Course Project: Milestone 4

Cesar Munguia

04/16/2024

—

IS-4543-001

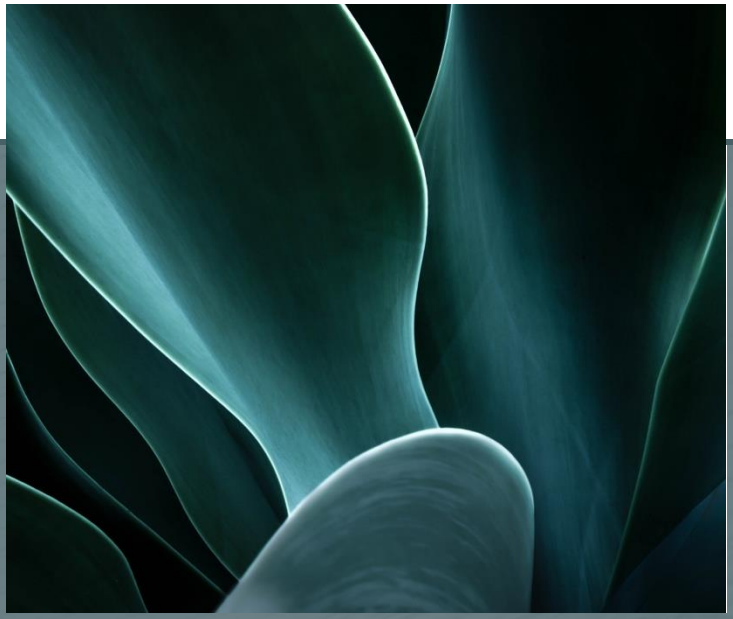
—

Jose Mireles

Objectives

Each milestone submission will be a write-up that includes:

- What did you do?
- What did you learn?
- Documentation of your work
  - Screenshot
  - Picture
  - Video
  - Interpretive Dance



Project Proposal

The project involves in-depth analysis of a virtual machine infected with malware, focusing on understanding the malware's behavior, persistence mechanisms, and potential impact on the system. Through forensic techniques and dynamic analysis, I will dissect the malicious code, identify evasion tactics, and extract indicators of compromise. The project aims to enhance cybersecurity skills by providing hands-on experience in malware analysis and incident response, crucial for defending against and mitigating the effects of sophisticated cyber threats.

- Milestone 4: Conduct a dynamic analysis of the chosen malware file using several tools

In Milestone 4 I will be focusing in conducting a dynamic analysis of the malicious file to gain a better understanding of the overall behavior. Dynamic analysis comes with advantages just as static analysis does as well. With dynamic, one is able to literally watch how the malicious file behaves, in other words, one could visually see the actions it takes. One of the disadvantages with static analysis was exactly this, you don't exactly what it's going to do until you double-click the executable. Another significant aspect about dynamic analysis is that, if the sandbox is configured correctly, one could even see if the malware tries to establish connections outside of this network. That is the reason why I included the REMNUX machine at very beginning (milestone 2). REMNUX will act as the victim's router and will also imitate the internet. My analysis will be divided into two portions: host-based indicators and network-based indicators.

Summary of Activities

Before executing the file, I went ahead and made sure the victim's machine had the proper default gateway and DNS server, and also ran Wireshark in REMNUX. While at VM, I used command **inetsim** to start the simulation. Then, I double-clicked the Core1Installer.exe and began my analysis.

Host-Based Indicators

My first step was to utilize sysinternals from Microsoft. While at the folder, I opened up Procmon64.exe and immediately made some filters to filter out the excessive information shown that could be irrelevant. I made 3 filters, 'Process name is Core1Installer.exe', 'Operation contains CreateFile', and 'Operation contains WriteFile' (refer to screenshot 1). The first I noticed was that a lot of dynamic link libraries were being queried by the file (refer to screenshot 2). Then, I noticed that the executable created a file called "Images" at the same directory where the executable resided (refer to screenshots 3 & 4). I also noticed that this same file was creating and writing files in that same directory. By convention these file names had the syntax *year-month-day* followed by 3 sets of consecutive numbers *xx-xx-xx* with a *.png* file extension (refer to screenshot 5).

