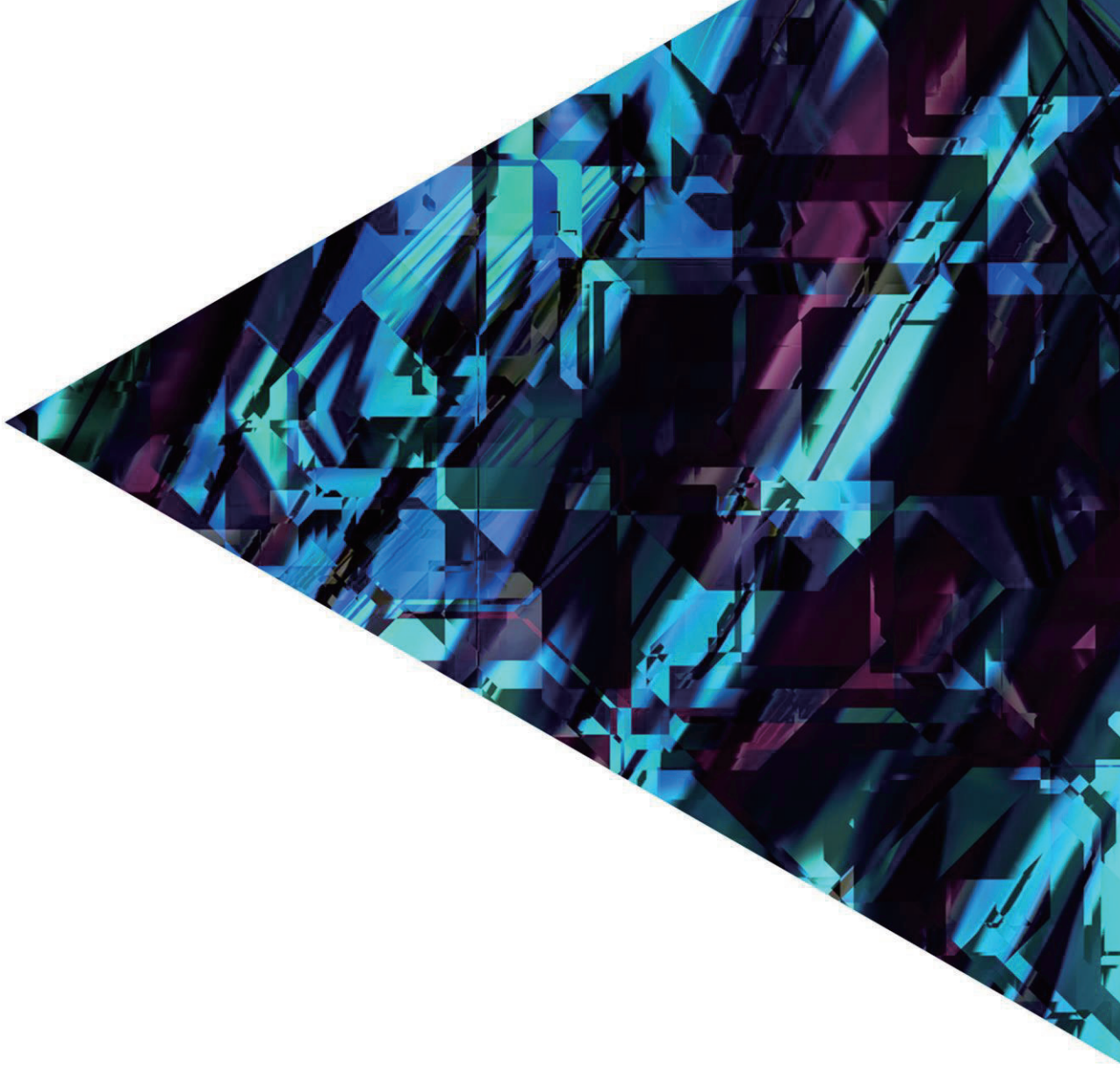


IT THREAT EVOLUTION IN Q1 2016

ーランサムウェア型トロイの木馬

Alexander Gostev, Roman Unuchek, Maria Garnaeva, Denis Makrushin, Anton Ivanov

*本資料は、英語版からランサムウェアの章を抜粋した抄訳版です。

KASPERSKY lab

ランサムウェア型トロイの木馬

ランサムウェア型トロイの木馬は、第1四半期のメイントピックとなりましたが、更なる警戒が必要です。1年を通じた最大の問題となる可能性も十分にあります。

わずかな期間でここまでランサムウェアの猛威が広がっている要因は、多少の知識があれば誰でもソースコードという形で多数のランサムウェアを利用できる状況が挙げられます。また、身代金の支払いにビットコインが利用されているため、犯罪者の特定が難しくなっています。

さらに、ランサムウェア・アズ・ア・サービス（RaaS）というビジネスモデルの普及も大きいとみています。既存のアフィリエイトの仕組みが取り入れられ、攻撃者はランサムウェアやその拡散に対する報奨金や身代金のレベニューシェアを取り入れることで、分業と「ビジネス」の拡大を実現しています。「パートナー」は主にアダルトサイトの管理者です。これと逆のパターンもあり、利用者にツール一式を提供して、利用者がトロイの木馬を拡散すると、身代金の10%が手数料として支払われます。

2016年第1四半期には、多数の有名なAPTグループ（主に中国のグループ）がランサムウェアを使用したインシデントが報告されていますが、カスペルスキーの調査では中国のグループに限りません。上記のようなインシデントがトレンドになれば、ランサムウェアの脅威は新たな段階に進むことになるでしょう。

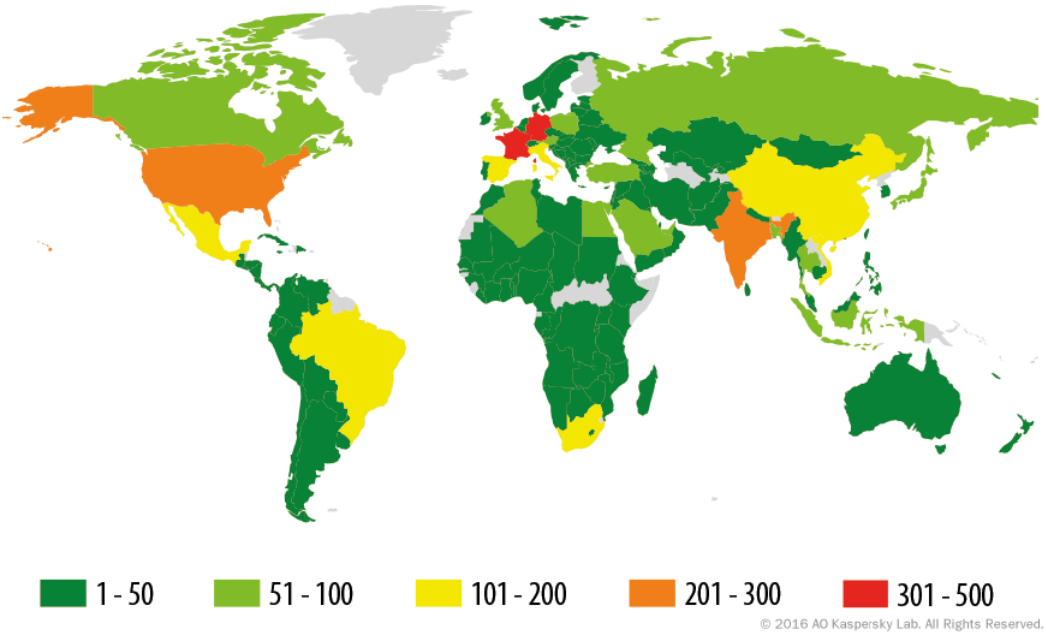
ランサムウェア型トロイの木馬は活動の範囲を広げており、2016年第1四半期には、WebサーバーがCTB-Lockerの標的となりました。

CTB-Lockerの初期バージョンは、暗号化ランサムウェア「Onion」として知られており、他のランサムウェアとの違いは、匿名ネットワークTorを使用してコマンドサーバーを保護していたことでした。基本的に無効化できるのは静的なサーバーだけであるため、Torを利用することでコマンドサーバーの無効化を回避することが可能になります。Torの利用は、マルウェアの検知やブロックの回避にも有効な手段です。CTB-Lockerの活動を保護していた手段はもう1つあります。それは、ビットコインによる支払いだけを受け付けるということです。ビットコインは、中央機関が存在しない、ほぼ匿名の暗号通貨です。

新バージョンのCTB-Lockerは、Webサーバーを暗号化し、身代金として0.5ビットコイン（最大約150ドル）を要求します。期限までに支払いが行われない場合は、倍の約300ドルが要求されます。身代金が支払われると、Webサーバーのファイルを復号する鍵が生成されます。

しかし、2016年第1四半期に最も蔓延したランサムウェアはLockyでした。（カスペルスキー製品での検知名はTrojan-Ransom.Win32.Locky）

Lockyは今も拡散を続けており、カスペルスキーでは世界114か国で感染の試みを観測しています。



サイバー犯罪者は、悪意あるダウンローダーを添付したスパムメールを大量送信して、Lockyの拡散を図ります。当初は、悪意あるスパムメールにドキュメントファイルが添付されており、その中のマクロがリモートサーバーからトロイの木馬Lockyをダウンロードして実行していました。

本レポートの作成時点でもスパムメールは送信されていますが、ドキュメントファイルではなくZIPファイルが添付されるようになり、ZIPにはJavaScriptの難読化されたスクリプトが1つまたは複数含まれています。大半のメールは英語ですが、2言語のバージョンも確認されています。

ランサムウェアにおける最も大きな技術革新は、ファイルから、フルディスクの暗号化対象の変化（具体的にはファイルシステムテーブルの暗号化）でした。この手口はPetyaで初めて確認されています。（Petyaとはロシア人の名前「ピョートル」の愛称ですが、ランサムウェアとロシア語話者の関連性は不明です）

Petyaは主なファイルテーブルを暗号化した後、その本性を現し、ドクロと骨のASCIIアートを表示した後は一般的なランサムウェア同様に身代金を要求します。Petyaの要求額は0.9ビットコイン（約380ドル）です。

現時点で、Petyaが他のランサムウェアと異なる特徴は、インターネットに接続していなくても動作するという点だけです。これはさほど意外なことではありません。Petyaは基本的に、オペレーティングシステムを「飲み込んで」しまい、インターネット接続機能も使えなくするためです。したがって、ユーザーは別のコンピューターを使用して身代金を支払い、データを復元しなければなりません。

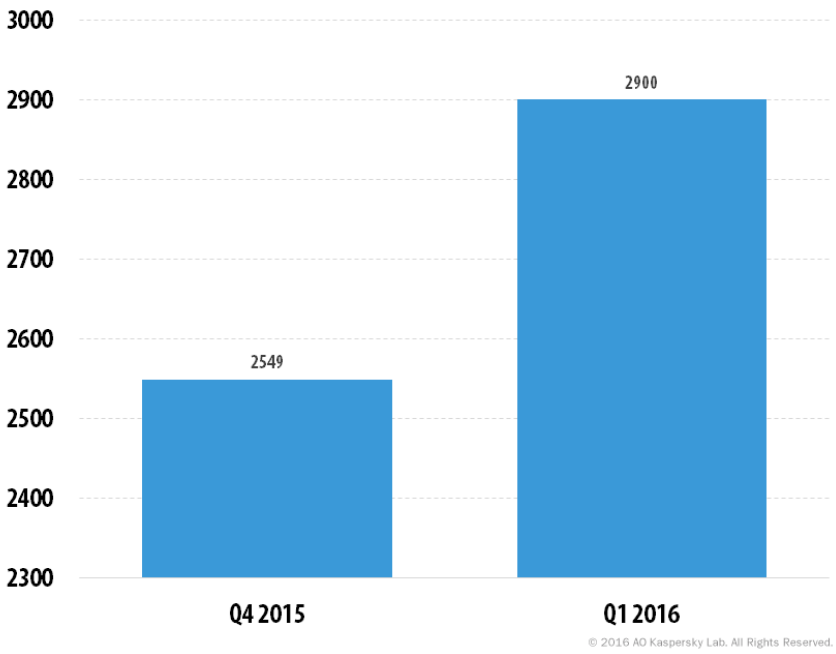
3月に発見されたMac OS Xを暗号化するTrojan-Ransom.OSX.KeRangerは、オープンソースプロジェクトTransmissionの公式Webサイトで提供されていたBitTorrentクライアントを介して拡散していました。おそらくこのサイトがハッキングされ、ダウンロード用のファイルが差し替えられていたと考えられます。似たケースでは、Macを暗号化するKeRangerが、Appleの有効な証明書で署名されていたため、Gatekeeperセキュリティ機能を通過できたと見られています。

