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。

●NISCと気象庁、相次いで不正アクセス…メールセキュリティ機器へのゼロデイ攻撃

https://www.asahi.com/articles/ASR8545P7R84ULZU009.html
https://www3.nhk.or.jp/news/html/20230805/k10014153901000.html
https://www.nisc.go.jp/news/20230804.html
https://www.jma.go.jp/jma/press/2308/04a/press_security_20230804.html
https://www.mandiant.jp/resources/blog/barracuda-esg-exploited-globally

このニュースをザックリ言うと･･･

- 8月4日(日本時間)、内閣官房内閣サイバーセキュリティセンター(NISC)と気象庁より、それぞれ電子メール関連システムが2022年から不正アクセスを受け、情報が漏洩していた可能性があると発表されました。

- 発表および一部報道によれば、 NISCについては、6月13日に不正通信の痕跡を発見、同14～15日に原因とされる機器を交換しており、2022年10月～2023年5月の間にNISCとやり取りをした約5,000人分の個人情報を含むメールデータの漏洩が発生していたとみられています。

- 気象庁については、6月2日に保守管理委託業者からの連絡で発覚したとされ、こちらも2022年6月～2023年5月の間、受信したメールデータの一部(件名・本文・アドレス・添付ファイル等)が漏洩していたとのことです。

- いずれもメールセキュリティ機器の脆弱性をパッチがリリースされる前から悪用していた、いわゆる「ゼロデイ攻撃」とされています。

AUS便りからの所感等

- ターゲットとされたのはBarracuda社のアプライアンスEmail Security Gateway(ESG)の脆弱性(CVE-2023-2868)とみられており、同社から5月21日にセキュリティアップデートがリリースされている一方、セキュリティ企業Mandiant社が6月に発表したレポートによれば、2022年10月の時点で、攻撃者グループ「UNC4841」がこの脆弱性を悪用したゼロデイ攻撃を全世界で行っていたとのことです。

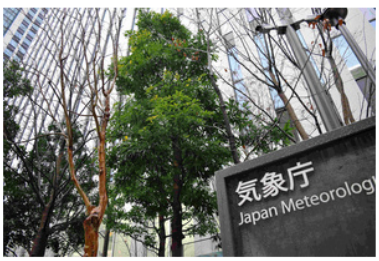
- 脆弱性の内容は、細工された添付ファイルを送信することにより、ESG上で指定したスクリプトを実行することが可能なものとされ、外部のサーバーから不正なプログラムをダウンロードしてバックドアを仕掛けていたと推測されています。

- 今日においてゼロデイ攻撃はもはや珍しいものではなく、特にUTMやセキュリティアプライアンスに対するゼロデイ攻撃に管理者・ユーザー側で防御することは困難であることを鑑み、少なくとも一つの防御手段が突破された場合でも情報流出を食い止められるよう多層防御を採用することは念頭に置くべきでしょう。

朝日新聞 DIGITAL

NISCにサイバー攻撃、メールデータ5千人分流出か　気象庁も被害

編集委員・須藤龍也　2023年8月5日 13時30分



気象庁

政府の内閣サイバーセキュリティセンター（NISC）は4日、電子メールシステムが サイバー攻撃 を受け、約5千人分の個人情報を含むメールのデータが外部に流出した可能性があると発表した。NISCと取引のある民間企業や協力組織が被害を受けた可能性があるという。

発表によると、流出した可能性があるのは、昨年10月から今年6月までの間に、インターネットを経由してNISCとメールのやりとりをした個人や組織のメール。該当者約5千人には4日までにメールで通知した。政府の 個人情報保護 委員会には報告済みという。

●7月度フィッシング報告件数は117,024件、5月度の水準に戻るも過去2位の多さ

https://www.antiphishing.jp/report/monthly/202307.html

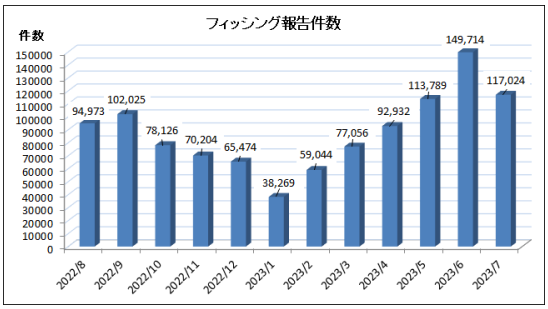
このニュースをザックリ言うと・・・

- 8月4日(日本時間)、フィッシング対策協議会より、7月に寄せられたフィッシング報告状況が発表されました。
- 7月度の報告件数は117,024件で、6月度(https://www.antiphishing.jp/report/monthly/202306.html)の149,714件から32,690件減少しています。
- フィッシングサイトのURL件数は21,585件で6月度(23,420件)から1,835件減少、悪用されたブランド件数も93件で6月度(107件)から14件減少となっています。
- 最も多く悪用されたブランドはAmazon(全体の約31.0%)で、以下三井住友カード・イオンカード・セゾンカード・クロネコヤマト・JALを合わせた5ブランドで全体の約63.5%、また1,000件以上の報告があった19ブランドで全体の約92.6%を占めたとしています。

