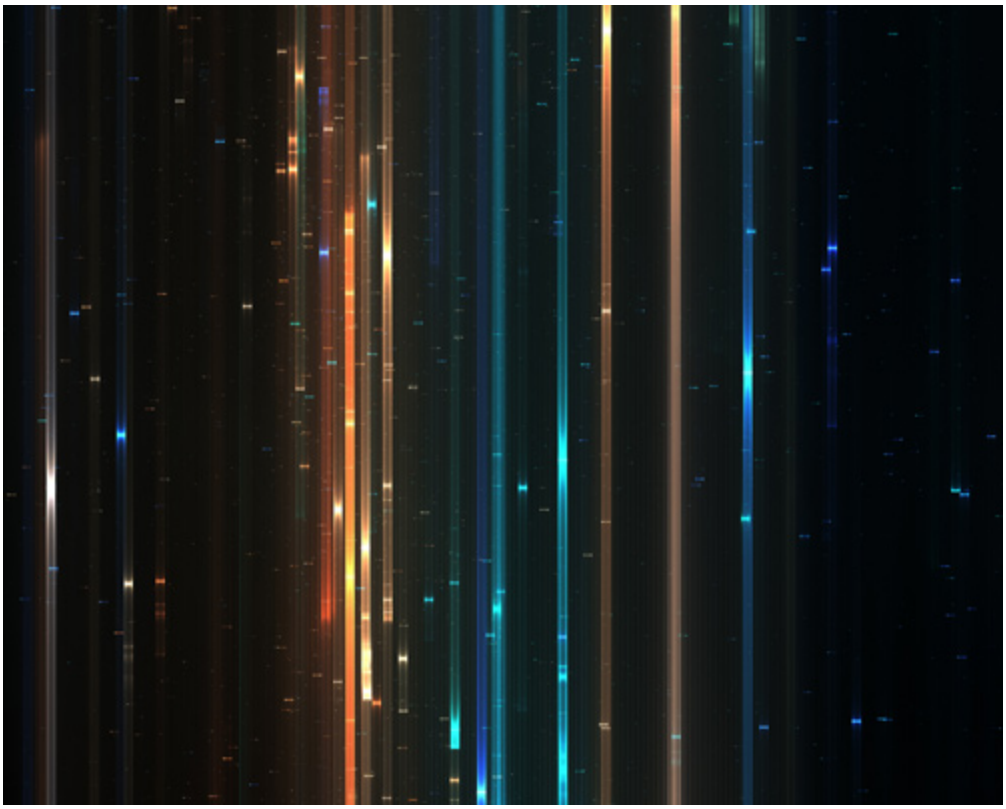
# The return of Mamba ransomware

securelist.com/the-return-of-mamba-ransomware/79403/

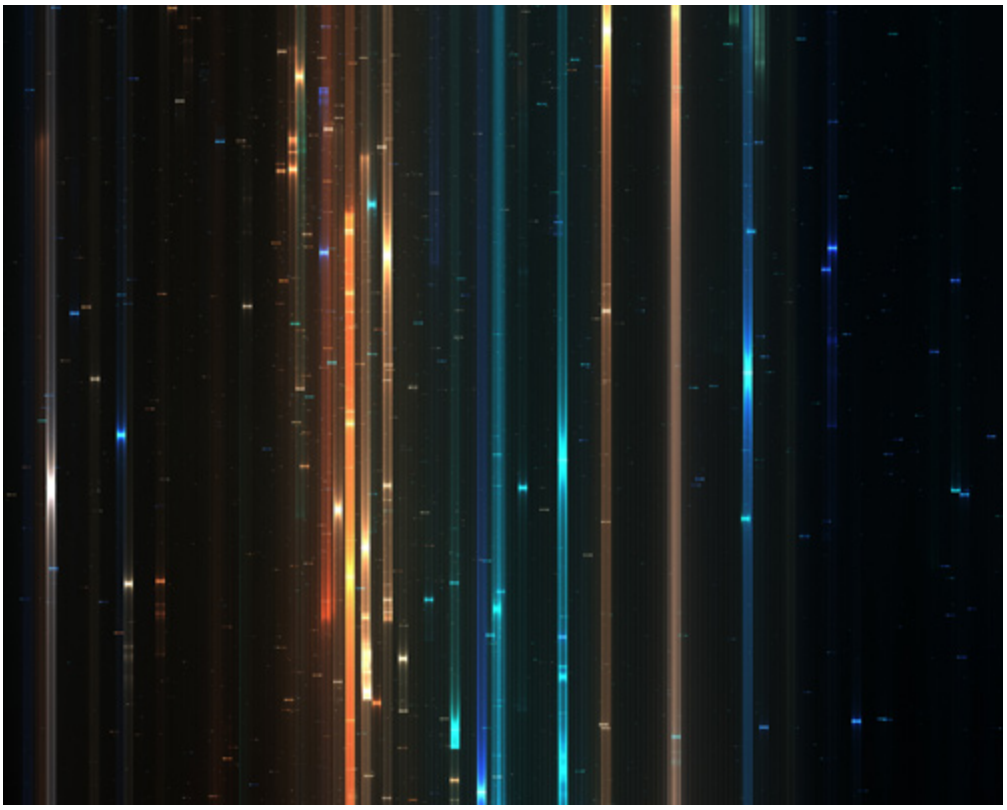


Malware descriptions

Malware descriptions

09 Aug 2017

minute read



Authors

- Expert Anton Ivanov
- Expert Orkhan Mamedov

At the end of 2016, there was a major attack against San Francisco's Municipal Transportation Agency. The attack was done using Mamba ransomware. This ransomware uses a legitimate utility called DiskCryptor for full disk encryption. This month, we noted that the group behind this ransomware has resumed their attacks against corporations.


## Attack Geography

We are currently observing attacks against corporations that are located in:

- Brazil
- Saudi Arabia

