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。

●「スーパーマリオ」二次創作ゲームにマイニングやPC情報窃取等を行うマルウェア入り偽インストーラー出回る

https://gigazine.net/news/20230626-trojanized-super-mario-malware/
https://blog.cyble.com/2023/06/23/trojanized-super-mario-game-installer-spreads-supremebot-malware/
https://www.bleepingcomputer.com/news/security/trojanized-super-mario-game-used-to-install-windows-malware/

このニュースをザックリ言うと･･･

- 6月24日(現地時間)、セキュリティ企業のCyble社より、Windows向けゲームソフトのインストーラーに第三者がトロイの木馬を紛れ込ませて配布するケースが確認されたとして注意喚起が出されています。

- 発表では、「スーパーマリオ」シリーズの非公式ゲームである「Super Mario 3: Mario Forever」のプログラムと一緒に、「java.exe」「atom.exe」という名前で仮想通貨のマイニングを行うボットが展開され、PC上で実行されるものが取り上げられています。

- さらにこのatom.exeが情報窃取マルウェア「Umbral Stealer」をインストールし、PCの画面やWebカメラ画像のキャプチャ、ブラウザーに保存されているパスワードやCookie、一部ネットサービスのアカウント情報等を奪取するとのことです。

AUS便りからの所感等

- 「Super Mario 3: Mario Forever」は2003年にリリースされたゲームで、問題となるインストーラーに含まれるゲームプログラム自体も不正なものではないとのことです。

- ゲームに限らず様々なアプリをインストールしようとしてこのような偽のインストーラーを掴まされるのは、往々にして検索エンジンでの検索結果の上位に出たサイトに安易にアクセスするケースが多くみられます。

- アンチウイルスやUTMによるダウンロードファイルのマルウェアチェック機能およびこれらやWebブラウザーに備わるアンチフィッシング機能を有効にするとともに、検索結果をより詳しく調査し、正規のインストーラーを入手するための情報収集を行うことが、偽インストーラーの回避に有用でしょう。

GIGAZINE

2023年06月26日 11時03分　セキュリティ

数百万回ダウンロードされたファンメイド版「スーパーマリオ」にPCを乗っ取るトロイの木馬が混入

任天堂の「スーパーマリオ」シリーズのクローンであるWindows向けゲーム「Super Mario 3: Mario Forever」のインストーラーに、仮想通貨を不正にマイニングさせたり、銀行口座などの情報を盗み出したりすることを目的としたトロイの木馬を紛れ込ませたものが発見されたと、セキュリティ企業のCybleが報告しました。

問題のインストーラーには3つの実行ファイルが格納されており、1つは正規のゲームのインストールする実行ファイル「super-mario-forever-v702e.exe」です。このゲームそのものに異常はないため、インストールすることで正常にプレイできるとのこと。

しかし、インストールと同時に「java.exe」と「atom.exe」も解凍され、隠しファイルとしてこっそり実行されます。ふたつのうち、「java.exe」は仮想通貨のMoneroをマイニングするツールで、「atom.exe」は被害者の端末をC&Cサーバーと接続し、マイニング設定を受信するものです。これにより、ゲームをインストールした人のPCではユーザーの同意や認識なしでのマイニングがバックグラウンドで秘密裏に実行されます。

●大学在学生約1万人分の個人情報流出…在学生宛メールに誤って添付

https://www.yomiuri.co.jp/national/20230630-OYT1T50299/
https://www.titech.ac.jp/news/2023/067083

このニュースをザックリ言うと･･･

- 6月30日(日本時間)、東京工業大学 学生支援センターより、在学生の個人情報が入ったファイルをメールで誤送信したと発表されました。

- 対象となる個人情報は、大学の発表では正規課程に在籍する学生約1万件の氏名および大学が発行したメールアドレス、また一部報道では在学状況・在留資格・国籍も含む計17項目とされています(住所・生年月日は含まれていないとのことです)。

