侵害を契機として セキュリティを強化

2018年データ漏洩/侵害ダイジェスト

verizon

概要

その日もいつもと変わらず、社外とのアクセスポイントのアラームの状態を確認していました。オフィスを出ようと出口近くの廊下を歩いていると、警察から電話がかかってきました。

そして、当社ネットワークの一部のシステムが侵害を受けている可能性があると告げられました。警察が悪意のあるものと確認したIPアドレスとこれらのシステムが通信を行っているからだといいます。

警察から、問題のIPアドレスと問題が発生している期間の情報を入手し、ITセキュリティチームと最高情報セキュリティ責任者（CISO）にコンタクトを取りました。ネットワークを確認してみると、カリフォルニア州とバージニア州にある計2つのシステムが悪意のあるIPアドレスと通信を行っていることがわかりました。

侵害の発生時における対応のヒント

インターネットにアクセスするすべてのシステムとアプリケーションのログをプロアクティブに確認する。

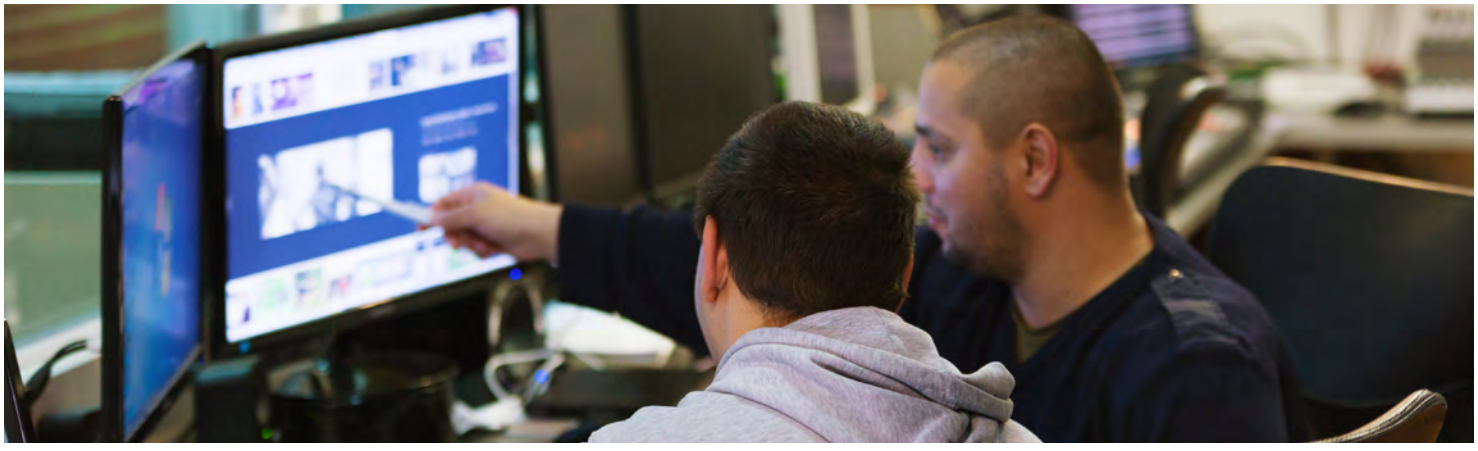
調査対応

ITセキュリティチームはさらに、これら2つのシステムに知的財産が保管されていることを突き止めました。これらが競合他社の手に渡れば、ビジネスに深刻な影響が生じてしまいます。CISOはVTRAC | Investigative Response Teamにリテーナサービスを依頼し、こうして、VTRACのメンバーがサポートで調査に加わることになりました。

VTRACの調査担当者は24時間以内に問題の各データセンターに到着し、2つのシステムからエビデンスの収集を始め、ITセキュリティチームから提供された手掛かりを参考にしながら、オープンソースのRemote Access Trojan（RAT）が活動しているのを確認しました。そして、このRATを解析したところ、悪意のあるIPアドレスのドメイン名の解決を処理していることが明らかになりました。

脅威の影響を軽減するためのヒント

あらゆる角度から体系的にセキュリティ体制を監視およびテストする。重要性の高いシステムについてセキュリティと監視を強化する。



アウトソーシングやクラウドによる問題点

もし、クラウドで使っているMicrosoft Active Directoryに障害が発生した場合、そのクラウドプロバイダーはすぐにその障害に気づくことはできるでしょうか？

多くの組織が、ローカルのIT機能をアウトソーシングしたり、クラウドに移行したりして、そのメリットを享受しています。しかし、このような場合、実際のサーバーを確認し、サーバー運用の担当者と直に顔を合わせて業務を進めることはできなくなります。

クラウドストレージはさまざまな組織で問題解決に貢献していますが、同時に新たな課題も生み出しています。たとえば、侵害を受けたある組織では、VTRAC | Investigative Response Teamが調査したところ、ローカルのテープドライブやディスク装置をデータのバックアップ先とする従来の方法をやめてしまい、コンシューマーグレードのインターネット接続であるのに、クラウドストレージをバックアップに使用していました。クラウドの利用は、1日あたり数メガバイト程度のドキュメントを保存するレベルに留めておけば、日々の業務に支障が出るような事態にはならなかったでしょう。

インシデントを取り巻く状況を調査することはできましたが、残念ながら、ある部門の作業環境全体がランサムウェアによって暗号化されてしまっていたのです。そして、用意していたオプションを確認した時点で、この組織はある事実に気付きます。業務を継続するために必要なファイルをクラウドからダウンロードするのに数週間はかかるのです。契約していたクラウドストレージプロバイダーからはほかのデータ転送の方法が提供されなかったため、身代金を支払いファイルの暗号が無事に解除されるのを祈るしか、この組織にはほかに手立てがありませんでした。

VTRAC | Cyber Intelligence Teamのサポートを得て調査を行った結果、このRATは、ATP10として知られるAdvanced Persistent Threat（APT）のグループと関係のあることがわかりました。APT10は一般に、知的財産の盗取を狙った攻撃に関係しており、マネージドサービスプロバイダー（MSP）を攻撃経路に利用します。

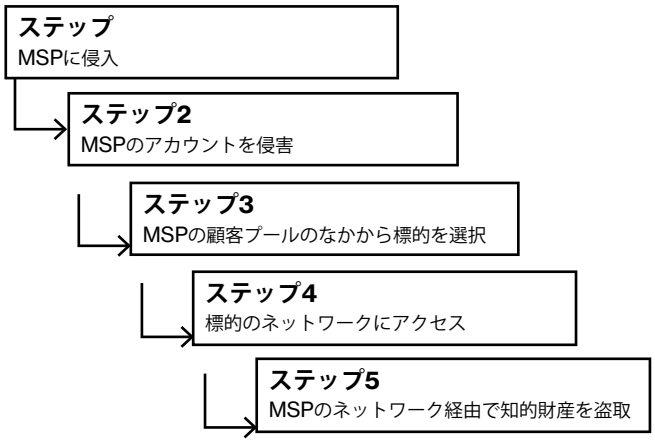


図1MSPを侵入経路とする攻撃の流れ

脅威の影響を軽減するためのヒント

- 第三者のアカウントによるすべてのアクセスを確認、調整、管理、監視する
- ローカルの管理アカウントも対象に含めて定期的なパスワードの変更を義務付け、ユーザーアカウントのセキュリティを強化する

ATP10に関係するセキュリティ侵害の痕跡（IoC）のリストをもとに、ITセキュリティチームはすぐにネットワークのスキャンを実行し、ほかにも侵害を受けた可能性のあるシステムが存在しないか確認を行いました。スキャンの結果、マルウェアに感染した複数のシステムが特定されました。しかもさらに悪いことには、マルウェアに感染したシステムの多くで、2015年から感染していた形跡が残っていました。

スキャンで見つかった最も一般的なマルウェアは、ネットワーク上に留まるためにATP10が使用するバックドアツールでした。さらに分析を進めると、管理者アカウントを含め、複数のユーザーアカウントが侵害を受けていることがわかりました。また、攻撃者は、MSPと関係のあるIPアドレス経由でもネットワークにアクセスしていました。

そして、VTRACの調査担当者は、環境への侵入経路にMSPのアカウントとネットワークが悪用されていることを突き止めます。この点は、APT10が利用する攻撃経路とも相互に関連性がありました。

ATP攻撃を示す証拠があり、また、侵害を受けていた期間も考慮すると、さまざまな認証情報も含め、ネットワーク内のほかのシステムもリスクにさらされていた可能性が大いにありました。そしてこの点が最も重要なのですが、社内の知的財産がすでに盗取されている可能性を否定できません。

検知のためのヒント

検知作業を支援するFile Integrity Monitoring（FIM）ソリューションを導入する。

この時点ではすでに、インシデント対応（IR）のステークホルダー全員が集められ、対策を立てるための作戦本部が設置されました。そして、侵害の影響を受けたすべてのシステムの特定とその再構築に取り掛かりました。さらに、適切な可視性が確保されていないことが判明したネットワークエリアについては、ロギングと監視の機能を強化しました。

侵害の発生時における対応のヒント

侵害の影響を受けたすべてのシステムを再構築し、ネットワークのロギング機能と監視機能を強化して、これまでネットワークの状態を把握できなかったエリアについても情報が得られるようにする。

ネットワーク内における攻撃者の全行動を完全に把握しようとすれば、多大なリソースが必要になるだろうとの判断から、まずは、データの漏洩の有無の確認と、ネットワークのセキュリティの確保に集中して取り組むことになりました。そして最終的には、隔離、駆除、修復の作業が功を奏し、はじめて検知で脅威が見つかって以降、APT-10に関係する新たなアクティビティはネットワーク内に存在しなくなりました。

調査の結果、データの漏洩を示す証拠は見つかりませんでしたが、侵害を受けていた期間の長さから、役員は攻撃者が知的財産にアクセスした可能性があるのではないかと懸念を抱いていました。そこで我々は、VTRACの調査担当者の協力を得て、ダークネット内を監視し、関連性の高いオンラインフォーラムやマーケットプレイスに、当社のデータが攻撃者によって「売りに出されて」いないか確認を続けました。

バックアップだけでなく復元も必要

ファイルレベルのバックアップのような構造化されていないデータであれ、データベースのような構造化されているデータであれ、あるいは仮想マシン全体であれ、クラウド環境から大量にデータを取得する方法がドキュメント化されていたとしても、多くの場合はデータをダウンロードする方法に過ぎず、これでは実用的ではありません。そして結局は、ハードドライブでデータを輸送したり、データセンターにデータを受け取りに行ったりせざるを得ません。

バックアップソリューションが正常に機能しているかどうかは、復元ができてはじめて確認できると言われています。ディザスタリカバリの訓練や情報セキュリティインシデントのシミュレーションの一環として少なくとも一度はデータが正常にリカバリできることを確認するまでは、クラウドサービスのデータリカバリが本当に機能するかどうかの保証は得られません。

得られた教訓

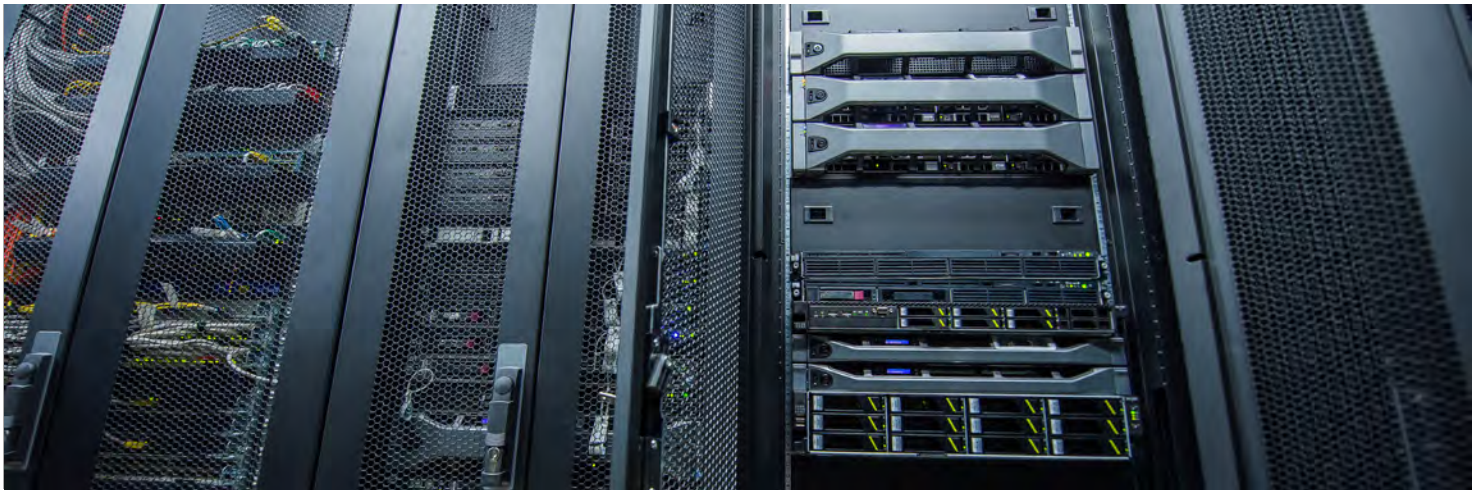
警察当局からの1本の電話で大きな問題が発覚し、当社はこれまでにない危機に見舞われることになりました。ステークホルダーの対応は的確でしたが、それでも、この事件からいくつかの教訓を学びました。

脅威の影響の軽減と防御のためのヒント

- あらゆる角度から体系的にセキュリティ体制を監視およびテストする。重要性の高いシステムについてセキュリティと監視を強化する
- 第三者のアカウントによるすべてのアクセスを確認、調整、管理、監視する
- ローカルの管理アカウントも対象に含めて定期的なパスワードの変更を義務付け、ユーザーアカウントのセキュリティを強化する

検知と対処

- インターネットにアクセスするすべてのシステムとアプリケーションのログをプロアクティブに確認する
- 検知作業を支援するFile Integrity Monitoring（FIM）ソリューションを導入する
- 侵害の影響を受けたすべてのシステムを再構築し、ネットワークのロギング機能と監視機能を強化して、これまでネットワークの状態を把握できなかったエリアについても情報が得られるようにする



認証情報の盗取 – モンスターキャッシュ

2018年データ漏洩/侵害ダイジェスト

verizon

セキュリティの現状

サイバーセキュリティの分野における一般的な傾向として、多くの場合、外部の第三者から報せを受けて組織がデータ侵害に気付くというケースが変わらず続いています。ここ最近、情報セキュリティ産業の分野では、脅威インテリジェンスを統合して、サイバーセキュリティ戦略や侵害対応の戦略を立案するという動きが見られます。

サイバーインテリジェンスチームのベライゾン脅威研究助言センター（VTRAC）は、ダークネット（匿名化されたコンテンツの共有に利用されている「簡単にはアクセスできない」インターネットの領域）の継続的な監視や、脅威インテリジェンスフィードの定期的な取得、過去のインシデントに基づくデータベース化された侵害指標の利用など、さまざまなサイバーインテリジェンスの手法を駆使して、世界各国の顧客の環境を対象に、24時間365日の体制で脅威の有無を監視しています。

蓄積された脅威インサイトを活用し、VTRACのサイバーインテリジェンスアナリストは、データ侵害の影響を軽減するための事前措置や、侵害発生時の対応アクションのサービスを顧客に提供しています。日々の業務においてVTRACのサイバーインテリジェンスアナリストは顧客から、「自身の組織は何を把握できていないのか教えて欲しい」と依頼されることが少なくありません。

脅威の影響を軽減するためのヒント

- サイバーセキュリティの脅威の現状について、また、自身の組織が属する業界を狙う脅威のアクションについて、常に最新の情報を把握する
- 脅威インテリジェンスを統合して運用し、脅威データを組織内にくまなく広める

攻撃者の目論見どおりとなった侵害を分析する場合、攻撃者の目的と能力、攻撃手法の観点から侵害を捉えることができます。このような視点に立てば、攻撃をモデル化することが可能になります。そしてさらに、組織のプロファイリングも組み合わせれば、固有のリスクレポーティングが可能となり、これは戦略的意思決定、戦術的意思決定を行ううえで有用な情報となります。ある日の午後、ベライゾンのサイバーインテリジェンスアナリストがVerizon Threat Intelligence and Response Service（TIRS）の新たな顧客にオンボーディングを行っていましたが、その際、アナリストが念頭に置いていたのがまさに上記の視点でした。

調査対応

ここである業界の組織の例を挙げます。この業界はスパイ活動を目的に攻撃を行うサイバー犯罪者の標的になることが多く、攻撃者は一番はじめの攻撃経路としてフィッシングメールを多用します。フィッシングメールでは通常、メールの受信者を誘導してユーザー名とパスワードの組み合わせを外部のアクセスポイントに入力させます。巧妙に作り込まれたフィッシングコンテンツや標的を誘導するためのリンクが使われるほか、Webサイトを改竄してそこで待ち伏せを行う手法などが用いられます。

検知のためのヒント

ログを確認し、攻撃者がどのようにして組織に攻撃を仕掛けようとしているのかを把握する。ハニーポットの構築を検討する。ハニーポットを使用すれば、特定の攻撃に的を絞った検知、防御、調査が可能になります。

サイバー犯罪者が販売や取引の対象にしているデータをベライゾンが確認したところ、最も多く扱われているデータはユーザーから盗んだ認証情報であることがわかりました。日和見的な攻撃者はときに、このデータさえあれば、さらに組織に攻撃を仕掛けることができてしまいます。

ダークネットの監視を始めたばかりのころ、このアングラネットには不正に入手されたありとあらゆる情報が存在するだろうと当然ながら考えていました。しかしそれでも、企業ユーザーのアカウントIDとパスワードの組み合わせが500を超える数でダークネットのフォーラムに投げ売りされているのを見つけたときには流石に驚きました。そして調査結果を報告してすぐに、同じ組織の別の担当者達がVTRACの調査対応チームとやり取りしていることを我々は知りました。彼らは、従業員のメールアカウントが不正に利用されている件の調査を行っていたのです。

調査担当者がフォレンジック調査を行い、侵害を受けたアカウントに関係する攻撃者のアクティビティを分析してその結果をレポートしてきましたが、そこには、このケースに関する重要な情報が記載されていました。フィッシングメール自体に加え、このメールアカウントのメール転送ログを調査し、脅威に関するこれまでの調査結果も利用した結果、犯人の素性と、犯人グループを取り巻く重要な背景情報が明らかになりました。

侵害の発生時における対応のヒント

ユーザーの認証情報について侵害が発生したとわかったら、すぐに認証情報を変更する

「$+r0^g」(strong 強い) パスワードを導入する

侵害の発生時には、すべてのユーザーアカウントについてパスワードをリセットする。以下に示す内容を盛り込んだ強力なパスワードポリシーを適用する

- すべてのユーザーを対象に個別で一意のアカウントを割り当てる。汎用的なアカウントやパスワードを使用したり、アカウントやパスワードを共有したりしない
- 新しいユーザーで初めてパスワードを設定する場合は一意の値を使用する。パスワードは最低でも8文字とし、9文字以上が望ましい。英数字の特殊文字の使用は必須とする
- 初回のユーザーパスワードはすぐに変更する。また、以後は少なくとも90日ごとに変更する
- 過去に少なくとも4回使用されているパスワードは再度利用できないようにする。ロックアウトのしきい値は6回に設定する
- 使用されていないユーザーアカウントを最低でも90日ごとに削除または無効にする。組織を離れたユーザーのアクセス権限はすぐに無効にする

さまざまな調査の結果によれば組織内で、あるユーザーアカウントが侵害受けた場合、これを契機としてこのアカウントからほかの多数のエンドユーザーに悪意のあるフィッシングメールが届くという攻撃パターンがあることが確認されています。メールのメッセージには、認証情報を盗むサイトにつながるリンクが埋め込まれており、このサイトにアクセスしたユーザーは、ユーザー名とパスワードを入力して認証を行うよう促されます。

得られた教訓

脅威インテリジェンスだけでは必ずしもデータ侵害の発生を完全に予測できるとは限りません。一方で、セキュリティに関する意思決定を下す際には、攻撃や攻撃者のモデリングを通じて得られるインサイトを考慮する必要があります。このモデリングのプロセスを活用すれば、攻撃者がどのような視点から組織に攻撃を仕掛けようとしているのかステークホルダーは把握できるようになります。また、攻撃への対処においては、脅威が影響を及ぼす範囲を特定する際の絞り込みが可能になります。フィッシングメールに対するエンドユーザーの意識を高め、フィッシングメールに遭遇したときにそれを報告できるようエンドユーザーに働きかける必要がありますが、これらに加えて、脅威の影響の緩和、検知、脅威への対処の3つの観点から以下のアドバイスをお伝えします。

脅威の影響の軽減と防御のためのヒント

- サイバーセキュリティの脅威の現状について、また、自身の組織が属する業界を狙う脅威のアクションについて、常に最新の情報を把握する
- 脅威インテリジェンスを統合して運用し、脅威データを組織内にくまなく広める

検知と対処

- ログを確認し、攻撃者がどのようにして組織に攻撃を仕掛けようとしているのかを把握する。ハニーポットの構築を検討する。ハニーポットを使用すれば、特定の攻撃に的を絞った検知、防御、調査が可能になります
- ユーザーの認証情報について侵害が発生したとわかったら、すぐに認証情報を変更する

事例：認証情報の流出による計り知れない影響

ログイン認証情報が毎日新たに盗まれ、アングラのダークネットのフォーラムやマーケットプレイスで売買されています。これらの認証情報の大半はストリーミングメディアやプライベートのEメールなどのサービスで利用されているものですが、ユーザー名とパスワードの組み合わせが盗まれた場合、その影響範囲は、お気に入りのストリーミングアプリで絶対に見逃せない最新の番組を試聴しようとしているユーザーにとどまらず、ずっと広く拡散します。

以下では、2017年に実際に起こったケースをもとに、被害の実態をお伝えします。ここでは攻撃者の手口に絞って情報を提供します。

- リモート管理アプリの認証情報が侵害を受けた結果、RAMを破壊するマルウェアがPoSシステムにインストールされてしまい、数十か所に上る小売店舗が影響を受けて、クレジットカードの情報が大量に漏洩
- 管理者アカウントの認証情報は、脆弱性攻撃を受けた外部からアクセスできるデータベースを通じて盗まれており、攻撃者はこのアカウントを使って多機能のWebシェルをインストール。ここではわずか数分のうちに匿名性の高いデータが、The Onion Router（Tor）ネットワーク上で動作している複数のシステムへと流出
- いったん管理者アカウントが侵害を受けるとそこからさらにほかのアカウントも次々と、認証情報を盗み出すマルウェアを介して認証情報が盗取される結果となった。また、初期アカウントのままの高いアクセス権限が存在したために、ネットワーク内でラテラルムーブメントが進行し、最終的には、機密性の高い人事情報ファイルが漏洩
- ある企業の財務部門では無許可で使用しているアカウントが存在したために、攻撃者はこの企業のベンダー支払い情報に簡単にアクセス。問題が検知される前にいくつもの支払い手続きが不正に行われ、すでに攻撃者のもとへ多額の送金が行われてしまっていた
- これまで以上に広まっているWebメールのフィッシング攻撃では、ある企業において、フィッシングに疑いを抱かなかった数十人の従業員が誘導されるままにログイン情報を盗取されている。そして、これら従業員のセルフサービスの給与アカウントが攻撃者のアクセスを受け、給与振込の情報が書き換えられてしまい、本来従業員が受け取るべき多額の給与が攻撃者の手に渡ってしまった

