라자루스 APT 조직, 오퍼레이션 익스트림 잡(Operation Extreme Job)으로 공격 수행

By 알약(Alyac)

Published: 2019-01-30 · Archived: 2026-04-06 00:03:31 UTC

라자루스(Lazarus)그룹 '익스트림 잡(Operation Extreme Job)' APT 공격

안녕하세요?

이스트시큐리티 CTI 조직인 시큐리티대응센터(이하 ESRC)는 정부후원을 받는 공격자(State-sponsored Actor)가 수행한 최신 지능형지속위협(APT) 캠페인을 확인했습니다.

이 그룹은 이른바 라자루스(Lazarus) 이름으로 널리 알려져 있고, 2018년 09월 06일 미 법무부에서 미국 소니픽쳐스 영화사 해킹, 방글라데시 은행 해킹, 워너크라이 랜섬웨어 유포 등의 혐의로 LA 연방법원에 기소고발을 하였고, 미연방수사국(FBI)에서는 지명수배를 내린 상태입니다.

https://www.fbi.gov/wanted/cyber/park-jin-hyok/@@download.pdf

https://www.justice.gov/opa/press-release/file/1092091/download

특히, 이번에 발견된 공격은 그동안 국내외 주요 침해사고에서 발견됐던 DOC 매크로와 거의 같은 코드기법이 재활용됐으며, 공격벡터상 DOC 파일명도 기존과 동일합니다.

이는 2017년 05월 작성된 ESRC 인텔리전스 리포트 '오퍼레이션 아라비안 나이트'(20170512_ESRC1705_White_Threat Intelligence Report_Arabian Night) 사례와 동일 연장선상에 있다고 볼 수 있습니다.

2019년 01월 30일 새로 발견된 악성파일의 이름은 '**Job Description.doc**' 으로, 이 워드파일은 2019년 01월 29일 오후 9시 경에 제작되었으며, 다음과 같이 한국어(949) 기반에서 제작된 것을 알 수 있습니다.

ESRC에서는 이번 공격벡터에서 사용된 키워드 등을 활용해 이른바 '극한직업'이라는 의미의 **'오퍼레이션 익스트림 잡(Operation Extreme Job)'**으로 사이버 작전명을 명명했습니다.

이와 관련된 APT 캠페인을 지속적으로 추적 분석 중이며, 보다 상세한 IoC 및 인텔리전스 리포트는 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 제공할 예정입니다.

DOC 매크로 코드를 이용한 공격벡터 흐름 분석

[그림 1] 'Job Description.doc' 파일의 속성 정보

이 파일은 한국의 특정 웹 사이트를 통해 유포되었으며, IP Camera 또는 CCTV 등을 판매하는 곳으로 악성 코드 유포에 악용되었습니다.

MS Word 파일의 내부 OLE 코드구조를 살펴보면, 아래와 같이 매크로 코드가 포함되어 있는 것을 알 수 있으며, 이 코드 역시 2019년 01월 29일 작성되어 있습니다.

[그림 2] 악성 코드 OLE 내부 구조

매크로 코드는 기존에 알려진 유사 위협사례 방식이 그대로 적용된 상태로 발견이 되었고, 'NewMacros' 함수에는 난독화된 매크로 코드들이 포함되어 있습니다.

[그림 3] 매크로 VBA 내부 코드 화면

난독화된 스트링 코드들은 다음과 같은 복호화 명령어를 통해 추가 악성코드를 생성하고 실행하게 됩니다. 여기에 사용된 연산루틴은 기존에도 여러차례 동일한 키로 사용된 기록을 가지고 있습니다.

'XOR 231(0xE7)' 키 연산을 통해 코드가 복호화되는데, 이 키값은 기존 유사한 위협에서도 지속적으로 발견된 바 있습니다.

[그림 4] 매크로 코드 복호화 연산 함수 루틴

2017년 3월 경 공격이 포착된 '오퍼레이션 아라비안 나이트'(20170512_ESRC1705_White_Threat Intelligence Report_Arabian Night)의 경우에는 한국의 특정 보안기업을 사칭해 스피어 피싱(Spear Phishing) 공격이 수행된 바 있습니다.

[그림 5] 한국 보안 기업으로 사칭한 스피어 피싱 공격 사례

'**Job Description.doc**' 악성파일이 실행되면 다음과 같이 보안 경고 메시지와 함께 [콘텐츠 사용] 매크로 실행 여부를 묻게 됩니다.

공격자는 DOC 문서 파일의 버전이 낮아 매크로를 실행해야만 정상적인 문서가 보인다는 가짜 메시지를 통해 이용자의 매크로 실행을 유도하게 됩니다.

[그림 6] 악성 문서 파일 실행시 보여지는 매크로 실행[콘텐츠 사용] 유도 화면

만약, 이용자가 [콘텐츠 사용] 버튼을 클릭해 매크로가 실행되면, 'Java Update Scheduler' 파일처럼 위장한 악성파일(jusched.exe)과 정상적인 문서가 다음과 같은 경로에 생성되고 몰래 실행됩니다.

