

Virus Report

2006年12月4日

トレンドマイクロ、ウイルス感染被害マンスリーレポート【2006年11月度】 ～再び、感染被害が分散化傾向に～

トレンドマイクロ株式会社（本社：東京都渋谷区、代表取締役社長 兼 CEO：エバ・チェン 東証一部：4704、NASDAQ：TMIC 以下トレンドマイクロ）は、2006年11月度のコンピュータウイルス感染被害報告件数マンスリーレポート（日本国内）をお知らせいたします。

ウイルス感染被害マンスリーレポート 2006年11月度

| 順位 | ウイルス名 (通称) | ウイルス種類 | 被害件数 | 先月被害 件数 | 先月 順位 | 先月 順位比 |
|-------|------------------------------|---------|------|------------|----------|-----------|
| 【1位】 | WORM_STRATION (ストレーション) | ワーム型 | 163件 | 563件 | 【1位】 | |
| 【2位】 | TSPY_LINEAGE (リネージュ) | スパイウェア | 85件 | 151件 | 【3位】 | |
| 【2位】 | WORM_SDBOT (エスディーボット) | ワーム型 | 85件 | 65件 | 【5位】 | |
| 【4位】 | WORM_RBOT (アールボット) | ワーム型 | 65件 | 78件 | 【4位】 | |
| 【5位】 | BKDR_AGENT (エージェント) | バックドア | 50件 | 221件 | 【2位】 | |
| 【6位】 | JAVA_BYTEVER (バイトバー) | その他 | 49件 | 58件 | 【6位】 | |
| 【7位】 | ADW_FLASHGET.E (フラッシュゲット) | アドウェア | 38件 | - | 【圏外】 | |
| 【8位】 | TROJ_SMALL (スモール) | トロイの木馬型 | 27件 | 4件 | 【圏外】 | |
| 【9位】 | PE_VIRUT (ヴィルト) | ファイル感染型 | 24件 | 56件 | 【7位】 | |
| 【10位】 | ADW_WINFIXER (ウィンフィクサー) | アドウェア | 23件 | 56件 | 【圏外】 | |

このランキングは、2006年11月1日から11月30日までに、日本のトレンドマイクロのサポートセンターに寄せられたウイルス被害件数をもとにランク付けを行ったものです。本数値は、2006年12月4日現在の情報に基づき作成されたものです。今後、サポート調査により、件数に変更が生じる可能性があります。

被害件数はウイルス発見のみの数字も含まれます。

()印のウイルスに関しては亜種をまとめてカウントした件数となります。

()印の「JAVA_BYTEVER.A」に関しては、パターンファイル番号1.546.00から「JAVA_BYTVERIFY.A」の検出名で対応いたしておりましたが、パターンファイル番号1.731.00から「JAVA_BTEVER.A」に改称いたしましたので、双方の数を集計したものになります。

()印のウイルスに関しては、「WORM_STRATION」、「WORM_STRAT」、「WORM_STRATIO」、「WORM_WAREZOV」をまとめてカウントした件数になります。

11月のウイルス傾向 「TrendLabs Japan」ウイルス解析担当者コメント

今月のウイルス感染被害の総報告数は、7477件と先月(8806件)から減少しました。ウイルス毎の報告数に関しても減少傾向にあることから、再び被害が分散化してきていることが伺えます。

大きな被害をもたらしたマスメール型ワーム「WORM_STRATION(ストレーション)」の感染被害報告数は先月と比べて減少していますが、新たな亜種の登場ペースは衰えていません。11月29日までに150種類以上の検体が集まっており、継続して注意が必要です。また、今までのこのワームは新しい亜種をダウンロードする動きを見せていましたが、その活動を応用し、スパイウェアなどの不正プログラムをダウンロードするようになってきました。これにより、亜種をダウンロードさせることによる多重感染だけではなく、PC内に保存されているメールアドレスの収集や、迷惑メールの踏み台に悪用される例が確認されています。

ますますエスカレートする亜種の頻発に対し、従来のパターンマッチングを拡張したジェネリックな検出技術が有効になってきています。例えば、ウイルスに悪用されやすい圧縮ファイル形式で判別する「Intelli Trap」が、「WORM_STRATION」の収束に大きく貢献しました。「WORM_STRATION」の亜種のうち、従来のウイルスパターンファイルで未検出の検体の約6割を「Intelli Trap」で捕らえられたことが確認されています。また、亜種に共通すると考えられるシグネチャをパターンファイルに採用する「Generic 検出パターン」も効果的です。これも未知の亜種に対しての予防措置に適した技術であり、「TSPY_LINEAGE(リネージュ)」の感染報告件数(85件)のうち43件は、この「Generic 検出パターン」により検出されました。現在では短期間で亜種が多く出現する傾向が強まっているため、今後もジェネリックな検出技術を活用していきたいと考えています。

新種ウイルス情報

「TROJ_STRAT.GG」(ストラット)

このトロイの木馬は、他の不正プログラムおよび不正リモートユーザにより、電子メールに添付されてコンピュータに侵入し、メモ帳のアイコンを利用し、正規のテキストファイルを装います。自身が実行されたフォルダ内にランダムな名称の.TMP ファイルを作成します。また、特定の Web サイトからファイルをダウンロードし、実行します。

・「TROJ_STRAT.GG」 詳細情報:

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ_STRAT.GG

トレンドマイクロ ウイルス情報

<http://www.trendmicro.co.jp/vinfo/>

トレンド フレックス セキュリティ

無償でウイルスやスパイウェアの検出・削除できるオンラインスキャンを提供しています。

<http://www.trendflexsecurity.jp/>

TRENDMICRO、Trend Labs はトレンドマイクロ株式会社の登録商標です。

各社の社名および製品名は、各社の商標又は登録商標です。

Copyright (c) 2006 Trend Micro Incorporated. All Rights Reserved.