

PRESS RELEASE

FOR IMMEDIATE RELEASE: 2006 年 9 月 26 日

コンピュータの乗っ取りをねらって複数の亜種を持つウィルスが発生

～ アイアンポートが 96,000 件ものウィルス混入メールを排除～
1 週間で 190 万ドルのコスト節減効果を達成し、世界的なウィルスの蔓延を阻止

事実関係

- 06 年 9 月 11 日の週に「IronPort Virus Outbreak Filters™」が一連のウィルスを検知・阻止しました。送信時刻にはばらつきがありましたが、大規模な波状攻撃でコンピュータを乗っ取って踏み台にし、そこから攻撃を仕掛けるねらいがあったものと見られます。
- 「Stration」と命名されたワームを若干改変した亜種 8 種がばらまかれ始めたのは、9 月 9 日。これが同 14 日まで続きました。
- この Stration ウィルスには攻撃プログラムが含まれており、感染したコンピュータには、裏口となる「バックドア」が作られます。このバックドアを利用して感染コンピュータを乗っ取ることができるため、大量発生の兆しがありました。
- 今回の Stration の大量発生では、受け取ったユーザーがウィルス混入メールをうっかり開けてしまう新手のテクニックが使われていました。IT 担当者からのメールを装い、「新しいウィルスが発生した模様のため、添付ファイルを適用して各自コンピュータを保護するように」と指示する内容でした。
- 多くのユーザーが騙されて添付ファイルを開けてしまったため、ウィルス対策を講じていなかったユーザーにいと簡単に感染してしまいました。
- アイアンポート®は、同ウィルスが発生した週だけで 96,000 件を超えるウィルス混入メールを阻止しました。もしそのままウィルス感染が広がった場合の除去費用は 190 万ドル(約 2 億円以上)に達していたと見られます。全メッセージの 10%を抽出して調査した結果、万一、感染した場合の復旧コストはデスクトップ 1 台当たり 200 ドルと推定されます。
- 最初のアンチウィルスシグネチャが公開される 4 時間 16 分前(平均)に「IronPort Virus Outbreak Filters」が攻撃に対するアラートを出して、攻撃を制限しました。

本件に関するコメント

「最近のウィルスは単にコンピュータをクラッシュさせるだけでは済みません。文字どおりコンピュータを乗っ取り、個人情報や機密情報を盗み出し、この情報を基に、さらにスパムやウィルスを広範囲にばらまきます。ひどいときには、感染したコンピュータを“ボットネット”(乗っ取った PC で構成するネットワーク)の一員に組み込み、闇市場で売買しているケースもあるほどです」----パット・ピーターソン(アイアンポート技術担当副社長)

「ウイルスを作る人間は、数日の間に数種類の亜種をばらまく傾向があります。このような手口をとられた場合、従来のアンチウイルスベンダーであれば、ウイルスを追跡して亜種 1 つひとつにシグネチャを作成する必要がある、シグネチャが 1 つで済むケースに比べてはるかに時間がかかります。従来型のアンチウイルスベンダーにとって、今回のような分散型攻撃を完璧に阻止する対策を即座に講じることは難しくなっています」--ジャン・マック (アイアンポート脅威対策センター所長、同センターは年中無休 24 時間態勢でウイルス発生の事前検知・阻止を担う専門チーム)

参考資料へのリンク

ウイルス発生の検知時に IronPort Virus Outbreak Filters からの自動アラートの受け取りをご希望の方は、下記 URL をご覧ください。

http://www.ironport.com/outbreak_alerts/

主要アンチウイルスベンダー各社が対応するまでの所要時間については、下記をご覧ください。

<http://www.ironport.com/toc/>

Virus Outbreak Filters の概要

ウイルス拡散防止ソリューションとして定評ある「IronPort Virus Outbreak Filters」は、新型ウイルス発生時に、アンチウイルスベンダー各社がシグネチャを公開する何時間も前の段階での、最初の防衛策となります。これまでの実績では、事後対応型アンチウイルスソリューションよりも平均 13 時間以上前にウイルスを阻止しており、きわめて高い捕捉率と限りなくゼロに近い誤判別率を誇っています。メールセキュリティアプライアンス「IronPort C-Series™」に搭載されており、送受信メールの危険度を判定して不審なメールがあれば、一時的に検疫対象とします。従来型アンチウイルスベンダー各社からシグネチャが公開された時点で、検疫対象のメールを自動的に解除します。

IronPort Virus Outbreak Filters (ウイルス拡散防止フィルタ):

- *従来型アンチウイルスベンダーのソリューションよりも平均 13 時間以上前にウイルスを阻止する実力派。
- *アイアンポート製品のお客様は、これまでに推定総額 3 億 2000 万ドル (約 375 億円) のウイルス除去費用の出費を節約できた計算に。
- *過去 12 カ月間だけでも、175 回以上のウイルス発生を阻止し、約 1600 万通のウイルス混入メールを排除。

アイアンポートシステムズの概要

アイアンポートシステムズは、中小企業にはじまり、フォーブス誌「グローバル2000」企業ランキングに名を連ねる世界の巨大企業に至るまで、幅広い企業向けにメールとウェブのセキュリティ製品を提供するリーディングベンダーです。今、多くの企業がミッションクリティカルなネットワークの管理や脅威への対策といった難題を抱えています。アイアンポートシステムズでは、先進の技術を駆使し、高性能で使い勝手に優れた製品で、こうした難題を解決します。アイアンポートの製品・サービスの詳細については、弊社ウェブサイト (<http://www.ironport.com/jp>) をご覧ください。