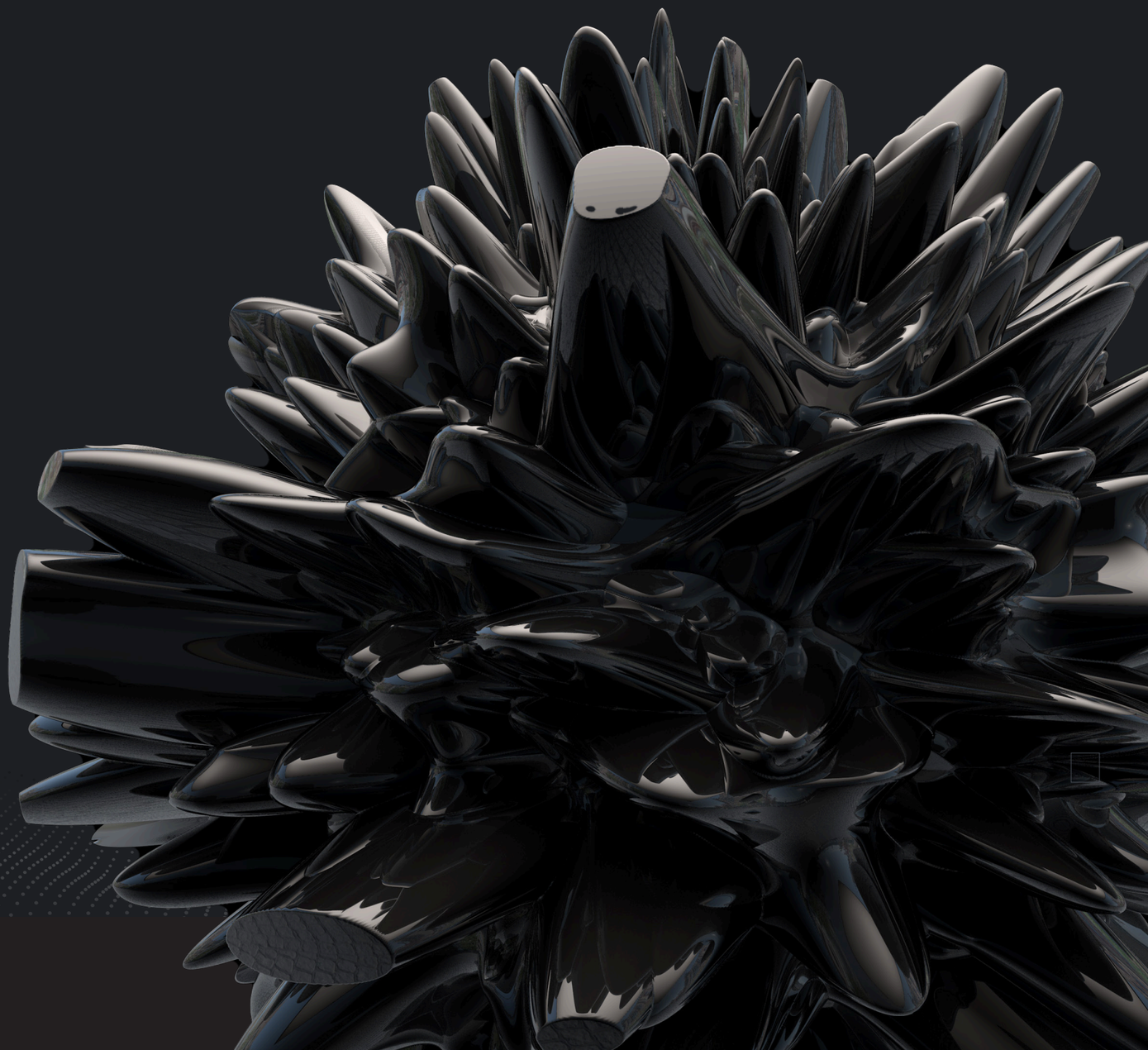
2020

脅威レポート



BlackBerry | CYLANCE

目次

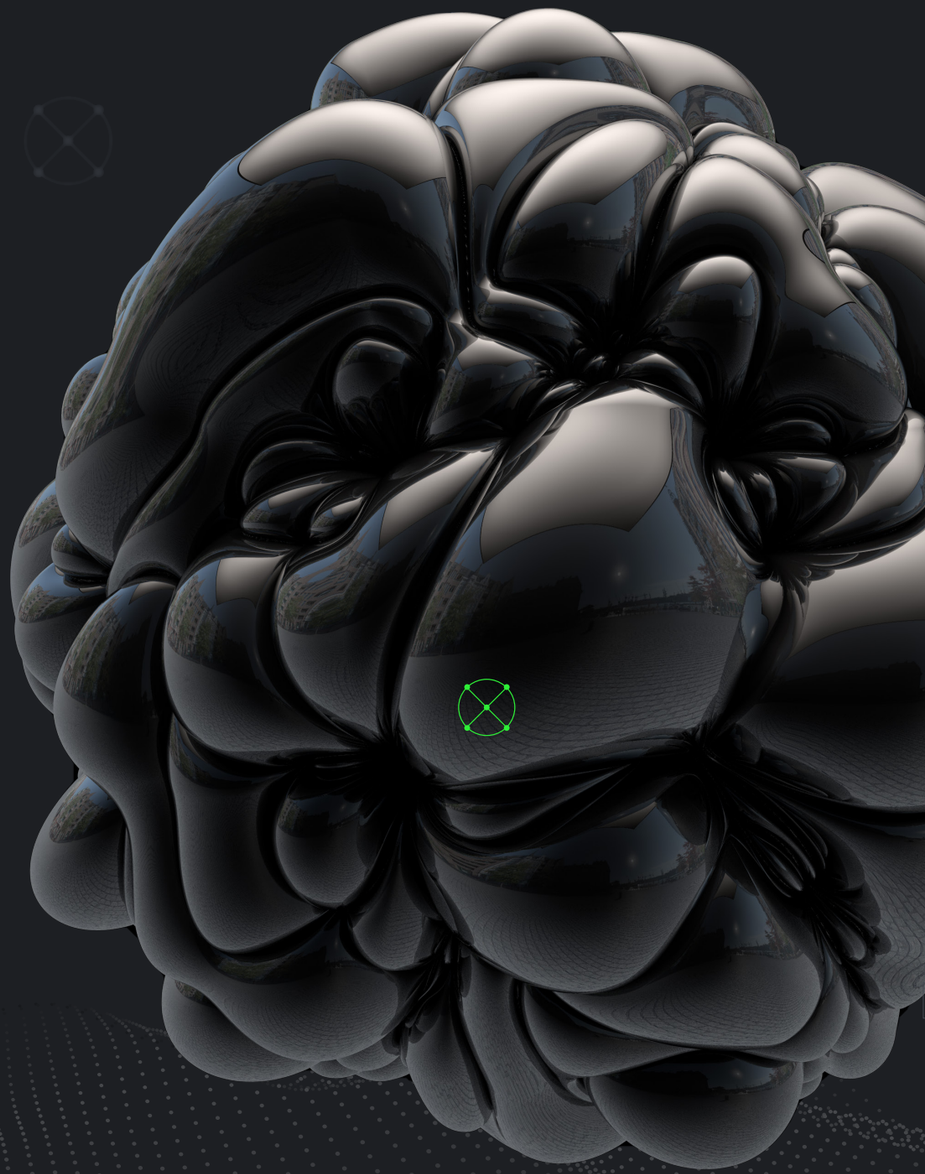
概要

「BlackBerry® Cylance® 2020 脅威レポート」には、ビジネス、政府、およびエンドユーザーの利益にとって重要な幅広いトピックが記載されています。このレポートでは、モノのインターネット（IoT）とモバイルセキュリティの先駆者である BlackBerry と、AI（人工知能）駆動型サイバーセキュリティの創始者でエンドポイントセキュリティ市場の破壊的革新者であるサイランス（2019 年 2 月に BlackBerry によって買収）のセキュリティに関する洞察を組み合わせて説明します。

これまでと同じとおり、全体的なセキュリティをパズルとするならば、このレポートは、弊社の考えを象徴するピースといえるでしょう。弊社の目標は、役割や役職に関係なく、誰もがセキュリティに関する情報、予測、教訓にアクセスできるようにすることです。「2020 脅威レポート」では、2019 年の重大なセキュリティ侵害を検証し、過去の過ちを繰り返さないようにすることができる最近の進歩について考慮します。ここでは、起きたことを単に時系列順に記述するだけでなく、そのようなイベントを許した条件を解析することも目的として、現在のサイバーセキュリティの問題について詳しく説明します。

しかし、このレポートは、単に 2019 年の重大な脅威を振り返って検証することが目的ではありません。ここでは、IoT、モバイルデバイス、ユーザー ID、組み込みシステム、敵対的 AI などの現代的問題の要素をはじめとして、2020 年のハイパーコネクテッドな世界に影響を及ぼすセキュリティの問題の概要を説明します。

このレポートに記載された情報により、今年から向こう 10 年の間に間違いなく明らかになる脅威の襲来に対して、読者が未然に行動を起こし、十分な情報に基づいて対抗措置に取り組めるようになることを心から願います。



エグゼクティブサマリー

- APT 攻撃グループとその他の敵対者は 2019 年を通じ、常に最新のマルウェアをリリースして巧妙な攻撃手法を誇示しました。敵対者が暗号化ルーチンを向上させ、ステガノグラフィによって悪意のあるペイロードを隠蔽することに力を注いだ結果、セキュリティ調査担当者と脅威検知ソリューションにとって作業の難易度が高まりました。さらに脅威アクターは、マネージドセキュリティサービスプロバイダー（MSSP）を侵害してその顧客の環境に侵入することで、攻撃を広く配布できるようにもなりました。
- 自動車やアプライアンスなどのデバイスが多様なネットワークに接続できるようになるにつれ、IoT は急成長しつつあります。接続がこれほど増加すると攻撃対象領域も同じように拡大するため、脅威アクターは複数の機会と場所を使ってシステムを侵害できるようになります。ビジネステクノロジーは IoT デバイスと相互作用するため、安全に保つのは困難ですが、継続的ユーザー認証の進化によって解決策が生まれる可能性があります。
- 最新の自動車は、エッジコンピューティングデバイスとほぼ同じくらいに進化しています。残念ながら、サプライチェーン、設計プロセス、および更新手順の脆弱性のため、自動車は攻撃者の格好の標的になっています。業界とサードパーティベンダーが自動車のサイバーセキュリティを向上させる手段を講じなければ、自動車の脆弱性は悲惨な結果を招くおそれがあります。
- ディープフェイクテクノロジーの普及が進んでいます。このため、ソーシャルメディアサイトにディープフェイクペルソナが登場し、フェイク音声による承認を使用して詐欺が行われるようになっています。組織は、ディープフェイクテクノロジーが使用されていることを表す指標を特定し、それに対処する方法に関して従業員をトレーニングすることを検討する必要があります。
- モバイルセキュリティは、脆弱なモバイルデバイス管理（MDM）サーバーから、エンタープライズクライアントと、それらと IoT デバイスの相互作用まで、さまざまな課題に直面しています。さまざまなセキュリティコントロールを自動化し、モバイルアプリコードの難読化を向上させ、スマートフォンをルート化／脱獄しないようユーザーに推奨すると、モバイルリスクの緩和に役立ちます。

ディープフェイクテクノロジーの普及が進んでいます。このため、ソーシャルメディアサイトにディープフェイクペルソナが登場し、フェイク音声による承認を使用して詐欺が行われるようになっています。

2019 年の APT のトレンド

APT 攻撃とは、高度な脅威アクターがエンタープライズネットワークへのアクセスを獲得し、そのネットワークに対して持続型攻撃を実行することを指します。APT は一般に、長期にわたって検知されない状態を維持したまま、監視、データの持ち出し、水平移動などの悪意のある操作を実行しようとします。

元々、APT グループは国の支援を受けている場合がほとんどで、その動機は対応する国のイデオロギーと利益に合致していました。最近では、この用語は、特定の国家との関連はないと考えられるものの、経済的利益を主な動機とする、高いスキルを持つ高度な脅威アクターを指す場合にも使われるようになっています。

APT は、侵害された組織内の特定の個人を標的にする場合もあります。標的として慎重に選んだ被害者に対し、ソーシャルエンジニアリングやスピアフィッシング、さらには不満を抱えた従業員から得た内部情報までもが使用されることがあります。

APT グループに関する脅威インテリジェンスを確認することで、企業は、エンタープライズに攻撃を仕掛けている人物、アクターの手口、および動機を理解できます。この情報は、脆弱なシステムを高度な脅威から保護するのに役立つ可能性があります。

以降の解析では、弊社が 2019 年に実施した脅威調査によって明らかになったツール、手法、および特定のアクターの概要について説明します。

標的として慎重に選んだ被害者に対し、ソーシャルエンジニアリングやスピアフィッシング、さらには不満を抱えた従業員から得た内部情報までもが使用されることがあります。

手法

ホスト依存型の暗号化

2019 年に BlackBerry Cylance が注目したのは、ホスト依存型の暗号化を使用してペイロードを保護する APT 関連のマルウェアサンプルが増加したことです。この手法はこれまで、最も機密性が高く高度にカスタマイズされたバックドアを保護するために使用されており、通常は Windows® データ保護 API によって実装されていました。

最近では、これらの暗号化メカニズムの多様化と普及が進んでいます。脅威アクターによっては、ホスト依存型の暗号化を、さまざまなツールやマルウェアと共に配布される汎用ローダーに組み込んでいます。

たとえば、OceanLotus グループは、ほぼすべてのインプラントをマルチステージローダーにラップし始めています。このローダーは、ユーザー名、コンピューター名、IP アドレス、または MAC アドレスの情報を使用して、ペイロードの復号鍵を派生するよう設定できます。この手法が使われていると、アナリストやマルウェアハンティングの専門家は、被害者の環境についての深い知識がなければペイロードを復号できません。

別の例では、第 1 段階のドロッパーが自身をコピーし、ランダムに生成されるワンタイムキーを使用して悪意のあるコードの一部を暗号化しています。その後、ドロッパーは元のバイナリを削除し、生成されたキーをパラメータとして使用して、暗号化されたバージョンを再実行します。このため、悪意のある機能が含まれるコードを復号するには、調査担当者は、マルウェアの 2 つ目のコピーを実行するために使用されたコマンドラインパラメータを知っている必要があります。ランダムに生成された鍵を見つけるのは、不可能ではないにしても、きわめて困難なタスクです。

ツール

サイバー兵器としてのランサムウェア

弊社が確認しているもう 1 つのトレンドは、標的型攻撃でのランサムウェアの使用です。このトレンドが初めて幅広い注目を集めたのは、WannaCry（2017）[1] が出現したときです。このランサムウェアは、少しの期間減少していましたが、その後、新たな機能を備えて復活しました。従来、ランサムウェアによる攻撃は、個人ユーザーや中小企業を狙った金銭的動機によるサイバー犯罪でした。しかし最近では、大企業や公的機関、政府がランサムウェアの攻撃を受ける事例が大幅に増加していることを確認しています。

最も洗練されたシナリオの場合、攻撃者は、被害者を慎重に選んで徹底的な偵察活動を行い、最適な侵入方法を見つけます。被害者の環境へのアクセスを獲得したら、まず情報窃取マルウェアを展開して機密データを持ち出してから、すべてのファイルを暗号化します。[2] 影響を受けた会社が復号ツールへの支払いを拒否した場合、攻撃者は、窃取した情報を公開すると脅して会社を恐喝しようとします。この情報には、会社の顧客の個人データが含まれることが多いため、データプライバシーの侵害になります。

標的型ランサムウェア攻撃の背後に潜む脅威アクターは、既知のマルウェアファミリーを再利用する傾向があります。このようなマルウェアファミリーの多くは、地下フォーラムで売られていたり、サービスとしてのランサムウェア（RaaS）ベンダーから購入したりします。このような攻撃の大半は、ほとんどの場合、単に恐喝が目的です。ただし、ランサムウェア攻撃の中には、重要なデータを破壊してプロセスやサービスを妨害することを目的としているものもあります。場合によっては、決済インフラストラクチャや暗号化ルーチンが被害が損なわれ、ファイルの復号や身代金の支払いができなくなることもあります。このような場合の攻撃は、単なるワイパーのようなもので、ランサムウェアを装ってはいるものの、最終的には単にデータを破壊します。2019 年の高度な標的型攻撃で使用されたランサムウェアファミリーとしては、Sodinokibi、Ryuk、Zeppelin などがあります。

手法

ランサムウェアの展開のために MSSP が標的に

2019 年半ば、Sodinokibi ／ Sodin ／ REvil と呼ばれる新たなランサムウェアが出現しました。これは企業を標的にしたもので、一部の米国政府機関で大規模な中断が発生しました。GandCrab と同じように、Sodinokibi の技術的詳細はきわめて平凡ですが、その展開方法は注目に値します。

ほとんどの場合、最初の侵害は、ターゲット組織の IT とセキュリティを管理しているマネージドサービスプロバイダー（MSP）と MSSP[3] を狙った標的型フィッシング攻撃によって発生しています。脅威アクターは、Go2Assist や NinjaRMM のようなリモート管理ツールを使用して、ターゲット組織内に築いた足掛かりを利用します。

内部に侵入すると、攻撃者は、Passcape のパスワード回復ツールのような一般的なツールを展開して認証情報を盗みます。さらに、セキュリティソフトウェアをホストしているサーバーにアクセスし、それらのサーバーを無効化します。続いて、ドメインコントローラに接続し、既存のソフトウェア展開ツールを使用して、環境内のすべてのマシンにランサムウェアを配信します。

MSP と MSSP は、脅威アクターにとって価値の高い標的であることが証明されつつあります。足掛かりを確立すると、攻撃者はそこを軸にして、環境内にある他の何百ものさまざまな脆弱な標的へ移動できます。2020 年には、MSP と MSSP が効果的なサイバーセキュリティツールを使用していることを確認することが組織にとって重要になります。

手法

自給自足・現地調達型

脅威アクターは依然として自給自足・現地調達（LotL）手法に大きく依存しており、これによって、セキュリティアラートをトリガすることなく、信頼されているシステムリソースをサイバー攻撃に使用しています。攻撃ベクトルはそれぞれ異なりますが、以下が含まれます。

- WMI などの偵察および水平移動用ツールと、組み込みのスクリプト言語（PowerShell、VBScript など）を使用する
- 管理ツールと開発ツールを使用して以下を行う
  - 検知回避
  - ファイルレスマルウェアの展開
  - プロキシ実行

LotL 攻撃は依然として多発している脅威であり、敵対者が攻撃ライフサイクルの後半の段階で利用する強力な手法です。

脅威アクター

OceanLotus の最新情報

2019 年初頭、OceanLotus（APT32 ／ CobaltKitty）として知られるベトナムの APT グループが、多国籍自動車メーカーを標的にした活発なキャンペーンを開始しました。[4] これらの攻撃はベトナムの国内自動車産業の支援が目的であった可能性がありますが、攻撃者の動機は依然として不明のままです。OceanLotus は、マクロが有効なドキュメントが含まれるスピアフィッシングメールを使用し、採用担当者やカスタマーサービスチームなど、インターネットに接続されている部門にそれらを送信することにより、自動車企業に侵入しました。

ドキュメントを開くと、一般的には、CobaltStrike ビーコン、または高度なバックドアの展開を実行する追加のダウンローダー（KerrDown）がダウンロード、実行されます。攻撃者は、多くの場合に LotL 手法を使用しており、偵察のために PowerShell と WMI、水平移動のために RDP に依存していました。

