

## Informationen aus dem BSI



<b>Name:</b>	W32.Korgo.F
<b>Alias:</b>	Worm.Win32.Padobot.e [Kaspersky] W32/Korgo.worm.g [McAfee] WORM_KORGO.F [Trend]
<b>Art:</b>	Wurm
<b>Größe des Anhangs:</b>	10.752 Bytes
<b>Betriebssystem:</b>	Windows XP, Windows 2000 nicht betroffen: Windows 98/Me/NT
<b>Art der Verbreitung:</b>	Ausnutzung einer Sicherheitslücke
<b>Verbreitung:</b>	gering
<b>Risiko:</b>	mittel
<b>Schadensfunktion:</b>	Systemabstürze, verminderte Systemleistung Installation einer Backdoor
<b>Spezielle Entfernung:</b>	Tool
<b>bekannt seit:</b>	01.06.2004

### Beschreibung:

**W32.Korgo** ist ein Internetwurm, der sich über eine nicht geschlossene Sicherheitslücke im Betriebssystem Windows XP, Windows 2000 verbreitet.

Es sind mehrere Varianten bekannt, die sich in ihrer Funktion nicht wesentlich unterscheiden.

Es handelt sich um eine Schwachstelle im sog. **Local Security Authority Subsystem Service (LSASS)**. Diese Schwachstelle ist seit dem 13. April 2004 bekannt. Durch einen Pufferüberlauf ist es einem Angreifer möglich, Programmcode auszuführen und somit **volle Kontrolle** über den angegriffenen Computer zu erlangen. Microsoft stellt eine [deutsche Beschreibung dieser Sicherheitslücke](#) zur Verfügung. Die Schwachstelle wird mit dem Sicherheits-Update KB835732 geschlossen.

Für die weitverbreiteten Betriebssysteme Windows 2000 und Windows XP stehen Updates bereit unter:

[Microsoft Windows 2000 \(SP2, SP3 und SP4\)](#) [Microsoft Windows XP](#) und [Microsoft Windows XP SP1](#) Updates für alle übrigen Windows-Betriebssysteme befinden sich in der Microsoft-Beschreibung zur Sicherheitslücke.

Der Wurm verbreitet sich **nicht** über E-Mail-Nachrichten. Computer mit der genannten Sicherheitslücke werden infiziert, wenn Sie **Verbindung zum Internet** haben.

Bei der Infektion (oder dem Infektionsversuch) eines Systems kann es zu einer **Fehlermeldungen** mit anschließendem **automatischen Neustart** des Systems kommen.

Bei einem erfolgreichen Angriff lädt **Korgo** von dem angreifenden Computer eine Datei auf den

angegriffenen Computer und führt diese aus. Damit wird der angegriffene Computer infiziert.

Im infizierten System befindet sich der Wurm in `%System%\<zufälligerName>.exe`. Diese Datei ist 10.752 Bytes groß.

Hinweis:

`%System%` ist eine Systemvariable, die den tatsächlichen Dateipfad enthält. Dieser variiert bei den verschiedenen Windows-Versionen. Beispiel: `%System%` enthält `C:\Windows\System` bei Windows 95/98/Me, `C:\Winnt\System32` bei Windows NT/2000, und `C:\Windows\System32` bei Windows XP.

Mit dem Registrierungs-Schlüssel

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Disk Defragmenter"="%System%\<zufälligerName>.exe"
```

wird Korgo beim Rechnerstart aktiviert.

Korgo versucht sich an die Datei Explorer.exe anzuhängen. Wenn dieser Versuch erfolgreich ist, taucht der Wurm im Taskmanager nicht mehr als eigener Prozess auf.

Bei der Installation eines Backdoors öffnet Korgo verschiedene Ports, darunter auch die TCP Ports 113 und 3067.

### Entfernung des Wurms Korgo.F

Zur Entfernung des Wurms sind folgende Schritte durchzuführen:

1. Vor der Entfernung muss die Sicherheitslücke des Betriebssystems geschlossen werden. Andernfalls kann es jederzeit zu einer Neuinfektion kommen, wenn der Computer ans Netz angeschlossen wird.
2. Kontrollieren Sie die ordnungsgemäße Installation in Systemsteuerung - Software. In der Liste der installierten Programme muss sich der Eintrag "Windows XP Hotfix - KB835732" befinden.
3. Laden Sie eines der unten aufgeführten speziellen Entfernungstools und durchsuchen Sie damit den Computer. Zur Verwendung der Programme müssen Sie **Administrator-Berechtigung** besitzen. Andernfalls erhalten Sie eine Fehlermeldung.  
**Symantec** (FixKorgo.exe): Direkt-Download oder Download mit englischer Beschreibung
4. Bei Windows XP muss vor der Entfernung die **Systemwiederherstellung deaktiviert** werden.
5. Starten Sie den Computer im **abgesicherten Modus** .
6. Durchsuchen Sie den Computer mit dem Entfernungstool.

(Erstellt: 03.06.2004)