WriteUp Malware
Keamanan Jaringan

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

Daftar Isi

Analisis Malware

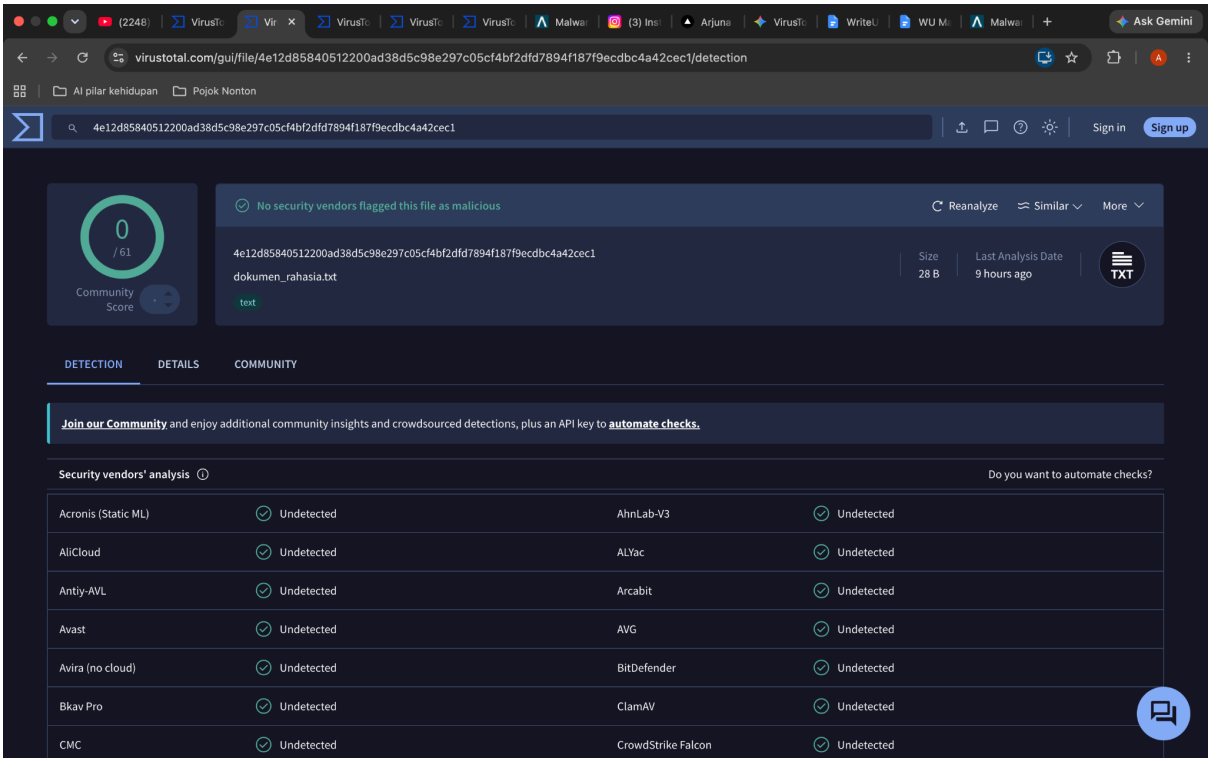
Kagetori: Malware Analyst
Desc: Kita di suruh buat analisis sebuah malware, trojan, dll sebagainyaa, serta kita harus memutuskan kategori apa yang harus di cap, dan eksekusi apa yang di gunakan seperti block, allow dan lain sebagainya.

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 belom masuk pada scanner VT/VirusTotal jadi kita perlu kirimkan programnya biar di scan).



