

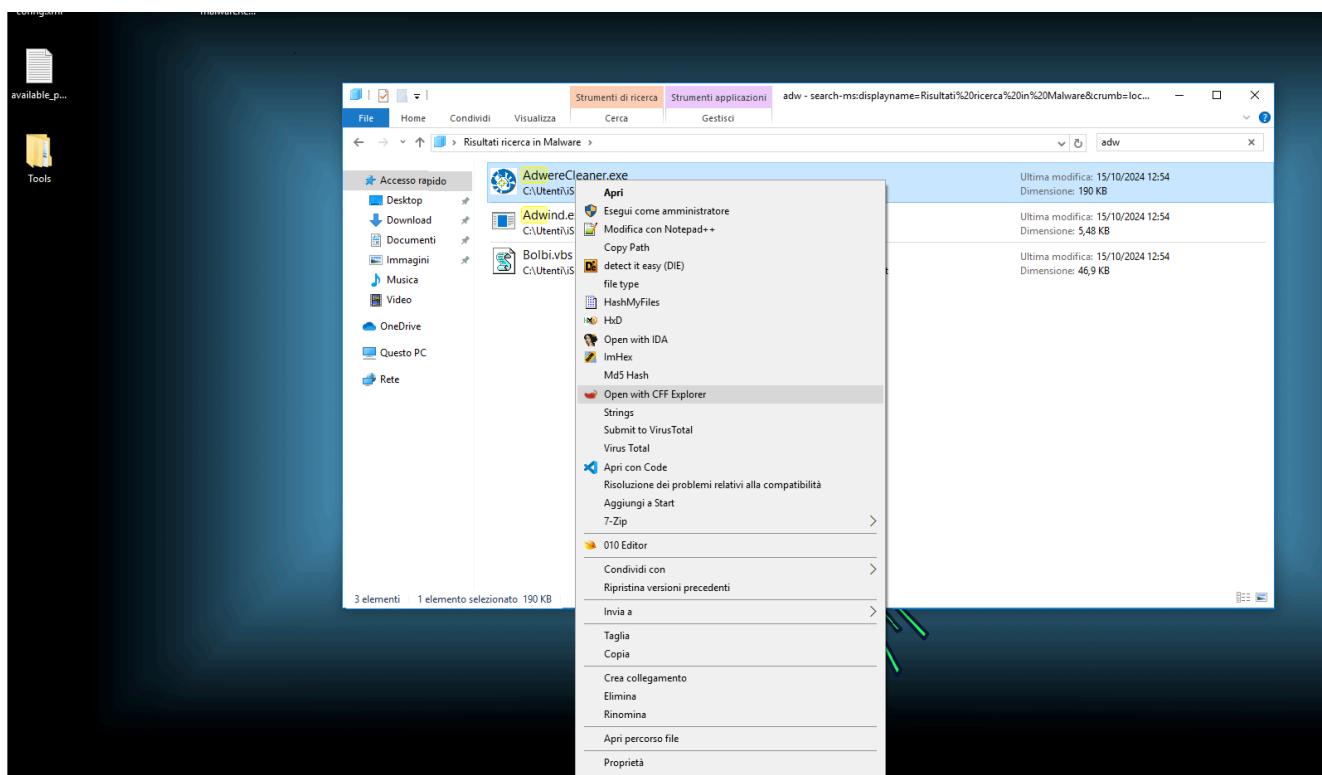
BW3 es.1 Adware Cleaner

Report AdwareCleaner.exe

Inizio Analisi con CFF Explorer

Floral icon **Tag:** #analisi #header #eseguibile

- Visualizzazione dettagliata del file sospetto in CFF Explorer, inclusi l'header e le proprietà del file.
- Rilevazione di potenziali indicatori di malware tramite la struttura del file eseguibile.



Verifica dell'Hash MD5

Floral icon **Tag:** #hash #md5 #analisi

- L'uso di AdwareCleaner per l'analisi dell'hash del file. I dettagli dell'hash confermano il file analizzato.

The screenshot shows the CFF Explorer VIII interface. On the left, there's a tree view of the file structure for 'File: AdwereCleaner.exe'. The right side displays detailed properties for the file, including its name, type, size, creation date, and MD5 hash. The MD5 hash is highlighted in blue.

Property	Value
File Name	C:\Users\iSushiLab\Desktop\Malware\rogues\AdwereCleaner.exe
File Type	Portable Executable 32
File Info	Nullsoft PiMP Stub -> SFX
File Size	190.82 KB (195400 bytes)
PE Size	75.50 KB (77312 bytes)
Created	Tuesday 15 October 2024, 11.54.18
Modified	Tuesday 15 October 2024, 11.54.18
Accessed	Tuesday 15 October 2024, 11.54.18
MD5	248AADD395FFA7FFB1670392A9398454
SHA-1	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5

Below the main table, there's another table with a single row:

Property	Value
Empty	No additional info available

Analisi VirusTotal

🌟 Tag: #virustotal #rilevamento #malware

- Il file sospetto è stato caricato su VirusTotal con vari motori antivirus che identificano il file come potenzialmente dannoso.
- Conferma di sospetti basati su rilevamenti di malware.

Security vendor	Detection	Family	Notes
AhnLab-V3	Dropper/Win32.Dapato.R137988	Alibaba	Hoax:MSIL/Porcupine.e666e97
Antiy-AVL	HackTool[Hoax]/MSIL.Agent	Arcabit	Trojan.Mint.Porcupine.ED5D10
Avast	Win32:FakeAV-FLW [Trj]	AVG	Win32:FakeAV-FLW [Trj]
Avira (no cloud)	JOKE/Agent.rlham	BitDefender	Gen:Heur.Mint.Porcupine.lu2@bOy2NApig
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.fakeav
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.FakeAV.17850

Sandbox Cuckoo

Tag: #sandbox #api #offuscamento

- Analisi in sandbox con Cuckoo dove sono monitorate funzioni API, come `NtProtectVirtualMemory` e `NtAllocateVirtualMemory`, tipicamente utilizzate dai malware per manipolare la memoria.

- Evidenze di tecniche di offuscamento tramite API che modificano la memoria del processo, indicando potenziali attività dannose.

Rapporto Completo Cuckoo

Tag: #cuckoo #fingerprinting #entropia

- Analisi completa su Cuckoo che evidenzia l'uso di funzioni di fingerprinting del sistema, controllo della memoria e comportamento del file eseguibile.
- Il file è identificato come sospetto con elevata entropia, suggerendo l'uso di compressione o crittografia.
- Rilevamenti antivirus confermano la presenza di attività potenzialmente malevole.

Run Windows (Old Instructions) Oracle VM VirtualBox

Cuckoo Sandbox Cuckoo Sandbox + cuckoo.certee/analysis/5378273/summary

Dashboard Recent Pending Search Submit Import

Allotates read-write-execute memory (usually to unpack itself) (43 events)

Time & API	Arguments	Status	Return	Repeated
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4995 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00000007fe0ff1000 process_handle: 0xffffffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4995 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00000007fe0ff1000 process_handle: 0xffffffffffffffffffff	1	0	0
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 region_size: 851968 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000000000002070000 allocation_type: 8192 (MEM_COMMIT) process_handle: 0xffffffffffffffffffff	1	0	0
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 region_size: 8192 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 1 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000000000002070000 allocation_type: 4995 (MEM_COMMIT) process_handle: 0xffffffffffffffffffff	1	0	0
	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0			

11:00 28/10/2024 CTRL+D (STRAY)

