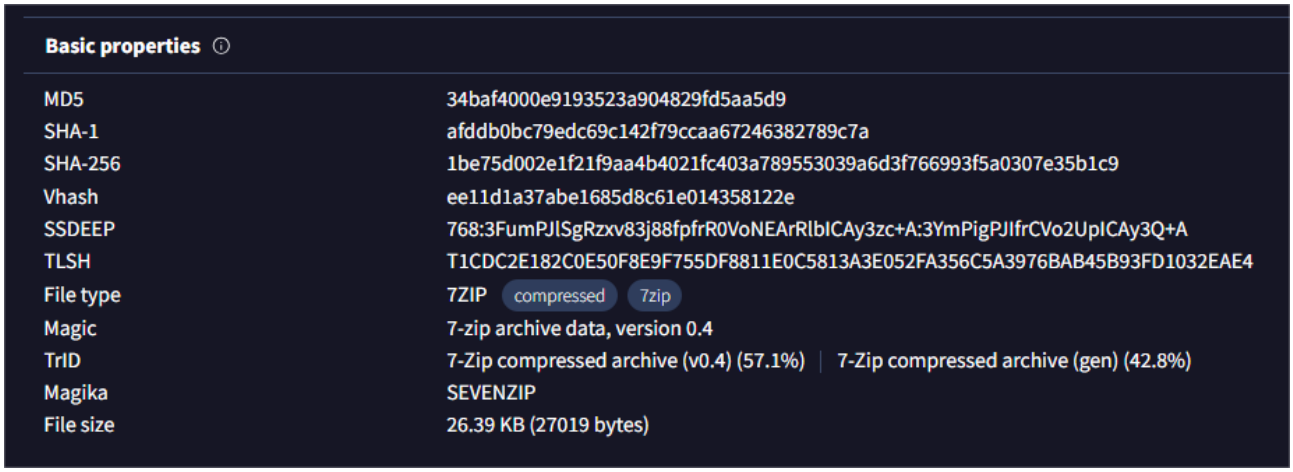
EXTRA 1 – BUILD WEEK 3

TRACCIA : Analisi Forense: Attraverso l'analisi del codice sorgente, potete imparare come funziona un malware dal punto di vista tecnico. Questo include l'analisi delle funzioni di propagazione, le tecniche di evasione dei sistemi di sicurezza, e la comprensione di come il malware gestisce la comunicazione con i server di comando e controllo.

https://github.com/akir4d/MalwareSourceCode/raw/main/Win32/Win32.Mydoom.a.7z.

PRESENTAZIONE: Ci viene presentato un file rar che contiene un malware che andremo ad analizzare. Per prima cosa per estrarre i metadati del campione lo vado a inserire su Virustotal.



