Computer-Virus Informationen

Name:	Sircam
Alias:	W32/Sircam@mm
Typ:	**Wurm**

Sircam ist ein Mass-Mailing Internet-Wurm, der eine Länge von etwa 130 KByte zuzüglich der Länge einer Datei von dem infizierten System (siehe unten) besitzt. Wird er von einem Benutzer zum Beispiel durch einen Doppelklick aufgerufen, kopiert er seinen Code in die Verzeichnisse c:\recycled\ als

```
SirC32.exe
```

und in das Windows System-Verzeichnis als

```
SCam32.exe
```

Die Datei SirC32.exe wird als Standard Startup-Command für EXE-Dateien benutzt. Dadurch wird diese Datei stets aufgerufen, wenn eine EXE-Datei ausgeführt wird.

```
HKEY_CLASSES_ROOT\exefile\shell\open\command
@="\"C:\\recycled\SirC32.exe\" \" %*"
```

Die Datei SCam32.exe wird als Treiber registriert. Dadurch wird Sie bei jedem Start von Windows aufgerufen.

```
HKLM\Software\Microsoft\Windows\Current Version
"Driver32"="C:\\WINDOWS\SYSTEM\\SCam32.exe
```

Der Wurm den Namen von rundll32.exe in

```
run32.exe
```

und kopiert dann seinen Code nach rundll32.exe.

Weiterhin kopiert sich der Wurm mit einer Wahrscheinlichkeit von 1/33 in das Windows-Verzeichnis mit dem Namen

```
ScMx32.exe
```

In diesem Fall kopiert sich der Wurm auch in das Start-Verzeichnis von Windows als

```
Microsoft Internet Office.exe
```

Dadurch wird der Wurm bei jedem Login in das System aktiviert.

Der Wurm Sircam ist nur auf WIN32-Systemen funktionsfähig.

Sircam sammelt E-Mail-Adressen aus Dateien (z.B. mit Extension HTM) und kopiert diese im Windows System-Verzeichnis in eine Datei scw1.dll. Dieser Name kann aber auch zufällig festgelegt werden.

In dem Verzeichnis "My Documents" (Eigene Dateien) wird vom Wurm eine weitere Datei gespeichert. Diese enthält eine Liste von Datei-Namen mit bestimmten Extensions, wie zum Beispiel DOC, ZIP und JPG. Sircam versucht diese Dateien, die in der Regel auch vertrauliche Informationen enthalten können, per E-Mail zu versenden.

Der Wurm besitzt für den Versand von E-Mails eine eigene SMTP-Engine. Jeweils eine Datei aus der oben erwähnten Liste wird ausgewählt und an das Ende des Wurm-Codes kopiert. Diese Dateien besitzen jeweils zwei Extensions, wie zum Beispiel: .DOC.EXE, .ZIP.COM oder .JPG.PIF. Der Name der Datei ist identisch mit dem Namen der Datei, die vom infizierten System kopiert wurde. Die zweite Extension wird zufällig aus PIF, LNK, BAT oder COM gewählt.

Wenn der Empfänger einer solchen infizierten E-Mail das Attachment öffnet, installiert sich der Wurm auf seinem System und die in dem Attachment zusätzlich enthaltene Datei wird angezeigt:

```
Extension .DOC: Aufruf von WinWord.exe oder WordPad.exe
Extension .XLS: Aufruf von Excel.exe
Extension .ZIP: Aufruf von WinZip.exe
```

Auf diese Weise versucht der Wurm, sich vor dem Benutzer zu verbergen.

