# 商業サイト改ざん事件から何を学ぶか

## ～サーバ対策とウイルス対策に注目して～

キヤノンシステムソリューションズ株式会社

セキュリティソリューション事業部

髙 本　勉

July 27, 2005

# 価格.com改ざん、ウイルス感染のおそれも

ITmedia News ニュース

速報
2005/05/16 09:59 更新

## 価格.comが不正アクセスで閉鎖　ユーザーにウイルス感染のおそれも

**価格.comが不正アクセスを受け、14日から閉鎖している。サイトを媒介にウイルスがばらまかれており、ユーザーは感染した可能性がある。**

価格比較サイト「価格.com」が5月11日ごろから不正アクセスを受けて一部が改ざんされた上、同サイトを媒介にウイルスがばらまかれたため、カカクコムは14日から同サイトを一時閉鎖し、セキュリティ対策を施している。復旧には1週間程度かかる見通し。同社が保有するメールアドレスが閲覧された形跡もあるという。

大手サイトがセキュリティ問題で一時閉鎖するのは極めて異例だ。

ばらまかれたウイルスは「trojandownloader.small.AAO」「PSW.Delf.FZ」で、11日から14日に価格.comにアクセスしたユーザーは感染したおそれがある。現時点で、キヤノンシステムソリューションズが販売するウイルス対策ソフト「NOD32アンチウイルス」（Windows版のみ）で対処可能という。その他のウイルス対策ソフトの対応状況については確認中としている。

Scan Daily EXpress

本記事は国内最大級のセキュリティ情報専門メールマガジンSCANシリーズの「Scan Daily Express」より転載しています。詳細はこちらから

## 05月16日　価格.com、改竄被害で一時閉鎖へ、閲覧者はウイルス感染の可能性も

価格.comを運営する株式会社カカクコムは5月15日、不正アクセスが集中し、数回にわたる改竄被害を受けたため同サイトを一時閉鎖すると発表した。復旧までは1週間程度かかるとしている。同社によると、5月11日からプログラムの異常が発生、不正アクセスが急増したことが原因であると判明した。警察当局などと相談した上で、24時間体制で監視を続け調査を進めたが、犯人はつかめなかった。5月14日午後2時頃にサイトを閉鎖し、プログラムを修正した上で同日午後10時に再開したものの、攻撃が止まないため全面閉鎖に踏み切った。

>> 利用者の資産をおびやかす重大な危険性も

改竄によって、攻撃者が価格.comを媒介して無差別にウイルスを送りつけた可能性があるとして、同社ではキヤノンシステムソリューションズが販売するウイルス対策ソフト「NOD32」を無償提供している。現在、判明しているウイルスは「trojandownloader.small.AAO」「PSW.Delf.FZ」の2種類。これらのウイルスはトロイの木馬と呼ばれるタイプと推定されている。このタイプのウイルスは、感染すると利用者のPCに潜み、重要な情報を盗み出して外部に送信するなどの活動を行う。

つまり同サイトの利用者は、自分のPCおよびPCを利用してアクセスする他のサービスに関するIDやパスワードなどの重要な情報も危険にさらされている可能性がある。トロイの木馬の中には「キーロガー」というキー操作を記録して盗むものもある。他のサイトにアクセスしてIDとパスワードを入力するとその入力の記録がそのまま盗まれてしまう可能性もあるのである。

同サイトでは個人向けの外為関連のサービス（いわゆるFX）も提供しており、取引に用いられるIDやパスワードの情報が盗まれた場合、利用者の資産に重大な被害をおよぼす可能性も否定できない。このような状況にも関わらず、同サイトではサイト閉鎖中にも関わらず、外為サービスは利用できるとのアナウンスを流している。別なシステムであるため、サーバ側には問題がないとのことであるが、同サイトでトロイの木馬に感染した利用者の個人情報が盗まれる危険性は他のサイトを利用しても同じである。利用者の危険性を考慮しない姿勢は問題である。

ウイルス「TrojanDownloader.Small.AAO」と「PSW.Delf.FZ」が、価格.comからばらまかれた。

「**NOD32アンチウイルス**」だけが対処可能と公表

Canon
キヤノンシステムソリューションズ株式会社

# 価格.com サイト閉鎖時のトップページ

【重要なお知らせ】
当社運営サイトに対する不正アクセスとサイト一時閉鎖に関してのご報告

2005/5/15

株式会社カカクコム（本社：東京都文京区、代表取締役：穐田誉輝）では当社運営サイトに対する不正アクセスによりプログラムが改ざんされ、セキュリティ対策を施すためサイトを一時閉鎖したことをご報告申し上げます。

日頃当社サイトをご支持頂いている方々には、大変なご迷惑をおかけすることとなりましたことを心よりお詫び申し上げます。

この改ざんにより、何者かが当社サイトを媒介としてウィルスソフトを無差別に送りつけ、当社サイトを閲覧されたお客様がウィルスファイルを取込んでしまった可能性があります。
判明しているウィルスは「trojandownloader.small.AAO」「PSW.Delf.FZ」の2種類であり、アンチウィルスソフト「NOD32」にて対処可能な事を確認しております。

