

ユーザ名/パスワード

ユーザ名/パスワード

アプリのセキュリティを第一に考える

クレデンシャル スタッフィング

セキュリティの蔓延

ユーザ名/パスワード

ユーザ名/パスワード

ユーザ名/パスワード

概要

2016年の情報漏洩は、2013年の11億件を塗り替え、42億以上¹という新記録を樹立しました。しかし、2016年も最悪でしたが、2017年はさらに最悪になりそうです。2017年上半期、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、膨大な数のアカウントが危険にさらされました。² これらの盗まれた全レコードのほとんどにはユーザ名とパスワードが含まれていて、『2017 Verizon Data Breach Investigations Report』

³ によると、これらはハッキングに関連するデータ漏洩の81%で利用されています。アプリケーションおよびデータの完全性に対する不安がますます高まる中、組織はそのセキュリティ戦略でIDの保護を優先しなければなりません。実際、ユーザIDを保護し、重要なビジネス アプリケーションへのユーザ アクセスのレベルを管理することは、2017年に組織が直面している最大のセキュリティ問題とも言えます。

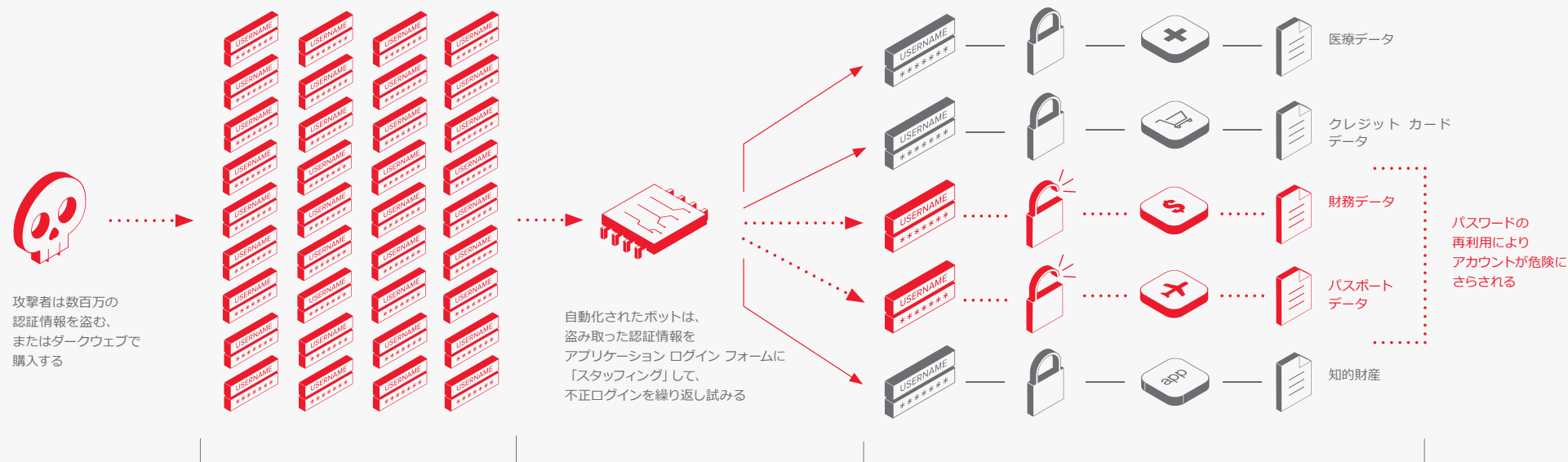
¹ <https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf>

² <https://pages.riskbasedsecurity.com/hubfs/Reports/2017%20MidYear%20Data%20Breach%20QuickView%20Report.pdf>

³ <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

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、盗んだ認証情報を利用して、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。



71 億件以上

過去8年間の情報漏洩事件で71億件のIDが流出しています。

10-20k

一般的な成功率は1~2%です。つまり、サイバー犯罪者は、盗まれた認証情報レコードを100万件購入すると、ボットを利用して10,000~20,000件のアカウントにアクセスできます。



