

クライアント側への攻撃

DDOS攻撃

アプリのセキュリティを第一に考える

進化するリスク ランドスケープ

緊急の脅威への準備

WEBアプリへの攻撃

アプリ インフラストラクチャへの攻撃

概要

現在のデジタル市場において、アプリケーションはビジネスそのものです。

アプリケーションは、イノベーションを推進し、常時稼働、常時接続の時代の競争に負けないための原動力となります。アプリは、顧客との関係構築、従業員への権限譲渡、成長の促進など、さまざまなことを実現します。

クラウドの台頭により、大量の機密データを保持する新しいアプリが数十億と生産されています。これらのクラウドベースのアプリは、規模の大小に関係なくすべての企業に、ますます加速する市場で成功するために不可欠な俊敏性を与えます。しかし、同時に多くの複雑な問題および新しいリスクを引き起こしています。さらに、自動化ツールおよび豊富な専門的知識を利用できることから、脅威はますます増加し、ハッキングは営利目的のゲームへと変わりました。

そのため、アプリは生産性を向上し、イノベーションを加速する一方で、これまでになかった脅威をもたらし、リスク ランドスケープが拡大し、企業のデータと評判は危険にさらされています。

¹ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

22%

2016年～2017年で、WEBアプリケーションの攻撃は約22%増加しました。¹



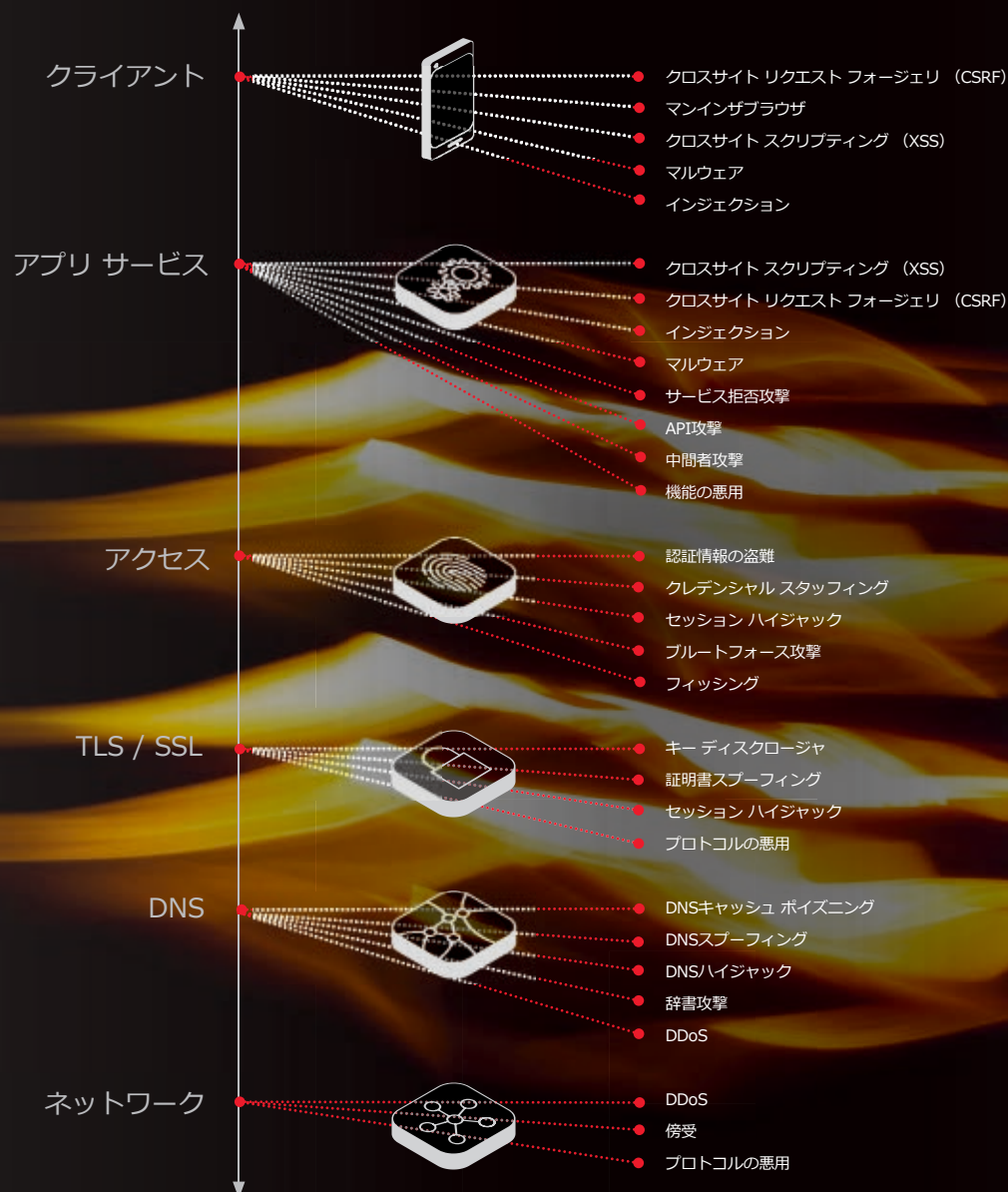
ビジネスの加速は、 アプリのセキュリティ

脅威と機会が複雑に入り組んだランドスケープでは、イノベーションとセキュリティをバランスよく実現することは勝者のない戦いのようなものです。しかし、これを変えることはできます。組織は、最も効果的にビジネスを保護するためにセキュリティ予算をどこに割り当てるかを考える必要があります。

まず、アプリケーション自体を理解し、特に脆弱な部分を特定することが重要です。組織は、アプリが使用するネットワーク、ユーザとアプリ間で送受信されるデータ、アプリ、Webおよびアプリケーション サーバにアクセスするためにIPアドレスを解決するDNS、他のアプリケーションおよびシステムにより利用される関連APIを考慮する必要があります。

