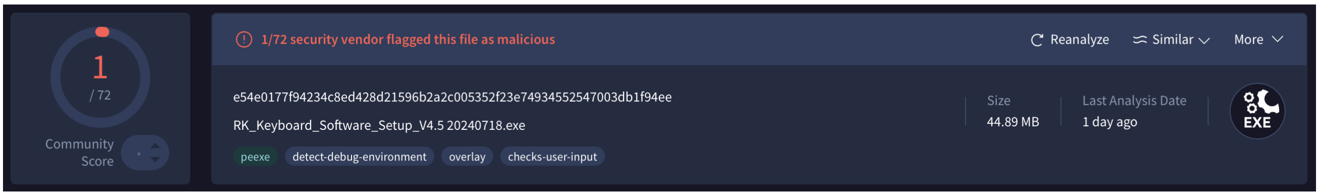
Analisi File e Software

Ho caricato il seguente file: "RK_Keyboard_Software_Setup_V4.5%2020240718.exe" si tratta dell'eseguibile per windows di un software per settare la tastiera.
Il file è stato scaricato dal sito originale della azienda che le produce: "Keyboards Link"

VirusTotal



1/72 security vendor flagged this file as malicious

1 / 72

Community Score

e54e0177f94234c8ed428d21596b2a2c005352f23e74934552547003db1f94ee

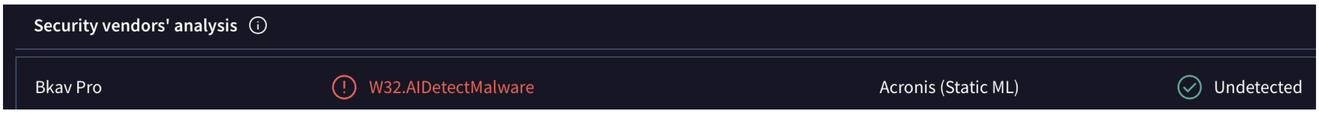
RK_Keyboard_Software_Setup_V4.5 20240718.exe

peexe detect-debug-environment overlay checks-user-input

Size 44.89 MB

Last Analysis Date 1 day ago

Vediamo dunque come ci sia una presenza di malware all'interno dell'eseguibile, vedendo nello specifico :

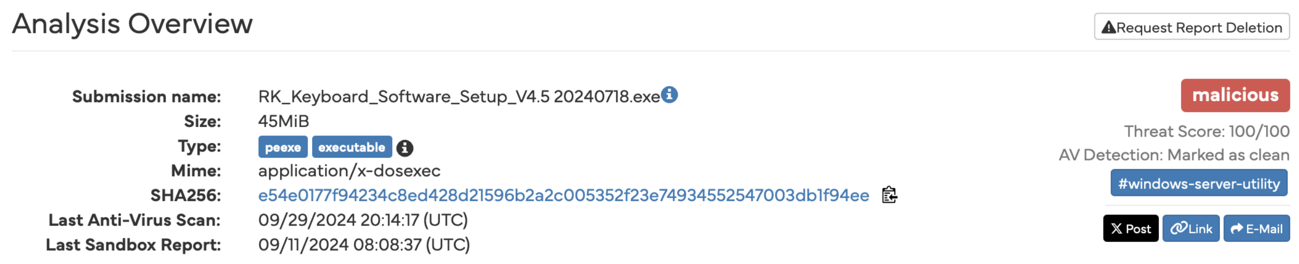


Security vendors' analysis

Bkav Pro	W32.AIDetectMalware	Acronis (Static ML)	Undetected

Documentandomi "Bkav Pro" sarebbe il software antivirus che ha trovato una traccia di malware, precisamente "W32" suggerisce che si tratta di un malware per il sistema operativo Windows, mentre la dicitura "AIDetectMalware" implica che è stato rilevato tramite una tecnologia di intelligenza artificiale o comunque un algoritmo di rilevamento avanzato. Esaminando la tipologia di malware in rete spesso parlano di un falso positivo. allora per esserne certi ho analizzato l'eseguibile con un ulteriore analizzatore.

