

## Benchmark EPICODE W24D4

Ci è stato chiesto di analizzare il malware presente nella cartella presente all'interno della macchina virtuale chiamato Build\_Week\_Unit\_3 e di rispondere a vari quesiti facendo Analisi statica e analisi dinamica.

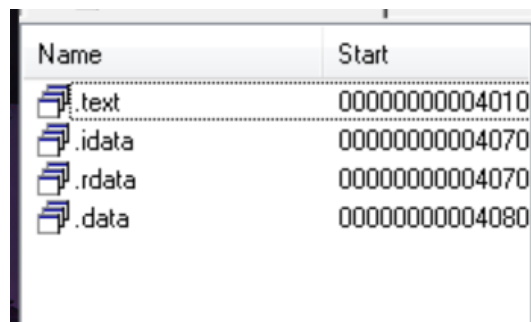
Come prima cosa ho avviato IDA PRO a prendo il Malware.

I parametri riscontrati nella funzione Main() sono 3 (`int arg`, `const char **argv`, `const char **envp`) e si identificano 8 variabili in totale (`hModule`, `Data`, `var_117`, `var_8`, `var_4`, `argc`, `argv`, `envp`) come dimostrato dallo screen sottostante.

```
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h
```

Successivamente ci è stato chiesto di scoprire in quante sezione fosse suddiviso il file al suo interno. Ci sono 4 sezioni trovate facendo click su “view”, open subviewers e segments (`.text`, `.idata`, `.rdata`, `.data`) dove per esempio la sezione “`.rdata`” contiene i dati di sola lettura mentre `.idata` è usata per memorizzare le funzioni da DLL esterne.



Name	Start
.text	00000000004010
.idata	00000000004070
.rdata	00000000004070
.data	00000000004080

Ci è stato chiesto infine quali librerie importa il file. Le librerie che importa sono 2: `kernel32.dll` e `advapi32.dll`. Considerando che all'interno della sezione ci sono API come la `LockResource`, `LoadResource`, `FindResource` e `SizeofResource` sono portato a pensare che il Malware sia un `Dropper` ovvero è un programma malevolo al cui interno contiene il Malware.

000000...	RegSetValueExA	ADVAPI32
000000...	RegCreateKeyExA	ADVAPI32
000000...	SizeofResource	KERNEL32
000000...	LockResource	KERNEL32
000000...	LoadResource	KERNEL32
000000...	VirtualAlloc	KERNEL32
000000...	GetModuleFileNameA	KERNEL32
000000...	GetModuleHandleA	KERNEL32
000000...	FreeResource	KERNEL32
000000...	FindResourceA	KERNEL32
000000...	CloseHandle	KERNEL32
000000...	GetCommandLineA	KERNEL32
000000...	GetVersion	KERNEL32
000000...	ExitProcess	KERNEL32
000000...	HeapFree	KERNEL32
000000...	GetLastError	KERNEL32
000000...	WriteFile	KERNEL32
000000...	TerminateProcess	KERNEL32
000000...	GetCurrentProcess	KERNEL32
000000...	UnhandledExceptionFilter	KERNEL32
000000...	FreeEnvironmentStringsA	KERNEL32
000000...	FreeEnvironmentStringsW	KERNEL32

Dopodichè sono passato all'analisi delle varie locazioni di memoria richieste.

-Lo scopo della funzione chiamata alla locazione di memoria 00401021 è RegCreateKeyExA cioè creare una chiave di registro.

-L'oggetto rappresentato nella locazione 00401017 è molto probabilmente la schermata di login di windows NT,XP ecc ecc.

-Il significato delle istruzioni tra gli indirizzi 00401027 e 00401029 quindi:

```
test eax,eax
jz short loc_401032
```

Significa che viene fatta una comparazione tra eax e eax se è 0 viene fatto un jump alla locazione 401032 con un jz ovvero jump zero.

