

IEXPLORE.EXE

ANALISI DINAMICA:

Avviamo Process Explorer

Avviamo AupdateDNS e avviamo il DNS filtro che intercetterà le chiamate della rete (mettiamo ip macchina locale)

Avviare RegShot ed effettuare uno snapshot delle chiavi (t0)

Avviare Procmon

Avviare Wireshark

Avviare IEXPLORE.exe

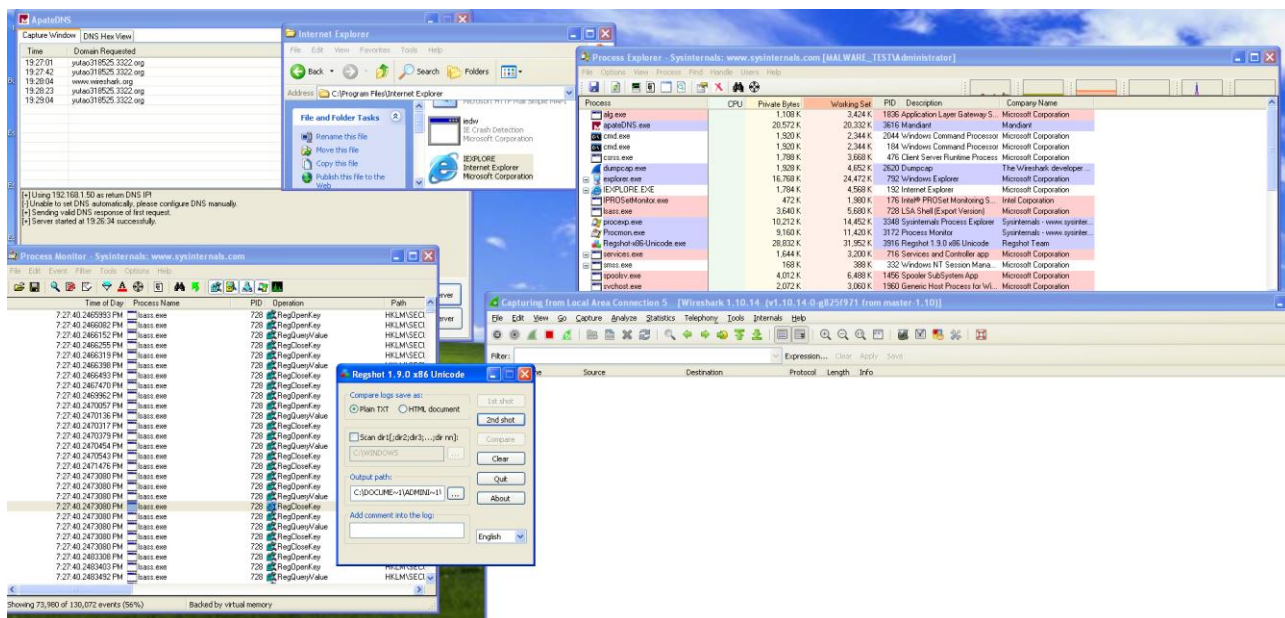
Stop catture Wireshark

Stop catture Procmon

Secondo snapshot Regshot (t1)

Stop server AupdateDNS

Stop Process Explorer



VirusTotal non rileva problematiche nel file

<https://www.virustotal.com/gui/file/814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e/behavior>

0

/ 71

File distributed by Microsoft

814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e

Size91.00 KB

Last Analysis Date5 months ago

EXE

peexeknown-distributortrusted

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY15

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

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
BitDefender	Undetected	ClamAV	Undetected
BitDefender	Undetected	CrowdStrike Falcon	Undetected
BitDefender	Undetected	Cylance	Undetected
BitDefender	Undetected	Cyren	Undetected
BitDefender	Undetected	DrWeb	Undetected
BitDefender	Undetected	Emsisoft	Undetected
BitDefender	Undetected	ESET-NOD32	Undetected
BitDefender	Undetected	Fortinet	Undetected
BitDefender	Undetected	Google	Undetected
BitDefender	Undetected	Ikarus	Undetected
BitDefender	Undetected	K7AntiVirus	Undetected

