kaspersky

Unraveling the Elpaco ransomware: A Mimic variant

Cristian Souza

Incident Response Specialist

Global Emergency Response Team | Kaspersky Lab

kaspersky

./whoami

- From Brazil.
- Incident Response Specialist @ GERT.
- PhD student in Computer Science at University of São Paulo.
- CISSP, GCFA, GREM, LPIC-3, CHFI, CEH.
- I code in my free time 😅

kaspersky

Agenda

- Introduction
- Analysis
- YARA rules
- Victims
- Tactics, techniques and procedures
- Conclusion
- Indicators of compromise

kaspersky

Full article

Analysis of Elpaco: a Mimic variant

MALWARE DESCRIPTIONS 26 NOV 2024 7 minute read

// AUTHORS

Expert CRISTIAN SOUZA Expert TIMOFEY EZHOV Expert EDUARDO OVALLE Expert ASHLEY MUÑOZ

kaspersky

Introduction

- In a recent incident response case, we dealt with a variant of the Mimic ransomware with some interesting customization features.

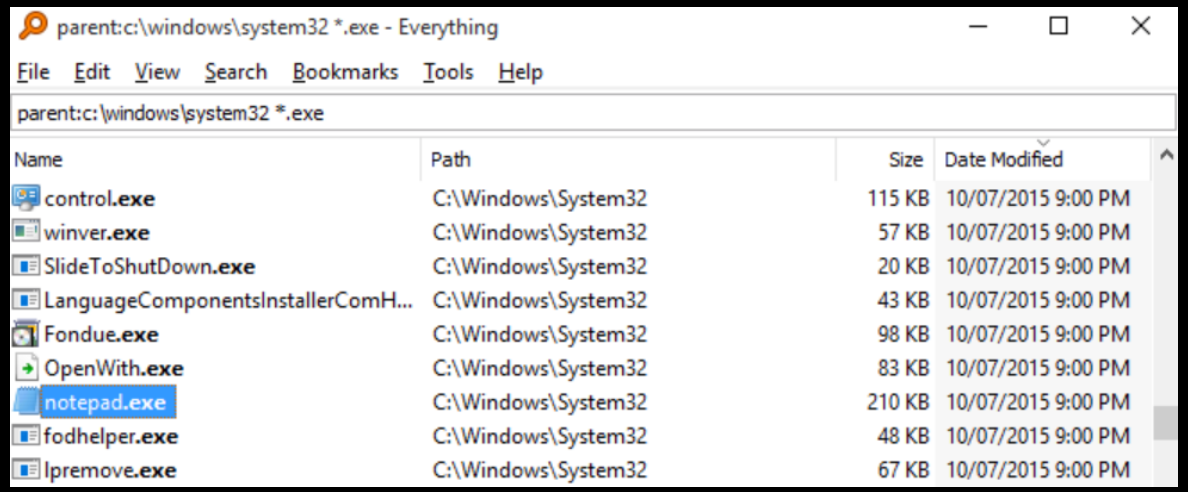
- The attackers were able to connect via RDP to the victim’s server after a successful brute force attack and then launch the ransomware.

- After that, the adversary was able to elevate their privileges by exploiting the CVE-2020-1472 vulnerability (Zerologon).

kaspersky

Introduction

- The identified variant abuses the Everything library and provides an easy-to-use GUI for the attacker to customize the operations performed by the malware.



- This ransomware variant is named “Elpaco” and contains files with extensions under the same name.

kaspersky

Analysis

- Our analysis started with a basic inspection of the sample. First, we verified its properties, such as the file type, strings and capabilities.

```
 $ file 33eeeb25f834e0b180f960ecb9518ea0
33eeeb25f834e0b180f960ecb9518ea0: PE32 executable (GUI) Intel 80386, for MS Windows
 $ trid 33eeeb25f834e0b180f960ecb9518ea0

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found:  14909
Analyzing...

Collecting data from file: 33eeeb25f834e0b180f960ecb9518ea0
 43.3% (.EXE) Microsoft Visual C++ compiled executable (generic) (16529/12/5)
 27.6% (.EXE) Win64 Executable (generic) (10523/12/4)
 13.2% (.EXE) Win16 NE executable (generic) (5038/12/1)
  5.3% (.EXE) OS/2 Executable (generic) (2029/13)
  5.2% (.EXE) Generic Win/DOS Executable (2002/3)
 $
```

kaspersky

Analysis

- Interestingly enough, the malware used a 7-Zip installer mechanism, so it was classified as packed by most malware analysis tools and raised suspicions with detection tools.

```
 $ diec 33eeeb25f834e0b180f960ecb9518ea0
PE32
    Installer: 7-Zip(1.0)[-]
    Compiler: Microsoft Visual C/C++(2005)[msvcrt]
    Archive: 7-Zip(0.4)[-]
```

```
 $ diec 33eeeb25f834e0b180f960ecb9518ea0 --entropy
Total 7.97788: packed
  0|PE Header|0|512|2.55981: not packed
  1|Section(0)['.text']|512|101888|6.67404: packed
  2|Section(1)['.rdata']|102400|15360|5.71349: not packed
  3|Section(2)['.data']|117760|2560|4.45154: not packed
  4|Section(3)['.rsrc']|120320|69120|2.79098: not packed
  5|Overlay|189440|3540503|7.99993: packed
```

kaspersky

Analysis

- We inspected the file as a ZIP and found that the sample abused the Everything library.

- Everything features:
  - Fast searching.
  - Real-time updates.

```
 $ 7z l -ba 33eeeb25f834e0b180f960ecb9518ea0
2021-11-24 10:00:00 ....A       791040      3539955  7za.exe
2021-12-17 01:01:18 ....A      1775264               Everything.exe
2022-04-07 11:54:26 ....A        86656               Everything32.dll
2024-06-05 12:09:48 ....A      2654321               Everything64.dll
```

kaspersky

Analysis

- The artifact was password-protected.
- Inside, there was a legitimate 7-Zip utility for extracting the malicious archive contents.
- We were able to retrieve the password from the file strings:

```
2e434 RunProgram="hidcon:7za.exe x -y -p71832043735857 82 Everything64.dll"
```

kaspersky

Analysis

- When executed, the malware unpacked the archive and dropped the necessary files into the **%AppData%\Local** directory, inside a separate directory with a randomly generated UUID as the name.

```
C:\Users\user\AppData\Local\BD3FDDDF-6CAF-3EBC-D9CF-C8DF72D8F78A\
```

kaspersky

Analysis

```
PS C:\Users\user> Get-ChildItem C:\Users\user\AppData\Local\BD3FDDDF-6CAF-3EBC-D9CF-C8DF72D8F78A


    Directory: C:\Users\user\AppData\Local\BD3FDDDF-6CAF-3EBC-D9CF-C8DF72D8F78A


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/23/2023   4:11 PM         791040 7za.exe
-a----         8/25/2021   1:05 PM         821944 DC.exe
-a----         4/27/2022  11:43 PM        2492416 ENC_default_default_2023-12-27_09-27-40=Telegram@datadecrypt.exe
-a----         4/15/2021  12:17 AM        1775264 Everything.exe
-a----          5/1/2021   3:41 AM            548 Everything.ini
-a----          5/9/2023   4:51 PM            550 Everything2.ini
-a----         3/24/2021   6:18 PM          86656 Everything32.dll
-a----          9/3/2021   8:17 PM        2654321 Everything64.dll
-a----         9/23/2024  11:10 AM           5934 global_options.ini
-a----         2/20/2022   1:11 AM         283136 gui35.exe
-a----          6/9/2021   1:49 AM         283136 gui40.exe
-a----         9/23/2024  11:10 AM             32 session.tmp
-a----         8/18/2021  10:32 PM        2491392 svhostss.exe
-a----         2/22/2021   8:18 AM         358784 xdel.exe
```

→ Main file

kaspersky

Analysis

- The sample also drops a file called **session.tmp** into the same destination directory. This is a session key for resuming encryption if the malicious process is interrupted, as by a process kill.

session.tmp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	0B	F2	83	C9	F2	79	3D	2D	58	5C	44	94	28	A0	5C	C8	.òƒÉòy=-X\D"(\È
00000010	1D	BF	E0	8E	23	A3	15	2F	E4	7D	E3	D3	C0	F1	DB	05	.¿àŽ#£./ä}ãÓÀñÛ.

