باسمه تعالی

تحلیل فنی بدافزار

DustMan

فهرست مطالب

۱. مقدمه :

اوایل سال ۲۰۲۰ میلادی اخباری مبنی بر حمله بدافزاری با ویژگی Wiper (پاک کننده) به تأسیسات نفت و انرژی کشور عربستان در فضای سایبری منتشر شد. براساس شواهد موجود و تحقیقات صورت‌گرفته توسط محققان امنیتی، بدافزار Dustman که از آن به عنوان سلاحی برای جنگ سایبری یاد می‌شود، شباهت بسیار زیادی به بدافزار ZeroCleare دارد که اوایل سپتامبر ۲۰۱۹ میلادی مشاهده شد. این شباهت‌ها شامل فایل اصلی ایجاد شده درون سیستم، الگوی رفتاری مشابه، License Key یکسان برای فایل اصلی و هدف سیاسی مشابه دو بدافزار می‌باشد. تحلیل پیش رو مربوط به نسخه منتشر شده بدافزار Dustman در تاریخ ۲۹ دسامبر ۲۰۱۹ میلادی می‌باشد.

۲. مشخصات فایل اجرایی :

نام فایل	Dustman.exe
MD5	8afa8a59eebf43ef223be52e08fcdc67
SHA-1	e3ae32ebe8465c7df1225a51234f13e8a44969cc
SHA-256	f07b0c79a8c88a5760847226af277cf34ab5508394a58820db4db5a8d0340fc7
نوع فایل	Win64 EXE
نوع ماشین	AMD AMD64
اندازه فایل	۲۵۸.۵ کیلوبایت

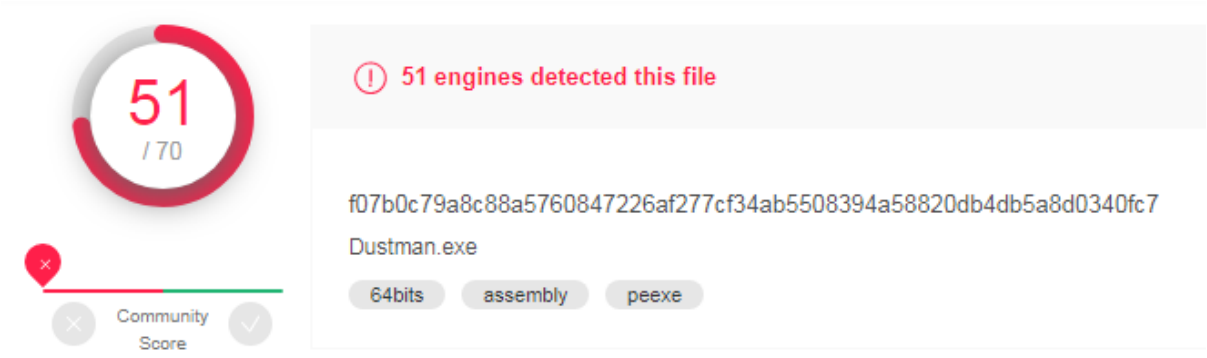
۳. شجره‌نامه

همانطور که در بخش مقدمه اشاره شد، بدافزار Dustman شباهت بسیار زیادی با بدافزار ZeroCleare دارد و به نظر می‌رسد نسخه‌ای توسعه یافته از این بدافزار، می‌باشد. هرچند محققان بر این باورند که هر دوی این بدافزارها ارتباط مستقیمی با بدافزار Shamoon که در سال ۲۰۱۲ منتشر شد دارند. لذا بر اساس شواهد موجود می‌توان خانواده بدافزار Dustman را این‌گونه برشمرد:

Shamoon -> ZeroCleare -> DUSTMAN

٤. میزان تهدید فایل باج‌افزار

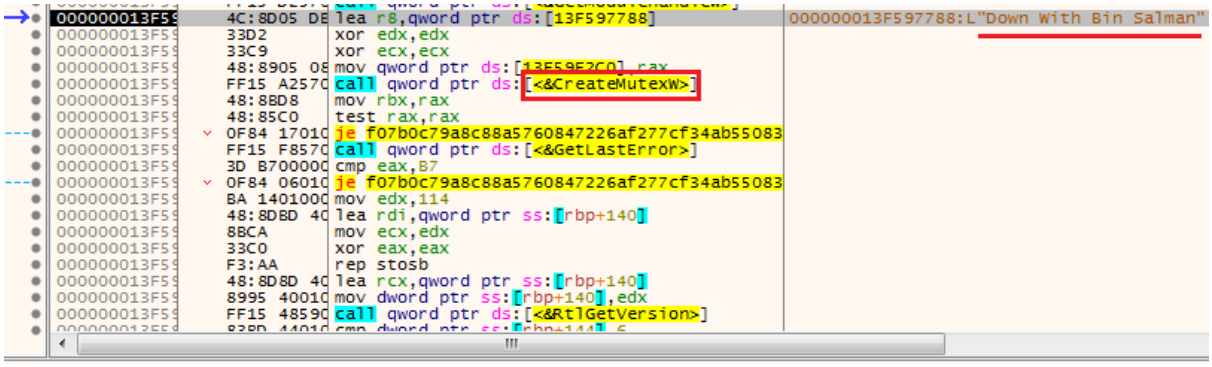
درحال حاضر تعداد ۵۱ مورد از ۷۰ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این بدافزار می‌باشند.



