KASPERSKY

Kaspersky Security Bulletin 2016

2016 年サイバー脅威の主要動向:
ランサムウェア革命

GREAT

目次

はじめに

2016年はランサムウェアが全世界で猛威をふるい続けました。データやデバイスを暗号化し、個人や企業への影響力を強めました。

数字で見る2016年ランサムウェアの状況

- 新たに62種のランサムウェアファミリーが出現しました。
- 新しいランサムウェアの亜種の数が1～3月期の2,900から7～9月期の32,091となり、11倍になりました。
- 年初には20秒に1回だった個人へのランサムウェア攻撃が、9月末には10秒に1回になりました。
- 年初には2分に1回だった企業へのランサムウェア攻撃が、9月末には40秒に1回になりました。
- 身代金を支払った中小企業の5社に1社がデータを取り戻せませんでした。

2016年はランサムウェアがさらに高度化し、多様化しました。たとえば、金融系ソフトウェアへの対処方法、スクリプト言語の利用、新たな感染経路、標的のさらなる絞り込みのほか、スキル、リソース、時間が十分でない犯罪者を対象としたRansomware-as-a-Service（サービスとしてのランサムウェア）ソリューションの提供などが確認されました。いずれも、闇市場でのエコシステムの規模と効率が高まっているとみられます。

世界が結束して反撃

7月には、オランダ警察、欧州刑事警察機構（ユーロポール）、Intel Security、Kaspersky Labが合同でNo More Ransomプロジェクトを立ち上げました。10月にはさらに13の警察機関が加わりました。この協力体制によって、数々の無償復号ツールが開発されました。これまでに数千人ものランサムウェア被害者が、これらのツールを利用してデータを復元しています。

これは氷山の一角に過ぎず、まだ多くの課題が残されています。関係組織が協力し合えば、それぞれが単独で対応するよりもはるかに多くを成し遂げることができます。

ランサムウェアとは

ランサムウェアには2つの形式があります。最も一般的な形式のランサムウェアは、クリプター（暗号化型）です。このプログラムは、標的のデバイス上にあるデータを暗号化し、データの復元を約束する見返りに金銭を要求します。一方、ブロッカー（画面ロック型）は、デバイス上のデータには影響を与えません。その代わりにコンピューターなどデバイスへのアクセスをブロックし、使えないようにします。画面全体に表示される身代金要求メッセージは、一般に法執行機関からの通知を装っており、標的が違法なWebコンテンツにアクセスしたため罰金を支払うように指示します。両形式のランサムウェアの概要については、こちらをご覧ください。

ランサムウェア：2016 年の主な動向

出現したものと消滅したもの

Cerber、Locky、CryptXXX、および44,287種のランサムウェアの亜種が新たに出現

CerberとLockyは春先に出現しました。どちらもかなり悪質なランサムウェアで、主にスパムの添付ファイルやエクスプロイトキットを通じて広く伝播します。両方とも瞬く間に「主役」の座に着き、個人や企業を狙っています。この2つに引けをとらないのがCryptXXXです。この3つのファミリーは進化を続けており、既知のランサムウェア（CTB-Locker、CryptoWall、Shadeなど）とともに世界中で被害者から金銭を搾取しています。

2016年10月時点での、カスペルスキー製品が検知したランサムウェアファミリー上位10種

	名称	検知名 *	攻撃を受けたユーザーの割合(%) **
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（2016年5月まで活動）	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

* 上記の統計は、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。

** 暗号化型ランサムウェアの攻撃を受けた全ユーザーに対して、特定の暗号化型ランサムウェアファミリーの攻撃を受けたユーザーの割合。

Teslascrypt、Chimera、Wildfireが活動を停止

2016年最大の驚きは、TeslaCryptの作成者が自ら活動を停止し、復号のためのマスターキーを公開したことです。

Ransomware-as-a-Service（RaaS）モデルを他の犯罪者に提供した最初のトロイの木馬の1つであるEncryptor RaaSは、そのボットネットの一部が警察によって壊滅されたのちに活動を停止しました。