**NOD32アンチウイルス体験版ダウンロード（Windowsユーザーのみ）**
http://canon-sol.jp/product/nd/trial.html

その他セキュリティソフト各社にも対応を確認中であり、判明次第ご報告させて頂きます。

また、この不正アクセスを通じ当社の保有するメールアドレスが閲覧された形跡がありました。
詳細は調査中であり、事実が判明次第ご報告させて頂きます。
尚、メールアドレス以外の個人情報等に関しましては閲覧された形跡はございません。

＜これまでの経緯＞
5月11日にプログラムの異常が発覚。調査したところ不正アクセスが原因であり、一種のサイバーテロ的な行為であると認識しました。
即時警察当局等とも相談し、24時間監視体制でサイト運営を続けながらプログラム改ざんの影響や対抗策、犯人の調査を続けて参りましたが不正アクセスは止まず、改ざんの範囲が拡大したため止む無く5月14日よりサイトを閉鎖しております。

閉鎖直後の価格.comのトップページ **NOD32** だけが対処可能との表示

# 価格.comでの出来事の概要

5/10　NOD32アンチウイルスユーザが、数社のホームページを閲覧時にウイルスの可能性があると警告される旨を当社に報告。
当社は、事態を確認後、開発元であるEset社にサンプル送付。

5/11　ウイルスのひとつは、既知のウイルス「TrojanDownloader.Small.AAO」、もうひとつは、未知のウイルスで、「Win32/PWS.Delf.FZ」と定義。

5/11　価格.comは、調査を開始。

5/14　価格.com原因究明できず、サイト閉鎖を決定。

5/15　価格.comは、トップページにお詫びを掲載し、「NOD32」だけがこのウイルスに対応できる旨を公表。

5/16　当社は、ウイルス情報をWebに掲載。

価格.comは、この事態をプレス発表。

5/18　当社は、「 NOD32 」が、価格.comのサイトのウイルスを未知のウイルスの状態でも検出し、NOD32のユーザは、そのウイルスが発生時点ですでに保護されていたことをプレスリリース実施。

# 一連の改ざん事件をどう分析するか (1)

- 今回の価格.comに代表されるおけるWebサイト改ざんの原因は?
  - 脆弱性のあるWebサーバに対して、悪意をもったクラッカーが意図的に不正なコードをWebサーバに仕組んだこと
  - 新聞記事等に依れば、SQLインジェクションを使って、当該Webサーバを改ざんしたとのこと(残念ながら、詳細は報告されていない。)
- この改ざんは、防止することはできたのだろうか?
  - SQLインジェクションを使ったとすると、「アプリケーション・ファイアウォール」を導入していれば、この改ざんは防げた可能性がある。
  - アプリケーション・ファイアウォールとは、通常のファイアウォールとは違って、通信パケットそのものではなく、HTTPリクエストなどのアプリケーションのレベルでそのフィルタリングを行うもの。
  - もし改ざんされたサーバがIISならば、「SecureIIS Web」、Linux Apacheならば、「NGSecureWeb」が利用できる。

# Webサーバを攻撃する代表的手法

- プログラムのバグを悪用する攻撃
  - 「バッファオーバーフロー」攻撃
- CGI・Webアプリケーションの実装ミスを悪用する攻撃
  - 「ディレクトリ・トラバーサル」攻撃
  - OSコマンドの挿入（「OSコマンド・インジェクション」）
  - SQLコマンドの挿入（「SQLコマンド・インジェクション」）
- その他の攻撃
  - クロスサイト・スクリプティング
  - 設定ミスを突く攻撃（HTTPメソッドの悪用、など）

# 一連の改ざん事件をどう分析するか (2)

- 今回の改ざんで問題となる最も重要な点
  - Webサイトを訪れたユーザにウイルスをダウンロードさせてしまうこと
  - 今回このWebサーバにアクセスした際にダウンロードされるウイルスは、「TrojanDownloader.Small.AAO」と、「PSW.Delf.FZ」の2種類
  - 「TrojanDownloader.Small.AAO」は、既知のウイルスでNOD32では、2004/11/30に定義データが登録済み
  - 一方、「PSW.Delf.FZ」は、このウイルスが発生した(仕掛けられた) 時点では、どのアンチウイルスソフト会社も知らない、未知のウイルスだった。
- NOD32は何故未知のウイルスも検出するのか
  - NOD32のユーザが、価格.comのホームページを閲覧時に、「ウイルスの可能性あり」との警告表示を受けたのは、NOD32のアドバンスド・ヒューリスティック機能により検知したもの
  - 未知のウイルスを検知する機能が働いたためで、この他社にはない優れた機能によりユーザのPCが安全に守られた。この時点では、国内他社の製品では、検知していない。

