

بسمه تعالی

گزارش تحلیل فایل KMSAuto x64.exe

تهیه کننده :

ف. یعقوب خانی

شهریور 1403

مقدمه

برنامه KMSAuto x64.exe یک فعالساز ویندوز و محصولات مایکروسافت است که به صورت غیرقانونی اقدام به شبیه سازی key Management Server مایکروسافت نموده و به درخواست برنامه ها برای فعالسازی پاسخ می دهد. فعالسازهای غیرقانونی از روش های مختلفی استفاده می کنند، که رایج ترین آنها، نصب یک Key Management Service برای شبیه سازی رفتار KMS قانونی است. این سرویس جعلی روی پورت TCP 1688 که پورت پیش فرض KMS مایکروسافت است، به درخواست ها گوش می دهد، و در پاسخ پکت هایی مشابه KMS اصلی ارسال می نماید. پروتکل KMS از RPC برای ارتباط بین کلاینت و سرور استفاده می کند و دارای یک ساختار پیام خاص بوده و حاوی اطلاعات فعالسازی از جمله ID سیستم، مهر زمانی و کلید سرور KMS است. KMS جعلی داده های فعالسازی را درون تنظیمات سیستم Inject کرده و اقدام به اعمال تغییرات در برخی ساختارها و رفتار سرویس های مرتبط با فرآیند فعالسازی می نماید. این برنامه ها برای Persistent تنظیمات Activation از روش هایی مانند تغییر در رجیستری، ایجاد Task Scheduler یا نصب سرویس روی سیستم استفاده می کنند. همچنین از آنجایی که این برنامه ها غیر قانونی هستند، ممکن است آنتی ویروس و مکانیزم های امنیتی در عملکرد آنها اختلال ایجاد کنند، لذا معمولاً در KMS ها از تکنیک های به کار رفته در روت کیت ها برای مخفی سازی فعالیت های مشکوک استفاده می شود. در چنین حالتی اگر KMS جعلی با بدافزار یا شلکدی bind شده باشد، به دلیل تکنیک های Obfuscation به کار رفته در آن، احتمال اجرای موفقیت آمیز بدافزار و آلودگی سیستم افزایش می یابد.

مشخصات فایل

KMSAutox 64.exe	نام فایل
Portable Executable 64	معماری
E4F5236FA36221AF38CFB3E25312877B	MD5
E8FB4F8C8D78957955EAD90F383A1263 EDDB302B	SHA-1
4 روز	مدت زمان بررسی
Local Administrator	سطح دسترسی در تست ها

تحلیل عملکرد برنامه

در این بخش قصد داریم به ارائه ی شواهد و مستندات مربوط به عملکرد برنامه ی KMSAutox64.exe بپردازیم. نکات ارائه شده محدود به همین موارد نمی شود و ما تنها به ذکر شواهد مرتبط با هدف تحلیل بسنده می کنیم.

همان طور که در مقدمه ذکر شد، این برنامه به دلیل نیاز به مخفی سازی عملکرد داخلی خود از دید مکانیزم های امنیتی در چندین مرحله اقدام به پیاده سازی روش های Obfuscation می نماید. در بررسی اولیه مشاهده شد که این برنامه توسط برنامه ی UPX ، فشرده سازی و Pack شده است.

pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

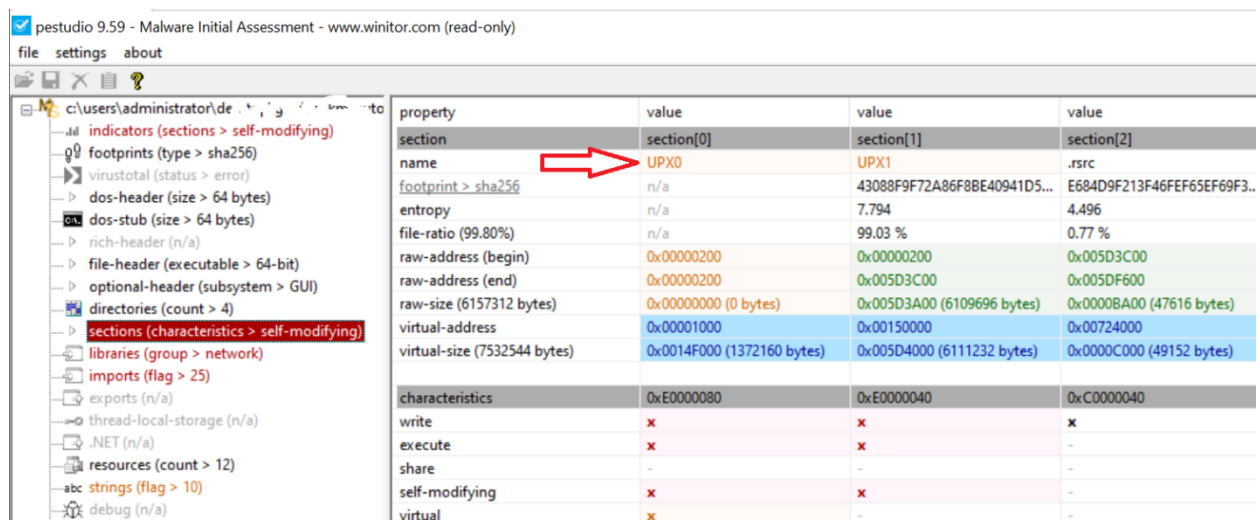
file settings about

file explorer: c:\users\administrator\desktop\KMSAutox64.exe

file properties:

