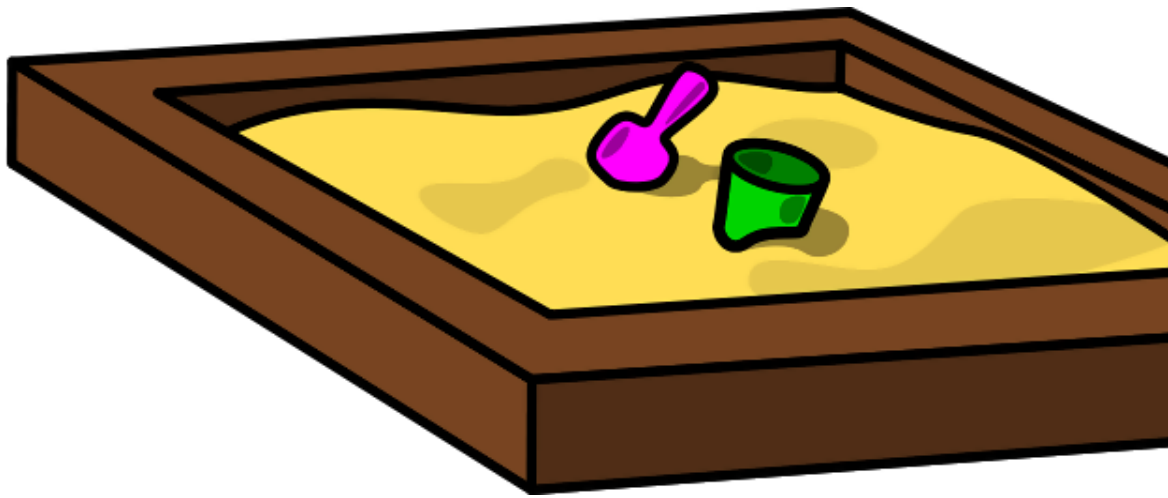


绿盟科技博客 (<http://blog.nsfocus.net/>)

巨人背后的安全专家

新的沙盒逃逸技术

2015-11-17 (<http://blog.nsfocus.net/escaping-sandbox-technology/>) zz (<http://blog.nsfocus.net/author/zz/>)



👁 阅读: 2,991

自从诞生沙盒技术来阻挡恶意软件之后, 恶意软件也在时刻想办法逃避沙盒, 所谓沙盒逃逸技术。关于绿盟科技防火墙的几个 (<http://blog.nsfocus.net/>) 安全研究员做分析的过程中, 发现Upatre木马新变种采用了新的逃逸技术。 (<http://blog.nsfocus.net/generation-firewall/>)

Upatre沙盒逃逸新技术

Upatre木马使用了一些新的逃逸技术, 来逃逸动态沙盒引擎的检查, 这些技巧都非常的简单, 但是非常的有效。目前, VirusTotal上Upatre的检出率并不高, 此次的新变种就检测不出来, 这说明现在的恶意越来越有办法了。

目前在恶意软件上加壳倒是越来越少了, 因为加壳容易引起杀软引擎的注意, 相反地目前的行边修改自身代码的方法来躲避杀软, 不执行的话看起来就像是一个正常的软件, 而真正执行起来代码却主文了, 这也算是一种进化。

