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。

●米フィットネス機器大手、ランサムウェアによる攻撃でネットサービス等停止

https://japan.cnet.com/article/35157255/
https://www.watch.impress.co.jp/docs/news/1267891.html

このニュースをザックリ言うと・・・

- 7月23日(現地時間)、スポーツ・フィットネス関連のIoT機器・サービス等を提供する米Garmin社より、「Garmin Connect」をはじめとする同社サービスがサイバー攻撃による障害で停止していることが発表されました。

- 同27日の同社の発表では、「WastedLocker」と呼ばれるランサムウェアにより、システムの一部が暗号化されたことが原因としています。

- システムの復旧作業は同30日(日本時間)現在も完了していない一方、ユーザーデータが失われたり盗まれたりした疑いはないとのことです。

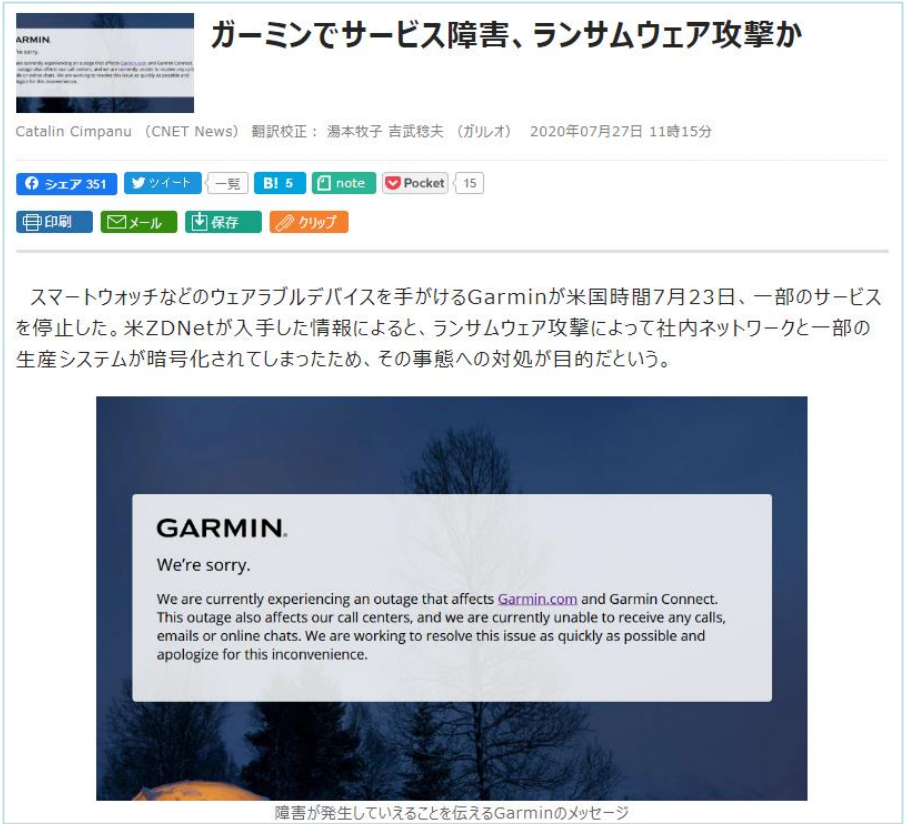
AUS便りからの所感等

- WastedLockerは今年5月に詳細が報告された比較的新しいランサムウェアとされ、ロシアの攻撃者グループが使用しているとのことです。

- 同社で7月29日に四半期決算の発表を控えていた時期の障害で、一時的に株価の乱高下も発生したとのことです。

- たとえユーザーに関するデータの機密性に影響しなかったとしても、サービスの利用に関する可用性、ないし会社の評判への影響に結び付く可能性がありますので、ランサムウェアないしマルウェア全般への備えとして、サーバー・クライアントそれぞれにおけるアンチウイルスやデータバックアップ等、また各ネットワークでの感染発生が他方に影響しないためのUTM等による隔離を適切に実行することが肝要です。

c|net Japan



ガーミンでサービス障害、ランサムウェア攻撃か

Catalin Cimpanu （CNET News） 翻訳校正： 湯本牧子 吉武稔夫 （ガリレオ） 2020年07月27日 11時15分

シェア 351 ツイート 一覧 B! 5 note Pocket 15
印刷 メール 保存 クリップ

スマートウォッチなどのウェアラブルデバイスを手がけるGarminが米国時間7月23日、一部のサービスを停止した。米ZDNetが入手した情報によると、ランサムウェア攻撃によって社内ネットワークと一部の生産システムが暗号化されてしまったため、その事態への対処が目的だという。

