ivanti

2023 サイバー戦略ツールキット ステークホルダーを説得する方法

サイバーセキュリティ戦略が重要である理由を情報セキュリティ部門以外の関係者に説明することで、予算確保を促す方法

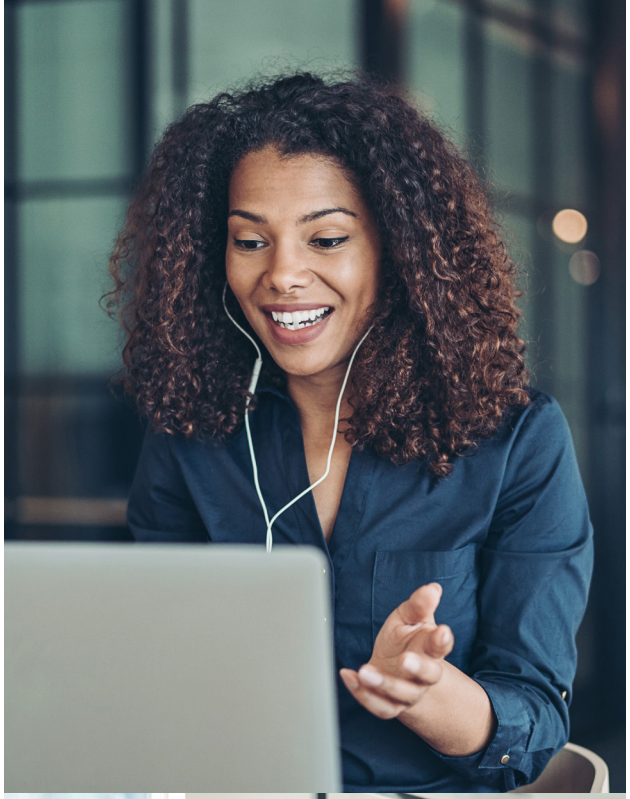
in collaboration with

CSW Cyber SecurityWorks

はじめに

本書をお読みいただき、誠にありがとうございます。

本書は、ご自身や組織のサイバー防衛戦略を誰もが理解し、予算確保を促せるようにサイバー防衛戦略の正当性を説明します。



本書は、次のようなこと要点で解説しています。

1. **情報セキュリティ部門以外の関係者に対して、2022年以降の主な脅威とその攻撃パターンについて、文脈に沿ってまとめ、**エンドユーザーがメディアで目にするパニックを引きおこすような見出しを、戦略的セキュリティ勧告に関連付けて説明しています。

2. **プロアクティブ（先を見据えた）**なセキュリティ対策が、どのように壊滅的な攻撃を阻止したかを示しています。破壊的な攻撃を未然に防ぐことができます。

3. すべてのステークホルダーとエンドユーザーが、何年も前からお願いしていることを実行し、コミットすることで、**重大な侵害や攻撃を防ぐ**ことができたと感じられるようにします。

私たちは、2023年に組織を安全に保つお手伝いをしたいと考えています。しかし、隔月でパニックに陥ったようなユーザーからの依頼が殺到するような「発生したインシデントにパッチを適用する」リアクティブ（反応的）なアプローチではありません。

そのようなアプローチは、チームを疲弊させてしまいます。

チームは疲弊しているのです。

代わりに、本書を最初のステップとして使い、 「何（とは）」 だけでなく、防衛戦略の背後にある 「理由（わけ）」 を、情報セキュリティ部門以外の人が理解できるように示すことができます。そうすれば、サイバー攻撃を事前に阻止するために必要な投資の下地を作ることができます。

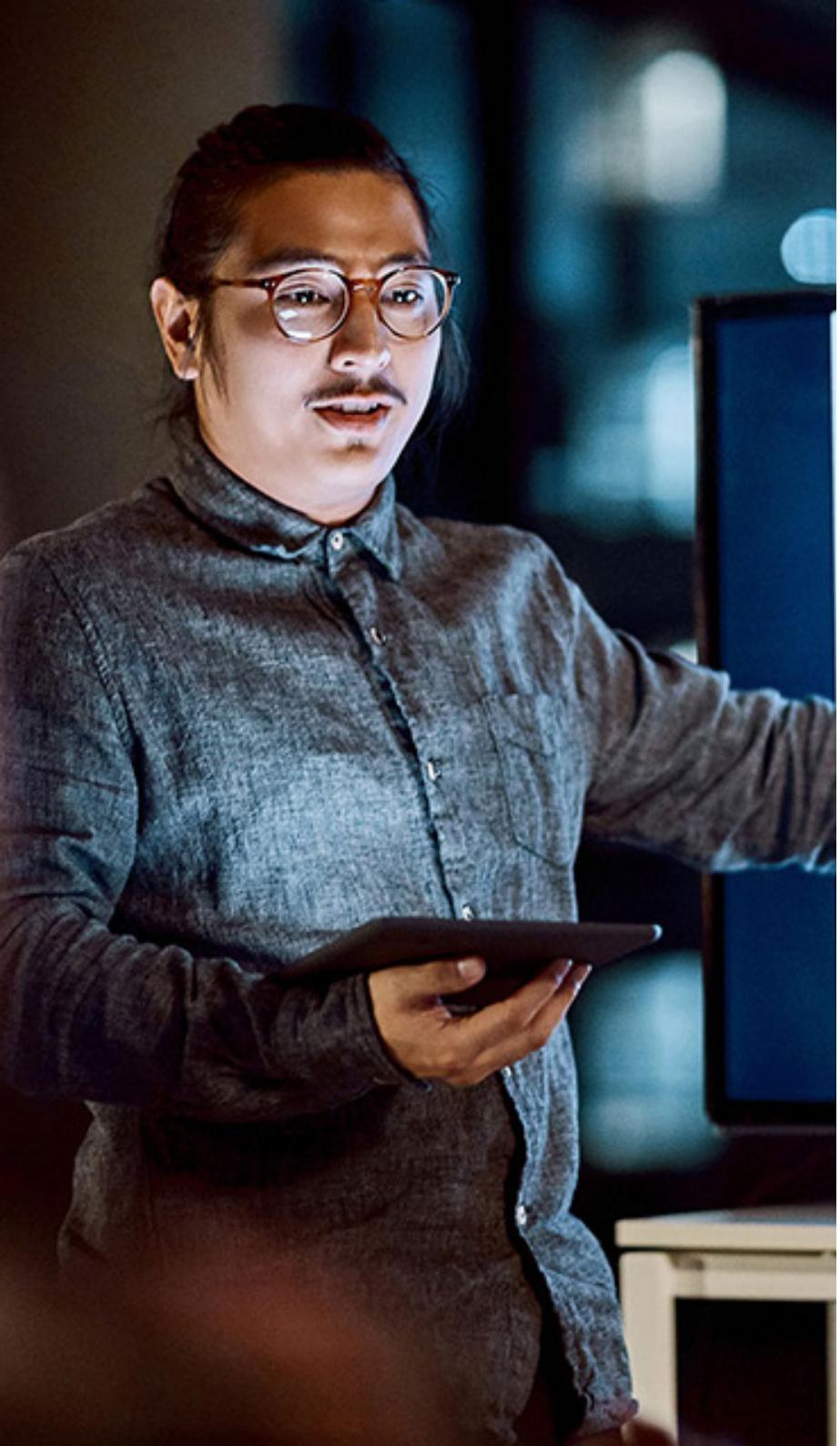
サイバー防御戦略「とは」だけではなく、その背景にある「理由」が大切です

皆様が最善の状況に置かれることを願っております。来年以降もお自身のチームが組織の安全を守るという重要な業務を遂行するために、必要なリソース、人員、時間を確保する上で本書が役に立てば嬉しい限りです。

ここでは、独自の動機や侵入スタイルを特徴としたさまざまなサイバー犯罪者に攻撃された、組織の実話を紹介し、**統計化**をします。

MITREの分析やCVEの重要度にとどまらず、「追加のセキュリティ」への小さな投資が、現実世界の壊滅的な攻撃を阻止するのに役立ったことを、情報セキュリティ部門の以外の人にも理解できる言語と形式でステークホルダーに示します。

数ヵ月の時間とリソース を追加することで、組織横断的なパッチや修復をテストし、通常の業務を中断することなく展開することができ、犯罪者がシステムを狙う前に対応できることを証明します。



目次

防御ディレクトリ:
従業員を武装し、チームに
リソースを割り当てる方法

ivanti CSW Cyber SecurityWorks

今後12ヵ月間、私たちがネットワークを守るために戦うことになる相手の話をする前に、どのように組織は防御を準備すべきかから始める必要があります。そして、それには大規模な侵害が起こる前に導入しておくべきツールや戦術が含まれます。

実際、これらの選択されたソリューションは、このツールキットで取り上げられたほぼすべての脅威アクターに対して、何らかの方法で防御することができます。

時間、経営陣の同意、リソースがあれば、チームが導入できる可能性のある防御メカニズムを全員が明確に理解した上で、これらの手法が2022年から最も流行した悪質なサイバー攻撃のいくつかをどこでどのように阻止できた可能性があるかを説明します。

各サイバー防御戦術には次の内容があります。

- ✓ 機能するまでの時間とコスト
- ✓ 防御ツールとは何を簡潔に説明
- ✓ 特定の種類のサイバー攻撃に対する防御にどのように役立つか説明
- ✓ 社内関係者からのよくある反対意見を克服し、会話を「なぜこれが必要なのか」から「どうすればこの費用を負担し、実施することができるのか」へ転換し、「従業員の武装」を促進

防御ディレクトリ:
従業員を武装し、チームに
リソースを割り当てる方法

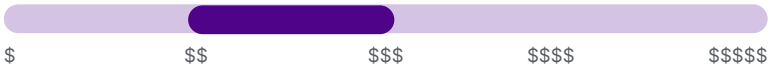
ivanti CSW Cyber SecurityWorks

セクション

フィッシング対策

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

一般的に、「フィッシング対策」とは、複数のプラットフォーム、デバイス、ブラウザー、アプリケーション、テキストメッセージにおいて、ハッカーがユーザーを騙して不正なリンクをクリックさせたり、悪意のあるファイルをダウンロードさせたりするのを阻止するために設計された一連のツールを指すことが多いです。

防御が機能する仕組み

人間は完璧ではありません。ハッカーに騙されてリンクをクリックさせられたり、ファイルのダウンロードを開始させられたりしても、これらのツールにより、実際に悪意のある行為が実行されることを防げます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

スパムメールはフィルタリングされているのになぜ別のツールが必要なのか?

たしかに、一部のブラウザーや電子メールでは無料のツールがあります。しかし、そのようなツールはすべてのプラットフォームに対応しているわけではありません。また、従業員が仕事目的で個人用のデバイスを使用する頻度が多くなるほど、インシデントは増えていきます。

フィッシング対策ツールを購入してから導入するまでに時間がかかるのはなぜ?

フィッシング対策が必要とするOS、デバイスの種類、ネットワークシステム、ブラウザー、その他のエンドポイントなどをすべて挙げてみてください。これだけで、なぜ時間がかかるののかが分かるはずです。

無料版もあるのに、なぜこのようなツールに高い料金を支払うべきなのか?

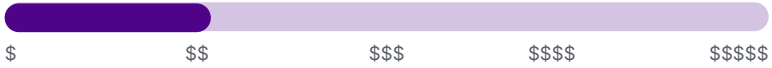
通常、堅牢性の高いフィッシング対策ツールに関するコストの増加は、複数のプラットフォームやデバイスに対応するためです。フィッシングによる認証情報ハッキングは、その最終的な動機にかかわらず、ほとんどの脅威アクターの共通の戦術です。

つまり、フィッシング対策ツールは、高いコストにつながるサイバーセキュリティ侵害を防ぐための最もシンプルで安価な方法の1つなのかもしれません。

ウイルス対策/マルウェア対策

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

これは、サイバーセキュリティソリューションの中で最も基本的なもので、広範囲な保護と基本的な侵入の試みに対する一般的な抑止力を提供します。

防御が機能する仕組み

基本的に、ウイルス対策とマルウェア対策は、最も基本的な脅威や日和見的な脅威をブロックし、抑止するために、あらゆる組織が導入すべき必要最低限のツールです。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

ベンダーが「無料」で提供するビルトインのツールがあるのに、なぜこのような機能に支出しなくてはいけないのか?

