we protect your digital worlds™

世界のセキュリティ脅威年間レポート

2008年12月

目次

はじめに

本書では、2008年における脅威の動向を振り返り、その傾向とそこから得られた教訓を明らかにするとともに、2009年に向けての予測を示します。

ESETでは2007年以降、個々の悪意あるコードの細かな点ではなくより幅広い傾向に注目するため、マルウェアに関するレポートの集計方法を見直してきました。これにより、ESET製品の強みであるプロアクティブ検出の結果がより明確にレポートに反映されるようになりました。脅威を巡る状況は非常に変化が激しく、現在、ESETが発表しているマルウェアランキングの上位は、亜種ごとに固有のシグネチャで検出された従来のようなマルウェアではなく、汎用シグネチャまたはヒューリスティック技術によって検出されたマルウェアがほとんどを占めるようになっています。そのためESETでは、マルウェアが出現してからそれに対応したシグネチャを作成するのではなく、まったくの新種でもプロアクティブに検出およびブロックできる技術の開発に注力しています。コードや振る舞いを分析することによって新種のマルウェアを検出する汎用シグネチャとアドバンスドヒューリスティックは、従来のシグネチャ検出を補完し、より幅広いタイプの脅威を検出することを可能にします。
本書の分析は、ESET製品の継続的なメンテナンスと強化に利用されているデータリソースに基づいて行われています。その1つであるThreatSense.Netテクノロジーは、ヒューリスティック技術によって検出された新種および既知の脅威についてのデータを自動的に収集し、ESETの脅威ラボに送信します。2008年のVirus Bulletinカンファレンス[1]でもESETの研究者が指摘しましたが、「クラウド」の分散コンピューティングリソースは、脅威の動向を監視してその傾向を分析するのに大いに役立てることが可能です。これらのデータは製品の検出機能の強化に役立ち、高度なプロアクティブ検出技術を継続的に改善して、既知の脅威だけでなくまったく新しい脅威を検出できるようにします。そしてこれは、セキュリティ市場における大きな武器となります。

またここ1、2年、実行可能ファイルを電子メールに添付して感染を広めるタイプのマルウェアは常に減少傾向にありましたが、依然として、この種の攻撃手法について分析を続ける意義があるだけの量は流通しています。ESETのVirus Radarは、電子メールを媒介とするマルウェアに特化してデータを収集するシステムですが、このシステムも引き続き活用されています。

概要

ESETのマルウェア追跡/レポーティングシステムで2008年におけるマルウェアの動向を分析した結果、次のような幅広い傾向が明らかとなりました（各項目の詳細については、それぞれの脅威がエンドユーザーに与える影響と合わせ、以降の章で解説します）。

偽アンチマルウェア製品が急増：この種の製品のほとんどはPCユーザーを標的としていますが、中にはMacユーザーを狙った製品も存在します。

通常は安全であると考えられる文書ファイル形式（PDFなど）の脆弱性を悪用するケースが増加：実際のところ、多くのデータ形式で埋め込みのマクロや実行可能ファイルが使用されているように、データファイルと実行可能ファイルは完全に区別できるものではなく、マルウェア作者は以前からこの曖昧さを利用しようとしてきました。その結果、今日のマルウェア作者は、「羊の皮をかぶったオオカミ」とでも言うべき危険なデータファイルの作成方法を熟知するまでに至っています。2000年代の初めに登場した、PIFファイルやLNKファイルを電子メールに添付して送り付けるなどのマルウェア拡散手法は、それほど高度な知識を持たないWindowsユーザーにもすぐさま警戒されるようになりました。しかしマルウェア作者らは、マルウェアを正規のファイルに見せかける方法を常に模索しており、現在では、細工を施したPDFファイルやリンク、FacebookやLinkedInなどへの悪意ある招待状など、決して安全とはいえないWeb 2.0的な技術を利用した、一見正当な活動に見える攻撃が深刻な脅威となっています。

WindowsのAutorun機能を悪用するマルウェアが引き続き数多く登場：ESETのヒューリスティック技術はすでにこの種のマルウェアに対応していますが、エンドユーザーは、抜本的な対策としてWindowsのAutorun機能を無効にすることを強く推奨します。

ソーシャルエンジニアリングや悪意のあるソフトウェア（キーロガーやバックドアなど）、あるいはその両方の組み合わせによって、オンラインゲームのユーザーアカウント情報を盗み出そうとするマルウェアが急増：この種のトロイの木馬の脅威はアンチマルウェアソフトウェアによって軽減することができますが、オンラインゲームのユーザーは、その仮想空間でどのような不正活動が行われる可能性があるかを認識しておく必要があります。

アドウェアなど、ユーザーにとって好ましくない動作をする可能性のあるアプリケーション（Potentially Unwanted Application：PUA）が引き続き検出された脅威全体の相当部分を占める：PUAはその動作の詳細を明らかにしていないことが多く、ホストシステムを改変することやアンインストールが困難であることが伏せられている場合が少なくありません。

2008 年の傾向と 2009 年の予測

米国カリフォルニア州サンディエゴに拠点を置くESETのリサーチチームは協議のうえ、いくつかの傾向と予測のトップ10を作成し、それらがエンドユーザーに及ぼす影響についてまとめました。その際、まずは2008年におけるマルウェアの主な傾向を見つけ出し、それに基づいて2009年に予測される傾向を導き出すという手法を採用しました。なお、ここに示す傾向は重要度の順ではありません。すべての傾向について、慎重な検討と注意が求められます。

表1：2008年におけるマルウェアの主な傾向

●	偽アンチウイルス/アンチスパイウェア製品が増加、高度化。
●	オンラインゲームのパスワードを盗み出すマルウェアが増加：攻撃者は、これらのマルウェアを通じてユーザーアカウントに不正アクセスし、ゲームのアバターやアイテムなどの資産、通貨を盗み出して転売します。
●	感染確率を高めるため、ほとんどのマルウェアファミリーがWindowsのAutorun機能を悪用。
●	トロイの木馬的な活動を行う不正なPDFファイルなど、通常「安全である」と考えられる文書を悪用する攻撃が増加。
●	ゼロデイの脆弱性に対する攻撃者側の研究が進み、オーバーフローなどを引き起こすアプリケーションやオペレーティングシステムのバグを悪用した攻撃が増加（攻撃が自動化されているケースも多い）。
●	MicrosoftのMS08-067に代表されるセキュリティ脆弱性の悪用（MS08-067の脆弱性は、ConficklerやGimmivなどのマルウェアファミリーに利用された）。
●	Stormワームボットネットの終焉（あるいは、その運用者たちによる自主的な一時休止）：このことからわたしたちは、「ボットハーダーは巨大ボットネットからより小規模なボットネットへと移行し始めているのではないか」という疑念を強くしています。小規模なボットネットは、大規模なボットネットよりも存在を隠ぺいしやすく、またメンテナンスも容易です[2]。
●	「ドライブバイダウンロード」など、Webブラウザやブラウザプラグインの脆弱性を悪用した手法で感染を広げようとするマルウェアが増加。
●	コーデックを装うマルウェアが引き続き数多く登場：この種のマルウェアは、何らかのデジタルコンテンツを再生するために必要な正規のプログラムに見せかけて自分自身を実行させようとします。また、ソーシャルエンジニアリングや感染プロセスの一環として不正なメディアファイルを使用するケースも多く見られました（代表例はGetCodec）[3]。
●	ランタイムパッカーや難読化を利用して、アンチマルウェアソフトウェアによる検出（主に従来型のシグネチャスキャン）を逃れようとするマルウェアが引き続き多く登場（ランタイムパッカーを利用するマルウェアの代表例はThemida）[4]。

