CISCO
SECURE

重大な脅威に対する防御

主要なインシデントの傾向分析

CISCO The bridge to possible

サイバー犯罪のパターンを探る

Hazel Burton
（編集責任者）

イーグルスのギタリスト、ジョー・ウォルシュはかつてこう言いました。「人生を送っている中で、偶発的な出来事が次々と起こり、無秩序と混乱の世界にいるように思えるかもしれません。でもいずれ振り返ってみたとき、まるで精緻に組み立てられた小説に見えるのです」

残念ながら、あまりにも多くの重大な脅威に立ち向かっていた（今も立ち向かっている）2021 年のサイバーセキュリティの防御者にとって、そのような明快なイメージを得るのは困難なことです。例を挙げると、Log4j、重要インフラへのランサムウェア攻撃、これまでにない数の脆弱性の報告、勢いを増すサプライチェーン攻撃、Emotet の復活などがありました。組織は日常的に出会うリスクに先手を打ちながら、これらのリスクにも対応しなければなりません。

2021 年の主要な脅威の傾向を分析し、防御者に「精緻に組み立てられた小説」のような明快さを得ていただくために、私は Cisco Secure の各部門から専門家である脅威ハンターとアナリスト 6 名と対談しました。参加者には過去 12 ヵ月に経験した何らかの具体的なサイバーセキュリティの脅威やインシデントについて得られた知見の共有を依頼しました。各専門家は、攻撃者が今何を試みようとしているのかがよく分かる事例を選んで説明してくれました。

新しい内容を追加するために、このコンテンツは 2022 年 1 月に作成されています。ウクライナ情勢については記載していませんが、最新情報については、順次更新されている Talos の脅威アドバイザリブログをご覧ください。

このレポートでは、今後 1 年間に起こることの予測と先触れについても詳しく触れています。混沌とした 2021 年が続いた後、私は今後をどのように見通せばよいのか確証が持てませんでした。しかし、Cisco Talos の脅威インテリジェンスと脅威防御担当ディレクタ Matt Olney は対談の中で、次のような視点を指摘しました。

「大まかに言って、過去 5 年間、防御者としての私たちのアプローチを根本的に変えるようなことは何も起きていません。毎年、どこからともなく恐ろしい脆弱性が平均 1 つか 2 つ発生しています。そして、脆弱性をエクスプロイトする攻撃者と、脆弱性を理解し攻撃から守ろうとする防御者との間でせめぎあいになります」

「サプライチェーン攻撃とランサムウェアは言うまでもなく大きな懸念事項です。各国政府がこの脅威に対する対応策を拡大しているのはこれが理由です」

レポートで取り上げている専門家の分析を読むと、シスコのセキュリティ担当者が担っている重要な役割が見えてきます。また、攻撃者の過去の行動を綿密に調査することで、シスコがセキュリティ企業としての能力を築き上げてきたことがお分かりいただけます。

このレポートでは、サイバー犯罪のパターン特定に取り組む専門家からのアドバイスを基に、重大な脅威に対処する優れた方法についてご紹介します。

目次

© 2022 Cisco and/or its affiliates. All rights reserved.

Colonial Pipeline 社：

ランサムウェアへの対応を言葉だけで終わらせない

Matt Olney
（Cisco Talos 脅威インテリジェンスと脅威防御担当ディレクタ）との対談

2021 年には話題にできる脅威が他にもあったと思いますが、なぜ Colonial Pipeline 社を選択したのですか。

Colonial Pipeline 社の件については興味深い点が 2 つあります。1 つ目は、実社会に与えた影響と、米国東海岸のガソリン供給が直面した事態です。この攻撃は政治的圧力を招き、事件後ランサムウェア活動に対する米国政府の対応が迅速化されました。

2 つ目は攻撃者からの反応です。それはまさに、「太陽に近づきすぎたイカロス」的状況でした。攻撃者たちは、重要なインフラストラクチャを攻撃したために一線を越えてしまったことを知ったのです。そして攻撃者の側から来た反応は迅速で深い意味のあるものでした。

Colonial Pipeline 社への攻撃の後、状況は確かに変化しました。その状況は今も続いています。

Colonial Pipeline 社 事実と数字

- 米国東海岸に供給される石油全量のうち Colonial 社の石油が占める割合は 45%
- パイプラインの長さは約 47,000 キロメートル (29,000 マイル)
- 身代金は 75 ビットコイン (約 440 万ドル)
- ワシントン D.C. で燃料の在庫切れを起こした給油所の割合は 87%

ランサムウェアの攻撃はいつ始まり、初動対応はどのようなものだったのでしょうか。

誤解のないように言うと、シスコは Colonial Pipeline 社の対応には関与していません。ここで申し上げる情報はすべて公開されたレポートからのものです。

5 月上旬のある金曜日の早朝、以前から感染していた Colonial Pipeline 社のネットワークが暗号化され、IT ネットワーク全体が実質的に使えなくなりました。

重要なインフラストラクチャ環境は、通常、IT (情報テクノロジー) と OT (運用テクノロジー) に分離されています。操業に関わる情報があるのは後者の方です。パイプラインの駆動、給油、あらゆる監視は OT の中で行われます。

報告によると、Colonial Pipeline 社の OT 環境は影響を受けていませんでした。暗号化の影響を受けたのは IT 環境でした。Colonial 社はすぐに 75 ビットコインの身代金を支払いました。当時のレートで約 440 万ドルに相当します。

しかし、攻撃者から提供された復号用のツールでは非常に時間がかかり、従来の方法でデータを回復する方が早いことが分かりました。身代金を払う価値はなかったと考えたのではないかと思います。

報告によれば、Colonial Pipeline 社はガソリンの供給を追跡できず、料金も請求できなかったため (その機能は企業の IT 環境にあったため)、給油を停止したとのことです。OT ネットワークが稼働していて利用可能であったにもかかわらず、このような結果になりました。

誤解がないように言うと、Colonial 社側では、OT ネットワークの安全性を確保することについても懸念がありました。Colonial 社は、暗号化が発生してから 1 時間以内にパイプラインの操業を停止しています。その後、6 日間連続して東海岸にまったくガソリンを供給しませんでした。

これがどれほど深刻かというと、東海岸における燃料の 45% は Colonial 社が供給しているのです。同社が供給しているのは自動車用のガソリンだけではありません。天然ガスや航空燃料も供給しています。

一般大衆の立場での対応と言えば、大部分がパニック買いでした。給油所のガソリンがなくなり始めるにつれて買いだめが始まり、これがさらに事態を悪化させました。また、規格外の容器にガソリンを詰めようとする不幸な出来事もありました。政府は、ポリ袋にガソリンを入れないように求める通達を出しています。

再稼働した翌水曜日以降も、東海岸には空のままの給油所がまだ 10,000 ヵ所以上ありました。

バイデン政権に対しては、ガソリンの供給に向けて対策を講じるよう求める政治的圧力が強まりました。この状況があまりにも長く続くと (さらに 3 日から 4 日かかると)、より広範な経済的影響が出始めていたと思われます。公共交通機関などが深刻な影響を受け、通勤に支障が出た可能性があります。

長期的な影響についてきわめて現実的な懸念が生じていました。

© 2022 Cisco and/or its affiliates. All rights reserved.

この攻撃の犯人について分かっていることは何ですか。

ここで興味深い点がいくつかあります。

すぐに、アンダーグラウンド フォーラムとダーク Web が騒がしくなりました。「過ちを犯したようだ」という主旨のコメントがありました。

その後、さまざまなランサムウェアグループが声明を発表し、Colonial Pipeline 攻撃との関連を否定しました。「当グループは重要なインフラストラクチャや病院を攻撃しない」という公式な方針を公表したグループさえあります。

また、さまざまなアンダーグラウンド フォーラムが、ランサムウェアサービスを宣伝してはならないとするルールを確立させたことも確認しました。ランサムウェアに関与したことで法執行機関に注目されることを回避したいからです。

それ以来、この状況は何ヵ月も続いています。犯罪者たちは、この出来事によって各国が考え方を変えたことを知り、政府がランサムウェアを使う攻撃者をどのように扱い始めようとしているかを理解しました。

私は、Ransomware Task Force（ランサムウェア対策タスクフォース、RTF）に加わっています。このタスクフォースは、ランサムウェア攻撃に対する包括的な対応策を国際政府機関と民間部門のパートナーに提言することを目的としています。Colonial 社への攻撃が発生する 2 週間ほど前に、調査結果を発表しました。そこでのアドバイスの 1 つは、各国はランサムウェアを国家安全保障の問題として扱うべきだということです。

その一環として、バイデン政権は矢継ぎ早にいくつかの大統領令を出しました。また、アメリカサイバー軍の活動も活発化し、FBI はランサムウェア資金の一部を回収しています。

