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。

●推測されやすいデフォルトパスワード禁止へ…イギリスで新法施行

https://gigazine.net/news/20240430-uk-bans-default-passwords-iot-devices/
https://internet.watch.impress.co.jp/docs/yajiuma/1588493.html
https://www.gov.uk/government/news/new-laws-to-protect-consumers-from-cyber-criminals-come-into-force-in-the-uk

このニュースをザックリ言うと･･･

- 4月29日(現地時間)、イギリスにおいて「製品セキュリティおよび通信インフラストラクチャー法(PSTI法)」が施行されました。
- 同法では、電話・テレビ・スマートドアベル等のIoT機器メーカーに対し、サイバー脅威に対する最低限のセキュリティ基準の導入を義務付けるとし、例えばIoT機器のデフォルトパスワードとして「admin」「12345」といった推測されやすいものの設定を禁止するとしています。
- 同法は2022年に成立したもので、イギリス政府では「英国の消費者と企業をハッキングやサイバー攻撃から守るための世界初の法律」としています。

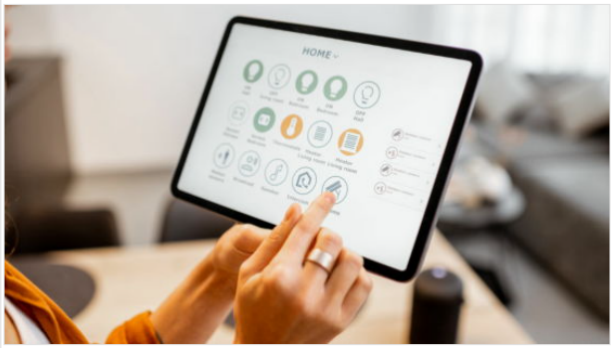
AUS便りからの所感等

- 国内外製のルーター・NAS等において、あるいはソフトウェアであればLinuxディストリビューションのインストール時等において、デフォルトのパスワードが簡単なものであったり、そうでなくても同品番の全ての機器で同じであるケースは珍しくなく、そういったデフォルトパスワードの情報を集めているWebサイトも存在します。
- 攻撃者は、オープンポートや管理画面等に外部からアクセス可能な機器が検索可能な「Syodan」「Censys」等のサイトも利用し、パスワードが変更されていない機器がないか日々探し回り、侵入の機会を窺っていることでしょう。
- あらゆるサーバーからネットワーク機器に至るまで、導入時には必ず管理者パスワードをデフォルトのものから機器ごとに異なるかつ推測されにくいものに変更することが肝要です。

GIGAZINE

2024年04月30日 11時00分　セキュリティ

IoTデバイスの「admin」や「12345」など推測が容易なデフォルトパスワードをイギリスが世界で初めて禁止



スマートテレビやスマート電球などのIoTデバイスは、家具や家電をインターネットに接続することで日常生活を便利にしてくれますが、同時にセキュリティ上のリスクをもたらす可能性もあります。イギリスでは2024年4月29日(月)に「Product Security and Telecommunications Infrastructure Act(PSTI法：製品セキュリティおよび通信インフラストラクチャー法)」の改正案が施行され、世界で初めて「IoTデバイスの推測しやすい脆弱(ぜいじゃく)なデフォルトパスワード」を禁止しました。

New laws to protect consumers from cyber criminals come into force in the UK - GOV.UK
https://www.gov.uk/government/news/new-laws-to-protect-consumers-from-cyber-criminals-come-into-force-in-the-uk

UK becomes first country to ban default bad passwords on IoT devices
https://therecord.media/united-kingdom-bans-defalt-passwords-iot-devices

The UK beefs up smart home security by going after bad default passwords - The Verge
https://www.theverge.com/2024/4/29/24144325/uk-psti-password-requirements-network-connected-devices-iot-smart-home

●消し忘れていたテスト用アカウントから侵入…サーバーがランサムウェア感染

https://www.itmedia.co.jp/news/articles/2404/24/news181.html
https://endless-inc.jp/blogs/news/20240423
https://www.startia.co.jp/news/detail/?id=1868&site_name=startia

このニュースをザックリ言うと・・・

- 4月23日(日本時間)、アクセサリー・パーツ販売業のエンドレス社より、同社サーバーが不正アクセスを受け、ランサムウェア「LockBit」に感染したと発表されました。
- 発表時点で社内情報の流出の事実は確認されておらず、またサーバーに顧客情報は入っていなかったとしています。
- 感染に至った原因として、UTM導入を委託したスターティア社が使用していたテスト用アカウントを削除していなかったためとしています。

AUS便りからの所感

- 委託先会社に不手際があったと名指しで指定する事態となっており、同26日にはスターティア社からも本件について発表がありました。
- テスト用か否かに拘らず、パスワードはもちろんIDが推測されやすいものは攻撃者にターゲットとされやすいため、導入前のテスト段階から複雑なものであるべきです。
- また、任意のアクセス元からSSHによってサーバーにログインするような場面では、既にIDとパスワードのみでの認証は推奨されず公開鍵による認証が一般的となっており、UTMを経由してのVPN接続においてもユーザー毎に証明書を発行したり、その他の多要素認証の導入が強く推奨されます。


