

WriteUp Malware
Keamanan Jaringan



Nama : Arjuna Nazril Ramadhan
No : 08
Kelas : XII TKJ 1

Daftar Isi

Analisis Malware.....	3
Walkthrough:.....	3
Sampel 1:.....	3
Sampel 2:.....	4
Sampel 3:.....	5
Sampel 4:.....	7
Sampel 5.....	9

Analisis Malware

Kategori: Malware Analyst

Desc: Kita di suruh buat analisis sebuah malware, trojan, dll sebagainya, serta kita harus memutuskan kategori apa yang harus di cap, dan eksekusi apa yang di gunakan seperti block, allow dan lain sebagainya.

Walkthrough:

Sampel 1:

kategori: Malware Analyst

Desc: Setelah tugas 1 kemaren kita hitung hash dari “Rencana Ujian SMK 2026.” kita lanjut ke analisis hashnya adakah yang disisipin?? harusnya tidak yaa karna kita sendiri yang buat.

lanjut ini hashnya : `4e12d85840512200ad38d5c98e297c05cf4bf2dfd7894f187f9ecdbc4a42cec1`
(Nahh, jadi untuk hash ini karna ini kita buat sendiri dan belum masuk pada scanner VT/VirusTotal jadi kita perlu kirimkan programnya biar di scan).

The screenshot shows the VirusTotal analysis page for a file named `dokumen_rahasia.txt` with hash `4e12d85840512200ad38d5c98e297c05cf4bf2dfd7894f187f9ecdbc4a42cec1`. The file is 28 B in size and was analyzed 9 hours ago. The community score is 0/61. The analysis shows that no security vendors flagged this file as malicious. Below the analysis, there is a table of security vendors' analysis results, all of which are "Undetected".

Security vendors' analysis	
Acronis (Static ML)	Undetected
AliCloud	Undetected
Antiy-AVL	Undetected
Avast	Undetected
Avira (no cloud)	Undetected
Bkav Pro	Undetected
CMC	Undetected
AhnLab-V3	Undetected
ALYac	Undetected
Arcabit	Undetected
AVG	Undetected
BitDefender	Undetected
ClamAV	Undetected
CrowdStrike Falcon	Undetected

Nahh bisa kita lihat disini statusnya emang Undetected karna dari database VT tidak menunjukkan kecurigaan dan belum diuji jadi....

Skor Detection : 0/61
Kategori Ancaman : Clean/ Undetected
Tindakan : Allow

Sampel 2:

Kategori: Malware Analyst

Desc: Ini adalah sebuah web login page yang mengandung Phising atau biasa disebut Login Phising, kita akan coba analisis bagaimana dalamnya?? dan adakah di VirusTotal?..

INI URLNYA : <http://testsafebrowsing.appspot.com/s/phishing.html>

kita cek

The screenshot shows the VirusTotal web interface. The URL being analyzed is <http://testsafebrowsing.appspot.com/s/phishing.html>. The community score is 12/92. The URL report shows the status as 200, content type as text/html, and last analysis date as 1 hour ago. The security vendors' analysis table shows the following results:

Security vendor	Detection
ADMINUSLabs	Malicious
BitDefender	Phishing
Chong Lua Dao	Malicious
CyRadar	Phishing
G-Data	Phishing
Google Safe Browsing	Phishing
Kaspersky	Phishing
LevelBlue	Phishing
Lionic	Phishing
Sophos	Phishing
VIPRE	Malware
Webroot	Malicious
ESET	Suspicious

ini adalah sebuah web phising login page, yang mana ketika kita ngeinput sebuah username dan password nanti akan masuk ke perangkat, dengan Vendors's analyst positif 12 dari 92 (12/92).

Kebanyakan disini adalah masuk ke Kategori Phising, karena memang ditujukan buat mancing.

