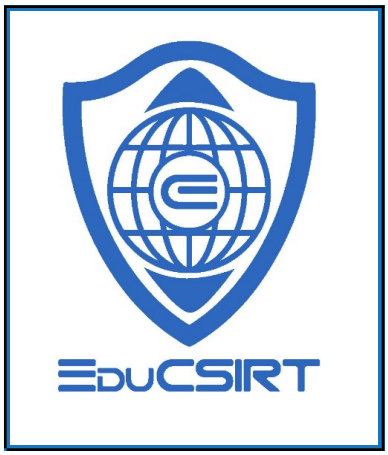


Cara Mencegah Serangan Malware

Pusat Data dan Teknologi Informasi

Kementerian Pendidikan dan Kebudayaan

Rebuplik Indonesia

Malware adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, server atau jejaring komputer tanpa izin (*informed consent*) dari pemilik. Malware bisa menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data / informasi. Hal yang pada umumnya terjadi penyebab malware adalah mendownload software ilegal yang memungkinkan disisipan sebuah malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit, spyware, adware (infected), serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna perangkat komputer.

Ada pepatah bagus untuk mengingatkan kita akan pentingnya aware terhadap malware yaitu : "*Malware attacks would not work without the most important ingredient: you*." ada juga yang lain *Sec_rity is not complete without U*. Kita sendiri sebagai brainware yang mempunyai sebab terbesar membawa malware menginfeksi perangkat yang kita gunakan. Kadang kita terlena dari informasi digital yang ingin kita ketahui tanpa bersabar berearapa waktu untuk berfikir sebentar sebelum memberi klik pada link file tersebut. Apakah kita mudah tertipu?, bisa jadi karena literasi teknologi yang perlu ditingkatkan. Membuka lampiran email yang tidak kita kenal siapa pengirimnya, walaupun judul dari attachment file tersebut menggoda untuk diklik. Sebagai ilustrasi, Berita virus corona yang sedang melanda di kota wuhan, yang menyebabkan kekhawatiran bagi kita semua, bisa jadi anggota keluarga saudara berada di sana. Khawatir?, Pada saat tersebut, saudara mendapat email masuk dengan judul file "tips mengobati" atau "menghindari virus corona". STOP. Jangan terburu-buru klik link tersebut, bisa jadi file tersebut adalah malware. Banyak cara attacker mengirim malware ke end point (perangkat) kita, selain dari email, bisa pula dari blunded free software programs, File sharing bittorent, removable media, Scareware (jenis perangkat lunak yang muncul sebagai jendela pop-up pada komputer) dan tidak menggunakan internet security software.

AZORult adalah salah satu malware dengan membawa misi mencuri informasi data yang kita miliki. Malware ini membaca cookies dari Google Chrome, Membaca Internet Cache Settings, dan Membaca cookies dari Mozilla Firefox.

