

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。

●ユニクロ・GUの通販サイトにリスト型不正ログイン攻撃46万件…氏名や住所、身体のサイズなど流出

<https://www.itmedia.co.jp/news/articles/1905/14/news059.html>
<https://www.nikkei.com/article/DGXMZO44756050U9A510C1H63A00/>



このニュースをザックリ言うと…

- 5月13日（日本時間）、ユニクロ・GUを傘下に持つファーストリテイリング社より、各社**公式通販サイトのアカウント461,091件が不正ログインの被害を受けた**と発表されました。
- 4月23日～5月10日にいわゆる「リスト型攻撃」を受けたことにより、ユーザの氏名・住所・電話番号・メールアドレス・性別・生年月日・購入履歴・クレジットカードの一部情報（カード番号の一部・名義人・有効期限。セキュリティコードは対象外）および、自身や家族の体のサイズといった情報が第三者に閲覧された可能性があると考えられています。
- 同社では13日に被害を受けたアカウントのパスワードを無効化する等の対応を行っています。

AUS便りからの所感等

- 今回の事件はWebサーバ自体からアカウント情報が流出したのではなく、**他のサイトから流出したアカウントのリストを攻撃者が入手し、使用した**とみられ、不正ログインの被害を受けたユーザは複数のサイトで同じID・パスワードを使い回していた可能性が高いようです。
- 「リスト型攻撃」が多発し始めた2014年以降、アカウントの保護においては、それまで常識とされていた「パスワードを定期的に変更する」こと以上に「**簡単でなく推測されにくいパスワードを使う**」「**複数のサイトで使い回さない**」ことが重要とされている他、2段階認証を使うこと等も推奨されています。
- 不特定多数のユーザが登録するようなサービスを運営していない場合でも、自組織で運用しているWeb・メールサーバに対し不正ログインの試行が行われる可能性も考えられますので、攻撃の兆候を検知および遮断できるよう、サーバの設定やUTM等によるIDS・IPS機能の有効化も検討すべきでしょう。



ユニクロ・GUの通販サイトにリスト型攻撃、不正ログイン 46万件 氏名や住所、身体のサイズなど流出

© 2019年05月14日 07:35:59 公開 [ITmedia]

印刷 2199 Share B! 220

ファーストリテイリングと傘下のユニクロ、ジーユー（GU）は5月13日、ユニクロ・ジーユーの公式オンラインストアがリスト型アカウントハッキング攻撃を受け、約46万件のIDに不正ログインされたことと発表。不正ログインを受けたユーザの氏名や住所、電話番号などの個人情報が第三者に流出したと発表。不正ログインを受けたユーザの氏名や住所、電話番号などの個人情報が第三者に流出したと発表。

不正ログインを受けたことを確認したアカウントは46万1091件。氏名や住所、電話番号、メールアドレス、性別、生年月日、購入履歴、クレジットカード番号の一部（上4ケタと下4ケタ）とカード名義人、有効期限などに加え、自身や家族の身体のサイズを登録できる「マイサイズ」に登録した氏名・サイズが第三者に閲覧された可能性があるという。クレジットカードのセキュリティコードは保存していないため、漏えいの可能性はない。

顧客から「身に覚えのない登録情報変更の通知メールが届いた」という申し出を受けて調査を進めたところ、4月23日から5月10日にかけて、不正ログインが試行されたことを確認した。現在は、不正ログインが試行された通信元を特定してアクセスを遮断し、その他のアクセスの監視も強化したという。不正ログインされたIDは、13日にパスワードを無効化し、パスワードの再設定と登録内容確認を依頼するメールを個別に送信した。また、監視中に通報したという。

リスト型攻撃は、他社で流出したID・パスワードのリストを使ってログインを試みる攻撃。同社は、他社サービスとは異なるパスワードを設定することや、第三者が容易に推測できるパスワードを使わないことなどをユーザーに呼び掛けている。また、同社が顧客に対して、メールや電話、SNSなどでパスワードやクレジットカード番号を聞くことはないとして注意喚起している。

日本経済新聞

ユニクロやGU、46万件不正ログイン 通販サイト

ネット・IT サービス・食品 小売り・外食

2019/5/14 8:57

保存 共有 印刷 印刷 ツイット その他

ユニクロを運営するファーストリテイリングは13日、ユニクロとGU（ジーユー）のネット通販サイトで不正アクセスがあったと発表した。現時点で不正ログインされたアカウント数は46万1091件で、住所やメールアドレスなど個人情報の一部が流出した可能性がある。アカウントのパスワードは同日に無効化したという。

同社によると、今回の不正ログインは4月23日から5月10日にかけて確認。あらかじめ用意したIDとパスワードの組み合わせでログインを試みる「リスト型攻撃」という手法で行われた。

不正ログインにより、顧客の名前や住所、電話番号、クレジットカード情報の一部などが閲覧された可能性がある。現時点では情報流出による被害は確認されていないという。

顧客から「身に覚えのない登録情報変更の通知メールが届いた」との連絡があり、調査を進めたところ、不正ログインが判明した。現在は不正ログインが実施された通信元を特定してアクセスを遮断。個人情報が見えられた可能性のあるユーザーIDのパスワードは無効化し、各顧客にパスワードの再設定などを求めている。



