'오퍼레이션 배틀 크루저' 다양한 취약점으로 국내외 APT 공격 지속

By 알약(Alyac)

Published: 2018-04-11 · Archived: 2026-04-05 21:09:36 UTC

안녕하세요. 이스트시큐리티 시큐리티대응센터(ESRC)입니다.

이스트시큐리티 대응센터에서는 오퍼레이션 아라비안나이트를 수행했던 라자루스(Lazarus) 조직이 국내외에서 다양한 작전을 수행하고 있는 것을 확인했습니다.

이번 '**오퍼레이션은 배틀 크루저(Operation Battle Cruiser)**'로 명명하고 지속적인 추적과 연관성 분석을 진행하고 있습니다.

정부 차원의 후원을 받는 것으로 추정되는 공격(state-sponsored actor)그룹은 HWP 문서 파일 취약점을 활용해 한국의 특정 분야 이용자에게 스피어피싱(Spear Phishing) 공격을 수행했습니다.

이 악성 문서 파일은 2018년 03월 26일 제작되었으며, 취약점 발생시 다운로드되는 바이너리 파일도 HWP 악성문서와 동일하게 2018년 03월 26일 제작되었습니다.

[그림 1] HWP 문서 파일의 구조 및 생성 날짜

문서파일의 구조를 살펴보면 'BinData/BIN0001.PS' 스트림에 8,176 바이트의 Post Script 파일이 포함되어 있는 것을 알 수 있습니다.

[그림 2] Post Script 코드 사이즈 화면

'BIN0001.PS' 이름의 Post Script 파일은 압축된 Stream으로 존재하며, Zlib 압축코드를 해제하면, 내부에 다음과 같이 악의적인 스크립트 코드가 존재합니다.

스크립트는 내부에 포함되어 있는 Shellcode 값을 XOR 0x29 변환을 거쳐 특정 명령제어(C2) 서버로 통신을 시도하게 됩니다.

[그림 3] BIN0001.PS 압축해제 화면

Shellcode 인코딩 부분이 변환되면 내부에 숨겨져 있던 특정 도메인이 보여지게 됩니다. 해당 도메인(naviilibs.com)에는 중간에 0x00 코드가 다수 포함하고 있어, 탐지 및 분석에 어려움이 있을 수 있습니다.

아울러 공격자는 악성 바이너리 파일명을 **'battle32.avi', 'battle64.avi'** 형식으로 지정한 부분이 흥미롭습니다.

'avi' 확장명이 마치 동영상 파일로 인식할 수 있지만, 실제로는 DLL 기반의 라이브러리 파일이며, 운영체제 플랫폼에 따라 32비트, 64비트 형태가 실행됩니다.

[그림 4] Shellcode 내부에 숨겨져 있는 C2 화면

- naviilibs.com/video/battle32.avi

- naviilibs.com/video/battle64.avi

추가로 다운로드되는 악성 파일은 이른바 라자루스(Lazarus) 그룹이 사용하는 Manuscrypt (Kaspersky Lab) 시리즈이며, 다음과 같은 사이트로 정보 유출 시도를 하게 됩니다.

- hypnosmd.com/include/top.php

- 0756rz.com/include/left.php

- 51xz8.com/include/top.php

또한, 공격에 사용된 코드는 수년 전부터 한국의 국방, 대북, 안보단체 및 다수의 공기업과 기관, 학계 등에서 지속적으로 발견되었던 계열과 유사하며, 2014년 미국 소니픽쳐스(사) 공격 캠페인 시리즈 종류와도 비슷한 형태입니다.

[그림 5] 좌측 2018년 악성파일('battle32.avi')과 우측 2016년 제작 악성파일 비교 화면

더불어 2018년 2월 24일 해외 서버에서 발견된 악성 파일과도 코드 기반 유사도가 높은 것으로 분석되었습니다. 이 파일은 터키 금융기관 등을 대상으로 공격이 수행됐다고 알려져 있습니다.

해당 공격은 2018년 02월 26일 작성된 MS오피스 문서(.docx)의 CVE-2018-4878 Flash Exploit 코드가 사용되었습니다. 이 취약점은 2017년 공격 당시 '**금성121(Geumseong121)**' 그룹이 최초 사용한 Zero-Day 공격이었습니다.

[그림 6] 가상통화 사칭 명령제어(C2) 서버 화면

공격에 사용된 서버(falcancoin.io)는 마치 해외 특정 가상통화 사이트 도메인처럼 사칭했으며, 압축파일(ZIP) 확장자로 위장한 악성 DLL 파일을 다운로드하게 제작했습니다. 이 악성파일은 2018년 02월 24일 제작되었고, 서버에 등록된 날짜와도 일치합니다.

