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。

●YouTuberをターゲットにしたフィッシング、チャンネル乗っ取りも…Googleが注意喚起

https://www.itmedia.co.jp/news/articles/2110/21/news090.html
https://wired.jp/2021/10/25/youtube-bitcoin-scam-account-hijacking-google-phishing/
https://blog.google/threat-analysis-group/phishing-campaign-targets-youtube-creators-cookie-theft-malware/
https://www.itmedia.co.jp/news/articles/2002/13/news087_2.html

このニュースをザックリ言うと･･･

- 10月20日(現地時間)、米Google社より、同社傘下のYouTubeにおいて発生しているフィッシングについて注意喚起が出されています。

- フィッシングは2019年9月頃から報告され、YouTube投稿者(YouTuber)のチャンネルで公開されるメールアドレス宛に商品のコラボレーション依頼を騙るメールを送り、新型コロナ関連のニュースサイト等に偽装したサイトに誘導、マルウェアをダウンロードさせ、YouTuberがログインしているセッションのCookieをブラウザーから奪取するという手口をとっているとのことです。

- 攻撃者はこれによってチャンネルを乗っ取り、暗号資産(仮想通貨)の取引所を騙る動画による詐欺を行ったり、チャンネル・アカウントを売却したりしているとのことです。

- 同社では「セーフブラウジングの警告を真剣に受け止める」「ソフトウェアの実行前にアンチウイルスによるスキャンを実行する」「Chromeの『保護強化機能』を有効にする」「暗号化されたアーカイブに注意する(マルウェアスキャンをすり抜ける可能性が高いため)」「二段階認証(あるいは多要素認証)によってアカウントを保護する」ことを推奨しており、特に二段階認証について、11月1日以降、チャンネルでの収益化を行っているYouTuberがYouTube Studio等を利用する際に義務付けるとしています。

AUS便りからの所感等

- Googleでは2021年5月以降、同社のGMailアドレスを利用したフィッシングメールの99.6%を遮断している一方、攻撃者はemail.cz(および.czドメインの複数のサービス)やaol.com等別のメールサービスへ移行しており、フィッシングやマルウェアをはじめ明らかな攻撃メールの送受信を遮断することをあらゆるメールサービスが団結して行うことが望まれるところです。

- YouTubeでは、やはり2019年9月に、Googleのセキュリティアラートを騙るフィッシングメールでチャンネル乗っ取りを狙うケースも確認されており、こちらはフィッシングサイト上で二段階認証の入力までユーザー本人に行わせることで認証を突破する手口となっていた模様です。

- 二段階認証や多要素認証において、攻撃者に奪取されないことを意図してSMS等別の経路で送信される情報であっても、フィッシングサイトから全て入力して攻撃者に手渡してしまっては元も子もありませんので、とにかくネット上で報告されているフィッシングの情報や手口に関する知識を随時取得し、誤った判断をしかねない場面において複数の防御策によってカバーするよう心掛けましょう。


YouTubeチャンネルを乗っ取るフィッシング攻撃についてGoogleが警告

2021年10月21日 11時10分 公開 [ITmedia]

米Googleは10月20日（現地時間）、傘下のYouTubeでYouTuberを標的とする金銭目的のフィッシング攻撃についての対策などについて説明した。この攻撃は2019年後半から始まっており、攻撃者は「ロシア語を使うフォーラムで募集されたハッカーグループ」だとしている。

手口は、YouTuberが自分のチャンネルで公開しているメールアドレス宛に動画広告コラボの相談などのフィッシングメールを送って偽の企業サイトに誘導し、信用させてマルウェア入りのデータをダウンロードさせるというもの。

誘導先のWebサイトはSteam上のゲームや新型コロナ関連ニュースサイトなど、本物と見紛うものが多いという。

フィッシング用に作られたニュースサイト

● TCPポート6379番宛パケット増加、redisサーバーのフィルタリングを…JPCERT/CC定点観測レポート

https://news.mynavi.jp/article/20211021-2165012/
https://blogs.jpcert.or.jp/ja/2021/10/tsubame_overflow_2021-07-09.html