クリプトジャッキング – 不審なアウトバウンドトラフィックの裏に隠された真相

2018年データ漏洩/侵害ダイジェスト

verizon

概要

過去数年と同様に2017年もまた、暗号通貨やクリプトジャッキングに対する関心が大きな高まりを見せました。従来のビットコインに加え、新たな暗号通貨もその対象になっています。ビットコインの価値が急激に増加しているため、当然ながら、投資家以外も暗号通貨に興味を示すようになりました。2017年にVTRAC | Investigative Response Teamが調査を行ったいくつかのサイバーセキュリティインシデントでは、攻撃者の動機は、暗号通貨のマイニングを行うマルウェアを利用して金銭を稼ぐことにありました。

さまざまな種類が存在するこのマルウェアは、感染したシステムのCPUやグラフィックカードなどの処理能力を利用して暗号通貨のマイニングを行っています。暗号通貨は従来の現金のように物品の購入に利用できるほか、法定通貨に直接両替することも可能です。マイニングそのものは暗号通貨のライフサイクルにおける合法的なプロセスです。しかし、許可を得ずに他人のシステムを使用する行為は違法です。

ビットコインは最も広く知られた暗号通貨ですが、ビットコイン以外にも暗号通貨は数百種類も存在し、これらの通貨のほうがマルウェアを通じたマイニングに適している場合もあります。その理由は、ビットコイン以外の仮想通貨のほうが比較的秘匿性が高く、一般的なシステムでマイニングがしやすいためです。2017年にベライゾンが調査に携わったインシデントの場合、ビットコインのマイニングを行うマルウェアが関係したケースはごくわずかで、モネロやジーキャッシュをマイニングするマルウェアの案件が大多数を占めました。

そのようなビットコイン以外の仮想通貨に関係する1つのケースをご紹介しましょう。このケースではまず、ファイアウォールが大量のアラートを発信していると顧客から問い合わせがありました。ファイアウォールがThe Onion Router（Tor）ネットワーク向けの不審なアウトバウンドトラフィックをブロックしており、その過程でアラートが発生していたのです。この顧客は事態を掌握できていると確信していました。ファイアウォールがトラフィックをブロックしていたからです。そして、このトラフィックが発生している原因の特定を弊社に依頼してきました。また、事態を完全にコントロールできていること、データの漏洩が発生していないこと、ネットワーク内でラテラルムーブメントが起きていないことを確認して欲しいとのことでした。

侵害対応のヒント

システムのCPU使用率やネットワークにおける送受信トラフィックの急増など、異常な動きが存在しないか警戒する。ファイアウォールとネットワークアプライアンスのログを監視して不審なアクティビティが発生していないか確認する。

暗号通貨がサイバー犯罪者にとってきわめて魅力的な存在である理由

- 通貨として利用できる：技術に長けた攻撃者にとって、暗号通貨は現金と同じ価値のある存在です。物品の購入に直接利用でき、盗み出されたID情報やハッキングツール、薬物などの違法な物品をダークネットで購入する際にはうってつけです。
- 両替が容易である：暗号通貨を直接使用するつもりのない攻撃者には、暗号通貨を通常の通貨と簡単に交換できる場所が数多く用意されています。
- 移動が容易である：暗号通貨は簡単に、世界中で場所を移動することができます。電信送金や銀行での処理のように遅延が生じたり煩雑な手続きが必要になったりすることはありません。
- 匿名性が確保される：ビットコインはもともと追跡可能な暗号通貨として開発されていますが、そのロンダリングを行うサービスが複数存在します。かかる手数料はわずかであり、攻撃者の興味をそそるサービスとなっています。最近では、モネロなどのようなビットコイン以外の暗号通貨のように、プライバシーや匿名性を組み込んで開発されたものもあり、攻撃者にとって魅力的な暗号通貨となっています。
- 大きな利益が期待できる：ランサムウェア攻撃ではほとんどの場合、標的となった相手が身代金を支払うことはありませんが、暗号通貨のマイニングでは、もっと高い確率で見返りを期待できます。

侵害対応のヒント

コマンドアンドコントロール（C2）サーバーとの通信をファイアウォールレベルで遮断する。グループポリシーオブジェクト（GPO）を展開して、既知の悪意ある実行ファイルのブロックとマクロの無効化を行う。

調査対応の詳細

この顧客では弊社に問い合わせをする前に、ネットワークトラフィックの完全なパケットキャプチャ（FPC）を取得していました。また、不審なアウトバウンドトラフィックを生成しているシステムの物理メモリダンプも採取しています。ネットワークのFPCとメモリダンプを調査した結果、すぐに有用な情報が得られました。この情報を通じ、ネットワーク上にあるほかのシステムについて、侵害を受けている可能性のあるものを特定できたのです。この情報、すなわち、セキュリティ侵害の痕跡（IoC）は、システムの名前、IPアドレス、マルウェアのファイルハッシュ/ファイル名、悪意のあるプロセスの名前などから構成されています。

また、アクティブなネットワーク接続を確認してすぐにわかったことがあります。大部分のトラフィックはファイアウォールによってブロックされていましたが、Torネットワークのリソースと接続できているトラフィックも存在したのです。原因はファイアウォールのフィルタリング機能がIPアドレスのブラックリストをもとにしていることにありました。これでは、マルウェアが使用するTorアドレスを完全に網羅することはできません。さらには、

暗号通貨、モネロに関係するマイニングプールとネットワーク接続を試みる動きも確認されました。そして、悪意のあるネットワークアクティビティはすべて、コマンドラインシェルとスクリプティングツールからなるMicrosoftの「powershell.exe」プロセスから生成されていることがわかりました。このプロセスは、マルウェアの感染が確認された検体のシステムやほかのシステム上で実行されていました。

一方、ベライゾンのVTRAC | Applied Intelligence（Network Forensics）チームがFPCを調査した結果、このマルウェアは、よく知られたランサムウェアのインスタンスに類似する増殖手法を使用していることが確認されました。この手法では、「The Shadow Brokers」というハッキンググループがリークしたハッキングツールを利用しています。さらに、検体のシステムのイメージを調査したところ、既知の脆弱性パッチ（CVE-2017-0143：Windows SMBリモートコード実行の脆弱性）が適用されていないことが判明しました。これでは、マルウェアの増殖を許してしまいます。顧客は適切なセキュリティが確保されていると信じていたのに、現実はまったく違っていたのです。

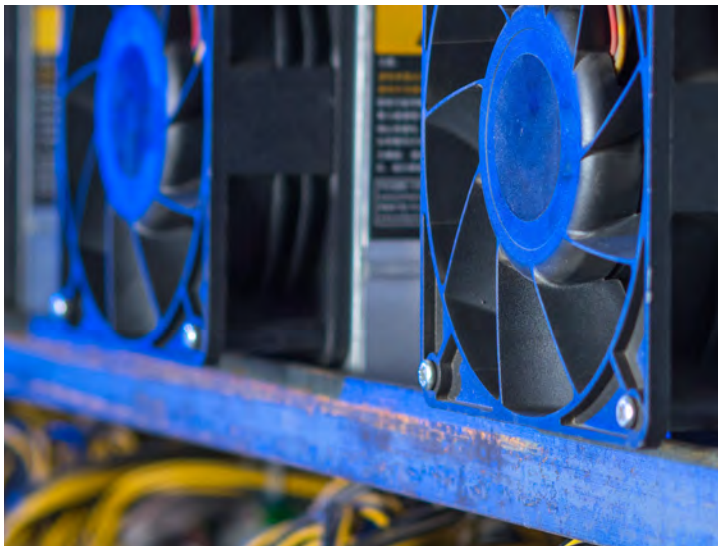
また、ファイアウォールのログを解析した結果、Torネットワークと通信を行っているシステムがほかにもあることがわかりました。これらのシステムも修復を施さねばなりません。ベライゾンの支援を受けながら、この顧客は修復プランを実施しました。このプランでは、マルウェアの検体をアンチウイルスベンダーに提供するとともに、脆弱性パッチをシステムに適用し、マルウェアを駆除しました。また、レガシーの運用システムをもとに主要なシステムの再構築を行っています。

侵害対応のヒント

マルウェアの分析を行い、機能を把握して、脅威の検知と脅威への対処、影響の軽減と防御に役立てる。

暗号通貨に関係した攻撃

- 暗号通貨のマイニング：この記事で説明したように、多くの場合、この攻撃の目的は、暗号通貨のマイニングを直接行い違法な利益を上げることにあります。
- 暗号化マルウェアによる攻撃/ランサムウェア攻撃：ここ数年のあいだに多くなった攻撃です。この攻撃では通常、利用資格のあるファイルの所有者がファイルを利用するのを暗号化により妨害します。身代金が暗号通貨で支払われた場合に限り、暗号を解除するキーが攻撃者から提供されます。
- 暗号通貨のウォレットの盗取：通常、暗号通貨は、個人のシステムやオンラインウォレットサービス上のウォレットファイルに保管されます。これらのウォレットには暗号通貨を制御するプライベートキーが含まれており、そしてこのプライベートキーこそ、サイバー犯罪者の興味をそそる標的なのです。ウォレットファイルの盗取を狙い、オンラインウォレットサービスの認証情報を取得しようとフィッシング攻撃を仕掛けるマルウェアの数は増加するばかりです。
- 暗号通貨ウォレットサービス/ブローカーに対する分散DoS攻撃：これらのDDoS攻撃は暗号通貨のウォレットを使用不能するものです。たとえば、ビットコインの価格が下落しているとしたら、できるだけ早くビットコインを売却すべきですが、それができなくなってしまいます。



得られた教訓

調査を進めていくなかで、ネットワーク内の数百に上るシステムにおいて、Microsoft Windowsの最新のパッチが適用されていないことがわかりました。迅速に適切なパッチを適用していれば、今回の問題は回避することができました。

今回のケースでは、マルウェアの狙いは暗号通貨のマイニングを実行することにありました。しかし、マルウェアがもっと悪意のあるものであったとしたら、同じ脆弱性を突いて、ビジネスにずっと大きな被害をもたらしたことでしょう。

脅威の影響の軽減と防御のためのヒント

- 定期的なセキュリティの評価を行う。サンドボックス機能、Webブラウザの分離、特定のアクティビティを対象とした仮想化の観点をベースに、防御アーキテクチャの設計を評価する。
- 脆弱性パッチの管理プログラムを確立する。セキュリティパッチは速やかに適用する。パッチが適切に適用されているかどうかを確認する。
- 最新のシグニチャを実装したホストベースのエンタープライズアンチウイルスソリューションを導入し、脅威を発生時点で検知、駆除する。
- 重要なシステムやサーバーを対象に、ファイル整合性管理（FIM）ソリューションやアプリケーションホワイトリスティング（AWL）ソリューションを導入する。侵入防止システム（IPS）のルールを追加する。インターネットのブラウジング機能を無効にする。
- Torネットワークなど、暗号通貨のマイニングプールとのインターネット接続を行うビジネス上の相応な理由が存在しない場合は、接続をブロックしたり、接続のアラートを発信したりする。
- できるだけローカルでの管理は行わないようにする。Webブラウジングでは、標準ユーザーとしての使用を義務付ける。また、それ以外の利用シーンで特権ユーザーとしての使用を行う場合は、エスカレーションを義務付ける。

検知と対処

- システムのCPU使用率やネットワークにおける送受信トラフィックの急増など、異常な動きが存在しないか警戒する。ファイアウォールとネットワークアプライアンスのログを監視して不審なアクティビティが発生していないか確認する。
- コマンドアンドコントロール（C2）サーバーとの通信をファイアウォールレベルで遮断する。グループポリシーオブジェクト（GPO）を展開して、既知の悪意ある実行ファイルのブロックとマクロの無効化を行う。
- マルウェアの分析を行い、マルウェアの機能を把握して、脅威の検知と脅威への対処、影響の軽減と防御に役立てる。
- ネットワーク全体を対象として定期的に脅威ハンティングを行い、通常のサイバーセキュリティツールでは検知できない脅威アクティビティを見つけ出す。、
- 暗号通貨に関するシナリオを想定したインシデント対応のプレイブックを作成する。効果的、効率的な対応が取れるよう、インシデント対応の担当者のトレーニングを行う。

暗号通貨のマイニングマルウェアを分析する際のポイント

分析を通じてマルウェアの機能を把握する場合、以下のポイントを検討します。

- キルスイッチや構成ファイルを明確化し、これらがマルウェアの機能に与える影響を把握する。
- C2サーバーに加え悪意のあるリモートサーバーについても、ファイアウォールやプロキシサーバーでブロックする機能を評価する。
- 悪意のあるドメイン名をDomain Name System（DNS）レベルでブラックリスト登録する機能を評価する。
- 新たな検知ルールを作成する。YARAルールやファイルハッシュなど、ネットワーク侵入検知システム（nIDS）やホスト侵入検知システム（hIDS）のシグニチャを使用し、脅威ハンティングを行う。
- マルウェアの自己増殖メカニズムを特定する。ベンダーへの報告、脆弱性パッチの適用など、是正措置を講じる。
- 持続メカニズムを一掃する。
- マルウェアが使用している暗号化メカニズムを割り出し、暗号化されたファイルを元に戻す方法を突き止める。

サイバー諜報活動 – 一通のフィッシングメールがもたらした甚大な被害

2018年データ漏洩/侵害ダイジェスト

verizon

概要

諜報活動というものはすでに何千年も前から存在していましたが、デジタルシステムの機密データや知的財産のデータを狙ったサイバー諜報活動は比較的新しい概念です。最近、VTRAC | Investigative Response Teamは、ある製造業の顧客からサポートの要請を受けました。データ侵害を受けている可能性があると警察当局から連絡を受けたというのです。

最高情報セキュリティ責任者（CISO）は、社内環境のシステムと通信している可能性のある国外のIPアドレスがいくつか存在すると知らされていました。そして、ベライゾンは、このCISOからサポートの要請を受けました。すぐに本社に来て疑わしいIPアドレスを調査して欲しいというのです。

侵害対応のヒント

- 警察当局が侵害の事実を把握していない場合は、速やかに警察当局に通報する。また、可能であれば、第三者に調査を依頼する。
- 主要なサーバーとメールについてアクセスログを収集する。また、システムをシャットダウンする前に、対象範囲の揮発性データやシステムイメージも収集する。そして、これらを速やかに調査する。
- 内部と外部のインテリジェンスリソースを活用し、攻撃者の手口やセキュリティ侵害の痕跡（IoC）に関し、すぐにアクションに活かせるインテリジェンスを整える。

調査対応の詳細

ベライゾンのVTRAC I Investigative Response Teamの調査担当者は深刻な事態が予想されることを認識していました。チームは翌日、顧客の本社に赴きます。まずは顧客のCISOと打ち合わせをしてから、侵害を受けたと思われるサーバーなどの機器を対象にトリアージを開始しました。そして、メモリダンプとディスクのフルイメージを複数採取して、すぐにエビデンスデータの洗い出しに着手しました。

同日の夕刻、我々は、プライマリシステムの1つに特殊なソフトウェアプログラムが存在することを突き止めます。このプログラムは、侵入テスターやITセキュリティプロフェッショナルにはよく知られた「Mimikatz」と呼ばれる強力な認証情報盗取ツールです。Microsoft Windowsの認証（LSASS）を担うプロセスのメモリを探り、平文のパスワードやNT LAN Manager（NTLM）のハッシュを引き出します。

これらの情報があれば、攻撃者はネットワーク内の複数のシステムを横断することが可能です。この情報は侵害の全容を解明するうえで不可欠なものであるとわかっていたため、すぐに当社のVTRAC | Cyber Intelligence Teamにファイルのメタデータを送りました。

翌朝、VTRACのインテリジェンスアナリストから連絡がありました。アナリストによれば、米国の企業に攻撃を仕掛けているある特定の国が、繰り返しこのファイルを使用しているといいます。さらに調査を進めた結果、攻撃者がある従業員を狙って攻撃を仕掛けていたこともわかりました。この従業員は、ITシステムの上級管理者で、エンジニアリング部門のドメインコントローラーを含む複数のサーバーにアクセスすることができたのです。

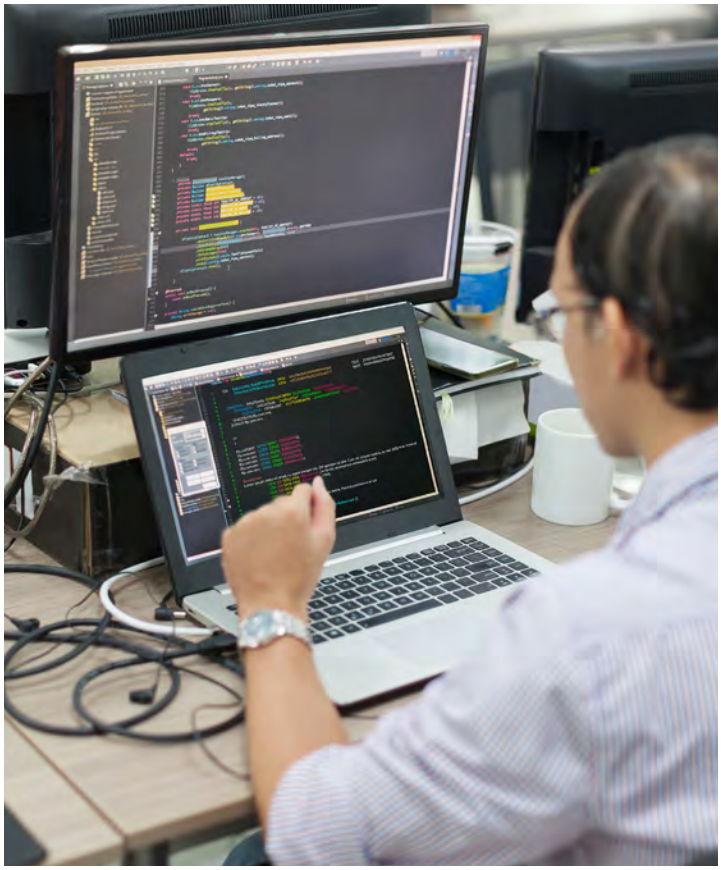
また、攻撃に使われた主要なコンポーネントも明らかになりました。具体的には、このシステム管理者のもとへ、401Kプランに関する情報を装ったフィッシングメールが送り付けられており、その内容はプランの管理者から送付されたように見えるものでした。メールにはPDFファイルが添付されており、このファイルを開くと密かにMimikatzのインストールが行われる仕組みになっていたのです。

そして攻撃者は管理者の認証情報を盗み出してラテラルムーブメントを行い、複数のドメインコントローラーやエンジニアリングファイルサーバーにアクセスしており、その際に、エンジニアリング部門の複数のサーバーやファイル共有の状況を体系立てて探ることができるようになっていました。

さらにエビデンスデータを詳しく解析した結果、機密扱いの知的財産であるCAD図面や回路図、エンジニアリング設計ドキュメントが約3,000件、あるFTPサイトにアップロードされていることが判明しました。このサイトが存在する国が侵害を行ったのは間違いありません。

この顧客は大量のCAD図面を移動するためにFTPを大規模に使用していたため、攻撃者はこれに紛れて比較的容易にドキュメントを盗み出すことに成功しています。

攻撃者は小さなチャンクとしてデータを送信し、データ漏洩防止（DLP）の検知を逃れていました。この際に利用されたのがWinRARアーカイブツールです。攻撃者が好んで使用するソフトウェアユーティリティの1つで、盗み出したデータを、これを使ってアーカイブファイルにパッケージングし外部に持ち出していたのです。アーカイブはパスワードで保護されており、DLPシステムからは中身のデータが確認できないようになっていました。



脅威の影響を軽減するためのヒント

- サイバーセキュリティに対する認識を高めるためのトレーニングをユーザー向けに少なくとも年1回は行う。疑わしいメールに気を配り、そのようなメールを受信した際にはその旨を報告するよう、組織に促す。
- 外部から届いたメールはそれとわかるように目立たせる。外部から送信されたメールである旨を示すマーカーをメールの「件名」に付与するようにする。
- 単一要素認証をやめて多要素認証を導入する。社内環境にリモートで接続する場合に仮想プライベートネットワーク（VPN）の使用を義務付ける。

得られた教訓

この件で得られた教訓のまとめとして、脅威の影響の軽減と防御の側面ならびに検知と対処の側面から以下のアドバイスをお伝えします。

脅威の影響の軽減と防御のためのヒント

- サイバーセキュリティに対する認識を高めるためのトレーニングをユーザー向けに少なくとも年1回は行う。疑わしいメールに気を配り、そのようなメールを受信した際にはその旨を報告するよう、組織に促す。
- 外部から届いたメールはそれとわかるように目立たせる。外部から送信されたメールである旨を示すマーカーをメールの「件名」に付与するようにする。
- 単一要素認証をやめて多要素認証を導入する。社内環境にリモートで接続する場合に仮想プライベートネットワーク（VPN）の使用を義務付ける。

検知と対処

- 警察当局が侵害の事実を把握していない場合は、速やかに警察当局に通報する。また、可能であれば、第三者に調査を依頼する。
- 主要なサーバーとメールについてアクセスログを収集する。また、システムをシャットダウンする前に、対象範囲の揮発性データやシステムイメージも収集する。そして、これらを速やかに調査する。
- 内部と外部のインテリジェンスリソースを活用し、攻撃者の手口やセキュリティ侵害の痕跡（IoC）に関し、すぐにアクションに活かせるインテリジェンスを整える。

Eコマース分野におけるセキュリティ侵害：フラタバイ効果

2018年データ漏洩/侵害ダイジェスト

verizon

概要

コールセンターには、オンラインショッピングの決済トラブルを訴える電話が次々とかかってきました。弊社Webサイトの決済ページで支払いの処理をしようとすると「画面がフリーズ」してしまう問題が頻発しているようでした。ネットショッピングのトラブルを扱う責任者であった私はすぐに警戒しました。この事態はネットショッピングの売上に影響を及ぼす可能性があったからです。

しかも問題は最悪のタイミングで起こりました。ホリデーシーズンに入っていたため、ITスタッフは、Webアプリケーションに変更を加えたり、本番環境に手を入れたりするのを禁じられていたのです。

まず最初に思いついたのがポイントツーポイント暗号化（P2PE）設定のバグでした。これに関係した問題が発生していると考えたのです。決済の際に、ここでクレジットカードのデータを処理していたからです。クレジットカードのデータは弊社のシステムに送られる前に暗号化されるので、カードの不正使用のリスクが軽減されます。

まずは、開発環境で決済処理をテストしてみました。何度もテストをしてみましたが、決済処理に問題は見つかりません。データの入力も出力も正常に処理できているように見えます。

これには混乱しました。開発環境の決済処理は本番環境のそれと完全に同じはずだったからです。変更管理プラットフォームには何の変更記録もありませんでした。ここ数週間のうちに本番プラットフォームに変更を加えた従業員は誰もいません。

