MITRE ATT&CK の利用によるランサムウェアからの保護 - 持ち出されてからでは遅い

はじめに

サイバーセキュリティ業界によれば、ランサムウェアが急増し、ランサムウェア攻撃に起因する混乱は長期化しています。ランサムウェアの多くはマルウェア・ファミリの技術的な詳細と分類が明らかになっていますが、この脅威のネットワーク通信の側面に関する包括的な議論はまだ行われていません。

第一に、ランサムウェアはエンドポイント上でローカルに実行されるため、ネットワークは重要でないと思われている可能性があります。しかし、ネットワーク・トラフィックでこのアクティビティの初期兆候を捉えることができるので、大きな被害が出る前に攻撃を妨げる時間ができます。

本ホワイトペーパーでは、幅広い顧客環境に展開された Arista NDR プラットフォームが検出した兆候を基に、ランサムウェア脅威アクターに対するネットワーク脅威検知で何をどのように探すべきかを説明します。また、このガイダンスを MITRE ATT&CK のフレームワークにマッピングします。

ランサムウェアの簡単な歴史

ランサムウェアは、防御することが困難な攻撃の 1 つであり続けています。ランサムウェアは、被害者をだましたり恐喝したりしようとする高度なアクターや、高度に組織化されたサイバー犯罪に利用されています。2021 年の Gartner の推計では、ランサムウェアに関する規制があるのは世界各国の政府の 1%にすぎませんが、この割合は 2025 年までに 30%に増加すると予測されています。

ランサムウェアはしばらく前から存在していますが、2021 年にはランサムウェアによる影響がかなり大きくなり、範囲も広がりました。IDC の「2021 Ransomeware Study」によれば、2021 年には世界中の組織の約 37%が何らかの形でランサムウェア攻撃の被害を受けたと回答しています。セキュリティ・ベンダーの BeyondTrust は、攻撃者がさらにパーソナライズされた攻撃を実行しようとするため、2022 年にはランサムウェアによる恐喝が 2 倍になると予測しました。その結果、ランサムウェア攻撃を食い止めるため、世界中の組織と政府が適切な対応策の導入を開始しています。

---

https://www.idc.com/getdoc.jsp?containerId=US48093721

https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions

Ransomware as a Service

アフィリエイトがランサムウェア・オペレーターに金を払って攻撃を実行させるという、この 2～3 年の新しいトレンドにより、現在では組織を標的にして有害な行為をするアクターの数が増加しています。このようなサービス・キットはわずかな金額で入手でき、組織の攻撃対象領域をさらに広げます。

ランサムウェアの防御策と MITRE ATT&CK フレームワークの対応付け

持ち出しや暗号化が行われる前には、複数の早期兆候があります。ほとんどの場合、そのような早期兆候からランサムウェアが爆発的に広がるまで 3 日間かかることが調査から判明しています。ご想像のとおり、非常に重要な 3 日間に介入することで、被害をかなり封じ込めることができます。

では、このように微弱だけれど重要な早期兆候をセキュリティ・チームが見つけるにはどうすればよいでしょうか。アリスタの経験では、エンドポイント・セキュリティ検出・対応（EDR）を導入している組織もありますが、ログ記録のレベルが適切な組織はわずかです。EDR、ログ記録、ネットワーク監視（NDR）を組み合わせれば、このような脅威を完全に可視化できます。残念ながら、たいていの場合、組織がネットワークを監視することは困難なため、ランサムウェア・アクターの観測から明らかな早期インジケーターの多くが見逃されています。アリスタはこのようなインジケーターを共有して、早期の検出からメリットを得られるようにしています。さらに、MITRE のカテゴリ別に分類して、情報を活用できるようにしました。

ネットワークの初期アクセスを見つける

ランサムウェア・アクターには、フィッシングの添付ファイルとリンク、サプライチェーン攻撃、Microsoft のリモート・デスクトップ・プロトコル（RDP）などの外部公開されているリモート・アクセス、有効なアカウントを通じたアクセスなどの初期アクセス・ベクトルがあります。これらはすべて、トラフィック全体にわたるネットワーク脅威検知時に発見できます。さらに、これがアクターによる最も早い時期の環境への侵入を表していることを考えると、このような初期アクセスの検出は、組織が影響を大幅に緩和するための最善策です。

以下のインフォグラフィックは本ペーパー全体で使用するフォーマットです。グラフィックの最初の列は、MITRE ATT&CK のカテゴリを表しています。次の列は、実際の攻撃に使われているランサムウェアで観測された、具体的な MITRE の手法（と ID）です。最後に、ネットワーク脅威検知プロセスの促進に役立つ早期兆候のリストを示します。

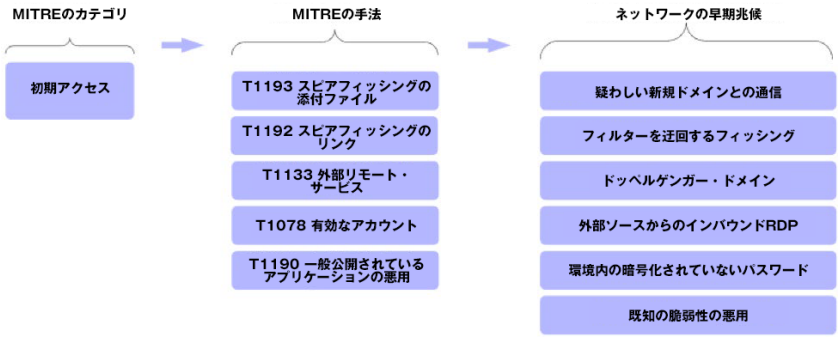

図 1：攻撃者によるネットワークの初期アクセス

https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

MITRE の手法を基に、推奨事項を以下に示します。

フィッシング手法

ネットワーク・アナリストはまずインターネット宛てのトラフィックを調べ、以前は見られなかったドメインを探します。もう 1 つの役に立つ情報源は、ユーザーの設定した情報が不正なチャネルに送信された可能性があるドメインです。最後に、うまくいけば既存のネットワーク・セキュリティ・ツールが既にフラグを立てているはずの既知の Maze IOC が多数あるので、これらを探すのもいいでしょう。実際、ネームサーバーやレジスタなどの基盤となるドメイン・インフラストラクチャに基づく検知で、ボーナス・ポイントを獲得できます。