## Attack Vector

As usual, this group gains access to an organization's network and uses the psexec utility to execute the ransomware. Also, it is important to mention that for each machine in the victim's network, the threat executor generates a password for the DiskCryptor utility. This password is passed via command line arguments to the ransomware dropper.

```
C:\TEMP\721.exe longPassword /accepteula
```

Example of malware execution

## Technical Analysis

In a nutshell, the malicious activity can be separated into two stages:

Stage 1 (Preparation):

- Create folder "*C:\xampp\http*"
- Drop DiskCryptor components into the folder
- Install DiskCryptor driver
- Register system service called **DefragmentService**
- Reboot victim machine

Stage 2 (Encryption):

- Setup bootloader to MBR and encrypt disk partitions using DiskCryptor software
- Clean up
- Reboot victim machine

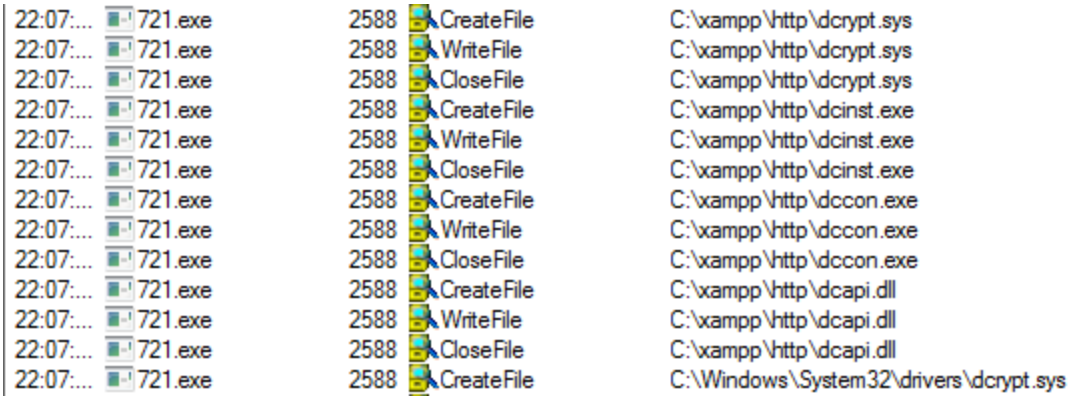
### Stage 1 (Preparation)

