www.idsirtii.or.id

23 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 111

OVERVIEW

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

General News

RIG Exploit Kit Menginfeksi PC Korban dengan Dridex

Aktor dibalik Rig Exploit Kit telah menukar *malware* Raccoon Stealer dengan *financial trojan* Dridex sebagai bagian dari kampanye berkelanjutan yang dimulai sejak Januari 2022. Rig Exploit Kit terkenal dengan penyalahgunaan eksploitasi *browser* untuk mendistribusikan berbagai *malware*. Dridex sendiri memiliki kemampuan untuk mengunduh *loader* tambahan, menyusup ke *browser* untuk mencuri informasi *login* pelanggan yang dimasukkan pada situs web perbankan, menangkap tangkapan layar, dan melakukan perekaman *keystrokes*. Rig Exploit Kit ini memungkinkan penggantian *loader* yang cepat apabila terdeteksi atau disusupi.

Prioritas: *1. Critical*

< https://thehackernews.com/2022/06/rig-exploit-kit-now-infects-victims-pcs.html >

Tropic Tropper Menargetkan *Script Kiddies* dengan *Info-Stealer Trojan*

Peneliti keamanan siber telah menemukan kampanye baru yang dikaitkan dengan kelompok peretas Tropic Tropper, yang menggunakan *loader* baru bernama Nimbda dan varian baru *trojan* Yahoyah. *Trojan* dikemas dalam alat *greyware* bernama SMS Bomber, yang digunakan untuk melakukan serangan *denial-of-service* (DoS) terhadap ponsel. Alat seperti ini biasanya digunakan oleh peretas pemula yang ingin melancarkan serangan terhadap situs. Infeksi dimulai dari pengunduhan versi berbahaya SMS Bomber yang berisi fungsi biner dan standar alat. Eksekusi yang diunduh sebenarnya merupakan *loader* Nimbda yang menggunakan ikon SMS Bomber. *Loader* kemudian akan menginjeksikan *shellcode* ke dalam proses, mengambil *executable* yang disamarkan, melakukan *decode*, dan menjalankannya melalui dllhost.exe. *Payload* ini merupakan varian baru Yahoyah yang mengumpulkan data tentang *host* dan mengirimkannya ke server C2.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/chinese-hackers-target-script-kiddies-with-info-stealer-trojan/>

Breachs/Hacks/Leaks

Sirene Serangan Udara Palsu di Israel Kemungkinan Dipicu oleh Serangan Siber

Sirene serangan udara terdengar di kota-kota Israel di Yerusalem dan Eilat pada Minggu malam, dan nampaknya dipicu oleh serangan siber. Investigasi yang dilakukan oleh militer Israel menemukan bahwa alarm kemungkinan dipicu oleh serangan siber yang tampaknya menargetkan sistem alamat publik kota. Terdapat kemungkinan pula bahwa sirene tersebut hanyalah pengalih perhatian dari serangan lainnya apabila melihat kejadian sebelumnya. Contohnya, serangan siber Iran 2017 di Aramco Arab Saudi, dimana pelanggaran ditemukan untuk membuat ribuan sistem komputer dikompromikan, dan menyebabkan kehancuran atau ledakan yang besar.

Prioritas: *3. Important*

<https://www.securityweek.com/false-air-raid-sirens-israel-possibly-triggered-iranian-cyberattack?&web_view=true>

Vulnerabilities

Kerentanan Kritis PHP Memaparkan Perangkat QNAP NAS ke Serangan RCE

QNAP telah memperingatkan pelanggan bahwa beberapa NAS rentan terhadap serangan yang mengeksploitasi kerentanan PHP dan memungkinkan terjadinya *remote code execution*. Kerentanan mempengaruhi PHP versi 7.1.x sebelum 7.1.33, 7.2.x sebelum 7.2.24, serta 7.3.x sebelum 7.3.11. Pelanggan disarankan untuk memperbarui sistem secara berkala ke versi terbaru untuk mendapatkan manfaat dari perbaikan kerentanan. Vendor perangkat keras Taiwan juga telah menambal kerentanan CVE-2019-11043 untuk beberapa versi sistem operasi yang terkena dampak. Sementara itu QNAP telah menerbitkan imbauan keamanan QSA-22-20 dan bekerja untuk menambal kerentanan PHP CVE-2019-11043 di semua versi *firmware* yang rentan. QNAP menjelaskan bahwa perangkat dengan konfigurasi *default* tidak terpengaruh oleh CVE-2019-11043.

Prioritas: *1. Critical*

< https://www.bleepingcomputer.com/news/security/critical-php-flaw-exposes-qnap-nas-devices-to-rce-attacks/?&web_view=true >

Peneliti Ungkapkan Pemecahan Enkripsi Layanan Penyimpanan *Cloud* MEGA

Penelitian baru dari akademisi ETH Zurich telah mengidentifikasi adanya sejumlah masalah keamanan kritis dalam layanan penyimpanan *cloud* MEGA yang dapat dimanfaatkan untuk memecahkan kerahasiaan dan integritas pengguna. Peneliti menunjukkan bagaimana sistem tidak terlindungi dan membahayakan privasi *file* yang diunggah. Salah satu kerentanan utamanya yaitu RSA *key recovery attack* yang memungkinkan MEGA atau pelaku kejahatan mengendalikann infrastruktur API-nya untuk memulihkan kunci pribadi RSA pengguna. Serangan dapat dipersenjatai oleh MEGA atau entitas apapun yang mengendalikan infrastruktur intinya untuk mengunggah *file* yang mirip dan mendekripsi semua *file* dan folder yang dimiliki atau dibagikan dengan korban.

Prioritas: *1. Critical*

< https://thehackernews.com/2022/06/researchers-uncover-ways-to-break.html >

Google Memperbaiki 14 Kerentanan Melalui Rilis Chrome 103

Google telah mengumumkan rilis Chrome 103 sebagai perbaikan dari 14 kerentanan yang ada. Kerentanan terparah yaitu CVE-2022-2156 yang digambarkan sebagai kerentanan *use-after-free* dengan tingkap keparahan kritis. Kerentanan yang menyebabkan eksekusi kode arbitrer, kerusakan data, *denial-of-service*, kerentanan *use-after-free* ini dipicu ketika sebuah program mengosongkan alokasi memori tetapi tidak menghapus *pointer* setelahnya. Chromer 103 mengatasi tiga kerentanan *use-after-free* lainnya yang ditemukan oleh peneliti eksternal, yang memengaruhi komponen seperti Interest Group (CVE-2022-2157), WebApp Provider (CVE-2022-2161), serta Cast UI dan Toolbar (CVE-2022-2163). Pembaruan ini juga menyelesaikan masalah yang dilaporkan terkait V8 JavaScript dan WebAssembly (CVE-2022-2158) bersama empat masalah lainnya.

Prioritas: *1. Critical*

< https://www.securityweek.com/google-patches-14-vulnerabilities-release-chrome-103?&web_view=true >