暗号化された攻撃の現状（2020年版）

サイバー攻撃者がSSL/TLS暗号化の利用を一層拡大させ、従来型のセキュリティを回避している現状に対して、ゼットスケーラーの調査チームThreatLabZが行った重要な洞察

2020年1月～9月

目次

ThreatLabZについて

ThreatLabZは、新たな脅威からゼットスケーラーのお客様を保護するとともに、ゼットスケーラーのクラウド内を行き交う企業トラフィックの分析を行う、ゼットスケーラーのグローバルなセキュリティ研究部門です。ThreatLabZは、サイバーセキュリティ、データサイエンス、AI/機械学習の専門知識を保有していることに加え、ゼットスケーラーのゼロトラストエクスチェンジクラウドプラットフォームで処理される、1日あたり1,200億件以上にのぼるトランザクションの分析から膨大なデータを入手できる利点を活かし、企業のトラフィックとセキュリティのトレンドに関する洞察を提供しています。

ThreatLabZでは、他では見られない手法や能力を持つ新しい攻撃やマルウェアを検知し、それらのファイルを活性化させ、そのコードを分析することで、検知の回避、ペイロードのドロップ、情報の不正取得、デバイスのコントロール、ユーザの偵察、マルウェアの伝播や拡散といった行動がどのようにプログラミングされているかを詳しく調査しています。これらの分析結果は**ゼットスケーラーのリサーチブログ**で公開しており、セキュリティコミュニティでご利用いただくことができます。

ThreatLabZの研究者は、先日、暗号化されたチャネルを使用する脅威の検知と分析によって得られたデータから明らかになった、SSLにおける以下のようなトレンドを報告しました。

- **インフォスティーラーを拡散する偽のVPNサイト**
- **StackBlitzツールを悪用したフィッシングページのホスティング**
- **JavaScriptスキマー**
- **Higaisa APT（標的型攻撃）**

また、ゼットスケーラーのクラウドの活動状況は**「Cloud Activity Dashboard」**で、1秒あたりのトランザクション処理やブロックされた脅威の数をご確認いただけます。

SSLトラフィックに隠れる脅威が急速に増加

セキュリティエキスパートにとっての悩みは、多くのユーザがSSL暗号化に対し、「WebサイトでSSL暗号化が使われている限り安全である」と誤解していることです。

SSL暗号化は、トラフィックに含まれるデータを保護する目的で設計されたものですが、攻撃を隠す手段としても利用されるため、適切にインスペクションを実行しなければ、潜在的な脅威になり得ます。

サイバー犯罪者も、セキュリティエキスパートと同様に、転送中のデータを保護する対策としてSSL/TLS暗号化が業界の標準的な手法であることを熟知しており、自らも暗号化を取り入れることで、マルウェアを暗号化されたトラフィックに巧妙に隠し、セキュリティ検知の回避や攻撃に生かしています。事実、ゼットスケーラーのクラウドは1月から9月の間に、暗号化されたトラフィックに隠れていた66億件のセキュリティ脅威をブロックしています。月平均に換算すると、7億3,300万件をブロックしたことになり、2019年にゼットスケーラーのクラウドがブロックしたのが月あたり約2億8,300万件であるのに対して、月平均で2.6倍近く、暗号化されたトラフィックに潜む脅威の件数が増加したことになります。

すべての組織のセキュリティ対策において、暗号化されたトラフィックのインスペクションは重要な要素ですが、問題は、次世代ファイアウォールなどの従来型のオンプレミスのセキュリティツールには、多くの場合、トラフィックの復号化、インスペクション、再暗号化に必要なパフォーマンスと能力が備わっていないことです。すべてのSSLトラフィックに対してインスペクションを実行しようとすると、パフォーマンス（と生産性）が低下するため、多くの組織は、クラウドサービスプロバイダや「信頼できる」と判断したプロバイダからのトラフィックなど、一部の暗号化トラフィックに対してインスペクションを行っていません。これは重大な問題です。すべての暗号化トラフィックに対してインスペクションを実行しないと、組織はそこに隠されたフィッシング攻撃やマルウェアなどに対して脆弱になり、いずれも悲惨な結果につながる恐れがあります。

ゼットスケーラーの
クラウドでは、
1月から9月までの間に、
暗号化トラフィックに
隠された**66億の脅威が**
特定され、ブロック
されました

ThreatLabZチームは、2020年の1月から9月にゼットスケーラークラウドの暗号化トラフィックを対象に、業種ごとの利用状況の分析を行いました。この分析の目的は、暗号化を使用するトラフィックの総量だけでなく、このトラフィックに隠れる脅威を理解することです。分析結果によって、主に以下のような事実が明らかになりました。

- **インターネットトラフィックの大半が暗号化されるようになった**
  トラフィックの80%がSSL/TLS暗号化をデフォルトで使用しています
- **脅威の量が爆発的に増加している**
  新型コロナウイルス（COVID-19）の流行にともない、クラウドベースのコラボレーションアプリが急増したことで、過去9か月間でSSLベースの脅威が2.6倍増加しています
- **医療機関が攻撃の標的になっている**
  最も標的とされたのは医療業界で、16億件もの暗号化された脅威が検知、ブロックされており、金融と製造がこれに続きました
- **クラウドベースのファイル共有サービスの悪用が増加している**
  SSLベースの攻撃の30%以上が、Google Drive、OneDrive、AWS、Dropboxなどのコラボレーションサービスに隠されていました
- **暗号化トラフィックに隠れるランサムウェアが増加している**
  暗号化されたWebトラフィックで送り込まれるランサムウェアが5倍以上も増加しました

サイバー犯罪者によるSSL/TLSの悪用
暗号化されたトラフィックのインスペクションが重要である理由

SSL（Secure Sockets Layer）とその後継である最新のTLS（Transport Layer Security）によるインターネットトラフィックの暗号化は、転送中のデータを保護する手法として世界標準であり、今ではインターネットトラフィックの大半が暗号化されるようになりました[1]。問題は、犯罪者も暗号化を利用してマルウェアやその他のエクスプロイトを隠そうとしていることです。これは、暗号化されたチャネルを通過するトラフィックもデジタル証明書があるというだけでは信頼できなくなっていることを意味します。

サイバー犯罪者は、エクスプロイトや隠されたマルウェアが含まれる、無害であると見せかけたフィッシングメールから始まる高度な攻撃チェーンを構築しています。疑いを持たないユーザがそのようなメールをクリックすると、マルウェアのインストールという次の段階へと攻撃が移行し、最終的には企業の価値あるデータが外部に持ち出されてしまう事態に陥ります。

エクスプロイトや隠れたマルウェアも暗号化されているため、ファイル構造が完全に変わってしまうのが、この攻撃が極めて悪質である点です。サイバーセキュリティシステムは、ファイルの構造（すなわち「フィンガープリント」）を頼りに脅威を識別するため、ファイルの構造をシステムが認識していれば、脅威としてブロックできます。ところが、ファイルが暗号化されるたびに、脅威として認識されていない、まったく新しいフィンガープリントに生まれ変わります。

セキュリティエンジンは
見えないものをブロック
できません

SSLインスペクションこそが、これらのサービスを利用して送り込まれる不正ファイルをブロックする唯一の方法です

[1] https://transparencyreport.google.com/https/overview?hl=en

SSLトラフィックのトレンド

多くの企業が、転送中のデータを傍受する、または抜き取るといった攻撃に対して保護対策を実行するには暗号化が必要だという事実に同意しています。我々の分析では、教育部門のトラフィックの暗号化率が最も高く、製造、金融、医療がこれに続きます。ただし、小売・卸売、サービス、テクノロジ・通信、公的機関などのいずれの業種にも、大きな差はありません。分析期間である2020年1月から9月に、暗号化の使用が全業種の平均で約75%、ピーク時に80%以上であることがわかりました。

