Rippersec

그룹 동향

분석

Name : 조민혁

Class Number : 5

Phone Number : 010-4923-2198

목 차

1. 서론

1-1. 보고서 목적 및 작성 배경

그림 1. RipperSec Logo

최근 국제 사이버 공간에서 정치적·이념적 동기를 기반으로 하는 해킹 조직의 활동이 활발히 이루어지고 있다. 특히, RipperSec 은 단기간 내에 전 세계적으로 다수의 공격을 수행하며 주목받고 있는 핵티비스트 그룹으로 알려져있다. 2024 년 이후 해당 그룹이 한국의 공공기관 및 민간 웹사이트를 대상으로 공격을 수행한 정황이 확인되면서 국내 보안 환경에 대한 우려가 커지고 있다.

이에 따라 본 보고서는 RipperSec 그룹에 대해 알아보고, 해당 그룹의 활동 전반을 정밀하게 분석한다. 또한 공격 기법 및 영향을 분석함으로써 RipperSec 그룹의 위험도를 파악하고, 해당 그룹에 대한 대응 전략을 수립하는 데 목적이 있다

1-2. 보고서 구성 안내

본 보고서는 총 3 장으로 구성되어 있으며, RipperSec 의 조직적 성격 및 사이버 위협 양상을 종합적으로 분석하고 그에 따른 대응전략을 제시하는 것을 목적으로 한다.

제 2 장 본론에서는 다음의 네 가지 측면을 중심으로 RipperSec 에 대한 심층 분석을 진행한다.
먼저, '조직 개요 및 성격' 항목에서는 해당 그룹의 탄생 배경과 설립 시기, 정치·이념적 성향, 운영 구조 및 관련 연계 조직, 활동 채널(예: 텔레그램 등)을 통해 조직의 역사와 특성을 상세히 규명한다. 다음으로 '공격 방식'에서는 RipperSec 이 활용하는 주요 공격 기법, 사용 도구 및 프레임워크를 분석한다. 세 번째 항목인 '주요 사건 타임라인'에서는 글로벌 및 국내 피해 사례를 시기별로 정리함으로써 RipperSec 의 공격 양상 및 타깃 전략을 실증적으로 파악할 수 있도록 하였다. 또한 '영향 분석'을 통해 해당 그룹의 공격이 야기한 실제적 피해와 그 사회·기술적 파급력을 평가하며 단순한 사건 나열을 넘어 조직적 리스크에 대한 종합적 인식 기반을 제공한다.

제 3 장 결론에서는 보고서 내용을 간략히 요약하고, 기술적, 조직적, 전략적 측면에서의 실행 가능한 대응방안을 제시함으로써 보고서를 마무리한다.

2. 본론

2-1. 조직 개요 및 성격

2-1-1. 조직 탄생 배경 및 설립 시기

RipperSec 은 2023 년 6 월경 중동 지역의 지정학적 갈등과 이에 대한 국제적 여론 분열이 심화되던 시점에 등장한 해킹 조직이다. 명확한 정치적·이념적 정체성을 바탕으로 활동을 전개해온 핵티비스트 그룹이다. 조직의 결성 시점은 이스라엘-팔레스타인 간 갈등이 새로운 국면으로 확산되던 시기와 겹친다. 해당 그룹은 친팔레스타인 그룹으로써 팔레스타인 지지를 명시적으로 표방하며 사이버 공간을 '디지털 저항의 장'으로 활용하겠다는 메시지를 공개적으로 선포했다.

공식적인 첫 사이버 공격 성명은 2023 년 6 월 19 일경 텔레그램 채널을 통해 발표된 것으로 확인되며 이후 해당 그룹은 미국, 이스라엘, 인도 등 지정학적 분쟁에서 팔레스타인과 대립하거나 반대 입장을 취한 국가의 주요 기관 및 기업을 대상으로 다수의 사이버 공격을 전개하였다. 주요 공격 대상은 정부기관, 언론사, 금융기관 등으로 기술적 마비를 유도함과 동시에 정치적 상징성을 극대화하는 양상을 보였다.

특히 2024 년 하반기 이후에는 한국 내 공공기관 및 민간 웹사이트에 대한 DDoS 공격 정황과 데이터 유출 시도가 보고되며 RipperSec 의 활동 범위가 아시아권으로 확장되고 있음이 관측된다. 이는 단순히 특정 국가에 대한 일회성 보복 차원을 넘어 국제적 연대와 이념 기반의 광역적 사이버 작전 체계로 진화하고 있음을 시사한다.

2-1-2. 이념적 성향 및 정치적 목적

RipperSec 은 명확한 정치적·이념적 기반 위에서 활동하는 대표적인 핵티비스트 그룹이다. 이 그룹은 사이버 공간을 단순한 공격 수단이 아닌 정치적 메시지를 전달하고 이념적 투쟁을 전재하는 전장으로 인식한다.

