

باسمه تعالی

تحلیل فنی بدافزار

DustMan

فهرست مطالب

۱. مقدمه : ۳
۲. مشخصات فایل اجرایی : ۳
۳. شجره نامه ۳
۴. میزان تهدید فایل باج افزار: ۳
۵. تحلیل پویا ۴
- ۵-۱ آناتومی حمله: ۴
- ۵-۲ روش انتشار: ۴
- ۵-۳ روش جلوگیری: ۷
- ۶- تحلیل ایستا ۸
- ۶-۱ تحلیل کد: ۹
- ۶-۲ تحلیل ترافیک شبکه: ۱۴

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 صورت گرفته توسط محققان امنیتی، بدافزار Dustman که از آن به عنوان سلاحی برای جنگ سایبری یاد می شود، شباهت بسیار زیادی به بدافزار ZeroCleare دارد که اوایل سپتامبر ۲۰۱۹ میلادی مشاهده شد. این شباهت ها شامل فایل اصلی ایجاد شده درون سیستم، الگوی رفتاری مشابه، License Key یکسان برای فایل اصلی و هدف سیاسی مشابه دو بدافزار می باشد. تحلیل پیش رو مربوط به نسخه منتشر شده بدافزار Dustman در تاریخ ۲۹ دسامبر ۲۰۱۹ میلادی می باشد.

۲. مشخصات فایل اجرایی :

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

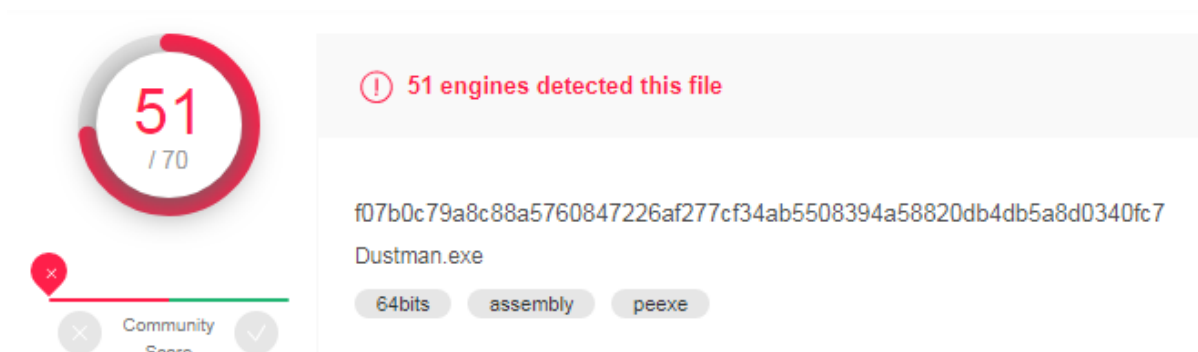
۳. شجره نامه

همانطور که در بخش مقدمه اشاره شد، بدافزار Dustman شباهت بسیار زیادی با بدافزار ZeroCleare دارد و به نظر می رسد نسخه ای توسعه یافته از این بدافزار، می باشد. 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 می توان خانواده بدافزار Dustman را این گونه برشمرد:

Shamoon -> ZeroCleare -> DUSTMAN

۴. میزان تهدید فایل باج افزار

در حال حاضر تعداد ۵۱ مورد از ۷۰ ضدبدا افزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این بدافزار می باشند.



۵. تحلیل پویا

۵-۱ آناتومی حمله:

برای تحلیل دقیق و گام به گام بدافزار Dustman، از محیط دیباگر استفاده کرده ایم 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 می کند. عنوان مذکور به روشنی بیانگر هدف مشخص این بدافزار می باشد که به آن اشاره شد.

```

000000013F597788 4C:8D05 DE lea r8,qword ptr ds:[13F597788] 000000013F597788:L"Down With Bin Salman"
000000013F597788 33D2 xor edx,edx
000000013F597788 33C9 xor ecx,ecx
000000013F597788 48:8905 08 mov qword ptr ds:[33E59E7C0],rax
000000013F597788 FF15 A257C call qword ptr ds:[<&CreateMutexW>]
000000013F597788 48:88D8 mov rbx,rax
000000013F597788 48:85C0 test rbx,rax
000000013F597788 0F84 1701D je F07b0c79a8c88a5760847226af277cf34ab55083
000000013F597788 FF15 F857C call qword ptr ds:[<&GetLastError>]
000000013F597788 3D B70000C cmp eax,B7
000000013F597788 0F84 0601D je F07b0c79a8c88a5760847226af277cf34ab55083
000000013F597788 BA 140100C mov edx,114
000000013F597788 48:8DBD 4C lea rdi,qword ptr ss:[rbp+140]
000000013F597788 8BCA mov ecx,edx
000000013F597788 33C0 xor eax,eax
000000013F597788 F3:AA rep stosb
000000013F597788 48:8D8D 4C lea rcx,qword ptr ss:[rbp+140]
000000013F597788 8995 4001C mov dword ptr ss:[rbp+140],edx
000000013F597788 FF15 4859C call qword ptr ds:[<&RtlGetVersion>]
000000013F597788 83BD 4401C cmp dword ptr ss:[rbp+144],6

