BIMANTARA Labs

SECURITY REPORT

Awal tahun 2022 ditemukan kembali sampel malware berbahaya. Dimana sampel tersebut terindikasi sebagai malware Destructive. Malware tersebut bernama WhisperGate.

Abdi Bimantara

abdibimantara91@gmail.com

abdibimantara

abdibimantara

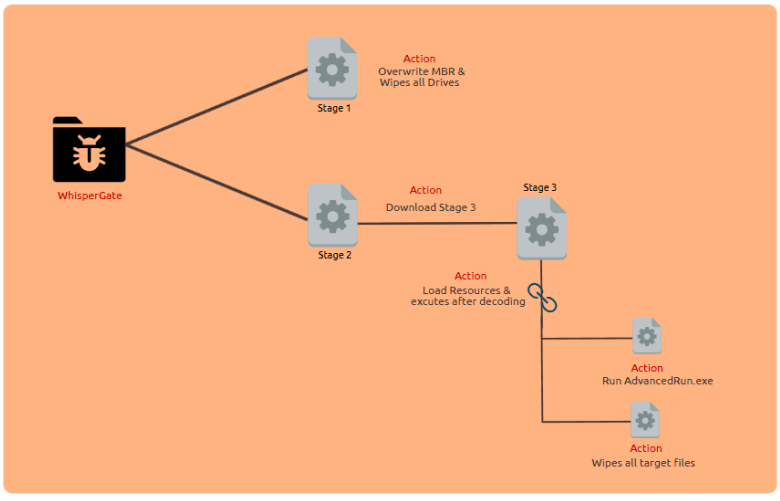
Daftar Isi

Latar Belakang

Laporan merah kembali tercatat pada awal tahun 2022. Hal ini terbukti dengan terdeteksinya beberapa jenis malware baru. Menurut laporan yang ditulis oleh cisa pada tanggal 26 februari 2022 kemarin, terdapat jenis malware baru yang termasuk dalam kategori malware destructive. Dimana terdeteksinya malware tersebut bertepatan dengan isu agresi militer Rusia terhadap Ukraina. Malware ini pun teridentikasi ditujukan khusus untuk organisasi ataupun instansi pemerintahan ukraina.

WhisperGate, begitu beberapa forum memberikan nama untuk jenis malware baru ini. Umumnya berbagaia jenis antivirus mendeteksi malware WhsiperGate sebagai salah satu jenis keluarga dari ransomware. Namun pada kenyataanya malware WhisperGate ini cukup berbeda jika dibandingkan dengan Ransomware. Malware WhisperGate akan menghancurkan atau menghapus total file yang berada pada device target, dan tidak akan mengembalikan data walaupun korban telah membayar tebusan.

Karakteristik WhisperGate memiliki kesaaman terhadap malware NotPetya. Dimana malware NotPetya telah lebih dulu muncul. Hal ini membuktikan bahwa, Teknik penyamaran sebagai ransomware bukan pertama kalinya. Dalam kasus penyebaran yang dilakukan oleh WhisperGate ini, korban akan menerima beberapa payload yang mencoba melakukan proses penghapusan MBR serta menuliskan catatan seperti ransomware umumnya. Di waktu yang bersaaman, WhisperGate akan mencoba melakukan perusakan partisi C:\ dengan cara menuliskan beberapa data pada MBR.



Gambar 1. Diagram penyebaran malware whispergate

Secara umum, terdapat 3 tahap penyebaran serangan WhisperGate. Pada gambar 1 terlihat bahwa stage 1 akan melakukan aksi penulisan payload secara terus menerus pada MBR device target dan disaat yang bersamaan juga menjalankan perintah penghancuran semua partisi pada device target. Pada stage2, proses penyebaran tergolong cukup singkat. Dimana pada stage2 ini akan menjalankan proses download file stage3. Pada akhir tahap penyebaran yang dilakukan oleh stage3, akan melakukan beberapa proses. Proses pertama yaitu menjalankan perintan advancerun yang dimana akan menghasilkan menonaktifkan layanan windows defender serta mengijinkan device untuk menginstall file apa saja. Proses kedua yaitu akan menjalankan proses penghapusan massal semua data pada device target termasuk juga malware tersebut.