ドッペルゲンガー・ドメイン

フィッシング手法を発展させて、ネットワークから環境内のドッペルゲンガー・ドメインの利用を把握できます。理想としては、使用されている最も一般的な組織やサードパーティのドメインや、Alexa Top 500 のような世界的に人気のあるドメインのタイポ・スクワッティングをセキュリティ・チームが探すべきです。

インバウンド RDP

すべてのインバウンド・リモート・アクセス・プロトコル接続や、スキャニング・アクティビティまたはブルートフォース・アクティビティの証拠をモニタリングすることが重要です。さらに、外部公開されていることが予期される全ユーザー・アカウントのリストや、これらのアカウントのネットワーク上でのアクティビティと、このアクティビティを比較できます。

暴露されているパスワードとパスワード・ストア

最もシンプルな形としては、SMB、FTP、HTTP などのプロトコルによる内部および外部のデバイスへの接続をモニタリングして、パスワード・ファイル・ストア、転送中の平文パスワード、URI やトラフィック・ペイロード内の HTTP Basic 認証、Base64 などの難読化されたパスワードを探します。これらはすべて、弱いパスワードをセキュアでない認証方法と組み合わせて使用または保存しているシステムやプロセスを発見するのに役立ちます。見つかったものは、修復または少なくとも何らかの補完コントロールの適用を検討する必要があります。

既知の脆弱性

通常は、悪用可能なデバイスとバージョンが環境内に存在するかどうかをまず特定してから、悪意あるアクティビティが成功したことがあるかどうかを検証することにより、ネットワーク全体にわたり脆弱性の悪用を検出できます。たとえば、Citrix NetScaler の脆弱性（CVE-2019-19781）4 の場合は、“//vpn/../t/../vpns/./cfg/smb.conf“などの URI 文字列とそれに続く HTTP POST リクエスト、さらに XML ファイルの HTTP GET を検知します。

サプライチェーン攻撃

攻撃者が製品または製品の配送メカニズムを操作して、その製品の利用者のところにあるデータやシステムに不正アクセスすることがあります。そのため、組織のソフトウェア・サプライチェーン全体を完全に可視化することが重要です。サプライチェーン攻撃は、ハードウェアやソフトウェアのあらゆる構成要素に影響を与えることができますが、実行権限を取得しようとしている攻撃者は、多くの場合、ソフトウェアの配布やチャネルのアップデートで正当なソフトウェアに悪意のある追加を行うことに重点を置いています。

図 2 は、Citrix NetScaler の脆弱性の悪用を特定するために URI 文字列を検知する例を示しています。

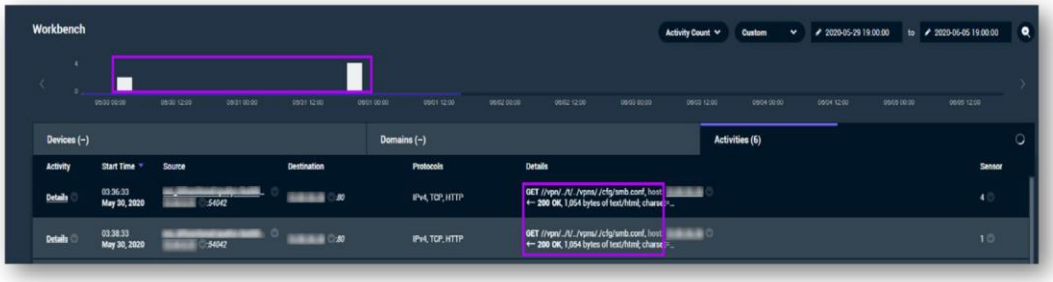

図 2：Citrix NetScaler の脆弱性（CVE-2019-19781）を悪用する試みの脅威検出

ネットワーク全体にわたり実行を見つける

次は、実行段階のランサムウェア・アクターに共通する特性を詳しく見ていきましょう。以下の図は、上記と同じ規則で、ユーザーがだまされてフィッシングのリンクや添付ファイルをクリックしたり、PsExec など特定のツールが環境内で使用されるといった一般的な早期兆候を表したものです。

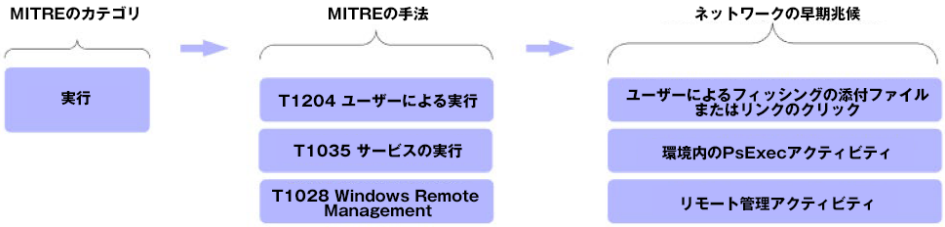

図 3：実行段階の早期兆候

実行の検知によって、以下のものが発見されます。

フィッシング手法

このタイプのアクティビティを生じやすいユーザーを特定して、トラッキングすることができます。この種の情報は、フィッシング関連のトレーニングや、これまでにフィッシング攻撃の被害に遭ったことがあるユーザーの傾向のモニタリングを通じて収集できます。それに加えて、初期アクセスのセクションで説明したように、疑わしい接続のモニタリングと検知を行うことが重要です。要求ヘッダーを調べて、電子メール・フィルタを迂回して攻撃者のインフラストラクチャにアクセスした可能性がある、疑わしいフィッシング・ドメインを特定してください。さらに、データのダウンロードの有無とその量を検証することができます。

PsExec の使用

PsExec は、いくつかの特徴的なネットワーク・フィンガープリントを残します。最もシンプルな形としては、SMB 全体にわたり PsExec などのファイル名を検知します。しかし、この方法が簡単に回避できることは明らかなので、セキュリティ・チームはより洗練された手法を使うといいでしょう。たとえば、PsExec を使用してコンテンツを抽出した後、別のデバイス上で SMB 経由のファイル入出力（IO）を実行するなど、連鎖して発生するアクティビティを探すことができます。scshell など他のツールでも使用される、基盤となる手法を探すことも重要です。

リモート管理

SVCCTL サービスに接続後、CREATE、READ、WRITE、CLOSE といったアクションを実行しているデバイスを調べて、敵対的なリモート管理の可能性を特定することができます。さらに、このリストをフィルタリングして、正当なビジネス・プロセスの一部であり、動作が予期されている既知の正常なシステムを除外できます。

