アンドロイドへのマルウェア攻撃が本格化～G Data

ドイツにおけるセキュリティソフトウェアのリーディングカンパニーであるG Data Software AG（本社：ドイツ
ボーフム市、代表取締役：フランク・ハイスラー、ディルク・ホッホシュトラーテ）のセキュリティラボによる2011年上半期のマルウェア動向の分析を、G Data Software株式会社（本社：東京都千代田区、日本支社長：Jag 山本）がお知らせします。

・ウィンドウズ関連のマルウェアが、昨年上半期と比べて1.5倍に増加
・モバイル関連のマルウェアが13.8倍に急増

これまでのマルウェアは、大半が、ウィンドウズOSで動作するコンピュータを攻撃対象としていました。マックやリナックス上で動作するマルウェアは、きわめて数が少なく、さらにはスマートフォンもごくわずかでした。マルウェア対策といえば、まず、ウィンドウズが主でした。

G Dataのセキュリティラボによる2011年上半期におけるマルウェア動向の分析においても、ウィンドウズのマルウェアが圧倒的に多く、99.5%ほどを占めていました。

ウィンドウズのマルウェアは、2007年（約4万種）から2008年より（約894万種）にかけて約7倍ほどに急増し、その後、上昇カーブはやや緩やかになってはいるものの、増加の一途をたどり、2011年上半期で約120万種が確認されました。下半期も同様のペースで増加するとすると、2011年の1年間で、約250万種のマルウェアが出現すると予測されます。2010年は1年間で約210万種が出現したので、昨年と比べると、1.2倍ということになります。これは、12秒ごとに新種マルウェアが出現したことを意味します。

この数は、きわめて膨大であり、上昇率が落ち着いているとは言うものの、引き続き、ウィンドウズには、きめの細かいセキュリティ対策が必要であるとG Dataは考えます。

しかし他方で、これまで、ごくわずかであった他のマルウェアのなかで、アンドロイドを含むモバイルのマルウェアが、急増してきました。

ウィンドウズのマルウェアが2010年下半期と比べて1.5倍の増加だったのに対して、アンドロイドを中心としたモバイルのマルウェアは、13.8倍の増加となりました。その数は、55から803に増えました。確かに、ウィンドウズのマルウェア数との差は歴然としています。しかし、少なくとも、アンドロイド端末ユーザーが急増するに伴い、マルウェア（および攻撃する人間）もウィンドウズのみならず、アンドロイドも狙いはじめている、ということは確かです。

簡潔に言えば、ネット犯罪者たちは、これまで通り、ウィンドウズ
ユーザーを中心に攻撃を行うと考えられますが、新たに、アンドロイド端末のユーザーをも狙いはじめた、ということになります。

・クロスプラットフォームのトロイの木馬型マルウェアに今後注意が必要

ウィンドウズのマルウェアについては、全体的には、一度パソコンに侵入してから不正な動きをする「トロイの木馬」型が相変わらず多数を占めました。次いで、次々と回線を通じてマルウェ

アを投下する「ダウンローダー」と個人情報やデータを盗み出すための出入り口を用意する「バックドア」の割合が多くなりました。ただしこの両者は、昨年下半期と比べるとやや数が少なくなっています。その他では、個人情報やデータをこっそり盗み出す「スパイウェア」はほぼ横ばい、感染の拡散はしないものの悪質な挙動を行う「ワーム」と広告と思わせてお金をまきあげる「アドウェア」はやや上昇しました。

一方アンドロイドのマルウェアですが、注目すべきものとして、第一は、2011年5月
に大規模に発生した「Zsone」で、iCalenderなど、グーグルのアンドロイドマーケットにアップされていたアプリのデベロッパーの名称からとられたマルウェアです。トロイの木馬型で、SMSでの送信を行います。これをアンドロイドにインストールすると、中国の高額通信サービスにつながるようになります。レジストレーションの確認が妨害されるため、感染ユーザーが気づくのは、高額請求をチェックする時点になってからになります。

第二は、「NickiBot」です。NickiBotには、感染者をスパイする機能があります。Google++と呼ばれるマルウェアの亜種で、ソーシャルネットワークGoogle+のアプリケーションとして利用可能なようにみせかけます。アイコンも似ています。これは、バックグラウンドの雑音や通話を記録します。マルウェアは、攻撃者に対して、GPSの追跡データを含む、この情報を送るのにウェブサイトを使用します。これは、加害者がいつでも個人情報にアクセスして、ユーザーの現在の位置を決定するのを可能にします。

また、ネット犯罪市場において今流行しているのは、クロスプラットフォームのトロイの木馬型マルウェアです。スパムメールに添付されていたり、SNSに貼ってあるインターネットのURLリンクをクリックすると感染するなど、さまざまな手段を用いて今後活動することが予測されます。

「モバイルマルウェアで、サイバー犯罪者は新しいビジネスモデルを発見しました」と、ラルフ・ベンツミュラー（G
Dataセキュリティラボ所長）は説明します。「現在、アンドロイドへの攻撃者は、端末ユーザーに危害を加えるのにバックドア、スパイプログラム、および高価なSMSサービスを主に利用します。」
ネットの裏市場が関心をもちはじめたのはまだはじまったばかりですが、アンドロイド端末とそのユーザーは、かなり大きなリスクをもちはじめたと考えてよいでしょう。「さらに2011年下半期には、アンドロイドのマルウェアは、大幅に上昇するでしょう。」

基本データ

１）新種マルウェア数の変化
2005年 31,849
2006年 39,670
2007年 133,253
2008年 894,250
2009年 1,588,005
2010年 2,093,444
2011年 1,245,403（上半期のみ）
＊2011年通年の予想数値は約2,500,000です。

２）プラットフォーム別新種マルウェア数と比率（2011年上半期）
Win32 1,218,138（97.8%）

MSIL(.NET) 21,736 (1.7%)
WebScripts 3,123 (0.3%)
Scripts 832 (0.1%)
Mobile 803 (0.1%)
Java 313 (<0.1%)
ix 233 (<0.1%)
NSIS 131 (<0.1%)
＊文中の「99.5%」とは、Win32とMSILを合わせた割合です

＊上記はいずれもG Dataセキュリティラボ調べ

ジーデータソフトウェアとは
G Data Softwareは、1985年に創業し、1987年に世界最初の個人向けウイルス対策ソフトを発売した、ドイツのセキュリティソフトウェア会社です。
EUを中心に、個人向け・法人向け製品を展開しています。日本法人は2007年に設立しました。最大の特徴は、ダブルエンジンによる世界最高位のウイルス検出率です。また、新種や未知ウイルスへの防御、フィッシング対策、迷惑メールへの外国語フィルターなど、インターネットやメール環境を安全・快適にする機能を豊富に搭載しています。その結果G Dataのセキュリティ製品群は、マルウェアやフィッシング詐欺サイトを常に高検出することに定評があり、過去5年間以上にわたって、第三者機関・雑誌における受賞獲得数は他社の追随を許しません。

＊本リリースに記載されている各種名称、会社名、商品名などは各社の商標または登録商標です。

【本リリースに関する問合せ先】
G Data Software株式会社
101-0042 東京都千代田区神田東松下町48 ヤマダビル6F
窓口： 瀧本往人
E-mail: gdata_japan_info@gdatasoftware.com
URL： http://www.gdata.co.jp/

Generated by ぷれりりプレスリリース
https://www.prerele.com