

T E C H N I C A L  
A N A L Y S I S  
O F C U B A  
R A N S O M W A R E

# REPORT

## TABLE OF CONTENTS

4	SUMMARY OF FINDINGS	12	PROCESS / SERVICES KILL LIST
5	ATTACK OVERVIEW	12	MITRE ATT&CK TECHNIQUES
5	IMPACTED COUNTRIES	14	YARA RULES
6	TECHNICAL ANALYSIS	14	CUBA DEC 2019
6	LATERAL MOVEMENT	15	CUBA VARIANT MAY 2020
7	RANSOMWARE ANALYSIS	17	CUBA VARIANT DEC 2020
7	PACKED SAMPLE	18	CUBA RANSOMWARE MARCH 2021
7	UNPACKED SAMPLE	20	CUBA RANSOMWARE MARCH 2021 UNPACKED
10	RECENT SAMPLE	23	ABOUT MCAFEE
10	CONCLUSION	23	MCAFEE ATR
11	IOCS	23	ADDITIONAL RESOURCES
11	EMAIL ADDRESSES		
11	DOMAIN		
11	SCRIPT FOR LATERAL MOVEMENT AND DEPLOYMENT		
11	CUBA RANSOMWARE		

### INTRODUCTION

Cuba ransomware is an older ransomware that has been active for the past few years. The actors behind it recently switched to leaking the stolen data to increase its impact and revenue, much like we have seen recently with other major ransomware campaigns.

In our analysis, we observed that the attackers had access to the network before the infection and were able to collect specific information in order to orchestrate the attack and have the greatest impact. The attackers operate using a set of PowerShell scripts that enables them to move laterally. The ransom note mentions that the data was exfiltrated before being encrypted. In similar attacks we have observed the use of a Cobalt Strike payload, although we have not found clear evidence of a relationship with Cuba ransomware.

We observed Cuba ransomware targeting financial institutions, industry, technology, and logistics organizations.

For active protection, more details can be found on our website:

<https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.cuba-ransomware.html>

The following report provides an overview analysis of the capabilities of Cuba ransomware and an explanation of how it works. The data included in this report is related to a Cuba ransomware sample from late 2020. We have also updated the findings with a recent sample.

### AUTHORS

---

This report was researched and written by:

- Thomas Roccia
- Thibault Seret
- Alexandre Mundo

[Subscribe to receive threat information.](#)

---

CONNECT WITH US



# TECHNICAL ANALYSIS OF CUBA RANSOMWARE SECOND LINE

## SUMMARY OF FINDINGS

- Cuba ransomware has targeted several companies in north and south America as well as in Europe.
- The attackers used a set of obfuscated PowerShell scripts to move laterally and deploy their attack.
- They used an online website to publish the stolen data.
- The malware is obfuscated and comes with several evasion techniques.
- The actors have sold some of the stolen data.
- The ransomware uses multiple argument options and has the possibility to discover shared resources using the NetShareEnum API.

CONNECT WITH US



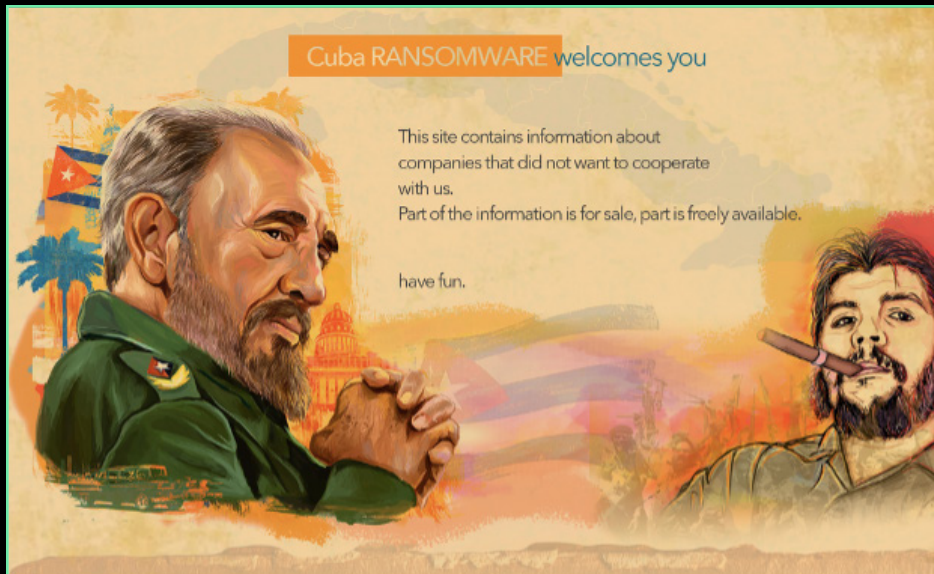
## REPORT

### ATTACK OVERVIEW

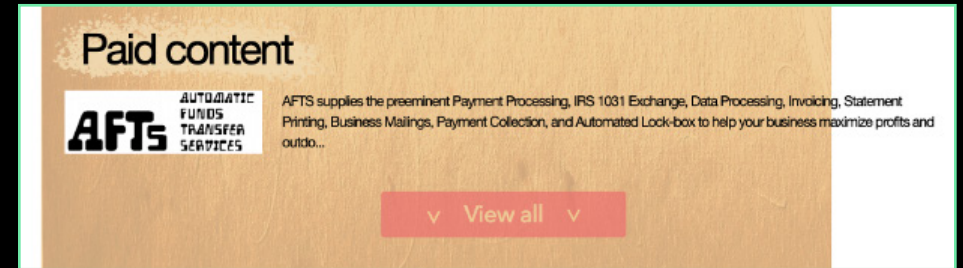
The current infection vectors are currently unknown. Once the network is breached, the attackers deploy a set of PowerShell scripts to move laterally and deploy the next stages.

The attackers recently leaked the stolen data online at this address: [http://cuba4mp6ximo2zlo\[.\]onion](http://cuba4mp6ximo2zlo[.]onion).

The following screenshot shows the website.

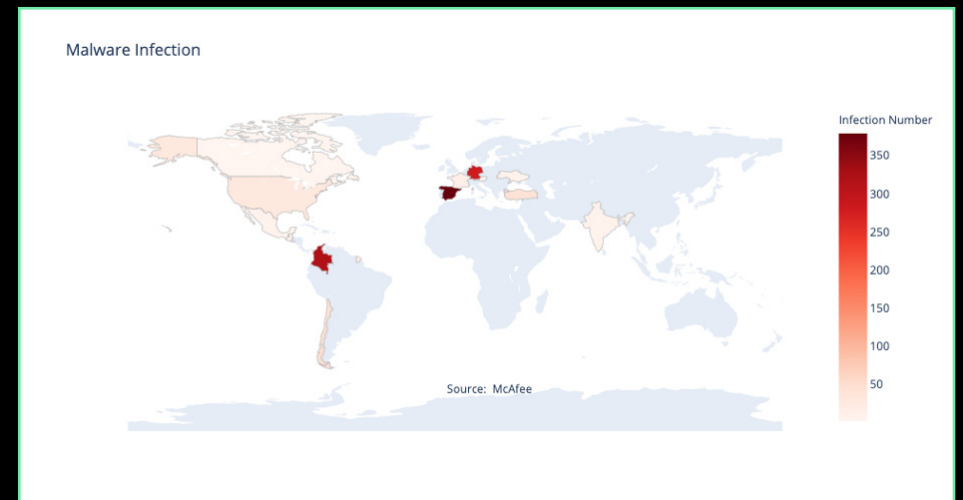


It is interesting to note that the actors sold some specific stolen data rather than just leaked it. Below is an example for data stolen from the company AFTS.



