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。

●「PPAP」送信禁止企業17.9%、受信禁止も14.4%…JIPDEC調べ

https://www.itmedia.co.jp/news/articles/2203/17/news149.html
https://www.jipdec.or.jp/topics/news/20220317.html

このニュースをザックリ言うと･･･

- 3月17日(日本時間)、日本情報経済社会推進協会(JIPDEC)とアイ・ティ・アール(ITR)社より、1月に国内企業982社のIT/情報セキュリティ担当者に対し実施した「企業IT利活用動向調査2022」の速報結果が発表されました。

- 暗号化ZIPファイルとそのパスワードを(同じメールアドレス宛に)別々のメールで送る行為、いわゆる「PPAP」に関しては、政府・大企業から廃止の動きが進んでいる一方、現時点でそういったメールの送信を禁止している(元々利用していない+明確に禁止した)企業は17.9%、受信は14.4%(および今後禁止予定32.6%)との結果が出ています。

- 今後、特に受信禁止の動きに伴って送信時の対策の必要性が高まることから、送信禁止を予定している企業(26.6%)および他の方法での送信を推奨する企業(15.5%)の割合は、さらに高まる可能性があると分析されています。

AUS便りからの所感等

- 速報では、この他にもコロナ禍を機にテレワークを導入した企業が49.4%(それ以前から導入していたものを合わせると72.7%)等、計6点に関する調査結果が挙げられています。

- PPAPでのデータ送信においては、ZIPファイルとパスワードを電子メールという同じ経路によって送っているために、ビジネスチャットと併用する等別々の通信手段で送る場合に比べ両方が奪取される可能性が理論上高くなること、また暗号化されたファイルでマルウェアスキャンができないこと等が問題視されています。

- 特に現在も感染拡大している「Emotet」がこの手法を悪用し、暗号化ZIPと文面等のなりすましによって、より高い確率で感染しようとする手口をとったことが、PPAP廃止への大きなきっかけとなっています。

- 相手にデータ等を送るための代替手段としては、オンラインストレージ(Google Drive, OneDrive, Dropbox, Box等)やビジネスチャット(Slack, Chatwork等)といったより先進的なサービスの利用が挙げられる一方、企業によってセキュリティポリシーによってアクセスを禁じているケースが未だに多いのは、従業員が個人で契約したサービスを安易にプライベートと企業とで共用していたこと等が原因で情報流出事故が度々発生していたことによるものとみられ、そういった事情は踏まえつつも、頑なにそれらを禁止し続けるよりは、企業向けサービス・プランを正式に契約して従業員に使わせること等を検討すべき段階と思われます。

ITmedia NEWS

PPAP禁止企業は1割前後　なりすましメールの爆発的流行で今後の利用は減少か――JIPDEC調べ

2022年03月17日 16時15分 公開　[松浦立樹，ITmedia]

印刷　141　Share　B!　42　1

PPAPを廃止した、または利用していない企業は計17.9%――そのような調査結果を日本情報経済社会推進協会（JIPDEC）とアイ・ティ・アール（東京都新宿区）が3月17日に発表した。

パスワード付き圧縮ファイルとパスワードを同一経路で時間をずらして送信するPPAPについて、「（メール送信時に）利用している」と答えた企業は30.5%、「利用を禁止していないが他の方法を推奨中」が15.5%、「利用中だが、禁止する予定で他の手段の導入検討中」が26.6%、「利用制限を特に設けていない」は9.5%となった。

● Chromeブラウザーに脆弱性、Edge他にも影響…至急アップデート確認を

https://forest.watch.impress.co.jp/docs/news/1398216.html

このニュースをザックリ言うと・・・

- 3月25日(米国時間)、Googleより、Chromeブラウザーに重大な脆弱性が存在するとして、セキュリティアップデート v99.0.4844.84 がリリースされています。

- 同26日にはMicrosoftより、Chromeと同じエンジン(Chromium)を使用しているEdgeブラウザーにおいてもセキュリティアップデート v99.0.1150.55 がリリースされています。

- 脆弱性はChromiumのスクリプトエンジン「V8」に存在し、既にこれを悪用した攻撃も確認されているとして、至急アップデートが呼び掛けられています。

AUS便りからの所感

- Chromiumを利用しているブラウザーはChromeとEdge以外にも複数存在し、VivaldiやBraveについてもそれぞれセキュリティアップデートがリリースされています(Operaについても後日リリースされるとみられます)。

