APT 공격 대응 전략 : Purple-Team 향상을 위한 Caldera, Sliver, Havoc, OpenCTI 기반 Red-Team 공격 시나리오 고도화에 대한 실험적 연구

박현기[1], 곽진[2]
[1]아주대학교 사이버보안학과 학부생
[2]아주대학교 사이버보안학과 교수
gusrl02@ajou.ac.kr, security@ajou.ac.kr

APT Attack Response Strategy : Experimental Study on Red-Team Attack Scenario Enhancement Using Caldera, Sliver, Havoc, and OpenCTI for Purple-Team Improvement.

Hyeon-Gi Park[1], Jin Kwak[2]
[1]Dept. of Cyber Security, Ajou University
[2]Dept. of Cyber Security, Ajou University
gusrl02@ajou.ac.kr, security@ajou.ac.kr

요 약

최근 사이버보안위협으로 인한 피해사례가 늘어나고 있다. 여러 보안 위협들이 존재하는데, 그 중 최신 보안 위협으로 APT 공격이 이슈가 되고 있다. 이는 정찰, 침입, 거점 확보, 권한 상승, 지속 유지, 데이터 유출 등을 통해 침투 후 지속적으로 대상의 정보를 정밀하게 빼내는 공격 방식이다. 이에 대한 방안으로 Red-Team 과 Blue-Team 의 협력을 통한 Purple-Team 이 제안한다. Red-Team 으로서 고도화된 공격 시나리오를 제안한다면, Blue-Team 에서도 이에 맞는 방어전략을 개선할 것이며, 결론적으로 보다 더 나은 Purple-Team 을 이끌어낼 수 있을 것이다. 본 연구에서는 Red-Team 으로서 고도화된 공격 시나리오를 도출하는 것이 목표이다.

키워드: APT(Advanced Persistent Threat), Purple-Team, Metasploit, Sliver, Caldera, Havoc, OpenCTI

Ⅰ. 서론

최근 사이버보안위협으로 인한 피해사례가 늘어나고 있다. 여러 보안 위협들이 존재하는데, 그 중 최신 보안 위협으로 APT 공격이 이슈가 되고 있다. 이는 정찰, 침입, 거점 확보, 권한 상승, 지속 유지, 데이터 유출 등의 순환적 구조를 통해 침투 후 지속적으로 대상의 정보를 빼내는 공격 방식이다.

실제 국내 사례로 2025 년 4 월 19 일, 국내 유명 통신 기업 S 사의 USIM 서버가 악성코드 감염으로 인해, 고객의 개인정보 유출이 된 사례가 있다. 감염된 악성코드는 중국계 APT 조직에서 높은 빈도로 사용하고 있는 공격 기법인 BPFdoor[1]인 것으로 밝혀졌다. 사이버 보안 업체이자 사고 대응 기관인 '시그니아'의 정보에 따라 중국의 APT 조직인 'Weaver Ant'의 공격 수법과 유사하다고 분석하고 있다. 앞으로 더 발생할 수 있는 APT 공격 대응해야 할 것이다.

이처럼 APT 공격에 대응해야 하는 차선책에 대한 필요성이 생겼다. 본 연구는 이에 대한 방안으로 Purple-Team 을 제안한다. Purple-Team 이란, 공격자인 Red-Team 과 방어자인 Blue-Team 의 협력을 통해, 공격 시나리오를 실시간으로 재현하고, 그에 따라 방어 전략을 함께 개선해 나가는 조직이다. 본 연구의 목적은 보다 더 나은 Purple-Team 을 이끌어내기 위해 Red-Team 으로서 고도화된 공격 시나리오를 도출하는 것이다. 이를 위해 MITRE ATT&CK FRAMEWORK 의 Caldera, Sliver, Havoc, OpenCTI 를 활용할 것이다.

Ⅱ. MITRE ATT&CK FRAMEWORK 및 OpenCTI, Sliver, Caldera 등 주요 도구의 역할

MITRE ATT&CK FRAMEWORK 는 사용자에게 실제 공격자의 TTP[2]를 구조화하여 제공하는 프레임워크다. 이를 통해 Red-Team 은 실제 공격자의 활동을 기반으로 정

[1] BPFdoor : Linux Kernel 의 Berkeley Packet Filter(BPF)를 활용하여 네트워킹 트래픽을 가로채고, 리버스 셸을 획득하여 원격 명령을 통해 시스템에 접근할 수 있는 스텔스형 백도어 악성코드.

[2] TTP : 공격자의 공격전술(Tactics), 공격기술(Techniques), 공격절

교한 공격 시나리오를 설계하고 시뮬레이션할 수 있다.

Caldera 는 MITRE ATT&CK 에 기반한 자동화 공격 시뮬레이션 도구이다. 사용자가 정의한 공격 시나리오를 자동으로 실행하며, 다양한 플러그인을 통해 정찰부터 권한 상승까지의 공격 체인을 재현할 수 있다.

Sliver 는 경량화된 C2(Command and Control) 프레임워크로, 원격 명령 실행, 파일 업로드, 쉘 획득 등 다양한 공격 기능을 제공한다. Caldera 와 Sliver 를 연동하면 초기 침투부터 Agent 설치까지 자동화된 공격을 수행할 수 있다.