### IMPACTED COUNTRIES

The following picture shows an overview of the countries that have been impacted according to our telemetry.



# REPORT

## TECHNICAL ANALYSIS

### LATERAL MOVEMENT

Several files, including deployment scripts, were discovered in the environment. The following batch files were created to deploy an obfuscated PowerShell script that loads into memory and installs the ransomware.

<b>File type</b>	DOS batch file, ASCII text, with CRLF line terminators
<b>File name</b>	151.bat
<b>File size</b>	175
<b>Hash SHA256</b>	54627975c0befee0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc

The extract below shows the contents of this batch file. It is used to run a custom PowerShell script with the name 151.ps1 then autodeletes itself.

```
@ echo off

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -windowstyle
hidden -executionpolicy bypass -file c:\windows\temp\151.ps1

Timeout /t 15

del %0

exit
```

The number 151 for naming the script is related to the campaign number.

<b>File type</b>	ASCII text, with very long lines, with CRLF line terminators
<b>File name</b>	151.ps1
<b>File size</b>	2642
<b>Hash SHA256</b>	c385ef710cbdd8ba7759e084051f5742b6fa8a6b65340a9795f48d0a425fec61

The below screenshot shows an extract of the PowerShell script.

```
1 Add-Type -TypeDefinition @"
2 using System
3 using System.Diagnostics
4 using System.Runtime.InteropServices
5 public static class ngLkTfP0ThEjITxRmdfFe {
6     [DllImport("kernel32.dll")]public static extern IntPtr VirtualAlloc([IntPtr a,uint b,uint c,uint d);
7     [DllImport("user32.dll")]public static extern IntPtr EnumWindows(IntPtr a,IntPtr b);
8     #
9     #
10    #
11    #
12    #
13    #
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  #

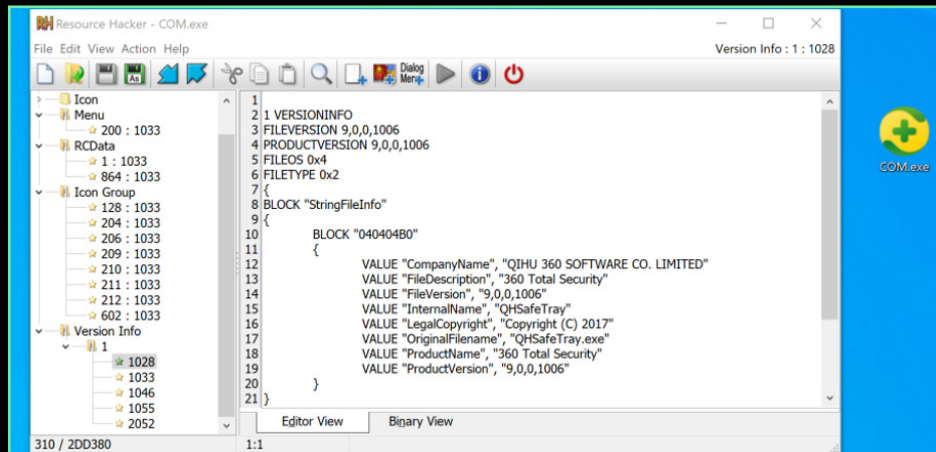
```

# REPORT

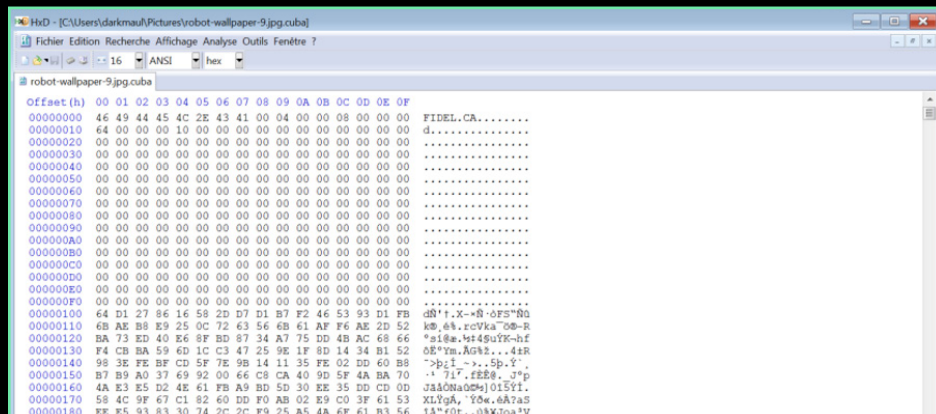
## RANSOMWARE ANALYSIS

In the version we analyzed, the ransomware comes packed and obfuscated. It uses the 360-antivirus icon and metadata to trick the user. In a more recent sample, the ransomware is using the OpenVPN metadata.

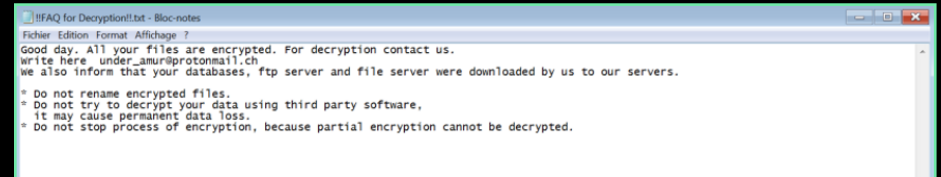
At the end of the encryption process the ransomware will display a fake message to prompt restarting of the system.



It uses the extension “.cuba” and the file marker in the encrypted file is “FIDEL.CA,” as shown below:



In every folder, the sample will write the following ransom note:



The sample uses multiple layers of obfuscation to avoid analysis and detection. Once unpacked, however, it is possible to analyze it.

## PACKED SAMPLE

File type	PE32 executable (GUI) Intel 80386, for MS Windows
File name	COM.exe
File size	3012952
Hash SHA256	c4b1f4e1ac9a28cc9e50195b29dde8bd54527abc7f4d16899f9f8315c852afd4
Compile time	1983-03-01 22:41:12
Sections	4 (0 suspicious)
Directories	import, resource, security
Detected	sign, antidbg
Import Hash	255ee022f76f062a24b690a8edb70334

## UNPACKED SAMPLE

File type	PE32 executable (GUI) Intel 80386, for MS Windows
File name	400000.COM.exe
File size	72544
Hash SHA256	944ee8789cc929d2efda5790669e5266fe80910cabf1050cbb3e57dc62de2040
Compile time	2020-09-03 00:05:36
Sections	5 (0 suspicious)
Directories	import, resource, debug, tls, relocation
Detected	packer, mutex, antidbg
Import Hash	e9fcbfea37836d5b16c8427ecb7ba2a7