Infizierte E-Mails besitzen folgenden Inhalt:

```
From:    [E-Mail-Adresse des Benutzers] oder
         [Benutzer des infizierten Systems@prodigy.net.mx]
To:      [Name@email.aus dem Adressbuch]
Subject: Name des Dokuments [ohne Extension]
```

und zusätzlich:

```
Hi! How are you?
I send you this file in order to have your advice
```

oder

```
I hope you can help me with this file that I send
```

oder

```
I hope you like the file that I send you
```

oder

```
This is the file with the information that you ask for
See you later. Thanks
```

Falls spanisch eingestellt ist, lauten die Texte (Subject):

```
Hola como estas?
Te mando este arcivo para que me des tu punto de vista
```

oder

```
Espero me puedas ayudar con el archivo que te mando
```

oder

```
Espero te guste este archivoque te mando
```

oder

```
Este es el archivo con la informaci n que me pediste
Nos vemos pronto, gracias.
```

Der Body der infizierten E-Mail kann englisch oder spanisch sein. Die erste Zeile ist stets

```
Hi! How are you?         Hoja como estas?
```

Die letzte Zeile lautet stets:

```
See you later. Thanks    Nos vemos pronto, gracias
```

Dazwischen kann folgendes stehen:

```
I send you this file in order to have your advice
I hope you can help me with this file that I send
I hope you like the file that I send to you
This is the file with the information that ask you for
```

Bzw. in spanisch:

```
Te mando este archivo para que me des tu punto de vista
Espero me puedas ayudar con el archivo que te mando
Espero te guste este archivo qu te mando
Este es el archivo con la informacion que me pediste
```

Die als Attachment an eine infizierte E-Mail angehängte Datei besitzt den gleichen Namen wie die Datei, in die sich der Wurm auf dem infizierten System kopiert hat. Sie hat zwei Extensions, wie bereits oben erwähnt.

Ausbreitung in Netzwerken

Der Wurm ermittelt alle shared Verzeichnisse auf Remote-Systemen, um sich im Netzwerk auszubreiten, und kopiert seinen Code auf diese Systeme. Findet er ein Verzeichnis "recycled", so kopiert er seinen Code nach:

```
\recycled\SirC32.exe
```

Findet er ein Verzeichnis "Windows", ändert er den Datei-Namen RUNDLL32.EXE in

```
RUN32.EXE
```

und kopiert den Wurm-Code nach RUNDLL32.exe.

Alle Kopien des Wurm-Codes erhalten das Attribut hidden.

Der Wurm besitzt zwei Schadfunktionen. Am 20. Oktober löscht der Wurm mit einer Wahrscheinlichkeit von 1/20 alle Dateien des Laufwerks, auf dem Windows installiert ist.

An einem anderen Tag generiert der Wurm mit einer Wahrscheinlichkeit von 1/50 in dem Laufwerk, in dem Windows installiert ist, eine Datei

```
\recycled\sircam.sys
```

und kopiert in diese

```
SirCam_2rP_Ein_NoC_CuiTzeo_MicH_MeX
```

oder

```
SirCam Version 1.0 Copyright 2001 2rP Made in Hecho en - Cuitzeo,
Michoacan Mexico
```

so lange bis kein freier Speicher auf dieser Festplatte mehr verfügbar ist.

Hinweise für die Säuberung infizierter Systeme:

Holen Sie sich zunächst folgende REG-Datei:

```
ftp://ftp2.percomp.de/pub/tools/sirc_dis.reg
```

Mit Hilfe dieser REG-Datei kann der Eintrag des EXE-Keys in der Registry gesäubert werden und dadurch der Start des Wurm-Programms beim Start von Windows verhindert werden.

Wichtige Warung: Das infizierte System kann unter Umständen nicht mehr gestartet werden, wenn der Wurm-Code gelöscht wurde bevor der Registry-Eintrag (wie oben angegeben) gelöscht wurde! Also zuerst die Registry mit Hilfe der oben genannten REG-Datei säubern und erst danach den Wurm-Code löschen.

Unter Umständen ist es nicht möglich, die Dateien mit den Wurm-Code mit einem Anti-Viren-Programm zu löschen. In einem solchen Fall muss das System mit MS-DOS gestartet werden und dann die Dateien manuell gelöscht werden. Selbstverständlich kann nach einem Kaltstart mit MS-DOS auch F-PROT für DOS bzw. FP-DOS für das Löschen dieser Dateien verwendet werden.

Selbstverständlich sollte auch die vom Wurm in autoexec.bat zusätzlich eingefügte Zeile gelöscht werden.

Zurück