Then, I used the "Show Registry Activity" option in Procmon64.exe. First thing I noticed was that the most used registry paths used were HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER. Both of these paths have similarities in that the file was accessing registries relating to "Tcpip", "Interfaces", "Internet Settings", "Connections", "ShareCredsWithWinHttp", "WinHttp", "Tcpip6", and "WinSock" (refer to screenshot 6 & 7).

Lastly, I've decided to let the program execute for about 20 minutes. In that time period, I found that the binary took about 247 screenshots of my computer and placed them at same directory where the .exe was (refer to screenshot 8).

Network-Based Indicators

Before I began my analysis that focused on the network primarily, I made Wireshark was capturing packets in its respective interface just in case I might get something useful. Then, I went to my Sysinternals folder and opened tcpview64.exe, which it's a version of the netstat command but with more relevant information in it. Everything looked normal, until I noticed a TCP connection

from the binary Core1Installer.exe (refer to screenshot 9). I noticed that it was trying to establish a connection with the previous discovered IP address. Then, I went back to procmon64.exe and used the "Show Network Activity" option to show only relevant information. I quickly realized that this same binary was sending a lot of SYN packets, however, it seems that it was failing to establish a connection due to routing (refer to screenshot 10). I checked the log report of the INETSIM back at REMNUX and saw only DNS logs (refer to screenshot 11). Finally, I checked the .pcap file from Wireshark to analyze it further. The whole file was filled with TCP, TCP retransmissions, and DNS packets (refer to screenshot 12).

My curiosity led me to believe that maybe I could change the IP address of the malicious actor to the IP address of my REMNUX machine to see if I was able to establish the connection needed. For that, I utilized HxD to change certain bytes of the Core1Installer.exe file. I was able to find the exact place where the suspicious IP was placed in the file and changed the IP from 188.120.240.203 to 192.168.240.203 (refer to screenshot 13 & 14). I changed the bytes from 38 to 39, bytes 32 to 36, bytes 30 to 38, all in offset 45C0 and renamed the file Core1Installer2.exe. Then, I changed the victim's IP to 192.168.240.202 and the REMNUX's IP to 192.168.240.203. Finally, I ran the executable again, but with no luck, failed to establish a connection how I wanted to (refer to screenshot 15 & 16).

Description of Learning Completed

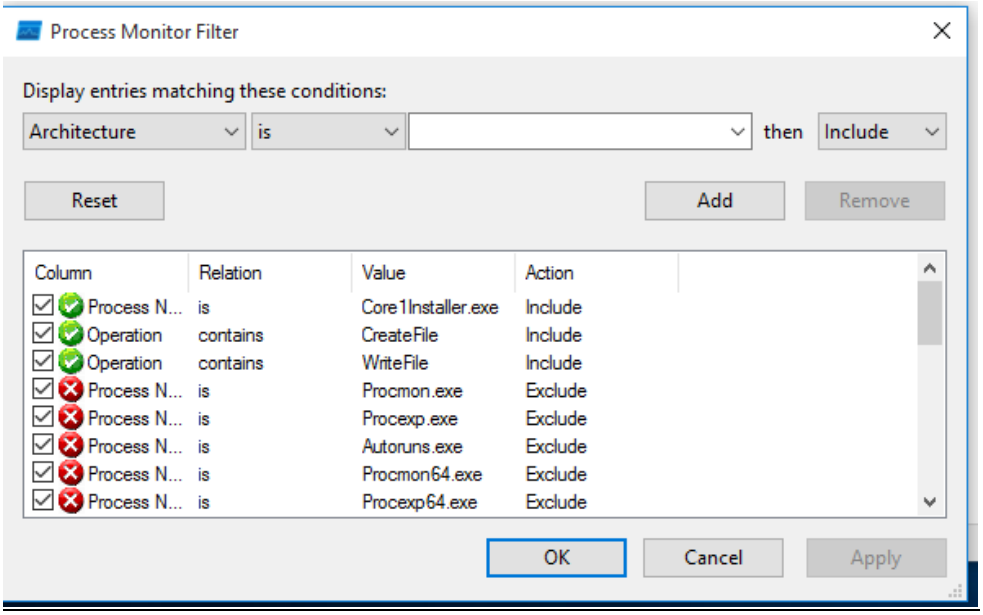
The sysinternals folders contains a bunch of useful programs for analysts to use to better understand the machine's current state. There are also a lot of useful commands that one can I use in Windows at the command prompt like tasklist, taskkill, netstat, and ipconfig. However, sysinternals is more simplistic and shows more significant information and for that reason I utilized those resources. Overall, in the host-based portion I learned that at execution, the binary created a directory called "Images", and then inserted a number of screenshots with a specific name syntax in that same directory. One big aspect about conducting dynamic analysis is to find how a binary works in relation to the registry. With this, I'd be able to have a grasp about the sort of things this binary was trying to

