

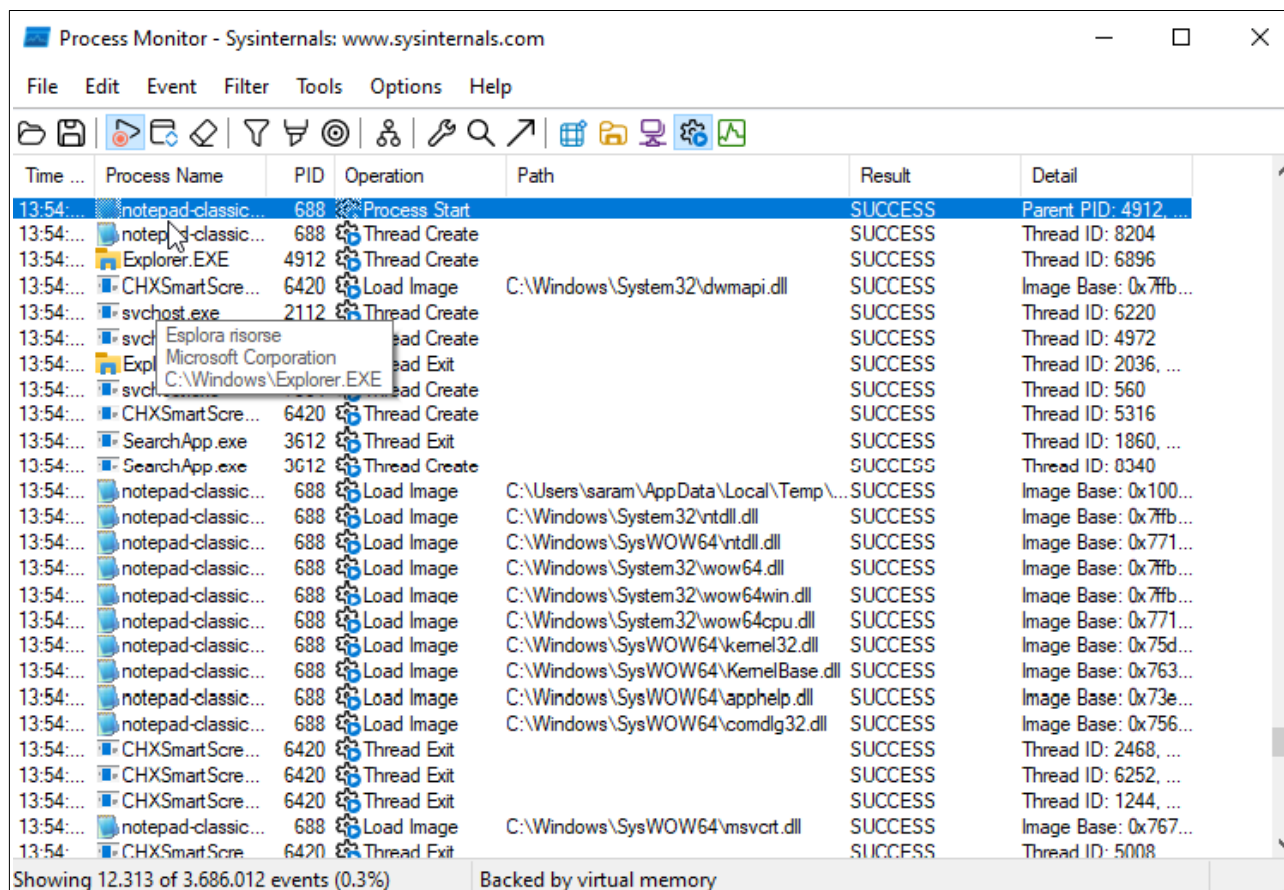
Report Analisi dinamica basica W22D1

In questo esercizio dovremo eseguire l'analisi dinamica del file fornito per studiarne il comportamento.

Prerequisiti:

- VM di Windows 10;
- Strumenti per l'analisi dinamica dei file come Procmon;
- Isolamento della macchina dopo aver scaricato il file malevolo.

Step 1 Una volta scaricato il file ed averlo decompresso in un ambiente sicuro possiamo procedere ad avviare Procmon e successivamente eseguire il file notepad-classico.exe .
Noteremo subito controllando i processi una riga contenente il nome del file malevolo e la dicitura process start SUCCESS (PID 688), questo implica che il file è stato avviato con successo.
Possiamo anche vedere che il file è stato segnalato dall'antivirus come riportato nella riga CHXSmartScreen (PID 6420).



