2020 年 10 月 21 日

ブリテン: アカウントテスティングのペイメントセキュリティへの脅威

The PCI Security Standards Council (PCI SSC) https://www.pcisecuritystandards.org/ と米国 NCFTA(The National Cyber-Forensics and Training Alliance) https://www.ncfta.net/ は緊急性のある脅威について注意を呼び掛けています。

何が脅威なのか?

アカウントテスティング攻撃は、ペイメントアカウント目録、カードのテスト、BIN 攻撃などとして参照され、犯罪を犯す目的でカード会員情報の有効性を確認するためにペイメントカード番号をテストするサイバー犯罪を含む。フル桁のカード番号のテストや不完全なカード番号のデータをブルートフォースで攻撃する主な 2 つのテスト技術が含まれる。カード番号の有効性が確認されるとダークウェブサイトで販売され換金化されるか即座に不正取引のために使用される。

これらの攻撃はどのように行われるのか?

犯罪者がアカウントテスティングを可能にする異なる手法が存在し、それぞれが加盟店や他の事業体にペイメントライフサイクルの中で異なる影響を及ぼす。カード会員データはこれらのタイプの攻撃の中で 2 つの主な技術を通じ取得される、それはカード会員データ環境内で POI マルウェアまたはシステムへの侵害、もしくは不正目的でのアカウント番号目録によるものである。自動化されたソフトウェアを活用し膨大な数の攻撃により短時間に膨大な量のアカウントテスティング が可能となっている。

これらの攻撃の全ては犯罪者は大量の PAN、有効期限、CVV もしくは CVC をすでに取得していると想定される。これらの機密認証データが不知であるが、アカウントテストはこのデータの特定と有効性確認のために使うことができる。

カードテスティングツールはカード番号チェッカーとして知られており、CC チェッカー、CVV チェッカーまたは CCN チェッカーなどと略語で参照される。これらのツールは通常クリアネット(ダークネットではなく公共的にアクセス可能)上でホストされており、攻撃者が大量のカード番号を入力することを可能にしている。典型的には有効期限、CVV を使いどのカード番号が有効であるか特定することができる。これらのツールの中には登録が必要で手数料を払うもの、無料で登録不要なものもある。さらに攻撃者は地下組織やダークウェブ市場やフォーラムで商用カードのテストツールにアクセスするために手数料を支払うことがある。

攻撃者が完全なカード番号を保持していない場合でも BIN 攻撃を行うことができる。 BIN 攻撃には攻撃者が特定の BIN を携えている場合と、カード番号生成ツールを使い完全なカード番号にするために残りの桁を生成するツールを使う場合がある。カード番号生成ツールはしばしばクリアネットウェブサイ

ト上にホストされており登録なしで無料で使うことができる。これらのツールは「クレジットカード・ジェネレーター」として参照される。これらのツールは典型的に潜在的に有効なカード番号を生成するのみのツールであり生成されたカード番号の有効性は確認されていない。

加盟店 ID の乗っ取り

この攻撃では犯罪者は加盟店 ID と信用情報を取得する。これらの信用情報は脆弱な決済処理の導入や管理、もしくは加盟店システムへのアクセスに繋がる他の手段が原因で取得される。 多くの場合、脆弱なネットワークセキュリティとパスワード選択もしくはデフォルトパスワードなどの組み合わせなどが犯罪者にアクセスやコントロールを可能にさせる。 幾つかのケースでは、犯罪者がセキュリティの脆弱な運用と推測可能な端末 ID の環境がある場合にネットワークに侵入する偽の端末機を導入する。

犯罪者はクレジットカードで少額のオーソリゼーションが大量に発生する加盟店を効率的に狙う。有効期限と CVV や CVC が判明している状況ではこれは単純で即効性のあるプロセスとなる。承認されたカードの詳細は犯罪者に販売するためのカードの「確認済みリスト」に追加される。 これらの番号が不明の状況では有効な番号にたどり着くまで限定的な手法が行われるが比較的容易なタスクである。

カーディング または カードスタフィング

カーディングまたはカードスタフィングとは自動化されたウェブサイトへの侵入を通じクレジットカードの盗難と有効性確認を試みる手口である。PAN のみが既知である場合、自動化されたソフトウェア（例えばボット）を使い、PAN とオプションとして有効期限、CVV または CVC を入力し複数の加盟店を通じ少額の取引を試すことができる。 カードが承認された場合は攻撃者は正しい値が入力されたことを認識する。

サイバー犯罪者が同時並行で試すことによって取引頻度の上限を知ることができる。一般にカードの有効期限は 4～5 年であり、有効な有効期限は 60 回の試行で確認できる。 これは1サイトあたり5回の試行で12サイトを並行して試すことによる。

