

名前の由来

友人の山田くんがメッセで送ってきた
youjo.exeを踏んで感染したという[書き込み](#)より。

症状

感染するとhttpサーバを立ち上げ、感染者のスクリーンショット(*1)やハードディスクの中身を参照可能な状態にします。
また掲示板に自らのリモートホスト(*2)を書き込もうとします。
さらにhostsファイルを書き換えることによりマイクロソフトやセキュリティベンダーへの名前解決を妨害します(*3)。

**【危険】感染者に外部から任意のコマンドを実行可能にしてしまうようです、
[これを利用した攻撃の例がこちらです。](#)(*4)**

掲示板への書き込みは亜種によって異なります。2ちゃんねる(*5)へ書き込もうとするものがほとんどですが、中にはJBBSなどに書き込もうとする亜種もあるようです。
リモートホストの晒し方も複数あり、IPアドレスとコンピュータ名を晒すもの、fusianasan(*6)を使うもの、グローバルアドレスからホスト名を所得するものなどが確認されています。
現在は2ちゃんねる側で対策が施されており、ウイルスによる書き込みはほとんど阻止されているようですが、トラップをすり抜ける新種も現れたようです。また、TCP/IPプロトコルを使っている限り**あなたのIPアドレスを所得する機会はいくらでもあります。**

亜種によってはUPnPを利用してUPnP対応ルータやWindows XP付属のファイアウォールを超えるものも確認されています(*7)。
また、<http://127.0.0.1/>ではアクセスできないものもあるようです。

ウイルスが設置したhttpサーバはある程度のアクセスがあるとエラーを起こして終了します。

ウイルス本体のファイル名はsvchost.exeとなっているものが主流ですが、youjo(空白).exeやrundll32.exe、mdi.exeとなっているものもあるそうです。

起動時にウイルスが存在するフォルダの下にmellpon、fusianasan、kawaisosu、yamadaといった名前のフォルダを作り、ハードディスク内の全ファイルのリストをそこに置くようです。

感染源・感染経路

ShareなどのP2Pネットワークやうpろだ(*8)からファイルをダウンロードしてそれを実行してしまうことにより感染します。ロリ画像や少年ジャンプのスキャン画像、音楽関係のものなどが確認されています。



どうやらファイルの種類をアイコンで判断し、フォルダを開いたつもりで実行してしまうケースが多いようです。

このときウイルスが同名のフォルダを作成し、その中に本物のファイルを設置するため感染したことに気づきにくいようです。

感染時にウイルス本体を%ProgramFiles%内のランダムなフォルダの下にコピーし、Windows起動時にウイルスを実行するようにレジストリまたはスタートアップを書き換えます。hostsファイルが書き換えられるのはどうやらこのタイミングのようです。C:\boot.iniも書き換えるようです。

なお、山田亜種Makerというものも流通していて、これによりウイルスに任意の画像を埋め込んで偽装することと2ちゃんねるへの投稿文の改変が可能になっています。

感染確認方法

[ニユイルススレの通報屋氏が山田チェックツールを公開しています。](#)

なお、これを使って疑いがあるとされた場合でも、次にあげる確認方法を試してみて全て大丈夫であった場合は、安心していいと思います。(*9)

- <http://127.0.0.1/>をブラウザで表示させ、~ss.jpgやC.htmlといったものが見えるならば、感染しています。<http://127.0.0.1/~ss.jpg>で自分の画面が表示されても感染しています。
- 上のリンクで見えない場合、ウイルスによりブロックされている可能性もありますので念のために[プロキシを使って自分のホストをブラウザで表示](#)させてみてください。
- メモ帳などでC:\Windows\system32\drivers\etc\hosts"というファイル(*10)を開いてみて「127.0.0.1」以外のIPアドレスが記載されていたら感染している可能性があります。なお「#」で始まる行はコメントとして無視されるので問題ありません。
- svchost.exe(*11)やrundll32.exe(*12)、mdi.exe(*13)といったプログラムが実行されていてそれが標準の場所以外にある場合、ウイルスの可能性が高いです。実行されているプロセスを調べるにはSlightTaskManagerというソフトが便利です。
- 上で書いてあるファイル名のプログラムが実行されていないからと言って、安心してはいけません。できたらひとつひとつ実行されているプロセスを調べ、覚えのない物があつたら下の駆除方法を試してみましょう。ただし、本来必要な物まで消してしまう可能性がありますので、設定を元に戻せるように作業時は逐一メモを取ってください。

