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。

●楽天カードをかたるウイルスメールが出回る…警視庁等警告

http://news.livedoor.com/article/detail/13744143/
https://www.rakuten-card.co.jp/info/news/20171012/

このニュースをザックリ言うと･･･

- 10月13日（日本時間）以降、警視庁、日本サイバー犯罪対策センター（JC3）および楽天カード株式会社より、楽天カードのカスタマーセンターをかたった「ウイルスへのリンクが記載されたメール」が拡散しているとして警告が出されています。

- メールは、件名が「口座振替日のご案内【楽天カード株式会社】(楽天カード)」等となっており、本文中で「重要なお知らせ」や「請求金額の確認」へのリンクとして、ウイルスがダウンロードされるようなURLが含まれているとのことです。

- 楽天カード社では、「弊社からお送りするメールでお客様に直接ファイルをダウンロードさせるようなものはございません」として、身に覚えのないメールは記載されたURLをクリックせず、削除するよう呼び掛けています。

AUS便りからの所感等

- 絶えることなく手を変え品を変えてはウイルスに感染させようとするあまたのメールの中でも、今回のケースは特に「本物と見分けがつきにくいもの」の一つとされており、利用者は十分な注意が必要でしょう。

- 電話番号も偽の番号が記載されており、こちらも電話をかけてきた相手をだます目的があると考えられます。

- こういったウイルスメールからのウイルス感染、あるいはフィッシングサイトへの誘導の恐れを可能な限り低減させるには、ユーザ側の自衛策として、通常使用するサービスのログインページはブックマークに登録してそこからアクセスすること、またシステム側での防御策としては、Webブラウザやアンチウイルスソフト・UTMが提供する不審なサイトへのアクセスを警告あるいは遮断する機能を可能な限り有効にすること、等が重要です。

livedoor NEWS

楽天カードカスタマセンターを騙る不審メールが出回る 注意を呼びかけ

155 1411 2017年10月13日 18時3分

ざっくり言うと

- 楽天カードを騙るウイルスメールが出回っていると警視庁が注意喚起している
- 不審メールの件名には「カスタマセンターからのご案内」などとある
- URLはクリックせず、メールを削除するよう楽天カード社は呼びかけている

◆ウイルスメールへの注意喚起

警視庁サイバーセキュリティ対策本部
@MPD_cybersec

【サイバー犯罪対策課】
ウイルスをダウンロードさせるメールが拡散中。件名は「口座振替日のご案内【楽天カード株式会社】(楽天カード)」。実在の会社を装っていますが、本文中のリンクをクリックしてダウンロードされるファイルはウイルスです。ご注意ください。

2017/10/13 17:8

221 RETWEETS 93 FAVORITES

Rakuten Card

楽天カードを装った不審なメールにご注意ください

先日より、楽天カード株式会社を装った不審なメールが配信されているという情報が寄せられております。
こちらの不審なメールは、弊社から送信したメールではございません。
ウイルスに感染するなどの被害に遭う可能性がございますので、差出人が「楽天カード株式会社」となっていても、身に覚えのない内容のメールに記載されているURLは絶対にクリックせず、送られてきたメールそのものを削除していただきますよう、何卒宜しくお願いいたします。

・身に覚えのない内容のメールに記載されてるリンク
・リンク・URLをクリックしてファイルがダウンロードされ
・不明な添付ファイル（zip）は開かない。
・宛先に自分以外の複数の受信者（メールアドレス）が
い。

弊社からお送りするメールでお客様に直接ファイルをダウン口
せん。

■メールの一例

ご請求予定金額のご案内

いつも楽天カードをご利用いただきありがとうございます。

2017 年 10 月分のご請求予定金額をご案内いたします。

カードご利用代金のお支払いは、毎月 20 日(金融機関が休業日の場合、翌営業日)
に口座ご指定いただいております金融機関の口座より自動振替いたします。

19 日までに引落口座へのご準備をお願いいたします。

◆◇◆ ご請求予定金額

【ご利用カード】 楽天カード

【お支払い日】 2017/10/20

なお、弊社の引き落とし日は毎月27日（休日の場合は翌営業日）となっております。
上記以外にも、口座振替日をお知らせする内容のメールが配信されているという情報もございます。

●IPAとJPCERT/CC、「ランサムウェア特設サイト」を開設

http://itpro.nikkeibp.co.jp/atcl/news/17/101802468/
https://internet.watch.impress.co.jp/docs/news/1088558.html

このニュースをザックリ言うと・・・

- 10月18日（日本時間）、情報処理推進機構（IPA）より、ランサムウェアの脅威について情報を集約する「ランサムウェア特設サイト」の開設が発表され、同26日にはJPCERT/CCが同様のサイトを開設しています。

- これらのサイトでは、「ランサムウェアとは何か」から「ランサムウェアに感染しないための対策」「感染した場合の対処法」まで様々な情報がまとめられており、多くのセキュリティベンダーや警察機構等が参加する「No More Ransom」プロジェクトについても紹介されています。

- この他IPAのサイトでは、ロシア等で同24日頃から新たなランサムウェア「Bad Rabbit」による感染被害が報告されている（https://www.ipa.go.jp/security/ciadr/vul/20171026-ransomware.html）として注意が呼び掛けられています。

AUS便りからの所感等

- IPAの情報セキュリティ安心相談窓口には、2015年以降、ランサムウェアによってPC上のファイルが暗号化され、身代金を要求された等の相談が多く寄せられるようになったとのことです。

- 挙げられている対策は、「ファイルやシステムの定期的なバックアップを実施する」ことのほか、ランサムウェア以外のマルウェアへの対策でも通用する各種対策となっており、是非とも目を通し、普段から実施しているかのチェックリストを作成する等により、システム・ネットワークの安全性を保つ一助としてほしいものです。

●新たなIoTボットネット出現、「Mirai」級のDDoS攻撃発生の懸念も

https://japan.zdnet.com/article/35109216/

このニュースをザックリ言うと・・・

- 10月19日と20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とQihuu 360社より、新たなIoTボットネットが形成されつつあるとする調査結果が相次いで発表されています。

- 「IoTroop」あるいは「IoT_reaper」と名付けられたマルウェアは、主にインターネットに接続された監視カメラに感染するとされており、少なくとも8~9社のメーカーの製品について脆弱性が悪用されているとのことです。

- 各社とも20日までの時点では大規模な攻撃は確認されていないとしながらも、ボットネットの構築は急速に進んでいるとして、攻撃に備えた準備を行うよう警告しています。

AUS便りからの所感等

- チェックポイント社の発表では、一例として、兵庫県芦屋市に設置されているとみられるネットワークカメラがマルウェアに感染し、海外の別のカメラに対し攻撃を仕掛けているとされるケースが挙げられています。

- PCやスマートフォンと異なり、人が頻繁に触ることの少ない傾向にあるIoT機器では、セキュリティパッチの適用が後手に回ることや、攻撃や侵入の発生が検知されにくいことが容易に想定されます。

- IoT機器の設置にあたっては、まず資産管理等において必ずその存在を把握しておくこと、機器自体において適切なパスワードやアクセス制限、あるいは不要なサービスの無効化といった設定を行うこと、セキュリティパッチのリリース情報の把握と迅速な適用、加えてUTM・IDS・IPS等によってもさらなるアクセス制限や侵入検知・遮断を行うよう防御すること、等が重要となります。

- また、既に設置された機器に対し外部から不正にアクセスされる恐れがないか、ネットワーク診断を行うことも是非とも視野に入れるべきでしょう。