



McAfee Systems Protection

スパイウェア検出数のカウント方法

認識と実際

目 次

目 次	3
シグネチャ数にまつわる誤解	
多くのごまかし	
脅威が一意としてカウントされる場合	
ほかにもある数字の根拠	
実態を曇らせるもの	

どのようにして製品を比較すべきか	3
次のステップ	3
業界の協力	5
第三者テストの改善	5

まとめ	10
-----	----

シグネチャ数にまつわる誤解

多くのごまかし

ウイルス対策業界が誕生して間もない頃、シグネチャの数を自慢し、他のウイルス対策ベンダーに追いつかれないためにサンプルを公開しないというベンダーが多く見られました。しかし最終的には、これが誤解を与える主張を生み出し、市場に悪影響を及ぼすことをすべてのベンダーが認識しました。そしてこの方法は、多くの意味で、ICSA ラボ、VTC、AV-Test.org などの第三者テスト機関の登場につながりました。

残念ながら、総じてスパイウェア対策業界は、このレベルにまで成熟していません。多くのベンダーは、各社のパッケージに付属する実行ファイル、データファイル、レジストリキーなどを新しいシグネチャとしてカウントしています。検出される脅威の種類にも、大きな差があります。一部のベンダーはバックドアトロイやワームを検出しますが、他のベンダーは検出しません。セキュリティに影響がなく、議論すべきプライバシーへの影響もないクッキーを大量に検出するベンダーもあります。

脅威が一意としてカウントされる場合

ウイルス対策の考え方

ウイルス対策業界は、ウイルス命名規則の混乱に対して長い間非難を受けてきました。製品の検出能力として主張される脅威の数だけでなく、脅威の命名やカウント方法には大きな相違があります。この不一致は、さまざまな理由でウイルス対策業界に生じてきました。

- ・ 従来から使用している規則がある
- ・ 感染拡大中に名前を同期させる時間がない
- ・ 単なる頑固さ
- ・ ジェネリック検出とヒューリスティック検出の技術の違い

最後に挙げた理由を理解するために、6文字の文字が

ら成る次の4つのファイルがすべてウイルスであると仮定してください。

1. ABCDEF
2. ACCDEF
3. AACDEF
4. AACDFF

さらに、これらすべてのウイルスを検出するために、ウイルス対策ベンダーが規則的な検出コードを作っていると想定してください。

ベンダーX:

- A*CD*F をウイルス1として検出

ベンダーY:

- AACD*F をウイルス1として検出
- A*CDEF をウイルス2として検出

ベンダーZ:

- ABCD**をウイルス2として検出
- ACCD**をウイルス3として検出
- AACD**をウイルス4として検出

まとめると、次のような結果になります。

表 1: 仮定に基づいたウイルス命名の一致

ファイル	ベンダー X: シグネチャ数 1	ベンダー Y: シグネチャ数 2	ベンダー Z: シグネチャ数 3
ABCDEF	ウイルス 1	ウイルス 2	ウイルス 2
ACCDEF	ウイルス 1	ウイルス 2	ウイルス 3
AACDEF	ウイルス 1	ウイルス 1	ウイルス 4
AACDFF	ウイルス 1	ウイルス 1	ウイルス 4

この非常に簡略化された例では、シグネチャ数に200%のばらつきがある3社のベンダーは4つのサンプルをすべて検出しますが、サンプルは異なる名前で検出されません。

Virus Bulletin用にマカフィーが管理する Vgrep (<http://www.virusbtn.com/resources/vgrep/index.xml>) では、このような混乱を軽減するために、大量のサンプルを対象として各ベンダーのウイルス名を相互参照できるツールを提供しています。

より現実的な例を挙げると、AV-Comparatives の最近のテスト (http://www.av-comparatives.org/seiten/ergebnissebnisse_2004_08.php) では、テスト対象製品が公表しているシグネチャの数は、53,000 という控えめな数 (Dialogue Science) から、123,000 に近い数 (Frisk Software) まで多岐に渡っています。

しかし最終的には、ほぼすべてのテスト対象製品が、323,000 の一意サンプルのうち 300,000 以上を検出しました。したがって、シグネチャ数の大きな差は、実際の検出能力においては小さな差にしかならないと言えるでしょう。

