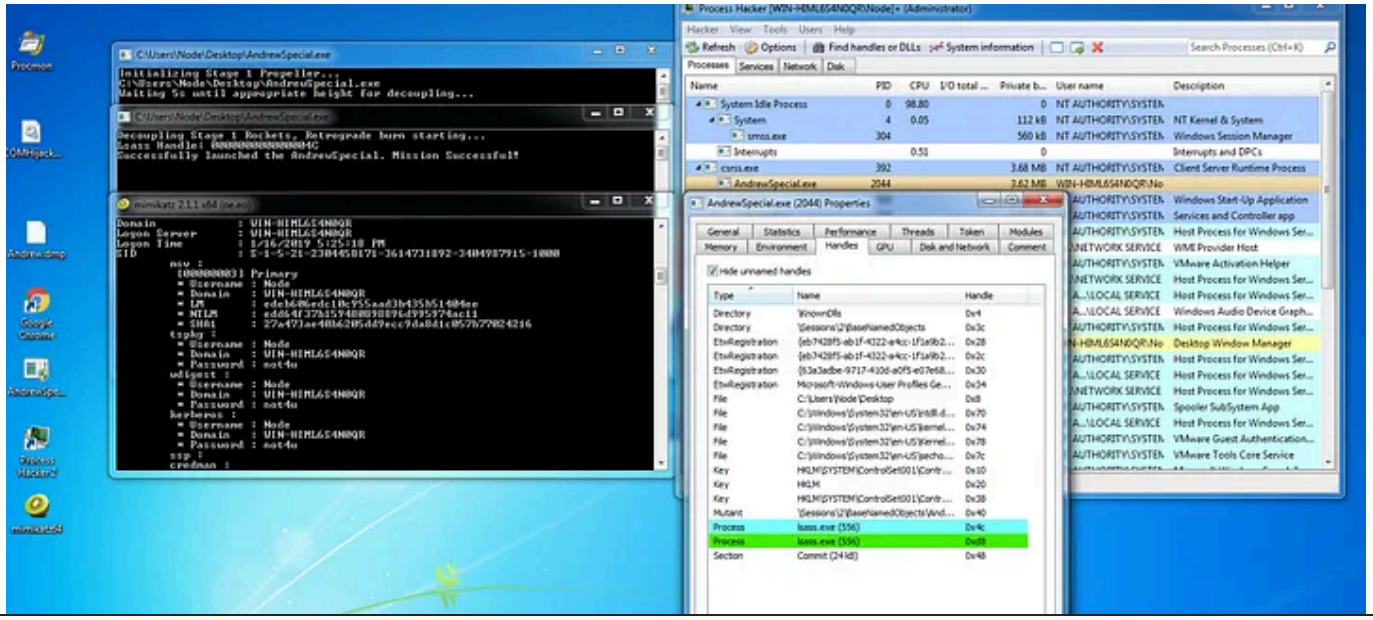
Bypass EDR’s memory protection, introduction to hooking

Hoang Bui · Follow

For those who recommends ProcDump

The Wrong Path

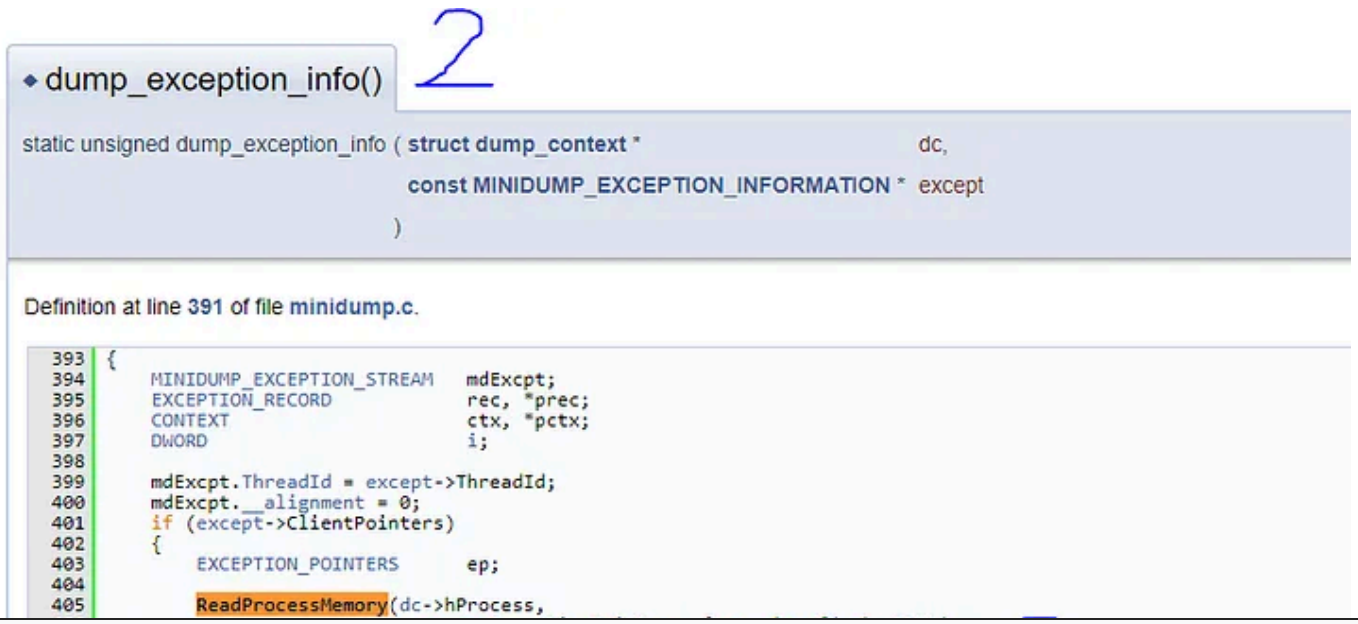
So now, as an ex-malware author — I know that there are a few things you could do as a driver to accomplish this detection and block. The first thing that comes to my mind was Obregistercallback which is commonly used by many Antivirus products. Microsoft implemented this callback due to many antivirus products performing very sketchy winapi hooks that reassemble malware rootkits. However, at the bottom of the msdn page, you will notice a