FBI はビットコインの 80% を取り返していますが、残念ながら回収した時にはビットコインは値崩れを起こしていました。最終的には 220 万ドルの価値しかありませんでした。

あなたは、攻撃直後の記事の中で、「ランサムウェアへの対応を言葉だけで終わらせる時代は終わった」という言葉を引用しました。その主旨は何でしょうか。

その当時までは、政府の対応の多くは情報共有、つまりメッセージの発信でした。政府は従来の法執行のやり方に頼ってランサムウェアグループを追跡していたものです。

残念ながら、これが実行可能なアプローチではないことは、しばらく前から明らかでした。ランサムウェアは壊滅的な影響を引き起こす可能性があるにもかかわらず、逮捕の実績は驚くほど貧弱です。

「ランサムウェアの脅威を危機的水準に引き上げている攻撃者がいる限り、ランサムウェアを国家安全保障上の脅威として扱う必要があります」

つまり、政府に全面的な対応を促す必要があるということです。国務省が必要です。財務省が必要です。サイバー軍が必要です。司法省が必要です。海外でも同様の組織が必要です。これは世界的な問題だからです。

これは、もはや公報や通知で終わらせられる状況ではありません。ときたま法執行機関が調査して東ヨーロッパのどこかで行き詰っている場合ではないのです。

7 月には、Kaseya 社に対して REvil グループがランサムウェアによるサプライチェーン攻撃を実行したことが新たに確認されました。今年の経験を踏まえると、2022 年にはランサムウェアとサプライチェーン攻撃の本質はどのようなものになるでしょうか。

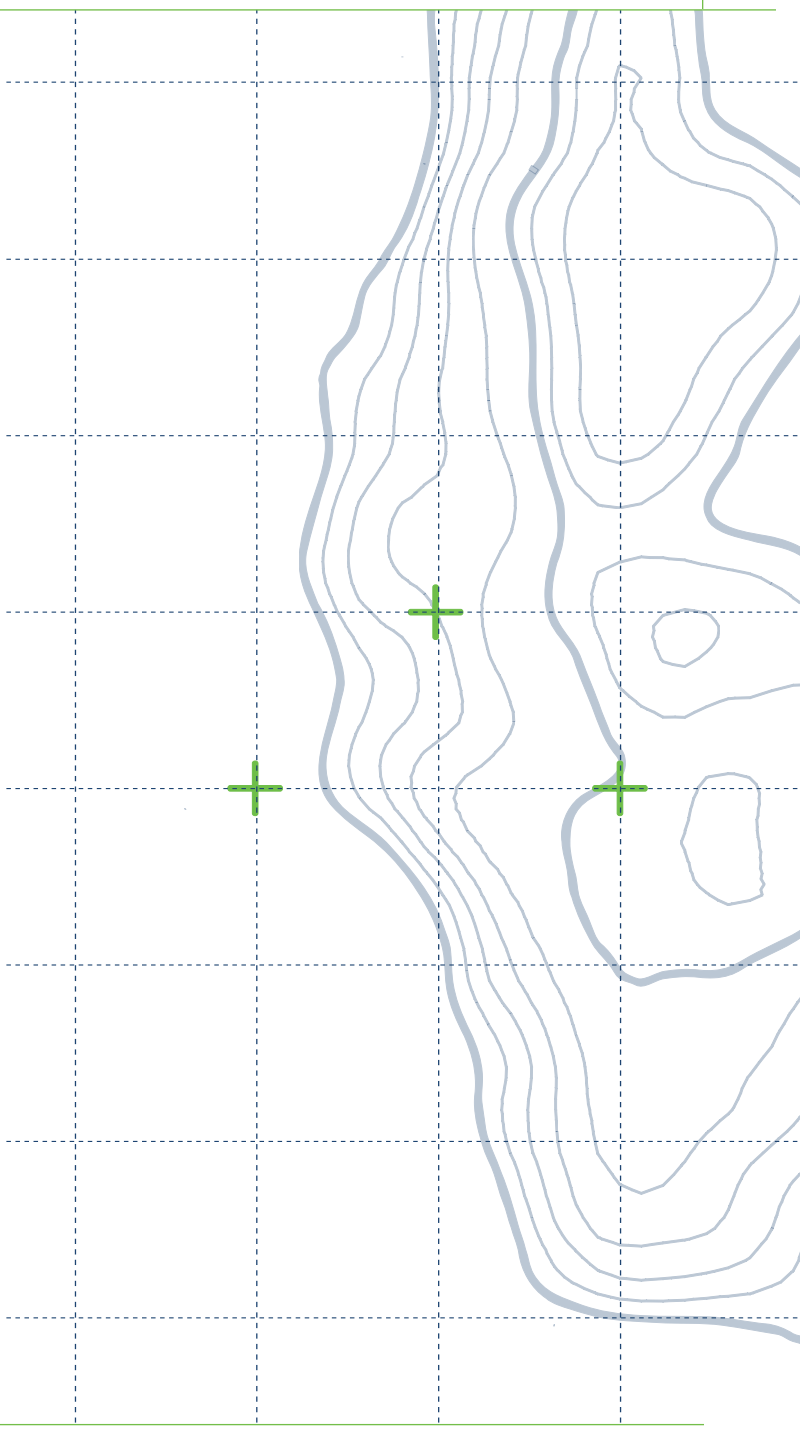
ランサムウェアに関して言うと、私たちはサプライチェーン攻撃がもたらす広範な影響を常に懸念しています。2017 年、サプライチェーンを介してランサムウェアもどきの攻撃が行われると何が起こるか、NotPetya の事例から明らかになりました。この攻撃で世界が被った被害は 100 億ドルを超えています。誤解のないように言うと、これは純粋に破壊を目的とした国家支援の攻撃であり、ランサムウェアではありませんでした。意図的にランサムウェアに見せかけていただけなのです。

「現時点ではサプライチェーンがセキュリティで最も難しい問題になっています。これほど頭が混乱するものは他にないでしょう」

Kaseya 社の件で言うと、同社は中規模企業を顧客として、ネットワークとシステムの管理サービスを提供しています。攻撃者が必要としていたのは、まさにこれです。この件が明確に示しているのは、脅威が新しいレベルに達したことです。

このレベルの脅威が一般化していると言うつもりはありません。攻撃者は複数の企業を同時に攻撃しますが、企業の環境ごとに異なる復号キーのセットを用意する必要があります。そのため、攻撃をやり遂げるのは困難です。ある会社が支払いをして鍵を入手しても、その鍵を使ってすべての暗号化を解除することができないようにする必要があります。

これが、この種の攻撃がまだ一般的になっていない理由の 1 つだと思います。それに、攻撃者は現在行っている個別攻撃の方法で多くのお金を稼いでいます。



ランサムウェア攻撃から組織を保護しようとしている防御者に向けて何かアドバイスはありますか。

過去に、「このパッチを適用してください」とか「二要素認証がインストールされていることを確認してください」といったことを述べたことがあります。それは今でも重要ですが、新しいアドバイスとして主に伝えたいことは、「注意を払う」ことです。

Cisco Talos インシデント対応チームと連携し、攻撃者がどのようにランサムウェアを持ち込むか観察していますが、彼らの活動に関してはあまり進化していません。「これは新しい」と思えるランサムウェア攻撃が発生することはめったにありません。

「脅威の状況に細心の注意を払い、資本と時間をランサムウェア攻撃者が使用する手段（つまり、盗まれたログイン情報や特定の脆弱性）をブロックするために適切に用いていれば、攻撃者に先んじることは非常にたやすくなります」

ほとんどの場合、攻撃者は攻撃相手を選びません。彼らはただ、金を稼ぎ続けたいだけです。守りを固めていれば手を出されることはまずありません。攻撃者はもっと簡単な獲物を狙うはずです。

さらに深く知るために：

重要なインフラストラクチャにおけるセキュリティの新しい状況について詳しく知りたい方は、Colonial Pipeline 社への攻撃に関する Talos の記事をご覧ください。

© 2022 Cisco and/or its affiliates. All rights reserved.

