ソフォスラボ： セキュリティ脅威が迅速に変遷するなか、「デイ・ゼロ」攻撃に対する保護を提供

ソフォス ポジショニング技術資料

2005年6月

現代の企業は、急速に蔓延するウイルスや、スパム、そしてフィッシング攻撃詐欺やスパイウェア攻撃など、複雑に絡み合うセキュリティ脅威の増加に先手を取って対処しなければならないという課題に直面しています。このホワイトペーパーでは、ソフォスラボ（SophosLabs™）が提供する専門知識とシステムを活用して、あらゆる種類の脅威から確実かつ迅速にビジネスを防御する方法について説明します。また、ソフォスの Genotype™（遺伝子型）テクノロジーを使用して、プログラムやメールメッセージの遺伝子型構造を解析し、新たなウイルスやスパムからの保護を先制的に提供実現する方法についても説明します。

変遷する課題

新しいウイルスやスパムのような悪意のあるソフトウェアの脅威は、さまざまな蔓延方法を組み合わることにより、急速に変化しています。新たなウイルス脅威やスパムの出現に、セキュリティソフトのベンダーは迅速に対応し、特定のウイルス検出アルゴリズムや、脅威を検出して対処する新しいスパムルールを作成します。ウイルス作成者はそれに対抗し、新ウイルスをできる限り頻繁に放出し、作成したウイルスの残存率を上げるために、多様な亜種を短期間にたびたび配信します。同様にスパマーは、多様なトリックを駆使して特定のスパム対策テクノロジーを回避する手口を発見し、フィルタを無効化します。

この絶えず変遷していく脅威環境で、ウイルス/スパム作成者の動機は、金銭を搾取する目的に変わりつつあり、ウイルス、スパム、フィッシング攻撃、そしてスパイウェア攻撃を組み合わせたセキュリティ脅威を発生させつつあります。以前は無作為な破壊行為が行われていましたが、現在は、より目的のはっきりした犯罪行為へと変わっており、ウイルス定義 (IDE) ファルに基づく従来のウイルス保護と既存のスパムルールを無効にするために同種のセキュリティ脅威から複数の亜種が絶えず作成され、より短期間で配信される傾向が強くなっています。

専門知識と高度なテクノロジー：最高の組み合わせ

深刻化するセキュリティ脅威に対処する方法として、さまざまなスタンドアローン型「デイ・ゼロ」攻撃ソリューションが出現してきました。しかし、効果的に保護するためには、新規ウイルスおよびスパム定義ファイルの迅速な作成と、包括的かつ先制的な検出機能とが必要です。テクノロジーの連携とソフォスラボに蓄積された専門知識をベースに、経験豊富なソフォスのアナリストが、蔓延の手法がどのような組み合わせであろうとも、新たなセキュリティ脅威に対して迅速かつ有効に対処します。

新しいセキュリティ脅威は、日の昇る順に従って、世界各地で感染を広げます。つまり、最初に朝を迎えるアジアから、ヨーロッパ、アフリカ、そしてアメリカ大陸の順に蔓延していきます。世界各地に展開するセキュリティ解析センター、ソフォスラボは、アジア・太平洋地域、ヨーロッパ、および北アメリカの東海岸と西海岸に配置され、すべてのタイムゾーンをカバーしています（図1参照）。多くの地域で始業時間前に、アップデートを作成して配信することができます。

