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。

●災害時用無料Wi-Fi「00000JAPAN」悪用した攻撃に内閣府が注意喚起

http://www.itmedia.co.jp/news/articles/1807/10/news063.html
https://twitter.com/nisc_forecast/status/1016246248649605121

このニュースをザックリ言うと・・・

- 7月9日（日本時間）、内閣サイバーセキュリティセンター（NISC）より、災害時用の無料Wi-Fi（統一SSID）である「00000JAPAN」を悪用する攻撃への注意が呼び掛けられています。

- 西日本を中心に発生したいわゆる「平成30年7月豪雨」で提供されていることを受けてのもので、利便性確保のため暗号化がされていないこと等から、通信の盗聴や偽のアクセスポイント（AP）への接続による情報の奪取が行われる危険性があるとしています。

- NISCでは、利用にあたり、
●緊急時のやむを得ない安否確認や情報収集のみに利用すること
●ID・パスワード・個人情報の入力やお金が関係するサービスの利用は極力避けること
●携帯電話回線が通じる場合はそちらを利用すること
を推奨しています。

AUS便りからの所感等

- Webサイトに対しHTTPSでアクセスできる場合、Wi-Fi通信が暗号化されていなくても理論上盗聴はされなくなりますが、偽のAP等でフィッシングサイトに誘導される可能性も考えられるため、アクセス先サイトの十分な確認は不可欠でしょう。

- NISCでは、「00000JAPAN」に限らず無料Wi-Fiを利用する必要がある場合、VPNソフトを使うことも呼び掛けており、こちらもスマホ等からVPN接続先のルータまでの暗号化が行われ、安全性が高まることが期待できますが、利用される割合はまだまだ低い印象がありますので、ルータやUTMが機能を提供しているのであればぜひ活用し、可能な限り通常から利用するよう心掛けられれば幸いです。


ITmedia NEWS

災害時用無料Wi-Fi「00000JAPAN」悪用した攻撃に内閣府が注意喚起

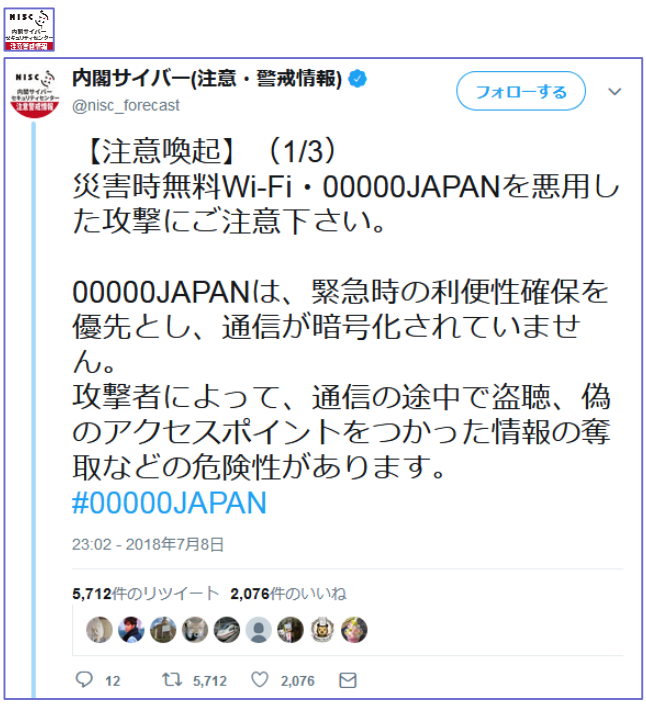
2018年07月10日 09時30分 公開 [ITmedia]

印刷 通知 816 503 B! 45

西日本豪雨の被災地などで、災害時用の無料Wi-Fi（統一SSID）「00000JAPAN」（ファイブゼロジャパン）が提供されている。ただ、通信が暗号化されておらず、同名のSSIDを設定したなりすましも可能。通信内容が第三者に盗聴されるリスクがあるため、「緊急時のやむを得ない安否確認や情報収集のみに利用してほしい」と、内閣サイバーセキュリティセンター（NISC）が注意を呼び掛けている。

「00000JAPAN」は、大規模災害時に無料開放する災害用統一SSIDとして2014年に世界で初めて策定。冒頭に「00000」を付けてSSIDの検索結果上位に表示されるようにし、「JAPAN」を加えて海外からの救援者にも理解しやすい文字列にした。6月18日に発生した大阪府北部を震源とする地震の被災地や、7月上旬に西日本を襲った豪雨の被災地で提供されている。

ただ「00000JAPAN」は、緊急時の利便性確保を優先して通信が暗号化されていない。このため、「攻撃者によって、通信の途中で盗聴、偽のアクセスポイントを使った情報の奪取などの危険性がある」と内閣府は指摘。「緊急時のやむを得ない安否確認や情報収集のみに利用し、ID、パスワード、個人情報の入力、お金が関係するサービスの利用は極力避けて下さい」とし、携帯電話回線が通じる場合は、そちらを利用するよう呼び掛けている。また、これに限らず無料Wi-Fiを利用する必要がある場合は、VPNソフトを使って通信することをすすめている。


内閣サイバー(注意・警戒情報)
@nisc_forecast
フォローする

【注意喚起】（1/3）
災害時無料Wi-Fi・00000JAPANを悪用した攻撃にご注意下さい。

00000JAPANは、緊急時の利便性確保を優先とし、通信が暗号化されていません。
攻撃者によって、通信の途中で盗聴、偽のアクセスポイントをつかった情報の奪取などの危険性があります。
#00000JAPAN