accomplish during execution. Furthermore, I learned that the malware accessed particular registry paths. These paths correlate to my same findings back in my static analysis. Where I stated that the program most likely establishes a connection outside of its network.

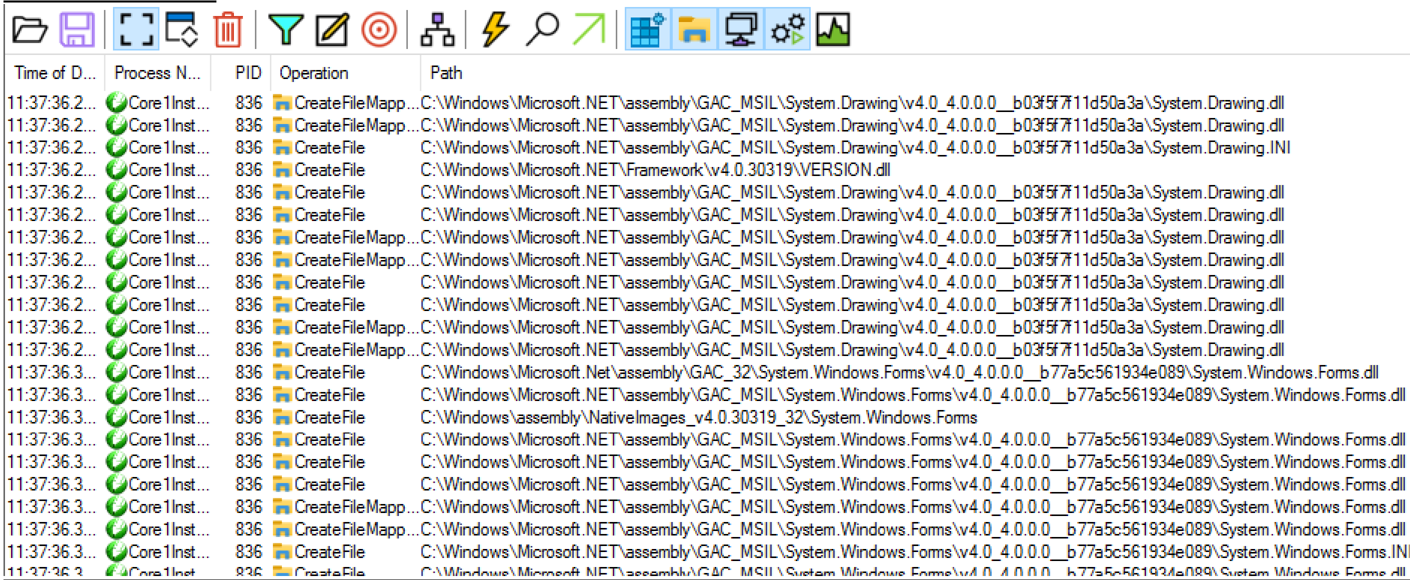
Back to when I executed capa.exe, the output showed me that one of its capabilities was that the program would try to send packets of a certain protocol, but using a not corresponded port. For example, it's common sense to say that HTTP packets transverse through port 80. However, this program violated this rule and tried sending these HTTP packets through port 9000, which is unusual. That appears to me to be the most reasonable rationale of why the malware in the victim's machine was not able to establish a connection correctly with the INETSIM in place. Port 9000 was not in use during the simulation, which is also why I did not get any relevant information in my logs or even in Wireshark. If maybe I was able to change the destination port of the program to be 80 I could've probably gotten further significant data. My assumption is that this program most likely created a socket to transmit data, or in this case, screenshots. However, I don't exactly if the malware executed other actions when establishing the connection properly.