つまり、この程度の混乱が、次のような性質を持つ業界に存在するということになります。

- ・ 何らかの形で 20 年近くの実験がある。
- ・ ウイルスまたはトロイかどうかについて一貫した定義を持っている (ウイルスの定義は数学用語で表現でき、「An Abstract Theory of Computer Viruses」(Adleman、1988 年) に極めて明確に記述されています)。
- ・ 協力と一貫性を促進する各種の専門機関 (AVPD、CARO、AVED、AVAR、EICAR) がある。
- ・ ベンダーの大多数の間で日常的にコレクションの交換が行われている。
- ・ 質の高いコレクションを持つ定評あるテスト機関が多数存在する (ICSA、VTC、VB、AV-Test.org、AV-Comparatives.org など)。

実際、ウイルス対策ベンダーの検出能力を評価するすべての根拠は、規範的な、あるいは少なくとも極めて包括的なコレクションが存在するという事実の上に

存在します。これにより、ウイルス対策製品は、カウント方法および命名に本質的な不一致があるにも関わらず、対応するもの同士を明白な方法で比較することができます。

スパイウェアの考え方

それでは、スパイウェア業界に話を移しましょう。次の表は、マカフィーが最近 (2004 年 9 月) 実施した社内調査で明らかになったシグネチャ数の「生データ」です。

表 2: スパイウェア製品のシグネチャ数

ベンダー	製品	検出数
Aluria	Spyware Eliminator	18625
Lavasoft	Ad-Aware	9637
CA	PestPatrol	118060
Safer Networking	Spybot S&D	17679
Spycop	SpyCop	467
Webroot	Spyware Sweeper	31104
Javacool	SpywareBlaster	3183
PC Tools.com Ltd	Spyware Doctor	10684
Giant Company Software‡	Giant Antispyware	> 100,000
McAfee	VirusScan Enterprise	3175*
McAfee	Antispyware**	384

* PUP (Potentially Unwanted Program : 不審なプログラム) の検出のみカウント

** McAfee のコンシューマ向けスパイウェア対策製品

‡ 現在は Microsoft Antispyware

この表から、各種製品の最多および最少シグネチャ数の間には 3 桁の差があることがわかります。次に、これらの製品がマカフィーの APP コレクション (ウイルスおよびトロイ以外の検出) をスキャンした際のパフォーマンスを検討してみましょう。

表 3: スパイウェア製品によるマカフィーAPP コレクションの検出

ベンダー	検出数	所要時間
McAfee VirusScan Enterprise	11288	0:19:50
Spyware Doctor	135	0:00:24
SpySweeper	951	0:02:54
Adwaresafe	151	0:00:57
Adaware	356	0:03:19
PestPatrol	2601	0:25:00
McAfee Antispyware*	270	0:03:53
Aluria Spyware Eliminator	358	0:12:07
Giant Antispyware	617	0:22:19
SpyBot	0	0:03:08

*McAfee のコンシューマ向けスパイウェア対策製品

注意：

- ・これはひどいテストなので、実際の比較や競争評価に使用するべきではありません。
- ・McAfee Anti-Spyware Enterprise (企業向け製品) は、テスト時には提供されていなかったため含まれていません。

上記の結果からわかることはただ 1 つ、無意味なテストを実行するのは「極めて」容易であるということだけです。これはなぜ、ひどいテストなのでしょう。

- ・これは、各 DAT のリリース前に当社が PUP と考えるものを検証するために使用されるコレクションなので、1 社 (マカフィー) が収集したサンプルしか含まれておらず、VirusScan Enterprise に有利なように大きく偏っています。
- ・これは、検出のトリガとしてファイル以上のものに依存する製品に不利なように大きく偏っています。たとえば、SpyBot は、正常にインストールされたパッケージ (レジストリ項目などを含む) がシステムに存在する場合、PUP のみを検出します。ダムファイルのコレクションによってトリガされるものは何もありません。実際、Spy Bot は活動中の PUP に対する優れたスパイウェア対策製品ですが、このテストではその点を確認することはできません。
- ・これには、クッキーやレジストリ項目の検出が含まれていません。これらは、製品によってはシグ

