
変化を続ける
ランサムウェア
F-Secure

目次

ランサムウェアとは何か

ランサムウェアは悪意を持ったアプリケーションの一種で、ユーザーのマシンまたはデータの制御権を奪ってアクセスできないようにした上でそのマシンまたはデータを元に戻すために身代金を支払うよう要求します。ランサムウェアによる被害はここ数年で急増していますが、これはオンラインでの強請（ゆすり）に他なりません。

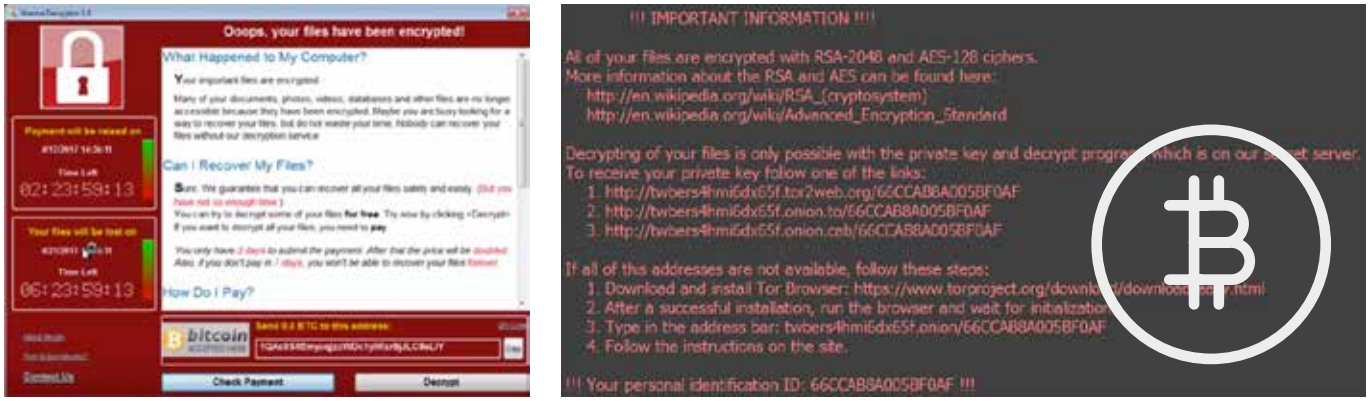

図 1: WannaCry（左）およびLocky（右）が表示する身代金要求画面

ランサムウェアは誰を狙っているのか

ランサムウェアは昔からありますが、最近の2年間で被害が急速に拡大しており、今では個人および企業にとって無視できない脅威になっています。従来は、ランサムウェアを使った攻撃は場当たり的で、スパムメールやエクスプロイトキット、マルバタイジングなどを使って手当たり次第にばらまいていました。しかし最近では、多くのサイバー攻撃者が意図的に企業や組織を狙うようになっています。

通常身代金の金額はデバイスの数によって決まるため、企業や組織を狙うほうが個人を狙うよりも稼ぎが良いためです。エフセキュアが2016年に5つのランサムウェアファミリーについて行った調査では、最初に請求される身代金の金額は$150-$1,900（ビットコインによる支払いが可）でした。[1] 個人のデバイスを狙っても、復号化のためのコストはせいぜい数百ドルにしかなりませんが、企業や組織が相手であれば、攻撃者は数万ドルの利益を得ることもできるのです。

さらに、ランサムウェアに感染することは往々にして企業や組織のビジネス上の利益を毀損するため、犯罪者にとっては身代金を請求しやすいという側面もあります。

多くの場合、ITシステム上のドキュメントやデータベース無しでは企業や組織は運用できません。また、被害者の中には、顧客から提供されたデータを管理し守る法的責任を負っていた事例もいくつかありました。

これらの理由から、ランサムウェアの被害が起きた場合、企業や組織には迅速かつ極秘に問題を解決しなければならないというプレッシャーが生じ、その結果身代金を支払ってしまうのです。

いくつかの調査によると、多くの企業や組織が実際に身代金を支払っているということです。オーストラリアのテレコム企業であるTelstraの調査によると、アジア太平洋地域の企業や組織の約57%がランサムウェアの被害に対して支払いを行っています。[2] 2016年に公表された同様の調査では、70%の企業が支払ったということです。

しかし、控えめな推定もあり、2018年の調査によると、身代金を支払ったのは約40%の企業や組織であるということが分かりました。(データを復旧できたのは、そのうちの半分程度でした)[4]

