

2017年10月

ランサムウェア エコノミー

ランサムウェアのダークウェブ市場はなぜ、
またいかにして1年で2,500%を超える成長を遂げたのか



エグゼクティブ・サマリー

CryptoLocker(クリプトロッカー)、GoldenEye(ゴールデンアイ)、Locky(ロッキー)、WannaCry(ワナクライ)。2017 年が、ランサムウェアに関しては史上最悪の 1 年だったということになるのは明らかです。ニュースにあまり関心のない消費者でさえ、世界中の企業がこの 1 年で 10 億ドルとも想定されるコストを浪費した、危険なランサムウェア攻撃のことは、その全部とは言わずとも、どれかひとつくらいは耳にすることでしょう。

サイバーセキュリティの面からランサムウェアが注目される中、**カーボンブラックの脅威分析部門(TAU)**はそのインテリジェンスネットワークを駆使し、急成長するアンダーグラウンドエコノミーの中で、今まさにランサムウェアが作られ、購入され、販売されているウェブの最深部、最暗部に切り込んで調査を行いました。

この調査でわかったのは、2016 年から 2017 年にかけて、ダークウェブでは**ランサムウェアの販売が 2,502% も増加した**ということです。この増加は主に、需要と供給という単純な経済原理に基づいたものです。サイバー犯罪者はますます市場参入の好機ととらえるようになり、違法な経済活動で手に入る無数のランサムウェアのどれかを使って一儲けしようとしています。しかも、ランサムウェアの基本的な魅力は、すぐに使えるという、いたってシンプルなものです。他の多くのサイバー攻撃の様式とは異なり、ランサムウェアは何も考えなくともすぐにデプロイすることができて、儲けに繋がりがやすいのです。

この調査でわかったように、これらのダークウェブ経済のせいで、DIY(ドゥイットユアセルフ)キットを使えばまったくの初心者でもランサムウェア攻撃をしかけることができるようになってしまい、ランサムウェアの制作者に 10 万ドル以上の年収を許してしまっているのです。

主な発見

1

現時点で、ランサムウェアを販売するダークウェブのマーケットは **6,300 以上**あり、**45,000 以上**の現行製品が流通していると推定される。

2

DIY(ドゥイットユアセルフ)キットの価格は **0.50 ~ 3,000 ドル**で、中間価格は **10.50 ドル**。

3

2016 年度と 2017 年度の現在までの累計を比較すると、ダークウェブでのランサムウェアのマーケットは **249,287.05 ドルから 6,237,248.90 ドル**へと増加し、その成長率は **2,502%**となっている。FBI によれば、2015 年度には **2,400 万ドル**だった被害額は、2016 年度にはおよそ **10 億ドル**にのぼる¹。

4

業者の中にはランサムウェアを販売するだけで年間 **10 万ドル以上**を売り上げるものもいる。(これに比べ、PayScale.com の数字によると、適法なソフトウェア開発業者の売り上げは 69,000 ドル。)

5

ダークウェブにおいてランサムウェア・エコノミーが急成長し成功している背景としてもっとも目立ったイノベーションは、身代金の支払い方法として**ビットコイン**が登場したことであり、また匿名化したネットワークの**Tor**が違法なアクティビティを隠蔽したことである。ビットコインは、法執行機関が「現金を追跡する」ことがほぼ不可能になるような方法での送金を可能にした。従来は、銀行送金やクレジットカード決済が詐欺事案をすぐに削除していた。ビットコインを使用すれば、口座所有者を特定する銀行すら存在しなくなってしまう。

6

ランサムウェア販売業者は、サプライチェーンのうち 1 分野に専門化してきており、それが**ランサムウェアのブームと経済的發展**を支えている。

¹ <http://www.ciodive.com/news/symantec-size-of-ransomware-demands-jumped-266-in-2016/441365/>

分析

2017 年の 8 月から 9 月にかけて、21 か所の大規模ダークウェブのマーケットで、ランサムウェアに関連したネットワーク上の新規の仮想の入札に対し、カーボンブラックの調査員がモニターを行いました。それぞれの入札については、その説明や販売価格を記録しました。

ダークウェブ経済全体を把握するために 21 の大規模マーケットで発見したサンプルを、同様のマーケットで構成される**ダークウェブのウェブサイト総人口**のおよそ 25%という推定に基づいて母集団全体の値に当てはめました。(注：すべての価格および値は米ドル表記とする。価格がビットコインで提示されている場合、該当の入札が特定された日のレートで米ドルに換算した)

本調査から、ランサムウェアはターンキーシステムをベースにした独自の経済体系になったことが分かりました。本稿執筆時点で、**6,300** 以上のダークウェブのマーケットでランサムウェアが販売され、**現行製品は 45,000 以上**あると推定されます。

