

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。

●ルータにサイバー攻撃か…ネット接続で不具合相次ぐ

<https://www.asahi.com/articles/ASL3X5SXGL3XULZU00Z.html>
<http://blog.nicter.jp/reports/2018-02/router-dns-hack/>
https://www.ntt-east.co.jp/info/detail/180328_01.html



このニュースをザックリ言うと…

- 3月26日(日本時間)、情報通信研究機構(NICT)より、「**自宅のWi-FiルータのDNS情報が書き換えられ、接続障害や不審なAndroidアプリのダウンロードが発生している**」という報告がTwitter等で寄せられているとして注意を呼び掛けています。

- 3月28日にはNTT東西各社も、同社が法人向けに販売する「**Netcommunity OGシリーズ(OG410Xa, OG410Xi, OG810Xa, OG810Xi)**」について報告が多いことを受けて注意喚起をしています。

- 問題の発生時には、正規のサイトにアクセスしようとしても「**Facebook拡張ツールバックを取付て安全性及び使用流畅性を向上します。**」というメッセージとともにAndroidアプリがダウンロードされ、これをインストールするとGoogleアカウントの入力を求める不審なページが表示されるということです。

AUS便りからの所感等

- 特定機種ルータ利用時の報告が多いとのことですが、実際には機種固有の問題ではなく、**ルータの管理画面にログインするパスワードが「初期状態から変更されていない」ことが原因**で設定を書き換えられるケースが多いようです。

- 初期設定からパスワードを変更しないまましていると、一たび内部ネットワークに攻撃者が侵入した場合、容易に機器を乗っ取られ、特にこのようなルータの場合は大きな影響をもたらすことに繋がるため、NTT東西各社では、このような現象が発生した場合は管理画面のパスワードを変更すること等を推奨しています。

- PCやスマホ・タブレットと比較して、ネットワーク機器・IoT機器はユーザが頻繁に触らず、適切に管理するよう意識が及びにくいことが往々にして有り得ますが、全ての機器について、設置の際に必ずパスワードを設定するとともに、以後も確実に管理を行うよう注意してください。

朝日新聞 DIGITAL

ルータにサイバー攻撃か ネット接続で不具合相次ぐ

編集部員・須藤健也 2018年3月28日20時46分

3月26日

NTTが法人向けに販売するインターネット接続用のルータ…機器などにつ

き、Wi-Fiルータやスマートフォン画面に意味不明なメッセージが表示され、ネットにつながらなくなる不具合が相次いでいる。被害規模は分かっていないが、サイバー攻撃を受けた可能性があり、国立情報学研究所の「情報通信研究機構(NICT)」などが調べている。

NICTの久保正樹さんによれば、NICTもこうした不具合を把握しており、メッセージが表示された後、ウイルスとみられるファイルが送り込まれる仕掛けがあることを確認したという。久保さんは「対策は今のところ見つかっていない。特定のルータ…固有の事象ではないとみられる部分があり、今後も調査する」と話す。

ツイッターでは15日ごろから同様の不具合を訴える書き込みがあり、NTTの法人向けルータ…以外の名前も挙がっている。兵庫県 姫路市のパソコン保守・修繕会社に電話取材すると、26日に顧客の企業から不具合の相談があり、対応したところNTT以外の家庭用ルータ…製品だったという。

NTT東日本・西日本の両社は28日夜、不具合が認められたルータ…について注意喚起する情報をホームページ上に掲載した。機器の設定変更によって不具合が解消するとい

設定変更方法の問い合わせ先は東日本が0120-970413(携帯電話は03-5667-7100)、西日本が0120-248995。受付時間はいずれも年末年始を除いた午前9時~午後5時。(編集部員・須藤健也)

NICTER Blog

Wi-FiルータのDNS情報の書き換え後に発生する事象について

Mar 26, 2018
Categories: Events
#android, #router, #dns, #wifi
5 min read

3月18日ごろより、Twitterやブログ等で、自宅のWi-FiルータのDNS情報が書き換えられ、インターネットに接続できなかったり、不審なAndroidアプリケーションがダウンロードされるという情報が公開されています。

