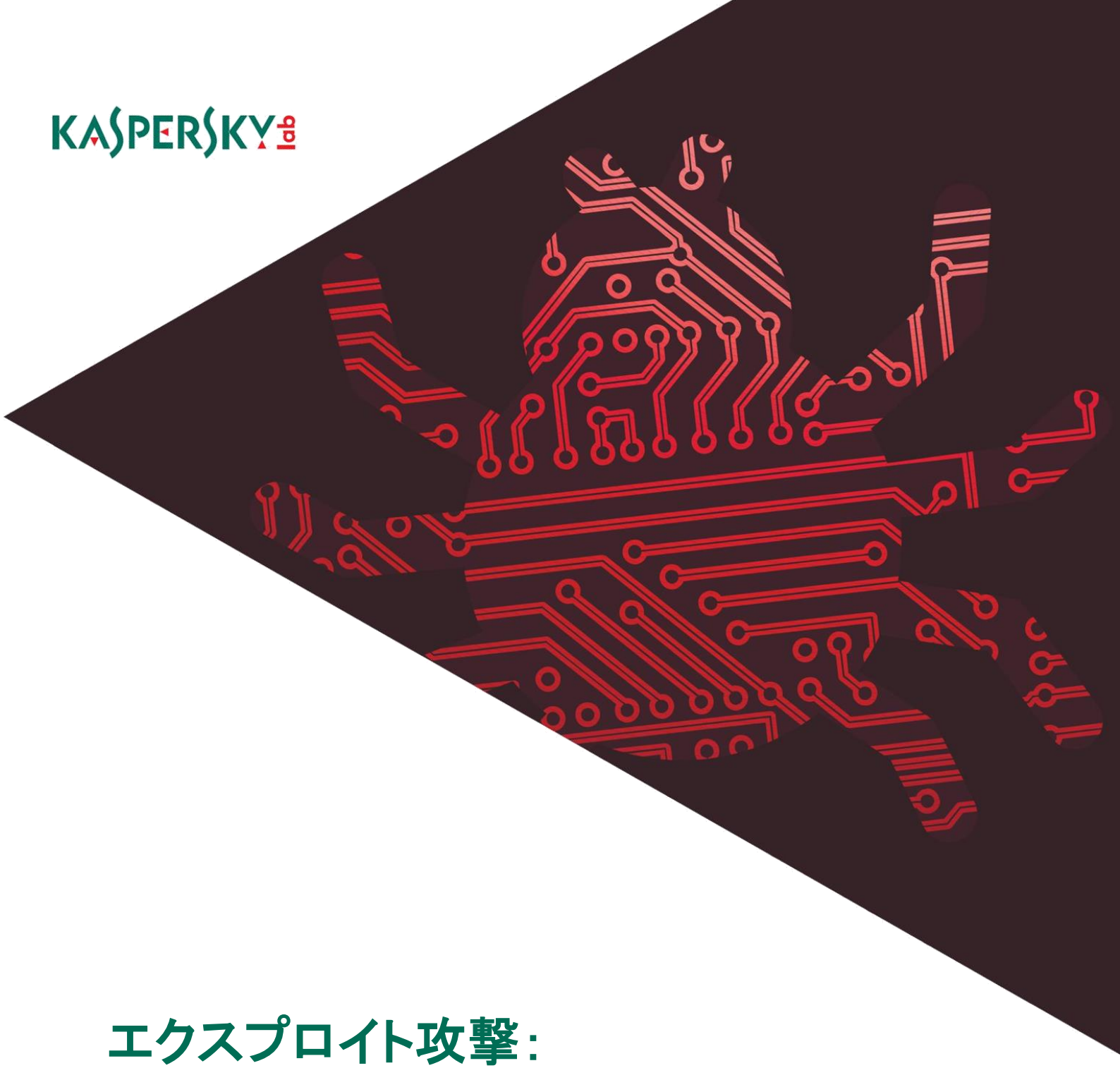

エクスプロイト攻撃：日常の脅威から標的型攻撃まで

2017 年 4 月

Kaspersky Lab

目次

概要および調査結果

「エクスプロイト」とは、ソフトウェアプログラムの脆弱性を悪用し攻撃を行うために作成されたコンピュータープログラムです。エクスプロイトは、攻撃者にとって新たなマルウェアを感染させるための手段の1つであるため、サイバー脅威を取り巻く状況を語る上で欠かせません。

ソフトウェア製品は数千行、あるいはそれをはるかに超える行数のコードから作成されており、エクスプロイトの標的になりうるギャップやエラーはどうしても存在します。脆弱性の中には、アンダーグラウンドマーケットで膨大な金銭を得る目的で売買されたり、脆弱性を悪用する攻撃者によってその存在が隠されたりし、数年経過してから表面化するものもあります。これらの中で最も値打ちがあるのが、未知でかつ修正プログラムが存在しない「ゼロデイ」です。そのほかにも、既知で修正プログラムが存在するけれども、活発で破壊力を保持したまま広く出回っているエクスプロイトキットに組み込まれたものや、アップデートされていないシステムを侵害できるものもあります。

エクスプロイトを用いた攻撃は通常、ユーザーによる操作を一切必要としないため、ユーザーに疑いの念を抱かせないまま危険なコードを送り込むことが可能です。

エクスプロイトから家庭や企業のネットワークを保護するためには、普段使用しているアプリケーションにエクスプロイト可能な脆弱性が存在するかどうかを把握することが重要です。

本レポートは、2 つのセクションで構成されます。

パート I ： 2015 年と 2016 年の 2 年間のデータを元に、ユーザーに影響を及ぼした上位のエクスプロイトと脆弱なアプリケーションについて解説します。また、同データを元に、カスペルスキー製品の「脆弱性攻撃ブロック」技術の観点から考察します。この技術は、ゼロデイなどの未知のエクスプロイトや、難読化された既知のエクスプロイトを特定してブロックするための技術であり、Kaspersky Lab が特許を取得しています。

パート II ： 大規模な標的型攻撃キャンペーンと、攻撃に使用された脆弱性について説明します。このパートでは、例外的に 2010 年から 2016 年という非常に長い期間を対象にしました。

本レポートの情報源は次のとおりです。

パート I ： Kaspersky Security Network ※1 によって収集された情報と、一般公開情報を利用しました。

パート II ： 過去 6 年間に公開した Kaspersky Lab の脅威インテリジェンスレポートと、一般公開情報を利用しました。

本レポートの目的は 2 つあります。

1. 脆弱性およびそれに関連するエクスプロイトの影響力と持続性について知り、その対策として堅牢なセキュリティおよびソフトウェアアップデートの必要性について認識を深める。
2. 顧客や企業ユーザーに対して、特に注意すべきアプリケーションを浮き彫りにすること。

主な調査結果 （カスペルスキー製品での観測）

パート I ： 2015 年および 2016 年のエクスプロイトの状況と攻撃、カスペルスキー製品での検知

- 2016 年にエクスプロイトを利用した攻撃の試みは 702,026,084 回で、前年比で 24.54%増加しました。
- 2016 年は 4,347,966 の個人ユーザーが、エクスプロイトによる攻撃を受けました（2015 年から 20.85%減少）。
- エクスプロイトに 1 回以上遭遇した企業ユーザーの数は 28.35%増加し、690,557 に達しました。これは、エクスプロイトによる攻撃を受けたユーザー総数の 15.76%にあたります。
- ブラウザー、Windows、Android、Microsoft Office が、悪用される頻度の最も高いアプリケーションです。2016 年、これらのアプリケーションのいずれかで、ユーザーの 69.8%がエクスプロイトに遭遇しました。
- 2016 年、世界中の 297,000 以上のユーザーが未知のエクスプロイト（ゼロデイおよび難読化された既知のエクスプロイト）による攻撃を受けました。

パート II ： 2010～2016 年のエクスプロイトおよび標的型攻撃グループ

- 2010 年から 2016 年までに Kaspersky Lab が報告した標的型攻撃グループが保持、利用、再利用した脆弱性は 80 を超えるものとみられます。追跡した脆弱性の約 3 分の 2 が、複数の攻撃グループによって利用されていました。

- Sofacy（別名 APT28、Fancy Bear）は 25 もの脆弱性を利用してきたとみられます。その脆弱性には少なくとも 6 つのゼロデイが含まれています。Equation Group も約 17 の脆弱性を利用し、そのうち少なくとも 8 つはゼロデイでした（一般公開データおよび Kaspersky Lab 独自の調査による）。

- ロシア語圏の標的型攻撃グループが、脆弱性の利用トップ 4 のうち 3 つを占め（残りの 1 つは第 2 位の Equation Group）、他の英語圏および中国語圏の脅威グループはさらに下位に位置しています。