脅威インテリジェンスを利用して、アプリケーションにとって現在最も重要な脅威、つまり、アプリが主要な標的となっているか、またはより大規模な攻撃（IoTボットネットなど）のための二次的要因となっているかを認識しておくことが重要です。新しい攻撃ベクトルおよび戦略を常に把握しておくことで、脅威ランドスケープの理解を深め、アプリおよび組織をより安全にするための実用的な情報を得ることができます。この知識に基づき、ビジネスに最適なソリューションを採用し、アプリの脆弱性へのすべての接点に対する脅威を保護でき、アプリおよびデータの機密性、完全性、可用性を向上できます。

アプリケーション脅威のランドスケープ



新たな脅威を 理解しこれに備える

WEB不正行為

Web不正行為は主に銀行業界と関係があります。実際、金融サービス企業は、その資産が最も際立つため、最も多くの攻撃を受けています。しかし、すべての業界の企業が、組織に年間数十億ドルの損害を与える多面的な脅威であるWeb不正行為のリスクにさらされています。この脅威では、犯罪者は、ボットを利用して、限定品の靴、人気イベントのチケット、さらに政府発行のビザなどの需要のある商品を取得し転売します。

- 電子商取引の不正行為は2016年で33%増加しました。²
- サイバー犯罪者は、銀行口座、ポイント プログラム（マイレージ サービス ポイントなど）、クレジット カード、および金銭目的に利用または販売できる医療記録などのその他の個人情報を狙っています。
- Web不正行為では、コンテンツ スクレイパがコンテンツを盗み再公開するため、オンライン情報の完全性にも影響を与えます。
- Web不正行為は、ビジネスのブランドおよび一般消費者の認知にも悪影響を及ぼします。製品の入荷時期や価格競争力により、顧客が競合会社に移る可能性があるためです。

解決策

Web不正行為の攻撃面を最小限に押さえるには、人間の努力と機械の力を組み合わせ、金融およびブラウザ内マルウェア、ゼロデイ不正行為、その他の不正オンライン活動を識別し対処する必要があります。

