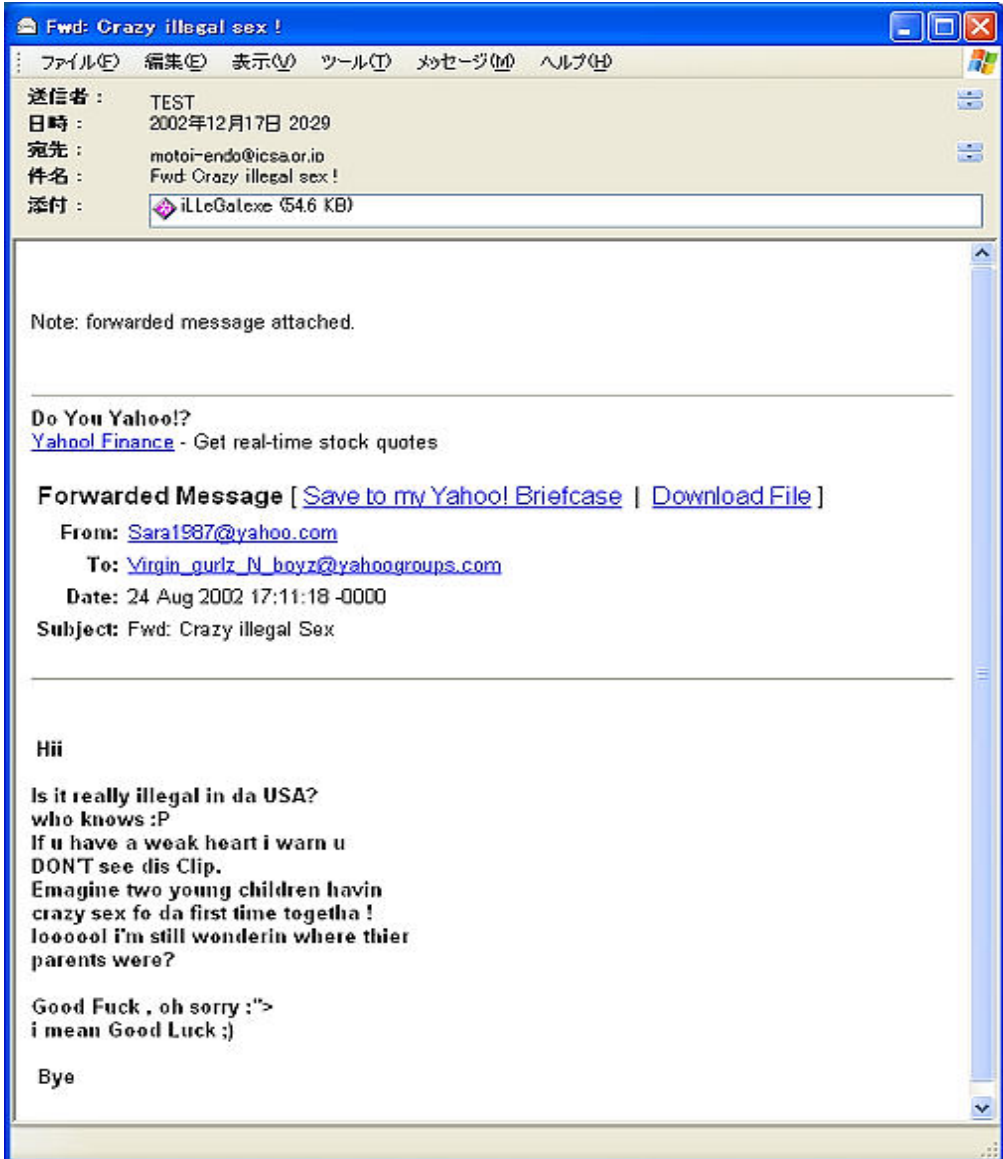
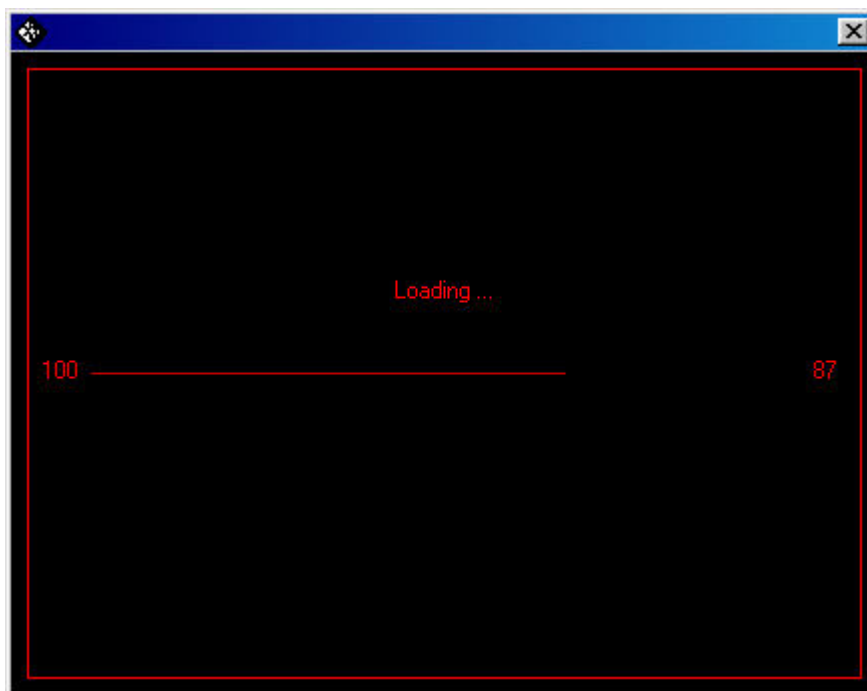