## REPORT

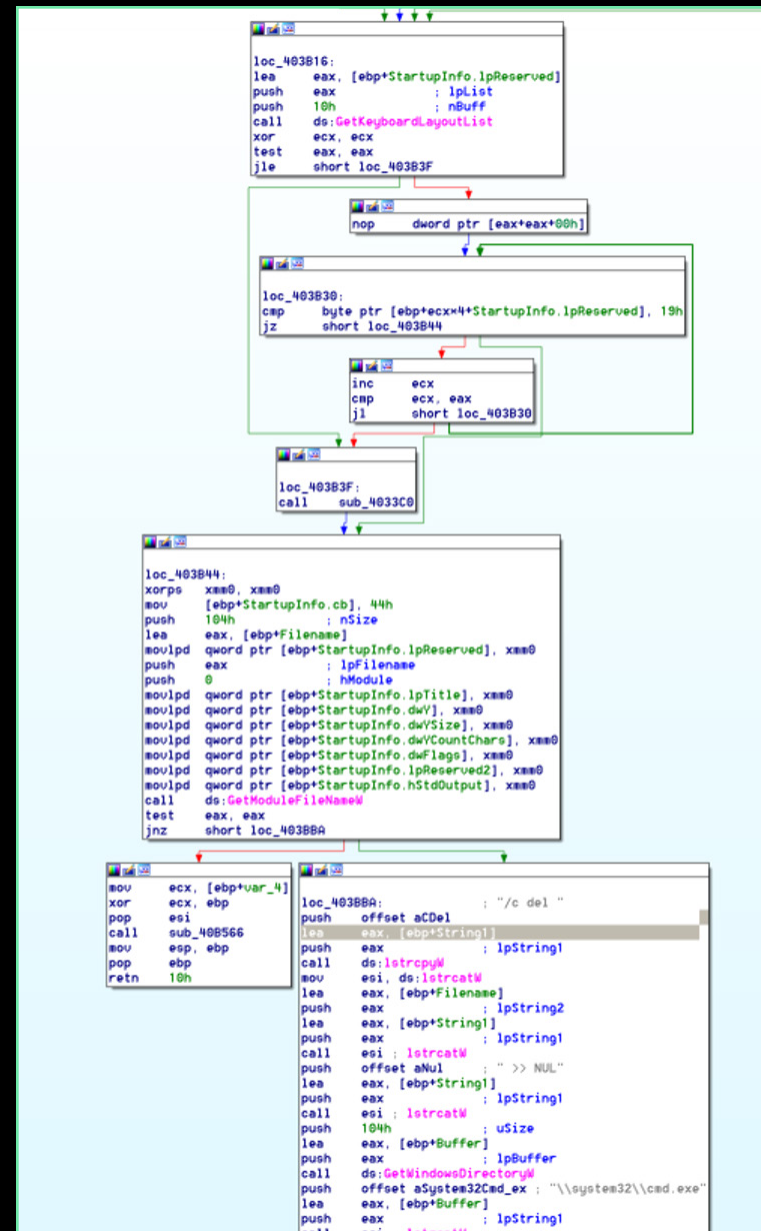
In the unpacked sample, we can see that the compilation timestamp is dated “2020-09-03.”

The ransomware has special options that can be used, allowing the threat actor to have flexibility in the attack. The sample will also check the installed languages (looking, for example, for the Russian language).

```
/dm
/min
/max
/net
/scan
```

The switches “/min” and “/max” can be used by an operator to encrypt files with a size between two values to make it faster and more impactful.

After the end of the attack, or by using the option “/dm”, it will terminate the execution of the process and delete itself using “cmd.exe /c del”.



## REPORT

The switch “/net” will get the ARP table using the function GetIpNetTable and search the machine’s network shares with the function NetShareEnum. Using GetIpNetTable can recover the last connections to the victim machine, allowing those IP addresses to be used to attack more targets.

Prior to encrypting files, it will terminate the following services and processes:

```
mov     edx, offset aMysql ; "MySQL"
call    close_and_terminate
mov     edx, offset aMysql80 ; "MySQL80"
call    close_and_terminate
mov     edx, offset aMssqlserver ; "MSSQLSERVER"
call    close_and_terminate
mov     edx, offset aSqlwriter ; "SQLWriter"
call    close_and_terminate
mov     edx, offset aMsdtc ; "MSDTC"
call    close_and_terminate
mov     edx, offset aSqlbrowser ; "SQLBrowser"
call    close_and_terminate
mov     ecx, offset aSqlservrExe ; "sqlservr.exe"
call    terminate_process
mov     ecx, offset aSqlwriterExe ; "sqlwriter.exe"
call    terminate_process
mov     ecx, offset aMsdtcExe ; "msdtc.exe"
call    terminate_process
mov     ecx, offset aSqlbrowserExe ; "sqlbrowser.exe"
call    terminate_process
mov     ecx, offset aVmwpExe ; "vmwp.exe"
call    terminate_process
mov     ecx, offset aVmospExe ; "vmosp.exe"
call    terminate_process
mov     ecx, offset aVmmsExe ; "vmms.exe"
call    terminate_process
```

The malware also has the capability to encrypt shared resources.

```
lpCriticalSection = a2;
v2 = (void (*)(LPWSTR, LPCWSTR, ...))wsprintfw;
bufptr = 0;
entriesread = 0;
totalentries = 0;
resume_handle = 0;
wsprintfw(&servername, L"\\\\\\%.%.%.%", (unsigned __int8)a1, BYTE1(a1), BYTE2(a1), a1 >> 24);
do
{
    result = NetShareEnum(&servername, 1u, &bufptr, 0xFFFFFFFF, &entriesread, &totalentries, &resume_handle);
    result_ = result;
    if ( result && result != 0xEA )
        break;
    bufptr_1 = bufptr;
    v5 = 1;
    if ( entriesread >= 1 )
    {
        do
        {
            v2(&FileName, L"%s\\%s\\", &servername, *(_DWORD *)bufptr_1);
            if ( *((_DWORD *)bufptr_1 + 1) >= 0 )
            {
                v6 = FindFirstFileW(&FileName, &FindFileData);
                if ( v6 != (HANDLE)-1 )
                {
                    wsprintfw(&FileName, L"%s\\%s\\", &servername, *(_DWORD *)bufptr_1);
                    v9 = 0;
                    v10 = 7;
                    LOWORD(lpMem) = 0;
                    sub_403E40(&lpMem, &FileName, wcslen(&FileName));
                    v20 = 0;
                    sub_4012F0(lpCriticalSection, (int)&lpMem);
                    v20 = -1;
                    if ( v10 >= 8 )
                    {
                        v7 = lpMem;
                        if ( 2 * v10 + 2 >= 0x1000 )
                        {
                            v7 = (_BYTE *)*((_DWORD *)lpMem - 1);
                            if ( (unsigned int)((_BYTE *)lpMem - v7 - 4) > 0x1F )
                                _invalid_parameter_noinfo_noreturn(v7, 2 * v10 + 37);
                        }
                        freebase_0(v7);
                    }
                    FindClose(v6);
                }
                v2 = (void (*)(LPWSTR, LPCWSTR, ...))wsprintfw;
            }
            ++v5;
            bufptr_1 += 12;
        } while ( v5 <= entriesread );
        bufptr_1 = bufptr;
    }
    result = NetApiBufferFree(bufptr_1);
} while ( result_ == 234 );
return result;
```

