



VIRUS FIZZER

"Fizzer registriert alles von seinem Opfer getippte, und speichert es in einer Datei, die später durch einen Eindringling heruntergeladen werden kann, der so Daten, die die Sicherheit und Privatsphäre des infizierten Benutzers betreffen, erhält."

1. WAS IST ES?

Fizzer ist ein gefährlicher Wurm, der dazu geschaffen ist, die vom Benutzer gedrückten Tasten zu registrieren und in einer Textdatei zu speichern.

Auf diese Art kann jeder Hacker, der sich Zugang zu dieser Datei verschafft, vertrauliche Daten dieses Benutzers erfahren, wie z.B. Passwortcodes für gewisse Dienste (Internet chat, Email, Passwort zu Bankkonten, usw.).

Ausserdem ist Fizzer fähig, gewisse Prozesse, die prinzipiell mit der Handlung des Antivirus verbunden sind, zu beenden.

Fizzer verbreitet sich hauptsächlich durch Chat-Programme wie IRC und Email. Es versendet eine Kopie seiner selbst an alle im Adressbuch von Windows gefundenen Adressen.

2. WAS FÜR ARTEN GIBT ES?

Alias: W32/Fizzer@MM (McAfee), W32/Fizzer-A (Sophos), W32/Fizzer (Panda Software), WORM_FIZZER.A (Trend Micro), W32.HLLW.Fizzer@mm (Symantec), Win32.Fizzer.A@mm (Bit Defender), W32/Fizzer (Hacksoft), Fizzer (F-Secure), I-Worm.Fizzer (Kaspersky (viruslist.com)), Win32.Fizzer (Computer Associates), Win32/Fizzer.A@mm (RAV)

3. WIE FUNKTIONIERT ER?

Die verschiedenen Bestandteile des Virus übernehmen folgende Aufgaben:

1. Registrieren der Adressen des Outlook Adressbuches
2. Registrieren der Adressen des Adressbuches von Windows (WAB)
3. Aufnahme der im lokalen System gefunden Adressen
4. Schaffen von Adressen nach dem Zufallsprinzip.
5. Launcher für IRC bot (Internet Relay Chat)
6. Launcher für AIM bot (AOL Instant Messenger)
7. Keylogger
8. Wurm für KaZaA
9. HTTP Server
10. Beender für Antivirus-Software.
11. Der Wurm hat seinen eigenen SMTP Motor und kann den im Register des Betriebssystems konfigurierten verwenden.
12. Er kommt in einer Datei, die einer der verschiedenen Nachrichten anhängt, die er zur Verbreitung nutzt. Der Inhalt des Feldes From (Von) ist nicht notwendigerweise der Originalabsender. Der Inhalt der Nachricht und der Betreff können über verschiedene Themen handeln. Die Endungen der anhängenden Dateien können (.com, .exe, .pif, .scr) sein.



Die **Nachrichten** sind den folgenden ähnlich:

Subject: why?

Body: The peace

Attachment: desktop.scr

Subject: Re: You might not appreciate this...

Body: lautlach

Attachment: service.scr

Subject: Re: how are you?

Body: I sent this program (Sparky) from anonymous places on the net

Attachment: Jesse20.exe

Subject: Fwd: Mariss995

Body: There is only one good, knowledge, and one evil, ignorance.

Attachment: Mariss995.exe

Subject: Re: The way I feel - Remy Shand

Body: Nein

Attachment: Jordan6.pif

Wenn der Anhang ausgeführt wird, wird er folgende **Aufgaben** durchführen:

1. Er zieht Dateien über das Verzeichnis ab (%WinDir%).
 - a. initbak.dat (220,160 bytes) - Kopie des Wurms
 - b. iservc.exe (220,160 bytes) - Kopie des Wurms
 - c. ProgOp.exe (15,360 bytes) - Prozessmanager
 - b. iservc.dll (7,680 bytes) - temporärer Treiber.



