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。

●山口県産業技術センターのメールサーバー、設定ミスによりスパムメールの踏み台に

https://www.iti-yamaguchi.or.jp/docs/2020051300018/

このニュースをザックリ言うと･･･

- 5月13日(日本時間)、山口県産業技術センターより、同センターが管理するメールサーバーが4月30日～5月13日の間にスパムメール送信の踏み台として悪用されていたと発表されました。

- 国外から当該サーバーを中継して、ポルトガル語によるスパムメールが送信されていたとのことで、マルウェア感染や情報漏えい等は発生していなかったものの、当該メールサーバーがブロックリストに登録された結果、サーバーから送信された正規のメールが一部相手に受信されないケースが発生していたとのことです。

- 2016年にメールサーバーの更新の際、設定ミスにより外部からの任意のメールを第三者に中継可能になっていたとのことで、対策を行うとともに、以後も関連機器の設定確認やセキュリティ強化等の対応を行うとしています。

AUS便りからの所感等

- メールサーバーのいわゆる「第三者中継(オープンリレー)」はインターネットが広く利用されるようになった90年代から問題視されている古典的なもので、既にIPアドレスによる制限やSMTP認証による対策が一般的となっています。

- 今回のように、サーバーの更新によるセキュリティ設定の漏れ、あるいは何らかの脆弱性が新たに発生することも時々起こり得るため、こういった攻撃手法が存在することを踏まえた上で、第三者機関によるネットワーク診断も含めたチェックを行うことが重要です。

- また、スパムメールやマルウェアメールを拡散しようとする攻撃者が、このような対策を回避するため、不正アクセスやマルウェアを用い、外部への送信が許可された社内LANあるいはメールサーバーを利用するユーザーのPCに侵入することも今や定石となっており、攻撃者やマルウェアの侵入そして外部への不正行為を阻止するために、アンチウイルスやUTMによる防御を行うこともやはり重要です。

地方独立行政法人 山口県産業技術センター
YAMAGUCHI PREFECTURAL INDUSTRIAL TECHNOLOGY INSTITUTE

【お知らせ】山口県産業技術センターのメールサーバによる外部メールの不正中継について

2020年5月13日

令和２年４月３０日（木）から５月１３日（水）までの間、山口県産業技術センター（以下「センター」という。）が管理するメールサーバが、外部から第三者に宛てた電子メールを意図せずに中継していたことが判明しました。

1　状況

悪意のある第三者により、センターが管理するメールサーバが利用され、不特定多数に対して、迷惑メールが送信された。

- 送信数は不明。
- メールは国外のサーバから発信されており、センターのメールサーバを中継して送信された先は、フリーアドレス（HotmailやGmail等）やアドレス末尾の国別コードがブラジルを示す「.br」が多い。
- メールの文面は、ポルトガル語により、広告掲載を勧誘する内容が記載されている。
- 本件によるセンターからの**情報漏洩はなし。**
- センターが管理するメールサーバへのウイルス感染はなし。
- 本件に伴いセンターのIPアドレスが一部の「ブロックリスト（不正中継データベース）」に登録されたため、センターから送信された一部の電子メールが相手に届いていない（現在順次復旧中）。

●日経にサイバー攻撃…社員ら12,514人分の個人情報流出

https://www.nikkei.com/article/DGXMZO58987830S0A510C2CR8000/
https://www.nikkei.co.jp/nikkeiinfo/news/release_20200512_01.pdf

このニュースをザックリ言うと･･･

- 5月12日(日本時間)、日本経済新聞社より、同社および関係者12,514人分の個人情報が流出したと発表されました。
- 被害を受けたのは同社と一部グループ会社・団体の役員・社員・OBおよび業務委託先社員らの氏名・所属・メールアドレスで、同8日に同社従業員が使用するPC1台がメールに添付されたマルウェアに感染したことが流出の原因とされています。
- 同社では、発表時点で個人情報の悪用は確認されていないものの、以後も情報が悪用されていないか監視を続けるとともに、成りすましメールの可能性もあるとして注意を呼びかけるとしています。

AUS便りからの所感

- 取材で得た情報や、読者・顧客の情報は流出しておらず、不審な通信も遮断しており、新聞・電子版作成等のシステムにも影響は生じていないとのことです。
- 同社ではマルウェア検知システムを導入していたものの、感染したマルウェアは検知システムが対応しない新型であったために検知が遅れたとしており、いわゆる「ふるまい検知」型のような新規のマルウェアにも強い検知システムでも見落としてしまうような特徴だったのであれば、今後の改善のためにも、当該マルウェアの詳細について注目したいところです。
- 感染したマルウェアがどのようにして情報を奪取・流出させたかの経緯も不明ですが、例えば権限を持たないユーザーが大規模な情報に直接アクセス可能なシステム・ネットワーク構成となっていないか等について、他社においても適宜確認と見直しを行うべき機会となることでしょう。