## REPORT

### RECENT SAMPLE

In a recent sample, the actors behind Cuba ransomware updated some of its functions. In this variant the ransomware is using SeDebugPrivilege to elevate privileges. Additionally, they updated the list of services and processes to terminate.

```
{
HANDLE v0; // esi
struct _TOKEN_PRIVILEGES NewState; // [esp+8h] [ebp-1Ch]
struct _LUID Luid; // [esp+18h] [ebp-Ch]

v0 = GetCurrentProcess();
if ( LookupPrivilegeValue(0, "SeDebugPrivilege", &Luid) )
{
NewState.Privileges[0].Luid = Luid;
NewState.PrivilegeCount = 1;
NewState.Privileges[0].Attributes = 2;
if ( AdjustTokenPrivileges(v0, 0, &NewState, 0x10u, 0, 0) )
GetLastError();
}
closeservice(L"MySQL", 0xFFFFFFFF);
closeservice(L"MySQLB0", 0xFFFFFFFF);
closeservice(L"SQLSERVERAGENT", 0xFFFFFFFF);
closeservice(L"MSSQLSERVER", 0xFFFFFFFF);
closeservice(L"SQLWriter", 0xFFFFFFFF);
closeservice(L"SQLTELEMETRY", 0xFFFFFFFF);
closeservice(L"MSDTC", 0xFFFFFFFF);
closeservice(L"SQLBrowser", 0xFFFFFFFF);
terminateprocess(L"sqlagent.exe");
terminateprocess(L"sqlservr.exe");
terminateprocess(L"sqlwriter.exe");
terminateprocess(L"sqlceip.exe");
terminateprocess(L"msdtc.exe");
terminateprocess(L"sqlbrowser.exe");
closeservice(L"vmcompute", 4u);
closeservice(L"vmms", 4u);
terminateprocess(L"vmmp.exe");
terminateprocess(L"vmsp.exe");
terminateprocess(L"outlook.exe");
closeservice(L"MSExchangeUMCR", 0xFFFFFFFF);
closeservice(L"MSExchangeUM", 0xFFFFFFFF);
closeservice(L"MSExchangeTransportLogSearch", 0xFFFFFFFF);
closeservice(L"MSExchangeTransport", 0xFFFFFFFF);
closeservice(L"MSExchangeThrottling", 0xFFFFFFFF);
closeservice(L"MSExchangeSubmission", 0xFFFFFFFF);
closeservice(L"MSExchangeServiceHost", 0xFFFFFFFF);
closeservice(L"MSExchangeRPC", 0xFFFFFFFF);
closeservice(L"MSExchangeRepl", 0xFFFFFFFF);
closeservice(L"MSExchangePOP3BE", 0xFFFFFFFF);
closeservice(L"MSExchangePop3", 0xFFFFFFFF);
closeservice(L"MSExchangeNotificationsBroker", 0xFFFFFFFF);
closeservice(L"MSExchangeMailboxReplication", 0xFFFFFFFF);
closeservice(L"MSExchangeMailboxAssistants", 0xFFFFFFFF);
closeservice(L"MSExchangeIS", 0xFFFFFFFF);
closeservice(L"MSExchangeIMAP4BE", 0xFFFFFFFF);
closeservice(L"MSExchangeImap4", 0xFFFFFFFF);
closeservice(L"MSExchangeHMRecovery", 0xFFFFFFFF);
closeservice(L"MSExchangeHM", 0xFFFFFFFF);
closeservice(L"MSExchangeFrontEndTransport", 0xFFFFFFFF);
closeservice(L"MSExchangeFastSearch", 0xFFFFFFFF);
closeservice(L"MSExchangeEdgeSync", 0xFFFFFFFF);
closeservice(L"MSExchangeDiagnostics", 0xFFFFFFFF);
closeservice(L"MSExchangeDelivery", 0xFFFFFFFF);
closeservice(L"MSExchangeDagMgmt", 0xFFFFFFFF);
closeservice(L"MSExchangeCompliance", 0xFFFFFFFF);
return closeservice(L"MSExchangeAntispamUpdate", 0xFFFFFFFF);
}
```

The other function remains the same in the new variant.

### CONCLUSION

Cuba ransomware has recently impacted several organizations. In this short report we briefly detailed the threat actors' capabilities and provided an overview of the ransomware. It is interesting to note that the website for leaking stolen data was put online some months ago and follows the same trends as other ransomware actors.

The use of arguments demonstrates that the ransomware has been developed to be modular and practical for the authors to gain access, discover, and encrypt data more easily.

While this brief threat report shows some aspects of the Cuba ransomware, it also provides an overview of the operating methods used by the attackers.

McAfee® Advanced Threat Research Team is actively monitoring this threat for future releases.

# REPORT

## IOCS

### EMAIL ADDRESSES

```
under_ amur@protonmail[.]ch  
helpadmin2@cock[.]li  
helpadmin2@protonmail[.]com  
iracomp2@protonmail[.]ch  
fedelsupportagent@cock.li  
admin@cuba-supp.com  
cuba_ support@exploit.im
```

### DOMAIN

```
kurvalarva[.]com
```

### SCRIPT FOR LATERAL MOVEMENT AND DEPLOYMENT

```
54627975c0befee0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc  
c385ef710cbdd8ba7759e084051f5742b6fa8a6b65340a9795f48d0a425fec61  
40101fb3629cdb7d53c3af19dea2b6245a8d8aa9f28febd052bb9d792cfbefa6
```

## CUBA RANSOMWARE

```
c4b1f4e1ac9a28cc9e50195b29dde8bd54527abc7f4d16899f9f8315c852afd4  
944ee8789cc929d2efda5790669e5266fe80910cabf1050cbb3e57dc62de2040  
78ce13d09d828fc8b06cf55f8247bac07379d0c8b8c8b1a6996c29163fa4b659  
33352a38454cfc247bc7465bf177f5f97d7fd0bd220103d4422c8ec45b4d3d0e  
672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1  
e942a8bcb3d4a6f6df6a6522e4d5c58d25cbe369ecda1356a66dacbd3945d30  
907f42a79192a016154f11927fbb1e6f661f679d68947bddd714f5acc4aa66eb  
28140885cf794ffe27f5673ca64bd680fc0b8a469453d0310aea439f7e04e64  
271ef3c1d022829f0b15f2471d05a28d4786abafd0a9e1e742bde3f6b36872ad  
6396ea2ef48aa3d3a61fb2e1ca50ac3711c376ec2b67dbaf64eeba49f5dfa9df  
bda4bddcbd140e4012bab453e28a4fba86f16ac8983d7db391043eab627e9fa1  
7a17f344d916f7f0272b9480336fb05d33147b8be2e71c3261ea30a32d73fecb  
c206593d626e1f8b9c5d15b9b5ec16a298890e8bae61a232c2104cbac8d51bdd  
9882c2f5a95d7680626470f6c0d3609c7590eb552065f81ab41ffe074ea74e82  
c385ef710cbdd8ba7759e084051f5742b6fa8a6b65340a9795f48d0a425fec61  
54627975c0befee0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc  
1f825ef9ff3e0bb80b7076ef19b837e927efea9db123d3b2b8ec15c8510da647  
40101fb3629cdb7d53c3af19dea2b6245a8d8aa9f28febd052bb9d792cfbefa6  
00ddbe28a31cc91bd7b1989a9bebd43c4b5565aa0a9ed4e0ca2a5cfb290475ed  
729950ce621a4bc6579957eabb3d1668498c805738ee5e83b74d5edaf2f4cb9e
```

