— AUS（アルテミス・ユーザ・サポート）便り 2018/01/29号 —
https://www.artemis-jp.com

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などが監視されるマルウェア「Skygofree」が見つかる、通信速度改善のシステムアップデートを装う

https://internet.watch.impress.co.jp/docs/news/1102139.html
https://blog.kaspersky.co.jp/skygofree-smart-trojan/19255/
https://blogs.mcafee.jp/line-android-spyware-skygofee

このニュースをザックリ言うと・・・

- 1月16日（現地時間）、セキュリティベンダーのカスペルスキー社より、Androidに感染するトロイの木馬型マルウェア「Skygofree」について警告が出されています。

- 警告によれば、Skygofreeは大手モバイル通信事業者の偽サイトから、「モバイルのインターネット通信速度を改善する」というAndroidのシステムアップデートに偽装して拡散し、インストールしたスマートフォン・タブレット等において「位置の追跡」「周囲の会話等の録音」「フロントカメラでのユーザの顔写真撮影」「メッセージアプリ(LINE・Facebook・WhatsApp等)のメッセージを傍受」あるいは「攻撃者が用意するWi-Fiネットワークに密かに接続させる」等を行うとされています。

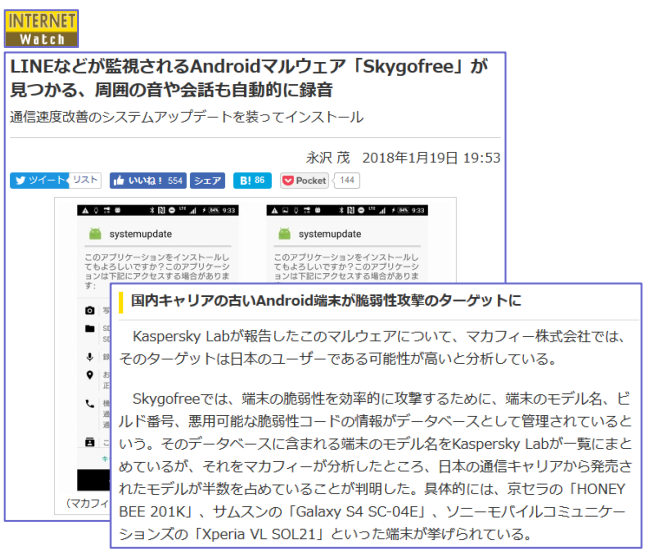
- 同社ではSkygofreeの存在を2014年から確認しており、監視ソリューションを提供するイタリアのIT企業が開発したものと推測しています。

- 同様にSkygofreeについて警告しているセキュリティベンダーのマカフィー社では、日本の通信キャリアから発売された古い機種のスマートフォンを狙う、あるいは世界的にはシェアが低いLINEを監視対象としていることから、特に日本国内のユーザを狙って拡散された可能性が高いと指摘しています。

AUS便りからの所感等

- 現時点でSkygofreeの拡散を目的とした日本の通信キャリアの偽ページ等は確認されていない模様ですが、今後日本語の偽サイトを攻撃者が用意し、例えばCPUの脆弱性の修正と偽る等して拡散を図る可能性は決して否定できません。

- 警告を出している両社とも、「アプリやシステムアップデートはGoogle Playといった公式ストアからインストールし、疑わしいアプリ等はダウンロードしない」「信頼できるアンチウイルス等のセキュリティアプリをインストールする」よう呼び掛けており、また外部で利用する場合でも、UTMによるVPNを経由してインターネットに接続した場合に不正なサイトへのアクセスを遮断する機能があれば、それを利用するのが良いでしょう。



●定番圧縮ソフト「Lhaplus」に脆弱性、2017年5月リリースの最新バージョンで修正済み

https://twitter.com/nisc_forecast/status/953494578979422208

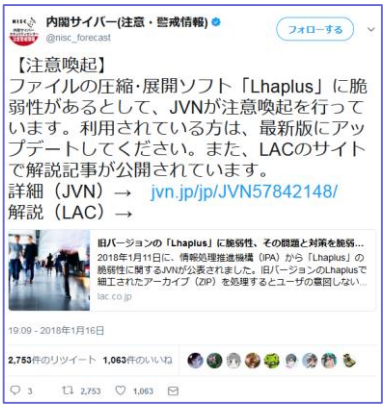
このニュースをザックリ言うと・・・

- 1月11日（日本時間）、IPAとJPCERT/CCが運営する脆弱性対策情報データベース「JVN」において、定番圧縮・展開ソフトウェア「Lhaplus」の古いバージョンに脆弱性が存在すると発表されました。

- 同16日には内閣サイバーセキュリティセンター（NISC）がTwitter上で注意喚起を行っている他、脆弱性を報告した国内大手セキュリティベンダーのラック社の技術者からも脆弱性について解説されています。

- 脆弱性はLhaplusのバージョン1.73以前に存在するもので、細工されたZIPファイルを展開することにより、本来とは異なる内容がファイルのコンテンツとして展開される可能性がありますが、2017年5月にリリースされた1.74で修正されており、最新バージョンへのアップデートが推奨されています。

AUS便りからの所感等



- Lhaplusは国内で人気が高いソフトである一方で、脆弱性をはらんでいる古いバージョンがインストールされているケースが多いことから、iTunesやJavaと並び危険度が高いソフトと見なす調査結果もありました（AUS便り 2017/04/03号参照）。

- 上記の調査の時点では最新バージョンのリリースから2年たっている状態でしたが、今回も1年前にリリースされていた最新バージョンへのアップデートが行われていないケースが多々あると考えられたため、注意喚起につながったものと考えられます。

- よほどの事情がない限りは、修正バージョンへのアップデートが脆弱性への攻撃を回避するための根本的な対策であると心得た上で、アップデート等の対策を行っている間に攻撃を受ける可能性を低減するために、アンチウイルスやUTMによる防御を加えることが重要です。

●NTTデータ、社内システムが一時「WannaCry 2.0」亜種に感染…現在は駆除完了

http://itpro.nikkeibp.co.jp/atcl/news/17/012202996/

このニュースをザックリ言うと・・・

- 1月22日（日本時間）、NTTデータ社より、1月5日以降、同社社内システムがランサムウェアに感染していたことが発表されました。

- 発表では、感染したランサムウェアは「WannaCry 2.0」の亜種とされ、社内ポータルや事務用PCをつなぐイントラネット環境の他、社内の開発環境を経由して顧客1社にも感染していたとのことです。

- 外部持ち出し用PCを社内ネットワークに接続した際に感染が広がったとされていますが、データの暗号化や情報流出を引き起こすものではなかったとされ、22日までに社内からの完全駆除を行ったとしています。

AUS便りからの所感等

- 同社を狙った標的型攻撃であったかは不明ですが、大手IT企業でも何らかの隙にチェックがすり抜けられてマルウェアが侵入する事態は起こりうるものであり、またマルウェアは組織の大小をいちいち考慮するものではなく無差別に感染拡散し得るもので、決して対岸の火事としてはいけないと改めて心得るべきでしょう。

- 同社ではネットワークの遮断、端末へのセキュリティパッチの適用、フルスキャンの実施を行い、ホームページや同社からの送信メールを介してインターネットを通じて被害が拡大することがないことを確認するなど、事後の対策体制は十分に整っていたことにより、外部への大規模な拡散等を抑え込むことに繋がりました。

- 今後侵入経路や対策過程について詳細が発表される可能性があり、各社にとってマルウェア感染からの防御対策を行う一助になることを期待したいものです。