IT THREAT EVOLUTION IN Q3 2016

― 2016 年第 3 四半期 Kaspersky サイバー脅威レポート

David Emm, Roman Unuckek, Maria Garnaeva, Anton Ivanov, Denis Makrushin, Fedor Sinitsyn

＊本資料は、英語版「IT THREAT EVOLUTION IN Q3 2016」の一部を抜粋した抄訳版です。

目次

統計

本レポート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情報を世界規模で共有しています。

第 3 四半期の数字

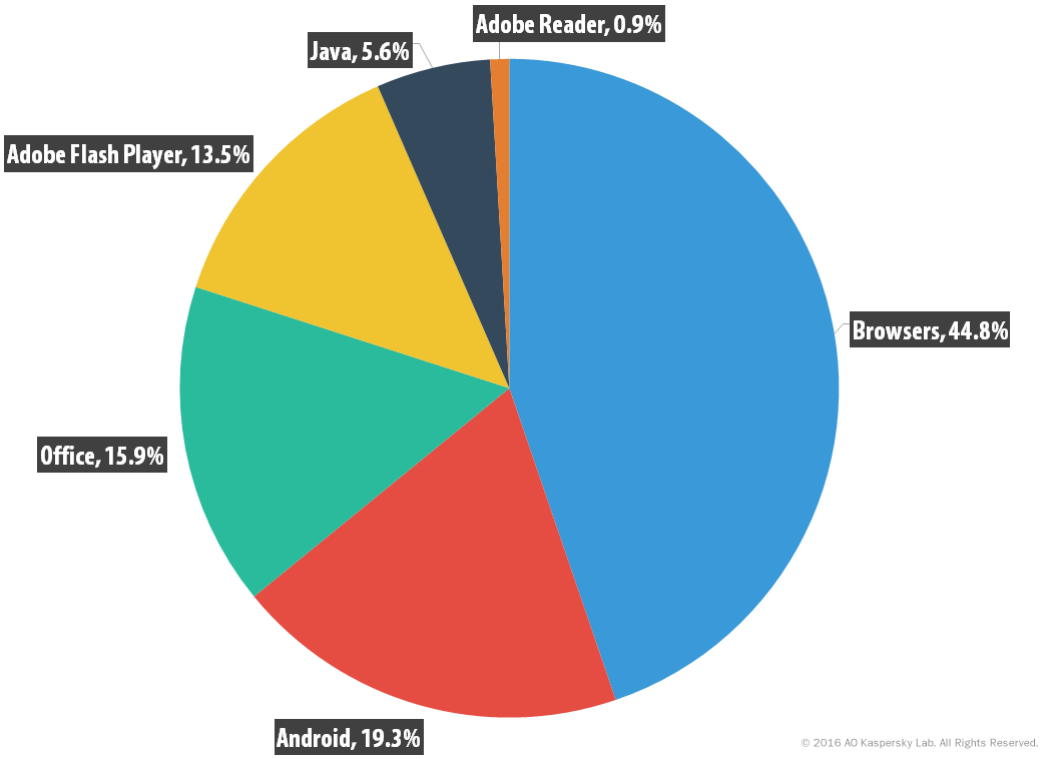
- カスペルスキー製品は世界 190 か国のオンラインリソースから **171,802,109** 件の悪意ある攻撃を検知し、ブロックしました。
- Web アンチウイルスは、**45,169,524** の URL（重複を除く）を悪意ある URL と判定しました。
- Web アンチウイルスは、**12,657,673**（重複を除く）の悪意あるオブジェクト（スクリプト、エクスプロイト、実行ファイルなど）を検知しました。
- 暗号化型ランサムウェアによる攻撃を受けたユーザーは、**821,865 人**（重複を除く）でした。
- 金融系マルウェアの攻撃を受けたユーザーは、**1,198,264** 人でした。
- ファイルアンチウイルスは、合計 **116,469,744**（重複を除く）の悪意あるオブジェクトと不要と思われるオブジェクトを検知しました。
- モバイルセキュリティ製品で、以下を検知しました。
  - **1,520,931** の悪意あるインストールパッケージ
  - **30,167** のモバイルバンキング型トロイの木馬（インストールパッケージ）
  - **37,150** のモバイル向けランサムウェア型トロイの木馬（インストールパッケージ）

サイバー犯罪者に悪用される脆弱なアプリケーション

2016 年第 2 四半期にサイバー犯罪者市場から姿を消した Angler と Nuclear に続き、第 3 四半期には Neutrino エクスプロイトキットが消えました。

RIG と Magnitude は依然として活動を続けています。特に RIG の活動は顕著で、エクスプロイトキット市場に空いた隙間を瞬く間に埋めました。

下のグラフは、第 3 四半期におけるエクスプロイトの利用の全体像を示しています。



サイバー攻撃に使用されたアプリケーション種類別の分布
（2016 年第 3 四半期）

このグラフからわかるように、第 3 四半期に最も攻撃されたソフトウェアは、各種ブラウザーとそのコンポーネントに対するエクスプロイト（45%）でしたが、全体に占める割合は 3 ポイント低下しました。2 番目は Android OS の脆弱性を悪用するエクスプロイト（19%）で、こちらの割合も第 3 四半期には 5 ポイント低下しています。3 番目は Microsoft Office 向けのエクスプロイトキットです。その割合は、第 2 四半期の 14%から今期は 16%に増加しました。

