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。

●不正なChrome拡張機能、公式ストアで多数発見される

https://gigazine.net/news/20230602-chrome-web-store-malicious-extensions/
https://palant.info/2023/05/31/more-malicious-extensions-in-chrome-web-store/
https://palant.info/2023/06/08/another-cluster-of-potentially-malicious-chrome-extensions/

このニュースをザックリ言うと･･･

- 5月31日(現地時間)、セキュリティ研究者のウラジミール・パラント氏より、Chrome公式の拡張機能ストアにおいて悪意のある拡張機能が多数発見されたとして注意喚起が出されています。

- 同氏は、「PDF Toolbox」という拡張機能において、任意のWebサイトへのアクセス時に外部のアドウェア配布サイトからスクリプトを読み込む挙動を確認し、5月16日にブログで発表していましたが、その後これを含む34の拡張機能で同様に不正なスクリプトを読み込むものが報告されたとのことです。

- 6月以降これらの拡張機能はGoogleによる公式ストアからの削除が進んでおり、その後当初報告された34の拡張機能は全て削除されましたが、新たに120近くの不正な拡張機能が報告されています。

AUS便りからの所感等

- 人気のあるソフトウェアの公式の拡張機能ストアで不正な挙動を示す拡張が発見された事例は、先日も開発者向けツール「Visual Studio Code」で発生しています。

- ストアに登録された当初は害のなかった拡張機能が、ある程度人気を得るまで潜伏してから悪意のあるコードを追加するケースや、買収等で開発元が変わったことをきっかけに不正な挙動が追加されるケースも決して珍しくはありません。

- Chrome以外にもFirefox等のWebブラウザーあるいはスマートフォンアプリと同様、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。

GIGAZINE

2023年06月02日 19時00分　　セキュリティ

悪意あるコードが仕込まれたChrome拡張機能が大量に発見される

セキュリティ研究者で、有名な拡張機能「AdBlock Plus」の元開発者でもあるウラジミール・パラント氏が、Chromeウェブストアにある多数の拡張機能に難読化された悪意あるコードが含まれていたことを発表したと報告しました。

More malicious extensions in Chrome Web Store | Almost Secure
https://palant.info/2023/05/31/more-malicious-extensions-in-chrome-web-store/

パラント氏が最初にこの問題を発見したのは、PDFファイルの編集や結合などの機能を持つ「PDF Toolbox」という拡張機能です。200万人以上のユーザーと「4.2」の評価を得ていたこの拡張機能は、表面的には何の変哲もない拡張機能でしたが、アドウェアを配布している「serasearchtop[.]com」というドメインにアクセスし、ブラウザで訪問したあらゆるサイトに任意のJavaScriptコードを挿入する機能を持つことが、パラント氏の詳細な分析により判明しました。

しかし、この拡張機能には広範な権限の要求を正当化するために実装されたPDF変換機能や、無害なデータに見せかけて不審なファイルをダウンロードする偽装コード、すぐにはリクエストを出さないようにして検知を回避する仕組みなどが備わっており、この問題は少なくとも1年間は誰からも気づかれないままだったとのこと。

● FortiOSのSSL-VPNに新たな脆弱性…最新バージョンへアップデートを

https://www.ipa.go.jp/security/security-alert/2023/alert20230613.html
https://www.fortinet.com/jp/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

このニュースをザックリ言うと･･･

- 6月13日(日本時間)、Fortinet社より、同社の各種製品に存在する脆弱性に関する21件の情報が発表されました。
- このうちFortiOS・FortiProxyのSSL-VPN機能に存在する脆弱性の一つ(CVE-2023-27997)について、機器上で任意のコード・コマンドが実行される可能性がある、特に危険度が高いものとされており、既にこれを悪用した攻撃も確認されているとして、同社の他IPAからも注意喚起が出されています。
- Fortinet社ではFortiOS等について脆弱性を修正した最新バージョンをリリースしており、速やかにアップデートを行うよう呼び掛けています。

AUS便りからの所感

- CVE-2023-27997の脆弱性が修正されたのは、FortiOSバージョン6.0.17・6.2.14・6.4.13・7.0.12・7.2.5・7.4.0、FortiOS-6K7KバージョンFortiOS-6K7K 6.0.17・6.2.15・6.4.13・7.0.12、FortiProxyバージョン2.0.13・7.0.10・7.2.4となっています。
- FortiOSやFortiProxyでは、ここ数年にSSL-VPNの重大な脆弱性が度々発見・修正され、これらを悪用して組織内ネットワークに侵入する等の攻撃が発生しています。
- 未対策の機器については早々に攻撃者に発見されてターゲットとなること、さらには脆弱性情報が発表される前に脆弱性を悪用されている可能性も考えられるため、SSL-VPN機能を使用している場合は速やかにアップデートを行い、またVPNアクセスログ等を確認し、アップデートまでの間に攻撃を受けた様子が見られた場合はアカウント情報の変更等を行うことを強く推奨致します。


