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。

●親露攻撃者集団によるとみられるサイバー攻撃多発…政府機関等Webサイトにてアクセス障害

https://www.itmedia.co.jp/news/articles/2209/06/news174.html
https://www.itmedia.co.jp/news/articles/2209/08/news215.html
https://www3.nhk.or.jp/news/html/20220907/k10013806691000.html
https://piyolog.hatenadiary.jp/entry/2022/09/07/025039

このニュースをザックリ言うと･･･

- 9月6日(日本時間)、ロシアを支持しているとされる攻撃者集団より、日本国内の政府機関やWebサービスへのサイバー攻撃が宣言され、攻撃による被害の発生が報告されています。
- 「KILLNET」を名乗る攻撃者集団は9月6日、メッセージアプリ「Telegram」上において、デジタル庁が運営する「e-Govポータル」および地方税ポータルシステム「eLTAX」のサイトをオフラインにさせたと宣言、のちそれぞれのサイトにおいて、アクセス障害が発生していたことが発表されています。
- KILLNETはこの他にも、同6日から7日にかけて、JCB・mixi・名古屋港管理組合・東京メトロおよび大阪メトロに対し攻撃をかけてアクセス障害を発生させており、「日本政府全体に宣戦布告」等とする動画も投稿していたとのことです。
- 同8日に松野官房長官が会見を行い、政府機関サイトでの被害は4省庁23サイトに上るとされていますが、情報漏洩は確認されていないとのことです。

AUS便りからの所感等

- 各報道においてデジタル庁等が取材に答えたところでは、今回行われた攻撃はいずれもDDoS攻撃とみられています。
- 一方でKILLNETとの関連は不明ですが、ロシアからとみられるSQLインジェクション攻撃が9月4日に通常の3倍観測されたとする発表もあります(https://www.itmedia.co.jp/news/articles/2209/13/news136.html)。
- 今後行われる攻撃が今回のようなDDoS攻撃のみか、情報漏洩やマルウェア拡散等を目的としたものに発展するか、あるいは中小企業も含め無差別にターゲットとされる可能性はあるか、全くの未知数であり、あらゆる攻撃の可能性を想定し、UTMの導入等を含めた各種防御策を各組織において検討頂くことを強く推奨致します。

ITmedia NEWS

政府運営「e-Gov」などにサイバー攻撃か　ロシア支持のハッカー集団「KILLNET」が声明　mixiやJCBへの攻撃にも言及

2022年09月06日 21時49分 公開　[松浦立樹，ITmedia]

ロシアを支持しているというハッカー集団「KILLNET」は9月6日、日本政府運営の行政情報の総合窓口サイト「e-Gov」などのWebサービスにサイバー攻撃を行ったと、メッセージアプリ「Telegram」上に投稿した。

「宣戦布告もその後の攻撃も知っている」　松野官房長官、KILLNET声明に言及

2022年09月08日 18時00分 公開　[ITmedia]

ロシアを支持するハッカー集団「KILLNET」が日本政府に宣戦布告した問題を巡り、松野博一官房長官は9月8日の会見で「（同集団が）宣戦布告のあと、東京メトロ、大阪メトロを攻撃したとしているのは承知している」と話した。

● Officeファイルのマクロ実行ブロック強化が展開、回避策実行は慎重に

https://forest.watch.impress.co.jp/docs/serial/yajiuma/1437540.html
https://togetter.com/li/1938662
https://officesupportjp.github.io/blog/cl0m4f5o1003504vsa5tp25c2/
https://faq.mypage.otsuka-shokai.co.jp/app/answers/detail/a_id/314030/

このニュースをザックリ言うと・・・

- 8月30日頃(日本時間)より、Officeファイル(Word・Excel等)におけるマクロの実行がブロックされるようになったという報告がTwitter上などで相次いでいます。

- マイクロソフト(以下・MS)では、インターネットからダウンロードしたOfficeファイル上でのマクロ実行をデフォルトでブロックする措置を既に実行しており(AUS便り 2022/08/02号)、マクロが実行できない「保護ビュー」でファイルが開かれた場合に「編集を有効にする」ボタンのクリックでマクロを実行可能にできる回避策が、一部のケースでは実行できないようになります。

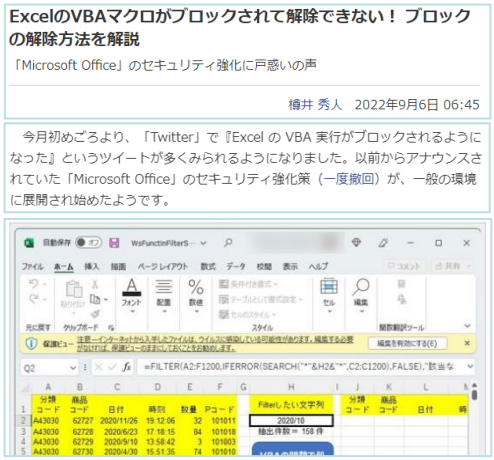
- 今回、このセキュリティが強化された設定が広範囲に展開されたとみられ、ネットメディア等でも取り上げられるとともに、この場合でもブロックを回避する正式な方法も各所で紹介されています。

