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。

●人気ゲーム「8番出口」開発者がスマホ等向けの偽アプリに注意喚起…本物は現在PC向けのみ

https://game.watch.impress.co.jp/docs/news/1553611.html
https://twitter.com/NOTOKEKE/status/1733475921590677872

このニュースをザックリ言うと･･･

- 12月9日(日本時間)、人気インディーゲーム「8番出口」の開発者コタケノトケケ氏より、同ゲームの偽アプリが確認されたとしてTwitter(現:X)上で注意喚起が出されています。

- 対象とみられるアプリは、Apple公式のApp StoreにてiPhone・iPad・Mac向けの無料アプリとして「8番出口 - 通路からの脱出」というタイトルで公開されており、スクリーンショットとして本物の画像を不正に流用している模様です。

- コタケノトケケ氏は現在Steamで PC向けに提供されているものだけが本物であり、App Storeで公開されているものは詐欺アプリであるとして注意するよう呼び掛けています。

AUS便りからの所感等

- 偽の「8番出口」はプレイ時に多数のスキップできない広告が表示され、肝心のゲーム内容は本物と全く似ていないものとの報告がネット上で挙がっています。

- 10月にはやはり人気となっている「スイカゲーム」の偽アプリがApp Storeで確認されており(AUS便り2023/10/11号参照)、その後削除された模様ですが、現在は別のアプリが公開されています。

- App StoreでもGoogle公式のPlayストアでも、広告を大量に表示するのみならず、場合によってはデバイス上の情報を奪取する等の不正行為を行うアプリがアップロードされるケースが度々報告されており、インストールにあたっては必ずアプリストアやソーシャルネット等での評価・評判を参考とし、デバイス上の権限の利用が不自然に要求された場合にはその場で許可せず削除する等、慎重な行動をとるよう心掛けましょう。

Impress Watch

ホラーゲーム「8番出口」偽物がApp Storeに出現。制作者が注意喚起

製品版はSteamにてPC向けに配信中

岩瀬賢斗　2023年12月11日 16:14

ゲーム開発者のコタケノトケケ氏は12月9日、ウォーキングシミュレーター「8番出口」の偽物に関する注意喚起を行なった。

「8番出口」はSteamにて配信されているPC用タイトル。駅の地下道をイメージしたウォーキングシミュレーターで、プレーヤーは周囲をよく観察しながら8番出口を目指すことになる。作中にはホラー要素なども存在し、ゲーム実況などを通じて話題となっている。

PC向けに配信されている作品だが、Appleのアプリ配信プラットフォーム「App Store」では本作とよく似たアプリが存在している。タイトルは「8番出口-通路からの脱出」となっており、ストアページに掲載されているスクリーンショットも同じものと思われる画像が使われている。

●11月フィッシング報告件数は72,456件、大幅減少

https://www.antiphishing.jp/report/monthly/202311.html

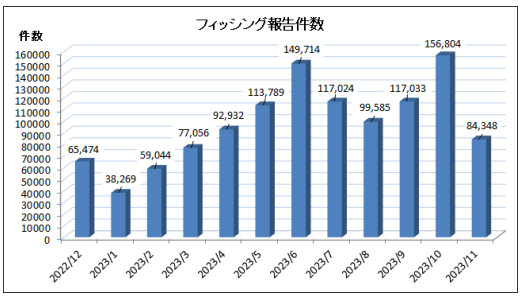
このニュースをザックリ言うと・・・

- 12月12日(日本時間)、フィッシング対策協議会より、11月に寄せられたフィッシング報告状況が発表されました。
- 11月度の報告件数は72,456件で、過去最高を更新した10月度(https://www.antiphishing.jp/report/monthly/202310.html)の156,804件から72,456件減少しています。
- フィッシングサイトのURL件数は10,678件で10月度(13,507件)から2,829件減少、悪用されたブランド件数も73件で10月度(78件)から5件減少となっています。
- 最も多く報告されたのはAmazonを騙るフィッシングで報告数全体に対する約26.7%、次いでそれぞれ1万件超だったETC利用照会サービス、マイナポイント事務局、三井住友カードと合わせて約74.4%、さらに1,000件以上報告された12ブランドまで含めると約91.4%を占めたとのことです。

