最新個人情報漏えい事件・関連ニュース

LATEST

DATE：2022.09.13

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

- 09月08日：玄関マット製造業者に対するランサム攻撃 - 流出VPN認証情報で侵入か
- 09月08日：廃材リサイクル業者、サーバに不正アクセス、基幹システムや関連システムに被害が及び業務に影響も
- 09月08日：キルネットが日本政府に宣戦布告、東京メトロでアクセス不良
- 09月08日：産業用IT技術専門商社、不正アクセスでウェブサイトが改ざん被害
- 09月07日：キルネットがe-Govなどにサイバー攻撃の可能性、JCBなども対象か
- 09月07日：防衛省、サイバーセキュリティ強化の防衛企業に税制優遇を要望
- 09月07日：ランサム被害、リモート接続の脆弱性が侵入口に – ゴム製品製造業
- 09月06日：人材派遣登録者管理サーバへの不正アクセス、
  「代引き注文で嫌がらせするぞ」といった不審メールの送信を確認
- 09月05日：首都圏自治体、マンション管理状況届出システムが不正アクセス被害
- 09月05日：みずほ銀行装うフィッシングに注意 - 顧客情報の確認などとだます手口
- 09月05日： QNAP製NASを狙うあらたなランサム攻撃 - アプリの更新を
- 09月05日：国立大学法人工業大学、新たにEmotet感染端末判明
- 09月02日：製菓会社のグループ会社がランサム感染、10万ドル要求断ると情報公開か
- 09月02日：医療・福祉児童施設の委託先が205名のアドレスを誤送信
- 09月02日：工業部品・産業資材の専門商社、ベトナムグループ会社に不正アクセス

キルネットの犯行声明
日本政府4省23サイトで障害、DDos攻撃が原因か、民間サイトでも影響

PICKUP!

出典：Microsoftウクライナを守る: サイバー戦争からの初期の教訓
https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

ロシア支持ハッカー集団「キルネット」
政府機関の他、東京メトロ、JCB、ミクシーなどでも障害

出典：キルネットの投稿動画
親ロシア派のハッカー集団「キルネット」と見られる犯行声明

「キルネット」は今年初めに組織され、ロシアに制裁を科した国などに対してハッカー攻撃を仕掛けてきている。

当社公式ホームページにアクセスしにくい事象について

2022年9月7日（水）19時頃以降、当社公式ホームページにアクセスしにくい状況が生じておりました。
ご利用の皆様にはご不便とご迷惑をおかけしたこと、お詫び申し上げます。

なお、当社の運行情報につきましては、
東京メトロアプリ、各路線の運行情報ツイッターアカウントからもお届けしております。

■東京メトロmy!アプリ
https://www.tokyometro.jp/mobiledevice/smartphone/my/

■各路線の運行情報ツイッターアカウント
銀座線　@G_line_info
丸ノ内線　@M_line_info
日比谷線　@H_line_info
東西線　@T_line_info
千代田線　@C_line_info
有楽町線　@Y_line_info
半蔵門線　@Z_line_info
南北線　@N_line_info
副都心線　@F_line_info

2022年9月7日
東京地下鉄株式会社

出典：東京地下鉄株式会社 掲載

Microsoft社が6月に発表したレポートでは、ロシアはウクライナを支援する42カ国、128の組織に情報窃取などを狙う攻撃をしかけた、としています。今後、ロシア政府やロシア系サイバー集団の攻撃が増える可能性は高く、日本も官民を問わず起きうる攻撃として対策は必要です。

参考情報　国家が支援するサイバー組織によるサイバー事案

PICKUP!

- 出典：「第3節 サイバー領域をめぐる動向」（令和4年 防衛白書 P179 ～184）を加工して作成

  国際戦略研究所（IISS）「サイバー能力と国家能力：ネットアセスメント」https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

