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。

●「go.jp」でも過信は禁物、政府系ドメインにフィッシングサイトが発覚

https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00598/073100032/
https://www.ncchd.go.jp/news/2019/20190925.html

このニュースをザックリ言うと･･･

- 9月25日(日本時間)、国立成育医療研究センターより、同センターの看護師採用サイトについて、不正アクセスを受けたため停止したと発表されました。

- 当該サイトは同センターのドメイン名「ncchd.go.jp」のもとで開設されていましたが、セキュリティ研究者のpiyokango氏の調査によれば、発表のあった25日の段階でフィッシングサイトらしきコンテンツが表示されるようになっていたとのことで、後日9月30日の時点でもChromeによるアクセス時にGoogleセーフブラウジングによる警告が表示される状態にあったとのことです。

- 同氏は、「政府系機関のみが使えるgo.jpドメイン名を使ったサイトは安全だと思われがち」「悪用されればユーザーはだまされやすい」として、注意を呼び掛けています。

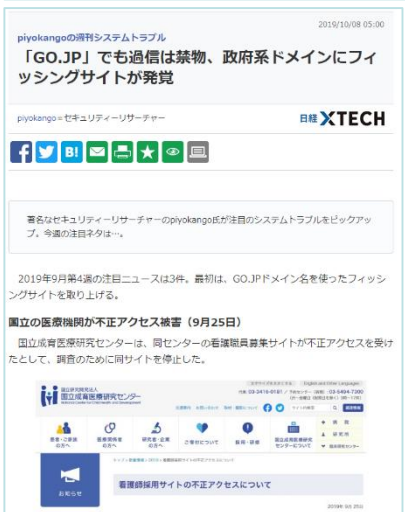
AUS便りからの所感等

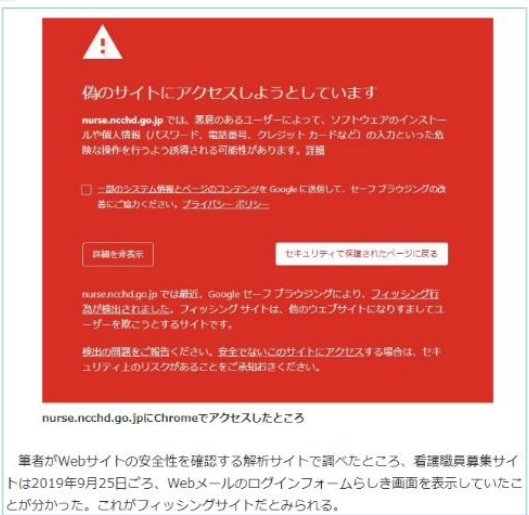
- サイトを改ざんしてフィッシングサイトやマルウェア拡散に悪用するケースは枚挙にいとまがありませんが、特にそのサイトに多くのアクセスがあったり、外部から多くリンクされていたりすると、アクセスしてきたユーザーへの被害は増加し、時にはドメイン名を所有する組織の風評にも影響が及ぶことでしょう。

- 一方でサイトではなくドメイン名自体の方がターゲットとされるケース、例えば政府系組織がgo.jp以外で取得したドメイン名が期限切れとなって第三者に取得されるケース(AUS便り2019/3/18号参照)や、不正なドメイン移管によってドメイン名が乗っ取られるケース(同2019/4/8号参照)も発生しています。

- Webサイトの運用にあたっては、Webサーバー上の各種ソフトウェアを可能な限り最新に保つこと、ドメイン名について適切な管理体制をとること、またコンテンツのアップロード等を行う管理担当者のPCについてもマルウェアが侵入しないようOS等を最新に保ち、かつアンチウイルス・UTM等による防御を固める等、攻撃者に狙われる隙を与えないよう心がけるべきです。

日経 XTECH





nurse.ncchd.go.jpにChromeでアクセスしたところ

筆者がWebサイトの安全性を確認する解析サイトで調べたところ、看護職員募集サイトは2019年9月25日ごろ、Webメールのログインフォームらしき画面を表示していたことが分かった。これがフィッシングサイトだとみられる。

●中継動画を装いクレカ番号詐取…ラグビーワールドカップ便乗詐欺に注意喚起

https://www.fortinet.co.jp/blog/threat-research/free-rugby-world-cup-streaming-foul-play.html