해당 조직의 중심 이념은 친팔레스타인 정체성에 뿌리를 두고 있으며 이는 단순한 지역 갈등 지지 수준을 넘어서 반이스라엘·반서구·반제국주의 성향으로 확장된다. 특히 RipperSec 은 자신들의 사이버 공격을 팔레스타인의 민간인 피해와 국제 사회의 불균형적 시선에 대한 디지털 보복으로 규정하며 이스라엘과 그 우방국을 지지하는 국가나 기업을 주요 타깃으로 설정해왔다.

이들의 공식 성명과 공격 대상 선택 패턴은 이념적 의도성과 정치적 선전 효과를 극대화하는 방향으로 설계되어 있다. 예들 들어, 유엔 결의안과 상충되는 정책을 시행하거나 이스라엘에 대한

군사·경제적 지원을 공표한 국가의 정부 기관 및 언론사 웹사이트를 공격 대상으로 삼는 방식이다. 이러한 경향은 2023 년 하반기 미국, 인도, 프랑스 등에서 발생한 공격 사례에서 두드러지며 단순히 기술적 피해를 주는 것을 넘어 공공 인식에 영향을 주는 전략적 심리전 요소로 작용하고 있다.

더불어 RipperSec 은 종교적 극단주의와는 일정한 거리를 두며 국제 핵티비즘 연대 형성을 통한 정치적 정당성 확보를 주요 전략으로 삼고 있다. 이는 러시아의 NoName057, 이란의 CyberFattah 등과의 협업에서도 드러나며 국제적 협공을 통해 '사이버 민병대'로서의 지위를 자처하고 있음을 알 수 있다. 특히 2024 년 이후 공격 메시지에는 '자유', '인권', '억압된 목소리' 등의 표현이 빈번히 등장하고 있으며 이는 자신들의 활동을 '민간인의 대변자'이자 '디지털 정의 실현자'로 위치하려는 시도로 해석된다.

결과적으로 RipperSec 의 정치적 목적은 단순히 특정 국가에 대한 항의 차원을 넘어서 국제 질서와 권련 불균형에 대한 반감 그리고 사이버 공간에서의 이념 투쟁과 여론전 수행이라는 장기적 전략을 목표를 하고 있다. 이러한 성향은 향후 사이버 안보 환경에서 전통적 위협 분석만으로는 포착하기 어려운 비대칭적 위협 요소로 작용할 가능성이 크다

2-1-3. 운영 구조 및 주요 연계 그룹

RipperSec 은 전통적인 계층형 조직 구조를 따르지 않는 분산형·탈중앙화 운영 구조를 기반으로 활동하는 대표적인 핵티비스트 집단이다. 특정한 중앙지휘체계 또는 고정된 리더십이 존재하기보다는 온라인 커뮤니티 기반의 느슨한 네트워크 구조 속에서 핵심 운영진과 다수의 자발적 참여자들이 비공식적으로 연결되어 있다.

핵심 운영진은 대체로 익명성을 유지하며 활동하고 있으며 이들은 직접적인 공격 명령, 도구 배포, 대상 선정, 작전 명칭 부여 등의 기능을 수행한다. 대표적인 예로, RipperSec 이 개발한 DDoS 도구인 MegaMedusa 는 이러한 운영진에 의해 제작·배포되었고 사용자 친화적인 인터페이스와 공개 레포지토리를 통해 비기술 사용자들도 쉽게 공격에 참여할 수 있도록 설계되어 있다. 이처럼 핵심 운영진은 기술적 역량뿐만 아니라 커뮤니티 조직력과 전략적 메시지 관리 능력까지 갖춘 사이버 공간의 '작전 기획자' 역할을 수행한다.

참여자 그룹은 보통 자발적으로 채널에 가입하거나 작전에 동조하여 활동하는 일종의 '디지털 자원 봉사자'의 성격을 가진다. 이들은 운영진이 공유하는 공격 대상 정보 및 도구를 사용해 DDoS 공격 등에 참여하며 다수의 참여로 공격의 규모와 파괴력을 배가시킨다. 이러한 크라우드소싱 기반 공격 모델은 전통적인 APT 나 해커 그룹과 달리 낮은 비용으로도 고위험군 공격을 구현할 수 있는 특징을 가진다.

또한 RipperSec 은 단독 그룹으로서 작전만을 수행하는 것이 아니라 다양한 국가 기반 혹은 이념 연대 기반 해커 그룹들과 동맹 체계를 형성하여 활동의 확장성과 지속성을 확보하고 있다. 2024 년 9 월에는 국제 해킹 연합체 결성을 발표했으며 이는 러시아, 이란, 인도네시아 등 14 개국 이상 40 여개 해커 그룹이 참여한 것으로 파악된다.

