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。

●Uber侵入・人気ゲーム情報流出に関わった攻撃者、手口は「多要素認証疲れ」

https://www.itmedia.co.jp/news/articles/2209/19/news041.html
https://www.itmedia.co.jp/news/articles/2209/28/news050.html
https://www.itmedia.co.jp/news/articles/2209/20/news091.html

このニュースをザックリ言うと･･･

- 9月18日(米国時間)、人気ゲーム「Grand Theft Auto(GTA)」の未発表の新作を含む一部シリーズ作品のソースコードとプレイ動画がインターネット上にアップロードされる事件が発生しました。

- 「teapotuberhacker」を名乗る人物が、2013年発売の最新作である「GTA 5」と、開発中の新作「GTA 6(仮)」のソースコードをオンラインストレージサービス「MEGA」にアップロード、「GTA 6(仮)」のプレイ動画をYouTubeに公開したとされています(ソースコードは約19時間後、動画は数時間後に削除されたとのことです)。

- teapotuberhackerは、サイバー犯罪グループ「Lapsus$」のメンバーとみられ、同15日に発表された、Uberの社内システムへの侵入にも関与したと称しています。

- Uberへの侵入には、一種のソーシャルエンジニアリングを用いてユーザーアカウントを奪取する手口がとられたとされ、GTAの件でも同様の手口で開発会社のシステムに侵入した可能性があるとのことです。

AUS便りからの所感等

- 何らかの方法でターゲットとなるユーザーのアカウント情報を奪取した攻撃者が、ユーザー本人に多要素認証(MFA)の承認を求める通知が大量に送信されるよう仕向け、同時にIT担当者になりすました上で、通知を止めたければ認証を承認するよう指示し、本人に承認させることにより、多要素認証を突破したとされており、この手口が「MFA Fatigue(多要素認証疲れ、MFA Bombingとも)」攻撃と呼ばれています。

- 多要素認証でユーザーに要求されるアクションは、モバイルデバイスに表示されたメッセージに対し「了承」のボタンをタップすることで成立するものから、別経路(メール・SMS・アプリ等)で送信される認証コードの入力を求めるものまで様々ですが、後者の形をとったものでも、ソーシャルエンジニアリングにより攻撃者が認証コードを奪取・入力して不正ログインが行われる恐れは十分に考えられます。

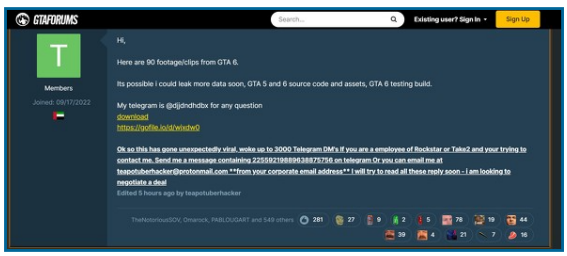
- 多要素認証といえど、全ての不正ログインを完璧に阻止できる万能な仕組みではありませんが、FIDO/FIDO2による生体認証・パスワードレス認証をはじめとした先進的な仕組みの導入、あるいはユーザー側に対しても、パスワード流出の可能性がある場合は速やかに変更すること、ソーシャルエンジニアリングの手口を周知徹底して慎重に行動するよう教育する等、安全性の向上を可能な限り図っていくことが重要です。

ITmedia NEWS

「GTA 6」（仮）のコードとプレイ動画流出か YouTubeはTake Twoの要請で削除済み

2022年09月19日 07時31分 公開 [ITmedia]

「やぁ、GTA 6のプレイ動画90本を公開するよ。後で、GTA 5と6のソースコードもリークするつもり。GTA 6はまだテストビルドだけどね」――。teapotuberhackerと名乗る人物が9月18日（米国時間）、GTA（米Take Two傘下のゲームメーカーRockstar Gamesの人気ゲームグランド・セフト・オート）のソースコードを盗んだとして、そのプレイ動画をYouTubeで、コードをMEGAで公開した。



GTAForumへの投稿

YouTubeへの投稿は数時間後には削除された。URLには「この動画はTake 2

この頃、セキュリティ界隈で

GTA新作リークに使われた“多要素認証疲れ”攻撃とは 1時間以上通知攻め、従業員の根負け狙う

2022年09月28日 08時00分 公開 [鈴木聖子，ITmedia]

人気ゲーム「グランド・セフト・オート」（GTA）などを手掛けるゲームメーカーの米Rockstar Gamesや米Uber Technologiesのネットワークが不正侵入を受け、情報が流出する事件が相次いだ。同じような被害は過去にMicrosoftやCisco、Twitterなどの大手でも発生している。各社とも、そうした侵入を防ぐために多要素認証を設定して従業員のアカウントを保護していたが、攻撃者は「MFA Fatigue（多要素認証疲れ）」攻撃と呼ばれる手口を使ってMFA（多要素認証）を突破していた。

多要素認証で守られたアカウントは、ユーザー名とパスワードを入力してログインしようとすると、登録された端末に電話をかけたりプッシュ通知を送信したりする方法で、そのログインを許可するかどうか確認する。MFA Fatigueの手口ではこれを逆手に取り、故意にログイン試行を繰り返すことで確認通知を何度も執拗（しつよう）に受信させ、相手を疲れ果てさせて承認に追い込む。

