KASPERSKY lab

KSNレポート

ランサムウェアの脅威状況(2016年～2017年)

Kaspersky Lab

2017年7月

目次

エグゼクティブサマリー 3

はじめに：
過去1年間におけるランサムウェア進化の概況 4

パート1：
Windowsを狙うランサムウェア– 標的の推移 5

ランサムウェア同士のつぶし合い 12

WannaCryの大流行 15

パート2：モバイルを狙うランサムウェア
統計 19

パート3： どのように組織化していったのか 24

結論と予測 26

※本レポートは、2017年6月26日にKaspersky Labが発表したレポートに基づき作成したものです。

エグゼクティブサマリー

「ランサムウェア」はマルウェアの一種で、使用しているPCやモバイルなどの端末に感染し、その端末自体や保存されているデータを使用不能な状態にし、アクセスできないようにします。デバイスやデータを使用可能な状態に戻す（ロックを解除する）には、身代金を支払わなければなりません。多くの場合、支払いにはビットコインなどの仮想通貨が使用されます。

ランサムウェアは、画面ロック型と暗号化型の2タイプに分類できます。また、ランサムウェアを感染させる為のダウンローダー型トロイの木馬もランサムウェアとして分類されることもあります。

このレポートでは、ランサムウェアの脅威の状況についての調査結果を紹介しています。調査対象期間は2015年4月から2017年3月の2年間で、2016年度（2016年4月～2017年3月）と2015年度（2015年4月～2016年3月）のデータを比較します。

手法：

本レポートの統計情報は、Kaspersky Security Network（KSN）によって収集された匿名データを基にしています。KSNは、Kaspersky Labのセキュリティ製品の各種コンポーネントから情報を収集するクラウドベースのセキュリティネットワークです。インターネット上の新しい脅威を即時に検知し、感染源を数分でブロックすることでKSNに接続されたすべての端末を保護します。KSNには全世界で数千万の個人および法人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。すべての情報は、ユーザーの同意を得て収集されています。KSN機能が有効化されたカスペルスキー製品のユーザーが利用する端末のうち、期間内に少なくとも1回、ランサムウェアの攻撃を検知した端末台数を測定基準としています。また、Kaspersky Labのエキスパートによるランサムウェアの脅威の状況に関する調査の結果も併せて使用しています。

主な調査結果：

- ランサムウェアの攻撃を検知した端末数は**2,581,026台**で、前年より**11.4%**増加しました（2015年度は**2,315,931**台）。
- マルウェアの攻撃を検知した端末のうち、一度でもランサムウェアの攻撃を検知した割合は**3.9%**と、前年より0.4ポイント減少しました（2015年度は**4.3%**）。
- ランサムウェアの攻撃を検知した端末のうち、暗号化型ランサムウェアだった割合は**44.6%**で、前年より**13.6**ポイント上昇しています（2015年度は**31%**）。
- 暗号化型ランサムウェアの攻撃を検知した端末は**1,152,299**台で、前年の**1.6**倍に増加しました（2015年度は**718,536**台）。
- モバイルランサムウェアの攻撃を検知したAndroid端末は**130,232台**で、前年より**4.6%**減少しています（2015年度は**136,532台**）。

はじめに:
過去1年間におけるランサムウェア進化の概況

「Ransomware-as-a-Service」の台頭

2016年5月、Kaspersky Labは、ハードディスクドライブのマスターブートレコード(MBR)を上書きし、感染した端末のオペレーティングシステムを起動できないようにするランサムウェア、「Petya」を発見しました。

このマルウェアは、Ransomware-as-a-Service(サービスとしてのランサムウェア、以下RaaS)モデルとして注目に値する事例です。これは、ランサムウェア開発者が悪意ある製品を「オンデマンド」で提供し、複数の別の攻撃者が感染を拡大させ、ランサムウェアによって得た利益の一部を手に入れるといったビジネスモデルです。Petyaの開発者は、自身の取り分を確保するため、Petyaに「保護メカニズム」を組み込むことでサンプルを無断で使用できないようにしていました。

RaaSは新しいトレンドではありませんが、商品としてランサムウェアを提供する開発者もますます増え、この拡散モデルは進化を続けています。このアプローチは、自分自身でマルウェアを開発するだけのスキルやリソースを持たない、または独自でマルウェアを開発する気のない犯罪者にとって魅力的なビジネスモデルであることを証明しています。

2016年に登場した、このようにビジネスモデル化しているランサムウェアは、Petya/Mischaや「Shark」(後にAtomという名前でリブランドされたもの)が有名です。

標的型攻撃の増加

2017年初め、Kaspersky Labのエキスパートは、個人ユーザーへの攻撃から企業や組織を狙ったランサムウェア攻撃に切り替えるサイバー犯罪者が増加しているという危険な傾向を見つけました。

このような攻撃の標的は主に世界各地の金融機関で、Kaspersky Labのエキスパートは要求された身代金が50万ドルを超えるケースを複数確認しています。

このような状況は、ランサムウェアの犯罪者がより高額な金銭窃取を見込める企業や組織を対象にし始めた憂慮すべき傾向です。ランサムウェア攻撃の被害を受けるであろう組織も数多く存在しており、今後大規模なサイバー攻撃につながる可能性があります。

本レポートでは、攻撃の規模の把握と、世界的に新たな角度からランサムウェア開発が行われている理由について明らかにします。

パート1： Windowsを狙うランサムウェア– 標的の推移

調査対象期間である2015年4月～2017年3月のデータを見ると、伸び率が悪くなっているとはいえ、依然としてランサムウェアは増え続けています。2016年度にランサムウェアの攻撃を検知した端末数は全世界で**2,581,026**台となり、前年の**2,315,931台**から**11.4%**増加しました。2014年度から2015年度の上昇率は**17.7%**であることから、増加のペースは落ちています。

マルウェアの攻撃を検知した端末のうち、一度でもランサムウェアの攻撃を検知した割合は**3.9%で**、前年の**4.3%**から0.4ポイント減少しました。

図1と図2は、2015年4月～2017年3月の2年間に、1回以上ランサムウェアの攻撃を検知した端末台数の変化を表しています。ランサムウェア攻撃は散発的で波がありますが、2015年10月と2016年3月に急増しています。これらはランサムウェア「Locky」の活動が盛んな時期でした。

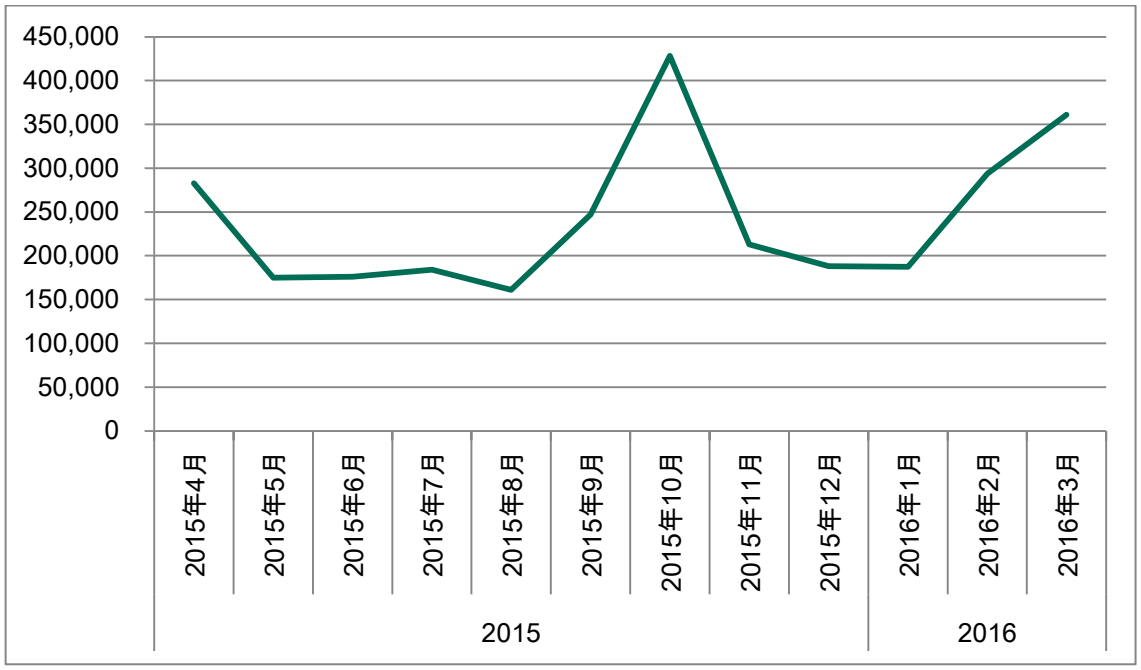


図1：2015年4月～2016年3月に、1回以上ランサムウェアの攻撃を検知した端末台数

2016年4月～2017年3月の状況はやや変化したように見えますが、それでも不安感は消えません。2016年度、ランサムウェア攻撃の回数は比較的一定で、1か月平均200,000～250,000回と前年よりも増加しています。これは憂慮すべき傾向かもしれません。それまで犯罪者が脅威の勢力を広げるため、秩序なく散発的に行っていた攻撃が、一定のペースを保った大規模な攻撃へと変化している可能性があります。また、図2の2016年6月と7月の増加も興味深いところです。この2か月間には、通信機能にTorを用いる「Onion」ランサムウェアが多数検知されています。

