ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●上半期の新型コロナ関連犯罪608件、3分の2が詐欺と不審メール…警察庁発表

https://www.itmedia.co.jp/news/articles/2010/05/news075.html
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf

このニュースをザックリ言うと･･･

- 10月1日(日本時間)、警察庁より、「令和２年上半期におけるサイバー空間をめぐる脅威の情勢等について」と題した広報資料が発表されました。

- 今年上半期(2020年1月～6月)において都道府県警察から報告された「新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案」は608件で、うち「詐欺」が286件で全体の47.0%を占め、次いで「不審メール・不審サイト」が115件(18.9%)等、また「個人情報等不正取得」も55件(9.0%)となっています。

- 新型コロナ関連以外も含めサイバー空間の脅威は引き続き深刻な情勢とされ、例えば同庁が設置する定点観測センサーに対するアクセス観測状況については6,218.1件/日・IPアドレスとなっており、2019年上半期の3,530.8件/日・IPアドレスおよび同下半期の4,842.4件/日・IPアドレスからの上昇傾向が続いている模様です。

AUS便りからの所感等

- 詐欺の例としては「ショッピングサイトでマスクを注文して指定された口座にお金を振り込んだが商品が届かず、出品者とも連絡がとれない」「商品を発注した国外取引会社の社員を名乗る者から『感染症の影響のためいつもの銀行が利用できないので、別の口座に代金を振り込んで欲しい』とメールで依頼があった」、不審メール・サイトの例としては「携帯電話事業者を名乗る者から『政府の要請を受けて給付金を送るので記載されたURLから申請するように』という内容のメールが届いた」といったものが挙げられています。

- 「実在する保健所をかたり、新型コロナウイルス感染症に関する通知が発出されたと称して、添付ファイルを開くよう誘導するメール送信される」事例として挙げられているマルウェアEmotetは、自身を拡散させるメールの文面として、感染したPCから実際に送受信されたメールのものを用いる等、感染の可能性を高める手口を使っています。

- メールの添付ファイル等からのマルウェア感染回避には、アンチウイルスやUTM等による防御はもちろん、単に不審なメールに気を付けるという以上に、このような各企業・機関からの発表をもとに、流行している手口の情報収集や組織内への適宜啓発を行うことが重要となります。

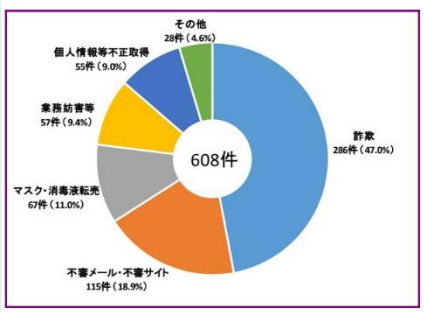
ITmedia NEWS

新型コロナ関連のサイバー犯罪、20年上半期で608件　詐欺や標的型攻撃など多発

2020年10月05日 13時00分 公開　[谷井将人，ITmedia]

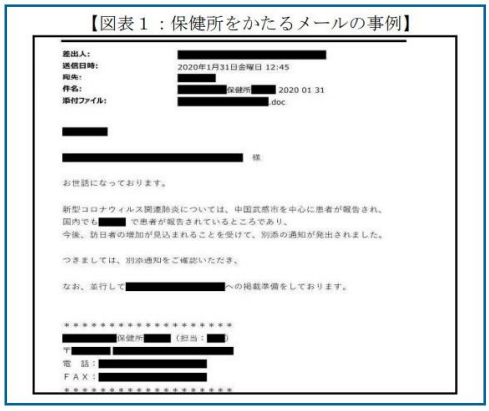
印刷　見る　Share　B!　3

警察庁はこのほど、2020年上半期に起きたサイバー犯罪のうち、新型コロナウイルス感染症に関連するものが608件に上ったと明らかにした。6月末までに各都道府県警察から報告を受けた事案を集計したところ、ECサイトでの詐欺や標的型メールによる攻撃などが多発していたという。



標的型メールの被害では、実在の保健所をかたって「コロナに関して情報があります」とするメールを送り、添付ファイルを開かせてマルウェア「Emotet」などに感染させる手口がみられた。「給付金を送るので記載のURLから申請するように」として不審なサイトに誘導するメールも出回っていた。

【図表１：保健所をかたるメールの事例】



●SBI証券で顧客資金1億円近く流出…「ログインパスワード」「取引パスワード」が同じユーザーが狙われる

https://securitynews.so-net.ne.jp/news/sec_30314.html
https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&came&cat2=corporate&dir=corporate&file=irpress/prestory200916_02.html

このニュースをザックリ言うと･･･

- 9月16日(日本時間)、SBI証券より、顧客の証券口座が不正ログインの被害を受け、同証券の計6口座、約9,864万円分の資産が、ユーザーと同じ名義の偽の銀行口座へ流出していたと発表されました。

- 不正ログインには外部から何らかの方法で取得したとされる「ユーザーネーム」「ログインパスワード」「取引パスワード」等の情報が、出金先の銀行口座は偽造された本人確認書類によって不正に開設されたものが用いられたとしています。

- 9月7日に顧客から身に覚えのない取引があったとの連絡を受け発覚したもので、同証券では不正ログインの恐れが考えられる他のユーザーについても出金停止およびパスワード強制リセットを行った他、出金先口座登録について本人確認を強化する等の再発防止策をとるとしています。

