BAD RABBIT

Ransomware

Bad Rabbit is a locally self-propagating ransomware, spreading via SMB once inside.

Requires User Interaction

Mostly targeted Russia and the Ukraine.

Primary affected Windows XP thru 7.

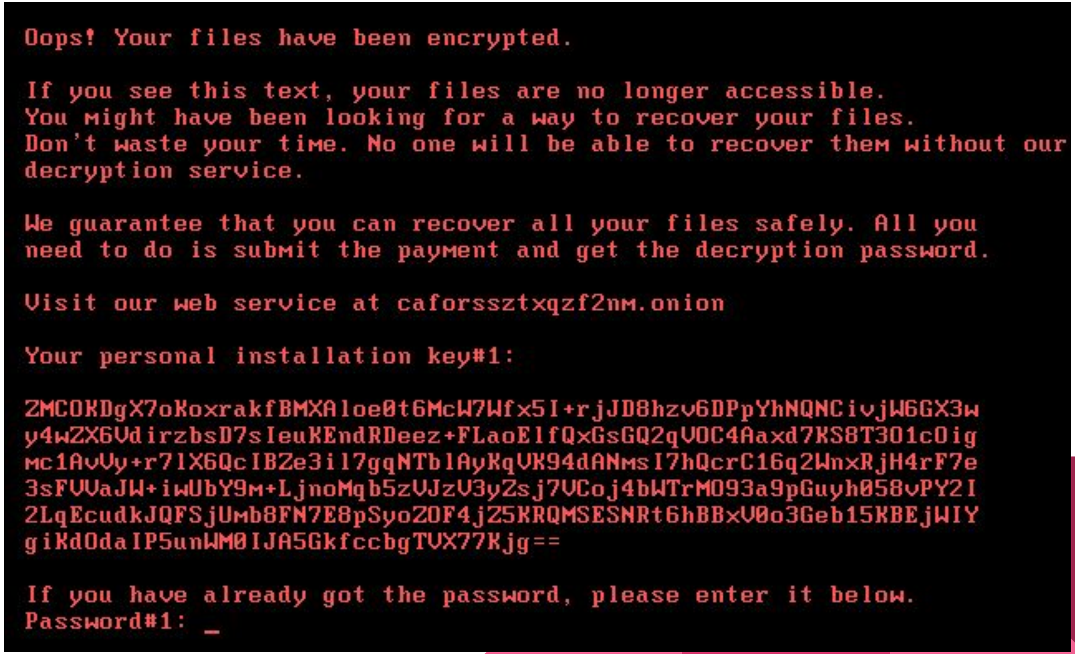
```
$  echo   -e "\nLance Magnanao   \nConstantine Politis  \nHenry Lueders"  > authors.txt
$ cat authors.txt
```

What damage was done?

When Bad Rabbit infects a computer; it will distribute or block access to data for ransom.

Individuals that are victimized by this ransomware are directed to a payment site and given 40 hours to pay or the data will be spread across the net; or an increase of ransom for additional time.

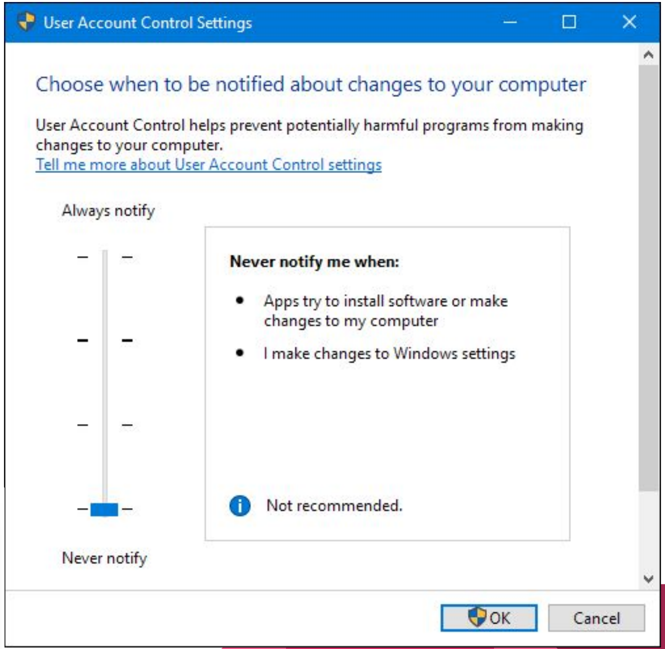
Usually the amount would start around 0.05 bitcoins or around $285 (with the price of bitcoin back then).



```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#1:

ZMCOKDgX7oKoxrakfBMXAloe0t6McW7Wfx5I+rjJD8hzv6DPpYhNQNCivjW6GX3w
y4wZX6VdirzbsD7sIeuKEndRDeez+FLaoElfQxGsGQ2qVOC4Aaxd7KS8T3O1cOig
mc1AvVy+r7lX6QcIBZe3il7gqNTblAyKqVK94dANmsI7hQcrC16q2WnxRjH4rF7e
3sFVVaJW+iwUbY9m+LjnoMqb5zVJzV3yZsj7VCoj4bWTrMO93a9pGuyh058vPY2I
2LqEcudkJQFSjUmb8FN7E8pSyoZOF4jZ5KRQMSESNRt6hBBxV0o3Geb15KBEjWIY
giKdOdaIP5unWM0IJA5GkfccbgTVX77Kjg==

If you have already got the password, please enter it below.
Password#1: _
```

How was the damage done?

Bad Rabbit Uses Social Engineering to Infect: The infection vector starts by visiting a compromised website requesting an Adobe Flash update that downloads the malware. Various reports suggest that the initial infection is caused by compromised web servers that delivered the malicious file (under the name "install_flash_ player.exe"). In order to start the infection, a user will need to download the file from the infected web server and execute it. Depending on User Access Control (UAC) settings, most users will have to accept a popup in order to execute the file. Also, when the user has no admin privileges (high integrity), the malware would not perform malicious actions.



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

Tell me more about User Account Control settings

Always notify

Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended.

Never notify

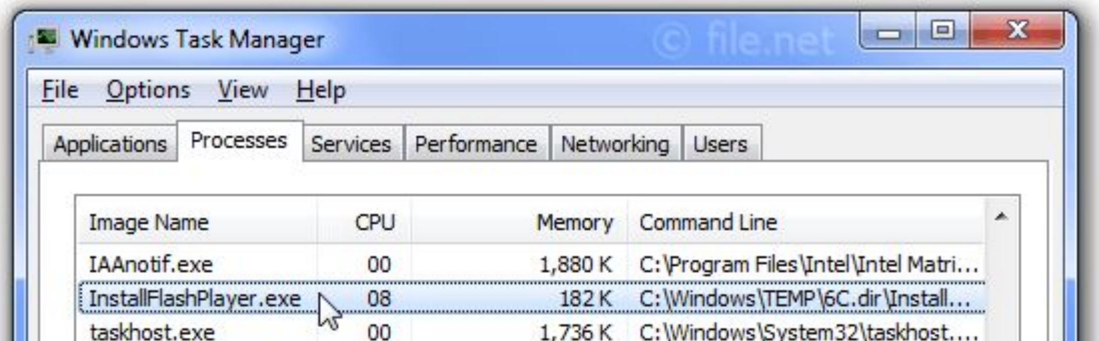
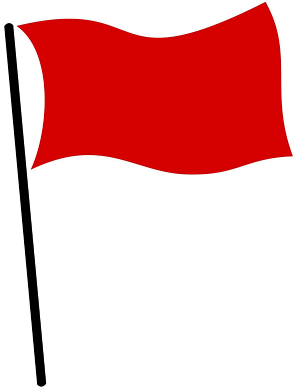
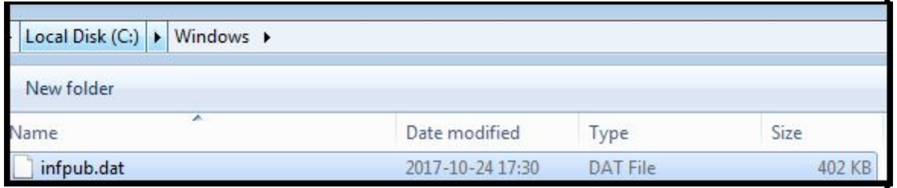


Image Name	CPU	Memory	Command Line
IAAnotif.exe	00	1,880 K	C:\Program Files\Intel\Intel Matri...
InstallFlashPlayer.exe	08	182 K	C:\Windows\TEMP\6C.dir\Install...
taskhost.exe	00	1,736 K	C:\Windows\System32\taskhost....

