#44u6115f

GameGuard에 대한 간단한 분석.

By Dual5651

(http://dualpage.muz.ro)

요약 : 이 문서는 분석자의 입장에서 GameGuard의 동작을 모니터링 한 것에 대한 것입니다. 실제 GameGuard의 동작방식과는 다소 차이가 있을 수 있습니다.

1. Execution sequence

첫번째로 GameGuard의 실행 순서는 다음과 같습니다.

00000011 오전 10:10:03 Type : Create
00000012 오전 10:10:03 Parent ID : 0xA78
00000013 오전 10:10:03 Process ID : 0x848
00000014 오전 10:10:03 EPROCESS : 0x82E45DA0
00000015 오전 10:10:03 Process Name : Loader.exe

대게, 게임을 실행 시키기 전, Loader가 먼저 실행된다.

00000016 오전 10:10:04 Type : Create
00000017 오전 10:10:04 Parent ID : 0x848 – Loader.exe
00000018 오전 10:10:04 Process ID : 0x6B8
00000019 오전 10:10:04 EPROCESS : 0x83FC4DA0
00000020 오전 10:10:04 Process Name : game.exe

game.exe이 Loader에 의해 실행된 것을 볼 수 있다.

00000021 오전 10:10:04 Type : Destroy
00000022 오전 10:10:04 Parent ID : 0xA78
00000023 오전 10:10:04 Process ID : 0x848
00000024 오전 10:10:04 EPROCESS : 0x82E45DA0
00000025 오전 10:10:04 Process Name : Loader.exe

Game.exe를 실행시킨 후, Loader.exe는 파괴된다.

00000034 오전 10:10:05 Type : Create
00000035 오전 10:10:05 Parent ID : 0x6B8 – game.exe
00000036 오전 10:10:05 Process ID : 0x1C4
00000037 오전 10:10:05 EPROCESS : 0x819BBB28
00000038 오전 10:10:05 Process Name : GameGuard.des

GameGuard.des의 역할은 보호를 수행하기 위한 초기화 작업등을 수행하는 것으로 보인다. Game.exe에 의해 실행 된다.

00000039 오전 10:10:08 Type : Create
00000040 오전 10:10:08 Parent ID : 0x6B8 – game.exe
00000041 오전 10:10:08 Process ID : 0x4A4
00000042 오전 10:10:08 EPROCESS : 0x829D0DA0
00000043 오전 10:10:08 Process Name : GameMon.des

gameMon.des은 실제적인 감시자의 역활로 보인다.
(많은 프로세스에 접근을 시도한다.)
이 파일이 메모리에 로드 될 쯤 해서 SDT Restore과정이 수행되어 진다.
(SDT Restore 0.2에 기반을 둔 것이 아닌, 0.1에 기반을 둔 것으로 보인다.)

00000044 오전 10:10:16 Type : Destroy
00000045 오전 10:10:16 Parent ID : 0x6B8 – game.exe
00000046 오전 10:10:16 Process ID : 0x1C4
00000047 오전 10:10:16 EPROCESS : 0x819BBB28
00000048 오전 10:10:16 Process Name : GameGuard.des

초기화 작업을 마치고, gameMon.des가 실행된 후, GameGuard.des는 파괴된다.

사용자가 game.exe의 종료를 요구하면,
다음과 같은 순서에 따라 파괴되게 된다.
00000292 오전 10:11:02 Type : Destroy
00000293 오전 10:11:02 Parent ID : 0x848
00000294 오전 10:11:02 Process ID : 0x6B8
00000295 오전 10:11:02 EPROCESS : 0x83FC4DA0
00000296 오전 10:11:02 Process Name : game.exe

게임이 먼저 사용자의 요구에 따라 파괴된다.

00000297 오전 10:11:09 Type : Destroy
00000298 오전 10:11:09 Parent ID : 0x6B8 – game.exe
00000299 오전 10:11:09 Process ID : 0x4A4
00000300 오전 10:11:09 EPROCESS : 0x829D0DA0
00000301 오전 10:11:09 Process Name : GameMon.des
다른 프로세스에 Injection하여 둔, npggNT.des를 모두 unload 하고,
사용하였던 Device Driver를 unload한 후, GameMon.des도 파괴된다.