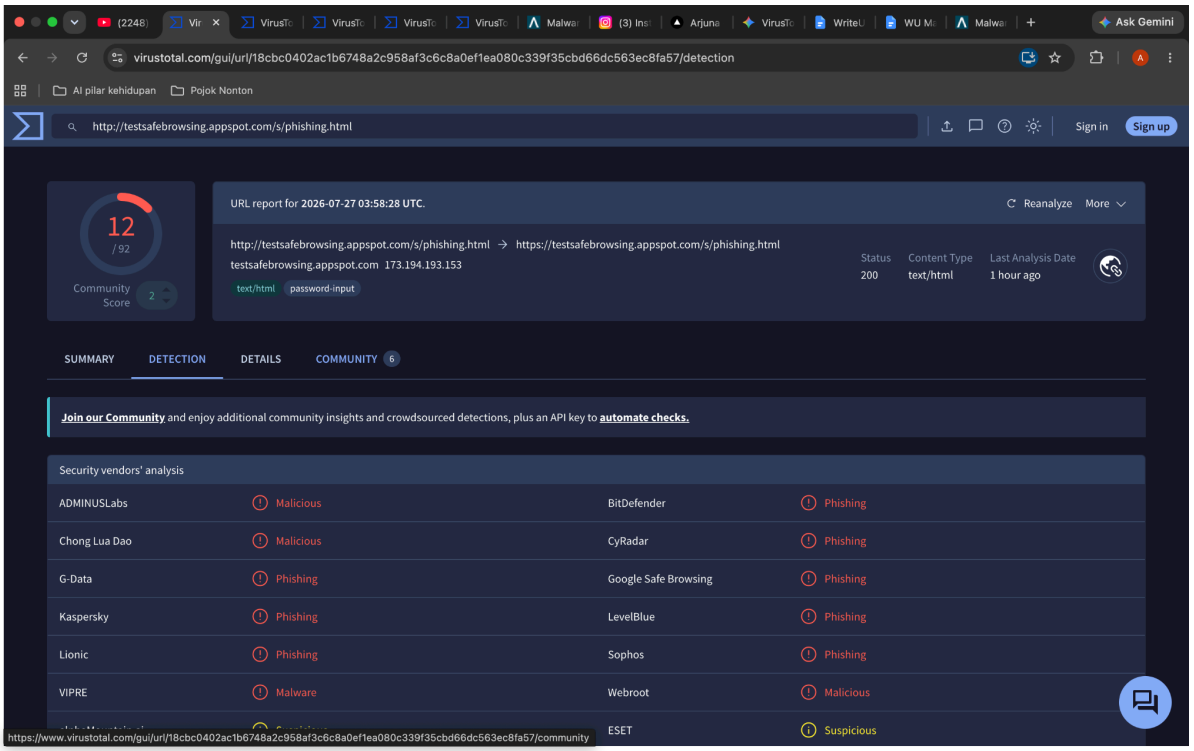
Nahh bisa kita lihat disinii statusnya emang Undetected karna dari database VT tidak menuntukkan kecurigaan dan belum diuji jadi….

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

Sampel 2:

Kategori: Malware Analyst
Desc: Ini adalah sebuat web login page yang mengandung Phising atau biaasa disebut Login Phising, kita akan coba analisis bagaimana dalamnyaa?? dan adakah di VirusTotal?..

