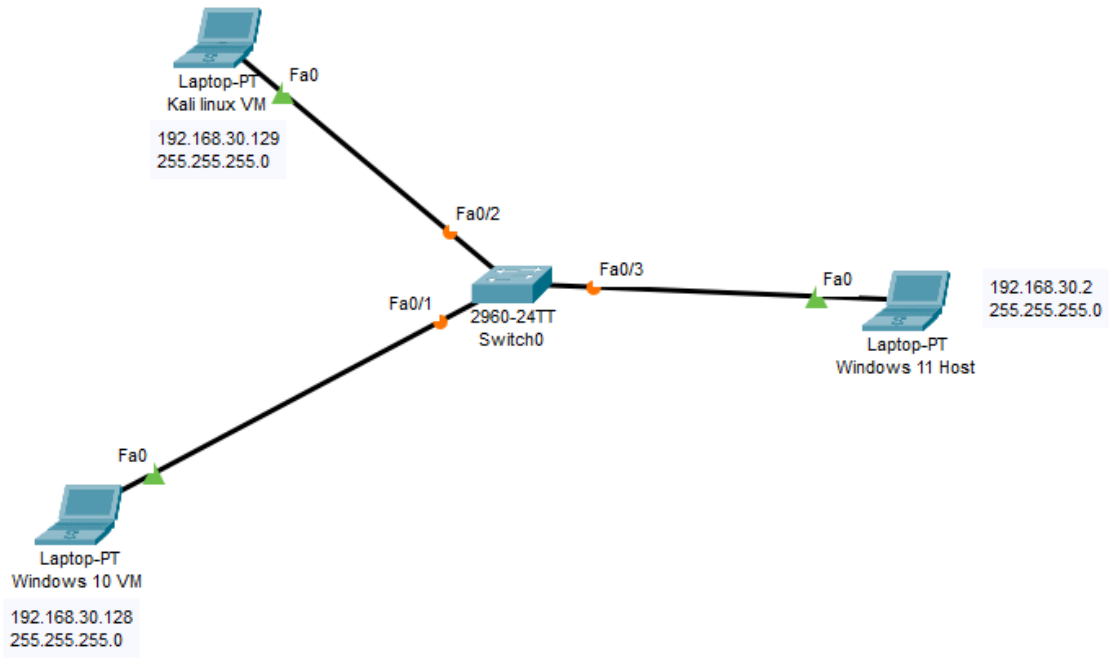
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.129  netmask 255.255.255.0  broadcast 192.168.30.255
        inet6 fe80::f7dd:b744:b640:c9c0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:85:e5:b7  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 1302 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2972 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(kali㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.30.2    0.0.0.0         UG    100    0        0 eth0
192.168.30.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Linux VM – 192.168.30.129
Windows VM – 192.168.30.128
Windows Host (Gateway) – 192.168.30.2

Przykładowy podgląd sieci:



Skanowanie maszyny z Windowsem za pomocą nmap:

Otwarte porty: 135, 139, 445, 5357
Nazwa DESKTOP-MR396HI
Wyświetla się też informacja, że jest to wirtualna maszyna

```
┌──(kali㉿kali)-[~/sledcza/iLEAPP-v.1.18.1]
└─$ nmap -A 192.168.30.128
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 16:54 EST
Nmap scan report for 192.168.30.128
Host is up (0.00043s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DESKTOP-MR396HI, NetBIOS user: <unknown>, NetBIOS MAC: 000c29169263 (VMware)
| smb2-time:
|   date: 2023-01-18T21:55:10
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.98 seconds
```

Kiedy próbujemy pingować linuxem samego siebie, w TCPdump nie jest odnotowane takie zajście

Natomiast kiedy pingujemy Gateway, TCPdump to odnotowuje

```
    192.168.30.129 > 192.168.30.2: ICMP echo request, id 31021, seq 6, length 64
17:06:04.151801 IP (tos 0×0, ttl 128, id 22761, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.30.2 > 192.168.30.129: ICMP echo reply, id 31021, seq 6, length 64
17:06:05.045244 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.30.2 tell 192.168.30.1, length 46
17:06:05.175550 IP (tos 0×0, ttl 64, id 57163, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.30.129 > 192.168.30.2: ICMP echo request, id 31021, seq 7, length 64
17:06:05.175691 IP (tos 0×0, ttl 128, id 22762, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.30.2 > 192.168.30.129: ICMP echo reply, id 31021, seq 7, length 64
17:06:06.199817 IP (tos 0×0, ttl 64, id 57413, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.30.129 > 192.168.30.2: ICMP echo request, id 31021, seq 8, length 64
```

