今日の重大な脅威から防御する

2019 年 2 月脅威レポート

CISCO

目次

振り返って前進する

脅威の展望について考える場合、時々バックミラーを見て確認することが重要です。

そうすると、運転の場合と同様に、背後にあるものがよく見えるだけでなく、多くの場合、追い越そうとしてどんどん近づいてくるものを特定することができます。

それがこの脅威レポートの目的です。シスコは、過去 1 年ほどの間の 5 つの主要な事例を選びました。それらが大きな事象であったという理由だけでなく、これらの脅威や類似した脅威が近い将来に現れる可能性が非常に高いからです。

たとえば、Emotet および VPNFilter などのモジュール型の脅威を考えてみましょう。これらは、感染しているデバイスや攻撃者の意図した目標に応じて攻撃と脅威をもたらすことができるオンデマンド型のマルウェアです。近年、このようなモジュール型の脅威は数多く観察されており、将来さらに増加するとしても驚くことはありません。

電子メールは依然として攻撃者の常套手段であり、クリプトマイニングから Emotet まで、脅威を拡散するために電子メールが使用されています。また、無許可の MDM プロファイルなど、他の脅威でも高い確率で使用されています。これは、メールボックスに届くものを監視することの重要性を強調しています。

手口

攻撃者の主要な動機はいつでも収益の創出です。マルウェアはお金を追いかけます。たとえば、クリプトマイニングの脅威は、この目標に焦点を絞っています。一方、Emotet は、脅威分散ネットワークに焦点を合わせて、お金を稼ぐためのさまざまな選択肢を利用しています。

データ漏洩も徐々に注目を浴びています。これは、情報を盗むことを企んだ、VPNFilter などの最近の脅威の主要な動機となっています。Emotet は、拡散に利用するためのネットワーク クレデンシャルを盗むだけでなく、情報を盗むための別の一般的なバンキング型トロイの木馬である Trickbot も拡散しています。

これらのレポートでは、5 つの主要な事例を選びました。これらの脅威または類似の脅威が再び現れる可能性があるからです。

最後に、Olympic Destroyer の場合のように、世間を騒がせることだけを目的とした脅威もあります。昨年、このような脅威がいくつか見られましたが、冬季オリンピックを妨害することだけを目的とした攻撃のように、大きく取り上げられたものはありませんでした。

そこで、2018 年の最も影響力のある脅威をいくつか振り返り、これらの脅威が成功した理由に留意することが重要です。現在のところ、脅威の多くはバックミラーに映っているかもしれません。しかしそれらはすでに通過したのでしょうか。それとも貴社や貴社のセキュリティ戦略を通過しようとして加速しているのでしょうか。

脅威の展望について考える場合、時々バックミラーを見て確認することが重要です。そうすると、運転の場合と同様に、背後にあるものがよく見えるだけでなく、多くの場合、追い越そうとしてどんどん近づいてくるものを特定することができます。

攻撃の種類と防御策

セキュリティに対する階層型アプローチが常に推奨されます。各事例の最後には、使用されている（または使用されている疑いのある）主要な脅威ベクトルを示すアイコンと、それぞれのケースでそれらから保護するのに役立つツールが含まれています。以下では、アイコンの意味と、統合セキュリティ アーキテクチャの一部としてさまざまな保護を展開することの利点について説明します。

高度なマルウェア検出および防御テクノロジー（Cisco AMP（高度なマルウェア制御）など）は、未知のファイルを追跡し、既知の悪意のあるファイルをブロックし、エンドポイントおよびネットワーク アプライアンスでのマルウェアの実行を阻止できます。

ネットワーク セキュリティ（シスコの次世代ファイアウォール（NGFW）や次世代侵入防御システム（NGIPS）など）は、インターネットからネットワークへの侵入を試みたり、ネットワーク内の移動を試みたりする悪意のあるファイルを検出できます。ネットワークの可視性およびセキュリティ分析プラットフォーム（Cisco Stealthwatch など）は、マルウェアがペイロードを活性化させている兆候を示す内部のネットワーク異常を検出できます。最後に、セグメンテーションは、ネットワーク内の脅威の水平移動を防止し、攻撃の拡散を封じ込めることができます。

セキュア Web ゲートウェイ（SWG）や**セキュア インターネット ゲートウェイ（SIG）**（Cisco Umbrella など）での Web スキャンは、ユーザがエンタープライズ ネットワークの内外で悪意のあるドメイン、IP、URL に接続するのを阻止します。これにより、マルウェアがネットワークにアクセスするのを間違って許可してしまうことを防いだり、それをうまく通過したマルウェアがコマンド & コントロール（C2）サーバに再び接続するのを阻止したりできます。

E メール セキュリティ テクノロジー（Cisco E メール セキュリティなど）は、オンプレミスまたはクラウドに導入され、攻撃者がそのキャンペーンの一環として送信した悪意のある電子メールを阻止します。これにより、スパムの全体量が減少し、悪意のあるスパムは削除されます。また、電子メールのすべてのコンポーネント（送信者、件名、添付ファイル、埋め込み URL など）がスキャンされて、脅威を含むメッセージが検出されます。電子メールは依然として攻撃者が攻撃を仕掛けるために使用する第一の手段であるため、これらの機能は重要です。

高度なマルウェア検出および防御テクノロジー（Cisco AMP for Endpoints など）は、エンドポイントでのマルウェアの実行を防ぐことができます。また、最も強力な防御策でさえ通過する 1% の攻撃について、感染したエンドポイントを隔離、調査、および修正するのにも役立ちます。