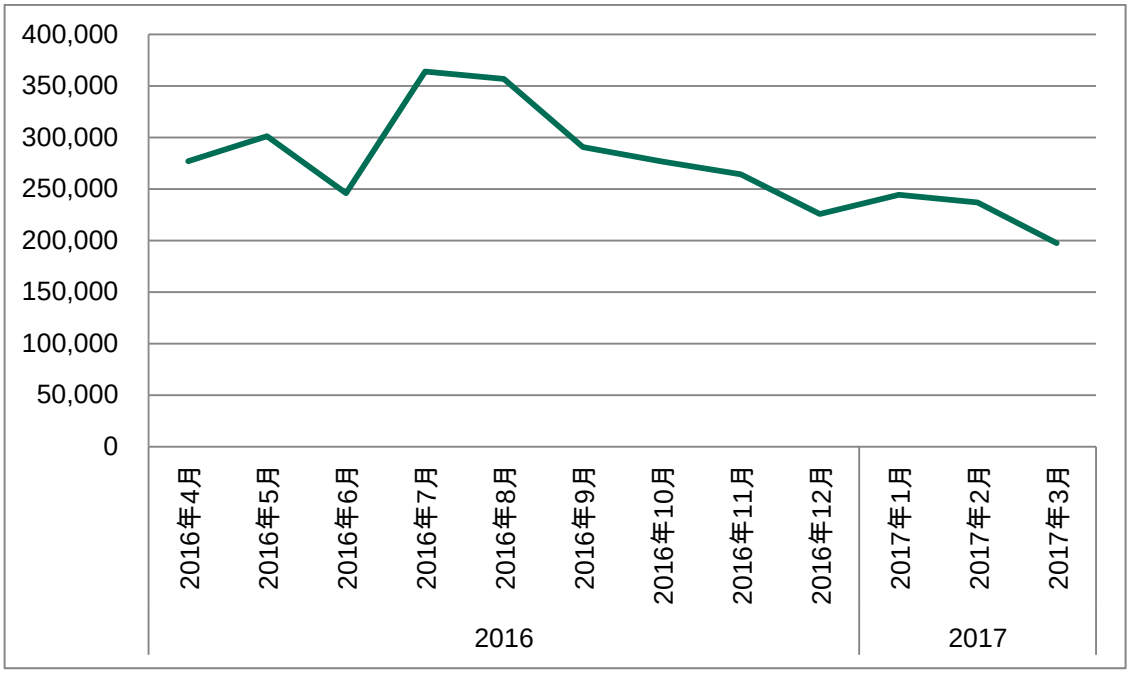


図2：2016年4月～2017年3月に、1回以上ランサムウェアの攻撃を検知した端末台数

その一方で、良い傾向とみられる点も2つあります。まず、増加率が緩やかになったのは、セキュリティベンダーや世界各地の司法当局などが共同で実施した対抗措置が成功した証である可能性があります。また、大規模な攻撃を世界中のメディアが報道したことにより、脅威に対する世間の関心が高まったことも一役買ったことでしょう。2つめの良い傾向は、年度末の状況が、2016年3月の上昇から、2017年3月には下降に転じている点です。

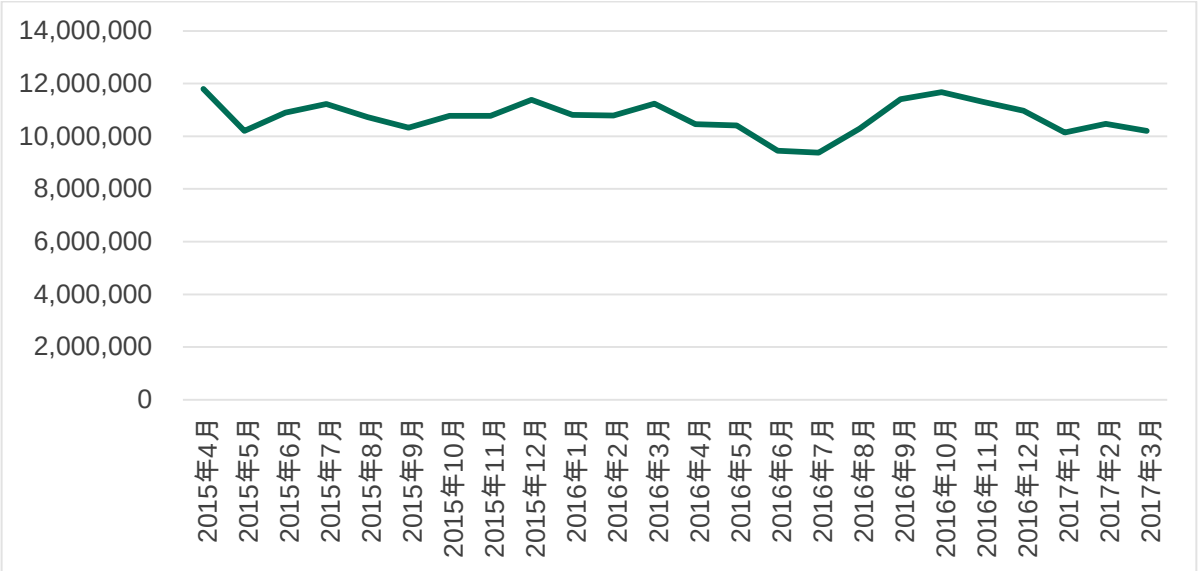


図3：2015年～2017年に、マルウェアの攻撃を検知した端末台数

図1と図2のランサムウェアの活動状況と図3のマルウェア攻撃の全体的な傾向は一致していません。ランサムウェア攻撃は、2015年秋をピークに2016年秋以降は減少していますが、マルウェアの攻撃は逆の動きを見せています。このような変動の背後に潜む理由を発見するためには、ランサムウェア攻撃の統計情報をさらに詳しく分析していく必要があります。

主な暗号化型ランサムウェア

本レポートの調査対象期間に活動していたマルウェアグループを見ると、暗号化型ランサムウェアによる攻撃の多くは、多様化したマルウェアグループによって引き起こされていることがわかります。2015年度に最も活発に感染を広げていたファミリーは、Bitman、Cryakl、Cryptodef、Onion、Shade、Morでした。これらのファミリーによる攻撃を検知した端末は、世界中で223,782台にも上りますが、この期間中の暗号化型ランサムウェアの攻撃を検知した端末台数の31%に過ぎません。

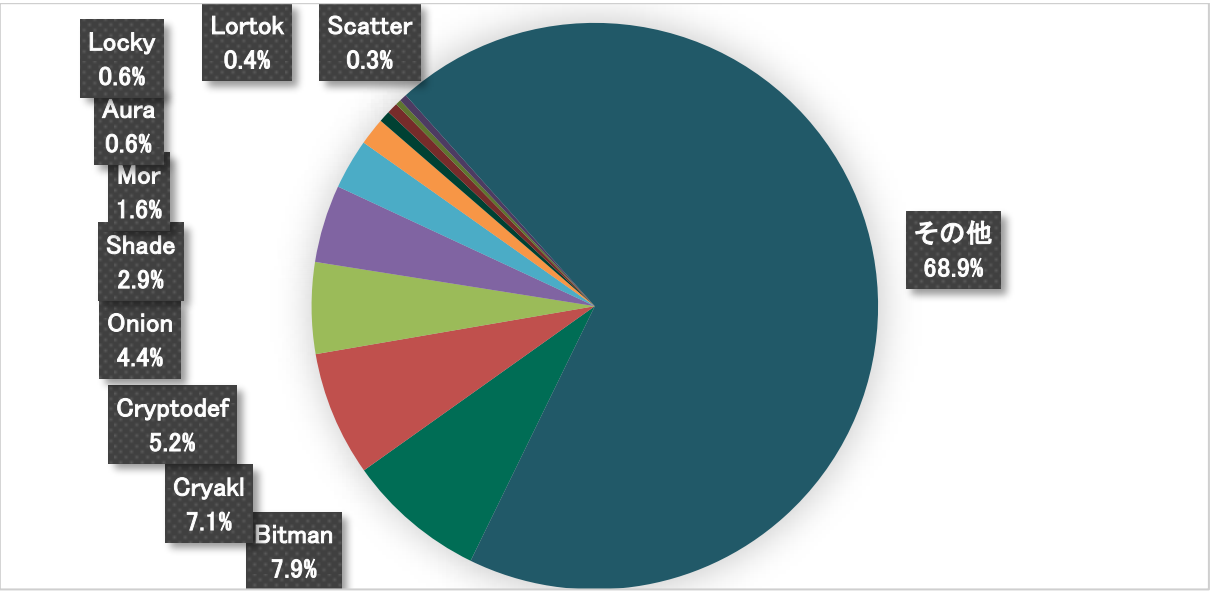


図4：2015年4月から2016年3月に、利用された暗号化型ランサムウェアの内訳

2016年度でも状況はそれほど大きく変わっていません。この期間中、Locky、CryptXXX、Zerber、Shade、Crusis、Cryrar、Snocry、Cryakl、Cryptodef、Onion、Sporaなど、広く拡散しているファミリーをすべてあわせても、暗号化型ランサムウェアの標的となった端末全体の約33%です。