Sample

Sampel malware WhisperGate yang digunakan dapat di download pada website https://bazaar.abuse.ch/ . Jenis malware yang dianalisa yaitu stage1.exe. berikut adalah beberapa penjelasan mengenai program stage1.exe yang kami download.

Sample	: Whisper Gate (Stage1.exe)
Source	: https://bazaar.abuse.ch/
SHA256 Hash	: a196c6b8ffcb97ffb276d04f354696e2391311db3841 ae16c8c9f56f36a38e92
File Size	: 27'648 bytes
File Ektensi	: Exe
Target	: Sistem Operasi Windows
Tanggal Terdeteksi	: 15 Januari 2022

Lab Environment & Tools

- Kami menggunakan environment linux dengan distribusi linux ubuntu. Sedangkan distro linux yang dipilih adalah remnux yang dapat didownload pada website: https://remnux.org/ . Selain itu kami juga menggukanan environment windows dengan bantuan dari FlareVM https://github.com/mandiant/flare-vm

- Tools yang kami gunakan yaitu
  - Malwareoverview
  - Detect it Easy
  - Triage
  - Strings
  - IdaPro
  - Peid
  - Wireshark

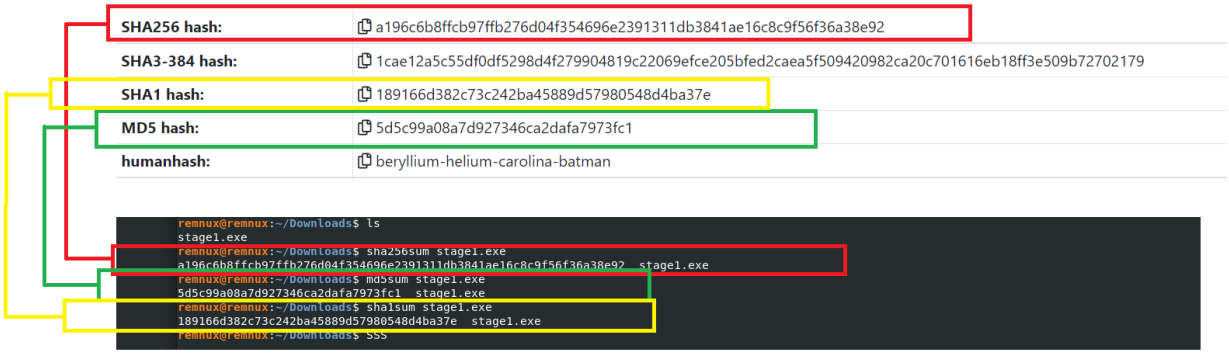
Technical Analysis

Secara umum proses analisis malware terbagi menjadi 3, static, dynamic serta hybrid. Proses analisis static adalah proses analisis yang dilakukan tanpa menjalankan program dan hanya menganalisa melalui source codenya. Untuk analisis dynamic adalah proses analisa yang dilakukan dengan cara menjalankan langsung program dan mencatat hasil dari apa yang terjadi. Sedangkan pada proses analisis hybrid adalah gabungan dari kedua proses analisis sebelumnya. Proses analisis hybrid sangat diperlukan guna memperkuat hasil dari beberapa analisa.

