Kaspersky Security Bulletin 2014:

2014年 脅威の統計概要

KASPERSKY lab

目次

Maria **GARNAEVA**
Victor **CHEBYSHEV**
Denis **MAKRUSHIN**
Roman **UNUCHEK**
Anton **IVANOV**

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213の国と地域に及ぶ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。

提供されたデータは、2013年11月から2014年10月までのものです。

数字で見る2014年

—KSNのデータによると、カスペルスキー製品は**6,167,233,068**件の脅威を検知して無害化しました。

—カスペルスキーの製品がブロックした、Mac OS Xベースのコンピューターに対する感染の試みは**3,693,936**件でした。

—カスペルスキーの製品は、Androidデバイスへの攻撃**1,363,549**件をブロックしました。

—カスペルスキー製品は、全世界のオンラインリソースから実行された**1,432,660,467**件の攻撃をブロックしました。

—サイバー犯罪者が攻撃に使用したユニークホスト数は、**9,766,119**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**44**%は、米国とドイツに置かれた悪意あるWebリソースを使用して実行されていました。

—ユーザーのコンピューターの**38**%が、年間に少なくとも1回はWebからの攻撃対象になっていました。

—2014年にユーザーのコンピューター上でバンキング型マルウェアを実行しようとして無効化されたケースは、**1,910,520**件に及びました。

—カスペルスキーのウェブアンチウイルスは、**123,054,503**種類のオブジェクト（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。

—カスペルスキーのアンチウイルス製品は、合計**1,849,949**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。

モバイルの脅威

Kaspersky Labがレポート期間中に検知したデータは以下のとおりです。

— **4,643,582**の悪意あるインストールパケット

— **295,539**の新しい悪質モバイルプログラム

— **12,100**種のモバイルバンキング型トロイの木馬

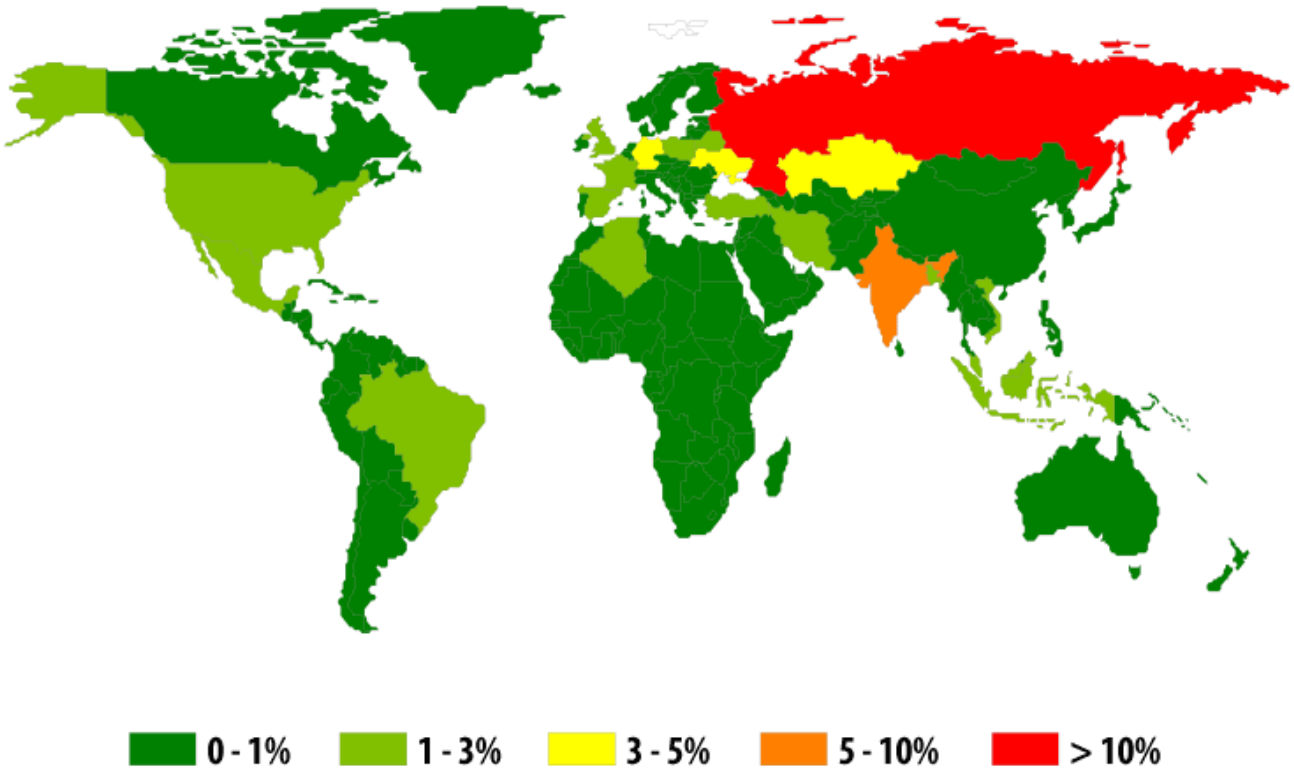
Kaspersky Labは2013年11月初旬から2014年10月末までに、**1,363,549**件（ユニーク数）の攻撃を撃退しました。2012年から2013年の同期間を見ると、この数値は**335,000**件でした。Android端末に対する攻撃は、1年前と比べて4倍に増加したことになります。

Androidユーザーの**19%**が、1年間に少なくとも1度はモバイルの脅威を経験しました。これはほぼ5人に1人の割合です。

Androidに対する攻撃の**53%**で、金銭を目的とするモバイルトロイの木馬が使用されていました（SMS型トロイの木馬、バンキング型トロイの木馬）。

モバイルの脅威の地理的分布

モバイルマルウェアによる攻撃は、**200**か国以上で確認されています。



攻撃された全ユーザー数に対し、攻撃されたユーザー数が占める割合

攻撃を受けたユーザー数が多い上位10か国

	国	攻撃を受けたユーザーの割合*
1	ロシア	45.7%
2	インド	6.8%
3	カザフスタン	4.1%
4	ドイツ	4.0%
5	ウクライナ	3.0%
6	ベトナム	2.7%
7	イラン	2.3%
8	英国	2.2%
9	マレーシア	1.8%
10	ブラジル	1.6%

**各国で攻撃されたユーザーの数を、攻撃された全ユーザーの数で割った値*

攻撃を受けたユーザーの数で見ると、ロシアが引き続き1位でした。

記録された攻撃の数は、国ごとのユーザー数によって大きく変わります。そこで、各国のモバイルマルウェアによる感染の危険性を評価するため、ユーザーがインストールしようとしたアプリケーションの総数に悪質アプリケーションが占める割合を調べました。この方法で算出された数字は、上記のデータと大きく異なります。

感染のリスクで比較した上位10か国

	国*	悪質なアプリケーションが占める割合
1	ベトナム	2.34%
2	ポーランド	1.88%
3	ギリシャ	1.70%
4	カザフスタン	1.62%
5	ウズベキスタン	1.29%
6	セルビア	1.23%
7	アルメニア	1.21%
8	チェコ	1.02%
9	モロッコ	0.97%
10	マレーシア	0.93%

** ダウンロードされたアプリケーションの数が10万未満の国は計算結果から除外*

トップはベトナムで、ユーザーがダウンロードしようとした全アプリケーションのうち**2.34%**がマルウェアでした。

ロシアは攻撃を受けた数で見ると圧倒的な第1位でしたが、感染のリスクという点では22位（**0.69%**）にとどまっています。

その他の国の感染リスクは、スペインが**0.54%**、ドイツが**0.18%**、英国が**0.16%**、イタリアが**0.09%**、米国が**0.07%**となっています。最も良い状況だったのは日本で、ユーザーがインストールしようとした全アプリケーションのうち、マルウェアは0.01%にすぎませんでした。

