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。

●勝手に仮想通貨を発掘するスマホアプリ、Android公式ストアで複数発見…トレンドマイクロ社発表

https://www.is702.jp/news/2233/
http://blog.trendmicro.co.jp/archives/16293

このニュースをザックリ言うと・・・

- 10月31日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、不正に仮想通貨を発掘する能力を備えたAndroid向けアプリが公式アプリストア「Google Play」で複数確認されたと同社ブログにて発表されました。

- 記事によれば、今回確認された不正なアプリはユーティリティアプリや壁紙アプリ等の計3つで、正規アプリに仮想通貨発掘のためのライブラリを追加して再パッケージしたものも含まれていたとされています（なおこれらのアプリは既に削除されています）。

- アプリを作成した犯人は24時間で170ドル（約19,300円）相当の仮想通貨を発掘したとされており、同社ではこういったアプリによる発掘のために「ユーザが犯人の代わりに電気代・通信費を支払う羽目になる」として、スマホにもセキュリティアプリを導入するよう呼び掛けています。

AUS便りからの所感等

- 記事によれば、仮想通貨を発掘する不正アプリ自体はすでに2014年3月に確認されており、今回確認されたアプリの特徴として、検出を逃れるために、JavaScriptを読み込み、不正なコードを追加する手法をとっていたことを挙げています。

- PCのみならず、スマホ・タブレットのようなスマートデバイス向けにも、アンチウイルスベンダー各社がアプリを提供していますが、偽物を掴まされては元も子もありませんので、ネット上の評判を十分に確認し、正規のアプリを導入するよう注意しましょう。

TREND MICRO | is702 インターネットセキュリティナレッジ

勝手に仮想通貨を発掘するスマホアプリ、公式ストアで複数発見

2017/11/02

ツイート　いいね！ 1　G+　B!ブックマーク 0　EMail

トレンドマイクロは10月31日、公式ブログで「モバイル端末向け仮想通貨発掘マルウェア、Google Playで確認」と題する記事を公開しました。それによると、2017年10月中旬、不正に仮想通貨を発掘する能力を備えたAndroid向けアプリが、トレンドマイクロによりGoogle Play上で複数確認されました。

インターネットを通じて流通する「仮想通貨」は、通常の通貨等で購入する以外に、「発掘（マイニング）」と呼ばれる作業を通して得ることができます。ただし、それには高機能なPC端末や電気代が必要です。そのため、他人のPCやスマートフォンに忍び込み、この発掘作業を代わりに行わせる、不正プログラムや詐欺サイトが存在します。

仮想通貨を発掘する不正アプリは、すでに2014年3月に確認されています。目新しいものではありませんが、仮想通貨への注目が高まりつつある中で今回新たに見つかったアプリは、検出を逃れるために、JavaScriptを読み込みコードを追加する手法を使っていました。アプリは、お祈りのためのアプリ、ツールアプリ、壁紙アプリに偽装したものが見つかっていますが、とくに壁紙アプリは、正規アプリに仮想通貨発掘ライブラリを追加して再パッケージした“トロイの木馬”方式でした。

こうして発掘された仮想通貨は犯人のものになりますが、24時間で170ドル超相当（約19,300円超）の仮想通貨が発掘されたとトレンドマイクロでは分析しています。なお、今回見つかった不正アプリは、すでにGoogle Playから削除されています。

いずれも画面表示などは行わず、秘密裏に発掘を行いますが、不正アプリが稼働しているスマホは、極めて高いCPU利用率を示します。結果的にユーザは、犯人に代わって電気代・通信費を支払うはめになります。意図せぬ不正アプリの侵入を防ぐためにもスマホでもセキュリティアプリの導入を検討しましょう。

TREND MICRO トレンドマイクロ セキュリティブログ

モバイル端末向け仮想通貨発掘マルウェア、Google Play で確認

投稿日: 2017年10月31日
脅威カテゴリ: 不正プログラム，モバイル，TrendLabs Report
執筆: Trend Micro

モバイル端末の性能は、ある程度の仮想通貨を実際に発掘するには不十分だという疑いがあります。しかし、機器の消耗、電池の短命化、通常よりも重たい動作など、感染端末がユーザに与える影響は明確です。

