SHAPE
Part of F5

攻撃者の経済学

サイバー攻撃の裏にある経済学を理解する：
あなたの会社が標的となる理由とは

概要

世界中の企業で自動化された攻撃が急増しています。これらの攻撃を仕掛けるための費用と投資額が大幅に低減されていることで、企業は、アカウント乗っ取りや不正行為につながるクレデンシャルスタッフィング攻撃の被害に遭うことが増えています。

これらの攻撃に必要な材料である、ダークウェブ上で見つけられる以前に侵害された消費者の認証情報、攻撃をオーケストレートするツール、および攻撃を実行するためのボットネットについては、購入やレンタルの費用さえも安くなってきています。その結果、クレデンシャルスタッフィング攻撃が成功すると、攻撃者は高額な報酬を得ることができます。このような攻撃を開始するかどうかは、攻撃者側に有利なことが容易にわかる単純な費用対効果の分析に基づき決定されます。

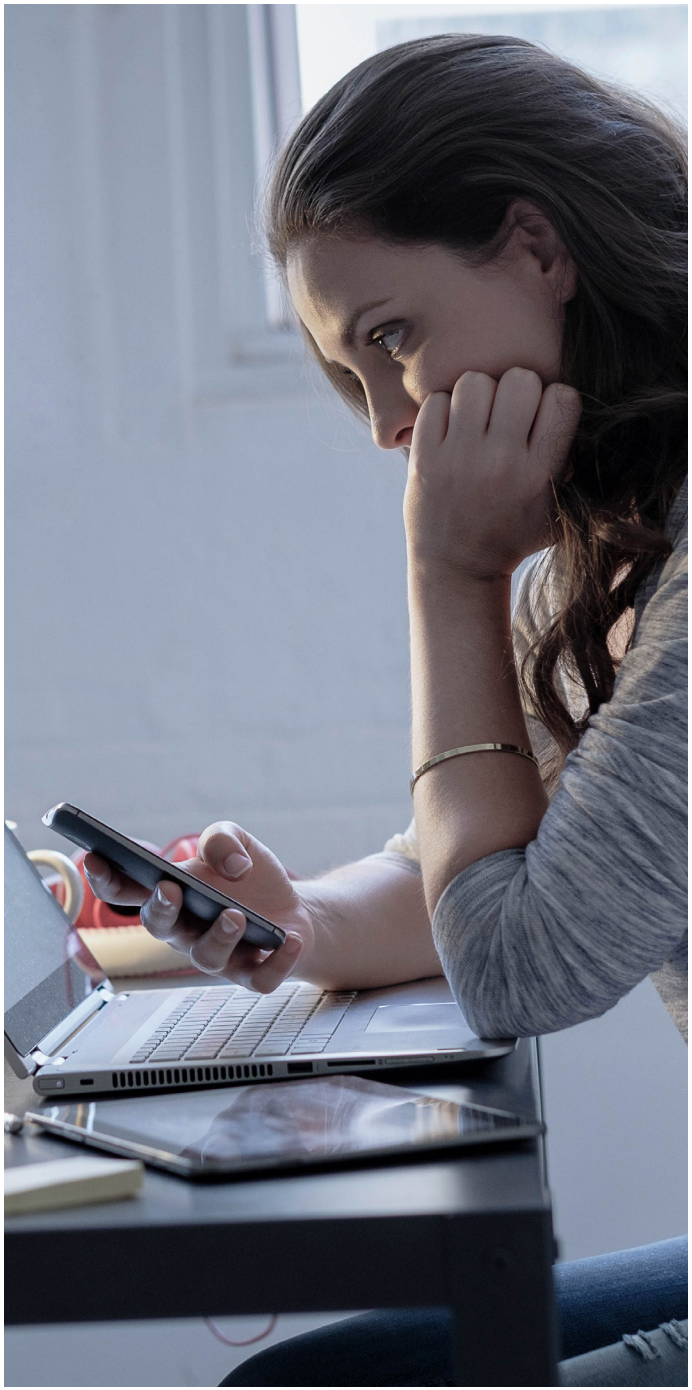
日常生活で大きな買い物のコストとその価値を比較検討するのと同じように、攻撃者は自分の時間とリソースを費やす最適な場所を決定する必要があります。安価で機会を手に入れ、天文学的な価値を得られればROIは高くなります。その決定は簡単です。

