한국 대상 최신 APT 공격, 작전명 미스터리 베이비(Operation Mystery Baby) 주의!

By 알약(Alyac)

Published: 2018-11-01 · Archived: 2026-04-05 18:26:54 UTC

알약(Alyac) 2018. 11. 2. 01:44

안녕하세요? 이스트시큐리티 사이버 위협 인텔리전스(CTI) 전문조직인 시큐리티대응센터 (이하 ESRC) 입니다.

ESRC에서는 지난 2018년 10월 31일 제작된 최신 APT공격용 악성파일을 다수 발견해 긴급 대응을 완료하였습니다.

이 악성파일들은 한국시간(KST) 기준으로 10월 31일 00시 48분경 부터 13시 15분경 사이에 집중적으로 빌드되었고, 감염 환경에 따라 32비트와 64비트용이 각각 다르게 생성됩니다.

특히, 이 악성파일들은 한국의 특정 보안제품 아이콘으로 위장하고 있으며, 해당 리소스와 그룹 아이콘 등의 언어가 한국어 코드(1042)로 설정되어 있고, 컴퓨터가 감염될 경우 시스템의 주요 정보와 키보드 입력 내용, 사용자 계정 등의 민감 자료가 외부로 무단 유출될 수 있습니다.

[그림 1] 한국 보안 제품 아이콘으로 위장하고 있는 악성코드 화면

금번 발견된 악성코드의 다이얼로그 리소스에는 "About baby" 내용의 캡션이 포함되어 있고, "baby, Version 1.0", "Copyright (C) 2017" 텍스트 코드가 존재하며, 뮤텍스 함수로도 유사한 키워드를 사용하고 있습니다.

ESRC는 위협 인텔리전스 기반으로 과거 유사 사례를 비교 분석했으며, 지난 04월 19일 "작전명 베이비 코인(Operation Baby Coin)" 내용으로 포스팅한 공격 벡터와 기반 코드들이 강력하게 연결되는 것을 확인했습니다.

그리고 이번 최신 APT공격을 **"작전명 미스터리 베이비(Operation Mystery Baby)"**로 추가 명명하고, "쓰렛 인사이드(Threat Inside)" 서비스를 통해 보다 다양한 침해지표(IoC) 등을 별도 제공할 예정입니다.

과거 초기 시리즈는 한국의 보안 블로그에서 "문서파일로 위장한 북한 사이버공격 전격해부"라는 문서로 공개된 바 있고, 해외 malware.lu 사이트에서 초기 변종에 대한 분석 자료를 "KimJongRAT/stealer" 제목으로 공개하기도 했습니다.

[그림 2] "작전명 미스터리 베이비" 악성코드의 다이얼로그 데이터

현재 해당 위협그룹은 특정 정부가 지원하고 있는 것으로 분류되어 있으며, ESRC에서는 해당 그룹이 최근 매우 활발하게 사이버 첩보작전에 참여하는 의심 정황을 포착했습니다.

지난 4월에는 "CVE-2017-11882" 취약점과 스피어 피싱(Spear Phishing) 기법을 결합해 암호화폐 소재로 공격이 수행되었고, 공격자는 한글 표현을 자유자재로 구사하는 것이 확인된 바 있습니다.

ESRC는 이와 유사한 위협을 면밀히 추적 조사하던 중 한국 포털 회사의 고객센터로 위장해 피싱 공격을 수행한 사례를 확인했는데, 해외 호스팅 서비스를 활용해 서버를 구축한 후, 한국의 특정 이용자를 겨냥해 무료 웹 메일 계정탈취를 시도한 바 있습니다.

또한, 동일한 공격 흐름에서 HWP 문서파일 취약점을 이용한 공격도 복합적으로 사용한 이력이 확인되었고, 이 공격은 지난 02월에 공개했던 "오퍼레이션 김수키(Kimsuky)의 은밀한 활동, 한국 맞춤형 APT 공격은 현재 진행형" 포스트를 참고하시기 바랍니다.

[그림 3] 한국 무료 웹 메일 보안서비스 공지로 사칭한 피싱 메일 사례

주요 악성코드는 한국의 간호 의료 분야의 출판사 웹 사이트를 통해 유포되었으며, 기존 공격벡터와 동일하게 일부는 암호화된 형태로 존재했습니다.

