KASPERSKY lab

Kaspersky Enterprise Cybersecurity

脅威の最新動向に関するガイド

～現実に起きていることと、思い込まされていること～

2016年12月

脅威の最新動向に関するガイド
～現実に起きていることと、思い込まされていること～

次世代の脅威は存在するか？

サイバー犯罪者とセキュリティベンダーの終わりなき戦いは、「適者生存」の原則をよく描いています。世界有数のセキュリティ保護ソリューションの開発元は、攻撃者の活動を阻止する解決策を考察し、これまでは大きな成功を収めていました。しかし、この種のプレッシャーが攻撃者を強く刺激してきたのも事実です。攻撃者は、サイバー犯罪を商売として続けるために、新しいトリックや技術、ビジネスモデルを考え出してきました。

このような進化論的な発展は、「単純化」と「高度化」という両極の方向性を生み出しました。この両方の発展の結果、脅威の動向は複雑化しています。この動向に対抗してセキュリティを保護し続けるためには、さまざまなレベルでの創意工夫、リソース、経験が求められます。これらを満たす次世代セキュリティベンダーの名にふさわしい市場参入者はほとんどいません。

では、「次世代の脅威」が目前にあり、今現在、ビジネスユーザーも個人ユーザーも同じように標的にされているのでしょうか。その答えは、どちらとも言えません。

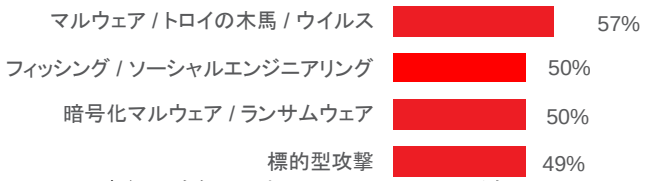
ITセキュリティの専門家の答えは当然「**いいえ**」です。

攻撃者があらゆるセキュリティシステムに対抗できるような神の力を持つほど、サイバー攻撃の技術が急激に向上しているわけではありません。数年前に挑戦した攻撃者もいましたが、ほとんど成功することはありませんでした。その主な理由は、当時のグローバルIT環境に技術的な制約があったことです。しかし、ITの世界があるべき場所へと向かっている今、サイバー攻撃の技術が突如として進歩し、多くの既存のセキュリティソリューションを脅かしています。

先ほどの話に戻ると、堅牢なセキュリティ保護システムを提供するベンダーは、常に攻撃者の最新攻撃手法を警戒し、ユーザーが気づかない間に新しい対抗手段を配備して保護しています。ユーザーにとっては何もかもが当たり前のように感じられます。そのため、どのセキュリティベンダーも、ユーザーの利用パターンを変えるような新しい技術を自社のインターフェイスに導入して、複雑な状況やコストが発生することを望んでいません。その技術を何も伝えず気づかれずに配信でき、ユーザーにとって「できる中での最高の結果」を保証できるのなら、そちらの方がよいのです。

しかし…

IT環境が進化していく中でますます情報流出が生じやすくなる中、突然攻撃を受けたエンドユーザーは、青天の霹靂のように感じます。また、攻撃のない穏やかな日々を何年も過ごしている中で突然マルウェアの侵入に遭うと、企業は、活発で熱心なサイバー犯罪者にとっての金のなる木になってしまったと悟ります。犯罪者は決して、そのような企業を手放す気はありません。企業はようやく、「次世代の脅威」が現実だと感じるのです。



ビジネス全般に対するITセキュリティ上の懸念：
上位4つが直接的な脅威に関するものである*1

したがって、「次世代の脅威は存在するか？」という問いの答えは簡単ではありません。サイバー脅威は新しくなくとも強力で、ブロックするのが困難かもしれません。高度なスキルと経験、そしてセキュリティ保護製品を提供するベンダーの熱心な対応が必要になります。さらに、極めて重要なのは、基盤となる脅威インテリジェンスの深さと広さであり、この脅威インテリジェンスがユーザーとベンダーの両方で稼働する技術とシームレスに統合されることなのです。

次世代のウイルス対策技術こそ、この新たな猛撃と戦うために必要なものだ、とすぐに思い付くかもしれませんが、ほとんどの場合、結論を急ぐのはよいことではありません。その理由の1つとして、次世代のサイバー脅威の多様性を考慮すると、保護アプローチも少なくとも同程度の多様性が必要です。つまり、現在最も活発な攻撃者が気に入っているやり方だけでなく、あらゆる角度からやって来るすべての脅威から保護できる、真の意味でマルチレイヤーのサイバーセキュリティが必要になるのです。

