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。

●LINEヤフーより個人情報約44万件流出…海外委託会社PCがマルウェア感染か

https://www.nikkei.com/article/DGXZQOUC270BU0X21C23A1000000/
https://www.lycorp.co.jp/ja/news/announcements/001002/

このニュースをザックリ言うと･･･

- 11月27日(日本時間)、LINEおよびYahoo! JAPANを運営するLINEヤフー株式会社(以下・LY社)より、同社サービスユーザー・取引先及び従業者等の個人情報合わせて最大約44万件が不正アクセスにより流出したと発表されました。

- 発表によれば、被害を受けた情報の内訳(いずれも推測値を含む最大数)は、LINE各サービスのユーザーに関する個人情報302,569件(うち日本ユーザー129,894件)、取引先等に関する個人情報86,105件、従業者等に関する個人情報51,353件とされています。

- 同社の韓国における関係会社であるNAVER Cloud社の委託先企業においてPCがマルウェアに感染し、そこを踏み台にLY社のサーバーへ不正アクセスが行われたとされています。

AUS便りからの所感等

- 不正アクセスは10月9日から発生していたとされ、同17日に発覚、同27日までに調査を行った後、委託先企業からのアクセス遮断を行ったとされています。

- 被害を受けた情報は殆どがLINE側とみられますが、奇しくもYahoo!JAPAN ユーザーに対し、10月中にLINEとの連携に同意するよう求めていた(同意しない場合11月以降LINEが利用できなくなるとしていた)中で不正アクセスが発生したことが、ユーザーの不信を招く結果となっているようです。

- ともあれ、委託先企業といったレベルからユーザー・取引先等の情報に安易にアクセスされないよう、サーバー側でアクセス権限の厳密な設定や詳細なログの取得、不審なアクセスに対する速やかな検知・遮断が行えるような体制を整え、クライアント側に対してもアンチウイルスやUTM等の導入により、マルウェアの感染のみならず万が一の感染時の不審な行動を抑制できる環境とさせることが理想です。

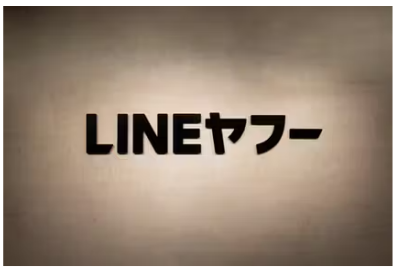
日本経済新聞

LINEヤフー、個人情報流出発表　ネイバー経由で44万件か

ネット・IT　＋フォローする
2023年11月27日 12:00 (2023年11月27日 20:47更新)

保存

Think! 多様な観点からニュースを考える　佐藤一郎さんの投稿



LINEヤフーは過去にも個人情報の取り扱いを巡り問題が発覚している

LINEヤフーは27日、同社のサーバーが第三者から攻撃され、LINEアプリの利用者情報など約44万件が流出した可能性があると発表した。大株主である韓国ネット大手ネイバーと一部システムを共通化していたことが一因だ。過去にもLINEの利用者情報を中国の関連会社が閲覧できた問題が起きており、情報管理体制が改めて問われる。

今回流出した恐れのある44万件の個人情報のうち約30万件は利用者に関するものという。対話アプリ「LINE」の利用者は9600万人に上る。流出した情報の中には解析すればアプリのプロフィル情報にある氏名などを第三者が閲覧できる可能性があるものもある。利用者の性別やLINEスタンプの購入履歴なども流出したもようだ。

●偽のブラウザーアップデートでマルウェア感染させる攻撃に注意喚起、Macを狙うものも

https://news.mynavi.jp/techplus/article/20231122-2824884/
https://www.malwarebytes.com/blog/threat-intelligence/2023/11/atomic-stealer-distributed-to-mac-users-via-fake-browser-updates
https://www.daj.jp/security_reports/35/
https://www.daj.jp/security_reports/36/

このニュースをザックリ言うと･･･

- Webブラウザーのアップデートを騙りマルウェアへ感染するよう誘導する攻撃について、セキュリティベンダー各社より相次いで注意喚起が出されています。

- 国内セキュリティベンダーのデジタルアーツ社より、Webサイトの改ざんで埋め込まれたスクリプトでGoogle Chromeブラウザーの偽のアップデートページを表示する事例として、11月14日(日本時間)に「SocGholish(FAKEUPDATES)」、同28日に「ClearFake」についての調査結果がそれぞれ発表されています。

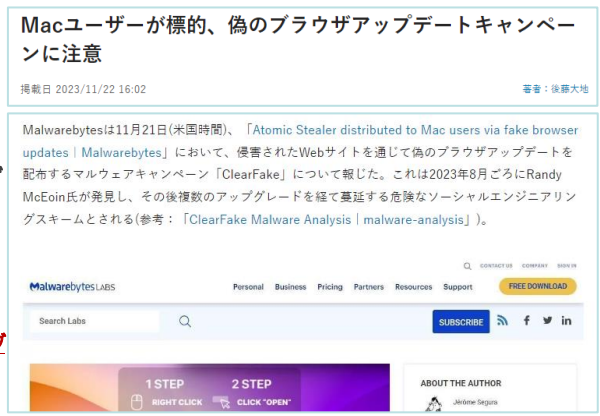
- また11月21日(現地時間)には、Malwarebytes社より、ClearFakeにおいてMacに感染するマルウェア「Atomic Stealer(AMOS)」が用いられる事例が発表されています。

AUS便りからの所感

- Malwarebytes社では9月にも、Mac向けソフトウェアの偽サイトからAMOSへ感染させる事例について報告しています(AUS便り 2023/09/27号参照)。

- またデジタルアーツ社では、偽のブラウザーアップデートによる攻撃キャンペーンとして上記のSocGholish(FAKEUPDATES)・ClearFakeを含め5種類を挙げていますが、いずれも2023年から攻撃が確認されているとしています。

- ソフトウェアをインストール・アップデートしようと考えていないところにいきなり表示されるようなサイトに安易にアクセスせず、ソフトウェア自身に自動更新機能やアップデートの有無を確認する機能があるものについては必ずそれを利用すること、またサーチエンジンでの検索結果に偽サイトが広告として表示される事例も度々報告されていますので、アンチウイルスおよびブラウザーのアンチフィッシング機能は必ず有効化し、信頼できる情報源からのリンクを辿る等の自衛策をとることが重要です。



●11月はWordPressの19のプラグインに脆弱性…Sucuri社発表

https://blog.sucuri.net/2023/11/wordpress-vulnerability-patch-roundup-november-2023.html
https://news.mynavi.jp/techplus/article/20231128-2827247/

このニュースをザックリ言うと･･･

- 11月24日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、11月に報告された19のWordPressプラグインに存在する脆弱性のまとめ記事が発表されました。

- クロスサイトスクリプティング(XSS)の脆弱性が11のプラグインで報告されており、特に「Elementor」におけるものが今回発表分では最も危険度が高い「High」の評価とされています。

AUS便りからの所感

- WordPressにおいては、提供されるプラグインも、またそれらで報告される脆弱性も数多く存在しており、Sucuri社による月毎のまとめでは、毎月20件台の報告がまとめられています(ただし別の情報源ではここでまとめられていない脆弱性も報告されており、調査の際は複数の情報源をあたることが重要です)。

- WordPress本体においても10月に6.3.2がリリースされるなど、不定期に更新されることがあり、本体・プラグインともインストールした状態のままで放置するようなことは決してせず最新に保つよう努めること、加えてセキュリティを強化する何らかのプラグインを導入し、さらに並行して(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFやIDS・IPSの導入についても検討するのが良いでしょう。