FickerStealer

Technical Analysis Report

Contents

Introduction

FickerStealer is a infostealer threat offered as a MaaS (Malware-as-a-Service) on underground hacker forums. FickerStealer is distributed by various phishing methods.
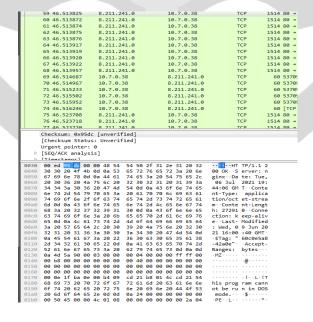Infected computers of this malware;

- Credentials saved in web browsers,
- Desktop messaging clients,
- To FTP clients,
- Blockchain wallets,
- It provides access to computer documents.

Preview

The FickerStealer malware in the examined version continued to spread as a DLL with phishing methods. The malicious file was originally named "file.dll". As a result of the analysis, it has been determined that this file acts as a loader to realize Stage 1.

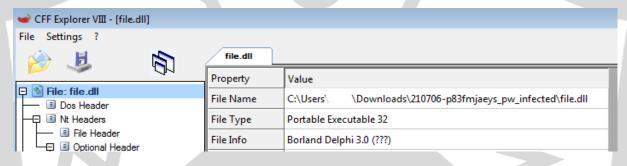| File Name:	file.dll
MD5	9b59d4744ff1de8b338eeb2b85748cf2
SHA1	f3306e866bc9992c2268f204f55e88f89833a25d
SHA256	fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4

It has been observed that the file.dll malware downloads a file titled MZ when network traffic is monitored.

file.dll ANALYSIS

When file.dll is examined statically, it is seen that it is a 32-bit executable file.

Dynamically loaded DLLs:

GDI32.dll	USP10.dll
MFC42.dll	msvcrt.dll
VERSION.dll	ADVAPI32.dll
MSCTF.dll	SHLWAPI.dll
OLEAUT32.dll	IMM32.dll

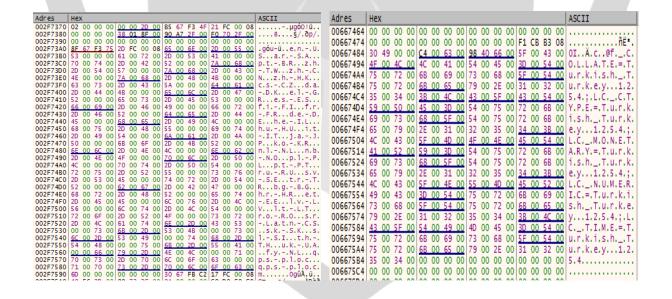In general, when the behavior of file.dll is examined, it re-runs itself as suspend using the Process Hollowing technique.

Information Collected:

Targeted languages and countries:

cmd.exe path:

```
edi:L"=::=::\\"

edi:L"=::=::\\"

esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe", edi:L"=::=::\\"
edi:L"=::=::\\"

esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"

esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
```

```
EBX    00000001
ECX    00000000
EDX    00000002
EBP    0013F264
ESP    0013F258
ESI    0030342E    L"ComSpec=C:\\Windows\\system32\\cmd.exe"
EDI    00303210    L"=::=::\\"

EIP    6F199802    fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699e

EFLAGS    00000206
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  0000007F (ERROR_PROC_NOT_FOUND)
```

username:

```
6F1997E1    FF15 20411A6F    call dword ptr ds:[<&GetEnvironmentStringsW>]
6F1997E7    8BF8             mov edi,eax                                          edi:L"=::=::\\"
6F1997E9    33C0             xor eax,eax
6F1997EB    85FF             test edi,edi                                         edi:L"=::=::\\"
6F1997ED  v 74 75            je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8a
6F1997EF    56               push esi                                             esi:L"USERNAME=        "
6F1997F0    8BF7             mov esi,edi                                          esi:L"USERNAME=        ",
6F1997F2    66:3907          cmp word ptr ds:[edi],ax                             edi:L"=::=::\\"
6F1997F5  v 74 10            je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8a
6F1997F7    83C6 02          add esi,2                                            esi:L"USERNAME=        "
6F1997FA    66:3906          cmp word ptr ds:[esi],ax                             esi:L"USERNAME=        "
6F1997FD  ^ 75 F8            jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8
6F1997FF    83C6 02          add esi,2                                            esi:L"USERNAME=        "
6F199802    66:3906          cmp word ptr ds:[esi],ax                             esi:L"USERNAME=        "
6F199805  ^ 75 F0            jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8
6F199807    53               push ebx
```