セキュリティ負債：

増加している「臨機目標」

Dave Lewis
(Cisco Secure アドバイザリ CISO)
との対談

セキュリティ負債とは何でしょうか。なぜその重要度が増しているのでしょうか。

セキュリティ負債は私が 20 年ほど前に使い始めた用語です。さまざまな電力会社に勤務した経験から生まれました。私がいた多くの環境で、減価償却が終わったシステムや適切に保守されていないシステムが使われていることに気付いていました。その結果、攻撃者にとっては、多くの臨機目標がありました。

私はこれを、時間の経過や怠慢、もしくは環境に導入された別のシステムとの相互作用の結果、セキュリティの問題として顕在化した技術的負債と見なしています。

セキュリティ負債が顕在化する要因

- プロジェクトの納期を守るためにリスクを受容する
- 予算を巡る争いが継続している
- システムがファイアウォールの背後にあるためにパッチが適用されない

セキュリティ負債がどのようなものか、これまでのキャリアの中で出会った例で説明していただけませんか。

ご紹介できる例は実にいろいろあります。しかし、非常に単純な例を 1 つ挙げるとすると、私がテクノロジー企業で働いていたときに出会ったものがあります。断っておきますがシスコではありません。最初の 1 週間に、組織内のすべてのユーザー名とパスワードを調査しました。

「スーパーユーザーのステータス」のユーザーアカウント 10 個について、持ち主が組織に所属していないことが判明しました。ほとんどの人が離職していました。死亡した不幸なケースも過去 5 年間に 1 件ありました。それにもかかわらず、この人たちのアカウントが過去 2 年間使用され続けていたのです。

幸いなことに、悪意を持って使われたアカウントはありませんでした。しかし、セキュリティプログラムを運に任せるわけにはいきません。環境内で起こっていることの可視化が非常に重要です。

攻撃者の観点から見ると、組織内にあるセキュリティ負債はどのようにエクスプロイトできるでしょうか。

多くの組織で、簡単に悪用されかねません。たとえば、スタッフが不足しているとか信頼できるサードパーティがいないといった理由で、パッチが適用されていない脆弱性があるかもしれません。

検討の対象から漏れるものもあります。廃止期限が計画に織り込まれないまま展開されるプロジェクトがあります。結果として、耐用年数を過ぎて何年も使い続けられ、環境にセキュリティの脆弱性をもたらすという不幸な結果になります。

攻撃者は、さまざまな角度からそれを見ることができます。Shodan といったスキャンツールを使うこともできますし、オープンソースの情報を収集することも可能です。たとえば、LinkedIn にアクセスすれば、他人が履歴書に何を記入しているか、つまり、ある製品を使っていたかを確認することができます。

次に、その環境で使用されていたと思われる製品を絞り込み、公開されている脆弱性や、ダーク Web で見つけられる脆弱性と対比できます。

© 2022 Cisco and/or its affiliates. All rights reserved.

セキュリティ負債を抱えていて対策を講じたい組織へのアドバイスは何でしょうか。

3 つあります。まず、下調べが必要です。環境内にある資産、環境内にいる人物、利用されているアプリケーションとハードウェアを明らかにします。これらを一覧表にしてすぐに利用できるようにします。

次に、問題が特定されたときに追跡が可能になるように、リスクの登録簿を用意します。これは追跡目的だけでなく、監査人の訪問を受けたときにも使用できます。リスクの登録簿を用いれば、監査人に問題を特定していたことを説明し、問題を解決するために用意しているロードマップの概要を示すことができます。

最後に、最も重要なカギは、反復可能なプロセスを定義することです。私がかつて働いていた組織では、何か問題が発生すると、全員が大騒ぎをして役割分担を決めようとしていたものです。

「連絡網を用意して、問題が発生したときに連絡しなければならない人物を特定したうえで、だれがどの仕事を担当するか明確にしてください」

重要なのは、個人名で指定しないことです。役割で指定すれば、組織で異動が発生したときの問題を解決することができます。役割が特定されていることは、実際に何か問題が発生したとき、それを解決するための道筋があることを意味します。

セキュリティ負債によって他のリスク要因はどのような影響を受けますか。

セキュリティ負債は、物理的な観点だけでなく、ソフトウェアの観点でも、サプライチェーンに影響を与えます。

「サードパーティにアプリケーションの構築を依頼している場合は、そのサードパーティが、環境に脆弱性を持ち込まない定義済みの反復可能なプロセスに従っていることを確認してください」

私は過去に複数の組織でそれを経験しました。脆弱性が持ち込まれたのは、悪意からではなく、誰もライブラリをチェックしていなかったからです。

私が常に推奨しているのは、使用している環境に対して分析的なアプローチを取ることです。「これらのシステムは必要なものか」、または、「これら特定のハードウェアをそっくり交換できるか」と自問してみてください。このようにして技術を更新すれば、明らかにデバイスの待ち時間を改善し、以前から存在していた可能性のある多くのセキュリティ問題を回避することもできます。

また、だれもが恩恵を受けられるセキュリティとなるようなアプローチをとってください。世界の多くの国でハイブリッドワークが取り入れられ、しばらくの間はこれが続くと思われます。

エンドユーザーが安全かつセキュアに仕事を遂行できるように、必要な環境を整備してください。エンジニアがエンジニアのために作成したツールをエンドユーザーが利用し続けると期待すべきではありません。

さらに深く知るために：

セキュリティ負債に対応する方法について、さらに洞察を得るには最新の『Duo Trusted Access』レポートをご覧ください。

『第 2 回セキュリティ成果調査』にはこの問題に対して組織が採用した取り組み方法について、役立つデータが掲載されています。

最も重大な脆弱性：気付いていない恐れがある

Jerry Gamblin
（Kenna Security セキュリティリサーチ担当ディレクタ）
との対談（Kenna Security はシスコグループになりました）

脆弱性を調査するためにチームで行っている作業について教えてください。

Kenna では、公開されているあらゆる脆弱性を注意深く監視し、お客様が最初に何に注目すればよいか把握できるよう、脆弱性にリスクスコアを付与しています。

脆弱性とその拡大状況の全体像をイメージしていただくために言うと、今年確認された CVE（共通脆弱性識別子）の件数は初めて 20,000 件を超えました。これは、1 日あたりで言うと 55 件の CVE が確認されたことになります。1 日に 55 件を超える CVE を評価して環境にリスクをもたらす脆弱性とそうでない脆弱性を区別できるようなレベルのスタッフがいるセキュリティチームはほとんどありません。

一般的な脆弱性フレームワークでは、たいてい、CVSS（共通脆弱性評価システム）によるスコアが 7.0 を超える脆弱性に対してパッチを当てることとしています。問題は、現在、平均 CVSS スコアが 7.1 という状況に置かれていることです。つまり、すべての CVE のうち少なくとも半分にパッチを適用することになります。

分かっているのはこの問題が大きくなり続けているということです（CVE の大半は正当な脆弱性であるため、「悪化している」という表現は避けています）。報告の漏れが少なくなったことと、可視化が進んだことも一因です。GitHub は現在 CNA（CVE 採番機関）であり、昨年オープンソースプロジェクトに関して最も多くの CVE を発行した機関になりました。

2021 年に特定された脆弱性にはよく知られたものがあります（たとえば、Log4j や Microsoft Exchange の脆弱性）。ただし、重大な脆弱性の中には、よく知られておらず気付かれない可能性があるものが相当数あります。

Chrome や Edge などのオープンソースプロジェクトに影響する脆弱性が多く見つかり、この夏には PrintNightmare CVE など Windows を標的とする脆弱性も見つかりました。

