— AUS（アルテミス・ユーザ・サポート）便り 2020/11/02号 —
https://www.artemis-jp.com

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。

●Chrome向け広告ブロック拡張「Nano Defender」「Nano Adblocker」がマルウェア化？…ストアから削除

https://internet.watch.impress.co.jp/docs/yajiuma/1283656.html
https://togetter.com/li/1609270
https://280blocker.net/blog/20201016/2590/

このニュースをザックリ言うと･･･

- 10月15日(日本時間)、Google Chrome向けの広告ブロック用アドオン(拡張)「Nano Defender」「Nano Adblocker」が「マルウェア化」したことが確認され、その後Google公式の拡張ストアから削除される事件がありました。

- 同11日、同種のアドオンである「280blocker」の開発者より、Nano Defender等の開発者がこれらを身元不明の第三者に売却したとして、これらをインストールしている場合は削除するよう注意喚起が出されていました。

- そして同15日にアップデートがリリースされ、ブラウザーの行動データをリモートサーバーへと送信できるソースコードが挿入されていたことが、やはり同種のアドオン「AdGuard」「uBlock Origin」の開発者等により確認されています。

- その後同17日頃までには、Nano Defender等は拡張ストアから削除されたとのことです(批判を受けての撤回か、拡張ストア側での対応かは不明です)。

AUS便りからの所感等

- Nano Defender・Nano Adblockerは、広告ブロック用アドオンとして人気が高かった「uBlock Origin」から派生したものとされますが、その後開発が停滞したことから第三者の売却に応じたとされています。

- 国内ではそのuBlock Originほどではなくともある程度のユーザーがいたとされる一方、今回のように他の拡張の開発者等が状況を監視し、注意喚起を出していなかったならば、当該拡張をインストールしていたユーザーが表沙汰にならないまま被害を受けていた恐れも考えられます。

- 2018年にはChromeの他Firefoxでも人気のあった拡張「Stylish」が不審な挙動を示していたことが発覚し、削除されています(AUS便り 2018/7/17号 参照、ただし現在復活している模様で、「Stylus」等代替拡張の使用が推奨されています)。

- Webブラウザーのアドオンをインストールする際はネット上の情報・評判に随時目を向け、そして現在インストールされている全てのアドオンについても問題が報告されたものは速やかに削除し代替アドオンに切り替えること、また可能な限り必要最小限のインストールに留めることが肝要です(これはスマートフォンアプリの導入あるいはSNSにおけるアプリ連携についても同様に言えることです)。

Impress Watch

やじうまWatch

Chrome向け広告ブロッカーが突如マルウェアへと変貌、アンインストールを呼び掛け中

tks24　2020年10月19日 14:00

ツイート　リスト　B! 85　Pocket　78　いいね！ 284　シェア

Chromeで動作する広告ブロッカーが第三者に売却されたのち、わずか10日後にはマルウェアへと変貌したことが発覚し、専門家はアンインストールを呼び掛けている。

これはChrome拡張機能「Nano Defender」および「Nano Adblocker」。フィルタリングツール「uBlock Origin」に手を加えて作られたこれら拡張機能は、20万件のダウンロード実績を持ち、星4.7つという高いスコアを誇る広告ブロッカーだが、収益化を断念した開発者が第三者に権利を売却したところ、わずか10日後には新バージョンが予告なく公開された。不審に思ったコミュニティメンバーがファイルを調査したところ、ユーザーのブラウザーの行動データをリモートサーバーへと送信できるソースコードが追加されていることが判明し、現在、ユーザーに対してアンインストールを呼び掛けている。この拡張機能自体、登場したのが昨年ゆえ、日本では決して知名度は高くないが、日本語での導入記事はこれまで何本か公開されているので、Chromeユーザーは知らず知らずのうちに導入していないか、ざっとチェックしておいたほうがよさそうだ。なお、これらの拡張機能は現在、

●「カードのご利用を一部制限」…MyJCBを騙るフィッシングに注意喚起

https://internet.watch.impress.co.jp/docs/news/1286280.html
https://www.antiphishing.jp/news/alert/myjcb_20201029.html
https://www.jcb.co.jp/news/phishing_20200929.html

