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に不正ログイン…被害者数は4,000人超、乗っ取りや二次被害の可能性も

https://www.itmedia.co.jp/news/articles/2002/27/news075.html
https://linecorp.com/ja/security/article/251

このニュースをザックリ言うと･･･

- 2月26日(日本時間)、メッセージアプリ「LINE」を運営するLINE社より、2月にLINEアカウント4,225件が不正ログインの被害を受け、意図しないメッセージやタイムライン投稿が確認されているとして注意喚起が出されています。

- 送信された投稿には、購買誘導のスパムの他、LINEアカウントの乗っ取りを目的としたフィッシングサイトへのURLが含まれているとのことです。

- 同社では不正ログインが確認されたユーザーに対しパスワードの変更を依頼、あるいは強制リセットを行っているとしています。

AUS便りからの所感等

- メールサービスへの不正ログインによるスパムの大量送信への悪用事例は最近のAUS便りでも度々取り上げていますが、LINEアカウントの乗っ取りはより身近な脅威である場合が多く、友人に対し偽のメッセージを送信されることにより、連鎖的な被害をもたらす恐れが十分に考えられます。

- LINE社から直接連絡を行ったのは実際に同社側で不正ログインが確認できたユーザーに留まっているとのことで、連絡がなかったユーザーにおいても各自同社からの発表に目を通し、不正なメッセージ送信等の痕跡がないか確認する等の対応を行うことを強く推奨致します。

- 不正ログインに成功したアカウントについては、メールアドレスとパスワードがいわゆる「リスト型攻撃」のためのリストに登録され、他のサービスについても同様のアカウント情報でログイン試行が行われる恐れがありますので、万が一同じパスワードを使用しているのであれば、LINEおよびそれらのサービスそれぞれについて必ず別々の推測されにくいパスワードに変更してください。

LINE

LINEへの不正ログインに対する注意喚起

2020.02.26

---

1. 概要

2020年2月、LINEのアカウントに対して複数の不正ログインの試みが発生し、約4千名を超えるLINEアカウントが不正ログインの被害を受け、ユーザーの意図に反するメッセージやタイムライン投稿が行われていることを確認しております。

ユーザーの皆さまからの通報内容をもとに調査したところ、これらのメッセージ及びタイムライン投稿の内容は、購買誘導をするためのスパムの他、LINEのアカウントの恒久的な乗っ取りを目的としたフィッシング詐欺のためのURLが含まれておりました。

当社では引き続き、被害の拡大防止のための対応を行っておりますが、現在、LINEの機能やメールを通じたフィッシング行為が増加しており、被害を受けた場合には、侵害されたアカウントを通じた二次被害が発生する状況となっております。

友だちからのメッセージであっても、投稿中の不審なリンクは決して開かず、LINEアカウントのパスワード確認を求めるメッセージには応じないようにしてください。

本記事では、利用者への注意喚起を目的として、被害状況についての公表及び、被害に遭われた際の対応方法についてご案内いたします。

●日本国内を狙う新しいマルウェア「LODEINFO」、JPCERT/CCが警告

https://internet.watch.impress.co.jp/docs/news/1236585.html
https://blogs.jpcert.or.jp/ja/2020/02/LODEINFO.html

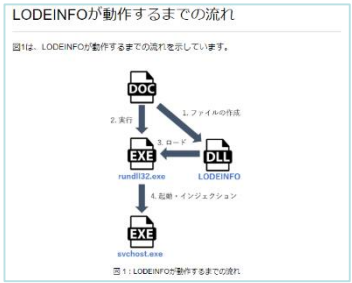
このニュースをザックリ言うと・・・

- 2月20日(日本時間)、JPCERT/CCより、昨年12月頃から日本国内の組織を狙い、これまで確認されていなかった新種のマルウェア「LODEINFO」が添付された標的型攻撃メールが送信されるケースがあったとして注意喚起が出されています。

- 注意喚起によれば、LODEINFOはメールに添付されたWord文書のマクロを有効にすることによってPC上に作成され、外部の指令サーバーとHTTP通信を行うとのことです。

- そして、受信した命令に応じてシェルコードの実行、ファイルのアップロード／ダウンロード、プロセスの停止、ファイル一覧の送信などを実行する機能を備えていたとされています。

日本国内の組織を狙ったマルウエアLODEINFO



AUS便りからの所感

- 日本国内を狙った攻撃が確認されているマルウェアとしては昨年10月以降に大規模な攻撃が確認された「Emotet」が挙げられ、こちらもWord文書のマクロを悪用して感染する形をとっています。

- JPCERT/CCでは、コード解析の結果からLODEINFOが未だ開発途中の段階にあると推測しており、EmotetがWebサイト閲覧で感染するよう仕込まれる等、感染経路を刻々と変化させていたのと同様の事象が発生する可能性は否定できません。

- Word文書のマクロからマルウェアに感染させる手法自体は古典的なものであることから、そのような不審なWord文書は開かない、かつWordのセキュリティ設定においてマクロを自動的に実行しないようにするよう心がけ、加えてアンチウイルスによるマルウェアの感染防止、WindowsファイアウォールやUTM等によるマルウェアの外部への通信検知・遮断といった複数の対策をとることが肝要です。

●マイクロソフト、過去14年分・2億5,000万件のカスタマーサポート情報が誤って公開状態に

https://gigazine.net/news/20200123-microsoft-css-data-leak/
https://eset-info.canon-its.jp/malware_info/trend/detail/200226.html

このニュースをザックリ言うと・・・

- 1月22日(現地時間)、IT関係のレビュー・比較を行う英Comparitech社のセキュリティ研究者より、マイクロソフト(以下、MS)の2億5,000万件以上のカスタマーサービスとサポートのレコードが外部に公開されていたと発表されました。

- 発表によれば、レコードには過去14年分のカスタマーサポートにおけるユーザーのメールアドレス・契約番号・支払い情報・IPアドレスといった個人情報およびユーザーとの通話ログ・内部メモが含まれていたとのことです。

- Comparitech社では2019年12月29日、5台のデータベースサーバーがアクセス状態にあったことを確認してMSに通知を行ったとしており、またMS側でも24時間以内に対応を行い、サーバーが悪用された痕跡はなかったとしています。

AUS便りからの所感

- データベースサーバーは分散処理型検索エンジン「Elasticsearch」が稼働していましたが、2019年7月には日本国内でも、本田技研工業の内部情報を格納したElasticsearchサーバーが第三者からアクセス可能な状態で稼働していたことが明らかになっている(AUS便り 2019/8/5号)等、同様の事例は度々発生しています。

- データベースサーバーに限らず、不特定多数への公開を想定していないサービスについては、サーバ自身もしくはルータ・UTMのファイアウォール機能を設定してアクセスを許可するIPアドレス等を制限し、加えてパスワードが設定可能であれば必ずかけ、かつ公開サービスも含めたアクセスログの収集により、インシデント検知や原因等の調査を迅速に行える体制を確実に整えるようにしてください。