FileInsightを使ったパッカー情報収集

シマンテック役務からの情報提供

山本様

お疲れ様です。
シマンテックの山下です。

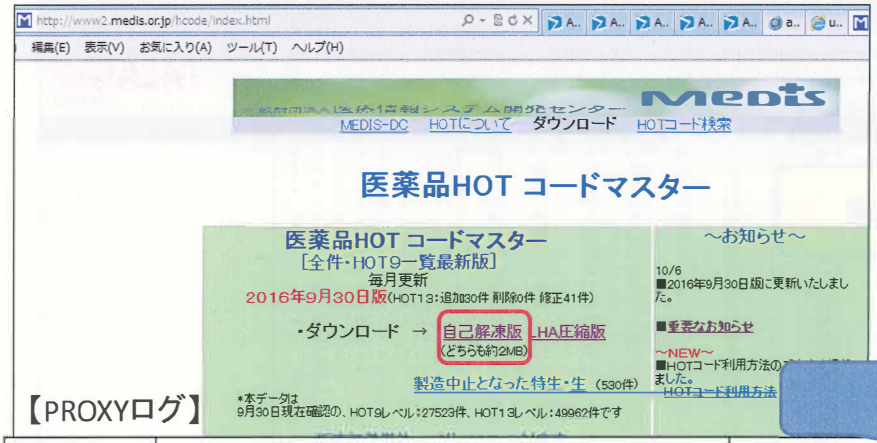
昨日の加入からの通信で気になるものがあったので、詳細を記載します。

検知シグネチャ：IPS-B : UPX_Packed_Executable
検知時刻：11:31, 18:49, 18:51
発信元：10.116.0.28（陸自：三宿：陸自インターネット）
アクセス先：http://www2.medis.or.jp/hcode/moto_data/h20160930.exe
ステータスコード：200

上記のexeファイルをVirusTotalにかけた所、2件検知されました。
検知名：
Win32.Trojan.WisdomEyes.16070401.9500.9524（検知AV名：Baidu）
Trojan.Generic.aamcm（検知AV名：Jiangmin）

シマンテックやトレンド、マカフィーなどの大手が検知している訳ではないので、
信憑性は低いかもしれませんが、念のため情報共有させていただきます。
ちなみに、SEPでウイルスチェックをした所、検知無しでした。

