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。

●リスト型攻撃か、マルウェアか…パスワード管理サービス「LastPass」から不正ログイン試行のアラート

https://gigazine.net/news/20211229-lastpass-master-password-compromised/
https://blog.lastpass.com/2021/12/unusual-attempted-login-activity-how-lastpass-protects-you/

このニュースをザックリ言うと・・・

- 12月28日(米国時間)頃、複数のIT系ネットメディアにおいて、パスワード管理サービス「LastPass」の複数のユーザーが「(LastPass自体にログインするための)マスターパスワードが侵害された」との警告を受けたことが取り上げられています。

- 例えば、LastPassユーザーの一人で、音声広告を提供する企業のCTOであるGreg氏は、(自分が住んでいない)ブラジルから、実際に設定されているマスターパスワードによるログイン試行をブロックしたというアラートメールを受け取ったことを報告しており、(パスワードを暗号化してローカルPCにのみ保存する)KeePass上にのみ保存されていたはずのマスターパスワードが第三者に把握されている可能性があるとしています。

- IT系メディアの一つ「AppleInsider」がサービス運営元のLastPass社に問合せを行ったところ、他のサービスから流出したメールアドレス・パスワードによる、いわゆる「リスト型攻撃」によるログイン試行をブロックしたとの回答を得たとしており、またLastPass社のブログでも不正ログイン試行があったことについて取り上げられていますが、実際にアカウントへのログイン成立に至った例はなかったことが報告されています。

AUS便りからの所感等

- 別のLastPassユーザーからは「マスターパスワードを変更したにも拘らず、直後に変更後のマスターパスワードによるログイン試行を受けた」との報告がある一方、あるセキュリティ研究者は、感染したPC上でパスワードの奪取を行うマルウェア「RedLine Stealer」に関するログにLastPassに関するものがあったとして、マルウェアが関与した可能性を示唆しています。

- 別のIT系メディア「BleepingComputer」では、今回アラートメールを受けたユーザーのメールアドレスはRedLineのログには見当たらなかったとしているものの、LastPassのサーバーにマスターパスワードそのものは送信されない仕様となっていること等から、RedLineあるいはそれ以外のマルウェアがPC上のキー入力を読み取ってマスターパスワードを奪取したものと推測されます。

- LastPass以外にも、その競合として注目されるBitWarden等や、前述したKeePassのようなリモートにデータが保存されない形のパスワード管理ツール・サービスが多く存在しており、またLastPassを使い続ける場合でも、同サービスが提供する二段階認証を有効にする等、安全な設定を確実に行うことにより、攻撃者の侵害を未然に防止できるケースはあると思われます。

- ただし、マルウェアに感染している場合、最悪PCから送信されるあらゆるサービスのパスワードを奪取される恐れもあるため、アンチウイルスやUTM等により、PC(ないしモバイル)にマルウェアが侵入しないよう万全の防御策をとることが肝要です。


GIGAZINE

2021年12月29日 10時57分　セキュリティ

パスワードマネージャー「LastPass」で本人しか知らないマスターパスワードを使って他人がアクセスしようとする事態が複数発生

パスワードや個人情報を管理するパスワードジェネレーターの「LastPass」で、複数のユーザーが「マスターパスワードが侵害された」と警告するメッセージを受け取っていると報告しています。

Ask HN: How did my LastPass master password get leaked? | Hacker News
https://news.ycombinator.com/item?id=29705957

LastPass master passwords may have been compromised | AppleInsider
https://appleinsider.com/articles/21/12/28/lastpass-master-passwords-may-have-been-compromised

LastPass users warned their master passwords are compromised
https://www.bleepingcomputer.com/news/security/lastpass-users-warned-their-master-passwords-are-compromised/

音声広告を提供するdecibelの最高技術責任者であるGreg Technology氏は、ある日LastPassから「ブラジルからのログイン試行をブロックしました」というアラートメールを受け取ったそうです。

Login attempt blocked

Hello,

Someone just used your master password to try to log in to your account from a device or location we didn't recognize. LastPass blocked this attempt, but you should take a closer look.

Was this you?

Account [redacted]

Time Tuesday, December 28, 2021 at 12:25 AM EST

● JNSA「セキュリティ十大ニュース」発表、ランサムウェア等事件が関係する話題が独占

https://www.jnsa.org/active/news10/index.html
https://www.mcafee.com/enterprise/ja-jp/about/newsroom/press-releases/press-release.html?news_id=2021121401

このニュースをザックリ言うと・・・

- 12月24日(日本時間)、日本ネットワークセキュリティ協会(JNSA)より、「2021セキュリティ十大ニュース」が発表されました。

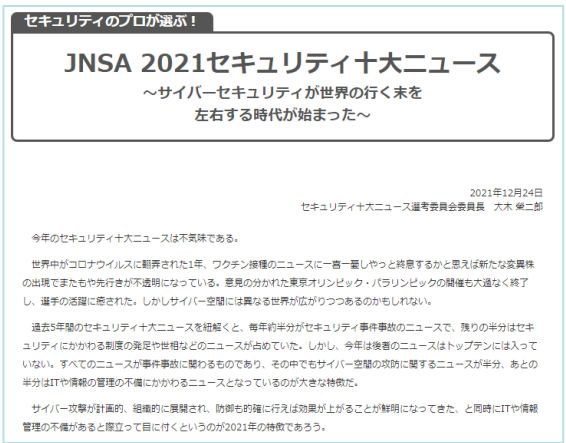
- 1位「ランサムウェアの被害広範囲に、影響は一般市民にも」、2位「LINEデータ管理の不備が指摘される」、3位「EMOTETテイクダウンの朗報、しかし再燃の動きも」、以下10位まで全てセキュリティインシデントに関連するトピックがランクインしています。