アクセサリー販売事業者がランサムウェア感染　“委託先名指し”で原因説明　「Parts Club」など運営

2024年04月24日 21時20分 公開　[ITmedia]

アクセサリーパーツを販売する「Parts Club」など、アクセサリー関連事業を手掛けるエンドレス（東京都台東区）は4月24日、自社のサーバがランサムウェア「LockBit」に感染したと発表した。原因について、セキュリティソリューションを導入したスターティア（東京都新宿区）のミスによるものだと説明している。

企業情報 / 2024年04月23日

弊社サーバーのマルウェア感染に関する お詫びとお知らせ

この度、本社サーバーがコンピュータウイルス「LockBitランサムウェア」に感染しました。

今回の不正アクセスの直接の原因は、セキュリティ強化の一環で FortiGate(統合型セキュリティアプライアンス)の設置を昨年

●終了サービスが不審なサイトに？ 原因はサブドメイン名の削除忘れか

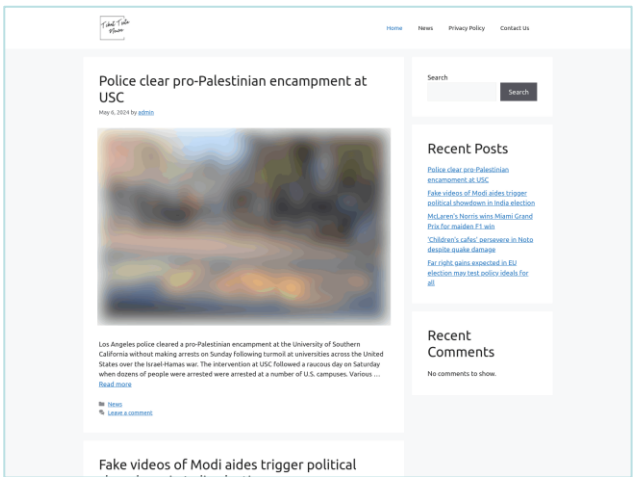
https://twitter.com/tss_0101/status/1787691268010823762
https://megalodon.jp/2024-0507-1253-14/https://www.google.com:443/search?q=site%3Atchat.tsite.jp&tbm=vid&hl=ja
https://web.archive.org/web/20231119153349/https://tchat.tsite.jp/

このニュースをザックリ言うと・・・

- 5月7日(日本時間)、X(旧Twitter)において、Tポイント(現・Vポイント)がかつて提供していたサービスの一つ「Tチャット」の旧サイトで不審なサイトが表示されたとする事例が報告されました。
- Tチャットは2022年12月に終了していましたが、当該サービスで使われていた「tchat.tsite.jp」へのアクセスにより、英語等のニュースを転載するサイトが表示されていました。
- 「tchat.tsite.jp」は同日中にDNSが引けなくなり、対策された模様です。

AUS便りからの所感

- 上記サイト内では他にも外部の動画サイト等にリダイレクトするページもあったとみられ、またインターネットアーカイブでは、2023年11月時点でインドネシア語のオンラインカジノサイトとなっていたことが記録されています。
- 「tchat.tsite.jp」はDNS上ではCNAMEレコード(別のドメイン名を参照する)となっており、AWS上のホストを参照していましたが、参照先のホストを解約した後もCNAMEが有効のままで、かつ第三者が同じホスト名で登録を行ったために、別のホストが表示されるようになった可能性が指摘されています。
- この攻撃手法は「サブドメインテイクオーバー」と呼ばれ、独自に取得したドメイン名(***.jp, ***.com等)が失効した後で第三者に取得される「ドメインドロップキャッチ」と類似した攻撃手法である一方、第三者がどちらを乗っ取る攻撃かに違いがあります。
- 不要になったDNSレコード(CNAMEに限らず、また特に参照先について管理が及ばなくなる可能性があるもの)を削除することが最も確実な対策と言えますが、いずれにしろサブドメインからWebサーバー等の契約まで一貫した管理を行うことに越したことはありません。


Police clear pro-Palestinian encampment at USC

May 6, 2024 by admin

Los Angeles police cleared a pro-Palestinian encampment at the University of Southern California without making arrests on Sunday following turmoil at universities across the United States over the Israel-Hamas war. The intervention at USC followed a raucous day on Saturday when dozens of people were arrested were arrested at a number of U.S. campuses. Various ...

Read more

News
Leave a comment

Search

Recent Posts

Police clear pro-Palestinian encampment at USC
Fake videos of Modi aides trigger political showdown in India election
McLaren's Norris wins Miami Grand Prix for maiden F1 win
'Children's cafés' persevere in Noto despite quake damage
Far right gains expected in EU election may test policy ideals for all

Recent Comments

No comments to show.

Fake videos of Modi aides trigger political