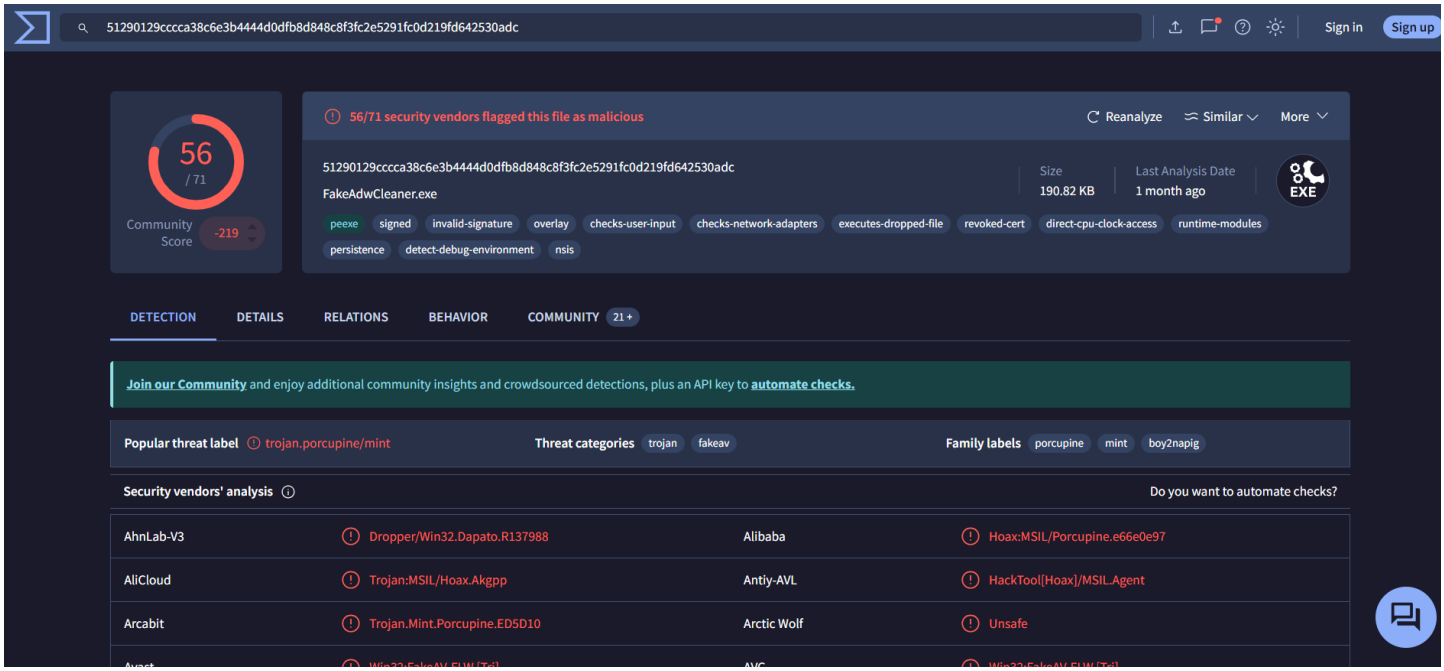
BUILD WEEK III

"Esercizio 1 – Malware Analysis"

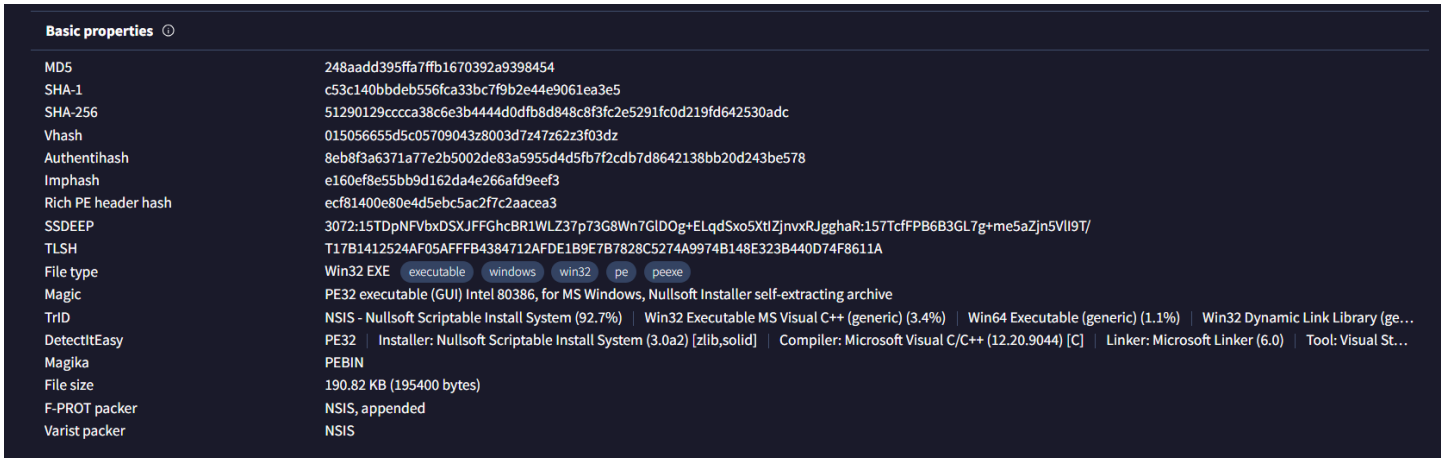
Dopo aver scaricato il malware come richiesto siamo passati inizialmente all'analisi statica ed in seguito dinamica dello stesso.

