KASPERSKY lab

Kaspersky Security Bulletin 2015

2015年 脅威の統計概要

GREAT

目次

数字で見る2015年 3
サイバー攻撃で使用された脆弱なアプリケーション 4
金融機関におけるオンラインの脅威 6
攻撃の地理的分布 7
バンキング型マルウェアの上位10ファミリー 8
ランサムウェアの興味深い動向 10
攻撃を受けたユーザー数 10
TROJAN-RANSOMの上位10ファミリー 11
TROJAN-RANSOMマルウェアの攻撃を受けた上位10か国 12
暗号化プログラム 13
新しいTROJAN-RANSOM暗号化プログラムの数 13
暗号化プログラムの攻撃を受けたユーザーの数 13
暗号化プログラムの攻撃を受けた上位10か国 14
オンラインの脅威（WEBベースの攻撃） 15
オンラインで検知された悪意あるオブジェクト上位20種 15
オンラインリソースにマルウェアが仕掛けられた上位10か国 17
ユーザーのオンライン感染のリスクが高い国 18
ローカルの脅威 21
ユーザーのコンピューター上で検知された悪意あるオブジェクトの上位20種 21
ユーザーのローカル感染のリスクが高い国 23
まとめ 26

本書に掲載された統計はすべて、Kaspersky Security Network（KSN）で取得されたものです。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分散型アンチウイルスネットワークで、すべての情報はカスペルスキー製品ユーザーの同意を得て収集されています。KSNには全世界で数百万の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。

統計データは、2014年11月から2015年10月までのものです。

数字で見る2015年

- オンラインバンキング口座から金銭を窃取するマルウェアを感染させようとする試みを、1,966,324台のコンピューターでブロックしました。
- 753,684台のコンピューターからランサムウェアプログラムが検知されました。そのうち、暗号化ランサムウェアの標的となったコンピューターは、179,209台に上りました。
- カスペルスキーのウェブアンチウイルス製品は、121,262,075種類の悪意あるオブジェクト（スクリプト、エクスプロイト、実行可能ファイルなど）を検知しました。
- カスペルスキー製品は、世界各地のオンラインリソースから実行された798,113,087件の攻撃をブロックしました。
- ユーザーのコンピューターの34.2%が、1年間で少なくとも1回のWeb攻撃を受けました。
- サイバー犯罪者が攻撃に使用したユニークホスト数は、6,563,145台でした。
- カスペルスキー製品によって無害化されたWeb攻撃のうち、24%は米国内の悪意あるWebリソースを使用して実行されていました。
- カスペルスキーのアンチウイルス製品は、合計4,000,000種類の悪意あるオブジェクトと不審なオブジェクトを検知しました。

サイバー攻撃で使用された脆弱なアプリケーション

2015年は、新たな手法でエクスプロイト、シェルコードやペイロードを隠し、感染の検知と悪意あるコードの分析を困難にしているケースが確認されました。サイバー犯罪者が実際に使った手法には次のようなものがあります。

- ディフィー・ヘルマン暗号化プロトコルを使用
- Flashオブジェクト内にエクスプロイトパックを隠蔽

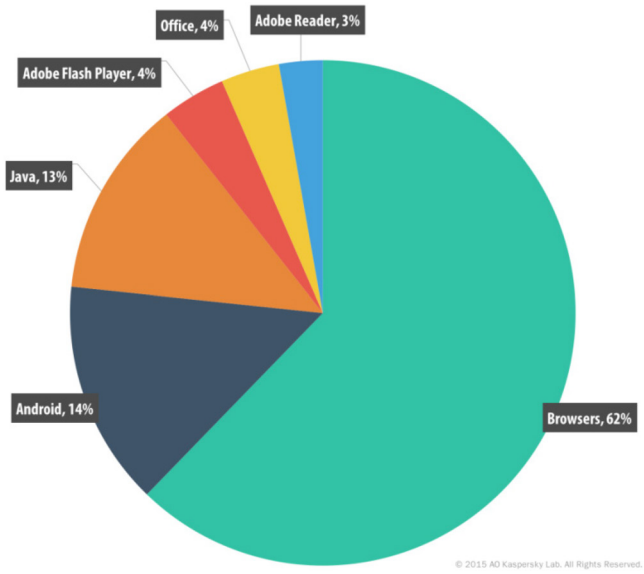
2015年の特筆すべき出来事の1つは、同じ系統の重大な脆弱性が2件、Androidで検知されたことです。攻撃者がStagefrightの脆弱性を悪用した場合、特殊な細工を施したMMSを被害者の電話番号に送り付けるだけで、リモートからそのデバイス上で任意のコードを実行できるようになります。Stagefright 2を悪用する場合も同様ですが、こちらは特殊な細工を施したメディアファイルを使用します。

Adobe Flash Playerのエクスプロイトは、この1年で多くのマルウェアで利用されました。その理由は、年間を通じてこの製品で多数の脆弱性が見つかったことから説明がつきます。また、Hacking Team社がデータ侵害を受けたことによって明らかになった、Flash Playerの未知の脆弱性に関する情報がサイバー犯罪者によって悪用されました。

エクスプロイトパックの開発者は、Adobe Flash Playerの新たな脆弱性が公表されるとすぐに反応し、新しいエクスプロイトを自らの製品に追加しました。次に挙げるのは、「悪魔の1ダース」と呼ばれるAdobe Flash Playerの脆弱性です。これらの脆弱性はサイバー犯罪者の間で流行し、一般的なエクスプロイトパックに追加されました。

1) CVE-2015-0310
2) CVE-2015-0311
3) CVE-2015-0313
4) CVE-2015-0336
5) CVE-2015-0359
6) CVE-2015-3090
7) CVE-2015-3104
8) CVE-2015-3105
9) CVE-2015-3113
10) CVE-2015-5119
11) CVE-2015-5122
12) CVE-2015-5560
13) CVE-2015-7645

有名なエクスプロイトパックの中には、以前からInternet Explorerの脆弱性（CVE-2015-2419）を悪用するエクスプロイトを含むものがありました。また、2015年には、Microsoft Silverlightの脆弱性（CVE-2015-1671）を使用してユーザーに感染したケースも確認されました。ただし、このエクスプロイトは、エクスプロイト市場の主要な「プレーヤー」の間ではあまり使われていません。



サイバー攻撃で使用されたエクスプロイトのアプリケーション種類別の分布（2015年）

カスペルスキー製品がブロックしたエクスプロイトに関するデータに基づいて、脆弱なアプリケーションを分類しました。これらのエクスプロイトは、オンライン攻撃やローカルアプリケーション（モバイルデバイス上のアプリを含む）への感染に使用されました。

この分類では、Adobe Flash Playerエクスプロイトの割合は4%にとどまりましたが、実環境ではかなり普及しています。この統計で留意すべきは、弊社のテクノロジーがさまざまな段階でエクスプロイトを検知している点です。エクスプロイトとして機能するランディングページの検知は、ブラウザーのカテゴリ（62%）に含まれており、こうしたページで最もよく利用されるのはAdobe Flash Playerのエクスプロイトでした。

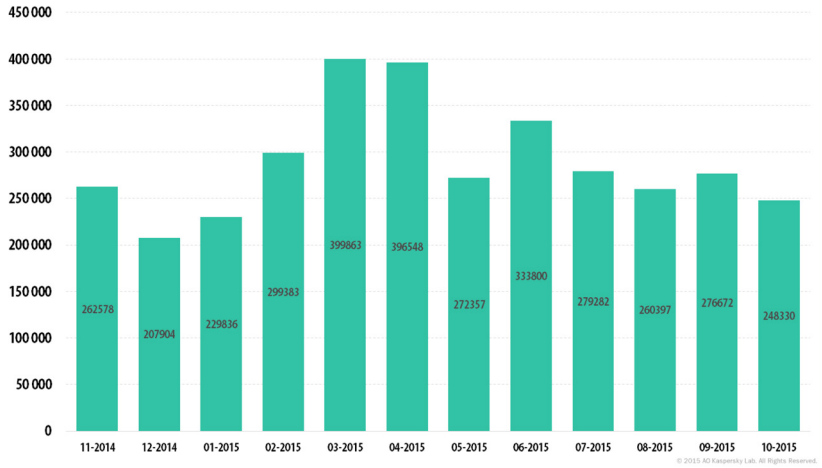
Javaエクスプロイトを使用した事例の数は、この1年で減少しています。2014年後半、ブロックされた全エクスプロイトに占めるJavaエクスプロイトの割合は45%でしたが、この1年でこの割合は徐々に減少し、32ポイント減の13%まで低下しました。さらに、Javaエクスプロイトは主なエクスプロイトパックからすべて削除されています。

