www.idsirtii.or.id

10 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 210

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	1
URGENT	3	1	1
IMPORTANT	0	1	0

General News

Malware Baru Bernama StrelaStealer Dapat Mencuri Akun Outlook dan Thunderbirds

Malware pencuri informasi jenis baru bernama StrelaStealer kini tengah aktif melakukan aksinya dalam pencurian kredensial akun Outlook dan Thunderbird, dua penyedia layanan *email* yang paling banyak digunakan masyarakat global. Aktivitas malware ini terdeteksi seperti *malware* pencuri data lainnya yang mencoba melakukan pencurian data seperti data *browser*, aplikasi dompet mata uang kripto, aplikasi gim *online*, maupun *clipboard*. Penemuan adanya *malware* ini diidentifikasi oleh analis keamanan siber di DCSO CyTec, yang melaporkan indikasi aktivitas *malware* ini pada awal November 2022. *Malware* ini diduga menargetkan pengguna yang berbahasa Spanyol. *Malware* ini menyebar melalui kampanye *phising*, yaitu melalui lampiran yang dikirimkan via *email* dengan tipe *file* .ISO, yang biasanya merupakan *file* gambar. *File* tersebut berisi muatan yang dapat dieksekusi dengan nama 'msinfo32.exe'. Meskipun *malware* ini diketahui menyebar di kalangan pengguna berbahasa Spanyol, namun DCSO CyTec sendiri belum dapat menyimpulkan apaka ada perluasan distribusi *malware* tersebut.

Prioritas: ***2. Urgent***

< https://medium.com/@DCSO_CyTec/shortandmalicious-strelastealer-aims-for-mail-credentials-a4c3e78c8abc >

Pakar Memperingatkan Munculnya *Malware* Ekstensi *Browser* yang Dapat Memata-matai Pengguna

Kelompok pelaku kejahatan siber, Keksec telah dikaitkan dengan jenis *malware* yang belum terdokumentasi. Mereka telah menciptakan *malware* baru yang diketahui mampu untuk menyamar sebagai ekstensi untuk *browser* web berbasis Chromium. Perangkat yang telah berhasil disusupi oleh *malware* ini akan menjadi *botnet* yang dikendalikan oleh peretas. Diberikan nama Cloud9 oleh perusahaan keamanan Zimperium, ekstensi *browser* berbahaya ini hadir dengan berbagai fitur yang memungkinkannya untuk mencuri *cookie*, mencatat penekanan tombol, menyisipkan kode berbahaya JavaScript, menambang koin kripto, dan bahkan memberikan perintah kepada *host* untuk melakukan serangan DDoS. *Malware* ini tidak disebarkan melalui Toko Web Chrome atau Microsoft Edge, melainkan disebarkan melalui situs web berbahaya yang menyarankan pengguna untuk mengunduh pembaruan Adobe Flash Player. *Malware* ini menginfeksi sistem dengan memanfaatkan kerentanan di *browser* web seperti Mozilla Firefox (CVE-2019-11708, CVE-2019-9810), Internet Explorer (CVE-2014-6332, CVE-2016-0189), dan Edge (CVE -2016-7200).

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/11/experts-warn-of-browser-extensions.html >

Tim Siber Polda Jawa Timur Tangkap Empat Tersangka Pembuat *Website* Paypal Palsu

Polda Jawa Timur berhasil menangkap empat tersangka kasus pemalsuan *website/scampage*, yaitu pemimpin kelompok Umbrella Corp dan tiga anggotanya. Wakil Kepala Polda Jawa Timur mengatakan bahwa pembuatan dan penyebaran *website* palsu ini mengatasnamakan perusahaan Paypal, tujuannya untuk mendapatkan data perbankan dan data pribadi milik warga di berbagai negara, kurang lebih 70 negara. Keuntungan yang telah diterima oleh kelompok peretas ini mencapai kurang lebih 5 Miliar. Pihak Polda Jawa Timur mengamankan 14 barang bukti berupa mobil, rumah, senpi, komputer, dan ATM. Pihaknya mengatakan bahwa keempat tersangka telah dijerat dengan Pasar 30 Ayat 2 dan Pasal 46 Ayat 2 UU RI Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dengan hukuman maksimal 7 tahun penjara.

Prioritas: ***2. Urgent***

< https://tribratanews.polri.go.id/blog/nasional-3/siber-polda-jatim-tangkap-4-tersangka-pembuat-website-paypal-palsu-51346 >

Breachs/Hacks/Leaks

Singapura Mengkonfirmasi Kebocoran Data Di Hotel Shangri-La Tidak Berdampak Besar Terhadap Acara Penting Tahun Ini

Insiden kebocoran data yang menimpa delapan cabang hotel Shangri-La dinyatakan tidak memberi dampak besar terhadap para delegasi luar negeri yang hadir di acara internasional bertema pertahanan negara yaitu: "The IISS Shangri-La Dialogue". Acara internasional bertaraf menteri tersebut dilaksanakan di hotel Shangri-L:a Singapura pada Juni 2022 lalu dan dihadiri oleh delegasi level atas dari berbagai negara. Delapan cabang hotel yang terdampak di antaranya Shanri-La SIngapura, Taipei, Hong Kong, dan Chiang Mai. Wakil Presiden Shangri-La Group menyatakan bahwa insiden siber tersebut dilakukan oleh aktor ancaman kelas kakap yang berhasil menerobos keamanan dan mengelabui sistem *monitoring* milik perusahaan. sehingga pelaku berhasil mengakses database para tamu hotel. Meskipun begitu, Shangri-La menyatakan bahwa data berupa nama, nomor paspor, NIK, tanggal lahir, dan nomor kartu kredit berada di database dalam keadaan terenkripsi.