攻撃にかかるコスト

攻撃者が標的とする企業を探すとき、格好の標的、つまり安いコストで攻撃できる企業を狙います。多くのIT専門家は、Webやモバイルアプリケーション上で公開されるAPIなどの攻撃面に関する知識を深めています。

自動化された攻撃をオンラインアプリケーションに仕掛けるときの経済学は、チャリティくじを購入するときのようなものです。攻撃者は、攻撃のコストと成功の可能性を「賞品」の価値と比較します。この賞品は、アカウントの価値や、金銭的利益のためのアカウント侵害であれ価格操作のための企業データへのアクセスであれ、攻撃者の具体的な動機により企業ごとに異なることに注意する必要があります。

たとえば、自動化された攻撃が顧客ロイヤルティプログラムに仕掛けられると、アカウント乗っ取り、顧客ポイントの流出、および利益目的の転売といった不正行為により、巨額の損失、顧客の離脱およびブランドの毀損を招く可能性があります。



大数の法則

自動化された攻撃は、大数の法則を利用します。クレデンシャルスタッフィングの成功率は一般的に0.2 ～ 2%です。 攻撃者は数十億の認証情報を無料または安価で利用できるので、高い成功率は必要としていません。[1]

以下の計算式は、クレデンシャルスタッフィング攻撃がサイバー犯罪者にとってコスト効率の優れた手法となっている理由を示しています。成功したすべてのアカウント乗っ取り（ATO）に重要な価値があります。ダークウェブでは、攻撃者は、特定の業界の企業や同様のビジネスモデルを共有している企業のアカウントの価値を見つけ、攻撃を最大限成功させるために調整できます。

$0：23億件の認証情報
$50：ツール構成
$139：100,000回のCAPTCHA
$10：1,000のグローバルIP

} 100,000件のATOの試行にかかる費用は$200未満

攻撃者は簡単に成果を挙げたいと考えるので、一般的に、認証情報、自動化ツールおよびボットネットなどの自動化された攻撃の設定にかかるコストと、推定される利益を比較します。これらの攻撃は、1回あたりの価値が低くてもサイバー犯罪者に安定したROIをもたらします。

攻撃者の方程式

攻撃者は、ユーザアカウントにアクセスして乗っ取り、金銭的価値を抜き出すために自動化とボットを利用しますが、それだけではなく、ギフトカードの認証、または在庫や価格設定などの重要な企業情報の収集など他の目的にもこれらを利用する場合があります。攻撃者が攻撃ツールを拡張して複数のターゲットアプリケーションやWebサイトを狙うことで、特にコストや初期投資が安定している場合、利益率はより一層魅力的になります。

これがクレデンシャルスタッフィング攻撃がますます普及している理由の1つです。利益率を判別するには、**攻撃の価値に成功率を掛け**、これを**コストで割ります**。次に、その値から**初期投資**（100%）を引きます。

$$\frac{\text{価値} \times \text{成功率}}{\text{コスト}} - 100\% = \text{利益率}$$

悪意ある攻撃者がユーザ100人程度の企業に攻撃を仕掛けた場合、経済的な成功の可能性はほぼありません。恐らく、攻撃が成功するアカウントは1～2件のみです。しかし、5,000万人の顧客がいる大手銀行に攻撃を仕掛けた場合、攻撃は100,000～1,000,000件のアカウントで成功することが期待できます。恐ろしいことです。

ラスベガスにあるような古典的なペニースロットの原理はこれと同じです。プレイヤーは大当たりの可能性が極めて低くても喜んで1セント硬貨（現在では10および25セント硬貨）をスロットにつぎ込みます。これは、少額の賞金を低コストで手に入れる方法で、その価値はコストを上回ります。テーブルゲームではコストが高くなりますが、その分賞金を手に入れる可能性も高くなります。

