug/

CISA Menambahkan Kerentanan Adobe ColdFusion pada Katalog KEV

The U.S Cybersecurity and Infrastructure Security Agency (CISA) telah menambahkan kerentanan dengan kemungkinan dampak kritikal pada Adobe ColdFusion ke dalam katalog *Know Exploited Vulnerabilities* (KEV). Kerentanan yang dilacak sebagai CVE-2023-26359 berdampak pada Adobe ColdFusion 2018 dan Adobe ColdFusion 2021 yang memungkinkan penyerang untuk melakukan eksekusi *arbitrary code*. Kerentanan tersebut diketahui hingga saat ini masih dieksploitasi secara aktif.

Prioritas : 1. Critical
Sumber : https://thehackernews.com/2023/08/critical-adobe-coldfusion-flaw-added-to.html

Kerentanan pada Perangkat IoT TP-Link Smart Bulbs

Peneliti dari Universitas Catania dan Universitas London menemukan kerentanan pada TP-Link Tapo L530E Smart Bulb dan aplikasi TP-Link Tapo. Terdapat 4 (empat) kerentanan yang berhasil diidentifikasi yaitu *improper authentication, hardcoded sensitive data, improper cryptography*, dan *improper session*. Hasil penelitian tersebut telah disampaikan kepada TP-Link dan akan segera dilakukan perbaikan pada aplikasi dan *firmware* Tapo L530E. Sebagai saran dalam penggunaan IoT, disarankan untuk perangkat IoT terisolasi dari jaringan penting, menggunakan *firmware* terbaru, serta menerapkan MFA dan kata sandi yang kuat.

Prioritas : 1. Critical
Sumber : https://www.bleepingcomputer.com/news/security/tp-link-smart-bulbs-can-let-hackers-steal-your-wifi-password/

Malwares

Threat Actor Mengirimkan *Malware* untuk Menjadikan Windows dan MacOS Sebagai Proxy Server

Peneliti keamanan AT&T Alien Labs mengamati aktivitas *threat actor* yang memanfaatkan perangkat Windows dan MacOS yang telah terinfeksi *malware* untuk mengirimkan aplikasi server proxy. Aplikasi server proxy tersebut digunakan sebagai *exit node* untuk merutekan kembali *proxy request*. *Server proxy* dikembangkan dengan menggunakan bahasa pemograman Go dan dapat menghindari deteksi dengan menggunakan tandatangan yang valid. Server proxy dapat dikendalikan secara *remote* dan dapat mengumpulkan informasi tentang sistem seperti proses yang berjalan, penggunaan CPU dan memori, serta status baterai.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/08/this-malware-turned-thousands-of-hacked.html

Malware HiatusRAT Menargetkan Organisasi Komersial, Pemerintahan, dan Militer

Peneliti keamanan Black Lotus Labs aktivitas *malware* HiatusRAT yang menargetkan organisasi komersial seperti produsen semikonduktor dan bahan kimia, organisasi pemerintah di Taiwan dan sistem pengadaan militer AS. Artefak HiatusRAT ditemukan telah dihosting pada *virtual private server* (VPS) baru. HiatusRAT pertama diungkapkan pada Maret 2023 yang menginfeksi di Amerika Latin dan Eropa. Sebanyak 100 perangkat jaringan telah terinfeksi secara global dan mengubah perangkat tersebut menjadi jaringan proxy *command and control* (CnC). Identitas *threat actor* dibalik *malware* HiatusRAT hingga saat ini masih belum diketahui.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/08/hiatusrat-malware-resurfaces-taiwan.html

KONTAK KAMI

DIREKTORAT OPERASI KEAMANAN SIBER
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