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。

●Honda、ランサムウェア感染による大規模障害…現在は復旧

https://www.yomiuri.co.jp/economy/20200612-OYT1T50263/
https://forbesjapan.com/articles/detail/35133

このニュースをザックリ言うと・・・

- 6月9日(日本時間)、本田技研工業(以下Honda)より、同8日以降、同社ネットワークがサイバー攻撃を受け、国内外拠点で大規模なシステム障害が発生していると発表されました。

- 社内ネットワーク上のサーバーにランサムウェア「EKANS(Snake)」が感染、サーバーに接続するPCにも拡散する事態となった他、北米・トルコ・インド・ブラジル等で工場が操業停止、また国内でも完成車の検査システムが一時停止したとのことです。

- その後同12日には、各拠点で11日までに復旧したことが発表されており、顧客の個人情報や開発技術などの機密情報の流出は確認されていないとしています(一方で、復旧にあたり多くのPCで安全のため初期化が行われ、一部データが消失したとのことです)。

AUS便りからの所感等

- 海外のセキュリティアナリストからは「今回の攻撃はテレワークに関連するものである可能性がある」「新型コロナウイルスのパンデミックは、オフィスの外から勤務する社員らを増加させたが、これによって企業ネットワークの脆弱性を突く攻撃も増加した」との指摘もあります。

- EKANSは2019年末から今年に入って確認された新種のランサムウェアで、石油・ガス・電力・製造などの業界で使われる産業用制御システムを強制停止させる機能を持つとされています。

- 一時期程騒がれることがなくなったとはいえ、ランサムウェアの脅威は依然として見過ごせないものとなっており、今回のように感染の発生時に数日で適切な対応がとれるよう、アンチウイルスやUTMによる対策のみならず、バックアップ等によるデータの保護を行う体制を整えておくことが大切です。

読賣新聞 オンライン

サイバー攻撃受けたホンダ、世界の工場復旧

2020/06/12 21:39

ホンダは１２日、サイバー攻撃で停止していた世界各地の工場が、全て復旧したことを明らかにした。顧客の個人情報や開発技術などの機密情報の流出は確認されていないという。

障害は８日午前に確認され、北米やトルコ、ブラジル、インドで工場を停止した。日本でも完成車の検査システムが不調になり、出荷を一時、見合わせた。社内ネットワークを通じてウイルスが拡散し、生産管理システムなどにも影響が及んだ。

外部からのサイバー攻撃が原因に挙がっており、パソコンなどを使用不能にさせ、復旧の見返りに金銭を要求する「ランサム（身代金）ウェア」と呼ばれるコンピューターウイルスが使われたとみられる。

●5月のフィッシング報告件数、15,000件に迫る勢い…対策協議会発表

https://www.antiphishing.jp/report/monthly/202005.html

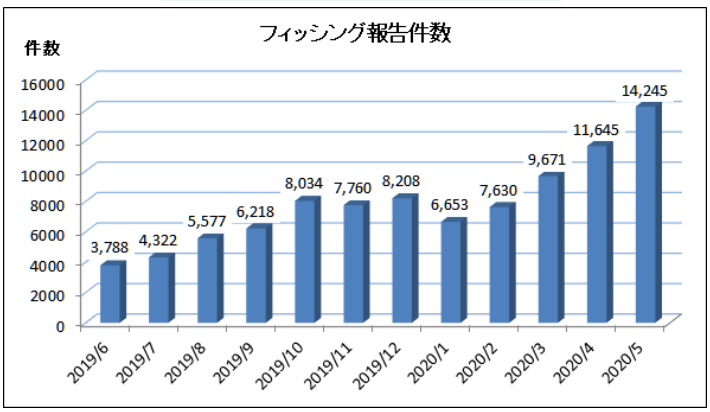
このニュースをザックリ言うと・・・

- 6月3日(日本時間)、フィッシング対策協議会より、5月に同協議会に寄せられたフィッシング報告状況が発表されました。
- 5月度の報告件数は14,245件で、初めて10,000件を突破した4月度(11,645件)より2,600件増加している他、フィッシングサイトのURL数も4,052件(4月度4,283件)と、4,000件以上を維持しています。
- 前月と同様、Amazon・Apple・LINE・楽天を騙るフィッシングメールについての報告が多く、Amazonを騙るものは4月の約1.5倍、3月の約2.1倍の報告数とのことです。

AUS便りからの所感

- 同協議会への月間報告件数は、2月度7,630件、3月度9,671件と、4月度まで約2,000件ずつの増加がみられていましたが、5月度はさらに勢いを増しており、6月度に15,000件を突破するのはほぼ確実とみられます。
- また、短縮URLサービスやメール配信サービスのトラッキング用URLを用い、短時間で誘導先のURLを変えることにより、アンチウイルスやブラウザーのアンチフィッシング機能を回避しているとされています。
- アンチフィッシング機能を回避して行われるフィッシングに引っ掛かることのないよう、不審なメールが届いたらネット上の情報を調査して確認する、利用しているサービスのサイトにはブックマークからアクセスする、等の多重防衛を日頃から行うことを推奨致します。

フィッシング対策協議会
Council of Anti-Phishing Japan



●Windows10の修正済み脆弱性の攻撃コード確認…パッチの確認を

https://www.us-cert.gov/ncas/current-activity/2020/06/05/unpatched-microsoft-systems-vulnerable-cve-2020-0796
https://www.jpcert.or.jp/wr/2020/wr202201.html#7

このニュースをザックリ言うと・・・

- 6月5日(現地時間)、米US-CERTより、3月に修正パッチが公開されたWindowsの脆弱性を悪用する攻撃コード(PoC)が確認されているとして注意喚起が出されています。
- 脆弱性(CVE-2020-0796)はWindows 10に実装されたSMBv3.1.1に存在、悪用によりホストを乗っ取られる可能性があるとされているもので、3月11日(日本時間)にパッチがリリースされています(AUS便り 2020/3/16号参照)。
- 6月10日にはJPCERT/CCからも、週間のトピックスの一つとして取り上げられ、パッチの適用あるいは回避策を実行しているか、対策状況を確認するよう呼び掛けられています。

AUS便りからの所感

- 通常SMBが使用するポート(TCPポート139, 445番等)にインターネット上から直接アクセス可能である可能性は低いですが、社内LAN上のPCにマルウェアが侵入し、それを踏み台として同一LAN上のPCやWindowsサーバーに感染が拡大するケースは十分に考えられます。
- Windows自体やアンチウイルスに備わっているパーソナルファイアウォール機能の活用、UTM等によるセグメントの分割も重要ですが、毎月のセキュリティアップデートを全てのPCにおいて確実に実行できていることが根本的な対策として不可欠です。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

【7】Microsoft SMBv3 の脆弱性 (CVE-2020-0796) への対策を

情報源

US-CERT Current Activity
Unpatched Microsoft Systems Vulnerable to CVE-2020-0796
https://www.us-cert.gov/ncas/current-activity/2020/06/05/unpatched-microsoft-systems-vulnerable-cve-2020-0796

概要

2020年6月5日、CISA (US-CERT) は 3月に公開された Microsoft SMBv3 の脆弱性 (CVE-2020-0796) について、本脆弱性を悪用可能な実証 (PoC) コードを新たに確認しており、セキュリティ更新プログラムが未適用のシステムが攻撃を受ける可能性があるとして、改めて注意を呼び掛けています。CISA は、ユーザに向けて、早急にセキュリティ更新プログラムを適用することや、必要な回避策を適用することを推奨しています。今一度対策状況をご確認ください。