# REPORT

## PROCESS / SERVICES KILL LIST

```
MySQL, MySQL80, SQLSERVERAGENT, MSSQLSERVER, SQLWriter, SQLTELEMETRY, MSDTC, SQLBrowser, sqlagent.exe, sqlservr.exe, sqlwriter.exe, sqlceip.exe, msdtc.exe, sqlbrowser.exe, vmcompute, vmms, vmwp.exe, vmsp.exe, outlook.exe, MExchangeUMCR, MExchangeUM, MExchangeTransport-LogSearch, MExchangeTransport, MExchangeThrottling, MExchangeSubmission, MExchangeServiceHost, MExchangeRPC, MExchangeRepl, MExchangePOP3BE, MExchangePop3, MExchangeNotificationsBroker, MExchangeMailboxReplication, MExchangeMailboxAssistants, MExchangeIS, MExchangeIMAP4BE, MExchangeImap4, MExchangeHMRecovery, MExchangeHM, MExchangeFrontEndTransport, MExchangeFastSearch, MExchangeEdgeSync, MExchangeDiagnostics, MExchangeDelivery, MExchangeDagMgmt, MExchangeCompliance, MExchangeAntispamUpdate
```

## MITRE ATT&CK TECHNIQUES

Tactic	Technique	Observable	IOCs
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	Cuba team is using PowerShell payload to drop Cuba ransomware	f739977004981fbe4a54bc68be18ea79 68a99624f98b8cd956108fedcc44e07c bdeb5acc7b569c783f81499f400b2745
Execution	System Services: Service Execution (T1569.002)		
Execution	Shared Modules (T1129)	Cuba ransomware links function at runtime	Functions: "GetModuleHandle" "GetProcAddress" "GetModuleHandleEx"
Execution	Command and Scripting Interpreter (T1059)	Cuba ransomware accepts command line arguments	Functions: "GetCommandLine"
Persistence	Create or Modify System Process: Windows Service (T1543.003)	Cuba ransomware can modify services	Functions: "OpenService" "ChangeServiceConfig"
Privilege Escalation	Access Token Manipulation (T1134)	Cuba ransomware can adjust access privileges	Functions: "SeDebugPrivilege" "AdjustTokenPrivileges" "LookupPrivilegeValue"

## REPORT

Tactic	Technique	Observable	IOCs
Defense Evasion	File and Directory Permissions Modification (T1222)	Cuba ransomware will set file attributes	Functions: "SetFileAttributes"
Defense Evasion	Obfuscated files or Information (T1027)	Cuba ransomware is using xor algorithm to encode data	
Defense Evasion	Virtualization/Sandbox Evasion: System Checks	Cuba ransomware executes anti-vm instructions	
Discovery	File and Directory Discovery (T1083)	Cuba ransomware enumerates files	Functions: "FindFirstFile" "FindNextFile" "FindClose" "FindFirstFileEx" "FindNextFileEx" "GetFileSizeEx"
Discovery	Process Discovery (T1057)	Cuba ransomware enumerates process modules	Functions: "K32EnumProcesses"
Discovery	System Information Discovery (T1082)	Cuba ransomware can get keyboard layout, enumerates disks, etc.	Functions: "GetKeyboardLayoutList" "FindFirstVolume" "FindNextVolume" "GetVolumePathNamesForVolumeName" "GetDriveType" "GetLogicalDriveStrings" "GetDiskFreeSpaceEx"
Discovery	System Service Discovery (T1007)	Cuba ransomware can query service status	Functions: "QueryServiceStatusEx"
Collection	Input Capture: Keylogging (T1056.001)	Cuba ransomware logs keystrokes via polling	Functions: "GetKeyState" "VkKeyScan"
Impact	Service Stop (T1489)	Cuba ransomware can stop services	
Impact	Data encrypted for Impact (T1486)	Cuba ransomware encrypts data	

# REPORT

## YARA RULES

### CUBA DEC 2019

```
rule RANSOM _Cuba _Dec2019 {
meta:
description = "Rule to detect Cuba Ransomware 2019 version"
author = "McAfee ATR"
date = "2021-02-23"
rule _version = "v1"
hash = " bda4bddcbd140e4012bab453e28a4fba86f16ac8983d7db391043eab627e9fa1"
malware _type = "Ransom"

strings:
$s1 = "VirtualProtect" fullword ascii
$s2 = "GetStartupInfoA" fullword ascii
$s3 = "GetModuleHandleA" fullword ascii
$s4 = "ListDrop" fullword ascii
$s5 = "WinExec" fullword ascii

$pattern1 = {BF90C5BC9827B183908CB29090103240409A1DCD40BE90004D6C8704433AC0B6BF294087400D878C2940C5C17940BB00903AC3064062400D9B8940B80DBF88CB90902ABFBF-
C9517C9057C472C6908E41904F}

$pattern2 = {000CADD1B48CCB34848CCB34848CCB34827D3B84840CCB348CBD0BD4854CCB34827D3B94813CCB348B7ECB7484DCCB34848CCB24809CCB3482AD3A0484ACCB348B7EC-
B9484ACCB3481CEF82484ECCB348}

$pattern3 = {F2FB58C3A06EA22ED5FB2BD44D066BA6862B6B187B123740FB2FC36B107EEF2A2463D6FB406B6BFB33A36B76FB01D66BFB0CC02BFBA70FD36B6B2E2CA20A6B6B286E-
6BA06B2B}
```

## REPORT

```
$pattern4 = {4090D8BC00BF909000C9908F00CB90798559C64090CB54B255A870900DBDDC09B290149090AF35BE3490C307BFB476CB40901B0AD840BFA32590FB409078053D0040F4814853}  
  
$pattern5 = {6B6BE03967E0397FE01943017332589458ABC7570A1769474BAAA4666893899BEA9430D72101E0317BE0791EB0E2369B0AE02E9BE0269B682357E2E65B949494D1636B}  
  
condition:  
  
filesize <= 750KB and  
  
4 of ($s*) and  
  
4 of ($pattern*)  
  
}
```

## CUBA VARIANT MAY 2020

```
rule RANSOM_Cuba_variant_May2020 {  
  meta:  
    description = "Rule to detect Cuba Ransomware variant from May 2020"  
    author = "McAfee ATR"  
    date = "2021-02-23"  
    rule_version = "v1"  
    hash = "7a17f344d916f7f0272b9480336fb05d33147b8be2e71c3261ea30a32d73fecb"  
    malware_type = "Ransom"  
  
  strings:  
    $s1 = "Good day. All your files are encrypted. For decryption contact us." fullword ascii  
    $s2 = "CryptGenRandom" fullword ascii
```

## REPORT

```
$s3 = "VirtualAlloc" fullword ascii

$s4 = {0021002100460041005100200066006F0072002000440065006300720079007000740069006F006E00210021002E007400780074}

// !!FAQ for Decryption!!.txt

$pattern1 = {C1C109334D8C8D3C01C1C70D337D94897D9C8D0439C1C01233C28B55988945A08D0413C1C00733458803D0C1C2093355848D1C02C1C30D335DB0895DB08D3C1A8BDF897DB-
8C1C312335D98895DB88B5DB403D8C1C30733DE8B75B4895D90895DC08D3C33C1C70933F9897D8C897DC48D0C3BC1C10D33C8894D}

$pattern2 = {B08D4DFB33C03BF977078D4DBC3BD1730B8D4E3F3BF977253BD672218B5DB48B75B88D55BC03D0408A0C16320A880C1383F84072ED8B750C8B5DACEB3E0F1045B-
C0F100E660FEFC80F10}

$pattern3 = {837E283872EF0FB646078846640FB646068846650FB646058846660FB646048846670FB646038846680FB646028846690FB6460188466A0FB60688466B8D462C5056E81E01}

$pattern4 = {342A3464349434C43402355A35A235D4350A366536B536F236A337CD37F2371A384A389938D43804392A395A39A939DA39143A323A6E3AAE3AD23AFC3A223B5C}

$pattern5 = {512085F6773372133B15FC294600732985F67725720583FA1D731E0FB682AC28460039411875128B0495802946005F5B890133C05E8BE55DC30BD6750B5F5B89}

condition:
filesize <=600KB and
3 of ($s*) and
4 of ($pattern*)
}
```

