

何かあったらしいと飛んできた人へ

自分が該当するか不安でとりあえず来た人は、必ず右側の「今北産業はここから」の各項目、リンクのまとめを見て下さい。そろそろ沈静化しつつありま(････)ス。
初めて山田ウイルスを知った人は、前山田ウイルスと今回の山田オルタウイルスは動きは似ていますが、**確認箇所**が違います。
Winnyばかりが取り上げられていますが、テンプレの通りWinny、Shareの両方での感染が確認されています。

マイクロソフトの[日本のセキュリティチームの Blog](#) で有名な奥天さんが山田（オルタは書いてませんけど）にも対応しようと奮闘されているようで(････)ス。
ふぁいと(････)ス。

悪意のあるソフトウェアの削除ツールが対応しました。
Microsoft (Windows) Update しましょう (2006/04/12)
[日本のセキュリティチームの Blog / 4月のセキュリティリリース](#)
また、「悪意のあるソフトウェアの削除ツール」では、いわゆる「山田オルタナティブ」の一部に対応しており、Agent.AE として検出します。
Agent ファミリ全体ではなく、Antinny 対応の一環として追加しています。

[ヲチャ回帰\(････\)カイク山田ヲチスレ 222](#)

430 名前: [名無し]さん(bin+cue).rar [sage]
投稿日: 2006/04/12(水) 06:36:30 ID:ZH35tmUQ0
>>427>>428 mjsk!
というわけで試した。山田オルタナティブ (Me11-1-0.11) に感染したマシンで Windows Update 実施。

「悪意のあるソフトウェアの削除ツール」4月版が実行され、Me11-1-0.11のファイルupdate.exeと稼働中していたプロセス、自動実行レジストリがあぼーん。

検出された名前はBackdoor:Win32/Agent.AE。
情報ページへのリンクはこれだけど、スカカ(････)ス
<http://www.microsoft.com/security/encyclopedia/details.aspx?name=Backdoor%3aWin32%2fAgent.AE>

亜種というか、バージョンアップ版のMe11-1-0.12、Me11-1-0.12Aは検体を持っていないため未確認(････)ス

「山田オルタナティブウイルス････」と書いてあるメールを受け取った方

現在テンプレから外れています。
心配な場合は、[駆除方法](#)で確認してください。

とりあえず、何がどういうものなのか知りたい人は？

[山田オルタナティブって何？](#)へGO(････)ス。
なお、このウイルスの流通は、現在ファイル交換ですがWinnyなどP2Pをしていなくても、**ファイルを実行するだけで感染、晒されます。**
また、今までの山田ウイルスのように独立せず、リンクリストを作成してお互いを見つけます。
(厨房板 (<http://tmp6.2ch.net/kitchen/>)へ書き込みを利用して、Linkリスト作成のノードになっている?)

とりあえず、感染してるらしい人は？

最近、「山田ぢゃないのに、山田山田と言われる」、「山田うんたらとかいうメールをもらってここに来た」人は、[駆除方法](#)へ。

緊急

とくダネetcでWinnyネタが紹介されていた模様で(・・・)が「山田とキンタマをませこぜに説明していた」模様。。イナバウアーといい、嘘の説明は辞めましょう(・・・)ス。。

過去の**緊急事態**履歴は、[緊急履歴](#)を見る(・・・)ス。

業務連絡

検証カキコがホントかネタか交錯してるみたいなので、過去ログ整理を落ち着くまでしてま(・・・)ス。

過去の**業務連絡**履歴は、[業務連絡履歴](#)を見る(・・・)ス。

ヲチ初心者の方は？

ヲチスレは、気づかせる機会を見つけるまで(・・・)加伊ノの精神で生暖かく見守ってあげるようにする(・・・)ス。
(ヲチの時にファイルへアクセス(ダウンロードを)するとログが残ることが判明しました。自己責任でDL(・・・)ス)

現状テンプレ

(仮) 山田オルタナティブ (Mell-1-0.12a, Mel-1-0.12, Mell-1-0.11)

【主な被害】

- 2段階の画質でSSを出力し、他の(・・・)加伊ノな香具師へ相互リンク
- アップロードらしきフォームで、コンピュータ上の全HDD上の全ファイルのHTTPでのダウンロードを可能にする