下面说说两种 Upatre 使用的沙盒逃逸的办法, 样本MD5: ac3558b973402ef6a27e03c391f20533

检查开机时间

一般使用沙盒的分析引擎的做法都是安装一个全新的系统, 做系统镜像。然后在检查的时候加载镜像, 执行操作。而开机的时间往往都被忽略了, 基本都不会超过10分钟。

Upatre 样本所采取的方法是利用GetTickCount 获取开机的毫秒数, 当开机时间小于12分钟 是不执行恶意的行为。

- 1 乌克兰电厂攻击事件分析 (<http://blog.nsfocus.net/plant-attack-analysis-pro>)
 - 2 FortiGate SSH漏洞分析及 (<http://blog.nsfocus.net/fvulnerability-analysis-pro>)
 - 3 Dedecms远程写文件漏洞 (<http://blog.nsfocus.net/cvuln/>)
 - 4 虚拟防火墙典型部署 (<http://blog.nsfocus.net/vtypical-deployment/>)
 - 5 文档安全加密系统的实现 (<http://blog.nsfocus.net/document-security-encryption-approach/>)
 - 6 浏览器fuzz框架介绍 (<http://blog.nsfocus.net/fuzzing/>)
 - 7 关于绿盟科技防火墙的几个 (<http://blog.nsfocus.net/generation-firewall/>)
 - 8 动态加解密技术综述 (<http://blog.nsfocus.net/encryption-technology-re>)
- 选择操作系统
Windows 8.1
win8_debug
win8_1
win8_2
win8_3
win8_4
win8_5
win8_6
win8_7
win8_8
win8_9
win8_10
win8_11
win8_12
win8_13
win8_14
win8_15
win8_16
win8_17
win8_18
win8_19
win8_20
win8_21
win8_22
win8_23
win8_24
win8_25
win8_26
win8_27
win8_28
win8_29
win8_30
win8_31
win8_32
win8_33
win8_34
win8_35
win8_36
win8_37
win8_38
win8_39
win8_40
win8_41
win8_42
win8_43
win8_44
win8_45
win8_46
win8_47
win8_48
win8_49
win8_50
win8_51
win8_52
win8_53
win8_54
win8_55
win8_56
win8_57
win8_58
win8_59
win8_60
win8_61
win8_62
win8_63
win8_64
win8_65
win8_66
win8_67
win8_68
win8_69
win8_70
win8_71
win8_72
win8_73
win8_74
win8_75
win8_76
win8_77
win8_78
win8_79
win8_80
win8_81
win8_82
win8_83
win8_84
win8_85
win8_86
win8_87
win8_88
win8_89
win8_90
win8_91
win8_92
win8_93
win8_94
win8_95
win8_96
win8_97
win8_98
win8_99
win8_100
win8_101
win8_102
win8_103
win8_104
win8_105
win8_106
win8_107
win8_108
win8_109
win8_110
win8_111
win8_112
win8_113
win8_114
win8_115
win8_116
win8_117
win8_118
win8_119
win8_120
win8_121
win8_122
win8_123
win8_124
win8_125
win8_126
win8_127
win8_128
win8_129
win8_130
win8_131
win8_132
win8_133
win8_134
win8_135
win8_136
win8_137
win8_138
win8_139
win8_140
win8_141
win8_142
win8_143
win8_144
win8_145
win8_146
win8_147
win8_148
win8_149
win8_150
win8_151
win8_152
win8_153
win8_154
win8_155
win8_156
win8_157
win8_158
win8_159
win8_160
win8_161
win8_162
win8_163
win8_164
win8_165
win8_166
win8_167
win8_168
win8_169
win8_170
win8_171
win8_172
win8_173
win8_174
win8_175
win8_176
win8_177
win8_178
win8_179
win8_180
win8_181
win8_182
win8_183
win8_184
win8_185
win8_186
win8_187
win8_188
win8_189
win8_190
win8_191
win8_192
win8_193
win8_194
win8_195
win8_196
win8_197
win8_198
win8_199
win8_200
win8_201
win8_202
win8_203
win8_204
win8_205
win8_206
win8_207
win8_208
win8_209
win8_210
win8_211
win8_212
win8_213
win8_214
win8_215
win8_216
win8_217
win8_218
win8_219
win8_220
win8_221
win8_222
win8_223
win8_224
win8_225
win8_226
win8_227
win8_228
win8_229
win8_230
win8_231
win8_232
win8_233
win8_234
win8_235
win8_236
win8_237
win8_238
win8_239
win8_240
win8_241
win8_242
win8_243
win8_244
win8_245
win8_246
win8_247
win8_248
win8_249
win8_250
win8_251
win8_252
win8_253
win8_254
win8_255
win8_256
win8_257
win8_258
win8_259
win8_260
win8_261
win8_262
win8_263
win8_264
win8_265
win8_266
win8_267
win8_268
win8_269
win8_270
win8_271
win8_272
win8_273
win8_274
win8_275
win8_276
win8_277
win8_278
win8_279
win8_280
win8_281
win8_282
win8_283
win8_284
win8_285
win8_286
win8_287
win8_288
win8_289
win8_290
win8_291
win8_292
win8_293
win8_294
win8_295
