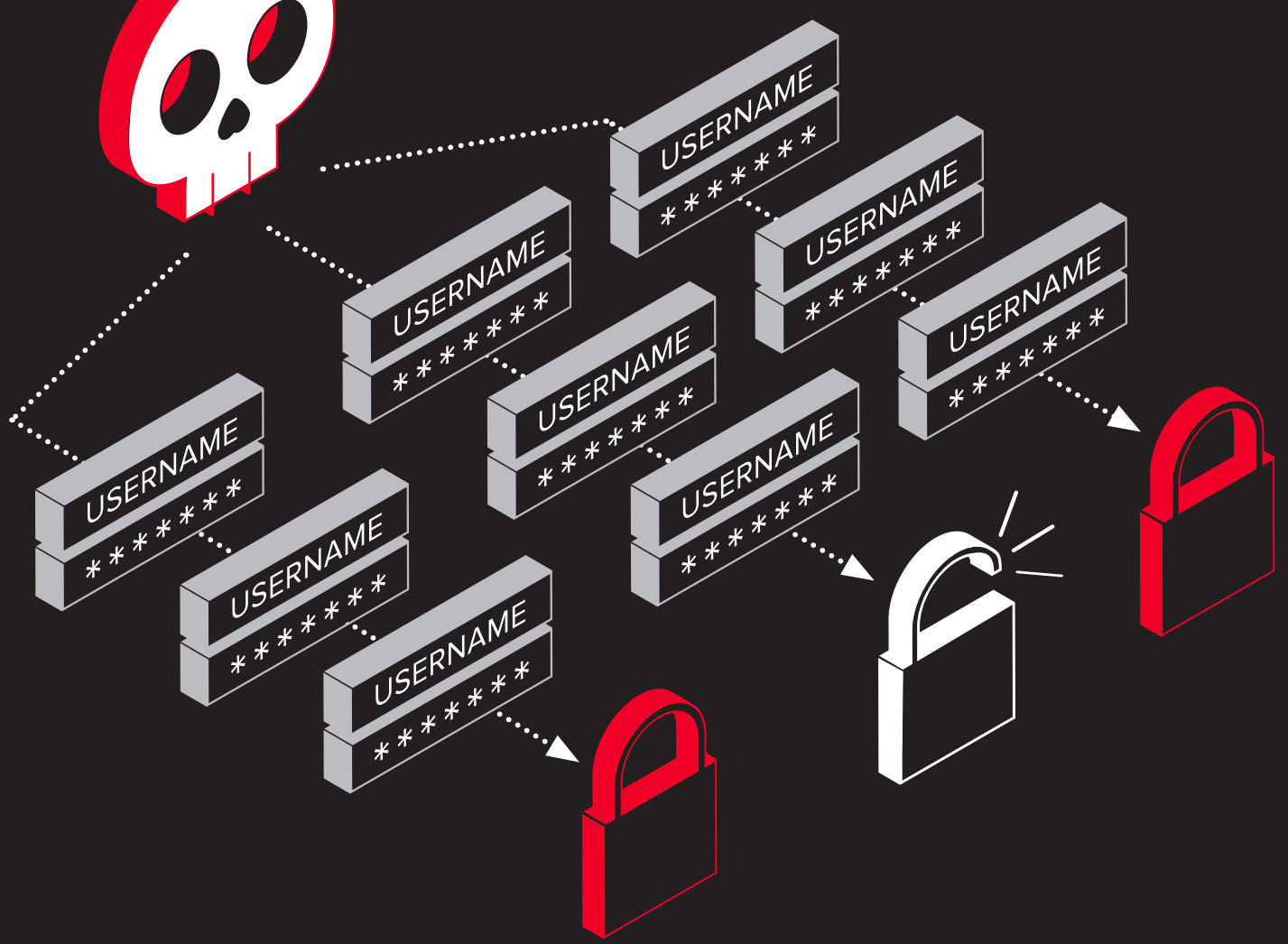
SHAPE
Part of F5



クレデンシャルスタッフィング 2021：最新の攻撃トレンドとツール

対抗策を回避する巧妙な攻撃者を理解し、撃退する

概要

地下室の一匹狼というステレオタイプから組織化された犯罪組織や国家へと、攻撃者は過去10年間でますます巧妙になってきています。攻撃者は、企業のITチームと同様のスキル、ツールおよびサービスをすぐに利用でき、人工知能（AI）や機械学習（ML）を使用して企業のセキュリティ対策に適応する高度なキャンペーンを作成することもできます。これらのダイナミックな攻撃手法は進化を続け、コスト対価値の方程式では攻撃者に桁外れのROIをもたらし続けています。特に、クレデンシャルスタッフィングは、魅力的なものから儲かるものへと進化しています。