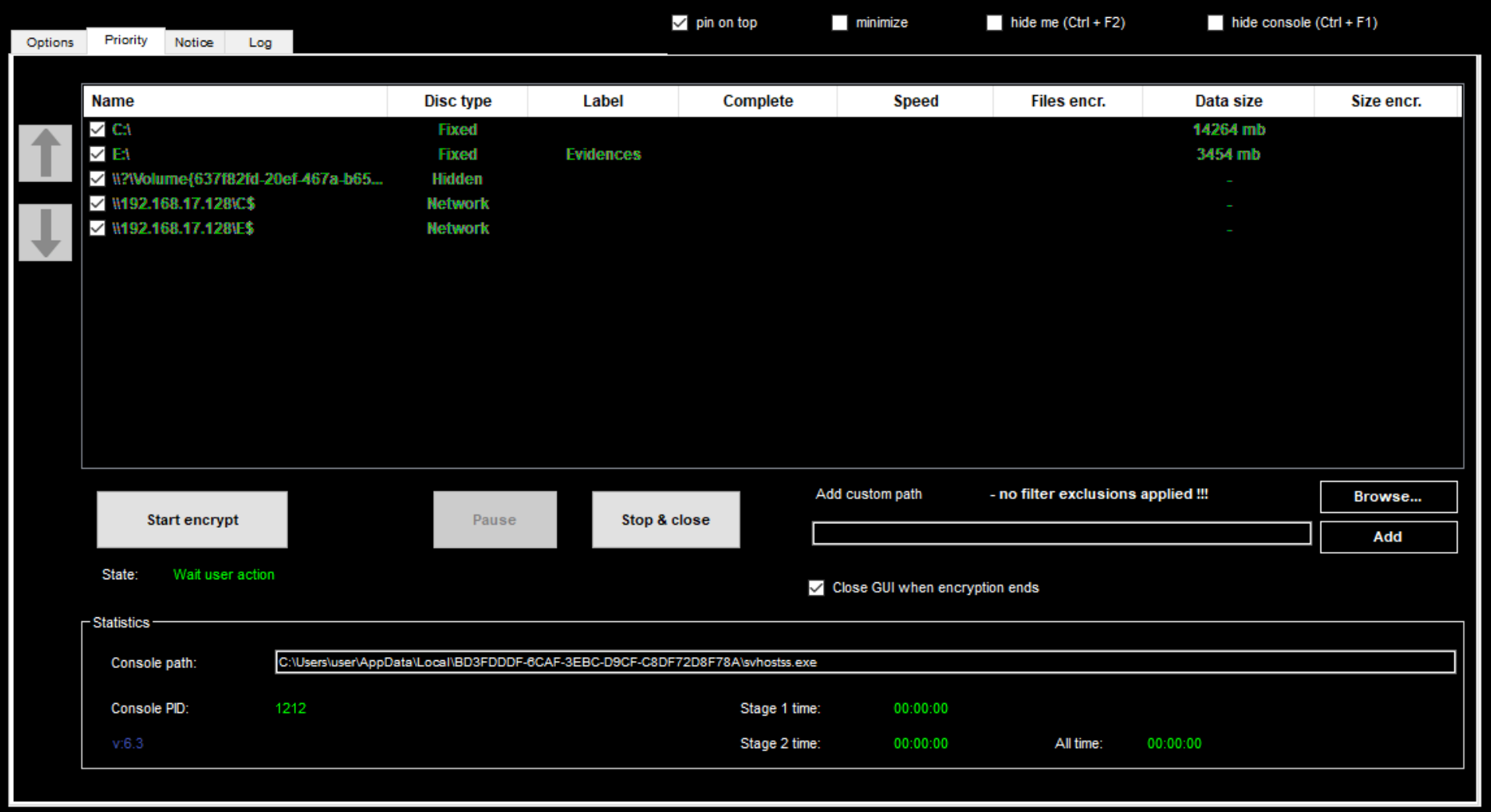
kaspersky

Analysis

- **svhostss.exe** is the main console used by the malware.
- **gui40.exe** is a GUI for customizing and executing the ransomware.
- In the GUI, the operator can:
  - Select entire drives for encryption;
  - Perform a process injection to hide malicious processes;
  - Customize the ransom note;
  - Change the encryption extension;
  - Set the order of encryption based on the original file format;
  - Exclude specific directories, files or formats from encryption.

