



VIRUS OPASERV

Seine Fähigkeit, sich durch die Netze zu verteilen, machen Ihnen zu einem arglistigen, für Firmen sehr gefährlichen Code.

1. WAS IST ES?

Familie der Würmer W32/OPASERV, W32/OPASOFT, I.worm.Opaserv

Seit September 2002 bis heute droht eine Wurmfamilie aus dem Internet und hat Verwirrung zwischen einigen Antivirusherstellern hervorgerufen, da sie ihm offensichtlich denselben Namen, aber mit verschiedenen Endungen gegeben haben. Anscheinend ist er heute schon bei Version M oder N.

Es ist wichtig, hervorzuheben, dass ein Virus eine festgelegte Programmierungsstruktur hat und, wenn sein Author Varianten herstellt, haben diese leichte Änderungen in ihrer payload oder es wird einfach die Endung einer untergeordneten Datei geändert.

Im gegenteiligen Fall handelt es sich um einen neuen Virus oder einen spezifischen Wurm.

Diese Familie ist vollkommen unter Kontrolle, da es genügt, eine spezifische heuristische Routine, für seine bereits bekannte Virusstruktur zu entwickeln. Daher nennen wir nur einige der wichtigsten, ohne uns in technische Einzelheiten zu verlieren, die für den Benutzer irrelevant sind.

2. WAS FÜR ARTEN GIBT ES?

OPA_SERV.E ist eine Variante, die bei Ausführen ihren Code dechiffriert und sich selbst in **%Windows%** mit den Namen **BRASIL.PIF** oder **BRASIL.EXE** kopiert.

Um beim nächsten Starten des Systems ausgeführt zu werden, erschafft es die folgenden Codes in der

Registrierung: **[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]**

Brasil=%Windows%\BRASIL.PIF

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

Brasil=%Windows%\BRASIL.EXE Der Wurm verbreitet die infizierten Dateien BRASIL.PIF oder BRASIL.EXE und führt sie als einen Vorgang, der nicht auf der Leiste des Task Managers von Windows gezeigt wird.

Er infiziert die Einheiten, die das Laufwerk C:\ teilen, und sucht die Geräte, die vollen Zugang zum Internet haben, wozu er die Verwundbarkeit des Share Level Password von Windows (geteiltes Niveau von Passwörtern) ausnutzt, womit einem Eindringling auf Distanz erlaubt wird, in die Systeme einzudringen, ohne die Passwörter kennen zu müssen.

Der Sicherheitspatch für diese Verwundbarkeit kann von folgendem Link heruntergeladen werden: <http://www.microsoft.com/technet/security/bulletin/ms00-072.asp>

OPA_SERV.G ist ein am 30. Oktober 2002 gefundener Virus, Mitglied derselben Familie und Variante des Wurms **Opasoft**, der im September 2002 gefunden wurde. Beide stammen vom selben Autor, der, basierend auf der ersten Variante begann, seine Untervarianten mit verschiedenen Namen von Dateien mit Endungen **.EXE, PIF, SCR**, usw. zu verteilen, aber alle mit derselben Virusstruktur.

Diese letzte ist 28 KB gross und hat eine Routine zum heimlichen Zugang, bekannt als **backdoor**, die sich durch lokale und geteilte Netze mit dem Service **NETBIOS** von MS Windows verbreitet.

Es ist eine ausführbare Tür, (**Portable Ejecutable**) und infiziert alle Betriebssysteme.

Windows95/98/NT/Me/2000/XP, inclusive die Server **NT/2000**.

Der Wurm installiert sich selbst im Verzeichnis von Windows mit dem Namen **scrsvr.exe** und fügt diesen zu der Registrierung, um bei Neustarten des Systems ausgeführt zu werden.

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

ScrSvr="%Name_des_Wurms%"

Dieser Wurm durchsucht die Subnetze durch **Port 137** des NETBIOS Services und sucht bestimmte IP-Adressen in den Netzeinheiten, Wenn er feststellt, dass die Netzeinheiten oder die Geräte den Service „**File and Print Sharing**“ geöffnet haben, beginnt sein Infizierungsprozess, wobei er von diesen Kontrolle auf Distanz übernimmt.