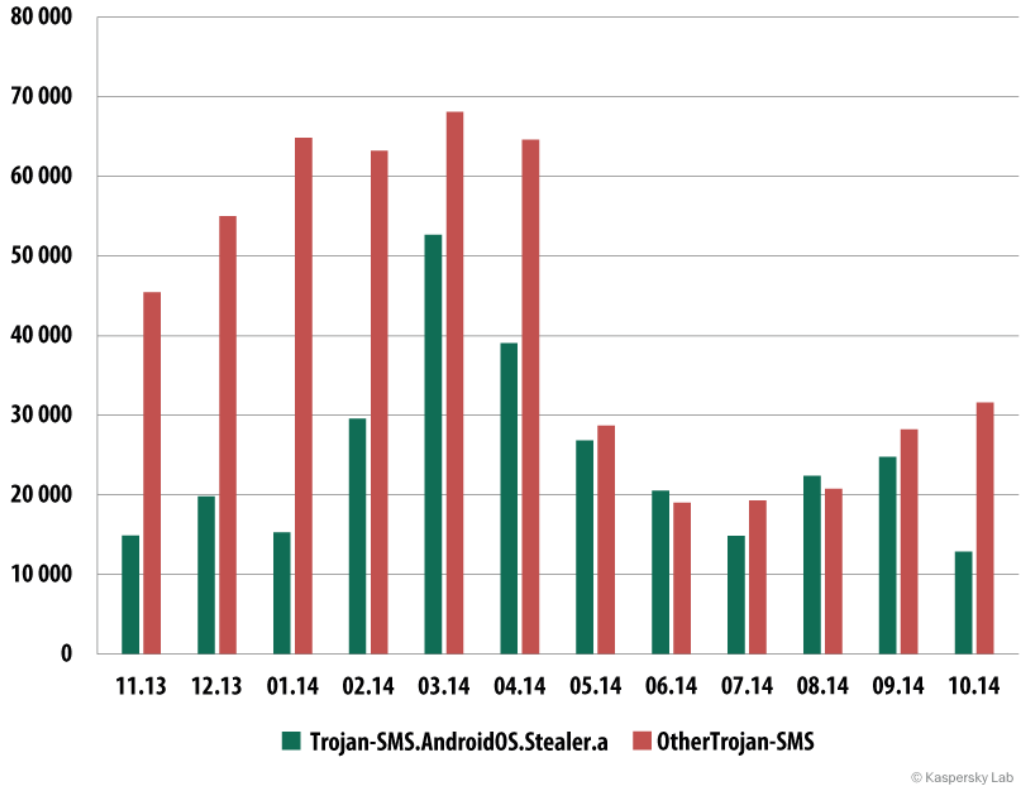
2014年のモバイルの脅威上位20種

	検知名	攻撃の割合
1	Trojan-SMS.AndroidOS.Stealer.a	18.0%
2	RiskTool.AndroidOS.MimobSMS.a	7.1%
3	DangerousObject.Multi.Generic	6.9%
4	RiskTool.AndroidOS.SMSreg.gc	6.7%
5	Trojan-SMS.AndroidOS.OpFake.bo	6.4%
6	AdWare.AndroidOS.Viser.a	5.9%
7	Trojan-SMS.AndroidOS.FakeInst.a	5.4%
8	Trojan-SMS.AndroidOS.OpFake.a	5.1%
9	Trojan-SMS.AndroidOS.FakeInst.fb	4.6%
10	Trojan-SMS.AndroidOS.Erop.a	4.0%
11	AdWare.AndroidOS.Ganlet.a	3.8%
12	Trojan-SMS.AndroidOS.Agent.u	3.4%
13	Trojan-SMS.AndroidOS.FakeInst.ff	3.0%
14	RiskTool.AndroidOS.Mobogen.a	3.0%
15	RiskTool.AndroidOS.CallPay.a	2.9%
16	Trojan-SMS.AndroidOS.Agent.ao	2.5%
17	Exploit.AndroidOS.Lotoor.be	2.5%
18	Trojan-SMS.AndroidOS.FakeInst.ei	2.4%
19	Backdoor.AndroidOS.Fobus.a	1.9%
20	Trojan-Banker.AndroidOS.Faketoken.a	1.7%

上位20種のプログラムのうち10種がSMS型トロイの木馬で、Stealer、OpFake、FakeInst、Agent、Eropのファミリーに属するものでした。

年間を通じて最も広く拡散したファミリーはTrojan-SMS.AndroidOS.Stealer.aです。他を大きく引き離してトップとなりました。

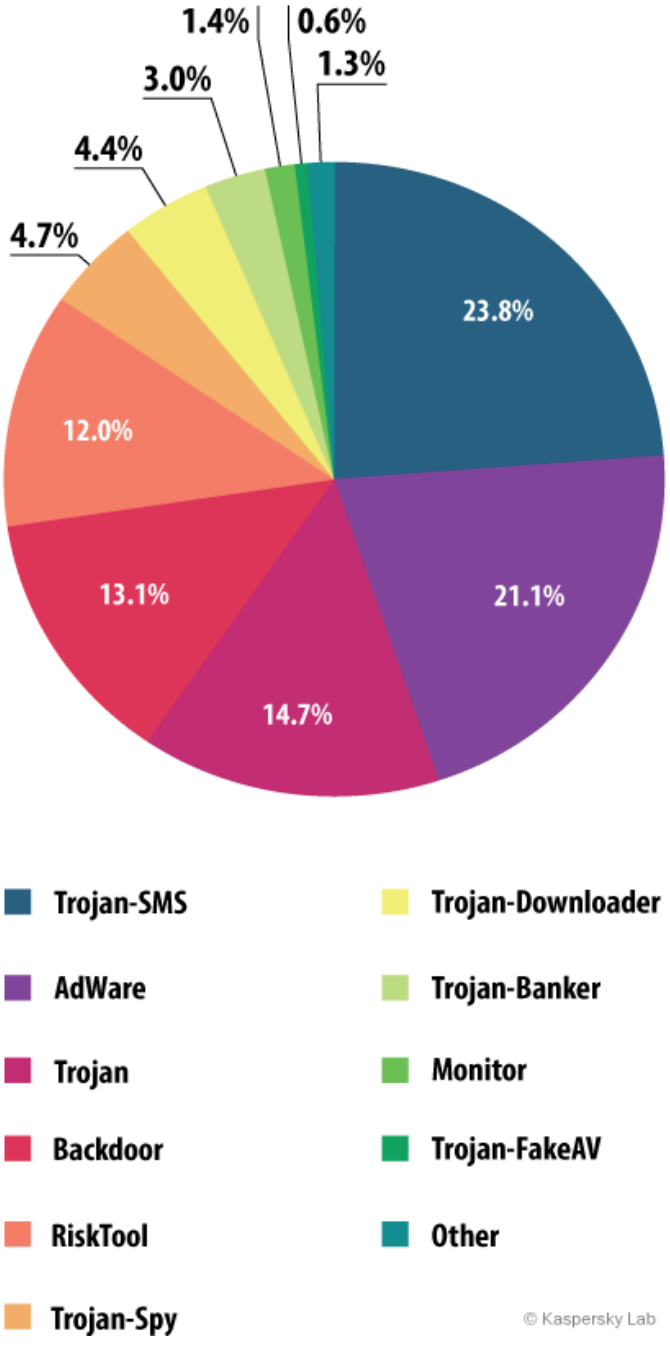
このSMS型トロイの木馬は非常に速いペースで拡散しています。2014年5月以降のStealerによる攻撃件数は、他のSMS型トロイの木馬すべてを合わせた件数に匹敵します。



Trojan-SMS.AndroidOS.Stealer.aによる攻撃を受けたユーザーの数と、他のすべてのSMS型トロイの木馬による攻撃を受けたユーザーの総数（2013年11月～2014年10月）

SMS型トロイの木馬による攻撃の減少

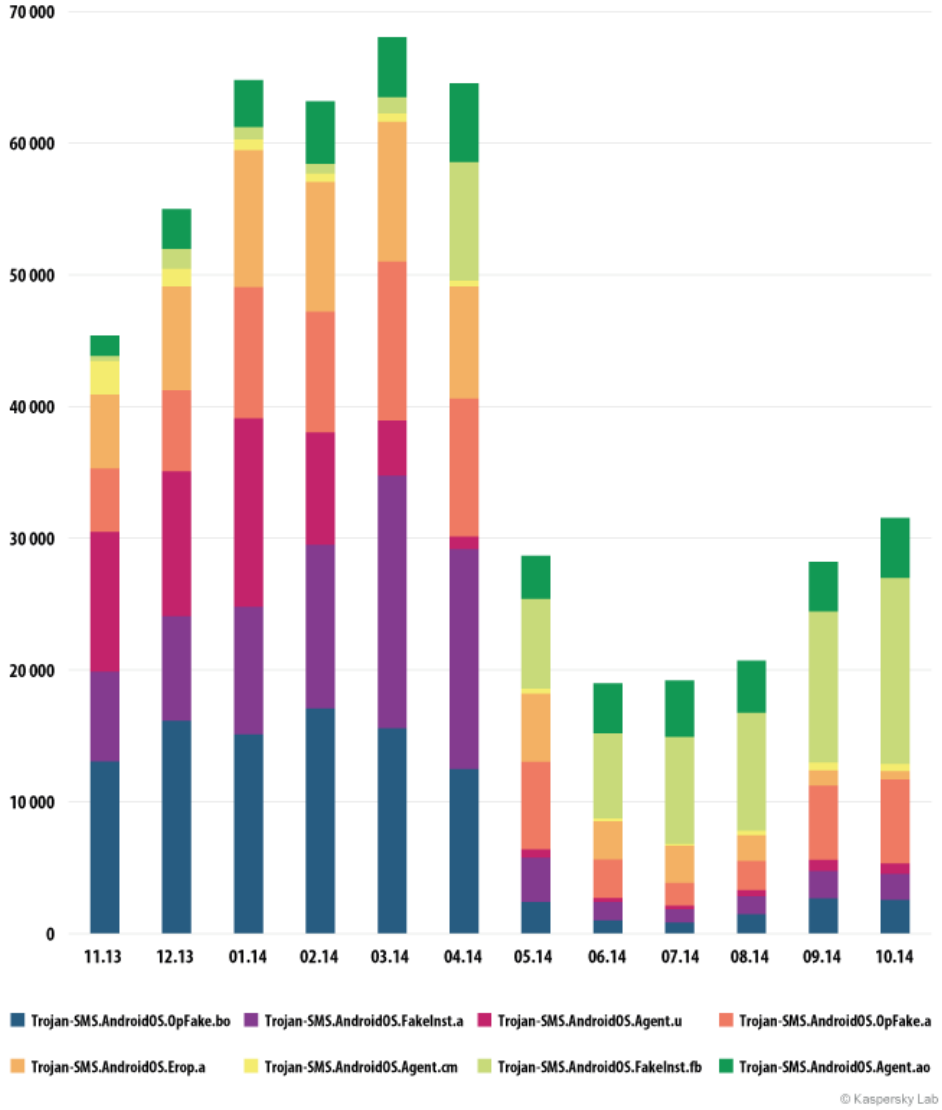
前回と変わらず、モバイルマルウェアの最大のタイプはSMS型トロイの木馬でした。今回のデータでも全体の**23.9%**を占めています。



