www.idsirtii.or.id

10 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 102

OVERVIEW

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

General News

OJK Keluarkan Aturan Pengaduan Nasabah Korban Kejahatan Siber

Otoritas Jasa Keuangan (OJK) memastikan prinsip penanganan pengaduan nasabah korban kejahatan siber telah diatur dalam peraturan OJK No.6/2022 tentang perlindungan konsumen dan masyarakat sektor jasa keuangan. Direktur Eksekutif Penelitian dan Pengaturan Perbankan OJK Anung Herlianto mengatakan pelaku jasa keuangan, termasuk perbankan, harus menerapkan kebijakan dan prosedur tertulis mengenai perlindungan konsumen. Selain itu, jika kerugian yang diterima masyarakat disebabkan oleh sistem atau infrastruktur perbankan, maka bank harus mengganti. Menurutnya saat ini kejahatan siber menjadi salah satu tantangan di tengah era digitalisasi yang terus berkembang. OJK pun telah mengatur mengenai mekanisme pengaduan konsumen di POJK No.18/2018 tentang Layanan Pengaduan Konsumen Sektor Jasa Keuangan yang mengatur batas waktu penyelesaian sengketa yang harus dipenuhi oleh perbankan. OJK juga menyediakan layanan kepada masyarakat untuk menyalurkan pengaduan melalui aplikasi portal perlindungan konsumen (APPK) yang dapat digunakan masyarakat untuk menyampaikan keluhan dalam aplikasi tersebut.

Prioritas: ***2. Urgent***

< https://www.republika.co.id/berita/rd7idl349/ojk-keluarkan-aturan-pengaduan-nasabah-korban-kejahatan-siber >

Breachs/Hacks/Leaks

MyEasyDocs Mengekspos 30GB Data *Personal Identity Information* (PII) Siswa Israel dan India

MyEasyDocs adalah platform verifikasi dokumen online berbasis di Chennai, India yang server Microsoft Azure-nya mengekspos data lebih dari 57.000 siswa. Tim peneliti keamanan TI di vpnMentor yang dipimpin oleh Noam Rotem mengidentifikasi server Microsoft Azure yang salah konfigurasi telah mengungkap catatan pribadi dan pendidikan dari puluhan ribu siswa dari India dan Israel. Server yang terbuka milik Myeasydocs merupakan platform verifikasi data online yang berbasis di Chennai, India. Myeasydocs mengkhususkan diri dalam memverifikasi dokumen yang berkaitan dengan perbankan, perguruan tinggi, universitas, lembaga pemerintah dan lembaga penegak hukum. Setelah menganalisis kumpulan data, peneliti mengidentifikasi catatan berikut sebagai data-data yang diindikasikan telah terungkap yaitu nilai, nama lengkap, jurusan, nomor telepon, alamat email, tanggal kelulusan, ID nasional hingga nomor registrasi universitas/perguruan tinggi dan banyak lagi.

Prioritas: ***3. Important***

< https://www.hackread.com/myeasydocs-exposed-30gb-israel-india-students-pii-data/?web_view=true >

Vulnerabilities

Onapsis Research Labs Mengidentifikasi Tiga Kerentanan SAP yang Dapat Dieksploitasi

Onapsis Research Labs terus memantau lanskap ancaman yang berkembang untuk lebih memahami apa yang digunakan untuk menargetkan aplikasi bisnis seperti SAP dan Oracle. Analisis mendalam yang dilakukan memungkinkan Lab Penelitian Onapsis untuk lebih cepat mengidentifikasi ancaman, aktivitas, dan kerentanan baru serta perubahan perilaku yang meningkatkan risiko pada aplikasi bisnis penting. Baru-baru ini, penelitian yang dilakukan telah mendeteksi aktivitas eksploitasi terkait dengan tiga kerentanan yang telah diperbaiki oleh SAP CVE-2021-38163, CVE-2016-2386, dan CVE-2016-2388. Hal menarik yang dapat diamati pada ketiga kerentanan ini yaitu dua dari tiga CVE ini memiliki peringkat CVSS yang kritis, sebagian besar CVE ini memiliki PoC dan eksploitasi yang tersedia untuk umum, sebagian besar CVE ini dapat dieksploitasi dari jarak jauh dan melalui protokol HTTP.