そこで、本番環境に的を絞って調査を行うことにしました。そして実際の環境で決済処理を行うと、ページがフリーズしました。

検知のためのヒント

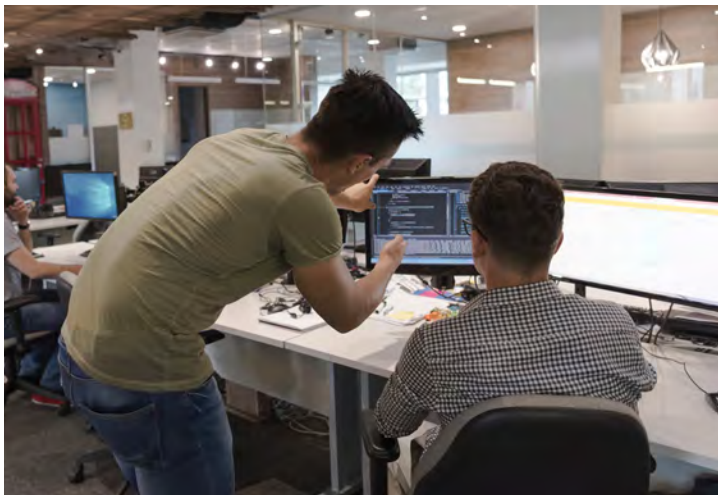
通常は検知できないコードの変更をプロアクティブに検出できるよう、慎重な扱いを要するコードの整合性チェックを定期的に行う。Webサイトに加えられた変更を追跡、監視するツールを実装する 。

次は、決済処理に関係する開発環境のページを本番環境のそれと突き合わせ、ハッシュチェックを行いました。もしも開発環境と本番環境のあいだで何か違いがあるとすれば、問題の生じているページをハッシュチェックで特定できるはずです。決済処理のWebページのハッシュには確かに違いがありました。クレジットカードの処理に関係するJavaScriptコードが埋め込まれていたのです。

ざっと比較したところ、本番環境のページには5行のコードが挿入されていることがわかりました。とりあえずコードを確認して判明したのは、シンプルなRegexの文字列が使われていることでした。これを通じて、クレジットカードのデータ文字列を探し出し、外部のドメインに送信しようとしていたのです。

脅威の影響を軽減するためのヒント

P2PEソリューションだけでなく、決済処理全体を評価する。詳細な防御アプローチのできる制御機能をあらたに導入する 。



調査対応の詳細

このような事実が明らかになる前に、弊社の最高情報セキュリティ責任者（CISO）はすでにベライゾンのVTRAC | Investigative Response Teamに連絡を取っていました。VTRAC | Investigative Response Teamの調査によれば、攻撃者はこれ以前にすでに弊社の決済処理アプリケーションにアクセスしていたのです。

アプリにアクセスした攻撃者は、アプリの決済処理のコードに変更を加えています。決済処理が行われているあいだ、問題のJavaScriptコードはWebブラウザ経由でクレジットカードのデータをリモートのインターネットドメインにリダイレクトしていました。P2PEを使用していましたが、このソリューションは今回の攻撃では何の役にも立ちませんでした。データが弊社の決済処理システムに渡される前に侵害が発生していたからです。

しかし、悪意のあるこのコードは処理に失敗しており、Internet Explorerをハングさせてしまったのです。このコードのセクションは消去しました。そして、今後はコードを改変されないよう、従来より強力なアクセス制御の機能を実装しています。

脅威の影響を軽減するためのヒント

システムベースの制御機能を実装して、不正アクセスを防止する。必要な場合にのみ管理者アカウントを使用するようなポリシーやプラクティスを導入する 。

検知のためのヒント

重要性や機密性の高いシステムにアクセスしているアカウントのログを定期的に確認し、不自然に権限を昇格しているアカウントのアクティビティを検知する 。

Eコマース業界におけるサイバーセキュリティのトレンド

現在、Eコマース業界は、さまざまなソースから多岐にわたるサイバー攻撃を受けています。サイバーセキュリティのプロフェッショナルは顧客の個人情報を保護し、企業ブランドの信頼性を守らねばなりませんが、今の状況は彼らにとって厳しいものがあります。Eコマース業界が直面しているサイバーセキュリティの脅威には、次のようなものがあります。

- DDoS攻撃：分散DoS（DDoS）攻撃は、標的型、無差別型のどちらの攻撃パターンもありえます。Eコマースの企業が利用しているサービスが攻撃を受けた場合、その企業のサービスにも影響が生じます。2017年にDynDNSがDDoS攻撃を受け、EtsyやShopify、Twitter、PayPal、Pinterestのサービスが停止したケースがまさにこれに該当します 。
- HTTPSを通じたデジタルマルウェア攻撃：Eコマースプラットフォームでは、顧客の個人情報やクレジットカードのデータをSSL（Secure Sockets Layer）/TLS（Transport Layer Security）暗号化を用いて保護していますが、この方法ももはや一般的となり、攻撃者はこれらの暗号化チャネルを悪用してマルウェアを送り込んできます。このような状況に直面したEコマース業界では、パケットを詳細に検査できるファイアウォールの導入を進め、攻撃者にHTTPSのチャネルを利用されないようにしています。
- 標的型APTフィッシング攻撃：APT（Advanced Persistent Threat）攻撃でよく使われる手法の1つに、APTフィッシングメールがあります。この手法では、標的となるユーザーを欺き、マルウェアをダウンロードさせます。いったん攻撃者にアクセスを許すと、データの盗取、データの不正使用などの被害を一定期間受けることになります。そして、単一の決済処理に関する侵害よりもずっと大きなリスクとなるのが、Eコマースプラットフォームの管理者アカウントの認証情報に関する侵害です。これが発生すると、データの漏洩と金銭的な損失が大規模に生じるおそれがあります。

得られた教訓

問題発生の当初より明らかになったことの1つは、ポリシーベースの制限をかけても不正アクセスを防ぐことはできないという事実です。本番環境の設定を変更されないようにするため複数のポリシーを設定していましたが、物理的なシステムも論理的な制限も、重要性や機密性の高いシステムへの不正アクセスを防げず、これらシステムの内容の書き換えを許してしまいました。

幸いにも、我々は早期に問題を収束させることができました。しかし、今回の侵害は繁忙期に発生しているので、一歩間違えば、大規模な顧客ベースを失うところでした。このことを念頭に置き弊社では事態が収束した時点で、取るべきアクションを事後レビュー（AAR: After Action Review）の一環としてリストにまとめました。弊社のAARから得られたいくつかの特に重要なポイントを以下に示します。

脅威の影響の軽減と防御のためのヒント

- P2PEソリューションだけでなく、決済処理全体を評価する。詳細な防御アプローチのできる制御機能をあらたに導入する 。
- システムベースの制御機能を実装して、不正アクセスを防止する。必要な場合にのみ（2要素認証で）管理者アカウントを使用するようなポリシーやプラクティスを導入する。

検知と対処

- 通常は検知できないコードの変更をプロアクティブに検出できるよう、慎重な扱いを要するコードの整合性チェックを定期的に行う。Webサイトに加えられた変更を追跡、監視するツールを実装する。
- 重要性や機密性の高いシステムにアクセスしているアカウントのログを定期的に確認し、不自然に権限を昇格しているアカウントのアクティビティを検知する。

産業用制御システムを標的とするサイバー攻撃

2018年データ漏洩/侵害ダイジェスト

verizon

概要

その電話を受けたのは夜も更けたころでした。電話の相手は「これからオフィスに来て欲しい」と言っていました。セキュリティオペレーションセンター（SOC）のリードアナリストとして重要インフラ保護（CIP）の業務を担当していた私は、仕事が終わってから呼び出しを受けることに慣れてしまっていましたが、電話口で次の言葉を聞いて、事態がいつもとは違うと気づきました。警察当局から連絡があって、弊社がセキュリティ侵害を受けている可能性が高いと伝えてきたというのです。

オフィスに着くと、そこは混乱状態になっていました。仮に侵害を受けていたとしても、その原因がわからなかったからです。最悪の事態を想定し、通常の社内チャンネルでのコミュニケーションは避けるようにしました。この結果、オフィスの外にいる同僚との情報共有が難しくなってしまいました。

また、FBIを通じて知りえた情報はトラフィックライトプロトコル（TLP）の「レッド情報（関係者外秘）」扱いとし公に共有できないとも知らされていました。

我々が最初に入手したセキュリティ侵害の痕跡（IoC）は、1つのメールアドレスでした。警察当局によれば、このメールアドレスは、エネルギー業界のさまざまな組織を標的としたスピアフィッシング攻撃に使われているといいます。

メールアプライアンスを詳しく調査すると確かにそのアドレスがいくつかのメールを発信していることがわかりました。メールの発信先は、弊社発電所の役員やリードエンジニアです。

メールには、「レジメ」とうタイトルのWordファイルが添付されており、受取人に内容の確認を求めるかたちになっていました。しかし、この添付ファイルをマルウェアの分析環境で調査してみましたが、何も怪しいところは見つかりません。Webリンクもマクロもありません。子プロセスの生成も確認できませんでした。私は、VTRAC | Investigative Response Teamに支援要請の電話をしました。

侵害対応のヒント

- ユーザーアカウントの生成や変更をはじめとした構成変更について、ロギング機能、アラート機能を強化する。PowerShellスクリプトがトリガーするアクションについてのロギング機能を強化する。
- サイバーセキュリティの問題が発生する前に、セキュアで信頼性の高い代替のコミュニケーション手段を準備しておく。このコミュニケーション手段をインシデント対応（IR）プランに盛り込む。

トラフィックライトプロトコル（TLP）のカテゴリ

- TLPレッドは、最も重要性が高く、最も公開が制限されている情報です。その公開は、これを知る必要のある個人だけに厳しく制限されています。
- TLPアンバーは、2番目に重要性の高い情報です。その公開は一部の個人や組織に制限されています。
- TLPグリーンは、3番目に重要性の高い情報です。その公開は、これを知る必要のあるコミュニティだけに制限されています。
- TLPホワイトは、最も公開の制限が緩い情報です。公開の制限はなく、この情報は一般に公開することが可能です。

TLPの定義と使用方法の詳細については、US-CERTのWebサイト（https://www.us-cert.gov/tlp）を参照してください

調査対応の詳細

不審な添付ファイルの調査に着手したVTRACの調査担当者はすぐに問題を特定しました。攻撃者はインターネット上にあるMicrosoft Wordのテンプレートを悪用し、コマンドアンドコントロールサーバーと通信を行っていたのです。この手法は、悪意のあるペイロードのダウンロードにMicrosoft Wordを利用する新手の手口で、後に「テンプレートインジェクション」と呼ばれるようになりました。

Wordドキュメントは開くと、攻撃者のサーバーにホストされたサーバーメッセージブロック（SMB）プロトコルを介して悪意のある特定のテンプレートを探しに行きます。そして、悪意のあるテンプレートがダウンロードされると、このテンプレートは、ユーザーアカウントの認証情報を盗取するMicrosoft PowerShell（コマンドプロンプト）インスタンスをマクロで生成します。

ターゲットとなったユーザーの誰もが、過去に攻撃者とメールをやり取りしていないことがわかりました。しかし、これらのユーザーは皆、広く使用されているプロフェッショナルネットワーキングソーシャルメディアのサイトにプロファイルを詳しく公開していました。攻撃者はこれらのプロファイルを悪用して標的を選別していたとみられます。

これらの新たな情報を得た我々は標的となったユーザーにアカウントのパスワードを変更するようすぐに依頼しました。そして、調査に使用すべく、これらのユーザーに関するシステムデータと揮発データの収集に取りかかりました。

プラント内の運用テクノロジー（OT）システムにアクセスできるエンジニアが数名存在しましたが、このシステムにアクセスするには、きわめて高い権限が必要でした。そしてこのシステムに関して問題が生じたのです。SOCのアナリストは一人として、プラントシステムへのアクセスに必要な、北米電力信頼度協議会（NERC）による重要インフラ保護（CIP）のトレーニングを受けていなかったのです。

早急な対応が必要でありながら、これらのシステムにアクセスできるSOCアナリストがいなかったので、セキュリティ侵害の痕跡（IoC）を探し出すPowerShellスクリプトを作成して、USBデバイスにロードすることにしました。そして、適切なアクセス権限のあるプラントエンジニアを選び出し、1回限りの例外としてUSBデバイスをこのエンジニアに託しました。USBをOTシステムに接続してスクリプトを実行し、IoCを探索してもらったのです。

脅威の影響を軽減するためのヒント

- OTネットワークをはほかのネットワークと分離する。OT用の専用システムを導入する。メールやインターネットへのアクセス機能は無効にする。OT環境よりもセキュリティレベルが低いネットワークへのアクセスも遮断する。
- 未知のパブリックインターネットスペースに対するSMBコネクションをブロックするファイアウォールルールを導入する。PowerShellの子プロセスを生成する、Microsoft Officeなどのユーザーアプリケーションを検出できるよう、検知機能を付加する。
- ソーシャルネットワークサイトに機密性の高い情報を投稿することで生じるセキュリティリスクを従業員によく理解させる

侵害対応のヒント

業界で求められているトレーニングや認定の要件を満足できるようにする。セキュリティオペレーションセンター（SOC）のアナリストやインシデント対応の担当者に自社の産業用制御システム（ICS）の環境を詳しく伝える。ICS関連のサイバーセキュリティインシデントに対応できるよう、トレーニングを行う。

得られた教訓

新たな侵害の痕跡は確認されませんでしたが、インシデント対応のアプローチで改善すべき点をいくつか見出しました。そして、早急な実現を目指し、事後レビュー（AAR）において以下のアクションに着手しました。

第一に、社内ネットワークとは別に、代替のコミュニケーション手段を確立しました。社内ネットワークに侵害が起きても、これでSOCアナリストは「安全なコミュニケーション」が可能です。

そして次に、インターネット上に公開する情報に注意を払うようエンドユーザーに教育を行いました。攻撃者はネット上の情報を悪用して「最も攻撃すべき」標的を選別するからです。

さらには、未知のパブリックアドレスとの外部SMBコネクションを遮断するファイアウォールのルールも導入しました。

そして最後に最も重要なこととして、SOCアナリストと、サイバーセキュリティインシデント対応担当者全員に、NERCによるCIPトレーニングの受講を義務付けました。また、新たなセキュリティ施策として、追加のバックグラウンドスクリーニングを受けることも必須事項として課しました。

脅威の影響の軽減と防御のためのヒント

- OTネットワークをはほかのネットワークと分離する。OT用の専用システムを導入する。メールやインターネットへのアクセス機能は無効にする。OT環境よりもセキュリティレベルが低いネットワークへのアクセスも遮断する。
- 未知のパブリックインターネットスペースに対するSMBコネクションをブロックするファイアウォールルールを導入する。PowerShellの子プロセスを生成する、Microsoft Officeなどのユーザーアプリケーションを検出できるよう、検知機能を付加する。
- ソーシャルネットワークサイトに機密性の高い情報を投稿することで生じるセキュリティリスクを従業員によく理解させる。

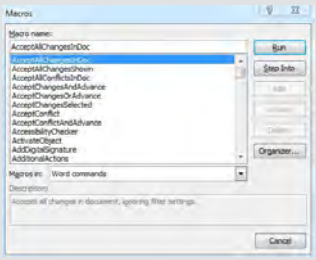
検知と対処

- サイバーセキュリティの問題が発生する前に、セキュアで信頼性の高い代替のコミュニケーション手段を準備しておく。このコミュニケーション手段をインシデント対応（IR）プランに盛り込む。
- ユーザーアカウントの生成や変更をはじめとした構成変更について、ロギング機能、アラート機能を強化する。PowerShellスクリプトがトリガーするアクションについてのロギング機能を強化する。
- 業界で求められているトレーニングや認定の要件を満足できるようにする。セキュリティオペレーションセンター（SOC）のアナリストやインシデント対応の担当者に自社の産業用制御システム（ICS）の環境を詳しく伝える。ICS関連のサイバーセキュリティインシデントに対応できるよう、トレーニングを行う。

マクロ、ハイパーリンク、プロセスに十分な注意を払う

Microsoft Wordのマクロ

マクロとは、複数の機能をグループ化し、繰り返し使用する処理を自動化するものです。



攻撃者はマクロの機能を悪用してシステム上でマルウェアを実行します。

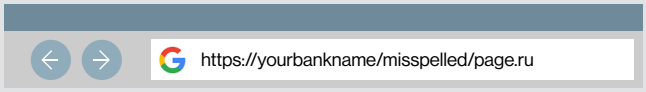
サイバーセキュリティの観点からは、マクロの使用を禁止または制限することを検討してください。

Webサイトのハイパーリンク

ハイパーリンク（リンク）を使用すると、マウスをクリックするだけで、ドキュメント、Webページ、メールにアクセスすることができます。

いつもご利用ありがとうございます。
ご利用の口座のパスワードは有効期限が切れています。www.yourbankname.com から今すぐパスワードを変更してください。
今後とも××銀行をよろしくお願いいたします。

攻撃者はハイパーリンクを悪用し、ユーザーにハイパーリンクをクリックさせて、それにより、密かにマルウェアがインストールされるようにします。



マウスカーソルをメールのリンクに合わせ、リンク先のWebサイトが正規のサイトであるかどうかを確認します。ドメイン名が一致することを確認してください。

プロセスの実行

プロセスとは、アプリケーションを実行中のインスタンスを意味します。「子プロセスの生成」とは、あるプロセス（「親プロセス」）が別のプロセスを生成することを意味します。

マルウェアがシステム上で実行されると、プロセスが生成されます。

```
Name          Process Id
Idle                   0
  System               4
    smss             280
csrss                392
wininit              432
  services           536
    svchost          604
explorer            2308
  cmd               3852
    badness         3876
```

不審なプロセスをチェックする場合は、時刻、親プロセス、子プロセス、アプリケーション自体など、あらゆる背景情報に気を配る必要があります。

認証情報を狙った脆弱性攻撃

2018年データ漏洩/侵害ダイジェスト

verizon

概要

私はある大手の企業で最高執行責任者（COO）の職にあります。海外旅行から帰宅してMourning Dove Investments（MDI）の取引口座をチェックしたのですが、すぐにショックを受けることになりました。数日前に2回の送金が行われており、口座の残高が減っていたのです。1回目が150,000ドル、2回目が160,000ドルでした。

検知のためのヒント

ポート転送やアカウントのオーナーシップなどについてアカウントの設定が変更された場合にアラートが発信されるよう設定を行う 。

不安になった私はMDIに問い合わせました。MDIが確認したところによれば、2回の送金は香港のある銀行向けに行われているといいます。MDIは手順に従い、私の自宅に電話をかけ、妻に送金の処理をしてもよいか確認したとのことでした。確認の際には、妻の免許書の番号と、セキュリティ上の「秘密の質問」についても尋ねたといいます。質問の答えは最近の旅行に関するものでした。

侵害対応のヒント

情報の不正使用による被害を受けた場合は、警察当局など適切な関係機関に報告を行う。

しかし妻は、MDIから何の電話もかかってこなかったと言っています。自宅の電話がスプーフィングされているのではないかという不安がすぐに頭をよぎり、私はVTRAC | Investigative Response Teamに連絡を取りました。

調査対応の詳細

転送などのような、自宅の電話で使用しているオプションや機能にはどのようなものがあるかと、VTRACの調査担当者から尋ねられましたが、はっきりと覚えていなかったので、電話会社に問い合わせてみなければなりませんでした。

一方、妻によれば、数か月ほど前に家の電話を取ったときに、3、4秒間、高音の雑音が聞こえてからダイアルトーンに変わったことがあるといいますが、今まで気にとめていなかったそうです。私はVTRACの調査担当者に、直近の通話明細の入手を許可しました。

さらに私は、タブレットが侵害を受けていないか、心配になりました。タブレットには、秘書からのメールや旅程、スケジュール、クレジットカードの使用履歴をはじめとした扱いを注意すべきであろう情報を保存していたからです。また、旅行中に私はタブレットで車両管理局（DMV）のWebサイトにアクセスし、新たに妻の運転免許証の申請手続きをしましたが、この手続きをホテルのインターネット回線を通じて行っていました。記憶する限り、妻の運転免許証の情報をインターネット経由で車両管理局に送ったのはこれが最後です。もちろん、これは正規の手続きです。

モバイルデバイスのセキュリティ：IT部門向けのベストプラクティス

モバイル化が進み、テクノロジーが絶えず進化するなかで、スマートフォンを通じて処理、保存、やり取りされる重要なデータの量は増えるばかりです。ところが企業は、ネットワークやシステムについてはサイバーセキュリティの取り組みに力を入れる一方、モバイルデバイスのセキュリティは軽視しがちです。しかし、以下に示すような簡単なルールやポリシーを取り入れれば、モバイルデバイスをデータ侵害から保護することができます。

- モバイルデバイス管理（MDM）コンソールを利用して、会社所有のデバイスとBYODデバイスの両方に一元的なルールとポリシーを適用する。
- 社内情報のアクセスに使用するデバイスには、スクリーンロック機能の使用とパスコードの設定を義務付ける。パスコードは8文字以上とし、大文字、小文字の英数字、特殊文字を含めるようにする。
- 機密性の高い情報の保存、転送、処理を行う場合は、情報が保管中、移動中のいずれの状態にあっても、暗号化の機能を有効にする。
- 使用を許可したすべてのモバイルデバイスアプリについてセキュリティ監査を行う
- ユーザーと会話する機会を設ける：ユーザーはセキュリティに関する手続きを省略する抜け道を知っています。これに気付かないままだとしたら、ユーザーを脅威から保護することはできません。
- モバイルセキュリティテクノロジーの最新の動向を常に意識する：サイバーセキュリティの脅威に常に目を配り、新たなリスクに関する知識を取り入れて、ユーザーを教育できるようにするとともに、攻撃者に先んじた体制を整えられるようにする。

脅威の影響を軽減するためのヒント

- セキュリティの高くないネットワークからは金融機関のWebサイトや機密性の高い情報にはアクセスしない。
- パスワードは複雑なものを用いる。できればすべてのメールアカウントで2要素認証を使用する。
- 見知らぬ相手から送られてきた添付ファイルは開かない。実行形式の添付ファイルは絶対に開かない。

不正送金の調査と平行してクレジットカードの口座を調べてみると、利用している回線業者から身に覚えのない請求のあることが判明し、さらに詳しく調査をした結果、不正なメールアカウントが作成されていることがわかりました。このメールアカウントが回線事業者のアカウントと関連付けられていたのです。

はっきりとは覚えていませんが、回線事業者のメールアカウントは、「first_name」の次に「@cablecompany.com」が付くようなものであったと記憶しています。通常、私が使用しているメールアカウントは「MrSmith@Corporation.com」だったので、この新たなアカウントの存在を知ったときには驚きました。

VTRACの調査担当者は、妻と私のタブレットおよびラップトップと、会社のMicrosoft Windowsシステムについて、フォレンジックイメージの収集を行いました。タブレットには、ほとんどのユーザーデータを暗号化できるよう、パスワードで保護された暗号化バックアップを作成する設定がありました。しかし妻も私もタブレットにパスワードを設定しておらず、バックアップから情報を復元することはできませんでした。

インターネットの閲覧履歴やメッセージなどのユーザーデータなしでは、タブレットに関しては、フィッシングや不審なアクティビティの痕跡を探し出すことができませんでした。それでもVTRACの調査担当者は、数十個に上る不審なファイルと悪意のあるファイルを妻のラップトップで見つけました。これらの悪意のあるファイルは主に、「/Users/MrsSmith/Downloads/」と「MrsSmith@InternetCompany.com \INBOX \ Attachments」のフォルダで見つかりました。