win8_296
win8_297
win8_298
win8_299
win8_300
win8_301
win8_302
win8_303
win8_304
win8_305
win8_306
win8_307
win8_308
win8_309
win8_310
win8_311
win8_312
win8_313
win8_314
win8_315
win8_316
win8_317
win8_318
win8_319
win8_320
win8_321
win8_322
win8_323
win8_324
win8_325
win8_326
win8_327
win8_328
win8_329
win8_330
win8_331
win8_332
win8_333
win8_334
win8_335
win8_336
win8_337
win8_338
win8_339
win8_340
win8_341
win8_342
win8_343
win8_344
win8_345
win8_346
win8_347
win8_348
win8_349
win8_350
win8_351
win8_352
win8_353
win8_354
win8_355
win8_356
win8_357
win8_358
win8_359
win8_360
win8_361
win8_362
win8_363
win8_364
win8_365
win8_366
win8_367
win8_368
win8_369
win8_370
win8_371
win8_372
win8_373
win8_374
win8_375
win8_376
win8_377
win8_378
win8_379
win8_380
win8_381
win8_382
win8_383
win8_384
win8_385
win8_386
win8_387
win8_388
win8_389
win8_390
win8_391
win8_392
win8_393
win8_394
win8_395
win8_396
win8_397
win8_398
win8_399
win8_400
win8_401
win8_402
win8_403
win8_404
win8_405
win8_406
win8_407
win8_408
win8_409
win8_410
win8_411
win8_412
win8_413
win8_414
win8_415
win8_416
win8_417
win8_418
win8_419
win8_420
win8_421
win8_422
win8_423
win8_424
win8_425
win8_426
win8_427
win8_428
win8_429
win8_430
win8_431
win8_432
win8_433
win8_434
win8_435
win8_436
win8_437
win8_438
win8_439
win8_440
win8_441
win8_442
win8_443
win8_444
win8_445
win8_446
win8_447
win8_448
win8_449
win8_450
win8_451
win8_452
win8_453
win8_454
win8_455
win8_456
win8_457
win8_458
win8_459
win8_460
win8_461
win8_462
win8_463
win8_464
win8_465
win8_466
win8_467
win8_468
win8_469
win8_470
win8_471
win8_472
win8_473
win8_474
win8_475
win8_476
win8_477
win8_478
win8_479
win8_480
win8_481
win8_482
win8_483
win8_484
win8_485
win8_486
win8_487
win8_488
win8_489
win8_490
win8_491
win8_492
win8_493
win8_494
win8_495
win8_496
win8_497
win8_498
win8_499
win8_500
win8_501
win8_502
win8_503
win8_504
win8_505
win8_506
win8_507
win8_508
win8_509
win8_510
win8_511
win8_512
win8_513
win8_514
win8_515
win8_516
win8_517
win8_518
win8_519
win8_520
win8_521
win8_522
win8_523
win8_524
win8_525
win8_526
win8_527
win8_528
win8_529
win8_530
win8_531
win8_532
win8_533
win8_534
win8_535
win8_536
win8_537
win8_538
win8_539
win8_540
win8_541
win8_542
win8_543
win8_544
win8_545
win8_546
win8_547
win8_548
win8_549
win8_550
win8_551
win8_552
win8_553
win8_554
win8_555
win8_556
win8_557
win8_558
win8_559
win8_560
win8_561
win8_562
win8_563
win8_564
win8_565
win8_566
win8_567
win8_568
win8_569
win8_570
win8_571
win8_572
win8_573
win8_574
win8_575
win8_576
win8_577
win8_578
win8_579
win8_580
win8_581
win8_582
win8_583
win8_584
win8_585
win8_586
win8_587
win8_588
win8_589
win8_590
win8_591
win8_592
win8_593
win8_594
win8_595
win8_596
win8_597
win8_598
win8_599
win8_600
win8_601
win8_602
win8_603
win8_604
win8_605
win8_606
win8_607
win8_608
win8_609
win8_610
win8_611
win8_612
win8_613
win8_614
win8_615
win8_616
win8_617
win8_618
win8_619
win8_620
win8_621
win8_622
win8_623
win8_624
win8_625
win8_626
win8_627
win8_628
win8_629
win8_630
win8_631
win8_632
win8_633
win8_634
win8_635
win8_636
win8_637
win8_638
win8_639
win8_640
win8_641
win8_642
win8_643
win8_644
win8_645
win8_646
win8_647
win8_648
win8_649
win8_650
win8_651
win8_652
win8_653
win8_654
win8_655
win8_656
win8_657
win8_658
win8_659
win8_660
win8_661
win8_662
win8_663
win8_664
win8_665