INI URLNYA : http://testsafebrowsing.appspot.com/s/phishing.html
kita cek



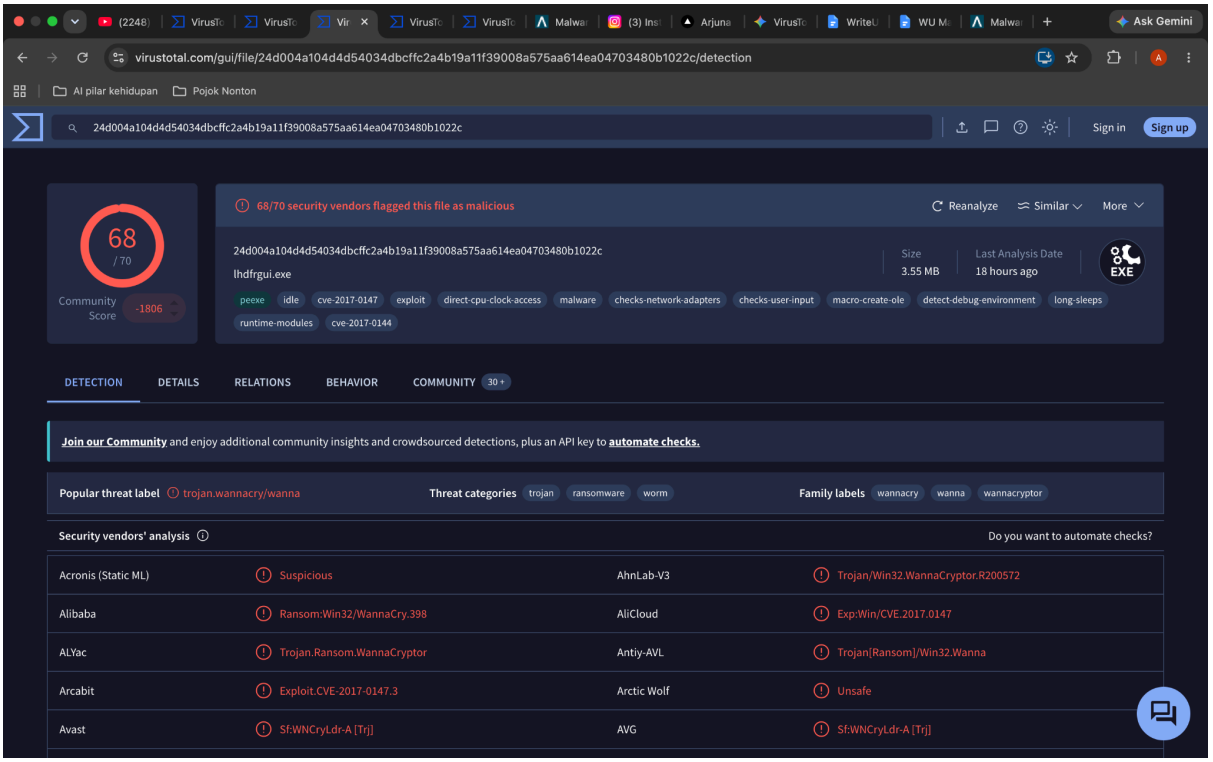
ini adalah sebuah web phising login page, yang mana ketika kita ngeinput sebuah username dan password nanti akan masuk ke perangkat, dengan Vendors's analyst positif 12 dari 92 (12/92). Kebanyakan disini adalah masuk ke Kategori Phising, karena emang ditujukan buat mancing.
Skor Detection : 12/92
Kategori 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:

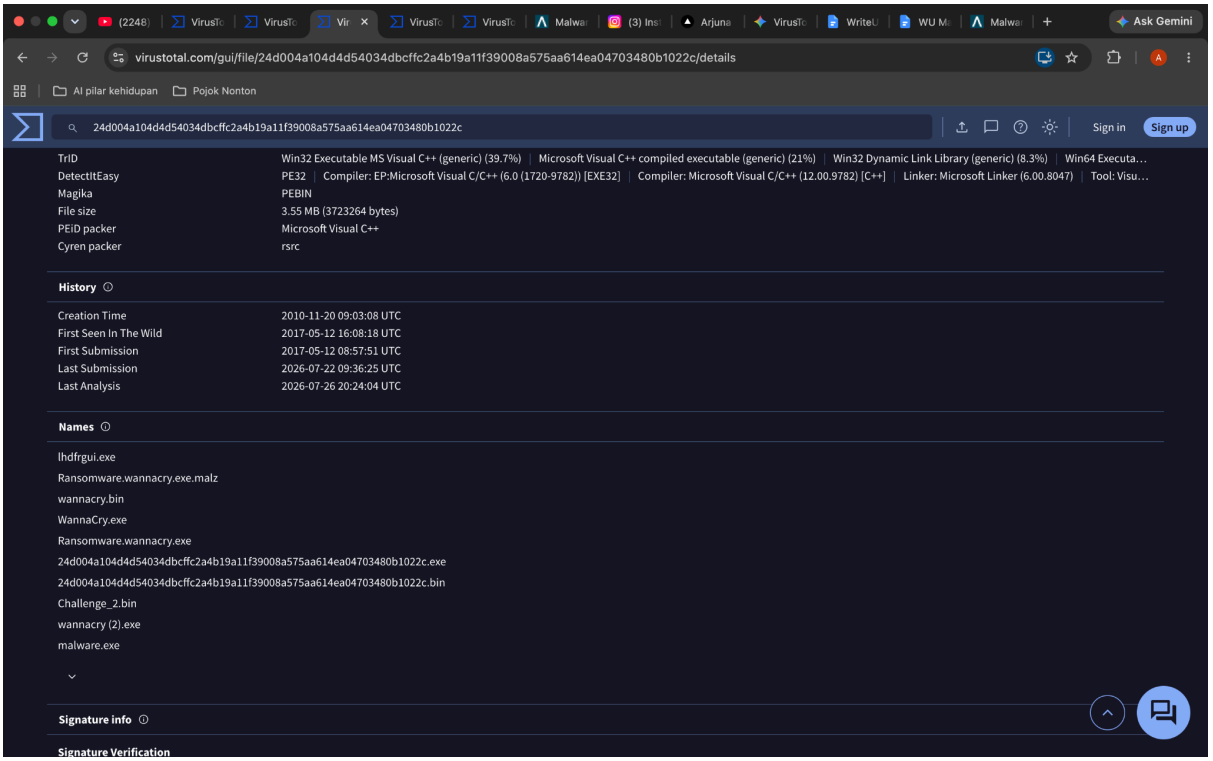
Kategori: MA (Malware Analyst)
Desc: Kita akan analyst sebuah malware dengan nama yang cukup terkenal yaitu WannaCry, kita nanti bahas… nahh di JOOBSHEET itu 3 dari Malware hashnya ratarata pada ga bisa, jadi kita cari hashnya yang asli dan origin dari https://bazaar.abuse.ch/ Saya sangat sangat…. berterima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

