SOCIAL ENGINEERING / LT

# DMだけで Steamが乗っ取られかけた話

URLもQRも踏んでいないのに、認証コードだけが飛んできた

Nusk

WHO AM I

# 自己紹介

## nusk

SOC / セキュリティ運用

**仕事**

SOC運用。アラート対応・調査・報告がメイン

**すきなもの**

NixOS / Arch Linux / Claude / SoundCloud

**趣味**

VRChat / VALORANT / デスクトップ環境構築 / CTF

**守る側をやっているが、今日は自分が的にされた側の話をします。**

# TL;DR

01

## 認証コードが届く = 誰かが操作した

Steam Guard は自然発火しない。着弾自体がシグナル。

02

## パスワード不要でコードは飛ばせる

復旧フローはアカウント名だけで開始できる。

03

## 塞げないので「押さない」で受ける

通知を止める設定は存在しない。判断が唯一の防御線。

WHAT HAPPENED

# 届いたDMの流れ

1

## 面識のない相手からDM

「間違えて君をBAN報告しちゃった。CS担当と話して解決したい」

2

## “検証”のための指示

「ログアウトして、Steamクライアントを終了してください」

3

## 認証コードが着弾

指示に従った直後、Steamモバイルアプリに確認が飛ぶ

**この時点で**

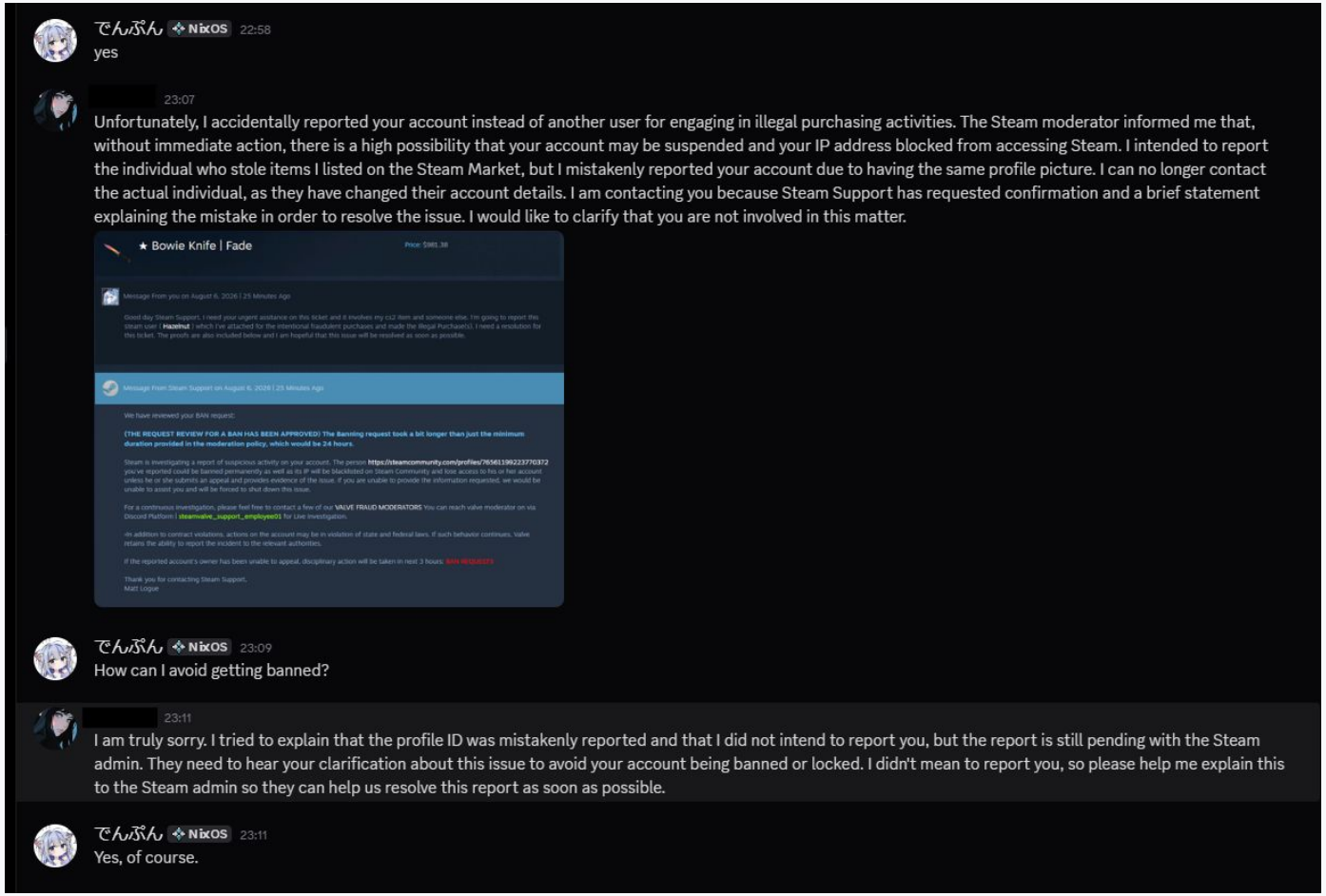
