KASPERSKY lab

THE POWER OF PROTECTION

APT
今そこにある脅威

先進的なサイバー攻撃に対する効果的な対策のために

URL : www.kaspersky.co.jp

目 次

Advanced Persistent Threats
APT攻撃の脅威

日々何万ものサイバー攻撃が発生し、様々な対策がそれを防御
しています。しかしサイバーセキュリティはその件数だけでなく、
ビジネスに対する被害こそが問題です。
たった一度の事故が与えるビジネスへのダメージは計り知れず、
大半の攻撃に備えるだけでは不十分なのです。

私たちは、頻発するよくあるタイプの脅威への対策だけでなく、より高度な脅威に対しても注意を向けなければなりません。

世界で発生するマルウェアは、既知の脅威 (70%)、未知の脅威 (29%)、先進的な脅威 (1%) の３つに分類されます。

マルウェアの70%を占める既知の脅威は比較的容易に対策を打つことができます。悪意あるコードを認知してさえいれば、それをブロックすることが可能だからです。伝統的なシグネチャベースの対策がその典型です。

‘未知の脅威’ である29%のマルウェアに対しては、より洗練されたツールが必要です。標準的なアンチウィルスソフトウェアの範囲を超えた、ヒューリスティック分析や動的なホワイトリストといった手法を用いることによってこれらと戦うことが可能です。

それでは残る1%に対していかに対処するか。
先進的な脅威、それは多面的で持続的な標的型の攻撃です。組織のネットワークに侵入するためにデザインされ、目に見えないところで活動し重要なデータを盗む、そしてそれは一旦侵入すると発見されないままに数年間活動を続けるのです。

‘Darkhotel’ と呼ばれるAPT攻撃では、豪華なホテルのネットワーク接続が宿泊客のデータを盗むために使われていましたが、これは発見される７年前から活動を継続していました。企業の上級役員やCEOなどをターゲットとした典型的な標的型攻撃であり、また企業のラップトップPCやタブレットといったエンドポイントが社外のネットワークで利用される際のセキュリティへの挑戦として注目されるべきものです。

‘Darkhotel’ と呼ばれるAPTでは、豪華なホテルのネットワーク接続が宿泊客のデータを盗むために使われていましたが、これは発見される７年前から活動を継続していました。

これまで大企業や政府機関などの組織がAPT攻撃の被害者となってきましたが、あなたの組織が同じようにサイバー犯罪の被害者として報道されてしまわないとも限りません。
そうならないために対策を行うことが重要です。

企業はデータの流出や長期に渡る操業の停止、社会的評価へのダメージなど、APT攻撃によって被る被害のリスクを低減する能力を備えなければなりません。そしてAPT対策は攻撃を受けてしまった後の修復に比較して遥かに低いコストで実施することが可能です。何故なら、密かにかつ確実に活動するAPT攻撃では、それが発見されたときには既に数ヵ月間或いは数年間に渡って甚大な被害を受けてしまった後だからです。

この問題に対して唯ひとつの回答があるわけではありません。既知の脅威と未知の脅威に対するテクノロジーは有効ですが、APT攻撃に対してはそれだけでは不十分です。益々複雑化し洗練されていく脅威に対抗するためには多層のセキュリティアプローチが必要です。既知、未知、そして先進的なマルウェアを全体的かつ包括的に検知し防御することのできる統合されたテクノロジーが必要なのです。

このレポートはAPT攻撃と戦うあなたの組織がより良い対策をおこなうためのものです。

1件のマルウェア感染事故にかかるコストは、中小企業の平均で $56,000、大企業で $649,000 と報告されています。[1]

!

APT攻撃は甚大な被害をもたらします。2014年カスペルスキーは Carbanak APTを発見しました。この複雑な攻撃は国際的な犯罪グループによって行われ、多くの金融機関から 10億ドルを盗み出しました。このグループは銀行内部のネットワークに侵入して行員の端末スクリーンを記録し、いかに発見されずに送金処理をおこなうかを学んだのです。

[1] The high cost of a security breach, Kaspersky Lab.