モバイルの脅威のタイプ別分布（Kaspersky Lab調べ）

しかし、上の棒グラフでも分かるように、2014年の後半に入るとSMS型トロイの木馬による攻撃は減少しています。そのため、年間で見た総数は**12.3%**の減少となりました。

以下では、サイバー犯罪で最も多用されるSMS型トロイの木馬について、分布状況の変化をもう少し詳しく見ていきます（Stealer.aは除く）。



主要SMS型トロイの木馬の攻撃を受けたユーザーの数
（2013年11月～2014年10月）

ロシアはSMS型トロイの木馬が特に蔓延している国ですが、同国で検知されたSMS型トロイの木馬の数は5月に入って激減しています。これは、ロシアの有料メッセージに関する制度に変更があったことが原因です。2014年5月、ロシアの携帯電話会社は料金情報通知（AoC）制度の利用を義務付けられました。モバイルデバイスから有料番号にメッセージを送信する場合、電話会社はそのデバイスの所有者にサービス料金を通知して、支払いの確認を受けなければなりません。

そのため、SMS型トロイの木馬は犯罪者にとっての利益が小さくなり、その犯罪性も明白になりました。今では、有料番号にSMSを送信し、電話会社からの要求を傍受して、ユーザーに代わって確認を返信するトロイの木馬を使用しなければ、利益を得られなくなっています。

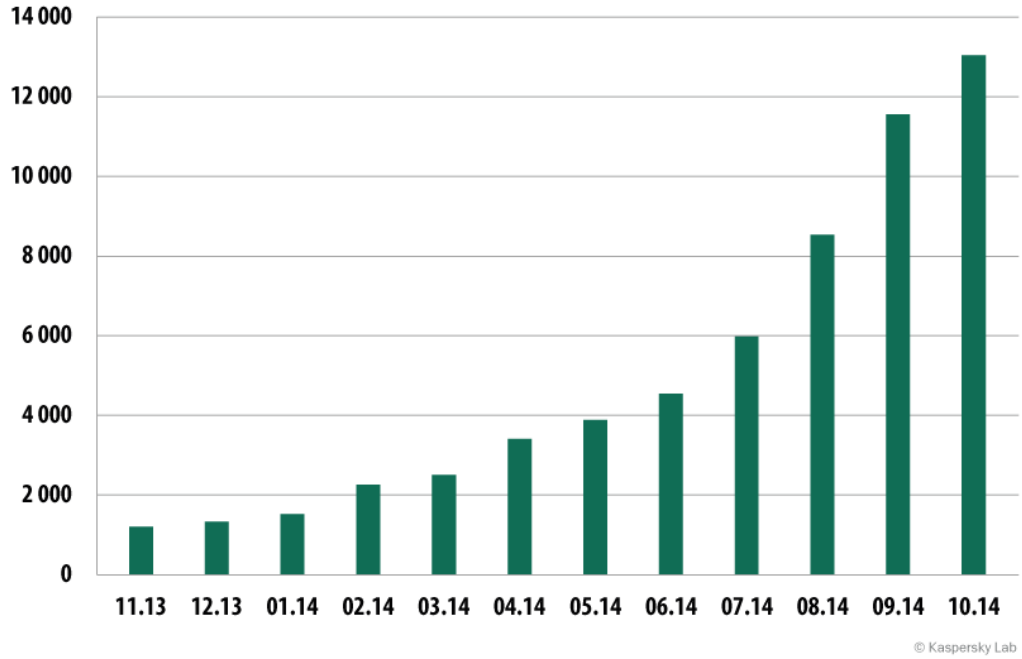
結果的に、合法性の疑わしいプログラムに関わり、これまでSMS型トロイの木馬の機能を持つアプリケーションを拡散していた業者は、この手口に見切りをつけています。こうした業者の基本的な手口は、有料サービスの提供について説明を曖昧にする、あるいは登録やサービスの料金を提示しないという方法だったためです。

ロシアでSMS型トロイの木馬を開発していた犯罪者は、そのビジネスから撤退し、新しいプロジェクトを探すことになるでしょう。こうした犯罪者が、標的を他国のユーザーに切り換える可能性や、銀行を狙うプログラムなど、さらに深刻なマルウェアを開発する可能性が考えられます。できることなら、ごく一部でも犯罪の世界と決別し、そのスキルを合法的な目的に活かしてほしいものです。

こうした分布パターンの変化は、OpFake.boやFakeInst.a、OpFake.aなど、かつて隆盛をきわめたSMS型トロイの木馬で顕著に見られます。以前は毎月**10,000〜20,000**件あった攻撃が、今では**1,000〜2,000**件にまで減少しています。

モバイルバンキング型トロイの木馬

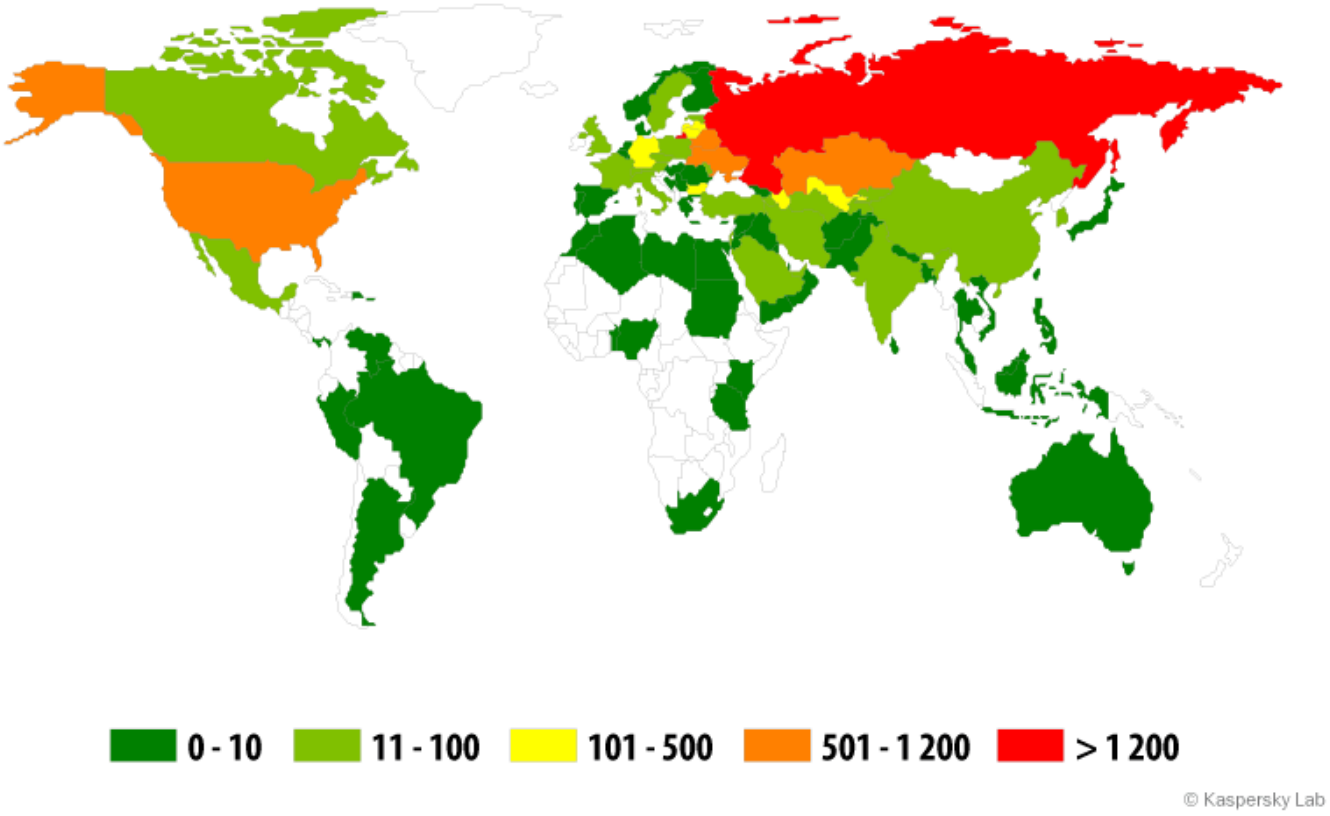
当該期間に検知されたモバイルバンキング型トロイの木馬は**12,100**種でした。2013年比で9倍となっています。



