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。

●人気アニメ公式サイト、ドメインの不正移管で一時乗っ取られる

https://www.itmedia.co.jp/news/articles/1904/05/news051.html
https://www.itmedia.co.jp/news/articles/1904/05/news109.html
https://www.itmedia.co.jp/news/articles/1904/05/news110.html

このニュースをザックリ言うと･･･

- 4月5日（日本時間）未明から午後3時すぎにかけて、人気アニメ「ラブライブ！」シリーズの公式サイトにおいて、一時的に不正な内容が表示される状態になっていました。

- 公式サイトのドメインは元々アニメ制作会社サンライズ名義の所有となっていましたが、5日午前1時18分に情報が更新され、第三者名義に移管されていたとされています。

- 偽サイトに掲載されたメッセージでは、不正移管を行った手口として「移管オファーを行い元所有者が移管オファーを承認しただけだった」としています。

- 同日午後3時38分には当該ドメインの所有者は元のサンライズ名義に戻っていますが、サイトは「安全確認中」のため現在非公開状態となっています。

AUS便りからの所感等

- Webサーバ上のデータの改ざんではなく、ドメイン名を乗っ取る形で偽サイトへ誘導しようとするケースについては、今年1月に米国のいくつかの組織やJPドメインを管理するJPRS社等から注意喚起が出されていました（AUS便り 2019/02/04号参照）。

- 一方でJPドメインでは、移管を行わせないようにする「レジストリロック」はなく、かつ移管申請から10日以内に申請を拒否しなかった場合に自動的に移管が承認されるルールになっていたことが不正移管が成立した一因とみられます。

- JPドメインを管理する業者によっては独自にレジストリロックを設定する等の対応を行っているところもありますので、ドメイン移管や情報の変更に関するメールを管理者が確実に受け取り、攻撃者による不正な移管申請を食い止められるよう、契約している管理業者が提供する機能と設定状況を随時確認しておくことが必要です。


ITmedia NEWS

「ラブライブは我々が頂いた！」　人気アニメの公式サイト乗っ取りか　公式「原因究明中」　ドメイン移管された？

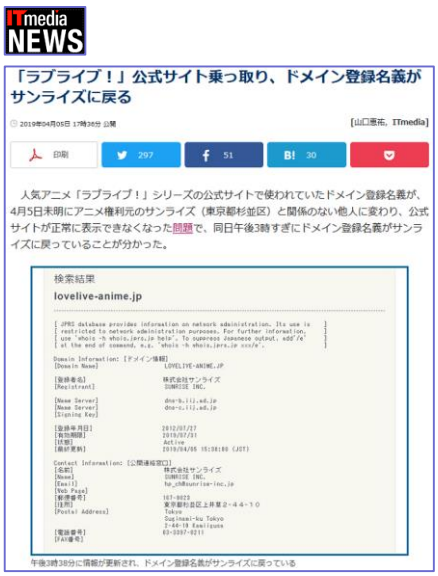
2019年04月05日 04時00分 公開　[山口恵祐, ITmedia]

印刷　15110　654　B!　445

人気アニメ「ラブライブ！」シリーズの公式サイトが、4月5日未明から正常に表示できない状態になっている。ページを開くと「ラブライブは我々が頂いた！」といったテキストが表示され、別アニメ作品の公式サイトに移動するように仕掛けられている。ラブライブ！の運営チームは「現在原因究明中」としている。

ページを開くと表示されるテキスト

同日の午前2時ごろから、「ラブライブのページが開けない」「表示がおかしい」「ページが乗っ取られた？」といった報告がネット上で相次いだ。実際にページを開くと、本来表示されるアニメ紹介ではなく、以下のテキストが表示される。


ITmedia NEWS

「ラブライブ！」公式サイト乗っ取り、ドメイン登録名義がサンライズに戻る

2019年04月05日 17時36分 公開　[山口恵祐, ITmedia]

印刷　297　51　B!　30

人気アニメ「ラブライブ！」シリーズの公式サイトで使われていたドメイン登録名義が、4月5日未明にアニメ権利元のサンライズ（東京都杉並区）と関係のない他人に変わり、公式サイトが正常に表示できなくなった問題で、同日午後3時すぎにドメイン登録名義がサンライズに戻っていることが分かった。

午後3時38分に情報が更新され、ドメイン登録名義がサンライズに戻っている


ITmedia NEWS

ラブライブ！公式サイト乗っ取りに使われた「ドメイン移管」の仕組みとは　“10連休”に危険潜む？

2019年04月05日 17時39分 公開　[井上輝一, ITmedia]

印刷　1163　403　B!　314

4月5日未明に、人気アニメ「ラブライブ！」シリーズの公式サイトが何者かに乗っ取られた。同サイトのURLからページを開くと、「我々の方法は、移管オファーを行い元所有者が移管オファーを承認しただけだった」という文言が確認できた（5日午後3時時点でページは開けなくなっている）。

