ManageEngine
Log360

The MITRE ATT&CK 概要説明編

www.manageengine.jp/products/Log360/

はじめに

”サイバー空間の脅威”は、物理空間におけるそれと同様に、綿密に立てられた作戦の遂行に徹します。実空間、つまり物理空間の戦術では、防御体制の強い箇所を避け、弱点を突くような攻撃が繰り広げられてきました。

サイバー空間における脅威において、攻撃者の目標は通常、脆弱性を特定し、情報保証の5つの柱（機密性、整合性、可用性、否認防止、認証）の1つをノックダウンすることです。この目標を達成するには、攻撃者が被害者のネットワークを精査し、脆弱性を特定する必要があります。攻撃者は、悪用できる可能性のあるアクセスポイントを把握するために、攻撃対象ネットワークの技術的側面に関する十分な情報を収集する必要があります。それに加えて、検出されずにできるだけ短い期間でこれらの目標を達成することも、攻撃者にはもとめられます。攻撃者が作戦を綿密に立てている間、組織側も想定される攻撃に対して頑強な防御体制を確立しておくことが不可欠です。組織は、適切な人材、プロセス、およびテクノロジーを駆使して、独自の防御戦略を策定しておく必要があります。

たとえば、あるオンラインの人気アパレルショップの競合他社が、サイバー攻撃者を雇って競合アパレルショップのサーバーを数時間停止させようとします。これにより、Webサイト中心に顧客対応行っている人気アパレルショップにとって、重要な「可用性（情報保証の一つ）」が妨害される可能性があり、大規模な損失に繋がりかねません。

攻撃者は、まず攻撃対象のネットワークインフラを偵察するところから始める場合が多いです。ネットワークを偵察する、ということは、顧客ユーザーのIPアドレスの検出、トラフィックパターンの調査、許可および拒否されたトラフィックの調査、また既存のセキュリティポリシーや侵入検知システムの把握などが含まれます。ここから、攻撃者はフィッシングメールを介して、その人気アパレル店の顧客ユーザーのリストを標的として、ネットワーク侵入のための最初の足がかりを得ようとします。

ユーザーが無意識のうちにフィッシングメールを開き、悪意のある添付ファイルをダウンロードしてしまえば、マルウェアがリリースされてしまいます。そしてこのマルウェアは、攻撃対象のデバイスと攻撃者側のデバイス間で通信チャネルを確立します。そこから、攻撃者はコマンドを送信して、ネットワーク上のより多くのシステムに感染を広げていきます。

これらの感染したシステムたちは、攻撃対象のサーバーに過負荷をかけるボットネットを形成し、サーバークラッシュの原因となる大量の偽リクエストを送信するようになります。これは、分散型サービス拒否（DDoS）攻撃の例です。図1は、このシナリオを図で表したものです。

