LATEST & PICKUP! SECURITY NEWS

Fuva Brain
Vol.49

最新個人情報漏えい事件・関連ニュース

LATEST

DATE：2022.08.08

サイバーセキュリティ.com　SecurityNEXT、jiji.com、Yahoo!NEWS

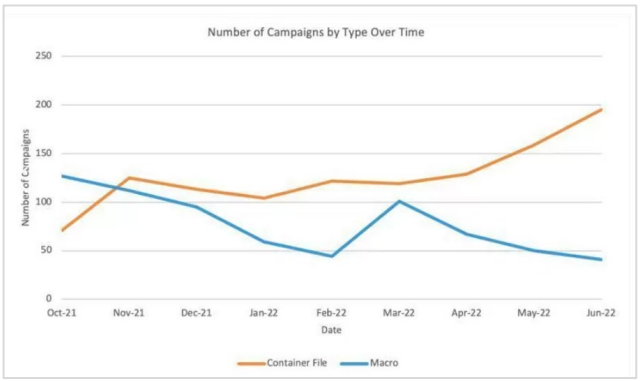
- 08月05日：自治体運営マンション管理状況届出システムで不正アクセス、迷惑メール2,044通を送信
- 08月04日： 米国債権回収会社 ランサムウェア感染して190万人の患者情報流出。医療関連情報では2022年最大規模
- 08月04日：オンライン通販サイトに不正アクセス、偽のクレジットカード情報入力ページに意図的に誘導
- 08月04日：人材派遣事業者、ランサムウェアによるサイバー攻撃を確認
- 08月03日：資格検定申込サイトで最大29万8,826件のアドレス流出懸念
- 08月02日：倉庫業者で不正アクセスによる障害発生、物流システムが稼働停止
- 08月02日：事業者向けEコマースサイトが不正アクセス被害、122名のカード情報流出か
- 08月02日：私立大学の専任教員、学生らの個人情報記録されたメモリを盗まれる
- 08月01日：個人情報117名記録の顔認証サーマルデバイス紛失、システム開発事業者
- 08月01日：国立大学法人教員のメルアカが不正認証、128件の受信メール不正閲覧の可能性
- 07月29日：患者2名の電子カルテを不正閲覧しLINEで流出、県立病院
- 07月25日：婦人服製造・販売会社のサーバに不正アクセス、ECサイトでの販売や配送に影響
- 07月22日：製造業者（自動車等）のサーバーにランサムウェア攻撃、範囲が広範に及び復旧に時間を要す

PICKUP!

VBAマクロ封じられたサイバー犯罪者次の一手、LNKファイル悪用が1,675%増加

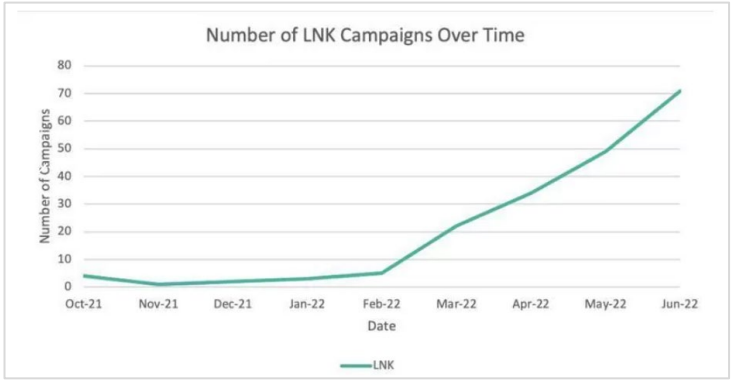
Microsoft社がOfficeファイルのマクロをデフォルトでブロック措置により、サイバー攻撃の手口に変化

- 出典：2022 年7月28日 Proofpoint https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world/



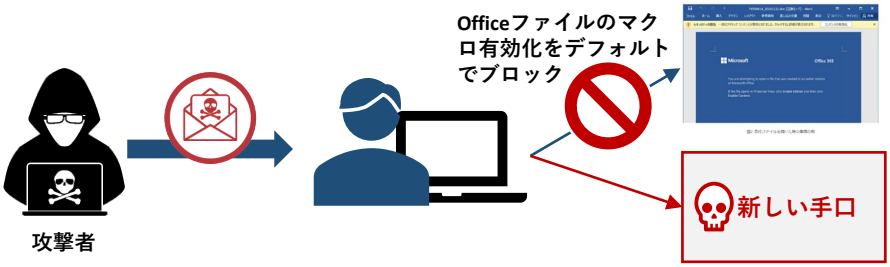
コンテナー ファイルとマクロ有効ドキュメントを電子メールの添付ファイルとして利用するキャンペーンの数

