BASIC
Confertas Office

身を守るには
知ることから！

社内回覧用

情報セキュリティ被害の最新事例
2023年2月版

【大切なお願い】
会社を守るため、社長様、幹部様、従業員様、
パソコンやスマホを利用する**皆さまに回覧ください。**
自分事で実態を知ることが対策の第一歩です。

【この冊子の活用の仕方】
この冊子では、セキュリティの最新情報を月刊で
お伝えしています。被害事例を**自社に置き換えて、**
対策と意識向上にお役立てください。

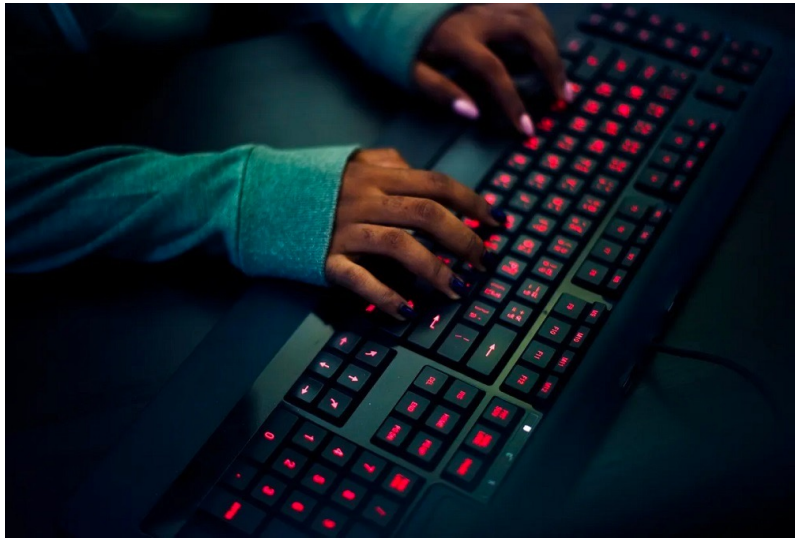
■ランサムウェア被害、前年比57%増（警察庁）

2023年2月2日

・昨年、パソコンなどのデータを暗号化して使えなくし、復元と引き換えに身代金を要求するコンピューターウイルス「ランサムウェア」の被害を受けたとの申告が、その前年対比57%増加していると警察庁が発表した。

・昨年の被害も企業や団体の規模を問わず出ているという。社外から社内ネットワークに接続するVPN機器や、職場のパソコンを遠隔で操作するリモートデスクトップから侵入されるケースが引き続き目立つ。

・警察庁は、パソコンのOSやVPN機器を最新なものに更新するなど、システムの脆弱性を埋める対策をとるよう呼びかけている。



■画像：イメージ（Getty）

ランサムウェアによる被害報告が増えています。依然として脅威を増しているランサムウェアの被害に遭わないよう、メール、Webサイトアクセス、VPN、ルータ、エンドポイント、使用アプリケーション、パスワードなど、総合的なセキュリティ強化が求められていると言えるでしょう。

■出典：朝日新聞デジタル
https://www.asahi.com/articles/ASR223DB1R1ZUTIL04B.html

■ランサム被害の75%は中小企業

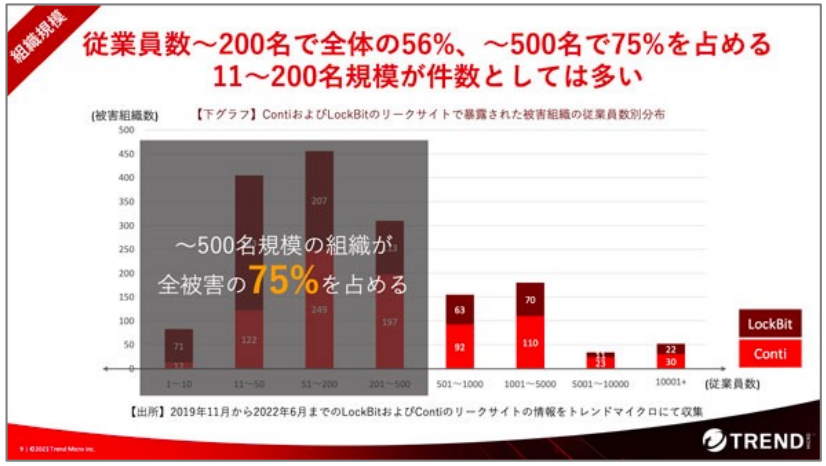
2023年2月14日

・トレンドマイクロは2023年2月、「アンダーグラウンド調査から解明したランサムウェア攻撃グループの実態」と題するリサーチ結果を発表した。

・これによると、ランサムウェアの攻撃傾向から、500人規模の従業員数を持つ組織が全ランサムウェア被害の75%を占めていることが明らかになったとのこと。

・この数字は、ContiとLockbitというランサムウェアグループが公開したリークサイトにおける公表内容を集計したものであるため、信ぴょう性が高いと言えるだろう。