これらの自動車産業への攻撃中に、BlackBerry Cylance の調査担当者は、OceanLotus によって新たなバックドアが展開されていることを確認しました。更新されたこれらのバックドアは、モジュール式のコマンドアンドコントロール（C&C）通信を実行でき、通常は、大幅にカスタマイズされたファイルレスローダーによってメモリにロードされます。OceanLotus の新しいバックドアでは、潜伏状態を維持するために、高度な難読化、暗号化、およびステガノグラフィ[5] の手法が用いられています。

さらに、BlackBerry Cylance の調査担当者は、高度なネットワーク攻撃機能を用いた一連の新しいリモートアクセス型トロイの木馬（RAT）も発見しました。これらの RAT は Ratsnif と呼ばれ、OceanLotus によって開発されたものでした。このマルウェアは、2016 年から積極的に開発されているように見え、複数のネットワーク攻撃手法を組み込んだ真の万能ツールで、パケットスニッフィング、ゲートウェイ／デバイスの ARP ポイズニング、DNS ポイズニング、HTTP インジェクション、MAC スプーフィング[6] などの機能が結合されています。

ツール

オープンソースツールと既成の商用ツール

オープンソースツールや既成の商用ツールを悪意を持って使用する手法は、今年も拡大し続けたもう 1 つのトレンドです。Cobalt StrikePowerSploit、Empire などのツールキットが、国の支援を受けた活動から金銭的動機の攻撃まで多岐にわたるアクションのため、脅威アクターによって使用されています。[7]

これらのツールは元々、侵入テストのために作成されたもので、脅威アクターによる悪意のある用途に簡単に適応できます。広く利用可能なツールを使用することの利点の 1 つは、攻撃のアトリビューションが難しくなり、攻撃者が検知を回避できるようになる可能性があることです。企業は、これらのツールのアラートを過去の侵入テストに関連したものだと思い込み、無視または軽視する可能性があります。

手法

ステガノグラフィ

攻撃者は、引き続きステガノグラフィを使用してペイロードや通信を隠しています。ステガノグラフィでは、ファイルやメッセージを別のファイル内に隠すことが含まれます。その際、疑念を一切抱かせないのが理想です。攻撃者はグラフィックファイル形式の中に何年にもわたってコードやデータを隠し続けており、その好例が OceanLotus による PNG ファイル[8] の悪用です。

2019 年後半に、弊社は WAV オーディオファイル[9] 内にペイロードを隠している攻撃者を発見しました。一般的には、ステガノグラフィを使用した場合、鍵となる悪意のあるコンテンツはメモリ内にしか存在しないため、敵対者は検知を回避しやすくなります。ステガノグラフィ攻撃を検知してブロックするには、効果的なメモリ監視と脅威防御が必要です。

脅威アクター

APT-28 の活動

APT-28 グループは、2019 年も引き続き、ロシアの外交および経済上の利益と合致する攻撃を実行しました。[10] APT-28 の仕業と思われる攻撃の標的になったのは、またしても世界アンチドーピング機関（WADA）でした。WADA が国の支援を受けたサイバー攻撃の被害者になるのは今回で 2 度目です。これらの攻撃は、2020 年東京オリンピックへのロシアの参加の審査中に発生しました。

BlackBerry Cylance 脅威インテリジェンスが 2019 年に実施した解析により、それまで知られていなかった APT-28 のバックドアについての洞察が得られました。この解析が示す内容はすべて、比較的未熟な機能のセットを使った、記録のない新しいインプラントを指しています。独自のドメイン生成アルゴリズム（DGA）が実装されていることから、そのコードは公表されている APT-28 の他のツール[11] と関係があることを強力に示しています。この新しいバックドアは、低い検出率と、大容量の実行可能ファイルの展開のトレードオフとして、複数の静的ライブラリを使用しています。この APT-28 バックドア[12] を

解析したところ、このグループが標的ごとにツールの作成や作業を行って、機能セットを新しいツールとして再構築していることがわかりました。

ツール

Ryuk

Ryuk は、弊社が 2019 年に確認した中で最も活発なランサムウェアです。ほとんどの攻撃で、脅威アクターは Ryuk を Trickbot および Emotet と共に展開していました。その主な感染ベクトルは、悪意のある Microsoft® Office マクロが含まれるフィッシングドキュメントであり、このマクロによって Emotet マルウェアがダウンロードされます。その後、Trickbot がドロップされ、これを使用して特定の目標がいくつか達成されます。

第 1 に、Trickbot は銀行の認証情報を侵害することができ、以前から金融機関を標的とするトロイの木馬として知られていました。一部の攻撃では、まず Trickbot を使用して銀行情報を侵害してから、Ryuk を投入して暗号化操作を行います。この攻撃手法では、攻撃者は 2 つの攻撃を連続して実行できます。

第 2 に、Trickbot は優れたマルウェア拡散能力を持ちます。Trickbot は、まずメモリからパスワードをダンプしてから、Windows SMB の既定の共有を使用して横方向に移動して増殖します。

第 3 に、Trickbot は、Ryuk の展開も行う C&C チャネルによって制御されています。攻撃者は通常、環境内部で数週間かけてマッピングと偵察を行い、重要なサーバーと暗号化するバックアップを特定します。より高度な脅威アクターになると、通常はワークステーションは暗号化せず、サーバーのみを標的とします。

脅威アクター

Fin9

一般的に Fin9 として知られるこのグループは、2019 年には米国および米国外の MSSP を標的にしました。ネットワークへのアクセスを得た後は主にギフトカード詐欺を働いていることから、動機は金銭目的のようです。このグループは、フィッシングメールを使用して最初の足掛かりを得た後、認証情報を侵害し、さまざまな方法で環境内を横方向に移動します。

Fin9 は、LotL 手法を使用して、被害者の環境内でサポートされているリモートアクセステクノロジーの中から好ましいものを利用します。この脅威グループは、Keseya VSA、ScreenConnect、TeamViewer、およびネイティブの RDP を使用していることが確認されています。さらに、専用のインフラストラクチャに接続するよう設定された ScreenConnect クライアントの修正バージョンを使用していることも観測されています。

また、防御インフラストラクチャを標的にするほか、検知を免れるためにエンドポイントエージェントをアンインストールまたは無効化することもわかっています。MSSP のクライアントを特定したら、信頼されているアクセスを使用して、そのクライアントのネットワーク内へと拡散します。

手法

敵対的機械学習

アンチウイルス産業の誕生以来、悪意のあるアクターは、コンテンツスキャンエンジンによる検知を迂回、回避しようとしてきました。攻撃者は、脅威が検知されずに潜伏し続けるようにすることにより、攻撃の成功確率を向上させます。長い年月にわたりサイバーセキュリティスペシャリストは、当時の卓越した検知テクノロジーを迂回するための新しい（およびさほど新しくない）回避手法を数多く目撃してきました。例をいくつか示します。

- シグネチャスキャンを回避するためのポリモーフィズム
- エミュレーションとサンドボックスを迂回するための対仮想化
- スパムフィルターを迂回するためのテキスト操作
- 難読化と暗号化に基づくその他の変異手法

予想どおり、弊社は現在、サイバー脅威に対抗するための最新テクノロジーである機械学習と AI に対する標的型攻撃の増加を目撃しています。

機械学習モデルに対して敵対的攻撃を実行するというアイデアは新しいものではありません。機械学習の意思決定プロセスを覆そうと、調査対象者と敵対者の両方がデータを操る方法を探っています。[13] 人気があるのは、スパムエンジンの検知を回避する、画像認識機能をだまして物体を見落とさせる、AI モデルのトレーニングに使用されるデータセットを汚染する、といった方法です。

ここ 1 年で、機械学習分類器に影響を与えて、モデルの判定を有害から無害へ覆すことを目的としたさまざまな攻撃が明るみに出ました。たとえば、過剰な量の無害な機能を組み込むことによって既存の脅威を変異させるスタッフィング攻撃です。別の例としては、ファイルヘッダーを改変する攻撃、コードやデータを変更して無害なサンプルに偽装する改ざん攻撃があります。

幸いなことに、業界にとって永遠と思われる問題であっても、機械学習にとってはやっかいなように見えて実は好機でもあります。機械学習分類器に対する攻撃の増加を受けて、セキュリティ調査担当者は精力的にトレーニングセットを拡張し、トレーニングモデルに使用する特徴空間を洗練させています。これらのステップにより、最終的には異常に対する機械学習分類器の回復力が強化され、将来の攻撃に対する有効性が向上するはずです。

2019 年の全体的な脅威トレンド

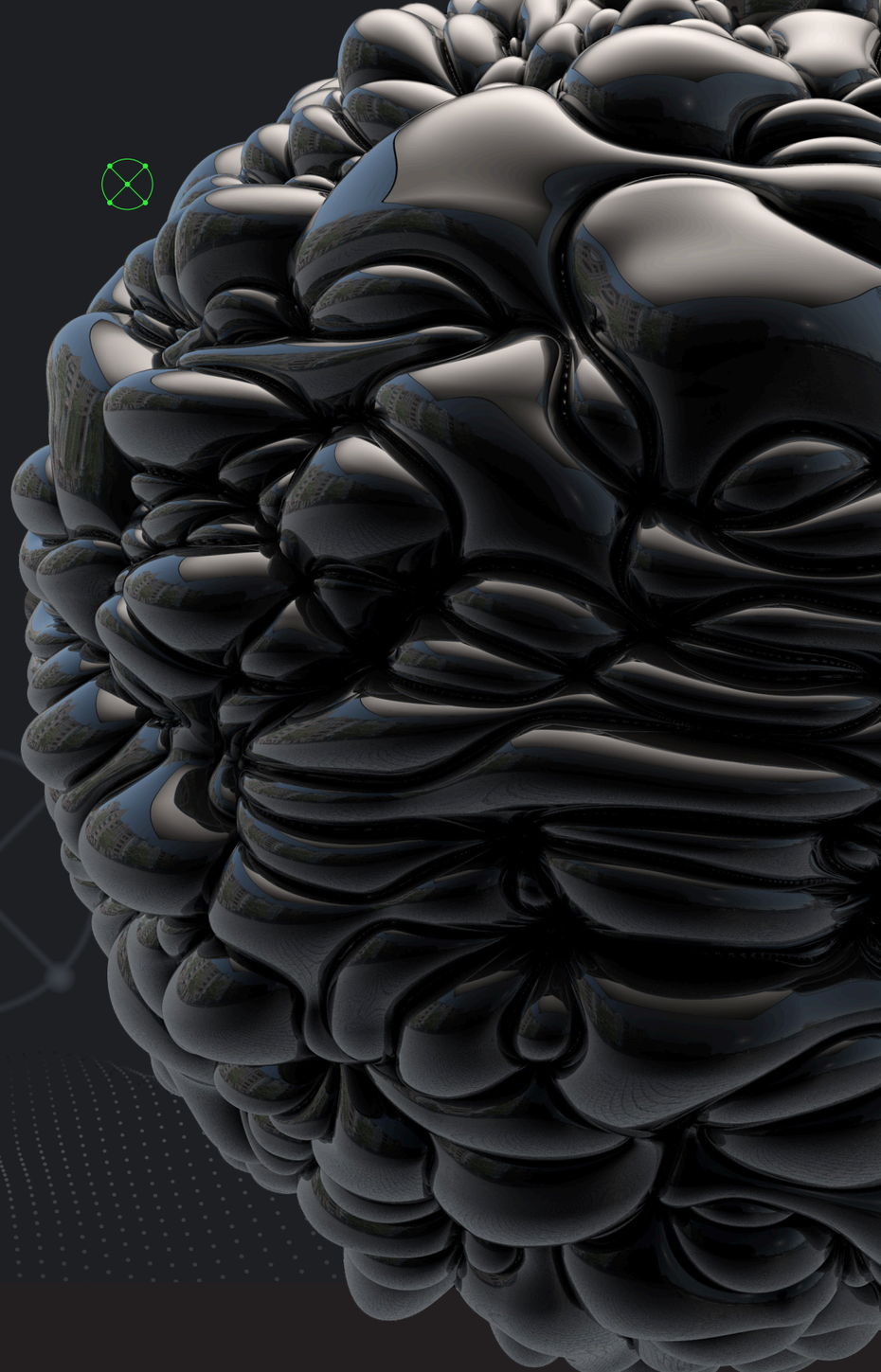
フィッシング

フィッシングは、ソーシャルエンジニアリングによって被害者をおびき出し、パスワードや銀行の詳細情報などの機密情報を暴露させる手法です。ユーザーに対するフィッシング方法として最も一般的なのは、悪意のある添付ファイルやリンクが含まれるメールを使ったものです。

フィッシングキャンペーンはきわめて広範かつ無差別に行われ、潜在的な被害者を最大限まで増やすために同じルアーで数百万の個人を標的にする場合があります。この方法は通常、特定の個人や組織に的を絞っていない、金銭的動機を持つ攻撃者によって使用されます。または、フィッシングを微調整して、被害者に関連する具体的な詳細情報を使用して、単一の犠牲者を標的にすることもできます。この手法はスピアフィッシングと呼ばれ、特定のシステムへのアクセスを求める攻撃者が使用する傾向があります。

人的エラーの可能性を考えると、フィッシングは現在も依然として脅威です。これらの攻撃は、被害者をだまして添付ファイルや悪意のあるリンクを開かせるよう構成されています。しかし、最近のフィッシング攻撃の急増を受けて、この分野のテクノロジーが向上しつつあります。Verizon の「2019 年度データ漏洩／侵害調査報告書」では、フィッシングは最上位の脅威アクションで、確認された侵害の 32%、サイバースパイインシデントの 78%[14] に関係していると述べられています。

サイバーセキュリティの多くの側面と同じように、最適な防御はトレーニングと意識向上です。しかし、フィッシングは人的要素に特化して標的とするため、フィッシングに対抗するには特にユーザーの教育が重要です。トレーニングでは、不明なソースから送られた添付ファイルやリンクを開くことについての意識向上に的を絞る必要があります。不審に見える添付ファイルをスキャンしたり、リンクの完全な URL を確認したりすることも、効果的なフィッシング対策手段です。



ランサムウェア

ランサムウェアは、マルウェアのカテゴリの 1 つで、マシンやネットワークストレージデバイス上のファイルを暗号化します。その上で脅威アクターは、ファイルの復号とアクセスの復元を望む犠牲者に支払いを強要します。多くの場合、攻撃者はランサムウェアを展開する前に環境から機密データを持ち出しており、被害者に支払いを強要する手段としてそのデータを使用する場合があります。盗まれたデータの機密度によっては、データの内容が、脅威アクターの要求する最終的な身代金額に影響する場合があります。

これらの攻撃の被害者は、ほとんどの場合、暗号通貨での支払いを要求されます。しかし、身代金を支払ってもデータが復号される保証はありません。ランサムウェアの影響を受けた組織では、システムのダウン中に収益の損失が発生するため、当初の復号コストを上回る財務的影響が発生することがあります。さらに、データが復号されなかった場合はデータが永久に失われ、そこからもコストが発生する可能性があります。

ランサムウェアにはいくつかの種類があります。多くの場合、他の形式の悪意のあるペイロードに比べて、そのようなランサムウェアを生成して使用する方が簡単です。場合によっては、ランサムウェアは、オペレーティングシステムに組み込まれた機能を使用することもあります。ランサムウェアには適応性もあり、場合によっては、支払い用アドレスを変更するだけでキャンペーンを変更できます。

ランサムウェアは、多くの場合、フィッシングのような広く使用されているソーシャルエンジニアリング手法によってエンドポイントに展開されます。組織のセキュリティを維持する責任はもはや単一のチームの役目ではなく、すべてのエンドユーザーがベストプラクティスを遵守するよう徹底する必要があります。ユーザーそれぞれがセキュリティの維持において重要な役割を果たします。とは言え、次に示すようなさまざまな方法で、ランサムウェアへの感染確率を効果的に下げることができます。

- AV 製品を最新の状態にし、すべてのデバイスで最新バージョンを実行する
- 可能であれば、ファイルや添付ファイルを開く前にスキャンする
- 定期的にデータをバックアップし、コピーをオフサイトに維持する

コインマイナー

暗号通貨の普及により、犯罪者は、侵害したマシンで追加の収入源を生成するまたとない機会を得ました。コンピューターのハードウェアを使用することで、悪意のあるソフトウェアによって暗号通貨を生成し、それを攻撃者のウォレットに自動的に預け入れることができます。

攻撃者の視点から見ると、コインマイニングには最小限の作業（および技術スキル）しか必要ありません。さらに、コインマイニングマルウェアは、感染したすべてのマシンからパッシブに収入を発生させることができます。これは、被害者 1,000 人中 1 人からしか収益を上げられない可能性があるランサムウェアとは異なります。[15]

システムパフォーマンスが低い場合、コインマイナーの感染の兆候である可能性があります。このマルウェアは、暗号通貨をマイニングするために、動作の際に CPU リソースと GPU リソースを大量に使用します。ユーザーがコインマイナーに対して自衛するには、不審なリンクをクリックしたり、悪意のあるメール添付ファイルを開いたりしないようにします。

攻撃者にとって標的が魅力的である理由

小売および卸売

小売および卸売業界が脅威アクターにとって魅力的である理由は、この業界が機密性の高い顧客情報を扱うためです。モバイル POS デバイスは、クレジットカードやデビットカード、電子商取引プラットフォームに定期的にアクセスします。多くの小売業者と卸売業者は、オンライン決済も受け付けており、これが脅威アクターにとってもう 1 つの情報収集手段になっています。

これらの攻撃の主要な目標は組織の中断ではありませんが、そのような結果を回避できない可能性があります。ほとんどの場合、守秘情報や個人情報が窃取されると、評判や財務の面で被害が発生し、顧客は将来、詐欺行為に遭うことになります。

テクノロジー／ソフトウェア

テクノロジーとソフトウェアコンポーネントに対する悪意のある攻撃は、通常、知的財産を盗んだり、マルウェア配布プラットフォームを確立したりすることが目的です。マルウェア配布プラットフォームは、サプライチェーン攻撃を実行するのに便利です。サプライチェーン攻撃では、情報の発信元にある正常なファイルに感染します。これにより、脅威アクターは、高度な配布キャンペーンを準備しなくても、下流への感染を開始できます。

サプライチェーン攻撃では、攻撃の存在を隠したままにすることが重要であるため、かなりの時間と、標的とするテクノロジーに関する中核的な理解が必要です。その他の場合、脅威アクターは、感染させた信頼済みソフトウェアのコピーではなく、独自のソフトウェアを配信できます。2017 年の CCleaner 攻撃 [16] で確認されたように、このような攻撃は実行が難しいものの、検知も困難です。

脅威アクターは、知的財産を盗んでソースコードを入手し、それらを使用してエクスプロイトを作成できます。目的の知的財産を一から調査するのにはコストがかかりますが、ソースコードを盗むことでそのコストを回避することもできます。多くの場合、攻撃者は組織内の特定のデータを探す際に、水平移動と他の情報収集戦術を実行します。

サービスプロバイダー

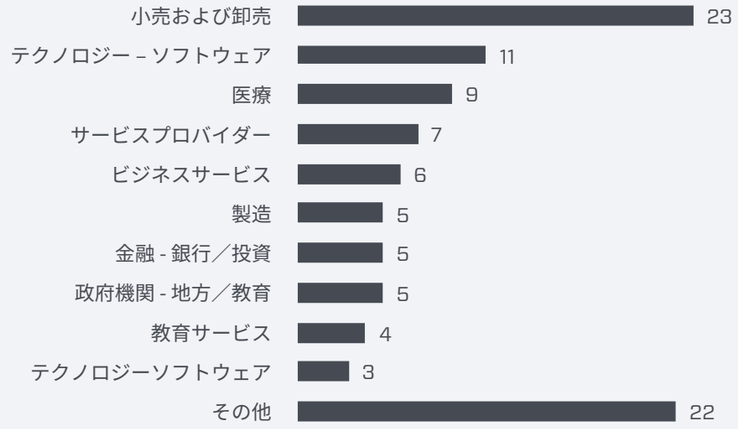
テクノロジーおよびソフトウェア企業と同じように、脅威アクターはサービスプロバイダーの顧客ベースを使用して配布量を増やします。脅威アクターは、サービスプロバイダーに侵入して、悪意のあるツールの配布に使用するワンストップショップを確立します。侵害された中央のサービスプロバイダーに顧客がアクセスするたびに、攻撃者は、悪意のあるインフラストラクチャの勢力範囲を拡大できます。

