KASPERSKY lab

Kaspersky Security Bulletin 2016

2016 年 脅威の統計概要

GREAT

目次

数字で見る 2016 年（カスペルスキー製品での観測） 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
オンラインの脅威（Web ベースの攻撃） 6
オンラインリソースに潜むマルウェアが多い上位 10 か国 6
オンラインで検知判定された上位 20 種 7
暗号化型ランサムウェア 9
検知された暗号化型ランサムウェア亜種の数 9
ランサムウェアの攻撃を受けたユーザーの数 9
攻撃の地理的分布 10
広範囲に蔓延した暗号化型ランサムウェアファミリー上位 10 種 11
暗号化型ランサムウェアと法人 13
金融機関におけるオンラインの脅威 13
攻撃の地理的分布 15
バンキング型マルウェアの上位 10 プログラム 16
ユーザーのオンライン感染リスクが高い国 18
ユーザーローカル環境の脅威 21
ユーザーのコンピューターで検知された プログラムの上位 20 種 21
ユーザーのローカル環境で感染リスクが高い国 23

＊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KSNユーザーの同意を得て収集されています。KSNには全世界213の国と地域の数百万のカスペルスキー製品ユーザーが参加しており、悪意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、2015 年 11 月から 2016 年 10 月までのものです。

数字で見る 2016 年 （カスペルスキー製品での観測）

- ユーザーのコンピューターの**31.9%**で、年間で1回以上Webベースの攻撃を検知しました。
- 全世界のユーザーの端末で検知された、オンラインリソースからの攻撃は**758,044,650**件に上ります。
- **261,774,932**のURL（重複を除く）が、Webアンチウイルスコンポーネントによって悪意あるURLと判定されました。
- カスペルスキー製品によって無害化された Webベースの攻撃のうち、**29.1%**は米国内の悪意あるオンラインリソースを使用して実行されていました。
- Webアンチウイルスコンポーネントは、**69,277,289**種類の悪意あるオブジェクトを検知しました。
- **1,445,434**台のコンピューターが暗号化型マルウェアの標的になりました。
- オンラインバンキングで金銭を窃取するマルウェアの起動の試みを、**2,871,965**台のデバイスでブロックしました。
- ファイルアンチウイルスコンポーネントは、合計**4,071,588**種類（重複を除く）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。

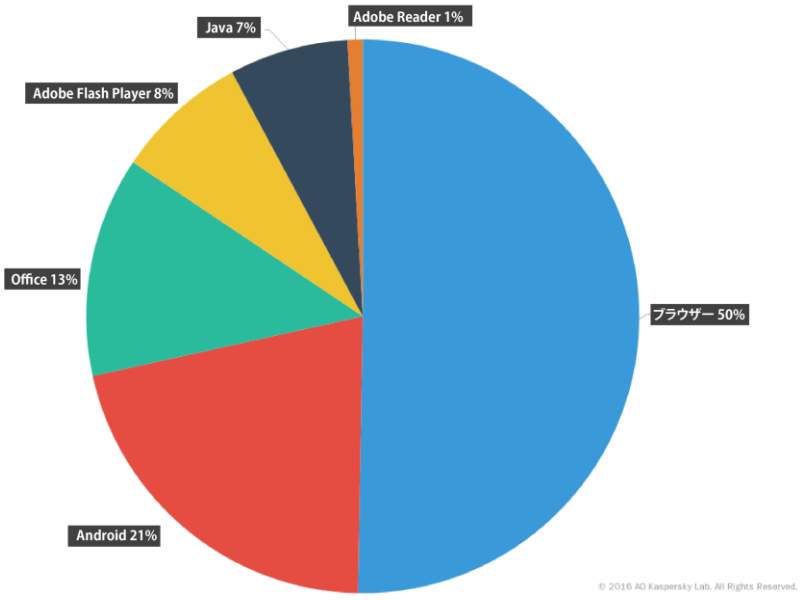
サイバー攻撃で使用された脆弱なアプリケーション

2016年は、エクスプロイトキットの主要プレイヤーの多くがこの市場から撤退していきました。第2四半期には、長年この市場をリードしてきたAnglerやNuclearといった主要キットが終息に至りました。つまりこれは、サイバー犯罪者が他のエクスプロイトキットへの転換を余儀なくされたことを示しており、同時期にNeutrinoの使用が急増しました。しかしこのNeutrinoも第3四半期には終息を迎えています。2016年終盤現在、活発な使用が続いているのはRigとMagnitudeです。RigはNeutrinoの終息によって生まれたニッチな空間を奪う形で使用頻度を伸ばしています。

2016年も、2015年同様、Adobe Flash Playerの脆弱性を悪用したエクスプロイトの使用傾向が高くなっています。Kaspersky Labが作成した、サイバー犯罪者のエクスプロイトに使用されるケースが最も多い脆弱性のリストにも、Adobe Flash Playerの脆弱性が4つ入っています。

- CVE-2015-8651 (Adobe Flash)
- CVE-2016-1001 (Adobe Flash)
- CVE-2016-0034 (Microsoft Silverlight)
- CVE-2015-2419 (Internet Explorer)
- CVE-2016-4117 (Adobe Flash)
- CVE-2016-4171 (Adobe Flash)

現在この市場ではAdobe Flash Playerの脆弱性を狙ったエクスプロイトキットが概して優勢であり、Flash関連のエクスプロイトが市場に占める割合を昨年と比較すると、昨年の3%から8%へと急増しています。



サイバー攻撃に利用されたエクスプロイトのアプリケーション種類別分布（2016年）

カスペルスキー製品が2016年に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、Webベースの攻撃や改ざんされたローカルアプリケーション（ユーザーの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。

Microsoft Officeアプリケーションの脆弱性を対象としたエクスプロイトの割合も、昨年の4%から13%へと大幅に増加しました。この背景には、Microsoft Officeのエクスプロイトを含む悪意あるスパムの件数が急増したことがあります。しかしこのタイプのスパムも年末に向けて減少傾向にあります。

Android OSに対するエクスプロイトの割合は、昨年より7ポイント増加し、21%となっています。この増加の主な背景には、モバイルデバイスでのルート権限昇格を可能にする新しいエクスプロイトが増えたことがあります。

全体としては、2016年も長期的なトレンドが変わらない1年となり、エクスプロイトの主な対象は依然として、Adobe Flash Player、Microsoft Office、Internet Explorerでした。Internet Explorer向けのエクスプロイトは、エクスプロイトを配布するためのランディングページが検知対象となるため、円グラフでは、「ブラウザー」に分類されています（全エクスプロイトの50%）。