주요 연계 그룹으로는 러시아의 NoName057, 이란의 CyberFattah, 인도네시아의 HacktivistSulawesi 등이 있다. 이와 같은 연계 구조를 통해 RipperSec 은 특정 지역을 넘어서 글로벌 사이버 영향력 확대를 실현하고 있으며 단일 그룹의 역량을 초월하는 연합 작전 체제를 구축하였다. 이로 인해 실시간 동시다발적 공격, 공동 도구 활용, 공동 메시지 배포 등의 형태가 가능해졌으며 이는 기존 사이버 방어 체계가 대응하기 어려운 비국가 행위자간 유동적 동맹 모델을 실현하고 있다는 점에서 높은 위험도를 지닌다.

결론적으로 RipperSec 의 운영 구조는 탈중앙화된 커뮤니티 기반이며 다국적 이념 연대를 통해 지속성과 범위 확장을 실현하고 있다. 이러한 구조는 전통적인 조직 기반 공격과 달리 빠르게 형성되고 빠르게 소멸하는 임시적, 유동적 연합 모델로 진화하고 있으며 방어 측면에서도 보다 민첩한 탐지·분석·공조 대응 체계 구축이 요구된다.

2-1-4. 활동 범위 및 온라인 채널

RipperSec 의 활동 범위는 단순히 지역적 한계를 초월한 글로벌 사이버 작전 영역을 지향하며 이들의 타깃은 지저학적 이해관계, 종교·이념적 가치, 외교적 입장에 따라 전략적으로 선정된다. 2023 년 설립 초기에는 이스라엘 및 중동권 국가에 대해 중심 공격을 수행했다. 이스라엘 정부기관, 언론사, 군사 관련 웹사이트를 집중 타격하였고 #OpIsrael, #OpsZionism 등 해시태그 기반 이념 작전 전개를 하였다. 이후 2024 년 친이스라엘 국가 및 서방 동맹국으로 확대하여 미국, 영국, 프랑스, 독일, 인도 등의 정부·공공기관을 공격하였고 해당 시기에 팔레스타인 지지 성향을 이유로 러시아, 이란 기반 그룹과 연계를 강화하였다. 2025 년 현재는 아시아·오세아니아 지역으로 확장하여 한국, 일본, 호주 등 외교적·군사적 친서방 행보를 보이는 국가를 대상으로 공격을 수행해 한국 내 공공기관, 전력 기술사, NGO 등을 대상으로 공격이 수행되었다. 이와 같이 RipperSec 은 단순히 기술적 취약점을 노리는 것이 아니라 정치·외교적 맥락을 기반으로 '의도된 타깃 선정'을 수행한다는 점에서 전통적 사이버 범죄 그룹과 뚜렷이 구별된다.

RipperSec 의 활동은 전통적 웹이 아닌 비중앙화된 정보 확산 채널과 소셜 미디어 기반의 작전 플랫폼을 통해 수행된다. 이를 통해 은닉성과 파급력을 동시에 확보하며 자체적인 사이버 커뮤니티를 유지·확장해나가고 있다. 아래는 RipperSec 이 활동하는 온라인 채널의 종류와 링크이다.

표 1. RipperSec의 온라인 채널 종류 및 링크

Index	종류	링크	설명
1	Telegram	https://t.me/WeRipperSec	작전 본부 역할
2	Twitter	@RipperSec	대외 선전 수단
3	GitHub	https://github.com/TrashDono/MegaMedusa	자체 도구 배포

2-2. 공격 방식

2-2-1. 주요 공격 기법 개요

RipperSec 은 전통적인 사이버 범죄 조직과는 달리 금전적 이득보다는 정치적·이념적 메시지 전달과 여론전 수행을 핵심 목표로 하는 핵티비스트 그룹이다. 이에 따라 이들의 공격 기법은 특정 기술에만 국한되지 않으며 목표에 따라 혼합적·비정형적 방식의 공격 벡터를 유연하게 조합하여 수행한다. 기술적 정교함보다는 범용 도구의 대중적 활용과 참여자 기반의 대규모 실행을 통해 타격 효과를 극대화하는 것이 특징이다. 대표적인 공격 기법은 3 가지로 DDoS 공격, 웹사이트 변조, 데이터 유출 및 정보 공개로 나뉜다.