Hybrid Analysis



Analysis Overview

Submission name:	RK_Keyboard_Software_Setup_V4.5 20240718.exe
Size:	45MiB
Type:	peexe executable
Mime:	application/x-dosexec
SHA256:	e54e0177f94234c8ed428d21596b2a2c005352f23e74934552547003db1f94ee
Last Anti-Virus Scan:	09/29/2024 20:14:17 (UTC)
Last Sandbox Report:	09/11/2024 08:08:37 (UTC)

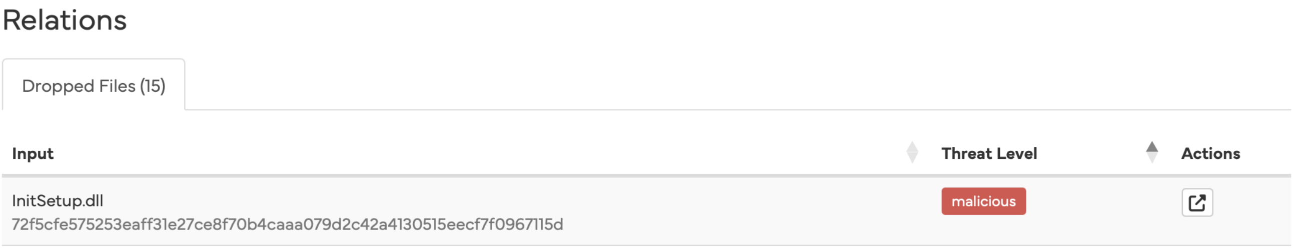
malicious

Threat Score: 100/100

AV Detection: Marked as clean

#windows-server-utility

Anche in questo caso abbiamo che lo stesso file precedente riporta un malware, andiamo quindi a vedere nello specifico di cosa si tratta.