- 脆弱性の情報が公開された後は、危険性がはるかに増します。数時間以内に巨大な脅威グループによって情報が把握され、それぞれの目的で利用されるためです。
- 標的型攻撃者が一般的な攻撃者と同じ脆弱性を利用することも多く、2010 年から 2016 年までの標的型脅威グループによって利用された上位の脆弱性と、2015 年から 2016 年までのすべての攻撃で利用された上位の脆弱性はかなり似ています。

※1 Kaspersky Security Network （KSN）

KSN は、Kaspersky Lab のアンチマルウェア製品の各種コンポーネントから情報を収集する、クラウドベースのアンチウイルスネットワークです。ネット上の新しい脅威を即時に検知し、感染源を数分でブロックすることで KSN に接続されたすべてのコンピューターを保護します。KSN には全世界で数千万の個人および法人ユーザーが参加しており、悪意のある活動に関する情報を世界規模で共有しています。すべての情報は、ユーザーの同意を得て収集されています。

パート 1：統計情報

2016 年、Kaspersky Lab のセキュリティ製品は、合計で全世界 4,347,966 ユーザーに対するエクスプロイトを利用した攻撃を 702,026,084 回ブロックしました。この攻撃数については、2015 年から 24.54%増加しましたが、エクスプロイトによる攻撃を受けたユーザーの実数は 2015 年から 20.85%減少しました。

攻撃数、ユーザー数/年	2015 年	2016 年	増減率
攻撃をブロックした数	563,888,454	702,026,084	+ 24.54%
攻撃を受けたユーザー数	5,493,568	4,347,966	− 20.85%

図 1：攻撃を受けたユーザーおよび攻撃をブロックした数（2015～2016 年）

このような変化にはいくつかの理由が考えられます。その 1 つは、エクスプロイトの発信元の数が減少したことです。2016 年は、いくつかの大規模なエクスプロイトキット（Neutrino および Angler という名称のエクスプロイトキット）がエクスプロイトのアンダーグラウンドマーケットから消え去りました。このことは、全体的なエクスプロイトを取り巻く状況に大きく影響しました。多くのサイバー犯罪グループがマルウェアを拡散しようとする取り組みを減らしたようです。一方で、ユーザーを感染させようとする平均試行回数は、2015 年から 2016 年にかけて、ユーザー1 人あたり 102 回から 161 回に増加しました。

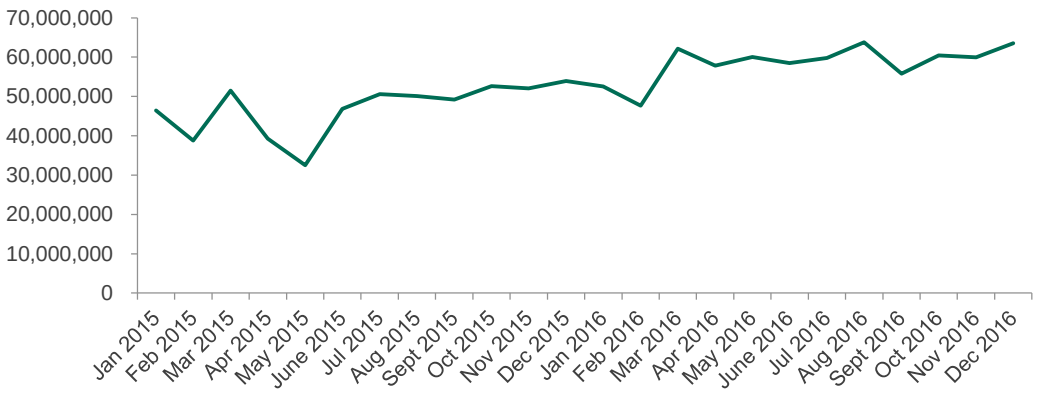

図 2：エクスプロイトによる攻撃総数の増減（2015～2016 年）

つまり、エクスプロイトに遭遇するユーザー数は減少しましたが、ユーザー1 人当たりがエクスプロイトによる攻撃を受ける可能性は上がったということになります。言い換えれば、エクスプロイトによって感染した Web サイトの数や悪意のある添付ファイル付きのスパムメッセージの数は増え続けています。

興味深いことに、エクスプロイト攻撃を受けた企業ユーザーの割合は、2016 年に 6.03 ポイント増加しました。

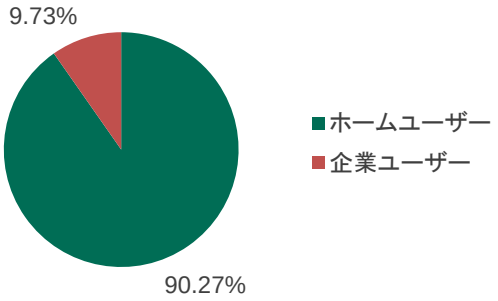

図 3：ユーザーが利用している保護製品の種別を基準とした、エクスプロイトによる攻撃を受けたユーザーの分布（2015 年）

エクスプロイトによる攻撃を受けたユーザーの総数は減少しましたが、これは企業ユーザーには当てはまりません。攻撃者が企業を狙う目的でエクスプロイトを使用する数が増えています。絶対的な数値としては、エクスプロイトに 1 回以上遭遇した企業のマシン数は、2015 年から 2016 年にかけて 28.35%増加しました（538,037 台から 690,557 台へ増加）。

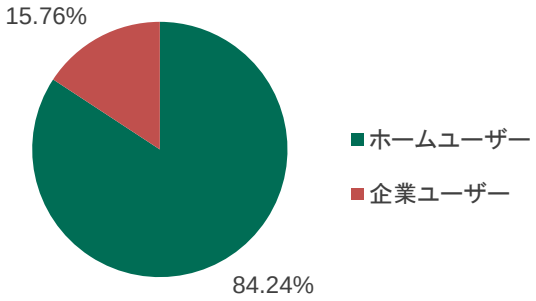

図 4：ユーザーが利用している保護製品の種別を基準とした、エクスプロイトによる攻撃を受けたユーザーの分布（2016 年）

最も攻撃を受けたアプリケーション

実際の攻撃で脆弱性が悪用されたアプリケーションについて見てみると、2015 年はインターネットブラウザーおよび Windows コンポーネントにとって厳しい一年であったことが容易に見てとれます。2016 年、状況は大きく変わりました。おそらく、開発者が懸命に、新しく発見された脆弱性に対する修正プログラムを開発したことにより、ブラウザーおよび Windows のエクスプロイトによる攻撃を受けたユーザーの数は、それぞれ 33.4%、21.56%減少しました。一方で、Microsoft Office ソフトウェア、Adobe Flash、Android の脆弱性を利用したマルウェアによる攻撃を受けたユーザーの数は、それぞれ 102.91%、23.01%、11.61%増加しました。

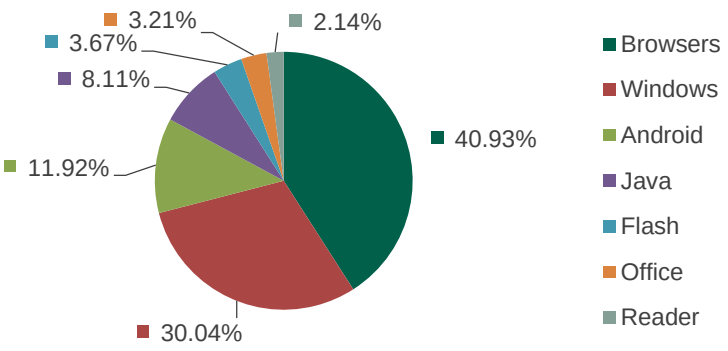

図 5: それぞれのアプリケーションを標的とした、エクスプロイトによる攻撃を受けたユーザーの分布（2015 年）

ブラウザーの割合は、2015 年から 2016 年にかけて 40.93%から 26.95%に減少しました。Windows も 30.04%から 23.3%に減少しています。一方、Android のエクスプロイトによる攻撃を受けたユーザーの割合は、2015 年から 2016 年にかけて 11.92%から 13.15%に増加しました。

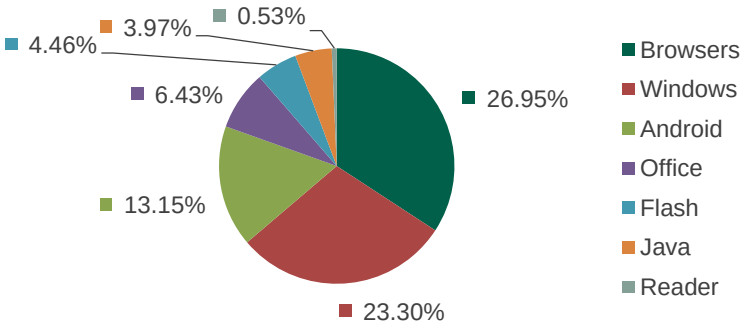

図 6：それぞれのアプリケーションを標的とした、エクスプロイトによる攻撃を受けたユーザーの分布（2016 年）

全体的に、2015 年から 2016 年にかけて、攻撃を受けたユーザーの数は以下のように変化しました。

攻撃を受けたユーザー数	2015 年	2016 年	増減率
ブラウザー	2,310,118	1,538,443	− 33.4%
Windows	1,695,340	1,329,888	− 21.56%
Android	672,609	750,716	+ 11.61%
Java	457,824	226,852	− 50.45%
Flash	206,945	254,561	+ 23.01%
Office	180,953	367,167	+ 102.91%
Reader	120,581	30,431	− 74.76%