Run Windows (Old Instructions) Oracle VM VirtualBox

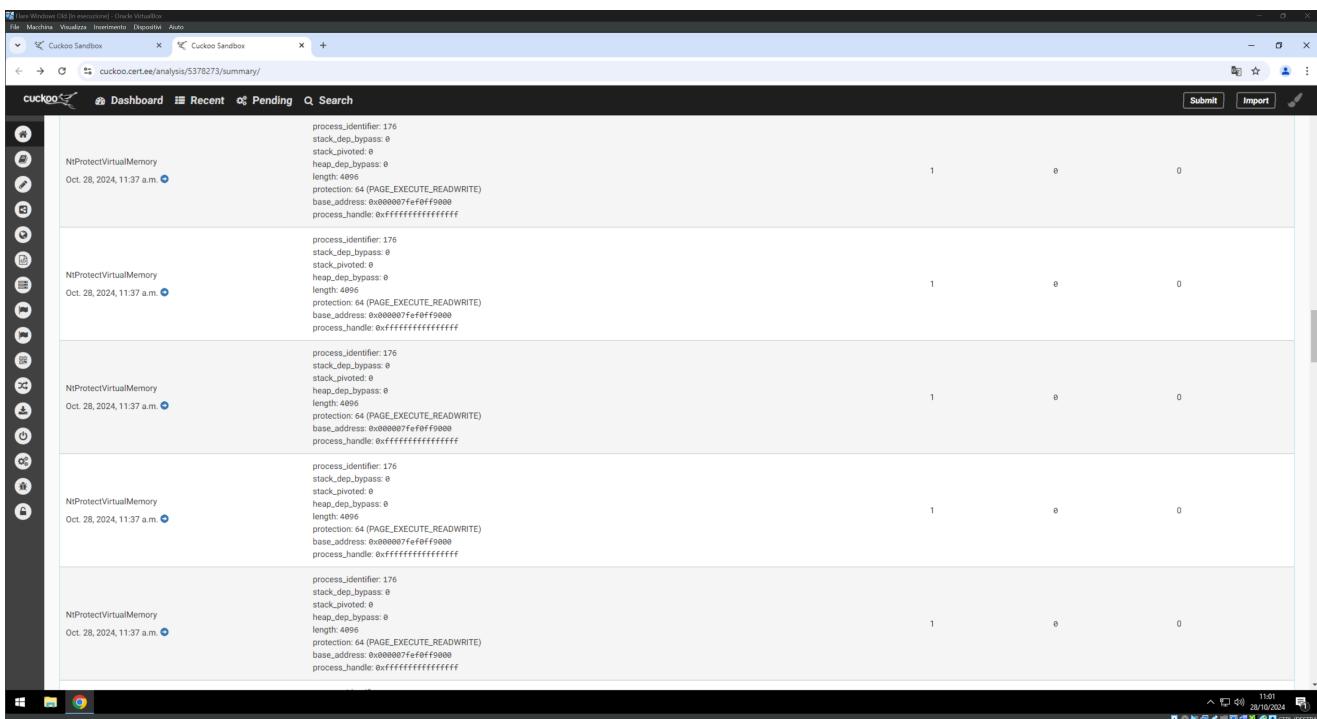
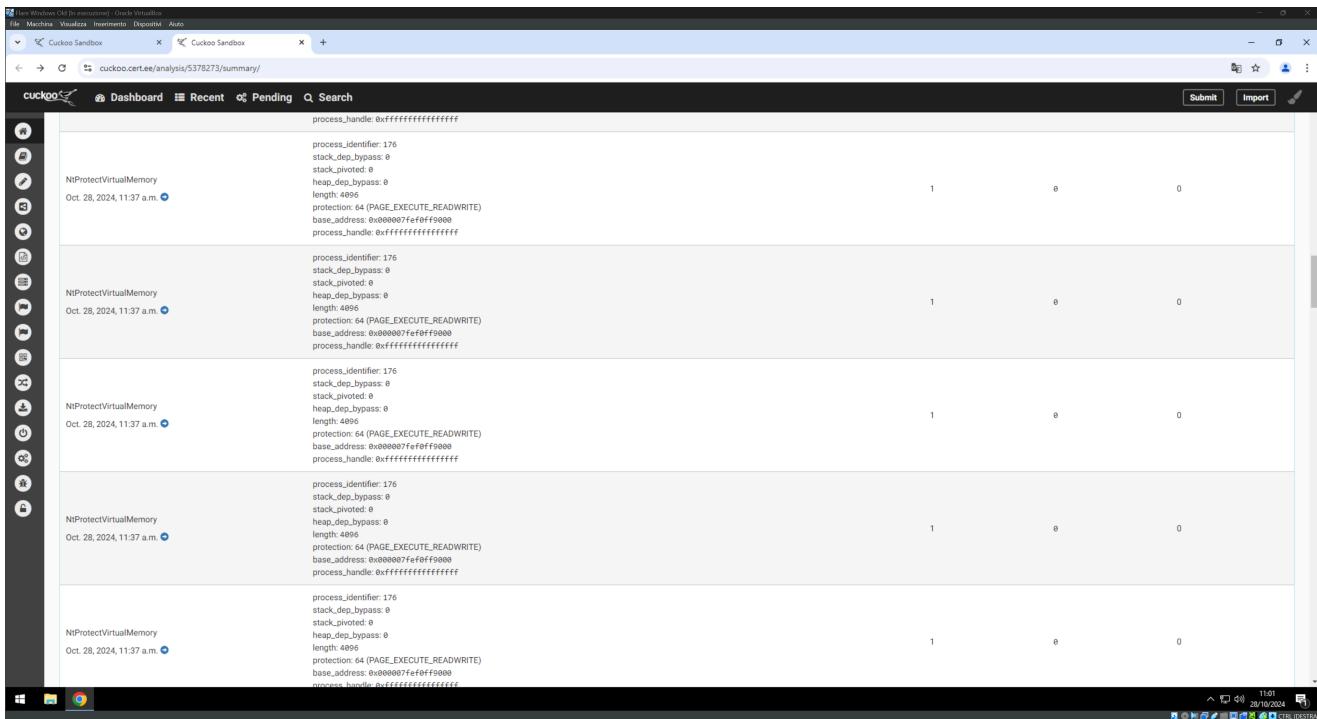
Cuckoo Sandbox Cuckoo Sandbox + cuckoo.certee/analysis/5378273/summary

Dashboard Recent Pending Search Submit Import

Allotates read-write-execute memory (usually to unpack itself) (43 events)