その後7月には、Petya/Mischaランサムウェアの関係者と主張する何者かによって、Chimeraランサムウェアの約3,500の復号キーが公開されました。ただし、PetyaランサムウェアにChimera独自のソースコードの一部が使われていたため、実際はPetyaが同じグループに属し、その製品群をアップデートしていたずらを仕掛けただけという可能性もあります。

Wildfireについては、サーバーが押収され、Kaspersky Lab、Intel Security、ユーロポールが協働して復号キーを開発しましたが、Hadesとして復活したとみられています。

「教育用」ランサムウェアの悪用

「教育用」ランサムウェアは、攻撃に対するシミュレーションテストを目的とし、システム管理者に提供するために善意の研究者が開発したものです。犯罪者は、これらのツールをすぐさま手に入れて悪用しました。

教育用ランサムウェアHidden Tear & EDA2の開発者は、役立つようにと、GitHubにソースコードを投稿しました。2016年には当然のごとく、このコードに基づいた悪質なトロイの木馬が多数出現しました。その1つが、被害者のコンピューターの壁紙を人相の悪いサンタクロースの写真に差し替えて、2ビットコイン（約1,300ドル）を身代金として要求するDed Cryptorです。ほかにも、本物そっくりのWindows Update画面を表示するFantomというプログラムがあります。

従来とは異なる手法

- **ディスクの暗号化**

  2016年に初めて確認されたランサムウェアの攻撃手法に、ディスクの暗号化があります。この手法では、攻撃者が全ファイルを一度に暗号化してアクセス不能にします。その一例であるPetyaは、ユーザーのハードディスクのマスターインデックスにスクランブルをかけ、再起動を不可能にします。もう1つのトロイの木馬であるDcryptor（別名 Mamba）は、さらにもう一歩進んで、ハードディスク全体をロックダウンします。このランサムウェアは、オープンソースのDiskCryptorソフトウェアのコピーを使用して、オペレーティングシステム、アプリケーション、共有ファイル、全個人データを含むあらゆるディスクセクターにスクランブルをかけるため、特に厄介です。

- **「手動方式」での感染テクニック**

  Dcryptorは、攻撃者が標的のマシンにリモートアクセスするためにパスワードを総当たり攻撃するという手動方式によって感染します。2016年はこの従来型の手法が多く確認され、そのほとんどはサーバーを標的にして企業システムに侵入する手段として利用されています。

  攻撃が成功すると、サーバー上、さらにはサーバーからアクセス可能なすべてのネットワーク共有上にトロイの木馬がインストールされ、ファイルが暗号化されます。Kaspersky Labでは、この手法でランサムウェアをブラジルのサーバーに拡散させたTeamXRatを発見しました。

- **ツーインワン形式の感染**

  8月には、予想外の機能を持つShadeの検体を発見しました。感染したコンピューターが金融系サービスに関連している場合、Shadeが金銭窃取という長期的な目的でスパイウェアをインストールします。

スクリプト言語で作成されたランサムウェア

2016年に注目すべきもう1つの動向は、スクリプト言語で作成されたクリプターの増大です。第3四半期だけでも、Pythonで作成された新たなファミリー（HolyCrypt、CryPyなど）や、自動化言語のAutoItで作成されたStampadoが見つかっています。

続々と現れる素人と模倣

2016年に検知された新たなランサムウェア型トロイの木馬の多くは、高度なものではなく、ソフトウェアの欠陥や身代金要求メッセージの誤植など、低品質なものでした。これに伴い、Kaspersky Labでは既存のランサムウェアの模倣の増加を観測しています。

- BartはLockyの身代金要求メッセージと支払いページのスタイルを模倣している。
- AutoItで作成されたLockyを模倣したランサムウェア（名称はAutoLocky）は、同じ拡張子「.locky」を使用している。
- Crusis（別名Crysis）は、元々Shadeで使用されていた拡張子「.xtbl」を模倣している。
- Xoristは、Crusisで暗号化されたファイルの命名体系全体を模倣している。