AUS便りからの所感

- 報告件数は5月度(https://www.antiphishing.jp/report/monthly/202305.html)の113,789件に近い水準に立ち戻ったものの、過去最高だった先月度に次ぐ多さを維持しています。
- 同協議会では、件数の減少について、特定の海外クラウドサービスからのフィッシングメール配信が7月中旬に減少したためとしている一方、金融系ブランドを騙るフィッシングの報告が先月度に比べ31.6%増加したとしており、確認されているフィッシングメールも、実際の注意喚起等の文面や正規ドメインを不正に利用するなりすましを行っており、受信者自身では判断しづらいものとなっているとしています。
- 同協議会の調査用メールアドレスへ配信されたフィッシングメールについて、約87.8%が中国の通信事業者からの配信(6月度約94.8%)、また約97.6%がDNS逆引き設定(IPアドレスに対しドメイン名を設定)がされていないIPアドレスからの送信(6月度約99.7%)とされているものの、該当するメール配信等の遮断だけでフィッシングへの対策とすべきではなく、SPF・DMARC等対策機構の採用を是非とも検討してください(SPF・DMARCもまた単に採用・設定して終わりではなく、メールサーバー構成の変更時あるいはレポートの分析をもとにしてのポリシーの調整もまた重要です)。

フィッシング対策協議会 Council of Anti-Phishing Japan



●「夏休みにおける情報セキュリティに関する注意喚起」IPAから発表

https://www.ipa.go.jp/security/anshin/heads-up/alert20230803.html

このニュースをザックリ言うと・・・

- 企業・組織によっては長期休暇となるお盆の時期を迎えるにあたり、8月3日(日本時間)、IPAより、「夏休みにおける情報セキュリティに関する注意喚起」が発表されました。
- 長期休暇の時期は、システム管理者が長期間不在になる等「いつもとは違う状況」になりがちであるとし、ウイルス感染・不正アクセス等セキュリティインシデント発生時の対処が遅れたり、思わぬ被害が発生したりして、休暇明けにおける業務継続にも影響が及ぶ可能性があるとしています。
- IPAでは「長期休暇における情報セキュリティ対策(https://www.ipa.go.jp/security/anshin/measures/vacation.html)」と題した、「企業・組織システムの管理者」「システムの利用者」それぞれを対象とした「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得、また「(SNS等を利用する)個人」としての立場での注意事項についてまとめています。

AUS便りからの所感

独立行政法人 情報処理推進機構

- 注意喚起の内容の殆どはゴールデンウィーク時に出されたものと大きく異なるようなものではありませんが、インターネット境界に設置された装置の脆弱性を突いた攻撃について8月1日にIPAが出した注意喚起(https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html)に言及されています。
- この他にも、リモートデスクトップサービス(RDP)の不正ログインやサポート詐欺、ランサムウェアによるサイバー攻撃に関する相談が多く寄せられているとのことです。
- 休暇までに日にちがなく十分な対応が間に合わなかったとしても、お盆明け以降に点検すべきことは多く存在しますし、以後も年末年始・ゴールデンウィーク等に備えて対応しておくべき事柄も変わらず、また長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策(https://www.ipa.go.jp/security/anshin/measures/everyday.html)」として別途まとまっており、それぞれにおいて準備・点検を行うよう意識していくことが肝要です。


夏休みにおける情報セキュリティに関する注意喚起

最終更新日：2023年8月3日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人がお盆休みや夏休みなどの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生したり、長期休暇後の業務継続に影響が及ぶ可能性があります。

これらのような事態とならないよう、(1)企業や組織の管理者、(2)企業や組織の利用者、(3)個人の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。

長期休暇における情報セキュリティ対策

また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

日常における情報セキュリティ対策

被害に遭わないためにもこれらの対策の実施をお願いします。

ランサムウェアによるサイバー攻撃被害に関する相談や報告が企業や組織から寄せられています。
インターネットに接続された機器・装置類に対し、脆弱性の悪用などが原因による外部からの不正アクセス事案が報告されています。
リモートデスクトップサービス（RDP）の認証を突破されたり、VPN装置のアップデートが行われておらず侵入されたという事例が多くあります。
インターネットからアクセス可能な装置全体について、アクセス制御が適切にできているか、認証が突破される可能性はないか、脆弱性は解消されているかといった点を、今一度確認することを推奨します。