Tcpdump z filtrowaniem pakietów

```
┌──(kali㉿kali)-[~/sledcza/iLEAPP-v.1.18.1]
└─$ sudo tcpdump -i eth0 -v host 192.168.30.2
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:07:50.327770 IP (tos 0×0, ttl 64, id 5191, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.30.129 > 192.168.30.2: ICMP echo request, id 31021, seq 110, length 64
17:07:50.327989 IP (tos 0×0, ttl 128, id 22904, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.30.2 > 192.168.30.129: ICMP echo reply, id 31021, seq 110, length 64
17:07:50.400463 IP (tos 0×0, ttl 64, id 57628, offset 0, flags [DF], proto UDP (17), length 71)
    192.168.30.129.53189 > 192.168.30.2.domain: 6153+ PTR? 2.30.168.192.in-addr.arpa. (43)
17:07:50.402855 IP (tos 0×0, ttl 128, id 22905, offset 0, flags [none], proto UDP (17), length 130)
    192.168.30.2.domain > 192.168.30.129.53189: 6153 NXDomain 0/1/0 (102)
17:07:50.403157 IP (tos 0×0, ttl 64, id 31169, offset 0, flags [DF], proto UDP (17), length 73)
    192.168.30.129.40812 > 192.168.30.2.domain: 29480+ PTR? 129.30.168.192.in-addr.arpa. (45)
17:07:50.405130 IP (tos 0×0, ttl 128, id 22906, offset 0, flags [none], proto UDP (17), length 132)
    192.168.30.2.domain > 192.168.30.129.40812: 29480 NXDomain 0/1/0 (104)
```

TCPdump widzi, że użytkownik wszedł na stronę twitter.com

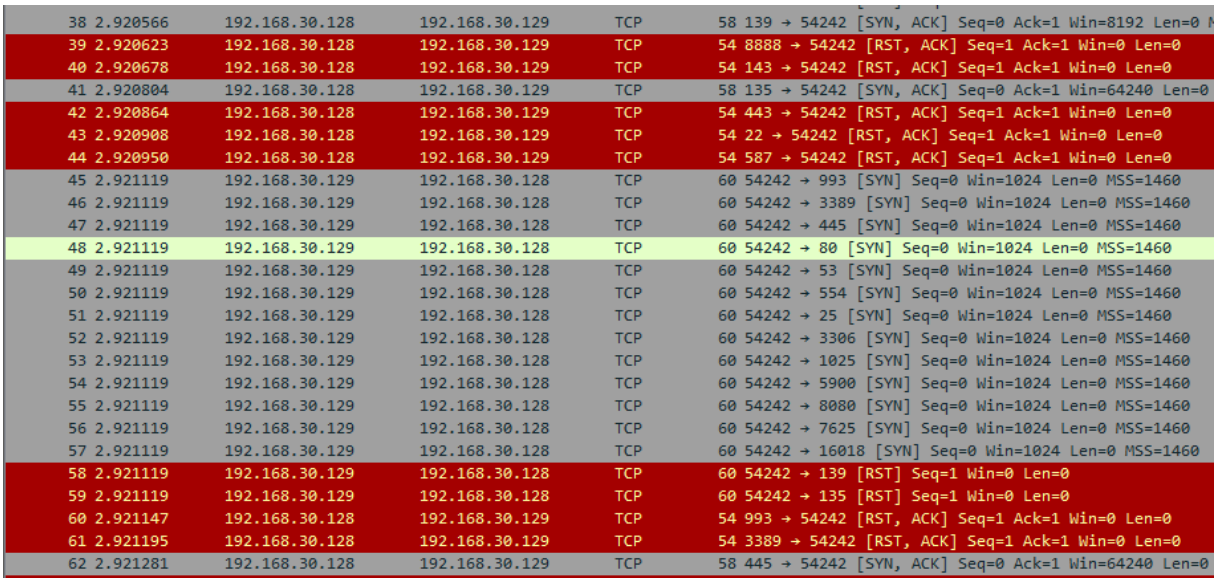
```
    192.168.30.129.51085 > 192.168.30.2.domain: 16001+ A? twitter.com. (29)
17:09:26.243706 IP (tos 0x0, ttl 128, id 22990, offset 0, flags [none], proto UDP (17), length 73)
    192.168.30.2.domain > 192.168.30.129.51085: 16001 1/0/0 twitter.com. A 104.244.42.129 (45)
17:09:27.625467 IP (tos 0x0, ttl 64, id 34071, offset 0, flags [DF], proto UDP (17), length 59)
    192.168.30.129.36372 > 192.168.30.2.domain: 29076+ A? abs.twimg.com. (31)
17:09:27.625550 IP (tos 0x0, ttl 64, id 34072, offset 0, flags [DF], proto UDP (17), length 59)
    192.168.30.129.36372 > 192.168.30.2.domain: 15255+ AAAA? abs.twimg.com. (31)
17:09:27.627210 IP (tos 0x0, ttl 128, id 23033, offset 0, flags [none], proto UDP (17), length 114)
    192.168.30.2.domain > 192.168.30.129.36372: 29076 2/0/0 abs.twimg.com. CNAME cs510.wpc.edgecastcdn.net., cs510.w
pc.edgecastcdn.net. A 152.199.21.141 (86)
```

