# IT THREAT EVOLUTION IN Q2 2016

## ー 金融機関におけるオンラインの脅威、ランサムウェア型トロイの木馬

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

＊本資料は、英語版「IT THREAT EVOLUTION IN Q2 2016」の一部を抜粋した抄訳版です。

KASPERSKY lab

# 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る情報を世界規模で共有しています。

## 第2四半期の数字

- KSNのデータによると、カスペルスキー製品は世界191か国のオンラインリソースからの悪意ある攻撃を**171,895,830**件検知し、ブロックしました。
- **54,539,948**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。
- Kaspersky LabのWebアンチウイルスは、**16,119,489**（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。
- 暗号型ランサムウェアによる攻撃が、ユーザーのコンピューター**311,590台**（重複を除く）でブロックされました。
- 銀行口座へのオンラインアクセスによって金銭を窃取しようとするマルウェアの感染の試みが、**1,132,031** 台のユーザーコンピューターで検知されました。
- Kaspersky Labのファイルアンチウイルスは、合計**249,619,379**（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。
- Kaspersky Labのモバイルセキュリティ製品では、以下のものが検知されました。

  ・**3,626,458**の悪意あるインストールパッケージ

  ・**27,403** 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）

  ・**83,048** 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

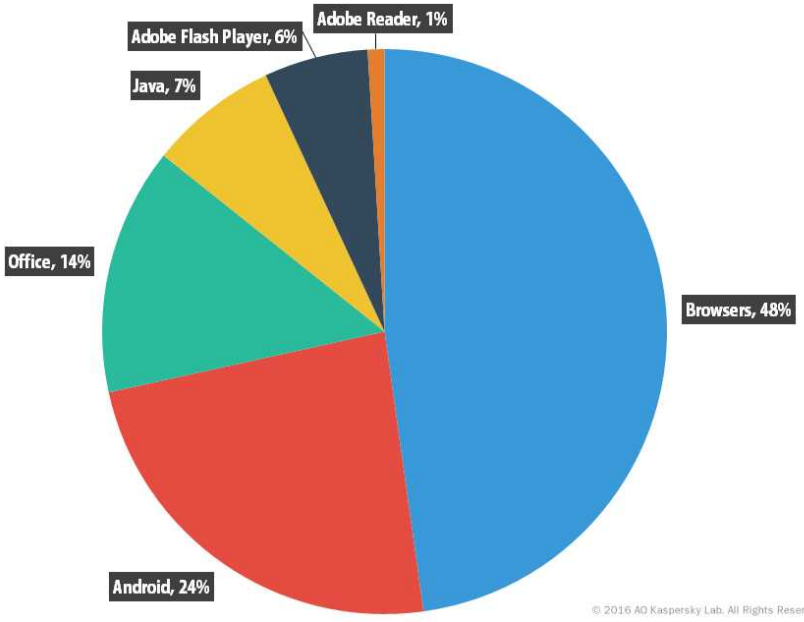
2016年第2四半期は、Adobe Flash Playerが引き続き広い範囲で不正利用されました。本レポートの対象期間中に、このソフトウェアで新たに2件の脆弱性が発見されています。

- CVE-2016-4117
- CVE-2016-4171

CVE-2016-4117のエクスプロイトは、エクスプロイトキットMagnitudeとNeutrinoに追加されました。CVE-2016-4171の脆弱性は、ScarCruftグループが標的型攻撃の実行に利用しています。同グループの活動の詳細については、弊社が6月中旬に公開したブログをご覧ください。

今期の重要な出来事は、長らく市場をリードしてきたエクスプロイトキットであるAnglerとNuclearが姿を消したことです。Anglerが消えたことで、マーケットプレイヤーは他のエクスプロイトキットに乗り換えてマルウェアを拡散するようになりました。特にNeutrinoエクスプロイトキットは大幅な利用拡大が観測されています。

下のグラフは、第2四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エクスプロイトのアプリケーション種類別の分布（2016年第2四半期）**

このグラフからわかるように、市場リーダーが退場したにもかかわらず、エクスプロイトの分布は第1四半期からほぼ変化していません。エクスプロイトの割合は、Microsoft Office（14%）とJava（7%）が1ポイント低下した一方で、Androidは2ポイント増の24%に達しました。これは、エクスプロイトキットの需要がRIG、Magnitude、Neutrinoという残りのプレイヤーへと流れたことを示唆しています。Neutrinoは、マルウェアダウンロードの試行回数という点で間違いなく今期のリーダーでした。