As the trojan uses the DiskCryptor utility, the first stage deals with installing this tool on a victim machine. The malicious dropper stores DiskCryptor's modules in their own resources.

| Type | Size | ID | Name |
|---|---|---|---|
| 32DCAPI.DLL | 193024 | 2057 | 105 |
| 32DCCON.EXE | 61736 | 2057 | 104 |
| 32DCINST.EXE | 10752 | 2057 | 103 |
| 32DCRYPT.SYS | 181448 | 2057 | 101 |
| 64DCAPI.DLL | 211968 | 2057 | 110 |
| 64DCCON.EXE | 59688 | 2057 | 109 |
| 64DCINST.EXE | 9728 | 2057 | 108 |
| 64DCRYPT.SYS | 210632 | 2057 | 106 |
| Manifest | 392 | 1033 | 1 |

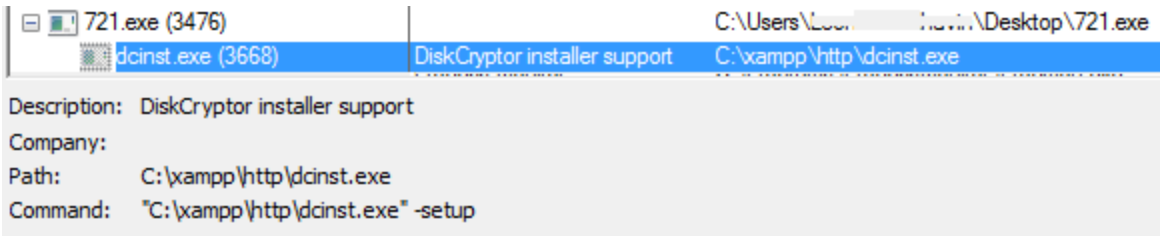
DiskCryptor modules

Depending on OS information, the malware is able to choose between 32- or 64-bit DiskCryptor modules. The necessary modules will be dropped into the "*C:\xampp\http*" folder.