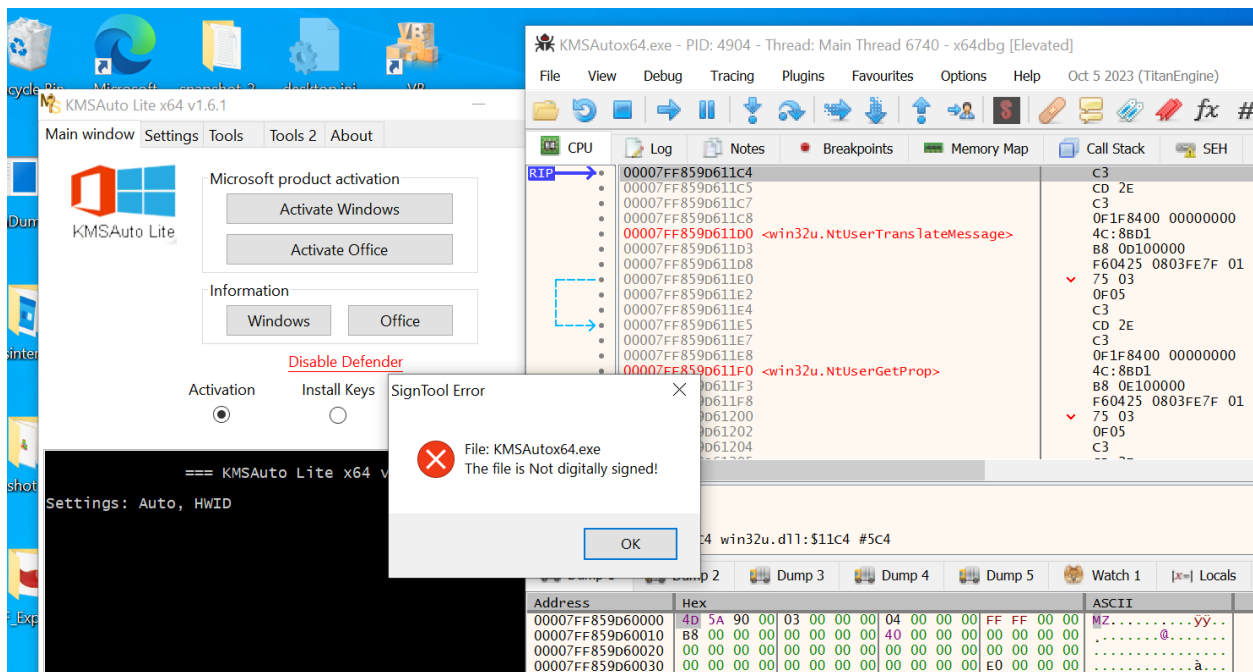
property	value
footprint > sha256	8D34BC0C8049751CABA7D4BC626B9F6ECD4826A3!
entropy	7.570
file-offset	0x00717400
size	11704 (bytes)
signature	unknown
first-bytes-hex	B8 2D 00 00 00 02 02 00 30 82 2D AB 06 09 2A 86 48 86
first-bytes-text	.. - 0 .. - * .. H - .. 0 .. - ..
file-ratio	0.16 %