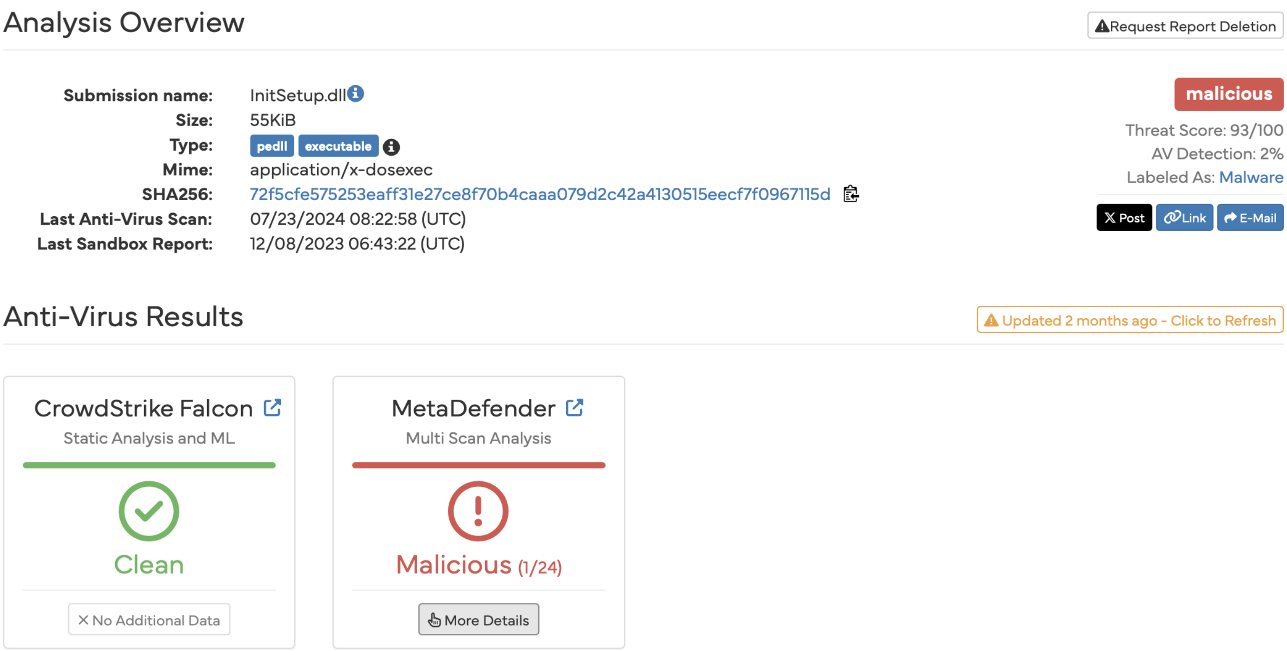


Relations

Dropped Files (15)

Input	Threat Level	Actions
InitSetup.dll 72f5cfe575253eaff31e27ce8f70b4caaa079d2c42a4130515eecf7f0967115d	malicious	

Vediamo che il file "InitSetup.dll" riporta al suo interno una minaccia, andando ad analizzare quel file in effetti l'antivirus "MetaDefender" riporta un messaggio di file infetto.



Analysis Overview

Submission name:	InitSetup.dll
Size:	55KiB
Type:	pedll executable
Mime:	application/x-dosexec
SHA256:	72f5cfe575253eaff31e27ce8f70b4caaa079d2c42a4130515eecf7f0967115d
Last Anti-Virus Scan:	07/23/2024 08:22:58 (UTC)
Last Sandbox Report:	12/08/2023 06:43:22 (UTC)

malicious

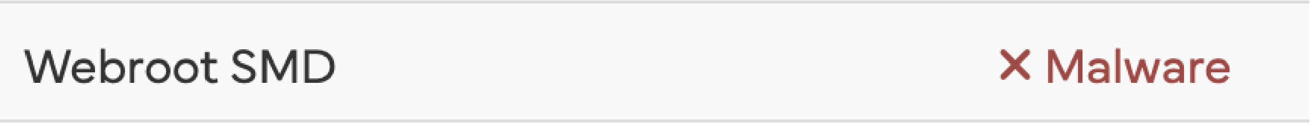
Threat Score: 93/100
AV Detection: 2%
Labeled As: Malware

Anti-Virus Results

CrowdStrike Falcon
Static Analysis and ML
Clean

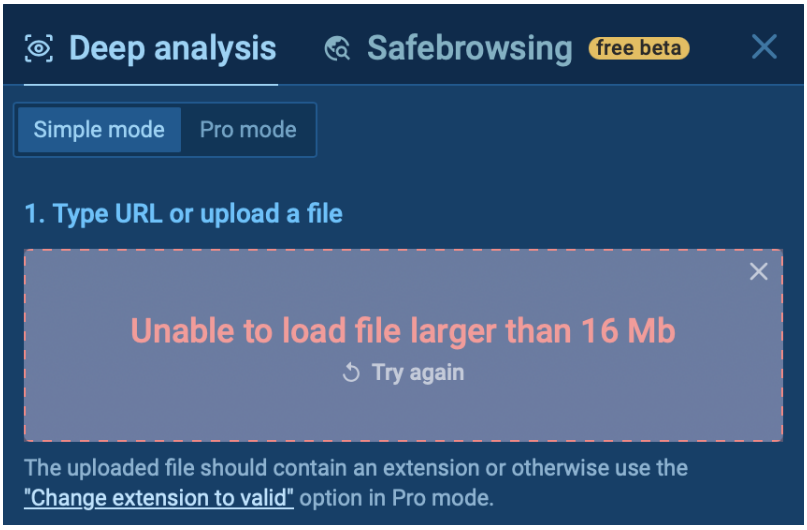
MetaDefender
Multi Scan Analysis
Malicious (1/24)

Di seguito riportata la tipologia di malware.