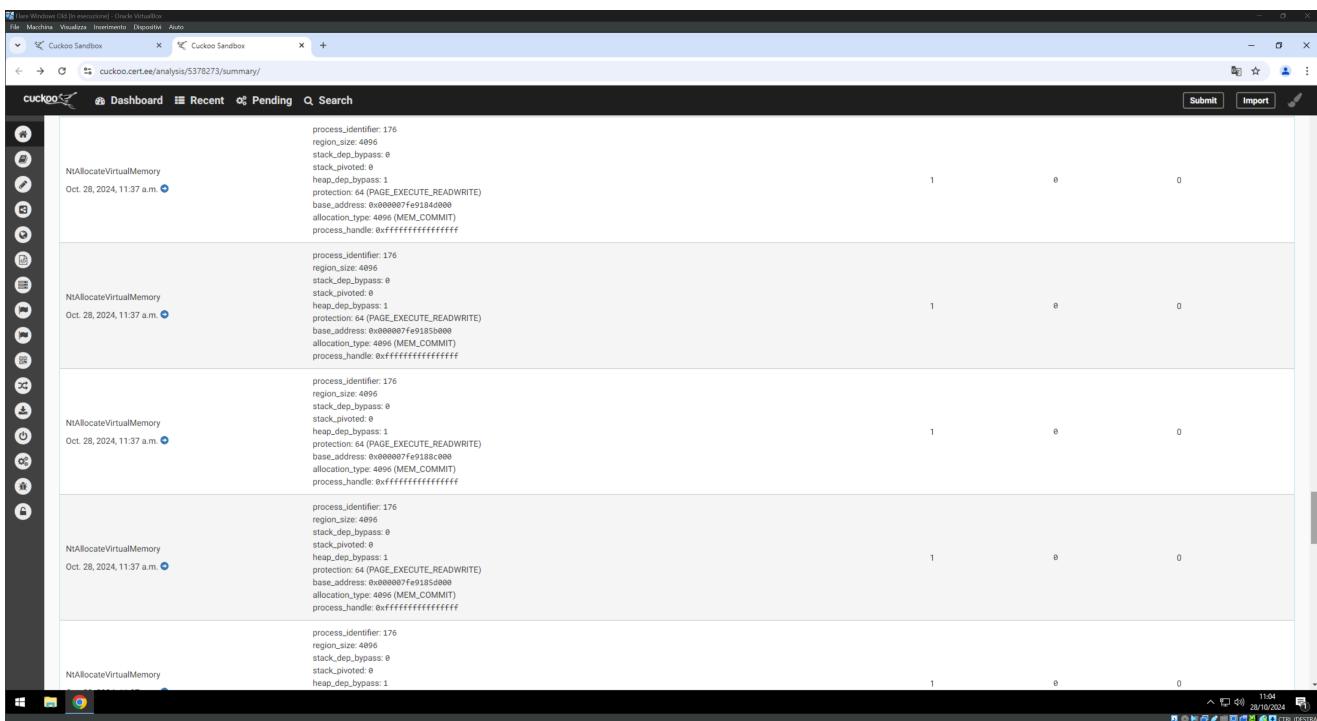
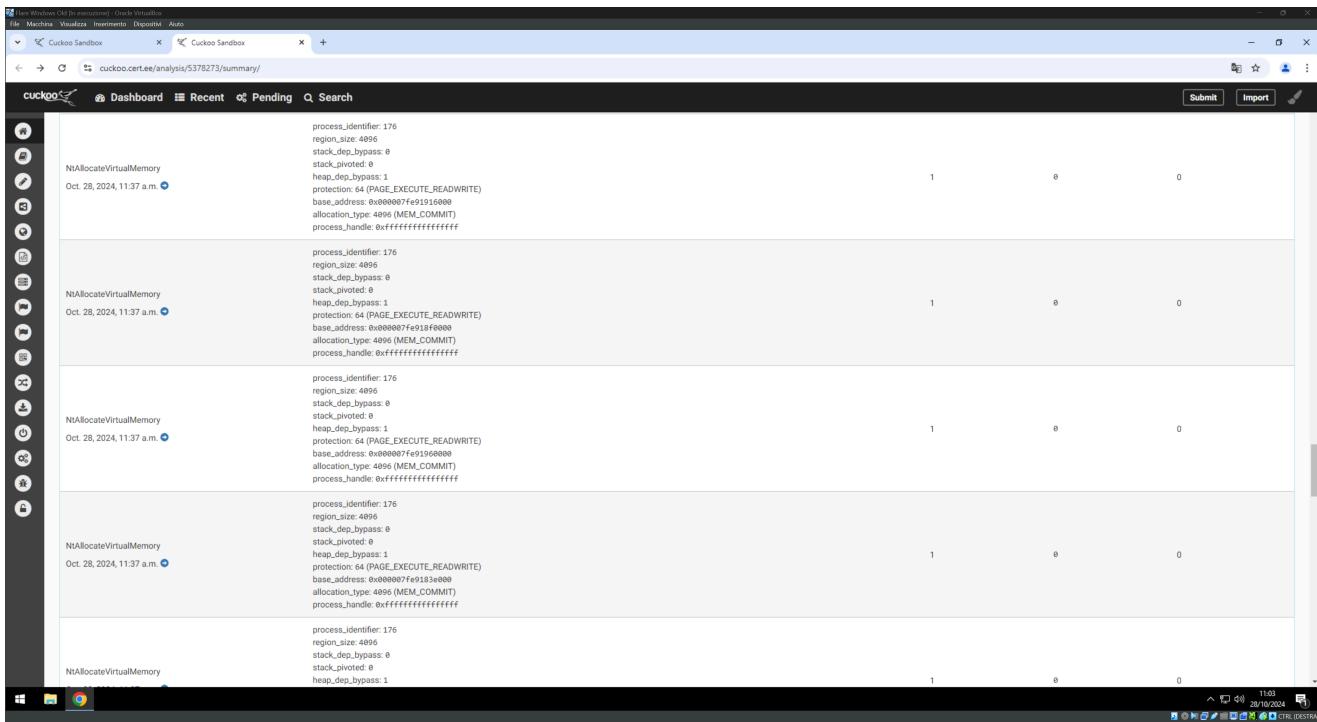
Time & API	Arguments	Status	Return	Repeated
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4995 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00000007fe0ff1000 process_handle: 0xffffffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4995 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00000007fe0ff1000 process_handle: 0xffffffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4995 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00000007fe0ff1000 process_handle: 0xffffffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4995 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00000007fe0ff1000 process_handle: 0xffffffffffffffffffff	1	0	0
	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4995 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00000007fe0ff1000 process_handle: 0xffffffffffffffffffff			

11:00 28/10/2024 CTRL+D (STRAY)



```
File Machine Visualize Instruments Dispositivo Auto
Cuckoo Sandbox Cuckoo Sandbox + 
cuckoo.certee/analysis/5378273/summary/
Dashboard Recent Pending Search Submit Import
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 65536
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 1056788 (MEM_RESERVE|MEM_TOP_DOWN)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 65536
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 1056788 (MEM_RESERVE|MEM_TOP_DOWN)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
Windows Taskbar 11:03 28/10/2024 CTRL (DESTRÁK)
```

```
File Machine Visualize Instruments Dispositivo Auto
Cuckoo Sandbox Cuckoo Sandbox + 
cuckoo.certee/analysis/5378273/summary/
Dashboard Recent Pending Search Submit Import
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 65536
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 1056788 (MEM_RESERVE|MEM_TOP_DOWN)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 65536
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 1056788 (MEM_RESERVE|MEM_TOP_DOWN)
process_handle: 0xfffffffffffffff
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m. 1 0 0
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x00000000fffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xfffffffffffffff
Windows Taskbar 11:03 28/10/2024 CTRL (DESTRÁK)
```



Cuckoo Sandbox						
Dashboard		Recent	Pending	Search	Submit	Import
cuckoo.cert.ee/analysis/5378273/summary/						
	NtAllocateVirtualMemory	process_identifier: 176 region_size: 4996 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 1 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x0000007fe9188d000 allocation_type: 4996 (MEM_COMMIT) process_handle: 0xfffffffffffffff	1	0	0	0
	NtAllocateVirtualMemory	process_identifier: 176 region_size: 1245184 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x0000000001ba0000 allocation_type: 8192 (MEM_RESERVE) process_handle: 0xfffffffffffffff	1	0	0	0
	NtAllocateVirtualMemory	process_identifier: 176 region_size: 6132 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 1 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x0000000001bb8000 allocation_type: 4996 (MEM_COMMIT) process_handle: 0xfffffffffffffff	1	0	0	0
	NtAllocateVirtualMemory	process_identifier: 176 region_size: 4996 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 1 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x0000007fe9181f000 allocation_type: 4996 (MEM_COMMIT) process_handle: 0xfffffffffffffff	1	0	0	0
	NtAllocateVirtualMemory	process_identifier: 176 region_size: 4996 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 1	1	0	0	0

File Windows Help (Esc) Machine Visualize Instrumentation Diagnostic Auto

Cuckoo Sandbox Cuckoo Sandbox +

cuckoo.cert.ee/analysis/5370273/summary/

cuckoo Dashboard Recent Pending Search Submit Import

NAllocateVirtualMemory process_identifier: 176
region_size: 4996
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 44 (PAGE_EXECUTE_READWRITE)
base_address: 0x0000007fe9184ee00
allocation_type: 4996 (MEM_COMMIT)
process_handle: 0xfffffffffffffff

NAllocateVirtualMemory process_identifier: 176
region_size: 4996
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 44 (PAGE_EXECUTE_READWRITE)
base_address: 0x0000007fe9184ef00
allocation_type: 4996 (MEM_COMMIT)
process_handle: 0xfffffffffffffff

NAllocateVirtualMemory process_identifier: 176
region_size: 4996
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 44 (PAGE_EXECUTE_READWRITE)
base_address: 0x0000007fe919a9000
allocation_type: 4996 (MEM_COMMIT)
process_handle: 0xfffffffffffffff

NAllocateVirtualMemory process_identifier: 176
region_size: 4996
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 44 (PAGE_EXECUTE_READWRITE)
base_address: 0x0000007fe919a9000
allocation_type: 4996 (MEM_COMMIT)
process_handle: 0xfffffffffffffff

Checks if process is being debugged by a debugger (2 events)

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosData) (1 event)

The screenshot shows the Cuckoo Sandbox analysis interface for a sample named 5378273. The main window displays a detailed event log. Key findings include:

- Checks if process is being debugged by a debugger (2 events)
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosData) (1 event)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory (1 event)
- The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)
- Creates executable files on the filesystem (1 event)
- Drops a binary and executes it (1 event)
- Drops an executable to the user AppData folder (1 event)
- Checks adapter addresses which can be used to detect virtual network interfaces (1 event)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)

The analysis interface includes tabs for Machine, Visualize, Instruments, and Disassembler, and features like Dashboard, Recent, Pending, and Search.