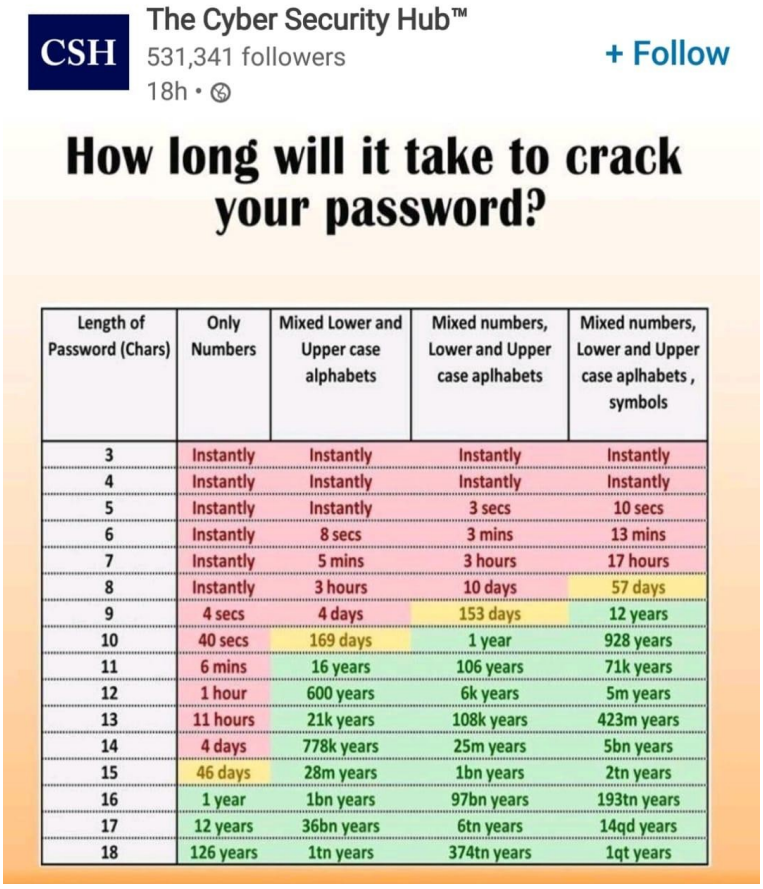
Selain Azorult ada malware lain yang bertipe info stealer yaitu Knot Stealer, pony formgrabber dan lainnya. Tanpa disadari perangkat kita pun terinfeksi malware-malware tersebut. Tidak perlu khawatir, berikut tip cara mencegah malware menginfeksi perangkat kita.

1. Segera ganti password aplikasi khususnya Administrator

   kami menyarankan saudara mengganti password dengan karakteristik password yang kuat. Pada umumnya, password yang dibuat mengandung unsur nama keluarga, hobi, atau pola sederhana lainnya. Password ini memang mudah diingat, tetapi kurang aman.

   UK National Cyber Security Centre (NCSC) menganalisa public databases untuk melihat karakteristik password yang digunakan pengguna. Ditemukan bahwa, daftar teratas adalah lebih dari 23 juta orang menggunakan password 123456. Peringkat kedua ditempati dengan string, 123456789, Passsword seperti itu tidak jauh lebih sulit untuk dipecahkan, sementara yang lain dalam lima teratas termasuk menggunakan dengan prase "qwerty", "password" dan 1111111.

   Nah saudara, berikut informasi dari the cyber security Hub,



Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

menginformasikan bahwa berapa lama password dapat di crack yang dikategorikan mulai dari panjang password, password yang hanya menggunakan angka, menggunakan kombinasi huruf kapital dan kecil, kombinasi angka, huruf kecil dan kapital serta kombinasi dari angka, huruf kecil, besar serta simbol.

Jadi kita tahu kan, mengapa kita harus menggunakan password yang kuat. Nah berikut ini tips awareness terhadapa password yang kita miliki.

a. Gunakan kata sandi unik (berbeda) untuk setiap akun saudara
b. Panjang password minimal 8 karakter, lebih panjang lebih baik
c. Lengkapi, yaitu kombinasi huruf kapital, huruf kecil, angkaa dan simbol
d. Jangan menggunakan password yang umum dan mudah di prediksi. Contoh password yang buruk adalah tanggal lahirmu, nama orang dan nomor handphone.
e. Rubahlah password secara periodik, setiap bulan, dua bulan atau bahkan 3 bulan sekali.
f. Jagalah kerahasiaan password saudara (jangan share kepada siapapun)

2. Update lah selalu Patches Windows saudara.

Update patches dilakukan untuk pembaharuan keamanan berupa perbaikan windows dari kerentanan.

Saudara, Berikut cara update Windows 10 secara,

a. Klik tombol Start atau Windows yang ada di sisi kiri bawah layar.
b. Buka menu Settings atau pengaturan yang ditandai dengan iko roda gigi.
c. Setelah masuk menu Settings, klik pilihan Update & Security.
d. Klik opsi Windows Update yang ada di sidebar sebelah kiri.
e. Klik Check for Updates, jika perangkat kalian memang menerima update baru, update tersebut akan secara otomatis diunduh.