以前は、単純なcURLツールを使用してウェブサイトからデータを抜き出すことができました。しかし企業はCAPTCHAのような防御手段を追加して対策しました。これに対して攻撃者は攻撃方法を変化させ、CAPTCHAソルバーやスクリプト可能な消費者向けブラウザを利用して人間の行動を模倣するようになりました。これらの変化は、ターゲットの価値が高まっていることを利用するための努力でした。

現在、攻撃者は、企業や組織がそのアプリケーションの保護に利用しているのと同じ技術を使って、標的に関する情報を収集できます。攻撃者は、セキュリティチームや不正対策チームが攻撃者の情報を集めるときと同様の方法で、弱点を見抜くことができます。このような状況下で、セキュリティチームと不正対策チームはどのようにして相手の一歩先を行くことができるのでしょうか。その鍵となるのは、自動化、機械学習およびAIを使用したセキュリティ抑止力を構築すること、つまり、攻撃者がツールを替えてセキュリティ対策に適応しても耐障害性と効率性を維持することで攻撃のROIを破壊することができるのです。

クレデンシャルスタッフィングは企業にとって最大の攻撃

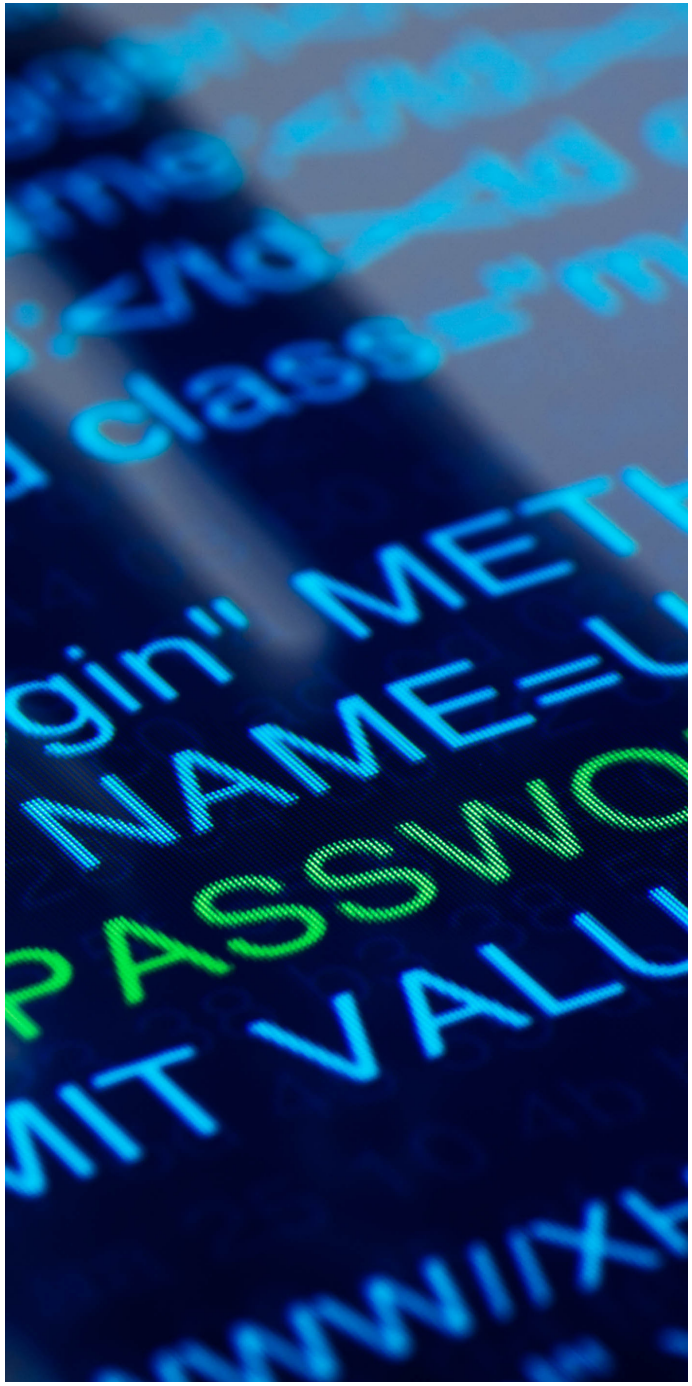
クレデンシャルスタッフィング攻撃は、信じられないほど簡単かつ安価になっています。以下の計算式を見れば、これらの攻撃がなぜこれほど人気があり、利益を生み出すかがわかります。