ネチャデータベースの大部分を占めています。

- ・これには、スパイウェア対策製品に含まれることの多いバックドアトロイやその他の「従来の」マルウェアが含まれていません。たとえば、Pest Patrol の Pest Encyclopedia (<http://research.pestpatrol.com/search/browse.aspx>) にある 25,000 以上のペストのうち、70% 近くのファイルは、AVERT が一般にトロイの木馬として扱うカテゴリに分類されるものです。裏を返せば、Pest Patrol のシグネチャベースの 4 分の 3 近くには、McAfee VirusScan Enterprise がすでに検出している項目が含まれていると言えます。
- ・これには、McAfee DAT ファイル内の 100 以下のシグネチャで検出される 200,000 以上の一意のダイヤラープログラムのコレクションが含まれていません。

ほかにもある数字の根拠

しかし、スパイウェア対策の数字のゲームに意味を持たせる試みはこれだけではありません。ほとんどのウイルスやトロイは、自己完結型のコードであり、通常は 1 つのファイル、または別のファイル内のほんの小さなコードでできています。ポリモルフィックやパラサイトによってウイルスの全体像がもう少し複雑になり、ウイルス対策ベンダー間で正しいファミリー名をめぐる意見の不一致が高まる可能性はありますが、PUP と比べれば、それらは多くの点で複雑ではありません。

一方、PUP の多くは、完全なソフトウェアパッケージです。PUP にはインストーラ、アンインストーラ、readme、EULA (エンドユーザー使用許諾契約)、データファイル、サポート DLL、ショートカット、およびその他の Windows アプリケーション共通の付属ツールが含まれています。当社の McAfee Anti-spyware (MAS) コンシューマチームがスパイウェアのコレクションを収集した初期の経験から、当社は次のことを認識しています。

- ・ MAS コレクションには約 14,000 のファイル (txt、jpg、レジストリなどのデータファイルを削除したあとに残るのは約 5,000 のみ) が含まれており、製品に含まれるわずか 400 程度のシグネチャで一意に検出されます。したがって、DAT が 3,000 シグネチャで 11,000 のファイル(シグネチャ当たり約 3 ファイル)を検出するのに対し、MAS は約 14,000 ファイルをカバーするのに 400 シグネチャしか必要としない(シグネチャ当たり約 35 ファイル) こととなります。
- ・ 1 つの MAS 検出には、DAT 内の 5~10 のまったく異なる名前検出されるファイルが含まれることが多くあります。
- ・ PUP では非常に多くのコードが再使用されており、まったく同じバイナリが 15 以上の別々の PUP パッケージに存在することさえあります。さらに悪いことには、同じバイナリが、PUP の特徴をまったく持たないパッケージ、つまり当社がこの関連で検出しようと考えないパッケージに存在する可能性もあります。

簡潔に言えば、データベース内のシグネチャの数と、ある脅威に対する当該製品の有効性との間には、対応関係はまったくありません。

スパイウェア対策ベンダーの間では、検知数のカウント方法に関する一貫性はほとんどありません。しかし、どのベンダーも包括的なコレクションを持っていないので、一貫性を要求することができないのです。AVERT では、当社がウイルス対策の領域で行っているいくつかの方法でカウントした場合、約 7,000~10,000 の一意の PUP が実際に検出されていると推定しています。そこで、ウイルス対策中心のベンダーが全体の半分しか認識していないと仮定し、それを 2 倍して、ベンダー間の命名規則の多様性とジェネリック検出のレベルの違いを加味するとします。結果は、約 20,000 を超えるものがすべて警告を発生し、カウント数を増やすことになるでしょう。

実態を曇らせるもの

ホストベースのスパイウェア対策製品では、検出を報告する方法が複数存在すると考えられます。

- ・ 一意の検出名の数
- ・ 検出名および亜種の数
- ・ 検出されたファイルおよびレジストリ項目の数
- ・ 削除されたファイルおよびレジストリ項目の数

あるレベルでは、これらの方法は本質的にどれが一番正しいということはありません。しかし、最初の方法を使用するベンダーからの報告と、最後の方法を使用するベンダーからの報告を比較した場合、両社がまったく同じオブジェクトを検出し削除したとしても、明らかに偏った結果となるでしょう。

一部の製品は、Windows システムにデフォルトで存在するレジストリキーを検出しますが、他の製品では、この検出が「ミス」としてカウントされる可能性があります。

また、同じオブジェクトを複数回報告する製品もあります。あるテストでは、1 つの DLL が 1 つのレポートに 50 回記載されるという例がありました。多くのスパイウェア対策製品は、レジストリキーを複数回報告します。その場合、たとえば次のような処理の単位となるハイブごとに 1 回報告されます。