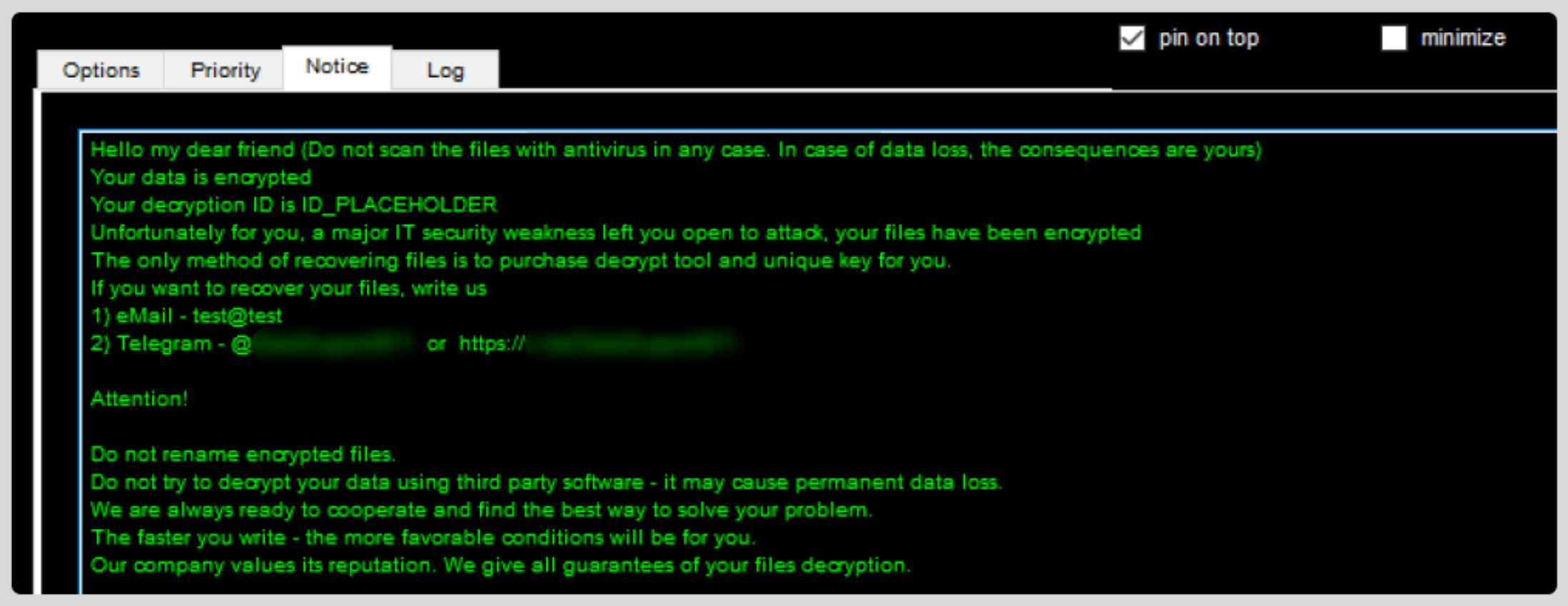
kaspersky

Analysis



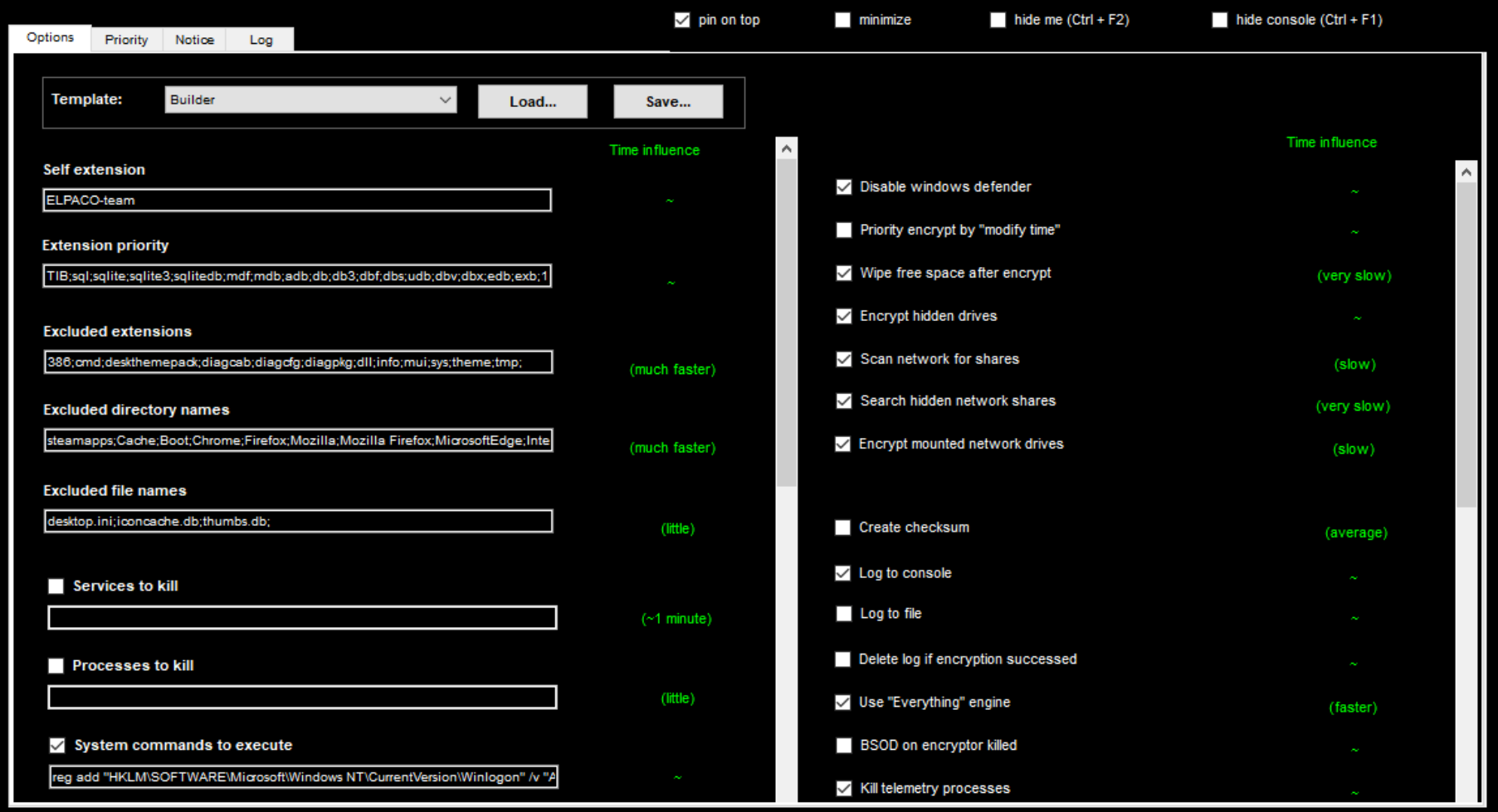
kaspersky

Analysis



kaspersky

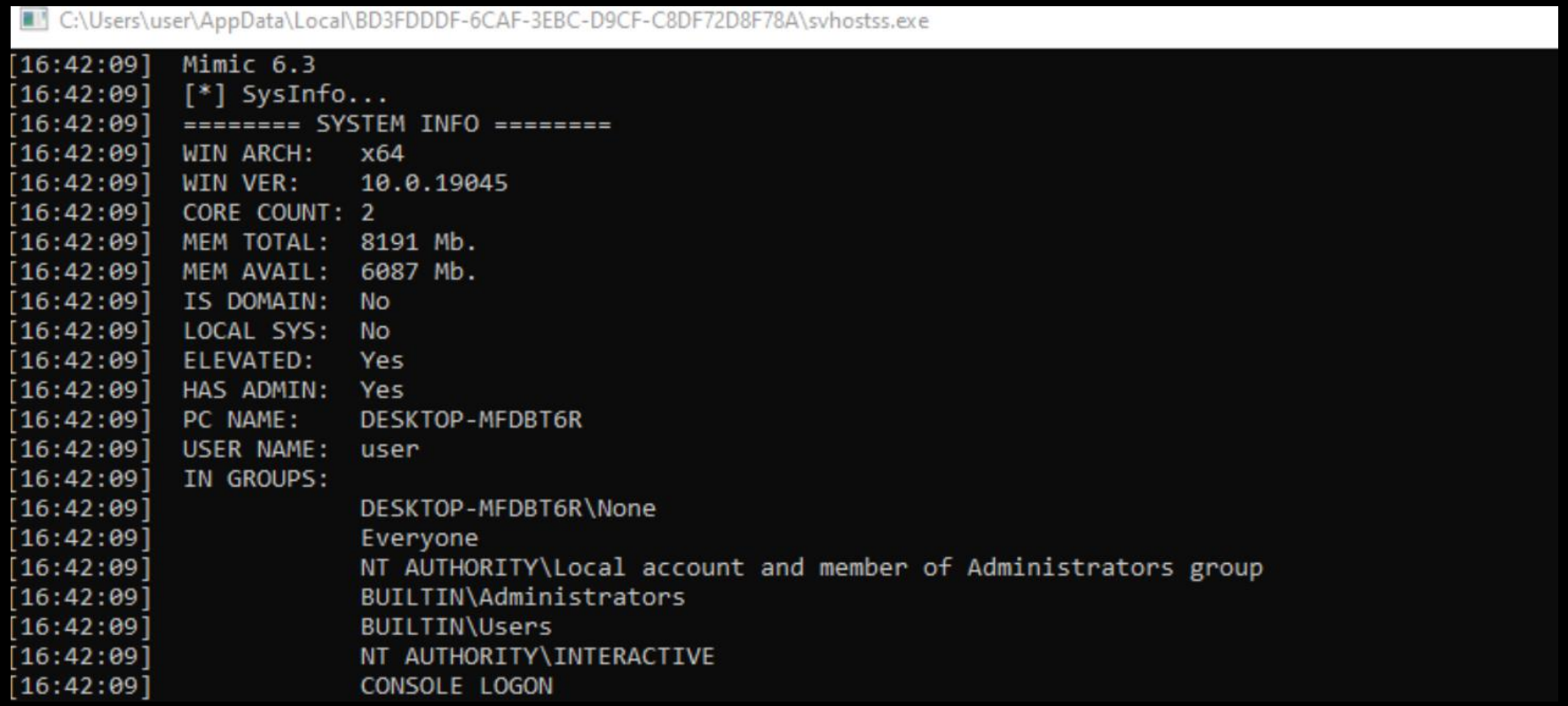
Analysis



kaspersky

Analysis

- The console interface, running alongside the GUI, gathers detailed information about the system, including drives and file shares.



kaspersky

Analysis

- The sample allows for the import and export of malware configuration files according to the parameters set by the operator.


Custom_Template.tpl - Notepad

File Edit Format View Help

```
26=ELPACO-team
27=TIB;sql;sqlite;sqlite3;sqlitedb;mdf;mdb;adb;db;db3;dbf;dbs;udb;dbv;dbx;edb;exb;1cd;fdb;idb;mpd;myd;odb;xls;xlsx;doc;docx;bac;bak;back;zip;rar;dt;4dd;4dl;abcddb;abs;abx;accdb;accdc;accde
;accdr;accdt;accdw;accft;ade;adf;adn;adp;alf;arc;ask;bacpac;bdf;btr;cat;cdb;chck;ckp;cma;cpd;dacpac;dad;dadiagrams;daschema;db-shm;db-
wal;db2;dbc;dbt;dcb;dct;dcx;ddl;dlis;dp1;dqy;dsk;dsn;dtsx;dxl;eco;ecx;epim;fcd;fic;fm5;fmp;fmp12;fmpsl;fol;fp3;fp4;fp5;fp7;fpt;frm;gdb;grdb;gwi;hdb;his;hjt;ib;icg;icr;ihx;itdb;itw;jet;jtx;
kdb;kexi;kexic;kexis;lgc;lut;lwx;maf;maq;mar;mas;mav;maw;mdn;mdt;mrg;mud;mwb;ndf;nnt;nrmlib;ns2;ns3;ns4;nsf;nv;nv2;nwdb;nyf;oqy;ora;orx;owc;p96;p97;pan;pdb;pdm;pnz;qry;qvd;rbf;rctd;rod;rod
x;rpd;rsd;s2db;sas7bdat;sbf;scx;sdb;sdc;sdf;sis;sl3;spq;sqlite2;te;temx;tmd;tps;trc;trm;udl;usr;v12;vis;vpd;vvv;wdb;wmdb;wrk;xdb;xld;xmlff;7z;
28=386;cmd;deskthemepack;diagcab;diagcfg;diagpkg;dll;info;mui;sys;theme;tmp;
29=steamapps;Cache;Boot;Chrome;Firefox;Mozilla;Mozilla Firefox;MicrosoftEdge;Internet Explorer;Tor Browser;Opera;Opera Software;Common Files;Config.Msi;Intel;Microsoft;Microsoft
Shared;Microsoft.NET;MSBuild;MSOCache;Packages;PerfLogs;ProgramData;System Volume Information;tmp;Temp;USOShared;Windows;Windows Defender;Windows Journal;Windows NT;Windows Photo
