Cisco 2016
中期サイバーセキュリティ レポート

目次

要約および主な調査結果

防御側は攻撃者の活動時間を削減しなければなりません。
それが攻撃を成功させないための鍵です。

攻撃者は現在、時間に制限されることなく活動しています。攻撃者のキャンペーンでは既知の脆弱性を利用することがよくありますが、その脆弱性は、組織やエンド ユーザが把握して対処する機会があり、またそうすべきであったものです。こうしたキャンペーンは数日間や数ヵ月間、またはそれ以上の長期にわたって検知されずに活動し続ける場合があります。その間、防御側では、脅威のアクティビティを確認し、既知と新規の両方の脅威の検出時間（TTD）を短縮しようと苦戦します。進展を遂げているのは明らかですが、それでも敵が攻撃の基盤を構築する能力を実質的に削いで、有益な強い打撃を与えるというには、ほど遠い状態にあります。

シスコ 2016 年中期サイバーセキュリティ レポートでは、シスコ セキュリティ リサーチによる調査、洞察、および見解を示し、以前のセキュリティ レポートで調査した動向の最新情報をセキュリティ プロフェッショナルに提供し、今年後半のセキュリティ状況に影響すると思われる展開を取り上げます。

地下経済内の最新の動向を調査した結果、攻撃者の関心は収益の獲得に集中していることがわかりました。中でもランサムウェアは効果的に金銭を得ることができ、一部の攻撃者にとって企業ユーザは格好の標的となっていると思われます。本レポートで取り上げる脅威およびセキュリティ トレンドの多くは、ランサムウェアに関連するものです。キャンペーンの実行や攻撃者の活動の隠蔽に使用されるテクニックから、この影響力のある脅威の次世代がどのように進化するかという予測について、説明します。

本レポートでは、組織が防御を強化するために講じることができ、また講じるべき、数々の対策を検証します。シスコの調査担当者からの推奨事項の一部を以下に示します。

- ランサムウェア攻撃を受けた後、通常業務の運用にすばやく切り替えられるインシデント対応計画を策定してテストする。
- HTTPS 接続および SSL 証明書を盲目的に信頼しない。
- 重要なインターネット インフラストラクチャのコンポーネントであるスイッチおよびルータを含めて、ソフトウェアおよびシステムに存在する公開された脆弱性に即座にパッチを適用する。
- 悪意のあるブラウザの感染の脅威についてユーザを教育する。
- 実用的な脅威インテリジェンスとは本当は何かを理解する。

このレポートでは、4 つの主なトピックを取り上げます。

I. 注目のサイバー犯罪トレンド：ランサムウェア

シスコのセキュリティ調査担当者は、ランサムウェアに焦点を当て、このタイプのマルウェア攻撃がこれほどまでに広く流行した原因と考えられる技術を調査しました。過去の動向の分析に基づくランサムウェアの進化の予測についても説明します。さらに、パッチが適用されていないシステムや旧式のデバイスにおける脆弱性が、攻撃者に活動する時間を与えていることも検討します。ランサムウェアの実行者は、今や企業ユーザを標的としています。そのため、組織は、重要なデータを保護された場所にバックアップし、攻撃を受けた後はできる限り迅速に通常のビジネス業務に戻れる、実用的な計画を策定しなければなりません。

II. 活動するための時間

このセクションでは、攻撃者が脅威を考案してキャンペーンを実行に移す時間と機会を提供する、クライアント側の攻撃ベクトルについて考察します。暗号化や認証を伴う脆弱性の増加は、脅威アクターが安全な接続の改ざんを狙っている兆候です。多様なデータ セットへのアクセスを試みるオンライン犯罪に対するサーバ エクスプロイトの台頭など、エクスプロイト キットや攻撃ベクトルにおける動向を調査します。「サービスとしてのマルバタイジング」の登場とそれによって生じる防御側への複雑性、そして Web ユーザは誰が保護すべきかという問題についても、議論します。

III. 保護するための時間

このセクションでは、シスコのセキュリティ調査担当者が攻撃者の活動とセキュリティ対策との間のギャップについて考察します。たとえば、ベンダーは公開された脆弱性の通知からパッチの提供までの期間を短縮していますが、ユーザがこのようなパッチを適用するまでに時差が生じています。このセクションでは、検出時間（TTD）の中央値を短縮するためのシスコの絶え間ない取り組みの最新情報と、攻撃者と防御側の「軍拡競争」の影響についても取り上げます。シスコの調査担当者は、悪意のあるキャンペーンでの HTTPS の利用の増加と、悪意のあるユーザによる Transport Layer Security（TLS）を使用した通信の暗号化についても、詳しく述べています。

IV. グローバルな視点およびセキュリティの勧告

このセクションでは、セキュリティに関連する現状の地政学的な動向を、脅威の理解とデータの管理またはアクセスのために、テクノロジーの変化に対応するという課題への政府の関与の増大を含めて、考察します。攻撃者の活動時間を短縮するための防御側への推奨事項も提示しています。さらに、侵害の指標（IOC）と脅威インテリジェンスとの重大な違いについても説明します。

主な発見

- ランサムウェアはマルウェア市場の大部分を占めています。新しい脅威ではありませんが、過去最高の収益性を誇るマルウェアに発展しています。また、一部のランサムウェア実行者は企業を標的に選ぶようになっています。2016 年上半期において、個人および企業ユーザの両方を標的とするランサムウェア キャンペーンはその感染範囲を広げ、影響力を強めています。今後の展望として、ランサムウェア キャンペーンの効果を最大化し、攻撃者が多大な利益を生み出す可能性を高める、さらに効率的で迅速に拡大する感染手段が生み出されます。
- エクスプロイト キットはランサムウェアの存在をこれほどまでに広める一助となりましたが、Adobe Flash の脆弱性を引き続き利用します。先頃、シスコの調査担当者が有名な Nuclear エクスプロイト キットを調査したところ、成功したエクスプロイト試行の 80 % に Flash が関与していました。
- 企業アプリケーション ソフトウェア JBoss に存在する脆弱性は、攻撃者がランサムウェアなどのキャンペーンを実行するために使用できる新たなベクトルの供給元となっています。シスコの調査では、JBoss 関連の侵害によってサーバ内に重大な影響が及び、攻撃に対して脆弱性が生じています。
- 2015 年 9 月から 2016 年 3 月にかけて、シスコのセキュリティ調査担当者は悪意のあるアクティビティに関連する HTTPS トラフィックが 5 倍に増加したことを確認しました。この種の Web トラフィックの増加は、主に悪意のある広告インジェクタおよびアドウェアに起因すると考えられます。脅威アクターは HTTPS で暗号化されたトラフィックの使用を増加することで、Web 上での活動を隠蔽し、活動時間を延長しようとしています。
- 大手ソフトウェア ベンダーからは、脆弱性の通知とほぼ同時にパッチが公開されてはいますが、シスコの調査によると、多くのユーザはこれらのパッチを適時にダウンロードしてインストールしていません。このようなパッチの公開と実際の実装との時間差は、攻撃者がエクスプロイトを開始するには十分な期間です。
- 老朽化したインフラストラクチャを適切に維持しなかったり、脆弱なオペレーティング システムにパッチを適用しなかったりすることで、組織が生み出すセキュリティ リスクに注意を向けさせるために、シスコの調査担当者は、シスコのデバイスのサンプル セットを調査し、基盤のインフラストラクチャで実行される既知の脆弱性の年代を確認しました。その結果、このようなデバイスの 23 % に、2011 年に端を発する脆弱性があり、16 % 近くに 2009 年に最初に公開された脆弱性がありました。
- ネットワーク トラフィックの暗号化に使用されているプロトコルである Transport Layer Security（TLS）を不正なアクターが使用してアクティビティを隠蔽していることを示すマルウェアのサンプルが、少数ではありますが増加しています。このため、ディープ パケット インスペクションがセキュリティ ツールとして有効に機能しなくなってしまうので、セキュリティ プロフェッショナルの悩みの種となっています。機械学習法と新しいデータ ビューを組み合わせることで、この動向に対する高品質な情報が得られます。
- 2015 年 12 月から 2016 年 4 月の期間で、シスコは TTD 中央値をおよそ 13 時間に短縮しました。これは、現在の業界の推定値である 100 ～ 200 日という許容できない値を十分下回るものです。同期間内に確認された TTD の増減は、攻撃者が新しい脅威を休みなく連続して繰り出し、セキュリティ ベンダーが特定にすばやい対応を迫られるという、攻撃者と防御側の間で継続される、白熱した「軍拡競争」を如実に表しています。

はじめに

防御側がシステムを保護する方法は、攻撃者が活動する方法と同じではありません。防御側ではオンライン犯罪者に対抗するための戦略やツールを発展させていますが、攻撃者の活動時間を制限するには至っていません。

問題は可視性の欠如で、ユーザは攻撃にさらされています。セキュリティ プロフェッショナルは、ポイント ソリューションと「トリアージ」アプローチに頼っており、セキュリティの課題を全体的に見るのではなく、あちこちで発生する攻撃を阻止しようとしているので、攻撃者が有利な立場になります。

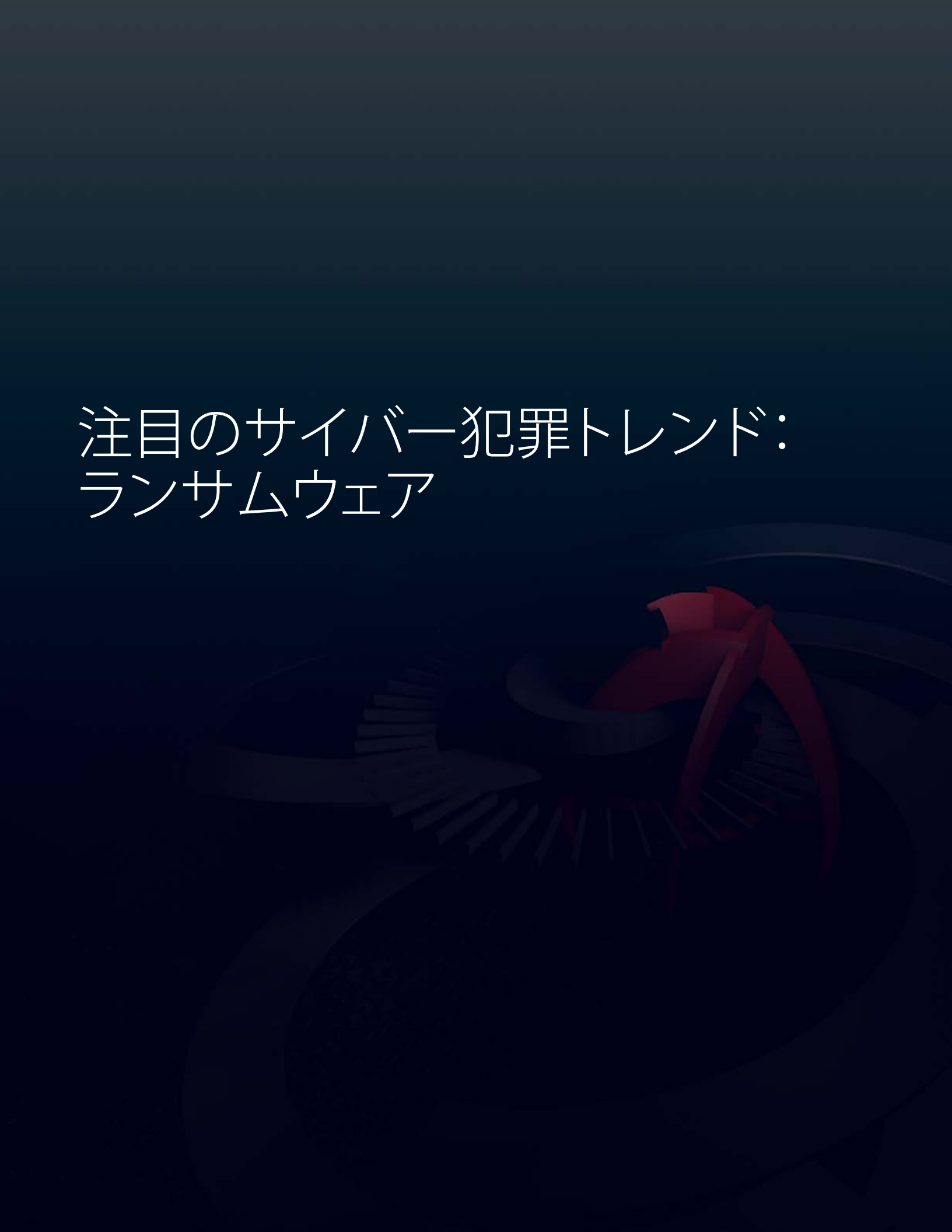
攻撃者には時間の余裕があるので、インフラストラクチャ、システム、導入されたが保守されていないか単に長い間忘れられているデバイスの脆弱性を突き止めて、利用できます。ネットワークに足場を築いて、水平方向に移動できます。サーバベースのキャンペーンを開始して、活動の拠点とするスペースを広げ、投資回収率を向上することができます。

「防御側が脆弱性パッチの適用やインフラストラクチャのアップグレードにかかる時間を減らし、その時間で自由にツールを改善できれば、攻撃者があぶりだされ、その結果、攻撃者の活動スペースを抑え込んで完全に封じ込むこともできます」

時間の面で優位ではあっても、攻撃者は活動方法を制限されています。多数の手段があるのは、ネットワークへの侵入方法だけです。防御側が自由にツールを改善して、脆弱性へのパッチ適用とインフラストラクチャのアップグレードに必要な時間を短縮すると、攻撃者が既知になり、防御側は攻撃者の活動スペースを封じ込め、さらには閉鎖することもできます。また防御側は、セキュリティ環境の全体像を把握できます。攻撃者が存在するかどうか、どのように侵入したのか、どのシステムへの侵入に成功したか（あるいは失敗したか）を、悪意のあるアクティビティを特定する際に知ることができます。

しかし、防御側は、あまりに多くのレベルでネットワークをセキュリティ保護する責任で手いっぱいとなり、最初の手段としてトリアージ アプローチを採用することになります。こうした対応では、攻撃者が、実行する時間と、攻撃者にとって最も容易なパスを防御側がブロックできなかったという利点が相まって、キャンペーンを強化することを許してしまいます。このようにしてランサムウェアは、攻撃者が防御を破って金銭的利益を得る、「最悪の状況」を招きます。しかも、ランサムウェアは増加し、対応が困難になっています（**7 ページ**の「ランサムウェア：脅威的なスタミナで莫大な金を生み出す」を参照）。

注目のサイバー犯罪トレンド：ランサムウェア



注目のサイバー犯罪トレンド：ランサムウェア

ランサムウェアはマルウェア市場の大部分を占めています。新しい脅威ではありませんが、過去最高の収益性を誇るマルウェアに発展しています。2016 年上半期において、個人および企業ユーザの両方を標的とするランサムウェア キャンペーンはその感染範囲を広げ、影響力を強めています。

医療業界における複数の組織を含む、企業に対して行われた先頃のランサムウェア攻撃の成功により、今後、多くの攻撃者による同様のキャンペーンの計画が誘発される可能性があります。ネットワークおよびサーバ側の脆弱性は、業界全体に影響を及ぼす可能性のあるランサムウェア キャンペーンを、攻撃者が誰にも気付かれずに実行するチャンスとなります。

ランサムウェア：脅威的なスタミナで莫大な金を生み出す

ランサムウェアのバリエーションは数十種類もあり、言語固有のものも多数あり、すべてが復元性を備えています。この分野における革新者、すなわち、CryptoLocker や CryptoWall などの著名なランサムウェア ブランドの作成者は、暗号化の面で健全なファイル暗号化を取り入れることで、マルウェアの効果を一段と引き上げました。現在、既知のランサムウェアの大部分は容易に復号することができず、多くの場合、被害者には要求された金額を支払う以外に手立てはないと言えます。

攻撃者は通常、ビットコインでの支払いを求めます。ビットコイン アドレスのユーザは匿名性を維持できるので、仮想通貨は、意図せずにランサムウェア業界の繁栄に手を貸すことになってしまいました。セキュリティ研究者を悩ますもう 1 つの複雑性は、ほぼすべてのランサムウェアにおける情報交換は、インターネット アノニマイザーである Tor を通じて行われることです。ビットコインは分割することもできるので、攻撃者は 1 つのビットコインからチーム全体に、便利で、しかも実質的に追跡できない方法で支払いが可能です。

ランサムウェアの新しいベクトル

電子メールや悪意のある広告（マルバタイジング）は、ランサムウェア キャンペーンの主要なベクトルです。ただし、一部の脅威アクターは、ネットワークおよびサーバ側の脆弱性を利用するようになっています。

今年初めに、医療業界を標的としたと思われる拡散したキャンペーンは、Samas/Samsam/MSIL.B/C（「SamSam」）ランサムウェアのバリエーションを利用しており、侵害されたサーバを通じて拡散されました。脅威アクターはサーバを使用してネットワーク中を移動し、さらに別のマシンを侵害して、そのマシンを身代金のために拘束しました。

攻撃者は JexBoss（JBoss アプリケーション サーバの開発/テスト用オープンソース ツール）を利用して組織のネットワークに足場を築きました。いったんネットワークにアクセスできれば、攻撃者は SamSam ランサムウェア ファミリを使用して複数の Microsoft Windows システムの暗号化を始めます。

「ランサムウェアは、次の段階ではさらに範囲を広げて強力になることが予想されています。組織とエンド ユーザは今すぐ重要なデータをバックアップし、それらバックアップが危険にさらされることがないように準備する必要があります」

多くの面で、SamSam 攻撃は必然的でした。多くの組織では、脆弱性にパッチを適用せずに JBoss サーバを運用していたからです（**18 ページ**の「JBOSS：インフラストラクチャ内の脆弱性が攻撃者に活動時間を与える」を参照）。2016 年 4 月の調査では、シスコは、少なくとも 2100 台の JBoss サーバがすでに侵害されており、悪意のあるアクターが悪用できる状態にあったと報告しています。すべての組織は、サーバをオフラインにして、即座にアップグレードするよう、通告されました。

脆弱なインターネット インフラストラクチャは広範囲に存在する問題です。企業だけでなく、業界全体をも標的とするマルウェア キャンペーンをひそかに実行する方法として、このチャネルを悪用する脅威アクターが増加することは、想像するに難くありません（**30 ページ**の「老朽化したインフラストラクチャ：ランサムウェアの増加により長期にわたる脆弱性へのパッチ適用が急務に」を参照）。

もう 1 つの新たな懸念：データの整合性

ランサムウェアの標的にされたユーザおよび企業は、攻撃者を信頼しなければならないという、苦境に立ちます。身代金を支払えば簡単に物事が進み、他に手段はないように思われますが、ランサムウェアの被害にあったユーザは、ファイルは復号化できず、失われることさえあると理解しておくことが大切です。あるランサムウェアのバリエーションの初期バージョンにはバグがあり、身代金を払ったのにファイルは失われる結果となりました。

また、攻撃者がファイルを乗っ取っている間に意図的にファイルを改ざんするというリスクもあります。医療記録や技術設計など、暗号化されるファイルの種類に応じて、データの改ざんや盗難による副次的影響は災難をもたらします。

再感染の可能性もまた懸念の 1 つで、ランサムウェアが同じユーザの同じマシンを 2 回攻撃した例が確認されています。場合によっては、身代金の金額は 2 回目には減額されており、いわば得意客向けの割引が適用された形になっています。攻撃者は反対のアプローチを取ることもあります。つまり、最初に要求した金額の支払いをユーザが渋った場合、身代金を引き上げるというものです。

ランサムウェアは非常に効率的で収益性も高くなったため、手軽に利益を得る手段としてランサムウェアを利用する攻撃者が増加することは明らかです。当然ながら企業は攻撃者にとって、個人のエンド ユーザが支払える額を大幅に上回る金額を要求するチャンスになります。ランサムウェアの標的となった組織または業界に対する潜在的な損害とコストも、はるかに大きくなるのも明らかです。

次世代のランサムウェアでは、さらに感染力と復元性が強化されると予測しています（**9 ページ**の「ランサムウェアの進化：自己増殖」を参照してください）。組織とエンド ユーザは、重要なデータをバックアップし、これらのバックアップが侵害されないよう確認して、今すぐ準備を始めるべきです。また、バックアップ データが実際に、攻撃後に速やかに復旧できることも確認する必要があります。企業の場合、復元は大規模な作業になります。したがって、潜在的なボトルネックを事前に突き止めておくことが重要です。また、インターネット インフラストラクチャとシステム内の既知の脆弱性にパッチが適用されていることを確認する必要があります。

SamSam キャンペーンと JBoss の脆弱性の詳細については、以下の Cisco Talos のブログ投稿をご覧ください。

「SamSam：治療は身代金を支払った後で」

「JBoss バックドアが深刻な脅威として拡散中」

ランサムウェアの進化：自己増殖

SamSam 攻撃は、ランサムウェアのターゲットが、個々のエンドユーザからネットワーク全体に移行していることを示すものです（**16 ページ**参照）。SamSam の増殖方法は、シンプルながら非常に効果的です。SamSam が成功していることから、攻撃者がさらに高速で効果的な増殖方法を開発して、効果を最大化し、身代金支払いの可能性を高めるようとするのも時間の問題です。

シスコのセキュリティ調査担当者は、現時点で見受けられるトレンドと進歩に基づいて、この分野のイノベーターにとって自己増殖型ランサムウェアが次のステップになると予測しています。またユーザには、ただちにそれに備えることを強く求めています。攻撃者は今年初めに JBoss バック ドアを利用して、医療業界の組織に対するランサムウェア キャンペーンを開始しました。これは攻撃者に時間を与えてしまうと、彼らはネットワークとユーザを侵害する新たな方法を見つけ出してしまうことを意味します（パッチを適用しないまま長期間放置されていた脆弱性を悪用するなど）。

自己増殖型マルウェアは新しいものではなく、ワームやボットネットの形式で十数年前から存在しています。これらの脅威の多くは拡散し、まだ有効な状態にあります。自己増殖型マルウェアには次のような特徴があります。

- **広範に導入された製品の脆弱性を利用する：**これまでで最も脅威を振るったワームでは、インターネットに広範に導入された製品の脆弱性が利用されています。
- **利用可能なすべてのドライブに複製される：**一部の種類のマルウェアは、ネットワーク ドライブや USB ドライブなどのローカル ドライブとリモート ドライブを特定し、それらのドライブに自身をコピーして、拡散と存続の手段にします。それによって、オフライン システムや、パブリック インターネット経由では到達できないシステムへの感染を可能にします。
- **ファイルに感染する：**ファイル感染型マルウェアは、自身をファイルの先頭や末尾に追加します。特に、Windows SFC または SFP（System File Checker、System File Protector）によって保護されていない実行ファイルに自身を追加します。ワームによっては、非実行ファイルに自身を追加して拡散する場合もあります。
- **限定されたブルート フォース アクティビティ：**これまでにこの方法を試みたワームは少数です。
- **回復力の高いコマンド アンド コントロール：**ワームによっては、コマンド アンド コントロール インフラストラクチャの妨害に通常使用されるアクションを考慮して、そうした妨害を回避する事前対策を導入する場合があります。ワームには多くの場合、コマンド アンド コントロール インフラストラクチャがありません。単純なデフォルト アクションによって、可能な限りすばやく拡散するだけです。
- **他のバックドアを使用する：**一部のマルウェア作成者は、システムに他の感染が発生している可能性を認識した場合、そのようなバックドアに便乗して自身が作成したマルウェアを拡散します。

「シスコのセキュリティ研究者は、トレンドとこれまでの進歩を考えた結果、ランサムウェアの次のステップは自己増殖型だと予想しています。ユーザはただちにこの状況に対応できるように備える必要があります」

