Dr.WEB®
sinse 1992

アンチウイルスソフトウェアに関する誤解

Dr.WEB®
sinse 1992

アンチウイルスソフトウェアに関する誤解

現在、マルウェアのせいで被害を受けたPCやモバイル端末ユーザーが少なくありませんが、アンチウイルス開発会社がウイルスを作成する、LinuxやMacを狙うマルウェアが存在しない、あるいはユーザー自身の不注意でない限りAndroid対応端末上へのウイルス進入があり得ない、といった誤解が定着しています。実際はどうでしょうか?

固定観念に囚われて客観的データに基づく情報を把握できないと重大なトラブルを招きかねません。

一般的に流布している誤解に基づいた判断が、大きなリスクに繋がる可能性があります。この冊子では、アンチウイルスに関する誤解、誤解の根源、及びその誤解によってアンチウイルスユーザーの情報セキュリティに出ている影響などの課題を取り扱います。

誤解№ 1　「ウイルスが存在しない」

狭義でのウイルス、つまり、自己増殖メカニズムを備えた悪意のあるプログラムと、それ以外の悪意のあるプログラムを区別することが必要です。ウイルスは確かに存在しますが、現在、大量に拡散されるトロイの木馬と比較すると少ない数です。

狭義でのウイルスは、自己増殖メカニズムを備えた悪意のあるプログラムのみを言います。つまり、この悪意のあるプログラム（マルウェア）は自己コピーを作成し、他のファイルに自己コードを組み入れることができます

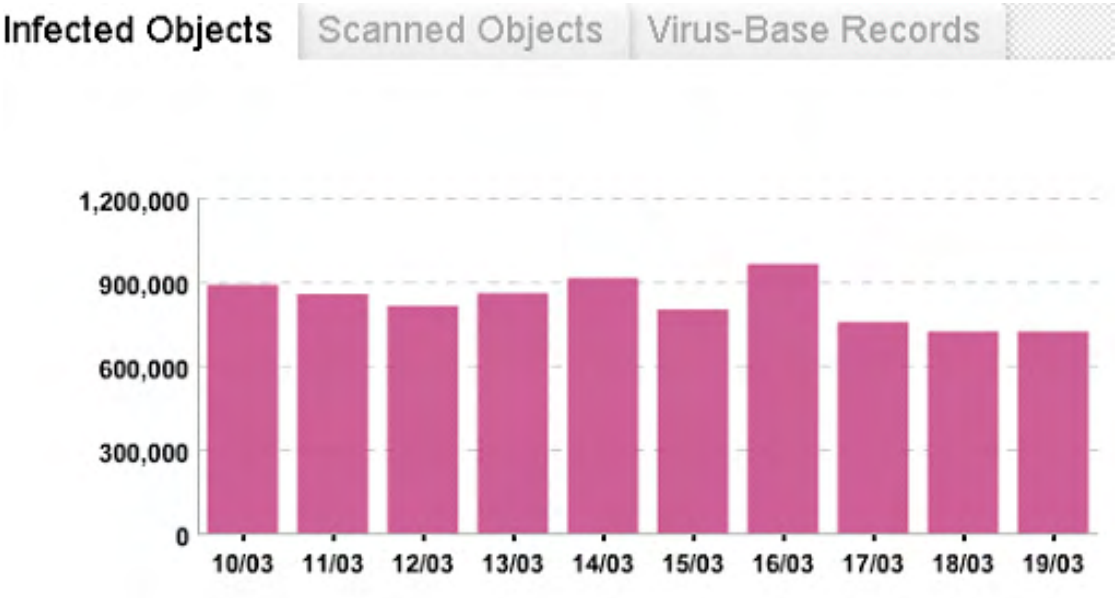
しかし、現時点ではマルウェアのうち、90%以上の割合をトロイの木馬が占めています。トロイの木馬は自己増殖メカニズムを備えておらず、狭義のウイルスにはあてはまりません。