```

بدافزار در ادامه، اطلاعات مربوط به نسخه سیستم عامل قربانی را دریافت می کند و آن را با حداقل نسخه ای که به صورت پیش فرض در نظر گرفته است، مقایسه می کند.

```

000000013F59 FF15 4859C call qword ptr ds:[<&RtlGetVersion>]
000000013F59 838D 4401C cmp dword ptr ss:[rbp+144],6
000000013F59 0F82 D4000 jb f07b0c79a8c88a5760847226af277cf34ab55083
<-----
000013F597248 <f07b0c79a8c88a5760847226af277cf34ab5508394a58820db4db5a8d0340fc7.&RtlGetVersion>]
3F5918FA f07b0c79a8c88a5760847226af277cf34ab5508394a58820db4db5a8d0340fc7.exe:$18FA #CFA

Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | [x=] Locals | Struct
ASCII
80 | ... S.e.r.v.i.c.e. .P.a.c.k. .1. ....
90 |

```

در صورتی که سیستم عامل مورد هدف با نسخه پیش فرض برابر یا جدیدتر از آن باشد، بدافزار به مرحله بعدی فرآیند خود وارد می شود.

در این قسمت، با استفاده از مقادیر رجیستری سیستم، وضعیت نصب یا عدم نصب نرم افزار VirtualBox در سیستم قربانی، مورد بررسی قرار می گیرد.

```

000000013F25 48:8D15 C2 lea rcx,qword ptr ds:[13F297688] 000000013F297688:L"Software\Oracle\VirtualBox"
000000013F25 48:C7C1 02 mov rcx,FFFFFFFF80000002
000000013F25 FF15 354FD call qword ptr ds:[<&RegOpenKeyExW>]
000000013F25 48:884C24 mov rcx,qword ptr ss:[rsp+40]
000000013F25 33DB xor ebx,ebx
000000013F25 48:85C9 test rcx,rcx
000000013F25 0F95C3 setne bl
000000013F25 48:85C9 test rcx,rcx
000000013F25 74 06 je f07b0c79a8c88a5760847226af277cf34
000000013F25 FF15 254FD call qword ptr ds:[<&RegCloseKey>]
000000013F25 88C3 mov eax,ebx
000000013F25 48:83C4 30 add rsp,30
000000013F25 58 pop rbx
000000013F25 C3 ret

```

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

```

Breakpoint Not Set 48:8D8C24 lea rcx,qword ptr ss:[rsp+108]
FF15 4549C call qword ptr ds:[<&NtCreateFile>]
85C0 test eax,eax
000000013FD1 0F88 5E01C js f07b0c79a8c88a5760847226af277cf34ab5508394a58820db
4D:8BE7 mov r12,r15
85FF test edi,edi
000000013FD1 74 0F je f07b0c79a8c88a5760847226af277cf34ab5508394a58820db
000000013FD1 834C24 70 or dword ptr ss:[rsp+70],FFFFFFFF
000000013FD1 834C24 74 or dword ptr ss:[rsp+74],FFFFFFFF
<-----
0013FD171E0 <f07b0c79a8c88a5760847226af277cf34ab5508394a58820db4db5a8d0340fc7.&NtCreateFile>]
12895 f07b0c79a8c88a5760847226af277cf34ab5508394a58820db4db5a8d0340fc7.exe:$2895 #1C95

Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | [x=] Locals | Struct
ASCII
N ..... äf@. .... È%N?. .... 0 ..... 0&. .... @ .....
i.n.\.D.e.s.k.t.o.p.\.e.l.r.a.w.d.s.k..s.y.s.....C.:\.U.s.e.r.s.\.A.d.m.

```

این فایل یک درایور مربوط به شرکت EldoS می باشد که امکان تغییر مستقیم داده ها بر روی هارد دیسک را می دهد. در برخی موارد، درایور می تواند این تغییرات را در سطح کاربر (User-Mode) اعمال کند و

مکانیزم‌های امنیتی سیستم عامل ویندوز را دور بزند. 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.

