情報流出を引き起こすAntinnyの特徴

情報流出の被害範囲の特定や根本的な情報流出防止策の策定に当たってAntinnyの特徴を知ることは極めて重要です。この資料では、事案発生時の対応の一助となる Antinny の特徴を紹介します。なお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。また、以下の確認作業を実施するにあたっては必ずインターネットから切断されていることを確認の上で実施してください。

１　Antinny感染時の経緯

Antinny の感染ルートについてはそのすべてが判明しているわけではありませんが、少なくともWinnyネットワークからダウンロードしたファイルに混入されていることが確認されています。Winnyによりダウンロードしたファイルやウイルスファイルの有無を調べることで、感染原因の候補が判明する場合があります。

(1) ダウンロードしたファイルの検索

Winny では、ダウンロードする時の保存場所をあらかじめ設定しておく必要があります。初期設定での保存場所はWinnyの本体の実行ファイルが保存されているフォルダ内の「Down」フォルダになります。このフォルダにはAntinnyを含んだファイルが保存されている場合があります。

(2) Antinny関連ファイル

Antinnyによる感染の原因を調査する場合、感染源となるファイルとAntinnyが作成したファイルを調査する必要があります。

①　感染源ファイル

以下の例に挙げたようなファイル名で感染源となるウイルスファイルが存在することが確認されています。これらのファイルは、ダウンロードした圧縮ファイル等の中に含まれ、パーソナルコンピュータ（以下「ＰＣ」という。）上で解凍後に実行することで Antinny に感染します。なお、以下の例以外のファイル名のものも存在する可能性があります。

【感染源となるファイルの名前の例】
- 新しいフォルダ　…(空白)…　.exe
- 新しいフォルダ(2)　…(空白)…　.exe
- 新しいフォルダ.exe
- PHOTOS.exe
- ホームページ.exe
- レポート.exe
- ダウンロード.exe
- デジカメ.exe
- 家.exe

②　Antinnyにより作られたファイルの検索

Antinny の活動が始まると、ウイルスファイルのコピーやいくつかのファイルをシステムフォ

ルダ内に保存します。Antinny の種類によりファイル名や保存される場所は異なります。以下に一例を紹介します。なお、システムフォルダはＯＳによりフォルダ名が異なります。

[仁義なきキンタマ]〇〇のドキュメント.zip の場合（「〇〇」はユーザ名。以下同様）

・svchost.exe（Antinny 実行ファイル）
　　C:¥WINDOWS¥system32¥drivers フォルダ内
・空白　　（値の設定なしと表示）　　.exe
　　C:¥WINDOWS¥system32¥wbem フォルダ内

[仁義なきキンタマ]〇〇(@@@@@@@@)のドキュメント.zip の場合（以下「@@@@@@@@」は８桁の英数字。以下同様）

・svchost.exe（Antinny 実行ファイル）
　　C:¥WINDOWS¥system32¥Microsoft フォルダ内
・winms.exe
　　C:¥WINDOWS¥system32¥フォルダ内

(3) レジストリの改ざん

Antinny は、ＰＣの再起動時に(2)で例示したファイルで再び活動できるようにするための設定をレジストリ内に書き込みます。レジストリエディタを起動して、この設定の有無について確認します。

① 「スタート」ボタンをクリックし、「ファイル名を指定して実行」をクリックします。
② テキストボックス内に「regedit」を入力し、レジストリエディタを起動させます。
③ Antinny を起動するファイル名で探索します。

※探索結果としての代表的な例を以下に紹介します。

[仁義なきキンタマ]〇〇のドキュメント.zip の場合

¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
→「HKEY_LOCAL_MACHINE」
→「SOFTWARE」
→「Microsoft」
→「Windows」
→「CurrentVersion」
→「Run」

「名前」の列　「Windows Driver Adapter」
「データ」の列　「C:¥WINDOWS¥system32¥drivers¥svchost.exe /device-auto」

※Antinny が追加したファイルは C:¥WINDOWS¥system32¥drivers に存在します。

[仁義なきキンタマ] ○○(@@@@@@@@)のドキュメント.zip の場合

¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥RunOnce
→「HKEY_LOCAL_MACHINE」
→「SOFTWARE」
→「Microsoft」
→「Windows」
→「CurrentVersion」
→「RunOnce」

「名前」の列　「Windows Security Manager」
「データ」の列　「C:¥WINDOWS¥system32¥Microsoft¥svchost.exe -c -ax」

※Antinny が追加したファイルは C:¥WINDOWS¥system32¥Microsoft に存在します。

(4) Antinny プロセス

Antinny に感染後、またはＰＣの再起動時に、(2)②で発見した Antinny 実行ファイルがログインユーザの権限で実行されます。この活動は、Windows プロセスで確認ができます。