GARMIN.
We're sorry.
We are currently experiencing an outage that affects Garmin.com and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

障害が発生していえることを伝えるGarminのメッセージ

● Facebookメッセンジャーへの不審なメッセージ、IPAが注意喚起

https://k-tai.watch.impress.co.jp/docs/news/1267968.html
https://twitter.com/IPA_anshin/status/1288055792965316608

このニュースをザックリ言うと･･･

- 7月28日(日本時間)、情報処理推進機構(IPA)より、Facebookメッセンジャーに不審な動画メッセージが送られてきたという相談が増えているとして、Twitterにて注意喚起が出されています。

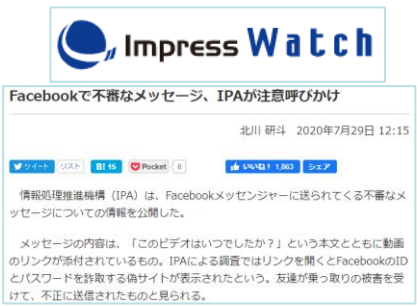
- 注意喚起によれば、「このビデオはいつでしたか？」という一文とともに動画が送られてくるものの、メッセージをタップしても動画は再生されず、Facebookアカウント情報を詐取する偽ページ、さらにはアンケートサイトや不審なアプリのインストールを促すページに誘導されるとのことです。

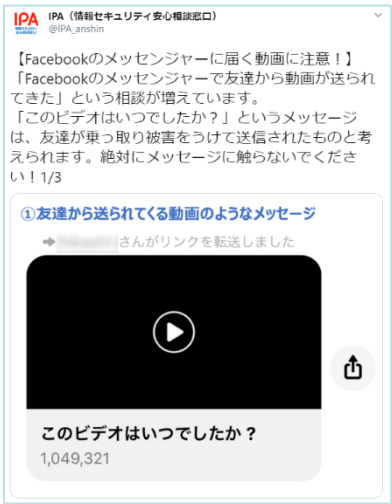
- IPAでは、このようなページに情報等を入力したり、不用意にアプリをインストールしないよう呼び掛けています。

AUS便りからの所感

- 注意喚起では、友達のアカウントが乗っ取られてメッセージが不正に送信されたものと推測しており、アカウント情報を入力したり、不正なアプリをインストールしたりした場合、自分のアカウントの権限でさらに友達へ不審なメッセージを拡散させることに繋がり得ます。

- スマートフォンに対し非公式のアプリストアからのインストールを考えなしに行わないこと、フィッシングメールと同様、不審なメッセージについても、ネット上に報告がないか検索しながら慎重に対応することが重要であり、場合によっては送信元の相手に連絡して注意を促すことも行うべきでしょう。





●サイバー攻撃集団「Tropic Trooper」、USB経由で閉域ネットワークへ侵入

https://blog.trendmicro.co.jp/archives/25719

このニュースをザックリ言うと･･･

- 7月28日(日本時間)、セキュリティベンダーのトレンドマイクロ社より、サイバー攻撃グループによるUSBメモリーを悪用した攻撃の手口が同社ブログ記事で紹介されています。

- 「Tropic Trooper」と呼ばれる攻撃グループは、台湾やフィリピンの軍事機関の、外部と物理的に接続されていない隔離されたネットワークに対し、USBメモリーから重要な情報を窃取するマルウェア「USBferry」を利用して侵入したとしています。

- 同社ではこのような攻撃から回避するための対策として「最小特権の原則を適用する(ネットワークのセグメント化等)」「システムとアプリケーションを最新のバージョンにしておく」および「定期的に周囲の監視を実行する」ことを挙げています。

AUS便りからの所感

- 同社の調査では、USBferryによる攻撃は2014年から活発になっており、標的のネットワークから「defense-(防衛)」「ocean-(海洋)」 および「ship-(船舶)」に関連した文書の窃取に焦点を当てており、主な目的を機密情報の窃取であると推測しています。

- USBメモリーを仲介しての攻撃は決して新しいものではないことは、同じくセキュリティベンダーのカスペルスキー社もブログで述べており、同様のマルウェアとして2010年に発見されたStuxnetを挙げている他、隔離されたネットワークからデータを窃取する様々な方法も挙げています(https://blog.kaspersky.co.jp/jumping-over-air-gap/28678/)。

- USBメモリーを使用せざるを得ない状況である場合は、組織の管理下にないUSBメモリーを持ち込んだり、管理下にないPCに接続させたりしないこと、またUSBメモリーに侵入したマルウェアにデータを奪取され、外部で待っている攻撃者に渡されることを食い止めるための出口対策を確実に実行することが重要でしょう。