www.idsirtii.or.id

25 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 221

OVERVIEW

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

General News

Repositori Docker Hub Menyembunyikan Lebih dari 1.650 Kontainer Berbahaya

Lebih dari 1.600 Docker Hub *images* yang tersedia di publik menyembunyikan perilaku berbahaya, termasuk penambang *cryptocurrency*, kode tersembunyi yang dapat digunakan sebagai *backdoor*, pembajak DNS, dan pengalih situs web. Docker Hub adalah *cloud-based container library* yang memungkinkan orang untuk mencari dan mengunduh Docker *images* dengan bebas atau mengunggah kreasi mereka ke *public library* atau repositori pribadi. Docker *image* adalah *template* untuk pembuatan kontainer yang cepat dan mudah yang berisi kode dan aplikasi siap pakai. Oleh karena itu, mereka yang ingin menyiapkan instans baru sering beralih ke Docker Hub untuk menemukan aplikasi yang mudah diterapkan dengan cepat. Karena penyalahgunaan layanan oleh pelaku ancaman, lebih dari seribu unggahan berbahaya menghadirkan risiko besar bagi pengguna yang tidak diketahui yang menyebarkan image *malware* di wadah yang di-*hosting* secara lokal atau berbasis *cloud*.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/docker-hub-repositories-hide-over-1-650-malicious-containers/ >

Breachs/Hacks/Leaks

Lapor Kominfo, Lazada Klaim Tak Ada Kebocoran Data Penjual

Lazada mengklaim tidak menemukan kerentanan dalam sistem atau proses apapun dari sisi perusahaan yang menyebabkan akses tidak sah ke akun penjual. *Perusahaan e-commerce* itu menegaskan selalu mengutamakan perlindungan data konsumen. Sebelumnya, beredar informasi satu akun penjual di Lazada diakses secara tidak sah. Lazada pun mengaku telah berkoordinasi dengan penjual yang bersangkutan dalam rangka investigasi dan membantu penjual tersebut memblokir akunnya. Hasil investigasi lazada menyimpulkan bahwa insiden ini hanya terjadi terhadap satu akun penjual yang disebabkan oleh kelalaian penjual tersebut dalam menjaga kerahasiaan informasi login akunnya sendiri, sebagaimana dikonfirmasi oleh penjual. Lebih lanjut, Lazada juga telah melapor kepada Kemenkominfo terkait peristiwa ini. Lazada juga meminta para konsumen untuk menjaga kerahasiaan dan data mereka di *platform* tersebut.

Prioritas: ***1. Critical***

<https://www.cnnindonesia.com/teknologi/20221124171627-192-878283/lapor-kominfo-lazada-klaim-tak-ada-kebocoran-data-penjual >

Perusahaan Perangkat Lunak Medis Memaparkan Data Sensitif Anak-anak yang Rentan

Peneliti keamanan Jeremiah Fowler bekerja sama dengan tim peneliti Website Planet menemukan *database* yang tidak terlindungi yang berisi lebih dari 16.000 catatan. Lebih buruk lagi, *database* yang salah konfigurasi berisi *Personally Identifiable Information* (PII) yang sensitif dari ribuan anak. Fowler mencatat bahwa *database* yang salah konfigurasi berisi PII yang sangat sensitif, termasuk nama orang tua dan anak, tanggal lahir, nomor identitas pasien, alamat fisik, kebutuhan khusus, sekolah yang dihadiri, diagnosis medis, dan riwayat masalah sosial/perilaku. Peneliti meninjau sampel 1.000 catatan untuk menentukan siapa yang memiliki data dan memberi tahu mereka tentang *database* yang terbuka. Sesuai temuan mereka, setiap rekaman yang mereka ulas memiliki beberapa bentuk PII terkait anak.