This screenshot shows the same Cuckoo Sandbox analysis interface for the same sample. The event log is expanded to show more details for specific findings:

- Drops an executable to the user AppData folder (1 event): C:\Users\Administrator\AppData\Local\6AdwCleaner.exe
- Checks adapter addresses which can be used to detect virtual network interfaces (1 event)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events):
 - section: {u'size_of_data': 0x0000b400, 'virtual_address': 0x00037000, 'entropy': 7.9152412068139935, 'name': 'usrsrc', 'virtual_size': 0x0000b268}
 - entropy: 7.9152412068139935
- File has been identified by 11 AntiVirus engine on IRMA as malicious (11 events)
- File has been identified by 55 AntiVirus engines on VirusTotal as malicious (50 out of 55 events)

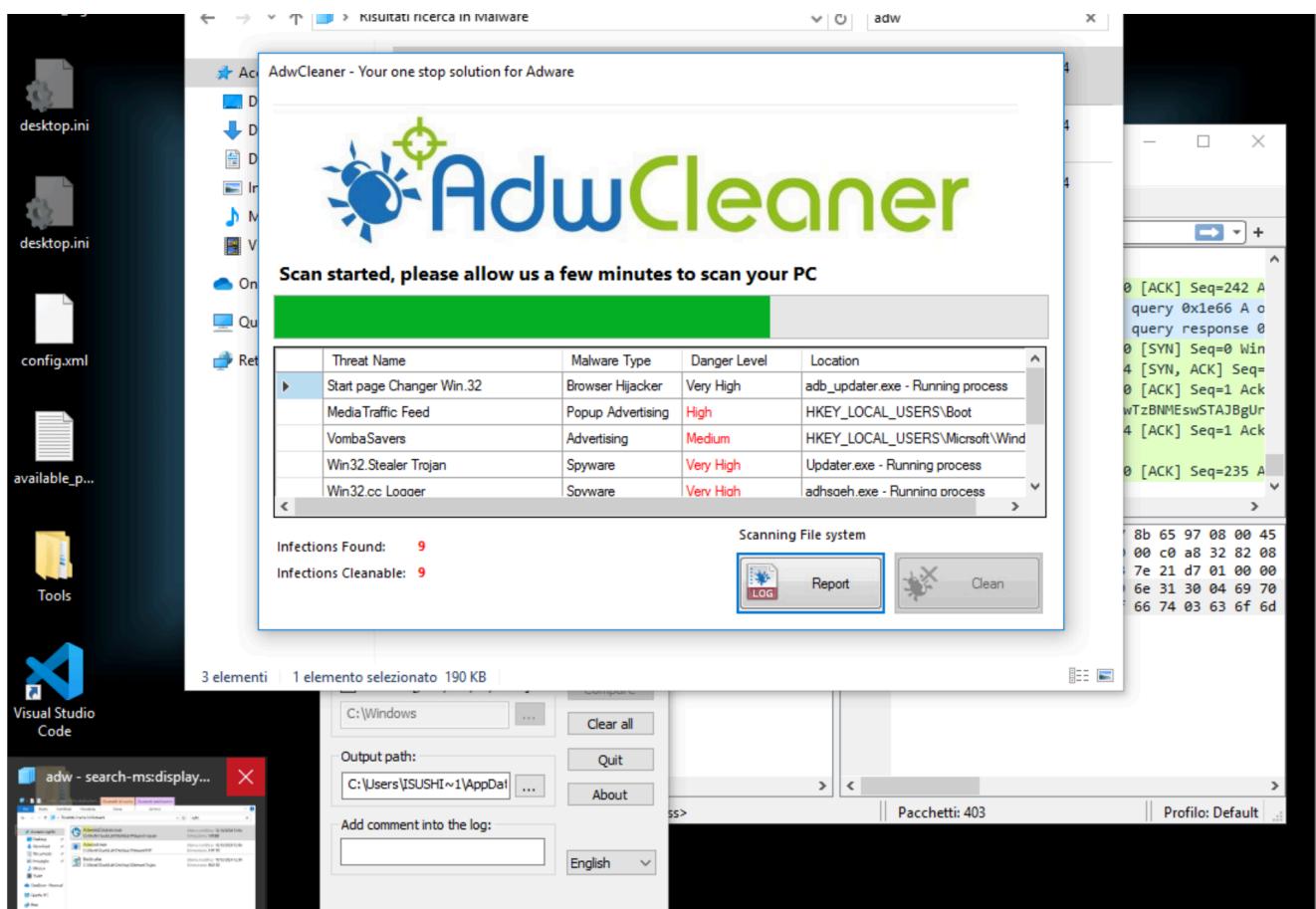
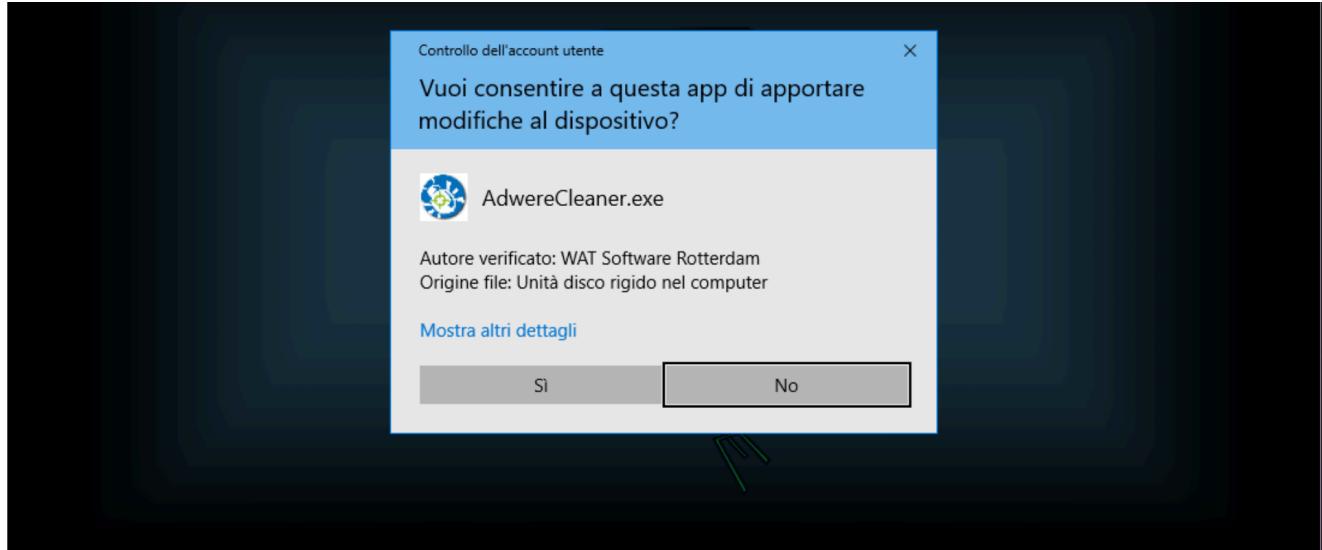
The interface also includes a Screenshot section showing a dogeza icon, and a Post-Analysis Lookup table with no hosts contacted.

Schermate di AdwareCleaner

Tag: #adwarecleaner #interfaccia #rilevamento

- Durante l'installazione, AdwareCleaner chiede i permessi amministrativi.

- Una volta lanciato, rileva diverse minacce di adware e spyware, classificandole per tipo di malware e livello di pericolo.
- L'interfaccia mostra le infezioni rilevate e invita l'utente all'aggiornamento per la rimozione.



