www.idsirtii.or.id

08 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 208

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	0
URGENT	2	1	1
IMPORTANT	0	1	1

General News

Azov *Ransomware* Hancurkan 666 Byte Data Sekaligus

Azov *ransomware* terus didistribusikan secara masif di seluruh dunia melalui *crack* dan *software* bajakan yang berpura-pura mengenkripsi *file* korban. Alih-alih memberikan informasi kontak untuk menegoisasikan uang tebusan, catatan yang dittinggalkan meminta korban untuk menghubungi peneliti keamanan dan jurnalis untuk menjebak mereka sebagai pengembang *ransomware*. Peneliti keamanan, Jiří Vinopal, mengonfirmasi bahwa *malware* ini dibuat khusus untuk merusak data. Peluncuran *malware* dilakukan melalui *backdooring* pada *executable. Backdooring file* bekerja dengan cara polimorfik, yang berarti *shellcode* yang sama yang digunakan untuk *file backdoor* setiap kali dikodekan berbeda. Azov akan menimpa konten *file* dan merusak data dalam potongan 666 *byte* data secara bergantian. *Threat actor* juga menggunakan Smokeloader untuk mendistribusikan data Azov, terdapat kemungkinan adanya instalasi *malware* lain dalam distribusi yang dilakukan, misalnya *malware* pencuri kata sandi.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/azov-ransomware-is-a-wiper-destroying-data-666-bytes-at-a-time/ >

SocGholish Mendiversifikasi dan Memperluas Infrastruktur *Malware*

SocGholish, *threat actor* berbasis JavaScript yang digunakan untuk mendapatkan *initial access* melalui *social engineering*, menipu pengguna agar menjalankan JavaScript *loader* yang menyamar sebagai pembaruan sistem atau perangkat lunak. Sejak pertengahan 2022, operator SocGholish secara signifikan mendiversifikasi dan memperluas infrastrukturnya untuk membuat *malware* dengan server baru. Ini membantu operator untuk melawan operasi defensif terhadap server yang dikenal dan meningkatkan operasi mereka. Setidaknya terdapat 18 server yang diperkenalkan operator SocGholish dengan *server uptimes* yang bervariasi. Dalam kampanye terbaru, SocGholish menginfeksi situs web yang sah dengan menginjeksi kode JavaScript dengan mekanisme *drive-by-download* yang memicu unduhan *payload* melalui *second-stage server*. Operator SocGholish mengaburkan URL ke *second-stage server* menggunakan pengodean Base-64 tunggal atau ganda.

Prioritas: ***2. Urgent***

< https://www.sentinelone.com/labs/socgholish-diversifies-and-expands-its-malware-staging-infrastructure-to-counter-defenders/?&web_view=true >

Breachs/Hacks/Leaks

Pakar Temukan Pemindai Keamanan URLScan Secara Tidak Sengaja Membocorkan URL dan Data Sensitif

Peneliti keamanan memperingatkan adanya data sensitif yang bocor melalui urlscan[.]io, pemindai situs web untuk URL yang mencurigakan dan berbahaya. UrlScan digambarkan sebagai *sandbox* untuk web, diintegrasikan ke dalam beberapa solusi keamanan melalui API-nya. Dengan jenis integrasi API ini, terdapat berbagai macam url dan data sensitif yang dapat dicari dan diambil oleh penyerang, mencakup tautan *reset* kata sandi, tautan berhenti berlangganan *e-mail*, URL pembuatan akun, kunci API, informasi tentang bot Telegram, permintaan penandatanganan DocuSign, tautan Google Drive bersama, transfer *file* Dropbox, tautan undangan ke layanan seperti SharePoint, Discord, Zoom, faktur PayPal, Cisco Rekaman rapat Webex, dan bahkan URL untuk pelacakan paket.

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/11/experts-find-urlscan-security-scanner.html >

Catatan Kesehatan Pelajar di Victoria Berpotensi Terdampak Akibat Peretasan Data di Perusahaan IT

PNORS Technology Group, perusahaan IT yang bekerja dengan enam departemen negara bagian yang berbeda, termasuk Pendidikan dan pelatihan, mengalami peretasan. Diketahui bahwa data kuisioner kesehatan pelajar di Victoria termasuk informasi yang dicuri. Kuisioner diisi oleh seluruh keluarga yang masuk di sekolah dasar Victoria, termasuk sekolah pemerintah, Katholik, dan independen. Informasi pribadi yang sensitif pada kuisioner meliputi demografi, masalah perkembangan dan perilaku, serta masalah alkohol atau obat-obatan dalam keluarga. Eksekutif PNORS, Paul Gallo, mengatakan bahwa *threat actor* telah merilis data yang berpotensi dicuri ke perusahaan pada hari Sabtu. Perusahaan telah melakukan respons insiden, termasuk memberi tahu klien yang terpengaruh dan melibatkan pakar keamanan siber eksternal untuk membantu penanganan masalah ini.

Prioritas: ***3. Important***

< https://www.theage.com.au/national/victoria/data-hack-at-it-firm-may-include-health-records-of-victorian-school-students-20221105-p5bvuz.html?&web_view=true >

Vulnerabilities

Apple Merilis Safari Technology Preview 157 dengan Perbaikan *Bug* dan Peningkatan Kinerja

Apple telah merilis pembaruan untuk Safari Technology Preview, *browser* eksperimental yang pertama kali diperkenalkan Apple pada Maret 2016. Pembaruan ini mencakup perbaikan *bug* dan peningkatan kinerja untuk Web Inspector, CSS, Rendering, JavaScript, WebCodecs, Web API, Media, Web Animations, HTML, Accessibility, Security, Privacy, dan Safari Web Extensions. Rilis ini dibangun atas pembaruan Safari 16 dan mencakup dukungan untuk fitur yang ada di macOS Ventura, seperti Live Text, Passkeys, peningkatan Web Extension, dan sebagainya. Versi baru Safari Technology Preview kompatibel dengan perangkat yang menjalankan macOS 13 Ventura, tidak seperti versi sebelumnya. Apple bertujuan untuk mengumpulkan umpan balik dari pengembang dan pengguna tentang peroses pengembangan *browser*-nya melalui Safari Technology Preview ini.

Prioritas: ***2. Urgent***

< https://www.macrumors.com/2022/11/07/apple-releases-safari-technology-preview-157/ >

Paket Microsoft WinGet Alami Kegagalan Akibat Masalah CDN

Windows Package Manager (WinGet) mengalami masalah dalam menginstal atau memutakhirkan paket akibat Azure Content Delivery Network (CDN) mengembalikan *file database* 0-*byte*. Pembaruan WinGet akan menampilkan kesalahan yang menyatakan *"Failed in attempting to update the source: winget" and winget install <program> would display the error, "An unexpected error occurred while executing the command: 0x8a15000f : Data required by the source is missing"*. Manajer Produk Microsoft, Demitrius Nelon, telah mengonfirmasi kesalahan ini untuk pengguna tertentu. Beberapa pengguna terlihat memodifikasi file HOSTS mereka dengan melakukan *pointing* ke alamat IP yang berfungsi untuk CDN, namun hal ini tidak menyelesaikan masalah yang ada,

Prioritas: ***3. Important***

< https://www.bleepingcomputer.com/news/microsoft/microsoft-winget-package-manager-failing-due-to-cdn-issues/ >