Emotet の方向転換：バンキング型から分散型へ

Emotet は何年もの間、背後に隠れていました。この戦術は功を奏しています。

脅威の展望では多くの場合、何か新しいことや斬新なことをする事例が大きく取り上げられます。大量のデバイスに影響を与える脆弱性が発見されたり、主要な組織に対する攻撃が明るみに出ます。

しかし、**最も一般的な脅威の中には脚光を浴びないものもあります。それらは最新かつ最高の技術ではなく、十分に試行された方法に頼る場合があります。**そしてこれが攻撃者に利用されます。目立たずに作用するものは成長する可能性があり、注目度の高いものは成長しない可能性があります。

Emotet はその見本です。WannaCry や NotPetya などの脅威については取り沙汰されていますが、Emotet は何年もの間、陰に隠れていました。この戦術は功を奏し、今日最も成功している脅威のタイプの 1 つになるまでに成長しました。

Emotet の成功は、それが進化した方法にあります。バンキング型トロイの木馬として「控え目に」に姿を現しましたが、攻撃者はすぐにその脅威をさまざまな種類の攻撃を実行できるモジュラ型プラットフォームにすることに方向転換しました。現在まで話を進めると、かつて競争相手と見られていた他の脅威のタイプは、今ではそれ自身の脅威を広めるために Emotet を使用しています。そして、脅威の展望が再び変化するにつれて、Emotet は他のすべての脅威より目立つようになりました。

控え目な脅威からモジュール型の脅威への移行

Emotet が最初に現れたとき、それはバンキング型トロイの木馬の 1 つでした。この脅威は、通常は請求書または支払いを主題としたスパム メールを使用して、スパム キャンペーンを通じて配信されました。多くの場合、マクロ対応の Office ドキュメント、JavaScript ファイル、または悪意のあるリンクとして含まれていました。配信手法は多岐にわたりましたが、キャンペーンの多くは、特定の地域、特にヨーロッパのドイツ語圏の国々とアメリカの銀行を対象としていました。

当初、この脅威の主な目標は銀行の情報を盗むでした。たとえば、ユーザ名、パスワード、メール アドレス、およびその他の金融情報です。時間が経つにつれ、Emotet は一般市民に拡散し始めました。この脅威の新しいバージョンは、さまざまな機能に対応するさまざまなツールを含む、今日見られるモジュール型構成の基礎を築きました。電子メール ログイン情

電子メール：最も一般的な脅威媒体

今日の主要な脅威のほとんどに含まれていると思われる 1 つのテーマは、電子メールです。それは依然として脅威の攻撃者がマルウェアを拡散するための最も一般的な感染経路であり、近い将来もそのようにして存続すると考えられます。

たとえば、Emotet を見てみましょう。毎週、この脅威の背後にある攻撃者は、新しいフィッシング キャンペーンを作り出しています。

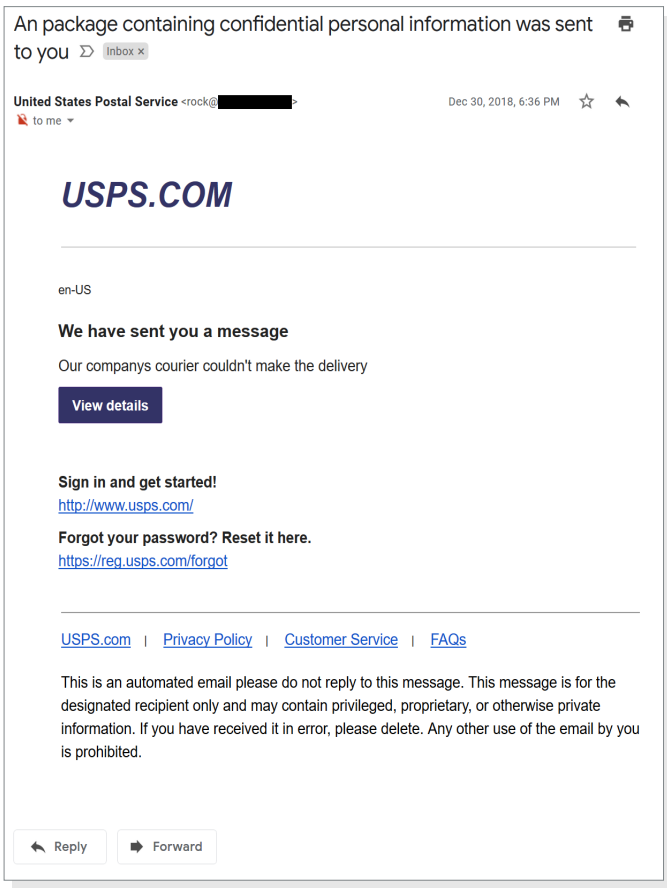
同じことは悪意のあるクリプトマイニングにも当てはまります。この場合、スパム キャンペーンが常にユーザを欺いて、マイナーを自分のコンピュータにダウンロードさせています。

また、モバイル デバイス管理（MDM）の脅威に関しては、攻撃はソーシャル エンジニアリングの電子メールを介して始まったと考えられています。

（続く）

報を盗むモジュールや、ブラウザに保管されているユーザ名とパスワードを標的としたモジュールがあります。DDoS（分散型サービス攻撃）機能を備えたものや、ランサムウェアを配布するものもあります。

図 1　Emotet からのスパム メールのサンプル



特に携帯電話に表示される多くのフィッシング メールの説得力のあるデザインを考えれば、それも驚くことではありません。そして、忙しいユーザにとっては、電子メールによって伝達される危険と緊急性が、受信者に即座に行動を起こさせ、待ち受けている脅威の明らかな兆候を見逃してしまう可能性があります。