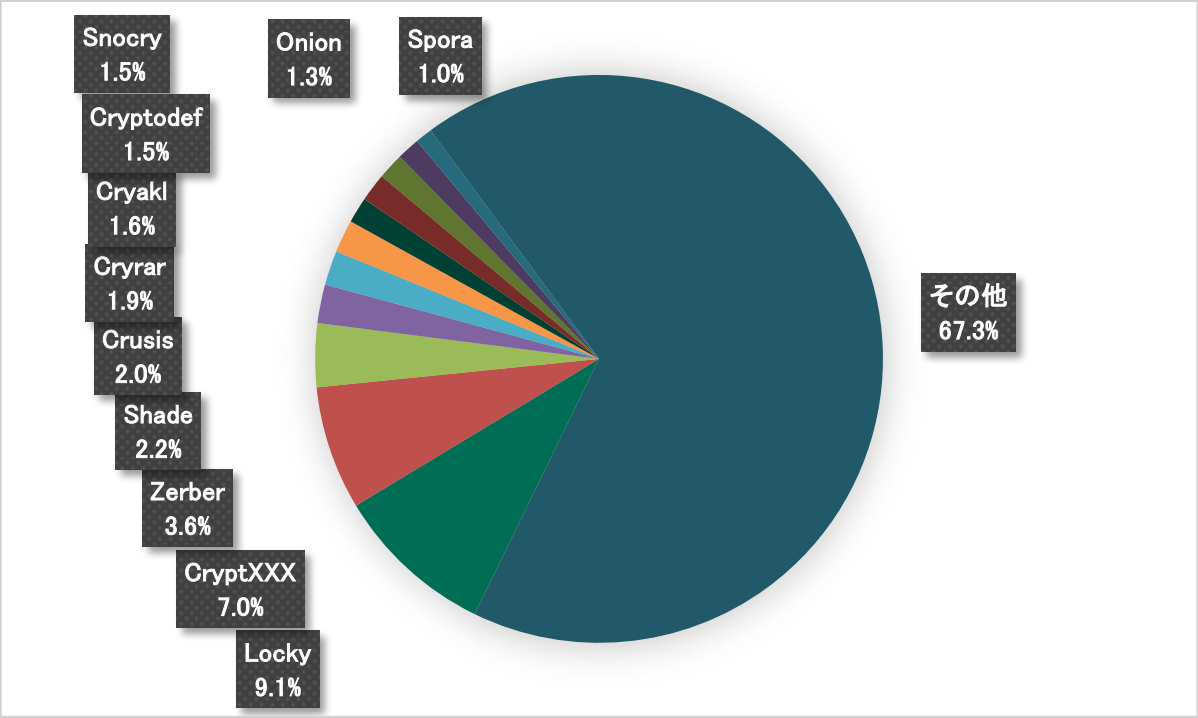


図5：2016年4月～2017年3月に、利用された暗号化型ランサムウェアの内訳

興味深いことに、7割近くを占める「その他」の割合は、暗号化型ランサムウェアの種類がさらに多様化していることを示しています。その原因は、特定のファミリーと関係していない暗号化型ランサムウェアのダウンローダーにあります。これは、金銭を窃取しユーザーを攻撃するその場限りのツールが容易に出現し、それを供給するようなインフラが、犯罪者間で広がっている兆候かもしれません。このプロセスについては、「パート3：どのように組織化していったのか」セクションで説明しますが、その前に、地理的な統計を詳しく見てみましょう。

地理的分布

攻撃を検知した端末の地理的分布を分析するときには、このデータが各国でカスペルスキー製品を利用しているユーザー数に影響を受けることに留意する必要があります。

ランサムウェアの攻撃を検知した端末の地理的分布を正確に把握するため、「マルウェアの攻撃を検知した端末全体のうちランサムウェア攻撃を検知した割合」を測定基準として使用しています。この測定基準を使用するほうが、各地域でランサムウェアに攻撃された端末台数を直接比較するよりも、脅威の地域的な分布状況を正確に理解できるからです。現在の状況を統計情報から正確に表すため、調査対象をカスペルスキー製品のユニークユーザー数が3万人を超える国に限定しています。

2015年度ランサムウェアの攻撃を検知した割合が高かった国は図6のとおりです。インド、ロシア、カザフスタン、イタリア、ドイツでは、ランサムウェア攻撃の割合が4%を超え、ランキングの上位を占めました。

	国名	マルウェアによる攻撃を検知した端末のうち、ランサムウェア攻撃を検知した割合（2015年4月～2016年3月）
1	インド	9.6%
2	ロシア	6.4%
3	カザフスタン	5.8%
4	イタリア	5.3%
5	ドイツ	4.3%
6	ベトナム	4.0%
7	アルジェリア	3.9%
8	ブラジル	3.7%
9	ウクライナ	3.7%
10	米国	1.4%

図6：2015年4月～2016年3月に、マルウェアによる攻撃を検知した端末のうち、ランサムウェア攻撃を検知した割合が高かった国
（対象：カスペルスキー製品のユニークユーザーが3万人を超える国）

	国名	マルウェアによる攻撃を検知した端末のうち、ランサムウェア攻撃を検知した割合（2016年4月～2017年3月）
1	トルコ	7.9%
2	ベトナム	7.5%
3	インド	7.1%
4	イタリア	6.6%
5	バングラデシュ	6.3%
6	日本	6.0%
7	イラン	5.9%
8	スペイン	5.8%
9	アルジェリア	3.8%
10	中国	3.8%

図7：2016年4月～2017年3月に、マルウェアによる攻撃を検知した端末のうち、ランサムウェア攻撃を検知した割合が高かった国
（対象：カスペルスキー製品のユニークユーザーが3万人を超える国が対象）

2016年度に新たにランクインした5か国の中では、日本、トルコでは急速に検知が増加しています。調査データによると、これらの国では2016年度、CrysisファミリーとLockyファミリーの活動が著しく活発になっていたことがわかります。一方、検知数が減少したのはインドだけでした。

トロイの木馬の機能を持つランサムウェアによる攻撃を検知した端末台数			
国名	2015年4月～2016年3月	2016年4月～2017年3月	前年比
トルコ	25,259	77,894	208.4%
ベトナム	89,247	181,469	103.3%
インド	325,638	292,846	△10.1%
イタリア	59,130	101,558	71.8%
バングラデシュ	22,005	35,160	59.8%
日本	12,822	63,472	395.0%
イラン	31,131	41,145	32.2%
スペイン	29,182	67,314	130.7%
アルジェリア	38,530	38,914	1%
中国	12,247	36,815	200.6%

図8:トロイの木馬の機能を持つランサムウェアによる攻撃を検知した端末台数の前年比

上記の分析結果は、ランサムウェアの状況が世界的に変化したことを示しています。暗号化ランサムウェアに攻撃を検知した端末台数を詳しく分析してみると少し違った印象を受けるかもしれません。

ランサムウェアによる攻撃を検知した端末のうち、暗号化型ランサムウェアの攻撃を検知した割合		
国名	2015年4月～2016年3月	2016年4月～2017年3月
トルコ	1.2%	2.2%
ベトナム	0.9%	2.2%
インド	0.7%	1.0%
イタリア	4.7%	4.4%
バングラデシュ	1.0%	2.1%
日本	4.7%	10.4%
イラン	0.8%	1.4%
スペイン	1.2%	1.9%
アルジェリア	0.5%	0.9%
中国	0.5%	1.3%

図9:ランサムウェアによる攻撃を検知した端末のうち、暗号化型ランサムウェアの攻撃を検知した割合

図9で明らかなとおり、ランサムウェアによる攻撃を検知した端末のうち、暗号化型ランサムウェアの攻撃を検知した割合に大きな変化は見られません。

前述した10か国で、2015年度にランサムウェアの攻撃を検知した端末全体の25%を占めています。2016年度には、この割合が40%に上昇しています。暗号化型ランサムウェアに限定してみても、20%強から30%と、同様の増加が見られます。