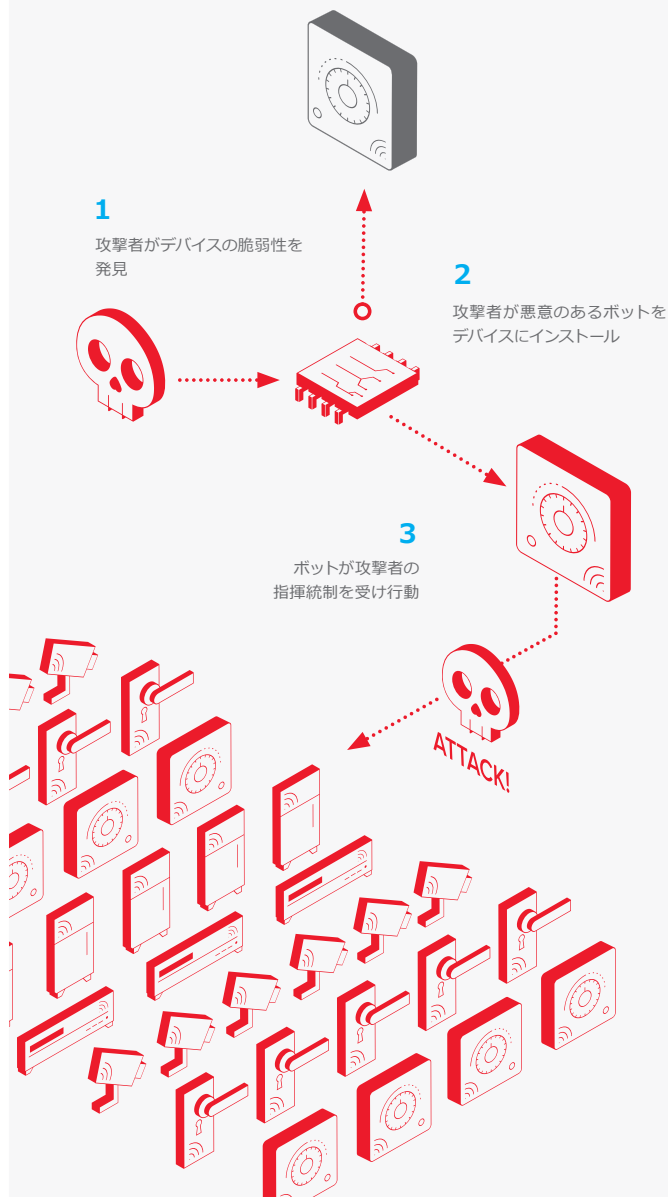
33%

電子商取引の不正行為は2016年に33%増加しました。

- 高度な識別技術を利用することで、組織は、たとえば、悪意のあるスクリプトの注入、自動転送の試行、攻撃者が犠牲者のコンピュータを乗っ取るリモート アクセスのトロイの木馬/マルウェアなどのマルウェア パターンを認識および理解できます。
- さまざまなデバイス固有および行動的変数を評価するだけでなく、人間のユーザと自動化スクリプトまたはボットを区別することで、マルウェアまたはボットによる自動支払いおよび自動送金を検知して防ぐことができる不正行為対策ソリューションを採用します。
- ボットが不正行為に使用されることはよくあるので、ボット対策および管理ソリューションを導入し、不正行為が関連する問題を防止および管理します。
- ビジネス プロセスの詳細な分析を検証します。これにより、金銭目的に利用される可能性がある弱点の領域を発見できます。

² <http://www.experian.com/blogs/insights/2017/03/e-commerce-fraud-rates-spike-in-2016/>

ボット軍の召集



ボット

2016年にソフトウェアおよび人間以外から発信されたオンライントラフィックは全体の半数以上でした。³ 正当なボットと悪質なボットの両方を含めたボットの台頭により、これまでのインターネットの性質が変わりました。悪名高いDDoS攻撃からMiraiボットネット⁴、Webスクレイピングボット、スパムボット、スクレイパボット、クレデンシャルスタッフィングボットまで、インターネットを乗取る自動化アプリケーションは悪評を得ています。どのようなボットでも正当なサイトにさまざまな影響を与えることができ、攻撃者の武器としてよく利用されているため、そのほとんどは当然の評価です。また、各業界で競合会社より安く売るために、ボットがビジネスインテリジェンス（価格データなど）の収集に使用されることもよくあります。