以上、よろしくお願い致します。



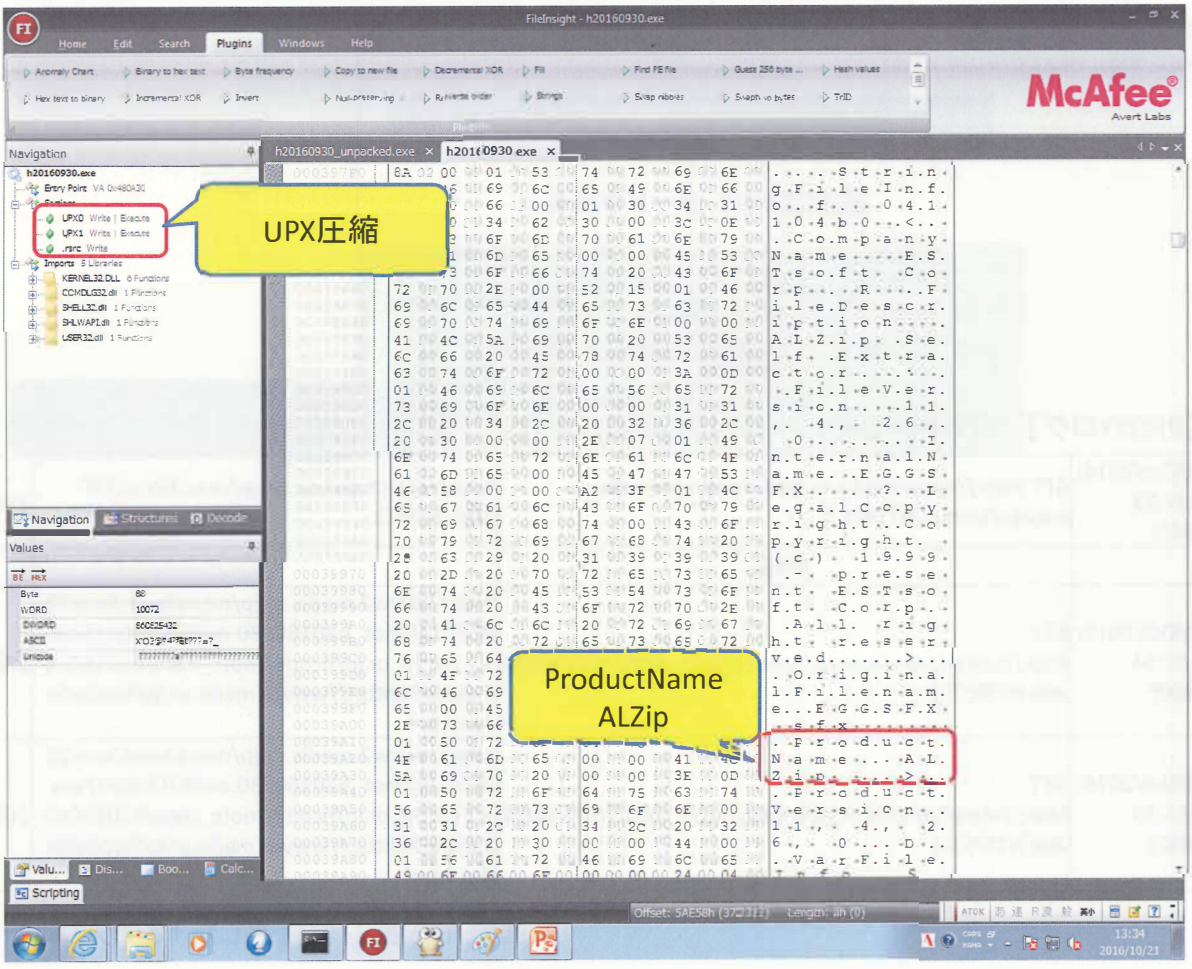
「HOT13」※で検索

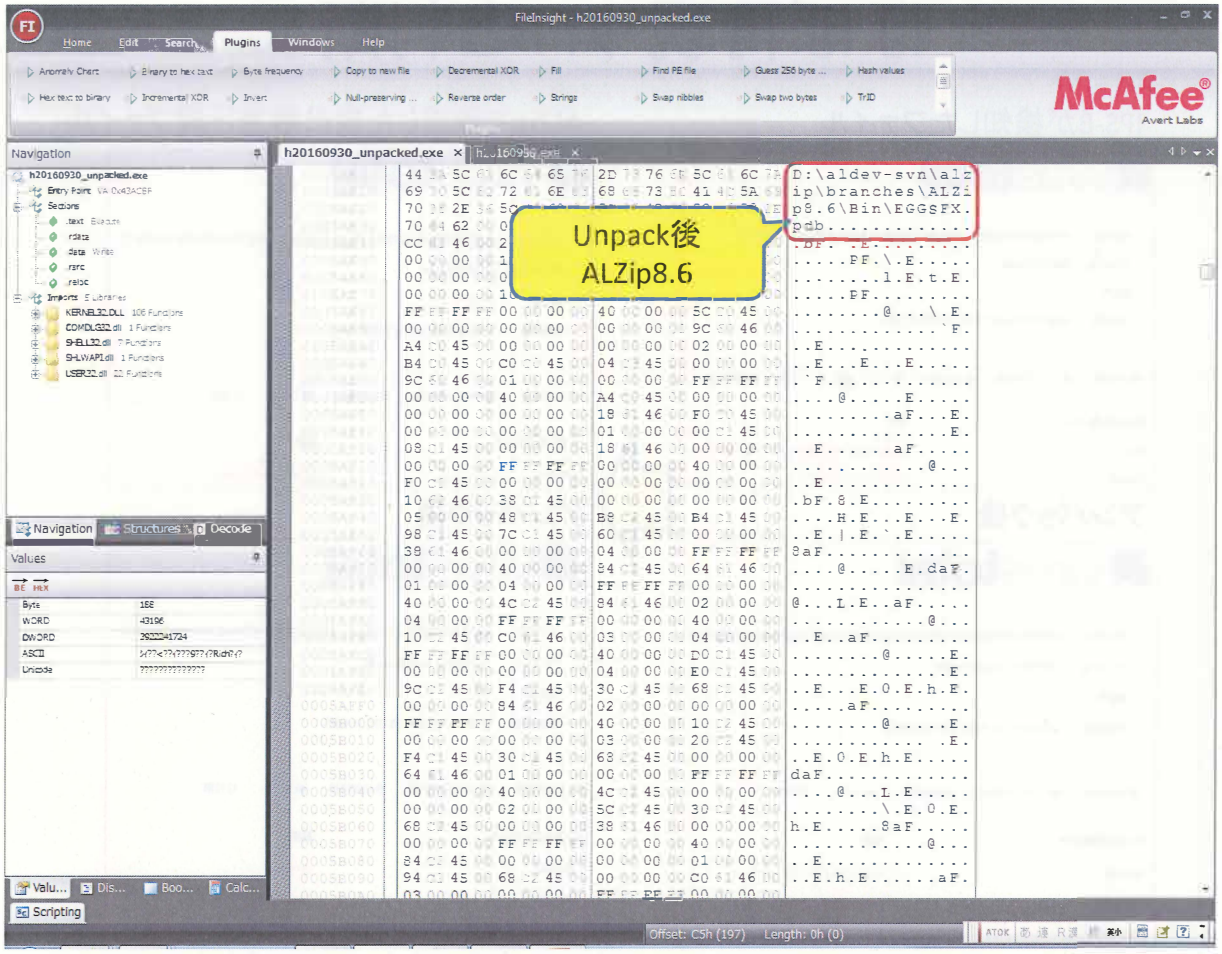
【PROXYログ】

[20/Oct/2016:18:47:53 +0900]	GET http://www.medis.or.jp/4_hyojyun/medis-master/terms/ HTTP/1.1	http://search.yahoo.co.jp/search?ei=UTF-8&p=HOT13	200
	中略		
[20/Oct/2016:18:49:44 +0900]	GET http://www2.medis.or.jp/hcode/moto_data/h20160930.exe HTTP/1.1	http://www2.medis.or.jp/mousikomi/anw20060607.cgi?hot_h20160930.exe%2Chttp://www2.medis.or.jp/hcode/moto_data/h20160930.exe%2Chttp://www2.medis.or.jp/hcode/index.html	200