図 7：広く普及したアプリケーションおよび OS を標的としたエクスプロイトによる攻撃を受けたユーザー数の変化（2015～2016 年）

攻撃を受けたユーザー数の増減率を見てみると、Office ソフトウェアの脆弱性を突いたエクスプロイトの増加数が圧倒的に多く、約 103%増加し、367,167 人に達しました。一方、Adobe Reader を標的としたエクスプロイトに遭遇したユーザーの数は 2015 年から 2016 年にかけて 74.76%減少しました。Java の数値も大きく減少し、その減少率は 50%を超えています。Windows コンポーネントを標的としたエクスプロイトは 21.56%減少しました。Flash および Android を標的としたエクスプロイトによる攻撃を受けたユーザーの数は、2016 年にそれぞれ 23.01%、11.61%増加しました。

エクスプロイトによる攻撃を受けたユーザー数を母数として、エクスプロイト対象となるアプリケーションの割合分布にも変化が見られました。

以下の時系列グラフに示すとおり、攻撃を受けたユーザー数の面で、Microsoft Office の 2015 年は比較的穏やかでしたが、2016 年 1 月より、その数は急増し始めました。これらのピークの原因として可能性が高いのは、Microsoft Office の CVE-2015-1641 の脆弱性を標的としたエクスプロイトを仕込んだスパムメールが大量に配信されたことです。

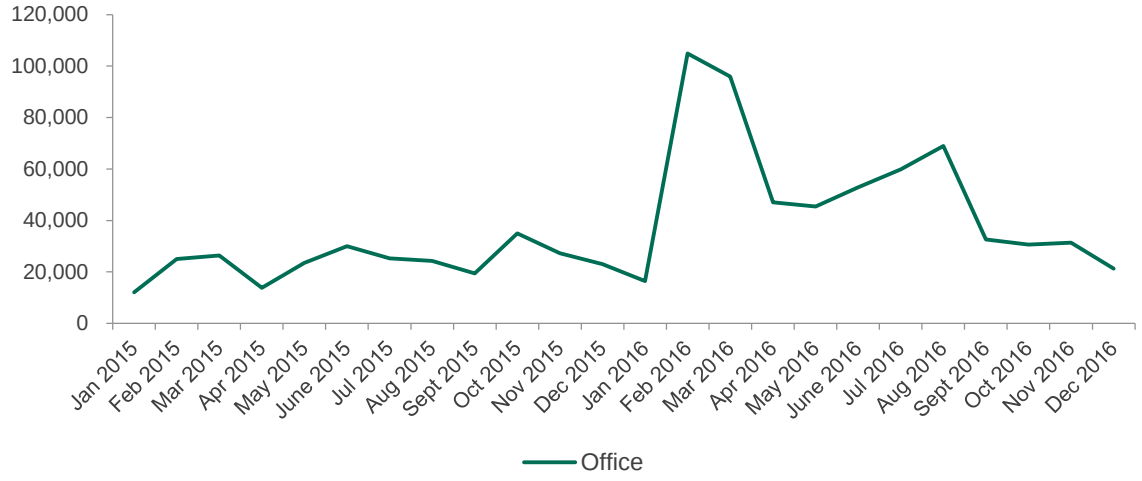

図 8：Office のエクスプロイトによる攻撃を受けたユーザー数の変化（2015～2016 年）

Flash の場合、2015 年 10 月と 2016 年 6 月、7 月が特に厳しい時期で、攻撃を受けたユーザー数の急増が 2 回、これらの月に記録されています。1 回目のピークは Nuclear エクスプロイトキットの活動によるもので、2 回目のピークは Neutrino エクスプロイトキットからエクスプロイトが大量に配信されたことが原因です。

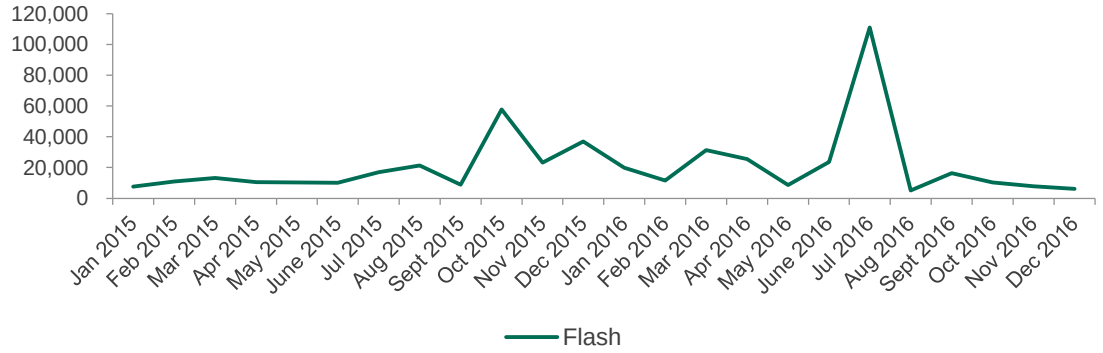

図 9：Flash のエクスプロイトによる攻撃を受けたユーザー数の変化（2015～2016 年）

Android を標的としたエクスプロイトに遭遇したユーザーの数は大きく変化していませんが、ピークが 2015 年 12 月と 2016 年 4 月の 2 回あります。

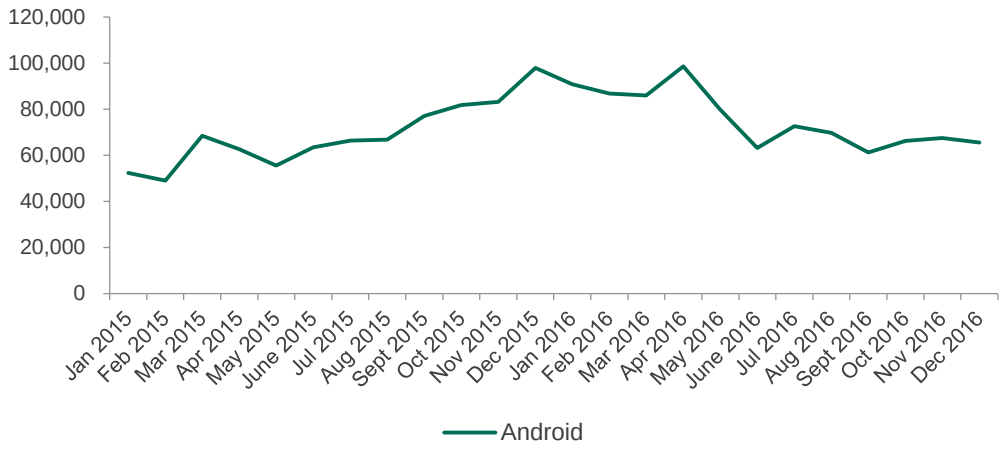

図 10：Android のエクスプロイトによる攻撃を受けたユーザー数の変化（2015～2016 年）

このような変化が発生した正確な原因について断定するのは早計ですが、一般に、攻撃を受けたユーザー数に急増が見られるのにはいくつかの原因があるだろうということは言えます。

まず、新しい脆弱性の発見がこの数値に影響を及ぼします。脆弱性が多く明るみに出るほど、攻撃も増加します。そのほかにも、実効性のあるエクスプロイトが存在し、そのエクスプロイトがエクスプロイトキットに含まれるという要因もあります。エクスプロイトキットの所有者が何らかの重大な脆弱性に対するエクスプロイトを積極的に配信し始めれば、攻撃を受けるユーザー数はすぐに増加し始めます。もう 1 つ原因として可能性があるのが、攻撃でエクスプロイトを利用する悪意のある攻撃者が活動していることです。そのような攻撃者が大規模攻撃を実施した場合、検知数の急増は避けられません。

おそらく、発見された脆弱性の数を概観することで、攻撃を受けるユーザー数の増減の理由について部分的に解明できます。そのために、Kaspersky Lab は自社独自のデータベースと、前述のアプリケーションや OS の一部で発見された脆弱性に関する公開情報を元に、これらの数値が時間とともにどのように移り変わっていったかを調査しました。そのほかの情報源として、ソフトウェアの脆弱性の大半について詳細情報を収集している Web サイト「CVEdetails.com」を参照しました。一般的な数値のほかにも、発見された脆弱性のうち、深刻度が高いもの（スコアが 9 以上）がいくつあるかを調査しました。ほとんどのケースで、深刻度が高い脆弱性は攻撃対象システムのリモートハッキングや完全なセキュリティ侵害を可能にします。