無料版ではコンピューターの動作が遅くなったり、一般的に操作上の問題が発生したりする場合は、改良されたウイルス対策やマルウェア対策ソリューションに切り替えることを正当化できる可能性があります。

業務への影響が極端に大きくなるようであれば、無料版のソフトウェアは価格に見合わないと主張することができます。おそらく、ステークホルダーも、新しいウイルス対策やマルウェア対策ツールを調達することに賛同されるでしょう。

アプリケーションコントロール

概要

アプリケーションコントロールは、保護された環境内の特定のアプリケーションのみを許可します。一般的に、このような制御は、非常に厳しい規制が適用される組織や企業レベルの組織で最も多く見られます。

防御が機能する仕組み

アプリケーションコントロールは、すでに審査されたプロバイダーの「ホワイトリスト」のアプリケーションやソフトウェアのみを許可するので、従業員が、マルウェアやトロイの木馬を隠している未知のペイロードを誤ってダウンロードしないように防ぎます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜアプリケーションコントロールにコストを費やさなくてはいけないのか? 既に他のユーザーコントロールを使っているが！

すべてのアプリケーションコントロールは連携し、重ね合わせることで、より強固なサイバー防御を実現します。

しかし、アプリケーションコントロールに特別な予算を確保したいのであれば、アプリケーションの使用状況を監視し、未使用の「シェルフウェア（購入後に放置されているソフトウェア）」を排除することで、アプリケーションコントロールが会社のコスト削減につながることを、情報セキュリティ部門部門以外のステークホルダーに伝えることができます。

このようなことをされると、業務で必要な XYZアプリを実行できません。

このような場合にも、情報セキュリティ部門以外のすべてのステークホルダーとの積極的なコミュニケーションが重要です。

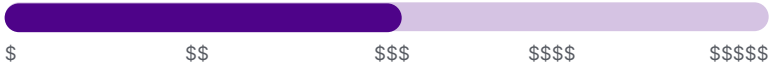
すべての部署で現在使用されているアプリケーションの包括的なリストを入手し、可能であれば、「シャドーIT」アプリケーションとして部署が個人的に支払っているアプリケーションを見つけます。そして、ホワイトリストプロセスの一環として、そのリストにあるすべてのアプリがセキュリティの脅威とならないことを再確認し、大きな支障をきたすことなく業務を継続できるようにします。

また、保護された環境に新しいアプリを追加する申請のプロセスを、できるだけ簡単にすばやく行えるようにします。同時に、それぞれの申請に対して少なくとも1人監視する担当者を確保します。このプロセスを完全に自動化してしまうと、ハッカーがそれを悪用して、自分たちの活動に密かにアクセス許可を付与する可能性があります。

構成管理

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

設定、ポート、プロトコル、これらのすべてを構成管理で考慮し、システム全体が安全なベースラインで設定されている必要があります。また、構成管理では、購入したすべての製品が適切なデバイスにインストールされ、使用されるるようにすることも含まれています。

防御が機能する仕組み

一般的にオープンポートや構成は、脅威アクターにも知られています。既定値やサポートが終了したバージョンをそのまま使用し続けていると、攻撃範囲が拡大します。

構成管理は、他のセキュリティプログラムが忘れられたり、デバイスや環境で適切に設定されていなかったりすることがないようにすることで、全体的なセキュリティ技術スタックをサポートすることもできます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜ構成管理ソリューションを購入する必要があるのでしょうか。

規制がそれほど厳しくない小規模な組織では、費用対効果としてはコスト側に傾きすぎて、構成管理ツールの真価が発揮されない可能性があります。また、人的・時間的コストのかかる手作業になる可能性もあるため、必要なツールがチームの管理負担にならないことを証明する必要があります。

しかし、構成管理を適切に実施すると、すべての部署で投資したテクノロジーが実際に導入されていることを確認することができ、組織のコスト削減につながります。

デバイスの衛生と管理

資産の検出を含む

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)

概要

この防御ディレクトリでは、デバイスの衛生と管理ソリューションを、環境内のあらゆるエンドポイントデバイス、ハードウェア、ソフトウェア資産の脅威を継続的に検出、一覧化、監視、対応するために必要なツールまたはツールスイートとして定義しています。また、セキュリティの観点から、侵入者が特定された場合に必要となる、直接的な修正や対処の促進または統合するこのようなソリューションも必要です。

防御が機能する仕組み

把握できていない脅威から組織を守ることはできません。従来のデバイス監査の正確性は、検出が確定した時点の一点に限定されていたため、サイバーセキュリティソリューションセットでは、保護されたネットワーク内のすべてのエンドポイントを堅牢、動的、自動的な方法で管理する必要があります。資産検出機能は、保護されていないデバイスを特定し、場合によってはネットワークで「普通のノートパソコン」を装った潜在的な侵入を発見することで、衛生管理プログラムをサポートします。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

すでに ITAM を導入していますが、なぜまだ必要なのか。

一般的に、通常のITAM ツールは、入力された購入記録から Active Directory まで検出されることが想定されているデバイスと資産のみを追跡します。このようなステークホルダーには、「目に見えないもの、未確認のものこそ、通常の業務に影響を及ぼす最大の潜在的なリスク」だということを改めて説明してください。

Active Directory、調達、エンドポイント管理、エンドポイントプロジェクションの各システムを調整しても、組織が保護すべき資産の20～30%は見落とされる可能性があります。さらに、ハッカーや脅威アクターが持ち込むデバイスや、管理されていないBYODから配信されるマルウェアペイロードは特定されません。

なぜアップグレードする必要があるんですか。

組織の規模が拡大すると、デバイスの数も急増し、安価なオプション機能では対応できなくなります。また、1つのプロジェクトで調整を行っても、その瞬間に劣化してしまいます。

さらに、ソフトウェアには無料ツールが付属していますが、不明なデバイスや管理されていないデバイスが環境に接続、切断したときに検知する動的資産検出機能がそのようなツールに含まれていることはほとんどありません。

セキュリティにとって、資産検出は、攻撃面を管理するうえで、「推奨」機能ではなく、問題解決のための重要な要素です。

エンドポイントデバイス&レスポンス (EDR)

不正侵入検出システム (IDS) と不正侵入防止システム (IPS) を含む

機能するまでの時間

概要

EDRソリューションは、不正アクセスを特定し、実行される前に阻止することができます。多くの場合、このようなソリューションは、ファイアウォールやウイルス対策/マルウェア対策保護などの他の初期アクセスソリューションと組み合わせられています。このようなツールは、不正IPアドレスの送信元の検出といったファイアウォールに組み込むこともできます。EDRソリューションを自動化すると、ベースラインから逸脱するアクセスパターンとトラフィック傾向を検出し、攻撃の可能性を警告できます。

防御が機能する仕組み

インシデントに対応できるのは、インシデントを把握している時だけです。ハッカーに対して設定するアラームや検知機能が多いほど、把握し、阻止できる攻撃も多くなります。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

無料のファイアウォールがあるのになぜEDRにコストを費やさなくてはいけないのか?

情報セキュリティ部門以外のユーザーには、壁だけの防御と、壁と警備員で防御することの違いを説明してください。壁は抑止力としては優れていますが、脅威を能動的に検出して、その侵入を阻止しようとするものではありません。

EDRは、比較的少ないコストと人的リソースでの投資で、多数の自動セキュリティを実現できます。

時間がかかるのはなぜですか。

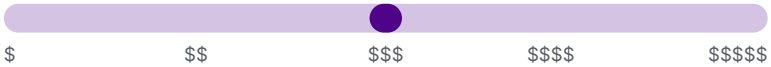
チームが心配しているような、微調整が必要な舞台裏がたくさんあることをステークホルダーに伝え、導入されたときにはその存在が気づかれないようにします。

また、EDRが信頼できるものであることを確認するために、チームは、初期導入時のモニタリングを長期にわたって行う必要があります。

悪意のある暗号化の検出および隔離

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

不正行為者が身代金を要求したり、盗んだりする目的でファイルの暗号化や抽出を始めた場合、この種類のソフトウェアは、攻撃を受けているファイルを自動的に検出し、ネットワークやサーバーの一部を隔離して、暗号化の進行を防止することができます。

防御が機能する仕組み

他のすべてが失敗した場合、悪意のある暗号化の検出と隔離によって、サイバー犯罪者が十分なデータを盗んだりロックしたりする前に、サイバー攻撃を検出することができます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜこのような機能にコストを費やさなくてはいけないのか。

情報セキュリティ部門以外のステークホルダーには、「備えあれば憂いなし」という諺で説明してください。

他のセキュリティツールでは、サイバー攻撃を未然に防ぐことができますが、このソフトウェアは、機密データの暗号化や抽出を検知したときに、緊急ブレーキとして機能します。

もし、組織が情報を守るために、あらゆる可能性を想定し対処していないということが知れ渡ったら、世間はどう思うでしょうか。あるいは、知的財産の盗難から株主の投資を守るために可能なかぎり最善の対策が取られていないと知ったら、株主はどう思うでしょうか。

なぜサイバー保険だけでは十分ではないのでしょうか。

サイバー保険は、損害調査や事後処理の費用に充てることができます。しかし、壊滅的な侵害の事後処理よりも、侵入を阻止した方が、圧倒的に時間、人的リソース、コストが低いでしょう。

保険料は急騰することになり、保険の加入資格を得るためだけでも、おそらくさらに高価な安全対策を導入する必要があるでしょう。

ネットワークセグメンテーション

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)

概要

ネットワークセグメンテーションとは、インターネットやイントラネットのネットワークを分割し、特定のデバイスだけがアプリケーションやサーバーの特定の部分にアクセスできるようにすることです。独自のネットワークセグメントに接続されたモノのインターネット (IoT) 対応デバイスといったシンプルな構成から、各部署やサーバーが独自の環境とネットワークを持つような複雑な構成まであります。

防御が機能する仕組み

ネットワークセグメンテーションは、ハッカーが、最初に漏洩した認証情報やアクセスポイントを悪用して、ネットワークの他の部分にアクセスすることを防ぎます。たとえば、攻撃者がIoT対応のオーブントースターなどの環境の無害な部分に侵入したとしても、さらにアクセスを拡大して機密情報にアクセスすることはできません。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜネットワークセグメンテーションツールにも高いコストを費やさなくてはいけないのか。

ネットワークセグメンテーションツールは、セキュリティチームの時間とリソースを節約し、ネットワーク侵入者を特定し、環境間の認可フローをより直感的にすることができます。

ネットワークの管理や監視にかかる時間を短縮することで、セキュリティチームは会社や上司から求めている他の業務に着手できるということを、情報セキュリティ部門以外のステークホルダーに伝えてください。

また、高機能なツールほど、必要なときにネットワークセグメント間を移動する手間を省くことができます。

なぜ、今の環境から必要な文書を取り出すことがそれほど難しいのでしょうか。

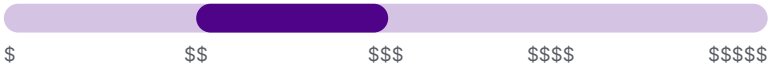
情報セキュリティ部門以外のステークホルダーが変更許可申請を提出するプロセスは、できるだけシンプルで直感的にしてください。

特に最初のうちは、苦情があってもできるだけ我慢するように、チームに周知してください。このような不満のほとんどは、各部署のリードをプロジェクトコンサルタントとして導入プロセスに積極的に参加させることで最小限に抑えることができ、誰がどのセグメントにアクセスする必要があるのかということと、その一般的なワークフローがわかります。

パスワードレス多要素認証 (MFA)

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

パスワードレスMFAは、アプリケーションへのアクセスや権限の付与に、テキスト/SMS、電子メール、認証アプリの要求、または生体情報などの二次認証を必要とするログインツールです。ただし、従来の二要素認証とは異なり、パスワードレス多要素認証ログインではパスワードが不要です。

防御が機能する仕組み

概して、一般的な情報セキュリティ部門以外の従業員は、複雑なパスワードや固有のパスワードの作成を避けるでしょう。パスワードをなくすことで、ハッカーはクレデンシャルスタッフィングやブルートフォース攻撃で入手したパスワードや、従業員が付箋にメモしたパスワードを使用してシステムにアクセスすることができなくなります。

さらに、パスワードレスMFAプログラムでは、「覚えること」が減るので、セキュリティプログラムのコンプライアンスを高めるのに役立ちます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

パスワードレスMFAは、なぜ別の方法よりもコストが高いのでしょうか。

利用可能なパスワードレスMFAツールは多数あります。一般的に、1ユーザーあたりのコストが高いほど、利用できる暗号化レベルやカスタム制御が高くなります。

暗号化レベルが高いほど、ハッカーがコンピューターを駆使してシステムを破壊するのを防ぐことができます。

また、カスタム制御は、誰にとっても使いやすくなると同時に、人件費の減少にもつながります。

セッションのタイムアウトは本当に煩わしいです。無効にすることはできますか。

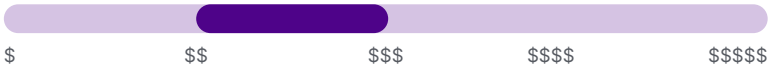
まず、ステークホルダーとの関係性によっては、「煩わしいと思うなら、常に追い出されるハッカーの方がどれほどストレスを感じているのかを想像してみてください。少なくとも、こちらはもう一度やり直すことができるのですから」と冗談を言うこともできます。

そして、もっと真剣に説明するならば、本書で後述する「防御の方法」の一部を使用して、ネットワークへのアクセスの取得はサイバー攻撃の最初の部分に過ぎないことを、情報セキュリティ部門以外のステークホルダーに示すことができます。不正なハッカーが侵入しにくい組織ほど、チームが侵入を阻止し、不正なハッカーを永久的に追い出すことが容易になります。

権限管理

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

権限管理は、個人またはネットワークのコンピューターで、どのタイプの従業員がどのような権限を必要とするのかを制御します。たとえば、一般的な従業員は、個人のコンピューターで管理者のステータスを使用できるかもしれませんが、一般的にPowerShellをインストールするための権限は必要ありません。

防御が機能する仕組み

アクセスコントロールと同様に、ハッカーが一般社員のデスクトップコンピューター (その社員はスーパー管理者としてログインしている) にアクセスしたとしても、権限が制限されているため、多数のハッキングツールを展開したり、ネットワークへのアクセスを拡大したりすることはできません。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜこのような機能にコストを費やさなくてはいけないのか。展開と管理には人による作業がもっと必要です。

適切な権限管理プログラムの導入と維持には、常時監視とユーザーレベルの更新が必要なため、必要な労働力は多くなることがあります。そのため、企業や規制の厳しい業界では、メンテナンスの必要性が一般的に高まっています。

