BADAN SIBER DAN SANDI NEGARA

16/MLW/2025

RANSOMWARE
EL PACO

2025

TLP:CLEAR

DIREKTORAT OPERASI KEAMANAN SIBER

Jl. Harsono RM No.70, Ragunan, Ps. Minggu, Jaksel

Ransomware El Paco merupakan turunan dari varian *ransomware* Mimic. *Ransomware* El Paco pada dokumen ini diperoleh dari sumber terbuka dengan nilai *signature hash* MD5 yaitu 33eeeb25f834e0b180f960ecb9518ea0. Berdasarkan sumber Microsoft, *malware* ini bernama Ransom:Win32/Mimic.MA!MTB.

Pada salah satu kasus El Paco yang terjadi, diduga penyerang memanfaatkan celah kerentanan *Remote Desktop Protocol* (RDP) pada sistem elektronik. *Ransomware* El Paco memiliki *Graphical User Interface* (GUI) yang memudahkan penyerang untuk melakukan konfigurasi jangkauan enkripsi pada sistem elektronik target, isi *ransomnote*, dan hal lainnya yang dibutuhkan oleh penyerang.

Rekomendasi untuk menghindari infeksi *ransomware* ini antara lain dengan menggunakan sistem keamanan berlapis, batasi atau nonaktifkan penggunaan fungsi kendali jarak jauh seperti RDP apabila tidak digunakan, penggunaan kata sandi yang kuat dan autentikasi multi-faktor (MFA), mematikan *port* komunikasi yang tidak digunakan, *update* sistem secara berkala serta meningkatkan *security awareness* terhadap *email attachments, malicious online advertisements, social engineering software ilegal*.

ANALISIS MALWARE

Ransomware El Paco

DAFTAR ISI

A. NOTIFIKASI

MALWARE RATING : EXTREME

Malware Rating System dibuat sebagai metode penilaian yang akurat dan objektif dalam menilai sebuah *malware* sehingga dapat diketahui tingkat risiko dan keterkaitan dengan dampak penyebaran yang ditimbulkan dan memudahkan bagi personel teknis dan nonteknis untuk menentukan upaya mitigasi penyebaran *malware*.

Ransomware El Paco memiliki nilai 74 dari formula perhitungan Potential Payload (dampak *payload* pada target), Proliferation Potential (potensi penyebaran *malicious file*), dan Hostility Level (motif pelaku). Dengan nilai tersebut, *ransomware* El Paco termasuk ke dalam kategori **EXTREME.**

Sumber: The *Malware* Rating System (MRS) by Robert J. Bagnall and Geoffrey French

B. DESKRIPSI

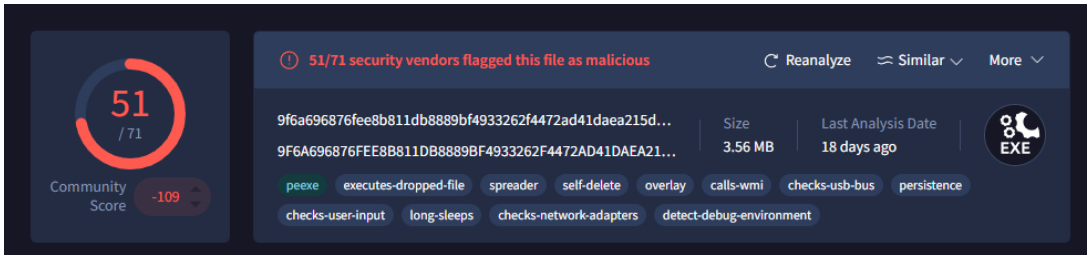
1. Serangan *ransomware* El Paco berawal dari adanya kerentanan pada *Remote Desktop Protocol* (RDP) sistem elektronik. Penyerang diduga melakukan serangan *brute force* untuk mengeksploitasi kerentanan RDP pada sistem dan meningkatkan kemampuan hak akses sehingga dapat menginjeksi *malware* pada sistem elektronik yang menjadi target. Akibat serangan ini, sistem elektronik korban menjadi tidak dapat diakses.
2. Tim Analisis Malware – Direktorat Operasi Keamanan Siber melakukan analisis *file Ransomware* El Paco dan *dropfile* yang berkaitan dari sumber terbuka. Tim Analisis Malware memperoleh file *malware* dengan *signature hash* MD5 dengan nilai 33eeeb25f834e0b180f960ecb9518ea0.
3. El Paco termasuk dalam klasifikasi *ransomware* yang diduga merupakan turunan dari *family ransomware* Mimic. El Paco menyediakan *Graphical User Interface* (GUI) sehingga memudahkan penyerang untuk melakukan konfigurasi jangkauan enkripsi, *ransomnote*, dan hal lain yang dibutuhkan pada sistem elektronik target.
4. *Ransomware* El Paco terindikasi menggunakan algoritma kriptografi *Stream Cipher* ChaCha20 yang dikombinasikan dengan algoritma Message Authentication Code (MAC) Poly1305.

Gambar 1 menunjukkan Diagram 5W1H yang menggambarkan profil dari *Ransomware* El Paco:

Gambar 1. Diagram 5W1H *Malware* Ransom:Win32/Mimic.MA!MTB

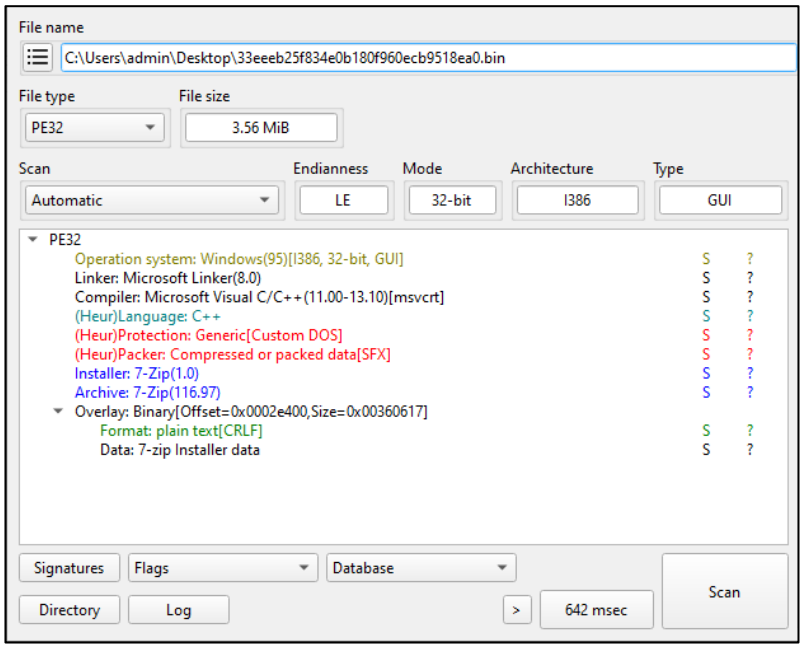
C. ANALISIS STATIS

1. Informasi *malware*



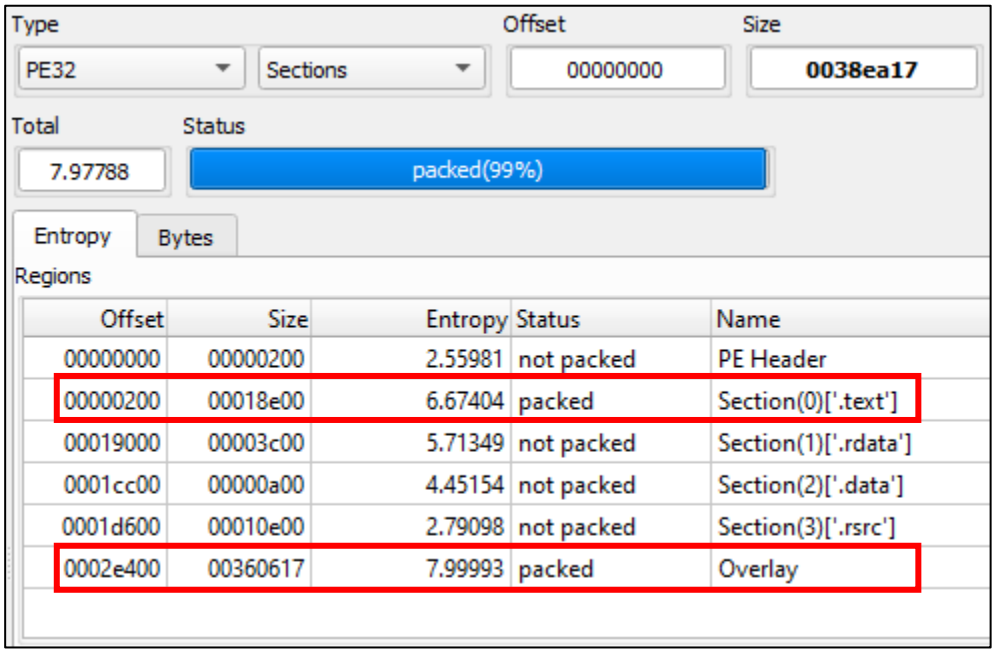
Gambar 2. Hasil pemindaian pada VirusTotal

Malware El Paco yang didapatkan dari sumber terbuka memiliki *signature* dengan nilai *hash* MD5 33eeeb25f834e0b180f960ecb9518ea0. *Malware* tersebut mendapatkan reputasi *malicious* 51 dari 71 dari vendor keamanan. *Malware* El Paco tergolong sebagai *ransomware* dengan penamaan yang diberikan Microsoft sebagai Ransom:Win32/Mimic.MA!MTB.



