
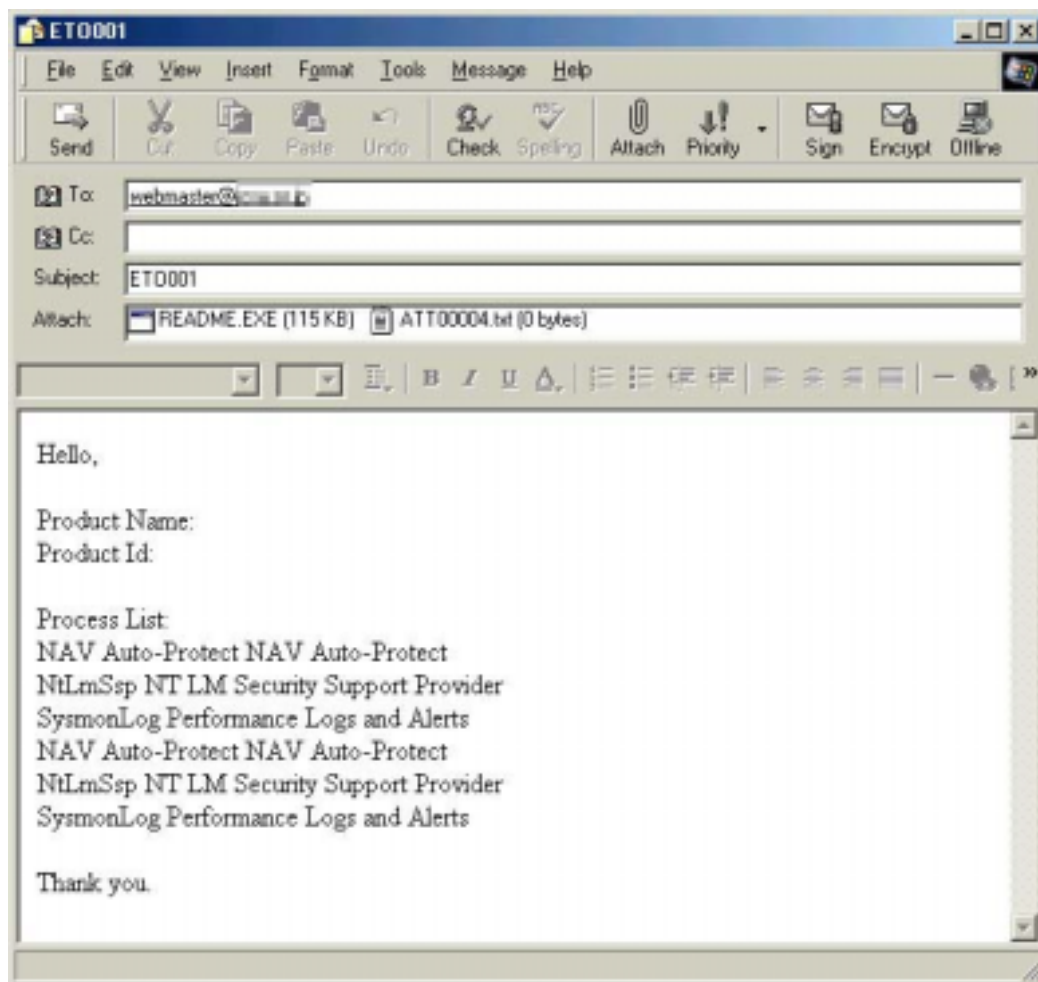


## ウィルス解析報告書

ウイルス名	Brid (W32/Brid.A-mm, W32.Brid@mm, W32/Braid-A)
プログラム名及び容量 (添付ファイル名)	README.EXE 114,690バイト
種別	ワーム
プログラム言語	Visual Basic 6.0
発症環境	Windows95/98/ME/NT/2000/XP
発見日時	2002年11月4日
発見場所(発信地)	不詳
危険性	5段階で低い方から2
発症条件	Brid自体には発病はない
<b>ウイルスの活動、影響</b>	<p>このワームはWindows95/98/ME/NT/2000/XPで動作する。 ワームはInternetExplorerのアイコンを含んでいる。</p> <div style="text-align: center;">         README     </div> <p>ワームは実行されると自身をコピーしてシステムにインストールする。 インストールされると起動時にウイルスが実行されるようになる。</p> <p>またこのワームはW32/FunLoveの亜種を含んでおり、ワームが実行されるとFunloveウイルスを実行するため、コンピュータのシステムはW32/FunLoveに感染する。</p> <p>ワームは拡張子がhtm、dbxのファイルからメールアドレスを収集してメールを送信する。 メールの送信者は送信者のコンピュータに登録されたユーザ名、件名は送信者のコンピュータに登録された組織名である。添付ファイルはウイルス自身で、ファイル名が必ずREADME.EXEになる。</p> <p>なお、メールはワームが宛先ドメインに直接SMTP接続してメールを送り込み、この際、From:やReturn-Path:も偽造される。</p> <p>メール 本文は下記のとおり。(％sはそれぞれレジストリから読み出した値)</p> <p>Hello,</p> <p>Product Name: %s        Product Id: %s        Product Key: %s        Process List: %s</p> <p>Thank you.</p>



