今年の脅威

2019 年の攻撃の手口とツールを振り返る

目次

2019 年の標的と攻撃ツール

一部のサイバー犯罪者は、特定の組織を念頭に置いて攻撃を計画します。誰を標的にすべきか、そしてどれだけの収益が得られるかを把握しているのです。しかも、攻撃を阻むものはほぼ皆無です。今年に世界中で発生した標的型ランサムウェア攻撃がその最たる例です。攻撃者が標的を慎重に選んでいたこともあり、影響は甚大でした。

標的型だけでなく、数で勝負する脅威も存在します。その狙いは、特定の組織や個人ではなく、できるだけ多くの標的を攻撃することです。

たとえば今年出現した DNS ハイジャック攻撃では、特定の DNS エントリが攻撃者によって改ざんされました。DNS の改ざんにより、被害者を悪意のあるシステムへと秘密裏にリダイレクトできるため、マルウェアのインストールや、機密情報あるいはログイン情報の傍受などが可能になったのです。

リモートアクセスのトロイの木馬から、暗号化されたトラフィックに脅威を隠蔽する手口に至るまで、検出を回避するための新たな手口が続々と確認されています。

本レポートでは今年一年の調査結果を振り返り、注目すべき 6 つの脅威を解説します。より詳細な分析は「Threat of the Month」のブログシリーズをご覧ください。ぜひこちらから購読し、2020 年に予想される脅威についての最新情報をお受け取りください。

本レポートの最後には奨励事項が記載されています。セキュリティ対策の役員会議やビジネスプランニングなどでぜひご活用ください。今後必要となるセキュリティ関連のツールとプロセスについて、優れたガイダンスを提供しています。標的型攻撃に対して現在のセキュリティ態勢がどの程度有効で、どこに弱点があるかを特定するためのリソースとしてもご活用いただけます。レポートで解説する 6 つの脅威にどれだけ迅速に対処できるか?脅威をいつ検知できるのか?対応時間を短縮するために何をすべきか?などの疑問にもお答えします。

1. DNS ハイジャック

DNS(ドメインネームシステム)は、人間が読み取れるドメイン名(www.example.com など)を、機械で読み取り可能な IP アドレス(1 ～ 3 桁ごとに区切られた数列、例:208.67.222.222)に変換する、インターネットの中核技術です。DNS を例えるならば、蔵書の検索を助けてくれる図書館司書です。名前を入力すると DNS(司書)が IP アドレスに変換し、対応する IP アドレスを本棚の中で検索し、探している Web サイト(蔵書の場所)を返すのです。

シナリオ

ある朝のこと、普段どおり午前 9 時に出社して社内ネットワークにログインします。毎朝の日課はコーヒーを飲みながら業界ニュースをチェックすることです。ブラウザを起動してブックマークをクリックすると、いつものニュースサイトが開きます。

ただしこれは偽の Web サイトです。

シスコの脅威インテリジェンスグループ Cisco Talos では DNS を厳重に監視してきましたが、今年は DNS ハイジャックに関係した攻撃を複数発見しました。

DNS 攻撃で特異なのは、標的を直接攻撃せず、最初に司書(先の例では、毎朝チェックしている業界ニュースサイト)を攻撃する点です。このため司書に場所を尋ねても、完全に誤った場所に誘導されることになります。ただし最大の問題は、ユーザがそれに気付いていないことです。誘導された棚の本(偽サイト)は、一見すると目的のものです。しかし実際の中身は完全なる別物で、子ども向けの本を装った『アナーキストクックブック』(爆発物、薬物の作成法などについて書かれた本)が置かれていたりします。

DNS 攻撃の目的は、Web サイトへの正当なルートを改ざんして不正サイトに誘導することです。被害者は目的ドメインの IP アドレスを要求しますが、DNS レコードが改ざんされているため、実際には不正サイトの IP アドレスが返されるのです。不正サイトに到着した無知な被害者は、攻撃者にとって格好の餌食になります。