2015 年	合計	深刻度高	深刻度高の脆弱性の割合(%)
Office	40	37	92.5%
ブラウザー	624	240	38.46%
JRE	80	26	32.5%
Flash	329	294	89.36%
Android	125	88	70.4%

図 11:2015 年に頻繁に攻撃を受けたアプリケーションで発見された脆弱性の数(出典:CVEdetails.com および Kaspersky Lab の独自データベース)

2016 年に普及率の高いブラウザー(Google Chrome、Mozilla Firefox、Microsoft Edge、Microsoft Internet Explorer)で発見された脆弱性の数は、2015 年よりも 8.81%減少しました。また、おそらくはエクスプロイトの作成者によって利用されやすい、深刻度が高い脆弱性の割合は、2015 年から 2016 年にかけて 38.46%から 14.76%に減少しました。前述のとおり、ブラウザーのエクスプロイトによる攻撃を受けたユーザーの数も同じ期間で減少しています。

しかし一方で、Microsoft Office 製品内の脆弱性の数は 20%増加し、前述のとおり、Office のエクスプロイトによる攻撃を受けたユーザーの数も増加しました。

2016 年	合計	深刻度高	深刻度高の脆弱性の割合(%)
Office	48	32	66.67%
ブラウザー	569	84	14.76%
JRE	37	13	35.14%
Flash	266	224	84.21%
Android	523	254	48.57%

図 12:2016 年に頻繁に攻撃を受けたアプリケーションで発見された脆弱性の数(出典:CVEdetails.com および Kaspersky Lab の独自データベース)

Android OS では、発見された脆弱性の数が最も劇的に増加しました(2015 年から 2016 年にかけて、125 から 523 に増加)。Kaspersky Lab の脅威に関する統計情報によれば、Android の脆弱性を突いたエクスプロイトによる攻撃を受けたユーザーの割合と、その実数の両方がこの期間に増加しましたが、その増え方は穏やかです。

そもそも、発見された脆弱性の数と攻撃の数には必ずしも相関があるわけではありません。たとえば、Flash の脆弱性を突いたエクスプロイトによる攻撃を受けたユーザーの割合と実数は、2015 年から 2016 年にかけて増加しましたが、その期間に発見された脆弱性の数は減少しています。

それでも、ある特定のアプリケーションで発見された脆弱性の数を概観することは、それぞれのアプリケーションを対象とした潜在的な攻撃について、ある程度明確な理解を与えてくれます。同時に、特定の脆弱性を突いた、広く拡散したエクスプロイトが存在しないかどうかに注目すべきでしょう。

実際に利用されている、広く拡散した脆弱性

前章で確認したとおり、発見された脆弱性の数という面では、潜在的な攻撃対象の数は非常に多いことがかわります。しかし、実際に攻撃に使用されたエクスプロイトの統計情報を見れば、悪用された脆弱性はごくわずかです。ここで重要なことは、一部のケースでは、Kaspersky Lab の統計処理システムに技術的な特性があるため、どの具体的な脆弱性が実際に利用されてきたかに関しては部分的にしか明らかにできないということです。つまり、エクスプロイトの一部の検知名は、単一の脆弱性に対する単一のエクスプロイトを指すのではなく、複数のエクスプロイトをグループ化したものを指しています。エクスプロイトはよく利用されるエクスプロイトキットでの存在に基づいてグループ化されることがあります。また、よくある検知名の例として、別々のエクスプロイトが 1 つのエクスプロイトチェーンを構成していたり、何らかのエクスプロイト技術を共有するような場合があります。

これらの特性を考慮して、2015 年に広く拡散したエクスプロイトは以下のようになります。

エクスプロイトの名称	エクスプロイトとして分類されるマルウェアに遭遇した全ユーザーに対する、特定のエクスプロイトに遭遇したユーザーの割合(%)
CVE-2010-2568	27%
Exploit.AndroidOS.Lotoor (複数のエクスプロイト)	11.02%
Neutrino(複数のエクスプロイト)	4.49%
Angler(複数のエクスプロイト)	3.14%
CVE-2013-2423	2.02%
CVE-2014-3153	1.57%
CVE-2012-0158	1.25%
CVE-2015-1641	0.31%
MSOffice ASLR バイパス (複数のエクスプロイト)	0.07%

図 13:広く拡散したエクスプロイトのリスト(2015 年)

数年連続で、悪名高い Stuxnet でも利用されたショートカットファイル(LNK)の脆弱性 CVE-2010-2568 を突いたエクスプロイトが、このタイプの広く拡散したマルウェアの第 1 位になっています。2015 年には、この 1 年で 1 回以上何らかのエクスプロイト攻撃を受けたユーザーの 27%が、この特定の脆弱性を突いたエクスプロイトに遭遇しました。その理由として考えられるのは、これらのエクスプロイトを利用するマルウェアに自己複製機能があり、脆弱性を持つコンピューターが設置された攻撃先のネットワーク内で、継続的に自らを再作成していることです。この脆弱性については、本レポートの次のパートで詳しく説明します。

第 2 位には Exploit.AndroidOS.Lotoor(CVE-2011-1823、CVE-2012-6422、CVE-2013-2596、CVE-2013-2094 など)が入りました。Exploit.AndroidOS.Lotoor は、攻撃を受けたスマートフォンやタブレットのルート権限を奪取するために利用されるエクスプロイトのグループに付けられた検知名です。2015 年に 1 回以上何らかのエクスプロイトに遭遇したユーザーのうち、10 人に 1 人(11.02%)がこのグループによる脅威に遭遇しました。

第 3 位と第 4 位はそれぞれ、Neutrino（攻撃を受けたユーザーの 4.49%）と Angler（攻撃を受けたユーザーの 3.14%）というエクスプロイトキットです。Neutrino および Angler は、これらのエクスプロイトキットによって広く配信されたエクスプロイトのグループに付けられた共通の検知名です。

Java の CVE-2013-2423 脆弱性を突いたエクスプロイトが第 5 位に入りました（攻撃を受けたユーザーの 2.02%）。この脆弱性については、2013 年 4 月に修正プログラムが出ていますが、エクスプロイトキットの作成者は今でもこの脆弱性を突いたマルウェアを開発し続けています。その理由はおそらく、修正プログラムが入手可能な状態であるにもかかわらず、インターネットに接続している PC の多くが長年アップデートされていないことにあります。

第 6 位に入った CVE-2014-3153 は、Linux OS カーネルの脆弱性であり、Android のマルウェアによって、攻撃対象のデバイスを root 化するために積極的に利用されてきました。2014 年夏に修正プログラムがリリースされましたが、エクスプロイトは未だに有効です。その理由の大部分は、2014 年 6 月以前にリリースされた Android デバイスのほとんどが脆弱なままであることです。これらのデバイスの多くについて、サポート期間が終了しているにもかかわらず、世界中で古い OS バージョンのまま使用されている Android スマートフォンが未だに多いことがあげられます。

もう 1 つの非常に古くからある CVE-2012-0158 という脆弱性を利用するエクスプロイトが、第 7 位に入りました（攻撃を受けたユーザーの 1.25%）。この脆弱性は、Microsoft Office や他の Windows 製品およびコンポーネントに存在します。前述の Java エクスプロイトと同様に、この脆弱性に対しても 2012 年に修正プログラムが提供されましたが、2015 年以降も実際の攻撃で利用されています。

CVE-2015-1641（第 8 位、攻撃を受けたユーザーの 0.31%）も、Microsoft Office の別の重大な脆弱性です。2015 年と 2016 年に、Kaspersky Lab のリサーチャーは、さまざまな悪意のあるペイロードを配信する大規模スパム攻撃で、この脆弱性に関連するエクスプロイトの存在を確認しました。

2015 年のランキングの最終位（攻撃を受けたユーザーの 0.07%）には、Microsoft Office で Windows のアドレス空間をランダムに配置するメモリ保護プロセス（ASLR）をバイパスするテクニックを利用した複数のエクスプロイトが入りました。

全体的に、2015 年の間にこれら 9 つのエクスプロイトに遭遇したユーザーは、1 つ以上のエクスプロイトによる攻撃を受けたすべてのユーザーの 50%以上に達します。

残りの 50%は、名前があまり知られていない数百種類のエクスプロイトに分布しています。興味深いことに、2016 年に広く拡散したエクスプロイトは、前年よりも明らかに少なくなっています。しかし、Web サーフィン中にそれらのエクスプロイトに遭遇したユーザーの数はほぼ同じ(50%をやや超過)でした。

エクスプロイトの名称	エクスプロイトに遭遇したユーザーの割合(%)
CVE-2010-2568	24.68%
Exploit.AndroidOS.Lotoor	15.6%
CVE-2014-3153	3.27%
MSOffice ASLR バイパス	3.1%
CVE-2015-1641	2.6%
CVE-2012-0158	2.45%

図 14:広く拡散したエクスプロイトのリスト(2016 年)

