回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.41

あさまセキュリティニュースレター

日本語でも登場！見覚えのあるパスワードが！？

（2018年10月12日）

すぐにお読みください！　（件名は複数パターンあり）

宛先 [redacted]

こんにちは！

あなたは私を知らないかもしれませんし、なぜあなたはこの電子メールを受け取っているのだろうと思っていますか？
この瞬間、私はあなたのアカウント [redacted]@[redacted].jp をハッキングし、そこからメールを送りました。
私はあなたのデバイスに完全にアクセスできます！

今私はあなたのアカウントにアクセスできます！
たとえば、[redacted]@[redacted].jp のパスワードは[redacted]です

実際に、私は大人の vids（ポルノ資料）のウェブサイトにマルウェアを置きました。あなたは何を知っていますか、あなたはこのウェブサイトを訪れて楽しんでいました。
あなたがビデオクリップを見ている間、インターネットブラウザは RDP（Remote Desktop）として動作するようになりました。
それは私にあなたのスクリーンとウェブカメラへのアクセスを提供するキーロガーを持っています。
その直後に、私のソフトウェアプログラムはあなたのメッセンジャー、ソーシャルネットワーク、そして電子メールから連絡先全体を集めました。　・・・以下略

【使用されているメールの件名の一部】
- すぐにお読みください！
- 緊急対応！
- あなたの心の安らぎの問題
- あなたの秘密の生活
- セキュリティ警告
- アカウントの問題
- 読んだ後に電子メールを削除！
- 緊急のメッセージ
- あなたのアカウントは亀裂です
- それはあなたの安全の問題です。
- あなたのアカウントについて。
- あなたの安全は危険にさらされています！
- 私はあなたのアカウントをハックしている

こちらも前回同様、お客様よりメールが届いたとご連絡が！

前回ご案内した英文表記での脅迫メールに続き、日本語でのメールも出回っております。本文には、実際に使っている、使っていたパスワードが記載されていることも･･･

攻撃のパターン

- ウイルス感染させたパソコンや大手サービスへの不正アクセス等から搾取したメール、パスワード情報をもとに、メール本文にパスワードを付与したメールを送信
- 実際使用しているパスワードを本文に載せることで、メール受信者を脅迫し仮想通貨で支払うよう指示

被害

すでにウイルス感染の可能性　**利用しているサイトで不正アクセス**　**費用の支払い**　**費用を払った後も、再度同様な攻撃を受ける**

対策

- 各WEBサービスのログイン履歴の確認、パスワードの変更
- パスワードの複雑化（大小英字、記号、数字の組み合わせ）、長いパスワード（12文字以上が推奨）にする
- 同一のメール・パスワードの組み合わせで、他サイトを使用することは避ける
- ウイルス対策の強化、不正なWEBサイトへのアクセス制御

情報源

IPA安心相談窓口だより　https://www.ipa.go.jp/security/anshin/mgdayori20181010.html

JPCERT/CC　https://www.jpcert.or.jp/newsflash/2018091901.html

トレンドマイクロセキュリティブログ　https://blog.trendmicro.co.jp/archives/19682

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414