Skor Detection : 12/92
Kategori Ancaman : Phising
Tindakan : Block

Karna kita mau lebih aman lebih baik diblok ketika menemukan malware atau algorithm yang samaa, cuman ini di buat ujicoba dan harusnya amann cuma buat testing dan contoh jadi bisa kita allow/quarantine.

Sampel 3:

Kategori: MA (Malware Analyst)

Desc: Kita akan analyst sebuah malware dengan nama yang cukup terkenal yaitu WannaCry, kita nanti bahas... nahh di JOOBSHEET itu 3 dari Malware hashnya rata-rata pada ga bisa, jadi kita cari hashnya yang asli dan origin dari <https://bazaar.abuse.ch/> Saya sangat sangat.... berterima kasih dengan developer yang buatt.... trims trimss.

nah coba hashbnya kita tampilin di VT.

hashnya : **24d004a104d4d54034dbcf2a4b19a11f39008a575aa614ea04703480b1022c**

coba kita cek....

68/70 security vendors flagged this file as malicious

24d004a104d4d54034dbcf2a4b19a11f39008a575aa614ea04703480b1022c

Size: 3.55 MB | Last Analysis Date: 18 hours ago

lhdfrgui.exe

peexe | idle | cve-2017-0147 | exploit | direct-cpu-clock-access | malware | checks-network-adapters | checks-user-input | macro-create-ole | detect-debug-environment | long-sleeps | runtime-modules | cve-2017-0144

Community Score: -1806

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.wannacry/wanna

Threat categories: trojan | ransomware | worm

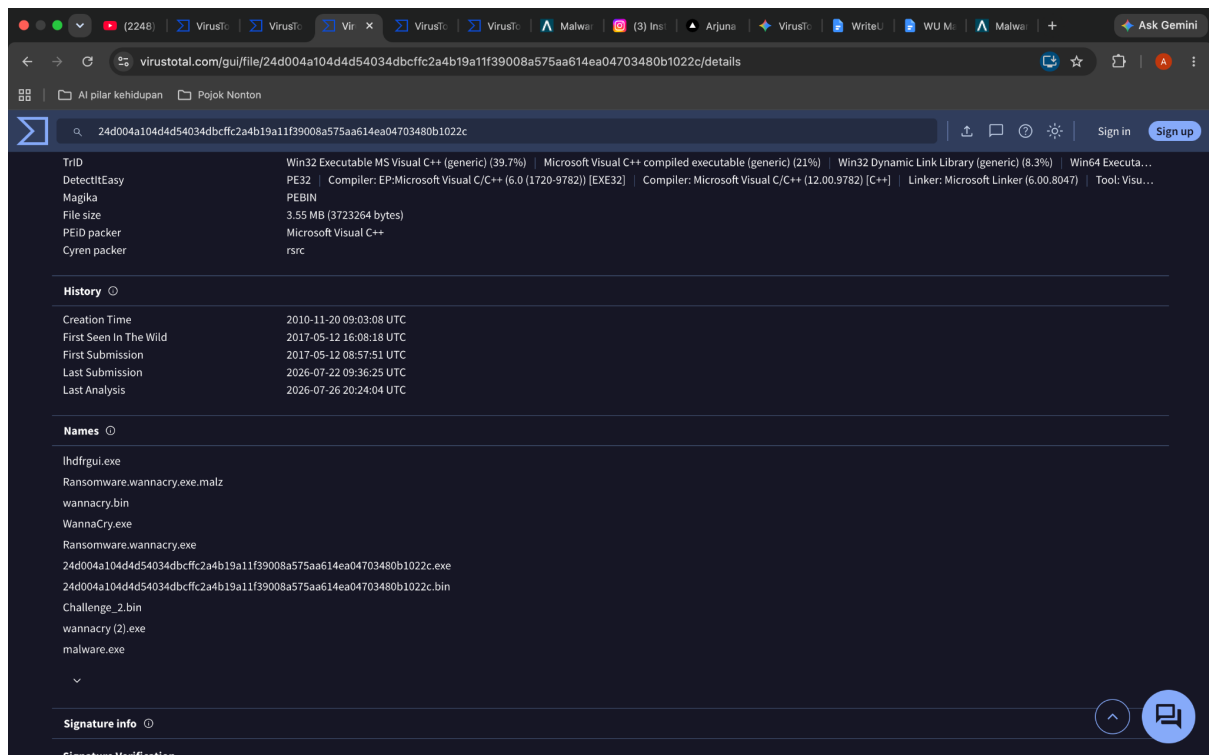
Family labels: wannacry | wanna | wannacryptor