➢ Static Analysis

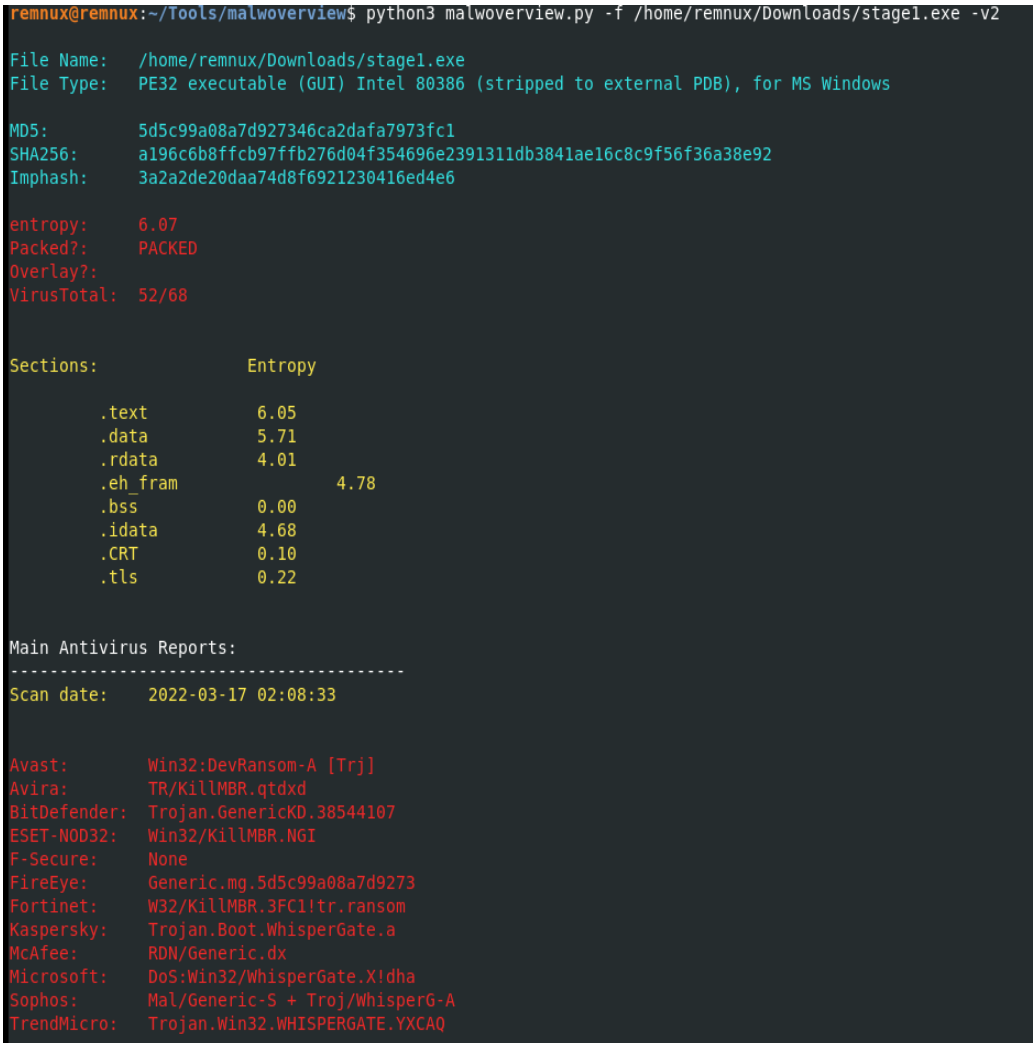
Sampel yang berhasil kita dapatkan dari website https://bazaar.abuse.ch/ terlebih dahulu kita ekstrasi (Masih berbentuk .zip). Diketahui sampel tersebut memiliki format .exe, sehingga ada baiknya lingkungan yang digunakan dalam menganalisa adalah non windows. Kali ini kami menggunakan system operasi linux.

Sampel malware yang kami download memiliki nama **stage1.exe.** Untuk memvalidasi apakah sampel ini benar benar sama dengan sampel terduga "**Malware whispergate**" maka kami melakukan pengencekkan hash.



Gambar 2. Hasil pengecekkan hash stage1.exe

Berdasarkan informasi gambar 2, sampel yang telah kita download sudah tervalidasi sama dengan sampel yang terindikasi sebagai malware whistpergate. Setelah melakukan validasi menggunakan bantuan hash, proses Analisa akan dilanjutkan menggunakan bantuan tools maloeverview.