KING'S RANSOM フレームワーク

ランサムウェアのイノベーターの手法を見ると、次世代型ランサムウェアを開発する攻撃者は、モジュール型設計のソフトウェアを利用する傾向があります。このタイプのアーキテクチャは、多くの一般的なオープン ソース型の侵入テスト スイートに見られます。このアプローチでは、攻撃者は必要に応じて特定の機能を使用できます。効率性が高く、新たな方法が検出されるか現在の方法で効果がなかった場合に、攻撃者は戦術を切り替えることができます。

シスコでは、次世代型ランサムウェア フレームワーク（シスコでは King's Ransom フレームワークと呼ぶ）には次のようなコア機能が含まれていると考えています。

- ユーザ ファイルの標準的な場所の暗号化、ディレクトリおよびファイル タイプをカスタマイズする機能（ターゲットごとのカスタマイズに対応）。
- すでに暗号化されたシステムとファイルをマーキングする機能
- ビットコインによる支払い方法の説明の提供
- 攻撃者が身代金額を設定し、二重の期限（金額を増額する前の期限と、データの暗号化に使用した鍵を削除する期限）を指定できる機能

このフレームワークでは各種のモジュールがサポートされるため、攻撃者はさまざまな環境に応じてランサムウェアをカスタマイズし、セキュリティの隙を突いて強力な攻撃ができるように手法を変更できます。たとえば次のようなモジュールがあります。

AUTORUN.INF/USB マス ストレージへの感染

このモジュールは、感染したシステムを検索し、ローカルとリモート両方のマップされたドライブを見つけます。次にこれらのドライブの場所に自身を複製し、複製の発見や削除が難しくなるようにファイルの属性を設定します。さらに、今後ドライブが接続されるすべてのコンピュータにこの感染プログラムの実行を要求する「autorun.inf」ファイルをこれらのドライブに記述します。

認証インフラストラクチャの悪用

このモジュールは、多くの企業ネットワークで使用されている主要な認証インフラストラクチャで、既知の弱点を利用します。得られたクレデンシャル情報は、他のシステムへのアクセス、場合によっては管理者レベルのアクセスを提供するために悪用できます。

コマンド アンド コントロールおよびレポートの感染

発見されるリスクを低減するために、次世代型ランサムウェアは、コマンド アンド コントロール機能を持たないように設定できます。このモジュールは、ビーコンと GUID（globally unique identifier）をコマンド アンド コントロール ドメインに転送します。このデータを転送するために、一般的なプロトコル/サービス（HTTP、HTTPS、DNS など）を通じてコマンド アンド コントロール ドメインへの到達を試みます。コマンド アンド コントロール ドメインはこれらの GUID を収集し、標的のネットワーク内の感染済み/暗号化済みシステムの数の統計を取ります。攻撃者はこの情報を利用して、キャンペーンの効果を判断できます。

レート リミッタ

このモジュールは、ランサムウェアをシステム リソースに対して「礼儀正しく」ふるまわせ、ユーザにランサムウェアの実行を気づかれないようにする役割を果たします。このモジュールは、使用する CPU 容量を制限し、ネットワークの使用を最小限に抑え、できるだけ静かにランサムウェアを実行できるようにします。

RFC 1918 ターゲット アドレス リミッタ

このモジュールは、ホストが RFC 1918 アドレスを持っている場合のみターゲット ホストを攻撃して埋め込みを行うよう設計されます。これらのアドレスは内部ネットワークによって使用されます。

入念に構築されたアーキテクチャと厳格なパスワード管理によって、未来の自己増殖ランサムウェアが水平移動することをはるかに困難にすることができます。次世代型ランサムウェアの防御の詳細については、**52 ページ**の「セキュリティに関する推奨事項」を参照してください。

ランサムウェアの進化、およびこの分野の次世代脅威に備えるために企業ができることについては、Cisco Talos のブログ投稿をご覧ください。

「ランサムウェア：過去、現在、そして未来」

脆弱性

脆弱性は、不正行為を行うための時間を攻撃者に与えてしまいます。攻撃者はそれを利用して、防御側が弱点にパッチを適用する前にキャンペーンを開始します。攻撃者はエクスプロイト キット、ランサムウェア、さらにソーシャル エンジニアリングによるスパムを使用して、パッチが適用されていないシステムや旧式のデバイスを攻撃します。

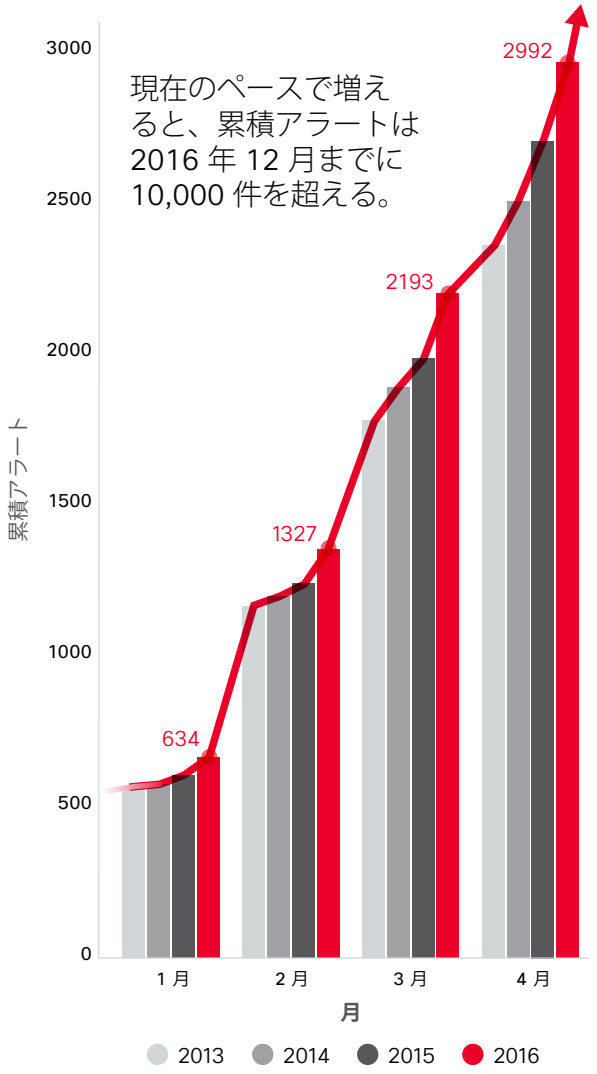
脆弱性は、攻撃者のチャンスと組織の防御能力の隙間に存在するものです。防御側が脆弱性にパッチを適用して攻撃者が攻撃できる時間を狭めることができれば、脅威は低減します。防御側がパッチを適用せずに脆弱性を放置すれば、攻撃者はそれをキャンペーンを開始する足掛かりにします。

ベンダーは Secure Development Lifecycle（SDL）の実施を通じて、脆弱性の特定と公開に注意を払うようになっています。しかし **15 ページ**で説明するように、攻撃者はパッチにも周到な注意を払い、リバース エンジニアリングによってどの部分が修正されているかを判断して、それに基づく新たなアプローチを開発します。

2016 年の最初の 4 ヵ月間には、年間累積アラート数が前年の同期間よりもわずかに増えました。これは Microsoft や Apple などのベンダーによるソフトウェアのメジャー アップデート、コード レビューの増加、コード レビュー ツールの改善、前述の SDL の実施などが原因であると考えられます（図 1）。これらのトレンドはすべて、製品の脆弱性特定の増加につながっています。

防御側はプロセスの改善や変革を行い、脆弱性の公開とパッチ適用の間のギャップを埋めようとしますが、攻撃者はスキルを駆使して、防御側の対応を弱体化させるような膨大で複雑な攻撃を作り出し、そうしたギャップを広げてしまいます。防御側は、攻撃者が攻撃する余地を特定して解消する必要があります。それには、公開された脆弱性に対応し、堅牢なパッチ管理システムを導入することが重要になります。

図 1. 年間累積アラート総数



出典：シスコ セキュリティ リサーチ

シェアする

「防御側はプロセスの改善や変革を行い、脆弱性の公開とパッチ適用によってギャップを埋めようとしますが、攻撃者はスキルを駆使して、防御側の対応を弱体化させるような膨大で複雑な攻撃を作り出し、そうしたギャップを広げてしまいます」

セキュアな接続に関する誤った安全意識

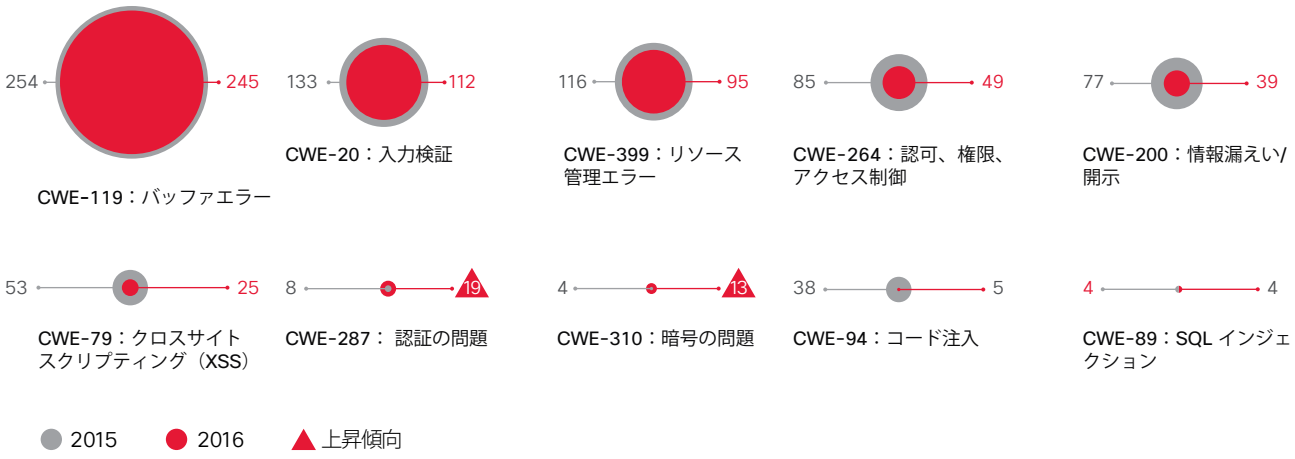
HTTPS 接続や SSL 証明書によって確立されるセキュアな接続は、オンライン アクティビティに関するある種の安全意識をユーザに与えます。しかし暗号化と認証に関する脆弱性アラートが最近増加していることから、攻撃者がセキュアな接続を簡単に侵害する懸念が高まっています。接続のセキュリティに不安が生じていることになります。

次に示す共通脆弱性タイプ一覧（CWE）チャート（図 2）によれば、2014 年から 2015 年にかけて認証と暗号化の問題が増えています。2015 年 12 月から 2016 年 3 月までの間だけでも、認証に関する 19 の問題と暗号化に関する 13 の問題が特定され、すでに前年までの合計数に達しています。

暗号化の使用が増えていることは、情報を傍受から守る意味で、前向きな進展だと言えます。しかしそれにはリスクもあります。暗号化によって複雑性が増大し、暗号化に使用するツールと、暗号化が保証できないほどのプライバシーが期待されるという両面で、新たな脆弱性が生まれるからです。暗号化を正しく行わなければ、適切な保護も実現しません。

セキュアな接続を確立するには、プロセスとツールの複雑な連携が必要になります。証明書の範囲外では、そうした連携が取られているかはわかりません。接続と接続の間には、セキュリティが保証されているかわからない VPN ゲートウェイなどのデバイスがあります。さらに、セキュアであるとされる Web サイトでも侵害されている可能性があります。つまり、一般的には安全であると見なされるような「ロック」アイコンが付いている URL でも、無条件でセキュアであると見なすことはできないということです。

図 2. 認証と暗号化に関する問題の発生：12 ～ 3 月



出典：シスコ セキュリティ リサーチ

活動するための時間

活動するための時間

ランサムウェアのアクティビティの増加と最近のキャンペーンの範囲を見ると、実行に移す時間が無制限にあるということが、いかに攻撃者にメリットを与えているかがわかります。この時間で攻撃者はキャンペーンの基礎を密かに構築し、準備ができたところで攻撃を開始し、最終的に利益を得ることになります。

こうした活動を隠すために、攻撃者は暗号通貨、Tor、HTTPS 暗号化トラフィック、Transport Layer Security（TLS）を使用しています。一方エクスプロイト キットの作成者は、パッチのリバース エンジニアリングを行い、公開された管理されていない脆弱性を悪用します。また攻撃者は、効率性が高く追跡が困難なマルバタイジングの新しい形態を生み出し、侵害されたサイトへのトラフィックを増大させています。それによってユーザのマシンを侵害し、最終的にランサムウェア攻撃を開始することになります。

攻撃ベクトル：クライアント側

攻撃者は以前からクライアント側を主体に攻撃してきました。それはユーザを関与させるチャンスが多いからであり、またユーザは常にセキュリティ上の弱点であるためです。さらにクライアント側では、攻撃できる隙を得るためにさまざまな方法を取ることができます。選択肢が非常に多くなるわけです。

それでも、PDF などのベクトルを利用する攻撃は、長年の成長を経て安定化したように思われます。同時に、攻撃者がサーバ側でも新たなチャンスを探している形跡も見つかっています。これが成功するとネットワーク間を水平方向に移動して攻撃をさらに強化することができます。

PDF および JAVA 攻撃の減少

攻撃ベクトルとして PDF と Java を使用する方法は、減少し続けています。2016 年 1 月に、Oracle は Java ブラウザ プラグインを廃止することを発表しました。これは、ブラウザのベンダーがそのようなプラグインのサポートを終了する計画を進めているためです。[1] Oracle は代わりに、プラグイン不要な Java Web Start テクノロジーに重点を移しています。

Java ブラウザ プラグインが終了することで、それが攻撃ベクトルとして利用される例は減っていくでしょう。しかし攻撃者が旧来の脅威を進化させて、Java の新しい形態を利用していないかどうか、セキュリティ調査担当者は監視を続けるはずです。セキュリティの専門家やセキュリティ企業は、必要とされる場合を除き、サイトで Java をブロックすることを考慮すべきです。

[1]「Moving to a Plugin-Free Web（プラグインが不要な web へ）」、Java Platform Group、2016 年 1 月：
https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free

PDF の悪用も減少していますが、電子メールでは、メールの受信者に不正な添付ファイルをクリックさせるなどの目的で、依然として攻撃に利用されています。スパムの作成者はそうした戦術を、最新ニュースや季節のイベントを装った件名と合わせて使用しています（スパムの詳細については **19 ページ**を参照）。

エクスプロイト キットの開発者は依然として Flash を使用していますが、オンラインの Flash コンテンツは徐々に減っています。しかしリッチ メディア コンテンツやインタラクティブ広告などを使用する多くのオンライン アプリケーションでは、いまだに Flash が多用されています。

HTML5 などの代替アプリケーションも少しずつ採用されていますが、移行の速度は遅く、Flash に依存する状況が継続しています。Flash が残存する限り、攻撃ベクトルとして利用され続けることになります。

最先端のエクスプロイト キットは引き続き FLASH を利用

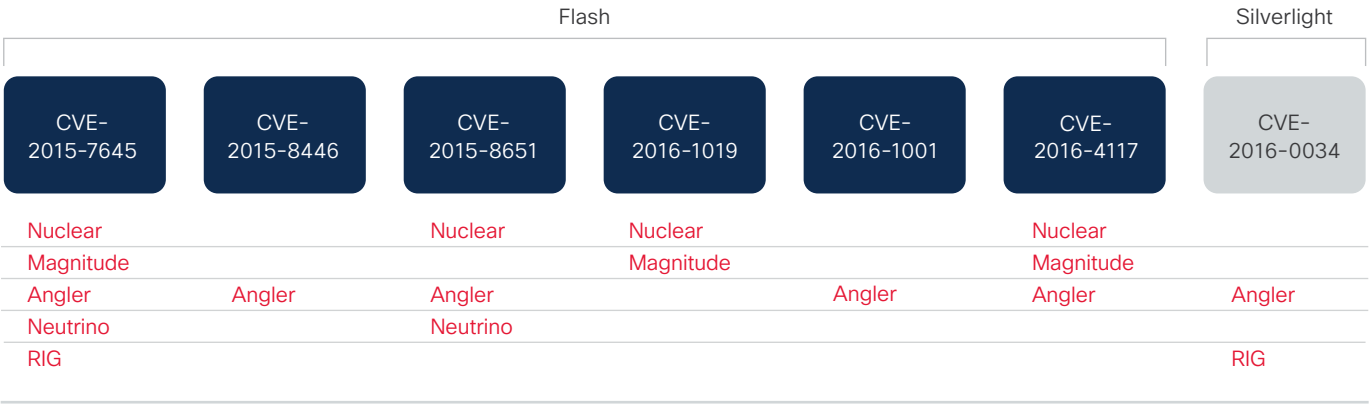
エクスプロイト キットはランサムウェアの存在をこれほどまでに広める一助となりましたが、Adobe Flash の脆弱性を引き続き利用します。先頃、シスコの調査担当者が有名な Nuclear エクスプロイト キットを調査したところ、成功したエクスプロイト試行の 80 % に Flash が関与していました。[2]

Adobe は頻繁に明らかになる脆弱性にパッチで対応していますが、攻撃者も負けていません。Adobe が脆弱性のパッチとして Flash のアップデートをリリースすると、エクスプロイト キットの作成者はパッチのリバース エンジニアリングを行って、修正内容を特定しようとします。エクスプロイトの作成者は 1 週間以内に Flash の脆弱性を特定して、リモート コード実行のための攻撃手段として利用します。

ユーザと管理者は不要なブラウザ プラグインを無効にするか削除して、脅威の対象にならないようにすることをお勧めします。少なくとも、アップデートがリリースされたらすぐに Flash をアップグレードしてください。

パッチのインストールが良い影響を及ぼすことを示すために、Flash と Microsoft Silverlight の最近の脆弱性を利用した、各種のエクスプロイト キットを図 3 に示します。これらすべての脆弱性に対して利用可能なパッチをインストールすることで、エクスプロイト キットによって配信されるランサムウェアの影響を軽減させることができます。

図 3. エクスプロイト キットが悪用する脆弱性



出典：シスコ セキュリティ リサーチ

シェアする

[2]「Threat Spotlight: Exploit Kit Goes International, Hits 150+ Countries（注目の脅威：エクスプロイト キットが世界中に拡散、150 ヵ国以上が被害に）」、Cisco Talos ブログ、2016 年 4 月 20 日：**http://blog.talosintel.com/2016/04/nuclear-exposed.html**

エクスプロイト キットは Tor で通信を隠蔽

エクスプロイト キットの作成者は、セキュリティ防御を回避する方法を常に探しており、これを達成するために彼らは豊かな創造性を発揮します。最近の例では、Nuclear エクスプロイト キットがこれに該当します。Nuclear キットは一般的にランサムウェアのバリアントをドロップするものですが、この例では匿名の通信に使用されるソフトウェア、Tor のバリアントを配信していました。これは、悪意のあるペイロードを最終的に匿名化し、防御側がアクティビティを追跡しにくくする戦術のようです。

一般的に、エクスプロイト キットが悪意のあるファイルをドロップする場合、コマンド アンド コントロール トラフィックをモニタリングすることで検出できます。つまり、マルウェアが「Call Home」を行ったときに検出できます。ただし、この Nuclear エクスプロイト キットがペイロードをドロップする様子をシスコが確認したところ、Tor 実行可能ファイルが先にドロップされ、次に Tor を通じて通信要求が実行されます。Tor は End-to-Exit で暗号化されたルーティング プロトコルであるため、セキュリティ プロフェッショナルは Tor 内のマルウェアの動作を見ることができません。

エクスプロイト キットによって配信されるランサムウェアは、作成者に莫大な利益をもたらしています（**7 ページ**の「ランサムウェア：脅威的なスタミナで莫大な金を生み出す」を参照）。当然ながら、ランサムウェアの開発者はマルウェアの効果を上げる新しい方法を探し、他のエクスプロイト キットと競争します。Nuclear エクスプロイト キットで Tor が使用されているということは、マルウェア開発者がさらに巧妙な進化をとげたことを意味します。

Nuclear エクスプロイト キットでの Tor の使用については、Cisco **Talos のブログ記事**を参照してください。

攻撃者はサーバベースのキャンペーンに価値を見出す

攻撃者はキャンペーンの見返りとして高い価値を求めています。マルウェアやエクスプロイト キットをクライアントやエンド ユーザに配信することには効果がありますが、攻撃の影響を低下させる原因にもなります。クライアント側の攻撃で攻撃者が利用できる帯域幅や機能は限られているからです。

しかし攻撃者はサーバ側を利用するキャンペーンにまで拡大することで、より大きな見返りを求めています。エンタープライズ アプリケーション プラットフォームの JBoss は最近、ネットワークにアクセスしてランサムウェアのバリアントである SamSam を拡散するために利用されました（**7 ページ**を参照）。シスコの調査担当者によると、攻撃者は JBoss アプリケーション サーバのテストとエクスプロイトに使用するオープンソース ツールの JexBoss を使用して、医療機関用ネットワークへの足掛かりとしました。攻撃者は一度ネットワーク内に入ると、SamSam を使用して Windows ファイルを暗号化できます。

サーバの脆弱性を標的とするランサムウェアの拡散によって、流行しつつある脅威は新たな次元に突入しています。シスコの調査担当者は、インターネット上のマシンについても調べ、すでに侵害され、ランサムウェアのペイロードに対して待機状態になっているマシンを発見しました。さらに、1600 の IP アドレスにわたって 2000 のバック ドアがインストールされていることも特定しました。バック ドアの多くは、学校用の一般的なライブラリ管理システムを使用するシステムで見つかりました。シスコの連絡を受けて、ソフトウェア開発者はすぐに必要なパッチのリリースに取り掛かりました。

主にサーバ側システムの脆弱性を利用することで、攻撃者の攻撃対象は広範になり、損害を封じ込めるために多くの時間と労力が必要になります。Web ブラウザなどのクライアント側アプリケーションは自動更新によってパッチが適用されることが多くなり、脆弱になりにくくなっています。

一方サーバ側アプリケーションは、パッチとアップグレードが時間が限られた IT スタッフの作業によって行われ、また運用に影響を与えずにアップグレードすることがむずかしいため、慢性的に対応が遅れがちです。さらにネットワークの境界には穴が多く、その境界に防御を依存していたサーバへのアクセスが容易になっています。