誤解№ 2　「新しいマルウェアの出現頻度が少ない」

一日に作成されるマルウェア数がおよそ100個程度であると考えるIT専門家がいます。しかし、実際はそうではありません。

ウイルスラボに提供される潜在的危険性のある検体数が月に約2500万個となっています。

2015年3月に分析のためにDoctor Webウイルスラボに提供された検体の推移

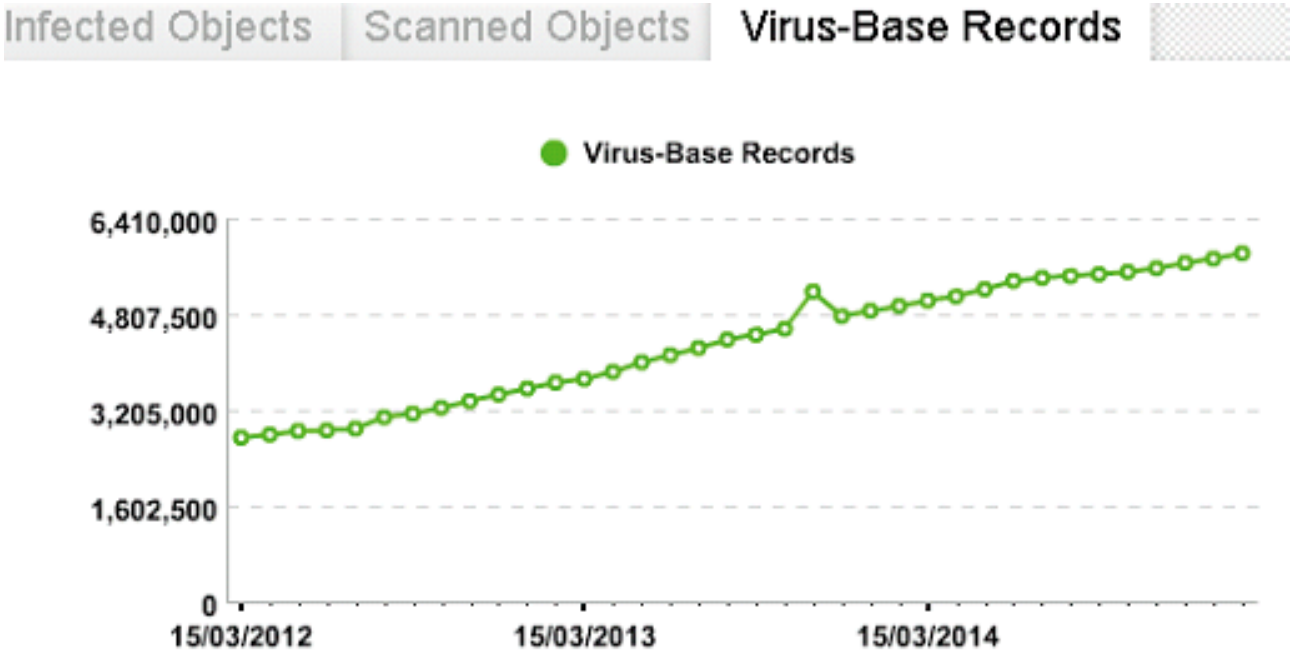


もちろん、提供された検体の中にはマルウェアではないプログラム、または繰り返しで提供される検体も含まれていますが、全ての検体は弊社スタッフによって分析されます。

月に数百万個に及ぶ検体数を手動で処理することは極めて困難な作業となります。

そのため、検体の多くは、弊社が開発した専用の解析ロボットによって処理され、自動処理が不可能な複雑な検体のみ、ウイルスアナリストに分析されることになっています。そうしてDr.Webウイルスデータベースは一時間ごとに増加しています。

Dr.Web ウイルスデータベースにおけるウイルスレコードの推移



誤解№ 3 「アンチウイルス開発会社がマルウェアを作成している」

上記のことが真実であると思うユーザーが数多くいます。ウイルスがなければアンチウイルスは販売できないから、アンチウイルス開発会社がウイルスを作成しているという考え方です。この誤解は世界的にも広く流布しています。