How was the damage done?

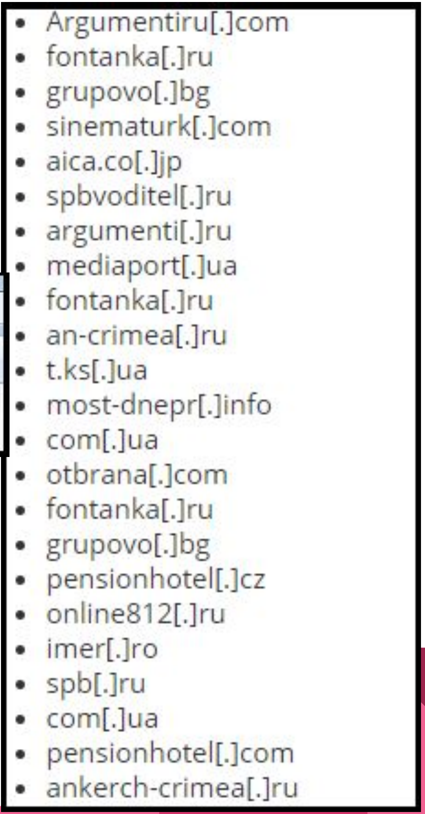
Installation: The executable "install_flash_player.exe" contains the payload of an encrypted copy of the "infpub.dat" file; so, the first stage of the "BadRabbit" malware is to deploy the second stage of the malware:





Name	Date modified	Type	Size
infpub.dat	2017-10-24 17:30	DAT File	402 KB

Sample Sites of compromised sites delivering Bad Rabbit:



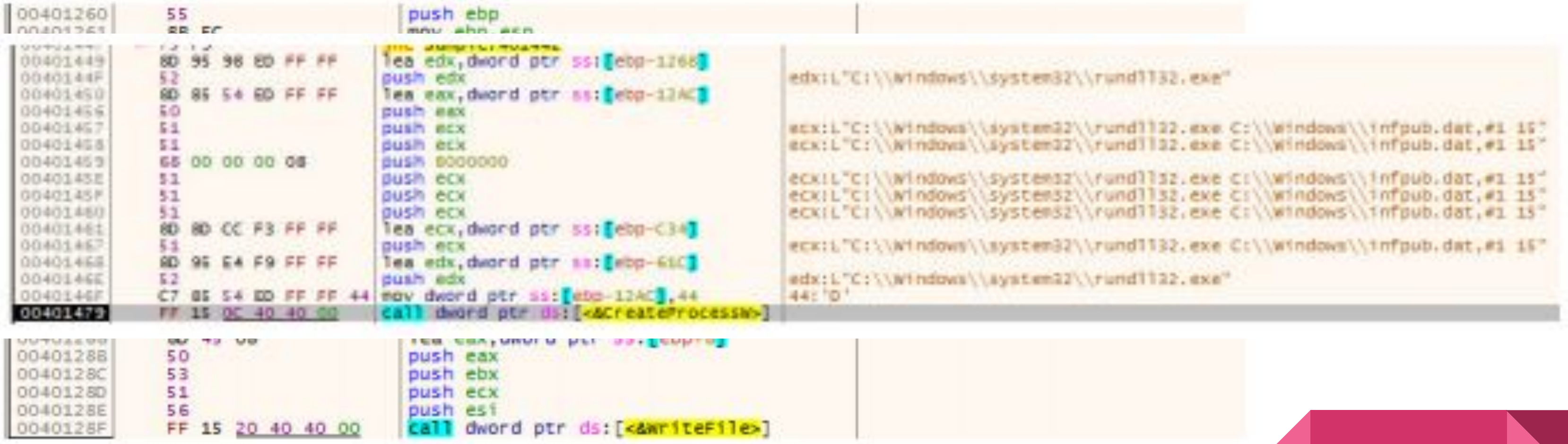
- Argumentiru[.]com
- fontanka[.]ru
- grupovo[.]bg
- sinematurk[.]com
- aica.co[.]jp
- spbvoditel[.]ru
- argumenti[.]ru
- mediaport[.]ua
- fontanka[.]ru
- an-crimea[.]ru
- t.ks[.]ua
- most-dnepr[.]info
- com[.]ua
- otbrana[.]com
- fontanka[.]ru
- grupovo[.]bg
- pensionhotel[.]cz
- online812[.]ru
- imer[.]ro
- spb[.]ru
- com[.]ua
- pensionhotel[.]com
- ankerch-crimea[.]ru

Disclaimer:DON'T VISIT THESE SITES!

How was the damage done?

After the file is dropped, it is executed using rundll32.exe
“C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15”

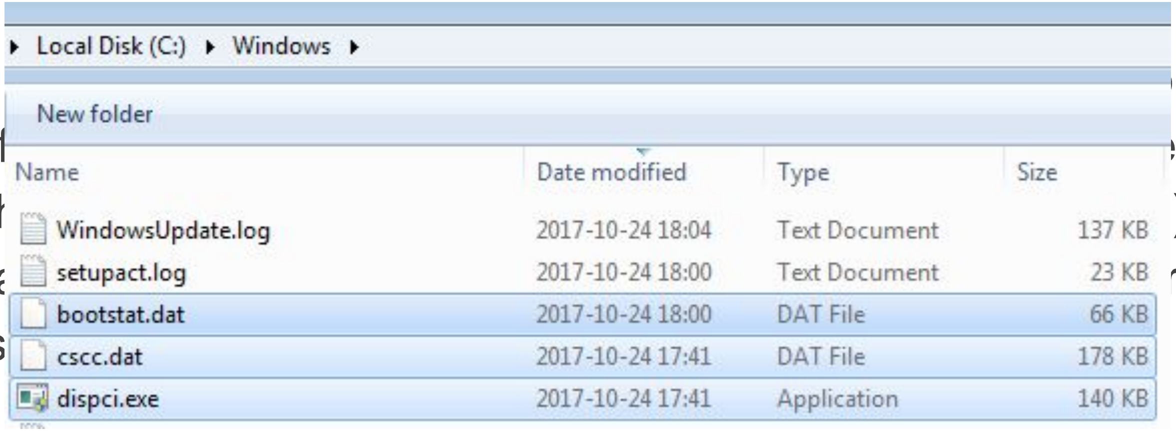
payload is decrypted in memory, the ” file is created and the decrypted data is written to the file.



```
00401260    55                       push ebp
00401263    8B EC                    mov ebp,esp
00401449    8D 95 98 ED FF FF        lea edx,dword ptr ss:[ebp-1268]
0040144F    52                       push edx                              edx:L"C:\\Windows\\system32\\rundll32.exe"
00401450    8D 85 54 ED FF FF        lea eax,dword ptr ss:[ebp-12AC]
00401456    50                       push eax
00401457    51                       push ecx                              ecx:L"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"
00401458    51                       push ecx                              ecx:L"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"
00401459    68 00 00 00 08           push 8000000
0040145E    51                       push ecx                              ecx:L"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"
0040145F    51                       push ecx                              ecx:L"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"
00401460    51                       push ecx                              ecx:L"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"
00401461    8D 8D CC F3 FF FF        lea ecx,dword ptr ss:[ebp-C34]
00401467    51                       push ecx                              ecx:L"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"
00401468    8D 95 E4 F9 FF FF        lea edx,dword ptr ss:[ebp-61C]
0040146E    52                       push edx                              edx:L"C:\\Windows\\system32\\rundll32.exe"
0040146F    C7 85 54 ED FF FF 44     mov dword ptr ss:[ebp-12AC],44        44:'D'
00401479    FF 15 0C 40 40 00        call dword ptr ds:[<&CreateProcessW>]
00401288    8D 45 08                 lea eax,dword ptr ss:[ebp+8]
0040128B    50                       push eax
0040128C    53                       push ebx
0040128D    51                       push ecx
0040128E    56                       push esi
0040128F    FF 15 20 40 40 00        call dword ptr ds:[<&WriteFile>]
```

How was the damage done?