以下では、WindowsXP でのプロセス確認作業を例として紹介します。

① 「Ctrl」＋「Alt」＋「Del」を同時に押し、Windows タスクマネージャを表示させます。
「プロセス」タブ画面からプロセスを探します。

② 一覧表示から「ユーザ名」を２回クリックします。
（２回クリックすると、ログインユーザのプロセスが上段に表示されます。）

③ 「ユーザ名」がログインユーザであるイメージ名「svchost.exe」((2)②で異なるファイル名のものが発見されていればそれを探します。）を探します。

④ もし発見されれば、当該パソコンにおいて Antinny が活動している可能性が極めて高いと言えます。

２ Antinny ウイルスの特徴情報について

Antinny の代表的な検体の特徴情報について紹介します。

(1) 検体その１

ファイルサイズ 11,539,968 (11.0MB)

MD5 HASH 54540d887aa7fcb1ff388bff05f52e0c

ウイルス検索ソフト対応(検出)状況

ウイルスバスター２００６	TROJ_UPBIT.A
Symantec AntiVirus	W32.HLLW.Antinny.G
McAfee virusscan	W32/Generic.Delphi.b

① 検証ファイルの実行にて感染活動が開始

② ファイルの追加

svchost.exe
C:¥WINDOWS¥system32¥Drivers フォルダ内

.exe （ファイル名はなし）
エクスプローラー上では、(値の設定なし) .exe と表示される
C:¥WINDOWS¥system32 フォルダ内

③ レジストリへの記述追加

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
［**名前**］
Windows Driver Adapter
［**データ**］
C:¥WINDOWS¥system32¥drivers¥svchost.exe /device-auto

④ フォルダの作成

ウイルスの活動により、C:¥Documents and Settings¥〇〇¥Local Settings¥Temp フォルダ内に以下のフォルダが作られます。

jktemp
├ up （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。））
└ packed

⑤ スクリーンショットの保存

流出用フォルダに [仁義なきキンタマ]〇〇のデスクトップ.jpg を保存します。

⑥ ファイルの収集及び保存

流出用フォルダに [仁義なきキンタマ]〇〇のドキュメント.zip として保存します。

(2) 検体その２

ファイルサイズ 11.6 MB (12,182,528 バイト)
MD5 HASH 25accbf5e49c6d8c9cd8f726e88955d0

ウイルス検索ソフト対応(検出)状況

ウイルスバスター２００６	TROJ_ANTINNY.AX
Symantec AntiVirus	W32.Antinny.AX
McAfee virusscan	W32/Antinny.gen!p2p

① 検証ファイルの実行にて感染活動が開始

[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 ファイルの追加

```
svchost.exe
  C:¥WINDOWS¥system32¥Microsoft フォルダ内
    ﾌｧｲﾙｻｲｽﾞ  11,897KB

winsm.exe
  C:¥WINDOWS¥system32 フォルダ内
    ﾌｧｲﾙｻｲｽﾞ  891KB

svdat.m1v
  C:¥WINDOWS フォルダ内
  ﾌｧｲﾙｻｲｽﾞ  1KB
```

③ レジストリへの記述追加

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥RunOnce
  [名前]
    Windows Security Manager
  [データ]
    C:¥WINDOWS¥system32¥Microsoft¥svchost.exe -c -ax
```

④ フォルダの作成

C:¥Documents and Settings¥〇〇¥Local Settings¥Temp フォルダ内に以下のフォルダが作られます。

4407A9BE6535
- ├ 773232357FF9　　(Antinny による流出用フォルダとなります。)
- └ 6A8C9B51993A

⑤ スクリーンショットの保存

流出用フォルダに[仁義なきキンタマ]〇〇(@@@@@@@@)のデスクトップ(日付-時刻).jpg を保存します。

⑥ ファイルの収集及び保存

以下の拡張子のファイルのあるフォルダを収集します。

.doc
.xls
.eml
.ppt
.dbx
.txt
.pdf

上記ファイルが保存されている主なフォルダ

Favorites
Recent

COOKIES

OUTLOOK EXPRESS

MY DOCUMENTS

流出用フォルダに　[仁義なきキンタマ]〇〇(@@@@@@@@)のドキュメント.zip　として保存します。

ファイルは分割されて保存される場合があります。

[仁義なきキンタマ] 〇〇(@@@@@@@@)のドキュメント.zip

[仁義なきキンタマ] 〇〇(@@@@@@@@)のドキュメント vol.2.zip