



Report di Analisi Statica del Malware

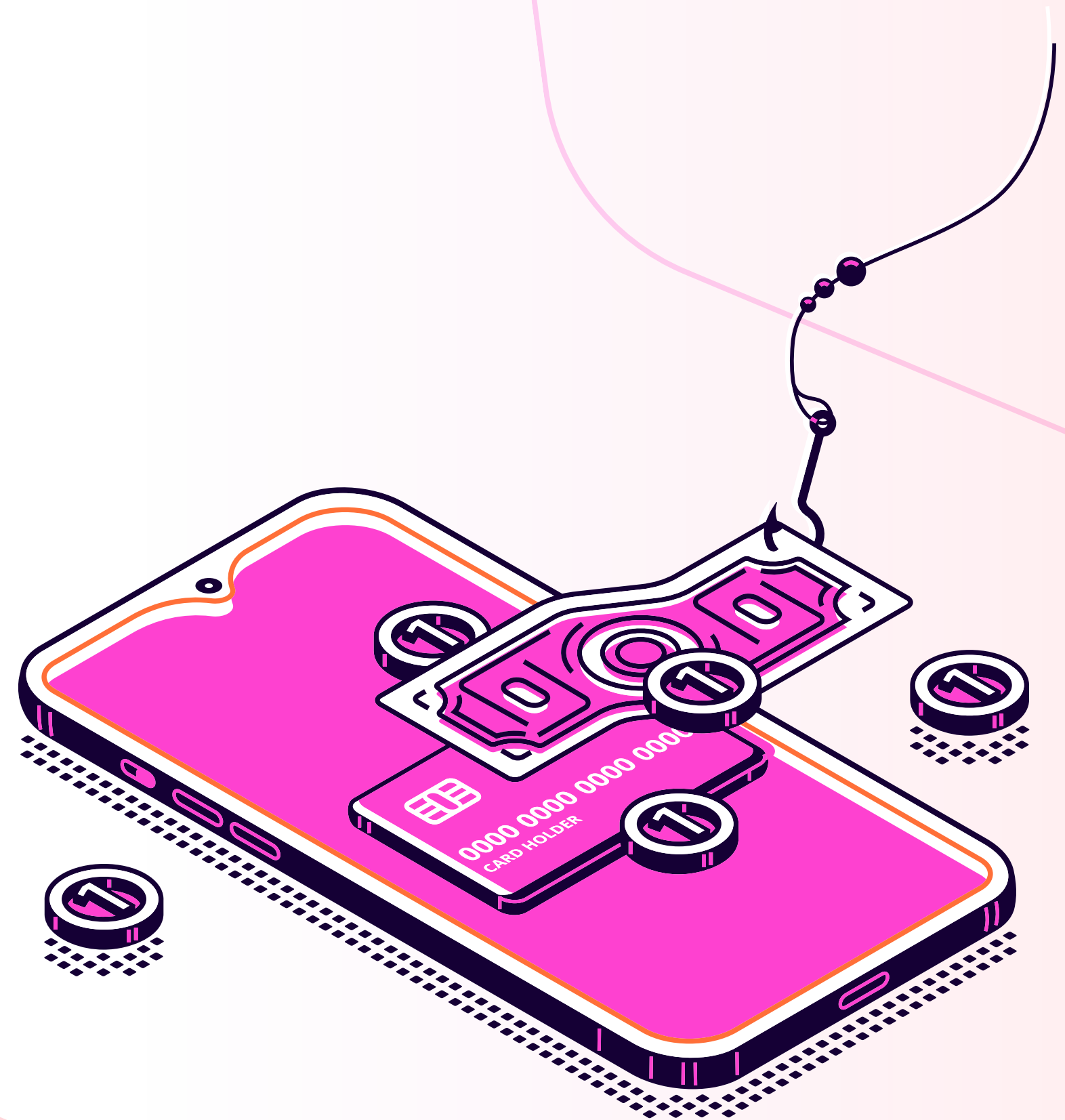
Michele Covi

10/06/2024

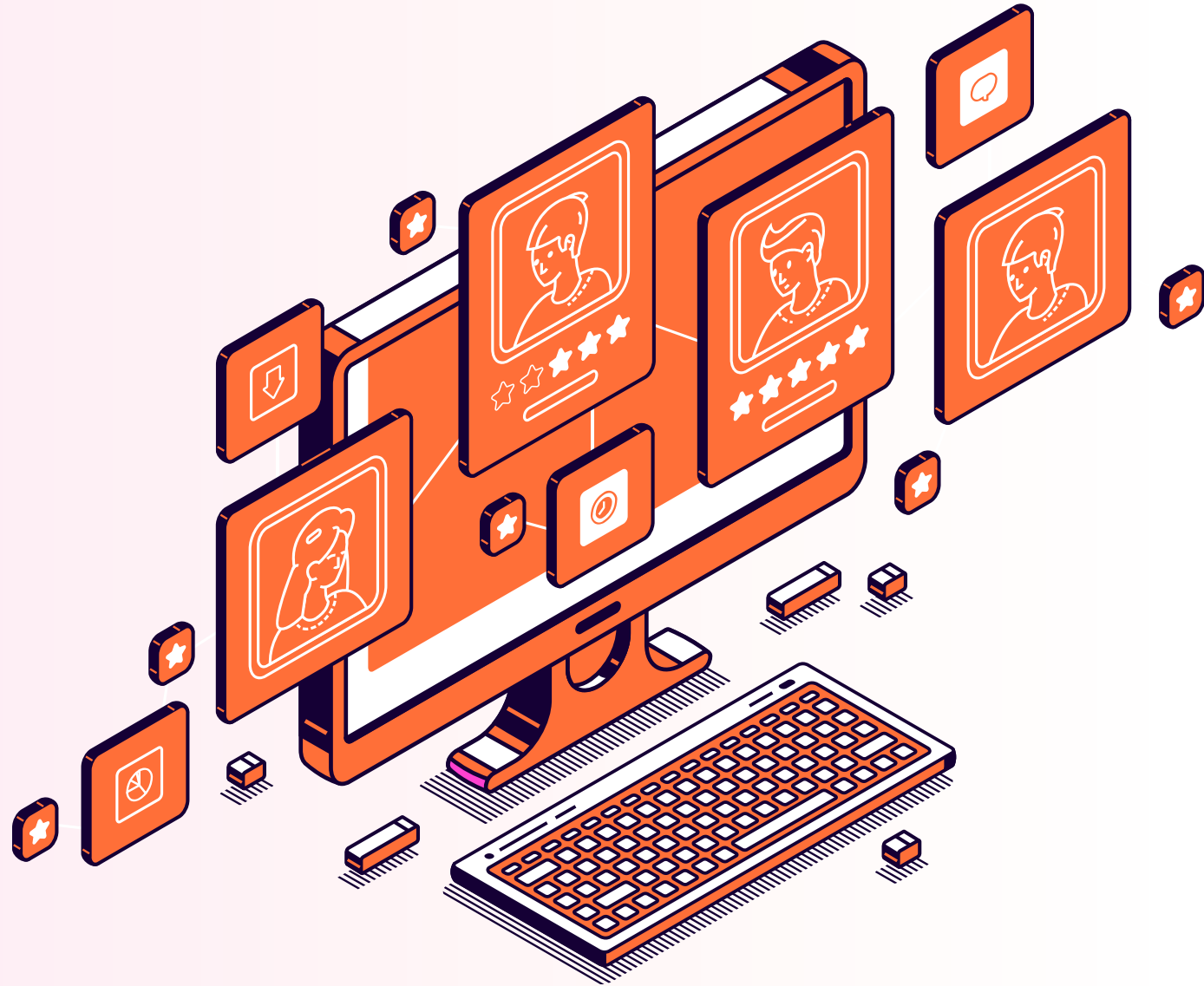
Introduzione

Il presente report dettaglia l'analisi statica del file eseguibile `Malware_U3_W2_L1.exe`, condotta nell'ambito delle attività di sicurezza informatica per identificare e comprendere le potenziali minacce rappresentate dal file in esame. L'obiettivo è valutare le capacità del malware, le sue interazioni con il sistema ospitante e delineare le misure preventive e di mitigazione appropriate.

L'analisi è stata eseguita utilizzando CFF Explorer, uno strumento avanzato per l'analisi di file eseguibili Windows. Questo strumento permette di esaminare dettagliatamente le strutture interne del file, inclusi headers, sezioni e importazioni di librerie, fornendo una visione comprensiva delle capacità operative del malware.