表2：2009年に予測される脅威の傾向

●	実際には存在しないマルウェアを検出してみせる偽アンチマルウェアソフトウェアビジネスがさらに拡大し、ユーザーから金銭をだまし取ろうとする犯罪者がますます増加する：ソフトウェアの機能だけでなく、ユーザーをだます際のソーシャルエンジニアリングの手法もさらに洗練されていくと予想されます。
●	悪意のある広告、詐欺的な広告が増加する：この背景には、マルウェア作者がこのような形で投資を行うようになったこと、広告掲載サイトの管理人が掲載する広告の内容をきちんと確認しないことがあります。
●	Webブラウザ（特にシェアの高いブラウザ）を狙う脅威が増加する：Webブラウザが狙われるのは、利用頻度が高く、その性質上ユーザーを攻撃サイトに誘導しやすいソフトウェアの1つであるからです。
●	コンセプト実証（Proof-of-Concept：PoC）のための攻撃やモバイル用ブラウザを悪用する攻撃を含め、モバイルデバイスに対する脅威が増加する：具体的には、iPhoneやGoogle Androidベースの携帯電話で使用されているWebKit採用ブラウザに対する攻撃が増えると予想されます。
●	Mac OS XやLinuxなど、Windows以外のオペレーティングシステムが普及するにつれ、それらに対する脅威が増加する（ユーザーの意識や対策がその普及に追いついていないため）：Mac OS Xがマルウェア作者に狙われるようになるかどうかは、同OSが一定の市場シェアを獲得するかどうかにかかっているといわれてきましたが、同OSに対するマルウェア作者の関心は、ここ数年で確実に高まりつつあります[5]。
●	検出されるまでの時間をできるだけ長くするため、多くのマルウェア作者がデータ隠ぺい技術を採用するようになる：現在のほとんどのマルウェアは以前とは違い、できるだけ速く、そして広範囲に感染を広げるようには設計されていません。今日のマルウェア作者は、投資対効果が最大になるようにマルウェアを作成しています。
●	検出を逃れるため、さまざまなファイル形式（PDF、JavaScript、メディアファイルなど）を用いて悪意のあるコードを隠ぺいしようとするマルウェアが増加する：特に、ファイルを単なるデータファイルに見せかけ、その中に実行可能コードを隠すという手法が増えると予想されます。
●	ソーシャルエンジニアリングを利用した攻撃が増加し、攻撃の際に用いられる手法がますます洗練されていく：標的の心理を操るソーシャルエンジニアリングは成功確率の高い「攻撃技術」の1つであり、セキュリティにおける最大の弱点、つまりキーボードを操作する人間（ハッカー用語でいうところの「ウェットウェア」）をターゲットとします。 ただし、最も成功している攻撃の多くは、単純にユーザーの軽率な行動を突破口にしています。攻撃者はそのために、悪意のあるアプリケーションを正規のソフトウェアに見せかけたり、ほとんどの人からは特に問題がないように見える行動やコンテキストにユーザーを誘導したりします。具体的には、一見問題のなさそうな文書に悪意のあるコードを埋め込んだり、普通の文面に見える電子メール、Twitterのメッセージ、インスタントメッセージに悪意のあるリンクやコードを忍ばせたりするのです。Web 2.0的な技術は確かにすばらしいものではありますが、セキュリティ面では決して安全とはいえず、FacebookやLinkedIn、Twitterは、悪意のある招待状やフィッシングといった新たなリスクをもたらします。オンラインでの活動は多かれ少なかれリスクを伴うものであり、安全性を保つためには、これまでと同様、いかに現実に即してリスクを管理するかが重要となってくるでしょう。

●	多くのサイバー犯罪者が高度なビジネスモデルを取り入れるようになる[6]：マルウェアはもはや、研究熱心な10代のプログラマが、自らの技術や創造性を証明するために作成するようなものではなくなっています。マルウェア作成は投資対効果に基づいて行われており、悪意のあるコードは金儲けのための実利的な手段として用いられています。
●	VM（仮想マシン）を認識するマルウェアが増加し、仮想環境である場合には活動を停止したり、仮想環境固有の脆弱性を探したりするようになる：また、ますます高度化するボットが、動作マシン上でボットネットとしての活動を隠ぺいするために仮想化技術を使用するようになると予想されます。さらに、カーネルモードrootkitを利用するケースも増加し、動作中のマルウェアの検出が困難になると考えられます。

エンドユーザーへの影響

偽のアンチマルウェア製品

2009年は、偽のアンチマルウェアソフトウェアを売りつけてエンドユーザーから金銭を巻き上げようとする詐欺的行為が増加、高度化の一途を辿ると予想されます。現在のところ、ユーザーは何の役にも立たない偽のアンチマルウェアソフトウェアの代金を支払わされるという形で被害を受けていますが、近い将来には、ユーザーを食い物にするまた別の方法が登場してくるものと予想されます。現時点においても、これらの偽セキュリティソフトウェアをインストールする際、同時にスパイウェアやアドウェアがインストールされることは十分に考えられます。またユーザーがだまされてクレジットカード番号などの機密情報を漏えいさせてしまった場合、その情報は最初の漏えい先から転売されてさまざまな形で悪用される恐れがあります。

決してこの手のソフトウェアにだまされてはなりません。インターネット上には、自分たちを正規のセキュリティベンダーに見せかけようと、あの手この手を使って詐欺的ソフトウェアと正当なソフトウェアとの境界線を曖昧にしようとしている詐欺師が数多く存在します。例えば、2008年10月29日付のNY Times紙によると、ロシア某所に本拠を置くBakasoftwareは、スパムメールを活用した手の込んだ戦略のもとに偽のアンチウイルスソフトウェアの販売で年間500万ドル以上の売上を得つつ、それらを購入したユーザーの数千台ものコンピュータを間接的にコントロールしているとされています。また別の詐欺的ベンダーは、自分たちの「製品」が業界規格の認定を取得していると虚偽の主張をする、本当に機能する簡単なマルウェア検出機能を偽ソフトウェアに搭載する、公開のフォーラムで正規ベンダーを中傷する、自分たちを偽のセキュリティベンダーだと非難する正規ベンダーを訴えると脅す、などの行為を行っています。これらの点を踏まえると、この種のソフトウェアは、エンドユーザーにとっての敵であると同時に、セキュリティコミュニティにとっての敵でもあるといえるかもしれません。

データファイルがもたらす脅威

通常は安全であると考えられる文書ファイル形式（PDFなど）の脆弱性を悪用するケースが増加しています。多くのユーザーは、データファイルには（アプリケーション固有のマクロや埋め込みの実行可能ファイルなどの形で）実行可能コードが含まれている場合があることを現在も理解しておらず、そのことがマルウェアに感染する原因の1つになってしまっています。この数年、Microsoft Officeのマクロを利用したマルウェアは、主に同製品の最近のバージョンでマクロ機能が強化された結果として減少傾向が続いていますが、NCPHをはじめとするマルウェア作成グループが仕掛ける大規模攻撃では、マルウェアに感染させるために引き続きデータファイルが使用されています[7]。

正規ファイルの悪用

正規ファイルと悪意のあるファイルの境界線が曖昧になるシチュエーションはほかにもあります。例えば「Win32/Patched.BU」というのは、マルウェアによって改ざんされた正規のシステムファイルに付けられる名前で、この改ざんはそのシステムファイルと同時に悪意のあるファイルが読み込まれるようにすることを目的としています。Win32/Patched.BUは、同様のアプローチで感染を試みる不正プログラムファミリーの唯一の亜種です。これらのプログラムが正規ファイルを利用するのは、そのほうがファイル名だけに基づく検出を免れやすいからです（アンチマルウェア業界では、以前より一貫して「ファイル名だけに基づいてマルウェアを特定しようとすることには無理があり、正しく悪意あるコードを検出することはできない」と主張してきましたが、負荷の高いシグネチャスキャンをできるだけ避けようといまだにこの種の手法を採用しているベンダーも存在します）。ある意味でこのアプローチは、悪意のあるコードを実行またはダウンロードするために、無害に見えるプログラムを使用して真の悪意を隠ぺいしようとする手法と似ています。

ランダムなファイル名を付けるという方法も、ファイル名でのマルウェア検出を困難にする手法の1つであり、古くからよく用いられています。そのためアンチマルウェアソフトウェアを選択するにあたっては、メインのマルウェア検出手段としてファイル名を使用しているような製品に注意する必要があります。特に、「nastytrojan.dllを検出した唯一の製品」などと謳っている製品には注意が必要です。プログラムの悪意を判断する唯一の手段としてファイル名を使用するのは、ほとんどの場合、現実的であるとはいえません。