“infpub.dat” r portion of
the malicious f nsion is
familiar from th) to perform
most of the ma rops three
additional files



Name	Date modified	Type	Size
WindowsUpdate.log	2017-10-24 18:04	Text Document	137 KB
setupact.log	2017-10-24 18:00	Text Document	23 KB
bootstat.dat	2017-10-24 18:00	DAT File	66 KB
cscc.dat	2017-10-24 17:41	DAT File	178 KB
dispci.exe	2017-10-24 17:41	Application	140 KB

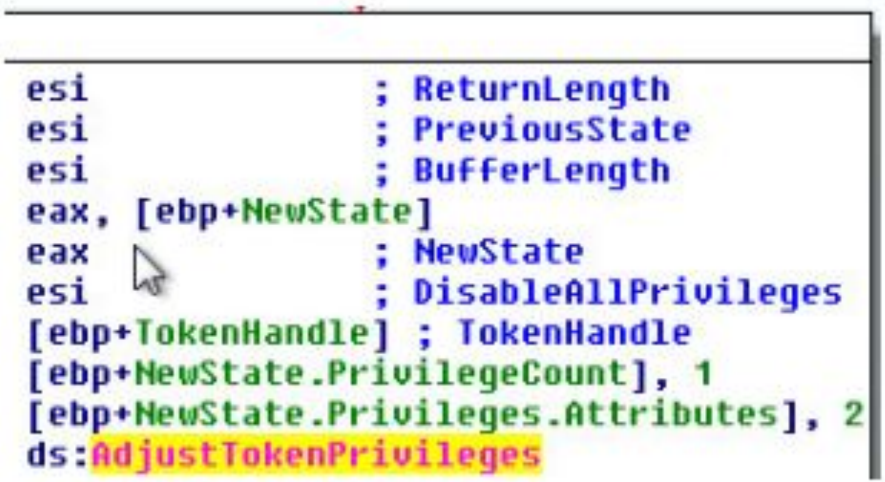
- “C:\Windows\cscc.dat” - *cscc.dat* – legitimate driver used for the disk encryption (diskcryptor.net)
  - “C:\Windows\dispci.exe” - *dispci.exe* – installs the bootlocker, communicates with the driver
    - “C:\Windows\<random-name>.tmp” - mimikatz binary used for obtaining passwords

How was the damage done?

First, the malware enables privileges using AdjustTokenPrivileges().

The malware enables the following privileges:

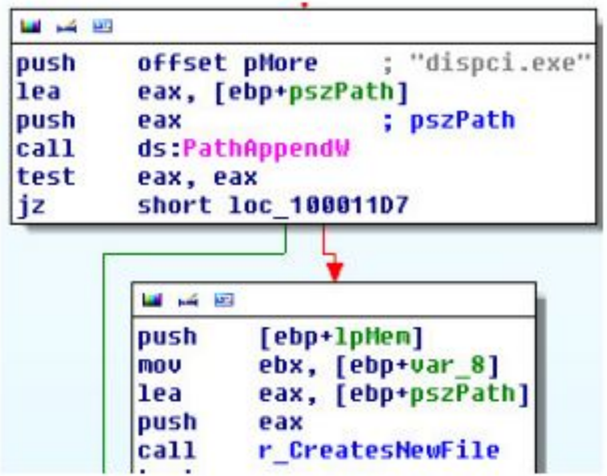
- “SeShutdownPrivilege” - gives the ability to shut down local system.
- “SeDebugPrivilege” - gives the ability to debug.
- “SeTcbPrivilege” - its holder is recognized as part of the trusted computer base.



```
esi               ; ReturnLength
esi               ; PreviousState
esi               ; BufferLength
eax, [ebp+NewState]
eax               ; NewState
esi               ; DisableAllPrivileges
[ebp+TokenHandle] ; TokenHandle
[ebp+NewState.PrivilegeCount], 1
[ebp+NewState.Privileges.Attributes], 2
ds:AdjustTokenPrivileges
```

How was the damage done?

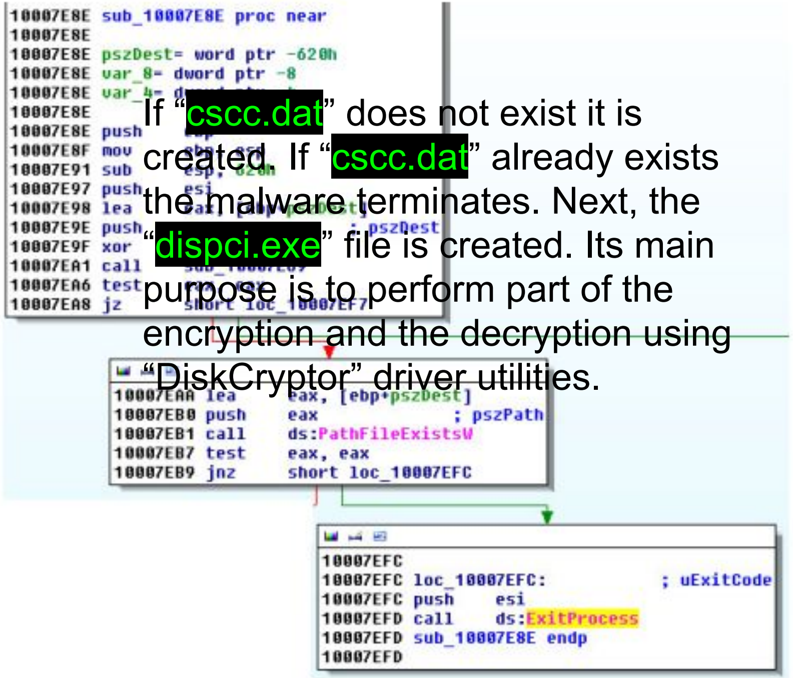
Next, the malware drops additional files. The first is “cscc.dat” that will b e



```
push    offset pMore      ; "dispci.exe"
lea     eax, [ebp+pszPath]
push    eax               ; pszPath
call    ds:PathAppendW
test    eax, eax
jz      short loc_100011D7
```

```
push    [ebp+lpMem]
mov     ebx, [ebp+var_8]
lea     eax, [ebp+pszPath]
push    eax
call    r_CreatesNewFile
```

If “cscc.dat” does not exist it is created. If “cscc.dat” already exists the malware terminates. Next, the “dispci.exe” file is created. Its main purpose is to perform part of the encryption and the decryption using “DiskCryptor” driver utilities.



```
10007E8E sub_10007E8E proc near
10007E8E
10007E8E pszDest= word ptr -620h
10007E8E var_8= dword ptr -8
10007E8E var_4= [illegible]
10007E8E
10007E8E push    ebp
10007E8F mov     ebp, esp
10007E91 sub     esp, 620h
10007E97 push    esi
10007E98 lea     eax, [ebp+pszDest]
10007E9E push    eax             ; pszDest
10007E9F xor     [illegible]
10007EA1 call    sub_10007E[illegible]
10007EA6 test    eax, eax
10007EA8 jz      short loc_10007EF7
```

```
10007EAA lea     eax, [ebp+pszDest]
10007EB0 push    eax             ; pszPath
10007EB1 call    ds:PathFileExistsW
10007EB7 test    eax, eax
10007EB9 jnz     short loc_10007EFC
```

