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。

●「ドコモ口座」悪用による預金引き出し相次ぐ…本人確認に問題

https://this.kiji.is/675685194667443297
https://nlab.itmedia.co.jp/nl/articles/2009/10/news092.html
https://www.itmedia.co.jp/news/articles/2009/11/news087.html
https://www.nttdocomo.co.jp/info/news_release/detail/20200909_00_m.html
https://docomokouza.jp/maintenance/info_20200910.html

このニュースをザックリ言うと･･･

- 9月7日(日本時間)以降、国内メディアより、NTTドコモ提供の決済サービス「ドコモ口座」を悪用し、銀行口座の預金を不正に引き出される事件が相次いでいると報じられています。

- 預金口座の番号・名義および暗証番号を攻撃者に取得(および推測)され、その攻撃者が作成したドコモ口座に不正に登録されるという手口で引き出しが行われたとされており、また「ドコモ口座」「携帯電話やスマートフォン(NTTドコモやその他キャリア)」あるいは「銀行のネットバンキング等」を利用していない場合でも被害に遭う可能性が指摘されていました。

- 同4日の七十七銀行を皮切りに、複数の地方銀行から注意喚起が出され、各銀行にて「Web口振受付サービス」の利用によるドコモ口座への登録が停止されていますが、その後も引き出しは完全に停止されず、被害が発生したケースもある模様です。

- 同10日にはNTTドコモが記者会見を開き、再発防止策として本人確認書類とSMSによる認証を導入予定としています。

AUS便りからの所感等

- ドコモ口座の開設がメールアドレスのみで可能なことと、銀行口座の登録が実質口座番号と暗証番号のみで可能(口座名義も例えば振込時に口座番号入力で取得可能)であったことに対し、それぞれ本人確認としては不十分であったことがセキュリティ研究者等から指摘されています。

- いわゆる一般的な「ブルートフォース攻撃」のように一つの口座へ暗証番号を変えながら攻撃するのでは口座のロックアウトが発生する恐れがあり、これを回避するために、暗証番号の方を特定の値に固定し、ランダムに指定した口座番号毎に一回ずつ攻撃する手法(「リバースブルートフォース攻撃」「パスワードスプレー攻撃」)をとっていた可能性を指摘する声もあります。

- 前述のNTTドコモの記者会見では「悪意を持つユーザーを排除する仕組みが欠落していた」とのことですが、最悪「ドコモ口座に対応する銀行に口座をもつ全ての利用者」を「本人がドコモ口座を利用できるような状態か確認しなくとも」被害に晒しかねない仕組みであったと言えるもので、銀行側も含め、安易なユーザー拡大ではなく、正当なユーザーを保護するためのセキュアなシステムの構築が求められることでしょう。

KYODO

ドコモ口座に預金不正流出

七十七銀、数人が引き出し被害

2020/9/7 21:51 (JST) | 9/8 07:40 (JST) updated ©一般社団法人共同通信社

仙台市の七十七銀行で、NTTドコモの電子マネー決済サービス「ドコモ口座」を利用した不正な預金引き出し被害が発生したことが7日、分かった。第三者が勝手に七十七銀行の預金者の名義でドコモ口座を作成。不正に盗み出した銀行の口座番号やキャッシュカードの暗証番号を使って銀行の口座から預金をドコモ口座にチャージする手法で、数人が被害を受けたとみられる。

docomo

ドコモ口座への銀行口座の新規登録における対策強化について
<2020年9月9日>

一部の銀行において、ドコモ口座を利用した不正利用が発生していることを受け、9月10日（木曜）から、ドコモ口座における銀行口座(35行)の新規登録を当面停止いたします。
本不正利用は、第三者が銀行口座番号やキャッシュカードの暗証番号等を不正に入手し、ドコモ口座に銀行口座を新規に登録することで発生しておりました。お客さまに、より安心・安全にご利用いただくため、本人確認をオンライン本人確認システム（eKYC）で確実に行う対策を講じた上で、再開時期を検討いたします。加えて、更なるセキュリティ強化に向け、SMS認証も導入いたします。

