1ZE-04

2FA をバイパスする中間者攻撃ツール Evilginx によるフィッシング脅威分析

太田 和希 †　菊池 浩明 †

明治大学総合数理学部 †

1　はじめに

サイバーセキュリティの脅威の一つにフィッシング攻撃がある．2022 年に発生したデータ侵害の 36 %にフィッシングが関与している [1]．そこで，その対策として 2FA(二要素認証) が広く講じられている．しかし，Evilginx[2]，Muraena，Modlishka などの中間者攻撃によるフィッシングツールキットの中には，2FA をバイパスして，不正アクセスをできるものがある．

そこで，本研究では，フィッシングツールキットの一つである Evilginx の動作確認を行い，2FA を破るかどうかを検証する．さらに，主要な Web サービスの二要素認証方式を調査して，本攻撃に対する影響を仕様から評価する．

2　準備

2.1　AitM 攻撃

Adversary-in-the-Middle(AiTM) 攻撃は中間者攻撃の一種であり．攻撃者はユーザと正規サイトの間でリバースプロキシとして働き，ログイン情報を取得する．

図 1 に AiTM 攻撃の概要を示す．1. 攻撃者 *B* からユーザ *A* に対して，フィッシング URL を含むメール等を送り，攻撃者が作り出したフィッシングサイト *B* に誘導する．2. 攻撃者は ID とパスワードを取得し，それらを正規サイト *C* に転送する．3. 正規サイト *C* はユーザ *A* に二要素認証の要求をして，メールや SNS などで 2FA コードを送る．4. 攻撃者 *B* はユーザ *A* から 2FA コードを取得し，正規サイト *C* に転送する．

2.2　Evilginx

Evilginx は，フィッシングツールキットの一つである．リバースプロキシとして働き，2FA をバイパスしてユーザと Web サイト間のセッションを不正に取得することができる．Evilginx は Go 言語で書かれており，OS は Windows と Linux の両方で使用することができる．CLI でコマンドを打ち込み操作を行う．

Impact Assessment of a man-in-the-middle phishing tool, Evilginx, that bypasses 2FA

†Kazuki Ohta, Hiroaki Kikuchi, School of Interdisciplinary Mathematical Science, Meiji University.

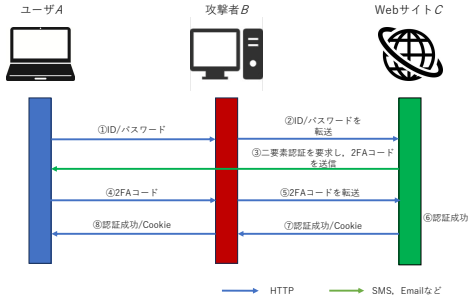

図 1　AiTM 攻撃の概要

3　Evilginx の評価

3.1　基本動作

Evilginx は config，phishlets，lures を設定し攻撃を行う．config コマンドで，中間者として働くサーバのドメインと IPv4 を入力する．phishlets コマンドで，phishlet と呼ばれる特定のサイトをターゲットにするための設定ファイル (yaml) を読み込む．lures コマンドで，フィッシングサイトの URL を取得する．また，Evilginx は TLS を欺くために Let's Encrypt から偽の公開鍵証明書を自動で取得する．

3.2　実験方法

正規サイトと Evilginx を用いたフィッシングサイトでページの読み込み時間，ログインにかかる時間の計測を行った．ローカル環境で行い，ターゲットとなる Web サイトには，Evilginx の学習サイトである Enilginx Mastery * を用いた．

フィッシングサイトのほうが正規サイトよりも処理速度が遅いと仮定し，正規サイトとフィッシングサイトの処理時間の違いからフィッシングサイトのシステムの遅延を計測する．また，その遅延によって，一般ユーザが異変に気付くことができるか推測する．

正規サイトとフィッシングサイトでページの読み込み時間を 50 回ずつ，ログイン時間を 30 回ずつ計測し，平均の時間を比較する．ページの読み込み時間は，ページ上のすべての要素が表示されるまでの時間として計測を行った．時間の計測には Selenium[4] を使用した．

3.3　結果

表 1 に実験結果を示す．読み込み時間では約 0.8 秒，ログイン時間では約 3.0 秒の差が発生した．証明書の読み込み時間，中間者を介した通信によって処理速度に差が生じたと考えられる．一方で，計測した時間は本来使用するネットワークの状況で前後するものであるため，これらの差が生じても一般ユーザは攻撃の存在に気づくことができないと推測される．

*https://academy.breakdev.org/evilginx-mastery

表 1　実験結果

		平均値	最小値	最大値	標準偏差
読み込み時間	正規	4.28	1.19	8.89	0.84
	フィッシング	5.04	3.64	8.02	0.87
ログイン時間	正規	4.10	3.38	4.97	0.41
	フィッシング	7.14	4.85	12.40	1.70

表 2　調査結果 (一部)

カテゴリ	サイト名	国	多要素認証	ソーシャルログイン	SMS	phone call	Email	認証アプリ	専用アプリ	セキュリティキー	パスキー	プッシュ通知
Backup and Sync	Dropbox	アメリカ	○		○			○		○		○
Communication	LINE	日本	○						○			
Creativity	pixiv	日本	○	○				○				
Developer	unity	アメリカ	○		○			○				
Domains	Crazy Domains	オーストラリア	○	○	○	○						