Security vendors' analysis

Security vendors' analysis		Do you want to automate checks?	
Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.WannaCryptor.R200572
Alibaba	Ransom:Win32/WannaCry.398	AliCloud	Exp:Win/CVE.2017.0147
ALYac	Trojan.Ransom.WannaCryptor	Antiy-AVL	Trojan[Ransom]/Win32.Wanna
Arcabit	Exploit.CVE-2017-0147.3	Arctic Wolf	Unsafe
Avast	SF:WNCryLdr-A [Trj]	AVG	SF:WNCryLdr-A [Trj]

wow... hampir semuanya adalah malware dengan vendor's point 68 DARI 70 wow. Jadi si file atau malware Wannacry ini adalah Ransomware atau Malware yang menargetkan ke aplikasi Office dengan cara ATTCker akan mengunci data Office dengan format .WCRY, sebagai kompensasi biasanya si ATTCker minta tebusan bitcoin..

kita cek lebih rinci.. ke detail



Disitu terlihat IDnya Win32 dan banyak dari aplikasi yang di targetkan adalah app OFFICE..
jadiiii..

Skor Detection : 68/70
Kategori Ancaman : Trojan Ransomware
Tindakan : Block

Jadi karna ini adalah Ransomware yang berbahaya yaaa kita perlu Block untuk alasan
Keamanan(Protect) atau perlindungan.

Sampel 4:

Kategori: MA

Desc: EMOTET nihhh.. unikk jadi dia ini adaalah ransomware yang seiring tambah canggihnya teknologi jadi trojan yang mengambil atau mencuri data sampai uang melalui gmail spam, coba ini kita test dan cek di VT.

hash: **251037ceebfbacd419b663ebcf0e01ec80a2c46dbfc85f66492c8585b481fb8c**

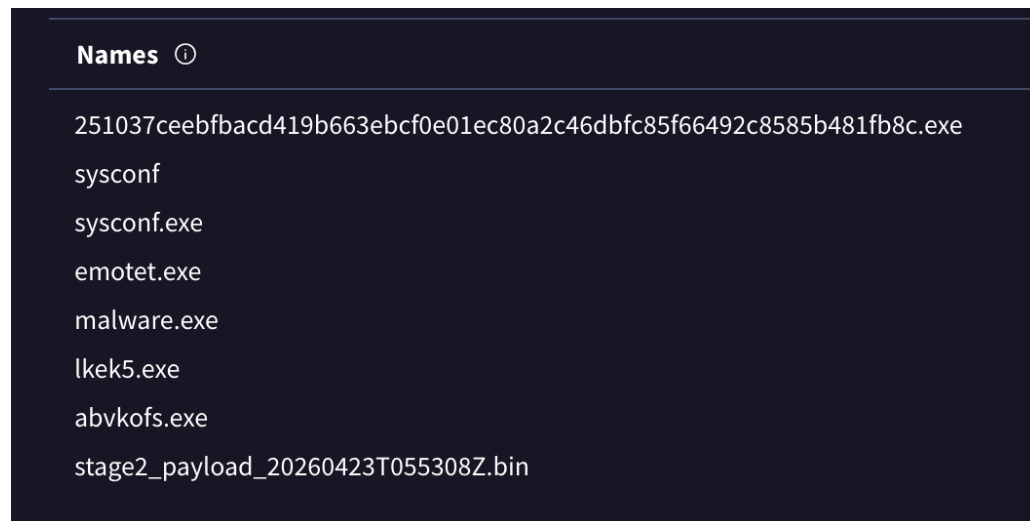
ohh yah.. ketiga inii mulai dari Wannacry sampai EICAR nanti adalah hash asli, mungkin ada modifikasi dari dev. lain saya ambil di <https://bazaar.abuse.ch/> okee lanjut.