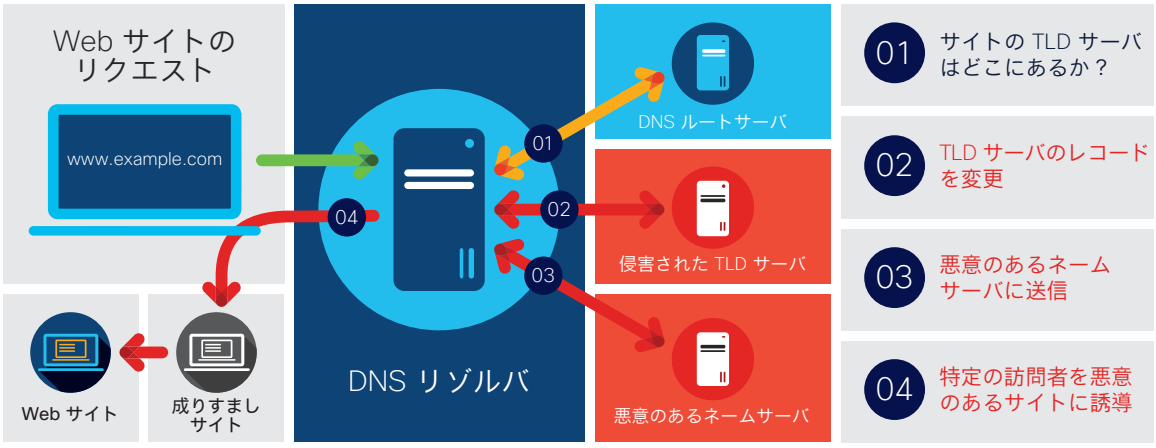
マルウェアがインストールされ、ユーザ名とパスワードが盗まれるかもしれません。正当なサイトとの間に潜み、トラフィックをすべて傍受して他の目的(個人情報の窃取、身代金の要求など)に利用する可能性もあります。

「Sea Turtle」が活動を開始する

「Sea Turtle」は、TLD(トップレベルドメイン)の管理組織に侵入した DNS ハイジャックの一例です。攻撃では複数の脆弱性をエクスプロイトすることにより、ドメイン全体でネームサーバを乗っ取ることに成功しました。

「Sea Turtle」が特異なのは、DNS 要求に対して返される IP アドレスを攻撃者が操作できた点です。侵害したネームサーバの設定によって、特定ドメインに対する要求を正当なサイトと不正なサイトに振り分けられるからです。

図 1　Sea Turtle の攻撃プロセス



実際に「Sea Turtle」攻撃では、Web メールサーバの DNS レコードが改ざんされました。このため、Web メールにログインしているユーザからのトラフィック、つまりログイン情報や会話内容などが攻撃者に傍受されたのです。

DNS ハイジャックは非直接攻撃の一種で、特定の組織ではなくインターネットインフラへの侵入が目的です。

「Sea Turtle」のようなサイバー脅威から守る方法については、本レポートの最後で解説しています。ただし最初に取っておくべき基本対策もいくつかあります。パッシブ DNS データの監視や、ドメインレコード変更の把握による、DNS の不正改ざんの検出などです。

2020 年の予想

2019 年は、「Sea Turtle」の攻撃者が手を緩めることはありませんでした。Cisco Talos が最近入手した情報によれば、Talos が最初の調査結果を公開した後に「Sea Turtle」の攻撃者が再編成され、新しい攻撃インフラの開発を強化しています。大半の攻撃者は発見・公開されると勢いを失うため、「Sea Turtle」の攻撃者はかなり大胆だと言えます。「Sea Turtle」のような脅威に対抗する手段は、DNS セキュリティを特に重視し、ユーザをより厳格に確認できる多要素認証を導入することです。

DNS ハイジャックの詳細はこちらの記事をご覧ください。

出典: https://gblogs.cisco.com/jp/2019/05/talos-seaturtle/

注目すべき点: 標的型ランサムウェア

今年は、注目を集めた標的型ランサムウェア攻撃が世界中で多発しました。ただし新しい種類のランサムウェアがどれほど生まれても、以前からある有効なランサムウェアが消滅することはありません。以下に説明する 3 つの例は、ランサムウェア攻撃によって基幹サービスが停止した場合に、どれだけ大きな影響が出るかを物語っています。

米国のボルチモア市は 5 月に大規模なランサムウェア攻撃を受け、市庁舎で勤務する 7,000 人の職員に影響が及びました。市側は身代金の支払いを拒否し、すべて手作業でシステムとデータの復旧にあたりました。これらの作業に費やされた額は 1,000 万ドルを超えると推定されています。

同じく米国のユタ州レイクシティ市と、フロリダ州リビエラビーチ市も同様のランサムウェア攻撃を受けましたが、身代金の要求に応じて合計 100 万ドル相当のビットコインを支払っています。ただし暗号化されたデータを復号するのは困難な作業であり、現在も終わっていません。

英国警察の法医学検査を請け負う Eurofins Scientific 社は、標的型ランサムウェアによる大規模な攻撃を受けました。同社は毎年 7 万件以上の刑事事件を扱っていますが、代替企業が見つかるまで多くの訴訟が延期されるなどの影響が出ました。

身代金が要求された場合に関する Talos のアドバイスや、標的型ランサムウェアについての詳しい情報は[こちらの記事]をご覧ください。

2. リモートアクセスのトロイの木馬（RAT）

シナリオ

大手のテクノロジー企業に勤務していて、革新的な新製品を間もなく発表する場面を想像してみてください。発表まで新製品のリークを防ぐことが目標ですが、残念ながら情報が漏れるのは時間の問題でしょう。