ウイルス解析報告書

ウイルス名	W32/Galil (W32/Holar.C, Galil)
プログラム名及び容量 (添付ファイル名)	iLLeGal.exe (54,514バイト)
種別	ワーム (32ビットWindows)
プログラム言語:	Visual Basic 6.0
発症環境	Windows 9x/ME/NT/2000/XP
発見日時	2002年12月4日
発見場所(発信地)	不詳 (アラビア語圏の可能性が高い)
危険性	低い。5段階で1と2の間位。 なお、日本語環境では感染も発病もしない。2バイト言語圏では感染・発病しない可能性が大である。
発症条件	感染のあと、ワーム実行回数とパソコンの再起動回数の和が5の時 (通常もっともあり得るシチュエーションは感染後4回再起動したとき)
	<p>このワームは下記のような電子メールによって伝染する。</p>  <p>このメールに添付されたEXEファイルを実行すると、システムフォルダにiLLeGal.exeという名前でコピーされる。</p>

また、システムフォルダにMplayer.exe(不可視属性)とSMTP.ocxが作成されて Mplayer.exeが実行される。ただし、VisualBasicのランタイムライブラリの仕様により、日本語環境ではSMTP.ocx もMplayer.exeも壊れた状態で作成されるため、ワームは感染も発病もしない。

ワームは次に下図のようなプログレスバーを表示する。



ウイルスの活動、
影響

そして、次のエラーメッセージを表示する。



これは壊れたプログラムを装ってユーザーをだます(ワームであることを隠蔽する)ためのものと思われる。

さらにワームはパソコンの再起動時に自分自身が実行されるよう、レジストリに設定を行い、またワームメール発信のためのSMTPサーバーアドレスと、パソコン内部のHTMLファイルからメールの送信先アドレスを収集する。集まったアドレスに対し、ワームを添付したメールを送信する。(上記参照)

Mplayer.exeが5回実行されたことをレジストリに設定したカウンタから知り、発病する。発病内容は、Cドライブファイルの上書き破壊とD,E,F,Gドライブ内の全ファイル削除である。Cドライブのファイルは一部を除きすべて下記の内容で上書きされる。このためパソコンは起動しなくなる。

1-No PeaCe WithOut WaR

```
-
>> TT TT >>> 11>>>OoO>>>9¥Om
>> TiiT >>> YX >>OOo>>11¥Om
>> OXBYL -> Haw >> ()9.9.12MP
_1s00x05y988z877c7y7756477v77x7777g8oro885t55oro312852oro14P,u
```

2- Made By ZaCker

被害の規模

なし

亜種、変種の有無

現時点(2002年12月17日)では知られていない

ウイルスは実行されるとウイルス自身をシステムフォルダにiLLeGaL.exeという名前でコピーする。またシステムフ

フォルダにMplayer.exe(不可視属性)とSMTP.ocxを作成して Mplayer.exeを実行する。

ウイルスは「it was a lil Joke don't be mad :)」と書かれたウィンドウを表示する。

ウイルスはタイトルが「Sorry !」で内容が「Looooooooooooo , thanx fo da time u spent thinkin ov me」のメッセージボックスを表示する。OKを押せば終了する。

Mplayer.exeには下記のメッセージが含まれている。
No Peace Without war,i hate war but im forced to love it,Hidden Power's gonna b there wherever u r