Gambar 3. Proses identifikasi Ransomware El Paco

Malware El Paco diidentifikasi sebagai *file Portable Execution* 32-bit (PE32) dan teridentifikasi sebagai *installer* aplikasi sumber terbuka 7-Zip. Aplikasi 7-Zip berfungsi sebagai alat pengarsipan *file*. *Malware* El Paco memiliki ukuran *file* sebesar 3,56 MB dan terindikasi dibuat menggunakan bahasa pemrograman C++ sebagaimana ditunjukkan pada Gambar 3.

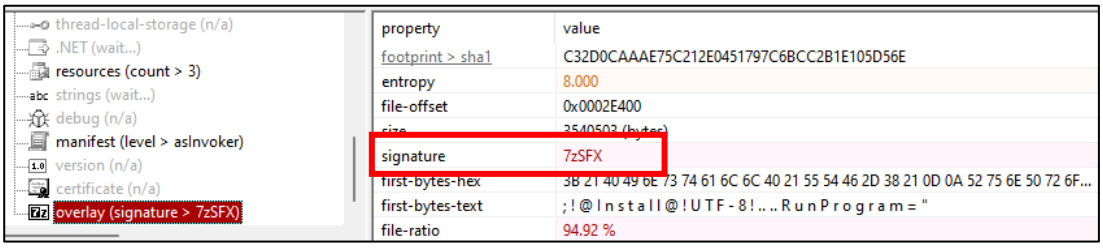


Gambar 4. Nilai entropi Ransomware El Paco

Malware El Paco memiliki nilai entropi sebesar 7,97788. Nilai entropi tersebut menunjukkan bahwa *malware* tersebut dalam kondisi *packed*. Suatu indikasi *malware* dibuat agar dalam kondisi *packed* bertujuan untuk:

a. Menghindari deteksi antivirus;
b. Menyembunyikan kode berbahaya;
c. Mempersulit proses analisis;
d. Mengecilkan ukuran *file*;
e. Meningkatkan persistensi dan polimorfisme. Polimorfisme adalah kemampuan untuk menghasilkan varian *malware* yang berbeda setiap kali dijalankan.

Apabila kita lakukan pengecekan nilai entropi setiap bagian (*section*) dari *malware* El Paco maka dapat diketahui pada bagian ".text" dan bagian "Overlay" memiliki nilai entropi lebih dari 6,5 (nilai entropi minimal suatu aplikasi dapat dikategorikan *packed*). Pada bagian ".text" memiliki nilai entropi sebesar 6,67404, sedangkan bagian "Overlay" memiliki nilai 7,99993 mendekati nilai maksimal yaitu 8 (delapan). Berdasarkan practicalsecurityanalytics.com disebutkan rentang wajar nilai entropi suatu aplikasi adalah 4,8 s.d. 7,2. Apabila nilai entropi suatu aplikasi lebih dari 7,2 maka dapat dikategorikan sebagai aplikasi berbahaya. Data statistik menunjukkan, sekitar 55% dari semua sampel aplikasi berbahaya memiliki entropi 7,2 atau lebih dibandingkan 8% sampel aplikasi normal.



Gambar 5. Signature pada bagian “Overlay”

Bagian “Overlay” memiliki *signature* sebagai 7-Zip SFX (*Self Extracting Archive*). Informasi tersebut yang mengindikasikan bahwa *malware* El Paco di-*packed* dengan menggunakan alat 7-Zip dan dapat melakukan ekstraksi otomatis tanpa harus mendapatkan perintah dari manusia. Hal ini juga diperkuat melalui temuan SFX *script* pada salah satu baris string di bagian “Overlay” sebagaimana ditunjukkan pada Gambar 6.

Overlay	1e	A	RunProgram="hidcon:7za.exe i "
Overlay	44	A	RunProgram="hidcon:7za.exe x -y -p7183204373585782 Everything64.dll"
Overlay	38	A	RunProgram="hidcon:\"ELPACO-team.exe\" %SfxVarCmdLine0%"

Gambar 6. String “Overlay” berisi SFX *script*

Script pertama yaitu `RunProgram=”hidcon:7za.exe i”` bertujuan untuk menjalankan fungsi ekstraksi pada *file* malware El Paco dengan menghiraukan nama file *malware* yang tersimpan pada perangkat terinfeksi. Hasil ekstraksi adalah beberapa file salah satunya *file* "Everything64.dll". *Script* kedua `RunProgram=”hidcon:7za.exe x -y -p7183204373585782 Everything64.dll”` bertujuan untuk menjalankan fungsi ekstraksi pada *file* Everything64.dll secara tersembunyi dengan parameter yang bertujuan untuk menyetujui semua *prompt* yang mungkin muncul dan menggunakan *password* 7183204373585782. Hasil dari proses *script* kedua adalah beberapa *file* yang salah satunya adalah “ELPACO-team.exe”. Penjelasan terkait hal ini akan disampaikan lebih mendetail dalam analisis dinamis.

Malware El Paco memiliki informasi waktu pembuatan pada tanggal 31 Desember 2012 pukul 00.38.51 UTC. Informasi ini tidak dapat dikatakan valid karena sangat memungkinkan untuk pembuat *malware* memanipulasi informasi waktu pembuatan dengan tujuan untuk menyamarkan umur *malware*.

Di bawah ini terdapat Tabel 1 yang berisi rangkuman yang berkaitan dengan informasi *malware* El Paco sebagai berikut:

Tabel 1. Identifikasi *Malware*

Parameter	Rincian
Nilai MD5	33eeeb25f834e0b180f960ecb9518ea0
Nilai SHA 1	61f73e692e9549ad8bc9b965e25d2da683d56dc1
Nilai SHA-256	9f6a696876fee8b811db8889bf4933262f4472ad41daea215d2e39bd537cf32f
Jenis	*Ransomware*
Ukuran *File*	3.56 MB (3729943 bytes)
Nilai Entropi	7,97788
File Packed	*Packed*
Packer	7zip
Waktu Pembuatan	2012-12-31 00:38:51 UTC
PE Imphash	f6baa5eaa8231d4fe8e922a2e6d240ea

2. *Import Address Table*

Import Address Table (IAT) adalah tabel yang menunjukkan daftar fungsi yang dipanggil dalam sistem operasi Windows. Dari tabel tersebut juga menunjukkan *dynamic-link libraries* (DLLs) yang diimpor dari pemanggilan fungsi tersebut. Berikut ini merupakan IAT dari *malware* El Paco:

Tabel 2. *Import Address Table*

No.	Nama Fungsi	*Library* (DLL)
1	GetWindowTextW	USER32.dll
2	FreeSid	ADVAPI32.dll
3	AllocateAndInitializeSid	ADVAPI32.dll
4	CheckTokenMembership	ADVAPI32.dll
5	CopyImage	USER32.dll
6	GetEnvironmentVariableW	KERNEL32.dll
7	VirtualAlloc	KERNEL32.dll
8	GlobalMemoryStatusEx	KERNEL32.dll
9	GetKeyState	USER32.dll
10	UnhookWindowsHookEx	USER32.dll
11	CallNextHookEx	USER32.dll
12	SetWindowsHookExW	USER32.dll
13	SHGetPathFromIDListW	SHELL32.dll
14	SHBrowseForFolderW	SHELL32.dll
15	SHGetFileInfoW	SHELL32.dll
16	FindFirstFileW	KERNEL32.dll
17	DeleteFileW	KERNEL32.dll
18	FindNextFileW	KERNEL32.dll

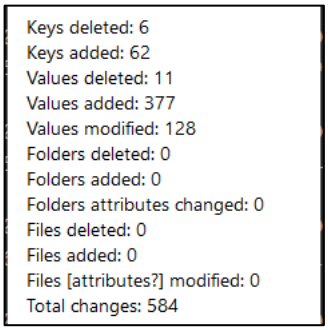
19	RemoveDirectoryW	KERNEL32.dll
20	SetFileAttributesW	KERNEL32.dll
21	WriteFile	KERNEL32.dll
22	ShellExecuteW	SHELL32.dll
23	ShellExecuteExW	SHELL32.dll
24	GetCurrentThreadId	KERNEL32.dll
25	SuspendThread	KERNEL32.dll
26	GetCurrentProcess	KERNEL32.dll
27	CreateProcessW	KERNEL32.dll
28	GetExitCodeProcess	KERNEL32.dll
29	SetEnvironmentVariableW	KERNEL32.dll
30	SystemParametersInfoW	USER32.dll
31	SetCurrentDirectoryW	KERNEL32.dll
32	SetThreadLocale	KERNEL32.dll

D. ANALISIS DINAMIS

Analisis dinamis dilakukan melalui eksekusi *malware* pada *environment* dengan spesifikasi sistem operasi Windows 10 versi 64-bit berbasis *virtual machine* dan sistem *sandbox.* Berikut merupakan beberapa hasil analisis dinamis yang didapatkan:

1. *Registry*

   Malware El Paco melakukan modifikasi *registry* pada perangkat terinfeksi dengan total perubahan sebanya 584 *registry* dengan rincian sebagaimana ditunjukkan pada Gambar 7.