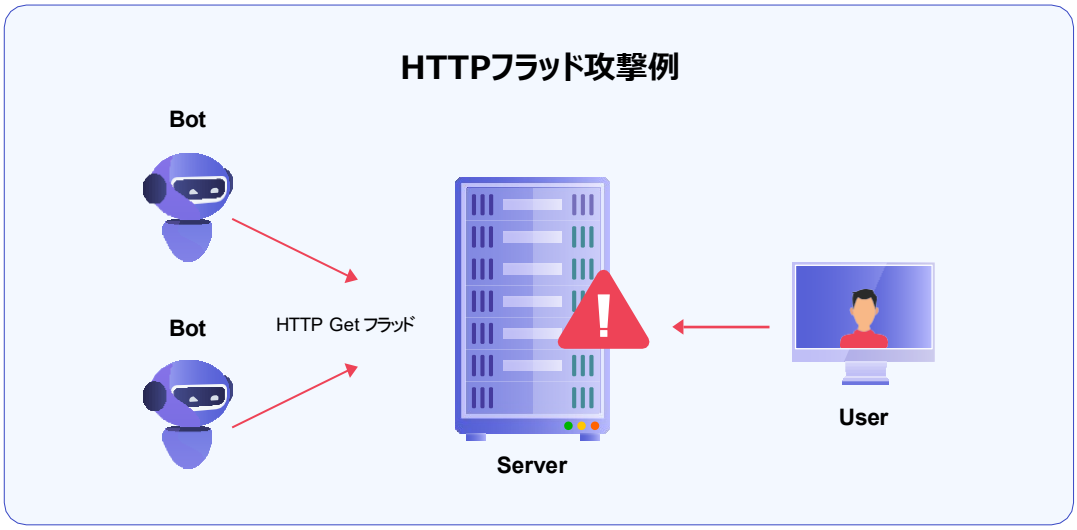

図 1 -a：HTTPフラッド攻撃のメカニズム

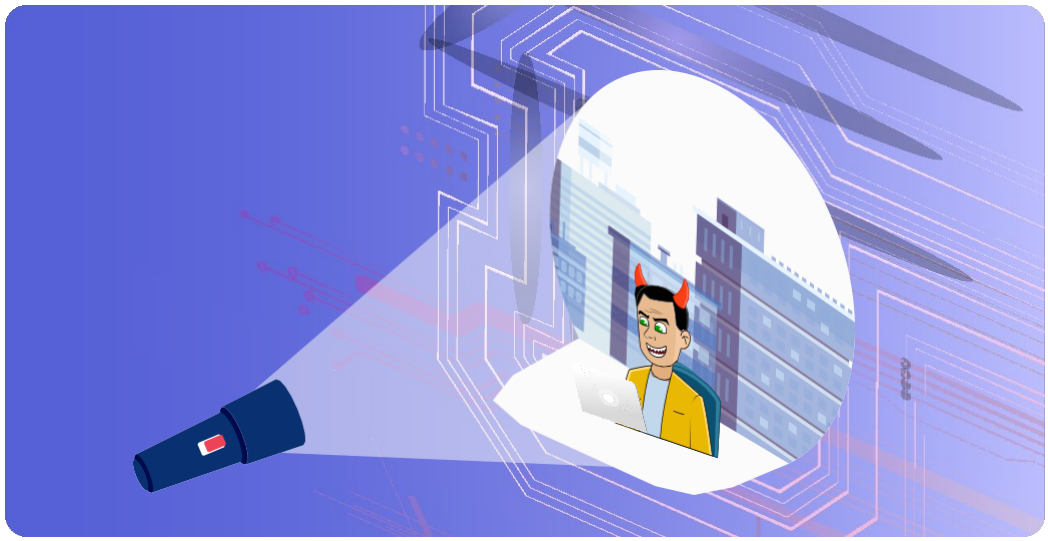

図 1 -b：オンラインのアパレルショップに対するDDoS攻撃を仕掛け続けるハッカー

※DDoS攻撃の詳細については[こちら]のホワイトペーパーをご覧ください。

DDoS攻撃から身を守るには、アパレルショップ側で適切な防御策を講じる必要があります。まず組織全体のネットワークで発生するすべてのアクティビティを完全に可視化しておく必要があります。潜在的な脅威を検出するには、これらのアクティビティを相互に関連付けて可視化できていなければなりません。また、これらの脅威を検出した際に迅速に対応できる体制も確立できていなければなりません。

これらすべてを効果的に行うために、組織としては、サイバーセキュリティフレームワークを実装したSIEMソリューション（Security information and event management）ソリューションを有効に活用するのが良いでしょう。

攻撃者側は常時戦争を仕掛け、機密データを盗もうとしています。実際、COVID-19のパンデミックにより、サイバー犯罪は600%も増加しています[*1]。さらに、サイバー攻撃は2025年までに1兆ドルもの被害がでると推定されています[*2]。守備範囲が広く、また再現性があり費用効果の高いアプローチを実現するサイバーセキュリティフレームワークの実装は、ビジネスの保護において大いに役立つでしょう。

2013年にMITRE社によって開発されたMITREATT&CKフレームワークは、2015年に一般公開されました[*3]。MITREATT&CKフレームワークは業界内で高く評価され、一般公開されている既知のサイバー攻撃に関する情報を参考に作成されたナレッジベースです。このフレームワークは、実際に攻撃者が用いた戦術や手法について記載されているので、セキュリティの専門家はより強固な防御体制を敷く際に、参考にすることができます。