あなたの企業は標的となっている ～ 5つのキーポイント

企業は直面するITセキュリティの脅威を認識しなければなりません。この脅威はますます標的型となり、技術や手法は洗練され続けています。

1 APTに対処するための戦略を立案するにあたって、その最初のステップはあなたの企業が攻撃者の標的であることを認識することです。
知的財産であれ個人情報であれ金銭に関わる情報であれ、あなたの組織は犯罪者が利益を得るに値する情報を保有しています。
犯罪者が狙うデータが仮にあなたの企業自身のものでなくても、彼らはあなたのパートナーやお客様に辿り着くためのルートとしてあなたのネットワークを利用するのです。まさにDark Hotelがその例です。

2 2番目に、私たちは脆弱性に対する認識をより強く持つ必要があります。
大勢の人々が多様なプラットフォームのデバイスを利用して、様々なアプリケーションを活用する大きな組織では、すべてのリスクから無縁で居つづけることは不可能です。攻撃者が突破することができる潜在的な抜け道が必ず存在します。
APTが狙う脆弱性、それが人的なものであっても技術的なものであっても、規模が大きく組織が複雑であればあるほど、より多くの潜在的なエントリーポイントが存在するのです。

3 BYODと柔軟なワークスタイルが新たなチャレンジとして付け加えられます。スマートフォンやタブレットはしばしば安全でないネットワークに接続されます。さらに面倒なことに、iOSのようなオペレーティングシステムではデバイスが感染しているかどうかを知ることすら困難です。
モバイルワーカーはさながら動く標的なのです。安全な社内ネットワークの外でデバイスが使用されることを制御することは困難であるため、効果的なエンドポイントセキュリティは防衛面での重要なコンポーネントです。

4 この多様なエンドポイントに加えて、犯罪者がネットワークに侵入しようとする手法の多様さを考えれば、単純なセキュリティ対策は全く不十分と言わざるを得ません。
リスク低減のためには多面的かつ多層の強固な対策の組合せが必要です。スレットインテリジェンス、セキュリティポリシー、そして単に既知の脅威だけでなく新たな未知の脅威を浮かび上がらせることのできる特別なテクノロジー(例えばホワイトリストのような) の統合が必要なのです。

5 リスク低減のためにはエンドポイント対策に対する再検討が必要です。サイバー犯罪者は脆弱性を突破します。そしてエンドポイントは常に大企業の最大の弱点です。デバイスそのものだけでなく、人の不注意な行動や安全でない利用環境からセキュリティが破られるのです。

リスク低減対策の重要性

企業はリスク低減対策に着手しなければなりません。攻撃されてしまってからの対応に比べて、事前の防御対策はより効果的かつ低いコストで実施することが可能だからです。

APTをおこなう攻撃者は強い動機に加えて極めて高いスキルと潤沢なリソースを持っています。しかしながら、その他の多くのサイバー犯罪者と同様に、一部の特殊な例外を除けば彼らはより容易な道を選ぼうとするのです。
従って、APTから免れることを保証することは出来ないにしても、攻撃の成功を困難にするための対策を講じることが可能です。
APTそれ自体が多層の脅威であることから、効果的な対策もまた多層であることが求められます。単純なセキュリティツールだけでは不十分です。このアプローチはどのようなものでしょうか。
以下にオーストラリアシグナル社の役員会が作成した戦略リストを提示します。カスペルスキーはこのリストが先進的な脅威に対抗するための広範で綿密なものであり、他の企業においても良いスタートポイントとして適用可能であると考えています。
この戦略は４つのカテゴリーに分けられます。

1 セキュリティポリシーと教育

ITセキュリティは単にITに関することにとどまりません。人の過ちや不注意な行動はサイバー犯罪者にとって大きな助けとなります。セキュリティに関する包括的な教育を定期的におこなうこと、正しい行動を促すこと、そして適切で現実的なポリシーを設定することによって、従業員によってサイバーの脅威が組織に持ち込まれるリスクを低減することが可能になります。

2 ネットワークセキュリティ

ネットワーク構造を工夫することは、感染による潜在的なインパクトを大きく減らすことに役立ちます。リスクを低減するための多様なネットワーク戦略が存在します。例えば、特定の部門を分離することで、センシティブなデータにアクセス可能なエンドポイントの数を削減でき、リスクレベルを大きく低減することができます。