攻撃者がマルウェアを拡散するために電子メールを使用し続けるのも不思議ではありません。

実際に得られた金額

Emotet の主な目的は、侵入先のコンピュータを収益化する方法を発見することです。そこでモジュールの出番です。まるで、特定のデバイスにインストールされるモジュールは、感染したデバイスを最大限に収益化する方法によって決まるかのようです。以下のシナリオについて考えてみましょう。

- コンピュータのブラウザの履歴から、銀行の Web サイトに頻繁にアクセスしていることがわかりますか？そうであれば、ログイン情報を盗んでお金を送金するための銀行モジュールを導入します。
- デバイスは、標的に可処分所得があることを示すほどの最高級のラップトップですか？そうであれば、マルウェア配布モジュールを導入して、ランサムウェアまたはクリプトマイニング ソフトウェアをインストールします。
- マシンは高帯域幅ネットワーク上にあるサーバですか？そうであれば、電子メールおよびネットワーク配布用のモジュールをインストールして、Emotet をさらに拡散します。

盗人にも仁義あり

今日の脅威の展望において Emotet が他の多くの脅威と本当に異なるのは、その到達範囲とモジュール方式だけではなく、その脅威の背後にいる攻撃者が他の攻撃グループの配布経路としてそれを物色しているように思われることです。

たとえば、シスコでは、Trickbot をペイロードとしてシステムに投下するだけの目的で、Emotet がコンピュータを感染させる状況を観察しました。この一見矛盾するケースでは、バンキング型トロイの木馬としてよく知られている Emotet は、独自の情報を盗むモジュールを利用するのではなく、実際には別のバンキング型トロイの木馬を投下しています。さらに興味深いことに、Trickbot は Emotet によって投下された後、Ryuk ランサムウェアを投下することがあります。

これは奇妙に思えるかもしれませんが、グループ間の協力は、単に互いに手を結ぶことが最大の収益をもたらすという事実から行われていると考えられます。Emotet がデバイスを利用してそれ以上拡散することができない場合、Trickbot が銀行レコードを盗むことができます。銀行レコードが見つからない場合、Ryuk はデバイスを暗号化し、身代金を要求できます。もちろん、この不自然な同盟がどの程度の期間続くのかは誰にも推測できません。

待ち受ける未来

もちろん、増大する脅威が気付かれずにいることはめったにありません。2018 年の最後の数ヶ月間に、セキュリティ業界は Emotet の規模に強い関心を示し始めました。その注目を集めているのは、電子メール スパムのディストリビュータが、クリプトマイニングのペイロードから Emotet およびリモート アクセスのトロイの木馬（RAT）の拡散に移行したように思われることです。そして、その影響は感じられています。実際に、US-CERT によると、Emotet に感染すると、駆除するのに最大 100 万ドルかかるものもあります。

Emotet の背後にいる攻撃者は、他の攻撃グループのための配布経路としてそれを物色しているようです。

Emotet は衰退する可能性が低く、近い将来の脅威の展望において勢力を振るう可能性があります。そして、過去から将来を予測すると、Emotet の勢いは最終的に低下するでしょう。その結果、脅威の展望では他の支配的なプレーヤーが現れることになります。

このトピックの詳細については、以下を参照してください。

https://gblogs.cisco.com/jp/2019/02/talos-return-of-emotet/

https://www.us-cert.gov/ncas/alerts/TA18-201A

https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

https://gblogs.cisco.com/jp/2019/01/talos-cryptocurrency-future-2018/

IoT の陰謀：VPNFilter のケース

画像：Talos

VPNFilter は今後必然的に現れる脅威の前触れとして存在しています。

過去 10 年間で、Internet of Things（IoT）に関連する多くの注目すべき脅威がありました。DDoS 攻撃を仕掛けるために IP カメラやルータに感染する Mirai ボットネットがありました。また、ベビー モニタ ハックもあります。これは、親が子供部屋に入ると、デバイスに侵入したハッカーが子供たちに話しかけている、というものです。

好むと好まざるとにかかわらず、スマート アシスタントからインターネットに接続された病院のデバイスまで、IoT は個人の家や企業に入り込みました。残念ながら多くの場合、そのプロセスで適切なセキュリティ プラクティスは見過ごされてきました。結果として、そのようなデバイスは悪意のある攻撃者の標的にされています。

しかし、**VPNFilter ほど悪質なものはありません。この脅威は、さまざまな製造元の幅広いルータを標的とし、パッチが適用されていない脆弱性を悪用してそれらを侵害します。**その目的の 1 つは、侵害されているネットワークからセンシティブ データを漏洩させることでしたが、それにはさらに多くのことを可能にするモジュラ システムも含まれていたため、特に懸念されていました。

合計すると、この脅威は 54 ヵ国で少なくとも 50 万台のデバイスに感染しています。幸いにも、シスコの Talos グループの研究者は早い段階でこの脅威に気付きました。感染が増加したとき、その場でそれを阻止する準備ができていました。今日、VPNFilter がもたらす脅威は、公共部門と民間部門の脅威インテリジェンス パートナーの協力と法執行機関のおかげで、大部分はおさまっています。それでも、VPNFilter は今後必然的に現れる脅威の前触れとして存在しています。