Adobe Flash Player は、引き続き広い範囲で不正利用されました。実際に、その割合は 6%から 13%へと倍以上に増加しています。その原因は、前述の RIG エクスプロイトキットです。これが複数の攻撃で使用されていたため、SWF エクスプロイトの割合が劇的に増加しました。

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、不正な Web サイトや感染サイトの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。不正な Web サイトとは、悪意あるユーザーが意図的に作成したサイトを指します。感染サイトには、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、侵害された正規のサイトが含まれます。

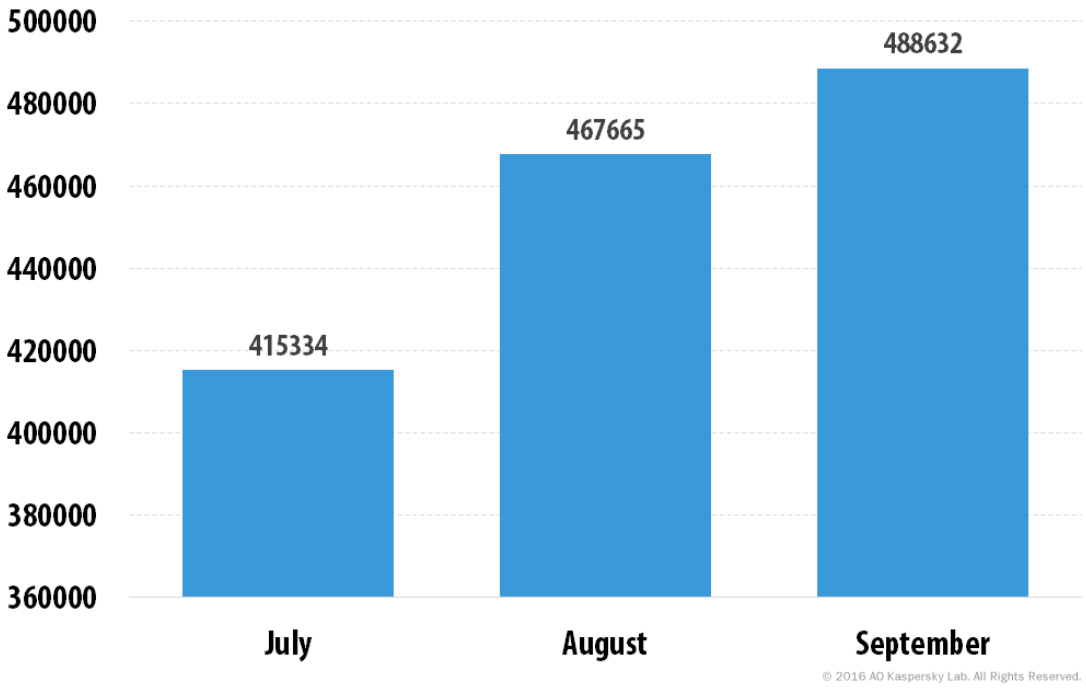
2016 年第 3 四半期に Web アンチウイルスが検知した悪意あるオブジェクト（スクリプト、エクスプロイト、実行ファイルなど）の数は、重複を除き **12,657,673** 個でした。また、Web アンチウイルスコンポーネントによって、重複を除く **45,169,524** の URL を悪意ある URL と判定しています。また、世界 190 か国のオンラインリソースからの悪意ある攻撃を **171,802,109** 件検知し、ブロックしました。

銀行業界におけるオンラインの脅威

これらの統計は、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のコンピューターから収集した検知判定結果に基づいています。

2016 年第 3 四半期、オンラインバンキングで金銭を窃取する金融系マルウェアの攻撃を受けたユーザーは、**1,198,264** 人で、第 2 四半期（**1,132,031** 人）から 5.8%増加しました。