3 システム・アドミニストレーション

セキュリティポリシーに従ってシステム管理者権限を適切に制限することによって、対処すべき脆弱性を低減することが可能です。更に、利用するプログラムに組み込まれたセキュリティ機能を活用することで大きな効果を得ることが可能です。不必要な機能を無効に設定することは、攻撃者に突破される潜在的な穴を閉じることになります。

ブラウザのJavaコード実行を無効に設定するだけでセキュリティレベルは格段に上がります。

4 特別なセキュリティ・ソリューション

前述のステップに加えて、特別なセキュリティソフトウェアが持つ機能によって、極めて効果の高い防御レイヤーを付け加えることが可能です。特別な、とは言ってもその機能を統合するために莫大な投資や労力を必要とするわけではありません。下の3つの特別なセキュリティソリューションをシステム管理者権限の管理と合わせて活用することで、85%の脅威を排除することができます。

- ホワイトリストとデフォルト拒否によるアプリケーションコントロール
- アプリケーションプログラムの脆弱性パッチを適用すること
- オペレーティングシステムの脆弱性パッチを適用すること

リスク低減のための方策

企業が必ず実施すべき、或いは検討すべきリスク低減対策が数多く存在します。

アプリケーションコントロールとホワイトリスト

ホワイトリストはAPTやその他の攻撃のリスクを大幅に低減する強力なツールです。
アプリケーション (実行可能ファイル) が有害なものかどうかを問い合わせるのではなく、ホワイトリストはそのアプリケーションが確かに自組織で許可したものかどうかを確認します。これによりアプリケーションの起動や実行はユーザーから管理者に委ねられることとなります。ホワイトリストは既知の信頼できるアプリケーションのみから成り、このリストに存在するもののみが許可されるのです。
マルウェアはしばしば何等かの実行可能ファイル形式をとっていますから、このアプローチによってマルウェアの実行をブロックすることが可能です。伝統的なアンチウィルスのブラックリスト方式の逆をおこなうことによって、既知の悪意あるファイルとしてリストに掲載された場合にのみ検知されるという弱点を克服します。

さらに厳格なコントロールをおこなうために、管理者は ‘デフォルト拒否’ の設定をおこなうことも可能です。ここでは管理者によってあらかじめ許可されたアプリケーションのみが起動可能となり、リスクは極端に低減されます。
これはネットワークからマルウェアを遮断するためには大変有効な方法ですが、従業員の生産性を向上させるための有効なツールまでをもブロックしないように十分考慮することが必要です。
よりきめ細かいアプリケーションコントロールと動的なホワイトリストを組み合わせることによって、管理者は強力なコントロールツールを手にすることが出来るのです。ソフトウェアのカテゴリー毎、ビジネスユニット毎、個人毎やその他の要素ごとにブロック、許可といった制御が可能となります。

もちろん、ホワイトリストを有効に活用するためには事前に利用されているアプリケーションを棚卸しなければなりません。従ってソフトウェア資産管理は死活的に重要です。そこに存在することを知らなければそれをモニターすることは不可能なのです。

カスペルスキーのアプリケーションコントロールと動的なホワイトリスト

カスペルスキーの動的なホワイトリストデータベースは10億件を超える正当なアプリケーションのリストであり、世界の企業向けアプリケーションの97.5%をカバーしています。クラウド基盤であるカスペルスキーセキュリティネットワークと日々継続するスレットインテリジェンス活動によってそのデータベースは常時更新されています。

カスペルスキーのアプリケーションコントロールは単にアプリケーションを許可/禁止とするだけではありません。あるアプリケーションをブロックする必要が生じた際、オペレーティングシステム上のすべての変更されていないコンポーネントを正常に稼働させます。
これによってユーザーの利用に支障を与えることなく攻撃をブロックすることが可能になります。またデフォルト拒否モードに関してテストモードを提供することによって、本番適用前に問題がない事を確認することが可能です。

カスペルスキーの脆弱性診断とパッチ管理
脆弱性スキャンのためにカスペルスキーが利用するデータベースは大変広範なものです。Kaspersky Endpoint Security for Business は自動的にマイクロソフトをはじめとするベンダーのアップデートを検知し導入します。それによって貴重な労力を割くことなく、すべてのアプリケーションとオペレーティングシステムを最新の状態に保つことが可能です。