Non si notano chiamate sospette al DNS

ApateDNS

Capture WindowDNS Hex View

Time	Domain Requested	DNS Return...
19:28:23	yutao318525.3322.org	FOUND
19:29:04	yutao318525.3322.org	FOUND
19:29:45	www.microsoft.com	FOUND
19:29:45	yutao318525.3322.org	FOUND
19:30:26	yutao318525.3322.org	FOUND
19:30:40	www.microsoft.com	FOUND
19:31:07	yutao318525.3322.org	FOUND
12:55:51	auto.search.msn.com	FOUND
12:55:52	www.127.0.0.1.com	FOUND
12:55:53	www.127.0.0.1.org	FOUND
12:55:53	yutao318525.3322.org	FOUND
12:55:54	www.127.0.0.1.net	FOUND
12:55:55	www.127.0.0.1.edu	FOUND

[+] Using 192.168.1.50 as return DNS IP!

[!] Unable to set DNS automatically, please configure DNS manually.

[+] Sending valid DNS response of first request.

[+] Server started at 12:55:49 successfully.

DNS Reply IP (Default: Current Gateway/DNS):192.168.1.50

of NXDOMAIN's:0

Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter - Packet Sch

Start Server

Stop Server

Sono state cambiate delle chiavi di registro

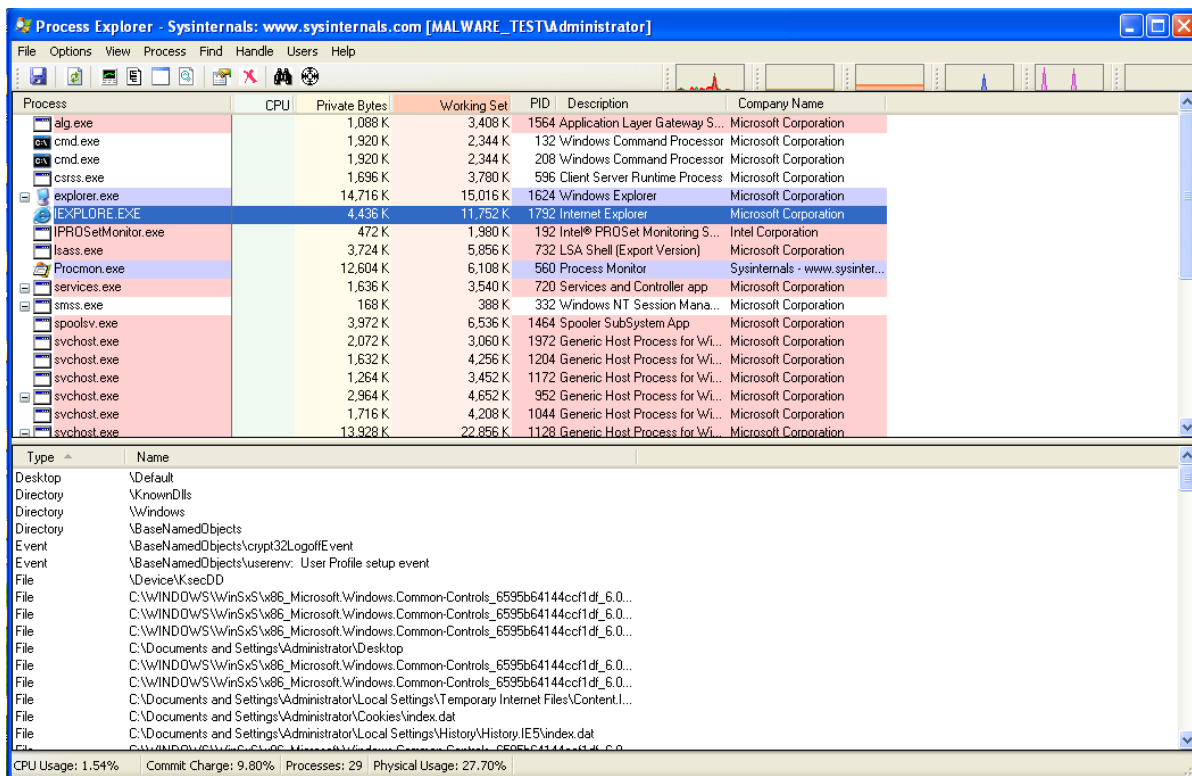
```
-res-x86_0012 - Notepad
File Edit Format View Help
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/10/28 12:14:31 , 2023/10/28 12:14:52
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

-----
Values modified: 1
-----
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 1F F2 3A FD E1 21 7A 68 E7 73 30 62 C4 ED B
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 2C BE 6C EF AD 80 98 F1 A6 C8 CF D5 70 81 0
-----
Total changes: 1
-----
```