먼저 DDoS 공격은 대규모 애플리케이션 계층 기반의 DDoS 공격이다. 이들은 웹서버의 HTTP 요청 처리 능력을 마비시키기 위해 MegaMedusa, MiniMedusa 등의 자체 도구를 활용하여 동시다발적인 HTTP 요청을 생성한다. 단순한 패킷 플러딩 방식이 아닌 정교하게 구성된 헤더와 무작위 URL 패턴을 통해 정상적인 요청처럼 보이도록 위장하여 필터링을 우회한다. 특히 RRiperSec 의 DDoS 공격은 커뮤니티 구성원들의 동시 참여를 통해 수행되며 공격 대상과 타이밍이 텔레그램 채널을 통해 실시간으로 공지된다. 일부 캠페인에서는 수천 명에 달하는 참가자들이 동일 시간에 동격 도구를 실행함으로써 일반적인 방화벽이나 WAF 의 대응 능력을 초과하는 트래픽을 유발한다. 이러한 크라우드소싱 기반 DDoS 는 공격 규모를 기술적 능력보다 사회적 동원력에 기반하여 증폭시키는 전략으로 해석할 수 있다.

두 번째로는 웹사이트 변조이다. RipperSec 은 종종 정부 기관, 교육기관, 공공단체 등의 웹사이트를 해킹하여 홈페이지를 변조하는 행위를 수행한다. 이는 단순한 가용성 저해를 넘어 공격자가 정치적 메시지 또는 이미지를 노출함으로써 대외적인 정치 선전 효과를 극대화하는 방식이다. 이러한 변조 공격은 보통 취약한 웹의 취약점, 디폴트 인증 정보, SQL 인젝션 등 비교적 기초적인 웹 취약점을 이용해 서버 권한을 획득한 후 실행된다. 기술적으로는 고난도 APT 공격과 구별되나 사회적 파급력 측면에서는 그 이상의 충격을 유발할 수 있다는 점에서 고위험군으로 평가된다.

세 번째로는 데이터 유출 및 정보 공개이다. 최근 RipperSec 은 단순한 서비스 방해를 넘어 데이터 유출 및 정보 공개 행위로 활동 범위를 확장하고 있다. 이들은 공격을 통해 확보한 사용자 정보, 내부 문서, 자격 증명 파일 등을 익명 게시판이나 텔레그램 채널을 통해 '디지털 증거'라는 명목으로 유포하며 표적 대상의 사회적 신뢰도를 저하시키고자 한다. 주요 기법으로는 관리자 계정 탈취, FTP/WebShell 설치, 데이터베이스 SQL 인젝션을 통한 직접 추출 등이 활용되며 일부 공격에서는 제 3 자 유출된 정보를 수집·가공하여 마치 자력 침해로 위장해 배포하는 경우도 존재한다. 데이터 유출은 RipperSec 의 2 차적 타격 전략으로 자리잡고 있으며 피해 기관에 심각한 법적·신뢰적 피해를 유발할 수 있다.

마지막으로 캠페인 기반 복합 공격이다. RipperSec 의 작전은 종종 단일 기법에 의존하지 않고 DDoS+웹변조+정보 유출이 순차 또는 병렬로 이루어지는 복합공격 형태를 띤다. 예를 들어 DDoS 공격으로 주의를 분산시킨 후 백엔드 침투를 통해 정보 유출을 시도하거나 특정 국가의 주요 사이트를 DDoS 공격한 뒤 언론에 공격 성명을 발표하는 식의 심리적인 연계를 보인다.

이러한 다중 벡터 혼합형 공격 구조는 단일 방어 체계를 우회하고 공격 효과를 시간적으로 지속시키는 전략으로 볼 수 있으며 이는 RipperSec 이 단순한 스크립트 키디 레벨이 아닌 작전 개념이 내재된 사이버 심리전 수행 조직임을 보여준다.

