— AUS（アルテミス・ユーザ・サポート）便り 2019/07/16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。

●2,500万台のAndroid端末が感染しているマルウェア「Agent Smith」見つかる

https://gigazine.net/news/20190712-mobile-malware-agent-smith/
https://news.mynavi.jp/article/20190711-858218/

このニュースをザックリ言うと・・・

- 7月10日（現地時間）、セキュリティベンダーのチェック・ポイント・ソフトウェア・テクノロジーズ社より、全世界のAndroidデバイス約2,500万台に感染しているとされるマルウェアについての調査結果が発表されました。

- 映画「マトリックス」の登場人物にちなみ「Agent Smith」と名付けられたマルウェアは、無料のゲームやユーティリティ等のアプリに紛れ込む形で配布されており、それらのアプリをインストールした端末上の他のアプリにも感染、ユーザに対して不要な広告を表示してくるとされています。

- Agent Smithの感染対象は、1,500万台の被害が出たインドを中心に、パキスタンやバングラディシュ等のアジアの国々とされている他、日本でも感染が確認されている模様です。

- Google公式のアプリストア「Google Play」でも同様のアプリが配布されており、現在は削除されたものの、1,000万回以上ダウンロードされていたとのことです。

AUS便りからの所感等

- Agent Smithは2017年に発見されたAndroidの脆弱性を悪用するとされ、脆弱性へのパッチは当時既にリリースされていたもののアップデートされなかった端末も多く存在していることが感染を広げた要因の一つと推測されており、もし手元の端末がもうアップデートが提供されていない機種であればサポートが続けられている機種に乗り換えることが推奨されますが、そういった機種でもすぐにアップデートが提供されなくなる可能性は十分に考えられるのは悩ましいところです。

- 通常Androidがアプリをインストールすることができる唯一のサイトであることから、Google Playに不正なアプリをアップロードしようとする攻撃者は多く、Googleでは日々そういったアプリを削除するとともにAndroid端末を有害なアプリから保護する「Google Play プロテクト」を提供していますが、いたちごっこは今も続いています。

- 結論としては、インストールするAndroidアプリは最小限に留め、決して非公式のアプリサイトからはインストールしないこと、事前にアプリストアでのレビューやSNS等での評判を参考とすること等により、可能な限りマルウェアからの脅威を回避する為の対策をとって頂ければ幸いです。


GIGAZINE

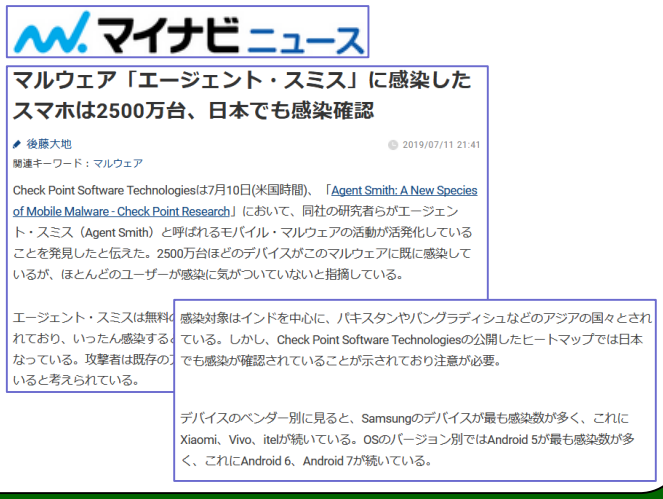
セキュリティ
2500万台のAndroid端末が感染しているマルウェア「Agent Smith」見つかる

セキュリティ会社・Check Point Researchの調査により、世界で2500万台に感染している新種のマルウェアが見つかりました。「Agent Smith(エージェントスミス)」と呼ばれるこのマルウェアは、他のアプリを悪質なコード入りの

しかし、アップデートが世界中のすべてのAndroid端末で適用されたわけではないため、今回のように未対応端末の大規模感染が発生したようです。報告によれば、「Agent Smith」は主にヒンディー語、アラビア語、ロシア語、インドネシア語のユーザーをターゲットにしていて、インドで1500万台の被害が出ているほか、パキスタン、バングラデシュなどのアジア諸国でも大規模な感染が確認されていて、アメリカでも30万台が感染しています。

「Agent Smith」を配布していたグループは、これとは別にGoogle Playでも同様のマルウェアを配布していたことがあり、すでに当該アプリはGoogle Playから削除されているものの、1000万回以上ダウンロードされていたとのこと。

テック系ニュースサイトのPhys.orgに対して、セキュリティ会社であるトレンドマイクロのダスティン・チャイルズ氏は「ウェブサイトを閲覧するだけでアプリをインストールしてくる悪質な広告があります。広告ブロッカーは、単に『広告』をブロックするだけではないのです」と、広告ブロックアプリの利用を推奨し、アプリをダウンロードするときはサードパーティ製ストアを利用せず、Google Playからダウンロードするように呼びかけました。