この度は、被害を受けられたお客さまにお見舞い申し上げるとともに、補償については銀行と連携し、真摯に対応してまいります。

ドコモは今後もお客さまへの一層のサービス向上に取組んでまいりますので、何卒ご理解を賜りますよう、よろしくお願い申し上げます。

●WordPressの「File Manager」プラグインに脆弱性…35万以上のサイトに影響か

https://news.mynavi.jp/article/20200903-1266120/
https://gigazine.net/news/20200903-wordpress-file-manager-vulnerability/
https://ja.wordpress.org/plugins/wp-file-manager/

このニュースをザックリ言うと・・・

- 9月1日(現地時間)以降、米Sucuri社およびタイNinTechNet社といった複数のセキュリティ企業により、WordPressのプラグイン「File Manager」に脆弱性が存在することが相次いで発表されています。

- File Managerはより高機能なファイル管理機能を提供するプラグインですが、脆弱性の悪用により、第三者が不正なファイルをアップロードし、WordPressサイトのコンテンツを改ざんすること等が可能になるとされ、影響を受けるサイトは35万以上に上るとみられています。

- 既に脆弱性を修正したバージョン6.9がリリースされており、利用者はアップデートが強く推奨されています。

AUS便りからの所感

- WordPressには機能拡張のための数多くのプラグインが提供されていますが、利便性を向上させるプラグインのインストールにより、今回のような意図しない脆弱性が導入されることも珍しくなく、特に最初にサイトを構築してから、WordPress本体およびプラグインをアップデートしないままにしているケースが最も危険と言えます。

- 本体・テーマ・プラグインのアップデートは管理画面でまとめて確認できるため、管理者にて随時管理画面へのログインを行い、各種アップデートの確認と実施を行うことが(および不必要なプラグインをインストールしない、無効化する、等も)脆弱性への根本的対策として重要です。

- WordPressサイトや管理画面等の防御を固めるセキュリティプラグイン、あるいはWordPressに特化した攻撃を遮断するWAF等も、前述の2社をはじめ多くのベンダーによって提供されており、また何らかのプラグインが導入されていない素の状態のWordPressについても防御すべきポイントは少なくないため、そういったソリューションの導入の検討は不可欠と言えます。

●8月のフィッシング報告件数、20,000件突破…対策協議会発表

https://www.antiphishing.jp/report/monthly/202008.html

このニュースをザックリ言うと・・・

- 9月3日(日本時間)、フィッシング対策協議会より、8月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 8月度の報告件数は20,814件で、7月度(https://www.antiphishing.jp/report/monthly/202007.html)の16,767件より4,047件の増加、一方でフィッシングサイトのURL件数は4,953件で、7月度の5,536件から583件の減少となっています。

- Amazon・LINE・楽天・楽天カードを騙るフィッシングメールについての報告が全体の約92.6%、特にAmazonについては全体の約67.3%を占めているとのことです。

AUS便りからの所感

- 2020年以降右肩上がりで増加していた報告件数が8月度で一気に2万件の大台を突破、1月時点の6,653件からは3倍にまで膨れ上がっており、今後も同程度の水準を維持することが考えられる一方、挙げられている手口の傾向は6・7月度から大きく変わっていない模様です。

- 差出人メールアドレスとして正規サービスのドメイン名を騙るなりすましメールが全体の4割、特に前述の4ブランドを騙るものでは8割を占めるとされていますが、送信ドメイン認証技術(SPF・DKIM・DMARC等)によるチェックおよびフィルタリングが有効とされており、逆に中小企業側からのメール送信においても、正当な送信元であることを証明するため、これらの技術を導入することは有用でしょう(ただし、外部へのメール送信に指定されたメールサーバーを使うことが通常必須となりますし、万が一PCに感染したマルウェアからメールが送信された場合は別の方法で遮断する必要があるでしょう)。

- 今後も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こと、受信した不審なメールについて旧来の手口か、全く新しい手口が発生したかも含めネット上の報告等から確認すること等を心がけるようにしてください。

フィッシング対策協議会
Council of Anti-Phishing Japan