www.idsirtii.or.id

28 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 222

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	0
URGENT	0	3	1
IMPORTANT	2	0	0

General News

Mahkamah Konstitusi Bentuk Tim Respon Ancaman Siber

Mahkamah Konstitusi (MK) bersama dengan Badan Siber dan Sandi Negara (BSSN) meluncurkan *Computer Security Incident Response Team* (CSIRT) yang diberi nama MK-CSIRT. Pelaksana tugas (Plt) Kepala Pusat Teknologi Informasi dan Komunikasi, Sigit Purnomo mengatakan sejak awal MK didesain sebagai lembaga negara yang modern dan terpercaya. Seluruh kegiatan MK dilaksanakan secara efektif dan efisien dengan menggunakan teknologi informasi dan komunikasi. Diharapkan MK-CSIRT dapat memberikan pemahaman bersama serta menunjukkan komitmen mewujudkan dan meningkatkan ketahanan siber dalam pelaksanaan tugas dan fungsi MK yang lebih baik. Sementara itu, Plt. Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia BSSN Hasto Prastowo mengatakan, "Pembentukan CSIRT merupakan salah satu langkah konkret dalam upaya BSSN mewujudkan keamanan siber di Indonesia".

Prioritas: *3. Important*

< https://www.inews.id/news/megapolitan/mk-gandeng-bssn-kelola-sistem-informasi-dan-komunikasi >

Black Basta dan Qakbot Menargetkan Perusahaan Amerika Serikat

Peneliti Cybereason berhasil mengidentifikasi bahwa telah terjadi kampanye serangan malware Qakbot (QBot atau Pinkslipbot) yang tersebar luas dengan menargetkan perusahaan yang berbasis di AS. Diduga kelompok kejahatan ransomware, Black Basta berada di belakang kampanye serangan ini. Sejak pertengahan November, Black Basta telah menyebarkan email phishing untuk mendistribusikan tautan URL dan file gambar berbahaya. URL atau file ini berisi muatan Qakbot, yang menjadi titik masuk awal di jaringan korban. Setelah itu, Qakbot akan mengunduh Cobalt Strike dari server penyerang. Cobalt Strike digunakan untuk mendapatkan hak istimewa administrator dari jarak jauh. Pada tahap ini, penyerang sudah dapat mencuri kredensial dan melakukan pergerakan lateral. Setelah itu, penyerang dapat mengenkripsi seluruh file di komputer korban dan meminta tebusan. Tentunya kampanye serangan ransomware ini patut untuk diwaspadai oleh setiap organisasi dengan meningkatkan tindakan pendeteksian dan pencegahan serangan siber.

Prioritas: *3. Important*

< https://thehackernews.com/2022/11/black-basta-ransomware-gang-actively.html >

Breachs/Hacks/Leaks

Server Boa Dimanfaatkan oleh Penyerang Dengan Menargetkan Sektor Industri Kritikal

Peneliti Microsoft telah mengidentifikasi bahwa terdapat komponen yang rentan dari server web Boa yang dapat menimbulkan resiko serangan rantai pasokan (*supply chain attack)* yang dapat mempengaruhi jutaan organisasi yang masih menggunakan server web Boa. Dari laporan peneliti tersebut, komponen rentan sulit untuk diidentifikasi akan tetapi memungkinkan untuk dieksploitasi dengan menargetkan industri-industri kritikal. Seperti yang diketahui, Boa web server telah menghentikan pengembangannya pada tahun 2005, akan tetapi masih banyak organisasi dan vendor dari berbagai produk seperti perangkat IoT, router, dan kamera yang masih menggunakannya. Diketahui lebih dari satu juta server Boa yang telah diidentifikasi terdampak di seluruh dunia selama rentang waktu seminggu. Disarankan setiap organisasi untuk memeriksa dan mewaspadai potensi serangan siber dari kerentanan yang ditemukan.