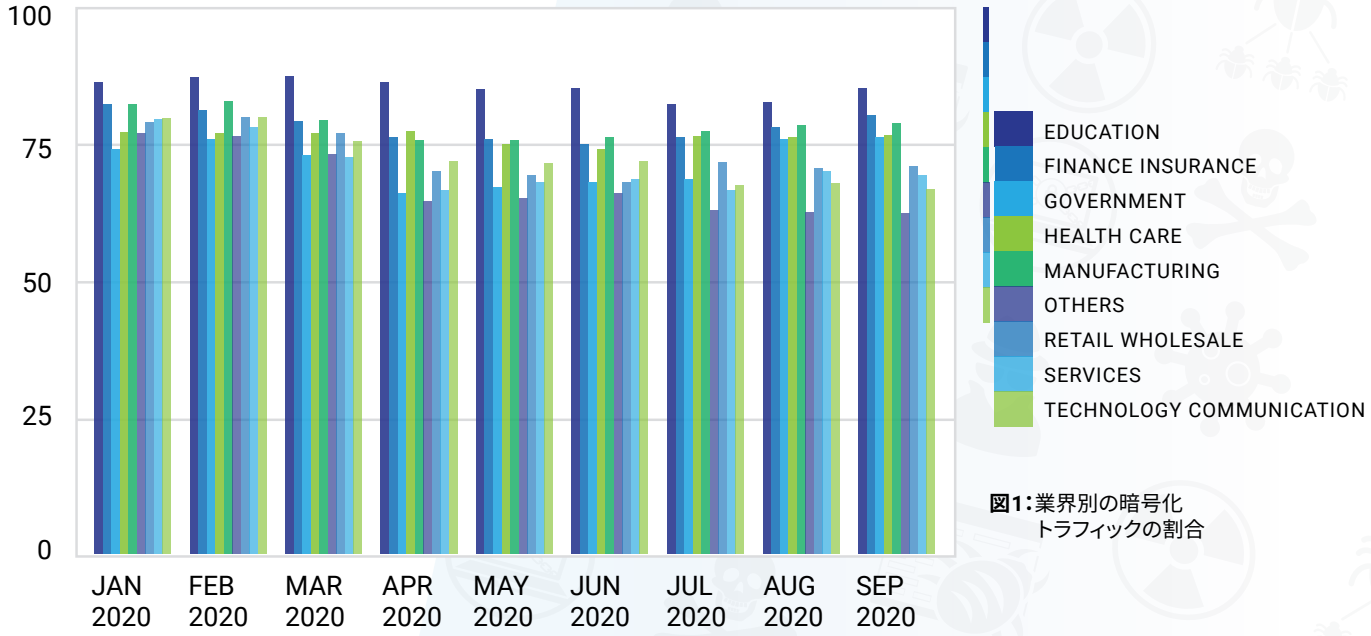


図1：業界別の暗号化トラフィックの割合

暗号化されたトラフィックの割合が高いことはどの業種でも確認されており、脅威を検知するには、どの組織も同様に、SSL/TLSに対してインスペクションを行う必要があります

ThreatLabZの調査によると、サイバー犯罪者は暗号化されたマルウェア攻撃で医療機関を標的にしており、他のどの業種より多くの脅威が発生しています。2020年1月から9月にゼットスケーラーのクラウドでブロックされた暗号化チャネル経由の高度な脅威の中では、医療が25.5%を占め、金融・保険が18.3%、製造が17.4%、公的機関が14.3%でそれに続きました。

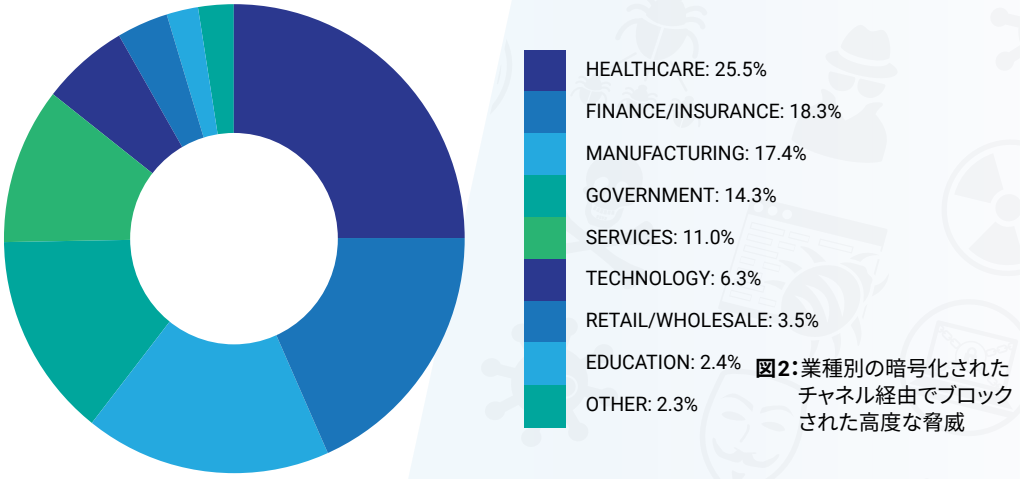


図2: 業種別の暗号化されたチャネル経由でブロックされた高度な脅威

世界的なパンデミックによって医療サービスがこれまで以上に重要になっているにもかかわらず、医療機関は、暗号化されたチャネル経由で送り込まれる脅威の最大の標的になっています。 攻撃者はパンデミックに乗じ、ニュースや製品、治療方法を提供すると称して、偽サイトで新たな攻撃を展開しています。ThreatLabZによると、2020年の最初の3か月間にCOVID関連の脅威は**300倍**にも急増したと報告されています。

注目すべき業種 — 医療

暗号化されたチャネル経由で16.9億件以上の攻撃が医療機関に対して試行され、他のどの業種より多かったことが分かりました。この業種に対する攻撃の大半が、不正 URLを使用するものでした（84.2%）。不正 URLは、電子メール、テキストメッセージ、ポップアップ、ページに表示される広告を使ってユーザに配信され、結果として、マルウェア、スパイウェア、ランサムウェアがダウンロードされたり、アカウントが攻撃される仕組みです。

医療機関がサイバー攻撃の標的になることが多いのは、医療機関の環境に存在する、FDA（アメリカ食品医薬品局）の承認に時間がかかる、古いシステムによるものです。これらの古いシステムはセキュリティコントロールが不十分であるため、既知の問題に対する脆弱性が数多く存在します。そのような状況で、コントロールの統合、可視性の一元化、ポリシーの適用を怠ると、セキュリティコントロールのギャップが発生し、サイバー犯罪者に悪用される恐れがあります。

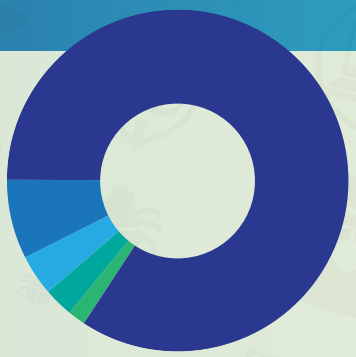


図3: 暗号化されたチャネル経由で送り込まれた、医療機関を標的とする脅威

攻撃はさらに高度化している

多くのITプロフェッショナルがユーザに対し、URLをよくチェックして、エラーやスペルミスを始めとする、正規のサイトではない可能性を示す手掛かりから、偽サイトや不審サイトであるかどうか、確認を行うよう呼びかけています。ところが最近では、ドメインスクワッティングやIDNホモグラフ攻撃などの手法によって、本物のサイトそっくりの偽サイトが生成されており、見極めが困難になっています。