オンラインの脅威（Web ベースの攻撃）

本セクションの統計は、カスペルスキー製品のWebアンチウイルスコンポーネントのデータに基づいています。Webアンチウイルスは、悪意あるWebサイトや感染したWebサイトに設置されている悪意あるオブジェクトをダウンロードさせる試みから、ユーザーを保護する機能です。悪意あるWebサイトとは、攻撃者が意図的に作成したサイトを指します。感染したWebサイトには、ユーザーがコンテンツを寄稿するサイト（フォーラムなど）のほか、侵害された正規サイトが含まれます。

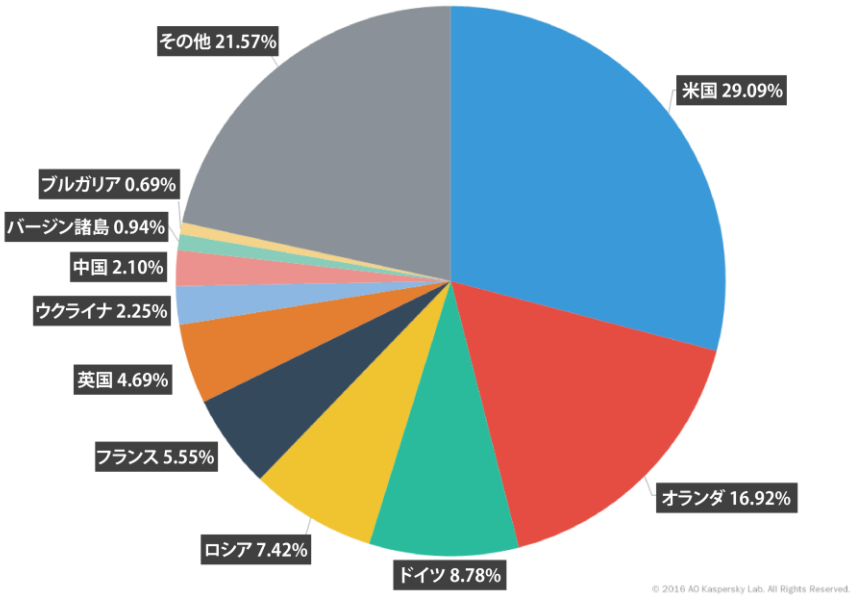
2016年にWebアンチウイルスコンポーネントが検知した悪意あるオブジェクト（スクリプト、エクスプロイト、実行ファイルなど）は、重複を除き **69,277,289**種類でした。また、Webアンチウイルスコンポーネントによって、**261,774,932**のURL（重複を除く）が悪意あるURLと判定されています。カスペルスキー製品は世界212か国のオンラインリソースからの悪意ある攻撃を**758,044,650**件検知し、ブロックしました。

オンラインリソースに潜むマルウェアが多い上位 10 か国

次の統計は、攻撃で使用され、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サイト、エクスプロイトなどのマルウェアを含むサイト、ボットネットのコマンドセンターなど）が物理的に存在する場所に基づいています。どのようなホストであっても、1つまたは複数のWebベースの攻撃の発信元となり得ます。Webベースの攻撃の発生源の地理的な位置を判断するために、ドメイン名を実際のドメインのIPアドレスと照合してから、具体的なIPアドレスの地理的な位置（GEOIP）を確定しています。

2016年、世界各国にあるオンラインリソースから実行された**758,044,650**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、3,014,685台の個別端末が使用されました。

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通知の78%は、上位10か国のオンラインリソースからの攻撃によるものでした。



Webベースの攻撃ソースの国別分布（2015年11月から2016年10月）

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9か国は昨年と同じですが、オランダとドイツ、および中国とバージン諸島の順位が入れ替わりました。スウェーデンはトップ10から外れ、代わりにブルガリアが10位に入りました。

オンラインで検知判定された上位 20 種

2016年、Webアンチウイルスコンポーネントは**69,277,289**（重複を除く）の悪意あるオブジェクト（スクリプトを含むユニークなハッシュ値、エクスプロイト、実行ファイルなど）を検出しました。

同期間、Webアンチウイルスコンポーネントが反応したユーザーコンピューターの15.6%で、広告プログラムとそのコンポーネントの登録が発見されました。

以下の一覧は、2016年にコンピューターを対象とするWebベースの攻撃に関わった悪意あるプログラムの上位20種です。これら20種のプログラムでWebベースの攻撃の96.6%を構成しています。

	検知名*	全攻撃に占める割合**
1	Malicious URL	77.26
2	Trojan-Clicker.HTML.Iframe.dg	8.15
3	Trojan.Script.Generic	6.74
4	Trojan.Script.Iframer	3.14

5	Trojan-Downloader.Script.Generic	0.35
6	Exploit.Script.Generic	0.20
7	Packed.Multi.MultiPacked.gen	0.15
8	Trojan.JS.FBook.bh	0.13
9	Exploit.Script.Blocker	0.11
10	Trojan-Downloader.JS.Iframe.div	0.11
11	Trojan.JS.Redirector.ns	0.09
12	Trojan-Dropper.VBS.Agent.bp	0.08
13	Trojan-Downloader.JS.Agent.hjc	0.08
14	Trojan.JS.Iframe.ako	0.07
15	Trojan.Win32.Generic	0.06
16	Trojan.Win32.Generic	0.06
17	Trojan.JS.Agent.ckf	0.05
18	Trojan-Spy.HTML.Fraud.gen	0.05
19	Trojan.Win32.Invader	0.04
20	Exploit.SWF.Agent.gen	0.04

* ここでの統計は、Webアンチウイルスコンポーネントによる検知判定を示しています。

** ユーザーのコンピューター上で記録されたすべてのWebベースの攻撃に占める割合（重複を除く）です。

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ダウンロード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ています。

1位のMalicious URLは、Kaspersky Lab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Webサイト、ボットネットのC&C（指令サーバー）、脅迫的なWebサイトなど）が確認されたケースです。

8位のTrojan.JS.FBook.bhは、特定のC&Cアドレスのリンクを取得し、そのユーザーのFacebookのステータスを更新したり、ステータスにそのリンクを追加したり、そのユーザーの全友達にタグ付けしたりするスクリプトです。このリンクの取得が、ユーザーのFacebookアカウントにアクセスできるブラウザー拡張機能のインストールにつながります。つまりこれにより、この拡張プログラムを実行するなど、ユーザーに代わってさまざまなアクションの実行が可能になるということです。

13位のTrojan-Downloader.JS.Agent.hjcは、C&Cにアクセスして設定ファイルを読み取る「動的な」クリッカーです。このファイルに含まれるリンクは、iframeに含まれたり、感染したWebサイトでユーザーがクリックしたときのリダイレクト先になったりします。