「WMA/TrojanDownloader.Wimad.N」は、メディアブラウザを悪意のあるURLにリダイレクトし、アドウェアなどの悪質な追加コンポーネントをダウンロードするWindows Mediaファイルです（TrojanDownloader.Wimad.Nをここで取り上げるのは、2008年を通じてたびたびランキングのトップ10に登場し、典型的なソーシャルエンジニアリングの手法を用いているためです。ただし、TrojanDownloader.Wimad.Nの検出は、現在は汎用シグネチャによって行われています）。このダウンローダは、ユーザーをだましてダウンロードさせるために、人気のある音楽ファイルを装ってピアツーピアネットワークで流通しています。マルウェアをMP3やFlashムービーに偽装してダウンロードさせるというソーシャルエンジニアリングの手法は、マルウェア作者の間で広く用いられています。つまり、一見無害なファイルが実行可能ファイルであったり、無害なファイルを通じて悪意のあるコードをコンピュータに送り込まれ、バックドアを設置されたりすることがあるのです。このような手法にだまされないためには、それ自体は実行可能でないファイルも、悪意のあるコードを送り込むために利用される場合があるということを認識する必要があります。また、コーデックなど、ある目的のために必須とされるコンポーネントのインストールを要求する画面が表示された場合も、十分注意することが必要です。これは、エンドユーザーをだまして悪意あるコードを実行させるためにマルウェア作者が用いる典型的なソーシャルエンジニアリングの手法です。

偽のコーデックと関連する脅威

悪意のあるファイルを新しいビデオコーデックに見せかけるというソーシャルエンジニアリングの手法は、多くのマルウェア作者が用いる定番のテクニックです。ほかのトロイの木馬と同様、この種のマルウェアは、何か便利なもの、おもしろそうなものに見せかけてユーザーに悪意のあるコードを実行させようとします。コーデックとされるファイルが本物のコーデックであるかトロイの木馬であるかを見分ける簡単で万能な方法はありません。したがって、自分から要求したのではない何かをダウンロードするように求められた場合は、慎重に、そして用心深く対処することが重要となります。信頼できるサイトから提供されているように思える場合でも、それが本物であるかどうか改めて確認することが推奨されます。例えばWMA/TrojanDownloader.GetCodec.Genは、メディアファイルを改ざんします。このトロイの木馬は、コンピュータ上で見つかったすべてのオーディオファイルをWMA形式に変換し、ユーザーを悪意あるコンテンツに誘導するURLが指定されたフィールドをヘッダに追加します。そして、メディアファイルを再生するにはそのURLからコーデックをダウンロードする必要があるというメッセージを表示します。 WMA/TrojanDownloader.GetCodec.Gen は、Win32/GetCodec.AなどのGetCodecの亜種による感染を支援するダウンローダです。

Autorun機能を悪用するマルウェア

コンピュータの攻撃手段としてautorun.infファイルを使用するさまざまなマルウェアは、ESET製品ではINF/Autorunと総称されています。autorun.infファイルには、USBフラッシュドライブなどのリムーバブルメディアをWindows PCに挿入した時に自動実行するプログラムについての情報が記述されています。

WindowsのAutorunは、リムーバブルメディアをコンピュータに挿入したとき、autorun.infファイルに記述されているプログラムを自動実行するようにデフォルト設定されています。そのため多くのマルウェアが、自分自身をリムーバブルストレージデバイスにコピーする機能を備えるようになっています。メインの拡散手段ではないにしても、ひと手間かけて追加の感染機能をプログラムに組み込むことで、感染の可能性を少しでも高めようと考えるマルウェア作者が増えた結果、多くのマルウェアファミリーがAutorunを悪用するルーチンを備えるようになったのです。

ヒューリスティック技術では、この特徴を手がかりにすることでこの種のマルウェアを容易に検出することができますが、ESETのRandy Abramsがブログ[8]で指摘しているように、アンチウイルススキャナに頼るよりもAutorun機能をデフォルトで無効にしてしまうほうがより安全です。

モバイルデバイスを狙う脅威

2009年は、コンセプト実証のための攻撃やモバイル用ブラウザを悪用する攻撃を含め、モバイルデバイスに対する脅威が目に見えて増加すると予想されます[9]。ESETのWindows Mobile用スキャナ[10]はすでに高い評価を得ており、今後はほかのモバイルプラットフォーム用の製品も投入していく予定です。モバイルプラットフォームに対する攻撃は、今後1～2年のうちに、コンピュータに対する攻撃として中心的なものになっていくと考えられます。

アドウェア（MyWebSearch、Virtumondeなど）

2008年を通じて最も多く月間ランキングに登場したPUAの1つとして、Win32/Toolbar.MyWebSearchが挙げられます。Toolbar.MywebSearchは、検索の際にMyWebSearch.comを経由させる機能を備え、ツールバーとしてインストールされます。アンチマルウェアベンダーは、PUAを完全なマルウェアとして扱うことには消極的であり、スキャナではPUAの検出がデフォルトでオフに設定されていることが少なくありません。ベンダー各社がPUAの検出に消極的なのは、一部のアドウェアやスパイウェアは、ユーザーにとって好ましくない動作をする可能性がある場合でも、合法と見なされることがあるためです（特に、使用許諾契約書であるEULAにごく小さな文字で書かれている場合を含め、そのことを表明している場合）。したがって、アドウェアやスパイウェアの被害に遭わないためには、小さい文字であろうともEULAに目を通すことが重要となります。アドウェアに代表されるPUAは、2009年も引き続き大量に検出されることが予想されます。PUAはその動作の詳細を明らかにしていないことが多く、ホストシステムを改変することやアンインストールが困難であることが伏せられている場合が少なくありません。

Virtumondeをはじめとするトロイの木馬型アドウェアは、あまりにも多くの広告コンテンツを表示するため、そのシステムで本来の作業を行うことをほとんど不可能にしてしまう場合があります。したがってユーザーは、EULAに同意する前に、プログラムがそのような振る舞いをするかどうかを確認する必要があります。また、この種のプログラムをインストールすることで、EULAに明記されていない追加のコンポーネントやアプリケーションがインストールされる可能性があることにも注意が必要です。

Win32/PSW.OnLineGames

Win32/PSW.OnLineGamesは、キーロガー機能を備えたトロイの木馬ファミリー（rootkit機能を備える場合もある）で、オンラインゲームとそのユーザーアカウントに関する情報を収集してリモートの攻撃者に送信します。攻撃者は、これらの情報を利用してゲーム内で使われる仮想資産（アイテムやアバターなど）を盗み出し、現実世界で転売します。

「Lineage」や「World of Warcraft」といったMMORPG（多人数同時参加型オンラインロールプレイングゲーム）、あるいは「Second Life」などの仮想空間を利用するユーザーは、そこでどのような脅威に直面する可能性があるかについても認識しておく必要があります。この種のゲームや仮想空間では、単なる嫌がらせや無意味な疑似ウイルス攻撃（Second Lifeに出現したGrey Gooなど）だけでなく、現実世界での金銭的被害を引き起こすフィッシングなどの詐欺行為にも注意しなければなりません。オンラインゲームの仮想資産やユーザーアカウント、通貨は現実世界で売ることができるという認識が犯罪者の間に広まったことで、オンラインゲーム関連の機密情報を漏えいさせたり盗み出したりするマルウェアが激増しました。これらの情報の入手は、ソーシャルエンジニアリングや悪意あるソフトウェア（キーロガーやバックドアなど）、あるいはその両方の組み合わせによって行われます。この種の脅威は、2008年9月度に検出数が爆発的に増加したあと「市場シェア」が低下傾向にありますが、依然として大量に検出されていることに変わりはなく、ゲームユーザーは引き続き警戒が必要です[11]。特定の難読化手法を用いる悪意あるファイルは、ESET製品ではWin32/Pacex.genと総称されています。「.Gen」という接尾辞は、「汎用的な」という意味の「generic」を表しており、この名称は既知の多くの亜種に使用されます。また、特徴が類似する未知の亜種に対して使用されることもあります。この種の難読化手法は主に、パスワードを盗み出すトロイの木馬で使用されているため、オンラインゲームユーザーを狙った脅威も、PSW.OnLineGamesではなくPacexとして検出される場合があります。

