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。

●えきねっとの偽サイト、Google検索のトップに一時表示される

https://www.sankei.com/article/20221019-JW6B4XO2PBOQLLBNJSWKAHCXIU/
https://togetter.com/li/1960772

このニュースをザックリ言うと･･･

- 10月18日(日本時間)から19日にかけて、JR東日本の予約サイト「えきねっと」の偽サイトがGoogle検索の上位に表示されるとして、Twitter上などで話題となっていました。
- 本物のえきねっとのURLが「www.eki-net.com」なのに対し、末尾が「.ru」「.pro」の偽サイトへのリンクが広告として表示されていたもので、偽サイトはJR東日本の新チケット「どこかにビューーン！」のキャンペーンサイトを模倣し、えきねっとやJRE-POINTの会員情報等を詐取しようとするフィッシングサイトとなっていました。
- 10月25日時点で前述の広告や偽サイトは表示されなくなっています。

AUS便りからの所感等

- えきねっとを騙るフィッシングメールは過去にもフィッシング対策協議会などで注意喚起が出ていましたが、前述の偽サイトが現れていた時期からまた大量に確認されるようになっています。
- JR東日本では以前からフィッシングに対し「URLを確認してほしい」あるいは「メールのリンクではなく、公式アプリやブラウザのブックマークから正規のサイトにアクセスしてほしい」と注意喚起しているとのことで、普段利用しているサービスについては特に後者の対策をもって効果的なフィッシングの回避を行いましょう。
- Googleの検索結果では、他にも有名なソフトウェアの名前を検索した場合にも非公式のダウンロードサイトが上位に現れることもあり、場合によってはマルウェアを掴まされる恐れもありますので、Webブラウザーやアンチウイルス・UTM等による不審なサイトへのアクセス時に警告を出す機能を有効にするとともに、上位に表示されているサイトが目当てのものか、他の検索結果のページも参照する等して精査することも心掛けるに越したことはありません。
- 一方で、模倣の被害を受けた本物のキャンペーンサイトも、本来のえきねっとのURLとは異なる独自のドメイン名を使用しており、そういったドメイン名の使い分けも「これもフィッシングなのではないか？」という疑いの種や、ドメイン名の失効後に第三者が取得するリスクがあることには注意すべきでしょう。

THE SANKEI NEWS 産経新聞

グーグルで「えきねっと」検索→偽サイトへ　ＪＲ東が削除依頼

2022/10/19 16:02
社会 | 事件・疑惑　エンタメ　経済 | 産業・ビジネス　IT

グーグルで「えきねっと」と検索。偽のサイトが検索結果の最上位に表示されたスマートフォンの画面

ＪＲ東日本のインターネット予約サービス「えきねっと」とそっくりの偽サイトが一時的に、グーグルの検索結果の最上位に表示されていたことが１９日、同社への取材で分かった。偽のサイトに誘導し、個人情報を盗みとるフィッシング詐欺とみられ、同社が注意を呼び掛けている。

ＪＲ東によると、偽のサイトはインターネット上の住所に当たる国別の「ドメイン」が、ロシアのサイトであることを示す「．ｒｕ」となっている。正規のサイトは「．ｃｏｍ」のため、同社は「ＵＲＬを確認したうえでアクセスしてほしい」としている。

１９日朝の時点で、検索結果の最上位に表示されるケースも確認され、その後も正規の「えきねっと」のサイトよりも上位に表示されていた。偽のサイトは、検索された語句（キーワード）やコンテンツに関連した広告が表示される「リスティング広告」と呼ばれるサービスを利用しているとみられる。ＪＲ東は産経新聞の取材に「グーグルに検索結果の削除依頼を実施している」と説明した。

●沖縄県の図書館がランサムウェアの被害、業務に一時支障も

https://ryukyushimpo.jp/news/entry-1599931.html
https://www.city.naha.okinawa.jp/lib/n-information/20221013.html

このニュースをザックリ言うと・・・

- 10月14日(日本時間)、沖縄県那覇市より、同市の8つの図書館でシステムがランサムウェアの攻撃を受け、図書貸出を停止していると発表されました。

- 感染は同13日朝に確認され、利用者情報(約19万人分)および蔵書等のデータが暗号化されアクセスできない状態になったとのことです。

- 利用者情報のうち、個人情報部分についてはシステム側で既に暗号化しており、流出の可能性は少ないとしている一方、長期返却延滞者約500人分の情報は暗号化されておらず、流出の有無は不明としています。

AUS便りからの所感

- 10月25日時点でシステム復旧の発表はなく、同22日以降、手作業による貸出業務の再開を行っている模様です。

- 公共機関でのランサムウェア被害は、昨年10月と今年6月に徳島県のそれぞれ別の病院で発生し、前者は数ヶ月間業務に支障が出る事態となっています(AUS便り 2022/06/21号)。