DNS書き換え後に発生する攻撃の流れ

- 悪性DNSサーバは、自身への名前解決クエリに対してマルウェア配布用WebサーバのIPアドレスを返答する。ただし、facebook.com, twitter.com, www.google.comについては、正規のIPアドレスが返答される
- Wi-Fiルータ経由でWebサイトにアクセスしようとする、悪性DNSサーバによって名前解決が行われた結果、マルウェア配布用悪性Webサーバに誘導される。そして、「Facebook拡張ツールバックを取付て安全性及び使用流畅性を向上します。」のアラートが表示される



NTT東日本

「Netcommunity OGシリーズ」におけるインターネット接続不可事象について

2018年3月28日
東日本電信電話株式会社

現在、ひかり電話オプティクス/レノバ/電話オプティクス対応アダプター「Netcommunity OGシリーズ(以下、本機種)」のセキュリティ設定を無効している場合には、本機種に接続した端末(PC等)からWebサイト等を開けようとするとき、Facebook拡張ツールバックを取付て安全性及び使用流畅性を向上しますというメッセージが出てインターネット接続ができなくなるという事象が発生しています。

本事象が発生している場合は、ご利用機器の設定を変更いただくことで解決いたします。本機種を安全に利用いただくための基本的対応として、機器設定画面のログインパスワードの変更及び、セキュリティ設定を有効にしていることを確認する必要があります。本機種をご利用のお客様は今一度設定内容も確認いただくようお願いいたします。

1. 対象機器
 - ひかり電話オプティクス/レノバ/電話オプティクス対応アダプター
 - Netcommunity OG410a
 - Netcommunity OG410Xi
 - Netcommunity OG810a
 - Netcommunity OG810Xi
2. 発生条件
 - 以下の条件を満たす場合に発生する可能性があります。
 - (1) 本機種をインターネット接続用途で利用している場合。
 - (2) インターネット接続設定でセキュリティ設定を無効して利用している場合。
 - (3) 機器設定画面のログインパスワードを初期値より変更していない場合。
3. 発生事象
 - 本機種に接続した端末(PC等)からWebサイト等を開けようとするとき、Facebook拡張ツールバックを取付て安全性及び使用流畅性を向上しますというメッセージが出てインターネット接続ができなくなるという事象が発生しています。
4. 対処方法
 - ご利用機器の設定変更は下記手順を参照してください。
 - 設定変更の方法については、下記の窓口にお問い合わせください。
 - 【機器の設定に関するお問い合わせ先】
お客様窓口(お問い合わせセンター)
お問い合わせ先:03-6708-9913(03-6708-7100)

●「Windows 10」と「7」でマルウェア感染数に大差…ウェブルート調査



<https://japan.zdnet.com/article/35116730/>

このニュースをザックリ言うと…

- 3月下旬、セキュリティベンダーのWebroot社より、同社製品を2017年に利用していた**Windows 10搭載PCとWindows 7搭載PCにおけるマルウェアへの感染レベルの調査結果**が発表されました。
- Win10搭載PC1台あたりの平均マルウェア検出数が0.04個だったのに対し、Win7搭載PCでは0.08個であったことから、**Win10はWin7より「2倍安全である」と結論**付けています。

AUS便りからの所感等

- 3月22日（米国時間）のMicrosoftの発表によれば、企業が所有するWin10搭載PCの50%超が同社製の「Windows Defender」を利用している（Win7・8搭載PCでは18%）とのこと。
- Win7からWin10まで6年近くの間に新たに組み込まれたセキュリティ技術もさることながら、ユーザが能動的にアンチウイルスソフトをインストールしなくても**Windows Defenderが稼働するようになってきていることがマルウェアの感染率を下げている一因**とみられます。
- ともあれ、企業・個人に関わらず、「アンチウイルスソフトを導入する」「OSや各種ソフトウェアを随時最新にアップデートする」よう引き続き意識づけることがセキュリティレベルの向上には必要不可欠です。