$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

クレデンシャルスタッフィングを制御できていると思っていても、攻撃者が攻撃方法を変え続ける中でこれらの攻撃がどのような軌道をたどっているかを理解することが重要です。F5 Labsの脅威インテリジェンスによると、クレデンシャルスタッフィングなどのアクセスベースの攻撃は、データ漏洩を引き起こす攻撃方法として最も多く利用されていました。[1] このような不正使用は、ログインページを超えて重要なアプリケーションのさまざまなコンポーネントに広がっています。

2019年だけでも、Webアプリケーションの攻撃の80%以上で、盗まれた認証情報の利用が関与しています。[2] また、Webアプリケーションへの攻撃は情報漏洩の43%を占め、前年比で2倍に増加しています。リスク面は組織ごとに異なり、攻撃者の動機もさまざまなので、攻撃の意図を理解することが重要です。



動機と逆境

動機と逆境の間の緊張感が進化を促進します。逆境とは、機密情報や顧客アカウントを侵害するために必要な投資など、攻撃の難易度のことですが、ツール、インフラおよび侵害されたデータを容易に入手できることから、攻撃の難易度は低下しています。同時に、オンライン商取引への急速な移行により顧客アカウントの潜在的な価値が高まっているので、攻撃への動機も高まっています。これが攻撃者にとっての好機となっています。

逆境は、組織が防御を強化するときにも作用し、攻撃への参入コストや攻撃の運用コストを上げます。コストが上がると攻撃者は自問自答して、攻撃を実行するために必要なツールを次世代のものに移行する価値があるかどうか、あるいは、もっと簡単に狙える標的に変えるかどうかを考えます。

残念なことに、ジレンマ的な状況が生じています。AI、クラウド、自動化、および企業がより少ないコストでより多くのことをできるようにするツールが増えていますが、攻撃者が参入コストを下げ、攻撃を武器化するために使用する技術と全く同じ種類のものです。進化が起きるのは、攻撃者がより価値の高い資産を手に入れるためにより高度な方法に移行するときです。攻撃者が次の世代へと進化したら、企業がやるべきことは、昔からあるコストと価値の問題に適切に対応しながら、攻撃者をより簡単な標的に仕向けるだけの十分な防御を行うことです。

しかし、攻撃にコストがかかりすぎて攻撃者が諦めるという至福の境地に達したとしても、それがいつまでも続くわけではありません。熟練した攻撃者は、通常、新しい対策が導入されるとすぐにツールを替えて、新たな攻撃を開始しようとします。最も高度な攻撃者になると、自動化ツールキットを使うのを止め、人間ではない自動化を検出するように設計された防御を回避する手動攻撃を仕掛ける場合もあります。組織は、すべての防御が既に回避されている、あるいは間もなく回避されることを前提として運用する必要があります。

収益の損失から規制違反による罰金、評判の低下、修復費用、チャージバックの損失に至るまで、攻撃はあらゆる市場分野の企業に大損害を与え続けています。最新の調査によると、電子商取引、航空券、送金および銀行業界の企業は、2020年から2024年[3]の間に、攻撃者の巧妙化と不正取引の攻撃手段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$2,000億を損失することが予想されています。

経済性が攻撃者側に有利な理由

消費者の認証情報にアクセスすることは、かつては困難なことでした。攻撃者は、独自の侵入方法を見つけるか、ゼロデイエクスプロイトを利用するか、または適切な（ここでは不正な）場所を周回しなければなりませんでした。現在では、誰でも無料またはわずかな料金で認証情報リストを入手することができます。リストはダークウェブ上で入手できますが、Twitterのような主流サイトやさまざまなオンラインフォーラムからアクセスすることもできます。さらに、データ侵害の影響を受けた個人の検証済み認証情報やデジタルフィンガープリントを販売するサービスもあります。