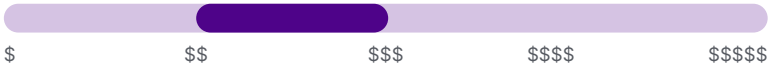
したがって、このプログラムに対するコストや社内サポートが、他の情報セキュリティ部門以外のステークホルダーの間で問題になっているのであれば、今年度の検討は控えることも考慮してください。そして、オンボーディング時の初期の権限設定に細心の注意を払い、誰にでも管理者アクセス権限を付与することは原則として避けてください。

ルールの例外を求める (適格な)要求が増え始めたら、これらの要求をサポートまたはより技術に基づく権限管理ソリューションとして収集します。ある時点で、プロセスの少なくとも一部を自動化できるツールに投資することは、経済的に合理的です。

リスクベースのパッチおよび脆弱性管理

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

このツールは、組織の環境とニーズに基づいて修正プログラムを特定して、優先度を決定し、パッチを展開します。重要度やベンダーのセキュリティに関する外部脆弱性評価に基づいてパッチを適用するのではありません。

防御が機能する仕組み

RBVMツールでは、デバイスやユースケースにとって最も重要なパッチやセキュリティ欠陥の優先度を設定できます。これには、サイバー犯罪者が今まさに利用している弱点や脆弱性を強調することも含まれます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

以前にパッチを適用していましたが、今回はどのように違うのですか。

まず、以前にパッチを適用したことを確認します。そして、火災訓練は常に行われていることをステークホルダーに思い出させます。報道される緊急事態は避けたいのではないでしょうか。 RBVMは、ハッカーに攻撃される前に、それぞれ重要な脆弱性をプロアクティブに特定し、パッチを適用させます。

そして、あなたのような組織を攻撃した脅威アクターであるDefense Playsを明示的に参照し、悪用された脆弱性や古い脆弱性にパッチを適用していれば、ハッカーの攻撃を早期に阻止できたであろうという点をポイントごとに示します。

最後に、この種類のパッチは手動では実行できないことを強調します。 RBVMだけが、独自の脅威環境においてどのエクスプロイトが重要であるかを自動的に把握し、デバイスとデータが保護されているかどうかを判断することができます。

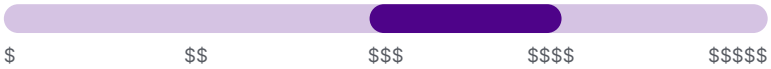
無料版の自動パッチソフトウェアがあるのに、なぜこのツールにコストを費やさなくてはいけないのか。

リスクベースの脆弱性管理ツールは、本書で説明されている脅威アクターにとっての複数の接点に影響を及ぼせるため、パッチの優先順位付けし、パッチを展開します。 RBVMツールへの投資によって、ハッカーがシステムに侵入しているかどうかがわからなくても、ハッキングによる複数の攻撃ポイントを防ぐことができます。

セキュリティプログラム監査

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

セキュリティプログラム監査は、幅広いサービスを提供しますが、一般的には、サイバーセキュリティソリューションやプログラムが機能しているか、環境や役割に問題ないか、調整が必要かどうかを確認するサードパーティのコンサルタントまたはアナリストとして要約されます。ペネトレーションテストや従業員のフィッシングに対するトレーニングもこのカテゴリに含まれます。

防御が機能する仕組み

率直に言って、どのようなプログラムやプロジェクトに携わっている人でも、欠点に気づくのはとても難しいことです。多くの場合、セキュリティプログラムが実際に設計したとおりに機能しているかどうかを知るには、信頼できるプロバイダーによる外部セキュリティ監査が唯一の方法です。

また、より深い監査は、内部の脅威や外部ハッカーによる通常とは異なる方法や潜在中の侵入を洗い出すことができます。監査は、調整されていない未解決の部分や、現在の役割に再調整されていないランダムな詳細を一掃することができます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

監査を実施したばかりではありませんか。なぜもう一度コストを費やさなくてはいけないのか。

リスクが高い環境、パートナー、ベンダーに対しては監査の頻度を増やす必要があります。ある環境が基幹業務システム、または政府機関や軍事請負業者など既知のターゲットや脅威要因に接続されているほど、ハッカーがその環境にアクセスしようとしている可能性は高くなります。

また、頻繁に監査を行うことで、攻撃を実行する前に情報収集を行う潜伏ハッカーを特定することもできます。特に精通した脅威アクターを早期に特定することで、データの損失、評判、訴訟費用など、数百万ドルの損失を防ぐことができます。

戦略的オートメーション

特にアラートおよび権限要求

概要

この文脈では、通常とは異なる、あるいは不適切な権限要求など、不要な、あるいは想定外のアクティビティに対する自動アラートについて説明します。自動化は、一般的なセキュリティプログラムの日常的な活動を促進するのにも役立ちます。

防御が機能する仕組み

イベントログ1つとっても、細部にこだわるセキュリティのプロでも気づかないことがあります。しかし、同じイベントがアラート閾値をトリガーして適切な修復チームに通知し、分析と修復のシームレスなプロセスを自動的に開始することができます。

脅威がより複雑になり、情報セキュリティ部門の責任が拡大するにつれ、自動化は、企業の安全を犠牲にすることなく、セキュリティチームに過度な負担をかけることなく、作業を支援することができます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜ自動化ツールにコストを費やさなくてはいけないのか。

多くの場合、より自動化されたソリューションに費やす方が、セキュリティの専門家を増やすよりも安く、より正確です。

自動化は、他のツールの主要な機能であることがよくあります。他と比較することで、ツールやソリューションを選択することを正当化する付加価値のある利点となり得ます。

以前にも自動化を試しましたが、すべてが上手く機能しませんでした。

神経質なステークホルダーには、自動化は人間の評価に代わるものではなく、思考、テスト、注意がなければ、ビジネスプロセスを混乱させずに展開されることはないことを強調します。

そのため、要望を伝える際には、自動化でできること、できないことを正確に一覧化して、期待できることを設定し、全体の不安を取り除かせるようにします。

なぜまだアクセス要求のためにチケットを提出するのですか。(<サービス>を自動化できますか。)

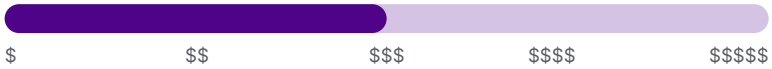
自動化によって管理上の負荷を軽減することはできますが、ハッカーは完全に自動化されたシステムを悪用する可能性があります。

たとえば、ハッカーは完全に自動化されたアクセス要求プロセスを騙して、より高い権限を取得し、より多くのネットワークに到達することができます。人がチェックすることで、そのようなエスカレーションを特定し、阻止することができます。

ユーザーアクセス制御

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

ユーザーアクセス制御ツールは、どの従業員と職務が、ネットワークのどの部分や業務に必要なアプリケーションにアクセスする必要があるかを、プロアクティブに管理するのに役立ちます。また、職務や役割は時間の経過とともに変化するため、これらのツールは、以前の権限にアクセスできないようにするのにも役立ちます。

防御が機能する仕組み

仮にハッカーが一般従業員から認証情報を入手したとしても、ユーザーアクセス制御によってハッカーがアクセスできるのは、その従業員がアクセスできる範囲に限られため、あらゆるファイルやデータサーバーにアクセスできるわけではありません。また、ユーザーアクセス制御は、通常とは異なるアクセス要求や侵入の試みに対して警告を発することができ、これまで検知されていなかったハッカーからの横の動きを早期に察知することができます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜユーザーアクセス制御のコストは高いのでしょうか。

一般的には、ユーザーアクセス制御ツールは「シート単位課金」モデルです。つまり、組織が大きくなればなるほど、全体としてコストがかかることになります。また、組織の成長や統合の計画に応じて、毎年、予算配分の変更も計画する必要があります。

この問いかけを、「保険」という観点で捉え直してみてください。従業員が誤ってノートパソコンの認証情報を外部に漏らしてしまって、知的財産や顧客記録がすべて漏洩されるリスクを避けるために、たとえその従業員がその情報にアクセスする必要がないとしても、ステークホルダーは1人あたりX費用を支払うことに抵抗するのでしょうか？

必要な部分にアクセスできなくなりました。

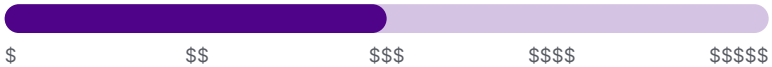
情報セキュリティ部門以外のステークホルダーが変更許可申請を提出するプロセスは、できるだけシンプルで直感的にしてください。

特に最初のうちは、苦情があってもできるだけ我慢するように、チームに周知してください。このような不満のほとんどは、各部署のリードをプロジェクトコンサルタントとして導入プロセスに積極的に参加させることで最小限に抑えることができ、誰がどのセグメントにアクセスする必要があるのかということと、その一般的なワークフローがわかります。

ユーザートレーニングおよび教育

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

情報セキュリティ部門以外の一般の従業員に対するセキュリティトレーニングや教育は、基本的なトレーニングモジュールから、デスクで行うエクササイズや没入型のシミュレーションまで多数あります。

防御が機能する仕組み

人は、あらゆるセキュリティチェーンの中で最も弱いリンクです。世界中のあらゆるテクノロジーを駆使しても、個人が善意だと思う行動によって引き起こされたセキュリティ事故を防ぐことはできません。トレーニングは、従業員が自分自身のサイバーセキュリティに責任を持つようにし、従業員自身での理解を深め、組織全体のセキュリティ環境を強化するのに役立ちます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

どのようにすれば効果的にトレーニングを導入できるのでしょうか。

フィッシング攻撃の報告など、従業員が個人的に防止に貢献した攻撃を知らせることで、情報セキュリティ部門以外の従業員がトレーニングを活用する動機付けをします。

また、パスワード管理ソフトに補助金を出すことで、健全なセキュリティプロトコルを実施できます。

原則として、コンプライアンス違反を理由に従業員を罰することはしないようにします。その代わり、コンプライアンスに則った行動を意図的に強調し、賞賛することで、セキュリティを共有責任とします。

なぜユーザーセキュリティトレーニングのコストは高いのでしょうか。

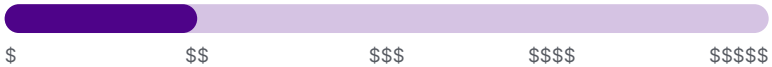
効果的なユーザートレーニングは、通常、高品質な表現によるインタラクティブな内容であり、時にはカスタムスクリプトを使用することもあります。このようなトレーニングモジュールは作成が難しいので、割高になることがあります。

しかし、ユーザーがトレーニングをよりインタラクティブで適切なものと認識すればするほど、参加率が高まり、知識の定着率が上がる傾向があります。つまり、最も重要なときにセキュリティ教育を利用できるようになるのです。

Webベースのコンテンツ制限

機能するまでの時間

有償ツールのコスト (堅牢なソリューションの導入)



概要

これらのツールは、保護されたデバイスから作業している間、ユーザーがオンラインで閲覧またはアクセスできる内容を制限します。

防御が機能する仕組み

脅威アクターやその他のハッカーは、オンラインアプリケーションを通じてデータや資料を転送することができます。インターネットへのアクセスを制限すれば、Webトラフィックの中に潜むマルウェアや外部ネットワークへの侵入など、他の脅威へのアクセスを制限することができます。

従業員を武装させましょう! - ステークホルダーに対して合理的な根拠を説明する

なぜWebコンテンツを制限するツールにコストを費やさなくてはいけないのか。

一般的に、このようなツールは、高度に規制されたオンサイト環境で実装されます。その理由は、気が散ったり危険な潜在的オンラインコンテンツの制限と実際の業務上のオンラインニーズのバランスを取るという実装の複雑さ、およびリモートワークの人気の高まりです。

一般的には、政府機関、病院、コールセンター、銀行の ATMなどで利用されています。

ただし、金融、医療、政府機関など、規制の厳しい分野に進出したい場合は、より制限の多いツールを導入する価値があるかもしれません。

また、生産性の向上も期待できます。ただし、この利点をどのようにアピールするかは注意が必要です。従業員が業務に必要なコンテンツやリソースにアクセスできる場合だけであり、業務時間中には気が散るようなサイトはブロックされます。

2022年
注目の脅威アクター

2022年は、さまざまな犯罪グループや動機によるサイバーセキュリティインシデントが発生しましたが、ここでは、大きく異なる4つの脅威を選んで紹介します。

これらの各グループは、2023年に向けてどのようなサイバーセキュリティの戦略的目標を推進するにしても、十分かつ適切な事例を提供します。

ivanti CSW Cyber SecurityWorks

2022年
注目の脅威アクター

セクション

ALPHV

「BlackCat」としても知られるALPHVグループは、BlackMatterやDarkSideのハッカー集団の最新の公開版であり、「サービスとしてのランサムウェア」モデル、すなわちRaaSの作成、販売、展開を担当するサイバー犯罪集団の代表例です。

RaaSとは何ですか。また、なぜステークホルダーが注意する必要があるのでしょうか。

基本的に、RaaSはハッキングソフトウェアパッケージをダークウェブやさまざまなブローカーを通じて販売することで一部利益を得るサービスです。

RaaSは、戦略的なソーシャルエンジニアリングを少し利用して、漏洩した認証情報を使ってターゲットのコンピューターシステムやネットワークに侵入し、被害者がデジタルキーと引き換えに身代金を支払うことに同意しない限り、重要なファイルをロックしてしまいます。

ALPHV は、オリジナルソフトウェアの作成者として、追加の汚い仕事をすることなく、集められたランサム料金の何パーセントかを請求します。（ただし、この犯罪集団は特定のターゲットを直接攻撃し、身代金の100%を奪うこともできます。）