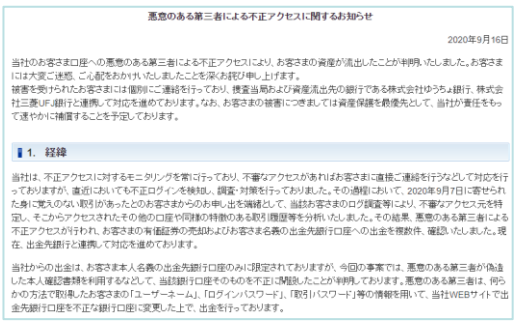
AUS便りからの所感

- 不正アクセスを受けたアカウントは、「ユーザーネーム」が初期設定である口座番号から変更されていなかったことや、本来別の文字列に設定されるべき「ログインパスワード」と「取引パスワード」が同一であった可能性が指摘されています。

- 不正な銀行口座開設のために本人確認書類を偽造するなど決して小規模ではない用意周到な準備が行われたとされ、その過程においても同証券のサイトへの不正ログインで個人情報を取得していたとみられます。

- 現時点で同証券のログインパスワード・取引パスワードは「半角英数6～10文字」とされており(https://search.sbisec.co.jp/v2/popwin/help/system_03_02.html)、より長い文字列や記号が使えない等、攻撃に対して心もとない点は否めず、この点を含め今後の再発防止策における改善に是非とも期待したいものです。

SBI GROUP SBI証券



悪意のある第三者による不正アクセスに関するお知らせ

2020年9月16日

当社のお客さま口座への悪意のある第三者による不正アクセスにより、お客さまの資産が流出したことが判明いたしました。お客さまには大変ご迷惑、ご心配をおかけいたしましたことを深くお詫び申し上げます。
被害を受けられたお客さまには個別にご連絡を行っており、捜査当局および資産流出先の銀行である株式会社ゆうちょ銀行、株式会社三菱UFJ銀行と連携して対応を進めております。なお、お客さまの被害につきましては資産保護を最優先として、当社が責任をもって速やかに補償することを予定しております。

1. 経緯

当社は、不正アクセスに対するモニタリングを常に行っており、不審なアクセスがあればお客さまに直接ご連絡を行うなどして対応を行っておりますが、直近においても不正ログインを検知し、調査・対策を行っておりました。その過程において、2020年9月7日に寄せられた身に覚えのない取引があったとのお客さまからのお申し出を端緒として、当該お客さまのログ調査等により、不審なアクセス元を特定し、そこからアクセスされたその他の口座や同様の特徴のある取引履歴等を分析いたしました。その結果、悪意のある第三者による不正アクセスが行われ、お客さまの有価証券の売却およびお客さま名義の出金先銀行口座への出金を複数件、確認いたしました。現在、出金先銀行と連携して対応を進めております。

当社からの出金は、お客さま本人名義の出金先銀行口座のみに限定されておりますが、今回の事実では、悪意のある第三者が偽造した本人確認書類を利用するなどして、当該銀行口座そのものを不正に開設したことが判明しております。悪意のある第三者は、何らかの方法で取得したお客さまの「ユーザーネーム」、「ログインパスワード」、「取引パスワード」等の情報を用いて、当社WEBサイトで出金先銀行口座を不正な銀行口座に変更した上で、出金を行っております。

●エレコム製ルーターにOSコマンドインジェクション脆弱性、アップデートを

https://news.mynavi.jp/article/20201006-1377051/
https://www.elecom.co.jp/news/security/20201005-01/

このニュースをザックリ言うと･･･

- 10月5日(日本時間)、JPCERT/CCおよびエレコム社より、同社製の無線LANルーター製品の一部に存在するOSコマンドインジェクションの脆弱性について注意喚起が出されています。

- 脆弱性の存在が発表された機種はWRC-2533GST2・WRC-1900GST2・WRC-1750GST2およびWRC-1167GST2で、ルーターの管理画面にアクセス可能なユーザーにより、管理者権限で任意のコマンドを実行され、ルーターを乗っ取られる可能性があるとされています。

- 各機種について脆弱性が修正されたファームウェアがリリースされており、アップデートを行うよう呼び掛けられています。

AUS便りからの所感

- 脆弱性が修正されたバージョンのファームウェアは各機種とも2019年にリリース済みで、また同社によればファームウェアの更新はデフォルトで自動的に行われるとのことですが、該当機種か否かに拘らず、自動更新が停止されている設定等でバージョンが古いままになっていないか確認することを推奨致します。

- PC・サーバーに比べ、ルーターをはじめとするネットワーク機器については、ファームウェアがアップデートされているか、あるいはサポートが終了している機種を使い続けていないかについて見過ごされる傾向がありますので、組織内で導入している全ての機器について把握し管理する体制を整えることが重要です。

マイナビニュース

エレコム製ルータにOSコマンドインジェクション脆弱性、アップデートを

2020/10/06 13:03　　著者：後藤大地

JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）は10月5日、「JVN#82892096: 複数のエレコム製 LAN ルーターにおける OS コマンドインジェクションの脆弱性」において、エレコム製LANルータにOSコマンドインジェクションの脆弱性が存在すると伝えた。

これら脆弱性を悪用されると、影響を受けたシステムにおいてroot権限で任意のOSコマンドが実行されるおそれがある。脆弱性に関する情報は次のページにまとまっている。