これと同じ原理が、自動化された攻撃にも当てはまります。盗まれた消費者の認証情報を複数の電子商取引サイトで繰り返してアカウントアクセスを取得しようとすることで、大規模なアカウント乗っ取りが発生します。アカウントに価値があり、攻撃者にスキルがあれば、事態はさらに悪化する可能性があります。電子商取引、航空券、送金および銀行サービスの企業は、2020年から2040年の間に、クレデンシャルスタッフィング、アカウント乗っ取りおよび不正取引の巧妙化と攻撃ベクトルの増加の影響を受け、オンライン決済の不正行為により累積で推定$2,000億を損失することが予想されています。[2]

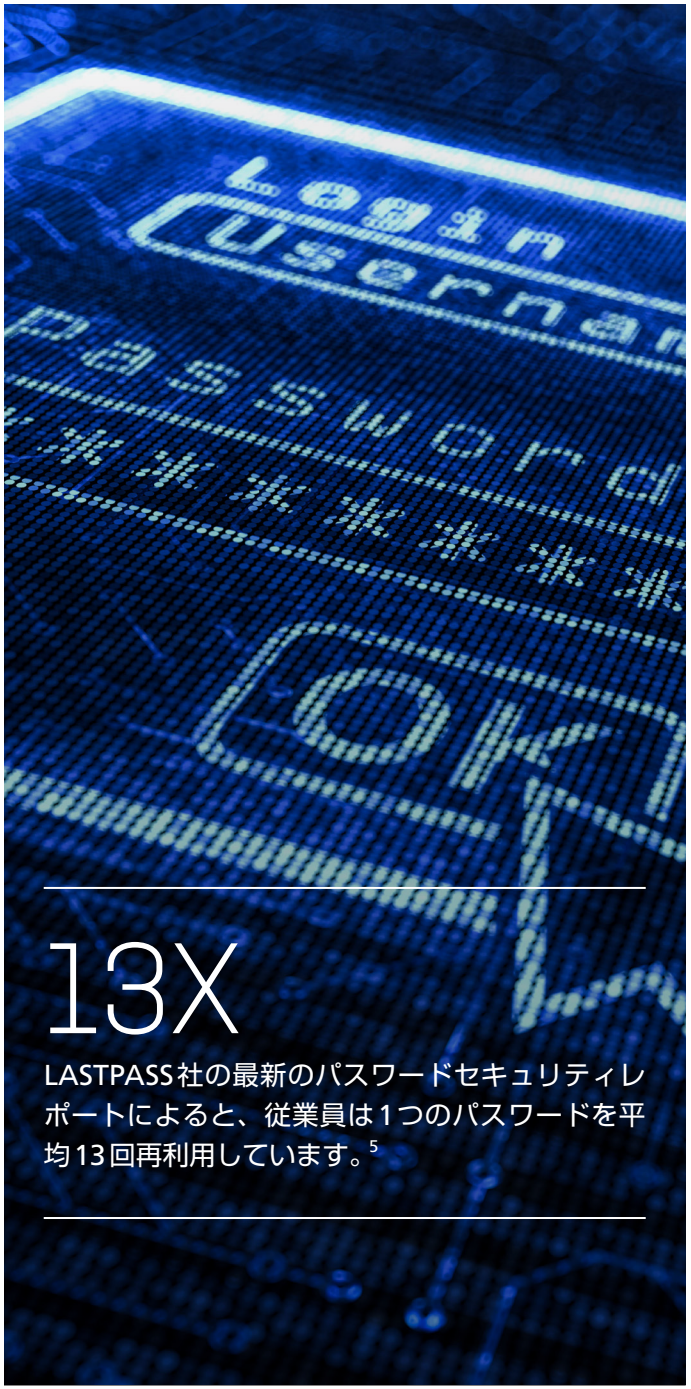
アプリケーションへのクレデンシャルスタッフィング攻撃が成功する可能性が高い場合、攻撃者の格好の標的になります。反対に、侵入にコストがかかる防御メカニズムを整備して成功の可能性が下がれば、ROIを著しく減少させることができます。攻撃者は、攻撃の労力に見合わないと諦め、別の企業に狙いを変えるかもしれません。