表 3　各二要素認証方式の AiTM 耐性

二要素認証方式	AiTM 耐性	認証コード秘匿
SMS, Phone, email, TOTP	×	×
App, Push notifcation	×	○
USB key, passkey	○	○

表 4　二要素認証導入率

ソーシャルログイン	国内 [%](件)	国外 [%](件)	全体 [%](件)
含まない	54.17 (26)	77.78 (37)	66.67 (68)
含む	77.08 (42)	88.89 (48)	83.33 (85)
計	(48)	(54)	(102)

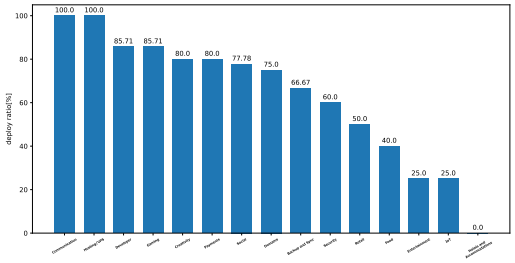

図 2　カテゴリごとの二要素認証導入率

4　Web サイトの脆弱性評価

4.1　仮定

二要素認証方式を 8 つの方式に分類し，AiTM 攻撃に対して脆弱であるかを仮定する．表 3 に各二要素認証方式とそれらの AiTM 攻撃への耐性を示す．

(1)-(3) SMS，phone call，Email を用いた二要素認証は脆弱であると考える．これらの認証方式は，4 桁や 6 桁のコードを用いる．従って，AiTM 攻撃の攻撃を受けると推測される．

(4) 認証アプリを用いた二要素認証は脆弱であると考える．この認証方式では，アプリが TOTP と呼ばれる 6 桁のコードを生成し，ユーザがそれを打ち込む．この方式は，SMS などの認証方式のようにサーバ側が認証コードを 送信することがない．しかし，ユーザが認証コードを送信する際は，中間者によって傍受されてしまう．

(5)(6) 専用アプリやプッシュ通知を用いた二要素認証は脆弱であると考える．これらの認証方式は Web サイトとユーザの持つアプリやデバイスの間で直接，認証要求と認証を行う．そのため，認証コードを中間者に取得されることはない．しかし，ユーザが認証をすることで Web サイトは正常に認証が成功したと判断し，セッションを中間者に送信してしまう．

(7)(8) セキュリティキー (例：YubiKey*) とパスキー (例：Windows Hello†) による認証方式は Evilginx に対して安全であると考える．これらの認証方式は，デバイスが認証サーバの正しい URL を保存しているため，中間者の偽の URL を区別可能である．

4.2　Web サイトの二要素認証方式の調査

二要素認証を導入しているか，どのような二要素認証方式をとっているのかを明らかにする．国内のサイトを 48 サイト，国外のサイトを 54 サイト，計 102 のサイトを調査対象とした．対象サイトは様々なカテゴリから網羅的に選択した．また，国外のサイトは，日本でも知名度が高いサイトを優先して選択した．

サイトの公式ドキュメントが公開されていれば参照して，対応している二要素認証の種類を調べた．ドキュメントがないサイトは自らアカウントを作成して調査をした．二要素認証の対応状況やカテゴリの分類に 2FA Directory[3] を利用した．

4.3　結果と考察

表 4 にそれぞれの二要素認証導入率を示す．

全体では，102 サイトのうち 68 サイト (67 %) が，ソーシャルログインを含めると 85 サイト (83 %) が二要素認証を導入していた．また，国外サイトのほうが二要素認証の導入率が高い．

対象 102 サイトを 2FA Directory[3] に従い 38 カテゴリに分類した．その中から 1 カテゴリに 4 サイト以上あるカテゴリを抽出し，15 カテゴリで比較を行った．

図 2 にカテゴリごとの二要素認証導入率，表 2 に調査結果の一部を示す．

調査した結果，4.1 節で脆弱でないと仮定した方式であるセキュリティキー，パスキーを導入していないサイトは 102 サイトのうち 87 サイト (85 %) であった．つまり，調査を行った 85 %のサイトは AiTM 攻撃に対して脆弱であると推測される．

5　おわりに

本研究では，主要な Web サイトの AiTM 攻撃に対する脆弱性を検討した．調査の結果，85% の Web サイトが脆弱であることがわかった．

参考文献

[1] Dataprot, “Phishing Statistics”（https://dataprot.net/statistics/phishing-statistics/, 2024 年 11 月参照）

[2] Kuba Gretzky, “Evilginx”（https://github.com/kgretzky/evilginx2, 2024 年 11 月参照）

[3] 2FA Directory, “2FA Directory”（https://2fa.directory/, 2024 年 11 月参照)

[4] Selenim, “Selenium”（https://www.selenium.dev/, 2024 年 12 月参照)

*https://www.yubico.com/yubikey/

†https://www.microsoft.com/en-us/windows/tips/windows-hello/