The screenshot shows a debugger window with assembly code. The highlighted instruction is `call qword ptr ds:[<ZwwriteFile>]`. Below the assembly view, the ASCII dump shows the file path `C:\U.S.E.R.S.\A.d.m.i.n.\D.e.s.k.t.o.p.\a.g.e.n.t..e.x.e.`.

سپس، تمام سریرگ‌های ممکن برای درایوهای سیستم عامل و همچنین درایوهای موجود در سیستم قربانی، جستجو می‌شود.

The screenshot shows assembly code for `<GetLogicalDriveStrings>` and `<GetDriveTypeW>`. The `<GetDriveTypeW>` instruction is highlighted. The register dump shows `rcx:L"C:\\", rdi:L"C:\\"`.

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

The screenshot shows assembly code for `<JMP.&memset>`. The register dump shows `edx:"C:\\windows\\system32\\cmd.exe"` and `r8d:"/c agent.exe C"`. The ASCII dump shows the command `A0... \... iyiy... (.....)`.

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

```

0000000013FDA 41:8D43 01 lea eax,qword ptr ds:[r11+1]
0000000013FDA 33C9 xor ecx,ecx
0000000013FDA 41:81F2 6E xor r10d,6C65746E
0000000013FDA 0FA2 cpu1d
0000000013FDA 45:0BC1 or r8d,r8d
0000000013FDA 890424 mov dword ptr ss:[rsp],eax
0000000013FDA 45:0BC2 or r8d,r10d
0000000013FDA 895C24 04 mov dword ptr ss:[rsp+4],ebx

```

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.

```

lea r8,qword ptr ds:[13FD887A0]
mov edx,C0000000
call agent.13FDA10C0
mov r15,rax
mov rcx,rax
call agent.13FDA1150
mov r12,rax
mov rcx,r15
call agent.13FDA1100
mov ecx,eax
xor edx,edx
mov eax,1400000
div ecx
mov esi,eax
mov edx,3E8
lea rcx,qword ptr ss:[rbp+420]
call qword ptr ds:[<&GetSystemDirectoryw>]
movzx ecx,word ptr ss:[rbp+420]
call agent.13FDA6D04

```

0000000013FD887A0: "b4b615c28ccd059cf8ed1abf1c71fe03c0354522990af63adf3c911e2287a4b906d47d"

\$2115 #1515

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.

۲-۵ 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.

۳-۵ 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.

۶. تحلیل ایستا

بررسی‌های اولیه بر روی کد بدافزار Dustman نشان می‌دهد که این بدافزار برای پردازنده‌های ۶۴ 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	00000000140000000	
Section alignment	00001000	
File alignment	00000200	
OS version (major)	0006	Windows Vista

۱-۶ تحلیل کد:

فایل اولیه این بدافزار با نام Dustman.exe، از تابع 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 سیستم عامل قربانی دریافت و بررسی می‌شود. در صورتی که نسخه سیستم عامل قربانی برابر با عدد ۶ (ویندوز ویستا) و بالاتر باشد، روند فعالیت فایل درون سیستم عامل 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 سیستم عامل

پس از بررسی نسخه سیستم عامل، از طریق جستجو در مقادیر رجیستری، وضعیت نصب یا عدم نصب نرم افزار VirtualBox درون سیستم عامل، بررسی می شود.

```

call    CheckVirBox; CheckVirBox    proc near                ; CODE XREF: start+A11p
mov     cs:dword_14...                ; DATA XREF: .pdata:00000001400100A8↓
lea     rdi, [rsp+...
xor     eax, eax                    ; phkResult = qword ptr -18h
lea     rdx, [rsp+...                ; hKey = qword ptr 8
mov     ecx, 20Ah
rep stosb
mov     ecx, 104h
call   cs:GetCurre...
lea     rdx, asc_14...
lea     rcx, [rsp+...
call   sub_1400020...
lea     rdx, aElrav...
lea     rcx, [rsp+...
call   sub_1400020...
mov     rdx, cs:qw...
call   cs:RegOpenKeyExW
lea     r8, [rbp+7...
lea     ecx, [rsi+...
call   sub_1400020...
test   rax, rax
jz     short loc_...