アプリケーションロジックを利用する攻撃

攻撃コストが安くてサイバー犯罪者の金銭的な報酬が高ければ、攻撃の格好の標的となることをほとんどの企業が理解しています。銀行、小売または航空のアカウントを標的とするクレデンシャルスタッフィングなどの自動化された攻撃の目的は、お金を盗む、それだけです。このような攻撃は正に金銭的な不正行為であり、取引のツールはますます安価になっています。

必然的に、攻撃の参入コストは世代を重ねるごとに下がっていきます。消費者の技術でも同じ傾向がありました。たとえば、家庭用ソーラーパネルの設置費用は、2010年は1ワットあたり$2でしたが、2019年では1ワットあたり$0.20に下がりました。[3] さらに顕著な例では、ハードドライブの1メガバイトの値段は1967年では$100万でしたが[4]、2017年では同じ容量のハードディスクドライブの値段は約2セントまで下がっていました。

隙がなさそうなアプリケーションのセキュリティ対策やセキュリティツールを導入している企業でも、最終的にはクレデンシャルスタッフィング攻撃に対して脆弱であることがわかります。ツール、インフラストラクチャ、および盗まれた認証情報をすぐに入手できるようになり、攻撃者が必要とする投資金額が少なくなっただけでなく、オンライン商取引の急速な移行により顧客アカウントの価値が高まったことで、攻撃者にとって魅力的な経済性がもたらされています。最も重要なことですが、クレデンシャルスタッフィングおよびその他の自動化された攻撃は、安全にコード化されているアプリケーションを悪用できます。そのため、サイバー犯罪者は、アプリケーションの弱点や脆弱性を利用する代わりに、アプリケーションロジックを悪用しています。



クレデンシャルスタッフィング攻撃は一般的な攻撃

ユーザ名とパスワードは一般的に複数のアプリケーションで再利用されています。実際、LastPass社の最新のパスワードセキュリティレポートによると、従業員は1つのパスワードを平均13回再利用しています。[5] さらに、消費者は、アカウントがセキュリティ侵害にあったことを通知されても、パスワードを変更するのはその約3分の1だけです。6クレデンシャルスタッフィングは、銀行、小売サイト、動画およびソーシャルメディアプラットフォーム、ホームオートメーションサービスなどの消費者サイトおよびサービスにおける大規模な企業セキュリティ侵害で抜き出されたこのようなアカウントとパスワードのペアを再生します。これらの攻撃が効果的である理由は、あるサイトで使用されたパスワードが他のサイトでも繰り返し使用されている可能性が高いことから、その経済性が攻撃者にとって魅力的であることです。

成功するクレデンシャルスタッフィング攻撃は、以下に示す4つの段階で展開されます。

1. 認証情報を入手する

従来、認証情報は攻撃者にとって見つけづらいものでしたが、現在ではすぐに入手できます。攻撃者は、RaidForumsやPastebinなどのサイトを使用したり、@checkmydumpのようなアカウントを介してTwitter上に公開されているリストを見つけたりできます。過去1～2日以内に盗まれた最新の認証情報は、サイバー犯罪者にとってより価値があり、購入費用も高くなります。一方古い認証情報はこれを使用した成功の可能性が極めて低くなるので、その価値も下がります。

2. ログインを自動化する

攻撃者がログインプロセスを自動化するときに利用できるツールやフレームワークには多くの種類があり、そのすべての価格は異なります。cURLやPythonなどの単純なスクリプトベースのツールはコストがかかりませんが、セキュリティチームおよびツールに簡単に検知および阻止されます。

