KASPERSKY lab

脆弱性攻撃ブロック機能のテクノロジー

内部からの新たな脅威

2012 年の脆弱性のうち、サードパーティのアプリケーションが占める割合は実に 87 % にものぼりました。[1] 同じ年、Kaspersky Lab は、1 億 3,200 万を超えるアプリケーションが危険な状態にあることを検知しました。

サイバー犯罪者による脆弱性攻撃の標的にもっともなりやすいものが、Microsoft Office の弱点や、Oracle Java、Adobe Flash Player および Adobe Reader の不具合です。2013 年の 3 月から 8 月にかけて、弊社のリサーチャーたちは Java に対するエクスプロイトを利用した攻撃を 854 万件登録しました。これは、過去 6 か月間と比較して 52.7 % の増加です。

この急速に増加しつつある脅威に対処するには、一般的なアプリケーションの脆弱性を狙ったエクスプロイトに対して、独自の保護層を提供する専用の技術が最適な手段であると弊社では考えています。コード内の悪意のある部分を最初の段階で実行させないようにすることで、中核となるエンタープライズアプリケーションやコンポーネントがより大規模な攻撃のゲートウェイとなることを防止できます。

この特別な保護層は、脆弱性攻撃ブロック（Automatic Exploit Prevention:AEP）と呼ばれる、Kaspersky Lab が開発した技術に基づいています。これは、既知および未知のエクスプロイトを検知してエンタープライズシステムとデータを保護するために非常に効果的な方法です。

抜け穴に注意 – 典型的なエクスプロイトのふるまい

あらゆるエクスプロイトの目的は、広く使用されているソフトウェアに含まれる脆弱性を利用することで、さまざまな悪意のあるコードを起動することにあります。このテクニックを用いてシステムを感染させるために、サイバー犯罪者たちは次のようなさまざまな方法を使用します。

- 悪意のある Web サイトや、正規であっても悪意のあるコードが侵入したことで感染した Web サイトにユーザーを誘導します。犯罪者の中には、大企業の開発者などの特定のユーザーが好む正規サイトを標的とする、いわゆる「水飲み場型」攻撃を仕掛ける者もいます。
- ユーザーをだまし、特別な細工を施して正規のものと見せかけたドキュメント（PDF や Office ドキュメント）や無害に見えるイメージなどをダウンロードさせたり、開かせたりします。
- USB メモリなど、エクスプロイトに使用されるマルウェアを実行するリムーバブルストレージデバイスは、企業に簡単に「こっそり持ち込む」ことができます。最近の研究で、会社の駐車場で USB メモリを見つけたエンドユーザーは、（そこに企業のブランド名が入っている場合はなおさら）必ず自分のコンピューターに差し込んでしまうことが分かっています。[2]

一般的に標的型攻撃は、メールに添付された一見すると問題のないファイルに見えて、実は特別な細工が施されたファイルをユーザーが開くことから始まります。

---

[1] Secunia Vulnerability Review、2013 年 3 月 14 日

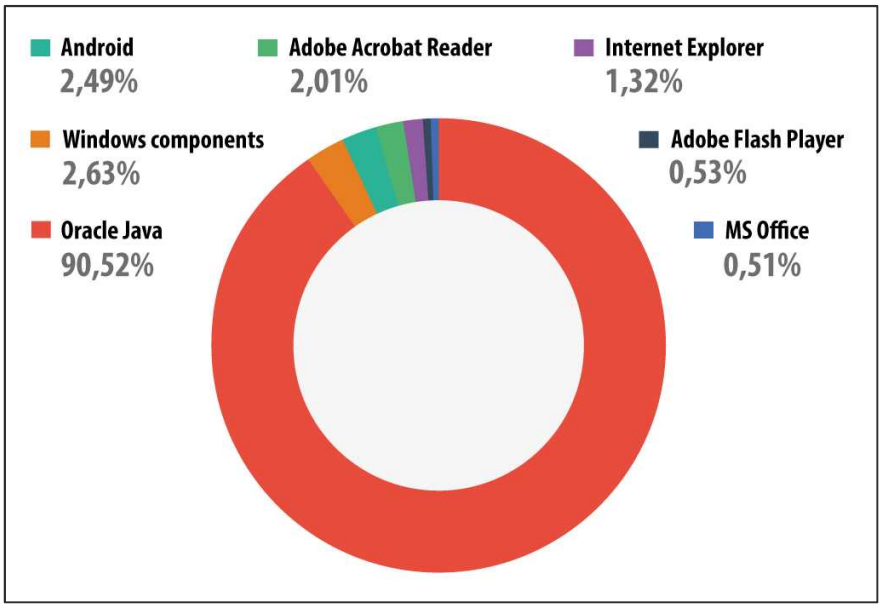
[2] 出典：https://www.schneier.com/blog/archives/2011/06/yet_another_peo.html リムーバブルメディアを経由して実行されるエクスプロイトについては、http://www.securelist.com/en/blog/208187475/Another_usb_media_infection を参照してください。