3/4

4分の3のユーザはアカウントの認証情報を
再利用および使い回しています。

クレデンシャル スタッフィングの問題

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、過去に盗まれたユーザ名およびパスワードをダークウェブから購入します。次に、自動化ツールにより他のWebサイトのログイン フィールドでこれらの認証情報を「スタッフィング」(総当たりに検証)することで、不正ログインを繰り返し試み、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権を取得しようとします。「スタッフィング」が成功した場合、攻撃者は、アカウントを詐欺に利用します。この成功率は一般的に1~2%です。つまり、サイバー犯罪者が、盗まれた認証情報(ダークウェブで1件わずか1セントで販売⁴)を100万件購入した場合、10,000~20,00件のアカウントを取得できます。

2016年、全体の約17%のユーザが アカウントのパスワードに 「123456」を使用

アクセスするサイトまたはアプリケーションごとに異なるユーザ名とパスワードを使用していればこれらの攻撃は失敗していました。しかし、約4分の3のユーザは、使用するたくさんのアカウントのそれぞれで一意的な認証情報を作る時間と手間を惜しみ、同じ認証情報を再利用および使い回しています。⁵

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、恐らく実際にそうしているように、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てい

る可能性が高いのが現実です。認証情報の盗難が急増し、サイバー犯罪者が手軽に自動化ツールを使用してユーザ アカウントを取得できるため、組織がアプリケーションおよびデータのセキュリティを懸念することは当然です。

問題は、これらの攻撃をどのように防ぐか、または少なくとも軽減できるかです。

⁴ https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?_r=0

⁵ <https://www.entrepreneur.com/article/246902>

認証情報の盗難防止の手引き

まずは悪い情報ですが、スイッチ1つでクレデンシャル スタッフィング攻撃から組織を守ることはできません。しかし、成功した攻撃の犠牲者となる可能性を劇的に軽減する方法はたくさんあります。ユーザにはより安全なパスワード利用を心掛けるよう指導し、企業側ではセキュリティを強化します。

人とポリシー： トレーニング、報告、改善

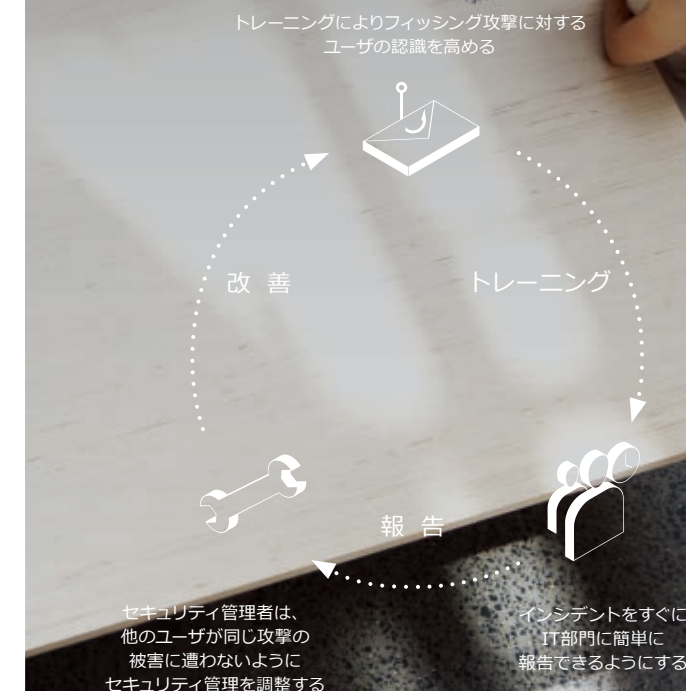
過去に盗まれた認証情報を取得および利用するほか、フィッシングも、サイバー犯罪者がクレデンシャル スタッフィングに使用するための認証情報を盗むときによく利用される方法です。フィッシングへの意識を高めるには、従業員をトレーニングおよび教育することです。しかし、これでもフィッシング攻撃が成功する可能性を完全になくすことはできませんが、サイバー犯罪者の手口をしっかりと理解しておくことで、ユーザは自身と組織をより効果的に守ることができます。