---

https://awakesecurity.com/blog/citrix-gateway-vulnerability-cve-2019-19781-analysis/

永続化

ランサムウェアを使う攻撃者は、インターネットに公開されているシステム上の Web シェルなどの一般的な手法や、環境内で取得した有効なアカウントを利用します。攻撃者の足がかりが永続化されると、影響を緩和することが次第に困難になり始めます。Web シェル・アクティビティや、不正アクセスされる可能性があるアカウントは、多くの場合は重大な影響が生じる前に、ネットワーク上で確実に特定できます。

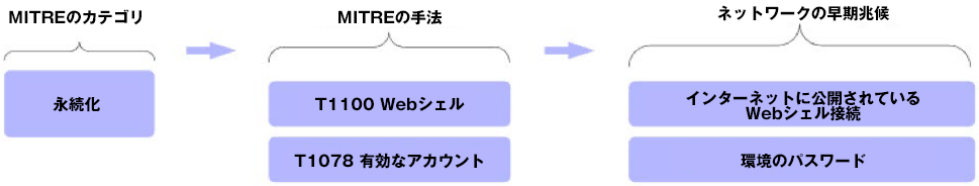

図 4：攻撃者が永続的な足がかりを築く方法

永続化手法の検知によって、以下のものを把握できます。

Web シェル

Web シェルの検出は少々複雑で、トラフィック全体にわたる高度なモニタリングや脅威検出が必要な場合があります。まず、外部ソースから外部公開されているデバイスへのやや珍しいデバイス・アクティビティ接続（変則的なポートやブラウザ・ユーザー・エージェントなど）を検知します。さらに、HTTP リクエストに成功している、一般的でないデバイス接続を特定します。この接続はスクリプト・アクティビティと同じように見え、他の既知の Web サーバーなどに比べ、そのデバイスへの接続数が限られています。

KeePass ストア

Maze アクターも KeePass ファイルを探します。これは重要な先行インジケーターです。攻撃者は暗号化されていないパスワードを探すため、セキュリティ・チームにとってもこの動作を検知することは不可欠です。たとえば、環境内のすべての SMB 共有で URI やパスワード関連ドキュメントを調べることによって、攻撃者によるパスワード・ストアの探査を検知します。これらのファイルの読み取りとコピーを伴うアクティビティに特に注意することが重要です。動作が外れ値である場合は、このアクティビティに関与しているユーザー・アカウントを特に詳細に調べることができます。

図 5 は、このような動作を検知した 2 つの例を示しています。ファイナンスの KeePass ファイルとデータベースの KeePass ファイル・ストアが、システム・ドライブからコピーされています。

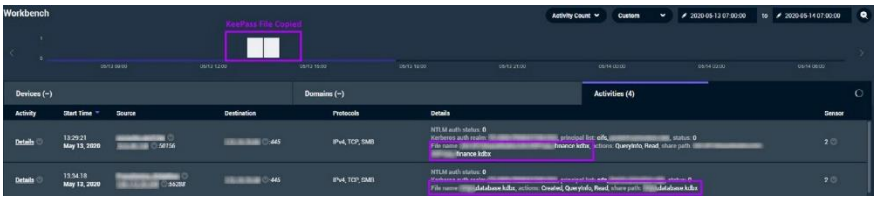

図 5：パスワード・ストアを読み取ってコピーする試みの脅威検出

新しい特権アクティビティ

攻撃者がより高いレベルのアクセス権を取得すると、環境内でさらなるアクティビティの兆候を見つけることが大幅に難しくなります。たとえば、特権アクティビティなど永続化のために使用される手法は、ネットワーク上で捕捉しない限り、多くの場合は検出できなくなります。これらが権限昇格手法としてどのように現れるかを詳しく説明します。

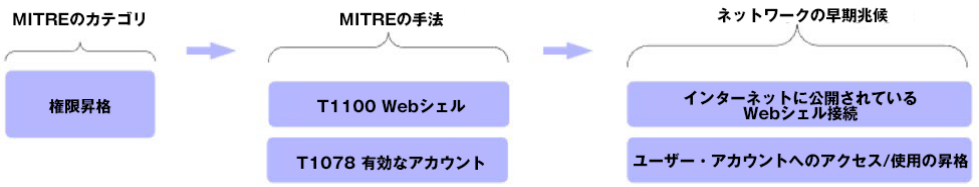

図 6：エンタープライズ・ネットワークへの特権アクセスの利用

Web シェル

永続化セクションで前述したとおり、Web シェルを発見するには複数のデータ・ポイントを統合する必要があります。このプロセスを分離し、高速化するには、外部公開されている Web とゲートウェイ・システムに焦点を絞ることが役立つ可能性があります。

アクセス権の昇格

暗号化されていないパスワードの保管に関して、ほぼすべての組織でハイジーン（衛生状態）は貧弱です。攻撃者は 1 つの環境全体でパスワード・ファイルを探すため、脅威ハンターはネットワーク・セキュリティ・ツールを利用して、SMB によるパスワード・ファイルへのアクセスとリモート・コピーをモニタリングできます。これを実現するには、ネットワークの SMB トラフィックで doc、txt、xls、docx、xlsx、csv、jpg など一般的な拡張子が付いている“passw”という語のバリエーションを探査します。

このデータを利用すると、ハイジーンの問題を検出して解消したり、このようなパスワードをすべてセキュアなパスワード・ストレージに格納するよう求めて、有効なアカウントへの大規模アクセスを防いだりすることができます。

図 7 では、URL にスクリプトを含む Apache Tomcat Web シェル・アクティビティが発見されています。

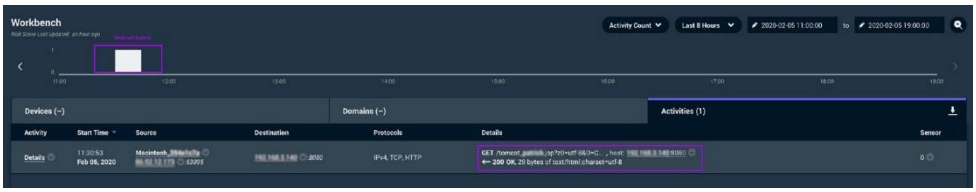

図 7：ネットワーク上の Web シェルの脅威検出

防衛回避の兆候

ファイルや、そのファイルからさまざまなシステムへのアクセスを隠すため、攻撃者はファイルの名前を変更し、エンコーディングし、アーカイブし、他のメカニズムを使用して証拠を残さないようにします。このような手法を用いたとしても、早期兆候が見られ、検出を回避しようとする攻撃者を検出できます。回避の試みは、それ自体が非常に疑わしいとアリスタは考えています。