Win32/Agent

Win32/Agentというのは、感染先のコンピュータからユーザー情報を盗み出す各種マルウェアの総称です。通常、このマルウェアは自身を一時フォルダにコピーし、このファイル（または、ほかのシステムフォルダにランダムに作成されたファイル）を指すレジストリキーを追加して、システムが起動するたびにこのプロセスが実行されるようにします。このような動作をするマルウェアは全マルウェア中のかなりの部分を占めていますが、ESET製品はこれらのマルウェアを必ずしも特定の名称で検出しません。ESET製品では、マルウェア固有のシグネチャ、汎用シグネチャ、そして広範なヒューリスティックアルゴリズムという複数の方法でマルウェアが検出されるからです。このため、よく似た特徴を持つマルウェアがまったく異なる名前で検出される場合がありますが、ESETでは、複数のヒューリスティックアルゴリズムを用いることで実現される高い検出性能は、名前の問題によって生じる混乱を補ってあまりあるメリットをもたらすと考えています。先日開催されたカンファレンスにおいても、わたしたちは「悪意あるソフトウェアやその亜種はそれぞれ固有の名前で検出するべきだとする考え方は脅威の現状にそぐわなくなっている。重要なのは、マルウェアの名前ではなくそれらを効果的に検出できるかどうかがである」と主張する論文を発表しています[12]。

Win32/Conficker

Win32/Confickerは、先ごろ発見されたWindowsオペレーティングシステムの脆弱性を悪用して感染を広げるネットワークワームで、2008年後半から大量に検出されています。この脆弱性はRPCサブシステムに存在し、攻撃者によってリモートから悪用される可能性があります。この攻撃は、有効なユーザーアカウントがなくても実行可能です。Confickerは、FakeAlertやWigonなどのアドウェアファミリーに関係があると思われるマルウェアをダウンロードしようとします。また、Windowsファイアウォールを終了し、ランダムなポートでhttpサーバーを稼働させようとします。

ESETの製品はすでにConfickerに対応していますが、同じ脆弱性を突く別のマルウェアに感染するのを防ぐため、Microsoftが10月末に公開したパッチも必ず適用するようにしてください。この脆弱性の詳細については、http://www.microsoft.com/technet/securityをご覧ください。

表3：2009年に予測される脅威から身を守る10の方法

●	WindowsのAutorun機能を無効にする：WindowsのAutorun機能は、ESET製品でINF/Autorunとして検出されるマルウェアやその他多くの脅威によって広く悪用されています[8]。
●	アプリケーションとオペレーティングシステムのコンポーネントを常に最新の状態に維持する：そのためには、アップデートとパッチの適用を自動的に行い、各製品の更新情報をベンダーのWebサイトで定期的に確認する必要があります。多くのユーザーは、オペレーティングシステムや各種ソフトウェアの脆弱性問題があるのはMicrosoft製品だけだと考えがちですが、このような考え方が不適切なのは、前週に発見された重大な脆弱性とそれらに対する攻撃についての情報が週に一度掲載されるSANSの「Consensus Security Vulnerability Alert」（http://portal.sans.org）を見れば明らかです。Microsoftの定例パッチ公開日（「Patch Tuesday」）がある週でさえ、ベンダー各社が提供するアプリケーションに驚くほど多くの問題が見つかっています。「Consensus Security Vulnerability Alert」は、すべてのシステム管理者にとって必見のリソースです。
●	コンピュータにログオンする際は、どうしても必要な場合を除き、管理者権限を持たないアカウントを使用する：これにより、マルウェアが自動インストールされる可能性とその被害を小さくすることができます。マルチユーザーに対応しているオペレーティングシステム（現在のほとんどのオペレーティングシステムは、複数のユーザーが複数の権限レベルでマシンを使用できるように考慮されています）では、管理者アカウントよりも権限が制限された日常使用のためのアカウントを作成することが可能です。優秀なシステム管理者は、ユーザーの持つ権限が大きいほど被害も大きくなるという「最小権限の原則」を理解しており、特定の作業を行うために必要なときにだけ特権アカウントを使うようにしています。
●	コンピュータと各種オンラインサービスのパスワードを同じものにしない：パスワードを定期的に変更し、簡単なパスワード（特に推測が容易なもの）を使わないようにすることも重要ですが、覚えにくいパスワードを頻繁に変更することを強制した場合、パスワードをメモした付箋をディスプレイに貼り付けるなどの行為が増える可能性があるため、このような規則が常に有益かどうかは議論が分かれるところです。しかし、サービスごとに異なるパスワードを使用することは、被害の拡大抑止に大きな効果があります。

●	心当たりのないファイルやリンクが送られてきた場合、たとえ友人からのものであっても信用しない：メールアドレスを詐称したり有害なリンクを無害なものに見せかけたりすることは容易に行えます。フィッシングメールなどで行われるこの種のリンクの偽装は、Webブラウザの改良などによって比較的簡単に見破れるようになっていますが、基本的な対策すら行っていないユーザーは依然として数多く存在します。
●	FacebookやLinkedInなどのサイトでむやみに情報を公開しない：特に問題がないと思われる情報でも、ほかの情報と組み合わせてソーシャルエンジニアリング攻撃に使用される場合があります。
●	機密情報をハードディスクに保存する場合は、暗号化したうえで定期的に別のディスク（可能な場合は遠隔地の施設）にバックアップする：またサーバーにデータを保存する場合は、サーバー自体をバックアップすることを忘れないようにする必要があります。
●	セキュリティをアンチウイルスソフトウェアだけに依存しない：アンチウイルスソフトウェアだけでなく、パーソナルファイアウォールやアンチスパムソフトウェア、アンチフィッシングツールバーといった追加のセキュリティ対策も導入する必要がありますが、最近では偽のセキュリティソフトウェアが登場してきていることにも注意が必要です。とはいえ、最良のセキュリティ対策を講じ、用心深く、良識を持って行動したとしても、それですべての脅威に確実に対処できるとはかぎりません。わたしたちが常日頃から多層防御の重要性を提唱しているのは、マルウェア対策に特効薬など存在しないからです。またマルウェア作者は、特定のスキャナによる検出を免れるべく、バイナリを工夫することに多大な時間を費やしているということも認識しておく必要があります。スキャナが優秀であればあるほど、そのスキャナ対策が行われる可能性が高くなります。もちろん、ESETとしてもそのようなトリックの研究と検出性能の向上に注力していますが、そのような強化が行われる前にマルウェアがユーザーのコンピュータに侵入してしまう可能性は否定できません。もしESETの製品で検出できないマルウェアが見つかった場合（あるいは誤検出が生じた場合）は、ESET Smart Security & ESET NOD32アンチウイルス　サポートセンターにご連絡ください。お問い合わせ窓口は、http://canon-its.jp/product/eset/supp.htmlをご覧ください。
●	むやみに無料の無線アクセスポイントに接続しない：無料のアクセスポイントは、DNSクエリを改ざんしたり、正規のアクセスポイントを装った偽のアクセスポイント（「Evil Twin」）であったりする可能性があります。このようなアクセスポイントに接続すると、ログイン情報や通信の内容を盗聴される恐れがあります。
●	クラックされたソフトウェアや海賊版のソフトウェアを使用しない：このようなソフトウェアは、マルウェアやシステムの脆弱性を突く攻撃の侵入口に利用される可能性があります。また、違法なP2Pネットワークで流通している著作権のある音楽ファイルや動画ファイルについても注意が必要です。これらのファイルは、マルウェアの配布に利用するために偽装あるいは改ざんされている場合があります。

上記の内容は、ESET Threatblog（http://www.eset.com/threat-center/blog/）に掲載された一連の記事に加筆したものです。