人気が脆弱性を呼ぶ – もっとも攻撃されるソフトウェア

ほとんどすべてのプログラムにはバグに起因する脆弱性があり、一部には悪意のあるコードの不正実行を可能にするものもあります。平均的なユーザーがおよそ 72 のプログラムを自分のマシンにインストールしていることを考えると[3]、企業には膨大な脆弱性が存在することになります。しかし、現実には、被害者となり得るユーザーを確実に増やすため、犯罪者はもっとも普及しているアプリケーションにこだわる傾向があります。結局のところ、犯罪を成功させるには、一人のユーザーがクリックしさえすればよいのです。

Kaspersky Lab の調査によると、もっとも多くエクスプロイトの標的になっているソフトウェアは Oracle Java で、2013 年に検知された脆弱性に対するエクスプロイトの試みの 90.52 % を占めました。このような脆弱性へのエクスプロイトは、インターネットを使用した「ドライブバイ攻撃」によって実行され、今では Java に対する新たなエクスプロイトが多数のエクスプロイトパック内に存在するようになりました。[4]

脆弱性攻撃の標的で 2 番目に多いものは、脆弱性を含む Windows OS ファイルなどの「Windows コンポーネント」のカテゴリです。Kaspersky では Internet Explorer や Microsoft Office については、これとは別のカテゴリを割り当てています。このコンポーネントカテゴリでの攻撃のほとんどは、win32k.sys-CVE-2011-3402 で見つかった脆弱性を標的にしたもので、有名な Duqu エクスプロイトで最初に使用されました。



出典：http://www.securelist.com/en/images/vlill/stat_ksb_2013_04.png

エクスプロイトの圧倒的多数を占める Oracle Java の脆弱性

[3] Secunia: *Vulnerability Review* 2013
[4] Kaspersky Lab: Java Under Attack – The Evolution of Exploits 2012-2013
http://www.securelist.com/en/analysis/204792310/Kaspersky_Lab_Report_Java_under_attack_the_evolution_of_exploits_in_2012_2013

時間とともに、標的となるソフトウェアの顔ぶれも変化します。たとえば、2010 年にもっとも多く攻撃の標的となったのは、Microsoft Office でした。マイクロソフトが 2014 年 4 月で Windows XP と Office 2003 のサポートを終了し、このソフトウェアについてはセキュリティの更新もパッチの開発も行われないため、中には深刻な弱点をさらしたままの組織もあります。サイバー犯罪者たちは、すでにその弱点に狙いを定めています。クラウドベースのアンチウィルスネットワークである Kaspersky Security Network に参加している弊社製品ユーザーのうち、6.3% がいまだに Windows XP を使用しています。

脆弱性攻撃に対する一般的な保護手段

Kaspersky Lab のソリューションでは、エクスプロイトをブロックする方法を複数採用しています。たとえば、エクスプロイトを使用しているマルウェアに対しては、悪意のあるファイル（メール添付ファイルなど）を開く前でも検知できる特別なシグネチャが追加されています。プロアクティブ保護や他の技術により、脆弱性を含むファイルが開かれた場合、マルウェアを検知してブロックすることができます。最終的に脆弱性スキャンの使用により、脆弱性を含むソフトウェアを任意のエンドポイントで簡単に検知し、パッチ管理機能や他のシステム管理機能と連携して、自動的な更新の適用やパッチが適用されていないソフトウェアのロードを防止することができます。

もちろん、ほとんどの脆弱性攻撃を回避するための最善の方法は、Windows システムコンポーネントや他のインストール済みソフトウェアを定期的に更新することです。

ただし、日常の保護技術では効果がないケースもあります。特に、検知されなかったり、新たに発見されたりしたソフトウェアの不具合のゼロデイ脆弱性がこれに当てはまります。この環境では、セキュリティベンダーがシグネチャベースの手法でゼロデイ脆弱性を標的にした攻撃を見分けることは困難です。また、複雑なエクスプロイトがさまざまなテクニックを駆使してプロアクティブ保護技術をすり抜けたり、突破したりする場合もあります。従来のセキュリティ層をすり抜ける脅威は比較的少ないとしても、エクスプロイトが 1 回でも網の目をくぐり抜けることによって莫大な損害が生じる可能性を考慮すると、企業へのさらなるセキュリティ層の導入が不可欠となり、脆弱性攻撃ブロックが効力を発揮します。

脆弱性攻撃ブロック：仕組み

脆弱性攻撃ブロック（AEP）技術は、企業のエンドポイントおよびネットワークに足がかりを得るためにソフトウェアの脆弱性を攻撃するマルウェアを対象にしています。ユーザーが悪意のあるファイルをダウンロードしたり開いたりしても、AEP 技術によってマルウェアの実行が阻止されます。

Kaspersky Lab は、広く拡散した脆弱性攻撃のふるまいや特徴を徹底的に分析し、AEP を開発しました。これは、弊社の技術によって、脆弱性攻撃に特徴的な行動パターンを認識し、攻撃が完了するのを阻止できることを意味します。