Conclusione della Scansione con AdwareCleaner

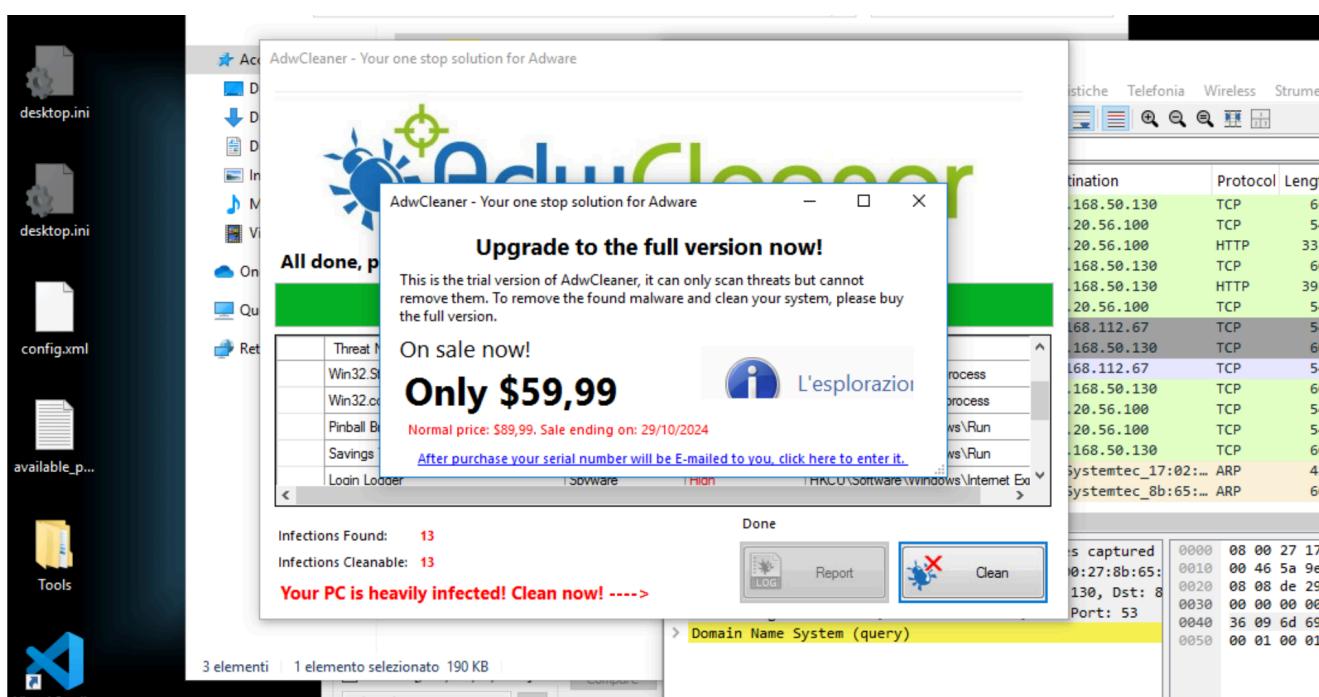
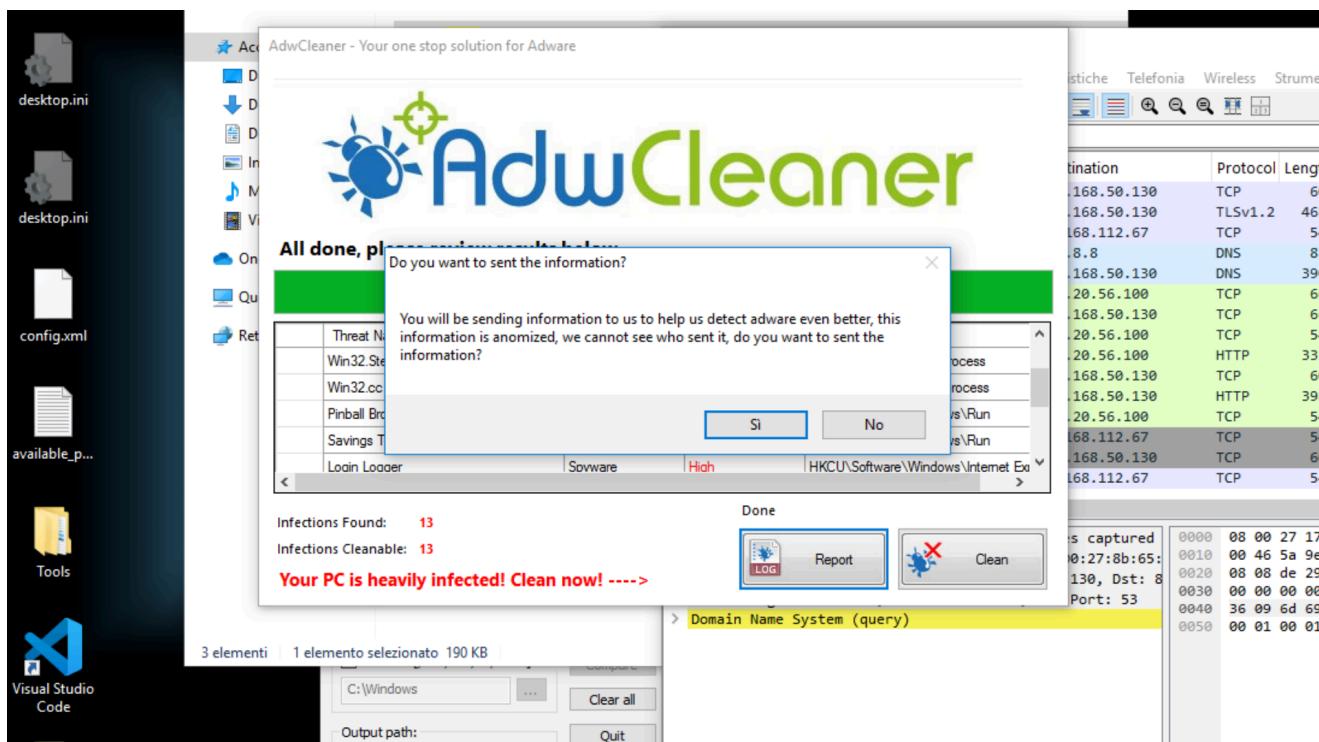
**Tag:**

#scareware

#notifiche

#rimozione

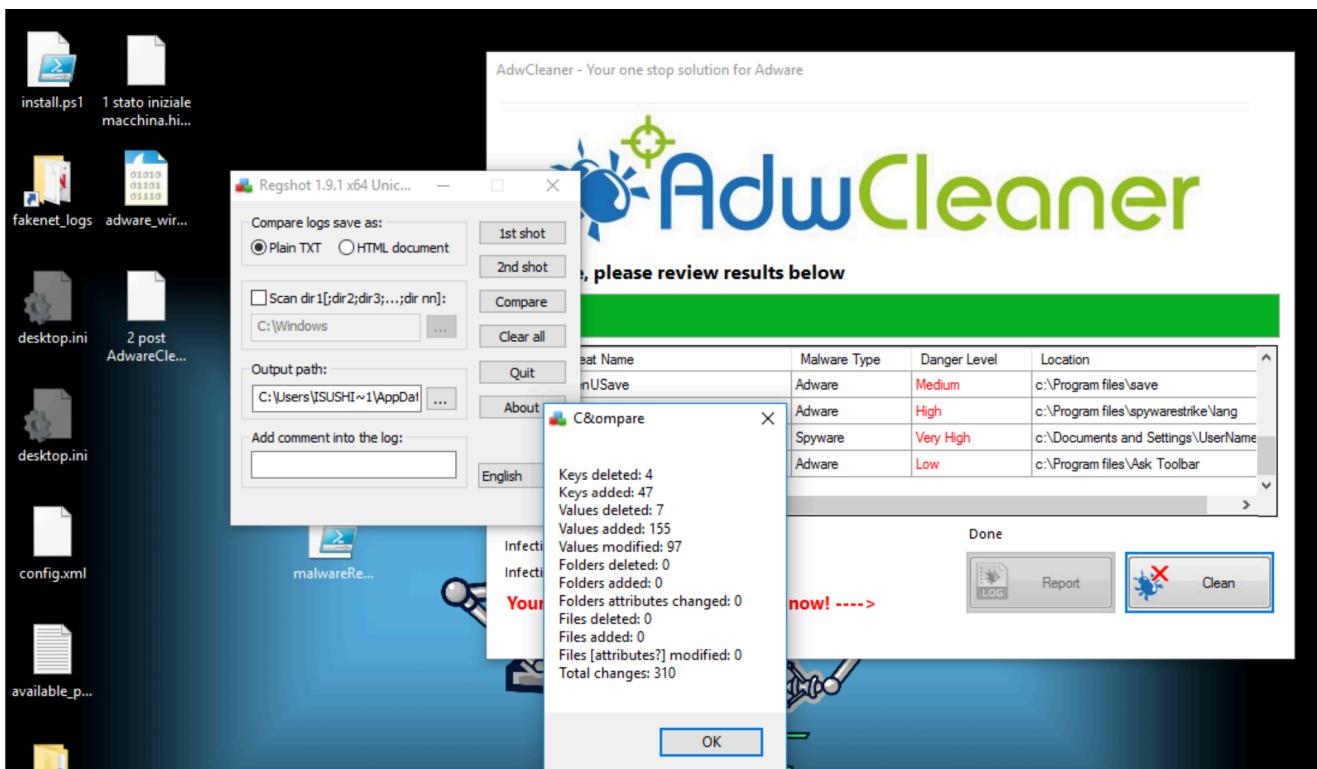
- Alla fine della scansione, l'utente viene sollecitato a inviare dati per migliorare il rilevamento.
- Un messaggio promozionale invita l'utente ad acquistare la versione completa per rimuovere le minacce.
- Evidenza di comportamento tipico di scareware che manipola l'utente con notifiche di infezione critica.