その一方で、Microsoft Officeエクスプロイトの割合が1%から4%に増加しています。弊社の調査によると、2015年にこれらのエクスプロイトはマスメール経由で配信されました。

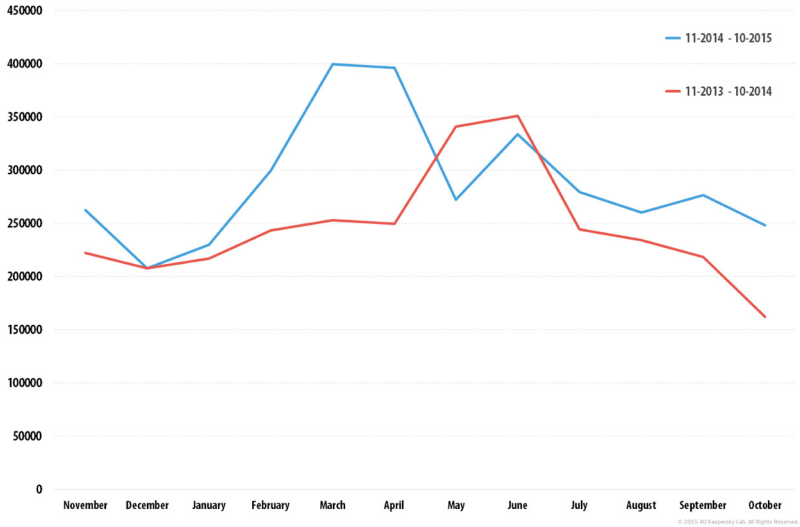
金融機関におけるオンラインの脅威

このセクションでの統計は、アンチウイルスモジュールから返された検知判定に基づいており、統計データの提供に同意したカスペルスキー製品ユーザーから取得したものです。

2015年、カスペルスキー製品は、オンラインバンキング口座から金銭を窃取するマルウェアを実行しようとする試みを1,966,324台のコンピューターでブロックしました。この数値は2014年（1,910,520台）を2.8%上回っています。



金融系マルウェアの攻撃を受けたユーザー数（2014年11月から2015年10月）

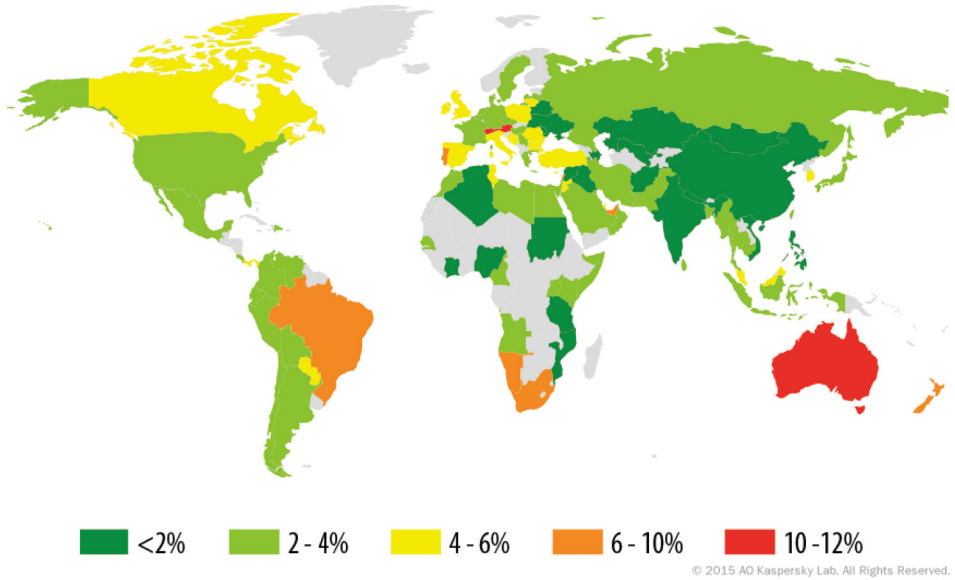


金融系マルウェアの攻撃を受けたユーザー数（2014年と2015年）

2015年、攻撃の数は2月から4月まで徐々に増加し、3月から4月にかけてピークを迎えました。また、6月にも急増しています。2014年に金融系マルウェアの攻撃が多かったのは5月と6月です。両年とも6月から10月にかけては、攻撃を受けたユーザー数が少しずつ減少しています。

攻撃の地理的分布

サイバー犯罪者における金融系マルウェアの流行度と、世界中のユーザーのコンピューターがバンキング型トロイの木馬に感染するリスクを評価するため、カスペルスキー製品の全ユーザーの中で、レポート期間中にこの種の脅威に遭遇したユーザーが占める割合を国別に算出しました。



2015年のバンキング型マルウェア攻撃の地理的分布（マルウェア攻撃を受けた全ユーザー数に対し、バンキング型トロイの木馬の攻撃を受けたユーザー数が占める割合）

攻撃を受けたユーザーの割合が高い上位10か国

	国*	攻撃を受けたユーザーの割合（%）**
1	シンガポール	11.6
2	オーストリア	10.6
3	スイス	10.6
4	オーストラリア	10.1
5	ニュージーランド	10.0
6	ブラジル	9.8
7	ナミビア	9.3
8	香港	9.0
9	南アフリカ共和国	8.2
10	レバノン	6.6

* カスペルスキー製品のユーザー数が比較的少ない（10,000未満）国は除外。
** バンキング型マルウェアの攻撃を受けたコンピューターのユニークユーザー数を、その国のカスペルスキー製品の全ユニークユーザー数で割った値。

最も数値が高かったのはシンガポールです。マルウェア攻撃を受けた同国のカスペルスキー製品の全ユーザーのうち11.6%が、この1年で少なくとも1回、バンキング型トロイの木馬の標的になっています。これは、シンガポールの全脅威の中で、金融系の脅威が流行していることを示しています。

スペインでは、2015年に1回以上バンキング型トロイの木馬の攻撃を受けたユーザーは5.4%でした。各国の数値はイタリアが5%、英国が5.1%、ドイツが3.8%、フランスが2.9%、米国が3.2%、日本が2.5%でした。

ロシアでバンキング型トロイの木馬の標的となったユーザーは、2%でした。

バンキング型マルウェアの上位10ファミリー

2015年に、オンラインバンキングのユーザーに対する攻撃で最も多く使用されたマルウェアの上位10ファミリーを下表に示します（攻撃されたユーザーの割合）。

	検知名*	攻撃されたユーザーの割合 (%) **
1	Trojan-Downloader.Win32.Upatre	42.36
2	Trojan-Spy.Win32.Zbot	26.38
3	Trojan-Banker.Win32.ChePro	9.22
4	Trojan-Banker.Win32.Shiotob	5.10
5	Trojan-Banker.Win32.Banbra	3.51
6	Trojan-Banker.Win32.Caphaw	3.14
7	Trojan-Banker.AndroidOS.Faketoken	2.76
8	Trojan-Banker.AndroidOS.Marcher	2.41
9	Trojan-Banker.Win32.Tinba	2.05
10	Trojan-Banker.JS.Agent	1.88

