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。

●国内38社のVPN認証情報流出か…悪用は確認されず

https://this.kiji.is/670824175439250529
https://www.asahi.com/articles/ASN8T3TNMN8TUTIL002.html
https://cybersecurity-jp.com/news/38962

このニュースをザックリ言うと･･･

- 8月25日(日本時間)、複数のメディアより、国内大手企業を含む世界の企業等からVPN接続のための認証情報が流出したと報じられています。

- 流出は内閣サイバーセキュリティセンター(NISC)への取材で明らかになったもので、被害を受けたのは、共同通信によれば住友林業・日立化成を含む国内38社、また朝日新聞によれば国内外900社に及ぶとのことです。

- NISCによれば、8月中旬にダークウェブ(サーチエンジンに表示されない、あるいは特殊な手段でアクセス可能なサイト)上で情報がやりとりされていたことを確認したとのことですが、情報は暗号化されており、実際に不正ログインが行われたケースは確認されていないとのことです。

AUS便りからの所感等

- 認証情報は、いずれもPulse Secure社の、2019年に脆弱性が報告されていたSSL-VPN製品から流出したとみられ、また同社からアップデートがリリースされる(AUS便り 2019/9/24号参照)前に攻撃者が脆弱性を悪用して奪取していた可能性も指摘されています。

- 対象の各社では既に機器のアップデート・パスワードの変更あるいはVPNサービス自体の停止といった対策をとっている一方、被害を受けたうち一社は、以前交換した脆弱性のある古い機器を、テレワーク実施時の負荷分散のため再度稼働させていたという事情を発表しています(https://www.itmedia.co.jp/news/articles/2008/26/news123.html)。

- 万が一機器に対しOS・ファームウェアのアップデートを適用できないというケースでは、その他の多重の対策で攻撃を確実に防御できるかを検討すること、一方で適切なアップデートもなく所在が把握されていない機器が稼働していないかについても、十分な注意が必要です。

朝日新聞 DIGITAL

VPN欠陥つくサイバー攻撃　国内外900社の情報流出

会員記事

2020年8月25日 11時58分

シェア　ツイート　ブックマーク　メール　印刷

list　0

社外から企業内のネットワークに接続するときに使う「仮想プライベートネットワーク（VPN）」の 通信機器 の欠陥をついたとみられる サイバー攻撃 があり、国内外900社が機器を使う際の情報が流出していたことが内閣サイバーセキュリティセンター（NISC）への取材でわかった。VPNは テレワーク の拡大もあり、利用者が広がっている。

KYODO

在宅勤務の認証情報38社が流出

住友林業や日立化成など悪用恐れ

2020/8/25 11:55 (JST)　8/25 18:45 (JST) updated　©一般社団法人共同通信社

住友林業や日立化成などで在宅勤務する社員らが社内システムの利用時に必要な機器「VPN（仮想私設網）」の認証情報が、不正アクセスによって盗まれていたことが25日、情報セキュリティー専門家への取材で分かった。両社を含む38社分の認証情報がインターネット上に流出している。

● IPA が「事業継続を脅かす新たなランサムウェア攻撃」に関する注意喚起を公開

https://www.ipa.go.jp/security/announce/2020-ransom.html

このニュースをザックリ言うと･･･

- 8月20日(日本時間)、情報処理推進機構(IPA)より、「事業継続を脅かす新たなランサムウェア攻撃について」と題した注意喚起が発表されました。

- IPAによれば、2018～2019年頃より、明確に標的を企業・組織に定め、「人手によるランサムウェア攻撃」および「二重の脅迫」という新たな手口を取り入れた攻撃が現れてきているとのことです。

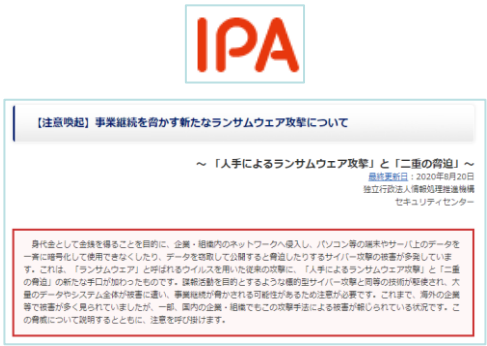
- 「人手によるランサムウェア攻撃」は攻撃者自身がターゲットのネットワークに侵入し、PC・サーバー等をランサムウェアへ感染させる等を行う、「二重の脅迫」は機密情報を暗号化するのみならず元のデータを奪取し、身代金を払わなければデータを(段階的に)公開するとも脅迫する、としています。

AUS便りからの所感

- 注意喚起では「人手によるランサムウェア攻撃」が発生した3つの事例、「二重の脅迫」が発生した1つの事例が挙げられていますが、前者の事例の1つでは、同時期に本田技研工業の社内ネットワークにも感染が報告されていたランサムウェア「EKANS」が用いられていた模様です(AUS便り 2020/06/15号参照)。

- 「人手によるランサムウェア攻撃」では攻撃者の侵入経路の一つとしてリモートデスクトップ等が挙げられているものの、今回新たに警戒すべきポイントとなったわけではなく、一方「二重の脅迫」についても、これまでのような「確実なバックアップの取得とバックアップデータの保護」だけで防げない新たな脅迫方法が追加された一方、攻撃者に機密データを持ち出されないための防衛策も確実に行っているか等が鍵となるでしょう。

- 見方を変えれば既存の攻撃手法の組合せによるものであり、これまでに推奨されていた各種対策について、改めて実施の有無・可否を点検・検討し、UTMの採用やネットワーク構成の見直し等による対策を着実に実行することが肝要です。



●宅配便の不在通知を装うフィッシング…対策協議会が注意喚起

https://www.antiphishing.jp/news/alert/fuzaiSMS_20200821.html
https://www.netbk.co.jp/contents/company/info/2020/mg_notice_200811_info_2.html

このニュースをザックリ言うと･･･

- 8月21日(日本時間)、フィッシング対策協議会より、宅配便の不在通知を装い、金融機関等のフィッシングサイトへ誘導するSMSの報告が続いているとする注意喚起が出されています。

- SMSの一例として、本文が「お荷物のお届けにあがりましたが不在の為持ち帰りました。ご確認ください。」と書かれ、「http ://●●●●.duckdns.org/」というURLのリンクが記載されており、クリックにより、住信SBIネット銀行を騙りネットバンキングの各種ユーザー情報を詐取しようとするサイト(URLは「http ://netatar-●●●●.com/netbk/」等)に誘導されるケース(および不審なアプリをダウンロード・インストールさせるケース)が挙げられています。

- 同銀行からも8月11日に注意喚起が出されており、それぞれリンクをクリックしたり、誘導先のサイトで情報を入力しないよう呼び掛けています。

AUS便りからの所感

- SMSによるフィッシング(スミッシング)はメールによるものに比べ一般にUTM等で防御することが難しく、ネット上の注意喚起やユーザーによる報告がないか検索することがより大事となり、併せて可能な限りモバイル機器自身に信頼のおけるベンダーによるセキュリティアプリをインストールすることを推奨致します。

- 住信SBIネット銀行では、SMSに掲載するURLに前述したドメイン名は用いず、「***.netbk.co.jp」「***.netbk.jp」を用いる等としており、サービス提供者側としては、このように自社サービスで使用するドメイン名を告知すること(そしてドメイン名の追加あるいは使わなくなったドメイン名についても随時情報を更新すること)が、フィッシングの標的となったユーザーを安心して行動させる意味で重要と言えます。