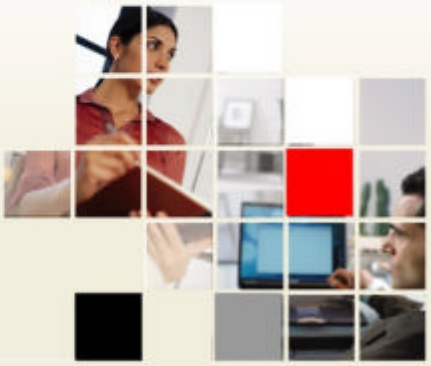
Trend Micro
Enterprise Customer Advocacy Group

TREND MICRO

今昔物語
～トレンドマイクロのウイルス検出技術向上への取組み～



サポートサービス本部
Threat Monitoring Center
平原 伸昭
2007年1月

2007-3-20

アジェンダ

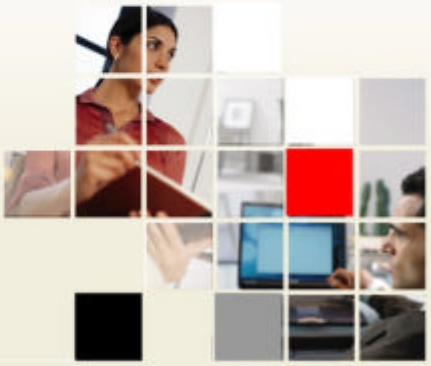
1. 脅威の変化！？
   1. マルウェアライターのモチベーション変化
   2. マルウェアの特徴変化
   3. まとめ
2. 現在と昔の検出ポリシーの違い
   1. 昔の検出ポリシー
   2. 現在の検出ポリシー
   3. まとめ
3. ウイルス検出技術
   1. Unpackerパターン
   2. Genericパターン：Family/variantsポリシー
   3. Genericパターン：Behaivoralポリシー
   4. IntelliTrap機能
   5. Generic Clean
   6. 疑わしいファイルの対処方法
   7. まとめ

Trend Micro
Enterprise Customer Advocacy Group

Trend Micro
Enterprise Customer Advocacy Group

TREND MICRO

脅威の変化！？
～マルウェアライターのモチベーション変化～



2007-3-20

かつては・・・

商売っ気無し!!
愉快犯的な動機

- プロフィール:
  - 男性
  - 14～34歳
  - パソコンオタク
  - 彼女居る歴・・0年
  - 社交性がない
  - 技術力を誇示したいという願望を持っている

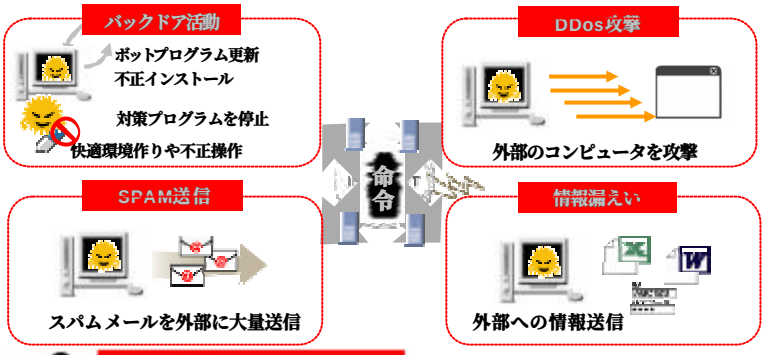
Trend Micro
Enterprise Customer Advocacy Group

今では・・・

組織化された犯罪集団へと進化を遂げる！

就業時間：1日約2分（ボットネットの管理）
- 月間売上： 平均6,800ドル（約81万6千円）

職務内容: 20カ国以上に13,000以上のボットを管理
- 感染したボット端末にAdwareをインストールさせてから新たに感染活動を行います。
- Adwareを随時表示させ、感染者のブラウジングの趣味趣向を探ります。
- パスワード、emailアドレス、クレジットカードや銀行口座番号などを収集します。



Trend Micro
Enterprise Customer Advocacy Group

Source: Washington Post: *Invasion of the Computer Snatchers*

Trend Micro
Enterprise Customer Advocacy Group

TREND MICRO

脅威の変化！？
～マルウェアの複雑化～

2007-3-20

～変化その1～

大規模なウイルスアラートの数の激減

弊社が出しているレッドアラート、イエローアラートの数は、2004年の32回をピークに減少し、2006年には激減し2006年は、1件しか発令されていません。

Year	Red Alert	Yellow Alert
2003	2	10
2004	2	30
2005	0	20
2006	0	1
2007	0	0

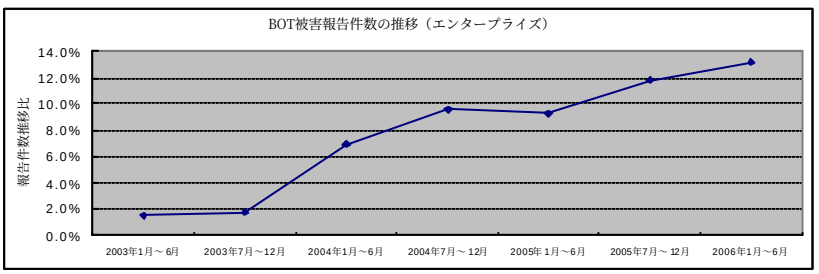
- シグネチャ型のウイルス対策以外に大規模感染予防、パーソナルファイアウォール機能といった複合型のウイルス対策の成果が考えられます。
- マルウェア作成の目的が感染活動から金銭や情報取得へと変化したために、摘発を逃れるために感染拡大をコントロールしていることが考えられます。
- 「マルウェア自体の数が減っている」という説も考えられます。

Trend Micro
Enterprise Customer Advocacy Group

～変化その2～

しかし、ウイルス数は年々増えている傾向にあった！

- ウイルスの出現数は急激に増加しており、2005年と2006年の同時期（5月1日から14日）を比べてみると2005年のこの時期に追加された**シグネチャは856個**でしたが、2006年の同時期に追加された**シグネチャはなんと、2780個と3倍以上の数**となっており、一日平均で200弱の新種マルウェアが発見されていることになります。
- 弊社サポートセンターにお問合せいただくBOT型ウイルスの被害報告を見ても右肩上がりになっています。



Trend Micro
Enterprise Customer Advocacy Group

～変化　その3～

- **マルウェアの特徴**
  - **従来の定義では限界！？**
    - ワームタイプ、トロイの木馬タイプ、複合タイプなど多種多様になっています。
  - **感染に気がつきにくい（1日平均10,000台の感染がある）**
    - 脆弱性やソーシャルエンジニアリングを使用
    - 新しい亜種が多いため、パターンファイルの対応が困難（ソースコードがインターネット上に公開されていることで、亜種の作成が容易）
  - **インターネットに接続して、不正プログラムをアップデート**
    - アップデート機能はBOT型ウイルスの特徴（BOT型ウイルスに限らず、最近のウイルスには自身の不正プログラムをアップデートする機能が実装されているケースがある）
    - 代表的なウイルス：WORM_RBOT, WORM_SDBOTなど

すべてのBOT型ウイルスでアップデート機能が実装されている訳ではございません。

～変化　その4～

不特定多数への攻撃から特定（限定へ、さらに連続型・・・・

- 従来は、不特定多数のインターネットユーザを狙って、迷惑メールやスパイウェアなどを「ばらまく」手口が主流でした。
- 最近では、特定の組織や企業、団体あるいは限られた人数のグループなどを陥れるために、ソーシャル エンジニアリングを応用しあたかも本物のように装ったメールやウイルスを送付する手口が確認されるようになっています。

『ターゲット型』攻撃

日本では、「狙った獲物をやりで仕留めること」や、「水中銃（spear gun）や銛(もり)で魚を仕留めること」が由来するスピアと表現されることもあります。つまり、ある特定のターゲットだけをピンポイントで標的としたインターネットの脅威が『ターゲット型』攻撃です。

～被害は甚大～

- FBIは2005年度アメリカではスパイウェアやコンピュータ関連における被害総額は**62,000,000,000ドル（約7兆440億円）**に達すると報告しています。
- アメリカ財務省によるとサイバークライムは違法な**麻薬取引よりもお金になる**と言われています。
- アメリカでは**毎日24,000,000,000ドル（約2兆880億円）の預金**が危機に瀕していると言われています。
- 日本国内のブロードバンドユーザの**2～2.5%**がBOT型ウイルスに感染
  - 国内ブロードバンド接続コンピュータ約2,000万台中**40～50万台**が感染していると予測
- ウイルス対策の未対策端末は、インターネット接続後**平均4分**でウイルスに感染するという結果がでております。

「ボットネット実態把握プロジェクト」より一部抜粋
2005年4月-5月Telecom-ISACおよびJPCERT/CCにて実施 ＊トレンドマイクロではTelecom-ISACメンバーとして解析に協力

Trend Micro
Enterprise Customer Advocacy Group

脅威の変化！？ ～まとめ～

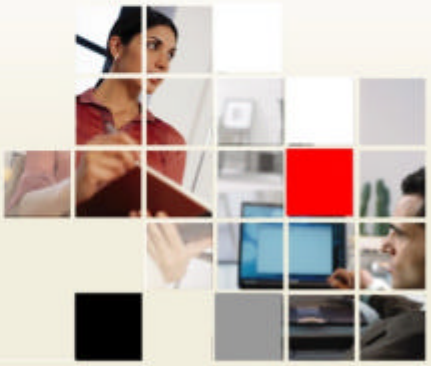
- **マルウェアライターのモチベーションが変化**
  - **悪戯から詐欺へ**
  - **アピールからハイドへ**
  - **個人から組織犯罪へ**
- **マルウェアの特徴が複雑化**
  - **従来の定義では区分することは困難**
  - **ウイルスからマルウェアへ**
  - **ソーシャルエンジニアリングとの組み合わせ**

Trend Micro
Enterprise Customer Advocacy Group

Trend Micro
Enterprise Customer Advocacy Group

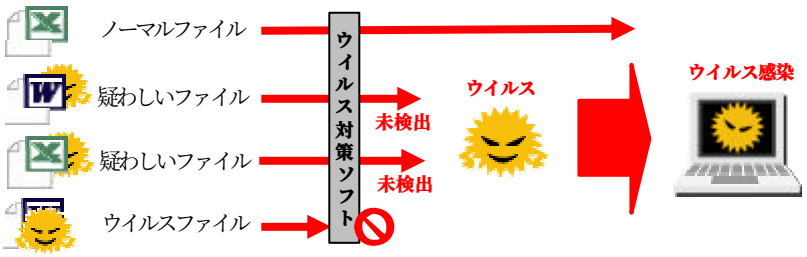
TREND MICRO

いまと昔の検出ポリシーの違い



2007-3-20

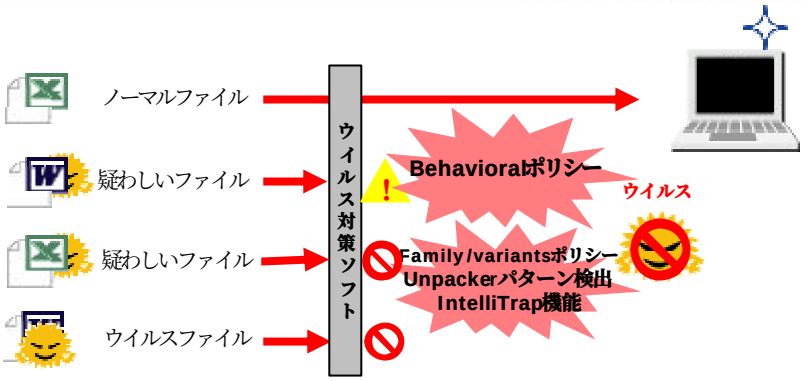
～昔の検出ポリシー～



従来の検出ポリシーでは、ウイルス感染の疑いのあるファイルは、検出することはありませんでした。これでは、近年の巧妙かつ複雑化したウイルスには対抗できません。

Trend Micro
Enterprise Customer Advocacy Group

～現在の検出ポリシー～



現在の検出ポリシーでは、ウイルスの特徴を持つ疑わしいファイルには、プロアクティブに検出や 警告」を行うことで、ウイルス感染のリスクを軽減いたします。

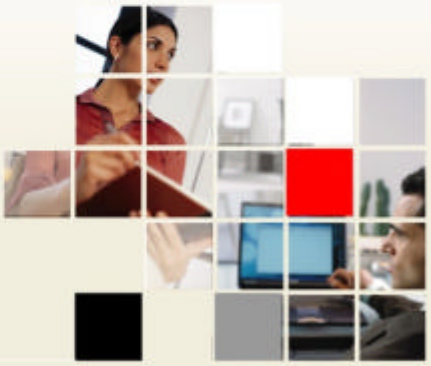
現在と昔の検出ポリシーの違い ～まとめ～

- 昔の検出ポリシー
  - 既知のウイルスのみに対応
  - 疑わしいファイルでも、そのままスルー
  - 新種・亜種への対応がリアクティブ
- 現在の検出ポリシー
  - 既知のウイルスと未知のウイルスに対応
  - 疑わしいファイルは、 警告」もしくは「検出」
  - 新種・亜種への対応がプロアクティブ

Trend Micro
Enterprise Customer Advocacy Group

TREND MICRO

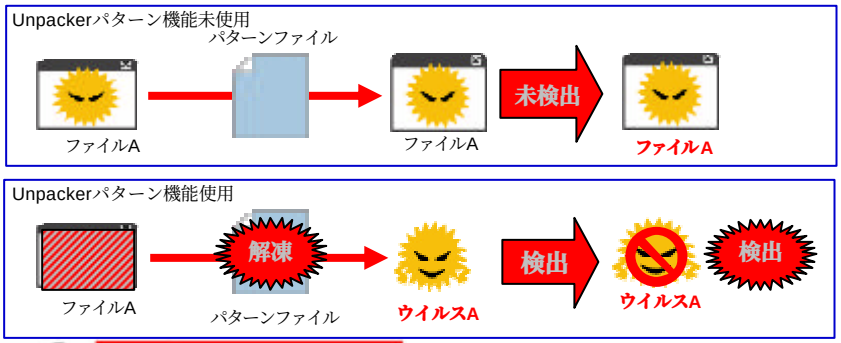
ウイルス検出技術



2007-3-20

～Unpackerパターン～

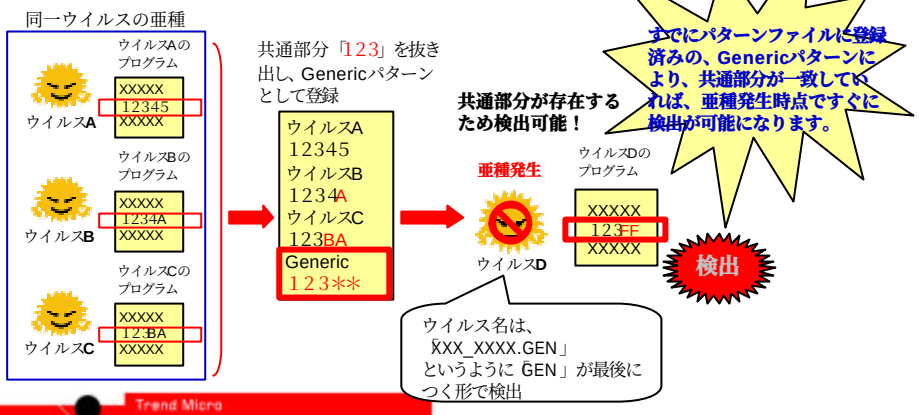
- 圧縮ファイルの解凍機能
  - 検索エンジン :ZIP、LZHなどのメジャーな多くの圧縮形式は、検索エンジンの機能により解凍可能です。
  - パターンファイル：検索エンジンに含まれていない圧縮形式の対応を迅速に行うために、パターンファイル内にも解凍ロジックを含めることができるようになりました。



Trend Micro
Enterprise Customer Advocacy Group

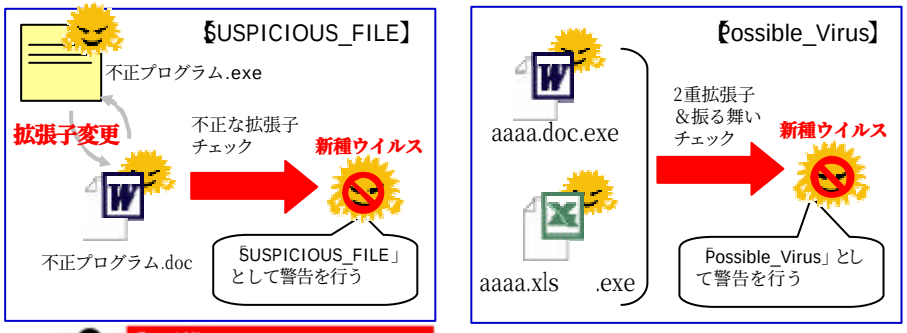
～Genericパターン Family/variantsポリシー～

- GenericパターンFamily/variantsポリシーによる亜種への対応
  - 亜種それぞれの、共通部分（コード）を抜き出し、パターンに登録しておくことで、ヒューリスティックに亜種への対応を可能にします。



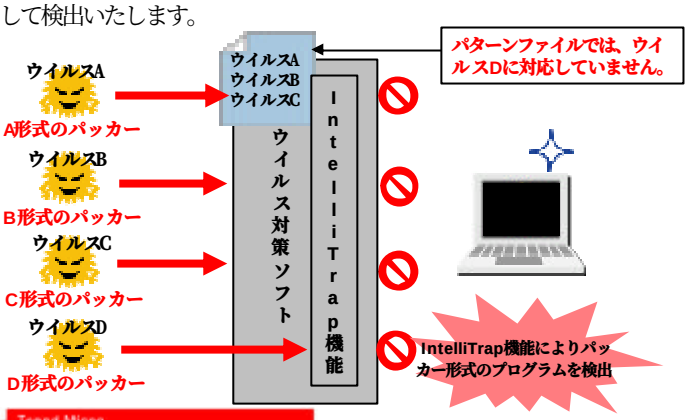
～ Genericパターン Behavioralポリシー～

- Behavioralポリシーによる新種への対応
  - SUSPICIOUS_FILE
    - 拡張子の偽装チェックを行い、不正プログラムの疑いがある場合には 警告」します
  - Possible_Virus
    - 2重拡張子と振る舞いのチェックを行い、不正プログラムの疑いがある場合には 警告」します



～IntelliTrap機能～

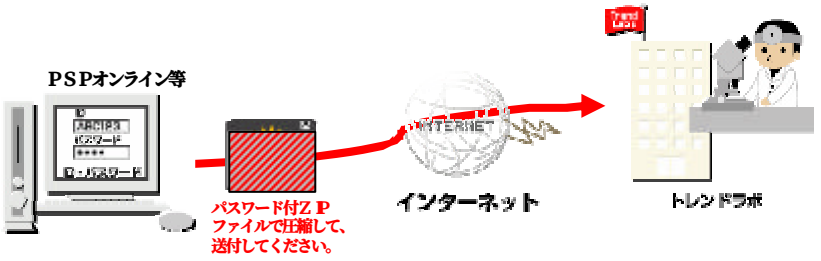
- IntelliTrap機能
  - 不正プログラムが持つ典型的な特徴の一つである自動実行型の圧縮ファイル形式（パッカー）をウイルスとして検出いたします。
  - パッカーにより圧縮されたプログラムは「PAK_GENERIC.001」，「PAK_GENERIC.002」として検出いたします。



ウイルス検出技術　～疑わしいファイルの対処方法～

- Genericパターン Behavioralポリシーで、「SUSPICIOUS_FILE」もしくは「Possible_Virus」として「警告」されたファイルは、不正プログラムの可能性が非常に高いため、PSPオンラインから弊社のトレンド・ラボまで検体の解析を依頼してください。
- 不正プログラムの疑いのあるファイルを「警告」として処理するには、ウイルス対策製品の検出アクションを「トレンドマイクロの推奨処理」に設定していただく必要があります。この設定にしていただくことで、Genericパターンでの検出処理設定が「放置(DoNothing)」となり、「警告」で留めることができます。

※「トレンドマイクロの推奨処理」以外に設定した場合には、お客さまが設定されたアクションに沿って処理（「削除」や「隔離」など）が行われます。



ウイルス検出技術　～まとめ～

- **Unpackerパターン**
  - 様々な圧縮形式を展開するための展開パターンをウイルスパターンファイル内に搭載することで、未知の亜種に対応します。
- **Genericパターン　Family/variantsポリシー**
  - 亜種ウイルスで共通すると考えられるシグネチャで未知の亜種に対応します。
- **Genericパターン　Behavioraポリシー**
  - ウイルスの特徴を持つ疑わしいファイルを「警告」することで、ウイルス感染を未然に防ぎます。
- **IntelliTrap機能**
  - 自動実行型の圧縮ファイル形式（パッカー）をウイルスとして検出します。
- **疑わしいファイルの対処方法**
  - 「警告」されたファイルは、不正プログラムの可能性が非常に高いため、弊社のトレンド・ラボで解析する必要があります。

Trend Micro
Enterprise Customer Advocacy Group

安心を、ひとつ上のステージへ。

TREND MICRO™

Trend Micro
Enterprise Customer Advocacy Group

用語説明　　(文責:SS研事務局)

【スライド5】

adware :
　侵入したPC上で強制的に広告を表示するソフトのこと。ある種のトロイの木馬がユーザの知らないうちにadwareプログラムをダウンしインストールしてしまうこともある。

バックドア :
　クラッカーにより侵入を受けたサーバに設けられた不正侵入を行なうための 裏口」。

【スライド7】

シグネチャ(signature) :
　signatureは、攻撃を示すsystemやnetwork activityパターンを反映したもの。IDSやfireWallはこれらのsignatureで危険なパターンを区別することで攻撃を判別する。

【スライド12】

ソーシャルエンジニアリング(Social Engineering) :
　id/passwordを入手するため、メールに仕掛けられた攻撃を実行するリンクをクリックさせたりする等、心理的な弱点をついて、人を騙すハッキングの一種。

【スライド16】

リアクティブ：事後対処型
プロアクティブ：予防型