ユーザがフィッシング攻撃に気付けるようにするトレーニングから始めます。独自のテストを構築するか、無料のオンライン テストを利用できます。⁶パスワード管理に関するベスト プラクティスをユーザに提供することもできます。従業員にとって最も重要なことは、企業ネットワークのログイン認証情報をサードパーティ サイトで使用しないことです。その理由は、そのサイトのデータが漏洩した場合、サイバー犯罪者は、企業ネットワークおよびその中のアプリケーションにアクセスできるためです。従業員が他のサイトで企業の認証情報を使用したことがわかった場合、その認証情報をすぐに変える必要があります。また、一部のユーザがパスワードを再利用することを想定し、Yahoo!やLinkedInなどの大規模なデータ漏洩が発生した場合は、すべてのユーザのパスワードを設定し直すことをお勧めします。

どのようなトレーニングを実施しても、誰も間違いを犯すため、認証情報の盗難の可能性は完全にはなくならないということを覚えておいてください。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。IT部門がすぐに報告を受ければ、セキュリティ管理者は、システムをクリーンアップ、パスワードをリセット、他の従業員に詐欺事件を警告、そして最も重要なことですが、他のユーザが同じ攻撃の被害に遭わないように企業のセキュリティ管理を調整できます。

⁶ <http://resources.infosecinstitute.com/top-9-free-phishing-simulators/>

IT 部門がすぐにインシデントの報告を受ければ、他のユーザが同じ攻撃の被害に遭わないように、企業のセキュリティ管理を調整できます。



テクノロジー：さまざまな使用事例、さまざまな防御

クレデンシャル スタッフィング攻撃を防ぐためのアプリケーション セキュリティ戦略を作成する場合、2種類のユーザに対応する必要があります。企業従業員は、多要素認証 (MFA) などの面倒なプロセスでも進んで受け入れる、または少なくともこれに従います。しかし、電子商取引または小売業の顧客は、ログインプロセスが複雑になることを受け入れたがりません。これらの献身的な従業員と一時的なユーザの両方を守る方法があります。

安全性と暗号化

強力なWebアプリケーション ファイアウォール (WAF) は、クレデンシャル スタッフィング攻撃に対する最初の対策です。フル装備の最新WAFは高度なボット検知および対策機能を提供でき、ほとんどの攻撃で自動化プログラムが利用されているた

めこれは重要です。WAFは、IPロケーション、日時、および1秒あたりの接続試行数などの行動を分析できるので、セキュリティチームがブラウザ以外によるログイン試行を特定する上で役に立ちます。さらに、シグニチャ マッチングを使用することで、悪意のないボット (検索エンジン ボットなど) がサイトにアクセスできるように、ホワइटリストを簡単に作成できます。

WAFは、漏洩が報告された認証情報のリストとユーザ名およびパスワードを照合することで、盗まれた情報がログイン試行に使用されているかどうか検知することもできます。また、WAFを使用することで、セキュリティ チームは、一定時間内に複数回失敗したログインを追跡することで、潜在的なクレデンシャル スタッフィング攻撃を監視できます。プロアクティブな防御として、一定秒数以内の一定回数以上のログイン試行を防ぐようにWAFを設定することで、攻撃の速度を押さえ、セキュリティを調


整するまでの時間を稼ぐことができます。

攻撃面を軽減するための別の方法として、ジオインテリジェンスを使用して、既知の不正IPアドレスまたは地理的地域からの接続を除外します。また、攻撃者を特定したら、不正IPアドレスおよびデバイスのフィンガープリントを脅威フィードに追加して、その活動のブロックまたは検知に利用できる他のセキュリティ ソリューションと統合することもお勧めします。しかし、多くのボット オペレータはIPアドレスを頻繁に変えるため、この効果は一時的であることに注意してください。