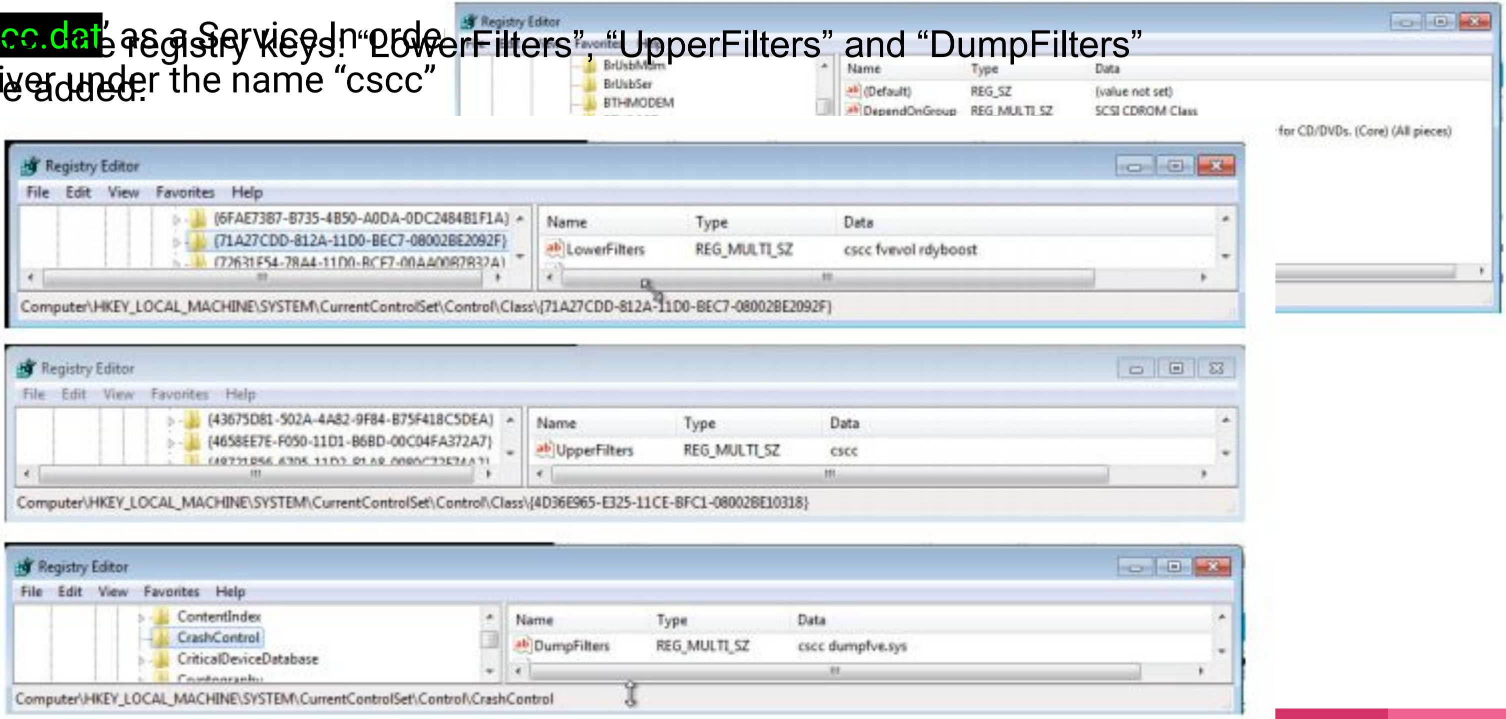
```
10007EFC
10007EFC loc_10007EFC:                   ; uExitCode
10007EFC push    esi
10007EFD call    ds:ExitProcess
10007EFD sub_10007E8E endp
10007EFD
```

How was the damage done?

Registering 'cscc.dat' as a Service In orde… service as a driver under the name "cscc"

…e registry keys: "LowerFilters", "UpperFilters" and "DumpFilters" are added.

Then the ma… following reg… Key:"HKEY_… SYSTEM\Cu… vices\cdfs"



Registry Editor
Favorites
BrUsbMdm
BrUsbSer
BTHMODEM
File Edit View Favorites Help
{6FAE73B7-B735-4B50-A0DA-0DC2484B1F1A}
{71A27CDD-812A-11D0-BEC7-08002BE2092F}
{72631E54-78A4-11D0-BCF7-00AA00B7B32A}
{4367SD81-502A-4A82-9F84-B75F418C5DEA}
{4658EE7E-F050-11D1-B6BD-00C04FA372A7}
ContentIndex
CrashControl
CriticalDeviceDatabase
Cryptography

Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnGroup	REG_MULTI_SZ	SCSI CDROM Class

for CD/DVDs. (Core) (All pieces)

Name	Type	Data
LowerFilters	REG_MULTI_SZ	cscc fvevol rdyboost

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}

Name	Type	Data
UpperFilters	REG_MULTI_SZ	cscc

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}

Name	Type	Data
DumpFilters	REG_MULTI_SZ	cscc dumpfve.sys

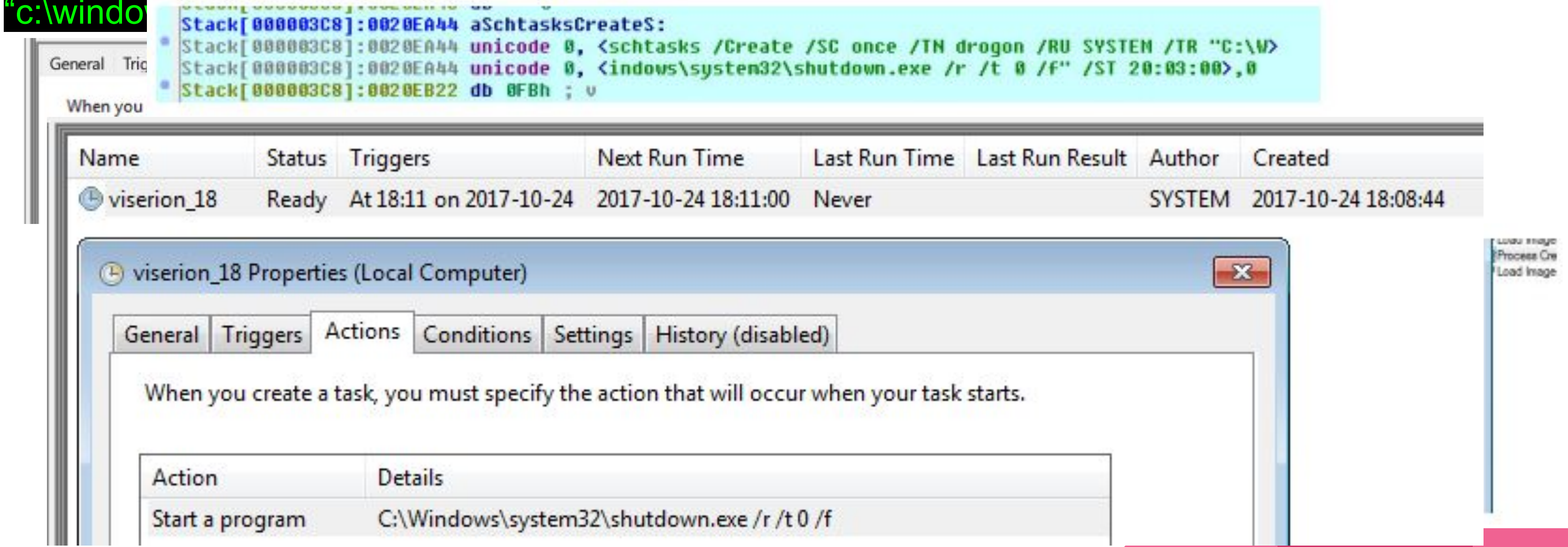
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl

How was the damage done?

