06 Oktober 2023

SECURITY ADVISORY

Malware Win32/Blacksuit.B

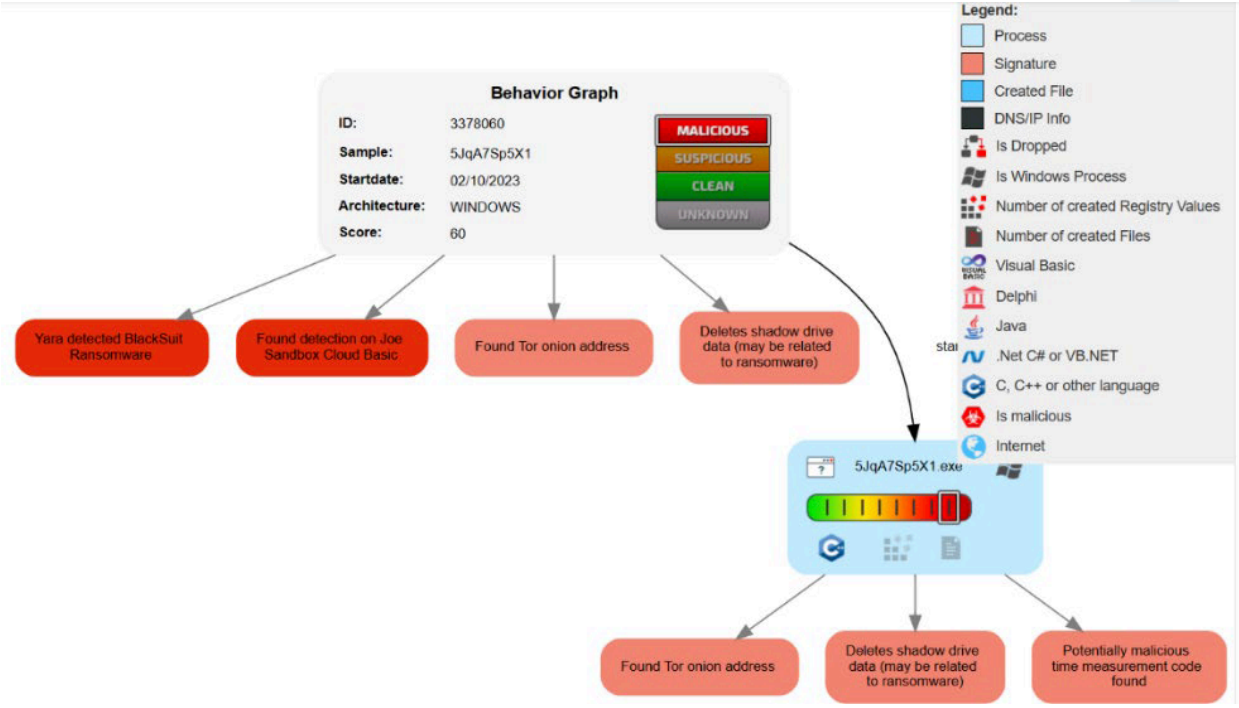
Tingkat

IK

Imbauan Keamanan

Win32/BlackSuit.B adalah jenis ransomware yang mengenkripsi file pada sistem korban dan menuntut pembayaran untuk mendapatkan kunci dekripsi 2 . Ransomware ini masuk ke dalam sistem sebagai file yang dijatuhkan oleh malware lain atau sebagai file yang diunduh tanpa disadari oleh pengguna saat mengunjungi situs web yang berbahaya

Direktorat Operasi Keamanan Siber Siber melalui Tim Analisis Malware melakukan analisis terhadap file malicious bernama “sys32.exe”. Pada analisis menggunakan sandbox didapatkan behavior graph sebagai berikut.