LOGONSERVER:

```
edi:L"=::=::\\"

edi:L"=::=::\\"

esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J", edi:L"=::=::\\"
edi:L"=::=::\\"

esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"

esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
```

```
EBX    00000001
ECX    00000000
EDX    00000002
EBP    0013F264
ESP    0013F258
ESI    00303538    L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
EDI    00303210    L"=::=::\\"

EIP    6F199802    fc1f9739dc9d6e9c61222beb9e3552bbc9a5

EFLAGS    00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

NUMBER_OF_PROCESSOR:

```
call dword ptr ds:[<&GetEnvironmentStringsW>]
mov edi,eax
xor eax,eax
test edi,edi                                                                     edi:L"=::=::\\"
je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199864
push esi                                                                         esi:L"NUMBER_OF_PROCESSORS=1"
mov esi,edi                                                                      esi:L"NUMBER_OF_PROCESSORS=1", edi:L"=::=::\\"
cmp word ptr ds:[edi],ax                                                         edi:L"=::=::\\"
je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199807
add esi,2                                                                        esi:L"NUMBER_OF_PROCESSORS=1"
cmp word ptr ds:[esi],ax                                                         esi:L"NUMBER_OF_PROCESSORS=1"
jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7
add esi,2                                                                        esi:L"NUMBER_OF_PROCESSORS=1"
cmp word ptr ds:[esi],ax                                                         esi:L"NUMBER_OF_PROCESSORS=1"
jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7
```

COMPUTERNAME:

```
edi:L"=::=::\\"

491a404e8ad4.6F1998    edi:L"=::=::\\"

esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
esi:L"COMPUTERNAME=WIN-L1KDN79P80J", edi:L"=::=::\\"
edi:L"=::=::\\"
491a404e8ad4.6F1998
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
6491a404e8ad4.6F199
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
6491a404e8ad4.6F199
```

```
EBX    00000001
ECX    00000000
EDX    00000002
EBP    0013F264
ESP    0013F258
ESI    003033F4    L"COMPUTERNAME=WIN-L1KDN79P80J"
EDI    00303210    L"=::=::\\"

EIP    6F199802    fc1f9739dc9d6e9c61222beb9e3552bbc9a5a9

EFLAGS    00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

PROCESSOR:

```
<&GetEnvironmentStringsW>]
                                                             edi:L"=::=::\\"

                                                             edi:L"=::=::\\"
:61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8
                                                             esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
                                                             esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
i],ax                                                        edi:L"=::=::\\"
:61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8
                                                             esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
i],ax                                                        esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
:c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e
                                                             esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
i],ax                                                        esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
:c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e
```

7gfdg5egds.exe ANALYSIS

File Name:	7gfdg5egds.exe
MD5	270C3859591599642BD15167765246E3
SHA1	E227A8A338166DC97E360CA9CDDDA5E007079C58
SHA256	DEE4BB7D46BBBEC6C01DC41349CB8826B27BE9A0DCF39816CA8BD6E0A39C2019

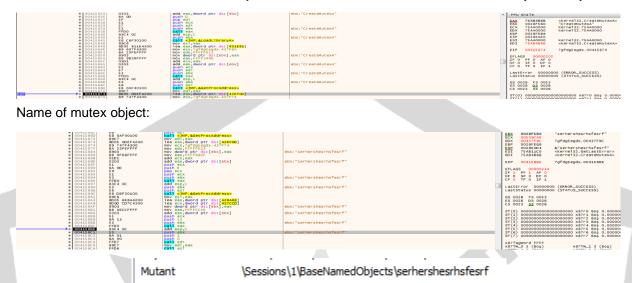When we look at the imports of the pest, it uses important libraries such as USER32 and WS2_32. When we look at the WS2_32 library, it is understood that it has the capacity to perform network operations, as can be seen from the functions it uses.