脅威が生じるステージ

第 1 ステージ – VPNFilter には、脅威を構成する 3 つの主要コンポーネント、つまり「ステージ」があります。第 1 ステージの主要な目標は、デバイスを永続的に保留にすることです。VPNFilter までは、IoT デバイスを標的にしたマルウェアは、デバイスを再起動するだけで、通常であれば駆除できます。VPNFilter の第 1 ステージのコンポーネントの場合、マルウェアはこのような操作を切り抜けます。また、第 1 ステージには、コマンド & コントロール（C2）サーバに接続するための複数のオプションが含まれており、マルウェアに何をすべきか指示します。

第 2 ステージ – VPNFilter の悪意のある目的を実行するために使用されるコア コンポーネントである第 2 ステージは、ファイル収集、コマンド実行、データ漏洩、およびデバイス管理などの機能を備えています。第 2 ステージのいくつかのバージョンには「キル スイッチ」さえ含まれており、このスイッチがアクティブにされていると、感染したデバイスは永続的に使用できなくなる可能性がありました。

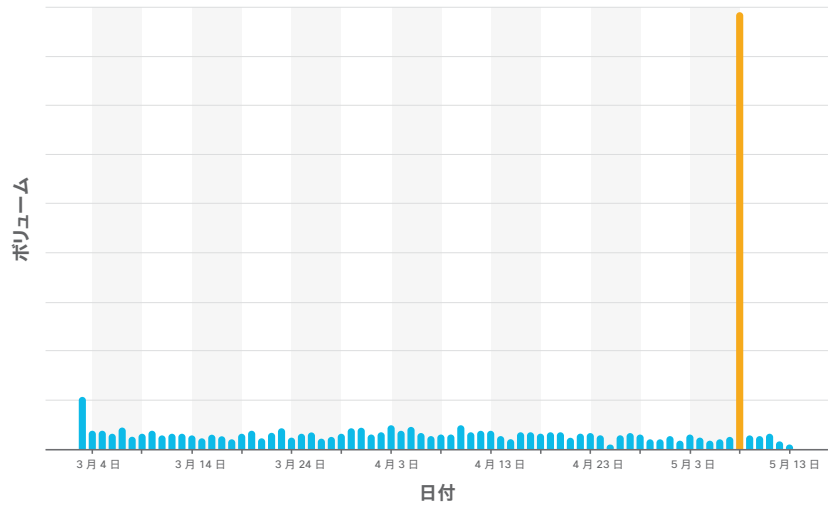
第 3 ステージ – 第 3 ステージは第 2 ステージの機能を拡張し、さらに悪意のある行動を促進するためのプラグインを提供します。注目すべきプラグインの中には以下の機能を含むものがあります。

- ネットワーク トラフィックを監視する
- さまざまな資格情報を盗む
- 特定の業界用 IoT デバイスのトラフィックを監視する
- C2 サーバとの通信を暗号化する
- ネットワークをマッピングする
- エンドポイント システムを不正利用する
- その他のネットワークに拡散する
- DDoS 攻撃を実行する
- 将来の攻撃のソースを隠すために使用できるプロキシ ネットワークを構築する

VPNFilter の（ほぼ）開始

Talos は数ヶ月間 VPNFilter を研究しており、感染率はかなり安定していました。このチームは、マルウェアに含まれる脅威とその機能をさらに理解するために、感染したデバイスを監視およびスキャンしていました。

図 2　日別の新しい VPNFilter 感染



出典: Talos

2018 年 5 月 8 日になると、感染活動が急増しました。それだけでなく、感染の大部分はウクライナを中心としていました。ウクライナでの VPNFilter 感染の 2 回目の急増が 5 月 17 日に起こりました。それは、NotPetya の猛威から約 1 年後のことです。過去にウクライナで破壊的な攻撃があったことを考慮して、Talos は、調査はまだ継続中であるとしても、可能な限り早くこのインフラストラクチャ攻撃に対処することが最善であると感じました。

Talos は、2018 年 9 月に脅威の制圧を宣言できるまで、ボットネットに関する情報の調査と公開を継続しました。

脅威は去ったが、忘れられない

VPNFilter は過去の脅威になるかもしれませんが、残念ながら、IoT デバイスには引き続き脆弱性が発見されています。IoT を標的にした別の脅威が将来出現することは避けられません。

このような脅威から防御することは困難です。一般に、ルータなどの IoT デバイスはインターネットに直接接続されます。それに加えて、多くのユーザはそれらにパッチを適用するための技術的な専門知識を持っていないか、またはそれらを脅威と見なしていないため、状況は非常に危険になっています。

結局のところ、ネットワークの一部としての IoT は成長を遂げていきます。VPNFilter は、将来これらのデバイスを保護するために適切な対策を講じないとどうなるかを示しています。

このトピックの詳細については、以下を参照してください。

https://gblogs.cisco.com/jp/2018/05/talos-vpnfilter/

https://gblogs.cisco.com/jp/2018/06/talos-vpnfilter-update/

https://gblogs.cisco.com/jp/2018/10/talos-vpnfilter-part-3/

https://gblogs.cisco.com/jp/2019/01/talos-year-in-malware-2018-most-prominent/

VPNFilter は過去の脅威になるかもしれませんが、残念ながら、IoT デバイスには引き続き脆弱性が発見されています。IoT を標的にした別の脅威が将来出現することは避けられません。

モバイル デバイス管理：祝福と呪い

Talos は、悪意のある攻撃者が MDM を悪意のある目的に使用する方法を考案したことを発見しました。

モバイル デバイス管理（MDM）機能は、企業に恩恵をもたらしています。これにより、組織はネットワーク上のデバイスを詳細に制御できるようになります。しかし、2018 年に発見されたように、それはまた十分な資金がある悪意のある攻撃者にチャンスを与えるものとなりました。