暗号化型ランサムウェアの攻撃を検知した端末台数との前年比			
国名	2015年4月～2016年3月	2016年4月～2017年3月	前年比(倍)
トルコ	10,302	21,097	+2.05
ベトナム	20,409	52,339	+2.56
インド	22,572	40,562	+1.78
イタリア	53,039	66,983	+1.26
バングラデシュ	5,380	11,816	+2.19
日本	32,470	110,168	+3.39
イラン	4,144	10,013	+2.42
スペイン	10,516	22,329	+2.12
アルジェリア	5,195	8,635	+1.66
中国	4,537	13,018	+2.87
その他	549,972	795,339	+1.45

図10:暗号化型ランサムウェアの攻撃を検知した端末台数との前年比

地理的分布については、トロイの木馬の機能を持つランサムウェアの攻撃を検知したユーザーの割合が一部の国で大きな変化を見せてはいますが、全世界的に見ると、攻撃を検知した端末台数はほとんど増えていないように見えます。繰り返しますが、これは攻撃が多様化し、今まで犯罪者の手が届かなかった地域に攻撃が拡大している傾向のあらわれかもしれません。結論として、特に前述した国のユーザーは、インターネットを利用する際にランサムウェアの被害に遭わないためにも、より注意を払う必要があるといえるでしょう。

ランサムウェア同士のつぶし合い

はじめに述べたように、悪名高いPetyaの開発者は、Petyaに「保護メカニズム」を組み込み、サンプルを無断で使用できないようにしています。2017年3月、Kaspersky Labのエキスパートは新種のマルウェアファミリー、PetrWrapを発見しました。PetrWrapは、RaaSのプラットフォーム経由で配信されたオリジナルのPetyaランサムウェアのモジュールを悪用して、企業や組織に標的型攻撃を仕掛けるランサムウェアです。またPetrWrapの作者は、Petyaのメカニズムを解明し、Petyaの作者に一銭も払わずに使用する方法を発見しました。サイバー攻撃者が別のサイバー攻撃者から「盗んだ」ランサムウェアツールの一例と言えます。

PetrWrapがどのように感染を広めているかはいまだに不明です。PetrWrapは感染後にPetyaを起動し、標的のデータを暗号化してから身代金を要求します。PetrWrapの作者は、「売り物」のPetyaに付属してきた秘密鍵と公開鍵の代わりに、独自の鍵を使用しています。これにより、身代金が支払われた場合、Petyaオペレーターの秘密鍵がなくとも、被害端末のデータを復号できるのです。

PetrWrapの開発者たちが、悪意ある活動のためにPetyaを選択したのは偶然ではありません。Petyaファミリーの暗号化アルゴリズム（暗号化型ランサムウェアの根幹となる暗号化コンポーネント）には非の打ち所がなく、解読が非常に困難といえます。セキュリティリサーチャーは過去に、暗号化する際のミスを手がかりとして、ファイルの復号方法を発見し、犯罪者たちが攻撃作戦に注ぎ込んだ努力をすべて無駄にしたケースがいくつかありました。これまでのバージョンのPetyaも該当していましたが、ランサムウェア開発者たちの手によってほとんどのミスが修正されました。

そのため、最新バージョンのPetyaの攻撃を受けた端末は確実に暗号化されてしまいます。このことからも、PetrWrap攻撃の首謀者たちがPetyaの使用を決めた理由は明白です。さらに、PetrWrapの攻撃を受けたユーザーに表示されるロック画面は、Petyaのことは一言も書かれていないため、セキュリティ専門家が状況を把握し、ランサムウェアファミリーを迅速に特定することが難しくなっています。

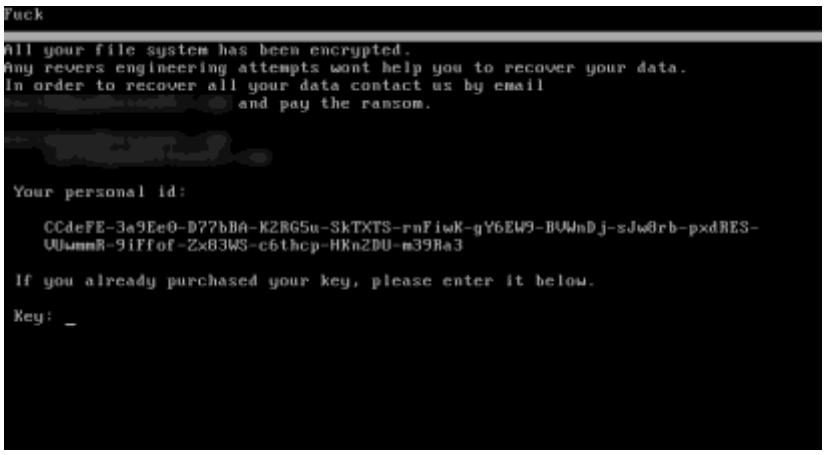


図11：PetrWrapに感染した端末の画面

PetrWrapは以下によって目標を達成します。

- 標的の端末をロックし、Windows NT系のファイルシステムであるNTFSパーティションのMFT（マスターファイルテーブル）を確実に暗号化する（この攻撃に使用されるPetya v3では、それ以前のバージョンに存在した欠陥が解決され、Salsa20暗号を正しく実装しているため）。
- ロック画面では、Petyaについて一切触れないため、状況の把握と被害範囲の特定が困難。
- PetrWrapの開発者は、低レベルのブートローダーコードを書く必要がなかったため、従来のバージョンのPetyaで見られたようなミスをするリスクを冒していない。

このようなことから、サイバー犯罪者が、互いのつぶし合いを始めたと考えられ、ランサムウェア犯罪グループ同士の競争が激化していることを表しています。犯罪者同士が闘い、欺き合う時間が長ければ長くなるほど、その悪意ある作戦の組織力が弱まるので、良いこととともいえますが、PetrWrapが標的型攻撃に使用されていることが懸念点です。標的型ランサムウェア攻撃の初めての事例ではありませんし、残念ながら今後も使用されるでしょう。

標的型攻撃

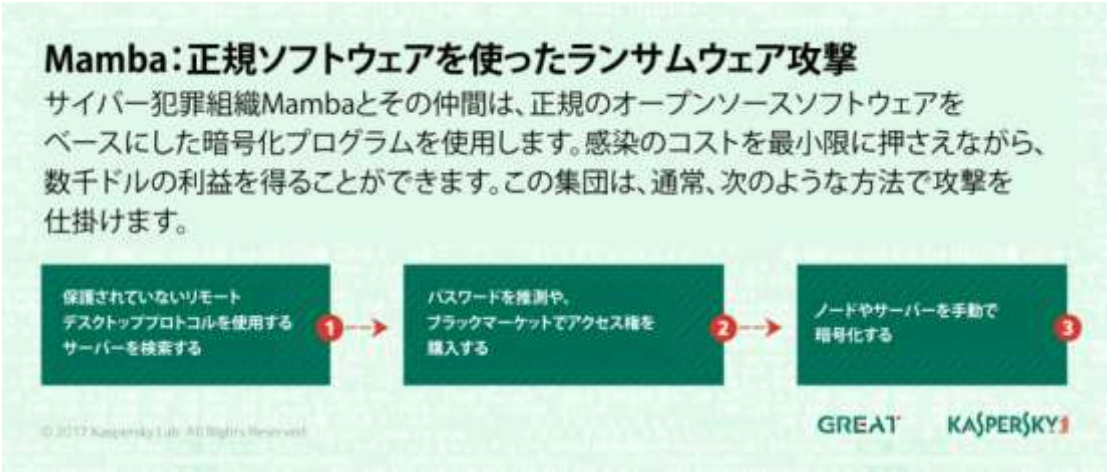
標的型ランサムウェア攻撃はますます広まる傾向にありますが、その理由は明らかです。犯罪者は、個人ユーザーへの大規模攻撃よりも、標的型ランサムウェアで企業を攻撃する方が、より多くの利益を見込めると考えているためです。企業に対するランサムウェア攻撃が成功すれば、その企業のビジネスプロセスを数時間または数日間にもわたって容易に停止させ、企業が身代金を支払うように仕向けることができます。

2017年、Kaspersky Labは世界中の金融組織を攻撃した8つの犯罪グループを特定しました。その中には、PetrWrapの開発者や悪名高いMambaグループが含まれます。残りの名もない6つのグループも企業や組織を標的にしていました。

全体的に見て、これらのグループの戦術やテクニック、手段は極めてよく似ています。まず、脆弱なサーバーやスピアフィッシングメールを通じて、標的とした組織をマルウェアに感染させます。次に、標的のネットワークに恒久的な足がかりを確立して、その企業の重要なリソースを特定し、暗号化してから、復号と引き換えに身代金を要求します。このような類似点のほか、一部のグループは独自の機能も持っています。

たとえば、PetrWrapは、標的型ランサムウェア攻撃で独自のツールを使っています。PetrWrapの主な標的は、ネットワークノードが多数ある大企業です。標的の選択は慎重に行われます。これは、PetrWrapの攻撃が長期にわたるためで、最大6か月もネットワーク内に居座ったといった事例もありました。