Gambar 7. Informasi *registry* yang dimodifikasi oleh *Malware* El Paco

2. *File*

   Malware El Paco melakukan *dropping file* secara bertahap. Adapun *file* yang di-*drop* oleh *malware* El Paco disebutkan pada Tabel 3 dan Tabel 4.

Tabel 3. Tahap pertama *dropping file malware* El Paco

Tahap 1			
Sumber File	**Ukuran File**	**MD5**	**Reputasi VirusTotal**
paco.exe	3,56 MB	33eeeb25f834e0b180f960ecb9518ea0	51/71
Dropped File	**Ukuran File**	**MD5**	
7za.exe	773 KB	b93eb0a48c91a53bda6a1a074a4b431e	1/72
Everything.exe	1,7 MB	c44487ce1827ce26ac4699432d15b42a	0/72
Everything32.dll	85 KB	3b03324537327811bbbaff4aafa4d75b	0/72
Everything64.dll	2,59 MB	245fb739c4cb3c944c11ef43cddd8d57	0/72

Tabel 4. Tahap kedua *dropping file malware* El Paco

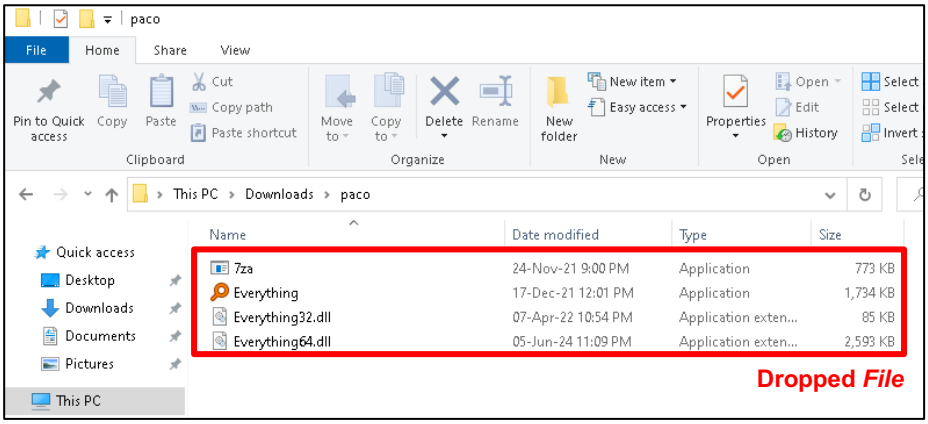
Tahap 2			
Sumber File	**Ukuran File**	**MD5**	**Reputasi VirusTotal**
Everything64.dll	2,59 MB	245fb739c4cb3c944c11ef43cddd8d57	0/72
Dropped File	**Ukuran FIle**	**MD5**	**Reputasi VirusTotal**
DC.exe	803 KB	ac34ba84a5054cd701efad5dd14645c9	45/72
ELPACO-team.exe	2,4 MB	b951e50264f9c5244592dfb0a859ec41	61/72
ENC_default_default_2023-12-27_09-27-40=Telegram@datadecrypt.exe	2,4 MB	0bf7c0d8e3e02a6b879efab5deab013c	60/76
Everything.ini	1 KB	742c2400f2de964d0cce4a8dabadd708	0/62
Everything2.ini	1 KB	51014c0c06acdd80f9ae4469e7d30a9e	0/63
global_options.ini	1 KB	26f59bb93f02d5a65538981bbc2da9cc	Not found
gui35.exe	277 KB	03a63c096b9757439264b57e4fdf49d1	58/72
gui40.exe	277 KB	57850a4490a6afd1ef682eb93ea45e65	59/71
xdel.exe	351 KB	803df907d936e08fbbd06020c411be93	0/75

Dari tabel tersebut menunjukkan metode pengarsipan yang dilakukan pembuat *malware* untuk menghindari deteksi antivirus dapat dikatakan

berhasil. Hal ini ditunjukkan dari reputasi *malicious file* Everything64.dll yang mendapatkan 0/72 padahal di dalam *file* Everything64.dll tersebut terdapat *file* lain yang memiliki reputasi *malicious* yang tinggi.

3. Proses Analisis *behaviour*

Berdasarkan dari hasil analisis statis, diketahui bahwa *malware* El Paco memiliki kemampuan SFX atau kemampuan untuk mengektrasi *file* secara otomatis. Adapun *script* yang digunakan adalah *script* untuk mengoperasikan aplikasi 7-Zip. Tim mencoba melakukan ekstraksi pada bagian "Overlay" Secara manual menggunakan alat 7-Zip sehingga didapatkan hasil sebagai ditunjukkan pada Gambar 7.

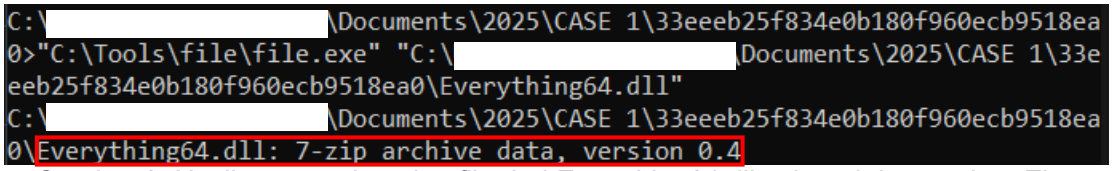


Gambar 8. Hasil ekstraksi *malware* El Paco

Hasil ekstraksi menunjukkan adanya 4 (empat) *file* yang dibuat oleh malware dengan rincian sebagai berikut:

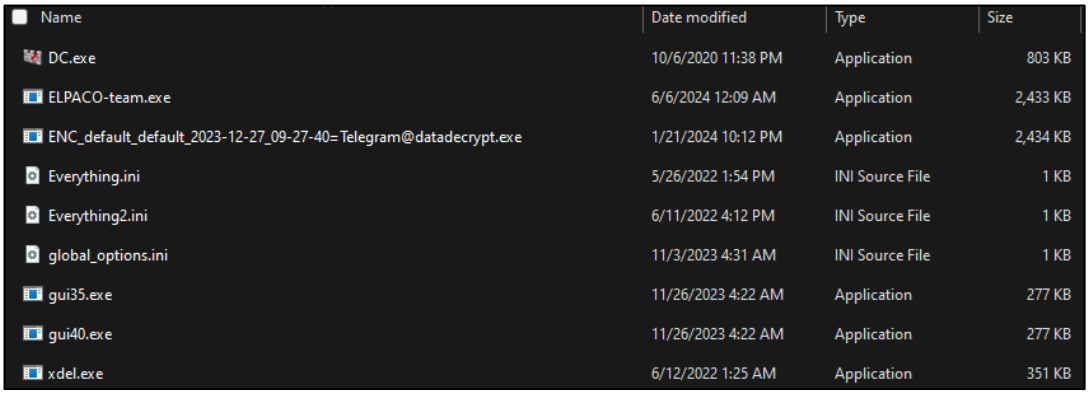
a. 7za, sebuah aplikasi pengarsipan dari sumber terbuka dari 7-Zip yang dapat digunakan untuk mengarsipkan dan ekstraksi dari *file* yang telah diarsipkan. Aplikasi ini adalah aplikasi *legitimate* yang bisa didapatkan dari www.7-zip.org;
b. Everything, sebuah aplikasi *legitimate* dari VoidTool yang berfungsi untuk melakukan pencarian *file* di lingkungan Windows tanpa harus membebani memori komputer. Aplikasi ini dapat diperoleh dari www.voidtools.com;
c. Everything32.dll diduga merupakan *library legitimate* yang dibutuhkan oleh aplikasi Everything.exe; dan
d. Hasil pengecekan tipe *file* dari Everything64.dll menunjukkan bahwa Everything64.dll terdeteksi sebagai data arsip 7-Zip sebagaimana

ditunjukkan pada Gambar 9. Hal ini juga dilengkapi dengan temuan string pada *malware* El Paco yang menjalankan SFX *script* `RunProgram="hidcon:7za.exe x -y -p7183204373585782 Everything64.dll"` sebagaimana ditunjukkan pada Gambar 6.



