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。

●「個人情報等暗号化」「委託先から情報漏洩」…ランサムウェア被害依然高水準、警察庁も注意喚起

https://www.itmedia.co.jp/news/articles/2409/03/news129.html
https://www.nichiigakkan.co.jp/topics/assets/d300a058b2e1447b1744f33d2ce2065cba1b2e23.pdf
https://www.itmedia.co.jp/news/articles/2408/20/news133.html
https://www.kumon.ne.jp/oshirase/2024081.html
https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.7cpal.pdf

このニュースをザックリ言うと･･･

- 8月16日(日本時間)、医療・介護事業大手のニチイホールディングスより、同社グループ内のPCがランサムウェアに感染し、データ暗号化の被害を受けたと発表されました。

- その後9月2日に続報が発表され、PC計20台を経由して、顧客・関係企業等の担当者や同社採用候補者・従業員・元従業員の個人情報を含む約2.6万件のファイルが暗号化されたことが明らかになっています。

- また8月20日には、教育サービス大手の公文教育研究会より、業務委託先のイセトー社で発生したランサムウェア感染で74万人弱の個人情報が流出した可能性があると発表されています(これも6月29日の初報からの続報となります)。

- 9月6日には、警察庁サイバー警察局より「サイバー警察局便り R6 Vol.7」が発表され、ランサムウェア被害が依然として高水準で推移としている他、感染経路の63%がVPN機器、18%がリモートデスクトップとなっているとして注意が呼び掛けられています。

AUS便りからの所感等

- ニチイの事例ではPC上に保存されていたデータが暗号化の被害を受けたとされますが、6月に発生したKADOKAWAの事例(AUS便り 2024/08/22号参照)においても従業員のPC上に個人情報を含むファイルが保存され流出したとみられるケースが報じられています。

- イセトー社でのランサムウェア感染は、クボタ社および同子会社(同 2024/07/04号参照)をはじめ同社に業務委託していた多数の企業・自治体に被害が及んでいます。

- ランサムウェアによる攻撃を大手企業で発生しているものと決して捉えることなく、あらゆる組織においてVPN等リモートからのアクセスに関わる機器・ファームウェア・OSを随時最新の状態に保つ、サーバーにおけるデータの保護(バックアップはもちろんバックアップしたデータの隔離等含め)、またクライアントPCに対してもアンチウイルス等エンドポイント保護やUTMによる保護のみならず、各々のPCに保存された状態の重要なファイルがターゲットとなる可能性にも注意を払うべきでしょう。

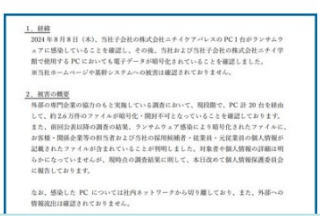
ITmedia NEWS

ニチイHD、ランサムウェア被害で2.6万ファイル暗号化される　顧客の個人情報も

2024年09月03日 13時35分 公開　[ITmedia]

医療・介護事業などを展開するニチイホールディングス（HD）は9月2日、ランサムウェア攻撃を受け、PC 計20台を経由して、約2万6000件のファイルが暗号化されたことが分かったと発表した。

暗号化されたファイルには、同社の採用候補者や顧客などの個人情報が含まれていたが、その詳細はまだ分かっていないという。



公文、75万人分の情報漏えい新たに発覚　子どもの氏名なども　委託先・イセトーのランサムウェア被害で

2024年08月20日 13時27分 公開　[吉川大貴，ITmedia]

発送物の印刷や送付を委託していたイセトーがランサムウェア攻撃を受けた影響で、情報が漏えいした恐れがある件を巡り、公文教育研究会（公文）は8月20日、新たに個人情報など約75万人分の漏えいを確認したと発表した。

公文研究会（公式サイトから引用）

● WordPressプラグイン「LiteSpeed Cache」、新たに致命的な脆弱性…6.5.0.1以降に更新を

https://news.mynavi.jp/techplus/article/20240908-3020068/
https://patchstack.com/articles/critical-account-takeover-vulnerability-patched-in-litespeed-cache-plugin/

このニュースをザックリ言うと･･･

- 9月5日(現地時間)、WordPress向けセキュリティサービス等を提供するPatchStack社より、WordPressのサイト高速化機能を提供するプラグイン「LiteSpeed Cache」に脆弱性(CVE-2024-44000)が存在するとして注意喚起が出されています。
- 脆弱性により、外部の攻撃者にユーザーセッションCookieの情報等を奪取され、ユーザーセッションの乗っ取り等に繋がり得るとされています。
- 既に脆弱性を修正したバージョン6.5.0.1がリリースされており、アップデートが強く推奨されています。