この誤解はアンチウイルスに関する誤解のうち、最も典型的かつ定着しつつある誤解であるといえます。弊社へのフィードバックフォームに意見を記入するユーザーには、このような誤解をしているユーザーは毎月現れています。

こうした誤解の根源として、

1. 一日に作成されるマルウェアの数が少ない、
2. マルウェアを作成するのに多数の専門家が要らない、
3. マルウェアを作成できる専門家がアンチウイルス開発会社に勤めているに違いない、

といった思い違いが挙げられます。

- 開発されるマルウェアの数は、ウイルスラボが休みなく3交代勤務シフトで分析業務をやらざるを得ないほど多いのです。分析のために提供される検体数が極めて多く、マルウェアを作成できる状況であるとは言いがたいです。
- IT情報セキュリティ専門家や企業にとってマルウェアの作成は意味のない無駄な作業になります。なぜならば、マルウェアを作成したとして、その検体は、まず勤務先のアンチウイルス会社のデータベースに追加されるため、ユーザーはマルウェア出現時にこのマルウェアから保護されることになるためです。しかも、作成されたトロイの木馬は他社アンチウイルス会社のデータベースにも加えられる可能性があります。
- マルウェアの開発は犯罪です。ウイルスアナリストに対して好意を持たない人や犯罪者が少なくないことを考慮すれば、ウイルスアナリストがマルウェア作成に関わっていることは、いつか必ず暴露されます。
- アンチウイルス開発会社はウイルスを作成しないし、アンチウイルス比較テスト、あるいは新しいソフトウェア導入を目指すジャーナリストやユーザーに対して既知のウイルスが含まれる悪意のあるファイルは提供しません。あるアンチウイルス開発会社もしくはその社員がウイルス作成・拡散に関わっていたことが明らかになれば、その企業にとって極めて大きなダメージを与えます。
- Doctor Webを含み、アンチウイルス開発会社の多くは、クラッカー活動経歴のある就職希望者を採用しません。ウイルスを作成していた候補者は品行方正な人物であるとは考えられないためです。

マルウェアは、実際、誰に作成されているのでしょうか？

確かに、コンピュータ時代の幕開けに自己表現のためにウイルスを作成する人がいました。今でも、名声を博すのにウイルスを作成する人がいますが、このような人物は、脅威であるとはいえません。

現在、ウイルス開発に単なるプロではなく、よく組織化された犯罪集団が関わっており、以下のメンバーから構成されます。

- マルウェアの開発及びその利用を管理する人物
- マルウェアの開発者
- マルウェアのテストを行う専門家
- OSやアプリに潜む悪用可能な脆弱性を探し出す専門家
- マルウェアを拡散するメンバー
- 組織内のセキュリティ及びボットネットの管理を行うメンバー
- マルウェアを拡散するためにウェブサイトの作成者
- マルウェア販売・貸し出しを管理する人物（トロイの木馬の一部は販売や貸し出しのために開発されています）
- DDoS攻撃の実行者
- アドウェア型トロイの木馬を用いて利益を得る広告ウェブサイトの開発者

マルウェアの開発・拡散に携わる犯罪集団が、このように組織化されているため、悪意のあるプログラムが大量に作成されるようになりました。このようにマルウェア数が激増していることを背景に、ウイルスデータベースに毎日追加されるレコード数にも影響を与えています。

一つの犯罪組織が一日で作成できるマルウェアの検体数が数百個以上に及ぶ可能性があります。リリース後しばらくの間、それらの検体は標的となる被害者のアンチウイルスソフトウェアにて検知できないリスクがあります。検知されない理由については、後ほど説明します。

