

ウイルス解析報告書

ウイルス名	W32.Korgo.F (別名 :Worm.Win32.Padobot.e [Kaspersky], W32/Korgo.worm.g [McAfee], WORM_KORGO.F [Trend])
プログラム名及び容量 (添付ファイル名)	プログラム名 :不定 容 量 :10,752 バイト
種別	ワーム
プログラム言語	不明
発症環境	Windows 2000, Windows XP
発見日時	2004 年 5 月 29 日
発見場所	台湾 (最初の感染報告)
危険性	感染力が強い。短時間で多くの届出が寄せられた。危険度は 5 段階の 3 (5 が最も危険)。
発症条件	脆弱性が存在するコンピュータがワームの攻撃を受けたとき。
ウイルスの活動、影響	W32.Korgo.F は、TCP ポート445 で Microsoft Windows LSASS のバッファ・オーバーランの脆弱性 (MS04-011) を悪用することで拡散する。また、TCP ポート113、3067、およびその他のランダムなポートで待機する。
被害の規模	発見から 63 時間で 458 件の届出がシマンテック社に寄せられている。
亜種、変種の有無	W32.Korgo.A(2004 年 5 月 22 日発見)以降, W32.Korgo.B, W32.Korgo.C, W32.Korgo.D, W32.Korgo.E
ウイルスの動作概要	<p>W32.Korgo.F が実行されると、次のことを行う</p> <ol style="list-style-type: none"> ワームが実行されると%System%フォルダから、Ftpupd.exe ファイルを削除します。 %System%フォルダは、標準で C:\WINNT\System32 (Windows NT/2000)または C:\Windows\System32 (Windows XP)である。 レジストリキーから値を削除する。 次の値を "System Service Manager" "System Restore Service" "Bot Loader" "Windows Update Service" "WinUpdate" "Windows Security Manager" "avserve.exe" "avserve2.exe" 次のレジストリキーから削除する。 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run レジストリの変更及び自分自身をコピーする。 次のレジストリキーに HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 次の値が存在するか調べる。 "Disk Defragmenter" 値 "Disk Defragmenter" が存在しない場合は次の値を "Client"="1" 次のレジストリキーに追加する。 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wireless

値 "Disk Defragmenter" は存在するが、ファイルのパスがワームとは異なる場合は次のことを行う

自分自身を %System%\%<ランダムなファイル名>.exe としてコピーする。

次の値を

"Disk Defragmenter" = "%System%\%<ランダムなファイル名>.exe"

次のレジストリキーに追加する。

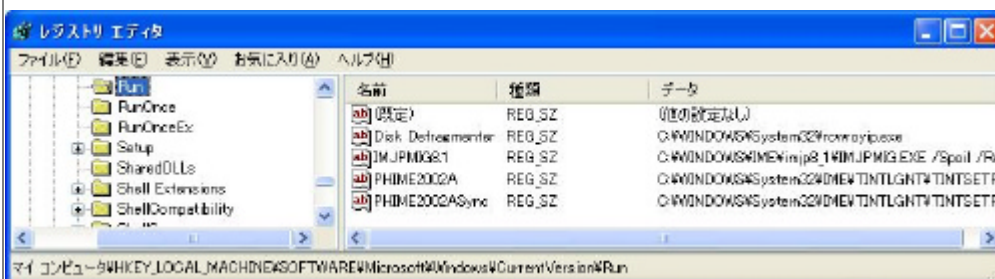
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

値 "Disk Defragmenter" が存在し、かつ、その値のパスがワームのパスと一致する場合は次の値を

"Client"

次のレジストリキーから削除する。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wireless



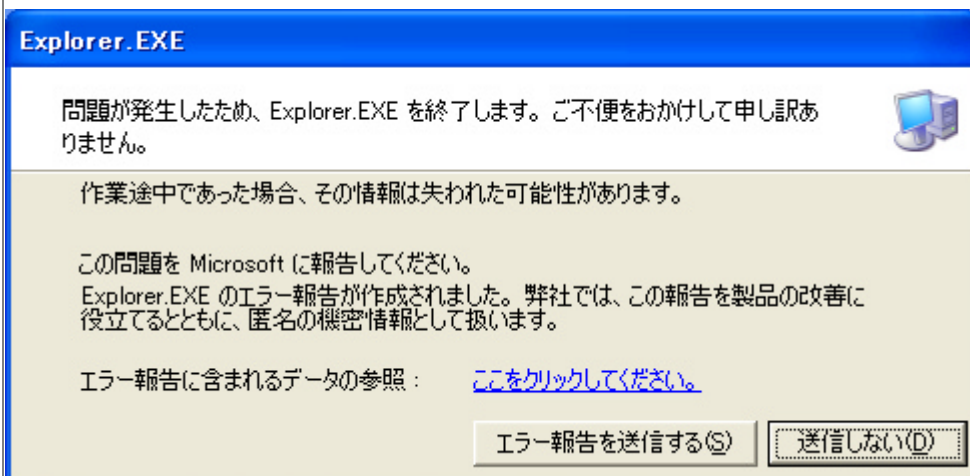
4. Explorer.exe が今後のアクションを行うように試みる。
成功した場合、今後のワームのアクションは Explorer.exe によって実行されるため、Windows タスクマネージャでプロセスリストを表示しても、ワームのプロセスは表示されない。
失敗した場合、ワームは現在のプロセスのまま動作する。
5. 別のスレッドを作成し、次のことを行う
 - ・TCP ポート113、3067、および、その他のランダムなポートを開く。ワームはこれらのポートで待機し、特定のメッセージを受信すると、自身のコピーをリモートのコンピュータへ送信する。
 - ・ランダムな IP アドレスの TCP ポート445 に対し Windows LSASS の脆弱性 (MS04-011) を悪用し攻撃する。脆弱なコンピュータが攻撃を受けると、脆弱なコンピュータは攻撃元のコンピュータのワームが開いた TCP ポートの 1 つを通じて接続しようとする。
 - ・次のいずれかの IRC サーバの TCP ポート6667 に接続を試み、コマンドを受信しようとする。
 - gaspode.zanet.org.za
 - lia.zanet.net
 - irc.tsk.ru
 - london.uk.eu.undernet.org
 - washington.dc.us.undernet.org
 - los-angeles.ca.us.undernet.org
 - brussels.be.eu.undernet.org
 - caen.fr.eu.undernet.org

flanders.be.eu.undernet.org
 graz.at.eu.undernet.org
 moscow-advocat.ru
 gaz-prom.ru

W32.Korgo.F の感染状況について動作検証を行った結果を次に記す。

OS 種別	2000 Pro.	2000 Sv	XP Home	XP Pro.	2003 Sv
SP なし	感染しないが、 レポートする	感染しないが、 レポートする	感染の後、発症 するが、再起動 後は発症しない	感染の後、発症 するが、再起動 後は発症しない	感染しな い
SP あり [2000:SP4] [XP:SP1]	感染しないが、 レポートする	感染しないが、 レポートする	感染の後、発症、 再起動後も 発症する場合 がある	感染の後、発症、 再起動後も 発症する場合が ある	-
MS04-011 パッチ適用	感染しない	感染しない	感染しない	感染しない	-

WindowsXP Home 及び Pro の SP1 において再起動後に発症しない場合には、次のダイアログが表示される。



感染 発症防止方法

1. マイクロソフト社の提供する修正パッチ (MS04-011) を適用する。
2. ファイアウォールでTCP ポート445, 3332, 3067 及び TCP ポート6667 に向けた IRC セッションをブロックする。

ウイルスの駆除方法

手動による修復を行う場合、コンピュータに関する高度な知識が必要とされ、間違えるとコンピュータが正常に起動しなくなる場合もある。

1. 被害拡大防止のため、感染したコンピュータをネットワークから切り離す。
2. システムの復元オプションを無効にする。(Windows Me/XP)
3. コンピュータをセーフモードで再起動する。
4. 感染ファイルを削除する。
%System%¥<ランダムなファイル名>.exe (レジストリキーの値を参照すること)
5. レジストリに行われた変更を元に戻す。
次の値を
"Disk Defragmenter"="%System%¥<ランダムなファイル名>.exe"

	<p>次のレジストリキーから削除する。 HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run</p> <p>次の値を "Client"="1"</p> <p>次のレジストリキーから削除する。 HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Wireless</p> <p>各操作については Microsoft のホームページ、付属のマニュアル等を参照すること。</p> <p>無償修復ツールがワクチンベンダーから配布されているので、使用上の注意をよく読み自己責任において使用すること。</p>
その他	無