2. Hook Chain

GameGuard는 다음과 같은 Hooking을 시도한다.

2.1 User Level

GameGuard는 모든 프로세스에 npggNT.des를 Injection 시키는데,
이 파일은 다음과 같은 Hooking을 시도 한다.

+ [0x7C930000] ntdll.dll
  - target : 0x458AA5D0 (npggNT.des), func : NtLoadDriver
  - target : 0x458AA720 (npggNT.des), func : NtOpenProcess
  - target : 0x458AA020 (npggNT.des), func : NtProtectVirtualMemory
  - target : 0x458AD6A0 (npggNT.des), func : NtQuerySystemInformatio
  - target : 0x458AA270 (npggNT.des), func : NtReadVirtualMemory
  - target : 0x458AB9D0 (npggNT.des), func : NtSuspendProcess
  - target : 0x458AB5A0 (npggNT.des), func : NtSuspendThread
  - target : 0x458AB860 (npggNT.des), func : NtTerminateProcess
  - target : 0x458AB6F0 (npggNT.des), func : NtTerminateThread
  - target : 0x458AA430 (npggNT.des), func : NtWriteVirtualMemory
  - target : 0x458AD6A0 (npggNT.des), func : RtlGetNativeSystemInfor
  - target : 0x458AA5D0 (npggNT.des), func : ZwLoadDriver
  - target : 0x458AA720 (npggNT.des), func : ZwOpenProcess
  - target : 0x458AA020 (npggNT.des), func : ZwProtectVirtualMemory
  - target : 0x458AD6A0 (npggNT.des), func : ZwQuerySystemInformatio
  - target : 0x458AA270 (npggNT.des), func : ZwReadVirtualMemory
  - target : 0x458AB9D0 (npggNT.des), func : ZwSuspendProcess
  - target : 0x458AB5A0 (npggNT.des), func : ZwSuspendThread
  - target : 0x458AB860 (npggNT.des), func : ZwTerminateProcess
  - target : 0x458AB6F0 (npggNT.des), func : ZwTerminateThread
  - target : 0x458AA430 (npggNT.des), func : ZwWriteVirtualMemory
+ [0x7C800000] kernel32.dll
  - target : 0x458A70E0 (npggNT.des), func : CreateProcessInternalW
  - target : 0x458AAB80 (npggNT.des), func : DebugActiveProcess
  - target : 0x458AACA0 (npggNT.des), func : DeviceIoControl
  - target : 0x458ABB10 (npggNT.des), func : GetProcAddress

- target : 0x458AAFA0 (npggNT.des), func : LoadLibraryExW
- target : 0x458AD0B0 (npggNT.des), func : MapViewOfFile
- target : 0x458AD310 (npggNT.des), func : MapViewOfFileEx
- target : 0x458ABC50 (npggNT.des), func : MoveFileW
- target : 0x458AA970 (npggNT.des), func : OpenProcess
- target : 0x458A8F80 (npggNT.des), func : ReadProcessMemory
- target : 0x458A96D0 (npggNT.des), func : VirtualProtect
- target : 0x458A9DB0 (npggNT.des), func : VirtualProtectEx
- target : 0x458A9240 (npggNT.des), func : WriteProcessMemory

+ [0x77F50000] ADVAPI32.dll
- target : 0x458AB4D0 (npggNT.des), func : CreateProcessWithLogonW

+ [0x77E20000] GDI32.dll
- target : 0x458ABE40 (npggNT.des), func : GetPixel

+ [0x77CF0000] USER32.dll
- target : 0x458AC080 (npggNT.des), func : GetWindowThreadProcessI
- target : 0x458A7FE0 (npggNT.des), func : PostMessageA
- target : 0x458A8350 (npggNT.des), func : PostMessageW
- target : 0x458A7410 (npggNT.des), func : SendInput
- target : 0x458A87F0 (npggNT.des), func : SendMessageA
- target : 0x458A8A10 (npggNT.des), func : SendMessageW
- target : 0x458A8A40 (npggNT.des), func : SetCursorPos
- target : 0x458A8BA0 (npggNT.des), func : SetWindowsHookExA
- target : 0x458A8DF0 (npggNT.des), func : SetWindowsHookExW
- target : 0x458A78B0 (npggNT.des), func : keybd_event
- target : 0x458A7D70 (npggNT.des), func : mouse_event