医療

過去数年で、複数の医療機関がサイバー攻撃による侵害を受けました。医療業界は、次のようなさまざまな理由から脅威アクターにとって魅力があるものとなっています。

- 機密の医療情報を所有している
- IoT デバイスが動作していて、機密性の高い場所で情報を収集している

攻撃全体で標的となった上位業種



脅威アクターは、知的財産を盗んでソースコードを入手し、それらを使用してエクスプロイトを作成できます。

- 多大な攻撃対象領域を提供するレガシーシステムが引き続き使用されている
- IT 部門に、適切なセキュリティカバー率を提供するためのリソースが不足している

医療機関の業務は重要であり、業務にはその性質上、時間的制約があります。そのため、医療機関は平均的なユーザーよりも身代金の支払いに応じやすい傾向があります。[17] さらに、医療保険企業は金融情報と併せて個人情報も保管しており、これらは闇市場で高額で販売できます。後でこの情報を使用して、ID を盗んだり、銀行詐欺を働いたりすることができます。医療業界に対して最もよく使用されるマルウェアのタイプは、インフォスティーラーとランサムウェアです。

金融／銀行

金融サービス業界は、機密データを所有していること、および金融口座にアクセスできることから、攻撃者に人気のある標的です。金融サービスが現金からデジタル空間への移行を進めるのに応じて、脅威アクターがこれらの機関に寄せる関心が高まっています。最近増加している ATM マルウェアのように、攻撃者は、能力の強化を示すことで業界の変化に対応しています。[18] このマルウェアは、クレジットカードとデビットカードの情報を大規模に窃取するために使用されています。

会社は、その規模のために魅力的な標的になる場合もあります。たとえば、2017 年に起きた Equifax のデータ侵害では、1 億 4,300 万件以上の顧客レコードが盗まれ、6 億ドル超の損失が発生しました。金融業界に限らず、財務部門が脅威アクターの標的になる傾向があります。攻撃者は、会社の多額の支払いを不正に許可するために、特定のスタッフのアカウントやシステムへのアクセスを得ようとします。こうして得た支払いは、分割して海外に送金した後、複数の口座を経由して転送し、銀行が取引を取り消すことができないようにすることによって、迅速にロンダリングされます。

政府機関

政府組織は、次のようなさまざまな理由から、脅威アクターにとって高価値の標的です。

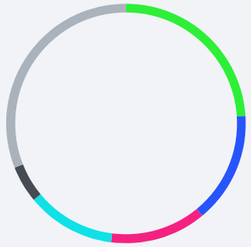
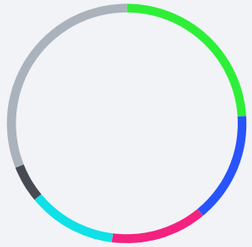
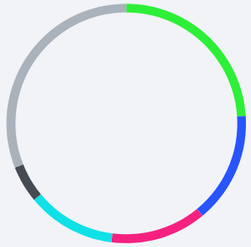
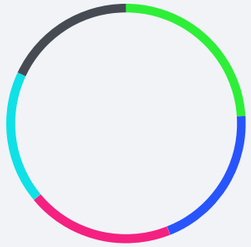
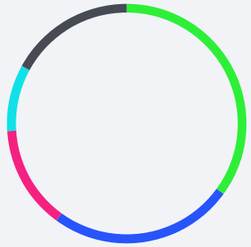
- 軍事情報へのアクセス
- さまざまな政治的動機
- 財務情報へのアクセス
- 大量の個人情報
- 機密の政府契約に関する情報

政府機関に対する攻撃はカスケード効果を及ぼす可能性があり、その場合、重要な国家インフラストラクチャだけでなく、個人にも影響が及びます。政府に的を絞ったサイバー攻撃の中でも、深刻な形態の攻撃の場合、生命が脅かされる可能性があります[19]。

2019 年には、警察と地方自治体が攻撃を受け[20]、多大な財務的影響が発生し、追跡調査に多額のコストがかかる事態になりました。さらに、情報が盗まれた場合、データ規制によっては、政府組織が訴訟にさらされる可能性もあります。

政府機関に対する攻撃はカスケード効果を及ぼす可能性があり、その場合、重要な国家インフラストラクチャだけでなく、個人にも影響が及びます。政府に的を絞ったサイバー攻撃の中でも、深刻な形態の攻撃の場合、生命が脅かされる可能性があります。

2019 年のトップ 3 の脅威による影響を受けた上位業種

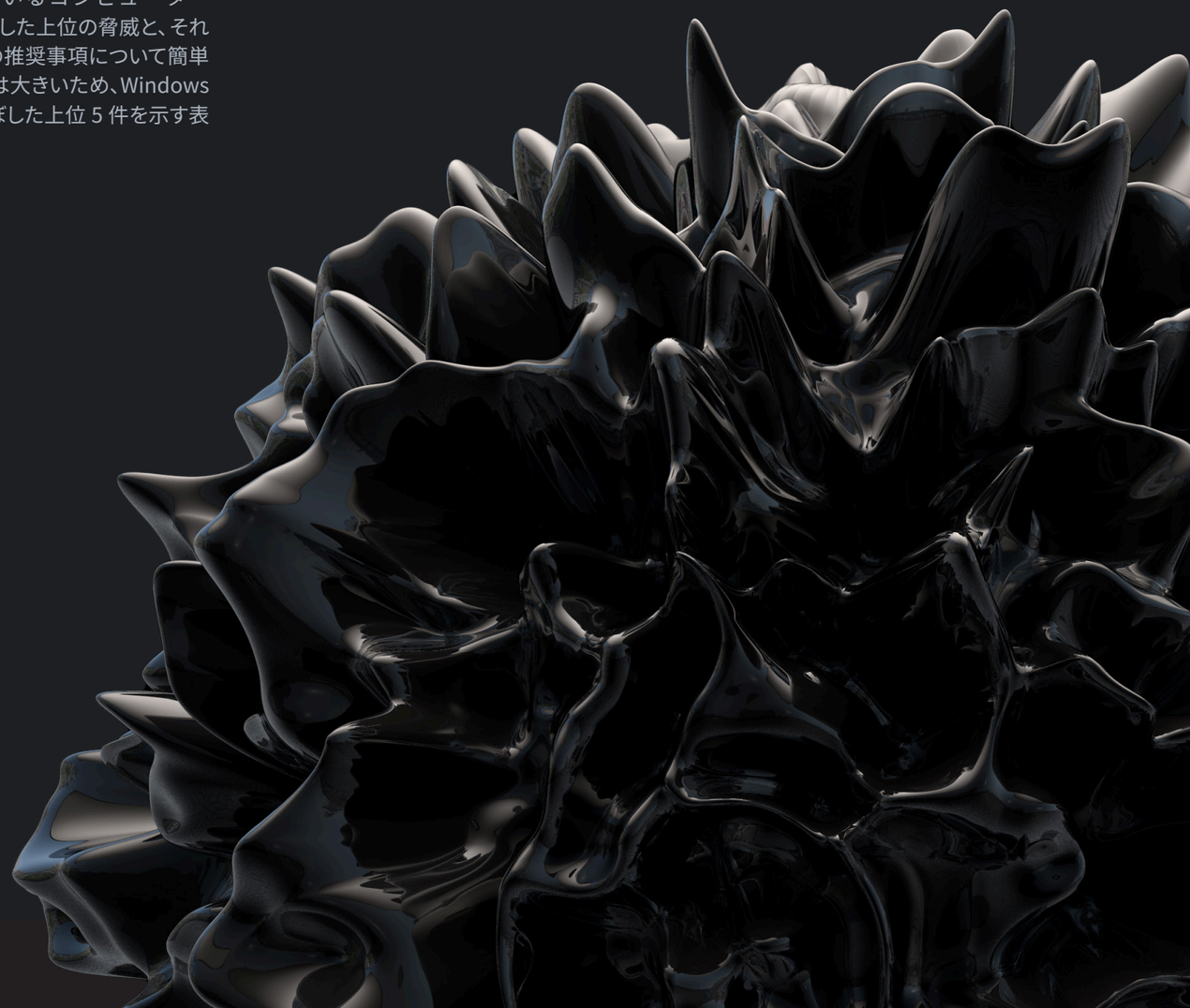
	Emotet	Ramnit	Upatre
2019	小売および卸売：24% 運輸：15% 教育サービス：13% 政府機関 — 地方／教育：12% 製造：5% その他すべて：31%		小売および卸売：27% テクノロジー - ソフトウェア：10% 製造：8% テクノロジー／ソフトウェア：7% 金融 — 銀行／投資：7% その他すべて：41%		小売および卸売：29% テクノロジー／ソフトウェア：21% 防衛および航空宇宙：10% 製造：9% 金融 — 銀行／投資：5% その他すべて：26%	
2018	政府機関：24% 医療：20% 非営利：20% ロジスティックス：18% その他すべて：18%		製造：35% プロフェッショナルサービス：25% メディア：14% 消費財：9% その他すべて：17%		テクノロジー：50% プロフェッショナルサービス：12% 製造：6% 金融：4% その他すべて：28%	

2019 年の上位のサイバー脅威：Windows、Mac、Linux

BlackBerry Cylance Research Operations は、社内のツールフレームワークを使用し、複数のオペレーティングシステムにわたって脅威環境を監視し、攻撃がないかどうかを確認しています。出回っている悪意のあるファイルを観測することで、未然に脅威データを利用して、現在と未来の両方の機械学習モデルを向上できます。

この情報は、弊社の顧客とビジネスコミュニティにとって有意義な脅威インテリジェンスにもなります。ここで説明する上位の脅威は、2019 年の脅威データから収集、特定され、社内で決められた業種に関連付けられています。

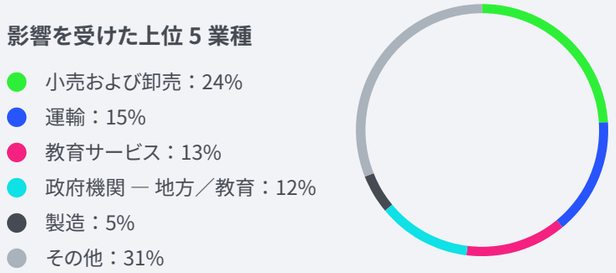
ここでは、2019 年に、広く使用されているコンピューターオペレーティングシステムに最も影響を及ぼした上位の脅威と、それらの脅威に関連するリスクを緩和するための推奨事項について簡単な概要を示します。Windows の顧客ベースは大きいため、Windows のセクションには、各業種に最も影響を及ぼした上位 5 件を示す表を含めています。



Windows の脅威

Emotet

影響を受けた上位 5 業種



Emotet として知られるマルウェアファミリーは、2014 年夏に、金融機関を標的とするスタンドアロンのトロイの木馬として初めて出現しました。当初は、ドイツとオーストリアの選ばれた金融機関の顧客を標的としていました。Emotet は、念入りにカスタマイズされたスパムメールを感染ベクトルとして使用し、ホストを侵害します。

初期の Emotet は、主に銀行の認証情報と共に他の機密情報を窃取することを目的に設計されていました。Emotet は、ソーシャルエンジニアリング手法と、ユーザーをだましてマルウェアを実行させる悪意のある zip 添付ファイルが含まれるスパムメールを組み合わせて伝搬されます。

感染すると、Emotet は、高度な手法を使用して悪意のあるペイロードを正当なプロセスに注入します。また、ポリモーフィズムを使用して、従来のシグネチャベースのサイバーセキュリティを回避します。これらの難読化手法により、Emotet は、検出される可能性を最小限に抑えながら動作できます。

Emotet は、自動開始のレジストリキーとサービスエントリを変更することで、再起動してもパーシスタンスを実現します。Emotet は、進化の過程でモジュール形式のマルウェアになりました。つまり、別のモジュールとプラグインをダウンロードして機能を拡張することができます。モジュールは、Outlook のスクレイピング、スパムメールの送信、パスワードのスクレイピング、ボットネットへの接続機能など、追加の機能を提供します。

発見から 3 年後、Emotet は、侵害されたシステムに他のマルウェアの脅威をダウンロードするための配信メカニズムとして機能し始めます。Emotet は、金融機関を標的とするトロイの木馬である Dridex や Panda Banker などのサードパーティのマルウェア、AzoRult や Gootkit などの情報窃取マルウェアを配信しました。Emotet の感染ベクトルも絶えず変化していました。当初は、悪意のある zip ファイルと埋め込みリンクが含まれるスパムメールを利用していましたが、後には、高度に難読化された悪意のあるマクロを含む武器化された Microsoft® Word ドキュメント、PDF、.xml ファイル、およびパスワードで保護された Word ドキュメントが添付されたスパムメールを使用するようになりました。

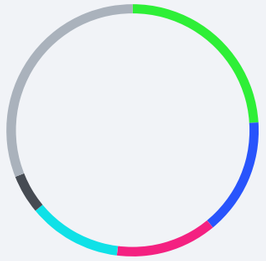
Emotet の背後にいる脅威アクターは、継続的にコードを更新して、最新の AV による検知と防御対策を回避しています。Emotet は、2019 年夏に短期間休止した後、9 月にソーシャルエンジニアリング手法を使用した新たなスパムキャンペーンで再び出現しました。いったんシステムが感染すると、このマルウェアは、ユーザーのメールの受信トレイを列挙し、自身を既存の正当なメールスレッドに挿入します。続いて、現在のニュースイベントを参照する新しいメールを作成し、悪意のあるドキュメントをスレッドに添付し、自身をメールで被害者に送信します。この方法により、何も知らないユーザーがだまされて悪意のあるメールと感染した添付ファイルを開いてしまう確率が大幅に上がります。

Emotet のリスクを軽減するには

- すべてのデバイスとソフトウェアを最新に保つ
- 最新のセキュリティソリューションを利用する
- ホストのログで、不審なサービスが作成されていないかどうか（Windows イベント ID 7045）を監視する
- ホストのログで、スケジュールされた不審なタスクが作成されていないかどうか（Windows イベント ID 106）を監視する
- 強力なメールセキュリティおよびスパム対策フィルターを展開して、悪意のある添付ファイルや不審なリンクをブロックする
- スパムブラックリストを利用する
- Microsoft Office が、デフォルトですべてのマクロを自動的に無効化し、信頼できることが確認されているマクロのみを実行するよう設定されていることを確認する
- 既知の Emotet ／ Heodo ボットネットの IP と URL へのネットワーク接続をすべてブロックする

Kovter

影響を受けた上位 5 業種



- テクノロジー／ソフトウェア：23%
- 金融 ― 銀行／投資：21%
- ビジネスサービス：15%
- 製造：9%
- 医療：6%
- その他：26%

Kovter は、ファイルレスの高度なトロイの木馬ファミリーです。感染したシステム上でパーシスタンスを維持するため、Kovter は、難読化されたスクリプトコードをレジストリに保存し、これが起動時に毎回実行されます。技術的には、このペイロードは、ディスク上のファイルとしてではなく、レジストリ内に存在します。その結果、セキュリティアナリストが感染源を探すことが難しくなります。

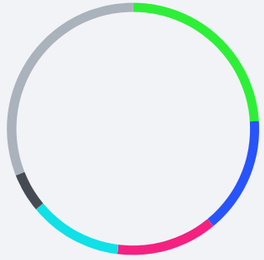
Kovter は主に、不正広告とエクスプロイトキットを介して拡散されます。このマルウェアの主な目的は、クリック詐欺を実行することです。Kovter のボットネットは 2018 年末に停止しましたが、2019 年にも Kovter の亜種が引き続き確認されています。

Kovter のリスクを軽減するには

- メールの脅威を防御するためのポリシーを導入する
- Microsoft Office 製品のマクロの読み込みを無効にする
- ブラウザーとプラグインを最新にし、不審な動作がないかどうかを監視する
- JavaScript® を無効にすることを検討する
- 必要ない場合、コマンドラインシェルスクリプト言語を無効にする
- PowerShell が更新されていて、セキュリティ重視の設定になっていることを確認する
- レジストリの異常な変更がないかどうかシステムを監視する
- ログと、インバウンド／アウトバウンドネットワークトラフィックを監視する

Poison Ivy

影響を受けた上位 5 業種



- 小売および卸売：44%
- 防衛および航空宇宙：12%
- テクノロジー／ソフトウェア：7%
- 製造：7%
- 金融 ― 銀行／投資：6%
- その他：24%

Poison Ivy は人気のある Windows RAT ツールキットで、2005 年に初めて特定されました。これはオンラインで無料で利用できます。何年にもわたり、このコモディティマルウェアは、さまざまなグループと脅威アクターによって使用され、いくつもの有名なキャンペーンで展開されてきました。

このツールキットは、純粋なアセンブリ（Poison Ivy サーバーまたはバックドア）と Delphi（Poison Ivy クライアント）で記述されています。Poison Ivy はグラフィカルユーザーインタフェースを備えており、そこでビルダーによって、カスタマイズ可能な Poison Ivy サーバーをシステムに依存しない PE ファイルまたはシェルコードとして生成します。

その機能には、圧縮された暗号化通信、キーロギング、ウェブカメラ／画面／音声／動画のキャプチャ、ファイル転送、システム管理、パスワードの窃取、トラフィックの中継などがあります。また、サードパーティのプラグインにも対応しています。

Poison Ivy は、ActiveX の起動か、システムの起動時に実行されるレジストリキーエントリによってパーシスタンスを実現します。Poison Ivy サーバーは、システムフォルダーか Windows フォルダーにコピーすることも、検知を回避するために別のデータストリームにコピーすることもできます。Poison Ivy には、プロセスミューテックスを設定し、プロセスインジェクションを実行するためのオプションが含まれます。デフォルトのブラウザープロセスへのインジェクションを実行してファイアウォールを迂回したり、指定された別の実行プロセスにインジェクションを実行したりできます。

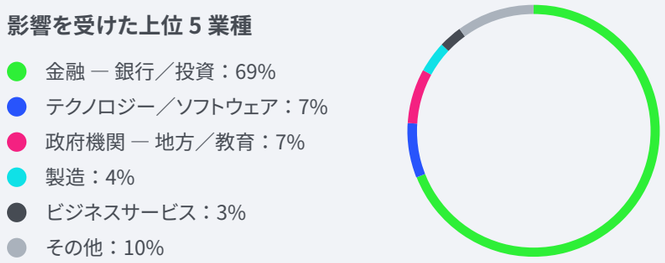
Poison Ivy は、多くの場合、スピアフィッシングキャンペーンによって拡散され、武器化された Microsoft Word ドキュメント、PDF、および Microsoft® ヘルプファイルによって Poison Ivy サーバーがドロップされます。Poison Ivy サーバーがターゲットマシン上で実行されると、攻撃者のマシン上の Poison Ivy クライアントに接続します。攻撃者は、この接続を使用してターゲットシステムを制御できます。