ファイルの拡張子は「.zip」か「.exe」となっており、これは、ファイルがWindowsのシステム上で機能することを意味します。これらのファイルがラップトップ上で実行される可能性は高くありませんが、もしも、Windowsのシステムに転送されていたら、そこで被害をもたらしたことでしょう。

VTRACの調査担当者がこのラップトップのメールボックスを調査したところ悪意のあるファイルが3つ見つかりました。これらのファイルは添付ファイルとして、妻のメールアカウントから彼女の同じメールアドレスに送られていました。一方、私の「MrSmith@Corporation.com」のメールアカウントには、悪意のあるファイルが添付されたメールは1つも届いていませんでした。

検知のためのヒント

業務用のメールに使用するパーソナルデバイスはアンチウイルスソフトウェアを最新の状態にしておく。

得られた教訓

この件では、影響の軽減と対応の観点から多くの教訓が得られました。事後の反省から学んだいくつかの重要なポイントを以下に示します。

脅威の影響の軽減と防御のためのヒント

- セキュリティの高くないネットワークからは金融機関のWebサイトにアクセスしない。
- パスワードは複雑なものを用いる。できればすべてのメールアカウントで2要素認証を使用する。
- 見知らぬ相手から送られてきた添付ファイルは開かない。実行形式の添付ファイルは絶対に開かない。

検知と対処

- ポート転送やアカウントのオーナーシップなどについてアカウントの設定が変更された場合にアラートが発信されるよう設定を行う。
- 情報の不正使用による被害を受けた場合は、警察当局など適切な関係機関に報告を行う。
- 業務用のメールに使用するパーソナルデバイスはアンチウイルスソフトウェアを最新の状態にしておく。

モバイルデバイスのセキュリティ：ユーザー向けのベストプラクティス

モバイルデバイスは今や日常生活においてなくてはならない存在になっていますが、このような状況を受けて、モバイルデバイスを狙った脅威の数が増加しています。モバイルデバイスの侵害はコンピューターと比べて件数こそ少ないものの、その規模が増加しています。以下に挙げるアドバイスをご活用ください。モバイルデバイスのデータが侵害を受けるリスクを軽減できます。

- 常にパスワードを利用する：パスコードは8文字以上とし、大文字、小文字の英数字、特殊文字を含めるようにします。これで、標準の4から6桁のピンコードよりもセキュリティを高められます。
- デバイスは常に携帯する：モバイルデバイスを他人が物理的に利用できる状態にしておくのは、不正使用につながる最も大きなリスクとなります。
- デバイスは最新の状態にしておく：デバイスを最新の状態にしておけば、モバイルデバイスでよく使われる侵害の手口からデバイスを保護できます。
- 信頼できるソースのアプリだけを使用する：Appleのデバイスの場合はiTunes Storeのアプリを、Androidデバイスではgoogle Playのアプリを使用するようにします。それ以外のソースからサードパーティのアプリをダウンロードしてインストールすると、悪意のあるソフトウェアをインストールしてしまう危険が高くなります。
- スクリーンロックを有効にする：デバイスを使用していない状態からデバイスが自動ロックされるまでの時間を短く設定するほど、不正アクセスを受けるリスクを減らすことができます。
- 脱獄デバイスは使用しない：デバイスの脱獄という行為はその性質上、モバイルデバイスのセキュリティリスクを高めます。

クレジットカードのデータを狙った組織内部からの攻撃

2018年データ漏洩/侵害ダイジェスト

verizon

概要

ほとんどのセキュリティ侵害は、ハッキングやスピアフィッシングなどにより外部からもたらされますが、組織はその内部のネットワーク環境から攻撃を受けることもあります。

そのような侵害の1つに、現金自動預払機（ATM）からの不正な引き出しなど、カードのデータを狙った攻撃があり、この攻撃は大きな金銭的損害をもたらします。このレポートのケースの依頼では、ベライゾンのVTRAC | Investigative Response Teamは、クレジットカード業界においてフォレンジック調査を行っています。

調査対応の詳細

現場に到着してまず気が付いたことがあります。なんのセキュリティチェックやIDチェックも受けることなくすぐに建物に入ることができてしまったのです。状況を考えれば予想もしないことであり異常ともいえます。また、話を聞きたいと思っていたスタッフのほとんどがインシデント対応に関わっていたため解雇され、別の新たなスタッフが我々の対応に応じたのですが、彼らはまだ環境のことをよくわかっていませんでした。

まずは、セキュリティ情報管理とイベント管理（SIEM）のログを分析したところ、環境内に悪意のあるシステムが存在するらしいことを確認しました。このシステムはこの企業が所有しているものではなく「未知」のシステムです。それゆえ、いくつもの疑問が浮かびました。このシステムはどのようにしてネットワークに侵入し、どこにいるのか。どうやってPCI環境にアクセスしたのか。なぜ、最初にアラートが発生したときに誰もそれに気が付かなかったのか、などといったことです。

検知のためのヒント

- SIEMや侵入検知システム（IDS）などのネットワークセキュリティ監視ソフトウェアをユースケースに応じて適切に構成する。定期的に出力結果とイベントを確認する。
- サイバーセキュリティに関するポリシーや問題対応の手順について従業員の教育を行い、これを通じて従業員のセキュリティ意識を高めて、不審なサイバーセキュリティインシデントに遭遇したり、実際に問題が発生したりしたときにエスカレーションができるようにする。

ネットワークに接続されていた悪意のあるシステムの存在と、このシステムが重要度の高いPCIサーバーデータベースにアクセスして不正にデータの引き出しを行ったという事実だけが、調査を行う上での頼りの綱でした。しかし、このシステムがどのようにしてネットワークに侵入したのか突き止めることができません。具体的な攻撃の手法がわかりませんでした。そのため我々は、さらなる情報の収集を中心に作業を進めました。

まずは問題の影響範囲と考え得る侵入経路を特定するために、ネットワークトポロジーなどの技術情報の収集と聞き取り調査に取りかかりました。そしてさらに情報を収集した結果、ネットワークの構造全体に、その基盤レベルで欠陥のあることがわかったのです。

内部ファイアウォールをいくつか導入していましたが、ネットワークの構造は本質的にはフラットでした。基本的なアクセス制御すら行われていなかったので、ネットワークのどの部分にもデバイスからアクセスできるようになっていました。ネットワーク監視の機能を使用していましたが、構成が正しく行われていませんでした。また、SIEMも利用していましたが、誰もアラートの確認や調査をしていませんでした。

ネットワーク全体に見られるこれらの根本的な設計上の不備により、攻撃者は自由な攻撃が可能になるばかりか、相手に全く気付かれずに攻撃を仕掛けることが簡単にできてしまいます。

我々は、攻撃があったときに攻撃者のシステムがネットワークに接続していた場所を突き止めました。そしてその場所の物理的なセキュリティ管理がどうなっているのか確認しました。その場所はメインのデータセンターでした。誰もがアクセスできるエリアの大きなオフィスビルの中にそのデータセンターはありました。

驚いたことに、データセンターの扉には、ごく普通の鍵しか付いていませんでした。物理的なセキュリティはそれだけです。いったん中に入ってしまえば、どのオフィスにも簡単に出入りができるようになっていました。ID認証は行われておらず、アクセス管理リストもなく、セキュリティデスクに誰も人がいないこともあるといったように、ずさんなセキュリティ体制をさらに示す状況も確認されました。物理的なセキュリティが不十分であったため、部外者が比較的容易に社内に立ち入ることができてしまうこともすぐにわかりました。

そして、このような物理的なセキュリティの不備に加え、組織のデジタルセキュリティ体制にも大きな欠陥のあることが判明しました。たとえば、容易に予想のつくパスワードを使用していたり、管理者アカウントのパスワードを変更していなかったり、ユーザーと管理者でアカウントが共有されていたりするといった事実や、デフォルトのユーザーアカウントでデータベースにアクセスしているケースが確認されました。また、データベースのユーザーアカウントすべてに管理者権限が付与されていました。

そして、フォレンジック分析により明らかになったのは次の事実でした。物理的なアクセスを果たした攻撃者は管理者アカウントを用い、犯行に使用されたと思われるシステムからアプリケーションサーバーの1つにアクセスしていたのです。攻撃者はスクリプトを作成してデータベースを操作しており、一連の犯行は当日の夜に行われていました。しかし残念ながら、この問題のシステムは見つからず、そのため、さらに分析を行うことはできませんでした。

脅威の影響を軽減するためのヒント

- 物理的なアクセス制限の実施：IDカードやカードスワイプ機能の導入、入出場ゲートの設置など、物理的なセキュリティ対策を講じる。機密情報を扱うエリアへの入場を制限する。
- 論理的なアクセス制限の実施：ネットワークのセグメンテーションを行う。悪意のあるシステムからのネットワーク接続を遮断する。多要素認証を導入する。すべてのユーザーアカウントで複雑なパスワードを使用する。

得られた教訓

最終的には、以下のような方法での侵害が明らかになりました。

ステップ1：物理的なアクセス
物理レベルでセキュリティ管理が脆弱であったため、攻撃者に物理的なアクセスを許してしまい、組織内の環境に不正なシステムが侵入してしまいました。

↓

ステップ2：論理的なアクセス
ネットワークのアクセス制御が不十分であり、ネットワークのセグメンテーションが不完全であったため、内部ネットワークや重要なサーバー、データベースシステムに攻撃者が侵入してしまいました。

↓

ステップ3：管理者権限を悪用したアクセス
パスワードのポリシーが脆弱であったため、攻撃者は管理者権限でのログインが可能になり、ターゲットのデータベースを操作して攻撃を完了できてしまいました。

図1：攻撃の分析

最終的には、今回の攻撃を早期に検知できなかった原因は、ネットワーク監視の機能を適切に利用していなかったことにあります。

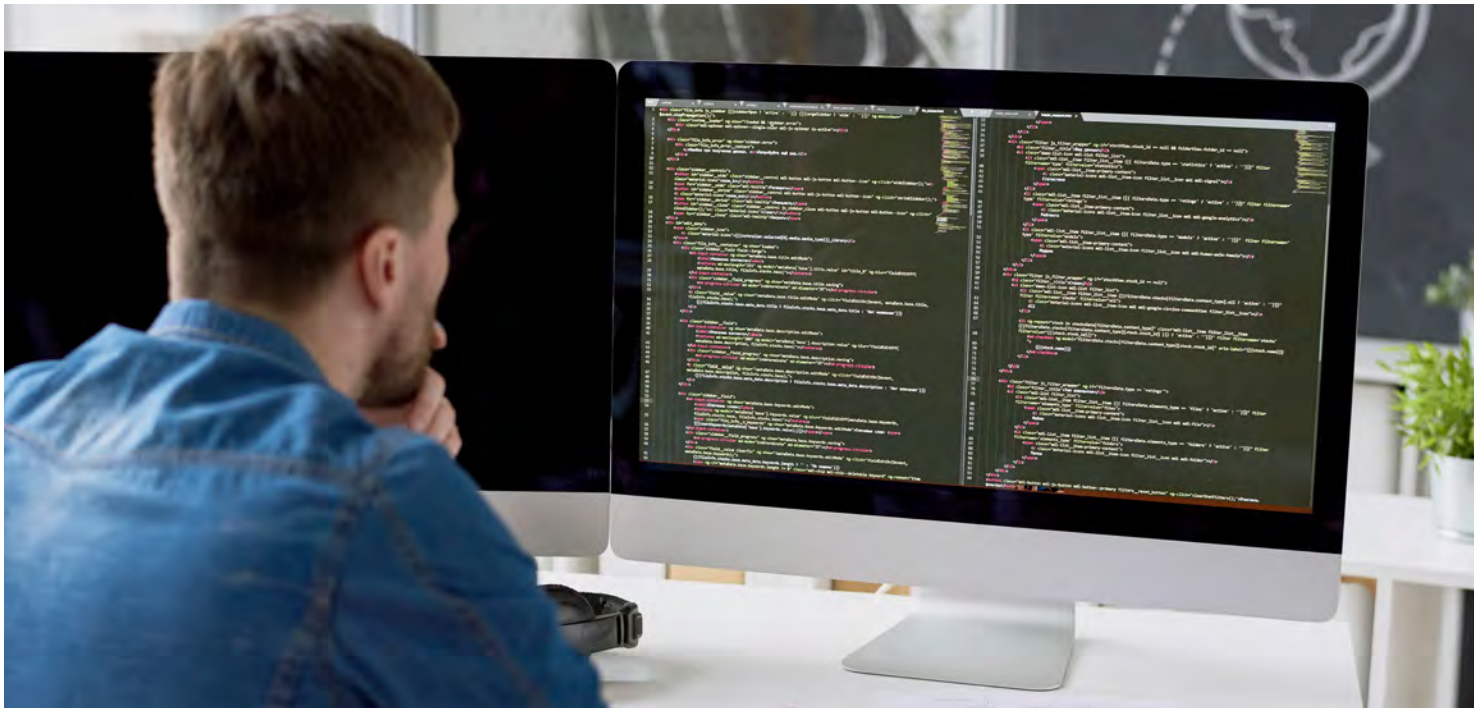
攻撃者が「内部の人間」からどの程度のサポートを受けていたのか、調査の完了時点でも依然不明です。犯行に使用されたと思われるシステムを特定できなかったため、多くの疑問について、答えを推測することが不可能になってしまいました。

検知と対処

- SIEMや侵入検知システム（IDS）などのネットワークセキュリティ監視ソフトウェアをユースケースに応じて適切に構成する。定期的に出力結果とイベントを確認する。
- サイバーセキュリティに関するポリシーや問題対応の手順について従業員の教育を行い、これを通じて従業員のセキュリティ意識を高めて、不審なサイバーセキュリティインシデントに遭遇したり、実際に問題が発生したりしたときにエスカレーションができるようにする。

脅威の影響の軽減と防御のためのヒント

- 物理的なアクセス制限の実施：IDカードやカードスワイプ機能の導入、入出場ゲートの設置など、物理的なセキュリティ対策を講じる。機密情報を扱うエリアへの入場を制限する。
- 論理的なアクセス制限の実施：ネットワークのセグメンテーションを行う。悪意のあるシステムからのネットワーク接続を遮断する。多要素認証を導入する。すべてのユーザーアカウントで複雑なパスワードを使用する。



PoSシステムのクレジットカード情報を狙った侵害

2018年データ漏洩/侵害ダイジェスト

概要

サードパーティに業務委託する企業の数が大きく増えています。企業にとって、このような業務委託のメリットはコスト面だけにとどまりません。サードパーティが得意とする個々の業務をこれらの第三者に委託して、企業自身はみずからの強みであるコアのビジネス領域にリソースを集約することが可能になります。

弊社はアジア太平洋地域において「実店舗」での小売事業を展開しており、私はそこで事業部門の責任者を務めています。事業委託の効果を期待し、サードパーティのベンダーの協力のもとで、ポイントツーポイント暗号化（P2PE）ソリューションを利用してセキュリティに優れた取引フローを構築し、PoSシステムと取引先の加盟店銀行のあいだで運用を始めました。

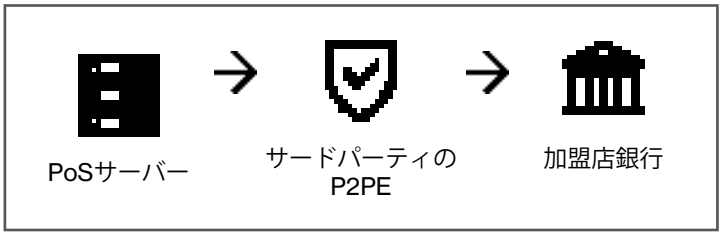


図1：クレジットカード情報の処理フロー

取引している加盟店銀行からある知らせを受けるまではすべてが順調でした。その知らせとは、カード業界でデータ侵害が発生しているおそれのあることを伝えるものだったのです。世界中のさまざまな場所で、数百万ドル規模の取引詐欺が発生していました。

そして、クレジットカード会社によるCCP（Common Point of Purchase）分析によれば、弊社がクレジットカード情報の流出元になっている可能性があるといいます。データの侵害は1つの店舗や地域にとどまらず、グローバルの販売網全体で起きていました。

検知のためのヒント

ネットワークベースおよびエンドポイントベースでプロアクティブに脅威ハンティングを行って、未知の脅威を検知し対処する。

私は自問し続けました。「何が原因だったのか？」、「どこで侵害を受けたのか？」、「ネットワークか？」、「それともどこかの店舗か？」、「あるいはいずれかのサービスプロバイダーが侵害を受けたのではないか？」

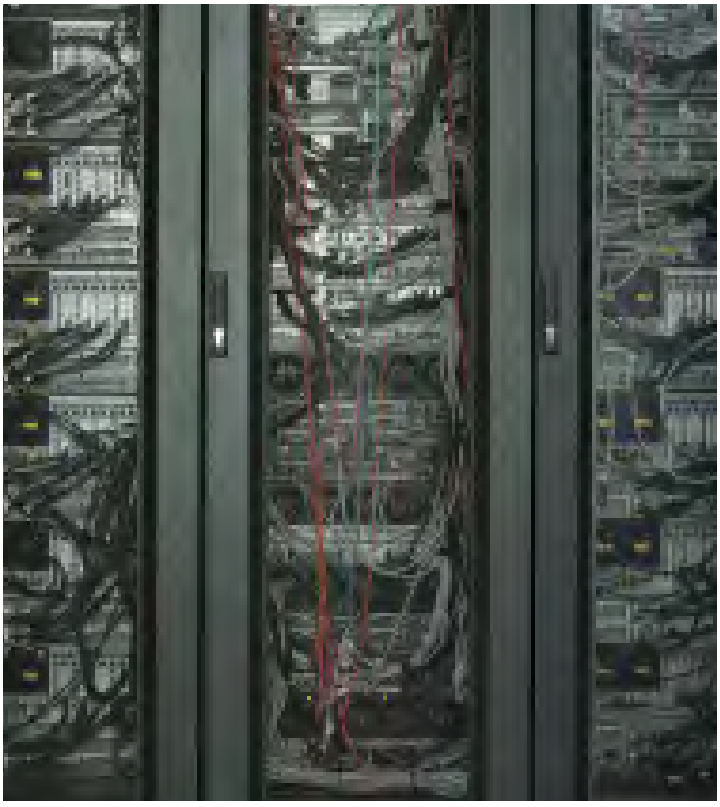
調査対応の詳細

すぐに対策本部を立ち上げ、加盟店銀行、クレジットカード業者とのセッションや内部ミーティングの調整にあたるコアチームを編成しました。また、これと並行して我々は、VTRAC | Investigative Response Teamと連絡を取りました。PCI関連の調査ではPCIフォレンジック捜査担当者（PFI）による調査が必要ですが、VTRAC | Investigative Response Teamはこの捜査担当者の資格を有していたのです。

VTRACのフォレンジック捜査担当者は、インシデントの背景情報、クレジットカード情報の処理フロー、クレジットカード会社によるCCP分析のデータ、弊社のIT環境の詳細、サードパーティについての評価などを入念にチェックしました。

そしてこれらの作業に続き行われたのが、CCP認定の店舗に設置されているPoSサーバーと端末のデータの収集と分析です。関係する事業部門のサーバーや、数十台に上るサードパーティのサーバーも調査の対象になりました。

しかし残念ながら、フォレンジックに役立つアーティファクトは、ベンダーによるさまざまなアクションが原因で失われていました。ベンダーは、システムの再起動やアンチウイルススキャンの実行、既存のローカルシステムアカウントの削除、パスワードの変更、各種ログの削除、システムの変更などを行っていたのです。これはすべて、弊社の許可なく実施されていました。しかもエビデンスを収集する前にです。



被害受けた組織に起因し調査を妨げる上位5つのポイント（再掲）

2年前の『2016年データ漏洩/侵害ダイジェスト：フィールドで得られたシナリオ』において、補足記事「被害受けた組織に起因し調査を妨げる上位5つのポイント」を掲載しました。

この内容は2016年の時点と同様に現在でも有効であるため、以下に再度記載します。

- ログ：ログそのものが存在しないか、あっても不十分（すぐに内容が書き換わる）。すぐにログを特定したり取り出したりするのが困難
- ネットワークトポロジー：存在しない、あるいは著しく内容が古い
- ベースラインイメージと信頼できるタスクリスト：存在しない、不正確、または内容が古い
- PsExecなどのデュアルユースツール：侵害に無防備なままでツールを使用している。Windows Recyclerに置いてセキュリティオプションとして使用していない。ツールの使用が検知できない状態になっている。
- フォレンジックを妨げる要因をみずから誘発：システムの再構築やサポート要請のコール、隔離・駆除の処理は行っているが、適切なドキュメントを残していない。ネットワークケーブルの代わりに電源ケーブルを抜いている。資格のないIT部門のメンバーが、良かれと思い「チラ見」をしてしまう。

侵害対応のヒント

- インシデント対応のプレイブックを作成してインシデント対応プランを補完する。初動にあたる担当者向けにトレーニングを行い、タイムリーかつ効果的なインシデント対応の重要性を理解させる。
- ネットワークのログとアプリケーションのログを確認する。侵害を受けたシステムやユーザーアカウントに関係するログを調査して、ほかに影響を受けた資産がないか確認する。

脅威の影響を軽減するためのヒント

システムを強化するベースラインを構築、実装する。完全な脆弱性評価を少なくとも四半期ごとに実施する。侵入テストの訓練を年1回以上行う。

それでもVTRACのフォレンジック捜査担当者はすぐに多くの問題を特定しています。たとえば、インターネットからPoSサーバーへのアクセスには何の制限も加えられておらず、ログインには単一要素認証が使われており、未知の外部のIPアドレスから複数のログインのあったことが確認されました。この際、リモートデスクトッププロトコル（RDP）が悪用されたほか、バックドアのトロイの木馬ウイルスやRAMスクラッパー、ネットワークスニファソフトウェアがシステムにインストールされています。また、サードパーティのサーバー上には100,000を超えるトランザクションログのエントリーが存在し、プライマリアカウント番号（PAN）や、Track 1およびTrack 2の全データがプレーンテキストのかたちで残っていました。

そして、入手したエビデンスソースのフォレンジック分析を行い、クレジットカード情報の処理フローとCCP分析の内容を確認した結果、データ侵害が起きていることが確認されました。

侵害の発端はRDPアクセスを狙ったブルートフォース攻撃であり、これに続き、ネットワークスニファ、RAMスクラッパー、リモートアクセス型トロイの木馬（RAT）が順に、サードパーティのクレジットカードデータ処理サーバーにインストールされています。

PCI PANおよびトラックデータの定義

PCI Data Security Standard（PCI DSS）およびPayment Application Data Security Stand（PA-DSS）の用語略語集のバージョン3.2では、PCI PANとトラックデータを次のように定義しています。

- プライマリアカウント番号（PAN）：一意のクレジットカード番号で、通常、クレジットカードやデビットカードで使用されます。この番号でカードの発行元と、カードの所有者ごとの個別アカウントを識別します。
- トラックデータ：「フルトラックデータ」、「磁気ストライプデータ」とも呼ばれます。磁気ストライプやチップにエンコードしたデータで、決済処理時の認証や確認の処理に使用します。チップに埋め込んだ磁気ストライプのイメージを利用したり、磁気ストライプのTrack 1やTrack 2のデータだけを利用したりする場合もあります。