身代金がどのくらいの頻度で支払われているかを正確に知ることは難しいかもしれませんが、「ランサムウェア業界」は、今や企業に数十億ドルの損害を与えていると推定されています。[5] 成功しているランサムウェアファミリーの中には、数百万ドルから数千万ドルもの利益を生み出すものもあります。[6] これらの数値は、ランサムウェアのビジネスモデルがオンライン不正行為の方法として有効であることを示しており、この脅威が過去2年間にこれだけ流行した理由を十分に説明できます。

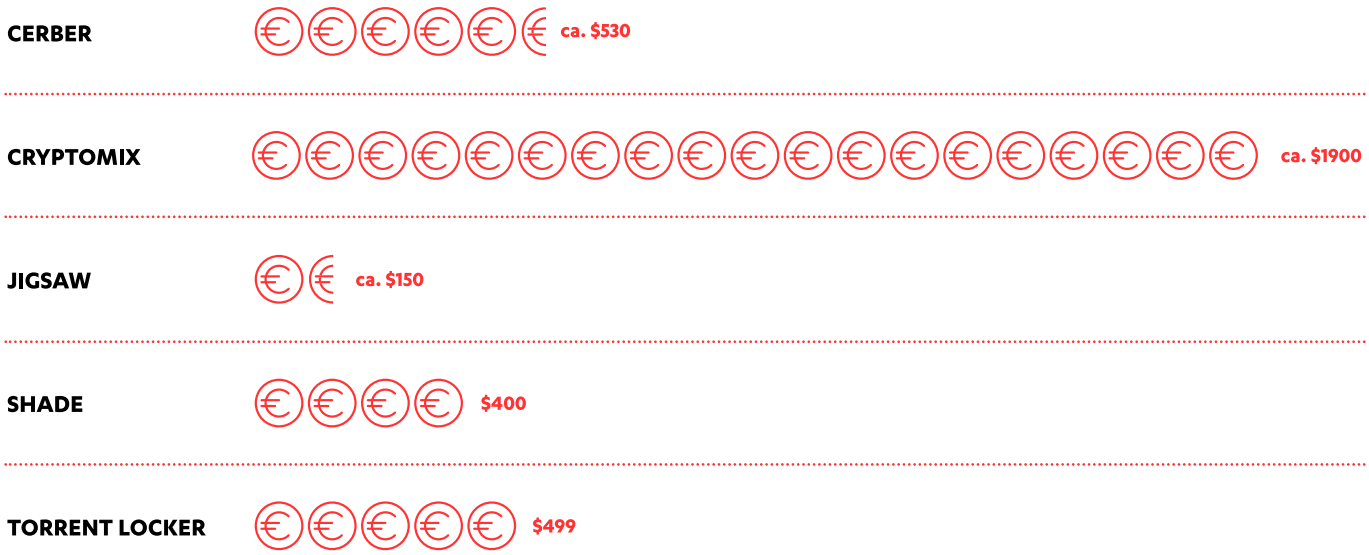

図 2: エフセキュアが2016年にランサムウェアの被害者の「カスタマージャーニー」を調査したところ、最初に提示される身代金の額は150ドルから1900ドルでした。(ビットコインで支払い可能)

ランサムウェアの歴史

ランサムウェアは1989年から存在していますが、ここ数年はサイバー犯罪者が使用するランサムウェアファミリーの数と攻撃の数がどちらも着実に増加しています。2012年に発見されたランサムウェアファミリーは1つだけでしたが、2016年には新しいランサムウェアファミリーまたは亜種がおよそ200種類も発見されました。2017年には、343種類の新しいランサムウェアが発見されました。これは前年より62%の増加です。

異なるランサムウェアファミリーは異なる特徴を持ち、それが実効性に影響するため、ユニークな亜種やファミリーがどれだけあるかは防御側にとって重要です。たとえば、多くのランサムウェアファミリーはCryptomixのように期限を設定することで被害者にプレッシャーを与え、支払いをさせようとしますが、そのうちのいくつかは（JigsawやBitKangorooなど）一定の間隔で選択的にファイルを削除することで、さらに支払いへのプレッシャーをかけます。

