— AUS（アルテミス・ユーザ・サポート）便り 2019/02/18号 —
https://www.artemis-jp.com

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。

●誤ったパスワードの入力で他人のIDをロックさせる「攻撃」がアイドルファンクラブサイトで発生

https://internet.watch.impress.co.jp/docs/yajiuma/1168355.html
https://togetter.com/li/1316142

このニュースをザックリ言うと・・・

- 2月4日（日本時間）頃、Twitter上で、アイドルのファンクラブサイトのログインページで他人のチケット申込みを妨害する攻撃を行う者がいるとして話題になっています。

- 複数回ログインに失敗した際にIDをロックする仕様を悪用し、適当なIDに対しわざと間違ったパスワードを複数回入力することにより、そのIDをロックさせ、チケット申込みを妨害するという、単純な手口となっています。

- Twitter上の議論によれば、こういった行為はログインが成功しない限り、現行の不正アクセス禁止法は適用できないとされています。

AUS便りからの所感等

- 攻撃の対象となったファンクラブサイトでは、IDとして会員番号（8桁の数字）を用いていることから、英数字の組合せやメールアドレスに比べれば、適当に入力したIDが実際に存在している確率は高いものと考えられます。

- アカウントのロックは、あるIDに対し大量のパスワードを入力してログインできないか試す、いわゆる「ブルートフォース」攻撃への対抗策として採用されていましたが、今回のように「不正ログインできなくても本来のユーザがログインできないよう妨害する」ために悪用される懸念もまた以前からありました。

- これに対し「一定時間のみロックする」等の調整を行うケースはよくありますが、各ユーザがログインを阻害される可能性を抑えられる方法としては、例えばログインのためのIDをパスワードと同様に非公開のものとし、英数字記号の組合せを使用でき、かつ後から変更可能にすること等も考えられます。

- 一方で既に回避策として「様々なIDを入力しながらログイン試行する」アプローチをとる例も確認されていること等も踏まえると、ID・パスワードによるログイン形式をとる限り、サイトと攻撃者との「いたちごっこ」を終わらせるのは困難ではないかとも考えられ、近年提唱されている「パスワード不要」を謳うような、より新たな認証技術が決め手となるかもまだ未知数と言えます。


INTERNET Watch

誤ったパスワードの入力で他人のIDをロックさせチケットをゲットする技にファン衝撃

tks24　2019年2月6日 06:00

ツイート リスト いいね！318 シェア B! 355 Pocket 210

パスワードを一定回数間違えるとロックされるという仕様を悪用し、他人のアカウントをロックさせてチケットなどの競争率を低くする手法がTwitterで紹介され、大きな波紋を呼んでいる。

これは会員制ファンクラブにおけるチケット申し込みの際、他の会員のIDで誤ったパスワードを連続入力してそのIDをロックさせることで、本物の会員が一定時間ログインできない状況を作り出し、結果的に自身のチケット当選率をアップするという手法。シンプルな数字だけのIDの場合、この手法で見知らぬ会員のIDをロックさせることは可能とみられ、Twitterでは「ゾッとした」「許せない」といった声が渦巻いている。また、過去に遭ったパスワードロック被害の原因がようやく分かったとツイートするユーザーもかなりの数に上っており、被害はかなり大規模に及んでいる可能性もある。今回話題になったのはある芸能プロダクションのファンクラブだが、他人が類推できるIDを採用している他のサイトでも起こりうる問題で、パスワードそのものを変更しても何ら効果がないことから、将来的に大掛かりなシステムの見直しを迫られる可能性はありそうだ。


