

スマートフォンセキュリティ脅威の動向を調査
ランサムウェア・データトラフィック盗用ウイルスが増加
「360 セキュリティ」でスマートフォンのセキュリティ対策を

360 モバイル・セキュリティ・リミテッドの研究開発機関である 360 Internet Security Centre では、「モバイルセキュリティ脅威動向調査 2016」を実施しましたのでその結果をお知らせします。2014年1月から2015年10月の期間に検出されたモバイルセキュリティ脅威の種類とその検出件数の推移を分析することで、今後ユーザーが対処しなければいけないセキュリティ脅威の動向と、その対策方法について考察しています。

■端末の自由を奪い、身代金を要求するランサムウェアが急増中！

ランサムウェアとは、スマートフォンのシステムやデータに侵入し、正常にアクセスできないようにしてしまうウイルスです。身代金要求型の不正プログラムとしても知られています。昨年と比較して2015年はランサムウェアが急速に増加しており、スマートフォンのセキュリティにとって最大の脅威のひとつとなっています。ランサムウェアの中にはゲームのプラグインを装うものもあり、ユーザーが実行すると端末がブロックされ、操作を受け付けなくなってしまいます。ロックを解除するには、インターフェイスに残されたチャット番号を通じてハッカーに連絡を取り、要求金額を支払わなければいけません。ハッカーはこのような悪質な方法で利益を得ています。

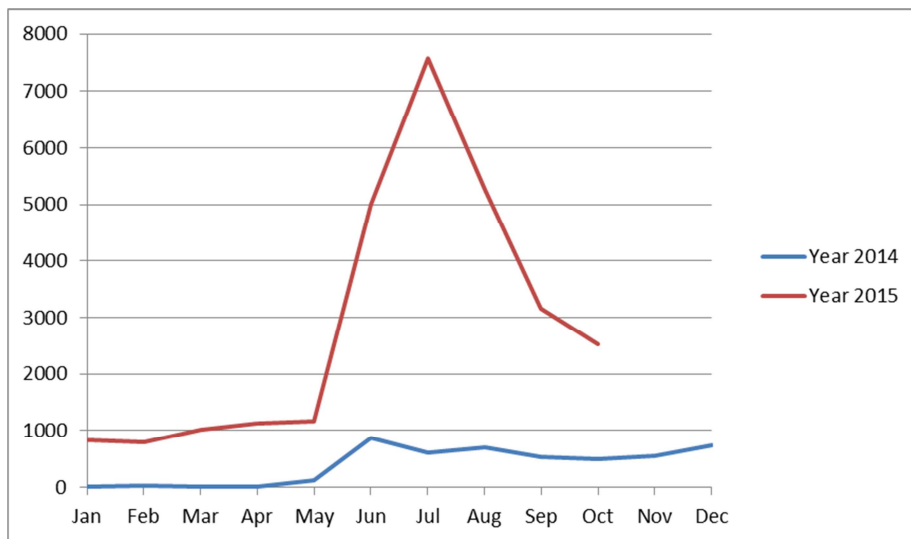


図 1.ランサムウェアの検出件数（2014年1月-2015年10月）

ランサムウェアの検出件数の推移を見ると、爆発的に増加する期間があることが分かります。常に増加しているわけではありませんが、去年と今年を比較すると、ランサムウェアが増加傾向にあることがわかります。

■スマートフォンセキュリティ脅威のほとんどは、データトラフィック盗用ウイルス

現在、スマートフォンのセキュリティ脅威は、データトラフィックを盗用するタイプと個人情報データを盗難するタイプがほとんどです。360 Internet Security Centre の調査によれば、データトラフィックを盗用するウイルスは去年と比較して急速に増加しています。