- 2016年、ボットネット活動はデータ漏洩の77%を占めていました。⁵
- スパム攻撃者は100,000台のIoTデバイスを利用して、100万通の電子メールの75%を送信しました。⁶
- 暗号通貨マイニングIoTワームが4か月で30,000台以上のコンピュータおよびデバイスに不正アクセスしました。⁷

しかし、すべてのボットが、悪質なボットというわけではありません。パーソナル デジタル アシスタント、Webのインデックスを作成するスパイダーボット、盗作を見つけ出す著作権管理ボットなど、正当なユーザにより、または正当な目的で使用するボットもたくさんあります。インターネットでのボットの領域がますます拡大しているため、組織は、悪質なボットを識別、分類および対処できる強力なメカニズムを開発および導入しなければなりません。しかし、そのためには、正当な理由でのボットの活動をサポートできる、または少なくとも妨害しない、インテリジェンス、コンテキストおよび関係が必要となります。

³ <https://www.recode.net/2017/5/31/15720396/internet-traffic-bots-surpass-human-2016-mary-meeker-code-conference>

⁴ <https://f5.com/labs/articles/threat-intelligence/ddos/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-attack-on-ovh-22422>

⁵ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

解決策

インターネット上の悪意のあるボットから組織を守るには、疑わしい自動化活動を識別、検知されたボットを分類、高精度で攻撃を軽減できる最新のプロアクティブなボット検知機能が必要です。

- 動的にポリシーを適応させ、プロアクティブにボットを見つけることができる、高度にプログラムが可能なトラフィック管理を採用し、プロセスを最適化して、セキュリティチームの時間を最大限活用します。
- 常時稼働の防御で自動化DoS攻撃、Webスクレイピング、およびブルートフォース攻撃が発生する前に防ぎます。
- 高度な防御方法（JSおよびCAPTCHAチャレンジなど）およびレピュテーションマッチングを使用して、人間以外のユーザを特定します。
- IPインテリジェンスなどの脅威インテリジェンスフィードを利用できるシステムをインストールし、L3のボットホストエンドポイントを自動的にブロックします。
- Webアプリケーションに潜在的な脆弱性がないか検査します。
- 多要素認証を使用して、ボットによるアプリケーションおよびネットワークへの不正アクセスを難しくします。
- Webアプリケーションに保存される個人情報の量を制限し、リスクを最小限に押さえます。
- 実用的な脅威インテリジェンスを実施し、特定の脅威アクターまたは攻撃行動の標的になる可能性を判断します。

⁶ <http://www.dailytech.com/Hackers+Use+Refrigerator+Other+Devices+to+Send+750000+Spam+Emails+/article34161.htm>

⁷ <https://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency>

クレデンシャル スタッフィング

クレデンシャル スタッフィング攻撃では、サイバー犯罪者は、盗んだログイン ユーザ名およびパスワードを利用して、企業ユーザまたは顧客が保持するアカウントへのアクセスを取得しようと繰り返し試みます。データ漏洩件数が毎年増加する中、ますます多くの認証情報が流出しています。ユーザ名とパスワードの平均セットは、盗んだクレジット カード番号より17倍以上高く売れるため、認証情報の盗難は急成長のビジネスとなっています。⁸クレデンシャル スタッフィングは概して一般消費者側の問題ですが、複数のアカウントでパスワードを使い回している場合は、企業のアカウントもリスクにさらされます。

- 2017年上半年、2,227件のデータ漏洩事件が報告され、60億件のレコードが漏洩しました。⁹
- 4人中3人のユーザは、複数のアカウントで認証情報を再利用および使い回しています。¹⁰
- 顧客から盗んだ認証情報は、Webアプリケーション不正アクセスするための一般的な方法として使用されます。¹¹