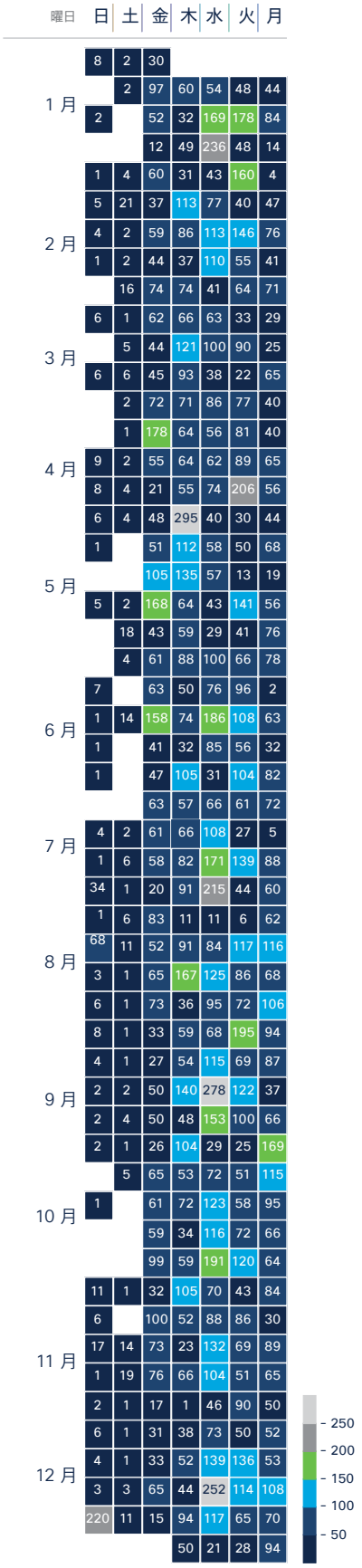
2021 年における CVE の要約

- CVE の総数：20,129
- CVE の 1 日あたりの平均数：55.3
- CVSS スコアの平均：7.1

2022 年 1 月 における CVE の要約

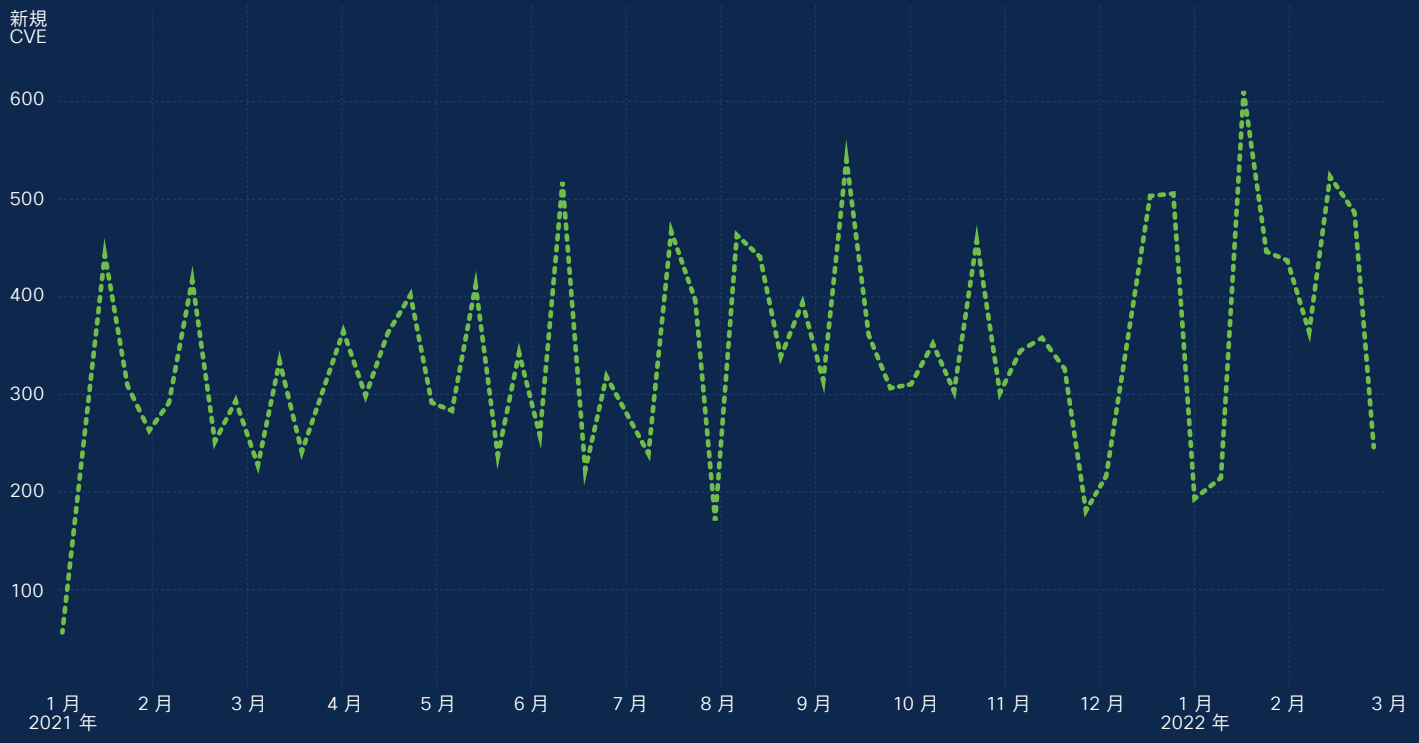
- CVE の総数：2,020
- CVE の 1 日あたりの平均数：65.16
- CVSS スコアの平均：6.86
- 2021 年 1 月 (1,523) と比較した増加：32% すなわち +497

2021 年に発見された 1 日あたりの CVE



出典：Kenna Security

2021 年における週ごとの CVE の数：



出典：Kenna Security

脆弱性の開示がトップ記事になることはあまりありませんが、なぜもっと注目される必要があるのですか。

脆弱性管理に関して言えば、組織に最も重大なリスクをもたらすのはニュースの見出しに出てこない CVE であることが多いため、必要な経営層の注目や組織のリソースを防御者が得るのが難しいことがあります。

20,000 を超える CVE があるため、メディアの注目を集めるものもあるでしょう。しかし、そのメディアの注目から漏れてしまった脆弱性の方が、組織に重大な影響を与える可能性がずっと大きいと言えます。

脆弱性管理のリソースに関して言えば、この状況はまさに綱渡りです。ニュースはすぐに伝わりますし、関係者からの圧力は支配的です。情報が不足しているリソースが最新の脆弱性への対応が最優先だと判断すると、1 週間を無駄にすることになります。このような時には、リスクベースの優先順位付け（および修正リスト）が有効であり、これによって本当に重要なことを常に把握しておくことができます。

Cybersecurity and Infrastructure Security Agency（CISA）は、組織に脆弱性修復へのアプローチを進化させることを訴えている影響力のある機関の 1 つです。CISA が 2021 年 11 月に発令された拘束力のある運用指令 22-01 で述べたことは次のとおりです。

「攻撃者は、目標を達成するために「重大な」脆弱性だけに依存しているわけではない。最も広範で壊滅的な攻撃には、「高」や「中」、さらには「低」と評価された複数の脆弱性が関係していた。（中略）エクスプロイトされた既知の脆弱性は、最優先で修復すべきである」

- CISA、拘束力のある運用指令 22-01

© 2022 Cisco and/or its affiliates. All rights reserved.

2021 年にあなたのチームが多くの時間を割いたものは何でしょうか。重要な脆弱性をいくつか挙げてください。

Chrome V8 エンジンには多くの時間を費やしました。Microsoft も今年、Internet Explorer から Chromium ベースの Microsoft Edge に移行したときに大きな変更を行いました。そこで、お客様がクローズドソースのブラウザからオープンソースのブラウザへの切り替えを理解できるようにしています。

仮想化の脆弱性も一般的になりつつあります。今年は、リスクの高い VMware ESXi の脆弱性がこれまで以上に多く確認されました。

また、私たちが（内部的に）「累積 CVE」と呼んでいるものも出現し始めています（まだ適切な用語がありません）。基本となる CVE が公開されてから数週間すると、同じコードに対してさらに多くの CVE が公開されていることがあります。累積 CVE の例としては、Log4j と PrintNightmare があり、どちらにも固有の CVE が複数割り当てられています。

このような状況では、RCE（リモートコード実行）の脆弱性、特に攻撃対象領域が大きい（および潜在的な影響が大きい）脆弱性に対処するベンダーの進捗状況を監視することが賢明です。

脆弱性の傾向について何か指摘できますか。

脆弱性の大きさと数は、今年さらに深刻な問題になるでしょう。Facebook の Prophet フレームワークを使用して、あるモデルを毎晩実行していますが、今年の CVE の数は 23,000 を超えると思われます。

さらに、通常、知りたい情報は CVSS スコアにはありません。最新の『Priority to Prediction』レポートを発表したときニュースになりました。Twitter の方がエクスプロイトの可能性を示す指標として優れていると記載したためです。

このレポートでは、エクスプロイトの可能性を最小化するには、公開されているエクスプロイトコードを使用して脆弱性に優先順位を付ける方が、CVSS よりも 11 倍効果的である根拠についても説明しています。

特に傾向を 1 つ挙げるとすれば、エクスプロイトされた脆弱性に優先順位を付け、攻撃者が次に標的にするものを予測することで、我々が得るものはたくさんあると言えます。あるいは、解消されるリスクがたくさんあると言った方がよいかもしれません。

「組織は、リモートコード実行の可能性やそれに対して公開されたエクスプロイトコードがあるかどうかを確認できる、リスクベースの脆弱性管理システムに移行する必要があります。これは、可能な対策の中で最も重要なものです。これによって組織への影響が想定される重要な脆弱性を特定することができるようになります」

脆弱性への対応で防御者が優位性を取り戻すためのベストプラクティスについて何かアドバイスがありますか。

パッチの自動適用をオフにしないでください。私は、IT 分野でのキャリアの早い時期に政府機関と民間産業の両方にいたので、事情は分かっています。パッチによって何が壊れるか分からないため、だれもが自動適用をオフにしたいと思っています。すべてをオンにしておいた方がはるかに効果的に防御されます。