デフォルト拒否モードでは信頼できるアプリケーションのみが起動可能です。実際、APTで利用されるマルウェアの大半は信頼できない、或いは脆弱性パッチが適用されていないアプリケーションから侵入しているのです。

アプリケーションのパッチ適用とOS脆弱性
アプリケーションやオペレーティングシステムは犯罪者が破ることのできる脆弱性を内在しています。このような抜け穴が問題とならないような運用を行う、或いは常に最新の脆弱性パッチを適用することが重要です。そして広く使われているアプリケーションほどより多くの脆弱性が発見され、パッチが適用されない状態では危険もより多く存在します。

多層のITセキュリティ対策において、パッチ管理ツールは重要です。多くのエンドポイントアプリケーションを最新の状態に保つための管理作業を自動化でき、潜在的な攻撃のエントリーポイントを迅速にふさぐことが可能となるからです。

APTを100%確実に防ぐ方法は存在しないということを改めて認識しましょう。

しかし、システム管理者権限、アプリケーションコントロール、アプリケーションとOSのパッチ管理を正しく導入し運用することによって標的型攻撃の85%を防ぐことができます。これらの組み合わせが多重の防衛線となり、多くの悪意あるコードが検知されずに活動することを困難にするからです。

2014年、1年間に発生したマルウェア感染の92%が、Oracle JAVA、ブラウザ、Adobe Readerの脆弱性に起因しています。[2]

[2] Kaspersky Security Bulletin 2014, Kaspersky Lab

その他の有効な方策

ここまで見てきた方策によって大半の侵入を防御することができますが、
より高度な脅威から情報資産を守るためにはさらに対策が必要です。

さらに防衛線を追加するために利用することのできるいくつかの方策を見てみましょう。

オペレーティングシステムへの侵入防御

オペレーティングシステムに備わったテクノロジーは一般的な脅威の侵入を防ぐためにとても有効ですが、特別なソリューションによってさらに強固な防御を築くことができます。アプリケーションやOSの脆弱性パッチを定期的に適用しても、常にゼロデイ脆弱性の穴による潜在的なリスクが存在します。

既知の脅威に加えて特異なマルウェアや疑わしい振る舞いをあぶり出し、その動きを止めるソリューションが重要です。つまり未知の脅威からの保護です。これによってかつて誰も見たことのない攻撃を防ぐことが出来ます。

ホストベースの侵入防御

これまでの経験から、APT攻撃で使用されるマルウェアは検知されずに数ヵ月間あるいは数年間活動を続けることがわかっています。そういったマルウェアが既に社内ネットワークの内側で密かに活動しているとしたらどうでしょう。ですからネットワーク境界での防御策だけでは不十分と言わざるを得ません。明らかにマルウェアであると断定できなくても、疑わしい危険な動きをするプログラムを検知し止めるテクノロジーが必要です。Host-based Intrusion Prevention Systems (HIPS) はアプリケーションの信頼度に応じてそのシステム内での動作を制限します。HIPSはアプリケーションの特異な動き ～想定されない動作やリスクを示す動作～ を検知します。これは新たなアプリケーションが導入された直後、マルウェアに何らかの変更を加える機会を与える前に作動させることが望ましいと考えられます。

カスペルスキー Automatic Exploit Prevention (AEP)

Internet Explorer、Microsoft OfficeやAdobe Readerなど、特に広く利用されるアプリケーションに対して、AEPは一連のセキュリティチェックを実行します。メモリー内のプロセスを常に監視し、エクスプロイトの動作パターンと比較して疑わしい振る舞いを識別します。このアプローチによってカスペルスキーのAEPはゼロデイエクスプロイトをもブロックすることが出来るのです。[3]

カスペルスキー システムウォッチャー & アプリケーション権限コントロール

この２つの機能がコンピュータ内部のイベントを監視記録し、悪意ある動作からシステムを保護します。システムウォッチャーとアプリケーション権限コントロールが信頼性の低いプログラムが望ましくないシステム変更をおこなうことをブロックし、ロールバック機能によって改変の復元を行います。

[3] MRG Effitas の第三者評価テストによると、AEP以外のアンチウィルス機能をすべてオフにした状態で、エクスプロイト攻撃テストケースの95%をクリアしました。

