

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。

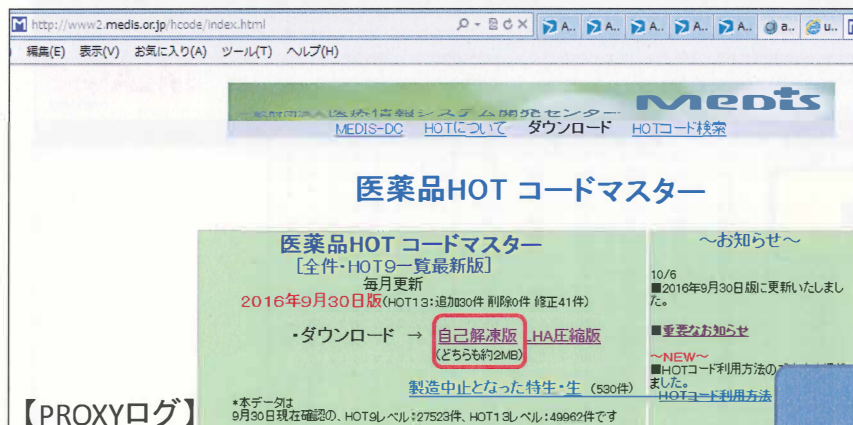
検知シグネチャ: IPS-B : UPX_Packed_Executable
検知時刻: 11:31, 18:49, 18:51
発信元: 10.116.0.28 (陸自: 三宿: 陸自インターネット)
アクセス先: http://www2.medis.or.jp/hcode/moto_data/h20160930.exe
ステータスコード: 200

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。

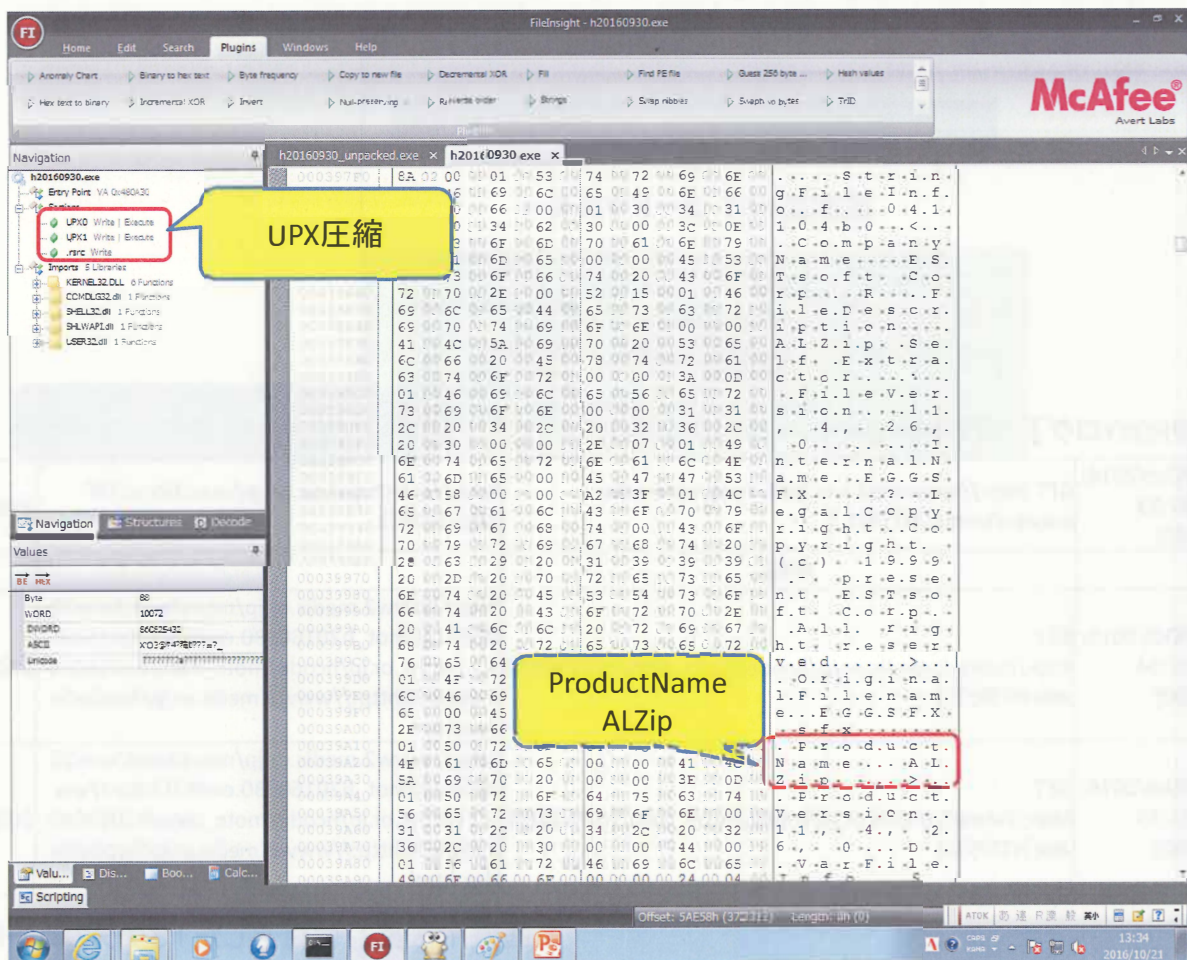
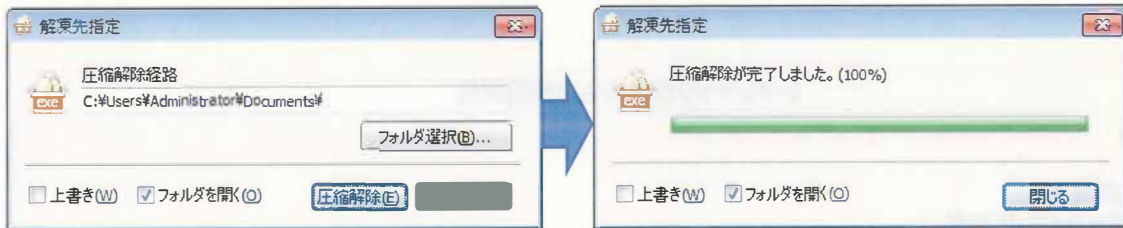
以上、よろしくお願い致します。