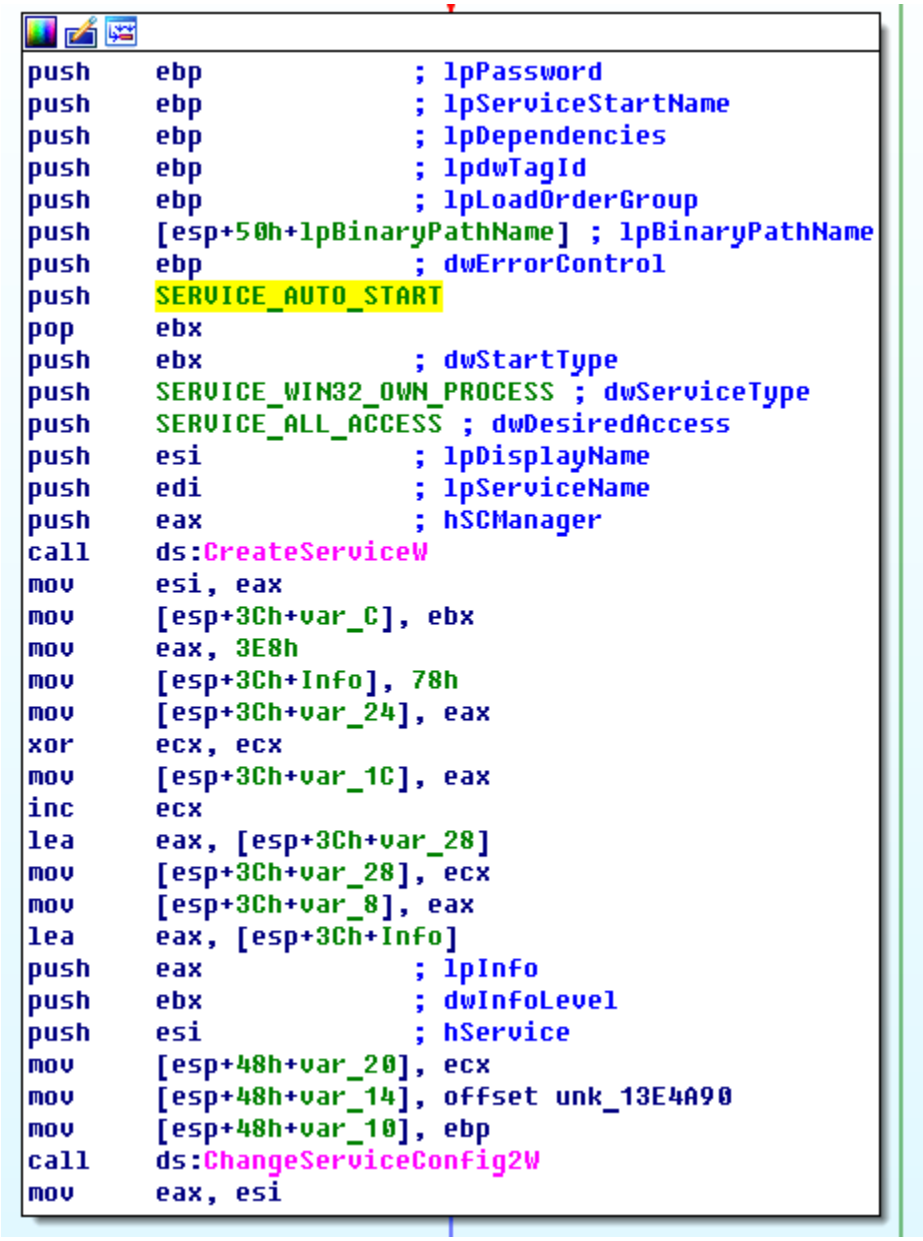

The malware drops the necessary modules

After that, it launches the dropped DiskCryptor installer.




The call of the DiskCryptor installer

When DiskCryptor is installed, the malware creates a service that has SERVICE_ALL_ACCESS and SERVICE_AUTO_START parameters.



```
push    ebp             ; lpPassword
push    ebp             ; lpServiceStartName
push    ebp             ; lpDependencies
push    ebp             ; lpdwTagId
push    ebp             ; lpLoadOrderGroup
push    [esp+50h+lpBinaryPathName] ; lpBinaryPathName
push    ebp             ; dwErrorControl
push    SERVICE_AUTO_START
pop     ebx
push    ebx             ; dwStartType
push    SERVICE_WIN32_OWN_PROCESS ; dwServiceType
push    SERVICE_ALL_ACCESS ; dwDesiredAccess
push    esi             ; lpDisplayName
push    edi             ; lpServiceName
push    eax             ; hSCManager
call    ds:CreateServiceW
mov     esi, eax
mov     [esp+3Ch+var_C], ebx
mov     eax, 3E8h
mov     [esp+3Ch+Info], 78h
mov     [esp+3Ch+var_24], eax
xor     ecx, ecx
mov     [esp+3Ch+var_1C], eax
inc     ecx
lea     eax, [esp+3Ch+var_28]
mov     [esp+3Ch+var_28], ecx
mov     [esp+3Ch+var_8], eax
lea     eax, [esp+3Ch+Info]
push    eax             ; lpInfo
push    ebx             ; dwInfoLevel
push    esi             ; hService
mov     [esp+48h+var_20], ecx
mov     [esp+48h+var_14], offset unk_13E4A90
mov     [esp+48h+var_10], ebp
call    ds:ChangeServiceConfig2W
mov     eax, esi
```

The creation of the malicious service's function

The last step of Stage 1 is to reboot the system.

