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。

●不正なChrome拡張機能「SHARPEXT」をインストールしてGmail等を盗聴する手口が報告される

https://www.itmedia.co.jp/news/articles/2208/15/news012.html
https://gigazine.net/news/20220805-north-korean-hackers-read-gmail/
https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/

このニュースをザックリ言うと･･･

- 7月28日(現地時間)、セキュリティ調査会社の米Volexity社より、Chromeブラウザーに Webメールの盗聴を行う不正な拡張機能をインストールする攻撃手法について取り上げられています。

- 「SHARPEXT」と呼ばれる拡張機能は、北朝鮮が関与するとされるサイバー攻撃集団「SharpTongue」によって2021年9月頃から使用されており、アカウント情報を盗むなどの挙動はとらないものの、インストールされたブラウザーでGMail(およびAOLメール)を開いた際に表示されたメールを盗み見るとされています。

- SHARPEXTがインストールされるブラウザーはChrome以外にもEdge等のChromiumエンジンを用いたブラウザーが対象とされています。

AUS便りからの所感等

- SHARPEXTは、攻撃者が何らかの手段でPCに侵入し、Chromeの設定ファイルの奪取・改ざん等を行うことで密かにインストールされるとのことです。

- 通常はGoogle等による正規の拡張機能サイト以外からの自動的なインストール・有効化に際しては警告が事前に表示されますが、SHARPEXTをインストールさせようとする際は同時に警告を出すウィンドウを表示させないためのスクリプト等も実行するとされています。

- SHARPEXTのインストールや警告の妨害などの一連の行動は、例えば遠隔からのPCへの不正ログインの他、不審なプログラムの実行等により行われることも考えられますので、常日頃からアンチウイルスやUTMによる防御を行っていること等がこのような攻撃の回避に重要と言えるでしょう。

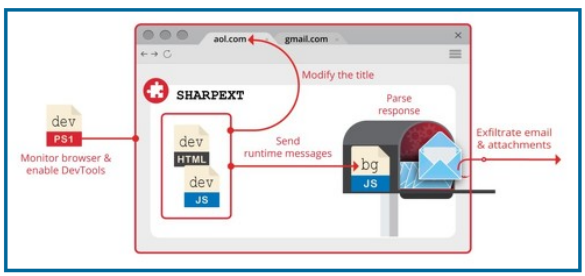
ITmedia NEWS

Innovative Tech

北朝鮮ハッカー集団によるGmailを盗み見るサイバー攻撃、Chrome拡張機能を活用

2022年08月15日 08時00分 公開　[山下裕毅，ITmedia]

米セキュリティ会社Volexityは、北朝鮮政府がスポンサーのハッカー集団「SharpTongue」が手掛ける新たなハッキング方法に関する情報を発表した。「SHARPEXT」と呼ぶ今回のマルウェアは、ブラウザの拡張機能を用いてGmailやAOLメールの内容を盗み取る攻撃を行う。



SHARPEXTのワークフロー

実はこのマルウェアは新しいものではなく、発見時の2021年9月には攻撃が始まっており、継続的な改善によりすでにバージョン3.0までアップデートしている。最初はGoogle Chromeだけだったが、最新バージョンではChromeに加え、

●警視庁・国税庁・KDDI返金を騙るフィッシングSMSに注意

https://www.itmedia.co.jp/news/articles/2208/16/news094.html
https://www.itmedia.co.jp/news/articles/2208/19/news149.html
https://www.itmedia.co.jp/news/articles/2208/15/news107.html

このニュースをザックリ言うと・・・

- 8月16日(日本時間・以下同様)、フィッシング対策協議会やIPAより、国税庁を騙るフィッシングSMS(スミッシング)が確認されているとして注意喚起が出されています。

- SMSの一例として「未払い税金支払いのお願い」「税金のお支払方法に問題があります」という文面が挙げられていますが、同庁からSMSを送信することはないとしています。

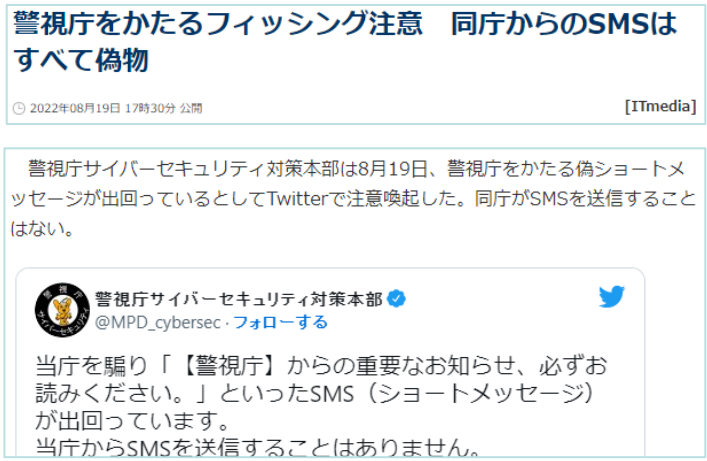
- 8月19日、警視庁サイバーセキュリティ対策本部より、「【警視庁】からの重要なお知らせ、必ずお読みください。」という文面のフィッシングSMSが出回っており、こちらも同庁からSMSを送信することはないとして注意喚起が出されています。