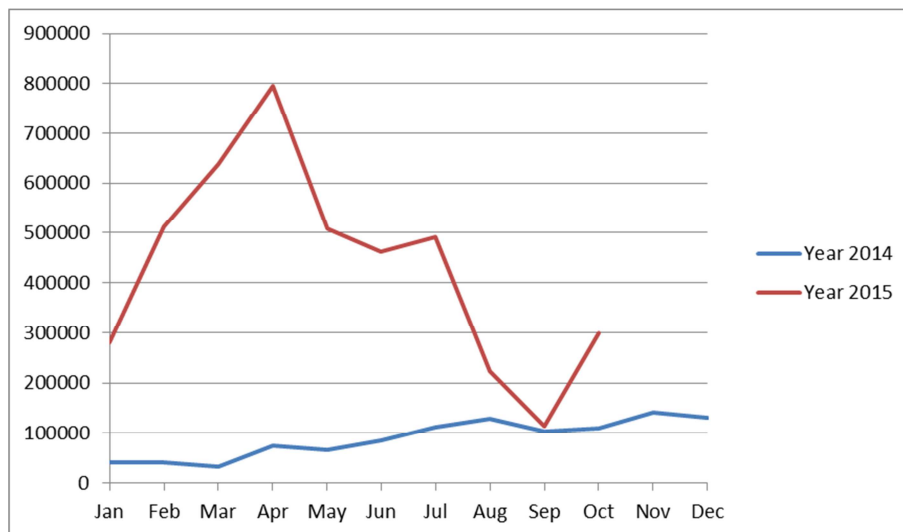


図 2.データトラフィック盗用ウイルスの検出件数（2014年1月-2015年10月）

データトラフィック盗用ウイルスは、端末の制御を奪って特定の Web ページにアクセスし、そのページの DAU（日次アクティブユーザー数）を不正に吊り上げます。これらのウイルスは、ユーザーのデータトラフィックを盗用することでハッカーに利益をもたらすことができます。

一例として、「Zombie of data traffic」というトロイの木馬型ウイルスが挙げられます。360 Internet Security Centre が実施したテストの結果では、このウイルスは、ユーザーが端末の画面をアンロックするたびに操作を実行し、データトラフィックを盗用することが確認されています。1 回に盗用されるデータの量は、約 0.76 MB です。ユーザーが端末の画面を 1 日に 150 回（第三者による実験から得られた値）アンロックする場合、このウイルスが 1 日に盗用するユーザーデータトラフィックの量は 114 MB になります。「Zombie of data traffic」による攻撃のプロセスは、3 段階に分かれています。

1. 悪意のあるプラグインをダウンロードする
2. 特定の Web ページにアクセスする
3. 特定の検索エンジンにアクセスする

クエリー1,000 回あたりの市場価格を 0.78~3.15 米ドルとして計算すると、このトロイの木馬型ウイルスは、1 日に 52,000~211,000 ドルの利益をハッカーにもたらすこととなります。このように利益が巨額であることから、ハッカーは今後も多くのウイルスを作成するものと考えられます。

■ 個人情報盗難ウイルスは依然として猛威を振るうものの、検出件数は減少傾向

データトラフィック盗用ウイルスが急増した一方で、個人情報データ盗難ウイルスは2014年11月から2015年2月にかけて爆発的な増加を示したものの、2015年4月以降は比較的安定した状態を保ち、検出件数が減少しています。個人情報データ盗難ウイルスは、2016年以降もこの安定した傾向を維持する可能性が高いと考えられます。

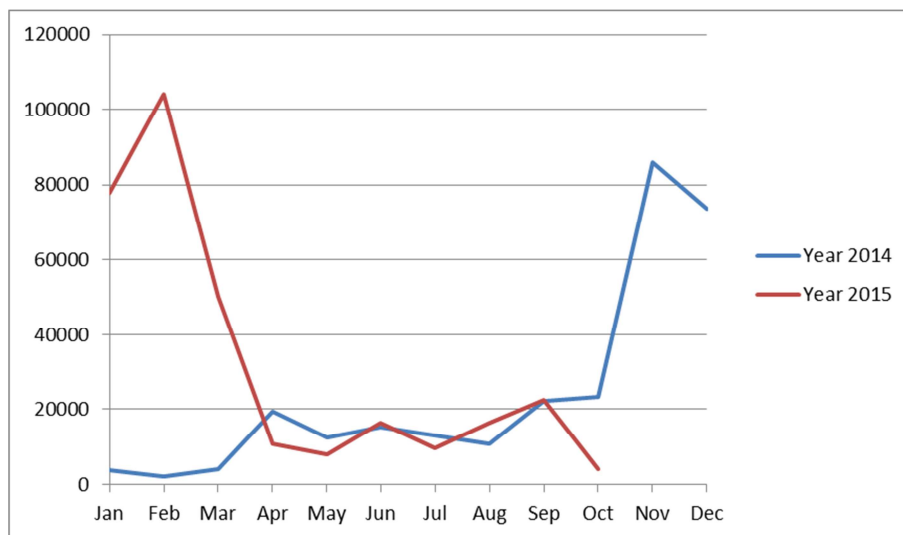


図3. 個人情報データ盗難ウイルスの検出件数（2014年1月-2015年10月）

■ 悪意のあるアドウェアも減少傾向

個人情報データ盗難ウイルスと同様に、悪意のあるアドウェアも減少傾向にあります。原因としては、ウイルス対策ソフトウェアの強化によって最近では悪意のあるアドウェアに対してアラートが表示されるようになり、ユーザーもこのようなアドウェアに対して注意を払い始めたことが挙げられます。悪意のあるアドウェアの減少は来年も継続すると予測されます。