Time ...	Process Name	PID	Operation	Path	Result	Detail
13:54:...	notepad-classic...	688	Process Start		SUCCESS	Parent PID: 4912, ...
13:54:...	notepad-classic...	688	Thread Create		SUCCESS	Thread ID: 8204
13:54:...	Explorer.EXE	4912	Thread Create		SUCCESS	Thread ID: 6896
13:54:...	CHXSmartScre...	6420	Load Image	C:\Windows\System32\dwmapi.dll	SUCCESS	Image Base: 0x7ffb...
13:54:...	svchost.exe	2112	Thread Create		SUCCESS	Thread ID: 6220
13:54:...	svchost.exe	2112	Thread Create		SUCCESS	Thread ID: 4972
13:54:...	svchost.exe	2112	Thread Exit		SUCCESS	Thread ID: 2036, ...
13:54:...	svchost.exe	2112	Thread Create		SUCCESS	Thread ID: 560
13:54:...	CHXSmartScre...	6420	Thread Create		SUCCESS	Thread ID: 5316
13:54:...	SearchApp.exe	3612	Thread Exit		SUCCESS	Thread ID: 1860, ...
13:54:...	SearchApp.exe	3612	Thread Create		SUCCESS	Thread ID: 8340
13:54:...	notepad-classic...	688	Load Image	C:\Users\saram\AppData\Local\Temp\...	SUCCESS	Image Base: 0x100...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffb...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x771...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffb...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffb...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x771...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75d...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x763...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x73e...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\comdlg32.dll	SUCCESS	Image Base: 0x756...
13:54:...	CHXSmartScre...	6420	Thread Exit		SUCCESS	Thread ID: 2468, ...
13:54:...	CHXSmartScre...	6420	Thread Exit		SUCCESS	Thread ID: 6252, ...
13:54:...	CHXSmartScre...	6420	Thread Exit		SUCCESS	Thread ID: 1244, ...
13:54:...	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x767...
13:54:...	CHXSmartScre...	6420	Thread Exit		SUCCESS	Thread ID: 5008