WIRESHARK

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.30.128 -v
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 06:20 EST
Initiating ARP Ping Scan at 06:20
Scanning 192.168.30.128 [1 port]
Completed ARP Ping Scan at 06:20, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:20
Completed Parallel DNS resolution of 1 host. at 06:20, 0.00s elapsed
Initiating SYN Stealth Scan at 06:20
Scanning 192.168.30.128 [1000 ports]
Discovered open port 139/tcp on 192.168.30.128
Discovered open port 135/tcp on 192.168.30.128
Discovered open port 445/tcp on 192.168.30.128
Completed SYN Stealth Scan at 06:20, 1.66s elapsed (1000 total ports)
Nmap scan report for 192.168.30.128
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:16:92:63 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
           Raw packets sent: 1123 (49.396KB) | Rcvd: 1001 (40.040KB)
```

Skanowanie maszyny z Windowsem w trybie stealth



38	2.920566	192.168.30.128	192.168.30.129	TCP	58 139 → 54242 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
39	2.920623	192.168.30.128	192.168.30.129	TCP	54 8888 → 54242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	2.920678	192.168.30.128	192.168.30.129	TCP	54 143 → 54242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	2.920804	192.168.30.128	192.168.30.129	TCP	58 135 → 54242 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
42	2.920864	192.168.30.128	192.168.30.129	TCP	54 443 → 54242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	2.920908	192.168.30.128	192.168.30.129	TCP	54 22 → 54242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44	2.920950	192.168.30.128	192.168.30.129	TCP	54 587 → 54242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 7625 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
57	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 16018 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
58	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 139 [RST] Seq=1 Win=0 Len=0
59	2.921119	192.168.30.129	192.168.30.128	TCP	60 54242 → 135 [RST] Seq=1 Win=0 Len=0
60	2.921147	192.168.30.128	192.168.30.129	TCP	54 993 → 54242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	2.921195	192.168.30.128	192.168.30.129	TCP	54 3389 → 54242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	2.921281	192.168.30.128	192.168.30.129	TCP	58 445 → 54242 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0

Skanowanie w trybie Stealth zostało wykryte przez wireshark
Czerwone pakiery to takie, które zawierają flagę RST (Reset). Kończą one połączenie natychmiastowo, a wszystkie dane są odrzucone

Szare pakiety to takie, które zawierają flagę SYN, które jest prośbą o nawiązanie połączenia.

Na powyższym zrzucie ekranu widać jeszcze 3 szare pakiety z flagą SYN i ACK, które oznacza, że maszyna, na którą wysyłamy zapytanie jest chętna nawiązać połączenie

Jak widać są to dokładnie porty 125, 129 oraz 445, które nmap wskazał jako otwarte.
Nie są odsyłane jednak pakiety z flagą ACK, przez co połączenie nie jest nawiązywane, ponieważ chcieliśmy tylko zeskanować otwarte porty

Można też zauważyć, że porty nie są skanowane po kolei, tylko w kolejności losowej

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.30.128 --data-length 32 -f -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 06:48 EST
Nmap scan report for 192.168.30.128
Host is up (0.00050s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:16:92:63 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

Przy użyciu takiego skanowania, dostajemy taki sam wynik
Różnica jest jednak w wireshark

11	1.280210	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=0, ID=c79a
12	1.280210	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=8, ID=c79a
13	1.280210	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=16, ID=c79
14	1.280210	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=24, ID=c79
15	1.280210	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=32, ID=c79
16	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=40, ID=c79
17	1.280984	192.168.30.129	192.168.30.128	SMUX	60 35809 → 199 [SYN] Seq=0 Win=1024 Len=32 MSS=1460[Ma
18	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=0, ID=bea9
19	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=8, ID=bea9
20	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=16, ID=bea
21	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=24, ID=bea
22	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=32, ID=bea
23	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=40, ID=bea
24	1.280984	192.168.30.129	192.168.30.128	TCP	60 35809 → 8888 [SYN] Seq=0 Win=1024 Len=32 MSS=1460
25	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=0, ID=7c11
26	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=8, ID=7c11
27	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=16, ID=7c1
28	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=24, ID=7c1
29	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=32, ID=7c1
30	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=40, ID=7c1
31	1.280984	192.168.30.129	192.168.30.128	SSL	60 Continuation Data
32	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=0, ID=aa96
33	1.280984	192.168.30.129	192.168.30.128	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=8, ID=aa96

Pomiędzy pakietami skanującymi wysyłane jest kilka pakietów IPv4. Pozwala to na uniknięcie wykrycia przez systemy zabezpieczające. Są one w pewnym sensie „przemycane”.

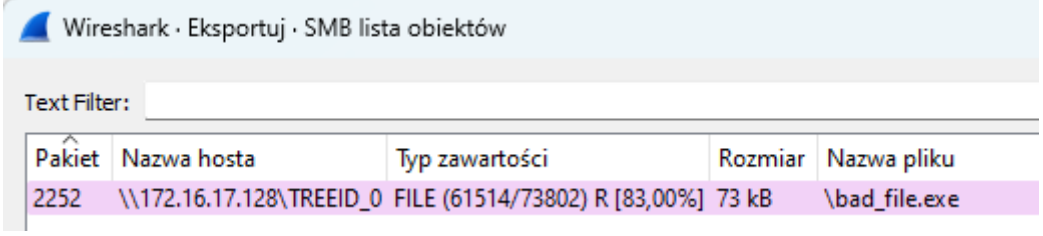
To rozwiązanie jest w mojej opinii mniej wykrywalne.

ANALIZA ZAINFEKOWANEGO KOMPUTERA

Adres analizowanego komputera: 172.16.17.131
Adres Gateway: 172.16.17.128
Oba urządzenia to wirtualne maszyny (widać to w dowolnym pakiecie)