ウイルスは実行されるとレジストリのHKEY_LOCAL_MACHINE¥iLLeGalの値を取得する。この値がなければ、レジストリに1を設定する。値を取得できたときには1増やした値を設定する。1加える前の値が5のときには最後に発病する。

ウイルスはレジストリの
HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥RunServices¥iLLeGal
にウイルス自身のフルパスを設定する。

ウイルスはレジストリの
HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥Outlook¥OMI Account Manager¥Default Mail Account
の値を読み出し、デフォルトのメールアドレスを取得する。そしてレジストリの
HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥Outlook¥OMI Account Manager¥Accounts
以下にあるデフォルトのメールアドレスのSMTP Email Addressの値を取得する。
この値をメールの送信者とする。

ウイルスはレジストリの
HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥Outlook¥OMI Account Manager¥Accounts¥00000001 ¥SMTP
Server
HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥Outlook¥OMI Account Manager¥Accounts¥00000002 ¥SMTP
Server
からSMTPサーバを取得する。

上記で取得できないときにはレジストリの
HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥Outlook¥OMI Account Manager¥Accounts¥00000001 ¥SMTP
Email Address
HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥Outlook¥OMI Account Manager¥Accounts¥00000002
¥SMTPEmail Address

HKEY_CURRENT_USER¥Software¥Microsoft¥Internet Account Manager¥Accounts¥00000001 ¥SMTP Email
Address
HKEY_CURRENT_USER¥Software¥Microsoft¥Internet Account Manager¥Accounts¥00000002 ¥SMTP Email
Address

HKEY_CURRENT_USER¥Software¥Microsoft¥Internet Account Manager¥Accounts¥00000001 ¥SMTP server
HKEY_CURRENT_USER¥Software¥Microsoft¥Internet Account Manager¥Accounts¥00000002 ¥SMTP server
からそれぞれ値を取得する。

いずれの値も取得できないときにはUser5@FBI.govとする。

ウイルスはCドライブを再帰的に検索して拡張子がhtmまたはhtmlのファイルを開く。それらのファイルの中から「mailto:」を探することでメールアドレスを収集する。収集したメールアドレスはシステムフォルダのMmails.dllに書き込まれる。

ウイルスはメールを送信する。レジストリから取得したSMTPサーバに接続するか、MAPI(Outlook)を利用してメールを送信する。受信者は収集したメールアドレスとなり、送信者はレジストリから取得した値(またはUser5@FBI.gov)になる。

ウイルスはシステムフォルダのiLLeGal.exeを添付する。
件名は「Fwd: Crazy illegal sex !」となり、本文は下記のHTMLとなる。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content="text/html; charset=windows-1256" http-equiv=Content-Type>
<META content="MSHTML 5.00.2614.3500" name=GENERATOR></HEAD>
<BODY><FONT face=Arial size=2>
<DIV><FONT face=Arial size=2><FONT face=Arial size=2></FONT></FONT>&nbsp;</DIV>
<DIV><FONT face=Arial size=2><FONT face=Arial size=2></FONT></FONT>&nbsp;</DIV>
<DIV><FONT face=Arial size=2><FONT face=Arial size=2>Note: forwarded message
attached. </DIV>
<P><BR>
<HR SIZE=1>

<DIV><B>Do You Yahoo!</B><BR><A href="" target=_blank>Yahoo! Finance</A> - Get
```

ウイルス動作概要

```

real-time stock quotes <BR></DIV><BR>
<TABLE border=0 cellPadding=4 cellSpacing=0 width="100%">
<TBODY>
<TR class=heada>
<TD><B>Forwarded Message</B> [ <A href="" target=_blank>Save to my Yahoo!
Briefcase</A> &nbsp;&nbsp;&nbsp;<A href="" target=_blank>Download File</A> ]
</TD></TR></TBODY></TABLE>
<TABLE border=0 cellPadding=3 cellSpacing=0>
<TBODY>
<TR class=bge>
<TD align=right noWrap vAlign=top><B><SMALL>From:</SMALL></B></TD>
<TD width="100%"><SMALL><A
href="mailto:Sara1987@yahoo.com">Sara1987@yahoo.com</A></SMALL></TD></TR>
<TR class=bge>
<TD align=right noWrap vAlign=top><B><SMALL>To:</SMALL></B></TD>
<TD width="100%"><SMALL><SMALL><A href=""></A></SMALL><A
href="mailto:Virgin_gurlz_N_boyz@yahoogroups.com"><FONT
color=#0000ff>Virgin_gurlz_N_boyz@yahoogroups.com</FONT></A></SMALL></TD></TR>
<TR class=bge>
<TD align=right noWrap vAlign=top><B><SMALL>Date:</SMALL></B></TD>
<TD width="100%"><SMALL>24 Aug 2002 17:11:18 -0000</SMALL></TD></TR>
<TR class=bge>
<TD align=right noWrap vAlign=top><B><SMALL>Subject:</SMALL></B></TD>
<TD width="100%"><FONT size=2>Fwd: Crazy illegal
Sex</FONT></TD></TR></TBODY></TABLE><BR>
<HR SIZE=1>