しかし、単純化やシステムリソースの使用量軽減のために、脅威から広い範囲で確実に保護する技術については、「次世代」ベンダーのスコープから除外されることがあまりにも多いのが現状です。この状況は、第三者評価機関によるテストの結果が明確に証明してきました。

その一方で、Kaspersky Labは、このような脅威の多様性および高度化を強く意識し、通常は様々な脅威から保護するための多くの技術を提供しています。また、最も実情に沿ったシナリオを使った詳細テストの重要性を認識しています。第三者評価機関のテストには可能な限りすべてに、継続的に参加し高い評価を獲得し続けることで、Kaspersky Labの実利用環境での保護性能を実証しています。

*1 出典：Global Corporate IT Security Risks Survey 2016（B2B InternationalとKaspersky Labが実施）

脅威の両極への発展

単純化

両極化への発展のひとつは、費用対効果を第一原則としており、開発の手間と攻撃自体の両方に見ることができる「単純化」への流れです。マルウェア開発者にとって、それは既成のマルウェアをほんの少し修正し、被害者が適切なセキュリティ対策を行っていない隙をつく方法であり、かなりの成功を達成してきました。以前からあるソフトウェアが同程度の効率なら、マルウェアを一から開発する必要はないのです。

単純化にはもう一つの側面があります。スキルもあまりなく、我慢もできないサイバー犯罪者が利益を得られるような、便利なビジネスモデルを提供するマルウェアの取引です。ただマルウェア単体で商売するのではなくサービスを売ること、つまり使いやすいインターフェイスでマルウェアアプリと詳細なFAQやユーザーサポートをセットで用意することで、「サイバー犯罪者の市場」が飛躍的に拡大し、スクリプトキディやその他の素人が大量に生まれました。このような状況によって全体的なサイバー犯罪件数が増加し、企業や組織が受けるプレッシャーが増大しました。

高度化

しかし単純化された新しいビジネスモデルがあるからと言って、今日のサイバー攻撃者が利用するツールやテクニックが技術的に進歩していないわけではなく、現実はむしろその逆です。

今では、高度な技術を持つマルウェア開発者でなくとも、以前に利用できたよりもはるかに高度なマルウェアを入手できるようになりました。また、（ハッキングコミュニティに多数存在する）実際の専門家が使うことで、最新のマルウェア開発事情は本当に侮れないものになります。

加えて、以前は標的型攻撃者の特権であると考えられていた、一部の高度な技術が、大量感染キャンペーンに利用されることも増えています（このキャンペーンは、いつでも、より標的型のものへと変換できます）。

匿名性のベール

脅威の動向における最近の構造転換の中で、おそらく最も重要な変化の1つが、匿名性の拡大でしょう。ビットコインやその他の仮想通貨の登場によって、出所を突き止められない支払いが可能になり、またTorのような匿名通信システムによって、悪意のある攻撃者が自分の身元が割れるリスクを背負うことなく、情報や技術について取引を行う新しい機会を得ています。熟練のサイバー犯罪者は未だ「招待した人だけ」という厳重なコミュニティを形成していますが、それでもこのような新しい技術によるメリットを享受しています。そのような状況で、ランサムウェア（世界中のITセキュリティ問題のうち3番目に懸念されている問題*2）のような、いくつかのサイバー犯罪ビジネスモデルが急増しているのです。

ランサムウェア

このランサムウェアという現象は、特定の技術を表しているわけではありませんが、それでも私たちが現在直面している真の意味で「次世代的」な脅威の1つです。

ランサムウェアの実情は、「サイバー犯罪のビジネスモデル」です。技術的には、ランサムウェアは幅広い攻撃ツールやテクニックだけでなく、多数の匿名化手段によって支えられています。仮想通貨やおよびメッシュネットワーク（Tor、I2Pなど）の登場によって、犯罪者は匿名のまま支払いを受けることができ、その結果、ランサムウェアはかつてないほど広まりました。適切に対処しなければ、ランサムウェアは最も直接的かつ破壊的な方法で1日を台無しにします。その結果を元に戻せるチャンスはほぼありません。一方で、統計によれば、身代金を支払った被害者の5人に1人は、身代金を支払ったにも関わらずファイルを復旧できませんでした。その結果、犯罪者に金銭を与えランサムウェアの拡散に貢献するだけになっています。