たとえば、Genesisは、攻撃者が被害者のデバイスに仕掛ける高度なブラウザプラグイン、マーケットプレイスであり、マルウェアでもあります。これは、ユーザのすべてのログインデータを収集して、それをマーケットプレイスに送り返して攻撃者に販売します。さらに悪いことに、このマルウェアは、ユーザがパスワードを変更するとマーケットプレイスを更新し、ブラウザと環境データを収集して指紋とデバイスの両方の特徴を生成するので、攻撃は常に、感染したユーザのブラウザから発生しているように見えます。

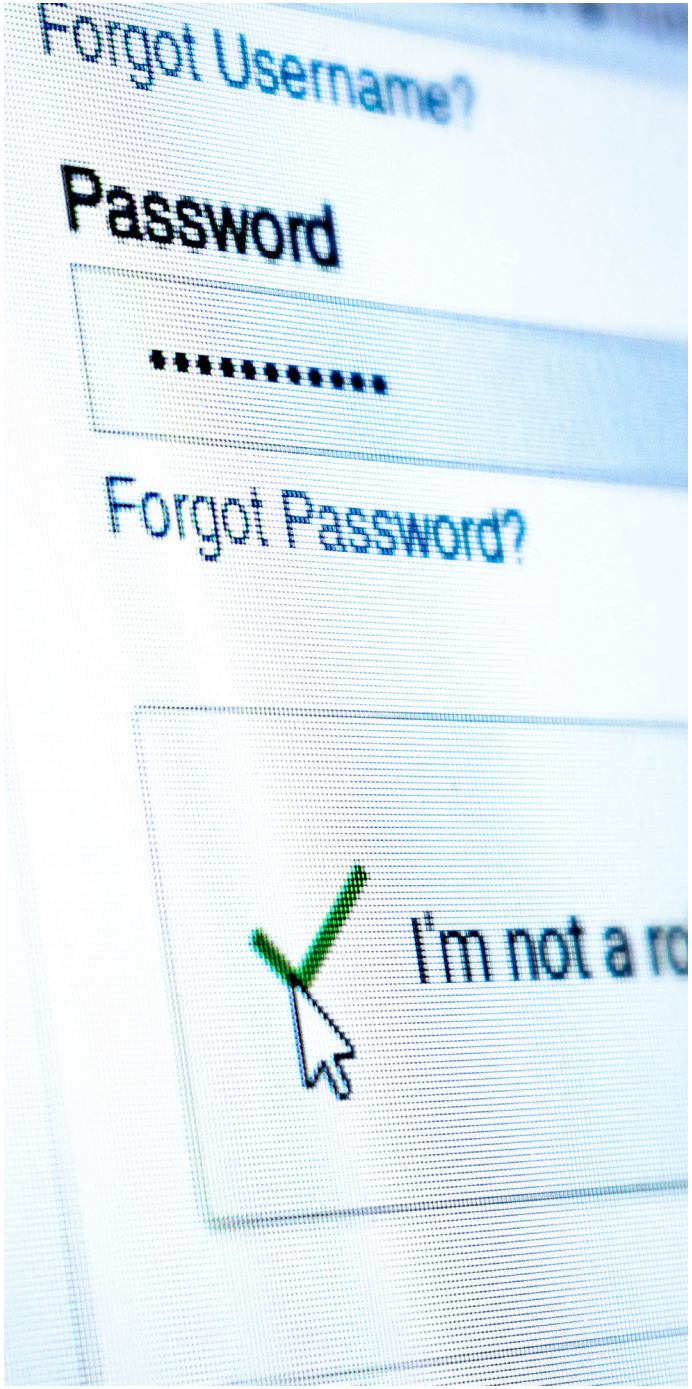
攻撃者が攻撃を拡大し適応させるためには、その運用を自動化するツールが必要です。現在では、プログラミングスキルの必要さえなく、CAPTCHAソルバーやアンチフィンガープリントなどのツールで技術的な作業を代行できます。また、すべてのサービスを設定する時間がない場合は、代わりに有料で攻撃を設定してくれるプロをフリーランス市場で探すことができます。

次の論理的なステップは、攻撃を運用することです。前の段階と同様に、CAPTCHAのような初歩的な防御を回避する方法はたくさんあります。クラウドサービスを利用することで、Hacking as a ServiceによりWebアプリに侵入したり、トラフィックを世界中に分散させたりすることが簡単になります。ソフトウェアの品質保証の一環として侵入テストを行うために設計されたツールは、ネットワーク、デバイスおよび人間の行動をエミュレートして自動化防止策を回避させるなど、不正目的にも使用できます。

