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

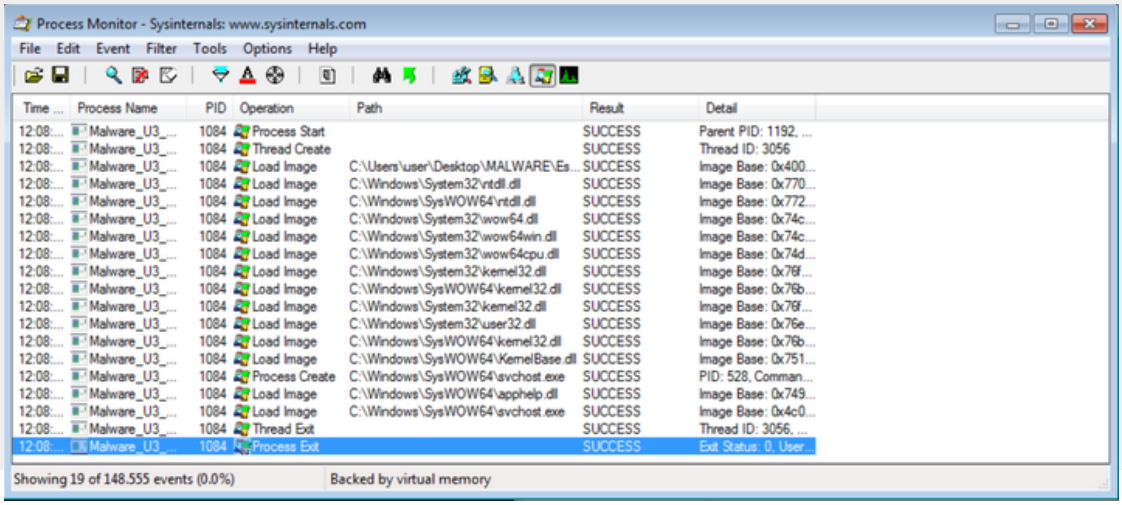
- IDENTIFY ANY MALWARE ACTIONS ON THE FILE SYSTEM USING - - PROCESS MONITOR (PROCMON)
- IDENTIFY ANY MALWARE ACTIONS ON PROCESSES AND THREADS USING PROCESSMONITOR
- REGISTRY CHANGES AFTER MALWARE ACTIONS (DIFFERENCES)
- TRY TO PROFILE THE MALWARE BASED ON THE CORRELATION BETWEEN «OPERATION» AND PATH.

WHAT IS PROCMON?

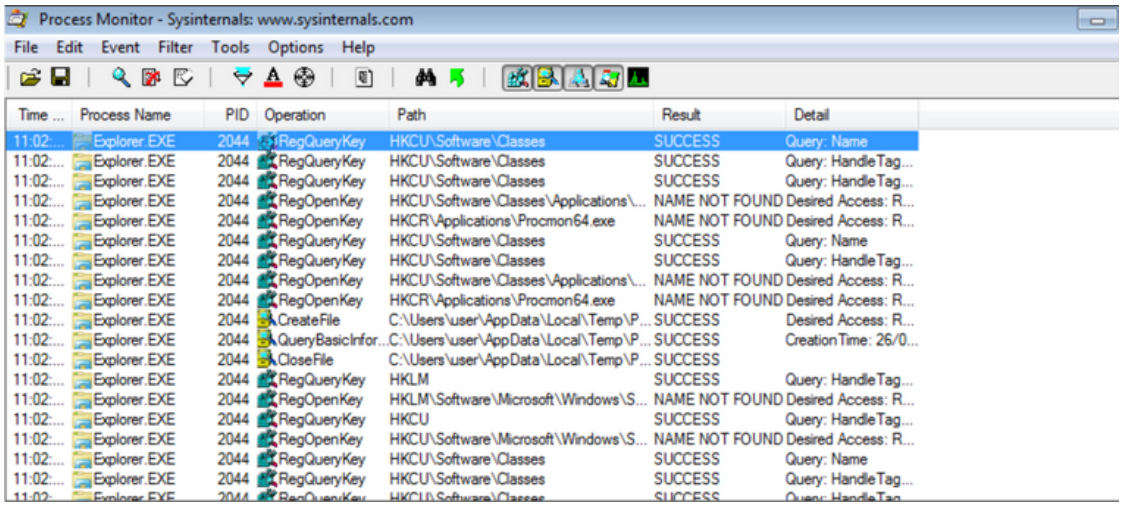
Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, registry, and process/thread activity. It combines the functionality of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements, including advanced and non-destructive 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