2016 年は、広く拡散したエクスプロイトのランキングで CVE-2010-2568 が再び第 1 位に入ったものの、その規模はやや縮小し、ユーザーの 24.68%がこの脆弱性を突いたエクスプロイトの標的になりました。Neutrino および Angler エクスプロイトキットは上位から消え去りました。これは Kaspersky Lab を含むセキュリティコミュニティによる努力の結果であり、Angler エクスプロイトキットは完全に崩壊し、Neutrino の場合は 2016 年秋に活動量が大きく低下しました。このことが、対応するキットを通じて配信されるエクスプロイトによる攻撃を受けた、ユーザーの総数に影響しました。

第 2 位には、Exploit.AndroidOS.Lotoor が再び入りました。ユーザーの 15.6%がこのグループのエクスプロイトに遭遇しました(2015 年よりも 4.58 ポイント増加)。この増加は、上位から Neutrino と Angler が突如消え去ったことによるものだと考えられますが、Exploit.AndroidOS.Lotoor の増加に影響を及ぼした要因はそれだけではありません。絶対数を見ると、このエクスプロイトによる攻撃を受けたユーザーの数は 2016 年に 12.12%増加しています(2015 年は 605,129 人、2016 年は 678,451 人)。CVE-2014-3153(別の Android の脆弱性)を突いたエクスプロイトによる攻撃を受けたユーザーも、1.57%から 3.27%に増加し、ASLR をバイパスするエクスプロイトグループ(3.1%)、CVE-2015-1641 の Office 脆弱性を突いたエクスプロイト(2.6%)、古い脆弱性の CVE-2012-0158 を突いたエクスプロイト(2.45%)も同じく増加しています。

これら上位リストには入っていませんが、非常に近い位置に 2 つの脆弱性があります。Internet Explorer における CVE-2016-0189 と、Windows のコンポーネントにおける CVE-2014-6332 です。いずれの脆弱性も、エクスプロイトキットの開発者やそれを利用する攻撃者、さらに標的型攻撃グループによって非常に積極的に利用されています。

言い換えれば、よく利用されるエクスプロイトキットと同様に、一部の大規模なエクスプロイトの発信元が 2016 年の脅威を取り巻く状況から消え去りましたが、すぐに他のエクスプロイトによってその空いたスペースが埋められました。一方で、ここで言及しておくべきこととして、エクスプロイトによる攻撃を受けたユーザーの総数は 2016 年に減少しました。これはある程度、Angler および Neutrino エクスプロイトキットの活動量低下によるものです。

前述の広く拡散したエクスプロイトについて、もう 1 つ興味深い点があります。それは、多くのケースで新しく発見された脆弱性の数が大幅に増加している一方、その中で本当の脅威となっているのは比較的少数のグループだけであるということです。発見された脆弱性の大部分が実際の攻撃ではほとんど使用されていないことがわかっています。Kaspersky Lab は、企業のパッチ管理ソリューションを強固にする独自の脆弱性データベースを保有しています。2015 年、このデータベースに 3,234 件の脆弱性情報があり、2016 年にはさらに 1,710 件が追加されました。2017 年 4 月現在、Kaspersky Lab の脆弱性データベースには 5,005 件もの脆弱性情報があります。これらは、企業や家庭の環境において最も頻繁に利用されるアプリケーションに潜む脆弱性です。これらの脆弱性に関する情報源となるのは、各ソフトウェアベンダーや、Kaspersky Lab のリサーチチーム自体を含むセキュリティコミュニティです。

これまでに確認した情報はすべて、既知の脆弱性を標的とした既知のエクスプロイトに関連するものです。一方で、未知の脆弱性を悪用した攻撃も多数存在します。そのようなエクスプロイトは、標的としている脆弱性がソフトウェアベンダーや公開情報としてまだ知られていないという意味で「ゼロデイ」エクスプロイトと呼ばれることもあります。エクスプロイトの脅威を概観して判明したことは、そのような実際に出回っているエクスプロイトに遭遇することはそれほど珍しくないということです。

未知のエクスプロイトを利用した攻撃に関する統計

エクスプロイトの大半は、標準のシグネチャおよび振る舞いによる検知技術によってブロックされます。しかし、そのような障壁をも回避して、すべての防御を突破できるほど高度なエクスプロイトが数パーセント存在します。それらは未知の脆弱性もしくは未知と既知の脆弱性を同時に狙うエクスプロイトで、何重にも難読化されており、多彩なトリックで標準的な保護を切り抜けるものです。カスペルスキー製品によって保護されたコンピューターでは、このようなエクスプロイトは脆弱性攻撃ブロック（Automatic Exploit Prevention: AEP）によって防御されます。脆弱性攻撃ブロックは、ソフトウェアの脆弱性を利用するマルウェアに狙いを絞った技術です。脆弱性攻撃ブロックは最も複雑な、あるいは未知であったエクスプロイトは排除され、Java、Adobe Reader、Flash、Internet Explorer、Microsoft Office などの標的にされやすいプログラムは特に重点を置いて監視します。

これらのプログラムが不審な実行可能ファイルやプログラムコードを起動しようとすると、さらに追加のセキュリティチェックが実行されます。それが正規の実行であったとしても（たとえば、Adobe Reader がアップデート

の確認をするために実行可能ファイルを起動した場合でも)、エクスプロイトの徴候を見逃さないために、ファイルの特性や、起動を試みる前にどのような動作を行ったのか確認します。AEP 技術は、プログラムコードの実行を試みる起点を検知します(この起点はソフトウェア自体から生じている場合も、エクスプロイトの動作が理由である場合もあります)。また、典型的なエクスプロイトの振る舞いに関するデータを利用することで、それがゼロデイ攻撃であったとしても検知します。

ドライブバイダウンロード(悪意のある Web ページにアクセスすると開始される攻撃)などの一部のエクスプロイトでは、実行前に特定の Web サイトからペイロードを読み込みます。脆弱性攻撃ブロックは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と、このファイルをダウンロードした URL を特定します。また、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します。不審なプログラムコードの起動が試みられると、この情報を利用してエクスプロイトの動作を特定し、これをブロックすることができます。

Kaspersky Lab の AEP は、ユーザーを高度なエクスプロイトから保護するだけでなく、未知のエクスプロイトや難読化されたエクスプロイトによる攻撃についての統計的な分析を可能にします。

この統計を基に、2016 年にコンピューターを感染させようとする試みの回数は 2015 年から 96.75%増加し、ブロックされた感染の試みが 2140 万回を超えたことがわかりました。同時に、これらの技術によって保護されたユーザーの数は 6.79%増加し、297,000 人以上に達しました。

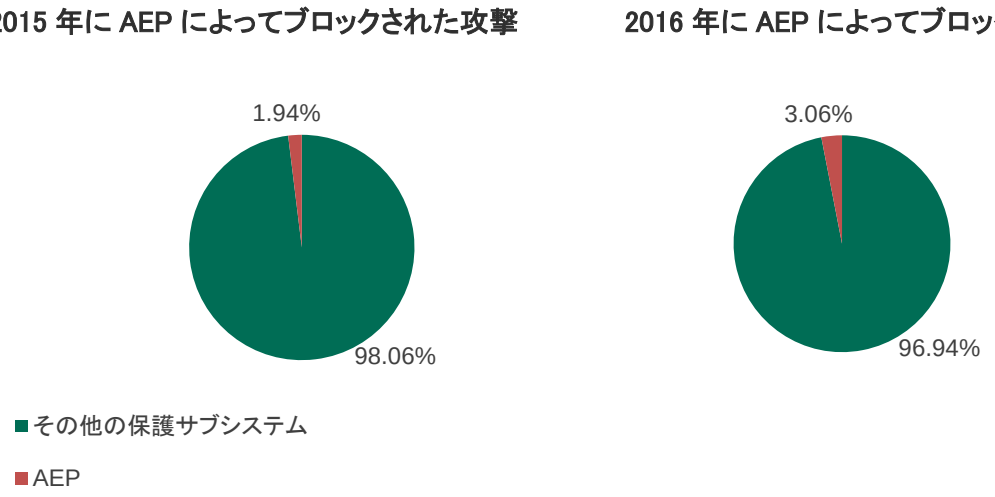

図 15：AEP によってブロックされた攻撃の割合の変化（2015～2016 年）

AEP の技術的な特性から、この攻撃数の増加の原因となったエクスプロイトの正確な特定は困難です。しかし、過去 2 年にわたって、エクスプロイトキットを利用してマルウェア、特にランサムウェアを配信する、大規模な攻撃キャンペーンを Kaspersky Lab は頻繁に確認してきました。本レポートですでに示した Neutrino と Angler が代表的な 2 つです。Neutrino と Angler の所有者は多大なリソースを新しいエクスプロイトの開発に費やして、アンダーグラウンドマーケットに手の込んだ悪意のあるツールを数多く送り込みました。これらのツールはマルウェア配信に関わる複数のグループによって積極的に利用されています。攻撃に偏りが出た主な理由の 1 つにはこのような大規模攻撃がある可能性があります。