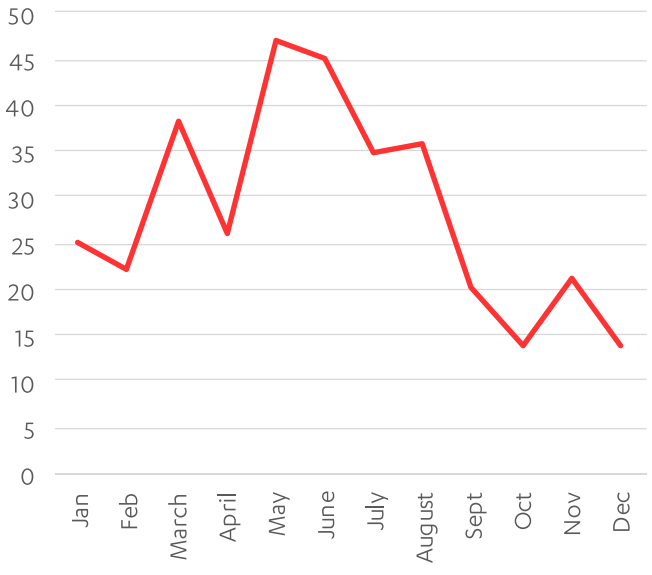

図 4: 2017年の月別のユニークなランサムウェアファミリーおよび亜種の数

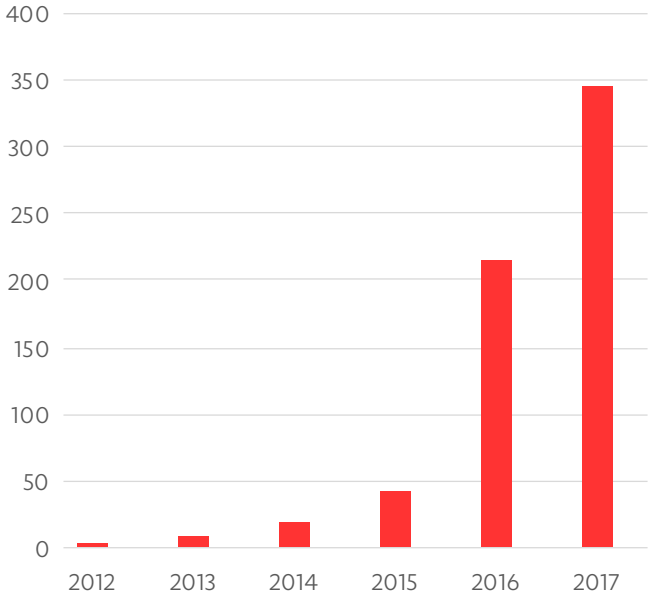

図 3: 年毎のユニークなランサムウェアファミリーおよび亜種の数

攻撃者側の人気が高いことに加えて、ランサムウェアが劇的に進化した理由の1つは、サイバー犯罪者が積極的にサポートしたことです。CerberやSatanのようなRansomeware-as-a-Serviceと、HiddenTearやEDA2などのオープンソースプロジェクトを利用できるようになったために、独自のマルウェアをゼロから開発するスキルやリソースが不足している攻撃者でも、手軽にランサムウェアを使うことができるようになりました。また、エクスプロイトキットやスパムサービスなどのサポートインフラも充実しており、これらを借りたり購入したりして、すぐに利用できます。

トレンドを前年と比較してみると、ユニークなランサムウェアファミリーと亜種が明確に増加しています。しかし、2017年を詳しく見てみると、これらの活動は実際には年末にかけて減少し始めています。この傾向が続くかどうかはわかりません。一方で、様々な種類のランサムウェアのうち攻撃に関与しているのは一握りのファミリーだけです。

数字で見るランサムウェア攻撃

エフセキュアラボのアップストリームテレメトリーデータから生成されたランサムウェア検出レポートによると、2015年以降急激にランサムウェア攻撃が増加しています。2017年にはランサムウェア検出レポートの件数が前年比で415%増加しましたが、これは2017年5月に起きたWannaCryのアウトブレイクによるものです。このアウトブレイクは、ワームに似た感染方法と、ほぼすべてのバージョンのWindowsに存在する脆弱性の悪用により起きたのです。[7]