メールとウェブコンテンツのダイナミック分析

シグネチャベースのアプローチがゼロデイ攻撃に無力であることと同様に、メールやウェブページを既知のマルウェアデータベースと比較するといった伝統的な '静的分析' だけでは新たな脅威から保護することは不可能です。

ダイナミック分析はメールやウェブページの疑わしい特徴をリアルタイムに分析し、例えば埋め込まれた実行可能なプログラムなどを発見してそれが開かれる以前にブロックします。

'ゼロデイ攻撃' はオペレーティングシステムやアプリケーションに内在する、一般には知られていない脆弱性をパッチが発行される以前に狙う攻撃です。

カスペルスキーのウェブコントロールとウェブアンチウィルス

カスペルスキーのウェブコントロールテクノロジーはウェブサイトへのアクセスを個人毎かつサイトの種類毎 (ギャンブルサイトなど) に設定することができます。またHTTP(S)トラフィックをモニターすることでユーザーがホワイトリストに合致したウェブリソースにアクセスすることを保証します。

一方、ウェブアンチウィルスはHTTP(S)やFTPプロトコルのトラフィックをダイナミック分析することによって悪意のあるコードを検知し、ドライブバイダウンロードなどの方法でシステムに侵入するAPT攻撃を遮断します。

カスペルスキーのメールアンチウィルスとSecurity for mail server

Kaspersky Endpoint Security for Businessは静的分析、動的分析とヒューリスティック分析を組み合わせることによって、メールによって送りつけられる脅威をブロックします。また添付ファイルの振る舞いをエミュレーションしてファイルベースのエクスプロイトを防御します。

Kaspersky Security for Mail ServerはDLPオプションによって重要な情報の漏えいを防止します。共有禁止が設定されたファイルがメールに添付されて社外に送付されることを防止します。

多層防御：カスペルスキーのアプローチ

今日、セキュリティに対する脅威は進化しつづけ、ますます複雑なものとなっています。カスペルスキーは世界の政府機関や大企業と協業して、リスク低減対策からスレットインテリジェンスサービスまでの多層防御アプローチを進めています。

カスペルスキーはテクノロジー企業として全体的なリスク低減対策のためのツール群を開発してきました。そしてそれらはすべて自社で、同じコードベースで開発し、切れ目なく統合されているために、本来あるべきではない隙間の存在しない包括的なセキュリティ対策をおこなうことができます。

核となるのは多くのアワードを受賞しているアンチマルウェアテクノロジーとエンドポイントファイアウォールです。これらが70%を占める既知の脅威をブロックし、加えて振る舞い分析、ヒューリスティック分析、アプリケーションコントロールと動的なホワイトリスト、ウェブコントロールなどの先進的なツールによって未知の脅威を防御します。そしてAPTなどの先進的な脅威に対しては、AEP (Automatic Exploit Prevention) やシステムウォッチャーなどの更に進んだテクノロジーによってより強固なセキュリティを実現しています。

インテリジェンスと検知 – 今そこにある攻撃に対抗する

リスク低減対策を徹底的におこなうことは不可欠です。しかし、APT攻撃に対抗するためには、今そこにある攻撃を迅速かつ間違いなく検知するための方策を持つ必要があります。更に攻撃を受けてしまった際にそれを即座にブロックし、ビジネスへの被害を最小化するためのテクノロジーをソリューションに含めておく必要もあるでしょう。

カスペルスキーが提唱する対策は、エンドポイントレベルの防御、ネットワークレベルの防御、インテリジェントサンドボックスと包括的なイベントデータベースで構築されます。

近年、ネットワークレベルの防御がいくつかのIT企業の関心事となり、そして多くのベンダーがネットワーク検知のための専用アプライアンスを発表していますが、カスペルスキーは分散型センサーアーキテクチャーこそがより優れたアプローチであると考えています。何故なら、ネットワークのキーポイントにセンサーを配置し、すべてのセンサーデータを集約することによってより高い検知性能を発揮することが可能となるからです。複雑な大規模ネットワークを防御する場合、このアプローチはスケーラビリティとコストの面からも優位性を持っています。