# REPORT

## CUBA VARIANT DEC 2020

```
rule RANSOM_Cuba_variant_Dec2020 {
  meta:
    description = "Rule to detect Cuba Ransomware variant from December 2020"
    author = "McAfee ATR"
    date = "2021-02-23"
    rule_version = "v1"
    hash = "33352a38454cfc247bc7465bf177f5f97d7fd0bd220103d4422c8ec45b4d3d0e"
    malware_type = "Ransom"

  strings:
    $s1 = "Good day. All your files are encrypted. For decryption contact us." fullword ascii
    $s2 = "SeDebugPrivilege" fullword ascii
    $s3 = "md5WithRSAEncryption" fullword ascii
    $s4 = "CryptGenRandom" fullword ascii
    $s5 = "CryptAcquireContextW" fullword ascii
    $s6 = "FindFirstFileExW" fullword ascii

  // Main function
  $main1 = { 55 8b ec 83 ec 44 a1 0c 70 42 00 33 c5 89 45 fc 8b 45 10 56 33 f6 66 39 30 74 03 50 eb 05 68 08 be 41 00 e8 17 ea ff ff 8d 45 bc 50 6a 10
  ff 15 c8 71 41 00 85 c0 7e 0c 80 7c b5 bc 19 74 0a 46 3b f0 7c f4 e8 11 ff ff ff 8b 4d fc 33 c0 33 cd 5e e8 34 74 00 00 c9 c2 10 00 }
  $main2 = {558bec83ec44a1????????33c58945fc8b45105633f666393074?50eb??68?????e8?????8d45bc506a??ff????????85c07e??807cb5bc1974?463bf07c??e8?????-
  ??8b4dfc33c033cd5ee8????????c9c21??0}
```

## REPORT

```
$main3 = {558bec83ec44a1????????33c58945fc8b45105633f6663930[2-6]50[2-6]68????????e8????????8d45bc506a??ff????????85c0[2-6]807cb5bc19[2-6]463bf0[2-6]e8????????8b4dfc33c033cd5ee8????????c9c21??0}

$main4 = { 55 8B EC 83 EC 44 A1 ?? ?? ?? ?? 33 C5 89 45 ?? 8B 45 ?? 56 33 F6 66 39 30 74 ?? 50 EB ?? 68 08 BE 41 00 E8 ?? ?? ?? ?? 8D 45 ?? 50 6A 10 FF 15 ?? ?? ?? ?? 85 C0 7E ?? 80 7C B5 ?? 19 74 ?? 46 3B F0 7C ?? E8 ?? ?? ?? ?? 8B 4D ?? 33 C0 33 CD 5E E8 ?? ?? ?? ?? C9 C2 10 00}

condition:

filesize <= 180KB and

4 of ($s*) and

any of ($main*)

}
```

## CUBA RANSOMWARE MARCH 2021

```
rule RANSOM_Cuba_March2021

{

meta:

description = "Rule to detect Cuba ransomware March 2021 version"

author = "McAfee ATR"

date = "2021-03-31"

hash = "2af30ca88d11eb0c1a4bd4f0aa0ce685"
```

## REPORT

strings:

\$s1 = "VirtualAlloc" wide ascii

\$s2 = "GetSystemDirectoryW" wide ascii

\$s3 = "ShellExecuteEx" wide ascii

\$s4 = "SHEmptyRecycleBinA" wide ascii

\$s5 = "CommandLineToArgvW" wide ascii

\$fnc1 = { 55 8b ec 83 ec 18 c7 45 fc 40 00 00 00 c7 45 f4 00 00 00 00 a1 40 c1 44 00 89 45 e8 c7 45 f8 ff ff ff ff 8b 0d 7c a7 44 00 89 0d a0 c1 44 00 ff 75 fc 68 01 30 00 00 83 2c 24 01 ff 75 e8 ff 75 f4 ff 35 a0 c1 44 00 59 ff d1 89 45 ec 8b 55 ec 89 15 84 c1 44 00 a1 40 c1 44 00 a3 44 c1 44 00 8b 0d 84 c1 44 00 81 c1 c0 51 02 00 89 0d 50 c1 44 00 8b 45 ec 8b e5 5d c3 }

\$fnc2 = {558bec83ec18c7????????????c745f4????????a1????????8945e8c7????????8b????????89????????ff75fc68????????832c2401ff75e8ff75f4ff????????59ff-d18945ec8b55ec89????????a1????????a3????????8b????????81????????89????????8b45ec8be55dc3}

\$fnc3 = { 55 8B EC 83 EC 18 C7 45 ?? 40 00 00 00 C7 45 ?? 00 00 00 00 A1 ?? ?? ?? ?? 89 45 ?? C7 45 ?? FF FF FF FF 8B 0D ?? ?? ?? ?? 89 0D ?? ?? ?? ?? FF 75 ?? 68 01 30 00 00 83 2C 24 01 FF 75 ?? FF 75 ?? FF 35 ?? ?? ?? ?? 59 FF D1 89 45 ?? 8B 55 ?? 89 15 ?? ?? ?? ?? A1 ?? ?? ?? ?? A3 ?? ?? ?? ?? 8B 0D ?? ?? ?? ?? 81 C1 C0 51 02 00 89 0D ?? ?? ?? ?? 8B 45 ?? 8B E5 5D C3}

condition:

filesize >= 350KB and filesize <= 500KB and

4 of (\$s\*) and

1 of (\$fnc\*)