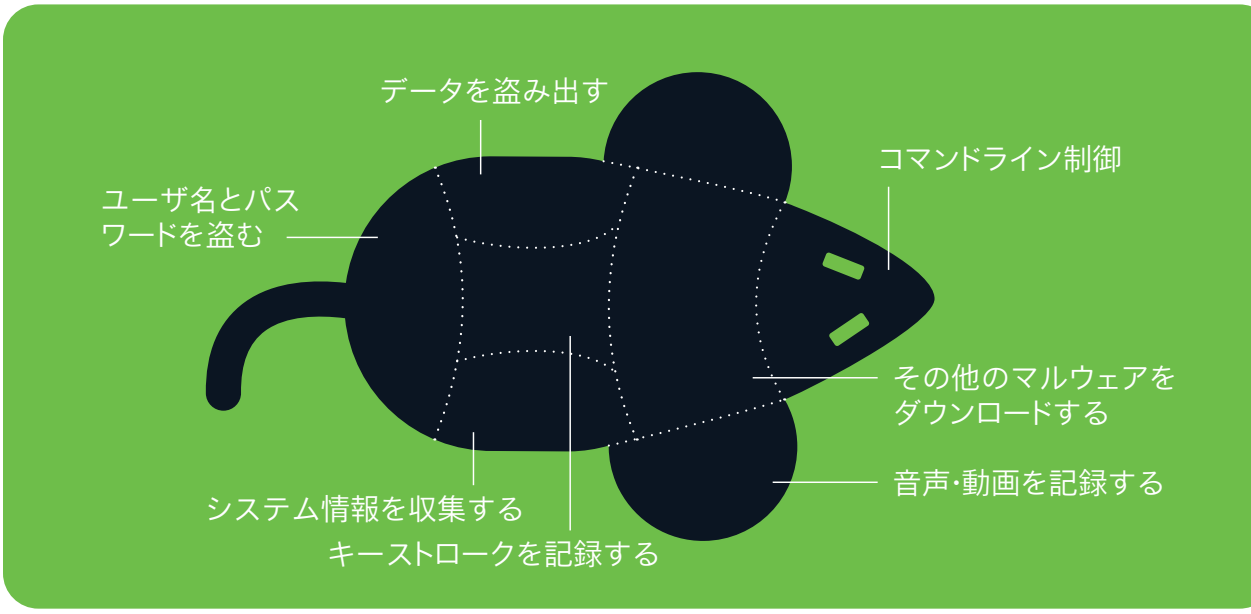
自社のセキュリティが破られ、新製品に関する情報が盗まれたからです。

知的財産の窃取を狙う攻撃者には、ダウンローダ、管理ツール、インフォスティーラーといった多数の武器があります。ただしこのような場面での主流はリモートアクセスのトロイの木馬（通称 RAT）です。

RAT が攻撃で使用される方法

RAT はツールであるため、さまざまな機能を備えています。たとえば財務データを盗むシナリオで RAT を利用すれば、侵入先のシステムから銀行口座の詳細を窃取したり、キーロガーをインストールしてクレジットカード番号を収集したりできます。

図 2　RAT の構成要素



多くの RAT には、キャッシュなどに保存されたパスワードを取得する機能が含まれています。攻撃者がユーザ名とパスワードを入手できれば、共有サーバにログインできます。

重要な点ですが、侵入したシステムでは RAT が攻撃者へのコマンドライン インターフェイスとして機能します。これにより攻撃者は管理者権限を使用して、ファイルの作成や削除、キーロガーのインストールなど、あらゆる操作を意のままに実行できます。

ただし RAT による侵入手口は他のマルウェアと同じです。配布経路も同様で、電子メールやドロッパー、エクスプロイトキットなどが使われています。

2020 年の予想

偶然の一致かもしれませんが、2020 年はねずみ(RAT)年です。最近多用されている RAT の一例は Orcus RAT と RevengeRAT です。たとえば今年の夏に Talos が確認した攻撃者は、幅広いマルウェア配布キャンペーンで RevengeRAT と Orcus RAT を使用していました。標的となっていたのは政府機関や金融機関、IT 企業やコンサルティング会社などです。

攻撃では、以下のような独自の戦術、手法、手順(TTP)が新たに使用されていました。

- 一般に「ファイルレス」マルウェアで使われる永続化手法
- C2 インフラを隠すための難読化手法
- 自動分析プラットフォーム（マルウェアサンドボックスなど）の回避手口