スレットインテリジェンスサービス

組織にとってリスク低減対策は極めて有効ですが、いかなるセキュリティソリューションでも100%の防御を保証することはできません。
仮に攻撃が成功してしまった場合、企業は即座に次の点を判定しなければなりません。

- どのデータが盗まれたのか ～ 損失を最小化するアクションを取るために
- いかに攻撃が成功したのか ～ 脆弱性やセキュリティの抜け穴を特定するために

そのためには、フォレンジック分析の能力を備えること、あるいは必要な専門能力に即座にアクセスできるよう準備を整えておくことが必要です。

カスペルスキーが提供する様々なインテリジェンスサービスの中から必要なものを適切に選択することが可能です。

- マルウェア分析サービス
  ～ フォレンジックチームを持つ組織のために
- デジタルフォレンジックサービス
  ～ マルウェア分析サービスを含む
- インシデントレスポンスサービス
  ～ デジタルフォレンジックサービスを含む

カスペルスキーの優位性

最前線でAPT攻撃と戦っているカスペルスキーGReATチーム (Global Research and Analysis Team) はRed Octoberと名付けたAPTや過去最強のサイバースパイ活動である‘Equation Group’ まで、世界の最も危険で複雑な脅威を発見してきました。

残念ながら、サイバー犯罪者にとって組織の規模は大した問題ではありません。即ち、国家規模の組織によって、極秘に莫大な費用を投じて開発された武器はすぐに犯罪者の手元に渡るのです。

この事実認識に基づいて、カスペルスキーはサイバー攻撃の現場で活動し、APTの調査から得たインテリジェンスを活用して各国政府にいかにサイバー防衛をおこなうかについてのアドバイスを行っています。それにとどまらず、この活動から得た知見を企業ユーザー向けの効果的で実際的なソリューションとして提供しています。

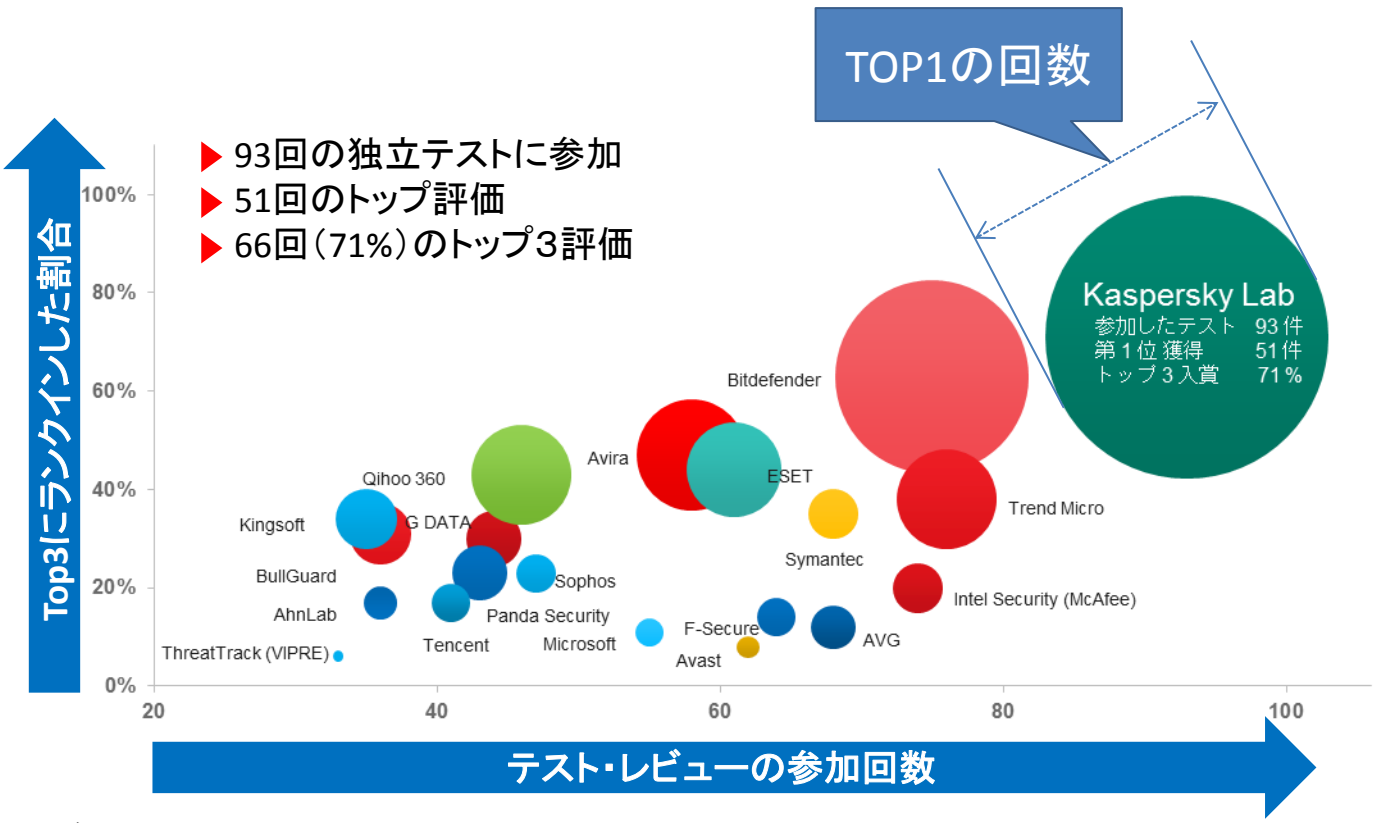
そのため、カスペルスキーは業界においても例を見ない人数をR&Dチームに配置し、比類のないセキュリティインテリジェンスとテクノロジーを統合することによって革新的なソリューションを生み出しているのです。