- Chromeをはじめとするこれらのブラウザーはいずれも自動更新機能を持っていますが、ブラウザーを実行している間は古いバージョンが動作し続け、また裏で新しいバージョンが用意され、再起動を促すメッセージがウィンドウ上に表示されるまでにもタイムラグが発生します。

- 「ヘルプ」→「Google Chromeについて」等を開くことにより、最新のバージョンかどうかの確認ができ、またより新しいバージョンがリリースされている場合はその場で自動更新が開始されるため、ブラウザーを可能な限り速やかに最新のバージョンに保つことが期待できます。

Impress Watch

「Chromium」にゼロデイ脆弱性 ～「Chrome」と「Edge」に緊急アップデート

「Chrome」はv99.0.4844.84、「Edge」はv99.0.1150.55になっていることを確認

樽井 秀人　2022年3月28日 00:05

米Googleは3月25日（米国時間、以下同）、デスクトップ向け「Google Chrome」の最新安定（Stable）版v99.0.4844.84を公開した。本バージョンは、ゼロデイ脆弱性（CVE-2022-1096）に対処したセキュリティアップデート。「Microsoft Edge」でも翌26日に緊急アップデート（v99.0.1150.55）が実施されている。

● JavaScriptライブラリ「node-ipc」にロシアの開発者を攻撃するための不正コードが追加される

https://gigazine.net/news/20220322-sabotage-code-to-node-ipc/
https://qiita.com/SnykSec/items/6e75bd78b4deb3371550

このニュースをザックリ言うと・・・

- 3月16日(現地時間)、イギリスのセキュリティベンダーSnyk Security社より、node.js(サーバーサイドで動作するJavaScript)用ライブラリ「node-ipc」に不正なコードの追加が確認されたと発表されました。

- 不正なコードは、開発者がロシアのウクライナ侵攻への抗議の目的で追加されたとみられ、ユーザーのIPアドレスがロシアおよびベラルーシのものである場合、ファイルの内容を消去してハートの絵文字を追加する挙動を示すとのことです。

- 同様にロシアへの抗議を意図したコードを含むライブラリ等が他にも確認されており、「Protestware」と総称されています。

AUS便りからの所感

- Protestwareの例としては、「es5-ext」や、node-ipcと同じ開発者による「peacenotwar」が挙げられています。

- node-ipcバージョン10.1.1・10.1.2および9.2.2に不正なコードが含まれ、ライブラリをホスティングするGithubやnpmといったサイトからこれらのバージョンは削除されたものの、現時点でnpmでは引き続き問題があるとされる最新バージョン11.1.0が公開されている模様です。

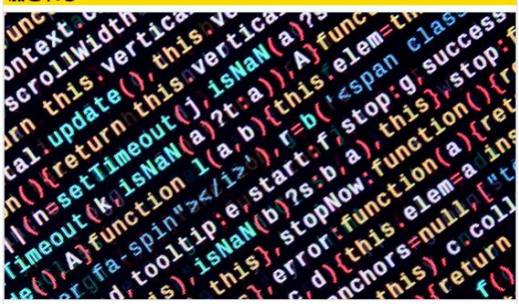
- node-ipcは多くのnode.jsソフトウェアで使用されていたために広範囲で不正なコードの影響があるとみられ、例えば代表的なソフトの一つ「Vue.js」では、node-ipcの安全なバージョンを組み込むよう対策した模様です。

- 今年1月にもJavaScriptライブラリ「colors.js」「faker.js」が開発者自身によって不正なコードへの改変が行われる事案が発生しており(AUS便り2022/01/12号参照)、このような事案を避けるためには、ライブラリを導入する側がSNS等で最新バージョンに関する報告がないか確認しつつ、安全なバージョンをインストールする(ただしセキュリティアップデートがリリースされた場合には必ずそれを使う)よう注意を払うべきでしょう。

GIGAZINE

2022年03月22日 14時00分　セキュリティ

オープンソースのnpmパッケージ「node-ipc」にロシア在住の開発者を標的にした悪意のあるコードがメンテナーによって追加される



オープンソースで開発される、ウェブアプリのUI構築用JavaScriptフレームワーク「Vue.js」のコードに、ロシアとベラルーシに在住する開発者を標的とした悪意のあるコードが追加されたと、開発者向けセキュリティプラットフォームのSnykが発表しました。メンテナーの1人がロシアのウクライナ侵攻に対する抗議行為として、問題のコードを追加したことがわかっています。