モバイル マルウェアについて言えば、モバイル オペレーティング システムが難題となる可能性があります。モバイル オペレーティング システムを中心に作成された壁に囲まれた庭は、大部分が悪意のあるアプリから保護されています。

それは、悪意のある攻撃者が携帯電話を攻撃しようとしなかったというわけではありません。公式のアプリ ストアで悪意のあるアプリが発見されていますが、ほとんどの場合、攻撃者はロックが解除されている、または「脱獄」されている、または使用可能であればサードパーティ製のアプリを許可するデバイスを侵害することに限定されていました。

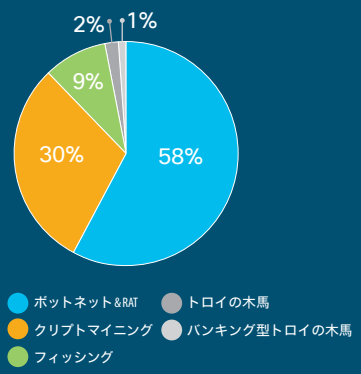
壁に囲まれた庭は安全であると同時に、監獄になる可能性もあります。このレベルの制限とそれが提供するセキュリティの欠点は、公式のアプリ ストアからしかアプリをインストールできないこと、または使用可能であればすべてのサードパーティ製のアプリにデバイスを公開しておくことができるということです。これは、独自のアプリケーションを作成して、従業員にアクセスを許可するだけでなく、そのデバイスのセキュリティを確保する必要がある企業にとっては問題になります。

MDM の導入

このニーズに対応するために、MDM システムが導入されました。これにより、企業は会社の携帯電話を使用し、会社に登録されているプロファイルをインストールし、最終的に任意のアプリをインストールすることができます。MDM は、多くの場合、デバイス設定の制御、不要な Web サイトへのアクセスの防止、または紛失したデバイスの検出など、企業向けの他の機能も提供しています。

セキュリティ インシデントのスナップショット

組織が直面している最も一般的なセキュリティ インシデントは何でしょうか。シスコ コグニティブ インテリジェンス グループのメンバーが試算しました。2018 年 7 月からとられた上位 5 つのカテゴリのスナップショットがあります。

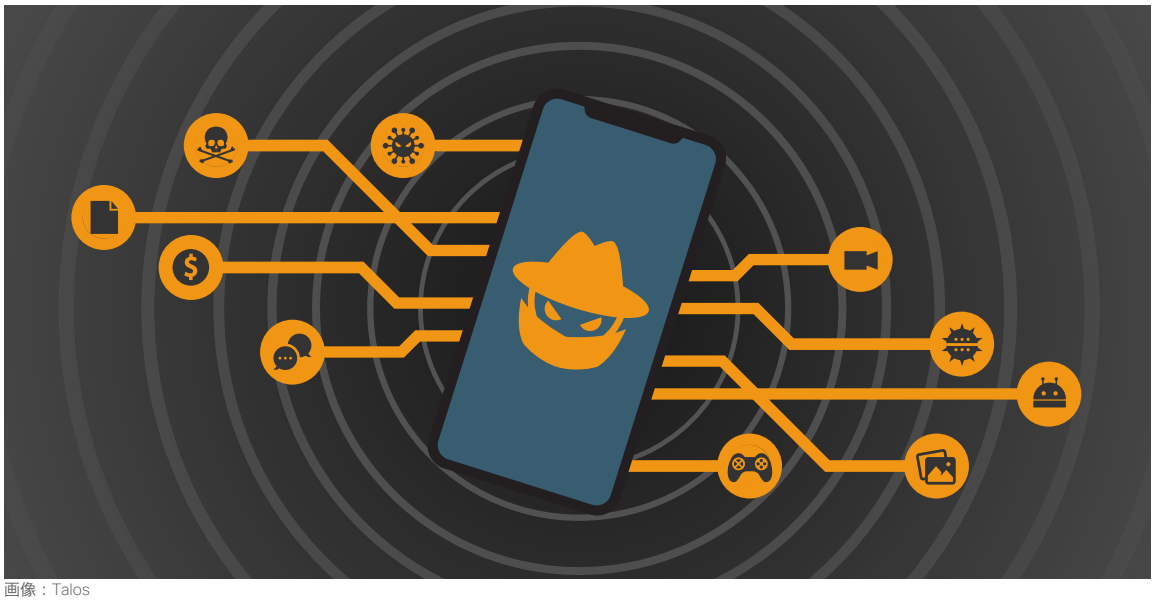


全般的に、ボットネットと RAT がセキュリティ インシデントの大半を占めています。Andromeda や Xtrat などの脅威はこのカテゴリに含まれます。

2 番目に大きい脅威カテゴリは、クリプトマイニングです。これにはとりわけ、無許可の Monero および Coinhive マイナーを明らかにしたインシデントが含まれています。

このスナップショットで最も顕著なのは、バンキング型トロイの木馬が占める割合が小さいことです。Emotet の活動が活発になるにつれて、これは間違いなく変化するでしょう。

シスコでは、将来のレポートでこの指標を再検討して、その変化を確認します。



画像：Talos

MDM が強力なツールであることは間違いありません。そのおかげで、Cisco Talos は、悪意のある攻撃者が MDM を悪意のある目的に使用する方法を考案したことを発見できました。