Kaspersky Labが検知したモバイルバンキング型トロイの木馬の数（2013年11月〜2014年10月）

この1年間でモバイルバンキング型トロイの木馬による攻撃を1回以上受けたユーザーは**45,032**人でした。

攻撃のあった国の数も増加傾向にあり、モバイルバンキング型トロイの木馬によって1回以上の攻撃があった国は全世界で**90**か国を数えました。



モバイルバンキングの脅威の地理的分布
（2013年11月～2014年10月の期間に攻撃を受けたユーザーの数）

バンキング型トロイの木馬による攻撃があった上位10か国

	国	攻撃を受けたユーザー数	攻撃が占める割合*
1	ロシア	39,561	87.85%
2	カザフスタン	1,195	2.65%
3	ウクライナ	902	2.00%
4	米国	831	1.85%
5	ベラルーシ	567	1.26%
6	ドイツ	203	0.45%
7	リトアニア	201	0.45%
8	アゼルバイジャン	194	0.43%
9	ブルガリア	178	0.40%
10	ウズベキスタン	125	0.28%

** 各国で攻撃を受けたユーザーの数を、攻撃を受けた全ユーザー数で割った値*

このランキングでは、引き続きロシアがトップでした。

Mac OS Xを狙う脅威

Mac OS X搭載コンピューター向けのカスペルスキー製品が2014年にブロックした感染の試みは**3,693,936**件でした。

Kaspersky LabのエキスパートはMac OS Xを狙う悪質プログラムを新たに**1,499**種検知しました。前年から**200**サンプルの増加となっています。

カスペルスキー製品ユーザーの2人に1人が悪意ある攻撃にさらされました。

平均的なMacユーザーは年間で**9**件の脅威に遭遇しています。

Mac OS Xを標的とする脅威の上位20種

	検知名	攻撃の割合*
1	AdWare.OSX.Geonei.b	9.04%
2	Trojan.Script.Generic	5.85%
3	Trojan.OSX.Vsrch.a	4.42%
4	Trojan.Script.Iframer	3.77%
5	AdWare.OSX.Geonei.d	3.43%
6	DangerousObject.Multi.Generic	2.40%
7	AdWare.OSX.Vsrch.a	2.18%
8	Trojan.Win32.Generic	2.09%
9	AdWare.OSX.FkCodec.b	1.35%
10	Trojan.OSX.Yontoo.i	1.29%
11	Trojan-PSW.Win32.LdPinch.ex	0.84%
12	AdWare.Win32.Yotoon.heur	0.82%
13	Trojan.OSX.Yontoo.j	0.80%
14	Exploit.Script.Generic	0.76%
15	AdWare.OSX.Bnodlero.a	0.58%
16	AdWare.JS.Agent.an	0.57%
17	Trojan.OSX.Yontoo.h	0.52%
18	Exploit.PDF.Generic	0.51%
19	AdWare.Win32.MegaSearch.am	0.50%
20	Trojan.Win32.AutoRun.gen	0.43%

** それぞれの悪質プログラムによる攻撃を受けたユーザーの数を、攻撃を受けた全ユーザー数で割った値*

トップも含めた上位20種のプログラムのほぼ半数が、アドウェアでした。こうしたプログラムは主に、開発者の公式Webサイト以外のソフトウェアストアからダウンロードされた場合に、正規プログラムに付随してユーザーのコンピューターに侵入します。正規プログラムがアドウェアの感染手段となっている可能性があります。ユーザーのコンピューターにインストールされると、ブラウザーのブックマークに広告リンクを追加する、既定の検索エンジンを変更する、コンテキストに応じた広告を表示する、などの動作が実行されます。

興味深いことに、8位にはWindows OSに感染するTrojan.Win32.Genericが入っています。これはおそらく、Trojan.Win32.GenericがWindows環境で稼働する仮想マシンに侵入できるためと考えられます。

2014年にKaspersky Labのエキスパートが検知したMac OS X向け悪質プログラムのうち、以下のものを個別に説明します。

— **Backdoor.OSX.Callme** - 犯罪者がシステムへのリモートアクセスに利用するバックドア。同時に連絡先リストを盗み出しますが、これは次の標的を探すためと考えられます。特別に細工されたMS Word文書の本文に埋め込まれて拡散され、その文書を開くとシステムの脆弱性を突いてバックドアを作成します。

— **Backdoor.OSX.Laoshu** - 1分ごとにスクリーンショットを撮影する悪質プログラム。このバックドアは開発元の信頼できる証明書によって署名されています。作成者がApp Storeで配信しようとしていたと見られます。

— Backdoor.OSX.Ventir - マルチモジュールのトロイの木馬型スパイウェアで、リモート制御機能を隠し持っています。キー入力を傍受するドライバー「logkext」が含まれており、そのソースコードは一般公開されています。

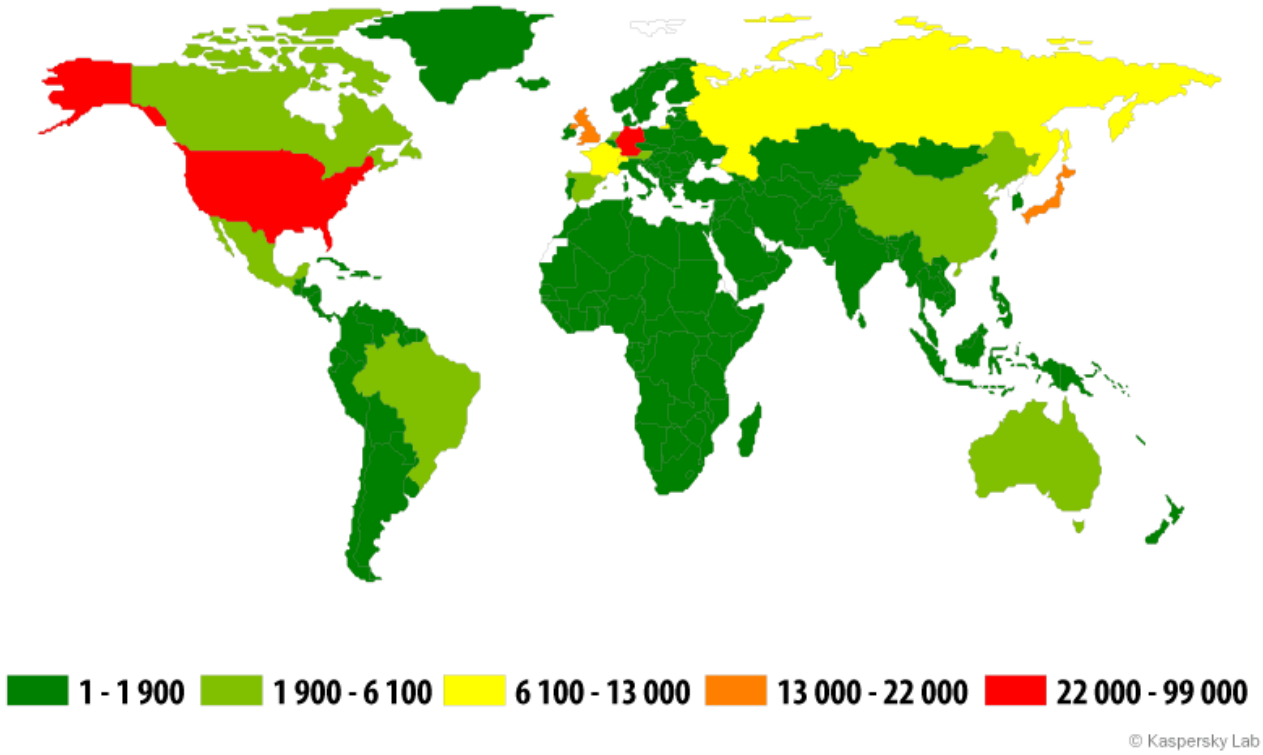
— Trojan.OSX.IOSinfector - Trojan-Spy.IPhoneOS.Mekir（OSX/Crisis）のモバイルバージョンをインストールします。

— Trojan-Ransom.OSX.FileCoder - OS Xを標的とした初のファイルコーダー。理由は不明ながらマルウェア開発を断念した開発者によって作成され、条件付きで動作するプロトタイプです。

— Trojan-Spy.OSX.CoinStealer - Bitcoinの窃盗を目的とした初のOS X向けマルウェア。オープンソースコードで作成された各種Bitcoinユーティリティに偽装し、悪意あるブラウザー拡張機能やパッチ適用済みのbitcoin-qtをインストールします。

— Trojan-Downloader.OSX.WireLurker - 標的のデータを盗み出す珍しいマルウェア。Macコンピューターだけでなく、Macに接続されたiOSデバイスも攻撃します。このマルウェアにはWindowsバージョンもあります。OS XとiOS向けのアプリを販売する中国の著名なストアから拡散しています。

