Song Yang (sy540)

Xin Yang (xy213)

Zhuohang Li (zl299)

Malware Review

Monero Mining Malware embeded in KMSpico v10.2.2

Introduction

KMSpico is a well-known Windows operating system activation tool, but the latest version has been embedded with a Monero miner in some unofficial sites.

Installing KMSpico would extract four files under the directory "C:\Program Files\KMSPico 10.2.2 Final", a batch file named INSTALL_KMS.bat would run the activation program and the win32.exe file. Win32.exe is exactly the Monero mining malware, which utilizes CPU resources for heavy hash computing tasks.

Comparing with the most famous Bitcoin, the speed of mining Monero using CPU is still acceptable for some high-end home PCs, also the Monero mining is completely anonymous thanks to the algorithms behind, which raises the interests of many malware developers.

Reverse Engineering

- **Static Analysis**

Uploading the win32.exe to VirusTotal, 57/67 engines report it as a malware, tags appeared mostly are shown as Trojan, CoinMiner, MoneroMiner, etc.. At the behavior page, we can see that under the Processes Created section, a fake svchost.exe process is created with the arguments standing for a Monero mining pool and Monero wallet email address.

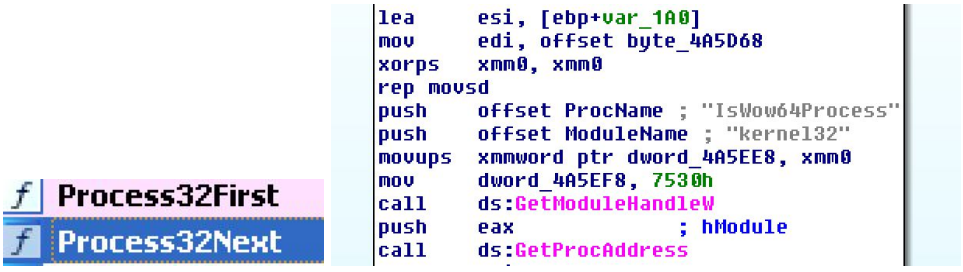
Processes Created

C:\WINDOWS\System32\svchost.exe" -a cryptonight -o stratum+tcp://xmr.pool.minergate.com:45560 -u zcashminer@gmx.com -p x -t 1"

From DependencyWalker, PEID, and PEView, we couldn't find much significant information. But when we run strings command, lots of hints infer this is a miner malware. As can be seen from the screenshots below, "50%CPU" and "100%CPU" infer the CPU usage. Such an abnormally high rate definitely links it to a miner tool considering this is an activation tool. Also, we can see there are words like "TASKMGR" and "taskmgr.exe", which might mean that this malware can detect the existence of task manager, and take some operations accordingly. Most of the rest parts are gibberish.

```
%`@@
0123456789
Error
ntdll.dll
LdrGetProcedureAddress
NtOpenSection
NtMapViewOfSection
IsWow64Process
0125789244697858
a341abf4064bb30b8ddc
33accef23e1993dfdXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
JRSF_UP\QFv^Z@
wBaVA@iwL
xnFLckt[|P}y@WV|N`zrXKg\
N]\tSV`N
J^u_eiQuvVgo
TEoiw__
G~wBaVA@iwL
xnFLckt[|P}y@WV|N`zrXKg\
N]\tSV`N
J^u_eiQuvVgo
0125789244697858
GWV^
Y_WRJRYDT
QSG\
]^\PEWQSG\
]^\PEWQSG\
]^\PEWQSG\
]^\PEWQSG\
TRUE
TRUE
TASKMGR
TASKMGR
50%CPU
50%CPU
100%CPU
100%CPU
0125789244697858
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
0125789244697858
taskmgr.exe
NtClose
```

From IDA Pro, we can find the functions Process32First, Process32Next and Windows Version related operations e.g. “IsWow64Process”, which determines the current version of victim machine and take operations differently.