高度な攻撃者は、より正確にネットワーク、デバイスおよびユーザの行動をシミュレートできるフレームワークを使用します。これらの攻撃ツールは、購入、レンタルまたは使用するためのコストがますます高額になっていますが、その分強力にもなっていて、これらの攻撃からアプリケーションを守るにはより特殊なセキュリティソリューションが必要になっています。

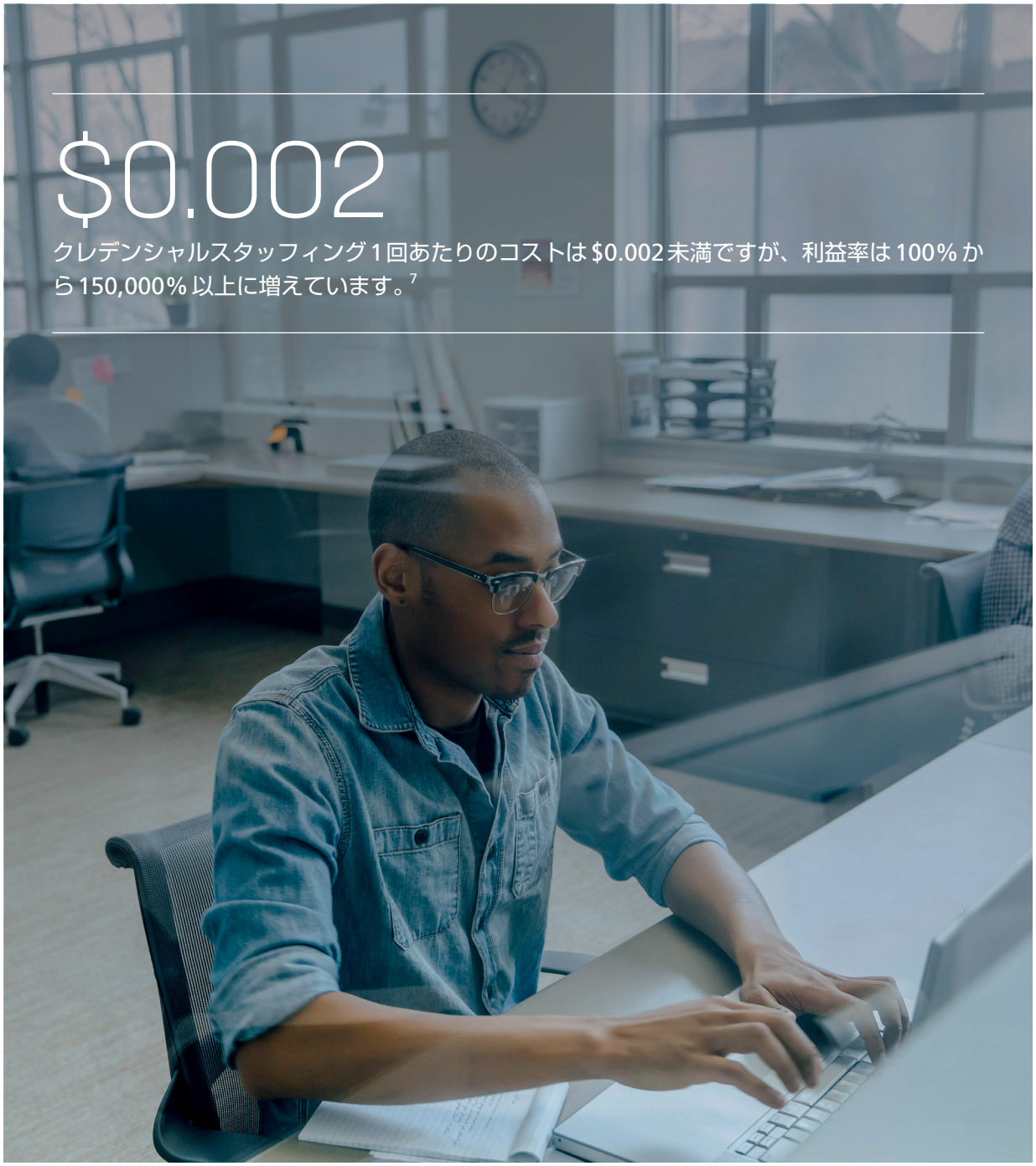
3. 関連する地理的状況をシミュレートする

攻撃者は、1つのIPアドレスから数十億のリクエストを送信するとすぐに警戒されることを知っています。プロキシサービスを使用することで、攻撃者は、簡単かつ安価でWebトラフィックが同じ地域の関連のあるユーザから送信されているように装うことができます。たとえば、ウクライナからニューイングランドの地方銀行に大量のトラフィックを突然送り付けることで、アラームが起動します（警鐘が鳴らされます）。しかし、攻撃者が、米国のアドレス、さらに望ましくはニューイングランドのアドレスで構成されるボットネットをレンタルできれば、より高い可能性で検知を回避できます。

4. 防御を破る

幅広い企業に使用される一般的なソリューションの防御は、攻撃者にいとも容易く破られてしまいます。たとえば、多くの組織は、無料または低価格のCAPTCHAソリューションを実装することで、自動化された攻撃を阻止しようとしています。これに対し、これらの防御を回避するためにDeath by CaptchaやXEvilなどのサイトが出現しました。ダークウェブに踏み込んでこれらのツールを探す必要はありません。ブラウザで検索するだけで、すぐに入手できるツールが数百見つかります。

多要素認証（MFA）によりこのような攻撃を防ぐことができると考える企業もありますが、これは理想的なソリューションではありません。サイバー犯罪者は、クレデンシャルスタッフィング攻撃によりアカウントにアクセスして、フィッシング、ビッシングまたはその他のソーシャルエンジニアリング技術を使用してMFAトークンを取得することもできます。さらに、MFAによるユーザ課題は、正規ユーザのストレスとなり、顧客離れや収益損失につながります。