* ここでの統計は、カスペルスキー製品から返された検知判定に基づいており、統計データの提供に同意したカスペルスキー製品ユーザーから取得したものです。
**金融系マルウェアの攻撃を受けたコンピューターのユニークユーザー数を、マルウェアの攻撃を受けた全ユニークユーザー数で割った値。

上位10位までのマルウェアの大半は、ブラウザーに表示されるWebページにランダムHTMLコードを注入し、ユーザーが元のWebフォームや挿入されたWebフォームに入力した決済データを傍受します。

Trojan-Downloader.Win32.Upatreファミリーは、年間を通じてランキングの1位でした。このマルウェアのサイズは3.5KB以下であり、役割は標的のコンピューターにペイロードをダウンロードするだけです。大半は、ユーザーの決済情報を盗み出すことを目的とするバンキング型トロイの木馬であるDyre/Dyzap/Dyrezaファミリーをダウンロードします。Dyreは、標的のブラウザーとオンラインバンキング用Webアプリとの間のバンキングセッションからデータを傍受する手法、つまりマンインザブラウザー（MITB）攻撃を使って決済情報を窃取します。このマルウェアは、ダウンローダーが仕込まれた文書を添付したメールを介して拡散されます。しかし、2015年夏、セキュリティ侵害を受けたホームルーターからTrojan-Downloader.Win32.Upatreが発見されました。これは、この多目的なマルウェアがサイバー犯罪者の間でいかに活用されているかを物語っています。

このランキングのもう1つの常連ともいえるマルウェアはTrojan-Spy.Win32.Zbot（2位）であり、常に上位に入っています。Zbotファミリーのトロイの木馬は、Webインジェクションを使って銀行のWebページのコンテンツを変更し、オンラインバンキングユーザーの決済情報を窃取した最初のマルウェアです。これらは、自らの設定ファイルを複数のレベルで暗号化します。復号した設定ファイルがすべてメモリに格納されるわけではなく、部分的にロードされます。

Trojan-Banker.Win32.CheProファミリーの代表的なマルウェアが最初に検知されたのは、2012年10月でした。当時、これらのバンキング型トロイの木馬は、ブラジル、ポルトガル、ロシアのユーザーを主な標的としていましたが、現在は世界中のユーザーに対する攻撃に使用されています。この種のプログラムの大半はダウンローダーであり、システムに感染するには別のファイルを必要としますが、そのファイルはバンキング型マルウェアであることが一般的なため、スクリーンショットの取得、キーストロークの傍受、コピーバッファの内容の読み取りなど、ほぼすべてのオンラインバンキングシステムを攻撃できる機能を備えています。

特に興味深いのは、FaketokenとMarcherというモバイルバンキング型トロイの木馬の2種類のファミリーがランキングに入っていることです。Marcherファミリーに属するマルウェアは、Androidデバイスから決済情報を窃取します。

Trojan-Banker.AndroidOS.Faketokenファミリーの代表的なマルウェアは、コンピューターベースのトロイの木馬と連携して動作します。このマルウェアの拡散には、ソーシャルエンジニアリング手法が使われています。ユーザーがオンラインバンキングアカウントにアクセスすると、トロイの木馬はそのページを変更し、取引の安全性を確保するために必要とされるAndroidアプリをダウンロードするよう要求します。実際にリンク先にあるのはFaketokenアプリケーションです。ユーザーのスマートフォンにFaketokenアプリケーションがダウンロードされると、サイバー犯罪者は、バンキング型トロイの木馬に感染したコンピューターからユーザーのバンキングアカウントにアクセスできるようになります。さらに、不正侵入したモバイルデバイスを介して、ワンタイムの確認コード（mTAN）を盗み取ります。

もう1つのモバイルバンキング型トロイの木馬ファミリーは、Trojan-Banker.AndroidOS.Marcherです。このマルウェアはデバイスに感染した後、ヨーロッパの銀行のモバイルバンキングアプリとGoogle Playの2つのアプリの起動状況を追跡します。ユーザーがGoogle Playを起動すると、Marcherは偽のウィンドウを表示して、クレジットカード情報の入力を要求します。入力された情報はその後、詐欺師の手に渡ります。ユーザーがバンキングアプリを起動した場合も、同じ手法が使われます。

2015年のランキング10位は、Trojan-Banker.JS.Agentファミリーでした。これは、オンラインバンキングページに注入される、悪意あるJavaScriptコードです。このコードの狙いは、ユーザーがオンラインバンキングフォームに入力する決済情報を傍受することです。

ランサムウェアの興味深い動向

Trojan-Ransomは、ユーザーデータを不正に変更し、コンピューターを動作不能にするか（暗号化プログラムなど）、通常の動作をブロックするマルウェアです。マルウェアの所有者は通常、ファイルの復号やコンピューターのブロック解除と引き換えに身代金を被害者に要求します。

2013年のCryptoLockerの出現以来、ランサムウェアは大きな進化を遂げました。たとえば、Kaspersky Labは2014年、Android向けランサムウェアの最初のバージョンを発見しました。そのわずか1年後、感染の17%がAndroidデバイスで確認されました。

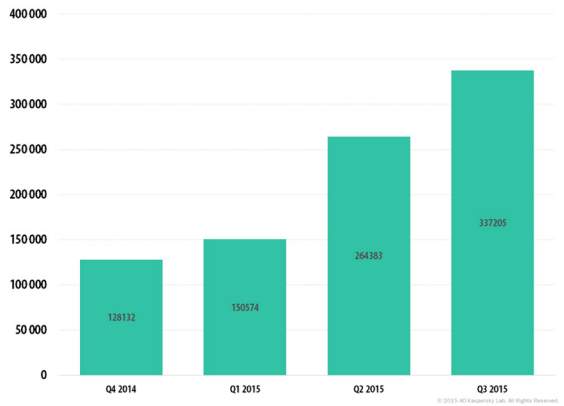
2015年には、初のLinux向けランサムウェアが見つかりました。これはTrojan-Ransom.Linuxクラスで検知されます。ただし、このマルウェアの作成者が小さな実装ミスを犯したため、身代金を支払わなくてもファイルを復号できます。

残念ながら、このような実装ミスが起きるケースは減る一方です。このため、「ランサムウェアは非常に巧妙にできているので、正直なところ、身代金を支払ってしまった方がいいとアドバイスすることが多いです」とFBIは発言しています。しかし2015年、オランダ警察がCoinVaultマルウェアに関与した疑いで2名を逮捕したことで、このアドバイスが必ずしも名案ではないことが証明されました。その後、弊社は14,000個の暗号鍵をすべて入手し、新しい復号ツールに追加しました。これにより、CoinVaultの被害者は無料でファイルを復号することができました。

2015年は、TeslaCryptが誕生した年でもありました。TeslaCryptはこれまで、別のランサムウェアファミリーのグラフィカルインターフェースを使用していました。当初はCryptoLockerのものでしたが、その後CryptoWallに変わりました。今回はCryptoWall 3.0のHTMLページを完全にコピーし、URLのみを変更しています。

攻撃を受けたユーザー数

下記のグラフは、この1年の間にTrojan-Ransomが検知されたユーザー数の増加を示しています。



Trojan-Ransomマルウェアの攻撃を受けたユーザー数
（2014年第4四半期～2015年第3四半期）

2015年全体を通じて、Trojan-Ransomは753,684台のコンピューターから検知されました。ランサムウェアの問題は深刻化する一方です。

Trojan-Ransomの上位10ファミリー

ここでは、広く蔓延しているランサムウェアの上位10ファミリーを示します。このリストには、ブラウザーベースの恐喝ファミリー、ブロッカーファミリー、そして悪名高い暗号化プログラムが含まれています。システムへのアクセスを制限して身代金を要求する、いわゆるWindowsブロッカー（Trojan-Ransom.Win32.Blockerファミリーなど）は、数年前はロシアから西側へと広まる形で大流行していましたが、現在はそれほど拡散しておらず、上位10ファミリーに含まれていません。