3. Update Web Browser Version

Menjaga web browser selalu ter*update* adalah tanggungjawab yang penting bagi pengguna. Karena Web Browser yang *out the date* mempunyai

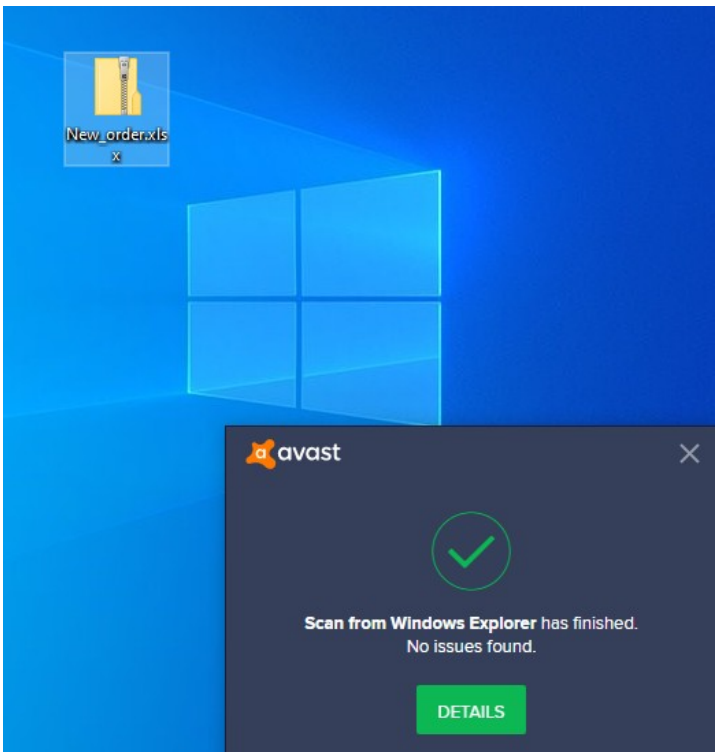
kerentanan keamanan yang serius. Disamping dari sisi keamanan, tentu mengupdate web browser akan menambah fitur-fitur baru.

4. Memasang free tools dari Microsoft;
   a. Windows Defender for Windows 10 and Windows 8.1, Microsoft Security Essentials for Windows 7 and Windows Vista
   b. Microsoft Safety Scanner
5. Memasang Antivirus

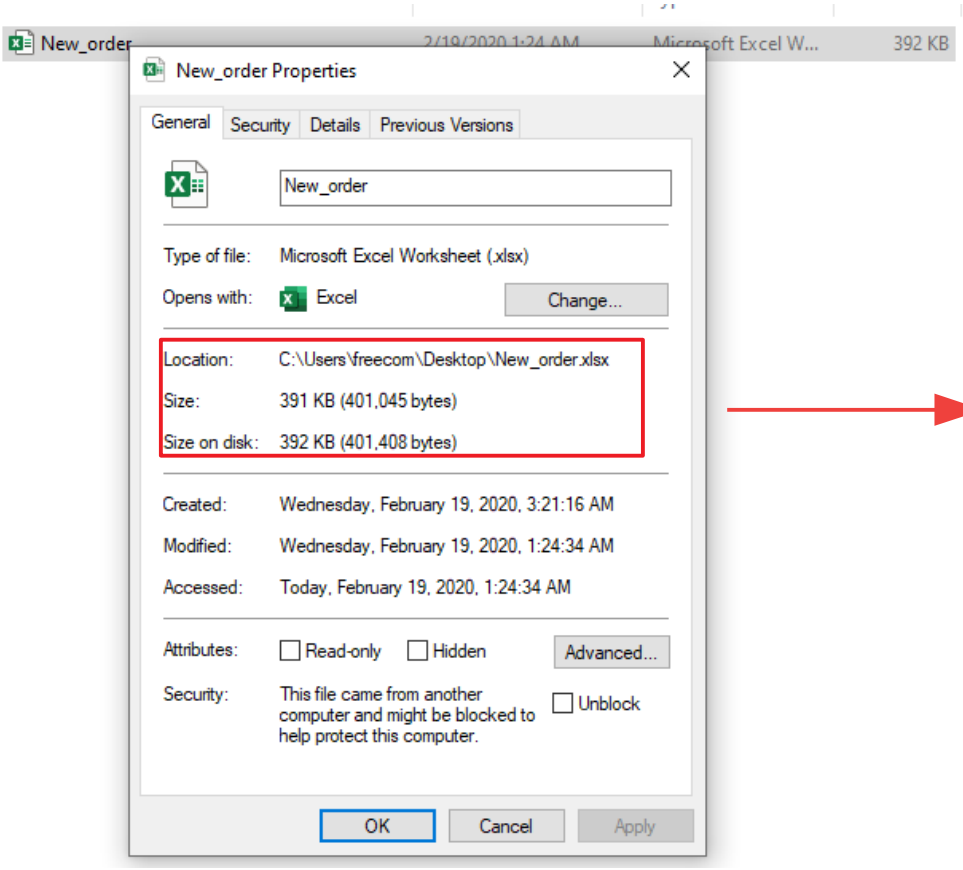
Berikut adalah cara melakukan scan file yang terinfeksi malware azorult pada Sistem Operasi Windows 10 64 Bit (OS Virtual), dengan pendekatan 2 antivirus yaitu Avast Business Pro Plus dan Eset Smart Security Premium. Ruang lingkup uji scan ini adalah scanning pada file compress, file compress yang sudah di extract dan scanning pada sistem operasi setelah ada threat dari file New_order.xlsx.