これにより、2016 年に AEP によってブロックされた攻撃の割合は、1.12 パーセント増加しました。また、未知のエクスプロイトに遭遇したユーザーの割合も 1.78 パーセント増加しました。

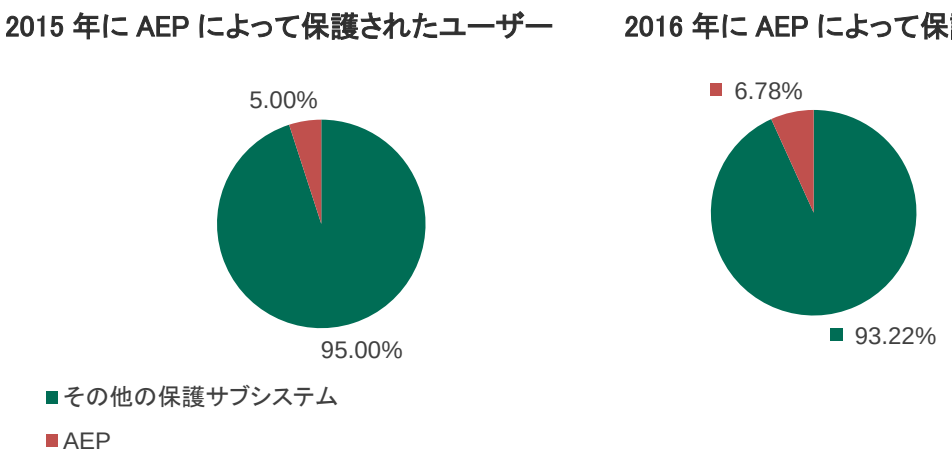

図 16：未知のエクスプロイトによる攻撃を受け、AEP によって保護されたユーザーの割合の変化（2015～2016 年）

この統計が示すように、未知のエクスプロイトによる攻撃の割合は比較的低いことがわかります。この結果から、攻撃者は多くの場合、高度なエクスプロイト開発に手が出せないことを意味しています。そのため、普及率の高いアプリケーションに存在する脆弱性を経由した攻撃は、検知される可能性が高くなります。一般のユーザーや組織がエクスプロイトに対する防御技術を備えるセキュリティ製品を利用する場合は、それにより確実に保護されます。しかし、高度な脆弱性攻撃を実際に悪用できる攻撃者についてはどうでしょうか。

パート 2：エクスプロイトと標的型脅威グループ

多くの攻撃者に利用されるエクスプロイトキットを作成するグループと並んで、標的型攻撃の脅威グループも熱心な脆弱性の利用者であり、概して脆弱性を利用するための資金とスキルの両方を持っています。その主な目的は、サイバースパイ活動、サイバー破壊工作、そしてデータや金銭の窃取です。標的型攻撃の実行者は、普及率の高いアプリケーション内の脆弱性を利用して、防御手段を突破し悪意のあるツールを送り込んでコンピューターを乗っ取るといった攻撃をします。

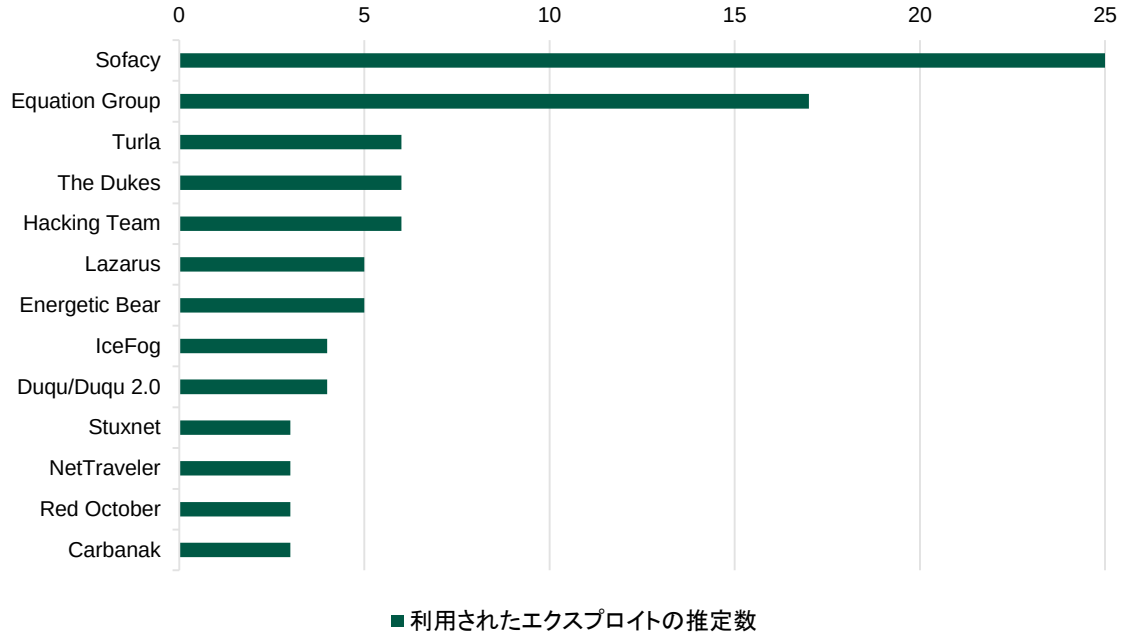

図 17：さまざまなサイバースパイ活動、サイバー破壊工作、高度なサイバー犯罪のグループによって利用されたエクスプロイトの概数（2010～2016 年）

脅威グループによって利用された脆弱性のほとんどは、Microsoft（Windows または Office）、Adobe Flash、および Java に由来しています。

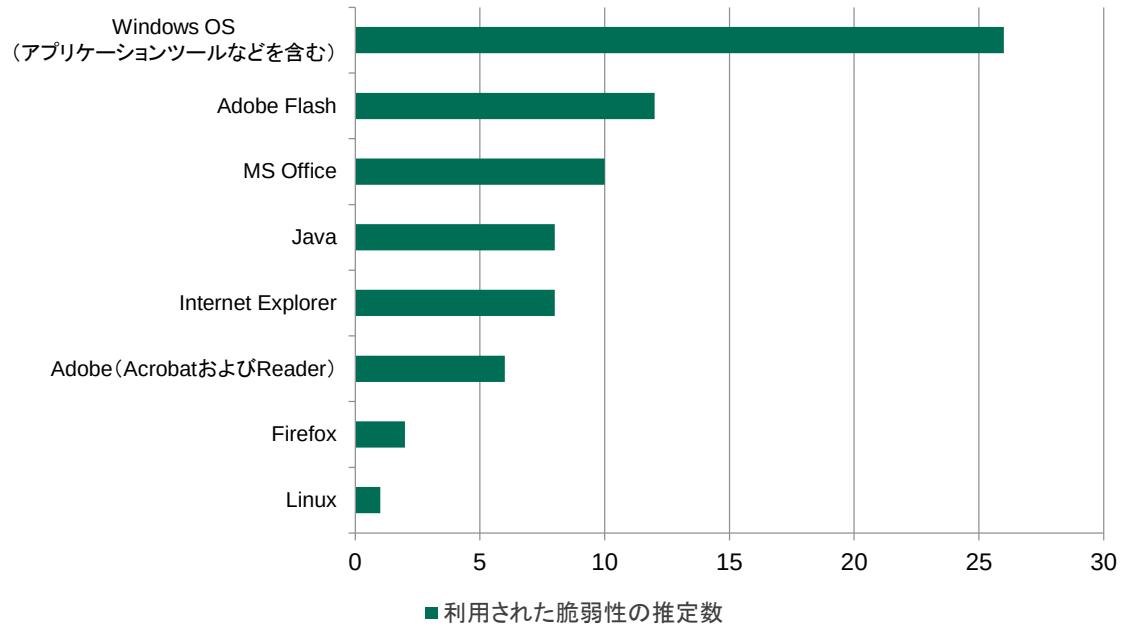

図 18：標的型攻撃グループによって頻繁に利用されたアプリケーション

脅威グループのお気に入りのバグ

最もよく利用される：CVE-2012-0158

Kaspersky Lab が発見、報告した中で、標的型攻撃グループが最もよく利用した脆弱性が CVE-2012-0158 です。Microsoft Office Rich Text Format（RTF）の脆弱性であり、2012 年に発見され修正プログラムが提供されていますが、4 年が経過しても APT 攻撃によって利用され続けています。このように長く続いている理由は主に、広く普及している Office エクスプロイトキットに組み込まれていることです。ただし、この脆弱性によって侵害されうるコンピューターの数は減少してきており、ヨーロッパと北米ではわずか 15%までになりました。それでも、アジアおよびロシア/ウクライナの半数のコンピューターが無許可でアクセスできる状態で、高度な標的型攻撃では CVE-2012-0158 が今も有効です。これらの地域に的を絞っている大規模な脅威グループが、サイバースパイ操作用に作ったスピアフィッシングの文書内で、この脆弱性を広く利用してきました。その攻撃では、政府機関、外交機関、軍事機関などの非常に機密性の高い組織を狙っています。