# 何故他社製品は検知できなかったのか

- 今回このWebサーバにアクセスした際にダウンロードされるウイルスは、NOD32では、2004/11/30に定義データが登録されている既知のウイルス「TrojanDownloader.Small.AAO」と、未知だった「PSW.Delf.FZ」の2種類。

- 重要なのは、この既知のウイルスでさえも他社製品で検知できなかった実態があるということ。

- 今回その理由として考えられるのは、これらのウイルスは、マイクロソフトHTML Help形式のコンポーネントとして.chmファイルにインポートされていたためと思われる。国内で流通している他社製品は、そのファイルの内部スキャンまでは十分になされていないのではと思われる。

# どのような挙動のプログラムか

- ウイルス自体の挙動に関する記述は、当社Webページをご覧ください。
  - 最新ウイルス情報 : Win32/PSW.Delf.FZ 公開日 :2005年05月16日
    http://canon-sol.jp/product/nd/virusinfo/vr_a50516.html

最新ウイルス情報 : Win32/PSW.Delf.FZ　公開日 : 2005年05月16日

このウイルスに関する危険度 : ■■■■□

| | |
|---|---|
| ウイルス名 | Win32/PSW.Delf.FZ |
| 対応定義ファイル | 1.1093 (20050511) 以降 |
| ウイルスの対処方法 | 検出ファイルを削除してください |
| ウイルスに関する危険度 | 4 - 感染が拡大している |

※ 1:注意　2 :感染可能性あり　3:感染報告あり　4:感染が拡大している　5:深刻な被害が拡大中



  - Win32/PSW.Delf.FZ は、オンラインゲームのLineage (リネージュ) のパスワードを盗聴する典型的なトロイの木馬。サイズは58,880バイトで、UPXで圧縮されている。

# NOD32はいつ頃から捉えていたか

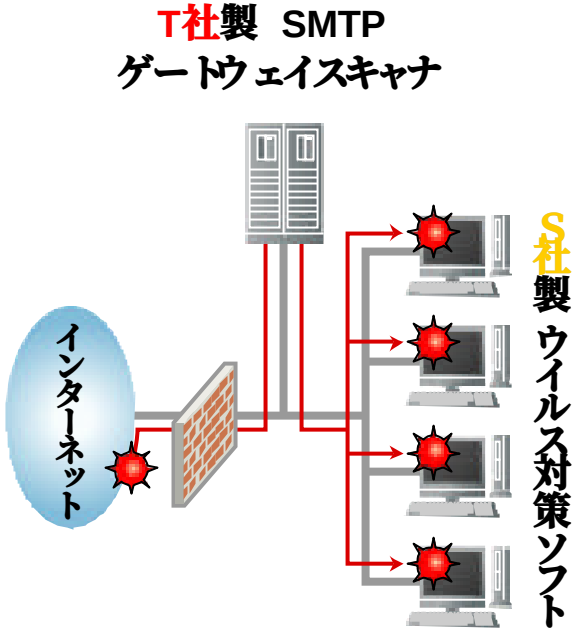
- NOD32には、ヒューリスティック機能が当初より組込まれ、当社がVer. 2として日本語版の販売を開始した2003/6の段階では、さらに高度な検出技術であるアドバンスド・ヒューリスティック機能も既に組込まれ、最新の未知ウイルス検出エンジンとして専門家の間で、広く認知されている。

- アドバンスド・ヒューリスティック機能は、日々改良が重ねられており、ユーザは日々の定義ファイルアップデートや更新期間内なら無償で行われるコンポーネント・アップグレード(他社で言うバージョンアップ)によって、改良の度に最新の検知エンジンが使えるようになっている。

- そういう意味で、今回の問題のウイルスに対しては、NOD32は発生時点から既にそれを捉えており、ユーザのPCを保護してきたと言うこと。

# 【他の事例】A社での出来事

- **A社**はセキュリティには非常に気を遣っており、社内のウイルス対策はほぼ万全な体制だと思っていた。
  導入済みのシステムは以下の通り
  - ゲートウェイに、**T社**製のSMTPスキャナを設置
  - 各クライアントには、**S社**製のウイルス対策ソフトを導入済み

