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。

●ワールドカップを安全に観戦するために…Kaspersky社が注意喚起

https://blog.kaspersky.co.jp/fifa-2018-security/20512/
http://www.security-next.com/094298

このニュースをザックリ言うと・・・

- 6月7日（日本時間）、セキュリティベンダーのKaspersky社より、「2018年サッカーワールドカップを安全に観戦するために」と題した記事が同社ブログ上で公開されています。

- 記事では、「ワールドカップのような大きなイベントには必ずサイバー犯罪者が集まってくる」として、
◆スパムメールから誘導されるショップでグッズを買わない
◆くじ引きや懸賞をうたうスパムメールの大半はフィッシングで、個人情報やゲーム配信サイト等のアカウント情報を詐取される可能性がある
◆試合のライブ中継を観たい場合は必ずFIFA公式パートナーのサイトを利用する
等を挙げています。

AUS便りからの所感等

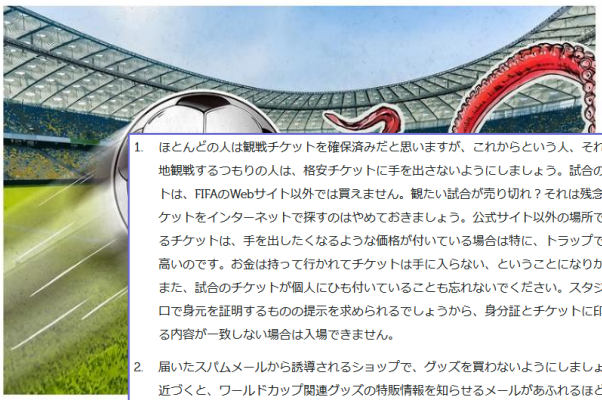
- 記事で挙げられている以外の便乗攻撃としては、「スター選手の名前で検索したユーザを悪意のあるサイトに誘導する」等も考えられ、実際に2014年のワールドカップではそのようなサイトが多く確認された模様です。

- 今後も、例えば2020年の東京オリンピック等で同様の攻撃は行われるとみられます。

- アンチウイルスやUTM等による防御を十分に固めた上で、どういった攻撃が行われ得るか普段から認識しながら行動することが肝要です。

KASPERSKY

2018年サッカーワールドカップを安全に観戦するために



大きなイベントに
ワールドカップも、
や個人情報を手に
りされないように

1. ほとんどの人は観戦チケットを確保済みだと思いますが、これからという人、それも個人で現地観戦するつもりの人は、格安チケットに手を出さないようにしましょう。試合の正規チケットは、FIFAのWebサイト以外では買えません。観たい試合が売り切れ？それは残念ですが、チケットをインターネットで探すのはやめておきましょう。公式サイト以外の場所で売られているチケットは、手を出したくなるような価格が付いている場合は特に、トラップである公算が高いのです。お金は持って行かれてチケットは手に入らない、ということになりかねません。また、試合のチケットが個人にひも付いていることも忘れないでください。スタジアムの入り口で身元を証明するものの提示を求められるでしょうから、身分証とチケットに印刷されている内容が一致しない場合は入場できません。
2. 届いたスパムメールから誘導されるショップで、グッズを買わないようにしましょう。試合が近づくと、ワールドカップ関連グッズの特販情報を知らせるメールがあふれるほど届きます。法外な高値で買わされるなら、まだいい方です。そもそもこのようなショップは実在せず、スパムメールを送ってきた何者かがお金を巻き上げるだけ巻き上げて、闇へと消えてしまうかもしれません。
3. くじ引きや懸賞をうたったスパムメールに、だまされないでください。ワールドカップのスポンサーのふりをしたサイバー犯罪者が、無料の観戦旅行やゲームを餌に詐欺を働く可能性があります。もちろん、中には本物の懸賞もあるでしょう。しかし、このようなメールの大半はフィッシングで、観戦旅行やユニフォームを手に入れるチャンスと引き換えに、個人情報を提供させようとするものです。中にはさらに悪質な、「リンクをクリックして必要なデータを入力すれば、人気のゲーム『FIFA 2018』を無料でダウンロードできる」としてゲーム配信サイトOriginのアカウント用ログインIDとパスワードを盗み取る詐欺もあります。