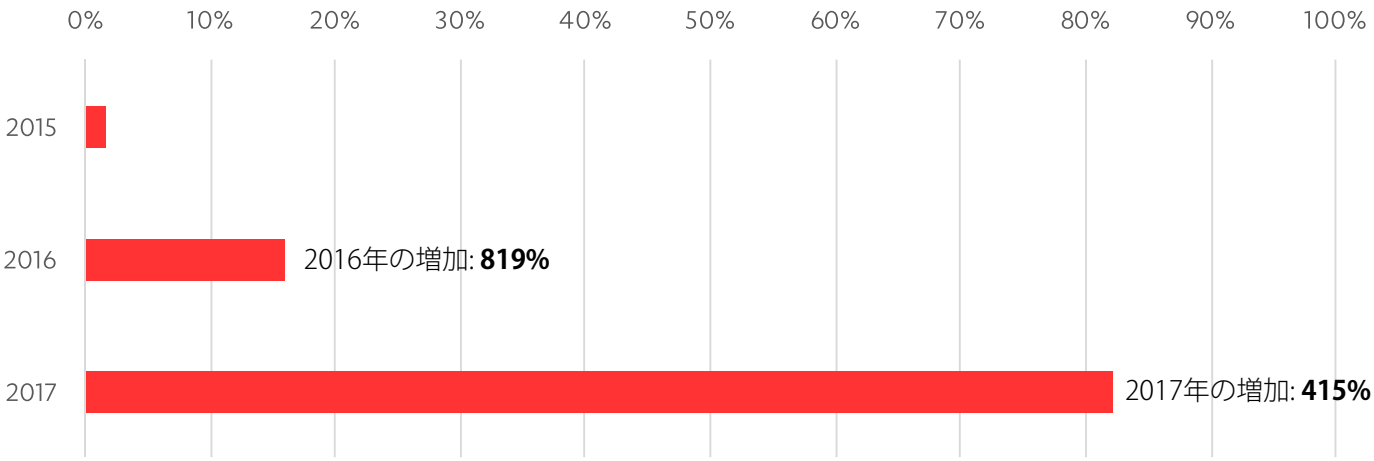

図 5: ランサムウェア検出数が全体に占める割合の推移（2015年から2017年）

2015	2016	2017
Browlock	Locky	WannaCry
Cryptowall	TeslaCrypt	Locky
Crowti	Cerber	Mole

図 6: 年毎のトップランサムウェアファミリー

多くの人はWannaCryで初めてランサムウェアという言葉を聞いたかもしれませんが、ランサムウェアは何年も前から増加を続けています。Lockyランサムウェアファミリーは2016年初頭[8] に登場し、ランサムウェアの拡大に大きく貢献しました。Lockyは、大規模なスパム攻撃に繰り返し使われたために2016年と2017年における主要な脅威となりました。[9] その活動は2016年7月にピークを迎え、毎時12万回のヒットを引き起こしたスパム攻撃が発生しました。これは、通常の日に見られるものよりも200%以上多かったのです。[10] Lockyは2016年のエフセキュアラボのテレメトリーからレポートされたすべてのランサムウェア攻撃の60%近くを占めました。2017年を通じて活動していましたが、2017年5月のWannaCryの出現後は急速に影を潜めました。