AUS便りからの所感

- 脆弱性は、WordPressにおいてデバッグ状態が有効の場合、Webサーバーのレスポンスヘッダー(セッションCookieを発行したSet-Cookie: ヘッダーを含む)がログファイルに出力される、さらに当該ファイルが外部から推測・アクセス可能な場所に保存されるという問題によるものです。
- LiteSpeed Cacheでは8月にも致命的な脆弱性が報告、対策されていました(AUS便り 2024/08/29号参照)が、これとは別の脆弱性で、かつ同様の危険度を持つと評価されています。
- 同じプラグインで短期間に複数回の脆弱性報告、セキュリティアップデートが行われる事態となっていますが、WordPress本体や使用している各プラグインについて常時セキュリティ情報を確認し、自動更新が設定されているか否かに拘らず、必要に応じ全て最新バージョンとなっているか確認する体制が重要です。

TECH+ Powered by マイナビニュース

WordPressの人気のプラグインに脆弱性、600万超のWebサイトに影響

掲載日 2024/09/08 17:36　　著者：後藤大地

Patchstackは9月5日(現地時間)、「Critical Account Takeover in LiteSpeed Cache Plugin - Patchstack」において、WordPressの人気のプラグイン「LiteSpeed Cache」に重大な脆弱性が存在すると報じた。この脆弱性を悪用されると、認証していない第三者に機密情報を窃取され、認証をバイパスされる可能性がある。

なお、LiteSpeed Cacheは2024年8月21日にも緊急(Critical)の脆弱性が存在すると報告され、アップデートを公開している(参考：「LiteSpeed Cacheプラグインに緊急の脆弱性、500万超のWebサイトに影響｜TECH+（テックプラス）」)。

●厚労省・総務省「テレワーク相談センター」の旧ドメイン名、サイト移転から2年足らずで第三者に取得…移転案内も半年のみ実施か

https://www.jiji.com/jc/article?k=2024090601036
https://telework.mhlw.go.jp/
https://www.jiji.com/jc/article?k=2024090601059

このニュースをザックリ言うと･･･

- 9月7日(日本時間)、時事通信より、厚生労働省・総務省が運営する「テレワーク相談センター」のWebサイトで使用していた旧ドメイン名(tw-sodan.jp)が第三者に取得(ドロップキャッチ)されていたと報じられました。
- 当該サイトは2022年10月21日をもって厚労省が使用する「mhlw.go.jp」ドメイン名下の「テレワーク総合ポータル」に移転し、旧ドメイン名は今年3月末に失効していたとのことですが、9月6日の段階で複数の転職サイトを紹介する別サイトの開設が確認されていたとしています(whoisによれば8月1日に「新規取得」された模様です)。
- 一方で他の省庁・地方自治体など公的機関のサイトでは、依然として旧ドメイン名へのリンクが多数残っているとのことです。
- 同9日には、移転先においても、旧ドメイン名は現在関係がないとして注意喚起が出されています。

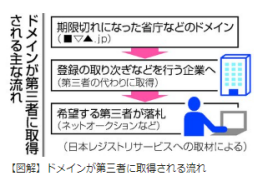
AUS便りからの所感

- 時事通信では、他にも公的機関が「go.jp」等以外で取得していたドメイン名が第三者に取得される事例が多く発生していることを報じています。
- インターネットアーカイブでの記録によれば、2022年12月時点で旧ドメイン名へのアクセス時に移転先を案内するページにリダイレクトするようになっていましたが、2023年3月時点ではリダイレクトがなくなり「404 Not Found」と表示されており、移転からわずか半年で旧サイトにアクセスしてきたユーザーへの案内がなくなっていたものとみられます。
- ドメイン名取得の段階で、外部の第三者がドロップキャッチしにくいとみられる「go.jp」等や、既存のドメイン名のサブドメインを選ぶよう検討することも重要ですが、旧サイトへの多数のリンクが残る中での、リダイレクトや移転案内の終了～ドメイン名の失効までの期間はあまりにも短すぎたと言え、ドメイン名を使用しなくなった後も10年程度は維持および移転先の案内を行うことを推奨致します。

JIJI.COM

厚労省旧ドメイン、第三者が取得　「テレワーク相談」、別サイトに一複数機関がリンク継続

時事通信 社会部　　2024年09月07日07時12分 配信



【図解】ドメインが第三者に取得される流れ

厚生労働省と総務省が行っているテレワーク相談事業で、過去に使っていた旧ウェブサイトのドメイン（インターネット上の住所）を第三者が取得し、複数の転職サイトを紹介する別サイトとなっていることが６日、時事通信社の取材で分かった。国や地方自治体の複数サイトで、同ドメインを使ったＵＲＬへのリンクが残っており、指摘を受けた厚労省は同日までに、同省サイトからリンクを削除した。