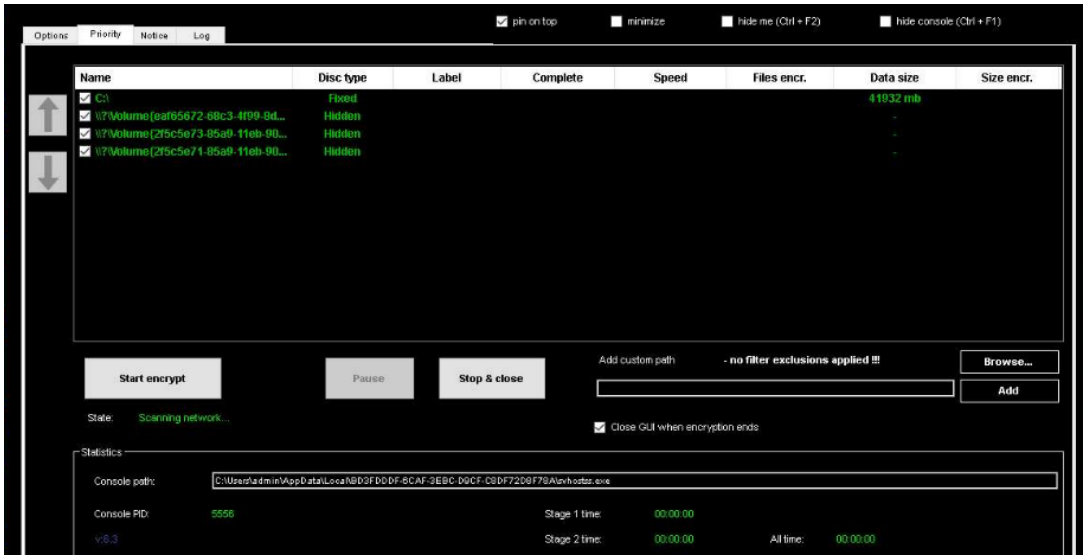
Gambar 9. Hasil pengecekan tipe file dari Everything64.dll sebagai data arsip 7-Zip

Dari hasil temuan terhadap *file* Everything64.dll, Tim melakukan ekstraksi *file* Everything64.dll menggunakan aplikasi 7-Zip dengan sebuah *password* yang didapatkan dari analisis string dan mendapatkan hasil sebagai berikut:



Gambar 10. Hasil Ekstraksi *file* Everything64.dll

Selanjutnya Tim mencoba menjalankan *malware* dan menemukan bahwa *malware* tersebut menampilkan GUI *console* dengan tampilan awal sebagai berikut:



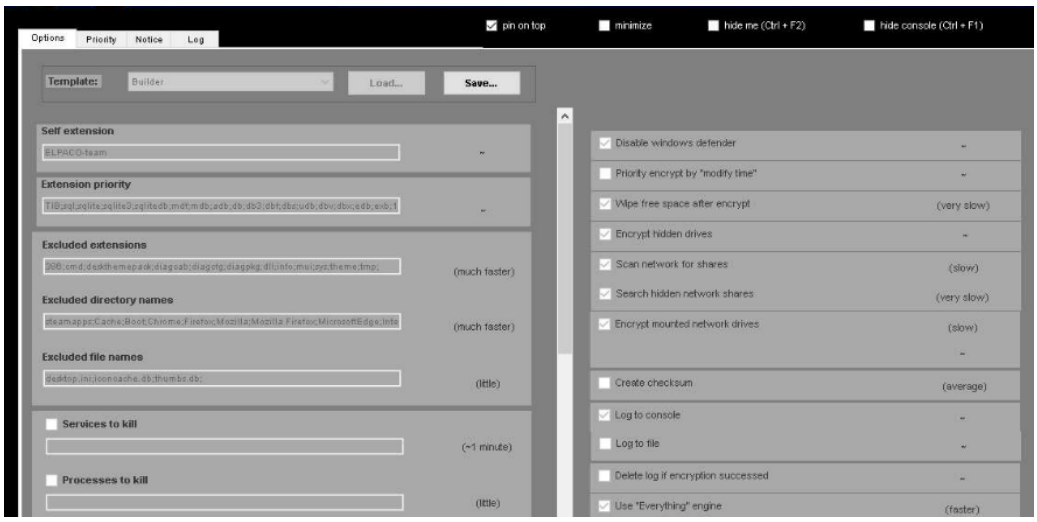
Gambar 11. GUI *console malware* El Paco

GUI dari *malware* El Paco memiliki beberapa Tab yang dapat diakses yaitu:

a. Options

Tab ini merupakan pengaturan yang dapat dikonfigurasikan oleh penyerang sebelum melakukan enkripsi pada sistem. Beberapa pengaturan penting yang menjadi perhatian yaitu penyerang dapat melakukan:

1) penyesuaian ekstensi file terenkripsi;
2) mematikan Windows Defender;
3) menghapus log setelah enkripsi selesai;
4) pengecualian enkripsi pada *file* atau direktori tertentu;
5) mematikan jenis *Services* dan *Process* sebelum menjalankan enkripsi pada sistem korban.

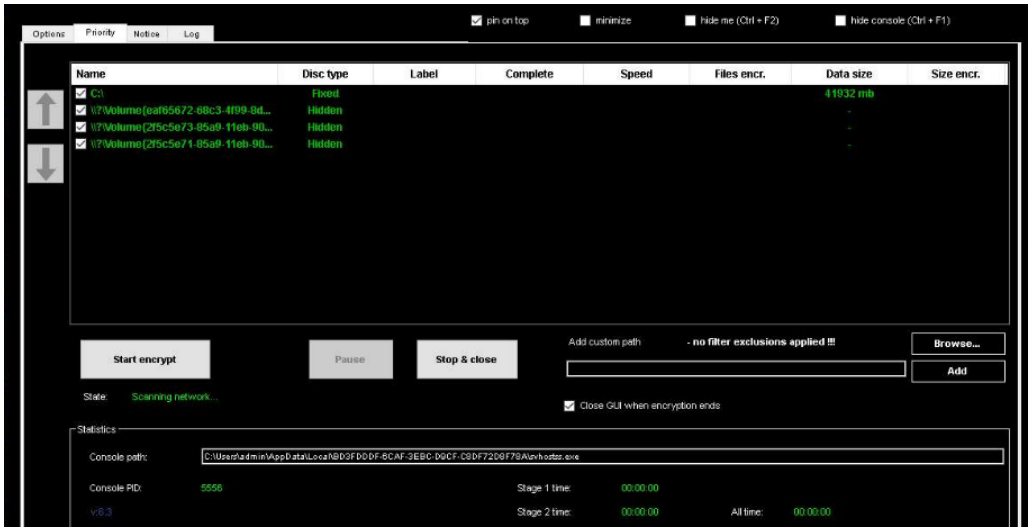


Gambar 12. Tab Options pada GUI *Ransomware* ELPaco

b. Priority

Tap Priority merupakan Tab yang berfungsi untuk mengendalikan *behavior ransomware*. Penyerang dapat melakukan untuk:

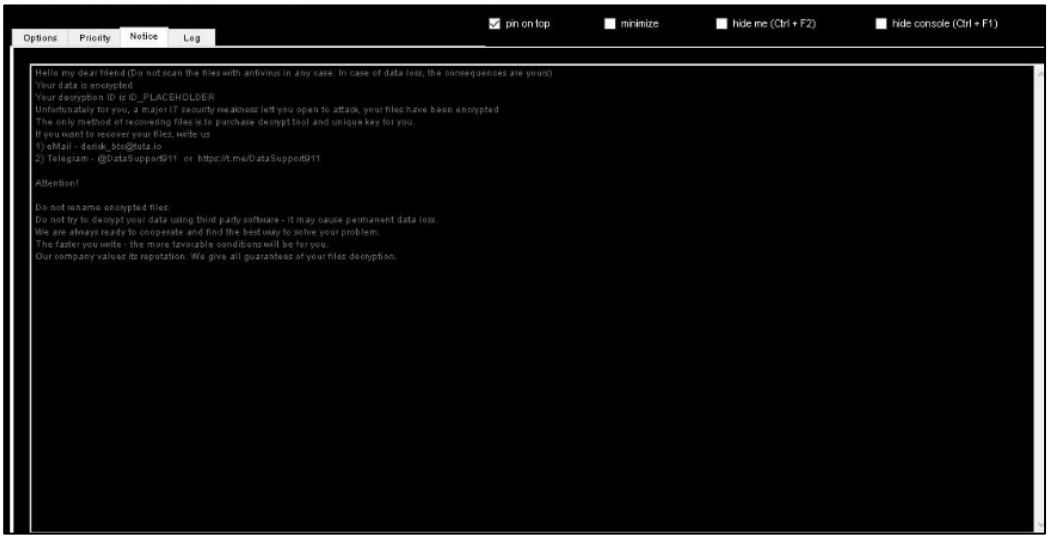
1) memulai dan mengakhiri proses enkripsi pada sistem korban;
2) melihat PID dari proses enkripsi;
3) memilih mempertahankan GUI atau menutupnya setelah proses enkripsi selesai;
4) kustomisasi alamat folder yang dikecualikan dari proses enkripsi.