このニュースをザックリ言うと・・・

- 10月19日(日本時間)、JPCERT/CCより、同組織がインターネット上で運営する観測用センサーによる2021年7月～9月の定点観測レポートが発表されました。

- 国内で観測されたパケットのうち最も多く宛先ポートに指定されていたのはTCPポート23番(Telnetで使用)ですが、次いでデータベースサーバーソフト「Redis」が使用する同6379番が徐々に増加し、2位にランクインしています。

- TCPポート6379番宛パケットは中国を送信元とするものが8割を占め(次いで米国・シンガポール)、またパケットの量は調査期間内にかけて約1.5倍に増加したとのことです。

AUS便りからの所感

- TCPポート6379番宛パケットは、既に外部からアクセス可能なRedisサーバーの存在を探索するのみならず、不正な認証の実行や情報の取得を意図したものが確認されているとのことです。

- またこれとは別に、ロシア国内とみられる特定のIPアドレス帯から、様々なポート宛のパケットが送信されているとの情報もあります。

- オンプレミス(社内・データセンター上)・クラウドに拘わらず、設置したホスト上の各種サーバープログラムに対し意図しないアクセスを受けることのないよう、OS自体および外側のルーター・UTM等のパケットフィルタリング機能を確実に設定し、加えて不審なパケットを監視する仕組みも用意し、攻撃から防御できるよう備えることが重要です。


JPCERT/CC、インターネットのパケットの動向伝える「TSUBAMEレポート Overflow」公開

2021/10/21 08:47

JPCERT/CCは10月19日、2021年7～9月期の「TSUBAMEレポート Overflow」（以下、TSUBAMEレポート）を公開した。

- TSUBAMEレポート Overflow（2021年7～9月） - JPCERT/CC Eyes | JPCERTコーディネーションセンター公式ブログ

「TSUBAME」はJPCERT/CCがインターネット上で通信されるパケットの動向を調査するために運営しているインターネット定点観測システムの名称。TSUBAMEレポートは、同団体が四半期ごとに公表している「インターネット定点観測レポート」の公開と併せて、レポートでは言及していない単外に設置しているセンサーの観測動向やその他の活動などをまとめたものである。なお、「インターネット定点観測レポート」は次のページで公開されている。

● 7～9月のIPA相談窓口への相談件数1,012件、過去最少水準

https://www.ipa.go.jp/security/txt/2021/q3outline.html
https://is702.jp/news/3913/

このニュースをザックリ言うと・・・

- 10月19日(日本時間)、情報処理推進機構(IPA)より、同機構の情報セキュリティ安心相談窓口で2021年第3四半期(7～9月)に受け付けられた相談状況について発表されました。

- 同時期における相談員対応件数は1,012件で、前四半期(4～6月)の1,827件より約44.6%減となっています。

- 相談件数の多い手口として「ウイルス検出の偽警告(192件)」「仮想通貨で金銭を要求する迷惑メール(98件)」「宅配便業者をかたる偽SMS(67件)」「iPhoneに突然表示される不審なカレンダー通知(21件)」「ワンクリック請求(21件)」「不正ログイン(16件)」等計7種類が挙げられていますが、いずれも過去1年間で最も少なくなっています。

AUS便りからの所感

- 同窓口の相談件数は、2020年第3四半期(7～9月)に3,000件を突破して以降、前四半期での一時的な増加を除いて減少傾向にあり、今回はここ10年間で最少水準となっています。

- 「ウイルス検出の偽警告」と並び最も相談件数が多い手口の一つだった「宅配便業者をかたる偽SMS」が1～3月241件・4～6月345件から急減、また「iPhoneの不審なカレンダー通知」は1～3月72件・4～6月109件から、「不正ログイン」も1～3月50件・4～6月55件からとそれぞれ増加から一転しての減少となっています。

- 第4四半期(10～12月)においてどういった攻撃が発生するかは未知数ですが、2022年北京冬季オリンピック、第6波の到来が予想される新型コロナ感染症あるいは相次ぐ金融機関の障害等、様々な出来事に便乗した詐欺が発生する恐れもあり、アンチウイルスやUTM等による防御も含め、油断なく各種防衛策をとるに越したことはありません。