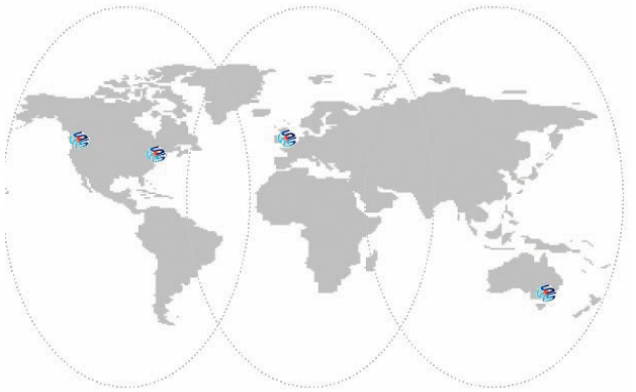
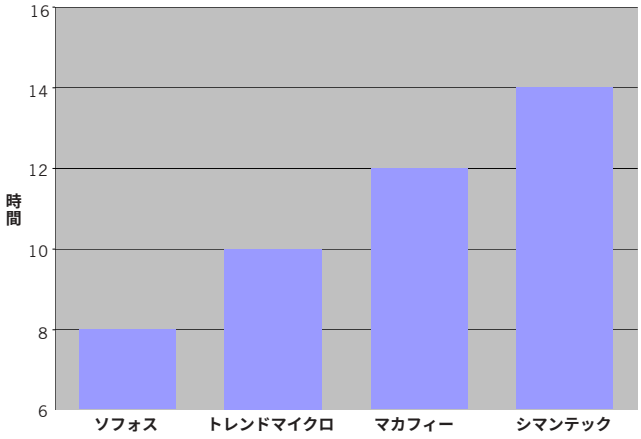


図1：ソフォスラボ、24時間/365日体制で解析と保護を提供

ソフォスラボは現在、1ヵ月に1万個以上のファイルをウイルス解析し、1日に400万件のメールをスパム解析しています。Mentor などの自動化されたシステムで、ウイルスを複製して解析し、新しい IDE ファイルをより迅速に作成しています。20年間以上におよぶセキュリティ対策の経験と実績を持つソフォスが蓄積した脅威情報のデータベースを、世界中のソフォスラボのアナリストが活用して解析を行っています。新しいスパムルールは1時間に2個ほどの早いペースで作成して配信されます。また、新種ウイルスの大規模感染が発生した場合にも、ソフォスは非常に迅速に対応しています(図2参照)。



出典：Andreas Marx, AV-Test, Virus Bulletin Conference, 2004

図2： ウイルス大規模感染時の平均対応時間

ソフォスラボは、セキュリティ脅威全般におよぶ専門知識と効率的に統合されたテクノロジーにより、スパムとウイルスが組み合わされた脅威に対しても包括的な保護を提供して、複雑化する新しいタイプのコンピュータ犯罪の増加に対抗するユニークな存在です。

優れたテクノロジーと強固な保護

ソフォスラボは、アナリストの経験と知識、そして高度で先進的なテクノロジーと検出方法により、迅速な保護を提供します。感染を広げる方法がいかに複雑であろうとも、既存および新種のセキュリティ脅威からビジネスを保護します。ウイルス、トロイの木馬、スパイウェアおよびワームは、以下に含まれる手法を組み合わせて検出されます。

- **ダイナミックコード解析（Dynamic Code Analysis™）： ソフォスのウイルス検出エンジンが使用する手法であり、特に、より複雑に暗号化されたウイルスの検出に有効。**
- **アルゴリズム型パターンマッチング： 入力データを、ウイルスとして認識されている既知コードシークエンスのセットと照合。**
- **エミュレーション： ポリモルフィック型ウイルス、すなわち、感染するたびに自身を異なった形に暗号化して身を隠すウイルスを検出。**
- **脅威の削減テクノロジー： 二重拡張子（例：.jpg.txt）や、ファイル形式を偽装した拡張子（例：拡張子 .txt を持つ実行ファイル）など、様々な基準によって、セキュリティ脅威となる可能性のあるファイルを検出。**

スパムは以下のような方法を使用して阻止されます。

- **自動チューニング： 主要フィルタリング機能を回避するように設計されたスパムに対応してチューニング。**
- **コンテンツスキャン： 複雑な偽装メッセージを解析し駆除。**
- **偽装検出： 一般的な偽装テクニックの検出。**
- **送信者確認フィルタリング（または DNS ブラックリスト）： 既知の IP アドレスを探知して阻止。**
- **URI 分析： 既知のスパマーの web サイトまたはドメインを検知。**