	検知名*	ユーザーの割合 (%) **
1	Trojan-Ransom.HTML.Agent	38.0
2	Trojan-Ransom.JS.Blocker	20.7
3	Trojan-Ransom.JS.InstallExtension	8.0
4	Trojan-Ransom.NSIS.Onion	5.8
5	Trojan-Ransom.Win32.Cryakl	4.3
6	Trojan-Ransom.Win32.Cryptodef	3.1
7	Trojan-Ransom.Win32.Snocry	3.0
8	Trojan-Ransom.BAT.Scatter	3.0
9	Trojan-Ransom.Win32.Crypmod	1.8
10	Trojan-Ransom.Win32.Shade	1.8

* ここでの統計は、カスペルスキー製品から返された検知判定に基づいており、統計データの提供に同意したカスペルスキー製品ユーザーから取得したものです。
** Trojan-Ransomファミリーの攻撃を受けたユーザー数を、Trojan-Ransomマルウェアの攻撃を受けた全ユーザー数で割った値。

1位はTrojan-Ransom.HTML.Agentファミリー（38%）、2位はTrojan-Ransom.JS.Blockerファミリー（20.7%）でした。これらはブラウザーをブロックするWebページであり、通常そのページには、脅迫メッセージ（法執行機関からの「警告」メッセージなど）や、ブラウザーをブロックするJavaScriptコードとメッセージなど、望ましくないコンテンツが含まれます。

3位のTrojan-Ransom.JS.InstallExtension（8%）もブラウザーをブロックするWebページであり、ユーザーにChromeの拡張機能をインストールさせようとします。ページを閉じようとすると、「ページを閉じるには、[追加] ボタンを押してください」というmp3の音声ファイルが再生されます。Chromeの拡張機能は有害なものではありませんが、メッセージが非常に目障りで拒否するのは困難です。このようにしてインストールされた拡張機能は、連携プログラムで使用されます。上位3ファミリーは特にロシアに蔓延しており、一部の旧ソ連諸国にも同様に広まっています。

ランサムウェアが最も拡散している場所に注目すると（上記3ファミリー以外も含む）、上位3か国はカザフスタン、ロシア、ウクライナが占めています。

2015年第3四半期に比較的活発化したCryaklは、ピーク時には1日に最大2,300件の感染の試みが確認されました。Cryaklの興味深い特徴は、暗号化方式にあります。ファイル全体を暗号化するのではなく、先頭29バイトと、ファイル内のランダムな場所にある3つのブロックを暗号化します。これはふるまい検知を逃れるための手法であり、同時に、先頭29バイトを暗号化することでヘッダーを壊します。

Cryptodefは、悪名高いCryptowallランサムウェアです。Cryptowallはここで取り上げたその他のファミリーとは違い、おもに米国で発見されています。実際、米国での感染数はロシアの3倍に上ります。CryptowallはJavaScriptが添付されたスパムメールを介して拡散します。JavaScriptが実行されるとCryptowallがダウンロードされ、ファイルの暗号化を開始します。身代金の要求メッセージが変更されたことが確認されており、「大規模なCryptowallコミュニティの一員となった」ことをマルウェアの作成者から祝福される内容になっています。

暗号化プログラムが実行可能ファイルとして実装されるだけでなく、Trojan-Ransom.BAT.Scatterファミリーのように、シンプルなスクリプト言語の中で使用されるケースもあります。2014年に出現したScatterファミリーはいち早く進化を遂げ、メールワームとTrojan-PSWの機能を備えています。2組の非対称鍵を使用して暗号化するため、秘密鍵を公開せずにファイルを暗号化できます。また、名前を変更した正規のユーティリティを使用してファイルを暗号化します。

Trojan-Ransom.Win32.Shade暗号化プログラムもロシアで蔓延しており、別のマルウェアのURLを含むリストをC&Cサーバーに要求することができます。その後、マルウェアをダウンロードしてシステムにインストールします。どのC&CサーバーもTorネットワーク内に存在します。Shadeも連携プログラムによって拡散されるとみられています。

Trojan-Ransomマルウェアの攻撃を受けた上位10か国

	国*	Trojan-Ransomの攻撃を受けたユーザーの割合 (%) **
1	カザフスタン	5.47
2	ウクライナ	3.75
3	ロシア連邦	3.72
4	オランダ	1.26
5	ベルギー	1.08
6	ベラルーシ	0.94
7	キルギス	0.76
8	ウズベキスタン	0.69
9	タジキスタン	0.69
10	イタリア	0.57

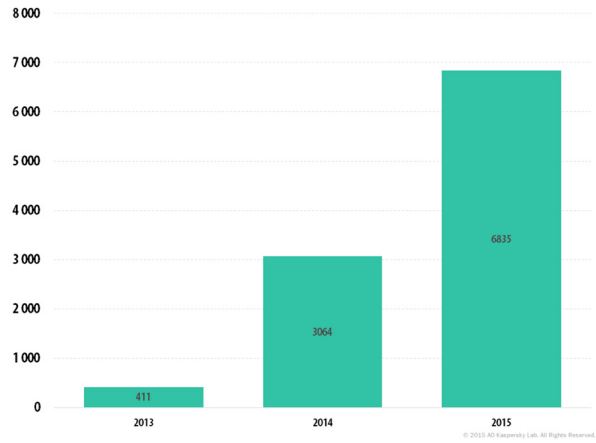
* カスペルスキー製品のユーザー数が比較的少ない (10,000未満) 国は除外。
** Trojan-Ransom攻撃を受けたコンピューターのユニークユーザー数を、その国のカスペルスキー製品を使用する全ユニークユーザー数で割った値。

暗号化プログラム

暗号化プログラムは、現時点ではサイバー犯罪者の間でブロッカーほど流行していないとしても、ユーザーに与えるダメージが大きいため、個別に調査する必要があると言えます。

新しいTrojan-Ransom暗号化プログラムの数

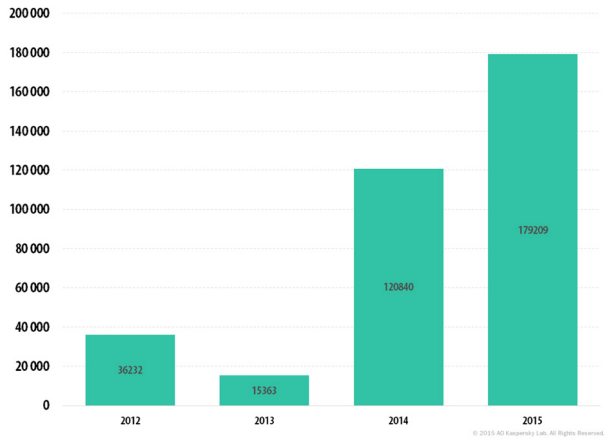
下のグラフは、新しく作成された暗号化プログラムの変種の発生数を年別に示しています。



Kaspersky Labのウイルスコレクションに含まれるTrojan-Ransom暗号化プログラムの変種の数（2013年～2015年）

弊社のウイルスコレクションに含まれる暗号化プログラムの変種の総数は、11,000以上に上ります。2015年には、新たな暗号化プログラムファミリーが作成されました。

暗号化プログラムの攻撃を受けたユーザーの数



Trojan-Ransom暗号化プログラムマルウェアの攻撃を受けたユーザー数（2012年～2015年）

2015年に暗号化プログラムの攻撃を受けたユニークユーザー数は179,209人でした。このうち、約20%は法人部門に含まれます。

実際のインシデント数は、数倍に上る点に注意が必要です。統計にはシグネチャベースの検知とヒューリスティック検知の結果のみが反映されていますが、ほとんどの場合、カスペルスキー製品はふるまい認識モデルに基づいて暗号化型トロイの木馬を検知しています。

暗号化プログラムの攻撃を受けた上位10か国

	国*	暗号化プログラムの攻撃を受けたユーザーの割合 (%)
1	オランダ	1.06
2	ベルギー	1.00
3	ロシア連邦	0.65
4	ブラジル	0.44
5	カザフスタン	0.42
6	イタリア	0.36
7	ラトビア	0.34
8	トルコ	0.31
9	ウクライナ	0.31
10	オーストリア	0.30