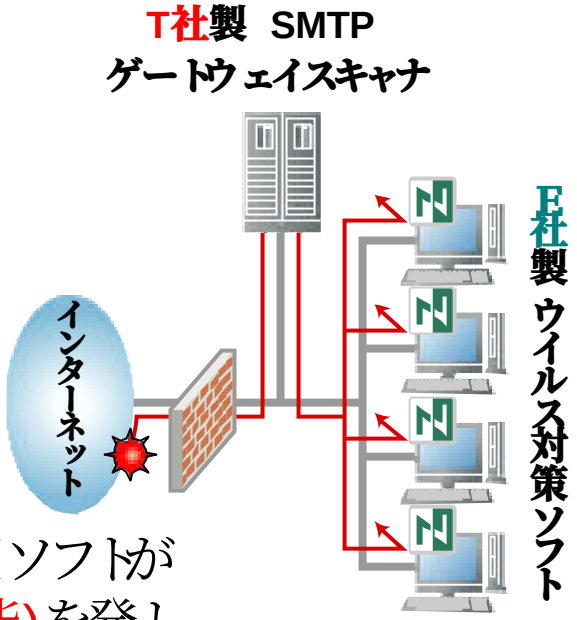



- 昨年、7/13(火)朝の出来事
  - 9:10amに受信したメールの添付ファイルから感染
  - その後次々と感染が増え、10台のパソコンが感染
- ウイルス対策担当者は、大慌てで調査をするが、各ウイルス対策ソフトはすべて最新のウイルス定義に更新済みだった。

**ウイルス対策を施しているのに、**
**感染するのは何故 ??**

# 【他の事例】B社での出来事

- **B社**も比較的セキュリティには気を遣っており、社内のウイルス対策は実施済み。
  導入済みのシステムは以下の通り
  - ゲートウェイに、**T社**製のSMTPスキャナを設置
  - 各クライアントには、**E社**製のウイルス対策ソフトを導入済み
- 同じく、7/13(火)朝の出来事
  - 9:05amに受信したメールに対し、**E社**製ウイルス対策ソフトがウイルスの可能性ありとの警告(ヒューリスティック機能)を発し、無事削除
- ウイルス対策担当者は、慌てず社内にウイルス侵入の警告をしたのち、侵入経路の調査に着手
  - その後同じようなメールも全員が削除して、感染なし!




**ウイルスはゲートウェイをすり抜けたものの**
**最終的にクライアントで防御!!**

# A社とB社の違いは何か?

- A社、B社共にゲートウェイ対策は同じ**T社**のもの
  - ウイルスは、ゲートウェイをすり抜けていた！
- 違いは、クライアントパソコンのウイルス対策ソフト
  - 感染したA社は、**S社**製のウイルス対策ソフトを使っていた。
  - 感染を防御したB社は、**Eset社**製のウイルス対策ソフトを使っていた。
- ここで、事実の整理をしましょう。
  - **T社**、**S社**共に発生したばかりの未知のウイルスに対しては残念ながら何の対策もできなかった。
  - 感染の実体となりうるクライアントPCで、**Eset社**のソフトが未知のウイルスに対して警告を発したことで、感染を防止できた。

**ウイルス対策を施しているのに**
**感染する理由はここにあった！**

# この事件のウイルスへの対応実態

ウイルス名： Win32/Lovgate.AK (この他、Win32/Lovgate.AJもあった)

比較的古い(一昨年5月発生)ウイルスの亜種(ASPack v.2.12版)

時間的経緯：当社調べ (時間はすべて日本時間で掲載)

| | | |
|---|---|---|
| 7/13 | 9:05 | T社のウイルスゲートウェイを未知ウイルスが通過 |
| | 9:10 | Eset社のクライアント用ウイルスソフトが、未知ウイルスとして発見 |
| 7/13 | 13:00 | T社クライアントソフトでは、未検出 |
| 7/13 | 17:27 | T社、ウイルス定義更新(PE_LOVGATE.AH-Oとして検出) |
| 7/13 | 20:10 | S社クライアントソフトでは、最新定義導入するも依然未検出 |
| 7/13 | 22:00 | Eset社、Win32/Lovgate.AKのASPack v2.12版として定義 |
| 7/14 | 早朝 | S社、ウイルス定義更新(W32/Lovgate.AD@mmとして検出) |

参考：M社の対応実態

7/13 早朝には既にW32/Lovgate.ah@MMとして情報掲載しているものの未検出
(ウイルス定義は未更新)

7/14 19:00の段階で未検出、発生から2日後の7/15 10:00 検出

# ウイルス感染防止の必要条件

企業ユーザにおけるウイルス感染防止策の必要条件

【既知ウイルス】

- ウイルス定義ファイルの早期更新・ダウンロード
- ウイルス定義ファイルの各クライアントでの確実な更新

⇒ 既知ウイルスへの対応の早い会社の製品を選ぶ。

ここまでは、今まで言われてきたこと。
大切なのは、ここから！

【未知ウイルス】

- 未知ウイルスを検出するヒューリスティック機能が必須

⇒ 未知ウイルスも高い確率で検出する製品を選ぶ。

# ヒューリスティック機能とは

- ヒューリスティック(Heuristics :発見的手法)とは

  「トライ・アンド・エラー」または、「探索的な」手法による問題解決であり、「形式的な技法の代わりに直感を使用すること」を意味する。

- ウイルス対策におけるヒューリスティック手法

  ヒューリスティックなアルゴリズムは汎用的で、解析したコードを「理解」し、不審な挙動を検出して、入手できたすべての情報を総合して最終的な判断をくだす。適切(妥当)であると判断されたときはウイルス警告を発する。