トレンドマイクロは、2017年10月中旬、不正に仮想通貨を発掘する能力を備えたアプリを Google Play 上で確認しました。これらのアプリは、検出を逃れるために、JavaScript を動的に読み込み、ネイティブコードを追加する手法を利用します。トレンドマイクロは、これらの不正アプリを「ANDROIDOS_JSMINER（ジェイエスマイナー）」および「ANDROIDOS_CPUMINER（シーピーユーマイナー）」として検出しています。

仮想通貨を発掘するアプリがGoogle Playで確認されたのは今回が初めてではありません。2014年3月には、密かに

■「ANDR
以前、本ブ
用してユー
ANDROID
のうち、17

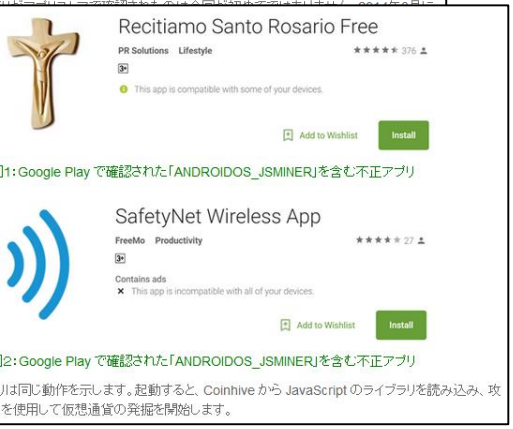


図1：Google Play で確認された「ANDROIDOS_JSMINER」を含む不正アプリ

図2：Google Play で確認された「ANDROIDOS_JSMINER」を含む不正アプリ

これら 2つのアプリは同じ動作を示します。起動すると、Coinhive から JavaScript のライブラリを読み込み、攻撃者の「Site key」を使用して仮想通貨の発掘を開始します。

●iOSとAndroidのセキュリティパッチ公開、「KRACKs」の脆弱性に対処

http://www.itmedia.co.jp/news/articles/1711/01/news071.html
http://www.itmedia.co.jp/news/articles/1711/07/news067.html

このニュースをザックリ言うと・・・

- 10月31日（現地時間）、米Apple社より、iOS（iPhone, iPad）等のセキュリティパッチが公開され、また11月6日には米Google社からも、Androidの月例のセキュリティパッチが公開されています。

- いずれのセキュリティパッチも、WPA2の脆弱性「KRACKs」（AUS便り 2017/10/23号参照）についての対策が含まれています。

- この他、さらに危険な脆弱性についても対策されていますが、Google社ではそれらの脆弱性の悪用が横行しているとの報告は入っていないとしています。

AUS便りからの所感等

- iOSおよびAndroidデバイスへのセキュリティパッチの対応は機種によって様々で、ほんの数年前にリリースされた機種でもパッチの提供が行われない場合もあるため、ベンダー情報の確認は不可欠でしょう。

- 例えば、iOSについては、iPhone 7以降と、2016年に発売された9.7インチのiPad Proのみがパッチ提供の対象となっています。

- 以前にも述べていますが、KRACKsに限って言うならば、HTTPSやVPN等、WPA2以外の暗号化通信を解読できるものではありませんので、社外でWi-Fiによる通信でインターネットへアクセスする場合でも、UTMのVPN接続を経由することにより、付近の攻撃者による盗聴を防ぐことが可能となるでしょう。


ITmedia NEWS

Apple、iOS 11やHigh Sierraのセキュリティ情報公開
KRACKの脆弱性に対処

iOSやmacOS、tvOS、watchOSの更新版で、「KRACK」と呼ばれるWi-Fi関連の脆弱性が修正された。

[鈴木聖子，ITmedia]