Prioritas: *2. Urgent*

< https://cyware.com/news/abandoned-boa-servers-abused-by-chinese-attackers-to-target-critical-industries-af7742a1 >

Bahamut Menargetkan Pengguna Android dengan Aplikasi VPN Bajakan

Kelompok serangan siber yang dikenal dengan nama Bahamut telah dikaitkan sebagai pelaku dibalik kampanye serangan siber yang menginfeksi pengguna perangkat Android dengan aplikasi berbahaya yang dirancang untuk mengambil informasi sensitif. Bahamut telah aktif melakukan kampanye serangan ini sejak Januari 2022. Keterangan dari perusahaan keamanan siber Slovakia ESET, setidaknya terdapat delapan varian berbeda dari aplikasi *spyware* telah ditemukan hingga saat ini, diantaranya adalah aplikasi VPN bajakan tiruan SoftVPN dan OpenVPN. Aplikasi bajakan dan pembaruannya ini tidak tersedia di Play Store melainkan didistribusikan ke pengguna melalui situs web palsu. Diketahui bahwa aplikasi bajakan tersebut dapat mencuri banyak informasi, termasuk file, daftar kontak, SMS, rekaman panggilan telepon, lokasi, dan pesan dari WhatsApp, Facebook Messenger, Signal, Viber, Telegram, dan WeChat.

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/11/bahamut-cyber-espionage-hackers.html >

Aplikasi Pengelola File Android Berbahaya Menyebabkan Infeksi Malware SharkBot Pada Ribuan Perangkat

Malware pencuri informasi perbankan pada Android yang dikenal sebagai SharkBot telah muncul kembali di platform Google Play Store resmi. Malware ini disamarkan sebagai aplikasi pengelola file. Diketahui dalam sebuah analisis yang diterbitkan minggu ini, aplikasi pengelola file berbahaya ini telah diunduh oleh pengguna mayoritas berada di negara Inggris dan Italia, kata perusahaan keamanan siber Rumania, Bitdefender. SharkBot, pertama kali ditemukan menjelang akhir tahun 2021 oleh Cleafy. Salah satu tujuan utama SharkBot adalah untuk mengalihkan transaksi uang yang seharusnya diterima oleh korban akan tetapi melalui perangkat yang terinfeksi transaksi tersebut dialihkan ke akun pengendali dari Sharkbot ini. Selain itu, Sharkbot juga memiliki kemampuan untuk meniru *overlay* tampilan login palsu dari aplikasi perbankan yang digunakan yang menyerupai tampilan aslinya dengan tujuan untuk mengelabui korban sehingga penyerang dapat mencuri kredensial akun perbankan tersebut.

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/11/this-android-file-manager-app-infected.html >

Vulnerabilities

Jutaan Perangkat Android Saat Ini Belum Memiliki *Patch* Perbaikan Untuk Kerentanan Pada GPU Mali

Kumpulan lima kerentanan keamanan pada perangkat Android dengan tingkat *severity medium* pada driver GPU Mali Arm masih belum diperbaiki selama berbulan-bulan. Google Project Zero yang menemukan dan melaporkan kerentanan tersebut, mengatakan bahwa Arm telah mengatasi kerentanan tersebut pada Juli dan Agustus 2022, akan tetapi perbaikan yang dirilis dari produsen chip ini belum dilakukan sampai ke hilir atau ke perangkat Android yang terpengaruh (termasuk Pixel, Samsung, Xiaomi, Oppo, dan lainnya). Eksploitasi kerentanan yang berhasil dapat memungkinkan penyerang dapat merebut kendali sistem dan melewati perizinan pada Android untuk mendapatkan akses luas ke data pengguna. Temuan ini sekali lagi menunjukkan bagaimana celah keamanan dapat membuat jutaan perangkat berisiko terhadap eksploitasi oleh pelaku ancaman.

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/11/million-of-android-devices-still-dont.html >