# 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、侵害された正規サイトが含まれます。**

2016年第2四半期にKaspersky Labの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**16,119,489**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**54,539,948**のURLが悪意あるURLと判定されています。

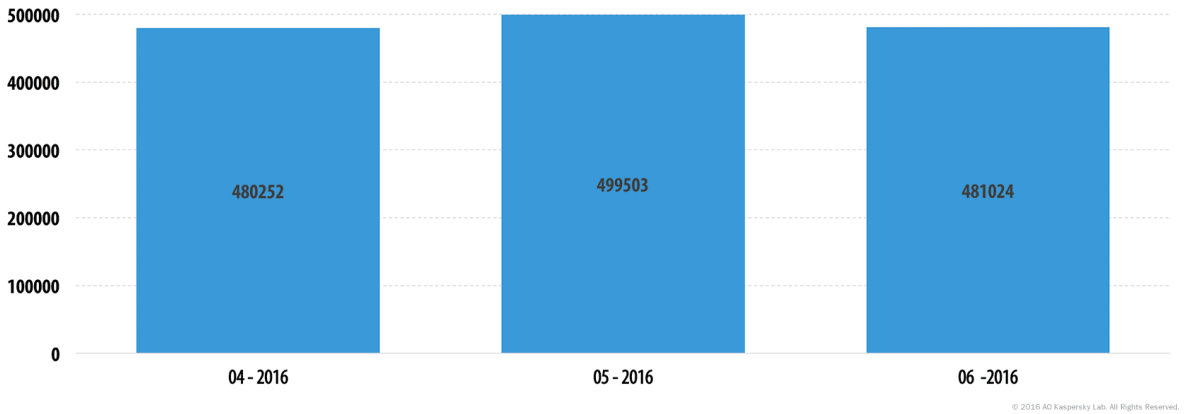
## 銀行業界におけるオンラインの脅威

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。

### 金融を標的としたマルウェアの攻撃を受けたユーザーの数

**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、2016年第2四半期は、金融のリスクとして分類される判定のリストを大幅に更新することになりました。つまり、金融系マルウェアの標的の数が、前四半期に公開されたデータから大きく変化したということです。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、第1四半期の統計を再計算しました。**

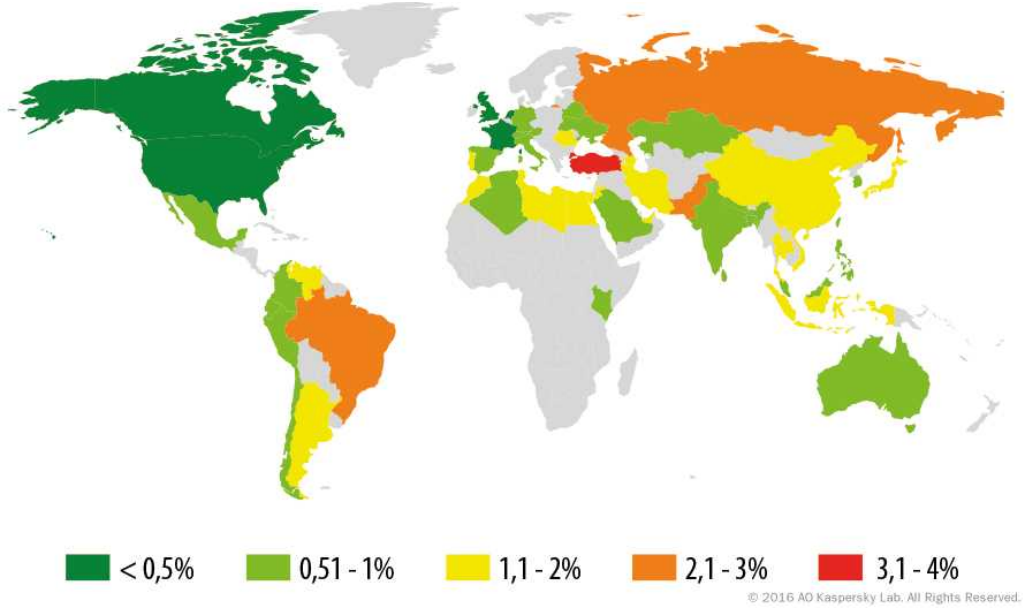
カスペルスキー製品は2016年第2四半期、オンラインバンキングで金銭を窃取するマルウェアの起動の試みを、**1,132,031**台のコンピューターでブロックしました。今期は金融系マルウェアの活動が増加しており、第2四半期は第1四半期（979,607件）から15.6%増となっています。