マルウェア作成の目的は何ですか？

マルウェアは利益を狙って作成されています。

窃盗を行うためのトロイの木馬の開発や配信、そしてトロイの木馬を動作させるために必要な設備維持などに関わっている人は共犯になります。

現在拡散されているトロイの木馬は、以下のように個人・法人で保有されるデータのほかに有形資産をも盗み取っています。

- オンラインバンク、決済システム、SNSなどへのアクセスに必要なログインやパスワード
- 仮想通貨（ビットコインなど）
- 電子メールのメッセージ、及び連絡先リスト
- 写真（被害者の写真を盗み取って、インターネット上に写真を掲載し身代金を要求するといった恐喝行為）
- 被害者のコンピュータに関するあらゆるテクニカルな情報
- ゲームアカウント及びゲームアイテム

コンピュータから盗み取られるものがなくても、ボットネットとして悪用されるリスクが残ります。

注意！

ボットネットを構成し、他のコンピュータやウェブサイトに対して攻撃を行う狙いでコンピュータが乗っ取られた場合、使用者本人がそれを知らなくても刑事責任が問われる国もあります。

誤解№ 4 「アンチウイルスはマルウェアがコンピュータに進入した時点でそれを検出しなければならない」

マルウェアがシステム上に進入した時点で必ずアンチウイルスに検出されるといった誤解が幅広く流布しています。しかし、実際、あらゆる病気からの治療薬が存在しないことと同様に、あらゆるマルウェアが検出できるわけではありません。

殆どのユーザーは、犯罪集団が運営しているウイルス開発事業の仕組みについて知識が浅いため、このような考え方が固定観念化されました。現在、犯罪集団によって作成されるトロイの木馬は、開発過程において、アンチウイルスに検出されない設計とテストが実施されていると考えられています。

標的型攻撃を行うために、ウイルス作成者はアンチウイルスソフトウェアに検出されないようにトロイの木馬を設計しています。

検出の難しい複雑なコードを持つトロイの木馬が出現してから、ウイルスラボに提供され対応機能が開発されるまでに一定の期間がかかります。一方、一般的なマルウェアである場合、Dr.Webアンチウイルスエンジンに採用されるシグネチャ型検出手法のほか、ヒューリスティック及びシグネチャ型ものと異なるテクノロジーによって検出されます。

誤解№ 5 「コンピュータに進入したウイルスの動作にユーザーが気付き易い」

上記の考えは最も深刻な誤解の一つです！

コンピュータ内のデータ全体を消去したり、自身コピーが含まれる迷惑メールを大量に配信させたりするウイルス活動でシステムへの負荷が高まり動作速度が落ちたため、こうしたウイルス動作に気が付くことが可能でした。

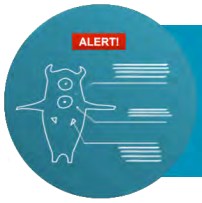
しかし、ユーザーの金銭やデータを狙う現在のウイルスは秘かに動作しています。

こんなことを知っていますか?

1. システムを感染させた後、他のマルウェア進入を防ぐためにシステムが抱えている脆弱性を修復し、システム上に潜伏する競合マルウェアの駆除を行うというマルウェアが存在します。
2. アンチウイルスの該当プロセスを終了し、Windowsタスクバーの通知領域でアンチウイルスのアイコンを表示させるトロイの木馬があります。これによって、ユーザーにアンチウイルスが動作しているような誤解を与えます。このようなマルウェアのリソースには人気のあるアンチウイルス全製品のアイコンが保管されるため、巧妙なトロイの木馬は攻撃対象コンピュータ上にインストールされたアンチウイルスに当てはまるアイコンを選択します。しかし、このアイコンをクリックすると反応しないため、アンチウイルスがフリーズしてしまったかのような感じになりますが、実際には、コンピュータは保護されない状態になります。Dr.Webでは、上記の攻撃を防ぐために、特殊な自己防御システムが用いられます。

ユーザーにとって姿の見えないトロイの木馬を開発し、ユーザーが気付くことなく情報を盗み取ることが、ウイルス作成者の目的であるため、「ウイルス挙動で気が付くはず。」という考え方は、もはや時代遅れであると言わざるをえません。

