— AUS（アルテミス・ユーザ・サポート）便り 2016/07/19号 —
http://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。

●「攻撃者でもファイル復旧できない」新型ランサムウェア？「Ranscam」

http://www.itmedia.co.jp/enterprise/articles/1607/14/news064.html
http://japan.zdnet.com/article/35085886/

このニュースをザックリ言うと･･･

- 7月11日（現地時間）、米Ciscoのセキュリティ部門Talosより、新種のランサムウェア「Ranscam」について警告が発表されました。

- Ranscamに感染すると「隠された暗号化パーティションにファイルを移動した」というメッセージとともに身代金を要求、また実際に身代金を支払い、ボタンをクリックしたとしても「認証に失敗した。ボタンをクリックするごとにファイルを削除する」と表示されますが、実際には単にファイルを削除する機能しか持っていない模様です（認証に関するメッセージも虚偽のものとされています）。

- Talosでは、Ranscamについて「アマチュアのマルウェア作者が開発したもの」「身代金を払えばファイルを復旧できると被害者に思い込ませる」と推測しています。

AUS便りからの所感等

- その定義上、ランサムウェアはいずれも暗号化したファイルを復号する手段を持っているものですが、Ranscamはそういう手段も持たず、ただファイルを削除して身代金を要求するだけのもののようで、ランサムウェアの流行に便乗した悪質なマルウェアではありますが、これ自身をランサムウェアと呼ぶべきものかについては少なからず疑問が生じます。

- しかし、Ranscamの感染によりシステムファイル等が削除されてしまい、復旧にはPCの再セットアップが必要とされる等、もたらされる被害で見れば結局は「PC上のファイルが破壊される」も同然と言えます。

- 感染されないため、また感染後の被害を最小限に抑えるためには、アンチウイルスやUTMによる防御、またTalosも改めて推奨するように、オフラインバックアップ（バックアップデータ自体が破壊・暗号化されないよう）を含めた適切な対策が重要です。

ITmedia エンタープライズ

2016年07月14日 07時49分 更新

また新型ランサムウェア、攻撃者でもファイル復旧は無理

たとえ被害者が要求に従って身代金を払ったとしても、マルウェア作者ですらファイル復旧は不可能だという。

[鈴木聖子，ITmedia]

被害者のファイルを人質に取って返さないまま、身代金だけだまし取ろうとする新手のランサムウェアの亜種が見つかった。米Ciscoのセキュリティ部門Talosが7月11日のブログで伝えた。

Talosによると、このランサムウェア「Ranscam」は、他のランサムウェアのように高度な機能は持たず、あらゆる手口でユーザーを脅して身代金をだまし取ろうとする。感染すると通告画面が表示され、「お前のファイルは隠しパーティションに移動して暗号化した」と脅迫する。

「Ranscam」の脅迫画面（Ciscoより）

ZDNet Japan

身代金を払っても復旧せず--粗雑なランサムウェア「Ranscam」が発覚

Charlie Osborne （Special to ZDNet.com） 翻訳校正： 編集部 2016年07月14日 16時49分

身代金を支払ってもファイルが復元されない新たなランサムウェアが発見された。Cisco Talosセキュリティチームによると、この新種のランサムウェア「Ranscam」は「Cryptowall」や「TeslaCrypt」など「本物の」ランサムウェアには遠く及ばず、複雑性に欠け、復号やファイル復元に関してはまともな機能を全く備えていないという。

このマルウェアは被害者のファイルを暗号化したと宣言し、ランディングページを立ち上げて、0.2ビットコインを[illegible]に関係ないクリックが実行されるくる。

しかし、これは完全な嘘である。

「泥棒たちに、もはや自尊心はない」とTalosは記している。「Ranscamは単に被害者のファイルを削除するだけだ。被害者がランサムウェア作成者の要求に応じたとしても、脅迫者が被害者のファイルを復元するとは必ずしも信じられないという根拠を示す、さらなる事例となる」

このランサムウェアでは、被害者のファイルが「隠され、暗号化されたパーティション」に移されたと表示される。これは珍しいことだ。多くのランサムウェアでは単に、該当ファイルは元の場所にあるが、アクセスできないように暗号化されていると表示される。

被害者が身代金を支払うと、決済を認証するというボタンをクリックできるようになる。しかし、実際には認証は実行されない。ボタンをクリックすると新たな画像が表示され、そこには認証が失敗したことと、支払いが実行されるまではクリックするたびに新たなファイルが削除される旨が書かれている。

つまり、支払いを要求されるものの、実際には期待しても無駄である。ファイルはすでに削除されており、このマルウェアにはファイルを復元する機能がない。

●発表されたばかりの「Pokemon GO」にマルウェア入りの偽物

http://internet.watch.impress.co.jp/docs/news/1009669.html

このニュースをザックリ言うと・・・

- 7月11日（日本時間）、大手セキュリティベンダーのマカフィー(インテルセキュリティ)社より、6日に公開されたばかりのスマートフォン（iOS・Android）向けゲーム「Pokemon GO」の偽物が出回っているとして、同社ブログで警告が発表されました。