【主な活動】

- Program filesフォルダにsysフォルダとupdateフォルダを作成する
- 最初の時点ではsys.exe、再起動後にupdate.exeとして動く
- update.exeのほうはHDDには現存せず
- 起動ごとにsys.exe update.exe sys.exeとファイル名を変え活動
- 起動時には引数として前述のTripが渡されている
- 実体あるのはC:\Program Files\で、sys.exeの時はsysフォルダ

update.exeのときはupdateフォルダに居座る

- フォルダ内には実体とreadme(拡張子無し、文字化けして読めない)、2つのフォルダを作成
- フォルダの一方は空、もう一方は

他の(・・・) 加伊々な香具師らを繋ぐリンク用のキャッシュファイル

- UPnP対応で穴を空ける
- 起動はレジストリのスタートアップに下記の2つが登録
- HKEY_LOCAL_MACHINE -> SOFTWARE -> MICROSOFT -> WINDOWS -> CURENTVERSION -> RUN

名前: sys.exe データ: "c:/program files/sys/sys.exe"20060223042347170169115

名前: update.exe データ: "c:/program files/update/update.exe"

- ポート80、ポート8080の空き領域を使う

(そのほかのポートを使う場合もある模様)

- Mell-1-0.12a, Mell-1-0.11の同時起動が可能。その場合は

それぞれ80ポートと8080ポートで起動し、0.12Linkリストと0.11 Linkリストは違うものをリスト化する模様(仕組みは不明)

- updateフォルダに2chの板一覧を取得(bbs2ch_bbsmenu_html)、

厨房板(<http://tmp6.2ch.net/kitchen/>)へ書き込み、ログ保持

- 厨房板への書き込みがLinkリスト作成のノードになっている?

山田オルタナティブ

- Mell-1-0.11, Mell-1-0.12, Mell-1-0.12A, Mell-1-0.12Bの四種類。
- 最古の存在確認は1月23日、現在、爆発的に感染が広がっている。
- ny、洒落の両方での感染が確認されている。うpログでも感染する可能性あり。
- 感染するとny、洒落を起動していなくとも関係なく自立Webサーバを起動、

感染者同士のPCをLINKさせ、HDDを全公開し、外部からアクセスも可能にしてしまう。

- sys.exeとupdate.exeを削除しても復活したとの報告もあり、別に卵が存在している?
- 感染者によってエロゲ、アニメ、音楽など収集ジャンルがまちまちなため、感染源がいまだに不明。
- 拡張子exe, scr, com, bat, pif, cmdは要注意

【感染確認方法(とりあえず安心程度)】

- タスクマネージャでSys.exe及びUpdate.exeの有無を確認。存在すれば(・・・) 加伊々
- Program filesフォルダにsysフォルダとupdateフォルダが存在すれば(・・・) 加伊々
- コマンドプロンプトからnetstat -anoと打ち込み

Local Addressに80, 8000, 8080の有無を確認。存在すれば(・・・) 加伊々

山田ヲチスレテンプレ

このスレの唯一のローカルルールは空気を読むこと（・・・）ス

感染者の方へ

- ・相談に乗るスレ住人もいる事もあるので、恐れずに最新レスを確認して書き込み（・・・）ス
- ・煽られても泣かない（・・・）ス

スレ住人（ヲチャ）の方へ

- ・各自「被害者さんへの（・・・）加傷」の念を忘れずに良心に従って行動してください（・・・）ス
- メールアドレスや個人サイトのURLや個人情報を晒すのは（・・・）加傷
- 感染しているマシンのURLを晒して被害を拡大するのは（・・・）加傷
- >>950 超えたあたりで次スレを建てて誘導しないと難民や重複が発生して（・・・）加傷

質問のある方へ

- ・ここは質問スレではないので適切なスレで質問されることを強くお勧めします（・・・）ス

前スレ NHKお前もか ドイツの少年（・・・）加傷 山田ヲチスレ 215

<http://tmp6.2ch.net/test/read.cgi/download/1142607448/>

kawaisosu@Wiki

<http://www2.atwiki.jp/kawaisosu/> まとめサイト

<http://www3.atwiki.jp/yamada/> まとめサイトミラー

山田オルタナティブ（・・・）加傷@まとめWiki - トップページ

http://www9.atwiki.jp/y_altana/

ニュイルス日誌 by 通報屋 Y39/vakKjY氏

http://blog.livedoor.jp/antiny_virus/ 山田ウイルスチェックツールあり

http://otd9.jbbs.livedoor.jp/1000004440/bbs_tree 山田ウイルスチェックツールサポートBBS

ハマーの出張所 by ハマー wEzG8/hlSg氏

http://www.geocities.jp/dkstr_hamar/index.html 感染レポートほか多数

http://www.geocities.jp/dkstr_hamar/kawaisosu/dokuro.html ドク口まとめ

http://www.geocities.jp/dkstr_hamar/alter/alter.html 山田オルタまとめ

（・・・）加傷について by 河磯洲 uuyy3yUfyc氏

<http://www.geocities.jp/kawaisosu/> 過去ログdat155まであり