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed

La chiave è progettata per puntare al driver basato su DLL per l'acceleratore di crittografia basato su hardware. Una DLL di questo tipo ha accesso alle chiavi crittografiche archiviate sulla macchina NT e, pertanto, la DLL Trojan potrebbe ottenere l'accesso alle chiavi crittografiche.

Process explorer non rileva side proces lanciati dall'ex



The screenshot shows Process Explorer with a list of processes and a file system view below. The processes list includes:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
alg.exe		1,088 K	3,408 K	1564	Application Layer Gateway S...	Microsoft Corporation
cmd.exe		1,920 K	2,344 K	132	Windows Command Processor	Microsoft Corporation
cmd.exe		1,920 K	2,344 K	208	Windows Command Processor	Microsoft Corporation
csrss.exe		1,696 K	3,780 K	596	Client Server Runtime Process	Microsoft Corporation
explorer.exe		14,716 K	15,016 K	1624	Windows Explorer	Microsoft Corporation
IEEXPLORE.EXE		4,436 K	11,752 K	1792	Internet Explorer	Microsoft Corporation
IPROSetMonitor.exe		472 K	1,980 K	192	Intel® PROSet Monitoring S...	Intel Corporation
lsass.exe		3,724 K	5,856 K	732	LSA Shell (Export Version)	Microsoft Corporation
Procmon.exe		12,604 K	6,108 K	560	Process Monitor	Sysinternals - www.sysinter...
services.exe		1,636 K	3,540 K	720	Services and Controller app	Microsoft Corporation
smss.exe		168 K	388 K	332	Windows NT Session Mana...	Microsoft Corporation
spoolsv.exe		3,972 K	6,536 K	1464	Spooler SubSystem App	Microsoft Corporation
svchost.exe		2,072 K	3,060 K	1972	Generic Host Process for Wl...	Microsoft Corporation
svchost.exe		1,632 K	4,256 K	1204	Generic Host Process for Wl...	Microsoft Corporation
svchost.exe		1,264 K	3,452 K	1172	Generic Host Process for Wl...	Microsoft Corporation
svchost.exe		2,964 K	4,652 K	952	Generic Host Process for Wl...	Microsoft Corporation
svchost.exe		1,716 K	4,208 K	1044	Generic Host Process for Wl...	Microsoft Corporation
svchost.exe		13,928 K	22,856 K	1128	Generic Host Process for Wl...	Microsoft Corporation

The file system view shows the following structure:

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\crypt32LogoffEvent
Event	\BaseNamedObjects\userenv: User Profile setup event
File	\Device\KsecDD
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\Documents and Settings\Administrator\Desktop
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.I...
File	C:\Documents and Settings\Administrator\Cookies\index.dat
File	C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...

At the bottom, system statistics are shown: CPU Usage: 1.54%, Commit Charge: 9.80%, Processes: 29, Physical Usage: 27.70%.