●Windows 7以前のリモートデスクトップサービスに脆弱性…XPにも異例のパッチ提供



<https://forest.watch.impress.co.jp/docs/news/1184520.html>

このニュースをザックリ言うと…

- 5月15日(日本時間)、マイクロソフト(以下MS)より発表された月例のセキュリティパッチにおいて、Windows 7(およびWindows Server 2008 R2)以前の**リモートデスクトップサービスに存在する、任意のコード実行が可能な脆弱性(CVE-2019-0708)**が修正されています(Windows 8以降には脆弱性は存在しないとのことです)。
- PCにおいてリモートデスクトップサービスが有効になっている場合、脆弱性の悪用により、攻撃者がPCを外部から乗っ取ることが可能であるとされています。
- MSでは脆弱性の内容を鑑み、既にサポート期限が切れている**Windows XP(およびWindows Server 2003)に対するパッチも「Microsoft Update カタログ」にてリリースしています。**

AUS便りからの所感等

- XPのサポートは2014年に終了していますが、MSでは2017年にマルウェア「WannaCry」に悪用された脆弱性を修正するパッチをやはりXP等に対しリリースしており、**今回も依然無視できないシェアを持つとされるXPに対し、脆弱性を悪用による同様のマルウェアの被害が発生することを懸念して対応を行ったとみられます。**
- Windows 7についても、2020年1月のサポート終了以降かなりの台数が稼働し続けると考えられ、MSから今回のように特別にパッチがリリースされる可能性が考えられますが、可能な限り8.1や10への移行を進めること、さもなくばアンチウイルスの導入およびUTMによる社内LANとの隔離等を検討するようにしましょう。



Windows XPにも異例のパッチ提供～リモートデスクトップサービスにコード実行の脆弱性
「WannaCry」再来の悪夢を防止するためにも速やかな対策を

梶井 秀人 2019年5月15日 08:00

※Microsoftは5月14日(現地時間)、リモートデスクトップサービス(Remote Desktop Services、かつてはTerminal Servicesとも)に重大なリモートコード実行の脆弱性(CVE-2019-0708)が存在することを公表した。Windows 7、Windows Server 2008 R2、Windows Server 2008などに影響し、現在「Windows Update」を介したパッチの提供が行われている。

今回公表された脆弱性はリモートデスクトッププロトコル(RDP)ではなくリモートデスクトップサービスの問題で、細工を施した接続リクエストを送信するだけで悪用が可能。ユーザーの操作を必要としないため、自己増殖して感染を広げる「ワーム」タイプのマルウェアに組み込まれる可能性がある。そうならば2017年に世界中で猛威を振るったランサムウェア「WannaCry」の再来にもなりかねない。

●生徒個人情報データ入りUSBメモリ紛失相次ぐ…静岡県・茨城県の高校

<https://www.sankei.com/affairs/news/190426/afr1904260022-n1.html>
<https://www.sankei.com/affairs/news/190509/afr1905090021-n1.html>



このニュースをザックリ言うと…

- 4月下旬から5月上旬にかけて、県の高校に通う**生徒の個人情報が入ったUSBメモリが紛失する事故が相次いでいます。**
- 4月26日(日本時間)、静岡県教育委員会より、同県立袋井商業高校の教諭が卒業生含む最大424人分の成績基礎データ等が入ったUSBメモリを**校内で紛失した**と発表されました。
- 同5月9日には茨城県教育委員会より、県立鹿島高校の教諭が全校生徒832人の個人情報(保護者氏名含む)を私用のUSBメモリに入れて持ち帰ったところ、**自宅で何者かに盗まれた**ことが発表されています。

AUS便りからの所感等

- USBメモリのみならずSDカードも含めた小さなデバイスについては、個人情報をコピーしたまま紛失するケース、出所が不明なデバイス等をPCに接続してしまうことにより、マルウェアに感染してしまうケース等枚挙に暇がなく、2018年5月にはIBMが各種ポータブルデバイスの使用を全社的に禁止する計画を発表しています。(AUS便り 2018/05/21号参照)
- 機密情報をUSBメモリに入れて持ち出さざるを得ない状況が度々発生するのであれば、万が一の紛失時に第三者へ流出する恐れを防ぐべく、**USBメモリ上あるいはハードディスク上のデータを自動的に暗号化する**といったソリューションの導入等も検討に値するでしょう。



静岡・袋井商の女性教諭、生徒424人の個人情報紛失

2019.4.26 19:21 | 社会 | 事件・犯罪

静岡県教育委員会は26日、県立袋井商業高校(袋井市久能)で業種別の女性教諭が、卒業生を含めて最大424人分の成績基礎データなどの個人情報が入ったUSBメモリを紛失したと発表した。

県教委によると、教諭は今年24日午前9時40分ごろ、生徒の名前や成績評価など成績基礎データなどを保存した私物のUSBメモリ3本をストラップで取り付けたポーチに入れ、業務を行っていた。同日午後3時40分ごろ、ポーチがストラップからとれて紛失しているの気づいたという。教諭は上司に報告し、25、26日に全職員で捜索したが、発見に至っていない。教諭は校外には出ていないという。

生徒個人情報832人分のUSB紛失 茨城県立高教諭

2019.5.9 19:05 | 社会 | 事件・犯罪

茨城県教育委員会は9日、県立鹿島高(鹿嶋市)の男性教諭が、全校生徒832人の氏名と住所、電話番号、保護者氏名が記録されたUSBメモリを紛失したと発表した。現時点で情報漏洩(ろうえい)に発生したかは確認されていない。

県教委高校教育課によると、男性教諭は4日、職員室の業務パソコンで生徒名簿を作成していたが、作業が終わらなかったため私用のUSBメモリにデータを保存して自宅に持ち帰った。6日未明の就寝中、何者か自宅に侵入する機密に違い、USBメモリや財布などが盗られたと気づいたという。自宅を所管する千葉県警捜査課が捜査事件として捜査している。