- ・ HKEY_CLASSES_ROOT¥ProgID
- ・ HKEY_LOCAL_MACHINE¥Software¥Classes¥ProgID

一部の製品は、親キーを削除したときに存在するそれぞれのサブキーやレジストリの値を報告するので、1 つの「既知の悪質な」オブジェクトが、修復ログに数十またはそれ以上の項目を記録させる原因となる場合があります。

当社では、異なるウイルス対策製品が、実際には同じ

成果として 1 つのアドウェアパッケージを検出し修復した、つまり、すべての製品が同じファイルおよびレジストリ項目を削除したにも関わらず、5~96 に及ぶ異なる数の「項目」を報告したという例を確認したことがあります。

言い換えれば、2 つの製品が報告するオブジェクトの数と、当該製品の有効性との間には、対応関係がないということです。

どのようにして製品を比較するべきか

検出テストの目的は、どの製品グループが最も多くの「悪いもの」を効果的かつ効率的に特定できるかを判断することです。有効な比較を行うためには、いくつかの前提条件があります。

- ・ テスト対象の全製品が、何が「悪いもの」であるかについて同意していること。少なくとも、全製品が明確に同意するサンプルだけを含めなければなりません。すべての製品がトロイの木馬やピアツーピアファイル共有プログラムを削除することを目的としていない限り、それらをテストセットに含めるべきではありません。
- ・ サンプルセットは、できるだけ大規模にすること。セット内のサンプルは、明確に規定した期間に収集されたものとし、その分野のエキスパートによる検証を受けるべきです。テストが不正に偏ることを避けるために、レビューアのサンプルセットは、理想的には業界のリソース、第三者のエキスパート、およびレビューア自身の調査から抜粋したスーパーセットであるべきです。
- ・ サンプルセットを限定しなければならない場合、サンプルは、たとえば流布度、潜在的リスクまたは発病ルーチン、削除の困難さといった意味のある基準に従って選択すること。サンプルの選択が適切でない小規模なサンプルセットを使用した場合、まったくの幸運でテスト対象製品のプラス

面とマイナス面の両方が隠されてしまう可能性があります。

- ・ 誤検出および非検出の両方をテストすること。すべてのサンプルをキャッチする検出ルーチンは容易に作成できますが、大量の誤検出やパフォーマンスの問題を招きます。
- ・ 成功または失敗の基準は、ファイル、プロセス、またはレジストリの変化を独立して測定したデータに基づくものとし、一部の「参照」製品のパフォーマンスを基準にしないこと。

スパイウェア対策市場全体には一貫性や定義が存在しないので、これまでのほとんどのテストは、うまく設計され実施されてきたとは言えません。サンプルセットは、小規模で独断的に選択されてきました。使用されたサンプルおよびそれらのシステムへの影響の文書化も不十分です。測定結果は多くの場合、当該サンプルとの関係のあるなしに関わらず、製品が報告した項目の数を記載したものになっています。

次のステップ

業界の協力

現在のスパイウェア対策業界は、まるで誰も他者のカードを見ることができない大規模なポーカーゲームを繰り広げているようです。すべてのベンダーが顧客から説明を求められないことを期待して、はったりをきかせてうまく切り抜けていますが、これは受け入れ難い状況です。マカフィーは、現在ウイルス対策コミュニティに存在するのと同様の協力関係を、スパイウェア対策コミュニティの信頼できるメンバー間で構築する取り組みを開始しようとしています。数社の大手ウイルス対策ベンダーの間では、すでに一部の PUP コレクションの交換が行われています。

当社は、この取り組みを拡大することで、より明確な競合勢力の全体像を把握し、現実には即した尺度で当社の進捗状況を測定できるようになることを目指して

います。当然ながら、他社も当社のコレクションを利用できるという意味で、このアプローチには多少のリスクがあります。しかし、ウイルスコレクションの交換を実施してきた数年間の経験では、この方法の実施が原因で大きな変動が生じた例はありません。以前から有能な企業は今も有能であり、うまくまとまっていない企業は今も遅れをとっています。スパイウェア対策市場でも、同じことが当てはまると考えられます。いずれにしても、ウイルス対策の領域で開発してきたツールや技術を備えた当社は、ほかのどのベンダーよりも、新たな内容にうまく対処できる状況にあると言えます。