通常のメンテナンスはパッチの自動適用に任せてください。そうすれば、テストとパッチ適用に多くの時間と労力が必要な脆弱性に時間をかけて取り組むことができます。

さらに深く知るために：

ニュースにならない可能性のある脆弱性を常に把握できるように、Kenna Security ブログでは最新情報を網羅しています。

私（Jerry）は CVE.ICU で毎日 Notebook を実行する個人プロジェクトも持っています。このプロジェクトでは CVE データセットに対してオープンソースのデータ分析を行っています。

Log4j とゼロデイへの備え方

Liz Waddell
（Cisco Talos インシデント対応チーム
プラクティスリード）との対談

Cisco Talos インシデント対応チーム（CTIR）チームは、Log4j の脆弱性に対するお客様の対応を最前線に立って支援しました。2021 年末のことです。まず、Log4j に関する事態の推移を説明します。

2021 年 11 月 24 日、Alibaba 社のクラウドセキュリティチームが Apache に、Java ロギングライブラリである Apache Log4j2 にリモートコード実行（RCE）の脆弱性があることを警告しました。後でこのことが関係してくるため重要です。

この特定のログライブラリを持つクラウドサービスとエンドポイントに統合されているコードライブラリとプロジェクトが、重複を除いて少なくとも 1,800 あります。Log4j が特定されたときには、この脆弱性の露出は… 新聞が取り上げたように、膨大な量になっていました。

11 月 30 日、Twitter ハンドル @p0rz9 を持つ匿名のセキュリティ研究者が、コンセプト実証への GitHub リンクを共有しました。翌日、世界各地の組織に対して実行されたエクスプロイトに関する最初のレポートが発表されました。

世間の注目が集まり始め、Apache から最初のパッチがリリースされたのは 12 月 9 日のことです。それから、私たち（Cisco Talos）がエクスプロイトを確認し始めると、ある奇妙なことが起こっていました。人気ゲーム Minecraft のユーザーが、このゲームの Java バージョンを実行しているクライアントやサーバーで、攻撃者が悪意のあるコードを実行する可能性があると警告し始めたのです。

12 月 10 日に初版の Talos ブログを公開し、最新の情報で更新を続けました。私は今では「脆弱性地獄」と呼んでいますが、大量の情報が集まり信じられないほど忙しい時期でした。

防御者は検出方法を調べ続け、企業は自社に脆弱性があるか解明しようと努力を続け、研究者は手当たり次第にスキャンして脆弱性が何人に影響を与えるのか調べていました。信頼できる唯一の情報源を持つことが防御者にとって非常に重要なのはそれが理由です。不要な情報をすべて切断する人物が必要です。

「この 1 年間で分かったことがあるとすれば、脆弱なアプリケーションに対して最初のパッチが公開されても、決してそれだけで終わらないということです」

Log4j では、このパターンのとおり 12 月 18 日までに 3 つのパッチが公開されました。昨年のホリデーシーズンを台無しにした SolarWinds の攻撃の後、2021 年のクリスマスも同じように過ごすことになると恐れていました。しかし、全体的に見て、休暇中に Log4j について問い合わせるお客様は多くありませんでした。

Log4j タイムライン

TALOS

2021 年 11 月 24 日
Alibaba 社 のクラウドセキュリティチームが Apache Log4j2 RCE の脆弱性を Apache に報告。

2021 年 11 月 30 日
Github プルリクエストにより脆弱性が公開される。

2021 年 12 月 01 日
最初のエクスプロイトが報告される。

2021 年 12 月 02 日
シスコがエクスプロイトを始めて確認。

2021 年 12 月 09 日
Apache が最初のパッチをリリース。

2021 年 12 月 10 日
Cisco Talos ブログが稼働。最初の記事を公開。

アクティブなエクスプロイトの拡散を確認。当初はマイナーを配信。

2021 年 12 月 11 日
Mirai ボットネットに関連する活動を確認。追加の記事を公開。

2021 年 12 月 13 日
Cisco Talos が、攻撃ベクトルとして電子メールの使用が試みられている証拠に加え、新たな難読化やプロトコルの悪用の証拠を発見。これを受け、ブログを更新し追加の記事を公開。

CISA が Log4j2 に関するアドバイザリを公開。

2021 年 12 月 14 日
Apache が追加のパッチ 2.16.0 をリリース。すべてのユーザーに対しアップグレードを要請。

Cisco Talos が、画像や Word ドキュメントなどのさまざまなメタデータソースに埋め込まれた Log4j2 を検出。ブログを更新し追加の記事を公開。

2021 年 12 月 18 日
Apache が、新たなサービス拒否の脆弱性に対処する追加のパッチ 2.17.0 をリリース。

これは、何も起こらなかったという意味ではありません。Talos は、マイナーやその他の金銭目的の攻撃者による活動など、アクティブなエクスプロイトに気付いていました。国家機関の攻撃者に関する報告があり、Talos のハニーポットやテレメトリソースでも広範な活動が観測されました。

脆弱性のエクスプロイトに関する報告が増加したのは 1 月 5 日で、このとき、英国の国民健康保険（NHS）から VMware Horizon サーバーで Log4Shell の脆弱性が確認されたとの報告がありました。

ゼロデイに対する Talos のインシデント対応計画

Log4j や 2022 年に予想されるゼロデイ攻撃に対処する組織にとって、Talos の 7 つのアクションプランが役に立つと思われます。

1 背景と脅威の概要

集まった情報がすべて集約され、お客様が独自の防御計画を立案する際に活用できるような、信頼できる単一の情報源が必要です。

Talos ブログを公開しており、そこには常に最新情報が掲載されています。

2 脅威対策機能

脆弱性が何であるかだけでなく、脆弱性を使うと何ができるかにも関心があります。CVE について心配する必要がありますか。Log4j と Microsoft Exchange の脆弱性については、まさに「イエス」でした。

攻撃者はシステムを制御できるだろうか。システムを制御できれば何ができるだろうか。攻撃者はラテラルムーブメントによってデータを盗みランサムウェアを展開できるだろうか。

エクスプロイトの経路を追跡していけば、これらの質問に答えることができ捜査が進展します。

3 自分に脆弱性があるかどうか知るにはどうすればよいですか。

これは、最もよくある質問です。

Log4j のようなものに関して言えば、最初に次の質問をします。「どのシステムが Log4j を実行しているか分かりますか」

Log4j によってアプリケーションに一律に脆弱性が生じるわけではありません。アプリケーションが Log4j を介してユーザー制御のデータを記録しているところは、正真正銘のベクトルであると判断する必要があります。

このベクトルは、ユーザー制御の URI、着信するユーザーエージェントと POST パラメータ、ユーザーが提供するファイルのログから何らかの形で表面化します。多くの場合、ユーザーが関与する値が取り込まれてから Log4j フレームワークがその値を使用するまでの間に、間接的なレイヤがいくつか存在します。そのために、個々の経路のリスクを評価する作業がますます複雑になっています。

また、影響を受けるのはシステムだけではありません。ベンダーやパートナーが影響を受ける可能性もあります。このエクスプロイトが表面化したときに私たち全員が大きな不安を感じたのはそのためです。

4 自分がエクスプロイトされたかどうかを知るにはどのようにすればよいですか。

組織がエクスプロイトされているかどうかを判断するために使用できるリソースがいくつかあります。私たちのチームには一覧化したリストがあります。

リソースには Log4j 専用のものがあります。それ以外は一般的なもので、アラートを設定する必要があります。いくつかの例を次に示します。

- 侵入の痕跡（IOC）の存在を確認するには、境界セキュリティデバイスログ（ファイアウォール、IDS/IPS など）を検索します。
- ネットワーク境界で RMI と LDAP のプロトコルとポートを検査します。これらのプロトコルを使用すれば、必要に応じて既知の信頼できる通信を許可するブロックリストの例外を作成できます。
- オペレーティングシステムのイベントログを検査し、HTTP リクエストの中に疑わしいものや悪意のあるものがないか確認します。
- Web サーバーのログを検査し、関連する IOC がないか確認します。
- アプリケーションがあるシステム（Log4j ライブラリなど）の上に構築されていないか識別するために Talos のアナリスト（あるいはお客様）が使えるスクリプトを提供することも可能です。

5 脆弱性があるもののエクスプロイトされていない場合はどうすればよいですか。

現在のガイダンスに基づいて共有可能な脅威の軽減策を特定します。軽減策が「そのシステムにパッチを適用する」といった簡単な場合もあります。一例を挙げると、「Log4j：最新のパッチを用いて更新し、Java Naming and Directory Interface（JNDI）を無効化する」。パッチを適用できない場合は、他の軽減策を調査します。

6 脆弱性がありエクスプロイトされた場合はどうすればよいですか。

お客様の立場からすると状況によって異なります。しかし、Log4j のケースでは次のようなかなり簡単はものでした。手順 1 ～ 5 のすべてを実行し、組織のインシデント対応計画をスタートさせてください。そしてお電話ください。

7 侵入の痕跡

作成して更新するのに最適なリソースの 1 つとして、侵害の痕跡（IOC）のリストがあります。私たちは、IOC を含めてあらゆる情報を Talos ブログに掲載しました。通常、IOC のタイプは、IP、ドメイン、ユーザーエージェントです。または Log4j の場合のように SHA-256 ハッシュといった特定の Web シェルのこともあります。

© 2022 Cisco and/or its affiliates. All rights reserved.