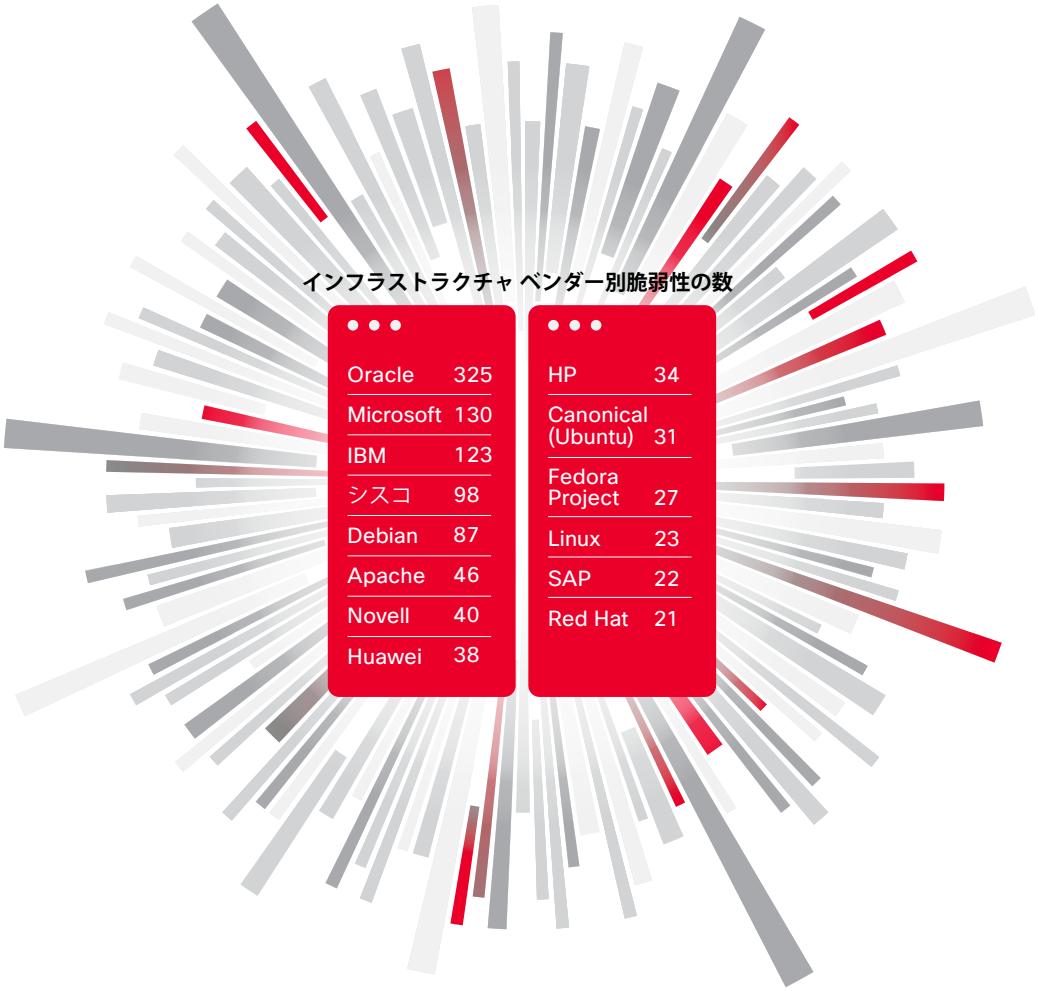
図 4 に示すように、多くの主要なインフラストラクチャ ベンダーの製品が、クライアント側とサーバ側両方のアプリケーションについて脆弱性を示しています。

サーバ ソリューションの脆弱性の危険については、Cisco Talos の次のブログ記事を参照してください。

「JBoss バックドアが深刻な脅威として拡散中」

「SamSam：治療は身代金を支払った後で」

図 4. インフラストラクチャ ベンダーの脆弱性：2016 年 1 月 1 日 ～ 3 月 30 日



出典：シスコ セキュリティ リサーチ

JBOSS：インフラストラクチャ内の脆弱性が攻撃者に活動時間を与える

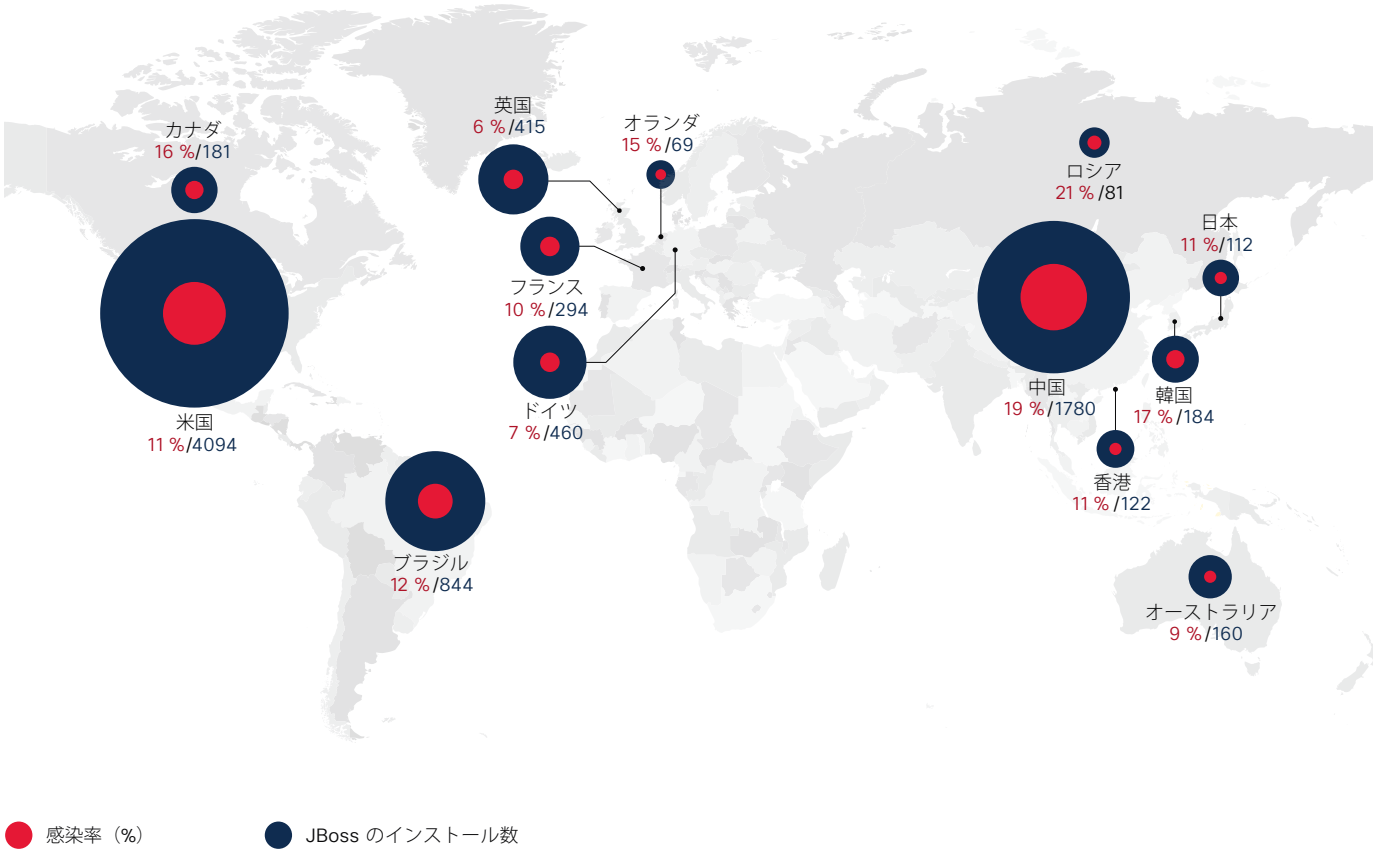
ランサムウェアの作成者は、企業アプリケーション ソフトウェアである JBoss を利用して、キャンペーンを優位に進めています。先頃発生した、医療機関を巻き込んだランサムウェア キャンペーン（**7 ページ**）からわかるように、JBoss の脆弱性をついて不正アクターはネットワークに侵入し、データを収集してマルウェアを起動する時間を確保しています。JBoss を利用した侵害は、ネットワークのメンテナンスを怠っていると、犯罪者にアクセスを許してしまうというさらなる事実を示しています。こうしたアクセスはブロックできるのです。

シスコの調査によると、JBoss 関連の侵害によって重大な影響が及び、攻撃に対して脆弱性が生じています。インターネットのスキャンでは、次の手順で調査しました。

- HTTP ヘッダーまたはページ コンテンツに JBoss がインストールされていると報告されたサーバを調べました。
- その後、ホストに存在する各種のバックドア、Web シェル、その他の .jsp 侵害の数を調べました。

図 5 に、JBoss がインストールされているサーバのうち、侵害されたとみられるサーバの割合を示します。米国を例にとると、調査対象の Web シェルの 11 % に侵害の兆候が見られます。

図 5. Web シェルの存在が JBoss の侵害を示す



出典：シスコ セキュリティ リサーチ

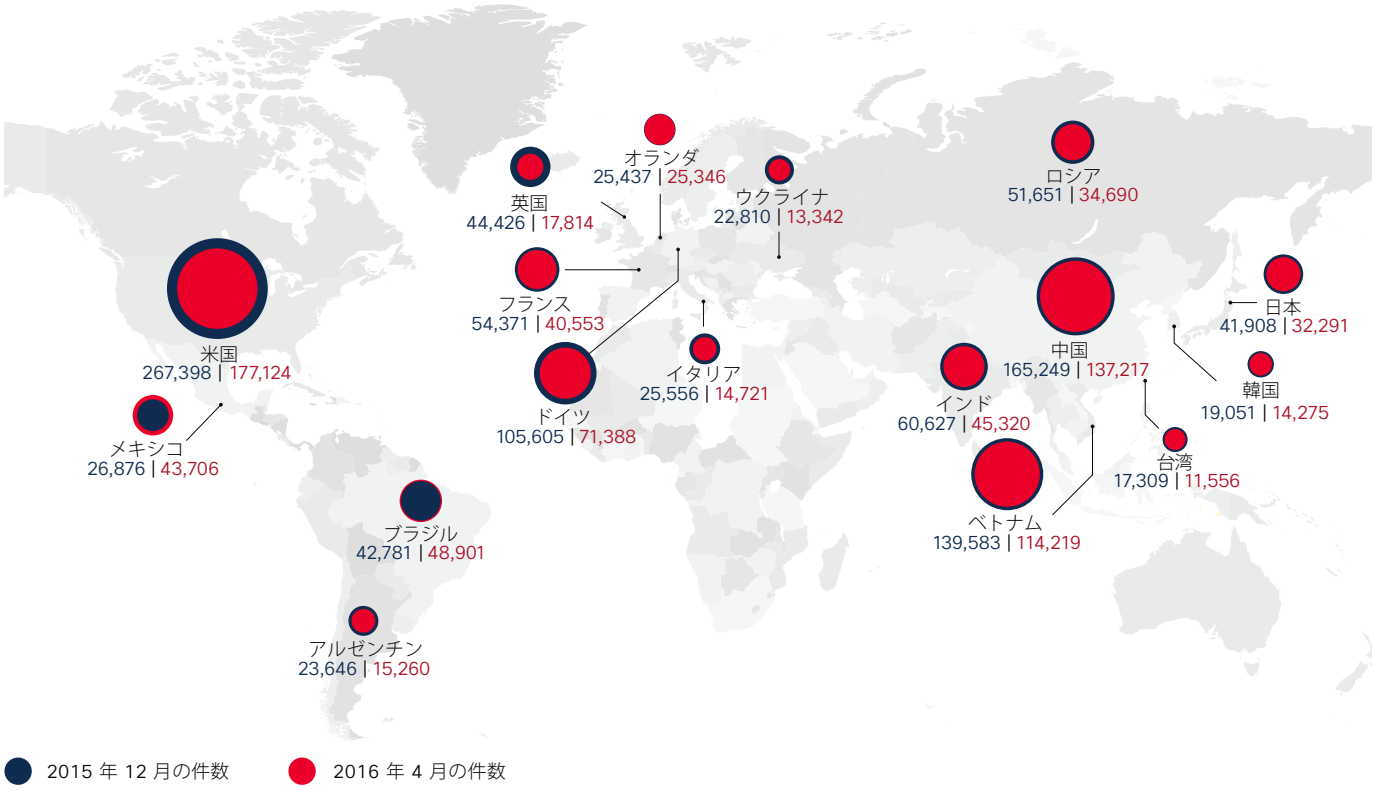
スパムの量は全世界で比較的横ばい

スパム トラフィックを世界規模で把握するために、シスコは電子メール アプライアンスからサンプルを収集しました。これは電子メール アプライアンスとゲートウェイにコード化されたポリシー決定の影響を示すもので、たとえば、ブロックされた電子メールや不明とマークされた電子メールなどです。スパム メールは攻撃ベクトル、中でもランサムウェアによく使用されます。

電子メール トラフィックに関するシスコの調査によると、スパムの量は 2015 年 12 月から 2016 年 5 月にかけて、着実に増加しています（図 6）。ブラジル発信のスパム トラフィックは、2016 年 1 月と 3 月に急増しています。この増加は、当時活動していたスパム ボットネットが原因と思われます。

地域別の Web ブロック アクティビティのセクション（**47 ページ**）で説明するように、攻撃者は活動拠点とする国やホスト プロバイダーを転々とし、キャンペーンを着手しやすい環境を探します。スパム業者は、信頼できるホスト内で所有され、共存するボットネット マシンを使用します。検出システムで発見されるまでそのマシンを利用し、見つかると別のボットネットに移動します。

図 6. 国別のスパム数：2015 年 12 月 ～ 2016 年 5 月



出典：シスコ セキュリティ リサーチ

図 7. スパムでよく使用されるソーシャル エンジニアリングのトピック

バージョン番号	URL	メッセージの概要	言語	最終公開日（GMT）
95	RuleID4626	請求書、支払い	ドイツ語、英語	3.18.16
82	RuleID4400KVR	発注書	英語	2.1.16
64	RuleID4626(cont)	請求書、支払い、出荷の確認	英語、ドイツ語、スペイン語	1.28.16
62	RuleID4961KVR	支払い、転送、注文、出荷	英語	3.25.16
58	RuleID4961KVR	見積り依頼、製品の注文	英語、ドイツ語、複数の言語	1.25.16
52	RuleID5118KVR	製品の注文、支払い	ドイツ語、英語	3.17.16
49	RuleID858KVR	送料の見積書、支払い	英語	3.14.16
47	RuleID4961	転送、出荷、請求書	英語、ドイツ語、スペイン語	2.22.16
44	RuleID4627 と RuleID4627KVR	飛行機の E チケット	英語	3.29.16
30	RuleID8337KVR	注文、支払い、見積書	英語	1.21.16

出典：シスコ セキュリティ リサーチ

スパム作成者は、添付ファイル（マルウェアを伝達する PDF など。**15 ページ**を参照）や、巧妙なソーシャル エンジニアリングによってメッセージ間のリンクをクリックするよう、ユーザを誘導します。図 7 に示すように、スパム作成者は、請求書、旅行の手配、ビジネスの引き合いなど、重要な情報を装った添付ファイルやリンクを作成します。また、メッセージを他の言語でも作成して、より多くの被害者をわなに掛けようとします。

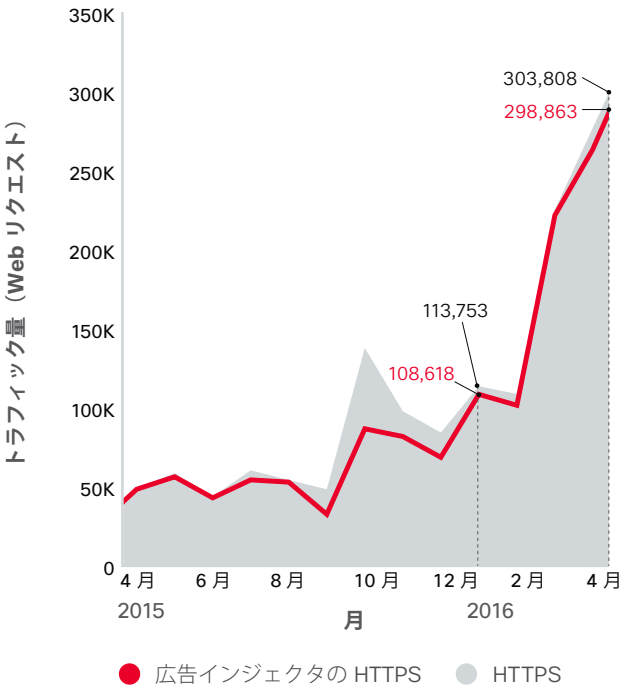
ブラックリストに戻るのか：攻撃者による HTTPS の利用で複雑化する防御側の調査

広告インジェクタが HTTPS で暗号化されたトラフィックを通じて悪意のある広告を提供する状態では、ユーザおよびセキュリティ チームは、潜在的な脅威を特定するために、URL を通じて送信された情報を信頼できなくなります。この点を知っている攻撃者は、HTTPS で暗号化されたトラフィックの使用を飛躍的に増加することで、Web 上での活動を隠蔽し、活動時間を延長しようとしています。

2015 年 9 月から 2016 年 3 月にかけて、シスコのセキュリティ調査担当者は悪意のあるアクティビティに関連する HTTPS トラフィックが 5 倍に増加したことを確認しました。HTTPS の使用におけるこの動向を突き止めるため、8 つの脅威カテゴリに分散する 80 の悪意のあるキャンペーンを、16 ヵ月間にわたって追跡しました。HTTPS トラフィックの増加は、シスコの調査によれば、主に広告インジェクタとアドウェアに起因すると結論付けられます（図 8）。

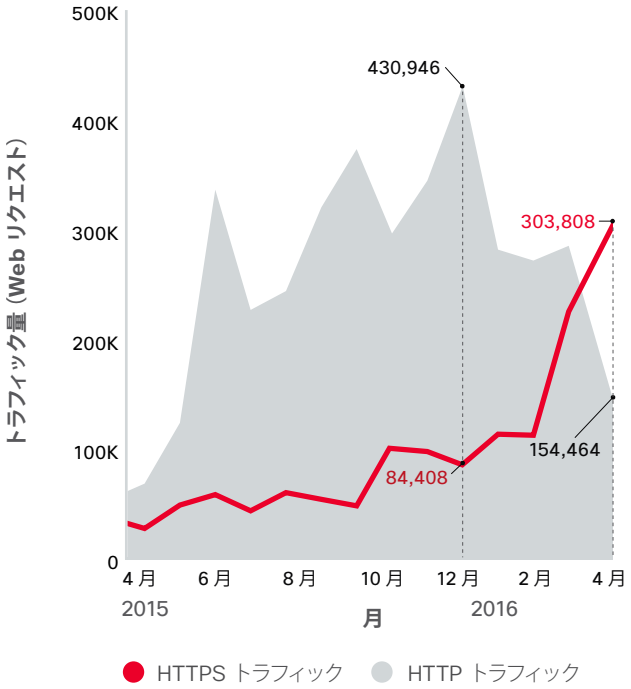
また、広告インジェクタに関連した HTTPS トラフィックが、2015 年 12 月から 2016 年 4 月にかけて、300 % 増加したことも明らかになりました（図 9）。

図 8. HTTPS 増加の主要因はアド インジェクタ



出典：シスコ セキュリティ リサーチ

図 9. アド インジェクタの HTTPS トラフィックが 4 ヵ月で 300 % 増加



出典：シスコ セキュリティ リサーチ

悪意のある広告インジェクタは、アドウェア感染の主な要因です（図 10）。サイバー犯罪者はこのようなブラウザ拡張機能を利用してマルバタイジングを Web ページに挿入し、ユーザに広告やポップアップを表示し、ランサムウェアやその他のマルウェア キャンペーンを成功させようとします。マルバタイジングや悪意のある広告インジェクタは、広告エコシステムの一角に潜み、正規の動作を悪意のあるアクティビティから区別することは困難です。

広告インジェクタおよびアドウェアへの感染は、無視すべきではありません。今年、シスコのセキュリティ調査担当者は、トロイの木馬 DNSChanger の新しいバージョンがアドウェア経由で配布されていることを見つけました。この状況は、広告インジェクタおよびアドウェアの感染によって、個人と企業が被る危険が増加していることを示しています。[3]

また、攻撃者がマルウェアを HTTPS に移行している証拠も突き止めました。この動きは、広告インジェクタで起きている動向よりもゆっくりとしています。これはおそらく、攻撃者は常に利益の最大化を狙っているため、インフラストラクチャを変更するのは必要になったときに限定されるからと考えられます。

皮肉にも、サイバー犯罪者がインフラストラクチャの更新を遅らせるというのは、合法的なビジネス業界の傾向と呼応しています。多くの組織が、インターネット インフラストラクチャにある既知の脆弱性へのパッチ適用を延期しています。それも何年も先延ばしにしているのは、デバイスやソフトウェアをオフラインにしてアップグレードを実行する間に、収益を失うのを恐れているからです（**30 ページ**の「老朽化したインフラストラクチャ：ランサムウェアの増加により長期にわたる脆弱性へのパッチ適用が急務に」を参照）。感染した多数のホストにパッチを適用する課題も、明らかに、攻撃者がレガシー技術を稼働し続ける動機となります。

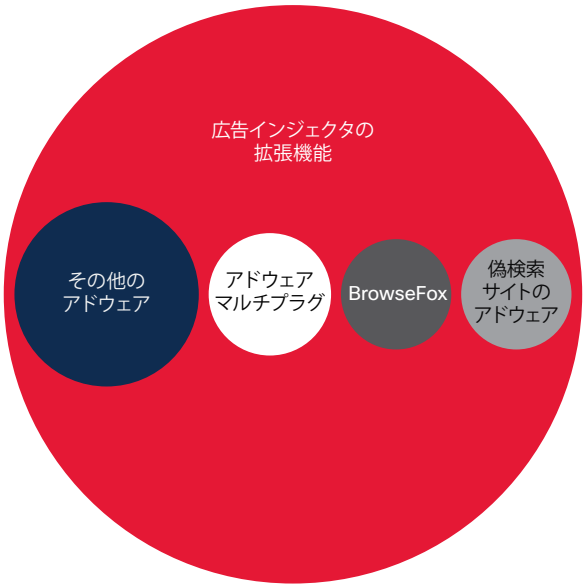
16 ヵ月間の分析から、次のマルウェア ファミリで HTTPS の使用が増加していることを確認しました。

- Gamarue/Andromeda、多目的ボットネット
- Necurs、情報を盗み取るボットネット
- Miuref/Boaxxe、クリック詐欺ボットネット
- Ramdo/Redyms、クリック詐欺ボットネット
- データ窃盗用トロイの木馬

悪意のあるアクティビティに関連する HTTPS 暗号化されたトラフィックの増加はやっかいで、マルウェア キャンペーンの追跡と調査を担当するセキュリティ研究者にとって大きな問題になります。HTTP トラフィック内の脅威を特定するために防御側が使用する、シグネチャベースの IDS や URL パターンに基づく検出などの技法では、SSL インスペクション機能を追加しなければ HTTPS トラフィックに適用できません。多くの場合、セキュリティ調査担当者が調査を開始する時点では、ドメイン名か IP アドレスしか手元にありません。

脅威がインフラストラクチャを共有することが多いため、脅威の分類もまた困難です。防御側が利用できる戦略の 1 つは、ブラックリスト（すべての既知のマルウェアのリスト）の使用です。しかしこの方法はエラーが起きやすく、きめが粗いので効果的ではありません。また、時間のかかる作業でもあり、アナリストが手作業で脅威を調査し、分類しなければなりません。

図 10. アドウェア感染ではアド インジェクタが主流なコンポーネント



出典：シスコ セキュリティ リサーチ

[3]「DNSChanger Outbreak Linked to Adware Install Base（アドウェアのインストール ベースにリンクされた DNSChanger アウトブレイク）」、シスコ セキュリティ ブログ、2016 年 2 月：**http://blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base** [英語]