svchostプロセスの起動している数は環境によってまちまちです。また、svchostプロセスのユーザー名で判断する方法は今のところは有効ですが、SYSTEMというユーザー名で動かすことも技術的には可能ですので、安心できません。実行されているプロセスの場所を特定した方がより確実となります。

駆除方法

悪質な攻撃を受ける可能性がありますので、感染していると分かったらすぐにLANケーブルや電話線を抜いておくことをお勧めします。

まずウイルス本体の位置を確認してください。

確認したら、レジストリエディタ(*14)を起動し、左のツリーから

```
+HKEY_LOCAL_MACHINE
+SOFTWARE
+Microsoft
+Windows
+CurrentVersion
+Run
```

と開き、ウイルス本体が記述されている箇所があったら削除します。次に

```
+HKEY_CURRENT_USER
+Software
+Microsoft
+Windows
+CurrentVersion
+Run
```

を開き、同じように削除します。

スタート すべてのプログラム スタートアップを見て、上から順番に右クリック プロパティを実行し、そのリンク先がウイルスだったらもう一度スタートアップの該当するものを右クリックして削除します。

メモ帳を起動して開くを選び、ファイルの種類を「すべてのファイル」にしてファイル名の欄に「C:\Windows\system32\drivers\etc\hosts」(*15)と入れて開きます。「#」で始まる行と「127.0.0.1 localhost」という行以外のものがあればそれらを全て削除して上書き保存しましょう。

これらの操作後、再起動して山田ウイルスらしき挙動が確認できなければ、まず大丈夫です。ウイルスの活動が止まったことを確認したら、ウイルス本体をフォルダごと削除しましょう。

誤って重要な物を削除してしまわないように、メモを取りながら作業することをお勧めします。また、これらの作業は自己責任でお願いします。

なお自由にコマンドを実行可能なため、感染している間に何をされていてもおかしくありません、念のため使っていたハードディスクを全てフォーマットし、システムを完全に入れ直した方がいいでしょう。
やり方がよく分からない方は「クリーンインストール」という言葉を自分で調べてください。

被害の予防

P2Pは使わない

OpenNapクライアント(*16)、WinMX、Winny、Shareといったファイル共有ツールを使用していると、ウイルスに感染する確率が飛躍的に上がります。これらのツールは使わないようにしましょう。

拡張子は表示させる

エクスプローラのツール フォルダオプション 表示というところで「登録されている拡張子を表示しない」というチェックを外しましょう。

これによりファイルの種類をファイル名から特定できるようになります。

フォルダのアイコンで拡張子(*17)がexeならばそれはアプリケーションです。

ただし、多数の空白が拡張子の前に挿入されている場合もありますので注意しましょう。

hostsファイルをチェックする

www.hoge.comといったURIを123.45.67.89といったIPアドレスに変換する時に参照されるhostsファイル(*18)を書き換えられてしまうと、セキュリティベンダーのサイトが見られなくなったり**ファームウェア詐欺**にあたりたりします。これを防ぐために、Windows 2000/XPではNTFSというファイルシステムの機能を用いてhostsファイルのアクセス権を制限するという方法があります。やりかたは、hostsファイルを右クリックしてプロパティを選び、上のタブからセキュリティを押します。次に、継承可能なアクセス許可を...の所のチェックを外し、削除を選びます。名前欄が空欄になったら右の追加を押してEveryoneを追加し、アクセス許可は読み取りのみにしておきます。Windows 9xの方や、NTFSを利用していない方は何日かに一度、メモ帳等でhostsファイルを開