The screenshot shows the VirusTotal analysis page for the file `sysconf.exe` with hash `251037ceebfbacd419b663ebcf0e01ec80a2c46dbfc85f66492c8585b481fb8c`. The community score is 51/70. The file is identified as a trojan and dropper. The security vendors' analysis table is as follows:

Security Vendor	Detection
AhnLab-V3	Trojan.Win.Generic.R779905
AliCloud	Trojan[stealer].Win/Lumma.azxl
Antiy-AVL	Trojan[PSW].Win32.Lumma
Arctic Wolf	Unsafe
AVG	Win64:MalwareX-gen [Pws]
BitDefender	Trojan.Generic.39866243
Alibaba	TrojanPSW:Win32/Lumma.3ba3ff15
ALYac	Trojan.Generic.39866243
Arcabit	Trojan.Generic.D2604F83
Avast	Win64:MalwareX-gen [Pws]
Avira (no cloud)	DR/W64.MalwareX
Bkav Pro	W32.Malware.41961ED4

yuupp kokk?... kenapa Emotet malah 51/70 lebih sedikit timbang Wannacry yah..?? jadi konsep ini bisa di katakan Emotet adalah ransomware yang cukup baru dan fleksibel. Ketika Wannacry codenya cuma statis ya itu aja jadi yang terscan atau yang terbaca darii VT itu ya banyakk vendor's lebih nangkap klo ini ransomware, sedangkan Emotet dia lebih Fleksibel dan karakteristiknya biasanya dia mengubah kode ketika di kirim via gmail spam maupun di unduh secara langsung, jadii yaa dia lebih pintar dan terstruktur, karna malah biasanya kode aslinya di umpetin untuk mengelabui.

Cobaa kitaaaa cek lebih detail.....



terbukti dan terlihat kalo ini adalah Emotet yahh..

Magic	PE32+ executable (GUI) x86-64, for MS Windows
TrID	OS/2 Executable (generic) (33.6%) Generic Win/DOS Executable (33.1%) DOS Executable (generic) (33.1%)
DetectItEasy	PE64 Compiler: Microsoft Visual C/C++ (19.29.30148) [C++] Linker: Microsoft Linker (14.29) Tool: Visual Studio (2019 version 16.11)

kok ada DOS?? kalo ini emang dari sistem windows mau yang baru ataupun lama tetep harus ada jadi bukan semata Emotet dibuat untuk DOS.
jadiiii....

Skor Detection : 51/70
Kategori Ancaman : Trojan
Tindakan : Block

Karnaa rata rata data vendor's yang melaporkann adalah trojan, memang asal usulnya ini adalah trojan kuno di kisaran tahun 2014an kemudian ada beberapa modif jadi file emotet aslinya di modif dan di fusion dengan ransomware lain.

Sampel 5

Kategori: MA

Desc:

Inii EICAR niiihh... jadi inii semacam testingg yang dibuat oleh seseorang, yaitu user buat testing yang sengaja buat Antivirus test file yhhh...