結論からすると、組織のセキュリティがどんなに強力であっても、ユーザまたは顧客がパスワードを再利用していれば、それらの認証情報がすでに盗まれ、ダーク ウェブで売られている可能性は高いです。

解決策

クレデンシャル スタッフィング問題を確実に解決できる方法はありませんが、従業員/ユーザをトレーニングしながら独自の防御を強化すれば、組織を保護できます。

- トレーニングや教育によりフィッシングに関するセキュリティ意識を高めることで、ユーザが自らを認証情報盗難から守ることができるように支援します。
- Webアプリケーション ファイアウォールにより高度なボット検知および対策機能を提供できます。これは、ほとんどのクレデンシャル スタッフィング攻撃で自動化プログラムが利用されているため重要です。
- 攻撃者のボットが正しいフィールドを認識して、盗んだ認証情報を挿入できないように、動的フォーム難読化を使用してサイトのログイン フォームを設計します。
- ユーザから転送される情報を保護して、データが傍受されてもその価値がなくなるように、ブラウザまたはモバイル アプリのデータを暗号化します。
- アクセス ゲートウェイを一元化しシングル サインオン (SSO) およびリスクベースの多要素認証を使用してリスクを軽減します。
- ユーザの認証を統合して責任を最小限に押さえます。認証統合には、ユーザが別のパスワードを管理しなくて済むというメリットもあります。
- 失敗した認証を監視し、そのソースを分類して、悪意のあるエンドポイントを識別およびブロックしやすくします。

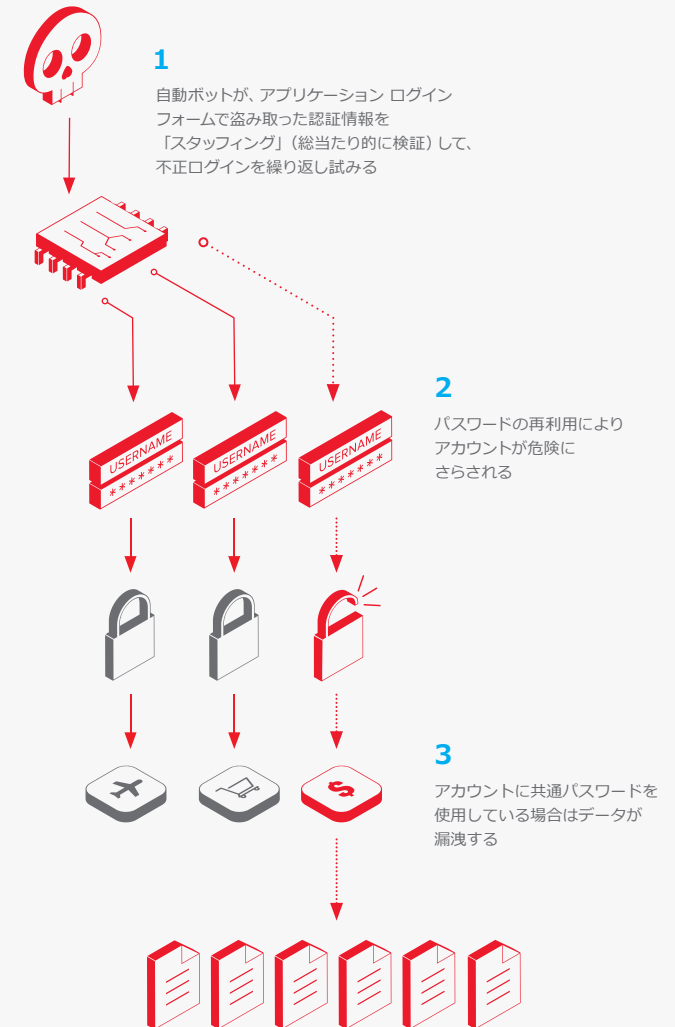
⁸ <http://www.darkreading.com/endpoint/anatomy-of-an-account-take-over-attack/a/d-id/1324409>

⁹ <http://www.securityweek.com/2227-breaches-exposed-6-billion-records-first-half-2017-report>

