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。

●ポイントカードのQRコードから不審なサイトへアクセスの恐れ…注意喚起

https://internet.watch.impress.co.jp/docs/news/2027717.html
https://www.atre.co.jp/news/5360/
https://www.jrepoint.jp/information/important/20250627001
https://www.nichizeiren.or.jp/whats-new/250703b/

このニュースをザックリ言うと･･･

- 6月27日(日本時間)、JR東日本およびアトレより、2016年2月まで発行されていたポイントカード「(旧)アトレカード」に印字されているQRコードから第三者のWebサイトにアクセスする可能性があるとして注意喚起が出されています。

- QRコードは元々会員向けサービス「マイアトレ」にアクセスするものでしたが、2016年2月にURLが変更し、また以前のサイトで使用していたドメイン名(atre-club .jp)も失効した後に第三者に取得(ドロップキャッチ)されたとみられます。

- 7月4日現在、当該ドメイン名はSuspendedとなっており、サイトにはアクセスできない状態です(同31日に再び期限切れになる予定で、別の第三者に取得される可能性については不明です)。

AUS便りからの所感等

- サイト閉鎖から約10年程経ってからの注意喚起となっており、本来であれば使用されなくなったドメイン名を組織で保持しておくべき期間としては十分という見方もできますが、特にカードや印刷物にURL自体あるいはQRコードとして印刷する場合にはより長期～半永久的にアクセスされる可能性が考えられるでしょう。

- 7月3日には、日本税理士会連合会より、同会が3月まで開設していた成年後見支援センターのドメイン名(nichizeiren-seinenkouken .org)が第三者に再取得されたと発表されていますが、こちらはサイト閉鎖からドメイン名の失効まで明らかに期間が短く、前述の事案よりもさらにドロップキャッチの被害が発生する可能性があるものと考えられます。

- また衆議院議員総選挙・参議院議員選挙では都道府県が特設サイトのために独自にドメイン名を取得しているケースが毎回みられ、今回7月20日に実施される参議院議員選挙でも同様となっており、独自ドメイン名を取得することは避け、既存のドメイン名やそのサブドメインを用いること(サブドメインでも運用次第では別のセキュリティ上の注意事項があります)、独自ドメイン名の場合は閉鎖後も長期間(10年以上等)そのドメイン名を保持することもまた最低限考慮すべき事項です。

Impress Watch

アトレ、「旧アトレカード裏面のQRコードを読み取らないで」と注意喚起、不審なサイトに接続してしまうことが確認される

木下 明音　2025年7月2日 15:50


atré

News | アトレからのお知らせ

【お知らせ】旧アトレカードをご利用のお客さまへ

UP：2025.06.27

以前、アトレクラブ会員向けに提供しておりましたWebサービス「マイアトレ」において2015年度まで使用していたインターネットドメイン「atre-club.jp」が、現在、第三者により取得され、アクセスすると不審なWebサイトへ誘導される状況にあることが確認されております。

株式会社アトレは、旧アトレカード（下図参照）の利用者に対し、カード裏面のQRコードを読み取らないようにと注意喚起を行っている。

旧会員向けサービス「マイアトレ」で利用していたドメインが現在第三者によって取得され、QRコードを読み取ったURLにアクセスすると、不審なウェブサイトへ誘導されることを確認したという。

●乗っ取られた知人のアカウントとビデオ会議、マルウェア感染で暗号資産奪取される

https://internet.watch.impress.co.jp/docs/column/netliteracy/2025729.html

このニュースをザックリ言うと･･･

- 6月27日(日本時間)、「INTERNET Watch」において、ディープフェイクによる巧妙なネット詐欺の被害を受けたという事例が紹介されています。

- この事例では、事前に乗っ取られたアカウントからメッセージアプリTelegram(あるいはXやFacebookメッセンジャー)で連絡を受け、Zoomでオンラインミーティングを行った際に発生するトラブル解消のために ファイルをダウンロードさせるリンクを送り付ける という手口がとられています。

- ダウンロードされるファイルは暗号資産やTelegram・Xのアカウントを奪取するマルウェアとされ、ここで乗っ取られたアカウントがさらに他のユーザーに対する詐欺に悪用されるとのことです。

AUS便りからの所感

- ミーティング中に音声が聞こえないといった事象が発生し、その解決のために サウンドドライバーのアップデート としてマルウェアを送付するシナリオとなっています。

- Zoomで表示される相手の画像もAIで生成されたディープフェイク動画が用いられるとされ、被害者はアカウントを乗っ取られた10分間のやり取りでも気付かなかったとしています。

- 記事では、「声が聞こえない」「マイクの調子が悪い」などと言われた場合は一旦詐欺を疑うこと、一方で本当にマイクの調子が悪い可能性等もあり、電話・メール等で相手に連絡することも検討するよう呼び掛けています。

- 他にも全般的な詐欺行為からの回避策として「送られてきたリンクはクリックしない」「怪しいファイルはダウンロードしない・実行しない」、アカウント乗っ取りの回避策として「多要素認証を利用する」等を挙げており、併せて今回のような事例の情報を随時収集することもまた肝要です。

●管理者権限でコマンド実行するツールsudoに脆弱性

https://rocket-boys.co.jp/security-measures-lab/linux-sudo-chroot-cve-2025-32463-root-escalation/
https://innovatopia.jp/cyber-security/cyber-security-news/59622/
https://www.sudo.ws/security/advisories/

このニュースをザックリ言うと･･･

- 6月30日(現地時間)、Linux等でroot(管理者)権限でのコマンド実行のために使用されるツール「sudo」に2件の脆弱性(CVE-2025-32462, CVE-2025-32463)が存在することが発表され、セキュリティアップデート1.9.17p1がリリースされています。

- CVE-2025-32462はsudoバージョン1.8.8～1.9.17、CVE-2025-32463は1.9.14～1.9.17に影響し、本来想定されていない箇所でrootによるコマンド実行が可能になるとされています。

- Linuxディストリビューション(Almalinux・Debian・Ubuntu等)のパッケージの多くでCVE-2025-32462について影響を受けるとされ、既に修正バージョンがリリースされています。

AUS便りからの所感

- 通常、Webサーバー・メールサーバー等に対し直接攻撃を行うことは困難とみられ、何らかの方法でサーバー上への侵入に成功した攻撃者が攻撃コードをダウンロード・実行するケース、あるいはサーバー上にSSH等でログイン可能な一般ユーザーが悪意を持って攻撃を行うケースが考えられます。

- 大抵のLinuxディストリビューションでは、全てのソフトウェアパッケージを一括してアップデートする仕組みが提供されていますので、OSを常に最新に保つために随時これを実行するルーチンを確立すること、またパッケージからではなくソースからコンパイルしたソフトウェアについても、同様に新しいバージョンを確実にインストールする管理体制を整えることが肝要です。

- Linuxを使用するNAS等のアプライアンスでもアップデートがリリースされる可能性があり、これらについてもベンダー情報の確認は必須でしょう。