- 中央官庁以外では、8月16日にKDDIより、7月の通信障害によるau・povo等ユーザーへの返金措置に便乗したフィッシングへの注意が呼び掛けられています。

AUS便りからの所感

- KDDIについては、返金等の対象者へSMSによる連絡を行うものの、ユーザー側での手続きは不要で、SMSからWebサイトへの誘導および個人情報の入力を求めることはしないとしています。

- 不審なSMSやメールを受け取った際には、セキュリティ関連団体あるいはなりすましの対象となる本物の業者・組織からの注意喚起およびメールやSMSの運用に関するポリシーを必ず確認し、くれぐれも無闇にリンクをクリックしないよう慎重に行動することが肝要です。


警視庁をかたるフィッシング注意　同庁からのSMSはすべて偽物
2022年08月19日 17時30分 公開　[ITmedia]

警視庁サイバーセキュリティ対策本部は8月19日、警視庁をかたる偽ショートメッセージが出回っているとしてTwitterで注意喚起した。同庁がSMSを送信することはない。

警視庁サイバーセキュリティ対策本部
@MPD_cybersec · フォローする
当庁を騙り「【警視庁】からの重要なお知らせ、必ずお読みください。」といったSMS（ショートメッセージ）が出回っています。
当庁からSMSを送信することはありません。

●TikTok等のiOSアプリ内ブラウザーに「キーロガー」の指摘

https://www.itmedia.co.jp/news/articles/2208/22/news087.html
https://japan.cnet.com/article/35192132/
https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser

このニュースをザックリ言うと・・・

- 8月18日(現地時間)、ウィーン在住のソフトウェア研究者Felix Krause氏より、動画サイト「TikTok」のiOS版アプリに「キーロガー」が含まれているとする報告が出されました。

- 具体的には、TokTokアプリ内のリンクからウェブサイトにアクセスした際にアプリのブラウザー機能が用いられ、キー入力や何をタップしたかといった行動を監視するJavaScriptコードが挿入されるとのことです。

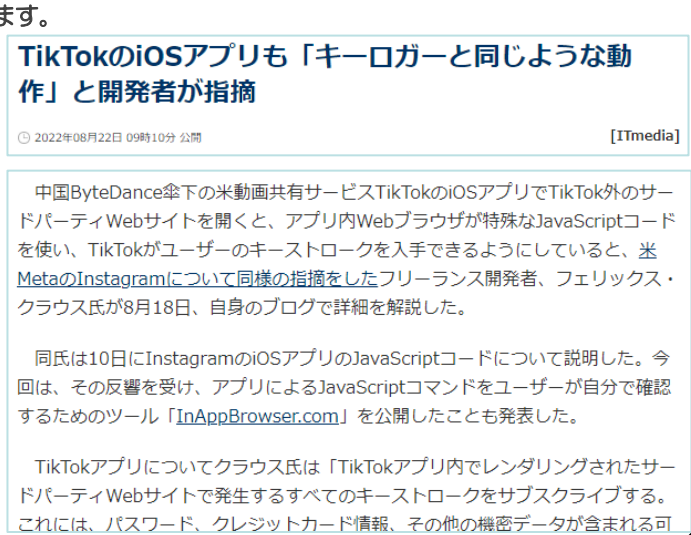
- 同氏は他の複数のWebサービスが提供するiOSアプリについても調査し、「Facebook」「Facebook Messenger」「Instagram」アプリについて同様のコードの存在を指摘しています。

AUS便りからの所感

- 報告に対し、TokTok側はコードの存在を認めつつもユーザーの追跡には用いていないと主張しています。

- 前述のアプリのうち「Facebook」等はアプリ内リンクを開いた際にデフォルトのブラウザーを使うオプションが提供されているとのことですが、TikTokのみ同様のオプションがないとのことです。

- Krause氏はこのようなJavaScriptコードが含まれていないか確認できるWebサイト「InAppBrowser.com」を発表しており(https://gigazine.net/news/20220822-in-app-browser-javascript/)、適宜こういったツールで確認するとともに、可能な限りアプリ内ブラウザーではなくデフォルトのブラウザーを使用することにより、不審な監視行為を回避することを心掛けるのが良いでしょう。


TikTokのiOSアプリも「キーロガーと同じような動作」と開発者が指摘
2022年08月22日 09時10分 公開　[ITmedia]

中国ByteDance傘下の米動画共有サービスTikTokのiOSアプリでTikTok外のサードパーティWebサイトを開くと、アプリ内Webブラウザが特殊なJavaScriptコードを使い、TikTokがユーザーのキーストロークを入手できるようにしていると、米MetaのInstagramについて同様の指摘をしたフリーランス開発者、フェリックス・クラウス氏が8月18日、自身のブログで詳細を解説した。

同氏は10日にInstagramのiOSアプリのJavaScriptコードについて説明した。今回は、その反響を受け、アプリによるJavaScriptコマンドをユーザーが自分で確認するためのツール「InAppBrowser.com」を公開したことも発表した。

TikTokアプリについてクラウス氏は「TikTokアプリ内でレンダリングされたサードパーティWebサイトで発生するすべてのキーストロークをサブスクライブする。これには、パスワード、クレジットカード情報、その他の機密データが含まれる可