サイバー犯罪者は RAT の用途を広げることに躍起なため、RAT の脅威が来年も続くことは確実です。

3. 暗号化トラフィックに潜む脅威

シナリオ

標的のシステムへ侵入するためなら、攻撃者はあらゆる労力を惜しみません。しかしネットワーク監視ツールによって不正なトラフィックが見つかると、苦労も水の泡となります。そのため多くの攻撃者はトラフィックを暗号化しています。

攻撃の中では、攻撃者が隠したいトラフィックが多く発生します。たとえばコマンドアンドコントロール(C2)サーバとの通信や、収集したデータの外部送信などです。これらのトラフィックは実際にほぼ例外なく暗号化されています。

暗号化された不正なトラフィックを検出する方法

暗号化された不正なトラフィックを検出するひとつの方法は、「トラフィック フィンガープリント」です。トラフィック フィンガープリントでは、ネットワークを通過する暗号化されたパケットを監視し、既知の不正パターン(フィンガープリント)がないか調べます。

ただし、これにより暗号化された不正なトラフィックをすべて検出できるわけではありません。ランダムまたはダミーのパケットをトラフィックに挿入することで、パターンをカモフラージュできるからです。カモフラージュされた不正なトラフィックを検出するには、より複雑な不正接続を特定できる機械学習アルゴリズムなどの高度な検出技術が必要です。ただし機械学習アルゴリズムを導入しても回避される可能性があります。そのため階層型アプローチを実装し、さまざまな手口に対応できる態勢を整えておくことをお勧めします。

2020 年の予想

暗号化された不正なトラフィックの脅威は着実に増加しています。シスコが収集したデータによると、Cisco Stealthwatch によって発見された脅威全体の 63% は、暗号化されたトラフィックの中で発見されました。だからと言って HTTPS(暗号化)の採用が撤回される可能性はありません。つまり組織としては、暗号化されたトラフィックに潜む脅威を過小評価しないことが重要です。こうした点も踏まえて、結論のセクションではネットワーク分析の利点について解説しています。

暗号化トラフィックに潜む脅威について詳しくはこちらの記事をご確認ください。

図 3 バンキング型トロイの木馬は外部に送信するデータを暗号化

4. Office 365 内のフィッシング攻撃

シナリオ

Office 365 アカウントを使って同僚と電子メールで会話をしている最中です。取締役会に提出するレポートについての会話ですが、同僚からレポートの最終版が送られてきます。

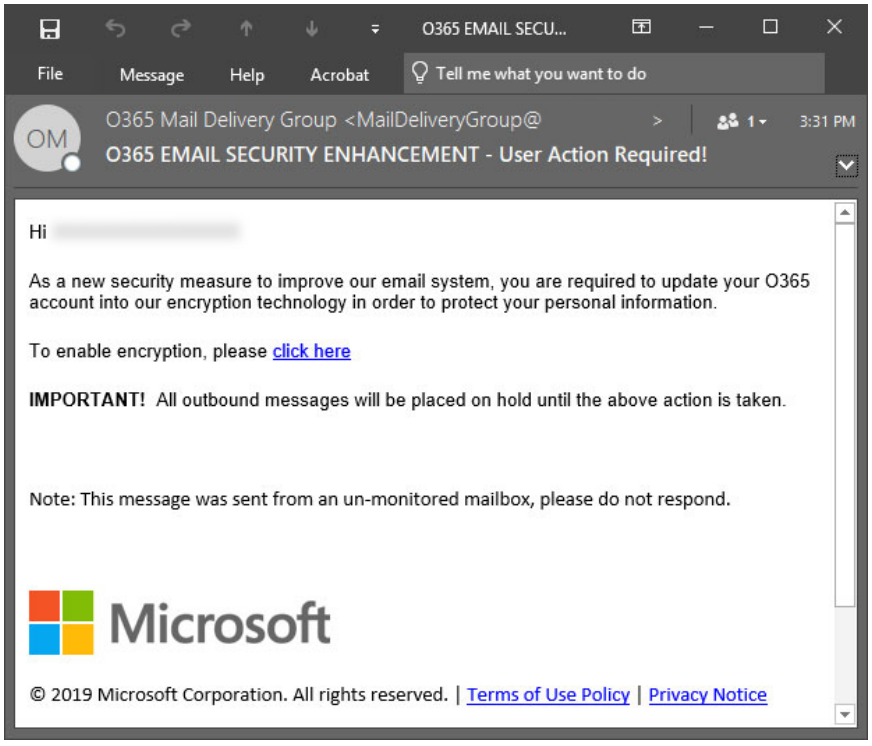
しかし実際の相手は同僚ではなく、レポートも本物ではありません。相手は組織の Office 365 に侵入した攻撃者だったのです。同僚宛てに送った電子メールが、実は攻撃者によって傍受されていました。攻撃者の狙いは会話を操作して情報を引き出すことです。

