モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース／第87号

巧妙な中間者攻撃（AiTM攻撃）に注意

中間者攻撃の一種であるAiTM攻撃（Adversary-in-the-Middle）が確認されています。中間者攻撃は、通信を行いたい二者の間に第三者が通信相手になりすまして割り込み、通信内容の盗聴や改ざんを行う攻撃の総称です。

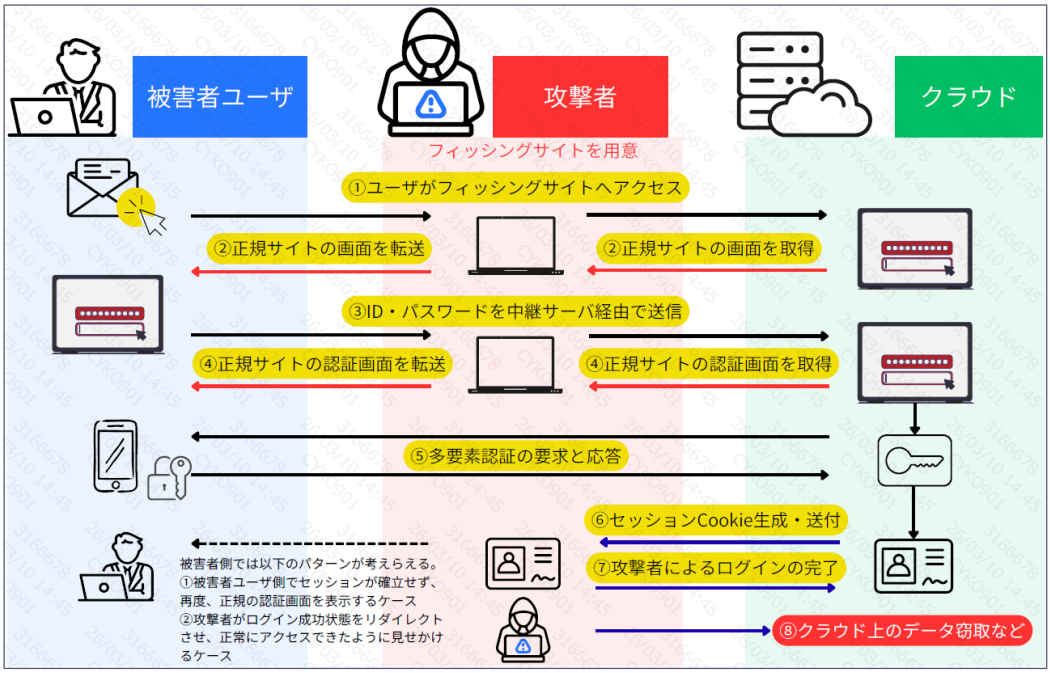
一方、AiTM攻撃は、この中間者攻撃の中でもユーザ認証の窃取に特化した手法です。攻撃者は本物そっくりのフィッシングサイトを用意し、ユーザが偽サイトへ入力したID/パスワードや多要素認証コードを正規サイトへ中継します。これにより、Webサービス側では正規利用者のアクセスとして認証が進み、認証成功時に発行されるセッションCookieが攻撃者に窃取されます。その結果、攻撃者は多要素認証を回避し、正規ユーザーになりすまして継続的にアクセスできるようになります。

特に、利用者の多いクラウドサービスであるMicrosoft365やGoogleなどに不正ログインされ、クラウド上に保存していたデータを窃取される事例が発生しています。

機密情報への適切なアクセス権限の付与や、データ自体の保護（パスワード設定等）も重要です。

【ＡｉＴＭ攻撃のイメージ】

引用：Canon サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2512.html



対　策

- **ドメイン名の確認**
  例：（正）microsoft.comではなく、（偽）login-microsoft.security.netとなっている。
- ブラウザの警告の確認
  「このサイトは安全ではありません」等の警告が出ないか確認する。
- **認証後の挙動の確認**
  「ログインしたはずなのに再度ログイン画面が出る」「リダイレクト先が不自然」といった挙動がないかどうか確認する。
- 条件付きアクセスの設定
  会社管理外のデバイスや社外からのアクセスを拒否する設定とする。
- **不審なサインインの監視**
  あり得ない場所からのログインや、新しいブラウザからのセッション生成を検知・ブロックする監視ツールの導入
- パスキーの利用、証明書ベースの認証

異常を検知すれば、警察へ速報をお願いします

京都府警察本部モノづくりプリザーブ事務局 075-451-9111