表4：エンドポイントセキュリティに関して予測される10の傾向

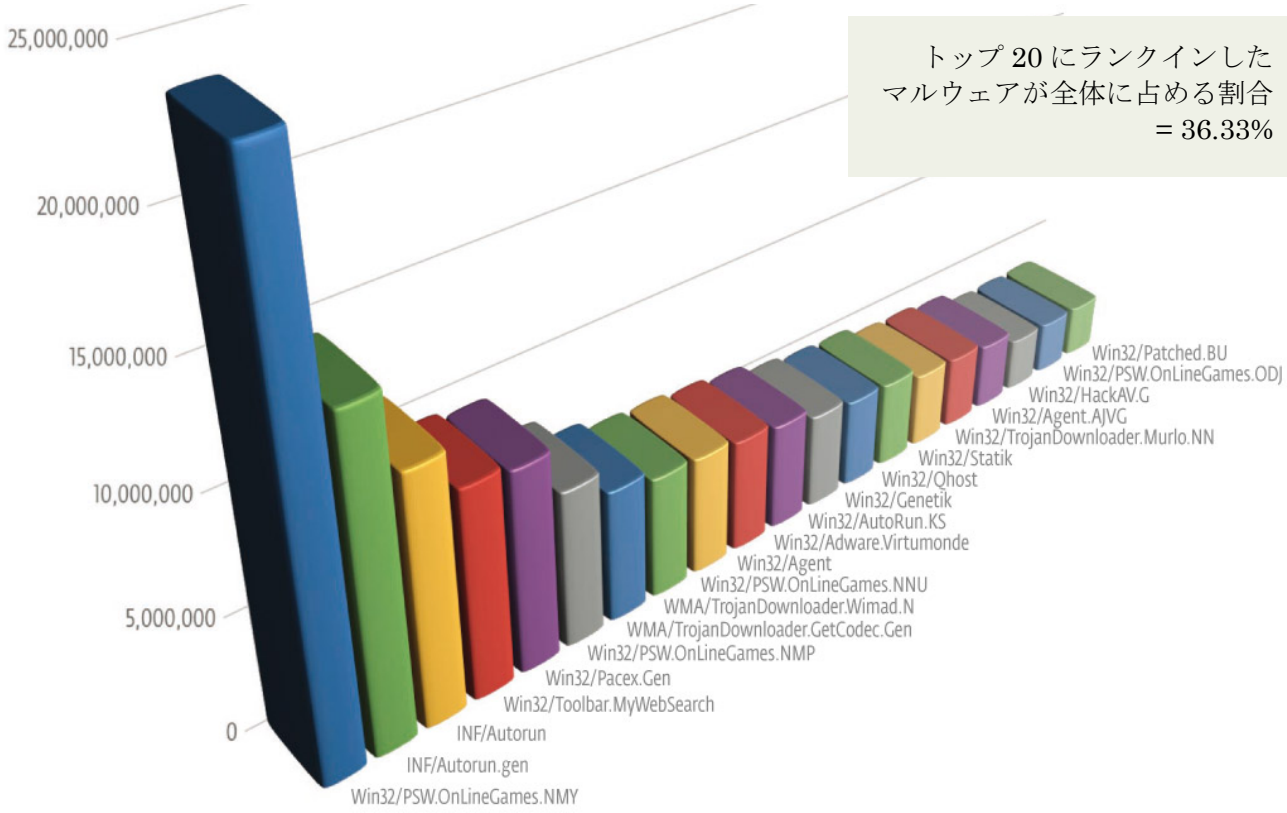
●	より多くの製品がヒューリスティック分析などのプロアクティブな技術を採用し始める（あるいは発明したと主張する）：ESETでは引き続き、プロアクティブな技術の開発と強化を進め、新種の脅威にも対処できるよう同技術の対応範囲を広げていきます。
●	セキュリティソフトウェアがメモリなどのシステムリソースに与える影響を軽減するための取り組みが引き続き行われる：具体的な方法としては、より汎用的なアプローチでマルウェアをフィルタリングしたり、処理をサーバー側で行ったりといったことが考えられます。
●	業界の再編・統合がさらに広がる（純粋なアンチウイルスベンダーが減少し、アンチマルウェアの複数の機能を搭載した統合型の製品が増加する）：また、Macやモバイルデバイスなどがマルウェア作者に狙われる機会が増えることに伴い、多くのベンダーがこれらの非主流プラットフォーム向けの製品を提供し始めると予想されます。
●	AMTSO（Anti-Malware Testing Standards Organization）の活動が活発化し、より多くの啓発資料が提供されるのに伴い、アンチマルウェアテスト問題に対する認識が高まる：動的なテストの重要性が増し、普及が広まる一方、大きなサンプルセットに対して動的なテストを実施する際のリソース問題がネックとなり、期待されるほどの影響を及ぼすまでには至らないと予想されます。ただし、適切でないテスト手法を正当化することは困難となり、各テスト機関には、そのテスト内容と結果報告の質についてより大きな説明責任が求められることになるでしょう。
●	従来型アンチウイルスの終焉と、それに変わる手段としてのクラウドコンピューティングおよびホワイトリスト方式によるアンチマルウェアが誇大に取り上げられるようになる：これらの技術が広く使われることによってアンチマルウェアのあり方が変化し、検出率の向上やシステムリソースに対する負荷の軽減といったメリットが生まれてくると予想されます。ただし、一部で喧伝されているように、それがマルウェアに対する完全なる解決策になるとは考えられません。誤検知の問題を含め、サンプルの妥当性や処理方法に関する課題は、これらの技術によって解決されるものではないということが徐々に理解されていきます。また、すでに実績のある技術にまったく新しい名前を付け、怪しげな特許を取得した派生的な技術が数多く登場してくると予想されます。
●	アンチウイルスベンダー間の協業が活発になる：このような協業は、研究者レベルではこれまでも行われてきましたが、公式な形、例えば最も大きな成果であるAMTSOのような形で行われることは必ずしもありませんでした。
●	情報漏えい防止対策が大きく注目されるようになる：情報漏えい防止対策はこれまであまり普及が進んでいませんでしたが、政治的、社会的な機密データが漏えいした大規模なセキュリティ侵害事件が英国などで発生したことを受けて、ハードウェアやソフトウェアによる情報漏えい防止ソリューションに大きな関心が寄せられるようになっています。
●	サイバー犯罪を取り締まる法律の強化や、政府と民間セキュリティ企業の連携強化を求める声が強まる：これは、厳密にはエンドポイントセキュリティに関する問題ではありませんが、このような動きが起きてくると予想されます。多くの人々は、このような活動によってあらゆる問題が排除されることを期待していますが、多くの取り組みと同様、現実的にそこまでの効果が得られることはないでしょう。

●	エンドポイントデータの保護は、暗号化と侵入防御の双方を相互補完的に用いて行うのが効果的であるとの認識が広まる：セキュリティの世界では長い間、暗号化技術を用いてリスクを軽減するデータ中心的なアプローチと、脅威の侵入を防ぐことで悪意のあるコードを排除するというアプローチの分断が続いていましたが、これらの技術は相互排他的ではなく相互補完的なものであるとの理解が広がっていくでしょう。
●	テクノロジーの進化がセキュリティの進化をはるかに上回る速さで進む：2009年は、セキュリティ企業がエンドポイントセキュリティの革新と刷新を迫られる重要な年になると予想されます。サイバー犯罪者がセキュリティベンダーとの差を広げることになれば、2009年はセキュリティの歴史上、大きな転換点になるでしょう。

ThreatSense.Net による年間マルウェアランキング

図1は、ThreatSense.Netによってレポートされた脅威を分析して得られたマルウェア検出数の年間ランキングです。各マルウェアは、その名称での検出数に基づいてランキングされています。注意が必要なのは、これらの名称はあくまでも検出名であり、必ずしも（あるいは多くの場合）特定のマルウェアファミリーを指しているわけではないということです。マルウェアファミリーのメンバーは、ヒューリスティックアルゴリズムで検出されている場合も、マルウェア固有のシグネチャで検出されている場合も、汎用シグネチャで検出されている場合もあるため、このランキングは、2008年に流通したマルウェアファミリーの実数を正確に反映していない場合があります。