- この時に発表された報告書、あるいは6月の事例ではオフラインバックアップから早々に復旧がなされたという事実をもとにして、ランサムウェアを含むマルウェアや各種攻撃に対しアンチウイルスやUTM等による防御のみならず、適切なバックアップと確実な復旧が行えるシステム体制の整備を行うことが肝要です。

琉球新報

那覇市立の8図書館、ウイルス攻撃でシステム障害　貸し出し停止、復旧の見通し立たず

2022年10月14日 21:05

図書館でのシステム障害について説明する那覇市教委の小嶺理生涯学習部長（右）と島袋元治中央図書館長＝14日、那覇市役所

那覇市教育委員会は14日、会見を開き、第三者がデータを暗号化して身代金を要求するウイルス（ランサムウェア）の攻撃に伴うシステム障害で、市立図書館8館で本の貸し出しを停止していると発表した。ウイルスの侵入経路は不明で、復旧の見通しは立っていない。

>>より詳しく 【身代金要求「応じない」那覇市の図書館がランサム被害、19万人分のアクセスが不能に>

那覇市によると、ウイルスへの感染は13日朝、職員が図書館システムを起動できないことに気づいたことで発覚した。外部から暗号化されたのは利用者情報や蔵書などのデータで、図書館側がアクセスできない状態になっている。利用者情報（約19万人分）は氏名のほか、住所や連絡先などを含んでいるが図書館側で既に暗号化していたため、流出の可能性は少ないとい

●リモートアクセスへの攻撃でよく狙われるユーザー名とパスワード…Rapid7が注意喚起

https://thinkit.co.jp/news/bn/19940
https://www.rapid7.com/blog/post/2022/10/20/new-research-were-still-terrible-at-passwords-making-it-easy-for-attackers/

このニュースをザックリ言うと・・・

- 10月20日(現地時間)、セキュリティベンダーのRapid7社より、特に企業ネットワークへの不正ログイン試行時において頻繁に使用されるユーザー名とパスワードに関する調査結果が発表されました。

- クラウド上の仮想マシンを管理するために用いられるプロトコルとしてRDP(リモートデスクトップ)とSSHを取り上げており、同社が仕掛けたハニーポット上のRDP・SSHで使用されたユーザー名・パスワードを分析したものとのことです。

- RDPに対し最も頻繁に試行されたユーザー名は「administrator」「user」「admin」、SSHについては「root」「admin」「nproc」とされており、同様に最も多く試行されたパスワードは「admin」「password」「123456」だったとのことです。

- また、ハニーポットに対して施行された50万件のパスワードが、2009年にソーシャルゲームサイト「RockYou」から流出した情報を元に作成された攻撃用のID・パスワードリストとほぼ一致したことから、攻撃者は全くランダムなパスワードではなく、既存のパスワードリストを使用していると同社では結論づけています。

AUS便りからの所感

- RDPはWindows上で、SSHはLinux上で主に使用されるプロトコルであることから、ユーザー名の上位も各OSで管理者アカウントに使われるもの(WindowsのAdministrator、Linuxのroot)が出ています。

- 不正ログインの試行では、パスワードに使われやすい単語の大規模なリストを用いる「辞書攻撃」や、IDとパスワードが同一な「JOEアカウント」を狙う等は昔から行われてきた古典的なものであり、アカウントにパスワードを設定するにあたってはこうした攻撃のセオリーを避け、同社も推奨するようにデフォルトで設定されているパスワードから変更し、推測されにくいパスワードを設定するのが重要です。

- またSSHについては、公開鍵ベースでの認証を用いるようにし、パスワードでの認証を無効にすること、SSHでログインするユーザーを制限する(root等は直接SSHでログインできないようにする)こと等が推奨されており、一方RDPにはSSHのような鍵ベースの認証はないものの、近年Windowsサーバーでも SSHサービスが利用できるようになっており、RDPポート(TCP/UDP 3389番)に外部から直接アクセス可能な状態から、SSHによるトンネリングとの組合せを必要とし、より安全性を高める設定とする等も考慮に値するでしょう。

シンクイット ThinkIT

Rapid7、RDPおよびSSHにおいてセキュリティが懸念される調査結果に対して注意喚起を発表

© 2022年10月23日(日)

Rapid7は10月20日、RDPおよびSSHにおいて頻繁に利用されるアカウント名およびパスワードに、セキュリティが懸念される調査結果が得られたとして注意喚起を発表した。

RDP(Remote Desktop Protocol)とSSHは、いずれもクラウドの仮想マシンを操作するために頻繁で利用されているプロトコル。Rapid7の調査では、

○RDPで最多く使われているユーザ名の上位3つは、「administrator」「user」「admin」
○SSHで最多く使われているユーザ名の上位3つは、「root」「admin」「nproc」
○SSHとRDPで最多く使われているパスワードの上位3つは、「admin」「password」「123456」

という結果となった。