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。

●任天堂のアカウントサービスで約16万件の不正ログイン…ゲーム不正購入被害も

https://www.asahi.com/articles/ASN4S72LMN4SPLFA01F.html
https://www.nintendo.co.jp/support/information/2020/0424.html

このニュースをザックリ言うと･･･

- 4月24日(日本時間)、任天堂より、同社3DS・Wii U向けサービス「ニンテンドーネットワークID(以下NNID)」において約16万件の不正ログインの被害が発生したと発表されました。

- SwitchおよびPC・スマートフォン向けの同社別サービス「ニンテンドーアカウント」においても、NNIDと連携していたアカウントが連鎖的に不正にログインされ、それぞれのサービスで登録ユーザーの指名・生年月日・国/地域およびメールアドレスの情報が第三者に閲覧され、ゲームの不正購入等の被害も発生したとのことです(ただしクレジットカード番号については閲覧された可能性はないとしています)。

- 同社ではNNIDを経由してニンテンドーアカウントへログインする機能を廃止、不正ログインされた両サービスのアカウントについて順次パスワードのリセットを行うとした上で、二段階認証の設定等を呼び掛けています。

AUS便りからの所感等

- 例によって、他のWebサイトで流出したアカウント情報を悪用した、いわゆる「リスト型攻撃」の可能性が発表では示唆されており、同社からもパスワードの使い回しを行わないよう注意喚起が出されています。

- 前述の通りNNIDとニンテンドーアカウントは別サービスで、遊ぶゲーム機の乗換えでNNIDの方を使わなくなったことにより、パスワードを変更しないまま放置されたアカウントが狙われた可能性、またNNIDの方で推測されやすいパスワードを設定していた可能性も考えられます。

- ともあれ、数多くのサービスに登録するにあたり、その全てのアカウントについて管理を怠らないことが重要であり、パスワードの使い回しはもちろん、推測されやすい簡単なパスワードを設定していた場合も必ず変更するよう注意してください。

Nintendo

お客様各位

2020年4月24日
任天堂株式会社

「ニンテンドーネットワークID」に対する不正ログイン発生のご報告と「ニンテンドーアカウント」を安全にご利用いただくためのお願い

日頃は弊社商品をご愛顧賜りまして、誠にありがとうございます。

この度、何らかの手段で弊社サービス以外から不正に入手したログインIDとパスワード情報を用いて、４月上旬ごろから「ニンテンドーネットワークID（※１、以下NNID）」に、なりすましログインを行ったと思われる現象が発生していることを確認いたしました。
また、このなりすましログインを利用し、NNID経由で一部の「ニンテンドーアカウント」に不正にログインされた事象があることも確認いたしました。

そのため、本日**NNIDを経由してニンテンドーアカウントにログインする機能を廃止いたしました**のでお知らせいたします。
また、**不正ログインされた可能性があるNNIDやニンテンドーアカウントに対し、順次パスワードリセットを行います。**

●JPCERT/CCとIPA、ゴールデンウィークにおける情報セキュリティ注意喚起を発表

https://www.ipa.go.jp/security/topics/alert20200421.html
https://www.jpcert.or.jp/newsflash/2020041401.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となるゴールデンウィークを迎えるにあたり、4月14日(日本時間)にJPCERT/CC、同21日にはIPAより、情報セキュリティに関する注意喚起が出されています。

- 各組織では、夏季や年末年始そして今回のようなGWといった長期休暇毎に、組織内に常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象にした基本的な対策と心得をまとめ、注意喚起を出しています。

AUS便りからの所感

- IPAでは今回、テレワーク勤務者に向けたセキュリティの注意事項も同時に発表しており(https://www.ipa.go.jp/security/announce/telework.html)、使用するPC等をできる限り他人と共有せず、やむを得ない場合も業務用のユーザーアカウントを別途作成することや、自宅で使用するルーターも最新のファームウェアに更新すること等を挙げています。

- JPCERT/CCでも、テレワーク環境の脆弱性等を起因とした攻撃(VPN装置の脆弱性を突いた攻撃を例に挙げています)や、新型コロナウイルス感染拡大に乗じた攻撃(今年初頭から確認されている保健機関等になりすましたEmotet感染を狙うメール等)への注意を呼び掛けています。

- 一方で、各組織が呼び掛けるセキュリティ対策の内容は常時から注意すべき普遍的なものも多く、GWまでに十分な対応が間に合わなかったとしても、GW明け以降に点検すべきことは多く存在しますし、以後も夏季休暇等に備えて、準備・点検を行うよう意識していくことが肝要です。

●住信SBI・ヨドバシ・auを騙るフィッシング…対策協議会が相次いで注意喚起

https://www.antiphishing.jp/
https://www.netbk.co.jp/contents/company/info/2020/mg_notice_200421_info.html
https://www.yodobashi.com/ec/support/news/200421326750/index.html
https://www.au.com/support/faq/view.k20000002846/

このニュースをザックリ言うと・・・

- 4月21日(日本時間)から同22日にかけて、フィッシング対策協議会より、国内大手企業3社を騙るフィッシングについて注意喚起が出されています。

- 対象となるのは、住信SBIネット銀行・ヨドバシカメラおよびau(注意喚起発表順)で、いずれもアカウントの異常検知やロックが発生したと偽り、アカウント情報や、銀行のキャッシュカードに記載された認証番号あるいは個人情報およびクレジットカード情報を詐取するサイトに誘導するものとなっています。

AUS便りからの所感

- 対策協議会が例に挙げているフィッシングメールによれば、住信SBIのフィッシングメールでは同社のURLが表示されたリンクをクリックすると全くの別サイトに誘導され、またヨドバシのフィッシングメールでは正規のメール配信サービスを悪用してアクセス先を隠蔽している可能性がある模様です。

- ともあれ、このようなフィッシングの事例は普段から様々なサービスを騙って行われており、Webブラウザー・メーラー・アンチウイルスおよびUTMにおけるアンチフィッシング機能等を活用する、不審なメールが届いたらネット上の情報を調査して確認する、利用しているサービスのサイトにはブックマークからアクセスする、等の自衛策をとることを随時心がけて頂ければ幸いです。