出来事の一連の流れ

Office 365 アカウントにアクセスするために攻撃者が主に使用する方法は、非常にシンプルです。一般的なフィッシング攻撃では、Microsoft 社からの電子メールだと見せかけます。偽の電子メールは、パスワードをリセットする必要がある、前回のログインから時間が経っている、あるいはアカウントに問題が発生したなどの口実でログインを要求します。ログインして問題を解決するための URL も含まれています。

Office 365 内のフィッシング攻撃では、騙されたユーザが偽のページにログイン情報を入力し、それを攻撃者が盗み取ります。偽のページでは何も起きません。「ログイン情報が正しくない」とのメッセージを表示するか、あるいはユーザを実際の Office 365 のログインページにリダイレクトします。

図 4　Office 365 内で送られたフィッシングメールの例



こうした一連の流れの中でログイン情報が盗まれたことに気付くのは困難です。

攻撃者は多くの場合、上述のように、侵入先の受信トレイにすでにある電子メールに返信する(会話を乗っ取る)ことでペイロードを配信します。

2020 年の予想

シスコの依頼で ESG 社が実施した最近の調査によれば、回答者の 80% 以上がクラウドベースの電子メールサービス(Office 365 など)を組織で利用しています。[1] ただし 43% は、クラウドベースの電子メールに移行した後でさえ、電子メール保護を強化するために追加のセキュリティ対策が欠かせないと述べています。

シスコの『CISO ベンチマーク調査』では、ユーザの行動(電子メールや Web サイトに含まれる不正リンクのクリックなど)に対する懸念が依然として高く、CISO にとって最大の懸念事項であることが指摘されています。しかも、「包括的なオンボーディングと、従業員の転勤 / 退職に対処する適切なプロセスを通じて、セキュリティ分野で従業員をうまく管理できている」と自己評価した回答者は 51% にすぎませんでした。シスコの『2019 年データ漏洩調査レポート』では Verizon 社の調査について取りあげ、あらゆる脅威の中で最も成功率の高いのがフィッシング攻撃であることを指摘してます。実際に、昨年起きたデータ漏えいのほぼ 3 分の 1(32%)はフィッシング攻撃が主な原因でした。

注目すべき点:「Magecart」が活動を再開

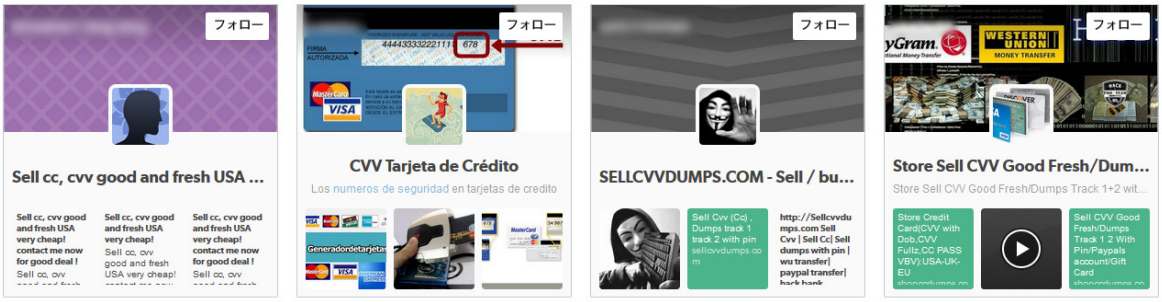
2019 年には、オンライン上のスキミングによってクレジットカード情報を盗む犯罪集団「Magecart」が活動を再開しました。Magecart は、大手の航空券やホテルのオンライン予約サービスが被害を受けるなど、ここ数か月で注目を集めた複数のデータ侵害事件に関わっています。

活動再開で注目すべき点は、Magecart 製のマルウェアが、いくつかのサプライチェーン攻撃で使用されたことです。その例が 1 月に起きたサプライチェーン攻撃です。前述のオンライン予約サイトだけでなく、化粧品や医薬品、衣料品などのオンライン販売サイトが数百件規模で影響を受けたのです。

被害が拡大した要因は Magecart 製のマルウェアです。各サイトで使用されるサードパーティの決済サービスをマルウェアで攻撃することにより、個別に攻撃した場合よりも多くのデータが盗み出されたからです。

1.「Solution Showcase: Cisco Email Security」、Mark Bowker、Adam DeMattia 著、ESG、2018 年 10 月

図 5　商品やサービスを販売する攻撃者の例



5. ソーシャル メディアとブラック マーケット

「サイバー犯罪」と言えば、インターネットの目立たない場所で起きていると考えるかもしれません。複雑なソフトウェアと幾十ものアクセス許可が必要な、高度に暗号化されたネットワークを駆使している･･･と思われがちです。しかし必ずしもそうとは限りません。ソーシャル ネットワークなどの目立つ場所で堂々と行われている場合もあります。