ドメインスクワッティング（サイバースクワッティング）とは、フィッシングや認証情報の不正取得、マルウェアの拡散などの目的で、有名ブランド（gmali.comなど）によく似たトップレベルドメインを登録することです。

ドメインスクワッティングなどの**ホモグラフ攻撃**は、たとえば、AppleのURLの「l」の代わりに「1」という数字を使う（https://www.app1e.com）といった方法でユーザを騙し、リンクをクリックさせようとします。

クラウドストレージサービスの悪用

攻撃の手段として多く使われるようになったのは、クラウドストレージサービスです。これらのサービスは、WebのSSLベースの送受信によってファイルを安全に共有する優れた手段ですが、サイバー犯罪者は、ほとんどの組織ですべてのSSLトラフィックをインスペクションしているわけではないこと、また、クラウドサービスが一般的に「信頼されている」ことを熟知しており、これらのサービスが送信元であるかのように見せかけた攻撃を仕掛けてきます。

ゼットスケーラーのクラウドでは、2020年3月から9月に、暗号化されたトラフィックに含まれていた**20億件の脅威**をブロックしましたが、その大半が、Google、AWS、Dropbox、OneDriveでホスティングされている不正コンテンツに関係していました。これらの脅威は3月から9月に約2倍に増加し、この間のSSL/TLSで暗号化された脅威全体の約30%を占めました。

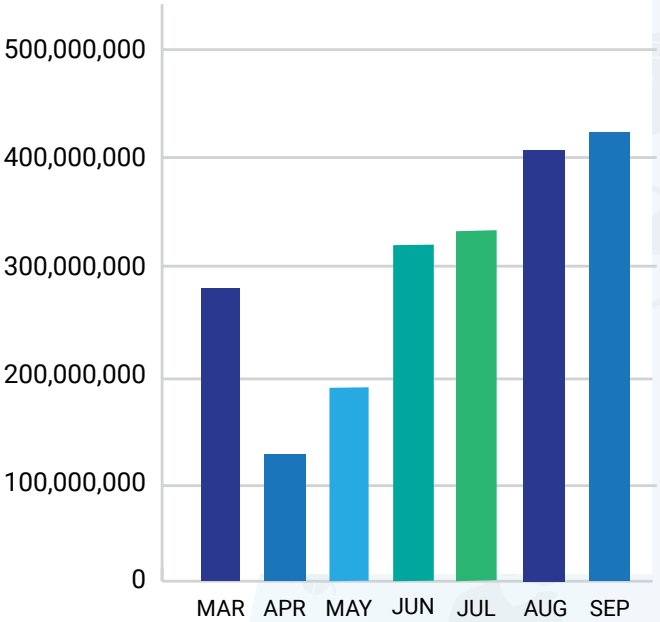


図4： TLS/SSL経由で主要クラウドストレージサービスから送り込まれ、ブロックされた、高度な脅威

ゼットスケーラーのクラウドは、3～9月にクラウドストレージサービスプロバイダが送信元であるSSLトラフィックに含まれていた**20億件の脅威**をブロックしました

図5は、クラウドサービスがマルウェアのホスティングやサービスにどのように悪用されているかを示しています。サイバー犯罪者は、マルウェアのペイロード（多くの場合、第1段階のダウンローダファイル）をひとつ以上のサービスにアップロードし、電子メールのスパム攻撃の一部としてそのURLを拡散します。Google、Microsoft、Amazon、Dropboxなどの有名なサービスを利用することで、エンドユーザがリンクをクリックする確率が高くなります。

また、これらのサービスプロバイダを所属先とする、ワイルドカードSSL証明書の悪用も確認されています。クラウドプロバイダのトラフィックは安全だという前提でインスペクション対象から除外してしまうと、暗号化されたチャネル経由でマルウェアのペイロードが送り込まれたり、アンチスパムや電子メール保護、ファイアウォールなどを含むURLフィルタリングベースのセキュリティソリューションが機能しなくなります。**信頼できるクラウドベースのサービスでホスティングされている場合、従来型のメールセキュリティソリューションでは、不正ファイルへのリンクを含んでいるフィッシングメールをブロックできないのです。**

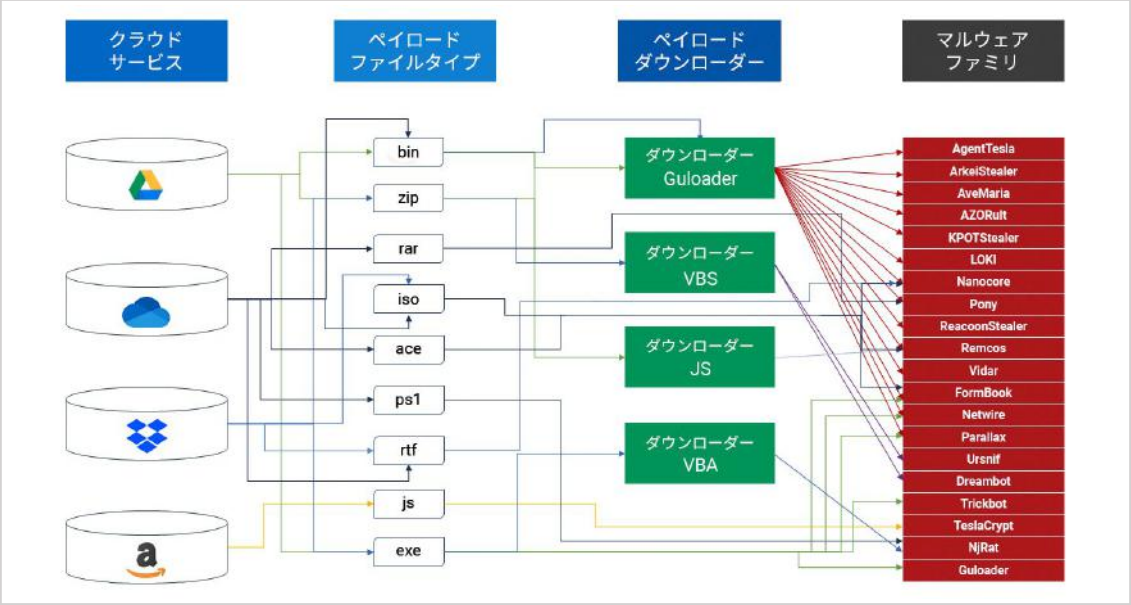


図5： クラウドサービスを使って送り込まれるマルウェアのペイロード

以下の例は、クラウドストレージサービス「OneDrive」のURLを示しています。この例では、最初の2件が不正URLで、「Trojan EdLoader」と「Backdoor LokiBot」というファミリに所属するマルウェアがダウンロードされます。ただし、3件目は正規のURLで、ユーザの実際のファイルがダウンロードされます。サブドメインとURI（Uniform Resource Identifier）はランダムな文字列パターンであるため、正規のURLなのか不正なURLなのかを判断することはできません。セキュリティエンジンは見えないものをブロックできません。これらのサービスを利用して送り込まれる不正ファイルをブロックする唯一の方法は、SSLインスペクションを実施することです。