win8_666
win8_667
win8_668
win8_669
win8_670
win8_671
win8_672
win8_673
win8_674
win8_675
win8_676
win8_677
win8_678
win8_679
win8_680
win8_681
win8_682
win8_683
win8_684
win8_685
win8_686
win8_687
win8_688
win8_689
win8_690
win8_691
win8_692
win8_693
win8_694
win8_695
win8_696
win8_697
win8_698
win8_699
win8_700
win8_701
win8_702
win8_703
win8_704
win8_705
win8_706
win8_707
win8_708
win8_709
win8_710
win8_711
win8_712
win8_713
win8_714
win8_715
win8_716
win8_717
win8_718
win8_719
win8_720
win8_721
win8_722
win8_723
win8_724
win8_725
win8_726
win8_727
win8_728
win8_729
win8_730
win8_731
win8_732
win8_733
win8_734
win8_735
win8_736
win8_737
win8_738
win8_739
win8_740
win8_741
win8_742
win8_743
win8_744
win8_745
win8_746
win8_747
win8_748
win8_749
win8_750
win8_751
win8_752
win8_753
win8_754
win8_755
win8_756
win8_757
win8_758
win8_759
win8_760
win8_761
win8_762
win8_763
win8_764
win8_765
win8_766
win8_767
win8_768
win8_769
win8_770
win8_771
win8_772
win8_773
win8_774
win8_775
win8_776
win8_777
win8_778
win8_779
win8_780
win8_781
win8_782
win8_783
win8_784
win8_785
win8_786
win8_787
win8_788
win8_789
win8_790
win8_791
win8_792
win8_793
win8_794
win8_795
win8_796
win8_797
win8_798
win8_799
win8_800
win8_801
win8_802
win8_803
win8_804
win8_805
win8_806
win8_807
win8_808
win8_809
win8_810
win8_811
win8_812
win8_813
win8_814
win8_815
win8_816
win8_817
win8_818
win8_819
win8_820
win8_821
win8_822
win8_823
win8_824
win8_825
win8_826
win8_827
win8_828
win8_829
win8_830
win8_831
win8_832
win8_833
win8_834
win8_835
win8_836
win8_837
win8_838
win8_839
win8_840
win8_841
win8_842
win8_843
win8_844
win8_845
win8_846
win8_847
win8_848
win8_849
win8_850
win8_851
win8_852
win8_853
win8_854
win8_855
win8_856
win8_857
win8_858
win8_859
win8_860
win8_861
win8_862
win8_863
win8_864
win8_865
win8_866
win8_867
win8_868
win8_869
win8_870
win8_871
win8_872
win8_873
win8_874
win8_875
win8_876
win8_877
win8_878
win8_879
win8_880
win8_881
win8_882
win8_883
win8_884
win8_885
win8_886
win8_887
win8_888
win8_889
win8_890
win8_891
win8_892
win8_893
win8_894
win8_895
win8_896
win8_897
win8_898
win8_899
win8_900
win8_901
win8_902
win8_903
win8_904
win8_905
win8_906
win8_907
win8_908
win8_909
win8_910
win8_911
win8_912
win8_913
win8_914
win8_915
win8_916
win8_917
win8_918
win8_919
win8_920
win8_921
win8_922
win8_923
win8_924
win8_925
win8_926
win8_927
win8_928
win8_929
win8_930
win8_931
win8_932
win8_933
win8_934
win8_935
win8_936
win8_937
win8_938
win8_939
win8_940
win8_941
win8_942
win8_943
win8_944
win8_945
win8_946
win8_947
win8_948
win8_949
win8_950
win8_951
win8_952
win8_953
win8_954
win8_955
win8_956
win8_957
win8_958
win8_959
win8_960
win8_961
win8_962
win8_963
win8_964
win8_965
win8_966
win8_967
win8_968
win8_969
win8_970
win8_971
win8_972
win8_973
win8_974
win8_975
win8_976
win8_977
win8_978
win8_979
win8_980
win8_981
win8_982
win8_983
win8_984
win8_985
win8_986
win8_987
win8_988
win8_989
win8_990
win8_991
win8_992
win8_993
win8_994
win8_995
win8_996
win8_997
win8_998
win8_999
win8_1000
win8_1001
win8_1002
win8_1003
win8_1004
win8_1005
win8_1006
win8_1007
win8_1008
win8_1009
win8_1010
win8_1011
win8_1012
win8_1013
win8_1014
win8_1015
win8_1016
win8_1017
win8_1018
win8_1019
win8_1020
win8_1021
win8_1022
win8_1023
win8_1024
win8_1025
win8_1026
win8_1027
win8_1028
win8_1029
win8_1030
win8_1031
win8_1032
win8_1033