Regshot - Monitoraggio Modifiche al Sistema

Flower Tag: #regshot #modifiche #chiavi

- Comparazione dei risultati tramite Regshot, mostrando dettagli delle chiavi e valori modificati.
- Totale di 310 modifiche al sistema durante l'esecuzione di AdwareCleaner, confermando il comportamento modificativo del sistema.



Process Monitor e Dettagli di Processo

Flower Tag: #processmonitor #query #scritture

- Con Process Explorer e Process Monitor, viene osservata l'attività dei processi di AdwareCleaner e altri file correlati.
- Evidenze di query del registro e scritture sui file, indicativi di un'attività sospetta continua.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-H48GIR0\iSushiLab] (Administrator)						
File	Options	View	Process	Find	Users	Help
	CPU	Private Bytes	Working Set	PID	Description	Company Name
Process						
└ svchost.exe	< 0.01	31.496 K	63.388 K	920	Process host per servizi di...	Microsoft Corporation
└ svhost.exe		4.304 K	19.160 K	2196	Shell Infrastructure Host	Microsoft Corporation
└ taskhost.exe		5.384 K	17.844 K	3036	Process host per attività di...	Microsoft Corporation
└ WMIADAP.exe		1.788 K	8.044 K	5356	WMI Reverse Performance ...	Microsoft Corporation
└ svchost.exe	< 0.01	6.000 K	17.256 K	972	Process host per servizi di...	Microsoft Corporation
└ svchost.exe		15.912 K	24.676 K	232	Process host per servizi di...	Microsoft Corporation
└ svchost.exe		11.008 K	20.404 K	484	Process host per servizi di...	Microsoft Corporation
└ svchost.exe		9.288 K	30.400 K	348	Process host per servizi di...	Microsoft Corporation
└ VBoxService.exe		2.052 K	6.436 K	1028	VirtualBox Guest Additions S...	Oracle and/or its affiliates
└ svchost.exe		6.940 K	17.100 K	1140	Process host per servizi di...	Microsoft Corporation
└ svchost.exe		2.340 K	9.916 K	1324	Process host per servizi di...	Microsoft Corporation
└ audiodg.exe		5.956 K	11.052 K	3296	Isolamento grafico dispositiv...	Microsoft Corporation
└ svchost.exe		2.032 K	6.920 K	1438	Process host per servizi di...	Microsoft Corporation
└ spoolsv.exe		5.640 K	14.260 K	1576	Applicazione sottosistema sp...	Microsoft Corporation
└ svchost.exe		1.508 K	6.776 K	1832	Process host per servizi di...	Microsoft Corporation
└ svchost.exe		8.056 K	23.844 K	1876	Process host per servizi di...	Microsoft Corporation
└ OfficeClickToRun.exe		16.388 K	35.140 K	1884	Microsoft Office Click-to-Run...	Microsoft Corporation
└ openvpn.exe		1.284 K	5.700 K	2020	openVPN Service	The OpenVPN Project
└ svchost.exe		1.808 K	7.184 K	2028	Process host per servizi di...	Microsoft Corporation
└ svchost.exe		5.536 K	17.748 K	1188	Process host per servizi di...	Microsoft Corporation
└ SearchIndexer.exe		21.752 K	26.396 K	3020	Microsoft Windows Search I...	Microsoft Corporation
└ SearchProtocolHost.e...		2.084 K	11.556 K	4176	Microsoft Windows Search P...	Microsoft Corporation
└ SearchFilterHost.exe		1.272 K	6.604 K	4232	Microsoft Windows Search F...	Microsoft Corporation
└ svchost.exe		4.144 K	19.228 K	2144	Process host per servizi di...	Microsoft Corporation
└ svchost.exe		1.936 K	7.360 K	628	Process host per servizi di...	Microsoft Corporation
└ dwm.exe		4.712 K	13.876 K	620	Local Security Authority Proc...	Microsoft Corporation
└ winlogon.exe	< 0.01	2.052 K	9.096 K	544	Applicazione Accesso a Win...	Microsoft Corporation
└ explorer.exe	< 0.01	52.156 K	110.000 K	868	Gestione finestre desktop	Microsoft Corporation
└ dwm.exe	< 0.01	36.040 K	116.488 K	2872	Esplora risorse	Microsoft Corporation
└ BoxTray.exe	< 0.01	2.496 K	10.256 K	860	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
└ openvpn-gui.exe		1.980 K	10.792 K	556		
└ Zoom54.exe		1.664 K	7.508 K	4084	Syarinamente Screen Magnifier	Syarinamente - www.sysinter...
└ AdwCleaner.exe		26.940 K	34.268 K	2700	AdwareBooC	5/5/27
└ Promon.exe	< 0.01	7.768 K	17.476 K	5992	Process Monitor	Syarinamente - www.sysinter...
└ Promon64.exe		73.772 K	58.404 K	6056	Process Monitor	Syarinamente - www.sysinter...
└ procesexp.exe	< 0.01	4.404 K	11.516 K	3484	Syarinamente Process Explore	Syarinamente - www.sysinter...
└ procesexp64.exe	< 0.01	26.444 K	54.400 K	3904	Syarinamente Process Explore	Syarinamente - www.sysinter...
└ chrome.exe	< 0.01	34.932 K	133.444 K	1256	Google Chrome	Google LLC
└ chrome.exe		1.724 K	7.304 K	4388	Google Chrome	Google LLC
└ chrome.exe		11.772 K	44.312 K	4660	Google Chrome	Google LLC
└ chrome.exe		13.936 K	41.244 K	4863	Google Chrome	Google LLC
└ chrome.exe		7.704 K	20.368 K	4884	Google Chrome	Google LLC
└ chrome.exe	1.93	115.816 K	168.080 K	4896	Google Chrome	Google LLC
└ chrome.exe		12.024 K	26.444 K	5768	Google Chrome	Google LLC