Poison Ivy のリスクを軽減するには

- フィッシング
  - フィッシング試行について従業員を教育する
  - メールおよびフィッシングの脅威を防御するためのポリシーを導入する
  - システムとアプリケーションを最新に保つ
- Poison Ivy のバックドア
  - 組織内に強力なパスワードポリシーを導入する
  - ログとネットワークアクティビティを監視する
  - 適切なアカウント特権をユーザーに割り当てる
  - システムの起動時に実行されるアプリケーションやサービスを監視する

Qakbot

影響を受けた上位 5 業種



Qakbot は、2009 年に初めて出現した多面的脅威のファミリーです。出回っていることが確認されている亜種のほとんどは、非常に堅牢で適応性に優れています。その多くには、トロイの木馬ファミリーのさまざまなコンポーネントに加え、進化、変異、および自己伝搬の機能が含まれています。初期の亜種は主に、データを盗んで、ターゲット環境内に永続的な足掛かりを確立するために使用されていました。

2009 ～ 2012 年の Qakbot キャンペーンは、オンラインバンキングの認証情報の窃取を目的としていたため、予想どおりサイバー犯罪者の間でこのマルウェアの人気が高まりました。2017 年に、Qakbot の新しい亜種で注目に値する差異がいくつか見つかりました。2017 年の変化としては、Qakbot がターゲットの 64 ビットシステムに適応したこと、およびマルウェアが完全に作り直されたことがあります。更新された Qakbot は、そのコード機能の 20% 以上を検知回避とパーシスタンスに関する処理に割いています。Qakbot は、当初はフィッシングメールで拡散されていましたが、現在では、自己複製用のモジュールと、ネットワーク共有を水平移動する機能を含んでいます。

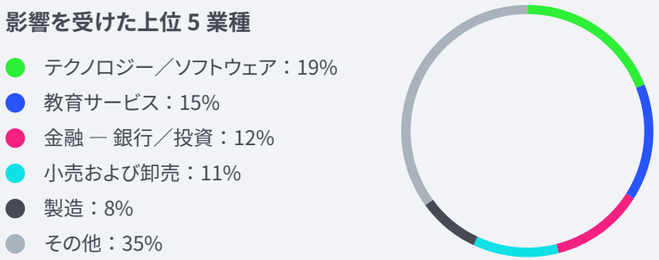
Qakbot は、アカウントと管理者をロックアウトしてビジネスに影響を及ぼすことができます。これにより、マルウェアの封じ込めと削除がきわめて困難になります。Qakbot は回復力に優れた脅威で、2009 年以降、法執行機関と AV ベンダーの両方による取り組みにもかかわらず、繰り返し出現しています。

Qakbot のリスクを軽減するには

- Qakbot の感染の拡散を封じ込める
- C&C サーバーとの通信を遮断する
- 権限とアクセス権をエンドユーザー間で適切に分散する
- 新しく作成されたサービスと、新しく作成されたスケジュールタスクを監視する（イベント ID 7045 を追跡することで監視可能）
- エンドポイントに最新の効果的なアンチウイルステクノロジーを展開する
- 以前の攻撃に関連する IP ／ドメインを記録し、再感染していないかどうかを監視する
- 元々の攻撃ベクトルを特定し、これを使用して将来の攻撃を回避する

Ramnit

影響を受けた上位 5 業種



Ramnit は、Windows PE の実行可能ファイルに感染する寄生ウイルスです。これは、リムーバブルメディアに拡散し、マルウェアのコピーへのショートカットを作成できるワーム機能も備えています。Ramnit は、VBS コードを注入することによって、HTML ファイルに感染することができます。後でユーザーがこれらの HTML ファイルにアクセスすると、ウイルスに感染します。

Ramnit は、リモートアクセス型トロイの木馬および金融機関を標的とするトロイの木馬として機能するよう設計されています。時間と共に、Ramnit のオリジナルバージョンが変更され、新機能が含まれるようになりました。アップグレードにより、バックドア、C&C サーバー、および通信を作成して、感染したマシンをボットネットキャンペーンで連携させる機能が組み込まれました。2015 年 2 月、欧州当局は、320 万台のコンピューターを感染させた Ramnit ボットネットを閉鎖しました。しかし Ramnit は 2015 年 12 月に再び出現します。

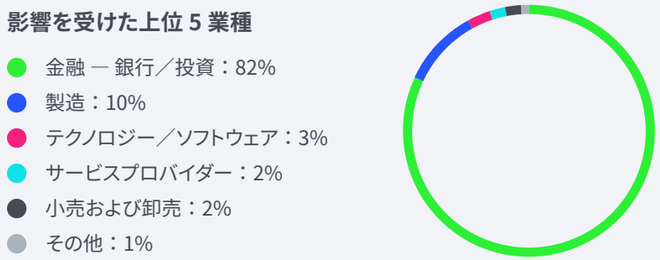
2016 年には、Ramnit の新しい亜種は、英国の大手銀行をターゲットとするようになりました。Ramnit の一部のキャンペーンと攻撃は、真のファイルレス方式であり、Power Shell や JavaScript のコードを直接実行せずに動作します。Ramnit は、レジストリに、XOR で暗号化したペイロードデータを保存することが確認されています。これにより、Ramnit のローダースレッドは、レジストリからバイナリラージオブジェクト（BLOB）を解析して復号し、プロセスインジェクションを実行します。

Ramnit のリスクを軽減するには

- 不審なアドレス／ IP へのアウトバウンド接続要求を監視する
- フィッシングおよびスピアフィッシングの一般的な手法について従業員を教育する
- アカウント特権が適切な従業員に合わせて調整されていることを確認する
- エンドポイントの検知および緩和ソフトウェアを最新に保つ
- エンドユーザーに送信された未検証のメール添付ファイルの実行を停止する

Sakurel

影響を受けた上位 5 業種



Sakurel は、Sakula または VIPER としても知られ、サーバーに接続してリモートシェルを開く RAT です。Sakurel のサンプルのコンパイルタイムスタンプから、このマルウェアが最初に出現したのは 2012 年 11 月であることがわかります。このマルウェアは通常、標的型攻撃で使用されます。Sakurel は、Microsoft® Internet Explorer のメモリ解放後使用によるリモートコード実行の脆弱性（CVE-2014-0322）のエクスプロイト [21] を配信する、悪意のある URL からダウンロードされます。これは、発見時点では Internet Explorer のゼロデイ脆弱性でした。

トロイの木馬は、実行されると、自身を %Temp%\MicroMedia\MediaCenter.exe にコピーします。%Temp%\MicroMedia\MicroSoftSecurityLogin.ocx ファイルをドロップし、ActiveX コンポーネントとして登録します。

その後、レジストリエントリ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\” MicroMedia” = “%Temp%\MicroMedia\MediaCenter.exe” を作成し、Windows の起動時に毎回実行されるようにします。

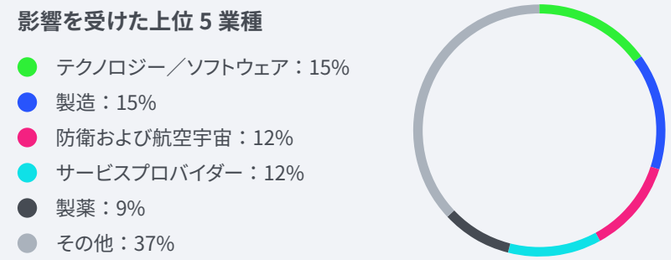
続いて、Sakurel は Hosts ファイルを変更し、ブラウザーを侵害された URL または IP アドレスへリダイレクトします。そして、oa[.]ametekesen[.]com にあるリモートサーバーに接続し、リモートシェルを開きます。さらに、被害者のブラウザーのアクティビティを監視し、追加のファイルをダウンロードします。

Sakurel のリスクを軽減するには

- すべてのソフトウェアとハードウェアが最新であることを確認する
- 不明なリンクをクリックすることの危険について従業員を教育し、デバイスやネットワークが意図せず侵害されるのを防ぐ
- 重要なデータの定期的なバックアップを含む戦略を導入し、そのデータを複数の場所に保管して冗長性を確保する
- ユーザーが適切なアカウント特権に制限されていることを確認する
- 使用されていないポートや不要なポートはマルウェアによって攻撃ベクトルとして使用されるおそれがあるため、無効にする
- セキュアリモートアクセスの制御を設定する（たとえば、VPN または強化されたセキュリティゲートウェイ経由でのリモートアクセスのみを許可する）
- すべてのネットワークアクティビティを監視してログに記録する

Upatre

影響を受けた上位 5 業種



Upatre は 2013 年 8 月に最初に確認され、2015 年にピークに達しました。その後人気は低下しましたが、特にテクノロジー組織や他のプロフェッショナルサービスプロバイダーにとっては、今も現実味のある脅威です。

Upatre は通常、感染した添付ファイルが含まれるスパムメールを通じて拡散します。これらのメールは、多くの場合、請求書やボイスメールメッセージの通知を装っています。また、パスワードで保護されたアーカイブ添付ファイルとして発生することも、感染した Web サイトのリンクを通じてドライブバイでインストールされることもあります。

Upatre は、実行されると、金融機関を標的とするトロイの木馬である Zeus ／ Zbot や、Rovnix ルートキットの亜種、Crilock ランサムウェアなど、他のマルウェアを感染したシステムにダウンロードできます。

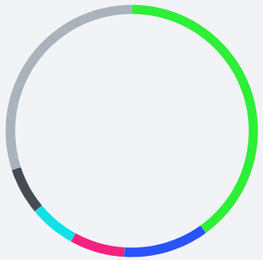
Upatre のリスクを軽減するには

- システムとアプリケーションが最新であることを確認する
- フィッシング攻撃のシナリオについて従業員を教育する（人的エラーが主な感染ベクトルであるため）
- 不明な送信者からのメールで受信した添付ファイルをクリックまたはダウンロードしない
- 見慣れた添付ファイルアイコン（たとえば、PDF アイコン）にだまされない
- 最新の AV ソリューションを導入する
- Microsoft Office のマクロを無効にする

Ursnif

影響を受けた上位 5 業種

- サービスプロバイダー：40%
- エネルギーおよび鉱工業：11%
- アパレルおよびファッション：7%
- 製造：6%
- テクノロジー／ソフトウェア：6%
- その他：30%



金融機関を標的とするトロイの木馬である Ursnif は、出現から 10 年以上経っており、特に興味深い歴史があります。ソースコードが漏洩して多数の変種が作成されたため、この脅威は、Gozi、ISFB、Rovnix、および Dreambot としても知られています。Ursnif は、Web インジェクションまたは Man-in-the-Browser（MiTB）として知られる手法を使用して、銀行情報や被害者の資金を盗み出します。

Ursnif は、有名なブラウザー DLL 内のコア関数をフックすることにより、ユーザーに表示される前に Web ページのコンテンツを変更することができます。この手法により、Web サイトでトランスポート層セキュリティ（TLS）が使用されていても認証情報を盗むことができます。その後、攻撃者は、盗んだ認証情報を使用して、被害者に気付かれることなく、被害者の銀行から金銭を引き出すことができます。この攻撃は正当な取引を偽装しているため、銀行が検知するのはきわめて困難です。

Ursnif の大半は依然として金融機関を標的とするトロイの木馬ですが、最新バージョンには次のような幅広い機能があります。

- 他のソフトウェアやマルウェアファミリーをダウンロードして起動する
- SOCKS プロキシサーバーを実行する
- スクリーンショットをキャプチャする
- キーロギングを実行する
- Microsoft Internet Explorer、Microsoft ®Outlook®、および Mozilla® Thunderbird® の各ブラウザーから認証情報を盗む
- 暗号通貨ウォレットを盗む

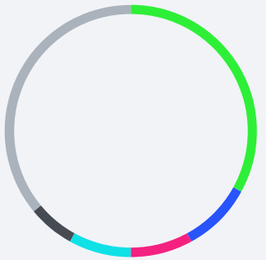
Ursnif のリスクを軽減するには

- 保護されていないネットワーク（公衆 Wi-Fi など）への接続を確立するのを避ける
- 機密情報（クレジットカード情報など）をブラウザーの履歴に保持しない
- ブラウザーを最新バージョンに更新し、パッチ情報を一貫して監視する
- 元々の攻撃ベクトルを特定し、これを使用して将来の攻撃を回避する
- ブラウザーのプラグインを最新にし、不審な動作がないかどうかを監視する
- 以前の攻撃に関連する IP ／ドメインを記録し、再感染していないかどうかを監視する
- ファイアウォールを利用して、検証されていない場所や信頼できない場所へのインバウンド接続とアウトバウンド接続をすべてフィルターしてブロックする
- Windows® Defender でクラウドによる保護とサンプルの自動送信を有効にする

Vercuse

影響を受けた上位 5 業種

- 小売および卸売：33%
- 防衛および航空宇宙：9%
- テクノロジー／ソフトウェア：8%
- 製造：8%
- テクノロジー - ソフトウェア：6%
- その他：36%



Vercuse は、通常はドライブバイダウンロードまたは侵害されたリムーバブル USB ドライブを介して配布される脅威です。複数の隠しフォルダーに Vercuse のコピーがドロップされます。パーシスタンスを確立するため、このマルウェアは、起動時に実行されるレジストリキーも追加します。具体的には、サブキー「HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce」をデータ「’SecurityUpdate<5 つのランダムな数 >’」に変更し、値「%APPDATA%\Microsoft\Windows\~temp~<5 つのランダムな数 >iN.exe」を設定します。

Vercuse がドロップするペイロードはさまざまですが、多くは Backdoor:Win32/Poison として出現します。Vercuse は、Microsoft のマルウェア削除ツールなどの正当なソフトウェアを装います。このマルウェアは、サンドボックス対策手法とツール固有の検知（ウィンドウ名に表示されるテキストに基づく）を含む、複数の AV 回避手法を使用します。特定のツールが使用されている場合、Vercuse はその実行中のプロセスを終了します。Vercuse がもたらす最大の脅威は、追加のマルウェアサンプルをドロップする機能です。

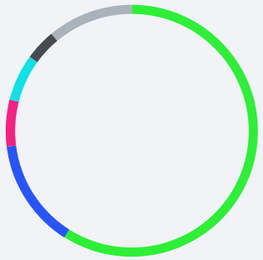
Vercuse のリスクを軽減するには

- エンドポイントのすべてのアプリケーションとシステムが最新のソフトウェアによって最新になっていることを確認する
- 主な攻撃ベクトルの性質を考え、ビジネスで必要ではないサイトは避ける
- ネイティブではないアンチウイルスアプリケーションがエンドポイントに存在しないかどうか監視する
- スケジュールされていないセキュリティ更新が実行されるかどうかに注意する

Zegost

影響を受けた上位 5 業種

- サービスプロバイダー：59%
- 政府機関― 州／地方：14%
- テクノロジー／ソフトウェア：6%
- 製造：6%
- ビジネスサービス：4%
- その他：11%

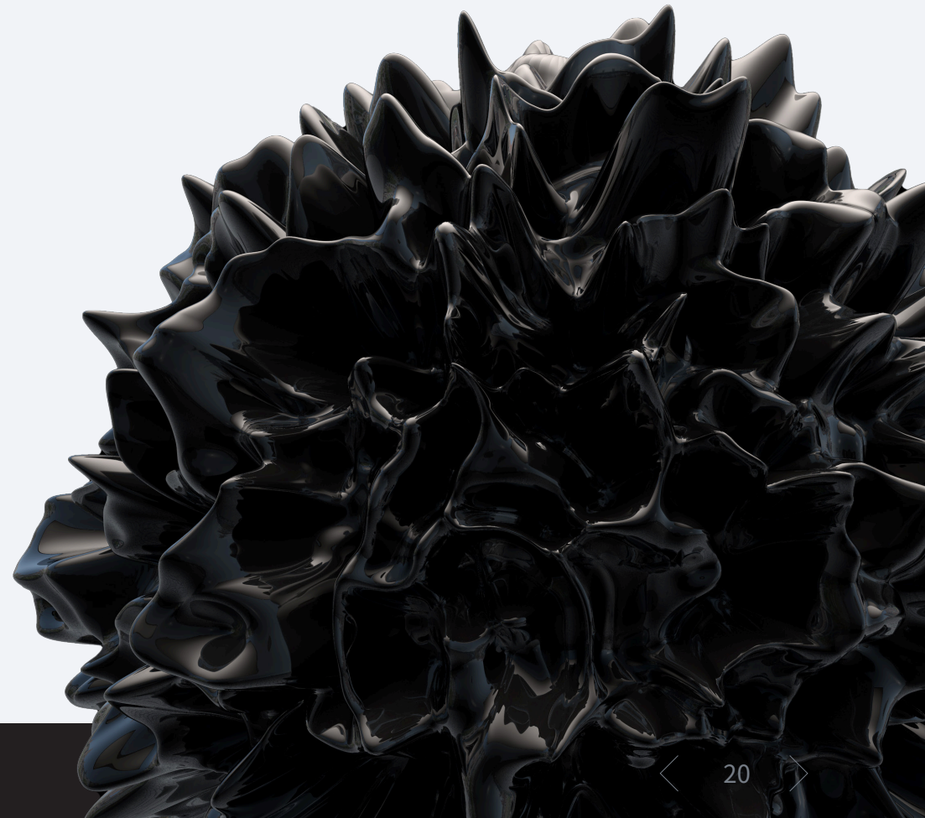


Zegost はインフォスティーラーで、通常は、悪意のある添付ファイルが含まれるフィッシングメールや、感染した Web サイトに疑いを持たずにアクセスするユーザーによって拡散されます。このマルウェアの主な目的は、ユーザー情報を盗んで持ち出し、C&C アーキテクチャにレポートすることです。Zegost は 2012 年に初めて発見され、CVE-2012-0507[22] で説明されている Java® エクスプロイトを使用してネパール政府のサイトを標的としたことで注目を集めました。このマルウェアにはさまざまなアクティブな亜種があり、現在も引き続き使用されています。

Zegost は、システムに感染すると、ユーザー情報を盗んで、キーストロークロギングを実行し、マウスイベントを監視します。また、侵害されたデバイスを使用して分散型サービス拒否（DDOS）攻撃に参加することも観察されています。マルウェアが収集した情報はすべて C&C サーバーに送信されます。Zegost は、その C&C サーバーを使用して自身の更新や削除を行うこともできます。このマルウェアは、パーシスタンスを確立するため、起動時に実行されるレジストリキーを追加します。さらに、C&C サーバーの要求に応じて他のマルウェアをインストールすることもできます。

Zegost のリスクを軽減するには

- フィッシングの脅威と危険について従業員を教育する
- メールおよびフィッシングの攻撃ベクトルを防御するためのポリシーを導入する
- システムとアプリケーションを最新に保つ
- Java の最新バージョンをインストールする
- 不正な接続がないかどうかネットワークアクティビティを監視する
- このマルウェアファミリーに関連するレジストリキー「Kris」や実行可能ファイル「BJ.exe」が存在するかどうか確認する



Mac の脅威

CallMe

CallMe は、特に macOS® オペレーティングシステムとそのユーザーを標的としたマルウェアバックドアです。2013 年に初めて出現が確認され、アジア太平洋地域の標的に的を絞る傾向があります。このマルウェアは、巧妙に作られた悪意のある Microsoft Word ドキュメントを使用してユーザーのデバイスにドロップされ、2009 年からパッチが提供されている脆弱性、CVE-2009-0563[23] をドキュメントで悪用しています。

システムにドロップされると、C&C サーバーとの接続を試み、自身をデバイス上にコピーし、起動ポイントを作成します。再起動後もバックドアがルート許可アクセスを維持できるよう、複数のファイルを「LaunchDaemons」にコピーします。