もう1つの事例は、Mambaグループによる攻撃です。このグループは、オープンソースソフトウェアであるDiskCryptorを基に、独自の暗号化マルウェアを使用しています。攻撃者たちは標的のネットワーク内に足掛かりを得ると、Windowsのリモート制御用の正規ツールを使用して、暗号化型ランサムウェアをインストールします。このアプローチは、標的となった組織のセキュリティ担当者からは怪しまれません。Kaspersky Labのエキスパートは、1つの端末の復号につき最高1ビットコイン（2017年3月末の時点で約1,000米ドル）の身代金を要求したケースに遭遇したことがあります。



WannaCryの大流行

2017年5月中旬、暗号化型ランサムウェアWannaCryが世界的に猛威をふるいました。今回の調査対象期間には該当しませんが、本レポートからは外せないインシデントのためご紹介します。

WannaCryの感染は、世界規模で発生しました。攻撃の検知総数は、わずか1日のうちに45,000件を超えましたが、実際の件数はこれをはるかに上回っています。

最初の1週間の攻撃を検知した端末台数を時系列で表すと、脅威に対抗するサイバーセキュリティの影響力がわかります。

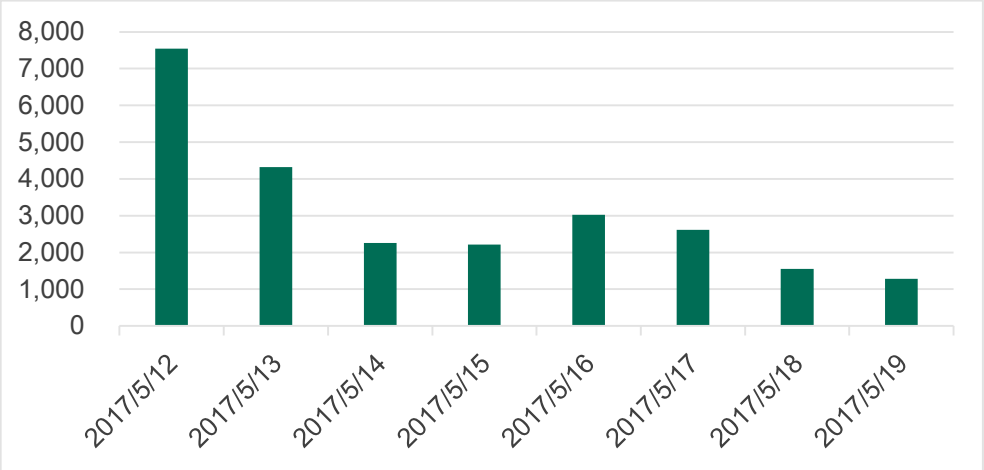


図12：2017年5月12～19日の間に、WannaCryの攻撃を検知した端末台数

攻撃の多くはロシアで起きていますが、ウクライナ、インド、台湾でもWannaCryによる攻撃も検知しています。Kaspersky Labでは74か国でWannaCryを発見しました。以下の図12は攻撃発生初日のデータです。

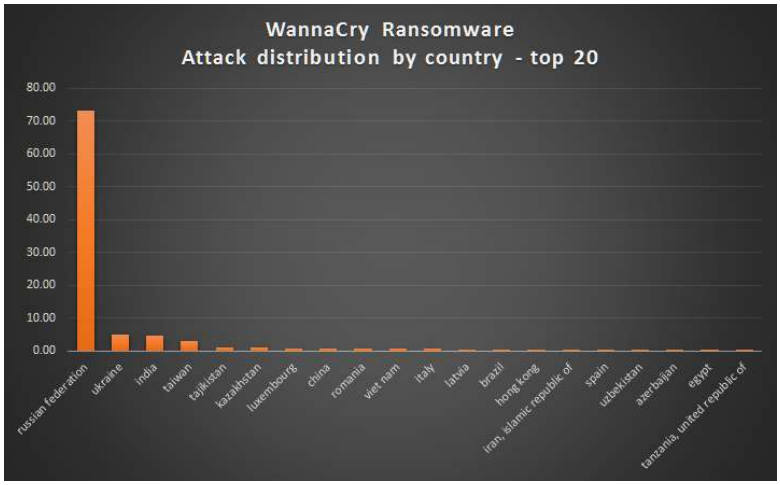


図13：WannaCryの攻撃を検知した国

一般的に、WannaCryは2段階で実行されます。第1段階では、感染と感染拡大のためのエクスプロイトが利用されます。その後、第2段階として暗号化型ランサムウェアが感染先の端末にダウンロードされます。

WannaCryには、ほかの大多数の暗号化型ランサムウェアとは異なる特徴があります。一般的な暗号化型ランサムウェアが端末に感染するには、不審なリンクをクリックする、悪意あるマクロが仕組まれたWordファイルを開く、怪しいメールの添付ファイルを実行するなど、ユーザー側でのアクションが必要です。WannaCryの場合、このような操作は一切必要ありません。

WannaCryは、Microsoft Windowsの脆弱性を悪用するEternalBlueと呼ばれるエクスプロイトを使用します（この脆弱性は、2017年3月15日（日本時間）のセキュリティ更新プログラムで修正されています）。EternalBlueを使えば、標的の端末にリモートアクセスして暗号化型ランサムウェアをインストールすることが可能です。

Microsoftの脆弱性の重要性を考慮して、最初の1週間で攻撃を検知した、Windows XP、7、およびWindows 10の割合の変化を分析したところ、興味深い結果が得られました。

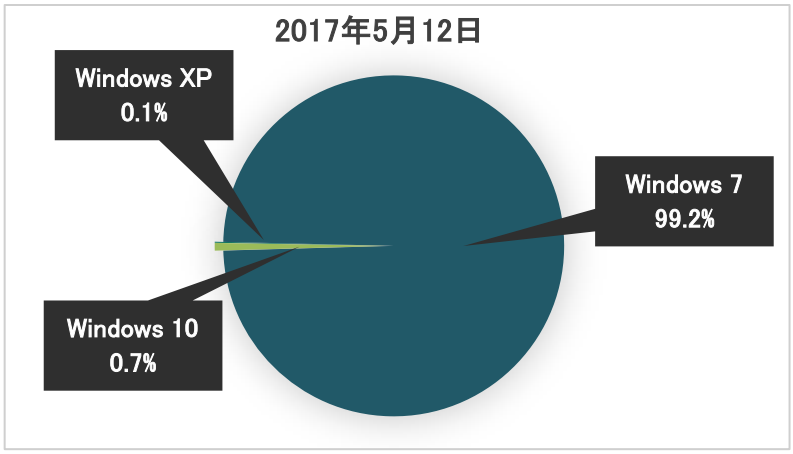


図14：2017年5月12日時点で攻撃を検知したWindows XP、7、およびWindows 10の割合

この図が示すように、初日の5月2日に攻撃を受けたプラットフォームの中で、Windows 7が圧倒的に高い割合を占めていました。

その翌週5月19日時点では、状況はやや変化しました。Windows 7は相変わらず1位を維持していましたが、Windows 10の割合が6%に増加し、初日の0.7%から8.4倍になりました。

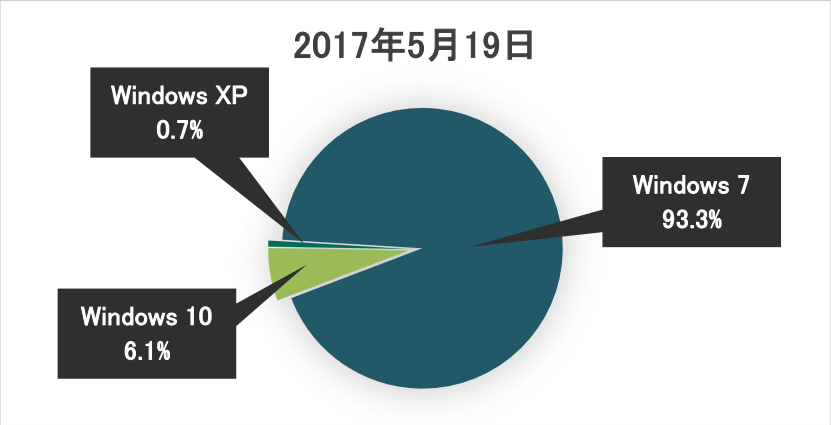


図15：2017年5月19日時点で攻撃を検知したWindows XP、7、およびWindows 10の割合

端末への感染に成功すると、WannaCryはコンピューターワームのように、ネットワークを通じてほかの端末へと感染を広げます。WannaCryはEternalBlueを悪用して、さらに侵入できる端末を探索します。同じ脆弱性を抱えた端末を見つけると、攻撃を仕掛け、そこに保存されているファイルを暗号化します。

1台の端末に感染したWannaCryは、LAN全体に感染を広げ、そのネットワーク上にある端末のファイルをすべて暗号化することができます。つまり、ネットワーク上にある端末の数が多いほど、被害の規模が大きくなります。これがWannaCryの攻撃で大企業が最も被害を受けている理由です。