When we examine the important DLL and functions in the pest;

- CreateToolhelp32Snapshot
- WriteFile
- GetSystemInfo
- CreateMutexA

It is seen that the malware can Access system information, create a mutex object, get information about the system and files, write files, and take a snapshot of the process.
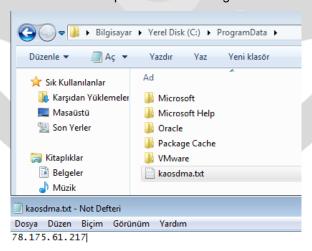
The malware first creates the mutex object with the "CreateMutexA" API that it loads dynamically.

Name of mutex object:

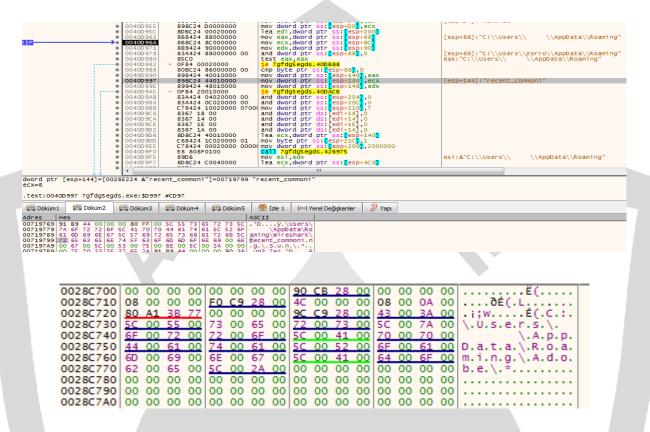| Mutant | \Sessions\1\BaseNamedObjects\serhershesrhsfesrf |

Some other DLL's and APIs it loads dynamically:

The malware then drops the .txt file with an ip address into ProgramData.

In general, it is seen that the malware has 2 basic behaviors. First, it scans the software installed on the system.

Another behavior is to steal personal data and identity information from web browsers. Since most applications are not installed, it seems that it just checks.

Google Chrome:

Phone number, credit card information kept in Google Chrome:

The email address that Google Chrome keeps after logging in:

Bitcoin wallet:

```
00419244    8D0D 13794300        lea ecx,dword ptr ds:[437913]
0041924A    8906                 mov dword ptr ds:[esi],eax
0041924C    B8 7ADAFFFF          mov eax,FFFFDA7A
00419251    0306                 add eax,dword ptr ds:[esi]
00419253    51                   push ecx
00419254    6A 19                push 19
00419256    8D9C24 38070000      lea ebx,dword ptr ss:[esp+738]
0041925D    53                   push ebx                          ebx:"%appdata%\\Bitcoin\\wallets"
0041925E    FFD0                 call eax
00419260    83C4 0C              add esp,C
00419263    31D2                 xor edx,edx
00419265    8D8C24 40030000      lea ecx,dword ptr ss:[esp+340]
0041926C    8D8424 B0040000      lea eax,dword ptr ss:[esp+4B0]
```

Exodus wallet:

```
0041955B    FFD0                 call eax
0041955D    83C4 0C              add esp,C
00419560    8D8C24 40030000      lea ecx,dword ptr ss:[esp+340]      [esp+340]:"%appdata%\\Exodus\\exodus.walletA"
00419567    89FA                 mov edx,edi
00419569    E8 5098FEFF          call 7gfdg5egds.402DBE
0041956E    8D05 33364300        lea eax,dword ptr ds:[433633]
00419574    B9 5C7D4300          mov ecx,7gfdg5egds.437D5C           ecx:&"%appdata%\\Exodus\\exodus.walletA"
00419579    8903                 mov dword ptr ds:[ebx],eax          [ebx]:"Jaxxp"
0041957B    B8 E920FFFF          mov eax,FFFF20E9
00419580    0303                 add eax,dword ptr ds:[ebx]          [ebx]:"Jaxxp"
00419582    6A 95                push FFFFFF95
00419584    5A                   pop edx
00419585    01D1                 add ecx,edx                         ecx:&"%appdata%\\Exodus\\exodus.walletA"
00419587    51                   push ecx                            ecx:&"%appdata%\\Exodus\\exodus.walletA"
```