After the driver is registered, the malware adds two new scheduled tasks:

1. The first scheduled task is set with the purpose of shutting down the ‘cmd.exe /c schtasks /Create /SC once /TN drogon /RU SYSTEM /TR “C:\Windows\system32\shutdown.exe /r /t 0 /f /ST ’

2. Another scheduled task that is set to make sure that after a reboot the dispci.exe e he scheduled task is set using the ¨EM /SC ONSTART /TN rhaegal / TR “c:\windo



```
Stack[000003C8]:0020EA44 aSchtasksCreateS:
Stack[000003C8]:0020EA44 unicode 0, <schtasks /Create /SC once /TN drogon /RU SYSTEM /TR "C:\W>
Stack[000003C8]:0020EA44 unicode 0, <indows\system32\shutdown.exe /r /t 0 /f" /ST 20:03:00>,0
Stack[000003C8]:0020EB22 db 0FBh ; v
```

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
viserion_18	Ready	At 18:11 on 2017-10-24	2017-10-24 18:11:00	Never		SYSTEM	2017-10-24 18:08:44

viserion_18 Properties (Local Computer)

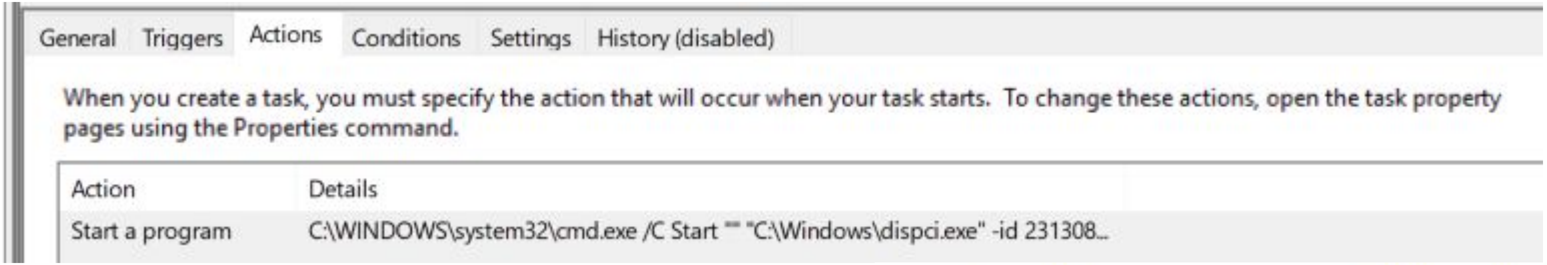
When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Windows\system32\shutdown.exe /r /t 0 /f

How was the damage done?

File Encryption Process:

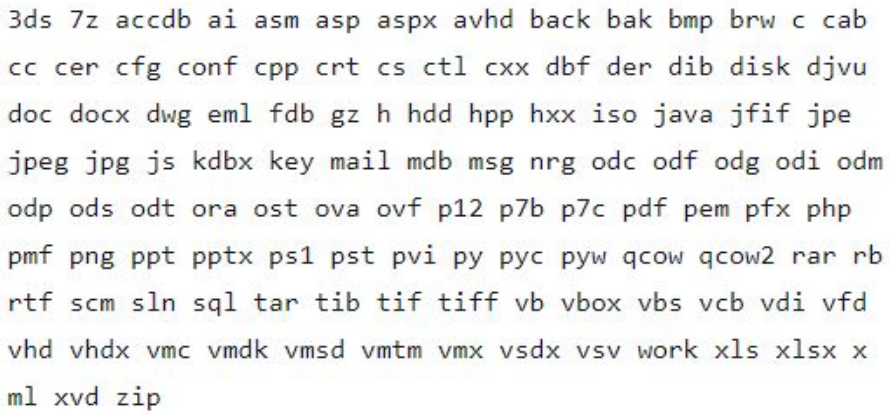
The dropped application “dispci.exe” (DiskCryptor) is run with the help of one of the scheduled task:



When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\WINDOWS\system32\cmd.exe /C Start "" "C:\Windows\dispci.exe" -id 231308...

The malware encrypts files with the selected extensions. All the files are encrypted with the same key (the same plaintext gives the same ciphertext).



```
3ds 7z accdb ai asm asp aspx avhd back bak bmp brw c cab
cc cer cfg conf cpp crt cs ctl cxx dbf der dib disk djvu
doc docx dwg eml fdb gz h hdd hpp hxx iso java jfif jpe
jpeg jpg js kdbx key mail mdb msg nrg odc odf odg odi odm
odp ods odt ora ost ova ovf p12 p7b p7c pdf pem pfx php
pmf png ppt pptx ps1 pst pvi py pyc pyw qcow qcow2 rar rb
rtf scm sln sql tar tib tif tiff vb vbox vbs vcb vdi vfd
vhd vhdx vmc vmdk vmsd vmtm vmx vsdx vsv work xls xlsx x
ml xvd zip
```

How was the damage done?

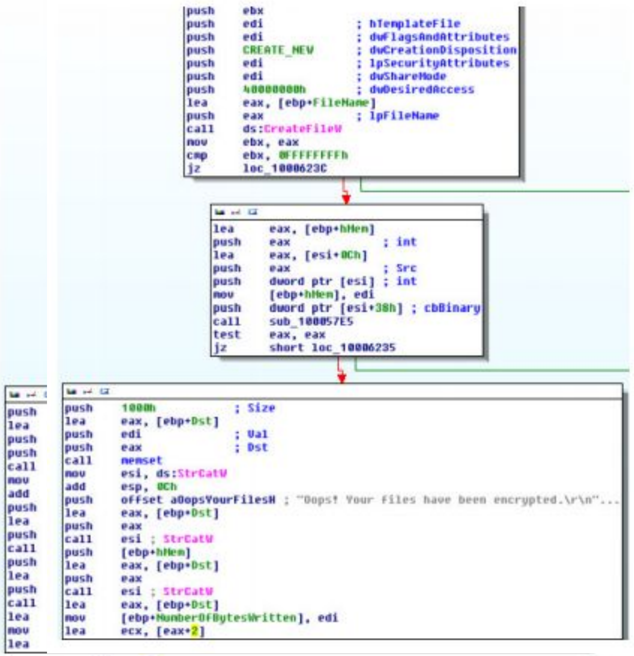
Some of the system directories are exempted from the attack:

```
\\Windows
\\Program Files
\\ProgramData
\\AppData
```

File Encryption Process:

“infpub.dat” malware performs a major par[t of] encryption. First it ... the list of the drives c... Next, it