a. Avast businesss Pro Plus

1). Avast business Pro Plus tidak mendeteksi file yang terinfeksi Malware Azorult dalam keadaan di compress.

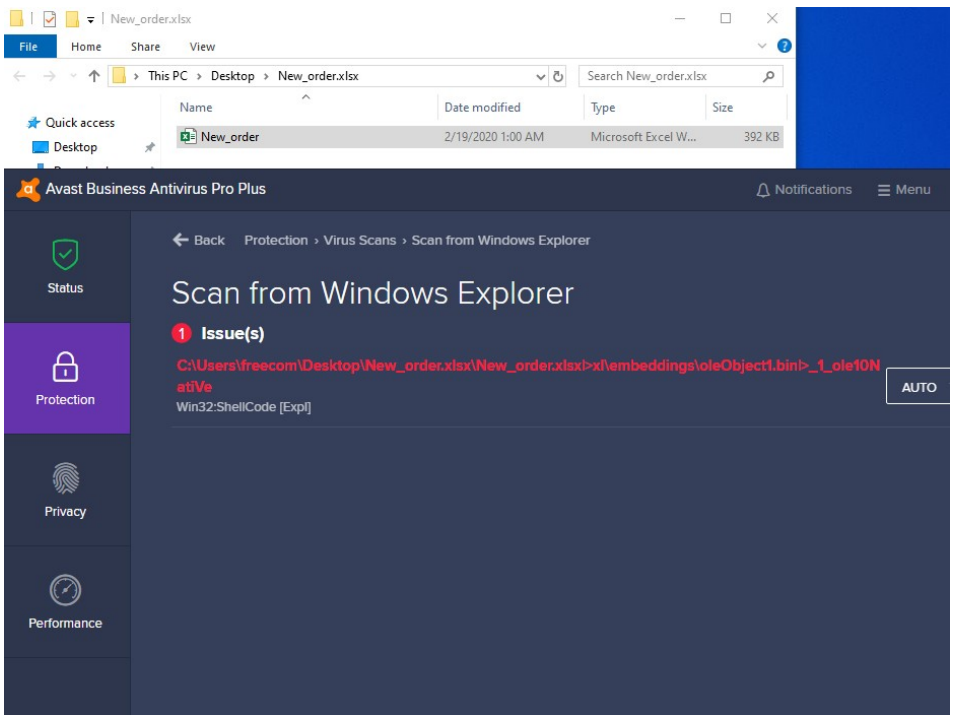


2). Mengektract file compress untuk memastikan apakah antivirus mendeteksi

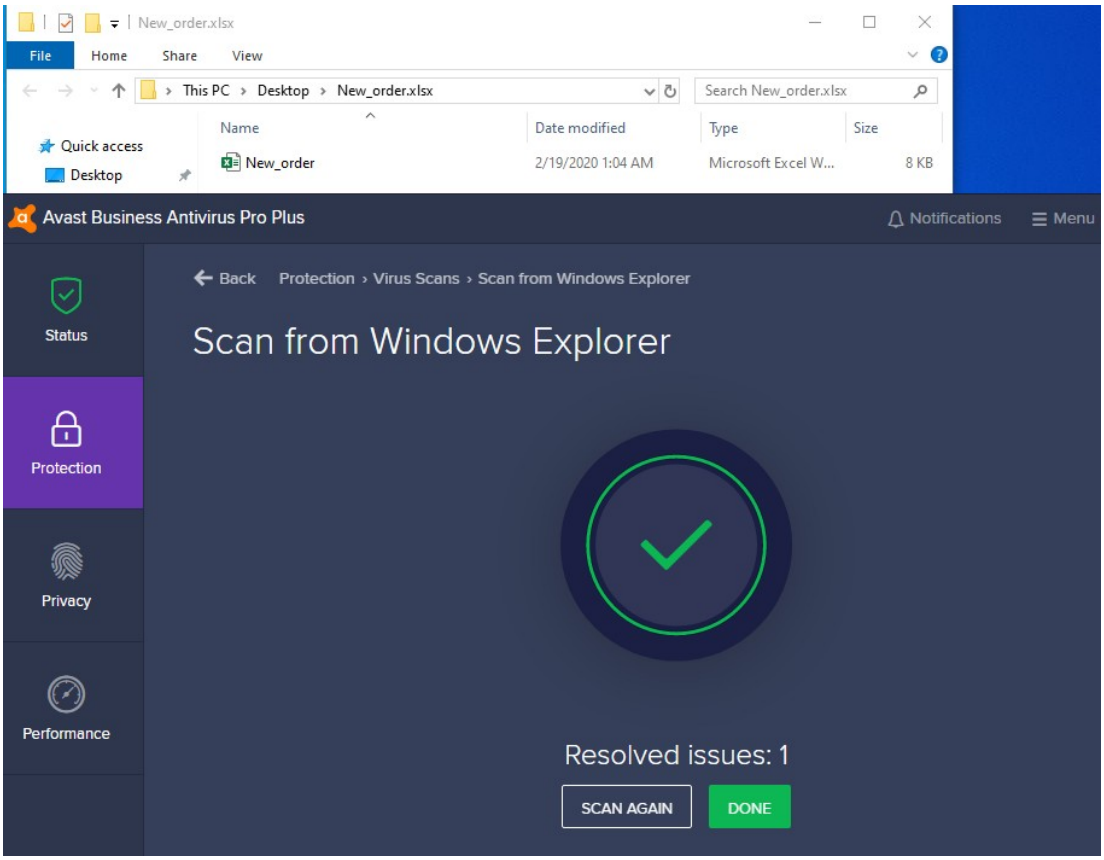


Perhatikan ukuran file New_older.xlsx yaitu 391 KB