Webroot SMD ✕ Malware

> Per quanto riguarda il sito "Anyrun", il file era troppo pesante e non sono riuscita ad analizzarlo, richiede un massimo di 16 MB:



1. Type URL or upload a file

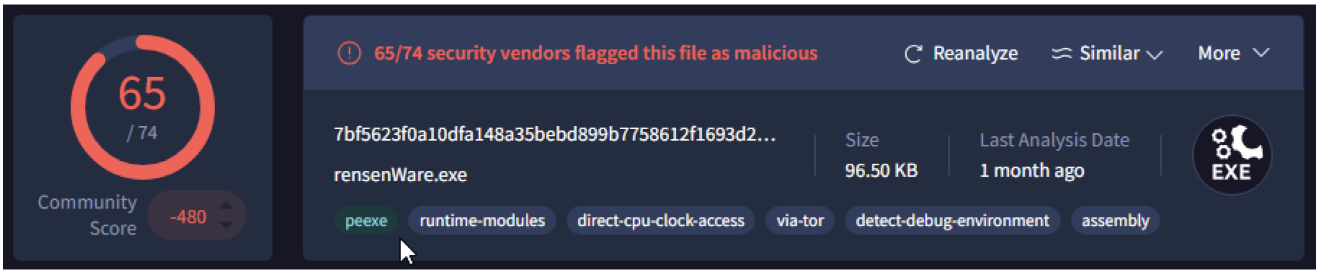
Unable to load file larger than 16 Mb

The uploaded file should contain an extension or otherwise use the "Change extension to valid" option in Pro mode.

Proviamo ora a testare un altro tipo di file, così da poter sfruttare anche l'ultimo sito.

Tramite una macchina virtuale con installato il sistema operativo Windows, ho deciso di provare ad analizzare un malware di tipo ransomware chiamato, appunto, ransomware.exe scaricato da una repository di github.

VirusTotal



65 / 74

Community Score -480

65/74 security vendors flagged this file as malicious

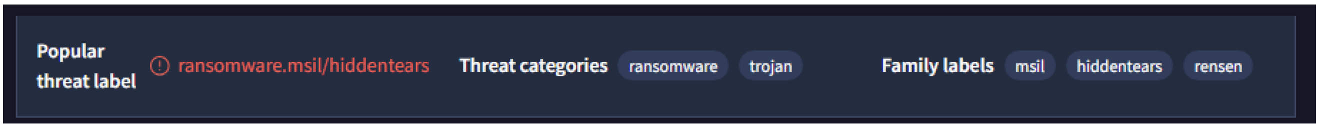
7bf5623f0a10dfa148a35bebd899b7758612f1693d2...

rensenWare.exe

Size: 96.50 KB

Last Analysis Date: 1 month ago

peexe · runtime-modules · direct-cpu-clock-access · via-tor · detect-debug-environment · assembly