さらに、ユーザーの連絡先データが含まれる一時ファイル「/tmp/tmpAddressbook.vcf」と、実行されるバックドア「tmp/ system」も作成します。このバックドアは、macOS と Microsoft Word の最近のエディションで使用するようには開発されていません。ユーザーが macOS Mountain Lion 以降を実行している場合、このバックドアがユーザーの連絡先にアクセスしようとすると通知が表示されます。さらに、このマルウェアが使用している Word の脆弱性は Microsoft によってパッチが提供されていることも通知されます。

CallMe のリスクを軽減するには

- Microsoft 製品（Microsoft Word など）が最新であることを確認する
- macOS が更新されていることを確認する
- デバイスで不明なプログラムの実行を許可することの危険についてエンドユーザーを教育する
- 不審なアクティビティがないかどうかネットワークを監視する

KeRanger は、macOS オペレーティングシステムを標的とした最初のランサムウェア脅威の 1 つです。

KeRanger

KeRanger は、macOS オペレーティングシステムを標的とした最初のランサムウェア脅威の 1 つです。このマルウェアは、BitTorrent クライアントアプリケーションである Transmission のインストーラーを侵害する脅威アクターによって配布されました。KeRanger は、2016 年には有効な Mac Developer ID で署名されていました。つまり、macOS の組み込み機能である Gatekeeper を迂回することができたのです。この不正な署名は、発見後直ちに取り消されました。

KeRanger は、実行されると、/Volumes ディレクトリとそのサブディレクトリ内にあるさまざまなファイルタイプを暗号化します。また、ユーザーのファイルを暗号化する際に、ファイル拡張子「.encrypted」をファイルに付加します。その後、TOR ブラウザーをダウンロードするようユーザーに指示し、支払い方法を示した「README_FOR_DECRYPT.txt」ファイルをドロップします。

KeRanger のリスクを軽減するには

- macOS が更新されていることを確認する
- 不明なサイトからアプリケーションをダウンロードしないようユーザーを教育する
- できる限り頻繁にシステム情報をバックアップする
- ランサムウェアインシデントに対処するためのビジネス戦略を導入する

LaoShu

LaoShu は 2014 年初頭に初めて発見され、スパムメールを主な感染ベクトルとして使用する RAT です。この署名済みマルウェアは、PDF ファイルを装うことで、何も知らないユーザーをだましてマルウェアを実行させようとします。このファイルは、実際には .app Mach-O アプリケーションファイルです。実行されるとバックドアを開き、これによって攻撃者が機密情報を制御、窃取、または持ち出しできるようにします。

LaoShu の亜種の中には、.doc ／ docx、.xls ／ xlsx、.ppt ／ pptx などのよく使用されるドキュメントファイルをホストでスキャンできるものもあります。これらのドキュメントファイルが見つかると、.zip 形式に圧縮され、その後、攻撃者が制御する C&C サーバーに持ち出されます。LaoShu の亜種は、追加のファイル／マルウェアを被害マシンにダウンロードしたり、スクリーンショットを作成したり、シェルコマンドを実行したりできます。

LaoShu のリスクを軽減するには

- すべてのデバイスとソフトウェアを最新に保つ
- 最新のセキュリティソリューションを利用する
- 強力で複雑なパスワードポリシーを導入および適用する
- ファイアウォールを利用して、検証されていない場所や不明な場所へのインバウンド接続とアウトバウンド接続をすべてフィルターしてブロックする
- 強力なメールセキュリティおよびスパム対策フィルターソリューションを展開して、悪意のある添付ファイル、不審なリンク、およびファイルをダウンロードするためのリンクをブロックする
- スパムブラックリストを使用する
- 不審なメールの処理の重要性に重点を置いた内部の従業員教育プログラムを導入する
- アクセス制御リスト（ACL）とパスワード保護を利用して、共有ファイルへのユーザーアクセスを制限する
- 必要がない場合は、ファイル共有を無効にする

NetWiredRC

NetWiredRC はマルチプラットフォームの RAT で、Windows、macOS、および Linux® のシステムで使用できます。その形態は、ユーザーの知らないうちにインストールされる悪意のあるソフトウェアです。NetWiredRC は、機密情報を収集する、キーロギングを実行する、画面をキャプチャする、攻撃者が侵害されたマシンへのリモートアクセスを得るといった目的で使用されます。

NetWiredRC は、OSX.Wirenet ／ OSX.Netwire としても知られ、2012 年に初めて発見されました。これは、Linux システムと macOS システムからパスワードを盗む最初の情報窃取マルウェアファミリーの 1 つです。パーシスタンスを確立するため、NetWiredRC は、起動エージェントおよびログイン項目として機能します。このマルウェアは、特に APT33 グループで人気があります。

NetWiredRC のリスクを軽減するには

- ルーター／ファイアウォールで 212[.]7[.]208[.]65（NetWire の C&C）をブロックする
- ホームディレクトリに「%home%/WIFIADAPT.app」が存在しないかどうかを監視し、見つかった場合は削除する

XcodeGhost

2015 年に初めて特定された XcodeGhost は、iOS® と macOS の両方に影響するマルウェアです。また、macOS 初のコンパイラマルウェアでもあります。XcodeGhost の悪意のあるコードは、Xcode のインストーラーの複数のバージョンに再パッケージされていました。Xcode は、iOS および macOS 用アプリを開発するための Apple の公式ツールです。

これらの悪意のあるインストーラーは、中国の iOS および macOS 開発者が使用する Baidu のクラウドファイル共有サービスにアップロードされていました。これは複数の iOS アプリに感染することに成功し、そのうち少なくとも 2 つは App Store に提出されて許可されていました。XcodeGhost の主な目的は、感染デバイスから情報を収集して、C&C サーバーにアップロードすることです。

XcodeGhost は、多くの場合、Apple の App Store® に対する最初の大規模攻撃と見なされます。XcodeGhost に感染すると、攻撃者は、リモートアクセス機能、デバイス情報を盗むためのオプション、クリップボードの読み書き機能、およびブラウザーの乗っ取り機能を利用できるようになります。

XcodeGhost のリスクを軽減するには

- すべてのソフトウェアとハードウェアが最新であることを確認する
- 重要なデータの定期的なバックアップを含む戦略を導入し、そのデータを複数の場所に保管して冗長性を確保する
- iOS App Store からダウンロードするアプリが 100% 信頼できることを確認する
- セキュアリモートアクセスの制御を設定する（たとえば、VPN または強化されたセキュリティゲートウェイ経由でのリモートアクセスのみを許可する）

Linux の脅威

Gafgyt

Gafgyt は、競合するボットネットである JenX の亜種です。Gafgyt は 2014 年に初めて発見され、ごく最近の 2019 年 9 月まで更新されていました。このマルウェアは、リモートコード実行エクスプロイトを使用してアクセスを取得し、ルーターを IoT ボットネットに参加させます。Gafgyt は特にゲーミングサーバーを標的として DDOS 攻撃を実行します。また、小規模な組織や、Zyxel、Huawei、および Realtek の各モデルを含む家庭用無線ルーターも標的とします。

通常は、特定の脆弱性に関連する機能がハードコードされており、複数の亜種が異なるエクスプロイトを標的としています。システムに感染すると、ハードコードされた URL から追加のバイナリを取得します。さらに、侵害されたデバイスの情報を C&C サーバーに送信し、その情報をボットネットに追加します。

Gafgyt ボットネットは、HTTP フラッディングを使用して攻撃を実行します。ここには、Cloudflare サービスと Valve Source Engine サービスを攻撃するための特殊なコマンドが含まれています。このマルウェアには、感染したデバイス上に現在存在する他のボットネットを強制終了する機能もあります。

異常なネットワークアクティビティがある場合、Gafgyt の感染を示している可能性があります。Gafgyt は、幅広いメーカーのネットワーキングデバイスのパッチ未適用の脆弱性を標的とします。

Gafgyt のリスクを軽減するには

- すべての無線ルーターに最新のファームウェア更新がインストールされていることを確認する

Mirai

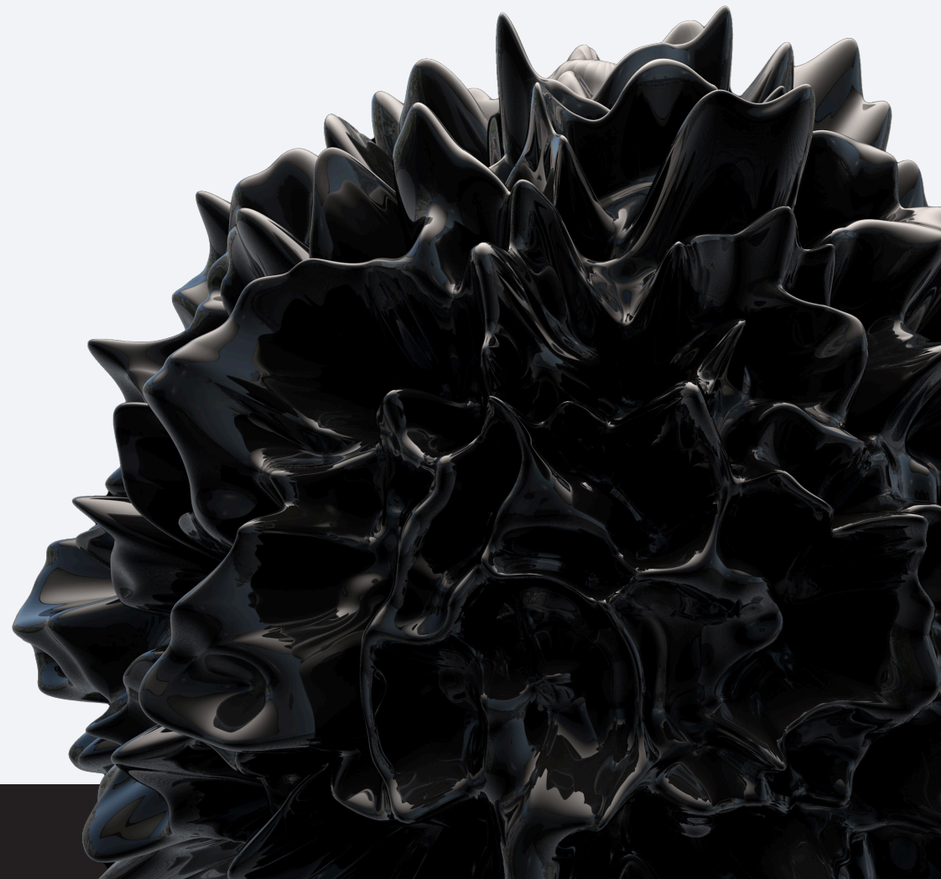
Mirai は、Linux プラットフォームをベースにしたマルウェアボットネットです。Mirai は、大規模な分散型 DDOS 攻撃を実行するために IoT デバイスを侵害します。Mirai は 2016 年 8 月に初めて特定され、世界最大規模の複数の DDOS 攻撃で利用されました [24]。最も有名な例を 2 つ挙げると、Brian Krebs 氏の Web サイトへの攻撃と、数百万のエンドポイントに影響を及ぼした DNS サーバーへの Dyn 攻撃です。

Mirai には、感染対象から除外する IP アドレスのハードコードリストがあり、ここには米国郵便公社と米国防総省が含まれています。脆弱な IoT デバイスが見つかると、Mirai は、出荷時のデフォルトのログイン認証情報が 60 以上含まれる辞書を使って、辞書攻撃を開始します。システムへの感染に成功すると、システムスキャンを実行して、競合するマルウェアを特定して削除します。

2016 年にオリジナルが検知されてから、Mirai には複数の亜種が出現しており、そのそれぞれが IoT デバイスで見つかった特定の脆弱性に合わせて調整されています。Mirai のソースコードは GitHub® で簡単に入手できるため、脅威アクターが亜種を作成するのも容易です。原作者が逮捕されても、ボットネットの持続性が収まる様子はほとんどありませんでした。IoT デバイスの普及、およびユーザーがデフォルトのパスワードを使い続ける傾向を考えると、Mirai は依然として深刻なリスクです。

Mirai のリスクを軽減するには

- IoT デバイスのネットワークアクティビティを一貫して監視する
- 侵害されたデバイスを分離する
- 効果的なネットワーク監視ツールを導入する
- アンチウイルスソフトウェアを最新に保つ



Setag

Setag は、2016 年に初めて出回っているのが発見された Linux ベースのマルウェアの亜種です。Setag は通常、悪意のあるサイトにアクセスした何も知らないユーザーによってダウンロードされた後に、バックドアをインストールします。また、他のマルウェア亜種によってシステムにドロップされる場合もあります。

ホストにインストールされると、Setag は、DDOS 攻撃を容易にするために使用する IP アドレスのリストなど、さまざまな設定ファイルをドロップします。このマルウェアにより、攻撃者は、機密情報の制御、抜き取り、持ち出しも実行できるようになります。

Setag はその進化の過程で、/etc/rc（1 ～ 5 の整数）.d/ および /etc/init.d/ の各場所にスクリプトを追加することで、再起動してもパーシスタンスを確立する能力を得ました。さらに、Apache Struts2 のリモートコード実行の脆弱性（CVE-2017-5638）[25] を悪用してホストに配信され始めました。

Setag の亜種は、Elasticsearch データベースを標的とした攻撃チェーンなど、ごく最近の 2019 年 7 月にも確認されています。

Setag のリスクを軽減するには

- すべてのデバイスとソフトウェアを最新に保つ
- 最新のセキュリティソリューションを使用する
- システムパッチが最新であることを確認する（Setag は Apache Struts2 のリモートコード実行の脆弱性（CVE-2017-5638）を悪用することがわかっています）
- インターネットを安全に閲覧すること（不審な添付ファイルを開かない、不明なソフトウェアを実行しないなど）の重要性についての従業員教育プログラムを社内に導入する
- Setag の侵入の痕跡である「/usr/bin/dpkgd/」フォルダーが作成されていないかどうか、システムを監視する
- 定評あるネットワークセキュリティソフトウェアを導入して、Setag の既知の C&C インフラストラクチャへの接続をすべてブロックする

XOR.DDoS は 2014 年に最初に確認され、2015 年に大規模な DDOS 攻撃で使用されました。XOR.DDoS は感染した Linux ベースのシステムを利用します。

XOR.DDoS

XOR.DDoS は 2014 年に最初に確認され、2015 年に大規模な DDOS 攻撃で使用されました。XOR.DDoS は感染した Linux ベースのシステムを利用します。このマルウェアは、ブルートフォース攻撃を利用して脆弱なデバイスの Secure Shell（SSH）サービスのパスワードを見つけて、システムに感染します。SSH の認証情報を手に入れたら、ルート特権を使用して、他の XOR.DDoS マルウェアをダウンロードしてインストールするスクリプトを実行します。

XOR.DDoS は、基本的なシステム情報を収集してから、その情報を暗号化して C&C サーバーに送信します。このマルウェアは、1 時間ごとに実行される cron ジョブを作成し、XOR.DDoS を確実にアクティブにします。さらに、他のファイルのダウンロードと実行、自己更新、実行中のプロセスの強制終了、ファイルの削除、および DDOS 攻撃を行うことができます。また、TCP-SYN フラッディング、TCP-ACK フラッディング、および DNS 増幅攻撃も使用できます。

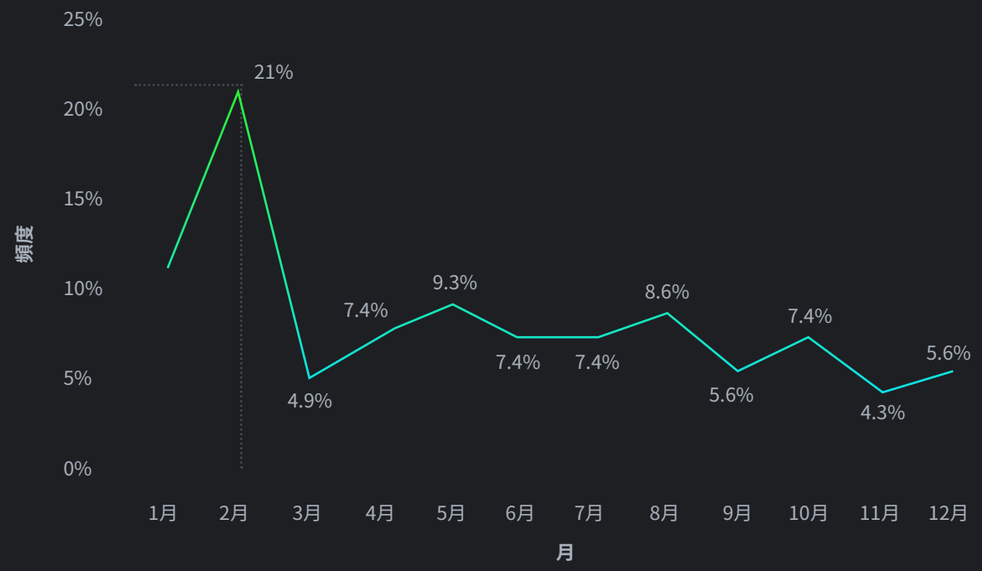
XOR.DDoS のリスクを軽減するには

- システムにパッチが適用されており、最新バージョンの Linux によってシステムが最新になっていることを確認する
- XOR の主な攻撃ベクトルとして、すべてのデバイスにパスワード強化を導入する（DDoS は不十分なセキュリティと脆弱なパスワードが原因です）
- ルート特権の不正アクセスを防止する
- 不審なネットワークアクティビティがないかどうかシステムを監視する
- 予期せずスクリプトが実行されていないかどうかシステムを監視する

2019 年の特筆すべきデータ侵害

残念なことに、2019 年の特筆すべきデータ侵害の大半は依然として、最新の攻撃者が展開した高度な新しい方法によるものではなく、保護されていないデータベースのために発生しています。2019 年は、またしてもデータ侵害における史上最悪の年になりました。現代の組織には、教育とセキュリティ強化の点でやるべきことが山積していることは明らかです。

2019 年の特筆すべきデータ侵害の頻度



American Medical Collection Agency（AMCA）

医療費回収サービスプロバイダーである American Medical Collection Agency の支払いポータルが攻撃を受けて漏洩が発生し、200,000 人以上の被害者が影響を受けました。このデータ漏洩は、2018 年 9 月前後に発生し、少なくとも 7 ヶ月続きました。この侵害は、AMCA の非対面取引（CNP）データベースがダークウェブで販売されているのが見つかって発覚しました。[26]

社会保障番号と生年月日の証拠が見つかった後、データを遡っていくと AMCA のオンラインポータルにたどり着きました。[27] AMCA の影響を受ける顧客には、医学的検査の大手企業、LabCorp と Quest Diagnostics が含まれていました。この侵害により、AMCA は最終的に破産を申請することになりました。その理由として、顧客への通知の送付と、最大の顧客を失ったことによるコストが挙げられています。[28]

2018 年 9 月

- 140,000 件の社会保障番号と生年月日
- 200,000 人の被害者

脅威アクターによる大規模侵害

2019 年 2 月、侵害された Web サイトから 6 億 1,700 万件のレコードが盗まれました。レコードを公開したのは、以前からダークウェブで 10 億件のレコードを売りたいと望んでいた攻撃者でした。公開されたデータの大半は 2018 年に発生した侵入によるものでしたが、その当時は公開されてはいませんでした。影響を受けた標的には以下が含まれます。

- Dubsmash、ビデオメッセージングアプリケーション
- 500px、写真投稿ソーシャルネットワーキングサイト
- Mindjolt、ゲーミングプラットフォーム
- Wanelo、デジタルモール
- Yanolja、韓国の旅行会社