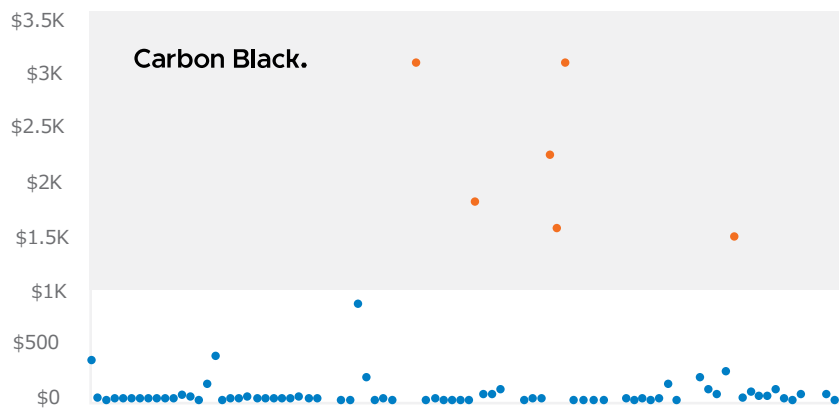
これらのマーケットにおける入札件数は膨大で、Android デバイスをターゲットとするロックスクリーン型ランサムウェア(1 ドル)から、ソースコードを含むカスタム型ランサムウェア(1,000 ドル以上)まで幅広く取引しています。下の表は 2017 年 9 月時点のアンダーグラウンドで入札されたランサムウェアの一覧および米ドル価格のサンプリングを反映しています。

ランサムウェア	価格(米ドル)
カスタム・スティーラー・ランサムウェアBTC	\$199
コードソース・ビットコイン窃盗&ランサムウェア BTC	\$99
インテリジェントビットコイン窃盗 コピー/ペースト ソースコード/ランサムウェア 2017年に高攻撃性に修正済	\$50
Android ロッカーランサムウェア	\$250
ランサムウェア - カスタムメイド	\$1470
ランサムウェア・ピグソー・ソースコード 修正済 2017	\$30
パーソナル・カスタム・スティーラー&ランサムウェア BTC	\$75
ソースコード ビットコイン窃盗&ランサムウェア BTC HQ	\$50
インテリジェント・ビットコイン窃盗 コピー/ペースト ソースコード/ランサムウェア 2017年に高攻撃性に修正済	\$25
?コードソース ビットコイン窃盗&ランサムウェア BTC???	\$99
6 ビットコイン・ランサムウェア イージー・マネー・システム	\$5
フィラデルフィアランサムウェアほか、トップ \$\$\$ (クローン)	\$1
カスタム・スティーラー&ランサムウェア	\$50



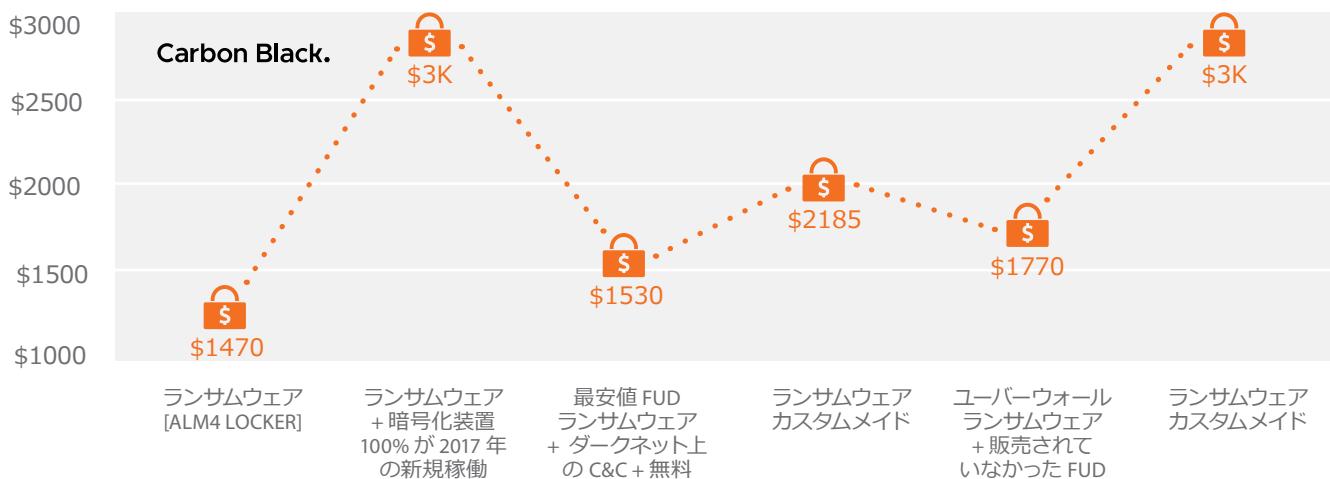
8月および9月の全データ集計から、**ランサムウェアの提供価格の中間値は10.50ドル**であることが分かりました。

