

PREPARED BY
PHANTOM SRL

REPORT MALWARE ANALYSIS

PIGNATELLO GIUSEPPE
IANNONE LUCA
ALESSIO D'OTTAVIO
FRANCESCO PIO SCOPECE



PHANTOM s.r.l

**IMPOSSIBLE IS
OUR TARGET**

CONTENTS

1) Exercise Trace

2) What is ProcMon?

3) Exercise Resolution

4) Conclusions

EXERCISE TRACE

- IDENTIFY ANY MALWARE ACTIONS ON THE FILE SYSTEM USING - - PROCESS MONITOR (PROCMON)
- IDENTIFY ANY MALWARE ACTIONS ON PROCESSES AND THREADS USING PROCESSMONITOR
- REGISTRY CHANGES AFTER MALWARE ACTIONS (DIFFERENCES)
- TRY TO PROFILE THE MALWARE BASED ON THE CORRELATION BETWEEN «OPERATION» AND PATH.



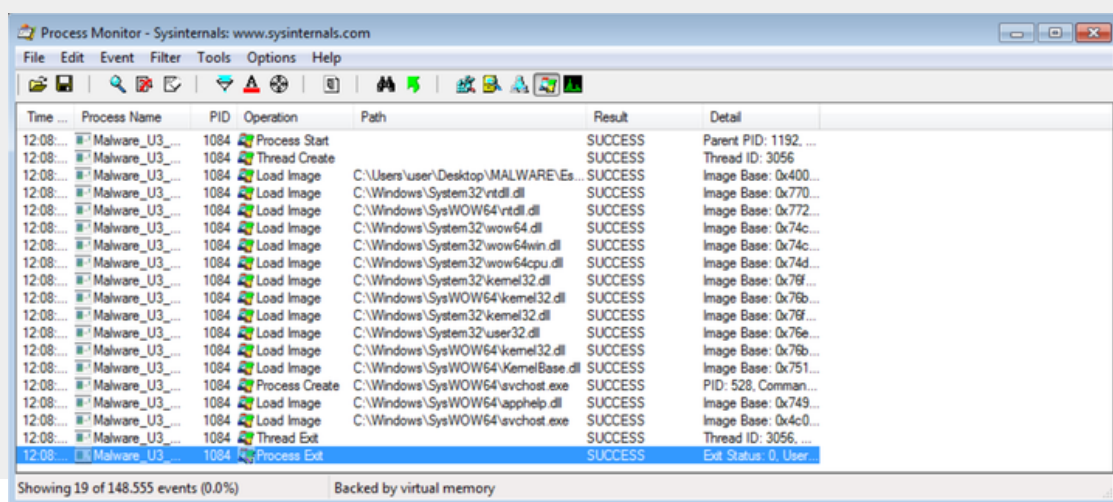
WHAT IS PROCMON?

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, registry, and process/thread activity. It combines the functionality of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements, including advanced and non-destructive filtering, comprehensive event properties such as session IDs and usernames, reliable process information, full thread stacks with built-in symbol support, and for each operation, simultaneous recording to file and much more. With its unique and powerful features, Process Monitor is an essential utility for system troubleshooting and as a malware research toolkit.



EXERCICE RESOLUTION

FILE SYSTEM:

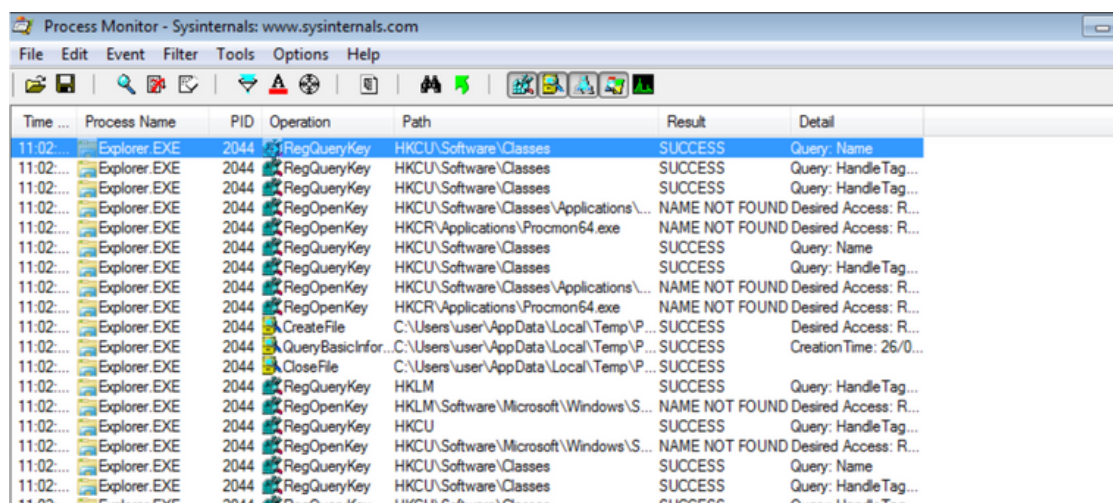


Process Monitor - Sysinternals: www.sysinternals.com

| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|----------|---------------|------|----------------|------------------------------------|---------|-------------------------|
| 12:08... | Malware_U3... | 1084 | Process Start | | SUCCESS | Parent PID: 1192... |
| 12:08... | Malware_U3... | 1084 | Thread Create | | SUCCESS | Thread ID: 3056 |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Users\user\Desktop\MALWARE\E... | SUCCESS | Image Base: 0x400... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\System32\ntdll.dll | SUCCESS | Image Base: 0x770... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\SysWOW64\ntdll.dll | SUCCESS | Image Base: 0x772... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\System32\wow64.dll | SUCCESS | Image Base: 0x74c... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\System32\wow64cpu.dll | SUCCESS | Image Base: 0x74d... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\System32\kernel32.dll | SUCCESS | Image Base: 0x76f... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\SysWOW64\kernel32.dll | SUCCESS | Image Base: 0x76b... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\System32\kernel32.dll | SUCCESS | Image Base: 0x76f... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\System32\user32.dll | SUCCESS | Image Base: 0x76e... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\SysWOW64\kernel32.dll | SUCCESS | Image Base: 0x76b... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\SysWOW64\KernelBase.dll | SUCCESS | Image Base: 0x751... |
| 12:08... | Malware_U3... | 1084 | Process Create | C:\Windows\SysWOW64\svchost.exe | SUCCESS | PID: 528, Comman... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\SysWOW64\apphelp.dll | SUCCESS | Image Base: 0x749... |
| 12:08... | Malware_U3... | 1084 | Load Image | C:\Windows\SysWOW64\svchost.exe | SUCCESS | Image Base: 0x4c0... |
| 12:08... | Malware_U3... | 1084 | Thread Exit | | SUCCESS | Thread ID: 3056... |
| 12:08... | Malware_U3... | 1084 | Process Exit | | SUCCESS | Exit Status: 0, User... |

Showing 19 of 148.555 events (0.0%) Backed by virtual memory

PROCESSES AND THREADS:



Process Monitor - Sysinternals: www.sysinternals.com

| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|----------|--------------|------|--------------------|----------------------------------------|----------------|-----------------------|
| 11:02... | Explorer.EXE | 2044 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name |
| 11:02... | Explorer.EXE | 2044 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Handle Tag... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCU\Software\Classes\Applications\... | NAME NOT FOUND | Desired Access: R... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCR\Applications\Procmon64.exe | NAME NOT FOUND | Desired Access: R... |
| 11:02... | Explorer.EXE | 2044 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCU\Software\Classes | SUCCESS | Query: Handle Tag... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCU\Software\Classes\Applications\... | NAME NOT FOUND | Desired Access: R... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCR\Applications\Procmon64.exe | NAME NOT FOUND | Desired Access: R... |
| 11:02... | Explorer.EXE | 2044 | CreateFile | C:\Users\user\AppData\Local\Temp\P... | SUCCESS | Desired Access: R... |
| 11:02... | Explorer.EXE | 2044 | QueryBasicInfor... | C:\Users\user\AppData\Local\Temp\P... | SUCCESS | CreationTime: 26/0... |
| 11:02... | Explorer.EXE | 2044 | CloseFile | C:\Users\user\AppData\Local\Temp\P... | SUCCESS | |
| 11:02... | Explorer.EXE | 2044 | RegQueryKey | HKLM | SUCCESS | Query: HandleTag... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKLM\Software\Microsoft\Windows\S... | NAME NOT FOUND | Desired Access: R... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCU | SUCCESS | Query: Handle Tag... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCU\Software\Microsoft\Windows\S... | NAME NOT FOUND | Desired Access: R... |
| 11:02... | Explorer.EXE | 2044 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name |
| 11:02... | Explorer.EXE | 2044 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Handle Tag... |
| 11:02... | Explorer.EXE | 2044 | RegOpenKey | HKCU\Software\Classes | SUCCESS | Query: Handle Tag... |