And what do you know, I got a handle with FULL CONTROL over lsass.exe. The EDR did not make a single fuzz about this. This is when I realized, I started off the approach the wrong way and the EDR never really cared about you gaining the handle access. It is what you do afterward with that handle that will come under scrutiny.

Back on Track

Knowing there was no fancy trick in getting a full control handle to lsass.exe, we can now move forward to find the next point of the issue. Immediately



◆ dump_exception_info()

```
static unsigned dump_exception_info ( struct dump_context *                    dc,
                                      const MINIDUMP_EXCEPTION_INFORMATION *  except
                                    )
```

Definition at line 391 of file minidump.c.

```
393 {
394     MINIDUMP_EXCEPTION_STREAM   mdExcpt;
395     EXCEPTION_RECORD            rec, *prec;
396     CONTEXT                     ctx, *pctx;
397     DWORD                       i;
398
399     mdExcpt.ThreadId = except->ThreadId;
400     mdExcpt.__alignment = 0;
401     if (except->ClientPointers)
402     {
403         EXCEPTION_POINTERS      ep;
404
405         ReadProcessMemory(dc->hProcess,
```

ReadProcessMemory is just a wrapper. It does a bunch of sanity check such as nullptr check. That is all RPM does. However, RPM also calls a function "NtReadVirtualMemory", which sets up the registers before doing a *syscall* instruction. Syscall instruction is just telling the CPU to enter kernel mode which then another function ALSO named NtReadVirtualMemory is called, which does the actual logic of what ReadProcessMemory is supposed to do.

— — — — — -Userland — — — —-— — | — — — Kernel Land — — —

RPM — > NtReadVirtualMemory — > SYSCALL >NtReadVirtualMemory

nature and that solution is known as Kernel Patch Protection (KPP or Patch Guard). KPP scans the kernel on almost every level and will triggers a BSOD if a modification is detected. This includes ntoskrnl portion which houses the WINAPI's kernel level's logic. With this knowledge, we are assured that the EDR would not and did not hook any kernel level function inside that portion of the call stack, leaving us with the user-land's RPM and NtReadVirtualMemory calls.

The Hook

Now, this provides us with the address of both RPM and ntReadVirtualMemory. I will now use my favorite reversing tool to read the memory and analyze its structure, Cheat Engine.

ReadProcessMemory

normal. The first 5 bytes of the function is modified and the rest are left as-is. You can tell this by looking at other similar functions around it. All the other functions follows a very similar format:

0x4C, 0x8B, 0xD1, // mov r10, rcx; NtReadVirtualMemory

0xB8, 0x3c, 0x00, 0x00, 0x00, // eax, 3ch — aka syscall id

0x0F, 0x05, // syscall

The EDR placed a jump instruction where the original NtReadVirtualMemory function is supposed to be, redirect the code flow into their own module which then checked for any sort of malicious activity. If the checks fail, the Nt* function would then return with an error code, never entering the kernel land and execute to begin with.

The Bypass

It is now very self-evident what the EDR is doing to detect and stop our WINAPI calls. But how do we get around that? There are two solutions.

The Result

I went with the first approach. It is simple, and it allows me to get out the blog quicker :). However, it would be trivial to do the second method and I have plans on doing just that within a few days. Introducing AndrewSpecial, for my manager Andrew who is currently battling a busted appendix in the hospital right now. Get well soon man.

Programming Hacking Malware Bypass Endpoint Security

-- 6