サービスとしてのマルバタイジング：効率の高い感染が重要

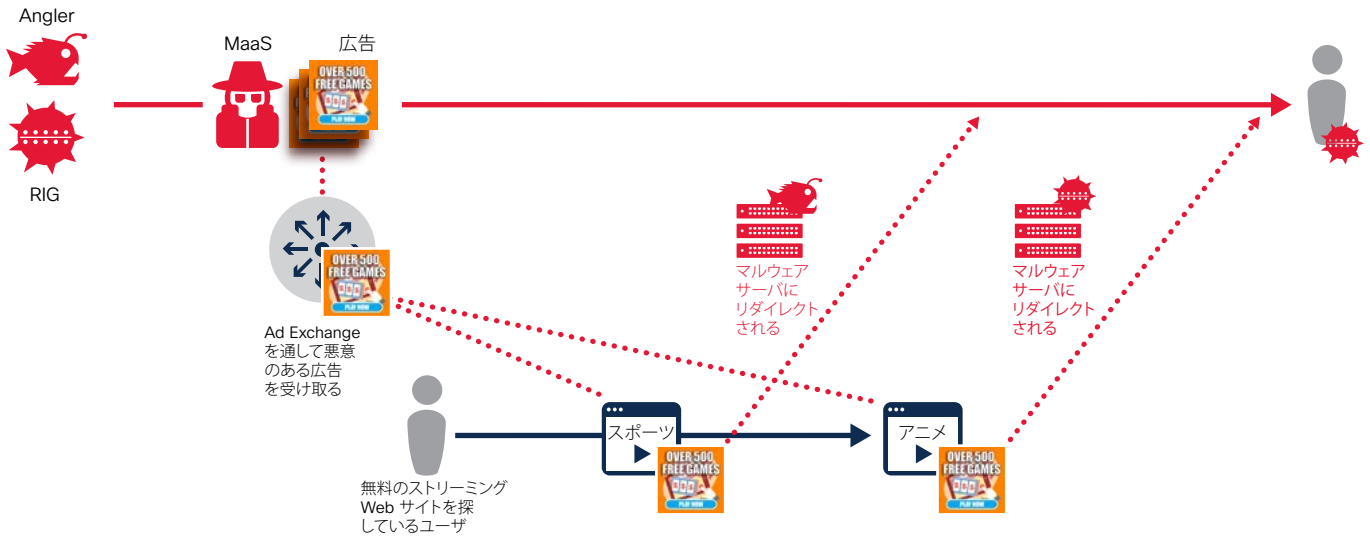
広告代理店は、知ってか知らずか、Web 上での悪意のある広告の感染媒体となり、事実上、攻撃者の新しいビジネス モデル「サービスとしてのマルバタイジング」を実現しています。脅威アクターは、マルバタイジングを実行する手段として、人気のある正規の Web サイトの広告スペースを購入します。これによって、防御側に新たな問題が生じ、ユーザをマルバタイジングから保護する責任は誰にあるのかという疑問が持ち上がります。

正規の広告スペースを購入することで、攻撃者は関係のないサイトにまで容易に脅威を拡散できます。広告が表示される時間はほんのわずかで、防御側が脅威の存在を確認する間もありませんまた、広告代理店はブラウザの種類やバージョンといった情報を使用してユーザを絞り込むので、攻撃者が特定のユーザグループを、言語を含めて詳細なレベルで攻撃しやすくなります。

サービスとしてのマルバタイジングの動向は、ドメイン占拠に似ています。ドメインの不法占拠者は、ユーザが正規の企業や有名ブランドと結び付けてしまいそうなドメイン名を販売または使用して、利益を得ます。こうしたドメインからトラフィックを転送すると、脅威の拡散に自ら手を下さなくても、マルウェアの配布を促進できます。

広告ブロッカーの有効化は、マルバタイジングの攻撃を回避する論理的な手段です。とりわけ、マシンへの感染とペイロードの分散にユーザ操作を必要としない、新たに確認された変種に関して有効です。しかし、オンライン コンテンツの大手プロバイダーの一部は、収益の大部分をデジタル広告に依存していることもあり、サイト上の他のコンテンツを表示したいなら広告ブロッカーを無効にするようユーザに要求しています。このことから明らかにユーザに対するリスクが生じます。セキュリティ チームにとってもジレンマが生じ、アドエクスチェンジから広告を提供するサイトをブロックするかどうかを決定しなければなりません。

図 11. Malvertising as a Service（MaaS）の仕組み



出典：シスコ セキュリティ リサーチ

多段階のリダイレクション

シスコの調査担当者は、脅威アクターが広告スペースを購入して悪意のある広告を配信して、直接ユーザのコンピュータに感染したり、ユーザを別の場所にリダイレクトしてマルウェアのペイロードを配信したりする様子を確認しました。多くの場合、リダイレクションは多段階で行われます。別の例では、マシンが感染するにはユーザが悪意のある広告を操作する必要すらありません。すべては画面の向こうのバックグラウンドで処理されます。

2015 年 10 月に最初に出現したサービスとしてのマルバタイジング キャンペーンは、Angler や RIG など、複数のエクスプロイト キットにユーザをリダイレクトし、これによってペイロードが送信されました。ペイロードの多くは TeslaCrypt や CryptoWall などのランサムウェアのバリエーションです。ユーザはギャンブル サイトを装った悪意のある広告によって騙されていました。JavaScript へのリンクが広告のコードに埋め込まれていました。このリンクがユーザを Angler ランディング ページに誘導しましたが、iFrame などのその他のリダイレクションもありました。

マルバタイジングを拡散するためのこのような新しいアプローチの出現は、地下経済の産業化が進んでいることのもう 1 つの指標です。シスコの調査担当者は、多数の Web ユーザを正規のサイトを通じて効果的に感染させ、検出を回避する手段を求めるサイバー犯罪者の増加に伴い、サービスとしてのマルバタイジングは増え続けると予測しています。マルバタイジングは、ランサムウェア キャンペーンの実行に中心的な役割を果たします。ランサムウェアは、攻撃者にとって高い収益を得られる仕組みなので、攻撃方法として急速に人気を高めています（**7 ページ**の「ランサムウェア：脅威的なスタミナで莫大な金を生み出す」を参照）。

Malvertising as a Service のトレンドの詳細については、Cisco Talos の次のブログ記事を参照してください。

「注目の脅威：成果を求めて急激に変化するマルウェア」

「シスコの調査担当者は、サイバー犯罪者が正当なサイトを通じて多数の Web ユーザを効率的に感染させ、検出を回避する方法を探す中で、Malvertising as a Service のトレンドが拡大すると予想しています」

WEB 攻撃の手法：成功するランサムウェアのセットアップ

2016 年上半期における Web 攻撃手法の動向は、ランサムウェアの爆発的な増加に結び付いています。たとえば疑わしい Windows バイナリは、図 12 に示すようにトップに挙げられますが、攻撃者がスパイウェアやアドウェアなどの脅威の配信に使用しています。これらのツールによって攻撃者はネットワーク インフラストラクチャに足場を築き、ランサムウェアなどの攻撃を実行できます。

Facebook 詐欺（ソーシャル エンジニアリング）、トロイの木馬、iFrame も、ユーザのコンピュータや組織ネットワークへ最初のアクセスを得るためのツールとして依然としてよく使用されています。

Facebook 詐欺は、最新のサイバーセキュリティ レポートで述べているように、2015 年下半期に調査した中で最多の Web 攻撃手法です。Windows バイナリは、リストの 4 番目です。JavaScript マルウェアは、前回のトップ 10 の調査では 3 つもランクインしていましたが、今回のトップ 10 には入っていません。

しかし、JavaScript マルウェアは消え去ったわけではありません。それどころか、このタイプのマルウェアは、今年発生した多数のランサムウェア キャンペーンを推進する基本コンポーネントとなっています。

図 13 は、それほど発生頻度が高くなく、感染の連鎖に深く食い込んでいる可能性が高いマルウェアを示します。

図 13 に並べた多数の項目は、ランサムウェアのシグニチャ、トロイの木馬、ドロッパーが存在するサンプルを示します。ランサムウェアを利用する攻撃者が増加するに伴い、情報窃盗用マルウェアよりも、ランサムウェアのインフラストラクチャ コンポーネントのほうが頻繁に確認されるようになりました。

図 12. 最も広く確認されたマルウェア

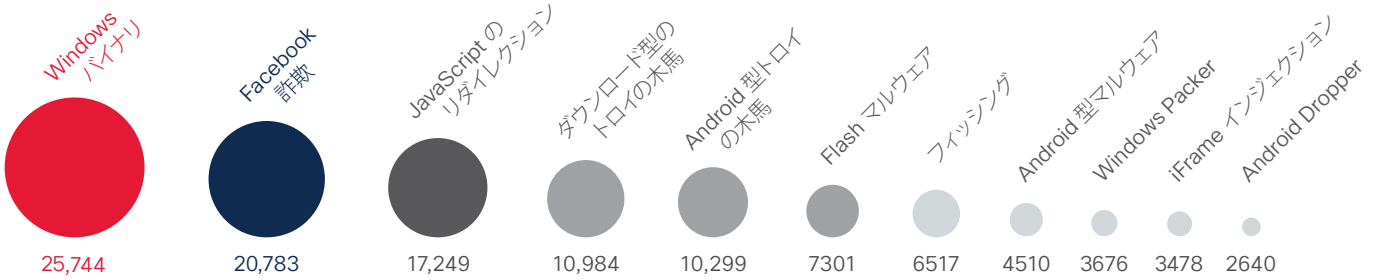
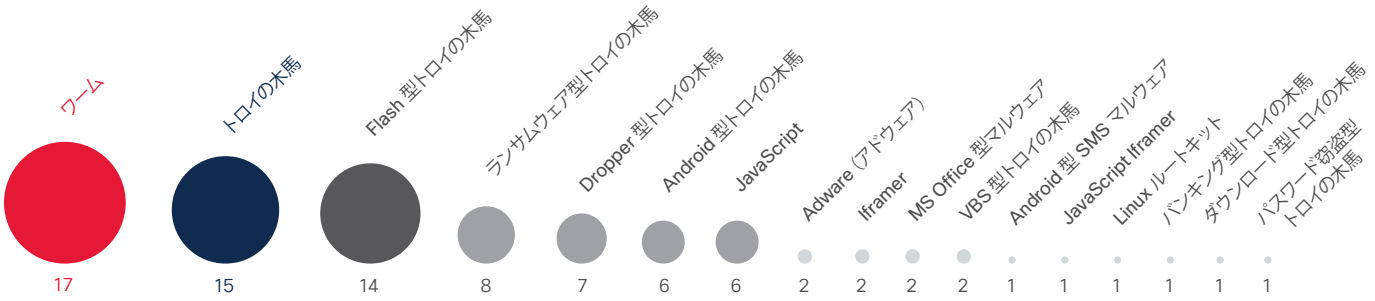


図 13. 比較的数が少ないマルウェアの例



出典：シスコ セキュリティ リサーチ

保護するための時間

保護するための時間

防御側は常に新たな技術を開発していますが、デジタル エコノミーが基盤とするインフラストラクチャは脆弱なままで、不適切なセキュリティ対策に頼っています。現在、大半の組織では導入されている Web ブラウザ、アプリケーション、インフラストラクチャに統一性がないため、攻撃者の侵入経路が多数あります。

これらのデバイスやソフトウェアの保護が不十分では、攻撃者に活動の余地を与えてしまいます。セキュリティ プロフェッショナルはこうした機会を締め出す必要があります。攻撃者が制限なく活動する範囲を狭めて、攻撃者の存在を確認することが、セキュリティに対する最重要の職務です。

パッチ適用までの時間：パッチおよびアップグレードが公開されてから実装するまでの時差がセキュリティ ギャップを生む

近年、主要ベンダーはプロアクティブな対応を強め、脆弱性やエクスプロイトが発見されてからパッチ配布までの時間を短縮し、これらの脆弱性を発見したセキュリティ研究者との協力を深めています。実際、数千件の Common Vulnerabilities and Exposures（CVE）を精査したシスコの調査によると、脆弱性の公表からパッチ公開までの時間の中央値は、主要なエンドポイント ソフトウェア ベンダーではゼロデイだと判明しました。つまり、脆弱性が一般に公開されると同時に、パッチも公開されるということで、ベンダーは連携して開示手順を実践しています。

ただし、パッチは速やかに提供されていますが、シスコの調査によると、多くのユーザはこれらのパッチを適時にダウンロードしてインストールしていません。このようなパッチの公開と実際の実装との時間差は、攻撃者がエクスプロイトを開始するには十分な期間です。つまり、ネットワーク内で活動する時間ですが、簡単なソフトウェア パッチを行っていれば侵入を防止できたはずです。不正アクターは、脆弱性が一般に公開される前でも、エクスプロイトを進める手順を開始できます。そこで、パッチ公開からインストールまでの時差をなくすことが、防御側にとって重要です。

この時差を解消するために、ベンダーは自社製品に自動更新機能をさまざまな形で取り入れました。ユーザ通知による定期的なチェックをはじめとして、無効化の難易度が高いオプトインとオプトアウトのバックグラウンド更新まで、さまざまです。

自動更新ポリシーに応じて、ユーザは、都合の良いタイミングまで更新を延期するか、場合によっては更新を完全にスキップするかを選択できます。シスコのお客様が使用しているエンドポイント上のブラウザ ソフトウェアのインストール状況を調査した結果、自動更新が重要であることがわかりました。強力なオプトアウト ポリシーを設けている Google Chrome Web ブラウザのインストール状況を調査すると、多くのユーザ（ユーザベースの 60 ～ 85 %、自動更新ポリシーの強度が増すにつれて増加）が最新バージョンのソフトウェアを実行しており、自動更新の重要性が実証されています。

控えめに見積もっても、75 ～ 80 % のユーザが最新バージョンか、1 つ前のバージョンのブラウザを使用しています（図 14）。Google は、古いバージョンのブラウザの実行を困難にする手段を強めています。自動更新を無効にするには管理者アクセスが必要で、ベンダーの自社サイトや他のサイトからは古いバージョンのダウンロードは許可されません。

自動更新ポリシーは、単に自動更新を適用するだけでなく、ユーザが実行するバージョンに大きな影響力を持っています。シスコが調査したすべてのソフトウェアは、ユーザへの通知のポップアップから、サイレント モードの自動処理まで、何らかのタイプの自動更新システムを採用していました。このプロセスを意図的に無効にするには、ユーザに多大な手間がかかります。ポリシーが厳格になるほど、目的の動作は把握しやすくなります。

図 14. インストールされている Chrome のバージョン（上位 50 % のユーザ）

注：このセクションのパッチ適用までの時間を示すグラフは、調査対象者の上位 50 % に関する結果を示しています。単純に上位の調査対象者数を示すことで、アップデートの効果が現れているか、またカスタマー ベースの保護に有効な防御が他にあるかどうかがわかりやすくなります。

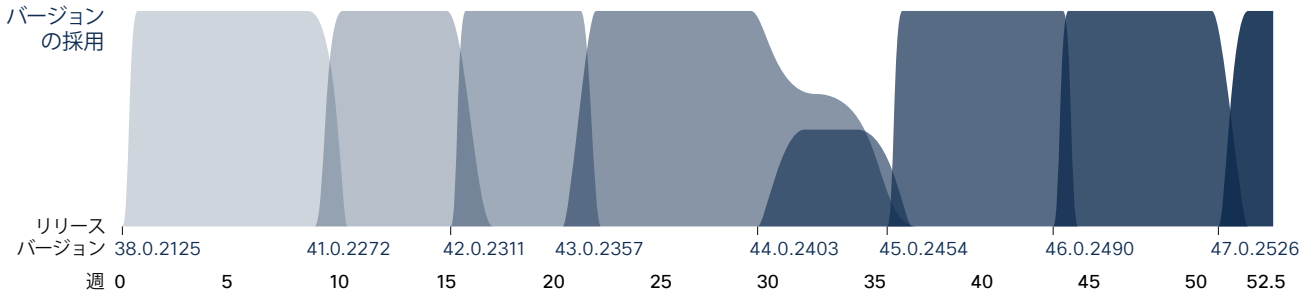


図 15. インストールされている Java のバージョン（上位 50 % のユーザ）

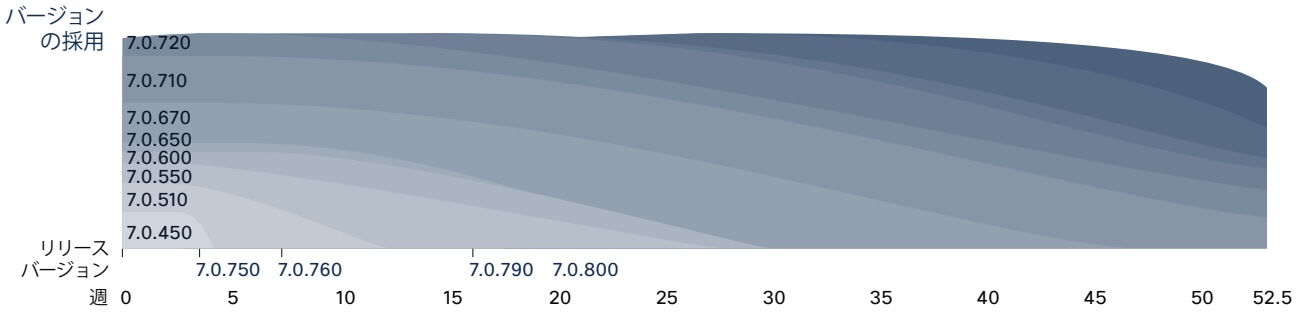
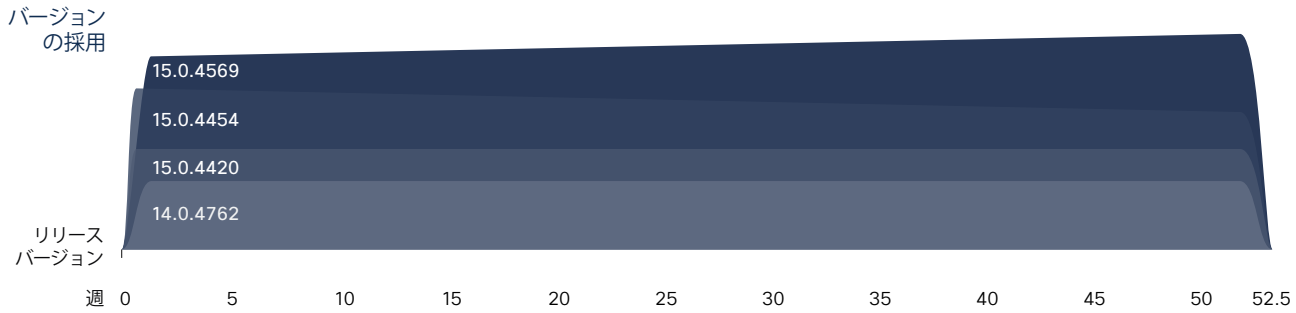


図 16. インストールされている Microsoft Office のバージョン（上位 50 % のユーザ）



出典：シスコ セキュリティ リサーチ

調査対象をブラウザからソフトウェアに移すと、自動更新ポリシーの欠如による影響を確認できます。シスコのお客様が使用しているエンドポイント上の Java ソフトウェアのインストール状況を調査した結果（前のページの図 15）、シスコの調査担当者は、侵害の指標（IOC）も検出しました。調査対象のシステムの 3 分の 1 が Java SE 6 を実行しており、これは Oracle が廃止を進めているバージョンです。最新バージョンは SE 10 です（実際の割合は 1 年の調査期間の開始時は 33 % で、1 年後には 23 % でした）。

さらに、Java の最新バージョンをインストールしているユーザの多くは、システムに古いメジャー バージョンをまだ残しています。他のソフトウェアのサポートに使用しているか、ただ削除していない場合もありますが、既知の脆弱性があるバージョンがまだ有効で、エクスプロイト可能な状態にあるということです。ユーザの他の防御として、侵入防御システムなどでも保護機能が実現しますが、保証にはなりません。エンドポイント側での防御に他の保護機能が欠けていれば、リスクは一層大きくなります。

Microsoft Office のインストール状況を調査した結果（前のページの図 16）、スイートの企業管理の課題が浮かび上がってきました。多少の自動更新が認められますが、ユーザの大多数は決まったバージョンを使用し、そのバージョンを使い続けています。アップグレードにライセンスまたは IT サポート コストが必要であったり、生産性ツールの動作を変更する機能変更がセキュリティ修正と同じパッケージで提供されることをユーザが恐れていると、既存のパッチの問題がさらに困難になります。

調査期間中に使用可能な Office のメジャー バージョンは 4 つありましたが、最新バージョンのリリースの導入率はそれほど多くありませんでした。広く導入されている 3 つのメジャー バージョンについて、その割合の内訳はおよそ 28-52-20 で、1 年を通じて上位への移行が多少進んでいます。メジャー バージョンへの移行にはライセンス処理が必要ですが、マイナー バージョンの更新は通常のソフトウェア メンテナンス ライフサイクルの一貫として実行されます。メジャー バージョンのほとんどがすべて最新のサービス パック バージョンで運用していると予測されましたが、最新バージョン（Office 2013/バージョン15x）に注目すると、区切りに指定した 3 つの主要なセキュリティ更新ポイントでほぼ均等に分割されます。

結論として、多くの大手ベンダーは、脆弱性パッチの通知、修正、配信をタイムリーに提供することで、セキュリティに関する責任を果たしています。ただし、このようなパッチ適用への配慮は、エンド ユーザには反映されず、その結果、エンド ユーザは自身の安全とビジネスを危険にさらしています。

迅速なパッチ リリースの利用に加えて、セキュリティ プロフェッショナルは、自動更新機能をタイムリーなパッチ適用の便利なツールとして使用することを検討すべきです。もっとも、一部のシステムは他のシステムよりも自動更新の適用が容易です。たとえば、ブラウザの更新はエンドポイントへの最も軽量な更新ですが、企業アプリケーションやサーバ側のインフラストラクチャは更新が困難で、ビジネスの継続性の問題を引き起こしかねません。そのため、それほど頻繁に対処されません。セキュリティ プロフェッショナルは、更新とパッチ適用の優先順位を決めて、既知で明白な脅威からネットワークを保護しなければなりません。

こうした課題に加え、セキュリティ リリースは機能リリースと混合されることが多く、現在使用している機能が変更されるので、ユーザが更新を回避する原因となります。リリースの混合によってサポートの負荷とベンダーの複雑性が増加します。

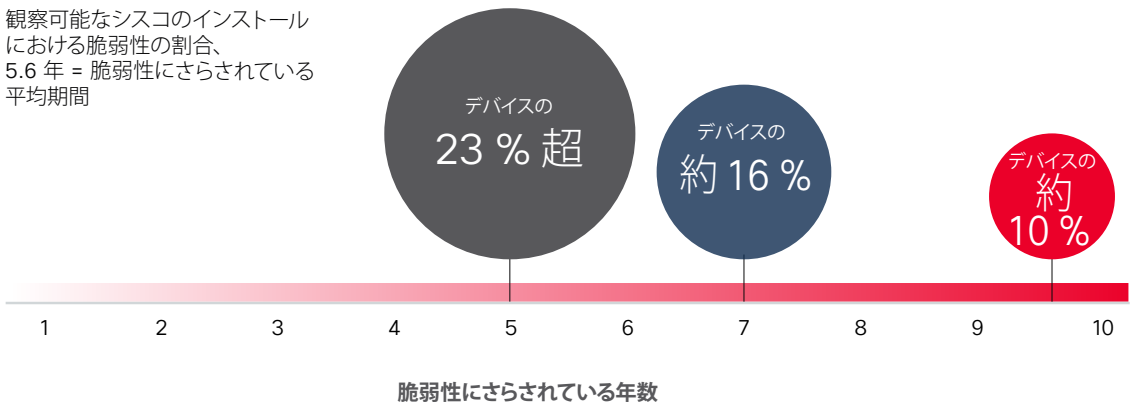
老朽化したインフラストラクチャ：ランサムウェアの増加により長期にわたる脆弱性へのパッチ適用が急務に

2015 年、シスコは、インターネット上およびお客様の環境における 115,000 台のシスコ製デバイスを分析し、老朽化したインフラストラクチャを適切に維持していない、または脆弱なオペレーティング システムにパッチを適用していない組織に警告を発しました。[4] 115,000 台のシスコ デバイスの 92 % を占める 106,000 台で、実行しているソフトウェアに脆弱性が検出されました。

このレポートでは、シスコ デバイスのサンプル セットを調査して、基幹インフラストラクチャ（ルータとスイッチ）で実行する既知の脆弱性の年代を確認します。サンプルには、インターネット上の 103,121 台のシスコ デバイスを使用しました（2002 ～ 2016 年の期間で既知の CVE による監視可能なソフトウェア）。各デバイスは、平均して 28 個の既知の脆弱性を実行していました。