¹⁰ <https://www.entrepreneur.com/article/246902>

¹¹ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

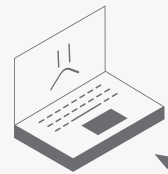
クレデンシャル スタッフィング 攻撃の概要



マルウェアの例

1

マルウェアに感染したユーザがブラウザを開く。マルウェアは、認証情報を盗むサイトとして、そのURLを認識する



2

マルウェアが、トランザクションを監視またはWEBコンテンツを改竄できる悪意のあるJAVASCRIPTを注入する



本来の接続



3

注入されたスクリプトが、ログイン、セッション認証情報およびその他の機密情報を収集して、攻撃者に送信する

マルウェア

トロイの木馬からウイルス、アドウェア、ルートキットまで、マルウェアは至るところに存在します。Web不正行為、認証情報盗難、およびDDoS攻撃を実行するボットネットの構築など、マルウェアはあらゆる場所で利用されています。マルウェアの種類は信じられないくらい多くありますが、これらすべてが、財務利益、デバイスのボットネットへの追加、スパムの増殖または口座乗っ取りなど、攻撃者の最終目標を促進するように設計されています。マルウェアの管理リンクの鍵となるのは、業界固有のリスク特性、および一般的な脅威アクターが利用するマルウェアの種類を理解することです。

- 2017年第一四半期で、新種のマルウェアが4.2秒ごとに発生しました。¹²
- 2016年に発生した全データ漏洩事件の半分以上（51%）にマルウェアがなんらかの形で関与していました。¹³

解決策

アンチウイルス プログラムやブラックリスト ソフトウェア パッケージなどの従来のマルウェア ソリューションでは、急増するトロイの木馬、スパイウェア、アドウェアなどに効果的に対応できなくなっています。組織をマルウェアから最適に保護するには、行動分析と脅威インテリジェンスを組み合わせる利用することが重要です。

- アプリケーション ホワイトリストにより、マルウェアが実行されないように防ぎます。
- 行動分析によりソフトウェアを評価し、ファイル シグネチャだけでなく、ソフトウェアの行動を検証します。
- 隔離した実行環境で添付ファイルまたはリンクを開くサンドボックスを利用して、ユーザのシステムおよびネットワークを保護します。

66%

マルウェアの66%は悪意のある電子メール添付ファイルを介してインストールされています。¹⁴

- ほとんどのユーザがソフトウェアをインストールできないように権限を制限します。これにより、IT部門への負担は増えますが、マルウェアの蔓延を最小限に押さえることができます。
- ユーザが詐欺行為を見抜き、正当なサイトおよびサービスと、マルウェアの侵食を促進するためのサイトおよびサービスを区別できるように支援します。
- ネットワークへのリスクを高めずにユーザの業務を効率化できる、品質が証明されたソフトウェアを集めた、使いやすいライブラリを作成します。

¹² <https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017>

¹³ <https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017>

¹⁴ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

ランサムウェア

ランサムウェアは、マルウェアの一種で、スクリーンをロックまたはファイルを暗号化することで、ユーザがその所有するデータやコンピュータにアクセスできないようにします。ランサムウェアはここ数年で、特に行政機関、医療および金融業界でますます増加しています。

実際、ランサムウェアは、2014年版『Verizon Data Breach Investigations Report』において、最も頻出するマルウェアリストで22位でしたが、2016年版では5位まで浮上しました。¹⁵攻撃者は、ユーザをロックする、またはそのシステムの特定のファイルを暗号化することで、被害者から身代金を要求しようとします。

- ランサムウェアは特にダウンロードやフィッシング行為を利用してシステムに不正アクセスしようとします。
- ここ数年、攻撃者は、収益増加を狙い、一般消費者に加え、脆弱な組織を標的にし始めています。¹⁶
- サイバー犯罪者は、サービスとしてのランサムウェア（Ransomware as a Service）を提供し、ユーザまたは組織から得た金額の一部の分け前を得ています。¹⁷
- 最近の研究では、ランサムウェアは従来のアンチウイルスを100%回避しています。¹⁸