ANALISI STATICA

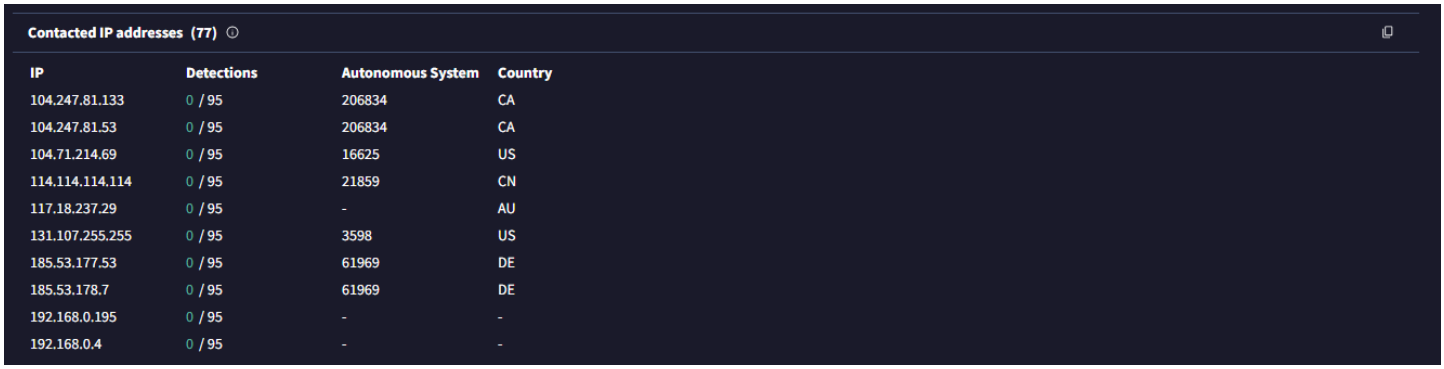
In prima analisi abbiamo sfruttato VirusTotal per testare il malware, ottenendo così i seguenti dati:



-estratto generale dell'analisi-



-proprietà di base-



-indirizzi IP contattati-

Contacted Domains (40)

Domain	Detections	Created	Registrar
1.155.190.20.in-addr.arpa	0 / 95	-	-
106.89.54.20.in-addr.arpa	0 / 95	-	-
133.81.247.104.in-addr.arpa	0 / 95	-	-
202.216.231.44.in-addr.arpa	0 / 95	-	-
79.49.8.65.in-addr.arpa	0 / 95	-	-
80.69.35.23.in-addr.arpa	0 / 95	-	-
a233.dscd.akamai.net	0 / 95	1999-03-03	MarkMonitor Inc.
adobe.com	0 / 95	1986-11-17	NOM-IQ Ltd dba Com Laude
armmf.adobe.com	0 / 95	1986-11-17	NOM-IQ Ltd dba Com Laude
assets.msn.com	0 / 95	1994-11-10	MarkMonitor Inc.

-domini contattati-

Dropped Files (13)

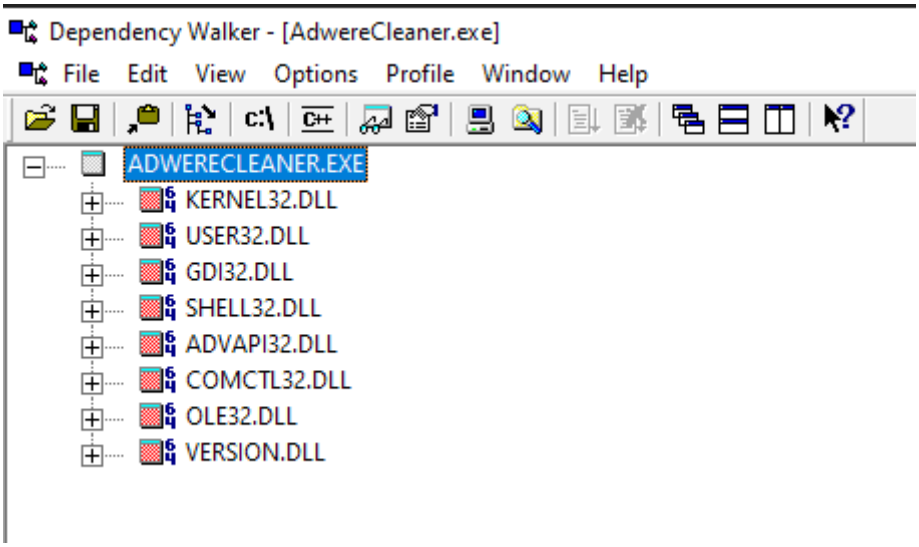
Scanned	Detections	File type	Name
2025-05-30	0 / 62	?	1F356F4D07FE8C483E769E4586569404
2025-05-30	0 / 62	?	B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F
2025-08-14	53 / 72	Win32 EXE	6AdwCleaner.exe
2025-03-10	44 / 68	Win32 EXE	6adwcleaner.exe
?	?	file	0bfa420acf2ad034dca670926bf30a1d5f05ffd6087fde2d8ae4eee5d29c74da
?	?	file	4F0033E811FE2497B38F0D45DF958829D01933EBE7D331079EEFC8E38FBEAA61
?	?	file	5d695998f311e05d7bfc4f76f948fb6c78572a2137e03f5cb6c41794c06afa0e
?	?	file	7a2e8ffe5697837feedebc5525e1ea3305589f2de399195dbd5860bf7b4760d8
?	?	file	819b63fa98c0f590ed6e6404270cbe5d262918e141fa3cfb2f81e09886c47f4d
?	?	file	91a623eacdf1e2a0c229d52c64c980833dc332053f7003c163e35f2cfa7d4ef3