togetter

まとめトップ › カテゴリー › エンタメ

チケット申し込み時に申し込み数を減らす為こんな酷いイタズラをしている輩がいるらしい「怖い、酷い、最低」

人として恥ずかしくない行動をしたい

申込み パスワード ログイン チケット イタズラではなく犯罪 コメント欄がまた本番 不正アクセス 迷惑行為

philosophyszk 85101view 164コメント

418 B! 96 60 お気に入り 133

まとめ メニュー

そー言えばファミクラ横のセブンで中学生くらいの2人が満タン笑顔で

『チケ申し込みの時に申し込み減らすためにFCのログインページに適当な番号をいれてわざと3回パスワードを間違えてロックかけるんだ(笑)』

「わかるー!!うちもよくやる(爆笑)」

と言ってて恐ろしくなったわ

当気をつけて…

2019-02-04 18:45:26

酷い！

●7,000台以上の業務用冷凍庫にデフォルトのパスワードで侵入、遠隔解凍される可能性

https://jp.techcrunch.com/2019/02/12/2019-02-08-industrial-refrigerators-defrost-flaw/

このニュースをザックリ言うと・・・

- 2月7日（現地時間）、セキュリティ研究者のNoam Rotem氏より、インターネットに接続されている7,000台以上の業務用冷凍庫が遠隔から簡単に解凍を指示できる状態にあるとする報告が発表されました。

- 報告によれば、これらの冷凍庫はイギリスの会社が製造した温度制御システムを使用していますが、同社Webサイト上にあるドキュメントに掲載されているデフォルトのパスワードを入力することにより、操作可能になっているとのことです。

- このシステムはイギリス・アイルランド・スウェーデン・ドイツ等のレストラン・病院・スーパーマーケット等の業務用冷凍庫、およびマレーシアの製薬会社等の冷却施設でも使用されていることがわかっており、これらに外部から解凍指示が出されることにより、予想できないほどの水害、経済的損失、そして在庫の破壊につながる可能性があるとしています。

AUS便りからの所感等

- インターネット上から接続可能な状態になっている複合機やIoT機器等を検索できる「SHODAN」等のサーチエンジンが存在しており、問題となっている冷凍庫もSHODANで検索できる様子が報告には掲載されています。

- 主に攻撃者が使用するSHODANを逆に「自分が設置した機器が見えていないか」等の確認のために使用することも一手ですし、万一そこに掲載されたとしても攻撃を防ぐことができるよう、機器のパスワードは変更することがまずは肝要であり、さらにファイアウォールやUTM等による適切な遮断を行い、場合によってはネットワーク診断を受けることによる安全性の確認等も行うとなお良いでしょう。

●WindowsやAcrobat Readerにセキュリティアップデート、必ず適用を

https://forest.watch.impress.co.jp/docs/news/1169446.html

このニュースをザックリ言うと・・・

- 2月12日（米国時間）、マイクロソフト（以下MS）より、Windowsをはじめとした各種MS製プロダクトの脆弱性を修正する月例のセキュリティアップデートが、同日にはAdobe社からも、「Flash Player」「Acrobat Reader/Reader DC」等でセキュリティアップデートがリリースされています。

- MSのセキュリティアップデートで修正されたものとしては、Windowsのファイル共有機能等で用いられるSMBの脆弱性や、外部から指定したPC上のファイルの有無をテストできるInternet Explorer（IE）の脆弱性等があり、特にIEの脆弱性は既に悪用が確認されているとのことです。

- Acrobat Reader等で修正された脆弱性の一つには、細工したPDFファイルを開くことにより、攻撃者が指定したサーバにSMBリクエストを送信させ、そこに含まれたユーザのハッシュ化されたパスワードを奪取できるものがあり、こちらも既に攻撃コードが公開されていたとされています。

AUS便りからの所感等

- 前述した各社プロダクトはいずれも毎月同じ日に月例のセキュリティアップデートをリリースし、多くの脆弱性が修正されていますので、必ず確認し、アップデートを行うことが根本的対策として重要です。

- また、アップデートを即座に行っている・いないに関わらず、もしくは完了に間に合わない状態でマルウェア等の攻撃を受ける可能性を考慮し、アンチウイルスやUTMによる防御、そしてWindows10であれば少なくとも同梱されているWindows Defenderを有効にする等により、無防備な状態を作らないよう十分に注意しましょう。