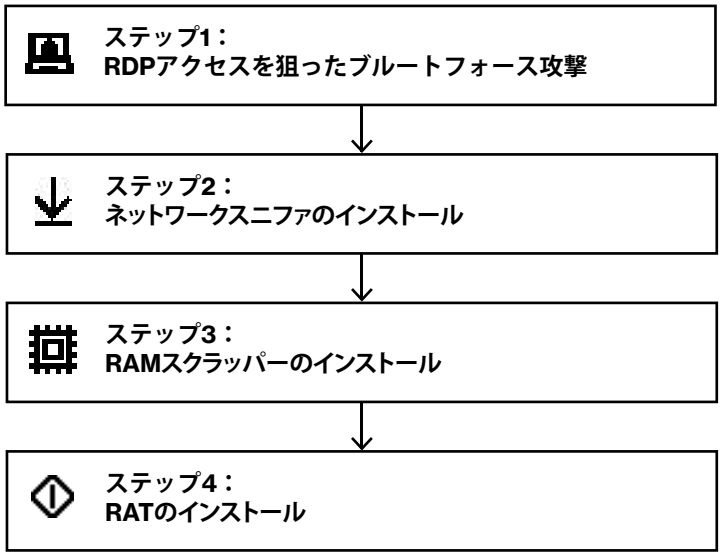


図2：サードパーティのサーバーを狙った攻撃の流れ

調査が完了した時点で、修復作業、リカバリ作業、防御および影響緩和のアクションについて優先順位付けを行いました。

影響を受けたシステムについては、駆除や再構築を行い、RDPアクセスには、ソースアドレスベースのフィルタリング機能で制限を加えました。また、リモートログインによる接続では、すべてのケースで多要素認証（MFA）の使用を義務付けました。

サードパーティのサービスプロバイダーのセキュリティ管理を詳しく確認した結果、PCI DSSの観点だけでなく、基本的なセキュリティハイジーン管理の面からみても、さまざまな欠陥のあることが判明しました。企業におけるセキュリティの確保においては、セキュリティハイジーン管理の施策が求められます。

我々はすぐに、PCI DSSの遵守状況を定期的に個別評価するプロセスをサードパーティのサービスプロバイダーを対象に始めました。サービスプロバイダーは常に適切に業務を行っていると盲目的に信じることはできません。

脅威の影響を軽減するためのヒント

- コンソールを経由しないシステムアクセスすべてを対象に多要素認証（MFA）を導入する
- サードパーティのPCI DSS遵守のリスクを継続的に監視、評価する

得られた教訓

今回のインシデントにつながった手続き上および技術上の問題がいくつかあることが調査により明らかになりました。また、重要ないくつかのデジタルエビデンスが入手できなかったために、調査自体が、複雑をきわめ骨の折れるものとなりました。

そして、調査報告を通じ、VTRACのフォレンジック捜査担当者から以下のアドバイスを受けました。

脅威の影響の軽減と防御のためのヒント

- システムを強化するベースラインを構築、実装する。完全な脆弱性評価を少なくとも四半期ごとに実施する。侵入テストの訓練を年1回以上行う。
- コンソールを経由しないシステムアクセスすべてを対象に多要素認証（MFA）を導入する。
- サードパーティのPCI DSS遵守のリスクを継続的に監視、評価する。

検知と対処

- インシデント対応のプレイブックを作成してインシデント対応プランを補完する。初動にあたる担当者向けにトレーニングを行い、タイムリーかつ効果的なインシデント対応の重要性を理解させる。
- ネットワークベースおよびエンドポイントベースでプロアクティブに脅威ハンティングを行って、未知の脅威を検知し対処する。
- ネットワークのログとアプリケーションのログを確認する。侵害を受けたシステムやユーザーアカウントに関係するログを調査して、ほかに影響を受けた資産がないか確認する。

サプライチェーン全体を標的とする攻撃

2018年データ漏洩/侵害ダイジェスト

verizon

概要

VTRAC | Labsでの調査では多くの場合、調査対象は汎用的なサーバーやオペレーティングシステムなどですが、組み込みシステムやハードウェアコンポーネントを直接調査して欲しいという依頼をユーザー顧客からもらうこともあります。このような場合、作業は弊社の研究所内で行います。この環境であれば、「Go Kit」以上に最適な特別のツールを自由に利用できます。

ある顧客からサイバー諜報活動の疑いについて調査を求められたケースでは、特定のデバイスにみられる異常な挙動の理由を突き止めて欲しいとの要請を受けました。ネットワークトラフィックを調査していたところ、長期間にわたり使用していた特殊なサーバーモデルが東南アジアのIPアドレス向けにSNMP（Simple Network Management Protocol）トラフィックを送信し続けていることを、顧客が確認したというのです。

このIPアドレスは取引先のベンダーや顧客とは無関係のものであったため、データ漏洩の懸念が生じていました。この件についてサーバーベンダーから明確な理由が得られなくなったときに、懸念はさらに深まりました。

検知のためのヒント

営業時間外の異常なネットワークアクティビティや外部への大量なデータの発信、リモート接続など、不審なネットワークトラフィックが存在しないか確認し警戒する。

調査対応の詳細

顧客から与えられたのは物理サーバー1台と、ほんの一瞬の状況を捉えた検証済のフォレンジックイメージのほか、問題の不審なリモートIPアドレスでした。まずは、サーバーの物理的な調査やテストが自由に行えるよう、隔離環境のセットアップに取り掛かりました。

しかし物理レベルのチェックでは、何も異常は見つからず、リモート管理モジュール（通信の管理を担うシステムコンポーネント）の存在が確認できただけでした。

そして次の手順として、不審な通信の挙動を再現してみることにしました。サーバーは、フルパケットキャプチャ（FPC）デバイスに接続します。サーバーは起動するとすぐに、内部の（RFC 1918）IPアドレス、IP 172.16.x.xに関係したネットワークノードの探索を試みました。

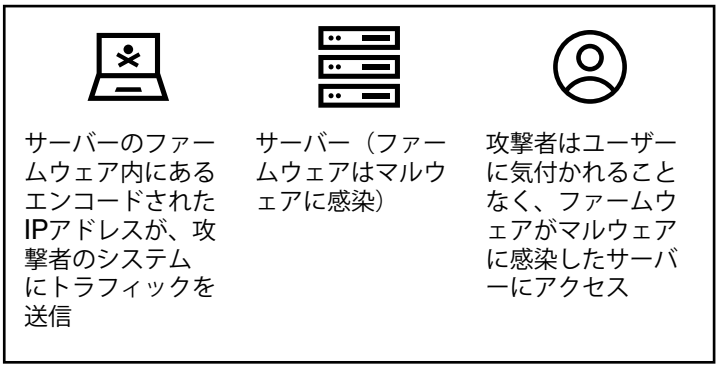


図1：ファームウェアによるトラフィックの生成

侵害対応のヒント

- ベースラインのシステムイメージと、信頼できるプロセスのリストを用意しておく。これらを既知の基準として、侵害を受けたシステムと比較照合する。
- 外部向けのインターネットトラフィックを一時的にブロックし、ユーザーアカウントのパスワードの変更し、侵害の痕跡を特定する。
- 侵害を受けたユーザーアカウントの無効化、悪意のあるファイルの削除、影響を受けたシステムの再構築を通じて問題を一掃する。

デフォルトゲートウェイと思われるサーバーはシャットダウンし、IP 172.16.x.xのトラフィックはFPCデバイスにルーティングされ、そしてサーバーが再起動しました。IP 172.16.x.xの応答を受信したサーバーは、問題の不審なIPアドレスとの通信を試みました。

通信の処理はサーバーのファームウェアが制御しているので、次にファームウェアを調査することにしました。そしてベンダーのWebサイトからいくつかのバージョンのファームウェアをダウンロードして確認を行った結果、ブートローダーとファイルシステムが使用されていることを突き止めました。一方、ファームウェアのなかに不審なリモートIPアドレスがハードコーディングされている形跡は見当たりませんでした。

ソフトウェアには問題がないと判断し、オシロスコープを使って、デバッグ用のアクティブなシリアルポートの場所と仕様を把握することにしました。このデバッグポートにより、リモート管理に関係するメインプロセッサーへ接続できるようになったほか、管理カードの起動プロセスの監視とコマンドシェルへのアクセスが可能になりました。

そして不審なIPアドレスを探し出すことなどを目的として、分析のためにサーバーからファームウェアのソースコードを抽出しました。手間のかかる作業でしたが、最終的には、構成ファイルのなかに16進形式のコードが見つかっています。この構成ファイルはベンダーのサイトからダウンロードしたものと同じでした。しかし、そのなかには、エンコード形式の不審なIPアドレスが組み込まれていたのです。

結局のところ、システムコンポーネントとコードは、ベンダーが出荷しているものとすべて同じであることがわかりました。現代のコンピューティング環境や企業ネットワークは非常に複雑になっているため、業務で必要となるサーバーやネットワーク接続の状態をすべて追跡するのは容易ではありません。このようなIPアドレスが存在し使われていることをベンダーさえも知らなかったのです。そのため、調査に多くの時間を費やすことになりました。

リモート管理モジュールや類似の組み込みデバイスをはじめとした不正なメカニズムをシステムに付加すると、システムに出入りするルートとして攻撃者に悪用されるおそれがあります。そのため、このようなメカニズムは、デバイス全体のセキュリティを左右する要素として捉え扱わねばなりません。

脅威の影響を軽減するためのヒント

- 機器の製造元や付加価値再販業者を含め、ハードウェアのサプライチェーンを精査し、評判や信頼度をチェックする。
- 機密保持、整合性と可用性の維持のために、設計、テスト、管理、レビューを網羅するIT管理プロセスを採用する。
- 資産管理表を維持管理する。重要性の高いサーバーやシステムなど、あらゆる資産の状態を追跡し把握する。

得られた教訓

この顧客には、いくつかの優れたセキュリティプラクティスが存在していました。たとえば、ネットワークの監視を定常的に行っているため、問題のあるトラフィックがあれば、それを検知できます。しかし、システムの展開前のテストは行っていませんでした。これを実施していれば、今回遭遇したような不審なトラフィックの存在がわかり、そのリスクの評価が可能であったはずです。そしてさらには、十分な時間的余裕をもって、ベンダーと調査ができたことでしょう。

いずれにせよ、展開前のテストにあたりファームウェアのバージョンを最新の状態にアップグレードする習慣をもつのが大事です。ファームウェアが最新のものになっていれば、ベースラインとなるシステムの挙動をもとに、どのような状態が「正常」であるのか判断できます。正しい設定や正常な挙動がわかるので、攻撃を受けていることを示す異常を検知する場合や、不都合が生じているのを把握するうえで効果を期待できます。

脅威の影響の軽減と防御のためのヒント

- 機器の製造元や付加価値再販業者を含め、ハードウェアのサプライチェーンを精査し、評判や信頼度をチェックする。
- 機密保持、整合性と可用性の維持のために、設計、テスト、管理、レビューを網羅するIT管理プロセスを採用する。
- 資産管理表を維持管理する。重要性の高いサーバーやシステムなど、あらゆる資産の状態を追跡し把握する。

検知と対処

- 営業時間外の異常なネットワークアクティビティや外部への大量なデータの発信、リモート接続など、不審なネットワークトラフィックが存在しないか確認し警戒する。
- ベースラインのシステムイメージと、信頼できるプロセスのリストを用意しておく。これらを既知の基準として、侵害を受けたシステムと比較照合する。
- 外部向けのインターネットトラフィックの一時的なブロックやユーザーアカウントのパスワードの変更、侵害の痕跡の特定する。
- 侵害を受けたユーザーアカウントの無効化、悪意のあるファイルの削除、影響を受けたシステムの再構築を行う。

サイバー脅威インテリジェンスの活用

サイバー脅威インテリジェンス（CTI）を自社のサイバーセキュリティのワークフローに導入する組織が増えています。サイバー脅威インテリジェンスには多くのメリットがありますが、サプライチェーンの問題をより詳細に把握できるようになる点もまさにその1つです。CTIは、攻撃者についてのナレッジを集約、分類、利用するものですが、CTIは、「攻撃者の存在」が確認されない場合にも役に立つ情報が得られます。

脅威インテリジェンスの設定により、以下に示す不審なトラフィックの特定が可能です。

- 情報フィード/ブラックリスト：問題にしているIPアドレスが悪意のあるものとしてタグ付けされた場合、脅威インテリジェンスフィードをSIEMアラートと関連付ければ、そのIPアドレスのアクティビティが開始したときに、それをアラート通知でSOCに知らせることができます。理想的には、このナレッジにより、特定のエスカレーション手順を開始できます。
- 脅威インテリジェンスプラットフォーム（TIP）：TIPを活用すれば、IPアドレスについて、以下に示すさらに詳しい背景情報が得られます。
  - Whois情報（組織、NetRange、登録日付、連絡先情報）
  - パッシブDNS（ドメインマッピングに対応したIPアドレスの履歴）
  - アナリストに関する詳細情報、アナリストの信頼性
  - 関係のある侵害の痕跡
  - 関係のある攻撃者および攻撃活動。関係のあるツール・戦術・攻撃の流れ（TTP）
- ジオブロッキング：問題のあるIPアドレスがほかの国のものである場合、そのIPアドレスの国や地域と取引をしていないのであれば、ジオブロッキングの機能を利用して遮断することが可能です。
- 脅威インテリジェンスの共有：信頼できるパートナーとコンタクトが取れるようになっていれば、不審なアクティビティが認められたときに大きな助けになります。サプライチェーンを標的とする場合、攻撃者は同じ手法で複数の組織に攻撃を仕掛けることが少なくありません。特定の業種で不審なアクティビティが複数確認された場合、同じ手法での攻撃の可能性があります。

人間の心理につけこむソーシャルエンジニアリング攻撃

2018年データ漏洩/侵害ダイジェスト

verizon

概要

事件の発端は、2月のある月曜日の朝の出来事でした。私の職場は財務部門でしたが、その日もいつもと変わりませんでした。チームミーティングがあり、毎週どおりのタスクリストに向き合い、メールの受信トレイには大量のメールが届いていました。そしてそのなかに、長年取り引きしているあるベンダーからのものと思われるごく普通のメールがあるのに気付きました。

それは、毎日受け取って処理している多くのメールと同じようなものに見えました。代金の支払いを求めるメールで、請求書が添付されており、請求書には、代金振り込み先の銀行口座の情報が記載されていました。

しかしそれを確認したところ、弊社のシステムにその口座が見当たりません。そこで、細心の注意を払い、情報を求める返信のメールを相手に送りました。先方の説明によれば、口座は子会社のもので、確認の意味でメールを送ったとのことでした。さらに相手は、送金が完了したら確認のメールを送って欲しいとも言ってきました。

請求書の内容の変更をベンダーが求めることはよくあったので、特に不審な思いは抱かず、同じ規模の取引がこれまでにもあったので、ほとんど何も考えませんでした。

そして振り込みを行った日に相手に確認のメールを送りました。しばらくして返信があり、銀行に入金があった旨を伝えてきましたが、国内でテロの危険があり、代金をいったん返金すると言います。

そして、支払いの処理を再度して欲しいと述べ、ただし、それを4等分して処理してもらえないかと言ってきました。処理を遅らせたくなかったのですぐに再度振り込みの処理を行いましたが、相手にはそれを感謝されました。

脅威の影響を軽減するためのヒント

- メールの送信元のアドレスやドメインを確かめる。メールにミススペルがないか確認する。受信したメールの発信元が得意先企業の正式なアドレスであるか確かめる。
- 得意先からの要求内容に不審な点がある場合は電話で確認の問い合わせを行う。メールの送り主の連絡先が承認済みの正規のものであることを確認する場合は、サプライヤーを登録しているマスターのレポジトリデータベースを使用する。支払いの請求メールについて問い合わせる際は、メールではなく個別のチャンネルを使う。

調査対応の詳細

次の日に私は、財務担当のVP、ITセキュリティ担当のVP、法務担当のVPから緊急のミーティングに参加するよう命じられました。そしてミーティングでは、席に着く間もなく問いただされました。なぜ、承認されていない口座に送金の処理をしたのか、なぜ、支払いを4つに分割して再度送金を行ったのか説明を求められたのです。

背筋を伸ばして椅子に座り、送金にいたる経緯を話し始めましたが、1分も経たないうちに話を遮られ、こう言われました。私は信用詐欺に引っかかり、多額のお金をだまし取られたのだそうです。会社が被った被害総額は数十万ドルにも上るおそれがあると言います。

そして、次々と質問を浴びせられ、なぜ、メールアドレスを確かめなかったのか、なぜ、メールのドメインが一文字違うのに気が付かなかったのか、なぜ、同僚にメールの内容を確認してもらわなかったのか、なぜ、内容明細票や注文書の内容と請求書を突き合わせなかったのかと言われました。

このメールの送り主は、正規のアカウント情報と「本物」の様式の文面を、我々と取引のある親会社から入手していたのです。のちにわかったことですが、取引先サードパーティベンダーの1社に我々の債権回収部門とのやり取りで個人のWebメールアカウントを使用していた会社があり、このアカウントがハッキングを受けていたのです。

そして攻撃者は、これまで我々が交わしたメールの文面から弊社内部の事務プロセスや請求書の受付窓口に関する情報を入手し、これらの情報を悪用して正規のサードパーティベンダーのものに似せた一文字だけ異なるメールアドレスを作成していたのです。

脅威の影響を軽減するためのヒント

- 業務を分担して進めるようにする。送金の処理を行う場合は、準備を経験の浅い社員が行い、チェックや承認の処理をベテランの社員が担当するようにする。
- 内部管理において、内容明細票や注文書の内容が請求書の内容と一致していることを確認する。
- ベンダーにセキュアな業務用メールシステムの使用を義務付けるベンダー管理ポリシーを導入する。個人のWebメールアカウントを業務に使用するのを禁止する。

フィッシングメールに騙されないようにするためのアドバイス

- メールの送り主のアドレスをよく確認する。タイポやメールのドメイン名の不一致がないか確かめる。
- メール本文の内容をよく確認する。ミススペルがないか確かめる。「緊急」や「至急」のアクションを求めるメールには注意する。
- メールに埋め込まれたハイパーリンクの扱いに注意する。リンクの上にマウスカーソルを置いてドメイン名を確かめる。

期日を経過しているお支払いについて

差出人：Kimberly Jones <kjones@spoofedemailaddress.com>

受信日時：2018/10/17 月曜日 5:09 PM

宛先：John Smith

Cc:

John Smith様

請求書番号4327394の件ですが、お支払い期日を90日経過しており、まだ入金の確認ができておりません。こちらをクリックして今すぐお支払いをお願いいたします。お支払いいただけない場合は本件を債権回収業者に回します。

以上、よろしくお願いいたします。

アカウント担当

Kim Jones

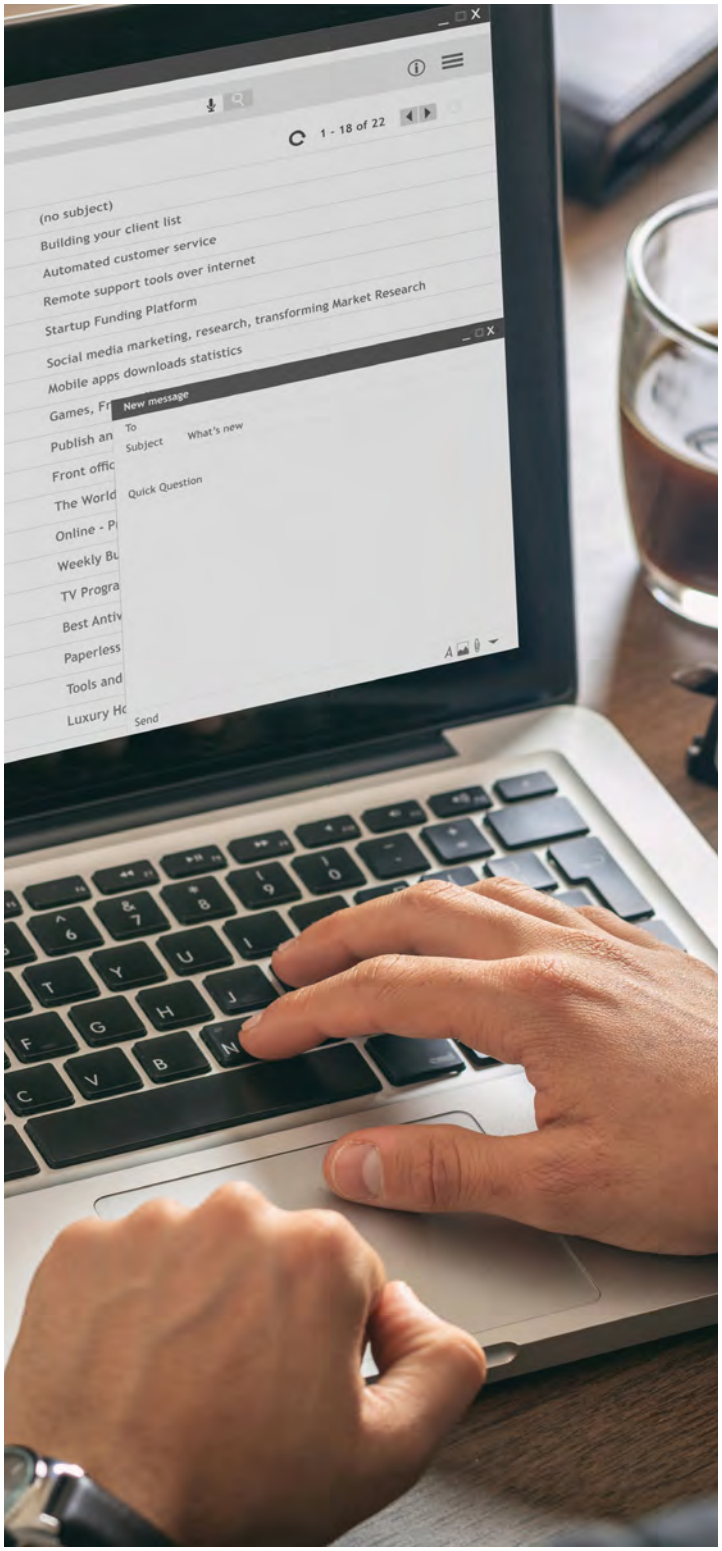
得られた教訓

事態は一応収まりましたが、銀行に振り込まれた大金は戻ってこず、問題の社員はどこで間違いを犯したのかと悩みながら会社を辞めました

この件では、失った大金のように自分も消えてしまいたい思いにかられますが、以下のようなすぐにアクションを取るべき重要なことを学びました。

脅威の影響の軽減と防御のためのヒント

- メールの送信元のアドレスやドメインを確かめる。メールにミススペルがないか確認する。受信したメールの発信元が得意先企業の正式なアドレスであるか確かめる。
- 得意先からの要求内容に不審な点がある場合は電話で確認の問い合わせを行う。メールの送り主の連絡先が承認済みの正規のものであることを確認する場合は、サプライヤーを登録しているマスターのレポジトリデータベースを使用する。支払いの請求メールについて問い合わせる際は、メールではなく個別のチャンネルを使う。
- 業務を分担して進めるようにする。送金の処理を行う場合は、準備を経験の浅い社員が行い、チェックや承認の処理をベテランの社員が担当するようにする
- 内部管理において、内容明細票や注文書の内容が請求書の内容と一致していることを確認する。
- ベンダーにセキュアな業務用メールシステムの使用を義務付けるベンダー管理ポリシーを導入する。個人のWebメールアカウントを業務に使用するのを禁止する。



verizonenterprise.com

物理的な脆弱性を狙った侵害

2018年データ漏洩/侵害ダイジェスト

verizon

概要

弊社にとってネットワークのセキュリティの確保は最優先事項であり、その取り組みのコストを予算に反映しています。サイバーセキュリティ製品の購入にあってはさまざまな製品を細かく調べ、我々の定めた基準を満たすものだけを調達しています。さらには、ネットワークインフラストラクチャの強化に向けて、独自ソリューションの開発と展開に大がかりな投資を行っています。情報の保護をきわめて重視しており、そのためのコストは惜しみません。