18位のTrojan-Spy.HTML.Fraud.genは、オンラインショッピングページや金融機関の

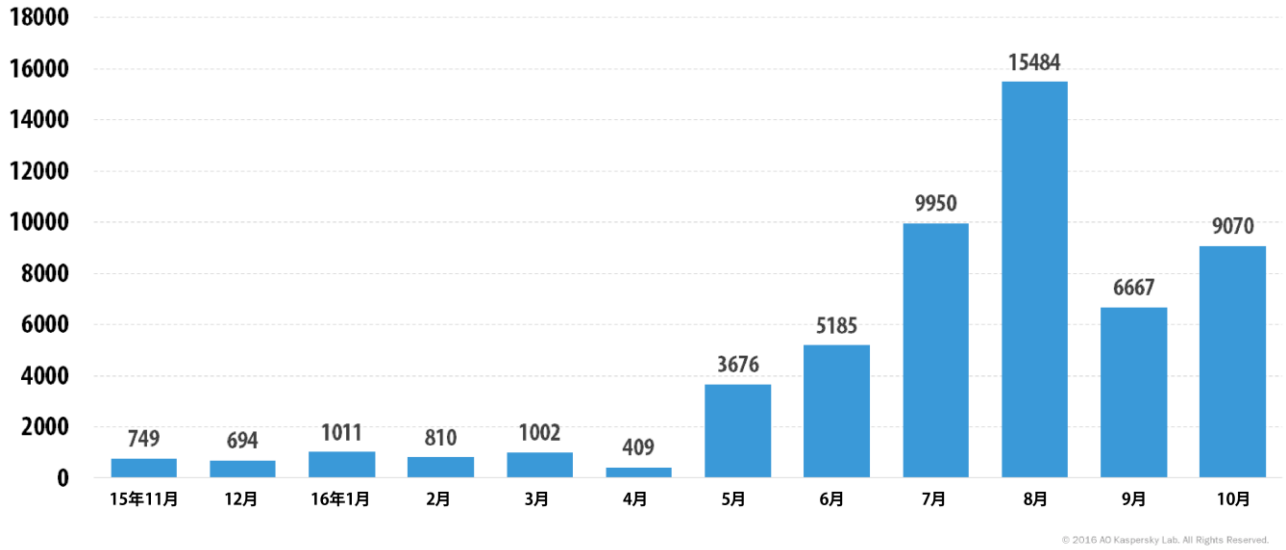
Webページに偽装するフィッシングHTMLページに利用されるプログラムで、フィッシングWebメールに含まれます。

暗号化型ランサムウェア

暗号化型ランサムウェアの脅威は拡大を続けており、2016年後半はファミリーの数も亜種の数も増加しました。新しいランサムウェアは活発に拡散していますが、そのほとんどが実力の低い開発者による低労力なものであったことが判明しています。しかし、LockyやCerber、CryptXXXといった一部のランサムウェアは個人にも企業にも新しい大きな脅威となっています。CTB-Locker、CryptoWall、TorrentLockerなど従来のランサムウェアも引き続き健在で、TeslaCryptのように活動を停止する気配もありません。