win8_1034
win8_1035
win8_1036
win8_1037
win8_1038
win8_1039
win8_1040
win8_1041
win8_1042
win8_1043
win8_1044
win8_1045
win8_1046
win8_1047
win8_1048
win8_1049
win8_1050
win8_1051
win8_1052
win8_1053
win8_1054
win8_1055
win8_1056
win8_1057
win8_1058
win8_1059
win8_1060
win8_1061
win8_1062
win8_1063
win8_1064
win8_1065
win8_1066
win8_1067
win8_1068
win8_1069
win8_1070
win8_1071
win8_1072
win8_1073
win8_1074
win8_1075
win8_1076
win8_1077
win8_1078
win8_1079
win8_1080
win8_1081
win8_1082
win8_1083
win8_1084
win8_1085
win8_1086
win8_1087
win8_1088
win8_1089
win8_1090
win8_1091
win8_1092
win8_1093
win8_1094
win8_1095
win8_1096
win8_1097
win8_1098
win8_1099
win8_1100
win8_1101
win8_1102
win8_1103
win8_1104
win8_1105
win8_1106
win8_1107
win8_1108
win8_1109
win8_1110
win8_1111
win8_1112
win8_1113
win8_1114
win8_1115
win8_1116
win8_1117
win8_1118
win8_1119
win8_1120
win8_1121
win8_1122
win8_1123
win8_1124
win8_1125
win8_1126
win8_1127
win8_1128
win8_1129
win8_1130
win8_1131
win8_1132
win8_1133
win8_1134
win8_1135
win8_1136
win8_1137
win8_1138
win8_1139
win8_1140
win8_1141
win8_1142
win8_1143
win8_1144
win8_1145
win8_1146
win8_1147
win8_1148
win8_1149
win8_1150
win8_1151
win8_1152
win8_1153
win8_1154
win8_1155
win8_1156
win8_1157
win8_1158
win8_1159
win8_1160
win8_1161
win8_1162
win8_1163
win8_1164
win8_1165
win8_1166
win8_1167
win8_1168
win8_1169
win8_1170
win8_1171
win8_1172
win8_1173
win8_1174
win8_1175
win8_1176
win8_1177
win8_1178
win8_1179
win8_1180
win8_1181
win8_1182
win8_1183
win8_1184
win8_1185
win8_1186
win8_1187
win8_1188
win8_1189
win8_1190
win8_1191
win8_1192
win8_1193
win8_1194
win8_1195
win8_1196
win8_1197
win8_1198
win8_1199
win8_1200
win8_1201
win8_1202
win8_1203
win8_1204
win8_1205
win8_1206
win8_1207
win8_1208
win8_1209
win8_1210
win8_1211
win8_1212
win8_1213
win8_1214
win8_1215
win8_1216
win8_1217
win8_1218
win8_1219
win8_1220
win8_1221
win8_1222
win8_1223
win8_1224
win8_1225
win8_1226
win8_1227
win8_1228
win8_1229
win8_1230
win8_1231
win8_1232
win8_1233
win8_1234
win8_1235
win8_1236
win8_1237
win8_1238
win8_1239
win8_1240
win8_1241
win8_1242
win8_1243
win8_1244
win8_1245
win8_1246
win8_1247
win8_1248
win8_1249
win8_1250
win8_1251
win8_1252
win8_1253
win8_1254
win8_1255
win8_1256
win8_1257
win8_1258
win8_1259
win8_1260
win8_1261
win8_1262
win8_1263
win8_1264
win8_1265
win8_1266
win8_1267
win8_1268
win8_1269
win8_1270
win8_1271
win8_1272
win8_1273
win8_1274
win8_1275
win8_1276
win8_1277
win8_1278
win8_1279
win8_1280
win8_1281
win8_1282
win8_1283
win8_1284
win8_1285
win8_1286
win8_1287
win8_1288
win8_1289
win8_1290
win8_1291
win8_1292
win8_1293
win8_1294
win8_1295
win8_1296
win8_1297
win8_1298
win8_1299
win8_1300
win8_1301
win8_1302
win8_1303
win8_1304
win8_1305
win8_1306
win8_1307
win8_1308
win8_1309
win8_1310
win8_1311
win8_1312
win8_1313
win8_1314
win8_1315
win8_1316
win8_1317
win8_1318
win8_1319
win8_1320
win8_1321
win8_1322
win8_1323
win8_1324
win8_1325
win8_1326
win8_1327
win8_1328
win8_1329
win8_1330
win8_1331
win8_1332
win8_1333
win8_1334
win8_1335
win8_1336
win8_133

```
004013E3  B8 D8FED800  MOV EBX,0AD8FED8
004013E8  FF55 DC      CALL DWORD PTR SS:[ESP+24] ; kernel32.GetTickCount
004013ED  5BC3        CMP EAX,EBX
004013EE  0F82 6F020000 JB 00401632
00401632  9A 00       PUSH 0
00401634  FF55 F4     CALL DWORD PTR SS:[ESP+C] ; kernel32.ExitProcess
```