* カスペルスキー製品のユーザー数が比較的少ない (10,000未満) 国は除外。
** Trojan-Ransom暗号化プログラムの攻撃を受けたコンピューターのユニークユーザー数を、その国のカスペルスキー製品を使用する全ユニークユーザー数で割った値。

1位はオランダで、最も蔓延している暗号化プログラムファミリーはCTB-Locker (Trojan-Ransom.Win32/NSIS.Onion) です。2015年、CTB-Lockerを利用する関連プログラムが出現し、オランダ語を含む新しい言語が追加されました。ユーザーの大半は、悪意ある添付ファイルを含むメール経由で感染しています。このメールはかなり正確なオランダ語で書かれているため、この感染活動にはオランダ語のネイティブスピーカーが関わっている可能性があります。

ベルギーも同様の状況であり、ここでもCTB-Lockerが最も広く拡散しています。

ロシアでは、Trojan-Ransom.Win32.Cryaklが、ユーザーを狙った暗号化プログラムの1位となっています。

オンラインの脅威（WEBベースの攻撃）

このセクションの統計は、ウェブアンチウイルスコンポーネントから取得したものです。このコンポーネントは、悪意ある（または感染した）Webサイトから悪意あるオブジェクトがダウンロードされようとしたときにユーザーを保護します。悪意あるWebサイトとは、悪意あるユーザーが意図的に作成したものです。感染したサイトには、不正侵入されたユーザー参加型コンテンツ（フォーラムなど）や正規のリソースなどがあります。

オンラインで検知された悪意あるオブジェクト上位20種

2015年を通じて、カスペルスキーのウェブアンチウイルスは、121,262,075種類の悪意あるオブジェクト（スクリプト、エクスプロイト、実行可能ファイルなど）を検知しました。

2015年にコンピューターに対して実行されたオンライン攻撃で、最もよく使用されたマルウェアの上位20種を特定しました。昨年に続いて、アドウェアとそのコンポーネントが上位20種のうち12種を占めています。この1年で、カスペルスキーのウェブアンチウイルスがインストールされた全ユーザーコンピューターの26.1%に、アドウェアとそのコンポーネントが登録されました。アドウェアの数の増加とその強引な配信手法、アンチウイルス検知への対抗活動は、2014年の傾向を引き継いでいます。

強引な広告はユーザーにとって煩わしいものですが、コンピューターに害を及ぼすものではありません。このため、オンラインで検知された悪意あるオブジェクトから、アドウェアクラスまたはリスクウェアクラスのプログラムを除外し、別のランキングを作成しました。このランキングの上位20種のプログラムが、全オンライン攻撃数の96.6%を占めました。

	検知名*	攻撃が占める割合（%）**
1	Malicious URL	75.76
2	Trojan.Script.Generic	8.19
3	Trojan.Script.Iframer	8.08
4	Trojan.Win32.Generic	1.01
5	Expoit.Script.Blocker	0.79
6	Trojan-Downloader.Win32.Generic	0.69
7	Trojan-Downloader.Script.Generic	0.36
8	Trojan.JS.Redirector.ads	0.31
9	Trojan-Ransom.JS.Blocker.a	0.19
10	Trojan-Clicker.JS.Agent.pq	0.14
11	Trojan-Downloader.JS.Iframe.diq	0.13
12	Trojan.JS.Iframe.ajh	0.12
13	Exploit.Script.Generic	0.10
14	Packed.Multi.MultiPacked.gen	0.09
15	Exploit.Script.Blocker.u	0.09
16	Trojan.Script.Iframer.a	0.09

17	Trojan-Clicker.HTML.Iframe.ev	0.09
18	Hoax.HTML.ExtInstall.a	0.06
19	Trojan-Downloader.JS.Agent.hbs	0.06
20	Trojan-Downloader.Win32.Genome.qhcr	0.05

* ここでの統計は、ウェブアンチウイルスモジュールによる検知判定を示しています。この情報は、ローカルデータの共有に同意したカスペルスキー製品ユーザーから提供されたものです。
**ユーザーのコンピューター上で記録された全Web攻撃に占める割合。

例年どおり、上位20種の大半を占めているのはドライブバイ攻撃で使用されるオブジェクトです。これらはヒューリスティック検知により、Trojan.Script.Generic、Expoit.Script.Blocker、Trojan-Downloader.Script.Genericなどの検知名で検知されるオブジェクトであり、20種中7種を占めています。

1位のMalicious URLは、弊社のブラックリストのリンク（エクスプロイトへのリダイレクトを含むWebページ、エクスプロイトやマルウェアを含むサイト、ボットネットのコントロールセンター、脅迫的なWebサイト、などへのリンク）が確認されたケースです。

Trojan.JS.Redirector.ads（8位）は、感染したWebリソースへサイバー犯罪者が配置したスクリプトに割り当てられており、オンラインカジノなどのWebサイトにユーザーをリダイレクトします。この検知名がランクインしているということは、それほど複雑なプログラムでなくても、簡単にサイトに自動感染する可能性があることをWeb管理者は認識すべきです。

Trojan-Ransom.JS.Blocker.a（9位）は、周期的にページを更新することでブラウザーをブロックしようとするスクリプトです。不適切なコンテンツを表示したことに対して「罰金」が必要というメッセージを表示し、指定したデジタルウォレットに送金するようユーザーに指示します。このスクリプトは主にアダルトサイトで確認されており、ロシアおよびCIS諸国で検知されています。

Trojan-Downloader.JS.Iframe.djq（11位）を含むスクリプトは、WordPress、Joomla、Drupalで実行される感染サイトで見つかっています。このスクリプトを使用した大規模なサイト感染活動は、2015年8月に始まりました。このスクリプトはまず、感染したページのヘッダー、現在のドメイン、ユーザーがスクリプトを含むページに移動する前のアドレスに関する情報を詐欺師のサーバーに送ります。次に、iframeを使用して、別のスクリプトをユーザーのブラウザーにダウンロードします。このスクリプトが、ユーザーコンピューターのシステム、タイムゾーン、Adobe Flash Playerを使用できるかどうかに関する情報を収集します。その後リダイレクトが続き、ユーザーはAdobe Flash Playerの更新プログラム（実際はアドウェア）、またはブラウザープラグインをインストールするよう要求されます。

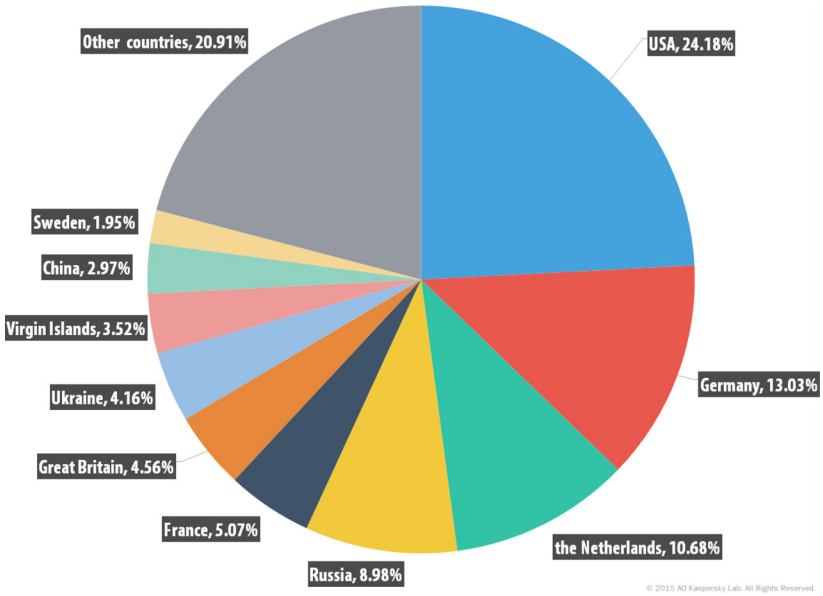
オンラインリソースにマルウェアが仕掛けられた上位10か国

ここでの統計は、攻撃に使用されたオンラインリソース（エクスプロイトへのリダイレクトを含むWebページ、エクスプロイトやマルウェアなどを含むサイト、ボットネットのコマンドセンターなど）を、カスペルスキーのアンチウイルスコンポーネントがブロックした物理的な場所に基づいています。どのユニークホストもWeb攻撃の発信源となりえます。この統計には、アドウェアの配信に使用された発信源やアドウェアの活動に関連付けられたホストは含まれません。

