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。

●既に使用されていないWebページが攻撃…ユーザー等情報最大83万件流出か

https://www.itmedia.co.jp/news/articles/2405/24/news180.html
https://www.sekisuihouse.co.jp/company/topics/library/2024/20240524_1/20240524_1.pdf

このニュースをザックリ言うと･･･

- 5月24日(日本時間)、積水ハウス社より、同社会員サイト「積水ハウス Net オーナーズクラブ」が不正アクセスを受け、会員や従業員のメールアドレス等の情報が流出した可能性があると発表されました。

- 流出が確認されたのは、当該サイト会員のメールアドレスとアカウント情報108,331人分(この他漏えいの可能性を否定できないもの464,053人分)、および同社グループないし協力会社スタッフ等のメールアドレスと社内システムログイン用パスワード183,590人分(この他漏えいの可能性を否定できないもの72,194人分)で、被害を受けた可能性がある情報は最大のべ828,168人分とみられます。

- 2008年～2011年に使用、現在は使用されていなかったWebページのセキュリティ設定に不備があり、同21日に当該ページへの不正アクセスを受けたことが情報流出に繋がったとされています。

AUS便りからの所感等

- 発表では不正アクセスの原因を「データベースを操作するための言語を用いたサイバー攻撃」としており、SQLインジェクションの脆弱性を悪用された可能性があります。

- SQLインジェクションは近年でもECサイトからの情報流出等の原因として挙げられることがありますが、問題となったページが開設された2008年当時には攻撃によるWebサイトの改ざんが頻発し、セキュリティ企業等から注意喚起が出されていました。

- Webアプリケーション開発の時点で、SQLインジェクションをはじめサーバーへの侵入や情報流出等に繋がる脆弱性が可能な限り入り込まない体制をとること、自社や第三者機関でのセキュリティ診断実施による脆弱性等の発見・対策を行うこと、またWAF・IDS・IPSの採用による攻撃の検知・遮断の検討が肝要であり、またWebサイト全体の管理において既に使用されていないコンテンツやページの棚卸しと削除を行うことも、攻撃の余地を残さない意味でセキュリティ対策の一環として考慮に値するでしょう。

ITmedia NEWS

積水ハウスにサイバー攻撃　約30万件の情報漏えい、パスワードも　流出疑いも50万件超【追記あり】

2024年05月24日 17時50分 公開　　[吉川大貴，ITmedia]

積水ハウスは5月24日、住宅オーナー向けの会員制サイト「積水ハウス Net オーナーズクラブ」で情報漏えいがあったと発表した。会員・従業員のメールアドレスやパスワードなど30万件近くが漏えいした他、これとは別に50万件超の情報が漏えいした可能性も否定できないという。

漏えいした情報は、サイト会員10万8331人のメールアドレス、ログインID、パスワード。過去に在籍していた人を含む積水ハウスグループの従業員や協力会社スタッフなど18万3590人のメールアドレスと、社内システムにログインする際に使うパスワードも漏えいした。これとは別に、会員46万4053人のメールアドレス、ログインID、パスワードと、従業員や協力会社のスタッフなど7万2194人のメールアドレス、パスワードも、漏えいの可能性が否定できないという。

● Windowsの「クイック アシスト」を悪用するサポート詐欺、MSが注意喚起

https://forest.watch.impress.co.jp/docs/news/1591899.html
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

このニュースをザックリ言うと･･･

- 5月15日(現地時間)、マイクロソフト(以下・MS)より、Windowsに標準搭載されている「クイック アシスト」を悪用したソーシャルエンジニアリング攻撃が4月以降確認されているとして注意喚起が出されています。

- いわゆる「サポート詐欺」の一種で、IT担当者・ヘルプデスク担当者になりすました攻撃者が電話口でクイック アシストの実行等を指示する等により、PCに不正なツールやランサムウェア「Black Basta」をインストールさせるとしています。

- 同社では、クイック アシストをはじめリモート管理ツールを使用していない場合はブロックやアンインストールすること、サポート詐欺から身を守るための教育を行うこと、クイック アシストでの接続を許可する相手はMSのサポートやITサポート担当者に直接連絡してやり取りできる場合に限ること、遠隔操作中に不審な行為があった場合はセッションを切断し警察や社内の関連部署に連絡することを呼び掛けています。