$0.002

クレデンシャルスタッフィング1回あたりのコストは$0.002未満ですが、利益率は100%から150,000%以上に増えています。[7]

攻撃レベルの経済学

経済的に意欲的な攻撃者は、目標を達成するために必要なだけの投資をしています。サイバー犯罪者は、防御力ゼロのアプリケーションを狙い、無料のcURLスクリプトやPastebinダークウェブからの古い認証情報を使用して、そのホームIPアドレスからの攻撃に成功できれば、その最低レベルの攻撃を使用し続けます。しかし、アプリの防御によりこの攻撃が阻止されれば、攻撃者は対策を練り、攻撃レベルを上げ、より新しく、より高価な認証情報やデバイスの行動をエミュレートできるツールを使用するかもしれません。

このレベルの攻撃が成功すれば、攻撃者は、攻撃レベルを上げることなくさらに投資する必要もありません。しかし、この攻撃が失敗すれば、攻撃者は、さらに攻撃レベルを上げ、より優れた認証情報と人間の行動をエミュレートできるより高度な攻撃ツールを使用します。

この攻撃の段階を理解することがアプリケーションの防御に成功するための鍵となります。アプリ強化は唯一のソリューションではありません。プライバシー侵害となり得るセキュリティ制御は、ユーザにストレスを与え、正規の顧客との交流を台無しにします。その代わり、攻撃者が破ることを諦めるぐらいコストがかかる防御を整備する必要があります。攻撃を実現できないほどコストが高く、諦めて標的を変えざるを得なくなるレベルまで、攻撃者の攻撃レベルを強制的に上げさせます。

自動化された攻撃を検知する方法

攻撃されているかどうかを、どうやって知ることができるでしょうか？ 組織に自動化された攻撃が仕掛けられているかどうかを診断する重要な方法が3つあります。

1. アプリケーショントラフィックパターンを調べる

新規アカウント作成ページとログインページを調査します。これらのページは、自動化された攻撃およびボットの攻撃を最も受けやすいアプリページです。トラフィックが正常のように見えても、アプリケーションが攻撃に包囲されている可能性は十分にあります。