- ヒューリスティック実装の利点

  (1) 未知ウイルスの侵入検知ができる。

  (2) 開発されたツール(エミュレータ)によって、問題の正確な特定が可能になったり、その効率が高まったりする。

# メジャー各社のヒューリスティック機能と結果

【T社】2004/03/17の記述

新エンジンで、ワームトラップ（WormTrap）に新規対応。ワームに特化したヒューリスティック検索機能で、亜種、変種のワームを検知可能になった。

⇒ 簡単なヒューリスティック機能のみ
実際、**未検出**

【M社】2003/06/03の記述

ヒューリスティックスキャナは、プログラム コードを分析してこの種のコンピュータ命令を検出。プログラムファイルから予期されない数値を検索することにより暗号化されたウイルスも検出。

⇒ 簡単なヒューリスティック機能のみ
実際、**未検出**

【S社】2001/02/02および2003/04/09の記述

スタティック・ヒューリスティック法：

ウイルスのプログラム ・コードを予め定義情報DBに登録し、いくつかの行動パターンが一致した場合、ウイルスと判断。

ダイナミック・ヒューリスティック法：

ウイルス感染プログラム をメモリ上で仮想的に実行 （エミュレーション）し、行動パターンがウイルスの動作と確認された場合に、ウイルスと判断。

http://www.xxxxxxxx.com/region/jp/sarcj/reference/heuristc.pdf

(1998年 特許出願、2002年米国特許登録)

⇒ 調査した中で最も詳しい説明ではあるが、実際の検出事例の記述は、全く無い。
実際、**未検出**

ヒューリスティック機能を搭載していると言うが、実際には検出していないことが多い。

# 日本でのヒューリスティック研究の現状

1.徳島大学 三宅崇之他、「仮想サーバを使った未知ウイルス検知システムの提案」
情報処理学会研究報告「コンピュータセキュリティ」No.018-008, 2002
- ホストエミュレータ(VMware)を用いた仮想マシン上でメールの添付ファイルを検査
- SMTP通信に注目した検出手法では、3種中1種を検出。
- ハッシュ値比較手法では、残り2種を検知したが、この手法は膨大な時間を要する。

2.徳島大学 神薗雅紀他、「仮想ネットワークを使った未知ウイルス検知システム」
情報処理学会研究報告「コンピュータセキュリティ」No.022-016, 2003
- 上記同様、SMTP通信を監視し、2種中1種を検出。
- ハッシュ値比較手法で残り1種を検知したが、その所要時間は3分10秒であった。

3. 金沢工業大学 菅原啓介他、「未知ウイルス検出技術に関する一考察」SCIS 2004
- ダイナミックヒューリスティック手法をビヘイビア法と呼び、この方式を有効とした。

4.北陸日本電気ソフトウェア 西川弘幸他、
「セキュリティホールを狙うワーム検出の実験」SCIS 2004, 2004
- ポート監視と特定ディレクトリ監視により、11種中5種を検出。

残念ながら、国内の研究もまだ実用化できる段階ではない。

# NOD32の未知ウイルス検出率は?

- WildCore(WildList* 2004年8月) 381種のInTheWildウイルスのうち、336種をウイルス定義ファイルなしに、ヒューリスティック機能で検出し、検出率を算定。

*: The WildList Organization International http://www.wildlist.org/WildList/

WildCoreウイルスにおけるNOD32の検出率の予測値

| | |
|---|---|
| スタンダード・ヒューリスティック： | 24.1% (92/381) |
| アドバンスド・ヒューリスティック： | 64.0% (244/381) |
| 合計 | **88.1%** (336/381) |

- ヒューリスティック機能は、日々改良される。
  - Virus Bulletin Conference 2002 (VB2002)で、Eset社Chief DeveloperのRichard Markoが、アドバンスド・ヒューリスティックに関する論文(ヒューリスティック: その過去と未来)を発表し、その後も研究と改良を加えている。