しかしそれなのになぜ、侵害を受けてしまったのでしょうか。

1日の業務が終わる頃、弊社のサイバーセキュリティアナリストの一人が偶然、アラートを見つけたのです。マルウェア関連の侵害を示すものであり、データが漏洩している可能性があります。インシデント対応プランに従い、関係者総動員ですぐにログの収集にあたりました。また、証拠の収集と分析を迅速に進められるよう、ベライゾンのRapid Response and Retainer Service（RRR）を開始しました。

侵害対応のヒント

データ侵害対応およびインシデント対応の模擬訓練を定期的に行う。訓練においては現実的なシナリオを使い、発生が予想されるサイバーセキュリティインシデントに適切な対応が取れるようにする。

調査対応の詳細

フォレンジック分析の結果判明したのは次の事実です。すなわち、ネットワークに侵入した悪意のあるソフトウェアの感染経路は、フィッシングキャンペーンや脆弱性攻撃などのような我々がよく目にするものではなく、外部のUSBストレージデバイスだったのです。

脅威の影響を軽減するためのヒント

- 外部のUSBストレージデバイスに対する無許可のシステムアクセスを無効にする。
- 退職した従業員の物理的および論理的なアクセス権限をすぐに無効にする。

ユーザーのシステムが最初に侵害を受け、そこを起点としてネットワーク内にマルウェアが侵入したことが分析で判明したが、そうであるとすれば、攻撃者が一体どのようにしてワークステーションにアクセスしたのかという点で疑問が深まります。ここは、デジタルレベルの調査に旧来の手法を組み合わせて答えを出すときです。

現場の従業員に聞き込みを行い、監視カメラの記録映像を確認した結果、最近退職した元従業員の関与が確認されました。まだ無効になっていないビルの入退出用のIDを使っていたのです。

この元従業員は、ビルと、そして最終的にはシステムの設置してある部屋に侵入しています。システムにロックは掛かっていませんでした。ビルの周辺には警備員が配置されており、常時警備にあたっていましたが、彼らにできるのは、従業員のIDカードを確かめて、それが有効であるかどうかをチェックすることだけでした。

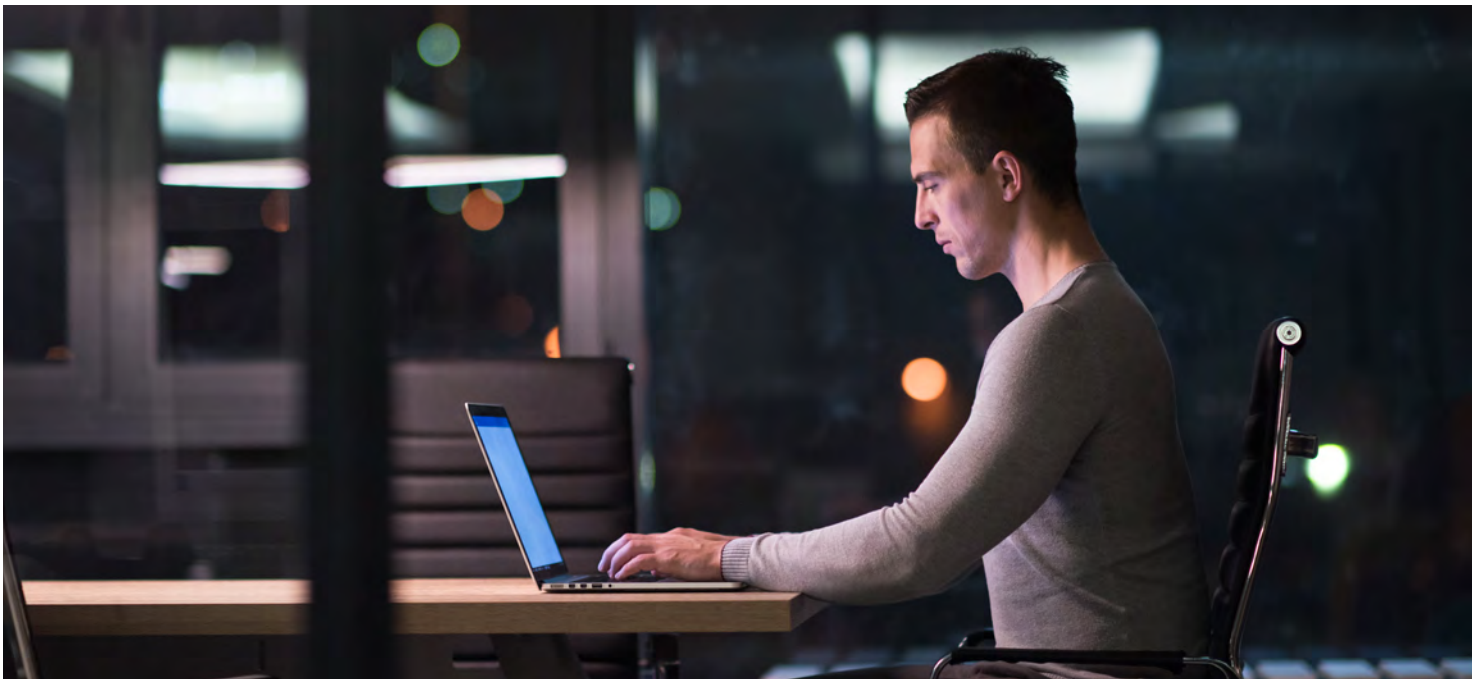
この元従業員のネットワークアクセス用の認証情報はすでに無効になっていましたが、セキュリティデータベースにはその情報がまだ反映されておらず、データベース上では雇用された状態になっており、この結果、正規従業員としてのなりすましを許してしまったのです。

元従業員は我々の情報が機密性の高いものであることを知っており、情報が失われたり、外部に漏洩したりしたときにどのような問題となるのかを理解していました。そして何の理由もなく解雇されたとしてその恨みを晴らそうと、我々のネットワークについて知っていたことを利用して、セキュリティ対策の裏をかいたのです。

犯人は機密情報の収集と拡散を狙っていました。システムをマルウェアに感染させてデータを集め、匿名のWebサイトに送ろうとしています。マルウェアを使ったのは証拠を隠そうとしてのことかもしれません。いずれにせよ、あやうく犯人の計画どおりとなるところでした。

侵害対応のヒント

- サイバーセキュリティ対応においては、事業部門の責任者や法務部門、人事部門、セキュリティ部門など、各ステークホルダーと連携を図る。
- ネットワークの監視には特に力を入れて取り組む。従業員のセキュリティ意識を高めて、不満を抱えた同僚の存在など不安を覚える状況があればエスカレーションできるようにする。



得られた教訓

幸いなことに、ネットワークセキュリティソリューションのおかげで悪意のある行動を検知することができました。しかし一方で、ポリシーの適用が不十分なままであることを認識させられました。ネットワークシステムにロックを掛けず無人の状態にしていたことや、ビルの入退出用のIDカードを速やかに無効にしていなかったことが、今回のデータ侵害につながっています。

セキュリティ対策では、ある特定の領域だけに集中して取り組むあまり、（物理的なアクセスなどのような）細部に配慮できなくなることがあります。今回のケースでは、サイバーセキュリティ対策だけに専念した結果、物理的なセキュリティ上の脅威に対して脆弱な状態となり、その隙を突いた攻撃に無防備になってしまいました。

脅威の影響の軽減と防御のためのヒント

- 外部のUSBストレージデバイスに対する無許可のシステムアクセスを無効にする。
- 退職した従業員の物理的および論理的なアクセス権限をすぐに無効にする

検知と対処

- データ侵害対応およびインシデント対応の模擬訓練を定期的に行う。訓練においては現実的なシナリオを使い、発生が予想されるサイバーセキュリティインシデントに適切な対応が取れるようにする。
- サイバーセキュリティ対応においては、事業部門の責任者や法務部門、人事部門、セキュリティ部門など、各ステークホルダーと連携を図る。
- ネットワークの監視には特に力を入れて取り組む。従業員のセキュリティ意識を高めて、不満を抱えた同僚の存在など不安を覚える状況があればエスカレーションできるようにする。

Webアプリケーションを狙った脆弱性攻撃

2018年データ漏洩/侵害ダイジェスト

verizon

概要

弊社は、成長著しいテクノロジーコンサルティング企業です。最近、ある大型のプロジェクトを受注しており、短期間で大量の技術スタッフを雇わねばならなくなりました。この商談により弊社の知名度は大きく高まり、入社を希望する人たちからいくつかの問い合わせを受けています。

履歴書の経歴が優れていても実務のスキルに乏しい人材を、採用を急ぐあまり雇用してしまうケースを、人事部門のマネージャーとして私は何度も目にしてきました。一方、従来の採用面接では求職者が萎縮してしまうために優秀な人材を見逃してしまうケースもありました。そのため私は、オンラインによる「ハッカソン」イベントの開催を提案しました。このイベントを通じて技術的なスキルをほぼリアルタイムで評価し、才能のある人材を見つけ出そうとしたのです。

弊社では、さまざまなプロジェクトにおいて仮想的なチームが、国境を越えてコラボレーションを行っています。それゆえ、今回のハッカソンでは、チームワークを通じてビジネス上の問題を解決できる人材を募ることにしました。これにより、技術的なスキルとチームワークのスキルを評価することができるのです。このハッカソンを通じて採用しようとしていた職種は、プロジェクトマネージャー、ビジネスアナリスト、ネットワークアーキテクト、情報セキュリティアナリストでした。

マネジメント層に対しハッカソンのメリットを説明し、ハッカソンが「ハッキング」行為とは関係のないことを彼らに納得させたところ、この案は採用され、私はプロジェクトのリーダーに任命されました。そして人事部門の同僚がIT部門と連絡を取り、このイベントを開催するための支援を要請しました。IT部門からは、Webアプリケーションを使ってはどうかとの提案を受けましたが、その設計、テスト、導入には少なくとも3か月はかかるといいます。使える時間は2週間しかないと告げ、最初に提案を押し返した後、IT 部門は同意し、すぐに作業に取り掛かりました。

2週間を超えた後、私は、外部のリクルート会社の協力を得て、ハッカソンイベントに招待する候補者のリストを作成しました。ハッカソンのテーマは「ビジネスと個人の生産性を高めるテクノロジー」とし、弊社のコンサルティングビジネスと従業員をワークライフバランスの観点からサポートする仕組みを目指す成果としました。

この間にIT部門は、Webアプリケーションの設計とテストを行っていました。アプリケーションには、ハッカソンプロジェクトに関する質問事項のほか、オンラインの登録フォームを設定しました。これを通じて、候補者の情報がデータベースに保存されます。人事部門と経営層がこのアプリケーションを承認した翌日に、我々は登録の運用を開始しました。

ハッカソンは大きな成功を収め、多数の人材を雇用することができました。ところがハッカソンが終了してから数日して、私のスマートフォンにアラートが届いたのです。その内容は、「社外秘：Webアプリケーションでデータ侵害が発生」となっていました。そして最高情報セキュリティ責任者（CISO）からインシデント対応（IR)に向けたステークホルダーミーティングの招集がかかりました。

脅威の影響を軽減するためのヒント

- 脆弱性の確認のために、Webアプリケーションは業界のベストプラクティスにもとづき開発する。ソフトウェアの開発では、セキュアな開発ライフサイクルに従う。ライフサイクル全体に情報セキュリティの概念を組み込む。
- 脆弱性の確認のために、Webアプリケーションのスキャンを行う。侵入テストを定期的に行う。脆弱性が発見された場合にパッチの適用やアップデートが迅速にできるよう、パッチ管理プログラムを開発する。
- 企業レベルでホストベースのアンチウイルスソリューションを導入し、これを継続的にアップデートして、そのエンジンとウイルス定義を最新の状態にしておく。

調査対応の詳細

ITセキュリティチームは、Webアプリケーションサーバーにアクセスしているインバウンドトラフィックが大量にあるのを見つけました。アンチウイルスによる検知アラートも複数発生しています。我々はVTRAC | Investigative Response Teamと連絡を取り、VTRACのチームがこちらで調査をすることになりました。

インシデント対応のステークホルダーミーティングに出席したのは、ジェネラルマネージャー、法務部の担当部長、CISO、ITセキュリティ部門のほか、ハッカソンのWebアプリケーションを運用していたIT部門、VTRACの2名の調査担当者、そして私でした。

まず、CISOの報告によれば、今回のサイバーセキュリティインシデントの原因は「ハッカソンタレントサーチイベント」にあるとみて間違いないとのことでした。そして、個人情報（PII）のデータ侵害が発生しているというのです。

私にはこの話が信じられませんでした。候補者を調査するうえで慎重を期していたからです。そして、「就職先を探している人間がこのようなシステムトラブルを引き起こす理由などあるものか」とうっかり口走ってしまいました。

そのときです。法務部の担当部長が身を乗り出し、こう尋ねてきました。「直接的に表現すると、つまり、侵害の責任は我々の側にあるとおっしゃりたいのでしょうか」

VTRACの調査担当者が弊社のITセキュリティ部門とともに調査をした結果、採用候補者は誰もこの問題に関与していないことがわかりました。犯人は、Webアプリケーションサーバーの存在に気付いた悪意のある攻撃者だったのです。攻撃者はWebアプリケーションサーバーの脆弱性を突いた攻撃を仕掛けていました。

攻撃は、リモートでのコード実行の機能（RCE）にある脆弱性を狙ったものでした。そして、使用していたWebアプリケーションのフレームワークが旧版のもので、Webアプリケーションファイアウォール（WAF）が導入されていなかったことも、調査担当者は突き止めました。

侵害対応のヒント

- インシデント対応チームを編成する。チームには、個々のサイバーセキュリティインシデントに関係のあるステークホルダーを含める。適切なタイミングで警察当局と連絡を取るとともに、弁護士のアドバイスを受ける。
- マルウェア分析、エンドポイントフォレンジック、ネットワークフォレンジック、脅威インテリジェンス、隔離・駆除のサポートの項目を含め、調査対応では、資格と経験のあるデジタルフォレンジック企業と連携する。
- 証拠を収集、保存する。収集と保存に使うツールや手順はよく調査する。対象とする証拠には、揮発データ、ハードディスクイメージ、ネットワークパケットキャプチャ、ログデータを含める。
- 証拠の処理にあたっては、実績がありドキュメント化されている手順を使用する。エビデンスタグ、保管フォームチェーン、エビデンストラッキングログを用いて、証拠のセキュリティの確保、収集、維持・保存を行う。

サーバーには、リモートアクセスを許可するWebシェルが多数見つかりました。そして、環境にインストールされているアンチウイルスソフトウェアが検知・隔離を行う前に、攻撃者はこれらのWebシェルにアクセスしていました。

また、調査では、リモートログインの痕跡が確認されています。採用候補者の情報を格納しているデータベースに対しクエリ処理が行われ、それが完了していることもわかりました。そして最後にこれはログからわかったことですが、採用候補者の個人情報などをはじめとしたデータを、攻撃者はすでに盗み出していました。

攻撃者がアクセスしていたのが個人情報だったため、我々には、州の検事総長複数と被害を受けた個人に通知を行う法的義務が生じました。すぐに法務部門およびエグゼクティブマネジメント部門と連携し、データ侵害の発生を伝えるレターを作成したほか、問題を公表する場を設け、本件に関連するコーポレートメッセージの内容を検討します。

IT部門は、Webアプリケーションで実行しているフレームワークが旧版のものであることを認識していました。初回のハッカソンのあとにフレームワークをアップグレードするつもりでいながらそのままになっていたのです。案内状を送る候補者の数が少なかったため、WAFのない状態で旧版のフレームワークを運用しても短期間であれば問題ないだろうと決めてかかっていたのでした。

幸い、Webアプリケーションは社内ネットワークから分離したので、データがさらに漏洩するリスクは抑えることができました。

脅威の影響を軽減するためのヒント

- Webアプリケーションファイアウォール（WAF）、整合性管理（FIM）ソリューション、ホスト/ネットワーク侵入検知システム（IDS）を導入する。十分なログの取得を維持する。
- データの分離とネットワークのセグメンテーションを適切に行う。重要なデータやシステムの場合は特にこれを徹底する。

侵害対応のヒント

さまざまなデータ侵害のシナリオを想定して事前に広報対応の準備をしておく。個々のデータ侵害に合わせて実際の対応を調整する。

得られた教訓

セキュリティを構成せずにインターネット上にサーバーを配置した場合、我々が招待した特定の個人に限らずそこに誰もがアクセスして情報を閲覧できてしまうのだと思い知らされました。今回の件から学んだ大きな教訓です。

侵害が起こってから対応することだけがITセキュリティ部門の役目ではありません。ITセキュリティ部門は、あらゆるプロジェクトにおいて積極的に役割を果たす必要があります。また、組織のセキュリティに生じる影響を広範に考慮することなく開発を急いではいけません。この点は非常に重要です。

脅威の影響の軽減と防御のためのヒント

- Webアプリケーションは業界のベストプラクティスにもとづき開発する。ソフトウェアの開発では、セキュアな開発ライフサイクルに従う。ライフサイクル全体に情報セキュリティの概念を組み込む。
- Webアプリケーションのスキャンを行い、脆弱性が存在しないか確認する。侵入テストを定期的に行う。脆弱性が発見された場合にパッチの適用やアップデートがすばやくできるよう、パッチ管理プログラムを開発する。
- 企業レベルでホストベースのアンチウイルスソリューションを導入し、これを継続的にアップデートして、そのエンジンとウイルス定義を最新の状態にしておく。
- Webアプリケーションファイアウォール（WAF）、整合性管理（FIM）ソリューション、ホスト/ネットワーク侵入検知システム（IDS）を導入する。十分なログの取得を維持する。
- データの分離とネットワークのセグメンテーションを適切に行う。重要なデータやシステムの場合は特にこれを徹底する。

検知と対処

- インシデント対応チームを編成する。チームには、個々のサイバーセキュリティインシデントに関係のあるステークホルダーを含める。適切なタイミングで警察当局と連絡を取るとともに、弁護士のアドバイスを受ける。
- マルウェア分析、エンドポイントフォレンジック、ネットワークフォレンジック、脅威インテリジェンス、隔離・駆除のサポートの項目を含め、調査対応では、資格と経験のあるデジタルフォレンジック企業と連携する。
- 証拠を収集、保存する。収集と保存に使うツールや手順はよく調査する。対象とする証拠には、揮発性データ、ハードディスクイメージ、ネットワークパケットキャプチャ、ログデータを含める。
- 証拠の処理にあたっては、実績がありドキュメント化されている手順を使用する。エビデンスタグ、保管フォームチェーン、エビデンストラッキングログを用いて、証拠のセキュリティの確保、収集、維持・保存を行う。
- さまざまなデータ侵害のシナリオを想定して事前に広報対応の準備をしておく。個々のデータ侵害に合わせて実際の対応を調整する

リモートでのコード実行の機能における脆弱性

リモートでのコード実行の機能（RCE）にはいくつかの欠陥があり、これらの存在が、リモートでの悪意あるコードの実行を攻撃者に許しており、この結果、攻撃者は、Webアプリケーションサーバーをアプリケーションのユーザーアカウントの権限で完全に制御できてしまいます。

RCEの脆弱性を突き、これに成功すれば、攻撃者はアクセス権限が得られ、さらなる攻撃としてシェルのコンテキスト内にシェルコードを埋め込み実行することが可能になり、このコードは事実上、任意のコマンドを手動で実行できる簡易チャネルとして機能します。

RCEには、入出力データを評価する適切な手段や、信頼できないデータを適切に処理する方法がありません。RCEの脆弱性を突いた攻撃が効果を発揮する理由としてよく指摘される点です。そのため、ユーザーの入力データは、クライアントレベルとサーバーレベルで無害化することをお勧めします。特に後者のレベルでの無害化はより重要です。

偽のアクセスポイントを設置してWiFiを狙うフィッシング攻撃

2018年データ漏洩/侵害ダイジェスト

verizon

概要

企業ワイヤレスネットワークにはよく目にする設定の不備があり、これを初回攻撃で突かれ多くの企業ネットワークが侵害を受ける可能があると、弊社の最高経営責任者（CEO）は最近あるレポートを通じて知ったそうです。サイバーセキュリティディレクターである私は、ワイヤレスネットワークの侵入テストをなんとしても実施しなければならないと考えていましたが、このレポートのおかげでやっと、ベライゾンのProfessional Servicesを通じたテストの実施の承認を得ることができました。

侵入テスト

評価が完了して、ベライゾンの侵入テスト担当が説明するところによれば、リスクのきわめて高い固有のワイヤレスに関する脆弱性が複数、私たちのネットワークに見つかったといいます。このままでは、Active Directoryが攻撃者から脆弱性攻撃を受け、社内ワイヤレスネットワークに侵入されて、ネットワークがさらにいくつもの攻撃に見舞われる危険があるとのことでした。

侵入テストの担当者ははじめに、弊社のワイヤレスネットワーク名、すなわち、Service Set Identifier（SSID）のふりをして強力な信号を発するアクセスポイント（AP）を設定しました。デフォルトではデバイスは、SSIDをベースとして既知のAPを自動的に識別し、最も信号の強力なAPとの接続を試みます。

Wi-Fiを狙ったこの攻撃では、「エビルツイン」と呼ばれる偽のAPを設置し、これを通じてワイヤレス接続を補足傍受します。すでにワイヤレスネットワークに接続しているクライアントに対しては、認証解除のパケットである「deauth」を送信します。確立済のクライアントのコネクションをdeauthパケットが強制的に切断し、「エビルツイン」APにクライアントを無理やり再認証させるのです。

脅威の影響を軽減するためのヒント

脆弱性の評価を定期的に実施する。ワイヤレスクライアント、アクセスポイント（AP）ならびに、認証サーバー、認可サーバー、アカウンティングサーバー（AAA）のすべてに対し、定期的にパッチを適用する。

検知のためのヒント

ワイヤレスネットワーク対応の侵入検知システム/侵入防止システム（IDS/IPS）ソリューションを導入し、問題のあるワイヤレスネットワーククライアントやAPを検知し、攻撃を阻止する。

ワイヤレスネットワークのグループポリシー

「Wireless Network Policies Group Policy」というグローバルポリシーの拡張機能をMicrosoft WindowsのActive Directoryに実装することを検討する。

