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。

●国内500件近くの屋内・敷地内防犯カメラ映像が公開状態に…トレンドマイクロ他調査

https://www.yomiuri.co.jp/national/20251103-OYT1T50134/
https://www.yomiuri.co.jp/national/20251104-OYT1T50000/
https://mezamashi.media/articles/-/218902
https://youtu.be/IO_m7D9Wxo8

このニュースをザックリ言うと･･･

- 11月4日(日本時間)、読売新聞より、日本国内の屋内・敷地内設置の「ネットワークカメラ」に外部から接続し、映像が閲覧可能な状態となっていたと報じられています。

- 同社とトレンドマイクロ社の調査によれば、海外7つのサイトにおいて、世界中のネットワークカメラ映像合わせて約27,000件以上が確認され、日本国内のものが約1,340件、うち90件が屋内、400件超が敷地内のものとしています。

- 対象のカメラは「パスワード認証が未設定」「映像の公開範囲を誤って設定」といった不備があったとしており、同紙からの指摘で不備を把握、設定変更等の対応をとったとしています。

AUS便りからの所感等

- ネットワークカメラに想定していない不特定多数から不正アクセスされる事案は既に10年近く前から報じられており、単に映像が公開状態にあるだけでなく、不正な操作が行われるケースや、DDoSを行う「Mirai」等のマルウェアが感染してボットネットを構築されるケース等が知られています。

- PCやスマートフォンと異なり、人が頻繁に触ることの少ない傾向にあるIoT機器では、管理画面等へのログイン情報がデフォルトのままであったり、ファームウェアアップデートの適用が後手に回ることや、攻撃や侵入の発生が検知されにくいことがしばしば起こり得ますので、くれぐれもログイン情報はデフォルトから変更して推測されにくいパスワードとすることを心掛け、機器自体やルーター・UTM等の設定により、不要なポートは完全にフィルタリングするか、特定のIPアドレスからのみのアクセスに制限する等を強く推奨致します。

- サーバーはもちろん複合機やネットワークカメラ等のIoT機器まで、インターネット上からアクセス可能な状態になっている機器を探し出すサーチエンジンとして「Shodan」「Censys」等があり、前述したカメラ映像公開サイトもこういったサーチエンジンで機器を検索したと考えられる一方、機器を設置した側においても不備がないか確認する用途に有用でしょう。

読賣新聞オンライン

保育園や工場の防犯カメラ映像、５００件が海外サイト流出…設定に不備「犯罪に悪用される恐れも」

2025/11/04 05:00

日本の屋内・敷地内に設置され、インターネットにつながった「ネットワークカメラ」のライブ映像約５００件が海外のサイトに公開され、誰でも見られる状態になっていることが読売新聞と情報セキュリティー会社「トレンドマイクロ」（東京）の調査でわかった。屋内の映像は保育園や食品工場など９０件。設置場所・状況を確認できた屋内のカメラの大半は、防犯・見守りや安全管理を目的に導入されたもので、無断でサイトに公開されていた。

【イメージ】ネットワークカメラの映像が漏えい

●正規VPNアカウント悪用…10月発生のランサムウェア攻撃について時系列報告

https://www.itmedia.co.jp/news/articles/2511/05/news107.html
https://www.mino-in.co.jp/?p=12341

このニュースをザックリ言うと･･･

- 10月4日(日本時間)、美濃工業株式会社より、同社システムがサイバー攻撃により障害が発生したと発表され、同6日の続報でランサムウェア攻撃であることが明らかになりました。

- その後同21日の第三報、11月3日の第四報において攻撃の時系列が発表され、10月1日にVPN機器を経由して社内ネットワークに侵入、同4日未明までデータの搾取等の活動、また同3日夜にファイル暗号化やシステムの不正な初期化等が行われたとしています。

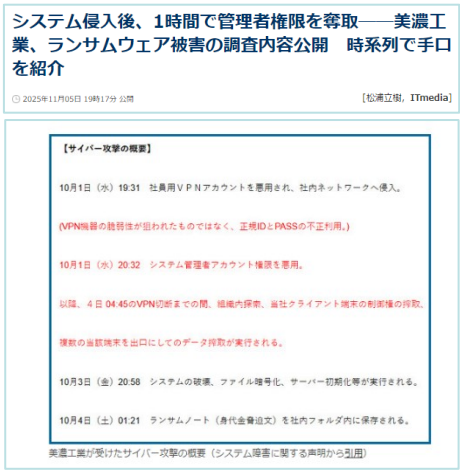
- 300GB程度の不正な通信があったことから情報が大量に流出した可能性があり、10月28日にダークサイトにおいて情報漏洩の事実を確認したとのことです。