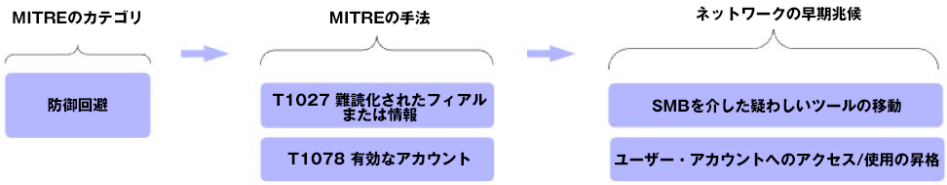

図 8：検出を回避しようとする攻撃者の早期兆候

一般的なネットワーク脅威検知アプローチには以下のものがあります。

難読化ツールなど

攻撃者は環境へのアクセスを増やそうと試みるので、アクターは共有間でさまざまなツールをコピーすることがあります。場合によっては、すべての SMB ファイル・アクティビティにわたり既知の攻撃ツールを検知することで、このようなアクティビティを検出できます。証明書発行者名で特定のツールを探したり、攻撃ツールの使用ポートと組み合わせて未知のプロトコルによる TCP セッションを検出したり、アクティビティがほとんどない隔離されたデバイス（問題のツールやプロトコルを使用しているように見える少数のアクティビティを実行している少数のデバイスなど）を検出することもできます。

新規アカウントの作成

多くの場合、正常なアクティビティに紛れ込むためのメカニズムとして、攻撃者は新規ユーザー・アカウントも作成します。このような動作は、DCERPC ネットワーク・トラフィックで SAMR UUID や、操作番号 12 の SamrCreateUserInDomain および操作番号 50 の SamrCreateUser2InDomain などのユーザー作成アクションを探す脅威検出で発見できます。

図 9 は、新規ユーザー・アカウント作成がネットワーク・トラフィックにどのように現れるかという例を示しています。このアクションは、ワークステーションからドメイン・コントローラではない別のデバイス宛てに net use コマンドまたは類似のコマンドを使用して実行された可能性があります。

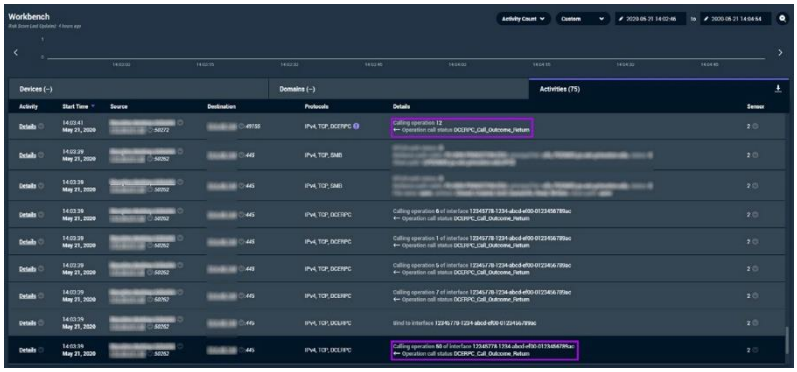

図 9：ネットワークから観測されるユーザー・アカウント作成

認証情報アクセスの早期兆候

アカウントのブルートフォースなど、認証情報の悪用の検知は早期兆候の 1 つです。さらに、認証情報へのアクセスを制限または制約するために、いくつかの防御手段を導入できます。脅威ハンターは、特定の攻撃ツールの使用、認証情報の悪用の試み、弱いパスワード、セキュアでないパスワード・ストレージなど、ネットワーク・ハイジーンの状況認識を提供することによって、このプロセスを実現できます。

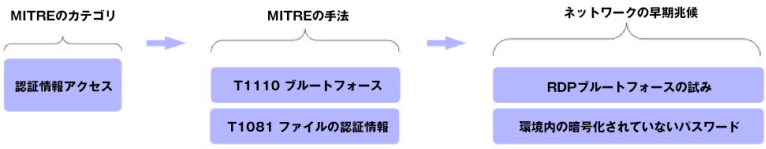

図 10：認証情報の悪用の兆候

MITRE のマッピングでわかるように、以下のいずれかを利用して、環境内の攻撃者の兆候を検出できます。

RDP ブルートフォース

予期される脆弱性スキャナや他の類似サービスを除外した後、RDP ネットワーク・アクティビティを検知し、頻度分析を利用して、暴露されているポート上でのブルートフォース攻撃を特定することができます。

たとえば、図 11 は、RDP ブルートフォースがネットワーク・アクティビティのタイムライン上でどのように突出しているか、どのように悪意を評価するかを示しています。

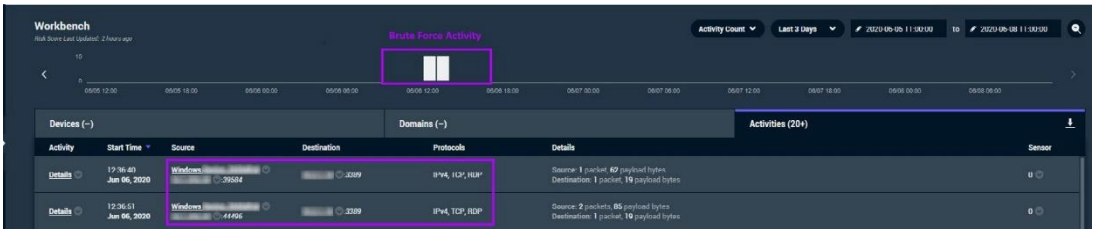

図 11：RDP ブルートフォース・アクティビティの脅威検出

ファイル内にある、またはツールによって抽出された認証情報

ここまでのセクションでは、パスワードを格納している KeePass ファイルや他のファイルの使用を検知したり、ネットワーク上で SMB などのプロトコル経由でこれらのファイルをコピーしているユーザーを検出する方法について、広く説明してきました。さらに、重要なシステムやファイル共有からのパスワードのコピーにツールが使われる場合は、潜在的な難読化ツール・アクティビティや、PsExec や PowerShell の使用を脅威ハンターが特定する方法も説明しました。予防のための重要な推奨事項は、前もってパスワード・ファイルの問題に対処することです。