報告によると、攻撃者は Web アプリケーションの脆弱性を悪用してユーザーアカウントデータにアクセスし、データを持ち出しました [29]。

2019 年 2 月

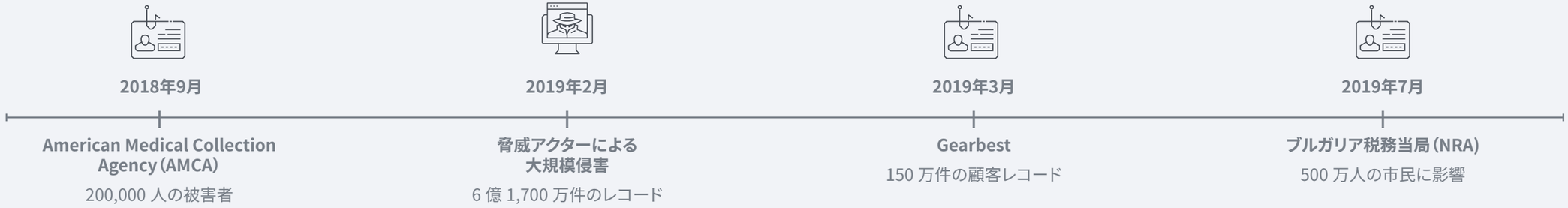
- 6 億 1,700 万件のレコード
- Web アプリケーションの脆弱性

Gearbest

2019 年 3 月、あるセキュリティ調査担当者が、オンラインショッピング大手の Gearbest に属する Elasticsearch サーバーが公開されているのを発見しました。このサーバーには、支払いレコードや注文などに関係する顧客データレコードが 150 万件以上入っていました。報告によると、このデータは暗号化されない状態で保存されていました [30]。Gearbest は公表時に、この侵害は、公開されていたデータベースに一時的にデータが保存されていた新規登録顧客に影響する可能性があると述べています。[31,32]

2019 年 3 月

- オンライン小売業者
- 150 万件の顧客レコード
- 暗号化されていないデータベース



ブルガリア税務当局（NRA）

2019年7月、匿名の脅威アクターがブルガリアのメディアに連絡してきて、「財務省のサーバー」に対する攻撃について詳しく報告しました。この攻撃は、国民識別番号、納税額と社会保障給付額、負債などが記録されたファイルが入った約57個のフォルダーに影響を及ぼし、この侵害によって影響を受ける可能性があるブルガリア市民は最大で500万人にも上りました。その翌日、NRAは攻撃を認め、「サーバーはめったに使用されない、海外取引用のVAT還付サービス経由でアクセスされた」と述べ、この侵害がデータベースの3%に影響することを発表しました。[33, 34]

2019年7月

- 500万人の市民に影響
- データベースの3%
- 国民ID番号、納税額と社会保障給付額

実施できる対策

データ侵害は複数の要因によって引き起こされます。適切なセキュリティ予防措置を実践し、原点に戻った対策を適用することで、侵害の可能性を効果的に低減できます。セキュリティ態勢を向上させることができるステップには、次のようなものがあります。

フィッシング攻撃を緩和するには

- ソーシャルエンジニアリング戦術に関するセキュリティ意識向上トレーニングをユーザーに対して定期的に実施する
- エンタープライズに展開されているアプリ全体に多要素認証を適用する
- ドメイン偽装に対抗するためにDMARCを設定する

認証情報の侵害を緩和するには

- 企業機密の保存にパスワードマネージャーを適用する
- AI駆動型のユーザー行動解析を使用してユーザーのアクティビティを監視する
- 強力なパスワードを適用して定期的にローテーションする
- 最小特権の原則に基づいて許可を割り当てる

セキュリティの設定ミスによる影響を緩和するには

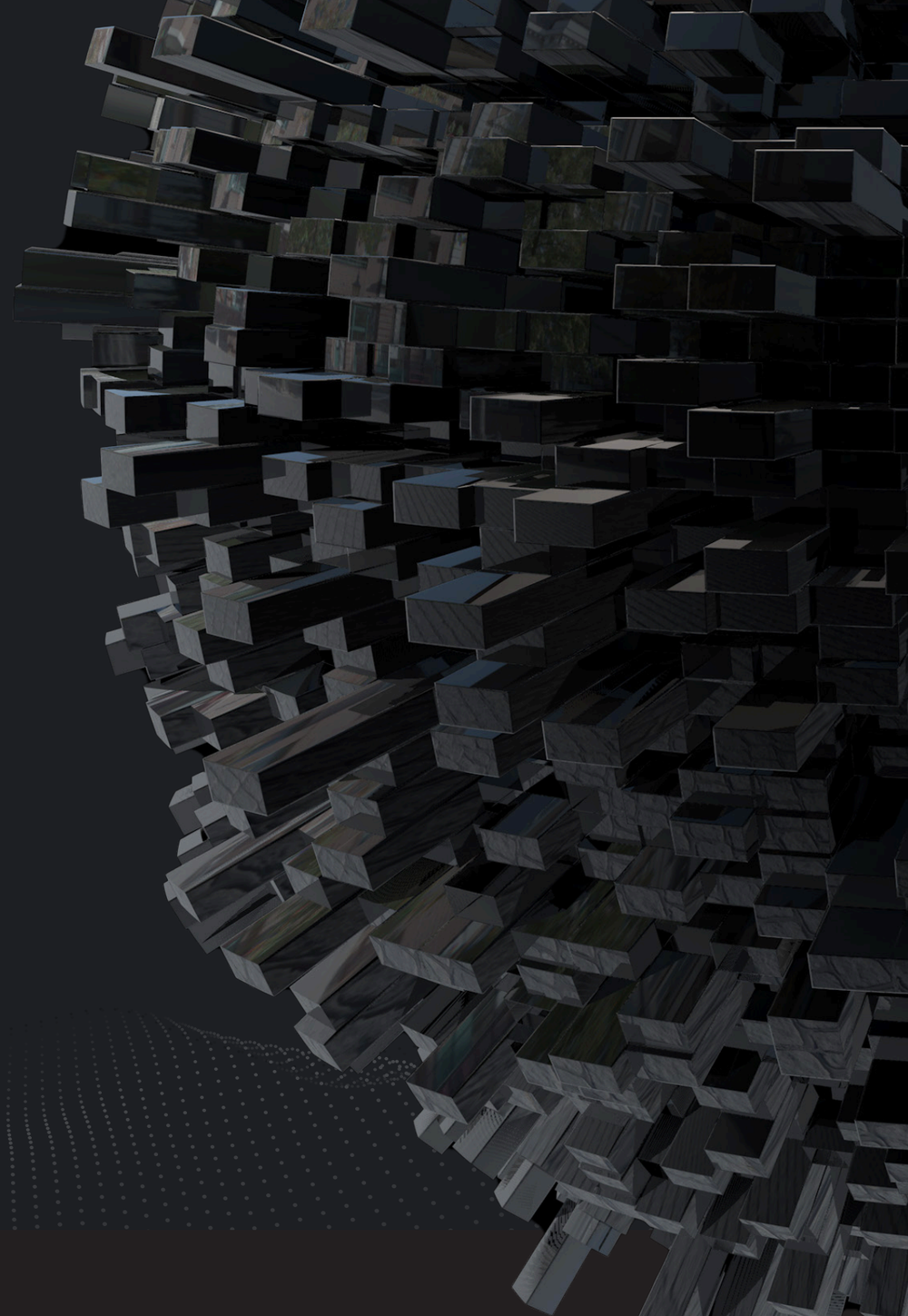
- ソフトウェア脆弱性に定期的にパッチを適用する
- 自動化された継続的統合プロセスを導入し、そのプロセスにより、組織で定義されたクラウドリソース展開ポリシーを適用する

ID アクセス管理：すべてのモノがつながったエンタープライズを保護

今日のプロフェッショナルは、かつてないほど自由にデータにアクセスできます。クラウドインフラストラクチャとグローバルな接続により、さまざまな場所で広く情報を利用できるようになった一方で、テクノロジー企業によって大量のデータアクセスデバイスが提供されています。しかし、無線情報の到達範囲および接続デバイスの増加と共に、攻撃対象領域が拡大していることに留意することが重要です。その結果、労働リソースが IoT デバイスを操作する際に、多くのエンドポイント保護戦略が課題に直面します。[35]

スマートフォンを使用して業務メールにアクセスしている従業員について考えてみましょう。この従業員は、出張時には自分の電話を車とペアリングします。この電話はどの程度安全でしょうか。電話にアクセスするさまざまなサードパーティアプリはどの程度安全でしょうか。そして自動車の組み込みシステムはどの程度安全でしょうか。IoT デバイスの性質上、各相互接続チェーンのどこかに脆弱なリンクが存在することはほぼ確実です。

会社支給デバイスのみを許可する体制から BYOD ポリシーを採用する体制へと組織が移行すると、攻撃対象領域は拡大します。個人のデバイスから組織のデータにアクセスする従業員が増えるに従い、ユーザー ID を検証するタスクがビジネスにとってますます重要になります。多要素認証（MFA）は、ID の検証に関する問題に対処するために使用されている手法の 1 つであり、広く採用されています。この方法では、ユーザーはアカウントにログインする際に、2 つ目のソースによって自身の ID を確認する必要があります。ユーザーの正当性を検証することにより、組織は、そのデータが悪意を持って侵害されるリスクを低下させることができます。



MFA は効果的なサイバーセキュリティ戦略の重要な要素ですが、ユーザー ID に関する問題をすべて解決できるわけではありません。たとえば、MFA は 1 回限りのアクションであることが多く、これではユーザーの通常の行動や習慣が考慮されません。多くの場合、ユーザーは朝、認証したら、その日は終日、信頼できるユーザーと見なされます。しかし、ユーザーがワークステーションを離れたらどうなるでしょうか。朝開始された認証済みセッションが午後も同じユーザーによって使用されているかどうかを、組織はどうすれば確認できるでしょうか。

これに関連する話として、アムネスティインターナショナルのレポートによると、脅威アクターは、フィッシングサイトを使用して 2 要素認証（2FA）コード [36] を傍受して盗んでいます。認証プロセスの特定要素の脆弱性に的を絞ることで、2FA または MFA の迂回方法を見つけようとする攻撃者もいます。有名な迂回手段の 1 つでは、SMS 通信の欠陥を悪用して、認証コードを目的の受信者ではなく攻撃者へリダイレクトします [37]。2FA と MFA は良い方向へ向かう確実な一歩ですが、改善の余地があるのは明らかです。

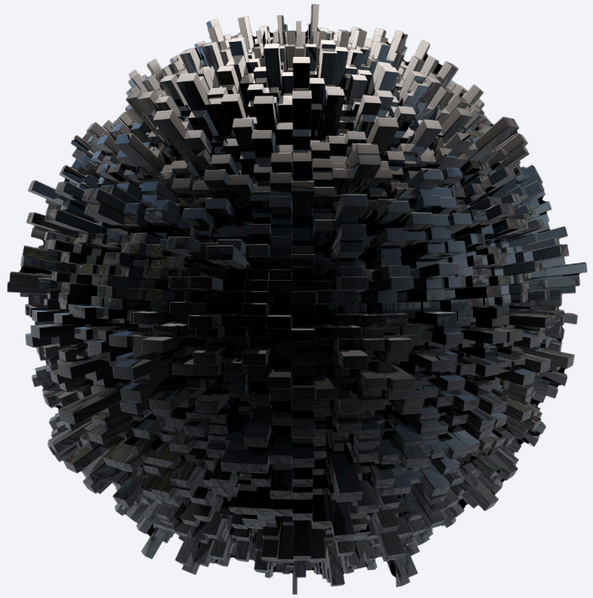
2016 年以降、侵害されたアカウントと認証情報が絡むインシデントは 280% 増加しました。[38] この増加は主としてスタッフィング攻撃によるもので、脅威アクターは、盗んだユーザー名とパスワードを使用して複数のオンラインサイトへのアクセスを獲得します。スタッフィング攻撃は、比較的単純ではあるものの成功を収めており、より優れた ID アクセス管理が早急に必要であることが浮き彫りになります。

再考を要するセキュリティ概念の 1 つは、単一で静的な、イエス／ノーの 2 つの値による ID 認証プロセスの考え方です。このアプローチは、システムへの初期アクセスを付与するのには有効ですが、長時間にわたって ID を検証する方法を備えていません。より賢明な代替手段は、認証システムによって継続的な信頼レベルを確立できるようにすることです。

たとえば、おそらく初回ログイン時に、システムでユーザーを 100% 確実に正しく識別できるとします。後になって、おそらくは異常なアクセス要求や新しいオンライン行動により、システムによるユーザーの信頼は 70% に低下します。このように信頼が失われた場合、それはユーザーの ID を再認証すべき時が来たことを示します。

継続的ユーザー認証は、リソースを多用する処理であり、それによってユーザーの生産性を損なうおそれがあるように思えるかもしれません。しかし、高度にトレーニングされた適応型 AI であれば、従業員に過度な負担をかけることなく、ユーザーの行動を検知、解析できます。さらに、信頼レベルを判断する際に、ユーザーの地理的な場所からその標準的な活動予定まで、さまざまな情報を考慮することもできます。AI 駆動型のユーザー識別では、従業員は、オフィス、自宅、公共の場など、仕事の場所に応じてユーザーのアクセスを使い分けることができます。

BlackBerry Cylance の新たな AI 駆動型の継続的ユーザー認証テクノロジーには、開発の原動力となった概念と考慮事項が多数ありますが、これらはそのうちのいくつかに過ぎません。近い将来、弊社は、その高度なユーザー ID テクノロジーを、既存の IoT、モバイル、およびエンタープライズのセキュリティプラットフォームに統合する予定です。



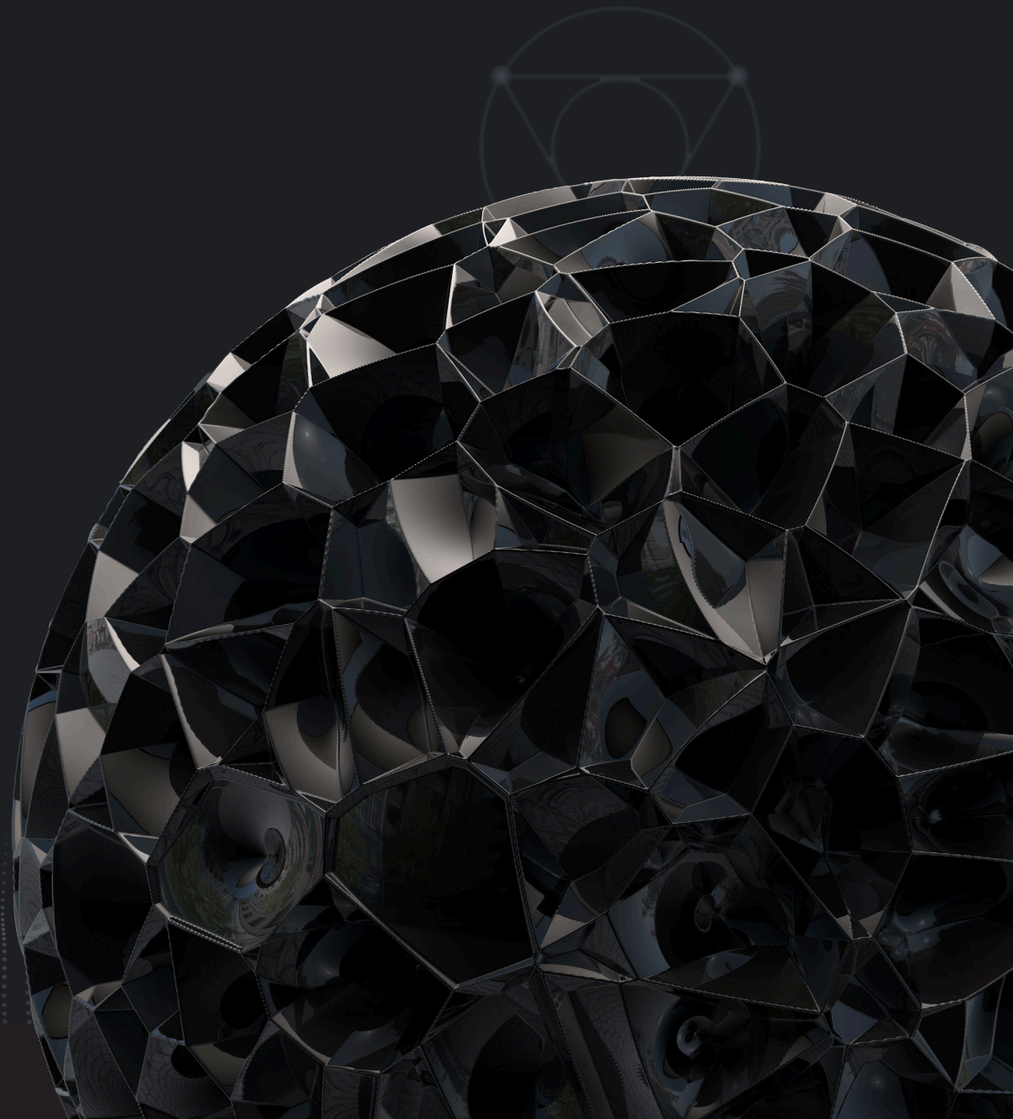
AI 駆動型のユーザー識別では、従業員は、オフィス、自宅、公共の場など、仕事の場所に応じてユーザーのアクセスを使い分けることができます。

モバイルセキュリティの問題

他者の間違いから学ぶ

多くの場合、侵害が発生する前にセキュリティ態勢の欠陥を特定するのは困難です。たとえば 2017 年、Equifax は機密の顧客データを保護するための適切な多層型セキュリティを実装していませんでした [39]。この侵害によって 1 億 4,800 万人の顧客が影響を受けました。その後の調査から、Equifax に対する以下の 11 個の推奨改善策を示した Mandiant のレポートが作成されました。

- 脆弱性スキャンとパッチ管理を強化する
- データベース内の機密データの保持期間を短縮する
- 重要なシステム内にあるデータにアクセスするための制限と制御を強化する
- ネットワークセグメンテーションを強化して、インターネットからのアクセスを制限する
- 追加の Web アプリケーションファイアウォールを展開し、シグネチャを調整して攻撃をブロックする
- アプリケーションと Web サーバーに、ファイルの完全性を監視するテクノロジーを展開する
- ネットワーク、アプリケーション、データベース、およびシステムの各レベルで追加のログを適用する
- 特権アカウント管理ソリューション展開する
- ネットワークトラフィックのインライン復号機能を追加展開し、暗号化トラフィックを増やす
- エンドポイント検知および対処エージェントテクノロジーを増やす
- 追加のメール保護および監視テクノロジーを増やす



弊社は、モビリティソリューションが、Equifax に影響を及ぼしたものと同じ脆弱性に直面しているかどうかを評価するため、調査を実施しました。潜在的なモビリティの脅威が見つかった場合、その脅威について検討し、潜在的な緩和策を特定しました。続いて、弊社が提供するさまざまな緩和策をエンタープライズの各部門が確実に検討、実装できるよう取り組みました。これらの戦略の責任を設定するには、それらを企業内の特定のチームに割り当てます。たとえば、モバイルセキュリティの特定の要素に責任を持つグループに緩和策を任せた場合、将来、緩和策を実装する際にもそのグループが責任を持ちます。

今後セキュアな MDM サービスを提供することを検討する場合、モビリティベンダーと IoT ベンダーは、セキュリティの回復力および向上プログラムなどの概念に重点を置くことになります。攻撃者の目的（業界の他の侵害から導出）を評価することにより、各ベンダーは、より効果的に次のようなさまざまな技術制御分野に対応できます。