AUS便りからの所感

- 今回の措置では、特に「¥¥192.168.*.*¥share¥file.xlsm」のようにIPアドレスで指定したサーバー下のファイルを直接開こうとした場合、「編集を有効にする」ボタンをクリックしても警告が表示され、マクロの実行が完全にブロックされる挙動となっていることが確認されています。

- ブロックを回避する方法は前述のとおり正式な方法があり、例えば「ファイルのプロパティにおいてセキュリティに関する注意書きの横にある『許可する』にチェックを入れて『OK』をクリックする」等いくつか存在します。

- ブロック措置が実行されたことにより、攻撃者がマクロを悪用する攻撃は減少した一方、このようなブロックを回避してOfficeファイルを開かせ、不正なプログラムを実行させるような手法に転じているとするセキュリティベンダーの報告もあるため、Officeファイルを開く際には、ウイルススキャンの実施を含め、くれぐれも安全なファイルであることを確認した上で実行することが重要です。


ExcelのVBAマクロがブロックされて解除できない！ ブロックの解除方法を解説
「Microsoft Office」のセキュリティ強化に戸惑いの声
樽井 秀人　2022年9月6日 06:45
今月初めごろより、「Twitter」で『Excel の VBA 実行がブロックされるようになった』というツイートが多くみられるようになりました。以前からアナウンスされていた「Microsoft Office」のセキュリティ強化策（一度撤回）が、一般の環境に展開され始めたようです。

● QNAP社製NASの脆弱性を悪用しデータを暗号化するランサムウェア…アプリケーション更新呼びかけ

https://gigazine.net/news/20220908-data-destroying-ransomware-qnap-nas/

このニュースをザックリ言うと・・・

- 9月3日(現地時間)、NAS大手のQNAP社より、同社製NASのデータを暗号化するランサムウェア「DeadBolt」による攻撃について注意喚起が出されています。

- DeadBoltによる攻撃はは1月の時点で確認され、同社からも警告が出ていましたが、今回はQNAPの写真管理アプリケーション「Photo Station」の脆弱性を悪用した攻撃が確認されたとしています。

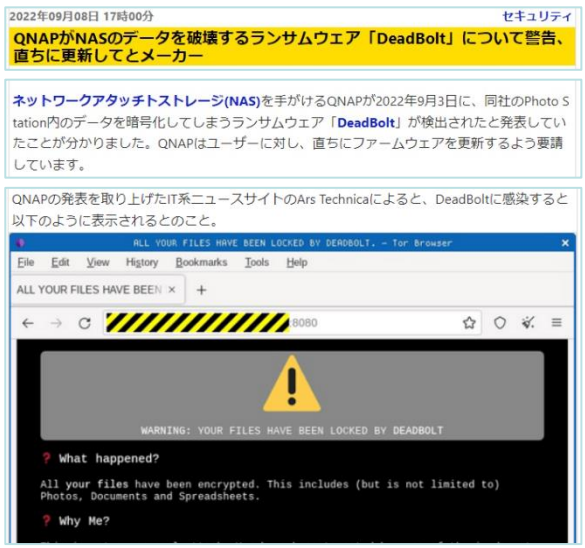
- 既にPhoto Stationのセキュリティアップデートがリリースされていますが、同社ではこのアップデートの他に同様の写真管理アプリ「QuMagie」への移行も推奨しているとのことです。

AUS便りからの所感

- 同社では、NASとルーターに対する防御策として「ルーターのポートフォワーディング機能を無効にする」「myQNAPcloudをセットアップしてNASに安全にリモートアクセスできるようにする」「ファームウェア・アプリケーションを最新に保つ」「全てのユーザーアカウントに強固なパスワードを設定する」「データ保護のため、定期的にスナップショットとバックアップを取る」ことを推奨しています。

- ことNASをはじめとするサーバーあるいはネットワーク機器については、一旦設置された後各種セキュリティアップデートが行われないまま放置されるケースが多いとみられ、セキュリティアップデートがリリースされて日が経っている脆弱性を悪用する攻撃が確認され、メーカーから注意喚起が出されることも珍しくありません。

- クライアントPCからサーバー・ルーター等に至るまで、組織内にある全ての機器について存在を把握し、ソフトウェア等を最新に保つこと、さらにはサポート切れとなったものを適切にリプレースできる体制を整えることが肝要です。


2022年09月08日 17時00分　セキュリティ
QNAPがNASのデータを破壊するランサムウェア「DeadBolt」について警告、直ちに更新してとメーカー
ネットワークアタッチトストレージ(NAS)を手がけるQNAPが2022年9月3日に、同社のPhoto Station内のデータを暗号化してしまうランサムウェア「DeadBolt」が検出されたと発表していたことが分かりました。QNAPはユーザーに対し、直ちにファームウェアを更新するよう要請しています。
QNAPの発表を取り上げたIT系ニュースサイトのArs Technicaによると、DeadBoltに感染すると以下のように表示されるとのこと。
ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT. - Tor Browser
WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBOLT
What happened?
All your files have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.
Why Me?