AUS便りからの所感

- 社内ネットワークへは機器の脆弱性の悪用ではなく正規のVPNアカウントによる侵入が行われ、1時間後には管理者権限を奪取されたとしています。

- VPNに関するニュースとしては、UTM機器大手のFortinet社が、2026年5月にその一種であるSSL-VPNのサポートを終了し、IPsec VPNへの移行を推奨することが発表されています。

- いずれにしろVPNからの侵入(あるいはリモートデスクトップからの侵入)がランサムウェア等の攻撃のきっかけとなるケースは多数報じられており、VPN機器のファームウェアを最新に保つ、全てのアカウントについて強力なパスワードを設定することに留意し、またVPNからログインしたユーザーにネットワーク上のあらゆるサーバーにアクセスされ、システム全体の管理者権限奪取まで行き着くのを阻止するため、UTM等を用いての適切に分割・隔離されたネットワーク構成により、他のサーバー・クライアントへの不審なアクセスを抑制することを検討すべきでしょう。


システム侵入後、1時間で管理者権限を奪取――美濃工業、ランサムウェア被害の調査内容公開　時系列で手口を紹介

2025年11月05日 19時17分 公開　[松浦立樹，ITmedia]

【サイバー攻撃の概要】

10月1日（水）19:31　社員用ＶＰＮアカウントを悪用され、社内ネットワークへ侵入。

(VPN機器の脆弱性が狙われたものではなく、正規IDとPASSの不正利用。)

10月1日（水）20:32　システム管理者アカウント権限を悪用。

以降、4日 04:45のVPN切断までの間、組織内探索、当社クライアント端末の制御権の搾取、

複数の当該端末を出口にしてのデータ搾取が実行される。

10月3日（金）20:58　システムの破壊、ファイル暗号化、サーバー初期化等が実行される。

10月4日（土）01:21　ランサムノート（身代金要求文）を社内フォルダ内に保存される。

美濃工業が受けたサイバー攻撃の概要（システム障害に関する声明から引用）

●高市総理の映像を悪用、フェイク広告に警視庁等注意喚起

https://www.itmedia.co.jp/aiplus/articles/2510/24/news079.html
https://www.itmedia.co.jp/news/articles/2510/29/news077.html
https://x.com/jimin_koho/status/1981533027277951122
https://twitter.com/NPA_KOHO/status/1983148604555702418

このニュースをザックリ言うと･･･

- 10月24日(日本時間)に自由民主党より、高市早苗総理の画像・映像を悪用したフェイク広告が出回っているとして、X(旧Twitter)上で注意喚起が出されています。

- 注意喚起ではAIで生成されたとする映像に、偽サイトへ誘導するとみられるQRコードが表示されている例が挙げられており、このような広告は同総理や自民党と一切関係ないとしています。

- 同28日には警察庁からも、同総理の主導の下で開発されたと称する暗号資産(仮想通貨)プラットフォームへの投資を呼び掛ける偽広告が例に挙げられ、投資詐欺・フィッシング等の被害に遭う可能性があるとしています。

AUS便りからの所感

- AIを悪用した詐欺等の事例は、ターゲットの知人になりすましたフェイク映像によってマルウェアに感染させられ、暗号資産を奪取される等の巧妙なものが既に報告されています(AUS便り 2025/07/07号参照)。

- とにかく前述の注意喚起でも挙げられている通り、安易にQRコードを読み取ったり、URLをクリックしたりしてフィッシングサイト等にアクセスしたり、アクセス先で個人情報やクレジットカード情報等を入力したりしないという基本的な回避策を押さえるとともに、ブラウザーやアンチウイルス・UTMのアンチフィッシング機能等による防衛も確実に行うようにしましょう。


高市首相の映像を悪用した偽広告、警視庁が注意喚起「お金の話が出たら詐欺！」

2025年10月29日 11時40分 公開　[ITmedia]

警察庁は10月28日、高市早苗首相の映像を悪用した偽広告が確認されているとし、アクセスしないよう注意を呼び掛けた。「個人情報を入力しない！」「お金の話が出たら詐欺！」と注意喚起している。

警察庁 @NPA_KOHO

＼⚠ 注意 ⚠／
高市総理の映像を悪用した偽広告が確認されています。
画面に表示されたQRコードから偽サイトに誘導され、投資詐欺やフィッシングなどの被害に遭う可能性があります。

QRコードを読み取らない・URLをクリックしない！
個人情報を入力しない！
お金の話が出たら詐欺！

高市早苗氏と日本の主要機関が新たな投資プラットフォームを発表

日本人が月533万円以上を稼ぐ方法