Dettagli del File Analizzato



✦ **Nome del File: Malware_U3_W2_L1.exe**

✦ **Dimensione del File: 16 KB**

✦ **Tipo di File: Eseguitabile Windows (PE)**

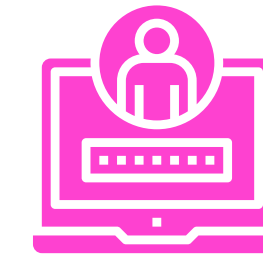
Analisi delle Librerie Importate

Durante l'analisi statica con CFF Explorer, sono state identificate diverse librerie dinamiche cruciali per la funzionalità del malware:



Kernel32.dll

Gestisce operazioni essenziali di sistema quali creazione di processi e thread, e manipolazione della memoria.



Advapi32.dll

Implementa funzioni avanzate relative alla sicurezza, quali la gestione dei registri e dei servizi Windows



Msvcrt.dll

Libreria standard C di Microsoft, utilizzata per operazioni generali come manipolazione di stringhe e calcoli.

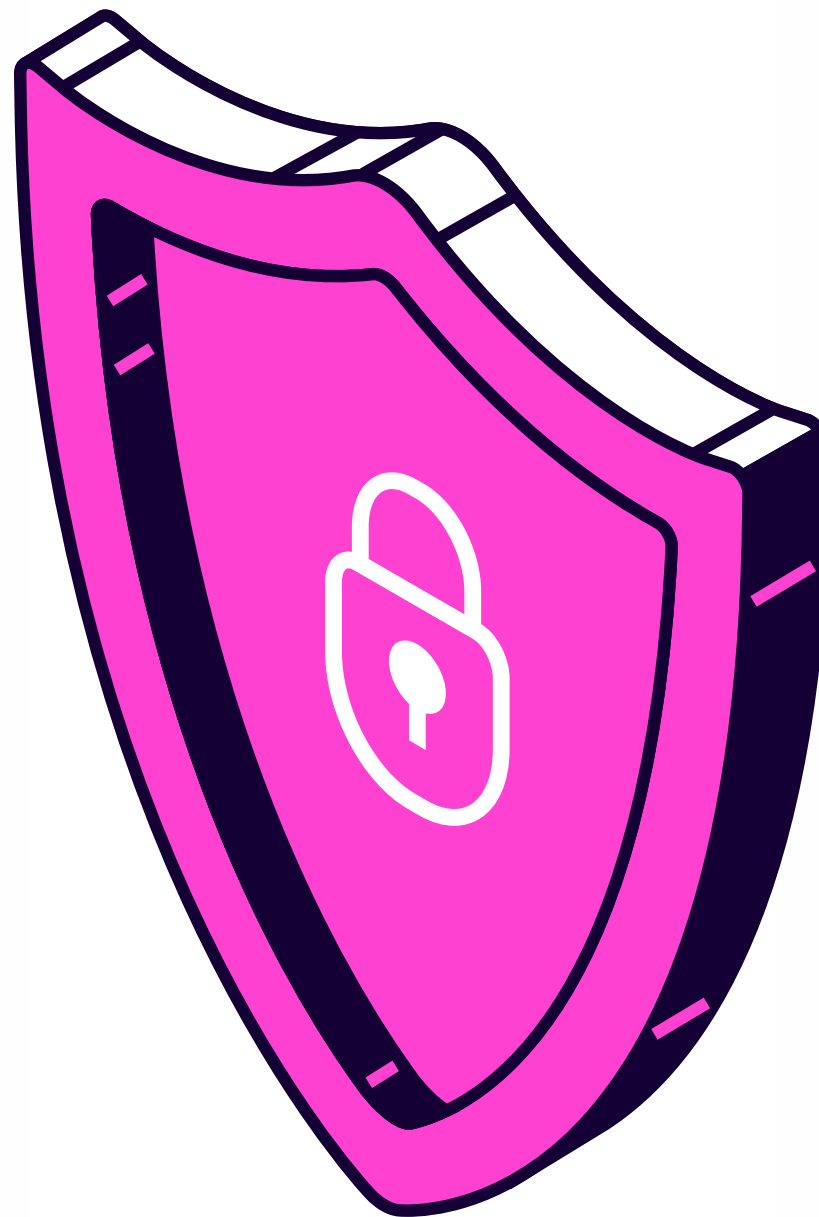


Wininet.dll

Fornisce funzionalità di networking, inclusi protocolli come HTTP e FTP, per comunicazioni di rete.