このサンプルのデバイスは、既知の脆弱性をおよそ 5 年半の間実行していました。これらのデバイスの 23 % を超える割合に 2011 年にさかのぼる脆弱性がありました。16 % 近くのデバイスに、2009 年に初めて公開された脆弱性がありました。また、ほぼ 10 % に 10 年以上前から既知の脆弱性がありました（図 17）。

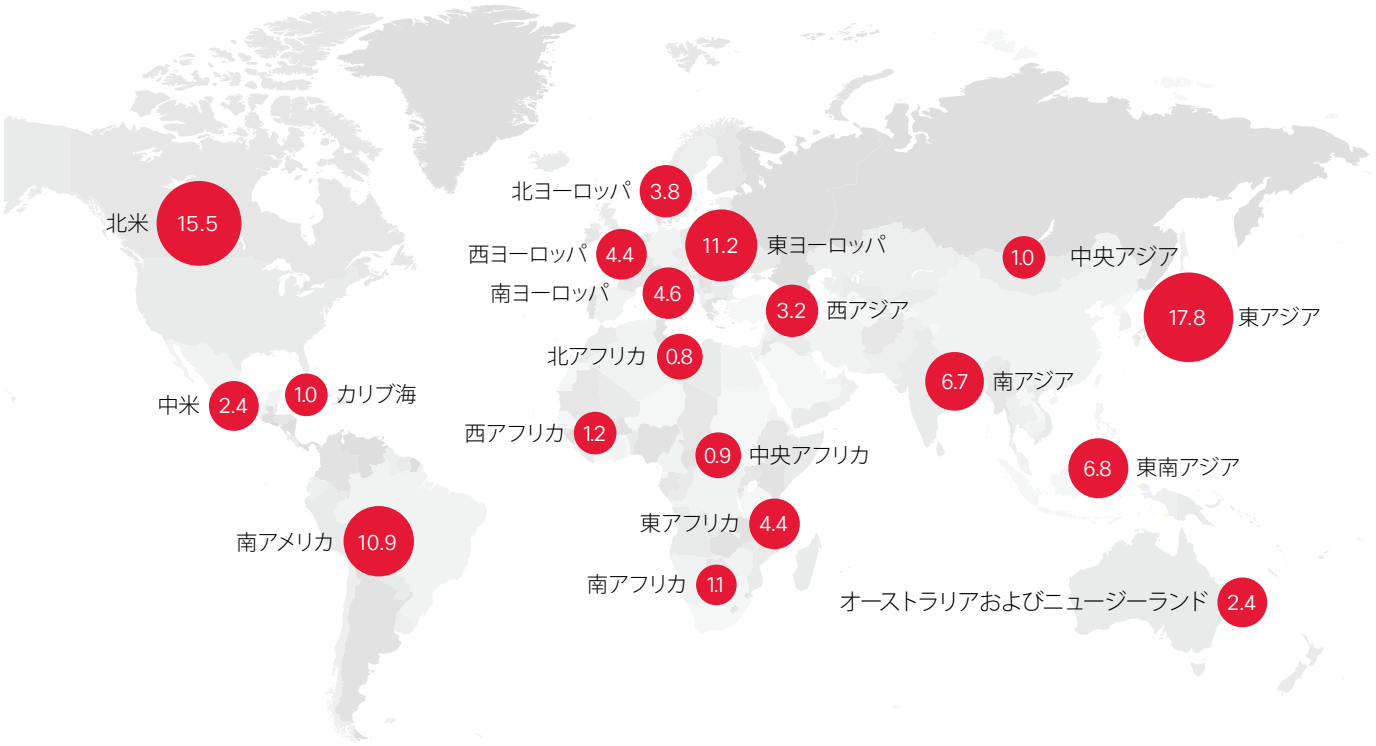
図 17. 既知の脆弱性が存続しているデバイスの割合（年数別）



出典：シスコ セキュリティ リサーチ

[4] 115,000 台のデバイスは、インターネットをスキャンして得られた 1 日分のサンプルと、その後デバイスを「裏側から」確認することで特定しました（インターネットからの観点とエンタープライズへの観点から）。分析方法の詳細については、2016 年シスコ年次セキュリティ レポートを参照してください。**cisco.com/jp/go/msr2015**

図 18. 脆弱なシスコ デバイス割合（地域別）



出典：シスコ セキュリティ リサーチ

シスコの調査担当者によると、脆弱なシスコ デバイスの割合が最も高かったのは、東アジア（17.8 %）と北米（15.5 %）でした（図 18 を参照）。

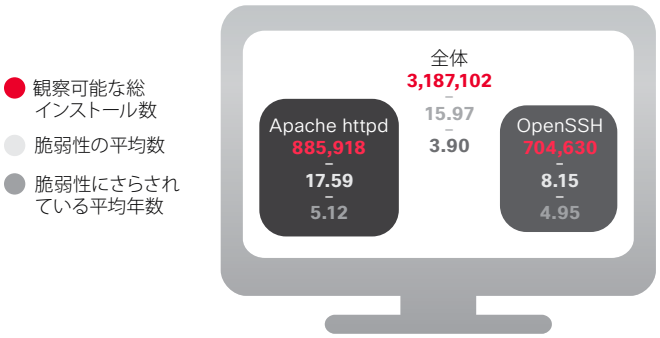
比較項目：脆弱なソフトウェア インフラストラクチャ

シスコの調査担当者は、一般的なソフトウェア インフラストラクチャにおける脆弱性を調査し、組織がこれらの製品にある既知の脆弱性へのパッチ適用をきちんと実施しているか確認しました（図 19）。脆弱性を持つ 300 万を超える監視可能なソフトウェアからなるサンプルには、多様な製品が含まれていましたが、その大半は Apache httpd（885,918）または OpenSSH（704,630）でした。これらのソフトウェア製品に関する既知の脆弱性の数は平均して約 16 個でした。

シスコの調査によると、Web サーバ ソフトウェアを使用している組織は、平均 3.9 年間、既知の脆弱性を実行しています。

地域別の結果については、北米、西ヨーロッパ、および東ヨーロッパにおいて脆弱なソフトウェアのインストール数が最も多いことが確認されました（図 20）。

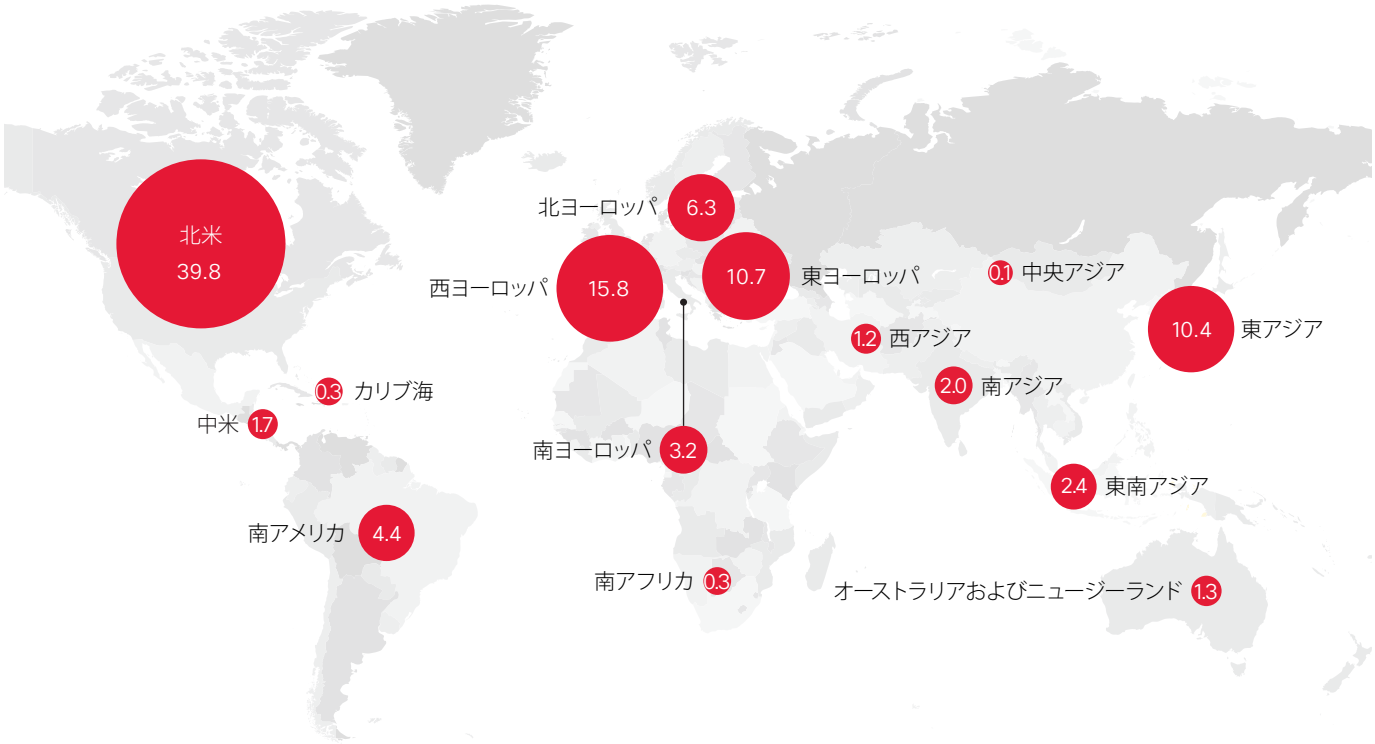
図 19. 脆弱なソフトウェアのインストール数（製品別）



出典：シスコ セキュリティ リサーチ

シェアする

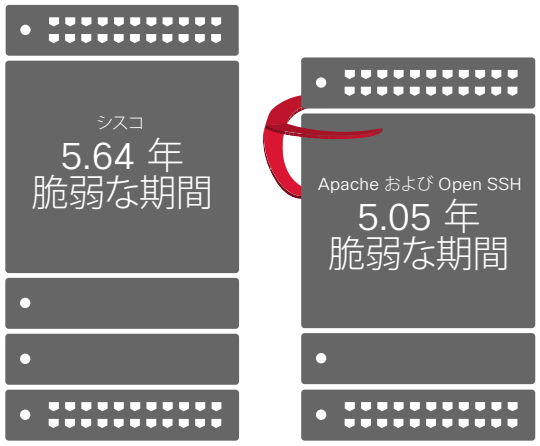
図 20. 脆弱なソフトウェアがインストールされている割合（地域別）



出典：シスコ セキュリティ リサーチ

シスコ、Apache、OpenSSH 製品の分析により、いずれの製品グループにおいても、既知の脆弱性への対応に組織は熱心ではないことがわかりました（図 21）。中には、面倒なアップグレード作業を行うよりもインフラストラクチャの交換時期まで待つことを選び、あまりに長く待機したので製品のサポートが切れてアップグレードできなくなっている組織もあるでしょう。いずれにしても、製品が平均 5 年間、既知の脆弱性を抱えたまま実行されていることがわかりました。

図 21. ソフトウェアのセキュリティ対策の概要：シスコ対 Apache および OpenSSH



出典：シスコ セキュリティ リサーチ

もう遅れは取らない：行動するのは今

組織にとってネットワーク インフラストラクチャのアップグレードは時間とコストがかかる作業ですが、必要な更新を怠ると、攻撃者にとって絶好のチャンスを与えてしまいます。SamSam ランサムウェア キャンペーン（**7 ページ**を参照）は、攻撃者がインターネット インフラストラクチャに長期間存在する既知の脆弱性を利用して、組織を無力化してコストを発生させる、標的を絞った攻撃を気付かれずに実行できるという証拠です（**18 ページ**の「JBOSS：インフラストラクチャ内の脆弱性が攻撃者に活動時間を与える」を参照）。

組織にとって特に重要なのは、シスコの分析対象の製品インストールのすべてが、適切なツールと専門知識があるユーザが外部から確認できるという点に留意することです。このユーザには脅威アクターも含まれます。

世界中の組織にとって、老朽化したインフラストラクチャとシステムの問題への対処に優先順位を付けることが不可欠です。これは単に、悪化するに任せている古い脆弱性にパッチを適用することだけではなく、導入されたインフラストラクチャとシステムの全体的な強みとサイバー攻撃耐性を評価することでもあります。多くの組織にとって、現実を直視して、サポートが切れてアップグレードできなくなったために現在のセキュリティの問題に対処できない製品から移行する時期が来ました。

発展途上国ではこうした取り組みが遅れていることが図 22 と図 23 に示されています。

図 22. シスコ デバイスに脆弱性が存在した平均年数（地域別）

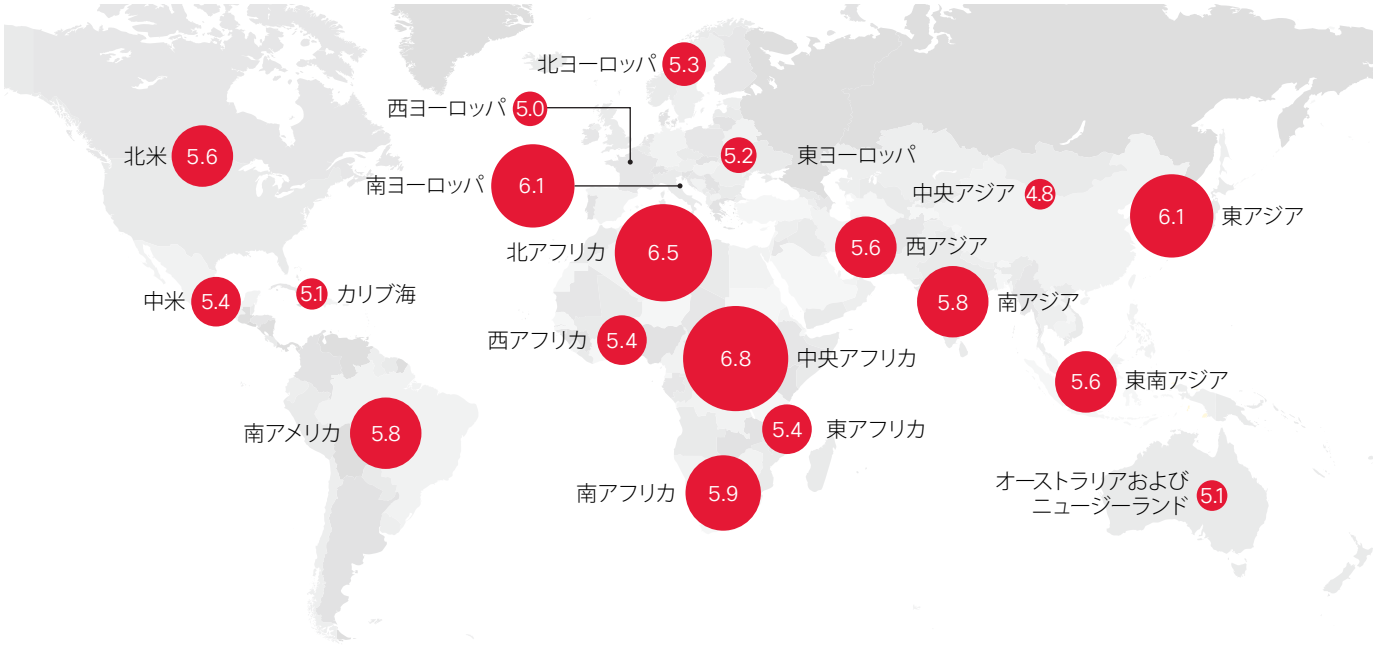
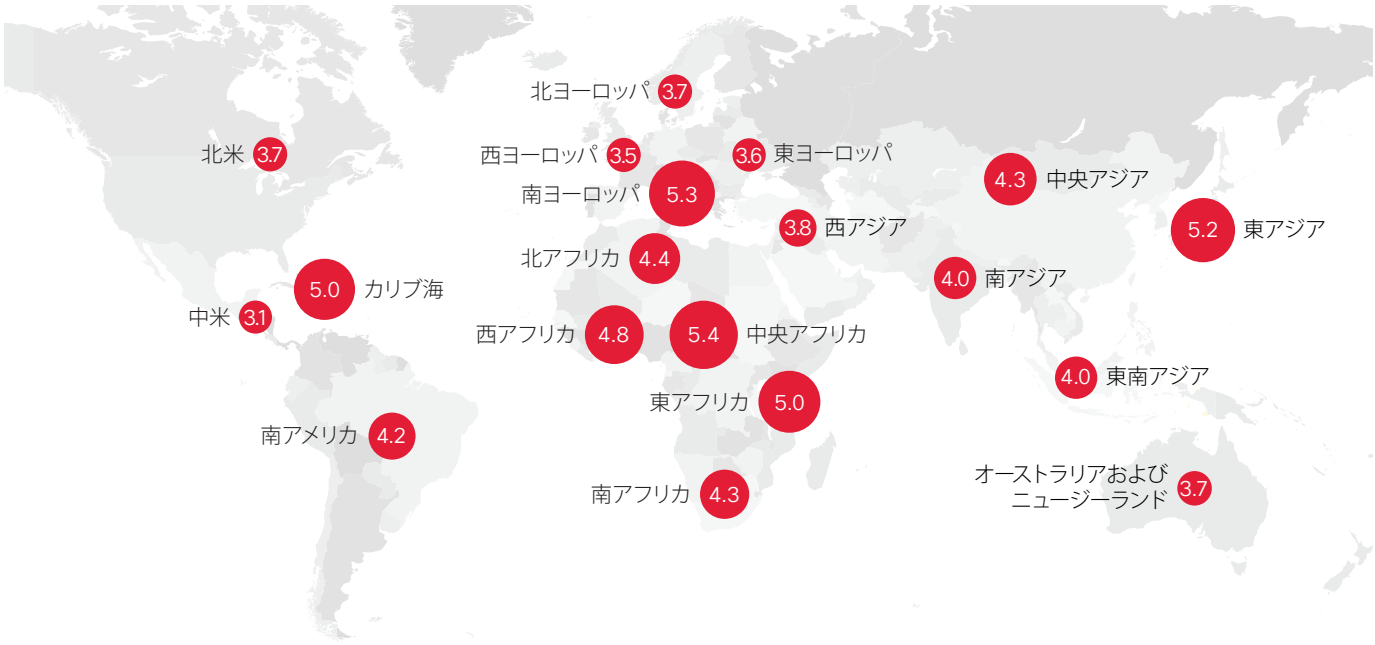


図 23. 各種のサーバ ソフトウェアに脆弱性が存在した平均年数（地域別）



出典：シスコ セキュリティ リサーチ

脆弱で安全ではないインフラストラクチャでは、新たな次世代のデジタル エコノミーに対応できません。デジタル化と Internet of Things がもたらすメリットを正しく実現するには、組織は最初のデジタル化の波によるセキュリティ問題に取り組む必要があります。

この問題の一因は、インターネット インフラストラクチャに組み込むべきセキュリティのニーズに関する見通しの甘さにあります。インターネットの創成期には、インフラストラクチャが攻撃者の標的になるなど誰も考えませんでした。しかし老朽化したインフラストラクチャのセキュリティの問題は、既知の脆弱性に対する修正を知りながら、対応を先延ばしにしている組織の責任でもあります。アップグレードのために重要なインフラストラクチャを一時的にオフラインにした場合の計算されたリスクに直面する代わりに、攻撃者の標的になることはないという、非常に低い可能性に賭けています。

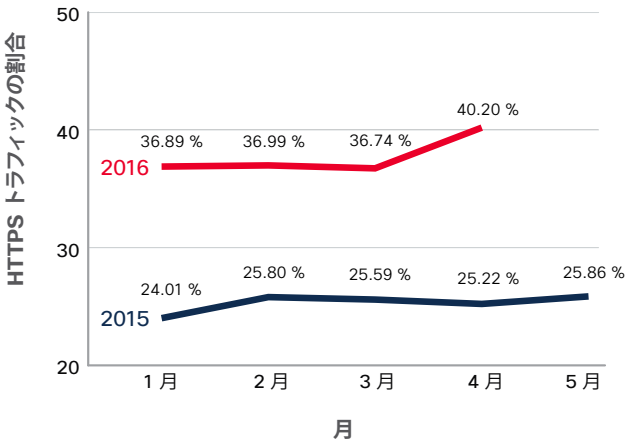
「セキュリティが確保されていない脆弱なインフラストラクチャでは、次世代のデジタル エコノミーをサポートできません。デジタル化と Internet of Things のメリットを実現するには、最初のデジタル化の波で生じるセキュリティ上の問題を解決する必要があります」

暗号化：2016 年の HTTPS トラフィックは今のところ横ばい

前回のセキュリティ レポートで説明したように、暗号化は、機密データおよび顧客のプライバシーの保護を模索する組織に好まれるツールとなりました。2016 年 1 月から 4 月の間、HTTPS リクエストの量は比較的一定していますが、それ以前の 2015 年は徐々に上昇し、年間を通じて大幅に増加していました。

2015 年における暗号化の利用増加から判断して、セキュリティ業界の専門家は、2016 年の現時点でのトラフィックの増加量は少ないものの、暗号化の利用は増加すると予測しています（図 24）。

図 24. 2016 年時点で比較的安定している暗号化 HTTPS トラフィック



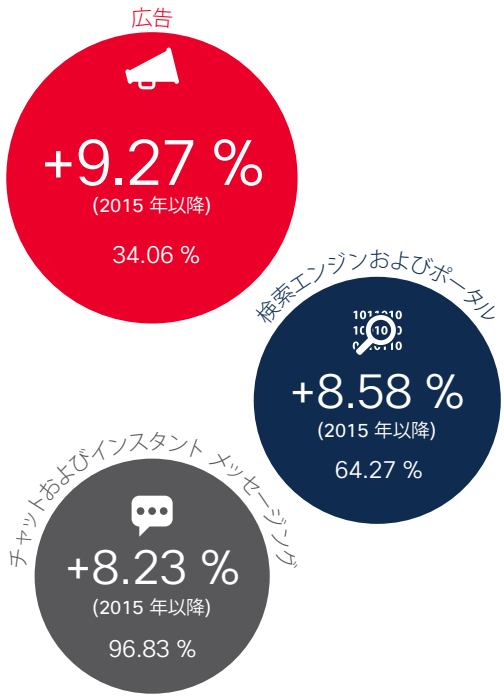
出典：シスコ セキュリティ リサーチ

広告分野では、2016 年の最初の 4 ヵ月間に HTTPS トラフィックの増加が見られました（図 25 を参照）。この増加は、ユーザのプライバシーを保護し、悪意のあるキャンペーンを阻止しようとする業界の動きのためと考えられます。しかし、増加の原因は、悪意のあるキャンペーンの開発者が HTTPS を多用した結果という可能性もあります。アドウェア感染の主なコンポーネントである広告インジェクタは、HTTPS を使用する悪意のあるキャンペーン数の増加の主な原因となっています。

HTTPS を使用する上位 3 件のアプリケーションは、図 26 に示すように、業務用電子メール、チャットとインスタント メッセージ、そして Web ベースの E メールです。

合法的な組織による暗号化の安定的な使用は、ユーザにとっては一般に朗報ですが、セキュリティ プロフェッショナルにとってはそれほど良いことではありません。犯罪者も、防御側からアクティビティを隠蔽する際の暗号化の価値を認識しており、不正アクターが活動を中断されずに継続する時間が増加しています（マルウェアの作成者による HTTPS の使用の詳細は、**22 ページ**を参照）。暗号化されたトラフィックによって隠されている侵害の指標（IOC）を確認できなければ、ポイント ソリューションの効果は低下し、防御側にとって、長期にわたる損害を被る前に悪意のあるアクティビティを見抜くのは、ますます困難な作業になります。