WAFによる保護

フル装備の最新WAFは高度なボット検知および対策機能を提供でき、ほとんどの攻撃で自動化プログラムが利用されているためこれは重要です。





ユーザの身元証明のために静的パスワード以外の提供が要求される場合、クレデンシャル スタッフィング攻撃は失敗します。

動的なフォームの難読化ツールを利用することで、サイトのログイン フォームを攻撃者から見つかりづらくできます。動的なフィールドの難読化は、入力フィールドの名前に、「passwd」や「usrnme」などの内容を特定できるラベルではなく、頻繁に変わる特定しづらい長い文字列が使用されます。これにより、攻撃者のボットは正しいフィールドを認識して、盗んだ認証情報を利用できなくなります。

最後に、ブラウザまたはモバイル アプリケーションのデータを暗号化して、ユーザから転送されるすべての情報を保護して、傍受されたデータの価値をなくすこともできます。さらなるセキュリティ強化として、クライアント側の機能を使用してフォーム パラメータを暗号化できます。これにより、自動化クレデンシャル スタッフィング ツールがページを正しく実行して、フォーム フィールドを暗号化し、正しい安全なチャンネルcookieを送信することが難しくなります。暗号化されていない認証情報がボットにより送信されると、システム アラートがトリガされ、クレデンシャル スタッフィング攻撃が発生している可能性があることをセキュリティチームに通知できます。

認可の管理

WAFは、クレデンシャル スタッフィング攻撃を防御するだけでなく、OAuth (Open Authorization) と呼ばれるトークンベースの認可を実装することで、アプリケーションの攻撃面を大幅に削減できます。これにより、ユーザは、認証情報をアプリケーション自体に提供することなく、アプリケーションにアクセスできます。ユーザがFacebook、Google、Microsoft Azureまたは独自の認可サーバなどのサイトで認証によりIDを確立すると、ユーザが接続しようとしているアプリケーションに、ワンタイムの一時的なアクセス

トークンが発行されます。アプリケーションにはこれ以外の認証情報は必要ないので、ユーザにとって便利です。また、信頼できるソースまたは「認可サーバ」は、安全な認証を保証し、クレデンシャル スタッフィング攻撃の効果を劇的に軽減します。

トークンベースの認可は、APIをクレデンシャル スタッフィング攻撃から守る上でも優れたソリューションです。APIは、プログラムの（ソフトウェアからソフトウェア）にアクセスすることを目的として設計されているため、このような攻撃の第一の標的となります。そのため、認可をOAuthサーバに分割することがさらに重要になります。OAuthを介したAPIへのアクセスにより、アプリケーション開発者はアプリケーションへのログイン認証情報をハードコーディングする必要がなくなり、APIのセキュリティが向上します。これ以外のメリットとして、トークンを設定して、フルアクセスやアクセス拒否だけでなく、さまざまなレベルのアクセス権を提供できます。

ほとんどの組織は、いくつかのアプリケーションでその独自のユーザ ログインまたはAPIを使用しています。また、OAuth自体が安全というわけではないので、脆弱な方法でこれを実装してしまうというリスクがあります。

しかし、OAuth認可をアプリケーションに戻すことができる中央アクセス ゲートウェイにより、アプリケーション、ネットワーク リソースおよびAPIへのアクセスすべてを一元管理することでリスクを軽減できます。これにより、すべてのアクセス決定の一元管理が可能になり、危険なOAuth実装のリスクを軽減し、認可フレームワークの構築に費やしていた貴重な設計時間を節約できます。