そのような脅威グループには、Red October、NetTraveler、サイバー傭兵グループの IceFog（2011～2013 年）、Cloud Atlas（2014 年）、史上初といわれる APT 犯罪である Carbanak、Sofacy、SpringDragon、Dropping Elephant（2016 年まで）が含まれます。これらについては後ほど詳しく説明します。

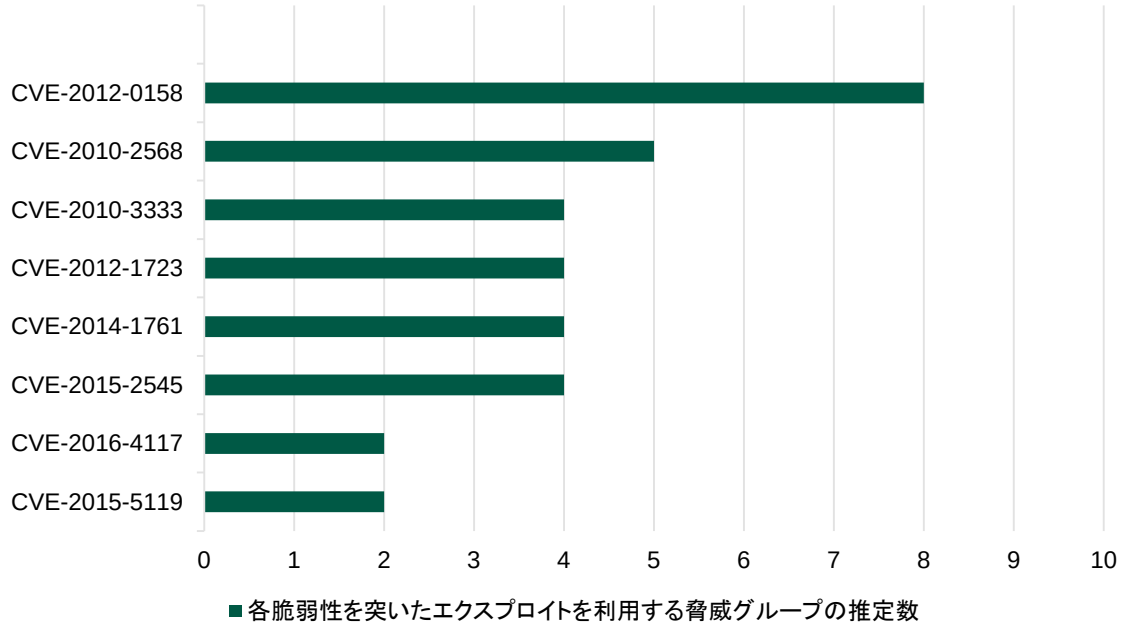

図 19：標的型攻撃グループによって利用された上位の脆弱性（2010～2016 年）

悪名高い Stuxnet ワーム：CVE-2010-2568

2010 年に、Microsoft Windows がショートカットリンク（LNK）を処理する方法に、ゼロデイのセキュリティ脆弱性が発見され、この脆弱性は他の 3 つのゼロデイと並んで、悪名高い Stuxnet ワームによって USB スティックを介してイランの核システムを攻撃するために利用されました。Microsoft によって迅速に修正プログラムが提供されましたが、この脆弱性は中国語圏の脅威グループである Naikon（2009 年以降）によって、極東地域の企業や地政学的団体に対するサイバースパイ攻撃を仕掛けるために利用されました。また、Gauss（2011 年）でも使われています。Gauss は、国家の出資を受けて開発された銀行系トロイの木馬/サイバー監視 APT であるとみられ、レバノン、シリア、イスラエル、パレスチナの特定の個人を標的としていました。

実際には、この LNK の脆弱性を利用したのは Stuxnet が最初ではありません。2001 年から活動する、大規模で複雑な英語圏サイバースパイ脅威グループである Equation Group が、2008 年にこの脆弱性を利用していたことがわかっています。

Stuxnet の分析中に、Kaspersky Lab のリサーチャーは「Zlob」という実行可能なワームを発見しましたが、そのファイルには「fanny.bmp」という名前が付けられていました。数年後、Equation Group の調査中に、再び Fanny を発見しました。これは、Stuxnet LNK エクスプロイトを利用して複製を行うワームで、2008 年に作成されたものです。リサーチャーは、Fanny が 2 つのゼロデイエクスプロイトを利用していることを確認しました。こ

れらは後で Stuxnet に、2009 年 6 月と 2010 年 3 月に追加されています。つまり、Stuxnet グループの数年前に、Equation がこれらのゼロデイ(およびその他のエクスプロイト)にアクセスしたことになります。

CVE-2010-2568 の話はこれで終わりではありません。2012 年、奇妙なメールがセキュリティリサーチャーに届きました。このメールには、Hacking Team まで遡ることが可能な悪意のあるコードの詳細が含まれていました。Hacking Team は、政府にスパイウェアを提供する、物議を醸している「攻撃的セキュリティ」組織です。このコードは、Hacking Team の主要製品、Remote Control Systems(RCS)の一部になっていました。Kaspersky Lab の分析によって、CVE-2010-2568 が RCS に組み込まれ、USB ドライブを介して自己複製ができる状態であることがわかりました。

Microsoft は最終的に、この CVE の脆弱なコードパスの最後を 2015 年 3 月に修正しました。

第 2 の RTF 脆弱性:CVE-2010-3333

長く続いているもう 1 つの脆弱性が CVE-2010-3333(Microsoft Office RTF のスタックバッファオーバーフローの脆弱性)です。2010 年 11 月に修正プログラムがリリースされたにもかかわらず、標的型攻撃者によって利用され続け、2016 年もまだ悪用されている兆候があります。

Hacking Team はこの脆弱性を利用して、攻撃を受けたコンピューターに RCS をインストールしました。Red October(東ヨーロッパ、旧ソ連、中央アジアの外交機関、政府機関、科学研究機関を標的とする大規模なサイバースパイネットワーク)も、2012 年以降この脆弱性を利用しています。この脆弱性を利用した他の標的型攻撃グループには、NetTraveler(2004 年から活動する中国語圏のサイバースパイ脅威グループで、主にロシアやインドなどの地域でチベット/ウイグル人の活動や科学研究機関を標的としている)や、Sofacy(別名 APT28、Fancy Bear)などがいます。

ここ何年かは、主に NATO 諸国を標的とするロシア語圏の脅威グループである Sofacy が活動を活発化しており、多用され、機敏で、活動的な脅威グループの 1 つになっています。2008 年に出現して以来、Sofacy は 25 を超える脆弱性を展開してきたとみられ、ペースを弱める兆候はほとんど見られません。

Java コーヒーのテイクアウト:CVE-2012-1723

標的型脅威グループが攻撃に利用できるバグの観点から見ると、Microsoft(Office および Windows プラットフォーム)と Adobe の次に脆弱なアプリケーションが Java です。CVE-2012-1723 の脆弱性によって、マルウェアが JRE(Java Runtime Environment)サンドボックスに侵入して、悪意のあるアクションを実行するように

作られた追加の Java クラスをロードできるようになります。このマルウェアは 2012 年に Blackhole Exploit Kit に組み込まれました。また、標的となったユーザーを、感染している Web サイトに誘導する水飲み場型攻撃でよく利用されています。

この脆弱性を利用してきた大規模な脅威グループは、IceFog、Equation Group のほか、Energetic Bear/Crouching Yeti（2010 年以降、米国、ヨーロッパ、中国で産業機械セクターを標的としている APT）、および Turla（40 か国以上の機密性の高い政府機関や研究機関を標的とする大規模なロシア語圏のサイバースパイ活動）です。

リッチテキストの亀裂がここにも：CVE-2014-1761

CVE-2014-1761 は、2014 年 3 月にゼロデイとして発見された Word の脆弱性です。ユーザーが感染後の Microsoft Word バージョンを使用して特別に作られた RTF ファイルを開くか、Microsoft Word をメールビューワとして使用中に特別に作られた RTF メールメッセージを Microsoft Outlook で開くと、リモートコード実行が可能になるというものです。

この脆弱性を利用してきた標的型攻撃者に、Energetic Bear/Crouching Yeti、Carbanak、Sofacy、および The Dukes が挙げられます。The Dukes は、複雑に絡み合う、異質だけれども関連性を持ったロシア語圏の脅威グループ達で、しばしば同時に活動し、米国、ドイツ、韓国、ウズベキスタンの政府機関および企業を標的としており、さらにはホワイトハウスや米国務省も標的であったと言われています。