- 6月28日に学生支援センターから全学生に進路相談会の案内メールを送信する際、誤って個人情報が入ったメールを添付していたのが原因としています。

AUS便りからの所感

- メール送信時のミスによる個人情報やメールアドレス流出の事案としては、大量のメールアドレスをBcc:に入力する運用を行っていたところに誤ってCc:の方に入力してしまうケースが近年に至るまで多く発生しています。

- 人間によるチェックに依存する運用はいつか破綻するものと心得て、メールサーバー側・メーラー側あるいはその間におけるUTM等で誤送信の可能性のあるケースを検知・遮断するといったシステムの導入を是非とも検討すべきでしょう。

- 例えばOutlookに無償で導入できるアドオンとして、誤送信防止のため様々な警告を出すものが存在します(AUS便り2022/05/24号参照)。

読賣新聞オンライン

東工大の全学生１万人分の個人情報、誤送信…間違えてファイルを添付


東京工業大学のキャンパス（読売ヘリから）

東京工業大の学生支援センターが６月、全学生約１万人分の個人情報が記載されたファイルを誤ってメールに添付し、ほぼ全ての学生に送信していたことがわかった。これまでに個人情報の流出による被害は確認されていないという。

大学関係者によると、ファイルの情報は在籍中の全学生（短期留学など除く）の氏名や性別、現況（在学、休学、留学）、メールアドレス、在留資格、国籍など１７項目で住所や生年月日、顔写真は含まれていない。

●CentOS 7サポート終了まで1年切る…後継バージョンめぐり一悶着も

https://xtech.nikkei.com/atcl/nxt/column/18/00989/062100120/

このニュースをザックリ言うと･･･

- 大手Linux OSディストリビューションの一つ「CentOS」バージョン7(以下・CentOS 7)について、2024年6月30日(現地時間)のサポート終了まで1年を切っています。

- CentOSはRedHat Enterprise Linux(RHEL)との互換性をうたう無償ディストリビューション(「RHEL互換OS」等と呼ばれる)でしたが、後継となる予定だったCentOS 8が大幅な前倒しとなる2021年12月でサポート終了(発表は2020年12月)しており、CentOS 7からより新しいバージョンへの移行にはディストリビューション自体の移行が必要となります。

- RHELバージョン8以降からの派生となる互換OSとしては、CentOS 8のサポート終了発表を受けて発表された「AlmaLinux」「Rocky Linux」や、他にも以前から存在するものとして「Oracle Linux」等があります。

AUS便りからの所感

- CentOSプロジェクトでは、CentOS 8以降の代わりかつRHEL 8以降の派生元となるプロジェクトとして、よりパッケージの更新頻度の高い「CentOS Stream」の提供を開始している一方、6月21日にRed Hat社より、RHEL派生OSに対するCentOS Streamのソースコード使用を実質禁止する規約更新を発表、Red Hat側とAlmaLinux・Rocky Linux側がそれぞれ意見を主張し合う事態となっています。

- CentOS StreamやRHELといった上流の更新に対する派生OSの追随やクオリティにどの程度影響するかは未知数ですが、前述した事態も考慮した上で、他のRHEL派生OSに移行するか、有償のRHELに移行するか、あるいは(パッケージ管理システム等の大きな違いはあれど)DebianやUbuntuへ移行するか等について、残り1年のサポート終了に対し今からでも慎重に検討し、サポート切れのバージョンはセキュリティ面の問題もあるため、くれぐれも使い続けないようにすることが重要です。

日経XTECH

CentOS Linux 7のサポートが2024年6月で終了、移行先の選択肢は

矢口 竜太郎　日経クロステック／日経コンピュータ

企業で多く使われている無償のLinuxディストリビューション「CentOS Linux 7（CentOS 7）」のコミュニティーサポートが2024年6月30日で終了する。サポートが終わるとセキュリティーパッチが提供されなくなり、重大な脆弱性が見つかった場合に対処できなくなる。直接的な後継製品はなく、利用企業は何らかの移行作業が求められる。