

ウイルス解析報告書

ウイルス名	WORM_RODOK.A (W32/BR2002, W32/Fleming.worm, W32.HLLW.Henpeck)
プログラム名及び容量 (添付ファイル名)	BR2002.exe (53,248バイト)
種別	ワーム(トロイの木馬)
プログラム言語:	Visual Basic
発症環境	Windows95/98/ME/NT/2000/XP
発見日時	2002年10月9日(米国時間)
発見場所(発信地)	主にアジア(韓国、中国) 発信地は不詳
危険性	低(現在はすでにワームを供給していたサイトはアクセス不能となっている)
発症条件	感染後即時

このワームはWindows95/98/ME/NT/2000/XPで動作する。

ワームはMSN Messengerのコンタクトリスト全てに対してメッセージを送信する。(図1)
 メッセージ受信者がURLからファイルをダウンロードして実行するとワームに感染する。
 ワームが自分自身をMSNメッセージャーで送信することはない。

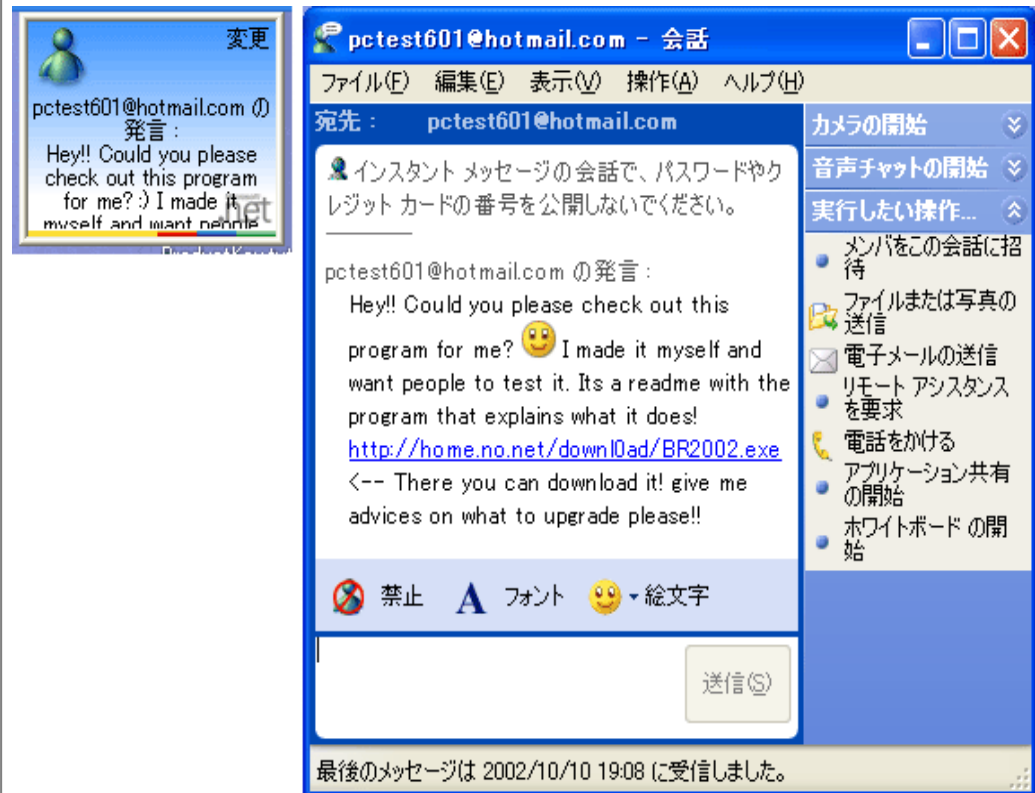


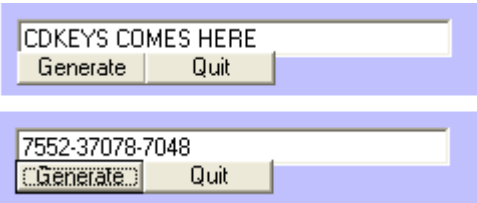
図1. 感染コンピュータから届いたメッセージ(左がポップアップ時で、右が内容を表示したところ)

ワームは実行されると「Generate」と「Quit」の2つのボタンとエディットコントロールだけがあるウインドウを開く。(図2上)

「Generate」を押すとエディットコントロールにCDキーのような数字が表示される。(図2下)

「Quit」を押すとウインドウは消える。

ウイルスの活動、
影響

	 <p>図2. 偽装キージェネレータウインドウ</p> <p>ワームは特定のサイトから2つのファイルをダウンロードする。 その中の1つはただちに実行される。</p> <p>このワームが利用するサイトは、現在、既に利用できなくなっている。</p>
被害の規模	<p>下記のキー情報が特定ユーザーにメールで送信される。(ハッキング・情報盗用)</p> <p>HKEY_CURRENT_USER¥Software¥Valve¥CounterStrike¥Settings¥Key HKEY_CURRENT_USER¥Software¥Valve¥Half-Life¥Settings¥Key (ゲームプロダクトのシリアルキーと思われる)</p>
亜種、変種の有無	現時点では確認されていない。
ウイルス動作概要	<p>ワームは下記の2つのキーがあればその内容をstyggefolk@hotmail.comに送る。 HKEY_CURRENT_USER¥Software¥Valve¥CounterStrike¥Settings¥Key HKEY_CURRENT_USER¥Software¥Valve¥Half-Life¥Settings¥Key</p> <p>ワームは実行されるとMSN Messengerのコンタクトリストのすべてに下記のメッセージを送信する。 Hey!! Could you please check out this program for me? :) I made it myself and want people to test it. Its a readme with the program that explains what it does! http://home.no.net/download/BR2002.exe <- - There you can download it! give me advices on what to upgrade please!!</p> <p>ワームはhttp://home.no.net/download/CS-Keygen.exeをダウンロードする。 それをC:¥hehe2397824.exeとして保存する。(このファイルは後で実行される)</p> <p>ワームはhttp://home.no.net/download/Update.exeをダウンロードする。 それをC:¥update35784.exeとして保存する。</p> <p>ワームは実行されると「Generate」と「Quit」の2つのボタンとエディットコントロールだけがあるウインドウを開く。 「Generate」を押すとエディットコントロールにCD鍵のような数字が表示される。 「Quit」を押すとウインドウは消えて次の処理を行う。</p> <p>ワームはC:¥hehe2397824.exeを実行する。</p>
感染・発症防止方法	<p>MSNメッセージャーで表示された当該URLをアクセスしない。 または内容の保証されていない実行ファイルを開かない。</p>
ウイルスの駆除方法	<p>< 確認 > C:¥update35784.exe、C:¥hehe2397824.exeがあれば感染している。</p> <p>< 駆除 > C:¥update35784.exe、C:¥hehe2397824.exeがあればそれらを削除する。</p>
その他	報告書作成:2002年10月11日現在

WORM_RODOKフローチャート