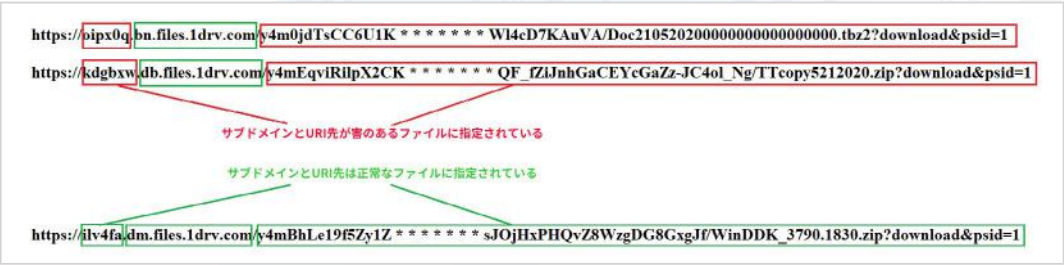


図6： サブドメインのランダムな文字列ではURLが不正か正規かを判断できない

モバイル攻撃

スマートフォンを標的とする攻撃も増えています。Webページのスプーフィングと同様、正規に見せかけた偽のアプリによる攻撃です。たとえば、Cerberus（ケルベロス）と呼ばれるAndroidの金融関係のトロイの木馬は、アプリケーション名とアイコンを使って、Google Playの正規のアプリケーションに見せかけ、ユーザを誘導します。疑いを持たないユーザがこの偽アプリをクリックすると、障害を持つユーザによるAndroidデバイスやアプリの使用を支援する「アクセシビリティサービス」の権限を取得するための通知が送信されます。

このエクスプロイトは、多くのユーザが通知をよく読まずに「同意する」をクリックしてしまうことを想定しています。「同意」をクリックすると、このアプリが画面に表示されている他のアプリのコンテンツを表示し、ユーザに気付かれることなく様々なアクションが実行されてしまいます。

このマルウェアによって、金融関係のアプリ、Gmail、またはGoogle認証システムの二要素認証アプリの認証情報が不正に取得され、外部に持ち出されています。それ以外に、音声を密かに録音したり、テキストメッセージを不正に取得したりすることもあるようです。アクセシビリティサービスへの権限をマルウェアによって取得された結果、さらに悪い状況に陥ると、ユーザがその権限を無効化できなくなり、場合によっては、アプリのアンインストールも困難になります。

図7: 偽のGoogle Playアプリ

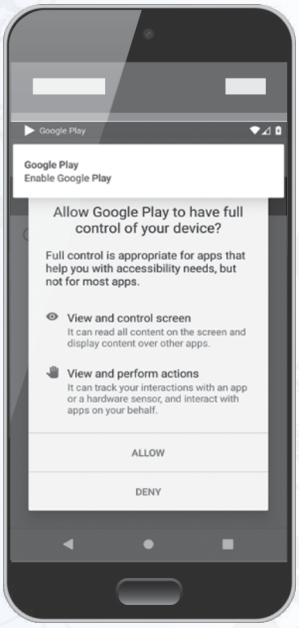
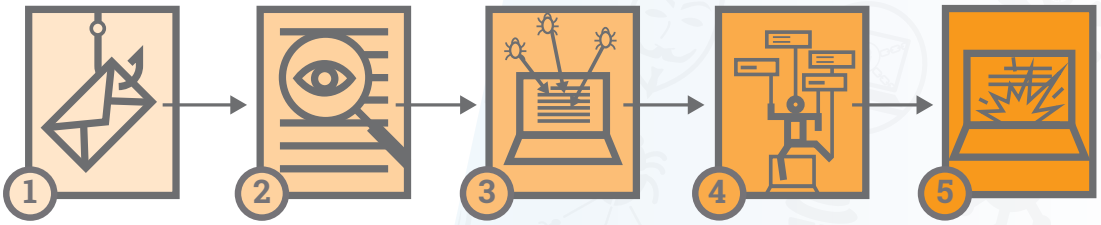


図8: 偽のGoogle Playアプリの通知

攻撃の分析



配信には、エクスプロイトやマルウェアが隠されたフィッシングメールが使用されます。ユーザがダウンロードしたり、メールのリンクをクリックしたりすることで、マルウェアが送り込まれます。

エクスプロイトは、プログラムがシステムの脆弱性を探し、コードを悪用して実行できる場合に発生します。

インストールは、マルウェアが被害者のマシンにロードされる場合に発生します。

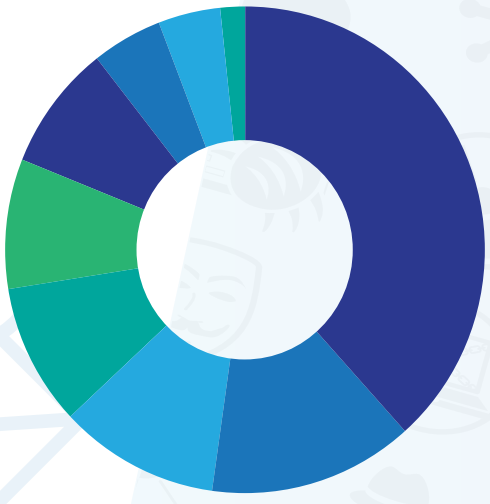
コマンド&コントロール(C&C)のコールバックとは、マルウェアがC&Cサーバとの通信を試行することであり、その目的は、多くの場合、何らかの指示を受け取ったり、不正取得したデータを送信したりすることです。

活性化とは、マルウェアが追加のマルウェアをインストールしたり、データを外部に持ち出したり、C&Cサーバがプログラミングした他のアクションを実行したりするステップのことです。

攻撃チェーンの分析

フィッシング

フィッシングは一般的に、認証情報を不正に取得するための、多段階のサイバー攻撃の第1段階です。ThreatLabZは、2020年1月から9月に暗号化されたチャネル経由で配信され、ゼットスケーラーのクラウドによって特定、またブロックされた、**1億9,300万件以上のフィッシング試行を分析しました。**これらの試行の業種別の内訳は以下の通りで、最も標的にされた業種は38.6%の製造で、13.8%のサービスがそれに続きました。施設によって異なるITインフラストラクチャやシステムが使用されていることから、脆弱性が高まっている可能性があります。



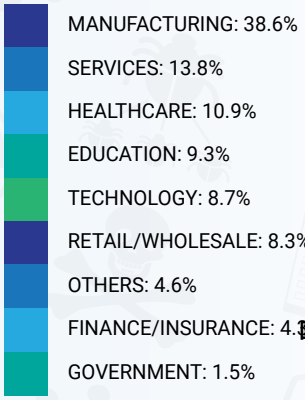


図9： 業種別の暗号化されたチャネル経由でブロックされたフィッシングの脅威

有名企業のサービスやブランドに見せかけたフィッシング

フィッシングの試行には、標的となるブランドに見せかけたWebサイトがよく使われます。電子メールを受け取ったユーザが指示に従ってリンクをクリックすると、偽のWebサイトに誘導され、ユーザ名やパスワードなどの重要な情報を入力するよう指示され、それらの情報がサイバー犯罪者による攻撃に使用されるというものです。

ThreatLabZの調査によると、フィッシングに最も多く悪用されているブランドはMicrosoftであることがわかりました。Office 365、SharePoint、OneDriveなどのMicrosoftのさまざまなWebプロパティに見せかけることで、企業のサービス認証情報を不正に取得しようとするというものです。2番目に多かったフィッシング攻撃は「テクニカルサポート」詐欺と呼ばれるもので、攻撃されたWebサイトから不正なWebサイトにリダイレクトされ、「ユーザのマシンがハッキングされた」というメッセージが表示され、クレジットカード情報を送信すればMicrosoftによるサポートが提供されるとして、クレジットカード情報を不正取得しようとする仕組みです。