- エンドポイントセキュリティ
- ソフトウェアインベントリによるログの強化
- データ保護
- 新製品導入プロセス

モビリティと IoT のスペシャリストは、モビリティソリューションの実現に使用する適用済みコンポーネントの責任を特に考慮する必要があります。機能コンポーネントは、独立した別個の機能として管理する必要があります。エンタープライズサーバー、エンタープライズクライアント、接続 IoT デバイス、および他のハードウェアによるソリューションは、それぞれ分離する必要があります。このアプローチにより、企業は、ビジネスプロセスと、それらを実現するテクノロジーとの間でより効果的にリスクを評価できます。

弊社の調査の結果、モビリティプロバイダーと IoT プロバイダーは、簡単に最重要事項を評価して、製品に対する主な脅威を特定できると考えられます。消費者も同様に、セキュリティへの対処と脅威緩和アクティビティを集中すべき最重要事項のリストを独自に作成できます。

モビリティプロバイダーと IoT プロバイダーは、体系的アプローチによって、漏洩の可能性を特定します。この脅威マッピングプロセスにより、保護と検知の制御を最大化し、環境全体で対処および回復プロセスを統合できます。

弊社は、次のような、モビリティプロバイダーと IoT プロバイダーが対処すべき機能コンポーネントの脅威を特定しました。

弊社の調査の結果、モビリティプロバイダーと IoT プロバイダーは、簡単に最重要事項を評価して、製品に対する主な脅威を特定できると考えられます。

エンタープライズ MDM サーバーに潜む危険

- 製品環境内の水平移動
- MDM エンドポイントと API の脆弱性
- 外部コンポーネントとルーティングメカニズムからの MDM の公開
- セキュリティに既存の問題がある他の MDM システムとの統合
- テナント間のクラウドの問題（クラウドユーザーの場合）
- 新機能で持ち込まれるセキュリティの問題
- オープンソースソフトウェアまたはサードパーティライブラリの脆弱性
- Web の脆弱性
- 脆弱な暗号
- 不十分なログと監視

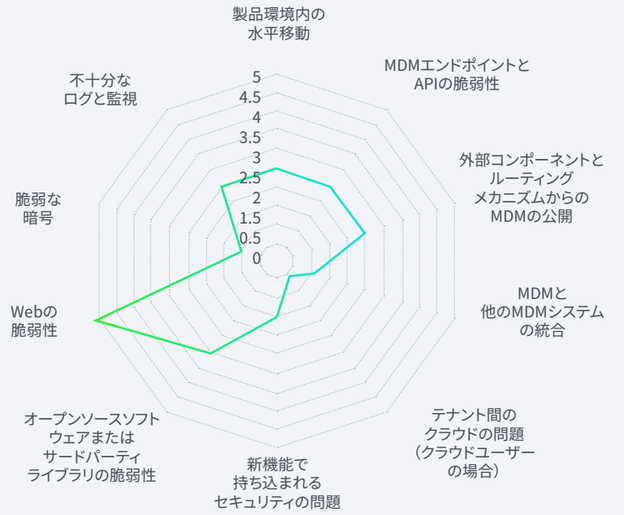


図 1：脅威の拡大と重大度／拡散性の予測の概要

エンタープライズクライアントに潜む危険

- クライアントアプリケーションのデータ漏洩
- 不適切な DLP 戦略と OS の変更の連動
- プレーンテキストでの転送と保存
- リバースエンジニアリングによる、アプリケーション開発時に判明していなかった脆弱性の特定
- ルート化ツールやフッキングフレームワークによる Android のルート化と iOS の脱獄に対する保護の迂回
- アプリケーション完全性保護の迂回または破壊
- 脱獄およびルート化検知の隠蔽またはマスク
- アプリケーション開発時に判明していなかった脆弱性
- クライアントのテスト

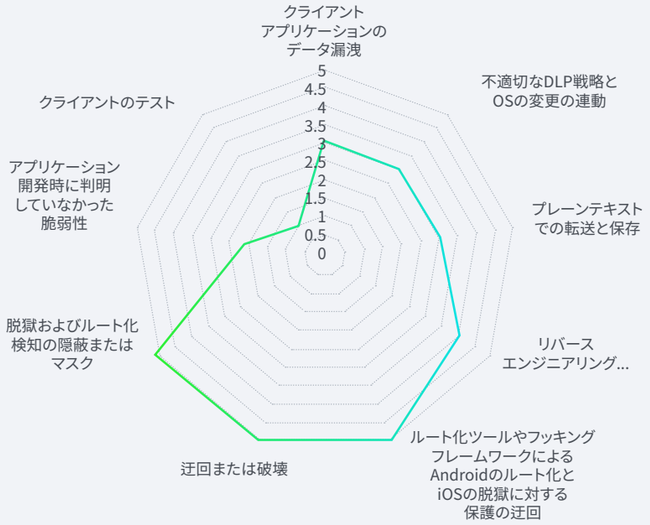


図 2：脅威の拡大と重大度／拡散性の予測の概要

IoT に潜む危険

- 自己ホスト型からクラウドへ移行する場合の課題（データの取り扱い、認証、および承認を含む）
- リソースがインフラストラクチャプラットフォームで管理されている環境でワークロードをスケールする際のクラウド内の機密情報の取り扱い
- アーキテクチャの変更または新規実装によって発生する、脅威モデルの想定外の変更
- データベースの移行または変更によるデータベースインジェクション攻撃
- ビジネスロジックの欠陥、特権エスカレーション、認証
- 汎用 Web アプリケーションの脆弱性（OWASP の上位 10 件）

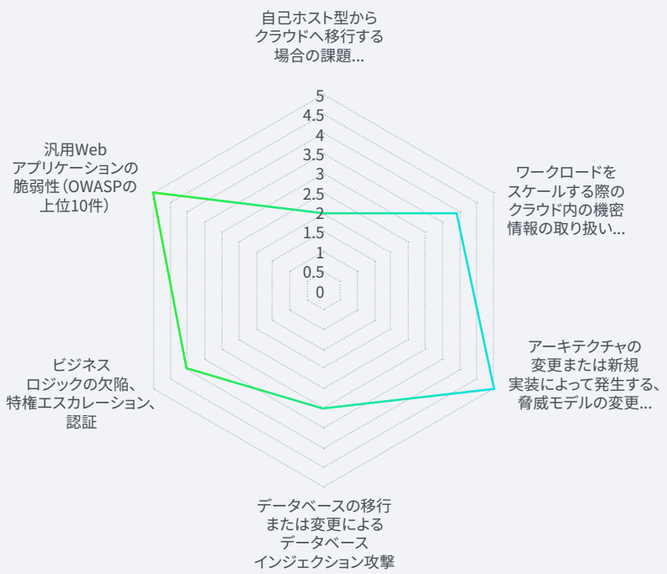


図 3：脅威の拡大と重大度／拡散性の予測の概要

エンドユーザー、MDM、および IoT ベンダーは、蔓延するこれらの脅威を包括的かつ体系的に考慮し、それらの管理計画を策定する必要があります。セキュリティ計画では、業界のベストプラクティスを使用しつつ、他社の失敗例も考慮する必要があります。顧客とベンダーが協力してセキュリティの維持管理に当たることで、攻撃の影響を大幅に軽減できます。

氷山効果

氷山効果とは、前述の図から生まれたパラダイム概念を指すもので、中心線より上に出現する危険は全体の 20% で、80% は中心線より下に出現することを表します。図 2 のクライアントの解析からわかるように、MDM プロバイダーと消費者は、中心線より下にある大きな割合を占める脅威に的を絞れば、外部の攻撃対象領域を大幅に削減できます。

この 1 年で、顧客からいくつかの攻撃に重点を置いたテストを委託されることが増えました。これには以下が含まれます。

- リバースエンジニアリングによる、アプリケーション開発時に判明していなかった脆弱性の特定
- アプリケーション完全性保護の迂回または破壊
- 脱獄およびルート化検知の隠蔽またはマスク

適切なスキルと十分な時間がある攻撃者であれば、通常は、セキュリティコントロールを迂回する独創的な方法を見つけることができます。攻撃者を支援する有名なツールや明確に文書化された標準をいくつも利用できます。このようなリソースの多くは、無料で公開されています。たとえば、Frida などのツールです。Frida は、動的なインストルメンテーションツールキットで、これにより、攻撃者はロックダウンしたソフトウェア内で独自のスクリプトを実行できます。Frida では、攻撃者はライブプロセスにフックしてアプリケーションに機能を追加できます。別のツールである Magisk では、攻撃者は、ルートアクセスを奪って他のシステムを変更できます。Magisk は、システムファイルを物理的に変更することなくシステムを変更します。これは一般的にシステムレスルートと呼ばれます。この

手法により、デバイスの改ざんチェックを迂回できます。さらに、攻撃者に他のシステムへのアクセスを付与する、悪意のあるアプリケーションやソフトウェアをインストールすることもできます。

モバイル脅威への対処

MDM ベンダーは、どうすればモビリティの問題をもっと効果的に管理できるでしょうか。弊社のアプローチは、脅威の防御、検知、対処を行うさまざまなセキュリティコントロールを自動化することです。また、手動コントロールも複数あり、これらは消費者の包括的なセキュリティ戦略に役立ちます。アプリケーションコードの難読化、完全性チェック、ルート化と脱獄の検知機能を抜本的に改善すると、攻撃対象領域を削減できます。コンパイル済みコードの解析に要する時間を増やすと、攻撃者にそのような作業の着手を断念させることができます。エンタープライズが侵害の検知、対処、回復のための時間を稼ぐことができるセキュリティ対策があれば、組織にとって純粋な利益になります。

MDM ベンダーのアプリケーションとコードでは、コードの流れと、文字列および記号の難読化に集中的に取り組む必要があります。モバイルアプリケーションのコードは、攻撃者が静的解析によって重要な属性や機能を特定して悪意のある用途に使おうとする行為に抵抗する必要があります。コーディングの抜本的向上は、2020 年のサイバーセキュリティ戦略において大きな役割を果たす可能性があります。また、難読化の抜本的向上は、現在のサイバーセキュリティ戦略においても基礎的な役割を果たすものと理解しています。サービスとしての難読化の提供において重要な役割を持つプロバイダーの重要性と需要が高まっています。

弊社では、脱獄およびルート化検知戦略を実装しているベンダーを複数確認しています。これらの戦略への関心は、その重要性を認識する人々が増えるにつれ、今後も引き続き成長します。場合によっては、ルート化および脱獄のアクションにより、デバイスや関連リソースが、対応策のない攻撃を受けることがあります。セキュリティスペシャリストは、重要なインフラストラクチャポイントで、強化されたルート化検知テクノロジーを使用することを考慮する必要があります。自己検知戦略を向上させて、検知が一切迂回されないようにする必要もあります。

組織は、完全性コントロールの強度とアプリケーションの両方を検討する必要があります。これにより、悪意のあるアプリケーションが攻撃プラットフォームとして使用されるのを防ぐことができます。

弊社では、重要な改ざん対策ソリューションが大きな注目を集めて向上したことを確認しています。これは、MDM プロバイダーと消費者が適切なオンデバイスの改ざん防止検知メカニズムを検討する必要があることを示します。ソリューションには、多角的な検知アプローチが含まれる必要があります。1 つの方法に特化したソリューションや、改ざん防止コードを分散化および難読化していないソリューションは避けてください。推奨される改ざん防止ソリューションには、機密性の高い操作（アプリケーションの起動など）が発生した場合のトリガが含まれる必要があります。

アプリケーションの完全性は、今日のエンタープライズの成功の土台になっています。弊社では、アプリケーションの完全性の検証がいくつかの大きな進化を遂げたことを確認しています。たとえば、Google SafetyNet は、次のようなセキュリティの脅威からアプリケーションを保護する一連のサービスを提供しています。

- デバイスの改ざん
- 不正な URL
- 潜在的に有害なアプリ
- 偽のユーザー

MDM ベンダーは現在、これらの種類のフレームワークを強化して厳格な完全性コントロールを可能にし、それによってモビリティエコシステムの信頼を構築しようとしています。組織は、完全性コントロールの強度とアプリケーションの両方を検討する必要があります。これにより、悪意のあるアプリケーションが攻撃プラットフォームとして使用されるのを防ぐことができます。

結論を述べると、弊社は、アプリケーション層（クライアントの業種内）を、ベンダーと消費者が焦点を当てる価値がある周辺境界と見なしています。ある意味、この領域ではいたちごっこのような問題が生じ、正当なビジネスやユーザーに対して、正体不明の攻撃が平行して続きます。多くのタイプの攻撃がコードレベルでのエンジニアリングに重点を置いています。したがって、認識している脅威と現実化した脅威の両方に従ってセキュリティパラメータを進化させるには、複数の戦略的目標があります。

- セキュリティを継続的に観察する
- 他人のミスから学ぶ（Equifax から学んだのと同じように）
- 各分野でエキスパートとして評価されているベンダーから学ぶ
- 消費者と攻撃者間の進化する力学を観察する
- すべての層（下層のコアテクノロジーまで）で検知、防止し、変化するセキュリティニーズに対処できる長期的なビジネス戦略を策定する

2020 年の注目トレンド

ディープフェイクが脅威アクティビティを支える

ディープフェイクは、Reddit® ユーザーが考え出した造語で、機械学習手法で作成された、操作されたデジタル表現のことです。具体的には、この操作プロセスは、敵対的生成ネットワーク（GAN）を使用して、改変された出力を生成および洗練させます。

2019 年、Katie Jones という名前の人物が、存在しないアイデンティティのプロファイル画像を使用しているのが見つかりました。このプロファイルの目的は依然として不明ですが、Katie は、CSIS（戦略国際問題研究所）に勤務する調査担当者を装い、LinkedIn でさまざまな著名人とのつながりを築いていました [40, 41]。

さらに、セキュリティ調査担当者は、2019 年の最初の 7 ヶ月間にディープフェイク動画の数が大幅に増加したことを発見しました。これは、2018 年に報告された数のほぼ 2 倍に当たる増加です [42]。また現実世界でも、AI 生成音声が CEO の声をまねて被害者をだまし、多額の金銭を送金させるという事例が 3 件発生しました [43]。

これは、2020 年に増加すると思われるトレンドで、そこには次のような要因があります。

- 地政学的アクティビティを支援する虚偽情報キャンペーン
- リアルな出力を生成するために必要なツールの入手性の上昇と高度化
- ソーシャルエンジニアリングツールとしてのディープフェイクの有効性

組織がこのトレンドに備えるには、財務取引を承認する前に多段階の検証を要求するポリシーを策定します。経営者は、ディープフェイクテクノロジーとは何で、どのように詐欺に使用されるかについて定期的に従業員を教育することを検討する必要があります。

… セキュリティ調査担当者は、2019 年の最初の 7 ヶ月間にディープフェイク動画の数が大幅に増加したことを発見しました。

クラウドリソースの設定ミスによるデータ損失の増加

BlackBerry Cylance が 2019 年に一般に公表されたデータ侵害を調べたところ、クラウドの設定ミスによって引き起こされたデータ漏洩に関して興味深いトレンドがわかりました。平均すると、保護されていないデータベースやサーバーによって引き起こされた漏洩が、毎月少なくとも 3 つ公表されていました。これらのデータ漏洩によって一般に漏洩したレコードは、合計 70 億件以上に上ります。

組織が継続的統合に対するニーズと安全な展開の実践のバランスを取ることに依然として苦慮していることを考えると、この数字は驚くに当たりません。セキュリティ対策は後付けで実装されることがほとんどで、規制遵守の圧力に後押しされることもあります。それとは逆に、責任共有モデル [44] における自社の役割に苦慮している企業もあります。責任共有モデルとは次のようなものです。

- クラウドサービスプロバイダー（CSP）は、採用するモデルに応じて、基礎となるハードウェアとソフトウェアをサポートするインフラストラクチャを保護することが期待されている
- 消費されるリソースに関連する設定は顧客が保護する

さらに、セキュリティオペレーションセンター（SOC）は、コンテキストを欠いた大量のアラートに疲弊している傾向が見られます。そのため、SOC アナリストが対処が必要なアラートを優先しようとすると、潜在的に悪意のあるアクティビティがアナリストのレーダーをすり抜けてしまう可能性があります。

ガートナーによると、クラウドへの投資に優先順位を付けようとする組織が増えるにつれ、パブリッククラウドで提供されるサービスとしてのインフラストラクチャ（IaaS）製品が増加し、その売上は 2019 年の 389 億ドルから年には 491 億ドルへ増加すると予想されています [45]。この予測と、クラウドのセキュリティ向上に関する継続的な課題を考慮して、弊社も同じく資産の設定ミスによって引き起こされるデータ侵害が増加するものと予測しています。これらの損失は、各セキュリティ対策のバランスを取るために適用する取り組みと、進化し続けるビジネスニーズをサポートするのに必要なソフトウェア定義インフラストラクチャを管理するために適用する取り組みとが、不十分であるために発生する可能性があります。

平均すると、保護されていないデータベースやサーバーによって引き起こされた漏洩が、毎月少なくとも 3 つ公表されていました。これらのデータ漏洩によって一般に漏洩したレコードは、合計 70 億件以上に上ります。

次のような多角的なクラウドセキュリティアプローチを取ると、組織はより効果的に準備できます（ただし、このアプローチに限定されません）。

- 継続的統合を促進し人的エラーを削減する、自動化された設定ポリシーを導入する
- 開発者向けに、脅威インテリジェンス駆動型の意識向上トレーニングを採用する（アクティブなクラウドセキュリティの脅威とベストプラクティスに焦点を当てる）
- システム設定とユーザーアクティビティの異常を発見できるネットワークおよびユーザー行動解析を利用して、環境の可視性を向上させる

2020 年の脆弱な自動車

サイバー攻撃を回避する確実な方法は、脅威アクターにとって価値があるものを一切保有しないことです。自動車が長い間攻撃から守られてきた理由は、価値の低い標的であったからです。最新の自動車がさまざまな通信ネットワークに接続されるようになるにつれ、この力学は変わりつつあります。残念なことに、自動車は急速に、他のコネクテッドテクノロジーで利用できたセキュリティ開発を完全に欠いたモバイルエッジデバイスになりつつあります。

たとえば、多くの自動車 OEM メーカーは、その製品の保護に熱心ではありません。実際、60% 以上の OEM は自社のハードウェアとソフトウェアの半数未満でしか脆弱性をテストしていません。[46] セキュリティスペシャリストにとってもう 1 つの課題となるのは、自動車の長いライフサイクルです。自家用車は 7 ～ 15 年使用される場合がありますが、その間、さまざまなソフトウェアコンポーネントやファームウェアコンポーネントが一度も更新されないことがあります。このような怠慢は、脅威アクターに対し、自動車の侵害方法を考案するのに十分な時間を与えることになります。

自動車の生産に必要なベンダーサプライチェーンも、広範な攻撃対象領域となります。サプライチェーンに含まれる各 OEM メーカーによって、自動車に不明な脆弱性が持ち込まれる可能性があります。最終製品に貢献している国や会社の数を考えると、状況は複雑化する一方です。

... 多くの自動車 OEM メーカーは、その製品の保護に熱心ではありません。実際、60% 以上の OEM は自社のハードウェアとソフトウェアの半数未満でしか脆弱性をテストしていません。

テクノロジーで自動車の評判を向上

自動車に技術システムが追加されるたびに、別の潜在的な攻撃ポイントが持ち込まれて、攻撃対象領域が増加します。現在の自動車で動作しているさまざまなオンボードシステムについて考えてみましょう。そこには、ネットワーク通信システム、センサーアレイ（LIDAR と RADAR を含む）、カメラ、地理位置情報デバイス、およびエンジンと燃料性能を制御するレガシーシステムがあります。自動車によって収集される個人データの量も増加しています。最新の自動車は、個人情報、パフォーマンスメトリック、地理位置情報などを保存または処理する場合があります。