AUS便りからの所感

- 大幅な減少の主な理由として、10月度にそれぞれ5万件の報告があったAmazon・ETC利用照会サービスを騙るフィッシングがいずれも3万件以上減少したことを挙げていますが、ETCやマイナポイントのフィッシングサイトに情報を入力してしまったという相談は依然として多く届いているとしています。
- 2022年9月の102,025件から2023年1月の38,269件まで減少した後に6月まで増加に転じていた一方、2021年は8月の53,177件から11月の48,461件まで微減が続いた後12月に63,159件と急増した実績があり、今月以降どこで件数の再度急増があるかは十分に予測しづらい状況となっています。
- 同協議会では引き続き「事業者のみなさまへ」において、特にメールサービスやオンラインサービスを提供する事業者に対しDMARC等によるドメイン名の保護を呼び掛けており、それ以外の企業等でも、自社ドメイン名でなりすましメールが届いた取引先を保護できるよう、導入を進める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



●TCPポート23番宛パケットを依然多く検知、Miraiによる通信か… NICTER発表

https://twitter.com/nicter_jp/status/1731577147658207379
https://twitter.com/nicter_jp/status/1734395665978097813
https://www.nicter.jp/

このニュースをザックリ言うと・・・

- 12月4日(日本時間)、情報通信研究機構(NICT)サイバーセキュリティ研究所が運営する「NICTER」プロジェクトより、10月にダークネットで観測されたパケットの調査結果がTwitter(現:X)上で発表されました。
- 最も多く観測されたのはTelnetサービスで用いられるTCPポート23番宛のもので、次いで同22番(SSH)・80番(HTTP)・8080番(HTTP・特殊なサーバー等)・3389番(リモートデスクトップ)等トップ30までが発表されています。
- 発表では1位のTCPポート23番宛パケットについて、9月から引き続き、ボット「Mirai」に感染したホストからのものとしています。

AUS便りからの所感

- 同12日には11月のパケット観測結果が発表され、23番・22番・8080番・80番・8728番(特定メーカールーターが使用)が上位に挙がっています。
- NICTERのWebサイトに挙がっている四半期毎の観測統計(最新は7～9月分)等でも、最も多く検出されているのはMiraiによるとみられるTCPポート23番宛パケットとされ、この傾向は何年もの間続いています。
- サーバー・クライアントPCのみならず、社内に設置されているネットワーク機器やIoT機器全てを確実に管理下に置き、意図してインターネットに直接接続しているかどうか、また外部から意図していないポートにアクセスされないか等の確認と対策をとることが重要です。


NICTER 解析チーム
@nicter_jp

遅くなりましたが，2023年10月にNICTER ダークネットで観測した全てのパケットを宛先ポート番号別に集計したTop 30 です．23/TCP宛では9月から引き続きMiraiに感染したホストからのパケットが多く観測されました．

今月	前月	宛先ポート番号						
1 (→)	1	23/TCP	11 (↑)	16	2222/TCP	21 (↑)	22	8081/TCP
2 (↑)	3	22/TCP	12 (↓)	7	5060/UDP	22 (↑)	26	8888/TCP
3 (↓)	2	80/TCP	13 (↑)	14	5555/TCP	23 (↓)	19	123/UDP
4 (→)	4	8080/TCP	14 (↓)	13	8088/TCP	24 (↑)	27	1433/TCP
5 (→)	5	3389/TCP	15 (↓)	11	6379/TCP	25 (↑)	93	7001/TCP
6 (→)	6	443/TCP	16 (↓)	15	53/UDP	26 (↓)	25	1900/UDP
7 (↑)	8	8443/TCP	17 (↑)	20	3128/TCP	27 (↑)	35	5432/TCP
8 (↑)	17	8728/TCP	18 (→)	18	2375/TCP	28 (↑)	39	1080/TCP
9 (↑)	12	445/TCP	19 (↑)	62	37215/TCP	29 (↑)	–	50802/TCP
10 (↑)	21	81/TCP	20 (↓)	9	27610/UDP	30 (↑)	32	9200/TCP

午後4:32 · 2023年12月4日 · **6,817** 件の表示