マイナビニュース

マルウェア「エージェント・スミス」に感染したスマホは2500万台、日本でも感染確認

後藤大地　2019/07/11 21:41
関連キーワード：マルウェア

Check Point Software Technologiesは7月10日(米国時間)、「Agent Smith: A New Species of Mobile Malware - Check Point Research」において、同社の研究者らがエージェント・スミス（Agent Smith）と呼ばれるモバイル・マルウェアの活動が活発化していることを発見したと伝えた。2500万台ほどのデバイスがこのマルウェアに既に感染しているが、ほとんどのユーザーが感染に気がついていないと指摘している。

エージェント・スミスは無料

感染対象はインドを中心に、パキスタンやバングラディシュなどのアジアの国々とされている。しかし、Check Point Software Technologiesの公開したヒートマップでは日本でも感染が確認されていることが示されており注意が必要。

デバイスのベンダー別に見ると、Samsungのデバイスが最も感染数が多く、これにXiaomi、Vivo、itelが続いている。OSのバージョン別ではAndroid 5が最も感染数が多く、これにAndroid 6、Android 7が続いている。

●TwitterでスパムDMが拡散…「ONLY FOR YOU」で始まるDMに注意

https://abematimes.com/posts/7009713

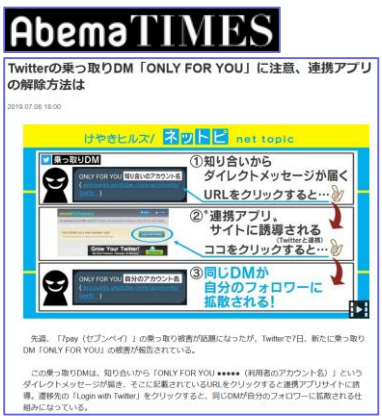
このニュースをザックリ言うと・・・

- 7月7日（日本時間）以降、Twitter上で不審なDMを受け取ったとする報告が相次いでいます。

- DMは「ONLY FOR YOU ●●●●●(利用者のアカウント名)」で始まり、記載されたリンクのクリック先でTwitterアプリとの連携を求めるメッセージが表示されるものとなっています。

- アプリとの連携を承認した場合、同様のDMをさらに別のユーザに送信してしまうため、これを承認しないよう呼びかけられています。

AUS便りからの所感等



- DMのリンクは一件YouTubeのページのものに見えますが、アクセスによりYouTubeと関係ないTwitterアプリの紹介ページが表示され、最終的にはアプリ連携を求めるTwitter上のページにリダイレクトする仕組みになっています。

- 不審なTwitterアプリとの連携は、自分のアカウントの権限でツイートの送受信、フォローおよびプロファイル・アイコンの修正等を勝手に行わせることにもつながり得ます（なお、連携した場合でもアカウントのパスワードを奪取されることはありません）。

- どんなアプリであっても、連携の際には要求される権限を明示した上で了承が求められ、了承しない限りはそのアプリにアカウントを利用されることはありませんので、ネット上の評判も注視しつつ、信頼できる必要最小限のアプリとのみ連携することを心掛け、不要になったアプリやうっかり連携してしまったアプリは「設定とプライバシー」→「アプリとセッション」（あるいは「アプリと端末」）から解除するようにしてください。

●地方自治体を襲う「死神リューク」…ランサムウェア身代金支払いで被害増大の連鎖

https://www.itmedia.co.jp/news/articles/1907/09/news052.html

このニュースをザックリ言うと・・・

- 6月27日（現地時間）頃、米国の複数の自治体でランサムウェア感染によるシステム障害が相次いでいるとして地元メディア等に報じられています。

- 例えばフロリダ州のリビエラビーチでは、これによるシステム障害でかかってきた通報電話の内容を書類で手書きする対応を強いられた上、3週間たってもシステム復旧の目途が立たず、最終的には60万ドル（約6,500万円）分の身代金をビットコインで支払っています。

- ランサムウェアは漫画「デスノート」のキャラクターである死神の「リューク」にちなんだとみられる「Ryuk」を名乗っており、同州レイクシティやキー・ビスケーン、ジョージア州アトランタやメリーランド州ボルティモア等でも被害をもたらしています。

AUS便りからの所感等

- ランサムウェアは決して廃れた攻撃ではなく、2018年に活動が確認された「GandCrab」への感染を狙うメールが今年初頭に日本を中心に大量に送信されています（AUS便り 2019/01/15号参照）。

- 国内の事例として、2018年10月に病院の電子カルテシステムが「GandCrab」に感染して一時使用できなくなりました（AUS便り 2018/10/29号参照）。

- 全てのマルウェアに言えますが、「絶対に感染しない体制」以上に「感染時のシステムやデータに関する被害を最小限に食い止められる体制」を整えることにも着目することもまた重要であり、アンチウイルスやUTMによる防御はもちろん、ネットワークセグメントの分割、データのバックアップを適切に行うこと、あるいはPCをネットワークに接続する際の検疫ソリューション等、様々な対策を検討すべきでしょう。