From the screenshots below, we can see the gibberish looking string and a number string, which might infer to an encrypted Monero wallet and the encryption password.

```
.text:004023D3    push    100h
.text:004023D8    push    0
.text:004023DA    push    offset byte_4A5D68
.text:004023DF    call    sub_401320
.text:004023E4    push    13h
.text:004023E9    push    offset aJrsf_upQfvZ@_ ; "JRSF_UP\\QFv^Z@\x1B[_\\"
.text:004023EE    push    offset byte_4A5D68
.text:004023F3    call    sub_401110
.text:004023F8    push    12h
.text:004023FD    push    offset byte_4A5D68
.text:00402402    push    10h
.text:00402404    push    offset a01257892446978 ; "0125789244697858"
.text:00402409    call    sub_4013A0
.text:0040240F    push    12h
```

This malware will detect the windows task manager in a loop and pause the miner if user aware something is wrong. A report of current CPU usage when it comes to 50% and 100% can also be found.

```
.text:0040247B                 cmp     eax, 9B8809D5h
.text:00402480                 jnz     loc_402735
.text:00402486                 push    offset aTrue    ; "TRUE"
.text:0040248B                 push    offset aTrue_0  ; "TRUE"
.text:00402490                 call    sub_4011E0
.text:00402495                 mov     ecx, dword_4A5EE8
.text:0040249B                 test    eax, eax
.text:0040249D                 mov     esi, 1
.text:004024A2                 cmovz   ecx, esi
.text:004024A5                 push    offset aTaskmgr ; "TASKMGR"
.text:004024AA                 push    offset aTaskmgr_0 ; "TASKMGR"
.text:004024AF                 mov     dword_4A5EE8, ecx
.text:004024B5                 call    sub_4011E0
.text:004024BA                 mov     ecx, dword_4A5EEC
.text:004024C0                 test    eax, eax
.text:004024C2                 push    offset a50Cpu   ; "50%CPU"
.text:004024C7                 cmovz   ecx, esi
.text:004024CA                 push    offset a50Cpu_0 ; "50%CPU"
.text:004024CF                 mov     dword_4A5EEC, ecx
.text:004024D5                 call    sub_4011E0
.text:004024DA                 mov     ecx, dword_4A5EF0
.text:004024E0                 test    eax, eax
.text:004024E2                 push    offset a100Cpu  ; "100%CPU"
.text:004024E7                 cmovz   ecx, esi
.text:004024EA                 push    offset a100Cpu_0 ; "100%CPU"
.text:004024EF                 mov     dword_4A5EF0, ecx
.text:004024F5                 call    sub_4011E0
.text:004024FA                 mov     ecx, dword_4A5EF4
```

We can also find the registry operations to the RunOnce record, which can make this malware auto launching each time windows is started.

```
.rdata:00404890 ; CHAR aShgetknownfold[]
.rdata:00404890 aShgetknownfold db 'SHGetKnownFolderPath',0 ; DATA XREF: sub_403880+16↑o
.rdata:004048A5                 align 4
.rdata:004048A8 ; CHAR aShgetfolderpat[]
.rdata:004048A8 aShgetfolderpat db 'SHGetFolderPathW',0 ; DATA XREF: sub_403880:loc_4038E8↑o
.rdata:004048B9                 align 4
.rdata:004048BC ; CHAR aWin32_exe[]
.rdata:004048BC aWin32_exe      db 'win32.exe',0        ; DATA XREF: sub_4036B0+27↑o
.rdata:004048C6 aXxxxxxxxxxxx_1 db 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX',0
.rdata:004048EA                 align 4
.rdata:004048EC asc_4048EC      db '\',0                ; DATA XREF: sub_4036B0+77↑o
.rdata:004048EE                 align 10h
.rdata:004048F0 aSoftwareMicr_0:                        ; DATA XREF: StartAddress+A8↑o
.rdata:004048F0                 unicode 0, <\Software\Microsoft\Windows\CurrentVersion\RunOnce>,0
.rdata:00404956                 align 4
.rdata:00404958 aSoftwareMicr_1:                        ; DATA XREF: StartAddress+1CC↑o
.rdata:00404958                 unicode 0, <\Software\Microsoft\Windows\CurrentVersion\RunOnce>,0
.rdata:004049BE                 align 10h
.rdata:004049C0 ; CHAR MultiByteStr[]
.rdata:004049C0 MultiByteStr    db 'kAUNCUkNWH',0       ; DATA XREF: sub_4036B0+C↑o
.rdata:004049CB aXtalxxxxx      db 'XTALXXXXX',0
.rdata:004049D5                 align 4
.rdata:004049D8 ; CHAR aJxudlnugma[]
.rdata:004049D8 aJxudlnugma     db 'jXuDLnugma',0       ; DATA XREF: sub_4036B0+39↑o
.rdata:004049E3 aKirbxxxxx      db 'kiRBXXXXX',0
.rdata:004049ED                 align 10h
.rdata:004049F0 asc_4049F0      db '\',0                ; DATA XREF: sub_4036B0+BF↑o
```