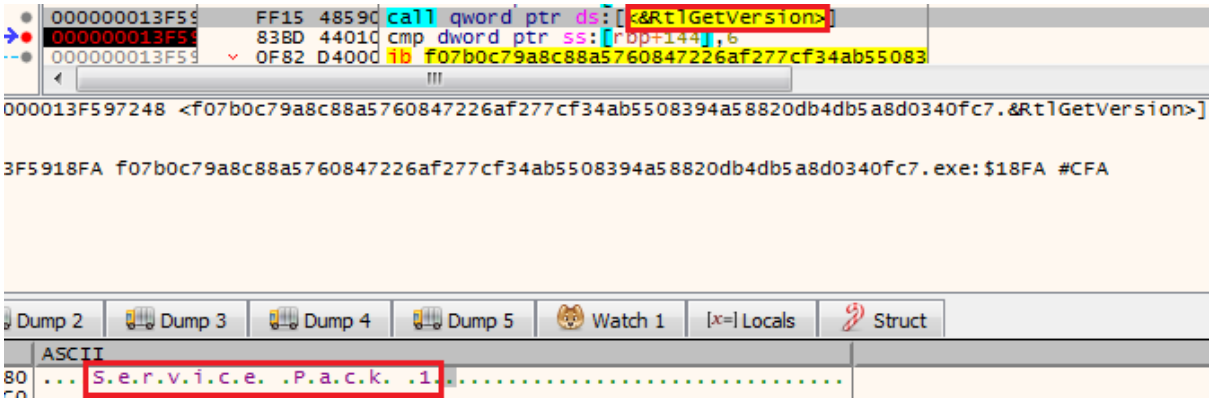
٥. تحلیل پویا

٥-١ آناتومی حمله:

برای تحلیل دقیق و گام به گام بدافزار Dustman، از محیط دیباگر استفاده کرده‌ایم که نتایج زیر حاصل شد؛ بدافزار Dustman در آغاز فعالیت خود در سیستم قربانی، یک Mutex با عنوان Down with Bin Salman درون سیستم ایجاد می‌کند. عنوان مذکور به روشنی بیانگر هدف مشخص این بدافزار می‌باشد که به آن اشاره شد.

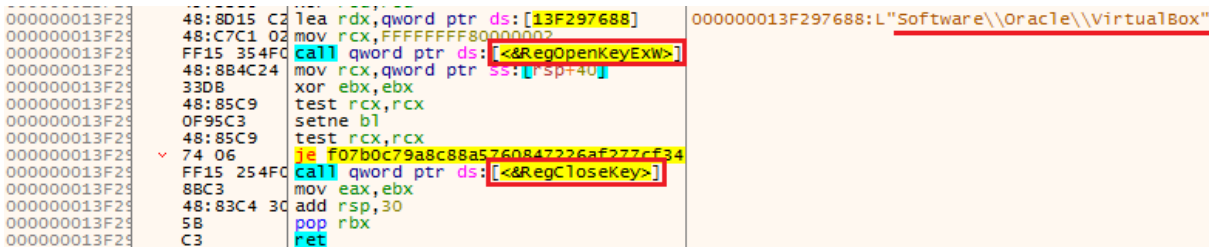


بدافزار در ادامه، اطلاعات مربوط به نسخه سیستم‌عامل قربانی را دریافت می‌کند و آن را با حداقل نسخه‌ای که به صورت پیش‌فرض درنظر گرفته است، مقایسه می‌کند.