“infpub.dat” also drops “Readme.txt” in each root of the directories

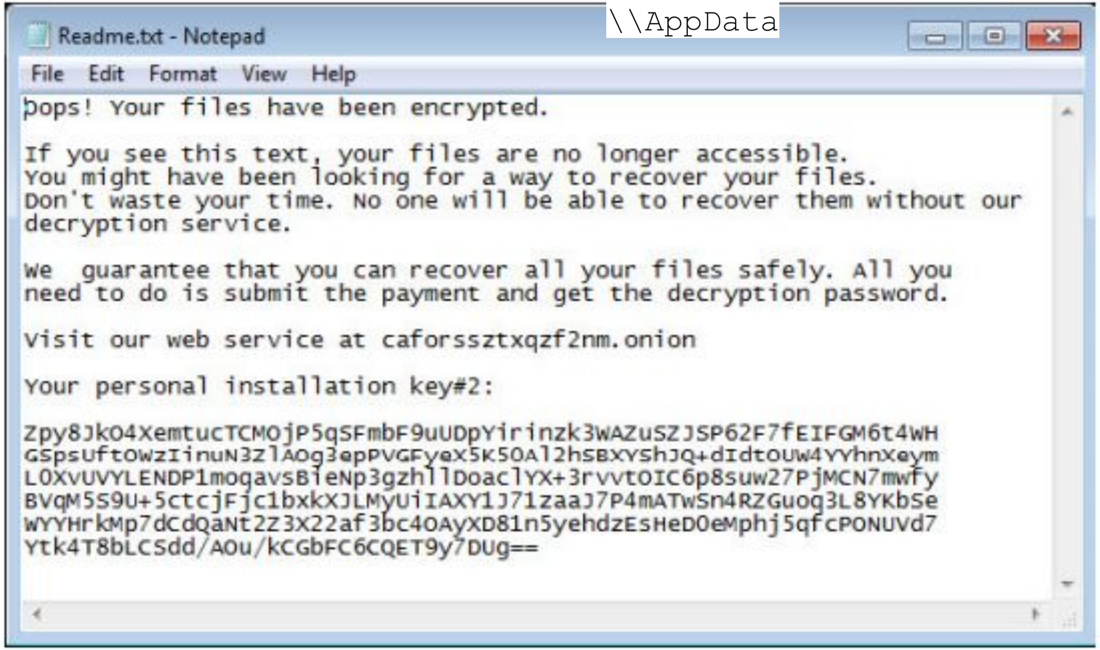


```
push    ebx
push    edi                 ; hTemplateFile
push    edi                 ; dwFlagsAndAttributes
push    CREATE_NEW          ; dwCreationDisposition
push    edi                 ; lpSecurityAttributes
push    edi                 ; dwShareMode
push    40000000h           ; dwDesiredAccess
lea     eax, [ebp+FileName]
push    eax                 ; lpFileName
call    ds:CreateFileW
mov     ebx, eax
cmp     ebx, 0FFFFFFFFh
jz      loc_1000623C
```

```
lea     eax, [ebp+hMem]
push    eax                 ; int
lea     eax, [esi+0Ch]
push    eax                 ; Src
push    dword ptr [esi] ; int
mov     [ebp+hMem], edi
push    dword ptr [esi+38h] ; cbBinary
call    sub_100057E5
test    eax, eax
jz      short loc_10006235
```

```
push    1000h               ; Size
lea     eax, [ebp+Dst]
push    edi                 ; Val
push    eax                 ; Dst
call    memset
mov     esi, ds:StrCatW
add     esp, 0Ch
push    offset aOopsYourFilesH ; "Oops! Your files have been encrypted.\r\n"...
lea     eax, [ebp+Dst]
push    eax
call    esi ; StrCatW
push    [ebp+hMem]
lea     eax, [ebp+Dst]
push    eax
call    esi ; StrCatW
lea     eax, [ebp+Dst]
mov     [ebp+NumberOfBytesWritten], edi
lea     ecx, [eax+2]
```

```
push
lea
push
push
call
mov
add
push
lea
push
call
push
lea
push
call
lea
mov
lea
```



```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We  guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#2:

Zpy8JkO4XemtucTCMOjP5qSFmbF9uUDpYirinzk3WAZuSZJSP62F7fEIFGM6t4WH
GSpsUftOWzIinuN3Z1AOg3epPVGFyeX5K5OA12hSBXYShJQ+dIdtOUW4YYhnXeym
LOXVUVYLENDP1moqavsBieNp3gzh11DoaclYX+3rvvtOIC6p8suw27PjMCN7mwfy
BVqM5S9U+5ctcjFjc1bxkXJLMyUiIAXY1J71zaaJ7P4mATwSn4RZGuoq3L8YKbSe
WYYHrkMp7dCdQaNt2Z3X22af3bc4OAyXD81n5yehdzEsHeDOeMphj5qfcPONUVd7
Ytk4T8bLCSdd/AOu/kCGbFC6CQET9y7DUg==
```

How was the damage done?

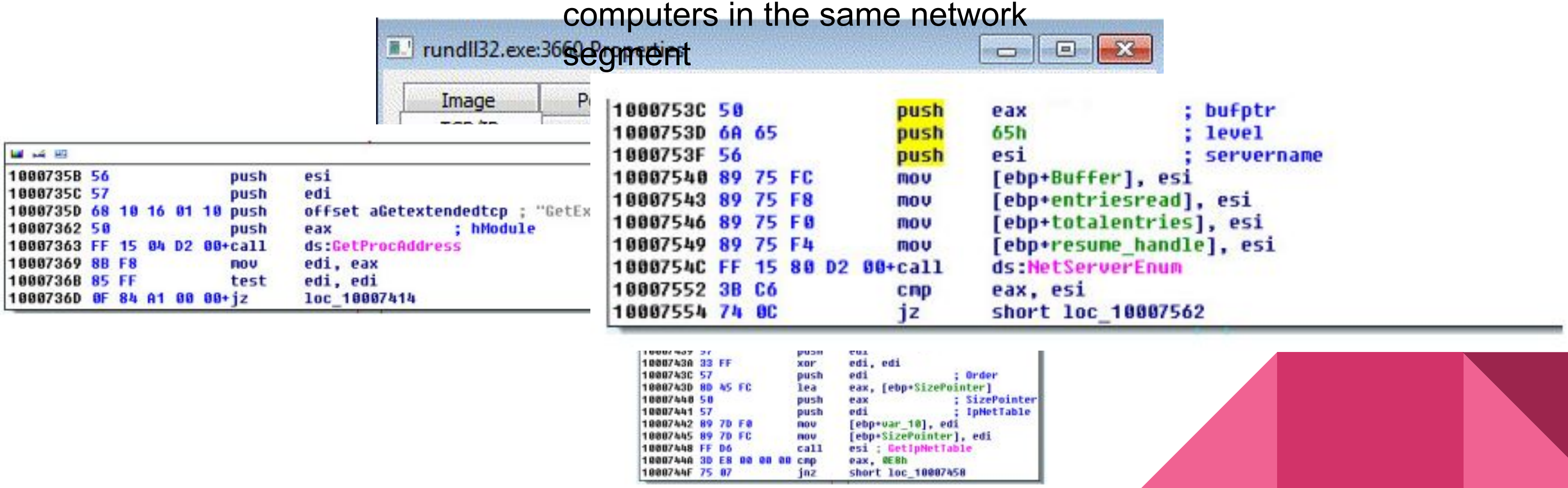
Lateral Movement:

1. GetExtendedTcpTable - which returns a list of active TCP connections.

Enumerating Nearby Hosts

2. GetIPNetTable - which gets the computer's ARP table, listing IP addresses and MAC addresses of computers in the same network segment

3. NetServerEnum - used to enumerate servers in the domain using a windows API function.



```
1000735B 56             push    esi
1000735C 57             push    edi
1000735D 68 10 16 01 10 push    offset aGetextendedtcp ; "GetEx
10007362 50             push    eax              ; hModule
10007363 FF 15 04 D2 00+call    ds:GetProcAddress
10007369 8B F8          mov     edi, eax
1000736B 85 FF          test    edi, edi
1000736D 0F 84 A1 00 00+jz      loc_10007414
```

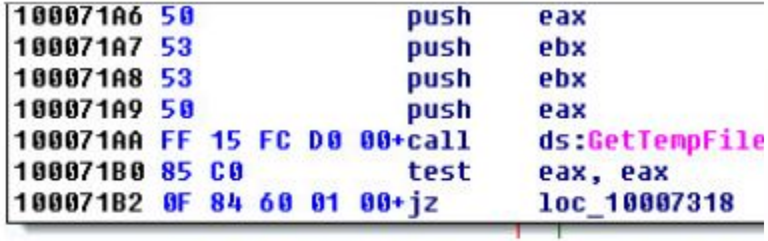
```
1000753C 50             push    eax             ; bufptr
1000753D 6A 65          push    65h             ; level
1000753F 56             push    esi             ; servername
10007540 89 75 FC       mov     [ebp+Buffer], esi
10007543 89 75 F8       mov     [ebp+entriesread], esi
10007546 89 75 F0       mov     [ebp+totalentries], esi
10007549 89 75 F4       mov     [ebp+resume_handle], esi
1000754C FF 15 80 D2 00+call    ds:NetServerEnum
10007552 3B C6          cmp     eax, esi
10007554 74 0C          jz      short loc_10007562
```

```
10007439 57             push    edi
1000743A 33 FF          xor     edi, edi
1000743C 57             push    edi                 ; Order
1000743D 8D 45 FC       lea     eax, [ebp+SizePointer]
10007440 50             push    eax                 ; SizePointer
10007441 57             push    edi                 ; IpNetTable
10007442 89 7D F0       mov     [ebp+var_10], edi
10007445 89 7D FC       mov     [ebp+SizePointer], edi
10007448 FF D6          call    esi ; GetIpNetTable
1000744A 3D E8 00 00 00 cmp     eax, 0E8h
1000744F 75 07          jnz     short loc_10007458
```

How was the damage done?