ランサムウェアの種類が異なると、使われる攻撃技術や感染方法も異なります。そのため、マルチレイヤーソリューションには、システム全体を保護する専用のランサムウェア対策技術を配備することが重要です。たとえば、Kaspersky Endpoint Security for Businessは、マルウェアをブロックして、すでにマルウェアによって暗号化されたファイルを以前の状態に戻す、暗号化攻撃に対抗するロールバックシステムを提供しています。Kaspersky Security for File Serversには、また別の補完的な暗号化対策エンジンが備わっており、このエンジンによって、ネットワーク上の異なるホストから起動された暗号化プロセスをブロックできます。さらに、他社製品の利用者に対しては、スタンドアロン（かつ無料）のKaspersky Anti-Ransomware Toolによって基本的な保護を行うことができます。この無料ツールのベースとなっている技術は、実際はKaspersky Endpoint Securityに搭載されているものと同じです。しかし、Kaspersky Lab独自のソリューション内では、この無料アプリケーションに含まれていない多くの追加保護レイヤーによってこの技術が強化されています。

*2 B2B International調べ、2016年5月

メモリにしか存在しないマルウェア

ほとんどのマルウェアが一般ファイル形式で侵入して来ることが、ファイルベース検知の重要性を証明しています。実行前検知の大部分はこのファイルレベルで行われます。言うまでもなく、単純で視野の狭いシグネチャだけでなく、あらゆる種類のヒューリスティック（構造分析やコードベース分析を含む）によって、まだ知られていなかったマルウェアも検知できるようになります。しかし、マルウェアがファイルシステムの外部で動作する場合、この豊富な機能は突如として役に立たなくなります。ファイルの残骸も、デジタルフォレンジックにとっては情報の宝庫です。これらすべてを考慮して、特に標的型攻撃においては攻撃者による「メモリ限定」アプローチの利用が増えています。メモリ限定アプローチは、「水飲み場型」感染技術の利用や、添付ファイル（早期の検知を避けるために十分に難読化されたもの）を開くなどのさまざまな手段で実現できます。その結果はどのケースでも同じです。既に実行中のプロセスにインジェクションし、その瞬間からマルウェアがファイルシステムに触れることなく動作し始め、追加のモジュールを読み込んで起動したり、影響を受けるインフラストラクチャ内を移動し始めたりします。

“メモリにしか存在しないマルウェア”など、世の中には既に多く存在する高度なタイプのマルウェアを検知するために、Kaspersky Endpoint Securityにはシステムウォッチャーという機能があります。これは、アプリの疑わしい振る舞いを、そのシステム内のアクティビティの調査によって検知することを基礎とした技術です。このアプローチでは、監視下にあるプロセスの背後にファイルの実体が存在するかどうかは関係なく、あらゆる悪意のあるアクティビティがブロックされます。システムウォッチャーの検知の原理は、常に実行されるマシンラーニングプロセスに基づいています。システムウォッチャーは、Kaspersky Security Networkのデータを通じ得られた広範な脅威インテリジェンスを利用します。

PowerShell：合法のスクリプトプラットフォーム、違法のアクティビティ

シェルスクリプトファイルは長らく、無害なものと思われてきました（言うまでもなく、創造性と悪意のある意図をもって使えば、無害ではなくなりますが）。しかし、PowerShellスクリプトとなると話は別です。本当に強力であるため、攻撃者にとって極めて幅広いチャンスが生まれます。インターネットから追加モジュールをダウンロードし、実体のないマルウェアを実行し、ネットワーク内の他のマシンにある任意のコードをリモートで実行する　－これらすべてが、本来は有益なアプリである、PowerShellインタープリター（Windows 7以降のWindows標準装備）の名の下で行われます。このテクニックを利用する悪名高いサイバー犯罪グループの1つが、金融機関を狙い金銭を窃取するCarbanakです。

Kaspersky Labは、一般的なシェルスクリプトを悪意のある目的で使うことに加え、このPowerShellマルウェアについても十分に認識しています。カスペルスキー製品のエンジンに渡される文字列については入念に分析し、悪意のあるものが見つかれば実行がブロックされるようになっています。