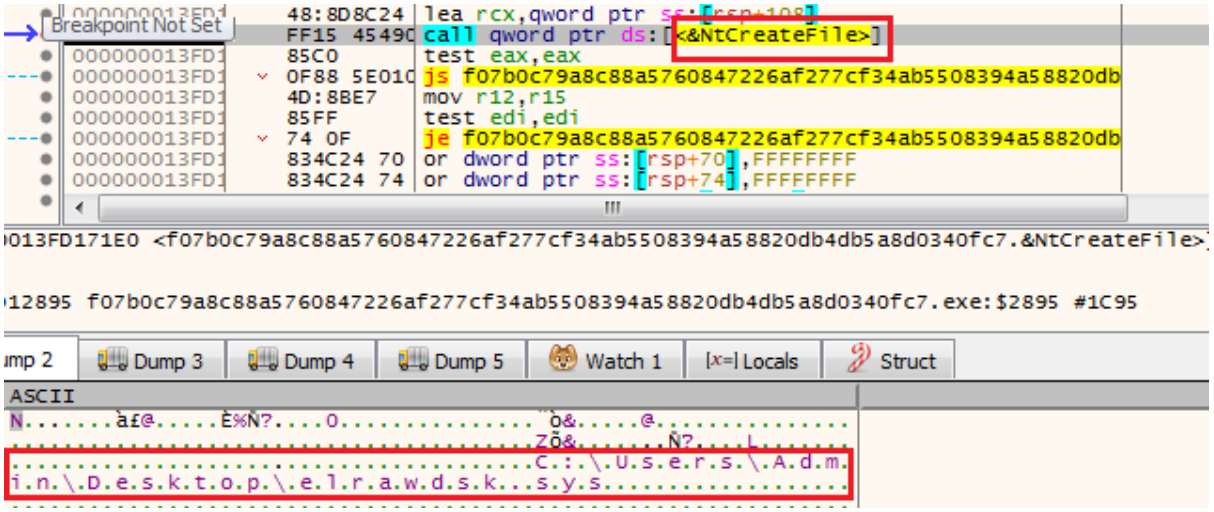


در صورتی که سیستم‌عامل مورد هدف با نسخه پیش‌فرض برابر یا جدیدتر از آن باشد، بدافزار به مرحله بعدی فرآیند خود وارد می‌شود.

در این قسمت، با استفاده از مقادیر رجیستری سیستم، وضعیت نصب یا عدم نصب نرم‌افزار VirtualBox در سیستم قربانی، مورد بررسی قرار می‌گیرد.



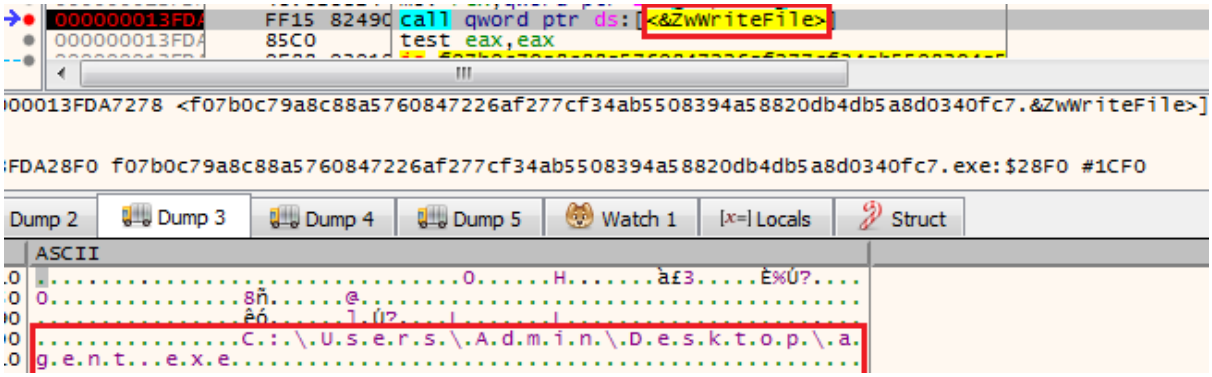
سپس، بدافزار فایلی با عنوان elrawdsk.sys (Eldos Rawdisk Driver) را در مسیری که خود در آن قرار گرفته است، ایجاد می‌کند.



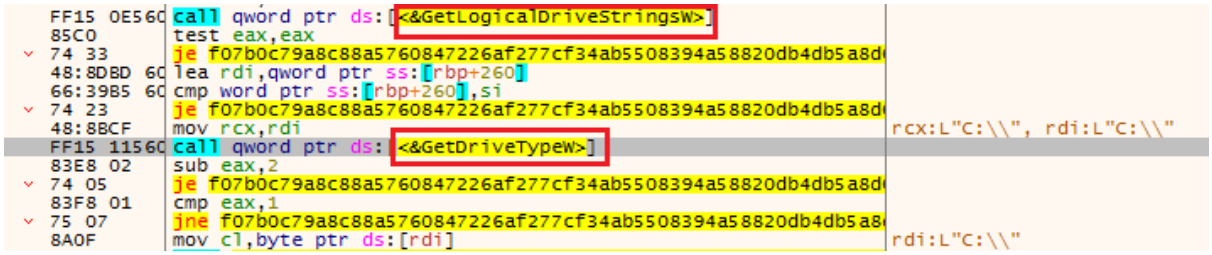
این فایل یک درایور مربوط به شرکت EldoS می‌باشد که امکان تغییر مستقیم داده‌ها بر روی هارددیسک را می‌دهد. در برخی موارد، درایور می تواند این تغییرات را در سطح کاربر (User-Mode) اعمال کند و

مکانیزم‌های امنیتی سیستم عامل ویندوز را دور بزنند. بدافزار Shamoon نیز از این درایور برای اعمال تغییرات در نقاط Write Protect ویندوز استفاده می‌کرد.

