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。

●水道システムへの不正アクセス…パスワードの使い回し等複数の穴が狙われる

https://www.itmedia.co.jp/news/articles/2102/09/news137.html
https://www.itmedia.co.jp/news/articles/2102/15/news055.html
https://gigazine.net/news/20210212-hacker-poison-water-supply-teamviewer/

このニュースをザックリ言うと･･･

- 2月8日(現地時間)、フロリダ州ピネラス郡保安官より、同州オールズマー市の水処理システム制御パネルが同5日に不正アクセスを受け、飲料水内のpH安定用の水酸化ナトリウム濃度を100倍以上に上昇させる遠隔操作が行われたと発表されました。

- その後の調査結果の発表によれば、浄水場の職員が使うPCが複数のセキュリティ上の問題を悪用されて攻撃者に侵入され、そこを踏み台にして制御システムにアクセスされたとみられます。

- なお、不正な濃度設定は直後にオペレーターが異変に気付いたことで対応され、実害は出ていないとのことです。

AUS便りからの所感等

- 職員のPCはリモートアクセスを行うため、遠隔操作ソフト「TeamViewer」がインストールされていたとのことですが、「OSがWindows 7」「TeamViewerを利用するためのパスワードが全PCで共通」「PCのファイアウォール設定が無効な状態でインターネットに接続されていた」といった複合的な問題があり、これらを悪用されたものとされています。

- PCに外部からリモートアクセスする機構を安全なものとするには、接続される側において、適切なユーザーであることを認証した上でアクセスを許可する(加えて場合によってはアクセス元IPアドレスを制限する等の)設定を行うことと、そもそも接続される側とする側の双方においてPC自体や周辺のネットワークがセキュアであることがやはり重要と言えます。

- また、前述した問題はそれぞれ単独でも攻撃者の侵入やマルウェアの感染を許す要素となり得ますので、現時点で見えている問題について一通り対策を行うこと、また見落としていた問題やあらたに問題として扱われる要素についても、見つかり次第可能な限り早めに対応することが、攻撃の余地を最小限に抑えるために有用です。

ITmedia NEWS

この頃、セキュリティ界隈で

パスワード使い回しや「Windows 7」使用、不正侵入を招いた水道システム管理の実情

2021年02月15日 07時00分 公開　[鈴木聖子，ITmedia]

印刷　通知　見る　Share　B! 121

米フロリダ州オールズマー市の浄水システムに何者かが不正侵入し、飲料水に含まれる水酸化ナトリウム（苛性ソーダ）量を100倍以上に増やす設定変更を行った事件。この時は管理者がすぐに気付いて対応したため実害は免れたものの、パスワードの使い回しや「Windows 7」の使用など、地方自治体の水道システムが抱える問題の一端が浮き彫りになった。こうした実態はたまたま明るみに出たにすぎず、氷山の一角だと専門家は指摘する。

オールズマー市の浄水システムが不正侵入されたのは2月5日。何者かがPC遠隔操作ソフトウェアの「TeamViewer」を介して2度にわたって浄水場の産業制御システム（SCADA）にアクセスを確立し、飲料水に混ぜる水酸化ナトリウムの量を、約100ppmから1万1100ppmに変更した。

●2月度のWindows Updateは適用必須、重大な脆弱性に対応

https://forest.watch.impress.co.jp/docs/news/1305707.html
https://forest.watch.impress.co.jp/docs/news/1305583.html

このニュースをザックリ言うと・・・

- 2月10日(日本時間)、マイクロソフト(以下、MS)より、月例のセキュリティパッチがリリースされています。

- 今月もWindows・Office・.NET Frameworkから各種サーバーに至るまで多数の脆弱性への修正が行われていますが、WindowsのTCP/IP実装においては3件の危険度の高い脆弱性が存在し、うち1件(CVE-2021-24086)については、リモートからOSに対しブルースクリーンエラー(BSoD)を容易に発生させられる恐れがあるとされています。

- この他にも、ローカルから権限昇格が可能で、既に攻撃への悪用が確認されている脆弱性(CVE-2021-1732)や、Windowsサーバーの DNS機能に存在する脆弱性(CVE-2021-24078)等も修正されており、今回のセキュリティパッチはMSをはじめセキュリティ機関等からも早急な適用が呼び掛けられています。

AUS便りからの所感

- 当初、Windows 10 バージョン1909向けパッチについては、WPA3を使用してWi-Fi接続を行うデバイスにおいて不具合が発生していたため、同12日にさらなる修正版がリリースされています。

- このようにパッチ適用後に別の不具合が発生することも度々ではあるものの、基本的には無闇に先延ばしせずにできる限り早めに適用を行い、またパッチ適用までの間に攻撃を受ける可能性に対し、アンチウイルスやUTM等による防御を固めることが肝要です。

- また、Windows 10 バージョン1909は5月11日にサポート終了予定で、その前の1903は既に昨年末にサポートが終了しており、セキュリティパッチが提供されなくなりますので、Windows Update画面において「Windows 10、バージョン 20H2 の機能更新プログラム」が表示されている場合は、現在のバージョンがサポート終了するまでにバージョンアップを行っておくようにしてください。

●モールス信号使って検出を回避するフィッシング詐欺メール発見

https://news.mynavi.jp/article/20210209-1713983/

このニュースをザックリ言うと・・・

- 2月7日(現地時間)、PC情報サイトの米Bleeping Computerより、フィッシングサイトへのURLがモールス符号で記載されたフィッシングメールの存在を確認したと発表されました。

- 具体的には、メールの添付ファイルに含まれるJavaScript中においてこのようなURLが記載されており、最終的にはログインがタイムアウトしたと偽ってアカウント情報を詐取しようとするフィッシングサイトに誘導される模様です。

- 同サイトでは過去に同様の手法がフィッシング攻撃に用いられたデータは見つけられず、新しい難読化手法だろうと説明しているとのことです。

AUS便りからの所感

- 動作の解説を見る限り、さすがにメールを受け取ったユーザーにモールス符号を解読させる類のものではなく、その場で符号をURLにデコードする仕組みとなっています。

- 悪意のあるデータを難読化する意味では、以前紹介した、コードが空白とタブのみで記述されたマルウェア(AUS便り 2021/02/08号参照)と似通っており、今回は人間の目ではなく、メーラーやアンチウイルス・UTMのアンチフィッシング機能を回避する目的で用いられている模様です。

- 手口が明らかになった今後は各社プロダクトにおいて対応されることが期待されるものの、攻撃者は今後も新たな難読化手法を採用し、フィルタリング等の回避を続けるとみられ、ユーザー側としてはBleeping Computerが呼び掛けるように、メールの添付ファイルや記載された不審なURLへの注意を払うことが大事でしょう。