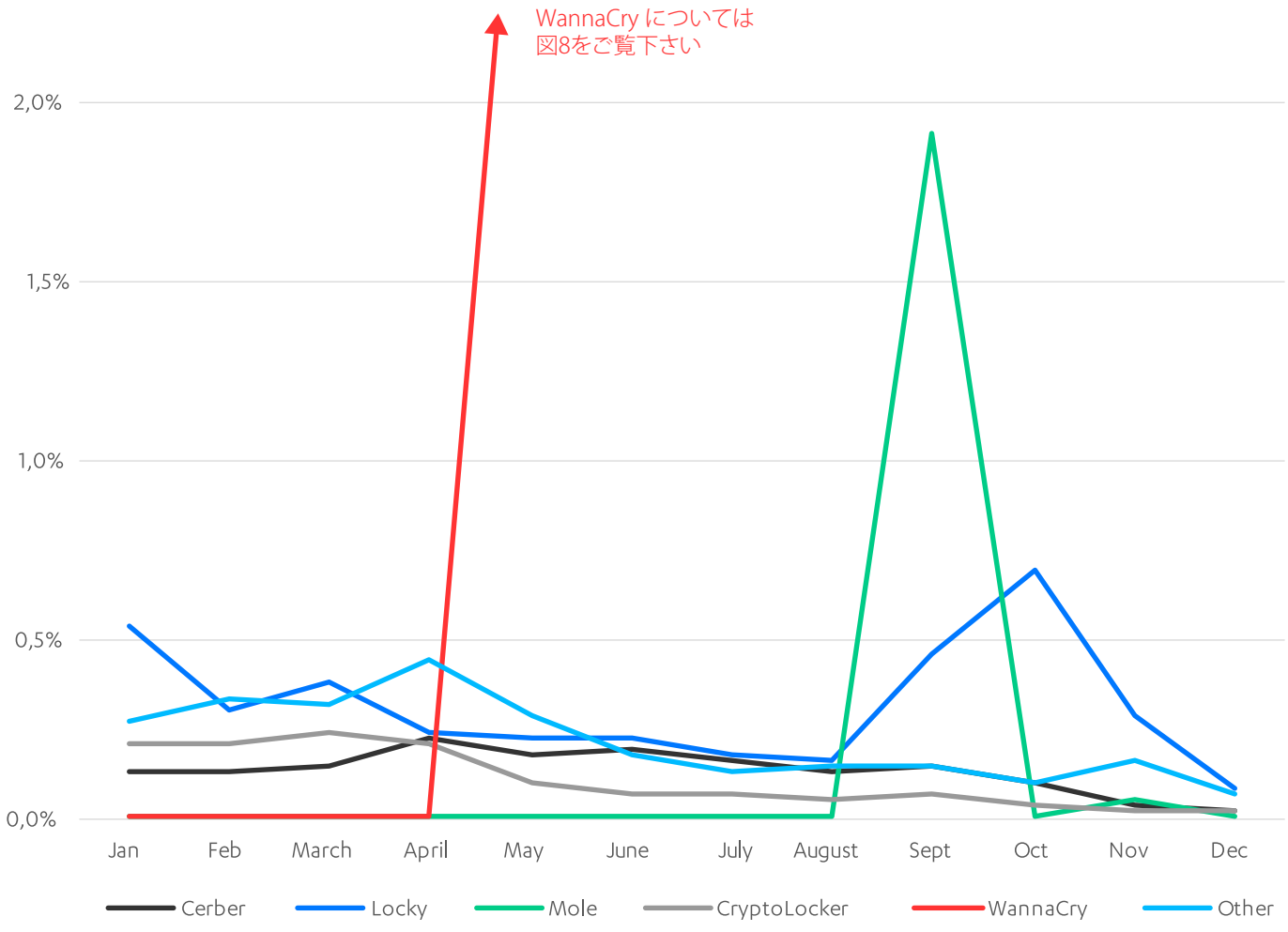

図 7: ランサムウェア検出数全体に占める特定のランサムウェアファミリーまたはユニークな亜種の数（2017年）

LockyやCerber、Cryptolockerのようなよく知られているランサムウェアファミリーは2017年に流行しましたが、時間の経過と共にその数は減少していったようです。一般的にはランサムウェア攻撃は年を追う毎に減少していきます。

LockyとMoleによる大規模な攻撃が2017年秋に検出されましたが、これらは例外的なもので、ワームに似た特徴を持つために現在も活動が続いているWannaCryもまた例外です。

このトレンドにはいくつかの要因が関係していますが、最も重要なのはビットコインの相場です。ビットコインの相場は2017年に急激に上昇[11]し、他の暗号通貨への投機も助長しました。サイバー犯罪者はこのトレンドに目を付け、仮想通貨のマイニングのためにCPUリソースを秘密裏に盗む暗号マイニングマルウェアを広めるなどして、利益を得ようとしています。[12] この企みはランサムウェアに比べてほとんど注意が払われていませんが、暗号通貨が価値を上げ続けるならば、利益を生み出すでしょう。

トレンドに影響を与える他の要因には、攻撃ベクタ（経路）としてのエクスプロイトキットの継続的な減少、ビットコイン相場の大幅な変動により身代金の請求と回収におけるロジスティクスが難しくなっていることなどがありますが、「No More Ransom Project」[13] のような業界の取り組みが存在感を増していることも関係しています。この取り組みでは、脅威に関する情報を提供し、復号化のためのツールも開発しています。

しかし最近では、ランサムウェアによる攻撃がよりターゲットを絞った方法に移行しているという兆候があります。これにより、脅威環境全体の中でランサムウェアが目立たなくなる一方で、企業にとっては依然として大きな懸念であり続けています。WannaCryは信じられないほど流行しましたが、SMBポートを介して拡散したことでその脅威が組織を狙っていたことが明らかになりました。エクスポーズされ侵害されたRDPポートを介して広がるランサムウェアはもはや珍しくなくなっており、犯罪者は標的の数ではなく脅威の品質に集中することで利益を増やすことができます。

WannaCryはDownadupの新しい形態

WannaCryは、2017年5月の世界的なランサムウェアパンデミックを起こしたファミリーで、過去最大のランサムウェアアウトブレイクとして認識されています。[14] 初期の感染は「キルスイッチ」の発見で不活性化されました[15] が、マルウェアの拡散を止めるまでには至りませんでした。