Richard Marko

# 主な感染での各社未知ウイルス検出実態

## 各社非常に低い検出率中で、NOD32だけが予測通り88%の好成績!

| ウイルス名 | 発生日 | AntiVir | Bit Defender | ClamAV | Dr. Web | eTrust | F-Prot | Kaspersky | McAfee | Eset NOD32 | Norman | Symantec | Panda | Sophos | Trend Micro |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bagle.AH | 2004/07/19 | - | ○ | | - | | | | | ○ | ○ | | | | |
| Mydoom.R | 2004/07/26 | - | | | - | | | | | ○ | ○ | | | | |
| Evaman.C | 2004/08/03 | - | | | - | | | | ○ | ○ | ○ | | | | |
| Bagle.AI | 2004/08/09 | - | ○ | | - | | | - | ○ | ○ | ○ | - | ○ | | |
| Bagle.AJ | 2004/09/02 | - | | | - | | | | ○ | | ○ | ○ | ○ | | |
| Bagle.AQ | 2004/09/28 | - | | | - | | | | | ○ | | | | | |
| Netsky.B1 | 2004/10/13 | - | ○ | | - | | | ○ | | ○ | ○ | | | | |
| Bagle.AS | 2004/10/29 | - | ○ | | - | | ○ | | | ○ | | | | | |
| Bagle.AU | 2004/10/29 | - | ○ | | - | | | | | ○ | | | | | |
| Sober.I | 2004/11/19 | - | | | - | | | | | | | | | | |
| Pawur.A | 2004/11/23 | - | | | | | | | | ○ | | | | | |
| Zafi.D | 2004/12/14 | | ○ | | | | ○ | | ○ | ○ | | - | ○ | | |
| Bagle.AW | 2005/01/26 | | ○ | ○ | | | ○ | | | ○ | ○ | | ○ | ○ | |
| Bagle.AX | 2005/01/27 | | ○ | ○ | | | ○ | | | ○ | ○ | | ○ | ○ | |
| Mydoom.R.MEW | 2005/02/16 | | ○ | | | | | ○ | | ○ | ○ | | ○ | | |
| Sober.O | 2005/05/02 | ○ | | | ○ | | | | ○ | ○ | ○ | - | ○ | | |
| Total | 検出数 | 1 | 9 | 2 | 1 | 0 | 4 | 2 | 5 | 14 | 10 | 1 | 7 | 2 | 0 |
| | 検出率 | 20% | 56% | 13% | 17% | 0% | 25% | 13% | 31% | 88% | 63% | 8% | 44% | 13% | 0% |

HispaSec Systems 調べ
http://www.hispasec.com/directorio/laboratorio/ultimasunaaldia

# 実用化されたヒューリスティック技術

ヒューリスティックにおける2種類のアプローチ

【パッシブ・アプローチ】 (スタティック法)

- パッシブ・アプローチは、アンチウイルスの専門家がとる方法に似ている。
- 解析対象ファイル等のコードを詳しく検討し、それが外部環境と相互作用する方法を人間が評価する場合と同様の方法で評価。

  例：バイナリ・ウイルスであれば、命令フロー、レジスタおよびスタックの値、API関数や割り込みの呼び出しなどを逆アセンブラを使用して追跡。

【アクティブ・アプローチ】(ダイナミック法)

- アクティブ・アプローチでは、システム全体をシミュレートする仮想環境（「sandbox」とも呼ぶ）で解析対象ファイルを「実行」。この環境は、ローカル・ハードディスクやネットワークなどを備え、Windowsのような現実のシステムと同じように動作する。
- この仮想コンピュータのさまざまな重要部分（実行可能ファイル、コンフィグレーション・ファイル、メモリの内容など）が変更されるたびにそれを評価。このアプローチでもっとも重要なのが強力なエミュレータである。

# ヒューリスティック検出の実際

## 2004/09/28 Bagle.AQワーム



(出典：VirusRadar.com)

- HispaSecの記述：

「強調すべきは、NOD32だけがヒューリスティックで検出し、流行開始時点で既にユーザを保護していた。」

### 各社の定義ファイル更新状況

| | |
|---|---|
| **Kaspersky** | **28.09.2004 20:25:: I-Worm.Bagle.as** |
| **ClamWin** | **28.09.2004 20:51:: Worm.Bagle.AP** |
| **BitDefender** | **28.09.2004 21:42:: Win32.Bagle.AU@mm** |
| **McAfee** | **28.09.2004 21:48:: W32/Bagle.az@MM** |
| **NOD32v2** | **28.09.2004 22:19:: Win32/Bagle.AQ** |
| **F-Prot** | **28.09.2004 22:24:: W32/Bagle.AM.worm** |
| **Panda** | **28.09.2004 22:40:: W32/Bagle.BB.worm** |
| **TrendMicro** | **28.09.2004 23:10:: WORM_BAGLE.AM** |
| **Norton** | **29.09.2004 00:05:: W32.Beagle.AR@mm** |
| **InoculateIR** | **29.09.2004 00:17:: Win32/Bagle.18883.Worm** |
| **Sophos** | **29.09.2004 03:10:: W32/Bagle-AZ** |
| **Norman** | **29.09.2004 10:25::Bagle.AO@mm** |

出典：**HispaSec**

# 実用的なヒューリスティック機能

- ヒューリスティック機能について、実用的ではないと言う人々が一部にいるが、それは誤り。実際に実用化されて効果をあげている。
  - 長年の解析と研究による正しいインプリメントを行うことで、未知のウイルスを日々発見する実用的な製品が開発できることが証明された。