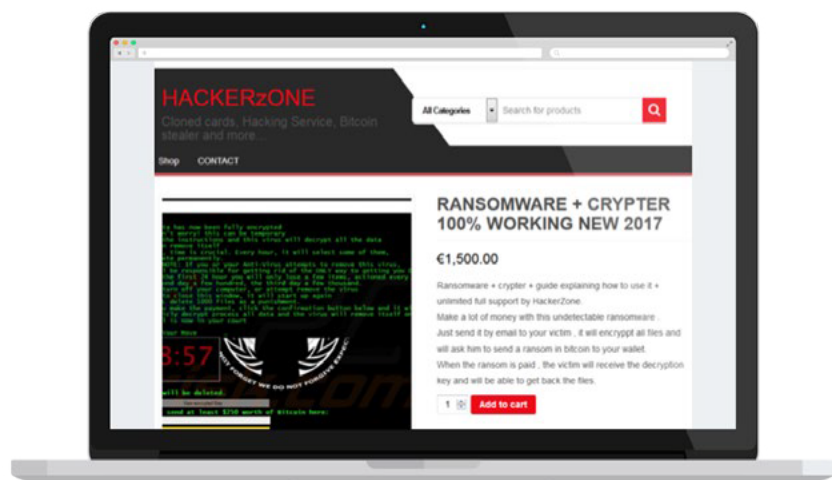
左図はダークウェブでランサムウェアを販売しているマーケットの一例



1,000ドル以上の価格がついた製品リストが6件見つかりました。これらは、カスタムで開発されたもの、独自コード、またはほとんど出回っていない製品です。

ランサムウェアの米ドルでの提供価格は下図を参照。



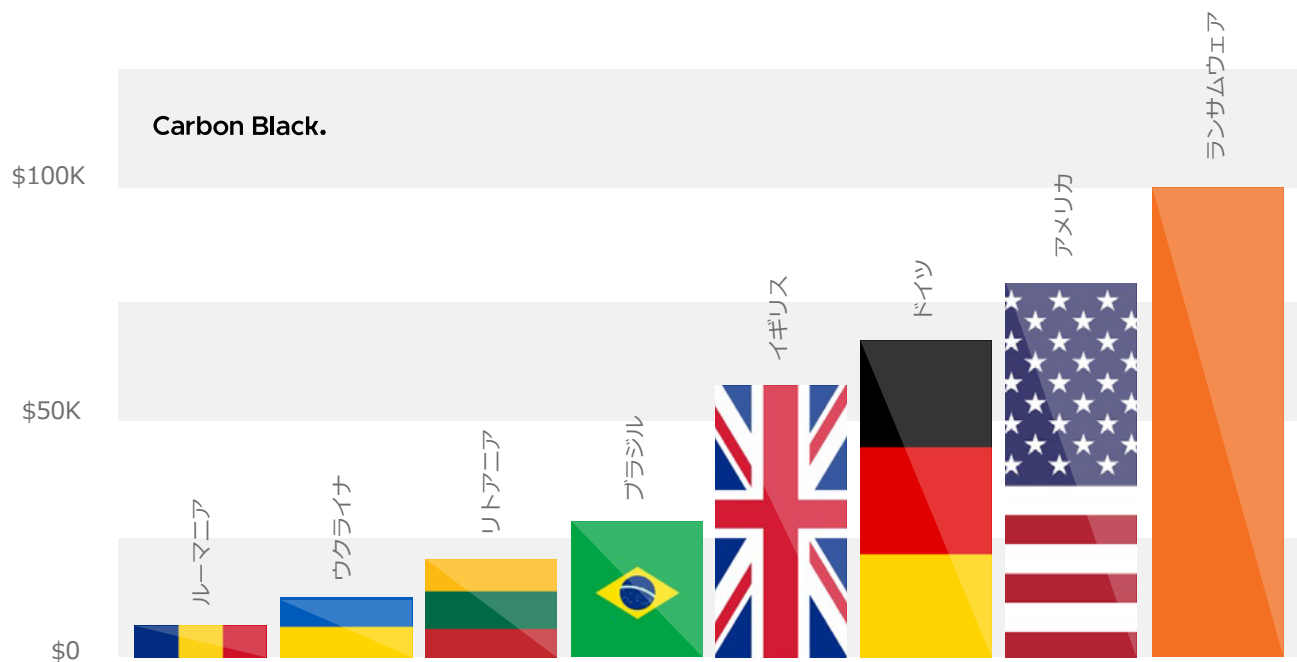


提示価格が高いものは、販売者はその値段の分だけその製品が高レベルで成功すると見込んでいます。

左図は、よりハイエンドなキットを販売しているダークウェブマーケットの一例

ランサムウェアの制作者にとっては、ランサムウェアをうまく作って売ることにはうまみがあるようです。本調査によれば、**ランサムウェア販売業者のなかには、ランサムウェアを販売するだけで年間 10 万ドルを売り上げるものもいます**。PayScale.com によると、正規のソフトウェアデベロッパーの年間平均売上は 69,000 ドル(東ヨーロッパではもう少し低く、およそ 45,000 ドルで推移)ですから、場合によってはその給料の 2 倍にもなるということです。