Lateral Movement:

Gaining local credentials using Mimikatz

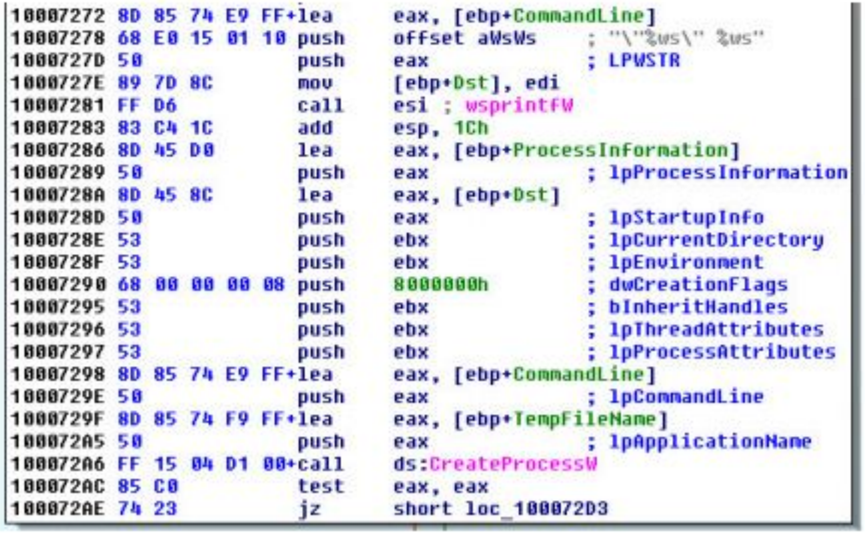


```
100071A6 50               push    eax
100071A7 53               push    ebx
100071A8 53               push    ebx
100071A9 50               push    eax
100071AA FF 15 FC D0 00+call    ds:GetTempFile
100071B0 85 C0            test    eax, eax
100071B2 0F 84 60 01 00+jz      loc_10007318
```

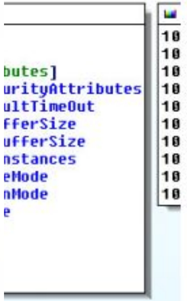
Next, e the

C:\Wi s to a

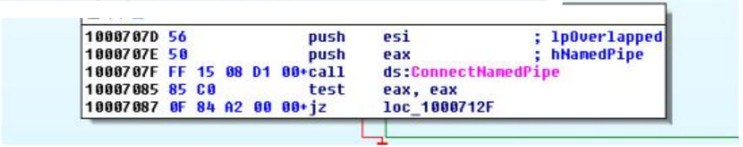
name .



```
10007272 8D 85 74 E9 FF+lea     eax, [ebp+CommandLine]
10007278 68 E0 15 01 10 push    offset aWsWs      ; "\"%ws\" %ws"
1000727D 50             push    eax               ; LPWSTR
1000727E 89 7D 8C       mov     [ebp+Dst], edi
10007281 FF D6          call    esi ; wsprintfW
10007283 83 C4 1C       add     esp, 1Ch
10007286 8D 45 D0       lea     eax, [ebp+ProcessInformation]
10007289 50             push    eax               ; lpProcessInformation
1000728A 8D 45 8C       lea     eax, [ebp+Dst]
1000728D 50             push    eax               ; lpStartupInfo
1000728E 53             push    ebx               ; lpCurrentDirectory
1000728F 53             push    ebx               ; lpEnvironment
10007290 68 00 00 00 08 push    8000000h          ; dwCreationFlags
10007295 53             push    ebx               ; bInheritHandles
10007296 53             push    ebx               ; lpThreadAttributes
10007297 53             push    ebx               ; lpProcessAttributes
10007298 8D 85 74 E9 FF+lea     eax, [ebp+CommandLine]
1000729E 50             push    eax               ; lpCommandLine
1000729F 8D 85 74 F9 FF+lea     eax, [ebp+TempFileName]
100072A5 50             push    eax               ; lpApplicationName
100072A6 FF 15 04 D1 00+call    ds:CreateProcessW
100072AC 85 C0          test    eax, eax
100072AE 74 23          jz      short loc_100072D3
```



```
butes]            10
urityAttributes   10
ultTimeOut        10
fferSize          10
ufferSize         10
nstances          10
eMode             10
nMode             10
e                 10
                  10
```



```
1000707D 56             push    esi               ; lpOverlapped
1000707E 50             push    eax               ; hNamedPipe
1000707F FF 15 08 D1 00+call    ds:ConnectNamedPipe
10007085 85 C0          test    eax, eax
10007087 0F 84 A2 00 00+jz      loc_1000712F
```

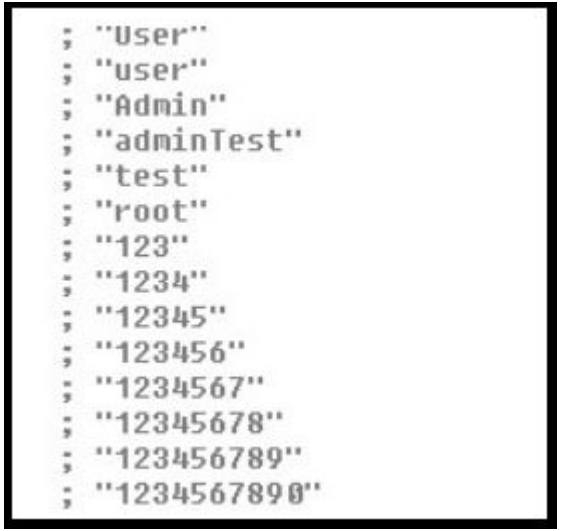
Mimikatz is then executed from the temporary location with the named pipe as a parameter to obtain credentials stored in the local machine.

How was the damage done?

Lateral Movement:

Executing BadRabbit in new hosts

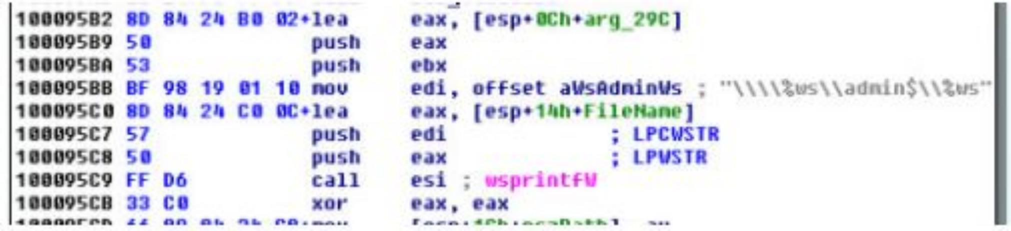
Sample usernames and passwords:



```
; "User"
; "user"
; "Admin"
; "adminTest"
; "test"
; "root"
; "123"
; "1234"
; "12345"
; "123456"
; "1234567"
; "12345678"
; "123456789"
; "1234567890"
```

The malware now attempts to connect to the enumerated servers using obtained credentials. In addition, the malware contains a list of hardcoded usernames and passwords that are used as backup in order to authenticate (so it would not miss out on easily vulnerable targets).