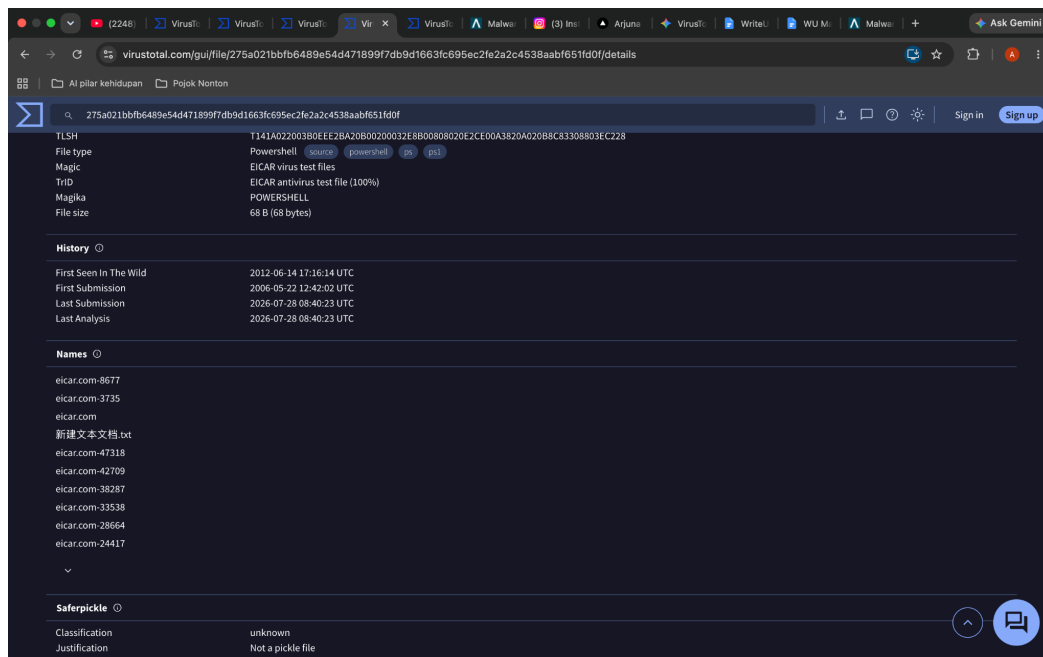
ini hashnya: **275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f**

coba kita add ke VT

The screenshot displays the VirusTotal analysis page for a file with the hash **275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f**. The page shows a community score of 63/65, a file size of 68 B, and a last analysis date of 8 minutes ago. It lists various threat categories like powershell, via-tor, idle, direct-cpu-clock-access, detect-debug-environment, long-sleeps, attachment, and known-distributor. The 'Code insights' section explains that EICAR is a test string used to detect and test antivirus software. The 'Security vendors' analysis' section shows detections from AhnLab-V3, AliCloud, Alibaba, and ALYac.

Security vendors' analysis	Detection	Vendor
AhnLab-V3	Virus/EICAR_Test_File	Alibaba
AliCloud	Engtest:Multi/Eicar	ALYac
		Virus:Win32/EICAR.A
		Misc.Eicar-Test-File

nahhh inii diaa sebuahh test yaa dengan Vemdor's rating yang cukup tinggi karna emang difungsikan untuk testing dan mentah berupa kode kode mencurigakan. Coba kita cek detail..



okee cukup terbukti yaa dengan nama [eicar.com-8677](https://www.eicar.org/download-anti-malware-testfile/) valid untuk testing dari web resmi Eicar <https://www.eicar.org/download-anti-malware-testfile/> dann itu diaa..

Skor Detection : 63/65
Kategori Ancaman : Virus (Test)
Tindakan : Quarantine

Kenapaa kita allow??? karna ini semacam antivirus atau file test buat check gitu.. jadi aman apa perbedaannya dari test url safebrowsing?.. cukup berbedaa kita tahu mereka sama sama buat uji cobaa klo EICAR itu user atau perorangan kaloo safebrowsing itu dari safebrowsing itu sendiri yang notabennya merupakan sebuah perusahaan yang buat testing hal tersebut.

Jadi kesimpulannyaa, Ketika kita ketemu file atau hash yang rusak dan tercurigai sudah di sisipin sebuah trojan atau malware kita perlu check dan tetap waspada dan jangan Writeup ini jadi patokan yang pasti...