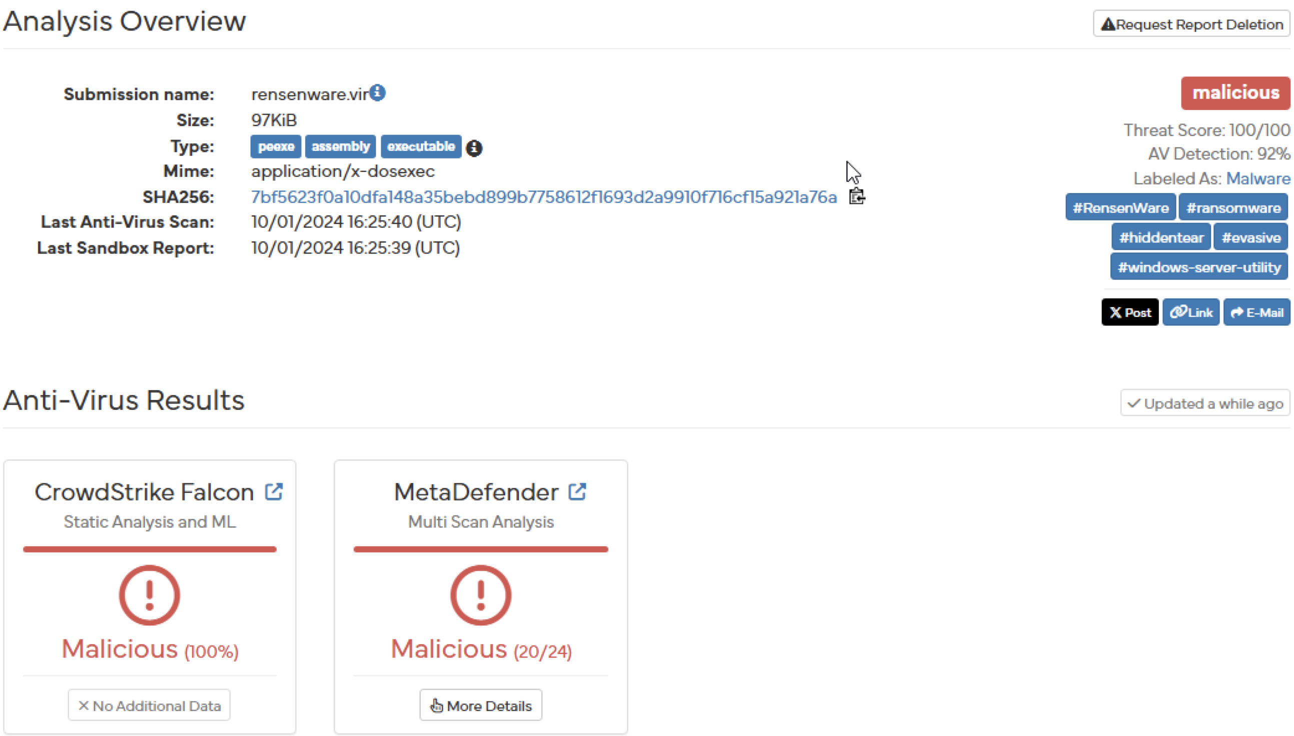
Popular threat label: ransomware.msil/hiddentears

Threat categories: ransomware · trojan

Family labels: msil · hiddentears · rensen

Possiamo vedere dagli screen che il sito VirusTotal rileva molte minacce, che vengono categorizzate in minacce di tipo ransomware e trojan.

Hybrid Analysis



Analysis Overview

Submission name:	rensenware.vir
Size:	97KiB
Type:	peexe assembly executable
Mime:	application/x-dosexec
SHA256:	7bf5623f0a10dfa148a35bebd899b7758612f1693d2a9910f716cf15a921a76a
Last Anti-Virus Scan:	10/01/2024 16:25:40 (UTC)
Last Sandbox Report:	10/01/2024 16:25:39 (UTC)