各国のサイバー空間における軍隊

ロシア
1,000人

中国
17万5,000人
うち、サイバー攻撃部隊は3万人

北朝鮮
約6,800人

英シンクタンク、国際戦略研究所（IISS）が発表した
各国のサイバー能力評価では最下位グループの日本

日本
540人

米国
6,200人

今年度サイバーセキュリティに関わる予算

日本	米国
約919.3億円 ※概算要求	約1.5兆円 ※軍事予算除く

キルネットは、ロシア政府との関係を指摘されているとの話も。

国家が関与したとされるサイバー事案

ロシア

スパイ活動や攻撃的なサイバー活動を行い、米国は、サイバー上の最大の脅威と認識していると言及。

- 2017年6月、ウクライナを中心に各国でランサムウェア「NotPetya」によるサイバー攻撃
- ジョージア政府機関、報道機関などに対する大規模なサイバー攻撃
- ウクライナ電力網に対するサイバー攻撃
- 平昌オリンピックに対するサイバー活動
- 2020年に東京オリンピック・パラリンピック関連組織に対してもサイバー偵察
- ウクライナの公的機関及び重要インフラに対しサイバー攻撃
- ウクライナ金融機関に対するサイバー攻撃

中国

中国は平素から機密情報の窃取を目的としたサイバー攻撃を行っているとされる。

- 米海軍の潜水艦搭載の超音速対艦ミサイルに関する極秘情報が流出
- 「APT10」が少なくとも12か国に対して知的財産などを標的とするサイバー攻撃を実行。日本においても民間企業、学術機関などを対象とした広範な攻撃
- 米国の消費者信用情報会社から個人情報が窃取
- 新型コロナウイルス感染症のワクチン開発にかかわる企業を含む民間企業などを標的とした知的財産や企業秘密の窃取を目的とするサイバー攻撃
- マイクロソフト社メールサーバーソフトの脆弱性を狙ったサイバー攻撃

米国、日本を含む同盟国が一斉に中国を非難

北朝鮮

2019 から2020 年11 月までに計3 億1,640 万ドル相当を窃取したとされる。

- 金銭を要求するマルウェア「ワナクライ」により、世界150か国以上の病院、学校、企業で被害、14万ドル分のビットコインを窃取。
- 日本の下層通過交換業者「コインチェック」から580億円相当が流出
- 韓国の複数業者から巨額の仮想通過が流出

日本は官民を問わず起きうる攻撃として対策は必要です。

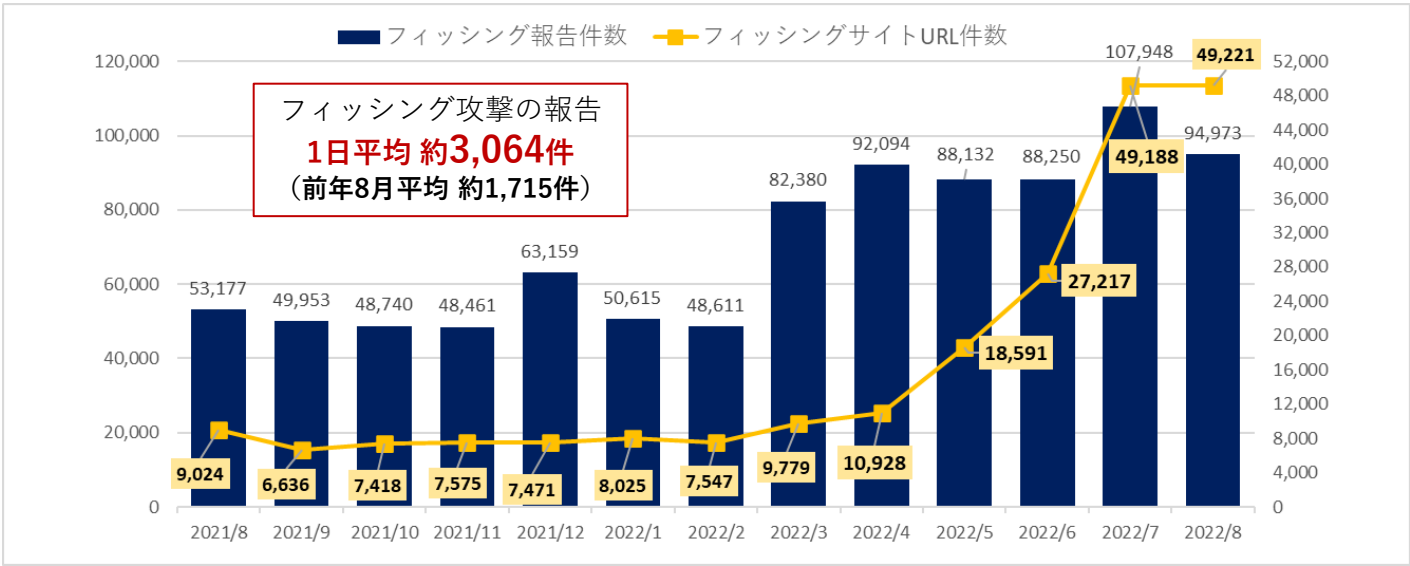
フィッシング急増！報告件数10万件を超える

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は高水準を維持、URL件数が最多更新。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、
引き続き高水準を維持。URL件数は、過去最多を更新。