CVV や CVC などの認証コード入力を求めない、または入力されたコードを有効性確認をしないウェブサイトがまだ多数存在する。CVV または CVC 入力を求めるウエブサイトでは正しいコードを取得するために 1000 回の試行が必要になる。1サイトあたり5回の試行を行うと正しいコードを取得するのに200サイトでの試行が必要になる。

成功したデータは有効確認されたカードデータのリストに連結され現金化されることになる。カードスタフィングはカード情報流出の波及被害であり、関係する消費者と事業者双方にとり影響をもたらす。

カードバリデーションサービスはカーディング市場の重要な一部として認識されている。確認者の裏に潜むプロセスはサービスごとに変化している。募金サイトはしばしば少額の寄付により大量のバッチ処理と単純な決済処理を伴うため、不正が検知されにくく自動化されやすい。少額の募金サイトではしばしば1～5ドルの範囲で少額決済が行われる。脅威アクターはしばしば脆弱な中小加盟店サイトをターゲットにし取得した大量のカードのチェックのために使う。

ブラインド ブルート フォース攻撃

ブルートフォース攻撃では犯罪者が CVV や CVC、有効期限など膨大な量の組合せをテストすることにより有効な信用情報を取得するためにシステム的に取引を開始する。

この攻撃では、犯罪者はカード会員データの詳細を知らず、カード番号の順番に有効な番号に到達するまで取引を繰り返すことによりカード番号をテストするソフトウェアを使う。たとえ98%以上のカード番号が否決されたとしても全体の中では大きな影響を及ぼすことになる。

例えば、犯罪者が 1 時間当たり 10,000 回取引を試し成功率が 2%だったとした場合 200 件の有効なカード情報を生成し、もしこれを自動化すれば 1 日あたり 4800 件になる。

主にリスクを負うのは誰か?

アカウントテスト攻撃はイシュア、アクワイアラそして加盟店にリスクをもたらす、そしてその脅威は多くのアクセプタンスチャネルに存在する。消費者は、また攻撃により金融情報、個人情報盗難の被害者となり得る。ペイメントチェーンに関係する誰もが潜在的な危険にさらされる、そしてこの種の攻撃に対する注意と警戒は関係者全員の責任となる。良いセキュリティ対策はイシュア、アクワイアラだけでなく加盟店、ペイメントプロセサーにとっても優先課題とされる必要がある。この増長する攻撃に打ち勝つにはすべての関係する機関による努力を必要とする。

加盟店への影響

アカウントテスティングは攻撃がどのように行われるかによって加盟店への影響も広範囲にわたる可能性がある。もし加盟店が取引の可否単位で課金される場合、アカウントテスティング攻撃による処理費用は数千ドルのコストをもたらす可能性がある。不承認取引比率が高い場合、正常取引の比率が低下する傾向がみられるとブランド、イシュア、アクワイアラなどとの加盟店手数料に悪影響がでてくる。加盟店はさらに正規のカード会員から大量のチャージバックを受けることになり、これは加盟店の財政、風評などに影響を及ぼす。

イシュアへの影響

イシュアは自社システムを通じ不承認率の高い大量の少額取引を受信することになる。これはイシュアが不正取引と正常取引を判断することを困難にする。さらにイシュアは正常なカードが盗難にあい不正使用された場合にその損失を被る可能性もあり得る。 特に小規模イシュアはこのような取引に関連する手数料で大きな財政的な影響を受けることがある。

アクワイアラへの影響

アクワイアラにとり、アカウントテスティング攻撃の規模やボリュームによりアクワイアラネットワークにいくつかのレベルの影響を及ぼす。さらに、取引の紛争やキャンセルに関わるコストの増大を招く。 電話対応など時間の消費とアクワイアラとして安全でセキュアな決済処理対応に対する加盟店の信頼や満足度の低下はアクワイアラに風評・評価に悪影響を及ぼす可能性がある。これは長期的に加盟店の自然減をもたらす可能性がある。

検知する方法は何か?