+ [0x762B0000] WINSTA.dll
- target : 0x458AD570 (npggNT.des), func : WinStationTerminateProc

* - 주로 Macro를 차단할 목적이나, game.exe,gameMode.des로의 접근을 차단하는 것 에 목적을 둔 Hook들로 보인다.

2.2 Kernel Level

GameGuard가 사용하는 sys파일은 dump_wmimmc.sys 라고 알려져 있으며, 다음과 같은 SSDT Hooking을 시도를 합니다.

service number_____ : 31

+ related nt function list_

- NtConnectPort
- ZwConnectPort

- hook_type_____ : entry hooking
- redirected address_____ : 0x848B2560
* hook module information__
- not found. maybe it is on the nonpaged pool area.

service number_____ : 122
+ related nt function list_
- NtOpenProcess
- ZwOpenProcess

- hook_type_____ : entry hooking
- redirected address_____ : 0xF7A6C682
* hook module information__
- not found. maybe it is on the nonpaged pool area.

service number_____ : 128
service number_____ : 137
+ related nt function list_
- NtProtectVirtualMemory
- ZwProtectVirtualMemory

- hook_type_____ : entry hooking
- redirected address_____ : 0xF7A6C7FA
* hook module information__
- not found. maybe it is on the nonpaged pool area.

service number_____ : 186
+ related nt function list_
- NtReadVirtualMemory
- ZwReadVirtualMemory

- hook_type_____ : entry hooking
- redirected address_____ : 0xF7A6C702
* hook module information__
- not found. maybe it is on the nonpaged pool area.

service number_____ : 277

+ related nt function list_
  - NtWriteVirtualMemory
  - ZwWriteVirtualMemory
- hook_type_____ : entry hooking
- redirected address_____ : 0xF7A6C77E
* hook module information__
  - not found. maybe it is on the nonpaged pool area.

* 주로 game.exe로의 접근을 차단하기 위한 hook으로 보인다.

service number_____ : 502
+ related function list____
  - SendInput
- hook_type_____ : entry hooking
- redirected address_____ : 0xF7A6C962
* hook module information__
  - not found. maybe it is on the nonpaged pool area.

* KeServiceDescriptorShadow의 SendInput을 Hook하여 Macro를
  차단하려는 시도를 하는 것으로 보인다.

또 ntoskrnl.exe의 export table에서 다음과 같은 함수의 Hooking을 시도한다.

module name_____ : ntoskrnl.exe
- base address_____ : 0x804D9000
- entry point address_____ : 0x806AE2BE
- module full path_____ : ₩WINDOWS₩system32₩ntoskrnl.exe
+ hooked function list_____
  + hooked function name_____ : KeAttachProcess
    - hook type_____ : opcode patching
    - redirected address_____ : 0xF79A513E
    - hook module information_ : not found.
  + hooked function name_____ : KeStackAttachProcess
    - hook type_____ : opcode patching
    - redirected address_____ : 0xF79A5038
    - hook module information_ : not found.

* 보호하는 Process로의 메모리 공간전환을 근본적으로 차단하고자
  설치한 Hook으로 보인다.

3. Miscellaneous

GameMon.des는 C:₩MyDocuments₩Local Settings₩Temp에
다음과 같은 파일들을 생성한다.
np5A.tmp np5B.tmp np5C.tmp np5D.tmp np5E.tmp np5F.tmp np60.tmp np61.tmp
위 파일들은 각각 내용은 다르며, PE포맷을 가진 실행파일이다.

ggscan.des 라는 파일은 GameMon.des에만 로드 된다.

Game.exe내에도 npggNT.des는 설치되나, Hooking의 범위에서는
제외되는 것으로 보인다.
npsc.des 라는 파일은 game.exe에만 로드 된다.