Documentation of Work Completed

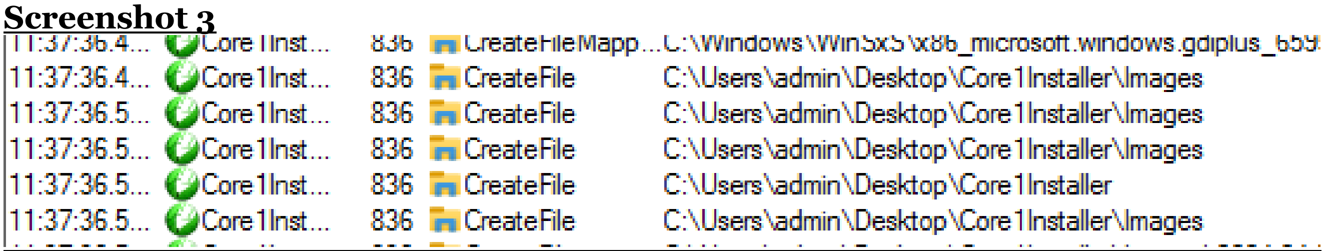
Screenshot 1



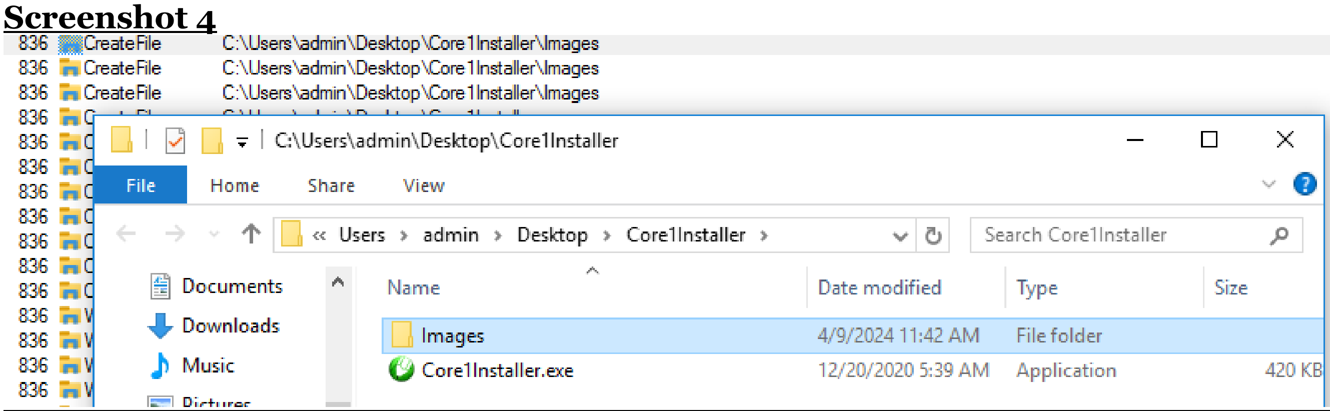
Screenshot 2



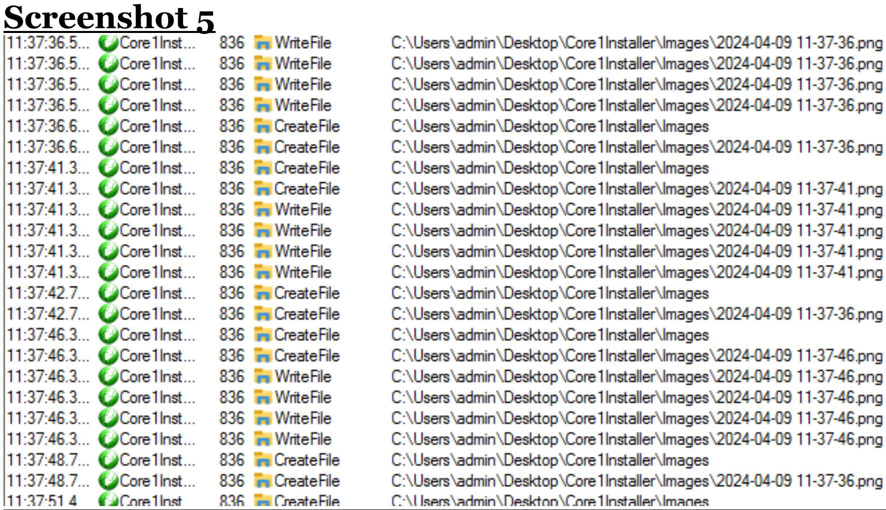
Screenshot 3



Screenshot 4



Screenshot 5



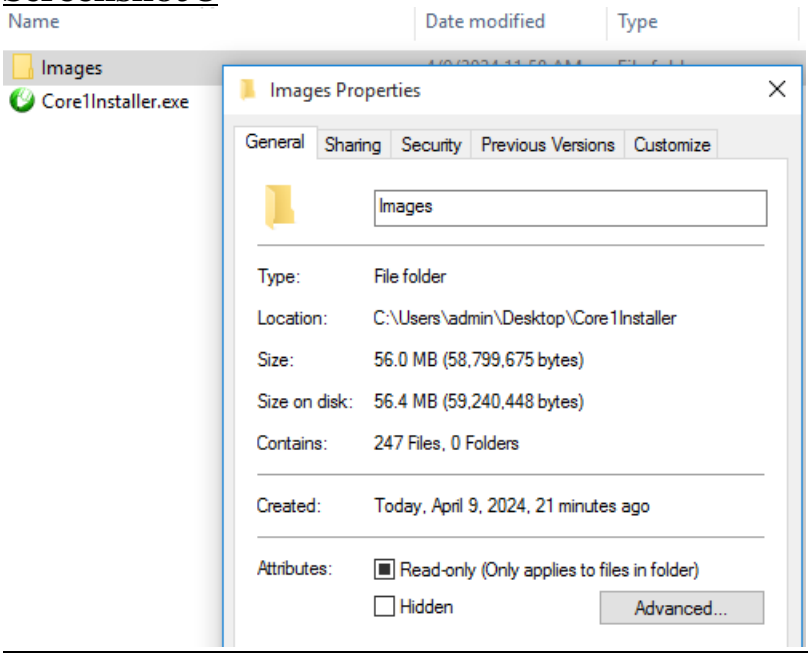
Screenshot 6

11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings
11:37:31.1...	Core1Inst...	836	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings
11:37:31.1...	Core1Inst...	836	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ShareCredsWithWinHttp
11:37:31.1...	Core1Inst...	836	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
11:37:31.1...	Core1Inst...	836	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
11:37:31.1...	Core1Inst...	836	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableBranchCache
11:37:31.1...	Core1Inst...	836	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
11:37:31.1...	Core1Inst...	836	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
11:37:31.1...	Core1Inst...	836	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableAutoProxyAuth
11:37:31.1...	Core1Inst...	836	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
11:37:31.1...	Core1Inst...	836	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

Screenshot 7

11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock
11:37:31.1...	Core1Inst...	836	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock
11:37:31.1...	Core1Inst...	836	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock\Mapping
11:37:31.1...	Core1Inst...	836	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock\Mapping
11:37:31.1...	Core1Inst...	836	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Setup Migration\Providers
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers
11:37:31.1...	Core1Inst...	836	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers
11:37:31.1...	Core1Inst...	836	RegQueryKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers
11:37:31.1...	Core1Inst...	836	RegOpenKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip6
11:37:31.1...	Core1Inst...	836	RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip6\WinSock 2.0 Provider ID
11:37:31.1...	Core1Inst...	836	RegCloseKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip6
11:37:31.1...	Core1Inst...	836	RegCloseKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers

Screenshot 8



Screenshot 9

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
svchost.exe	752	TCP	Listen	0.0.0.0	135	0.0.0.0	0
System	4	TCP	Listen	192.168.10.2	139	0.0.0.0	0
wininit.exe	456	TCP	Listen	0.0.0.0	49408	0.0.0.0	0
svchost.exe	900	TCP	Listen	0.0.0.0	49409	0.0.0.0	0
svchost.exe	848	TCP	Listen	0.0.0.0	49410	0.0.0.0	0
spoolsv.exe	1412	TCP	Listen	0.0.0.0	49411	0.0.0.0	0
services.exe	592	TCP	Listen	0.0.0.0	49412	0.0.0.0	0
svchost.exe	1628	TCP	Listen	0.0.0.0	49413	0.0.0.0	0
lsass.exe	600	TCP	Listen	0.0.0.0	49414	0.0.0.0	0
Core1Installer.exe	720	TCP	Syn Sent	192.168.10.2	49419	188.120.240.203	9000
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0
svchost.exe	752	TCPv6	Listen	::	135	::	0

Screenshot 10

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:17:...	Core1Installer.exe	720	TCP Reconnect	DESKTOP-TDJUVVL:49415 -> www.ine...	SUCCESS	Length: 0, seqnum:..
12:17:...	Core1Installer.exe	720	TCP Reconnect	DESKTOP-TDJUVVL:49416 -> www.ine...	SUCCESS	Length: 0, seqnum:..
12:17:...	Core1Installer.exe	720	TCP Reconnect	DESKTOP-TDJUVVL:49417 -> www.ine...	SUCCESS	Length: 0, seqnum:..
12:17:...	Core1Installer.exe	720	TCP Reconnect	DESKTOP-TDJUVVL:49418 -> www.ine...	SUCCESS	Length: 0, seqnum:..
12:17:...	Core1Installer.exe	720	TCP Reconnect	DESKTOP-TDJUVVL:49419 -> www.ine...	SUCCESS	Length: 0, seqnum:..

Screenshot 11

```
remnux@remnux:/var/log/inetsim/report$ sudo cat report.1653.txt
=== Report for session '1653' ===

Real start date            : 2024-04-10 07:16:01
Simulated start date       : 2024-04-10 07:16:01
Time difference on startup : none

2024-04-10 07:17:15  First simulated date in log file
2024-04-10 07:17:15  DNS connection, type: PTR, class: IN, requested name: 203.240.120.188.in-addr.a
rpa
2024-04-10 07:17:18  DNS connection, type: PTR, class: IN, requested name: 8.4.4.2.4.4.9.8.8.4.8.3.7
.4.b.8.8.4.9.0.4.7.f.f.3.0.a.0.8.a.0.c.ip6.arpa
2024-04-10 07:17:18  DNS connection, type: PTR, class: IN, requested name: 3.10.168.192.in-addr.arpa
2024-04-10 07:17:53  DNS connection, type: PTR, class: IN, requested name: 1.225.168.192.in-addr.arp
a
2024-04-10 07:17:53  DNS connection, type: PTR, class: IN, requested name: 250.255.255.239.in-addr.a
rpa
2024-04-10 07:19:00  DNS connection, type: PTR, class: IN, requested name: 255.10.168.192.in-addr.ar
pa
2024-04-10 07:19:00  Last simulated date in log file

===
remnux@remnux:/var/log/inetsim/report$
```