このような脅威を被害を受ける前段階で検知する能力は極めて重要である。不規則なパターンや通常と異なる行為を検知するセキュリティモニタリングの 24 時間の 体制の構築がセキュリティ対策上必要である。

以下のような項目がオーソリゼーション/アカウントテスティングのいくつかの共通した特徴として見られる。

- カードを発行していないBINレンジでのカード番号など存在していないカード番号が使われている
- 同一アカウントが繰り返しセキュリティのいろいろなパターン、例えば有効期限、CVV2/CID、カード会員の郵便番号など変化させ使われている
- 同一のBINレンジ内で複数のアカウントが試されるケースの増加(特に同一加盟店で少額取引)、テストはカード番号順もしくはカード番号内の特定の桁数で規則的かつ順番に発生しやすい
- AVS (Address Verification Service- 住所確認サービス) チェックの増加
- 加盟店もしくはBINレンジでの不承認率の増加。オーソリゼーションテストは犯罪者がカード番号、有効期限、セキュリティコード(CVV2/CID)の正しい組合せを探すために行うので大量の拒否回答が発生する
- 加盟店精算の起きない承認された取引比率の増加
- 新しい加盟店または精算比率の少ない加盟店で取引の頻度・金額の増加
- 休眠加盟店で取引の頻度・金額の急増
- 加盟店が従来の合法的な加盟店名と異なる加盟店名で取引データが提出され、さらにその取引が増加

予防のためのベストプラクティスは何か?

アカウントテスティング攻撃の影響を緩和する最良の予防策は重層化した防御策の採用になる。この中にはセキュアな認証手法、オペレーティングシステムとソフトウェアに対し最新のパッチ処理、用心深い侵入検知の運用、そして適確なペイメントシステムの導入が含まれる。 そしてまた、PCIDSS 準拠は未対応の基準と運用を優先対応する文化を作ることにより脅威への対応をサポートする強力なセキュリティ基盤を提供する。イシュア、アクワイアラそして加盟店にとりアカウントテスティング攻撃を阻止するためのいくつかの推奨事項とガイダンスには以下の項目が含まれる。

イシュア:

- PANを順番通りに発行することを避ける
- 同一BINレンジの中でランダムな有効期限を設定する
- 不使用BINレンジをブロックしておく
- BINレベルでの異変をモニターする
- セキュリティコード(CVV2/CIDなど)が提示される全ての取引において有効性をチェックし無効なコードはすべて拒否する
- これらの攻撃を検知し拒否するためのルールを調整する

アクワイアラ:

- ウェブサイトをセキュアにするために加盟店と協働する(3Dセキュア、その他)
- アクワイアラレベルでボットネットの検知について検討する
- 重要なデータ(例えばIPアドレス)がモニターされアクワイアラと共有されるようにゲートウェイと連携する
- ベロシティチェックの実施(テスト、承認、拒否回答の急増、特定のBINでの取引の速度)
- 既知の不良なIPアドレス用のネガファイルの活用の検討
- 有効な加盟店IDに接続する認識されていない、またはクローンPOS端末の接続を許さないためにホストシステムに接続するPOSデバイスの有効性確認
- イシュアBINレベルまたはアカウント番号、加盟店屋号のレベルで不正試行で検知された無効番号をベースとしてレポートの作成
- デューデリジェンスの実施 – 加盟店候補先に関する情報の確認
- 無作為の端末ID – 順番どおりのID番号設定は犯罪者の検索を容易にする
- ペイメントゲートウェイポータル用に、強固なユーザーIDとパスワードを発行し、加盟店信用情報を保護

加盟店:

- POS端末の厳格な在庫管理目録を維持
- ウェブサイトをセキュアにし、自動化された攻撃を避けるためアクワイアラと連携(3Dセキュアなど)
- ボットネットの検知につきアクワイアラと検討
- ブルートフォース攻撃の影響を緩和するため、カードチェック時にランダムに中断を差し込むことを検討
- 既知の不良 IP アドレス用のネガファイルの実行につきアクワイアラと協議
- 不審で共通に使われているパスワードでのログインをレビュー
- 不正確なユーザネームとパスワードのあとに推測値がある場合のアカウントをロック
- 多数の IP アドレスから同一のカードアカウントでのログインを検知

###

PCI セキュリティスタンダードカウンシル(PCISSC) について

PCI Security Standards Council (PCI SSC) はペイメントセキュリティを向上させるため、サイバー攻撃とデータ侵害を検知、緩和、予防を支援する、業界主導、柔軟で効果的なデータセキュリティ基準とプログラムを提供することにより、グローバルで業界横断的な努力をリードしています。PCISSC への連絡は LinkedIn. ツイッターによる会話は @PCISSC. ブログの購読は PCI Perspectives Blog になります。

NCFTA について

The National Cyber-Forensics and Training Alliance （NCFTA)は 2002 年に設立された、グローバルにサイバー犯罪脅威の特定、緩和そして中断にフォーカスした非営利団体です。NCFTA はサイバー脅威を特定、緩和、中断そして撲滅することを最終目的に、双方向の情報共有を可能にする 中立で信頼できる環境を構築することを唯一の目的として産業界、学術界、法執行機関によって設立されました。 https://www.ncfta.net/