2015 年 9 月 8 日
株式会社セキュアソフト

Sniper による対策：Adobe Flash Player の脆弱性を利用した悪性コード

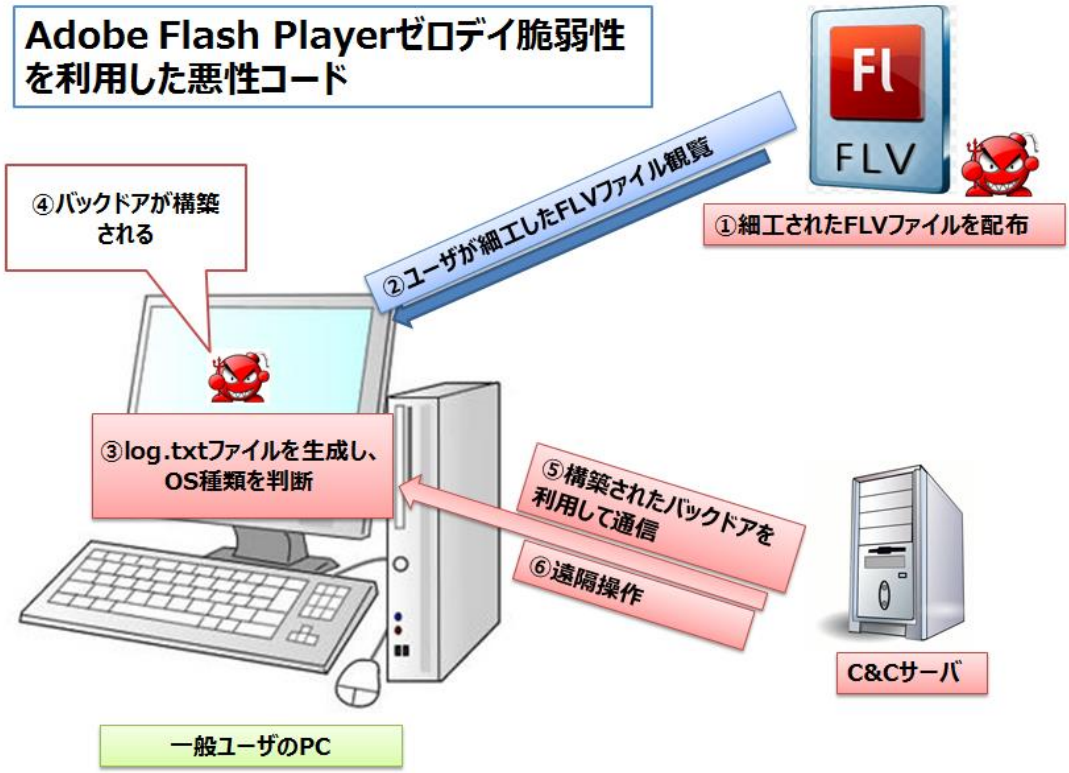
1. はじめに

2015 年 7 月にイタリアの企業である「Hacking Team」が攻撃を受けました。様々な機密情報が漏えいした結果、2 つの脆弱性「CVE-2015-5122」、「CVE-2015-5123」についても確認されています。これらの 2 つの脆弱性は Adobe Flash Player に関連するもので、「CVE-2015-5122」の脆弱性を利用して悪性コードを配布する攻撃が確認されています。本レポートではこの攻撃方法の解説と Sniper による対策に関してご案内いたします。

2. 攻撃方法

攻撃は IsSpace というバックドア系の悪性コードにより行われます。この悪性コードは NFLog というバックドア系と類似したタイプとなります。

IsSpace の悪性コードは Adobe Flash Player の脆弱性を利用した不正な FLV ファイルにより配布されます。 IsSpace バックドアが対象システムにインストールされると、特定のイベントを生成し、自分自身の不正行為を隠しながら実行します。対象 OS の種類を確認するため、特定の位置に log.txt というファイルを生成し判別します。このファイルを利用し対象システム OS を識別し、C&C サーバとのバックドアを構築します。攻撃者はユーザシステムにリモートアクセスして不正行為を行います。



【図 1】 IsSpace 悪性コードの攻撃方法

3. 対象システム

・Adobe Flash Player18.0.0.203 およびそれ以前のバージョン（Windows 版および Macintosh 版）
・Adobe Flash Player18.0.0.204 およびそれ以前のバージョン（Google Chrome がインストールされた Linux）
・Adobe Flash Player Extended Support Release 13.0.0.302 およびそれ以前の 13.x バージョン
（Windows 版および Macintosh 版）
・Adobe Flash Player Extended Support Release11.2.202.481 およびそれ以前の 11.x バージョン
（Linux 版）

4. 対応方法

① クライアント PC 側の対策

・悪性コードが実行された環境の場合、数個所に生成された悪性コードファイルの検索、削除

・Adobe Flash Player のアップデート

次の URL にアクセスし、Adobe Flash Player の最新版をインストールします。

https://get.adobe.com/jp/flashplayer/

・Adobe Flash Player の無効化

Adobe Flash Player には様々な脆弱性が確認されており、必要でない場合は無効化することも有効な対策です。
無効化の方法については各ブラウザの情報をご確認願います。

② ネットワーク側の対策（Sniper ONE および Sniper IPS による対策）

2015 年 9 月 2 日にリリースされた以下のシグネチャを利用して検知・遮断する事が可能です。

シグネチャ	説明
Win32/Backdoor.IsSpace.InitialConnection	IsSpace バックドアにより発生する C&C サーバとの通信を検知・遮断します。

以上