探索の兆候はいたるところに

ランサムウェア攻撃者の内部偵察活動を調べると、膨大な数と種類の探索手法が見つかります。列挙アプローチや、特定のツールおよびいくつかの収集手法の利用が、このカテゴリに分類されます。それぞれが独自の証拠を残すので、持ち出しや暗号化が行われる前に特定できます。

ランサムウェア攻撃者の内部偵察活動を調べると、膨大な数と種類の探索手法が見つかります。列挙アプローチや、特定のツールおよびいくつかの収集手法の利用が、このカテゴリに分類されます。それぞれが独自の証拠を残すので、持ち出しや暗号化が行われる前に特定できます。

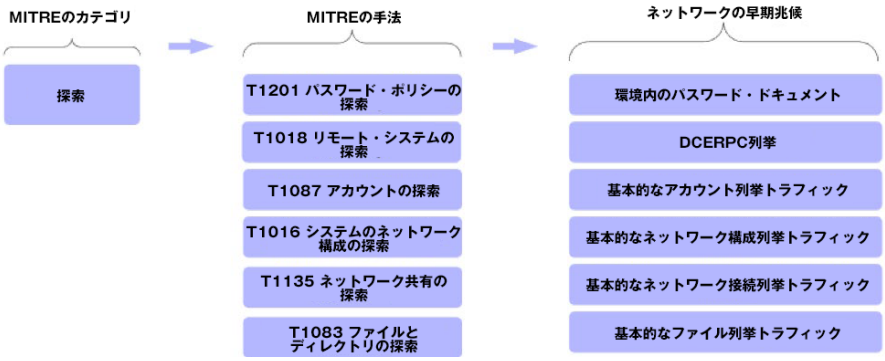

図 12：持ち出しや暗号化の前にランサムウェアを発見するための兆候

以下の例に示すように、探索アクティビティの早期兆候は多数あります。

パスワード・ポリシー・ドキュメント

パスワード・ストアを見つける方法と同様に、脅威検出で環境内のパスワード・ポリシー・ドキュメントを特定し、SMB 経由でコピーされているドキュメントを探すことができます。また、この情報をダウンロードしているデバイスが初めてネットワーク上に出現したのはいつかなど、他の情報と相互参照することもできます。これは、ドキュメントをダウンロードする可能性がある新入社員を除外する場合などに役立ちます。

DCERPC のパスワード・ポリシー列挙

パスワード・ポリシーの特定には、他の列挙手法やハーベスティング手法も利用できます。たとえば、すべての DCERPC 接続で SMB 経由の操作番号 44（SamrGetUserDomainPasswordInformation メソッド）を探し、脅威を検出することができます。

DCERPC のコンピューター名列挙

探索の一環として、攻撃者は環境の詳細なマップを作成して重要なシステムを探します。その方法の 1 つがデバイス名の列挙です。ネットワーク脅威ハンターは、DCERPC のトラフィックで“wkssvc”という文字列と操作番号 30（NetrEnumerateComputerNames メソッド）を探査して、攻撃者を探すことができます。

アカウント列挙

列挙を実行しているユーザーを検出する他の方法と同様に、以下の動作を検知することもできます。

- 操作番号 11 LsarEnumerateAccounts メソッド
- 操作番号 35 LsarEnumerateAccountsWithUserRight メソッド
- 操作番号 36 LsarEnumerateAccountRights メソッド

ネットワーク構成列挙

以下へのネットワーク接続を探すことによって、ネットワーク構成の詳細なマップを作成している攻撃者を検知できます。

- ポートの特定に操作番号 26 の NetrServerTransportEnum メソッドを使用している、RPC インターフェイス UUID が SRVSVC のプロトコル
- ワークステーションのポートに操作番号 5 の NetrWkstaTransportEnum メソッドを使用している、RPC インターフェイス UUID が WKSSVC のプロトコル

ファイル列挙

Maze などのランサムウェアを使用する攻撃者は、ファイルとディレクトリの一覧を取得して、データの収集と暗号化に役立てます。DCERPC を利用した検知で、具体的には操作番号 9（NetrFileEnum メソッド）を使用している“srvsvc”への RPC インターフェイス呼び出しを特定することによって、このような敵対的動作も特定できます。

図 13 は、攻撃者と脅威ハンターの双方が、Word ファイルやテキスト・ファイル内の個人パスワードなど、さまざまなフォーマットの複数の平文パスワード・ストアを見つける方法を示したものです。また、データ・プロバイダーや Chrome/ブラウザ・システムに含まれるストアも見つけることができます。これらすべてを攻撃者から守らなければならないことは明らかです。

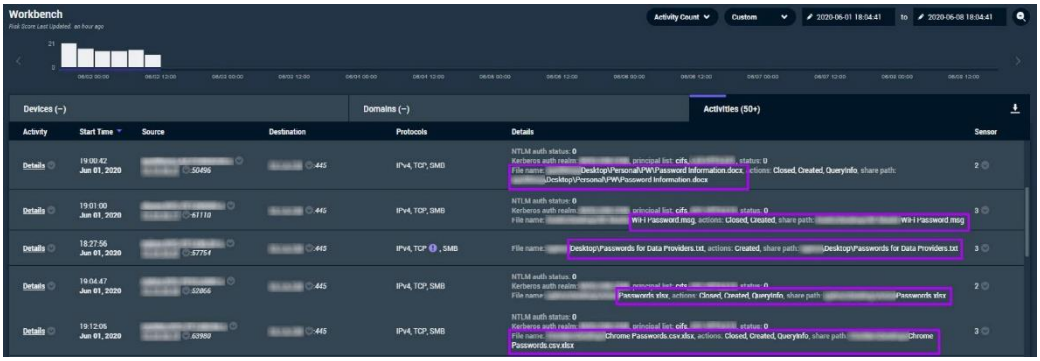

図 13：ネットワーク内のパスワード・ストア

水平展開の兆候

脅威アクターは水平展開手法を利用して環境を把握し、ネットワークを通じて広がります。これは、データを収集し、準備してから暗号化を実施する必要があるランサムウェアに特に当てはまります。Maze などのランサムウェアを使用するアクターは、正当な RDP セッションを乗っ取って多くのステージング・アクティビティを実行しているように見えますが、そのすべてが早期兆候を示します。