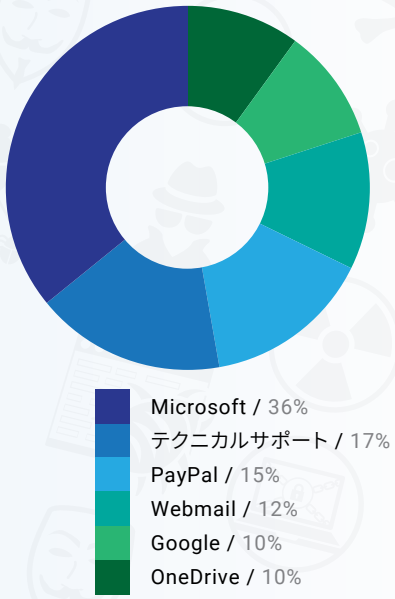


図10： フィッシングに悪用されることが多いブランドやサービス

また、PayPalやGoogleなどの有名ブランドのなりすましもフィッシング攻撃の上位に入りました。これらのなりすましサイトは実在するサイトに酷似しているため、偽物を見分けるのは極めて困難です。

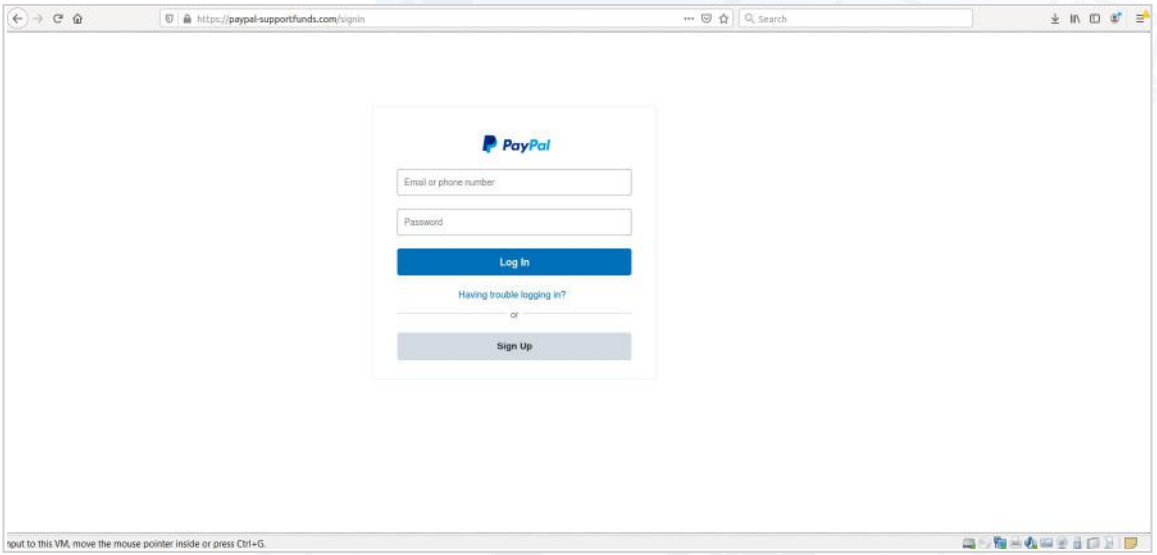


図11： HTTPSを使用するPayPalフィッシングサイト

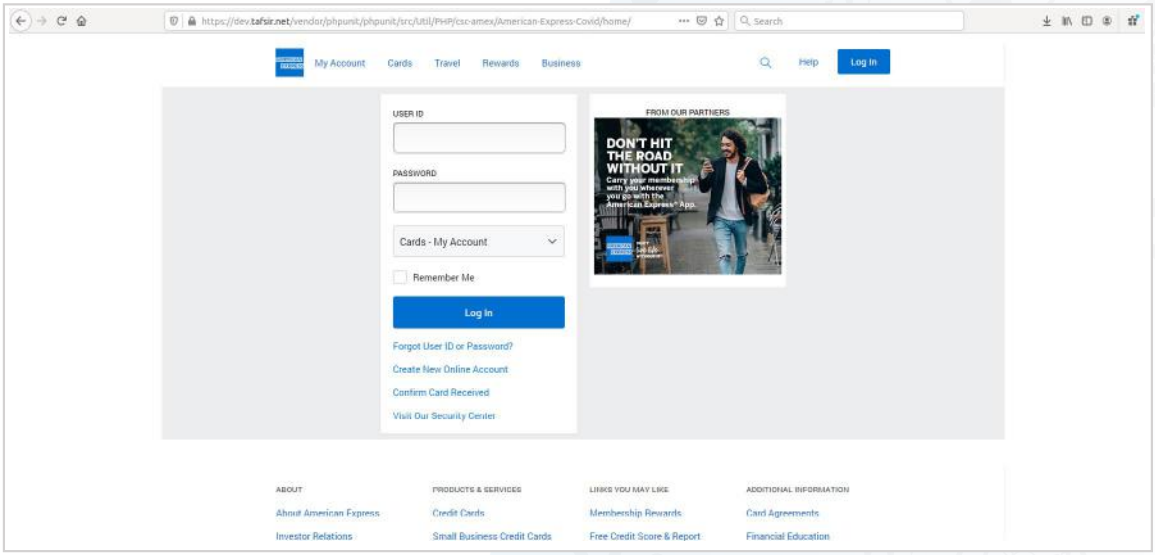


図12: HTTPSを使用するAmerican Expressのフィッシングサイト

HTTPSを使用するNetflixのフィッシング

Netflixなどのストリーミングエンターテイメントサービスの利用がパンデミックの渦中で増加しています。サイバー攻撃者はもちろん、それを十分に承知し、ストリーミングサービスを標的に、ユーザの認証情報のフィッシングを仕掛けています。図13でわかるように、これらの偽ページを本物のページと見分けるのは極めて困難です。

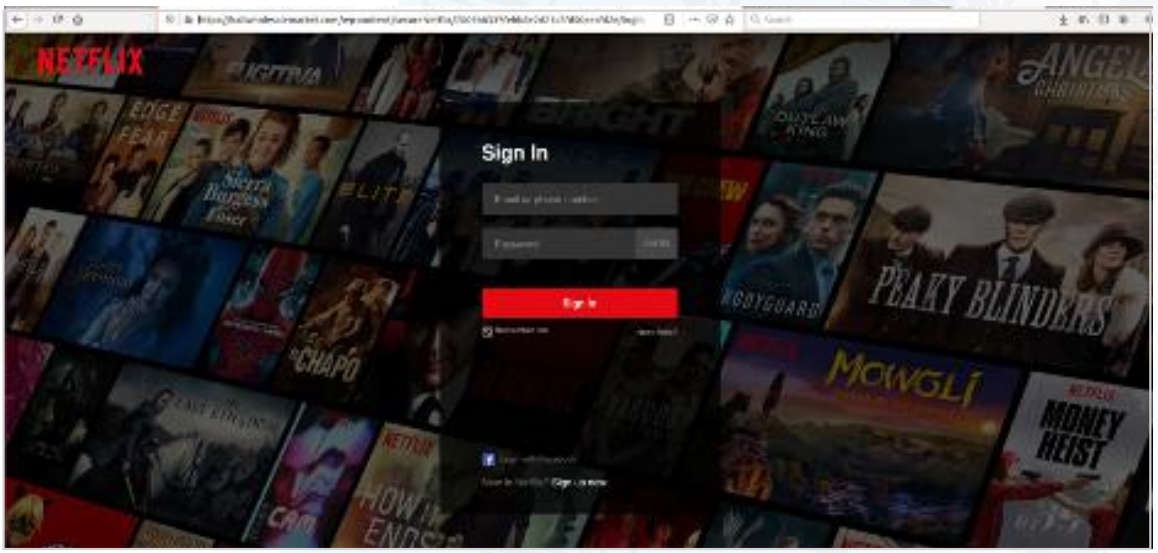


図13: Netflixのフィッシングの画像

Microsoftユーザを標的にし、HTTPSを利用したテクニカルサポート詐欺

図14は、Microsoftのテクニカルサポート詐欺ページの一例です。URLをクリックすると、Microsoftによって検証されたHTTPS証明書が表示されます。ここで使用されている証明書から、攻撃者がMicrosoftの有名ブランドであるAzureを利用することで、Microsoftから送信された正規のページであるかのように見せかけていることが分かります。