Metasploit 은 대표적인 침투 테스트 프레임워크로, 취약점 스캐닝, 악성 페이로드 생성, 원격 코드 실행 등의 기능을 제공한다. Caldera 와 연동 시 실시간 취약점 기반 공격 시나리오를 동적으로 구성할 수 있다.

Havoc 은 난독화된 페이로드 생성과 탐지 회피 기법에 특화된 APT 시뮬레이션 도구이다. Caldera 와 결합하면 보안 탐지 시스템을 우회하는 고도화된 시나리오 설계가 가능해진다.

OpenCTI 는 위협 인텔리전스 통합 관리 플랫폼으로, 공격자의 행동 데이터를 시각화하고 분석하여 Purple Team 의 실시간 대응 역량을 강화시켜준다. 다양한 위협 정보를 기반으로 Red-Team 의 공격 시나리오를 보완하고, Blue-Team 이 방어 전략을 최적화할 수 있게 한다.

이처럼 각 도구는 Red-Team 공격 시나리오 고도화에 필수적인 역할을 하며, Caldera 를 중심으로 연동 시 시너지 효과를 발휘한다. 특히 Sliver 는 초기 침투와 Agent 설치에, Metasploit 은 취약점 기반 페이로드 주입에, Havoc 은 탐지 우회에, OpenCTI 는 인텔리전스 기반 분석에 활용된다. 이러한 도구들의 유기적 결합은 Purple-Team 의 협업 기반 대응 전략을 실질적으로 강화할 수 있는 핵심 기제가 된다.

III. 공격 시나리오 개발 및 고도화

본 연구에서는 Caldera 를 중심으로 Sliver, Metasploit, Havoc, OpenCTI 등 다양한 Red-Team 도구들을 연동하여 APT 기반 공격 시나리오를 고도화하였다. 각 도구는 공격 체인의 특정 단계에서 상호 보완적으로 사용되며, 이들의 통합을 통해 실제 환경을 모사한 정밀한 공격 시뮬레이션이 가능해진다.

공격 시나리오는 초기 침투, 공격 자동화, 탐지 회피, 위협 분석의 4 단계로 구성된다. 첫 번째 단계에서는 Sliver 를 활용하여 피싱 기반 리버스 셸을 획득하고, 타겟 시스템에 Caldera Agent 를 설치함으로써 초기 거점을 확보한다. 두 번째 단계에서는 Caldera 내에서 미리 정의된 공격 체인을 기반으로 공격을 자동화하고, 다양한 공격 모듈을 통해 정찰, 권한 상승, 지속성 확보 등을 수행한다. 세 번째 단계에서는 Havoc 을 이용하여 페이로드와 명령 흐름을 난독화 함으로써 보안 솔루션의 탐지를 우회한다. 이는 공격의 은밀성과 효과성을 높이는 데 중요한 요소로 작용한다. 네 번째 단계에서는 OpenCTI 와 연동하여 공격 로그와 행위 데이터를 위협 인텔리전스 관점에서 분석하고, 공격의 성공 여부와 보안 체계의 대응 현황을 평가한다. 또한, Metasploit 을 통해 탐지되지 않은 취약점을 실시간으로 분석하여 Caldera 시나리오에 반영함으로써 공격의 유연성을 확보할 수 있다.

이러한 도구 간의 유기적인 연계는 각 도구의 기능적 한계를 보완하면서도 실시간 반응형 공격 시나리오 설계를 가능하게 한다.

IV. 결론

본 연구는 APT 공격에 효과적으로 대응하기 위한 전략으로 Purple-Team 을 제안하고, 이를 기반으로 Red-Team 의 역할을 고도화하는 방안을 실험적으로 제시하였다. 특히, Caldera, Metasploit, Sliver, Havoc, OpenCTI 등의 도구를 통합하여 실제 APT 공격 흐름을 모사하고, 이를 통해 실시간 대응 및 방어 전략 개선이 가능한 프레임워크를 구성하였다.

각 도구의 특성을 살려 정찰, 침투, 권한 상승, 탐지 우회 등 전 과정을 자동화하고, OpenCTI 를 통해 위협 인텔리전스를 기반으로 분석함으로써 공격의 효과성과 방어 전략의 취약점을 동시에 진단할 수 있었다. 이와 같은 접근은 단순한 도구 활용을 넘어서, Red-Team 과 Blue-Team 간의 실질적인 협업을 가능케 하여 Purple-Team 역량 강화에 기여한다.

향후 연구에서는 실제 운영 체제를 기반으로 한 실습을 통해 시나리오를 더욱 정교화하고, 다양한 환경에서의 대응 방안을 검증할 예정이다. 특히, Linux 를 시작으로 Windows 등 타 운영체제에서도 본 시나리오를 적용함으로써 범용적인 대응 전략을 수립하고자 한다. 본 연구는 APT 공격 대응을 위한 실질적이고 반복 가능한 테스트 기반을 제공함으로써, Purple-Team 체계의 내실화에 기여할 수 있을 것으로 기대된다.

참고문헌

[1] MITRE. "MITRE ATT&CK Framework". https://attack.mitre.org/
[2] Bishop Fox. "Sliver: Adversary Emulation Framework". https://github.com/BishopFox/sliver
[3] Rapid7. "Metasploit: The penetration testing software". https://www.metasploit.com/
[4] C5pider. "Havoc: The Havoc Framework". https://github.com/HavocFramework/Havoc
[5] OpenCTI. "Open Cyber Threat Intelligence Platform". https://www.opencti.io/