このレポートを作成している時点（2022 年 2 月）で、Log4j はどのような状況でしょうか。

NHS に影響を与えた Log4Shell の脆弱性が Web シェルを確立するためにエクスプロイトされていることが分かりました。残念ながら、攻撃者が Web シェルを使用すれば、マルウェア、ランサムウェア、リックロール、ログイン情報やデータの盗用など、無数の不健全な活動を行うことができます。

結論として、影響を受けた VMware 製品へネットワークからアクセスできる攻撃者は、これらの問題をエクスプロイトして、ターゲットシステムを完全に制御できたのです。

Huntress 社によると、1 月時点でインターネットからアクセスできた VMWare Horizon サーバーは約 25,000 台あります。また、Huntress 社によると、これらのサーバーの多くはパッチが適用されていません。

これらの脆弱性の取り扱いは、実行可能ファイルのいくつかが AV および EDR の監視から除外されていることから、複雑になっています。Talos や他のいくつかのセキュリティ企業は、攻撃者がこれを積極的に利用しているのを見てきました。

以上が今の状況です。いま目にしている主なエクスプロイトは、VMware Horizon サーバーをターゲットにしています。

ただし、どのように世界とダーク Web を監視すればよいか、何か変化やさらなるエクスプロイトがあった場合、どのようにすればそれに最大限効果的に対応できるか、引き続き精力的に検討を続けています。

このアプリケーションは、多くのものに組み込まれています。専用の Talos ブログにはすべての調査結果が掲載されており、最新の状況を把握することができます。

Log4j は今年、どのような影響を与えると思いますか。

Log4j は 2022 年も影響を与え続けるでしょう。VMWare Horizon エクスプロイトですでに確認済みです。今重要なことは、できる限りプロアクティブに行動し、この脆弱性を使って環境をエクスプロイトしようとする攻撃者がアクセスする可能性のあるポイントを見つけ出すことです。

重要なのは、活動の別の兆候を組織が監視し続けていることです。これらは最初のハンティングで見逃していた可能性があります。ラテラルムーブメントの兆候がありますか。環境が侵害されたことを示す兆候はありますか。

この脆弱性や今年予想されるゼロデイに対処する防御者に向けて何かアドバイスはありますか。

ゼロデイに関する緊急事態が発生している間は、脆弱性が 1 つ開示されると、脆弱性に関連するエクスプロイトが増加することを忘れないでください。分かったことを文書化し、常に更新し続けてください。

情報を文書化することでどれだけの時間が節約できるか、お客様の環境での経験に基づいて正確な数字で示せればよかったと思います。信じてください。非常に大きな数字になります。

さらに深く知るために：

2021 年のインシデント対応に見られる傾向についての詳細は、Cisco Talos ブログをご覧ください。

セキュリティ上の緊急事態が発生した場合は、Cisco Talos インシデント対応チームに電話してください。米国：1-844-831-7715 ｜ ヨーロッパ：(44) 808-234-6353

Emotet の現在の状況

Artsiom Holub
（Cisco Umbrella シニア セキュリティ アナリスト）との対談

脅威の世界における Emotet の歴史と、この脅威がどのようにして広く拡散したかを教えていただけますか。

Emotet にはかなりの歴史があります。Emotet は単純なバンキング型トロイの木馬として 2015 年に初めて登場しました。当時、多くのトロイの木馬が存在していましたが、Emotet には非常に強力な開発者チームがいたため、他とは少し異なっていました。つまり、常に進化を続けていたということです。

2016 年には、初めてローダーとして再構成されました。2017 年になると、「サービスとしてのローダー」モデルとして提供され始めました。Emotet が実際に幅広い影響を及ぼし始めたのはこのときです。TrickBot や QakBot などのマルウェアとの連携を試みたからです。

2018 年から 2019 年にかけてこのマルウェアが多発しています。また、Emotet、TrickBot、Ryuk ランサムウェアの 3 つを利用して重大な攻撃が複数実行されました。

ヨーロッパ最大の金融センターの 1 つであるドイツのフランクフルトにある IT ネットワークが、Emotet が関与したサイバー攻撃によって停止しました。ペンシルベニア州の都市アレンタウンでは、マルウェア攻撃により市の重要なシステムが機能不全に陥りました。このマルウェアは広範囲に広がり、軽減するために市が支出した費用は約 100 万ドルに上っています。また、ドイツのベルリンにある最大の州裁判所が攻撃され、大量の機密データが盗まれています。

Emotet の規模や併用された付随的なマルウェアについてイメージをつかんでいただくために言うと、Cisco Umbrella は 2019 年に月あたり最大 400 万件のリクエストをブロックしていました。

2020 年、セキュリティ業界では、Emotet を消滅させるための一丸となった取り組みが行われました。この作戦はほどほどの成功をおさめ、活動が停止した期間が幾度かありました。

しかし、攻撃者はこのような強力で儲かるビジネスをそれほど簡単にはあきらめません。活動の中断は、検出の回避を狙うだけでなく、これまで以上に強力になって復活する方法を練るのにも利用されたようです。

2020 年後半、Emotet は再作成されたコードと、悪意のあるペイロードを組織に大規模に配信する新しい方法を携えて戻ってきました。これは、民間部門と政府部門の両方でエンタープライズ ネットワークにアクセスできる最初の大規模ローダーの 1 つになりました。

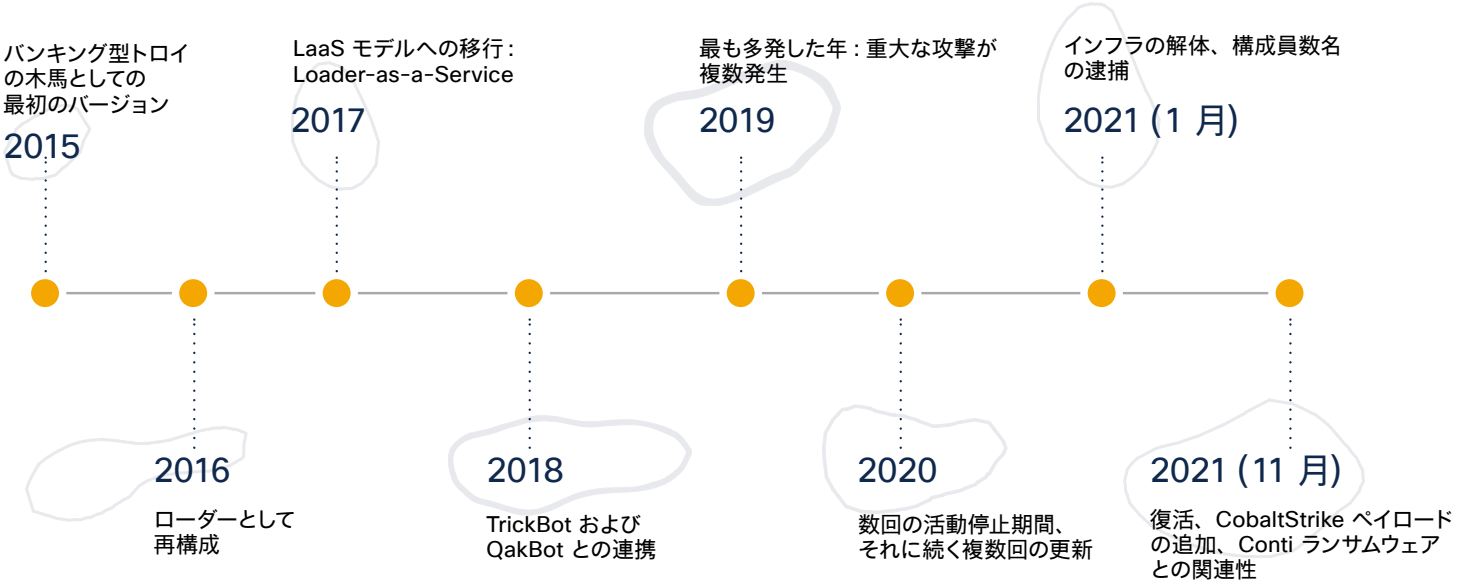
Emotet の活動に対する 2021 年の取り組みはどのようなものでしたか。

1 月、官民両セクターの協力にユーロポールとユーロジャスト（欧州司法機構）主導の作戦が加わり、Emotet の活動は再び停止に追い込まれました。Emotet のインフラストラクチャも大部分が解体されました。