たとえば 2019 年の春に、Talos の研究者は犯罪に関わる多数の Facebook グループを特定しました。それらのグループでは、数十万人のメンバーが攻撃についての投稿を一般公開していたのです。他の攻撃者と連絡を取り、ツールやテクニック、盗んだデータを共有、販売する場と化していました。中には互いに騙し合っているグループも確認されました。さらなる調査と分析により、Facebook グループを通じて共有されているツールの一部は、Talos が過去に監視していたキャンペーンと関連性があることも判明しています。

継続的な問題

サイバー犯罪者がソーシャル ネットワークの不正利用を始めたのは最近のことではありません。中には 8 年も前から存在している Facebook グループさえ見つかりました。Facebook グループが問題視されるのも、今回が初めてではありません。たとえば以前にも、セキュリティ研究者の Brian Krebs 氏が 120 の犯罪関連 Facebook グループと約 30 万のメンバーについて公開しています。これらのグループは削除されたようですが、2019 年に Talos が発見したグループの数から判断する限り、歯止めを掛ける効果は乏しいと言えます。

図 6　ソーシャルメディアとブラックマーケットに関する Talos の調査はこちらの記事をご覧ください。

「不幸中の幸い」とも言えるのは、問題になっている Facebook 上の不正グループがユーザを直接狙ったものではないことです。攻撃者の目的は、ソーシャルメディアを介して情報を共有したり、ツールを売買したり、攻撃のトレーニングを提供したりすることです。

2020 年の予想

「Spam professional(スパムのプロ)」や「Spam and hackers(スパムとハッカー)」などのあからさまキーワードで Facebook を検索してみたところ、本レポートの執筆時点(2019 年末)でも、不正なグループの存在や日常的な投稿を確認できました。Talos では今後も不正グループを見つけ次第 Facebook 社に報告しますが、セキュリティコミュニティ全体として発見し通報する努力も欠かせません。

6 デジタル恐喝

シナリオ

自分のユーザ名とパスワードが件名に含まれる電子メールを受け取ります。それだけでも十分に問題ですが、本当に問題なのは本文です。

自分が過去に訪れたポルノサイトに侵入したと攻撃者が主張しているからです。さらに攻撃者は、デスクトップと Web カメラを乗っ取り、ポルノコンテンツを見ている姿を録画したとも主張しています。

より恐怖心を煽るため、ソーシャルメディアや電子メールから連絡先をすべて収集済みだとも述べています。問題の録画ファイルが連絡先に一斉送信されると生き恥をさらすことになるが、攻撃者にも良心があるため、1,000 ドル相当のビットコインで消去すると伝えています。

偽情報

これは実質的に、はったりを用いた恐喝行為です。

第一に、これらの電子メールの内容はすべて偽情報です。ポルノサイトの侵害も、Web カメラの乗っ取りも、連絡先の流出も、すべて嘘です。人間の心理と罪悪感につけ込んでいるのです。大量送信されるフィッシング攻撃の一種であり、一部の受信者だけでも騙すことが狙いです。電子メールには本物のユーザ名やパスワードが含まれているため、信ぴょう性があります。しかし実際には、以前に漏えいしたデータを基に金銭を得ようとする詐欺手口です。