Kaspersky Labが今年発見した中で最も目を引くものは、Polyglot（別名MarsJoke）です。これはCTB-Lockerの外観とファイル処理手法を完全にまねています。

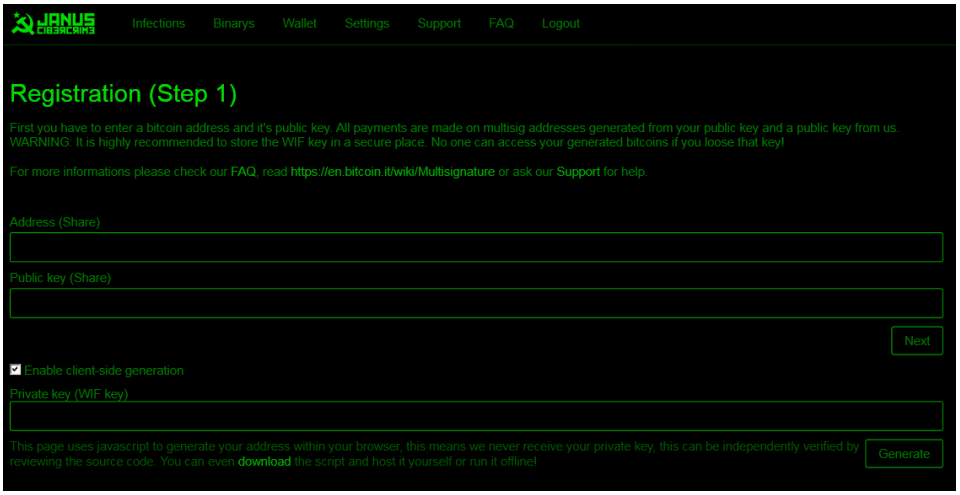
ほかのランサムウェアを模倣する動向は、2017年も高まることが予想されます。

繁栄するランサムウェアエコシステム

RaaS の台頭

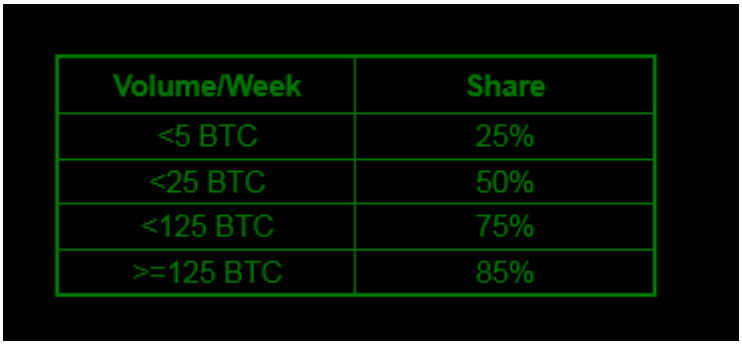
Ransomware-as-a-Service（RaaS）は新しい動向ではありませんが、2016年はこの伝播モデルが継続して開発され、これまで以上に多くのランサムウェア作成者が悪質な製品を「オンデマンド」で提供しました。独自に開発するためのスキル、リソース、あるいは意思に欠ける犯罪者にとって、この手法は非常に魅力的でしょう。

例として注目すべきものは、Petya/MischaとShark（のちにAtomという名前に変更）です。このビジネスモデルはますます高度化しています。



Petyaランサムウェアのパートナーサイト

パートナー（利用者）はほとんどの場合、従来型の手数料ベースの契約を結びます。たとえば、Petyaランサムウェアの「支払い表」によると、パートナーが1週間に125ビットコインを稼いだ場合、手数料を引いた106.25ビットコインがパートナーの取り分となります。



Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Petyaの支払い表

また、初期手数料もかかります。たとえば、Stompadoランサムウェアを使用するには、39ドルを支払う必要があります。

スパム配信や身代金要求メッセージなどのサービスを提供する犯罪者もいるため、意欲のある攻撃者は簡単に行動を起こすことができます。

カスタマーサポート提供やブランド化への動き

最も「プロフェッショナル」な攻撃者は、被害者にヘルプデスクやテクニカルサポートを提供して、身代金支払い用のビットコイン購入手続きを案内したり、場合によっては交渉にも応じ、被害者に支払いを促します。