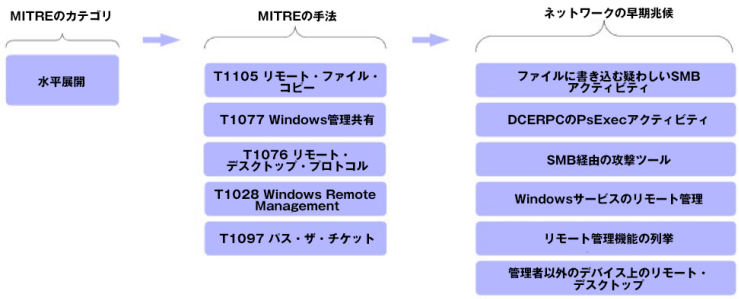

図 14：水平展開の兆候

ランサムウェア攻撃で観測される水平展開手法の多様さを考慮すると、以下の手法を複数利用して、環境内の脅威アクティビティを検出できます。

疑わしい SMB アクティビティ

たとえば、バッチ・ファイルやアーカイブ・ファイルへの複数の書き込みなど、一般的に暗号化の前に発生する疑わしいファイル・アクティビティが含まれます。bat、zip、7z などの一般的な Maze ファイル・タイプに関連付けられた書き込み回数のしきい値と外れ値分析に基づいて、このようなアクティビティを検知できます。

DCERPC の PsExec アクティビティ

DCERPC UUID 手法に関連するナレッジと操作番号の詳細を利用して、環境内での PsExec の使用を検知できます。

SMB による攻撃ツール

防衛回避の兆候のセクションで説明したとおり、アクターは共有間でさまざまなツールをコピーすることがあります。場合によっては、既知の攻撃ツールや、Mimikatz、PowerSploit/PowerView、tscon などの攻撃ツールを格納している可能性があるアーカイブについて、すべての SMB ファイル・アクティビティを調べ、このアクティビティを検出できます。検出の実行には、ネットワーク全体にわたり既知のファイル・ハッシュについてアクティビティを調べたり、正規表現（regex）パターンを使用したりします。

WinRM

初期アクセスのセクションで述べたように、SVCCTL サービスに接続するデバイスを調べることで、敵対的なリモート管理の可能性を検知できます。さらに、Microsoft WinRM Client ユーザー・エージェントを使用している HTTP POST リクエスト接続を検知することもできます。PowerShell と Cobalt のビーコンについても、同様のアクティビティを調べる価値があります。最後に、tscon のリモート・ハイジャック・セッションについては、以下のメソッドを使用していて、RPC インターフェイス UUID が SVCCTL のプロトコルを調べて、脅威を検出することができます。

- RCreateServiceW（操作番号 12）
- RCreateServiceA（操作番号 24）
- RCreateServiceWOW64A（操作番号 44）
- RCreateServiceWOW64（操作番号 45）

管理機能の列挙

操作番号 4 の inq_princ_name メソッドを使用していて、DCEPRC インターフェイス UUID が MGMT のプロトコルを調べることで、ネットワーク上のリモート管理機能を列挙している攻撃者を検知できます。

管理者以外のリモート・デスクトップ

ネットワークを利用して、リモート・デスクトップ（termsrv）アクティビティを効果的に探すことができます。その後、管理者以外のシステムに出現する動作について、見つかったアクティビティをフィルタリングします。この手法は、クライアント名や他の文字列値に基づくデバイスのフィルタリングに特定の命名規則を使用している組織にとって、特に効果があります。

たとえば、図 15 では、ユーザー・エージェント“Microsoft WinRM Client”を検知して、PowerShell のアクティビティを特定しています。

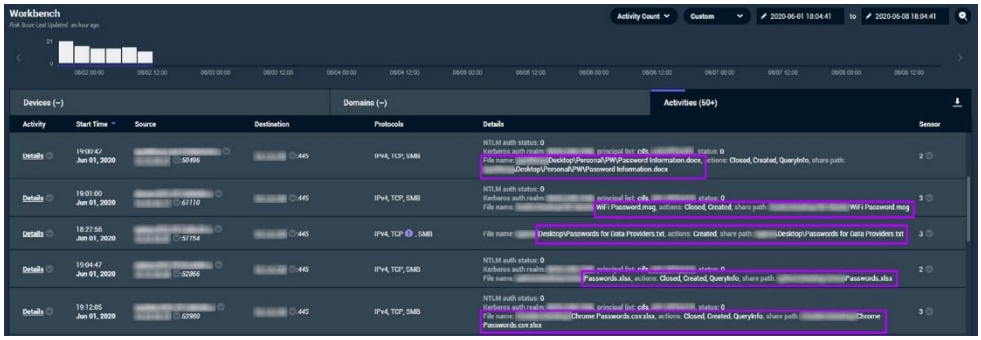

図 15：Windows Remote Management アクティビティの検知

収集して持ち出し

一般的に、データの収集は、環境の理解や、持ち出しの準備に利用されます。ランサムウェア・アクターは、ツールやバッチ・スクリプトを利用して情報を収集しています。そして、拡張子.7z または.exe を使ってこのデータを.batファイルやアーカイブにパッケージ化しますが、すべてネットワーク上に証拠が残ります。

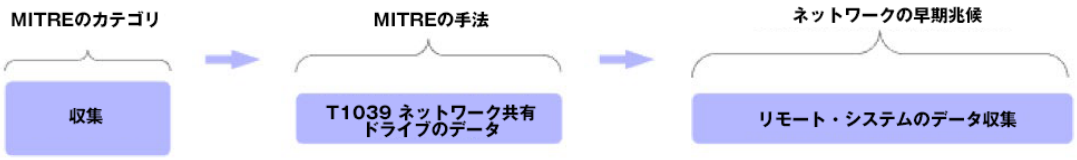

図 16:データ収集して持ち出し

一例として、ネットワーク上のランサムウェアと関連がある、同様の収集アクティビティを特定できます。

リモート・システムのデータ収集
バッチ・ファイルの SMB 書き込みアクティビティと、それに続く一般的なアーカイブ・ファイルの拡張子を使用したコピー・アクティビティを検知します。

