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。

●パスワードマネージャー「Bitwarden」CLI版にサプライチェーン攻撃、npmで一時有害なバージョン配布

https://gigazine.net/news/20260424-bitwarden-cli-supply-chain-attack/
https://socket.dev/blog/bitwarden-cli-compromised
https://blog.flatt.tech/entry/bitwarden_compromise

このニュースをザックリ言うと・・・

- 4月23日(日本時間)、米セキュリティ企業Socket社より、パスワードマネージャー「Bitwarden」のCLI(コマンドライン)版がいわゆる「サプライチェーン攻撃」を受け、一時マルウェアを含む有害なバージョンがリリースされていたと発表されました。

- GMO Flatt Security社のブログによれば、4月23日6:22から同24日未明にかけてnpm(JavaScript製ソフトウェアのパッケージ管理・配布システム)上でバージョン2026.4.0がリリースされており、当該バージョンをインストールしたサーバー上の機密情報を奪取される恐れがあったとされています。

- バージョン2026.4.0はnpmから削除され(バージョン2026.3.0以前および2026.4.1は無害)、ブラウザー拡張版・スマホアプリ版およびnpm以外で配布されるCLI版については有害なバージョンのリリースはなく、Bitwardenサービスに保存されたパスワード等の奪取等も確認されていないとのことです。

AUS便りからの所感等

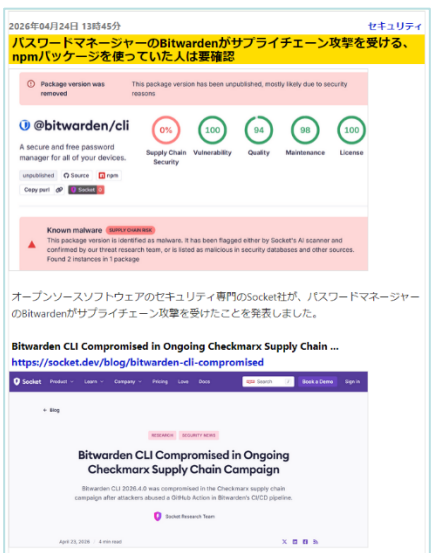
- マルウェアは、有害なバージョンをインストールする作業を行ったユーザーのホームディレクトリー下にある、npm・GitHub・SSH・AWS・各種AIツールに関する秘密鍵やトークン、あるいは実行したシェルコマンドの履歴といった情報を収集し、外部に送信する挙動をとっていたとされています。

- npmで提供されるJavaScriptパッケージにおいて発生したサプライチェーン攻撃の事例は先日もHTTPクライアントライブラリー「axios」で発生しています(AUS便り 2026/04/10号参照)。

- Bitwardenのような人気のあるパスワード管理サービスへの攻撃としては、サービスに保存されたパスワード情報をターゲットとするケースがよく想定され、2022年にはLastPassが不正アクセスを受け、暗号化された状態のパスワード等が奪取されたことが発表されています(前述の通り今回はそのような被害は確認されていません)。

- サプライチェーン攻撃は、ソフトウェアのユーザーにマルウェアを含む悪意のあるパッケージを配布することを目的とし、そのために開発者のアカウントを侵害することが主なシナリオとして考えられ、またその過程で他の開発者の開発環境上にもマルウェアが配布されるよう仕向けるケースもあり、組織内外全ての開発者においてマルウェア感染や認証情報奪取によるアカウントの侵害を受けないよう、アンチウイルスやUTM等による防御を確実に固めることが重要となります。

GIGAZINE



● 3月度フィッシング報告件数は122,381件、2月度から一転して回復傾向に

https://www.antiphishing.jp/report/monthly/202603.html

このニュースをザックリ言うと・・・

－4月21日(日本時間)、フィッシング対策協議会より、3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。

－3月度の報告件数は65,284件で、2月度(https://www.antiphishing.jp/report/monthly/202602.html)(AUS便り 2026/04/03号参照)の57,096件から65,285件増加しており、フィッシングサイトのURL件数も69,936件で2月度(17,037件)から52,863件増加しています。

－悪用されたブランド件数は123件で2月度(96件)から27件増加、最も報告が多かったブランドはAmazonが約20.9%、次いでApple(約10.5%)、マネックス証券、ANA、セゾンカードと合わせて約51.6%、さらに1,000件以上報告された28ブランドまで含めると約89.3%となっています。