REGISTRY:

Process Monitor - Sysinternals: www.sysinternals.com

| Time ... | Process Name | PID | Operation | Path |
|----------|----------------|-----|---------------|------------------------------------------------------------------------------------------------------|
| 15:57... | Malware_U3_... | 872 | RegSetInfoKey | HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings |
| 15:57... | Malware_U3_... | 872 | RegQueryValue | HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImproveZoneCheck |
| 15:57... | Malware_U3_... | 872 | RegCloseKey | HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\CurrentVersion\Internet Settings |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings |
| 15:57... | Malware_U3_... | 872 | RegSetInfoKey | HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings |
| 15:57... | Malware_U3_... | 872 | RegQueryValue | HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only |
| 15:57... | Malware_U3_... | 872 | RegCloseKey | HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\svchost.exe |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\SafeBoot\Option |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\SafeBoot\Option |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers |
| 15:57... | Malware_U3_... | 872 | RegSetInfoKey | HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\codeidentifiers |
| 15:57... | Malware_U3_... | 872 | RegQueryValue | HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\codeidentifiers\TransparentEnabled |

Process Monitor - Sysinternals: www.sysinternals.com

| Time ... | Process Name | PID | Operation | Path |
|----------|----------------|-----|---------------|-----------------------------------------------------------------------------------------------------------|
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options |
| 15:57... | Malware_U3_... | 872 | RegQueryValue | HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\DisableUserModeCallbackFil |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Session Manager |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Session Manager |
| 15:57... | Malware_U3_... | 872 | RegQueryValue | HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalDllSearch |
| 15:57... | Malware_U3_... | 872 | RegCloseKey | HKLM\System\CurrentControlSet\Control\SESSION MANAGER |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\SOFTWARE\Microsoft\WOW64 |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options |
| 15:57... | Malware_U3_... | 872 | RegSetInfoKey | HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options |
| 15:57... | Malware_U3_... | 872 | RegQueryValue | HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\DisableUserModeCallbackFil |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Session Manager |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Session Manager |
| 15:57... | Malware_U3_... | 872 | RegSetInfoKey | HKLM\System\CurrentControlSet\Control\SESSION MANAGER |
| 15:57... | Malware_U3_... | 872 | RegQueryValue | HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalDllSearch |
| 15:57... | Malware_U3_... | 872 | RegCloseKey | HKLM\System\CurrentControlSet\Control\SESSION MANAGER |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Terminal Server |
| 15:57... | Malware_U3_... | 872 | RegOpenKey | HKLM\System\CurrentControlSet\Control\Terminal Server |
| 15:57... | Malware_U3_... | 872 | RegSetInfoKey | HKLM\System\CurrentControlSet\Control\Terminal Server |

Showing 268 of 102,720 events (0.2%) Backed by virtual memory

WE CAN THEREFORE HYPOTHESIZE THAT OUR MALWARE, WHEN EXECUTED, TRIES TO DISGUISE ITSELF BY CREATING A NEW PROCESS CALLED "SVCHOST.EXE" IN ORDER TO KEEP HIMSELF INSIDE THE COMPUTER.

PREPARED BY
PHANTOM SRL

THANKS!

PIGNATELLO GIUSEPPE
IANNONE LUCA
D'OTTAVIO ALESSIO
SCOPECE FRANCESCO PIO



PHANTOM s.r.l

**IMPOSSIBLE IS
OUR TARGET**