歴史的を振り返ってみると、流行したランサムウェアはスパム攻撃やエクスプロイトキット、あるいはマルバタイジングによって拡散しています。これらは場当たり的な感染で広がるため、間違ったリンクをクリックしたり悪意のある電子メールの添付ファイルを開くことで、思ってもみなかった不幸を背負いこむことになります。しかしWannaCryは、脆弱なSMBポート経由でコンピュータワームのように広がって行きます。ひとつのデバイスに感染した後に自動的にネットワークを介して拡散し、より多くのマシンに感染します。感染するホストが多くなればなるほど、拡散のスピードは速くなります。これが、昨年5月の感染が非常に速い速度で多くの組織に広がった理由です。

ワームを完全に根絶することは難しく、マルウェアをホストする少数のマシンが周囲のネットワークに繰り返し感染することで、組織にとって大きな問題が発生します。10年前に最初に発見されたDownadup/Conficker ワームがいまだに年間何百万台ものデバイスに感染しているのは、これが理由です。[16]

下の図に見られるように、エフセキュアのアップストリームテレメトリーデータにおいて、WannaCryは他のすべてのランサムウェアファミリーを圧倒しています。この年のランサムウェア検出レポートのうち、9割がWannaCryでした。

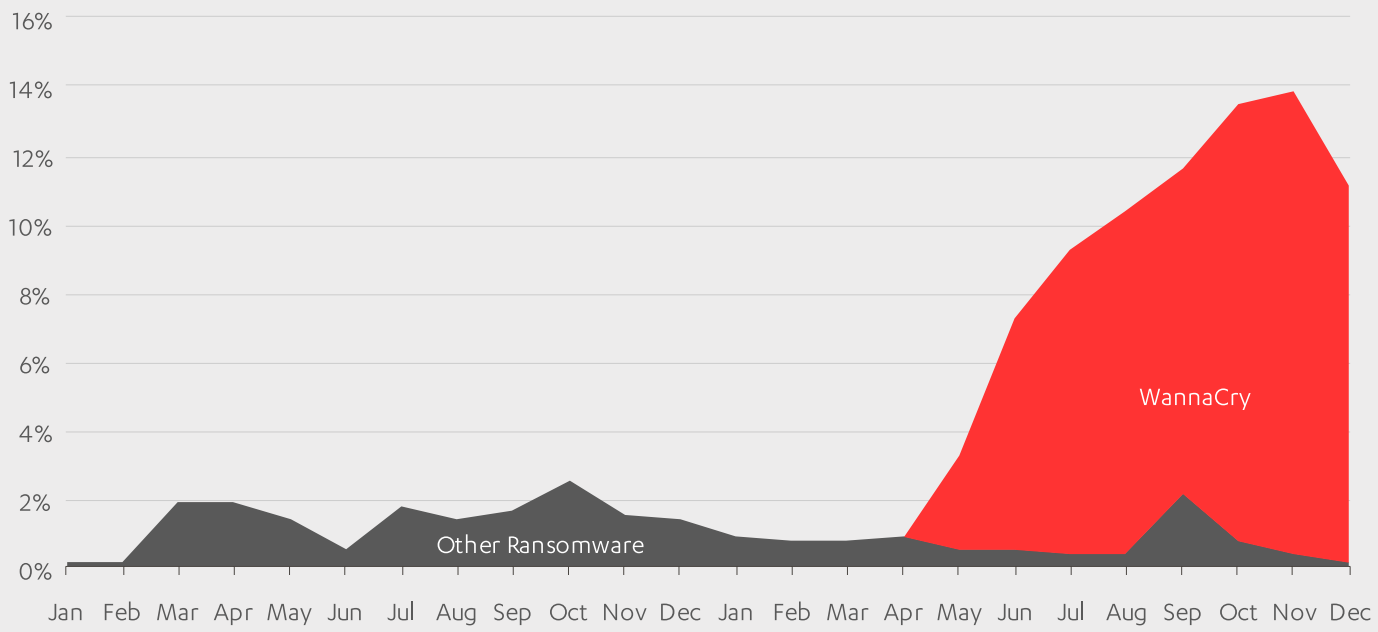

図 8: 全ランサムウェア検出数に対する割合をベースにしたWannaCryとその他のランサムウェア検出レポートの比較（2016年-2017年）

WannaCryの活動がまだ続いていることも驚きですが、5月のアウトブレイクの後の数ヶ月間にこのマルウェアのさまざまな亜種が流通し始めたことに注意することが重要です。WannaCryの亜種のいくつかは、ファイルを実際に暗号化せずにWannaCryの感染方法だけを利用したために、被害者は深刻な影響を受けませんでした。しかし、これらの亜種は、ワームがネットワーク帯域を消費することで起こるシステムダウンやサービス停止の形で損害を与えています。