**金銭を狙うマルウェアの攻撃を受けたユーザー数（2016年第2四半期）**

## 地理別の攻撃の状況

バンキング型トロイの木馬に感染するリスクを世界規模で比較検証するため、各国のすべてのカスペルスキー製品ユーザーのうち、その国で今回のレポート期間中にバンキング型トロイの木馬に遭遇した弊社製品ユーザーの割合を算出しました。




**2016年第2四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* | 攻撃されたユーザーの割合（%）** |
|---|---|---|
| 1 | トルコ | 3.45 |
| 2 | ロシア | 2.92 |
| 3 | ブラジル | 2.63 |
| 4 | パキスタン | 2.60 |
| 5 | ベネズエラ | 1.66 |
| 6 | チュニジア | 1.62 |
| 7 | 日本 | 1.61 |
| 8 | シンガポール | 1.58 |

| | | |
|---|---|---|
| 9 | リビア | 1.57 |
| 10 | アルゼンチン | 1.48 |

これらの統計は、アンチウイルスモジュールによって返され、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カスペルスキーユーザーの割合が最も高かったのは、トルコでした。金融の脅威が増大した理由の1つは、バンキング型トロイの木馬Goziの活動が激増したことです。Goziの開発者は、トロイの木馬Nymaimの作成者との連携が確認されています。

ロシアでは、2.92%のユーザーが第2四半期にバンキング型トロイの木馬に遭遇し、このランキングで2位になりました。

3位にはブラジルが入っています。リオデジャネイロオリンピックの影響で、次の第3四半期は中南米で金融の脅威が急増すると見込まれます。サイバー犯罪者にとって、オリンピックは無視できないほどに魅力的なイベントです。犯罪者は毎回、大規模なスポーツイベントのテーマを攻撃に利用して、潜在的な標的を欺こうとします。

バンキング型トロイの木馬の影響を受けたユーザーが少なかった上位5か国は、カナダ（0.33%）、米国（0.4%）、英国（0.4%）、フランス（0.43%）、オランダ（0.5%）です。

イタリ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の割合は0.62%、スペインは0.83%だったのに対し、ドイツは1.03%となりました。

## 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2四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* | 攻撃されたユーザーの割合（%）** |
|---|---|---|
| 1 | Trojan-Spy.Win32.Zbot | 15.72 |
| 2 | Trojan-Banker.Win32.Gozi | 3.28 |
| 3 | Trojan.Win32.Qhost | 2.35 |
| 4 | Trojan-Banker.Win32.Shiotob | 2.27 |

| | | |
|---|---|---|
| 5 | Trojan-Banker.Win32.BestaFera | 2.12 |
| 6 | Trojan.Win32.Nymaim | 1.98 |
| 7 | Trojan-Banker.Win32.ChePro | 1.90 |
| 8 | Trojan-Banker.Win32.Banbra | 1.77 |
| 9 | Trojan.Win32.Neurevt | 0.67 |
| 10 | Backdoor.Win32.Shiz | 0.66 |

* 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、このランキングで常に1位に入っています。これは偶然ではありません。このトロイの木馬は2012年にソースコードが公開され、その結果、Zbotコードの一部を採用した新たなバンキング型トロイの木馬が登場するようになったからです。

2016年第2四半期は、Trojan.Win32.Nymaimによる悪意ある活動が急激に増加しました。これにより初めてトップ10にランクインし、一気に6位まで登り詰めました。Nymaimは当初、貴重なデータへのアクセスをブロックし、解除と引き替えに身代金を要求する設計（ランサムウェア）でしたが、最新バージョンには金融情報を窃取するバンキング型トロイの木馬の機能も実装されています。このことは、NymaimとGozi（同じく第2四半期の金融リスクトップ10にランクイン）の作成者が手を組んだ事実から説明がつきます。現在のNymaimのソースコードにはGoziのコードの一部が含まれており、感染コンピューターへのリモートアクセスが可能になっています。

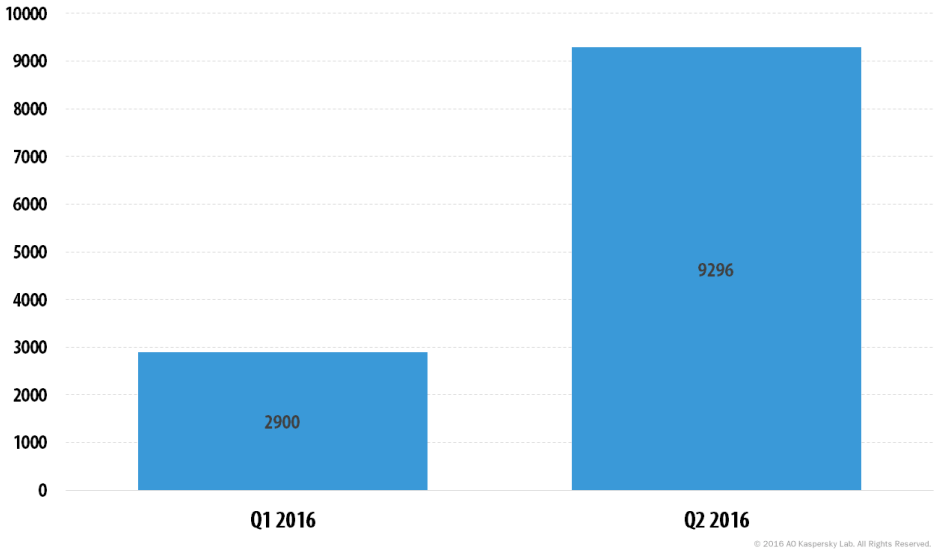
このランキングの常連であり、ブラジルで金融の脅威が猛威を振るっている原因の1つでもあるのが、Trojan-Banker.Win32.CheProファミリーです。このバンキング型マルウェアには、スクリーンショットの撮影、キー入力の登録、クリップボードの内容の読み取りという機能があります。すなわち、ほぼすべてのオンラインバンキングシステムを攻撃できる機能が備わっているということです。犯罪者は、検知されるまでの時間をできる限り引き延ばすために、新しい技術を採用しようとしています。このファミリーの一部トロイの木馬は、特定地域のユーザーへの感染を目的に、位置情報の利用や、システムのタイムゾーンとWindowsバージョンの取得を行います。

Trojan.Win32.Neurevtファミリーも、活発な金融の脅威として第2四半期に初めてトップ10入りしました。このファミリーのマルウェアは、2013年に発見されました。オンラインバンキングシステムのユーザーの決済データを窃取するだけでなく、スパムの配信（一部のバージョンは、たとえばSkypeでスパムメッセージを送信）や、DDoS攻撃の実行（Slowloris HTTPフラッド攻撃を実行可能な機能の追加による）に利用されています。

## ランサムウェア型トロイの木馬

弊社のウイルスコレクションに登録されている暗号化マルウェアの亜種の総数は、現在約26,000です。第2四半期には、新たに28のファミリーと**9,296**の亜種が確認されました。

