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。

●AndroidベースのTVボックスがトロイの木馬に感染…被害は200ヶ国、130万台に拡大か

https://gigazine.net/news/20240918-android-vo1d-malware-tv-streaming-boxes/
https://news.drweb.co.jp/show/?i=14900
https://www.bleepingcomputer.com/news/security/new-vo1d-malware-infects-13-million-android-streaming-boxes/

このニュースをザックリ言うと･･･

- 9月13日(日本時間)、アンチウイルス製品ベンダーのDoctor Web社より、AndroidベースのTVボックスがマルウェアに感染するケースが世界中で確認されているとして注意喚起が出されています。

- 「Android.Vo1d」と名付けられたマルウェアはいわゆるトロイの木馬型で、感染したデバイス上の一部システムファイルを上書きし、外部の指令サーバーから追加コンポーネントやAPKファイルをダウンロード、インストールするとしています。

- 同社の調査では、Android.Vo1dに感染したデバイスは全世界で約200ヶ国・約130万台に及ぶとされ、最も感染が多い国はブラジル(全体の28.0%)とのことです。

AUS便りからの所感等

- Doctor Web社では、感染の経路はまだ不明とし、OSの脆弱性を悪用してroot(管理者)権限を取得する中間マルウェアによる攻撃、もしくはroot権限を持つ非公式なファームウェアの使用による可能性を示唆しています。

- またIT系メディアBleeping Computerでは、Googleへの取材に対し、感染したのはGoogleのPlay Protectによる検査・認定を受けたAndroid TVではなく、Android Open Source Project(AOSP)を使用したデバイスであるとの回答を得たとしており、Androidベースを称するTVボックスの購入においても、Android TVのパートナーであることが提示されている(https://www.android.com/tv/)メーカーの製品を選ぶことが重要でしょう。

- Doctor Web社では同社のDr.Webアンチウイルス製品で今回のマルウェアと亜種の検知に対応しており、PCやスマートフォン同様、可能な限りセキュリティベンダー各社がAndroid・Android TV向けに提供するセキュリティアプリの導入を行うことを強く推奨致します。

GIGAZINE

2024年09月18日 08時00分　セキュリティ

約200カ国で130万台近いAndroidベースのTVボックスがマルウェアに感染していることが判明

世界197カ国の130万台近いAndroidベースのTVボックスが、「Android.Vo1d」と名付けられたマルウェアに感染していると、セキュリティ企業のDr.Webが報告しました。Android.Vo1dはシステムストレージ領域に自身のコンポーネントを配置し、バックドアを通じて追加のマルウェアをひそかにダウンロードする機能を備えているとのことです。

百万台を超えるAndroid TVボックスを襲うVo1d

https://news.drweb.co.jp/show/?i=14900

●転職大手、企業採用担当者情報が代理店から閲覧可能状態に

https://www.nikkei.com/article/DGXZQOUC170UT0X10C24A9000000/
https://www.persol-career.co.jp/newsroom/news/information/2024/20240917_1592/

このニュースをザックリ言うと･･･

－9月17日(日本時間)、転職サービス大手のパーソルキャリア社より、同社運営の「doda」を利用する法人の採用担当者の情報が代理店から閲覧可能にあったと発表されました。

－発表によれば、同社が保有する法人顧客情報のうち、採用担当者549,195人分の社名・会社住所・部署・役職・氏名・メールアドレスについて、代理店(およびその委託先)1,164社から閲覧できる状態になっていたとのことです。

－採用担当者が本来取引のない代理店から営業を受け、代理店側に当該担当者の情報を得た経緯を問合せたことで事象が発覚し、現在は改修により代理店等側から閲覧できないよう対策済みとのことです。

AUS便りからの所感

－代理店向けシステム開発時の仕様検討、プライバシー観点からの確認および検証が不十分であったため、社内基幹データベースで保有していた採用担当者情報が当該システムと連携されていたことが原因としています。

－システム利用者の各属性、および同じ属性内でも他の組織等に対し、互いの情報閲覧の可否を洗い出すとともに、各々設定が適切になっているか、ユーザーの属性毎でアクセス検証を行うことが必要です。

－Webサービスにおいては、ブラウザー上からのUIに従っての検証以外にも、攻撃者等がリクエストを改変して、本来アクセスできない属性の情報にアクセスされる可能性があることを鑑み、第三者機関によるセキュリティ診断を受けることも重要です。

● FreeBSDに致命的な脆弱性、PS5等にも影響？

https://jvndb.jvn.jp/ja/contents/2024/JVNDB-2024-007622.html
https://www.freebsd.org/security/advisories/FreeBSD-SA-24:14.umtx.asc
https://xexeq.jp/blogs/media/topics7996

このニュースをザックリ言うと･･･

－9月4日(現地時間)、UNIX-LikeなOS「FreeBSD」の開発元より、脆弱性「CVE-2024-43102」が確認されたとして注意喚起が出されています。

－脆弱性はネットワークを通じて容易に悪用可能とされ、OS上で任意のコード実行が可能になり、FreeBSDを利用しているサーバー機器などの乗っ取りが可能となる恐れがあります。

－少なくともFreeBSD 13系および14系が脆弱性の影響を受けるとされ、13.3-RELEASE-p6・14.0-RELEASE-p10および14.1-RELEASE-p4で修正されています。

AUS便りからの所感

－FreeBSDはいわゆる「PC-UNIX」にカテゴライズされるx86アーキテクチャ向けOSの一つで、一時期はLinuxと並ぶ人気を誇り、今日においてネットワークサーバーでLinuxが多く利用されている中、Netflixが配信用サーバーにFreeBSDを独自にカスタマイズして利用している事例等が知られています。

－「PlayStation 4(PS4)」「PlayStation 5(PS5)」のようなゲーム機のファームウェアにも使用されており、PS5も今回の脆弱性の影響を受けるとされていた一方、2023年にリリースされたPS5 Firmware 8.00では影響を受けないとのことです。

－サポート終了しているFreeBSD 12系以前について影響を受けないとは確認されておらず、もしそういったバージョンを使い続けている場合は速やかに最新バージョンへアップグレードすること、以後も毎回のアップデートに対し可能な限り早く適用できる体制を整えていることが重要です。