脅威の地理的分布



2014年のMac OS Xに対する攻撃の地理的分布
（攻撃を受けた全ユーザー数に基づく）

攻撃があった上位10か国

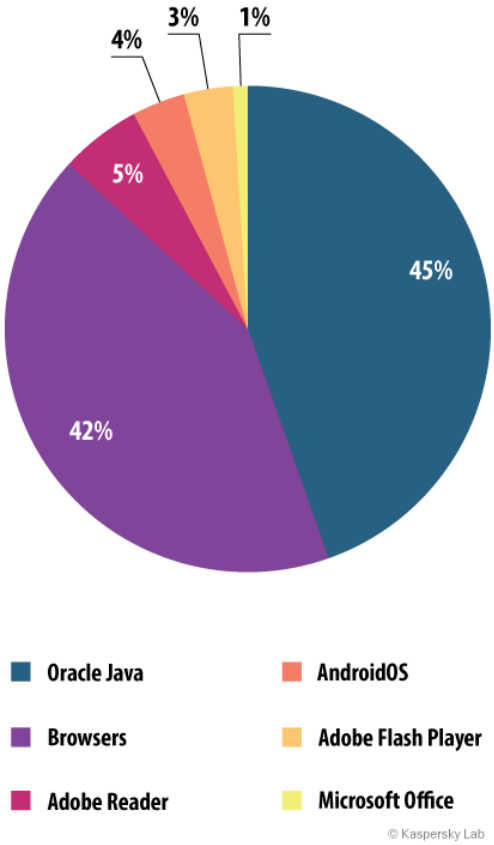
	国	攻撃を受けたユーザー数	攻撃が占める割合*
1	米国	98,077	39.14%
2	ドイツ	31,466	12.56%
3	日本	13,808	5.51%
4	英国	13,763	5.49%
5	ロシア	12,207	4.87%
6	フランス	9,239	3.69%
7	スイス	6,548	2.61%
8	カナダ	5,841	2.33%
9	ブラジル	5,558	2.22%
10	イタリア	5,334	2.13%

** 攻撃を受けたユーザーの国別の割合*

ここでは**米国**がトップ（39.14%）となりました。これは同国でApple製コンピューターの人気が高いためと考えられます。2位が**ドイツ**（12.56%）で、**日本**（5.51%）がそれに続いています。

犯罪者に利用される脆弱なアプリケーション

脆弱なアプリケーションのグラフ(下図)は、カスペルスキー製品によってブロックされたエクスプロイトに関する情報に基づいています。これらのエクスプロイトは、インターネット攻撃や、ローカルアプリケーション(モバイルデバイスにインストールされたアプリケーションなど)への攻撃で、ハッカーに利用されています。



2014年に犯罪者が利用したエクスプロイトのアプリケーション攻撃別の分布

2014年に犯罪者が最も多く悪用したのはOracle Javaの脆弱性でした。ただし、Javaの脆弱性の悪用は2014年を通じて減少を続けており、全体に占める割合は2013年の**90.5%**に対し2014年は**45%**と半分以下になっています。これは、古い脆弱性が対処され、新しい脆弱性に関する情報が不足しているためと考えられます。

2位は各種ブラウザーのカテゴリ（**42%**）で、Internet Explorer、Google Chrome、Mozilla Firefoxなどがこれに該当します。四半期別の数字を見ると2014年の大半で上位を占めていますが、2013年後半と2014年前半のJavaのエクスプロイトほどの数字にはなっていませんでした。

Adobe Readerの悪用が3位に続いています（5%）。この脆弱性はインターネットを介したドライブバイ攻撃で利用されており、PDFのエクスプロイトは多数のエクスプロイトパックの一部となっています。

2014年、エクスプロイトパックを利用した攻撃の数は減少しました。これには、開発者の何人かが逮捕されたなど、いくつかの理由が考えられます。また、エクスプロイトパックの多くは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への攻撃を停止しています（エクスプロイトパックは標的のコンピューターをチェックし、カスペルスキー製品がインストールされていると攻撃を中止します）。しかし、脆弱性を突く攻撃がコンピューターをマルウェアに感染させる主流の手口であることは変わっていません。

オンラインの脅威（Webベースの攻撃）

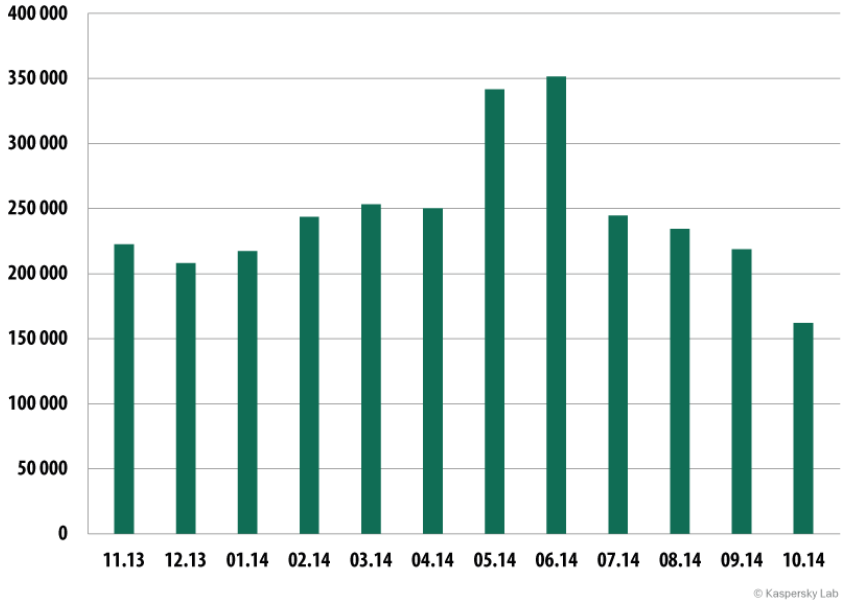
このセクションの統計はウェブアンチウイルスから取得されたものです。ウェブアンチウイルスは、悪意あるコードが悪質Webサイトや感染サイトからダウンロードされるときに、Windowsユーザーを保護します。悪質Webサイトとはサイバー犯罪者が意図的に作成したサイトを指し、感染サイトとはユーザー参加型のコンテンツ（フォーラムなど）や正規のリソースがハッキングされたものを言います。

2014年には、全世界のオンラインリソースから**1,432,660,467**件の攻撃が実行されました。カスペルスキー製品は、インターネットセッション中に1日平均**3,925,097**回ユーザーを保護したという計算になります。

主な攻撃手法はエクスプロイトパックによるものです。コンピューターがセキュリティ製品によって保護されておらず、かつ利用者の多い脆弱な（更新されていない）アプリケーションが1つ以上インストールされていれば、ほぼ確実に感染します。

銀行におけるオンラインの脅威

カスペルスキー製品はレポート期間中、オンラインバンキング口座から金銭を盗むマルウェアを起動しようとした**1,910,520**件の攻撃をブロックしました。

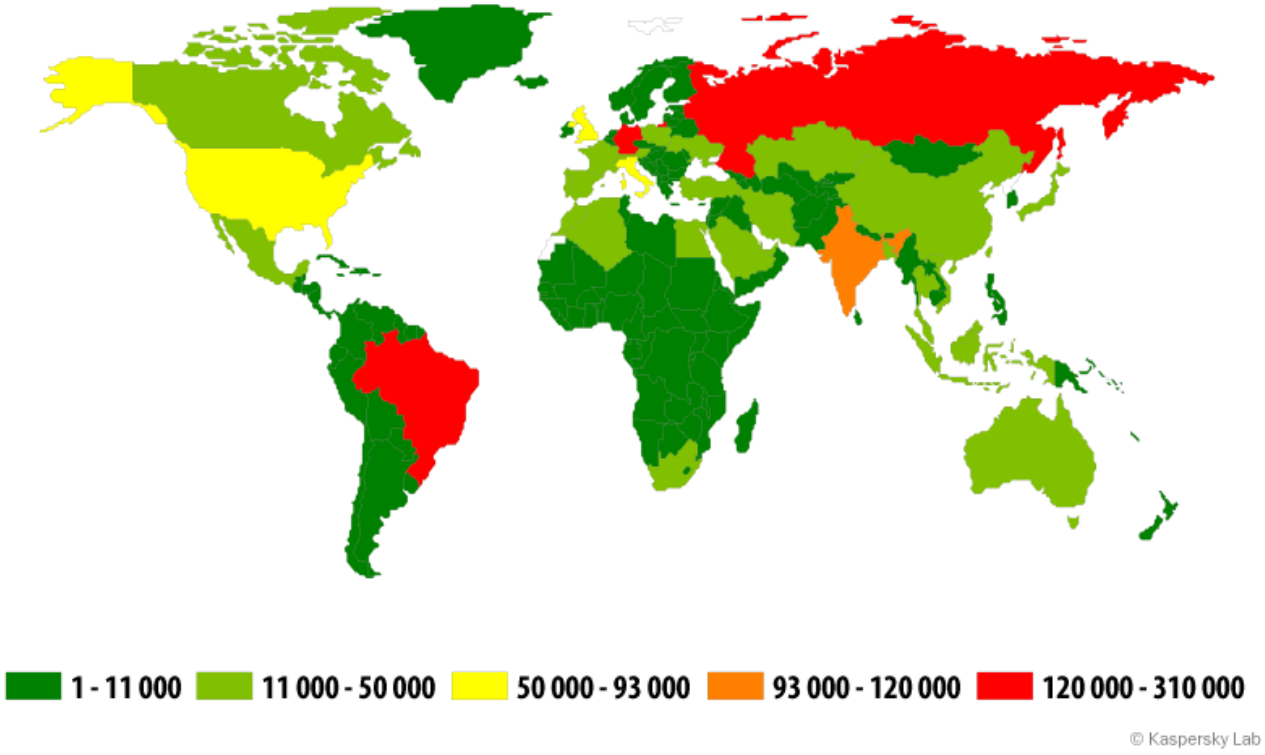


金融系マルウェアによる攻撃を受けたコンピューターの数
（2013年11月～2014年10月）

特に目立つのは、2014年の5月と6月に攻撃が大きく増えたことです。原因としては、ホリデーシーズンの始まる時期にオンラインバンキング処理が増えたことも考えられますが、この年最大のスポーツイベントだった2014ブラジルワールドカップも挙げられます。サイバー犯罪者はこの時期、金融系マルウェアを使って旅行者の支払いデータを盗もうとしていました。