Showing 12,313 of 3,686,012 events (0.3%) Backed by virtual memory

Step 2 Applichiamo i filtri adatti per poter visualizzare solamente i processi relativi a notepad-classico.exe, come possiamo notare dall'immagine sottostante, il programma richiede accesso a svariate librerie di sistema, una in particolare è sospetta: wininet.dll, questa libreria in particolare serve ad accedere ad internet e normalmente un'applicazione come Notepad non avrebbe nessun bisogno di creare questo processo. Tutte le operazioni eseguite da notepad-classico.exe sono contrassegnate con SUCCESS.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
13:54:53.0047750	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: 0x762b0000, Image Size: 0x7b000
13:54:53.0051153	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x75030000, Image Size: 0x49000
13:54:53.0073264	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x76bd0000, Image Size: 0x5da000
13:54:53.0093654	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x75e40000, Image Size: 0x7d000
13:54:53.0097963	notepad-classic...	688	Load Image	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	Image Base: 0x74c10000, Image Size: 0x210000
13:54:53.0098698	notepad-classic...	688	Load Image	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	Image Base: 0x9c0000, Image Size: 0x210000
13:54:53.0107216	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x75110000, Image Size: 0x77000
13:54:53.0111272	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	Image Base: 0x765f0000, Image Size: 0x19000
13:54:53.0144752	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\winspool.drv	SUCCESS	Image Base: 0x74fb0000, Image Size: 0x7d000
13:54:53.0441669	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x75620000, Image Size: 0x25000
13:54:53.1090907	notepad-classic...	688	Thread Create		SUCCESS	Thread ID: 5168
13:54:53.1108170	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Image Base: 0x74f30000, Image Size: 0x74000
13:54:53.1113570	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x761e0000, Image Size: 0x63000
13:54:53.1118838	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x75190000, Image Size: 0xf0000
13:54:53.1140305	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x73930000, Image Size: 0x455000
13:54:53.1210307	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Image Base: 0x744c0000, Image Size: 0xca000
13:54:53.1229094	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\mscftf.dll	SUCCESS	Image Base: 0x76a30000, Image Size: 0xd4000
13:54:53.1235935	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x75ec0000, Image Size: 0x96000
13:54:53.1262416	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x75c60000, Image Size: 0xe3000
13:54:53.1336245	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x74ed0000, Image Size: 0x52000
13:54:53.1384354	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\NapiNSP.dll	SUCCESS	Image Base: 0x74eb0000, Image Size: 0x11000
13:54:53.1413462	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\TextShaping...	SUCCESS	Image Base: 0x73890000, Image Size: 0x95000
13:54:53.1443539	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\pnprpnsd.dll	SUCCESS	Image Base: 0x74e90000, Image Size: 0x16000
13:54:53.1474602	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\wsbth.dll	SUCCESS	Image Base: 0x74e50000, Image Size: 0x16000
13:54:53.1486545	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\ntapi.dll	SUCCESS	Image Base: 0x74e30000, Image Size: 0x16000
13:54:53.1542830	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\IPHLPAPI.DLL	SUCCESS	Image Base: 0x74480000, Image Size: 0x32000
13:54:53.1561503	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\dnsapi.dll	SUCCESS	Image Base: 0x73800000, Image Size: 0x90000
13:54:53.1592208	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\ansi.dll	SUCCESS	Image Base: 0x75f60000, Image Size: 0x7000
13:54:53.1672269	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\winmr.dll	SUCCESS	Image Base: 0x74e80000, Image Size: 0xe000
13:54:53.1685534	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\WPUCLN I...	SUCCESS	Image Base: 0x73a0000, Image Size: 0x58000
13:54:53.1757313	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\rsadhip.dll	SUCCESS	Image Base: 0x74c00000, Image Size: 0x8000
13:54:53.2180205	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\kernel.appco...	SUCCESS	Image Base: 0x73f80000, Image Size: 0xf000
13:54:53.2186303	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\bcryptprimitiv...	SUCCESS	Image Base: 0x76060000, Image Size: 0x5f000
13:54:53.2474486	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\TextInputFra...	SUCCESS	Image Base: 0x736e0000, Image Size: 0xb9000
13:54:53.2494936	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\CoreMessagi...	SUCCESS	Image Base: 0x73640000, Image Size: 0x9b000
13:54:53.2500817	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\CoreUIComp...	SUCCESS	Image Base: 0x733c0000, Image Size: 0x27f000
13:54:53.2546233	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS	Image Base: 0x74450000, Image Size: 0x29000
13:54:53.2568935	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x732e0000, Image Size: 0xdd000
13:54:53.2569915	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x49000000, Image Size: 0xdd000
13:54:53.2575314	notepad-classic...	688	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS	Image Base: 0x49e0000, Image Size: 0xdd000
Showing 73 of 3.949.320 events (0.0%)			Backed by virtual memory			

Step 3 Cambiando filtro su Procmon possiamo vedere i processi relativi alle cartelle avviati da notepad-classico.exe, il malware crea continuamente nuovi file e richiede di leggerne altri. È probabile che in questa fase il malware stia eseguendo attività di ricognizione sul sistema.