2017年のWannaCry検出レポートの大部分は、アジア諸国からのものでした。しかし、最近のコネチカット州[18]とノースカロライナ州[19]からのWannaCry感染の報告は、WannaCryが世界の他の地域でも活動を続けていることを示しています。

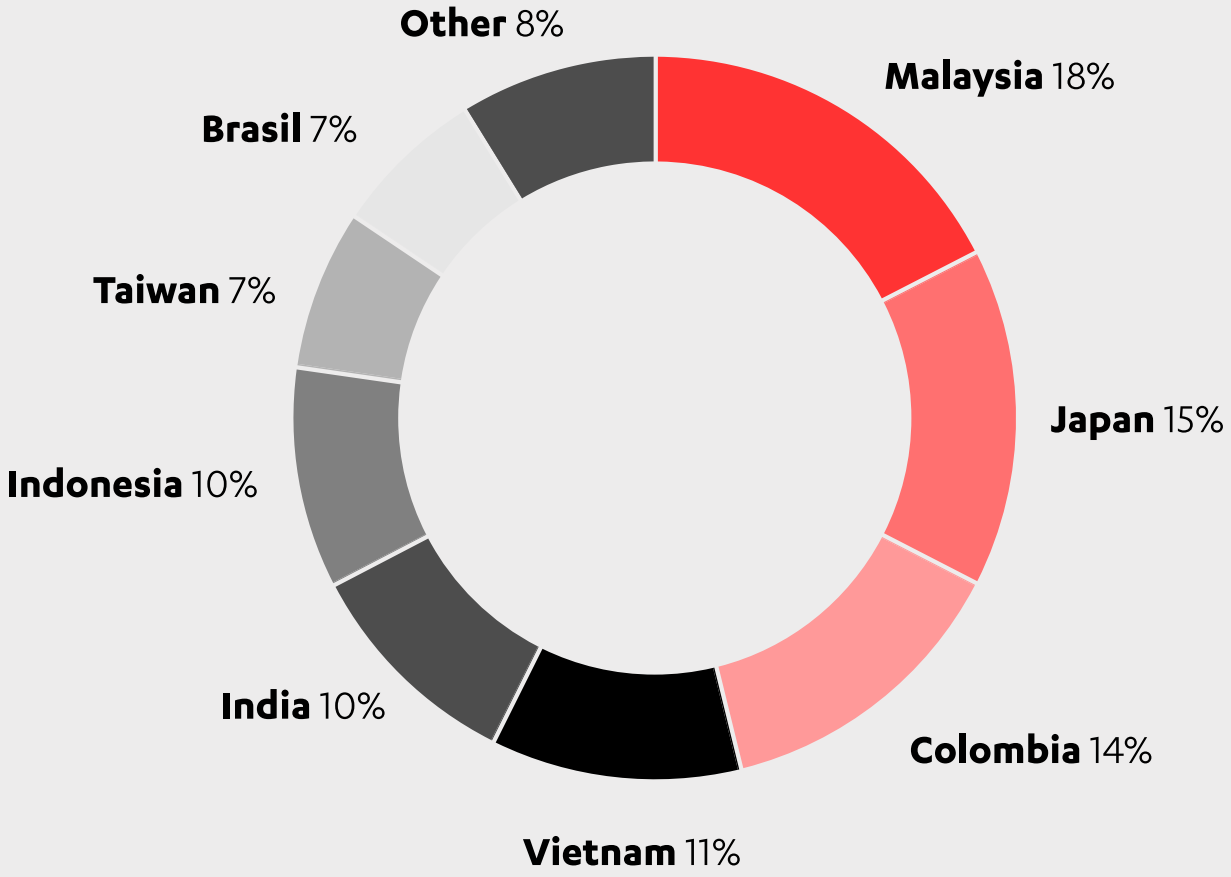

図 9: 国毎のWannaCry検出数

ワームを除去することは困難ですが、組織は感染を制限するためにファイアウォールを構成することによって脅威に対抗することができます。WannaCryの場合、ワークステーションがポート135/137/138および445（特定のサービスに必要でない場合）を介したインバウンドトラフィックを許可しないようにすることで、サーバーからのすべてのアウトバウンドトラフィックをブロックすることができます。

もう一つの重要な予防措置は、古いソフトウェアにパッチを当てることです。しかし、検出レポートにWannaCryが未だに出てくることからわかるのは、2017年のWannaCryやNotPetyaのアウトブレイクと同じSMB脆弱性を利用した攻撃に対して脆弱な未パッチマシンが未だに多数存在していることです。