乗っ取りの犯人の言葉を信じれば、犯人は「ドメイン移管」の手順を踏んで、ラブライブ！版権元のサンライズから同サイトのドメインを得たと考えられる。

ドメイン移管とは何か。関係各社に取材したところ、今回の手法に加え、新たな危険も見えてきた。

何者かに乗っ取られたラブライブ！シリーズ公式サイト

汎用JPドメインの扱い　10日以内に返事しないと……

●元号発表に便乗、ドコモ名乗る「なりすましメール」注意

https://www.asahi.com/articles/ASM413134M41UTFL001.html

このニュースをザックリ言うと・・・

- 4月1日（日本時間）、NTTドコモより、同日未明から同社をかた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「ご利用中のお客様へ大切なお知らせです。」や「新元号に伴い料金改正のお知らせ」で、本文が「5月1日に新元号が発表されdocomoは生まれ変わります。それに伴い新プランへの移行となりますので…」という内容になっており、「オフィシャルページ」と記載されたリンクから偽のサイトにアクセスする模様です。

- 同社ではこのようなメールは配信しておらず、メール中のリンクをクリックしないよう呼び掛けています。


朝日新聞 DIGITAL

元号発表に便乗　ドコモ名乗る「なりすましメール」注意

令和

2019年4月1日10時45分

シェア　ツイート　ブックマーク　メール　印刷

ドコモをかたって送りつけられたメール（画像の一部を加工しています）

1日の 新元号 発表に乗じて同日未明、ＮＴＴドコモ をかたった「なりすましメール」が携帯メールに送りつけられている。ドコモは「そのようなメールは送っていない」と注意を促している。

【特集】どうなる新元号

【速報中】新元号、きょうの動きをタイムラインで

なりすましメールは、 新元号 発表に合わせて新しい契約プランに移行するとの内容で、契約中のプランがどのように変更されるかを確かめるよう求め、リンク先にアクセスさせようとしている。 新元号 の発表日を「５月１日」とする誤りもあった。

ドコモの担当者は「新年度などの節目でなりすましメールは増える。心当たりのないメールは本文に書かれたリンク先にアクセスしないでほしい」と話した。

AUS便りからの所感等

- NTTドコモの注意喚起ページでは、これまでに出回った同社をかたるメールの例が多く取り上げられており、特に同社スマートフォン等を利用しているユーザは一度このページの内容をチェックし、またこのようなメールが届いた場合にも備えてブックマークする等を推奨致します。

- 新元号発表のような大きなイベントには、それに便乗しての詐欺行為等が必ずついて回るものと認識し、不審なメールが届いた場合は、件名や文面の一部で検索し、同様のメールを受け取ったという報告がないかチェックする習慣を是非ともつけて頂ければ幸いです。

●「10連休」ゴールデンウィークにおける情報セキュリティ注意喚起、IPA例年より早く発表

https://www.ipa.go.jp/security/topics/alert20190402.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となるゴールデンウィークを迎えるにあたり、4月2日（日本時間）にIPAより、情報セキュリティに関する注意喚起が出されています。

- 夏季や年末年始そして今回のようなGWといった長期休暇の前に、組織内に常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象にした基本的な対策と心得をまとめています。

- 今年は5月1日の改元に関連して、通常よりも長い「10連休」等となるケースが多いことや、改元に便乗した新たな手口が発生する可能性があることから、IPAでは例年より早い注意喚起を行ったとしています。

AUS便りからの所感等

- 4月5日時点で、上記ページのリンク「長期休暇における情報セキュリティ対策」の内容は昨年12月時点のものとなっていますが、「システム管理者」は休暇前の緊急連絡体制の確認や休暇明けのサーバ等ログのチェック、「組織の利用者」は休暇中の機器・データの持ち出しについてのルール確認と厳重な管理、「家庭の利用者」は休暇中のSNSへの投稿内容に注意する等、書かれている内容は基本的に毎回大きく変わるものではありません。

- 万一GWまでに十分な対応が間に合わなかったとしても、GW明け以降に点検すべきことは多く存在しますし、以後も夏季休暇等に備えて、準備・点検を行うよう意識していくことが肝要です。


IPA Better Life with IT 情報処理推進機構

ゴールデンウィークにおける情報セキュリティに関する注意喚起

最終更新日：2019年4月2日
独立行政法人 情報処理推進機構
セキュリティセンター

ゴールデンウィークまで1ヶ月を切りました。今年は5月1日に平成から令和に改元されることに伴い、10日間の超大型連休が控えています。その前後には、改元に便乗した新たな手口が発生することが懸念されます。そこで、例年より早く「ゴールデンウィークにおける情報セキュリティに関する注意喚起」を行います。

長期休暇中は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもと異なる状況になります。例えばウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込みから思わぬ被害が発生したり、場合によっては関係者にも被害が及ぶ可能性があります。

そのほか、改元に便乗した新たな手口が発生する可能性もあります。メールやショートメッセージ（SMS）、SNSでの不審なファイルやURLには、より一層の注意が必要です。基本的な心得、対策を（1）組織のシステム管理者、（2）組織の利用者、（3）家庭の利用者、それぞれの対象者別にまとめています。今年は10日間の超大型連休となるため、早めの準備をお勧めします。

■長期休暇における情報セキュリティ対策

また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

■日常的に実施すべき情報セキュリティ対策

被害に遭わないためにもこれらの対策の実施をお願いします。