Analisi delle Sezioni del File

Il file contiene tre sezioni principali che sono state esaminate per comprendere meglio la distribuzione del codice e dei dati



01.

.text:

Sezione che contiene il codice eseguibile del malware. Questa sezione è marcata come eseguibile e non modificabile.

02.

.rdata:

Contiene dati costanti, come stringhe e configurazioni. È configurata come non eseguibile e solo lettura.

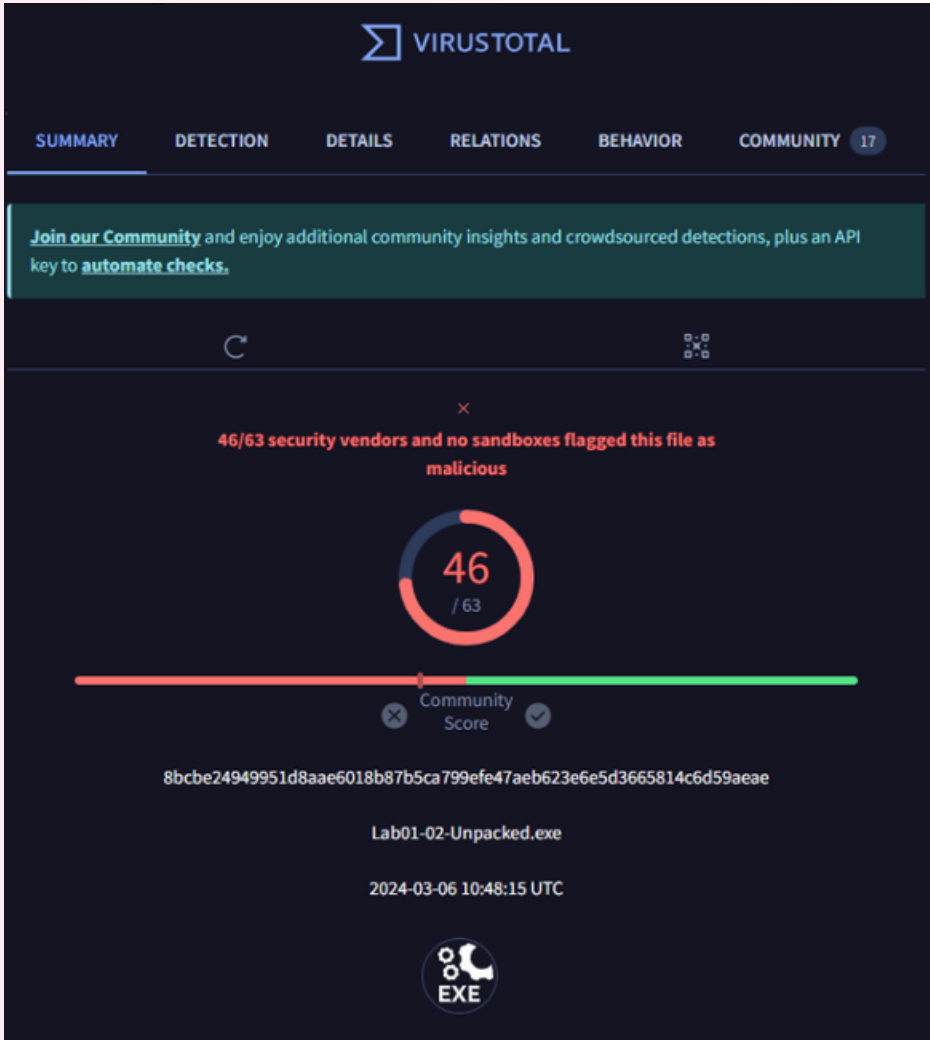
03.

.data:

Alloggia dati variabili utilizzati dal malware durante la sua esecuzione, marcata come leggibile e scrivibile.

Analisi con VirusTotal

Il file è stato inoltre sottoposto ad analisi tramite VirusTotal, che ha coinvolto 63 motori di sicurezza differenti. Il file è stato identificato come malevolo da 46 motori, evidenziando un'ampia riconoscenza del suo potenziale nocivo tra gli strumenti di sicurezza. È stato classificato principalmente come trojan, con attributi di spyware e rogue, indicando una capacità di compromissione significativa.