き、先頭が「#」の行と「127.0.0.1 localhost」という行以外が記述されていたら全て削除してください。

怪しいリンクや添付ファイルは開かない

掲示板やメールなどに記載されたアドレスにウィルスが潜んでいる場合があります。例えば拡張子が画像ファイルのようでも実際は違うものがありますので注意しましょう。

専用ツールを使う

自己解凍ファイルのアイコンを使ったウィルスも普及していますので、その形式に対応した解凍ツールを使いましょう。[WinRAR](#)などが多機能でお勧めです。なお、解凍ツールによっては指定したフォルダと違う場所に展開してしまうものもあります。解凍したらスタートアップに何か追加されていないか確かめた方がいいでしょう。画像を見たいだけの場合は[書庫形式のまま中身が閲覧できるビューア](#)も多数あります。(*19)

ルータを導入する

ルータを設置して外部から繋がれるのを防ぎましょう。ただし設定でポートはできるだけ閉じておき、UPnP機能は無効にしておきます。ルータによっては外部からでも設定が変更できてしまうものもあります。そのようなルータの場合は買い換えるか、認証パスワードを複雑で長いものにしておきましょう。

ファイアウォールを導入する

Windows XP標準のファイアウォールは信用せず、他のファイアウォールを導入しましょう。無料で使える[ZoneAlarm](#)は設定も容易です。

アンチウィルスを導入する

アンチウィルスソフト(*20)を入れて、なおかつアップデートはこまめにしましょう。せっかくソフトを入れていても有効期限が切れていたり無効になっていたりしたら意味がありません。買うのがどうしても嫌ならば[無料のアンチウィルスソフト](#)もあります。しかし、山田のような新種のウィルスには役に立たないことが多いので過信は禁物です。

システムは最新に

ソフトウェアにバグはつきものなので、使っているソフトが更新されたらできるだけすぐに新しいものを導入してください。Windows Updateもこまめに利用して、環境をできるだけ最新のものにしておきましょう。

重要なデータはハードディスクに保存しない

クレジットカードの番号や暗証番号、顧客リストなどをハードディスクに保存しておくとかの拍子でネット上に流出してしまう(*21)恐れがあります。このようなデータはできるだけパソコンに入れずに管理し、どうしてもコンピュータで処理させたい場合はUSBメモリなどの外部媒体を利用しましょう。ハードディスクで運用する場合そのパソコンを外部ネットワークから切り離すことを勧めます。

アイコンを標準のものから変えておく

フォルダやzipファイルのアイコンをWindows標準のものから変えておくだけでそれが本当にフォルダやzipファイルなのか見分けやすくなります。

htmlメールは表示しない

Windows付属のOutlook Expressでメールを開いた場合、勝手に添付してあるhtmlを開いてしまいます。他のメールソフトを利用し、htmlは開かない設定にしておきましょう。OE以外を使っている場合、そこから弱点が突かれる可能性があります。

ネットについて勉強する

プロトコルやポート、パケットといった用語や、名前解決・ルータの役割、などについて自分で勉

強してください。人に頼っていてその人任せにしていると、[その人が勘違いをしていた場合](#)に対処できなくなります。わからないことは人に聞く前に[Google](#)等で調べる癖をつけましょう。なお一部の雑誌では「**悪用厳禁!**」や「**無修正画像全部ぶっこぬき!**」などと題して暗に読者に犯罪行為を促している物があります。このような雑誌は決して信用しないように注意してください。

山田ウィルスデータ参考

ヤマイモ木から生えてくる観察ブログ：山田ウィルス

<http://nemoba.seesaa.net/article/2891535.html>