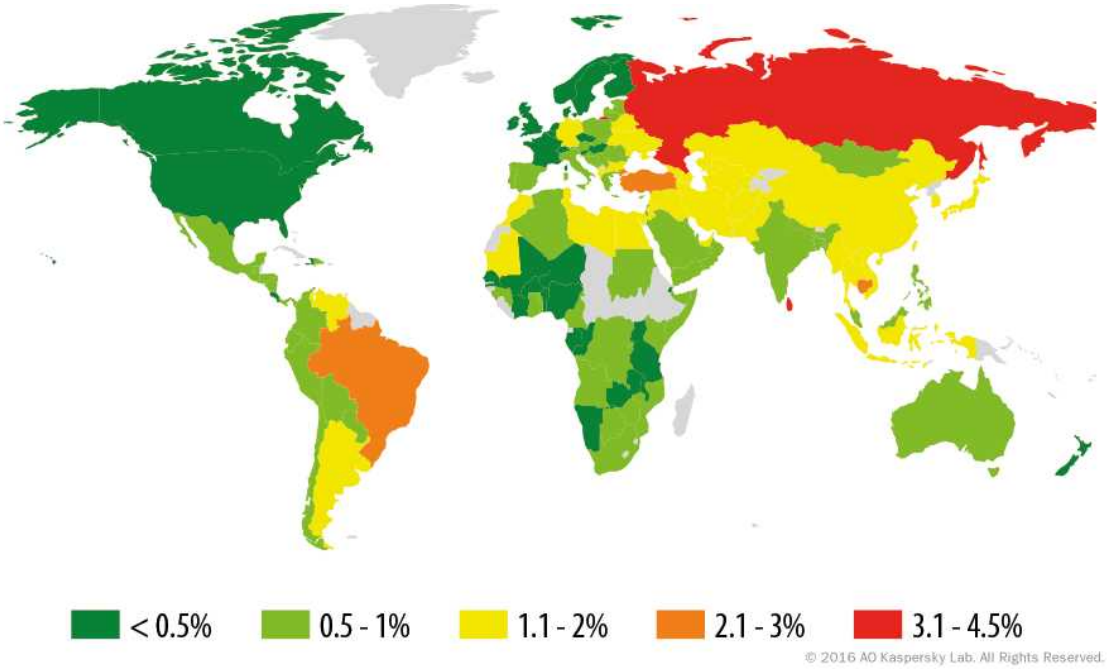
7 月～9 月は、欧州では一般的に休暇のシーズンです。つまり、第 3 四半期はオンラインバンキングユーザーによるオンライン決済の数が増加することになり、必然的に金融上のリスクも高まります。以下のグラフの通り、第 3 四半期は、金融系の脅威が月を追うごとに活発になりました。



金融系マルウェアの攻撃を受けた月毎のユニークユーザー数（2016 年第 3 四半期）

地理別の攻撃の状況

カスペルスキー製品ユーザーのうち、第 3 四半期にバンキング型トロイの木馬に遭遇したユーザーの割合を算出し、世界規模での感染リスクを比較検証しました。



2016 年第 3 四半期におけるバンキング型マルウェアの攻撃の地理的分布
（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*	攻撃を受けたユーザーの割合（%）**
1	ロシア	4.20
2	スリランカ	3.48
3	ブラジル	2.86
4	トルコ	2.77
5	カンボジア	2.59
6	ウクライナ	1.90
7	ベネズエラ	1.90
8	ベトナム	1.86
9	アルゼンチン	1.86
10	ウズベキスタン	1.77

これらの統計は、*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*から収集された、*アンチウイルスモジュール*の検知判定結果に基づいています。

* カスペルスキー製品のユーザーが 10,000 人未満の国は除外しています。

** 各国のカスペルスキー製品の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の標的になったユニークユーザーの割合。

バンキング型トロイの木馬の攻撃を受けたユーザーの割合が最も高かった国はロシアでした。攻撃を受けたユーザーの数が世界で最も多い Trojan-Banker ZeuS（Zbot）ファミリーのマルウェアは、ロシアで特に活発な動きを見せていました。この理由は、ロシアのサイバー犯罪者がこのマルウェアの開発に裏で関与していると見られているためです。ロシアの犯罪者は自国のオンラインバンキングシステムの特徴やロシア人の思考傾向を熟知しており、マルウェア開発に取り入れています。ロシアでは、バンキング型トロイの木馬 Gozi が引き続き勢力を伸ばしています。Gozi の開発者がトロイの木馬 Nymaim の作成者と手を組んだ後、第 2 四半期に Gozi の活動が爆発的に増加しました。ロシアは、モバイルバンキング型トロイの木馬に攻撃されたユーザーの割合が大きい国でも、トップになっています。

観光地として人気のスリランカは、金融系マルウェアに攻撃を受けたユーザーが 3.48%で、初めてこのランキングに登場し 2 位にランクインしました。攻撃を受けたユーザーの中には、休暇でスリランカを訪れ、オンラインバンキングを利用して決済を行った外国人も含まれていると考えられます。スリランカで最も活発だったバンキング型マルウェアは、Fsysna バンキング型ファミリーのマルウェアです。このファミリーは以前、中南米の銀行の顧客を標的とした攻撃で注目されていました。

ブラジルは 2 四半期連続で上位 3 か国に入りました。第 2 四半期時点の予測では、この夏のオリンピック開催により、中南米、特にブラジルで金融の脅威が急増すると見ていました。しかし、ブラジルで金融系マルウェアの脅威に遭遇したユーザーは第 2 四半期が 2.63%だったのに対し、第 3 四半期は 2.86%と 0.23 ポイントの微増にとどまりました。一方で、アルゼンチンでは悪意ある攻撃が急増し、ランキングの 9 位に入りました。

上位 10 か国のほぼすべての国が、休暇シーズンの影響を受けています。ロシア、ウクライナ、ウズベキスタンの人々は、伝統的に 1 年のこの時期に休暇を取ります。その他の国（スリランカ、ブラジル、トルコ、カンボジアなど）は観光地として人気です。旅行者はオンラインバンキングをよく利用する傾向があるため、サイバー犯罪者やバンキング型マルウェアの恰好の標的となるのです。