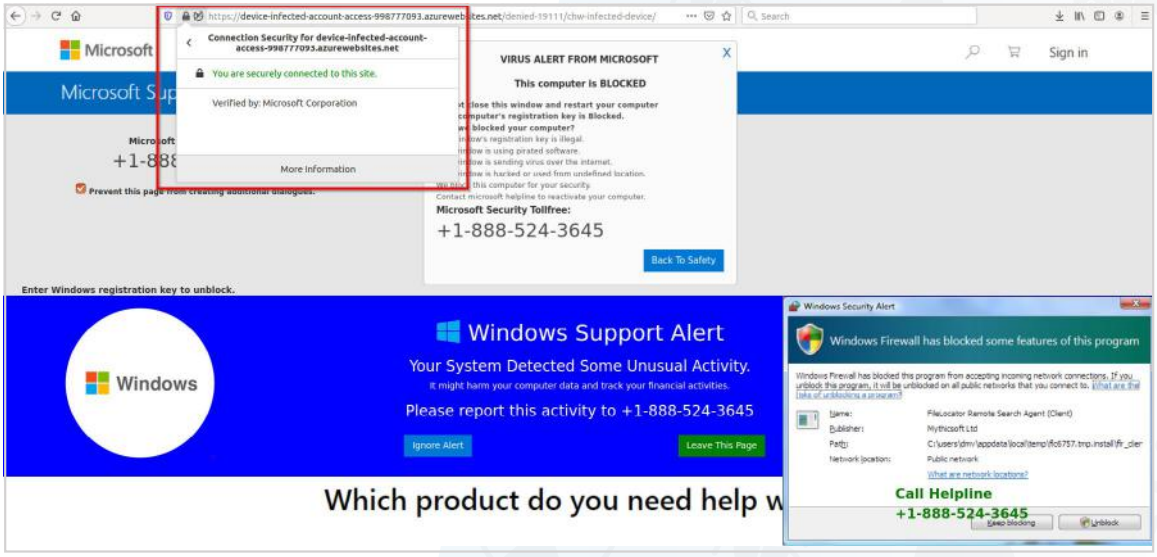


図14： Microsoftユーザを標的にし、HTTPSを利用したテクニカルサポート詐欺

ブラウザエクスプロイト

ブラウザエクスプロイトは、攻撃者がオペレーティングシステムの脆弱性を悪用し、ユーザに気付かれることなくブラウザ設定を変更することを可能にします。 ゼットスケーラーのクラウドでは、製造（26.5%）と金融・保険（19.9%）といった業界を標的とする、658,000件以上のブラウザエクスプロイトの脅威がブロックされています。

製造業がサイバー攻撃の標的になることが多いのは、（少なくとも過去からの傾向として）この業種は細かく分断されていて、施設ごとに異なるITインフラストラクチャや複数の連携していないシステムが使われているためです。 他の業種にも当てはまりますが、統合された管理と一元化された可視性とポリシーの適用がなければ、セキュリティは完全とは言えず、サイバー犯罪者にそれらのセキュリティホールを常に悪用されることになります。

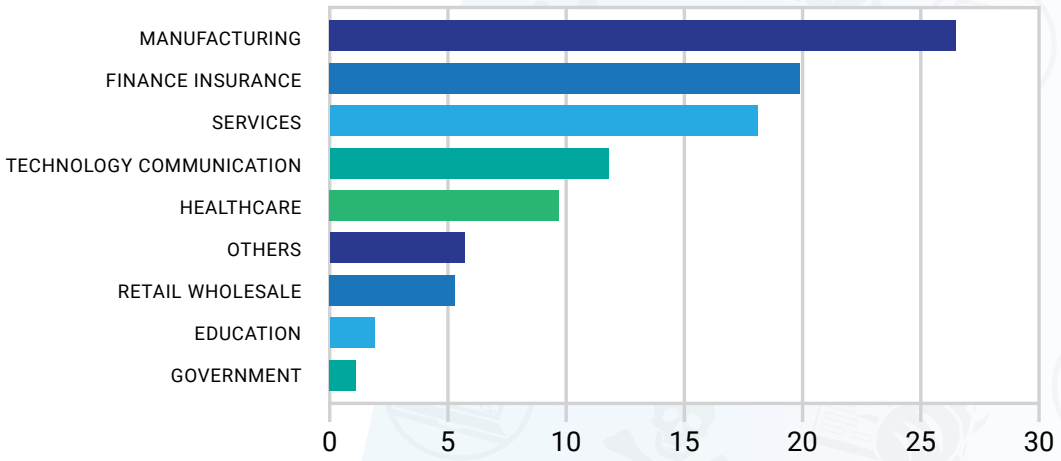


図15： 業種別の暗号化されたチャネル経由でブロックされたブラウザエクスプロイト

ランサムウェア

SSL/TLSチャネル経由で配信されるランサムウェア攻撃が2020年3月以降に5倍に増加したことが、ゼットスケーラーのThreatLabZによって確認されています。従業員の大半がリモートワークに移行し、社内のアプリケーションにアクセスするようになっていることから、被害や影響が大きく身代金を支払う可能性が高い業種を標的にするランサムウェアの活動が増加しています。

暗号化されたチャネル経由のランサムウェア攻撃で最も標的になった業種は、「テクノロジ・通信」(40.5%) と「医療」(26.5%) でした。

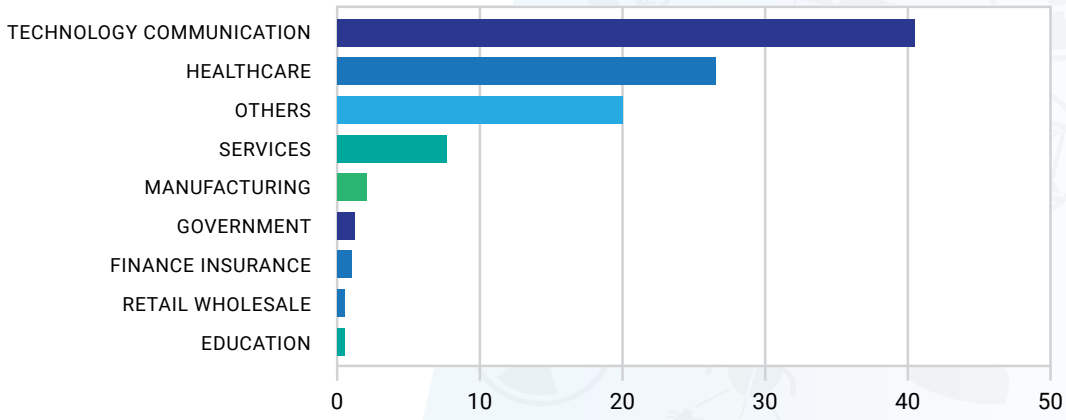


図16: 業種別の暗号化されたチャネル経由でブロックされたランサムウェア

これらの攻撃で最も多く見つかったランサムウェアファミリには、FileCrypt/FileCoderの亜種が含まれ、Sodinokibi、Maze、Ryukの亜種がそれに続きました。これらのランサムウェアファミリの亜種の多くにおけるこの1年間の注目すべきなのは、データを持ち出す機能が追加された点です。この新機能によって、ランサムウェアを悪用する犯罪者が、データが暗号化される前に機密データを外部に持ち出せるようになっています。ユーザの組織で適切にバックアップが実施されていた場合でも、持ち出されたデータが公開されるのを阻止するため、身代金を支払わざるを得ない状況に追い込まれるでしょう。