RaaSと通常のランサムウェアとの違いは、次の2つです。

1. 1ALPHVと他のRaaSプロバイダーは、ランサムウェアソフトウェアをパッケージ化して販売することで、コードを書けない (あるいは書きたくない) 他の犯罪者に代わってコードを作成し、サイバー攻撃の可能性のリスクを飛躍的に拡大させます。

   また、ハッカーがハッキング行為を行うためにコードを作成できなくてもよいのであれば、悪意を持った誰もがサイバー脅威となります。

2. Nobeliumのような国家的脅威アクターは、外国勢力に対するスパイ活動や攻撃の一環として、BlackCatのRaaSのような「既製品」のハッキングを使用します。これは、攻撃を加速させ、他人のコードを使用することで関与を偽装する一方で、より価値の高いターゲットには独自の秘密のハッキングを保持します。

ダークウェブの「ビジネスモデル」としてのRaaS の採用、拡大は、あらゆる種類の組織、企業、政府機関への攻撃を驚くほど増加させ続けています。一方で、経験豊富なセキュリティチームにとっては機会でもあります。

なぜでしょうか。なぜなら、多くのハッカーが同じか似たようなランサムウェアを使って、同じか似たようなソースの「既製品」のエクスプロイトを使うなら、ほんの少しの予防策で広範囲の攻撃を防ぐことができるからです。

ALPHV 統計情報シート

別名:

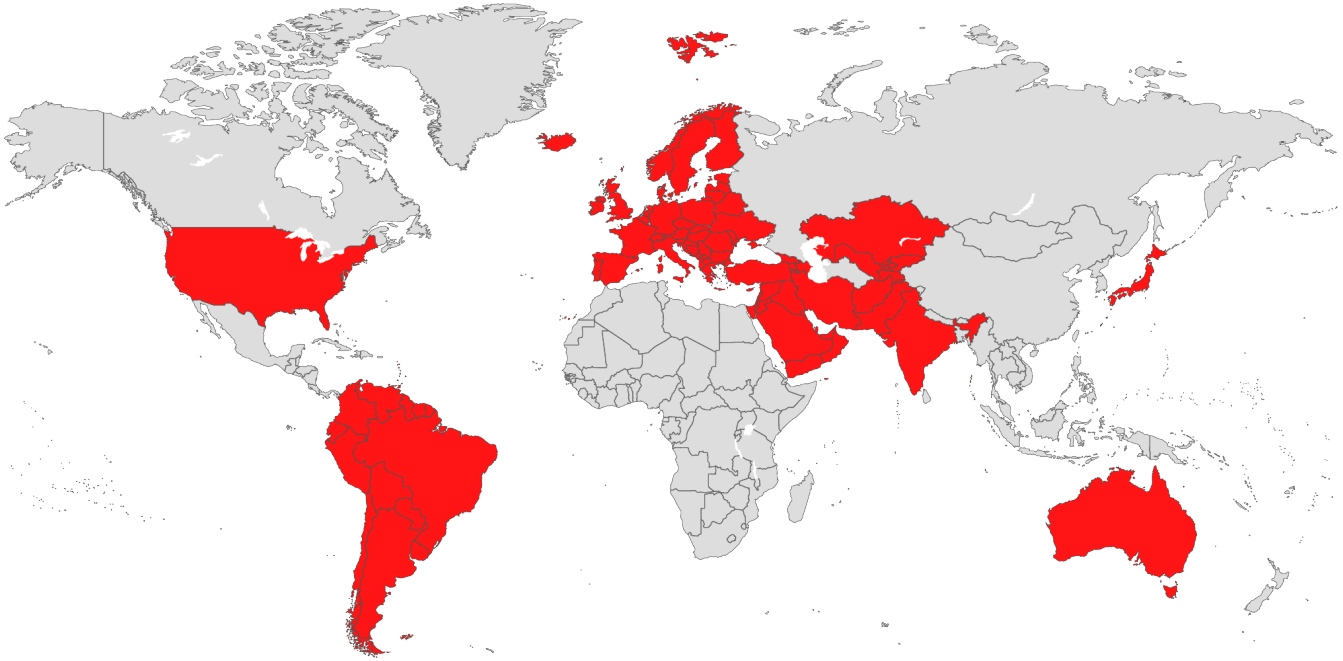
BlackCat
ALPHV
ALPHA
Noburus
AlphaVM

動機:

犯罪/金融

脅威タイプ:

サービス犯罪集団としてのランサムウェア



関係組織・団体

ロシア
Ryuk
Revil
DEV-0504
DEV-0237
FIN12
FIN7
Conti
BlackMatter
DarkSide

多く使用されるエクスプロイト:

CVE-2016-0099
CVE-2019-7481
CVE-2021-31207
CVE-2021-34473
CVE-2021-34523

確認済みのターゲット地域:

オーストラリア
オーストリア
欧州
ドイツ
インド
イタリア
日本
中東
南米
スイス
米国

ALPHV 攻撃の組織への影響

ITサービスの一時的な停止により、[...]物流センターおよび顧客サービス業務に影響がありました。

2021年12月23日: Moncler | ファッション/小売 | ミラン

「ターミナルの稼働能力が制限され、不可抗力 [外的な、不可避の、予見できない事象] を宣言しました。」

「ドイツ北部の223箇所のガソリンスタンドに影響しました。おそらく現金での支払いは可能です。」

2022年1月29日: Oiltanking + Mabanaft | 物流 | ドイツ

「影響を受けた 3,000台のITワークステーションのうち、最初の1台は [攻撃から4日後に] 再び利用可能になることを保証しています。[...] ITシステムに依存しているため、管理者は緊急モードになっています。」

2022年5月14日: Carinthia | 政府 | オーストリア

「[アクセスされた] サーバーやPCに顧客情報が含まれていた可能性があり、[...] 現在、漏洩の有無、被害範囲の特定、原因の究明を進めています [...]。」

2022年7月3日: バンダイナムコ | エンターテイメント | 日本

「月曜日も休庁が続くと予想され、再開の時期は未定です。[...]

私たちは、自分たちが脆弱であることを理解しています。」

2022年8月17日: フレモント郡 | 政府 | 米国

「[IT] 担当者は、文字通り24時間体制でこの [攻撃の] 解決に当たっています。完全な復旧と機能を目指して、ただひたすら努力を続けている同僚たちに、本当に感謝しています」。

2022年3月7- 11日: ノースカロライナ A&T州立教育大学 | 米国

「データが [ALPHV] によって暗号化されたりコピーされたりしたのかとの質問に対し、広報担当者はコメント以上の差し控えると述べました。」

2022年5月31日: CMC ELectronics | エレクトロニクス | カナダ軍事航空 Canada

「当社のシステムに何日もアクセスできないため、発生したバックログを取り戻すために [懸命に] 取り組んでいます。」

2022年7月23日: Creos | エネルギー | ルクセンブルク

AN ALPHV サイバーセキュリティ戦略:
身代金要求の前にALPHV攻撃を阻止する方法

漏洩した認証情報を使ってネットワークに侵入

ハッカーがネットワークに侵入する前に阻止することは、業務を中断することなく、すべての事業部を保護する最も簡単で安価で迅速な方法です。

- EDR
- Webベースのコンテンツの制限
- ウイルス対策/マルウェア対策
- モバイルデバイスのフィッシング対策
- ユーザートレーニングおよび教育
- パスワードレス多要素認証
- ユーザーアクセス制御
- アプリケーションコントロール
- デバイスの衛生と管理
- セキュリティプログラム監査
- 戦略的オートメーション
- 構成管理

システム情報とネットワークのマッピング

侵入者がネットワーク内を自由に移動できない環境の場合、重要なデータや脆弱性を見つけることができないため、ビジネスへの大きな影響を軽減できます。

- リスクベースのパッチおよび脆弱性管理
- デバイスおよびネットワークセグメンテーション
- デバイスの衛生と管理
- 資産の調整
- セキュアなアクセスプロトコル
- ネットワークセグメンテーション
- 権限管理
- 戦略的オートメーション
- 構成管理

独自の「穴」やエクスプロイトに基づき、被害者固有のランサムウェアを作成

サイバー犯罪者がランサムウェアを実行できなければ、身代金目的でデータをロックしたり盗んだりすることはできません。

- リスクベースのパッチおよび脆弱性
- アプリケーションコントロール
- ユーザーアクセス制御
- 権限管理
- デバイスの衛生と管理
- 戦略的オートメーション

セキュリティプログラムによるランサムウェアの攻撃やデータの持ち出しを阻止

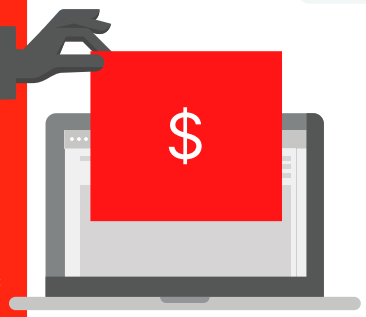
異常振る舞い検知は、ビジネスの停止や身代金の要求の前に、ランサムウェア攻撃の初期段階の兆候を通知します。

- アプリケーションコントロール
- 戦略的オートメーション
- ユーザーアクセス制御

ファイルを暗号化し、データの抽出（システムからの削除やコピー）を行うことで、被害者に有利な状況を作り出します。

ハッカーがデータを盗んだりロックすることができなければ、身代金を要求することはほぼできません。

- 悪意のある暗号化の検出および隔離
- デバイスおよびネットワークセグメンテーション
- Webベースのコンテンツ制限



先を見据えた対応はもう手遅れです。「災害復旧」モードに切り替えます。

APT29

米民主党全国委員会の内部メールや文書を流出させた悪名高いハッカー、APT29 (Nobelium) は、スパイ活動や諜報活動を専門とするロシアの対外情報機関につながるサイバー組織です。

「APT」とは「Advanced Persistent Threat (高度な持続的標的型攻撃)」の略です。この呼称は、通常、国または国家に支援された脅威集団を表し、組織のネットワークに侵入し、検出または攻撃の前に数ヵ月間、あるいは数年間潜伏することができます。

政府機関でもないのに、なぜステークホルダーがAPT29に関心を持つ必要があるのでしょうか。

情報セキュリティ部門以外のステークホルダーは、話題になっている最新の脅威アクターがロシア情報機関の一部であると聞くと、すぐにその脅威を完全に排除したくなるかもしれません。

「なぜAPT29が当社のような企業を気にするのか」と言われるかもしれません。「私たちは政府機関ではありません。私たちは戦争に加担しているわけではありません。」

少し視点を変えます。

博士論文からMetaのFacebook研究、俳優のKevin Bacon氏が登場するmemeゲームまで、多くのソーシャルネットワーク研究が、さまざまな規模の集団において、ある関係から次の関係へのつながりを調べています。どの出発点からも最終的な「目的地」までの平均的な「距離」は、3 ～ 4 回程度のつながりになるようです。

では、この仮定的なシナリオを、プロアクティブなサイバーセキュリティ戦略の推進に当てはめて考えてみましょう。

あなたの組織は、政府機関でも、ロシアに対して活動的な非営利団体でもないかもしれませんが、脅威アクターが危機に影響を与え、情報を引き出すために、最終目的地への到達、またはサプライチェーン攻撃による「つながり」による「つながり」を狙うことは、前例のないことではありません。

たとえば、有名なSolarWinds のインシデント (2020年に発生したAPT29のサイバー攻撃) を例に挙げます。

APT29のハッカーは、政府機関や重要インフラ組織を直接狙ったわけではありません。その代わりに、ネットワーク監視ソフトウェアのプラットフォームであるソフトウェアベンダーを感染させ、定期的なソフトウェア更新を通じて約 18,000人の顧客にバックドアをインストールしました。そして、その中には政府のユーザーも含まれていました。

18,000人の顧客全員がAPT29の標的となったわけではありませんが、全員がハッキングされ、強大な国家間のサイバーアンダーグラウンド戦争に巻き込まれ、全員が脆弱な状態に置かれました。

情報セキュリティ部門以外のステークホルダーが、APT29やその他の高度な持続的標的型攻撃集団に対して備えることについて、「中立」あるいは非戦闘員であるという理由で反発したいのであれば、「六次の隔たり」ゲームを机上演習やワークショップの活動として行ってみてください。

ただし、今回は、あなたの組織がロシアとつながっていることを演出してください。

統計的に言えば、情報セキュリティ部門以外のステークホルダーが信じようとするよりも、組織がAPT29の標的、あるいは他のAPTグループの標的になる可能性の方がはるかに高いのです。

APT29 統計情報シート

別名:

Nobelium	Cozy Bear	UNC-1151
YTTRIUM	CozyDuke	Cloaked Ursa
The Dukes	UAC-0113	

動機:

諜報活動/秘密工作

脅威タイプ:

高度な持続的標的型攻撃/APT

関係組織・団体:

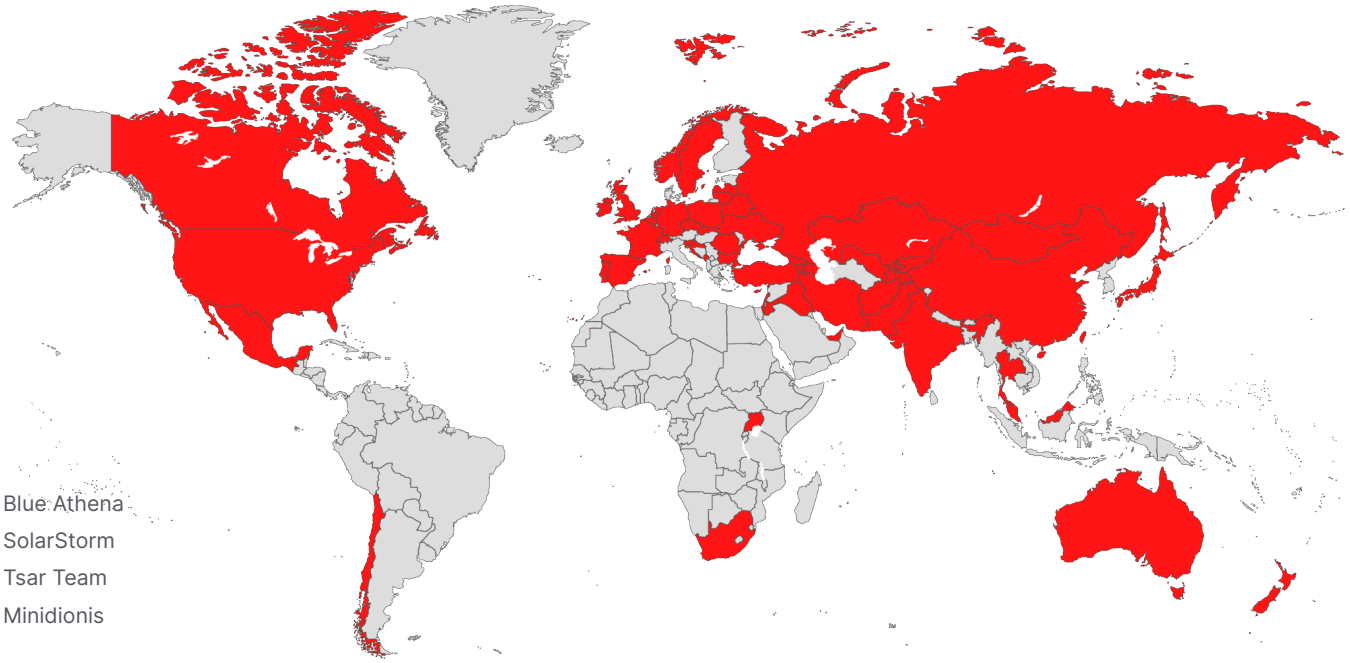
ロシア	APT28	Actinium	Blue Athena
Conti	Strontium	Bromine	SolarStorm
ALPHV	Iridium	Krypton	Tsar Team
Fighting Ursa	DEV-0586	StellarParticle	Minidionis

多く使用されるエクスプロイト:

CVE-2009-3129	CVE-2019-17026	CVE-2020-14882
CVE-2014-1761	CVE-2019-19781	CVE-2020-4006
CVE-2015-164	CVE-2019-2725	CVE-2020-5902
CVE-2018-13379	CVE-2019-7609	CVE-2021-1879
CVE-2019-11510	CVE-2019-9670	CVE-2021-21972
CVE-2019-1653	CVE-2020-0674	CVE-2021-26855

リスクが非常に高い業界:

政府	NGO・非営利団体	高等教育
軍事	運送	金融
エネルギー	IT	研究機関/シンクタンク
メディアと通信	医療	



確認済みのターゲット地域:

アフガニスタン	チリ	イラン	リトアニア	ポーランド	スイス
アルメニア	中国	イラク	ルクセンブルク	ポルトガル	タジキスタン
オーストラリア	クロアチア	アイルランド	マレーシア	ルーマニア	タイ
アゼルバイジャン	キプロス	イスラエル	メキシコ	ロシア	トルコ
ベラルーシ	チェコ	日本	モンゴル	スロバキア	アラブ首長国連邦
ベルギー	フランス	ヨルダン	モンテネグロ	スロベニア	ウガンダ
ブラジル	ジョージア	カザフスタン	オランダ	南アフリカ	英国
ブルガリア	ドイツ	キルギスタン	ニュージーランド	韓国	ウクライナ
カナダ	ハンガリー	ラトビア	ノルウェー	スペイン	米国
チェチェン	インド	レバノン	パキスタン	スウェーデン	ウズベキスタン

APT29 攻撃の組織への影響

APT29が送信したフィッシング電子メールは、各国大使館に関連する行政通知を装い、正規ながらも共同利用された電子メールアドレスを利用していました。

攻撃開始 2022年1月17 日 – 発表 2022年4月28日: 外交当局 | 欧州、アジア、北米

「APT29 を含むこれらの主体は、簡単なパスワード、パッチが適用されていないシステム、無防備な従業員を利用して初期アクセスを取得し、その後、ネットワークを通じて横方向に移動し、持続性を確立してデータを抽出します。」

攻撃開始 2020年1月 - 発表 2022年2月16日:防衛関連企業| 軍隊 |米国

「管理者はPCがロックされ、1万ドルのビットコインを要求するメッセージが表示されているのを発見しましたが、管理者が再起動したところ、コンピューターのハードディスクは不可逆的に破損していました。」

2022年1月13日: 政府・非営利団体 & IT団体|ウクライナ

「5月初旬以降、Cloaked Ursa [APT29] は、DropboxやGoogle Driveサービス [などの]、一般的なオンラインストレージサービスを利用してマルウェアを配信する能力を進化させ続けています。」

攻撃開始 2022年5月 – 発表 2022 年7月5日: 外国大使館|ポルトガルおよびブラジル

早ければ2021年5 月、ロシア国家に支援されたサイバーアクターは、非政府組織 (NGO) でデフォルトのMFAプロトコルに設定された誤った構成のアカウントを利用して、新しいデバイスをMFAに登録し、被害者のネットワークにアクセスすることができました。」

攻撃開始 2021年 5月 – 発表 2022 年3月15日: 非政府組織 | 米国

「サイバー攻撃の可能性は増大しています。これらは、[ロシアが行うサイバーキャンペーンの] 直接的な標的になっていない国や組織に対しても、深刻な影響を与える可能性があります。」

2022年2月18 日:「国家的に重要な組織」ニュージーランド

「[一般公開されている] コモディティ化したマルウェアの使用が顕著に継続しており、UAC-0113 [APT29] がさまざまなツールを使用することを厭わず、そのオペレーションを適応させていることがわかります。」

発表 2022年 9月19日: 政府および民間部門 | 「複数の地域」

APT29サイバーセキュリティ戦略:
検出または消去の前にAPT29攻撃を食い止める方法

フィッシングキャンペーンやまたは侵害されたサプライチェーンベンダー経由してネットワークに侵入

ハッカーがネットワークに侵入する前に阻止することは、業務を中断することなく、すべての事業部を保護する最も簡単で安価で迅速な方法です。

- EDR
- Webベースのコンテンツの制限
- ウイルス対策/マルウェア対策
- フィッシング対策
- ユーザートレーニングおよび教育
- パスワードレス多要素認証
- ユーザーアクセス制御
- アプリケーションコントロール
- デバイスの衛生と管理
- セキュリティプログラム監査
- 戦略的オートメーション
- 構成管理

管理者プロファイルにアクセスし、認証パケットを傍受してハッキングした権限を昇格

侵入者が認証情報を昇格させる能力を制限することで、データの盗難や恐喝を防ぐことができます。

- ユーザーアクセス制御
- 権限管理
- 構成管理
- セキュリティプログラム監査
- ユーザートレーニングおよび教育

有益な情報および弱点のネットワークをマッピング

侵入者がネットワーク内を自由に移動できない環境の場合、重要なデータや脆弱性を見つけることができないため、ビジネスへの大きな影響を軽減できます。

- リスクベースのパッチおよび脆弱性管理
- デバイスとセグメンテーション
- Device Hygiene & Management
- 資産の調整
- セキュアなアクセスプロトコル
- ネットワークセグメンテーション
- 権限管理
- 戦略的オートメーション
- 構成管理

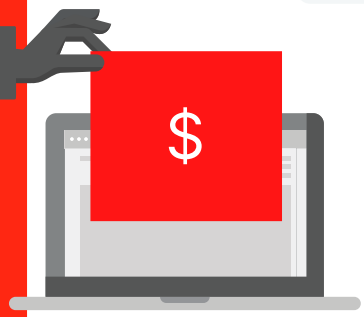
ログを消すことで、一部検出された場合、データを流出させ、防御に対抗する足がかりを増やすことになります。

異常振る舞い検知は、ビジネスの停止や身代金の要求の前に、ランサムウェア攻撃の初期段階の兆候を通知します。

- セキュリティプログラム監査
- EDR
- Web ベースのコンテンツの制限
- 戦略的オートメーション
- 悪意のある暗号化の検出および隔離

最大の混乱と影響を与えるために、コマンドで攻撃

先を見据えた対応はもう手遅れです。「災害復旧」モードに切り替えます。



Conti

最新のランサムウェアのニュースを追っているサイバーセキュリティ関係者にとって、「Conti」は馴染みのある名前です。このサービスとしてのランサムウェアは、2022年2月、ロシアのウクライナ侵攻後に「ロシア政府を全面的に支援する」と発表し、世間を騒がせました。

しかし、内部の不満分子が組織の系列のトレーニングプレイブックを公開し、外部のセキュリティ研究者が内部文書をTwitterで流出させて以来、1つの犯罪組織としての「Conti」は完全に解散したようです。

Contiのランサムウェア防止について言及すると、情報セキュリティ部門以外のステークホルダーは、行動を急がなければならない喫緊の事件がないため、サイバーセキュリティの戦略について疑問を持つかもしれませんが、それは本当の脅威から目をそらすための目くらましだとわかっています。

Contiがなくなったのに、なぜステークホルダーが過去の攻撃を防ぐことを気にする必要があるのでしょうか。

正直なところ、Contiにはしばらく評判の問題がありました。皮肉なことに、自身のオペレーション上のセキュリティや内々のモラルの低さが原因だったのです。

衰退の始まりは、Contiのメンバー向けトレーニングプレイブックの流出からでした。そして、ウクライナのITスペシャリストがネットワークに侵入し、長年にわたる内部資料を流出させたことです。

しかし、Contiが「死んだ」といっても、そのハッカーがまだ活動していないわけでも、そのコードが突然廃れたわけでもないのです。

Contiには広範な関連組織があり、脆弱性が存在する組織にとって脅威となる、作成されたランサムウェアのコードやテクニックの使用方法について明確に訓練されていました。

しかも、Conti組織自体のハッカーやプログラマー、ソーシャルエンジニアが逮捕されたり、死亡したりしたわけではありません。

実際、Contiがサーバーを停止してから丸2 ヵ月後、米国国務省は、「Conti」のハッカーの逮捕につながる情報に対して1,000万ドルの報酬を与えることを声明した新しい動画を公開しました。

最近、サイバーセキュリティの研究者やアナリストは、以下のような他のサイバー犯罪組織から Conti型の戦術を目にするようになりました。

- BlackByte
- Karakurt
- BlackBasta
- HelloKitty
- AvosLocker
- Hive
- ALPHV – など

Contiの過去のインシデントを研究することで、今日のプロアクティブな組織は、Contiの手口を使った小規模な脅威アクターによる同様の攻撃を多数防ぐことができます。

Conti 統計情報シート

別名:

なし

動機:

犯罪/金融

脅威タイプ:

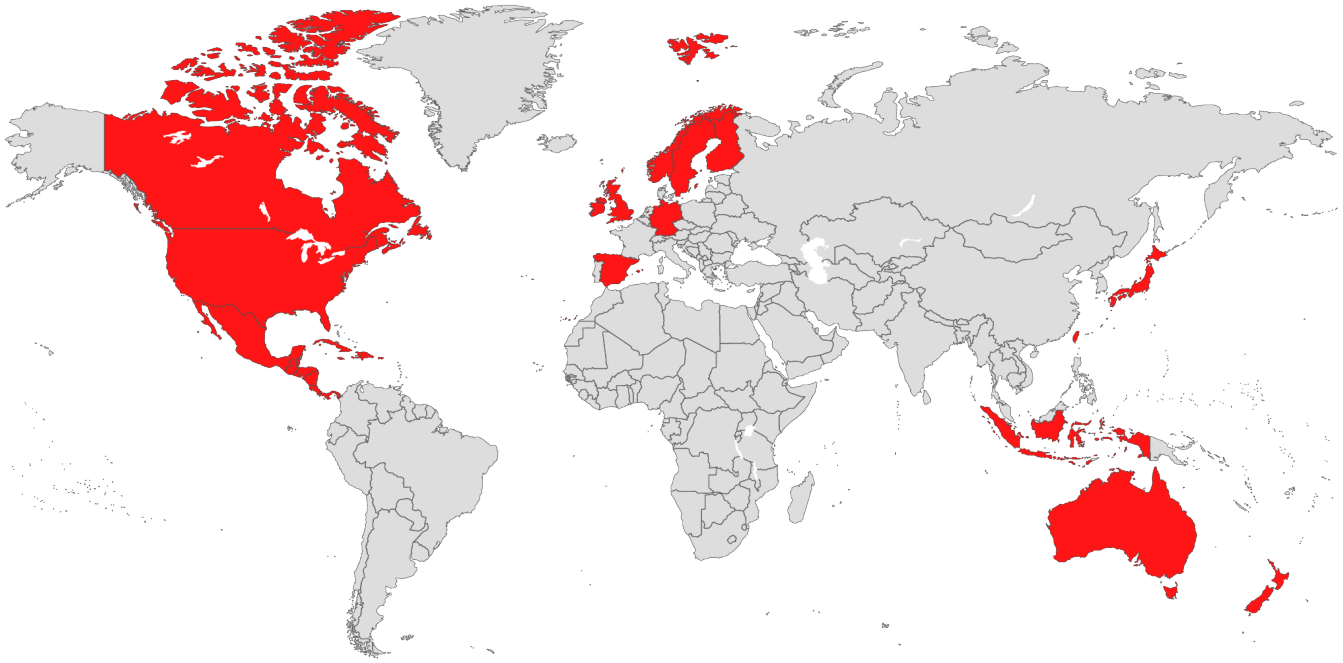
サービスとしてのランサムウェア (RaaS)