・調査結果からはランサムウェア被害が中小企業に移り、対策が急務となっていることが分かる。



■画像：中小企業がContiおよびLockbitの被害の多くを占めている
（トレンドマイクロ）

今一度、社内のネットワーク環境・PC環境だけでなく、従業員一人ひとりのセキュリティ意識の持ち方にも目を向けてみましょう。決して他人事ではない状況になってきているため、セキュリティに目を向けていく社内の雰囲気を意図的に作っていくことも大切になってくると言えるでしょう。

■出典：ITmedia エンタープライズ
https://www.itmedia.co.jp/enterprise/articles/2302/14/news047.html

BASIC Confertas Office

■Google検索から偽のAWSログインページに誘導。マルバタイジングに注意

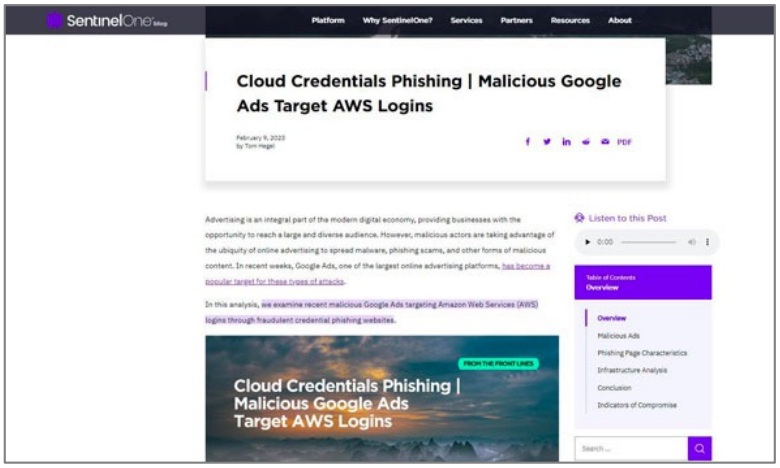
2023年2月11日

・セキュリティ企業のSentinelOneは2023年2月9日、Google広告を利用したマルバタイジングキャンペーンが展開されていると報告した。

・悪意あるWeb広告を利用してユーザーをフィッシング詐欺サイトなどに誘導する手口を「マルバタイジング」と呼ぶ。最近はこのマルバタイジングにGoogle広告が悪用されるケースが増加している。

・特に最近観測されたGoogle広告に偽の「Amazon Web Services」（AWS）ログインページを表示させる手法が取り上げられている。

・今回の手口では、ユーザーが「Google」で「AWS」と検索すると、「AWS - Console - Home Oficial」という悪意ある広告が表示された。ユーザーが勘違いしてこの広告をクリックすると、アクセスしたページから自動的にAWSの偽ログインページにリダイレクトされる。そこで認証コードを入力させようとする手口である。



検索結果に表示されたリンクが安全とは限りません。人の見極めは困難なため、疑わしいWebページへのアクセスは自動で遮断させるセキュリティの仕組みを取り入れましょう。

■画像：SentinelOneによる偽のAWSログインページを表示する攻撃手法についての解説（SentinelOne）

■出典：ITmedia エンタープライズ
https://www.itmedia.co.jp/enterprise/articles/2302/10/news155.html

■イオンカードをかたるフィッシング、件名「【重要なお知らせ】AEON ご利用確認のお願い」などの不審なメールに注意

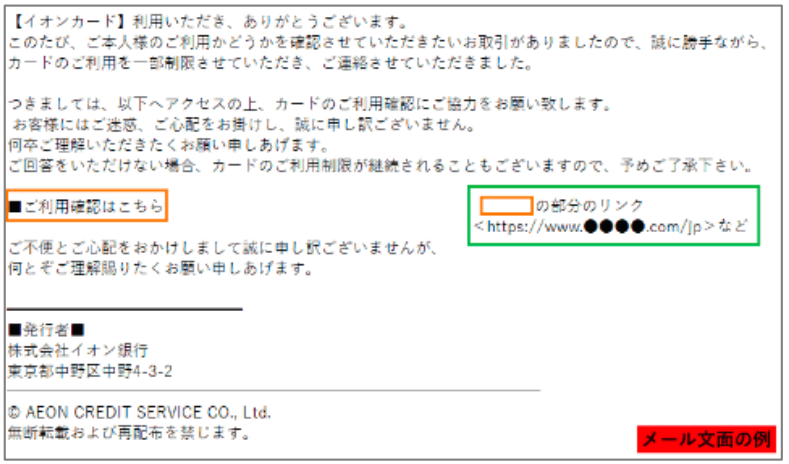
2023年2月21日

・イオンカードをかたるフィッシングの報告が増えているとして、フィッシング対策協議会が情報を公開した。

・フィッシングメールの件名は、以下が確認されている。なお、これ以外の件名も使われている可能性がある。
 -【重要なお知らせ】AEON ご利用確認のお願い
 -【緊急の連絡 】イオンカード ご利用確認のお願い
 -＜緊急通知＞クレジットカードの本人認証サービス（3Dセキュア）が完了しない

