社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（45）
2008 / 7 / 25

端末内の動作監視に基づく情報漏えいウイルスの検知手法に関する検討

鬼頭 哲郎† 松木 隆宏‡ 松岡 正明‡ 仲小路 博史† 寺田 真敏†

†株式会社 日立製作所 システム開発研究所
〒212-8567 神奈川県川崎市幸区鹿島田 890 日立システムプラザ新川崎
‡株式会社 ラック
〒105-7111 東京都港区東新橋 1-5-2 汐留シティセンター11 階

あらまし 近年，P2P ファイル交換ソフトウェアを悪用したウイルスによる情報漏えいが問題となっている．既存のパターンマッチングによる検知手法では，それらのウイルスに対応できるようになる前に，流通速度の速い P2P ネットワークでウイルスが蔓延してしまう危険性がある．本稿では，ユーザ端末内の動作を監視し，情報漏えいウイルス特有の活動を検出することにより，ウイルス感染を検知する手法を提案する．情報漏えいウイルスの活動を個人情報収集活動と収集情報公開活動に分け，それら両方の活動が検知された場合に情報漏えいウイルスに感染していると判断し，ユーザに感染した可能性がある旨を通知する．

キーワード P2P，情報漏えい，プロセス監視，ウイルス対策

A Study on Detecting Information Leak Virus by Activity Monitoring

Tetsuro KITO† Takahiro MATSUKI‡ Masaaki MATSUOKA‡
Hirofumi NAKAKOJI‡ and Masato TERADA‡

† Hitachi, Ltd., Systems Development Laboratory
Hitachi System Plaza Shinkawasaki, 890 Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa, 212-8567 Japan
‡ Little eArth Corporation Co., Ltd.
1-5-2 Higashi-Shinbashi, Minato,Tokyo, 105-7111 Japan

Abstract In these days, it becomes a serious problem that personal/private information are disclosed by computer viruses which abuse P2P file sharing software. It is difficult that the current pattern matching method updates pattern files before spreading viruses over the P2P network. In this paper, we propose the information leak virus detection method based on activity monitoring. We also propose that the activities of information leak viruses consists from two types of activities; "collection of personal/private information" and "disclosure of collected information." And our method serves a notice to the user as infected by the information leak virus when one process performs both of above two activities.

Keyword P2P, Information leakage, Process monitoring, Antivirus

1. はじめに

近年，Winny，Share 等の P2P ファイル交換ソフトウェア（P2P ソフト）を悪用したウイルスによる情報漏えいが多発し，未だ鎮静化の兆しが見えない状況にある．情報の内容によっては漏えいを引き起こした本人以外にも被害が及ぶため，大きな社会問題となっている．特に，個人情報取扱事業者が顧客情報を漏えいした場合には，被害範囲が広範に渡ってしまうことが問題となっている．個人情報が漏えいしたことに対し，企業・組織・経営トップの責任を問う訴訟を起こされた事例も出ている．P2P ファイル交換ソフトウェアによって流出した情報は不特定多数の利用者間で増殖しながら広がっていき，事後にそれら情報を回収することが事実上不可能な状況にあることを鑑みると，このような情報漏えい問題の解決に向けた取り組みが急務である．

我々は，P2P 環境における情報漏えい問題などの解決に向けて，情報流通対策アーキテクチャとそれをベースにした情報流通対策システムを提案している[1]．本稿では，情報流通対策システムの一機能である，暴露ウイルス感染通知機能について，検知方式の検討及び試作を行ったため，これを報告する．

2. 関連技術・関連研究

情報漏えいウイルスに対する対策には，事前対策と事後対策がある．

事前対策としては，端末内の情報をスキャンしてウイルスを検知・駆除する，アンチウイルスソフトによる対策が挙げられる．現在各種アンチウイルスソフト

は Antinny をはじめとする暴露ウイルスなどの情報漏えいウイルスに対応し，それらを検知できるようになっているため，既存の情報漏えいウイルスに対する対策として有効である．また，利用者端末における全てのファイルアクセスを監視し，未知のプログラムからのファイルアクセスを禁止することでファイル流出を防止する方式が喜田らによって提案されている[2]．