2. ログインの成功率を調べる

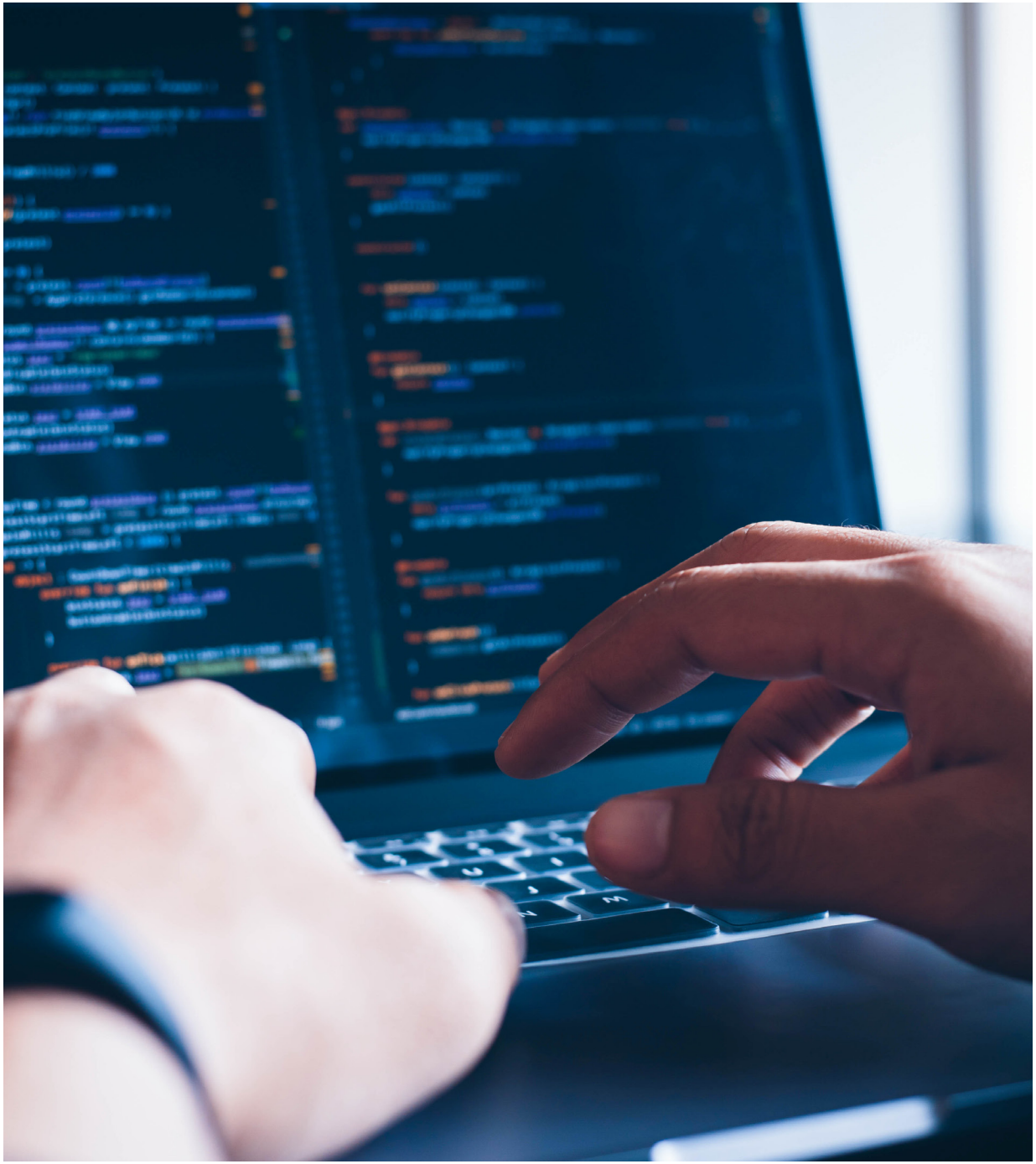
業界を問わず組織は、60 ～ 85% のログイン成功率を期待できます。7成功率がこれより高いまたは低い場合、特に急上昇パターンがプロモーションやバイラルマーケティングの取り組みなどの個別のイベントと一致しない場合、何か疑わしいことが起きている兆候です。