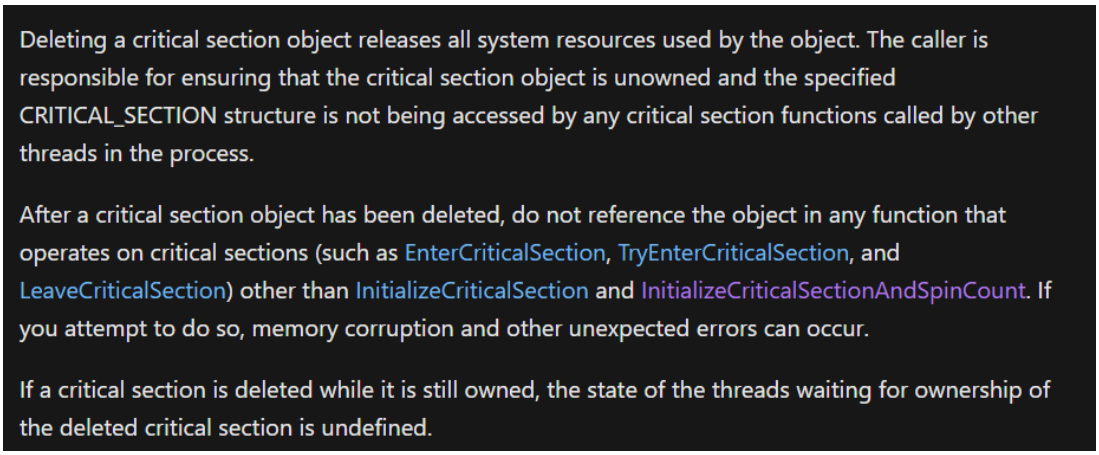
Gambar 3. Hasil pengcekkan stage1.exe.

Nilai entropi umumnya dimulai dari 0 sampai maksimum 8. Dan berdasarkan gambar 3, diketahui nilai entropi dari sampel tersebut yaitu 6.07. Informasi jelas juga didapatkan dari sampel tersebut, yaitu penulis atau pembuat stage1.exe melakukan packed atau obfuscated yang bertujuan untuk menyulitkan proses analisis dan deteksi antivirus. Hasil pengecekkan dari virus total juga

menunjukkan 52/68, yang berati file tersebut memang memilki ancaman yang sangat serius. Dari beberapa antivirus terkemuka, berhasi mendeteksi file tersebut dalam kategori malware **TROJAN**.

Gambar 4. Hasil pengcekkan function.

Melihat informasi yang ada pada gambar 4, program stage 1.exe terindikasi menjalankan function yang cukup critical yaitu **DeleteCriticalSection**. Function tersebut bila dijalankan akan melakukan proses penghapusan sumber daya system yang digunakan oleh suatu objek. Function **DeleteCriticalSection** memiliki hubungan erat terhadap function lainnya seperti, EnterCriticalSection, InitializeCriticalSection dan LeaveCriticalSection yang ditunjukkan pada gambar 5.



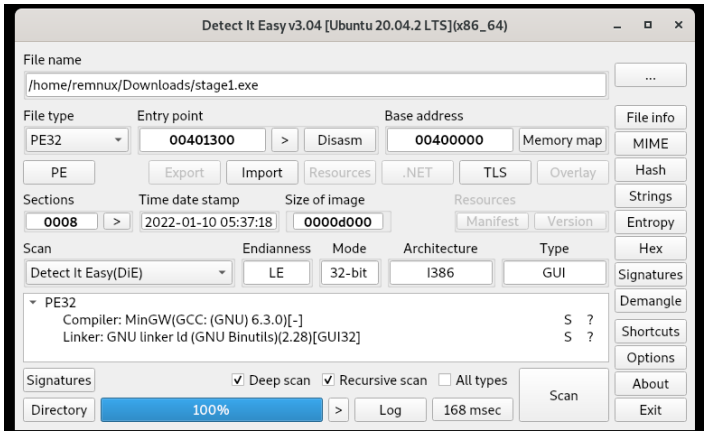
Gambar 5. Penjelasan mengenai DeleteCritical Function.