事後の措置としては，P2P ネットワークにダミーのデータを流し，流出してしまった情報の取得を困難にする技術があり，ダミーデータを流した場合の影響についての検討が行われている[3][4]．また，株式会社フォティーンフォティ技術研究所の開発した WinnyRadar，ShareRadar は，Winny や Share といった P2P ソフトのネットワークで流通しているファイルの情報を収集し，情報漏えいを起こしてしまった場合の事後対策や経過観測に役立てることができる．

その他，Telecom-ISAC Japan では ISP と連携し，Antinny 感染者への注意勧告を行っている[5]．

また，P2P ネットワークに情報が漏えいしていないかどうかを監視するサービスも存在している．

3. 情報流通対策システム

我々は，P2P 環境における情報漏えいなどの問題への対策として，情報流通対策アーキテクチャ及びそれをベースにした情報流通対策システムを提案している．

情報流通対策システムは，P2P ソフトの利用を妨げることなく，インターネット利用者が安全に，安心して P2P ソフトを利用できる環境を提供することを目的としている．

具体的には，個人情報や機密情報の流出はさせず，著作権侵害ファイルなど不適切なファイルのダウンロードもさせず，その他のファイルの流通は妨げないようにするものである（図 1）．

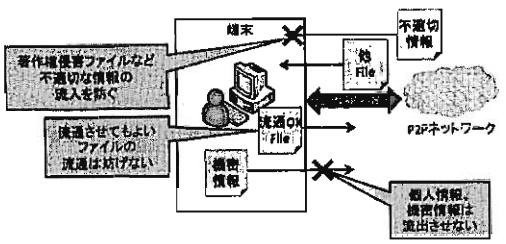

図 1 情報流通対策システム

この情報流通対策システムは，以下の 4 つの機能によって実現される．

1. 意図しないファイルアップロードの防止機能
2. 暴露ウイルス感染通知機能
3. 著作権法上適切でないファイルのダウンロード抑止機能
4. 不正活動ホストの広報機能

本稿においては，2の暴露ウイルス感染通知機能について述べる．

4. 暴露ウイルス感染検知

4.1. 課題と解決策

暴露ウイルスに限らず，ウイルスの検知にはアンチウイルスソフトの利用が有効である．しかし，昨今問題となっている暴露ウイルスは Winny や Share といった日本固有の P2P ソフトをターゲットにしたものであるため，全世界的に流通するウイルスに比べてアンチウイルスソフトベンダの対応が遅れてしまうことが危惧される．また，Winny や Share のネットワークでは，一度ダウンロードしたファイルは他のユーザに向けて公開される．暴露ウイルスはユーザの興味を引くようなファイル名であることが多く，ユーザが目的のファイルと間違えてダウンロードし，そのユーザからもファイルが公開され，ファイルの拡散が促進されるという構造が形成されている．このため，情報の流通速度が速く，アンチウイルスソフトがパターンファイルを更新して検知・駆除できるようになる前に未知のウイルスが蔓延する危険性がある．

上記課題を解決するため，本稿で提案する暴露ウイルス感染検知手法では，パターンファイルなどとのマッチングを取ることで検知するのではなく，暴露ウイルスに共通する動作に基づいて検知を行う．

本稿で述べる暴露ウイルス検知手法は，既存のアンチウイルスソフトに置き換わるものではなく，アンチウイルスソフトと共存し，補助するものである．両方式を併用することにより端末の安全性をより高めていくことができる．

4.2. 検知対象

本検知手法において検知対象とするのは，端末から情報を許可なく外部へと送信してしまう情報漏えいウイルスのうち，Antinny[6]に代表される，P2P ネットワークを介して個人情報などを流通させてしまう暴露ウイルスである．同じ暴露ウイルスでも，感染したユーザ端末を Web サーバにして端末内のファイルを公開する通称山田ウイルス[7]や，取得したスクリーンショットを外部のアップローダにアップロードするような暴露ウイルスは今回の検知手法では対象外とする．

4.3. 暴露ウイルスの挙動

本稿で検知対象とする暴露ウイルスの活動を以下の 2 つのカテゴリ，及びその他の活動に分類する．

- 個人情報の収集
- 収集情報の公開

個人情報の収集に分類される活動には，スクリーンショットの取得や，PC 内のドキュメントファイルやメールボックスなどの収集といった活動がある．

収集情報の公開に分類される活動とは，P2P ネットワークを介して情報を公開するための活動である．例えば，P2P ソフトのアップロードフォルダに収集した個人情報や機密情報を配置する，個人情報や機密情報を収集したフォルダを P2P ソフトのアップロードフォルダとして設定する，といった活動がある．