Androidの月例セキュリティ情報公開、「KRACK」の脆弱性に対処

Androidで特に深刻な影響が指摘されていたWi-Fiの暗号化技術「WPA2」の脆弱性（通称KRACK）に対処した。

[鈴木聖子，ITmedia]

米Googleは11月6日、Androidの月例セキュリティ情報を公開した。Wi-Fiに使われている暗号化技術「WPA2」の脆弱性（通称KRACK）などに対処している。

Androidのセキュリティ情報によると、11月の月例パッチは「2017-11-01」「2017-11-05」「2017-11-06」の3本が公開された。このうち「2017-11-06」のパッチレベルでは、KRACKの脆弱性に分類される9件の問題に対処した。端末メーカーなどのパートナー向けには過去1カ月以内に通知したとしている。

●ボットネットのプラットフォーム、Linuxが約7割…カスペルスキー社発表

http://news.mynavi.jp/news/2017/11/08/033/

このニュースをザックリ言うと・・・

- 11月6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、2017年第3四半期におけるDDoS攻撃関連の動向についての統計データが発表されました。

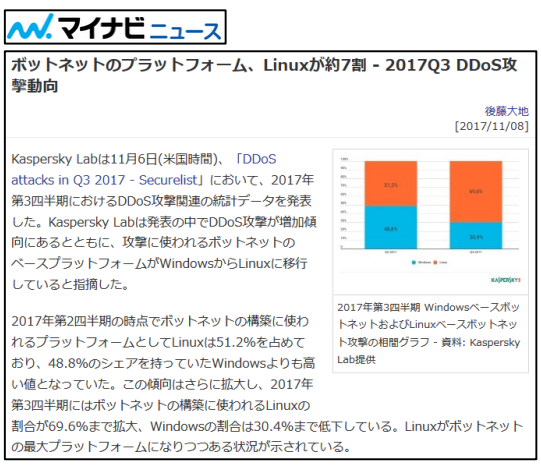
- それによると、DDoS攻撃は増加傾向にあり、かつボットネットを構築するプラットフォームはWindowsからLinuxに移行しつつあるとしています。

- 第2四半期での両者の割合は「Linux 51.2%、Windows 48.8%」でしたが、第3四半期では「Linux 69.6%、Windows 30.4%」とLinuxの割合が拡大しています。

AUS便りからの所感等

- 昨年猛威を振るった「Mirai」も主にLinux製のIoTデバイスに感染してボットネットを構築していましたが、OS自体のセキュリティレベル以上に、パスワードがデフォルトから変更されていない等、Windows PCに比べてメンテナンスが十分に行き渡らない傾向にあることが背景にあったと言えます。

- ネットワーク下にある全てのデバイスについてその存在を把握・管理し、適切なセキュリティ設定を行うこと、ファームウェア等に確実にパッチを適用すること、加えてUTMによる外部からの侵入、また万が一の感染時に外部へ行われる不正な通信を遮断できるような体制をとることが重要です。


マイナビニュース

ボットネットのプラットフォーム、Linuxが約7割 - 2017Q3 DDoS攻撃動向

後藤大地
[2017/11/08]

Kaspersky Labは11月6日(米国時間)、「DDoS attacks in Q3 2017 - Securelist」において、2017年第3四半期におけるDDoS攻撃関連の統計データを発表した。Kaspersky Labは発表の中でDDoS攻撃が増加傾向にあるとともに、攻撃に使われるボットネットのベースプラットフォームがWindowsからLinuxに移行していると指摘した。

2017年第2四半期の時点でボットネットの構築に使われるプラットフォームとしてLinuxは51.2%を占めており、48.8%のシェアを持っていたWindowsよりも高い値となっていた。この傾向はさらに拡大し、2017年第3四半期にはボットネットの構築に使われるLinuxの割合が69.6%まで拡大、Windowsの割合は30.4%まで低下している。Linuxがボットネットの最大プラットフォームになりつつある状況が示されている。

2017年第3四半期 Windowsベースボットネットおよびボットネットベースボットネット攻撃の相関グラフ - 資料：Kaspersky Lab提供