Informasi lebih detail kembali kami dapatkan, Program Stage1.exe diketahui mengimport beberapa library. Beberapa library yang di import pada program tersebut adalah KERNEL32.dll serta msvcrt.dll. Menurut beberapa sumber, kedua library tersebut umumnya terindikasi pada kegiatan malicious (malware). Library KERNEL32.dll bertugas untuk membantu proses manajemen

memori, operasi input dan ataupun output, interupsi serta proses sinkronisasi. Sedangakan untuk library msvcrt.dll memiliki persaaman fungsi seperti library standar pada bahas pemrogaman C yaitu printf. Tujuan dari program melakukan proses import library adalah agar proragm tersebut memiliki ukuran yang relative lebih kecil dan kinerja yang lebih efisien.

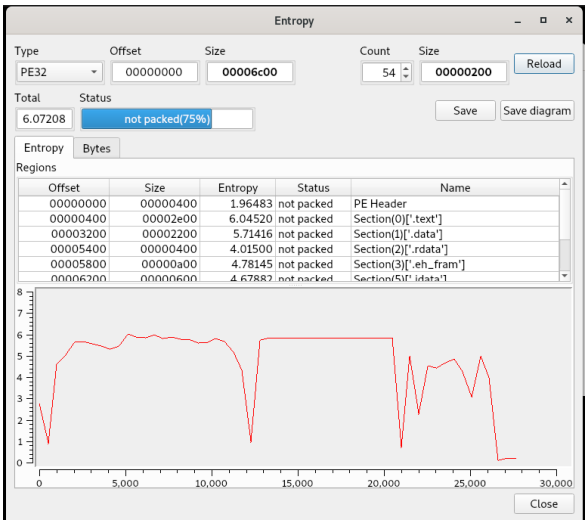
Gambar 6. Import Library stage1.exe

Menggunakan tools Detect it Easy (DiE) kami berharap menemukan informasi yang berguna. Tools DiE dapat didownload pada https://github.com/horsicq/Detect-It-Easy . Tools tersebut berguna untuk mendeteksi jenis apakah packed yang digunakan attacker dalam melindungi malware dari analysis orang lain.



Gambar 7. Hasil Deteksi DIE

Menggunakan tools Detect It Easy pada gambar 7, kami mendapatkan informasi yang berguna. Program stage1.exe tersebut terdeteksi menggunakan compiler MinGW, dan program tersebut tidak terdetesi menggunakan jenis packer apapun. Kami kembali masuk lebih jauh menggunakan menu entropy. Dimenu entropy tersebut, kami menemukan bahwa nilai entropi untuk program stage1.exe ini sama dengan nilai dari pengecekkan pertama. Dan ternyata benar bahwa, program stage1.exe ini memiliki nilai 75% non packed.