その他，PC 起動時に自動的に自身が実行されるようにレジストリを書き換える，偽のエラーメッセージを出力する，といった活動を行うものも存在する．

4.4. 感染検知方針

上述した暴露ウイルスの活動に基づいて感染検知を行うが，個々の活動は特異なものではない．

スクリーンショットの取得は，それを行うためのフリーソフトが存在する．ドキュメントファイルを複数まとめて圧縮ファイルを作成する，といった活動はユーザ自身がよく行う活動である．また，設定ファイルの書き換えに関しては，Winny の UI を用いてアップロードフォルダを設定した場合，Winny 自身がその設定を反映させるために設定ファイルを書き換える．

そこで，個人情報の収集に属する活動を行い，かつ，収集情報の公開に属する活動を行ったプロセスを暴露ウイルスとして検知することにした．

5. 提案する暴露ウイルス感染検知機能

以上に述べた感染検知方針に基づき，図 2に示す暴露ウイルス感染検知機能を提案する．

暴露ウイルス感染検知機能は，端末内のプロセスによる OS の機能呼び出し及びファイルシステムへのアクセスを監視する．暴露ウイルス感染検知機能内には個人情報収集検知部と情報公開検知部とがあり，監視によって得られた情報から，個人情報の収集に属する活動，収集情報の公開に属する活動を検知する．

同一のプロセスにより個人情報収集に属する活動，収集情報の公開に属する活動の両方が行われていた場合には，そのプロセスを暴露ウイルスのプロセスであると判断し，暴露ウイルスに感染している可能性が高い旨をユーザへと通知する．

6. 検知機能の実装

6.1. 検知対象の活動

暴露ウイルスの活動のうち今回検知対象とした活動は，スクリーンショットの取得，収集情報のアップロードフォルダへの配置，及び P2P ソフト設定ファイルの改変，の 3 つとした．前記の暴露ウイルス感染検知機能の各検知部と各活動との対応を表 1に示す．

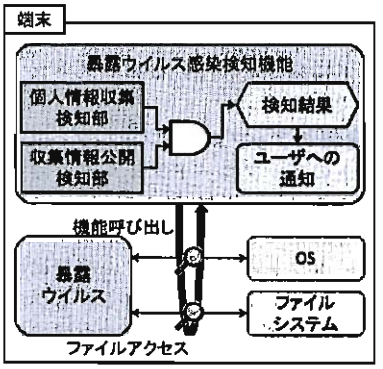

図 2 暴露ウイルス感染検知機能

表 1 検知部と対応する活動

検知部	対応する活動
個人情報収集検知部	スクリーンショットの取得
収集情報公開検知部	収集情報のアップロードフォルダへの配置
	P2P ソフト設定ファイルの改変

6.2. スクリーンショットの取得検知

スクリーンショット取得の検知には，アプリケーションから OS の機能を呼び出す際に API を利用することから，API フックを用いた方式を採用した．API フックにより，端末内のプロセスによる特定の API の呼び出しを検知することができるようになる．しかし，スクリーンショット取得のための専用 API は存在しないこと，スクリーンショット取得には数種類の方法が存在することから，スクリーンショット取得時に使用される API 群を API セットとしてグループ化（表 2）することで，複数の手法によるスクリーンショット取得を検知できる．

具体的には，API フックにより PC 内のプロセスによる API 呼び出しを監視し，いずれかのセットに含まれる API 全てを呼び出したプロセスはスクリーンショットを取得したと判定し，そのプロセス ID とスクリーンショットを取得した旨を記録する．

表 2 スクリーンショット取得用 API セット

API セット#	API
1	GetDesktopWindow
	CreateCompatibleDC
	CreateCompatibleBitmap
2	GetDC(NULL)
	CreateCompatibleDC
	CreateCompatibleBitmap
3	SendInput(VK_SNAPSHOT)
	GetClipboardData

API セット 1 と 2 は，デスクトップのデバイスコンテキストを取得することでデスクトップに表示されて

いる画像を取得する方式である．API セット 3 は，PrintScreen キーを押下したことを OS へと通知し，クリップボードに保存されているデスクトップ画像を取得する方式である．