次のグラフは、過去2四半期で新たに検知された、暗号化マルウェアの亜種の増加を示しています。




Trojan-Ransom暗号化マルウェア（ランサムウェア）の亜種の数
（2016年第1四半期と2016年第2四半期）

2016年第2四半期に検知されたトロイの木馬で、特に目立つものや特徴的なものを紹介します。

- **CryptXXX（Trojan-Ransom.Win32.CryptXXX）**

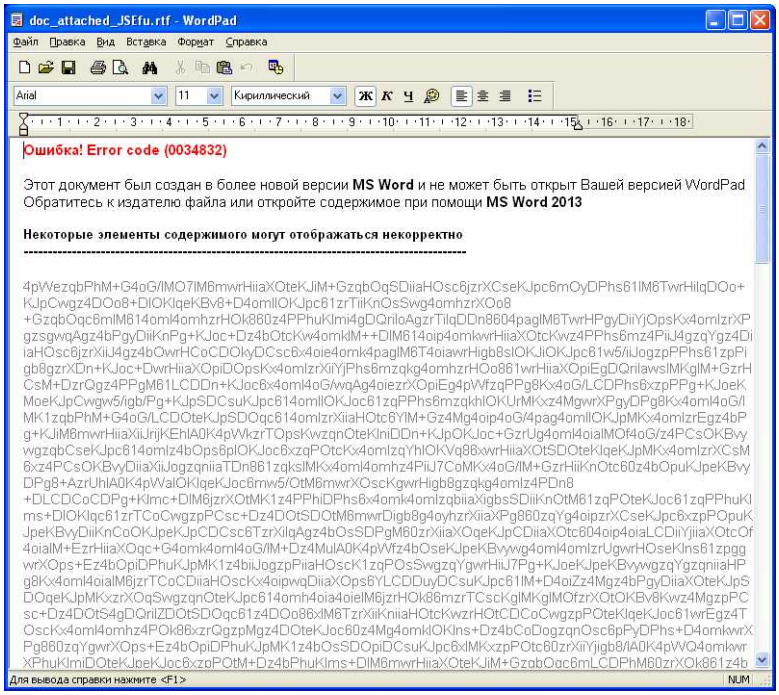
  この暗号化マルウェアは2016年4月以降、エクスプロイトキットによって広く拡散しました。以前のバージョンはファイル暗号化アルゴリズムに欠陥があったため、Kaspersky Labは復号化用のユーティリティをリリースすることができました。残念ながら、攻撃者は後続のバージョンで調整を行ったため、以降のCyprtXXX亜種の影響を受けたファイルは、復号化が不可能になっています。

- **ZCryptor（Trojan-Ransom.MSIL.Zcryptor）**

  これは、暗号化マルウェアの機能とワームの拡散手法を併せ持つマルウェアです。ランサムウェア型トロイの木馬は通常、自己拡散の機能を実装していません。ZCryptorは例外的な存在です。従来のワームと同様に、感染の際に自身のコピーをリムーバブルメディア内に作成し、autorun.infファイルを生成します。そのメディアが別のシステムに接続されると、実行ファイルが自動的に起動します（当然ながら、自動実行機能が無効になっていない場合）。

- **RAA（Trojan-Ransom.JS.RaaCrypt）**

  暗号化マルウェアは時折、他の暗号化マルウェアと機能面で異なるものが登場します。また、独特の実装がアナリストの目にとまることがあります。RAAの場合は、プログラミング言語の選択が興味深い点でした。全体がJavaScriptで作成されていたのです。プログラム全体が1つの.jsファイルに含まれており、スパムメッセージの添付ファイルとして標的に配信されていました。実行すると偽のエラーメッセージが表示され、その間にユーザーのファイルが暗号化されます。