<DIV>&nbsp;</FONT></FONT><FONT face=Arial size=2><FONT face=Arial size=2></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><FONT face=Arial></FONT>&nbsp;</DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT size=1><FONT
face=Arial>&nbsp;<FONT size=2>Hii</FONT></FONT></FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff">&nbsp;</DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>Is it
really&nbsp;&nbsp;&nbsp;illegal in&nbsp;&nbsp;&nbsp;da USA?</FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>who knows
:P</FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>If u have a weak
heart i warn u</FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>DON'T&nbsp;&nbsp;&nbsp;see
dis Clip.</FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>Emagine two
young children havin </FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>crazy sex
</FONT><FONT face=Arial>fo&nbsp;&nbsp;&nbsp;da first time togetha ! </FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>loooooo i'm
still wonderin where thier </FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG><FONT face=Arial>parents
were?</FONT></STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff">&nbsp;</DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG>Good Fuck , oh sorry
:&gt;</STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG>i mean Good Luck
;)</STRONG></DIV>
<DIV style="BACKGROUND-COLOR: #ffffff">&nbsp;</DIV>
<DIV style="BACKGROUND-COLOR: #ffffff"><STRONG>&nbsp;&nbsp;&nbsp;Bye</STRONG></DIV>
<DIV
style="BACKGROUND-COLOR: #ffffff">&nbsp;</DIV></FONT></FONT></FONT></BODY></HTML>

```

ウイルスは上記の条件に合致するときには発病する。

発病として下記のコマンドを実行する。

```

command.com /c deltree /y D:¥*.*
command.com /c deltree /y E:¥*.*
command.com /c deltree /y F:¥*.*
command.com /c deltree /y G:¥*.*

```

またCドライブは次図のように一部を除くファイルが215バイトの内容で上書きされ、システムは起動しなくなる。

UPWIZUN	EXE	57,344	06-08-00	5:00p
WAVEMIX	INI	215	12-17-02	6:41p
WAVES	BMP	215	12-17-02	6:41p
WIASERVC	LOG	215	12-17-02	6:41p
WIN	COM	215	12-17-02	6:41p
WIN	INI	215	12-17-02	6:41p
WIN1024	BIN	215	12-17-02	6:41p
WIN386	SWP	37,748,736	12-17-02	6:41p
WIN640	BIN	215	12-17-02	6:41p
WIN800	BIN	215	12-17-02	6:41p
WINCOOL	EXE	215	12-17-02	6:41p
WINFILE	EXE	215	12-17-02	6:41p
WINHELP	EXE	215	12-17-02	6:41p
WINHLP32	EXE	215	12-17-02	6:41p
WININIT	EXE	215	12-17-02	6:41p
WININIT	BAK	215	12-17-02	6:41p
WINIPCFG	EXE	215	12-17-02	6:41p

破壊されたファイルの内容は、次のようなテキストである。

```

1-No PeaCe WithOut WaR

>> TT TT >>> 11>>>0o0>>9\0m
>> TiiT >>> YX >>00o>>11\0m
>> 0XBVL -> Haw >> ()()9.9.12MP
_1s00x05y988z877c7y7756477v77x7777g8oro885t55oro312852oro14P,u

2- Made By ZaCker
    
```

<p>感染・発症防止方法</p>	<p>出所が定かではない添付ファイルを開かない。不明なEXEファイルを実行しない。</p>
<p>ウイルスの駆除方法</p>	<p><確認> ウィンドウズシステムフォルダにiLLeGaL.exe、Mplayer.exeという名前のファイルがあるか確認する。 なお、SMTP.ocxはワームではなく、また感染していなくても存在する可能性があるため、これは無視すること。</p> <p><駆除> ウィンドウズシステムフォルダにあるiLLeGaL.exe、Mplayer.exeという名前のファイルを削除する。</p> <p>レジストリの、 HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥RunServices¥iLLeGaL HKEY_LOCAL_MACHINE¥iLLeGal 各キーを削除する。</p> <p>当該ワームメールを削除する。</p>
<p>その他</p>	<p>報告書作成：2002年12月19日現在</p>

W32/Galil フローチャート