6.3. 収集情報のアップロードフォルダへの配置検知

P2P ソフトのアップロードフォルダは固定ではなく，また利用する P2P ソフトによっては複数のアップロードフォルダを設定できることから，収集したファイルのアップロードフォルダへの配置の検知には，ファイルシステムへの全アクセスを監視できるファイルシステムフィルタドライバを用いる方式を採用した．

どのフォルダを監視対象とするかに関しては，P2P ソフトで用いるアップロードフォルダを事前に設定し，そのフォルダを監視対象とする方式とする．監視対象のフォルダに対するファイルの新規作成，移動を監視し，ファイルの新規作成や移動が行われた場合にそれを行ったプロセスのプロセス ID とファイルがアップロードフォルダに配置された旨を記録する．

具体的な監視手法を以下に述べる．

ファイルシステムフィルタドライバには，ファイルシステムへのアクセス要求が I/O リクエストパケット（IRP）と呼ばれる形で送られてくる．IRP のうち，フォルダへのファイルの配置に関連するのは，ファイルオブジェクトを開くときに送られる IRP_MJ_CREATE，ファイルの移動やファイル名などの変更時に送られる IRP_MJ_SET_INFORMATION である．ファイルシステムフィルタドライバによりこれらの IRP をトラップし，ファイルの新規作成もしくは移動の要求であるかを確認する．新規作成または移動であれば対象となるファイルのパスを取得し，そのパスが監視対象となっているフォルダ内のものであれば，監視対象フォルダへのファイルの配置であると判断する．

6.4. P2P ソフト設定ファイルの改変検知

設定ファイルの改変の検知においてもアップロードフォルダへの配置の検知と同様に，ファイルシステムフィルタドライバを用いる方式を採用した．

複数の P2P ソフトを利用している環境や，新規 P2P ソフトが出現した場合にも対応可能な方式として，P2P ソフトでアップロードフォルダを指定する設定ファイルを事前に設定し，そのファイルを監視対象とする方式とする．監視対象のファイルに対して書き込みアクセスを行ったプロセスがあればそのプロセスは設定ファイルの書き換えを行ったとしてプロセス ID と設定ファイルが改変された旨を記録する．

具体的には，Winny の場合は Winny.exe と同じフォルダにある UpFolder.txt，Share の場合は Share.exe と同じフォルダにある folder.ini を監視対象ファイルとして設定する．ファイルシステムフィルタドライバにより，IRP_MJ_CREATE をトラップし，要求先のファイルが監視対象のファイルであるかを確認する．監視対象のファイルであった場合には，その要求が書き込み要求であるか確認し，書き込み要求であった場合には監視対象のファイルが改変されたと判断する．

6.5. 感染検知

6.2～6.4節で述べた各活動検知手法により検知された活動を端末内のプロセス ID ごとに記録しておく．同一のプロセスがスクリーンショットを取得し，かつ，収集ファイルのアップロードフォルダへの配置または設定ファイルの改変のいずれかを行った場合に，そのプロセスが暴露ウイルスのプロセスであると判断する．

あるプロセスを暴露ウイルスであると判断した場合，暴露ウイルスに感染している危険がある旨をメッセージボックスによりユーザに通知する．

7. 動作検証

暴露ウイルスの検体に端末を感染させ，今回開発した検知機能で検知可能であるか検証した．

7.1. 環境

検証環境を以下の表 3に示す．

表 3 動作検証環境

端末		VMWare による仮想マシン
OS		Windows XP Professional SP2
P2P ソフト		Winny v2.0β7.1
	パス	C:¥Program Files¥Winny
	アップロードフォルダ	C:¥P2PTest¥Up
暴露ウイルス感染検知機能の設定		-
	ファイル配置監視対象フォルダ	C:¥P2PTest¥Up
	改変監視対象ファイル	C:¥Program Files¥Winny¥UpFolder.txt

7.2. 検証対象の暴露ウイルス

表 4に検証対象とした暴露ウイルスと，推測される暴露ウイルスの活動について示す．表 4の情報は，アンチウイルスソフトベンダである Kaspersky が提供するウイルスデータベースである VirusListJP.com の情報[8]に基づく．

表 4 検証に用いた検体

検体名	Worm.Win32.Antinny.ad
MD5 ハッシュ値	0143222b37c87a5e5f75d60f725d7bde
スクリーンショットの取得	○
個人情報の収集	○
収集情報のアップロードフォルダへの配置	○
P2P ソフト設定ファイルの改変	×