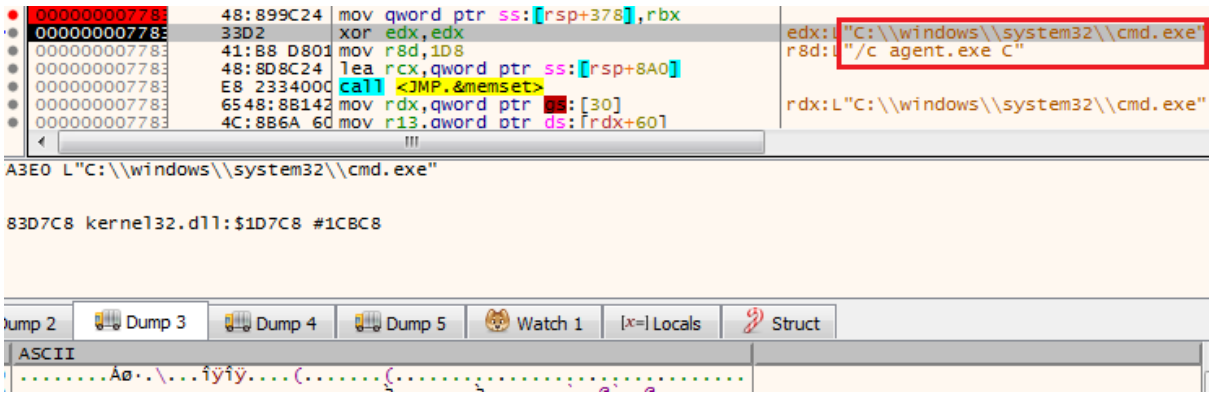
در ادامه روند فعالیت این بدافزار در سیستم قربانی، فایل دیگری با عنوان agent.exe مجدداً در همان مسیری که فایل اصلی بدافزار قرار دارد، ایجاد می‌شود.



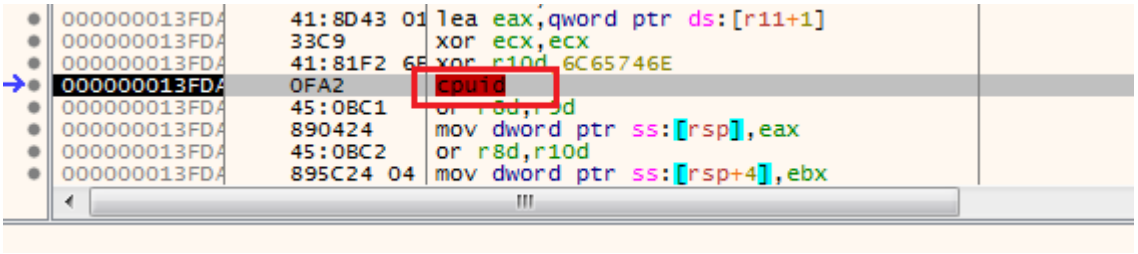
سپس، تمام سربرگ‌های ممکن برای درایوهای سیستم‌عامل و همچنین درایوهای موجود در سیستم قربانی، جستجو می‌شود.



درانتها فایل agent.exe در محیط CMD ویندوز و با استفاده از دستور مشخص شده در تصویر زیر اجرا شده و فایل اصلی متوقف می‌شود.



فرآیند agent.exe پس از اجرا، اقدام به جمع‌آوری تمام اطلاعات مربوط به پردازنده سیستم قربانی می‌کند.



با توجه به اینکه بدافزار DustMan برای سیستم‌های با پردازنده AMD طراحی شده است، در صورتی که براساس نتایج حاصل، پردازنده سیستم AMD باشد، روند فعالیت این فرآیند درون سیستم ادامه می‌یابد.

در ادامه مقداری به عنوان کلید License جهت استفاده از درایور elrawdsk.sys تنظیم می‌شود تا مهاجم امکان استفاده از توابع این درایور در سیستم قربانی را پیدا کند.

از آنجا که کلید License درون این فایل استفاده شده و همچنین از تابعی برای ارسال دستور به درایور بکارگیری شده است، در واقع فایل اجرایی agent.exe در نقش پایلود درایور قرار گرفته شده در سیستم قربانی عمل کرده و خود درایور elrawdsk.sys به عنوان فایل اصلی بدافزار، عمل پاکسازی دیسک در سیستم قربانی را انجام می‌دهد.