しかし、前述のような誤解は非常に幅広く流布しています。その結果、全くアンチウイルスを使わないか、アンチウイルス使用にあたって必要不可欠な定期スキャンさえ行わないユーザーがいます。



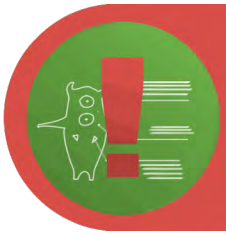
誤解№ 6 「アンチウイルスに用いられるマルウェア検出手法はシグネチャ型手法のみである」

これは、歴史上初めてアンチウイルスが登場して以来、最も根強く定着しつつある考えの一つで、ITセキュリティ企業や専門家ですら、アンチウィルスは定義ファイルに頼っていると唱えることがあるほどです。確かに、20年ほど前のアンチウイルスはそうでした。

しかし、シグネチャ型手法のみを用いるアンチウイルス（ウイルスデータベース内のレコードを基にマルウェアを検知するアンチウイルス）は、1990年代にポリモーフィック型ウイルスが登場してから、この手法が有効ではなくなったため、ほとんど使われなくなりました。ポリモーフィック型ウイルスは自己コードを変え、都度異なる方法を用いるため、同一ウイルスそれぞれの検体にはコード内のユニークなシグネチャがありません。ポリモーフィック型ウイルスの出現をきっかけに、ロシアのDr.Webアンチウイルスが開発されました。

仮に、ウイルスデータベース内のレコードを基にマルウェアを検知するという手法のみが現在のアンチウイルスに採用されれば、データベースの肥大化が著しくなり、現在の十分なメモリを持つコンピュータでさえ、動作が不安になると考えられます。この場合、スキャン実施が長時間を要するほか、システム速度の大幅な低下が予想されます。

ウイルスデータベースレコードに併せて、シグネチャ型手法と異なるヒューリスティック手法、パターンマッチング、及び予防的テクノロジーを併用する現在のアンチウイルスは最新の脅威からユーザーを守ります。



誤解 № 7「ウイルスデータベースに特定マルウェアのレコードがない場合、ヒューリスティック手法で確実に検出しなければならない」

この誤解の根源は、アンチウイルスが全てのマルウェアを検出しなければならないという考え方に基づいています。さらに、アンチウイルスのヒューリスティック分析テストが実施されることも影響しています。

実際には、ヒューリスティック手法で検出されることができるのは、既に解析された既知のマルウェアをベースとした新しい亜種のみです。

ウイルス作成者は、トロイの木馬がアンチウイルスデータベースに追加された場合、そのトロイの木馬をやり直す必要がないように、パッカーでトロイの木馬を圧縮するか、暗号化を行います。

さて、この場合アンチウイルスはどのようにトロイの木馬を検出するのでしょうか?

個別の検体が現れるときにそれをデータベースに追加することが一つの手法であり、この手法のみを用いるアンチウイルスは存在するかもしれません。一方、Dr.WebではFly-Codeテクノロジー及び構造エントロピーテクノロジーが用いられます。Fly-Codeテクノロジーによって、パックされた実行オブジェクトを効率よくスキャンするほか、ファイル実行仮想化という手法を用

いて非標準型パッカーを含めてあらゆるパッカーを解凍することができます。構造エントロピーテクノロジーを採用することで、パッカーに保護されたスキャン対象となるオブジェクト内にあるコードの配置を解析することによって未知の脅威を検出することが可能になります。

アンチウイルスの目的は、ウイルスによる感染を防ぎながら既に進入してしまったマルウェアの駆除・修復を行うことです。

とはいえ、アンチウイルスは全てのマルウェアを検出できるわけではありません。そのため、不明なプログラム起動の制限など、複合的な手段を用いて、セキュリティ対策を強化します。コンピュータ上に進入し、ウイルス対策をすり抜けようとするマルウェアからシステムを修復できる、それがアンチウイルスです。