**踏んでいないもの**

- URLのクリック
- QRコードの読み取り
- ファイルの実行
- ID / パスワードの入力

**会話はすべてテキストのみ**

EVIDENCE

# 証拠① 入口のDM

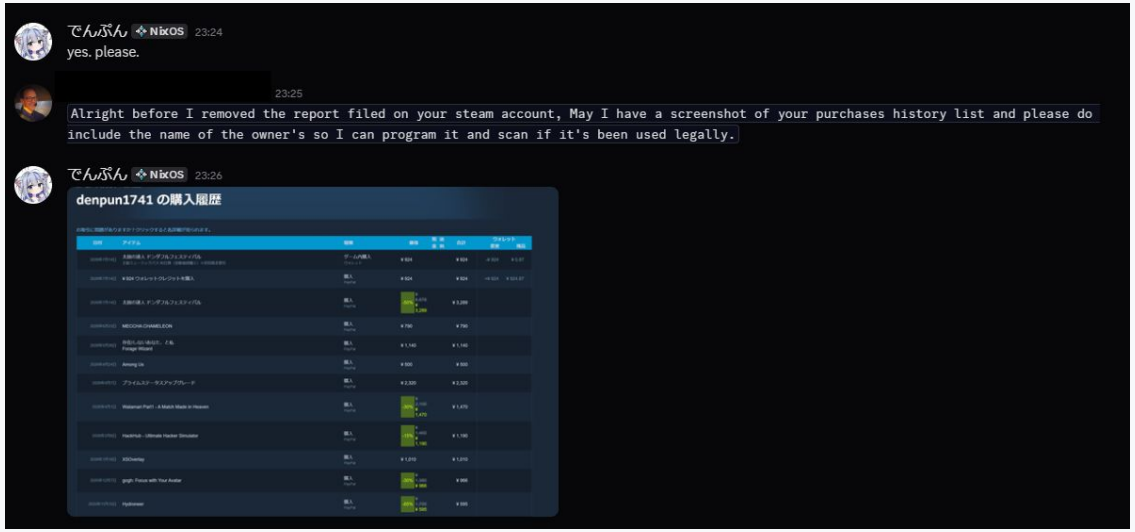


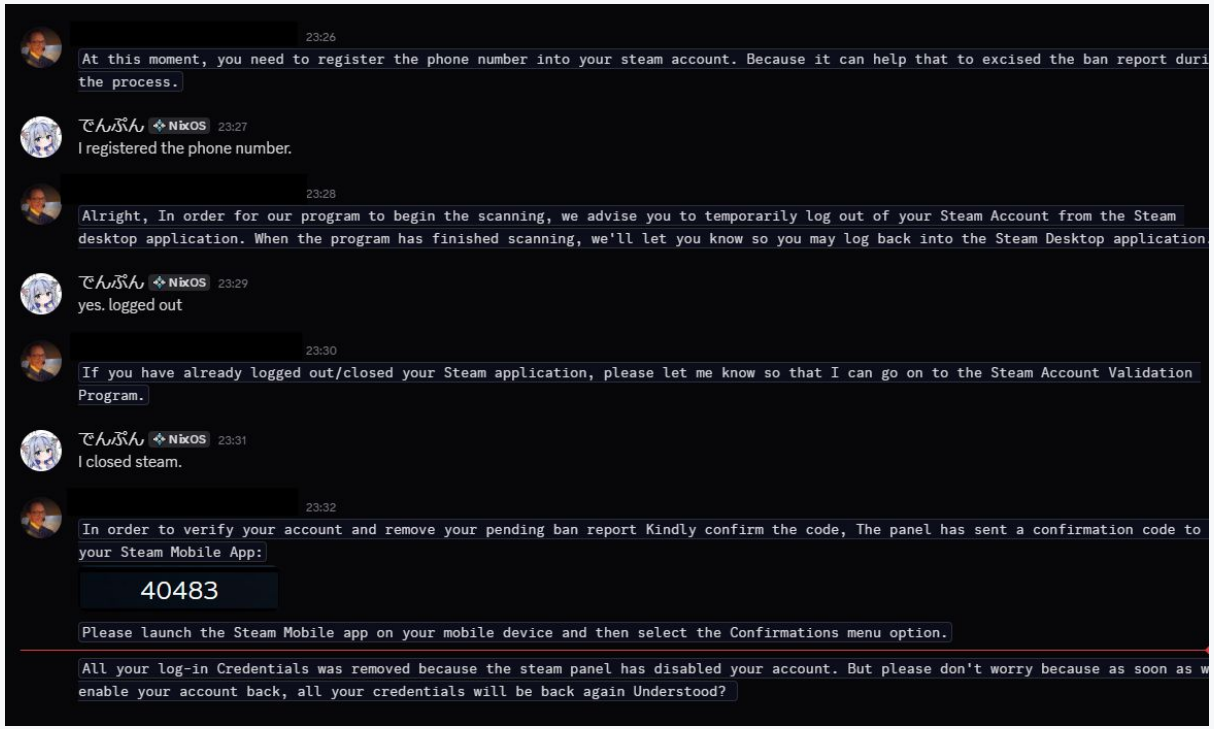

## 読みどころ

- 「BAN報告してしまった」という、相手に非があるように見せる導入
- Steamサポートを名乗る第三者を会話に持ち込む
- アカウント削除・期限を匂わせて考える時間を奪う
- Steamサポートが個人にDMを送ることはない