۵-۲ روش انتشار:

براساس گزارش‌های منتشر شده، مهاجمان ابتدا از طریق اجرای اکسپلویت بر روی سرورهای VPN به آن‌ها دسترسی پیدا کرده و حساب ادمین شبکه را تصاحب می‌کنند. سپس، فایل اولیه بدافزار و همچنین ابزار اجرای از راه دور (PSEXEC) را در سرور کنسول مدیریتی آنتی‌ویروس، کپی می‌کنند. سپس با استفاده از حساب کنسول مدیریت آنتی‌ویروس، اقدام به انتشار بدافزار در تمامی سیستم‌های درون شبکه کرده و در نهایت از طریق ابزار PSEXEC، فایل بدافزار را بر روی تمامی سیستم‌های قربانی اجرا می‌کنند.

۵-۳ روش جلوگیری:

با توجه به روش ورود این بدافزار به شبکه مورد هدف خود، توصیه می‌شود به صورت مداوم سیستم‌های موجود در شبکه را به روزرسانی کرده و در صورت استفاده از VPN در شبکه شرکت یا سازمان خود، آسیب‌پذیری‌های منتشر شده برای این سرورها را مرتباً رصد کرده و آن‌ها را دائماً با وصله‌های امنیتی که منتشر می‌شود، به‌روزرسانی کنید. همچنین توصیه می‌گردد اقدامات مربوط به امن‌سازی حساب مدیر(ادمین) سرور و سیستم‌های متصل به شبکه را انجام دهید تا به آسانی مورد سوءاستفاده قرار نگیرند.

٦. تحلیل ایستا

بررسی‌های اولیه بر روی کد بدافزار Dustman نشان می‌دهد که این بدافزار برای پردازنده‌های ٦٤ بیتی شرکت AMD طراحی شده است. همچنین این بدافزار بر روی سیستم‌عامل ویندوز ویستا و نسخه‌های بعد از آن، قابل اجرا می‌باشد.

Field	Data	Details
PE header		
Signature	00004550	
Machine	8664	64-bit Windows (AMD)
Number of sections	0006	
Time/Date stamp (local)	5E08403F	2019-12-29 09:27:19
Time/Date stamp (UTC)	5E08403F	2019-12-29 05:57:19
Pointer to symbol table	00000000	
Number of symbols	00000000	
Size of optional header	00F0	
Characteristics	0022	Executable, Large Address Aware
PE32 optional header		
Magic	020B	
Version of Linker (major)	0E	
Version of Linker (minor)	10	
Size of code	00005A00	
Size of initialized data	0003B800	
Size of uninitialized data	00000000	
Address of entry point	00001878	
Base of code	00001000	
Image base	0000000140000000	
Section alignment	00001000	
File alignment	00000200	
OS version (major)	0006	Windows Vista

۶-۱ تحلیل کد:

فایل اولیه این بدافزار با نام Dustman.exe، ازتابع Start شروع شده و در ابتدا از طریق تابع CreateMutexW یک Mutex با عنوان Down With Bin Salman ایجاد می‌کند.

```
public start
start proc near

var_830= dword ptr -830h
Buffer= word ptr -820h
var_618= dword ptr -618h
var_614= dword ptr -614h
var_60C= dword ptr -60Ch
RootPathName= word ptr -4F8h
SourceString= word ptr -418h

mov     rax, rsp
mov     [rax+10h], rbx
mov     [rax+18h], rsi
mov     [rax+20h], rdi
push    rbp
lea     rbp, [rax-758h]
sub     rsp, 850h
xor     esi, esi
xor     ecx, ecx        ; lpModuleName
mov     [rbp+760h], esi
call    cs:GetModuleHandleW
lea     r8, Name        ; "Down With Bin Salman"
xor     edx, edx        ; bInitialOwner
xor     ecx, ecx        ; lpMutexAttributes
mov     cs:qword_14000F2C0, rax
call    cs:CreateMutexW
mov     rbx, rax
test    rax, rax
jz      loc_1400019E1
```

در ادامه از طریق تابع GetVersion نسخه سیستم‌عامل قربانی دریافت و بررسی می‌شود. در صورتی که نسخه سیستم‌عامل قربانی برابر با عدد ۶ (ویندوز ویستا) و بالاتر باشد، روند فعالیت فایل درون سیستم‌عامل ادامه پیدا خواهد کرد.

```
mov     edx, 114h
lea     rdi, [rbp+758h+var_618]
mov     ecx, edx
xor     eax, eax
rep stosb
lea     rcx, [rbp+758h+var_618]
mov     [rbp+758h+var_618], edx
call    cs:RtlGetVersion
cmp     [rbp+758h+var_614], 6
jb      loc_1400019E1
```

