Win32/Bypass Abstract

Written by FraMe (frame at kernelpanik.org)

0.- Introduction

This document is a technical abstract of paper "Win32/Bypass: Anulando la detección de ficheros". The main objective is to explain few of techniques to allow bypassing security measures of many antivirus programs. For a better understanding, it´s recommended to read the original paper in Spanish, located at http://www.kriptopolis.org/la-eficacia-de-diez-antivirus-en-entredicho

1.- Techniques Used.

Thought the original paper I explain several techniques to go over the antivirus protection. This is a sum up of those techniques explained in the main paper:

1.1.- Unicode Directories

One simply technique is to use UNICODE paths. For example using "F:\Documents and Settings\frame\Mis documentos\FSPruebas\test♪".

1.2.- Path extension with 8.3

It is another technique in which we extend the length of a PATH, limited in Win32 to 260 bytes, using 8.3 format.

F:\Documents and Settings\frame\Mis documentos\FSPruebas\AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA> **mkdir subdirectorio**

El nombre del archivo o la extensión es demasiado largo.

F:\Documents and Settings\frame\Mis documentos\FSPruebas> **cd AAAAAA~1**

F:\Documents and Settings\frame\Mis documentos\FSPruebas\AAAAAA~1> **mkdir subdirectorio**

F:\Documents and Settings\frame\Mis documentos\FSPruebas\AAAAAA~1> **cd subdirectorio**

F:\Documents and Settings\frame\Mis documentos\FSPruebas\AAAAAA~1\subdirectorio> **echo "hola" > fichero**

F:\Documents and Settings\frame\Mis documentos\FSPruebas\AAAAAA~1\subdirectorio> **type fichero**
"hola"

1.3.- Path extension with remote shared units

The third technique extends a PATH using remote shared units.

F:\Documents and Settings\frame> **net share**

Nombre Recurso Descripción

Zero F:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
0\0\0\0\0\0\0\0\0

F:\> **mkdir \\Hawking\Zero\Prueba**
F:\>

1.4.- Path of 260 bytes.

In this technique the path's length is 260 bytes instead of 256, with the next format: "Drive" + ":" + "\" + 256 chars + "\0".

1.5.- Content execution at "noexec-files"

You can execute no-executable files from CMD.EXE (ie. txt or .log). The files must contain Win32PE file format.

```
C:\>copy C:\WINDOWS\system32\ftp.exe C:\ftp.txt
      1 archivos copiados.

C:\>ftp.txt
ftp> lcd
Directorio local ahora C:\.
```

1.6.- Resident Services Supression

When service's files aren't protected, it's possible to rename the service. In this case, the next reboot, will disable antivirus protection.

1.7.- StartUp´s Race Condition.

The inclusion of viral content within the "Start Up" may cause that this content is executed before the antivirus completes its load.

1.8.- Safeboot Init

Finally, the modification of the file boot.ini, allows the execution of viral content, and suppress any antivirus protection, when rebooting forces safeboot init.

```
C:\> type C:\boot.ini
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/fastdetect /SAFEBOOT:NETWORK
```

2.- Antivirus Analyzed

The evaluated antiviruses have been:

- BitDefender 8 Standard y BitDefender 10 Plus
- AVG 7.5.1 Free
- Avast! v4.7 Personal
- Panda Antivirus 2005 y Panda Antivirus 2007
- Norton Antivirus 2007
- Nod32 v2.5
- Zone Alarm Antivirus v6.5
- Kaspersky v6.0.1

The aspects analyzed during the tests are two:

- **Resident Shield:** the objective has been to determine if a procedure, or several, exist to exceed the protection, allowing the **execution** of "viral" content in the system.
- **File Scan:** the objective has been to determine if a procedure, or several, exist to exceed the protection, allowing **hide** "viral" content in the system.

2.1.- BitDefender 8 Standard

In order to exceed the protection offered by the resident shield of BitDefender 8 Standard we need shared resources with format UNICODE. In example: the execution of content from a folder shared in network with name "\\hawking\biohazard■" cannot be detected, or aborted, allowing the execution of viral content.

The analysis of files fails in paths with greater length to the maximum size of path established in the Win32 system. The creation of paths using "8.3 technique", described above, suppresses the detection of virus in those paths.