(<http://blog.nsfocus.net/wp-content/uploads/2015/11/Upatre样本.jpg>)

Upatre 样本

0xAFED8 是 720600毫秒 12分钟多一点，不到进程退出了。

检查鼠标位置

Upatre样本使用的第二种沙盒逃逸的方法是检查鼠标位置的变化，动态沙盒分析系统大多是自动化的系统，也就是不使用鼠标，如果Upatre样本检查到鼠标的位置没有发生变化，同样不会执行恶意行为。

```
0040197C  8085 0AFFFFFF lea eax,dword ptr ss:[ebp-0AFC]
00401982  50          push eax
00401983  FF95 20FFFFFF call dword ptr ss:[ebp-0A60] ; user32.GetCursorPos
00401989  8085 0CFFFFFF lea eax,dword ptr ss:[ebp-0AFC]
0040198F  50          push eax
00401990  FF95 20FFFFFF call dword ptr ss:[ebp-0A60] ; user32.GetCursorPos
00401996  8085 0AFFFFFF lea eax,dword ptr ss:[ebp-0AFC]
0040199C  8085 0CFFFFFF lea eax,dword ptr ss:[ebp-0AFC]
004019A2  3908        cmp eax,ebx
004019A4  74 06       je short 02.0040197C
```

(<http://blog.nsfocus.net/wp-content/uploads/2015/11/沙盒分析.jpg>)

沙盒分析

只要鼠标一动就退出循环，继续往下执行。

总结

最近出现的样本在反动态沙盒检测方面明显地进化了，针对性极强，不再局限于古老的 IsDebuggerPresent，而是利用PEB检查CPU核数等技术办法来检测，沙盒对抗估技术在后面的日子里一定会更加迅速的进化。

参考链接

<https://www.virustotal.com/en/file/7ef09594202e5b619ac0332ab122f722684e896f77a2b9839d13ba79f882243f/analysis/>
(<https://www.virustotal.com/en/file/7ef09594202e5b619ac0332ab122f722684e896f77a2b9839d13ba79f882243f/analysis/>)

致谢

非常感谢西安研究中心的同事提供的样本，同时感谢同事lzx在样本分析时给予的大力支持。

5
(<http://www.wumii.com/item/rLtofly>)

您可能也喜欢:





P)

动态加解密技术综述

(<http://blog.nsfocus.net/dynamic-encryption-technology-review/>)



数据安全保护之访问控制技术

(<http://blog.nsfocus.net/data-security-access-control-technology/>)



文档安全加密系统的实现方式

(<http://blog.nsfocus.net/implement-document-security-encryption-system-approach/>)



关于下一代防火墙的几个思考

(<http://blog.nsfocus.net/thoughts-next-generation-firewall/>)



再谈网络安全的自动化

(<http://blog.nsfocus.net/security-automation/>)

无关联推荐[?] (<http://www.wumii.com/widget/relatedItems>)

文章分类：漏洞分析 (<http://blog.nsfocus.net/category/vulnanalysis/>)

文章关键词：Upatre木马 (<http://blog.nsfocus.net/tag/upatre%E6%9C%A8%E9%A9%AC/>), 安全沙盒技术

(<http://blog.nsfocus.net/tag/%E5%AE%89%E5%85%A8%E6%B2%99%E7%9B%92%E6%8A%80%E6%9C%AF/>), 虚拟机逃逸技术

(<http://blog.nsfocus.net/tag/%E8%99%9A%E6%8B%9F%E6%9C%BA%E9%80%83%E9%80%B8%E6%8A%80%E6%9C%AF/>)

, 逃逸分析技术

(<http://blog.nsfocus.net/tag/%E9%80%83%E9%80%B8%E5%88%86%E6%9E%90%E6%8A%80%E6%9C%AF/>)

转载请注明“转自绿盟科技博客”： [permalink \(http://blog.nsfocus.net/escaping-sandbox-technology/\)](http://blog.nsfocus.net/escaping-sandbox-technology/).