図1：2008年の個別マルウェア検出数トップ20

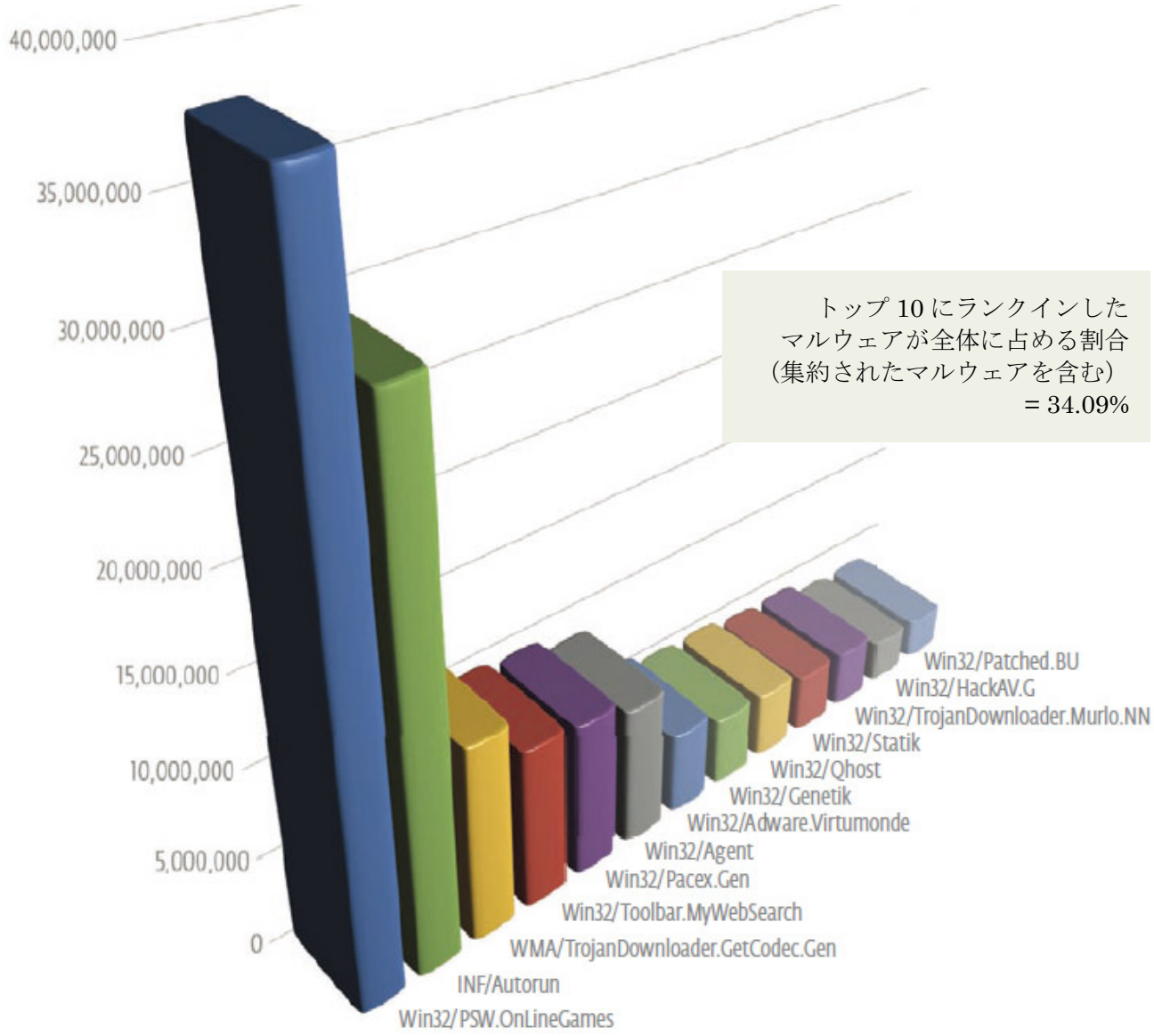


トップ20の中にはよく似た名前を持つマルウェアがいくつもありますが、これらは互いに深い関係にあるマルウェアファミリーであることを示しています。ESETは2008年より、全体的な傾向を把握しやすくするために、これらの深い関係にあるマルウェアの検出データを1つに集約する作業を始めています。

例えば、ThreatSenseの月間レポートでは、Win32/PSW.OnLineGamesのすべてのメンバーが1つの名称に集約されています。

表5（P.21）はこの方針に基づいて集計されており、オンラインゲームのパスワードを盗み出すマルウェアは基本的に1つの名称に集約されています。Win32/AgentとINF/Autorunについても同様です。以前にWMA/TrojanDownloader.Wimad.Nという名称で検出されていたマルウェアは、現在ではより汎用的なWMA/TrojanDownloader.GetCodec.Genという名称に集約されており、これによって全体的な傾向がわかりやすくなっています。

図2：2008年のタイプ別マルウェア検出数



上記のマルウェアは、さらに集約することが可能です。例えばPacex.genというのは、オンラインゲームのパスワードを盗み出すマルウェアで多く見られる難読化手法を用いるマルウェアを示しており、傾向分析という目的であれば、Win32/StatikやWin32/Genetikなど、アドバンスドヒューリスティックアルゴリズムで検出されるマルウェアもこのPacex.genに集約することができます。ただしここでは、月間レポートで現在使用しているものと同じ集計方法を用いています。

このデータからは、次のようなことが見て取れます。
オンラインゲームのパスワードを盗み出すマルウェアは、Pacex.genを加えなくても、年間を通じて最も多く検出されている：オンラインゲームのユーザーは、自分たちがマルウェア作者の最大の標的になっているということを認識する必要があります。

感染経路としてWindowsのAutorun機能を使用するマルウェア（ここには非常に幅広いマルウェアが含まれる）は、オンラインゲームのパスワードを盗み出すトロイの木馬に次ぐ僅差の第2位となっている：このマルウェアは、2008年の最終月をランキングの第1位で締めくくっているほか、2007年もしくはそれ以前から何度も第1位になっています。Autorunは悪意のない世界では便利な機能かもしれませんが、わたしたちの住むこの世界では、ほとんどの場合無効にしておくことが推奨されます。

非常に幅広いアドウェアが汎用名で検出される中、Win32/Toolbar.MyWebSearchとVirtumondeのさまざまな亜種がトップ10にランクインしている：このことは、アドウェアという問題がいかに大きいかを示しています。とりわけVirtumondeは、さまざまな点で大きな問題となっています。Virtumondeがインストールされたコンピュータはほとんど使用不可能な状態になるうえ、これを自動的に駆除することは難しく、その作業はしばしば危険を伴います。また、パッケージングの方法が定期的に変更されるため、プロアクティブな検出性能にすぐれる製品でも、変更直後は汎用シグネチャやヒューリスティックで検出することが困難となります。

ダウンローダのGetCodecとそれに関連する脅威は引き続き大きな勢力を保っている：このことは、「このコンテンツを再生するにはここをクリックしてプログラムをインストールしてください」といったメッセージを表示するソーシャルエンジニアリングの手法が依然として有効であることを示しています。

トロイの木馬ファミリーであるWin32/Agentが長期的にランクインし続けている：これは、コンピュータに侵入してデータを盗み出すことがマルウェア作者の首尾一貫した動機の1つであるということを示しています。ユーザーは、（1）同じような目的を持つマルウェアはWin32/Agentという名称以外にも数多く存在する、（2）悪意あるエージェントに侵入された場合、そのエージェントが侵入口となってデータ盗難以外にもさまざまな不正行為が行われる可能性がある、という点にも注意する必要があります。

アドバンスドヒューリスティックで検出されるINF/Autorun、Win32/Statik、Win32/Genetikがトップ10に継続的にランクインしている：これは、既知のマルウェアには似ておらず既存のシグネチャでは対応できない新種マルウェアをも検出できる高度なヒューリスティック技術がかつてないほど重要となっている、ということを示しています。