ランサムウェアデベロッパーと各国の正規ソフトウェアデベロッパーの給料の差を下图に示す²

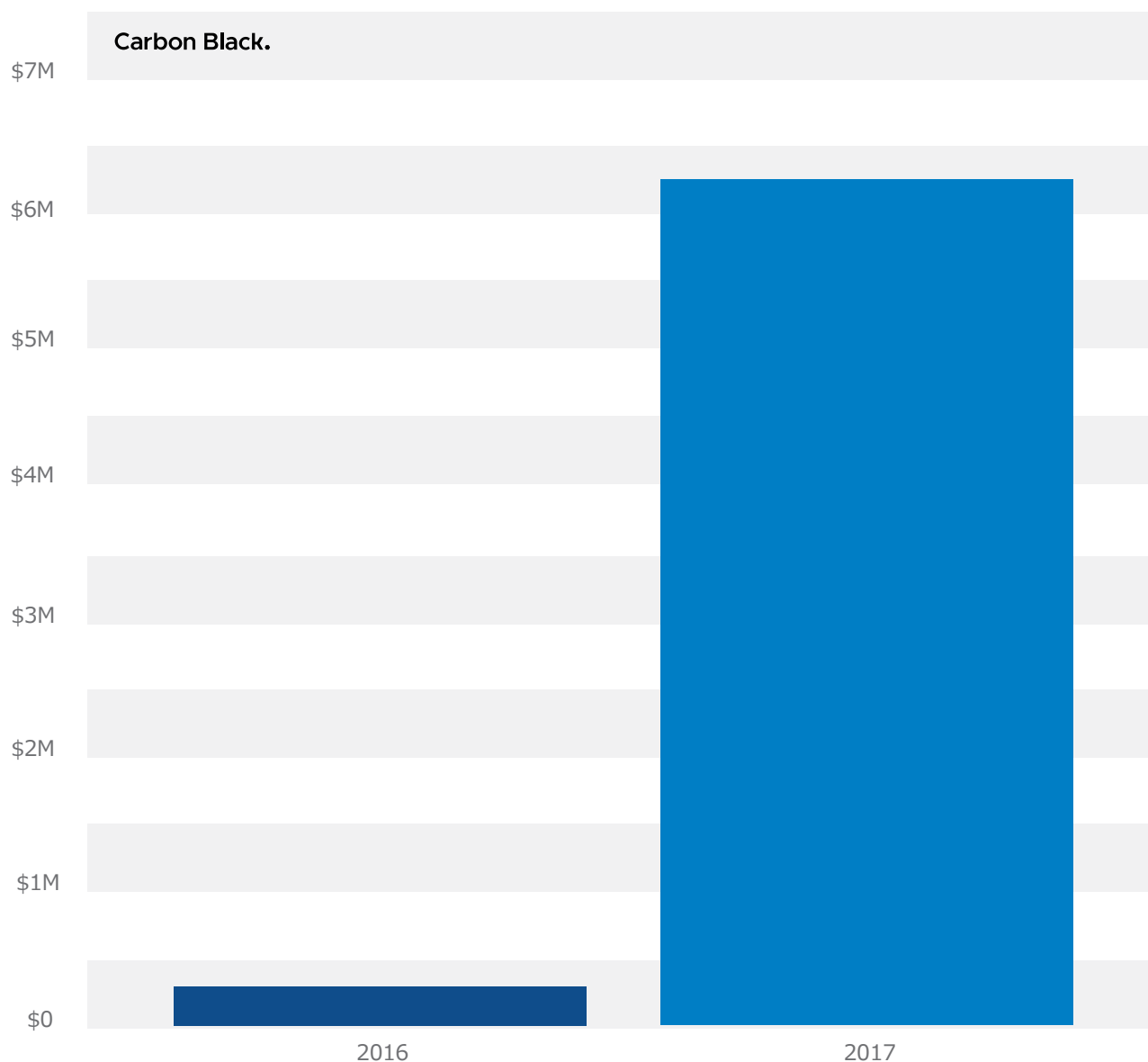


²<http://swexperts.com/news/software-engineer-salaries-by-country/>

ランサムウェアの制作者が年間10万ドル以上も稼ぎ出せるのであれば（しかもおそらくは税金も払わず）、ダークウェブのアンダーグラウンドエコノミーが活況を呈するのにも驚くようなことではありません。ダークウェブのデータベースダンプの履歴分析から、**2017年のランサムウェアによるアンダーグラウンドエコノミーは2016年に比べて2,502%成長した**、と結論づけることができます。

下図は、2016年と2017年のダークウェブ上でのランサムウェアの売上を比較したもの

ダークウェブ上のランサムウェアの売上 - 2016 vs. 2017



アンダーグラウンド・ランサムウェア市場: その登場とイノベーション

ダークウェブのランサムウェアエコノミーが2,502%の成長を遂げたことの背景とは



ビットコインおよびTorにより、偽名匿名による活動が可能になった



サービスプロバイダーの増加により、誰でもランサムウェア・ビジネスに参入できるようになった



根本的なセキュリティコントロールの欠如、つまり、バックアップや検査、復元、補修、可視性など、そして予防戦略の老朽化

ランサムウェアの登場から時間がたち、ビットコインおよびTorが普及するにしたがって、ランサムウェアで加害者になるリスクと障壁が一段と下がりました。いまでは、自分のトラフィックや決済のやりとりをどのように匿名化するかを知る必要もありません。そのようなサービスがすでに存在し、購入することができるからです。

このようなサービスが利用できるようになったことで、アンダーグラウンドのランサムウェアが見つかりにくくなり、法執行機関がそれを特定し削除することが非常に難しくなっていました。削除するにも、数か月から数年の努力の末にやっとできる、という状況です。