Web攻撃の地理的な発信源を特定するには、ドメイン名を実ドメインIPアドレスと照合した後、個々のIPアドレスの地理情報（GEOIP）を特定します。

2015年、カスペルスキー製品は、世界各国にあるWebリソースから実行された798,113,087件の攻撃をブロックしました。これらの攻撃を実行するため、6,563,145台のユニークホストが使用されました。

アンチウイルスコンポーネントによってブロックされた攻撃に関する通知の80%は、上位10か国のオンラインリソースから受信しました。



マルウェアが仕掛けられたオンラインリソースの分布（2015年）

オンラインリソースにマルウェアが仕掛けられた国の上位4か国は、昨年から変わっていません。フランスが7位から5位（5.07%）に浮上したのに対し、ウクライナは5位から7位（4.16%）へと順位を下げました。カナダとベトナムが上位20か国から外れ、新たに中国が9位、スウェーデンが10位に入りました。

この結果から、サイバー犯罪者は、ホスティング市場が十分に発達した国でホスティングサービスを運用、使用することを好む傾向が分かります。

ユーザーのオンライン感染のリスクが高い国

ユーザーがサイバー脅威に直面する頻度の高い国を調査するため、カスペルスキー製品ユーザーのコンピューターで検知判定が行われる頻度を国別に算出しました。そのデータから、各国のコンピューターが感染にさらされるリスクが明らかになり、世界各地のコンピューターを取り囲む環境の深刻さを示す指標となります。

ユーザーのオンライン感染のリスクが高い上位20か国

	国*	ユニークユーザーの割合（%）**
1	ロシア	48.90
2	カザフスタン	46.27
3	アゼルバイジャン	43.23
4	ウクライナ	40.40
5	ベトナム	39.55
6	モンゴル	38.27
7	ベラルーシ	37.91
8	アルメニア	36.63
9	アルジェリア	35.64
10	カタール	35.55
11	ラトビア	34.20
12	ネパール	33.94
13	ブラジル	33.66
14	キルギス	33.37
15	モルドバ	33.28
16	中国	33.12
17	タイ	32.92
18	リトアニア	32.80
19	アラブ首長国連邦	32.58
20	ポルトガル	32.31

ここでの統計は、ウェブアンチウイルスモジュールから返された検知判定に基づいており、統計データの提供に同意したカスペルスキー製品ユーザーから取得したものです。
* カスペルスキー製品のユーザー数が比較的少ない（10,000未満）国は除外。
** Web攻撃を受けたコンピューターのユニークユーザー数を、その国のカスペルスキー製品の全ユニークユーザー数で割った値。

2015年の上位3か国は前年から変わっていません。ロシアは引き続き1位にとどまっていますが、ユニークユーザーの割合が4.9ポイント低下しています。

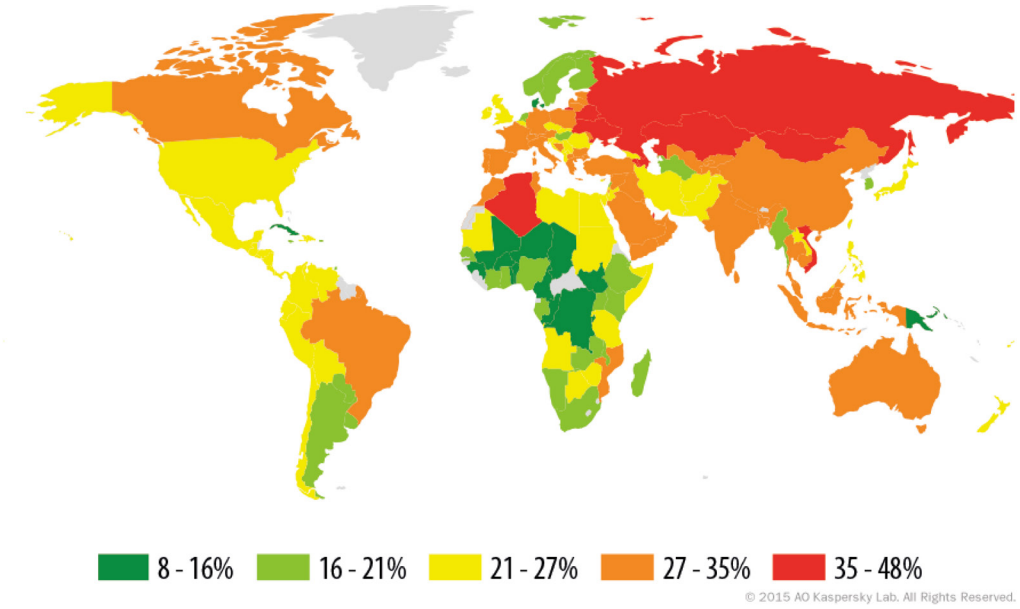
ドイツ、タジキスタン、ジョージア、サウジアラビア、オーストリア、スリランカ、トルコが上位20か国から姿を消し、ラトビア、ネパール、ブラジル、中国、タイ、アラブ首長国連邦、ポルトガルが新たに加わりました。

感染リスクのレベルに基づいて、各国を次の3つのグループに分類できます。

1. 高リスクのグループ(41%以上)
   2015年、このグループに該当したのは、20か国のうちの上位3か国(ロシア、カザフスタン、アゼルバイジャン)です。

2. 中程度のリスクのグループ(21～40.9%)
   このグループには109か国が該当しました。フランス(32.1%)、ドイツ(32.0%)、インド(31.6%)、スペイン(31.4%)、トルコ(31.0%)、ギリシャ(30.3%)、カナダ(30.2%)、イタリア(29.4%)、スイス(28.6%)、オーストラリア(28.0%)、ブルガリア(27.0%)、米国(26.4%)、ジョージア(26.2%)、イスラエル(25.8%)、メキシコ(24.3%)、エジプト(23.9%)、ルーマニア(23.4%)、英国(22.4%)、チェコ共和国(22.0%)、アイルランド(21.6%)、日本(21.1%)などです。

3. 低リスクのグループ(0～20.9%)
   オンライン環境が安全な国には、52か国が該当しました。ケニア(20.8%)、ハンガリー(20.7%)、マルタ(19.4%)、オランダ(18.7%)、ノルウェー(18.3%)、アルゼンチン(18.3%)、シンガポール(18.2%)、スウェーデン(18%)、韓国(17.2%)、フィンランド(16.5%)、デンマーク(15.2%)などです。



2015年には、ユーザーがオンラインの状態で、34.2%のコンピューターが少なくとも1回の攻撃を受けました。

平均すると、インターネット閲覧中に感染するリスクはこの1年で4.1ポイント低下しています。これには、いくつかの要因が考えられます。

- 第1に、ブラウザーと検索エンジンの開発元が、ユーザー保護の必要性を認識し、悪意あるサイトへの対策に乗り出しました。
- 第2に、インターネットの閲覧にモバイルデバイスやタブレットを使うユーザーが増加しています。
- 第3に、多くのエクスプロイトパックが、ユーザーのコンピューターにカスペルスキー製品がインストールされているかどうかをチェックするようになりました。カスペルスキー製品がインストールされている場合、エクスプロイトはコンピューターへの攻撃を試みません。