Gambar 13. Tab Priority pada GUI *Ransomware* ELPaco

c. Notice

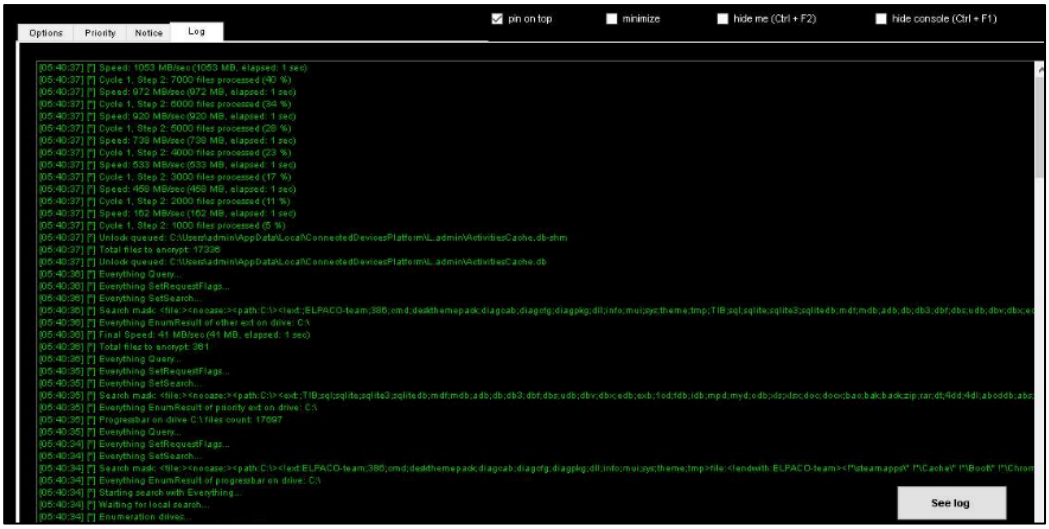
Tab Notice merupakan Tab dimana penyerang dapat melakukan penyesuaian dari *ransomnote* yang akan diterima korban setelah proses enkripsi selesai dilakukan.



Gambar 14. Tab Notice pada GUI *Ransomware* ELPaco

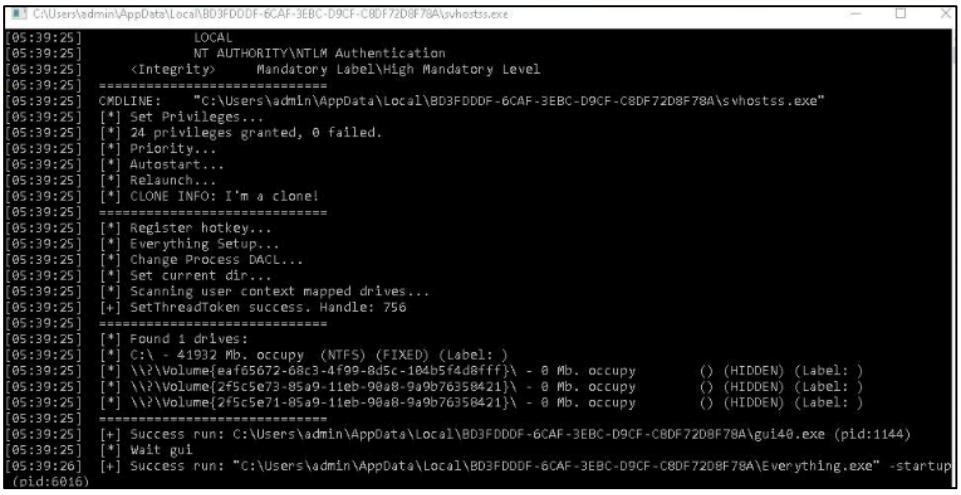
d. Log

Tab log merupakan catatan aktivitas yang dilakukan sejak *malware* dijalankan. Pada Tab ini juga disediakan tombol untuk menyimpan log. Pada Option, penyerang dapat memilih untuk dilakukan penghapusan log atau tidak setelah proses enkripsi selesai.

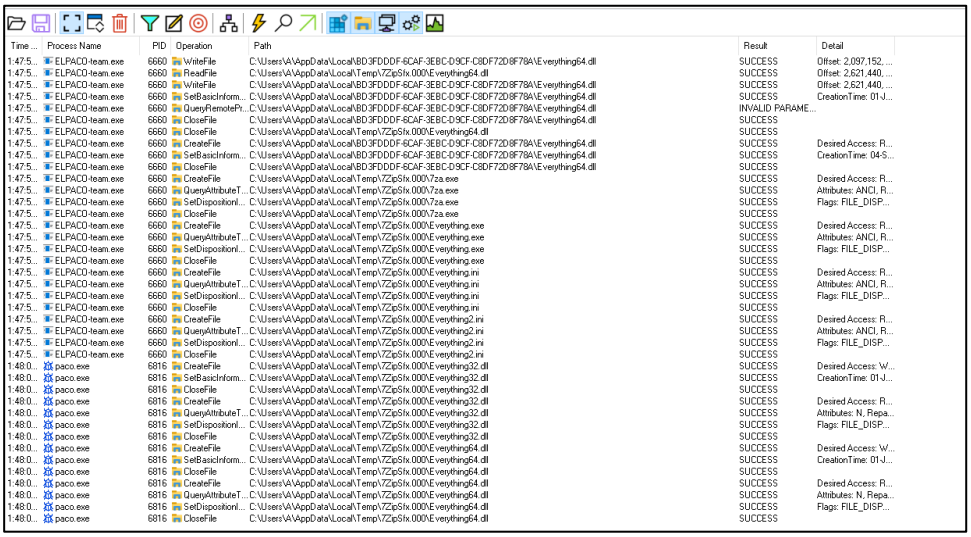


Gambar 15. Tab Log pada GUI *Ransomware* ELPaco

Setelah mendapatkan GUI dari *malware* El Paco, Tim selanjutnya melakukan percobaan enkripsi pada lingkungan tersiolasi. Proses enkripsi berjalan sebagai berikut:

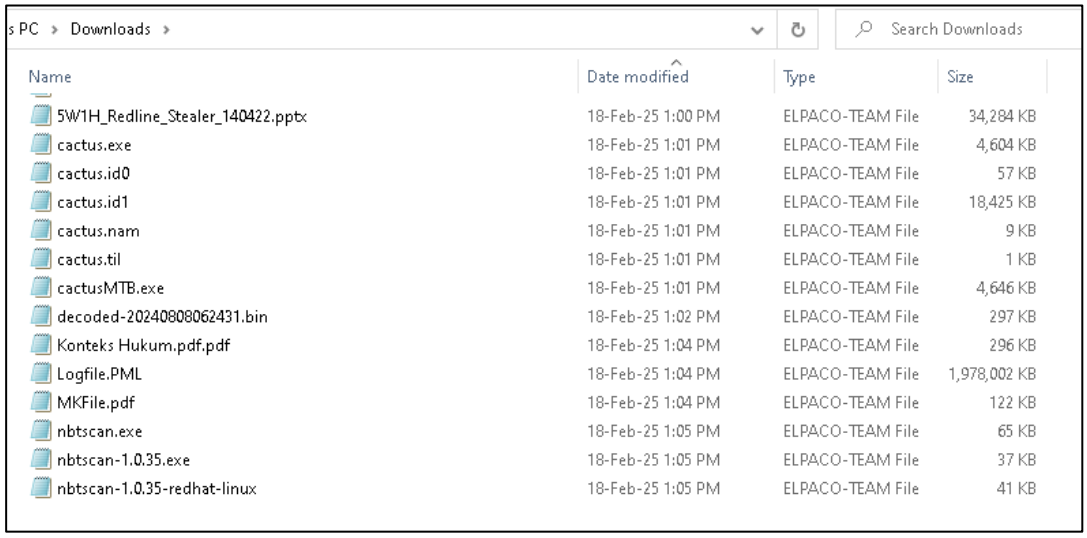


Gambar 16. Proses Enkripsi pada Terminal



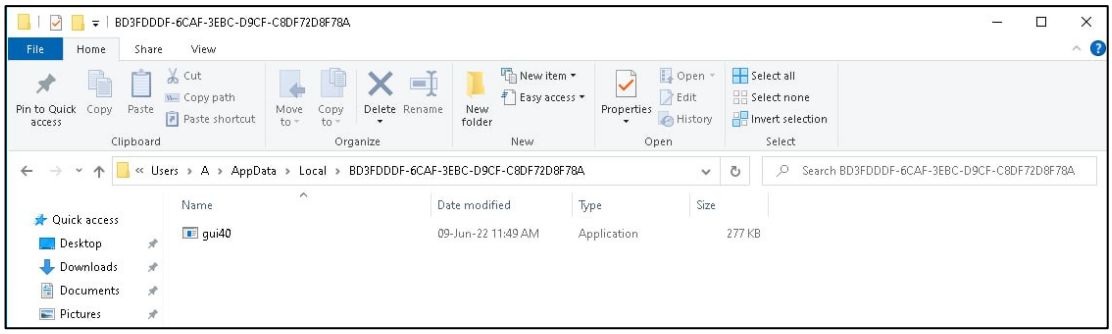
Gambar 17. Proses Enkripsi pada *Tool* Process Monitoring (ProcMon)

Setelah enkripsi berhasil dijalankan, dapat dilihat bahwa semua *file* di dalam sistem terenkripsi dan berubah tipe *file*-nya dan tidak dapat dibuka.