- ヒューリスティックは、スキャン・エンジン自体の精度の証
  - この点からすると、明らかにヒューリスティックは、スキャン・エンジン自体の技術レベルを測るものとして捉えることもできる。
  - ウイルス(ワーム)が日々現れてくる現状において、未知ウイルスに対応できなければ、ウイルス対策として不十分と言わざるを得ない。
  - 多くのウイルス対策ソフト会社が未知のウイルスに対して、ヒューリスティック手法を適用していると言っているが、十分に検出していないことも事実。
  - ヒューリスティック機能が十分にインプリメントされた製品は決して多くない。

# 最近の未知ウイルス検出実績

NOD32は、日々こんなに多くの未知ウイルスを発見し、ユーザのPCを保護している。

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2003/05/28 | **Win32/Holar.H** | 2004/03/02 | **Win32/Bagel.I** | 2004/10/29 | **Win32/Bagle.AS, AU** | 2005/03/25 | Win32/Mytob.K |
| 2003/05/29 | Win32/Auric.A* | 2004/03/03 | **Win32/Bagle.J** | 2004/11/23 | **Win32/Pawur.A** | 2005/04/04 | Win32/Mytob.T |
| 2003/06/02 | Win32/Naco.D | 2004/03/03 | **Win32/Mydoom.G** | 2004/12/05 | Win32/Maslan.A | 2005/04/09 | Win32/Mytob.Y |
| 2003/06/05 | **Win32/BugBear.B** | 2004/03/03 | Win32/Netsky.F | 2004/12/07 | Win32/Maslan.B | 2005/04/18 | Win32/Sober.N |
| 2003/06/08 | **Win32/Mapson.A*** | 2004/03/03 | Win32/Bagle.K | 2004/12/07 | Win32/Rbot.QBS | 2005/04/30 | Win32/Mytob.BS |
| 2003/06/14 | Win32/Crock.A | 2004/03/03 | **Win32/Mydoom.H** | 2004/12/14 | **Win32/Zafi.D** | 2005/05/02 | **Win32/Sober.O** |
| 2003/06/18 | **Win32/Sobig.D** | 2004/03/04 | Win32/Hiton.A | 2004/12/14 | Win32/Mydoom.AJ | 2005/05/04 | Win32/Mytob.BV |
| 2003/07/03 | Win32/Mylife.O,M | 2004/03/08 | **Win32/Sober.D** | 2004/12/28 | Win32/Rbot.CJL | 2005/05/09 | Win32/Mytob.CB |
| 2003/07/08 | Win32/Israz.A | 2004/03/14 | Win32/Netsky.M | 2005/01/18 | Win32/Rbot.CMZ | 2005/05/15 | Win32/Mytob.CI |
| 2003/07/16 | Win32/Gruel.A* | 2004/03/28 | Win32/Sober.E | 2005/01/25 | Win32/Swash.C | 2005/05/23 | Win32/Mytob.CU |
| 2003/09/05 | **Win32/Lablan.A** | 2004/04/04 | Win32/Sober.F | 2005/01/26 | **Win32/Bagle.AW** | 2005/06/25 | **Win32/Bagle.BI** |
| 2003/09/18 | **Win32/Swen.A** | 2004/04/19 | **Win32/Zafi.A** | 2005/01/27 | **Win32/Bagle.AX** | 2005/06/28 | Win32/Mytob.GK |
| 2003/10/12 | Win32/Logpole.A | 2004/05/11 | **Win32/Bagle.AB1** | 2005/02/16 | **Win32/Mydoom.R.MEW** | 2005/06/30 | Win32/Mytob.GO |
| 2003/10/22 | Win32/Winsux.A | 2004/05/15 | Win32/Sober.G | 2005/02/27 | Win32/Bagle.AZ | | |
| 2003/10/24 | **Win32/Sober.A** | 2004/06/10 | **Win32/Zafi.B** | 2005/02/27 | **Win32/Mytob.A** | | |
| 2003/11/18 | Win32/Mimail.J | 2004/06/11 | Win32/Sober.H | 2005/02/27 | **Win32/Mytob.B** | | |
| 2003/12/11 | Win32/Scold.A | 2004/07/13 | **Win32/Lovgate.AK, AJ** | 2005/02/28 | Win32/Mytob.C | | |
| 2003/12/18 | **Win32/Sober.B** | 2004/07/16 | Win32/Bagle.AF | 2005/03/01 | Win32/Mytob.D | | |
| 2003/12/20 | **Win32/Sober.C** | 2004/07/19 | **Win32/Bagle.AH** | 2005/03/07 | Win32/Sober.I | | |
| 2004/01/18 | **Win32/Bagle.A** | 2004/07/26 | **Win32/Mydoom.R** | 2005/03/07 | Win32/Sober.L | | |
| 2004/01/24 | Win32/Dumaru.Y | 2004/08/03 | **Win32/Evaman.C** | 2005/03/11 | Win32/Mytob.E | | |
| 2004/02/16 | **Win32/Netsky.A** | 2004/08/09 | **Win32/Bagle.AI** | 2005/03/14 | Win32/Mytob.F | | |
| 2004/02/17 | **Win32/Bagle.B** | 2004/08/16 | Win32/Mydoom.T | 2005/03/14 | Win32/Mytob.G | | |
| 2004/02/18 | **Win32/Netsky.B** | 2004/09/02 | **Win32/Bagel.AJ** | 2005/03/18 | Win32/Mytob.H | | |
| 2004/02/20 | **Win32/Mydoom.F** | 2004/09/28 | **Win32/Bagle.AQ** | 2005/03/13 | Win32/Mytob.I | | |
| 2004/02/25 | **Win32/Netsky.C** | 2004/10/13 | **Win32/Netsky.B1** | 2005/03/25 | Win32/Mytob.J | | |
| 2004/03/01 | **Win32/Netsky.D** | | | | | | |
| 2004/03/01 | Win32/Bagle.H | | | | | | |
| 2004/03/01 | Win32/Netsky.E | | | | | | |