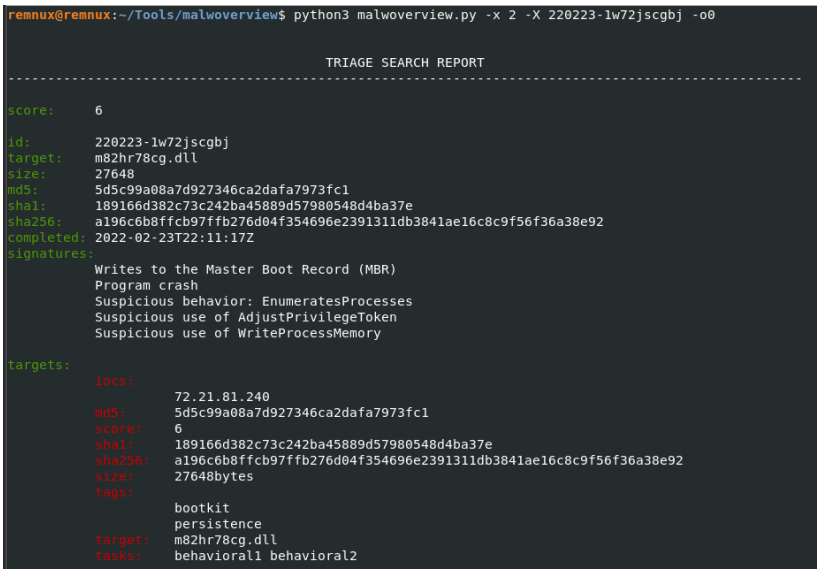


Gambar 8. Pengcekkan nilai entropi dan status program

Kembali menggunakan tools Malwoverview, kami mencoba mencari informasi mengenai report dari sample program stage1.exe. Berdasarkan gambar 9 mendapatkan lebih dari lima report mengenai program stage1.exe ini.

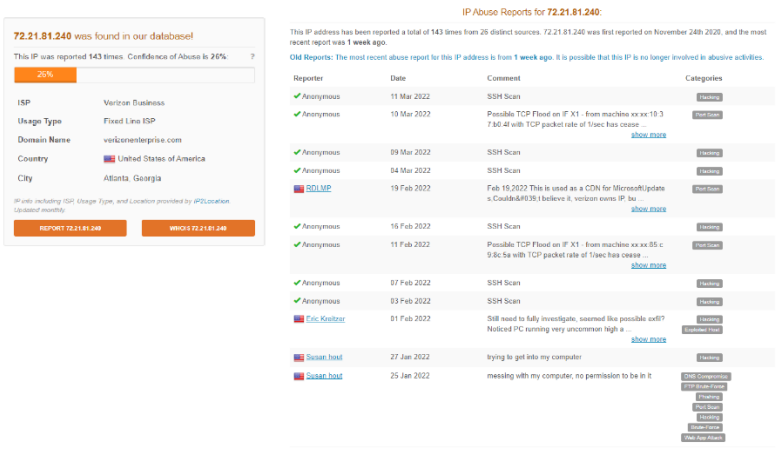
```
remnux@remnux:~/Tools/malwoverview$ python3 malwoverview.py -x 1 -X a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 -o0

                                    TRIAGE OVERVIEW REPORT
-----------------------------------------------------------------------------------------------

id:         220315-mrp4aacbak
status:     reported
kind:       file
filename:   a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92.exe
submitted:  2022-03-15T10:42:08Z
completed:  2022-03-15T10:44:19Z
-----------------------------------------------------------------------------------------------
id:         220225-t19bvagff4
status:     reported
kind:       file
filename:   a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
submitted:  2022-02-25T16:32:36Z
completed:  2022-02-25T16:35:11Z
-----------------------------------------------------------------------------------------------
id:         220224-z46b9aehfr
status:     reported
kind:       file
filename:   5d5c99a08a7d927346ca2dafa7973fc1.whisper.exe
submitted:  2022-02-24T21:17:18Z
completed:  2022-02-24T21:22:27Z
-----------------------------------------------------------------------------------------------
id:         220224-slhd5seean
status:     reported
kind:       file
filename:   a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
submitted:  2022-02-24T15:12:39Z
completed:  2022-02-24T15:13:20Z
-----------------------------------------------------------------------------------------------
id:         220223-1w72jscgbj
status:     reported
kind:       file
filename:   m82hr78cg.dll
submitted:  2022-02-23T22:01:05Z
completed:  2022-02-23T22:11:17Z
-----------------------------------------------------------------------------------------------
```