マクロ有効ドキュメントの件数は減って、コンテナファイルによる攻撃手口が増える



LNKショートカットファイルを利用したキャンペーン数

LNKファイルが増加し、2021年10月以降1,675%



簡単にマクロ有効化できないので、感染リスクを低減できている。

コンテナファイルのISO、RARやWindowsショートカットファイル（LNK）を使用する手口が増加で今後、注意が必要です。

フィッシング急増！報告件数10万件を超える

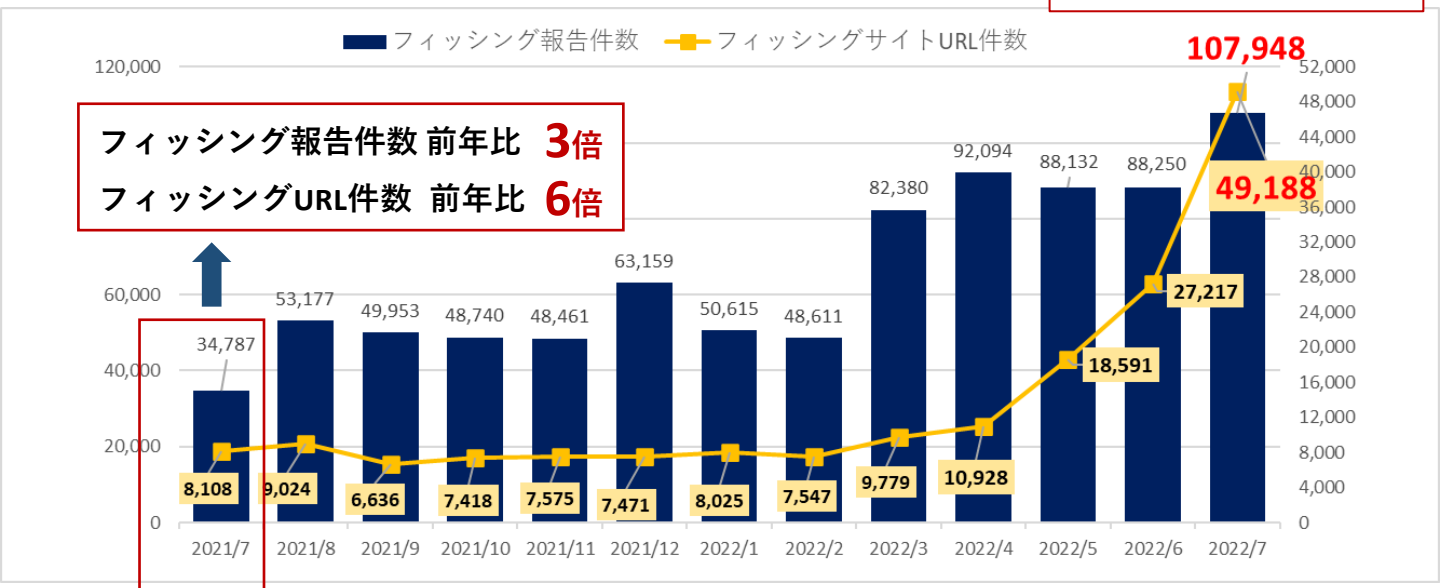
PICKUP!

- 出典：2022年8月3日 フィッシング対策協議会　2022/07フィッシング報告状況 https://www.antiphishing.jp/report/monthly/202206.html

フィッシングサイトの報告件数、URL件数がともに前月実績を大幅更新。フィッシングメールに注意！

3月から高い水準を保っていたフィッシング報告件数は、急増して107,948件（122%増）。フィッシングサイトのURL件数は、4月から過去最多を更新し続けてきたが、7月度も同様に大幅更新。前月比181%増の49,188件となった。