Viewer;Windows Security;Windows.old;WindowsApps;WindowsPowerShell;WINNT;$RECYCLE.BIN;$WINDOWS.~BT;$Windows.~WS;:\Users\Public\;:\Users\Default\;
30=desktop.ini;iconcache.db;thumbs.db;
31=
32=
33=reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "AllowMultipleTSSessions" /t REG_DWORD /d 0x1 /f;reg add "HKLM\system\CurrentControlSet\Control\Terminal Server"
/v "fSingleSessionPerUser" /t REG_DWORD /d 0x0 /f;reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "c:\windows
\system32\cmd.exe";

63=Hello my dear friend (Do not scan the files with antivirus in any case. In case of data loss, the consequences are yours)\nYour data is encrypted\nYour decryption ID is ID_PLACEHOLDER
\nUnfortunately for you, a major IT security weakness left you open to attack, your files have been encrypted\nThe only method of recovering files is to purchase decrypt tool and unique
key for you.\nIf you want to recover your files, write us\n1) eMail - [redacted] Telegram - [redacted] or https://[redacted] not rename
encrypted files. \nDo not try to decrypt your data using third party software - it may cause permanent data loss. \nWe are always ready to cooperate and find the best way to solve your
problem. \nThe faster you write - the more favorable conditions will be for you. \nOur company values its reputation. We give all guarantees of your files decryption.
66=1
```

kaspersky

Analysis

- When executed, the malware creates the following registry keys.

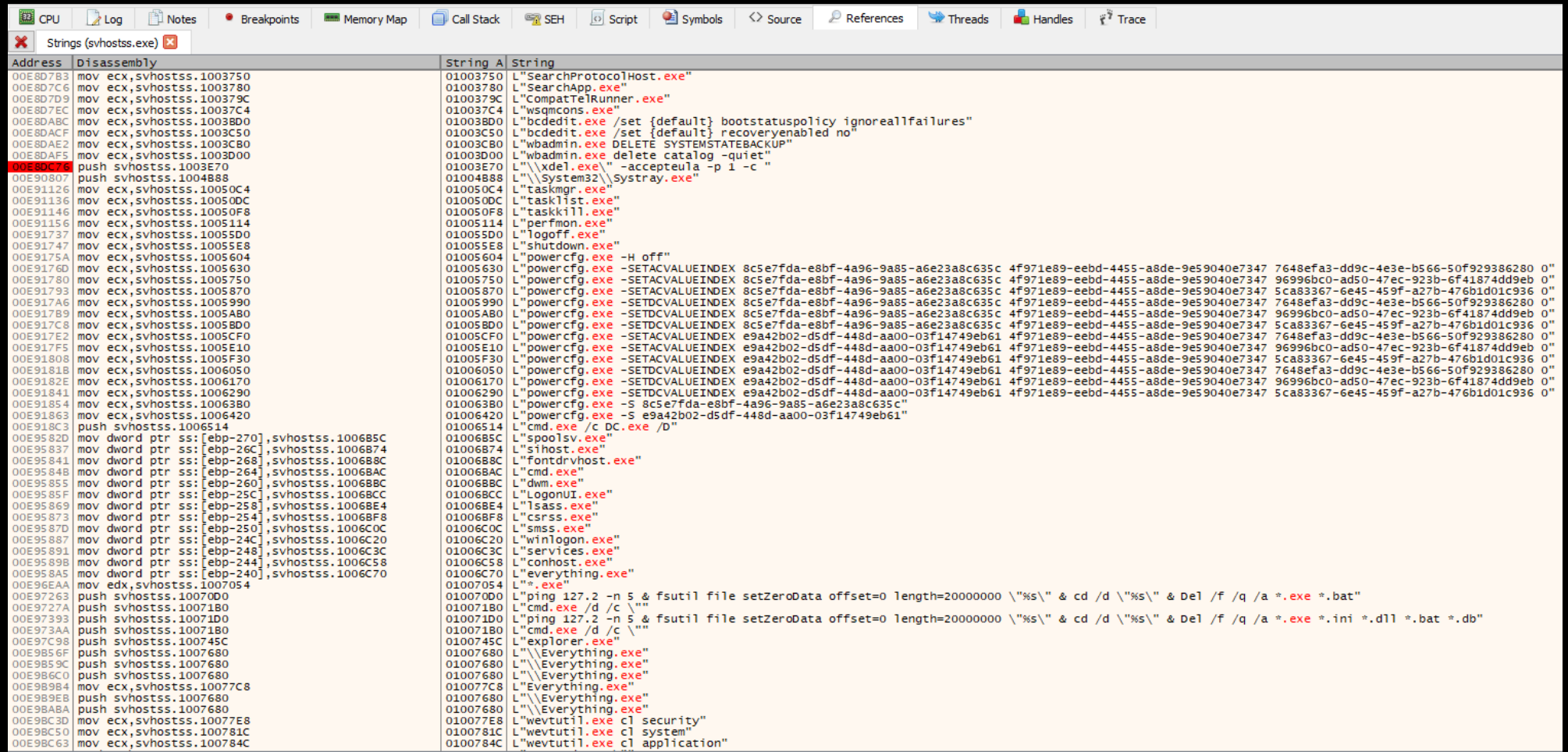
```
HKLM\SOFTWARE\Classes\.ELPACO-team\: "mimicfile"
HKLM\SOFTWARE\Classes\mimicfile\shell\open\command\: "notepad.exe
"C:\Users\user\AppData\Local\Decryption_INFO.txt""

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svhostss:
""C:\Users\user\AppData\Local\BD3FDDDF-6CAF-3EBC-D9CF-
C8DF72D8F78A\svhostss.exe""
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svhostss.exe: "notepad.exe
"C:\Users\user\AppData\Local\Decryption_INFO.txt""
```