インドで始まった

Talos の研究者は、オープン ソースの MDM システムを使用して侵害されていたデバイスをインドで発見しました。攻撃者は、デバイスで悪意のあるプロファイルを取得し、データの傍受、SMS メッセージの盗み見、写真や連絡先のダウンロード、デバイスの場所の追跡などを目的としたアプリを排除するのに成功しました。

これらのアプリには、追加機能が付加された（「サイドロードされた」）WhatsApp や Telegram などの一般的なアプリの修正版が含まれていて、攻撃者は侵入先の各機器で会話を監視できます。

これらのデバイスがどのようにしてこの攻撃に犠牲になったのかは依然として謎です。攻撃者がデバイスに物理的にアクセスし、それらを制御するプロファイルをインストールできるようにした可能性があります。ただし、攻撃者がソーシャル エンジニアリングを使用して、ユーザをだましてプロファイルをインストールさせた可能性もあります。

この悪意のあるアラートは電子メールまたはテキスト メッセージで届けられ、悪意のあるプロファイルをインストールする必要があるとユーザに思わせようとした可能性があります。そうだとしても、ユーザはデバイスが完全に侵害される前に、一連の指示に従って、いくつかのプロンプトをクリックする必要があったはずです。

庭を世話する

これは影響力のある重要な攻撃手法であることは間違いありません。幸いなことに、めったに生じません。Talos によって発見された

潜在的な報酬を考えると、将来は、資金が豊富な脅威の攻撃者によって実行されるこれらの攻撃がさらに増加する可能性があります。

攻撃キャンペーンは、この特定の種類のうちで一般に知られている唯一のキャンペーンです。また、悪意のある活動に備えてデバイスを構成するためにユーザが実行する必要がある手順の数を考慮すると、実行するのも困難です。しかし、潜在的な報酬を考えると、Talos は、より多くのモバイル デバイス攻撃が十分な資金のある攻撃者によって実行されているのをすでに目にしています。

皮肉なことに、悪意のある MDM に対する最善の保護は MDM です。

組織は、悪意のあるプロファイルやサードパーティのアプリ ストアからのアプリのインストールを監視および防止できるように、会社のデバイスにプロファイルが展開されていることを確認する必要があります。

また、ユーザに MDM のインストール プロセスを認識させ、これらの攻撃について教育して、悪意のある MDM をインストールしないようにさせることも重要です。

このトピックの詳細については、以下を参照してください。

https://gblogs.cisco.com/jp/2018/07/talos-mobile-malware-campaign-uses-malicious-mdm/

https://gblogs.cisco.com/jp/2018/08/talos-mobile-malware-campaign-uses-malicious-mdm-part2/

ランサムウェアに何が起こったか？

2017 年に戻ると、ランサムウェアが今後長い期間、脅威の状況を支配するように思われていました。SamSam や Bad Rabbit のような脅威が大きく取り上げられました。被害者は暗号通貨の支払いを要求され、そうしなければすべてのデータを失っていました。

1 年以上経つと、状況は確実に変化しました。

ランサムウェアは、主に悪意のあるクリプトマイニングによって主役の座を奪われました。

この急激な変化はなぜ起きたのでしょうか。ランサムウェアの場合、身代金を支払う被害者はごくわずかでした。支払ったとしても、それは 1 回限りのことであって、継続的な収入源にはなりませんでした。

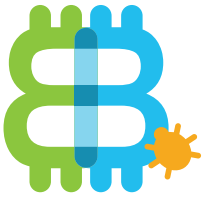
さらに大きなリスクとして、世界中の法執行機関がランサムウェア攻撃の一掃に乗り出しました。ランサムウェアに関連する逮捕が増加したため、攻撃者はよりリスクの低い攻撃タイプに移行しました。

ランサムウェアがなくなったわけではありません。2018 年にこのような脅威がいくつか確認されました。GandCrab は引き続きその存在感を示しており、Ryuk は Emotet と Trickbot の感染を介して拡散されました。ランサムウェアはもはやお山の大将ではありませんが、依然として存在し続けているため、大規模感染を回避するには警戒が必要です。

クリプトマイニング：羊の皮をかぶっていても、狼は狼

金銭を稼ぐ脅威として 2018 年に最も目に付いたものは、間違いなく、悪意のあるクリプトマイニングでした。Cisco Talos の脅威インテリジェンスは、このトピックについて、ここしばらく調査を続けてきました。攻撃者にとって、これはほぼ完全犯罪です。マイナーは多くの場合、ユーザの知らないうちにバックグラウンドで作業して、攻撃者のために収益を挙げながら処理能力を盗みます。

企業がランサムウェアへの対応を強化し、世界中の法執行機関がランサムウェアの攻撃者を厳重に取り締まるようになるにつれて、ますます多くの攻撃側が悪意のあるクリプトマイニング ソフトウェアを普及させるリスクの低い対象に移行しました。



ユーザが自分でインストールするクリプトマイニング ソフトウェアと、悪意のある攻撃者によってインストールされるクリプトマイニング ソフトウェアには、ほとんど違いはありません。

羊の皮を着た狼

ユーザが自分でインストールするクリプトマイニング ソフトウェアと、悪意のある攻撃者によってインストールされるクリプトマイニング ソフトウェアには、ほとんど違いはありません。違いは同意にあります。悪意のあるクリプトマイニング ソフトウェアの場合は、所有者が知らないうちに実行されます。これは、攻撃者にとって大きな魅力になっています。攻撃対象に意識されることなく利益を得ることができるからです。

