김수키(Kimsuky) 조직, 스텔스 파워(Operation Stealth Power) 침묵 작전

By 알약(Alyac)

Published: 2019-04-03 · Archived: 2026-04-05 17:47:07 UTC

안녕하세요? 이스트시큐리티 시큐리티대응센터 (이하 ESRC) 입니다.

2019년 04월 01일 【최근 한반도 관련 주요국 동향】이라는 내용과 【3.17 미국의 편타곤 비밀 국가안보회의】 등의 내용으로 스피어 피싱(Spear Phishing) 공격이 수행되고 있음을 확인했습니다.

파일명은 다르지만, 두개의 파일은 같은 공격기법과 내용을 담고 있으며, 미국 국방부 건물인 펜타곤(PENTAGON) 표현에서는 '편타곤'으로 일부 오타가 존재합니다.

이번 지능형지속위협(APT) 공격을 받은 곳들은 주로 외교·안보·통일분야 및 대북/탈북단체 등에서 활동하는 곳들 입니다.

ESRC에서는 지난 3월 21일 워터링 홀(Watering Hole) 공격 '오퍼레이션 로우 킥(Operation Low Kick)'을 보고한 바 있는데, 이번 공격들도 같은 위협조직에 의해 진행되고 있음을 확인했습니다.

■ 은밀한 파워쉘 위협, '오퍼레이션 스텔스 파워(Operation Stealth Power)' 배경

공격자는 한국의 특정 분야에 속한 사람들만 표적화하여, 해킹용 이메일을 발송한 정황이 포착되었습니다.

실제 공격에 사용된 화면을 입수하여 분석한 결과 나름 능숙하고 정교한 한국어 표현이 사용되었으며, 암호화된 HWP 악성 코드를 활용해 해킹된 한국의 특정 웹 서버(C2)와 통신을 수행합니다.

그런 다음 파워쉘 기반의 키로그(Keylog) 명령을 수행하여, 외부 노출을 최대한 은닉한 채 내부 정보탈취를 수행합니다.

ESRC는 이번 공격이 보안 레이더에서 탐지하기 어려울 정도의 암호화된 침투기능을 활용한 점과 파워쉘 코드 기반의 스파이 기능이 사용된 특징을 조합해 '**오퍼레이션 스텔스 파워(Operation Stealth Power)**'로 명명했습니다.

■ 정부후원을 받는 공격조직, 일명 '김수키(Kimsuky)' 조직 대남 사이버 위협 활동 증가

[그림 1] 해킹 공격으로 사용된 스피어 피싱(Spear Phishing) 이메일 화면

스피어 피싱 공격에 사용된 이메일을 확인해 보면, 마치 구글 지메일에서 발송된 것처럼 보이지만, 실제 분석을 해보면 발신자 도메인 조작을 수행했으며, 한국의 특정 호스트에서 발송되었습니다.

이메일에는 '최근 한반도 관련 주요국 동향.hwp' 파일이 첨부되어 있는데, 이것이 바로 악의적 코드가 담겨 있는 악성문서 파일입니다.

HWP 문서내부의 스트림 데이터에는 'BIN0001.eps' 포스트 스크립트(Post Script) 파일이 포함된 것을 볼 수 있습니다. 그리고 해당 데이터는 2019년 03월 31일 일요일에 생성되었습니다.

악성코드를 제작하는 공격자들이 일요일에도 활발하게 움직이고 있다는 것을 배제하기 어렵습니다.

[그림 2] HWP 내부 스트림 및 생성날짜 화면

HWP 파일은 문서작성 프로그램 자체의 암호화 기능을 적용해, 암호을 알기 전까진 EPS 코드를 분리해 분석할 수 없고, 보안 프로그램이 악성여부를 파악하는데도 어려움이 발생하게 됩니다.

그래서 해킹 이메일 본문에 별도의 암호를 지정해 발송하게 되는 것이며, 공격 수신자로 하여금 해킹 이메일 원문을 외부에 신고 또는 제보하지 않도록 삭제유도의 문구를 포함하고 있는 특징을 보이고 있습니다.

암호를 해독해 내부 포스트 스크립트(Post Script) 코드를 파악해 보면, 쉘코드(Shellcode)가 포함된 것을 알 수 있습니다.

[그림 3] EPS 내부 쉘코드 화면

쉘코드는 기존 김수키 조직이 사용하던 방식에서 한단계 더 변화가 되었으며, 암호화된 코드를 복호화하면 한국의 특정 호스트로 통신을 수행하는 것이 확인됩니다.

ESRC에서는 해당 웹 서버가 해킹되어 악용되고 있는 것으로 파악해, 한국인터넷진흥원(KISA)과 긴밀히 협력해 보안조치 강화를 진행 중입니다.

이번 공격에는 과거 사례와는 다르게 'mshta.exe' 프로세스를 통해 'HTML 응용 프로그램(.HTA)' 형태인 'first.hta' 파일을 실행하도록 만듭니다.

[그림 4] 쉘코드 내부에 숨겨져 있는 악성 HTA 연결 코드

해킹된 C2 서버의 보안조치가 일부 진행되면서, 공격자는 제거되었던 'first.hta' 파일을 다시 변경하고 있기도 합니다.