攻撃者は、AI対応のマルウェアプログラムを使用して偵察やプロファイリングを行い、組織の環境、アップデートのライフサイクル、通信プロトコルおよびシステムの脆弱性や従業員を調査することもできます。[4]

さらに、APIを介したモバイルアプリやサードパーティの統合がますます不可欠になっていて、APIがクレデンシャルスタッフィングの影響を受けやすいことから、脅威の対象が拡大しています。

これらのステップをまとめると、安価で、自動化された、世界中に分散する攻撃は高い確率で成功します。参入や運用にかかるコストはゼロに近く、自動化と手作業のバランスを考えれば、その利益は天文学的になる可能性があります。



攻撃手法の世代交代

どんなに優れた防御でも、攻撃者をいつまでも寄せ付けずにいることはできません。攻撃者も同様に進化しています。攻撃者はcURLから始めて、攻撃を自動化するために特別に設計されたツールを作成するようになりました。企業はこれらの異常をレート制限や拒否リストで検出しようとしましたが、簡単に克服されてしまいました。これらの第一世代の攻撃は、セキュリティ防御の戦術的転換をもたらしました。

CAPTCHAの登場により、新たな防御の層が追加されました。残念ながら、何百万もの企業が無料というだけでCAPTCHAを採用しました。しかし、攻撃者にとって、CAPTCHAは簡単に倒すことができる相手です。この広く普及したソリューションに潜入するために、さまざまな種類のCAPTCHAソルバーがすぐに利用できるようになりました。Webブラウザに「CAPTCHAソルバー」と入力するだけで、すぐに何百ものオプションやサービスを見つけることができます。

次の戦術的転換は、JavaScriptインジェクションによるブラウザ問題です。第二世代の攻撃は、Phantom JSやTrifle JSなど、IT組織がWebアプリケーションのテストに日々利用しているのと同じツールを使用して、これらの新しい防御を打ち破ることに変わっていきました。

第三世代の攻撃では、トラフィックが人間の行動をより正確に模倣するので、セキュリティチームは、攻撃トラフィックを識別する革新的な方法を見つける必要があります。また、人間の実際の行動とエミュレーションの微妙な差異をより詳細に可視化する必要もあります。たとえば戦術的防御として、ヘッダや環境データをチェックしてこのような微妙な差異を調べることで、トラフィックの理解を深めることができます。