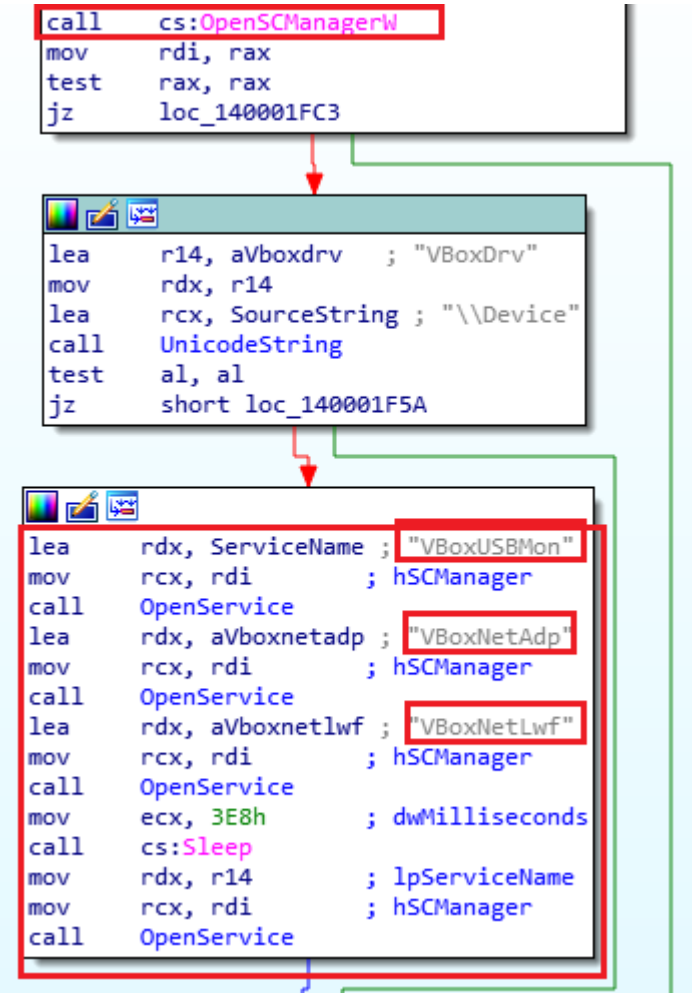
بررسی نسخه سیستم‌عامل

پس از بررسی نسخه سیستم‌عامل، از طریق جستجو در مقادیر رجیستری، وضعیت نصب یا عدم نصب نرم‌افزار VirtualBox درون سیستم‌عامل، بررسی می‌شود.

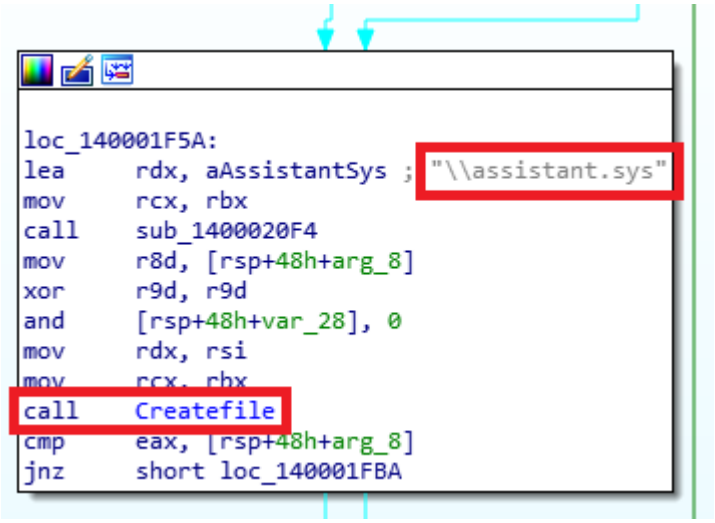
```
call    CheckVirBox
mov     cs:dword_14
lea     rdi, [rsp+8
xor     eax, eax
lea     rdx, [rsp+8
mov     ecx, 20Ah
rep stosb
mov     ecx, 104h
call    cs:GetCurre
lea     rdx, asc_14
lea     rcx, [rsp+8
call    sub_140002(
lea     rdx, aElra
lea     rcx, [rsp+8
call    sub_140002(
mov     rdx, cs:qw
lea     r8, [rbp+7
lea     ecx, [rsi+(
call    sub_140002
test    rax, rax
jz      short loc_
```

```
CheckVirBox     proc near               ; CODE XREF: start+A1↑p
                                        ; DATA XREF: .pdata:00000001400100A8↓o

phkResult       = qword ptr -18h
hKey            = qword ptr  8

                push    rbx
                sub     rsp, 30h
                and     [rsp+38h+hKey], 0
                lea     rax, [rsp+38h+hKey]
                mov     r9d, 20019h     ; samDesired
                mov     [rsp+38h+phkResult], rax ; phkResult
                xor     r8d, r8d        ; ulOptions
                lea     rdx, SubKey     ; "Software\\Oracle\\VirtualBox"
                mov     rcx, 0FFFFFFFF80000002h ; hKey
                call    cs:RegOpenKeyExW
                mov     rcx, [rsp+38h+hKey] ; hKey
                xor     ebx, ebx
                test    rcx, rcx
                setnz   bl
                test    rcx, rcx
                jz      short loc_1400020EB
                call    cs:RegCloseKey
```

پس از این مرحله، در صورتی که نرم‌افزار VirtualBox بر روی سیستم‌عامل سیستم قربانی نصب شده باشد، بدافزار تلاش می‌کند تا سرویس‌های مربوط به این نرم‌افزار را متوقف کند.



