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。

●大阪万博協会のメールアカウントに不正アクセス…迷惑メール約63,000件送信

https://www.itmedia.co.jp/news/articles/2010/16/news079.html
https://www.expo2025.or.jp/news/news-20201013/

このニュースをザックリ言うと・・・

- 10月13日(日本時間)、「大阪・関西万博」運営元の2025年日本国際博覧会協会より、同協会のメールアカウントが不正アクセスを受け、外部にフィッシングメールが送信されていたと発表されました。

- 発表によれば、不正アクセスは10月7日・8日に発生し、メールアカウントの一つから国外のメールアドレスに対し約63,000件のフィッシングメールが送信されたとしています。

- 当該メールアカウントのパスワード変更によって迷惑メールの送信は停止しており、個人情報の漏洩や受信トレイへのアクセスは確認されていないとのことですが、外部のセキュリティ専門機関に不正アクセスに至った経緯の調査を依頼しているとのことです。

AUS便りからの所感等

- メールアカウントへの不正アクセスによるフィッシングメールの大量送信は、10月8日にも岡山大学から同様の事案があったことが発表されており(AUS便り 2020/10/19号参照)、このときは安易なパスワードが設定されていたアカウントが狙われています。

- フィッシングメールやマルウェア添付メールの送信は、このようなサーバー上のメールアカウントの不正アクセスの他にも、PCに感染したマルウェアから行われるケースもよく知られ、また今回のメール送信が海外をターゲットにしたものであるのと同様に、日本語の文面メールが海外のPC等を踏み台にして送信されてくるケースも今更珍しいものではなくなっています。

- クライアントPCからの不正なメール送信をアンチウイルスやUTMで防ぐのと同様、サーバー上のメールアカウントについても、適切なパスワードの設定や、不正ログインおよび不正なメール送信を遮断する機構の導入が推奨されます。

ITmedia NEWS

大阪万博協会に不正アクセス、フィッシングメール6万件超送信

2020年10月16日 10時50分 公開　[ITmedia]

印刷　見る　Share　B!　4

2025年の「大阪・関西万博」を運営する2025年日本国際博覧会協会はこのほど、10月7日～8日にかけて外部から不正アクセスを受け、同協会のメールアカウントのうち1つから約6万3000件のフィッシングメールが国外のメールアドレスに送信されたと発表し、謝罪した。

対象のメールアカウントは、問題が発覚してすぐにパスワードを変更し、フィッシングメールの送信は止まったという。

問題のアカウントの受信トレイにアクセスされた痕跡はなく、情報漏えいなどの二次被害も確認していないが、不正アクセスの経緯などは、外部の情報セキュリティ専門機関に調査してもらっている。

公益社団法人2025年
日本国際博覧会協会

お知らせ

HOME ＞ ニュース ＞ お知らせ ＞ 【お詫びとお知らせ】協会メールアカウントへの不正アクセスによる国外へのフィッシングメール送信について

2020.10.13

【お詫びとお知らせ】協会メールアカウントへの不正アクセスによる国外へのフィッシングメール送信について

平素は格別のご高配を賜り、誠にありがとうございます。
2020年10月7日（水）から翌8日（木）にかけて、外部からの不正アクセスによって、当協会のメールアカウントの一つから、約6万3千件のフィッシングメールが国外のメールアドレスに向けて送信されるという事案が発生しました。関係者の皆さまにご迷惑、ご心配をおかけすることになりましたことを深くお詫び申し上げます。

当該メールアカウントについては事案の発生確認後、速やかにパスワードを変更し、フィッシングメールの送信は停止しております。

●Windowsの脆弱性「Zerologon」、ランサムウェア「Ryuk」による悪用も

https://www.itmedia.co.jp/news/articles/2010/26/news057.html
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

このニュースをザックリ言うと・・・

- 10月26日(日本時間)、ITMedia NEWSにおいて、9月に発表されたWindowsの重大な脆弱性「Zerologon」がランサムウェアに悪用されているとするレポートが取り上げられています。

- 10月18日のDFIR Reportの報告によれば、2019年に発生したランサムウェア「Ryuk」がZerologonを悪用した攻撃を行っており、発端となったフィッシング詐欺メールが送りつけられてから、わずか5時間で被害者のネットワーク全体が暗号化される事例があったとのことです。

- この事例では、最初に権限を持たないユーザーがマルウェア「Bazar」に感染し、そこからZerologonによって特権を獲得してドメインコントローラ(DC)のパスワードをリセット、さらに別のDCも乗っ取っていき、サーバーやクライアントPCを次々にRyukに感染させていったとしています。