2014年、銀行口座へのオンラインアクセスによって金銭を盗むプログラムの攻撃は、カスペルスキー製品で**16,552,498**件の通知が登録されました。

攻撃の地理的分布



2014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数の上位10か国

	国	攻撃を受けたユーザー数
1	ブラジル	299,830
2	ロシア	251,917
3	ドイツ	155,773
4	インド	98,344
5	米国	92,224
6	イタリア	88,756
7	英国	54,618

	国	攻撃を受けたユーザー数
8	ベトナム	50,040
9	オーストリア	44,445
10	アルジェリア	33,640

バンキング型マルウェアの上位10ファミリー

以下の表は、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利用されたプログラムの一覧です。感染の試行が報告された件数に基づいています。

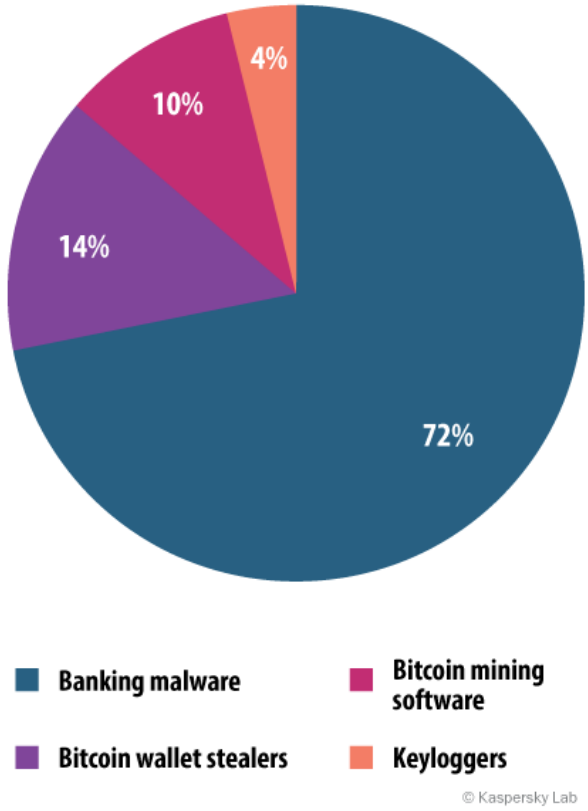
	検知名	攻撃を受けたユーザー数
1	Trojan-Spy.Win32.Zbot	742,794
2	Trojan-Banker.Win32.ChePro	192,229
3	Trojan-Banker.Win32.Lohmys	121,439
4	Trojan-Banker.Win32.Shiotob	95,236
5	Trojan-Banker.Win32.Agent	83,243
6	Trojan-Banker.AndroidOS.Faketoken	50,334
7	Trojan-Banker.Win32.Banker	41,665
8	Trojan-Banker.Win32.Banbra	40,836
9	Trojan-Spy.Win32.SpyEyes	36,065
10	Trojan-Banker.HTML.Agent	19,770

最も広く拡散しているバンキング型マルウェアは、依然としてZeus（Trojan-Spy.Win32.Zbot）でした。四半期ごとのランキングでもトップを維持していたため、年間の上位10種でトップになったことも当然と言えます。2位がTrojan-Banker.Win32.ChePro で、Trojan-Banker.Win32.Lohmysがそれに続いています。いずれのファミリーにも同じ機能があり、オンラインバンキングに関連する内容（オンラインバンキングサービスからの請求書を装うなど）のスパムメッセージによって拡散します。このときのメールには画像を含むWord文書が添付され、その画像をクリックすると悪意あるコードが実行されます。

Trojan-Banker.Win32.Shiotobは4位でした。この悪質プログラムは、スパムメッセージによって拡散することが最も多く、支払いデータの傍受を目的としてトラフィックを監視します。

上位10種のマルウェアの大半は、ブラウザーで表示されるWebページにランダムなHTMLコードを埋め込み、元のWebフォームや埋め込まれたWebフォームにユーザーが入力した支払いデータを傍受します。

ユーザーの金銭を狙った攻撃の4分の3はバンキング型マルウェアを利用して実行されましたが、金融関連の脅威はこれだけではありません。



ユーザーの金銭を狙う攻撃のマルウェアタイプ別の分布（2014年）

Bitcoinウォレットの盗取は、2番目に多用される金融関連の脅威です（14%）。暗号通貨に関連する脅威としては、コンピューティングリソースを利用してBitcoinを生成するBitcoinマイニングソフトウェア（10%）もあります。

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

2014年、Kaspersky Labのウェブアンチウイルスは、**123,054,503**種類の悪質オブジェクト（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。

Kaspersky Labは、2014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頻繁に利用された20種の悪質プログラムを特定しました。この20種がオンライン攻撃すべての**95.8%**を占めています。

	検知名 *	攻撃を受けたユーザーの割合**
1	Malicious URL	73.70%
2	Trojan.Script.Generic	9.10%
3	AdWare.Script.Generic	4.75%
4	Trojan.Script.Iframer	2.12%
5	Trojan-Downloader.Script.Generic	2.10%

	検知名 *	攻撃を受けたユーザーの割合**
6	AdWare.Win32.BetterSurf.b	0.60%
7	AdWare.Win32.Agent.fflm	0.41%
8	AdWare.Win32.Agent.aiyc	0.38%
9	AdWare.Win32.Agent.allm	0.34%
10	Adware.Win32.Amonetize.heur	0.32%
11	Trojan.Win32.Generic	0.27%
12	AdWare.Win32.MegaSearch.am	0.26%
13	Trojan.Win32.AntiFW.b	0.24%
14	AdWare.JS.Agent.an	0.23%
15	AdWare.Win32.Agent.ahbx	0.19%
16	AdWare.Win32.Yotoon.heur	0.19%
17	AdWare.JS.Agent.ao	0.18%
18	Trojan-Downloader.Win32.Generic	0.16%
19	Trojan-Clicker.JS.Agent.im	0.14%
20	AdWare.Win32.OutBrowse.g	0.11%

** これらの数字はウェブアンチウイルスによる検知の判定を示しています。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ました。*

*** ユーザーのコンピューター上で記録された全Web攻撃に対する割合。*

例年どおり、上位20種の大半はドライブバイ攻撃で利用されるオブジェクトと、アドウェアで占められました。全判定の**73.7%**で、これらのブラックリストからのリンクが特定されています。

2014年の特徴として、上位20種に入ったアドウェアが前年の5種から12種に増加し、オンラインで検知された全悪質オブジェクトの**8.2%**を占めました（7.01ポイントの上昇）。アドウェアの量が増え、その拡散が活発化し、アンチウイルスによる検知への対抗が強化されたことが、2014年のトレンドとなりました。

Trojan-Clicker.JS.Agent.imの判定も、広告とあらゆる種類の「不審な」活動に関連しています。Amazon Cloudfrontにスクリプトを置いて広告コンテンツのあるページにユーザーをリダイレクトする手口も、このようにして検知されています。このスクリプトへのリンクはアドウェアや各種ブラウザー拡張機能によって、主にユーザーの検索ページに挿入されます。スクリプトによって、Adobe FlashやJavaの更新を推奨する偽のページにユーザーがリダイレクトされることもあります。これはマルウェアを拡散するための典型的な手法です。

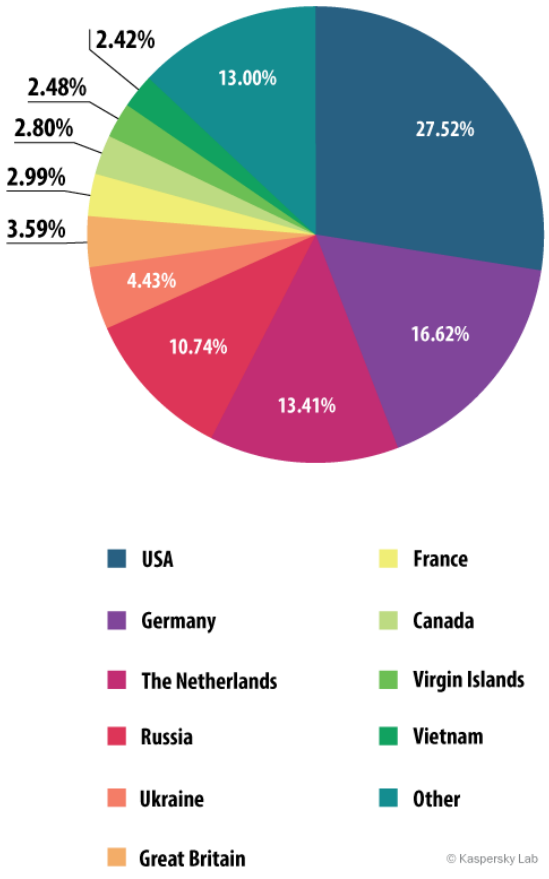
オンラインリソースにマルウェアが仕掛けられた国の上位10か国

次に示す数字は、攻撃に利用され、Kaspersky Labの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ページ、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）の物理的な所在地に基づいています。どんなホストであっても、1つ以上のWeb攻撃の発信源になり得ます。