注 :当社で確認したもののみを記載

# ウイルス感染防止の実践的方法

企業でのウイルス感染防止には、2つの砦で効果的に！

(1) ゲートウェイでのウイルス対策

- InTheWildの既知ウイルスは、包括的にゲートウェイで処理。
- 現状多くのゲートウェイは未知ウイルスへの対応が不十分。
  - 今後は、ゲートウェイでも未知ウイルス対応が必要。
  - ゲートウェイとクライアントで、異なった会社のものを選ぶのも一方法。
  - 将来的には、SMTP、POP3、IMAP、HTTP、FTPをすべてサポートし、近い将来IM、NNTPなどにも対応できるコンテンツ・セキュリティ・ゲートウェイが必要となる。

(2) クライアントでのウイルス対策

- 対策をしていても感染するという現実の中で、未知ウイルスへの対応は、必要条件。今後はどれだけの多く未知ウイルスに対応できるかが課題。
- 選定の基準は

①高い未知ウイルス検出率　②IntheWildウイルス100%検出

③軽快な動作(オンアクセスキャン)　④超高速オンデマンドスキャン

# サイト運営者とサイト利用者の対策法

【サイト運営者の対策法】

- サイトの運営者の立場としては、やはり改ざんを如何に防ぐかということ。
- Webサーバへのリクエストの検査機能、保護機能が必要で、SecureIIS WebやNGSecureWebなどのアプリケーション・ファイアウォールの導入が必要。
- さらには、その他の不正侵入を防ぐための防護策(IPS)が重要。これについては、他社の技術も非常に進んでいるので、それらを参照のこと。

【サイト利用者の対策法】

- サイトの利用者の立場としては、やはりウイルス対策ソフトを必ず導入すること。その選定については、未知のウイルスにも対応できる製品を選ぶことが重要。
- スパイウェアに対する防御も重要
  - NOD32はスパイウェア/トロージャンに対するCheckMarkも受けている。
- スパイウェア除去ソフト「Spybot Search&Destroy」や、パーソナルファイアウォール「Outpost」の採用も有効。

June 2005 VIRUS BULLETIN 100% www.virusbtn.com

ICSA labs CERTIFIED www.ICSALabs.com Antivirus

WEST COAST LABS CHECK MARK SEE YOUR SAFEGUARDS AT www.check-mark.com
Anti-Virus Level 2

WEST COAST LABS CHECK MARK SEE YOUR SAFEGUARDS AT www.check-mark.com
Spyware

WEST COAST LABS CHECK MARK SEE YOUR SAFEGUARDS AT www.check-mark.com
Trojan

# 今回の事件からどんな点を学ぶべきか

- 今回の事件で重要なのは、改ざんが行われたことと、仕掛けられたウイルスを検知できるウイルス対策ソフトが非常に限られているということ。
- このことは、仮にウイルスがダウンロードされたとしても、またそれが未知のものであったとしても、感染を防がなければならないというウイルス対策ソフトに課せられた使命を全うできるソフトウェアとは、どういうものなのかという議論をユーザの立場で、真剣にしなければならない時期に来ている。
- つまり、ウイルス対策ソフトは、従来の認識に立ったシグネチャ方式だけでは到底その使命を全うすることができないということ。

  ウイルス対策は、まさに新世代に入った！
- NOD32は、未知のウイルスに対応した「次世代ウイルス対策ソフト」であり、今回の事件は、まさにこのような備えが必要であるのにもかかわらず他社製のものでは十分に対応できないということを事実をもって示した結果となった。

# おわりに

- 商業サイト改ざん事件から何を学ぶか
  - 商業サイト自身がなさねばならないサーバ改ざん防止対策
  - ウイルス対策は、未知ウイルスへの対応が最重要課題
  - ヒューリスティック機能が未知ウイルス発見の決め手
  - これからのウイルス対策は、未知ウイルス対応のものを!

- ご清聴、ありがとうございました。