＃以下記載内容は、シマンテック セキュリティレスポンス ブログを翻訳。
http://www.symantec.com/connect/blogs/new-obfuscated-scripts-wild-lgpl

/*LGPL*/ で始まる新しい難読化コードが出現

昨年 12 月より、Web サイトに不正な JavaScript が貼り付けられ、Web サイトが改ざんされるという被害が相次いでいます。このスクリプトには 2 種類あり、それぞれ以下のような記述で始まります。

<script>/*GNU GPL*/ try{window.onload = function(){var ～
<script>/*CODE1*/ try{window.onload = function(){var ～

ところが今回、これとは異なる新しいバージョンが見つかりました。以前、"/*GNU GPL*/" で始まるスクリプトで改ざんされていたサイトの 1 つが、最近になって "/*LGPL*/" で始まるスクリプトに書き換えられていることが確認されました。

難読化されたこのスクリプトの開始部分は、次のような記述となっています。

<script>/*LGPL*/ try{ window.onload = function(){var C1nse3sk8o41s = document.createElement('s&c^$#r))i($p@&t^&'.repl

難読化を解除したあとに出てくる URL は下記のようなものです。

hxxp://free-fr.rapidshare.com.hotlinkimage-com.thechocolateweb.ru:8080/51job.com/51job.com/redtube.com/gittigidiyor.com/google.com/

良く知られているドメイン名を URL に使うことによって、攻撃者は保護メカニズムを迂回しようとしていることが読み取れます。上記の例では実際のドメイン名は thechocolateweb.ru に帰結し、他に表示されている様々な URL は関係しません。

ペイロード自体は昨年の攻撃からそれほど変化していません。ユーザーが改ざんされたサイトにアクセスすると、不正な JavaScript によって別の JavaScript がロードされます。この 2 番目の JavaScript は、2 つのリンクを含む iframe ページを開きます。1 つは Trojan.Pidief.H または Bloodhound.Exploit.288 として検出される不正な PDF ファイルへのリンクで（どちらに検

出されるかはアクセスする URL によって異なります)、もう 1 つは Downloader として検出される不正な JAR(Java ARchive)ファイルへのリンクです。

これら 2 つのファイルは、以下の脆弱性を利用してコンピュータへのマルウェア感染を試みます。

- Adobe Acrobat および Reader の任意のコード実行およびセキュリティに関する複数の脆弱性(BID 27641)
- Adobe Reader および Acrobat の 'newplayer()' JavaScript メソッドによるリモートコード実行の脆弱性(BID 37331)
- Sun Java Runtime Environment および Java Development Kit のセキュリティに関する複数の脆弱性(BID 32608)

なお、BID 37331 のパッチは 1 月 12 日の提供予定となっているため、それまでは Adobe Reader の JavaScript を無効にしておいた方がよいかもしれません。

最終的なペイロードには、Trojan.Bredolab や Trojan.Zbot などのマルウェアをはじめ、PrivacyCenter などのセキュリティリスク、およびその他多数のミスリーディングアプリケーション(Trojan.FakeAV などとして検出)が含まれます。ウイルス定義ファイルは頻繁に更新されているので、常に最新の状態に保つよう注意してください。

また、シマンテックではこの新しい不正な JavaScript をはじめ、同様のコードを含むスクリプトを汎用的に検出するウイルス定義「Trojan.Malscript.B」をリリースしました。