ウイルス/スパム特性の解析

ソフォスは、これらの多様なテクノロジーを駆使して、高信頼のウイルス/スパム対策を迅速に提供し、業界でもトップレベルの評価を得ています。さらに、Sophos Anti-Virus および PureMessage には、ソフォス独自の Genotype（ジェノタイプ - 遺伝子型）テクノロジーが組み込まれており、サーバー/クライアントマシン、モバイル PC、およびゲートウェイに最高の保護を提供します。Genotype テクノロジーは、セキュリティ脅威が蔓延する前に、包括的かつ先制的な保護を提供することによって、より早い段階でビジネスを保護することを可能にします。

Genotype テクノロジーは、特定のウイルス定義 (IDE) ファイルやスパムルールがリリースされる前、そして解析用サンプルをソフォスが入手する前に、ウイルスやスパムの亜種から企業を保護します。

Genotype テクノロジーは、ソフォスのウイルス/スパム検出エンジンに組み込まれており、既存のウイルス/スパムの新亜種を検出します。このテクノロジーは、遺伝子生物学を模して命名されました。生物学で遺伝子型は、個々の有機体の構造体であり、親から受け継いだ遺伝情報の単位である DNA 分子の配列である遺伝子から構成されます。ソフォスの Genotype テクノロジーは、新しいウイルスやスパムメッセージの「遺伝子情報」を分析し、既知のセキュリティ脅威に近い種類かどうかを解析して検出します。

ソフォスの Genotype ウイルス検出

ウイルス作成者は、ウイルスをより短期間により多く作成するために、既知のウイルスコードを再利用することがよくあります。たとえば、Rbot ウイルスでは800種類以上の亜種が作成されました。悪質な機能が新たに追加されても、亜種ウイルスは元の脅威と同じ特性を備えています。Genotype テクノロジーはこの点に注目し、プログラムの「遺伝子情報」を

Genotype ウイルス検出テクノロジーは、プログラムの遺伝子型を抽出し、現存するウイルスの遺伝子型とマッチングするかを解析し、ウイルス亜種を検知します。

抽出します。Genotype テクノロジーでは、特定のウイルスやスパムを対象とするので、従来のヒューリスティック方式に比較して高精度の検出を実現、誤検知を回避します。

すべてのプログラムは独自の「遺伝子」を持つと考えられますが、ウイルスなど悪質なプログラムの遺伝子は、通常のプログラムの遺伝子とは著しく異なった特徴を備えています。さらに、特定のウイルスファミリーの遺伝子は、他のウイルスファミリーの遺伝子とも異なっています。

ウイルスが持つ遺伝子には、次のような特徴があります。

- 自身をシステムフォルダにコピーする機能
- OS の脆弱性を利用して感染を広げるための機能
- レジストリキーを変更し、ユーザーがログオンした時に自動的に起動する機能
- ローカルディスク上のメールアドレスを検索する機能
- 自身をメールの添付ファイルとして送信する機能

Genotype による検出成功例
• Apribot の亜種を100%検出
• Baba の亜種を100%検出

Sophos Anti-Virus は、抽出された遺伝子情報を、高度にチューニングされたスコアリングシステムを使用して、既知のセキュリティ脅威の遺伝子型とマッチングします。検査されたファイルの遺伝子情報が、既知のウイルスファミリーの遺伝子情報と一致すると判定した場合、ウイルス遺伝子型（例：W32/Rbot-Gen）として報告します。