}

# REPORT

## CUBA RANSOMWARE MARCH 2021 UNPACKED

```
rule RANSOM_Cuba_Unpacked_March2021
{

meta:
description = "Rule to detect Cuba ransomware unpacked"
author = "McAfee ATR"
date = "2021-03-31"
hash = "aef29cad14fd64de387c274476887c94"
malware_type = "Ransom"

strings:

$s1 = "Good day" wide ascii
$s2 = "AppPolicyGetProcessTerminationMethod" wide ascii
$s3 = "GetOEMCP" wide ascii
$s4 = "GetCommandLineA" wide ascii
$s5 = "GetProcAddress" wide ascii

$main1 = { 55 8b ec 81 ec 78 06 00 00 a1 0c a0 42 00 33 c5 89 45 fc 56 8b 75 10 b9 b8 aa 42 00 6a 05 68 18 f0 41 00 e8 b8 04 00 00 66 c7 05 d0 aa
42 00 00 00 0f 57 c0 c6 05 d2 aa 42 00 00 66 0f 13 05 d8 aa 42 00 c7 05 e0 aa 42 00 ff ff ff ff c7 05 e4 aa 42 00 ff ff ff 7f 85 f6 0f 84 57 01 00
00 66 83 3e 00 0f 84 4d 01 00 00 8d 85 e0 f9 ff ff c7 85 e0 f9 ff ff 00 00 00 00 50 56 ff 15 c4 a1 41 00 8b 8d e0 f9 ff ff 89 85 88 f9 ff ff 85 c9
0f 84 21 01 00 00 57 8b 38 33 f6 66 83 3f 2f 74 31 8b d7 8d 72 02 66 8b 02 83 c2 02 66 85 c0 75 f5 2b d6 b9 b8 aa 42 00 d1 fa 52 57 e8 20 04 00 00
8b 8d e0 f9 ff ff be 01 00 00 00 8b 85 88 f9 ff ff 3b f1 0f 8d dc 00 00 00 53 66 0f 1f 44 00 00 8b 1c b0 33 ff 46 3b f1 7d 0c 8b 04 b0 66 83 38 2f
74 03 8b f8 46 68 24 f0 41 00 53 ff 15 5c a0 41 00 85 c0 75 0c c6 05 d2 aa 42 00 01 e9 8e 00 00 00 68 2c f0 41 00 53 ff 15 5c a0 41 00 85 c0 75 1a
85 ff 74 7a 57 e8 98 bd 00 00 83 c4 04 a3 d8 aa 42 00 89 15 dc aa 42 00 eb 64 68 38 f0 41 00 53 ff 15 5c a0 41 00 85 c0 75 1a 85 ff 74 50 57 e8 6e
bd 00 00 83 c4 04 a3 e0 aa 42 00 89 15 e4 aa 42 00 eb 3a 8b 3d 5c a0 41 00 68 44 f0 41 00 53 ff d7 85 c0 75 09 c6 05 d0 aa 42 00 01 eb 1f 68 50 f0
```

# REPORT

```
41 00 53 ff d7 0f b6 0d d1 aa 42 00 85 c0 ba 01 00 00 00 0f 44 ca 88 0d d1 aa 42 00 8b 8d e0 f9 ff ff 8b 85 88 f9 ff ff 3b f1 0f 8c 2c ff ff ff 5b
5f 8d 85 a0 f9 ff ff 50 6a 10 ff 15 cc a1 41 00 33 c9 85 c0 7e 14 0f 1f 44 00 00 80 bc 8d a0 f9 ff ff 19 74 0a 41 3b c8 7c f1 e8 7c f8 ff ff 0f 57
c0 c7 85 9c f9 ff ff 44 00 00 00 68 04 01 00 00 8d 85 e4 f9 ff ff 66 0f 13 85 a0 f9 ff ff 50 6a 00 66 0f 13 85 a8 f9 ff ff 66 0f 13 85 b0 f9 ff ff
66 0f 13 85 b8 f9 ff ff 66 0f 13 85 c0 f9 ff ff 66 0f 13 85 c8 f9 ff ff 66 0f 13 85 d0 f9 ff ff 66 0f 13 85 d8 f9 ff ff ff 15 74 a0 41 00 85 c0 75
11 8b 4d fc 33 cd 5e e8 b2 79 00 00 8b e5 5d c2 10 00 68 70 5e 42 00 8d 85 f4 fd ff ff 50 ff 15 bc a0 41 00 8b 35 9c a0 41 00 8d 85 e4 f9 ff ff 50
8d 85 f4 fd ff ff 50 ff d6 68 80 5e 42 00 8d 85 f4 fd ff ff 50 ff d6 68 04 01 00 00 8d 85 ec fb ff ff 50 ff 15 a4 a0 41 00 68 90 5e 42 00 8d 85 ec
fb ff ff 50 ff d6 8d 85 8c f9 ff ff 50 8d 85 9c f9 ff ff 50 6a 00 6a 00 68 00 00 00 08 6a 00 6a 00 6a 00 8d 85 f4 fd ff ff 50 8d 85 ec fb ff ff 50
ff 15 b4 a0 41 00 85 c0 74 16 ff b5 90 f9 ff ff 8b 35 54 a0 41 00 ff d6 ff b5 8c f9 ff ff ff d6 6a 00 ff 15 b0 a0 41 00 }
```

```
$main2 = {558bec81ec7806????a1??????33c58945fc568b7510b9??????6a??68??????e8??????66c7????????????0f57c0c6??????????660f13????????c7????????-
??????????c7??????????????????85f60f84??????66833e??0f84??????8d85e0f9ffffc785e0f9ffff??????5056ff??????????8b8de0f9ffff898588f9ffff85c90f84????-
????578b3833f666833f2f74??8bd78d7202668b0283c2026685c075??2bd6b9????????d1fa5257e8??????8b8de0f9ffffbe01??????8b8588f9ffff3bf10f8d??????53660f1f44-
????8b1cb033ff463bf17d??8b04b06683382f74??8bf84668????????53ff????????85c075??c6??????????e9??????68??????53ff????????85c075??85ff74??5
7e8??????83c404a3??????89??????eb??68??????53ff????????85c075??85ff74??57e8??????83c404a3??????89??????eb??8b????????68??????53f
fd785c075??c6??????????eb??68??????53ffd70fb6????????85c0ba01??????0f44ca88????????8b8de0f9ffff8b8588f9ffff3bf10f8c????????5b5f8d85a0f9ffff506a??-
ff????????33c985c07e??0f1f44??80bc8da0f9ffff1974??413bc87c??e8??????0f57c0c7??????????????68??????8d85e4f9ffff660f1385a0f9ffff506a??660f1385a8
f9ffff660f1385b0f9ffff660f1385b8f9ffff660f1385c0f9ffff660f1385c8f9ffff660f1385d0f9ffff660f1385d8f9ffff????????85c075??8b4dfc33cd5ee8??????8be55d-
c21??068??????8d85f4fdffff50ff????????8b????????8d85e4f9ffff508d85f4fdffff50ffd668????????8d85f4fdffff50ffd668????????8d85ecfbffff50ff?????-
????68??????8d85ecfbffff50ffd68d858cf9ffff508d859cf9ffff506a??6a??68??????6a??6a??6a??8d85f4fdffff508d85ecfbffff50ff????????85c074??fb590f9ffff-
8b????????ffd6ffb58cf9fffffd66a??ff????????}
```

```
$main3 = {558bec81ec7806????a1??????33c58945fc568b7510b9??????6a??68??????e8??????66c7????????????0f57c0c6??????????660f13????????
??c7????????????????c7????????????????85f6[2-6]66833e??[2-6]8d85e0f9ffffc785e0f9ffff??????5056ff??????????8b8de0f9ffff898588f9ffff85c9[2-
6]578b3833f666833f2f[2-6]8bd78d7202668b0283c2026685c0[2-6]2bd6b9????????d1fa5257e8??????8b8de0f9ffffbe01??????8b8588f9ffff3bf1[2-6]53660f1f44????8b-
1cb033ff463bf1[2-6]8b04b06683382f[2-6]8bf84668????????53ff????????85c0[2-6]c6??????????[2-6]68??????53ff????????85c0[2-6]85ff[2-6]57e8??????83c
404a3??????89????????[2-6]68??????53ff????????85c0[2-6]85ff[2-6]57e8??????83c404a3??????89????????[2-6]8b????????68??????53ffd785c0[2-6]
c6??????????[2-6]68??????53ffd70fb6????????85c0ba01??????0f44ca88????????8b8de0f9ffff8b8588f9ffff3bf1[2-6]5b5f8d85a0f9ffff506a??ff??????-
???33c985c0[2-6]0f1f44??80bc8da0f9ffff19[2-6]413bc8[2-6]e8??????0f57c0c7??????????????68??????8d85e4f9ffff660f1385a0f9ffff506a??660f1385a8f9ffff6
60f1385b0f9ffff660f1385b8f9ffff660f1385c0f9ffff660f1385c8f9ffff660f1385d0f9ffff660f1385d8f9ffff????????85c0[2-6]8b4dfc33cd5ee8??????8be55dc21??068
??????8d85f4fdffff50ff????????8b????????8d85e4f9ffff508d85f4fdffff50ffd668????????8d85f4fdffff50ffd668????????8d85ecfbffff50ff????????68??????-
8d85ecfbffff50ffd68d858cf9ffff508d859cf9ffff506a??6a??68??????6a??6a??6a??8d85f4fdffff508d85ecfbffff50ff????????85c0[2-6]ffb590f9ffff-
8b????????ffd6ffb58cf9fffffd66a??ff????????}
```