Security NEXT

「W杯」便乗のサイバー攻撃に注意を - 選手の検索結果に危険が潜む場合も

まもなく4年に1度の「FIFAワールドカップ」が開催される。注目度の高さに便乗するサイバー攻撃が増加する可能性があり、注意が必要だ。

前回の「2014 FIFAワールドカップ」を振り返ると、開催前後の時期にトロイの木馬などの増加がセキュリティベンダーによって観測されている。

ひとつはメールを使った攻撃。サッカーファンが興味をそそるファイル名を付けたバックドア
ケースが発生して

また個人情報やク
意が必要だ。出場
ケースがあったほ
取る詐欺も確認さ

（Security NEXT

「W杯」便乗のサイバー攻撃に注意を - 選手の検索結果に危険が潜む場合も

気になる選手の名前を検索エンジンで検索する場合も気を抜けない。検索結果から悪意あるサイトへ誘導されるケースもあるためだ。

前回のワールドカップにおいて、もっとも検索結果が危険だとされたクリスティアーノロナウド選手の場合、検索結果の3.8%が、マルウェアやスパム、フィッシングなどの危険が潜むサイトだった。

またリオネルメッシ選手は3.7%、日本人選手で最もリスクが高かった香川真司選手は、検索結果の1.6%が危険なサイトだったという。スクリーンセーバーのダウンロードや、動画配信を装っているケースも多く、「無料ダウンロード」といった文言で誘導することも多い。

またサッカーゲームのライセンスコードを作成できるなどとだますアドウェア「ADW_INSTALLREX」も、検索エンジン上で拡散が確認されている。

前ページ

（Security NEXT - 2018/06/11 ）

●IPA、セキュアなウェブサイトの開設と運営に向け、小規模事業者を対象とした「手引き」を公開

https://enterprisezine.jp/article/detail/10795

このニュースをザックリ言うと・・・

- 5月30日（日本時間）、情報処理推進機構（IPA）より、主に小規模事業者を対象とした「ウェブサイト開設等における運営形態の選定方法に関する手引き」が公開されました。

- ウェブサイトの新規開設および刷新において、クラウドサービスなどの運用形態別にメリット・デメリット、およびセキュリティ対策に必要な確認項目を整理したものとなっています。

AUS便りからの所感等

- IPAでは2004年からソフトウェアの脆弱性関連情報の届出を受け付けていますが、脆弱性が存在するとの届け出を受けて修正を依頼しても完全に修正されないサイトが全体の約5%程度存在しているとし、これらのサイトが小規模組織によって運営され、対策のための体制やコスト等の関係で問題修正やサイトの廃棄ができないために、「攻撃を受けてしまうウェブサイトの放置」に繋がっているとしていることから、今回の手引きを作成・公開したとしています。

- もし例えば「クラウドでサイトを構築するのは危険、自社ネットワーク上(オンプレミス)でサイトを構築する方が安全」という認識を今も持っているのであれば、それは一概に正しいとは言えず、また「クラウド」が意味するものも広義にはレンタルサーバ・VPSからASP等に至るまで様々で、得手不得手や注意すべきポイントがそれぞれに存在することを意識し、この手引きを必要なセキュリティ対策等を適宜実行するための参考として頂ければ幸いです。