Process Monitor - Sysinternals: www.sysinternals.com

FileEditEventFilterToolsOptionsHelp

Facoltativo

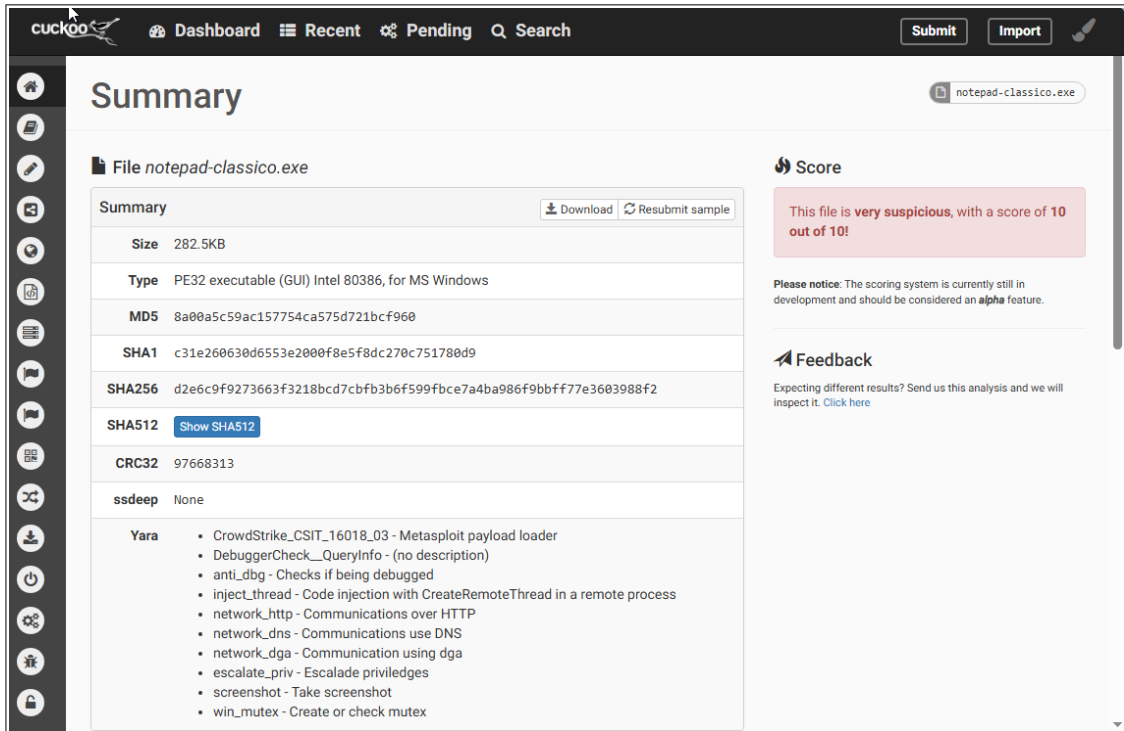
Il comportamento del programma notepad-classico.exe è sicuramente sospetto, in quanto si tratta di un trojan e cioè un programma appare come legittimo ma che in realtà esegue in background altri processi non standard.

Si tratta di un programma che serve ad aprire una backdoor sull'host per poi fornire il controllo della macchina ad un attore malevolo online, visto però che il programma è stato aperto in un ambiente controllato senza accesso ad internet, non si è potuto osservare appieno il comportamento del malware.

Pratica Extra

Caricare il file su una sandbox ed osservare il risultato.

Cuckoo



The screenshot shows the Cuckoo Sandbox web interface. The top navigation bar includes links for Dashboard, Recent, Pending, and Search, along with Submit and Import buttons. The main content area is titled "Summary" and displays details for the file "notepad-classico.exe".

File notepad-classico.exe

Summary [Download] [Resubmit sample]

Property	Value
Size	282.5KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8a00a5c59ac157754ca575d721bcf960
SHA1	c31e260630d6553e200f8e5f8dc270c751780d9
SHA256	d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2
SHA512	[Show SHA512]
CRC32	97668313
ssdeep	None
Yara	<ul style="list-style-type: none">CrowdStrike_CSIT_16018_03 - Metasploit payload loaderDebuggerCheck_QueryInfo - (no description)anti_dbg - Checks if being debuggedinject_thread - Code injection with CreateRemoteThread in a remote processnetwork_http - Communications over HTTPnetwork_dns - Communications use DNSnetwork_dga - Communication using dgaescalate_priv - Escalade privilegesscreenshot - Take screenshotwin_mutex - Create or check mutex

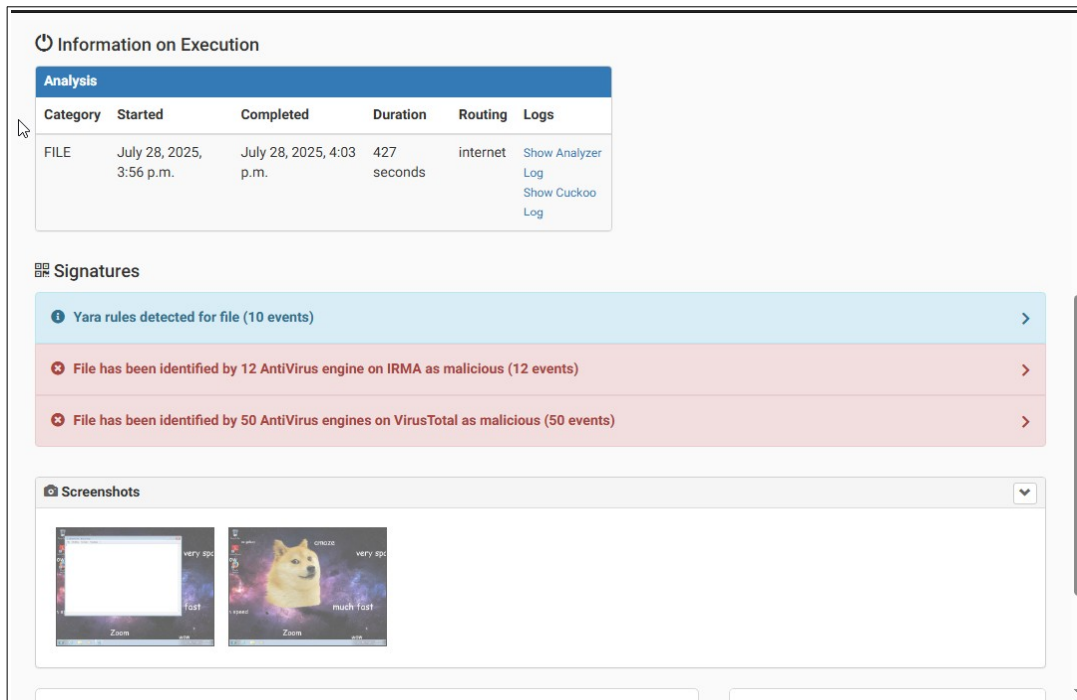
Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)



