回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.40

あさまセキュリティニュースレター

メールの件名に見覚えのあるパスワードが！？

（2018年9月10日）

From: [redacted]
Date: 2018-07-21 23:11 GMT+09:00
件名　ご自身が利用しているパスワード
To: [redacted]

I am aware 攻撃者が提示するパスワードis your pass. Lets get directly to purpo
Nobody has compensated me to investigate about you. You may not know
me and you are most likely thinking why you are getting this email?

actually, I actually installed a malware on the 18+ streaming (porn)
web site and there's more, you visited this website to have fun (you
know what I mean). When you were viewing video clips, your internet
browser started operating as a Remote Desktop with a keylogger which
provided me with access to your display screen and web cam. after

中略

Number two choice would be to pay me $1000. Lets think of it as a
donation. In this situation, I most certainly will instantly erase
your video footage. You can continue on your life like this never
happened and you would never hear back again from me.

You will make the payment by Bitcoin (if you don't know this, search
for "how to buy bitcoin" in Google search engine).

BTC Address: [redacted]
[case-sensitive so copy & paste it]

すでにお客様より同様なメールが届いたとご連絡頂きました！

メール本文には、どうやってパスワードを搾取したか、料金を支払わなければ、パスワード以外に、搾取した画像や情報を親戚やその他にメールを送るという内容･･･

2013年9月にお客様から、**件名**に**ネットバンキング**で使用している**暗証番号**が記載されたメールが届いたというご相談がありました。
そのパスワードを使用している、すべての暗証番号を変更するようご案内。
ウイルス対策ソフトは入っていましたが、念のため検知率の高いソフトで検査をかけると**29件ヒット**しました。

自分は大丈夫と思っていても、利用しているサイトが不正アクセス被害を受け、情報流出しているケースも。

個人・企業・規模を問わず攻撃が行われています。
インターネットには常に脅威が存在すると意識しましょう！

攻撃のパターン

- ウイルス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、件名にパスワードを付与したメールを送信
- 件名に実際使用しているパスワードを記載することで、メールの内容を確認させる
- 搾取した情報を知人やその他多数に送られたくなければ、という内容で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

情報源

JPCERT/CC　https://www.jpcert.or.jp/newsflash/2018080201.html

情報漏洩の仕組みとSTOP！パスワード使いまわし　https://www.jpcert.or.jp/pr/2018/stop-password2018.html

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