```
Destination: VMware_24:d0:a3 (00:0c:29:24:d0:a3)
Source: VMware_ec:8a:14 (00:0c:29:ec:8a:14)
```

Stacja była skanowana, ponieważ jest dużo zapytań na różne porty w krótkim czasie
Skanującym było urządzenie o adresie 172.16.17.128 za pomocą nmap
Adres MAC należy do skanującego
W logach znajduje się plik \bad_file.exe



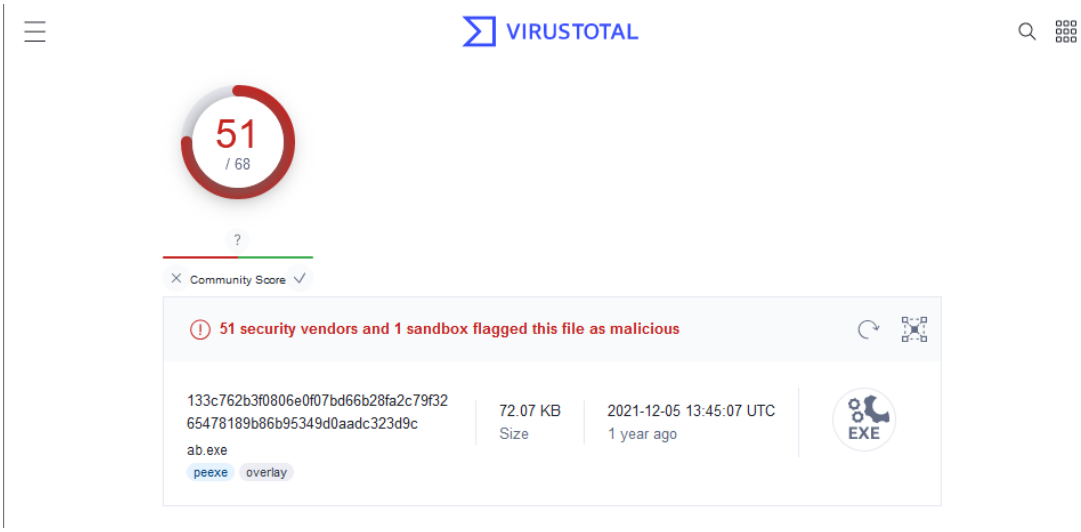
Plik został pobrany 24 listopada 2021 o godzinie 18:35:52 czasu Środkowoeuropejskiego z maszyny, która wcześniej skanowała (172.16.17.128)

Ciekawa obserwacja:
Próba obliczenia sumy kontrolnej na Windowsie się nie powiodła