- 同社では、公開翌日の時点で、正規アプリにマルウェアが仕込まれた偽の「Pokemon GO」を発見し、遠隔操作ツール「DroidJack」が動作することを確認しており、DriodJackにより、SMSメッセージ・通話履歴・電話帳・ブラウザ閲覧履歴・位置情報やインストールアプリの一覧といったユーザ情報の奪取、あるいは写真撮影・ビデオ録画・通話録音およびSMS送信といった行為が攻撃者により実行可能とされています。

- 7月15日時点で「Pokemon GO」はオーストラリア・ニュージーランド・アメリカ向けにのみ配布されており、その他の国のユーザーが非公式のアプリサイトから入手しようとしたのを狙ったものとみられています。

AUS便りからの所感等

INTERNET Watch

マルウェアを仕込んだ偽の「Pokemon GO」出回る

磯谷 智仁　2016年7月11日 14:54

マカフィー株式会社は11日、スマートフォンゲーム「Pokemon GO」を模倣したマルウェア入りのアプリが発見されたと発表した。なお、Pokemon GOは、7月6日よりオーストラリアやニュージーランド、米国で公開されているが、日本では現時点で未公開となっている。

インテルセキュリティのモバイルマルウェアリサーチチームは、公開翌日に正規アプリにマルウェアを仕込んだ偽のPokemon GOのマルウェアを発見。ファイル名には、ファイル共有サイト"apkmirror.com"で二次配布されていた正規アプリと類似した名称が付けられていたという。

- 世界中で話題になるイベントには必ずそれに便乗するサイバー犯罪が発生するのと同様、現在プレイできない国以外からも注目を集め、そしてそれ以上にさほどネットリテラシーの高くない子供たちがメインユーザとなる「Pokemon GO」が狙われるのは、ある意味必然だったとも言えます。

- 特にiOSやAndroidデバイスはPCに比べアンチウイルス等のセキュリティソリューションが導入される傾向が強くない印象があり、そこもつけこまれる要素の一つですので、そういったソリューション（他にも可能な限りUTMへのVPN接続でインターネットにアクセスする等）を確実に導入すること、アプリは信頼できるソースだけからインストールすること、またアプリがリクエストする許可の種類に注意を払うことも重要です。

●Macに感染するマルウェア2件が報告される

http://gigazine.net/news/20160707-mac-backdoor-malware/
http://japanese.engadget.com/2016/07/09/mac-gatekeeper/

このニュースをザックリ言うと・・・

GIGAZINE

2016年07月07日 17時17分00秒

Macからデータを盗んだりコードを勝手に実行したりとあらゆるコントロールを奪ってしまう極悪マルウェアが登場

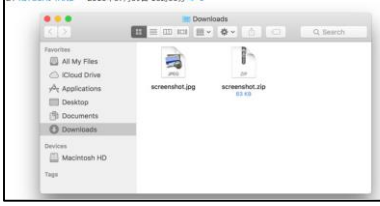
2016年初頭に、初めてmacOS(OS X)をターゲットとしたランサムウェアが発見されましたが、これに続く、macOSをターゲットとしたマルウェア「Backdoor.MAC.Elanor」の存在が、ルーマニアのセキュリティツール開発企業Bitdefender Labsにより明らかになりました。

New Backdoor Allows Full Access to Mac Systems, Bitdefender Warns | Bitdefender Labs

engadget 日本版

Macからパスワードを盗み出すマルウェアが登場。ただしGateKeeperが機能していれば実害なし

BY KIYOSHI TANE ・ 2016年07月09日 16時00分



- 7月上旬に、macOS（OS X）をターゲットとするマルウェアが2件報告されています。

- 7月5日（現地時間）、ルーマニアのアンチウイルスベンダーBitdefender Labs社が「Backdoor.MAC.Elanor」について警告しており、偽のファイル変換ソフトを介して侵入し、データの奪取、遠隔からのコード実行およびカメラへのアクセス等を行うとされています。

- 7月6日（現地時間）には、スロバキアのアンチウイルスベンダーESET社が「OSX/Keydnap」について警告しており、管理者権限により、Mac上に保存されたGMailやネットバンキング等のサービスのパスワードを奪取するとされています。

AUS便りからの所感等

- Macに感染するマルウェアとしてはまだ数は少ないものの、今年3月には初となるランサムウェアが確認される（AUS便り 2016/03/22号参照）等、その脅威がWindowsと同様になる日が来ることも想定されます。

- 一方で「OSX/Keydnap」については、OSに備わっているセキュリティ機能「GateKeeper」が有効であれば実行を防ぐことができるとされており、WindowsのUAC（User Account Control）でも言えることですが、安易に利便性を求めてそういったセキュリティ機能を解除しないことは、万が一のマルウェアへの感染を食い止めるためには大事なことです。

- Windowsで名の知られたアンチウイルスソフトの多くはMac向けもリリースされていますので、必ずそれらを導入すること、もちろん可能な限りUTM等によるさらなる防御を図るようにしましょう。