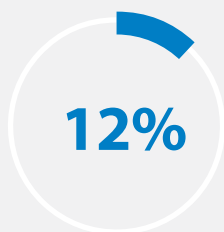
ダークウェブでのマーケットの発展は、第三者預託システムを利用した高リスクで信頼性の低い取引をサポートしてきただけでなく、要求した身代金をTorネットワークを介して支払わせることで、中心となるエンドポイントをなくし、地域をベースにした法執行機関による捜査を難しくしました。

このようなイノベーションが熟してきた結果として、アンダーグラウンドでのランサムウェアエコノミーはいまや商用ソフトウェアにも似た一大産業となっています。開発からサポート、ディストリビューション、品質保証、さらにはヘルプデスクまでそろっているありさまです。

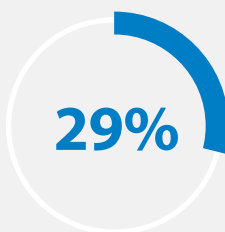
また、消費者側が身代金を払ってしまうことについても考えなくてはなりません。カーボンブラックの最近の調査で、もしも自分のパソコンやファイルがランサムウェアに暗号化されてしまった場合に個人的にはすすんで身代金を払うか、と質問したところ、52%が「イエス」と回答しました。

Carbon Black.

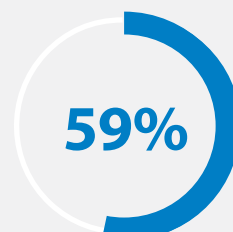
もしも自分のパソコンやファイルがランサムウェアに暗号化されてしまったら、
いくらまでなら身代金を払いますか？



データを取り戻すためなら、
500ドル以上でも支払う



データを取り戻すために、
100～500ドルなら支払う



データを取り戻すために、
100ドル未満なら支払う

アンダーグラウンド・ランサムウェア・エコノミーとサプライチェーン

本調査によると、ダークウェブのランサムウェア市場はこのような階層とプレイヤーが担っています。

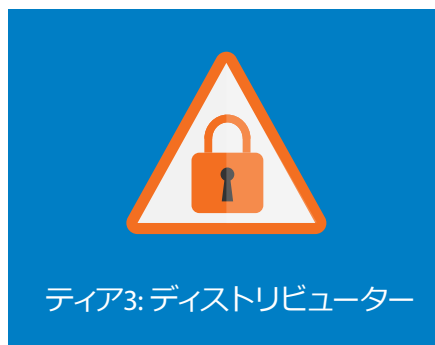
単一のサービスプロバイダー（全面的に行う）

開発製造 > ディストリビューション > 暗号化 > 支払い > 遠隔操作

コンポーネントサービスレイヤー（オプションのみ行う）

開発製造 > ディストリビューション > 暗号化 > 支払い > 遠隔操作

エコノミー（ティア）



ランサムウェア・キルチェーン



ロッキード・マーティン・キルチェーン

Carbon Black.

ティア1: 制作者

制作者は以下のようなことを担っています。

- 1- 販売する新しいランサムウェアの作成
- 2- コーディングスキルの向上
- 3- トレーニングとサポート

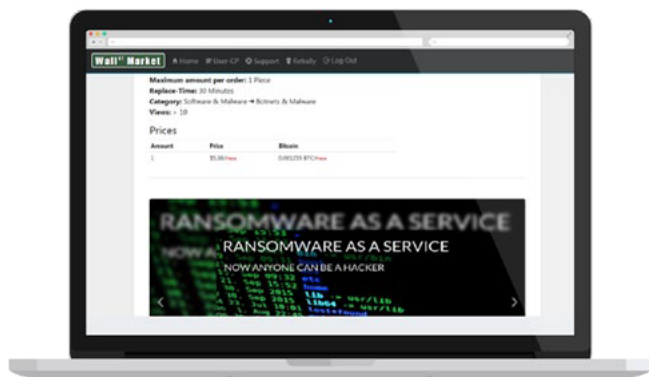
制作者は「武器製造者」であると考えてみましょう。彼らが自分で作ったものを使用することは決してありません。コードを売るだけです。サポートやコードに対する修正も売っています。

制作者の収入は(本調査によると時に年間10万ドルを超える)、ランサムウェアのコードそのものの販売、(コーディングスキルのない人のための)オースーコード用プラットフォームの販売、他社にコードを教える、などによって得ています。

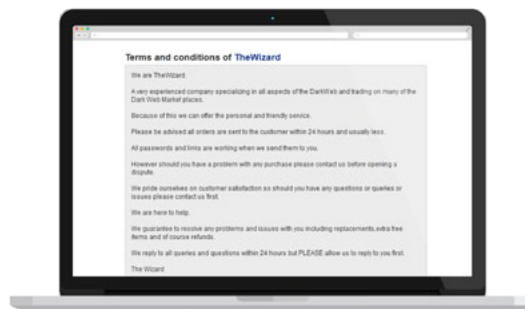
制作者は、特化したランサムウェアのコンポーネント(開発製造、ディストリビューション、暗号化、支払い、指揮統制)をサプライチェーンで売ることもできます。あるいは、キットを丸ごと売ることもできます。このようなキットには、ランサムウェアを構築しカスタマイズするために必要な一式が含まれています。