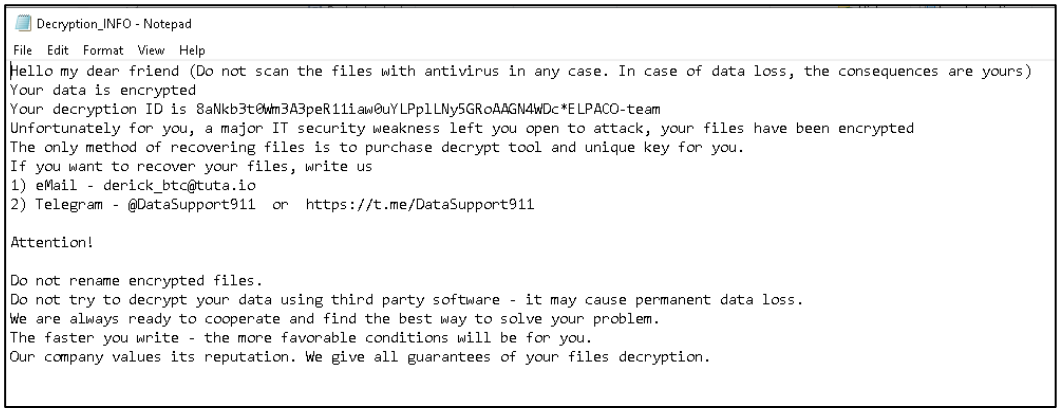


Gambar 18. Hasil Enkripsi *Ransomware* ELPaco

Selain itu, diketahui bahwa setelah enkripsi dijalankan, maka *ransomware* akan melakukan *dropping file* pada direktori C:\Users\A\AppData\Local\BD3FDDDF-6CAF-3EBC-D9CF-C8DF72D8F78A dan menghasilkan sebuah *ransomnote* yang sesuai dengan pengaturan yang dilakukan pada Tab Notice.



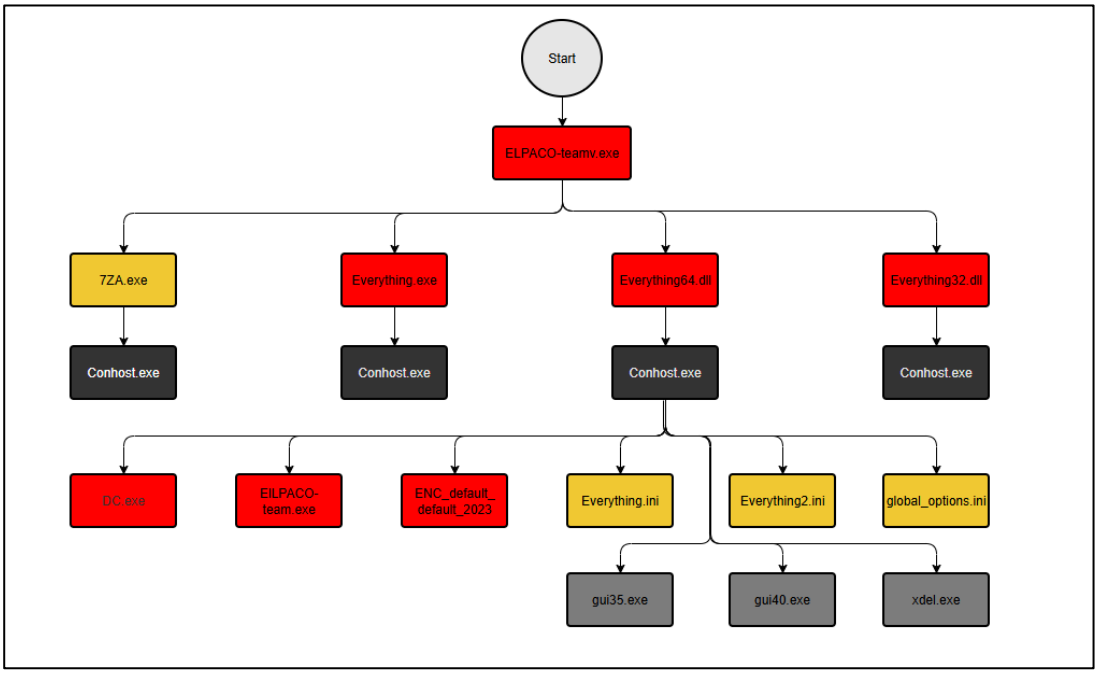
Gambar 19. *Dropping File Ransomware* El Paco



Gambar 20. *Ransomnote Ransomware* El Paco

2. *Process Tree*

Process tree (pohon proses) adalah representasi hierarkis dari semua proses ketika suatu aplikasi dijalankan. Ini menunjukkan hubungan antara proses induk (*parent process*) dan anak (*child process*), termasuk bagaimana suatu proses dibuat, eksekusi file, atau pemanggilan program lain. Berdasarkan analisis dinamis yang telah dilakukan, Tim Analisis Malware melakukan visualisasi proses *malware* El Paco yang didapatkan dari sumber terbuka. Di bawah ini merupakan gambar dari *process tree* yang telah dibuat:



Gambar 17. *Process Tree Ransomware* El Paco

a. Eksekusi Utama

- ELPACO-teamv.exe berperan sebagai *loader/dropper* yang memiliki SFX *script* sehingga ELPACO-teamv.exe dapat melakukan ekstraksi file tanpa harus berinteraksi dengan pengguna.
- Setelah dijalankan, ELPACO-teamv.exe akan menjalankan 7Za.exe dan Everything.exe dengan menggunakan Library Everything32.dll.

b. Eksekusi Sekunder

- 7ZA.exe digunakan untuk mengekstrak arsip pada file Everything64.dll yang berisi *file* lain yang dibutuhkan *malware*. Proses ini memungkinkan dilakukannya eksekusi perintah pada latar belakang tanpa menampilkan jendela CMD.

- Everything.exe digunakan sebagai alat pencarian cepat yang kemungkinan digunakan oleh *malware* untuk mencari file target yang akan dienkripsi.
- Everything32.dll dan Everything64.dll merupakan dua versi *library* yang digunakan untuk memastikan pencarian file berjalan di sistem 32-bit dan 64-bit.
- Everything64.dll idealnya merupakan *library* yang digunakan untuk memastikan aplikasi dapat berjalan di sistem operasi yang berbasis 64-bit. Namun, pada analisis *malware* El Paco ditemukan adanya ukuran *file* yang berbeda jauh dengan *library* Everything32.dll dan diketahui adanya bagian "Overlay" yang dapat diekstraksi untuk menghasilkan *file* yang sebagaimana ditunjukkan pada Gambar 10.
- Everything.ini dan Everything2.ini adalah *file* ini diduga berisi konfigurasi lanjutan untuk melakukan pencarian file target.
- global_options.ini file ini diduga berisi konfigurasi tambahan dalam aplikasi.
- ELPACO-team.exe dan ENC_default_default_2023-12-27_09-27-40=Telegram@datadecrypt.exe diduga sebagai *file* enkriptor pada *ransomware* El Paco.
- gui35.exe & gui40.exe aplikasi ini digunakan sebagai antarmuka untuk operator *ransomware*.
- xdel.exe aplikasi ini digunakan untuk menghapus artefak *file* dari *ransomware* yang telah dijalankan.

E. ANALISIS JARINGAN

Berdasarkan analisis jaringan yang telah dilakukan, *malware* El Paco tidak melakukan percobaan untuk komunikasi ke *Command and Control* (C2) *malware*. Namun ditemukan adanya aktivitas jaringan dalam bentuk pemindaian perangkat yang terhubung dalam jaringan yang sama.

No.	Time	Source	Destination	Protocol	Length	Info
3117	70.823207	VMware_ba:7e:2b	Broadcast	ARP	42	Who has 192.168.138.179? Tell 192.168.138.128
3118	70.823322	VMware_ba:7e:2b	Broadcast	ARP	42	Who has 192.168.138.180? Tell 192.168.138.128
3119	70.823491	VMware_ba:7e:2b	Broadcast	ARP	42	Who has 192.168.138.181? Tell 192.168.138.128
3120	70.823697	VMware_ba:7e:2b	Broadcast	ARP	42	Who has 192.168.138.190? Tell 192.168.138.128
3121	70.823822	VMware_ba:7e:2b	Broadcast	ARP	42	Who has 192.168.138.191? Tell 192.168.138.128
3122	70.828184	VMware_ba:7e:2b	Broadcast	ARP	42	Who has 192.168.138.198? Tell 192.168.138.128
3123	70.828507	VMware_ba:7e:2b	Broadcast	ARP	42	Who has 192.168.138.199? Tell 192.168.138.128