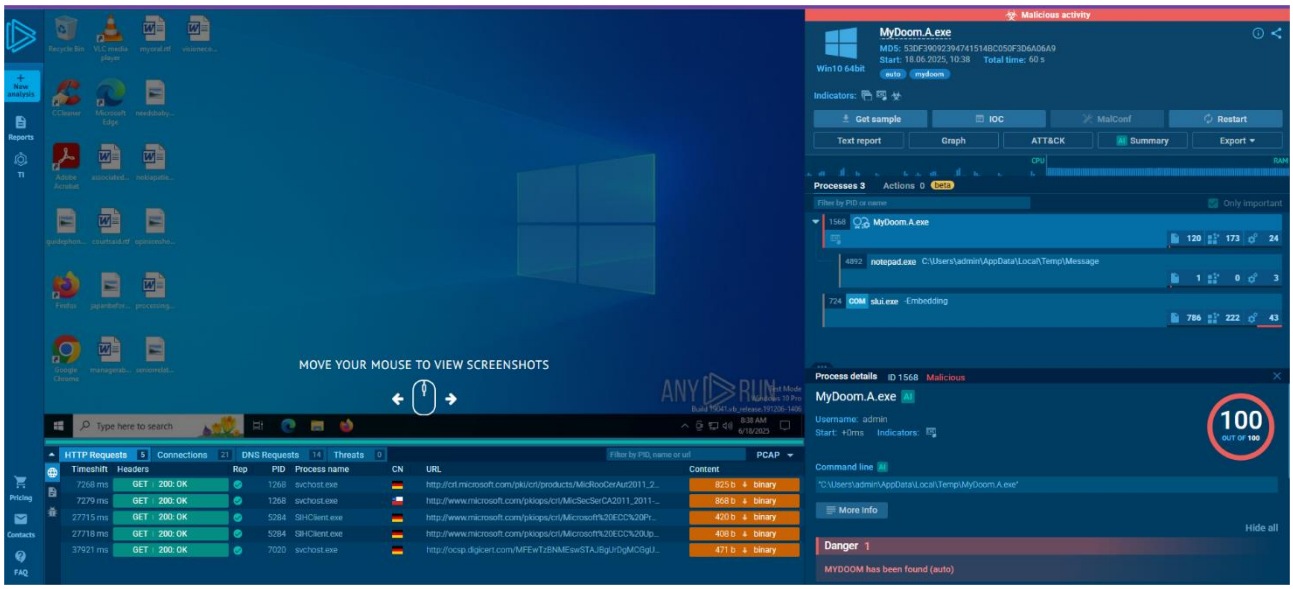
Basic properties

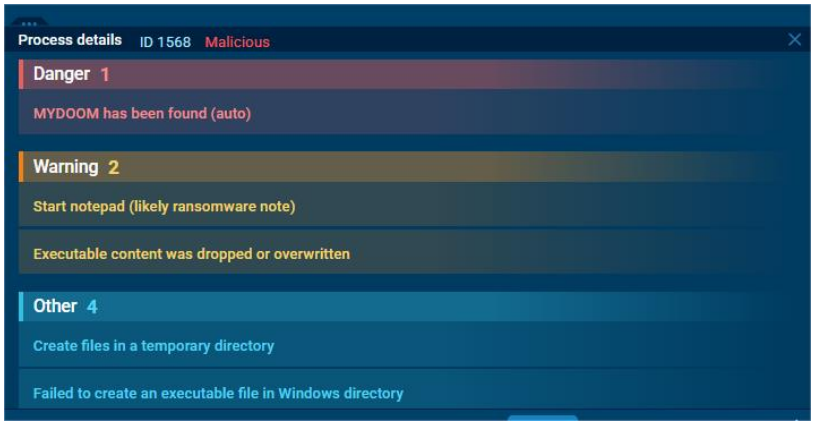
MD5	34baf4000e9193523a904829fd5aa5d9
SHA-1	afddb0bc79edc69c142f79ccaa67246382789c7a
SHA-256	1be75d002e1f21f9aa4b4021fc403a789553039a6d3f766993f5a0307e35b1c9
Vhash	ee11d1a37abe1685d8c61e014358122e
SSDEEP	768:3FumPJlSgRzxv83j88fpfrR0VoNEArRlbICAy3zc+A:3YmPigPJIfrCVo2UpICAy3Q+A
TLSH	T1CDC2E182C0E50F8E9F755DF8811E0C5813A3E052FA356C5A3976BAB45B93FD1032EAE4
File type	7ZIP compressed 7zip
Magic	7-zip archive data, version 0.4
TrID	7-Zip compressed archive (v0.4) (57.1%) | 7-Zip compressed archive (gen) (42.8%)
Magika	SEVENZIP
File size	26.39 KB (27019 bytes)

In questo screen troviamo le proprietà di base come **MD5**, **SHA-1** E **SHA-256.**

Come passo successivo ho deciso di analizzare il malware su anyrun cosi da avere una visione più completa e chiara.

L'archivio contiene un file eseguibile principale MyDoom.exe e vari fari ausiliari. L'analisi dei metadati mostra che il payload è una variante di MyDoom , con i comportamenti di un worm: **Capacità di droppare file** , **propagarsi sulla rete locale** e **persistere nel sistema**.





Processi del malware.

Durante l'esecuzione possiamo notare i processi principali e dopo l'estrazione possiamo notare come viene notato subito il pericolo, MyDoom.exe viene eseguito in PID multipli cercando tentativi continui di replicazione e persistence.

Il malware mostra comportamenti coerenti con la creazione di meccanismi di quest'ultima: è probabile che modifichi chiavi di registro tipo **HKCU...\Run** o **HKLM...\Run** per garantirsi l'esecuzione automatica all'avvio dell'utente/sistema.

Successivamente viene subito aperto un file messaggio di nome notepad.exe come un tipico payload secondario.

L’apertura di notepad.exe con un file di messaggio è un comportamento secondario tipico di alcune varianti di MyDoom: viene usato per distrarre l’utente o simulare un errore mentre le operazioni di droppaggio e persistence avvengono in background.Per concludere viene mostrata l’apertura di taskmgr.exe per monitorare i processi.