kaspersky

Analysis

- svhostss.exe, lacks significant protection from analysis.



CPU | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Threads | Handles | Trace

Strings (svhostss.exe)

Address	Disassembly	String A	String
00E8D7B3	mov ecx,svhostss.1003750	01003750	L"SearchProtocolHost.exe"
00E8D7C6	mov ecx,svhostss.1003780	01003780	L"SearchApp.exe"
00E8D7D9	mov ecx,svhostss.100379C	0100379C	L"CompatTelRunner.exe"
00E8D7EC	mov ecx,svhostss.10037C4	010037C4	L"wsqmcons.exe"
00E8DABC	mov ecx,svhostss.1003BD0	01003BD0	L"bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures"
00E8DACF	mov ecx,svhostss.1003C50	01003C50	L"bcdedit.exe /set {default} recoveryenabled no"
00E8DAE2	mov ecx,svhostss.1003CB0	01003CB0	L"wbadmin.exe DELETE SYSTEMSTATEBACKUP"
00E8DAF5	mov ecx,svhostss.1003D00	01003D00	L"wbadmin.exe delete catalog -quiet"
00E8DC76	push svhostss.1003E70	01003E70	L"\\xdel.exe\" -accepteula -p 1 -c "
00E90807	push svhostss.1004B88	01004B88	L"\\System32\\Systray.exe"
00E91126	mov ecx,svhostss.10050C4	010050C4	L"taskmgr.exe"
00E91136	mov ecx,svhostss.10050DC	010050DC	L"tasklist.exe"
00E91146	mov ecx,svhostss.10050F8	010050F8	L"taskkill.exe"
00E91156	mov ecx,svhostss.1005114	01005114	L"perfmon.exe"
00E91737	mov ecx,svhostss.10055D0	010055D0	L"logoff.exe"
00E91747	mov ecx,svhostss.10055E8	010055E8	L"shutdown.exe"
00E9175A	mov ecx,svhostss.1005604	01005604	L"powercfg.exe -H off"
00E9176D	mov ecx,svhostss.1005630	01005630	L"powercfg.exe -SETACVALUEINDEX 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 4f971e89-eebd-4455-a8de-9e59040e7347 7648efa3-dd9c-4e3e-b566-50f929386280 0"
00E91780	mov ecx,svhostss.1005750	01005750	L"powercfg.exe -SETACVALUEINDEX 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 4f971e89-eebd-4455-a8de-9e59040e7347 96996bc0-ad50-47ec-923b-6f41874dd9eb 0"
00E91793	mov ecx,svhostss.1005870	01005870	L"powercfg.exe -SETACVALUEINDEX 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 4f971e89-eebd-4455-a8de-9e59040e7347 5ca83367-6e45-459f-a27b-476b1d01c936 0"
00E917A6	mov ecx,svhostss.1005990	01005990	L"powercfg.exe -SETDCVALUEINDEX 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 4f971e89-eebd-4455-a8de-9e59040e7347 7648efa3-dd9c-4e3e-b566-50f929386280 0"
00E917B9	mov ecx,svhostss.1005AB0	01005AB0	L"powercfg.exe -SETDCVALUEINDEX 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 4f971e89-eebd-4455-a8de-9e59040e7347 96996bc0-ad50-47ec-923b-6f41874dd9eb 0"
00E917C8	mov ecx,svhostss.1005BD0	01005BD0	L"powercfg.exe -SETDCVALUEINDEX 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 4f971e89-eebd-4455-a8de-9e59040e7347 5ca83367-6e45-459f-a27b-476b1d01c936 0"
00E917E2	mov ecx,svhostss.1005CF0	01005CF0	L"powercfg.exe -SETACVALUEINDEX e9a42b02-d5df-448d-aa00-03f14749eb61 4f971e89-eebd-4455-a8de-9e59040e7347 7648efa3-dd9c-4e3e-b566-50f929386280 0"
00E917F5	mov ecx,svhostss.1005E10	01005E10	L"powercfg.exe -SETACVALUEINDEX e9a42b02-d5df-448d-aa00-03f14749eb61 4f971e89-eebd-4455-a8de-9e59040e7347 96996bc0-ad50-47ec-923b-6f41874dd9eb 0"
00E91808	mov ecx,svhostss.1005F30	01005F30	L"powercfg.exe -SETACVALUEINDEX e9a42b02-d5df-448d-aa00-03f14749eb61 4f971e89-eebd-4455-a8de-9e59040e7347 5ca83367-6e45-459f-a27b-476b1d01c936 0"
00E9181B	mov ecx,svhostss.1006050	01006050	L"powercfg.exe -SETDCVALUEINDEX e9a42b02-d5df-448d-aa00-03f14749eb61 4f971e89-eebd-4455-a8de-9e59040e7347 7648efa3-dd9c-4e3e-b566-50f929386280 0"
00E9182E	mov ecx,svhostss.1006170	01006170	L"powercfg.exe -SETDCVALUEINDEX e9a42b02-d5df-448d-aa00-03f14749eb61 4f971e89-eebd-4455-a8de-9e59040e7347 96996bc0-ad50-47ec-923b-6f41874dd9eb 0"
00E91841	mov ecx,svhostss.1006290	01006290	L"powercfg.exe -SETDCVALUEINDEX e9a42b02-d5df-448d-aa00-03f14749eb61 4f971e89-eebd-4455-a8de-9e59040e7347 5ca83367-6e45-459f-a27b-476b1d01c936 0"
00E91854	mov ecx,svhostss.10063B0	010063B0	L"powercfg.exe -S 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c"
00E91863	mov ecx,svhostss.1006420	01006420	L"powercfg.exe -S e9a42b02-d5df-448d-aa00-03f14749eb61"
00E918C3	push svhostss.1006514	01006514	L"cmd.exe /c DC.exe /D"
00E9582D	mov dword ptr ss:[ebp-270],svhostss.1006B5C	01006B5C	L"spoolsv.exe"
00E95837	mov dword ptr ss:[ebp-26C],svhostss.1006B74	01006B74	L"sihost.exe"
00E95841	mov dword ptr ss:[ebp-268],svhostss.1006B8C	01006B8C	L"fontdrvhost.exe"
00E9584B	mov dword ptr ss:[ebp-264],svhostss.1006BAC	01006BAC	L"cmd.exe"
00E95855	mov dword ptr ss:[ebp-260],svhostss.1006BBC	01006BBC	L"dwm.exe"
00E9585F	mov dword ptr ss:[ebp-25C],svhostss.1006BCC	01006BCC	L"LogonUI.exe"
00E95869	mov dword ptr ss:[ebp-258],svhostss.1006BE4	01006BE4	L"lsass.exe"
00E95873	mov dword ptr ss:[ebp-254],svhostss.1006BF8	01006BF8	L"csrss.exe"
00E9587D	mov dword ptr ss:[ebp-250],svhostss.1006C0C	01006C0C	L"smss.exe"
00E95887	mov dword ptr ss:[ebp-24C],svhostss.1006C20	01006C20	L"winlogon.exe"
00E95891	mov dword ptr ss:[ebp-248],svhostss.1006C3C	01006C3C	L"services.exe"
00E9589B	mov dword ptr ss:[ebp-244],svhostss.1006C58	01006C58	L"conhost.exe"
00E958A5	mov dword ptr ss:[ebp-240],svhostss.1006C70	01006C70	L"everything.exe"
00E96EAA	mov edx,svhostss.1007054	01007054	L"*.exe"
00E97263	push svhostss.10070D0	010070D0	L"ping 127.2 -n 5 & fsutil file setZeroData offset=0 length=20000000 \"%s\" & cd /d \"%s\" & Del /f /q /a *.exe *.bat"
00E9727A	push svhostss.10071B0	010071B0	L"cmd.exe /d /c \""
00E97393	push svhostss.10071D0	010071D0	L"ping 127.2 -n 5 & fsutil file setZeroData offset=0 length=20000000 \"%s\" & cd /d \"%s\" & Del /f /q /a *.exe *.ini *.dll *.bat *.db"
00E973AA	push svhostss.10071B0	010071B0	L"cmd.exe /d /c \""
00E97C98	push svhostss.100745C	0100745C	L"explorer.exe"
00E9B56F	push svhostss.1007680	01007680	L"\\Everything.exe"
00E9B59C	push svhostss.1007680	01007680	L"\\Everything.exe"
00E9B6C0	push svhostss.1007680	01007680	L"\\Everything.exe"
00E9B9B4	mov ecx,svhostss.10077C8	010077C8	L"Everything.exe"
00E9B9EB	push svhostss.1007680	01007680	L"\\Everything.exe"
00E9BABA	push svhostss.1007680	01007680	L"\\Everything.exe"
00E9BC3D	mov ecx,svhostss.10077E8	010077E8	L"wevtutil.exe cl security"
00E9BC50	mov ecx,svhostss.100781C	0100781C	L"wevtutil.exe cl system"
00E9BC63	mov ecx,svhostss.100784C	0100784C	L"wevtutil.exe cl application"