-file droppati-

Names

FakeAdwCleaner.exe
AdwereCleaner.exe
fakeadwcleaner.exe
Endermanch@FakeAdwCleaner.exe
7ac27f7b8c68f4c5d547891d991001661a1a6af1-d659d96d15c7a1206f44eb36ed72495563140859
bf832162-104c-4773-9c5e-9a9aaa876444.exe
858858dd-26e0-4876-bd5d-4ecb3d200fee.exe
91440ed8-e5ef-4a38-ada2-6666b60726a4.exe
AdwereCleaner (1).exe
AdwereCleaner.zOtfFhsJ.exe.part
Unconfirmed 567426.crdownload
AdwereCleaner (2).exe
ADWERECLEANER.EXE
481953.exe
AdwereCleaner(6).exe
AdwereCleaner(3).exe
AdwereCleaner(1).exe
Non confermato 637281.crdownload

-nomi alternativi del file-



-dll prese in esame-

In seguito all'analisi statica, siamo giunti già alla conclusione che 56 su 71 motori di sicurezza riconoscono il malware come altamente pericoloso, classificandolo come *Trojan* o *FakeAV* (Fake AntiVirus).

Nel dettaglio la natura del file è associata ad un eseguibile Windows 32bit legato alle possibili famiglie Porcupine, Mint.

Riusciamo inoltre ad intuire che il malware è progettato per ingannare l'utente simulando un software di pulizia o rimozione adware, che, dopo una scansione simulata troverà falsamente decine o centinaia di minacce critiche al fine di indurre il bersaglio ad eseguire azioni dannose o pagare per la rimozione di minacce inesistenti.

Siamo andati poi a visualizzare gli IoC (Indicator of Compromission), trovando i seguenti hash che sono essenziali per il rilevamento e la mitigazione:

- SHA-256 51290129cccca38c8c3b444d0fd8d0848c08fc2e5291fc0d219fd542530adc
- SHA-1 c53c140b0deb56fca33bc789b24e4e06c1ea3e5
- MD5 248aadd39f5fa7ffb1670392a8399454

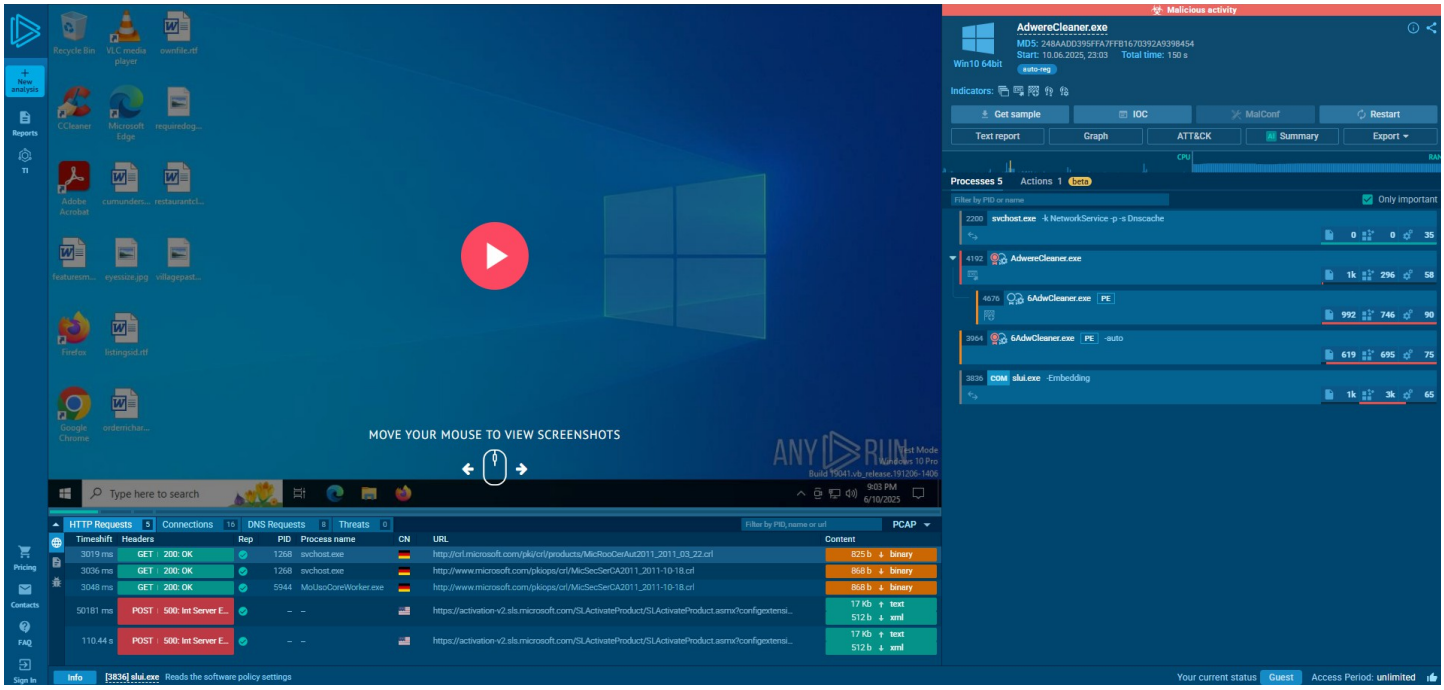
Abbiamo inoltre delle informazioni di base aggiuntive:

- Nome File Rilevato *FakeAdwCleaner.exe*
- Dimensione *190.82 KB*
- Tipo di File *PE32 executable* (GUI) *Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive*
- Compilatore/Packer *Il file è stato compilato utilizzando NSIS* (Nullsoft Scriptable Install System), *un programma di installazione legittimo spesso abusato dai malware per impacchettare script e payload dannosi.*

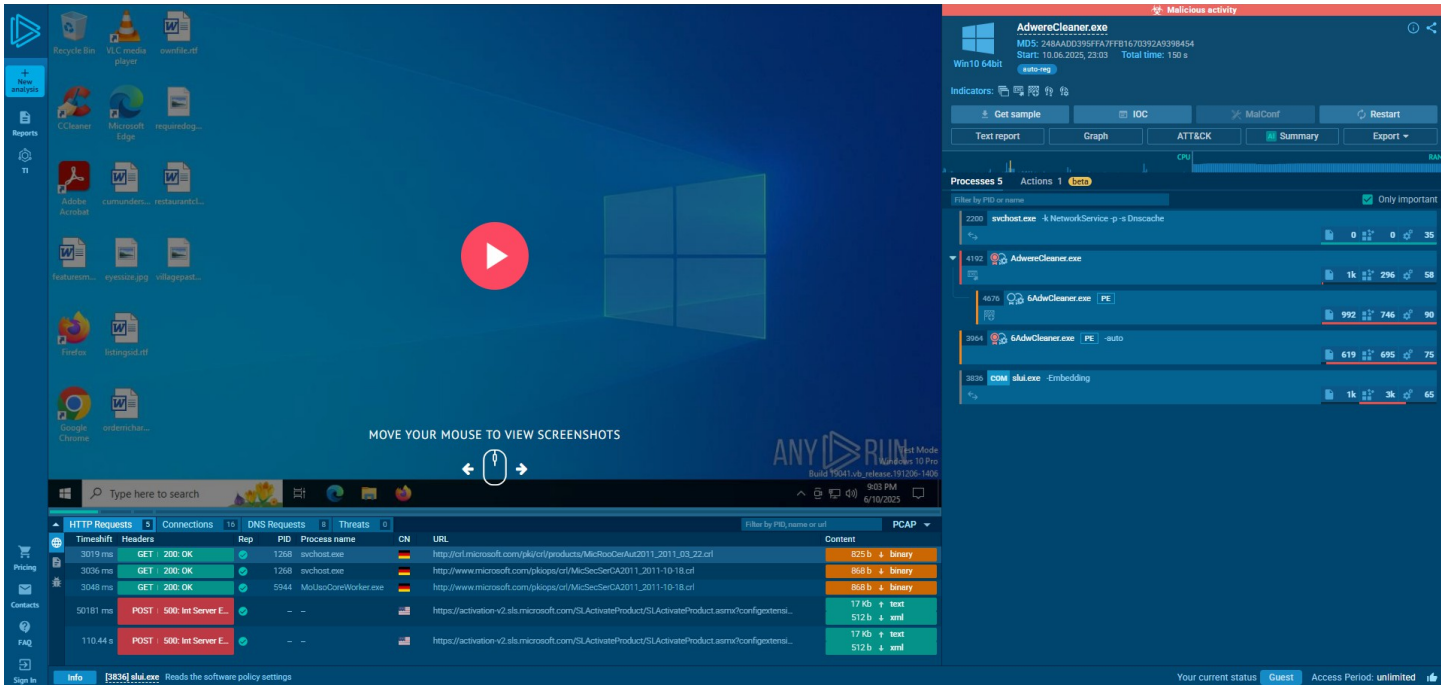
N.B. Non è da escludere una possibile installazione di adware o spyware.