※2022/08 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09月08日イオンカードをかたるフィッシング
- 2022年09月05日 みずほ銀行をかたるフィッシング
- 2022年08月23日 国税庁をかたるフィッシング
- 2022年08月15日 国税庁をかたるフィッシング
- 2022年08月09日 Google 翻訳の正規 URL から誘導されるフィッシング
- 2022年08月09日 経済産業省 資源エネルギー庁をかたるフィッシング

国税庁をかたるフィッシング

国税庁をかたり、個人情報やVプリカ発行コード番号等の入力を促すフィッシングの報告

メールの件名

未払い税金のお知らせ
【未払い税金のお知らせ】
税務署からの【未払い税金のお知らせ】
【督促状】滞納した税金がございます
【国税庁】最終通知
【国税庁】差押最終通知
<未払い税金のお知らせ>
NV TRUSTカー ドお取引のご確認 番号:M****

※上記以外の件名も使われている可能性があります。

参考情報

【フィッシング対策協議会】
JPCERT/CC が確認したフィッシングサイトの URL を公開
2022/08/31**https://www.antiphishing.jp/enterprise/url.html**

Webサイトのサーバー証明書種類の確認方法（2022/09/06）
https://www.antiphishing.jp/news/info/certificate_checker_20220906.html

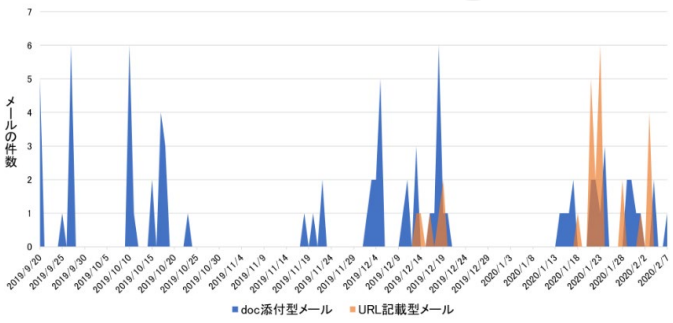
一定の停止期間と活動再開を繰り返す、Emotet引き続き警戒

PICKUP!

- 出典：2022年3月4日　NICTER Blog NICTに届いたEmotetへの感染を狙ったメール（2021年12月～2022年2月） https://blog.nicter.jp/2022/03/topic_emotet_2022/
  2022年5月27日 JPCERT/CC　https://www.jpcert.or.jp/at/2022/at220006.html

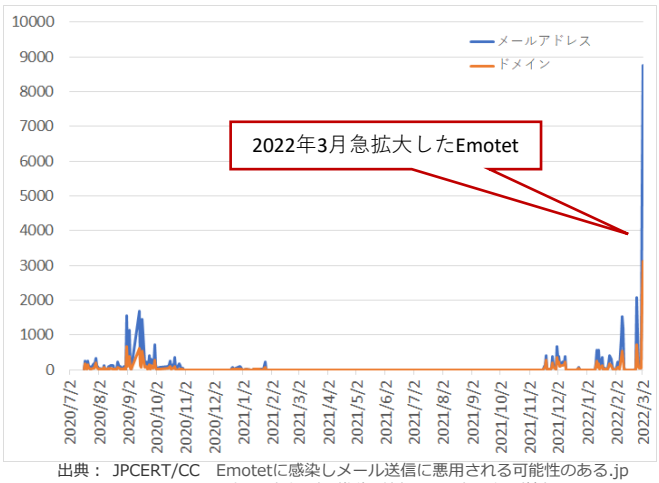
マルウェアEmotetは、例年、一定の停止期間と検知数が活発化する期間を繰り返します。引き続きご注意を！

観測期間　2019年9月～2020年2月



出典：NICTER Blog　NICTに届いたEmotetメールの件数の推移

観測期間　2020年7月～2022年3月



出典：　JPCERT/CC　Emotetに感染しメール送信に悪用される可能性のある.jp メールアドレス数の新規観測の推移 (外部からの提供観測情報)

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