結果として生まれたのが多層防御のアプローチであり、それによってAPT防衛のためのリスク削減対策を実施する企業を支援しているのです。

カスペルスキーは業界で最も多くの第三者評価機関テストに参加しています。2014年度には93回のテストに参加し、99%の検知率を示しました。結果として66回のトップ３評価、51回のトップ評価を得て、業界内での圧倒的な優位性を維持し続けています。またカスペルスキーは130社を超えるOEMパートナーにテクノロジーを提供しており、あなたの企業も既にそれを利用しているかもしれません。

業界最高の防御性能

2014年、カスペルスキー製品は93回の第三者評価機関テストに参加し、
51回のトップ評価と66回のトップ３評価を獲得しました。



注:
- 企業向け、個人向け、モバイル向けの各製品を対象に、2014年に実施された第三者評価機関によるテスト結果に基づいて作成しています。
- テスト結果には、次の第三者評価機関および専門誌が実施したテストが含まれます。テスト機関：AV-Comparatives、AV-Test、Dennis Technology Labs、MRG Effitas、NSS Labs、PC Security Labs、Virus Bulletin
- 円の大きさは第1位を獲得した件数を表しています。

よりよいサイバーセキュリティ対策を実現するためには

ますます高度化、複雑化する未知の攻撃や既知の攻撃からネットワークを防御する為には多層型のセキュリティ・プラットフォームが必要です。
カスペルスキーが提供するエンタープライズ向けのセキュリティ・ソリューションに関する詳細はこちらをご覧ください。
http://www.kaspersky.co.jp/business-security

弊社セキュリティ・ソリューションに関するお問い合わせ先

株式会社カスペルスキー コーポレートビジネス本部
E-mail: jp-sales@kaspersky.com

APT攻撃などサイバー攻撃に関するお問い合わせ先
E-mail: APT_taisaku@kaspersky.com

その他情報はこちらから
オフィシャルサイト：http://kaspersky.co.jp/
オフィシャルブログ（Kaspersky Daily）：http://blog.kaspersky.co.jp/

Kaspersky Lab について

Kaspersky Labは、世界最大の株式非公開のエンドポイント保護ソリューションベンダーです。ITセキュリティ市場におけるイノベーターとして、17年以上にわたり大企業から個人ユーザーまで幅広いお客様に効果的なITセキュリティソリューションを提供しています。現在、世界中のおよそ200の国と地域で事業を展開し、全世界で4億人を超えるユーザーをIT上の脅威から保護しています。

株式会社カスペルスキー
〒 101-0021 東京都千代田区外神田 3-12-8
住友不動産秋葉原ビル 7F
http://www.kaspersky.co.jp

PR-1012-201506