検知された暗号化型ランサムウェア亜種の数

この1年間にカスペルスキー製品は暗号化型ランサムウェアの亜種を54,000種以上検知し、新しいファミリーを62種発見しました。

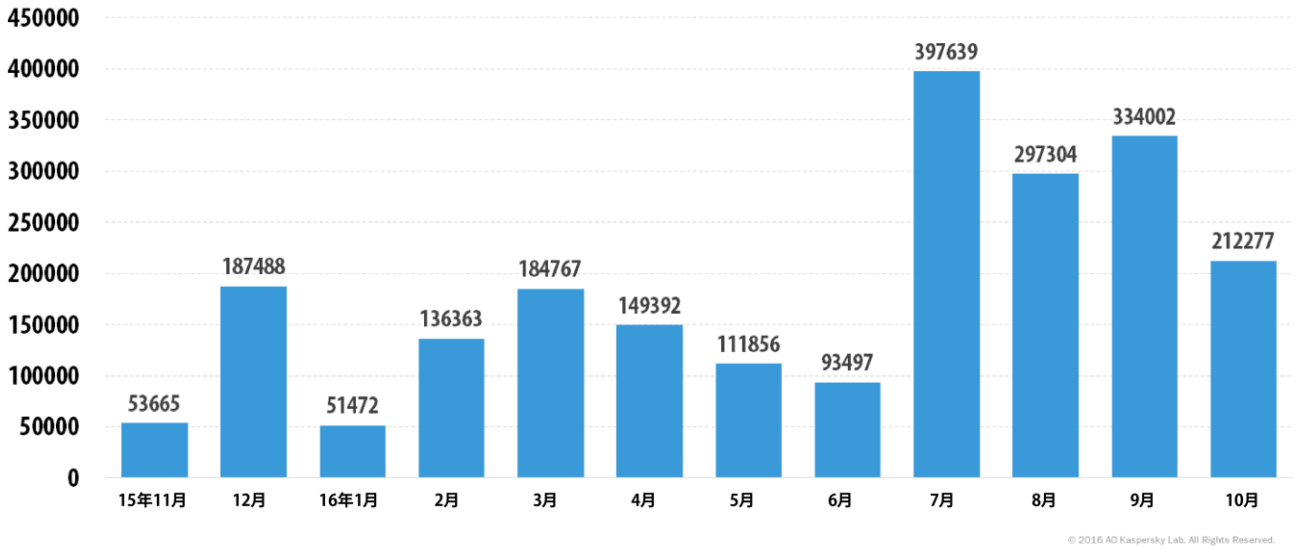


新しい暗号化型ランサムウェア亜種の数（2015年11月から2016年10月）

Kaspersky LabのVirus Collectionに登録されている暗号化型ランサムウェアの亜種の総数は、現在までに65,000種以上に及んでいます。

ランサムウェアの攻撃を受けたユーザーの数

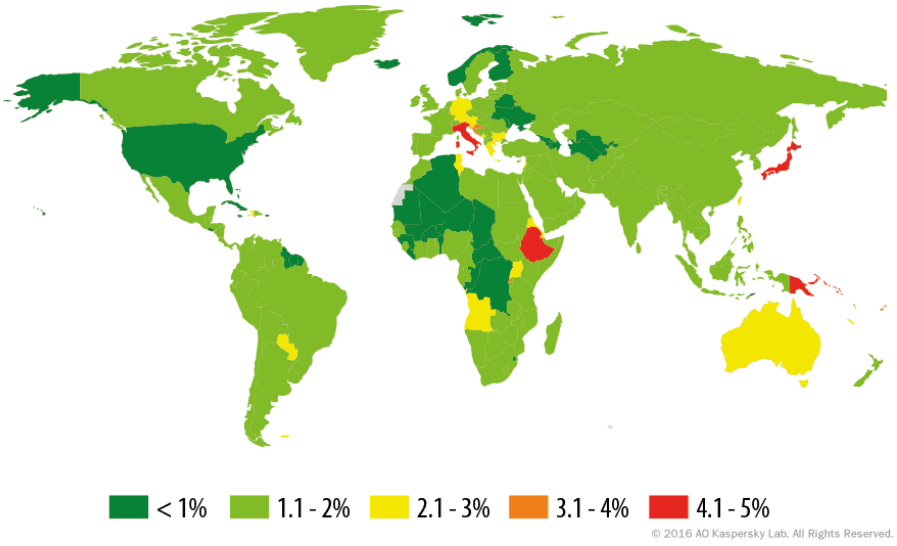
2016年に暗号化型ランサムウェア攻撃を受けたKSNのユーザー数は、1,445,434人でした（重複を除く）。



暗号化型ランサムウェアの攻撃を受けたユーザー数（2015年11月から2016年10月）

実際のインシデント数はさらに多くなります。統計にはシグネチャー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おり、新しい、または未知のマルウェアサンプルの場合、カスペルスキー製品は振る舞い認識モデルに基づいて暗号化型ランサムウェアを検知します。

攻撃の地理的分布



2016年の暗号化型ランサムウェア攻撃の地理的分布（攻撃を受けたユーザーの割合）

暗号化型ランサムウェアの攻撃が多い上位10か国

	国*	攻撃されたユーザーの割合（%） **
1	日本	4.46
2	イタリア	4.17
3	クロアチア	3.23
4	ルクセンブルク	3.15
5	ブルガリア	2.86
6	ウガンダ	2.55
7	チュニジア	2.54
8	オーストリア	2.45
9	香港	2.43
10	レバノン	2.39

* カスペルスキー製品のユーザー数が50,000未満の国は除外しています。

** 全ユニークユーザーのうち、暗号化型ランサムウェアの標的になったユニークユーザーの割合です。

広範囲に蔓延した暗号化型ランサムウェアファミリー上位 10 種

	名前	判定	攻撃されたユーザーの割合（%）*
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25.32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7.07
3	TeslaCrypt	Trojan-Ransom.Win32.Bitman	6.54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2.85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2.79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2.36
7	Shade	Trojan-Ransom.Win32.Shade	1.73
8	(generic verdict)	Trojan-Ransom.Win32.Snocry	1.26

9	Crysis	Trojan-Ransom.Win32.Crusis	1.15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0.90

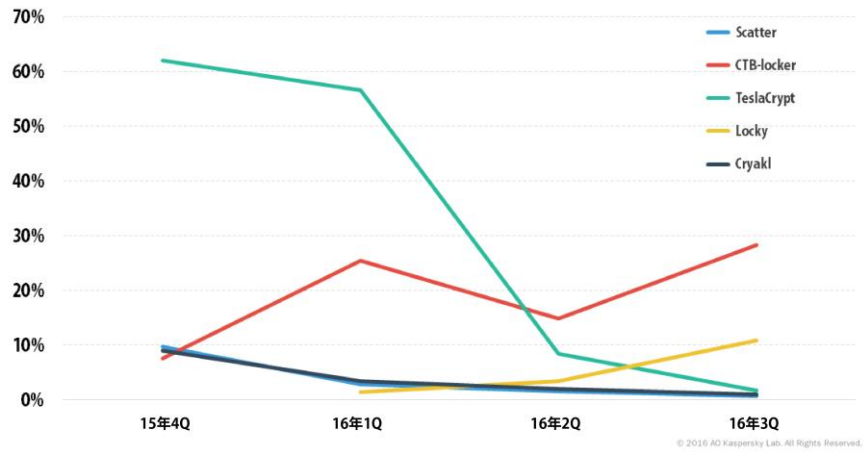
* 暗号化型ランサムウェアに攻撃されたカスペルスキー製品のユニークユーザーのうち、コンピューターが特定の暗号化型ランサムウェアファミリーの標的になったユニークユーザーの割合です。

上位10種の大半（CTB-Locker、CryptoWall、Shade、Cryakl、TeslaCrypt、Scatter、Cryrar）は、昨年リリースされた悪名高いランサムウェアです。

しかし2016年に確認されたLockyとCrysisもすでに拡散レベルの上位に登場しています。

2016年に確認された新しい暗号化型ランサムウェアは、旧バージョンと非常によく似ています。ランサムウェアが最も一般的に採用している標準的な暗号化の仕組みはすでに知られているため、サイバー犯罪者がランサムウェアを開発する際にも、新たに画期的なアプローチを考案する必要がないためです。ランサムウェアのプログラマーは現在、ファイルの暗号化には実績あるアプローチを採用し、新しい対解析技術および検知回避の手法のために労力を使っています。

またKaspersky Labは、多くの新しい暗号化型ランサムウェアが明らかに「実力の低い」開発者によって作られていることも発見しました。こうしたファミリーにはたいてい、質の低いコード、暗号文に存在する多数のエラーや欠陥、単純なアルゴリズムやアプローチの使用という特徴があり、さらには脅迫状に文法上の間違いが見られることもあります。こうしたサンプルが広く拡散することは稀ですが、これら「アマチュア」ランサムウェアの新しいファミリーの数を軽視することはできません。脅迫によって簡単に収入を得たいという欲求と、ランサムウェアに関する多くのメディア報道を背景に、他の詐欺行為を専門としていた犯罪者がますます多くこの分野に引き寄せられているものと考えられます。



最も拡散している暗号化型ランサムウェアファミリー上位5種の四半期の推移
（検知ユーザーの割合）

Teslacryptの検知ユーザーの割合は大幅に低下しましたが、これは2016年第2四半期にこのプログラムが配布を停止したことが影響していると考えられます。

対照的に、2016年第1四半期に初めて確認されたLockyは拡大傾向にあり、CTB-LockerもTeslacryptの撤退を受けて引き続き拡大を続けています。一方、ロシア語圏の国々を狙ったCryaklとScatterは着実に衰退しています。

暗号化型ランサムウェアと法人

2016年に暗号化型ランサムウェアの攻撃を受けたユーザーのうち、約22.6%が法人ユーザーでした。また法人において最も拡散している暗号化型ランサムウェアファミリーの上位10種の割合も、前表とほぼ同じでした。ただし、特筆すべき例外が1つあります。それはTrojan-Ransom.Win32.Rakhniで、2016年の法人ユーザーを狙った暗号化型ランサムウェア攻撃の2.42%がこのプログラムによるものでした。