In pseudo codice C potrebbe essere: if (eax==0) fai questo

else salta a loc\_401032

il valore del parametro ValueName della locazione 00401047 è gina.dll

Infine sono passato all'analisi dinamica mediante procmon, avviandolo, resettando tutti i filtri come suggerito, avviando il malware, lasciando che agisca per un po' di tempo e stoppando la cattura. Ho riscontrato che è stato generato un file chiamato msgina32.dll, il nome Gina.dll nello specifico viene associato alla pagina di login utente di Windows NT/XP. La mia idea attualmente è che questo file possa essere la resilienza del malware in questione, ovvero si riavvia ogni volta che viene fatto un login nella macchina, o comunque vengano caricati i dati utente.



virustotal.com/gui/file/f8a4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9/community

bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9

51 / 71

Community Score

51/71 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

f8a4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9

msgina32.dll

Size: 6.50 KB | Last Modification Date: 19 days ago

peidl detect-debug-environment armadillo c/c++

DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY **COMMUNITY 4**

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Voting details (2)

anonymous

9 years ago

-1

anonymous

12 years ago

-1

Comments (2)

PeppeP1

10 days ago

This malware is a credential stealer and he use msgina32.dll to take your credentials and save it all in a file system named msutil32.sys in the following path:  
%SystemRoot%\System32\msutil32.sys

Names

Names with which this file has been submitted or seen in the wild

msgina32.dll

dropped\_11-01.exe

tgad.dll

Lab11-01\_rsrc.dll

f8a4f61bccd5bab1\_msgina32.dll

7ce4f799946f0fa44e5b2b5e6a702f27.vir

LEHONGHAI-TGAD0.exe

UPN (1).dll

f8a4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9.bin

lab11-01-resource-BINARY\_TGAD.exe

Capabilities

— Host-Interaction

Create or open registry key

Terminate process

Get common file path

Set registry value

Terminate process

Get common file path

Set registry value

— Persistence

Persist via GinaDLL registry key

— Linking

Link function at runtime on Windows



virustotal.com/gui/file/fba4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9/detection

fba4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9

51 / 71  
Community Score

61/71 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

fba4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9  
msgina32.dll

Size 6.50 KB Last Modification Date 19 days ago

pe32 detect-debug-environment armadillo ide

DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan:fragtor/tiggre Threat categories trojan Family labels fragtor tiggre

Security vendors' analysis

Alibaba	Trojan:Win32/Tiggre.38765a16	AliCloud	Trojan.Win.Generic.F3be1728
ALYac	GenVariant.Fragtor.510142	Antiy-AVL	Trojan/Win32.FakeGina
Arcabit	Trojan.Fragtor.D/C8BE	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	HEUR/AGEN.1326250
BitDefender	GenVariant.Fragtor.510142	BitDefenderTheta	Gen:NN_ZedialF.36802.aq4@uocirOb
Bkav Pro	W32.Common.148/C8BC	ClamAV	Win.Trojan.Agent-595082
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInSight	MALICIOUS
DrWeb	BackDoor.Sliggen.1689	Emsisoft	GenVariant.Fragtor.510142 (B)

Do you want to automate checks?

### MITRE ATT&CK Tactics and Techniques

- Execution** TA0002
  - Shared Modules T1129
    - Link function at runtime on Windows
- Persistence** TA0003
  - Event Triggered Execution T1546
    - Persist via GinaDLL registry key
  - DLL Side-Loading T1574.002
    - Tries to load missing DLLs
- Privilege Escalation** TA0004
  - Event Triggered Execution T1546
    - Persist via GinaDLL registry key
  - DLL Side-Loading T1574.002
    - Tries to load missing DLLs
- Defense Evasion** TA0005
  - Rundll32 T1218.011
    - Runs a DLL by calling functions
  - Virtualization/Sandbox Evasion T1497
    - Checks if the current process is being debugged
  - DLL Side-Loading T1574.002
    - Tries to load missing DLLs
- Discovery** TA0007
  - System Information Discovery T1082
    - Reads software policies