kaspersky

Analysis

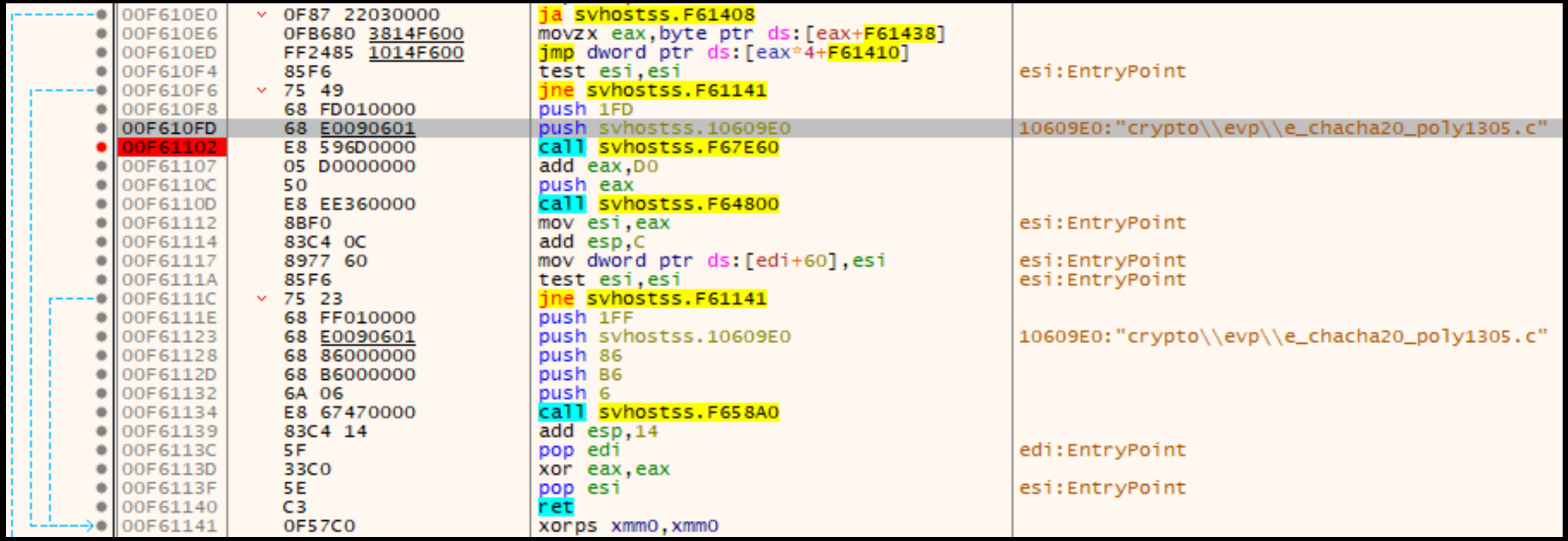
- SetSearchW function:

```
0023C415   0F4305 586E3B00   cmovae eax,dword ptr ds:[3B6E58]
0023C41C   50                push eax
0023C41D   FF15 FC003400     call dword ptr ds:[<Everything_SetSearchW>]
0023C423   68 A0793A00       push svhostss.3A79A0          3A79A0:L"[*] Everything SetRequestFlags..."
0023C428   E8 93E9FEFF       call svhostss.22ADC0
0023C42D   83C4 04           add esp,4
0023C430   56                push esi                      esi:"minkernel\\ntdll\\ldrinit.c"
0023C431   FF15 E4003400     call dword ptr ds:[<Everything_SetRequestFlags>]
0023C437   84DB              test bl,bl
0023C439   74 15             je svhostss.23C450
0023C43B   68 E4793A00       push svhostss.3A79E4          3A79E4:L"[*] Everything SetSort..."
0023C440   E8 7BE9FEFF       call svhostss.22ADC0
0023C445   83C4 04           add esp,4
0023C448   6A 0E             push E
0023C44A   FF15 00013400     call dword ptr ds:[<Everything_SetSort>]
0023C450   68 F4010000       push 1F4
0023C455   FF15 F0023400     call dword ptr ds:[<Sleep>]
0023C45B   68 187A3A00       push svhostss.3A7A18          3A7A18:L"[*] Everything Query..."
0023C460   E8 5BE9FEFF       call svhostss.22ADC0
0023C465   83C4 04           add esp,4
```

