サイエンティフィック・システム研究会
2006 年度システム技術分科会第 2 回会合　　2007 年 1 月 31 日

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～

トレンドマイクロ株式会社
平原 伸昭

■ アブストラクト

2004 年以降、インターネット上の脅威は従来のウイルス、ワームだけでなく、ボットネットやターゲット型攻撃に代表されるように、その脅威を見えなくさせる見えない化(不可視化)が進んでいます。今年はさらに WORM_STRATION に代表される連続攻撃化、Web Threats と呼ばれる新たな脅威が加わり脅威の複雑化という状況にあります。

本報告では、不可視化、連続攻撃型の新しい脅威などの最新動向を交え、トレンドマイクロのウイルス検出技術向上への取組みの中から「検出ポリシーの今と昔」、「検出技術」および「駆除技術」について、ご説明させていただきます。

■ かつては・・・

かつては、自分の技術を誇示するような愉快犯的な動機でマルウェア[1]を作成していたと言えます。作成者としても、パソコンオタクの延長線にいる人物像が特徴的です。また、これまでは単独犯がほとんどで組織だった犯行とは言い難いといえます。

■ 今では・・・

ボットネットから個人情報などを収集し売買することで、収益を得ていることが大きな特徴になっています。ボットネットとは、ボットと呼ばれるウイルスの一種が構成するネットワークの総称で、数百～数万台の規模で構成されるネットワークです。

ボットネットは、通常のウイルスやワームとは異なり、HERDER[2](牧夫)または MASTER と呼ばれる人間の指示により、DDoS 攻撃[3]やスパムメールの送信といったさまざまな活動を行います。

■ 脅威の変化！？　～マルウェアの複雑化～

～変化その１～ 世界的な大規模感染の現象

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ています。これは、シグネチャ[4]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ウイルス対策の複合化の成果とも考えられますが、それ以上に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、摘発を逃れる目的で感染拡大のコントロール（脅威の見えない化）が進んだためと推察されます。

---

1 マルウェア (malware) : 一般に不正プログラム全般を指す。

2 HERDER : ボットネットを操る攻撃者を指す。herder とは英語で羊飼いのこと。

3 DDoS 攻撃 (Distributed Denial of Service attack) : 攻撃の踏み台になった複数のコンピュータが、標的とされたサーバ等に対して攻撃を行うこと。

4 シグネチャ : 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。

(脚注文責:SS 研事務局)

～変化その２～ 亜種の増加

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新たな脅威のひとつである「Web Threats」の温床となっている 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。

～変化その３～ Web Threats

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おり、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/ダウンロードする Web Threats は 2005 年～2006 年にかけてその増加を加速しており、従来の SMTP[5]を介して感染を拡大するマスメーリング型と比較すると全世界で約 20 倍の感染報告件数が集まっています。

代表的なものには悪意のあるスクリプトが記述された Web ページからのダウンロードや PE_FUJAKCS や PE_LOOKED など他の不正プログラムが Mother Virus となり他の TORJ や TSPY をダウンロードする傾向となっており、トレンドマイクロではこの傾向が 2007 年度も引き続き続くと予想しています。

～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、Web Threat・・・・

このように、複雑化する脅威に対応するためには、パターンファイル＋検索エンジンといった One fit to All のソリューションでは対応できなくなってきています。

トレンドマイクロは、長年培った「未知の脅威」に対抗していくための技術研究をベースに、シグネチャを必要としないソリューションの開発に着手しております。

本日はその中のひとつであるパターンの強化について説明させていただきます。

■ いまと昔の検出ポリシーの違い(パターン強化編)

～昔の検出ポリシー～

従来の検出ポリシーでは、実際の検体を入手し、解析した後にパターンファイルへの反映を行っておりました。検出の精度が高い反面、ウイルス感染の疑いのあるファイル(未知の検体)の検出には弱く、これでは、近年の巧妙かつ複雑化したウイルスに対抗するには十分ではありません。

～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[6]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

既知のウイルスを中心とした対応

疑わしいファイルの対応はコンサバティブ[7]

新種・亜種への対応がリアクティブ[8]

---

5 SMTP(Simple Mail Transfer Protocol)：サーバ間でのメールのやりとり、クライアントがサーバにメールを送信する際に用いられるプロトコル。

6 プロアクティブ：予防型

7 コンサバティブ：後ろ向き

8 リアクティブ：事後対処型

(脚注文責:SS 研事務局)

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

■ ウイルス検出技術（パターン強化編）

～Unpacker パターン～

Unpacker **パターンは、さまざまな圧縮形式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、ウイルス検索エンジン上で圧縮ファイルを展開し、圧縮形式が異なる以外は同一のウイルスを** 1 **つのウイルスパターンファイルとして検出する技術になります。**

圧縮形式が違うだけで亜種としてパターンファイルのシグネチャ作成しなくとも既知として検出できる技術になります。

～Generic パターン Family/variants ポリシー～

Generic**パターンは亜種それぞれの、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**[9]**に亜種への対応を可能にします。**

これによりすでにパターンファイルに登録済みの、Generic **パターンにより、共通部分が一致していれば、亜種発生時点ですぐに検出が可能になります。**

～ 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 **機能は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。**

■ さいごに

トレンドマイクロでは日本特有の脅威に対応するための、「リージョナルトレンドラボ」を開設し、日本特有のセキュリティ脅威に関する情報収集活動を行い日本のユーザーを迅速にサポートする体制を整えています。

その一環として、リージョナルトレンドラボ内の Threat Monitoring Center **においては、日本国内におけるインターネット上の脅威に対して迅速かつ効果的に対応するため、実際に発生している攻撃の傾向を把握し、その経路上で流通しているマルウェアを収集しています。**

以 上

---

[9] ヒューリスティック：ウィルスの挙動パターンを推論して検知する手法。 (脚注文責:SS 研事務局)