← [Redis数据库漏洞防护 \(http://blog.nsfocus.net/redis-crackit-protection/\)](http://blog.nsfocus.net/redis-crackit-protection/)

[浏览器fuzz框架介绍 → \(http://blog.nsfocus.net/web-browser-fuzzing/\)](http://blog.nsfocus.net/web-browser-fuzzing/)

绿盟科技博客推荐文章

[Django任意代码执行漏洞分析 \(http://blog.nsfocus.net/django-code-execution-vulnerability/\)](http://blog.nsfocus.net/django-code-execution-vulnerability/) (13,267)

[绿盟科技网络攻防赛资料下载 \(http://blog.nsfocus.net/nsctf-network-attack-defence-game-download/\)](http://blog.nsfocus.net/nsctf-network-attack-defence-game-download/) (7,073)

[REST API 安全设计指南 \(http://blog.nsfocus.net/rest-api-design-safety/\)](http://blog.nsfocus.net/rest-api-design-safety/) (6,484)

[移动APP安全测试要点 \(http://blog.nsfocus.net/mobile-app-security-security-test/\)](http://blog.nsfocus.net/mobile-app-security-security-test/) (6,425)

[Dedecms远程写文件漏洞分析 \(http://blog.nsfocus.net/dedecms-write-file-vuln/\)](http://blog.nsfocus.net/dedecms-write-file-vuln/) (6,354)

绿盟科技博客近期文章

[FortiGate SSH漏洞分析及防护方案 \(http://blog.nsfocus.net/fortigate-ssh-vulnerability-analysis-protection-scheme/\)](http://blog.nsfocus.net/fortigate-ssh-vulnerability-analysis-protection-scheme/)


[乌克兰电力攻击事件分析及防护方案 \(http://blog.nsfocus.net/ukraine-power-plant-attack-analysis-protection-programs/\)](http://blog.nsfocus.net/ukraine-power-plant-attack-analysis-protection-programs/)


[文档安全加密系统的实现方式 \(http://blog.nsfocus.net/implement-document-security-encryption-system-approach/\)](http://blog.nsfocus.net/implement-document-security-encryption-system-approach/)

[动态加解密技术综述 \(http://blog.nsfocus.net/dynamic-encryption-technology-review/\)](http://blog.nsfocus.net/dynamic-encryption-technology-review/)

[数据安全保护之访问控制技术 \(http://blog.nsfocus.net/data-security-access-control-technology/\)](http://blog.nsfocus.net/data-security-access-control-technology/)


绿盟科技博客文章分类

技术分享 (<http://blog.nsfocus.net/category/techsharing/>)  (<http://blog.nsfocus.net/category/techsharing/feed/>) (38)

漏洞分析 (<http://blog.nsfocus.net/category/vulnanalysis/>)  (<http://blog.nsfocus.net/category/vulnanalysis/feed/>) (34)

运维安全 (<http://blog.nsfocus.net/category/opsafe/>)  (<http://blog.nsfocus.net/category/opsafe/feed/>) (24)

Web安全 (<http://blog.nsfocus.net/category/websafe/>)  (<http://blog.nsfocus.net/category/websafe/feed/>) (7)

安全报告 (<http://blog.nsfocus.net/category/securityreport/>)  (<http://blog.nsfocus.net/category/securityreport/feed/>) (7)

绿盟科技博客文章标签

DDoS (<http://blog.nsfocus.net/tag/ddos/>) 绿盟科技

(<http://blog.nsfocus.net/tag/%e7%bb%bf%e7%9b%9f%e7%a7%91%e6%8a%80/>) DDoS攻击

(<http://blog.nsfocus.net/tag/ddos%e6%94%bb%e5%87%bb/>) 互联网金融

(<http://blog.nsfocus.net/tag/%e4%ba%92%e8%81%94%e7%bd%91%e9%87%91%e8%9e%8d/>) UPack

(<http://blog.nsfocus.net/tag/upack/>) 软件逆向工程

(<http://blog.nsfocus.net/tag/%e8%bd%af%e4%bb%b6%e9%80%86%e5%90%91%e5%b7%a5%e7%a8%8b/>) UPack工作原理

(<http://blog.nsfocus.net/tag/upack%e5%b7%a5%e4%bd%9c%e5%8e%9f%e7%90%86/>) PE文件

(<http://blog.nsfocus.net/tag/pe%e6%96%87%e4%bb%b6/>) 渗透测试

(<http://blog.nsfocus.net/tag/%e6%b8%97%e9%80%8f%e6%b5%8b%e8%af%95/>) hacking team flash 0day

(<http://blog.nsfocus.net/tag/hacking-team-flash-0day/>) 云安全

(<http://blog.nsfocus.net/tag/%e4%ba%91%e5%ae%89%e5%85%a8/>) 云计算

(<http://blog.nsfocus.net/tag/%e4%ba%91%e8%ae%a1%e7%ae%97/>) hacking team (<http://blog.nsfocus.net/tag/hacking-team/>) 云安