リスクと報酬のゲームでは、クリプトマイニングは法執行機関に目を付けられる可能性が低くなります。逆に、所有者が知らないまま実行されるソフトウェアがデバイス上にあるというのは、それが何であれ、懸念すべきことです。

そして、悪意があるかどうかにかかわらず、クリプトマイニングは成功の可能性を秘めています。過去数年から 2018 年前半にかけて、暗号通貨の価値が急騰しました。ソフトウェアが絡むあらゆる種類の儲け話の例に漏れず、攻撃者はこれに目をつけました。特に、この急騰は、ランサムウェアが衰退するタイミングと一致していました。そして、ランサムウェアは通常、被害者から一度限りの支払いを受けるのに対し、クリプトマイニングは継続的な収益を生み出します。

悪意のあるクリプトマイニングの危険

防御者の観点から見ると、悪意のあるクリプトマイニングには、懸念すべき理由が数多くあります。コンピュータ上の他のソフトウェアと同様に、クリプトマイニングはシステム全体のパフォーマンスに悪影響を及ぼし、余分な電力を必要とします。1 つのシステムでの増加分は少なくても、それに組織内のエンドポイント数を掛ければ、電力コストの上昇は明らかになります。

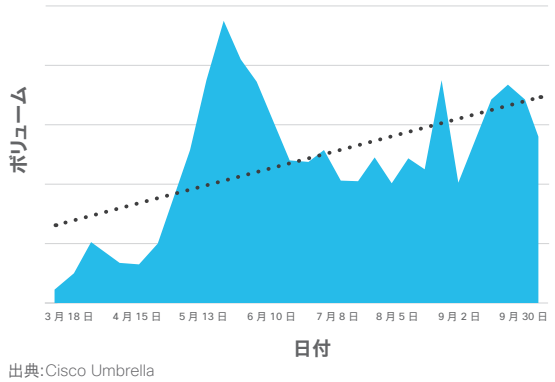
さらに、**クリプトマイニングによる収益獲得に社内ネットワークが使われているとなれば、規制へのコンプライアンス上の問題が生じる可能性もあります。**これは特に財務部門に関して言えることです。このような部門では、責任者が事態を認識しているかどうかにかかわらず、社内リソースを利用した収益獲得に対しては厳格な規則が適用されるためです。

しかし、おそらく最も大きな懸念は、セキュリティ ホールの発覚です。ネットワーク運用担当者が感知しないまま、悪意のあるクリプトマイニングが存在しているということは、ネットワーク設定またはセキュリティ ポリシー全体におけるセキュリティ ホールの存在を意味する可能性があります。そのようなセキュリティ ホールがあれば、他の手段をとる攻撃者からも容易に悪用されかねません。では、ネットワーク上でクリプトマイニングの感染が発見された場合に、悪意ある他の脅威によってその脆弱性が利用され別の行為に悪用される事態を阻止するには、どうすればよいでしょうか。

現状分析

急激な上昇や突発的な落ち込みはありますが、シスコが DNS レイヤで目撃したクリプトマイニング関連のトラフィック全体の中で、クリプトマイニングは時間の経過とともに増加する傾向にあります。

図 3 企業の DNS クリプトマイニング トラフィック量



出典:Cisco Umbrella

興味深いのは、多くの有名な暗号通貨の価値が同じ期間内に減少し、下落傾向になることです。悪意のあるクリプトマイニングでよく利用されている Monero の例を見てみましょう。

図 4 Monero 終値

出典:coinmarketcap.com

悪意のある攻撃者は、展開の容易さと発見された場合のリスクが低いという理由で、悪意のあるクリプトマイニングをプッシュし続けています。実際には、いったんデバイスにインストールされると、それが残っている限り悪意のある攻撃者のお金を稼ぎ続けます。

悪意のあるクリプトマイニングがシステムに侵入する方法

悪意のあるクリプトマイニングが環境に侵入する可能性がある方法はいくつかあります。

- 脆弱性を悪用する
- 悪意のあるファイルが添付された電子メールを送信する
- ボットネットを採用する
- Web ブラウザでクリプトマイニングを利用する
- ブラウザ用プラグインをインストールするアドウェアを利用する
- 内部の悪意のある攻撃者

残念ながら、しばらくの間、悪意のあるクリプトマイニングは普及します。スパムのディストリビュータはクリプトマイニングの脅威を送り続ける可能性があります。

ネットワーク管理者には知られていないクリプトマイニングの存在は、ネットワーク内の他のセキュリティ ホールを指す場合があります。

悪意ある攻撃者にとって、金銭は大きな動機の 1 つであり、おそらくこれからもそうあり続けるでしょう。多くの点で、悪意のあるクリプトマイニングは攻撃者がごくわずかな費用で迅速に利益を上げるための手段と見なすことができます。他の脅威と比較して、ターゲットは自分のデバイスでのクリプトマイニングの影響についてあまり心配していないため、これは特に当てはまります。狼が羊のように着飾って利益が転がり込むのを見る状況としては完璧です。

このトピックの詳細については、以下を参照してください。

https://gblogs.cisco.com/jp/2019/02/cryptomining-a-sheep-or-a-wolf/

https://gblogs.cisco.com/jp/2019/01/talos-cryptocurrency-future-2018/

https://gblogs.cisco.com/jp/2019/01/talos-cryptomining-campaigns-2018/

意識すべき点

このレポートでは、さまざまな脅威を取り上げました。レポートですべての脅威が扱われているわけではありませんが、今後数ヶ月以内に「今月の脅威」ブログ シリーズで以下のトピックが扱われる予定です。今後の内容の一部を示します。

