

# マルウェア解析レポート

[戻る](#)

## ファイル情報

マルウェア解析レポートを作成するために使用されたプログラムファイルの属性情報です。

ファイル名: W3LOVG-F.exe

プログラムの分類: WORM

サイズ: 107008 バイト

作成日時: 2003-03-18 22:48:08 (プログラムが作成された日時)

MD5のハッシュ値: 0x5d73aba7169ebfd2bdfd99437d5d8b11

SHA1のハッシュ値: 0xfd52b4134c4b6c4ec42ca2cb1efa919303bcda83

## アンチウイルスによるマルウェア名

複数のアンチウイルスソフトウェアのスキャン結果です。マルウェア解析レポートを作成するために使用されたプログラムファイルは、定期的にはスキャンされます。結果が[Unknown]の場合は、未検知を意味します。

1. [W32.HLLW.Lovgate.G@mm]
2. [W32/Lovgate.f@M]
3. [WORM\_LOVGATE.F]

## 詳細情報

Windows XPでプログラムを実行した時の動作レポートが記述されています。これらの動作は、プログラムにパラメータ入力やGUI操作などを行わなくても発生した物です。そのため、ファイル作成/コピーやレジストリ変更やネットワーク通信などある場合は、マルウェアである可能性が高いと思われます。本システムは、解析用のプログラムが破壊されていることも検知できます。

1. ファイルをコピーします。

---

### 次の場所に自分自身をコピーします。

コピー元: { 自分自身のファイル }  
コピー先: { システムディレクトリ } \WinDriver.exe  
コピー元: { 自分自身のファイル }  
コピー先: { システムディレクトリ } \WinHelp.exe  
コピー元: { 自分自身のファイル }  
コピー先: { システムディレクトリ } \winrpc.exe  
コピー元: { 自分自身のファイル }  
コピー先: { システムディレクトリ } \WinGate.exe  
コピー元: { 自分自身のファイル }  
コピー先: { システムディレクトリ } \RAVMOND.exe  
コピー元: { 自分自身のファイル }  
コピー先: { システムディレクトリ } \IEXPLORE.EXE  
コピー元: { 自分自身のファイル }  
コピー先: { システムディレクトリ } \kernel66.dll

---

2. サービスをインストールします。

---

サービス名: Windows Management Instrumentation Driver Extension  
説明: Windows Management Instrumentation Driver Extension

実行ファイルのパス:C:\WINDOWS\system32\WinDriver.exe -start\_server

サービス名:il\_reg

説明:Windows Management Instrumentation Driver Extension

実行ファイルのパス:C:\WINDOWS\system32\WinDriver.exe -start\_server

サービス名:Windows Management Instrumentation Driver Extension

説明:Windows Management Instrumentation Driver Extension

実行ファイルのパス:C:\WINDOWS\system32\WinDriver.exe -start\_server

- 
3. 次のレジストリキーを追加します。

**Windows起動時に自動的に実行されるようになります。**

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
WinHelp = { システムディレクトリ }\WinHelp.exe

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
WinGate initialize = { システムディレクトリ }\WinGate.exe -remoteshell

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
Remote Procedure Call Locator = RUNDLL32.EXE reg678.dll ondll\_reg

**.txtファイル実行時の動作を変更します。**

HKEY\_CLASSES\_ROOT\txtfile\shell\open\command  
(null) = winrpc.exe %1

- 
4. 次のファイルやフォルダを検索します。

{ システムディレクトリ }\IEXPLORE.EXE  
winpath\\*.ht\*  
C:\Documents and Settings\{ ユーザ名 }\My Documents\\*.ht\*  
{ システムディレクトリ }\kernel66.dll

5. 次のファイルを改ざんします。

{ システムディレクトリ }\ily668.dll  
{ システムディレクトリ }\Task688.dll  
{ システムディレクトリ }\reg678.dll

6. 次のファイルを作成します。

File: { システムディレクトリ }\ily668.dll

File: { システムディレクトリ }\Task688.dll

File: { システムディレクトリ }\reg678.dll

**Workstationサービスに名前付きパイプで接続します。**

File: \\.\PIPE\wkssvc

**名前付きパイプで接続します。**

File: \\.\PIPE\wkssvc

File: { システムディレクトリ }\kernel66.dll

7. ネットワークのコンピュータに接続してリソースをアクセスします。
-

ダイレクトホスティングSMBサービスでネットワークのリソースにアクセスします。  
TCP ポート445

---

NetBIOSセッションサービスでネットワークのリソースにアクセスします。  
TCP ポート139

---

8. ネットワークのコンピュータに接続してリソースにアクセスします。
- 

ネットワークリソースを列挙します。

---

9. 他のプログラムのプロセスを改ざんします。
- 

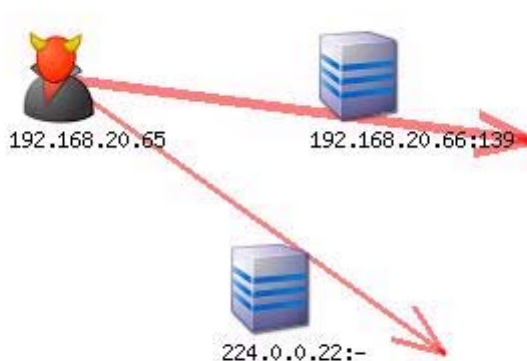
他のプロセスにウイルスコードを挿入して感染力を拡大します。複数のプロセスが改ざんされている場合は、動作中のプロセス全てをターゲットしている可能性があります。

C:\WINDOWS\system32\lsass.exe

---

## ネットワーク通信図

マルウェア解析レポートを作成するために使用されたプログラムが行った通信を視覚化した図です。赤い矢印線は、通信の方向を表します。また、矢印線が太くなると通信量が多いことを表現しています。



本レポートは、SecureBrain Zero-Hour Response System v.1.0 により自動生成されました。

本レポートに含まれる情報の著作権ならびにその他すべての知的所有権は、セキュアブレインへ独占的に帰属します。特別に明示的にセキュアブレインによって許可された場合を除き、事前にセキュアブレインの書面による承諾を得ることなく、ドキュメントの一部または全部を頒布、複製、改変、翻訳、二次的著作物の作成、または手段および形態に関係なく一切禁じられ



ています。

---

(C) SecureBrain Corporation, All rights reserved.