The screenshot shows the "Information on Execution" page in the Cuckoo Sandbox web interface. It includes a table of analysis results, a section for signatures, and a section for screenshots.

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
FILE	July 28, 2025, 3:56 p.m.	July 28, 2025, 4:03 p.m.	427 seconds	internet	Show Analyzer Log Show Cuckoo Log

Signatures

- Yara rules detected for file (10 events)
- File has been identified by 12 AntiVirus engine on IRMA as malicious (12 events)
- File has been identified by 50 AntiVirus engines on VirusTotal as malicious (50 events)

Screenshots

Two screenshots are displayed side-by-side. The left screenshot shows a Windows desktop with a taskbar and a window titled "Zoom". The right screenshot shows a similar desktop environment with a taskbar and a window titled "Zoom".

Virus Total

50

/ 70

Community Score

50/70 security vendors flagged this file as malicious

Reanalyze Similar More

d2e6c9f9273663f3218bcd7cbfb3b6f599fbc7a4ba986f9bbff77e3603988f2

Size282.50 KB

Last Analysis Date2 days ago

NOTEPAD.EXE

peexe

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY5

Join our Community

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

Popular threat label

trojan.rozena/meterpreter

Threat categories

trojan

Family labels

rozena

meterpreter

sworot

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C593931	AliCloud	Trojan:Win/Meterpreter.AA(dyn)
ALYac	Win32.Rozena.B	Antiy-AVL	Trojan/WIN32.Meterpreter.a
Avast	Win32.Generic.B	Avast-Web	Unsubf

Basic properties

MD5

8a00a5c59ac157754ca575d721bcf960

SHA-1

c31e260630d6553e2000f8e5f8dc270c751780d9

SHA-256

d2e6c9f9273663f3218bcd7cbfb3b6f599fbc7a4ba986f9bbff77e3603988f2

Vhash

0250666d155e6d5550701090018003916fz42z4afz

Authentihash

305d46f94f2c4f6165c684b56a7304810bf83884a2c5bce90de928006391585a

Imphash

419c3fe8c1ccfea9336b96f74f0951dd

Rich PE header hash

ec3976d3652ad6f6bd790c99374b79a6

SSDEEP

6144:GqNSDyDIAthp2/G1xu5ZN3VIX9lJja7rJthp:9SDyntj2/UurOX9XljjQtj

TLSH

T124546A01A2D2D075E0B7523415BB6B220F7EBD315E3A8BCF6BA46D4E5E30580EB25727

File type

Win32 EXE executable windows win32 pe peexe

Magic

PE32 executable (GUI) Intel 80386, for MS Windows

TrID

Win32 Executable MS Visual C++ (generic) (37.8%) | Microsoft Visual C++ compiled executable (generic) (20%) | Wi...

DetectItEasy

PE32 | Compiler: MASM (7.01.4035) | Linker: Microsoft Linker (7.10.4035)

Magika

PEBIN

File size

282.50 KB (289280 bytes)

Activity Summary

Download Artifacts Full Reports Help

Detections

1 MALWARE

IDS Rules

NOT FOUND

Dropped Files

8 OTHER

Mitre Signatures

3 MEDIUM 15 INFO

Sigma Rules

NOT FOUND

Network comms

2 DNS 7 IP

Dynamic Analysis Sandbox Detections

The sandbox CAPE Sandbox flags this file as: MALWARE