資料５
情報セキュリティ担当者向け資料

ＰＣ上で確認できる流出情報の検索方法

Antinny による情報流出は、当該ウイルスに感染してから適切な流出防止策を講ずるまでの間続きます。Antinny への感染は、Winny 利用者が Winny で構成されているネットワーク（以下「Winny ネットワーク」とする。）から動画や画像ファイルなどをダウンロードした後、入手したファイルに仕込まれている Antinny を実行したことで発生している場合が多いようです。

パーソナルコンピュータ（以下「ＰＣ」という。）が Antinny に感染すると、Antinny が Winny の機能を悪用してインターネットに流出させるファイルを保存しておくためのフォルダ[1]（以下「流出用フォルダ」という。）が作られ、当該ＰＣに保存されているファイル（当該ＰＣに接続されている外部記憶装置に保存されているファイルを含む。）や、当該ＰＣのデスクトップ画像が保存されます。流出用フォルダのファイルはWinnyによりWinnyネットワークを通じてインターネット上に公開されます[2]。Antinnyによるデータの収集保存は、感染期間中に任意の時期に繰り返し行われる場合もあるようです。

以下では、Antinny により作成されたファイルの探索方法を紹介します。なお、最近の事例では、現に情報流出が発生しているにもかかわらずＰＣに流出したファイルが残っていない事例（現在のところ原因不明）もあることから、ここにある方法で流出ファイルが発見されなかったからといって流出事案が発生していないというわけではないことを断っておきます。また、Antinny は亜種の発現頻度が極めて高いことから、既存のものとは異なる活動を行うものが発現する可能性もありますので、作業を実施する際にはウイルス対策ソフトウェアベンダ等が提供する情報を確認するようにしましょう。

最後に、Antinny に感染しているＰＣは他のコンピュータウイルスにも感染している場合が多く、そのウイルスの中にはデータの破壊などといった活動を行うものがあるため、作業を実施するに当たっては、ＰＣの所有者の同意が取れれば、コンピュータウイルスに感染していないこと及び既知の脆弱性が除去されていることが確認されている別のＰＣにハードディスク等を接続して行うことをお勧めします。

１　調査方法

(1) インターネットから切断する

作業中において、更なる流出を避けるためネットワーク機器類を確実に停止させます。

例　：ＬＡＮケーブルを抜く

　　：無線ＬＡＮ関連デバイスの停止

(2) ＰＣのエクスプローラの設定の確認

Antinny は隠しフォルダ内にファイルを保存しますので、エクスプローラではすべての拡張子と隠しファイルやフォルダを表示させるようにしておきます。多くの場合 Antinny は流出用フォルダを隠しファイルの属性とする等して発見しにくくしています。

---

[1] アップフォルダはウイルスにより自動的に作成されます。

[2] ウイルス対策ソフトウェアで Antinny を駆除した場合、アップフォルダ中のファイルの削除は行わないため、それだけでは情報流出を停止することはできません。

エクスプローラのメニューバー「ツール」
→「フォルダオプション」
→「表示」タブを選択
□ システムフォルダの内容を表示する　(WindowsXP のみ)
（チェックする）
□ すべてのファイルとフォルダを表示する
（チェックする）
□ 登録されているファイルの拡張子は表示しない
（チェックを外す）
□ 保護されたオペレーティング システム ファイルを表示しない
（チェックを外す）
設定を変更した場合、「ＯＫ」ボタンにより反映させます。

(3) 流出したファイルの検索

Antinny では、ＰＣのスクリーンショット画像が「[****] ****のデスクトップ****.jpg」というファイル名で、ＰＣ内に保存されていたデータが「[****] ****のドキュメント****.zip」というファイル名（「****」は任意の文字列）で流出用フォルダに作成されます。またＰＣに保存されていたファイルの複製が流出用フォルダに作成される場合もあるようです[3]。流出したファイルを検索するに当たってはこれらのファイル名の特徴をキーとしてファイルを検索します。

※ ファイルを検索する際は、検索時の詳細設定オプションとして「隠しファイルとフォルダの検索」を必ず指定して実行してください。

※ フォルダによっては、権限の無いユーザでは確認ができません。家族でＰＣを共有しており、複数のユーザを登録して使い分けている場合は、すべてのユーザで確認するか、管理者権限を有するユーザで確認してください。

