— AUS（アルテミス・ユーザ・サポート）便り 2018/09/25号 —
https://www.artemis-jp.com

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。

●「あなたの安全は危険にさらされています！」仮想通貨を要求する日本語の脅迫メール

https://www.jpcert.or.jp/newsflash/2018091901.html
https://blog.kaspersky.co.jp/blackmail-asking-for-cryptocurrency/21616/

このニュースをザックリ言うと･･･

- 9月20日（日本時間）、JPCERT/CCやカスペルスキー社等より、日本語の文章で仮想通貨を要求するばらまき型の脅迫メールが拡散しているとして注意喚起が出されています。

- 発表によれば、脅迫メールは同18日頃から確認されており、件名は「あなたの安全は危険にさらされています！」「あなたの心の安らぎの問題。」「あなたのアカウントは亀裂です」等多岐にわたり、「PCにマルウェアを感染させてユーザのプライベートな画像を撮影した」等として550ドル（570ドルのものもあり）をBitcoinで送金するよう要求するものとなっています。

- また、カスペルスキー社によれば、日本語や英語以外にも様々な言語の脅迫メールが出回っているとのことです。

AUS便りからの所感等

- 例によって現時点ではメールの日本語が比較的たどたどしい点がありますが、今後修正されていくことも十分に考えられます。

- JPCERT/CCでは7月21日頃から発生していた英語の脅迫メール（https://www.jpcert.or.jp/newsflash/2018080201.html）との関連性を指摘しており、そのメールでは、何らかの経路で奪取したとみられる相手のアカウントのパスワードを提示していたことから、今回についてもアカウントが不正ログインされていないか念のため確認するよう呼び掛けています。

- ともあれ、どのような内容のスパムメールが拡散しているかというネット上の情報を参考にしつつ、安易に要求に応じず冷静な対応をとること、またスパムメールやマルウェアメールあるいはマルウェアへの感染を防ぐためにアンチウイルスやUTMによる防御を確実に行うことが重要です。

JPCERT CC

仮想通貨を要求する日本語の脅迫メールについて　最終更新: 2018-09-20

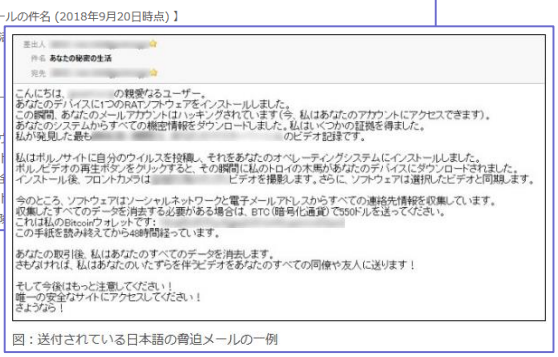
ツイート　メール

CyberNewsFlash一覧

2018年7月21日ごろより仮想通貨 (BTC) を要求する、複数パターンの不審なメールが広く出回っているとの情報を、CyberNewsFlash"仮想通貨を要求する不審な脅迫メールについて"で取り上げておりますが、2018年9月18日ごろより仮想通貨を要求する日本語のメールが確認されています。JPCERT/CCで確認している脅迫メールに使用されている件名は次のとおりです。

【使用されているメールの件名（2018年9月20日時点）】

- 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
- 緊急のメッセージ
- 私はあなたのアカウント
- あなたのアカウント
- それはあなたの安全
- あなたのアカウント
- あなたの安全は危険



差出人
件名 あなたの秘密の生活
宛先

こんにちは、　の親愛なるユーザー。
あなたのデバイスに1つのRAT/ソフトウェアをインストールしました。
この瞬間、あなたのメールアカウントはハッキングされています(今、私はあなたのアカウントにアクセスできます)。
あなたのシステムからすべての機密情報をダウンロードしました。私はいくつかの証拠を得ました。
私が発見した最も　のビデオ記録です。