7.3. 検証結果

7.3.1. 検体の挙動

本節では，検証において確認した暴露ウイルスの挙動をまとめる．

7.3.1.1. 全体の動作

検証に用いた検体の時系列的な動作は次の通りである．

- 実行されると自身のコピーを C:¥Windows¥system32¥drivers¥svchost.exe に作成する．
- レジストリの変更を行い，図 3に示すレジストリエントリを追加する．これにより，端末起動時に自動的に暴露ウイルスが実行されるようになる．
- レジストリに書かれたパスとオプションを用いて自身のコピーを起動し，終了する．
- 起動されたプロセスはバックグラウンドで常駐し，スクリーンショット取得，設定ファイル改変を複数回実行する．

```
[HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run]
Windows Driver Adapter =
  "C:¥Windows¥system32¥drivers¥svchost.exe /driver-auto"
```

図 3 暴露ウイルスが追加したレジストリエントリ

以下，本稿で検知対象とする活動に関する動作について詳しく述べる．なお，これらの活動の実行タイミングに規則性を見出すことはできなかった．

7.3.1.2. スクリーンショットの取得

スクリーンショットの取得に関する動作は次の通りである．

- ログインしているユーザの一時フォルダ（C:¥Documents and Settings¥(ユーザ名)¥LocalSettings¥Temp）の中に jktemp，その中に up というフォルダを作成する．
- デスクトップ画像をキャプチャし，作成した「up」フォルダの中に JPG ファイルとして保存する．

7.3.1.3. 収集情報のアップロードフォルダへの配置

今回の検証の範囲では，収集情報のアップロードフォルダへの配置を確認していない．

7.3.1.4. P2P ソフト設定ファイルの改変

P2P ソフト設定ファイルの改変に関する動作は次の通りである．

- Winny.exe と同じフォルダにある UpFolder.txt にアップロードフォルダの設定を追加する（図 4）．既に設定が追加されている場合には上書きする．
- Winny を再起動し，追加した設定を有効にする．

```
[BBS]
path=C:¥DOCUME~1¥(ユーザ名)¥LOCALS~1¥Temp¥jktemp¥up
trip={6DE6FBDE-7707-4D05-AF6D-6F141EC27A59}
```

図 4 設定ファイルに追加された設定

追加された設定は，「path=」で記述されたフォルダを BBS という名前で共有するという設定である．「path=」で記述されたフォルダは取得されたスクリーンショットが格納されているフォルダであり，この設定によりスクリーンショットが P2P ネットワークに公開されることになる．

7.3.1.5. 挙動に関する考察

暴露ウイルスの活動により端末のスクリーンショットが自動的に P2P ネットワークへと公開されることを確認した．

また，暴露ウイルスの挙動の中に，活動が露呈しないように考慮されていると思われる挙動を確認した．実行された際に自身のコピーを svchost.exe として作成するのは，Windows のシステムファイルである同名のファイルとの混同を狙っていると思われる．取得したスクリーンショットを格納するためのフォルダを，ユーザが通常目にすることのない一時フォルダに作成することで，自身の活動を隠蔽していると推測できる．また，設定ファイルに追加した設定を「BBS」という名前にしているのは，Winny が備えている BBS 機能の情報を記録するための設定と混同させて発覚の遅れを狙っていると推測できる．

7.3.2. 感染検知結果

検証対象とした Worm.Win32.Antinny.ad に関し本稿で提案する検知対象の活動として，スクリーンショットの取得及び設定ファイルの改変を検知し，暴露ウイルスの活動であると検知できた．以下，検知対象の活動に対する検知結果，及びそれらを総合して得られる感染検知結果について述べる．

7.3.2.1. スクリーンショット取得

スクリーンショットの取得については，引数が NULL の GetDC，CreateCompatibleDC，CreateCompatibleBitmap の 3 つの API が Worm.Win32.Antinny.ad のプロセス（ID:228）により呼び出された（図 5）．これにより6.2節に示した API セッ