① Winny の設定ファイルからの確認方法

Antinny は作成したファイルを Winny を利用して流出するように Winny の設定ファイル「UpFolder.txt」（通常 Winny の実行ファイルと同じフォルダに保存されている。）を変更しますので、そのファイルの内容を確認します。「UpFolder.txt」をキーとしてファイルを検索することで当該ファイルは見つけることができますので、当該ファイルが見つかりましたら、テキストエディタで開き、内容を確認してください。以下に、Antinny がアップフォルダの設定を変更し、流出用フォルダを作成している場合の設定例を紹介しますので参考としてください。

※ Winny を削除していた場合

Winny をフォルダごと削除していた場合やＯＳを既にインストールし直している場合などには、「UpFolder.txt」を検索することができない、または改変が確認できないことがあります。その場合②の方法で流出ファイルを検索します。

[3] 操作ミス等の原因により、Winny の本来のアップフォルダに業務ファイルの複製を作成してしまう場合もあるようです。

［仁義なきキンタマ］○○のドキュメント.zip の場合

※　○○にはユーザ名が入る

［BBS］の部分にアップ用のフォルダが記述されています。

```
［BBS］
path=C:¥DOCUME~1¥○○¥LOCALS~1¥Temp¥jktemp¥up
trip={$$$$$$$$-$$$$-$$$$-$$$$$$$$$$$$}
```

C:¥Documents and Settings¥○○¥Local Settings¥Temp¥jktemp¥up フォルダ内のファイルを流出させる設定となります。

［仁義なきキンタマ］○○(@@@@@@@@)のドキュメント.zip の場合

```
［BBS］
path=C:¥DOCUME~1¥○○¥LOCALS~1¥Temp¥4407A9BE6535¥773232357FF9
trip={$$$$$$$$$$$$$$$$}
```

C:¥Documents and Settings¥○○¥Local Settings¥Temp¥4407A9BE6535¥773232357FF9 フォルダ内のファイルを流出させる設定となります。

※この例で紹介した Local Settings フォルダは隠しフォルダのため、エクスプローラの設定変更が必要です。

Antinny によって作り出された流出用フォルダが見つかりましたら、ＰＣに保存されていたファイル自体に加えて、以下のファイルの有無を確認してください。ファイル名は Antinny の種類により若干異なる場合があります。

なお、流出用フォルダ内のファイルは、コンピュータウイルスが混入している場合があります。ファイルをむやみに解凍したり、閲覧したりしないようにしましょう。特に圧縮ファイル内に存在する「.exe」の拡張子を持つファイルは Antinny の可能性が高いプログラム実行ファイルです。疑わしいファイルが発見された場合は別途ウイルス感染しても実害が発生することのないコンピュータで内容を分析しましょう。

Antinny が作り出すファイルの一部を紹介します。

○　スクリーンショット（ＰＣ画面をキャプチャした画像ファイル）の流出

（主なファイル名）

［※※※※］○○のデスクトップ(日付-時刻).jpg
［※※※※］○○(@@@@@@@@)のデスクトップ(日付-時刻).jpg

※には文字、○○にはユーザ名、@には英数文字が入ります。

○　圧縮ファイル（Antinny が収集したファイルを圧縮したもの）の流出

（主なファイル名）

［※※※※］○○のドキュメント.zip
［※※※※］○○(@@@@@@@@)のドキュメント.zip

② ファイルが発見できなかった場合及びWinnyが既にアンインストールされていた場合

改変された設定を確認できなかった場合は、「のドキュメント」「のデスクトップ」を検索キーとしてファイルを検索します。ただし、ＯＳの再インストールを実施した後では、ファイルを見つけることができない場合があります。

(4) 流出したファイルの確認

(3)で発見したファイルの内容を確認します。確認に当たっては、必ずインターネット等のネットワークから切断されていることが確認されたＰＣで実施してください。（作業用ＰＣは作業終了後にクリーンインストールすることが望ましいので、それが可能なＰＣを用意することをお勧めします。）

なお、ここまでの作業で発見したファイルは、現に流出が継続していたデータに過ぎません。過去にこれ以外のファイルが流出したか否かについて確実に特定する方法はありません。