2. Er schafft folgenden Eintrag im Register, um zur gleichen Zeit wie Windows hochgefahren zu werden:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

```
Run "SystemInit" = C:\WINDOWS\ISERVC.EXE
```

3. Er verändert das Register, um die Ausführung des Wurms bei jeder Öffnung einer TXT-Datei zu hervorzurufen:

```
HKEY_CLASSES_ROOT\txtfile\shell\open\command
```

(Vorgegeben) =

```
c:\windows\PROGOP.EXE 0 7 ' c:\windows\notepad.exe %1'
```

```
'c:\windows\INITBAK.DAT' 'c:\windows\ISERVC.EXE'
```

4. Er wiederholt vorige Handlung für folgenden Registrierungseintrag:

```
HKCR\Applications\ProgOp.exe\shell\Open\Command
```

(Vorgegeben) =

```
c:\windows\PROGOP.EXE 0 7 ' c:\windows\notepad.exe %1'
```

```
'c:\windows\INITBAK.DAT' 'c:\windows\ISERVC.EXE'
```

5. In Betriebssystemen WinNT/2K/XP schafft er einen S1TRACE genannten Vorgang.

BEMERKUNG: In allen Fällen kann „C:\Windows“ je nach installiertem Betriebssystem anders sein (mit diesem Namen vorgegeben in Windows 9x/ME und XP und als „C:\WinNT“ bei Windows NT/2000).



Massensendungsroutine

Es nutzt seinen eigenen SMTP Motor, um sich an alle Adressen im Outlook Adressbuch zu versenden, und an zufällig kreierte Adressen, wie folgende:

- Zufällig gewählte Namen einer internen Liste des Wurms
- Zufällig gewählte Nummern
- Zufällig gewählte Domainnamen (@dominio) aus folgender interner Liste:

aol.com

earthlink.com

gte.net

hotmail.com

juno.com

msn.com

netzero.com

yahoo.com

Den Betreff, Nachricht und Namen der anhängenden Datei erstellt er per Zufall aus einer Auswahl von Texten, wie:

"So how are you?"

"Check it out"

"There is only one good, knowledge, and on evil, ignorance"

"I sent this program (sparky) from anonymous places on the net"

"you must not show this to anyone"

"Today is a good day to die"

"thought I'd let you know"

"The way to gain a good reputation is to endeavor to be what you desire ..."

"Filth is a death"

"wie geht es Ihnen?"

"Philosophy imputes, reinterprets faith"

"If you don't like it, just delete it"



"delete this as soon as you lokk at it"

"Did you ever stop to think that viruses are good for the economy? ..."

"the incredibly bright faith"

"you don't have to if you don't want to"

"I wonder what can be so bad ..."

"Watchin' the game, having a bud."

"the attachment is only for you to look at"

"Let me know what you think of this..."

IRC Bot:

Er versendet auch Kopien an die Benutzer, die die gleichen Chat-Kanäle wie das Opfer verwenden.

Ausserdem versendet er PINGS an verschiedene IRC Server (normalerweise durch den Port TCP/6667). PING (Packet Internet Groper) ist ein Kommando, dass benutzt wird, um die Verbindung zu einem oder mehreren Hosts mittels der Übersendung eines Bytpakets, das wie ein Echo wiedergegeben wird, zu überprüfen.

Wenn es eine Antwort erhält, verbindet es sich mit einem Kanal durch verschiedene Namen aus einer internen Liste und erwartet die Anweisungen des Angreifers, wobei es wie ein BOT reagiert (Kopie eines Nutzers in einem IRC Kanal, das zur Beantwortung gewisser Kommandos, die ihnen fernübertragen werden, vorbereitet ist, so dass mehrere koordinierte Handlungen gleichzeitig ablaufen).

Folgende ist eine Liste von **IRC Servern**:

1. irc2p2pchat.net
2. irc.idigital-web.com
3. irc.cyberchat.org
4. irc.othernet.org
5. irc.beyondirc.net
6. irc.chatx.net
7. irc.cyberarmy.com
8. irc.gameslink.net



Verbreitung durch KaZaA:

Um sich durch dieses Dateienaustauschprogramm von Punkt zu Punkt zu verteilen, benutzt es folgenden Vorgang:

Es schafft innerhalb des Shared Folders mehrere Kopien seiner selbst. Diese Kopien erhalten Zufallsnamen.

Andere Benutzer des KaZaA haben Zugang zu diesem Shared Folder. So laden sie unwissentlich einige der genannten Dateien herunter, häufig im Glauben, dass es sich um ein interessantes Programm handelt. In Wirklichkeit laden sie sich eine Kopie des Wurms herunter.

Wenn die Benutzer die heruntergeladenen Programme ausführen, wird ihr Computer infiziert.

Keylogger: Ergreifer von Tastenanschlägen.

Es erfasst die vom Benutzer durchgeführten Tastenanschläge. Fizzer speichert diese Anschläge in einer Textdatei, die er selbst in Windows unter dem Namen ISERVC.KLG geschaffen hat. Danach verschlüsselt er diese. Wenn ein Hacker diese Datei erhält, hat er Zugang zu den vertraulichen Daten des Benutzers des infizierten Computers, wie z.B. Internetpasswörter, Bankkonten, usw.

