

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](#)

M [abdibimantara](#)

Daftar Isi

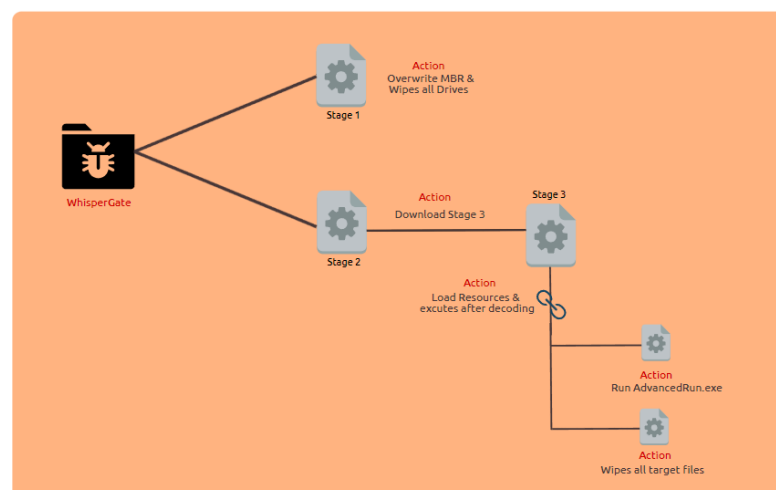
Daftar Isi	2
Latar Belakang	3
Sampel	4
Lab Environment & Tools	5
Technical Analysis	6
Static Analysis	6
Dynamic Analysis	12
Kesimpulan	14

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 teridentifikasi ditujukan khusus untuk organisasi ataupun instansi pemerintahan ukraina.

WhisperGate, begitu beberapa forum memberikan nama untuk jenis malware baru ini. Umumnya berbagai jenis antivirus mendeteksi malware WhisperGate sebagai salah satu jenis keluarga dari ransomware. Namun pada kenyataannya 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 kesaamaan 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 bersamaan, WhisperGate akan mencoba melakukan kerusakan 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 perintah 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 menggunakan 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 pengecekan hash.

SHA256 hash:	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
SHA3-384 hash:	1cae12a5c55df0df5298d4f279904819c22069efce205bfd2caea5f509420982ca20c701616eb18ff3e509b72702179
SHA1 hash:	189166d382c73c242ba45889d57980548d4ba37e
MD5 hash:	5d5c99a08a7d927346ca2dafa7973fc1
humanhash:	beryllium-helium-carolina-batman


```
remnux@remnux:~/Downloads$ ls
stage1.exe
remnux@remnux:~/Downloads$ sha256sum stage1.exe
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 stage1.exe
remnux@remnux:~/Downloads$ md5sum stage1.exe
5d5c99a08a7d927346ca2dafa7973fc1 stage1.exe
remnux@remnux:~/Downloads$ sha1sum stage1.exe
189166d382c73c242ba45889d57980548d4ba37e stage1.exe
remnux@remnux:~/Downloads$
```

Gambar 2. Hasil pengecekan 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.

```
remnux@remnux:~/Tools/malwoverview$ python3 malwoverview.py -f /home/remnux/Downloads/stage1.exe -v2
File Name: /home/remnux/Downloads/stage1.exe
File Type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows

MD5: 5d5c99a08a7d927346ca2dafa7973fc1
SHA256: a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
Imphash: 3a2a2de20daa74d8f6921230416ed4e6

entropy: 6.07
Packed?: PACKED
Overlay?:
VirusTotal: 52/68

Sections: Entropy
.text 6.05
.data 5.71
.rdata 4.01
.eh_frame 4.78
.bss 0.00
.idata 4.68
.CRT 0.10
.tls 0.22

Main Antivirus Reports:
-----
Scan date: 2022-03-17 02:08:33

Avast: Win32:DevRansom-A [Trj]
Avira: TR/KillMBR.qtdxd
BitDefender: Trojan.GenericKD.38544107
ESET-NOD32: Win32/KillMBR.NGI
F-Secure: None
FireEye: Generic.mg.5d5c99a08a7d9273
Fortinet: W32/KillMBR.3FC1ltr.ransom
Kaspersky: Trojan.Boot.WhisperGate.a
McAfee: RDN/Generic.dx
Microsoft: DoS:Win32/WhisperGate.Xldha
Sophos: Mal/Generic-S + Troj/WhisperG-A
TrendMicro: Trojan.Win32.WHISPERGATE.YXCAQ
```

