Atomic Stealer 攻撃の徹底解剖

Atomic Stealerがソーシャルエンジニアリングから認証情報窃取、さらにその後の侵害へどのように進んでいくかを把握しましょう。

1

情報収集

攻撃者は、攻撃の準備として標的に関する情報を収集します。

例：ソーシャルエンジニアリング攻撃によって、標的を見定めてプロファイリングを行います。

2

攻撃手段化

収集した情報に基づいて、攻撃ツールが構築され、パッケージ化されます。

例：正規を装ったアプリに悪意のあるコードが埋め込まれます。

3

デリバリー

悪意のあるアプリが不正なチャネルを通じて配信されます。

例：スポンサー広告によって、ユーザが偽のアプリをダウンロードするよう誘導されます。

4

エクスプロイト

偽の入力画面でユーザを騙して認証情報を入力させます。

例：偽のアップデート画面でログイン情報や機密データを窃取します。

5

インストール

持続化の手法を用いて、最初の侵害後もアクセスが維持されます。

例：隠されたバックドアによってデバイスへの継続的なアクセスが可能になります。

6

コマンド&コントロール（C2：遠隔操作）

盗んだ認証情報を使用して他のシステムにアクセスします。

例：攻撃者はC2を利用してアクセス範囲を拡大し、ネットワーク内を移動します。

7

目的の実行

攻撃者はアクセス権を悪用して、
より広範囲に侵害を実行します。

例：アカウントの乗っ取り、攻撃の横展開、データ窃盗、恐喝。

jamf

AMOS に注目する理由

33%

がインフォスティーラー関連のマルウェア

50%

がトロイの木馬ベースの攻撃

50%

の脅威が検出を回避

出典：Jamfセキュリティ360：2026年版 Macセキュリティ最新トレンドレポート

ホワイトペーパーを入手