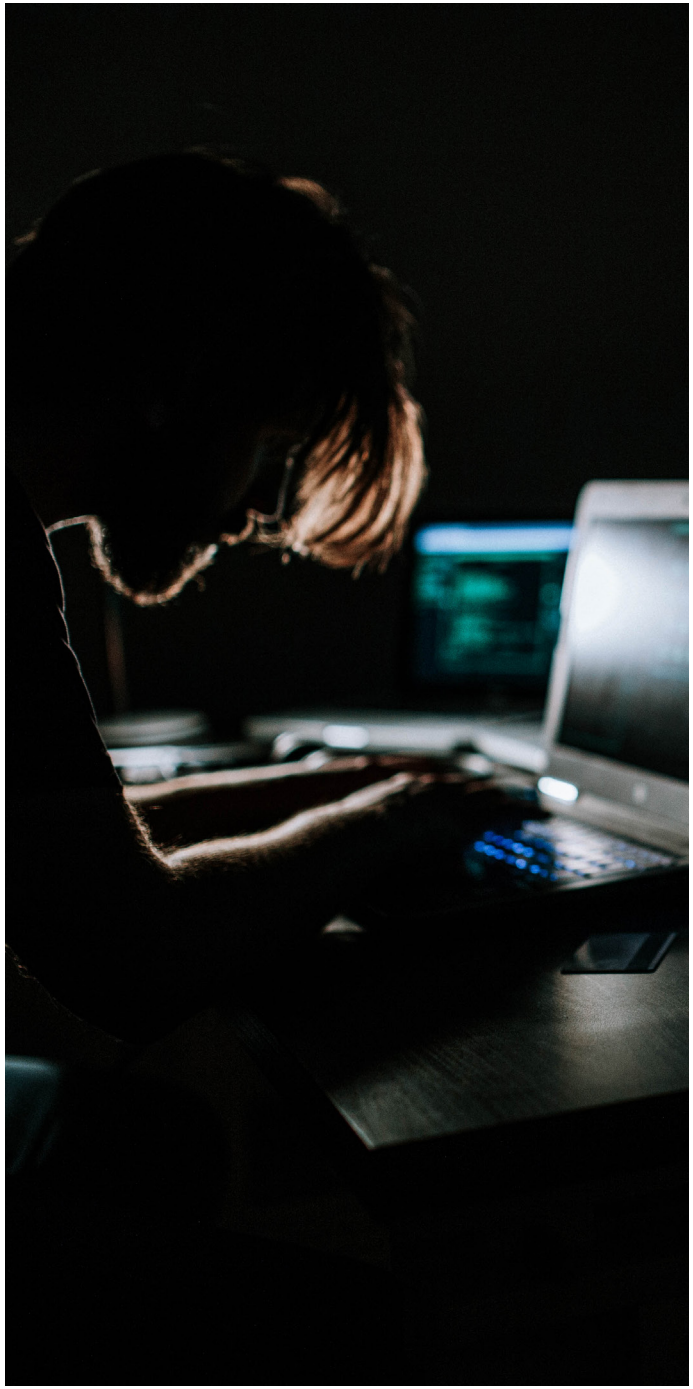
ハッカーは自分の行動を正当な人間とのやりとりに見えるようにより正確に偽装するようになっているので、ITチームは人間の行動と自動化された行動を区別する能力を高める必要があります。たとえば、攻撃者はアンチフィンガープリントツールを使用してデータソースをランダム化したり、BablosoftのFingerprint Switcherなどのツールを使用して、Canvas、音声およびwebGLのデータ、ビデオカードのプロパティ、Do not Track信号、オーディオ設定、ブラウザの言語、タッチサポート、ジオロケーションなどの実際のブラウザの指紋データを切り換えたりできます。

人間そっくりに装う

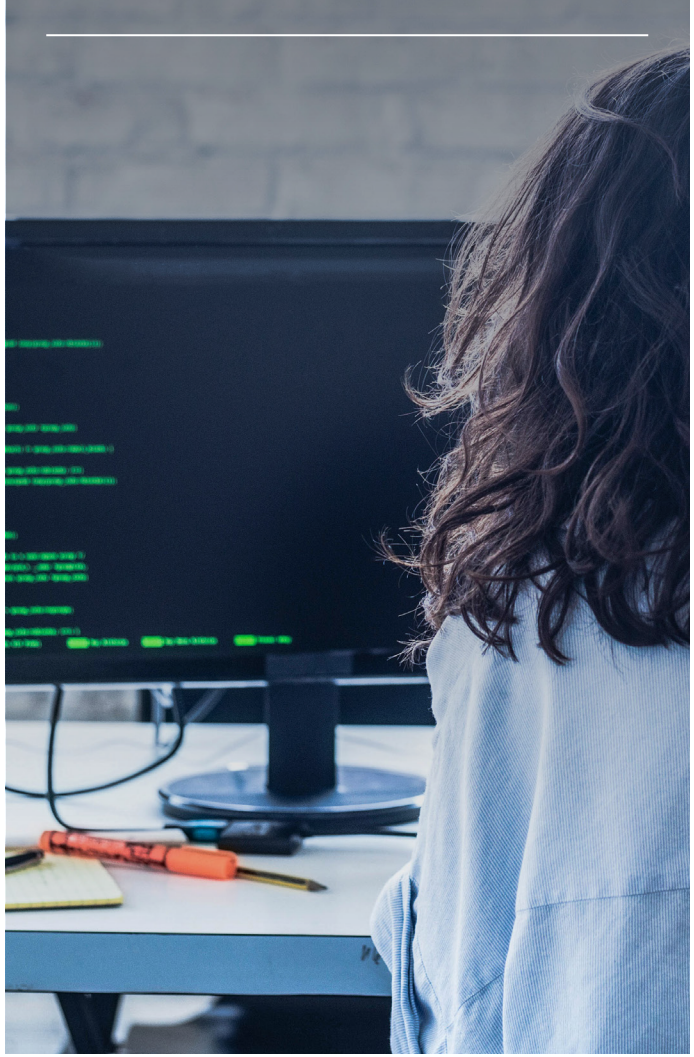
クレデンシャルスタッフィング対策は、いたちごっこです。企業が新たな防御を作り、ハッカーがこれらの防御を回避するための安く広く利用できるツールを開発し、これが繰り返されます。現在、攻撃者は、自動化されたツールやアルゴリズムを使用して、行動分析を回避する人間のような行動を作り出しています。従来の製品では、このような攻撃を検知するときには、必ず許容できないレベルの偽陽性が伴います。偽陽性のリスクに加えて、CAPTCHA や多要素認証（MFA）の課題は、実際のユーザにストレスを与え、顧客離れを引き起こします。一方、最悪のシナリオである偽陰性は、データ漏洩、アカウント乗っ取り、ブランド毀損、より一般的には不正行為につながります。