このニュースをザックリ言うと・・・

- 9月30日(現地時間)、セキュリティベンダーの米Fortinet社より、ラグビーワールドカップに便乗した詐欺サイトが確認されたとして、同社ブログで注意喚起が出されています。

- 記事によれば、確認された詐欺サイトはワールドカップの無料ライブストリーミングと宣伝しながら、メールアドレスだけでなくクレジットカード情報の入力も要求するものだったとのことです。

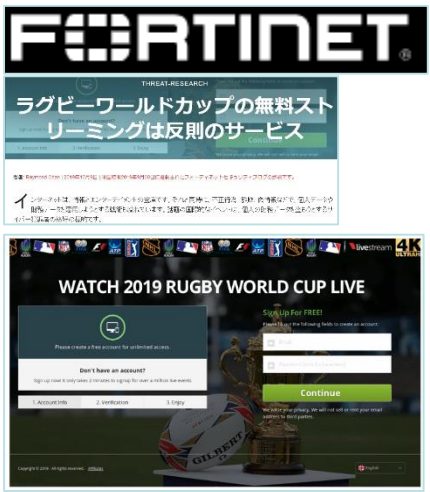
- 同社では、「ラグビーワールドカップの無料ストリーミングサイト」といったキーワードで検索してヒットする1億1,000万ものWebサイトの多くが不審なサイトであり、マルウェアが仕込まれている危険等もあるとして、正規のストリーミングサイトを利用するよう推奨しています。

AUS便りからの所感等

- 記事では複数の詐欺サイトの例が挙げられていますが、共有のテンプレートを用いているものがあることから、同じ犯罪者グループが複数のサイトを立ち上げている可能性があるとしている他、同じグループが動画や電子書籍を無料でダウンロードできると偽る詐欺サイトも運営している模様です。

- 便乗詐欺が発生するのは当然ながらスポーツイベントに限るものではなく、先日は10月の消費税率引き上げに関する手続きを騙り偽のフォームからのログインを要求するケースも確認されています(AUS便り 2019/10/7号参照)。

- 不審なフォームが表示されるだけでなく、最悪アクセスしただけでマルウェアに感染するようWebページに仕掛けられている可能性もありますので、ブラウザーのみならずアンチウイルス・UTMのセキュリティ機能を確実に有効にし、アクセス時の防御を十分に固めることが重要です。



●西京漬専門店の通販サイトに不正アクセス…クレジットカード情報等流出か

https://www.kyoto-np.co.jp/articles/-/29759
http://www.ichinoden.jp/topic/info01/

このニュースをザックリ言うと・・・

- 10月8日(日本時間)、西京漬専門店「京都一の傳(でん)」より、同社通販サイトが不正アクセスを受け、最大91,593人分の個人情報が流出した(あるいはその可能性がある)と発表されました。

- 対象となるのは、2018年3月1日～2019年6月9日に当該サイトで注文を行った注文者および宛先の個人情報(氏名・住所・電話番号等)ないしこれを含むサイト会員情報(メールアドレス・パスワード)最大72,738件と、2018年8月18日～2019年5月17日に決済で使用されたクレジットカード情報(カード番号・氏名・有効期限およびセキュリティコード)18,855件となっています。

- 5月17日に決済代行会社から連絡を受けてカード決済を停止、その後6月9日に流出の原因となる不正プログラムを除去したとしています。

AUS便りからの所感等

- クレジットカード情報流出に至る攻撃のパターンとしては、「SQLインジェクション等の脆弱性を突いてサーバーから情報を抜き取る」ものや「Webアプリケーションを改ざんして決済時のフォームに入力された内容を外部に送信する」「カード情報を入力させる偽ページに誘導する」等が考えられますが、カード情報のうち加盟店での保持が禁止されているセキュリティコード(CVV)等についてサーバー上には保持しない仕様であったとしても、前述の攻撃パターンのうち2番目や3番目が成立した場合、入力されたCVVが流出する可能性があります。

-特に2番目のパターンの場合、アプリケーションが改ざんされたことを利用者側のアンチウイルス等で検知することが困難な場合も考えられるため、サービス提供者側において改ざんを行う攻撃者の侵入を食い止めることがますます重要になりますし、その上で万が一不正プログラムが仕込まれた場合に備え、外部への不審な通信を遮断するよう、UTM等による出口対策をとれればなお良いでしょう。