Gambar 3. Hasil pengecekan 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 pengecekan dari virus total juga

menunjukkan 52/68, yang berarti file tersebut memang memiliki ancaman yang sangat serius. Dari beberapa antivirus terkemuka, berhasil mendeteksi file tersebut dalam kategori malware **TROJAN**.

```
Imported Functions
-----
CloseHandle
EnterCriticalSection
FindFirstFileA
GetCommandLineA
GetProcAddress
LoadLibraryA
VirtualProtect
_strdup
__mb_cur_max
__set_app_type
fpreset
_isctype
_setmode
calloc
malloc
realloc
strcoll
vfprintf
CreateFileW
ExitProcess
FindNextFileA
GetLastError
InitializeCriticalSection
SetUnhandledExceptionFilter
VirtualQuery
_stricoll
__p__environ
_cexit
_fullpath
_onexit
abort
free
mbstowcs
setlocale
strlen
wcstombs
DeleteCriticalSection
FindClose
FreeLibrary
GetModuleHandleA
LeaveCriticalSection
TlsGetValue
WriteFile
__getmainargs
__p__fmode
_errno
_iob
_pctype
atexit
fwrite
memcpy
signal
tolower
```

Gambar 4. Hasil pengecekan 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.

Deleting a critical section object releases all system resources used by the object. The caller is responsible for ensuring that the critical section object is unowned and the specified CRITICAL_SECTION structure is not being accessed by any critical section functions called by other threads in the process.

After a critical section object has been deleted, do not reference the object in any function that operates on critical sections (such as EnterCriticalSection, TryEnterCriticalSection, and LeaveCriticalSection) other than InitializeCriticalSection and InitializeCriticalSectionAndSpinCount. If you attempt to do so, memory corruption and other unexpected errors can occur.

If a critical section is deleted while it is still owned, the state of the threads waiting for ownership of the deleted critical section is undefined.

Gambar 5. Penjelasan mengenai DeleteCritical Function.

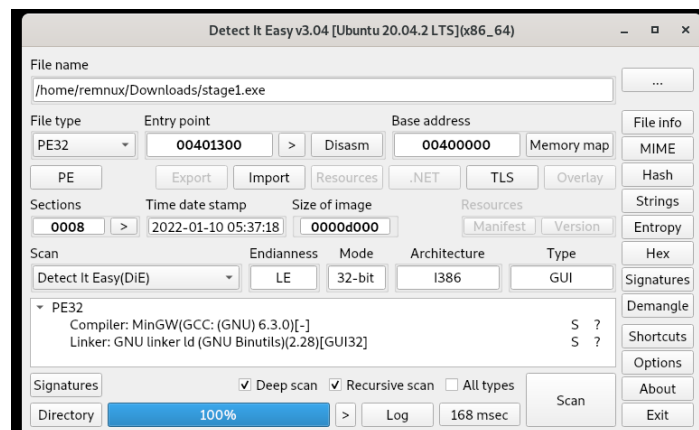
Informasi lebih detail kembali kami dapatkan, Program Stage1.exe diketahui mengimport beberapa library. Beberapa library yang di import pada program tersebut adalah KERNEL32.dll serta msvcrt.dll. Menurut beberapa sumber, kedua library tersebut umumnya terindikasi pada kegiatan malicious (malware). Library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

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



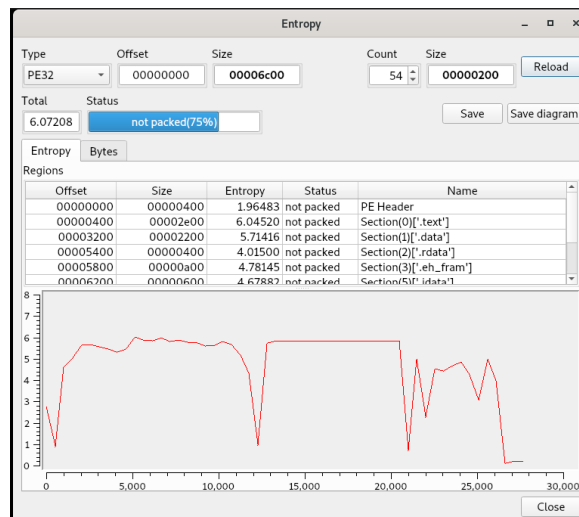
Gambar 6. Import Library stage1.exe

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 analisis 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 terdeteksi 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 pengecekan pertama. Dan ternyata benar bahwa, program stage1.exe ini memiliki nilai 75% non packed.