セキュリティーホール(MS01-020: (「不適切な MIME ヘッダーが原因で Internet Explorer が電子メールの添付ファイルを実行する」))があるメールでこのメールを表示すると、ワームがユーザーに知られることなく実行される。

ワームは一部のアンチウイルス製品やデバックなどを終了させる。

#### 被害の規模

Brid自体の危険性は高くないが、内包するW32/Funlove亜種によるLAN内感染を引き起こした場合、修復には相応の手間と時間がかかる。

#### 亜種、変種の有無

現時点ではA型以外は確認されていない。

ワームはコンピュータ名を取得する。またレジストリの  
 HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥RegisteredOrganization  
 HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥RegisteredOwner  
 HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥ProductName  
 HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥ProductId  
 HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥ProductKey  
 の値を取得する。

ワームは下記の文字列をクラスに含むウィンドウを持ったプロセスを終了させる。

MST  
 MS\_  
 - S  
 \_NP  
 VIEW  
 IRMON  
 SMTPSVC  
 MONIKER  
 PROGRAM

また下記の文字列をタイトルに含むウィンドウを持つプロセスを終了させる。

dbg  
 mon  
 vir  
 iom

ウイルス動作概要	<p>anti fire prot secu view debug</p> <p>ワームは「Bride Explorer」という名前のウインドウを探す。見つかったならば既にウイルスが起動しているとみなして終了する。</p> <p>ワームはcLac.eXeを実行する。(しかしこのファイルは存在しないので失敗する)</p> <p>ワームはデスクトップにHelp.emlとExplorer.exeを作る。 Help.emlはOutlook Expressのファイルで、セキュリティーホールがあるメーラーやブラウザで開くと、添付ファイルとして存在するウイルスが実行される。 Explorer.exeはワームのコピーである。</p> <p>ワームはシステムフォルダにregedit.exeを作る。 HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥regedit にシステムフォルダのregedit.exeのフルパスを登録する。</p> <p>ワームは自身の内部に含まれるW32/FunLoveウイルスでシステムフォルダのmsconfig.exeの先頭を上書きする(ファイルが無ければ作る)。このW32/FunLoveはファイル名が flcss.exeの代わりにbride.exeになっていることを除けば、機能はオリジナルの W32/FunLoveと同等である。</p> <p>一時的にテンポラリフォルダにBrade0.tmpを作る。 ワームはHDDを再帰的に検索して拡張子がhtmまたはdxbのファイルを開く。 そのファイルからメールアドレスを取得する。</p> <p>ワームは取得したメールアドレスすべてにメールを送信する。 Windows95/98/MEならばレジストリの</p> <p>HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥VxD¥MSTCP¥NameServer HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥VxD¥MSTCP¥Domain</p> <p>から、WindowsNT/2000/XPならばレジストリの</p> <p>HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters¥DhcpNameServer HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters¥DHCPDomain</p> <p>からDNSのアドレスを取得する。</p> <p>ワームはDNSに直接接続してメールアドレスに対応するSMTPサーバを求めて、そのSMTPサーバに接続してメールを送信する。 メールの内容はHelp.emlと同じで、メールの送信者は送信者のコンピュータに登録されたユーザ名、件名は送信者のコンピュータに登録された組織名、添付ファイルはワーム自身であり、ファイル名はREADME.EXEになる。</p> <p>本文は下記のとおり。%sはそれぞれレジストリから読み出した値になる。</p> <p>Hello,</p> <p>Product Name: %s Product Id: %s Product Key: %s Process List: %s</p> <p>Thank you.</p> <p>セキュリティーホールがあるメーラーやブラウザでこのメールを開くと、添付ファイルとして存在するワームが実行される。</p> <p>----- § 感染確認 ----- § 修復</p>
	感染・発症防止方法

ウイルスの駆除方法	<p>&lt; 確認 &gt; デスクトップにHelp.exeまたはExplorer.exeがあるか、システムフォルダにregedit.exeがあれば感染している。 (Windowsフォルダにあるregedit.exeは無害)</p> <p>またこのワームに感染している場合には、W32/Funloveの亜種に感染している可能性がある。基本的にオリジナルのW32/Funloveと同じだが、ファイル名は flcss.exeの代わりにbride.exeとなる。システムフォルダにbride.exeがあれば W32/Funloveの亜種に感染している。</p> <p>&lt; 駆除 &gt; セーフモードで起動してデスクトップのHelp.exeとExplorer.exeならびにシステムフォルダのregedit.exeを削除する。(Windowsフォルダにあるregedit.exeは無害) またレジストリの HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥regedit を削除する。</p> <p>またこのワームに感染している場合にはW32/Funloveの亜種に感染している可能性がある。基本的にオリジナルのW32/Funloveと同じだが、ファイル名は flcss.exeの代わりにbride.exeである。これについてはW32/Funloveの修復方法を参照のこと。</p>
その他	報告書作成:2002年11月14日現在

## W32/Brid.A-mm フローチャート