EnterpriseZine
データテクノロジー・情報セキュリティIT リーダー向け専門メディア

IPA、セキュアなウェブサイトの開設と運営に向け、小規模事業者を対象とした「手引き」を公開

セキュリティ　Webセキュリティ

10　3　G+0　B! 4　7　プッシュ通知

EnterpriseZine編集部[著]　2018/05/30 15:30

セキュリティ対策項目				運用形態			
区分	分類		代表的対策例	モール ASP SaaS	PaaS レンタルサーバ IaaS	データセンター	オンプレミス
システムセキュリティ対策	技術的対策	物理	・サーバ室 ・入退管理				○
		ネットワーク	・FW ・IDS/IPS ・WAF・VPN ・ウイルス対策製品 ・サンドボックス製製品 ・DDoS対策		△	△	○
		アプリケーション	・改ざん検知 ・認証 ・アクセス制御 ・データ保護		○	○	○
	運用管理的対策	セキュリティパッチ	・パッチ適用 ・仮想パッチ適用		△（アプリ）	○	○
		監視	・ログ収集、分析		△	○	○
		インデント対応	・バックアップ ・切り分け ・抜線		△	○	○
	人的対策	要員教育	・ポリシー教育 ・技術教育		△	○	○
業務セキュリティ対策	社員教育		・リテラシー教育	○	○	○	○
	ユーザ・顧客管理		・ポリシー教育 ・情報取扱い規則	○	○	○	○
	コンテンツ管理		・コンテンツ更新ルール	○	○	○	○

サイト運営者対応　○：対応の検討が必要　△：一部対応の検討が必要

運営形態ごとに検討すべきセキュリティ対策（「手引き」22ページより）

●生徒の個人情報入りUSBメモリ紛失、大阪で相次いで発生

https://www.mbs.jp/news/kansainews/20180612/GE000000000000023040.shtml

このニュースをザックリ言うと・・・

- 大阪の高校・大学で生徒の個人情報入りUSBメモリの紛失が相次いで発覚しています。

- 6月11日（日本時間、以下同様）、大阪府立泉大津高校の英語教師が同校および以前勤務していた別高校の生徒計153人分の個人情報が入ったUSBメモリを4月に紛失していたことが発表されましたが、同1日に当該個人情報を印刷した用紙が府教育庁に匿名で送られたことで発覚したとのことです。

- 6月12日には、関西大学・大阪電気通信大学・大阪産業大学等で外国語科目を担当している非常勤講師が学生計677人分の個人情報、あるいは成績情報が保存されていたUSBメモリを紛失したと発表されています。

AUS便りからの所感等

- USBメモリについては個人情報が保存された状態での紛失事件が度々発生している他、不審なメモリの挿入によるマルウェア感染の可能性等のデメリットを問題視する声が強まっており、IBMが社内での使用を全面的に禁止する方針を発表する等の状況となっています（AUS便り 2018/05/21号参照）。

- 代替手段としてオンラインストレージの利用を推奨する意見も有力となっていますが、それぞれのメリット・デメリットを十分に把握した上で利用や乗り換えの検討を行うこと、またアンチウイルスによる防御、あるいは暗号化によるデータの保護等、それぞれ安全な利用にあたって行うべき対策を確実にとることが重要と言えます。


MBS NEWS

個人情報保存のＵＳＢメモリーを非常勤講師が紛失　大阪産業大学

更新：2018/06/12 19:20

いいね！1　ツイート

MBS

大阪産業大学

NEWS CHECK

史上初の米朝会談 非核化に取り組む

岩の裂け目から… ガッツ石「松」

たばこに水銀注入「完全犯罪を計画」

個人情報USB 大産大講師が紛失

同居女性が死亡「暗闇になり殴った」

大阪産業大学は、学生１０６人分の名前や成績情報などが保存されたＵＳＢメモリーを紛失したと発表しました。

中国語を担当する非常勤講師の男性（５３）が今月５日、授業を終えた後ＵＳＢメモリーをズボンのポケットに入れ別の大学に向かいましたが、その途中で紛失したということです。ＵＳＢメモリーには、大阪産業大学のほかにもこの男性が非常勤講師を務める関西大学、大阪電気通信大学、神戸市外国語大学の学生合わせて６７７人分の個人情報が記録されていました。