フィッシング攻撃の報告
1日平均 約3,482件
（前月 約2941.7件）



※2022/07 フィッシング報告状況を参考にフーバーブレインが作成

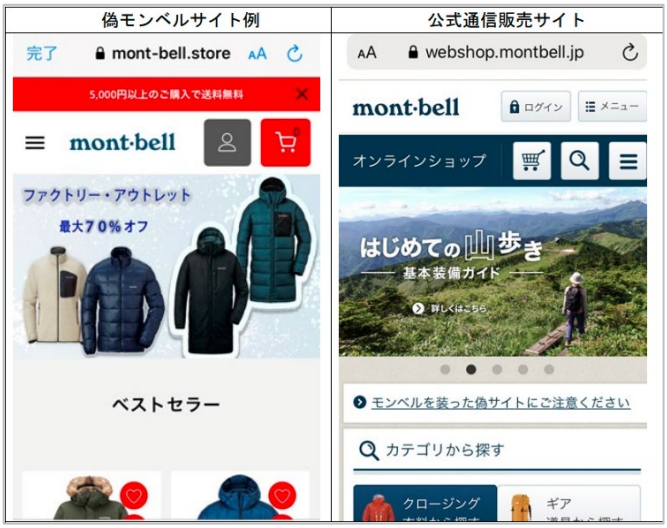
フィッシングサイトにご注意ください。

フィッシング対策協議会　緊急情報　掲載一覧

- 2022年07月29日 JR西日本をかたるフィッシング
- 2022年07月29日 えきねっとをかたるフィッシング

人気アウトドア用品公式通信販売サイトを装った偽サイトに関する注意喚起 （2022.07.28）

出典消費者庁
https://www.caa.go.jp/notice/assets/consumer_policy_cms103_220728_01.pdf



アウトドア用品を展開する「モンベル（mont-bell）」や「ロゴス（LOGOS）」の公式オンラインストアを装った偽サイトで被害が複数報告されているとして、消費者庁が注意喚起を発信した。注文をしても商品が届かず金銭をだまし取られる被害が多数発生しているという。新型コロナウイルス感染症の影響で、密な空間を避けて楽しめるアウトドアが人気を集めているが、その人気に便乗したフィッシングにご注意ください。

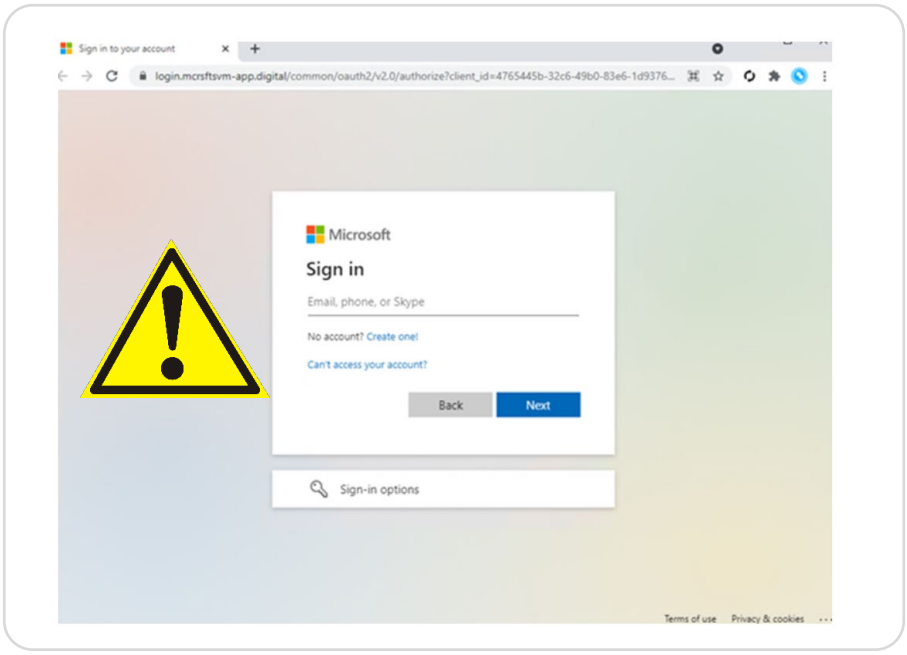
「多要素認証」破る攻撃　Microsoft 365利用企業はご注意ください。

PICKUP!

- 出典：Microsoft 365 Defender 研究チームマイクロソフト脅威インテリジェンス センター (MSTIC)
https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