```

پس از این مرحله، در صورتی که نرم افزار VirtualBox بر روی سیستم عامل سیستم قربانی نصب شده باشد، بدافزار تلاش می کند تا سرویس های مربوط به این نرم افزار را متوقف کند.

```

call cs:OpenSCManagerW
mov rdi, rax
test rax, rax
jz loc_140001FC3

lea r14, aVBoxDrv ; "VBoxDrv"
mov rdx, r14
lea rcx, SourceString ; "\\Device"
call UnicodeString
test al, al
jz short loc_140001F5A

lea rdx, ServiceName ; "VBoxUSBMon"
mov rcx, rdi ; hSCManager
call OpenService
lea rdx, aVBoxNetAdp ; "VBoxNetAdp"
mov rcx, rdi ; hSCManager
call OpenService
lea rdx, aVBoxNetLwf ; "VBoxNetLwf"
mov rcx, rdi ; hSCManager
call OpenService
mov ecx, 3E8h ; dwMilliseconds
call cs:Sleep
mov rdx, r14 ; lpServiceName
mov rcx, rdi ; hSCManager
call OpenService

```

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

```

loc_140001F5A:
lea rdx, aAssistantSys ; "\\assistant.sys"
mov rcx, rbx
call sub_1400020F4
mov r8d, [rsp+48h+arg_8]
xor r9d, r9d
and [rsp+48h+var_28], 0
mov rdx, rsi
mov rcx, rbx
call Createfile
cmp eax, [rsp+48h+arg_8]
jnz short loc_140001FBA

```

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 سیستم عامل، اکسپلویت می شود و از این طریق، درایور elrawdsk.sys به عنوان جزء اصلی در پاک کردن فضای ذخیره سازی، درون سیستم قربانی قرار می گیرد.

```

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

```

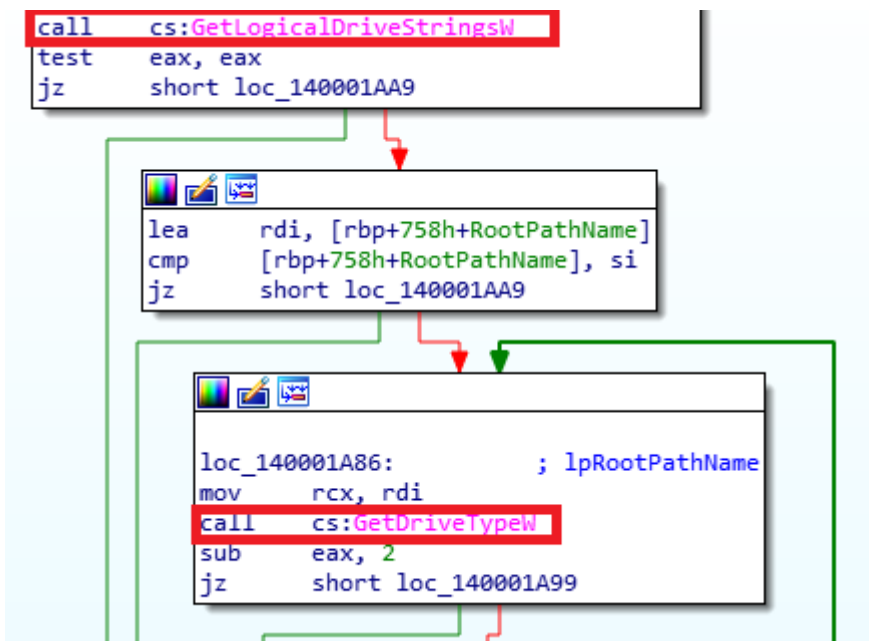
در ادامه فایل اجرایی با عنوان agent.exe همانند دو فایل دیگر، در مسیر قرارگیری فایل اولیه بدافزار، ایجاد می شود.

```

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 می شود.



همچنین فایل اجرایی agent.exe در محیط CMD ویندوز اجرا می شود.

```

lea   rcx, ApplicationName ; "C:\\windows\\system32\\cmd.exe"
mov   [rsp+0F0h+lpCurrentDirectory], rcx ; lpCurrentDirectory
mov   [rsp+0F0h+lpEnvironment], rdx ; lpEnvironment
mov   [rsp+0F0h+dwCreationFlags], 10h ; dwCreationFlags
mov   [rsp+0F0h+bInheritHandles], edx ; bInheritHandles
lea   rdx, [rbp+57h+CommandLine] ; lpCommandLine
movsd qword ptr [rbp+57h+CommandLine], xmm0
mov   byte ptr [rbp+57h+var_94+1], bl
call  cs:CreateProcessA
mov   rcx, [rbp+57h+ProcessInformation.hProcess] ; hObject
call  cs:CloseHandle
mov   rcx, [rbp+57h+ProcessInformation.hThread] ; hObject
call  cs:CloseHandle
mov   rbx, [rsp+0F0h+arg_0]
mov   eax, 1
add   rsp, 0F0h
pop   rbp
retn
CreateCMDProc endp

```

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

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 می کند.

```

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، در صورتی 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 پاک‌سازی 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

```

۶-۲ تحلیل ترافیک شبکه:

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