バンキング型トロイの木馬の標的となったユーザーの割合は、イタリアで 0.60%、スペインで 0.61%でしたが、ドイツでは 1.21%、UAE では 1.14%でした。

バンキング型マルウェアファミリー上位 10 種

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において、2016 年第 3 四半期に多く利用されたマルウェアファミリー上位 10 種を示しています（攻撃を受けたユーザーの割合）。

	名称*	攻撃を受けたユーザーの割合（%）**
1	Trojan-Spy.Win32.Zbot	34.58
2	Trojan.Win32.Qhost/Trojan.BAT.Qhost	9.48
3	Trojan.Win32.Fsysna	9.467
4	Trojan-Banker.Win32.Gozi	8.98
5	Trojan.Win32.Nymaim	8.32
6	Trojan-Banker.Win32.Shiotob	5.29
7	Trojan-Banker.Win32.ChePro	3.77
8	Trojan-Banker.Win32.BestaFera	3.31

9	Trojan-Banker.Win32.Banbra	2.79
10	Trojan.Win32.Neurevt	1.79

* 統計データの提供に同意したユーザーのコンピューターから収集した、カスペルスキー製品の検知判定
** 金融マルウェアに攻撃されたすべてのユーザーのうち、コンピューターが該当のマルウェアの標的になったユニークユーザーの割合

Trojan-Spy.Win32.Zbot は、攻撃されたユーザーが 34.58%という圧倒的な数字で 1 番で、ランキングでは常に 1 位です。2012 年にソースコードが公開され、ユーザーの決済データを容易に窃取できるツールとして広く悪用されています。このマルウェアがランキングのトップに君臨し続けていることも不思議ではありません。サイバー犯罪者はこのファミリーを絶えず強化しており、ソースコードをベースとして、オリジナルとは多少異なる新たな亜種をコンパイルしています。

2 番目に多かったのは、Qhost トロイの木馬ファミリー（Trojan.Win32.Qhost および Trojan.BAT.Qhost）です。このファミリーのマルウェアの機能は比較的シンプルです。まず、Hosts ファイル（ノードのネットワークアドレスを送信するときに使用されるドメイン名のデータベースを含む特別なテキストファイル）の内容を改ざんします。特定のリソースがアクセスされると同時に、このトロイの木馬の悪意あるコンポーネントが感染ワークステーションにロードされ、決済情報の窃取に利用されます。このトロイの木馬は、Host ファイルに大量のレコードを追加して、ユーザーのブラウザーが著名なアンチウイルスベンダーの Web ベースのアプリやリソースに接続できないようにします。

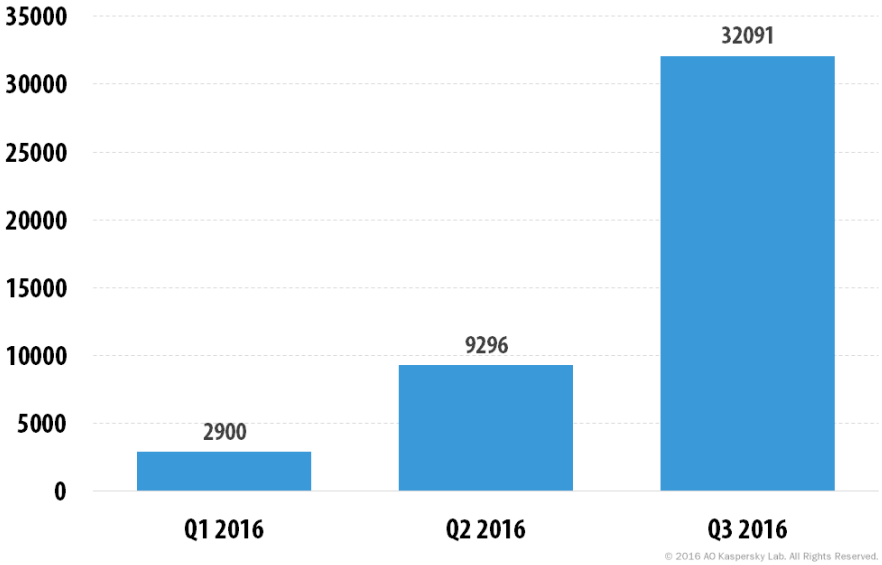
スリランカでその威力を既に実証した新しいマルウェア、Trojan.Win32.Fsysna ファミリーのバンキング型トロイの木馬もランキングに入っています。このファミリーのマルウェアは、感染したワークステーションから決済データを窃取するだけでなく、サイバー犯罪者によってスパムの拡散用にも使用されています。このトロイの木馬は感染したマシンを悪用して、コマンドセンターからメールサーバーへスパムメッセージをリダイレクトします。また、このファミリーの中には、ランサムウェア型トロイの木馬としての機能を持っているものもあります。Fsysna はある意味で、サイバー犯罪者が金銭窃取に使用する様々な機能を持った「スイスアーミーナイフ」のようなものと言えます。