解決策

ランサムウェア攻撃の早期検知と脅威インテリジェンスを組み合わせることで、サイバー犯罪者の行動を監視できます。

- エンドポイント保護システムを使用して、一般的なランサムウェア サンプルを検知し、ネットワークに影響を及ぼす前にブロックします。
- ランサムウェアがシステムに侵入する主な手口の1つである、フィッシング行為についてユーザを教育します。

- アプリケーション ホワイトリストにより、システムが不明なアプリケーションをインストールまたは実行できないようにします。
- 脅威インテリジェンスを共有して、ランサムウェアの蔓延を防ぎます。

¹⁵ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

¹⁶ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

¹⁷ <https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#2f19d94e4123>

¹⁸ <https://www.infosecurity-magazine.com/news/antivirus-fails-to-stop-ransomware/>

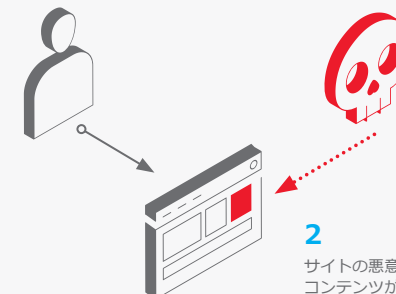
100%

最近の研究では、ランサムウェアは従来のアンチウイルスを100%回避しています。



ランサムウェアによるデータのロック

1 ユーザがサイトにアクセスする



2 サイトの悪意のあるコンテンツがマルウェアダウンロードをトリガする

3 マルウェアがバックグラウンドでファイルを暗号化する



4 データがロックされる
システムのロックを解除するために身代金が要求される

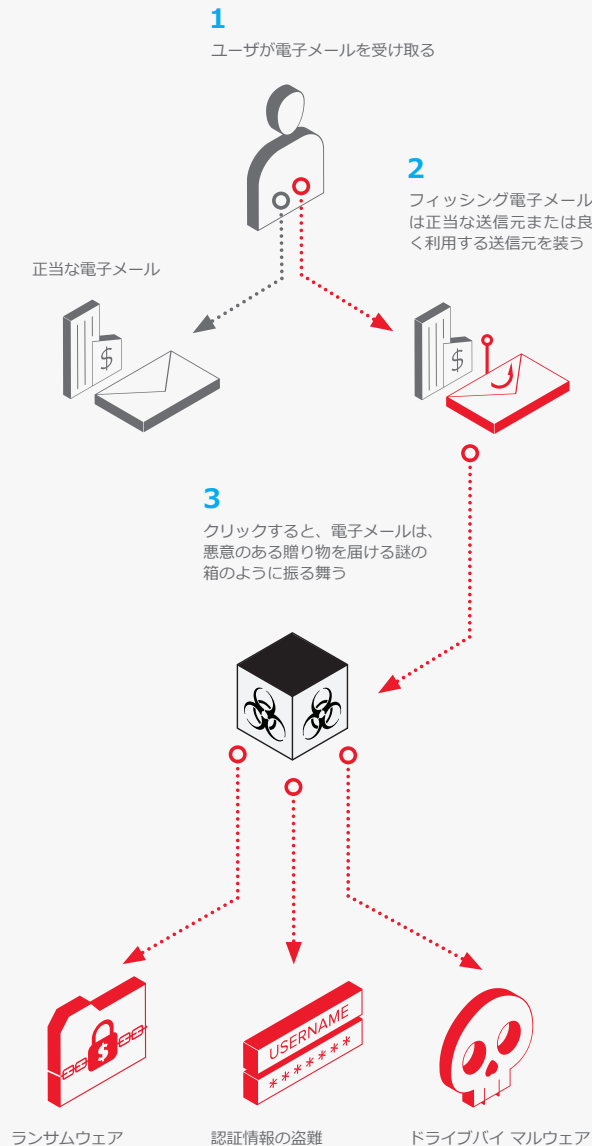


データがロックされたままになるか、消去される



身代金が支払われると、データのロックが解除される場合もあるが、されない場合もある

フィッシング攻撃



フィッシング

他の多くの脅威と同様、フィッシングは一括りにすることが難しく、他の目的に利用されることがよくあります。攻撃者は、フィッシング詐欺を利用し、ユーザを騙してシステムにマルウェアを感染させるリンクをクリックさせる、または個人情報盗むためのフェイクWebサイトにユーザを誘導します。