アンチウイルス以外に、マルウェアから感染したシステムを修復できるプログラムが存在しないため、修復という機能はアンチウイルスの主な目的ともいえます。

誤解№ 8 「マルウェアから保護するために、アンチウイルスを補完する他のプログラム製品が必要になる」

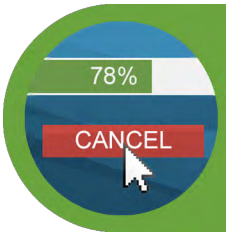
現在のアンチウイルスはスパイウェアとルートキットを検出できるため、

他のプログラムを併用することでアンチウイルスの動作を補うことは不要です。さらに、数多くのアンチウイルスにはファイアウォールが含まれおり、ネットワークを介しての不正アクセスを防止することができます。アンチウイルスはシステムに隠蔽しているあらゆるマルウェアの検知・駆除を独自で行えるため、他のプログラムを使ってアンチウイルス動作を補う意味はありません。

注意！アンチウイルスを装うプログラムが存在します。このようなプログラムはユーザーに役に立たないのはもちろん、ユーザーのコンピュータを危険にするリスクがありますので、ご注意ください。

どんなに慎重なユーザーであっても、プログラムが抱えている脆弱性、ソーシャルエンジニアリング、及びフィッシング行為などによって、ウイルスに感染するリスクが高まっています。

Java仮想マシンの脆弱性が犯罪者に悪用されたため、BackDoor.Flashback.39によるMac OS Xを狙う史上初の大量ウイルス拡散が起きました。**その結果、世界各国のおよそ650万台のコンピュータがBackDoor.Flashbackに感染されました。**



誤解№ 9 「疑わしいサイトの閲覧や、不明な送信者によるメールに含まれるリンク先のクリックをしなければ、アンチウイルスが要らない」

アンチウイルスはコンピュータのパフォーマンスを低下させるばかりで、ユーザー自身がメールにある悪意のあるリンク先をクリックし、トロイの木馬をダウンロードしない限り、ウイルスに感染するリスクが特にないため、アンチウイルスは要らないだろうと信じる人もいます。下記の内容から、このような考え方が重大な誤解であることが明らかになります。

ユーザーが意図せずに不注意で自分のコンピュータ上にトロイの木馬をダウンロード・インストールするケースが多々あります。

ユーザーが知らないうちにシステム上にトロイの木馬を密に仕掛けるという攻撃が存在します。つまり、ユーザーは操作していないのに、トロイの木馬は潜入してしまいます。

誤解№ 10 「ゲームの目的のみでコンピュータを使う場合アンチウイルスが要らない」

現在も急成長を続けるオンラインゲーム市場の年間売上げが数十億ドルに上っています。ゲームで遊ぶ人たち（プレイヤー）はインターネット経由で拡散される脅威に晒されないと考えるのは間違いです。

プレイヤーがゲームのアイテムを実際の現金に交換するケースがあって、このことは転売の目的でゲームのアイテムを盗むTrojan.SteamBurglar.1などのようなトロイの木馬に悪用されます。

トロイの木馬を仕掛ける手法のほか、貴重なゲームのアイテム及びゲームアカウントを盗む、ゲームサーバに対しDDoS攻撃を行う意図でプレイヤーのコンピュータをボットネットに加えるなどの手法が、犯罪者に用いられます。

最後に、エンコーダ型トロイの木馬についても説明します。この種のトロイの木馬は、被害者のコンピュータ上に残るオンラインゲームの痕跡、あるいはSteamアカウントを探し出し、ファイルの暗号化を行い、身代金を要求します。

Dr.Webアンチウイルスは上記のようなマルウェアからの保護を提供します。Web保護モジュールのSpIDer Gateによって、偽造サイトへのアクセスも制限されます。

株式会社Doctor Web Pacific〒210-0005
神奈川県川崎市川崎区東田町1-2NKF川崎ビル 2F
TEL 044-201-7711
FAX 044-201-7712

www.drweb.co.jp | www.av-desk.com | http://freedrweb.com | http://mobi.drweb.com