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。

●Google向け拡張機能「EditThisCookie」の偽物が公式ストアに登録される

https://securityonline.info/beware-fake-editthiscookie-extension-steals-user-data/

このニュースをザックリ言うと・・・

- 1月3日(現地時間)、Cybersecurity Newsより、Chromeブラウザーの拡張機能「EditThisCookie」の偽物がGoogle公式の拡張機能ストアに登録されていたとして注意喚起が出されています。

- 本物のEditThisCookieは拡張機能の新しい仕様「Manifest v3」に追随していないとしてストアから削除された一方で、Manifest v3に準拠したと称する「EditThisCookie(R)」が第三者によって登録されていたとのことです。

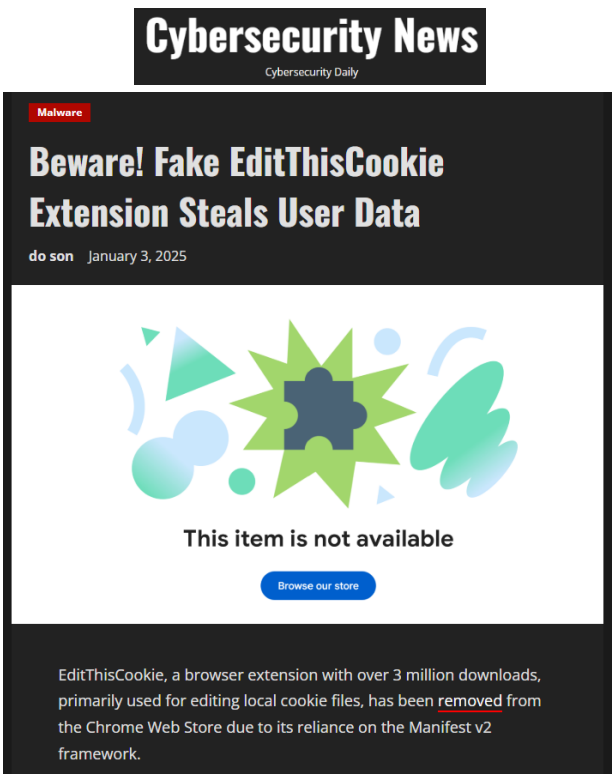
- EditThisCookie(R)には、ユーザーのCookieを盗んだり、SNSに不正な投稿を行うような不審なコードが含まれていたとしており、ストアから削除されるまで約30,000回ダウンロードされたとのことです(同様の偽拡張として「EditThisCookie - Updated for Manifest V3」の登録・削除が確認されています)。

AUS便りからの所感等

- Chromeの拡張機能管理画面において「デベロッパーモード」を有効にすることにより、使用している拡張機能のIDが確認できますが、IDが「fngmhnnpilhplaeedifhccceomclgfbg」でないEditThisCookieは偽物のため、速やかに削除してください。

- Cybersecurity Newsでは、もしも本物のEditThisCookieを使いたい場合は、githubにある本物のレポジトリからインストールすることを推奨していますが、一般的に用いられるインストール方法ではないこと、またEditThisCookie自体が既に6年以上開発が進んでいない古い拡張であることには留意が必要です。

- 同種の機能を提供する他の拡張機能もストアにいくつか登録されている一方、当該拡張がなくてもブラウザー自体でCookieを編集することは一応可能ですし、Chrome等Webブラウザーにインストールされる拡張機能はソフトウェア上で様々な機能の使用を許可されることになりますので、拡張ストアやSNS上でのレビュー・報告等を十分に確認し、必要最低限の拡張機能のみインストール・有効化すること、また後からでも不要な拡張機能の棚卸し、万が一身に覚えのない拡張機能が入っていた場合のアンインストール等を行うことが重要です。



●マカフィー日本法人の旧サイト、ドメイン名失効で乗っ取り

https://forest.watch.impress.co.jp/docs/serial/yajiuma/1652003.html
https://web.archive.org/web/*/https://blogs.mcafee.jp

このニュースをザックリ言うと・・・

- 12月27日(日本時間)、X(旧・Twitter)において、かつて存在したマカフィー日本法人のブログサイトが第三者による別のブログになっていたことが取り上げられています。
- 同法人が使用していたドメイン名(mcafee.jp)が失効、第三者に取得されたことによるもので、いわゆる「パパ活」を題材にしたブログが表示されていたことがインターネットアーカイブにて確認されています。
- ブログ記事は1月6日までには削除された模様ですが、同9日時点でWebサイト自体は存在しています。

AUS便りからの所感

- マカフィー日本法人による当該ブログは2022年10月に閉鎖し、以降「Trellix」ブランドのサイトへリダイレクトしていましたが、ドメイン名が2023年8月1日に第三者に取得されたことがwhoisから確認されており、ブログ閉鎖から1年弱程度で失効したとみられます。
- サイト・サービス終了からほどなくして失効したドメイン名が第三者によって奪取される、いわゆる「ドロップキャッチ」の事象は過去度々発生し、過去のサイトになりすまして詐欺サイトに誘導するケースも報告されており(AUS便り 2024/12/12号参照)、こと今回は大手セキュリティベンダーによってこのような事態が引き起こされたことが話題になっています。
- 安易に新規ドメイン名の取得を行わず、既存のドメイン名のサブドメイン等でサイト・サービスの設置が可能でないか検討すること、終了後もドメイン名を長期間保持すること等が推奨されている一方、昨年末には「サブドメインが第三者により乗っ取り可能な状態だったものを保護した」とするケースが報告され(後日取り上げます)、技術的に適切な対策はその都度異なることには注意が必要でしょう。

●「HTMLでありZIPでありPNG」なファイル

https://forest.watch.impress.co.jp/docs/serial/yajiuma/1650214.html
https://github.com/gildas-lormeau/Polyglot-HTML-ZIP-PNG

このニュースをザックリ言うと・・・

- 12月24日(日本時間)、インプレス社「やじうまの杜」において、同22日にX(旧・Twitter)で特殊な形式のファイルが取り上げられたことが話題となっています。
- ファイルはフランスのプログラマーが考案したもので、ZIPファイルおよびPNGファイルの形式を巧妙に利用し、ZIP・PNGあるいはHTMLファイルとして認識され得る内容になっているとのことです。
- 作者のgithubサイトから「demo.png.zip.html」というサンプルファイルをダウンロードし、そのまま開くことによりHTMLとして、.html拡張子を削ることでZIPファイルとして、さらに.zip拡張子を削ることでPNGファイルとして開かれることが確認できます。

AUS便りからの所感

- 複数の形式に認識され得るファイルは「Polyglot」、またある形式のファイルに別の形式のデータを埋め込んで秘匿・流通させる手法は古くから「ステガノグラフィー」という名称で知られています。
- 前述したサンプルファイルは特別なツールを用いずともHTML・ZIP・PNGそれぞれの形式としてデータを取り出すことができ、あくまでコンセプトを示したと思われますが、この状態で、あるいは別途秘匿技術を追加することにより、マルウェアの検出の回避に悪用される可能性も考えられます。
- アンチウイルス・UTM等において、実際にマルウェアの秘匿を回避されてしまうケースが発生するか、あるいはアンチウイルス等が安全側に倒してこのような「通常の用途では使用されない」であろうファイルを確実に不審なファイルないしマルウェアとして検出するようになるのかが注目されるところです。