フィッシングにより、サイバー犯罪は、ユーザのアカウントを乗取り、機密データへのアクセス権を取得して、金銭やマイレージ サービス ポイントなどのその他の貴重品を盗むことができます。また、ユーザを騙して、企業ネットワークへのバックドアとなる指揮統制マルウェアをシステムにインストールさせることも、フィッシングでよくみられます。

- フィッシングは、ランサムウェアやその他のマルウェアの主な配信メカニズムです。¹⁹
- フィッシング攻撃の影響を受けない業界はありません。フィッシング リンクをクリックしてしまうユーザの割合はどの業界でもほぼ同じです。²⁰
- フィッシング攻撃の増加は、APT攻撃（ターゲット型攻撃）の前兆である可能性もあります。実用的な脅威インテリジェンスは、一見小さいと思える問題を見つけ、それをより大規模またはより長期的な攻撃と関連付ける上で役に立ちます。

疑わしい電子メールを報告、またはフィッシング リンクをクリックしてしまった場合に組織に通知するようにユーザを促します。

解決策

フィッシング攻撃を確実に防止できる解決策はないので、組織は、フィッシング電子メールを見分ける方法、および誤ってクリックしてしまった場合の対処法についてユーザを教育する、そして教育し続ける必要があります。

- 従業員および契約者が新しいフィッシング攻撃を常に把握できるように、セキュリティ意識を高める訓練を実施します。
- ユーザがフィッシング電子メールのマルウェア リンクをクリックした、または認証情報を誤って流出したことに気付いたらすぐにIT部門に簡単に報告できるようにポリシーを定めます。
- 強力なエンドポイント保護メカニズムによりマルウェアを検知し見分けます。
- 疑わしい電子メールがあれば報告するようにユーザを促します。
- ユーザがフィッシング リンクをクリックしてしまった場合に組織に通知できるように簡単なプロセスを構築します。
- 脅威インテリジェンスを使用して、フィッシングによりシステム侵入を試みるAPT攻撃の標的に企業がなっている可能性を計算します。

¹⁹ <https://blog.barkly.com/phishing-statistics-2016>

²⁰ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>


新しい脆弱性 新しい機会

急劇に変化する現在のアプリ中心の世界では、複雑であることが当然です。サイロ化された脅威をポイント ソリューションで軽減できたのは遠い昔のことです。アプリケーションは全体論的なので、アプリケーションを保護するには全体論的な手法が必要です。

アプリはデータセンタ、プライベート クラウド、パブリッククラウド、コンテナ、SaaSプラットフォームなどあらゆる場所から提供されるため、セキュリティの総合型の手法を採用することは、インフラストラクチャ、アプリケーションおよびデータを保護する上で重要です。

現在と将来の脅威を慎重に検討し、脅威インテリジェンスを利用および共有して、予算要件に合ったソリューションを採用することで、現在と将来の両方において組織を成功に導き、安全にする包括的なセキュリティ プログラムを構築できます。

組織に影響を与える脅威、およびそれらの対策の詳細については、f5.com/securityをご覧ください。



アプリケーションは
全体論的であり、それらを
保護するには全体論的な
手法が必要です。

アプリのセキュリティを第一に考える

常時稼働、常時接続のアプリは、ビジネスを強化および変革する一方、ファイアウォールに保護されないデータへのゲートウェイにもなり得ます。ほとんどの攻撃はアプリ レベルで発生しているため、ビジネスを推進する機能を保護することは、攻撃を受けるアプリを保護することにつながります。



F5 ネットワークスジャパン合同会社

東京本社

〒107-0052 東京都港区赤坂 4-15-1 赤坂ガーデンシティ 19 階
TEL 03-5114-3210 FAX 03-5114-3201

お問い合わせ先：<https://f5.com/jp/fc/>

西日本支社

〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838