국가기반 APT 그룹 '오퍼레이션 스타 크루저(Operation Star Cruiser)' 수행 … 사이버 첩보활동 지속

By 알약(Alyac)

Published: 2018-04-25 · Archived: 2026-04-05 16:57:50 UTC

■ 한국 맞춤형 표적공격 '작전명 스타 크루저(Operation Star Cruiser)' 배경

이스트시큐리티(ESTsecurity)의 CTI 전문 조직인 시큐리티대응센터(이하 ESRC)는 정부 차원의 후원을 받는 것으로 추정되는 공격자(State-sponsored Actor)가 수행한 최신 지능형지속위협(APT) 캠페인을 발견했습니다.

이 캠페인은 현재 한국 대상의 고도화된 위협 중 가장 왕성하게 활동하고 있으며, ESRC에서는 이들이 '금성121(Geumseong121) 위협그룹'과 직·간접적으로 연계된 APT 조직인 라자루스(Lazarus) 그룹으로 판단하고 있습니다.

이른바 **'작전명 스타 크루저(Operation Star Cruiser)'**로 명명된 이번 캠페인은 HWP 문서파일 취약점을 사용했는데, 지난 2018년 02월부터 03월까지 핵심적으로 수행된 **'작전명 배틀 크루저(Operation Battle Cruiser)'**를 우선 참조해 주시기 바랍니다.

이 두개의 유사 오퍼레이션은 하나의 연장선에서 약 2주간의 일정 간격을 두고 진행되었고, 마치 쌍둥이처럼 TTPs(Tactics/Tools, Techniques and Procedures)의 유사성이 강력히 연결됩니다.

또, 공격에 활용된 Implants, Attribution, Infrastructure 등도 같은 패턴과 흐름을 유지하고, 최종 Payload 역시 유사 명령제어(C2) 프로토콜을 가지고 있습니다.

4월 현재 한국을 겨냥한 '오퍼레이션 스타 크루저'의 공격자는 이전 위협과 거의 유사한 체계를 그대로 활용했습니다. ESRC에서 이 캠페인들을 면밀히 조사한 결과 2014년 11월 24일 수행된 미국 소니픽쳐스 공격의 침해 지표와도 유사한 부분이 존재함을 관찰할 수 있었습니다.

특히, 흥미로운 점은 지난 2월 해외에서 DOC 문서 형태의 CVE-2018-4878 취약점을 결합해 마치 암호화폐 내용으로 위장된 공격이 처음 식별된 후, 연이어 3월과 4월에는 HWP 문서 취약점을 이용해 한국으로 표적지가 변경된 점입니다.

■ 문서파일 취약점을 활용한 스피어 피싱 위협은 현재 진행형

해당 위협그룹은 대표적으로 크게 3가지의 사이버 전술 무기 체계를 사용합니다. ① Supply Chain Attack ② Spear Phishing Attack ③ Watering Hole Attack 등이며, 침투 기반기술로 각종 시스템 및 응용프로그램 Zero-Day Exploit 등을 활용합니다.

이번 공격의 위협 벡터(공격자가 침해대상에 사용한 접근수단)는 스피어 피싱이며, 한국 로컬 환경에 최적화된 HWP 취약점이 사용 되었습니다.

실제 공격에 사용된 HWP 문서 파일의 스트림 속성을 살펴보면 정상 문서 포맷에 악성 스크립트가 삽입된 형태를 가집니다.

[그림 1] 공격에 사용된 HWP 취약점 파일의 내부 구조 및 날짜

4월 달 '오퍼레이션 스타 크루저' 공격에 사용된 문서 스트림의 생성날짜와 시간은 2018-04-10 03:19:51 (UTC)로 지정된 것을 볼 수 있으며, 한국 표준 시간(KST)으로 변환 시 2018년 04월 10일 오후 12시 19분 경에 제작된 것을 알 수 있습니다.

참고로 3월 달 '오퍼레이션 배틀 크루저' 공격에 사용된 HWP 문서는 2018-03-26 10:43:21 (UTC) 작성되었습니다.

상기 악성 문서 파일이 실행되면 다음과 같이 한국의 특정 암호화폐 거래와 관련된 회사의 거래처 원장 내용이 보여집니다.

[그림 2] HWP 취약점 문서 실행 시 보여지는 화면 (일부 모자이크 처리)

실제 공격에 사용된 문서 파일의 메타 데이터 기반 분석을 수행해 보면, 작성자와 마지막 수정한 사람의 아이디는 모두 'TATIANA' 값으로 일치합니다.

더불어 시계열 기반으로 살펴보면, 04월 10일 오후 12시 00분 경 최초 작성부터 12시 18분 경 마지막 수정까지 문서 제작에 대략 19분 정도가 소요된 것을 확인할 수 있습니다.

[그림 3] 공격에 활용된 문서 파일의 메타 데이터

문서 내부을 보다 자세히 살펴보면 'BinData' 스트림 영역에 'BIN0001.PS' 이름의 Post Script 코드가 삽입되어 있는 것을 알 수 있으며, Zlib 압축 포맷을 해제하면 내부에 Shellcode 영역이 XOR 명령으로 인코딩 된 것을 확인할 수 있습니다.

[그림 4] HWP 구조 중 'BIN0001.PS' 스크립트의 압축 해제 화면

인코딩되어 있는 Shellcode 영역을 복호화하면 다음과 같이 특정 명령제어(C2) 서버로 통신을 시도하는 것을 확인할 수 있습니다.

그리고 다운로드 시도되는 최종 파일명이 **'star3.avi', 'star6.avi'** 이름을 쓰고 있는 것을 알 수 있습니다.