図 25. HTTPS マルウェア トラフィックの増加 2015 年 1 月 ～ 2016 年 4 月



出典：シスコ セキュリティ リサーチ

図 26. HTTPS を使用する主要なアプリケーション

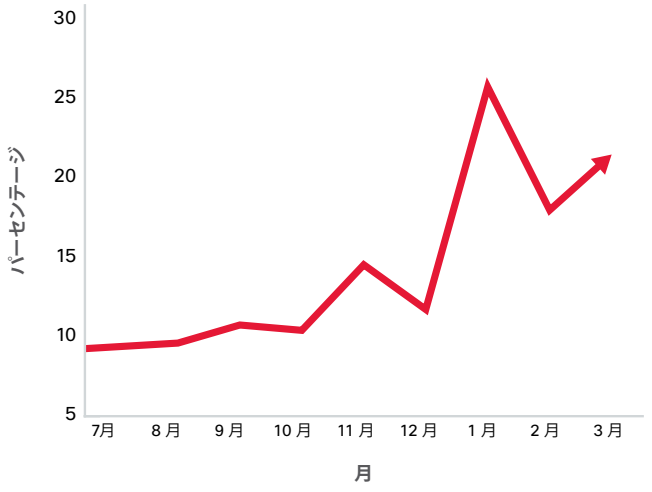
カテゴリ 1 月～ 4 月	HTTPS の平均（%）
企業 E メール	97.88 %
チャットおよびインスタント メッセージ	96.83 %
Web ベースの E メール	96.31 %
オンライン ストレージおよびバックアップ	95.70 %
インターネット電話	95.07 %
Professional Networking	90.78 %
ソーシャル ネットワーキング	81.15 %
ファイル転送サービス	67.63 %
ビデオ ストリーミング	64.71 %
検索エンジンおよびポータル	64.27 %
写真/画像の検索	61.90 %
Web ページ翻訳	54.60 %
SaaS and B2B	54.36 %

出典：シスコ セキュリティ リサーチ

TLS はペイロードを暗号化するが、マルウェアの動作は隠せない

より長い期間検出されずに稼働する方法を常に求めているマルウェアの作成者とユーザは、正規の目的でよく使用されるテクノロジー ツールを選択します。攻撃者に好まれる新たなツールとして Transport Layer Security（TLS）が挙げられます。これは、ネットワーク トラフィックの暗号化に使用される主流のプロトコルです。シスコの調査担当者は、暗号化されていない TLS ヘッダーを調べて、保護された通信に TLS が使用されていることを示すマルウェアのサンプルが、少数ではありますが増加していることを見つけました。このため、ディープ パケット インスペクションがセキュリティ ツールとして有効に機能しなくなってしまうので、セキュリティ プロフェッショナルの悩みの種となっています。

図 27. TLS を使用するマルウェア サンプルの割合



出典：シスコ セキュリティ リサーチ

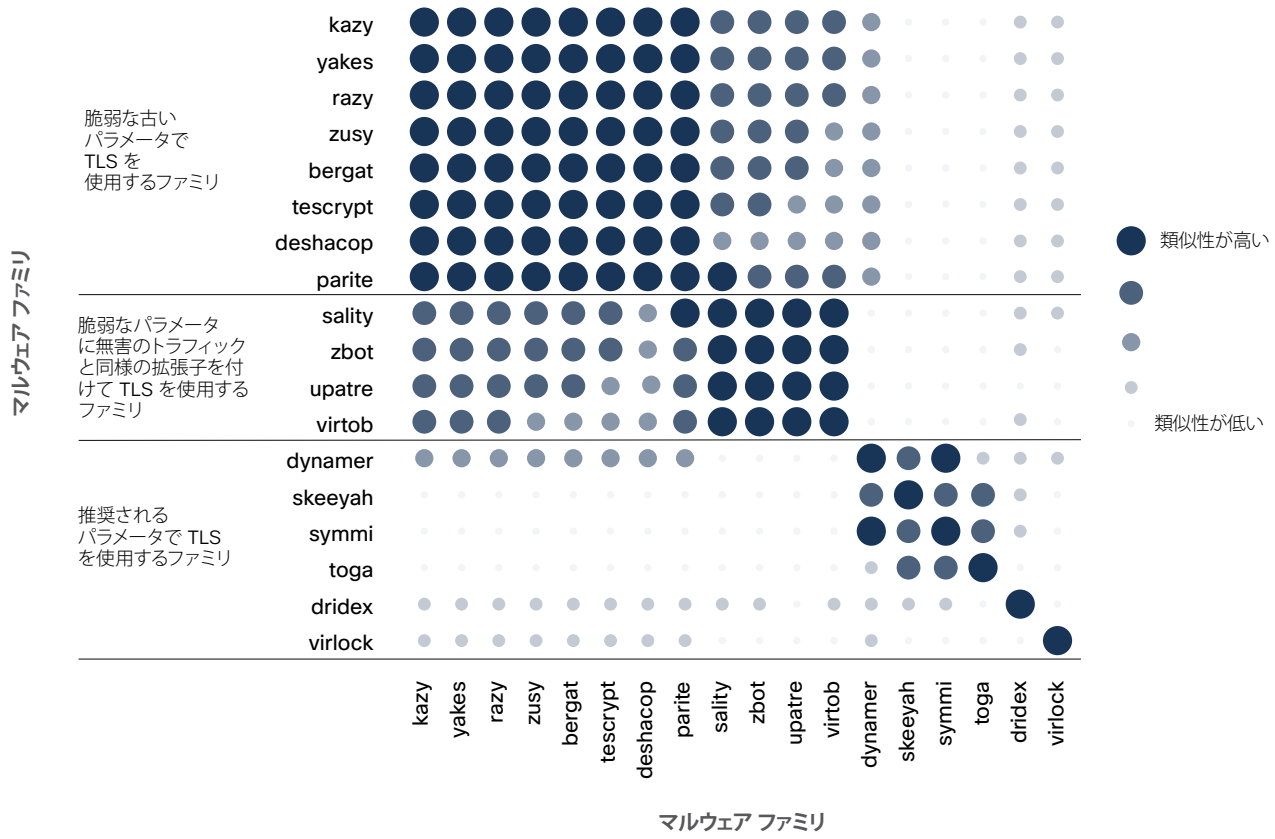
シスコの調査担当者によれば、すべてのネットワーク トラフィックの 60 % もが暗号化に TLS を使用しています。調査担当者が調査したマルウェア サンプルでは、約 10 % のマルウェアが TLS を使用していました。この割合は低いように思われますが、調査担当者は、無害なトラフィックでの暗号化の全体的な使用率が増加するにつれて、この数値も上昇すると考えています。2015 年 7 月から 2016 年 3 月までの期間で、暗号化された悪意のあるトラフィックでの数値の上昇が確認されています（図 27）。

不正アクターが TLS の使用を増やしていることを知ったうえで、セキュリティ プロフェッショナルはこの知識を利用して、こうした戦術を使用するマルウェアの検出をどのようにして改善できるでしょうか。マルウェアでの TLS の使用方法は、無害なトラフィックの使用方法とは異なります。大半のマルウェア ファミリにとって、この事実を使用して悪意のあるトラフィック パターンを高い精度で分類できます。

調査担当者が発見したように、マルウェアの作成者は通常、無害なネットワーク トラフィックで使用されるものよりも古い暗号化パラメータを使用します。マルウェアに使用される古い暗号スイートが、トラフィックに悪意があるという証拠を示す場合があります。無害なアプリケーションのほうが現行の TLS ベスト プラクティスを使用しますが、セキュリティを強化することで製品を差別化しようという動機があるからだと思われます。

その一方でマルウェアのユーザは、多くの運用環境で動作することがわかっており、エラーにもならないので、古い暗号化ライブラリを選びます。マルウェアの暗号化を阻むエラーの例として、マルウェア実行可能ファイルがホスト上にあると想定されるライブラリがない場合があり、このとき実行可能ファイルは実行できません。

図 28. TLS パラメータで比較したマルウェア ファミリの類似性



出典：シスコ セキュリティ リサーチ

マルウェア ファミリが TLS を使用するパターンを見つけるため、調査担当者は 18 種のマルウェア ファミリ、数千件の一意のマルウェア サンプル、数万件の暗号化されたネットワーク フローを調査しました。いくつかの方法でマルウェア ファミリを特定しました。

- TLS を推奨されるパラメータで使用する（Skeeyah マルウェアなど）
- TLS を弱いパラメータで使用するが、無害なトラフィックと類似した拡張で使用する（Sality など）
- 弱い古いパラメータを使用する（tescrypt など）

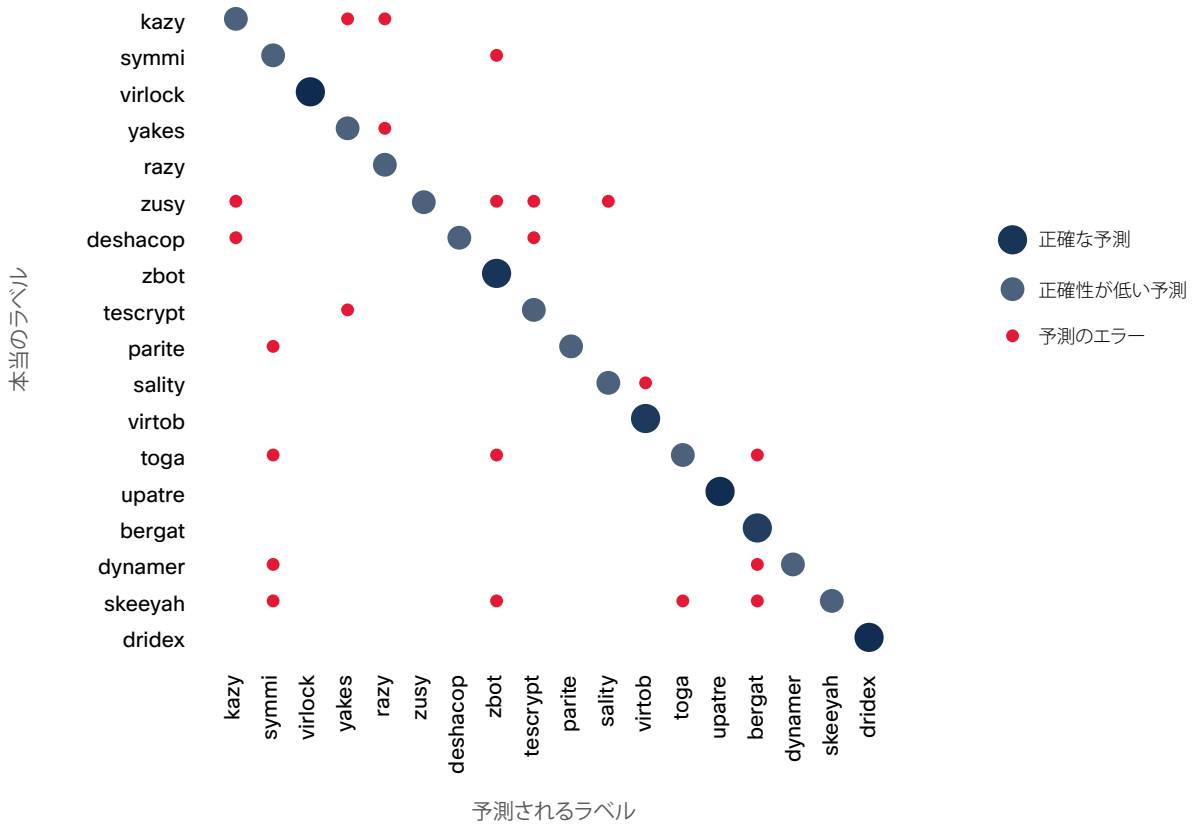
図 28 に示すように、調査担当者は、一部のマルウェア ファミリには TLS 暗号化の使用方法について類似点があることを実証できました。

混同行列（図 29）に、異なるマルウェア ファミリを容易に区別できることを示します。予測ラベルは実ラベル（大きな円）と一致率が高く、不正確な予測は一致率が低いものです（小さな円）。

当然ながら、TLS の使用方法を活発に進化させるマルウェア ファミリは、最も分類が困難です。ただし、TLS 証明書が自己署名かどうかなど、調査対象のトラフィックに関するドメイン固有の知識を適用すると、パターンを高い精度で特定できることがわかりました。たとえば、1 つの暗号化されたフローに制限された場合でも、86.8 % という精度で、ネットワーク通信を特定のマルウェア ファミリに正確に結び付けることができました。この結果は、特に単純な分類に加えて機械学習手法を使用する、統合された脅威防御の必要性とメリットの裏付けになります。機械学習法と新しいデータ ビューを組み合わせることで、セキュリティ プロフェッショナルは高品質な情報を得られます。

マルウェア サンプルを正確に既知のマルウェア ファミリに対応付ける機能は、セキュリティ プロフェッショナルにとって貴重です。このような対応付けにより、インシデント対応者は、対処している脅威の種類を、マルウェア サンプルのリバースエンジニアリングに取り掛かる前に把握できます。さらに、暗号化されたトラフィック フローを調査すると、インシデント対応チームは時間の優先度付けを改善できます。たとえば、最も重大度の高い感染に、より多くのリソースを割り当てられます。

図 29. 混同マトリクス：多様なマルウェア ファミリの識別



出典：シスコ セキュリティ リサーチ

検出時間の動向で浮き彫りになる白熱した「軍拡競争」

シスコは、「検出時間」(TTD)を、侵害から脅威が検出されるまでの時間と定義しています。この時間は、世界中に導入されているシスコ セキュリティ製品から収集したオプトイン セキュリティ テレメトリを使用して決定されています。グローバルな可視性と継続的分析モデルを使用して、エンドポイントで悪意のあるコードが実行された瞬間から、それが脅威であると判定されるまでの時間を、発生時には分類されていなかったすべての悪意のあるコードに対して測定できます。

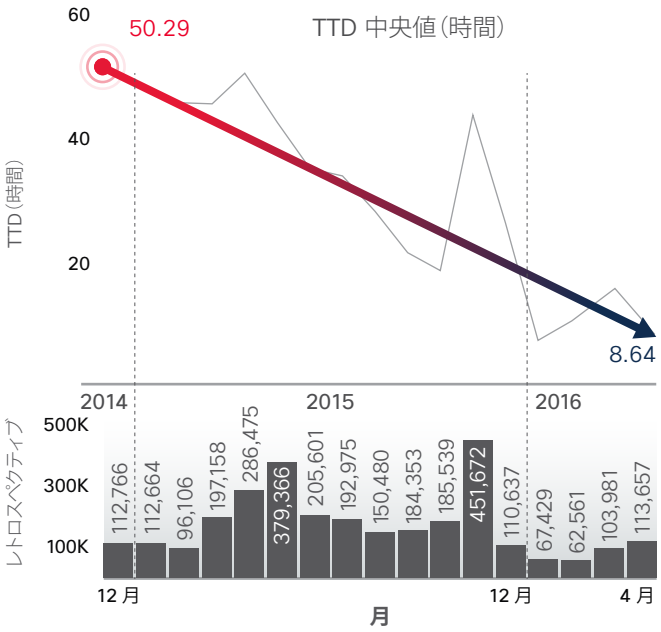
2014 年末から、TTD の短縮に向けて進捗状況を追跡しています。昨年、TTD 中央値は約 2 日(50 時間)であると報告しました。[5] 2015 年 10 月には、TTD 中央値を約 17 時間にまで大幅に短縮しました。

2015 年 12 月から 2016 年 4 月までの期間で、TTD 中央値はさらに短縮され、13 時間になりました。この数値は、調査期間の 5 つの中央値の加重平均です。

シスコの TTD 中央値は業界推定値の 100 ～ 200 日をはるかに下回り、多様な脅威を検出する能力を引き続き強化していきます。2014 年 12 月から 2016 年 4 月にかけて達成した TTD の全体的な減少を、図 30 に示します。

図 30 からは、TTD 中央値が着実に減少している様子がわかります。また、途中でくっきりした山と谷がいくつかあります。これらは攻撃者と防御側との「軍拡競争」の証拠です。

図 30. 月別平均 TTD 2014 年 12 月 ～ 2016 年 4 月



出典:シスコ セキュリティ リサーチ

シェアする

「シスコの平均 TTD は、業界の推定値である 100 ～ 200 日を大幅に下回っています。今後も脅威の検出機能向上に努めます」

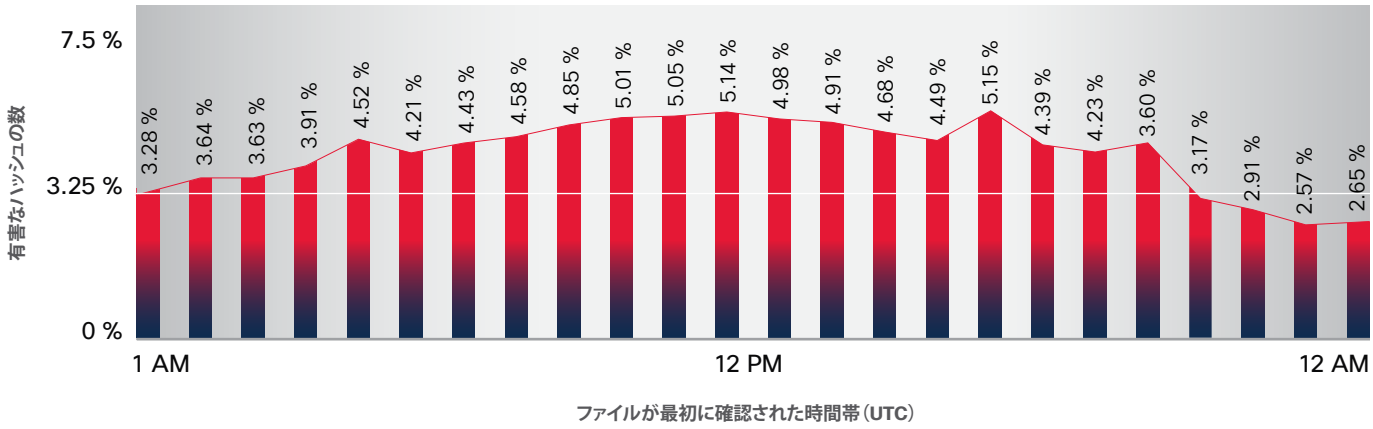
[5] シスコ 2015 年中期セキュリティ レポート:**cisco.com/jp/go/msr2015**

攻撃者は、検出をすり抜けようと常に人目に触れない技法を生み出します。セキュリティ ベンダーはこうした企みに対して、優れた統合と脅威の検出によって対抗します。そして、突き止めた侵害の指標（IOC）を自動化された検出テクノロジーに統合して、データにコンテキストを追加することで、お客様にとって実用的な脅威インテリジェンスになります（**53 ページ**の「侵害の指標は脅威インテリジェンスではない」を参照）。

TTD が大きく下がった時点は、シスコが攻撃者を打ち負かしたときで、攻撃者が新しい技法を開発して実行するよりも迅速に、脅威を検出しています。山の部分は、攻撃者が勝った期間を示します。検出するにはアナリストの作業やその他のインテリジェンス ソースが必要となるテクノロジーを使用したため、TTD 中央値が上昇しています。

攻撃者と防御側の軍拡競争に手加減はありません。攻撃者は新しい脅威を休みなく連続して繰り出し、セキュリティ ベンダーは特定にすばやい対応を迫られます。図 31 に、調査期間中（2015 年 12 月 ～ 2016 年 4 月）の標準的な 1 日に観察された有害なハッシュ（ファイル）の数を示します。全体として、有害なハッシュの割合は 1 日を通じて一定しています。

図 31. 有害なハッシュ検出数（時間別）



出典：シスコ セキュリティ リサーチ

「TTD の大幅な減少は、新たな手法が開発される前に脅威を検出することで、シスコが攻撃者の優位に立った期間を示しています」

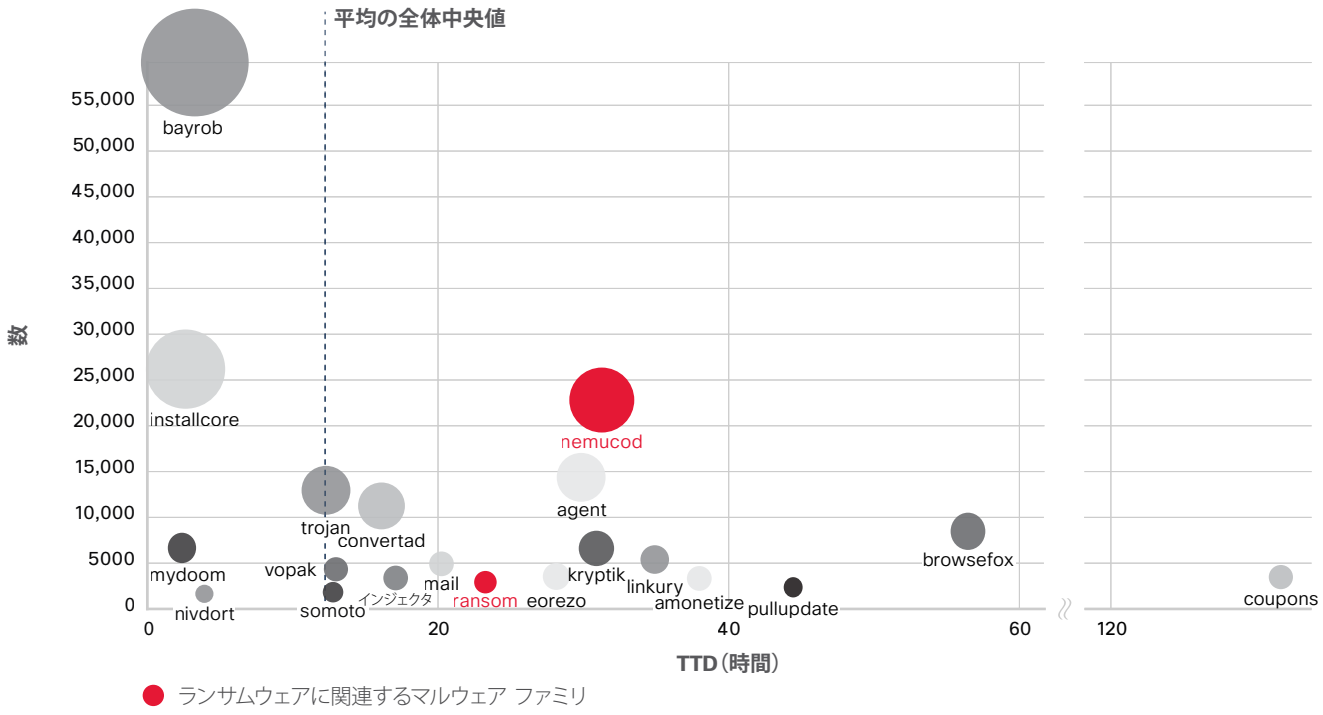
シェアする

ランサムウェアの急増：最近の TTD 中央値の変動の要因

前回のサイバーセキュリティ レポートで述べたように、地下経済の産業化や市販のマルウェア使用の増大は、2014 年 12 月以来、TTD を一貫して大幅に短縮する能力に強い影響を与えています。産業化された脅威は速やかに拡散し、検出は容易です。

2016 年になってから 5 ヵ月間でシスコが TTD 中央値（約 13 時間）付近で検出したマルウェア ファミリは、古いものですが、いまだに蔓延している脅威です。その 2 つの例を挙げると、Bayrob は2007 年から広まったボットネット マルウェアで、今年初めに復活したものです。もう 1 つの Mydoom は電子メールを通じて感染するコンピュータ ワームで、2004 年に最初に確認され、Microsoft Windows に影響します。有名な悪意のあるアドウェア InstallCore も普及しましたが、ランサムウェアの拡散を手助けする役割がその理由と思われます（図 32）。