Gambar 8. Pengeckkan 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: 5d5c99a08a7d927346ca2dafa7973fcl.whisper.exe
submitted: 2022-02-24T21:17:18Z
completed: 2022-02-24T21:22:27Z
-----
id: 220224-slhd5sean
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. Pengeckkan report stage1.exe

```
remnux@remnux:~/Tools/malwoverview$ python3 malwoverview.py -x 2 -X 220223-1w72jscbj -o0

-----
TRIAGE SEARCH REPORT
-----

score: 6

id: 220223-1w72jscbj
target: m82hr78cg.dll
size: 27648
md5: 5d5c99a08a7d927346ca2dafa7973fc1
sha1: 189166d382c73c242ba45889d57980548d4ba37e
sha256: a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
completed: 2022-02-23T22:11:17Z
signatures:
  Writes to the Master Boot Record (MBR)
  Program crash
  Suspicious behavior: EnumeratesProcesses
  Suspicious use of AdjustPrivilegeToken
  Suspicious use of WriteProcessMemory

targets:
  iocs:
    72.21.81.240
  md5: 5d5c99a08a7d927346ca2dafa7973fc1
  score: 6
  sha1: 189166d382c73c242ba45889d57980548d4ba37e
  sha256: a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
  size: 27648bytes
  tags:
    bootkit
    persistence
  target: m82hr78cg.dll
  tasks: behavioral1 behavioral2
```

Gambar 10. Pengecekan 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 merusak 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 pengecekan Ip reputation menggunakan 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 antivirus) dan **Persistence** (Program malicious akan mencoba mempertahankan akses pada device korban).

72.21.81.240 was found in our database

This IP was reported 143 times. Confidence of Abuse is 26% ?

26%

ISP: Verizon Business
Usage Type: Fixed Line ISP
Domain Name: verizonenterprise.com
Country: United States of America
City: Atlanta, Georgia

IPs including ISP, Usage Type, and Location provided by IP2Location (Updated monthly)

REPORT 72.21.81.240 INFO 72.21.81.240

IP Abuse Reports for 72.21.81.240:

This IP address has been reported a total of 143 times from 26 distinct sources. 72.21.81.240 was first reported on November 24th 2020, and the most recent report was 1 week ago.

Old Reports: The most recent abuse report for this IP address is from 1 week ago. It is possible that this IP is no longer involved in abusive activities.

Reporter	Date	Comment	Categories
Anonymous	11 Mar 2022	SSH Scan	Reporting
Anonymous	10 Mar 2022	Possible TCP Flood on IP X1 - from machine xxx.xx.10.3 / 30.40 with TCP packet rate of 1/sec has cease ... show more	Reporting
Anonymous	09 Mar 2022	SSH Scan	Reporting
Anonymous	04 Mar 2022	SSH Scan	Reporting
BOLWP	19 Feb 2022	Feb 16, 2022 This is used as a CDN for Microsoft/updates.Couldn't believe it, verizon owns IP. bu ... show more	Reporting
Anonymous	16 Feb 2022	SSH Scan	Reporting
Anonymous	11 Feb 2022	Possible TCP Flood on IP X1 - from machine xxx.xx.85.c 5.6c.5a with TCP packet rate of 1/sec has cease ... show more	Reporting
Anonymous	07 Feb 2022	SSH Scan	Reporting
Anonymous	03 Feb 2022	SSH Scan	Reporting
Eric Koelzer	01 Feb 2022	Still need to fully investigate, seemed the possible exploit? Noticed PC running very uncommon high a ... show more	Reporting
Suspect host	27 Jan 2022	trying to get into my computer	Reporting
Suspect host	25 Jan 2022	messing with my computer, no permission to be in it	Reporting

Gambar 10. Pengecekan 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.

General

Target: stage1.exe
Filesize: 27KB
Completed: 07-04-2022 06:38

bootkit persistence

Score: 6/10

MD5: 5d5c09a08a7d927346ca2dafa7973fc1
SHA1: 189166cd382c73c242ba45889d57980548d4ba37e
SHA256: a196c0b8fcb977fb276d04f554896e2391311db3841ae16c8d95f9f6a38e92

Malware Config

Signatures

Filter: none

Persistence

Writes to the Master Boot Record (MBR) stage1.exe

Program crash Werfault.exe

Reported IOCs

pid	pid_target	process	target process
1824	2016	WerFault.exe	stage1.exe

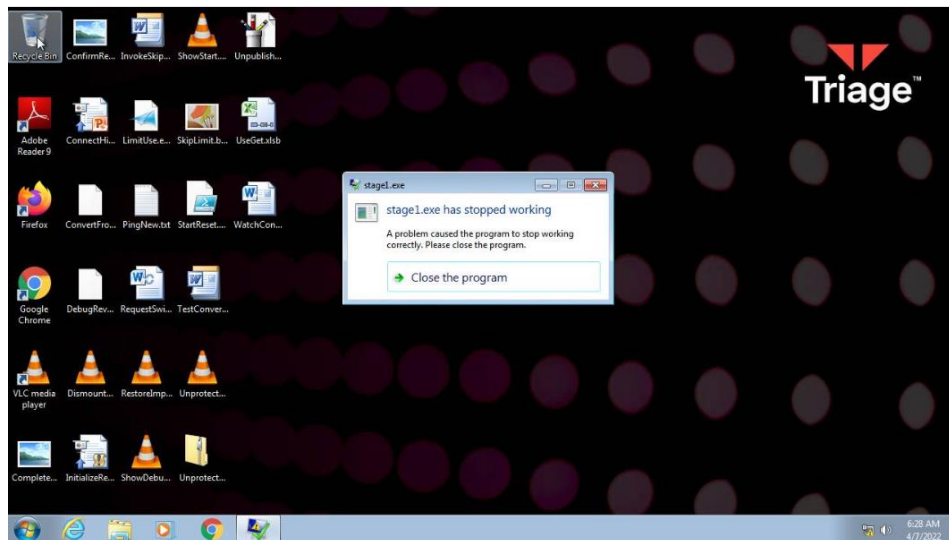
Suspicious use of WriteProcessMemory stage1.exe

Reported IOCs

description	pid	process	target process
PID 2016 wrote to memory of 1824	2016	stage1.exe	WerFault.exe
PID 2016 wrote to memory of 1824	2016	stage1.exe	WerFault.exe
PID 2016 wrote to memory of 1824	2016	stage1.exe	WerFault.exe
PID 2016 wrote to memory of 1824	2016	stage1.exe	WerFault.exe

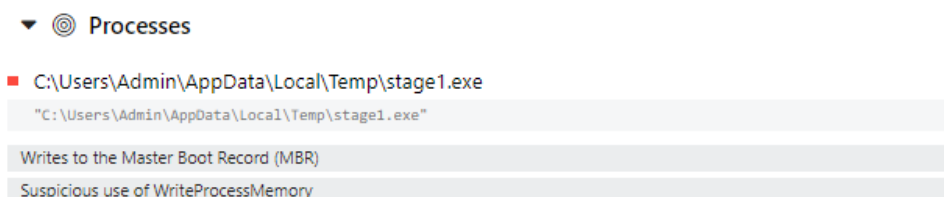
Gambar 11. Hasil pengecekan triage part 1

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 program stage1.exe termasuk dalam killchain persistence sebagai bootkit. Berdasarkan informasi yang kami dapatkan dari mitre ATT&CK, bootkit terletak pada lapisan dibawah system operasi dan sangat sulit untuk dideteksi.



Gambar 12. Hasil pengecekan 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 membuka **\\?\\PhysicalDrive0** dan akan memodifikasinya. Akibat dari aktivitas yang dijalan oleh stage1.exe ini menyebabkan WerFault.exe memunculkan pesan error kepada si user.



Gambar 13. Hasil pengecekan 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 menjalankan 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.