"작전명 베이비 코인(Operation Baby Coin)"에서는 암호화된 "UPDATE.CA" 파일이 복호화된 "UPDATE.TMP" 파일로 생성되었고, 당시 후속공격 때와 비슷하게 이번 작전에는 암호화된 "store.sys" 파일이 복호화된 "update.tmp" 파일명으로 변경되었습니다.

암호화된 파일은 다음과 같은 함수를 통해 복호화되는데, 다운로드된 파일의 최초 오프셋 0x00 ~ 0x0F 16바이트의 Hex 데이터를 16개(16X16=256바이트)로 만들어 Key Table 데이터로 생성합니다.

그리고 0x00 부터 0xFF 까지 총 256바이트의 Index Table 데이터를 순차적으로 만든 후 아래 연산 로직 등을 통해 복호화가 진행됩니다.

결국 암호화된 처음 16바이트를 Key 값으로 사용하는 RC4 암호화 암고리즘을 이용하고 있습니다.

```
v3 = a1;
v20 = operator new(a3);
v4 = 0;
v5 = (char *)(v3 + 260);
do
{
```

```
  v5[v4] = v4;
  ++v4;
}
while ( v4 < 256 );
v6 = 16;
do
{
  *(_BYTE *)(v3 + v6 + 4) = *(_BYTE *)(v6 % 16 + v3 + 4);
  ++v6;
}
while ( v6 < 256 );
v7 = 0;
v8 = 256;
do
{
  v9 = *v5;
  v7 += *v5 + *(v5 - 256);
  *v5++ = *(_BYTE *)(v7 + v3 + 260);
  --v8;
  *(_BYTE *)(v7 + v3 + 260) = v9;
}
while ( v8 );
v10 = a3;
v11 = 0;
v12 = 0;
v13 = 0;
```

```
if ( a3 > 0 )
{
  while ( 1 )
  {
    v17 = *(_BYTE *)(++v11 + v3 + 260);
    v18 = (unsigned __int8 *)(v11 + v3 + 260);
    v19 = (unsigned __int8 *)((unsigned __int8)(v17 + v12) + v3 + 260);
    *v18 = *v19;
    *v19 = v17;
    v14 = v20;
    v20[v13++] = *(_BYTE *)((v17 + *v18) % 256 + v3 + 260);
    if ( v13 >= a3 )
      break;
    v12 += v17;
  }
  v10 = a3;
}
else
{
  v14 = v20;
}
if ( v10 > 0 )
{
  v15 = a2;
  v16 = v10;
  do
```

```
  {
    *v15 ^= v15[v14 - a2];
    ++v15;
    --v16;
  }
  while ( v16 );
 }
 operator delete(v14);
}
```

그외 "sys32.msi", "sys64.msi" 파일은 각각 "micr.tmp", "micr.tmp64" 파일명으로 기존 형태를 그대로 유지하고 있으며, 32비트와 64비트 플랫폼 환경에 따라 선택적으로 감염이 진행됩니다.

[그림 4] 암호화된 파일을 로컬 경로에 파일명을 설정해 생성하는 함수

또한, 유사변종들은 'ttmp.log' 파일을 활용하는 공통적인 특징을 가지고 있습니다.

[그림 4-1] ttmp.log 파일을 활용하는 코드 화면

한편 메인 악성코드는 UPX 프로그램으로 실행압축되어 있고, "Microsoft Windows Security" 속성으로 위장하고 있습니다.

기존 시리즈와 동일하게 "sysninit - exe.dll" 오리지널 이름을 가지고 있으며, "Landstart", "Wakestart" 2개의 Export 함수를 사용합니다.

상반기 이후 유사 변종이 "ShellExploit" 함수를 사용한 것과 비교해 보면, 공격자가 코드를 계속 수정해 사용하고 있다는 것을 확인할 수 있습니다.

추가로 달라진 부분 중에 또 하나는 C2 서버와 통신할 때 사용하는 폼 데이터가 일부 수정된 것입니다. 이전에 사용된 폼 데이터와 이번에 사용된 폼 데이터를 비교해 보면 다음과 같이 달라진 것을 알 수 있습니다.