この他にも、特に企業従業員に対して、安全なアクセスゲートウェイを実装できるというセキュリティ上のメリット

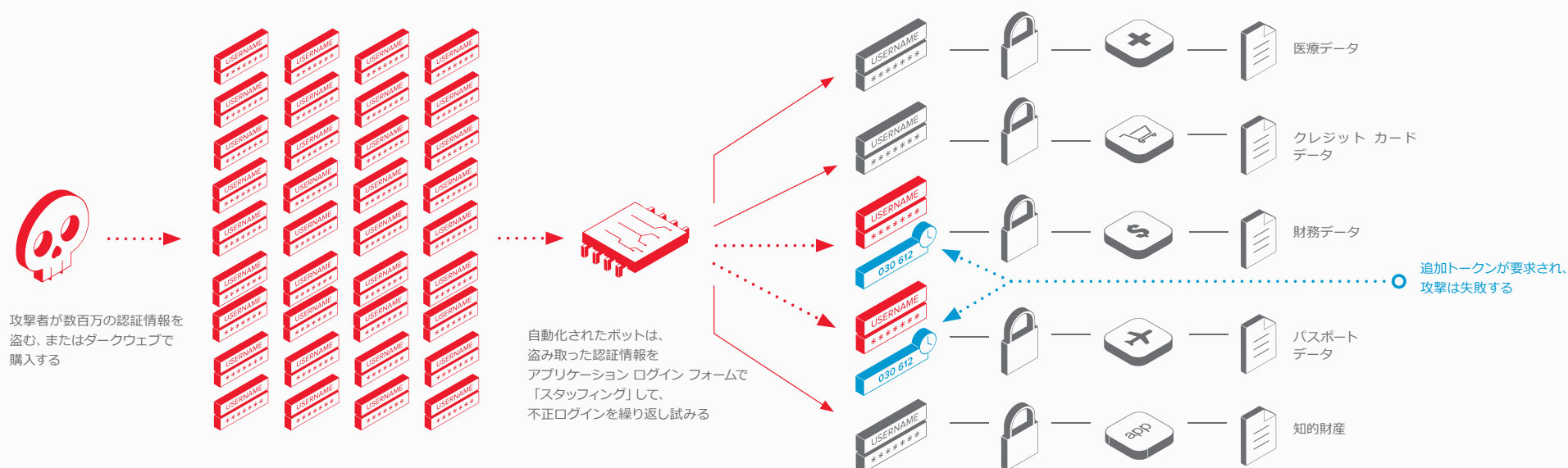
があります。すべての認証およびアクセス リクエストを1つの高性能ゲートウェイに集めることで、一貫した体験をユーザに提供でき、これにより、ユーザがフィッシング攻撃の被害に遭う可能性を軽減できます。このゲートウェイとともに、シングル サインオンおよびリスクベースのMFAは、IDセキュリティ ソリューションの重要な要素です。すべての認証およびアクセス リクエスト

は、中央アクセス ゲートウェイを介しますが、すべてのリクエストが同じというわけではありません。認証問題およびアクセス決定は、ユーザのロール、デバイス、地理的地域、日時、およびアプリケーション内のデータの機密性など、多くのリスク要因により異なる可能性があります。高リスクの要因が含まれる場合、ゲートウェイは、第二第三の要因でそのユーザの身元を確認

してからアクセス権を付与します。ユーザの身元証明のために静的パスワード以外の提供が要求される場合、クレデンシャル スタッフィング攻撃は失敗します。

多要素認証

クレデンシャル スタッフィング攻撃を防ぐために、ユーザの身元証明のために静的パスワード以外の提供を要求します。



IDのセキュリティ = 組織のセキュリティ

IDはサイバー犯罪者の第一の標的となるため、組織は、IDおよびアクセスのセキュリティがアプリケーションおよびデータの完全性を保証する上で重要だと理解する必要があります。ユーザのトレーニング、強力で一貫した企業ポリシー、信頼できるWebアプリケーション ファイアウォール、および一元化した認証認可ゲートウェイを組み合わせることで、組織は、現在のますます強力かつ執拗になるクレデンシャル スタッフィング攻撃を防止、または少なくとも軽減できます。

アプリケーション保護の詳細については、f5.com/securityをご覧ください。

包括的なセキュリティ手法は、現在の強力かつ執拗なクレデンシャル スタッフィング攻撃を防止、または少なくとも軽減できます。



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