第三者テストの改善

最後に、スパイウェア対策業界は、高度なスパイウェアの測定およびテストを促進する必要があります。欠陥のあるテストによってベンダーの優劣が判断される環境には、進歩の程度を判断したり、各社の進歩状況を測定する合理的な方法は存在しません。私たちは、どのテスト手法が最も正確で有意義な結果を出せるかを判断し、これらの手法を実施するために第三者テスト機関と協力しなければなりません。さらに、第三者レビューが法的影響に関する不安を克服し、有用なコレクションを構築できるよう支援する必要があります。

しかし、これが実現するまでは、引き続き「開拓時代」のテストを受けることとなります。顧客、十分な情報を持たないレビューア、パートナー会社、そしてOEMは、計画不足の場当たり的なテストを実施しようとし、その結果、実態を明らかにするのではなく、実態をさらに曇らせてしまうのです。レビューアが注意すべき点を次に挙げておきます。

- ・ 可能な限り、流布度をベースとしたデータを使用してテストセットを扱うこと。顧客の報告、サポートログ、ベンダーの流布度レポートなど、事実上どんなものからでも PUP 流布度のデータを集

めるほうが、偶然誰かの家族のコンピュータに存在していたり、いくつかの疑わしい Web サイトを訪れたときに偶然インストールされた N 個の PUP と比較してテストするよりも妥当性があります。

- ・ 経験不足のレビューアの多くは、独断的な大量の PUP をインストールした場所でテストを実行したあと、1 番目のスパイウェア対策製品を実行し、次に 2 番目の製品を実行し、1 番目の製品が見逃したものを示してそのベンダーを攻撃しようとしています。この Spyware Warrior の調査の結果からわかることは、ベンダーは特定のパッケージのすべてを検出するか、まったく何も検出しないかのどちらかである場合が多いけれども、すべてのベンダーがかなりの数のパッケージを見逃すということです。精通したセキュリティ研究者が、見逃されたものすべてを関連のあるもの（誤検出ではない）と確認し、テストを逆の順序でも実行しない限り、結果として示されたデータは無意味であると言えます。
- ・ 製品の誤検出、非検出、または修復誤りが報告された場合は、再現できるように関連のあるサンプルをベンダーに提供するか、主張の誤りを証明すること。「スパイウェア」とは何かについて確立された法的解釈や業界レベルの定義が存在しないために、製品間の差は意図的に作り出される可能性があります。少なくともベンダーには、今後のバージョンに反映できるように、報告されたすべての問題を修正する機会が与えられるべきです。

まとめ

スパイウェア対策市場は、10年前にウイルス対策市場が注目した方法と非常によく似た方法に目を向けています。そこには、大きなチャンスと同時に大きなリスクも存在しますが、市場は成熟の兆しを見せています。米国および海外における法的および強制的取り組みは、発展途上の現場に完全な見直しを迫っています。一方、PUPを作成する組織の行動が、セキュリティコミュニティの仕事を大幅に容易にしたり、難しくする可能性があります。しかし、このように頻繁に変化し、リスク/リターンの高い環境は、まさに私たちが過去に経験してきた環境であると言えるでしょう。

MCAWP-CSD-0503A-MC

マカフィー株式会社

www.mcafee.com/jp/

お問い合わせ先

東京本社	〒150-0043 東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20F TEL: 03-5428-1100(代) FAX: 03-5428-1480
名古屋営業所	〒460-0002 愛知県名古屋市中区丸の内 2-20-25 丸の内 ST ビル 8F TEL: 052-203-8421(代) FAX: 052-203-8422
西日本支店	〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL: 06-6344-1511(代) FAX: 06-6344-1517
福岡営業所	〒812-0013 福岡県福岡市博多区博多駅東 1-10-27 アステリア博多ビル 8F TEL: 092-452-3511(代) FAX: 092-452-3515

McAfee、VirusScan は米国法人 McAfee, Inc. またはその関係会社の登録商標です。

本書中のその他の登録商標及び商標はそれぞれその所有者に帰属します。© 2004 Networks Associates Technology, Inc. All Rights Reserved.

製品、サービス、サポート内容の詳細は、最寄りの代理店または弊社事業部までお問い合わせください。製品の仕様、機能は予告なく変更する場合がありますので、ご了承ください。