malicious

Threat Score: 100/100

AV Detection: 92%

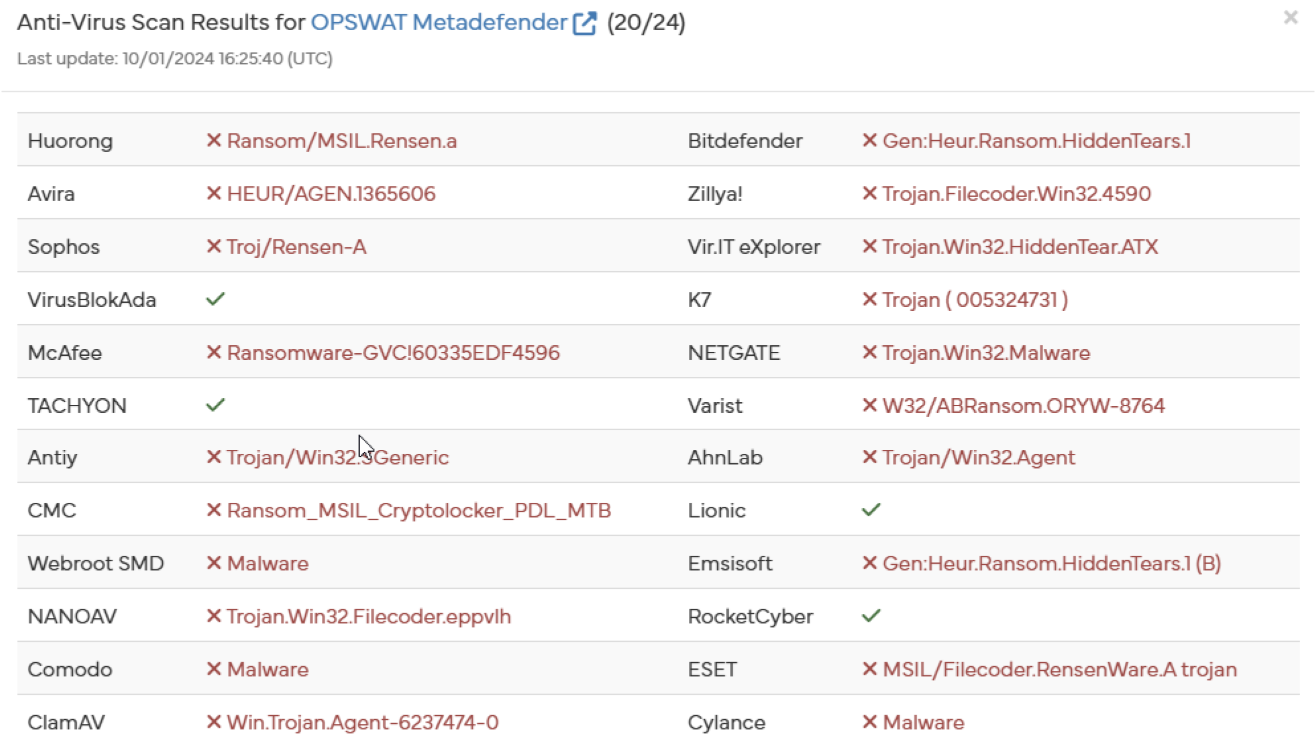
Labeled As: Malware

#RensenWare #ransomware #hiddentear #evasive #windows-server-utility

Anti-Virus Results

CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)

MetaDefender
Multi Scan Analysis
Malicious (20/24)



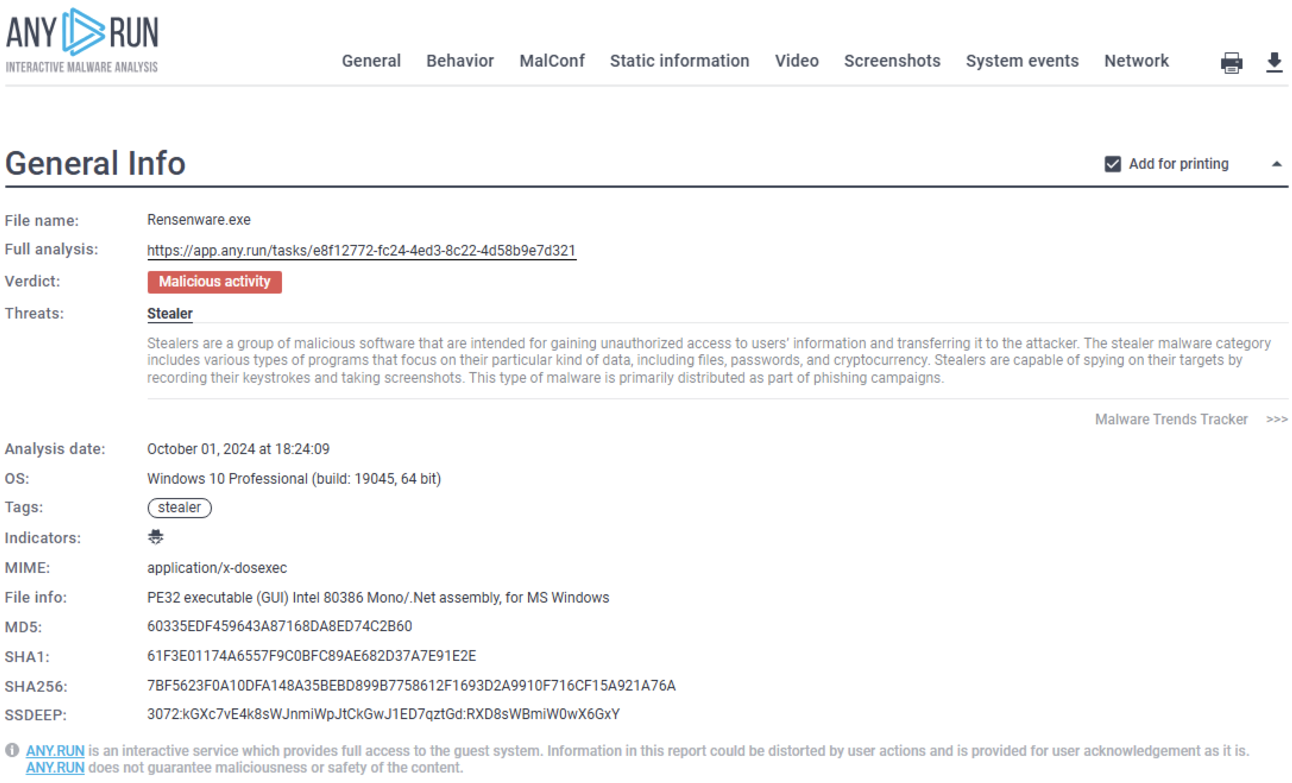
Anti-Virus Scan Results for OPSWAT Metadefender (20/24)
Last update: 10/01/2024 16:25:40 (UTC)