3). Avast business Pro Plus Scanning mendeteksi malware Azorult

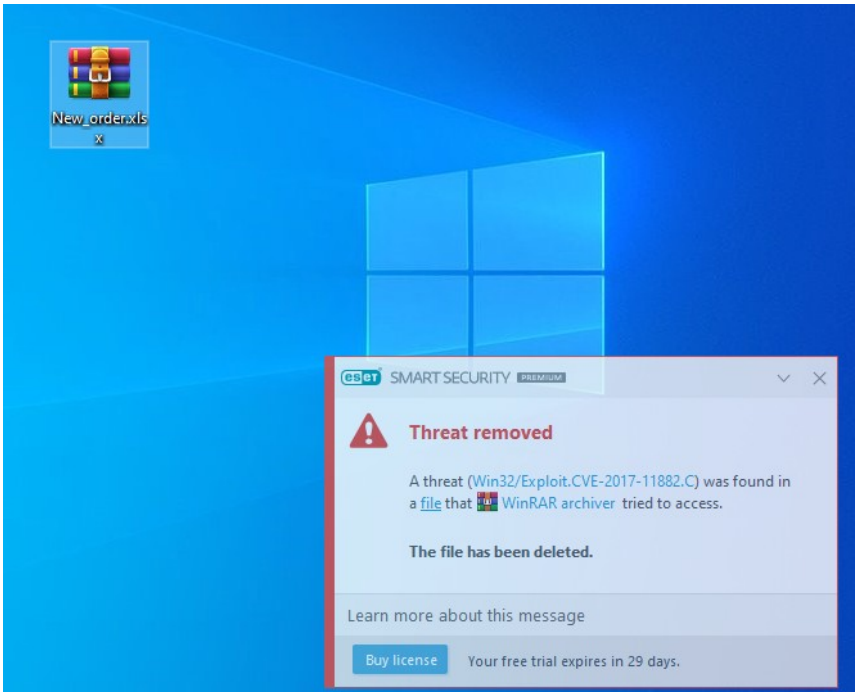


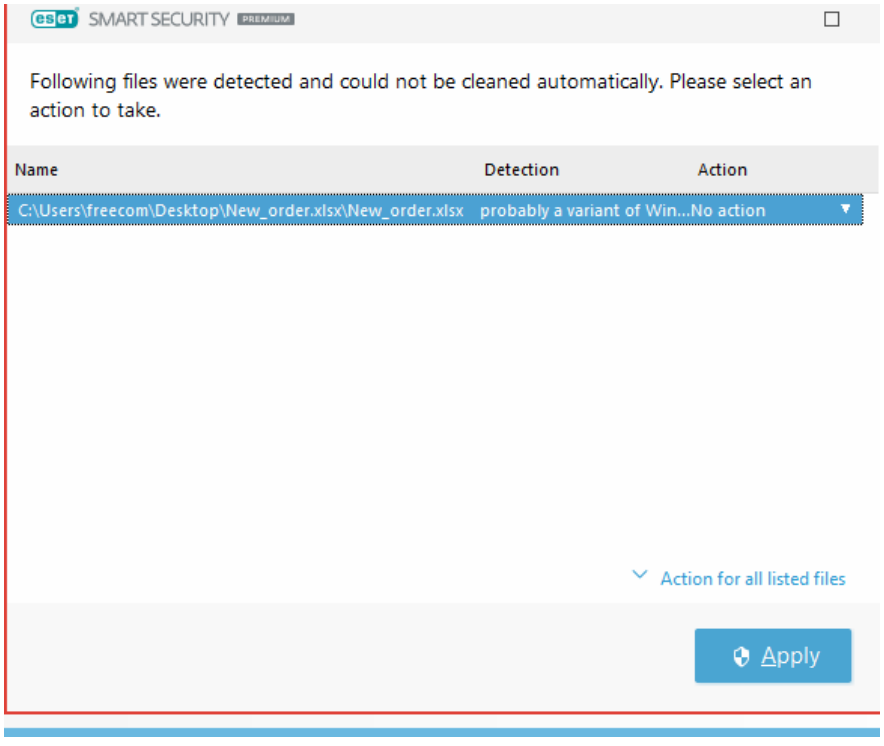
4). Avast business pro plus mendeteksi dan resolving file new_order.xlsx. File setelah di lakukan resoving oleh avast **ukuran 8 KB sebelumnya 392 KB**.