2-2-2. 공격 도구 및 프레임워크

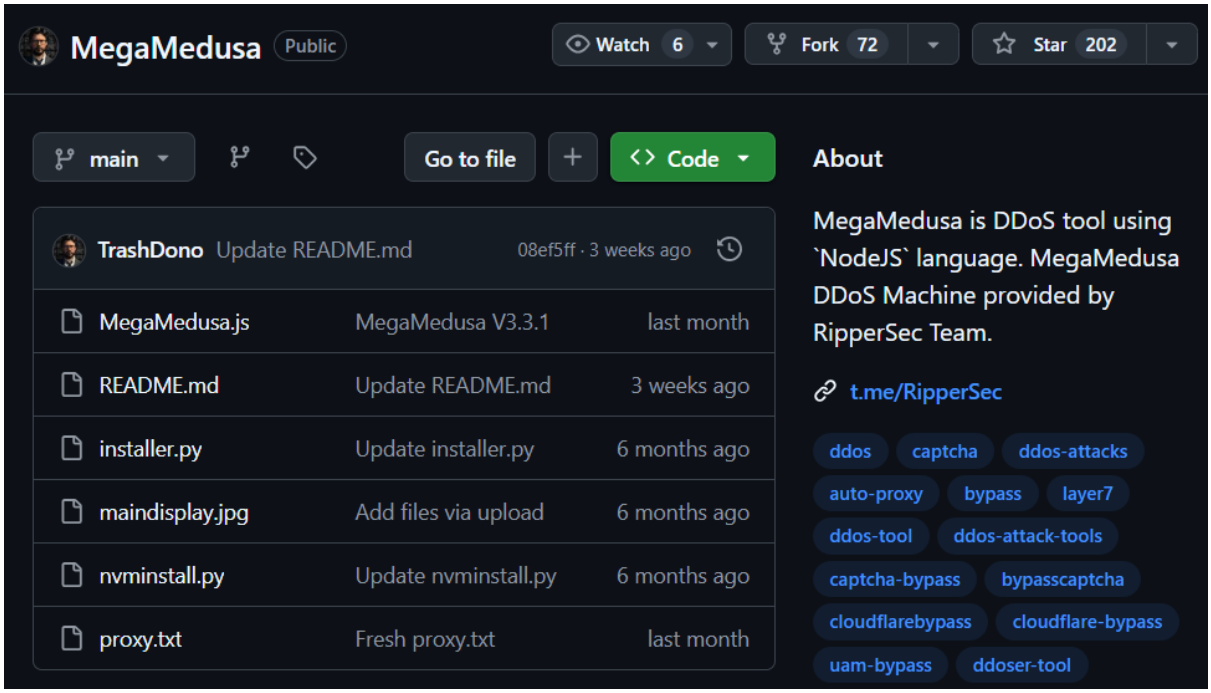

그림 2. MegaMedusa Code

RipperSec 은 금전적 목적보다 이념적 동기를 기반으로 한 해킹 활동을 수행하는 만큼 고도화된 APT 수준의 도구보다는 범용성, 접근성, 확장성이 높은 오픈소스 기반 도구 및 자체 제작 툴을 조합하여 사용한다. 이들의 공격 프레임워크는 '누구나 쉽게 사용할 수 있으며 동시에 대규모로 동원 가능한 구조'에 중점을 두고 설계되어 있으며, 특히 DDoS 공격을 위한 도구 생태계가 가장 발달되어 있다.

대표적으로는 MegaMedusa 오픈소스 도구가 존재한다. MegaMedusa 는 Rippersec 이 직접 제작·배포한 애플리케이션 레이어 기반 DDoS 공격 도구로 이 조직의 상징적 무기이자 핵심 프레임워크다. Node.js 기반 CLI 구조로 다중 스레드 요청 생성 엔진이 포함되어 있으며 대상 URL, 지속 시간, 동시 요청 수 등을 사용자 입력값으로 지정 가능하다. 기술적으로는 Header Randomization 을 통해 요청마다 HTTP 헤더를 동적으로 변경하여 정상 트래픽과의 구분을 어렵게 만들고, URL Path Mutation 을 통해 무작위 매개변수를 지속적으로 생성함으로써 서버 캐시를 우회한다. Method Rotation 을 통해 GET, POST, HEAD 등 다양한 HTTP 메소드를 무작위로 사용해 공격 트래픽의 일관성을 제거한다. 또한 Proxy 및 IP Spoofing 을 지원하여 공개 프록시를 통한 IP 분산 효과를 제공하고, Anti-CAPTCHA 회피 기능으로 일부 보안 시스템의 기본 차단 기제를 우회 가능하도록 설계되어있다. 해당 도구는 텔레그램을 통해 공격 대상과 설정값을 공유하여 참여자들이

MegaMedusa 를 병렬 실행해 수천 개의 병렬 연결이 한 번에 타겟 웹사이트로 접속해 짧은 시간에 서비스 마비를 유도한다.

RipperSec 은 자체적으로 만든 오픈 소스 도구 이외에도 여러 오픈 소스 도구를 활용한다. 대표적으로 SQLMap 을 활용해 취약한 웹사이트에 SQL 인젝션 공격을 수행하기도 하며 Nikto, Nmap 을 통해 웹 서버 및 네트워크 취약점 스캐닝을 수행한다. 또한 CVE Exploit Script 로 공개된 취약점을 이용해 침투 스크립트를 작성하며 WebShell 을 통해 웹 서버에 업로드된 후 지속적 원격 접근을 가능하게 한다. 마지막으로 Metasploit Framework 를 통해 초기 침투 후 추가 권한 획득 및 침투 테스트를 자동화한다.

이외에도 RipperSec 은 텔레그램 기반 커뮤니케이션 프레임워크를 통해 작전 코드명 부여, 공격 매뉴얼 게시, 전술 지도 배포, 성공 사례 실시간 공유를 수행한다. 이를 통해 사이버 작전 수준의 연계 체계를 갖추어 참여자들을 조직화할 수 있는 기반이 된다.