金融向けの脅威として悪名高い Trojan-Spy.Win32.Lurk の活動は減少しました。このマルウェアの攻撃を受けたユーザー数は 7.1%減となっています。Lurk はバンキング型マルウェアファミリーの上位 10 種には入っていませんが、オンラインバンキングを利用するユーザーにとって引き続き脅威であることに変わりありません。Lurk の背後に潜むサイバー犯罪者グループが逮捕されたため、第 4 四半期は Lurk の活動はさらに縮小すると予想しています。

ランサムウェア型トロイの木馬

暗号化型マルウェア（ランサムウェア）は、ユーザーと企業にとって最大のサイバー脅威の 1 つです。ランサムウェアは、犯罪者が多額の利益を得られることから、サイバー犯罪者の世界中で利用が大幅に拡大しています。

第 3 四半期には、新たに 21 のファミリーと 32,091 の亜種を確認しました。ウイルスコレクションに追加された新しい暗号化型ランサムウェアファミリーの数は第 2 四半期（25）より若干少なかったものの、新たに作成された亜種の数は 3.5 倍に増加しています。



新たに作成された暗号化型ランサムウェアの亜種の数

（2016 年第 1 四半期～第 3 四半期）

マルウェア作成者は、絶えずマルウェアの機能強化を図っています。彼らはコンピューターへの新たな感染手段を常に模索していますが、特に企業への攻撃を重視しており、その理由は一般ユーザーへの攻撃よりもはるかに利益が大きいと考えられているためです。

サイバー犯罪者による暗号化型ランサムウェアのリモート起動

サイバー犯罪者がパスワードを解読して、組織などの標的システムに遠隔からアクセスし、侵入したマシンをランサムウェア型トロイの木馬に感染させる事件が増加しています。第 3 四半期の例としては、Dcryptor や Xpan がありました。

Dcryptor/Mamba

Trojan-Ransom.Win32.Dcryptor は、インターネットでは「Mamba」という別称で知られています。感染は手動で実行されます。サイバー犯罪者が総当たり攻撃でパスワードを割り出し、標的マシンにリモートアクセスし、Mamba を実行します。このとき、コマンドライン引数として、暗号化のパスワードを渡します。

感染時、Mamba は正規の DiskCryptor のユーティリティを使用します。これにより、ネットワークドライブにある個々のファイルだけでなく、ローカルマシンにあるハードドライブのセクター全体が感染し、システムブートはブロックされます。コンピューターを起動すると、画面に身代金を要求するメッセージと攻撃者との連絡用のメールアドレスが表示

されます。この Mamba を見て思い出すのは、悪名高い Petya/Mischa トロイの木馬です。サイバー犯罪者の間では、データへのアクセスをブロックする新たな方法を模索するというトレンドが、引き続き増大しています。

Xpan/TeamXRat ランサムウェア

Trojan-Ransom.Win32.Xpan も、攻撃者がリモートでシステムに侵入した後に起動されるランサムウェアの例です。このトロイの木馬は、ブラジルのサイバー犯罪者が拡散しています。犯罪者は総当たり攻撃で RDP パスワード（Windows コンピューターにリモートアクセスするための標準プロトコル）を割り出し、侵入したシステムを Xpan に感染させ、ファイルを暗号化して身代金要求メッセージを表示します。

スクリプト言語で記述されたランサムウェア

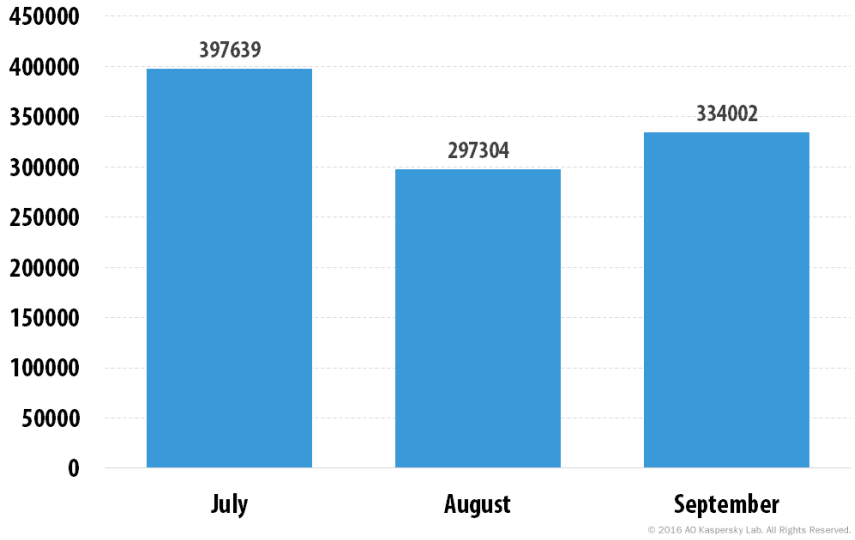
スクリプト言語で書かれた暗号化型ランサムウェアの数も増加傾向にあります。2016 年第 3 四半期には、Python で記述された次のような新しいファミリーを発見しています。

- HolyCrypt（Trojan-Ransom.Python.Holy）
- CryPy（Trojan-Ransom.Python.Kpyna）
- Trojan-Ransom.Python.Agent