C2 の兆候

多くの攻撃者は、一般的なポートやリモート・アクセス・ツールを使用して、コマンド＆コントロール（C2）アクティビティを獲得し、維持しようとします。ランサムウェア・アクターも同様です。アリスタは、このような標準的手法や、攻撃者のインフラストラクチャに接続する ICMP トンネルの証拠を観測してきました。

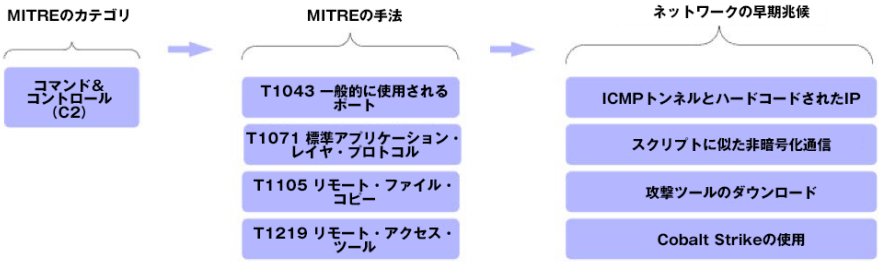

図 17:ランサムウェア攻撃者がコマンド＆コントロールを獲得する方法

C2 の早期兆候の例を以下に示します。

ICMP トンネルとハードコードされた IP
一部の C2 では、ICMP トンネリングなどトラフィック内のパターンによって、Maze アクターの正体が明らかになります。たとえば、このようなトンネルの接続先は、通常はハードコードされた IP です。ただし、プロキシ・デバイスとゲートウェイ・デバイスを除外して、ブラウザ以外からの HTTP トラフィックなどの変則的なトラフィック・パターンを検出する一方で、ICMP に限らずハードコードされた IP 接続を探査することもできます。

図 18 は、ICMP トンネル経由で C2 サイトに接触している Maze ランサムウェアの例を示しています。

図 18:コマンド＆コントロールのために Maze ランサムウェアが利用している ICMP トンネル

スクリプトに似た非暗号化通信

ネットワークを利用して、スクリプトに似たランダム化通信を効果的に特定することもできます。Maze は、このような通信をしばしばコマンド＆コントロール（C2）に利用します。一般的に、このような C2 は、他のネットワーク・アクティビティに比べて比較的珍しいものです。そのため、スクリプトによって作成されたように見えるドメインや IP へのリクエストを検知し、これらの HTTP リクエストを実行しているデバイスが 5 つ未満、同じユーザー・エージェントを持つデバイスが 20 未満など、特定の条件を共有することができます。

攻撃ツールのダウンロード

HTTP リクエスト内には攻撃ツールの証拠が残ります。多くの場合、Maze アクターは mini.zip をダウンロードします。脅威ハンターは、正規表現を利用して URI 内の文字列パターンを特定したり、探査にハッシュを利用したりすることができます。さらに、ハードコードされた IP や疑わしい可能性があるドメインからダウンロードされた特定のファイルのサイズとタイプを検知することもできます。

Cobalt Strike の使用

Cobalt Strike ビーコンと、“cobalt_uploads”などの Cobalt ディレクトリへの FTP も、実際の攻撃に使われている Maze アクターと関連があることが観測されています。Cobalt へのアップロードとダウンロードが行われる FTP ディレクトリの特定は、ネットワーク全体にわたる検知が可能なメカニズムの 1 つです。さらに、ビーコンとサーバーへのコールバックには特定のトラフィック・パターンがあり、サイト自体が IOC の役割を果たすことができます。

持ち出しを最小限に抑える

本ペーパーのタイトルからご想像のとおり、検知の重点を持ち出し段階に置く場合、攻撃サイクルは既に終盤であると考える人もいるでしょう。この段階では、公共の領域にある機密データの暴露のリスクは切迫しており、ネットワークの早期兆候の多くは見逃されてしまいました。しかし、影響を最小限に抑える機会はまだあります。

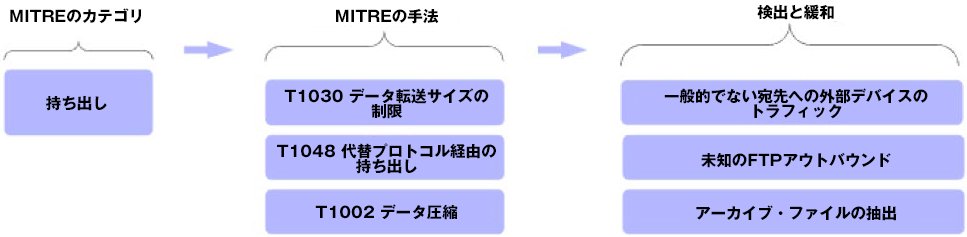

図 19：データ持ち出しの早期兆候

ランサムウェア・アクターは、いくつかの重要な持ち出し手法を使用します。以下に説明する一般的な手法を利用して、持ち出しを検出できます。

外部デバイスのトラフィック

3 つの効果的な手法を用いて、外部デバイスのトラフィックを検出することができます。その手法とは、外部の宛先への大規模な転送、有名なドメインへのブラウザ以外のトラフィックの使用、内部システムにデータをプッシュしているデバイスを探すことです。最後の手法は不思議に思えるかもしれませんが、多くの場合、持ち出しの前に外部デバイスへのデータのプッシュとステージングが観測されています。

未知の FTP アウトバウンド

攻撃ツールの検知と同様に、組織内での WinSCP の使用も探すことができます。また、すべての FTP 接続をすばやく調べて、限られた数のシステムからのみ発生している、一般的でない外部宛先向けであるなどの外れ値を特定することもできます。

アーカイブ・ファイルの抽出

アーカイブの持ち出しの脅威検出は、暗号化されたデータの持ち出しの検知に似ています。アナリストは、その環境について、ハードコードされた外部 IP アドレス、疑わしい IP アドレス、または一般的でない IP アドレスへのアーカイブのアップロードなど、特定のアクティビティを探します。