・メール本文は、以下の文面が確認されており、カードの利用確認のためとして、リンク先へのアクセスを促している。

・誘導先のフィッシングサイトは、イオンカードの「暮らしのマネーサイト」のウェブサイトを装っており、イオンスクエアメンバーIDとパスワードの入力を求められる。


【イオンカード】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申しあげます。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

■ご利用確認はこちら

の部分のリンク
＜https://www.●●●●.com/jp＞など

ご不便とご心配をおかけしまして誠に申し訳ございませんが、
何とぞご理解賜りたくお願い申しあげます。

■発行者■
株式会社イオン銀行
東京都中野区中野4-3-2

© AEON CREDIT SERVICE CO., Ltd.
無断転載および再配布を禁じます。

メール文面の例

イオンカードを保有している人は多いため、要注意なフィッシングです。保有していない人も、同様の手口は様々なサービス等を騙るため、もちろん油断はできません。

■画像：フィッシングメール文面の例（フィッシング対策協議会）

■出典：INTERNET Watch

■「【差押最終通知】未払い税金お支払いのお願い」などの不審なSMS、関税等お支払いサイト（F-REGI公金支払い）を装うフィッシングに注意

2023年2月22日

・関税等お支払いサイト（F-REGI公金支払い）を装い、Vプリカ発行コード番号などの入力を促すフィッシングの報告を受けているとして、フィッシング対策協議会が情報を公開した。

・SMSの内容は、以下のような複数の文面が確認されており、「差押最終通知」や「重要なお知らせ」といった文言とともに、記載されたURLへアクセスするよう誘導している。

-【差押最終通知】未払い税金お支払いのお願い。ご確認ください。
-■月■日関税局【重要なお知らせ】必ずお読みお知らせ【■■■】。

・誘導先のフィッシングサイトは関税等お支払いサイト（F-REGI公金支払い）を装っており、アクセスすると「差押最終通知」と書かれたメッセージが表示される。確認ボタンをタップすると支払い方法の選択画面に移行する。

税金関係など、より公共性の高い話題に便乗したフィッシングの手口も増えています。十分に注意しましょう。

■画像：フィッシングSMS文面の例（Impress Watch）

■出典：Yahoo!ニュース
https://news.yahoo.co.jp/articles/ead015cfd908b4a06aefa18d8022f7f09c226e1b

■ChatGPTがサイバーセキュリティにもたらす影響

・ChatGPTは、最近、世界的に（日本でも）急速に話題になっている、人工知能（AI）によるチャットボットである。あらゆる質問を打ち込むと、数秒後にはAIが回答を出してくれる。

・世界の言語の中でも非常に難しいと言われる日本語でも、驚くほど自然な日本語で返してくれると話題になっている。

・そんなChatGPTであるが、ChatGPTはコードを書いたり、あるプログラミング言語から別のプログラミング言語へ変換したり、マルウェアを書いたりできることが判明している。

・最近のアップデートによって、APIを使用して悪意のあるコードを開発しようとした場合には、マルウェアのリクエストを拒否するか、安全に関するプロンプトが表示されるようになった。もちろん、この発表後も知恵比べは続き、知恵のある連中はChatGPTを「脱獄」させて、悪事を働き続けられるようにする方法を見出している。

2022年12月13日

■画像：Getty

これからは、攻撃者がAIに書かせた悪意のあるマルウェアによる脅威が増してくる可能性は高いと言えます。最低限施すべきセキュリティ対策の水準を高めましょう。

■出典：Yahoo!ニュース
https://news.yahoo.co.jp/articles/78e9e1d9c7f634ffaeef734c52166b1e2c4e29d5?page=1

情報セキュリティ対策は、実績豊富で信頼できる企業をお選びください。

最近は、ランサムウェアや情報漏えいなど、経営に関わるサイバー攻撃の被害も増加し、ひとつの社会問題となっています。私たちは、「サイバー攻撃の脅威からお客様を守りたい」そして、「今後もお客様と一緒に永く成長していきたい」と強く思っています。

情報セキュリティは、社内ネットワークに関わる重要な部分であり、信頼できる会社と付き合うことが大切です。私たちは、お客様に正確な情報と知識、安心の技術サポートを提供できる体制を整えていますので、ぜひご安心ください。