ト2が満たされ，このプロセスはスクリーンショットを取得していたと判断した．なお，このプロセスの実行ファイルは「C:¥windows¥system32¥drivers¥svchost.exe」であり，検証に用いた検体が自身をコピーした先の実行ファイルであった．

```
c:¥windows¥system32¥drivers¥svchost.exe
  PID: 228, Function: GetDC(NULL)
c:¥windows¥system32¥drivers¥svchost.exe
  PID: 228, Function: CreateCompatibleDC
c:¥windows¥system32¥drivers¥svchost.exe
  PID: 228, Function: CreateCompatibleBitmap
```

図 5 スクリーンショット取得検知時のログ

7.3.2.2. 設定ファイルの改変

設定ファイルの改変については，ID:228 のプロセスによって Winny.exe と同じフォルダにある UpFolder.txt が改変されたことを検知した（図 6）．

```
c:¥program files¥winny¥upfolder.txt
  PID: 228, Operation: MODIFY_P2P_CONF
```

図 6 設定ファイル改変検知時のログ

7.3.2.3. 感染検知

個人情報収集検知部により ID:228 のプロセスがスクリーンショットを取得していたことが検知された．また，収集情報公開検知部により ID:228 のプロセスが設定ファイルの改変を行っていたことが検知された．両方の検知部により同一 ID のプロセスの活動が検知されたため，そのプロセスを暴露ウイルスのプロセスであると検知し，メッセージボックスによりユーザへの通知が行われた．

7.3.3. 結果のまとめ

今回開発した暴露ウイルス感染検知機能により，スクリーンショットの取得，設定ファイルの改変といった暴露ウイルスの活動を検知することができ，結果暴露ウイルスに感染していることを検知することができた．これにより，本稿で提案する暴露ウイルス感染検知手法が有効に働くことを確認した．

8. まとめと今後の課題

本稿では，端末内の動作監視に基づいた情報漏えいウイルスの検知手法に関して提案を行った．具体的には，暴露ウイルスの活動を個人情報の収集と収集情報の公開の2つに分け，個人情報の収集に分類される活動と，収集情報の公開に分類される活動を両方とも行ったプロセスを暴露ウイルスのプロセスとして検知する手法について提案した．

また，提案手法を実装し，実際に暴露ウイルスのプロセスを検知することができることを確認した．

現状の問題点としては，個人情報の収集活動検知部分に関して，スクリーンショットの取得にしか対応しておらず，検知可能なウイルスを限定しているという点がある．また，プロセス ID ごとに監視を行うため，一つ一つの活動を別プロセスで実行された場合には検知することができない，という点も問題点として挙げられる．これらの問題点に関しては，今後ドキュメントファイル収集などの活動を検知できるように拡張する，親プロセスなどの情報も含めて監視する，などの手法によって汎用的な検知を目指していく．

また，本稿で提案した機能は情報流通対策システムの一機能として位置づけている．今後は他の機能と連携させ，実環境における有効性の検証などを行っていきたい．

謝辞

本研究は総務省から受託した「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」の成果の一部です．本研究を進めるにあたって有益な助言と協力を頂いた関係者各位に深く感謝いたします．

文　献

[1] 寺田真敏 他：P2P ファイル交換ソフトウェア環境における情報流通対策アーキテクチャの検討，情報処理学会 CSEC 研究報告 No.21 pp.243-248(2008 年 3 月)

[2] 喜田弘司 他：ファイルアクセス制御エージェントの提案：P2P 型ファイル共有システムのセキュアな利用を目指して，情報処理学会論文誌 Vol.48 No.1 pp.200-212(2007 年 1 月)

[3] N. Christin, A. Weigend, and J. Chuang, "Content Availability, Pollution and Poisoning in Peer-to-Peer File Sharing Networks," ACM E-Commerce Conference (2005)

[4] J. Liang, R. Kumar, Y. Xi, and K. Ross. "Pollution in P2P file sharing systems." Proc. IEEE INFOCOM'05(2005)

[5] Telecom-ISAC Japan：ISP との連携による ANTINNY ウイルス感染ユーザへの注意喚起の取り組み，https://www.telecom-isac.jp/news/news20060315.html

[6] VirusListJP.com, Worm.Win32.Antinny.a http://www.viruslistjp.com/viruses/encyclopedia/?virusid=111218

[7] VirusListJP.com, Backdoor.Win32.Mellpon.a, http://www.viruslistjp.com/viruses/encyclopedia/?virusid=78589

[8] VirusListJP.com, Worm.Win32.Antinny.ad http://www.viruslistjp.com/viruses/encyclopedia/?virusid=76580