2-3. 주요 사건 타임라인

2-3-1. 글로벌 주요 공격 사례

2023 년 6 월 RipperSec 은 조직 창설 및 초기 활동을 수행했다.

2023 년 10 월 이스라일-하마스 전쟁 발발 이후 대규모 작전을 수행했다. 공격 대상은 이스라엘 정부 기관, 군 관련 웹사이트, 민간 포털이였으며 공격 유형은 L7 DDoS, 웹 변조, 정치 메시지 게시였다.

2024 년 1 월~8 월 범세계적으로 공격이 확대되어 미국, 인도, 영국, 프랑스, 태국 등이 공격을 받았다. MegaMedusa 기반 대규모 애플리케이션 계층 DDoS 공격을 수행하였다. 또한 텔레그램으로 동시 다발적 참여 유도를 하였다.

2024 년 11 월 #OpsAutralia 캠페인을 통해 호주 정부, 법률 시스템, 항공사, 교육기관 웹사이트 등 총 39 개의 서비스가 공격받았다.

2025 년 3 월 이스라엘 정부기관이 연속 공격을 받았다. 이스라엘 교육부, 역사정보포털이 공격 받아 실시간 사이트 마비, 정치적 메시지 삽입, 트래픽 초과에 의해 다운타임이 유발되었다.

2-3-2. 한국 대상 공격 사례

2024 년 8 월 한국 웹사이트 대상으로 최초 공격이 수행되었다. 한국의 5 개 웹사이트 해킹 및 DB 정보가 유출되었고 반이스라엘 외교 성향에 대한 경고성 해킹을 수행했다. 해당 공격은 국가 확장성 실험 성격이 있으며 동북아시아 첫 공격이었다.

2025 년 3 월 한국 내 공공기관 집중 공격으로 한국의 친이스라엘 외교 메시지에 대한 보복적 성격이 있다. 경기도지사 홈페이지, 경찰 웹사이트, NGO 사이트 등이 공격을 받았으며 KEPT 와 같은 전력 관련 기관이 피해받았고 유제품 홍보원 등 ICS/SCADA 시스템 해킹 주장 사례가 등장했따.

2-4. 영향 분석

RipperSec 의 사이버 공격은 단순한 시스템 마비를 넘어서 정치적, 사회적, 기술적, 전략적 수준에서 복합적인 영향을 유발한다. 특히 이들의 작전 방식은 대중의 심리적 반응을 자극하고 국가의 외교 노선과 사이버 안보 전략에 중장기적 영향을 미치며 그 파급 범위는 공격 대상국의 정책, 민간 인프라, 대중 여론에까지 이른다.

먼저 기술적·운영적으로는 RipperSec 이 사용하는 DDoS 공격과 웹 변조, 데이터 유출에서 표면적으로는 일시적 서비스 중단에 그치는 듯 보이지만 실제로는 여러 기술적 위협을 구조적으로 유발한다. RipperSec 의 반복적인 DDoS 공격은 웹사이트 접속 불능 및 네트워크 병목 현상을 초래하여 공공기관이나 기업 웹서비스에 대한 대국민 신뢰도 하락으로 이어진다. 또한 방화벽 및 보안장비 자원에 대해 고갈을 유발하여 WAF, IDS/IPS 장비의 처리량을 초과시키고 오탐률을 증가시킨다. 그리고 데이터 유출로 인해 2 차 피해가 유발된다. 유출된 정보에 대해 공격자가 다크웹이나 SNS 에 공개할 경우 피해자의 민감정보 노출, 2 차 스피어 피싱, 법적 책임 발생 등의 후속 피해가 수개월에서 수년간 이어질 수 있다.

3. 결론

3-1. 요약

본 보고서의 내용을 세 줄로 요약하면 다음과 같다.

- RipperSec 은 기존 범죄 조직과는 다르게 금전적 요구를 하지 않으며 정치적·이념적 핵티비스트 그룹이다.
- RipperSec 의 공격 기법은 주로 DDoS, 웹 사이트 변조, 정보 유출이 이들의 주요 공격이다.
- RipperSec 은 최근 아시아권에도 공격을 시작하였으며 주의할 필요가있다.

요약된 정보에 따라 마지막에 아시아권에도 공격을 시작하였음을 알 수 있다. 이에 따라 3-2 에는 대응 방안을 기술적 측면, 조직적 측면, 전략적 측면에 따라 알아보며 보고서를 마무리한다.