Ethereum wallet:

```
00419BF4    41                   inc ecx
00419BF5    8908                 mov dword ptr ds:[eax],ecx
00419BF7    8360 04 00           and dword ptr ds:[eax+4],0
00419BFB    8360 08 00           and dword ptr ds:[eax+8],0
00419BFF    894F 04              mov dword ptr ds:[edi+4],ecx
00419C02    8367 08 00           and dword ptr ds:[edi+8],0
00419C06    8D4424 20            lea eax,dword ptr ss:[esp+20]        [esp+20]:&"%appdata%\\Ethereum\\keystore"
00419C0A    8947 10              mov dword ptr ds:[edi+10],eax
00419C0D    894F 14              mov dword ptr ds:[edi+14],ecx
00419C10    8D8424 B0040000      lea eax,dword ptr ss:[esp+4B0]       [esp+4B0]:"%appdata%\\Ethereum\\keystore"
00419C17    8D8C24 40030000      lea ecx,dword ptr ss:[esp+340]
00419C1E    894424 20            mov dword ptr ss:[esp+20],eax        [esp+20]:&"%appdata%\\Ethereum\\keystore"
00419C22    C74424 24 C7264000   mov dword ptr ss:[esp+24],7gfdg5egds.4026C7
00419C2A    E8 418A0000          call 7gfdg5egds.422670
```

Data from the Discord app:

```
0041DE11    894424 04            mov dword ptr ss:[esp+4],eax
0041DE15    8D05 36124300        lea eax,dword ptr ds:[431236]
0041DE1B    8D0D C96F4300        lea ecx,dword ptr ds:[436FC9]
0041DE21    8906                 mov dword ptr ds:[esi],eax           esi:"%appdata%\\Discord\\Local Storage2\\Sessions"
0041DE23    B8 E644FFFF          mov eax,FFFF44E6
0041DE28    0306                 add eax,dword ptr ds:[esi]           esi:"%appdata%\\Discord\\Local Storage2\\Sessions"
0041DE2A    51                   push ecx
0041DE2B    6A 1F                push 1F
0041DE2D    56                   push esi                             esi:"%appdata%\\Discord\\Local Storage2\\Sessions"
0041DE2E    FFD0                 call eax
0041DE30    83C4 0C              add esp,C
0041DE33    8D8C24 40030000      lea ecx,dword ptr ss:[esp+340]
```

Steam:

```
0041E2F5    59                   pop ecx
0041E2F6    51                   push ecx
0041E2F7    53                   push ebx                             ebx:"SOFTWARE\\WOW6432Node\\Valve\\Steam\\Sessions"
0041E2F8    FFD0                 call eax
0041E2FA    83C4 0C              add esp,C
0041E2FD    8D05 630D4300        lea eax,dword ptr ds:[430D63]
0041E303    8D0D 25734300        lea ecx,dword ptr ds:[437325]
0041E309    898424 30070000      mov dword ptr ss:[esp+730],eax
```

.purple: It is the configuration directory in Windows. Here you can find information about the account, including chat logs, pictures from other users, passwords.

```
0041E18D    8DBC24 D80A0000      lea edi,dword ptr ss:[esp+AD8]
0041E194    57                   push edi                             edi:"%appdata%\\.purple\\accounts.xmle2\\Sessions"
0041E195    FFD0                 call eax
0041E197    83C4 0C              add esp,C
0041E19A    8D8424 A8010000      lea eax,dword ptr ss:[esp+1A8]
0041E1A1    89FA                 mov edx,edi                          edi:"%appdata%\\.purple\\accounts.xmle2\\Sessions"
0041E1A3    89F1                 mov ecx,esi                          esi:"%appdata%\\.purple\\accounts.xmle2\\Sessions"
0041E1A5    E8 144CFEFF          call 7gfdg5egds.402DBE
```

FileZilla:

```
0041D117    8DBC24 38070000      lea edi,dword ptr ss:[esp+738]
0041D11E    57                   push edi                             edi:"recentservers.xml"
0041D11F    FFD0                 call eax
0041D121    83C4 0C              add esp,C
0041D124    8D8C24 90000000      lea ecx,dword ptr ss:[esp+90]        [esp+90]:"%appdata%\\FileZilla"
0041D12B    89FA                 mov edx,edi                          edi:"recentservers.xml"
0041D12D    E8 145BFEFF          call 7gfdg5egds.402C46
0041D132    8D05 34A84200        lea eax,dword ptr ds:[42A834]
```

Here, the system information received by the malware is displayed.