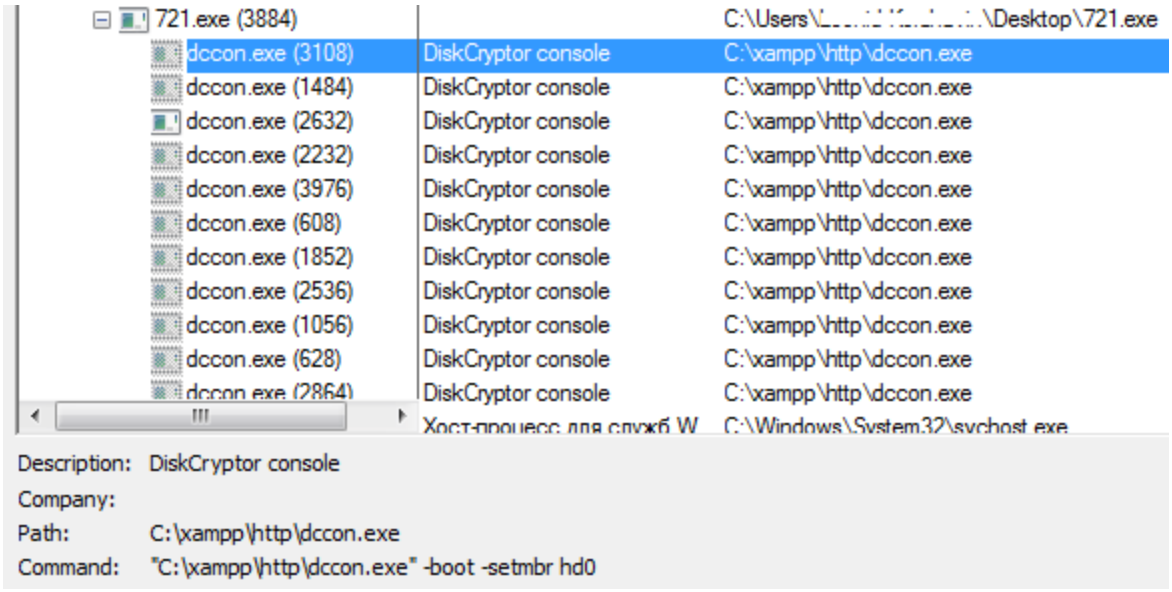
```
BOOL AdjustTokenPrivileges_ExitWindowsEx()
{
  HANDLE v0; // eax@1
  BOOL result; // eax@2
  HANDLE TokenHandle; // [esp+8h] [ebp-18h]@1
  struct _TOKEN_PRIVILEGES NewState; // [esp+Ch] [ebp-14h]@3

  v0 = GetCurrentProcess();
  if ( !OpenProcessToken(v0, 0x28u, &TokenHandle)
    || (LookupPrivilegeValueW(0, L"SeShutdownPrivilege", NewState.Privileges),
        NewState.PrivilegeCount = 1,
        NewState.Privileges[0].Attributes = 2,
        AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0, 0, 0),
        GetLastError()) )
  {
    result = 0;
  }
  else
  {
    result = ExitWindowsEx(EWX_FORCE|EWX_REBOOT, DISP_E_MEMBERNOTFOUND) != 0;
  }
  return result;
}
```

Force reboot function

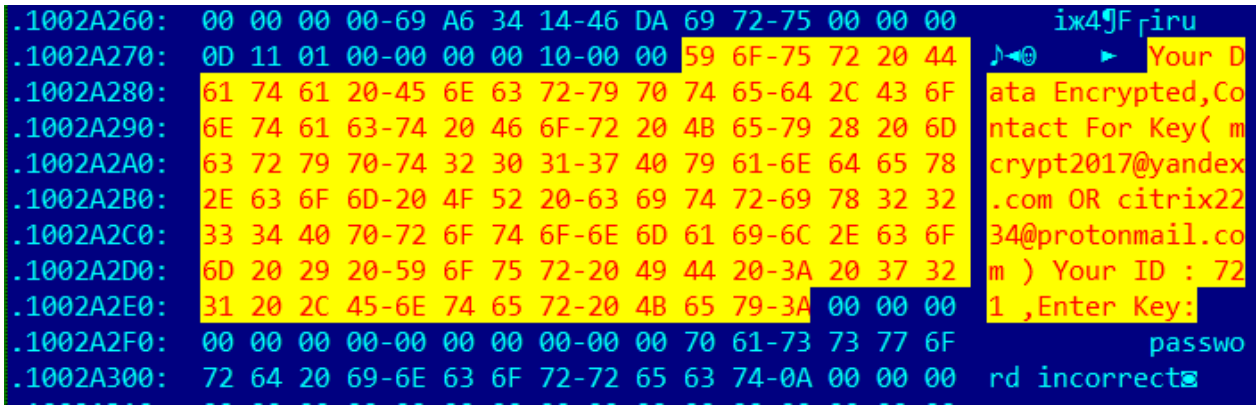
## Stage 2 (Encryption)

Using the DiskCryptor software, the malware sets up a new bootloader to MBR.