Prioritas: ***1. Critical***

<https://onapsis.com/blog/three-actively-exploited-sap-vulnerabilities-identified-onapsis-research-labs?&web_view=true >

Symbiote: *Malware* Linux Siluman yang Menargetkan Sektor Keuangan Amerika Latin

Peneliti keamanan siber telah mengungkap yang disebut sebagai *malware* Linux yang "hampir mustahil untuk dideteksi" dan dapat dijadikan senjata untuk sistem yang terinfeksi dari *backdoor*. Dijuluki Symbiote oleh perusahaan intelijen ancaman BlackBerry dan Intezer, *malware* tersembunyi ini dinamai demikian karena kemampuannya untuk menyembunyikan dirinya dalam proses yang berjalan dan lalu lintas jaringan dan menguras sumber daya korban seperti parasit. Operator di belakang Symbiote diyakini telah memulai pengembangan *malware* pada November 2021, dengan pelaku ancaman yang sebagian besar menggunakannya untuk menargetkan sektor keuangan di Amerika Latin, termasuk bank seperti Banco do Brasil dan Caixa. Tujuan utama Symbiote adalah untuk menangkap kredensial dan untuk memfasilitasi akses pintu belakang ke mesin korban, kata peneliti Joakim Kennedy dan Ismael Valenzuela dalam sebuah laporan yang dibagikan kepada The Hacker News. Apa yang membuat Symbiote berbeda dari *malware* Linux lainnya adalah ia menginfeksi proses yang sedang berjalan daripada menggunakan *file* yang dapat dijalankan yang berdiri sendiri untuk menimbulkan kerusakan.

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/06/symbiote-stealthy-linux-malware.html?&web_view=true >

SVCReady: *Malware* Baru pada Lanskap Ancaman Keamanan

Para peneliti telah mengamati kampanye spam berbahaya baru yang disebarkan oleh keluarga *malware* bernama SVCReady. Serangan telah berlangsung sejak April dan menggunakan cara pengiriman *malware* yang tidak biasa melalui Microsoft Word. Menurut HP, pengembang di balik *malware* tersebut merilis beberapa pembaruan pada bulan Mei. Tampaknya masih dalam tahap awal, dan saat ini sedang mengalami perkembangan yang berat. *Malware* ini mendukung berbagai fungsi seperti mengunduh *file* ke klien yang terinfeksi, mengambil tangkapan layar, memeriksa apakah proses berjalan di VM, menjalankan perintah *shell*, dan mengumpulkan informasi sistem. Selain itu, *malware* mendukung fitur anti-analisis, eksfiltrasi informasi, dan komunikasi C2 terenkripsi. Dalam satu kasus, mesin yang terinfeksi mengirimkan RedLine Stealer sebagai *payload* lanjutan.

Prioritas: ***2. Urgent***

< https://cyware.com/news/svcready-a-new-malware-in-the-threat-landscape-c299d39d >

Kerentanan 'Follina' Dieksploitasi untuk Mengirimkan Qbot, AsyncRAT, *Malware* Lainnya

Beberapa keluarga *malware* dikirimkan menggunakan kerentanan Windows yang baru-baru ini diungkapkan yang diidentifikasi sebagai Follina dan CVE-2022-30190, yang masih belum ada *patch* resmi. Kerentanan, terkait dengan Microsoft Support Diagnostic Tool (MSDT), dapat dimanfaatkan untuk eksekusi kode jarak jauh menggunakan dokumen yang dibuat khusus. Sementara akar penyebab lubang keamanan tampaknya telah diketahui setidaknya selama beberapa tahun, Microsoft tampaknya sebagian besar mengabaikan masalah tersebut sampai sekarang. Keberadaan kerentanan itu terungkap setelah seorang peneliti melihat sebuah dokumen yang mengeksploitasinya. Ada indikasi bahwa serangan dimulai pada bulan April, dengan pengguna di India dan Rusia menjadi sasaran. Proofpoint melaporkan minggu ini bahwa kelompok kejahatan siber yang dilacak sebagai TA570 telah mengeksploitasi CVE-2022-30190 untuk mengirimkan Qbot, pencuri informasi yang banyak digunakan yang juga dikenal sebagai Qakbot dan Pinkslipbot. Malware dapat menyebar di jaringan yang disusupi dan telah dimanfaatkan untuk akses awal oleh beberapa kelompok kejahatan siber. Penyerang mengirimkan eksploitasi dengan melampirkan file HTML yang dibuat khusus ke percakapan email yang dibajak. SANS Institute telah menerbitkan analisis teknis dari serangan ini, bersama dengan *Indicator of Compromised* (IoCs).

Prioritas: *1. Critical*

< https://www.securityweek.com/follina-vulnerability-exploited-deliver-qbot-asyncrat-other-malware >