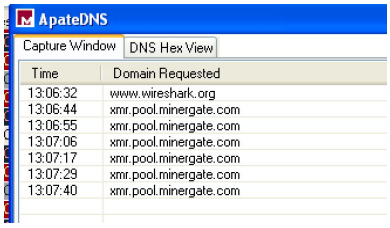
```
StartAddress
start
sub_401000
sub_401020
sub_4010B0
sub_4010D0
sub_401110
sub_401140
sub_401170
sub_4011E0
SoftwareMicr_0:                         ; DATA XREF: StartAddress+A8↑o
        unicode 0, <\Software\Microsoft\Windows\CurrentVersion\RunOnce>,0
```

```
lea     eax, [ebp+var_E3C]
push    offset aRegistryUser ; "\\Registry\\User\\"
push    eax
call    sub_4012D0
lea     eax, [ebp+var_63C]
push    eax
lea     eax, [ebp+var_E3C]
push    eax
call    sub_401280
lea     eax, [ebp+var_E3C]
push    offset aSoftwareMicr_0 ; "\\Software\\Microsoft\\Windows\\Current"...
push    eax
lea     eax, [ebp+var_E3C]
```

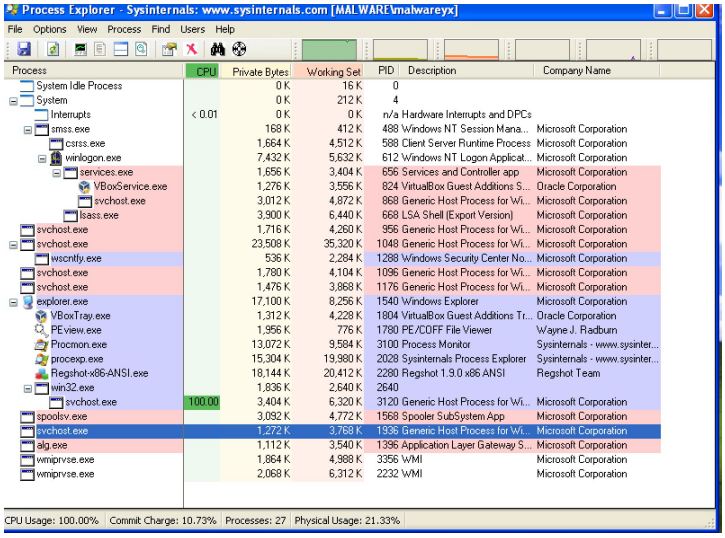
- **Dynamic Analysis**

First, we set the ApateDNS and opened Wireshark, and prepare the Regshot, process monitor and process explorer.

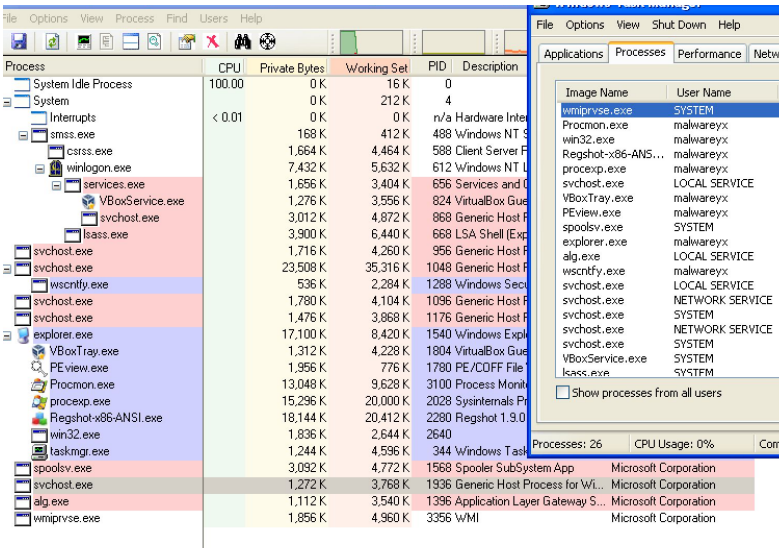
Once launched win32.exe, we can see this malware tries to connect with xmr.pool.minergate.com. As known to all, “xmr” refers to Monero and this is a Monero mining pool address. But from Wireshark we couldn’t get any valuable information.