ティア2: サービスとしてのランサムウェア (RaaS)

ランサムウェアの制作者が、サービスとしてのランサムウェア(RaaS)プラットフォームを立ち上げることもあります。逆に、バイヤーが制作者からプラットフォームを購入し、自分でサービスを立ち上げるケースもあります。



この分野では、リスクを最小限にしつつ稼ぐために、ランサムウェアの制作者が「アフィリエイト」プログラムを始めることも考えられます。



「アフィリエイト」は、既存のインフラを利用して市場投入時間を早めたり、リスクを加入者間で分散したり、ターゲットのリスクを提供しあったりします。

そのプロセスの一般的な仕組みは次のようになっています。

- 1- ディストリビューターがランサムウェアのキャンペーンで「割当て分」を購入する。通常、利益の分割のしかたはあらかじめ決めておく。
- 2- サービスオーナーが分割金をディストリビューションサーバーに埋め込んでおく。ディストリビューションサーバーを使ってキャンペーンを追跡する(メトリクスなど)。多くの場合、利益の割当てはディストリビューションを行うディストリビューターに有利になっている。彼らは、追跡しにくく回避されにくいコードに変更しなければならず、もっともリスクを負うからである。
- 3- RaaS のプロバイダーがサービスとしてキャンペーンの追跡を行い、ビットコイン取引を監視し、ビットコインのディストリビューションを行う。

キャンペーンで得たメトリクスを使って、次にもっとよくできた、利益の大きいキャンペーンを作ります。(例、報酬率をもとにすると、次にどの国をターゲットにすべきか?)

サービスオーナーは必要なプラットフォームとインフラをディストリビューターに提供します。

プログラムには2種類あります。「信頼と実証(trust-ed-and-verified)」モデルでは、ディストリビューターが犯罪者として分かっているながらサービスを提供します。こちらはプレミアムモデルと言えます。

スタンダードモデルはターゲットリストがあれば誰でも使えます。(注: サービスとしてのランサムウェアが成功したことで、その下の3番目のティアが崩壊し始めることになる)

ティア3: ディストリビューター

このティアでは、利益が多いと同時にリスクも高くなっています。ディストリビューターが担っているのは次のようなことです。

- 1- スпамキャンペーンやソーシャルエンジニアリング、ターゲットを絞ったハッキング、エクスプロイトキットなどの手段を使って、自分でランサムウェアのディストリビューションを行う。
- 2- サービスとしてのランサムウェアを利用する。RaaS は初心者でもランサムウェアに手を出しやすくしている。



Carbon Black.

ランサムウェア・サプライチェーン

アンダーグラウンド・ランサムウェア・エコノミーは、大きな利益を上げるビジネスモデルを形成しています。このエコノミーの蔓延を防ぐには、まずこのモデルの背後にある経済的側面を理解しなければなりません。

多くの人は、ランサムウェアの収益化を1つの面からしか見ていません。すなわち、犯人が被害者からの支払いを受け取るという部分です。これは目立つ部分ではありますが、じつはこのエコノミーの末端部分でしかありません。

では、「ランサムウェア・サプライチェーン」とはどういうものかを見てみましょう。



ランサムウェアの開発製造

ランサムウェアはソフトウェアです。誰かが作り、メンテナンスをして、試験をしなければなりません。マスマーケットに向けてランサムウェアが作られることもあれば、ターゲットを絞ったキャンペーンのために書かれることもあります。コードがどれほど特定のターゲットに合わせてあるかによってコストが決まります。

サプライチェーン全体を提供するのが1つのグループや1人の人間かもしれないのに、次第に積み重なっていく場合もあるということを理解することが重要です。アンダーグラウンドエコノミーの内部でDIYキットや特化が進んでいくことが、ランサムウェアのブームを後押ししています。



ランサムウェアのディストリビューション (ソーシャルエンジニアリング、スパム、ターゲットを絞ったハッキング、エクスプロイトキット)

多くの人が初めてランサムウェアに出会うのがこの段階です。ここでは、攻撃者は「数撃ちゃ当たる」方式で巨大リストに悪意のあるメールを送り、ほんのわずかでもクリックしてくれることを期待します。2018年に入れば、ランサムウェアがますますビジネスをターゲットにしていくであろうことは、2017年のWannaCry(「ワナクライ」)の攻撃を見ればわかります。より警戒すべきは、WannaCryがNSAツールを活用してどのように世界中に攻撃を広げたか、ということかもしれません。



暗号化／非暗号化

このモジュールが、じっさいにデータを暗号化するシステム上のアクティビティを担っています。ランサムウェアの攻撃で、大きな赤いシミがスクリーンに表示されるのを何度となく見てきました。表面的には、支払いが済めばデータは非暗号化されます。攻撃者にとっては、暗号化および非暗号化ツールはそれだけで購入することができたり、DIYキットに入っていたりします。



支払い

このモジュールは、一般的にはビットコインを使って、支払いをスムーズに行い、追跡して通信します。サービスプロバイダーやディストリビューターは、その後のキャンペーンがさらにうまくいくように、その情報を使います。