Huorong	✕ Ransom/MSIL.Rensen.a	Bitdefender	✕ Gen:Heur.Ransom.HiddenTears.1
Avira	✕ HEUR/AGEN.1365606	Zillya!	✕ Trojan.Filecoder.Win32.4590
Sophos	✕ Troj/Rensen-A	Vir.IT eXplorer	✕ Trojan.Win32.HiddenTear.ATX
VirusBlokAda	✓	K7	✕ Trojan (005324731)
McAfee	✕ Ransomware-GVC!60335EDF4596	NETGATE	✕ Trojan.Win32.Malware
TACHYON	✓	Varist	✕ W32/ABRansom.ORYW-8764
Antiy	✕ Trojan/Win32.SGeneric	AhnLab	✕ Trojan/Win32.Agent
CMC	✕ Ransom_MSIL_Cryptolocker_PDL_MTB	Lionic	✓
Webroot SMD	✕ Malware	Emsisoft	✕ Gen:Heur.Ransom.HiddenTears.1 (B)
NANOAV	✕ Trojan.Win32.Filecoder.eppvlh	RocketCyber	✓
Comodo	✕ Malware	ESET	✕ MSIL/Filecoder.RensenWare.A trojan
ClamAV	✕ Win.Trojan.Agent-6237474-0	Cylance	✕ Malware

Ovviamente anche Hybrid Analysis rileva molteplici malware di diverso tipo.

AnyRUN

Passiamo infine al sito web di analisi che ancora non avevamo affrontato e possiamo vedere come, anch'esso, rileva malware.