トレンドを超えて

2017年がランサムウェアにとって節目だったことは間違いありません。WannaCry、NotPetya[20]、Bad Rabbit[21] などのアウトブレイクによるインシデントのおかげで、攻撃数が急増しました。

米ホワイトハウスは、NotPetyaのアウトブレイクについて「これまでで最も破壊的で費用のかかったサイバー攻撃」という声明を出しました。[22] また、前述したように、多くのサイバー犯罪者がこのトレンドに乗じてランサムウェアの新しいファミリーや亜種によって利益を得ようとしました。これらは、ランサムウェアが個人、組織、および一般の人々への深刻な脅威として存在し続ける理由の一部でしかありません。

しかし、ランサムウェアの最も注目すべき進化のいくつかは、これらのトレンドに反映されていません。一般的にサイバー犯罪は、ルールの例外と見なされるものを達成した場合に「成功」したと見なされます。WannaCryやLockyは、数値上は大流行しましたが、これはおそらくランサムウェアの最大の「成功」の話ではありません。例えば2017年6月、韓国のWebホスティング会社はErebus ransomware[23] のLinux版による被害に遭い、サイバー犯罪者に100万ドルの身代金を支払いました。[23] ほとんどのランサムウェアがWindowsをターゲットにしていることを考えると、これは非常に希なことです。[24] しかしこのアプローチは、WannaCryよりもはるかに有益であると思われます。WannaCryは高い拡散力と知名度を持っていますが、攻撃者が稼いだのは14万ドルでした。[25]

実際には、WannaCryとNotPetyaが遺したものは、財政的な成果というよりも、これらの脅威の破壊的な本質でした。これらのインシデントによって、他の攻撃者が長期的なランサムウェア攻撃を思い留まる可能性があります。どちらのケースでも、被害者は身代金を支払う必要は無かったのです（WannaCryの暗号化処理は無効化されましたし、身代金の支払いはNotPetyaの復号化につながりませんでした）。もしWannaCryとNotPetyaで、身代金を支払っても必ずしもデータが返ってこないということがわかったら、将来の被害者は身代金を支払うでしょうか？ そして、これらの犯罪が利益を生まなければ、犯罪者はそれを続けるでしょうか？

個人と企業がランサムウェアから自分自身を守るためには、多くの異なる方法があります。良いニュースは、ランサムウェアと戦う多くの方法があるということです。[26] 悪いニュースは、身代金を支払ってしまう誰かが常に存在するということです。この状況が変わるまで、オンライン犯罪者に身代金を支払わずに済むように、誰もがファイルをバックアップし、ファイルを復元する練習を続けなければなりません。

リファレンス

1 https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf
2 https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf
3 https://www.infosecurity-magazine.com/news/70-of-businesses-pay-up-to/
4 https://www.bleepingcomputer.com/news/security/only-half-of-those-who-paid-a-ransomware-were-able-to-recover-their-data/
5 https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
6 https://www.theregister.co.uk/2016/01/13/ransomware_for_next_tech_unicorn_firm/
7 https://labsblog.f-secure.com/2017/05/15/wannacry-party-like-its-2003/
8 https://labsblog.f-secure.com/2016/02/22/locky-clearly-bad-behavior/
9 https://labsblog.f-secure.com/2017/11/23/necurs-business-is-booming-in-a-new-partnership-with-scarab-ransomware/
10 https://labsblog.f-secure.com/2016/07/13/a-new-high-for-locky/
11 http://nordic.businessinsider.com/bitcoin-price-in-2017-review-2017-12
12 https://www.youtube.com/watch?v=TP3gA6NRtN4
13 https://www.nomoreransom.org/en/index.html
14 https://safeandsavvy.f-secure.com/2017/05/12/wannacry-may-be-the-biggest-cyber-outbreak-since-conficker/
15 https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
16 https://www.cyberscoop.com/conficker-trend-micro-2017/
17 https://safeandsavvy.f-secure.com/2017/05/18/wannacry-now-hitting-asia/
18 https://www.scmagazine.com/wannacry-hits-12-connecticut-state-agencies/article/746764/
19 http://www.healthcareitnews.com/news/new-wannacry-variant-takes-down-north-carolina-provider
20 https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/
21 https://labsblog.f-secure.com/2017/10/26/following-the-bad-rabbit/
22 https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/
23 https://www.bleepingcomputer.com/news/security/south-korean-web-hosting-provider-pays-1-million-in-ransomware-demand/
24 https://www.techrepublic.com/article/report-99-of-ransomware-targets-microsoft-products/
25 https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/
26 https://www.f-secure.com/documents/996508/1030745/Ransomware_how_to_ppdr.pdf