リスクスコアリングや行動分析ツールを回避するために人間の行動を模倣する攻撃は、「模倣攻撃」（Imitation attack）と呼ばれ、人間の行動に紛れ込み、最終的な目的は、正規のネットワーク、デバイスおよび人間の行動を模倣することです。模倣攻撃は、自動化される場合もあれば、そうでない場合もあります。

結局、人間の行動を模倣するツールを利用した攻撃であっても、実際に人間が悪意を持って行った攻撃であっても、正当なユーザに許容できないほどのストレスを与えずに防御することがますます難しくなっています。



第三世代の攻撃では、トラフィックは人間の行動をより正確に模倣するので、セキュリティチームは攻撃トラフィックを識別する革新的な方法を見つける必要があります。



ここからどこに向かうべきか

商取引のオンライン化が進むことで、顧客アカウントの価値は今後も上がり続けます。そのため、攻撃者は顧客アカウントをより確実に侵害できる方法を開発し続け、戦略的なビジネスの重要性が脅かされ、売上と収益が圧迫されます。最善の防御を講じている企業は、耐障害性のある防御を配備し、攻撃成功のために必要になる投資を増やして攻撃者が諦めるように攻撃のコストを十分に引き上げています。

攻撃者の経済を攻撃する

ハッキングは、技術的な問題だけではなく、経済的な問題でもあります。データの収益化を目的とする犯罪者に対する完全な防御はありません。高度なクレデンシャルスタッフィングは、アカウント乗っ取りや不正行為につながります。これは単純な自動化をはるかに超えています。セキュリティチームは、一般的に、時間とリソースが足りないことから、この問題が手遅れになるまで特定および対策できず、結果として、不正行為による多額の損失、チャージバックおよび顧客ロイヤルティと信頼の損失を招くことがよくあります。そのため、セキュリティチームは事業部門チームと密接に連携することで、問題を理解し、ソリューションを構築して、より効果的に対策する必要があります。

模倣攻撃が人間の行動に紛れ込むことを忘れないでください。攻撃を示唆する可能性のある異常なネットワーク、デバイスおよび環境のパターンを正確に識別できるように、トランザクションを深く可視化できることが重要です。

最後に、攻撃者は経済で動きます。そのため、攻撃者の経済を攻撃する必要があります。その理由は、経済的な価値が高ければ、どのような防御でも高度な敵を阻止できないからです。このような攻撃者や不正ユーザは、防御を回避するツールを替えあらゆる対策に適応します。将来のすべての攻撃を予測することは不可能です。そのため、攻撃に遭ったときに適応して、本当の顧客が交流を止めたくなるほどのストレスを与えることなく、セキュリティの効果を完全に発揮できるようにする必要があります。唯一実行可能な防御は抑止力です。攻撃を成功させるために必要なコストを現実的にありえないほど高くすることで、攻撃者の経済を破壊します。

抑止力および不正対策について詳しくは、shapesecurity.com/attacks/credential-stuffing をご覧ください。

出典

[1] F5 Labs「2019 Application Protection Report」https://www.f5.com/labs/articles/threat-intelligence/2019-application-protection-report

[2] Verizon 2020 Data Breach Investigations Report https://enterprise.verizon.com/resources/reports/dbir/

[3] Juniper Research社「Online Payment Fraud Losses to Exceed $200 Billion over Next Five Years」（2020年2月25日）
https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion

[4] CISO MAG社「Artificial Intelligence as Security Solution and Weaponization by Hackers」（2019年12月19日）https://cisomag.eccouncil.org/hackers-using-ai/

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。

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