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

迷惑メールの動向とSymantecが考える対応策

株式会社　シマンテック
製品戦略本部
安元 英行

アブストラクト

シマンテックは、半期毎にセキュリティ脅威レポートを作成し配布しております。これは、シマンテックのセキュリティレスポンスと呼ばれるWorld Wideに張り巡らせた定点観測に基づいた、脅威の発生情報や、さまざまな脆弱性情報と解決方法の開示、新しいウイルスに対してのウイルス定義ファイルの作成、Spamメッセージの収集及び解析等を行っている部門が作成している物ですが、今回は、2005年度と2006年上半期の情報からSpam及びフィッシングの動向、これらの発生源となっているボットネットワークの動向を説明したいと思います。これらからスパマーの最新の活動状況がお伝えできると思っております。又、これに対してのシマンテックの対応製品及び対応体制について合わせてご紹介させて頂きます。

概要

シマンテックは、半期毎にセキュリティ脅威レポートと呼ばれる資料を作成し、これを広く公開しております。このレポートは、半年間に発生したさまざまレイヤーにおいて発生した脅威を解析し、管理者は基より一般ユーザにもリテラシー教育の一環としてお役に立てる様な報告書にしております。又今年からは、月毎にSpamの状況をレポートとして提示させて頂いております。セキュリティ脅威レポートは、百数十ページに及びますが、月次のSpamレポートは数ページの物でございます。

これらの情報は、シマンテックが誇るセキュリティレスポンスと呼ばれる組織が、World Wideに展開するセンサーから得られた情報を有能なアナリストが1ベンダーの意識に囚われず解析しまとめた物となります。

この度の講演は、これらの2005年から2006年のフィッシングを含めた迷惑メールの項目から判りやすくまとめた物で構成されております。

トピックとして抽出した物とその内容を下記にまとめます。

i)SMTPトラフィックにおけるSpamメッセージの割合の推移

一時期右肩下がりの傾向がありましたが、昨年末に増加傾向に転じています。

ii)Spamの種類の推移

種類は、時々に応じてカテゴリーを変えて送っている傾向があります、つまりカテゴリーでSpamの判断は難しい状況にあるという事が言えます。

iii)近年のイメージスパムと呼ばれる手法の紹介

イメージスパムと呼ばれる手法は、数年前にはやった手法ですが、これが進化を遂げております。これにより、シグネチャ[1]マッチングの手法で見つける事が極めて難しい状況に陥っていると言えます。

iv)スパムの発信源とボットの関連性

スパムの発信源がボットに感染したマシンとなっている事が裏づけられる結果となっている事が判ります。これによりスパマーと呼ばれる人は、大量のスパムを本当の発信源を探られる事なく、送り続け、大きな収入を得ていると言われています。

---

[1] 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)

v)フィッシングの傾向

スピアメール[2]と呼ばれる、配信先を企業の役員の方等に集中して悪意のあるメールの割合に関して、そのメールにて被害の数が多くなるという傾向がある事が憂慮されます。

講演の後半は、Symantec が提供する製品の内容となります。Spam スロットリング[3]と呼ばれる手法を装備した SMS8160 と呼ばれるアプライアンスから、メッセージの中身を精査して Spam の判定を行う SMS8300 シリーズを中心とした説明をさせて頂きました。
最後には、これらの製品を影で支える Spam の情報収集機関の説明とその能力を紹介しております。World Wide に 300 万以上のデコイ[4]アカウントを保持しており、これらに届く生きた迷惑メールを基に約 10 分間隔で、お客様の製品に、フィルター及びシグネチャを提供し、すぐれた検知率を提供しております。又合わせてこの機関では、リュピテーションサービスと呼ばれる悪意のある MTA[5]の情報を収集し、製品の精度の向上に一役買っております。
最後に、脆弱性が発見され時間を置かずに作成される Virus に対応すべく新しい手法を装備し、お客様から次々と現れるさまざまな脅威から守る製品を作り続けております。

Symantec は製品だけでなく、情報も提供する事にて管理者やユーザの方にも広くセキュリティの最新動向を学んで頂く事も努力させて頂いております。

以　上

---

2 スピアメール：spear phishing は特定の人物を狙い、偽のメールを送ったりウイルスを仕込んだりしてパスワードや個人情報などを搾取する詐欺。

3 スロットリング：spam メールの大量送信を抑制する手法(流量制限)。

4 デコイ ： 囮。

5 MTA(Mail Transfer Agent) ：MTA は SMTP(Simple Mail Transfer Protocol)を使用してホスト間でメールを転送する。

(脚注文責:SS 研事務局)