ローカルの脅威

ユーザーのコンピューターへのローカル感染の統計は、非常に重要な指標です。この指標には、ファイルやリムーバブルメディアに感染することでコンピューターシステムに侵入した脅威や、最初は暗号化された形でコンピューターに忍び込んだ脅威（複雑なインストーラーや暗号化ファイルに組み込まれたプログラムなど）が反映されています。また、カスペルスキーのファイルアンチウイルスによって初回のシステムスキャンを行った結果、ユーザーのコンピューターから検知されたオブジェクトも含まれています。

このセクションでは、ハードディスク上のファイルが作成またはアクセスされた時点で実行されたアンチウイルススキャンと、各種のリムーバブルデータストレージのスキャン結果から取得された統計に関する分析結果を示します。

2015年、カスペルスキーのアンチウイルス製品は、400万種類の悪意あるオブジェクトと不審なオブジェクトを検知しました。これは前年の2倍にあたります。

ユーザーのコンピューター上で検知された悪意あるオブジェクトの上位20種

下の表に、2015年にユーザーのコンピューター上で最も頻繁に検知された脅威のうち、上位20種を示します。この表にはアドウェアクラスとリスクウェアクラスのプログラムは含まれていません。

	検知名*	攻撃を受けたユニークユーザーの割合（%）**
1	DangerousObject.Multi.Generic	39.70
2	Trojan.Win32.Generic	27.30
3	Trojan.WinLNK.StartPage.gena	17.19
4	Trojan.Win32.AutoRun.gen	6.29
5	Virus.Win32.Sality.gen	5.53
6	Worm.VBS.Dinihou.r	5.40
7	Trojan.Script.Generic	5.01
8	DangerousPattern.Multi.Generic	4.93
9	Trojan-Downloader.Win32.Generic	4.36
10	Trojan.WinLNK.Agent.ew	3.42
11	Worm.Win32.Debris.a	3.24
12	Trojan.VBS.Agent.ue	2.79
13	Trojan.Win32.Autoit.cfo	2.61
14	Virus.Win32.Nimnul.a	2.37
15	Worm.Script.Generic	2.23
16	Trojan.Win32.Starter.lgb	2.04
17	Worm.Win32.Autoit.aiy	1.97

18	Worm.Win32.Generic	1.94
19	HiddenObject.Multi.Generic	1.66
20	Trojan-Dropper.VBS.Agent.bp	1.55

ここでの統計は、カスペルスキー製品ユーザーのコンピューター上で、リアルタイムとオンデマンドのスキャナーモジュールによって生成されたマルウェア検知判定から作成しました。統計データはユーザーの同意を得て収集したものです。
* カスペルスキー製品ユーザーのコンピューター上で、リアルタイムとオンデマンドのスキャナーモジュールによって生成されたマルウェア検知判定。統計データはユーザーの同意を得て収集したもの。
** アンチウイルスモジュールでこれらのオブジェクトがコンピューターから検知されたユーザー数を、コンピューターからマルウェアが検知された全カスペルスキー製品ユーザー数で割った値。

DangerousObject.Multi.Genericは、クラウドテクノロジーを用いて検知されたマルウェアで使用されており、これが1位になりました。マルウェアを検知するためのシグネチャやヒューリスティックが、アンチウイルスデータベースに登録されていなくても、弊社のクラウドアンチウイルスデータベースにそのオブジェクトに関する情報が登録されている場合、クラウドテクノロジーが効果を発揮します。実際に、最新のマルウェアはこの方法で検知されています。

ウイルスの割合は減少を続けています。たとえば、昨年Virus.Win32.Sality.genの影響を受けたユーザーの割合は6.69%でしたが、2015年は5.53%でした。Virus.Win32.Nimnulの場合、影響を受けたユーザーの割合は2014年に2.8%、2015年に2.37%でした。20位のTrojan-Dropper.VBS.Agent.bpはVBSスクリプトであり、解凍したVirus.Win32.Nimnulをディスクに保存します。

上位20種には、ヒューリスティックによる判定とウイルス以外に、リムーバブルメディアに蔓延しているワームとそのコンポーネントが含まれています。これらが上位に入っているのは、多数のコピーを作成して拡散するという性質があるためです。ワームは管理サーバーが動作していなくても、長期にわたって自己増殖を続けることができます。

ユーザーのローカル感染のリスクが高い国

1年間に発生したアンチウイルス検知数を国別に算出しました。このデータには、ユーザーのコンピューターまたはコンピューターに接続されたリムーバブルメディア（USB、カメラと携帯電話のメモリカード、外部ハードディスクなど）上で検知されたオブジェクトが含まれています。この統計は、各国のPCの感染レベルを示しています。

感染レベルの高い国、上位20か国

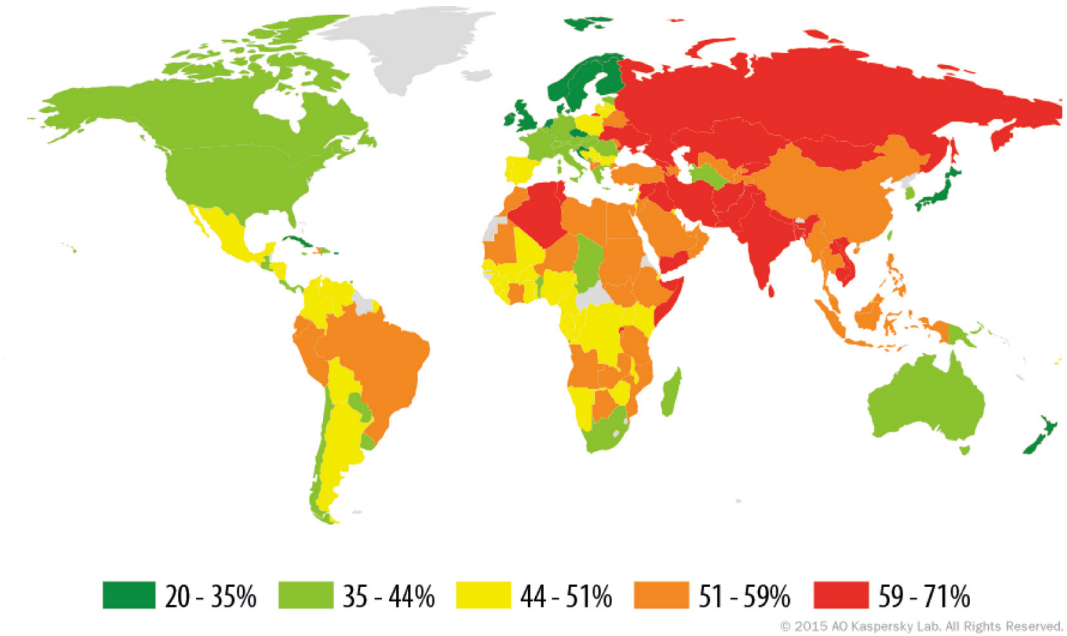
	国*	ユニークユーザーの割合（%）**
1	ベトナム	70.83
2	バングラデシュ	69.55
3	ロシア	68.81
4	モンゴル	66.30
5	アルメニア	65.61
6	ソマリア	65.22
7	ジョージア	65.20
8	ネパール	65.10
9	イエメン	64.65
10	カザフスタン	63.71
11	イラク	63.37
12	イラン	63.14
13	ラオス	62.75
14	アルジェリア	62.68
15	カンボジア	61.66
16	ルワンダ	61.37
17	パキスタン	61.36
18	シリア	61.00
19	パレスチナ	60.95
20	ウクライナ	60.78

ここでの統計は、アンチウイルスモジュールから返された検知判定に基づいており、統計データの提供に同意したカスペルスキー製品ユーザーから取得したものです。
*算出時にカスペルスキー製品 のユーザー数が10,000未満の国は除外。
** ローカルの脅威がブロックされたコンピューターのユニークユーザー数を、その国の全カスペルスキー製品ユーザー数で割った値。