nah coba hashbnya kita tampilin di VT.
hashnya : 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
coba kita cek….



wow… hampirr semuanyaa adlaah malware dengan vendor's point 68 DARIII 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.. jadiii..

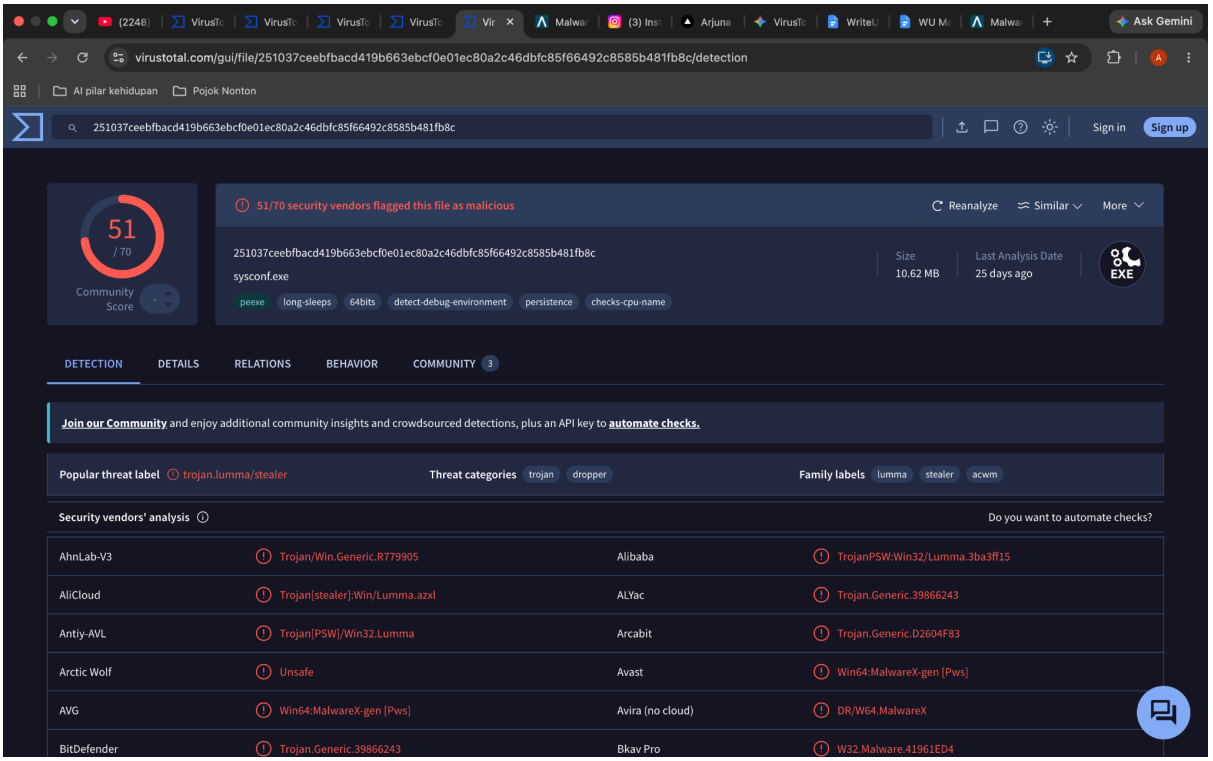
Skor Detection : 68/70
Kategori Ancaman : Trojan Ransomware
Tindakan : Block