● Exchange Serverにパッチ未リリースの脆弱性、攻撃も確認…緩和策適用を

https://forest.watch.impress.co.jp/docs/news/1444438.html
https://msrc-blog.microsoft.com/2022/09/30/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server-ja/
https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

このニュースをザックリ言うと・・・

- 9月30日(日本時間)、Microsoft(以下・MS)より、「Exchange Server」の未修正の脆弱性(CVE-2022-41040, CVE-2022-41082)とそれに対する攻撃が確認されているとして注意喚起が出されています。
- 脆弱性はExchange Server 2019, 2016, 2013に存在(Microsoft 365のExchange Onlineは影響なし)し、Exchange Serverに認証された攻撃者により、サーバーホストを乗っ取られる可能性があるとされています。
- 当該脆弱性については、MSに先立って、同28日にベトナムのセキュリティ企業GTSC社が発表しており、攻撃は8月から確認されていたとしています。
- 10月4日現在、MSからのセキュリティパッチはリリースされていませんが、脆弱性の緩和策が提示されており、リリースまでの間、これを適用することが推奨されています。

AUS便りからの所感

- セキュリティパッチは10月12日に予定されている月例のリリース、あるいはそれに先んじて緊急にリリースされる可能性もあります。
- 緩和策は、既知の攻撃パターンをブロックするもの、および(CVE-2022-41082に対するものとして)組織内の管理者以外のユーザーに対してリモートPowerShellアクセスを無効にするものの2つが提示され、できる限り両方の適用が推奨されますが、根本的な対策はセキュリティパッチの適用によるものとなるため、パッチがリリースされ次第速やかに適用を行うよう準備することが肝要です。
- Exchange Serverについては2021年3月にも危険度の高い脆弱性が修正され(AUS便り2021/03/08号参照)、その際は既にサポートが終了していた2010についてもセキュリティパッチがリリースされましたが、今回の脆弱性が2010に影響するかは不明で、万が一現在も2010を使い続けていたとしても、今回もパッチがリリースされることにはくれぐれも期待せず、より新しいバージョンへのアップグレードを必ず行いましょう。

Impress Watch

「Microsoft Exchange Server」に未修整のゼロデイ脆弱性 ～Microsoftが緩和策を発表

リモートからコードを実行されてしまう可能性

長谷川 正太郎　2022年10月3日 15:54

Microsoftは9月30日（日本時間）、「Microsoft Exchange Server」にすでに限定的な標的型攻撃が確認されている問題が存在することを発表した。同社は修正プログラムの開発を急いでいるが、現時点では未リリースとなっている。

同問題では、サーバーサイドリクエストフォージェリ（SSRF）の脆弱性「CVE-2022-41040」と、攻撃者が「PowerShell」にアクセスできる場合にリモートでコードを実行できる（RCE）脆弱性「CVE-2022-41082」という2つを組み合わせて使われている。脆弱な「Microsoft Exchange Server」の認証されたアクセス権をもつ攻撃者によって、リモートからコードを実行されてしまう可能性があるという。

●都水道局のWindowsアプリに注意…「詐欺被害につながる恐れ」

https://www.itmedia.co.jp/news/articles/2209/30/news117.html
https://twitter.com/tocho_suido/status/1575393899866357760

このニュースをザックリ言うと・・・

- 9月29日(日本時間)、東京都水道局より、同局のWindowsアプリをダウンロードできると騙る偽サイトの存在が判明したとして注意喚起が出されています。
- 注意喚起では、偽サイトは「https://windowsapp.」で始まるURLとされ、Windows PC用を名乗るアプリがダウンロード配布されているとしています。
- 同局では当該サイトとは無関係とし、アプリのダウンロードはApp StoreあるいはGoogle Playストアといった公式のサイトから行うよう呼び掛けています。

AUS便りからの所感

- 挙げられている「偽サイト」は、Windows用アプリを「悪用」と訳していたり、実際にはWindows用Androidエミュレーターを別途用意するよう求められたりと、安易に「Androidアプリ をWindowsで動かしたい」等と考えるユーザーに不正行為を行うよう誘導する不審な内容となっています。
- 東京都水道局アプリのように各種申込や決済を取り扱っているアプリについて、これを騙り、不審なコードが含まれるよう改変されたものであった場合、個人情報や決済サービスのアカウント情報が奪取される恐れがあるため、特に注意を払いましょう。
- ただし、同局の注意喚起で挙げられている偽サイトの見分け方は、今回のケースでは有効であっても、一般的な警戒手段として用いるべきではなく、あくまで本物のアプリがどのデバイスに対し、どこで提供されているかの情報を参考とすべきです。

ITmedia NEWS

都水道局の偽アプリに注意　「詐欺被害につながる恐れ」

2022年09月30日 10時32分 公開　[ITmedia]

東京都水道局は9月29日、同局のWindowsアプリをダウンロードできるとかたる偽サイトを確認したとし、ユーザーに注意を呼び掛けた。ダウンロードすると詐欺被害につながる恐れがあるとしている。

東京都水道局
@tocho_suido · フォローする

【#注意喚起】東京都水道局アプリを騙る偽サイトの存在が判明しました。
URL「https://windowsapp.」で始まるサイトは東京都水道局が準備しているアプリとは関係ありません。ダウンロードをクリックしないように注意ください