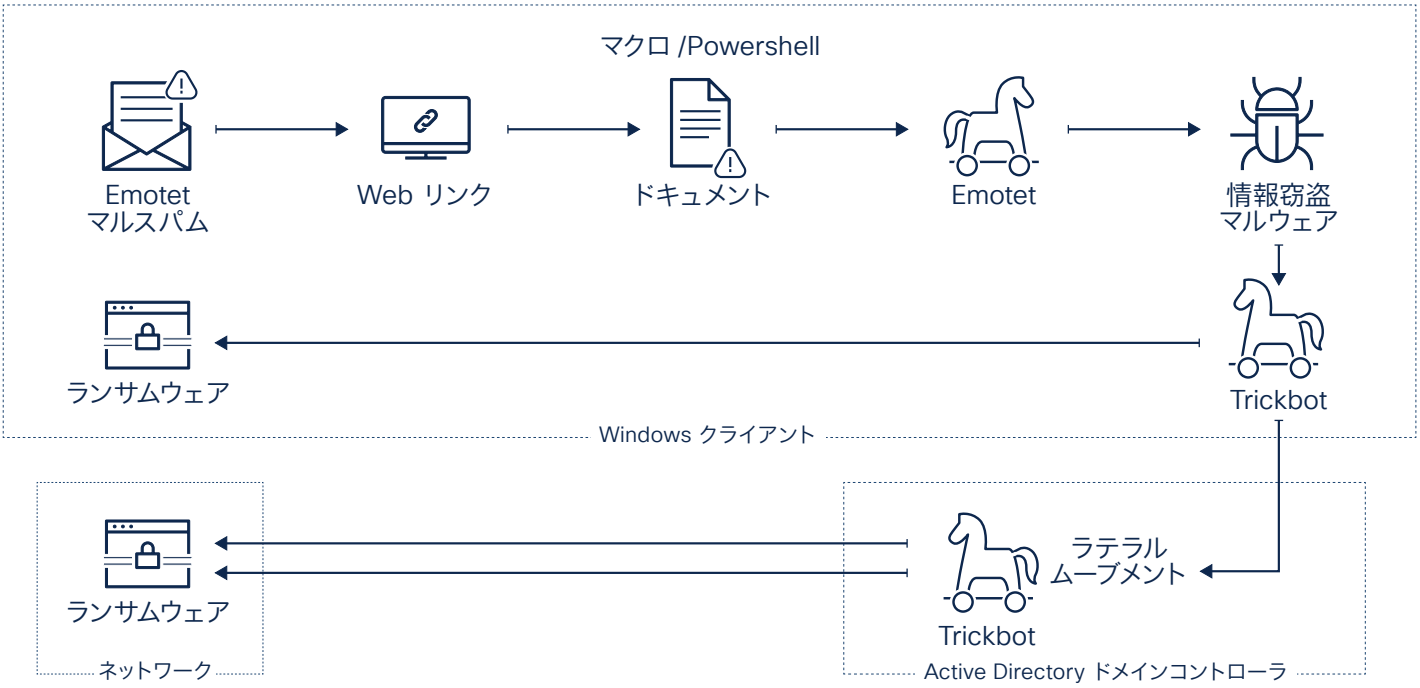
4 月には、感染が判明したすべてのデバイスから Emotet がアンインストールされました。さらに、ウクライナのサイバー警察による別の作戦が成功し、Emotet の主要な開発者であると思われるギャングの構成員数名が逮捕されました。

当時、私たちはこれが Emotet について聞く最後になると期待していました。残念ながら、そうではありませんでした。

Emotet の進化



ランサムウェアのキルチェーンに変化をもたらした Emotet



2021 年末の Emotet の復活はどのようなものでしたか。

活動の本質がマルウェアであったことと、サイバー犯罪コミュニティに利益をもたらすことができたことから、Emotet が実際に復活したことを確認しました。今回の復活には新たに再構築されたインフラストラクチャが伴っていて、このインフラストラクチャは現在も拡張を続けています。

Emotet の復活は、ランサムウェアの世界でそのような活動に対する需要が高まっていることを示しています。Emotet ボットネット開発者に無限の機会を提供するには、高度に組織化された犯罪組織がいくつかあれば十分です。

TrickBot と Emotet の 2 つは、Ryuk ランサムウェアによって頻繁に利用されていましたし、今では Conti が犯罪者にとって合理的な新しい手段になっています。

Conti は、収益を最大化するために、高度な標的型攻撃を組織しています。事態がこの方向に進み続けた場合、TrickBot と Emotet が Conti ランサムウェアを配布する独占的な方法となり、今後 1 年でこの攻撃がさらに広範に蔓延することはほぼ確実です。

もう少し詳しく説明していただけませんか。これまで見てきたことを踏まえて、2022 年には Emotet がどのような形で現れると予測していますか。

「私は、Emotet が 2022 年の最大の脅威になり得ると考えています。これは、（再び）復活を遂げた非常に強力なローダーです」

この予測は、Emotet、TrickBot、Ryuk の 3 つが、それ自身の振る舞いだけでなく、すべてのランサムウェア運用者の手口をどれほど変えたかを知ったうえで行ったものです。また、サプライチェーン攻撃で初歩的な手法として使用されていることも確認されています。

Emotet の脅威は複数のレベルからなっています。最初のレベルでは、システムに最初の足場を築き、影響を受けたネットワークの非常に強力なプロファイルを構築します。次のレベルでは、TrickBot や Cobalt Strike などの展開が行われます。ラテラルムーブメントのための非常に強力なツールであり、ネットワーク全体を奪取することができます。

現在、Conti が高度に組織化されたランサムウェアプロバイダーとなっているため、2022 年には、この独自のキルチェーンが絡んだ重大な攻撃を目にすることになると予測しています。

© 2022 Cisco and/or its affiliates. All rights reserved.

防御者へのアドバイスは何でしょうか。どのようにすればこの種の攻撃から組織を保護することができますか。

どのようなセキュリティにも言えますが、Emotet を止める確実な方法はありません。階層化されたアプローチを採用してください。さらに、ネットワークのどこに弱点があるか把握し、それらのポイントでセキュリティ管理を実施してください。

「アナリストとして私が常にお勧めしているのは、ラテラルムーブメントとインターネットへのデータ漏洩の検出を中心に防御戦略を立案することです。サイバー犯罪との結びつきを監視するために、発信トラフィックには特に注意を払ってください」

最後に、攻撃者が使う戦術、技術、手順（TTP）を知るために最新の脅威インテリジェンスを使用してください。攻撃者は、ツールや活動を変えることがあっても、過去にうまくいった手順を踏襲する傾向があります。

さらに深く知るために：

Cisco Umbrella のレポート『The modern cybersecurity landscape : Scaling for threats in motion』をご覧ください。

Emotet の復活についての詳細は、Cisco Talos ブログをご覧ください。

macOS マルウェアの台頭

Ashlee Benge
（Cisco Talos 戦略的インテリジェンスおよびデータ統合リーダー）との対談

macOS マルウェアの背景と、それを取り上げようと思った理由を教えてください。

これは私自身が関心を持っている研究分野です。このレポートでそれを取り上げたかったのは、macOS がマルウェアに対してある程度耐性があるという前提の下であまりにも長い間運用されてきたからです。この固定概念は、Mac が登場して以来ずっと続いています。

セキュリティ研究者の元には大量の情報がやってきます。私のチームの仕事は、そのような膨大な量のデータを掘り下げて、攻撃者の行動の変化を特定することです。何か変更があれば、新たに出現した脅威をハンティングします。

最近では、macOS マルウェアがこのような状況になっています。macOS が魅力的な攻撃対象領域になりつつあり、2021 年には懸念される新しいタイプの macOS マルウェアがいくつか発見されました。

macOS のみを標的とするマルウェアや複数のオペレーティングシステムを標的にできるマルウェアがますます増えています。オペレーティングシステムが Linux、Windows、macOS のいずれであっても、攻撃者は同じマルウェアを使用してシステムを実行したり侵害したりすることが可能です。

このレポートの執筆時点で Apple 社は、iOS および macOS デバイスのゼロデイ脆弱性に対する修正を 2022 年の最初の 2 ヵ月間に 2 つ発行しています。これらの脆弱性は、WebKit に影響を与え、iOS や macOS のユーザーをリモートコード実行攻撃にさらす可能性があります。