OS:

Processor:

Resolution:

Ram:

Machine-Guid:

We see that the malware takes a snapshot of the operation.

The values that the malware changes from the registry to escape antiviruses.

```
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\cval = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiVirusOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiSpywareOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\FirewallOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiVirusOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiSpywareOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\FirewallOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiVirusOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiSpywareOverride = 0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\FirewallOverride = 0
```

NETWORK ANALYSIS

It has been seen that the malware tries to connect to the address 95[.]213[.]179[.]67[:]80 after stealing data. But because the server is not active, it could not establish a connection.

```
Network Traffic:
==================
[UDP] svchost.exe:988 > 192.168.81.2:53
[UDP] 192.168.81.2:53 > svchost.exe:988
[UDP] svchost.exe:744 > 255.255.255.255:67
[UDP] 192.168.81.254:67 > svchost.exe:744
[TCP] 7gfdg5egds.exe:2536 > 50.16.239.65:80
[TCP] 50.16.239.65:80 > 7gfdg5egds.exe:2536
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:50805 > svchost.exe:988
[UDP] svchost.exe:988 > 224.0.0.252:5355
[UDP] System:4 > 192.168.81.2:137
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:57681 > svchost.exe:988
[UDP] System:4 > 192.168.81.255:137
[UDP] 192.168.81.129:137 > System:4
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:62065 > svchost.exe:988
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:54482 > svchost.exe:988
[TCP] jucheck.exe:1776 > 184.24.22.47:443
[TCP] 184.24.22.47:443 > jucheck.exe:1776
[TCP] jucheck.exe:1776 > 23.55.161.133:80
[TCP] 23.55.161.133:80 > jucheck.exe:1776
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:50409 > svchost.exe:988
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:52542 > svchost.exe:988
[TCP] jp2launcher.exe:1160 > b818:162f:0:0:0:0:0:0:443
[TCP] b818:162f:0:0:0:0:0:0:443 > jp2launcher.exe:1160
[TCP] jp2launcher.exe:1160 > 5db8:dc1d:0:0:0:0:0:0:80
[TCP] 5db8:dc1d:0:0:0:0:0:0:80 > jp2launcher.exe:1160
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:50460 > svchost.exe:988
[TCP] svchost.exe:988 > 23.55.161.165:80
[TCP] 23.55.161.165:80 > svchost.exe:988
```

SOLUTION PROPOSALS

- Actual and reliable anti-virus software should be used on the systems.
- Incoming e-mails should be read carefully, e-mails and URLs from unknown sources and files should not be opened without a full scan of attachments.
- All installed software and operating system should be kept up to date.
- Train users frequently to be aware of potential phishing schemas and how to handle them in the right way.
- The network movements of the processes running on the system should be examined.

Yara Rules

```
import "hash"
rule FickerStealer
{
meta:
author = "Hakan Soysal - ZAYOTEM"
description ="file.dll"
strings:
 $export0 = "Closewhether"
 $export1 = "Meantduck"
 $export2 = "My"
 $export3 = "Ropemay"

 condition:
hash.md5(0,filesize) == "9b59d4744ff1de8b338eeb2b85748cf2" or all of them
}
```

```
import "hash"

rule FickerStealer

{

meta:

author ="Hakan Soysal - ZAYOTEM"

description ="7gfdg5egds.exe"

strings:

 $a =
"0x000102030405060708091011121314151617181920212223242526272829303132
333435363738394041424344454647484950515253545556575859606162636465666
768697071727374757677787980818283848586878889909192939495969798990[]"

 $b = "_matherr(): %s in %s(%g, %g)  (retval=%g)\\n"

 $c = {48 09 0A 46 45 1B 48 08 53 1D 39 81 07 46 0A 1D}

 $d = {22 53 6F 6D 65 4E 6F 6E 65 00 00 00 BC 94 43 00}


 condition:

 hash.md5(0,filesize) == "270c3859591599642bd15167765246e3" or all of them

 }
```

Hakan Soysal

https://www.linkedin.com/in/hakansoysal/