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

Sampel 4:

Kategori: MA
Desc: EMOTET niihhh.. unikkk 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.

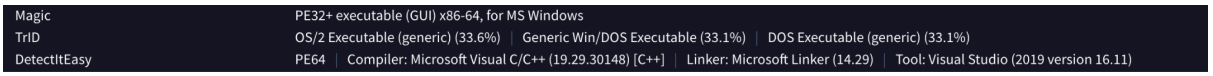
hash: 251037ceebfbacd419b663ebcf0e01ec80a2c46dbfc85f66492c8585b481fb8c
ohh yah.. ketiga inii mulai dari Wannacry sampai EICAR nanti adalah hash asli, mungkin ada modifikasi dari dev. lain saya ambil di https://bazaar.abuse.ch/ okee lanjut.



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 itu ajaa 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 pinter dan terstruktur, karna malah biasanya kode aslinya di umpetin untuk mengelabuhi.

Cobaa kitaaaa cek lebih detail…..

terbukti dan terlihat kalo ini adalah Emotet yahh..



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

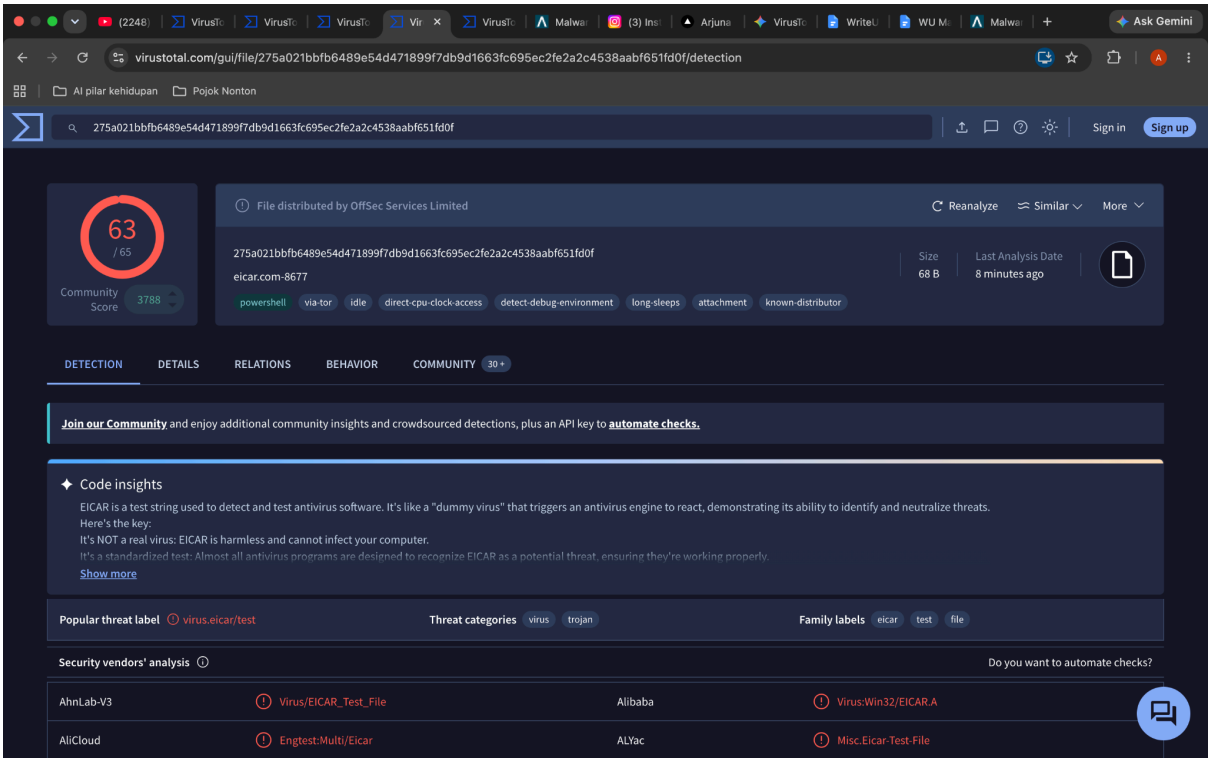
Kategori: MA

Desc:

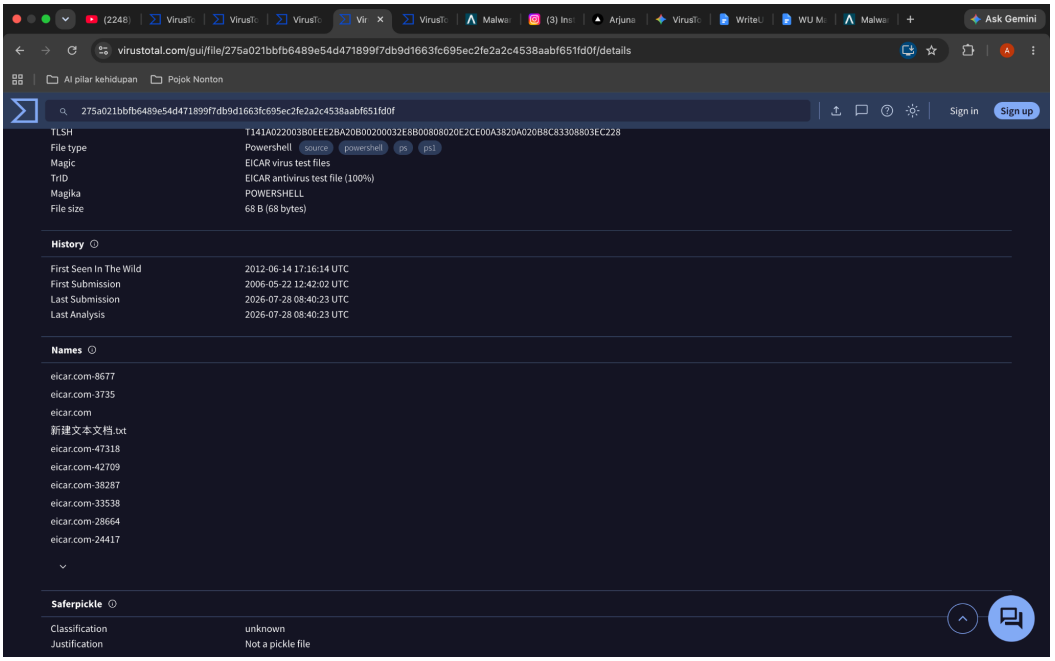
Inii EICAR niiihh… jadi inii semacam testinggg yang dibuat oleh seseorang, yaitu user buat testing yang sengaja buat Antivirus test file yahh…

ini hashnya:275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

coba kita add ke VT



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 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 gituu.. 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 perusahan 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…