関係組織・団体:

ロシア	BlackBasta	Hive
BlackByte	HelloKitty	AvosLocker
Karakurt	ALPHV	Wizard Spider

リスクが非常に高い業界:

政府	ホスピタリティ	食品・飲料
金融	テクノロジー	小売・eコマース
エネルギー	医療	
製造	教育	



多く使用されるエクスプロイト:

CVE-2017-0143	CVE-2018-13379	CVE-2021-44228	CVE-2019-1069	CVE-2019-1388	CVE-2021-21972
CVE-2017-0144	CVE-2020-0796	CVE-2015-2546	CVE-2019-1129	CVE-2019-1405	CVE-2021-21985
CVE-2017-0145	CVE-2020-1472	CVE-2016-3309	CVE-2019-1130	CVE-2019-1458	CVE-2021-22005
CVE-2017-0146	CVE-2021-1675	CVE-2017-0101	CVE-2019-1215	CVE-2020-0609	CVE-2021-26855
CVE-2017-0147	CVE-2021-31207	CVE-2018-8120	CVE-2019-1253	CVE-2020-0638	
CVE-2017-0148	CVE-2021-34473	CVE-2019-0543	CVE-2019-1315	CVE-2020-0688	
CVE-2018-12808	CVE-2021-34523	CVE-2019-0841	CVE-2019-1322	CVE-2020-0787	
CVE-2018-13374	CVE-2021-34527	CVE-2019-1064	CVE-2019-1385	CVE-2021-1732	

確認済みのターゲット地域:

オーストラリア	ニュージーラド
カナダ	スカンジナビア
コスタリカ	スペイン
ドイツ	台湾
インドネシア	英国
アイルランド	米国
日本	
ラテンアメリカ	

Conti攻撃の組織への影響

Delta [Electronic] のネットワークにある65,000台のコンピューターのうち、約1,500台のサーバーと約12,000台のコンピューターが暗号化されています。[...] インシデントから1週間近く経ちますが、Delta のWebサイトはまだ復旧しておらず、影響は予想以上かもしれません。

2022年1月 21日: Delta Electronics
製造 | 台湾

「[...]Contiは、Shutterfly に属する 4,000台以上のデバイスと120台のVMware ESXi サーバーを暗号化していました。個人情報流出ページには、Shutterflyから盗まれたデータのサンプルも掲載されており、その中には、法的契約書、銀行や加盟店の口座情報、[...]、クレジットカードの下4桁を含む顧客情報と思われるものが含まれていると言われています。」

攻撃 2021年12月3日 – 報告 2021 年 12月26日: Shutterfly | 小売・eコマース | 米国

「BI（インドネシア銀行）は、先月のランサムウェアのハッキング攻撃を認識しています。サイバー攻撃を受けていることを認識しています。これは犯罪で、現実であり、私たちはそれにさらされているのです。」

攻撃 2021年 12月 – 発表 2022年 1 月 20 日: インドネシア銀行 | 金融 | インドネシア

「現段階では、注文の処理、商品の発送を安全に行うことができません。解決に向けてチームが取り組んでいますが、いつ解決するかは未定です。」

2022年1月 28日: KP Snacks | 食品・飲料 | 英国

「お客様の資産を守るため、契約中のタービンはNordex GroupのITインフラからのリモートアクセスを無効化しました。事業継続を可能にするようなITシステムの復旧を継続し、合理的に可能な限り早く通常業務を再開できるように取り組んでいます。」

2022年 3月 31日: Nordex | 製造/エネルギー| ドイツ

“コスタリカの輸出業者会議所の事務局長であるChristian Rucavado氏は、次のように述べています。「税関への攻撃は、同国の輸出入物流を崩壊させました。冷蔵倉庫で保管している生鮮品は時間との競争であり、経済的損失は計り知れません。」

2022年4月18日：財務省、労働省、社会保障省政府|コスタリカ

2022年 6月までに解散

Contiのレガシーサイバー防御戦略:
身代金要求の前にConti型の攻撃を食い止める方法

ファイアウォールやインターネットに接続されたサーバーや機器の設定に不備がある場合、フィッシングキャンペーンを利用してネットワークに侵入

ハッカーがネットワークに侵入する前に阻止することは、業務を中断することなく、すべての事業部を保護する最も簡単で安価で迅速な方法です。

- EDR
- Webベースのコンテンツの制限
- ウイルス対策/マルウェア対策
- モバイルデバイスのフィッシング対策
- ユーザートレーニングおよび教育
- パスワードレス多要素認証
- ユーザーアクセス制御
- アプリケーションコントロール
- デバイスの衛生と管理
- セキュリティプログラム監査
- 戦略的オートメーション
- 構成管理

ハッカーのユーザーアカウントで管理者権限を取得し、合法的な活動であるかのように偽装

侵入者が認証情報を昇格させる能力を制限することで、データの盗難や恐喝を防ぐことができます。

- ユーザーアクセス制御
- 権限管理
- 構成管理
- セキュリティプログラム監査
- ユーザートレーニングおよび教育

有益な情報および弱点のネットワークをマッピング

侵入者がネットワーク内を自由に移動できない環境の場合、重要なデータや脆弱性を見つけることができないため、ビジネスへの大きな影響を軽減できます。

- リスクベースのパッチおよび脆弱性管理
- デバイスとセグメンテーション
- デバイスの衛生と管理
- 資産の調整
- セキュアなアクセスプロトコル
- ネットワークセグメンテーション
- 権限管理
- 戦略的オートメーション
- 構成管理

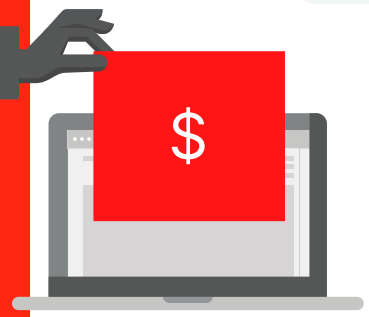
データを抽出し、恐喝のために利用

ハッカーがデータを盗んだりロックすることができなければ、身代金を要求することはほぼできません。

- セキュリティプログラム監査
- EDR
- Webベースのコンテンツの制限
- 戦略的オートメーション
- 悪意のある暗号化の検出および隔離

ランサムウェアを実行し、恐喝要求を行います。DoS攻撃で支払いを迫る可能性

先を見据えた対応はもう手遅れです。「災害復旧」モードに切り替えます。



Lapsus$

Contiと同様、2022年 3月にロンドン市警が、首謀者である16歳の自閉症を患っていたハッカー（「White」または「Breachbase」と名乗っていた）を逮捕したことで、誰もがLapsus$は終わったと思いました。

しかし、その数ヵ月後、大企業は過去の情報漏洩をこの集団に押し付けましたのです。そして、大手テクノロジー企業への全く新しい侵入が話題を呼びました。

Contiのように、Lapsus$がサイバー犯罪の脅威として自然発生的に復活したように見えることは、「死んだ」サイバー脅威であっても防御する必要があることを、情報セキュリティ部門以外のステークホルダーに思い出させるのに役立ちます。

しかし、Lapsus$は、攻撃の動機も侵入方法も全く異なるタイプのグループであるため、本書の4つのグループに含めました。

Lapsus$ は金銭を主な動機としているようには見えません。しかし、彼らは確かに情報の身代金を要求し、組織を脅迫して数百万ドルもの金を巻き上げたりしています。

Lapsus$のハッカーは「こんなことができるのか?」という好奇心から攻撃しているように見えます。どのような手段を使ってでも注目されたいという、昔ながらの若者の欲求からきているようです。

なぜ、10代のハッカー集団がステークホルダーの懸案事項となるのでしょうか。

Lapsus$攻撃を避けるために投資する価値があることをステークホルダーに納得してもらうためには、まず、これらの 10代の若者が活用した侵入と攻撃方法がいかに異なるかを説明する必要があります。

結局のところ、これらのハッカーは、今回取り上げた脅威アクターのように、多額の資金や人脈を持っていたわけではありません。大人のハッカーのように、犯罪行為で資金を集めることを専業とするような、犯罪行為に専念する時間がなかったのです。

Lapsus$のハッカーは、組織に潜入するために自由に使えるツールであるソーシャルメディアを活用したのです。

Lapsus$は公開されたテレグラムで、主要な企業や組織の初期ログインやその他のハッキング可能な情報を探していることを発表しました。情報提供者が報酬を望むのであれば、暗号通貨と情報を交換することにも積極的です。

そして、不満のある従業員は、その申し出を利用したようです。

テレグラムの最初の投稿から数週間、数ヵ月の間に、いくつかの主要な組織が Lapsus$集団に起因する侵害を公表しました。

一度、組織へのアクセスを取得したら、できる限りシステム内を横移動し、漏洩した認証情報を使って、他の従業員やIT部門を内部で騙すことができました。共有ドライブにアクセスし、会議の背景に潜み、暗号化されていないパスワードの文書を発見することができました。

そして、Lapsus$のハッカーはデータをエクスポートし、それを削除して、内部から騒乱が発生している見ることができます。社内のコミュニケーションチャネルを通じて身代金の要求を伝えることもできます。

従業員の士気が著しく低く、情報セキュリティ部門以外の担当者がサイバーセキュリティにおける自らの役割に主体性を持たない場合、組織の運用セキュリティ（内部と外部の両方）に対する重大な「内部脅威」となり、Lapsus$のサイバー攻撃パターンに代表されようになります。

Lapsus$ 統計情報シート

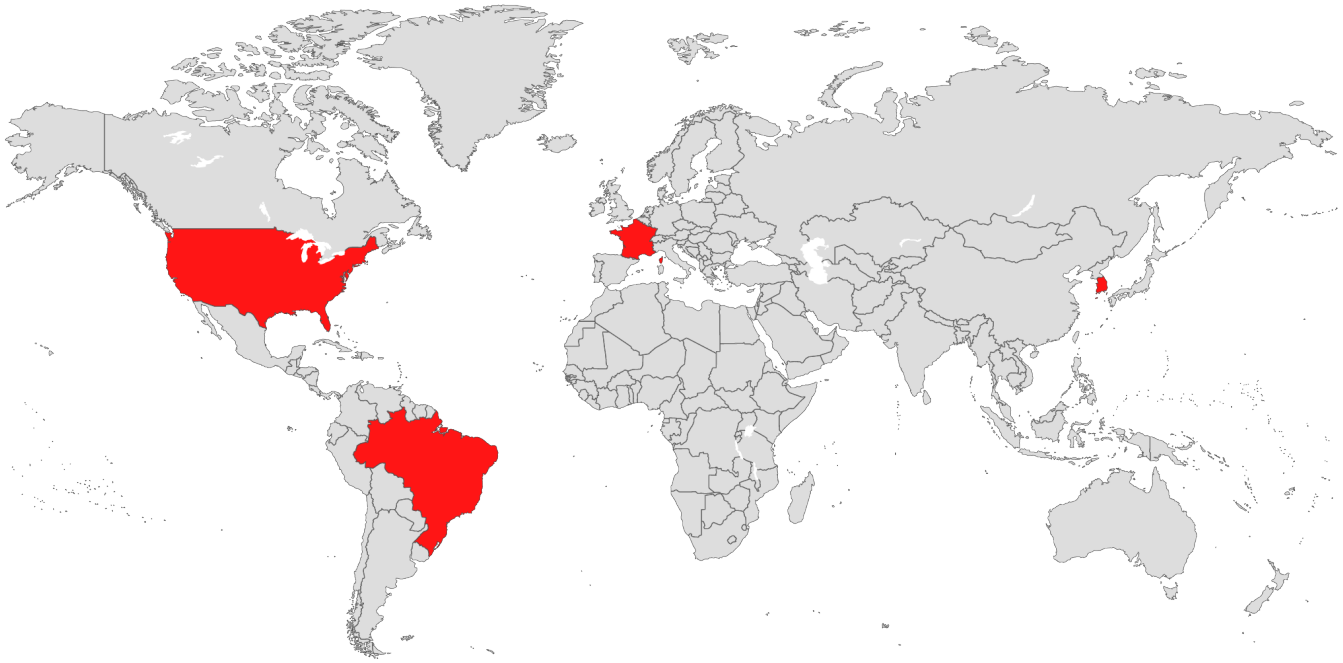
別名:
なし

動機:
ハクティビスト、金融

脅威タイプ:
一般的なハッカー

関係組織・団体:
UNC2447
Yanluowangr

リスクが非常に高い業界:
エンターテイメント
テクノロジー



多く使用されるエクスプロイト:

CVE-2021-34484
CVE-2018-13379
CVE-2020-12812
CVE-2020-23852
CVE-2021-26857
CVE-2021-31207
CVE-2021-44864
CVE-2021-44957
CVE-2021-45326
CVE-2021-45328
CVE-2022-0510
CVE-2022-21702
CVE-2022-0139
CVE-2021-45327
CVE-2021-45325
CVE-2021-44956
CVE-2021-34473
CVE-2021-26858
CVE-2021-26855
CVE-2020-23705
CVE-2019-5591
CVE-2021-34484
CVE-2022-21919
CVE-2022-26904
CVE-2021-34484