NIKKEI

PRESS RELEASE
2020 年 5 月 12 日
株式会社 日本経済新聞社

サイバー攻撃による社員等の個人情報流出について

当社グループ従業員のパソコン 1 台が 5 月 8 日、コンピューターウイルスに感染し、日経本社と一部グループ会社・団体の役員および社員・OB、日経への派遣社員・アルバイト・業務委託先社員の氏名など 1 万 2514 人分の個人情報が流出しました。

流出したのは日経社内のネットワーク端末を使用した社員らの情報で、氏名や所属、メールアドレスが含まれていました。取材で得た情報や日経読者・顧客の皆様に関するデータは流出しておりません。

当社はマルウェア検知システムを導入するなど情報セキュリティー対策を講じてきましたが、当該従業員が受信したメール添付のファイルに新種のウイルスが仕込まれていたため異常の検知が遅れてしまいました。サイバー攻撃で情報が流出したとみています。

● 10万円給付装うフィッシングメールを確認、JC3が注意喚起

https://cybersecurity-jp.com/news/36488
https://www.jc3.or.jp/topics/coronavirus/benefits.html

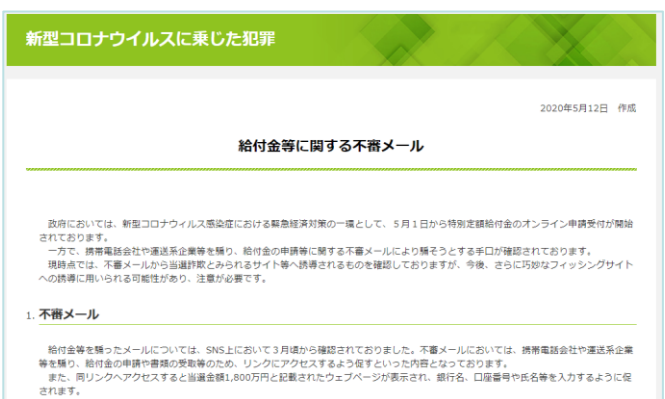
このニュースをザックリ言うと･･･

- 5月12日(日本時間)、日本サイバー犯罪対策センター(JC3)より、同1日からオンライン申請受付が始まった「特別定額給付金」に関連したフィッシングメールが出回っているとして注意喚起が出されています。
- 注意喚起によれば、メールは携帯電話会社や運送系企業等を騙り、給付金の申請や書類の受取等の為にリンクをクリックするよう促すものとなっているとのことです。
- JC3では「給付金に関して、市区町村や携帯電話会社等のメールからURLをクリックさせ申請手続きを求めることはない」とし、不審なメールのURLをクリックしたり、アクセス先で個人情報等を入力したりしないよう呼びかけています。

AUS便りからの所感

- JC3では、フィッシングメールの一例として、本文に「日本国民の皆様に給付金10万円の受け取り資格がございます」「感染拡大防止のため〇〇をご利用のお客様は、上記のURLからお申し込みして頂く事が決定いたしました」等と記載、リンクのアクセス先は「当選金額 金18,000,000円也」と表示され、銀行口座情報を詐取するサイトとなっているものを挙げており、今後、さらに巧妙なフィッシングサイトへの誘導に用いられる可能性もあるとしています。
- 今回の給付金は全国民が対象となり、ネット上以外を含めこれまでにない規模の様々な詐欺行為が行われる恐れがありますので、これまでにどういった手口の詐欺が発生したかを踏まえつつ、政府公式のサイトや信頼のおけるニュースサイトあるいはSNSからの情報を的確に得ながら備えることが肝要です。

JC3 日本サイバー犯罪対策センター
JC3 : Japan Cybercrime Control Center



新型コロナウイルスに乗じた犯罪

2020年5月12日　作成

給付金等に関する不審メール

政府においては、新型コロナウイルス感染症における緊急経済対策の一環として、５月１日から特別定額給付金のオンライン申請受付が開始されております。
一方で、携帯電話会社や運送系企業等を騙り、給付金の申請等に関する不審メールにより騙そうとする手口が確認されております。
現時点では、不審メールから当選詐欺とみられるサイト等へ誘導されるものを確認しておりますが、今後、さらに巧妙なフィッシングサイトへの誘導に用いられる可能性があり、注意が必要です。

1. 不審メール

給付金等を騙ったメールについては、SNS上において３月頃から確認されておりました。不審メールにおいては、携帯電話会社や運送系企業等を騙り、給付金の申請や書類の受取等のため、リンクにアクセスするよう促すといった内容となっております。
また、同リンクへアクセスすると当選金額1,800万円と記載されたウェブページが表示され、銀行名、口座番号や氏名等を入力するように促されます。