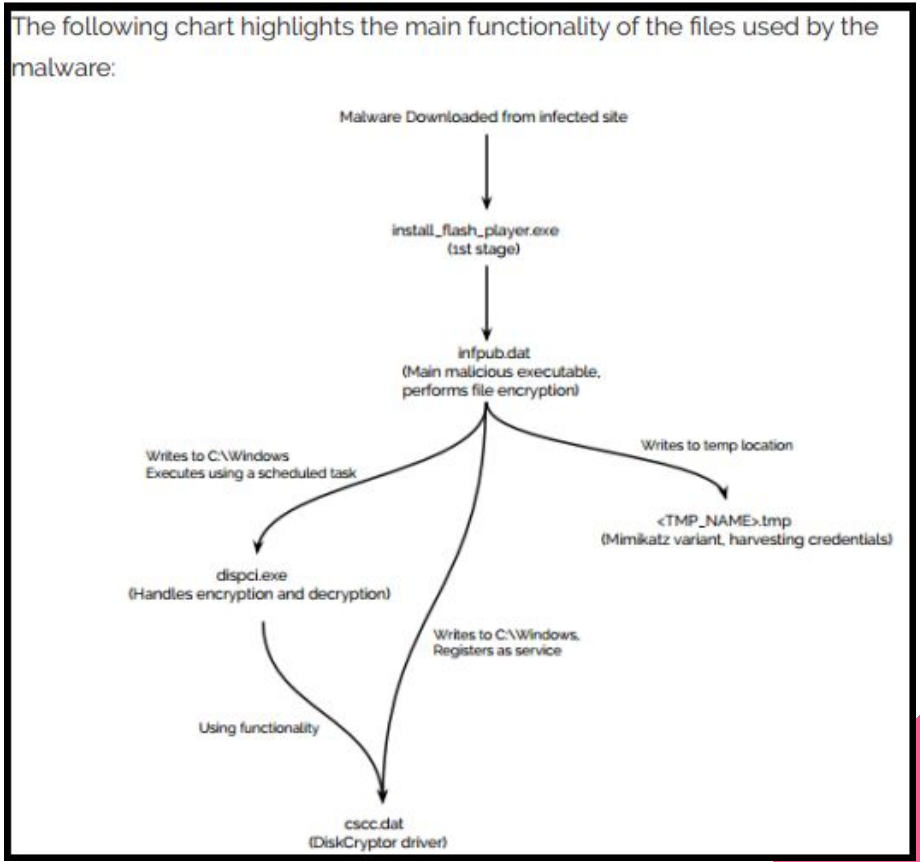
After the malware authenticates, it drops “cscc.dat” and “infpub.dat” in the “\\ admin$” share:



```
100095B2 8D 84 24 B0 02+lea     eax, [esp+0Ch+arg_29C]
100095B9 50             push    eax
100095BA 53             push    ebx
100095BB BF 98 19 01 10 mov     edi, offset aWsAdminWs ; "\\\\%ws\\admin$\\%ws"
100095C0 8D 84 24 C0 0C+lea     eax, [esp+14h+FileName]
100095C7 57             push    edi              ; LPCWSTR
100095C8 50             push    eax              ; LPWSTR
100095C9 FF D6          call    esi ; wsprintfW
100095CB 33 C0          xor     eax, eax
```

And, the saga continues...

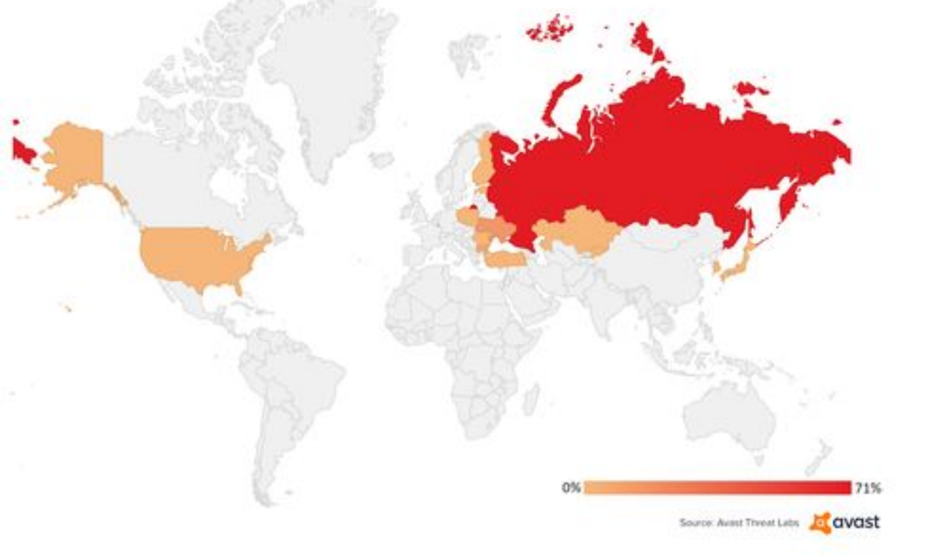
Installation in a nutshell:



The following chart highlights the main functionality of the files used by the malware:

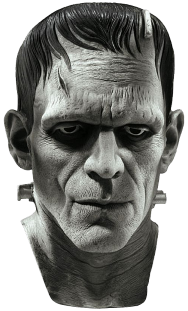
What and Where were the targets?

- May have been a targeted attack aimed at corporate networks.
- Targeted Eastern European countries.
- It infected government, media, transportation and corporate networks in 15 countries, including Russia's Interfax and Fontanka (news agencies), Ukraine's Kiev Metro, the Odessa International Airport, the Odessa naval port and various ministries of infrastructure and finance.

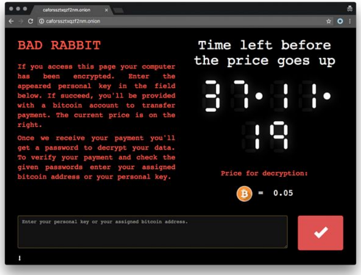


Source: Avast Threat Labs

Frankensteined Petya/NotPetya (aka EternalPetya) Clone ?



- Stolen petya kernel has been substituted with a more advanced DiskCryptor with a legitimate driver (stuxnet strategy?)
- Non destructive attack. The disk can be decrypted with a valid password.
- Does not use the EternalBlue and EternalRomance exploits.
- NotPetya was used a Ukraine-based company’s update server, while Bad Rabbit uses drive-by downloads as an attack vector.
- Both NotPetya and Bad Rabbit use SMB to spread.
- Similar Ransom Screens.
- Bad Rabbit and NotPetya's DLL (dynamic link library) share 67 % of the same code.
- The two campaigns are “linked” to a cybercriminal group named **TeleBots**. (aka **Sandworm group** aka **BlackEnergy**) believed to be a subunit of APT28/PawnStorm/**Fancy Bear**/Sofacy/Tsar Team/Strontium/Sednit.
- **Associated with Russian military intelligence (GRU)**



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

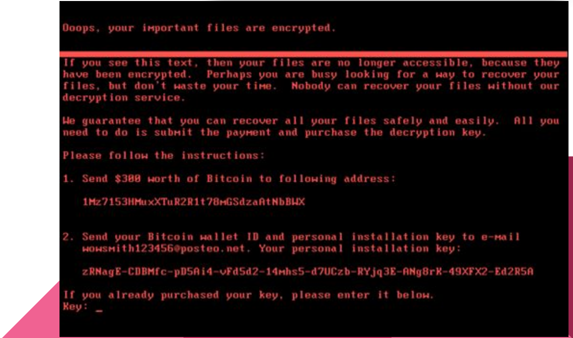
37:11:19

Price for decryption:

₿ = 0.05

Enter your personal key or your assigned bitcoin address.

✓



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

How to Mitigate Damage

- ★ Block the execution of files c:windowsinfpub.dat and c:Windowscscc.dat using Group Policy.
- ★ Disable WMI service (if it’s possible in your environment) to prevent the malware from spreading over your network.

Tips for everyone:

- ➢ Backup your data.
- ➢ Don’t pay the ransom.
- ➢ Lock down admin accounts.
  Run as a standard user.
- ➢ **Educate Users.**
- ➢ **Don’t just click. Double check.**

Sources & Reports:

- https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/
- https://securelist.com/bad-rabbit-ransomware/82851/
- https://threatpost.com/badrabbit-ransomware-attacks-hitting-russia-ukraine/128593/
- https://www.bleepingcomputer.com/news/security/bad-rabbit-ransomware-outbreak-hits-eastern-europe/
- https://unit42.paloaltonetworks.com/threat-brief-information-bad-rabbit-ransomware-attacks/
- https://threatvector.cylance.com/en_us/home/threat-spotlight-bad-rabbit-ransomware.html
- https://www.nyotron.com/collateral/Nyotron-BadRabbit-Report_FINAL.pdf
- https://sourceforge.net/projects/diskcryptor/
- https://www.offensive-security.com/metasploit-unleashed/mimikatz/
- https://arstechnica.com/information-technology/2017/06/notpetya-developers-obtained-nsa-exploits-weeks-before-their-public-leak/
- https://blog.skyboxsecurity.com/bad-rabbit-uses-social-engineering/
- https://www.darkreading.com/endpoint/bad-rabbit-dies-down-but-questions-remain/d/d-id/1330224
- https://www.tripwire.com/state-of-security/featured/october-2017-the-month-in-ransomware/
- https://www.theregister.co.uk/2017/10/26/bad_rabbit_post_mortem/
- https://www.zdnet.com/article/bad-rabbit-ten-things-you-need-to-know-about-the-latest-ransomware-outbreak/
- https://threatpost.com/bad-rabbit-linked-to-expetrnot-petya-attacks/128611/
- https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/