

3 Maret 2024

SECURITY ADVISORY

LockBit 4.0



LockBit 4.0 muncul sebagai iterasi baru dari ransomware LockBit. Ransomware ini ditemukan kasus pertamanya pada bulan Februari tahun 2024, versi ini ditemukann bersamaan dengan penangkapan dua operator LockBit oleh lembaga penegak hukum. Hanya lima hari setelah kebocoran, pelaku ancaman mengeluarkan pernyataan yang menguraikan rencana restrukturisasi mereka dan komitmen untuk bertahan dengan nama yang sama.

Tingkat
IK
Imbauan
Keamanan

Tipe Ransomware
Malware

Ransomware adalah program jahat yang menyusup ke perangkat Anda. Ransomware mengenkripsi data Anda sehingga tidak bisa diakses. Para pelaku kemudian meminta tebusan untuk mengembalikan akses ke data Anda.

Langkah Mitigasi

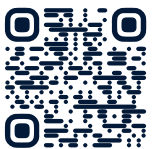
Gunakan password kuat dan lapiasi login dengan MFA sehingga hacker tidak mudah masuk. Update rutin semua perangkat lunak dan atur konfigurasi sistem yang benar. Backup data teratur, minimal satu copy simpan offline dan terpisah. Batasi akses data penting dengan mengatur izin pengguna. Jaga keamanan jaringan Anda dengan segmentasi dan pakai keamanan endpoint. Terakhir, selalu waspada dengan email mencurigakan.

Produk Terancam

- Semua versi Windows, serta beberapa versi Mac dan Linux

Referensi Lanjutan, Solusi, dan Alat

- <https://www.pcrisk.com/removal-guides/29237-lockbit-4-0-ransomware>
- <https://thecyberexpress.com/law-enforcement-lockbit-4-0-battle-heats-up/>



Informasi
Imbauan Keamanan
Lainnya di laman
Id-SIRTII/CC

<https://www.idsirtii.or.id/peringatan.html>

Sumber Penulisan

- [Diakses 13 Maret 2023] <https://nvd.nist.gov/vuln/detail/CVE-2021-4391>
- [Diakses 13 Maret 2023] <https://blog.aquasec.com/github-dataset-research-reveals-millions-potentially-vulnerable-to-repojacking>

TLP Level Clear ○○○

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

Diterbitkan Oleh

Id-SIRTII/CC

Indonesia Security Incident
Response team on Internet
Infrastructure Coordination Center

Badan Siber dan Sandi Negara

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan,
Pasar Minggu, Jakarta Selatan 12550