다운로드되는 파일은 'battle32.avi' 때와 마찬가지로 32비트와 64비트로 파일명을 구분해 사용했습니다. 또한, 파일 내부의 리소스는 한국어 기반으로 작성된 것을 알 수 있습니다.

[그림 7] 한국어 리소스 기반으로 작성된 'package32.zip' 화면

'battle32.avi' 악성파일과 'package32.zip' 파일을 비교해 보면 통신 등에 다음과 같이 동일한 코드가 사용된 것을 알 수 있습니다.

[그림 8] 동일한 코드를 사용하는 화면

'*dJU!*JE&!M@UNQ@' 코드는 다음과 같이 유사 시리즈 파일에서 지속적으로 발견이 되고 있으며, 동일한 소스코드가 재활용될 가능성도 배제할 수 없습니다.

[그림 9] 'package32.zip' 악성 파일 패킷 화면

더불어 이 계열의 악성파일은 한국을 포함한 국내외 가상통화거래소 공격에 사용된 것으로 추정되는 악성파일에서 발견된 바 있습니다.

2017년 03월 제작된 것으로 알려진 MS오피스 엑셀(XLS)문서이며, 마치 멕시코 금융문서 내용으로 위장한 형태는 매크로 기능을 통해 악성 파일을 추가 설치하고 있습니다.

[그림 10] 매크로 기법으로 유포된 유사 변종 XLS 악성 파일

그런데 이번 매크로에 사용한 기법은 2018년 01월 31일 알약 공식 블로그를 통해 공개됐던 '오퍼레이션 아라비안 나이트' 공격자가 사용한 방식과 여러가지로 비슷해 동일한 공격 그룹으로 추정되며, 지속적으로 다양한 오퍼레이션 수행을 확인할 수 있습니다.

[그림 11] 오퍼레이션 배틀 크루저와 아라비안나이트 매크로 계열 비교 화면

당시 시점에 발견된 다양한 유사 변종 중에는 주로 비트코인 관련 내용을 포함하고 있기도 합니다. 다음에 보여지는 엑셀 문서 역시 동일한 매크로 취약점을 이용해 유포된 것 중에 하나입니다.

[그림 12] 아라비안 나이트 계열의 엑셀 매크로 악성 문서 변종 화면

2017년 11월 HWP 취약점을 통해 한국 가상통화 거래자를 대상으로 한 스피어 공격용 악성파일과 2018년 02월 제작된 'package32.zip 파일의 코드 유사도를 비교해 보면 다음과 같이 매우 유사하다는 것을 알 수 있습니다. 또한, 두 파일 모두 리소스는 한국어 기반으로 제작되어 있습니다.

[그림 13] HWP 취약점과 CVE-2018-4878 취약점을 통해 유포된 악성파일 코드 유사도 화면

이스트시큐리티의 인텔리전스 보고서인 '20170512_ESRC1705_White_Threat Intelligence Report_Arabian Night' 자료를 보면 공격자는 다음과 같은 대한민국 명령제어(C2) 서버를 사용하였습니다.

[그림 14] 아라비안 나이트 인텔리전스 보고서 내용 화면

그런데 우연하게도 해당 명령제어 서버 중 일부는 2016년 국방관련 웹 사이트의 워터링 홀(Watering Hole) 공격에서도 동일하게 식별이 됩니다.

- 211.233.13.62 (KR)

- 221.138.17.152 (KR)

[그림 15] 국방 분야 사이버 공격에서 확인된 악성파일의 명령제어 화면

동일한 C2 IP 주소를 사용한 이 악성파일들은 2009년 7.7 DDoS 공격 때부터 이어진 명령조합코드 스타일을 그대로 사용하고 있는 특징이 있습니다.

[그림 16] 국방 분야 공격에 사용된 악성파일의 명령 조합 코드 화면

이처럼 국가 차원의 지원을 받는 것으로 추정되는 공격자(state-sponsored actor)의 활동이 한국뿐만 아니라 글로벌적으로 활동하고 있습니다.

그동안 널리 알려져 있지 않았지만, 금성121(Geumseong121) 그룹과 김수키(Kimsuky) 계열의 오퍼레이션에서 IoC간 오버랩된 부분이 다수 확인되었는데, 이번에는 라자루스(Lazarus) 그룹이 2017년 금성121(Geumseong121) 그룹에서 사용했던 CVE-2018-4878 취약점을 활용했다는 점이 주목됩니다.

이스트시큐리티 대응센터(ESRC)에서는 이와 관련된 인텔리전스 연구와 추적을 지속적으로 유지하고, 유사한 보안위협으로 인한 피해가 최소화될 수 있도록 관련 모니터링을 강화하고 있습니다.