このニュースをザックリ言うと・・・

- 10月29日(日本時間)、フィッシング対策協議会より、MyJCBを騙るフィッシングメールが出回っているとして注意喚起が出されています。

- フィッシングメールは、件名が「＜重要＞【My JCB】ご利用確認のお願い」、本文に「誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。」等と書かれ、カードの利用確認の為のサイトとして各種情報(MyJCB ID・パスワード・カード番号・有効期限・お名前・生年月日・ご登録電話番号・セキュリティコード・ご希望のMyJCBパスワード・Eメールアドレス)を詐取しようとする偽サイト(ドメイン名は「my.jcb.co.jp.●●●●.com」)に誘導されるとしています。

AUS便りからの所感

- JCBからの情報
(https://j-faq.jcb.co.jp/faq/show/1544?site_domain=default)
には、11月2日に確認された新たなフィッシングメールとして
「「お客様情報の変更」に関する手続きが未完了しました。」
という文面のものが挙げられており、今後も様々な内容のフィッシングメールが拡散するとみられます。

- 同協議会では、このようなサイトで個人情報等を入力しないことの他にも、日頃からサービスへログインする際、メールやSMS内のリンクではなく、いつも利用しているスマートフォンの公式アプリやブラウザーのブックマークなどからアクセスするよう呼び掛けています。

- サービスによっては実際に正式なメールやSMSにリンクを掲載しなくなったところも出てきており、自社サービスのユーザーをフィッシングから保護するための有用な方策として今後より広まっていくことに期待したいものです。

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

●Webサイト改ざん、選挙資金流出…トランプ氏陣営へのサイバー攻撃

https://japan.zdnet.com/article/35161629/
https://japan.zdnet.com/article/35161727/

このニュースをザックリ言うと・・・

- 10月27日(現地時間)、アメリカ大統領選挙の再選に向けて活動中のドナルド・トランプ氏陣営より、選挙キャンペーンのWebサイトが攻撃を受け、改ざんされていたと発表されました。

- 改ざんされたサイトには「donaldjtrump.com は差し押さえられた」「大統領が拡散するフェイクニュースに世界中がうんざりしている」等と書かれていたとされていたものの、機密データがリスクにさらされることはなかったとしています。

- 同29日には、ウィスコンシン州の共和党より、サイバー犯罪者からのフィッシング攻撃を受け、選挙資金230万ドル(約2億4000万円)が奪取されたと発表されました。

AUS便りからの所感

ZDNet Japan

- 選挙資金の流出については、選挙活動のメール送信や支持者の帽子製作を担当する業者を騙った、いわゆる「ビジネスメール詐欺」によるものとされています。

- 前回2016年の大統領選挙では、トランプ氏当選を目的としたロシアによるサイバー攻撃やSNSによる世論工作等が行われたとされますが、今回投票日まで一週間を切ったタイミングでこのような攻撃を行ったのが他国によるものか、トランプ氏や共和党に敵対する者か、あるいは純粋にイベントに便乗した犯罪なのかについては、選挙終了後に調査が行われ、明らかになるとみられます。

- オリンピックあるいは新型コロナウイルスと同様、世界的な注目を集める出来事にはサイバー犯罪がついて回るものであり、当然ながら攻撃の手が無関係の人々をターゲットとすることも珍しくないため、常に今発生している攻撃の情報に注目し、アンチウイルス・UTM等による防御を確実に行いつつ慎重に行動することが重要です。

トランプ陣営のウェブサイト、一時改ざんされる

this site was seized

the world has had enough of the fake-news spreaded daily by president donald j trump.

it is time to allow the world to know truth.

multiple devices were compromised that gave full access to trump and relatives. most internal and secret conversations strictly classified information is exposed proving that the trump-gov is involved in the origin of the corona virus.
we have evidence that completely discredits mr trump as a president. proving his criminal involvment and coorperation with foreign actors manipulating the 2020 elections. the US citizens have no choice

Trump大統領の選挙陣営サイトは、一時的に改ざんされていた。