Virus Radar の傾向

「Virus Radar Online」は、電子メールの添付ファイル経由で拡散しているマルウェアを監視、統計分析するためにESETがパートナー企業とともに開始したプロジェクトです。電子メール経由で拡散するマルウェアは、減少傾向にあるとはいえ依然として活発に活動しており、またマルウェア全般を対象とするThreatSense.Netによる観察結果とは違う傾向を示すことから、この種のマルウェアを詳細に監視することには現在も大きな意味があります。電子メールを感染経路とするマルウェアで最も多く用いられるのは、悪意のあるURLへのリンクを本文に記述するという手法ですが、この種の手法を用いるマルウェアはVirus Radarの統計には含まれていません。Virus Radarはあくまでも、ESETのアンチマルウェア製品でスキャンされた電子メールの実際のコンテンツ（添付ファイルなど）を分析することを目的としているからです。またVirus Radarは、電子メール本文で参照されているWebページのコンテンツの検証やレポートは行いません。これらを検証して得られる統計データは、その多大な処理負荷に値するほどの価値はないと考えられるためです。もちろんこれは、ESETが悪意あるWebサイトの追跡を行っていないという意味ではありません。ESETのラボでは、Webサイトにホストされているマルウェアの調査に膨大な時間と労力を費やしています。ただしこれらの情報は、現在のところ統計データの集計には使用されていません。

表5：2008年にVirus Radarで検出された悪意のある添付ファイルトップ10

順位	マルウェアの名称	件数
1	Win32/Zafi .B worm	1,865,121
2	Win32/Netsky.Q worm	1,852,664
3	a variant of Win32/Stration.XW worm	889,098
4	HTML/Phishing.gen trojan	324,109
5	Win32/Stration.XW worm	305,948
6	Win32/Spy.Goldun.NDO trojan	123,399
7	Win32/Netsky.D worm	115,351
8	Win32/Bagle.HE worm	84,725
9	Win32/Mytob.BK worm	76,868
10	Win32/AutoRun.FakeAlert.S worm	68,625

2008年の中間レポートでわたしたちは、「2007年と比べ、悪意のあるソフトウェアの直接的な拡散手段として電子メールを用いるケースは大幅に減少している一方、スパムメールに悪意のあるURLを記述するケースは非常に多くなっている」と指摘しました。ThreatSense.Netの2008年の統計では、ヒューリスティックによって検出されたマルウェアが全体のかなりの部分を占めていますが、Virus Radarの同時期の統計では、ヒューリスティックによって検出された新種のマルウェアおよび亜種はごく少数に留まっています。このことから悪意のある添付ファイルは、2008年後半に検出数が何度か激増して話題になったものの（複数のレポートによると、悪意のある添付ファイルは、2008年の第3四半期と第4四半期に、同年前半と比較して500%も増加しています）、電子メールに記載される悪意のあるURLとは対照的に、動きが活発なマルウェア配信グループではあまり使用されていないと見なすことができます。

NetskyやMytob、Bagleといった古くから存在する大量メール送信マルウェアは、2008年も大量に検出されました。ただしこの種のマルウェアは、Virus Radarのトップ10では引き続き勢力を保っているものの、全体的な検出数は2008年後半から減少し始めています。これは、セキュリティ意識が高まり、適切なセキュリティ対策を導入するユーザーが増えたことを示している可能性もありますが、実際にはもっと複雑な理由があると思われます。とはいえ、簡単なスキャナやWebベースのスキャナがホームユーザー向けに無償提供されるようになり、これらを利用するユーザーが増えたという要因があることは確かでしょう。

ランキングに登場したマルウェアの中で特に興味深いのは、Win32/AutoRun.FakeAlert.Sワームです。このワームは、11月に突如として大発生したあと（全体の0.025%以上にあたる約7万件）、数日のうちに再び姿を消しました。Virus Radarが捕捉したこのワームのサンプルは、6万8,625件に上ります。Win32/AutoRun.FakeAlert.Sは、WindowsのAutorun機能を悪用して増殖する偽のセキュリティアプリケーションです。

2007年、Stormボットネットの黎明期に登場したような、電子メール経由で広まるStorm関連のマルウェア（Fuclip、Nuwar）は、2008年にはそれほど多く検出されていません。このことから、Stormを拡散させていたグループは、2008年後半にStormボットネットの活動が沈静化し始めるはるか前から、その拡散手段として電子メールの添付ファイルを使うことをやめていたと考えられます。

図1のトップ10にランクインしたマルウェアは、2008年にVirus Radarで検出されたマルウェア全体の大部分を占めており、11位以下のマルウェアは合計しても59万1,298件に過ぎません。この事実は、新種の脅威に対するESETのプロアクティブな検出技術（既知の脅威との類似性に基づいて検出を行う汎用シグネチャと、まったく新しいマルウェアや亜種を検出する高度なヒューリスティック技術）が、引き続き極めて有効に機能していることを改めて示すものといえます。

図3：2008年の悪意ある添付ファイル検出数トップ10

Current Threats - Last 12 Months Analysis

Top 10 threats

Shows recent e-mail virus threats in the last 12 months

Time interval: Day | Week | Month | Year

Top 10 threats

All detected viruses

Virus	Count	Infection Ratio (%)	Infection Ratio
01. Win32/Zafi.B worm	1 920 732	0.055 %	1/ 1.8 ths
02. Win32/Netsky.Q worm	1 586 294	0.045 %	1/ 2.2 ths
03. a variant of Win32/Stration.XW worm	718 736	0.020 %	1/ 4.9 ths
04. HTML/Phishing.gen trojan	324 108	0.009 %	1/ 10.8 ths
05. Win32/Stration.XW worm	305 919	0.009 %	1/ 11.5 ths
06. Win32/Spy.Goldun.NDO trojan	123 399	0.004 %	1/ 28.4 ths
07. Win32/Netsky.D worm	103 077	0.003 %	1/ 34.0 ths
08. Win32/Bagle.HE worm	80 531	0.002 %	1/ 43.6 ths
09. Win32/AutoRun.FakeAlert.S worm	68 625	0.002 %	1/ 51.1 ths
10. a variant of Win32/Kryptik.BD trojan	68 265	0.002 %	1/ 51.4 ths
> OTHER VIRUSES	551 753	0.016 %	1/ 6.4 ths
> TOTAL THREATS	**5.9 mil**	**0.167 %**	**1/ 599.5**
Total clean messages	**3502.2 mil**		
Total messages	**3508.0 mil**		

To see the virus infection progress click on the desired virus name.

Report Summary

Report: Current Threats - Last 12 Months Analysis
Description: Shows recent e-mail virus threats in the last 12 months
Interval: Last 12 months (from 2008-02-1 00:00:00 to 2009-01-08 01:59:59)
Generated: 2009-01-08 01:59:59 +0100 (2009-01-08 00:59:59 UTC)
Note: All times and dates are in local time (CET).

ESET ThreatSenseラボのVirus Radarレポートのスクリーンショット

電子メール関連の迷惑行為

悪意のある添付ファイルやリンクは、エンドユーザーにとって引き続き大きな脅威となっています。この種の攻撃は、適切なセキュリティソフトウェアを使用することである程度防ぐことができますが、電子メール関連で注意すべきなのは添付ファイルやリンクだけではありません。