他のフレームワークと比較して、MITRE ATT＆CKの場合、攻撃者が示すさまざまな動作をより詳細に調査しており、組織内のシステムがどのように侵害されていくかについて説明しています。このナレッジベースを活用することで、組織はより頑強な防御体制を確立することが可能になります。

MITER ATT＆CKフレームワークは、攻撃者が組織のネットワークを侵害してデータを盗むために実行する14の戦術を詳述したマトリックスの形式で提示されます。同フレームワークにて記載されている多様かつ巧妙な攻撃手法が、これらの14の戦術に起用されます。

フレームワーク内には「Procedures」という箇所が各攻撃手法に追記されています。この「Procedures」では、実際の攻撃手法がどのように実行されたかに関する実例が記載されています。最近、MITRE ATT＆CKが更新され、各攻撃手法に関する非常に具体的な詳細として"サブテクニック"というものが追記されるようになりました。

たとえば、特権昇格または防御体制を回避するための「プロセスインジェクション」という攻撃手法についてより詳細に調査されたこの"サブテクニック"を参照することにより、悪意のあるコードがプロセスにどのようにインジェクトされたかをより理解できるようになります。フレームワークによると、この「プロセスインジェクション」には、11のサブテクニックが存在しており、PE（Portable Executable）インジェクション（PE形式のEXEファイルへのインジェクション）やスレッドハイジャックインジェクションなどがあります。

このホワイトペーパーでは、攻撃者が組織へ攻撃を仕掛ける際に利用する14の戦術について説明します。攻撃者が各戦術にどのような攻撃手法を起用するのかについて、より具体的に説明します。

※本稿で説明されている戦術と各種テクニックは、MITRE ATT＆CKフレームワークでカバーされている全てのリストを網羅しているわけではありません。ただし、ここで説明される戦術やテクニックは、一般的な攻撃のライフサイクルで実行されるものが多い部分をカバーしています。

MITRE ATT&CK マトリクス

MITER社は、ATT＆CKフレームワークを策定した非営利団体です。このフレームワークは、ネットワークの侵害に濫用される攻撃パターンについて、一般企業が理解出来るようになることを目的として策定された、世界的に誰でもアクセス可能なナレッジベースのことです。

またこのフレームワークは、実際のサイバー攻撃による実例に関する調査結果を基に作成されました。企業組織が攻撃者達と対峙する場合に役立つ支援ネットワークとして機能することを目的としています。同フレームワークは、昨今絶えず変化し続けるサイバーセキュリティ環境、に対応できるように、常にサイバー攻撃に関する新情報や調査によるインプットを基に日々更新され続けています。

頭字語の「ATT＆CK」は、Adversarial Tactics, Techniques and Common Knowledgeの略です。MITREのマトリクスはそれらの各分野ごとに構成されています。

戦略（Tactics）、テクニック（techniques）、サブテクニック（sub-techniques）

マトリクスに構成されている14の戦略は、攻撃者が組織内ネットワークで、達成を試みる段階的な目標を意味しています。

マトリクスに記載されいる戦術群は、攻撃対象ドメインの偵察から始まり、インパクト（通常のビジネスとしての機能を混乱させる結果）という段階で終わります。マトリクスで概説されている攻撃手法は、攻撃者が特定の「戦術」に起用するテクニックに関する詳細を説明しています。サブテクニックは、その攻撃手法がどのように実行されるかについて、より詳細についての解説となります。しかし、攻撃者がフレームワークに記載されているすべての戦術を段階的に踏むというわけではありません。なぜなら、攻撃者たちはできるだけ、踏むべき段階的な目標達成を最小限に抑えようとするからです。

MITRE ATT&CKフレームワークの「戦術」

MITRE ATT＆CKフレームワーク[*4]は、14の戦術で構成されています。各戦術にはTA00xxのような形式でIDが採番されています。xxは数字を示します。これらの14の戦術とそのIDを以下に示します:

- **偵察（TA0043）**：攻撃対象の組織が保有するIPアドレス、またセキュリティポリシー、ユーザーリストなどの詳細についての情報を収集します。

- **攻撃態勢の確立（TA0042）**：攻撃対象システムと攻撃者の間の通信チャネル設定など、攻撃時の操作を支援するようなリソースを充足させます。

- **初期アクセス（TA0001）**：フィッシングや外部リモートサービスの悪用などの常套手段でネットワークへ侵入します。

- **実行（TA0002）**：攻撃対象のシステムで悪意のあるコードを実行し、攻撃者がそのシステムをリモートコントロールできるようにします。

- **永続化（TA0003）**：攻撃者は、攻撃対象のネットワーク内で巧妙に存在し続けることにより、コンフィグレーションや資格情報の変更などを行い、正当なユーザーがネットワークへアクセスできないようにします。

- **権限昇格（TA0004）**：悪用したアカウントの権限を昇格させるための、より高いレベルのアクセス許可を取得します。

- **防御回避（TA0005）**：システム上の正当なソフトウェアと既存のツールにアクセスして、システム内で活動しているマルウェアをマスキングし、また自身の痕跡を隠蔽します。

- **認証情報アクセス（TA0006）**：キーボードキャプチャ用のソフトウェアなどを利用してユーザーの資格情報を盗み出します。

- **探索（TA0007）**：悪用できるネットワーク上の脆弱なポイントを探索します。これには、アカウントのリストや環境内でのステータスの発見、または悪用されるかもしれない同ネットワーク上の複数のドメイン間での信頼関係の調査等も該当します。

- **水平展開（TA0008）**：資格情報を使用して複数のシステムを水平展開することや、リモートセッションを悪用して組織のネットワーク内を縦横無尽に移動します。

- **収集（TA0009）**：クラウドストレージ内のデータへのアクセスなどによる、データ収集を行います。

- **C&C（TA0011）**：悪意あるタスクを実行するために、ネットワーク上にある攻撃者によって侵害されたシステムと通信することです。攻撃者は、アプリケーションやWebプロトコルを利用して、悪意のあるコマンドを通常のトラフィックに隠してしまうため、攻撃者と被害者のシステム間の通信を検出することが困難になります。

- **盗み出し（TA0010）**：自動化処理によりデータを盗み、検出を回避するために盗んだデータをパッケージ化します。盗み出されたデータは通常、圧縮および暗号化され、事前に確立しているC＆Cチャネルではなく、代替プロトコルを介して盗み出しが行われます。

- **インパクト（TA0040）**：情報保証５つの柱の１つ「可用性」を破壊するか、又はビジネスの運営や運用プロセスを操作することによってデータの整合性を損なおうとします。この「インパクト」に使用される攻撃手法には、データの破壊または改ざんも含まれるため、ビジネスに多大なる影響を与えかねません。

MITRE ATT&CKフレームワークの「攻撃手法／テクニック」

前述した各戦術は、攻撃者によって使う手法は様々です。その攻撃手法は、特定の戦術に起用される攻撃の技術を指します。各戦術には、1つまたは複数の関連する攻撃手法が起用されます。たとえば、「初期アクセス」では、10の異なる攻撃手法のいずれかを起用することで実行されます。各手法には、Txxxxの形式のIDが採番されています。ここで、xxxxは番号を表します。

MITRE ATT&CKフレームワークの「サブテクニック」

「サブテクニック」では、前述の「攻撃手法／テクニック」よりもより詳細な説明となります。たとえば、「Account Manipulation」という手法では、4つの異なるサブテクニックが関連付けられています。サブテクニックのIDはTxxx.yyyの形式で採番されており、ここで、Txxxはテクニック全体を表し、yyyは数字を表します。

Appendixでは、すべての「戦術」と「攻撃手法」を備えたMITRE ATT＆CKフレームワークが記載されています。

共通知識（Common Knowledge）

マトリクスには、攻撃者が組織のネットワークを侵害するために過去に使用したデータやその具体的な手順なども記載されています。これらのナレッジは、実際に行われた攻撃の調査、つまり、歴代の攻撃者たちが実行した実際の攻撃手法やサブテクニックの例となります。また、同ナレッジ内に記載されている情報としては、それらの攻撃手法やサブテクニックを実際に実行した世界中の名だたる脅威グループに関する情報も含まれます。