さらに、ブラジルのランサムウェアについて調査しているKaspersky Labのエキスパートは、多くの攻撃者がランサムウェアのブランド化をある程度重視していることに気付きました。メディアが注目し、ユーザーが恐怖することを期待するタイプの攻撃者は、人目を引いて名前を売るような話題や戦術を選ぶでしょう。その一方で、目立つことを危惧するタイプの攻撃者は、名声の誘惑を捨て、被害者からメールで連絡させて支払先のビットコインアドレスを通知するだけの手口にとどめるでしょう。

ビットコイン優位は変わらず

2016年全体を通して、利用度の高いランサムウェアファミリーでは、依然としてビットコインでの支払いが好まれました。ランサムウェアの要求額のほとんどは法外な金額ではありませんでしたが（平均300ドル前後）、一部では高額が請求され、実際に支払われています。

それ以外の場合、特別な地域や手作り的に行われる活動では、現地での支払方法が利用されましたが、それは同時に、その手段ではもはや隠れることができず、他の雑多なランサムウェアに紛れることができなくなることを意味します。

企業に矛先を向けたランサムウェア

2016年最初の3か月間は、ランサムウェア攻撃の17%が企業を標的としていました。これは、全世界で2分に1社が攻撃されたことになります。*2　第3四半期の終わりには、この割合が23.9%に上昇しました。これは40秒に1社が攻撃されたことになります。

Kaspersky Labの法人を対象にした調査によると、2016年は全世界の5社に1社が、ランサムウェア攻撃に起因するITセキュリティインシデントを経験しました。

- 過去12か月間に、中小企業の42%がランサムウェアの攻撃を受けました。
- そのうちの32%が身代金を支払いました。
- 身代金を支払った中小企業の5社に1社がデータを取り戻せませんでした。
- ランサムウェアの被害を受けた企業の67%が自社データの一部または全部を失い、4社に1社はアクセスの回復に数週間を要しました。

ソーシャルエンジニアリングとヒューマンエラーは、依然として企業の脆弱性の主な要因です。重大なデータ損失が生じた事例の5件に1件は、従業員の不注意や認識不足によって発生しています。

様々な業種がランサムウェアのリスクにさらされている

業種	攻撃を受けた割合(%)
教育	23
IT / 通信事業	22
エンターテインメント / メディア	21
金融サービス	21
建設	19
政府 /官公庁 / 防衛	18
製造	18
運輸	17
医療	16
小売 / 卸売 / レジャー	16

*2　2016 年第 1 四半期にカスペルスキー製品によってランサムウェア攻撃がブロックされたユニークユーザー372,602 のうち 17%、および第 3 四半期の同ユニークユーザー821,865 のうち 23.9%。

2016 年の注目すべき攻撃

- **病院が主要な標的に** – 手術の中止や患者の転院などの甚大な影響が生じる可能性がありました。
  - 3月に発生した最も有名なランサムウェア攻撃の事例では、ロサンゼルスの医療センターHollywood Presbyterian Medical Centerのコンピューターが犯罪者によってロックダウンされ、病院は17,000ドルを支払いました。
  - 数週間のうちに、ドイツの複数の病院も攻撃を受けました。
  - 英国では28のNational Health Service（国民保健サービス）トラストが、攻撃を受けたことを認めました。
- 9月には、**ホスト型デスクトップおよびクラウドプロバイダー**のVESKが、攻撃を受けた後にシステムの1つへのアクセスを回復するために約23,000ドルの身代金を支払いました。
- 3月には、ニューヨーク・タイムズ、BBC、AOLなどの**大手メディア**が攻撃を受けました。
- 有数の研究センターである**カナダのカルガリー大学**では、1週間にわたって暗号化されていたメールを復元するために、約16,000ドルを支払ったことを認めました。
- マサチューセッツ州の警察署では、警官が有害なメール添付ファイルを開いたことで、重要な事件関連データを復旧するために500ドルの身代金をビットコインで支払うことになりました。
- **モーターレース業界も攻撃を受けています。**業界屈指のレーシングチームであるNASCARは、4月にTeslaCryptの攻撃によって数百万ドルの価値があるデータを失う危機に直面しました。