- C:\Users\[사용자 계정명]\AppData\Roaming**jusched.exe** (악성파일)

- C:\Users\[사용자 계정명]\AppData\Roaming**Job Descriptions.doc** (정상문서)

[그림 7] 매크로가 실행되어 추가 파일이 생성된 화면

그리고 'Job Descriptions.doc' (직무 기술서)문서 내용을 보여주어, 이용자로 하여금 해당 문서파일이 정상으로 보이도록 현혹하게 됩니다.

정상 문서의 타이틀에는 'Systems Engineer' 내용을 가지고 있으며, 본문에는 미국의 하드웨어 네트워킹 및 보안서비스로 유명한 기업의 한국지사 직무기술과 모집내용을 담고 있습니다.

[그림 8] 특정 미국 기업의 한국지사 직무 기술 및 모집 내용

추가로 생성되는 악성파일은 마치 자바 업데이트 스케줄러처럼 위장하고 있는데, 이 악성파일은 한국시간(KST) 기준으로 '2019-01-29 21:00:47'에 제작되었습니다.

이 악성코드는 한국의 특정 웹 사이트(secuvision.co.kr)와 통신을 시도하고, 공격자의 추가 명령을 대기하게 됩니다.

[그림 9] 한국의 특정 웹 사이트와 통신을 시도하는 코드 화면

2009년 7.7 디도스 등 유사 공격 데이터 비교

이번 공격에 사용된 악성코드는 2009년 7.7 디도스 공격 당시 이후에 발견됐던 다수의 Lazarus 계열의 악성코드와 CMD 문자열 조합 방식이 유사하며, 'Job Descriptions.doc' 파일명도 여러차례 보고된 바 있습니다.

[그림 10] 과거 침해사고 악성코드와의 유사성 비교 화면

영문 직무기술서(Job Description) 문서로 위장한 APT 공격 사례는 2017년 12월 '3.20 공격 조직의 최신 오퍼레이션 '코인 매니저 (Coin Manager)" 내용으로 공개한 바 있습니다.

당시 악성코드 흐름의 유사성을 다시 한번 살펴보면 다음과 같습니다.

[그림 11] 2017년 공개한 라자루스 계열의 악성코드 함수 흐름 비교도

[Update]

CISCO Talos 블로그에서도 "Fake Cisco Job Posting Targets Korean Candidates" 내용으로 관련 분석자료를 공개하였습니다.

탈로스에서는 과거 유사 변종 케이스 2건에 대해 공개를 했으며, 모두 한국을 상대로 진행된 APT 공격 사례입니다.

- 주요 IT 정보보호 및 보안 업체 리스트.doc (MD5 : 78a5c82eb99266ed981f435d8c919a79)

- 이력서_자기소개서.xls (MD5 : fbd1cd15019c0dd6659a59bc93b8596f)

각각의 파일은 2017년 한국내에서 발견됐던 침해사고 관련 악성코드로 분류되어 있으며, 만든이가 'Jupiter' 계정과 C2 주소가 일부 동일하며, 악성 매크로 코드 내부에 페이로드 실행 파라미터를 보유하고 있습니다.

[그림 12] 시스코에서 공개한 악성 매크로 비교 화면

ESRC에서는 2017년 4월 21일 한국의 유명 컴퓨터 보안업체를 대상으로 유사 스피어 피싱(Spear Phishing) 공격이 수행된 것을 확인한 바 있습니다.

해당 공격에서는 DOC, XLS 매크로 공격이 아니라, HWP 취약점을 이용한 감염벡터가 사용되었습니다.

[그림 13] 한국 컴퓨터 보안기업을 대상으로 수행된 스피어 피싱 공격 화면

공격자는 미국 사이버 보안 시장의 현재와 미래라는 제목으로 수신자를 현혹했으며, '美 사이버 보안시장의 현재와 미래.hwp' 파일이 첨부되어 있었습니다.

HWP 악성파일은 EPS 취약점 코드에 의해 '%Temp%' 경로에 'jusched.exe' 파일명으로 악성코드를 생성하고, 재부팅시 자동 실행되도록 시작프로그램 경로에 'jusched.lnk' 형태로 등록합니다.

그리고 그 바로가기 대상의 실행인자 값에 'E5XT-RWW2-TW36-2ETS' 코드가 포함되어 있는 것을 확인할 수 있습니다.

이 코드는 '주요 IT 정보보호 및 보안 업체 리스트.doc' 매크로 코드에서 사용한 것과 일치합니다.

[그림 14] HWP 취약점으로 생성되는 악성코드의 동일한 파라미터 코드 값

그리고 명령제어(C2) 서버역시 다음과 같이 기존 매크로 공격 때와 동일하게 사용되었습니다.

- ilovesvc.com/HomePage1/Inquiry/privacy[.]asp

- syadplus.com/search/search_00[.]asp

ESRC에서는 라자루스(Lazarus) 계열의 오퍼레이션과 관련해 다음과 같은 내용 등을 공개한 바 있는데, 타임라인을 분석하는데 참고로 활용할 수 있습니다.

Source: https://blog.alyac.co.kr/2105