Beender für Antivirus-Software

Zur Vermeidung einer möglichen Detektierung beendet er Vorgänge, die in ihren Namen folgenden String beinhalten:

- ANTIV
- AVP
- F-PROT
- NMAIN
- SCAN
- TASKM
- VIRUS
- VSHW
- VSS



4. WIE BESEITIGT MAN IHN?

Antivirus

1. Aktualisieren Sie Ihren Antivirus auf den neuesten Stand
2. Führen Sie es in Scan-Mode durch, untersuchen Sie alle Festplatten Ihres Computers
3. Löschen Sie die als infiziert gefundenen Dateien

Löschung per Hand der vom Virus geschaffenen Dateien

Von Windows Explorer aus, suchen und löschen Sie folgende Dateien:

c:\windows\ISERVC.KLG
c:\windows\INITBAK.DAT
c:\windows\ISERVC.EXE
c:\windows\ISERVC.DLL
c:\windows\PROGOP.EXE

Klicken Sie mit dem rechten Mausknopf auf den Icon „Müllkorb“ auf dem Desktop und wählen Sie „Müllkorb entleeren“.

Löschen Sie alle den genannten Emails ähnliche Nachrichten.

Register editieren

1. Führen Sie den Registrierungseditor durch:

Start, ausführen, tippen Sie ‚regedit‘ und drücken Sie ENTER

2. Im linken Feld des Registrierungseditors klicken Sie auf das + Zeichen und öffnen Sie folgenden Pfad

HKEY_LOCAL_MACHINE
\SOFTWARE
\Microsoft
\Windows
\CurrentVersion
\Run

3. Klicken Sie im Verzeichnis ‚Run‘ und im rechten Feld, unter der Spalte ‚Name‘, suchen und löschen Sie folgenden Eintrag:
SystemInit

4. Im linken Feld des Editors, klicken Sie auf das + Zeichen und öffnen Sie folgenden Pfad:

HKEY_CLASSES_ROOT
\txtfile
\shell
\open
\command

5. Klicken Sie im Verzeichnis ‚command und im rechten Feld, unter der Spalte ‚Name‘, und ändern Sie den Eintrag (vorgegeben) auf folgenden:
(Vorgegeben) = C:\WINDOWS\notepad.exe %1

6. Im linken Feld des Editors, drücken Sie auf das + Zeichen, und öffnen Sie folgenden Pfad:

HKEY_CLASSES_ROOT
\Applications
\ProgOp.exe

7. Klicken Sie auf die Datei "ProgOp.exe" und löschen Sie sie.

8. Benutzen Sie ‚Registrierung‘, ‚Ausgang‘, um den Registrierungseditor zu verlassen und die Änderungen zu bestätigen.

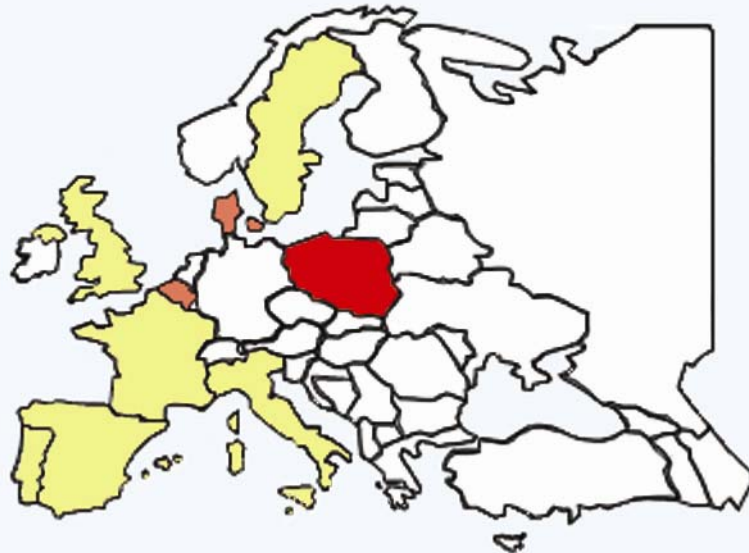
9. Fahren Sie Ihren Computer herunter und starten Sie ihn erneut (Start, System abstellen, neu starten).



BEMERKUNG: In allen Fällen kann „C:\Windows“ je nach installiertem Betriebssystem anders sein (mit diesem Namen vorgegeben in Windows 9x/ME und XP und als „C:\WinNT“ bei Windows NT/2000).

VIRUS FIZZER

Mayo 2003



- □ □ □ □ +

RECOVERY LABS®