Gambar 9. Pengecekkan report stage1.exe



Gambar 10. Pengecekkan report stage1.exe part 2

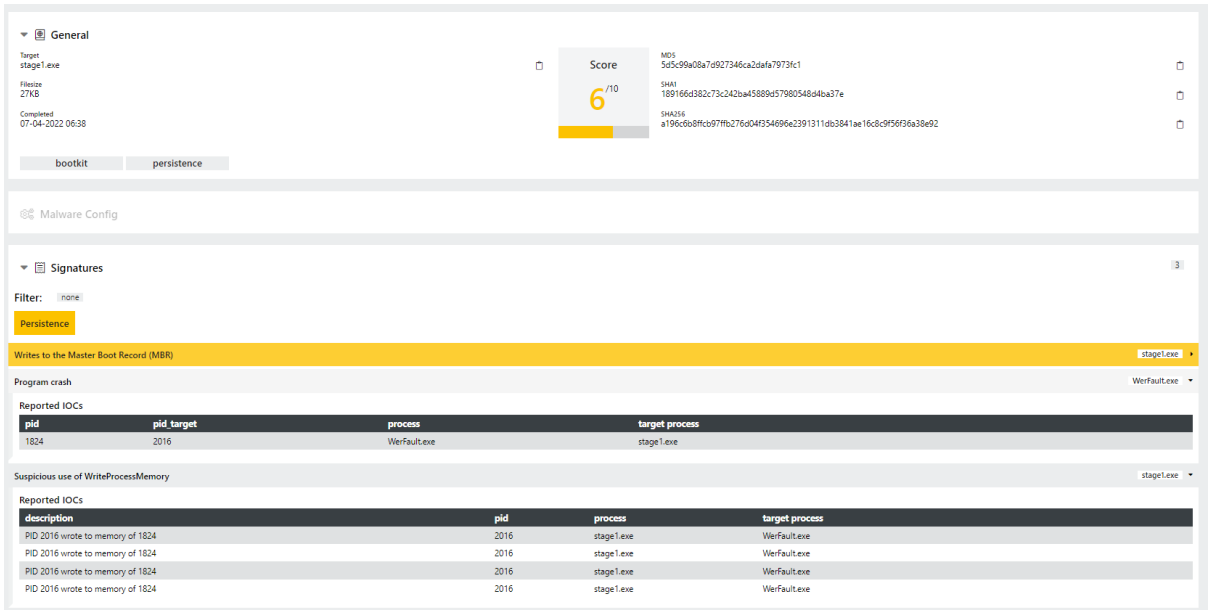
Pada gambar 10, kita mendapatkan informasi mengenai signature dari program stage1.exe. Program stage1.exe tersebut akan menulis MBR sampai penuh dan mengakibatkan kerusahakan data pada device korban. Selain itu juga diketahui pada gambar 10, terdapat ip yang diduga Indicator of Compromise (IoCs) yaitu **72.21.81.240.** saat dilakukan pengecekkan Ip reputation mengunakan tools ipabused, menghasilkan reputasi yang tidak baik . Informasi yang tak kalah menarik juga kami dapatkan mengenai program stage1.exe ini terkait dengan **Bootkit** suatu program malicious yang menargetkan Master Boot Record, dimana program tersebut biasanya sangat sulit terdeteksi oleh antiviurs) dan **Persistance** (Program malicious akan mencoba mempertahankan akses pada device korban)**.**