この脆弱性の重大度は大きく、攻撃者がこの脆弱性を利用すると、侵害されたネットワーク全体に存在を拡大することができます。最初のアクセスに成功した後、攻撃者が何をしたいかによって状況が変わります。

多くの場合、二次的なマルウェアがドロップされて実行されます。このマルウェアとしては、クリプトジャッカー、ランサムウェア、バックドアが考えられます。

バックドアは、機密情報を盗み出すのに利用できます。盗まれた情報が標的の組織に対する脅迫やその他の加害行為に利用される可能性があります。攻撃者は、標的のデバイスを使用不能にすることもできます。その結果、サービス拒否や運用の中断が発生する可能性があります。

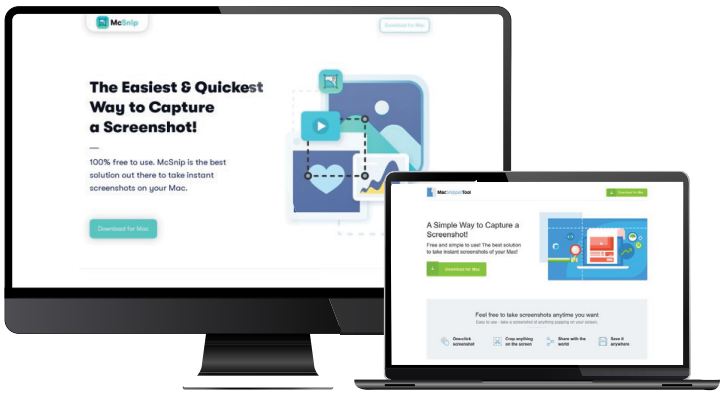
2021 年に発見された、macOS を標的としたマルウェアの例を説明してください。

2021 年 8 月にあった興味深い発見の 1 つが、McSnip バックドアと呼ばれるマルウェアでした。

いつもどおりの一日が始まりました。私たちは攻撃者の行動を監視し、新しいマルウェアファミリの特定につながる変化を探していました。

既存のドロッパー技術に変化があることを見いだしました。ドロッパーとは、エクスプロイトに先だってシステム上に最初のバイナリを取得するために、マルウェア攻撃者の特定のグループが用いている方法の 1 つです。

私たちは、この攻撃に関連すると思われる悪意のあるファイルを可能な限り捕捉し、これらのファイルを分離しました。非常に興味深いことがいくつか判明しました。



このバイナリには機密情報を流出させる機能がありましたが、それらの機能が利用されている形跡がありません。私たちが警戒したのはこの点です。

McSnip の場合、この悪意のあるバイナリは、スクリーンショットツールになりすましていて、正規の App Store からではなく、ある Web サイトから直接ダウンロードできるようになっていました。

アクティブな攻撃がないことを確認するために、このマルウェアのハンティングツールを開発しました。その後まもなく、McSnip メソッドを使用してシステムを侵害しようとする動きは収まりました。

11 月後半には、他のセキュリティ組織も McSnip を検出し始めました。私たちも、ほぼ同じ時期に 2 回目の攻撃を確認しています。8 月に確認されたマルウェアに対して小さな更新が加えられていて、新たに加えられた悪意のある機能を利用してデータ漏洩が行われていました。

8 月に確認されたのは最初のテスト段階であったと考えられます。このマルウェアの背後にいる攻撃者は、ドロップメカニズムが計画どおりに機能し、標的のデバイスにバイナリをドロップできることを確認しようとしていたのです。攻撃者が McSnip を使用してシステムを積極的に侵害しようとしていた 11 月が本当の攻撃の始まりでした。

今も、McSnip が出回っていてお客様に対して利用されています。あるいは利用が試みられています。しかし、積極的なハンティング活動とチームの働きのおかげで、これらの悪意のあるファイルが実際に実行されるのを阻止することができました。

McSnip バックドア

エンドポイントを保護する防御者に向けた 2022 年のアドバイスは何でしょうか。

攻撃対象領域を十分に理解することが、私の最大のアドバイスです。そのために、脅威モデリングを行うことと、複数のチーム間でコミュニケーションを取り、脆弱な部分はどこかをしっかり把握することが欠かせません。

「エンドポイントに関しては、積極的なハンティング演習が非常に効果的です。行動やパターンの変化を探すようにして、決して既知のものだけに頼らないようにしてください。未知のものを探せば、気付かなかったギャップを埋めるのに本当に役立ちます」

さらに深く知るために：

脅威モデリングの詳細については、「What is threat modelling?」リソースページをご覧ください。

© 2022 Cisco and/or its affiliates. All rights reserved.

Cisco Secure の有効性

セキュリティの復元力を構築し、予測不可能な脅威や変化の中で組織の完全性を保護しようとしている防御者にとって、Cisco Secure が役に立ちます。シスコはお客様のパートナーとなって、セキュリティのギャップを埋め、次に何が起こるかを予測します。同時に、組織全体の復元力構築に向けた投資を強化できるようお客様を支援します。

マシン規模の観察結果を人が理解できるレベルで提供する Cisco Secure は、視野の拡大と脅威検出の迅速化に貢献します。既知の脅威のみならず新たな脅威にも対応した Cisco Talos の比類のない実用的なインテリジェンスと組み合わせることで、防御者は一歩先んじることができます。シスコのプラットフォームアプローチについての詳細は以下をご覧ください。

Cisco SecureX

組み込み型プラットフォーム エクスペリエンスをシスコのポートフォリオ内で実現したクラウドネイティブな Cisco SecureX で、セキュリティ防御の一元化を実現してください。

Cisco SecureX は、統合型のオープンな構成でシンプルさを実現するとともに、一元化によって 1 つの場所で可視性を提供し、ネットワーク、エンドポイント、クラウド、およびアプリケーションを保護するために運用効率を最大限まで高めます。

Cisco SecureX の詳細

Cisco Talos インシデント対応チーム

当社のインシデント対応チームはお客様と向き合い、侵害の有無の確認と、侵害があった場合の正確な状況把握を支援します。その後、可能な限り迅速に業務を再開できるよう各組織にガイダンスを提供します。

2021 年 11 月、Cisco Talos インシデント対応チームは、2021 IDC MarketScape for Worldwide Incident Readiness Services でリーダーとして認められました。

Cisco Talos インシデント対応チームの詳細

Cisco Secure ソリューションについて：

セキュア アクセス サービスエッジ (SASE)

ネットワークとセキュリティ機能を単一のクラウド提供サービスに結合します。

SASE の詳細

Extended detection and response (XDR)

分析機能と自動化機能を内蔵したクラウドネイティブなプラットフォームで、生産性を向上させます。

XDR の詳細

ゼロトラスト

ユーザー、ネットワーク、アプリケーションを脅威から保護しつつ、セキュリティと使いやすさのバランスを追究します。

ゼロトラストの詳細

セキュアなハイブリッドワーク

どこにいても活躍できるよう、あらゆる場所でセキュリティを実現します。

ハイブリッドワークの詳細

ランサムウェア防御

多岐にわたる重要なコントロールポイントで、攻撃の防止と対応を行います。

ランサムウェア防御の詳細

さらに深く知るために

燃え尽き症候群について

このレポートを締めくくるにあたって、防御者が経験していると思われることについて個人的な観点から少し述べておきたいことがあります。最近発行した eBook『Creating Safe Spaces in Cybersecurity』では、サイバーセキュリティ業界の各分野で活躍する 20 名に、燃え尽き症候群の回避とメンタルヘルスの管理に関する事例を共有してもらいました。あなたや周囲の人が現在苦労しているなら、この eBook をぜひお読みください。

セキュリティ プラクティス トップ 5 の効果的な実践方法

『第 2 回セキュリティ成果調査』では、世界クラスのサイバーセキュリティ プログラムを構築するのに役立つ 5 つの必須プラクティスについて説明しています。レポートを読んで実用的な洞察を得たうえで、よりセキュアで効率的な作業環境の構築を開始してください。

『Talos Threat Source』ニュースレター

Talos Threat Source を購読してください。Cisco Talos からのインテリジェンスに関する最新情報を定期的に提供し、重大な脅威やその他のセキュリティ分野におけるトップニュースを毎週取り上げています。

Cisco Secure ブログ

シスコのセキュリティに関するブログを読んで、Cisco Secure 製品の発表、業界ニュース、ソートリーダーシップに関する最新情報を入手してください。

セキュリティ成功事例のポッドキャスト

Security Stories ポッドキャストを聞いてください。組織でサイバーセキュリティに取り組むリーダーに欠かせない要件の背景には、ユニークで刺激的、そしてしばしば面白いストーリーがあります。

©2022 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)
この資料の記載内容は2022年4月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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

834068962JA 22.04


cisco
SECURE