遠隔操作

このモジュールは、ランサムウェアのエンドツーエンドのオペレーションを担います。また、ランサムウェアのライフサイクルを通して感染したホストをコントロールするのもに使われます。これらはかなり標準化されつつあります。

防御する側ならではの利点

ランサムウェアのサプライチェーンを断ち切るにあたり、希望がもてることは、防御する側は元から優位に立っていることです。防御側がチェーンのつながりを1つでも断ち切ったり妨害したりできれば、攻撃全体が崩壊します。

ディストリビューターやオペレーターを排除しても、問題の枝葉を刈っているにすぎません。アンダーグラウンド・ランサムウェア・エコノミーを徹底して抑え込むには、サプライチェーンを根絶し、マルウェア制作者のやる気をなくす努力が必要です。攻撃者の投資利益を下げることで、防御側は犯罪の経済的動機を減らせるのです。

そのうえで、身代金の支払いを止めなければなりません。彼らの仕組みは被害者が支払いを選択することで成り立っているのです。

人々が支払いをしないと決意するまでは、問題は大きくなり続けます。それに、現状では法執行機関が問題に切り込むことができません。ランサムウェア攻撃を阻止することに関して、企業は概ね自力でなんとかするしかありません。

特化がアンダーグラウンドエコノミーの成長を促している

アンダーグラウンド・ランサムウェア・エコノミーの成長によって、不穏な流れが浮かび上がります。すなわち、私たちは業界としてセキュリティの基本を誤解しがちだということです。事象に対して、ファイルやシステムのバックアップ、復旧試験、補修、社内全体の適切な可視性の確保といった、セキュリティの基本的な防御や取り組みに失敗していることがあまりに多いのです。旧式のアンチウィルスなど、時代遅れな防止策を実施していることもそうです。

攻撃者は、お金のある所を狙いつづけます。今のところ、ランサムウェアを使えばたぐりよせることのできるお金があります。経済の流れを変えるには、組織はセキュリティのベストプラクティスをていねいに棚卸しすべきです。さらに、あるかもしれないギャップを埋めるために、ユーザー教育プログラムを導入することを検討すべきです。

ユーザー教育と並行して、組織全体の完全な可視性を提供し、ランサムウェア攻撃で被害を受ける前にそれを阻止してくれるセキュリティソフトウェアに取り組む必要もあります。

ランサムウェアのさまざまなコンポーネントが特化したことで、アンダーグラウンドでのランサムウェア市場は昨年、2,502%もの成長を遂げました。

ランサムウェアが利益を生むとはいえ、サプライチェーン全体に「通じている」必要はなく、個々のコンポーネントがどこで購入できるかだけを知っていればよいわけです。

いまやサービスレイヤーが存在することによって、このエコノミー自体がしっかりしたものになってきました。このようなサービスが参入の難易度を下げ、攻撃者は複数の専門分野を知る必要がなくなりました。それどころか専門知識などなくてもよいのです。ビットコインが少しばかりあればそれでいい。そのため、そうしようと思えば誰でも、攻撃をしかけられるようになったのです。

ランサムウェアはもう、小さな犯罪者グループが強盗や誘拐をするもの、とは言えません。むしろ、クラウドサービスの顧客のようなものです。パーツの組み合わせさえわかればできてしまいます。新興企業のCEOは、ITスタッフを山ほど抱えるようなことはせず、インフラに大きな投資もしません。彼らは既存のサービスを利用して市場投入時間を短縮しています。サイバー犯罪者も同じです。犯罪者は利益になるものにピンポイントで飛びつきます。

このように特化したことにより、ランサムウェア攻撃は成功しやすくなりました。攻撃の頻度や深刻度も増加していくでしょう。限られた専門家だけではなく、不法な金儲けを企む誰もが攻撃をする力を持てるようになったのです。

経済の流れを変えるには、組織はセキュリティのベストプラクティスをていねいに棚卸しすべきです。さらに、あるかもしれないギャップを埋めるために、ユーザー教育プログラムを導入することを検討すべきです。

今後の予測

改善した予防モデルが続々と市場に出てくれば、脅威はアンダーグラウンドマーケットにとどまり、利益共有モデルが増加して、脅威の統合と集中につながるでしょう。統合が進むということは、ランサムウェア被害は減っても影響は大きくなるということです。