－前月度より日々の「フィッシング報告受領件数」および「調査用メールアドレス宛てへのフィッシングメール着信件数」の推移が発表されており、それぞれ3月末にかけて徐々に増加傾向がみられています。

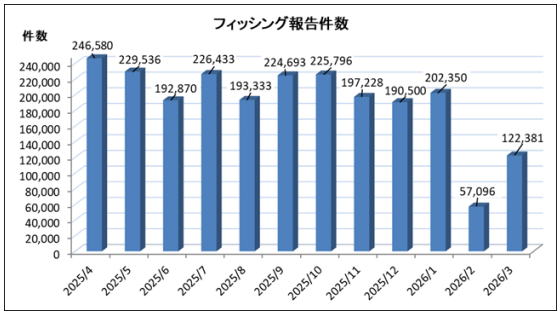
AUS便りからの所感

－2月度における報告数等の急減から一転しての回復となり、また悪用されたブランド数は過去最多となりました。

－報告を受けたフィッシングメールの文面の種類は、登録情報の更新や本人確認依頼、商品の注文およびキャンセル、商品配達に関する通知、税金や公共料金等の支払い依頼、多要素認証の設定を依頼する文面等とされています。

－4月後半以降、Microsoftを騙り、システムスキャン・セキュリティパッチの更新・Microsoftアカウントの認証のために偽のサポートサイト等への誘導を行うメールが大量に届いていますが、同協議会ではサポート詐欺として取り上げている他、日本データ通信協会の迷惑メール相談センター(https://www.dekyo.or.jp/soudan/contents/news/alert.html)にも掲載されており、不審なメールを受信した際はこういった情報等と文言が一致するか確認する等、慎重に行動することを日々心掛けましょう。

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



●ゴールデンウィークにおけるセキュリティ面の注意喚起、IPAから発表

https://www.ipa.go.jp/security/anshin/heads-up/alert20260420.html
https://www.ipa.go.jp/security/anshin/measures/vacation.html
https://www.ipa.go.jp/security/anshin/measures/everyday.html

このニュースをザックリ言うと・・・

－4月20日(日本時間)、IPAより、「ゴールデンウィークにおける情報セキュリティに関する注意喚起」が発表されました。

－多くの企業・組織において、この時期に従業員等が長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

－IPAでは、毎年のゴールデンウィークと夏季・冬季休暇の時期に注意喚起を行っており、一方で長期休暇に関係なく常時から注意すべき普遍的なものについても「日常的に実施すべき情報セキュリティ対策」でまとめています。

AUS便りからの所感

－近年の毎回の注意喚起においては、企業や組織の利用者・管理者に対し、インターネットに接続された機器・装置類の脆弱性を悪用する「ネットワーク貫通型攻撃」およびそれによる情報の漏えいや改ざん、ランサムウェアへの感染に加え、不正な通信の中継点とされてしまう、いわゆるOperational Relay Box(ORB)化等の被害への警戒が呼び掛けられています。

－機器類のファームウェア更新やサポート切れとなったものについての計画的なリプレースの他、こういった攻撃が特に管理者不在とみられる隙を突いて行われる可能性を鑑み、事前の監視体制、あるいは万一間に合わずとも事後のログ監査等の体制を確実に整備すべきでしょう。

－GWまでに日にちがなく十分な対応が間に合わなかったとしても、GW明け以降の点検、以後の夏季休暇等に備えて対応しておくべき事柄は多く、それぞれにおいて準備・点検を行うよう意識して頂ければ幸いです。

IPA 独立行政法人 情報処理推進機構


2026年度 ゴールデンウィークにおける情報セキュリティに関する注意喚起

公開日：2026年4月20日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人がゴールデンウィークの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生し、長期休暇後の業務継続に影響が及ぶ可能性があります。

このような事態とならないよう、(1)個人の利用者、(2)企業や組織の利用者、(3)企業や組織の管理者、それぞれの対象者に対して取るべき対策をまとめています。また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

・長期休暇における情報セキュリティ対策
・日常における情報セキュリティ対策

注釈：上記リンク先において、対象者毎に参照すべき範囲は以下のとおりです。

1. 個人の利用者：個人向けの対策（3.）
2. 企業や組織の利用者：個人及び企業・組織のシステム利用者向けの対策（2-2. / 3.）
3. 企業や組織の管理者：個人、企業・組織のシステム利用者及び管理者向けの対策（2-1. / 2-2. / 3.）