全技术 (<http://blog.nsfocus.net/tag/%e4%ba%91%e5%ae%89%e5%85%a8%e6%8a%80%e6%9c%af/>) 云安全监控

(<http://blog.nsfocus.net/tag/%e4%ba%91%e5%ae%89%e5%85%a8%e7%9b%91%e6%8e%a7/>) 云安全解决方案

(<http://blog.nsfocus.net/tag/%e4%ba%91%e5%ae%89%e5%85%a8%e8%a7%a3%e5%86%b3%e6%96%b9%e6%a1%88/>) 手机银行

(<http://blog.nsfocus.net/tag/%e6%89%8b%e6%9c%ba%e9%93%b6%e8%a1%8c/>) 电子银行安全评估

(<http://blog.nsfocus.net/tag/%e7%94%b5%e5%ad%90%e9%93%b6%e8%a1%8c%e5%ae%89%e5%85%a8%e8%af%84%e4%bc%b0/>) 电子银行安全评估指引

(<http://blog.nsfocus.net/tag/%e7%94%b5%e5%ad%90%e9%93%b6%e8%a1%8c%e5%ae%89%e5%85%a8%e8%af%84%e4%bc%b0%e6%8c%87%e5%bc%95/>) 银行安全评估报告

(<http://blog.nsfocus.net/tag/%e9%93%b6%e8%a1%8c%e5%ae%89%e5%85%a8%e8%af%84%e4%bc%b0%e6%8a%a5%e5%91%8a/>)

互联网金融 信息安全 (<http://blog.nsfocus.net/tag/%e4%ba%92%e8%81%94%e7%bd%91%e9%87%91%e8%9e%8d-%e4%bf%a1%e6%81%af%e5%ae%89%e5%85%a8/>) 远程代码执行

(<http://blog.nsfocus.net/tag/%e8%bf%9c%e7%a8%8b%e4%bb%a3%e7%a0%81%e6%89%a7%e8%a1%8c/>) TAC

(<http://blog.nsfocus.net/tag/tac/>) 信息安全评估方法

(<http://blog.nsfocus.net/tag/%e4%bf%a1%e6%81%af%e5%ae%89%e5%85%a8%e8%af%84%e4%bc%b0%e6%96%b9%e6%b3%95/>) r

cs (<http://blog.nsfocus.net/tag/rcs/>) hacking team rcs (<http://blog.nsfocus.net/tag/hacking-team-rcs/>) 手机银行 安全评估

(<http://blog.nsfocus.net/tag/%e6%89%8b%e6%9c%ba%e9%93%b6%e8%a1%8c-%e5%ae%89%e5%85%a8%e8%af%84%e4%bc%b0/>) ht (<http://blog.nsfocus.net/tag/ht/>) 0day (<http://blog.nsfocus.net/tag/0day/>) 银

行安全评估办法

(<http://blog.nsfocus.net/tag/%e9%93%b6%e8%a1%8c%e5%ae%89%e5%85%a8%e8%af%84%e4%bc%b0%e5%8a%9e%e6%b3%95/>)

一键加群，第一时间拿干货



加入QQ群

(<http://shang.qq.com/wpa/qunwpa?>

idkey=c4983b14ee61d57a2cec866e64db59c6f40889afefdc659883d9a7a0af990d67)

两步邮件订阅，方便获取文章

欢迎订阅！现在已有132个朋友订阅了。
在后续邮件的尾部，您可以退订及修改订阅内容。
选择订阅组：

- ☐ 最新文章
- ☐ 技术分享
- ☐ 漏洞分析
- ☐ 运维安全
- ☐ **Web安全**
- ☐ 安全报告

邮件 *

马上订阅！

绿盟科技博客文章归档

绿盟科技博客功能

登录 (<http://blog.nsfocus.net/wp-login.php>)

文章RSS (Really Simple Syndication) (<http://blog.nsfocus.net/feed/>)

评论RSS (Really Simple Syndication) (<http://blog.nsfocus.net/comments/feed/>)

WordPress.org (<https://cn.wordpress.org/>)

绿盟科技博客被dmoz收录



.../计算机/互联网络/网络资源/博客/技术
(http://www.dmoz.org/World/Chinese_Simplified/%E8%AE%A1%E7%AE%97%E6%9C%BA/%E4%BA%92%E8%81%94%E7%BD%91%E7%BB%9C/%E7%BD%91%E7%BB%9C%E8%B5%84%E6%BA%90/%E5%8D%9A%E5%AE%A2/%E6%8A%80%E6%9C%AF)