ランサムウェアへの対抗

テクノロジーによる対抗

Kaspersky Labが提供する法人向けランサムウェア対策ツール「Kaspersky Anti-Ransomware Tool for Business」は、他のアンチウイルスソフトウェアと同時に利用できる「軽量の」ソリューションです。このツールは、トロイの木馬を早期に検知するために必要な2つのコンポーネントを使用します。1つは分散型のKaspersky Security Network、もう1つはアプリケーションの動きをモニタリングするシステムウォッチャーです。

Kaspersky Security Networkでは、ファイルとWebサイトURLの信頼性がクラウドを通じて迅速にチェックされます。システムウォッチャーは、プログラムの動作をチェックしているため、未知のトロイの木馬を事前にブロックすることができます。また、システムウォッチャーは、不審なアプリケーションが開くファイルをバックアップし、プログラムのアクションが悪意のあるものと判明した場合、変更内容をロールバックすることができます。

コラボレーションによる：No More Ransom プロジェクト

2016年7月25日に、オランダ警察、ユーロポール、Intel Security、Kaspersky Labが No More Ransomプロジェクトを開始しました。この非営利の取り組みでは、法執行機関と民間団体を結び付けるとともに、ランサムウェアの危険性を人々に伝え、データの復元を支援することを目指します。

「No More Ransom」Webサイトでは、現在、Kaspersky Labが開発した5種を含む、計8種の復号ツールが提供されています。これらのツールは、20種類以上のランサムウェアで暗号化されたファイルが復元可能です。現在までに、2,500人を超える被害者がデータを取り戻し、約100万ドルの身代金支払いを防いだと試算されています。

10月には、さらに13か国の法執行機関がプロジェクトに加わりました（ボスニア・ヘルツェゴビナ、ブルガリア、コロンビア、フランス、ハンガリー、アイルランド、イタリア、ラトビア、リトアニア、ポルトガル、スペイン、スイス、英国）。

このプロジェクトの方針は、Eurojust（欧州司法機構）とEuropean Commission（欧州委員会）からも支持されており、さらに多くの警察機関や民間組織が同プログラムに参加する予定です。

ランサムウェアに立ち向かう - 安全を確保するには

1. データのバックアップを定期的に必ず行う。
2. 信頼できるセキュリティソリューションを使用し、システムウォッチャーなどの重要な機能は常にオンにしておく。
3. 使用するすべてのデバイスでソフトウェアを常に最新の状態にしておく。
4. メールの添付ファイルや知らない人からのメッセージは注意して扱い、疑わしい場合は開かない。
5. 企業の場合は、従業員やITチームの教育、機密データの隔離、アクセスの制限、全データの常時バックアップも行う。
6. ランサムウェアの被害を受けた場合は、まず、No More Ransomサイトでファイルを取り戻すための復号ツールを探す。
7. ランサムウェアは犯罪行為です。感染した場合、必ず警察機関に通報してください。

身代金を支払うべきでない理由 - オランダ警察ハイテク犯罪部からのアドバイス

1. 一度でも身代金を支払うと、格好の標的として狙われる。
2. 犯罪者は信頼できず、身代金を支払ってもデータを取り戻せるとはかぎらない。
3. 次回はさらに高額の身代金を要求される。
4. 身代金の支払いは、犯罪を助長する。

ランサムウェアへの反撃に勝機はあるか

ランサムウェアへの反撃で勝利できると信じています。しかしそれには対抗する側が一丸となって取り組むことが重要です。ランサムウェアは高利益の犯罪ビジネスです。これを阻止するには、世界が結束して犯罪者のキルチェーンを断ち切るとともに、攻撃を実行して利益を得ることがいっそう難しくなるようにする必要があります。

株式会社カスペルスキー
PR-1031-201612