モバイル

携帯電話とタブレットは、すでにインターネットへのアクセス手段として普及しています。2016年末までに、世界中で利用されるスマートフォンの台数は21億台に達する見込みで、攻撃者にとっては収穫に適した豊作地帯になっています。モバイルはすでに企業のビジネスプロセスやデータフローにも深くまで統合されていますが、残念ながら企業のサイバーセキュリティインフラに深くまで統合されているとは言えません。たとえば地政学的な緊張の高まり、モバイルでの金融取引の利用者増、モバイルデバイスに保存されている大量の機密情報など、多くの要因からモバイルに対する攻撃が一気に増加すると予想されています。ゼロデイエクスプロイトのモバイルサイバースパイ活動への悪用は現実的ですが、特に攻撃への対処が準備できていない場合、高度でない攻撃手段でも成功する確率が高まります。その一例が、オンライン広告を悪用した厚かましいマルバタイジング攻撃です。人気の高いサイトを閲覧し読み込んだ直後に、閲覧者に合った特定のオンライン広告が選ばれ、そこには悪意あるJavaScriptがあり、金融系トロイの木馬がダウンロードされるといった、オンライン広告を悪用した攻撃です。Androidスマートフォンの大半がそれほど困難もなくroot化でき（偽アプリや悪意のあるアプリによるものも含む）、中にはマルウェアが既にインストールされた状態で手元に届くデバイスもあります。そのため、利用者が管理できるOSレイヤーよりも下層でシステムレベルのマルウェアが稼働しているというのも、珍しくはありません。

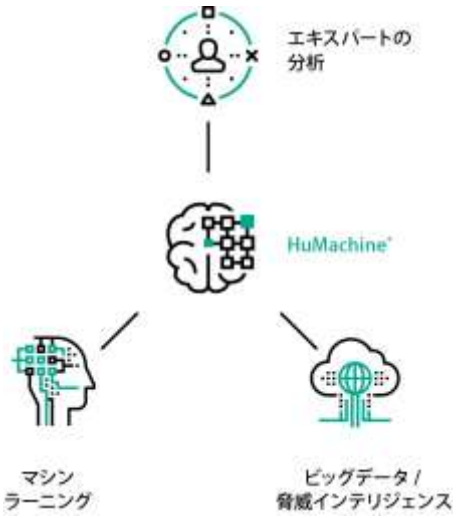
Kaspersky Security for Mobileは、多くのデスクトップソリューションに匹敵する幅広い検知レイヤーを保有しています。その一部はマシンラーニングによって支えられ、HuMachineインテリジェンスの力を最大限に活用している点は注目すべきです。また、アプリケーションコントロールなどの追加の強力なセキュリティレイヤーも存在します。モバイルセキュリティが1つの全体を占める一部分として、モバイルデバイス管理やモバイルアプリケーション管理とともに動作していることが重要です。そのようなアプローチによって、企業が特にセキュリティに優れた確実なモビリティ戦略を策定できるようになります。

まとめ

上述のサイバー脅威の数々は、包括的とは言えませんが、熟練の専門家だけが実現できた、さまざまなレベルの悪知恵について説明してきました。おそらく、このようなテクニックにより、皆さんの恐怖、不安、疑いの念が膨らんだかもしれませんが、それらを一掃するために、いくつか思い出して欲しいことがあります。

1つは前述のとおり、これらのサイバー脅威に特別新しいものはないということです。最も「次世代的」な変化は、実はビットコインやTor系ネットワークなどの、匿名でのコミュニケーションや決済の手段にあります。これらの技術ですら、はるか昔にそのルーツがあり、本来それ自体は悪意のあるものではありません。他の多くの合法ツールと同じように、サイバー犯罪者が悪意をもってする諸刃の剣なのです。

したがって、それらの技術はすでに既知のものであり、保護する手段は、Kaspersky Labなどのセキュリティベンダーから入手できます。さらに、Kaspersky LabのHuMachineアプローチ（脅威インテリジェンスの収集、マシンラーニングプロセスにより強化されたデータサイエンス、そして世界的に有名なエキスパートチームとの効率的な融合）によって、顧客は「最大限の結果」が得られると確信できます。明日の脅威がどれほど「次世代的」なものになろうとも、同じように「次世代的」な保護技術によって、脅威は常に顕在化し、効果的に防御されます。これが、真のサイバーセキュリティというKaspersky Labのビジョンの中で重要な部分です。



Kaspersky Lab www.kaspersky.com
インターネットセキュリティに関する情報：www.securelist.com
パートナー検索：www.kaspersky.com/buyoffline

www.kaspersky.co.jp

株式会社カスペルスキー
PR-1038-201704