2018 年に向け、ランサムウェアに関連して以下のようなことが予測できます。

- 1- ランサムウェアが向かう方向を見ると、1 回の感染でより多くのお金をゆすりとうろとするとするならば、Linux システムがターゲットにされることが増えるでしょう。例えば、攻撃者はサーバーを感染させてより高額の身代金を得るために SQL インジェクションを投入するようになるでしょう。すでに今年初めに、MongoDB を狙った攻撃が観測されたのは、その前兆といえます。
- 2- 今後ランサムウェアは、これまでよくみられたような「数撃ちゃあたる」方式ではなく、ある種のファイルタイプを探してターゲットにしたり、法律や医療分野、税務申告作成業務など、特定の企業を狙ったりするようになるでしょう。すでに、データベースを狙ったものや、ビジネスを餌食にするもの、AutoCAD の設計図のように致命的で所有権に守られたファイルを狙ってコードにちょっとした変更を加えたランサムウェアが登場しています。拡張子をターゲットにすれば、多くのランサムウェアサンプルが多くの防御策のレーダーをかいくぐるができるのです。
- 3- この調査で当社が分析したランサムウェアサンプルのほとんどは、その場でファイルを暗号化し、非暗号化のためだけに暗号化キーを送信するシンプルなものでしたが、これからは暗号化の前にデータを抜き取るようなひと手間をかけるものが出てくるでしょう。そうなれば、企業はデータの復元を強いられるだけでなく、所有データをブラックマーケットで売買されかねない危険もはらむことになります。
- 4- ランサムウェアはますます、偽装行為のために使われるようになります。例えば、過去には Zeus ボットネットのオペレーターが、追っ手を撒くような感染をさせた後に DDos 攻撃をしかけたことがありました。ランサムウェア攻撃にも似たような流れができつつあり、敵がより悪質な行動をとった後にファイルの暗号化をすることがあります。バックアップの可能性のあるファイルを削除するポリウム・シャドウ・コピーの削除という既存のテクニックの使用や、また Windows のイベントログを削除することで、対応側がデータや抜き取られた認証情報を調べられずにファイルの非暗号化を強いられている間に、敵は事象対応努力を帳消しにすることが可能になるのです。
- 5- ランサムウェアは、最初の攻撃方法が失敗した場合の二次的方法として浮上してくるでしょう。より巧妙でターゲットを絞った攻撃に頼る敵が、攻撃の最終手段としてランサムウェアを使うこともあるでしょう。リモートアクセスツール(RAT)や抜き取ったデータによる環境への侵入に失敗した敵は、投資した分を少しでも回収しようと環境全体にランサムウェアをつきつけてくるかもしれません。
- 6- NotPetya で見られたように、フォルスフラッグとして当たり前にランサムウェアが使われるようになるかもしれません。動態分析だけを見れば Petya だと思われ、より詳しい分析ではそうではないと思われました。迅速分析でも明らかなランサムウェアである可能性が示されましたが、さらに深く分解してみたところでは、データは人質に取られたのではなく、破壊されていたのです。
- 7- ランサムウェアはソーシャルメディアを利用して意図的であろうとなかろうとますます広がっていくでしょう。Koobface などのマルウェアと同様に、フェイスブックのようなサイトで悪意を持ってシェアされたコンテンツは、被害者がついついクリックしてしまうようなリンクに誘導します。上記のようなコンセプトに見られるような、故意にシェアされた Popcorn Time などのランサムウェアは、被害者が身代金を減らしたり帳消しにしたりする目的でシェアしてしまうタイプですが、これらが大規模に使われるようになるでしょう。
- 8- ランサムウェアは今後、システムにとどまって再暗号化することでしばらくの後にさらにお金を要求するように変化していくでしょう。

調査方法について

2017年8月から9月にかけて、21か所の大規模ダークウェブマーケットでランサムウェアに関連したネットワーク上の新規の仮想入札を調査員がモニターし、それぞれの入札について、その説明や販売価格を記録しました。ダークウェブ市場経済全体を把握するため、ダークウェブサイト全体のおおよそ25% (Wired, 2014) という仮定に基づいて、21か所の大規模マーケットからの結果サンプルを母集団全体で一日あたりに観測されたTorのunique.onionアドレスの値と推定しています。この値は、同様の市場で構成されるTor Metrics サイト (<https://metrics.torproject.org/hidserv-dir-onions-seen.html>) に掲載されています。すべての価格および値は米ドルで表示し、価格がBTC (ビットコイン) で提示されている場合は、その入札が確認された当日時点で米ドルに換算しています。

ダークウェブのマーケットの2016年度の活動に関する履歴は、ダークウェブのデータベースダンプの分析から展開しました。この歴史的視点のために分析したサイトのサンプルサイズは、2017年2月の段階でおよそ1万の.onion サイト (ダークウェブの20%) となっています。

ジェネレーティングポイントの基本となる統計モデルは、収集したサンプルに基づいて推定しています。期間中の観測数は総人口で乗じ、製品数はサンプルサイズ (観測した母集団) で除算しています。

カーボンブラックについて

カーボンブラックは、次世代エンドポイントセキュリティのリーディングプロバイダーです。次世代アンチウィルス (NGAV) ソリューションである Cb Defense は、画期的な防止テクノロジーである「Streaming Prevention」を活用し、サイバー攻撃が実行される前にそれを即座に発見し停止します。Cb Defense は、画期的な防止策に検出および対策を組み合わせ、独自に軽量のエージェントにまとめたもので、クラウドから配信されます。1,300 万以上のエンドポイントを管理下におくカーボンブラックは 3,000 社以上の顧客を持ち、そのうち80 社は Fortune 100 に含まれています。これらの顧客は、もはやレガシーとなったアンチウィルスに代わってカーボンブラックを利用し、クリティカルなシステムのロックダウンや脅威ハンティングを実施し、非マルウェア攻撃を含む高度なサイバー攻撃からエンドポイントを守っています。

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com