Webベース攻撃の地理的な発信源を特定するためには、ドメイン名をその実ドメインIPアドレスと照合します。これにより、特定のIPアドレスの地理的な所在地（GEOIP）が特定されます。

2014年、カスペルスキー製品は世界各国のWebリソースから実行された**1,432,660,467**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に、犯罪者は**9,766,119**台のホストを使用しました。この数は2013年から**8%**、実数にして**838,154**台の減少です。

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**87%**は、10か国のオンラインリソースから受信されました。これは前年比で5ポイント上昇しています。



悪意あるプログラムが仕掛けられたオンラインリソースの分布（2014年）

2014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10か国は、おおむね前年の構成と変わりませんでした。ただし、4か国の順位が入れ替わっています。ドイツとロシアの順位が入れ替わり、ドイツが2位に浮上してロシアが4位に下がりました。ウクライナは英国を追い抜き5位に上がりました。

全Web攻撃のうち**44%**が、米国とドイツのリソースから実行されています。

ユーザーのオンライン感染のリスクが高い国

ユーザーが頻繁にサイバー脅威にさらされている国を調べるため、各国のカスペルスキー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計算しました。その結果データには世界各国でコンピューターがさらされている感染のリスクが表れており、各国のコンピューターが置かれた環境の深刻さの度合いが分かります。

ユーザーがオンライン感染するリスクが高い国の上位20か国

	国*	ユニークユーザーの割合**
1	ロシア	53.81%
2	カザフスタン	53.04%
3	アゼルバイジャン	49.64%
4	ベトナム	49.13%
5	アルメニア	48.66%
6	ウクライナ	46.70%
7	モンゴル	45.18%
8	ベラルーシ	43.81%
9	モルドバ	42.41%
10	キルギス	40.06%
11	ドイツ	39.56%
12	アルジェリア	39.05%
13	カタール	38.77%
14	タジキスタン	38.49%
15	グルジア	37.67%
16	サウジアラビア	36.01%
17	オーストリア	35.58%
18	リトアニア	35.44%

	国*	ユニークユーザーの割合**
19	スリランカ	35.42%
20	トルコ	35.40%

これらの統計は、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います。これは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提供されたものです。

** 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攻撃の標的となっ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*

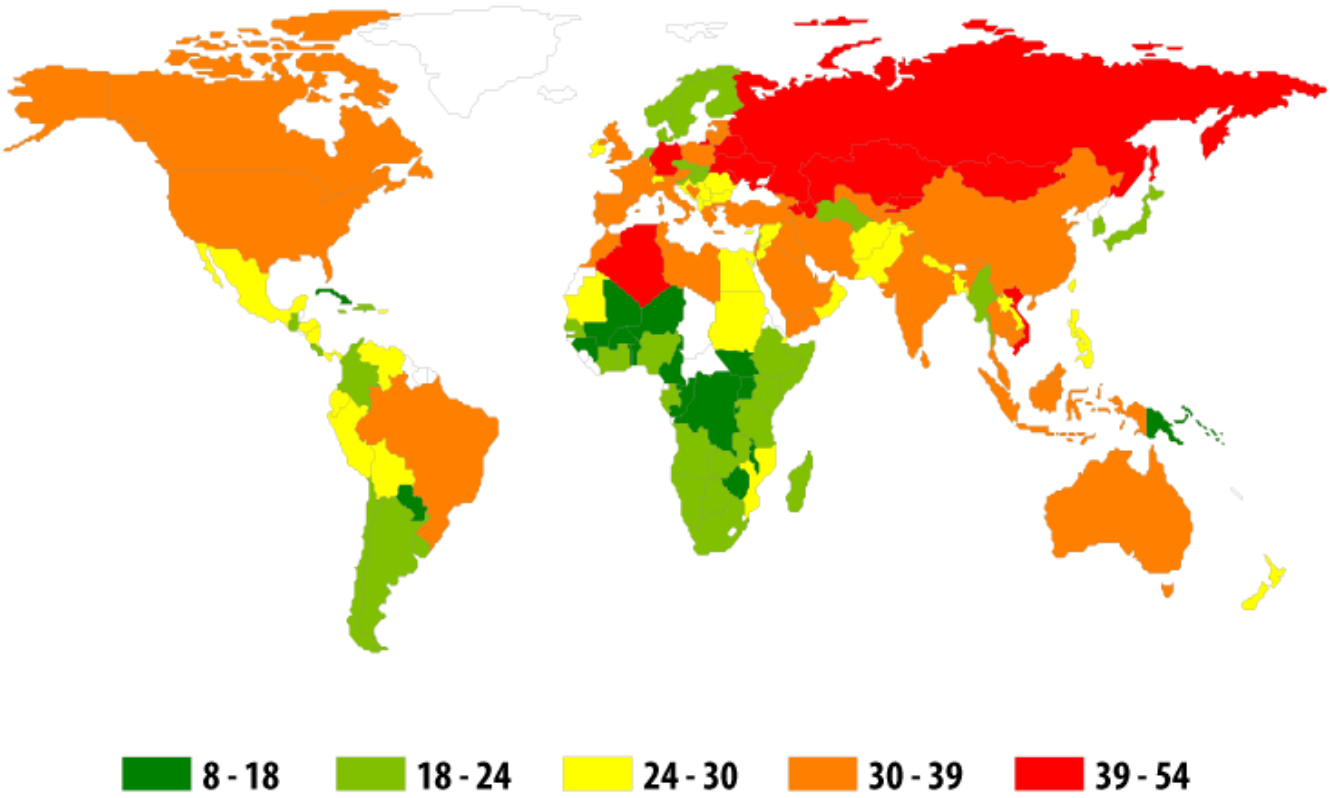
2014年は上位20か国の中で首位が入れ替わり、ロシアがトップに立ちました。同国では**53.81%**のユーザーがオンライン感染のリスクに直面しています。

昨年のトップだったアゼルバイジャンは、3位に後退しました(49.64%)。

ウズベキスタン、マレーシア、ギリシャ、イタリアは上位20か国から外れ、新たにモンゴル、カタール、サウジアラビア、トルコ、リトアニアが加わっています。

感染リスクのレベルで見ると、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(41%超)2014年には、上位20か国のうち9か国がこのグループに分類されています(2013年は**15**か国)。
2. 中程度のリスクのグループ(21～40%)このグループには**111**か国が該当します。キルギス(40.1%)、ドイツ(39.6%)、カタール(38.8%)、タジキスタン(38.5%)、グルジア(37.7%)、サウジアラビア(36%)、トルコ(35. 4%)、フランス(34.9%)、インド(34.8%)、スペイン(34.4%)、米国(33.8%)、カナダ(33.4%)、オーストラリア(32.5%)、ブラジル(32.1%)、ポーランド(31.7%)、イタリア(31.5%)、イスラエル(30.2%)、中国(30.1%)、英国(30%)、エジプト(27.8%)、メキシコ(27.5%)、フィリピン(27.2%)、クロアチア(26.2%)、パキスタン(26.1%)、ルーマニア(25.7%)、日本(21. 2%)、アルゼンチン(21. 1%)など。
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は**39**か国でした。スウェーデン(19.5%)、デンマーク(19.2%)、ウルグアイ(19.5%)、多数のアフリカ諸国が該当します。



2014年には、ユーザーがオンラインの状態で**38.3%**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年間で3.3%下がっています。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たことが挙げられます。

— 第2の原因は、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ったことです。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そうともしません。

— 第3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利用するユーザーが増えていることが挙げられます。

さらに、エクスプロイトパックを利用した攻撃もわずかながら減少しています。エクスプロイト開発者が逮捕されたことも無駄ではなかったようですが、エクスプロイトの状況が劇的に変わったと判断できる根拠はありません。標的型攻撃をはじめ、エクスプロイトは今もマルウェア配信の主な手段です。インターネットは今でもほとんどの国で、最大のマルウェア感染源となっています。

ローカルの脅威

ユーザーのコンピューターのローカル感染に関する統計は、非常に重要な指標です。このデータから、インターネット、メール、ネットワークポート以外の経路でWindowsオペレーティングシステムに侵入した脅威がわかります。

このセクションでは、ハードディスク上のファイルのアンチウイルススキャン（ファイルの作成時やアクセス時に実行）と、各種リムーバブルディスクのスキャン結果から取得された統計データの分析を紹介します。