Screenshot 12

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::20c:29ff:fe23…	ff02::2	ICMPv6	70	Router Solicitation from 00:0c:29:23:d3:b9
2	38.597943510	192.168.10.2	188.120.240.203	TCP	66	49415 → 9000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
3	41.611895779	192.168.10.2	188.120.240.203	TCP	66	[TCP Retransmission] 49415 → 9000 [SYN] Seq=0 Win=8192 …
4	43.126230602	VMware_fd:94:47	VMware_23:d3:b9	ARP	60	Who has 192.168.10.3? Tell 192.168.10.2
5	43.126259455	VMware_23:d3:b9	VMware_fd:94:47	ARP	42	192.168.10.3 is at 00:0c:29:23:d3:b9
6	44.354148728	192.168.10.2	188.120.240.203	TCP	66	49416 → 9000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
7	44.365443575	192.168.10.2	192.168.10.3	DNS	88	Standard query 0x197a PTR 203.240.120.188.in-addr.arpa
8	44.410558593	192.168.10.3	192.168.10.2	DNS	117	Standard query response 0x197a PTR 203.240.120.188.in-a…
9	46.893129601	192.168.10.2	192.168.10.3	DNS	132	Standard query 0x37c4 PTR 8.4.4.2.4.4.9.8.8.4.8.3.7.4.b…
10	46.893130316	192.168.10.2	192.168.10.3	DNS	85	Standard query 0x5965 PTR 3.10.168.192.in-addr.arpa
11	46.910023402	192.168.10.3	192.168.10.2	DNS	161	Standard query response 0x37c4 PTR 8.4.4.2.4.4.9.8.8.4.…
12	46.938870457	192.168.10.3	192.168.10.2	DNS	114	Standard query response 0x5965 PTR 3.10.168.192.in-addr…
13	47.360859080	192.168.10.2	188.120.240.203	TCP	66	[TCP Retransmission] 49416 → 9000 [SYN] Seq=0 Win=8192 …
14	49.527358621	VMware_23:d3:b9	VMware_fd:94:47	ARP	42	Who has 192.168.10.2? Tell 192.168.10.3
15	49.528296504	VMware_fd:94:47	VMware_23:d3:b9	ARP	60	192.168.10.2 is at 00:0c:29:fd:94:47
16	50.378303650	192.168.10.2	188.120.240.203	TCP	66	49417 → 9000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
17	53.393452115	192.168.10.2	188.120.240.203	TCP	66	[TCP Retransmission] 49417 → 9000 [SYN] Seq=0 Win=8192 …
18	55.127220421	VMware_fd:94:47	VMware_23:d3:b9	ARP	60	Who has 192.168.10.3? Tell 192.168.10.2
19	55.127271251	VMware_23:d3:b9	VMware_fd:94:47	ARP	42	192.168.10.3 is at 00:0c:29:23:d3:b9

Screenshot 13

Core1Installer.exe

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00004510	6F	78	00	73	65	74	5F	4D	61	78	69	6D	69	7A	65	42	ox.set_MaximizeB
00004520	6F	78	00	54	65	78	74	42	6F	78	00	44	65	6C	61	79	ox.TextBox.Delay
00004530	00	54	6F	47	72	61	79	00	54	6F	41	72	72	61	79	00	.ToGray.ToArray.
00004540	61	72	72	61	79	00	67	65	74	5F	41	73	73	65	6D	62	array.get_Assemb
00004550	6C	79	00	47	65	74	45	78	65	63	75	74	69	6E	67	41	ly.GetExecutingA
00004560	73	73	65	6D	62	6C	79	00	73	65	74	5F	52	65	61	64	ssembly.set_Read
00004570	4F	6E	6C	79	00	54	72	79	00	43	72	65	61	74	65	44	Only.Try.CreateD
00004580	69	72	65	63	74	6F	72	79	00	6F	70	5F	45	71	75	61	irectory.op_Equa
00004590	6C	69	74	79	00	45	6D	70	74	79	00	00	00	09	68	00	lity.Empty....h.
000045A0	74	00	74	00	70	00	00	15	61	00	67	00	65	00	6E	00	t.t.p...a.g.e.n.
000045B0	74	00	2F	00	70	00	75	00	73	00	68	00	00	1F	31	00	t./.p.u.s.h...1.
000045C0	38	00	38	00	2E	00	31	00	32	00	30	00	2E	00	32	00	8.8...1.2.0...2.
000045D0	34	00	30	00	2E	00	32	00	30	00	33	00	00	27	79	00	4.0...2.0.3..'y.
000045E0	79	00	79	00	79	00	2D	00	4D	00	4D	00	2D	00	64	00	y.y.y.-.M.M.-.d.
000045F0	64	00	20	00	48	00	48	00	2D	00	6D	00	6D	00	2D	00	d. .H.H.-.m.m.-.
00004600	73	00	73	00	01	07	70	00	6E	00	67	00	00	0D	49	00	s.s...p.n.g...I.