手遅れ - 封じ込めは最後の手段

この時点で、戦略は早期兆候から影響の封じ込めへと移ります。この時点で重点を置くのは、広がりを食い止め、被害を緩和することです。

図 20:ランサムウェアの影響の封じ込め

ネットワークで影響の検出に利用できる主なメカニズムには、以下のものがあります。

ファイル共有への過度の書き込み

通常、ランサムウェアの実行時には、短期間にアクティビティが連鎖して発生します。Maze で観測されるように、攻撃者は環境全体に一連のバッチ・スクリプトとテキスト・ファイルを展開します。SMB 全体にわたり、一連のアクティビティや、zip、doc、tmp、bat、txt などさまざまなファイル・タイプを探すことによって、このようなアクティビティや、同様の他のファイル共有への書き込みを検知できます。

SMB 経由での疑わしいファイル書き込み

通常、ランサムウェアによる書き込みが行われると、DECRYPT、encrypted、recover などの名前のファイルが作成されます。Maze の場合は、DECRYPT-FILES.html または DECRYPT-FILES.txt です。

ダウンロードと書き込みの組み合わせ

ランサムウェア攻撃者による利用を示すもう 1 つの重要な痕跡は、ファイルのすばやい取得と複数のホストへのプッシュです。特定のファイル拡張子を持つファイルの HTTP または他のプロトコルによるダウンロードに続き、ネットワーク内の複数のホストへの SMB 書き込みを検知することによって、ネットワークでこのようなアクティビティを検出できます。

まとめ

ランサムウェアが目の前に姿を現すというのは良いニュースではありません。しかし、規律あるネットワーク脅威検知とモニタリングを行えば、ライフサイクルのごく早い時期にランサムウェア攻撃を特定できます。早期兆候の多くはネットワーク上で可視化できるので、脅威ハンターはそのような兆候を特定して影響を緩和することが可能です。

アリスタネットワークスジャパン合同会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル　27F
Tel:03-3242-6401

西日本営業本部
〒530-0001　大阪市北区梅田 2-2　ヒルトンプラザウエストオフィスタワー　19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

www.arista.com/jp
ARISTA
2022 年 4 月 22 日

付録 A:リファレンス

- https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions
- https://www.crowdstrike.com/resources/reports/global-security-attitude-survey-2021/
- https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts#
- https://info.corvusinsurance.com/2021-corvus-risk-insights-index

付録 B:早見表

MITRE ATT&CK の戦術	MITRE ATT&CK の手法	検知対象
初期アクセス	T1193 スピアフィッシングの添付ファイル T1192 スピアフィッシングのリンク	• 以前見られなかった、または新規登録されたドメイン、珍しいレジスタ • 組織やパートナーのドメインや、Alexa Top 500 のドッペルゲンガー
	T1133 外部リモート・サービス	• 外部デバイスからのインバウンド RDP
	T1078 有効なアカウント	• SMB、FTP、HTTP により暴露されているパスワードやその他の平文の使用
	T1190 一般公開されているアプリケーションの悪用	• 既知の脆弱性の暴露と悪用
実行	T1204 ユーザーによる実行	• ユーザーからの疑わしい電子メール動作と関連するダウンロード
	T1035 サービスの実行	• PsExec を使用してシステム上のコンテンツを抽出後、別のシステム上で実行される SMB 経由のファイル IO
	T1028 Windows Remote Management	• 既知の正常なデバイスからの接続を除くリモート管理接続
永続化	T1100 Web シェル	• 外部接続からの珍しいアクティビティ接続(変則的なポートやユーザー・エージェントなど)
	T1078 有効なアカウント	• SMB または HTTP による KeePass ファイル・ストアのリモート・コピー
権限昇格	T1100 Web シェル	• 外部公開されている Web とゲートウェイ・システム上の Web シェル
	T1078 有効なアカウント	• SMB によるパスワード・ファイルのリモート・コピー(“passw”という名前のファイルなど)
防御回避	T1027 難読化されたフィアルまたは情報	• 使用ポート、証明書発行者名、または未知のプロトコルの通信で検知できる攻撃者ツール
	T1078 有効なアカウント	• ワークステーションや管理者以外が使用する他のデバイスからの新規アカウント作成
認証情報アクセス	T1110 ブルートフォース	• 既知のユーザー名のアカウントに対する RDP ブルートフォースの試み
	T1081 ファイルの認証情報	• 環境内の暗号化されていないパスワードとパスワード・ファイル

MITRE ATT&CK の戦術	MITRE ATT&CK の手法	検出対象
探索	T1201 パスワード・ポリシーの探索	• ファイル共有からパスワード・ポリシーをコピーしているデバイス • パスワード・ポリシーの列挙
	T1018 リモート・システムの探索 T1087 アカウントの探索 T1016 システムのネットワーク構成探索 T1135 ネットワーク共有の探索 T1083 ファイルとディレクトリの探索	• コンピューター名、アカウント、ネットワーク接続、ネットワーク構成、またはファイルの列挙
水平展開	T1105 リモート・ファイル・コピー T1077 Windows 管理共有	• 疑わしい SMB ファイル書き込みアクティビティ • PsExec の使用による攻撃ツールのコピーまたは他のシステムへのアクセス • SMB によりコピーされた攻撃ツール
	T1076 リモート・デスクトップ・プロトコル T1028 Windows Remote Management T1097 パス・ザ・チケット	• WinRM ユーザー・エージェントを使用する HTTP POST • リモート管理機能の列挙 • リモート・デスクトップ（termsrv）アクティビティを実行している管理者以外のデバイス
収集	T1039 ネットワーク共有ドライブのデータ	• 疑わしい、または一般的でないリモート・システムのデータ収集アクティビティ
コマンド＆コントロール（C2）	T1043 一般的に使用されるポート T1071 標準アプリケーション・レイヤ・プロトコル	• IP アドレスへの ICMP コールアウト • ブラウザ以外からの HTTP トラフィック • 珍しいデバイスからの HTTP スクリプトに似たリクエスト
	T1105 リモート・ファイル・コピー	• リモート・アクセス・ツールのダウンロード
	T1219 リモート・アクセス・ツール	• Cobalt Strike ビーコンと名前に Cobalt を含むディレクトリへの FTP
持ち出し	T1030 データ転送サイズの制限	• 一般的でない宛先への外部デバイスのトラフィック
	T1048：代替プロトコル経由の持ち出し	• 未知の FTP アウトバウンド
	T1002：データ圧縮	• アーカイブ・ファイルの抽出
影響	T1486：影響に関するデータ暗号化	• ファイル共有への過度の異常な書き込み • DECRYPT という語の使用など、SMB 経由での疑わしいファイル書き込み • ダウンロードとファイル書き込みの組み合わせ