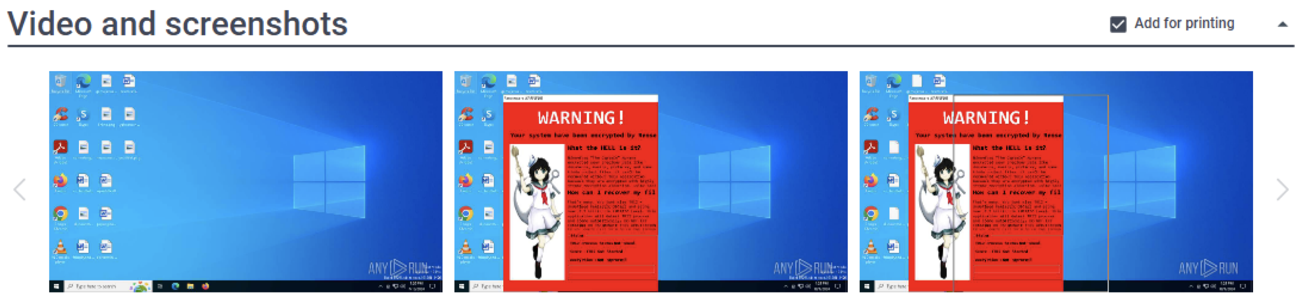
General Info

☑ Add for printing

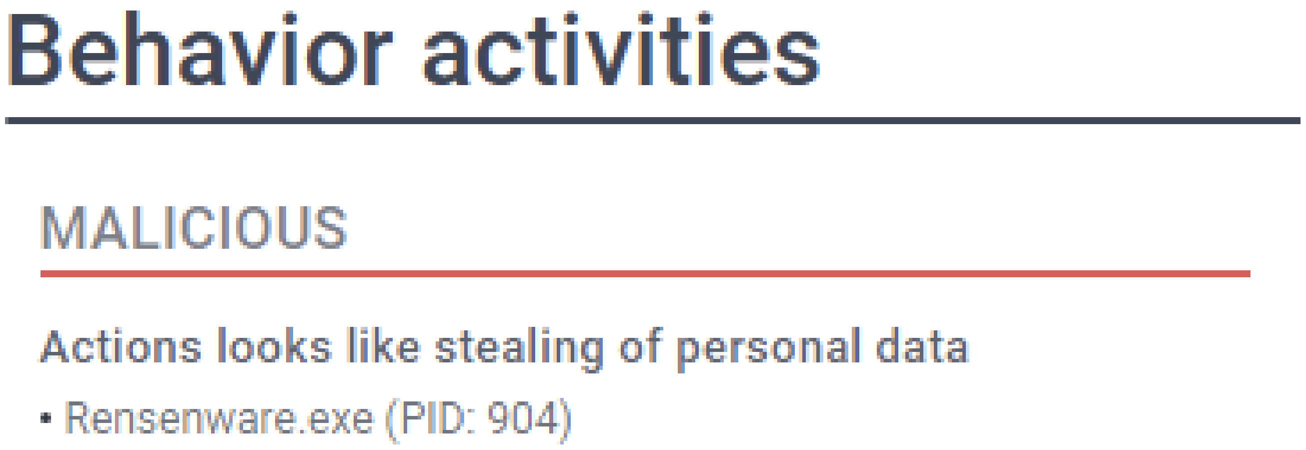
File name:	Rensenware.exe
Full analysis:	https://app.any.run/tasks/e8f12772-fc24-4ed3-8c22-4d58b9e7d321
Verdict:	Malicious activity
Threats:	Stealer Stealers are a group of malicious software that are intended for gaining unauthorized access to users' information and transferring it to the attacker. The stealer malware category includes various types of programs that focus on their particular kind of data, including files, passwords, and cryptocurrency. Stealers are capable of spying on their targets by recording their keystrokes and taking screenshots. This type of malware is primarily distributed as part of phishing campaigns. Malware Trends Tracker >>>
Analysis date:	October 01, 2024 at 18:24:09
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	stealer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	60335EDF459643A87168DA8ED74C2B60
SHA1:	61F3E01174A6557F9C0BFC89AE682D37A7E91E2E
SHA256:	7BF5623F0A10DFA148A35BEBD899B7758612F1693D2A9910F716CF15A921A76A
SSDEEP:	3072:kGXc7vE4k8sWJnmiWpJtCkGwJ1ED7qztGd:RXD8sWBmiW0wX6GxY

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Vediamo negli screen seguenti, l'apparizione di un pop-up poco raccomandabile, trattandosi a tutti gli effetti di un virus.



Il programma ci suggerisce che potrebbe essere un virus che potrebbe rubare i nostri dati personali.



Behavior activities

MALICIOUS

Actions looks like stealing of personal data

- Rensenware.exe (PID: 904)