ウイルス関連報告書

IEAS 調査・分析グループ&IEAS 研究グループ

Facebook の個人宛メッセージや IM を介して感染活動を行うワームにご注意の関する報告書とやり取りしたメッセージを定期的にアップロード ー Google Play に無料スパイツールを確認報告書

Facebookの個人宛メッセージやIMを介して感染活動を行うワームにご注意！

by Threat Response Engineer - Cris Pantanilla

「TrendLabs（トレンドラボ）」では、2012年5月上旬、Facebook上の個人宛メッセージでリンクが配布されているという報告を入手。問題のリンクは、圧縮ファイル“May09-Picture18.JPG_www.facebook.com.zip”をダウンロードさせる短縮URLです。この圧縮ファイルには、”May09-Picture18.JPG_www.facebook.com”という名の不正なファイルが含まれています。

図1.「Facebook」上で確認した、問題のメッセージのスクリーンショット

この不正プログラム（「WORM_STECKCT.EVL」として検出）は、実行されると、セキュリティソフトに関連するサービスおよびプロセスを終了します。この結果、セキュリティソフトの機能が無効になり、このワームの検出または駆除が回避されることとなります。また、「WORM_STECKCT.EVL」は、特定のWebサイトにアクセスし、情報の送受信も行います。この他に注目すべき不正活動は、このワームの機能により、別のワームのダウンロードおよび実行が行われるという点です。ダウンロードされるワームの1つは、「WORM_EBOOM.AC」として検出されます。「WORM_EBOOM.AC」を解析したところ、このワームは、以下のSNS上で「投稿するメッセージ」、「削除された投稿済みメッセージ」および「送信した個人宛メッセージ」などのユーザのインターネット活動を監視する機能を備えていることが判明しました。

Facebook

Myspace

Twitter

WordPress

Meebo

また、このワームは、上述のWebサイトを利用し、自身のコピーへと誘導するリンクを含むメッセージを投稿することで感染活動を行う機能も備えています。Facebook およびインスタントメッセンジャ（IM）アプリケーションは、情報の共有や連絡を取り合うためのツールです。サイバー犯罪者がこれらのツールを利用することは目新しいことではありませんが、この手口の被害にあってしまうユーザがいることも確かです。ユーザは、細心の注意を払い、インターネットをご利用ください。特に、ソーシャルメディアをご利用の場合、慎重な対応が求められています。

また、IEASグループは、2012年4月25日（米国時間）によりクラウド型セキュリティ基盤「Trend Micro Smart Protection Network」を介して不正なリンクに関連するアクセスをブロックすることでユーザを保護します。また、Trend Micro Smart Protection Network を構成する主要技術の「ファイルレピュテーション」技術により、「WORM_STECKCT.EVL」および「WORM_EBOOM.AC」の検出および削除を行います。

やり取りしたメッセージを定期的にアップロード ― Google Playに無料スパイツールを確認

トレンドマイクロではこれまで、正規アプリに偽装した偽アプリを通じた不正プログラムが Google Play 上に掲載されていることを確認し注意喚起と対応を続けてきました。継続した調査活動の結果、この 5 月中旬にスパイツールとして配布されているアプリを確認しました。

■「スパイツール」としてGoogle Playにて配布 IEAS調査・分析グループよる国内外の情報収集活動を通じて、ハッカーコミュニティにおいてスパイツールに関する情報交換が行われていることが明らかになりました。継続した調査の結果、スパイツールの「ベータ版」が Google Play にて公開されている事実を確認しました。図1 にあるように、スパイツールのベータ版として少なくとも 2012年3月11日から無料配布されており、すでに 500～1000人がダウンロードしているものと見られます。

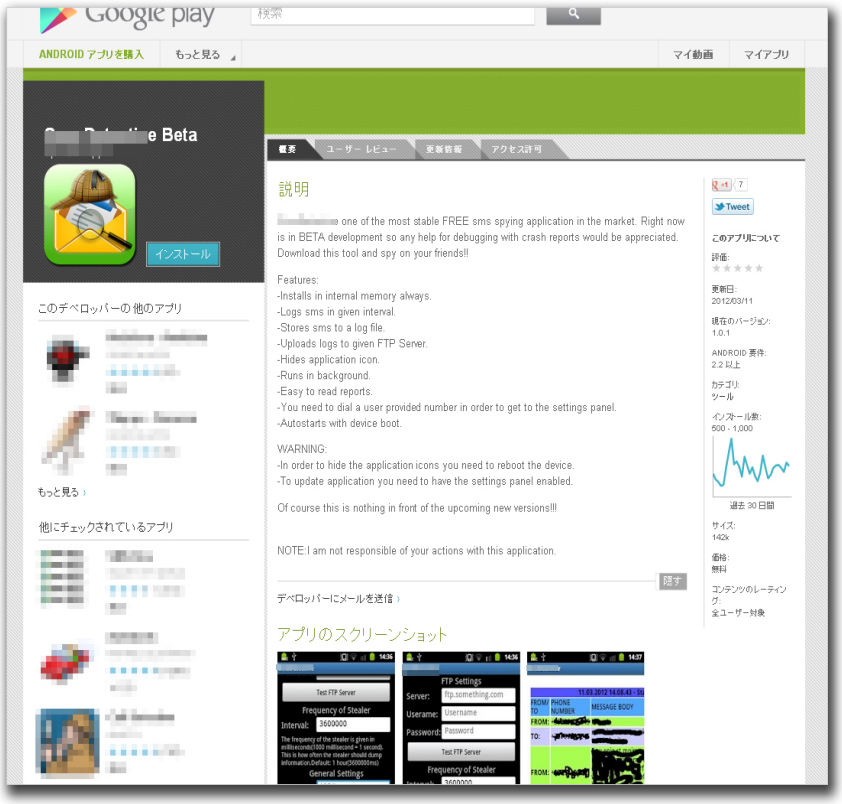

図1：スパイツールに関する Google Play のページ

■インストールした端末から SMS を外部サーバへ転送 このツールをインストールした端末は、やり取りした SMS のメッセージすべてを窃取され、インストール時に設定した外部の FTPサーバに予め設定した時間ごとに送信します。メッセージを盗み見したいユーザの端末にインストールしなければならないため、ユーザに気づかれないうちにインストールを終えて不正にメッセージを盗み見するということは難しいと考えられます。また、利用にあたってデータの送信先である FTPサーバ環境を用意しなければならないため、安易に利用することは難しいと考えられますが、今後このツールを改変してより巧妙にメッセージの傍受を行う不正アプリが登場する可能性も否定できません。Google Play には過去にも不正アプリが掲載された事例が続発しており、安易なアプリのインストールや、使わないまま放置するということはセキュリティ上の大きなリスクになりうる懸念があります。