マルウェア

マルウェアは、サイバー犯罪者にとって持続的に使える手段となり、被害者のマシンへの継続的なアクセスを可能にします。マルウェアは多くの場合に、脆弱性を突いたエクスプロイトが成功したり、ソーシャルエンジニアリング攻撃を利用したりすることでインストールされます。マルウェアは、ゼットスケーラーの研究者が特定した中で最も多いタイプの攻撃です。今回の分析でも**26億以上のマルウェア脅威**がブロックされました。

個人識別可能情報（PII）を取り扱う業種がマルウェアの標的となることが多く、我々の分析で、暗号化されたチャネル経由でブロックされたマルウェア攻撃が最も多かった業種は、医療（27.4%）と保険（19.6%）でした。

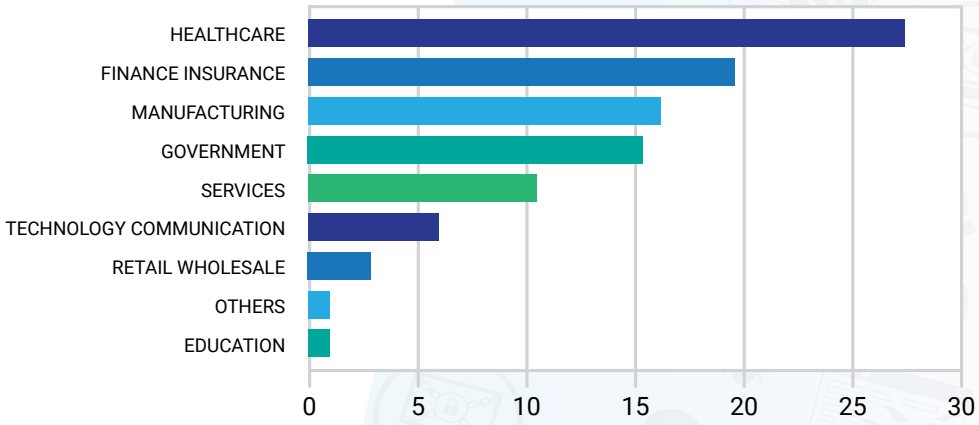


図17： 業種別の暗号化されたチャネル経由でブロックされたマルウェア

暗号化されたチャネル経由のマルウェアのコマンド &コントロール（C&C）活動

C&C通信は、攻撃チェーンにおけるもうひとつの重要な部分です。検知を逃れてエンドユーザのデバイスにインストールされたマルウェアは、C&Cサーバにコールバックすることで、データの外部への持ち出しなどを始めとする、さらなる攻撃を開始します。マルウェアのペイロードは多くの場合に、攻撃を開始する前にサーバからのコマンドを待機するようにプログラムされています。今回の分析で最も多く確認されたマルウェアファミリは、EmotetとTrickBotでした。

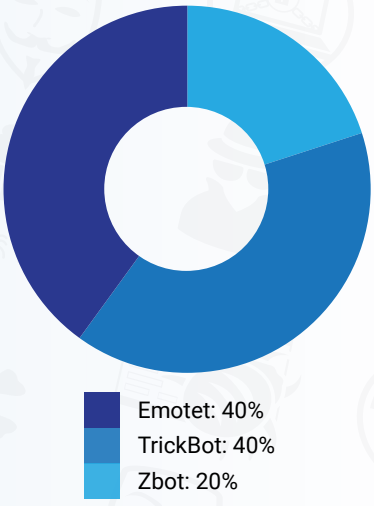


図18： 暗号化されたチャネル経由で最も多くブロックされたC&C活動

EmotetとTrickBotに加え、UrsnifとUnruyの活動も確認されました。Emotetはいずれの業種でも最も多く確認されましたが、TrickBotは金融・保険と公的機関で2番目に多く確認されました。また、Ursnifは医療や製造の業種の組織への攻撃で多く確認され、Unruyは教育機関への攻撃で2番目に多く確認されました。

マルウェアを理解する

Emotet:
Emotetは、初めて確認された2014年には金融関係のトロイの木馬でしたが、変異を経て極めて顕著な脅威へと生まれ変わり、主としてスパムや標的システムへのマルウェアのダウンロードに広く使用されるようになりました。米国土安全保障省（CISA）はEmotetのことを、公的機関と民間企業の両方が影響を受け、**最もコストがかかり、強力な破壊力を持つ**マルウェアの1つであると説明しています。Emotetは、定期的な機能強化によって組織による検知を困難にする能力を身に着け、優れた耐性とモジュール性を備えていることがわかっています。

TrickBot:
TrickBotは、金融関係のトロイの木馬であるDyreの後継で、今日の脅威環境で最も広範囲に拡散し、最も危険なマルウェアの1つです。TrickBotは、他のタイプのマルウェアと併用される場合も多く、標的であるホストに侵入するための初期感染ベクトルとして使用されたり、他のマルウェアファミリをダウンロードして感染の効果を最大限にする目的で使用されています。

Ursnif:
Ursnifは、Dreambotとも呼ばれるGoziマルウェアファミリで最も活発に活動し、広範囲に拡散している亜種の1つです。このトロイの木馬の一般的な拡散方法は、エクスプロイトキット、電子メールの添付ファイル、不正リンクです。

Unruy:
Unruyは、コンテキストに関係なく広告を表示し、アドクリックを実行することで利益を得ようとするトロイの木馬です。リモートホストと通信し、任意のファイルをダウンロードして何らかの行動を実行する場合もあります。

暗号化された脅威のブロックに何が必要か

SSLトラフィックが必ずしも安全なトラフィックではないことを認識することが、これまで以上に重要です。暗号化の利用の拡大に伴い、攻撃側も暗号化を悪用し、攻撃を隠すようになったことから、暗号化トラフィックのインスペクションがより一層求められています。多くの組織がセキュリティのベストプラクティスに従い、インターネットトラフィックを暗号化していますが、次世代ファイアウォールなどの従来型のツールは、多くの場合、大量のSSLトラフィックのインスペクションを実行する十分なパフォーマンスや能力を持ち合わせていません。もちろん、業務やワークフローを停止させることはできないため、多くのITチームが、暗号化トラフィックのほとんどに対してインスペクションを行っていません。

