22 Agustus 2023

SECURITY ADVISORY
NoEscape Ransomware

NoEscape Ransomware merupakan virus yang memberikan layanan (*Ransomware-as-a-service*) kepada penyerang lain yang bertindak sebagai afiliasi. Tujuan utama virus ini adalah untuk melakukan enkripsi *file*. Virus ini mirip dengan Ransomware Avaddon yaitu dengan menambahkan *string* karakter acak (".CAEGAAHJFA"). NoEscape menjalankan serangkaian perintah untuk menghilangkan salinan cadangan sistem. Korban tidak dapat membuka file yang disimpan pada komputer. File yang sebelumnya berfungsi kini memiliki ekstensi yang berbeda (misalnya, my.docx.locked). Pesan permintaan tebusan akan ditampilkan pada desktop korban. Penyerang meminta pembayaran uang tebusan (biasanya dalam bitcoin) untuk membuka kunci dari file yang sudah terkunci.

Nilai/Tingkat

N.a

Nilai belum Tersedia

Tipe	**Ransomware**
Serangan	Enumerasi Kerentanan tidak lengkap atau belum tersedia

Langkah Mitigasi

- Mengunduh perangkat lunak dari situs resmi dan menggunakan downloader dari browser secara langsung tanpa menggunakan software bajakan.
- Berhati-hati saat membuka dan menemukan lampiran email atau tautan situs web dari alamat email yang tidak dikenal atau tidak relevan
- Hindari mengunjungi tautan dan iklan di situs web yang meragukan.

Produk Terancam

- Linux
- Windows
- MacOS

Referensi Lanjutan, Solusi, dan Alat

- https://www.pcrisk.com/removal-guides/26937-noescape-ransomware
- https://www.bleepingcomputer.com/

Informasi Imbauan Keamanan Lainnya di laman **Id-SIRTII/CC**

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

Sumber Penulisan

- [Diakses 22 Agustus 2023] https://www.pcrisk.com/removal-guides/26937-noescape-ransomware
- [Diakses 22 Agustus 2023] https://www.bleepingcomputer.com/

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