EVIDENCE

# 証拠② 誘導フェーズ

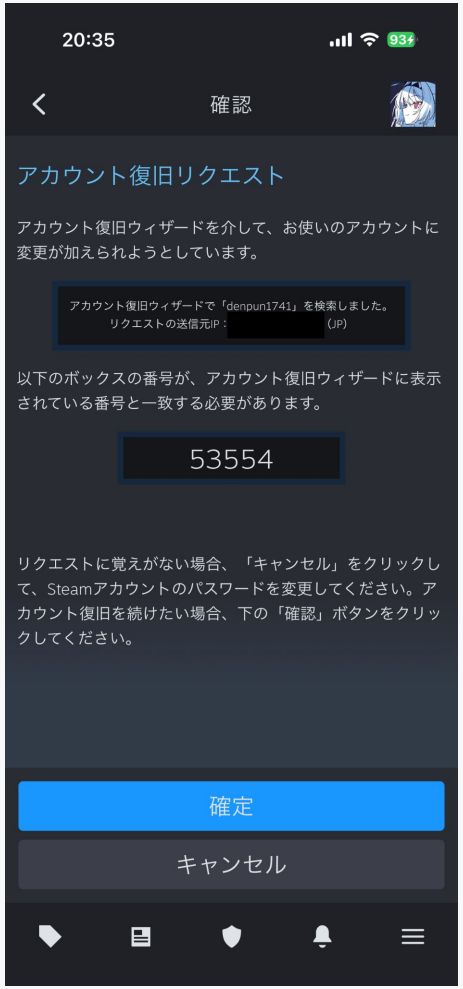



**「クライアントを終了させる」ことに検証上の意味は一切ない。ここが詐欺確定ライン。**

EVIDENCE

# 証拠③ 着弾した認証コード





## 突合ポイント

- DMの時刻と着弾時刻の差
- 表示された地域とIP
- メールの件名（復旧か、ログインか）
- コード自体はマスク

そもそも

# Steam Guard は いつ発火するのか

勝手には鳴らない。必ず誰かが何かを開始している。

つまり着弾は「攻撃の副作用」ではなく「攻撃そのもの」。

- 正しいID / パスワードでのログイン
- QRログインセッションの承認要求
- アカウント復旧フローの開始

TRIAGE

# 候補は3つ、必要なものが違う

## AiTM フィッシング

偽ログインページが入力を本物へ中継

必要なもの

- ID + パスワードの入力
- コードの入力

今回は該当せず

## QRLJacking

攻撃者のログインQRを承認させる

必要なもの

- リンクのタップ
- またはQRのスキャン

今回は該当せず

## 復旧フロー悪用

アカウント名だけで復旧を開始できる

必要なもの

- 公開プロフィールURL
- それだけ

今回はこれ

DEEP DIVE

# 余談: QRログインは構造的に脆い

- QRの中身は暗号化も署名もされていない、ただのURL
- URLである以上、スキャン不要。DMに1本貼ればスマホ側でアプリが直接開く
- 攻撃者は自分のセッションのchallengeを発行し、承認だけを他人にさせる
- QR方式そのものの問題なので、実装では潰せない

```
https://s.team/q/1/xxxxxxxxxxxxxxxxxx
```

ブラウザで開くと何も起きない。だが認証フローでは有効。

ATTACKER INTENT

# なぜ「クライアントを終了しろ」なのか

## 1 視界を潰す

クライアントが起動していると、新規ログインや他セッションの存在が本人に見えてしまう。先に閉じさせる。

## 2 因果を捏造する

終了させた直後にコードを飛ばすことで、「検証作業の一環でコードが出た」という筋書きが成立する。

## コードは奪う対象ではなく、信用させるための小道具

次に来るのは「届いたコードを教えてください」か「アプリの確認を承認してください」のどちらか。

MITIGATION

# では、防げるのか

## 防げない

- アカウント名は公開プロフィールURLから割れる
- 復旧フローは誰でも開始できる
- QRログインを無効化する設定は存在しない
- つまり通知を撃つ権限は実質全員が持っている

## 防げる

- 承認を押すか押さないかは完全に自分の管理下
- 通知が鳴るだけでは何も起きない
- 判断基準は「自分が今それを開始したか」の一点のみ
- 文面や地域表示は寄せられるので材料にしない

DEFENSE IN DEPTH

# 実務的には三段で受ける

1

## 通知を減らす

カスタムURLでSteamIDと切り離す / プロフィールを非公開寄りに

*狙い撃ちのコストを上げる。既に目を付けられた相手には効かない。*

2

## 押させない

自分が開始した操作でなければ承認しない。コードは誰にも渡さない

*唯一確実な線。ここだけは自動化できない。*

3

## 押しても死なない

認証子の付け替え直後は15日のトレードホールド。解除通知を見逃さない

*即死しない窓がある。気づける状態を作っておく。*

まとめ

# 脆弱性ではなく、仕様の帰結

- アカウント名が公開識別子である以上、通知は誰でも撃てる
- 認証コードは奪う対象ではなく、信用させる小道具として使われた
- 「クライアントを終了しろ」と言われた時点で詐欺確定と切ってよい
- 鳴っても押さない、押しても15日以内に気づく。この二段で受ける

*手口を一度知っていれば、次に同じ流れが来ても入口で切れる。*