2.2.- BitDefender 10 Plus

The protection offered by the resident shield of "BitDefender 10 Plus" is exceeded from any folder with characters UNICODE. In example: the execution of content from a path like the following one, "C:\test-avirs\AAAAAA~1\privatefolder■", cannot be detected, or aborted, allowing the execution of viral content.

The analysis of files fails in paths with greater length to the maximum size of path established in the Win32 system. The creation of paths using "8.3 technique", described above, suppresses the detection of virus in those paths.

2.3.- AVG 7.5.1 Free

Resident´s shield of "AVG 7.5.1 Free" only checks files with certain extensions. The execution of content using the technique described in point 1.4, makes possible the execution of viral content. This problem can be corrected by forcing the scan of all file extensions.

The analysis of files fails in paths with greater length to the maximum limit of path established in the Win32 system. The creation of paths using "8.3 technique", described above, suppresses the detection of virus in those paths.

2.4.- Avast! 4.7 Personal

Resident´s shield of "Avast! 4.7 Personal" only checks files with certain extensions. The execution of content, using the technique described in point 1.4, makes possible the execution of viral content. This problem can be corrected: we need forcing the scan of all file extensions.

The analysis of files fails on shared folders with format UNICODE, for example: "\\hawking\biohazard■".

2.5.- Panda Antivirus 2005

Resident´s Shield, of Panda Antivirus 2005, can't detect execution in paths of more than 256 characters, so paths of 260 characters allow the execution of viral content.

The analysis of files fails in paths with greater length to the maximum limit of path established in the Win32 system. The creation of paths using "8.3 technique", described above, suppresses the detection of virus in those paths.

2.6.- Panda Antivirus 2007

Resident´s shield of "Panda Antivirus 2007" only checks files with certain extensions. The execution of content, using the technique described in point 1.4, makes possible the execution of viral content.

Also a buffer overflow exists when executes contents from shared networks associated to local units.

The analysis of files fails in paths with greater length to the maximum limit of path established in the Win32 system. The creation of paths using "8.3 technique", described above, suppresses the detection of virus in those paths.

2.7.- Norton Antivirus 2007

Resident´s shield of "Norton Antivirus 2007" only checks files with certain extensions. The execution of content, using the technique described in point 1.4, makes possible the execution of viral content. This problem can be corrected by forcing the scan of all file extensions.

Problems in the file analysis have not been detected.

2.8.- Nod32 v2.5

Resident´s Shield, of Nod32, can be deactivated since it does not protect its own files.

There also exists a race condition in the resident shield. This race condition can be exploited by using the technique of point 1.7

The analysis of files fails in paths with greater length to the maximum limit of path established in the Win32 system. The creation of paths using "8.3 technique", described above, suppresses the detection of virus in those paths.

Also a buffer overflow exists when nested folders are analyzed.

2.9.- Zone Alarm v6.5

Zone Alarm can be deactivated using the technique described in point 1,8, because it does not protect the access to the file boot.ini

Problems in the file analysis have not been detected.

2.10.- Kaspersky v6.0.1

Kaspersky can be deactivated using the technique described in point 1,8, because it does not protect the access to the file boot.ini

In addition, the file "avp.exe" allows to overwrite its own protected files.

Problems in the file analysis have not been detected.

3.- Comparative Summary

TECHNIQUES
1.- Unicote Paths
2.- 8.3 Extension
3.- 260 bytes Path.
4.- No-Exec Execution
5.- Resident Shield Supression
6.- Race Condition
7.- Safeboot Init

Simbols

✘ Vulnerable
✘ Not Verified
✓ Not vulnerable

	UNICODE	8.3	260bytes	NO-EXEC	Supress	Race-Cond	Safeboot
BitDefender 8	✘	✘	✓	✘	✘	✘	✘
BitDefender 10	✘	✘	✓	✘	✘	✘	✘
AVG 7.5.1	✓	✘	✓	✘	✘	✘	✘
Avast! 4.7	✘	✓	✓	✘	✘	✘	✘
Panda 2005	✓	✘	✘	✘	✘	✘	✘
Panda 2007	✓	✘	✓	✘	✘	✘	✘
Norton 2007	✓	✓	✓	✘	✘	✘	✘
Nod32 2.5	✓	✘	✓	✓	✘	✘	✘
ZoneAlarm 6.5	✓	✓	✓	✓	✓	✓	✘
Kaspersky 6	✓	✓	✓	✓	✓	✓	✘

4. Legal Info