暗号化トロイの木馬に関する統計

暗号化マルウェアは、トロイの木馬のサブグループであるTrojan-Ransomに分類され、いわゆるブラウザーランサムウェアも含まれます。Trojan-Ransomに占める割合は、ブラウザーランサムウェアの25%で、主にロシアとCIS諸国に限定されているため、このセクションでは、ブラウザーランサムウェアについては深く掘り下げず、暗号化マルウェアについて詳しく解説します。

新種のTrojan-Ransom暗号化マルウェアの数

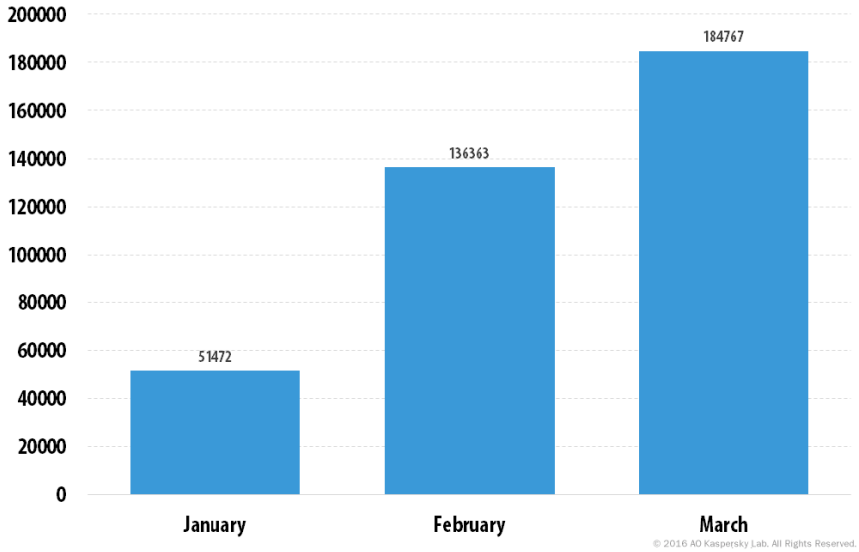
次のグラフは、過去2四半期で新たに検知された、暗号化マルウェアの亜種の増加を示しています。



Kaspersky LabのVirus Collectionに登録された、Trojan-Ransom暗号化マルウェア（ランサムウェア）の亜種の数
（2015年第4四半期と2016年第1四半期）

Virus Collection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15,000以上に上り、第1四半期には、9つのファミリーと2,900の亜種が確認されました。

暗号化マル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の数（2016年第1四半期）

2016年第1四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372,602人を数え、前四半期から30%増加しました。その内の約17%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（2016年第1四半期）

	国*	暗号化マルウェアに攻撃されたユーザーの割合（%）**
1	イタリア	3.06
2	オランダ	1.81
3	ベルギー	1.58
4	ルクセンブルク	1.36
5	ブルガリア	1.31
6	クロアチア	1.16
7	ルワンダ	1.15
8	レバノン	1.13
9	日本	1.11
10	モルディブ	1.11

