CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 104

14 Juni 2022

OVERVIEW

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

General News

Peretas Rusia Mulai Menargetkan Ukraina dengan Eksploitasi Follina

Ukraine's Computer Emergency Response Team (CERT) memberikan peringatan terkait dengan kelompok peretas Rusia Sandworm yang mengekploitasi Follina, sebuah kerentanan eksekusi kode jarak jauh di Microsoft Windows Support Diagnostic Tool (MSDT) yang saat ini dilacak sebagai CVE-2022-30190. CERT-UA mengatakan bahwa peretas Rusia meluncurkan kampanye *malicious e-mail* baru yang memanfaatkan Follina dan menargetkan lebih dari 500 penerima di berbagai organisasi media di Ukraina, termasuk stasiun radio dan surat kabar. Sandworm telah menargetkan Ukraina secara terus-menerus selama beberapa tahun terakhir, dan frekuensi serangan meningkat setelah invasi Rusia ke Ukraina. Pada bulan April, ditemukan bahwa Sandworm menargetkan gardu listrik Ukraina menggunakan *malware* baru Industroyer. Pada Bulan Februari, peneliti keamanan menemukan bahwa Sandworm adalah kelompok yang bertanggung jawab untuk mengoperasikan *botnet* Cyclops Blink, *malware* yang sangat gigih yang mengandalkan manipulasi *firmware*.

Prioritas: *3. Important*

< https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/?&web_view=true >

Data Breach

Kredensial dari Ribuan *Open Source Projects* Bocor

Travis CI sebagai layanan yang membantu *open source developers* menulis dan menguji perangkat lunak membocorkan ribuan token otentikasi beserta data sensitif lainnya. Kebocoran ini memungkinakn peretas mengakses akun pribadi *developer* di GitHub, Docker, AWS, dan repositori. Penyerang dapat memanfaatkan kemampuan mereka untuk mengubah aplikasi dan menargetkan sejumlah proyek besar yang mengandalkan aplikasi di server produksi. Meskipun hal ini telah diketahui, namun kebocoran masih terus berlanjut. Setelah mengambil sampel data, para peneliti bahkan menemukan adanya 73.000 token dan berbagai kredensial lainnya. Contoh *access token* yang diekspos meliputi *access token* ke GitHub yang memungkinkan akses istimewa ke repositori kode, AWS *access keys*, sekumpulan kredensial (*e-mail, username, password*) yang memungkinkan akses ke *database* seperti MySQL dan PostgreSQL, serta Docker Hub Password yang memungkinkan pengambilalihan akun jika *multi-factor authentication* tidak diaktifkan.

Prioritas: *2. Urgent*

< https://arstechnica.com/information-technology/2022/06/credentials-for-thousands-of-open-source-projects-free-for-the-taking-again/?web_view=true >

Shoprite *Group* Mengeluarkan Peringatan Tentang *"Suspected Data Compromise"*

Shoprite *Group* mengatakan bahwa mereka telah mengetahui adanya dugaan *data compromise* termasuk di antaranya nama dan nomor ID yang berpengaruh pada beberapa pelanggan yang terlibat dalam transfer uang di Eswatini, Namibia, dan Zambia. Pelanggan terdampak akan menerima SMS ke nomor ponsel yang digunakan pada saat transaksi. Investigasi telah dilakukan oleh ahli forensik dan professional keamanan data lainnya untuk menetapkan asal, sifat, dan ruang lingkup dari insiden tersebut. Langkah-langkah keamanan tambahan untuk mengurangi dampak kehilangan data lebih lanjut diterapkan dengan mengubah proses otentikasi, *fraud prevention*, dan *detection strategies* untuk melindungi *customer data*. Akses ke area jaringan yang terpengaruh juga telah dikunci. Berkaitan dengan hal tersebut, para pengguna disarankan untuk tidak mengungkapkan informasi pribadi kepada siapapun, mengubah kata sandi secara teratur serta melakukan verifikasi pada setiap permintaan informasi pribadi.

Prioritas: *2. Urgent*

< https://www.sowetanlive.co.za/news/south-africa/2022-06-11-shoprite-group-issues-warning-on-suspected-data-compromise/?&web_view=true >

Vulnerabilities

Gallium *Hackers* Menggunakan *Malware* PingPull pada *Cyberespionage Attacks*

Sebuah APT dari China yang dikenal dengan nama Gallium diamati telah menggunakan *Remote Access Trojan* baru bernama PingPull, sebuah *backdoor* yang sulit dideteksi karena penggunaan *Internet Control Message Protocol* (ICMP) untuk komunikasi *command and control* (C2). PingPull merupakan *malware* berbasis Visual C++ yang memberikan kemampuan kepada aktor ancaman untuk mengakses *reverse shell* dan menjalankan perintah arbitrer pada *host* yang disusupi. Gallium dikenal karena serangannya yang ditujukan pada perusahaan telekomunikasi sejak tahun 2012. Gallium juga dilacak dengan nama Soft Cell oleh Cybereason dan diketahui menargetkan lima perusahaan telekomunikasi besar yang berlokasi di negara-negara Asia. Saat ini Galium tidak hanya menargetkan perusahaan telekomunikasi namun meluas pada sektor keuangan, organisasi dan pemerintah di seluruh Asia Tenggara, Eropa, dan Afrika. Meskipun penggunaan *tunneling* ICMP bukanlah teknik baru, namun penggunaan ICMP pada PingPull mempersulit deteksi karena hanya sedikit organisasi yang menerapkan pemeriksaan lalu lintas ICMP pada jaringan mereka.

Prioritas: *1. Critical*

< https://thehackernews.com/2022/06/chinese-gallium-hackers-using-new.html >

Chinese Hackers Mendistribusikan *Backdoored* Web3 Wallet untuk Pengguna Ios dan Android

Pelaku ancaman yang secara teknis dikenal sebagai SeaFlower telah menargetkan pengguna Android dan iOS sebagai bagian dari kampanye ekstensif yang meniru situs Web3 Wallet Cryptocurrency resmi yang bermaksud mendistribusikan *backdoor* yang menguras dana korban. Modus operandi SeaFlower melibatkan pengaturan situs *web* kloning yang bertindak sebagai saluran untuk mengunduh versi trojan dari aplikasi Wallet. Aktivitas berbahaya ini juga dirancang untuk menargetkan pengguna iOS dengan cara menyediakan profil yang memungkinkan aplikasi dipindahkan ke perangkat.

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/06/chinese-hackers-distribute-backdoored.html >

Syslogk Linux Rootkit Baru Menggunakan *Magic Packets* Untuk Memicu *Backdoor*

Malware Rootkit Linux baru bernama 'Syslogk' digunakan dalam serangan yang bertujuan untuk menyembunyikan proses berbahaya menggunakan "magic packet"

yang dibuat khusus untuk men-*trigger backdoor* yang aktif di perangkat. Rootkit Linux adalah *malware* yang diinstal sebagai modul kernel di sistem operasi. Setelah diinstal, mereka melakukan *intercept* perintah Linux yang sah untuk menyaring informasi yang tidak ingin ditampilkan, seperti keberadaan file, folder, atau proses. Ketika pertama kali dimuat sebagai modul kernel, Syslogk akan menghapus entrinya dari daftar modul yang diinstal untuk menghindari pemeriksaan manual.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/new-syslogk-linux-rootkit-uses-magic-packets-to-trigger-backdoor/?&web_view=true >