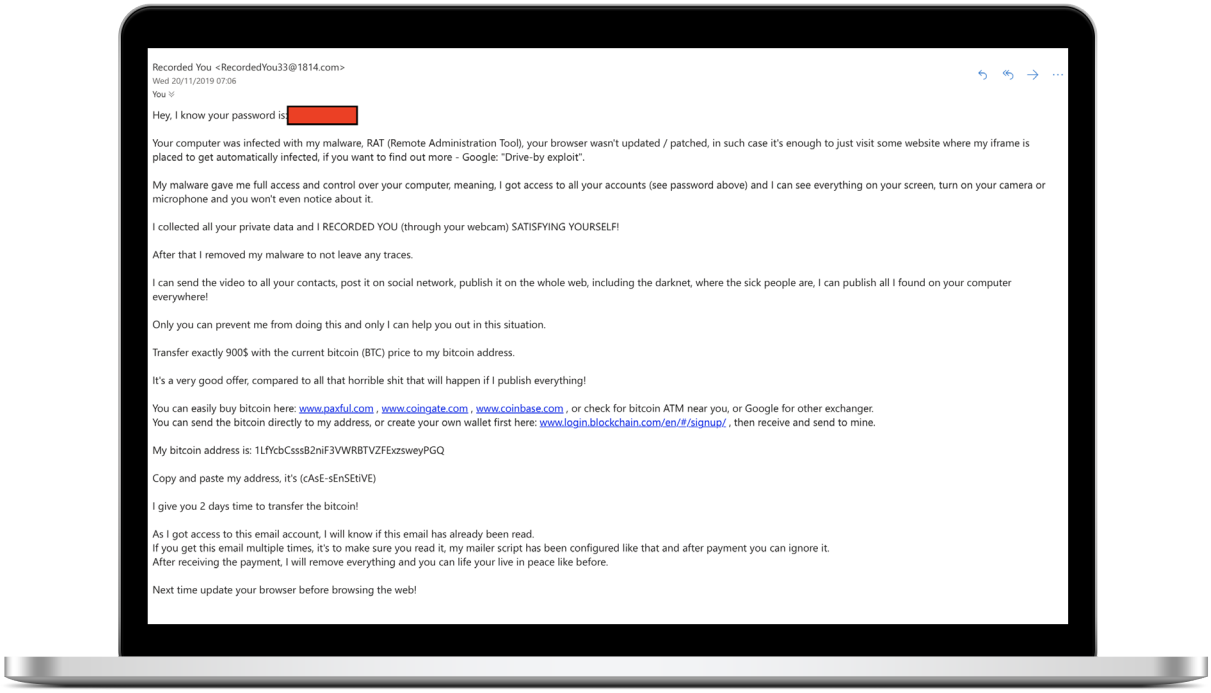
これらの電子メールにはデタラメ情報が満載されています。デスクトップや Web カメラに侵入した可能性がゼロだとは断言できません（実際に起きています）が、攻撃者による説明を読む限り、その可能性は限りなく低いでしょう。

このような電子メールに記載されている個人情報は、以前のデータ漏えい事件で流出したものです。以前と同じパスワードを使っている場合、速やかに変更してください。自身の電子メールアドレスが流出しているかどうかは、Have I Been Pwned のようなサービスで確認できます。

2020 年の予想

少しでも成功すれば大金を儲けられるという性質上、デジタル恐喝は依然として多発しています。図 7 は最近の例です。

図 7　デジタル恐喝メールの最近の例



脅威から守る方法

よく言われることですが、重要なインフラを保護するために設計された多層セキュリティは組織の保護に大いに役立ちます。

最も大切なことは、システムを最新の状態に保ち、定期的に修正プログラムを適用することです。たとえば Sea Turtle(DNS ハイジャック)のケースでは、侵入経路となった脆弱性の一部が 10 年前のものでした。

重要なのは、脅威インテリジェンスを防御戦略のバックボーンとして活用することです。シスコのセキュリティ製品をお使いであれば、あらゆる製品に張り巡らされた Talos の脅威インテリジェンスをすでに活用しています。

以下に、多層防御の一部を担うソリューションと、各ソリューションが対処する主な脅威をご紹介します。

DNS レコードの監視と不正ドメインのブロック

Umbrella Investigate は、インターネットドメイン、IP、およびファイルの関係性と変化を包括的に可視化できる DNS 検査コンソールです。攻撃者のインフラを特定し、将来の脅威を予測し、DNS レコードの変更をすばやく検知できます。多くの脅威にとって、機能するには C2 ドメインへの接続が不可欠です。Cisco Umbrella は DNS を使用して、すべてのポートとプロトコル(直接 IP 接続を含む)に対する脅威を阻止し、悪意のあるサーバへの接続を防ぎます。

防御できる主な脅威：DNS ハイジャック、RAT、標的型ランサムウェア、暗号化されたトラフィックに潜む脅威

強固なエンドポイント保護ソリューションの採用

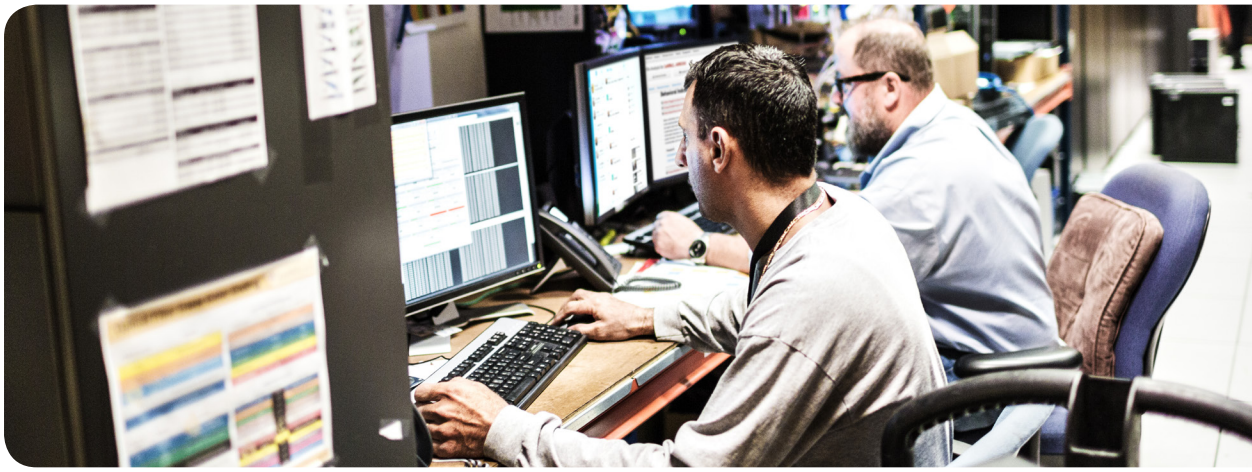
ネットワーク内のデバイスが増えるなか、エンドポイントにおける弱点を理解してプロアクティブにブロックし、脅威が防御網を突破した際には迅速に対応できる重要性が増しています。Cisco AMP for Endpoints は侵入地点でマルウェアをブロックし、高度な脅威を検出して封じ込め、排除します。