表6：電子メール関連の迷惑行為トップ10

●	フィッシング	銀行などの金融機関からオンラインで何らかの手続きを行うよう求める電子メールを受け取った場合は、手続きを行う前に、メールが本物かどうかをその金融機関に直接問い合わせることを推奨します。リンクの実際のジャンプ先は、容易に隠ぺいできることに注意してください。また、宛名が自分の名前や口座名義ではなく「お客様各位」などとなっている場合は特に用心する必要があります。
●	「運び屋」募集	フィッシング詐欺で実際に金銭を得るためには、資金移動や資金洗浄を行う者が必要になります。そこでフィッシング詐欺師たちは、金銭の受け渡しや物品の代理購入（この物品はのちに転売される）といった「仕事」を提供するといって求人を行い、「金銭の運び屋」をやらせようとします。
●	株関連の詐欺	ペニー株（投機的低位株）詐欺や株価操作などの株関連の詐欺では、「有望株」の購入を持ちかけてそれを高値で売り抜けるといった行為が行われます。多くの場合、その株価は急落し、株購入者と当該企業に経済的な損害がもたらされます。
●	419詐欺	典型的な419詐欺では、「暗殺された権力者の資産から謝礼を出すので、銀行口座を貸してほしい/投資先を紹介してほしい」などと持ちかけ、当座の費用として前渡し金を要求するソーシャルエンジニアリングの手法が用いられます。過去の419詐欺の多くは、その紋切り型の言葉遣いからすぐに見破ることができましたが、継続的に文章の内容や書き方を工夫しているグループも存在します。
●	その他の前渡し金詐欺（Advance Fee Fraud：AFF）	前渡し金詐欺のバリエーションとしては、求人詐欺や宝くじ詐欺などがあります。この種の詐欺では、求人に応募するため、あるいは当選金を受け取るためには、前渡し金を支払う必要があるなどと要求されます。
●	デマウイルス/チェーンメール	デマウイルスを見かけることは少なくなりましたが、電子メールを転送させて偽の情報を広めようとするチェーンメールは今でも健在です。友人や同僚に転送するよう求める電子メールは、どのようなものであっても決して信用してはなりません。

●	猛威をふるうスパムメール	ここに挙げたいずれの分類にも当てはまらないスパムメールも、そのほとんどは何らかの詐欺的要素を含んでいます。スパマーは、自らの身元やメールの送信元を偽り、「あなたが希望したからこのメールを送っている」「送金したら品物を送る」などと嘘をつきます。しかもほとんどのスパムメールは、所有者も気付かないうちにボットに感染したコンピュータから送信されているのです。
●	従来型の 大量メール送信マルウェア	大量メール送信マルウェアは、新種はそれほど多く登場していないものの、比較的古い亜種がセキュリティ対策の不十分なコンピュータから大量に拡散し続けています。中には、適切に対策が講じられているはずの大規模サイトが踏み台にされているケースもあります。
●	スパム関連の迷惑行為	スパム関連の迷惑行為としては、有効なメールアドレスを確認するために、自動生成した大量のアドレス宛てに電子メールを送信するDHA（Directory Harvesting Attack）や、偽装されたアドレスからの電子メールに対して自動返信されるメールが実際の送信者でないアドレス宛てに送られるBackscatterが挙げられます。特に後者では、実際の送信者でない人物の元にスパムメールに対する自動返信が送られるため、受け取った側は大きなフラストレーションを感じることになります。
●	ネズミ講	ネズミ講とは、「うまい儲け話（Make Money Fast : MMF）」があると多くの人を参加させながら、実際には早い時期に参加した人たちだけしか利益を得られないような仕組みのことをいいます。

参考文献

1. “Interpreting Threat Data from the Cloud”: David Harley

2. “The Passing Storm”: Pierre-Marc Bureau, David Harley, Andrew Lee and Cristian Borghello

3. ESET Global Threat Trends report for November 2008: http://www.eset.com/threat-center/threat_trends/Global_Threat_Trends_November_2008.pdf （日本語版: http://canon-its.jp/product/eset/topics/malware0811.html）

4. CARO Workshop 2008, http://www.datasecurity-event.com/downloads.html

5. “Malicious Macs: Malware and the Mac” by David Harley, in “OS X Exploits and Defense”, Syngress 2007.

6. “Net of the Living Dead: Bots, Botnets and Zombies” by David Harley and Andrew Lee: http://www.eset.com/download/whitepapers/NetLivingDead(20080225).pdf

7. “‘Wicked Rose’and the NCPH Hacking Group” by Ken Dunham and Jim Melnick, in Chapter 5 of “The AVIEN Malware Defense Guide for the Enterprise” (Ed. Harley), Syngress 2007.

8. “Auto-infect” by Randy Abrams, at http://www.eset.com/threat-center/blog/?p=94

9. “Smarter Smart Phones” by Randy Abrams, at http://www.eset.com/threat-center/blog/?p=250

10. http://www.eset.com/products/mobileantivirus.php

11. “Playing Dirty” by Cristian Borghello

12. “A Dose By Any Other Name” by Pierre-Marc Bureau & David Harley （2008年の第18回Virus Bulletinインターナショナルカンファレンス紀要より）

付録:ESET と ThreatSense について

ESET社について

1992年に設立されたESETは、企業およびコンシューマ向けのセキュリティソフトウェアを提供する世界的な企業です。数々の賞を受賞しているESETのアンチマルウェアソフトウェアシステム、ESET NOD32アンチウイルスは、既知および未知のウイルス、スパイウェア、rootkitといった各種マルウェアに対するリアルタイムの保護機能を提供します。ESET NOD32アンチウイルスは、最もコンパクトかつ最速・最新の保護テクノロジーを搭載しており、数あるアンチウイルス製品の中で最多のVirus Bulletin 100%アワード受賞回数を誇ります。ESETは過去5年連続でDeloitteの「Technology Fast 500」に選ばれており、Canon、Dell、Microsoftといった企業と広範なパートナー契約を結んでいます。ESETは、スロバキアのブラチスラバ、アルゼンチンのブエノスアイレス、チェコのプラハ、米国カリフォルニア州サンディエゴに事業所を置き、世界の160か国以上で事業を展開しています。
詳しくは、http://www.eset.comをご覧ください。

ESET NOD32アンチウイルスとESET Smart Securityについて

ESET NOD32アンチウイルスは、単なるアンチウイルスソフトウェアではありません。同製品は統合アンチマルウェアシステムであり、ウイルス、スパイウェア、アドウェア、トロイの木馬、ワーム、そしてフィッシング攻撃に対する保護を提供します。プロアクティブなThreatSenseテクノロジーを搭載しており、多くのゼロデイの脅威でさえも事前にブロックすることが可能です。エンジンの最適化により、数あるアンチウイルス/アンチスパイウェア製品の中でも最高の検出性能と最速のスキャンが実現されており、システムパフォーマンスに対する影響も最小限に抑えられています。また、一元的な管理およびレポーティング機能によって柔軟な構成が可能となっています。ESET Smart Security は、これらの機能をベースに、スパムメールの検出および管理機能とパーソナルファイアウォールを追加した製品です。ESET NOD32アンチウイルスとESET Smart Securityのライセンス製品では、リモート管理、LANアップデートミラー、サーバーへのインストール機能も提供されます。
製品の全ラインナップについては、http://canon-its.jp/product/eset/をご覧ください。

ThreatSenseについて

ThreatSenseは、NOD32アンチウイルスとESET Smart Securityに搭載された先進のアンチマルウェアエンジンです。ThreatSenseは、業界最先端のヒューリスティック技術と汎用シグネチャを組み合わせることにより、包括的で高度なセキュリティを実現します。両技術のアップデートは動的かつ自動的に行われ、すべてのユーザーに無償で提供されます。クライアント側のソフトウェアは、ESETの脅威ラボからアップデートが提供されているかどうかを1時間おきに自動チェックします。

ThreatSense.Netについて

Virus radarが電子メール経由で広まる脅威だけを対象としているのに対し、ThreatSense.Netは、ユーザーのコンピュータで検出されたあらゆるタイプの脅威に関する情報を収集しています。ThreatSense.Netは、ESETのセキュリティソフトウェアのレポーティング機能を有効にしているユーザーから統計データを匿名情報として収集し、現在のマルウェアの活動および拡散状況を包括的に把握できるようにします。現在、統計データは1,000万台以上ものコンピュータから収集されており、これまでにThreatSense.Netによって確認された脅威/マルウェアのファミリーは早くも1万種類以上に上っています。

本社

ESET, spol. s.r.o.

Aupark Tower

16th Floor

Einsteinova 24

851 01 Bratislava

Slovak Republic

TEL：+421 (2) 59305311

http://www.eset.sk

販売代理店（日本）

キヤノンＩＴソリューションズ株式会社

セキュリティソリューション事業部

〒108-0073

東京都港区三田3-11-28

TEL：03-5730-7198

http://www.canon-its.jp/