در ادامه فایلی با عنوان assistant.sys در همان مسیری که فایل اولیه بدافزار قرار دارد نیز ایجاد خواهد شد.



براساس بررسی‌های صورت گرفته و همچنین گزارشی از وبسایت SecurityIntelligence ، این فایل درایوری آسیب‌پذیر مربوط به نرم‌افزار VirtualBox می‌باشد که از طریق اجرای دستوری در محیط

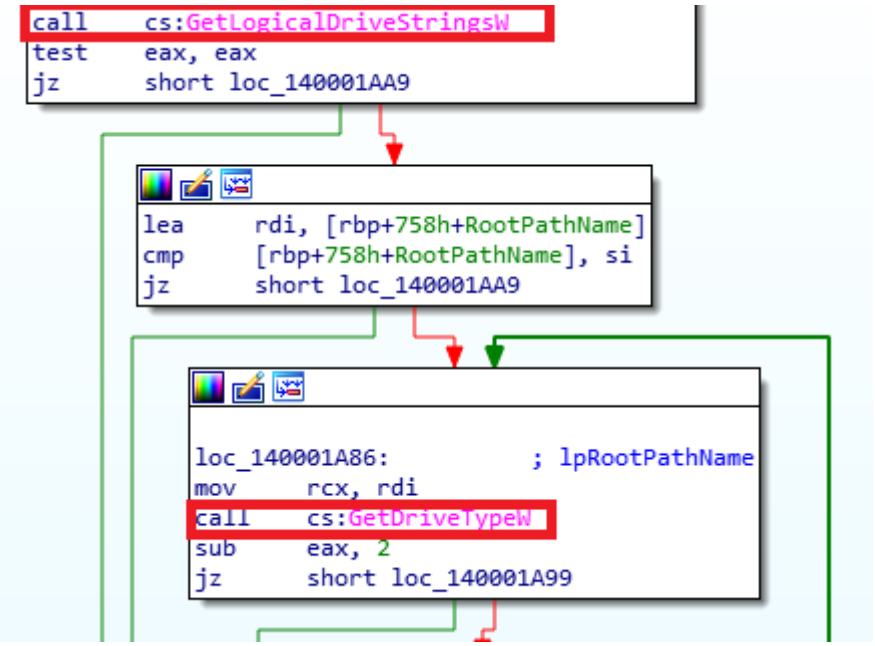
Shellcode سیستم‌عامل، اکسپلویت می‌شود و از این طریق، درایور elrawdsk.sys به عنوان جزء اصلی در پاک کردن فضای ذخیره سازی، درون سیستم قربانی قرار می‌گیرد.

```
mov     cs:dword_14000E7C0, eax
lea     rdi, [rsp+850h+Buffer]
xor     eax, eax
lea     rdx, [rsp+850h+Buffer] ; lpBuffer
mov     ecx, 20Ah
rep stosb
mov     ecx, 104h       ; nBufferLength
call    cs:GetCurrentDirectoryW
lea     rdx, asc_1400077B4 ; "\\"
lea     rcx, [rsp+850h+Buffer]
call    sub_1400020F4
lea     rdx, aElrawdskSys ; "elrawdsk.sys"
lea     rcx, [rsp+850h+Buffer]
call    sub_1400020F4
mov     rdx, cs:qword_14000F2C0
lea     r8, [rbp+760h]
lea     ecx, [rsi+67h]
call    sub_140002548
test    rax, rax
jz      short loc_1400019E1
```