また 6 月には、自動化言語 AutoIt で書かれた Stampado（Trojan-Ransom.Win32.Stampa）も登場しました。

ランサムウェアの攻撃を受けたユーザーの数

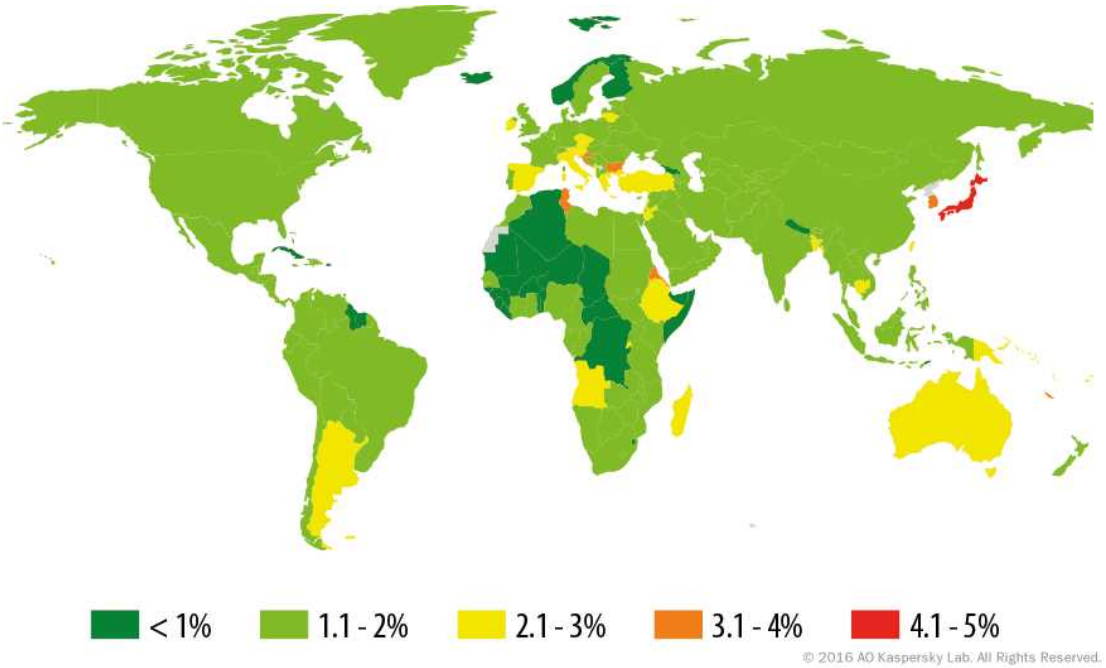
2016 年第 3 四半期は、821,865 人（重複を除く）のユーザーが暗号化型ランサムウェアの攻撃を受けました。これは前四半期の 2.6 倍です。そのうちの 23.9%が企業のユーザーです。



Trojan-Ransom 暗号化型ランサムウェアに攻撃を受けた月毎のユニークユーザー数

（2016 年第 3 四半期）

この攻撃に最も多く使われたのは、Trojan-Downloader.JS.Cryptoload ファミリーのマルウェアでした。これらのダウンローダーは、JavaScript で書かれており、システムにさまざまな暗号化型ランサムウェアファミリーのマルウェアをダウンロードし、インストールするように設計されています。



2016 年第 3 四半期における暗号化型ランサムウェアの攻撃の地理的分布
（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*	暗号化型ランサムウェアの攻撃を受けたユーザーの割合（%）**
1	日本	4.83
2	クロアチア	3.71
3	韓国	3.36
4	チュニジア	3.22
5	ブルガリア	3.20
6	香港	3.14
7	台湾	3.03
8	アルゼンチン	2.65
9	モルジブ	2.63
10	オーストラリア	2.56

* カスペルスキー製品のユーザーが 10,000 人未満の国は除外しています。
** 各国のカスペルスキー製品のユニークユーザーのうち、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

暗号化型ランサムウェアの攻撃を受けたユーザーの割合が高い国で、日本がランキングの 1 位となりました。第 2 四半期から 2 倍以上の 2.43 ポイント増加し 2 四半期連続でトップでした。
上位 10 か国には、新たにチュニジア、香港、アルゼンチン、オーストラリアが入り、イタリア、ジブチ、ルクセンブルク、オランダはランク外となっています。

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

	名称	判定*	攻撃を受けたユーザーの割合（%）**
1	CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	28.34
2	Locky	Trojan-Ransom.Win32.Locky	9.60
3	CryptXXX	Trojan-Ransom.Win32.CryptXXX	8.95
4	TeslaCrypt	Trojan-Ransom.Win32.Bitman	1.44
5	Shade	Trojan-Ransom.Win32.Shade	1.10
6	Cryakl	Trojan-Ransom.Win32.Cryakl	0.82
7	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0.73
8	Cerber	Trojan-Ransom.Win32.Zerber	0.59
9	CryptoWall	Trojan-Ransom.Win32.Cryptodef	0.58
10	Crysis	Trojan-Ransom.Win32.Crusis	0.51