デジタル恐喝。最近のより卑劣なフィッシング キャンペーンの 1 つは、ビットコインの支払いを強要するために受信者の恐怖心を悪用しました。あるキャンペーンでは、ポルノの Web サイトを見ている受信者をカメラで捉えたと主張します。別のキャンペーンには、偽爆弾の脅威があります。最終的に、攻撃者のビットコインの財布がいっぱいになるほど受信者を欺くことを狙って、脅威が巧妙に組み立てられます。

Office 365 のフィッシング。もう 1 つの重要なフィッシング キャンペーンは、Microsoft Office 365 アカウントから資格情報を盗むことを中心としています。攻撃者は、そのために複数の方法を使用しています。シスコは、今後のブログ投稿で、さまざまなキャンペーンとそれを認識する方法について概説します。

「今月の脅威」ブログ シリーズの最新情報を入手するには、必ずメーリング リストに登録して、「今月の脅威」ページにアクセスしてください。

購読：http://cs.co/9002ERAWM

今月の脅威：http://cisco.com/jp/go/threatofthemonth

冬がやって来た：Olympic Destroyer

画像：Talos

オリンピックの攻撃は 1 回限りだったかもしれませんが、その背後にあるグループは休むつもりはありません。

昨年は華々しく始まりました。サイバーセキュリティの専門家は、WannaCry と NotPetya のワンツー パンチの影響を依然として感じていて、今年はもっと静かなスタートを期待していました。韓国の平昌での 2018 年冬季オリンピックの開会式への妨害がマルウェアによって引き起こされたことを Talos が発見したとき、これらの願いはすぐに打ち砕かれました。

このマルウェアは非常に破壊的で、その環境に合わせて作成されていました。その名前は歴史的な出来事に関連している可能性がありますが、Olympic Destroyer による脅威は存続しています。

開会式の間、Wi-Fi は冬季オリンピックのスタジアムやメディアのエリアで機能しなくなり、競技の公式 Web サイトは停止されました。このような大規模な中断は、データ プライバシーのリスク、ブランドの評判の悪化、および顧客満足度の低下など、数々の課題をもたらします。

最終的に、この混乱はサイバー攻撃であることが明らかになりました。さらに長期的な調査により、このマルウェアは 2 つの特徴を示しました。1）それは、（たとえば、ランサムウェアとして実行するのではなく）資産を破壊するように設計されたワイパー型マルウェアでした。2）もっと興味深いことに、それは発生源を隠し、研究者を欺くために巧妙に細工されていました。これは高度なマルウェア技術と不正な戦略を組み合わせた高度な攻撃でした。

どのようにして Olympic Destroyer は破壊するか？

Olympic Destroyer の展開方法は推測の対象となっています。明らかなのは、いったんターゲット ネットワーク内に入ると、そのネットワーク内で移動すること、しかも高速で移動することです。

平昌での攻撃の結果を受けた分析によると、それはワームのように動き、すばやく、きわめて破壊的であったということです。このファイルはパスワードを盗み出し、バックアップ データを消去し、サーバに保管されているデータを標的にして、最短の時間で最大の破壊をもたらします。

Olympic Destroyer は非常に破壊的で、情報を壊す目的で設計されています。

攻撃者は合法的なツールを使用して水平移動しました。この場合のツールは、PsExec（リモート コンピュータでプログラムを実行できるようにする Windows プロトコル）です。オリンピックの開会式と攻撃のタイミングが一致することを考えると、攻撃は遠隔で開始されました。

Olympic Destroyer は、他の脅威の攻撃者に添付されている古いコードを使用して、作成者に妥当な否認権を与えようとした可能性があります。一部のセキュリティ研究者はこれによっても混乱しました。性急に攻撃の原因を特定しようとした研究者もいました。

冬はこれからもやって来る...

実際の動機が何であれ、Cisco Talos は Olympic Destroyer マルウェアの高度な攻撃者の標識を見つけました。これは、Olympic Destroyer はオーダーメイドの攻撃で、その背後にあるグループは休みなく動いています。彼らは、さらなる混乱を引き起こすため、または盗難や他の不正行為を実行するために、この非常に効果的な方法を再び使用する可能性があります。そのため、この種のマルウェアを探すときに警戒する必要があります。

2018 年はこのように始まりました。2019 年には、他の主要なイベントにおいて、悪意のある高度なマルウェアが現れないことを期待しましょう。

このトピックの詳細については、以下を参照してください。

https://gblogs.cisco.com/jp/2018/02/talos-olympic-destroyer/

https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html

https://gblogs.cisco.com/jp/2019/01/talos-year-in-malware-2018-most-prominent/

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 年間にわたり、全世界のサイバーセキュリティの状態に関心を持つセキュリティ プロフェッショナルを対象とした、最も信頼のおけるセキュリティと脅威インテリジェンスに関する多くの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、脅威の状況や組織にとっての脅威の意味を詳しく解説するとともに、データ漏洩がもたらす悪影響から組織を守るためのベスト プラクティスを紹介してきました。

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。シスコはそのタイトル数を増やし、それぞれに関心事の異なるセキュリティ プロフェッショナル向けのさまざまなレポートを提供してきました。セキュリティ業界の脅威研究者やイノベータに幅広い高度な専門知識を求めた 2019 年の一連のレポートには、データ プライバシー ベンチマーク調査、脅威レポート、CISO ベンチマーク調査などがあり、今後もいくつかのレポートが発表される予定です。

詳細については、https://www.cisco.com/c/ja_jp/products/security/security-reports.html を参照してください。

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