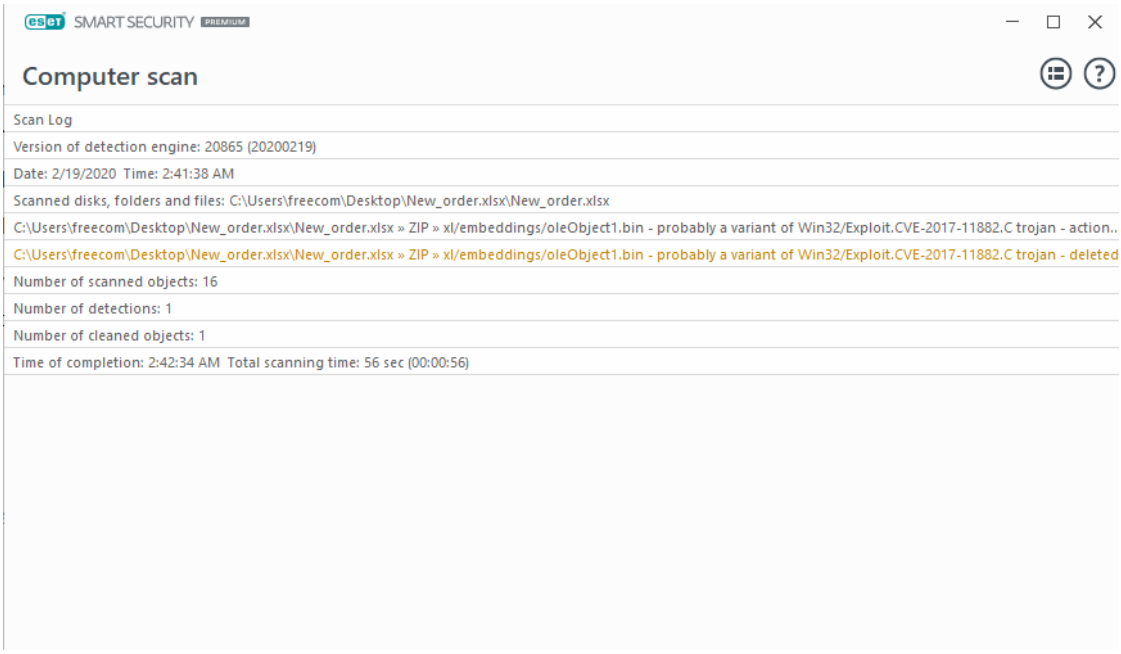
b. Uji Scan dengan ESET Smart Security Premium