["작전명 베이비 코인(Operation Baby Coin)"]

"Content-Type: multipart/form-data; boundary=----------**7dab371b0124**\r\n"

["작전명 미스터리 베이비(Operation Mystery Baby)"]

"Content-Type: multipart/form-data; boundary=--------**1650502037**\r\n"

[그림 5] 최신 변종의 폼 데이터 코드 화면

악성코드는 감염된 컴퓨터에서 키로깅과 다양한 데이터를 탈취해 한국의 특정 서버로 전송을 시도하며, 수집 대상의 목록에는 한국에서 주로 활용되는 문서와 압축포맷이 존재합니다.

특히, "%s*.keystore" 파일을 수집하는 것이 흥미로운데, 안드로이드 애플리케이션 개발 및 서명에 활용되는 파일까지 노리고 있는 점에 주목됩니다.

```
CommandLine = 0;

memset(&v26, 0, 0x207u);

v8 = 6044257;

WideCharToMultiByte(0, 0, &word_100E4FB8, -1, &MultiByteStr, 520, 0, 0);

v5 = 1;

v9 = GetLogicalDrives();

do

{

 sprintf(

  &CommandLine,

  "cmd.exe /c dir %s*.hwp %s*.pdf %s*.doc %s*.docx %s*.xls %s*.xlsx %s*.bin %s*.ppt %s*.zip %s*.rar %s*.alz %s*.txt %s*.json %s*.dat %s*.jpg %s*.png %s*.keystore /s >> \"%s\",

  &v8,

  &v8,

  &v8,
```

이전에 보고됐던 악성코드의 파일수집 대상 확장자 목록은 아래와 같으며, 위와 비교해 보면 "%s*.pptx"가 제거됐고, 그외 몇 가지 확장자가 추가된 것을 알 수 있습니다.

"cmd.exe /c dir %s*.hwp %s*.pdf %s*.doc %s*.docx %s*.xls %s*.xlsx %s*.ppt %s*.pptx %s*.zip %s*.rar %s*.alz /s >> \"%s\""

이 악성코드 시리즈의 초기 모델과 마찬가지로 공격자는 꾸준히 동일한 전략을 사용합니다.

물론 과거에는 제작자가 직접 구축한 서버와 이메일 계정 정보 등에서 다양한 개발자 흔적과 단서가 발견된 바 있는데, 국적과 특정 이름 등이 보고된 바 있습니다.

해당 악성코드에 감염되면, 수집된 다양한 정보는 한국어로 서비스되는 2개의 웹 사이트로 유출이 시도됩니다.

[그림 6] 감염된 시스템의 정보가 유출 시도되는 서버 화면

ESRC에서는 2018년 10월 31일 제작된 "작전명 미스터리 베이비(Operation Mystery Baby)의 정보수집 모듈 악성파일과 유사한 변종 중 한국 특정 회사의 디지털 서명 내용을 포함한 변종을 확인했습니다.

해당 변종은 2018년 02월 01일 제작되었으며, 디지털 서명 정보에는 "현재 시스템 시간을 확인하거나 서명된 파일의 스탬프를 확인하는데 필요한 인증서가 유효 기간내에 있지 않습니다" 내용을 포함하고 있습니다.

[그림 7] 디지털 서명 정보를 포함하고 있는 유사 변종 화면

이처럼 정부지원을 받는 것으로 추정되는 APT 공격그룹(state-sponsored actor)의 활동이 지금도 매우 활발히 움직이고 있다는 점에 각별한 주의가 필요합니다.

특히, 수 개월 이상 한국의 보안 제품처럼 위장을 하고, 국내외 다양한 웹 사이트를 해킹해 명령제어(C2)서버로 활용하고 있어 예기치 못한 피해를 입지 않도록 적극적인 보안강화가 요구됩니다.

이스트시큐리티 대응센터(ESRC)는 국가기반 사이버 위협그룹에 대한 체계적인 인텔리전스 연구와 추적을 통해, 유사 보안위협으로 인한 노출을 미연에 예방하고, 피해가 최소화될 수 있도록 관련 보안 모니터링을 강화하고 있습니다.