暗号化型ランサムウェアとしてWannaCry（WCrypt、Wanna Decryptorと呼ばれることもあります）は、ほかの暗号化型ランサムウェアと同様、端末にあるファイルを暗号化し、復号と引き換えに身代金を要求します。WannaCryは、悪名高いCryptXXX の亜種の一つとよく似ています。

WannaCryは、Office文書、画像、動画、圧縮ファイルほか、重要なユーザーデータを含む可能性のあるファイル形式を含む、さまざまなタイプのファイルを暗号化します（影響を受けるファイル形式の一覧については、こちらをご確認ください）。暗号化されたファイルの拡張子は「.WCRY」などに変更され、ファイルは開けなくなります。

ファイルを暗号化した後、続けて感染に関する情報と、ファイルを取り戻すために取るべき行動を記載したウィンドウを表示します。さらに、同じ内容の文章が書かれたテキストファイルを端末にあるすべてのフォルダーに保存して、感染者がこのメッセージに気づくようにします。

図16：WannaCry、日本語の脅迫文の一部

一般的なランサムウェアと同様、ある一定の金額を身代金としてビットコインで犯人の口座に送金することで、すべてのファイルを復号すると犯人は主張しています。

最初に要求された身代金は300ドルですが、一定期間を過ぎると、自動的に600ドルに引き上げられます。

Kaspersky Labのエキスパートがこのランサムウェアについて詳しく調査したところ、WannaCryの開発者はさまざまな間違いを犯しており、コードの品質は極めて低いことがわかっています。WannaCryに感染した場合でも、データ／ファイル復元ソフトを使って、暗号化されたファイルの多くを復元できる可能性があります。

パート2：モバイルを狙うランサムウェア 統計

2016年度にモバイルランサムウェアの攻撃を検知したAndroid端末は130,232台で、前年の136,532台から4.6%減少しています。

モバイルを狙うランサムウェアの活動は急速に激しさを増し、2017年初めに報告されたトロイの木馬の機能を持つモバイルランサムウェアのインストールパッケージ数は218,625に及びました。これは2016年第4四半期（2016年9月～12月）の3.5倍です。その後、活動は鎮静化し、過去2年間の平均レベルに戻りました。

2014年度（2014年4月から2015年3月）、カスペルスキー製品は35,413台のAndroid端末をモバイルランサムウェアから保護しました。2015年度に保護したAndroid端末は136,532台で、3.8倍に増加しました。その主な原因は、Fusobランサムウェアの活動で、特にドイツでの攻撃回数が増加していましたが、その活動は急速に衰え、2016年4月の24,061から2016年9月には7,855にまで減少し、その傾向は、残りの期間も続きました。しかし、2016年12月は唯一の例外で、14,274台まで増加しています。これは、Svpengファミリーの攻撃が通常の3倍以上に増加したことが原因でした。

マルウェアによる攻撃を検知したAndroid端末のうち、ランサムウェアの攻撃を検知した割合もやや変化し、2014年度の2.0%が2015年度には4.6%に上昇しましたが、2016年度には2.8%に低下しています。このような傾向は、Windowsを狙ったランサムウェアにも見られます。これは、マルウェアの総数が、ランサムウェア攻撃の数よりも急速に増加していることを表します。

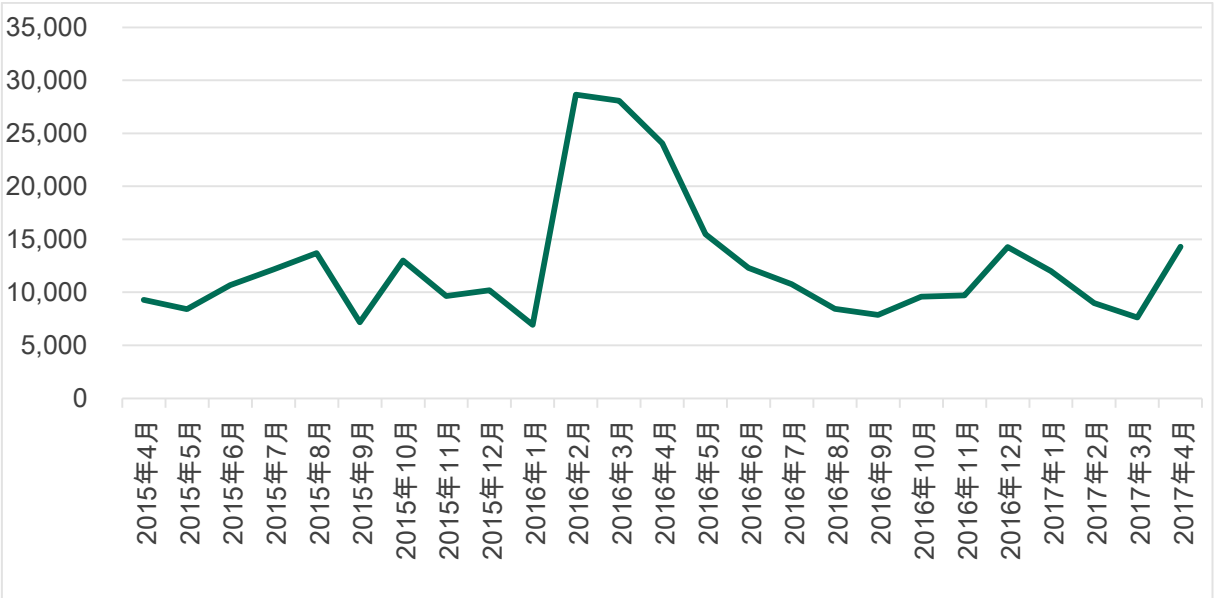


図17：2015年4月～2017年3月に、1回以上モバイルランサムウェアの攻撃を検知したAndoroid端末台数

モバイルランサムウェアの地理的分布は、Windowsを狙ったランサムウェアとはかなり異なります。これは、大規模なランサムウェアファミリー「Fusob」が、ヨーロッパ、カナダ、米国を重点的に攻撃しているのに対し、もう1つの大型ランサムウェア「Small」は主にCIS諸国を標的にしているからです。

	国名	トロイの木馬の機能を持つランサムウェアの攻撃を検知した割合(%)
1	ドイツ	22.9%
2	カナダ	19.6%
3	英国	16.1%
4	米国	15.6%
5	カザフスタン	14.4%
6	イタリア	12.5%
7	オランダ	12.3%
8	スペイン	5.3%
9	ロシア	4.9%
10	ウクライナ	4.6%

図18: 2015年4月～2016年3月に、モバイルマルウェアによる攻撃を検知したAndroid端末のうち、トロイの木馬の機能を持つランサムウェアに分類されるマルウェアの攻撃を検知した割合が高い上位10か国
(対象:Android向けのカスペルスキー製品のユニークユーザーが5,000人を超えている国)

トップはドイツ(22.9%)で、以下、カナダ(19.6%)、英国(16.1%)、米国(15.6%)と続きます。

これらの国が上位にランキングされているのは、経済力のある先進国では、収入のレベルが高いだけでなく、先進的なモバイルデバイスや電子決済が広く普及していることも理由として挙げられます。このような国では、数回のタップやクリックだけで身代金を送金できるため、資金回収率が高く、犯罪者にとっても魅力的であると考えられます。

2016年度、このランキングに登場する国の順位とランサムウェアに攻撃されたAndroid端末の割合の両方に大きな変化がありました。しかし、この変化の影響を受けたのは、ほとんどが下位にランク付けされる国で、上位3か国にはあまり変化はみられません。

	国名	トロイの木馬の機能を持つランサムウェアの攻撃を検知した割合（%）
1	米国	18.7%
2	カナダ	18.0%
3	ドイツ	15.5%
4	英国	13.4%
5	イタリア	11.9%
6	カザフスタン	6.8%
7	スペイン	6.4%
8	メキシコ	5.9%
9	ウクライナ	2.0%
10	ロシア	0.9%

図19：2016年4月～2017年3月に、モバイルマルウェアによる攻撃を検知したAndoroid端末のうち、
トロイの木馬の機能を持つランサムウェアに分類されるマルウェアの攻撃を検知した割合が高い上位10か国
（対象：Android向けのカスペルスキー製品のユニークユーザーが2,500人を超えている国）

この期間に検知されたトロイの木馬の機能を持つランサムウェアの数は世界全体で大きく減少しています。現状を正確に把握するため、Android向けのカスペルスキー製品のユニークユーザーが2,500人を超えている国まで対象を広げました。

米国の順位が4位から1位に上がりましたが、カナダとドイツは上位3位内にとどまっています。米国の順位が上がったのは、主にSvpengとFusobの攻撃が原因です。Svpengの主たる標的は米国で、そのほかの地域への攻撃は全体の3%にすぎませんでした。Fusobは、当初、ドイツに重点を置いていましたが、2017年第1四半期以降、攻撃の28%が米国に向けられ、ドイツの割合は24%になりました。米国に注目が集まるようになったのは、iTunesカードやMoneyPakなど、匿名での支払い手段が普及したことが原因と考えられます。