CVE-2012-0158 の王座に対抗：CVE-2015-2545

CVE-2015-2545 は、2015 年に発見されて修正プログラムが提供された Microsoft Office の脆弱性です。攻撃者が特別に作った EPS 画像ファイルを使用して任意のコードを実行できるようになります。

このエクスプロイトは 2015 年 8 月に発見されました。その時は、Platinum グループによる標的型攻撃で利用されており、この攻撃はインドを標的にしたものと推測されます。その後数か月で、この脆弱性を利用して攻撃を受けたマシンの防御手段を突破する脅威グループが急増しました。その攻撃者と主な標的のほぼすべてが東南アジア、中央アジア、極東にあります。

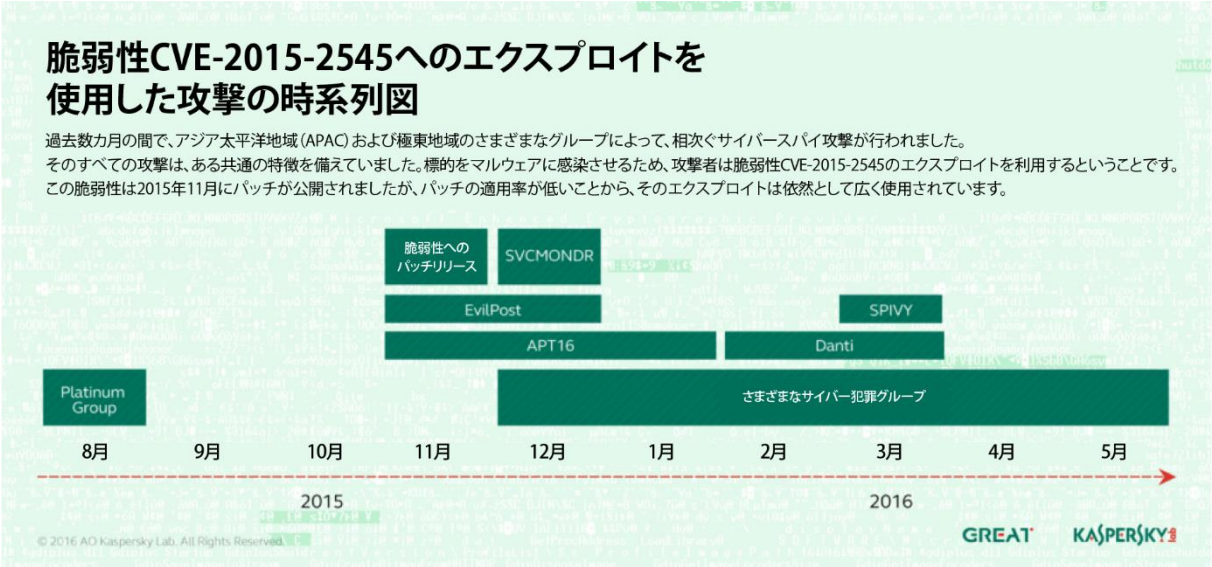

図 20：CVE-2015-2545 の脆弱性を突いたエクスプロイトを利用する攻撃

たとえば、Platinum の後、この脆弱性を突いた修正済みのエクスプロイトが APT16 によって利用されました。APT16 は、通信社を標的とする脅威グループで、中国語話者が関わっているとみられています。その後の 2015 年 12 月、Kaspersky Lab は、この脆弱性を利用して日本の防衛部門を標的とする EvilPost を発見しました。2016 年の春には SPIVY が登場しました。SPIVY は、香港の標的に対するスピアフィッシング攻撃で、この脆弱性を利用していました。

この脆弱性を利用する他の 2 つのグループについても、紹介する価値があります。1 つは Danti です。以前には知られていなかったグループで、おそらく NetTraveler に関連していますが、このグループは 2016 年の初めに、主にインドの外交機関に対する標的型攻撃でこの脆弱性を利用しました。もう 1 つは SVCMONDR です。このグループは 2015 年の終わりに、台湾のセキュリティソフトウェア再販業者を標的として、この脆弱性を利用しました。

トップの Flash ゼロデイ：CVE-2016-4117

このトップクラスの Adobe Flash ゼロデイは、2016 年に発見されました。この脆弱性は Scarcruft として知られる脅威グループによる水飲み場型攻撃で利用されています。Scarcruft は、比較的新しい標的型攻撃グループであり、攻撃を受けたマシンはロシア、ネパール、韓国、中国、インド、クウェート、ルーマニアにわたります。また、この脆弱性は Sofacy にも利用されています。

次に来る存在：CVE-2015-5119

Flash ゼロデイである CVE-2015-5119 は、2015 年の Hacking Team のデータ漏洩によって知られました。この脆弱性は Hacking Team によって、サイバー監視用のシステムに侵入するために利用されていました。Adobe はユーザーに対して、この脆弱性によりクラッシュが起きる可能性があること、および感染したシステムを攻撃者が乗っ取る可能性があることを警告しました。当然のことながら、ほかの攻撃者はこの漏洩から数時間以内に、新しい脆弱性の利用を始めました。攻撃グループの 1 つは、日本のさまざまな業種や政府機関を標的とした脅威グループの BlueTermite です。2013 年から活動するこの脅威グループの主な感染手段はスピアフィッシングメールですが、2015 年 8 月までには、CVE-2015-5119 を利用するドライブバイダウンロードを使用するようになりました。

Sofacy もこの脆弱性を利用しており、2015 年にはわずか 4 か月の期間に 6 つのゼロデイを送り込みました。そのうちの 5 つは Sofacy の組織内で作成され、6 つ目は CVE-2015-5119 が書き換えられたもので、リーク後わずか 24 時間で利用に至っています。

例外的存在：Lazarus Group

大型の標的型攻撃グループの中で、後 1 つの名前が残っています。それは Lazarus Group で、破壊的なワイパー攻撃やサイバースパイ活動を行う、特に悪意のある脅威グループです。2009 年から活動している Lazarus Group は、主に北米、南米および中東、極東を標的としており、2014 年の Sony Pictures Entertainment に対する悪名高い攻撃や近年の金融サービスへの攻撃で暗躍していると考えられています。このグループは数年かけて複数のツールを展開し、それには、CVE-2015-6585（韓国のワードプロセッシングアプリケーション「Hangul WP」を利用したゼロデイ脆弱性）を利用するスピアフィッシング攻撃が含まれます。

また、このグループは多数の新しい Adobe Flash の脆弱性や、謎めいた Microsoft Silverlight ゼロデイの CVE-2016-0034 を利用してきました。そのような Adobe Flash の脆弱性には、CVE-2016-4117（Sofacy も利用）、CVE-2015-8651（広く利用されている Angler Exploit Kit に組み込まれている）、CVE-2016-1019（Magnitude Exploit Kit に組み込まれている）などがあります。

2010 年から 2016 年までに Kaspersky Lab が報告した 35 以上の標的型攻撃グループおよび攻撃が保持、利用、再利用した脆弱性は 80 を超えます。その中にはゼロデイもあれば何年も存続しているものもあり、約 3 分の 2 が複数の脅威グループで利用されています。

結論とアドバイス

これまで述べてきたように、普及率の高いアプリケーションやオペレーティングシステム内のエクスプロイトは非常に重大なセキュリティ上の問題であり、世界中の何百万というホームユーザーおよび企業ユーザーにとって現実の脅威となっています。エクスプロイトは悪意のあるペイロードを配信する効果的なツールであるため、サイバー犯罪者グループ、標的型のサイバースパイ活動グループ、サイバー破壊工作グループなど、あらゆる悪意あるユーザーの間で高い需要があります。この問題の別の側面として、普及率の高いソフトウェアの開発者が製品のバグの発見や除去、およびエクスプロイトの軽減策に対して多大なリソースを投じていても、少なくとも予見可能な将来には脆弱性の困難が続くとみられます。

エクスプロイトを介した攻撃から、個人データやビジネスのデータを保護するためのアドバイスをお伝えします。

- PC にインストールされているソフトウェアを常に最新の状態に保ち、自動アップデート機能があれば有効にする。
- 可能な限り、脆弱性の問題に責任ある対応を示すソフトウェアベンダーを選択する。ソフトウェアベンダーが自社独自のバグ発見報奨金プログラムを設けているかどうかを確認する。
- PC のネットワークを管理している場合、管理下の全エンドポイントのソフトウェアを一元アップデートできるパッチ管理ソリューションを利用する。
- 組織の IT インフラストラクチャの定期的なセキュリティ評価を実施する。
- エクスプロイトに感染した文書を開いたり、リンクをクリックさせるために利用されることの多いソーシャルエンジニアリングについて、社員教育をおこなう。
- エクスプロイトに特化した防御機構を備えるセキュリティ製品か、少なくとも振る舞いベースの検知技術を持つ製品を利用する。
- エクスプロイトを含むサイバー脅威からの保護に、多層型アプローチを採用しているベンダーを選ぶ。