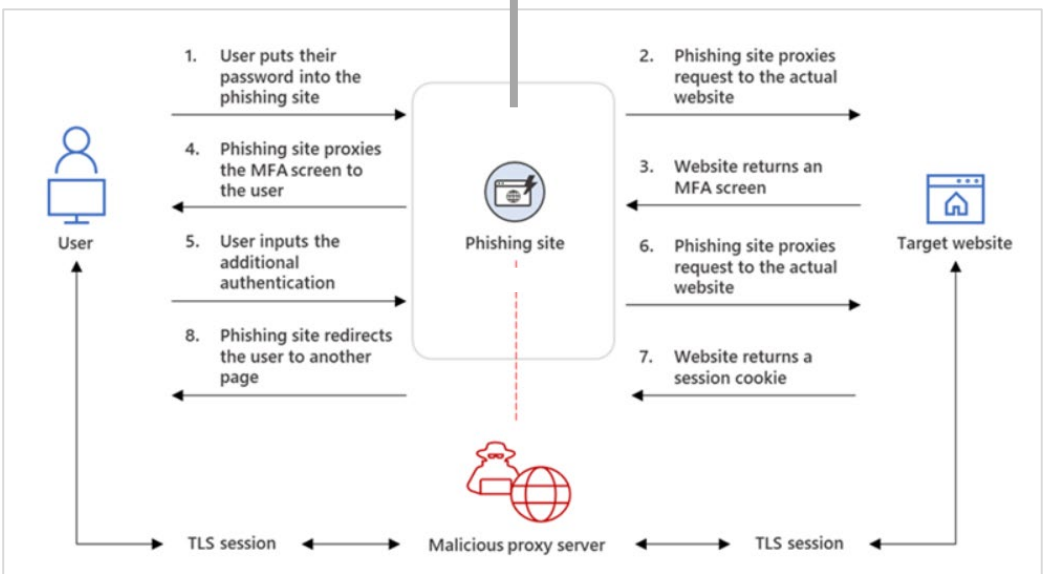
「Microsoft 365（旧称Office 365）」を利用している場合、AiTM フィッシングにご注意ください。

米Microsoft社は7月中旬、大規模なフィッシング攻撃が展開されているとして注意を呼びかけた。対象は業務用クラウドソフト「Microsoft 365（旧称Office 365）」を利用する企業や組織。
攻撃者は偽のメールを正規ユーザーに送り、偽サイト（フィッシングサイト）に誘導します。ワンタイムパスワードによる多要素認証を破られ、ビジネスメール詐欺に繋がる可能性があります。



出典：米Microsoft社　偽ログインサイトの例

図:AiTM フィッシングの概要



1.ユーザーが自分のパスワードをフィッシング サイトに入力する

4.フィッシングサイトはプロキシとしてMFA画面をユーザーに表示する

5.ユーザーが追加の認証を入力します

8.フィッシング サイトがユーザーを別のページにリダイレクトする

2.フィッシング サイトはプロキシとしてリクエストを実際のWeb サイトに通信する

3.Web サイトがMFA 画面を返す

6.フィッシング サイトはプロキシとしてリクエストを実際のWeb サイトに通信する

7.Web サイトがセッション Cookie を返す

出典：米Microsoft社　AiTM フィッシングの概要

Emotet引き続き警戒、JPCERT/CC　EmoCheck2.3.2で感染チェックを

PICKUP!

- 出典：2022年5月27日 JPCERT/CC　https://www.jpcert.or.jp/at/2022/at220006.html

侵入手口も感染後の動作も変わります。
マルウェア「Emotet」に引き続きご注意ください。

JPCERT/CC　2022年4月から6月を振り返って（2022年7月12日 注意喚起）

マルウェアEmotetの感染再拡大に関する注意喚起

- 直近3カ月においてもマルウェア「Emotet」の感染再拡大が特に注目すべきトピックに挙げられる。
- ブラウザ認証情報窃取機能が追加され、Chromeのクレカ情報が標的になっている。
- ショートカットファイル（LNKファイル）を含んだパスワード付きZipファイルを添付するなど、WordやExcelを使用せずに感染に至らせる新たな手口が広がる。

引き続き、不審なメールの添付ファイルやリンクは
開かぬようご注意ください。

https://www.jpcert.or.jp/newsflash/2022071201.html

その他、2022年4月から6月にかけて確認された影響範囲の広い脆弱性情報や脅威情報などがまとめられております。

参考情報

JPCERT/CC 提供

感染チェックツール「EmoCheck2.3.2」

JPCERTCC/EmoCheck - GitHub
https://github.com/JPCERTCC/EmoCheck/releases

EmoCheckの使用方法や更新履歴など
https://github.com/JPCERTCC/EmoCheck/blob/master/README_ja.md

マルウェアEmotetの感染再拡大に関する注意喚起

Emotetに関する最新動向
https://www.jpcert.or.jp/at/2022/at220006.html

マルウエアEmotetへの対応FAQ

Emotetに関する情報、対応を確認
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

解説動画
社内周知
注意喚起に

JPCERT/CC 提供

日本中で感染が広がるマルウェアEMOTET

JPCERTCC/Emotetの解説動画
https://youtu.be/wvu9sWiB2_U

EMOTET感染の確認方法と対策

JPCERTCC/Emotetの感染確認方法と対策解説動画
https://youtu.be/nqxikr1x2ag