- 一方で、これまで半数がランクインしていた「セキュリティにかかわる制度の発足や世相などのニュース」が今回は入っていないことも取り上げられています。

AUS便りからの所感

- 発表においては、「サイバー攻撃が計画的、組織的に展開され」る傾向が見える一方で「防御も的確に行えば効果が上がることが鮮明になってきた」とし、逆に「ITや情報管理の不備があると際立って目に付く」ことが2021年の特徴であろう、とされています。

- 12月14日に大手セキュリティベンダーのマカフィー社も「2021年の10大セキュリティ事件ランキング」を発表する等、年末年始にこのような振り返りが行われるのはどの分野でも定番ですが、両ランキングの顔ぶれや順位は互いに異なっており、視点や取り上げる範囲等の違いによる差異を踏まえながら複数の記事を参照することにより、情報セキュリティに関するトレンドを幅広くキャッチアップすることが大切でしょう。


セキュリティのプロが選ぶ！

JNSA 2021セキュリティ十大ニュース

～サイバーセキュリティが世界の行く末を左右する時代が始まった～

2021年12月24日
セキュリティ十大ニュース選考委員会委員長　大木 栄二郎

今年のセキュリティ十大ニュースは不気味である。

世界中がコロナウイルスに翻弄された1年、ワクチン接種のニュースに一喜一憂しやっと終息するかと思えば新たな変異株の出現でまたもや先行きが不透明になっている。意見の分かれた東京オリンピック・パラリンピックの開催も大過なく終了し、選手の活躍に感された。しかしサイバー空間には異なる世界が広がりつつあるのかもしれない。

過去5年間のセキュリティ十大ニュースを俯瞰すると、毎年約半分がセキュリティ事件事故のニュースで、残りの半分はセキュリティにかかわる制度の発足や世相などのニュースが占めていた。しかし、今年は後者のニュースはトップテンには入っていない。すべてのニュースが事件事故に関わるものであり、その中でもサイバー空間の攻防に関するニュースが半分、あとの半分はITや情報の管理の不備にかかわるニュースとなっているのが大きな特徴だ。

サイバー攻撃が計画的、組織的に展開され、防御も的確に行えば効果が上がることが鮮明になってきた、と同時にITや情報管理の不備があると際立って目に付くというのが2021年の特徴であろう。

● ECサイトを騙る詐欺サイトの見分け方、ecbeing社が解説

https://www.itmedia.co.jp/news/articles/2112/17/news163.html

このニュースをザックリ言うと・・・

- 12月16日(日本時間)、ECサイト制作などの事業を手掛けるecbeing社より、本物のECサイトと同様の見た目で個人情報や金銭の詐取を行う「詐欺サイト」を見分け、回避するポイントについて、同社セミナーで発表されました。

- 消費者庁発表の「令和3年版 消費者白書」によれば、ネット通販での商品未着・連絡不能等に関する相談件数は2018年の32,402件、2019年の41,786件から、2020年は71,515件に急増しているとのことです。

- ecbeing社の発表では、詐欺サイトにおいて気を付けるべきポイントとして「商品の価格が不自然に安い」「日本語表記が不自然」「『特定商取引法に基づく表記』や利用規約等が掲載されていない」を挙げており、他にも「問合せ先が企業ドメイン名ではなくフリーメールアドレス」「振込先が個人名義」「銀行振込しか取り扱っていない」等も注意点としています。

- また、サーチエンジンでは詐欺サイトを上位に表示しないような対策がされていることから、Instagram等のSNSで広告を出して流入を狙う事例が増えているとしています。

AUS便りからの所感

- 発表では他にも、詐欺サイトに記載される情報として、他のECサイトや企業サイトから内容をコピーしたものや、商品レビューを投稿者の名前だけ変更したもの等が掲載されること、また利用規約を社名を変えずにコピーされるケースもあること等が挙げられています。

- 狙われているソフトウェアの脆弱性や、拡散しているマルウェアの種類あるいはフィッシングメールの内容等といった、様々なサイバー攻撃の手口と同様、犯罪者が如何にして利用者から詐欺を行うかという情報を随時調査し、ネットの利用において慎重な行動をとり続けること、そしてそれだけに依存せず、Webブラウザーや UTM等のアンチフィッシング機能による防御も併せて行うことを強く推奨致します。


偽ECサイトで金銭をだまし取る「詐欺サイト」　その実情と見分け方

2021年12月17日 19時16分 公開　[松浦立樹，ITmedia]

印刷　96　Share　B!　3　0

あたかも本物のようなECサイトの見た目で、ユーザーの個人情報抜き取りや金銭窃取などを狙う「詐欺サイト」。消費者庁が発表した「令和3年版 消費者白書」によると、ネット通販での商品未着や連絡不能などに関するトラブルが2020年に急増したという。

図表I-1-4-3　商品未着・連絡不能等に関する消費生活相談件数の推移

(件)
80,000
70,000
食料品　保健衛生品　被服品
教養娯楽品　住居品　その他
71,515
4,422