2019년 04월 01일 오후에는 다음과 같이 'Hello!' 문구가 보여지고, 배경이 흰색이었지만, 2019년 04월 02일 오후에는 'This is Your First Screen!' 문구로 변경되었고, 배경화면이 적색으로 변경되었습니다.

[그림 5] 변경되었던 'first.hta' 웹 사이트 화면

겉으로 보기에는 마치 로그인 화면 사이트처럼 보이지만, 단순히 로그인 폼처럼 위장한 것이며 실제로 로그인 핵심 기능은 전혀 존재하지 않습니다.

다만, 내부 VBScript 코드를 통해 특정 호스트로 연결을 시도하게 되며, 이 다음부터 악의적인 C2와 명령을 주고 받게 됩니다.

그리고 2차 스테이지(Stage) 경로 등이 일부 변경되었습니다.

[그림 6] 'first.hta' 내부 1차 스테이지 코드 화면 비교

1차 스테이지에서 2차 스테이지로 연결되는 코드는 공격시점에 따라 하위주소가 변경된 바 있지만, 특별히 내부 코드에서 큰 변화는 발견되지 않았습니다.

'expres.php' 2차 코드가 작동하면, 다음과 같이 레지스트리 설정을 통한 보안 권한 변경과 함께 파워쉘 명령을 통해 또 다른 3차 스테이지로 연결을 시도합니다.

연결되는 URL 경로는 'moonx.hta' 파일이 연결되고, 조건에 따라 'cow.php', 'expres.php' 등을 다시 호출하게 됩니다. PHP 명령의 별도 인자(파라미터) 값의 조건에 따라 명령이 변경될 수 있습니다.

그리고 접속 상황에 따라 다음과 같은 파웰쉘 명령을 수행해 'mshta.exe' 프로세스를 종료하기도 합니다.

Set WShell=CreateObject("WScript.Shell"):retu=WShell.run("powershell.exe taskkill /im mshta.exe /f" , 0 ,true)

[그림 7] 'expres.php' 명령어 코드 화면

그리고 마지막 단계에서 연결되는 'driving.ps1' 파워쉘 스크립트를 통해 감염된 컴퓨터의 키보드 입력내용(키로깅)과 프로세스, 서비스 리스트 등의 정보를 수집해 해당 서버로 전송하게 됩니다.

[그림 8] 키보드 입력 내용 저장 함수

수집된 정보들은 'upload.php' 명령을 통해 C2 서버로 은밀하게 유출됩니다.

[그림 9] 컴퓨터 정보 수집 후 유출을 시도하는 코드

■ 유사 위협 연관성 분석

이번 HWP 문서파일 공격에서 문서 작성자는 'Tom' 계정이 사용되었습니다.

[그림 10] 악성 HWP 문서 메타 데이터 정보

ESRC는 2019년 03월 08일 동일한 C2 도메인에서 유포된 또 다른 위협사례를 포착한 바 있는데, 이때는 단순 URL 피싱 기법이었고, 한국 포털사의 아이디와 암호를 탈취 시도하는 형태입니다.

이메일 본문에 이번 C2와 동일한 호스트와 링크를 걸어 사용하였고, 마치 '국가안전보장회의(NSC)' 취재 내용처럼 이용자를 현혹하고 있었습니다.

[그림 11] 피싱용 악성 이메일 본문 내용

그리고 [다운로드] 링크를 통해 가짜 포털사 로그인 화면에서 계정과 암호가 성공적으로 탈취되면, 동일한 C2 서버 하위에 존재하는 정상 PDF 문서를 보여주어 이용자로 하여금 문제 없는 내용처럼 신뢰하도록 만듭니다.

[그림 12] 개인정보 유출 후에 보여지는 정상적인 PDF 화면

ESRC는 이 문서를 분석하는 과정에서 흥미로운 단서를 포착했습니다. 바로 이곳에 사용된 PDF 파일의 작성자 계정에서도 이번 HWP 취약점 공격과 마찬가지로 'Tom' 계정이 동일하게 발견됐습니다.

공격자는 실제 사용 중인 컴퓨터의 윈도우즈 계정명을 'Tom'으로 설정해 사용하고 있을 것으로 확신합니다.

[그림 13] PDF 문서 속성화면에 포함된 'Tom' 계정 화면

이 정상적인 PDF 문서를 보여주는 공격에 사용된 호스트를 살펴보면 다음과 같습니다.

- enindi25-142.godo.co[.]kr (106.249.25.142)

그리고 2019년 03월 04일 외교통일위원회를 사칭해 수행된 피싱에서도 이와 동일한 데이터가 사용됩니다.

이 공격에 사용된 Base64 코드를 분석하면, 'tcjst.com' 도메인으로 접속 신호로그를 전송하는 비콘(Beacon) 기능이 존재합니다.

- tcjst.com/img/dot[.]gif

[그림 14] 'tcjst.com' 비콘 코드 화면

이 비콘 코드는 한국의 여러 침해사고에서 발견되고 있는 특징이 있으며, 김수키(Kimsuky) 위협 조직의 피싱 사례에서 발견이 되고 있습니다.

이와 관련된 내용들은 추후 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 위협 인텔리전스 리포트와 IoC(침해지표) 등을 제공할 예정입니다.