確認済みのターゲット地域:
ブラジル
フランス
韓国
米国

Lapsus$ 攻撃の組織への影響

攻撃者は契約者のUberアカウントにログインの試行を繰り返しました。その都度、契約者は二要素認証ログインの承認要求を受信し、最初はアクセスをブロックしていました。しかし、最終的には契約者がその要求を許可してしまい、攻撃者はログインに成功しました。

2022年 9月 15日: Uber | テクノロジー | 米国

「私たちが [会社] に通知してから、完全な調査報告書が発行されるまで、長い時間がかかったことに非常に失望しています。反省点としては、[会社の] サマリーレポートを受け取った時点で、その意味を理解するためにもっと迅速に行動すべきだったということです。」

2022 年 1月: Okta | テクノロジー | 米国

「当社の初期分析によると、今回の侵害はGalaxyデバイスの操作に関する一部のソースコードに関わるものですが、当社のお客様や従業員の個人情報は含まれていません。」

発表 2022年 3月 3日: Samsung | エレクトロニクス/製造 | 韓国

2022年 9月 11日、本セキュリティインシデントのファイル名リストをダークウェブに公開した不正行為者が、同じダークウェブ上に、同ファイルの実際の内容を掲載しました。

攻撃 2022年 5月 24日 – 報告 2022 年 8 月 10 日: Cisco Electronics / 製造 | 米国

当社は、脅威アクター [Lapsus$] がシステムから従業員の認証情報といくつかのNvidia財産情報を奪い、それをオンラインで流出し始めたことを認識しています。」

2022年 2月 23日: Nvidia | エレクトロニクス/製造 | 韓国

「Lapsus$はTorrentを投稿する際、Bingのソースコードの90%、Bing Maps とCortanaのコードの約45%が含まれていると述べています。」

2022年 3月 20日: Microsoft | テクノロジー| 米国

「最近、不正な第三者が当社のシステムに不正アクセスし、機密情報をダウンロードするというネットワーク侵入の被害に遭いました。その中には、次の「Grand Theft Auto」の初期開発映像も含まれています。」

2022年 9月 19日: Rockstar Games | エンターテイメント | 米国

Lapsus$サイバーセキュリティ戦略:
略奪と消去の前にLapsus$攻撃を防ぐ方法

内部脅威者の認証情報を使ってネットワークに侵入し、従業員の個人アカウントも企業ネットワークへの「バックドア」

ハッカーがネットワークに侵入する前に阻止することは、業務を中断することなく、すべての事業部を保護する最も簡単で安価で迅速な方法です。

- ユーザーアクセス制御
- 権限管理
- セキュリティプログラム監査
- アプリケーションコントロール
- パスワードレス多要素認証
- ネットワークセグメンテーション
- ユーザートレーニングおよび教育
- 戦略的オートメーション

公開された共有データベースで露出した認証情報を検索したり、ソーシャルエンジニアリングによる内部からの攻撃

侵入者が認証情報を変更または昇格させる能力を制限することで、データの盗難や恐喝を防ぐことができます。

- ユーザーアクセス制御
- 権限管理
- セキュリティプログラム監査
- アプリケーションコントロール
- パスワードレス多要素認証
- ネットワークセグメンテーション
- ユーザートレーニングおよび教育
- 戦略的オートメーション

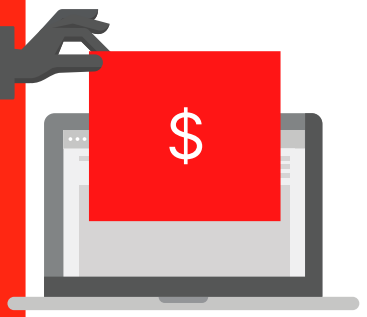
有名になるため (proff または hack0)、あるいは将来の恐喝のためにデータを流出

ハッカーがデータを盗んだりロックすることができなければ、身代金を要求することはほぼできません。

- Webベースのコンテンツの制限
- ユーザーアクセス制御
- 権限管理
- ネットワークセグメンテーション
- アプリケーションコントロール
- EDR
- セキュリティプログラム監査
- 戦略的オートメーション
- デバイスの衛生と管理

恐喝を開始 - おそらく被害者自身の内部ルートから開始 -組織がインシデント対応を始めるとき

先を見据えた対応はもう手遅れです。「災害復旧」モードに切り替えます。



情報セキュリティ戦術
インデックス

ivanti CSW Cyber SecurityWorks

情報セキュリティ戦術
インデックス

セクション

ALPHV MITRE ATT&CK マップ

1. 偵察

T1595: アクティブスキャニング
T1589: 被害者の個人情報の収集
　T1589.001: 認証情報

2. リソース開発

なし

3. 初期アクセス

T1078: 有効なアカウント
T1190: 公開アプリケーションの悪用

4. 実行

なし

5. 持続性

T1098: アカウント操作

6. 権限昇格

T1548: 昇格制御メカニズムの悪用
　T1548.002: ユーザーアカウント制御の回避

7. 防御回避

T1564: アーティファクトの隠蔽

8. 認証情報アーティファクト

T1003: OS 認証情報ダンピング
　T1003.001: LSASS メモリ
　T1003.004: LSA シークレット

9. 検出

T1082: システム情報検出
T1135: ネットワーク共有検出
T1018: リモートシステム検出
T1087: アカウント検出
　T1087.002: ドメインアカウント
T1487: ドメイン信頼検出
T1057: プロセス検出
T1083: ファイルおよびディレクトリ検出

10.横移動

T1563: リモートサービスハイジャック
　T1563.002: RDP ハイジャック
T1570: ラテラルツールの転送

11. 収集

T1005:ローカルシステムからのデータ

12. コマンドと制御

T1090: プロキシ
　T1090.003: マルチホッププロキシ

13. 抽出

T1567: Webサービスでの抽出
　T1567.002: クラウドストレージへの抽出

14. 影響

T1486: 影響を与えるためのデータ暗号化
T1489: サービス停止
T1490: システム回復の抑制

APT29 MITRE ATT&CK マップ

1. 偵察

なし

2. リソース開発

T1583: インフラストラクチャの取得
- T1583.001: ドメイン
- T1583.006: Webサービス

T1584: インフラストラクチャの侵害
- T1584.001: ドメイン

T1587: 機能の開発
- T1587.001: マルウェア
- T1587.003: デジタル証明書

3. 初期アクセス

T1078: 有効なアカウント
- T1078.002: ドメインアカウント

T1133: 外部リモートサービス
T1190: 公開アプリケーションの悪用
T1195: サプライチェーンの侵害
- T1195.002: ソフトウェアサプライチェーンの侵害

T1566: フィッシング
- T1566.001: スピアフィッシング添付ファイル
- T1566.002: スピアフィッシングリンク

4. 実行

T1047: Windows管理インストルメンテーション
T1204: ユーザー実行
- T1204.001: 悪意のあるリンク
- T1204.002: 悪意のあるファイル

T1053: スケジュールされたタスク/ジョブ
- T1053.005: スケジュールされたタスク

T1059: コマンドおよびスクリプトインタープリター
- T1059.001: PowerShell
- T1059.003: Windows コマンドシェル
- T1059.006: Python

T1203: クライアント実行のための悪用

5. 持続性

T1053: スケジュールされたタスク/ジョブ
- T1053.005: スケジュールされたタスク

T1078: 有効なアカウント
- T1078.002: ドメインアカウント

T1098: アカウント操作
- T1098.001: 追加のクラウド認証情報
- T1098.002: 追加の電子メール委任権限

T1133: 外部リモートサービス
T1546: イベントでトリガーされた実行
T1546.003: Windows 管理インストルメンテーションイベントサブスクリプション
T1546.008: アクセシビリティ機能

6. 権限昇格

T1053: スケジュールされたタスク/ジョブ
- T1053.005: スケジュールされたタスク

T1078: 有効なアカウント
- T1078.002: ドメインアカウント

T1484: ドメインポリシー修正
- T1484.002: ドメイン信頼通知

T1546: イベントでトリガーされた実行
- T1546.003: Windows管理インストルメンテーションイベント説明
- T1546.008: アクセシビリティ機能

T1547: ブートまたはログオン自動起動実行
- T1547.009: ショートカット修正

7. 防御回避

T1027: 曖昧にされたファイルまたは情報
- T1027.002: ソフトウェア圧縮

T1036: マスカレード
- T1036.004: タスクまたはサービスのマスカレード
- T1036.005: 合法的な名前または場所の照合

T1070: ホストのインジケーター削除
- T1070.004: ファイル削除
- T1070.006: Timestomp

T1078: 有効なアカウント
- T1078.002: ドメインアカウント

T1140: ファイルまたは情報の明確化/復号
T1218: システムバイナリプロキシ実行
- T1218.011: Rundll32

T1484: ドメインポリシー修正
- T1484.002: ドメイン信頼通知

T1548: 昇格制御メカニズムの悪用
- T1548.002: ユーザーアカウント制御の回避

T1550: 代替認証素材の使用
- T1550.003: チケットの送信
- T1550.004: Webセッション Cookie

T1553: 信頼制御の転覆
- T1553.002: コード署名

T1562: 防御の破壊
- T1562.001: ツールの無効化または修正
- T1562.002: Windows イベントログの無効化

T1562.004: システムファイアウォールの無効化または修正

8. 認証アクセス

T1003: OS 認証ダンピング
- T1003.006: DCSync

T1005: ローカルシステムからのデータ
T1552: 保護されていない認証情報
- T1552.004: 秘密鍵

T1555: パスワードストアの認証情報
T1558: Kerberos チケットの窃盗または偽造
T1558.003: Kerberoasting
T1606: Web 認証情報の偽造:
- T1606.001: Web Cookies
- T1606.002: SAML トークン

9. 検出

T1016: システムネットワーク構成検出
- T1016.001: インターネット接続検出

T1018: リモートシステム検出
T1057: プロセス検出
T1069: 権限グループ検出
T1082: システム情報検出
T1083: ファイルおよびディレクトリ検出
T1087: アカウント検出
T1482: ドメイン信頼検出

10. 横移動

T1021: リモートサービス
- T1021.006: Windows リモート管理

T1550: 代替認証素材の使用
- T1550.003: チケットの送信
- T1550.004: Web セッション Cookie

11. 収集

T1074: ステージングされたデータ
- T1074.002: リモートデータ署名

T1114: 電子メール収集
- T1114.002: リモート電子メール収集

T1560: 収集されたデータのアーカイブ
- T1560.001: ユーティリティによるアーカイブ

12. コマンドと制御

T1001: データの難読化
- T1001.002: データの難読化: ステガノグラフィ

T1071: アプリケーション層プロトコル
- T1071.001: Web プロトコル

T1090: プロキシ
- T1090.001: 内部プロキシ
- T1090.003: マルチホッププロキシ
- T1090.004: ドメインフロンティング

T1095: 非アプリケーション層プロトコル
T1102: Web サービス
- T1102.002: 双方向通信

T1105: 受信ツール転送
T1568: 動的解決

13. 抽出

T1048: 代替プロトコルでの抽出
- T1048.002: 非対称暗号化非 C2 プロトコルでの抽出

14. 影響

なし

Conti MITRE ATT&CK マップ

1. 偵察

T1595: アクティブスキャニング

2. リソース開発

なし

3. 初期アクセス

T1190: 公開アプリケーションの悪用
T1566: フィッシング
  T1566.001: スピアフィッシング添付ファイル
  T1566.002: スピアフィッシングリンク
  T1566.003: サービスを利用したスピアフィッシング

4. 実行

T1072: ソフトウェア開発ツール
T1203: クライアント実行のための悪用

5. 持続性

T1037: ブートまたはログオン初期化スクリプト
T1542: プレ OS ブート
T1542.003: ブートキット
T1543: システムプロセスの作成または修正
  T1543.001: エージェントの起動
  T1543.002: システムサービス
  T1543.003: Windowsサービス
  T1543.004: デーモンの起動
T1546: イベントでトリガーされた実行
  T1546.001: 既定のファイル関連付けの変更
  T1546.004: Unixシェル構成修正
  T1546.008: アクセシビリティ機能
T1547: ブートまたはログオン自動起動実行n
  T1547.006: カーネルモジュールおよび実行
  T1547.009: ショートカット修正
T1574: ハイジャック実行フロー
  T1574.008: 検索順序ハイジャックによるパスの傍受
T1574.009: ショートカット修正
  T1574.010: サービスファイル権限脆弱性
  T1574.011: サービスレジストリ権限脆弱性

6. 特権昇格

T1037: ブートまたはログオン初期化スクリプト
T1055: プロセスインジェクション
T1134: アクセストークン操作
T1543: システムプロセスの作成または修正
  T1543.001: エージェントの起動
  T1543.002: システムサービス
  T1543.003: Windows サービス
  T1543.004 デーモンの起動
T1546: イベントでトリガーされた実行
  T1546.001: 既定のファイル関連付けの変更
  T1546.004: Unix シェル構成修正
  T1546.008: アクセシビリティ機能
T1547: ブートまたはログオン自動起動実行
  T1547.006: カーネルモジュールおよび実行
  T1547.009: ショートカット修正
T1548: 昇格制御メカニズムの悪用
T1574: ハイジャック実行フロー
  T1574.010: サービスファイル権限脆弱性
  T1574.011: サービスレジストリ権限脆弱性