Analisi Any.Run



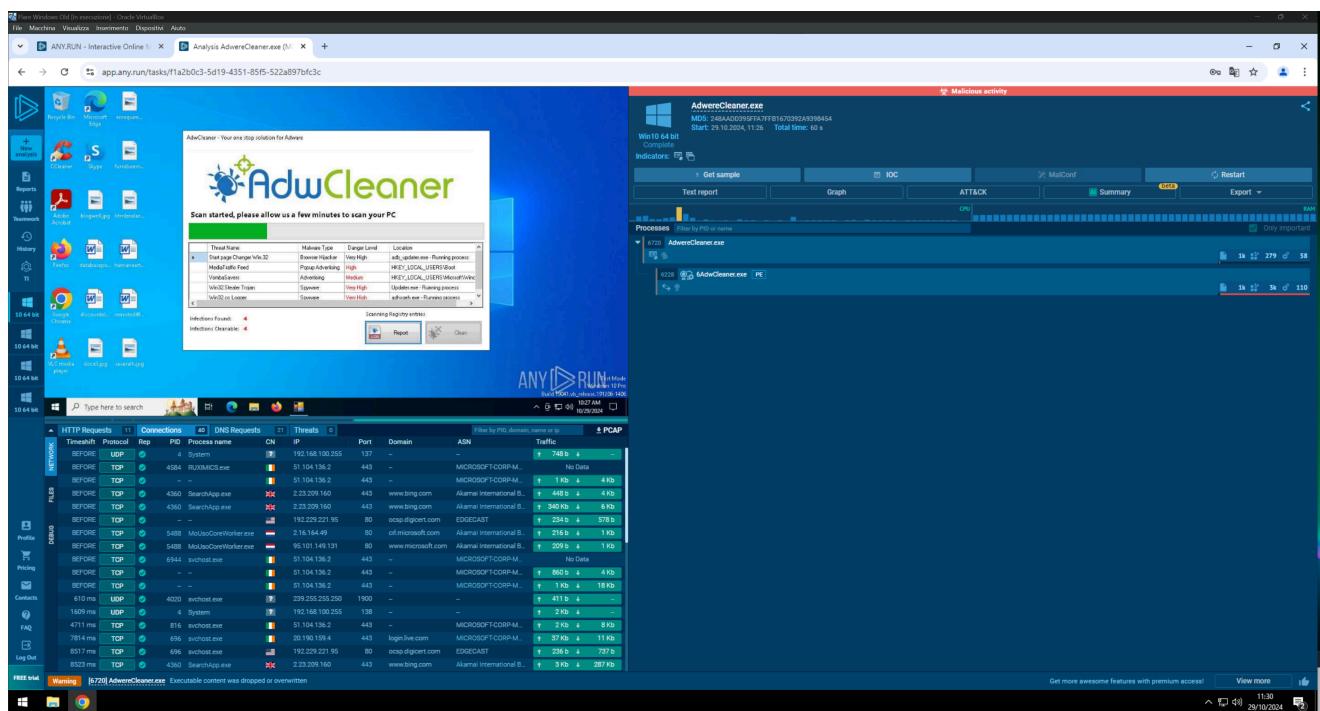
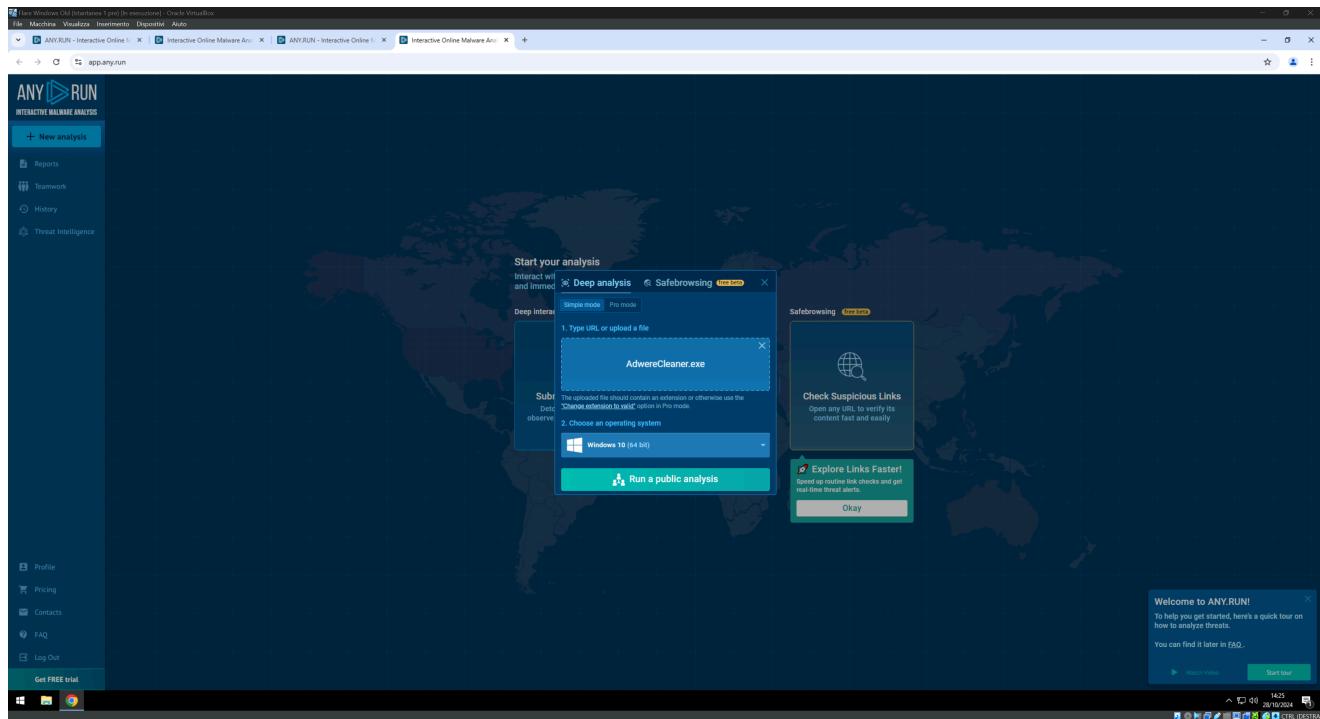
Tag: #anyrun

#attivitàrete

#connessioni

Any.Run mostra l'analisi live di AdwareCleaner, evidenziando attività di rete e connessioni verso indirizzi IP esterni.

L'analisi conferma attività sospette con comunicazioni verso domini esterni e richieste HTTP ripetute.



HTTP Requests 11				Connections 40	DNS Requests 21	Threats 0	Filter by IP or domain	PCAP
	Timeshift	Status	Rep	Domain				
NETWORK								
FILES	BEFORE	Responded	✓	google.com			2.23.209.176	
	BEFORE	Responded	✓	ocsp.digicert.com			2.23.209.175	
	BEFORE	Responded	✓	crl.microsoft.com			2.23.209.162	
	BEFORE	Responded	✓	www.microsoft.com			2.23.209.173	
DEBUG	2603 ms	Requested	🔥	www.vikingwebscanner.com			IP Addresses not found	
	7809 ms	Responded	✓	login.live.com			20.190.159.4	
							20.190.159.75	
							20.190.159.71	
							40.126.31.67	
							20.190.159.73	
							20.190.159.2	
							40.126.31.73	
							20.190.159.64	
							2.23.209.150	

The screenshot shows a Windows 10 desktop environment. In the center, a browser window displays the AdwCleaner software interface, which is a free tool for removing adware from a computer. The browser tabs show the URL `app.any.run/tasks/f1a2b0c3-5d19-4351-8f5f-522a957bf3c`. Below the browser, the Windows Task Manager is open, showing a list of running processes. One process, `AdwCleaner.exe`, is highlighted. The Task Manager details pane shows the following information for `AdwCleaner.exe`:

Thread Name	Malware Type	Damage Level	Location
Start page Change Win32	Browser Hijack	Very High	adw_update.exe - Running process
MediaFlic Feed	Program Advertising	High	MZ!:\LocalAppData\Temp\adwcleaner\adwcleaner.exe
MediaFlic Feed	Advertising	Medium	MZ!:\LocalAppData\Temp\adwcleaner\adwcleaner.exe
w32n! Shutter Trojan	Spoofer	Very High	Update.exe - Running process
w32n! Shutter Trojan	Software	Very High	adwcleaner.exe - Running process

At the bottom of the Task Manager, it says "MOVE YOUR MOUSE TO VIEW SCREENSHOTS". To the right of the Task Manager, there is a detailed analysis window for `AdwCleaner.exe`. The window includes sections for "Process", "File", "Network", and "CPU". It shows CPU usage over time, file modifications, network traffic, and a summary of the process's behavior. The analysis window also includes tabs for "IOC", "ATT&CK", "MalConf", and "Summary".

Approfondimento AdwareCleaner

Inizializzazione del Malware - Malware Initialization



Tag: #inizializzazione

#esecuzione

#trojan

Al momento dell'esecuzione, il Trojan si avvia sfruttando varie tecniche per garantire l'esecuzione immediata e la persistenza nel sistema:

1. **Processo di Esecuzione:** Il Trojan crea un processo principale, spesso duplicando o iniettandosi in processi di sistema legittimi come explorer.exe o svchost.exe .
 2. **Evasione dell'Ambiente Virtuale:** Il Trojan esegue controlli sull'ambiente per verificare la presenza di virtual machine o sandbox (come Cuckoo stessa), cercando di terminare l'esecuzione se identifica un ambiente di analisi.
-

Attività di Modifica del Registro - Registry Modifications

 **Tag:** #modificareregistro #persistenza #registro

Per mantenere la sua persistenza nel sistema e assicurare il riavvio automatico, il Trojan effettua modifiche alle chiavi del registro di sistema:

1. **Chiavi di Avvio:** Modifica o crea chiavi nelle sezioni del registro come:
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
 - Queste chiavi permettono al malware di avviarsi automaticamente ad ogni accensione del sistema.
2. **Modifica delle Politiche di Sicurezza:** Disabilita funzionalità di sicurezza di Windows o strumenti di monitoraggio di terze parti, sfruttando chiavi come:
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
3. **Persistenza tramite Task Schedulati:** Può anche impostare un task schedulato nel registro per eseguire il malware a intervalli regolari o

al riavvio.