ANALISI DINAMICA

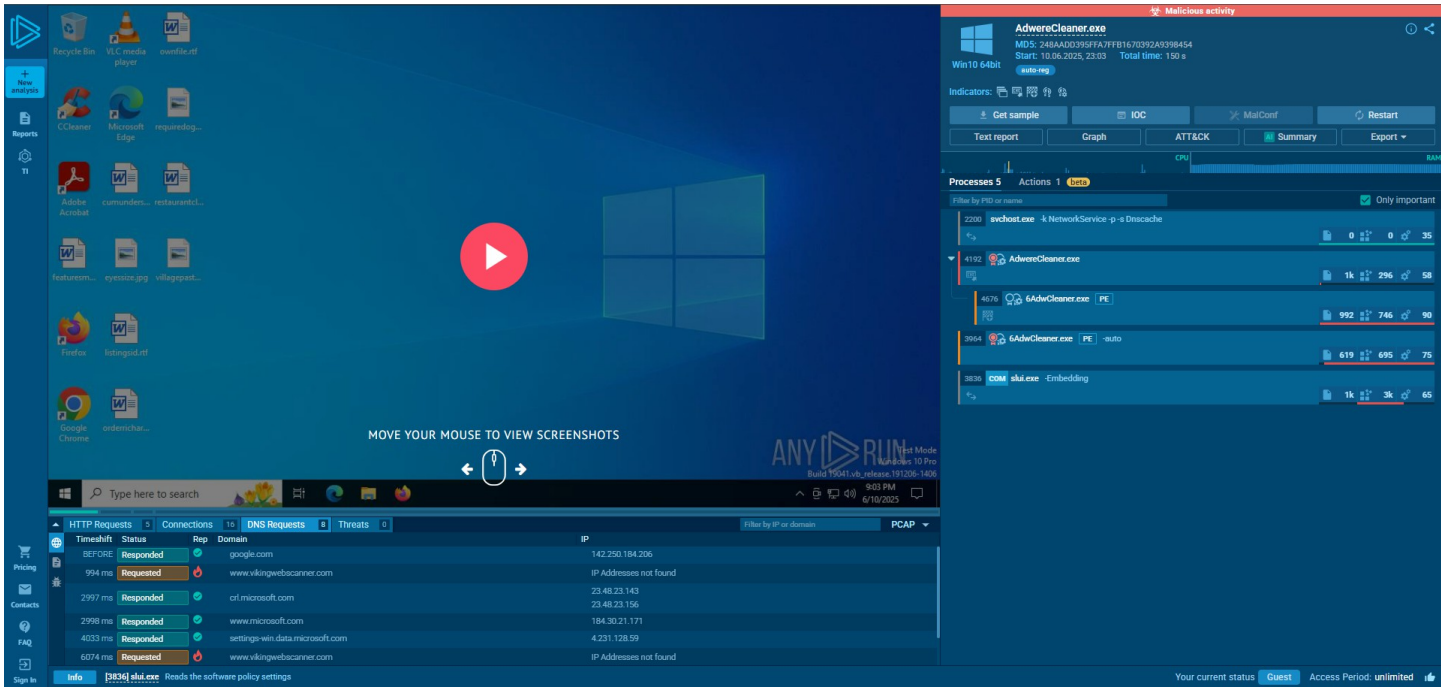
Ai fini di un'analisi dinamica del malware, abbiamo inserito nella sandbox any.run il file malevolo per osservarne il comportamento:



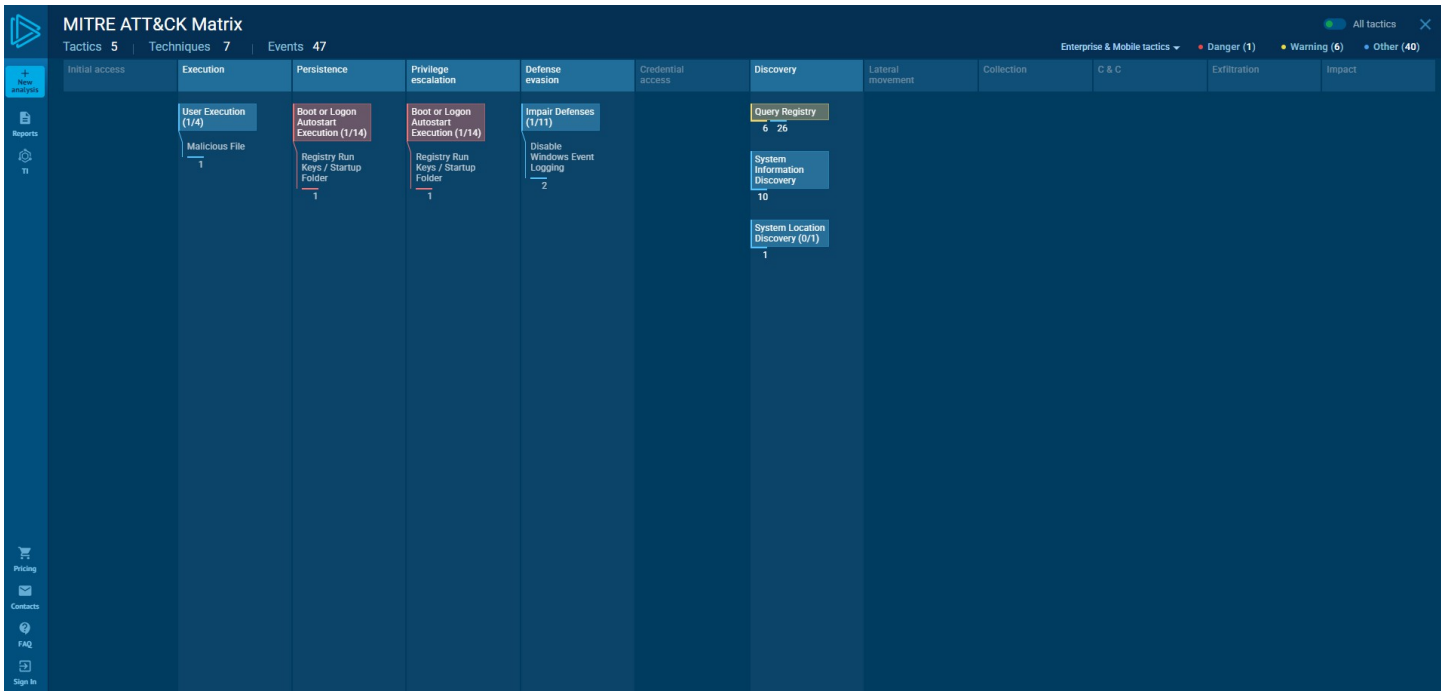
-schermata principale (http request)-



-schermata principale (connections)-



-schermata principale (dns request)-



-schermata MITRE ATT&CK Matrix-

Andando a fondo con l'analisi dinamica, si conferma il comportamento malevolo del file in oggetto.
I segnali che ce lo indicano sono:

PERSISTENZA NEL REGISTRO DI SISTEMA

- Chiave di persistanza — Il processo *6AdwCleaner.exe* scrive un valore nella chiave *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*

- Valore di esecuzione — Il valore creato è *AdwCleaner*, che punta all'eseguibile droppato con il flag di esecuzione automatica: *"C:\Users\admin\AppData\Local\6AdwCleaner.exe" -auto*

CREAZIONI DI FILE E DROP DEL PAYLOAD:

Il file iniziale, *AdwereCleaner.exe* (eseguito da desktop) è un installer che rilascia e lancia un secondo eseguibile:

- Drop del Payload *C:\Users\admin\AppData\Local\6AdwCleaner.exe*
- Hash del Payload

  MD5 *87E4959FEFEC297EBBF42DE7985088F6*

  SHA256 *4F0033E811FE2497B38F0D45DF958829001933EBE7D331079EEFC8E38FBEAA61*

PROCESS TREE (catena di infezione)

Il grafico mostra poi il flusso dell'attacco:

1. Start — La vittima esegue il file iniziale *AdwareCleaner.exe*
2. Drop/Esecuzione — *AdwareCleaner.exe*, rilascia ed esegue *6AdwCleaner.exe*
3. Persistenza/Esec. Automatica — *6AdwCleaner.exe* è il responsabile della scrittura su registro per la persistenza e dell'esecuzione con l'opzione *-auto*
4. Processi collaterali — Si notano inoltre attività relative a *slui.exe* (Windows Activation Client) e *svchost.exe*, che in questo particolare caso potrebbero essere tentativi di innalzamento dei privilegi o di interferenza dei processi

ALTRE ATTIVITA' SOSPETTE

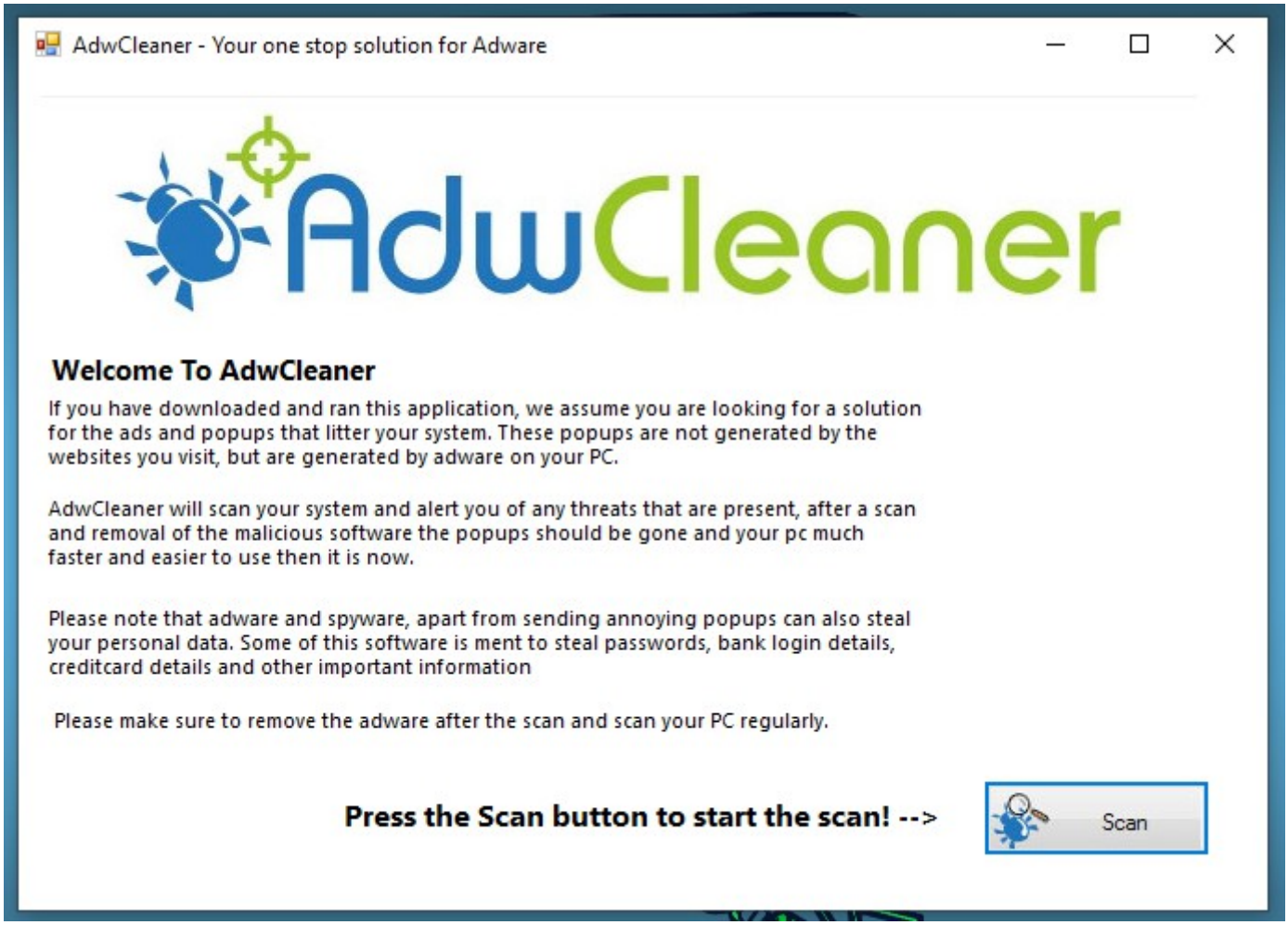
- Controllo delle lingue supportate
- Lettura del nome del PC
- Lettura del Machine GUID dal registro
- Controllo delle impostazioni del server proxy
- Lettura delle impostazioni di Internet Explorer