7. 防御回避

T1027: 曖昧にされたファイルまたは情報
  T1027.003: ステガノグラフィ
T1014: ルートキット
T1036: マスカレード
  T1036.005: 合法的な名前または場所の照合
T1055: プロセスインジェクション
T1112: レジストリの修正
T1134: アクセストークン操作
T1218: 署名されたバイナリプロキシ実行
  T1218.001: コンパイルされた HTML ファイル
T1542: プレ OS ブート
  T1542.003: ブートキット
  T1542.004: ルート証明書のインストール
T1548: 昇格制御メカニズムの悪用
T1553: 信頼制御の転覆
T1562: 防御の破壊
  T1562.001: ツールの無効化または修正
T1574: ハイジャック実行フロー
  T1574.010: サービスファイル権限脆弱性
  T1574.011: サービスレジストリ権限

8. 認証アクセス

T1005: ソフトウェア開発ツール
T1080: Taint 共有コンテンツ

9. 収集

T1005: ローカルシステムからのデータ
T1039: ネットワーク共有ドライブからのデータ
T1115: クリップボードデータ
T1123: 音声キャプチャ
T1125: 動画キャプチャ

10. コマンド

なし

11. 抽出

T1020: 自動抽出
  T1020.001: トラフィック複製

12. 影響

T1498: ネットワークサービス妨害
T1498.001: 直接ネットワークフラッド

Lapsus$ MITRE ATT&CK Map

1. 偵察

なし

2. リソース開発

なし

3. 初期アクセス

T1078: 有効なアカウント
T1133: 外部リモートサービス
T1190: 公開アプリケーションの悪用
T1199: 信頼できる関係

4. 実行

T1059: コマンドおよびスクリプトインタープリター
  T1059.001: PowerShell
  T1059.003: Windows コマンドシェル
  T1059.004: Unix シェル
T1072: ソフトウェア開発ツール

5. 権限昇格

T1068: 権限昇格のための悪用
T1078: 有効なアカウント
  T1078.002: ドメインアカウント

6. 持続性

T1021: サービス
  T1021.001: リモートデスクトッププロトコル
T1078: 有効なアカウント
  T1078.002: ドメインアカウント
  T1078.003: ローカルアカウント
  T1078.004: クラウドアカウント
T1114: 電子メール収集
  T1114.003: 電子メール転送ルール
T1133: 外部リモートサービス

7. 防御回避

T1027: 曖昧にされたファイルまたは情報
  T1027.002: ソフトウェア圧縮
T1078: 有効なアカウント
  T1078.002: ドメインアカウント
  T1078.003: ローカルアカウント
  T1078.004: クラウドアカウント
T1553: 信頼制御の転覆
  T1553.002: コード署名
T1562: 防御の破壊
  T1562.001: ツールの無効化または修正

8. 認証アクセス

T1003: OS 認証情報ダンピング
  T1003.001: LSASS メモリ
T1111: 二要素認証傍受
T1212: 認証アクセスの悪用
T1528: アプリケーションアクセストークンの窃盗
T1552: 保護されていない認証情報
  T1552.001: ファイルの認証情報
  T1552.004: 秘密鍵
T1555: パスワードストアの認証情報
  T1555.005: パスワードマネージャー

9. 検出

T1016: システムネットワーク構成検出
  T1016.001: インターネット接続検出
T1069: グループ検出
  T1069.002: ドメイングループ
T1082: システム情報検出
T1482: ドメイン信頼検出

10. 横移動

T1021: サービス
  T1021.001: リモートデスクトッププロトコル
T1534: 内部スピアフィッシング
T1078: 有効なアカウント
  T1078.002: ドメインアカウント

11. 収集

T1039: ネットワーク共有ドライブからのデータ
T1114: 電子メール収集
  T114.003: 電子メール転送ルール
T1213: 情報リポジトリからのデータ
  T1213.002: Sharepoint
  T1213.003: コードリポジトリ

12. 抽出

T114: 電子メール収集
  T1114.003: 電子メール転送ルール
T1537: クラウドアカウントへのデータ転送
T1567: Web サービスでの抽出

13. 影響

T1485: データ破壊
T1529: システムのシャットダウン/再起動

参考文献

ここに掲載したアナリスト、報告者、組織の皆様に加え、本ツールキットの実現に貢献した業界の見識や独自情報へのアクセスを提供してくださった Cyber Security Works および Ivanti の研究員および社内専門家に感謝を申し上げます。

NIST, “Advanced Persistent Threat.”

“2022 Global Threat Report.” Crowdstrike.

“Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology.” Cybersecurity & Infrastructure Security Agency (CISA).

“APT29.” MITRE ATT&CK.

“Cisco Data Breach Attributed to Lapsus$ Ransomware Group.” Dark Reading.

“Cisco Event Response: Corporate Network Security Incident.” Cisco Security.

“CISCO Talos shares insights related to recent cyber attack on Cisco.” Cisco Talos.

“DEV-0537 criminal actor targeting organizations for data exfiltration and destruction.” Microsoft Security.

“Encevo Cyberattack.” Encevo.

“Experts Call the Conti Ransomware Gang Who Broke BI Dangerous Hackers.” CNN Indonesia.

“General Security Advisory: Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine.” National Cyber Security Centre (NCSC).

“Globant official update.” Globant.

“Hacker attack on the province of Carinthia: “Black Cat” wants five million dollars in Bitcoin.” DerStandard.

“Incident and Agency Updates.” Fremont County Colorado.

“Lapsus$: An In-Depth Look at Data Extortion Group.” Avertium.

“MITRE Mapping of CISA KEVs and its Challenges.” Cyber Security Works.

“Moncler Press Release - Update on Malware Attack.” Moncler Group.

“Nordex Group impacted by cyber security incident.” The Nordex Group.

“RE: NOTICE OF DATA BREACH.” Meyer Corporation.

“RESPONSE TO LATEST MEDIA REPORTS ABOUT 27 NOVEMBER CYBER SECURITY INCIDENT.” CS Energy.

“Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability.” Cyber & Infrastructure Security Agency (CISA).

“Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine.” Insikt Group: Recorded Future.

“Security update.” Uber Newsroom.

“STATEMENT ABOUT CYBERSECURITY INCIDENT: DECEMBER 26, 2021.” Shutterfly, Inc.

“Statement from Oiltanking GmbH Group and Mabanaft GmbH & Co. KG Group.” Mabanaft Communications.

“Threat Report: T3 2021.” ESET Security Research.

“Ubisoft Cyber Security Incident Update.” Ubisoft.

“Update on cyber security incident.” The Nordex Group.

Abrams, Lawrence. “Lapsus$ hackers leak 37GB of Microsoft’s alleged source code.” Bleeping Computer.

Abrams, Lawrence. “Shutterfly discloses data breach after Conti ransomware attack.” Bleeping Computer.

Amitai Cohen via @AmitaiCo.

Australian Cyber Security Centre (ACSC). “2021-010: ACSC Ransomware Profile - Conti.”

Batra, Anirudh. “Detailed Analysis of LAPSUS$ Cybercriminal Group that has Compromised Nvidia, Microsoft, Okta, and Globant.” CloudSEK.

Bill Demirkapi via @BillDemirkapi.

Bradbury, David. “Updated Okta Statement on LAPSUS$.” Okta.

Brett Callow via @BrettCallow.

Brown, David; Matthews, Michael; Smallridge, Rob. “LAPSUS$: Recent techniques, tactics and procedures.” nncgroup.

Burgess, Matt. “The Workaday Life of the World’s Most Dangerous Ransomware Gang.” Wired.

Cimpanu, Catalin. “Disgruntled ransomware affiliate leaks the Conti gang’s technical manuals.” The Record.

Clark, Mitchell. “Nvidia says its ‘proprietary information’ is being leaked by hackers.” The Verge.

conti leads via @ContiLeaks.

CÓRDOBA, Javier; Sherman, Christopher. “Cyber attack causes chaos in Costa Rica government systems.” AP News.

Culafi, Alexander. “AdvIntel: Conti rebranding as several new ransomware groups.” SearchSecurity.

Cyberpedia. “What is the MITRE ATT&CK Framework?” Cortex.

DarkFeed via @ido_cohen2.

DarkTracer : DarkWeb Criminal Intelligence via @darktracer_int.

Davis, Griffin. “‘GTA 6’ Leaker Arrested! Authorities Claim Teenager is Linked to Lapsus$ Hacking Group.” Tech Times.

Digital Security Unit. “Special Report: Ukraine - An overview of Russia’s cyberattack activity in Ukraine.” Microsoft.

DISSENT. “AlphaV claims attack on Florida International University (updated).” DataBreaches.net.

Fadilpašić , Sead. “Conti ransomware group officially shuts down - but probably not for long.” techradar.pro.

Fardkhmanesh, Megan. “The Real Impact of the Grand Theft Auto and Diablo Leaks.” Wired.

Fox, Barbara. “Fremont County government services closed due to a cyber security breach.” KRDO News.

Ganti, Anil. “Samsung says your personal info wasn’t leaked in its recent data hack.” SamMobile.

Greenberg, Andy (2019) Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers.

Greenberg, Andy. “Destructive Hacks Against Ukraine Echo Its Last Cyberwar.” Wired.

Greig, Jonathan. “BlackCat ransomware group claims attack on Florida International University.” The Record.

Greig, Jonathan. “Louisiana authorities investigating ransomware attack on city of Alexandria.” The Record.

Greig, Jonathan. “North Carolina A&T hit with ransomware after ALPHV attack.” The Record.

Gupta, Surojoy. “All About Conti.” Cyber Security Works.

Gurevich, M (1961) The Social Structure of Acquaintanceship Networks, Cambridge, MA: MIT Press

Harbison, Mike; Renals, Peter. “Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive.” Unit 42, Palo Alto Networks.

Hill, Michael. “Cisco admits hack on IT network, links attacker to LAPSUS$ threat group.” CSO.

Jenkins, Luke; Hawley, Sarah; Najafi, Parnian; Bienstock, Doug. “Suspected Russian Activity Targeting Government and Business Entities Around the Globe.” Mandiant.

Kabelka, Laura. “Austria’s Carinthia halts passport issuance over ransomware attack.” Euractiv.

Kan, Michael. “Nvidia Confirms Company Data Was Stolen in Hack.” PC Mag.

Koczwara, Michael. “LAPSUS$ TTPs.”

Lakshmanan, Ravie. “Uber Blames LAPSUS$ Hacking Group for Recent Security Breach.” The Hacker News.

Lakshmanan, Ravie. “Uber Claims No Sensitive Data Exposed in Latest Breach… But There’s More to This.” The Hacker News.

Lyngaas, Sean. “‘I can fight with a keyboard’: How one Ukrainian IT specialist exposed a notorious Russian ransomware gang.” CNN.

Mari, Angelica. “Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes.” ZDNet.

Meta / Facebook, “Three and a half degrees of separation.”

Minggeng, Liu. “Exclusive / Delta was hacked and extorted 410 million yuan, estimated about 13,500 computers were encrypted.” CTWant News.

Newman, Lily Hay. “The Dire Warnings in the Lapsus$ Hacker Joyride.” Wired.

Panettieri, Joe. “Lapsus$ Cyberattack vs Okta, Sitel: Up to 366 Okta Customers Impacted.” MSSP Alert.

Pearson, James. “UPDATE 4-Shell re-routes oil supplies after cyberattack on German firm.” Reuters.

Peters, Jay. “Ubisoft says it experienced a ‘cyber security incident’, and the purported Nvidia hackers are taking credit.” The Verge.

Pink, Bidara. “Last month Bank Indonesia (BI) was hit by a cyber attack, but it has been resolved.” Kontan Indonesia.

Polityuk, Pavel. “EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack.” Reuters.

Ransomware Index Update: Q2-Q3 2022. Cyber Security Works, Ivanti.

Ravindran, Priya. “All about BlackCat (ALPHV).” Cyber Security Works.

Rewards for Justice via @RFJ_USA.

Rockstar Games via @RockstarGames.

Scullion, Chris. “Bandai Namco confirms it’s been hacked and says it’s investigating damage.” VGC News.

Sharma, Ax. “KP Snacks giant hit by Conti ransomware, deliveries disrupted.”

Soloman, Howard. “Canadian military provider suffered ransom attack, says news report.”

Taipei, Peng Yuwen. “Delta’s servers were hacked, and some system recovery operations are estimated to have no major impact.” Yahoo News: Taiwan.

Temple-Raston, Dina. “A ‘Worst Nightmare’ Cyberattack: The Untold Story of the SolarWinds Hack.” NPR.

The Reliants Project, “Six Degrees of Kevin Bacon.”

Tidy, Joe. “Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal.” BBC News.

Todd MicKinnon via @toddmckinnon.

Uchill, Joe. “Globant confirms falling victim to Lapsus$ extortion group.” SC Magazine.

Wadhwani, Sumeet. “Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members.” spiceworks.

Wadhwani, Sumeet. “Ransomware Group Lapsus$ Cries Foul After NVIDIA Allegedly Does a Tit-for-Tat.” spiceworks.

Werkmeister, Luke. “Ripple effects of ransomware attack against Suffolk County continue more than a week later.” The Suffolk Times.

Wolfram, John; Hawley, Sarah; McLellan, Tyler; Simonian, Nick; Veilby, Anders. “Trello From the Other Side: Tracking APT29 Phishing Campaigns.” Mandiant.

Zetter, Kim (2015) Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon.

2023
サイバー戦略ツールキット
ステークホルダーを説得する方法

サイバーセキュリティ戦略が重要である理由を情報セキュリティ部門以外の関係者に説明することで、予算確保を促す方法

in collaboration with

CSW Cyber SecurityWorks

ivanti

ivanti.com/ja/
03-6432-4180
contact@ivanti.co.jp