3-2. 대응 방안

3-2-1. 기술적 측면

RipperSec 이 주로 사용하는 MehaMedusa 는 HTTP 기반의 대규모 트래픽 요청을 통해 웹서버를 마비시키는 애플리케이션 레이어 공격에 특화되어 있다. 이에 대한 효과적 대응을 위해 다음의 조치가 필요하다. 먼저 WAF 정밀 튜닝을 통해 WAF 를 기본 적용하면서 MegaMedusa 의 공격 특성을 분석해 정규식 기반 규칙 또는 AI 기반 동적 탐지 룰을 적용해야한다. 또한 Bot Behavior 분석 기반 트래픽을 필터링하여 정상 사용자와 봇 기반 트래픽을 구분하기 위해 행위 분석 기반 시스템을 구축해야한다. 이를 통해 요청 간격, 세션 유지 시간, Cookie 변화 유무 등으로 트래픽 패턴 분류 및 이상치를 탐지해야한다. 추가적으로 Rate Limiting 및 IP Reputation 기반 필터링을 적용해 특정 IP 또는 세션에서 일정 요청 수를 초과하는 경우 차단을 하고 신뢰도가 낮은 프록시/봇넷 IP 에 대한 사전 차단 목록을 운영하도록한다.

웹 사이트 변조에 대비하기 위해 주기적으로 웹 애플리케이션 취약점 정기 진단 및 패치를 적용해 OWASP Top 10 기반의 취약점에 대해 정기 점검을 수행하도록한다. 또한 권한 기반 접근 제어를 강화하여 관리자 계정 접근시 다중 인증을 필수화하고 관리자 콘솔에 대해서는 사내 IP 또는 특정 VPN 으로 접속 제한하는 것이 바람직하다. 또한 비인가 외부 접근에 대해서는 탐지 로그 분석을 통해 침해사고에 대해 대응하도록한다.

마지막으로 데이터 유출에 대응하기 위해 웹 애플리케이션과 데이터베이스 서버를 분리하여 DB 서버에 대해서는 제한된 내부 IP 및 인증된 서비스 계정만 접근하도록 허용한다. 또한 전송구간 암호화를 통해 웹과 DB 간 통신은 반드시 암호화를 수행해 민감정보가 중간자 공격 및 세션 하이재킹에 대비하도록한다.

3-2-2. 조직적 측면

조직적 측면에서의 대응은 기술적 조치만으로는 방어가 불가능한 핵티비즘 기반 사이버 위협에 대응하기 위한 인적·제도적 기반을 강화하는 전략을 의미하며 이는 조직의 사이버 보안 성숙도 향상과 침해 대응 역량 내재화라는 두 축을 중심으로 체계화되어야 한다.

먼저 모든 임직원을 대상으로 한 사이버 보안 교육을 정례화하고 단순한 피싱 교육을 넘어 국가기반시설 위협, 핵티비즘, 사이버 심리전에 대한 이해를 포함한 고도화된 콘텐츠로 구성해야 하며, 특히 조직 내 보안 담당자와 운영자에 대해서는 모의 해킹, 디지털 포렌식, 보안 정책 설계 등의 전문 교육을 통해 위협 분석 및 대응 기술을 내재화시켜야 한다.

두 번째로는 조직 내 보안 거버넌스 체계를 재정비하고 최고정보보안책임자를 중심으로 IT 부서, 인사부서, 홍보부서, 법무팀 간 유기적 협조 체계를 갖춘 전사적 사이버 대응 태스크포스를 구성하여 비상시 신속한 의사결정과 대응이 가능하도록 해야 하며 이를 위해 위기 대응 매뉴얼, 보고 체계, 커뮤니케이션 채널을 정형화하여 정기적으로 모의훈련을 실시해야 한다. 또한 사이버 침해 사고 발생 시의 책임 분산 및 대응 시간 단축을 위해 사이버 공격 발생 단계별 Role &

Responsibility 을 명확히 정의하고 사후 보고 및 복구 절차 역시 ISO/IEC 27035, NIST 800-61 등 국제 침해대응 프레임워크에 기반해 표준화하여야 하며 보안 사고 대응이 단순한 IT 문제가 아닌 조직 전체의 위기관리에 해당한다는 인식을 조직 전반에 확산시킬 필요가 있다. 아울러 협력사 및 외부 위탁업체에 대한 사이버 보안 요구 수준을 명확히 하고, 공급망 보안 기준에 따라 보안서약, 정기 보안진단, 접근권한 관리 등을 체계화함으로써 제 3 자 리스크를 최소화해야 하며 특히 외부 홍보 또는 대외 커뮤니케이션 시에는 사이버 공격의 확산을 막고 불필요한 사회적 혼란을 방지하기 위해 사전 정의된 메시지 체계를 따르고 보안 TF 와 연계된 커뮤니케이션 전략을 수립해야 한다.