[20/Oct/2016:18:51:33 +0900]	GET http://www2.medis.or.jp/hcode/moto_data/h20160930.exe HTTP/1.1	http://www2.medis.or.jp/mousikomi/anw20060607.cgi?hot_h20160930.exe%2Chttp://www2.medis.or.jp/hcode/moto_data/h20160930.exe%2Chttp://www2.medis.or.jp/hcode/index.html	200

※医療用医薬品に付与した13ケタのコード

不審な動作は確認されず

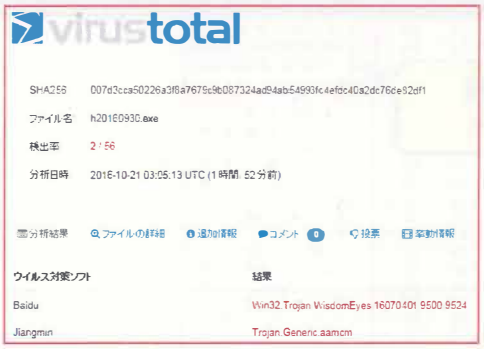




ALZipをDLし、自己解凍圧縮ファイルを作成

ほぼ再現→FPと判断

IPS-Bが検知したファイル



ALZipで作成した自己解凍圧縮ファイル

アンパック後

アンパック後