Prioritas: ***3. Important***

< https://www.zdnet.com/article/shangri-la-hotel-data-breach-likely-had-minimal-impact-at-singapore-ministerial-summit/ >

15.000 Situs Diretas untuk *Poisoning Campaign* Besar-Besaran Google SEO

Peretas sedang melakukan *black hat search engine optimalization* (SEO) *campaign* dengan mengorbankan hampir 15.000 situs web untuk mengarahkan pengunjung ke forum diskusi tanya jawab palsu. Serangan pertama kali ditemukan oleh Sucui, yang mengatakan bahwa setiap situs yang disusupi berisi sekitar 20.000 *file* yang digunakan sebagai bagian dari *campaign,* sebagian besar merupakan situs WordPress. Situs-situs ini berkemungkinan dijadikan sebagai situs *dropper malware* atau situs *phising*. Sucuri melaporkan bahwa peretas memodifikasi *file* WordPress PHP, seperti 'wp-singup.php', 'wp-cron.php', 'wp-settings.php', 'wp-mail.php', dan 'wp-blog -header.php', untuk menginjeksikan pengalihan ke forum diskusi tanya jawab palsu. Sebagian besar situs web yang digunakan peretas menyembunyikan server mereka di balik Cloudflare. Direkomendasikan bagi pengguna WordPress dan CMS untuk meningkatkan situs ke versi terbaru dan mengaktifkan *two-factor authentication* (2FA) di akun admin.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/15-000-sites-hacked-for-massive-google-seo-poisoning-campaign/ >

Vulnerabilities

Patch code execution penting dari Apple – bukan *Zero-day*

Kali ini hanya ada dua perbaikan yang dilaporkan: untuk perangkat seluler yang menjalankan iOS atau iPadOS terbaru, dan untuk Mac yang menjalankan inkarnasi macOS terbaru, versi 13, lebih dikenal sebagai Ventura. Perbaikan tersebut yaitu HT21304: Ventura diperbarui dari 13.0 menjadi 13.0.1 dan HT21305: iOS dan iPadOS diperbarui dari 16.1 ke 16.1.1. Dua kelemahan persis sama yang ditemukan oleh tim Project Zero Google, di perpustakaan bernama libxml2 dan didaftarkan sebagai CVE-2022-40303 dan CVE-2022-40304. Kedua bug ditulis dengan catatan bahwa "pengguna jarak jauh mungkin dapat menyebabkan penghentian aplikasi yang tidak terduga atau eksekusi kode arbitrer". Apple sudah memaksa pembaruan pada iPhone unduhannya kecil dan pembaruan berjalan dengan cepat dan tampaknya lancar.

Prioritas: ***2. Urgent***

< https://nakedsecurity.sophos.com/2022/11/10/emergency-code-execution-patch-from-apple-but-not-an-0-day/ >

Peneliti Google Project Zero Melaporkan Vendor Pengawasan Mengeksploitasi Kerentanan *Zero-Day* Ponsel Samsung

Google Project Zero mengungkapkan tiga kerentanan ponsel Samsung yang dilacak sebagai CVE-2021-25337, CVE-2021-25369, dan CVE-2021-25370 yang telah dieksploitasi oleh vendor pengawasan. CVE-2021-25337 terkait kontrol akses yang tidak tepat dalam layanan *clipboard* di perangkat seluler Samsung sebelum SMR Mar-2021 Rilis 1 memungkinkan aplikasi yang tidak terpercaya untuk membaca atau menulis *file* lokal tertentu. CVE-2021-25369 terkait kerentanan kontrol akses yang tidak tepat dalam *file* sec_log sebelum SMR Mar-2021 Rilis 1 yang mengekspos informasi sensitif kernel ke ruang pengguna. CVE-2021-25370 terkait implementasi yang salah dalam menangani *file* deskriptor di *driver* dpu sebelum SMR Mar-2021 Rilis 1 menghasilkan kerusakan memori. Para ahli menjelaskan bahwa sampel eksploitasi menargetkan ponsel Samsung yang menjalankan kernel 4.14.113 dengan SOC Exynos.

Prioritas: ***1. Critical***

< https://securityaffairs.co/wordpress/138302/hacking/surveillance-vendor-exploited-samsung-phone-zero-days.html>