*これらの統計は、統計データの提供に同意したユーザーのコンピューターから収集した検知判定結果に基づいています。
** Trojan-Ransom マルウェアに攻撃されたすべての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 Trojan-Ransom ファミリーの標的になったユニークユーザーの割合

第 3 四半期は、再び CTB-Locker がトップになりました。上位 3 位には、悪名高い Locky と CryptXXX も入っています。TeslaCrypt は、2016 年 5 月に所有者がサーバーを閉鎖し、ファイルの復号用マスターキーを公開したにもかかわらず、依然としてランク入りしています（ただし、第 3 四半期は割合が約 6 分の 1 に低下しました）。

Crysis

Crysis（判定：Trojan-Ransom.Win32.Crusis）は、第 3 四半期に初めてトップ 10 入りしました。このトロイの木馬が初めて検知されたのは 2016 年 2 月で、それ以来、数回コードの改変が行われました。

興味深いことに、Crysis を配布している犯罪者が身代金の要求に使用しているメールアドレスのリストは、Cryakl と Aura に関連するリストと部分的に一致しています。しかし、これらのファミリーの実行可能ファイルを解析したところ、同じコードを共有しているわけではないことがわかりました。おそらく、これらの悪意あるプログラムは 1 つのパートナースキームを経由して拡散されており、また、一部の配布者は同時に複数のトロイの木馬を配布しているため、標的への身代金要求に使用されるメールアドレスが同じになっているのだと考えられます。

Polyglot/MarsJoke

このトロイの木馬は 2016 年 8 月に登場しました（Kaspersky Lab は今年 10 月に、Polyglot/ MarsJoke に関する詳細な分析を発表しています）。トップ 10 にランクインしていないものの、作成者は 2 四半期連続でランキングのトップになっている有名な CTB-Locker を模倣を試みたとみられる興味深い特徴があります。このマルウェアの設計は、外部、内部とも「オリジナル」に非常によく似ていますが、作成したサイバー犯罪者がミスにより、身代金を支払わずにファイルを復号することができます。

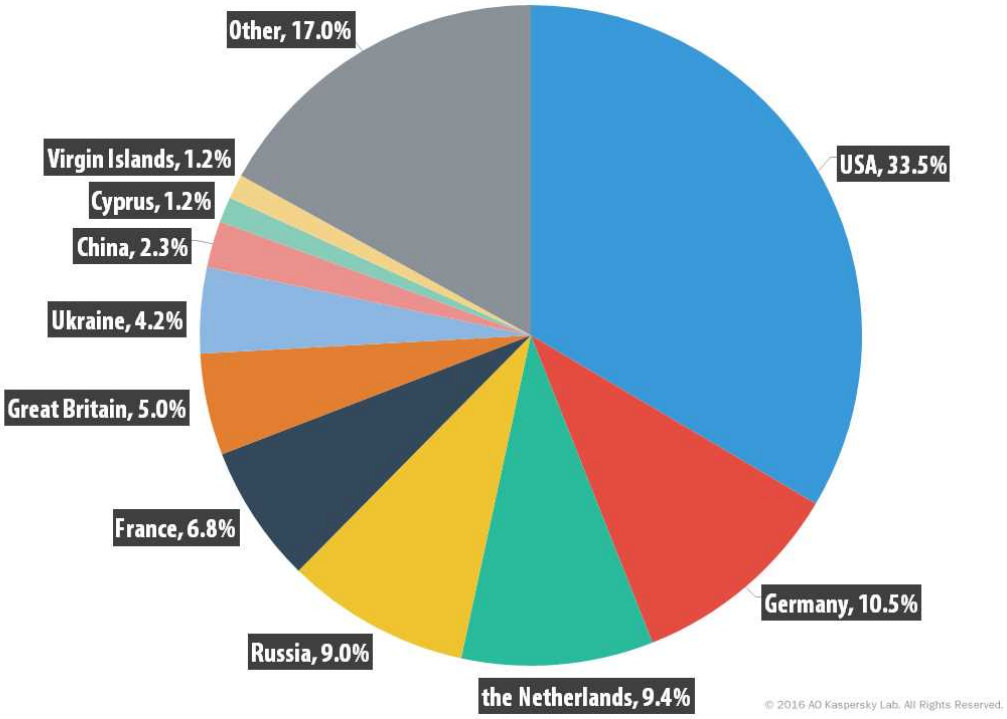
オンラインリソースに潜むマルウェアが多い上位 10 か国

次の統計は、Web 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）が物理的に存在する国に基づいています。どのようなホストであっても、1 つまたは複数の Web 攻撃の発信元となり得ます。

Web ベース攻撃の発生源を判断するために、ドメイン名を実際のドメインの IP アドレスと照合し、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。

カスペルスキー製品は 2016 年第 3 四半期、世界 190 か国のオンラインリソースからの悪意ある攻撃を **171,802,109** 件ブロックしました。**45,169,524** 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。

ブロックした Web 攻撃の 83%は、10 か国の Web リソースからの攻撃によるものでした。



Web 攻撃の発信源の国別分布（2016 年第 3 四半期）

第 3 四半期のランキングも前四半期と同様、米国（33.51%）がトップでした。ロシア（9%）は 2 位から 4 位に後退し、ドイツが 10.5%で 2 位に浮上しました。カナダが上位 10 か国から外れ、新たにキプロス（1.24%）が 9 位に入っています。