```
PS C:\Users\Marcel\Desktop\Studia\Śledcza\lab_5> Get-FileHash .\%5cbad_file.exe -Algorithm MD5
Get-FileHash : The file 'C:\Users\Marcel\Desktop\Studia\Śledcza\lab_5\%5cbad_file.exe' cannot be read: Operacja nie zak
ończyła się pomyślnie, ponieważ plik zawiera wirusa lub potencjalnie niechciane oprogramowanie.
At line:1 char:1
+ Get-FileHash .\%5cbad_file.exe -Algorithm MD5
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ReadError: (C:\Users\Marcel...%5cbad_file.exe:PSObject) [Write-Error], WriteErrorExcepti
   on
    + FullyQualifiedErrorId : FileReadError,Get-FileHash
```

System windows wykrył, że jest to wirus, a plik zaraz potem został usunięty

```
┌──(kali㉿kali)-[~/sledcza]
└─$ md5sum %5cbad_file.exe
c654e9eb9b0528ca65877930a44b601a  %5cbad_file.exe
```



Według jest to Trojan. Wirus oryginalnie nazywał się ab.exe i podszywał się pod aplikację ab.exe
Kompilowany był 26.08.2009, lecz pierwsze informacje o nim pojawiły się na virustotal dnia 5.12.2021. Wirus dedykowany jest na urządzenia z systemem windows
Program tworzy kilka plików:

Files Dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF32A.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF32A.tmp.WERInternalMetadata.xml

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF33B.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF33B.tmp.csv

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF34C.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF34C.tmp.txt

Wirus działa w taki sposób:
Najpierw sprawdza informacje o systemie. Czyta Software Policies

Następnie dokonuje DNS lookups

Wirus również próbuje połączyć się z tymi stronami:

DNS Resolutions

+ arc.msn.com
+ cs9.wac.phicdn.net
+ incoming.telemetry.mozilla.org
+ telemetry-incoming-a.r53-2.services.mozilla.com
+ telemetry-incoming.r53-2.services.mozilla.com

NETMINER

Frame nr.	Filename	Extension	Size	Source host
2123	autoupdate.opera.com.cer	cer	1 380 B	82.145.216.19 [eu2-autoupdate.op
2123	DigiCert TLS Hybrid ECC SHA3.cer	cer	1 095 B	82.145.216.19 [eu2-autoupdate.op
2589	meterpreter.dll	dll	175 174 B	172.16.17.128 [172.16.17.128] (Otl

Netminer nie znalazł zainfekowanego pliku, lecz nadal widać, że plik był przesłany:

SMB NT Create AndX Request 1344	\bad_file.exe
SMB NT Create AndX Request 1856	\bad_file.exe
SMB NT Create AndX Request 2048	\bad_file.exe
SMB NT Create AndX Request 2176	\bad_file.exe
SMB NT Create AndX Request 2304	\bad_file.exe
SMB NT Create AndX Request 2880	\bad_file.exe
SMB NT Create AndX Request 3072	\bad_file.exe.Manifest
SMB NT Create AndX Request 3200	\bad_file.exe
SMB NT Create AndX Request 3264	\bad_file.exe
SMB NT Create AndX Request 3904	\bad_file.exe
SMB NT Create AndX Request 4672	\bad_file.exe
SMB NT Create AndX Request 5056	\
SMB NT Create AndX Request 5504	\bad_file.exe
SMB NT Create AndX Request 6016	\bad_file.exe.Manifest
SMB NT Create AndX Request 6144	\bad_file.exe
SMB NT Create AndX Request 6208	\bad_file.exe
SMB NT Create AndX Request 6656	\bad_file.exe
SMB NT Create AndX Request 6784	\bad_file.exe
SMB NT Create AndX Request 7168	\bad_file.exe
SMB NT Create AndX Request 7296	\bad_file.exe
SMB NT Create AndX Request 7424	\bad_file.exe
SMB NT Create AndX Request 7552	\bad_file.exe
SMB NT Create AndX Request 8128	\bad_file.exe
SMB NT Create AndX Request 8192	\bad_file.exe.Manifest
SMB NT Create AndX Request 8320	\bad_file.exe
SMB NT Create AndX Request 8384	\bad_file.exe