kaspersky

Analysis

- Encryption using ChaCha20:



```
00F610E0   0F87 22030000    ja svhostss.F61408
00F610E6   0FB680 3814F600  movzx eax,byte ptr ds:[eax+F61438]
00F610ED   FF2485 1014F600  jmp dword ptr ds:[eax*4+F61410]
00F610F4   85F6             test esi,esi                          esi:EntryPoint
00F610F6   75 49            jne svhostss.F61141
00F610F8   68 FD010000      push 1FD
00F610FD   68 E0090601      push svhostss.10609E0                 10609E0:"crypto\\evp\\e_chacha20_poly1305.c"
00F61102   E8 596D0000      call svhostss.F67E60
00F61107   05 D0000000      add eax,D0
00F6110C   50               push eax
00F6110D   E8 EE360000      call svhostss.F64800
00F61112   8BF0             mov esi,eax                           esi:EntryPoint
00F61114   83C4 0C          add esp,C
00F61117   8977 60          mov dword ptr ds:[edi+60],esi         esi:EntryPoint
00F6111A   85F6             test esi,esi                          esi:EntryPoint
00F6111C   75 23            jne svhostss.F61141
00F6111E   68 FF010000      push 1FF
00F61123   68 E0090601      push svhostss.10609E0                 10609E0:"crypto\\evp\\e_chacha20_poly1305.c"
00F61128   68 86000000      push 86
00F6112D   68 B6000000      push B6
00F61132   6A 06            push 6
00F61134   E8 67470000      call svhostss.F658A0
00F61139   83C4 14          add esp,14
00F6113C   5F               pop edi                               edi:EntryPoint
00F6113D   33C0             xor eax,eax
00F6113F   5E               pop esi                               esi:EntryPoint
00F61140   C3               ret
00F61141   0F57C0           xorps xmm0,xmm0
```

kaspersky

Analysis

- All procedures performed by the ransomware during execution are logged to **C:\temp\MIMIC_LOG.txt**.

```
PS C:\temp> ls


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/25/2024   4:39 PM          48816 MIMIC_LOG.txt
-a----         9/25/2024   4:38 PM             32 session.tmp


PS C:\temp> gc -TotalCount 10 .\MIMIC_LOG.txt
[16:39:33] Waiting for signal to terminate

[16:39:33] [*] Backup session key success

[16:39:33] [*] Protect directory...: C:\Users\user\AppData\Local\BD3FDDDF-6CAF-3EBC-D9CF-C8DF72D8F78A

[16:39:33] [*] Using settings:

[16:39:33] [*] ------------------

PS C:\temp> gc -Tail 10 .\MIMIC_LOG.txt

[16:41:35] [*] Kill watcher

[16:41:35] [*] Self del

[16:41:35] [+] Success run: cmd.exe /d /c "ping 127.2 -n 5 & fsutil file setZeroData offset=0 length=20000000 "C:\Users\user\AppData\
Local\BD3FDDDF-6CAF-3EBC-D9CF-C8DF72D8F78A\svhostss.exe" & cd /d "C:\Users\user\AppData\Local\BD3FDDDF-6CAF-3EBC-D9CF-C8DF72D8F78A" &
 Del /f /q /a *.exe *.ini *.dll *.bat *.db" (pid:7752)

[16:41:35] Closing...
```

kaspersky

YARA rules

- Rule for detecting the Elpaco dropper:

```
import "pe"

rule elpaco_dropper
{
  meta:
  author = "Kaspersky - GERT"
  description = "Yara rule for detecting the Elpaco dropper."
  target_entity = "file"

  strings:
    $s1 = "-p71832043735857 82" wide ascii nocase
    $s2 = "Everything64.dll" wide ascii nocase
    $s3 = "ELPACO-team.exe" wide ascii nocase
  condition:
    (2 of ($s*)) and pe.imports("SHELL32.dll", "ShellExecuteW") and pe.imports("KERNEL32.dll", "LoadLibraryA")
}
```

kaspersky

YARA rules

- Rule for detecting the Elpaco main console:

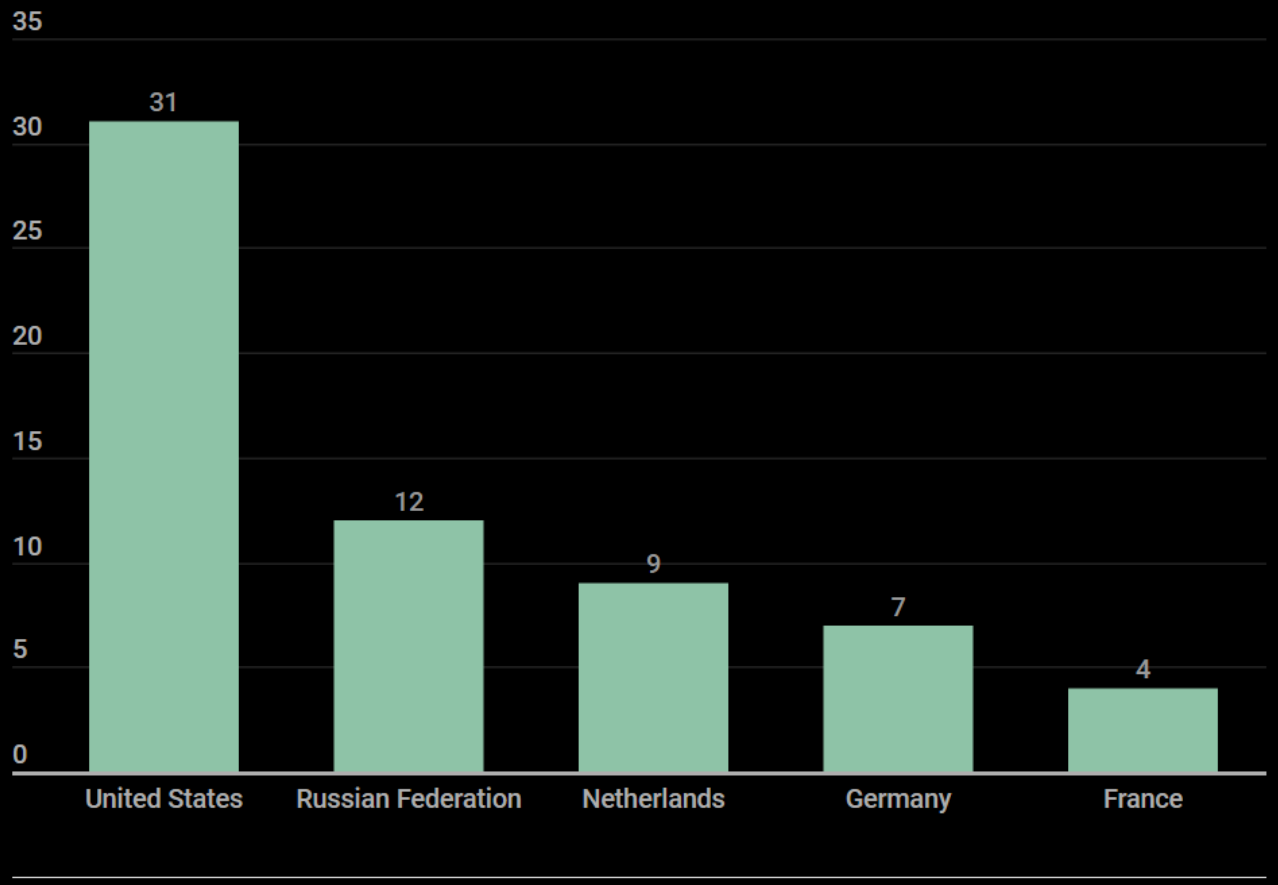
```
import "pe"

rule elpaco_console
{
  meta:
  author = "Kaspersky - GERT"
  description = "Yara rule for detecting the Elpaco main console."
  target_entity = "file"

  strings:
    $s1 = "powershell.exe -ExecutionPolicy Bypass" wide ascii nocase
    $s2 = "Software\\Classes\\mimicfile\\shell\\open\\command" wide ascii nocase
    $s3 = "cmd.exe /c DC.exe /D" wide ascii nocase
    $s4 = "MIMIC_LOG.txt" wide ascii nocase
    $s5 = "mimicfile" wide ascii nocase
    $s6 = "Everything Setup..." wide ascii nocase
    $s7 = "[*] Everything Query..." wide ascii nocase
  condition:
    5 of ($s*) and pe.imports("Everything32.dll", "Everything_SetSearchW") and pe.imports("bcrypt.dll", "BCryptGenRandom")
}
```