このフレームワークでは、企業組織が各攻撃手法またはサブテクニックに対して、防御対策を講じる上で、採用できるいくつかの「検出手段（Detection）」および「軽減戦略（Mitigation）」についても解説しています。

MITRE ATT&CKフレームワークの掘り下げ

大概のサイバー攻撃の軌跡は、MITRE ATT＆CKフレームワークでマッピングすることができます。前述のオンラインアパレルショップへのサイバー攻撃例を基に解説していきます。

上記のようなシナリオでは、攻撃者は次のような流れで攻撃を仕掛けてくるであろうと想定されます。

- EC（Eコマース）のトランザクション処理を担当するメインサーバーを発見するために**偵察（TA0043）**を行います。また、最初に特定の従業員との"信頼関係"を築くことで、フィッシングを通じた「被害者のネットワーク情報を収集」が可能になります。これは、攻撃者自身がマーケティング戦略としてターゲティングされる所謂オンラインペルソナに成り済ますことで、従業員のなかでも特に騙されやすい潜在的な攻撃対象者に信じてもらう、といったような方法で成功する場合が多いです。
- メールサーバーを保護するファイアウォールをこっそり通過する**防御回避（TA0005）**です。攻撃者がログを改ざんしたり、セキュリティオペレーションセンター（SOC）チームへの侵入検知に使われるしきい値などを変更したりすることはよくあります。この手の攻撃手法は、「Indicator removal on host」と呼ばれます。
- ネットワークへの「**初期アクセス（TA0001）**」の段階では、騙されやすい従業員にフィッシングメールのリンクをクリックするようにしむけることです。これにより、マルウェアをダウンロードして攻撃対象のシステムにインストール（実行）させることができます。
- 侵入先のコンピュータと攻撃者のシステムの間に通信チャネルが確立されている場合、攻撃者はシステムをリモートでコントロールしようとします。これは「**C&C（TA0011）**」チャネルと呼ばれ、このチャネル内の通信は暗号化されることがあるため、セキュリティチームは攻撃者のアクションを解読できません。攻撃者は、ネットワーク内の他のシステムに対してもコマンドを送ることで、攻撃者側のシステムとの通信チャネルを確立しようとします。現在侵害されているシステム（ボットネットとして機能）は、正当な顧客の要求を模倣した、複数の要求を送信することができます。これらは、サーバーをクラッシュさせるほどの、圧倒的な数を一挙に送信することができます。
- **インパクト（TA0040）**では、"Endpoint DoS"攻撃といわれるものが存在し、組織にとって重要となる情報保証の１つ「可用性」を破壊するか、又はビジネスの運営や運用プロセスを操作することによってデータの整合性を損なおうとします。この目的を達成するために起用される攻撃手法として、データの破壊または改ざんが含まれるため、ビジネスに多大なる影響を与えかねません。

PRE-ATT&CKマトリクス

PRE-ATT＆CKマトリクスでは、前述のATT＆CKマトリクスにて記載されている、攻撃者がネットワークへ侵入して情報を盗み出すまでの一連の流れが始まる前段階を示しています。

PRE-ATT＆CKでは、被害者のネットワークインフラに関する情報収集を徹底する段階的な目標や戦術に関する説明が成されます。攻撃者がネットワークの最初の偵察を実行し、攻撃を行うための準備リソースを開発するための手法についてより詳しく説明しています（ATT＆CKマトリックスの最初の2つの戦術）。図2は、潜在的な攻撃対象となりうるネットワークについて偵察している攻撃者の図となります。

図２：攻撃対象のネットワークを偵察し、IPアドレスやユーザーリスト、サブネットマスクなどを探索

Pre-ATT＆CKフェーズに記載されているマトリクスの注目すべき点としては、各段階的戦略に紐づく緩和戦略（"mitigation"の箇所）となります。その中でも従業員向けのトレーニングいった先制措置や、組織が実装する必要のある効果的なインシデント対応などのセキュリティ手順に重点を置いた解説が、各戦術毎になされています。

Pre-ATT＆CKフェーズでは、攻撃者がどのように攻撃態勢を整え、また逆にSOCチームがどのように攻撃者たちの目標を予測して、その証跡を辿れるようにすべきかについても解説がなされています。 Pre-ATT＆CKマトリクスの5つの顕著な特徴は次のとおりです。