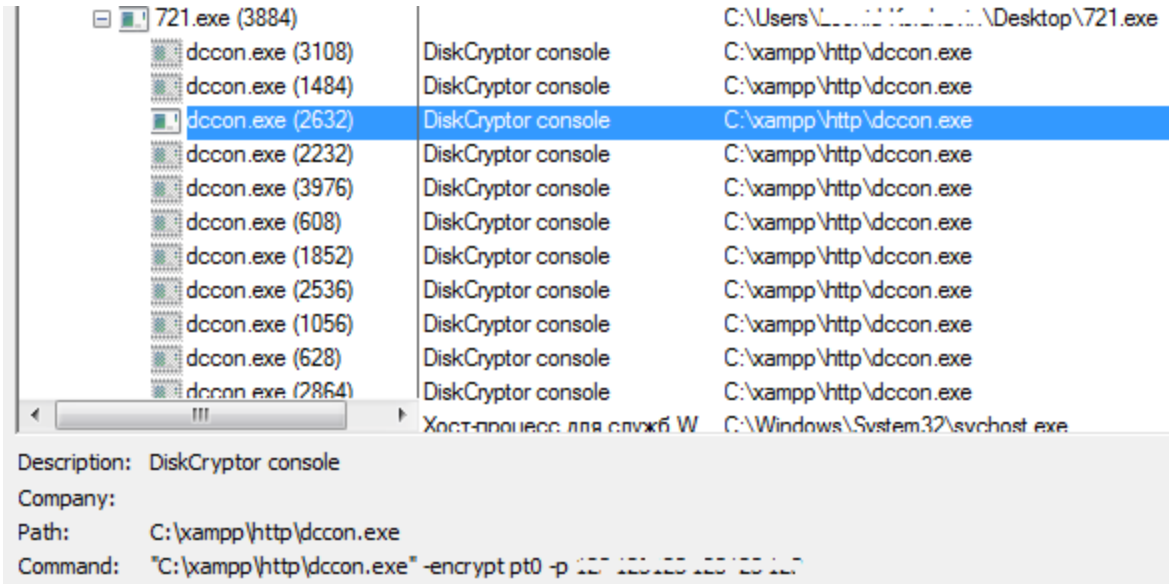

The call for setting up a bootloader to MBR

The bootloader contains the ransom message for the victim.



Ransomware note

After the bootloader is set, disk partitions would be encrypted using a password, previously specified as a command line argument for the dropper.



The call tree of encryption processes

When the encryption ends, the system will be rebooted, and a victim will see a ransom note on the screen.

Ransom notes

Kaspersky Lab products detect this threat with the help of the System Watcher component with the following verdict: PDM:Trojan.Win32.Generic.

## Decryption

Unfortunately, there is no way to decrypt data that has been encrypted using the DiskCryptor utility because this legitimate utility uses strong encryption algorithms.

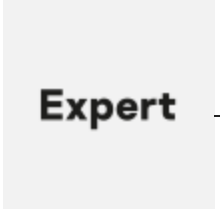
## IOCs:

79ED93DF3BEC7CD95CE60E6EE35F46A1

- Encryption
- Malware Descriptions
- Malware Technologies
- MBR
- Ransomware
- Targeted attacks

Authors


- 

Anton Ivanov
- 

Orkhan Mamedov


The return of Mamba ransomware

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

## GReAT Ideas. Balalaika Edition

From the same authors

## Sodin ransomware exploits Windows vulnerability and processor architecture

## KeyPass ransomware

## SynAck targeted ransomware uses the Doppelgänging technique


## Mining is the new black


## Bad Rabbit ransomware