Trojan-Ransom.Win32.Rakhniは、Trojan-Downloader.Win32.Rakhniのサポートによって拡散します。このダウンローダーは、docxファイルに埋め込まれた実行ファイルで、スパムメールの添付ファイルとして拡散するのが一般的です。Rakhniを用いる犯罪者は明らかにロシア語圏の国々の法人（具体的には人事部門）を標的としています。というのも、このdocxファイルは、採用応募フォーム（「Резюме Жанна.docx」など）を装って作成されることが一般的だからです。標的がdocxファイルを開くと、そこにPDFアイコンが現れ、それをクリックすると悪意あるダウンローダーが実行されるという仕組みです。このトロイの木馬は、相手の疑いを回避するため、履歴書としての体裁を完全に整えています。

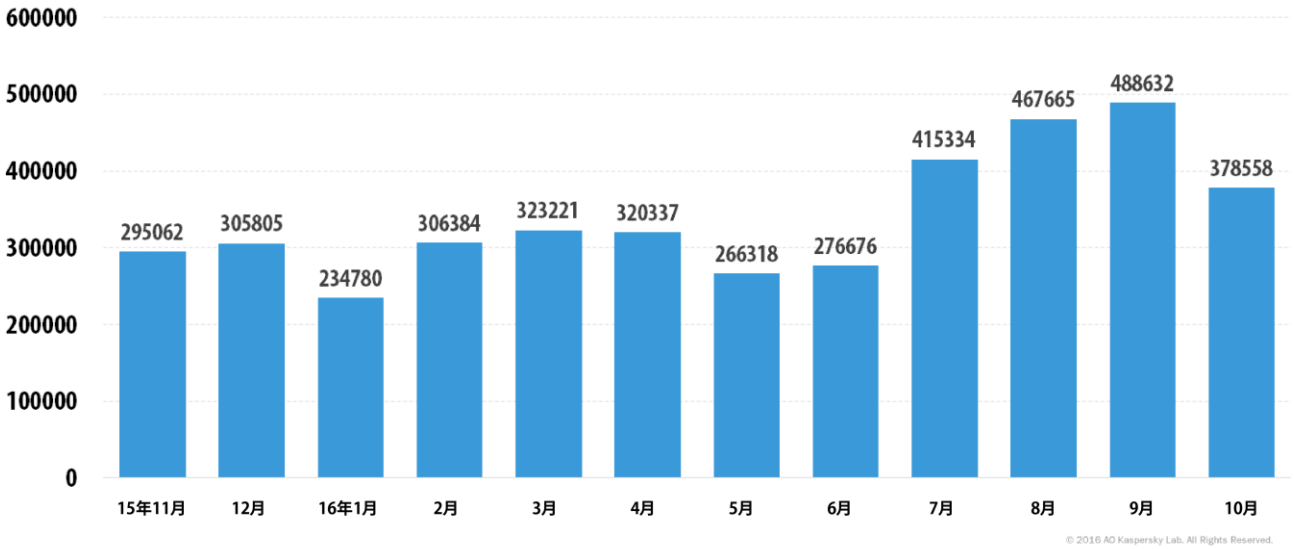
このトロイの木馬はメインのペイロード（Trojan-Ransom.Win32.Rakhni）をダウンロードし、ファイルを暗号化して身代金を要求するメッセージを表示します。

KSNのデータからは、Rakhniを用いる犯罪者が個人ユーザーを感染の標的とはしておらず、法人を狙う方法を心得ていることは明確です。このファミリーは上位10種には入っていないものの、法人では最も拡散しているランサムウェアの1つに数えられています。

金融機関におけるオンラインの脅威

新たなバンキング型トロイの木馬が次々に出現し、既存のバンキング型トロイの木馬も絶えず機能が変更されていることから、Kaspersky Labでは 2016年第2四半期は、金融系の脅威として分類される判定リストを大幅に更新することにしました。つまり、金融系マルウェアの標的の数が、前年に公開されたデータから大きく変わったということです。そこで比較のため、更新されたリストのすべてのマルウェアを考慮に入れて、前年の統計を再計算しました。

カスペルスキー製品は、オンラインバンキングで金銭を窃取するマルウェアを実行しようとする試みを、2,871,965台のデバイスでブロックしました。この数値は2015年（1,966,324台）を46%上回っています。

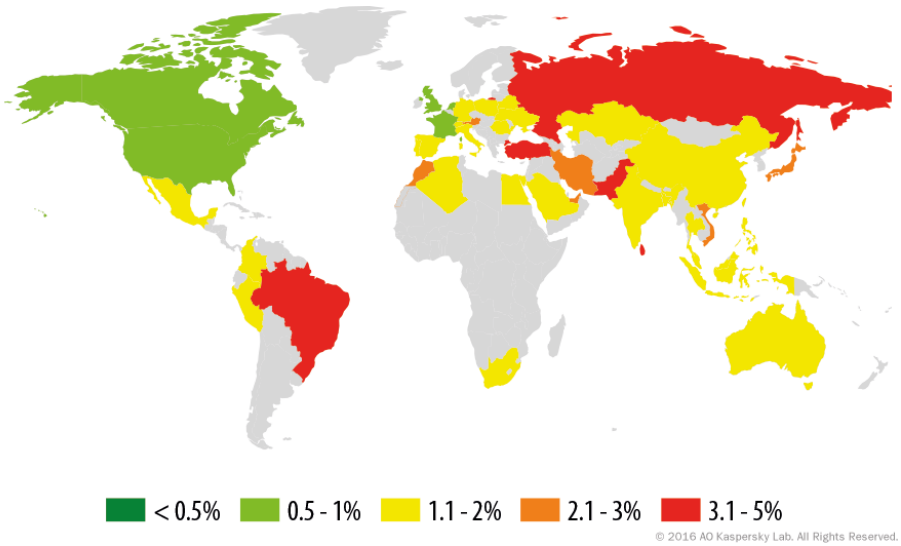


金融系マルウェアの攻撃を受けたユーザー数（2015年11月から2016年10月）

2015年末以降、攻撃を受けたデバイスの数が減少しましたが、この背景にはDyre（Dyreza）ボットネットの活動停止があります。しかし2016年中盤には攻撃件数が徐々に増加し始め、2016年9月には、モバイルバンキングユーザー（主にAndroid端末）への攻撃が増加したことにより、1か月間に攻撃を受けたデバイスの数が2014年および2015年の最大件数を上回りました。

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の評価を行うため、カスペルスキー製品の全ユーザーを母数として、統計データを算出した期間中に、この種の脅威に遭遇したユーザーの占める割合を国別に算出しました。