3. 日周パターンを探す

実際の人間によるトラフィックは日周パターンに従います。（ローカル地域またはユーザベースで）トラフィックは朝に上昇し始め、日中は高い状態を維持し、次第に減少して真夜中に底に達します。ランダムなパターンがある場合、組織はボット問題に巻き込まれているかもしれません。

4. 攻撃者のツール変更を調べる

トラフィックの急上昇の後に通常パターンはありましたか？ この期間中にセキュリティまたは不正対策チームは異常な動作を検知していませんでしたか？ 検知していたら、攻撃者はツールを替えて防御対策に対応しているかもしれません。重要なことは、経済性とROIであることを思い出してください。ツールを替えたということは、攻撃者がセキュリティ対策を回避するために投資していることを意味します。つまり、アカウントには追求するだけの価値があるということです。



攻撃されることを前提とする

一般的に、消費者と接するすべてのアプリケーションは自動化された攻撃の影響を必ず受けるということを前提としなければならず、そのための準備が必要です。これは、アプリを安全にコード化してパッチを適用し、最善の防御を尽くしている組織でも同様です。その理由は、攻撃者は不正行為のために欠陥を利用するのではなくロジックを悪用するからです。

まとめ

最も優れたサイバーセキュリティチームであっても、攻撃およびセキュリティ侵害のますます高まるリスクから組織を守ることに苦労しています。しかし、自動化された攻撃は、セキュリティの問題だけではありません。顧客やクライアント、会社の評価や収益のために適切に対処すべきビジネス上の課題でもあります。適切な防御策を講じることで、悪意のある攻撃を阻止し、コストを抑え、経済的にも有利な状況を維持することができます。

詳しくは、ウェビナー「Attacker Economics: Hacker Cost vs Value」をご覧ください。

出典

[1] F5「What Your Login Success Rate Says About Your Credential Stuffing Threat」（2019年8月23日）
https://blog.shapesecurity.com/2019/04/23/what-your-login-success-rate-says-about-your-threat-surface/

[2] Juniper Research社「Online Payment Fraud Losses to Exceed $200 Billion Over Next 5 Years」（2020年2月）
https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion

[3] Green Tech Media社「Solar Technology Got Cheaper and Better in the 20102. Now What?」（2019年12月17日）
https://www.greentechmedia.com/articles/read/solar-pv-has-become-cheaper-and-better-in-the-2010s-now-what

[4] Computer World社「CW@50: Data storage goes from $1M to 2 cents per gigabyte, (+ video)」（2017年3月23日）
https://www.computerworld.com/article/3182207/cw50-data-storage-goes-from-1m-to-2-cents-per-gigabyte.html

[5] LastPass社「3rd Annual Global Password Security Report」https://www.lastpass.com/business/articles/password-benchmark-report

[6] IEEE社「(How) Do People Change Their Passwords After a Breach?」https://www.ieee-security.org/TC/SPW2020/ConPro/papers/bhagavatula-conpro20.pdf

[7] F5「Attacker Economics:Hacker Cost vs Value」https://www.shapesecurity.com/app-security-and-fraud-summit/attacker-economics

F5について

F5は、差別化された高性能でセキュアなデジタル体験を提供できるよう、
アプリケーションを開発からライフサイクル全体でサポートします。

銀行および金融サービスについて詳しくは、f5.com/solutionsをご覧ください。

米国本社：801 5th Ave, Seattle, WA 98104 | 888-882-4447 // 米国：info@f5.com // アジア太平洋：apacinfo@f5.com // 欧州/中東/アフリカ：emeainfo@f5.com // 日本：f5j-info@f5.com EBOOK-BFSI-546894963