— AUS（アルテミス・ユーザ・サポート）便り 2021/07/27号 —
https://www.artemis-jp.com

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。

●偽映像サイト、マルウェア、購入者等情報流出…オリンピック便乗攻撃相次ぐ

https://japan.zdnet.com/article/35174142/
https://blog.trendmicro.co.jp/archives/28308
https://mainichi.jp/articles/20210721/k00/00m/040/493000c
https://www.itmedia.co.jp/news/articles/2107/23/news035.html

このニュースをザックリ言うと･･･

- 7月23日(日本時間)に開会式が行われた「東京2020オリンピック」に便乗しての様々な攻撃・不正攻撃が確認されています。

- 同19日、トレンドマイクロ社より、オリンピック開会式等中継映像の配信サイトを騙り、先に進むためとして「ブラウザ通知」を許可するよう誘導、さらにブラウザ通知から不審な警告を表示し、偽のセキュリティ商品等を買わせようとする手口が多数確認されたとして、注意喚起が出されています。

- また同20日頃、「【至急】東京オリンピック開催に伴うサイバー攻撃等発生に関する被害報告について.exe」というファイル名のマルウェアが出回っているとして複数のセキュリティ関連会社から警告が出されています。

- この他同21日には、「五輪チケット購入者とボランティアのID・パスワード情報が流出した」との報道がありましたが、のち同23日、流出は10人分で、組織委員会のシステムからの流出ではないことが確認され、フィッシング等で奪取されたものとみなされています。

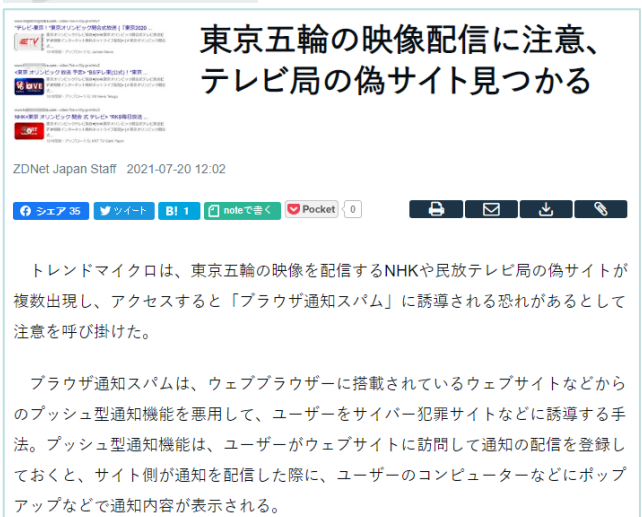
AUS便りからの所感等

- もはや言うまでもないことかもしれませんが、オリンピックやワールドカップといったスポーツイベントのみならず、世界的な注目を集める出来事には、それに便乗したサイバー攻撃が必ず付いて回るものと言えます。

- 7月21日には内閣官房内閣サイバーセキュリティセンター(NISC)より「夏季休暇等に伴うセキュリティ上の留意点について」と題した文書がリリースされており(https://www.nisc.go.jp/active/infra/pdf/summer20210721.pdf)、IPAやJPCERT/CCが通常行うような注意喚起に加え、ここでもオリンピックに関連するセキュリティリスクに考慮するよう書かれています。

- くれぐれもフィッシングやマルウェアの被害を受けないため、不審なメールやSMSの受信時には、公式機関の情報やソーシャルネットワーク等での報告を参照し、みだりにリンクをクリックしたり、添付ファイルを開いたりしないよう慎重な行動を心掛けてください。

ZDNet Japan



東京五輪の映像配信に注意、テレビ局の偽サイト見つかる

ZDNet Japan Staff　2021-07-20 12:02

シェア 35　ツイート　B! 1　noteで書く　Pocket　0

トレンドマイクロは、東京五輪の映像を配信するNHKや民放テレビ局の偽サイトが複数出現し、アクセスすると「ブラウザ通知スパム」に誘導される恐れがあるとして注意を呼び掛けた。

ブラウザ通知スパムは、ウェブブラウザーに搭載されているウェブサイトなどからのプッシュ型通知機能を悪用して、ユーザーをサイバー犯罪サイトなどに誘導する手法。プッシュ型通知機能は、ユーザーがウェブサイトに訪問して通知の配信を登録しておくと、サイト側が通知を配信した際に、ユーザーのコンピューターなどにポップアップなどで通知内容が表示される。