ソフォスの Genotype スパム検出

スパマーは、絶えず新しい手口を導入して、犠牲者を増やそうとします。たとえば、IPベースのブラックリストでブロックされることを回避するために、フレッシュなプロキシを使用してスパムを送信したり、URI ブラックリストのフィルタリングを回避するために、スパムごとに何百もの新ドメインを登録して対応を難しくさせたりします。偽装パターンを無作為化したり、語句を入れ替えたり、関連のない単語や語句を任意に追加したりすることにより、同じスパムファミリーでも、各受信者の受け取るメッセージが、他の受信者のものとは異なるものに見えるようにできます。これは、スタティックなスパムルールおよび基本的なコンテンツ分析の効率を低下させます。

それでも、スパムを検出し、阻止することは可能です。同じスパムキャンペーン内のメッセージは、メッセージのサイズや特定のメールヘッダおよび属性など、共通の特徴をもっています。ソフォスラボのアナリストは、個々のスパムファミリーに固有の遺伝子型スパムファミリーテンプレートを作成し、受信したメールトラフィックを解析します。

Genotype スパム検出テクノロジーは、スタティックおよびダイナミックな「遺伝子」を認識して、スパムファミリーの遺伝子テンプレートを作成します。

テンプレートの例として、以下があります。

- メッセージ内の URL に、文字列 .aspx と、それに続く疑問符「?」および 5〜7個の数字が含まれているか?
- HTML に、ピンク色の背景色指定と3列の表を含んでいるか?

テンプレートと一致するメールは、既知のスパムファミリーとして認識され、フィルタにより自動的に阻止されます。遺伝子情報の中には、特定のスパム大規模感染に対処するために作成され、短期間で使用されなくなるものもあります。一方、長期におよぶスパムキャンペーンに対処するものは、長期間使用されます。

従来のスパム対策テクノロジーで全スパムトラフィックの95% が阻止されるため、Genotype テクノロジーは、従来の方式があまり有効でない、または作動しない場合にのみ使用されます。しかし、図3が示すように、その価値はネットワークを保護する上で計り知れません。図3は、特定のスパムキャンペーンに対して1 ヵ月間に渡って計測された Genotype 検出の実績です。2004年11月以来、Genotype テクノロジーのみが、ほぼ毎日 100% の確率でスパムファミリーを検出しています。グラフは、Genotype テクノロジー、URI 分析、および送信者確認フィルタリングをそれぞれ使用した検知率の違いを示しています。

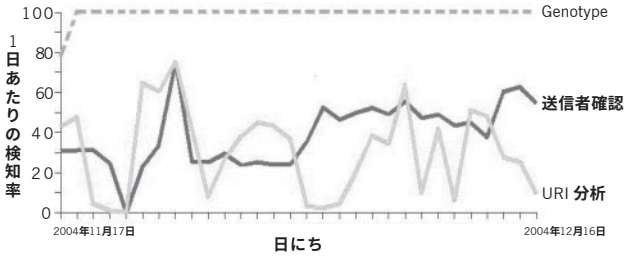


図3： Genotype テクノロジー、送信者確認フィルタリングおよび URI 分析の比較

最近のソフォスの分析によると、Genotype テクノロジーは、全スパムの約5%を阻止していますが、ブラックリストやヒューリスティック方式のみを用いたスパム対策ソリューションでは検出するのが難しいスパムファミリーに対し、100%の保護を提供して、最新のスパムキャンペーンに対する予防的な検出を実現します。

結論

ソフォスラボは、豊富な専門知識とテクノロジー、世界各地で新規のセキュリティ脅威を検出・解析する体制を効率的に組み合わせて、24時間/365日の解析と迅速な対応を提供し、複雑化するセキュリティ脅威からビジネスを保護します。Genotype テクノロジーを使用した「デイ・ゼロ」攻撃に対する保護は、その他高度にチューニングされた多様な手法やテクノロジーと統合され、比類のない高レベルの保護を、お客様に提供します。

ソフォスとソフォス製品を使用して貴社を保護する方法の詳細は、www.sophos.co.jp をご覧ください。