* 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、Trojan-Ransom暗号化マルウェアの標的になったユニークユーザーの割合

第1四半期は、1位から6位までを欧州諸国が占めました。1位はイタリア（3.06%）で、最も蔓延した暗号化マルウェアファミリーはTeslaCrypt（Trojan-Ransom.Win32.Bitman）でした。2位はオランダ（1.81%）、3位はベルギー（1.58%）となっています。

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（2016年第1四半期）

	名称	判定*	ユーザーの割合**
1	TeslaCrypt	Trojan-Ransom.Win32.Bitman/ Trojan-Ransom.JS.Cryptoload	58.43%
2	CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	23.49%
3	CryptoWall / Cryptodef	Trojan-Ransom.Win32.Cryptodef	3.41%
4	Cryakl	Trojan-Ransom.Win32.Cryakl	3.22%
5	Scatter	Trojan-Ransom.BAT.Scatter/ Trojan-Downloader.JS.Scatter/ Trojan-Dropper.JS.Scatter/ Trojan-Ransom.Win32.Scatter	2.47%
6	Rakhni	Trojan-Ransom.Win32.Rakhni/ Trojan-Downloader.Win32.Rakhni	1.86%
7	Locky	Trojan-Ransom.Win32.Locky	1.30%
8	Shade	Trojan-Ransom.Win32.Shade	1.21%
9	iTorLock / Troli	Trojan-Ransom.MSIL.Lortok	0.84%
10	Mor / Gulcrypt	Trojan-Ransom.Win32.Mor	0.78%

* 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内、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1四半期の1位はTeslaCryptファミリーでした。このファミリーには、Trojan- Ransom.Win32.BitmanとTrojan-Ransom.JS.Cryptoloadが含まれます。後者は、主にスパムメールに添付されたZIPファイルに含まれるスクリプトが該当します。以前はこれらのスクリプトによってFareitやCryptoWallといったマルウェアがダウンロードされていましたが、最近ではTeslaCryptに変わっています。第1四半期の注目すべき点として、暗号化アルゴリズムが強化された新バージョンのTeslaCryptが拡散されていました。作成者は、AESの代わりに「信頼性の高い」RSA-4096を使用しています。

2位はCTB-Locker（Trojan-Ransom.Win32 / NSIS.Onion）ファミリーです。CTB-Lockerに属するマルウェアは通常、アフィリエイトプログラムによって拡散され、多数の言語でサポートされています。先述のとおり、2016年第1四半期には、Webサーバーのみを標的とするCTB-Lockerの新種が発見されました。すでに10か国の70台以上のサーバーで、Webルートファイルが暗号化される被害が報告されています。

Trojan-Ransom.Win32.Cryptodefファミリー（別名CryptoWall）が3位となりました。TeslaCryptと同様、このファミリーのマルウェアもスパムメールで拡散します。

5位はScatterファミリーでした。今年に入って、スパムメールによるScatter拡散の新たな流れが来ています。メールにはJavaScriptへのリンクが含まれており、ユーザーがダウンロードしてローカルで起動するように偽装されています。興味深いことに、スクリプトが実行されると、Scatterの他にもNitol（DDoSボット）とPony（主にパスワードなどの情報を窃取するトロイの木馬）という2つの悪質プログラムがディスクに保存されます。

第1四半期の調査で7位となったLockyファミリーは、欧州を中心に広い範囲で拡散している点が特徴です。匿名通信Torネットワークにある犯罪者の身代金要求メッセージを含むWebサイトは、20言語以上をサポートしていますが、ロシアや他のCIS諸国の言語はサポートされていません。そのため、サイバー犯罪者はこうした国の標的を攻撃することに関心を持っていない可能性があり、これはカスペルスキーの統計でも裏付けられています。

＊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。

株式会社カスペルスキー
PR-1023-201605