ロシアの急降下は、マルウェア攻撃が全体的に増加すると同時に、その地域でのランサムウェア攻撃が減少したことで説明できるでしょう。Smallによる攻撃の規模も、大きく縮小しています。

主なモバイルランサムウェア

本レポートの全調査対象期間にわたり、Kaspersky Labのエキスパートは、カスペルスキー製品を利用するAndroid端末が頻繁に遭遇するモバイルランサムウェアファミリーをいくつか特定しました。2014年度には、Pletor、Fusob、Svpeng、Smallを特定しました。2015年度に最も検出回数の多かったトロイの木馬の機能を持つモバイルランサムウェアはFusobで、世界100以上の国で攻撃が確認されました。「Trojan-Ransom.AndroidOS.Fusob」の初の事例は、2015年1月初めにKaspersky Labのエキスパートが発見しました。

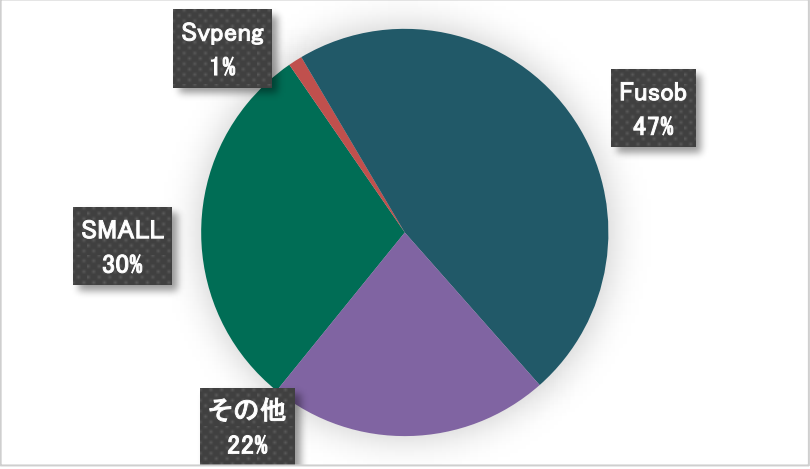


図20：2015年4月～2016年3月に、
Android端末で検知した代表的なモバイルランサムウェアファミリーの割合

Windowsを狙ったランサムウェアとは異なり、モバイルの脅威となっているランサムウェアは数種類だけで、これらが約80%の攻撃を行っていました。2016年度の状況は多少変化してきます。

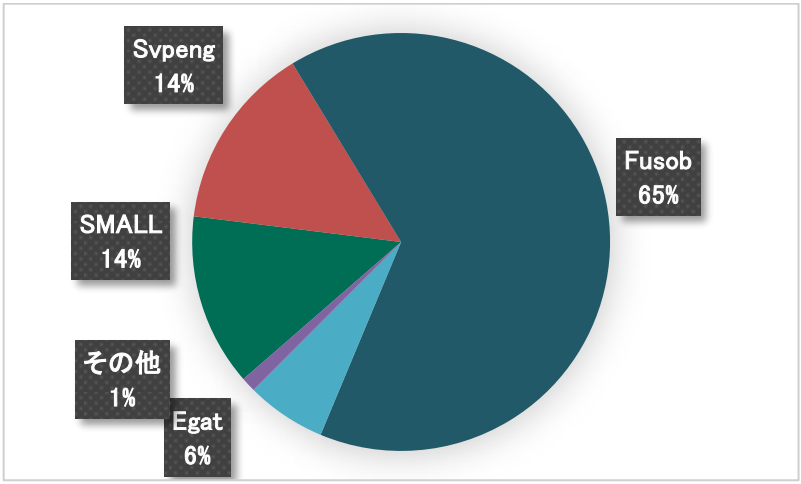


図21：2016年4月～2017年3月に、
Android端末で検知した代表的なモバイルランサムウェアファミリーの割合

「その他」が22%からわずか1%へと急落しました。その主な原因は、Fusobファミリーの拡大（47%から65%へ）とSvpengの活動再開（1%から14%へ）です。Fusobファミリーが圧倒的な割合を占めていることを前提に、この期間におけるFusobファミリーの進化を詳しく見ていきましょう。

Fusobランサムウェア

2016年前半にモバイルランサムウェアのインストールパッケージ数が増加したのは、主に、Trojan-Ransom.AndroidOS.Fusobファミリーの蔓延が原因です。2016年後半、このファミリーの活動が低下し、検知されるインストールパッケージ数にも影響が及びました。2016年第4四半期に再び増加し始め、2017年第1四半期にはさらに加速しました。

第1四半期に最も検知されたトロイの木馬の機能を持つモバイルランサムウェアは依然としてTrojan-Ransom.AndroidOS.Fusob.hで、モバイルランサムウェアに攻撃されたAndroid端末の45%近くが、このランサムウェアの被害を受けていました。このトロイの木馬の機能を持つランサムウェアは、起動されると、まず、管理者権限を要求します。次に、GPS座標や通話履歴などデバイスに関する情報を収集し、悪意あるサーバーへこのデータを転送します。その後、Android端末をロックするコマンドを受け取れるようになります。

パート3：どのように組織化していったのか

ランサムウェア市場の競争が激化している様子から考えると、RaaS（Ransomware-as-a-Service：サービスとしてのランサムウェア）の普及が、新たな犯罪者の参入に影響しています。しかし、ランサムウェア市場参入への障壁を下げているのは、これだけではありません。

過去12か月にわたり、ランサムウェアはより高度化し、多様化され、スキルやリソース、時間のない者でも手軽に使える攻撃サービスが多数提供されるようになりました。そのような攻撃サービスが流通するアンダーグラウンドのエコシステムも拡大し、さらに効率が上がっています。

今や、攻撃者や犯罪グループは、特別な努力をしなくても独自の暗号化型ランサムウェアを簡単に作成できます。オープンソースのDiskCryptorツールを基に作成されたMamba暗号化型ランサムウェアは目を見張る事例の一つです。中には、このようなツールを利用する際、プログラマーを動員して技術的に改良する手間すらかけず、そのまま使用しているサイバー犯罪グループもあります。

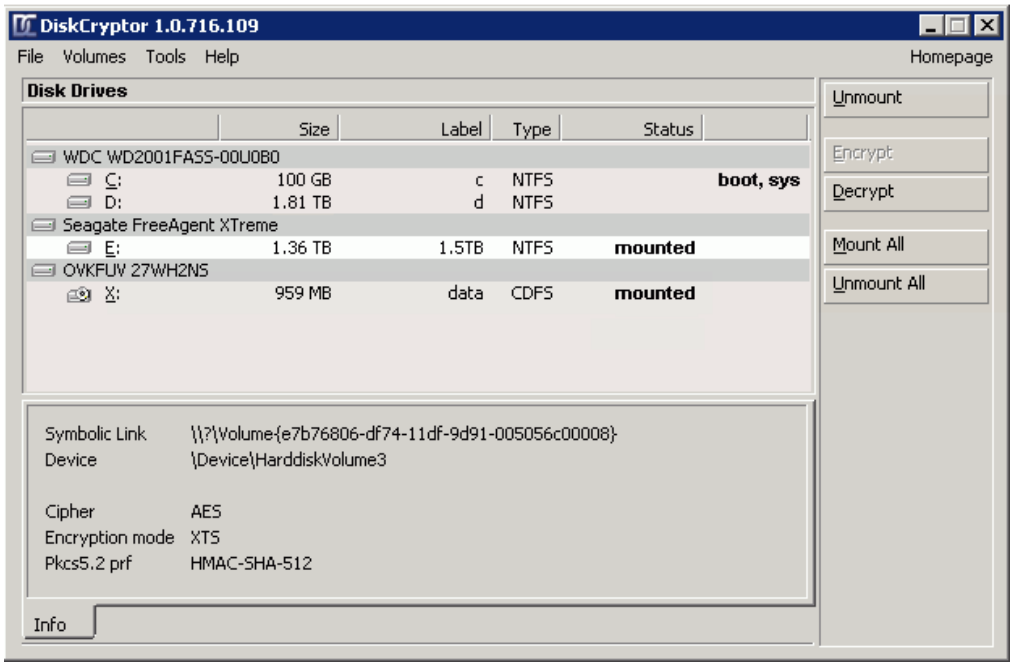


図22：Disk Cryptorツール

その主な理由は次の3つです。

- アンダーグラウンド市場でランサムウェアのマルウェア生成ツールが簡単に購入できる
- 配信サービスを簡単に購入できる
- ビジネスとしての暗号化型ランサムウェアが、仮想通貨を利用した極めて明瞭な収益化モデルを持っている

言うなれば非常に整備され利用しやすく、常に発展を続けるエコシステムとも言えます。Kaspersky Labでは過去数年間、このエコシステムの発展を調査し続けてきました。