Gambar 10. Pengecekkan IoC IP

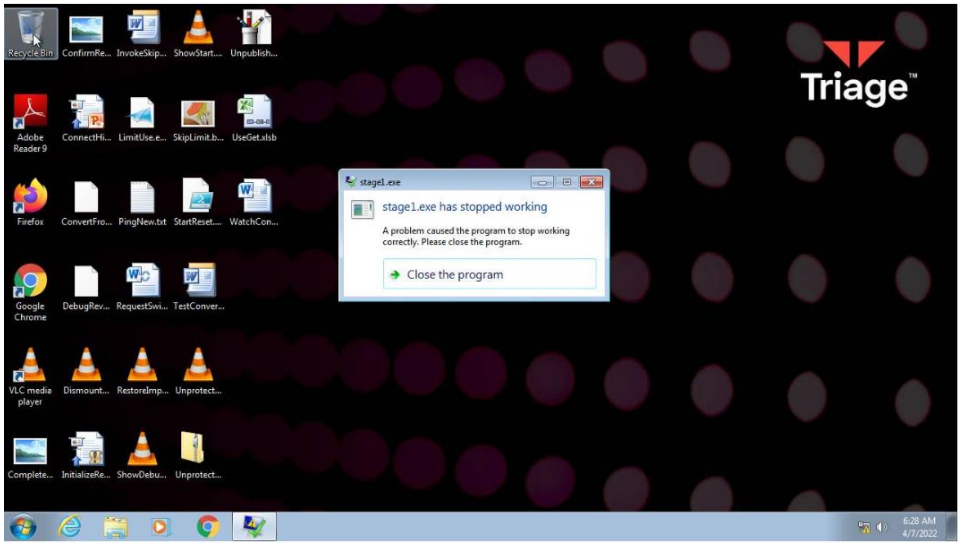
➢ Dynamic Analysis

Proses analysis program stage1.exe dilanjutkan ke tahap dynamic analysis. Pada tahap ini, kami menggunakan bantuan dari tools https://tria.ge/. Tools tersebut bertindak sebagai sandbox, sehingga memungkinkan kita untuk mengetahui behavior dari program tersebut.



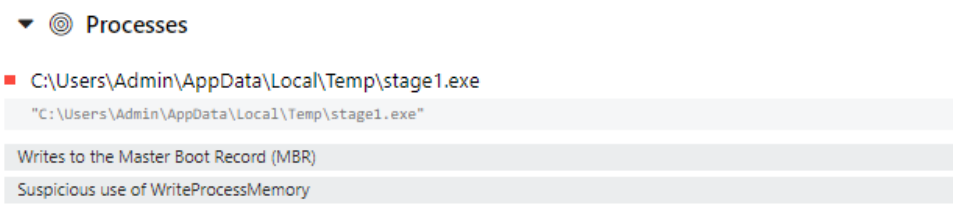
Gambar 11. Hasil pengecekkan triage part 1

Berdasarkan gambar 11, diketahui bahwa program stage1.exe mendapatkan nilai 6/10. Hal ini menandakan bahwa program tersebut termasuk dalam kategori cukup berbahaya. Hal ini juga dibuktikan dengan pogram stage1.exe termasuk dalam killchain persistence sebagai bootkit. Berdasarkan informasi yang kami dapakan dari mittre ATT&CK, bootkit terletak pada lapisan dibawah system operasi dan sangat sulit untuk dideteksi.



Gambar 12. Hasil pengecekkan triage part 2

Melalui tools triage, kita dapat mengetahui bukti dari adanya potensi (IoC) anomali yang ditimbulkan saat menjalankan program stage1.exe. IoC ini juga menunjukkan bahwa program stage1.exe. termasuk dalam kategori malicious. Dimana Ioc yang terdeteksi adalah **\??\PhysicalDrive0,** yang mana maksudnya program stage1.exe ini akan membuaka **\??\PhysicalDrive0** dan akan memodifikasinya. Akibat dari aktivitas yang dijalan oleh stage1.exe ini menyebabkan WerFault.exe memunculkan pesan eror kepada si user.



Gambar 13. Hasil pengecekkan triage part 3

Berdasarkan gambar 13, diketahui program stage1.exe terdapat pada path C:\Users\Admin\AppData\Local\Temp\stage1.exe. dan hal ini membuktikan bahwa program tersebut memang benar telah menjalanlkan suatu proses anomali. Dimana proses anomali tersebut adalah melakukan proses penulisan pada master boot record (MBR).

Kesimpulan

Berdasarkan hasil analisa yang kami lakukan. Program stage1.exe adalah benar termasuk dalam kategori malicious software (malware). menggunakan proses analisa *static* dan *dynamic*, kami menyimpulkan bahwa stage1.exe termasuk kedalam malware trojan. namun jenis ini sedikit berbeda terhadap jenis trojan ransomware.