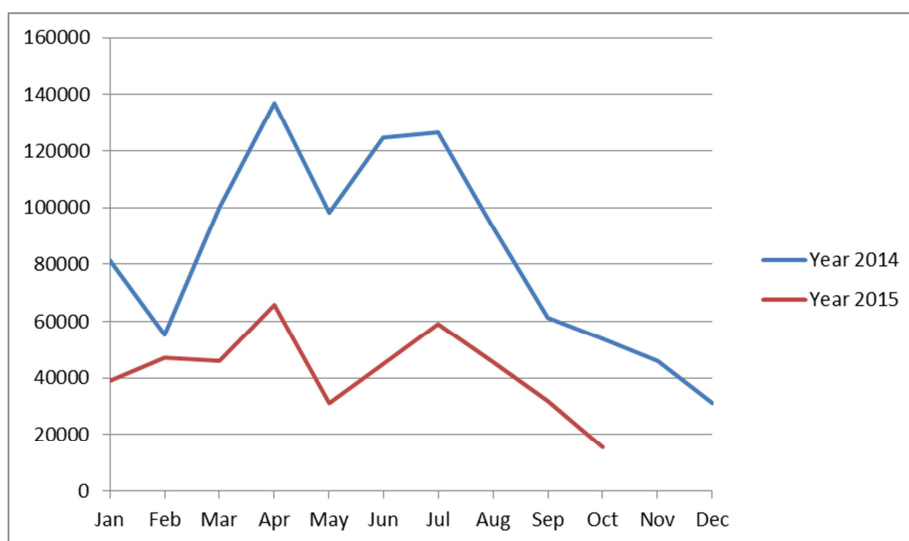


図4. 悪意のあるアドウェアの検出件数（2014年1月-2015年10月）

■スマートフォンの安全を守るために

スマートフォンをウイルスの脅威から守るために、アプリケーションをダウンロードする際は公式チャンネルのみを使用することをお勧めしますが、それだけでは不十分です。Google Playを含め、多くの公式ダウンロードチャンネルにも未検出のウイルスが残ったままのアプリケーションが存在するため、次の点に注意する必要があります。

1. USB デバッグ機能は、必要がない限りオフにする。
2. 端末のオペレーティングシステムを常に最新バージョンに維持する。
3. ウイルス対策ソフトウェアをインストールしてウイルスデータベースを常にリアルタイムに更新し、定期的に端末をスキャンする。

「360 セキュリティ」は無料でありながらも充実の機能を備えた総合セキュリティアプリとして、世界中の幅広い地域で支持されてきました。今後も、多くのユーザーに「安心・安全・快適」なスマートフォン利用を提供していきます。

《360 セキュリティ 製品概要》

「360 セキュリティ」は、中国国外向け製品として 2013 年に提供を開始して以来、世界 90 カ国で Google Play でのダウンロード数 1 位を獲得する¹など、無料でありながらも充実の機能を備えたオールインワンの総合セキュリティアプリとして多くの国と地域で支持されてきました。全世界のユーザー数は約 2 億人いますが、その 96%が中国国外の海外ユーザーです。また 30%は米国で、アジアにとどまらず欧米圏でも好評を博しています。360 セキュリティは Amazon のクラウドサービス AWS (Amazon Web Services) によって構築・運用され、全てのデータは中国国外の AWS 上で暗号化して処理されています。(※1 「ツール」カテゴリーにおける 1 日のダウンロード数が 1 位にランクインしたことのある国、App Annie より)

ダウンロード URL(Google Play) :

https://play.google.com/store/apps/details?id=com.qihoo.security&referrer=qihoo_id%3D105113

《360 モバイル・セキュリティ・リミテッド企業概要》

360 モバイル・セキュリティ・リミテッド(360 Mobile Security Limited)は Android 向けアプリの提供を担う、大手 IT 企業 Qihoo 360 Technology Co. Ltd.のグループ企業です。360 モバイル・セキュリティ・リミテッドが展開する「360 セキュリティ(360 Security)」は、高精度のアンチウイルス機能と、スピードアップやストレージ容量の確保といったスマートフォン最適化機能を兼ね備えたオールインワンのセキュリティアプリで、ユーザー数は世界中で 2 億人に上ります。本製品には「スマートフォンの安全を守るだけでなく、ユーザーに安心してその利用を楽しんでもらいたい」という思いが込められています。360 モバイル・セキュリティ・リミテッドは今後も、世界中のユーザーに快適でより良いスマートフォン生活を提供するべく、大きな情熱をもって「360 セキュリティ」をはじめとしたさまざまなアプリの提供に取り組んでいきます。

《360 セキュリティに関するお客様からのお問い合わせ先》
「360 セキュリティ」お客様お問い合わせ窓口 担当 藤田
MAIL : japan@360overseas.com