回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.56

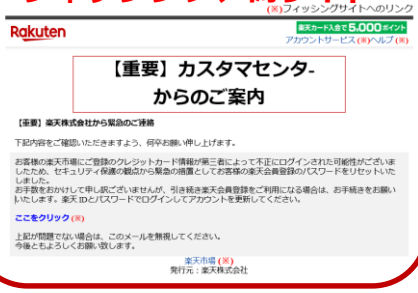
あさまセキュリティニュースレター

オリンピック開催に伴い、激増激化する攻撃に要注意！！　（2020年1月14日）

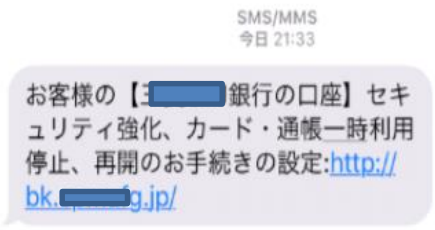
ランサムウェアの金銭要求

新しいランサムウェア
NextCry

フィッシング、偽サイト



偽SMS経由による攻撃



偽アクセスポイントによる個人情報の搾取

オリンピック関連の攻撃

偽チケットサイト
偽のオリンピック動画配信サイト
重要インフラへのサイバー攻撃
インターネット、メール等の障害
政府関係機関のHP改ざん・ダウン等

個人・企業問わず攻撃激増
盗んだ情報を元に、さらなる攻撃も！
知っていれば防げる脅威も多いです！！

攻撃のパターン　おさらい

・取引先からのメールにも要注意！（ただいま激増中、危険度大！！）
実際の取引先とのメールのやり取りに紛れ込んで、不正プログラムを含んだWord・Excel添付ファイルを送る。感染すると、メールアドレス・パスワード搾取、ご自身のメールを悪用され、取引先に同様の手口で感染拡大！！また、今後ランサムウェア等の攻撃にも使われる可能性あり、要注意！！

・フィッシングメールに要注意！
Microsoft、Apple、Google、Amazon、楽天、Yahoo、Line、銀行、カード会社、宅配業者のサービスを装ったメールは本物そっくり！　パスワード使いまわしていると、盗まれたID・パスワードを元に、他サービスでも悪用される危険性！！下記情報源より、常にフィッシングメールの最新情報をご確認ください！

・SMS（携帯番号で送れるショートメッセージ）に要注意！
不正送金被害が急増！銀行や宅配業者を装ったSMSから、不正なアプリのインストールや、個人情報、口座情報の入力させるパターンが急増中！

・フリーWiFiに要注意！
鍵マークのないWiFiは通信内容が丸見え！アクセスしたサイト、入力した文字情報等が搾取・悪用の可能性。各フリースポット、カフェ・ホテルが提供しているフリーWiFiに見せかけた偽のWiFiに接続しているケースも

・ネットワーク機器・IoT機器の脆弱性（ルータ、ネットワークカメラや、インターネットにつながる家電等）
インターネットにつながる機器は、攻撃対象に！被害にあっても気づかないケースも。
今一度設定の見直しを！（ファームウェアアップデート、初期パスワードの変更等）

情報源

IPA　https://www.ipa.go.jp/
フィッシング対策協議会　https://www.antiphishing.jp/　**日本サイバー犯罪対策センター**　https://www.jc3.or.jp/
マルウェア情報局　https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1911.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414