Popular threat label	trojan.rogue/trojanclicker	Threat categories	trojan	spy	Family labels	rogue	trojancli
Security vendors' analysis							
Do you want to automate checks?							
AhnLab-V3	!	Trojan.Win32.StartPage.C26214					
Alibaba	!	TrojanClicker:Win32/Tnega.2f275f7c					
ALYac	!	Gen:Variant.Ser.Ulise.216					
Antiy-AVL	!	Trojan.Win32.TSGeneric					
Avast	!	Win32:AdwareX-gen [Adw]					
Avert Labs	!	GenericRXEE-Y5IAE4CA70697DF					
AVG	!	Win32:AdwareX-gen [Adw]					
Avira (no cloud)	!	TR/Rogue.7734716					
BitDefenderTheta	!	Gen:NN.ZexaF.36802.bmW@aG9@v0b					
Bkav Pro	!	W32.AIDetectMalware					
CrowdStrike Falcon	!	Win/malicious_confidence_100% (W)					
Cylance	!	Unsafe					
Cynet	!	Malicious (score: 100)					
DeepInstinct	!	MALICIOUS					
Elastic	!	Malicious (high Confidence)					
eScan	!	Gen:Variant.Ser.Ulise.216					
ESET-NOD32	!	A Variant Of Win32/TrojanClicker.Agent.NVM					
Fortinet	!	W32/Agent.NVMltr					
Google	!	Detected					
Ikarus	!	Trojan.Win32.TrojanClicker					
Jiangmin	!	Trojan.Generic.fdlq					
K7AntiVirus	!	Spyware (0049d4ae1)					
K7GW	!	Spyware (0049d4ae1)					
Kingsoft	!	Win32.Troj.Generic.a					
Lionic	!	Trojan.Win32.Rogue.4lc					
Malwarebytes	!	RiskWare.Agent.MWLA					
MaxSecure	!	Trojan.Malware.2588.susgen					

Microsoft	!	Trojan.Win32/Tnega!MSR
NANO-Antivirus	!	Trojan.Win32.Click3.lvtltd
Rising	!	Trojan.Clicker-Agent!8.13 (TFE:5:kDYthMGEbcJ)
Sangfor Engine Zero	!	Suspicious.Win32.Save.ins
Skyhigh (SWG)	!	GenericRXEE-Y5IAE4CA70697DF
Sophos	!	Mal/Generic-R
Symantec	!	ML.Attribute.HighConfidence
Trapmine	!	Malicious.moderate.ml.score
Trellix (FireEye)	!	Generic.mg.ae4ca70697df5506
TrendMicro	!	TROJ_GEN.R002C0DAK24
TrendMicro-HouseCall	!	TROJ_GEN.R002C0DAK24
Varist	!	W32/Agent.DJC.gen!Eldorado
VBA32	!	Trojan.Click
VirIT	!	Trojan.Win32.Generic.CMEY
Webroot	!	W32.Malware.Heur
WithSecure	!	Trojan.TR/Rogue.7734716
Xcitium	!	Malware@#2m8d1kwsdlvz3
Yandex	!	Trojan.GenAsa!+rorTzIz07A
Zillya	!	Trojan.Agent.Win32.557086
Acronis (Static ML)	✓	Undetected
Baidu	✓	Undetected
ClamAV	✓	Undetected
CMC	✓	Undetected
Gridinsoft (no cloud)	✓	Undetected
Kaspersky	✓	Undetected
Palo Alto Networks	✓	Undetected
Panda	✓	Undetected
QuickHeal	✓	Undetected

Considerazioni Finali e Raccomandazioni

L'analisi statica fornisce un quadro preoccupante del potenziale di danneggiamento del malware, con capacità di manipolazione del sistema operativo e di comunicazione con server esterni.

Si raccomandano le seguenti azioni:

- Monitoraggio Continuo: Implementare un'analisi dinamica per tracciare il comportamento del malware in un ambiente controllato.
- Aggiornamenti di Sicurezza: Assicurarsi che tutti i sistemi operativi e le applicazioni siano aggiornati per mitigare le vulnerabilità note.
- Formazione e Consapevolezza: Educare gli utenti finali sulla identificazione e gestione dei file sospetti.