Gambar 21. Aktivitas jaringan yang dilakukan *malware* El Paco

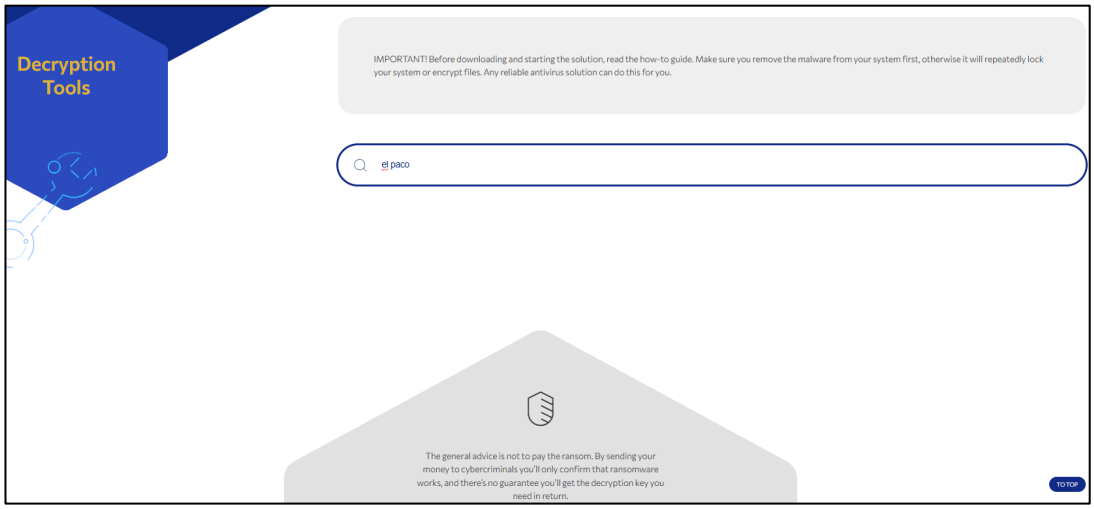
F. INFORMASI TAMBAHAN

Ransomware El Paco terindikasi menggunakan algoritma kriptografi *Stream Cipher* ChaCha20 yang dikombinasikan dengan algortima Message Authentication Code (MAC) Poly1305. Hal ini diketahui dari analisis string pada file ELPACO-team.exe dan ENC_default_default_2023-12-27_09-27-40=Telegram@datadecrypt.exe.

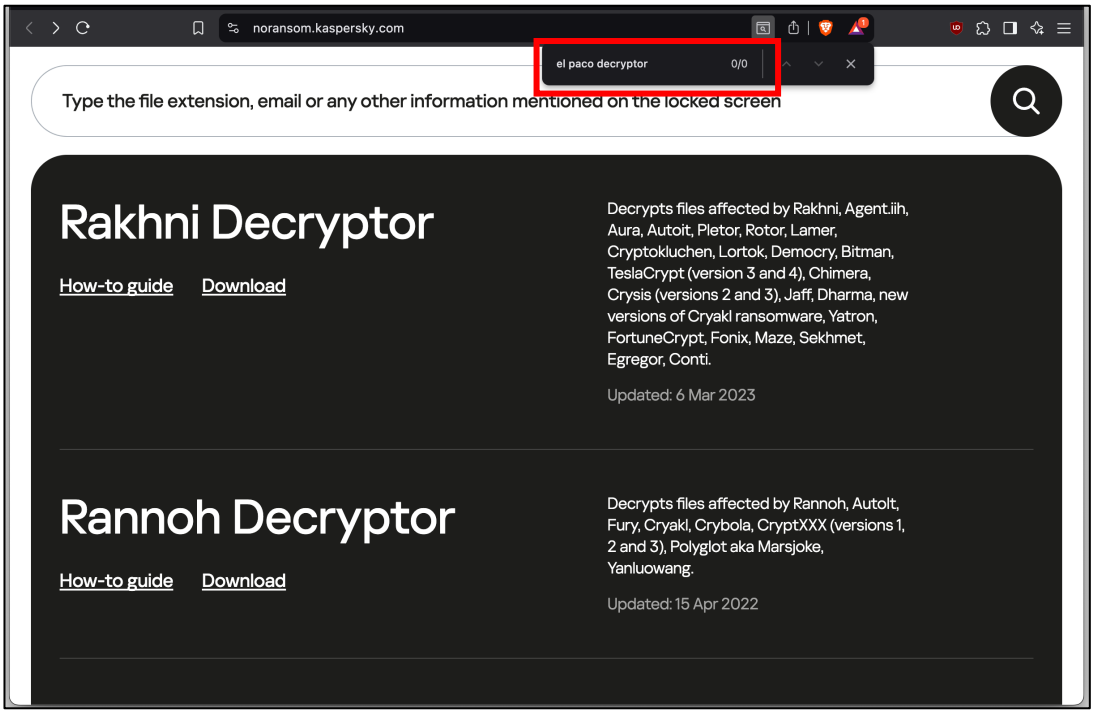
Address	String
0x00401dc0	ChaCha20 for x86, CRYPTOGAMS by <appro@openssl.org>
0x005809e0	crypto\\evp\\e_chacha20_poly1305.c
0x005949e4	ChaCha20-Poly1305
0x005949f8	chacha20-poly1305
0x00594a0c	ChaCha20
0x00594a18	chacha20
0x005b9e38	chacha20_poly1305_ctrl

Gambar 22. Temuan string terkait algoritma kriptografi pada ransomware El Paco

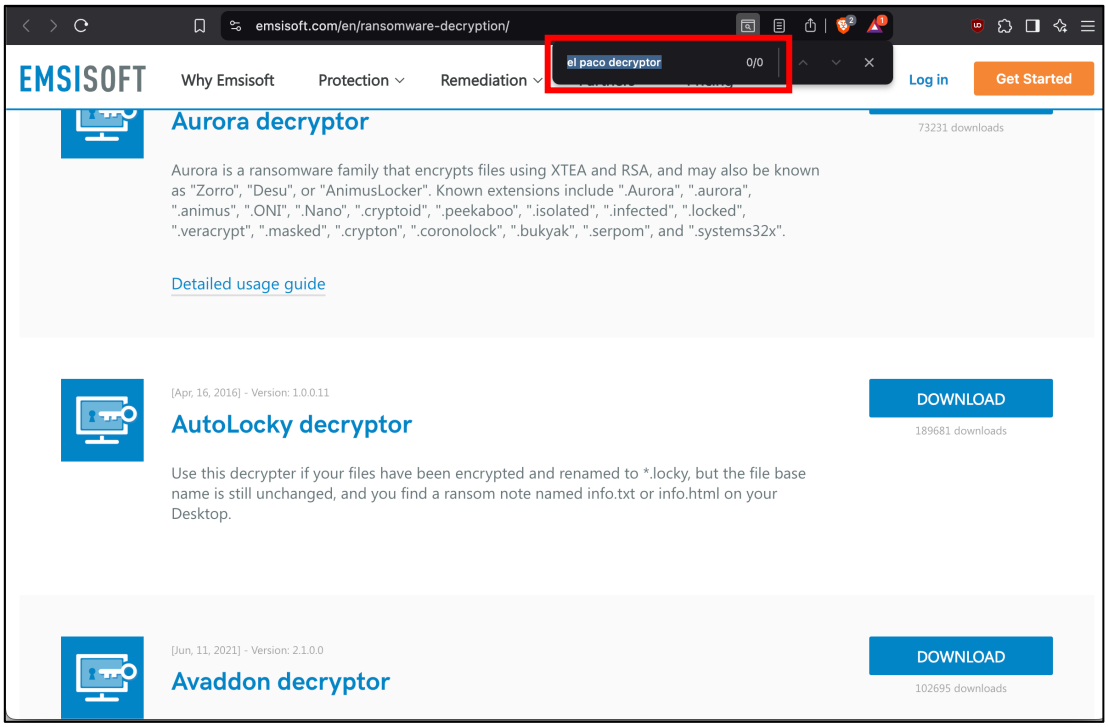
Tim Analisis Malware juga mencoba melakukan penelusuran dekriptor *ransomware* El Paco pada beberapa sumber terbuka namun dekriptor dari *ransomware* El Paco belum tersedia.



Gambar 23. Penelusuran dekriptor *ransomware* El Paco di nomoreransom.org



Gambar 24. Penelusuran dekriptor *ransomware* El Paco di noransom.kaspersky.com



Gambar 25. Penelusuran dekriptor *ransomware* El Paco di emsisoft.com

G. REKOMENDASI

Dalam rangka mengantisipasi penyebaran *malware* Ransom:Win32/Mimic.MA!MTB, berikut rekomendasi yang dapat dilakukan:

1. Menggunakan *firewall* untuk memblokir semua koneksi masuk ke layanan yang seharusnya tidak tersedia untuk umum, yang secara *default* menolak semua koneksi yang masuk dan hanya mengizinkan layanan yang digunakan;
2. Menggunakan keamanan jaringan dan akses berlapis serta menutup *port* yang tidak digunakan;
3. Melakukan *update* pada *Operating System*, Aplikasi/*Software*, *Firmware* dan *Browser* secara berkala untuk meningkatkan keamanan komputer dari kerawanan yang ada;
4. Menggunakan *antivirus* dan perangkat *security* yang *update* dan lakukan *scanning* antivirus baik terhadap *storage* dan *memory* secara berkala;
5. Mematikan fitur *file sharing* jika tidak diperlukan, dan gunakan proteksi kata sandi untuk membatasi akses;
6. Menghindari membuka atau menelusuri situs atau halaman yang tidak jelas dan memiliki reputasi buruk seperti situs bajakan, *keygen*, situs pornografi, dan sebagainya;
7. Melakukan *filtering* terhadap alamat IP, domain yang masuk dalam daftar *blacklist* yang terindikasi adanya serangan dan infeksi *malware*.
8. Menghindari menggunakan atau mengunduh aplikasi atau jenis program lainnya yang merupakan hasil *crack* (bajakan);
9. Melakukan pengubahan *password* dari akun-akun kredensial yang dimiliki secara berkala.