TENTATIVI DI OFFUSCAMENTO

6AdwClaner.exe tenta di disabilitare i log di traccia (disable trace logs), nel tentativo di ostacolare l'analisi.7

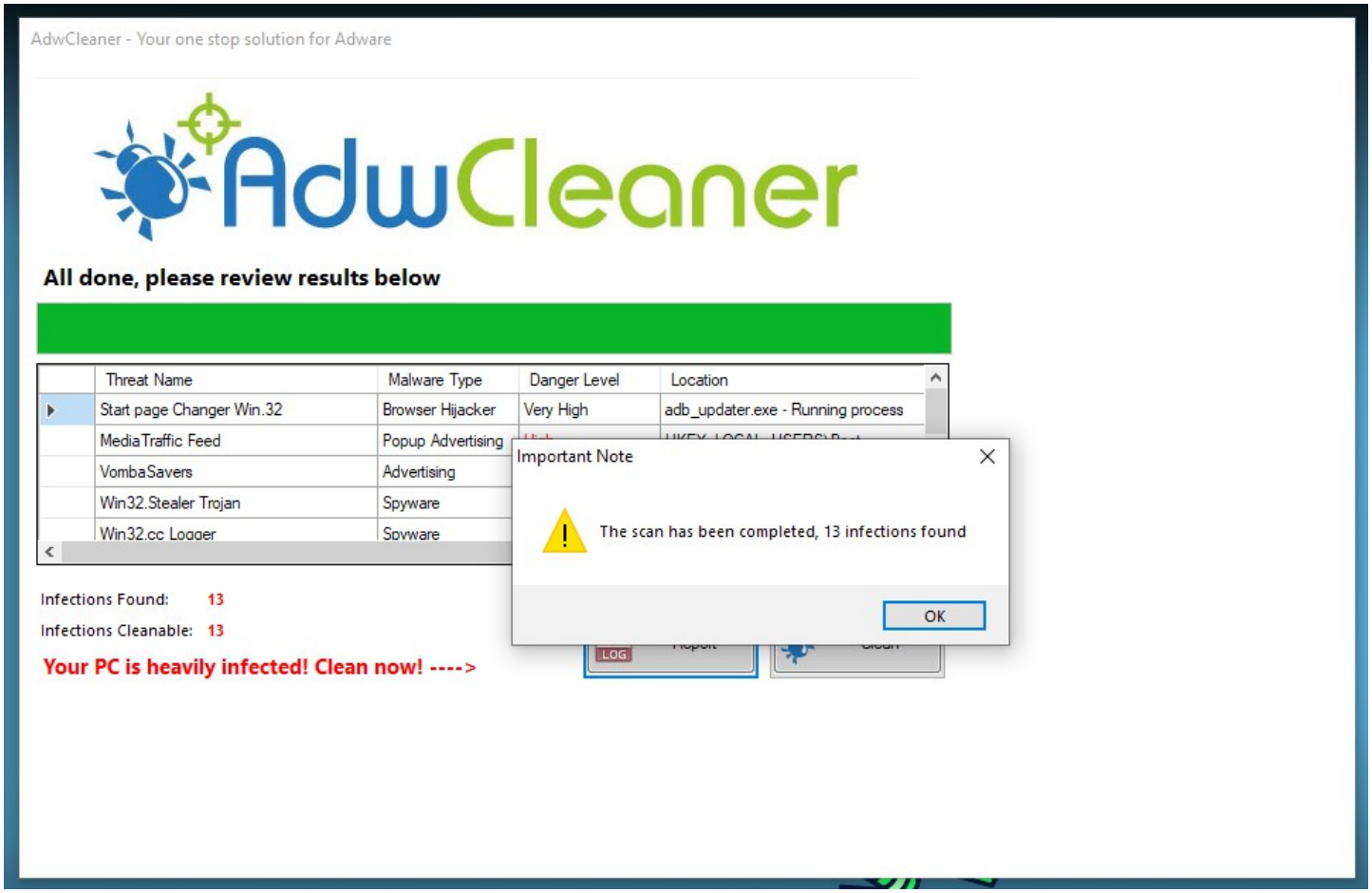
AVVIO IN AMBIENTE PROTETTO ED ULTIME IMPRESSIONI

In ultima analisi, **IN AMBIENTE PROTETTO**, abbiamo avviato il file sospetto per analizzarne il cmportamento:

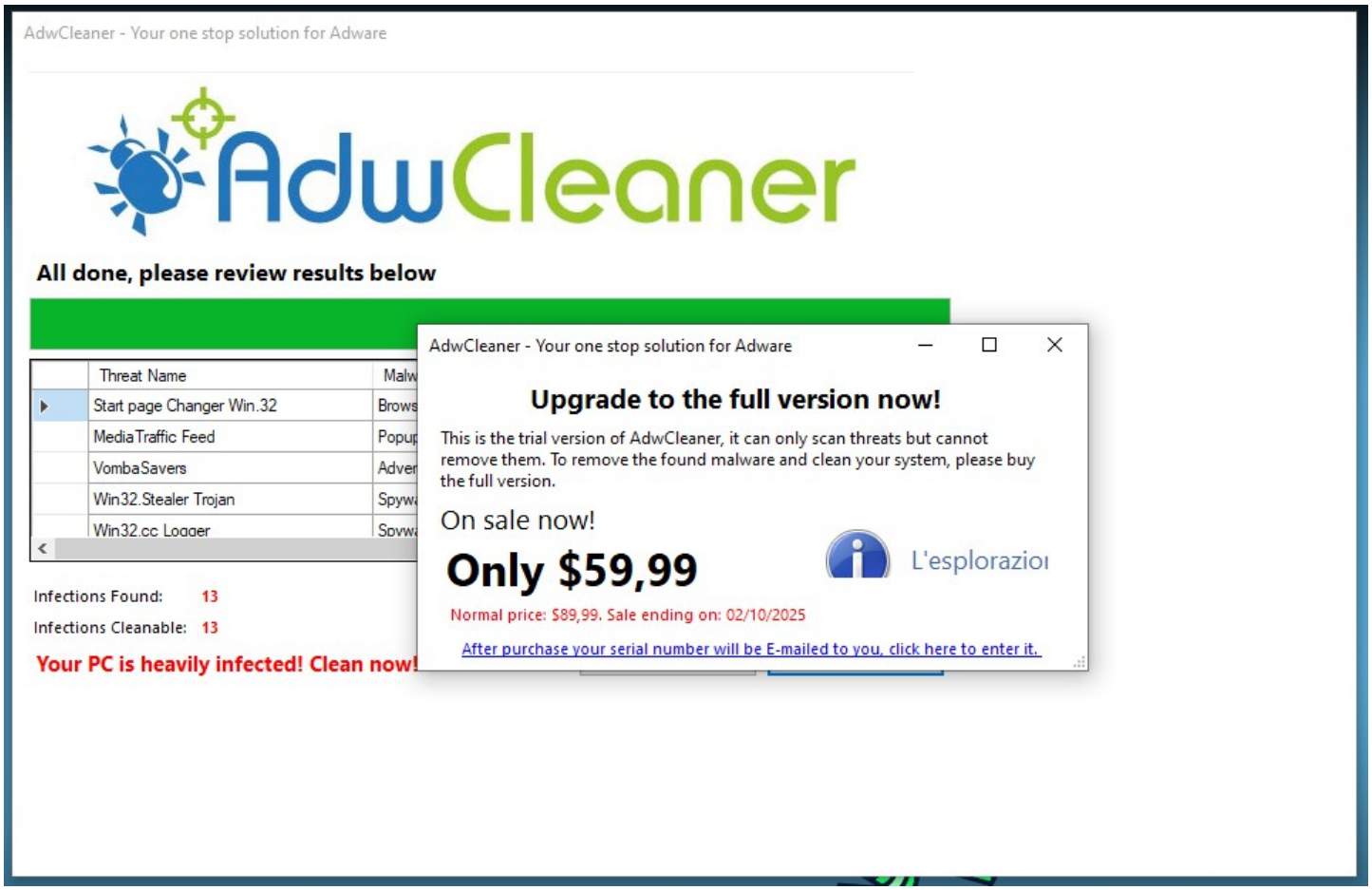


-avvio del file-

Subito dopo l'avvio, il software richiederà, come previsto una scansione del pc.



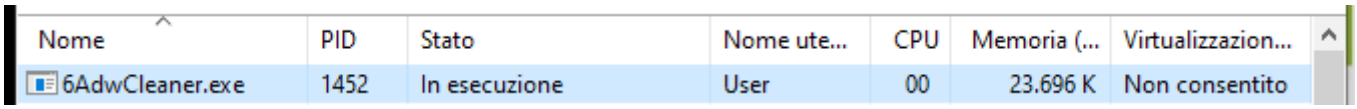
-fine della "scansione"-



-richiesta in denaro per provvedere alla rimozione-

Non appena avrà terminato, lo stesso richiederà informazioni personali come e-mail, numero della carta di credito per provvedere alla pulizia.

RICORDIAMO CHE DALLE PRECEDENTI ANALISI, E' RISULTATO UN FAKEAV/TROJAN.



Nome	PID	Stato	Nome ute...	CPU	Memoria (...	Virtualizzazion...
6AdwCleaner.exe	1452	In esecuzione	User	00	23.696 K	Non consentito

-avvio del software dannoso in background-

E possiamo notare come nel frattempo abbia avviato il processo prima descritto: 6AdwCleaner.exe.

CONCLUSIONI

Dopo l'analisi statica e dinamica, possiamo affermare che:

- Il file è un installer dannoso, che droppa un eseguibile secondario
- Il suo scopo primario, è stabilire la persistenza modificando la chiave Run del Registro
- Svolge chiaramente una ricognizione dell'ambiente prima di agire

Si raccomanda caldamente l'eliminazione sicura del file e l'impedimento della sua apertura all'interno delle piattaforme aziendali.