ベトナムは3年連続で1位となりました。モンゴルとバングラデシュの順位が入れ替わり、バングラデシュが4位から2位に上がったのに対し、モンゴルは2位から4位に下がりました。ロシアは昨年、上位20か国に含まれていませんでしたが、2015年は3位となりました。

インド、アフガニスタン、エジプト、サウジアラビア、スーダン、スリランカ、ミャンマー、トルコが上位20か国から姿を消し、ロシア、アルメニア、ソマリア、ジョージア、イラン、ルワンダ、パレスチナ自治区、ウクライナが新たに加わりました。

上位20か国では、KSNユーザーが所有するコンピューター、ハードディスク、リムーバブルメディアの平均67.7%から、少なくとも1つの悪意あるオブジェクトが発見されました。2014年の数値は58.7%でした。



ローカルの脅威レベルに基づいて、各国をいくつかのリスクカテゴリに分類できます。

1. リスク最大(60%超):キルギス(60.77%)、アフガニスタン(60.54%)など、22か国。
2. リスク高(41～60%):インド(59.7%)、エジプト(57.3%)、ベラルーシ(56.7%)、トルコ(56.2%)、ブラジル(53.9%)、中国(53.4%)、アラブ首長国連邦(52.7%)、セルビア(50.1%)、ブルガリア(47.7%)、アルゼンチン(47.4%)、イスラエル(47.3%)、ラトビア(45.9%)、スペイン(44.6%)、ポーランド(44.3%)、ドイツ(44%)、ギリシャ(42.8%)、フランス(42.6%)、韓国(41.7%)、オーストリア(41.7%)など、98か国。
3. リスク中(21～40.99%):ルーマニア(40%)、イタリア(39.3%)、カナダ(39.2%)、オーストラリア(38.5%)、ハンガリー(38.2%)、スイス(37.2%)、米国(36.7%)、英国(34.7%)、アイルランド(32.7%)、オランダ(32.1%)、チェコ共和国(31.5%)、シンガポール(31.4%)、ノルウェー(30.5%)、フィンランド(27.4%)、スウェーデン(27.4%)、デンマーク(25.8%)、日本(25.6%)など45か国。

安全性の高い上位10か国は次のとおりです。

	国	割合(%)*
1	キューバ	20.8
2	セーシェル	25.3
3	日本	25.6
4	デンマーク	25.8
5	スウェーデン	27.4
6	フィンランド	27.4
7	アンドラ	28.7
8	ノルウェー	30.5
9	シンガポール	31.4
10	チェコ共和国	31.5

* ローカルの脅威がブロックされたコンピューターのユニークユーザー数を、その国の全カスペルスキー製品ユーザー数で割った値。

前年と比較すると、2015年はマルティニークにかわり、アンドラがランキングに入った以外、変更点はありません。

安全性の高い上位10か国の平均では、26.9%のユーザーコンピューターが1年のうちに少なくとも1回の攻撃を受けています。この数値は2014年から3.9ポイント上昇しています。

まとめ

統計の分析結果から、サイバー犯罪活動における主な傾向が浮き彫りになっています。

- 一部のサイバー犯罪者は、刑事訴追のリスクを最小限に抑えようとしており、マルウェア攻撃から悪質なアドウェアの拡散へと移行しています。
- 比較的単純なプログラムがマス攻撃で使用される割合が増えています。このアプローチでは、攻撃者が短期間でマルウェアを更新でき、攻撃の有効性が増します。
- 攻撃者は、Windows以外にAndroidやLinuxプラットフォームも駆使するようになっています。これらのプラットフォーム用に、ほぼすべての種類のマルウェアが作成、使用されています。
- サイバー犯罪者は、指令サーバーを隠すためにTor匿名化テクノロジーを、取引にはビットコインを積極的に活用しています。

「グレーゾーン」に分類されるアンチウイルス検知の割合は、増加し続けています。これに該当するのは、主に各種アドウェアです。2015年のWebベースの脅威に関するランキングでは、このクラスの代表的なプログラムが上位20種のうち12種を占めました。この1年で、カスペルスキーのウェブアンチウイルスがインストールされた全ユーザーコンピューターの26.1%に、アドウェアが登録されました。アドウェアの数の増加とその強引な配信手法、アンチウイルス検知への対抗活動は、2014年の傾向を引き継いでいます。アドウェアの拡散はかなりの収入になるため、営利目的の作成者がマルウェアに特有の手口と技術を使用する場合もあります。

2015年、ウイルスの作成者が特別な興味を示したのは、Adobe Flash Playerのエクスプロイトでした。弊社の分析によると、エクスプロイトを含むランディングページの多くは、Adobe Flash Playerのエクスプロイトによってダウンロードされています。これには2つの要因が影響しています。1つ目は、この1年でAdobe Flash Playerで多数の脆弱性が見つかっていること。2つ目は、Hacking Team社によるデータ漏洩の結果、これまで知られていなかったAdobe Flash Playerの脆弱性に関する情報が明らかになり、これらの脆弱性が瞬く間に悪用されたことです。

バンキング型トロイの木馬の分野では、2015年、興味深い変化が確認されました。ZeuSの変種は膨大な数に上り、過去数年にわたって最もよく使用されるマルウェアファミリーの1位を維持していましたが、Trojan-Banker.Win32.Dyrezaが首位の座を奪いました。インターネットバンキングシステムを介して金銭を窃取するマルウェアのランキングでは、1年を通じてUpatreが先頭に立ちました。このマルウェアはバンキング型トロイの木馬であるDyre/Dyzap/Dyrezaファミリーを標的コンピューターにダウンロードします。バンキング型トロイの木馬の分野全体で見ると、Dyrezaの攻撃を受けたユーザーの割合が40%を超えました。このマルウェアはWebインジェクション手法を効果的に使用し、オンラインバンキングシステムにアクセスするためのデータを窃取します。

もう1つの注目すべき事実は、FaketokenとMarcherという2つのモバイルバンキング型トロイの木馬ファミリーが、2015年に最もよく使用されたバンキング型トロイの木馬の上位10種に含まれていたことです。現在の傾向から、来年はモバイルバンキング型の割合がランキング内で大幅に増加すると予想されます。

2015年のランサムウェアの活動には多数の変化が見られました。

1. ブロッカーの流行が徐々に廃れる一方で、2015年に暗号化ランサムウェアの攻撃を受けたユーザー数は48.3%増加しています。ほとんどの場合、被害者にとって単にコンピューターがブロックされるよりもファイルを暗号化された方が、情報へのアクセスの復元が難しくなります。一般のホームユーザーよりも身代金を支払う可能性の高いビジネスユーザーに対して、暗号化ランサムウェアを利用した攻撃が活発化しています。これは、Webサーバーを狙った初のLinux用ランサムウェアが2015年に出現したことからも裏付けられます。
2. 一方で、暗号化プログラムがマルチモジュール化しており、暗号化以外に、ユーザーのコンピューターからデータを窃取する機能が搭載されています。
3. 現在、詐欺師が関心を寄せているのはLinuxだけかもしれません。しかし、2014年にAndroid向けとして初のランサムウェア型トロイの木馬が検知され、2015年になるとAndroid OSを狙った攻撃は急増加しました。そして、ランサムウェアが関係する攻撃のうち、Androidデバイスでブロックされたものは年末までに17%に上りました。
4. 世界中で盛んに脅威が拡散されています。カスペルスキー製品がランサムウェア型トロイの木馬を検知した国と地域は200に上り、事実上、ほぼすべての地域を網羅しています。

Kaspersky Labの予測では、2016年、サイバー犯罪者はWindows以外のプラットフォームを狙った暗号化ランサムウェアの開発を継続するとしています。Androidを標的とした暗号化プログラムの割合が増える一方で、Macを狙うランサムウェアも出現するでしょう。Androidがさまざまな家電で広く利用されていることから、「スマート」デバイスに対する初のランサムウェア攻撃が発生する可能性があります。

株式会社カスペルスキー
PR-1021-201512