Screenshot 14

Core1Installer2.exe

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00004510	6F	78	00	73	65	74	5F	4D	61	78	69	6D	69	7A	65	42	ox.set_MaximizeB
00004520	6F	78	00	54	65	78	74	42	6F	78	00	44	65	6C	61	79	ox.TextBox.Delay
00004530	00	54	6F	47	72	61	79	00	54	6F	41	72	72	61	79	00	.ToGray.ToArray.
00004540	61	72	72	61	79	00	67	65	74	5F	41	73	73	65	6D	62	array.get_Assemb
00004550	6C	79	00	47	65	74	45	78	65	63	75	74	69	6E	67	41	ly.GetExecutingA
00004560	73	73	65	6D	62	6C	79	00	73	65	74	5F	52	65	61	64	ssembly.set_Read
00004570	4F	6E	6C	79	00	54	72	79	00	43	72	65	61	74	65	44	Only.Try.CreateD
00004580	69	72	65	63	74	6F	72	79	00	6F	70	5F	45	71	75	61	irectory.op_Equa
00004590	6C	69	74	79	00	45	6D	70	74	79	00	00	00	09	68	00	lity.Empty....h.
000045A0	74	00	74	00	70	00	00	15	61	00	67	00	65	00	6E	00	t.t.p...a.g.e.n.
000045B0	74	00	2F	00	70	00	75	00	73	00	68	00	00	1F	31	00	t./.p.u.s.h...1.
000045C0	39	00	38	00	2E	00	31	00	36	00	38	00	2E	00	32	00	9.8...1.6.8...2.
000045D0	34	00	30	00	2E	00	32	00	30	00	33	00	00	27	79	00	4.0...2.0.3..'y.
000045E0	79	00	79	00	79	00	2D	00	4D	00	4D	00	2D	00	64	00	y.y.y.-.M.M.-.d.
000045F0	64	00	20	00	48	00	48	00	2D	00	6D	00	6D	00	2D	00	d. .H.H.-.m.m.-.
00004600	73	00	73	00	01	07	70	00	6E	00	67	00	00	0D	49	00	s.s...p.n.g...I.

Screenshot 15

spoolsv.exe	1336	TCP	Listen	0.0.0.0	49411	0.0.0.0	0
services.exe	592	TCP	Listen	0.0.0.0	49412	0.0.0.0	0
svchost.exe	1580	TCP	Listen	0.0.0.0	49413	0.0.0.0	0
lsass.exe	600	TCP	Listen	0.0.0.0	49414	0.0.0.0	0
Core1Installer2.exe	1384	TCP	Syn Sent	192.168.240.202	49445	198.168.240.203	9000
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0
svchost.exe	748	TCPv6	Listen	::	135	::	0

Screenshot 16

```
TCP    0.0.0.0:49412          DESKTOP-TDJUVVL:0      LISTENING
TCP    0.0.0.0:49413          DESKTOP-TDJUVVL:0      LISTENING
TCP    0.0.0.0:49414          DESKTOP-TDJUVVL:0      LISTENING
TCP    192.168.240.202:139    DESKTOP-TDJUVVL:0      LISTENING
TCP    192.168.240.202:49457  www:9000               SYN_SENT
TCP    [::]:135               DESKTOP-TDJUVVL:0      LISTENING
TCP    [::]:445               DESKTOP-TDJUVVL:0      LISTENING
TCP    [::]:49408             DESKTOP-TDJUVVL:0      LISTENING
```