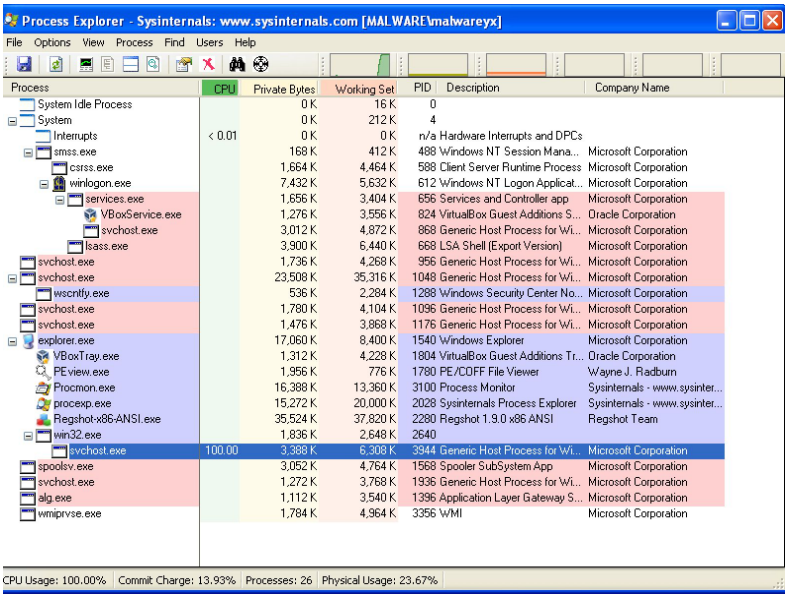


In Process Explorer, we can see there's a new process under the win32.exe and takes 100% of CPU, so this is the Monero mining process.



We opened the Windows task manager to see if this malware will react to taskmgr.exe. And from the below screenshot, the CPU rate falls to a low level after task manager is launched, meanwhile the svchost.exe is killed. Then we closed the task manager, the svchost.exe was created again and took full advantage of the CPU resources.





From the Regshot comparison, we can see this malware added a record in the “RunOnce” to achieve auto-running when Windows is started. And the directory is under “C:\Documents and Settings\[User]\Local Settings\Application Data\kAUNCUkNWH\win32.exe”, which means this malware copied itself to another directory to prevent user delete the installation files. The massive registry operations and file operations from the Process Monitor also proves this.

```
1-484763869-2111687655-1060284298-1003\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:
1-484763869-2111687655-1060284298-1003\Software\Microsoft\windows\CurrentVersion\RunOnce\jXuDLnugma: ""C:\DOCUME~1\MALWAR~1\LOCALS~1\APPLIC~1\KAUNCU~1\win32.exe"
```

Intrusion detection

If infected by this malware, users would feel the heat caused by massive CPU computing, and by launching Process Monitor (not task manager), users can see an svchost.exe under the win32.exe that takes 100% of CPU usage. Meanwhile, under the directory “C:\Documents and Settings\[User]\Local Settings\Application Data\kAUNCUkNWH\” will exist a

win32.exe file, as well under the “C:\Program Files\KMSPico 10.2.2 Final\”. There will also be a win32.exe registered inside the “\Microsoft\Windows\CurrentVersion\RunOnce”.

Intrusion recovery

Process Monitor can find the win32.exe and the svchost.exe processes which consume 100% CPU, killing the processes should stop the malware from mining. Then users can delete the win32.exe from the two directories mentioned above, and also remember to delete the KMSpico related directories completely, then restart the computer and it shall be fine.