ZDNet Japan

「Windows 10」と「7」でマルウェア感染数に大差--ウェブルート調査

Liam Tung (Special to ZDNet.com) 翻訳校正: 佐藤卓 高橋朋子 中村智恵子 吉武悠夫 (ガリレオ) 2018年03月27日 11時30分

「Windows 10」のセキュリティ機能は、「Windows 7」およびそれ以前のバージョンに被害を与えている最新のランサムウェア攻撃から消費者や企業を保護している、Microsoftはたびたび主張している。

実際、セキュリティベンダーのWebrootが、同社のウイルス対策製品を2017年に利用していたWindows 10搭載PCとWindows 7搭載PCを対象に、マルウェアへの感染レベルを調査したところ、Windows 10はWindows 7より「2倍安全」であることがわかったという。

この結論の根拠となっているのは、発見されたマルウェアファイルの数だ。Windows 10搭載PCでは1台あたり平均0.04個だったのに対し、Windows 7搭載PCでは0.08個にのぼった。

総じて、マルウェアと特定されたファイルのうち、Windows 10搭載PCで見つかったファイルは全体の15%だったのに対し、Windows 7で見つかったファイルは全体の63%を占めた。

●Facebook 5000万人分のユーザ情報流出か

<https://www.nikkei.com/article/DGXMZO28345660Q8A320C1000000/>



このニュースをザックリ言うと…

- 3月17日（現地時間）、米New York Timesと英Guardian各紙より、**Facebookユーザ約5000万人の個人情報**が2016年に流出していたと相次いで報じられました。
- 内部告発者の証言によると、ケンブリッジ大学の心理学教授がFacebook上でユーザの性格診断クイズを行うアプリによってユーザ約27万人分の個人情報を収集、さらにそのユーザの友人約5000万人分についても情報収集を行い、データをイギリスの分析会社に渡したとしています。
- Facebookでは、**サイバー攻撃での流出ではなく、またユーザの同意のもとでの情報収集は合法としており**、これを許可なく第三者に渡したことを規約違反としているとともに、報道があった直前にはこの分析会社のアカウントを削除する等の措置をとっています。

AUS便りからの所感等

- ユーザ情報が渡ったイギリスの分析会社は、米トランプ大統領の側近だったスティーブ・バノン氏が創設に関わっていたとされ、**2016年の大統領選でトランプ候補（当時）が有利になるようユーザ情報が使われた可能性**が指摘されています。
- 今回の報道により、Facebookは株価が一時大幅に下落する等の打撃を受けています。
- 全世界にユーザが存在する巨大SNSで、サイバー攻撃でなければ内部の犯行でもない、サービスを利用するユーザによって、その他の多数のユーザが知らない間に被害を受けるという出来事があったことが企業やサービスの個人情報保護・管理にどういった影響を及ぼすかが注目されます。

日本経済新聞

5000万人分の個人情報流出か フェイスブック

トランプ氏ともつながりある英分析会社、データを不正に取得

ネット・IT 北米

2018/3/20 4:57

【ラスベガス=中書紀】米フェイスブックのユーザ約5000万人分の個人情報不正に第三者にわたっていた可能性がでてきた。情報は英データ分析会社を通じて2016年の米大統領選でトランプ陣営に提供されたとの指摘がある。米英議会でフェイスブックの情報管理のあり方をめぐり批判が出ており、巨大デジタル企業への規制論が再び高まっている。

米紙ニューヨーク・タイムズと英紙ガーディアンが19日までに内部告発者の証言を基に報じた。

報道はフェイスブックを通じてユーザー調査した英ケンブリッジ大学の心理学教授が、そこで得た約27万人分の個人的嗜好や行動にまつわるデータを不正に英分析会社ケンブリッジ・アナリティカに渡したというもの。

教授が調査を通じてユーザーデータを取得するのはフェイスブックとの契約に基づき合法だが、それを許可なく第三者に渡すことは禁じられている。データはユーザーの友人情報も含まれており、結果的に約5000万人の情報がケンブリッジ・アナリティカに渡れたとされる。