ブラウザー通知の「許可」ボタンをクリックさせる手口（出典：トレンドマイクロ）

●Windows 11プレビュー版の偽物出回る、不正ソフトインストールの恐れ…Kasperskyが注意喚起

https://www.itmedia.co.jp/news/articles/2107/26/news093.html
https://blog.kaspersky.co.jp/fake-windows-11-installers/31265/

このニュースをザックリ言うと・・・

- 7月23日(現地時間)、セキュリティベンダーのKaspersky社より、新OS「Windows 11」プレビュー版の偽のインストーラーが出回っているとして注意喚起が出されています。

- 偽のインストーラーを実行すると、ライセンス条項への同意を求める画面が表示されますが、これに同意することにより、アドウェア・トロイの木馬・パスワードを盗み出すソフトウェアおよび何らかの攻撃コード等様々な悪意のあるソフトウェアをダウンロードするとのことです。

- 同社では既に、Windows 11関連の手口に似た形で感染を試みる動きを、防御しているとのことです。

AUS便りからの所感

- 同社では、本物のWindows 11プレビュー版を入手するために、Windows Insider Programに登録し、マイクロソフトの公式サイトからダウンロードを行うよう呼び掛けています。

- Windows 11は2021年中にリリース予定とされ、新しいOSを体験するために、可能ならばInsider Programに登録せずに入手したいというユーザーを狙った攻撃と考えられます。

- OSはもちろんのこと、あらゆるソフトウェアの入手にあたっては、公式サイトや実績のある配布サイトからダウンロードを行い、アンチウイルスによるスキャンを行う等の防御を欠かさず行うようにしましょう。

ITmedia NEWS

Windows 11プレビュー版を装ったマルウェア多数 「Microsoft公式からの入手を」 Kasperskyが注意喚起

2021年07月26日 13時30分 公開　[荒岡瑛一郎，ITmedia]

印刷　181　Share　B! 2

Windows 11のプレビュー版はMicrosoft公式からの入手を――ロシアのKasperskyは7月23日、同社の公式ブログでこんな注意喚起を出した。Windows OSの新バージョン「Windows 11」を装ったマルウェアをインターネット上で確認しているためだ。

同社がWindows 11関連で既に確認したマルウェアは数百件。具体的には「トロイの木馬」やユーザーのパスワードを盗む「パスワードスティーラ」、PCの脆弱性を攻撃する「エクスプロイト」、無駄な広告を表示するアドウェアなどが含まれているという。

●TCPポート9530番宛パケット増加、狙いは古いルーターか…JPCERT/CC定点観測レポート

https://www.jpcert.or.jp/tsubame/report/report202104-06.html

このニュースをザックリ言うと・・・

- 7月26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4月～6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445番(Windowsサーバー・SMB)、次いでTCPポート23番(Telnet)、そして2021年1月～3月レポートにて急上昇していたUDPポート123番(NTP)等となっています。

- 注目された現象として、5月23日頃から日本国内を発信源としたTCPポート9530番宛パケットが一時的に多数観測、6月には海外複数国からも同様のパケットの発信が観測されており、ロジテック社製ブロードバンドルーターの、脆弱性を持つ古い機種が稼働していたとみられるとのことです。

AUS便りからの所感

- JPCERT/CCでは前述したTCPポート9530番宛パケットの送信元となるIPアドレスの管理者に通知を行い、これを経由してユーザーが新しいルーターを手配したとする事例を挙げています。

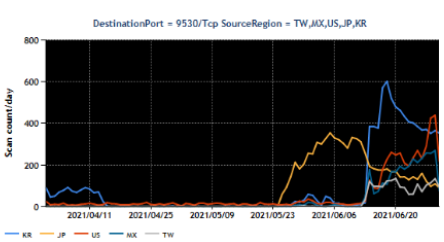
- 7月には親会社であるエレコム社製のルーターで脆弱性が報告されています(AUS便り 2021/07/13号参照)が、この例では比較的新しい年代の発売ながらファームウェアの更新が提供されないケースとなっています。

- 家庭ではもちろん、そして企業であればなおさら、使用・稼働しているルーター等ネットワーク機器全てについてその存在と機種を把握し、年数が経過したものや、脆弱性が報告され交換が呼び掛けられたものを、確実に交換できる体制を整えておくことが肝要です。

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

インターネット定点観測レポート（2021年 4～6月） 最終更新: 2021-07-26

2021年5月23日頃から日本を送信元としたPort9530/TCP宛のパケットが一時的に多数観測されました（図3）。6月14日頃からは韓国、米国、メキシコ、台湾などを送信元としたパケットが多く観測されました。日本を送信元としたパケットは期間中2番目に多く観測されました。



［図3：Port9530/TCP宛のパケット観測数の推移（送信元日本）］