

ウイルス解析報告書

ウイルス名	W32/Bibrog.C@mm
プログラム名及び容量 (添付ファイル名)	manzana.exe, academia.exe, itch.exe, itcj.exe 235,520バイト
種別	Windows 環境用ワーム(32ビット)
プログラム言語:	Visual Basic
発症環境	Windows95/98/98SE/ME/NT/2000/XP
発見日時	2003年3月13日
発見場所(発信地)	不明
危険性	低い(5段階で2)
発症条件	即時
	<p>このワームはWindows 95/98/ME/NT/2000/XPで動作する。</p> <p>ワームはOutlookのアドレス帳に登録されているメールアドレスに下記のメールを送信する。</p> <p>件名:Fwd:La Academia Azteca 本文:La cacademia azteca (muy bueno) !no es virus! 添付:academia.exe</p> <p>ウイルスはKaZaA、Grokster、Morpheus、ICQの共有フォルダにウイルスをコピーする。 これらの共有を通じて感染を広めるのが狙いと思われる。</p> <p>また、スタートアップフォルダにウイルスをコピーして、OSが起動されるたびにウイルスが実行されるようにする。 ファイル名は下記の何れかである。</p> <p>Kylie Minogue porn screen_saver.exe Shakira porn screen_saver.exe Salma Hayek porn screen_saver.exe Kirsten Dunst porn screen_saver.exe Jessica Alba porn screen_saver.exe Christina Aguilera porn screen_saver.exe Anna Kournikova porn screen_saver.exe Sandra Bullock porn screen_saver.exe AlessandraAmbrosia porn screen_saver.exe Jenna Jameson porn screen_saver.exe Karina Lombard porn screen_saver.exe Pamela Anderson porn screen_saver.exe Britney Spears porn screen_saver.exe Charlize Theron porn screen_saver.exe Helena Christensen porn screen_saver.exe Stacey Keibler porn screen_saver.exe Kelly Hu porn screen_saver.exe Halle Berry porn screen_saver.exe Cameron Diaz porn screen_saver.exe Donna D'Erico porn screen_saver.exe</p> <p>ワームは実行するとシューティングゲームのようなウィンドウを開く。</p>



図1 シューティングゲームのような画面

OSを再起動したときに壁紙が表示される。

ウイルスの活動、
影響



図2 quiettime.bmp



	図3 osiris.bmp
被害の規模	現時点では不明
亜種、変種の有無	少なくとも1つの亜種がある。BとCは差異がわずかか、または同じものだと考えられている。
ウイルス動作概要	<p>ワームは実行されると、ワーム自身をWindowsフォルダにmanzana.exe、システムフォルダにacademia.exeという名前でコピーする。</p> <p>ワームはスタートアップフォルダ以外から実行されると、ワーム自身をスタートアップフォルダにitch.exeとitcj.exeという名前でコピーする。(現在ログインしているユーザーのスタートアップフォルダを動的に取得する。)</p> <p>ワームはシューティングゲームのような画面(図1)を表示する。ウィンドウを閉じればゲームは終了して、ワームも終了する。</p> <p>スタートアップフォルダにコピーされたワームが実行されたときには、ワーム自身をカレントフォルダに以下のパス名でコピーする。 フォルダが存在しなければ、コピーは失敗する。</p> <p>KaZaA%My Shared Folder%Kylie Minogue porn screen_saver.exe KaZaA%My Shared Folder%Shakira porn screen_saver.exe KaZaA%My Shared Folder%Salma Hayek porn screen_saver.exe KaZaA%My Shared Folder%Kirsten Dunst porn screen_saver.exe KaZaA%My Shared Folder%Jessica Alba porn screen_saver.exe KaZaA%My Shared Folder%Christina Aguilera porn screen_saver.exe KaZaA%My Shared Folder%Anna Kournikova porn screen_saver.exe KaZaA%My Shared Folder%Sandra Bullock porn screen_saver.exe KaZaA%My Shared Folder%AlessandraAmbrosia porn screen_saver.exe KaZaA%My Shared Folder%Jenna Jameson porn screen_saver.exe KaZaA%My Shared Folder%Karina Lombard porn screen_saver.exe KaZaA%My Shared Folder%Pamela Anderson porn screen_saver.exe KaZaA%My Shared Folder%Britney Spears porn screen_saver.exe KaZaA%My Shared Folder%Charlize Theron porn screen_saver.exe KaZaA%My Shared Folder%Helena Christensen porn screen_saver.exe KaZaA%My Shared Folder%Stacey Keibler porn screen_saver.exe KaZaA%My Shared Folder%Kelly Hu porn screen_saver.exe KaZaA%My Shared Folder%Halle Berry porn screen_saver.exe KaZaA%My Shared Folder%Cameron Diaz porn screen_saver.exe KaZaA%My Shared Folder%Donna D'Erico porn screen_saver.exe Grokster%My Grokster%Kylie Minogue porn screen_saver.exe Grokster%My Grokster%Shakira porn screen_saver.exe Grokster%My Grokster%Salma Hayek porn screen_saver.exe Grokster%My Grokster%Kirsten Dunst porn screen_saver.exe Grokster%My Grokster%Jessica Alba porn screen_saver.exe Grokster%My Grokster%Christina Aguilera porn screen_saver.exe Grokster%My Grokster%Anna Kournikova porn screen_saver.exe Grokster%My Grokster%Sandra Bullock porn screen_saver.exe Grokster%My Grokster%AlessandraAmbrosia porn screen_saver.exe Grokster%My Grokster%Jenna Jameson porn screen_saver.exe Grokster%My Grokster%Karina Lombard porn screen_saver.exe Grokster%My Grokster%Pamela Anderson porn screen_saver.exe Grokster%My Grokster%Britney Spears porn screen_saver.exe Grokster%My Grokster%Charlize Theron porn screen_saver.exe Grokster%My Grokster%Helena Christensen porn screen_saver.exe Grokster%My Grokster%Stacey Keibler porn screen_saver.exe Grokster%My Grokster%Kelly Hu porn screen_saver.exe Grokster%My Grokster%Halle Berry porn screen_saver.exe Grokster%My Grokster%Cameron Diaz porn screen_saver.exe Grokster%My Grokster%Donna D'Erico porn screen_saver.exe Morpheus%My Shared Folder%Kylie Minogue porn screen_saver.exe Morpheus%My Shared Folder%Shakira porn screen_saver.exe Morpheus%My Shared Folder%Salma Hayek porn screen_saver.exe Morpheus%My Shared Folder%Kirsten Dunst porn screen_saver.exe Morpheus%My Shared Folder%Jessica Alba porn screen_saver.exe Morpheus%My Shared Folder%Christina Aguilera porn screen_saver.exe Morpheus%My Shared Folder%Anna Kournikova porn screen_saver.exe Morpheus%My Shared Folder%Sandra Bullock porn screen_saver.exe Morpheus%My Shared Folder%AlessandraAmbrosia porn screen_saver.exe Morpheus%My Shared Folder%Jenna Jameson porn screen_saver.exe Morpheus%My Shared Folder%Karina Lombard porn screen_saver.exe Morpheus%My Shared Folder%Pamela Anderson porn screen_saver.exe Morpheus%My Shared Folder%Britney Spears porn screen_saver.exe Morpheus%My Shared Folder%Charlize Theron porn screen_saver.exe Morpheus%My Shared Folder%Helena Christensen porn screen_saver.exe</p>

	<p>Morpheus¥My Shared Folder¥Stacey Keibler porn screen_saver.exe Morpheus¥My Shared Folder¥Kelly Hu porn screen_saver.exe Morpheus¥My Shared Folder¥Halle Berry porn screen_saver.exe Morpheus¥My Shared Folder¥Cameron Diaz porn screen_saver.exe Morpheus¥My Shared Folder¥Donna D'Erico porn screen_saver.exe ICQ¥shared files¥Kylie Minogue porn screen_saver.exe ICQ¥shared files¥Shakira porn screen_saver.exe ICQ¥shared files¥Salma Hayek porn screen_saver.exe ICQ¥shared files¥Kirsten Dunst porn screen_saver.exe ICQ¥shared files¥Jessica Alba porn screen_saver.exe ICQ¥shared files¥Christina Aguilera porn screen_saver.exe ICQ¥shared files¥Anna Kournikova porn screen_saver.exe ICQ¥shared files¥Sandra Bullock porn screen_saver.exe ICQ¥shared files¥Alessandra Ambrosia porn screen_saver.exe ICQ¥shared files¥Jenna Jameson porn screen_saver.exe ICQ¥shared files¥Karina Lombard porn screen_saver.exe ICQ¥shared files¥Pamela Anderson porn screen_saver.exe ICQ¥shared files¥Britney Spears porn screen_saver.exe ICQ¥shared files¥Charlize Theron porn screen_saver.exe ICQ¥shared files¥Helena Christensen porn screen_saver.exe ICQ¥shared files¥Stacey Keibler porn screen_saver.exe ICQ¥shared files¥Kelly Hu porn screen_saver.exe ICQ¥shared files¥Halle Berry porn screen_saver.exe ICQ¥shared files¥Cameron Diaz porn screen_saver.exe ICQ¥shared files¥Donna D'Erico porn screen_saver.exe</p> <p>ワームはWindowsフォルダにosiris.bmpとquiettime.bmpを作成する。WindowsフォルダのWIN.INIのDesktopセクションのWallpaperキーを書き換えてosiris.bmp(図3)またはquiettime.bmp(図2)を壁紙に設定する。ファイルは乱数で選ばれる。</p> <p>ワームはMy Documentsフォルダにhotmail.htm、yahoo.htm、msn.htm、citibank.htm、acafug.htmを作成する。acafug.htmを除き、これらは有名サイトのWebに似ているが、フォームに入力された内容はhttp://send.greetings.yahoo.com/greet/preview#personalizeに送られる。</p> <p>ワームはレジストリにHKEY_CURRENT_USER¥Software¥VB and VBA Program Settings¥pomme¥variaを作成する。</p> <p>ワームはMAPIを使ってアドレス帳にあるすべてのメールアドレスにワームを添付して下記のメールを送信する。 件名:Fwd:La Academia Azteca 本文:La cacademia azteca (muy bueno) !no es virus! 添付:academia.exe</p>
感染・発症防止方法	不明な電子メール添付ファイルを実行しない。
ウイルスの駆除方法	<p>< 確認 > Windowsフォルダにmanzana.exe、システムフォルダにacademia.exe、スタートアップフォルダにitch.exeまたはitcj.exeがあれば感染している。</p> <p>< 駆除 > ・Windowsフォルダのmanzana.exeとosiris.bmpとquiettime.bmp、システムフォルダのacademia.exe、スタートアップフォルダのitch.exeとitcj.exeを削除する。 ・レジストリのHKEY_CURRENT_USER¥Software¥VB and VBA Program Settings¥pomme¥variaを削除する。 ・KaZaA、Grokster、Morpheus、ICQの共有フォルダにある、上記のファイルを削除する。 ・壁紙の設定を元に戻す。</p>
その他	報告書作成：2003年3月20日現在

W32/BiBrog.C フローチャート