アンダーグラウンドの暗号化型ランサムウェア市場で取引されている、違法なランサムウェア「ビジネス」への参入方法は次の3つです。

- 販売用に新たなランサムウェアを開発する
- ランサムウェア“アフィリエイトプログラム”の共犯者になる
- “アフィリエイトプログラム”の所有者になる

- 販売用の新たなランサムウェアの開発

  この参入方法では、暗号に関する深い知識や、コードを記述するための高度なスキルが必要です。このカテゴリに分類される犯罪者は、銃を取引する商人のようなもので、実際の攻撃には通常は参加しません。ただコードを売るだけです。マルウェアの作者が、自分の「製品」にすべてのソースコードをつけて固定価格（通常、数千ドル）で売っているのを見かけることがあります。また、生成ツール（プログラミング経験のない犯罪者が、特定の機能を持った暗号化型ランサムウェアを生成できるようにするツール）を売っていることもあります。

- ランサムウェア“アフィリエイトプログラム”の共犯者になる

  ランサムウェアの生成ツールは、通常数百ドル程度と、ランサムウェアのソースコード全体を購入するよりも格安です。しかし多くの場合、このようなソフトウェアを利用してマルウェアを生成するたびに、料金が請求されます。

  マルウェアを生成するたびに課金されるシステムは、ランサムウェア開発者が使用する新しいタイプの収益モデルです。価格は数十ドル程度とさらに安くなりますが、購入者が手に入れるのは、機能が制限されたマルウェアです。

- “アフィリエイトプログラム”の所有者になる

  ランサムウェアを使った犯罪ビジネスへの参入方法の3つめ、アフィリエイトプログラムはサイバー犯罪では標準的な手口です。プログラムの所有者が、感染に必要なツールすべてを共犯者に提供し、共犯者はマルウェアを拡散します。マルウェア感染が成功すればするほど、得られる収入も増えます。違法行為を行う覚悟と、参加費用（2～3ビットコイン）があれば、このようなプログラムに簡単に参加することができます。

これとは対照的に、高度なサイバー攻撃にはだれでも参加できるわけではありません。アフィリエイトプログラムの参加者から個人的に推薦を受ける必要があります。さらに参加するためには、一定レベルのマルウェア配信能力を証明しなければなりません。昨年、調査していたあるケースでは、参加希望者は4,000台以上の標的の端末に対してマルウェアをダウンロードおよびインストールさせて、実力を証明しなければなりませんでした。その代わりに、共犯者にはセキュリティ製品に検知されにくくする難読化ツールが無料で与えられ、コンバージョン率も最大3%と正規のアフィリエイトプログラムと比べて、非常に良い条件になっています。

要約すれば、柔軟性こそがアンダーグラウンドでのランサムウェアエコシステムの主要な特徴です。犯罪行動に手を染めてしまう傾向の人々に多くの機会を提供します。その人が、どの程度のIT経験を持っているかはほとんど関係ありません。

結論と予測

本レポートで調査したデータと傾向に基づいて導き出された結論は次のとおりです。

- ランサムウェアを使う犯罪者は、互いにつぶし合いを始めました。これは、ランサムウェア犯罪グループ同士の競争が激化していることを表しています。
- 地理的分布は、攻撃者の標的が、ランサムウェア対策があまりできておらず、犯罪者間での競争がそれほど厳しくない国に切り替わったことを示しています。
- 標的型ランサムウェア攻撃がますます増加し、世界中の金融インフラが襲われています。犯罪者は、個人ユーザーへの大規模攻撃よりも、標的型ランサムウェアで企業を攻撃する方が、より多くの利益を見込めると考えているためです。
- 伸び率が悪くなっているとはいえ、Windowsを狙ったランサムウェアが依然として増え続けています。
- 調査対象期間中にモバイルランサムウェアの攻撃を検知したAndroid端末の台数は減少しています。これは、セキュリティベンダーや司法当局などの関係者が共同で実施した対抗措置が成功した証だと思われます。大規模な攻撃を世界中のメディアが報道したことにより、サイバー脅威に対する世間の関心が高まったことも一役買っているでしょう。
- 暗号化型ランサムウェアからユーザーを守るために、業界が連携して行った取り組みが発展したことも理由の1つです。
- 統計は、ランサムウェアを使った攻撃が大規模に行われたことを示していますが、モバイル攻撃の大半は、ごく少数のマルウェアグループによって担われており、そのほとんどがアフィリエイトプログラム経由で拡散されています。一方、Windowsを狙うランサムウェアは違っており、野放しにされている多数の犯罪者が、場当たり的に攻撃を行っています。

以上の結論とランサムウェアの脅威の現状は、この脅威が将来どのような展開を見せるか、その予測を可能にする根拠を提供していると思われます。

予測:

- 身代金を要求するランサムウェアのモデルは今後も定着します。平均するとやや高い水準を維持した成長率は、憂慮すべき傾向かもしれません。これまでは、犯罪者が脅威の勢力図に加わるための足がかりを築くために、秩序なく、散発的に行っていましたが、今後は一定のペースを保った大量攻撃へ変化する可能性があります。
- ランサムウェア市場の競争が激化している様子から考えると、RaaSがさらに普及し、新たな犯罪者の参入に影響を与えるでしょう。
- ランサムウェアはより高度化し多様化され、スキルやリソース、時間が無くても手軽に使える攻撃サービスが多数提供されるようになります。そのような攻撃サービスが流通するアンダーグラウンドのエコシステムも拡大し、さらに効率が上がっています。
- 犯罪者間のインフラが発展することで、標的型攻撃の実行や、金銭を窃取するために簡単に使えるツールの出現が進み、攻撃の範囲がさら広がります。この傾向はすでに確認されており、このまま続くと見ています。
- 暗号化型ランサムウェアからユーザーを保護する世界的な取り組みは、ますます勢いを増していくでしょう。

Kaspersky Labが提供する対抗措置

- **テクノロジーを通じて**

ランサムウェアから企業や組織を守るための補完的なセキュリティ機能を提供する無料のツール「Kaspersky Anti-Ransomware Tool for Business」を提供しています。既にインストールされている他社セキュリティ製品をアンインストールすることなく使用できます。

- **コラボレーションを通じて**

「No More Ransom」プロジェクト

2016年7月25日、オランダ警察、欧州刑事警察機構（ユーロポール）、Intel Security、Kaspersky Labは、No More Ransomプロジェクトを開始しました。これは公共団体と民間団体が協力して、ランサムウェアの危険性を人々に知らせ、データの復元を支援することを目的とした非営利的な活動です。

現在50種類の復号ツールが公開されており、そのうち7種類はKaspersky Labによって開発されたものです。既に全世界の29,000人以上の人々が、Kaspersky Labの復号ツールを活用して、金銭を支払うことなくファイルのロックを解除しています。

「No More Ransom」のポータルサイトは現在、イタリア語、ウクライナ語、オランダ語、スペイン語、スロベニア語、ドイツ語、フィンランド語、フランス語、ヘブライ語、ポルトガル語、英語、韓国語、日本語、の14か国語に対応しています。

ランサムウェアの感染リスクを低減するためのKaspersky Labからの推奨事項

1. 定期的にデータをバックアップする。
2. 信頼できるセキュリティ製品を使用し、「システムウォッチャー」など振る舞い検知機能を忘れずに有効化する。
3. 使用しているすべてのデバイスで、OSやソフトウェアを常に最新の状態に保つ。
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の取り扱いには十分注意し、不審な場合には開かない。
5. 企業や組織では、従業員やITチームの教育を継続的に実施する。機密データはその他のデータから隔離し、アクセスを制限する。
6. 万が一、暗号化型ランサムウェアに感染した場合は、復元ツールを確認する。「No More Ransom」のポータルサイトでは、最新の情報が確認できます。アクセスする場合は、マルウェアに感染していない端末からご利用ください。
7. Kaspersky Labでは、ランサムウェア対策機能を備えた小規模オフィス向けセキュリティ製品「カスペルスキー スモール オフィス セキュリティ」や、既にインストールされているセキュリティ製品に関係なく使用できる無料の補助ツール「Kaspersky Anti-Ransomware Tool for Business」の提供など、あらゆる企業や組織が使用できるランサムウェア対策を提供しています。
8. 攻撃を確認したら最寄りの法執行機関に通報してください。ランサムウェアによる攻撃は犯罪です。

身代金を支払うべきではない理由

- 身代金を払っても、データが戻ってくる保証はありません。
- さらに標的にされる可能性があります。
- 次に標的になったとき、身代金がさらに高額になる可能性があります。
- 犯罪者を経済的に助け、結果的に犯罪の片棒を担ぐことになります。

ランサムウェアとの闘いに勝てるのでしょうか？

勝てます。ただし、みなさんの協力が必要です。ランサムウェアは、収益の大きな犯罪ビジネスです。これを阻止するには、世界が1つになって犯罪者の活動を妨害し、攻撃から収益をあげられないようにする必要があります。

株式会社カスペルスキー
PR-1040-201707