Victims

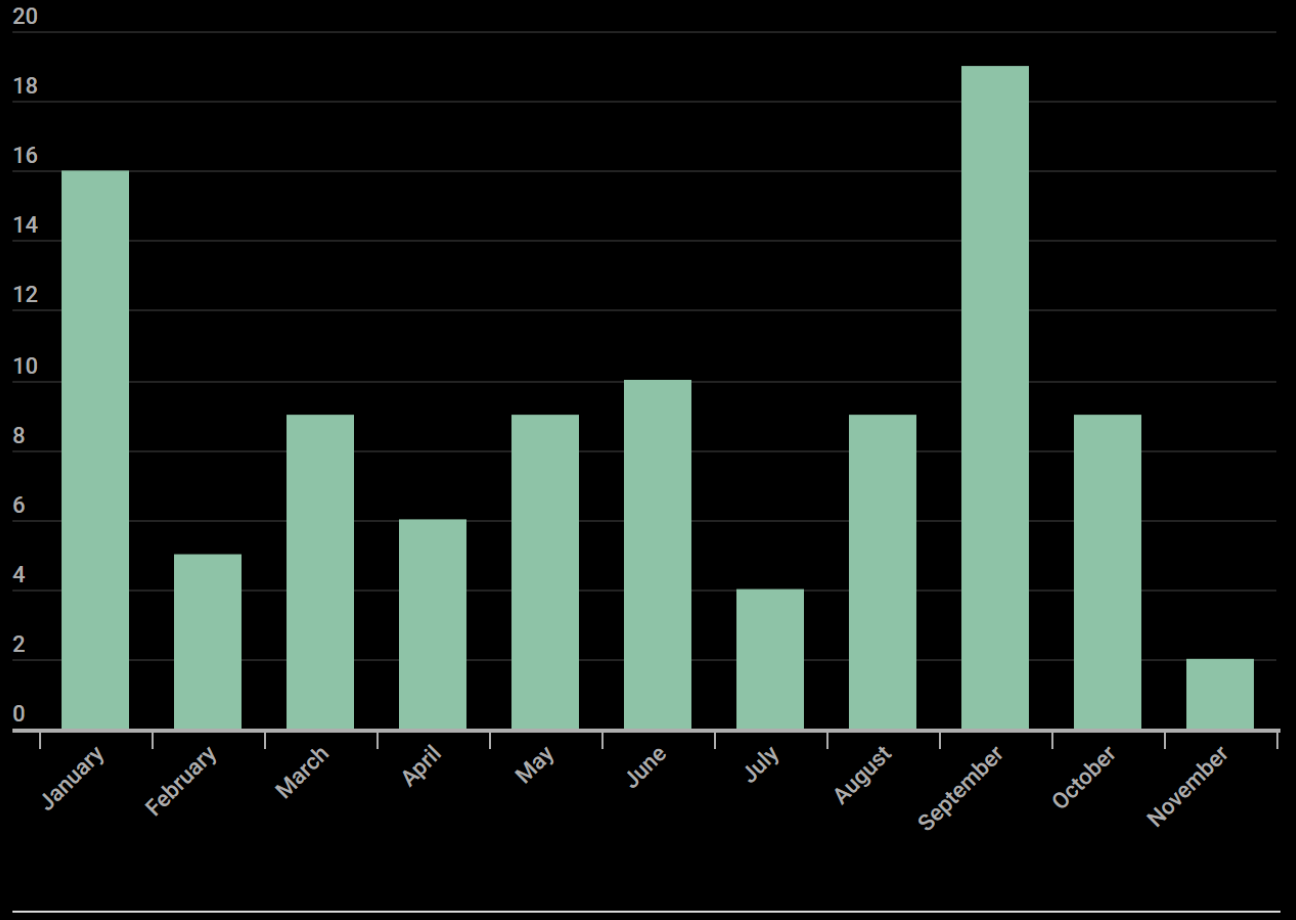
- Most affected countries:



kaspersky

Victims

- Mimic appearances per month:



kaspersky

Tactics, techniques and procedures

Tactic	Technique	ID
Discovery	Network Share Discovery	T1135
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003
Execution	Command and Scripting Interpreter: PowerShell	T1059.001
Impact	Data Encrypted for Impact	T1486
Impact	Service Stop	T1489
Impact	Inhibit System Recovery	T1490
Defense evasion	Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002
Defense evasion	Masquerading	T1036
Defense evasion	Modify Registry	T1112
Defense evasion	Disable or Modify System Firewall	T1562.004
Defense evasion	Process Injection	T1055
Defense evasion	Hide Artifacts	T1564
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001

kaspersky

Conclusion

- The artifact presented an interesting user interface for customizing its attributes, while allowing the operator to export the parameters to a configuration file.
- Unfortunately, the encryption algorithm makes it impossible to decrypt the files on an infected machine without the private key, which makes this threat hard to deal with.
- Another feature of Elpaco is that it deletes itself after encrypting files to evade detection and analysis.
- We have observed attacks with Elpaco and other Mimic samples on a massive scale, targeting a wide range of countries worldwide, and we'll continue monitoring this threat.

kaspersky

Indicators of compromise

- 61f73e692e9549ad8bc9b965e25d2da683d56dc1 (dropper)
- 8af05099986d0b105d8e38f305efe9098a9fbda6 (svhostss.exe)

Kaspersky products detect this threat with the following verdicts:

- HEUR:Trojan-Ransom.Win32.Generic (dropper).
- HEUR:Trojan-Ransom.Win32.Mimic.gen (svhostss.exe).

kaspersky

Unraveling the Elpaco ransomware: A Mimic variant

Cristian Souza

Incident Response Specialist

Global Emergency Response Team | Kaspersky Lab