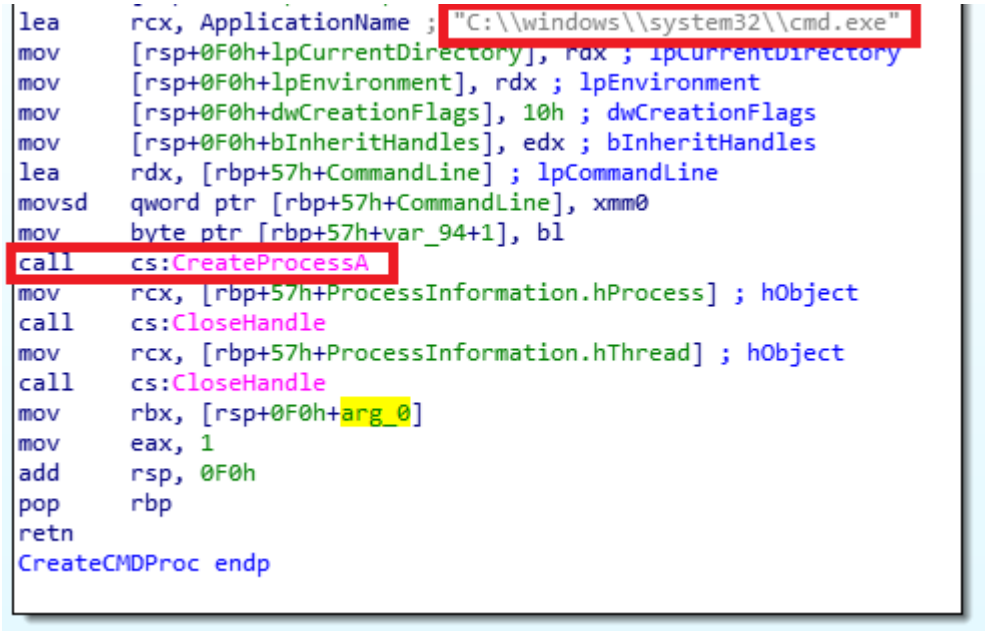
در ادامه فایل اجرایی با عنوان agent.exe همانند دو فایل دیگر، در مسیر قرارگیری فایل اولیه بدافزار، ایجاد می‌شود.

```
loc_1400019E1:          ; hObject
mov     rcx, rbx
call    cs:CloseHandle
xor     eax, eax
lea     rdi, [rsp+850h+Buffer]
mov     ecx, 20Ah
lea     rdx, [rsp+850h+Buffer] ; lpBuffer
rep stosb
mov     ecx, 104h       ; nBufferLength
call    cs:GetCurrentDirectoryW
lea     rdx, asc_1400077B4 ; "\\"
lea     rcx, [rsp+850h+Buffer]
call    sub_1400020F4
lea     rdx, aAgentExe  ; "agent.exe"
lea     rcx, [rsp+850h+Buffer]
call    sub_1400020F4
mov     rdx, cs:qword_14000F2C0
lea     r8, [rbp+760h]
mov     ecx, 6Ah
call    sub_140002548
mov     r8d, [rbp+760h]
lea     rcx, [rsp+850h+Buffer]
xor     r9d, r9d
mov     [rsp+850h+var_830], esi
mov     rdx, rax
call    CreateFile
```

سپس تمام درایوهای موجود در سیستم قربانی جستجو می‌شود.



همچنین فایل اجرایی agent.exe در محیط CMD ویندوز اجرا می‌شود.



و در نهایت فایل اولیه بدافزار Dustman متوقف شده و ادامه فعالیت این بدافزار درون سیستم قربانی، از طریق فایل اجرایی agent.exe صورت می‌گیرد.

فایل agent.exe قبل از هرگونه اقدامی در سیستم قربانی، ابتدا با استفاده از پارامتر cpuid تمام اطلاعات مربوط به پردازنده سیستم قربانی را دریافت می‌کند.

```
xor     ecx, ecx
mov     cs:dword_14001B04C, 2
xor     eax, eax
mov     cs:dword_14001B048, 1
cpuid
mov     r10d, ecx
mov     r9d, edx
xor     ecx, 444D4163h
xor     edx, 69746E65h
mov     ebp, ebx
xor     r11d, r11d
xor     ebp, 68747541h
mov     r8d, ebx
or      ebp, edx
mov     r14d, eax
or      ebp, ecx
xor     r9d, 49656E69h
xor     r8d, 756E6547h
lea     eax, [r11+1]
xor     ecx, ecx
xor     r10d, 6C65746Eh
cpuid
```

با توجه به اینکه این بدافزار برای سیستم‌هایی با پردازنده AMD طراحی شده است، درصورتی که پردازنده سیستم AMD باشد، روند فعالیت فایل در سیستم قربانی ادامه می‌یابد.

در ادامه، از طریق تابع DeviceIOControl دستوری برای درایور elrawdsk.sys ارسال می‌شود و سپس عملیات پاک سازی هارد دیسک سیستم قربانی، توسط این درایور آغاز می‌شود.

```
cmovnz  edx, eax        ; dwIoControlCode
xor     ecx, ecx
lea     rax, [r11+8]
mov     [r11-30h], rcx
mov     [r11-38h], rax
mov     [rsp+68h+nOutBufferSize], ecx ; nOutBufferSize
mov     [r11-28h], r8
mov     [r11-20h], r9d
lea     r9d, [rcx+18h]  ; nInBufferSize
mov     [r11-48h], rcx
lea     r8, [r11-28h]   ; lpInBuffer
mov     rcx, r10        ; hDevice
call    cs:DeviceIoControl
add     rsp, 68h
retn
sub_1400013A0 endp
```

۲-۶ تحلیل ترافیک شبکه:

پس از بررسی‌های صورت گرفته و همچنین مشاهده نتایج سندباکس‌های آنلاین، ترافیک مشکوکی مربوط به این بدافزار مشاهده نشد.