防御できる主な脅威：RAT

多要素認証(MFA)の使用

Cisco Duo などの MFA ソリューションは、ユーザ ID を検証し、あらゆるデバイスを可視化します。適応型ポリシーを適用することで、すべてのアプリケーションへのアクセスを保護します。攻撃者がログイン情報を取得できた場合に、システムへの不正ログインを防ぐ効果もあります。

防御できる主な脅威：RAT、標的型ランサムウェア、DNS ハイジャック



ネットワーク トラフィックを監視する

不正なアクティビティに対する監視も欠かせません。Cisco Stealthwatch は、既存のネットワークインフラから得られたエンタープライズテレメトリを活用する、最も包括的なネットワーク トラフィック セキュリティの可視化・分析ソリューションです。暗号化されたトラフィックの中から脅威を検出できる Encrypted Traffic Analytics も備えています。

防御できる主な脅威：RAT、暗号化されたトラフィックに潜む脅威

電子メールセキュリティ

スパム、ウイルス、マルウェア対策などの基本ソリューションは欠かせませんが、より高度なフィッシング保護には電子メールセキュリティが重要です。機械学習により電子メールの送信元や振る舞いを把握して認証し、巧妙なフィッシング攻撃をブロックできます。

防御できる主な脅威：Office 365 内のフィッシング、RAT、デジタル恐喝

悪意のあるファイルの動作を特定

Cisco Threat Grid などのソリューションは、悪意のあるファイルを探し出し、すべてのシスコセキュリティ製品に自動的に通知します。Threat Grid では、高度なサンドボックスと脅威インテリジェンスが 1 つのソリューションとして統合されており、組織をマルウェアから防御します。

防御できる主な脅威：標的型ランサムウェア、RAT

プラットフォーム アプローチの採用

Cisco Threat Response(CTR)などのプラットフォーム アプローチを採用すれば、複数の侵入経路を抱える場合でも、新しい感染、侵害の伝播、データの流出をシステム全体で阻止できます。脅威の検出、調査、排除などの主要なセキュリティ業務を自動化および迅速化します。CTR は、シスコの統合型セキュリティ アーキテクチャの重要な柱です。

防御できる主な脅威：全般

インシデント対応

攻撃に対する準備と対策を強化Talos Incident Response は、シスコが利用しているのと同じ脅威インテリジェンスを直接提供し、侵害への準備と対応、および侵害からの復旧を支援します。シスコの専門チームがお客様と協力して、既存の計画を評価して新しい計画を作成し、迅速な支援を適時に提供します。

シスコ サイバーセキュリティ シリーズについて

シスコは過去 10 年間にわたって、全世界のサイバーセキュリティ専門家を対象に、セキュリティと脅威インテリジェンスに関する多くの信頼できる情報を公開してきました。これらの包括的なレポートでは、脅威の現状や組織への影響を詳しく解説し、データ漏洩などから組織を守るためのベストプラクティスを紹介しています。

シスコのソートリーダーシップに対する新しいアプローチの中で、シスコセキュリティは『シスコ サイバーセキュリティ シリーズ』という旗印を掲げ、一連の調査とそのデータに基づく出版物を発行しています。シリーズの分野は徐々に増え、業界や担当が異なるセキュリティ専門家に向けた幅広いレポートが登場してきました。2019 年に発行された一連のレポートでは、セキュリティ業界の脅威研究者やイノベータに幅広い専門知識を求めたうえで、データ プライバシー ベンチマーク、脅威レポート、CISO ベンチマークなどの分野をカバーしています。今後も年間を通して複数のレポートが登場する予定です。

詳しい情報や過去のレポートは、https://www.cisco.com/c/ja_jp/products/security/security-reports.html 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