バックドアって何？

ウイルスの置き土産

最近、またしてもウイルスメールが活発化しています。皆様のところにはウイルスメールは届いていませんか？うかつに添付ファイルを開くのは大変危険です。英語のタイトルで添付ファイルがあるメールはウイルスメールと判断して間違いないと思われます。もし添付ファイルを送信する事がある時は、事前にその事を相手に知らせるメールをする気遣いも大事ですね。

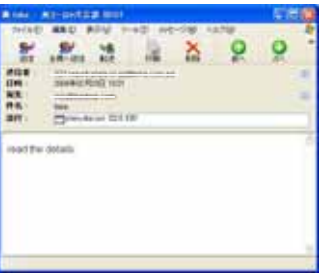
これが最近のウイルスメールだ！

最近のウイルスは、パソコンのデータを破壊や削除するものの他に、大量にメールを送信したり、特定のWebサイトに一斉にアクセスしたりして、ネットワークに大きな負荷をかけ、通信システムをダウンさせるものが増えてきました。現在危険視されている代表的なウイルスを下に挙げてみました。

NetSky　ネットスカイ

このウイルスはメールの添付ファイルとしてパソコンに侵入します。添付ファイルを実行しなければ感染はしません。メールの件名は「hi」「hello」などが多いようです。感染すると、パソコンの中にあるファイルからメールアドレスを探し出し、差出人を詐称したメールに自分自身をコピーした添付ファイルを付けて送信します。また、共有ドライブや共有フォルダに自分自身をコピーします。駆除ツールが、トレンドマイクロ、シマンテックより公開されています。

NetSky
件名：**fake**
添付ファイル：story.doc.scr



NetSky
件名：**hello**
添付ファイル：final.zip

特徴
件名には以下のものが使用されます。
hi , hello , warning , fake , read it immediately , stolen , posting aboutyou , something for you , unknown　このほか多数あります。
添付ファイル名には以下のものがあります。
document , msg , doc , talk , message , creditcard , details attachment , me , stuff , posting　このほか多数あります。
メールの本文は1行程度の比較的短めの英文です。
something is going wrong! , what does it mean? , take it easy yes, really? , kill the writer of this document!　この他にもあります。

MyDoom　マイドゥーム

このウイルスもメールの添付ファイルを実行しなければ感染しません。感染すると、ウイルスメールの送信、不正リモート操作のためのセキュリティホールを作成、Dos攻撃をします。AタイプとBタイプの種類があり、Aタイプは、2月12日以降は感染活動を行いません。また、Bタイプは、3月1日に活動を停止します。しかし、両タイプとも感染時に仕掛けたバックドア（不正アクセスを許すセキュリティホール）は残り、機能し続けます。駆除ツールが既に公開されています。

MyDoom
件名：**Server Report**
添付ファイル：file.exe

MyDoom
件名：**Mail Delivery System**
添付ファイル：document.zip

特徴
件名には以下のものが使用されます。
Returned mail , Delivery Error , Status , hello , hi , test , Error Server Report , Mail Transaction Failed , Mail Delivery System
添付ファイル名は不定ですが、拡張子は以下のものがあります。
二重拡張子の場合、1つ目は、htm txt docとなり、2つ目または1つだけのものは、pif scr exe cmd batになります。この他、上図のように、zip もあります。ファイルのアイコンも書き換えられますので注意して下さい。
メールの本文は、sendmail daemon reported:のほか6種類ほどあります。こちらは、NetSkyより長文になっています。

トレンドマイクロやシマンテックのサイトに、各ウイルスの特徴や詳しい情報が掲載されています。

ウイルスメールは非常に巧妙な手口で感染を試みます。感染したパソコン内からメールアドレスを探し出す場合は、ホームページを見た後のキャッシュファイルからも収集します。私の場合、当社のホームページにメールアドレスを公開していますので、社内でも一番多くのウイルスメールが届きました。

こんなウイルスもあります

期間限定活動

MyDoomなどのウイルスは期間限定で活動を行います。ですからある日を境にしてメール送信もDos攻撃もなくなり、ウイルスが居なくなったように感じられます。しかし、感染と同時に作成した不正アクセス用のセキュリティホール（バックドア）はそのまま残ります。不正アクセスが可能ということは、バックドアを入口にして、新たなウイルスを送り込んだり、そのパソコンをウイルスの発信源にさせる事も可能になります。ウイルス騒ぎが沈静化しても安心せず、日頃からウイルスチェックを行いましょう。

ウイルスを駆除するウイルス

ウイルスの中には、既に感染済みの特定のウイルスを駆除するウイルスがあります。「駆除してくれるからいいじゃん！」と喜んではいられません。他のウイルスを駆除して自分が居座るのです。結局ウイルスの棲家になってしまうのです。

ウイルスのバグ

バグとはプログラムの欠陥です。世界中で発見されるウイルスの中にはバグのあるウイルスも発見されています。バグのおかげで感染はしたが、発病しないと言う事もあります。人間の作ったウイルスですからたまにはこんな失敗作もあるのです。

■シマンテック・セキュリティスキャン
シマンテックのサイトではインターネット上でのウイルスチェックが行えます。ウイルスチェックのほかにセキュリティ関連のチェックも行えますので、こちらも一度チェックしてみて下さい。
http://www.symantec.com/region/jp/securitycheck/index.html

■ウイルスバスターオンラインスキャン
トレンドマイクロのサイトから行えるウイルスチェックです。チェックするドライブを選択して検索ボタンをクリックするだけで簡単です。ウイルスが見つかった時は、駆除ツールをダウンロードしましょう。
http://www.trendmicro.co.jp/hcall/index.asp

開発室から

毎日数十通ものウイルスメールが届いていました。英語のタイトル、添付ファイル付き、知らない差出人からのものでした。私はトレンドマイクロとシマンテックからのメルマガを受信していますので、今回のウイルス（MyDoom）のことは知っていました。それでもこれだけ大量のウイルスメールが来たのは初めてだったので、念のために常駐しているウイルス対策ソフトのほかにオンラインスキャンなど三重のスキャンを行いました。