私はポルノサイトに自分のウイルスを投稿し、それをあなたのオペレーティングシステムにインストールしました。
ポルノビデオの再生ボタンをクリックすると、その瞬間に私のトロイの木馬があなたのデバイスにダウンロードされました。
インストール後、フロントカメラは　ビデオを撮影します。さらに、ソフトウェアは選択したビデオと同期します。

今のところ、ソフトウェアはソーシャルネットワークと電子メールアドレスからすべての連絡先情報を収集しています。
収集したすべてのデータを消去する必要がある場合は、BTC (暗号化通貨) で550ドルを送ってください。
これは私のBitcoinウォレットです:
この手紙を読み終えてから48時間経っています。

あなたの取引後、私はあなたのすべてのデータを消去します。
さもなければ、私はあなたのいたずらを伴うビデオをあなたのすべての同僚や友人に送ります！

そして今後はもっと注意してください！
唯一の安全なサイトにアクセスしてください！
さようなら！

図：送付されている日本語の脅迫メールの一例

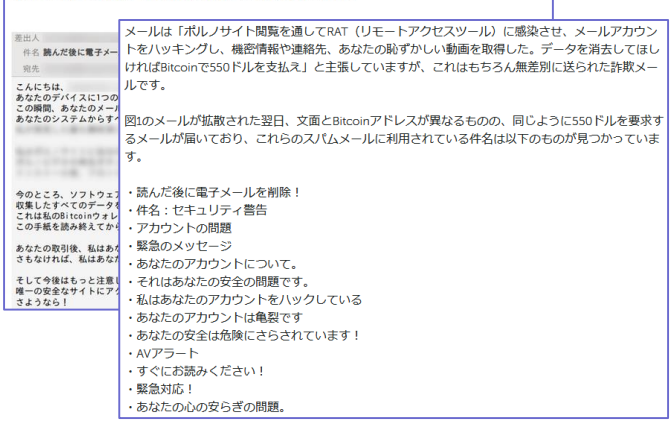
KASPERSKY DAILY

日本語を含めた多言語で拡散する脅迫メール

2018年9月20日

※2018年9月21日更新：新たに確認されたメール件名を追記し、日本語版メールでの要求額の情報を追記しました

詐欺やフィッシング、マルウェア感染を目的としたスパムメールの拡散は日常的なものです。カスペルスキーではつい最近、また新たなスパムメールを観測しました。



差出人
件名 読んだ後に電子メール
宛先

こんにちは、
あなたのデバイスに1つの
この瞬間、あなたのメール
あなたのシステムからす

今のところ、ソフトウェア
収集したすべてのデータ
これは私のBitcoinウォレ
この手紙を読み終えてから

あなたの取引後、私はあ
さもなければ、私はあな

そして今後はもっと注意
唯一の安全なサイトにア
さようなら！

メールは「ポルノサイト閲覧を通してRAT（リモートアクセスツール）に感染させ、メールアカウントをハッキングし、機密情報や連絡先、あなたの恥ずかしい動画を取得した。データを消去してほしければBitcoinで550ドルを支払え」と主張していますが、これはもちろん無差別に送られた詐欺メールです。

図1のメールが拡散された翌日、文面とBitcoinアドレスが異なるものの、同じように550ドルを要求するメールが届いており、これらのスパムメールに利用されている件名は以下のものが見つかっています。

- 読んだ後に電子メールを削除！
- 件名：セキュリティ警告
- アカウントの問題
- 緊急のメッセージ
- あなたのアカウントについて。
- それはあなたの安全の問題です。
- 私はあなたのアカウントをハックしている
- あなたのアカウントは亀裂です
- あなたの安全は危険にさらされています！
- AVアラート
- 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。

●Zaif、不正アクセスでBitcoinなど約67億円相当流出

http://www.itmedia.co.jp/news/articles/1809/20/news059.html

このニュースをザックリ言うと・・・

- 9月20日（日本時間）、テックビューロ社より、同社が運営する仮想通貨取引所「Zaif」が不正アクセスを受け、管理していた仮想通貨の一部が流出したと発表されました。