- **優先度の定義とターゲット決め**：この段階では、攻撃者たちが望む攻撃による社会的ないしは経済的効果であるとか、彼らが狙うであろう企業組織についてを解説しています。企業組織へ侵入しようとする攻撃者は、情報を盗んだり改ざんしたりすることを目的としたり、サーバークラッシュを引き起こして組織活動を中断させたりすると想定されます。

- **情報収集**：攻撃者は、攻撃を開始する前に、アクセスしやすそうなアクセスポイントについて把握するために、被害者のネットワークに関する情報を収集します。

- **弱点の特定**：攻撃者はターゲットについて徹底的な調査を行い、悪用できるネットワークの脆弱性を見つけ出します。

- **設置作業**：これには、攻撃者が攻撃対象のネットワーク上で悪意のあるアクティビティを実行するソフトウェアをディスパッチしたり、ソーシャルエンジニアリングを行うことなどが含まれます。

- **下地作り**：攻撃者は、攻撃対象の脆弱性に合わせた攻撃能力の開発や強化に取り組みます。また、被害者のネットワークでより広い範囲で感染を拡大させ、ネットワークに身をひそめることで、ハイブリッド攻撃を実行しようとします。

PRE-ATT&CKフレームワークでは、ネットワークを破壊する可能性のある攻撃を阻止するための運用の準備にも役立ちます。企業組織は、ソーシャルエンジニアリングの釣り餌テストや、脆弱性スキャンによる潜在的な弱点に対する評価などを利用して、事前に弱点を特定しておく必要があります。これにより、従業員へのセキュリティトレーニングの機会を増やすことが出来ます。組織としては、攻撃者の侵入箇所として機能するかもしれないネットワーク上のコンポーネントにも注意して置く必要があります。組織における効果的なリスク評価は、ネットワークの抜け穴と保護するべき資産の特定にも役に立ちます。 SOCアナリストは、アラートを設定して潜在するリスクを監視しておくことにより、ネットワーク上の疑わしいソフトウェアのインストールを早期検知できるようになります。さらに、行動分析ツールを使用することで、"通常の"アクティビティのベースラインを決めることができ、それに逸脱する異常なネットワークアクティビティを特定することが可能になります。

さいごに

効果的なSIEMソリューションは、攻撃者による異常な動作を検出し、ネットワーク全体で発生している一見無関係に見えるイベントを相関的に分析し、攻撃を封じ込めるための予備的緩和策を可能にしてくれます。Log360で、これらすべてを1つのコンソール上で行えるので、1つのアラートも見逃すことなく、ネットワーク上で発生している"すべて"を監視できます。

ManageEngine
Log360

概要資料ダウンロード

評価版ダウンロード

【第二部】
MITRE ATT&CK
−ManageEngine Log360で実現する防御対策編−

資料ダウンロード

ー関連資料ー

MITRE ATT&CK実装で
APT攻撃検知するには
ユースケース編

資料ダウンロード

SIEMソリューションで実践する
脅威インテリジェンス

資料ダウンロード

巧妙化するサイバー攻撃の現状と
機械学習を活用したソリューション
「UEBA」

資料ダウンロード

セキュリティ対策やコンプライアンス準拠に関する人気資料一覧はこちら

引用

1. Purplesec, "2021 Cyber Security Statistics: The Ultimate List of Stats, Data &Trends," Purplesec, 2021, https://purplesec.us/resources/cyber-security-statistics/
2. Ibid.
3. The MITRE Corporation, "MITRE ATT&CK," MITRE, 2021, https://attack.mitre.org/.
4. The MITRE Corporation, "Enterprise Tactics," MITRE, 2021, https://attack.mitre.org/tactics/enterprise/.

MITRE ATT&CK 概要説明編

2021年11月発行

本製品に関するお問い合わせ
ゾーホージャパン株式会社ManageEngine事業部
〒2220012 事業部神奈川県横浜市西区みなとみらい三丁目 6 番1 号みなとみらいセンタービル

Log360 製品ページ：https://www.manageengine.jp/products/Log360/
ホームページ：https://www.manageengine.jp/

ZJMR20211126871