www.idsirtii.or.id

17 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 107

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	0
URGENT	1	1	4
IMPORTANT	0	0	0

General News

Peneliti Lookout Mengungkap *Spyware* Android yang Digunakan di Kazakhztan

Peneliti Lookout Threat Lab telah menemukan Android *surveillanceware* tingkat perusahaan yang digunakan oleh pemerintah Kazakhstan. Berdasarkan hasil analisis para peneliti, *spyware* bernama "Hermit" tersebut kemungkinan dikembangkan oleh vendor *spyware* Italia RCS Lab S.p.A dan Tykelab Srl. Beberapa sampel Hermit telah terdeteksi sebelumnya dan secara luas dikenali sebagai *generic spyware*. Hermit adalah perangkat pengawasan modular yang menyembunyikan kemampuan jahatnya dalam paket yang diunduh setelah disebarkan. *Spyware* ini didistribusikan melalui pesan SMS yang berpura-pura berasal dari sumber yang sah. Hermit menipu pengguna dengan menyajikan laman *web* resmi dari merk yang ditirunya saat memulai aktivitas jahat di latar belakang. Hermit tidak hanya dikerahkan ke Kazakhstan, tetapi entitas pemerintah nasional kemungkinan berada di balik kampanye tersebut.

Prioritas: *2. Urgent*

< https://www.lookout.com/blog/hermit-spyware-discovery?&web_view=true >

Data Breach

Pesan *Phishing* yang Dikirimkan Melalui Facebook Mampu Menjerat 10 Juta Pengguna

Terdapat pesan *phishing* yang dibuat dengan baik dan dikirimkan melalui Facebook Messenger hingga mampu menjerat 10 juta pengguna Facebook dan terus bertambah setiap harinya. Menurut sebuah laporan kampanye *phishing* tersebut masih aktif dan terus mendorong korban ke halaman *login* Facebook palsu di mana korban dibujuk untuk menyerahkan kredensial Facebook mereka. Kredensial yang dimasukkan oleh korban akan dikirimkan ke server penyerang. Pelaku ancaman kemudian masuk ke akun korban dan mengirimkan tautan ke teman pengguna melalui Facebook Messenger. Para peneliti di PIXM Security mengungkap bahwa kampanye *phishing* dimulai tahun lalu dan meningkat pada Bulan September. PIXM menegaskan kampanye ini terkait dengan satu orang yang berlokasi di Kolombia. Alasan PIXM percaya bahwa penipuan Facebook besar-besaran ini berkaitan dengan satu individu adalah karena setiap pesan tertaut kembali ke situs *web* pribadi.

Prioritas: *2. Urgent*

< https://threatpost.com/acebook-messenger-scam/179977/ >

Vulnerabilities

MetaMask dan Phantom Memperingatkan Kerentanan Baru yang Berbahaya Bagi Crypto Wallets

MetaMask dan Phantom memperingatkan kerentanan baru yang dapat mengekspos *secret recovery phrase* sehingga memungkinkan penyerang untuk mencuri NFT dan *cryptocurrency* yang tersimpan di dalamnya. *Recovery phrase* merupakan serangkaian kata yang berfungsi sebagai wallet's *private key*. Siapapun yang mendapatkan akses ke *recovery phrase* dapat mengimpor wallet ke perangkat mereka sendiri sehingga memungkinkan penyerang untuk mencuri semua *cryptocurrency* dan NFTS yang tersimpan di dalamnya. Kerentanan ini ditemukan oleh Halborn pada September 2021 dan dilacak sebagai CVE-2022-32969. Kerentanan disebabkan oleh bagaimana *browser web* menyimpan masukan berupa kata sandi. Sebagai *browser* wallet *extensions*, Metamask, Phantom, dan Berani menyimpan *recovery phrase* yang dimasukkan pengguna dalam bentuk teks biasa. Hal ini tentu berbahaya apabila penyerang ataupun *malware* mendapatkan akses ke komputer pengguna.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/metamask-phantom-warn-of-flaw-that-could-steal-your-crypto-wallets/?&web_view=true >

Server Microsoft Exchange Diserang *Ransomware* BlackCat

Pertarungan antara Microsoft dengan *ransomware* semakin intens. Hal ini ditunjukkan dari serangan *ransomware* BlackCat yang mulai menyerang *server* Microsoft Exchange. Penyerang masuk melalui jaringan korban untuk kemudian mendapatkan kredensial dan mengekstrak informasi yang digunakan untuk *double extortion*. Pelaku ancaman menggunakan PsExec untuk menyebarkan muatan *ransomware* BlackCat ke seluruh jaringan, dua minggu setelah penetrasi awal menggunakan *server* Exchange yang belum ditambal. Kelompok kejahatan dunia maya FIN12 diduga terlibat dalam serangan ini. FIN12 terkenal karena sebelumnya menggunakan *ransomware* Ryuk, Conti, dan Hive dalam serangan.

Prioritas: *2. Urgent*

< https://cyware.com/news/microsoft-under-attack-by-blackcat-exchange-servers-hacked-9059bc2d >

Bug Sophos Firewall Zero-Day Dieksploitasi Sebelum Patch Dirilis

Peretas China menggunakan eksploitasi zero-day untuk *critical severity* pada Sophos Firewall guna menyusup ke perusahaan dan menembus *server web* yang dioperasikan korban. Masalah keamanan telah diperbaiki tetapi berbagai pelaku ancaman terus mengeksploitasinya untuk melewati otentikasi dan menjalankan kode arbitrer dari jarak jauh di beberapa organisasi. Pada tanggal 25 Maret, Sophos menerbitkan imbauan keamanan tentang CVE-2022-1040. Tiga hari kemudian, perusahaan memperingatkan bahwa pelaku ancaman memanfaatkan masalah keamanan untuk menargetkan beberapa organisasi di kawasan Asia Selatan. Minggu ini, perusahaan keamanan siber Volexity merinci serangan dari kelompok APT China yang mengeksploitasi CVE-2022-1040, tiga minggu sebelum Sophos merilis *patch*.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/sophos-firewall-zero-day-bug-exploited-weeks-before-fix/ >

730.000 Situs WordPress Diperbaharui Untuk Menambal *Bug Plugin*

Situs WordPress yang menggunakan Ninja Forms, telah diperbaharui secara massal minggu ini ke versi baru. *Code Injection Vulnerability* memengaruhi beberapa versi dari Ninja Forms dimulai dari versi 3.0 dan lebih tinggi. Eksploitasi yang berhasil memungkinkan mereka untuk sepenuhnya mengambil alih situs WordPress yang belum ditambal melalui beberapa rantai eksploitasi salah satunya menggunakan *remote code execution*. Meskipun belum ada pengumuman resmi, sebagian besar situs

web yang rentan tampaknya telah diperbarui secara paksa berdasarkan jumlah unduhan sejak kelemahan ini ditambal pada 14 Juni. Pembaruan keamanan telah diluncurkan lebih dari 730.000 kali sejak *patch* dirilis.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/730k-wordpress-sites-force-updated-to-patch-critical-plugin-bug/ >