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。

●コンテナターミナルシステムがランサムウェア感染…バックアップ保存サーバーにも感染で復旧遅れる

https://xtech.nikkei.com/atcl/nxt/news/18/15539/
https://meikoukyo.com/archives/category/news

このニュースをザックリ言うと･･･

- 7月5日(日本時間)、名古屋港運協会より、名古屋港におけるコンテナターミナルの管理システム「名古屋港統一ターミナルシステム(NUTS)」がランサムウェアに感染したと発表されました。

- 感染が発覚したのは同4日6時30分頃で、これによりコンテナの搬出入作業が中止される事態となっています。

- 同協会では当初同5日18時を目途にシステム復旧、翌6日早朝からの搬出入作業再開を予定していましたが、バックアップデータを保存していたサーバーにもランサムウェアの感染が確認されたこと等から、システム復旧は同6日7時30分頃までかかったとのことです(搬出入作業再開は同6日15時以降)。

AUS便りからの所感等

- 一部報道では、プリンターからランサムウェアによるとみられる英文の脅迫文が大量に印刷されたことから、ランサムウェア「LockBit」に感染したものと推測されています。

- ランサムウェア感染のきっかけはメール添付ファイル等に限らず、サーバーやネットワーク機器の脆弱性を突いての侵入も多くみられ、ネットワーク上の各種サーバーのOSやインストールされているソフトウェアはもちろん、あらゆる機器のファームウェアに至るまで最新バージョンに保つこと、またアンチウイルス・UTM等による多層防御も行うことがランサムウェアをはじめとするマルウェアの侵入を防ぐために肝要です。

- 今回のケースでは幸いにもバックアップからのデータ復元に成功していますが、そもそもバックアップをとっていなかったり、バックアップデータまでもが暗号化等で破壊されることにより、復元復旧が困難になるケースも珍しくないため、バックアップデータ保全のため「複数コピーをとる」「オンラインから隔離された場所あるいは書き換え不可能なストレージ(サービス)に保管する」さらには万が一の事態に備え「バックアップとリストアが確実に実行できるようテストする」ことが重要とされています(AUS便り 2021/09/14号参照)。

日経XTECH

バックアップからもマルウエア検出で復旧遅れ、名古屋港統一ターミナルシステム

森岡 麗　日経クロステック／日経コンピュータ

2023.07.06

名古屋港運協会は2023年7月6日、ランサムウエア被害によって停止していた「名古屋港統一ターミナルシステム（NUTS）」について、同日午前7時半に復旧したと発表した。当初は同日午前8時半から搬出入作業の再開を予定していたが、システム復旧の遅延に伴い午後からの再開予定に変更。開始時刻の詳細は別途案内するとしている。

NUTSのシステム障害は2023年7月4日午前6時半ごろに発生した。同協会は当初、7月5日午後6時をめどに復旧を図るとしていたが、同日午後8時に延期。だが、午後8時になっても復旧できなかった。同協会の菊川幸信専務理事は「感染前のバックアップをもとにセキュリティーのチェックをしながら復旧していたため時間がかかった。さらに、バックアップデータを保存していたサーバーからもランサムウエアが検出された。その駆除に相当な時間を要した。駆除を終えて復旧に至った」と説明する。

●NEC製のサポート終了済みWi-Fiルーターに脆弱性、リプレースか回避策確認を

https://internet.watch.impress.co.jp/docs/news/1512277.html
https://jpn.nec.com/security-info/secinfo/nv23-007.html
https://www.aterm.jp/support/tech/2023/0627.html

このニュースをザックリ言うと･･･

- 6月27日(日本時間)、NECプラットフォームズ株式会社より、同社提供のWi-Fiルーター「Aterm」シリーズにおいて脆弱性が報告されたとして注意喚起が出されています。
- 脆弱性が確認されたのはいずれもサポートが終了した機種で、悪用により、機器内部の機密情報等のファイルを閲覧(および削除)されたり、機器を乗っ取られたりする恐れがあるとのことです。
- 同社では対象機器に対しファームウェアの更新予定はないとし、機器の交換もしくは回避策の適用を呼び掛けています。

AUS便りからの所感

- 脆弱性はUSBポートに接続した外付けHDD等のファイルをSMBおよびWeb経由で共有する機能に存在するため、回避策としてはUSB接続を行わないこと、さもなくばユーザーパスワードやWi-Fiの暗号化キーを推測されにくいものにすることを挙げています。
- 対象機器は最も新しいものでも2016年10月に発売されたもので(ファームウェアが2022年末までリリースされていた機器もありますが)、古い機器は故障するまで使い続けられたり、ファームウェア更新を含めた管理が行き届いていない可能性もありますので、家庭・企業に拘わらず、使用されている各ネットワーク機器について機種を含め把握・管理し、機器交換についても計画的に行えるような体制を整えることが肝要です。

Impress Watch

「Aterm WG2600HP2」などNECプラットフォームズのWi-Fiルーター17製品に複数の脆弱性、製品のサポートは終了

後継製品への乗り換えなどを推奨

山田 貞幸　2023年7月10日 07:50

NECプラットフォームズ株式会社が発売していた、Atermシリーズの複数の製品に複数の脆弱性があるとして、「JVN（Japan Vulnerability Notes）」およびNECプラットフォームズが情報を公開した。

対象は、以下の17製品の全てのバージョンのファームウェア。NECプラットフォームズによれば、全てUSBポートを搭載した製品。また、全てサポート期間が終了している。JVNおよびNECプラットフォームズでは、後続製品への乗り換えなどを対策として呼び掛けている。また、乗り換えまでの対応として、NECプラットフォームズが脆弱性の影響を軽減する方法（後述）を公開している。

●6月度フィッシング報告件数は149,714件、15万件に迫る

https://www.antiphishing.jp/report/monthly/202306.html

このニュースをザックリ言うと･･･

- 7月5日(日本時間)、フィッシング対策協議会より、6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。
- 6月度の報告件数は149,714件で、5月度(https://www.antiphishing.jp/report/monthly/202305.html)の113,789件から35,295件増加、過去最多を大幅に更新しています。
- フィッシングサイトのURL件数は23,420件で5月度(18,991件)から4,429件増加、悪用されたブランド件数は107件で5月度(110件)から3件減少となっています。
- 最も多く悪用されたブランドはクロネコヤマト(全体の約18.1%)で、以下それぞれ1万件以上の報告があったイオンカード・Amazon・セゾンカード・ジャックスを合わせた5ブランドで全体の約60.2%、また1,000件以上の報告があった20ブランドで全体の約91.6%を占めたとしています。

AUS便りからの所感

- 報告件数は前月度より一気に急増して15万件に迫っており、今年中あるいは7月度において月間20万件に到達する可能性も十分に考えられます。
- 発表においては「事業者のみなさまへ」および「利用者のみなさまへ」と題し、それぞれがとるべき対策法や採用すべき機構についてまとめられていますが、前者ではDMARCを単に採用するのみならずレポートの分析をもとにより厳格なポリシーの設定を推奨、後者ではフィッシング対策機能が強化されているメールサービスの利用等を呼び掛けており、システム管理者から一般のユーザーに至るまで是非とも目を通し、実行可能な対策を検討して頂ければ幸いです。

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