2016年のバンキング型マルウェア攻撃の地理的分布（攻撃を受けたユーザーの割合）

攻撃を受けたユーザーの割合が大きい上位10か国

	国*	攻撃されたユーザーの割合（%）**
1	ロシア	4.8
2	ブラジル	4.7
3	トルコ	4.5
4	スリランカ	4.5
5	パキスタン	3.8

6	オーストリア	2.6
7	ベトナム	2.4
8	アラブ首長国連邦	2.3
9	日本	2.2
10	モロッコ	2.2

* カスペルスキー製品のユーザー数が50,000未満で、バンキング型マルウェアの通知件数が7,000件未満の国は除外しています。** 全ユニークユーザーのうち、バンキング型トロイの木馬の攻撃を受けたコンピューターのユニークユーザーの割合です。

最も数値が高かったのはロシアでした。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4.8%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攻撃にあっています。これは、ロシアの全脅威の中で、金融系の脅威が流行していることを示しています。

ブラジルでは、2016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4.7%でした。各国の数値はトルコが4.5%、ドイツが2%、スイスが1.7%、フランスが1%でした。

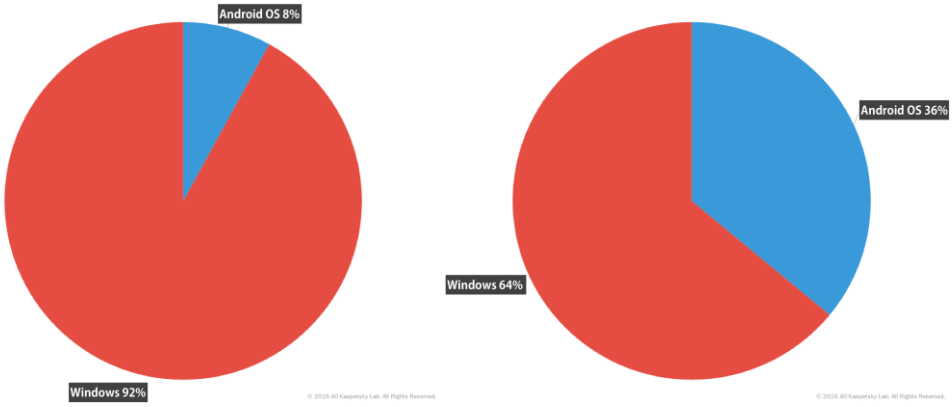
バンキング型マルウェアの上位 10 プログラム

2016年に、オンラインおよびモバイルのユーザーに対するバンキングを狙った攻撃で最も多く使用されたマルウェアの上位10種を下表に示します（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-Banker.AndroidOS.Svpeng.q	8.8
2	Trojan-Banker.Win32.Gozi.gr	5.7
3	Trojan.BAT.Qhost.abp	4.5
4	Trojan-Spy.Win32.Zbot.pef	3.5
5	Trojan-Banker.AndroidOS.Agent.ai	2.8
6	Trojan-Spy.Win32.Zbot.vho	2.5
7	Trojan-Banker.AndroidOS.Asacub.e	1.9
8	Trojan-Banker.AndroidOS.Svpeng.r	1.8
9	Trojan.Win32.Qhost.afes	1.4
10	Trojan-Banker.AndroidOS.Hqwar.t	1.2

* マルウェアの攻撃を受けた全ユーザーのうち、金融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の割合です。

バンキング型トロイの木馬の上位10種のうち、Android端末経由でモバイルバンキングのデータを取得しようとするプログラムは5種に及んでいます。Androidを標的とした攻撃の割合も、2015年の4.5倍に達しました。これは、サイバー犯罪者がユーザー行動に常に目を光らせ、その結果として、インターネットバンキングを扱うWebサイトへの攻撃から、モバイルバンキングアプリケーションの悪用へとシフトしていることを意味しています。



金融系マルウェアの標的となったデバイスタイプの割合（左：2015年、右：2016年）

Windowsを標的とした悪意あるプログラム上位10種の大半は、ブラウザーに表示されるWebページに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窃取するものです。一方、モバイルバンキング型トロイの木馬は、正規のモバイルバンキングアプリを偽のフィッシングウィンドウでカバーして表示し、金融機関から送られてくるショートメッセージをコントロールすることで、ワンタイム認証コードを取得します。

バンキング型マルウェアの1位はTrojan-Banker.AndroidOS.Svpeng.q.でした。1位の理由は、このプログラムが拡散する手段にあります。これは、大手ニュースサイトがユーザーに関連性の高い広告を掲載するなど、多くのWebポータルで使用されている広告ネットワークGoogle AdSenseを介して広がるタイプのプログラムです。このSvpengトロイの木馬の作成者は、このネットワークに悪意ある広告を置いていると考えられます。感染した広告が読み込まれると、ユーザーがその広告をタップしなくても、すぐにこのトロイの木馬が自己をダウンロードする仕組みになっています。2013年にKaspersky Labが確認した、このバンキング型トロイの木馬であるSvpengファミリーには、悪意ある機能が幅広く搭載されています。このプログラムは、インストールされ実行されるとすぐに、インストールアプリの一覧から消え、デバイスの管理権限をリクエストします（アンチウイルスソフトやユーザーによる削除を困難にするため）。このプログラムはフィッシングウィンドウ経由でユーザーの銀行カード情報を窃取し、テキストメッセージを傍受、削除、送信することが可能です。こうしたアクションはすべて、ワンタイム認証コード用のショー

トメッセージサービス（SMS）を使用する遠隔バンキングシステムを攻撃するために必要な措置とされています。

2位には、Trojan-Banker.Win32.Goziファミリーの代表的プログラムが入りました。これは、コードインジェクションのテクニックを使用して一般的なWebブラウザーの処理プロセスに入り込み、インターネットバンキングのサイトに入力された請求情報を窃取するものです。このファミリーの中には、MBR（マスターブートレコード）に感染し、OSがリセットされてもOS内に常駐するものもあります。10年前に最初のバージョンが確認されたこのトロイの木馬は、現在までに大きな変貌を遂げました。Goziは今年、バンキングデータを窃取するだけでなく、暗号化型ランサムウェアを使って脅迫ができるようにもなりました。Kaspersky Labは、Nymaimトロイの木馬のコードに、感染したコンピューターにリモートアクセスできるGoziバンカーのフラグメントが含まれていることを発見しました。つまり、このランサムウェアの被害者がインターネットバンキングを使用すると、犯罪者は金銭を要求することも、被害者の口座にあるすべての資金を窃取することもできるということです。