AUS便りからの所感

- Zerologonは9月に発表された(AUS便り 2020/09/28号参照)時点で、DC自体およびDC管理下のPCの乗っ取りが可能な非常に危険度が高い脆弱性とされ、米国土安全保障省(DHS)のセキュリティ機関CISAが8月リリース済みのセキュリティパッチを適用するよう全土に緊急指令を出す事態となっています。

- Zerologonの悪用には前段として、攻撃者が別の手段でDCにアクセス可能なネットワーク上に侵入する必要がありますが、その手段としてフィッシング詐欺やマルウェアを組合せることによる攻撃の可能性は、先の発表の時点で時間の問題だったと言えます。

- 企業・組織等、Active DirectoryでPC・アカウントを管理している所で、8月にリリースされたパッチを万が一にも意図せず適用していない状態になっていないか、今からでも関連する全てのサーバーについて確認することが肝要ですし、一旦感染したマルウェア・ランサムウェアの「横感染」等を抑止できるようUTM等を用いた安全なネットワーク構成とすることも是非検討されることが重要です。


ITmedia NEWS

この頃、セキュリティ界隈で：

ランサムウェアが見せつけたWindowsの脆弱性「Zerologon」の威力 (1/2)

2020年10月26日 07時02分 公開　[鈴木聖子，ITmedia]

印刷　通知　見る　Share　B! 30

Windowsのドメインコントローラが乗っ取られる極めて深刻な脆弱性「Zerologon」について、Microsoftやセキュリティ企業が繰り返し警戒を呼び掛けている。ランサムウェア「Ryuk」の攻撃に利用されて瞬く間に組織内で感染が広がった実例も紹介され、改めて危険性が浮き彫りになった。

Zerologonの脆弱性は、WindowsでActive Directoryのユーザー認証に使われる「Netlogonリモートプロトコル」（MS-NRPC）に存在する（CVE-2020-1472）。悪用された場合、認証を受けていない攻撃者がドメインコントローラにアクセスし、ドメイン管理者権限を取得できてしまう可能性がある。Microsoftは8月の月例セキュリティ更新プログラムでこの問題に対処した。

●ダイソン等を騙る偽ECサイト、消費者庁が注意喚起

https://www.itmedia.co.jp/news/articles/2010/22/news076.html
https://www.caa.go.jp/notice/entry/021659/

このニュースをザックリ言うと・・・

- 10月21日(日本時間)、消費者庁より、「実在の通信販売サイトをかたった偽サイトなどに関する注意喚起」が出されています。

- 注意喚起では大きく3種類の偽サイトが取り上げられており、掃除機等で知られる「ダイソン」と家具の販売サイト「LOWYA」の偽サイトが挙がっています。

- この他に、既存のブランド・サイト名ではない「特価用品専門店」という屋号を用い、衣料品・家電製品・化粧品・生活雑貨等を通信販売しているかのように装っているサイトも存在し、注意喚起されています。

- これらのサイトで代金を支払っても、商品が届かない、あるいは注文していない商品が届き、サイトに記載されているメールアドレスに連絡してもまともな返信が返らない等の問題が報告されているとのことです。

AUS便りからの所感

- 偽サイトは、サーチエンジンで商品の種類や型番などを検索した際の「リスティング広告」として、あるいはSNSの広告として表示され、アクセスするよう誘導する模様です。

- ダイソン・LOWYAの偽サイトは実際のサイトから画像・文章の盗用等巧妙な模倣を行っているとされ、また「特価用品専門店」も他の通信販売サイトから商品の画像や文章を盗用しているとみられています。

- 注意喚起のページからダウンロードできる資料PDFには偽サイトの詳細な特徴や判明しているURL等の情報が掲載されており、このような偽サイトやサイトへの誘導が発生しているという情報をもとに各々が行動、あるいは社内等への啓発を行って頂ければ幸いですが、一方で資料にないURLの偽サイトや新たな手口が発生する可能性にも十分に注意を払う必要があるでしょう。


ITmedia NEWS

ダイソンかたる偽サイト、消費者庁が注意喚起　商品が届かないなど被害相次ぐ

2020年10月22日 11時30分 公開　[谷井将人，ITmedia]

印刷　見る　Share　B! 2

消費者庁は10月21日、ダイソンをかたる偽のECサイトを通じて注文した商品が届かないなどの相談が相次いでいることから、消費者に注意を呼びかけた。公式サイトから商品の画像や文章をコピーしており、偽サイトと気付くのは困難だという。