- 被害を受けた仮想通貨は「Bitcoin」「Monacoin」「Bitcoin Cash(Bitcoinとは異なる仮想通貨)」で、14日17時～19時頃に不正アクセスが発生したとみられ、合計約67億円相当が外部に送金されたとのことです。

- 事件の発表を受けBitcoinの価格は、発表のあった同日2時頃の71万円前後から同4時頃には一時69万円を切る程の下落を見せましたが、以後は急反発しています。

AUS便りからの所感等

- 仮想通貨における事件としては、1月にも仮想通貨取引所「Coincheck」が同様に不正アクセスを受け、不正送金された事件が挙げられます。

- ある取引所でこういったセキュリティインシデントが発生することは、仮想通貨の価格変動や仮想通貨そのものの評価に大きなインパクトをもたらし得ます。

- Coincheckの事件と同様、より詳しい攻撃経路や、それに基づいてどういった対策がとられるかは後日発表されることとなるでしょうが、これまでの事件から得た、また今後得られるであろう知見をもとに、あらゆる取引所にとっては当然ながら対策を適切にとっているかの見直しを図る必要があり、その他の企業のネットワークにおいてもどういった攻撃経路があり得るか洗い出し、やはり不足している対策があれば随時実行していくことが重要になるでしょう。


ITmedia NEWS

Zaif、不正アクセスでビットコインなど約67億円相当流出

テックビューロ（大阪市）が運営する仮想通貨取引所「Zaif」は9月20日、ハッキング被害を受け、同社が管理する仮想通貨の一部を流出したと発表した。被害額は約67億円相当と見られ、現在確認を急いでいる。金融庁と捜査当局に報告し、調査や顧客資産の財源確保に努めているという。

同社によれば、9月14日ごろから仮想通貨の入出金サービスなどに不具合が発生。17日にサーバ異常を検知し、18日にハッキング被害を確認した。

ハッキングを受けたのは入出金用のホットウォレット（※）を管理するサーバ。14日午後5時ごろ～午後7時ごろまでの間に外部から不正アクセスを受け、このサーバで管理していた仮想通貨「ビットコイン」「モナコイン」「ビットコインキャッシュ」が不正に外部へ送金された。ハッキングの手法については、捜査中であることや同種犯行の予防のため「差し控える」としている。

●8月はトロイの木馬が再活性化…チェックポイント社発表

https://news.mynavi.jp/article/20180913-692140/

このニュースをザックリ言うと・・・

- 9月11日（現地時間）、セキュリティベンダーのチェックポイント社より、8月のマルウェアランキングが発表されました。

- 不正に使用されるケースが多いことから、仮想通貨のマイニングを行う「Coinhive」がマルウェアとして扱われ、9ヶ月連続で1位となっています。

- また、同ランキングでは、6月以降オンラインバンキングを狙うトロイの木馬が活発化していると分析しており、今月はその一種「Ramnit」が6位に登場しています。

AUS便りからの所感等

- オンラインバンキングを狙うトロイの木馬は、近年も「Gozi(別名URSNIF)」やその亜種「Dreambot」が猛威をふるっています。

- Ramnitは2017年6月に日本への感染が本格化し、改ざんされたWebサイトから閲覧したユーザのPCに感染する経路をとっているとされています。

- どういった種類のマルウェアが流行するかは日々変動し、また一旦沈静化した種類のものでもいつまた再び活動しだすか予測することは簡単ではありません。

- アンチウイルスやUTMによる防御が十分に行われているかを確かめつつ、様々な種類のマルウェアがどういった経路で感染するか、どうやって感染する可能性を抑えるか、についても随時情報収集していくことが肝要です。


マイナビニュース

トロイの木馬が再活性化 - 8月マルウェアランキング

順位	PCマルウェア	前月比較
1	Coinhive	=
2	Dorkbot	↑
3	Andromeda	↑
4	Cryptoloot	↓
5	Jsecoin	=
6	Ramnit	↑
7	XMRig	=
8	Roughted	↓
9	Conficker	↓
10	Nivdort	↑