شکل 1

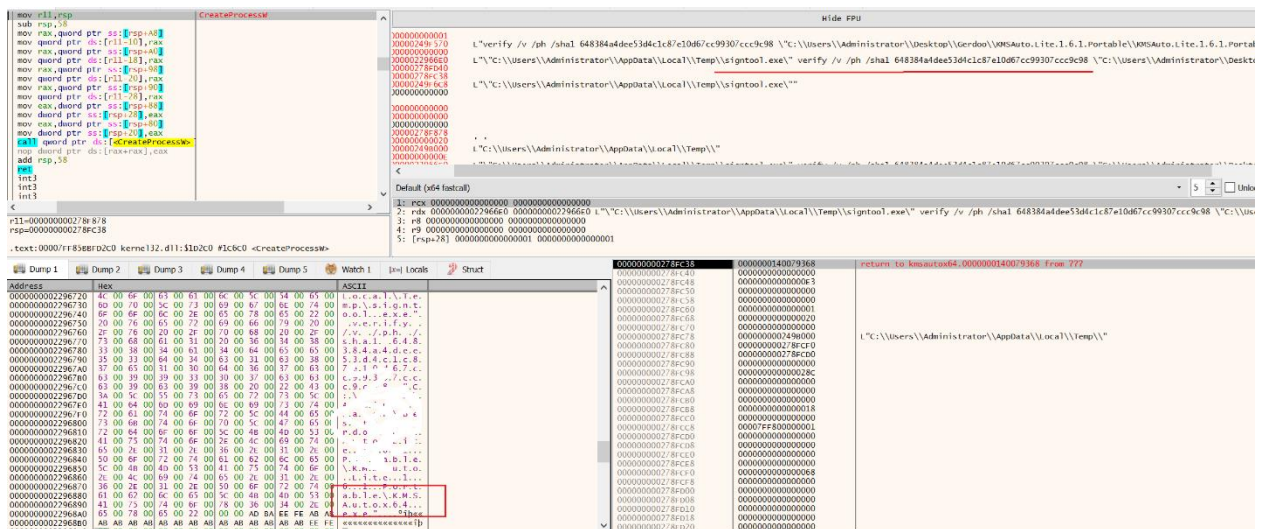


شکل 2

پس از Unpack نمودن برنامه که برای انجام موفقیت آمیز تحلیل استاتیک ضروری است، مشاهده شد که برنامه از روش های دیگری مانند Anti debugging و بررسی امضای دیجیتال برای جلوگیری از تحلیل دینامیک نیز استفاده کرده است. به عنوان مثال در شکل زیر مشاهده می نمایید، برنامه به دلیل Unpack شدن و تغییر Signature اجرا نمی شود.



در بررسی ها مشاهده شد، این برنامه با استفاده از دستور زیر Signature برنامه را با یک Hash از قبل تعیین شده مقایسه می نماید و در صورت مغایرت پیغام شکل قبل را نمایش می دهد.



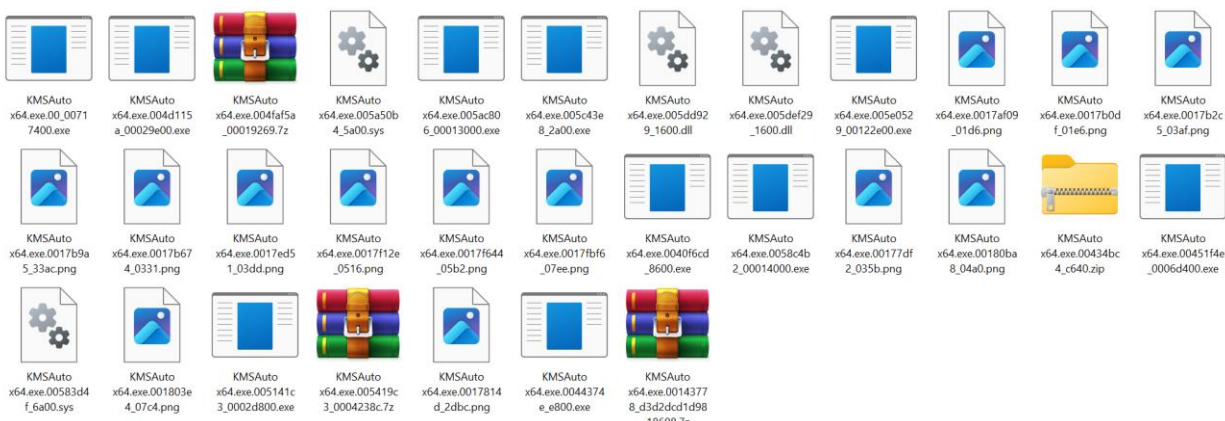
بر خلاف ظاهر نرم افزار که تنها یک فایل اجرایی است، این برنامه در هنگام تحلیل تعدادی اسکریپت، DLL و فایل های اجرایی دیگر از سورس خود استخراج کرده و در مسیر های مختلف روی سیستم کپی می کند. در ادامه چند مورد سرآیند PE که در محدوده ی data section پیدا شدند را مشاهده می کنید.

Offset	000102030405060708090a0b0c0d0e0f	Symbols
005d:d977	54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e	This program can
005d:d987	6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f	not be run in DO
005d:d997	53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00	S mode....\$.....
005d:d9a7	0000 50 45 0000 4c 01 04 00 bb 47 df 5f 0000	..PE..L....G..._
005d:d9b7	000000000000 e0 00 0f 23 0b 01 02 23 00 08#...#..
005d:d9c7	000000 0a 000000000000 68 15 00 00 00 10h.....
005d:d9d7	000000 20 00000000 fc 66 00 10 00 00 00 02f.....
005d:d9e7	0000 04 00000000000000 04 0000000000
005d:d9f7	000000 50 000000 04 0000 ac ec 00 00 03 00	...P.....
005d:da07	00000000 20 0000 10 00000000 10 00 00 10
005d:da17	000000000000 10 00000000 30 00 00 78 000...x.
005d:da27	000000 40 0000 08 05 0000000000000000	...@.....
005d:da37	00000000000000000000000000000000
005d:da47	00000000000000000000000000000000
005d:da57	00000000000000000000000000000000