ATTIVITA’ OSSERVATE

- Dropping di file in %TEMP% e C:\Windows\System32\ coerente con tentativo di persistence.
- Modifica di chiavi di registro relative a WinRAR
- Connessioni di rete principalmente broadcast/multicast su NetBIOS/LLMNR. Nessuna comunicazione http verso server esterni
- L’uso di traffico NetBIOS e LLMNR (broadcast/multicast su porte 137/138 e 5355) indica che la finalità principale è la **propagazione orizzontale**: il worm cerca altri host nella LAN per mappare condivisioni e infettare la rete locale.
- Comportamento coerente con worm/loader e replicazione multipla.

Nel periodo di osservazione non sono state rilevate comunicazioni HTTP o C2 verso server esterni: questo supporta la classificazione come **Worm/Loader** focalizzato sulla diffusione locale piuttosto che sul controllo remoto o sull’esfiltrazione massiva.

MAPPING MITRE&CK

- **Persistence:** Creazione di file e posizionamento di DLL in directory di sistema (es. shimgapi.dll).

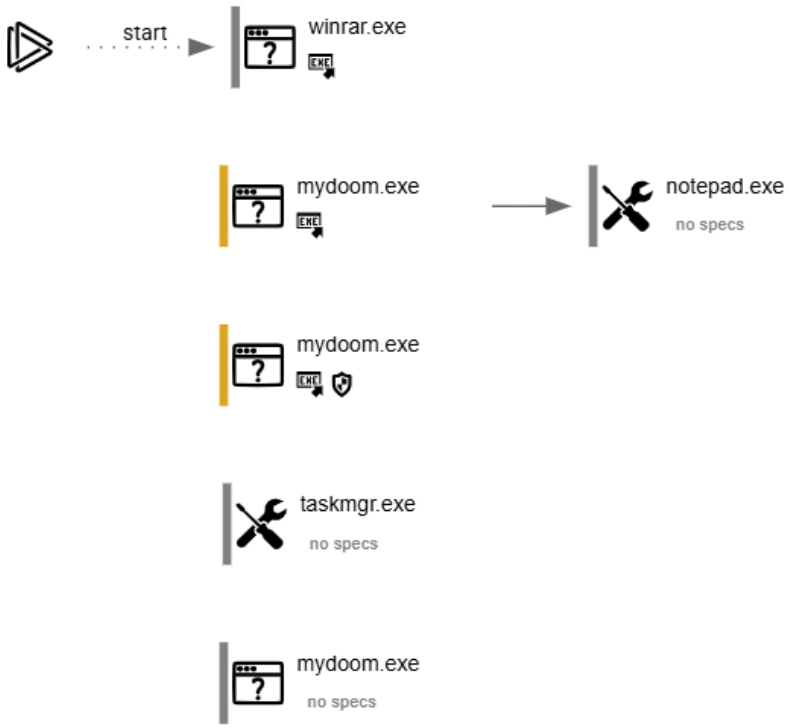
- **Lateral Movement:** Uso di NetBIOS/LLMNR per individuare e infettare host nella LAN.
- **Defense Evasion:** Camuffamento tramite nomi di file simili a componenti di sistema (DLL side-loading/hijacking).

Per capire meglio il funzionamento del worm ho raccolto i paths:

- %TEMP%\MyDoom\MyDoom.exe
- %TEMP%\MyDoom\shimgapi.dll
- %TEMP%\Message

È stato droppato un file DLL con nome simile a componenti di sistema (shimgapi.dll), comportamento tipico di **DLL hijacking / side-loading**: il malware posiziona una DLL che imita un file legittimo per essere caricata da processi affidabili e nascondere l'esecuzione malevola.

Nelle mie ricerche su internet ho trovato un process tree (un schematizzazione dei processi) che ci aiuta a capire chiaramente ciò che ho spiegato precedentemente.



IMPATTO E VALUTAZIONE DEL RISCHIO

Il rischio è molto alto su reti non isolate, il malware può propagarsi via lan e persistere nel sistema tramite DLL.

COSA FARE PER RIPARARE I DANNI

- Isolare la macchina
- Bloccare IoC sul firewall
- Scansionare la rete per traffico NETBIOS/LLMNR
- Rimuovere subito i file droppati e ripristinare eventuali modifiche di sistema
- Monitorare altri host nella rete

In conclusione possiamo dire che il file analizzato è un malware con capacità di propagazione LAN e persistence. L'azione principale è il dropping di file ed esecuzione di essi