ファイル共有ネットワーク由来の感染にご注意を～G Data

G Data Software株式会社（本社：東京都千代田区、日本支社長：Jag
山本）は、セキュリティラボにおいて収集された2011年11月
度のコンピュータ・マルウェア動向情報の分析を行いました。その結果、これまで多発していた脆弱性攻撃、USBメモリからの侵入に加えて、ファイル共有ネットワークに由来する攻撃も目立ったことを報告します。毎年、年末はマルウェア攻撃も増加する傾向にありますので、感染被害にはくれぐれもご注意ください。

G Dataセキュリティラボの集計データによれば、2011年11月
度に、上位を占めたマルウェア（＝拡散の度合いが高かったマルウェア種）は以下のとおりでした。

≪2011年10月 度マルウェア活動上位10種≫
1 Java.Exploit.CVE-2010-0840.E 3.66 % 上昇(10月8位)
2 Exploit.CplLnk.Gen 1.41 % 上昇（10月9位）
3 Worm.Autorun.VHG 0.83 % 同
4 Win32:DNSChanger-VJ [Trj] 0.74 % NEW
5 Trojan.AutorunINF.Gen 0.73 % 下降（10月3位）
6 Trojan.Wimad.Gen.1 0.61 % 下降（10月2位）
7 Java.Trojan.Downloader.OpenConnection.AI 0.44 % NEW（再登場）
8 Application.Keygen.BG 0.42 % NEW
9 Gen:Variant.Adware.Hotbar.1 0.37 % NEW（再登場）
10 PDF:Exploit.JS.V 0.33% NEW
注：「新」は先月の上位10になかったもの。「やや上昇」は先月より1-
2位上昇、「同」は先月と同位、「やや下降」は先月より1-
2位下降、「下降」は先月より3位以上の下降

この11月度のマルウェア活動の特徴は、三点にまとめることができます。

（１）脆弱性を狙った攻撃
個人のパソコンはもちろん、企業や官庁等への標的型攻撃も大半は脆弱性を衝いて侵入しており、今年もっとも目立ったマルウェア攻撃は、脆弱性を狙ったものであったと言えます。11月も、1位「Java.Exploit.CVE-2010-0840.E」、2位「Exploit.CplLnk.Gen」、3位「Worm.Autorun.VHG」、7位「Java.Trojan.Downloader.OpenConnection.AI」、10位「PDF:Exploit.JS.V」といったマルウェアが上位にランクインされました。

（２）USBメモリからの侵入
USBメモリの自動起動を使った攻撃は、外部ネットワークにつながっていないパソコンにまで感染被害を及ぼすという意味で、大変に危険な手口です。昨年イランの核施設に侵入したスタクスネットもUSBメモリからの感染が最初のきっかけでした。2位「Exploit.CplLnk.Gen」、3位「Worm.Autorun.VHG」、5位「Trojan.AutorunINF.Gen」が該当します。

（３）ファイル共有ネットワーク関連の攻撃
ファイル共有ソフトに関連したマルウェア攻撃は、「山田ウイルス」や「タコイカウイルス」など、日本でも頻繁に見られてきましたが、今も減少しているわけではなく、多数発見され続けています。6位「Trojan.Wimad.Gen.1」と8位「Application.Keygen.BG」が該当し、9位「Gen:Varia

nt.Adware.Hotbar.1」もフリーの動画コーデックのダウンロードを通じて侵入するため、ジャンルが近いと言えます。

これらの攻撃への対策として、特に気をつけたいのは、以下の五点です。

≪年末に向けたパソコンのセキュリティ対策のための5つのポイント≫

（１）OSや基本ソフト、メーラー、ブラウザ
バージョン情報を点検し、最新の状態にしましょう。

（２）USBメモリ
感染を避けるために性能の高いインターネットセキュリティ製品を使いましょう。

（３）ファイル共有ネットワーク
無数の危険がありますので、一般的な利用を控えることをお勧めします。

（４）違法キージェネレータ
法的にも、マルウェア感染の可能性としても、利用すべきではないでしょう。

（５）動画コーデック
フリーのコーデックを装うマルウェアに気をつけましょう。

年末には、マルウェア攻撃の増加が見込まれます。いつも以上に基本的な対策を怠らないようにすることを、G Dataはお勧めします。

≪上位10種のマルウェアについて≫

1 Java.Exploit.CVE-2010-0840.E
このJavaベースのマルウェア・プログラムは、CVE-2010-0840脆弱性を利用しようとするダウンロード・アプレットであり、サンドボックスの保護機構の裏をかき、かつコンピューター上に新たにマルウェアを追加ダウンロードします。そして、アプレットが一度サンドボックスをだましてしまえば、dllファイルのダウンロードが可能になります。このファイルは直ちには実行されませんが、Microsoft Register Server (regsvr32)のヘルプを伴うサービスとして登録され、後にシステムが立ち上がる際に自動的に開始されます。

2 Exploit.CplLnk.Gen
このエクスプロイトは、ウィンドウズのショートカットのプロセスにおいて.lnkや.pifファイルが不完全であることが確認された場合に使用され、2010年半ば以降、CVE-2010-2568（Stuxnetも利用した脆弱性）して知られています。ショートカットリンクを正しく処理しないことで任意のコードの実行を許し、偽装ショートカットファイル(.lnk)をウィンドウズのエクスプローラーでアイコン表示することにより、攻撃者のコードが実行されます。このコードは、ローカルのファイルシステム(たとえば、リムーバブル記憶装置から)から、あるいは、インターネット上のWebDAVシェアによってロードされます。

3 Worm.Autorun.VHG
ワーム型で、ウィンドウズOSの自動実行機能（autorun.inf）を使って拡散します。USBメモリや

外付ハードディスクドライブなどを介して感染します。「CVE-2008-4250」という脆弱性を悪用しています。

＊以下4-10位のマルウェアの詳細については、下記URLからお読みください。
http://www.gdata.co.jp/press/

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。2011年にはアンドロイド端末向けのセキュリティアプリも発売しました。

＊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