- インターネット接続の共有（ICS）は無効にする。Microsoft Windowsのファイアウォールを有効にする。
- 信頼できる正規のサーバー証明書のみを使用する。
- 信頼できるルート認証局（CA）を構築する。
- 新しいサーバーや信頼できるCAを受け入れる機能を制限する。
- コモンネーム（CN）はRADIUSサーバーだけに指定する。
- IDのプライバシーを有効にして、クライアントが暗号化されていない外部のトンネルでユーザー名を送信するのを防ぐ。

脅威の影響を軽減するためのヒント

- APへのクライアントの接続は、信頼できるルート認証局（CA）の証明書を使った接続だけに制限する。
- 2要素認証（2FA）または相互認証を義務付ける。

弊社で利用しているラップトップは構成が適切でなく、サーバー側の信頼できる証明書だけを有効にするようになっていませんでした。従業員は新しい証明書の受け入れを許されており、そのため信頼テストの担当者は偽の証明書を提示することが可能でした。

偽の証明書が受け入れられると、暗号化されたトンネルが確立されます。そしてこれにより、Windowsのドメインユーザー認証情報など、クライアントが送信する認証情報すべてがキャプチャできるようになります。

この時点でテスト担当者はワイヤレスネットワークへの接続が可能になりました。どのレベルで内部ネットワークにアクセスできるのかもわかります。弊社のワイヤレスネットワークにはセグメンテーションが施されていませんでした。そのため、テスト担当者はすぐにネットワーク全体にアクセスできるようになりました。

検知のためのヒント

ワイヤレストラフィックを監視し、想定外のトラフィックが就業後の時間帯に発生するなどといったように異常なアクティビティが存在しないか確認する。定期的にスキャンを実行し、未知のデバイスが存在しないか確認する。

侵害対応のヒント

攻撃の監視と検知、監査およびロギング、証拠の収集およびインシデント対応に、エンドポイントセキュリティソリューションを活用する。

テスト担当者からの情報によれば、このようなレベルのアクセスが許可された状況では、攻撃者はスキャンにより脆弱性を特定できるようになるほか、ドメインコントローラーに照会を行い、サービスプリンシパル名（SPN）を確認することも可能になるといいます。これは、あらゆるドメイン管理アカウントの略奪とWindows環境の侵害を攻撃者に許すことにつながります。

そして、ドメイン管理者アカウントの侵害に成功した攻撃者はさらならネットワーク攻撃の手段をほぼ無制限に利用できます。新たなアカウントを作成できるほか、TACACS+やRADIUSをはじめとした、認証サーバー、承認サーバー、アカウンティングサーバー（AAA）の侵害、バックドアのインストールが可能です。財務や知的財産などに関する機密性の高いドキュメントも閲覧できます。

脅威の影響を軽減するためのヒント

- ワイヤレスネットワーククライアントやAPなどの情報資産について目録の作成と分類を行う。
- ワイヤレスネットワークを有線ネットワークから分離する。

得られた教訓

自社のネットワークがいかに攻撃に対して脆弱であったのかを、実際にデータ侵害を受ける前に侵入テストを通じて把握できたのは非常に幸運でした。

ベライゾンの侵入テスト担当者から得られたアドバイスの内容を実行に移すべく、我々はすぐに作業に取り掛かりました。また、インシデント対応プランを見直し、以下のアドバイスを反映しました。

検知と対処

- ワイヤレスネットワーク対応の侵入検知システム/侵入防止システム（IDS/IPS）ソリューションを導入し、問題のあるワイヤレスネットワーククライアントやAPを検知し、攻撃を阻止する。
- ワイヤレストラフィックを監視し、想定外のトラフィックが就業後の時間帯に発生するなどといったように異常なアクティビティが存在しないか確認する。定期的にスキャンを実行し、未知のデバイスが存在しないか確認する。
- 攻撃の監視と検知、監査およびロギング、エビデンスの収集およびインシデント対応に、エンドポイントセキュリティソリューションを活用する。

脅威の影響の軽減と防御のためのヒント

- 脆弱性の評価を定期的に実施する。ワイヤレスクライアント、アクセスポイント（AP）ならびに、認証サーバー、認可サーバー、アカウンティングサーバー（AAA）のすべてに対し、定期的にパッチを適用する。
- APへのクライアントの接続は、信頼できるルート認証局（CA）の証明書を使った接続だけに制限する。
- 2要素認証（2FA）または相互認証を義務付ける。
- ワイヤレスネットワーククライアントやAPなどの情報資産について目録の作成と分類を行う。
- ワイヤレスネットワークを有線ネットワークから分離する。

その他Wi-Fiのセキュリティで考慮すべき点

Wi-Fiのセキュリティでは、以下の点についても考慮する必要があります。

- 「Wireless Network Policies Group Policy」というグローバルポリシーの拡張機能をMicrosoft WindowsのActive Directoryに実装する（前ページの補足記事を参照）。
- これらの接続はインターネットからの信頼できないリモートアクセスとみなす。バーチャルプライベートネットワーク（VPN）を導入する。
- Wi-Fiの利用を許可する時間を明確に定義する。
- 内部ネットワークへのアクセスを許可するに先立ち、ネットワークアクセス制御（NAC）テクノロジーを利用する。
- クライアントやサーバーの証明書に公開鍵暗号基盤（PKI）を組み合わせ、EAP（Extensible Authentication Protocol）とEAP-TTLS（Tunneled Transport Layer Security）の手法を併せて導入する。
- ワイヤレスクライアントをAPアイソレーションで個々にかつ動的に分割し、検疫を行う。
- リモート接続のデバイスに検疫を行う。たとえば、内部ネットワークリソースへの接続を許可する前に、パッチ適用の状態、設定、アンチウイルスの状態が最新かつ必要な要件を満たしているかチェックする。
- 会社が承認したワイヤレスネットワークだけを集め、「推奨するネットワーク」としてリストにまとめる。リストのネットワークとは別にユーザーが個別に利用しているネットワークがある場合にユーザーがそのネットワークをリストに追加できないようにする。注：これを行ったためにモバイルでの利用でラップトップをパブリックWi-Fiに接続できなくなってユーザーの「利便性が低下」する場合は、VPNを使用します。VPNであればモバイル環境でのネットワーク利用のリスクを軽減できます。

コロケーションデータセンターの利用がもたらした教訓

2018年データ漏洩/侵害ダイジェスト

verizon

概要

VTRAC | Labsでは大量のフォレンジックデータを扱っていますが、迅速に処理を進めています。システムイメージと関連する揮発性データの詳細分析に向けて、VTRAC | Investigative Response Teamの調査担当者がこれらデータの早期提供を強く望んでいるためです。

ある火曜日の朝、調査担当者は特に不安を抱いていました。顧客のデータがコロケーションデータセンターにホストされていたため、問題の調査の開始が遅れていたのです。データを収集する作業はデータセンターの「現場職員のチーム」に任せるしかありませんでした。調査対象のサーバーにハードドライブを接続してデータを収集してもらうことになっており、それが完了するのを待っていたのです。

数日が経過したのち、VTRACの調査担当者は、データのイメージを取得する処理が完了した旨の電話連絡を受け、この証拠データの発送に関する追跡番号を知らせる連絡を調査担当者が配送業者から受け取るまでにさらに日がかかりました。

そして発送された証拠データが到着したとの知らせがやっと届きました。配送業者からパッケージを受け取り、トレーサビリティの処理とリスト登録の処理を完了して、ドライブをステージング環境に接続しました。ドライブを接続してからわかったのですが、そのなかにはデータが何もありませんでした。

一体何が起きたというのでしょうか。

脅威の影響を軽減するためのヒント

- あらゆる資産について資産目録を維持管理する。遠隔地にあるシステムの情報をドキュメント化するとともにシステムにラベルを付ける。
- コロケーションサービスプロバイダーすべてについて、連絡先リストを最新の状態に維持する。
- インシデント対応手順をテストおよび評価する。コロケーションサービスプロバイダーと連携する。

調査対応の詳細

数日前に作業対象範囲を特定していたときに、VTRACの調査担当者は、対象のサーバーがコロケーションのデータセンターにホストされていることを知りました。調査担当者を現地に送りデータを収集したいと申し出ましたが、ポリシー上それはできないとコロケーションサービスプロバイダーに断られてしまい、プロバイダーの現場職員のチームにデータ収集の作業を任せるより仕方ありませんでした。

一般に、このようなデータ収集のリクエストに対応できる十分に体制の整ったシンプルなコロケーションデータセンターが存在する一方、一部のコロケーションデータセンターでは、現場の作業者との連携に問題を抱えています。多くの場合、問題のあるコロケーションデータセンターでは、ドキュメントされたプロセスがありません。そのため、ハードドライブの接続が必要となるサーバーや、個々の仮想マシンをホストしている物理アプライアンスを、特定できません。

コロケーションデータセンターでは、ユーザーは、物理システムをほかのユーザーとシェアしているため、データのイメージを取得する場合、ドライブにそれぞれのユーザーのデータが混在していることが原因で、ドライブのイメージを丸ごと取得できない可能性があります。

コロケーションデータセンターに関して考慮しておくべき事項

コロケーションデータセンターのデータを調査で利用する場合、十分な事前準備が必要です。調査にあたり考慮しておくべきいくつかの事項を以下に示します。

- 調査対象の証拠データがどのロケーションデータセンターにあるのかを理解しておく：複数のコロケーションデータセンターを利用している場合、システム、メモリ、ログ、データがどこにあるのか正確に理解していれば、証拠データの収集と保存にかかる時間を短縮できます。
- 誰が何をしているのかを把握する：データ侵害の発生時に個々のステークホルダーの役割を把握できていないと、混乱を招き、貴重なリソースを無駄にすることになります。役割を把握するうえで、RACIマトリックスの使用を検討しましょう。
- コロケーションデータセンターのシステムに物理的にアクセスできるのは誰なのか知っておく：サイバーセキュリティインシデントが発生しているときに承認プロセスを通じて、データストレージにアクセス権を得ていれば、余計な作業の遅れが生じてしまいます。
- コロケーションデータセンターでのデータの収集方法を知っておく：証拠データの収集プロセスを理解し、そのテストを事前に行っておけば、収集で遅延の発生するリスクを抑えられます。

侵害対応のヒント

- サードパーティーと連絡を取る際の手順をインシデント対応プランに取り込む。サイバーセキュリティインシデントの発生前に、連絡手順、エスカレーション手順の定期的なテストを行う。
- コロケーションサービスプロバイダーを利用する場合は、デジタルエビデンスの収集の経験を有し迅速にその対応ができるプロバイダーを選択する。
- システムのログとネットワークのログを含め、デジタルエビデンスへすぐにアクセスすることをコロケーションサービスプロバイダーに要求し、それを検証する。

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	* *
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	* *

図1：「ゼロクリア」されたハードドライブのセクター

コロケーションサービスプロバイダーが、正しいデータの格納されたドライブの提供を顧客に求めたことで、さらに1日の作業遅延が発生していました。また、これにより、我々の対応窓口では、1日で配送に対応する体制を急遽整える必要がありました。

データ収集のプロセスには何も問題がないと顧客は報告してきました。また、データを格納したドライブを発送前に暗号化するよう指示したとのことですが、その内容についても問題は見当たらないと言っています。しかし証拠スが入っているというドライブをマウントしても中身は空であり、我々はショックを受けました。

通常、ドライブを暗号化する場合、2つあるいずれかの方法が用いられます。暗号化したコンテナを使用しているのであれば、イメージのなかにそのファイルが存在します。ドライブ全体を暗号化している場合は、初期化が必要である旨が、Microsoft Windowsのオペレーティングシステムで示されます。

別のあまり一般的でないケースでは、暗号化された複数のパーティションのうちの1つで、ディスクが初期化されていながらデータにアクセスできなくなることがあります。しかしこの場合は当てはまりません。

別のディスクパーティションが存在していたり、ほかの暗号化手法が使われたりしていないかと疑い、フォレンジックツールの1つでディスクを調べてみましたが、残念ながらハードドライブのセクターには、16進文字の「00」しか存在しませんでした。つまり、ハードドライブには、何もデータがなかったのです。何が起こっているのか確認すべく、我々はすぐに顧客のコンタクト窓口に連絡を取りました。

先方の説明によれば、発送を担当した人間は当初より、収集と発送の指示に従って処理を行ったと主張していると言います。しかし、さらに調査を行った結果、すべてのデータを単一のドライブにまとめていたことを認めました。なぜそのようなことをしたのか、正確な理由は全くわかりませんでしたが、その過程で何かが起こり、データをドライブにコピーできなくなったのは間違いありません。翌日、我々のもとに、証拠データが正しく格納されたドライブが届きました。このドライブには、すでにトレーサビリティの処理も施されていました。データの収集を始めるだけですでに数日を要していたことを考えると、高い授業料を支払ったかたちになりました。コロケーションサービスプロバイダーのエビデンスデータの収集ミスで我々の調査も遅れ、顧客のビジネスに支障が生じています。

得られた教訓

今回の件で、顧客は、コロケーションデータセンターにデータを移したことを問題視していました。データの収集が必要になった場合の収集方法を詳しく理解せず、収集のための明確な手順を用意しないままに、データを移行してしまっていたのです。

脅威の影響の軽減と防御のためのヒント

- あらゆる資産について資産目録を維持管理する。遠隔地にあるシステムの情報をドキュメント化するとともにシステムにラベルを付ける。
- コロケーションサービスプロバイダーすべてについて、連絡先リストを最新の状態に維持する。
- インシデント対応手順をテストおよび評価する。コロケーションサービスプロバイダーと連携する。

検知と対処

- コロケーションサービスプロバイダーを利用する場合は、デジタルエビデンスの収集の経験を有し迅速にその対応ができるプロバイダーを選択する。
- サードパーティーと連絡を取る際の手順をインシデント対応プランに取り込む。サイバーセキュリティインシデントの発生前に、連絡手順、エスカレーション手順の定期的なテストを行う。
- システムのログとネットワークのログを含め、デジタルエビデンスへすぐにアクセスすることをコロケーションサービスプロバイダーに要求し、それを検証する。

誤警報 – 想定外の要因で発生したドメインユーザーアカウントのロックアウト

2018年データ漏洩/侵害ダイジェスト

verizon

概要

私はここ数年にわたり、ある企業でITセキュリティ部門の責任者を務めています。数週間前にDoS攻撃を受け、パスワードに関係するログオンのトラブルが原因で、数千のドメインユーザーアカウントがロックアウトされてしまいました。

ITヘルプデスクには、従業員から、ドメインユーザーアカウントのロックの解除を求める問い合わせが殺到しました。アカウントによっては、ロックを解除してから1日か2日で再度ロックされてしまうものもありました。

しかも問題の起こったタイミングが最悪でした。週末が祝日と重なっており、ITセキュリティチームのメンバーの多くが、すでに休暇を取っていたのです。

最初の調査でインシデント対応(IR)チームは、ドメインコントローラーのロックアウトの原因となっているログオンのトラブルが、まだ識別できないあるシステムに起因していることを突き止めました。ドメインコントローラーのMicrosoft Windowsのセキュリティイベントログを調査した結果、ログオンのトラブルはBase64エンコードされた引数を含むWindows PowerShellコマンドに関係していることが明らかになりました。

スタッフの数が限られていたために、根本原因をすぐに特定することができませんでした。調査のためにネットワーク管理者を休暇から呼び戻さざるを得ませんでした。また、真相究明に向けた調査の支援を要請すべく、VTRAC | Investigative Response Teamにリテーナサービスを依頼しました。

脅威の影響を軽減するためのヒント

- アカウントのパスワードのロックアウトポリシーをより現実的なものに修正する。たとえば、30分以内に5回パスワードの入力を間違えたらアカウントのロックアウトを起動するようにする。
- 侵入防止ソリューション（IPS）のルールを作成し、一定の時間内に複数回発生した特権アカウントのリクエストエラーを特定する。
- 侵入テストやセキュリティ評価を行う場合はその旨を、ITセキュリティ部門の主要な特定のメンバーに知らせておく。
- ユーザーアカウントポリシーをアップデートし、以下の内容をネットワーク管理者に明示的に義務付ける。上位の権限が必要な特定の業務では、2要素認証（2FA）を使用する。通常の業務では、上位の権限は使用しない。

調査対応の詳細

弊社のデータセンターに到着したネットワーク管理者とVTRACの調査担当者は、Windowsのセキュリティイベントログとほかのネットワークログ関連付けて、異常なPowerShellのアクティビティが問題の根本原因を特定しました。

さらに、VTRACの調査担当者は、弊社標準の命名規則に従わない不思議なな名前のシステムがそのアクティビティの元にあることをすばやく見抜きました。しかし、ここ数年、ネットワーク図をアップデートしていなかったため、このシステムの位置をすぐに特定できませんでした。さらに調査を進めた結果、このシステムは第三者の侵入テストベンダーに割り当てられていることが判明しました。

この侵入テストベンダーとの会話により次の事実が明らかになりました。問題の発生した週の火曜日から木曜日までのあいだに、約10,000のユーザーアカウントに対して1回限りのパスワードの推測を、ベンダーは何度か試みていたのです。さらには、48時間以内に3度ログオンに失敗したらアカウントをロックアウトするよう、アカウントのロックアウトポリシーが設定されていることが、MicrosoftのActive Directoryを扱うチームとの電話を通じてわかりました。

テストの間に侵入テストベンダーは、48時間以内に数回の推測であればほとんどのアカウントロックアウトポリシーで受け入れられるであろうと想定していたのです。しかし残念ながら我々の場合は、テストベンダーの想定どおりにはなりませんでした。

確認したログデータとアカウントのロックアウトポリシーを判断材料とし、侵入テストシステムによるパスワードの推測がアカウントのロックアウトにつながったとする結論に達しました。VTRACの調査担当者がBase64エンコードのコマンドをデコードすると、ロックアウトされるのは、特定のアカウントであることがわかりました。

調査を進めるなかで、あるユーザーアカウントが本番環境へのアクセスに上位の権限を使用していることが明らかになりましたが、このときユーザーが行っていた業務は標準のものであり、上位の権限は必要ありませんでした。この問題については、上位の権限を必要とする業務を行う場合に限り管理者アカウントを使用するようポリシーにおいてネットワーク管理者に義務付けることで解決を図りました。

サイバーセキュリティインシデントとその対応に関する指標

インシデントとその対応について追跡を行い、経営層に役立つ情報を提供します。これらの指標を活用すれば、サイバー攻撃のトレンドや、追加のリソースが必要な領域、トレーニングギャップの存在している箇所などを明らかにできます。

また、一部の指標は、主要パフォーマンス指標（KPI）を把握するうえでも役立ちます。KPIでは、主要なビジネス目標に照らし、組織の総合的なサイバーセキュリティ戦略の一環として、インシデント対応のパフォーマンスを評価できます。

サイバーセキュリティインシデントとその対応に関する指標の例を以下に示します。

- インシデント件数/年：年ごとのインシデントの総数
- タイプ別のインシデント件数/年：カテゴリ（優先順位、影響、緊急度）別での年ごとのインシデントの総数
- 時間数/インシデント：インシデントの解決に費やした時間の合計。サービスレベルアグリーメントに定められた時間内で処理されたインシデントの件数
- 日数/インシデント：インシデントの解決に費やした日数
- 投資コスト/インシデント：隔離、駆除、修復、復旧、情報の収集と分析などにかかる、インシデントごとの想定総投資コスト
- 影響を受けたシステムの数/インシデント：インシデントごとの影響を受けたシステムの総数

侵害対応のヒント

- IT部門、ITセキュリティ部門の重要なメンバーすべてを網羅した連絡先名簿を最新の状態に維持する。業務にあたるITセキュリティ責任者へ担当者の最新の空き状況を週単位で報告するよう、ファーストラインのスーパーバイザーに義務付ける。
- セキュリティ情報管理とイベント管理（SIEM）のソリューションを導入して、セキュリティアラートを発したソフトウェアやハードウェアの状態をリアルタイムに分析する。
- ネットワーク図と資産目録は定期的に、あるいは、ネットワークインフラストラクチャやネットワークコンポーネントに変更が生じた都度、アップデートする。

得られた教訓

すぐに問題のフォローアップを行い、インシデント対応チームと私は、所見と関係するアクションアイテムを今回の教訓の1つとしてリストにまとめました。

脅威の影響の軽減と防御のためのヒント

所見	パスワードのロックアウトポリーが適切であったなら、侵入テストを行っても、今回のような誤ったアラームが発生することはなかった。
アクションアイテム	アカウントのパスワードのロックアウトポリシーを修正し、30分間に5回パスワードの入力を間違えたらアカウントのロックアウトを起動するようにしました。また、侵入防止ソリューション（IPS）のルールを作成し、一定の時間内に複数回発生した特権アカウントのリクエストエラーを特定するようにしました。
所見	ユーザーアカウントがロックアウトされる現象についてITヘルプデスクが連絡を受けたものの、侵入テストが行われていたことを必ずしもITセキュリティ部門のメンバー全員が知っていたわけではなかった。
アクションアイテム	侵入テストやセキュリティ評価を行う場合はその旨を、ITセキュリティ部門の主要な特定のメンバー（例えば「テスト」の対象とならないメンバー）に知らせておくことを義務付けました。
所見	調査を進めるなかで、今回の問題とは直接関係ないことながら、あるユーザーアカウントが本番環境へのアクセスに上位の権限を使用していることが明らかになった。このときユーザーが行っていた業務は標準のものであり、上位の権限は必要なかった。
アクションアイテム	ユーザーアカウントのポリシーをアップデートし、上位の権限が必要な特定の業務では2要素認証（2FA）を使用することと、通常の業務では上位の権限は使用しないことをネットワーク管理者に明示的に義務付けました。

検知と対処

所見	問題対応の過程における重要性の高い局面において何人かのネットワーク管理者を休暇から呼び戻さねばならなかったが、連絡先名簿をアップデートしていなかったため、連絡を取るのに時間がかかってしまった。
アクションアイテム	IT部門、ITセキュリティ部門の重要なメンバーすべてを網羅した連絡先名簿を最新の状態にしました。また、業務にあたるITセキュリティ責任者へ担当者の最新の空き状況を週単位で報告するよう、ファーストラインのスーパーバイザーに義務付けました。
所見	Windowsのセキュリティイベントログを利用して監査証跡を残していましたが、広範かつ継続的にログオンデータフィールドをキャプチャするシステムを構築していませんでした。
アクションアイテム	システムロギングなどのセキュリティ情報ソースを集約する、セキュリティ情報管理とイベント管理（SIEM）のソリューションを評価しました。このソリューションにより、セキュリティアラートを発したソフトウェアやハードウェアの状態をより詳しく分析することが可能になります。
所見	ネットワーク図と資産目録を何年もアップデートしておらず、DHCP IPアドレスはリースしていたので、問題のシステムの特定に時間がかかってしまった。
アクションアイテム	ネットワーク図と資産目録のアップデートを義務付け、定期的なレビューを通じて、あるいは、ネットワークインフラストラクチャやネットワークコンポーネントに変更が生じた都度、アップデートをするようにしました。これにより、資産の管理人やオーナーをすばやく特定できるようになります。