23:02 - 2018年7月8日

5,712件のリツイート 2,076件のいいね

12 5,712 2,076

●「C:¥Temp」「C:¥Intel」フォルダは不正ツールが設置されやすい？　標的型攻撃に類似点

https://internet.watch.impress.co.jp/docs/news/1132436.html

このニュースをザックリ言うと・・・

- 7月11日（日本時間）、情報処理推進機構（IPA）傘下で標的型サイバー攻撃の被害拡大防止を目的とするサイバーレスキュー隊「J-CRAT(ジェイ・クラート)」の2017年下半期の活動状況が報告されました。

- 2017年にJ-CRATが受けた相談件数は412件（2016年519件）、同年の上半期・下半期ではそれぞれ254件・158件となっています。

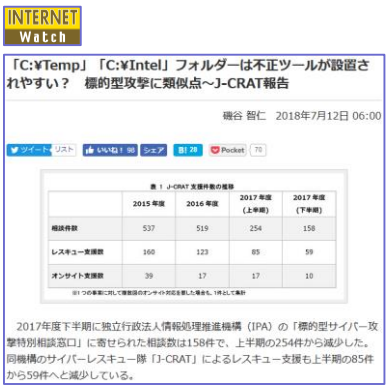
- 2017年度に発生した学術関係組織への複数の不正アクセス事例を調査した際にいくつかの共通点を確認しており、例えば「C:¥Temp」や「C:¥Intel」といったフォルダに不正ツールが設置されやすい等としています。

AUS便りからの所感等

- C:¥ の直下にはログインしているユーザの権限でフォルダを新規作成することが可能で、例えばマルウェアによって密かにフォルダを作成される可能性もあり、不審そうな名前のフォルダがあるか否か人間が安易に判断せず、アンチウイルスによるスキャンを行うことが重要です。

- 報告ではこの他に「マルウェアに感染したが情報窃取を免れた事例」として、既知の攻撃で行われていたような不審な通信をゲートウェイが検出して通信をブロックし、その後攻撃者が様々なマルウェアの設置を試みている間に感染端末が特定され、ネットワークから切り離されたというケースが挙げられています。

- これまでにあった攻撃がどういうものであったかという情報を収集しつつ、UTM等による十分なセキュリティ対策を整えることにより、万が一マルウェアに感染しても情報の流出を食い止められる場合もあるということです。


INTERNET Watch

「C:¥Temp」「C:¥Intel」フォルダーは不正ツールが設置されやすい？　標的型攻撃に類似点～J-CRAT報告

磯谷 智仁　2018年7月12日 06:00

	2015 年度	2016 年度	2017 年度（上半期）	2017 年度（下半期）
相談件数	537	519	254	158
レスキュー支援数	160	123	85	59
オンサイト支援数	39	17	17	10

2017年度下半期に独立行政法人情報処理推進機構（IPA）の「標的型サイバー攻撃特別相談窓口」に寄せられた相談数は158件で、上半期の254件から減少した。同機構のサイバーレスキュー隊「J-CRAT」によるレスキュー支援も上半期の85件から59件へと減少している。

●人気のFirefoxアドオン「Stylish」がポリシー違反でブロック、すべての閲覧履歴を収集か

https://forest.watch.impress.co.jp/docs/news/1131143.html

このニュースをザックリ言うと・・・

- 7月3日（現地時間）、Firefoxブラウザを提供するMozilla社より、人気のあったアドオン（拡張機能）「Stylish」をポリシー違反でブロックしたと発表されました。

- Stylishは2017年にWebサイト分析サービス等を提供するSimilarWeb社に買収されていましたが、ブラウザのアクセス履歴を収集していたことが7月2日にセキュリティ研究者の調査により発覚したものです。

- Stylishは既にアドオンサイト（addons.mozilla.org）から削除された他、インストール済みのものも無効化されるとのことです（また、Chromeブラウザにも提供されていましたが、こちらも削除されています）。

AUS便りからの所感等

- SimilarWeb社はユーザを特定できない「非個人情報」をサービス向上のため収集すると主張していましたが、実際にはパスワードのリセットなどで用いられる認証トークンを含んだURLや、コンテンツの共有に使われるワンタイムURLといったものまであらゆるURLを送信していたとされ、個人の特定どころか、機密情報の入手もでき得る状態にあったとされています。

- 今回のようにブラウザのアドオンが企業に買い取られ、不正な行為を行うようなアップデートがされ、批判を受けて削除されるケースは、有名・無名に拘らず確認されています。

- Stylishが買収された後に元開発者が同様のアドオンである「Stylus」をリリースしており、既に使用しているユーザも多いようですが、いずれにせよ、ネット上の評判を随時調べつつ、問題があったアドオンは速やかに削除すること、また不用意なアドオンのインストールを行わないよう注意しましょう。


窓の杜 WINDOWS FOREST

人気のFirefox拡張機能「Stylish」がポリシー違反でブロック、すべての閲覧履歴を収集か

有志のセキュリティエンジニアによる調査で発覚

樽井 秀人　2018年7月4日 13:40

Mozillaは3日（米国時間）、拡張機能「Stylish」を「Firefox」のブロックリストに追加したことを明らかにした。"Firefox Add-ons"での掲載が中止されるほか、利用中の場合は自動で無効化され、利用できなくなる。

「Stylish」は、「Firefox」のユーザースタイルシートを管理するアドオン。Webページをカスタマイズして見やすくできるとして人気を博し、2017年1月、Webサイト分析サービスなどを提供するイスラエルのSimilarWeb社によって買収されていた。