Lampiran 1. *Malware Rating System*

RATING MALWARE EL PACO

Tabel 5. Kriteria *Malware Rating*

Kriteria	Deskripsi
Payload potential	Potensi *malicious file* untuk menurunkan fungsi atau merusak target
Proliferation potential	Tingkat penyebaran *malicious file*
Hostility level	Niat dan tujuan dari *malicious file* (contoh: merusak, mengganggu, spionase)

Tabel 6. Ambang Batas Yang Diusulkan Untuk Menentukan *Rating Payload*

Rating	Deskripsi	*Malware*
10	*Polymorphic - patch immune*, atau sebelumnya tidak terdefinisi	-
9	Menghapus *file-file* penting, menginfeksi jaringan; dapat merusak jaringan dengan kapasitas *bandwidth* yang melimpah	-
8	Menghapus, memodifikasi, atau menimpa *file-file* penting dan menginfeksi jaringan	*Ransomware* El Paco
7	Memodifikasi atau menimpa *file* yang tidak penting, menginfeksi jaringan; dapat merusak jaringan dengan kapasitas *bandwidth* yang melimpah	-
6	Menghapus *file* yang tidak penting, menginfeksi jaringan	-
5	Menghapus *file* yang tidak penting	-
4	Dapat merusak jaringan dengan kapasitas *bandwidth* yang melimpah	-
3	Menginfeksi *file-file* penting	-
2	Menginfeksi *file* yang tidak penting	-
1	Tidak ada dampak berkelanjutan (hanya replikasi diri)	-

Tabel 7. Usulan Ambang Batas Untuk Menentukan *Proliferation Rating*

Rating	Deskripsi	*Malware*
10	Penyebaran dalam jaringan (via email, IRC, HTML, dll), tidak memerlukan lampiran dibuka untuk direplikasi; bukan OS spesifik	-
9	Penyebaran dalam jaringan (via e-mail, IRC, HTML, dll), tidak perlu lampiran untuk dibuka untuk direplikasi; spesifik OS	-
8	Penyebaran dalam jaringan (via email, IRC, HTML, dll), tidak perlu lampiran dibuka untuk direplikasi; spesifik aplikasi	-
7	Penyebaran dalam jaringan (via email, IRC, HTML, dll), memerlukan lampiran untuk direplikasi; Spesifik OS	*Ransomware* ELPaco
6	Penyebaran dalam jaringan (via email, IRC, HTML, dll), memerlukan lampiran untuk direplikasi; spesifik aplikasi	-
5	Penyebaran *file*; tidak spesifik OS	-
4	Penyebaran *file*; spesifik OS	-
3	Penyebaran *file*; spesifik aplikasi	-
2	Telah diinjeksi; tidak spesifik OS	-
1	Telah diinjeksi; spesifik OS	-

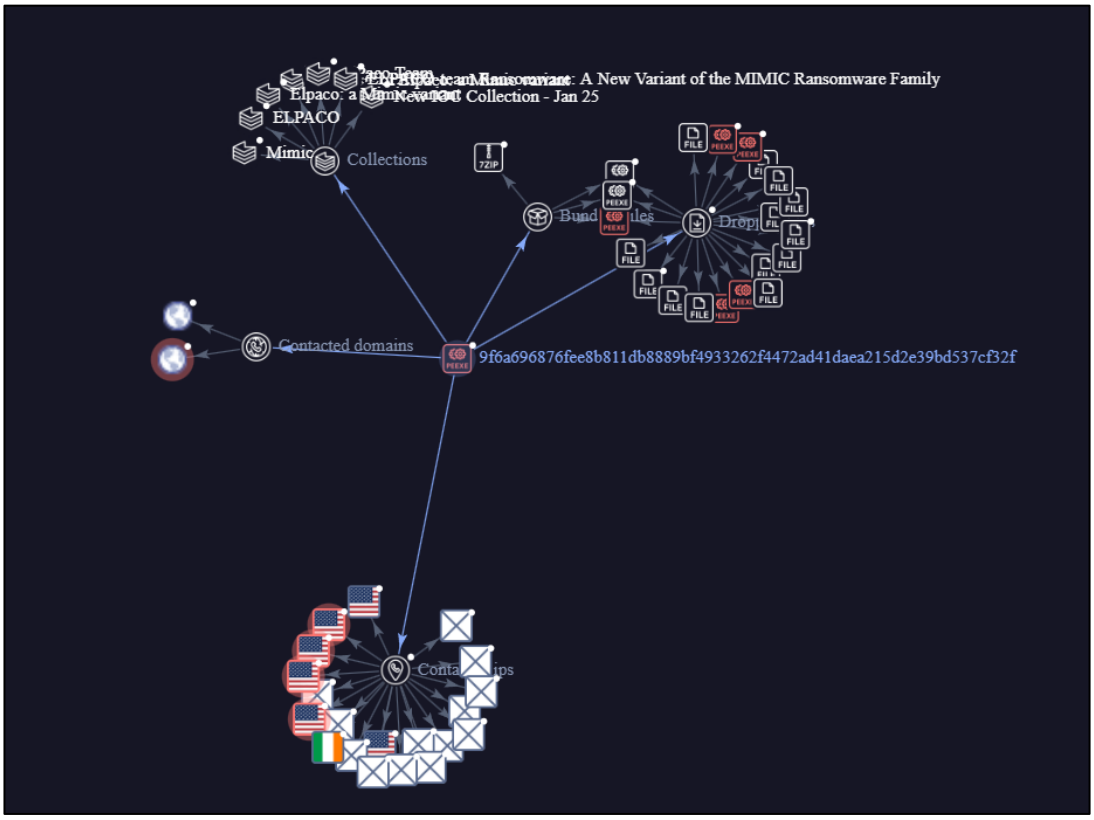
Tabel 8. Ambang Batas Yang Diusulkan Untuk Menentukan *Hostility Rating*

Rating	Deskripsi	*Malware*
5	Untuk merusak dan mengganggu dalam skala internasional	-
4	Untuk merusak	*Ransomware* ELPaco
3	Untuk mengganggu dalam skala internasional	-
2	Untuk mengganggu dalam skala nasional	-
1	Proses injeksi secara *accidental*	-

Lampiran 2. TTP berdasarkan *Framework* Mitre ATT&CK

Tabel 6. TTP berdasarkan *Framework* Mitre ATT&CK *pada malware* Ransom:Win32/Mimic.MA!MTB

Initial Access	Execution	Persistence	Defense Evasion	Discovery	Collection	Impact
Phishing T1566	User Execution T1059	Registry Run Keys / Startup Folder T1547.001	Indicator Removal: File Deletion T1070.004	System Information Discovery T1082	Data from Local System T1005	Data Encrypted for Impact T1486
Exploit Public-Facing Application T1190	Exploitation for Client Execution T1203			File & Directory Discovery T1083		
	Malicious File T1204.002			System Network Configuration Discovery T1016		



Gambar 26. Grafik Relasi *File* 33eeeb25f834e0b180f960ecb9518ea0

Lampiran 4. Daftar *Indicatior of Compromise* (IoC)

Tabel 9. Daftar IoC Nilai *Hash*

No	Nilai Hash	Keterangan
1	33EEEB25F834E0B180F960ECB9518EA0	ELPACO-team.vexe
2	B93EB0A48C91A53BDA6A1A074A4B431E	7za.exe
3	AC34BA84A5054CD701EFAD5DD14645C9	DC.exe
4	0BF7C0D8E3E02A6B879EFAB5DEAB013C	ENC_default_default_2023-12-27_09-27-40=Telegram@datadecrypt.exe
5	C44487CE1827CE26AC4699432D15B42A	Everything.exe
6	742C2400F2DE964D0CCE4A8DABADD708	Everything.ini
7	51014C0C06ACDD80F9AE4469E7D30A9E	Everything2.ini
8	3B03324537327811BBBAFF4AAFA4D75B	Everything32.dll
9	245FB739C4CB3C944C11EF43CDDD8D57	Everything64.dll
10	61CA00CB4A46596655F75B1B6A1ABA10	Everything64.dll
11	1B37DC212E98A04576AAC40D7CE7D06A	global_options.ini
12	26F59BB93F02D5A65538981BBC2DA9CC	global_options.ini
13	03A63C096B9757439264B57E4FDF49D1	gui35.exe
14	57850A4490A6AFD1EF682EB93EA45E65	gui40.exe
15	FADE75EDBF62291FBB99C937AFC9792C	session.tmp
16	B951E50264F9C5244592DFB0A859EC41	svhostss.exe
17	803DF907D936E08FBBD06020C411BE93	xdel.exe
18	B951E50264F9C5244592DFB0A859EC41	ELPACO-team.exe