Offset	000102030405060708090a0b0c0d0e0f	Symbols
005d:ef77	54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e	This program can
005d:ef87	6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f	not be run in DO
005d:ef97	53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00	S mode....\$.....
005d:efa7	0000 50 45 0000 64 86 04 00 76 47 df 5f 0000	..PE..d...vG..._
005d:efb7	000000000000 f0 00 2f 22 0b 02 02 23 00 08/"...#..
005d:efc7	000000 0a 000000000000 f6 14 00 00 00 10
005d:efd7	00000000 dc 66 000000000000 10 00 00 00 02f.....
005d:efe7	0000 04 0000000000000000 05 00 02 00 00 00
005d:eff7	000000 50 000000 04 0000 74 ae 00 00 03 00	...P.....t.....
005d:f007	00000000 20 000000000000 10 00 00 00 00

Offset	000102030405060708090a0b0c0d0e0f	Symbols
005e:0577	54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e	This program can
005e:0587	6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f	not be run in DO
005e:0597	53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00	S mode....\$.....
005e:05a7	00 00 50 45 00 00 4c 01 03 00 27 67 63 61 00 00	..PE..L...'gca..
005e:05b7	00 00 00 00 00 00 e0 00 0f 01 0b 01 02 32 00 b02..
005e:05c7	11 00 00 80 00 00 00 30 11 00 a0 ea 22 00 00 400...."..@
005e:05d7	11 00 00 f0 22 00 00 00 40 00 00 10 00 00 00 02"....@.....
005e:05e7	00 00 04 00 00 00 00 00 00 00 00 04 00 00 00 00
005e:05f7	00 00 00 70 23 00 00 10 00 00 66 fa 12 00 02 00	...p#.....f.....
005e:0607	00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10
005e:0617	00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00
005e:0627	00 00 38 67 23 00 10 05 00 00 00 f0 22 00 38 77	..8g#.....".8w
005e:0637	00 00 00 00 00 00 00 00 00 00 00 00 2e 12 00 c8 2d-
005e:0647	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

در فرآیند جستجو و استخراج فایل های embed شده ، موارد زیر به دست آمد.



همچنین در هنگام دیباگ با استفاده از x64dbg ، در مراحل مختلف به فایل ها و اسکریپت هایی برخورد کردیم، که ممکن است با برخی فایل های کشف شده در مرحله ی قبل همپوشانی داشته یا فایل جدید باشند. به عنوان مثال فایل های زیر :

FileHomeShareView

This PC

Local Disk (C:)

Users

Administrator

AppData

Local

Temp

BIN

Quick access

Desktop

Downloads

Documents

Pictures

dump

Name	Date modified	Type	Size
gatherosstate.exe	8/26/2024 12:44 AM	Application	
GenuineTicket.xml	8/26/2024 12:45 AM	XML Document	
slc.dll	8/26/2024 12:44 AM	Application extension	

ShareViewApplication Tools

This PC

Local Disk (C:)

Users

Administrator

AppData

Local

Temp

ss

ds

its

-1.1.1h_wir

Name	Date modified	Type	Size
BIN	8/26/2024 12:51 AM	File folder	
Low	8/17/2024 9:10 PM	File folder	
msdtadmin	8/26/2024 12:37 AM	File folder	
vmware-Administrator	8/17/2024 9:29 PM	File folder	
18e190413af045db88dfbd29609eb877.db	8/17/2024 9:27 PM	Data Base File	2
18e190413af045db88dfbd29609eb877.db.sess...	8/17/2024 9:27 PM	SESSION64 File	6
aria-debug-8040.log	8/25/2024 11:06 PM	Text Document	
BITA64E.tmp	8/24/2024 12:24 AM	TMP File	
dd_vcredist_amd64_20240817212705.log	8/17/2024 9:27 PM	Text Document	1
dd_vcredist_x86_20240817212704.log	8/17/2024 9:27 PM	Text Document	1
msedge_installer.log	8/17/2024 9:10 PM	Text Document	
OfficeVerifier.txt	8/26/2024 12:18 AM	Text Document	
offline	8/17/2024 9:27 PM	File	3
offline.session64	8/17/2024 9:27 PM	SESSION64 File	6
slmgr.vbs	12/7/2019 1:08 AM	VBScript Script File	14
StructuredQuery.log	8/20/2024 11:50 PM	Text Document	3
tem1F0D.tmp	8/25/2024 11:09 PM	TMP File	
tem2C6F.tmp	8/25/2024 11:22 PM	TMP File	