[그림 5] 특정 호스트의 명령제어(C2) 서버로 통신하는 코드 화면

추가로 설치되는 각각의 파일은 마치 동영상 파일(.avi)처럼 위장하고 있지만 실제로는 모두 실행 파일(.dll)이며, 감염 대상 시스템의 프로세서 조건에 따라 32비트와 64비트가 구분되어 선택됩니다.

'star3.avi' 바이너리 파일이 제작된 시점은 한국 표준(KST) 시간 기준으로 2018-04-02 11:06:45 입니다.

[그림 6] 'star3.avi' 악성파일의 PE 포맷 구조 화면

■ 각 오퍼레이션의 유사도 및 연관성 분석

3월 달 제작된 '오퍼레이션 배틀 크루저'의 다운로드 파일은 'battle32.avi', 'battle64.avi' 이름이 사용되었고, 4월 현재 제작된 '오퍼레이션 스타 크루저'의 다운로드 파일명은 'star3.avi', 'star6.avi' 형태로 변경된 특징이 있습니다.

※ 파일명 : 배틀(battle+**플랫폼) → 스타(**star+**플랫폼)**

- battle32.avi **(Operation Battlecruiser)** → star3.avi **(Operation Starcruiser)**

- battle64.avi **(Operation Battlecruiser)** → star6.avi **(Operation Starcruiser)**

최종 설치된 악성 DLL 파일은 다음과 같은 3개의 호스트 사이트로 감염된 시스템 정보를 유출시도하게 됩니다.

※ 오퍼레이션 배틀크루저 (Operation Battlecruiser) C&C

- hypnosmd.com/include/top.php (64.90.49.224 / US)

- 0756rz.com/include/left.php (104.222.239.110 / US)

- 51xz8.com/include/top.php (104.222.230.87 / US)

※ 오퍼레이션 스타크루저 (Operation Starcruiser) C&C

- 10vs.net/include/left.php (104.224.219.109 / US)

- 168va.com/include/data/left.php (104.222.238.198 / US)

- 1996hengyou.com/include/dialog/left.php (160.124.191.80 / ZA)

두개의 오퍼레이션에서 사용한 정보유출 호스트 구조를 비교하면 'include/left.php' 경로를 일부 공통적으로 사용한 것을 알 수 있고, 도메인의 IP주소 대역도 유사한 점을 찾을 수 있습니다.

그리고 명령제어(C2) 서버에 이용된 일부 호스트는 중국어 기반의 웹 서버로 구축된 공통점이 있어, 공격자가 사용하는 취약점이 관련되어 있을 것으로 추정됩니다.

[그림 7] 중국어 기반으로 구축되어 있는 일부 명령제어(C2) 서버 화면

더불어 'battle32.avi' 코드와 'star3.avi' 내부 코드 구조를 비교해 보면 일부 동일한 함수의 번지까지 일치하는 것을 알 수 있습니다.

[그림 8] 'star3.avi' 파일 코드(좌측)와 'battle32.avi' 파일 코드(우측)의 함수 비교 화면

명령제어(C2) 통신에 사용하는 일부 코드의 경우도 '*dJU!*JE&!M@UNQ@' 코드가 동일하게 사용됨을 확인하였습니다.

[그림 9] 'star3.avi' 파일 코드(좌측)와 'battle32.avi' 파일 코드(우측)의 통신 패킷 코드 화면

더불어 'star3.avi', 'battle32.avi' 악성코드의 함수 흐름을 비교해 보면 거의 동일한 패턴과 흐름으로 구성된 것을 확인할 수 있습니다.

[그림 10] 'star3.avi' 파일 코드(좌측)와 'battle32.avi' 파일 코드(우측)의 함수 실행 비교

명령제어(C2)서버로 정보를 유출할 때 사용하는 컨텐츠 폼 데이터 부분의 User ID 코드도 100% 일치하는 것을 확인할 수 있습니다.

[그림 11] 'star3.avi' 파일 코드(좌측)와 'battle32.avi' 파일 코드(우측)의 통신 데이터 비교 화면

감염 신호를 C2 서버로 보낼 때, 배틀크루저 시점에는 ko-KR(한국어) 언어가 사용되었고, 스타크루저 공격에서는 en-US(영어) 언어가 사용되었습니다.

[그림 12] 감염 악성코드가 명령제어(C2) 서버와 통신하는 신호 패킷

■ '오퍼레이션 스타크루저' 위협 분석 결론

ESRC는 인텔리전스 위협 분석을 통해 최근 발생한 '오퍼레이션 스타 크루저' 공격 그룹이 현재까지도 한국의 암호화폐 분야에 속해 있는 주요 인사들을 대상으로 꾸준히 공격 시도하고 있는 정황을 확인했습니다.

이번 조사를 통해 공격자들은 새로운 명령제어(C2) 서버를 은밀하고 지속적으로 구축하고 있으며, 추가적인 공격에 많은 시간과 노력을 기울이고 있다는 것도 파악하였습니다.

또한, 2014년 미국 소니픽쳐스 대상 공격그룹의 활동이 현재 매우 활발하고, 정치적인 성향의 공격과 함께 금전적인 수익을 위한 이른바 외화벌이 작전에도 적극적임을 알 수 있습니다.

분석된 내용 중 일부 생략된 부분도 있지만, 국가기반의 후원을 받는 위협그룹은 다양한 분야에 걸쳐 공격을 수행하고 있다는 점을 명심해야 합니다.

이스트시큐리티 시큐리티대응센터는 이와 유사한 공격에 대한 피해를 최소화하고, 보다 체계적인 위협 인텔리전스 연구와 보안 모니터링을 강화하고 있습니다.