ユーザーのコンピューターで検知された悪意あるオブジェクトの上位20種

2014年、Kaspersky Labのアンチウイルス製品は、**1,849,949**種類の悪質オブジェクトと不審なオブジェクトを検知しました。

	検知名	攻撃を受けたユーザーの割合*
1	DangerousObject.Multi.Generic	26.04%
2	Trojan.Win32.Generic	25.32%
3	AdWare.Win32.Agent.ahbx	12.78%
4	Trojan.Win32.AutoRun.gen	8.24%
5	Adware.Win32.Amonetize.heur	7.25%
6	Virus.Win32.Sality.gen	6.69%
7	Worm.VBS.Dinihou.r	5.77%
8	AdWare.MSIL.Kranet.heur	5.46%
9	AdWare.Win32.Yotoon.heur	4.67%
10	Worm.Win32.Debris.a	4.05%
11	AdWare.Win32.BetterSurf.b	3.97%
12	Trojan.Win32.Starter.lgb	3.69%
13	Exploit.Java.Generic	3.66%
14	Trojan.Script.Generic	3.52%
15	Virus.Win32.Nimnul.a	2.80%
16	Trojan-Dropper.Win32.Agent.jkcd	2.78%
17	Worm.Script.Generic	2.61%
18	AdWare.Win32.Agent.aljt	2.53%

	検知名	攻撃を受けたユーザーの割合*
19	AdWare.Win32.Kranet.heur	2.52%
20	Trojan.WinLNK.Runner.ea	2.49%

これらの統計は、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。

** アンチウイルスでこれらのオブジェクトが検知されたユーザーの数を、コンピューター上で悪質プログラムが検知されたカスペルスキー製品ユーザーの数で割った値*

DangerousObject.Multi.Genericの判定は、クラウド技術によって検知されるマルウェアに使用されるもので、これが1位となりました（26.04%）。クラウド技術が使用されるのは、悪質プログラムを検知する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まだ登録されていないものの、そのオブジェクトに関する情報が当社のクラウドアンチウイルスデータベースには登録されている場合です。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。

有名なワームNet-Worm.Win32.Kidoは上位20種から姿を消しました。一般的に、ウイルスの占める割合は減少を続けています。たとえば、2013年にVirus.Win32.Sality.genの影響を受けたユーザーは**13.4%**でしたが、2014年はわずか**6.69%**でした。

このランキングでもWeb検知のランキングでも、アドウェアが以前より増える傾向にあります。2014年、アドウェアに遭遇したユーザーの数は前年比で2倍になり、**25,406,107**人に達しました。それと同時に、アドウェアは迷惑度も危険性も高まっています。一部のアドウェアは「基準を越えて」不審なプログラムに分類され、「より深刻な」判定を受けています。たとえばTrojan-Dropper.Win32.Agent.jkcd（16位）は、広告を表示して検索結果を変更するだけでなく、コンピューターにマルウェアをダウンロードする機能も備えています。

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の数を国別に調べました。このデータには、ユーザーのコンピューター上と、コンピューターに接続されたリムーバブルメディア（フラッシュドライブ、カメラや携帯電話のメモリカード）上での悪質プログラムの検知が含まれています。

感染リスクの高い上位20か国

	国*	割合**
1	ベトナム	69.58%
2	モンゴル	64.24%

	国*	割合**
3	ネパール	61.03%
4	バングラデシュ	60.54%
5	イエメン	59.51%
6	アルジェリア	58.84%
7	イラク	57.62%
8	ラオス	56.32%
9	インド	56.05%
10	カンボジア	55.98%
11	アフガニスタン	55.69%
12	エジプト	54.54%
13	サウジアラビア	54.37%
14	カザフスタン	54.27%
15	パキスタン	54.00%
16	シリア	53.91%
17	スーダン	53.88%
18	スリランカ	53.77%
19	ミャンマー	53.34%
20	トルコ	52.94%

これらの統計は、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います。統計データはカスペルスキー製品ユーザーの同意を得て収集されたものです。

** 計算時にカスペルスキー製品ユーザーが10,000人未満の国は除外*

*** コンピューターでローカルの脅威がブロックされた各国のユニークユーザー数を、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*

ローカル感染のリスクが高い上位4か国は前年とほぼ変わらず、ベトナムが1位でした。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2位から4位に下がり、モンゴルが4位から2位に上がりました。

ジブチ、モルディブ、モーリタニア、インドネシア、ルワンダ、アンゴラは上位20か国から外れ、新たにイエメン、サウジアラビア、カザフスタン、シリア、ミャンマー、トルコが加わりました。

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**58.7%**で、悪意あるオブジェクトが少なくとも1つ見つかっています。2013年の数字は**60.1%**でした。

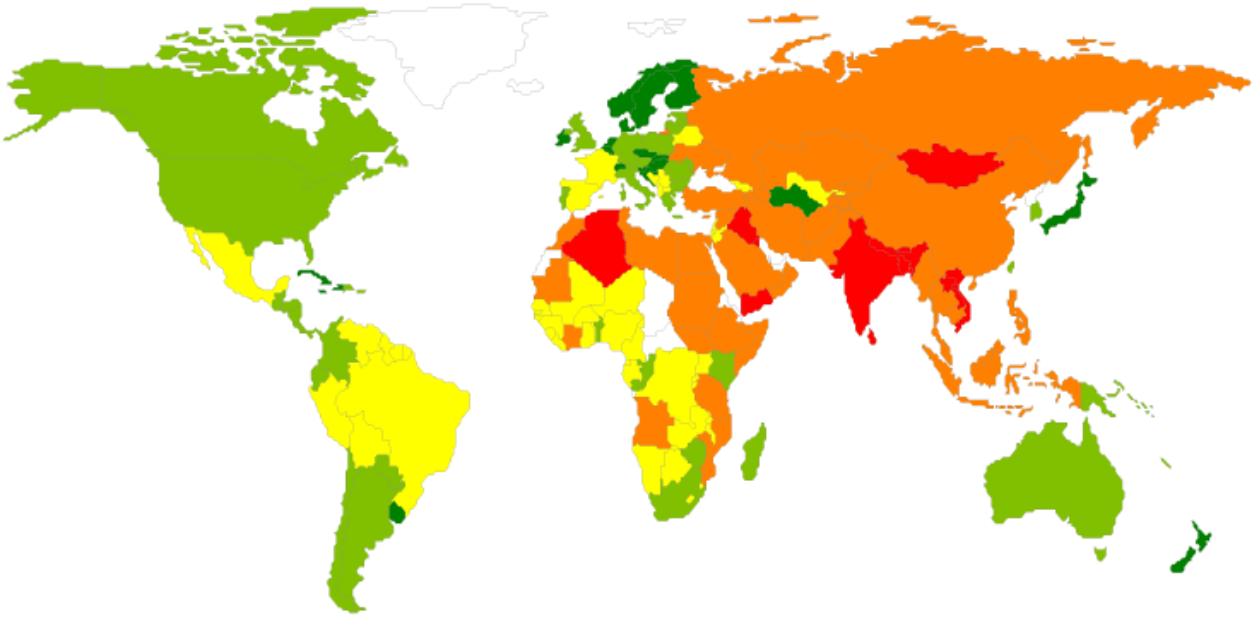
ローカルの脅威については、各国を4つのリスクカテゴリに分類できます。

1. リスク最大（60%超）：ベトナム（69.6%）、モンゴル（64.2%）、ネパール（61.0%）、バングラデシュ（60.5%）の4か国。

2.リスク高(41～60%):インド(56.0%)、カザフスタン(54.3%)、トルコ(52.9%)、ロシア(52.0%)、中国(49.7%)、ブラジル(46.5%)、ベラルーシ(45.3%)、メキシコ(41.6%)、フィリピン(48.4%)など83か国。

3.ローカル感染リスク中(21～40.99%):スペイン(40.9%)、フランス(40.3%)、ポーランド(39.5%)、リトアニア(39.1%)、ギリシャ(37.8%)、ポルトガル(37.7%)、韓国(37.4%)、アルゼンチン(37.2%)、イタリア(36.6%)、オーストリア(36.5%)、オーストラリア(35.3%)、カナダ(34.8%)、ルーマニア(34. 5%)、米国(34.4%)、英国(33.8%)、スイス(30.8%)、香港(30.4%)、アイルランド(29.7%)、ウルグアイ(27.8%)、オランダ(26.4%)、ノルウェー(25.1%)、シンガポール(23.5%)、日本(22.9%)、スウェーデン(23%)、デンマーク(21.3%)など70の国と地域。

4.ローカル感染リスク低(0～20.99%):フィンランド(20%)、キューバ(19.1%)、セーシェル(19%)の3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	セーシェル	19.03%
2	キューバ	19.08%
3	フィンランド	20.03%
4	デンマーク	21.34%

	国	割合*
5	日本	22.89%
6	スウェーデン	22.98%
7	チェコ	23.13%
8	シンガポール	23.54%
9	マルティニーク	25.04%
10	ノルウェー	25.13%

** コンピューターでローカルの脅威がブロックされた各国のユニークユーザー数を、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*

2014年は上位10か国にマルティニーク、シンガポール、スウェーデンが新たに加わりました。スロバキア、スロベニア、マルタがランキングから外れています。

平均するとユーザーのコンピューターの**23%**が、1年間に少なくとも1回の攻撃を受けました。前年から4.2ポイントの上昇です。

Securelist, Kaspersky Lab
エキスパートのテクニカルリサーチ、分析を主としたブログ

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

株式会社カスペルスキー

PR-1006-201501