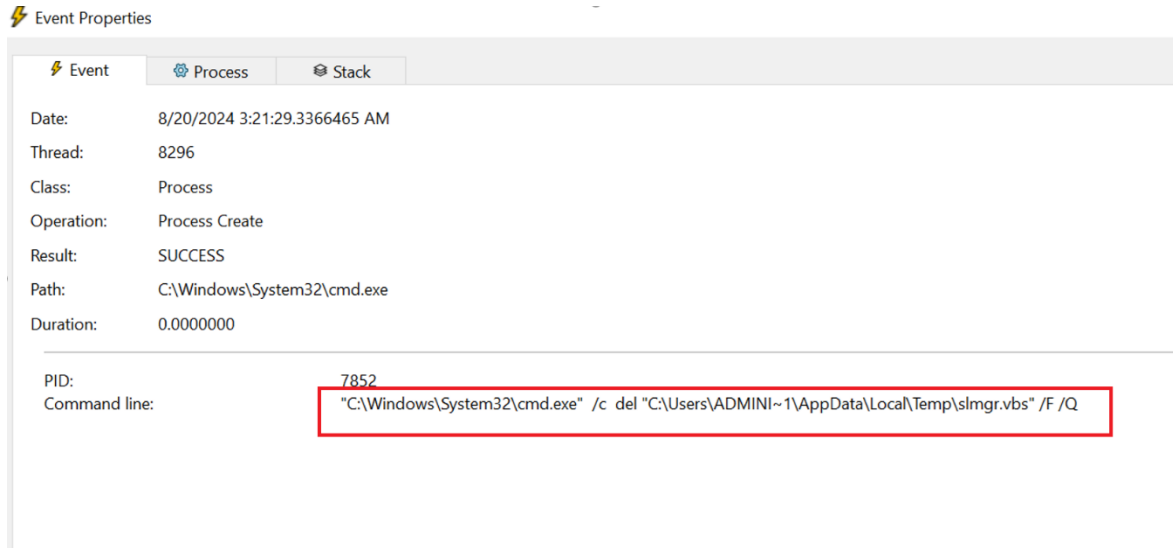
به صورت عادی در فرآیند تحلیل فایل، کلیه فایل های اجرایی، DLL و اسکریپت های استخراج شده نیاز به بررسی جداگانه دارند. اما با توجه به هدف ما از این تحلیل و با عنایت به اینکه تنها یک مورد رفتار مخرب برای تصمیم گیری نهایی (که استفاده نکردن از آن در سطح سازمان است) کافیهست، لذا سایر فایل ها بررسی نگردید.

در ادامه مشاهده شد که این فایل ها بعد از اتمام فرآیند فعالسازی به طور کامل از روی سیستم پاک می شوند، بطوریکه کاربر عادی متوجه وجود آنها نمی شود. به عنوان مثال این برنامه با استفاده از Process زیر اسکریپت slmgr.vbs را اجرا می نماید.

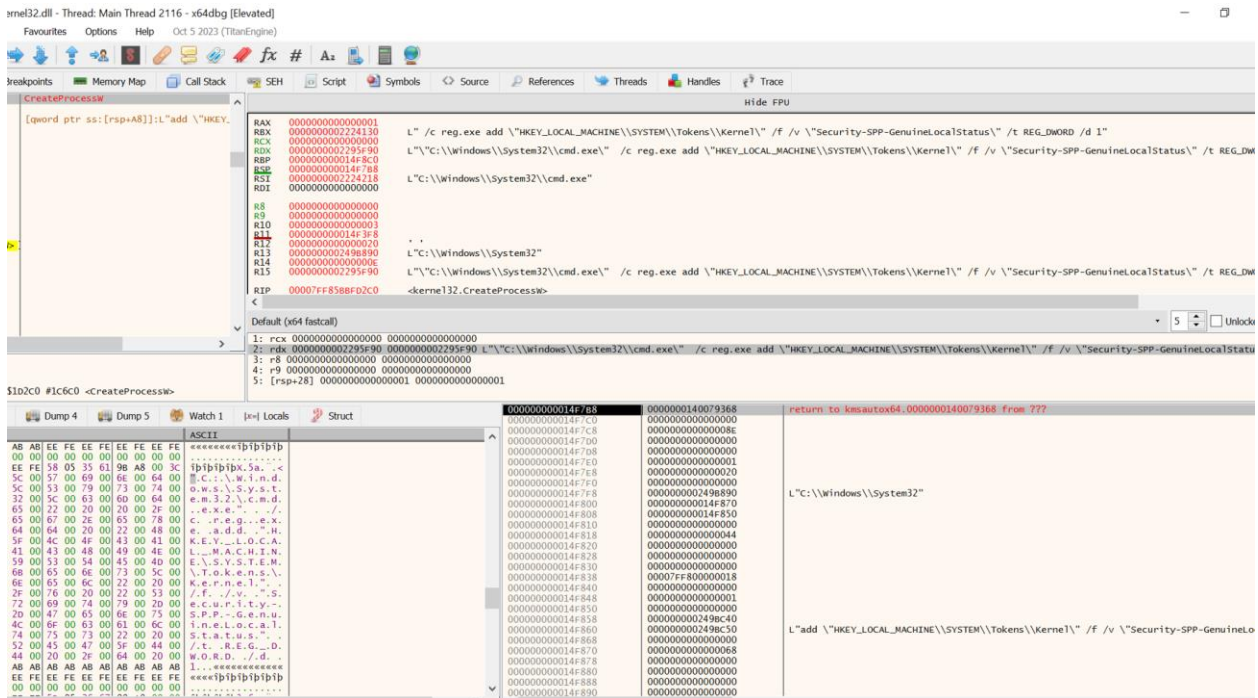
The screenshot displays a debugger interface with the following components:

- Breakpoints:** Shows a breakpoint set on the `CreateProcess` function.
- Memory Map:** Displays the memory layout of the process.
- Call Stack:** Shows the sequence of function calls.
- SEH:** Structured Exception Handling records.
- Script:** Shows the script being executed, which is a Windows command prompt script using `cscript` to run `slmgr.vbs`.
- Symbols:** Shows the loaded symbols for the process.
- Source:** Shows the source code of the script.
- References:** Shows references to the script.
- Threads:** Shows the threads of the process.
- Handles:** Shows the handles held by the process.
- Trace:** Shows the trace of the process.
- Default (x64 fastcall):** Shows the default fastcall convention for the `CreateProcess` function.
- Registers:** Shows the values of the registers, including `RAX`, `RDX`, `RBP`, `RSP`, `R10`, `R11`, `R12`, `R13`, `R14`, `R15`, and `RIP`.
- Disassembly:** Shows the assembly instructions being executed, including a `mov eax, ebx` instruction.
- Comments:** Shows comments for the assembly instructions, including `return to kmautox64.0000000140079368 from 777` and `return to ntdll.RtlAllocateHeap+AND from ntdll.RtlAllocateHeap+27C0`.

و سپس با دستور زیر این اسکریپت را از روی سیستم پاک می کند.



این برنامه برای Persistent سازی تنظیمات Activation اقدام به اعمال تغییراتی قبل و بعد از فرآیند فعالسازی می نماید. در شکل زیر یک نمونه از این تغییرات را مشاهده می کنید.



در trace اعمال تغییرات در رجیستری، یک کوئری مشاهده شد که وضعیت فعال یا غیر فعال بودن Defender را بررسی می نماید.

The screenshot shows a debugger window with the following content:

Trace:

```

CreateProcessW
RAX 0000000000000001
RBX 0000000002224130 L"query \"HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\" /v DisableAntivirus"
RCX 0000000000000000 L"C:\\Windows\\System32\\reg.exe" query \"HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\" /v DisableAntivirus"
RDX 0000000002A92C20
RBP 00000000014FCAD0
RSP 00000000014FB998
RSI 00000000022241E8 L"C:\\Windows\\System32\\reg.exe"
RDI 0000000000000000
R8 0000000000000000
R9 0000000000000000
R10 0000000000000000
R11 00000000014F7D8
R12 0000000000000020
R13 0000000000000000
R14 000000000000000E
R15 0000000000000000
Default (x64 fastcall)
1: rcx 0000000000000000 0000000000000000
2: rdx 0000000002A92C20 0000000002A92C20 L"C:\\Windows\\System32\\reg.exe" query \"HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\" /v DisableAntivirus"
3: r8 0000000000000000 0000000000000000
4: r9 0000000000000000 0000000000000000
5: [rsp+28] DC4808A400000001 DC4808A400000001

```

Memory Dump:

Address	Hex	ASCII
00000000014FB998	00000000014FB998	
00000000014FB9A0	00000000014FB9A0	
00000000014FB9A8	00000000014FB9A8	
00000000014FB9B0	00000000014FB9B0	
00000000014FB9B8	00000000014FB9B8	
00000000014FB9C0	00000000014FB9C0	
00000000014FB9C8	00000000014FB9C8	
00000000014FB9D0	00000000014FB9D0	
00000000014FB9D8	00000000014FB9D8	
00000000014FB9E0	00000000014FB9E0	
00000000014FB9E8	00000000014FB9E8	
00000000014FB9F0	00000000014FB9F0	
00000000014FB9F8	00000000014FB9F8	
00000000014FC000	00000000014FC000	
00000000014FC008	00000000014FC008	
00000000014FC010	00000000014FC010	
00000000014FC018	00000000014FC018	

Watch:

Variable	Value
00000000014FB998	00000000014FB998
00000000014FB9A0	00000000014FB9A0
00000000014FB9A8	00000000014FB9A8
00000000014FB9B0	00000000014FB9B0
00000000014FB9B8	00000000014FB9B8
00000000014FB9C0	00000000014FB9C0
00000000014FB9C8	00000000014FB9C8
00000000014FB9D0	00000000014FB9D0
00000000014FB9D8	00000000014FB9D8
00000000014FB9E0	00000000014FB9E0
00000000014FB9E8	00000000014FB9E8
00000000014FB9F0	00000000014FB9F0
00000000014FB9F8	00000000014FB9F8
00000000014FC000	00000000014FC000
00000000014FC008	00000000014FC008
00000000014FC010	00000000014FC010
00000000014FC018	00000000014FC018