[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/anw200607.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/anw200607.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



ほぼ再現→FPと判断

IPS-Bが検知したファイル



SHA256 007d5cca50226a3f6a7675c9e087324ad54ab54993fc4ef0c40a2d76e62df1
ファイル名 h20160930.exe
検出率 2 / 56
分析日時 2016-10-21 03:05:13 UTC (1時間 52分前)

分析結果 ファイルの詳細 追加情報 コメント 投票 家族情報

ウイルス対策ソフト 結果
Baidu Win32.Trojan.WisdomEyes.16070401.9500.9524
Jiangmin Trojan.Generic.aamcm

ALZipで作成した自己解凍圧縮ファイル



SHA256 aee64a575f7c35b6c1bc51595c34cd7814ee083b4a213a1d33370e144c798c10
ファイル名 h20160930.exe
検出率 1 / 56
分析日時 2016-10-21 02:42:11 UTC (0分前)

分析結果 ファイルの詳細 追加情報 コメント 投票

ウイルス対策ソフト 結果
Jiangmin Trojan.Generic.aamcm

アンパック後



SHA256 f4824bf5d971d8503b22a96865509ad107d56e55d9b352473daacd2585a495ff
ファイル名 h20160930_unpacked.exe
検出率 3 / 56
分析日時 2016-10-21 01:54:14 UTC (50分前)

分析結果 ファイルの詳細 追加情報 コメント 投票

ウイルス対策ソフト 結果
Invincea trojandropper.win32.sventore.a
Jiangmin Trojan.Generic.aamcm
Qhoo-360 HEUR:QVM10.1.0000.Malware.Gen

アンパック後



SHA256 266424c9870d61141428bdeacc83601cf683e5e36214a8cd47521fa95f03752c
ファイル名 h20160930_unpacked.exe
検出率 3 / 52
分析日時 2016-10-21 02:46:38 UTC (1分前)

分析結果 ファイルの詳細 追加情報 コメント 投票

ウイルス対策ソフト 結果
Invincea generic.a
Jiangmin Trojan.Generic.aamcm
Qhoo-360 HEUR:QVM10.1.0000.Malware.Gen

類似ファイル検索結果

ファイル名	検出率	分析日時
h20160930.exe	2 / 56	2016-10-21 03:05:13 UTC (1時間 52分前)
h20160930_unpacked.exe	3 / 56	2016-10-21 01:54:14 UTC (50分前)
h20160930_unpacked.exe	3 / 52	2016-10-21 02:46:38 UTC (1分前)