1). Eset smart security premium mendeteksi malware azorult

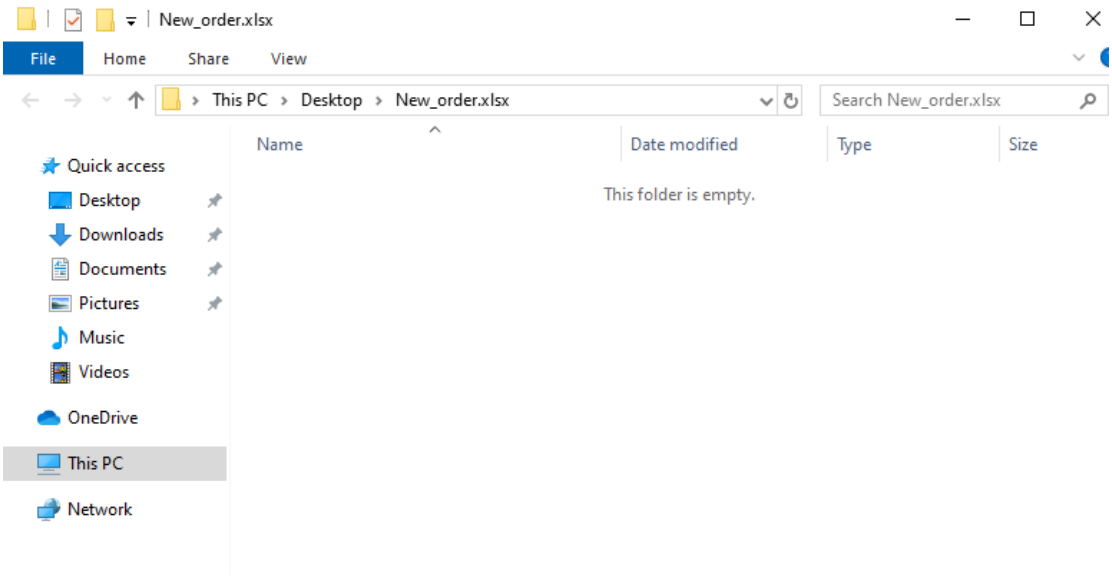




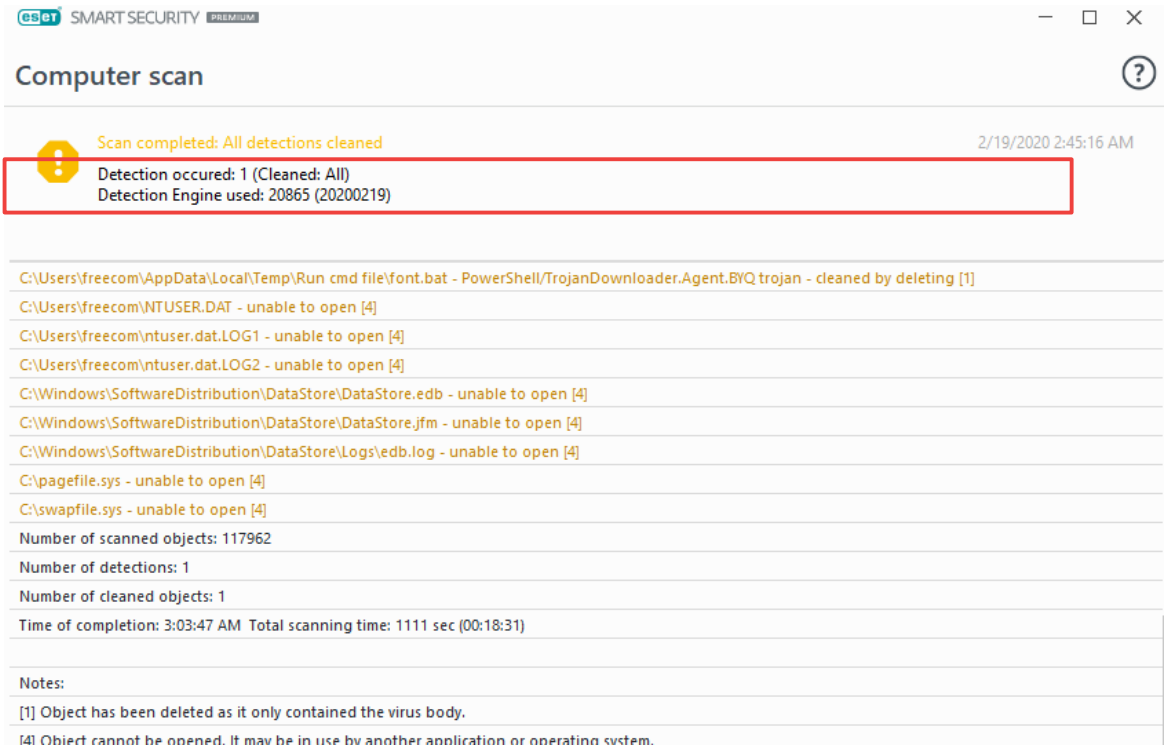
2). Probably a variant of win32/Exploit.CVE.2017-11882.C Trojan Deleted



3). Lebih baiknya Eset smart security premium adalah menghapus file terinfeski malware azorult setelah di lakukan cleaning. Hal ini berbeda dengan Avast Security, file tersebut masih ada dengan ukuran 8 KB.



4. Setelah Eset smart security premium melakukan cleaning pada file tersebut, uji lab berikutnya yaitu scan full OS Windows 10 menggunakan Eset smart security premium. Berikut hasilnyal, seperti bada border warna merah, yang tidak bisa ditemukan oleh Avast dengan scan OS Windows 10. Hal tersebut adalah bagian dari behavior graph dari malware azorult yang telah saya sertakan di atas.



Referensi :

https://id.wikipedia.org/wiki/Perangkat_perusak

https://idcloudhost.com/mengenal-apa-itu-malware-penyebab-dan-mengatasinya/

https://www.malwarebytes.com/malware/

https://www.infosecurity-magazine.com/opinions/malware-detection-signatures/

https://www.bbc.com/news/technology-47974583

https://app.any.

https://www.zunesis.com/why-install-windows-updates/