# REPORT

```
$main4 = { 55 8B EC 81 EC 78 06 00 00 A1 ?? ?? ?? ?? 33 C5 89 45 ?? 56 8B 75 ?? B9 B8 AA 42 00 6A 05 68 18 F0 41 00 E8 ?? ?? ?? ?? 66 C7 05 ?? ?? ??  
?? 00 00 0F 57 C0 C6 05 ?? ?? ?? ?? 00 66 0F 13 05 ?? ?? ?? ?? C7 05 ?? ?? ?? ?? FF FF FF FF C7 05 ?? ?? ?? ?? FF FF FF 7F 85 F6 0F 84 ?? ?? ?? ??  
66 83 3E 00 0F 84 ?? ?? ?? ?? 8D 85 ?? ?? ?? ?? C7 85 ?? ?? ?? ?? 00 00 00 00 50 56 FF 15 ?? ?? ?? ?? 8B 8D ?? ?? ?? ?? 89 85 ?? ?? ?? ?? 85 C9 0F 84  
?? ?? ?? ?? 57 8B 38 33 F6 66 83 3F 2F 74 ?? 8B D7 8D 72 ?? 66 8B 02 83 C2 02 66 85 C0 75 ?? 2B D6 B9 B8 AA 42 00 D1 FA 52 57 E8 ?? ?? ?? ?? 8B 8D  
?? ?? ?? ?? BE 01 00 00 00 8B 85 ?? ?? ?? ?? 3B F1 0F 8D ?? ?? ?? ?? 53 66 0F 1F 44 00 ?? 8B 1C B0 33 FF 46 3B F1 7D ?? 8B 04 B0 66 83 38 2F 74 ?? 8B  
F8 46 68 24 F0 41 00 53 FF 15 ?? ?? ?? ?? ?? 85 C0 75 ?? C6 05 ?? ?? ?? ?? 01 E9 ?? ?? ?? ?? 68 2C F0 41 00 53 FF 15 ?? ?? ?? ?? 85 C0 75 ?? 85 FF 74 ?? 57 E8 ?? ?? ?? ?? 83 C4  
57 E8 ?? ?? ?? ?? 83 C4 04 A3 ?? ?? ?? ?? 89 15 ?? ?? ?? ?? EB ?? 68 38 F0 41 00 53 FF 15 ?? ?? ?? ?? 85 C0 75 ?? 85 FF 74 ?? 57 E8 ?? ?? ?? ?? 83 C4  
04 A3 ?? ?? ?? ?? 89 15 ?? ?? ?? ?? EB ?? 8B 3D ?? ?? ?? ?? 68 44 F0 41 00 53 FF D7 85 C0 75 ?? C6 05 ?? ?? ?? ?? 01 EB ?? 68 50 F0 41 00 53 FF D7 0F  
B6 0D ?? ?? ?? ?? 85 C0 BA 01 00 00 00 0F 44 CA 88 0D ?? ?? ?? ?? ?? 8B 8D ?? ?? ?? ?? ?? 8B 85 ?? ?? ?? ?? 3B F1 0F 8C ?? ?? ?? ?? 5B 5F 8D 85 ?? ?? ?? ??  
50 6A 10 FF 15 ?? ?? ?? ?? 33 C9 85 C0 7E ?? 0F 1F 44 00 ?? 80 BC 8D ?? ?? ?? ?? 19 74 ?? 41 3B C8 7C ?? E8 ?? ?? ?? ?? 0F 57 C0 C7 85 ?? ?? ?? ?? 44  
00 00 00 68 04 01 00 00 8D 85 ?? ?? ?? ?? 66 0F 13 85 ?? ?? ?? ?? ?? 50 6A 00 66 0F 13 85 ?? ?? ?? ?? 66 0F 13 85 ?? ?? ?? ?? 66 0F 13 85 ?? ?? ?? ?? 66  
0F 13 85 ?? ?? ?? ?? 66 0F 13 85 ?? ?? ?? ?? 66 0F 13 85 ?? ?? ?? ?? FF 15 ?? ?? ?? ?? 85 C0 75 ?? 8B 4D ?? 33 CD 5E E8 ?? ?? ??  
?? ?? 8B E5 5D C2 10 00 68 70 5E 42 00 8D 85 ?? ?? ?? ?? 50 FF 15 ?? ?? ?? ?? 8B 35 ?? ?? ?? ?? 8D 85 ?? ?? ?? ?? 50 8D 85 ?? ?? ?? ?? 50 FF D6 68 80  
5E 42 00 8D 85 ?? ?? ?? ?? 50 FF D6 68 04 01 00 00 8D 85 ?? ?? ?? ?? 50 FF 15 ?? ?? ?? ?? 68 90 5E 42 00 8D 85 ?? ?? ?? ?? 50 FF D6 8D 85 ?? ?? ?? ??  
50 8D 85 ?? ?? ?? ?? 50 6A 00 6A 00 68 00 00 00 08 6A 00 6A 00 6A 00 8D 85 ?? ?? ?? ?? 50 8D 85 ?? ?? ?? ?? 50 FF 15 ?? ?? ?? ?? 85 C0 74 ?? FF B5  
?? ?? ?? ?? 8B 35 ?? ?? ?? ?? FF D6 FF B5 ?? ?? ?? ?? FF D6 6A 00 FF 15 ?? ?? ?? ??}
```

condition:

filesize >= 150KB and filesize <= 250KB and

4 of (\$s\*) and

1 of (\$main\*)

}

## REPORT

### ABOUT MCAFEE

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

[www.mcafee.com](http://www.mcafee.com)

### MCAFEE ATR

The McAfee® Advanced Threat Research Operational Intelligence team operates globally around the clock, keeping watch of the latest cyber campaigns and actively tracking the most impactful cyber threats. Several McAfee products and reports, such as MVISION Insights and APG ATLAS, are fueled with the team's intelligence work. In addition to providing the latest Threat Intelligence to our customers, the team also performs unique quality checks and enriches the incoming data from all of McAfee's sensors in a way that allows customers to hit the ground running and focus on the threats that matter.

[Subscribe to receive our Threat Information.](#)

### ADDITIONAL RESOURCES

<https://www.bleepingcomputer.com/news/security/us-cities-disclose-data-breaches-after-vendors-ransomware-attack/>



6220 America Center Drive  
San Jose, CA 95002  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2021 McAfee, LLC. 4713\_0421  
APRIL 2021