OPA SERV F. Verteilt sich auf den Geräten, die das Laufwerk C:\ teilen und vollen Zugang zum Netz haben, wo die Infizierung stattfindet, wozu er das Kommando SMB (Server Message Block Protocol) verwendet, um in die geteilten Einheiten hereinzukommen.

Dieser Wurm sendet Informationen an einen Ort im Internet, der nun geschlossen wurde, und von dem aus die infizierten Dateien mane!.dat und FDP!!!!.dat heruntergeladen wurden und im Verzeichnis C:\ installiert wurden, somit sind es die gleichen Dateien, die für den Datenaustausch in der Website in Brasilien benutzt werden.

In den entfernten Computern legt der Wurm die Datei **GAY.INI** in C:\ an und überschreibt in **%Windows%\win.ini** um beim nächsten Start des Betriebssystems folgenden Registrierungscode zu schreiben:

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

```
cronos = "%Windows%\MARCO!.SCR"
```

%Windows%, ist eine Variante die vorgegeben **C:\Windows** für Windows 95/98/Me/XP und **C:\Winnt** für NT/2000 lautet.

OPASERV.H verteilt sich auf den Einheiten, die C:\ teilen und kopiert sich selbst in das Verzeichnis %Windows% mit dem Namen **MSTASK.EXE**, und überschreibt gleichfalls in: **%Windows%\win.ini** und zur Ausführung beim nächsten Start des Computers schreibt er sich in die Registrierung:

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

```
Mstask = "%Windows%\MSTASK.EXE"
```

OPASERV.I verteilt sich auf den Einheiten, die C:\ teilen und kopiert sich selbst in das Verzeichnis %Windows% mit dem Namen **MQBKUP.EXE** und, um beim nächsten Start ausgeführt zu werden, erschafft er die folgenden Registrierungscode:

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

```
Mqbkup = "%Windows%\MQBKUP.EXE"
```

Der Wurm aktiviert sich an Tagen, die am oder nach dem 24. Dezember 2002 liegen und zeigt eine Nachricht in einem Fenster von MS-DOS, wonach er den Inhalt des CMOS und der Festplatte löscht:

NOTICE:

Illegal Microsoft Windows license detected!

You are in violation of the Digital Millennium Copyright Act

Your unauthorized license has been revoked

For more information, please call us at:

NOPIRACY

If you are outside the USA, please look up the correct contact information on our website, at:

www.bsa.org

Business Software Alliance

Promoting a safe & legal online world

OPASERV.J (einige Antivirus nennen ihn **Opaserv L/M/N**), nach dem 27. Dezember 2002 aufgefunden, verteilt er sich auf den Einheiten, die C:\ teilen und kopiert sich selbst in das Verzeichnis %Windows% mit dem Namen **MSTASK.EXE**, und überschreibt gleichfalls in **%Windows%\win.ini**, um beim nächsten Start ausgeführt zu werden, wobei er die folgenden Registrierungscode erstellt :

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

```
Mstask = "%Windows%\MSTASK.EXE"
```

Er infiziert auch durch die in C:\ geteilten Einheiten und sucht nach den Geräten, die vollen Zugang zum Internet haben, wozu er die Verwundbarkeit des **Share Level Password** von Windows benutzt.

Der Sicherheitspatch für diese Verwundbarkeit kann von folgendem Link heruntergeladen werden:

<http://www.microsoft.com/technet/security/bulletin/ms00-072.asp>

Er zeigt auch dieselbe Nachricht wie der **Opaserv.I** und startet das System erneut.



NOTICE:

Illegal Microsoft Windows license detected!
You are in violation of the Digital Millennium Copyright Act
Your unauthorized license has been revoked
For more information, please call us at:
1-888-NOPIRACY
If you are outside the USA, please look up the correct contact information on our website, at:
www.bsa.org
Business Software Alliance
Promoting a safe & legal online world

Die einzige Änderung in der Nachricht ist die Telefonnummer.