開発プロセスの中で、弊社の研究開発チームは、もっとも頻繁に標的となっているエンタープライズソフトウェアおよびアプリケーションについて深く考察し、それに合わせて AEP 技術を調整しました。AEP は現在、弊社のアンチウイルスおよびインターネットセキュリティソリューションを大きく特徴づけており、標準のシステムウォッチャーモジュールと一緒に動作して、以下の機能を含む追加のセキュリティ層を提供します。

脆弱性を含む可能性のあるアプリケーションの制御

AEP 技術は、Adobe Reader、Internet Explorer、Microsoft Office など、もっとも頻繁に標的となるアプリケーションに特に重点を置いています。これらのプログラムが例外的な実行可能ファイルやコードを起動しようとすると、追加のセキュリティチェックが開始されます。これらのアクションが正しい場合もあります。たとえば、Adobe Reader は更新をチェックするために別の実行可能ファイルを起動することがあります。それでも、何らかの関連するアクションとともに、悪意のあるアクティビティを表すような特徴を持つ実行可能ファイルがあるため、その場合は追加で調査を行う価値があるということになります。

起動前アクティビティの監視

アプリケーションの起動方法やコードの実行方法、そしてその直前に起きる内容から、多くのことが明らかになります。ある種のふるまいが、悪意のあるアクティビティを強く示唆することがあります。AEP 技術は、そのようなアクティビティを追跡して、コードを起動しようとする起点を検知できます。その起点はソフトウェア自体に起因する場合もありますが、脆弱性攻撃の結果である可能性もあります。もっとも一般的な脆弱性攻撃のふるまいに関するデータを利用することで、ゼロデイ脆弱性が使用されている場合でも、この種のアクティビティを検知することができます。これは、AEP では、悪意のあるアクティビティが発生していることを検知するために、攻撃されている脆弱性の詳細な性質を認識する必要がないことを意味します。

コード起点の追跡

一部の脆弱性攻撃、特にドライブバイ攻撃で使用される攻撃（悪意のある Web ページを通じて起動されるエクスプロイトなど）は、実行前に別の Web サイトからペイロードを読み込む必要があります。AEP はそのようなファイルの出所を追跡し、ダウンロードを開始したブラウザーを正確に特定して、このファイルのリモート Web アドレスを取得します。

ある種のプログラムについては、AEP はユーザーの同意を得て作成されたファイルと未承認の新規ファイルを区別できます。不審なコードの起動が試みられると、この情報を利用して脆弱性攻撃の動作を特定しブロックすることができます。

エクスプロイトが標的とした脆弱性へのアクセス防止

AEP は、いくつかのプログラムやソフトウェアモジュールと一緒に「アドレス空間配置のランダム化強制」と呼ばれるテクニックを使用し、エクスプロイトが攻撃の実行に必要な特定の脆弱性やコードを見つけられないようにします。

アドレス空間配置のランダム化（ASLR）技術は、Vista 以降のマイクロソフトの Windows オペレーティングシステムに含まれていますが、すべてのプログラムがこのデフォルト機能をサポートしているわけではありません。Kaspersky Lab の AEP 技術は、このデフォルトバージョンをサポートしないプログラムにも ASLR の機能を拡張し、エクスプロイトが動作に必要とするコードのロケーションを特定することをメモリ内などで阻止することで、一部のエクスプロイトタイプをブロックします。必要とするコードを繰り返し探そうとする行動は、悪意のあるコードを実行しようとする行動よりもアプリケーションクラッシュの原因となる可能性が高くなります。

AEP はどこから使用できるか

脆弱性攻撃ブロック技術は、Kaspersky Endpoint Security for Business の一部として使用できます。この技術は既定で有効化されていますが、個別に無効化することや、必要な場合は（システム内のプログラム活動を追跡する）システムウォッチャーモジュールと併せて無効化することもできます。

既定では、AEP はあらゆる疑わしいコードの起動をブロックします。もっとも一般的なエンタープライズアプリケーションへの詳細で継続的な調査だけでなく、Kaspersky のチェックおよび追跡の方法論によって、誤検知のリスクが非常に低くなります。この機能は、好みに合わせて対話モードで実行することが可能です。

エンタープライズ IT セキュリティへの利点

脆弱性攻撃ブロックにより、広く拡散したマルウェアから感染する危険性や、ゼロデイ脆弱性が使用されている場合でもエクスプロイトを使用した標的型攻撃を大幅に減らすことができます。Kaspersky Lab の広範な内部テストや研究開発プロセスの間、AEP は Adobe Flash Player、Quick Time Player、Adobe Reader、Java およびその他のプログラムで広く使用されている脆弱性を標的としたエクスプロイトのブロックに成功しました。

弊社の IT セキュリティへのアプローチは、常に脅威に関する情報を効果的に使用して未知の脅威の性質を予測することと併せて、複数の保護層を提供することに基づいてきました。脆弱性攻撃ブロックは、既知のエクスプロイトと未知のエクスプロイトの両方をブロックすることで、従来の IT セキュリティ技術を回避し得るような複雑で洗練されたコードを検知するための安全網が提供され、アンチウイルスやアンチスパムなどの弊社のほかの技術が補完されます。

Kaspersky Lab は、IT セキュリティの脅威を予測し阻止し続けながら、より複雑さを増す将来の企業リスクを軽減します。