図 32. 上位のマルウェア ファミリの平均 TTD（検出数が上位 20 のファミリ）



出典：シスコ セキュリティ リサーチ

シェアする

昨年におけるランサムウェアの急増は、特定のマルウェア ファミリの使用の増加と、それによる検出の増加を招きました。

ランサムウェアに関連付けられたいくつかのマルウェア ファミリについては TTD が中央値よりも高い傾向にあります。これは、ヒューリスティックやサンドボックスのような自動化された手法では早期検出が実現できないため、アナリストがこれらの脅威を調査する必要があり、その時間がかかるからです。

図 33 に、シスコが 2016 年 1 月から 4 月にかけて検出した、上位マルウェア ファミリの月別の推移を示します。強調表示した名前は、ランサムウェアに関連するマルウェア ファミリの例です。攻撃者による特定のマルウェア ファミリの利用が増減すると、TTD 中央値の変動につながります。検出にシスコのアナリストによる調査を要する脅威は、2016 年 2 月には 9 時間強だった TTD 中央値を、3 月には 14 時間以上に押し上げました。

図 34 は、TTD の短縮に取り組む防御側の課題を表し、組織が統合された脅威に対する防御を採用する必要性も示しています。TTD 中央値よりも早く検出できる脅威は、サンドボックスなどの自動化された方法で特定されます。新たに出現したより高度な脅威には、社内またはサードパーティの調査とインテリジェンスの活用が必要となるため、検出に時間がかかります。

マルウェア キャンペーンは次々と現れては消えていきますが、攻撃者と防御側との敵対関係だけは変わりません。攻撃者は常に、検出を回避できる脅威を作り出し、活動するための時間を延長しようとします。そして防御側は、こうした企てに絶えず対抗し、新たに出現したマルウェアを探し出し、見つけた侵害の指標（IOC）を自動検出テクノロジーに取り入れ、結果を現実の脅威インテリジェンスへと転換する必要があります。

シスコは今後数ヵ月間、継続して TTD 中央値を減少すべく注力します。各組織が自らの TTD 中央値を測定して改善に向けた取り組みを開始し、100 ～ 200 日という、現在の許容しがたい業界推定値の短縮に役立てることをお勧めします。

TTD および TTP（パッチ適用までの時間）実践方法の改善、暗号化の利用、そして老朽化したインフラストラクチャの問題への積極的な対処のすべてが相まって、攻撃者の制限のない活動空間の縮小に効果を発揮します。TTD と TTP は特に、防御側が攻撃の存在を検出する能力を改善すべき分野と改善する方法に集中し、攻撃者が戦術を変更して特定を回避する能力を制限できる、重要業績評価指標の役割を果たします。

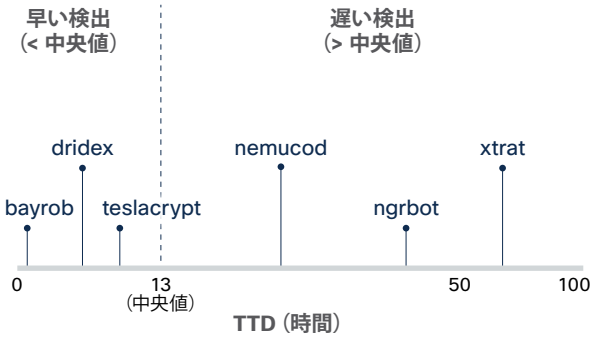
図 33. 検出された上位 10 のマルウェア ファミリ（月別）

	1 月	2 月	3 月	4 月
1.	bayrob	downloader	downloader	bayrob
2.	downloader	installcore	nemucod	downloader
3.	installcore	convertad	agent	installcore
4.	agent	msil	installcore	nemucod
5.	convertad	browsefox	convertad	agent
6.	ransom	linkury	mydoom	convertad
7.	linkury	nemucod	msil	fareit
8.	kryptik	agent	browsefox	msil
9.	browsefox	kryptik	kryptik	trojan
10.	msil	mydoom	vilsel	heur

● ランサムウェアに関連するマルウェア ファミリ

出典：シスコ セキュリティ リサーチ

図 34. 早期に検出されたマルウェア ファミリと遅れて検出されたマルウェア ファミリの例（13 時間の平均 TTD に基づく）



出典：シスコ セキュリティ リサーチ

インシデント対応：組織のセキュリティを損なう慣行

ネットワーク侵害、ランサムウェア攻撃、そして巧妙に作成されたマルウェアのニュースがセキュリティ メディアを賑わしています。そしてビジネスの停止やブランドの評判低下など、インシデントの影響も大きくなっています。しかしそうした攻撃は、多くの組織にとっては依然として寝耳に水です。実際にはセキュリティが脆弱でも、組織は脅威検出とインシデント対応システムが強固であると信じているためです。

そのような組織では多くの場合、最新の手法に比べて非常に古いセキュリティ テクノロジーとセキュリティ慣行を利用しています。したがって実際に攻撃が発生すると、ジェネラリストのセキュリティ プロフェッショナルはインシデント対応に要求される専門的なスキルがないため、対処できなくなってしまいます。

シスコがあらゆる規模の組織についてセキュリティの対応状況を調査したところ、セキュリティ強化のためのベスト プラクティスがない組織が多いことがわかりました。また攻撃者がそのような弱点を見つけ、ネットワークに侵入するチャンスとして利用することもわかっています。

たとえば、合併および買収（M&A）が行われる企業では、相手企業のリスクの状態について十分なデュー デリジェンスが行われない場合があります。M&A 後の企業でセキュリティ上の不備を認識しても、問題の修復が間に合わなかったり、ネットワークが複雑になって修復が困難になる可能性があります。最高情報セキュリティ責任者（CISO）は、M&A を開始する場合前に、セキュリティ保護について完全な評価を行う必要があります。少なくともカットオーバーの前に、それぞれのネットワークに疑わしい活動の痕跡がないことを確認しなければなりません。

「ネットワーク侵害を受けたことがないと報告する組織は、ネットワーク アクティビティに対する可視性が確保されていないと言えます。成熟した組織ではどこでも、コモディティ マルウェアや防御を侵害する試みなど、何らかのレベルの攻撃を受けているはずです」

ネットワークの評価が不十分であると、攻撃者はそれだけ長い間ネットワークに残存することができます。弱いパスワードや管理者権限を頻繁に使用するなど、不適切な慣行がある場合も同様です。高度な脅威に対抗できない組織の兆候としては、それまでにネットワークが受けた攻撃を認識していないということがあります。ネットワーク侵害を受けたことがないと報告する組織は、ネットワーク アクティビティに対する可視性が確保されていないと言えます。成熟した組織ではどこでも、コモディティ マルウェアや防御を侵害する試みなど、何らかのレベルの攻撃を受けているはずです。

また、攻撃者から見たら魅力的な弱点を十分に自己認識できていない組織もあります。貴重なデータを旧来の弱いセキュリティで守っていることがあるため、医療などの業界が近年、攻撃者を引き寄せる傾向にあります（**45 ページ**を参照）。シスコではさらに、攻撃者が学校などの脆弱な機関に注意を向け始めていることを指摘しています。セキュリティ防御が非常に低いと認識されているためです。効果的なインシデント対応をサポートするベスト プラクティスについては、**52 ページ**の「セキュリティに関する推奨事項」を参照してください。

医療機関に対するランサムウェア攻撃があらゆる組織にとってセキュリティの教訓となる

医療業界は今年に入って何度かのランサムウェア攻撃を受けています。ランサムウェア攻撃を受けた医療業界のシスコのお客様を分析すると、侵害の可能性を高めるような、企業レベルの脆弱性がいくつも発見されました。次のような脆弱性がありました。

- パスワードの共有があり、アカウントに過剰な権限が付与されている
- セキュリティ ロギングが不十分であるため、侵害されたパスワードを検出できない
- **OWASP** の上位 10 種類の脆弱性が Web アプリケーションで発見された
- オペレーティング システムとアプリケーションにパッチが適用されていない

さらにシスコの調査では、Windows XP、Adobe Flash Player、Java など、脆弱性がある同じバージョンが病院内のすべての PC で実行されている場合が多いことがわかりました。特に、医療機関のワークステーションで最近発生したランサムウェア感染は、シスコが調査したところ、Flash Player のパッチが適用されていないワークステーションから臨床スタッフが Web にアクセスしたことが原因であると判明しました。

セキュリティ パッチをすばやくインストールするための正式なプロセスがないということも、医療機関に共通する課題です。

さらに、ランサムウェアのターゲットになったほとんどの医療機関では、インシデント対応計画が確立されていないため、攻撃に効果的に対処することが困難になっていました。

また、専任のセキュリティ チームを置いている医療機関はほとんどありませんでした。IT 資産のメンテナンスは多くの場合、セキュリティの専門知識が不十分な、1 人または複数の IT ジェネラリストが行っていました。

同様のセキュリティ上の課題を抱える企業は、少なくとも次の対策をとり、全体的なセキュリティを向上させることをお勧めします。[6]

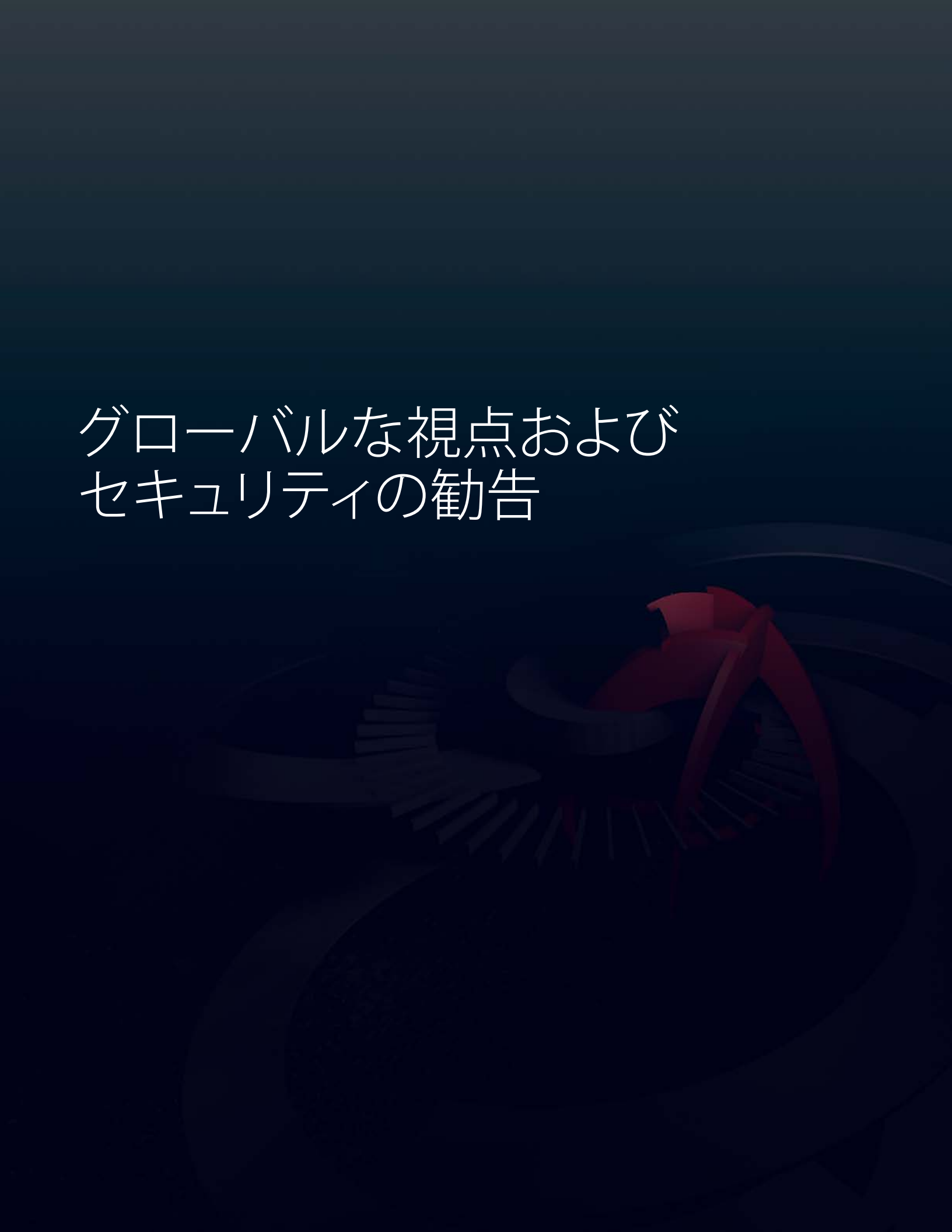
- マルウェアやハッキングを防御するために、システムの基本的な強化を行う
- 組織の IT 環境を評価する：ネットワークに接続しているデバイスの種類と数を特定するデバイスの場所を確認する
- 脅威とベスト プラクティスについてユーザに周知させる
- インシデント対応計画を作成する
- ネットワークを積極的に監視して侵害の痕跡を探す

セキュリティ上の既知の脆弱性に対応することも不可欠です。JBoss サーバに長く存在している脆弱性によって、最近の SamSam キャンペーンを実行した攻撃者は、インターネット インフラストラクチャ内を水平方向に移動して、医療機関のネットワークをターゲットにすることが可能になりました（**7 ページ**を参照）。シスコの調査担当者は、インターネット上の脆弱なデバイスとソフトウェアの数を考えると、インフラストラクチャをターゲットとしたランサムウェア キャンペーンがますます増えると予測しています（詳細については、**30 ページ**の「老朽化するインフラストラクチャ：ランサムウェアの増大を受けて古い脆弱性のパッチ適用が急務に」を参照）。

どの業界の組織も、医療業界でのランサムウェアの経験を教訓にすることができます。組織では、セキュリティ管理を担当するテクノロジー スタッフが、業務を効果的に行うために必要なツール、リソース、およびポリシーを持っていることを確認する必要があります。

[6] 注：組織がセキュリティ向上を図る場合は、準拠すべき規制や業界関連の各種指令を考慮する必要があります。こうした規制や指令は、組織がデータ保護やデータ プライバシーなど、セキュリティの特定の側面に取り組む方法に影響します。

グローバルな視点および
セキュリティの勧告



グローバルな視点および セキュリティの勧告

マルウェアは世界中のさまざまな場所から発生しており、攻撃者は必要に応じて、拠点をすばやく別の地域に変更しています。攻撃対象にならないと信じている組織でも、1 つはっきりしていることは、攻撃を受けない業種は存在しないということです。そして真の脅威インテリジェンスではなく、侵害の指標（IOC）によって脅威検出とインシデント対応を向上させようとする組織は、セキュリティ ポスチャを向上させることはほとんどできません。

一方、脅威がますます高度になる状況で、企業は別の不確実性に直面しています。データの制御またはアクセスの必要性に関する政府の関与が増え、相反する指示や法律、要件が生じています。このような関与によって、国際通商、セキュアなテクノロジー、信頼できるパブリック/プライベート パートナーシップに関して制限や不一致が生ずる可能性があります。

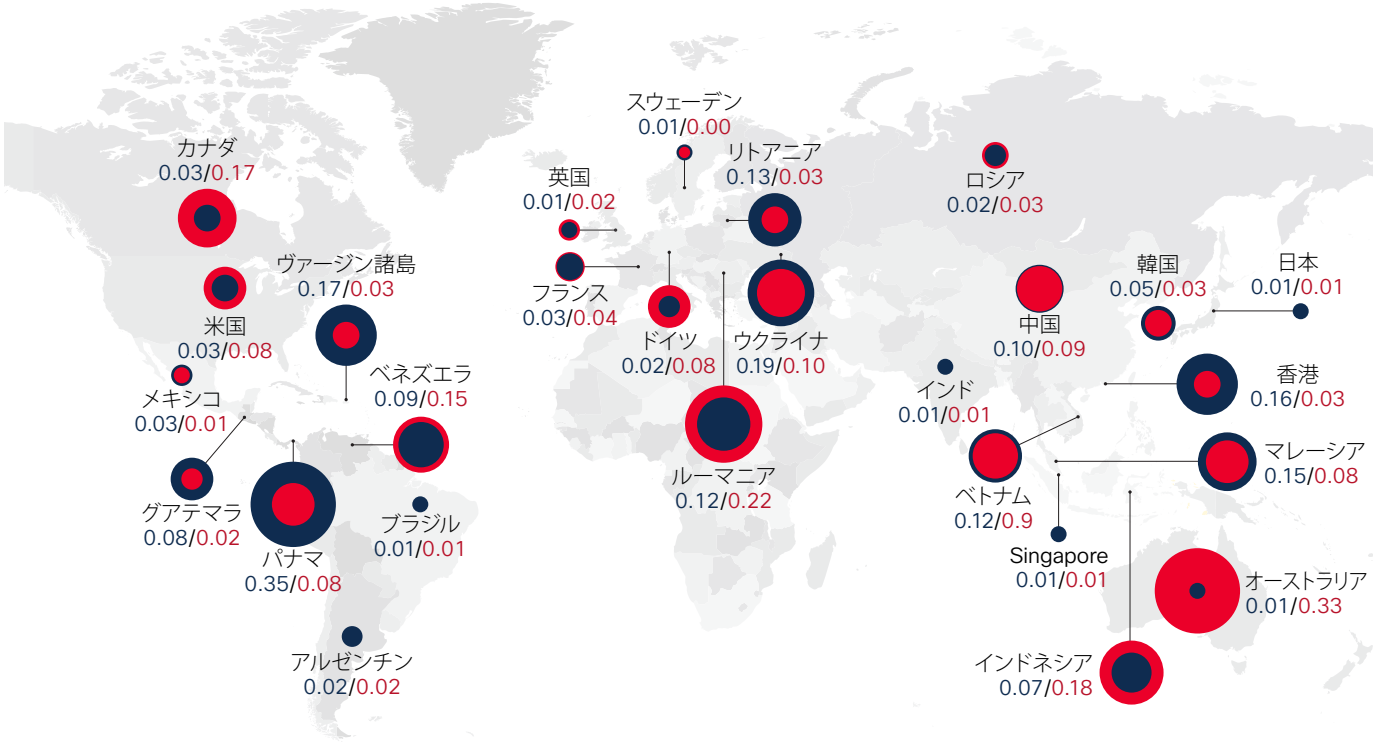
Web ブロック アクティビティの地域別概要

インターネット トラフィックの全体的なボリュームとブロック アクティビティを調査することで、シスコの調査担当者はマルウェアの発信元に関する情報を提供できます。南、北、中央アメリカでは、米国を除き、ブロックされたトラフィックの最大の発信元になっているのがカナダです。

欧州、中東、アフリカ地域では、全体のトラフィックの比率において、ブロックされたトラフィックを最も発信しているのはウクライナとルーマニアでした。アジア太平洋地域では、オーストラリアがトップになっています（次のページの図 35 を参照）。

簡単にハッキングできるサーバの有無などさまざまな理由で、攻撃者は拠点を置く地域を変更しています。

図 35. 国別 Web ブロック



出典：シスコ セキュリティ リサーチ

業種に関する調査によれば（**49 ページ**を参照）、マルウェア トラフィックの攻撃を受ける可能性がない国または地域は存在しません。マルウェアはグローバルな問題として考慮する必要があります。地域や国によっては、インフラストラクチャ内に悪用できる弱点を攻撃者が見つけたために、ブロック アクティビティが比較的高くなっている場合があります。さらに、2015 年 12 月と 2016 年 1 月にオーストラリアでマルウェア アクティビティが急増したことで、国ごとの比重とブロックされたトラフィックに顕著な変化があると考えられます。

マルウェアに遭遇する業界別リスク：攻撃を受けない業界はない

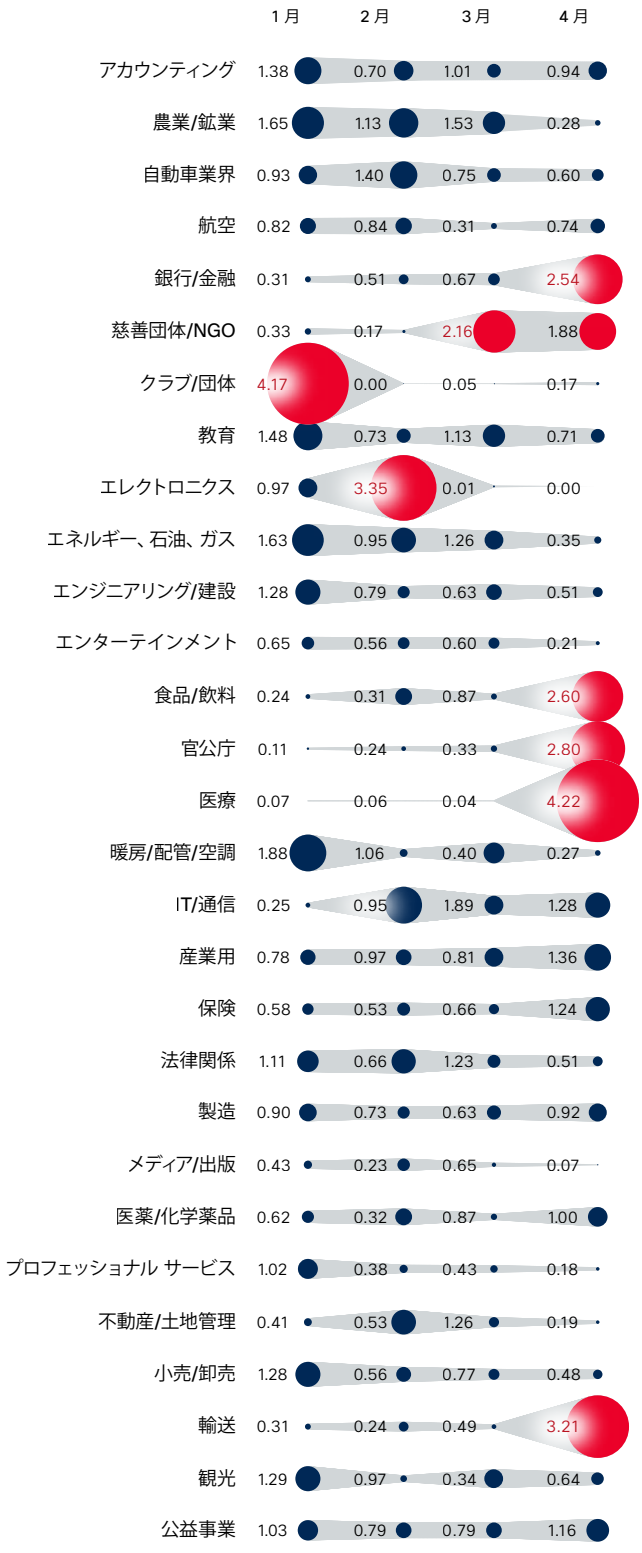
オンライン攻撃者のターゲットになるはずがないと信じるセキュリティ プロフェッショナルがいたら、その考えは間違いです。攻撃トラフィック（「ブロック率」）に関するシスコによる定期的な調査と、業界別の「正常な」トラフィックまたは予測されるトラフィックを考慮すると、マルウェアに対して安全な業種は存在しないことは明白です。どの業界でも、キャンペーンを実行する余地と時間を探す攻撃者のターゲットになる可能性があります。

医療業界はターゲットになりやすい業種であるとされていますが（**7 ページ**を参照）、シスコのデータによれば、2016 年の最初の数ヵ月で、他の業界でもそれに比例して多量のマルウェアが検出されています。たとえば各種のクラブ、組織、慈善団体、NGO、エレクトロニクス企業でブロック率が高くなっています。

このブロック率の調査からわかることは、あらゆる業界がリスクに直面しているということです。データによれば、ブロック トラフィックの急増は不定期に各種の業界で発生していますが、明らかなことは、ネットワークを侵害するチャンスを求めて、攻撃者がさまざまな業界をターゲットにし始めていることです。一度目的を達成すると、投資回収率が高い別の業界に移行していきます。キャンペーンは、業界がどこであるかよりも、利益が得られるところを狙って実行されています。