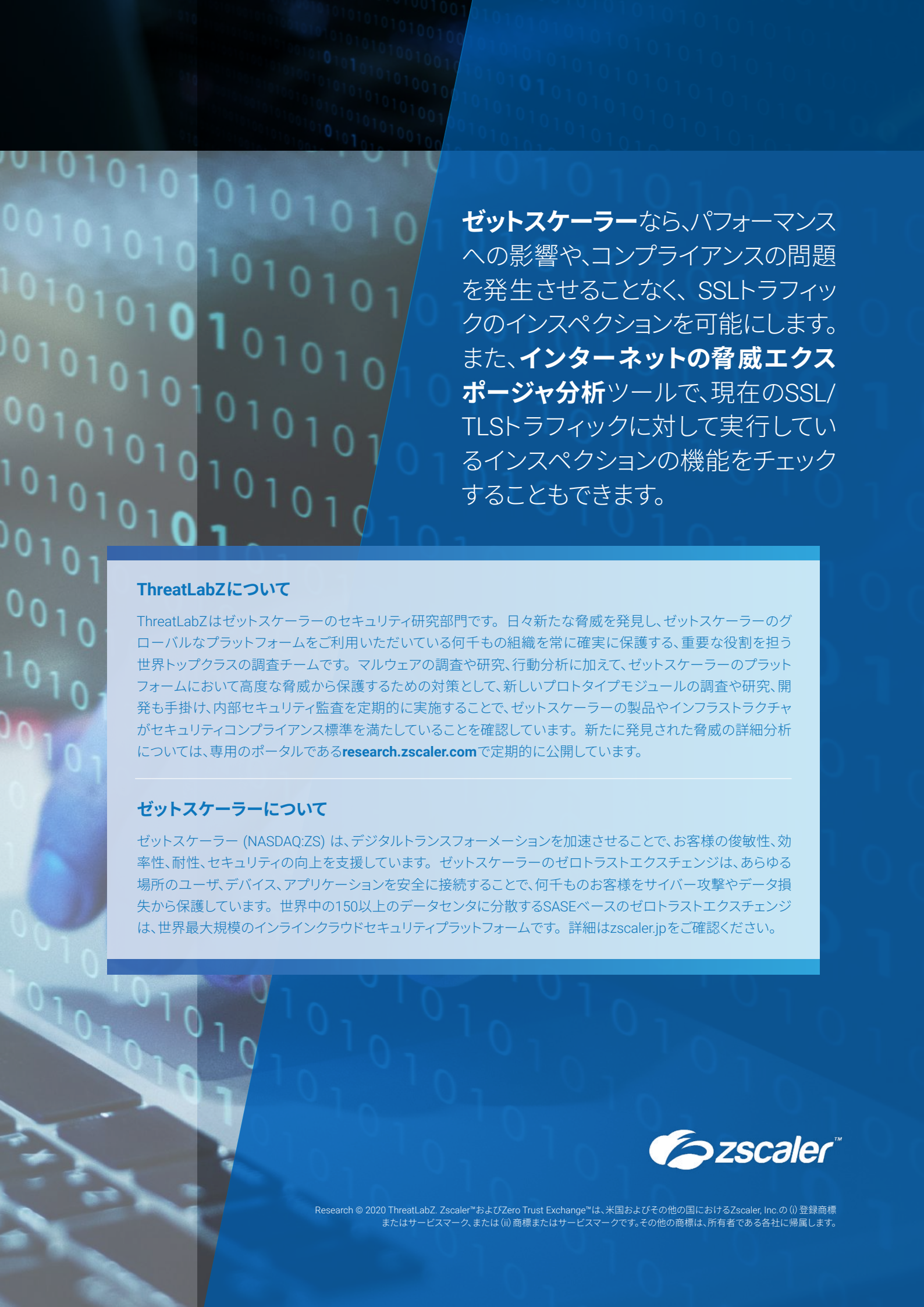
さらには、顧客や患者などの個人情報が含まれるデータの取り扱いについては、厳しい法規制が存在します。データのタイプごとにインスペクション方法についてのポリシーを個別に作成し、異なる場所にそれを複製するのは困難であるため、このプロセスを完全に省略してしまう組織も少なくありません。

それでは、パフォーマンスを低下させることなく、暗号化トラフィックに隠れる脅威から組織を保護するには、どうすればよいのでしょうか？　企業のトラフィックの大半が暗号化されるようになった今、以下のような要件を満たす方法で、オンネットワークとオフネットワークのすべてのユーザのコンプライアンスを維持しつつ、すべてのトラフィックを確実に復号化してインスペクションを行う必要があります。

- **すべてのSSLトラフィックの脅威を復号化、検知、防止する -** クラウドネイティブでプロキシベースのアーキテクチャを採用することで、すべてのユーザの、すべてのトラフィックに対しインスペクションを行います。
- **未知の攻撃を隔離し、それまでに見つかったことのないマルウェアもブロックする -** ファイアウォールベースのパススルーアプローチではなく、AIの活用によって隔離を図ることで、疑わしいコンテンツをストップし、分析します。
- **すべてのユーザ、すべての場所に一貫性あるセキュリティを提供する -** 自宅、本社、外出先のいずれの場所でも、すべてのユーザに対して常に強力なセキュリティを提供します。
- **攻撃対象領域を瞬時に減らす -** ゼロトラストベースで水平移動の可能性を排除します。アプリを攻撃者から見えなくし、許可されたユーザも、ネットワーク全体ではなく必要なリソースだけに直接アクセスするようにします。

これらを可能にするソリューションに必要なスケーラビリティとパフォーマンスを提供できるのは、ゼットスケーラーのゼロトラストエクスチェンジのような、クラウドネイティブかつプロキシベースのアーキテクチャだけです。クラウドベースのセキュリティプラットフォームであれば、コンピューティングリソースの柔軟な拡張によって復号化とインスペクションの要求に対応し、複数の場所に一貫性あるポリシーを適用できます。ゼットスケーラーは、サービスのプラットフォームの一部としてSSLインスペクションをスケーラブルに実行し、トラフィックの増加に合わせて即座に処理能力を追加できます。アプライアンスは一切不要です。

どの業種もセキュリティの脅威と無縁ではありません。さらには、暗号化トラフィックの増加に伴い、このトラフィックのインスペクションが極めて重要になっています。暗号化トラフィックに隠れる脅威の拡大を防ぐには、SSLインスペクションを完全サポートする多層型で確実な防御が不可欠です。



ゼットスケーラーなら、パフォーマンスへの影響や、コンプライアンスの問題を発生させることなく、SSLトラフィックのインスペクションを可能にします。また、**インターネットの脅威エクスポージャ分析**ツールで、現在のSSL/TLSトラフィックに対して実行しているインスペクションの機能をチェックすることもできます。

ThreatLabZについて

ThreatLabZはゼットスケーラーのセキュリティ研究部門です。日々新たな脅威を発見し、ゼットスケーラーのグローバルなプラットフォームをご利用いただいている何千もの組織を常に確実に保護する、重要な役割を担う世界トップクラスの調査チームです。マルウェアの調査や研究、行動分析に加えて、ゼットスケーラーのプラットフォームにおいて高度な脅威から保護するための対策として、新しいプロトタイプモジュールの調査や研究、開発も手掛け、内部セキュリティ監査を定期的に実施することで、ゼットスケーラーの製品やインフラストラクチャがセキュリティコンプライアンス標準を満たしていることを確認しています。新たに発見された脅威の詳細分析については、専用のポータルである**research.zscaler.com**で定期的に公開しています。

ゼットスケーラーについて

ゼットスケーラー (NASDAQ:ZS) は、デジタルトランスフォーメーションを加速させることで、お客様の俊敏性、効率性、耐性、セキュリティの向上を支援しています。ゼットスケーラーのゼロトラストエクスチェンジは、あらゆる場所のユーザ、デバイス、アプリケーションを安全に接続することで、何千ものお客様をサイバー攻撃やデータ損失から保護しています。世界中の150以上のデータセンタに分散するSASEベースのゼロトラストエクスチェンジは、世界最大規模のインラインクラウドセキュリティプラットフォームです。詳細はzscaler.jpをご確認ください。

zscaler™