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

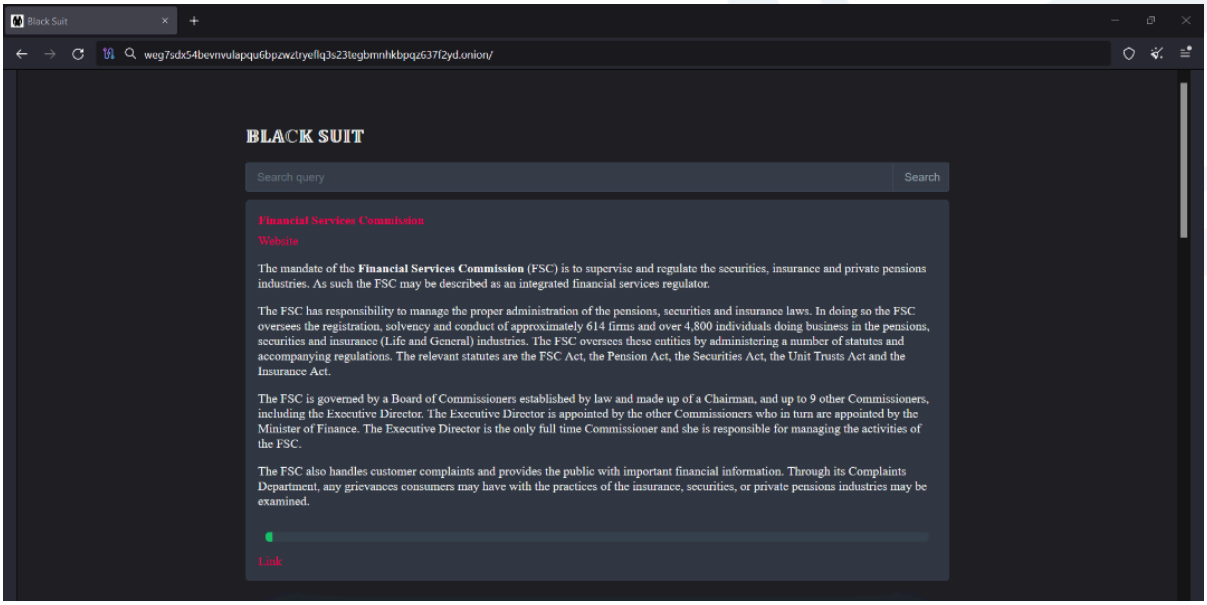
(021) 788 33610

bantuan70@bssn.go.id

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

SECURITY ADVISORY
Malware Win32/Blacksuit.B

Berdasarkan Behavior Graph ditemukan adanya TOR Onion yang diindikasikan sebagai halaman utama dari Ransomware Blacksuit. Berikut merupakan tampilan dari homepage tersebut:



Berdasarkan hasil analisis, diketahui beberapa hal sebagai berikut:

1. Ransomware melakukan enkripsi dan mengubah ekstensi file.
2. Encryptor tidak dapat dijalankan tanpa adanya argumen yang dimasukan pada file .bat.
3. Diduga penyerang telah memiliki akses kedalam sistem korban dan melakukan exfiltrasi data kemudian menjalankan ransomware ini dengan menginputkan ID sebagaimana telah dibuat pada link Blacksuit.
4. Ransomware ini bersifat targeted dan tidak bersifat masif.

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

SECURITY ADVISORY
Malware Win32/Blacksuit.B

Tipe Serangan **Ransomeware**

Ransomeware adalah perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data hingga tebusan dibayar. Ransomware biasanya bekerja dengan mengenkripsi data pengguna sehingga tidak dapat diakses, dan kemudian menuntut pembayaran tebusan untuk mengembalikan kunci enkripsi.

Langkah Mitigasi

- Backup data secara teratur. Dengan melakukan backup data secara teratur, maka dapat dipastikan bahwa data alan aman dan dapat dipulihkan jika terkena ransomware Win32/BlackSuit.B.
- Gunakan software antivirus dan firewall yang terbaru. Pastikan bahwa software antivirus dan firewall Anda selalu diperbarui ke versi terbaru dan diaktifkan secara terus-menerus untuk melindungi sistem Anda dari serangan malware.
- Jangan membuka email atau lampiran yang mencurigakan. Hindari membuka email atau lampiran yang tidak Anda kenal atau yang mencurigakan, terutama jika email tersebut berisi tautan atau lampiran yang tidak Anda harapkan.
- Jangan mengunduh software dari sumber yang tidak terpercaya. Hindari mengunduh software dari sumber yang tidak terpercaya atau situs web yang mencurigakan.
- Jangan membayar tebusan. Jangan pernah membayar tebusan yang diminta oleh penjahat siber setelah sistem Anda terkena serangan ransomware. Tidak ada jaminan bahwa Anda akan mendapatkan kunci dekripsi setelah membayar tebusan tersebut.

Referensi Lanjutan, Solusi, dan Alat

- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom%3AWin32%2FPrestige.B&threatId=-2147133973
- https://www.trendmicro.com/en_ph/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html

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

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

Sumber Penulisan

- [Diakses 6 Oktober 2023] Laporan Analisis Malware Win32/Blacksuit.B oleh Tim Analisis Malware Direktorat Operasi Keamanan Siber

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