Struct:

Variable	Value
00000000014FB998	00000000014FB998
00000000014FB9A0	00000000014FB9A0
00000000014FB9A8	00000000014FB9A8
00000000014FB9B0	00000000014FB9B0
00000000014FB9B8	00000000014FB9B8
00000000014FB9C0	00000000014FB9C0
00000000014FB9C8	00000000014FB9C8
00000000014FB9D0	00000000014FB9D0
00000000014FB9D8	00000000014FB9D8
00000000014FB9E0	00000000014FB9E0
00000000014FB9E8	00000000014FB9E8
00000000014FB9F0	00000000014FB9F0
00000000014FB9F8	00000000014FB9F8
00000000014FC000	00000000014FC000
00000000014FC008	00000000014FC008
00000000014FC010	00000000014FC010
00000000014FC018	00000000014FC018

ASCII:

Address	Hex	ASCII
00000000014FB998	00000000014FB998	
00000000014FB9A0	00000000014FB9A0	
00000000014FB9A8	00000000014FB9A8	
00000000014FB9B0	00000000014FB9B0	
00000000014FB9B8	00000000014FB9B8	
00000000014FB9C0	00000000014FB9C0	
00000000014FB9C8	00000000014FB9C8	
00000000014FB9D0	00000000014FB9D0	
00000000014FB9D8	00000000014FB9D8	
00000000014FB9E0	00000000014FB9E0	
00000000014FB9E8	00000000014FB9E8	
00000000014FB9F0	00000000014FB9F0	
00000000014FB9F8	00000000014FB9F8	
00000000014FC000	00000000014FC000	
00000000014FC008	00000000014FC008	
00000000014FC010	00000000014FC010	
00000000014FC018	00000000014FC018	

این موضوع احتمال اعمال تغییرات در تنظیمات آنتی ویروس توسط نرم افزار KMS را افزایش داد. از آنجایی دستکاری آنتی ویروس به هر دلیلی موجب بالا رفتن ریسک ها و تهدیدات امنیتی می شود، بررسی های بیشتر در این زمینه انجام گرفت و مشاهده شد یک پوشه ی Exclude توسط KMS در تنظیمات آنتی ویروس ساخته می شود.

The screenshot displays the Immunity Debugger interface. The top pane shows assembly code for a function that adds exclusion paths to the Windows Defender PATH MSFT_MpPreference. The code includes instructions for loading registers, pushing arguments, and calling the `AddExclusionPath` function. The bottom pane shows a memory watch at address `00000000268FC48`, displaying the ASCII string `L"C:\Windows\System32\"`.

وجود پوشه ی Exclude روی سیستم ، هر چند برای KMS ضروری است، اما یک آسیب پذیری جدی روی سیستم به وجود می آورد، به طوری که نفوذ گر می تواند فایل مخرب خود را در این مسیر کپی کرده و بدون بررسی توسط آنتی ویروس آن را اجرا نماید.

در ادامه مشاهده شد این برنامه با ایجاد یک Task در Task Scheduler، فعالیت های فعالسازی خود را Persistent می کند.

The screenshot shows a debugger window with the following assembly code:

```

RAX 0000000000000001 L" /c schtasks.exe /end /TN KMSAuto"
RDX 0000000023E6C70 L"C:\\Windows\\System32\\cmd.exe\" /c schtasks.exe /end /TN KMSAuto"
RBP 0000000000000000 L"C:\\Windows\\System32\\cmd.exe"
RSP 0000000000000000
RDI 0000000000000000
R8 0000000000000000
R9 0000000000000000
R10 0000000000000000
R11 0000000029BDF30
R12 0000000000000020
R13 0000000000000000
R14 0000000000000000 L"C:\\Windows\\System32\\cmd.exe\" /c schtasks.exe /end /TN KMSAuto"
R15 0000000029BEF20

```

The instruction pointer (RIP) is 0000000000000000. The instruction is:

```

1: rdx 0000000029BEF20 0000000029BEF20 L"C:\\Windows\\System32\\cmd.exe\" /c schtasks.exe /end /TN KMSAuto"
2: rdx 0000000029BEF20 0000000029BEF20 L"C:\\Windows\\System32\\cmd.exe\" /c schtasks.exe /end /TN KMSAuto"
3: r8 0000000000000000 0000000000000000
4: r9 0000000000000000 0000000000000000
5: [rsp+28] 0000000000000001 0000000000000001