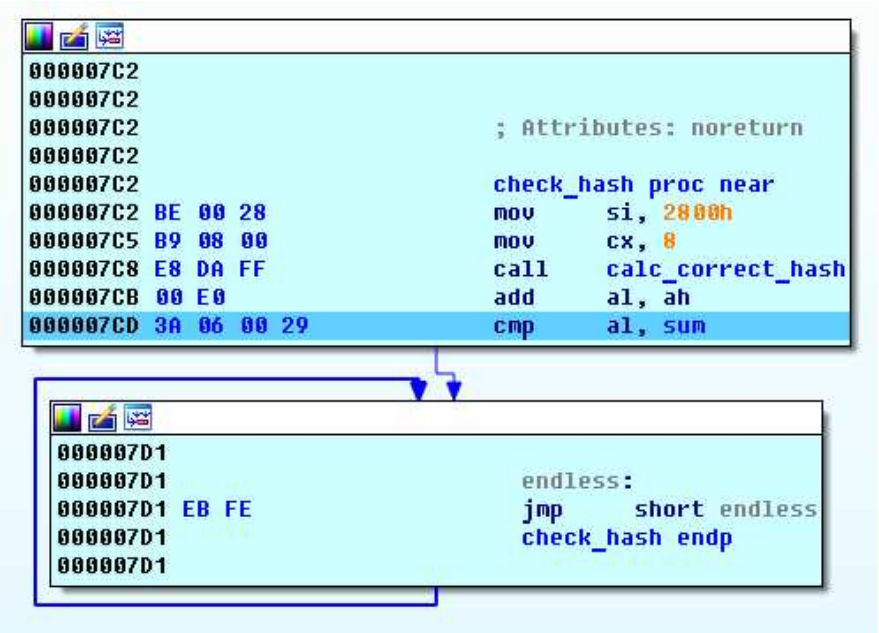



- **Bart（Trojan-Ransom.Win32.Bart）**

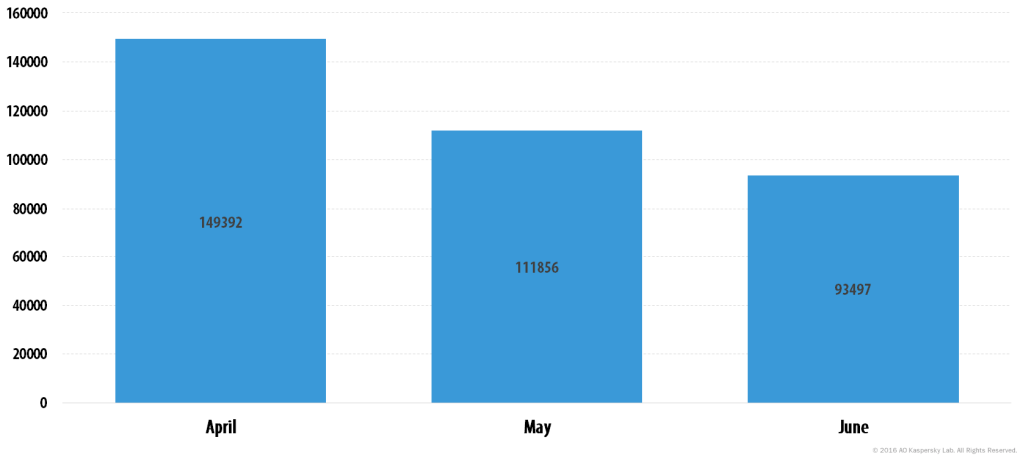
  この暗号化マルウェアは、標的のファイルをパスワードで保護されたZIPアーカイブに格納します。パスワードは、楕円曲線ディフィー・ヘルマンアルゴリズムを使って作成します。身代金メモと支払サイトのデザインは、悪名高きLockyのものを完全にコピーしています。

- **Satana（Trojan-Ransom.Win32.Satan）**

  これはマスターブートレコード（MBR）ブロッカーとファイル暗号化マルウェアを組み合わせたもので、悪名高きトロイの木馬PetyaとMischaの類似機能の影響を受けていると考えられます。SatanaはPetyaと異なり、マスターファイルテーブル（MFT）を暗号化しません。むしろ、SatanaのMBRモジュールは明らかに不完全です。標的が入力したパスワードをチェックするプロセスが、ループを繰り返すだけだからです。それを示すコードの一部を以下に示します。




## ランサムウェアの攻撃を受けたユーザーの数




Trojan-Ransom暗号化マルウェアに攻撃されたユーザー数（2016年第2四半期）

2016年第2四半期に暗号化マルウェアの攻撃を受けたユニークユーザーは311,590人で、第1四半期から16%減少しました。そのうちの約21%は、企業のユーザーです。

実際のインシデント数は、この数倍であることに注意する必要があります。統計にはシグネチャベースの検知とふるまい検知の結果しか反映されていませんが、カスペルスキー製品は多くの場合、マルウェアのふるまいに基づいて検知し、そこではマルウェアの種類を特定しないためです。

## 暗号化マルウェアの攻撃が多い上位10か国

| | 国* | 暗号化マルウェアに攻撃されたユーザーの割合（%） ** |
|---|---|---|
| 1 | 日本 | 2.40 |
| 2 | イタリア | 1.50 |
| 3 | ジブチ | 1.46 |
| 4 | ルクセンブルク | 1.36 |
| 5 | ブルガリア | 1.34 |
| 6 | クロアチア | 1.25 |
| 7 | モルジブ | 1.22 |
| 8 | 韓国 | 1.21 |
| 9 | オランダ | 1.15 |
| 10 | 台湾 | 1.04 |