なりすまし電話による認証情報の盗取

2018年データ漏洩/侵害ダイジェスト

verizon

概要

その日もITヘルプデスクではいつもと変わらぬ日常が過ぎていました。「処理の遅くなったコンピューター」の問題を解決したり、アプリケーションのインストールや再インストールをしたり、メール接続のトラブル対応のサポートをしたりしていました。しかし、そのような状況が、ITセキュリティディレクターとVTRAC | Investigative Response Teamからかかってきた電話を境に一変したのです。

彼らは、あるシニアエグゼクティブに関係したサイバーセキュリティインシデントの調査を行っていました。このエグゼクティブのアカウントでは、アカウントのロックアウトが大量に発生し何度もパスワードのリセットが行われていたので、その不審なアクティビティを理由にアカウントはすでに無効化されフラグが付けられていました。そして、WindowsのActive Directoryのログを調査したところ、私のチームの複数のメンバーによってパスワードのリセットが行われていたことが判明したというのです。

パスワードのリセットに関係するチケットの追跡で彼らは、ITヘルプデスクの責任者である私の協力が必要でした。

検知のためのヒント

短期間での多数のパスワードリセットや外部ソースからのアクセスなど、異常な認証イベントの発生時にアラートを発するようにして、監視を行う。

脅威の影響を軽減するためのヒント

VPNを利用する場合や外部ソースからメールを利用する場合など、機密性の高いリソースにアクセスするときは、多要素認証を使用する。

調査対応の詳細

先週のこのエグゼクティブのユーザーアカウントについて調査したところ、3件のチケットの発行が確認されました。これらは、パスワードのリセットと、VPNクライアントへのアクセスに関するサポートを扱ったものでした。このうちの2件はホットラインで受け付けており、残る1つは社内の窓口で直接対応したものです。幸い、ITヘルプデスクのホットラインにかかってきた電話の内容はすべて録音してありました。

そしてこの録音を聞くと、ホットラインに電話をかけてきた人物がシニアエグゼクティブ本人でないことは明らかでした。長年の経験上、私にはそれがわかりましたが、実際に対応したアナリストたちには区別がつかなかったことでしょう。

さらに電話の相手は、我々が用意していたいくつかのサイバーセキュリティ対策の目を逃れるための情報も準備していたのです。個々の通話の内容を以下に要約します。

なりすまし電話ケース1

ホットラインにかかってきた1番目のなりすまし電話の手口はきわめて単刀直入でした。

1. 慌てた口調から、スマートフォンのメールでトラブルを抱えている様子が伝わってきました。ユーザー名を忘れてしまったと言っています。電話の相手はシニアエグゼクティブの名前と役職を名乗りました。
2. ITヘルプデスクのアナリストがファイルにある秘密の質問を相手に尋ねました。「ご出身の大学はどちらですか」
3. 素性の知れないこの人物は、数秒間、黙りこみました。まるで何か情報を探しているかのようです。そしてためらいがちに答えました。
4. 「仰るとおりです」とITヘルプデスクのアナリストは声を上げ、シニアエグゼクティブのユーザー名を相手に伝えました。
5. 相手はアナリストに礼を言って電話を切りました。

なりすまし電話ケース2

最初の電話から2日して次のなりすまし電話がかかってきました。ある個人からのもので、仮想プライベートネットワーク（VPN）クライアントのインストールとメールへのアクセスでサポートを必要としていると言います。

1. 今度も同じシニアエグゼクティブになりすまし、その名前と役職、ユーザー名を名乗りました。ユーザー名という特別な情報のおかげで、電話の相手は秘密の質問を免れました。
2. ITヘルプデスクのアナリストは、この見知らぬ個人の「自宅」のコンピューターシステムにリモートでアクセスしてVPNクライアントをインストールし、Eメールポータルへのログイン方法を「改めて相手に伝え」ました。
3. しかし、ログインは失敗し、パスワードを「忘れてしまった」ようだと相手が述べたので、ITヘルプデスクのアナリストは躊躇なくパスワードをリセットしてしまい、電話の相手はメールポータルにアクセスできてしまいました。

社内の窓口に直接問い合わせのあった件が残っています。その件では、シニアエグゼクティブ本人が窓口に来たのです。あの電話の見知らぬ誰かのおかげでパスワードがリセットされてしまい、当の本人がシステムにログオンできなくなったためです。しかし、残念ながらそれでもまだ、問題は見過ごされたままでした。

調査の結果、最終的には次のことが明らかになっています。問題の素性の知れぬ相手はシニアエグゼクティブのメールアカウントにアクセスしており、盗取したユーザーアカウントを利用して、社外秘の財務データやビジネス戦略のドキュメントを盗み出していました。

侵害対応のヒント

ITヘルプデスクのチケットや、通話の録音記録、従業員への聞き取り調査の内容など、標準以外の情報源の利用を検討する

脅威の影響を軽減するためのヒント

技術的なサイバーセキュリティ上の脅威に加え、ソーシャルエンジアリング戦術などの非技術的な脅威にも焦点を当てて、エンドユーザーとヘルプデスクの担当者向けに意識啓発トレーニングを行う。

得られた教訓

ソーシャルエンジアリングという手法で、シニアエグゼクティブの機密データにアクセスするのに十分な情報を見知らぬ個人が収集できてしまいました。

脅威の影響を軽減するためのヒント

簡単に調査・特定のできる情報と関係を持たない強力な認証制御の仕組みを導入する。パブリックなフォーラムへの個人情報の投稿を制限する。

セキュリティ認証で使用する質問の内容は、一般によく利用されている職業ネットワーキングサイトなどのパブリックフォーラムで簡単に入手できるものであってはなりませんでした。

また、大量のパスワードリセットが発生したときにフラグの付与と調査をすばやく行えるプロセスも必要でした。このプロセスがあれば、今回のサイバーセキュリティインシデントを早期に把握できたことでしょう。

侵害対応のヒント

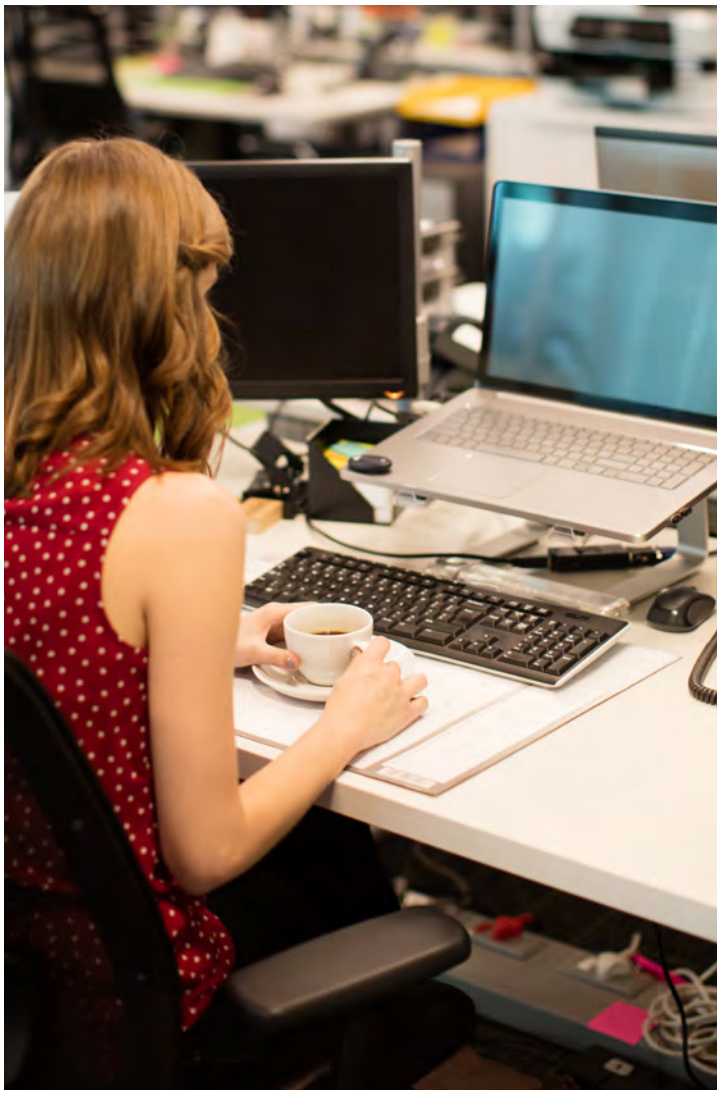
サイバーセキュリティイベントとインシデントの追跡を通じ、新たなリソースの割り当てが必要な領域を特定する。主要パフォーマンス指標（KPI）を使用して、インシデント対応のパフォーマンスを評価する。

脅威の影響の軽減と防御のためのヒント

- VPNを利用する場合や外部ソースからメールを利用し、機密性の高いリソースにアクセスするときは、多要素認証を使用する。
- 技術的なサイバーセキュリティ上の脅威に加え、ソーシャルエンジアリング戦術などの非技術的な脅威にも焦点を当てて、エンドユーザーとヘルプデスクの担当者向けにセキュリティ知識向上のためのトレーニングを行う。
- 簡単に調査・特定のできる情報と関係を持たない強力な認証制御の仕組みを導入する。パブリックなフォーラムへの個人情報の投稿を制限する。

検知と対処

- 短期間での多数のパスワードリセットや外部ソースからのアクセスなど、異常な認証イベントの発生時にアラートを発するようにして、監視を行う。
- ITヘルプデスクのチケットや、通話の録音記録、従業員への聞き取り調査の内容など、標準以外の情報源の利用を検討する。
- サイバーセキュリティイベントとインシデントの追跡を通じ、新たなリソースの割り当てが必要な領域を特定する。主要パフォーマンス指標（KPI）を使用して、インシデント対応のパフォーマンスを評価する。



なりすましメールによるデジタルハイジャッキング

2018年データ漏洩/侵害ダイジェスト

verizon

概要

トマス・ペインの詩のごとく、いまこそ人間の魂が試されるときです。そして、人事部門の気力が問われるときでもあります。怪しい人間が集まって、一般の人々を詐欺の罠に陥れようとしています。攻撃者は組織の内部の人間でしょうか。あるいは外部の人間でしょうか。アヒルの足並みを揃えて、羊の皮を被った狼から守るためには、誰が頼りになるのでしょうか。私利私欲のために誰もが悪事を働く可能性のある世の中では、用意しておかねばならないことがあります。

月曜日
エレベーターのドアが開いたとき、これから何か問題に巻き込まれるとアリスは気付きました。そして、トラブルが彼女の行く手に立ちはだかります。最高財務責任者（CFO）のボブがこちらに向かって歩いてきます。ボブの目的がアリスにはまだわかりません。辞任でも考えて悩んでいるのでしょうか。

「アリス、厄介なことになった」。ここは業界をリードするオーストラリアの洗濯洗剤メーカー、Wallaby Suds for Duds (WSD) Pty Ltdのオフィスです。この会社でアリスは人事部門のトップを務めています。二人の会話はいつものように重苦しい雰囲気で始まりました。「20万ドルもの大金が消えてしまった。記録を確認したところ、ある銀行振込の電信処理が行われていることがわかった。コピー機の修理契約に紐づいている。

まともに動いてもほとんど使いものにならないあのコピー機ね。年末に業者が修理に来るらしいけれど、それでも20万ドルだなんて。その金額はあり得ません」。

「アリス、事態は深刻だ。横領であることは間違いないが、誰が犯人なのかわからない。指示はすべて電子的に行われており、銀行は処理をすでに完了してしまっていた。代金の入金日に全額が現金で引き出され、どこかに消えてしまったんだ。追跡ができないらしい。詳細をメールで送ってある」

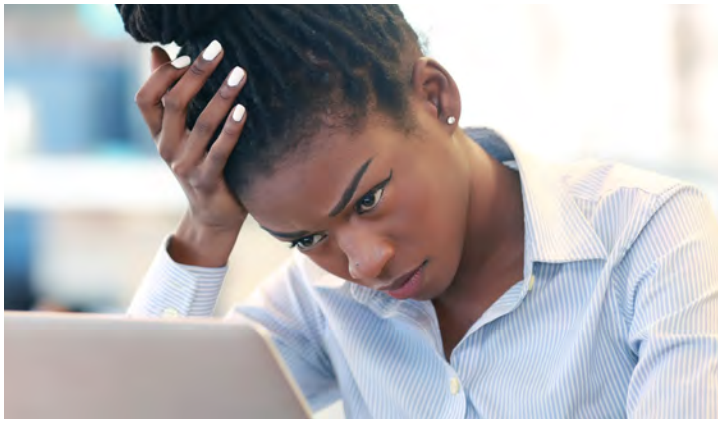
「買掛金を扱っている部署なんて、20世紀のままでしょう。コンピューターなんて使えるのかしら」。こう言ってからアリスは、自分を見るボブの目がちょっと睨んでいることに気付きました。「そんな目で見ないで。私を信頼してください、ボブ。いつものように、今回も私が何とかします」

いいかい、アリス。もしも買掛金を扱うスタッフのなかに犯人がいるとしたら、そのスタッフがさらに別の悪事を働くのをこのまま黙って見ているわけにはいかないんだよ。何が言いたいかわかるだろう？」ボブが帰っていくのをアリスが見送っていたとき、季節はずれの冷たい雨がアリスのオフィスの窓を打ち付けていました。部屋に戻ったアリスは、ぐったりと椅子にもたれました。長い1週間になりそうです。

検知のためのヒント

同じようなことがご自身の組織でもし起こった場合には、IT部門に連絡を取りましょう。また、買掛金を扱うスタッフが社内のどのような仕組みを利用できるのか、最新の包括的な資産台帳を使用して特定しましょう。そのような資産台帳を準備されていますか。

最新の人工知能ソフトウェアやセキュリティハードウェアイノベーションに惑わされず、まずは基本的な事柄をしっかり押さえておきましょう。具体的には、ネットワークの分離やユーザー権限の制限、資産の登録、ソフトウェアパッチの適用です。



調査対応の詳細

すぐに行動を起こさねばならないとアリスはわかっていました。WSDではセキュリティを重視しており、アリスはデータ侵害対応の模擬訓練のことを思い返していました。訓練では最初のステップとして、証拠の確保に努めたはずです。アリスにとって幸いだったのは、WSDが確立されたインシデント対応プランを準備していたことでした。すぐにチェックリストに目を通して、何をすべきか、誰に連絡を取るべきなのか把握することができました。

もしも今回の攻撃が財務部門に所属する内部の人間による犯行だとしたら、最優先で行うべきは、その犯人の手元にあるエビデンスの収集です。犯人の従業員に調査を行っていることを知られないよう、内密にことを進めねばなりません。

この後で、IT部門に電話を1本入れました。「ソフトウェアのアップデート」を名目に財務部門のラップトップを回収させたのです。そして、これらのラップトップを並べ、フォレンジック分析のためのイメージを収集しました。ITセキュリティチームはラップトップの電源をオンのままにしてメモリのダンプを採取し、現在進行中のアクティビティの証拠でディスクに書き出されていないものがないかチェックしました。インシデントチェックリストに従い作業を進めたことで、データを素早く収集できました。翌日の朝に1人目の従業員が出社してくる前に、ラップトップを元の場所に戻せています。

ラップトップのデータに加え、IT部門はネットワークのログデータも収集しました。疑わしいユーザーのシステムに関係するログデータをエクスポートし、分析のためにマーキングしました。そして徹底した調査をすべくアリスは、犯人が外部とコンタクトを取っていることを念頭に置き、Microsoft Exchangeのメールボックスの複製と中身の確認も要請しました。

アリスはそつなくチームを統制していましたが、それでも問題の全体像が見えません。そのため、専門家にサポートを依頼すべきときであると確信しました。アリスのスタッフは初動対応を行ううえでの訓練を十分に積んでいましたが、この問題を裁判で争う可能性があることも考えると、中立の立場での分析が必要でした。2時間にわたるスコーピングミーティングの後に、IT部門は、解析のためにVTRAC | Investigative Response Teamから求められたアイテムを暗号化し、コピーしました。

侵害対応のヒント

このような状況は関係者の誰にとってもにストレスになります。電子的な証拠を収集するための計画を立て、手順を確立しましょう。そしてこれらが機能するかどうかを、データ侵害対応のシミュレーションや障害復旧訓練の一環として定期的にチェックします。

インシデントに適切に対処するためには、計画と訓練が欠かせません。これらにより組織は、次のことが可能になります。

- 電子的な証拠を入手できる可能性が高まる。
- エビデンスの保存に要する時間を短縮できる。
- ステークホルダーごとに職務、職責の割り当てを行い、効率を高める。
- Iセキュリティ体制における弱点を特定してそれを補うことができる。

水曜日

フォレンジック分析が進行しているなかで、アリスは自らが得意とする調査の領域に集中して取り組むことにしました。木の枝を振って何かが落ちているかを見てみようとしました。しかしアリスはすぐに意気消沈してしまいました。不適切な要素が何か存在しないか探してもほとんど成果は上がりませんでした。従業員に対する聞き取り調査でも、何一つ不審な行動に辿り着く糸口を掴むことができません。

犯人は相当の知能犯なのか、あるいは内部の人間ではないのかもしれないと、ボブのオフィスへと向かう道すがら、アリスは思いを巡らしていました。そして、その日の聞き取り調査の成果を報告すると、ボブの顔には笑顔はありませんでした。

「アリス、君は任せて欲しいと言ったと思った」とボブの口調には容赦がありません。

「内部の者による犯行との見方で調査を進めてきましたが、方針の転換も視野に入れ始めています。別の可能性も検討する必要があると思います」

ボブは苛立って顔をしかめると、こう口にしました。「いいか。直接関与している者の存在なしにこのような問題が起こるはずがない。それは間違いない。その人物を探し出すんだ」

ボブのオフィスを出るときにアリスは、別のアプローチを見つけねばならないと確信していました。聞き取り調査を行っても成果は上がらず、ボブも何かを見失っているようです。新たな策を見出さねばなりません。アリスはスマートフォンを取り出すと、素早くEメール送信しました。相手は、証拠の調査を行っているセキュリティエキスパートです。「明日、電話会議をしたい。改めて状況を整理する必要がある」という趣旨のメールでした。

数分後に返事が来ました。会議の開始時刻とアクセス番号が書かれています。家に帰ると、アリスはお気に入りのスコッチを口にしながらつぶやきました。「何か答えが見つかるはず」と。そして止む気配のない雨を、ベネチアンブラインドの隙間越しにじっと見つめていました。

木曜日

アリスのスマートフォンが鳴りました。フォレンジックエキスパートからです。幸いなことにボブがひょっこりと姿を現しました。私の電話の会話に聞き耳を立てて、必要な情報を集めようとしています。

「ええ、ありがとう。それで内部での犯行ではないらしいと、そうなのね？ホエーリングですって。なんなのそれは？ああそうか、フィッシング詐欺の一種ね。彼が中間に、何ですって？ボブが会計パッケージをアップデートするようメールを送っていた？よく突き止めたわね。早くレポートを読んでみたいわ。ありがとう。それじゃまた」

「僕がこの件に関与しているだって」とボブがまくし立てます。

「ボブ、落ち着いて。犯人はあなたでもなければ、財務部門の誰かでもない。犯人は別にいます。これは中間者攻撃なんです」

アリスは話を続けました。そして、2週間前に攻撃者がボブになりすましたメールを偽造したと説明しました。そしてそのメールでは、使用している会計ソフトウェアにパッチを適用するよう財務部門の担当者に指示が出されていました。このアップデートは、ポーランド製の蛍光ペンを安く購入するためにユーロ記号をサポートできるようにするものであると称していました。

「ばかげている」とボブが声を上げました。

「仰りたいことはわかります。会計の専門家なら、ズウォティ（ポーランドの通貨）を使えばよいと知っているでしょう。とにかく、話を遮らないでください」。アリスはボブにかまうのは止めようと決め、攻撃者がどのような攻撃を仕掛けていたのか説明を続けました。

「マルウェアの仕業なんです。パッチだと思っていたものは実は、攻撃者が制御するサーバーを通じてインターネットトラフィックをルーティングしていたんです。おかげで攻撃者は、財務部門の従業員が使用していたあるゆるWebサイトを従業員に知られずに悪用し続けることができました。我々がシステムからログアウトした後に銀行の口座や分類コードが書き換えられてしまったら、それに気付く人は誰もいません。しかも、コンピューターに入力していたあらゆる情報を攻撃者は保存していたんです」

ボブが状況を理解したので、対応策を検討することになりました。失った金銭は戻らず、それが変わることはないでしょう。しかし、やらねばならないことが残っているのです。

脅威の影響を軽減するためのヒント

攻撃者は組織のプロセスやコンピューターのなかから弱点を見つけ出します。たとえば、財務部門では支払いの承認をする前に、振り込み先口座を詳しくチェックしているでしょうか。それともチェックしているのは振り込む金額だけでしょうか。

セキュリティ部門と連携して、ビジネスに対する個々の固有のリスクを緩和しましょう。これらのリスクには、データ侵害や従業員による不正行為、事業の停止、詐欺行為などがあります。

2週間後

許可を得ていないソフトウェアの実行を防ぐ目的で、アプリケーションのホワイトリスティング機能を導入しました。また、インターネットへのアクセスはプロキシサーバーを経由して接続するよう処理を変更しました。これにより、管理者や財務部門の従業員などの特権ユーザーが未知のWebサイトにアクセスするのを防ぐことができます。

メールのなりすましを容易にしてしまう、直近に見つかった脆弱性に対処できるよう、メールクライアントにはパッチを適用しています。また、DMARC（Domain-based Message Authentication, Reporting and Conformance）を有効にするようサーバーを再構成して、メールの送信者を認証するようにしました。

社外から届いたメールの件名には、「[外部より受信]」の文言を付加するようにして、なりすましメールの特定をこれまでよりずっと容易にしました。さらにアリスは、フィッシングについての知識を高めることを目的とした全従業員必須のトレーニングの予算をようやく獲得することができました。

「レッドチーム」演習も予約しました。強化した新たなWSDのセキュリティ体制を評価し、今回とは別のタイプの攻撃に関する脆弱性が存在しないか確認するためです。攻撃者は常に、脆弱性を見つけては攻撃を仕掛けてきます。しかし、アリス、ITチーム、セキュリティプロバイダーの三者は協力して、そのリスクの軽減に努めているのです。

教訓

ビジネスのセキュリティを確保するには、技術レベルでの管理を補うことのできる、手続きレベルでの管理が必要です。

脅威の影響の軽減と防御のためのヒント

- セキュリティ部門と連携して、ビジネスに対する個々の固有のリスクを緩和しましょう。これらのリスクには、データ侵害や従業員による不正行為、事業の停止、詐欺行為などがあります。

検知と対処

- 最新の人工知能ソフトウェアやセキュリティハードウェアイノベーションに惑わされてはいけません。まずは基本的な事柄をしっかり押さえておきましょう。具体的には、ネットワークの分離やユーザー権限の制限、資産の登録、ソフトウェアパッチの適用です。
- インシデント対応では、計画と訓練が欠かせません。これらにより組織は、次のことが可能になります。
  - 電子的な証拠を入手できる可能性が高まる。
  - 証拠の保存に要する時間を短縮できる。
  - ステークホルダーごとに職務、職責の割り当てを行い、効率を高める。
  - セキュリティ体制における弱点を特定してそれを補うことができる。