Prioritas: ***3. Important***

< https://www.hackread.com/medical-software-expose-child-data/?web_view=true >

Threat Actor Mengeksploitasi Penghentian Server Web Boa untuk Menargetkan Infrastruktur Penting

Pakar Microsoft percaya bahwa *threat actor* di balik kampanye jahat yang ditujukan untuk infrastruktur kritis India awal tahun ini telah mengeksploitasi kelemahan keamanan di server web yang sekarang dihentikan bernama Boa. Server web Boa banyak digunakan di berbagai perangkat, termasuk perangkat IoT, dan sering digunakan untuk mengakses pengaturan dan konsol manajemen serta layar masuk. Para ahli menunjukkan bahwa Boa telah dihentikan produksinya sejak 2005. Para peneliti di Recorded Future mengamati beberapa upaya penyusupan pada infrastruktur kritis India sejak 2020 dan berbagi IOC terkait kampanye ini. Pakar Microsoft menganalisis IOC ini dan menemukan bahwa server Boa berjalan pada alamat IP pada daftar IOC, mereka juga menjelaskan bahwa serangan jaringan listrik menargetkan perangkat IoT terbuka yang menjalankan Boa.

Prioritas: ***3. Important***

< https://securityaffairs.co/wordpress/138916/hacking/boa-web-servers-attacks.html >

Vulnerabilities

'ViperSoftX Menjatuhkan Ekstensi Chrome VenomSoftX untuk Mencuri *Cryptocurrency*

Malware yang kurang dikenal bernama ViperSoftX, yang telah ada sejak tahun 2020 mengalami pengembangan ekstensif sepanjang tahun 2022 untuk meningkatkan kemampuan mencuri informasi dan penghindarannya. Di antara kemampuan *malware* ini, salah satunya melibatkan menjatuhkan ekstensi Google Chrome berbahaya pada sistem yang terinfeksi untuk mencuri mata uang kripto. Para peneliti mengungkapkan bahwa versi ViperSoftX yang lebih baru mampu memuat ekstensi *browser* berbahaya khusus ke *browser* berbasis Chromium yang diinstal pada sistem yang terinfeksi. Ekstensi tersebut pada dasarnya adalah pencuri informasi lain yang disebut VenomSoftX yang menyamar sebagai berbagai ekstensi *browser* populer, seperti Google Sheets, untuk menghindari deteksi pengguna. *Malware* ini berfokus pada lima pertukaran/situs web *cryptocurrency* seperti Blockchain.com, Binance, Coinbase, Gate.io, dan Kucoin.

Prioritas: ***2. Urgent***

< https://cyware.com/news/vipersoftx-drops-venomsoftx-chrome-extension-to-steal-cryptocurrency-63568614 >

Peretas Memodifikasi Aplikasi Android OpenVPN Populer Untuk Memasukkan *Spyware*

Pelaku ancaman yang terkait dengan operasi spionase dunia maya setidaknya sejak tahun 2017 telah memikat korban dengan perangkat lunak VPN palsu Android yang merupakan versi trojan dari perangkat lunak resmi SoftVPN dan OpenVPN. Para peneliti mengatakan bahwa kampanye tersebut "sangat bertarget" dan ditujukan untuk mencuri data kontak dan panggilan, lokasi perangkat, serta pesan dari berbagai aplikasi. Operasi tersebut dikaitkan dengan *threat actor* tingkat lanjut yang dilacak sebagai Bahamut, yang diyakini sebagai kelompok tentara bayaran yang menyediakan layanan *hack-for-hire*. Analis *malware* ESET Lukas Stefanko mengatakan bahwa Bahamut mengemas ulang aplikasi SoftVPN dan OpenVPN untuk Android untuk memasukkan kode berbahaya dengan fungsi mata-mata. Dengan melakukan ini, aktor memastikan bahwa aplikasi tersebut akan tetap menyediakan fungsionalitas VPN kepada korban sambil mengekstraksi informasi sensitif dari perangkat seluler.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/hackers-modify-popular-openvpn-android-app-to-include-spyware/ >