```

The register values are:

```

RAX 0000000000000001
RDX 0000000023E6C70
RBP 0000000000000000
RSP 0000000000000000
RDI 0000000000000000
R8 0000000000000000
R9 0000000000000000
R10 0000000000000000
R11 0000000029BDF30
R12 0000000000000020
R13 0000000000000000
R14 0000000000000000
R15 0000000029BEF20

```

The instruction pointer (RIP) is 0000000000000000. The instruction is:

```

1: rdx 0000000029BEF20 0000000029BEF20 L"C:\\Windows\\System32\\cmd.exe\" /c schtasks.exe /end /TN KMSAuto"
2: rdx 0000000029BEF20 0000000029BEF20 L"C:\\Windows\\System32\\cmd.exe\" /c schtasks.exe /end /TN KMSAuto"
3: r8 0000000000000000 0000000000000000
4: r9 0000000000000000 0000000000000000
5: [rsp+28] 0000000000000001 0000000000000001

```

The register values are:

```

RAX 0000000000000001
RDX 0000000023E6C70
RBP 0000000000000000
RSP 0000000000000000
RDI 0000000000000000
R8 0000000000000000
R9 0000000000000000
R10 0000000000000000
R11 0000000029BDF30
R12 0000000000000020
R13 0000000000000000
R14 0000000000000000
R15 0000000029BEF20

```

Task Scheduler

File Action View Help

Task Scheduler (Local)

Task Scheduler Library

Microsoft

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
KMSAuto	Ready	At 10:00 AM every 10 days - After triggered, repeat every 10.00:00:00 indefinitely.	8/23/2024 10:00:00 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)
Microsoft...	Running	Multiple triggers defined	8/21/2024 12:55:10 AM	8/20/2024 12:55:11 AM	The operator or administrator has refused the request. (0x8004EE39)
Microsoft...	Ready	At 12:25 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	8/20/2024 2:25:10 AM	8/20/2024 1:39:21 AM	The operation completed successfully. (0x00000000)
OneDrive S...	Ready	At 12:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	8/21/2024 12:04:10 AM	8/17/2024 8:55:21 PM	(0x8004EE39)
OneDrive S...	Ready	At 9:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	8/20/2024 11:18:13 PM	8/19/2024 11:39:21 PM	(0x8004EE39)

لازم به ذکر است، وجود Task Scheduler غیر ضروری روی سیستم تهدیداتی با خود به همراه دارد، و می تواند به نفوذگر برای اجرا کد مخرب یا حملات ارتقای سطح دسترسی کمک کند.

نتیجه گیری

با توجه به ماهیت اصلی نرم افزار KMS که به صورت غیرقانونی اقدام به تغییر تنظیمات مربوط به فعالسازی و لایسنس نرم افزارهای مایکروسافتی روی سیستم می نماید، طبیعی است برخی رفتارها از جمله نصب سرویس، تغییر در رجیستری، نوشتن فایل روی دیسک و استفاده از تکنیک های مخفی سازی در این برنامه به چشم بخورد. با این حال بعد از بررسی ها و تحلیل های صورت گرفته مشاهده شد، تغییراتی که این برنامه روی سیستم ایجاد می کند، هر چند با اهداف خرابکارانه (به جز فعالسازی غیرقانونی) نیست، اما باعث بروز آسیب پذیری و تهدیدات دیگری می شود که می تواند امنیت کل سیستم را به مخاطره بیاندازد. به عنوان مثال افزودن مسیر Exclude در آنتی ویروس، موجب می شود فرد نفوذگر این مسیر برای کپی و اجرای فایل مخرب خود استفاده نماید. وجود Task Scheduler غیر ضروری، علاوه بر اینکه از روش های رایج در حملات ارتقای سطح دسترسی است، از روش های رایج Persistent بوده و می تواند برای اجرای کد مخرب و بدافزارها نیز مورد استفاده قرار گیرد. علاوه بر اینها استفاده از توابعی مانند OpenProcessToken از نشانه های تکنیک Impersonation است که در حملات ارتقای سطح دسترسی به کار می رود، و این موضوع نیز در تحلیل این فایل جای تامل و نیاز به بررسی بیشتر دارد. همچنین دیدیم که نرم افزار KMSAutox64.exe تعدادی فایل اجرایی و DLL روی سیستم کپی می کند. برخی از این فایل ها ظاهرا شناخته شده هستند مانند SignTool.exe یا slmgr.vbs. و تعدادی از آنها دارای نام و نشان مشخص و شناخته شده ای نیستند. از آنجایی که همه ی این فایل ها به صورت مجزا تحت بررسی کامل قرار نگرفته اند (و انجام این کار زمانبر است) نمی توان با قاطعیت اذعان داشت که بدافزار یا شلکدی به این نرم افزار bind نشده است. با توجه به موارد فوق پیشنهاد می شود روش هایی با امنیت بالاتر، مانند استفاده از WSUS و لایسنس معتبر برای فعالسازی محصولات مایکروسافتی، جایگزین استفاده از نرم افزار KMSAutox64.exe گردد.