Zbotトロイの木馬ファミリーは長い間、トップ3の常連でしたが、モバイルバンキング型トロイの木馬の台頭により順位に変化が生じました。しかし、Zbotは消滅したわけではなく（現在4位）、Citadel、Kins、ZeusVMといったその他の非常に多くのバンキング型トロイの木馬のベースとして使われていることは、認識しておく必要があります。

3位と9位には、Qhostトロイの木馬ファミリーのプログラムが入りました。これは最もベーシックなバンキング型トロイの木馬ファミリーの1つですが、その効果はベーシックではありません。これら2つのプログラムは標的となるコンピューターにあるHostsファイルのコンテンツを変更することで、金融機関サイトへのすべてのリクエストが悪意あるサーバー経由で送信されるようにし、それによって「会話に侵入」し、ユーザーのブラウザーに表示されるデータや金融機関に送信されるデータを書き換えます。

ユーザーのオンライン感染リスクが高い国

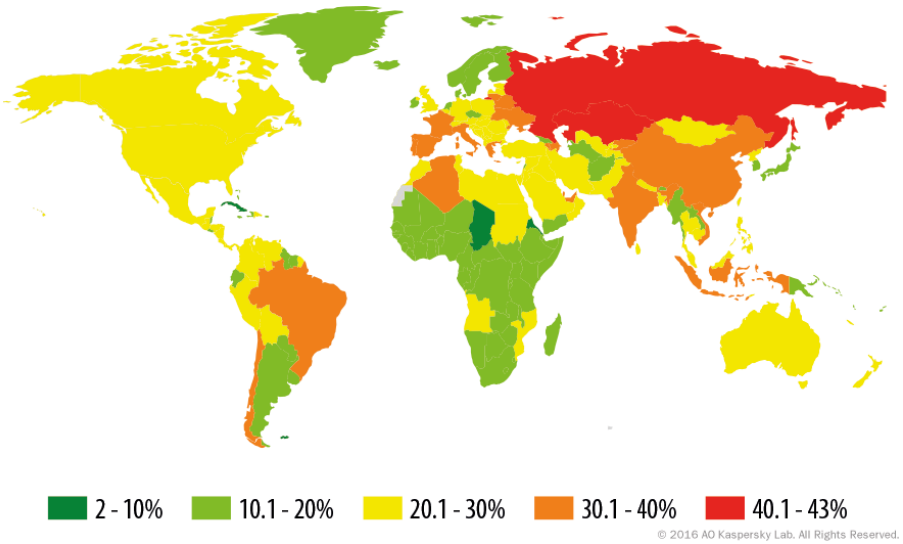
ユーザーがサイバー脅威に直面する頻度の高い国を調査するため、カスペルスキー製品ユーザーのコンピューターで検知判定が行われる頻度を国別に算出しました。そのデータから、各国のコンピューターが感染にさらされるリスクが明らかになり、世界各国のコンピューターを取り囲む環境の深刻さを示すことができます。

このデータには、悪意あるプログラムによる攻撃のみが含まれています。Webアンチウイルスコンポーネントによって検知された、潜在的に危険なプログラムや不要なプログラム（リスクウェアやアドウェアなど）は含まれません。

ユーザーのオンライン感染リスクが高い国上位20か国

	国*	ユニークユーザーの割合（%）**
1	ロシア	42.15
2	カザフスタン	41.22
3	イタリア	39.92
4	ウクライナ	39.00
5	ブラジル	38.83
6	アゼルバイジャン	38.81
7	スペイン	38.21
8	ベラルーシ	38.04
9	アルジェリア	37.11
10	ベトナム	36.77
11	中国	36.53
12	ポルトガル	35.86
13	フランス	34.74
14	アルメニア	33.01
15	ギリシャ	32.99
16	チリ	32.82
17	インド	32.61
18	カタール	32.53
19	インドネシア	32.30
20	モルドバ	31.42

* カスペルスキー製品のユーザー数が50,000未満の国は除外しています。** その国のカスペルスキー製品の全ユーザーのうち、悪意あるプログラムのWebベースの攻撃を受けたコンピューターのユニークユーザーの割合です。



2016年の悪意あるWebベース攻撃の地理的分布（攻撃を受けたユーザーの割合）

感染リスクのレベルに基づいて、各国を3つのグループに分類できます。

1. **高リスクのグループ（40%以上）**
   20 か国のうちの上位 2 か国（ロシア、カザフスタン）がこのグループに該当しました。
2. **中程度のリスクのグループ（20～39.9%）**
   このグループには 105 か国が該当しました。トルコ（29.3%）、カナダ（29.5%）、ポーランド（28.7%）、ルーマニア（27.4%）、メキシコ（26.8%）、オーストラリア（26.2%）、ドイツ（26.2%）、ベルギー（25.3%）、オーストリア（24.8%）、米国（24%）、スイス（23.6%）、英国（22.1%）、ハンガリー（21.3%）、アイルランド（20%）などです。
3. **低リスクのグループ（0～19.9%）**
   オンライン環境が安全な国には、チェコ共和国（19.6%）、アルゼンチン（19.5%）、日本（17.7%）、ノルウェー（15.9%）、スウェーデン（15.2%）、ジョージア（14.6%）、オランダ（14.5%）、デンマーク（12.2%）があります。

2016年、ユーザーがオンラインの状態で、31.9%のコンピューターが悪意あるプログラムのWebベースの攻撃を少なくとも1回以上受けました。

ユーザーローカル環境の脅威

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、カスペルスキー製品のファイルアンチウイルスコンポーネント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した統計に関する分析結果を示します。

2016年、ファイルアンチウイルスコンポーネントは、4,071,588種の悪意あるプログラムと不審なプログラムを検知しました。

ユーザーのコンピューターで検知されたプログラムの上位20種

下の表に、ユーザーのコンピューターで最も頻繁に検知された脅威の上位20種を示します。なお、この表にはアドウェアとリスクウェアのプログラムは含まれていません。

	検知名*	ユニークユーザーの割合（%）**
1	DangerousObject.Multi.Generic	42.32
2	Trojan.Win32.Generic	9.23
3	Trojan.WinLNK.Agent.gen	7.78
4	Trojan.WinLNK.StartPage.gena	6.25
5	Trojan.Script.Generic	5.86
6	Trojan.Win32.AutoRun.gen	4.78
7	Virus.Win32.Sality.gen	4.34
8	Trojan.WinLNK.Runner.jo	4.17
9	Worm.VBS.Dinihou.r	3.58
10	Trojan.WinLNK.Agent.ew	3.13
11	Trojan.Win32.Starter.yy	2.93
12	Trojan-Downloader.Script.Generic	2.80
13	Trojan.Win32.Autoit.cfo	2.27