Creazione e Modifica di File nel File System - File System Modifications

 **Tag:** #modificafile #creazionefile #persistenza

Il Trojan crea e modifica file strategici per garantire la sua operatività e compromettere ulteriormente il sistema:

1. **Cartelle Temporanee:** Genera copie di se stesso o crea file temporanei in cartelle di sistema come:
 - %AppData% , %Temp% , %System32%
 2. **Modifica di DLL e File di Sistema:** Sovrascrive o inietta codice in file di librerie dinamiche (DLL) legittime per ottenere privilegi elevati e accesso ai dati dell'utente.
 3. **File di Configurazione Nascosti:** Crea file di configurazione nascosti per registrare informazioni o tenere traccia delle attività svolte, spesso criptati per evitare il rilevamento.
-

Comunicazione di Rete e Esfiltrazione Dati - Network Communication and Data Exfiltration

 **Tag:** #esfiltrazionedati #comunicacionrete #C2

Il Trojan stabilisce connessioni di rete per inviare dati rubati e ricevere comandi:

1. **Connessione ai Server di Comando e Controllo (C2):** Stabilisce una comunicazione con server remoti, utilizzando IP e domini predefiniti, per inviare dati rubati e ricevere istruzioni.

2. **Esfiltrazione di Dati Sensibili:** Raccoglie informazioni personali, credenziali, e dati di sistema, e li trasmette ai server C2, spesso utilizzando canali cifrati per evitare il rilevamento da parte dei firewall.
 3. **Proxy e Canali Cifrati:** Il malware può stabilire connessioni usando proxy e crittografia (SSL/TLS) per confondere l'analisi e rendere il traffico meno visibile agli strumenti di monitoraggio di rete.
-

Azioni Malevoli sul Sistema - Malicious Actions on the System

 Tag: #azioni #malware #trojan

Durante l'esecuzione, il Trojan compie varie azioni malevoli che compromettono ulteriormente la sicurezza e l'integrità del sistema:

1. **Raccolta di Credenziali:** Utilizza strumenti di dumping per raccogliere password e credenziali memorizzate, inclusi i dati del browser e le password salvate nel sistema.
 2. **Keylogging e Monitoraggio Utente:** Integra un keylogger per registrare tutte le digitazioni, registrando potenzialmente dati sensibili come password, messaggi e informazioni bancarie.
 3. **Blocco di Processi di Sicurezza:** Termina i processi di sicurezza come antivirus o strumenti di monitoraggio di sistema per garantire la sua persistenza e impedire il rilevamento.
-

Conclusione - Conclusion

 Tag: #cybersecurity #malwareanalysis

L'analisi mostra che il Trojan impiega una combinazione di tecniche di **persistenza avanzata, esfiltrazione dati e evasione della sicurezza**. Attraverso la modifica del registro, la creazione di file strategici e la comunicazione con server C2, il malware compromette la sicurezza del sistema, minaccia la privacy dell'utente e può causare perdite significative di dati.

🔑 Chiavi:

[trojan, modifiche registro, persistenza, esfiltrazione dati, C2, malware analysis, cuckoo sandbox]

Guida per la Rimozione del Trojan - Per Tecnici IT Non Esperti

Passo 1: Isolamento Immediato del Computer Infetto

⚜ Tag: #isolamento #rete #contenimento

1. Collega dalla Rete:

- Rimuovi il cavo Ethernet o disabilita il Wi-Fi per scollegare il dispositivo infetto dalla rete aziendale.
- Scopo: Questo impedisce al Trojan di diffondere il malware su altri computer o inviare dati a internet.

2. Blocca le Connessioni Esterne:

- Parla con l'amministratore di rete e chiedi di bloccare gli indirizzi IP e i domini sconosciuti per il dispositivo infetto, specificando che potrebbe inviare dati a server esterni.
- Nota: Non serve conoscere l'indirizzo IP esatto; spiega solo che devi bloccare tutte le comunicazioni dal dispositivo finché non è pulito.

Passo 2: Verifica e Disabilitazione delle Modifiche al Sistema

 Tag: #registro #startup #puliziasistema

1. Controlla i Programmi in Avvio Automatico:

Premi **Ctrl + Shift + Esc** per aprire **Gestione Attività**.

- Vai alla scheda **Avvio** e disabilita qualsiasi programma sospetto (qualcosa che non riconosci e non è parte del sistema o dei software aziendali).
- Scopo: Il Trojan potrebbe impostarsi per partire da qui ad ogni avvio; disabilitare le voci non conosciute impedisce che si riattivi.

2. Modifica del Registro (Attenzione!):

- Digita **regedit** nella barra di ricerca di Windows per aprire l'Editor del Registro di sistema.
- Naviga verso le chiavi
`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` e
`\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`.
- Cancella solo le voci che non riconosci o sembrano sospette (ad esempio nomi strani o di programmi che sai di non aver installato).
- Nota: Fai molta attenzione, non cancellare nulla che non sei certo sia parte del malware.

Passo 3: Scansione con Strumenti di Rimozione e Pulizia

 Tag: #scansione #rimozionemalware #antivirus

1. Scarica uno Strumento Anti-Malware Affidabile:

- Scarica un software come Malwarebytes (versione gratuita va bene) e installalo.
- Scopo: Malwarebytes è semplice e identifica trojan, rootkit e malware senza bisogno di configurazioni avanzate.

2. Esegui una Scansione Completa del Sistema:

- Avvia Malwarebytes e scegli la **Scansione Completa**. Quando la scansione finisce, scegli di Rimuovere Tutti gli **Oggetti Rilevati**.
- Riavvia il computer al termine se il programma lo consiglia.

3. Rimozione dei File Temporanei:

- Digita **%Temp%** nella barra di ricerca e apri la cartella dei file temporanei.
- Elimina tutto ciò che si trova nella cartella (non ti preoccupare, sono file che Windows rigenera automaticamente).

Passo 4: Controllo delle Impostazioni di Sicurezza

 Tag: [#sicurezza](#) [#firewall](#) [#backup](#)

1. Verifica che Windows Defender sia Attivo:

- Vai in **Impostazioni > Aggiornamento e sicurezza > Sicurezza di Windows > Protezione da virus e minacce**.
- Assicurati che la **Protezione in tempo reale** sia attivata.

2. Firewall di Windows:

- Sempre in **Sicurezza di Windows**, vai su **Firewall e protezione della rete** e assicurati che il firewall sia attivato su tutte le reti (pubblica, privata, dominio).

3. Esegui un Backup dei Dati Importanti:

- Collega un'unità USB esterna e copia i dati importanti per sicurezza, in caso ci sia bisogno di un reset completo.

- Scopo: Se tutto il resto non funziona, puoi sempre reinstallare Windows senza perdere i file importanti.
-

Passo 5: Verifica Finale e Prevenzione



Tag:

#verifica

#educazioneutente

#prevenzione

1. Riavvia il Computer e Fai un Controllo Finale:

- Dopo il riavvio, apri di nuovo **Gestione Attività** per assicurarti che non ci siano nuovi programmi sospetti in avvio.
- Controlla anche che la connessione di rete non stia tentando di accedere a server sconosciuti (puoi vedere le connessioni attive nella sezione **Prestazioni > Rete**).

2. Formazione di Base sull'Email Phishing:

- Spiega agli utenti di non aprire email sospette e di evitare di scaricare allegati da fonti non affidabili, che sono una delle principali cause di infezione.

3. Mantenere il Sistema Aggiornato:

- Assicurati di aggiornare Windows e il software antivirus regolarmente; di solito Windows lo fa automaticamente, ma è sempre bene verificare.
-

Per ulteriori informazioni consultare il report

in allegato: Any.run_adware_report.pdf



General Info

File name: AdwereCleaner.exe
 Full analysis: <https://app.any.run/tasks/102bd588-0dc7-4d48-855d-fb42bdaca895>
 Verdict: Malicious activity
 Analysis date: October 28, 2024 at 14:34:23
 OS: Windows 10 Professional (build: 19045, 64 bit)
 Indicators:
 MIME: application/vnd.microsoft.portable-executable
 File info: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive, 5 sections
 MD5: 248AAD395FFA7FFB1670392A9398454
 SHA1: C53C140BDBE556FCA33BC7F9B2E44E9061EA3E5
 SHA256: 51290129CCCCA38C6E3B444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC
 SSDeep: 3072:1STDpNFVbxDSXJFF6hcBR1WLZ37p73G8Wn7GID0g+ELqdSxo5XtIZjnvxRJggHaR:157TcfFPB6B3GL7g+me5aZjn5VII9T/

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakeweb option:	off	Route via Tor:	off	Autoconfirmation of UAC:	
Network:	on			on	

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professional 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package