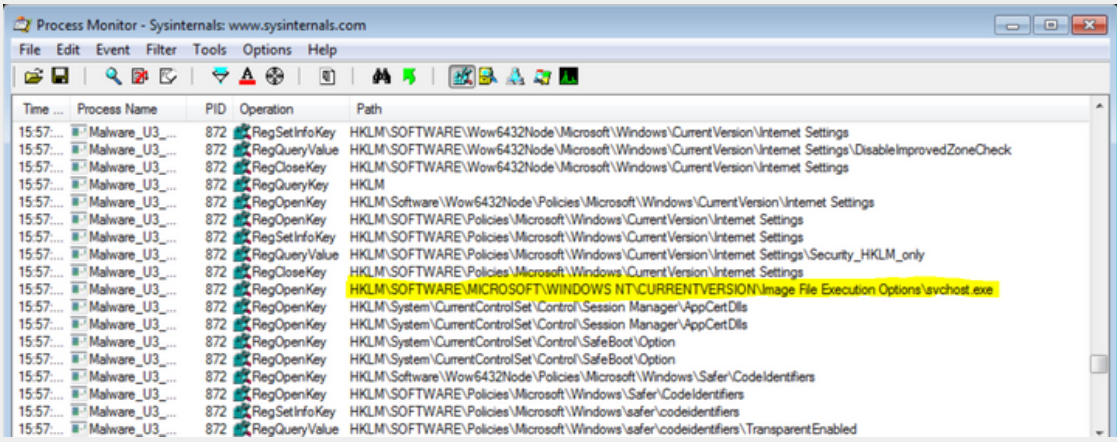
FILE SYSTEM:

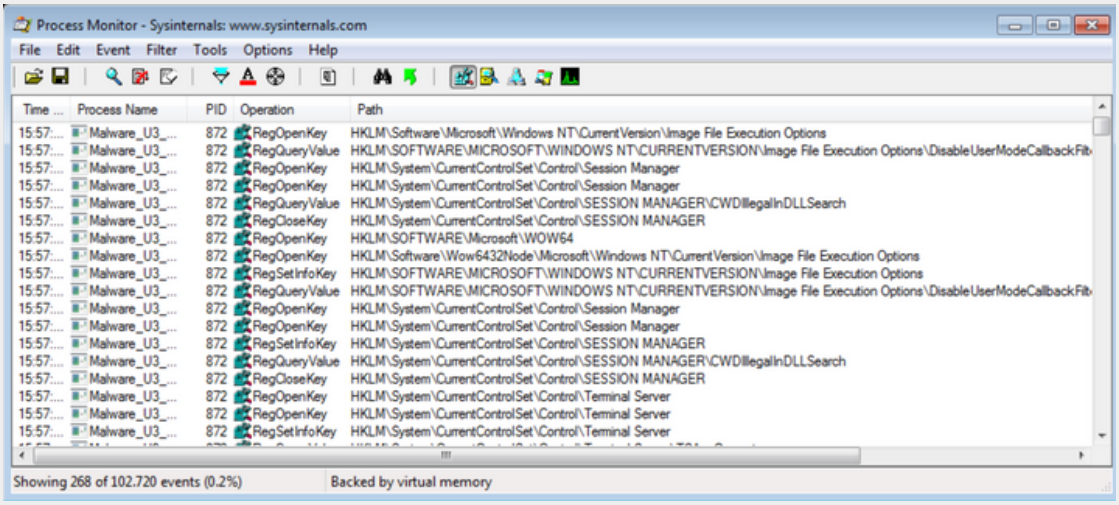


PROCESSES AND THREADS:



REGISTRY:





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