마지막으로 조직은 사이버 위협에 대한 대응을 단기적인 사건 중심 사고 처리로 인식해서는 안 되며 사이버 안보를 조직문화 차원에서 내재화하기 위해 지속적인 정책적 투자, 리더십의 관심, 인센티브 기반의 보안 행동 유도 전략 등을 종합적으로 실행하여야 한다.

3-2-3. 전략적 측면

RipperSec 과 같은 핵티비즘 기반 해커 집단의 등장은 기존의 기술 중심적 사이버 보안 대응의 한계를 드러내고 있으며 이에 따라 전략적 차원에서는 보다 포괄적이고 거시적인 관점의 대응체계가 요구된다.

우선, 국가 및 공공기관 차원에서는 사이버 위협을 군사, 외교, 정보 분야와 연계된 국가 안보 위협 요소로 인식하는 전환적 접근이 필요하다. 이를 위해 각 정부기관 및 핵심 기반시설 운영 주체는 보안 부서를 단순 운영기술 또는 정보기술 자산의 보호 역할에서 확장하여 사이버 정보전에 대응 가능한 전략기획 기능을 포함한 조직으로 재편해야 하며 특히 사이버 작전과 외교 정책 사이의 연계성을 고려한 국가적 사이버 대응 전략 프레임워크 구축이 필수적이다. 이 프레임워크는 사이버 위협의 이념적 성격, 국제 정치적 파장, 심리전 목적 등을 분석하여 적시 대응이 가능하도록 해야 하며 대응의 주체 역시 IT 인력에서 국방·외교·심리전 전문가까지 다분야로 확장되어야 한다.

둘째, 사이버 대응 정책은 국가 단위의 독립적 접근이 아닌 국제 연대 기반의 정보 공유 및 공동 대응 체계로 진화해야 한다. RipperSec 이 전개한 Holy League 등 해커 연합체가 다국적 공격 작전을 수행하는 상황에서, 각국의 CERT 간 실시간 위협 인텔리전스 공유와 침해사고 정보 연계는 필수적인 대응 자산이며 이를 위해 국가 간 MOU 체결, 사이버 위협 공동대응 훈련, 연합 분석 플랫폼 개발 등 실질적 연합 작전 수준의 협력이 강화되어야 한다.

셋째, 사이버 위협을 '디지털 심리전'의 영역으로 인식하고 이에 대응하는 사이버 인지전 체계의 수립도 전략적으로 중요하다. RipperSec 은 공격 이후 피해 사실을 SNS 나 다크웹에 의도적으로 유포함으로써 사회적 혼란과 불신을 조장하며 이는 물리적 피해보다 훨씬 장기적이고 깊은 영향력을 발휘할 수 있다. 따라서 정부 및 공공기관은 공격 사실이 확인되었을 경우 그 내용을 투명하게 공개하되 사전 정의된 커뮤니케이션 전략에 따라 공포 조장이나 허위 정보 확산을 방지하는 조치를 병행해야 하며 필요 시 민간 언론 및 플랫폼 기업과 연계한 허위 정보 모니터링 체계를 공동 운영해야 한다. 넷째, 정부 차원의 전략에는 장기적인 투자와 제도적 기반 강화가 수반되어야 하며 이는 단순한 장비 보강이 아니라 국가 사이버 방어 역량에 대한 지속가능한 연구개발 생태계 구축, 사이버 전문가 양성, 산업-학계-국가 간 기술이전 메커니즘 구축 등을 포함해야 한다. 이를 위해

사이버 위기관리 전담 기구 설립, 사이버 전쟁 대비 국가총력전 시나리오 개발, 핵심 인프라 보호법 제정 및 상시 개정 등이 병행되어야 한다.

마지막으로 비국가 해킹 주체에 의한 정치적 목적의 공격이 급증하고 있는 현 시점에서는 전통적인 사이버 보안 전략에서 벗어나 '국가 사이버 회복탄력성' 중심의 전략적 패러다임 전환이 필요하며 이는 위협 발생 이후의 복구와 적응, 정보 생태계 안정화를 고려한 중장기 정책 로드맵과 직접 연결되어야 한다.

4. Refereces

[1] S2W, Trends of Telegram DaaS (DDoS as a Service) groups: their hacktivist motivations, attack techniques (2023~2024)

[2] CheckPoint, Hacktivists Call for Release of Telegram Founder with #FreeDurov DDoS Campaign

[3] Cyjax, The Hacktivist Response to UK Foreign Policy

[4] 보안뉴스, 친팔레스타인 무슬림 해커조직 리퍼섹, 한국 사이트 4곳 해킹

[5] Falconfeed, DDoS Alert

[6] CyberKnow, RipperSec

[7] https://t.me/WeRipperSec