3. WIE FUNKTIONIERT ER?

Opaserv und seine Varianten gelangen durch das Internet in die Computer, sie benutzen hierzu die Kommunikationsports 137 und 139, die normalerweise als offen vorgegeben sind. Wenn der infizierte Computer Dateien oder Programme mit anderen Computern teilt, wird der bössartige Code sich auf diese verteilen, indem er eine Verwundbarkeit von Windows 9x, Me, den sog. „Share Level Password“ benutzt. Daher kann er sehr schnell alle Computer, die an ein Netzwerk angeschlossen sind, infizieren.

In Bezug auf Opaserv und seine Varianten bemerkt Luis Corrons, Director des Forschungslaboratoriums von Panda Software, „diese Würmer ermöglichen die Wiederkehr von älteren, bössartigen Viren, wie W95/CIH oder W32/Funlove. Dies geschieht,“ erklärt er, „da der Opaserv sich in die Geräte, die er infiziert, kopiert. Wenn diese Computer bereits von einem Virus infiziert sind, wird die den Opaserv enthaltende Datei auch infiziert werden und wird diese Infektion in ihrer weiteren Verbreitung mit sich tragen.“

F-Secure Corporation kündigt das Erscheinen in the wild des bössartigen Codes Opaserv, alias Opasoft an, der Merkmale eines Netzwurms mit Trojaner-Kapazität verbindet, um so entfernten, unbefugten Zugang zu den infizierten Computern zu haben.

Opaserv verbreitet sich durch die geteilten Netzeinheiten und kopiert sich selbst als ScrSvr.exe in das Verzeichnis des Systems Windows 9x, wobei es in dem infizierten Gerät verbleibt. Mit dem Ziel, jedesmal, wenn der Computer gestartet wird, ausgeführt zu werden, legt es eine Registrierung in Windows an.

Der trojanische Bestandteil des Opaserv ist zur ferngelenkten, unbefugten Kontrolle der infizierten Geräte geschaffen worden. Der Wurm versucht, Kontakt mit einer Adresse im Internet <http://www.opasoft.com> (jetzt inaktiv), herzustellen, um neue Versionen mit updates des bössartigen Codes herunterzuladen, falls solche verfügbar sind und einen Script über die Betriebssysteme zu überschreiben. In Bezug auf seine direkte Wirkung auf die Laufwerke, können wir sagen, dass der Virus eine Überschreibung der ersten zwei Drittel der Festplatte durchführt, die somit unwiederbringlich verloren sind. In den Versionen, die wir bis jetzt gesehen haben, haben wir festgestellt, dass die ersten zwei Drittel mit Codes in geometrischer Form überschrieben werden, wodurch diese Überschreibung sehr schnell erfolgt.



4. WIE BESEITIGT MAN IHN?

BitDefender bietet Ihnen ein unumgängliches Instrument zur Desinfizierung des Virus Win32.Worm.Opaserv.A, geschaffen zur Findung und Beseitigung der Viren, die Ihr System infiziert haben. Ein weiterer positiver Punkt dieser Anwendung ist ihr kleines Format, wodurch es sogar mit langsamen internetverbindungen leicht heruntergeladen werden kann. Ausserdem kann es per Email an Freunde, Verwandte und Geschäftspartner versandt werden.

Wenn Sie vermuten, dass Ihr Betriebssystem von dem Win-32.Worm.Opaserv.A infiziert wurde, laden sie das Programm herunter und führen Sie es in Ihren Computer aus. **AntiOpaserv.exe** Der Technische Dienst der Panda Software hat kostenlos die Anwendung PQREMOVE allen Benutzern zur Verfügung gestellt, mit der dieser neue Wurm sicher von den Computern entfernt werden kann.

PER ANTIVIRUS® Versión 7.8 mit Virusdatei zum 30. Dezember 2002 findet und beseitigt wirksam diesen Wurm und alle seine bestehenden und zukünftigen Varianten.