オンライン感染リスクが高い国

ユーザーがオンラインで感染するリスクを国別に評価するために、攻撃を受けたユーザーの割合を国別に計算しました。そのデータにより、さまざまな国でコンピューターが稼動している環境の攻撃性を把握できます。

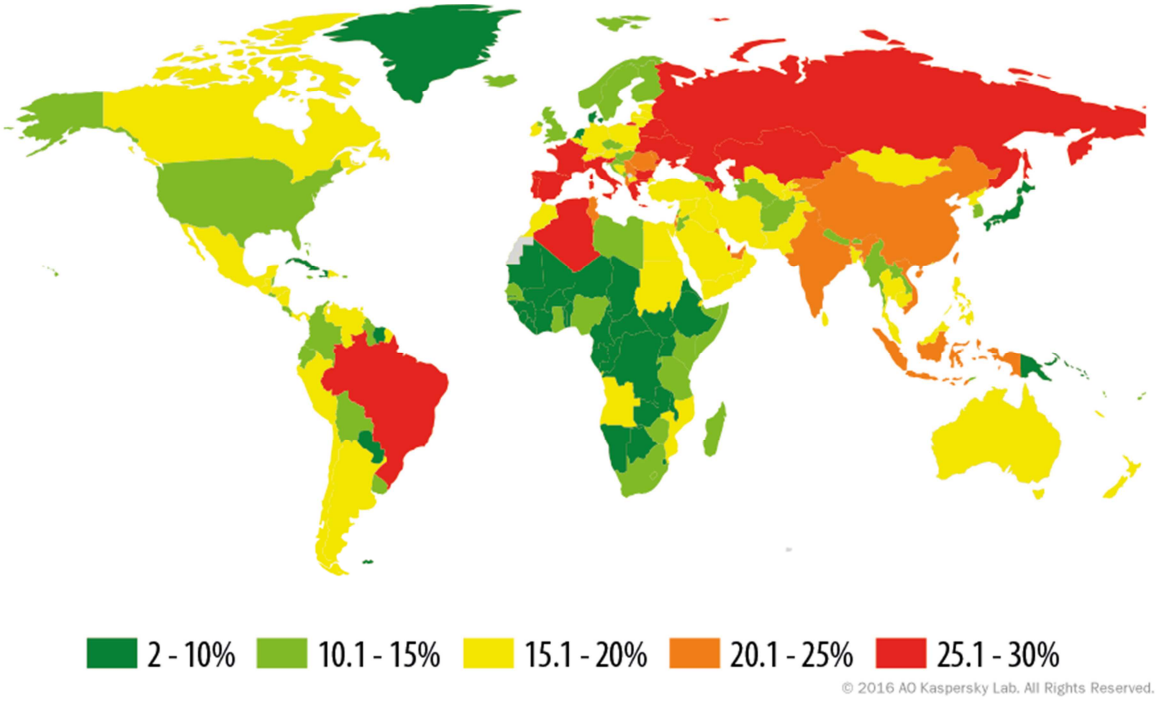
注：2016 年第 3 四半期より、このランキングには、マルウェアに分類される悪意あるプログラムの攻撃のみが含まれるようになりました。Web アンチウイルスコンポーネントによって検知された、潜在的に危険なプログラムや不要なプログラム（RiskTool やアドウェアなど）は含まれません。

	国*	攻撃を受けたユーザーの割合（%）**
1	スロベニア	30.02
2	ブルガリア	29.49
3	アルメニア	29.30
4	イタリア	29.21
5	ウクライナ	28.18
6	スペイン	28.15
7	ブラジル	27.83
8	ベラルーシ	27.06
9	アルジェリア	26.95
10	カタール	26.42
11	ギリシャ	26.10
12	ポルトガル	26.08
13	ロシア	25.87
14	フランス	25.44
15	カザフスタン	25.26
16	アゼルバイジャン	25.05
17	UAE	24.97
18	ベトナム	24.73
19	中国	24.19
20	アルバニア	23.23

これらの統計は、Web アンチウイルスコンポーネントによって返され、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収集された検知判定結果に基づいています。

* カスペルスキー製品のユーザーが 10,000 人未満の国は計算から除外されています。
** 各国のカスペルスキー製品のユニークユーザーのうち、**マルウェアクラス**の攻撃の標的になったユニークユーザーの割合。

平均すると、インターネットに接続された全世界のコンピューターの 20.2%が、マルウェアクラスの Web 攻撃を少なくとも 1 回受けています。



2016 年第 3 四半期の悪意ある Web 攻撃の地理的分布（攻撃を受けたユーザーの割合順）

オンライン環境が安全な国は、クロアチア（14.21%）、英国（14.19%）、シンガポール（13.78%）、米国（13.45%）、ノルウェイ（13.07%）、チェコ共和国（12.80%）、南アフリカ（11.98%）、スウェーデン（10.96%）、韓国（10.61%）、オランダ（9.95%）、日本（9.78%）です。

PR-1028-201611