* 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

第2四半期は、上位10か国の半数をヨーロッパ諸国が占めました。第1四半期から1か国減っています。

第1四半期に9位だった日本は、今回は1位となり、暗号化マルウェアの攻撃を受けたユーザーは2.4%でした。日本で最も蔓延している暗号化マルウェアファミリーはLocky、CTB-Locker、Cerber、TeslaCryptです。

このランキングに初めて入ったのは、ジブチ（1.46%）、韓国（1.21%）、台湾（1.04%）でした。

## 広範囲に蔓延した暗号化マルウェアファミリー上位10種

| | 名称* | 判定* | 攻撃されたユーザーの割合（%）** |
|---|---|---|---|
| 1 | CTB-Locker | Trojan-Ransom.Win32.Onion/<br>Trojan-Ransom.NSIS.Onion | 14.59 |
| 2 | Teslacrypt | Trojan-Ransom.Win32.Bitman | 8.36 |
| 3 | Locky | Trojan-Ransom.Win32.Locky | 3.34 |
| 4 | Shade | Trojan-Ransom.Win32.Shade | 2.14 |
| 5 | Cryrar/<br>ACCDFISA | Trojan-Ransom.Win32.Cryrar | 2.02 |
| 6 | Cryptowall | Trojan-Ransom.Win32.Cryptodef | 1.98 |
| 7 | Cryakl | Trojan-Ransom.Win32.Cryakl | 1.93 |
| 8 | Cerber | Trojan-Ransom.Win32.Zerber | 1.53 |
| 9 | Scatter | Trojan-Ransom.BAT.Scatter/<br>Trojan-Downloader.JS.Scatter/<br>Trojan-Dropper.JS.Scatter/<br>Trojan-Ransom.Win32.Scatter | 1.39 |
| 10 | Rakhni | Trojan-Ransom.Win32.Rakhni/<br>Trojan-Downloader.Win32.Rakhni | 1.13 |

*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2四半期の1位は、CTB-Locker（Trojan-Ransom.Win32/NSIS.Onion）ファミリーでした。2位はTeslaCryptファミリーで、判定はTrojan-Ransom.Win32.Bitmanのみです。Trojan-Ransom.JS.Cryptoload判定はかつて、マルウェアをダウンロードしており、TeslaCryptと関連づけられていましたが、現在はこのファミリーだけの特徴ではありません。TeslaCryptは、以前はこの統計で1位になっていましたが、幸いなことに2016年5月に消滅しました。所有者がサーバーを無効化して、ファイルを復号化するマスターキーを公開したからです。

第1四半期のランキングとの違いは、CerberとCryrarがランクインした点のみです。

暗号化マルウェアCerberは、スパムとエクスプロイトキットによって拡散します。Torネットワーク上のCerberのサイトは多数の言語に翻訳されています。特筆すべき機能には、以下のものがあります。

- 感染したシステムを慎重に調査します。アンチウイルスがインストールされているかどうか、仮想マシン（Parallels、VMWare、QEMU、VirutalBox）やWine上で稼働しているかどうかを確認するほか、さまざまなリサーチャーやアナリストのユーティリティをチェックし（ディスクドライブ上の特定のプロセスやファイルを検索することで確認）、さらにはシステムドライブのシリアル番号のブラックリストも保持しています。
- 感染システムのキーボードのレイアウトとIPアドレスを確認します。CIS諸国にあるマシンであることを検知すると、感染を停止します。
- アンチウイルスの保護機能を回避するために、アンチウイルスのプロセスの停止、サービスの中断、ファイルの削除を行います。
- 他のファミリーと同様に、暗号化したことをTXTとHTMLのファイル形式で知らせるほか、VBSスクリプトを実行し、次の音声メッセージを再生します。「Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!」（警告！ 警告！ 警告！ あなたのドキュメント、写真、データベース、その他重要なファイルを暗号化しました）

暗号化マルウェアCryrarは、Anti Cyber Crime Department of Federal Internet Security Agency（ACCDFISA）や、Anti-Child Porn Spam Protectionなどの名称でも知られており、2012年に初めて確認されました。標的のファイルをパスワードで保護された自己抽出型RARアーカイブに格納する特色があります。KSNの統計によると、新たなライバルにその地位を譲る気配はありません。