AUS便りからの所感

- クイック アシスト自体にセキュリティ上の問題があるというのではなく、Windowsに最初から入っているツールであることから攻撃者が使用しているものと考えられ、サポートのために外部からPCを操作してもらうために用いられる他のツール(TeamViewer等)でも、身元が不明な相手から使用するよう指定され、サポート詐欺に悪用される可能性はあります。

- サポートを申し出てくる相手が信頼できるか事前に確認すること、またサポート詐欺への呼び水となるような不審な画面表示が悪意のある広告やデスクトップ通知等から行われること等攻撃の手口を熟知しつつ、慎重に行動することが重要です。

Impress Watch

Windows 10/11の「クイック アシスト」を悪用した攻撃、Microsoftが注意喚起

金銭目的のリモートヘルプ詐欺に注意

樽井 秀人　2024年5月16日 10:29

Windows 10/11標準のリモートアシスタントツール「クイック アシスト」を悪用したソーシャルエンジニアリング攻撃が確認されているとのこと。米Microsoftが5月15日（現地時間）、公式ブログ「Microsoft Security Blog」でその詳細を解説している。

この攻撃は2024年4月中旬以降、「Storm-1811」と呼ばれているサイバー犯罪グループによって行われている。このグループは金銭を騙し取るため、さまざまな方法でユーザーをだまし、最終的に「Black Basta」ランサムウェアなどの悪意のあるツールをインストールさせる。その手口の一つとして、「クイック アシスト」が悪用されているという。

●非Miraiボットネットが日本国内で形成か…JPCERT/CC定点観測レポート

https://scan.netsecurity.ne.jp/article/2024/05/14/50987.html
https://www.jpcert.or.jp/tsubame/report/report202401-03.html
https://blog.nicter.jp/2024/05/nicter_statistics_2024_1q/

このニュースをザックリ言うと･･･

- 5月2日(日本時間)、JPCERT/CCより、同組織がインターネット上で運営する観測用センサーによる2024年1～3月の定点観測レポートが発表されました。

- 国内で観測されたパケットの宛先ポートに最も多く指定されていたのはTCPポート23番(Telnetで使用)、以下6379番(Redis)、22番(SSH)、80番(HTTP)、3389番(リモートデスクトップ)となっています。

- 国別の送信元としては最も多かったのがアメリカ、以下ブルガリア、オランダ、中国、ロシアとなっており、ブルガリアやオランダが2月に入ってパケットが増加していたとしています。

- Telnetポート宛パケットについては、Miraiによるものとは別に、Miraiの特徴を持たないパケットも観測されており、日本国内でMirai以外の独自のボットネットを形成しているものと推測されています。

AUS便りからの所感

- 5月14日には情報通信研究機構(NICT)運営の「NICTER」プロジェクトからも同様の定点観測レポートが発表されており、こちらでも非Miraiのボットネットについて言及されています(2023年後半から活動している「InfectedSlurs」によるもの としています)。

- オンプレミス(社内・データセンター上)・クラウドに拘わらず、設置したホスト上の各種サーバープログラムに対し意図しないアクセスを受けることのないよう、OS自体および外側のルーター・UTM等のパケットフィルタリング機能を確実に設定し、加えて不審なパケットを監視する仕組みも用意し、攻撃から防御できるよう備えることが重要です。

ScanNetSecurity

2024.5.14 Tue 8:00

日本国内では Mirai と別のマルウェアが独自ボットネット形成、2024年第1四半期 インターネット定点観測レポート

一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は5月2日、インターネット定点観測レポート（2024年 1～3月）を発表した。

2024年1～3月のポート番号宛のパケット観測数トップ5の推移

全 4 枚

拡大写真

一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は5月2日、インターネット定点観測レポート（2024年 1～3月）を発表した。

JPCERT/CCでは、インターネット上に複数の観測用センサーを分散配置し、特定の機器・サービス機能を探索するために行われていると推測される一定のIPアドレス帯に向けて網羅的に発信されるパケットを観測しており、これらパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類し、脆弱性情報やマルウェア、攻撃ツールの情報などと対比し分析することで、攻撃活動や準備活動の捕捉に努めている。