サイバーセキュリティ態勢を向上させないまま、自動車によって収集される貴重なデータを増やすと、自動車は間違いなく脅威アクターにとって魅力的な標的になります。サプライチェーンのために発生する脆弱性、ソフトウェアとファームウェアの更新の欠如、接続されている IoT デバイス、およびアフターマーケットのアップグレードは、脅威アクターにとって狙いやすい攻撃対象領域になります。今すぐ自動車のセキュリティを向上させる手段を取らなければ、自動車は格好の餌食を求めている攻撃者にとって最高の標的になって当然です。

誰が自動車を侵害するのか

Upstream[47] が最近公開したレポートでは、2010 ～ 2018 年に発生が報告された車両へのサイバー攻撃を解析しています。攻撃は、正当な調査を実施するホワイトハットアクターによるものと、悪意のあるブラックハットアクターによるものに分かれていました。自動車に対する攻撃は時間と共に全般的に増加していましたが、最も注目すべき変化が起きたのは、ブラックハット攻撃がホワイトハット攻撃を上回った 2018 年のことです。悪意のある攻撃が調査担当者による攻撃を上回っている場合、脅威アクターがセキュリティの脆弱な業界を発見したことを示している可能性があり、今後攻撃が増加します。

ホワイトハット／ブラックハットのパラダイム以外の別の侵害クラスは、自動車のドライバーによる意図しない情報漏洩です。複数の異なるドライバーが利用するレンタカーにおいて、各ドライバーが自身のモバイルデバイスをさまざまな車両システムと同期している状況を考えてみてください。車が次のドライバーに渡ったときに、これらのシステムにまだ前の利用者の個人データやプライベートデータが含まれている可能性があります。

車を売却したときにも同じ状況が発生するおそれがあります。自動車の使用状況を追跡する Web ポータルやモバイルアプリが自動車で提供されている場合、前の所有者がまだそれらにアクセスできる可能性があります。中古車の買い手は、自動車の元の所有者の地理位置情報、ガレージドアのアクセスコード、さまざまなログイン認証情報を漏洩させるリスクがあります。自動車の売り手も危険に直面します。古いモバイル Bluetooth® 接続には、連絡先情報、音楽、頻繁に訪れる場所が保存されているおそれがあるためです[48]。

実施できる対策

サイバー脅威から自動車を保護するのは途方もないタスクです。前述のように、自動車のサプライチェーン、OEM のプロセス、IoT 接続など、自動車の製造と運転に関する多数の要素が脆弱性の発生源になります。最新の自動車は急速に、サイバー脅威からの保護が不十分かまったく保護されていないモバイルコンピューターになりつつあります。これらの複数のセキュリティ脆弱性に対応する万能ソリューションはありませんが、次のように、状況の改善につながる可能性がある重要な変化がいくつか見られます。

- セキュリティを念頭に置いて設計する。自動車メーカーと OEM ベンダーは、サイバーセキュリティ戦略を後付けで追加するのではなく、設計の最初の段階から考慮する必要があります。
- 自動車やドライバーの情報を保存するすべての車両システムにデータ暗号化を実装する。
- コンポーネントをサイバーセキュリティ対応として認証するために、包括的な信頼システムを開発する。
- 自動車のライフサイクルの間、サイバーイベントを積極的に探して対処する。自動車のサイバー脅威を追跡、解析、および報告する Automotive Information Sharing and Analysis Center（Auto-ISAC）などのリソースを利用する必要があります。
- 自動車のソフトウェアとファームウェアを安全にリモートで更新するシステムを開発する。セキュリティパッチを Web サイトで一般に公開することもできますが、更新が他のリスクにさらされます。攻撃者が、一般に公開されている更新をリバースエンジニアリングする可能性があります。顧客が自動車を手動で更新するのは難しすぎるので、更新しないことに決める可能性もあります。

今後の見通し

時間が経つにつれて、自動車はますますテクノロジー主導になり、相互接続化が進んでいきます。サイバー脅威に対する保護を最初に行うことなく、自動化車両の時代に向かって突き進むことは、悲劇的な（また完全に回避可能な）間違いです。自動車業界がサプライチェーン、製造、および保守システムへの強力なサイバーセキュリティ対策の導入に取り掛かることが不可欠です。自動車を適切に保護しなければ、プライバシー法違反で会社に罰金を科される可能性があり、さらに重要な点としてドライバーの生命をリスクにさらす可能性があります。

予測：2020 年の展望

未来を予測するのは不可能ですが、BlackBerry Cylance では、弊社の経験豊富なエキスパートに依頼して、これからのサイバーセキュリティの問題についての考えを共有してもらいました。新しい年を迎えるに当たって弊社の人材が注視している問題を以下にいくつか示します。

サービスとしてのクライムウェアによってランサムウェア攻撃が増加

Everything-as-a-service は、現在の企業の状況をよく表している特性です。この概念がサービスとしてのクライムウェア（CaaS）として最終的にインターネットの最も暗い隅々にまで広まるのを避けることはおそらくできなかったでしょう。現在では、高度なスキルを持つ脅威アクターが、悪意のあるアクターのネットワークにサイバー犯罪ツールやサービスを販売しています。これにより、犯罪サービスを専門化して販売できるようになります。これは合法的なビジネス界にそっくりです。サイバー攻撃によって利益を上げられる可能性が高まっていることを考えると、サイバー犯罪者がますます高度化しても不思議はありません。残念ながら、接続と新しいテクノロジーによって攻撃対象領域が拡大しているため、CaaS のトレンドは今後 1 年間で加速する可能性があります。特に、サービスとしてのランサムウェアが急増し、今後も組織や政府機関が標的になるのは確実です。一部の業界や政府のデータシステムはレガシーである性質があるため、RaaS の波は 2020 年も依然として高まり、収まりそうにありません。

AI ベースのテクノロジーが従業員を強化し、サイバーセキュリティを簡素化

多くの場合、AI 製品を取り巻く宣伝では現実での価値が誇張されています。しかし、最近の AI のイノベーションは、そこにトランスフォーメーションにつながる影響が垣間見えることを示しています。2020 年、企業が増加する一方のセキュリティコントロールの管理負担に疲弊しつつあることを受けて、AI は進化し続けます。複数のセキュリティ層があると、システムがより複雑になりますし、善意に基づいてはいるもののリスクの多い、従業員による回避策を招いてしまうことがよくあります。人的エラーのリスクを緩和するには、AI によってセキュリティプロトコルを簡素化し、ソーシャルエンジニアリング攻撃の影響を抑えます。時間と共に、AI 駆動型ソリューションは、人間の能力の欠陥を示すものではなく、人間ならではのスキルセットを強力に拡張するものであると認識されていくはずです。

顔認識を巡る議論において深い考察が再び求められる

顔認識に関する懸念が大きく報道されており、警察や他の政府機関が顔認識を使用することを禁止する法律を制定した都市もあります。このような全面的な禁止は、プライバシーに関してより広範な懸念が存在することの表れですが、このテクノロジーに関する議論において深い考察が欠けていることによって引き起こされる過剰反応の表れである場合もあります。よくあることですが、最悪の事態と最善の事態を事実として提示すると、その中間のどこかで現実が見つかる傾向があります。一部の専制国家では顔認識を自由に使用でき、実際に使用されていますが、より慎重な方法であれば民主国家でも自由に実装できます。AI や自動運転車といった過去の革新的テクノロジーと同じように、顔認識の社会的位置付けは、思慮深い開かれた対話を通じて決定する必要があります。

モバイルサイバーセキュリティが組織にとって大きな懸念に

BlackBerry Cylance が最近実施した調査から、国の支援を受けた APT グループが何の処罰も受けることなくモバイルデバイスを悪用して以下を監視していることがわかりました。

- 関心のある特定の人物
- 従来の国外情報
- 経済スパイのターゲット

弊社が観測した APT グループは、中国、北朝鮮、およびイランを含む場所を活動拠点にしています。これらの攻撃に対する一般認識が高まっているため、エンタープライズや政府はモバイル脅威の検知と対処に多額の投資を行うと予想されます。

まとめ

脅威アクターは、2019 年を通して新しい戦略や戦術を革新し続けました。その特筆すべき成果を 2 つ挙げると、ステガノグラフィ手法を使用した悪意のあるペイロードの難読化と、暗号化スキームの向上です。また、2019 年のランキング上位のサイバー脅威からわかるように、レガシーマルウェアファミリーを更新する取り組みも成果を上げています。MSP と MSSP を侵害することで、脅威アクターは、複数組織に対する攻撃を簡単に配布できるようになりました。この戦術は今後さらに注目を集める可能性があります。2018 年に衰退したランサムウェアも復活しました。

自動車、設備、アプライアンス、および他のデバイスの組み込みテクノロジーがビジネスシステムに接続するようになるにつれ、グローバルな攻撃対象領域が急拡大しています。また、インターネットに接続する IoT デバイスの増加により、ID アクセス管理はサイバーセキュリティ戦略において一層重要な役割を果たすようになります。トレーニングされた AI によって実現される継続的ユーザー認証を使用すると、メーカーがよりセキュリティの高い製品を設計するまで組織を自衛することができます。

APT と国の支援を受けた脅威グループが、モバイルセキュリティの脆弱性を悪用しています。これらの攻撃に対抗するには、MDM ベンダー、アプリケーションエンジニア、およびスマートフォンを脱獄／ルート化し続けているユーザーの真剣な取り組みが必要になります。モバイルセキュリティベンダーは、他の業界が犯した過ちから学ぶことによって、サイバーセキュリティの問題のいくつかを未然に防止できます。

ディープフェイクテクノロジーは、すぐに、詐欺を働く脅威アクターの標準ツールになる可能性があります。このテクノロジーはさらに入手しやすく、使いやすくなるため、ディープフェイク脅威の検知と対処についての従業員のトレーニングが必要になります。既にディープフェイク ID によるアイデンティティを使用してソーシャルメディアプロファイルが作成されていることを確認できるため、この種類の脅威はすぐにでも起こる可能性があります。

2019 年には、クラウドリソースを使用している企業数社がシステムの設定ミスによって数十億件のレコードを失いました。組織がクラウドセキュリティ担当者のトレーニングとサポートへの投資を増やさなければ、このトレンドは今後も確実に続きます。クラウド関連の侵害を減らすには、CSP とその顧客が責任共有モデルの各自の担当部分を理解、導入、実施する必要があります。

2020 年も、多数のサイバーセキュリティの脅威が組織とエンドユーザーを待ち構えています。自動車メーカーにできることは、サプライチェーンのセキュリティ向上と無線更新の実現に集中することです。モバイルテクノロジーと IoT の開発者にできることは、コーディング手法と脅威検知機能を向上させることです。ユーザーにできることは、IoT デバイスを接続する際、およびスマートフォンの脱獄／ルート化をやめることによって、セキュリティをより意識することです。

BlackBerry Cylance は、世界中の人々と組織のためにサイバーセキュリティの理想を発展させることに力を注いでいます。弊社は、テクノロジー、プロセス、ユーザー ID を保護するため、今後とも有効性を高めた高度な AI モデルをトレーニング、導入していきます。また、グローバルな脅威環境で新たな脅威を監視すると共に、問題が発生した場合はソリューションを提供するよう努めていきます。弊社の 2020 年以降の計画の詳細については、www.cylance.com をご覧ください。

謝辞

「BlackBerry Cylance 2020 脅威レポート」は弊社の有能なチームと個人による共同作業です。特に、以下の方々に感謝します。

Adam Martin
Alan McCarthy
Andrew Crowley
Anuj Soni
Bob Slocum
Chris Greco
Claudiu Teodorescu
Dan Ballmer
David Rushmer
Dean Given
Douglas Kraus
Ebudo Osime
Eoin Healy
Eric Milam
Evelyn Ho
Garret Grajek
Geoff O’Rourke
Grant Courville
Ieva Rutkovska
Jessica Vose
John McGinnis
John Wood
Lydia McElligott
Lyndon Levett
Marisa Goodrich
Marta Janus
Masaki Kasuya 糟谷正樹
Patrick Huskey
Ryan Tracey
Shinsuke Honjo 本城信輔
Steve Barnes
T.J O’Leary
Tatsuya Hasegawa 長谷川達也
Thom Ables
Tim Davies
Tom Bonner
William Savastano
Yi Zheng

法的免責条項

「BlackBerry Cylance 2020 脅威レポート」に記載されている情報は、教育のみを目的としたものです。BlackBerry Cylance は、本書で参照されている第三者による記述または調査について正確性、完全性、および信頼性を保証せず、責任も負いません。このレポートで表されている解析は、利用可能な情報に関する弊社調査アナリストの現在の理解を反映したものであり、追加の情報が明らかになった場合、変更されることがあります。読者は、この情報を個人の生活または業務に適用する場合、適切な注意を払う責任を持ちます。BlackBerry Cylance は、本レポートで提示されている情報の悪意のある使用または誤用を容認しません。

注

1 https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

2 https://www.zdnet.com/article/another-ransomware-strain-is-now-stealing-data-before-encrypting-it/

3 https://www.msspalert.com/cybersecurity-guests/sodinokibi-ransomware-still-very-relevant-for-mssps/

4 https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/

5 https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html

6 https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html

7 https://cyberarch.eu/red-teaming-adversary-simulation-toolkit/

8 https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html

9 https://threatvector.cylance.com/en_us/home/malicious-payloads-hiding-beneath-the-wav.html

10 https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/#47d3e708617f

11 https://threatvector.cylance.com/en_us/home/flirting-with-ida-and-apt28.html

12 https://threatvector.cylance.com/en_us/home/inside-the-apt28-dll-backdoor-blitz.html

13 https://www.forbes.com/sites/forbestechcouncil/2018/02/20/how-ai-driven-systems-can-be-hacked/#2515d07179df

14 https://enterprise.verizon.com/resources/reports/dbir/

15 https://www.cyentia.com/ransomware-p1-payment-rate/

16 https://www.pcworld.com/article/3225407/ccleaner-downloads-infected-malware.html

17 https://securityboulevard.com/2019/09/taking-health-care-out-of-the-ransomware-hot-seat/

18 https://www.cpomagazine.com/cyber-security/atm-malware-and-jackpotting-attacks-could-be-making-a-return/

19 https://www.wired.com/story/russian-hackers-attack-ukraine/

20 https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/

21 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0322

22 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507

23 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0563

24 https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

25 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

26 https://www.helpnetsecurity.com/2019/06/04/quest-diagnostics-data-breach/

27 https://geminiadvisory.io/amca-largest-medical-breach/

28 https://krebsonsecurity.com/2019/06/collections-firm-behind-labcorp-quest-breaches-files-for-bankruptcy/

29 https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

30 https://www.verdict.co.uk/gearbest-data-breach/

31 https://en.wikipedia.org/wiki/2019_Bulgarian_revenue_agency_hack

32 https://en.gizchina.it/2019/03/gearbest-security-breach-official-statement/

33 https://en.wikipedia.org/wiki/2019_Bulgarian_revenue_agency_hack

34 https://thenextweb.com/security/2019/07/16/bulgaria-tax-agency-data-leak-hack/

35 https://www.zdnet.com/article/rogue-iot-devices-are-putting-your-network-at-risk-from-hackers/

36 https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/

37 https://hackernoon.com/why-do-most-people-ignore-two-factor-authentication-1bbc49671b8e

38 https://www.secureworldexpo.com/industry-news/2019-sotp-credentials-and-data-loss

39 https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

40 https://stratcomcoe.org/role-deepfakes-malign-influence-campaigns

41 https://www.welivesecurity.com/2019/10/31/deepfakes-seeing-isnt-believing/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+eset/blog+(ESET+Blog:+We+Live+Security)

42 https://www.bbc.com/news/technology-49961089

43 https://blog.malwarebytes.com/social-engineering/2019/11/deepfakes-and-linkedin-malign-interference-campaigns/

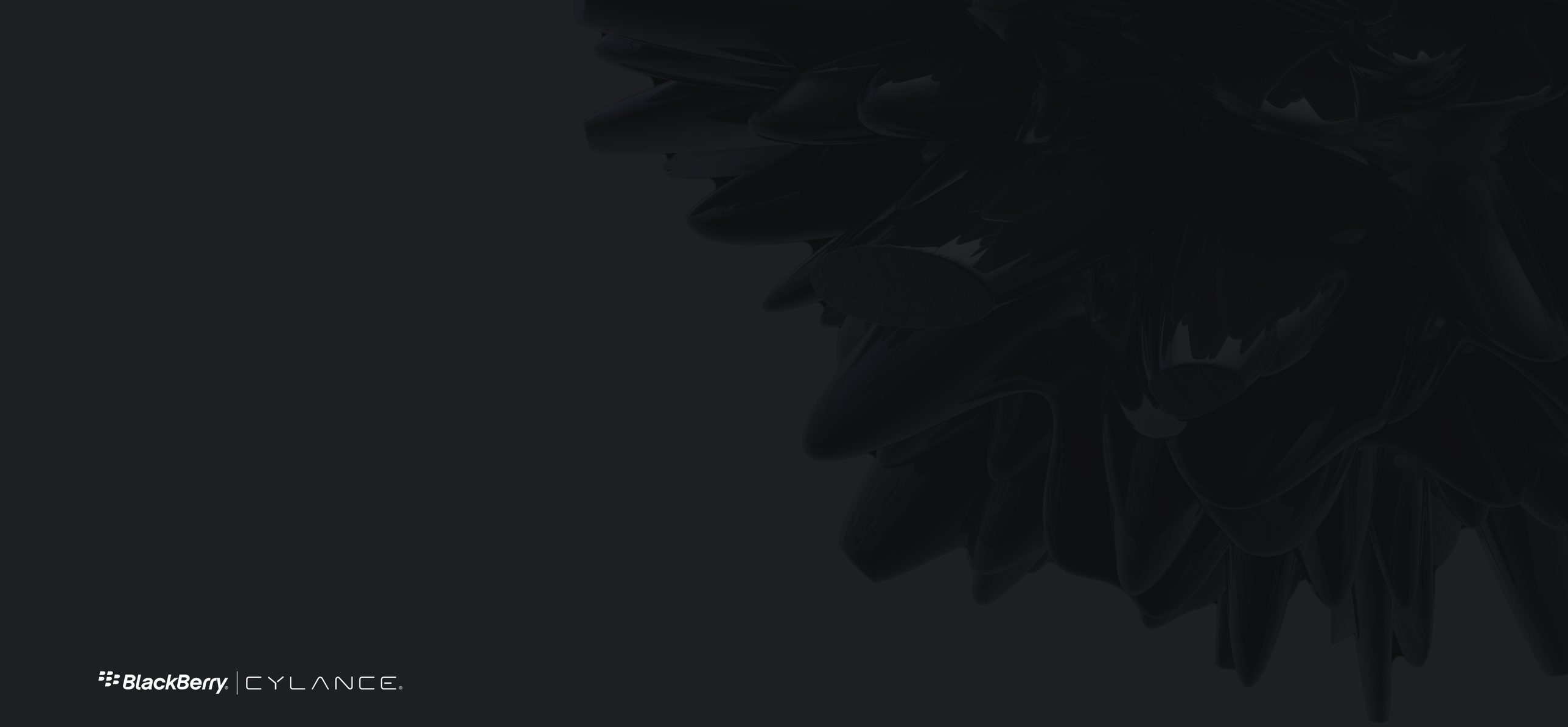
44 https://www.forbes.com/sites/forbestechcouncil/2019/07/05/how-to-prevent-security-breaches-resulting-from-cloudmisconfigurations/#34a085516c9e

45 https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

46 https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf

47 https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/

48 https://www.wmcactionnews5.com/story/39022826/used-cars-increase-identity-theft-chances-bbb-finds/



BlackBerry | CYLANCE

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 20-0049-20200211