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。

●令和6年能登半島地震便乗…Yahoo!の募金かたる詐欺に注意喚起

https://notice.yahoo.co.jp/donation/archives/20240103-a.html
https://security.yahoo.co.jp/news/0033.html
https://www.itmedia.co.jp/news/articles/2401/05/news084.html
https://www.caa.go.jp/disaster/caution_001

このニュースをザックリ言うと･･･

- 1月3日(日本時間)、LINEヤフー株式会社(以下・LY社)より、同社が「令和6年能登半島地震」に関する寄付金を募っている「Yahoo!ネット募金」「Yahoo!基金」を騙る偽サイトが確認されたとして注意喚起が出されています。

- 同社では、フィッシングサイトに誘導しようとしたり、個人情報を入力させて返信させようとしたりする偽メールや不正メッセージに十分注意し、受信しても開かずに削除するよう呼び掛けています。

- また、フィッシング詐欺かどうかの判断が難しい場合、メール内のリンクはクリックせず、予め登録したブックマーク等からアクセスするよう推奨しています。

- この他、消費者庁等からも、インターネット上に限らない義援金詐欺について、同様の注意喚起が出されています。

AUS便りからの所感等

- 地震や台風・豪雨による震災時には、必ずと言っていいほど便乗してのフィッシング詐欺やマルウェア感染を狙った攻撃等が発生します。

- 災害が予測される際に送信される「エリアメール」についても、これを騙り不審なサイトに誘導するSMSが確認された事例があります(AUS便り 2018/11/5号参照。本物はURLが記載されない等の特徴があります)。

- 不審なメールの受信やフィッシングサイトへの誘導およびマルウェアのダウンロード等を防止するため、アンチウイルスやブラウザー・メーラー・UTMのアンチフィッシング機能を確実に有効にすることを推奨致します。

- LY社では正規のサイトへのアクセス方法としてブックマーク以外にも検索サイトの利用も推奨していますが、検索結果においても不正な広告からフィッシングサイトに誘導されるケースが多発していることに留意が必要です。

YAHOO! JAPAN

【重要】Yahoo!ネット募金やYahoo!基金 をかたるフィッシングサイト（偽サイト）、不正メールにご注意ください

[お知らせ] 2024年1月3日

いつもYahoo!ネット募金をご利用いただき、誠にありがとうございます。

Yahoo!ネット募金やYahoo!基金の名称やロゴを悪用し、令和6年能登半島地震の寄付金を募るフィッシングサイト（偽サイト）が確認されています。フィッシングサイトに誘導しようとしたり、個人情報を入力させて返信させようとしたりする偽メールや不正メッセージに十分ご注意ください。

不審なメールやメッセージを受信した場合には、開かずに削除してください。
フィッシング詐欺かどうかの判断が難しい場合には、メール内のリンクはクリックせず、普段使っているブラウザーの「お気に入り（ブックマーク）」や検索サイトから目的のウェブサイトへアクセスするようお願いします。

● AndroidのPINコード・パスワードを盗み出すマルウェア「Chameleon」…「制限付き設定」解除に誘導

https://gigazine.net/news/20231225-android-chameleon-malware/
https://news.mynavi.jp/techplus/article/20231222-2847352/
https://www.threatfabric.com/blogs/android-banking-trojan-chameleon-is-back-in-action
https://news.mynavi.jp/techplus/article/20231107-2812940/

このニュースをザックリ言うと･･･

- 12月21日(現地時間)、オランダのセキュリティ企業ThreatFabric社より、Androidに侵入するマルウェア「Chameleon」について注意喚起が出されています。

- ChameleonはChromeブラウザーのインストーラーに偽装して侵入し、オンラインバンキングアプリの機密情報等をターゲットにするとのことです。

- また、Androidで不審なアプリの実行をブロックする「制限付き設定」を解除するよう誘導、画面ロックを生体認証(指紋・顔認証等)からPINコード入力によるものに変更し、入力されたPINコードやパスワードを奪取するという手口をとる模様です。

AUS便りからの所感

- 「制限付き設定」は2022年2月リリースのAndroid 13から導入され、有害とみられるアプリについて警告を表示して実行をブロックするものですが、ThreatFabric社は2023年11月の時点で、設定の解除へ誘導するマルウェアが確認されたとして注意喚起を行っています。

- Google公式のPlayストア以外からapkファイルのダウンロード・インストールしたアプリの実行時にこの制限付き設定がはたらく場合があり、その際には既にインストールの段階で別途設定の変更を行っていることが多いとみられ、制限付き設定の解除も安易に行ってしまう恐れがあります。

- Playストアからインストールするアプリでも同様ですが、インストール時や実行時に不必要に権限や設定変更を要求してくるアプリに対しては安易に従わず、アプリストアのレビューやSNS上での報告がないか確認し、普段から信頼のおける必要最低限のアプリのインストールに留めるよう心掛けましょう。

● Microsoftの月例セキュリティアップデートリリース、必ず適用を

https://www.jpcert.or.jp/at/2024/at240001.html
https://www.ipa.go.jp/security/security-alert/2023/0110-ms.html
https://msrc.microsoft.com/blog/2024/01/202401-security-update/

このニュースをザックリ言うと･･･

- 1月10日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

- Windowsの最新バージョンはWindows 10 22H2 KB5034122(ビルド 19045.3930)および11 23H2 KB5034123(ビルド 22631.3007)となります。

- JPCERT/CC・IPA等からも、必ずアップデートを適用するよう呼び掛けられています。

AUS便りからの所感

- 同社のEdgeブラウザーについては、これに先駆けて同6日にバージョン120.0.2210.121がリリースされていますが、その後Google Chromeにおいて同10日にセキュリティアップデートとなる120.0.6099.216がリリースされており、Edgeでも同様にアップデートがあるとみられます。

- 同日にはAdobeからも月例のセキュリティアップデートがリリースされている他、来週の同17日にはOracle社からJava等についての3ヶ月に一度のアップデートが行われる予定です。

- 今回修正された脆弱性を悪用する「ゼロデイ攻撃」は確認されなかったとのことですが、今後発生し得る新たな攻撃に備え、確実にアップデートを適用すること、それまでに発生する攻撃に対しアンチウイルス・UTM等による防御策をとることが肝要です。