14	Trojan.Win32.Wauchos.a	2.03
15	Virus.Win32.Nimnul.a	2.02
16	Trojan-Proxy.Win32.Bunitu.avz	1.90
17	Worm.Win32.Debris.a	1.83
18	Trojan.Win32.Hosts2.gen	1.80
19	Trojan-Dropper.VBS.Agent.bp	1.34
20	Trojan.WinLNK.StartPage.ab	1.26

* カスペルスキー製品の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ンモジュールによって生成されたマルウェア検知判定です。** 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のうち、ファイルアンチウイルスで、これらのプログラムがコンピューターから検知されたユーザーの割合です。

DangerousObject.Multi.Genericの検知名は、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（42.32%）。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、ユーザーコンピューター内のアンチウイルスデータベースに登録されていなくても、Kaspersky Lab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ある場合は検知されます。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。

Virusファミリー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5.53%でしたが、2016年は4.34%に減少しました。Virus.Win32.Nimnulの場合、影響を受けたユーザーの割合は2015年が2.37%で、2016年は2.02%でした。19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検知による判定名とVirusファミリー以外に、リムーバブルメディアに蔓延しているWormファミリー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。Wormは攻撃者の管理下になくとも、長期にわたって自己増殖を続けることができます。

たとえば、上位20種に初めて入ったTrojan.Win32.Wauchos.aは、Worm.Win32.Debrisファミリーのコンポーネントで、トロイの木馬をリムーバブルドライブにインストールします。このトロイの木馬は他のマルウェアをC&Cサーバーから読み込むことが可能で、Worm.Win32.Debrisの新バージョンを読み込むようになっています。

Trojan-Proxy.Win32.Bunitu.avzは、Trojan-Proxyファミリーです。自己複製のメカニズムを備えていないため、このリストの常連ではありません。

今年のTrojan.Win32.Hosts2.genサンプルの大半は、アンチウイルス製品サイトおよびサーバーへのアクセスをブロックするHostsファイルで構成されていました。

ユーザーのローカル環境で感染リスクが高い国

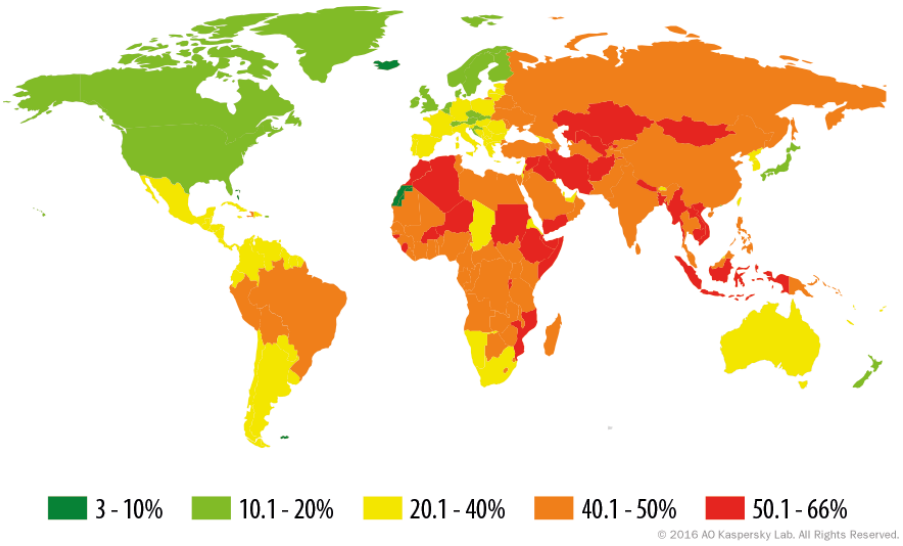
カスペルスキー製品のファイルアンチウイルスコンポーネントがこの1年間に検知した数を国別に算出しました。このデータには、ユーザーのコンピューターまたはコンピューターに接続されたリムーバブルメディア（USB、カメラや携帯電話のメモリカード、外部ハードディスクなど）上で検知された悪意あるプログラムが含まれています。この統計は、各国のコンピューターの感染レベルを示しています。

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	65.69
2	ソマリア	63.90
3	アフガニスタン	61.05
4	ルワンダ	60.17
5	アルジェリア	59.80
6	ラオス	58.90
7	エチオピア	57.75
8	バングラデシュ	57.39
9	ネパール	57.35
10	モンゴル	56.89
11	カンボジア	55.90
12	インドネシア	55.51
13	モザンビーク	54.95
14	ウズベキスタン	54.03
15	イラク	53.97
16	シリア	53.44
17	モロッコ	53.39
18	ミャンマー	53.11
19	カザフスタン	53.02
20	ニジェール	52.96

* カスペルスキー製品のユーザー数が50,000未満の国は除外しています。** カスペルスキー製品のユーザーのうち、マルウェアが端末内の脅威としてブロックされたコンピューターのユニークユーザーの割合です。

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36.8%から、少なくとも1つの悪意あるプログラムが発見されました。



2016年の悪意あるプログラムによるローカル環境への感染の地理的分布（攻撃を受けたユーザーの割合）

ユーザーのローカル環境でのリスクに対するレベルに基づいて、各国をグループに分類できます。

- **リスク最大のグループ（60%超）**

  上位 20 か国のうちこのカテゴリに分類されたのは、4 か国でした。

- **高リスクのグループ（41～60%）**

  イラン（51.9%）、インド（50.4%）、ベラルーシ（48.7%）、中国（48.6%）、ウクライナ（47.9%）、サウジアラビア（44.04%）、ロシア（43.6%）、トルコ（42%）、ブラジル（41.3%）など。

- **中程度のリスクグループ（21～40.99%）**

  モルドバ（40.8%）、アルメニア（40.4%）、メキシコ（39.1%）、南アフリカ（30.5%）、セルビア（28.6%）、ポーランド（29%）、ブルガリア（27.4%）、スペイン（27%）、ギリシャ（26.2%）、イタリア（24.8%）、イスラエル（24.8%）、ハンガリー（23.4%）、フランス（21.1%）など。

- **安全性の高い上位 10 か国は次の通りです。**

	国	ユニークユーザーの割合（%）*
1	デンマーク	10.4
2	スウェーデン	13.0

3	オランダ	13.9
4	日本	13.9
5	ノルウェー	14.5
6	アイルランド	15.1
7	チェコ共和国	15.2
8	スイス	15.75
9	米国	16.48
10	ニュージーランド	16.78

安全性の高い上位10か国では、この1年間に1回以上の攻撃を受けたユーザーのコンピューターの割合は、平均で16%でした。

株式会社カスペルスキー
PR-1033-201612