Fortinet 製 FortiOS および FortiProxy の脆弱性対策について(CVE-2023-27997)

最終更新日：2023年6月13日

概要

Fortinet 社より、FortiOS 及び FortiProxy に関する脆弱性が公表されました。

これらの製品において、ヒープベースのバッファオーバーフローの脆弱性が確認されています。

本脆弱性を悪用された場合、認証されていない遠隔の第三者によって細工したリクエストを送信され、任意のコードまたはコマンドを実行される可能性があります。

今後被害が拡大する可能性があるため、早急に対策を実施してください。

影響を受けるシステム

- FortiOS バージョン 7.2.0 から 7.2.4
- FortiOS バージョン 7.0.0 から 7.0.11
- FortiOS バージョン 6.4.0 から 6.4.12
- FortiOS バージョン 6.0.0 から 6.0.16
- FortiProxy バージョン 7.2.0 から 7.2.3
- FortiProxy バージョン 7.0.0 から 7.0.9
- FortiProxy バージョン 2.0.0 から 2.0.12
- FortiProxy 1.2 系の全てのバージョン
- FortiProxy 1.1 系の全てのバージョン
- FortiOS-6K7K バージョン 7.0.10

●「.zip」ドメイン名を悪用するフィッシングの可能性…5月より登録開始

https://news.mynavi.jp/techplus/article/20230601-2691564/
https://thehackernews.com/2023/05/dont-click-that-zip-file-phishers.html
https://mrd0x.com/file-archiver-in-the-browser/
https://gigazine.net/news/20230515-zip-tld/

このニュースをザックリ言うと･･･

- 5月29日(米国時間)、The Hacker Newsより、「.zip」ドメイン名(gTLD)を悪用したフィッシングの可能性を示唆するデモンストレーションが挙げられ、注意喚起が出されています。
- フィッシングのデモは、セキュリティ研究者のmr.d0x氏によるもので、圧縮展開ソフト「WinRAR」の画面を模倣したWebページを「.zip」ドメイン名の下でホスティングしており、圧縮ファイル内のPDFファイルに見立てられたリンク等をクリックすると関係ないファイルがダウンロードされるといった仕掛けになっています。
- mr.d0x氏のブログ記事では、リンククリック時に別のサイトへリダイレクトするような仕組みも可能としています。
- 「.zip」ドメイン名は、Googleが5月10日に一般登録受付を開始しましたが、技術者やセキュリティ研究者等の間ではマルウェアダウンロード等の攻撃に悪用される懸念が出される等の議論となっています。

AUS便りからの所感

- Googleでは「.zip」を含め計8つのgTLDの受付を開始しており、例えば「.mov」等についても悪用のリスクが指摘されています。
- またブラウザーのアドレスバーにキーワードを入力してサーチエンジンのページに飛ぶ場面で、「***.zip」といったキーワードを入力した際に、検索結果ではなくそのドメイン名を持つサイトに直接アクセスするケースがあり、これを狙ってフィッシングサイトなどを用意する事例も懸念されています。
- mr.d0x氏は組織内からのWebアクセスにおいて「.zip」「.mov」といったドメイン名のサイトをブロックすることを推奨しており、UTM等でそういった機能があり、安全側に倒してフィッシングサイト等へのアクセスを厳しくブロックしたいというのであれば、設定を検討するのも一考でしょう。


新しいドメイン「.zip」を悪用したフィッシング手法発見、WinRARを模倣

掲載日 2023/06/01 07:46　　著者：後藤大地

The Hacker Newsは5月29日(米国時間)、「Don't Click That ZIP File! Phishers Weaponizing .ZIP Domains to Trick Victims」において、.zipドメインを悪用する新たなフィッシングキャンペーンが展開されていると報じた。.zipドメインを使ってWebブラウザでファイルアーカイブソフトウェアを模倣するというフィッシング手法が特定されている。

The Hacker News　Subscribe to Newsletter

Along with lots of new features

Don't Click That ZIP File! Phishers Weaponizing .ZIP Domains to Trick Victims