図 36 は、通常のネットワーク トラフィックに対する比率として、29 の業界とその関連するブロック アクティビティを示します。比率 1.0 は、観察されたトラフィックの量にブロック数が比例していることを示します。1.0 よりも大きい値は、予想よりも高いブロック率を表し、1.0 よりも小さい値は、予想よりも低いブロック率を示しています。

図 36. 月ごとの業界のブロック率（2016 年 1 月 ～ 4 月）



出典：シスコ セキュリティ リサーチ

地政的動向の最新情報：政府と企業のデータ保護に伴うジレンマ

地政的な観点では、テクノロジー ベンダー、通信会社、およびその他のグローバル企業がサイバーセキュリティを確立するには、複雑で相反することも多い規制に対処する必要があります。この状況では、一方では政府と企業の問題があり、もう一方ではプライバシーとセキュリティの問題があるため、セキュリティについて競合する要素を考慮することが求められます。

データ セキュリティは、市民の個人データの保護、または国営の送電網や水道システムの物理インフラストラクチャの統合に関わるものなど、政府機関では最優先事項になっています。しかし政府機関では合法的な傍受などによって、必要なときにデータにアクセスすることも求めています。

政府機関はテクノロジーとデータ アクセスに対して制御を失っていると認識していて、それを取り戻そうとする動きがあります。この必要性は、テロ攻撃やグローバル経済の低成長などによって強まっており、政府機関は市民と民間企業を守る能力を示すことを迫られています。

- Edward Snowden による情報漏洩事件の後に、個人の権利と国の権利の対立に関する議論が行われ、セーフ ハーバーなどの協定を見直す動きがあります。新しい EU-U.S. Privacy Shield は、欧州市民の個人データを政府によるアクセスから保護するよう、米国の企業に対して厳しく義務付けています。
- EU の移民問題に加えて、パリ、ブリュッセル、トルコ、米国などで発生しているテロ攻撃を受けて、暗号化されたプライベートな通信に法執行機関がアクセスすることの是非が議論になっています。この問題が世界的に関心を集める中で、米国 FBI と Apple Inc. は、テロリストが使用する iPhone のロック解除について対決を強めています。
- 政府機関と民間セキュリティ企業は、国家的な諜報活動と窃盗に対して、積極的に対応しようとしています。北朝鮮が銀行に対して、国際金融ネットワーク SWIFT（Society for Worldwide Interbank Financial Telecommunication）を利用した攻撃を仕掛けたと言われています。またドイツ政府は、ドイツ連邦議会に対する攻撃がロシア政府によるものだと主張しています。

世界中の政府が、テクノロジーに対するコントロールを強化し、テロやサイバーセキュリティなどの脅威に対抗できる対策を検討しています。その過程で、新たな脆弱性が明るみに出るリスクがあります。また場合によっては、それらの脆弱性を悪用する権利も留保していることになります。この情報は、必ずしもすべてテクノロジー ベンダーと共有する必要はありませんが、そこで 1 つの疑問が生じます。脆弱性の公開については誰が責任を持つのかということです。民間企業は、政府介入の強化への市民反応に対して、対応していかなければなりません。

しかしグローバリゼーションが急速に進む一方で、サイバーセキュリティや、透過性、アカウンタビリティ、データ保護、暗号化などの問題に対する、グローバルに統一された対策はない状態です。グローバルなインターネットのための「交通規則」を確立する努力は継続されますが、優先順位の違いがあるため、企業は政治的かつ法的なリスクが大きい環境で存続する必要があります。

「グローバリゼーションが急速に進む一方で、サイバーセキュリティや、透過性、アカウンタビリティ、データ保護、暗号化など関連する問題に対する、グローバルに統一された対策はない状態です」

規制環境の進化

グローバルな通信会社やテクノロジー ベンダーは、自国の法的枠組みと国民の期待に応えながら、各国の規制に準拠しなければなりません。しかしこれは、各国の法律が多様であるため容易ではありません。

たとえば英国政府の Investigatory Powers Bill では、今年末までに 1 つの法律によって、英国のセキュリティ サービスによる監視を統合しようとしています。この法案については現在、英国議会で議論されています。政治家、企業、人権団体は、法案で議論の対象になっている各種対策を取り上げています。これには、「オンデマンド復号化」条項も含まれています。そこでは、テクノロジー ベンダーと通信プロバイダーが、英国のセキュリティ サービスの要求に応じて、暗号化を解除できます。

その他の国はさらに対策を進めていて、そうした方策を強化する取り組みを行っています。例：

- EU では、Network and Information Security Directive がこの夏にまとまる予定です。
- フランス議会では、テロ対策法案が議論されています。この法案には、企業に対する多額の罰金と、テロに関する捜査協力を拒んだ役員の懲役刑に関する規定が含まれています。法案の支持者は、11 月にパリで起きたテロに伴う非常事態が解除される前に、法案が成立することを望んでいます。
- ハンガリー政府は、暗号化ソフトウェアを違法にする法律を議題に挙げています。
- ロシアと中国では、テロに関する懸念の増大に応じて、国内のテクノロジー ネットワークに対する管理を強化する対策が推進されています。

こうした対策はすべて、要件が厳格であり、予期しない法的な問題が発生する可能性もあるため、通信会社とテクノロジー ベンダーにとって懸念事項になっています。

複雑性によるセキュリティの低下

このように規制上の複雑性が増大する状況は、民間企業にとって大きな課題になります。複雑性が増大すれば、最終的にセキュリティが低下し、攻撃者が悪用できる隙が増えてしまうことになります。

- 米国は特殊な状況にあり、現時点まで、政府にとって有益なデータのほとんどが米国政府のサーバに保存されてきたという事情があります。米国政府によるこの活動は現在行われていません。ドイツ、ロシア、中国などの各国では、データ ローカリゼーションに関する法律と規制プラットフォームの確立に取り組んでいます。
- 米国は、英国の Investigatory Powers 法を超える厳格な法律の制定を検討しています。この法律は、ソフトウェアまたはハードウェアを製造する企業、またはアプリ ストアを運営する企業に対して、政府機関が解読できる形式でデータを提供し、テクノロジーを「リバース エンジニアリング」するための機能を組み込んで、明確なデータを引き渡すことを要求するものです。

グローバルな一連のイニシアチブがない状態では、政府と民間企業はサイバーセキュリティについてのコミュニケーションを充実させ、お互いの理解を深めることがかなり必要になります。この取り掛かりとして、データ リクエストを効果的にやり取りできるシステムは、合理的と言えます。ただ、政府と民間企業間の情報共有が重要なのは確かですが、解決しなければならない意見の相違もあります。

たとえば企業は、テクノロジー ベンダーにデータへの「バック ドア」を提供するように強制することは、短期的にはセキュリティ上のメリットを得られるかもしれないが、最終的には消費者の信頼を破壊する可能性があると主張しています。そうなると、経済のバックボーンであるそれら企業までもが損害を受けてしまいます。

官民の双方にとって、データ保護はジレンマに陥っています。EU-U.S. Privacy Shield などの取り決めは、国と国との間でデータを速やかに移動できるように考えられており、分析を通して、消費者には消費者自身やデータを危険にさらすことなく、データを移動できるという信頼を与えることができます。ただ、消費者がこれらの対策を受け入れるかどうかはまだわかりません。

「グローバルに統一されたイニシアチブがない場合は、政府機関と民間企業の間で、サイバーセキュリティに関する理解を共有することが不可欠になります」

セキュリティに関する推奨事項

次世代ランサムウェアが進化するにつれ、組織は「防御の最前線」で対策を講じ、水平展開や増殖の機会を阻止して敵が攻撃する時間を与えないようにする必要があります。この最前線の対策には、脆弱なインターネット インフラストラクチャやとシステムへのパッチの適用（**22 ページ**と **29 ページ**を参照）やパスワード管理の改善（**44 ページ**）などの基本的なベスト プラクティスに加えて、ネットワークのセグメンテーションも含まれます。

ネットワークをセグメント化することで組織は、自己増殖型の脅威の水平方向の動きを阻止または鈍化させ、それらを封じ込めることができます。セグメント化されたネットワークには多くの要素がありますが、組織は以下の要素の実装を検討する必要があります。

- ワークステーション レベルなど、データへのアクセスを論理的に分離する VLAN やサブネット
- 専用のファイアウォールとゲートウェイによるセグメンテーション
- イングレスとイーグレスのフィルタリングが設定されたホスト ベースのファイアウォール
- アプリケーションのブラックリストとホワイトリスト
- ロールベースのネットワーク共有のアクセス許可（最小権限）
- 適切なクレデンシャル管理

最後の砦：バックアップ リカバリ

バックアップ リカバリは、現在はもちろん今後においても、ランサムウェア（**10 ページ**）でデータを暗号化してしまう攻撃者に、「高額な身代金」を払いたくない組織にとって最後の砦です。ただし、データの損失やサービスの中断を最小限に抑えてランサムウェア攻撃から復旧できるかどうかは、システム バックアップやディザスタ リカバリ サイトが侵害されたかどうかに左右されます。

ランサムウェアで攻撃者によってローカルのバックアップが削除されたり、アクセス不能になってしまった場合には、オフサイトのバックアップが身代金を払わずに組織がサービスを回復させる唯一の望みになります。バックアップをどれくらいの頻度でオフサイトに送るかによって、アクセス不能になるデータや失われるデータ（ある場合）の量が決まります。

ブラウザ感染の脅威を放置しない

広告インジェクタが HTTPS 暗号化トラフィックを通して悪意のある広告を表示する場合、防御側はすぐにはその脅威に気付くことができません（**21 ページ**を参照）。攻撃者たちはそれぞれの活動の隠れ蓑として HTTPS を使うことが増えているため、セキュリティ チームは、ブラウザ感染を組織やユーザにとって重要度の低い脅威として放っておくことがもはやできなくなっています。

一見無害に見えるブラウザ感染はすぐに重大な問題に発展することがあり、攻撃者がリスクの高い攻撃の土台作りに使用する重要なツールとして、悪意のある広告インジェクタが浸透していることが浮き彫りになっています。

ブラウザ感染のモニタリングの優先順位を高くすることで、組織はこれら脅威を迅速に特定して修正する体制を整えることができます。動作分析ツールとコラボレーティブな脅威インテリジェンスは、防御側にとってこれらのタイプの脅威を修復する重要なリソースになります。また、ポップアップ広告やその他の不要な広告の増加をセキュリティ チームに知らせるようにユーザを教育することも、重要な防御策になります。

日常的な作業としてパッチ適用サイクルを組み込む

規模や業界を問わず、すべての組織が、最新の脅威には不十分な「項目をチェックするだけ」のアプローチからさらに先に進む必要があります。「セキュリティが第一」という姿勢には、セキュリティ防御に資金を投入するだけでなく、脅威に対する防御を統合することが必要です。

たとえば、セキュリティ プロフェッショナルは、あるはずのないシステム アカウントや管理者アカウントがないかどうか、利用可能なツールを活用して定期的に確認してください。また、悪意のあるトラフィックに関するすべてのネットワーク通信を記録して分析し、IOC が疑われるトラフィックがないか確認してください。このような詳細な調査を行うのに必要なツールを提供することもリーダーの役割です。

さらに、日常的な作業としてパッチ適用サイクルを組み込むことで、提供されている最新のパッチを使って環境を最新の状態に維持し、オペレーティング システムや広く使われているソフトウェアの弱点を脅威の攻撃者が見つけて悪用しないようにしてください。

侵害の指標は脅威インテリジェンスではない

IOC は脅威インテリジェンスに関係し、脅威アクティビティの構成要素になります。しかし、このデータは調査を実施する防御側にとって貴重なものですが、IOC 自体は脅威インテリジェンスではありません。

組織は、脅威インテリジェンスであるとされる侵害の指標（IOC）に何百万ドルも費やすことがあります。しかしそのデータをビジネスに適応した形で活用できるかどうかは、セキュリティ チームにかかっています。このプロセスは多量のリソースを要するため、セキュリティ担当者が優先順位の高い業務に取り組めなくなる可能性があります。場合によっては、IOC に依存することで、攻撃から確実に保護されているという誤った前提が作られ、組織のセキュリティ ポスチャが正しく認識されなくなります。

では脅威インテリジェンスとは何でしょうか。それは、データが生成されたコンテキストを理解した上で、実用的な情報に変換されたデータです。脅威インテリジェンスでは、「データの背景を考慮して次に何をすべきか」が明確になります。こうしたビジネス レベルでの適応がなされていないデータは、砂浜の砂と同じように意味のないデータにすぎません。

組織が真の脅威インテリジェンスに投資してメリットを得るには、IOC と、組織にとって意味のあるコンテキスト、そしてデータの使用方法を組み合わせて提示できるセキュリティ ベンダーを見つけなければなりません。そうしたベンダーでは、プロセスに人的な要素を加えて、得られた情報をセキュリティ ツールに反映させます。それによって、セキュリティ チームにとってすぐに役立つ脅威インテリジェンスが実現します。

IOC と脅威インテリジェンスは区別することが重要です。脅威インテリジェンスによって、防御側は攻撃の全体像を把握し、検出とインシデント対応を向上させることが可能になります。

「IOC と脅威インテリジェンスは区別することが重要です。脅威インテリジェンスによって、防御側は攻撃の全体像を把握し、検出とインシデント対応を向上させることが可能になります」

まとめ

現在の攻撃は、防御側の能力を上回っているのが現状です。攻撃者が時間の制約を受けることなく自由に活動し、新しい技術を開発できるのであれば、攻撃者の成功は保証されたも同然です。しかし、土台を準備して攻撃を仕掛ける時間や機会を組織が制限できれば、攻撃者は存在が見つかってしまう危険、さらには封じ込められる危険にさらされ、切羽詰まった状態で判断をしなければならなくなります。

脅威を進化させ続けなければならない状況に攻撃者を追い込んで形勢を逆転することは、攻撃の時間を減らす戦略の 1 つになります。攻撃者は、クリアしなければならないことが増えるほど、最終的に身元の判明につながる痕跡を残す可能性が高くなります。どれだけたくさんの方法で検出を逃れようとしても、足跡を隠そうとしても関係ありません。

以上が TTD を測定することが重要である理由です。防御側は、脅威を検出する自分たちの能力の現状がわかっていなければ、改善のしようがありません。TTD と TTP（パッチを適用するまでの時間）を重要業績評価指標と考えて利用してください。そうすることでセキュリティ チームは、攻撃者を封じ込めて戦略を変更せざるを得ない状況に追い込むための方法に集中できます。

常にそうだったように、脅威の攻撃者の活動時間を減らす上で重要な役割を果たすのは、組織とエンド ユーザです。企業にとって、セキュリティ対策を改善するのに、おそらくこれほどよいタイミングは、あるいはこれほど差し迫っていることはありません。

老朽化したインフラストラクチャとシステムをアップグレードし、既知の脆弱性にパッチを適用すれば、これら資産を悪用してさまざまな犯罪に手を染めようとしているサイバー犯罪者の能力を弱体化することができます。SamSam ランサムウェア攻撃の仕掛け人は、闇経済の仲間たちに、未開拓の新しい領域は、ユーザを危険にさらし、収益性を新たなレベルに引き上げるために悪用できる古い脆弱性でいっぱいであることをすでに知らしめています。（「ランサムウェア：脅威的なスタミナで莫大な金を生み出す」**7 ページ**を参照）。

多くの組織はインターネット インフラストラクチャの転換点を迎えています。また、コストを削減し、新たな次世代のデジタル エコノミーでの成功を実現する強力な IT 基盤を構築するために、デバイスやソフトウェアを簡素化して新しくしたいと考えています。今こそ、セキュリティを強化してネットワーク全体の可視性を実現するチャンスです。そしてこれこそが、今はまだ攻撃者たちが制約されることなく、自由に攻撃を仕掛けている時間をなくすのに役立ちます。

「多くの組織が、インターネット インフラストラクチャの転換点に差し掛かっています。今こそネットワーク全体のセキュリティを強化し、可視性を高めるべきです。そして攻撃者が無制限に活動できる範囲を狭めることが重要です」

シスコについて

シスコは、実世界にインテリジェントなサイバーセキュリティを提供し、広い範囲に及ぶ攻撃ベクトルに対して、業界内で最も包括的で高度な脅威保護ソリューションのポートフォリオを提供しています。シスコによる脅威中心型の運用化されたセキュリティ アプローチを採用すると、複雑さが緩和され、分断化が抑えられます。同時に、優れた可視性、一貫した管理、そして攻撃前、攻撃中、攻撃後の高度な脅威保護が提供されます。

Collective Security Intelligence（CSI）エコシステムの研究者は、デバイスとセンサーの膨大なフットプリント、パブリック フィードおよびプライベート フィード、シスコのオープン ソース コミュニティから取得したテレメトリを使って、1 つの傘の下に業界トップの脅威インテリジェンスを集結させています。これにより、何十億もの Web リクエストと何百万もの電子メール、マルウェアのサンプル、およびネットワーク侵入という量が毎日取り込まれています。

当社の高度なインフラストラクチャとシステムでこのテレメトリを処理することで、機械学習システムと研究者は、ネットワーク、データセンター、エンドポイント、モバイル デバイス、仮想システム、Web、電子メールの境界を越える脅威、さらにはクラウドからの脅威を追跡して、根本原因と発生範囲を特定することができます。その結果得られたインテリジェンスは、当社の製品とサービス提供に対するリアルタイムの保護に変換され、全世界のシスコのお客様に即時に提供されます。

シスコの、脅威中心型のセキュリティ アプローチについては、**www.cisco.com/jp/go/security** を参照してください。

シスコ 2016 年中期サイバー セキュリティ レポートの執筆者

TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

Talos は、シスコの脅威インテリジェンス組織で、シスコのお客様、製品、およびサービスに優れた保護を提供するために尽力するセキュリティ専門家のエリート グループです。Talos は、最先端の脅威研究者で構成され、既知の脅威と新たな脅威を検出、分析、防御するシスコ製品向けに脅威インテリジェンスを構築するための高度なシステムでサポートされています。Talos は、Snort.org、ClamAV、SenderBase.org、SpamCop の公式ルール セットを維持し、シスコ CSI エコシステムに脅威情報を提供する主要なチームです。

SECURITY AND TRUST ORGANIZATION

シスコの Security and Trust Organization は、役員室のメンバーや世界のリーダーの考える最も重要な 2 つの問題に対処するためのシスコの取り組みを明確に示します。組織の基本的な使命には、シスコの公的機関および民間のお客様の保護、シスコの製品とサービス ポートフォリオにおける Cisco Secure Development Lifecycle と Trustworthy System の実現、および絶えず進化するサイバー脅威からのシスコの保護、が含まれています。シスコは、人員、ポリシー、プロセス、およびテクノロジーを含む全体的なアプローチでセキュリティと信頼を広めます。Security and Trust Organization は、InfoSec、信頼性の高いエンジニアリング、データ保護とプライバシー、クラウド セキュリティ、透明性と検証、および高度なセキュリティ調査と管理を中心に優れた運用効率を促進します。詳細は、**http://trust.cisco.com** [英語] を参照してください。

グローバル ガバメント アフェアズ

シスコは、さまざまなレベルで政府組織とかかわり、テクノロジー部門をサポートする公的なポリシーや規則の作成を支援したり、政府機関がその目標を達成できるよう支援します。グローバル ガバメント アフェアズ チームは、テクノロジー推進の公的ポリシーおよび規則を作成したり、これに影響を及ぼします。業界関係者や関連パートナーと協力することで、このチームは、世界、国内、および地域レベルでのポリシー決定の支援に目を向け、シスコのビジネスを左右するポリシーや全体的な ICT の採択に影響力を持つために政府機関のリーダーとの関係を構築します。グローバル ガバメント アフェアズ チームは、シスコが世界中でテクノロジーの使用を促進および保護することができるよう支援する、当選経験のある当局者、議院法学者、取締官、米政府高官、および政府業務の専門家で構成されています。

COGNITIVE THREAT ANALYTICS

シスコのコグニティブ脅威分析は、ネットワーク トラフィック データの統計的分析を使用して、漏洩、保護されたネットワーク内のマルウェアの動作、およびその他のセキュリティ上の脅威を検出するクラウドベースのサービスです。このソリューションは、動作分析と異常検出を使用してマルウェアへの感染や情報漏洩の症状を識別することにより、境界ベースの防御におけるギャップを解消します。高度な統計モデリングと機械学習を活用して、新たな脅威を独立的に特定し、検出内容から学習して、長期的に適応します。

INTELLISHIELD チーム

IntelliShield チームは、脆弱性と脅威の研究、分析、統合、およびシスコ セキュリティ リサーチ アンド オペレーションズ全体と外部ソースからのデータと情報の関連付けを行い、シスコの複数の製品とサービスを支える IntelliShield セキュリティ インテリジェンス サービスを生み出しています。

LANCOPE

シスコの傘下にある Lancope は、今日の脅威から企業を保護するためのネットワークの可視性とセキュリティ インテリジェンスを提供する主要なプロバイダーです。NetFlow、IPFIX、その他のタイプのネットワーク テレメトリを分析することによって、Lancope の StealthWatch® システムはコンテキスト認識型のセキュリティ分析を実現し、APT や DDoS からゼロデイ マルウェアや内部関係者による脅威に至る幅広い範囲の攻撃をすばやく検出します。企業ネットワーク間での継続的な横方向の監視と、ユーザ、デバイス、およびアプリケーションの識別を組み合せることで、Lancope はインシデント対応のスピードアップ、フォレンジック調査の向上、および企業リスクの削減を実現します。

ACTIVE THREAT ANALYTICS チーム

Cisco Active Threat Analytics（ATA）チームは、高度なビッグデータ テクノロジーを活用して、既知の侵入、ゼロデイ攻撃、高度な永続的脅威からの組織の保護を支援しています。この完全なマネージド サービスは、シスコのセキュリティ専門家と、シスコのセキュリティ オペレーション センターのグローバル ネットワークによって提供されます。これは、常時警戒とオンデマンド分析を 24 時間 365 日提供します。

SECURITY RESEARCH AND OPERATIONS（SR&O）

Security Research & Operations（SR&O）は、業界トップクラスの Product Security Incident Response Team（PSIRT）を含め、シスコの全製品およびサービスに対する脅威および脆弱性の管理に責任を負います。SR&O は、Cisco Live や Black Hat などのイベントやシスコおよび業界の仲間との協力などで、進化する脅威の状況を理解できるように顧客を支援します。さらに、SR&O はシスコの Custom Threat Intelligence（CTI）などの新しいサービスを提供します。このサービスでは、既存のセキュリティ インフラストラクチャでは検出または軽減されなかった侵害の指標を識別できます。

ADVANCED SECURITY RESEARCH AND GOVERNMENT（ASRG）

Advanced Security Research and Government（ASRG）は、シスコの長期的なセキュリティ ビジョンに関する方向性とガイダンスを提供します。この目的を達成するために、ASRG は、高度な暗号化とセキュリティ分析などの重要なセキュリティ分野で社内調査を実行します。また、大学の研究者に協力して資金を提供することで、長期的な問題の解決を支援しています。

CISCO SECURITY INCIDENT RESPONSE SERVICES（CSIRS）

Cisco Security Incident Response Services（CSIRS）チームは、シスコのお客様に、インシデントの発生前、発生中、発生後を通して支援を提供する世界レベルのインシデント対応者で構成されています。CSIRS はクラス最高の人材、エンタープライズクラスのセキュリティ ソリューション、最先端の対応技術、攻撃者との長年にわたる戦いで得られたベスト プラクティスを活用し、お客様がより積極的に防御できるようにすると共に、攻撃があればすばやく対応して復旧できるようにします。

グラフィックのダウンロード

このレポートのグラフィックはすべて次のサイトからダウンロードできます。**www.cisco.com/go/mcr2016graphics** [英語]

更新および訂正

このレポートに記載されている情報の更新と訂正については、**www.cisco.com/go/mcr2016errata** [英語] をご覧ください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp