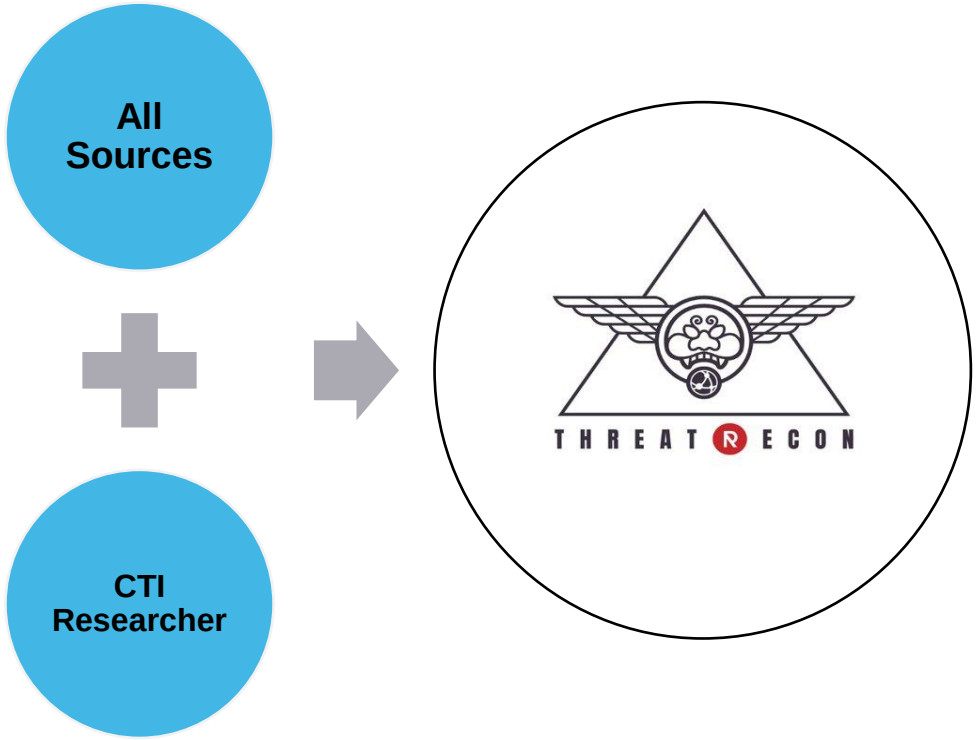
K-CTI 2022
2022 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

오픈 소스(Open Source) 기반 도구 및 프리웨어(Freeware)를 악용한 해킹 그룹들

장 영 준 수석
cyj@nshc.net
NSHC ThreatRecon Team

NSHC ThreatRecon Team

- NSHC ThreatRecon 팀은 사이버 위협 인텔리전스(Cyber Threat Intelligence) 서비스 담당
- **전 세계에서 활동하는 해킹 그룹들의 해킹 활동 관련 정보와 위협 데이터를 수집 및 분석**
- 현재 사이버 위협 인텔리전스 분석 업무로 한국과 싱가포르에서 팀을 운영 중
- **트위터(twitter.com/nshcthreatrecon)와 블로그(redalert.nshc.net/blog) 운영** 중



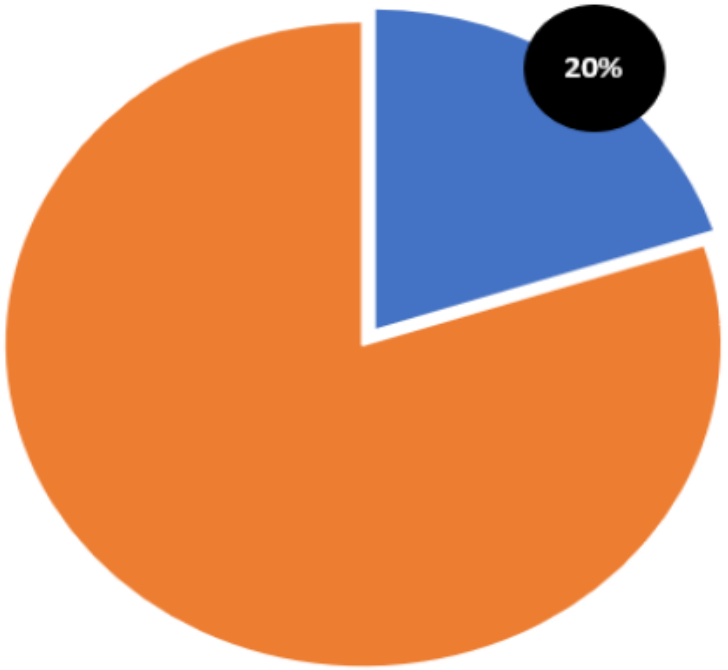
해킹 그룹 위협 데이터 현황

- **해킹 그룹들의 해킹 활동 관련 정보와 위협 데이터 확보**
  - 다양한 지역에서 발생하는 해킹 그룹들의 해킹 활동 분석
  - 해킹 그룹들의 활동 목적에 따라 정부 지원 그룹, 사이버 범죄 그룹과 미분류 그룹으로 분류
  - ThreatRecon Platform은 **총 17개 Sector의 179개 해킹 그룹** 관련 위협 데이터 제공 (2022년 2월 20일 기준)
  - 현재 **3,481건 이상의 위협 이벤트**와 **183,901건 이상의 위협 데이터 제공** (2022년 2월 20일 기준)

오픈 소스(Open Source)기반 도구 및 프리웨어(Freeware)를 악용한 해킹 그룹들

해킹 활동 관련 오픈 소스 기반 도구와 프리웨어

- 2021년 분석한 해킹 그룹 활동 관련 **전체 위협 이벤트 중 20% 악용 사례** 발견
- 2021년 발견한 해킹 그룹이 활용한 **오픈 소스 기반 도구와 프리웨어는 총 129개** 존재
- 해킹 그룹이 악용한 오픈 소스 기반 도구와 프리웨어는 대부분 **IT 인프라 관리 및 점검 용도**



[오픈 소스 기반 도구와 프리웨어를 악용한 2021년 사이버 공격 현황]

악용 빈도가 높은 오픈 소스 기반 도구 와 프리웨어 (1)

- **악용한 도구들 대부분이 깃허브(GitHub)에 소스 코드 공개 또는 별도 홈페이지에서 공개**

Cobalt Strike

- 상용 모의 해킹 도구, 구 버전이 깃허브에 공개

Mimikatz

- 계정 인증 정보 추출 도구, 깃허브에 소스코드 공개

Empire

- 파워쉘(PowerShell) 기반 모의 해킹 도구, 깃허브에 소스코드 공개

Remcos

- 원격 제어 도구, 공식 홈페이지에서 무료 버전 공개

QuasarRAT

- 원격 제어 도구, 깃허브에 소스코드 공개

악용 빈도가 높은 오픈 소스 기반 도구 와 프리웨어 (2)

- **악용한 도구들 대부분이 깃허브(GitHub)에 소스 코드 공개 또는 별도 홈페이지에서 공개**

rclone

- 클라우드 파일 관리 도구, 깃허브에 소스코드 공개

PsExec

- 원격 파일 전송 및 실행, 마이크로소프트(Microsoft)에서 무료 제공

NjRat

- 원격 제어 도구, 깃허브에 소스코드 공개

NBTscan

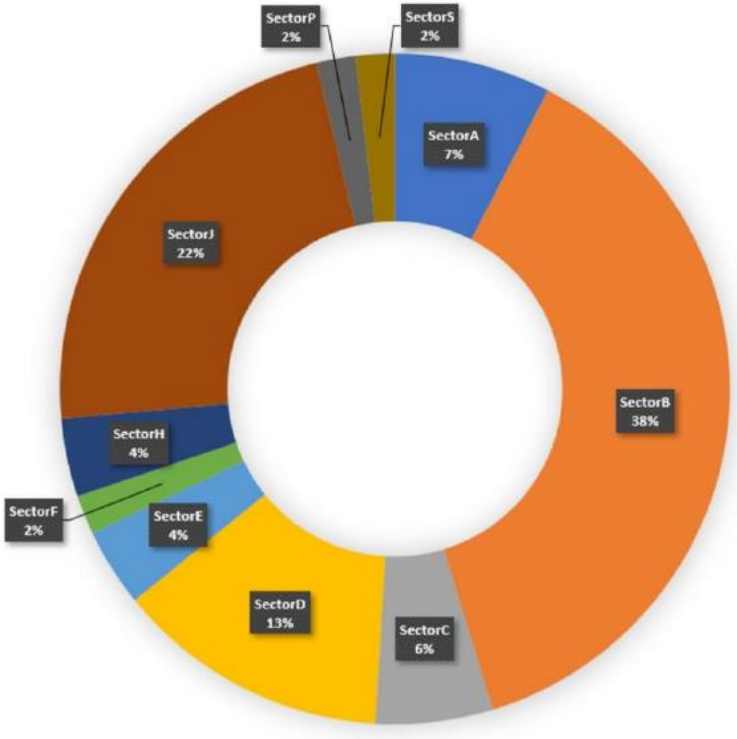
- 넷바이오스(NETBIOS) 스캔 도구, 공식 홈페이지에서 무료 버전 공개

FRP

- 리버스 프록시(Reverse Proxy) 도구, 깃허브에 소스코드 공개

해킹 그룹들이 악용한 오픈 소스 기반 도구와 프리웨어

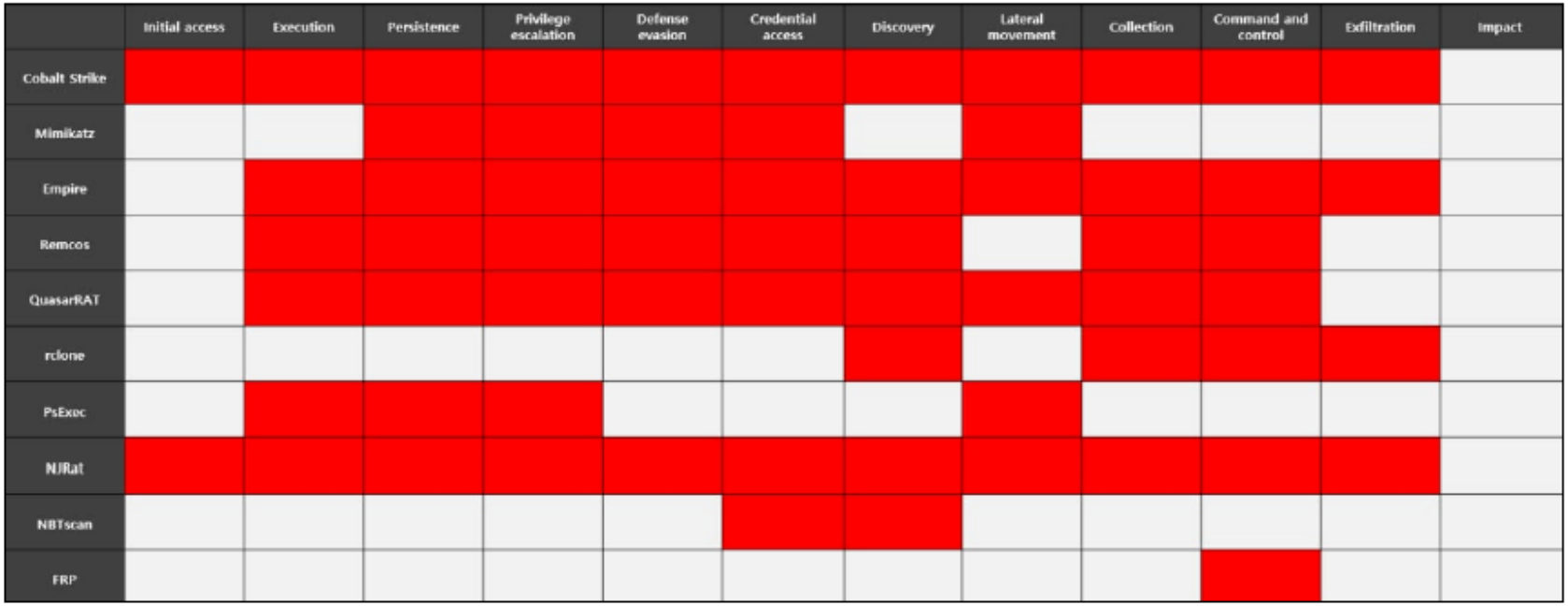
- 2021년 **총 53개 해킹 그룹들**이 해킹 활동에 오픈 소스 기반 도구와 프리웨어를 악용
- 특정 정부 지원 해킹 그룹인 SectorB의 20개 하위 해킹 그룹들이 악용 빈도 높음
- 사이버 범죄 목적의 해킹 그룹인 SectorJ의 12개 하위 해킹 그룹들이 악용



[오픈 소스 기반 도구와 프리웨어를 악용한 해킹 그룹들 분포]

공격 진행 단계에 따른 MITRE ATT&CK Matrix Tactics 구분

- 해킹 그룹의 악용 빈도가 가장 높은 10 개를 MITRE ATT&CK Matrix Tactics으로 구분
- 해킹 그룹은 오픈 소스 기반 도구와 프리웨어를 내부망 침입 이후 가장 활발히 악용
- 최초 침해 시스템에서 정보 및 권한 획득 후 인접 시스템 이동 그리고 데이터 유출 준비 단계



[오픈 소스 기반 도구와 프리웨어의 공격 진행 단계에 따른 구분]

CONCLUSION

해킹 그룹의 오픈 소스 기반 도구와 프리웨어 악용 목적

- 해킹 도구 개발에 따른 리소스(Resource) 절감
  - 과거 성공적으로 악용한 해킹 도구를 재사용하여 개발에 따른 비용 절감
  - 완성도 높은 알려진 모의 해킹 도구와 IT 인프라 관리 도구를 해킹 활동에 수월하게 악용

- 해킹 진행에 대한 탐지 및 대응 회피
  - 직접 제작한 독자적 해킹 도구는 상대적으로 보안 장비 등의 탐지에 노출이 쉬움
  - 해킹 그룹의 전략 자산인 해킹 도구 노출은 공격자의 해킹 활동 특성 분석과 추적 용이
  - 알려진 IT 인프라의 보안 관리 도구는 상대적으로 보안 장비 등의 우회가 용이

실제 해킹 그룹의 해킹 활동 방식 및 해킹 도구 관련

사이버 위협 인텔리전스 확보 필요

사이버 위협 인텔리전스 활용한 방어 체계

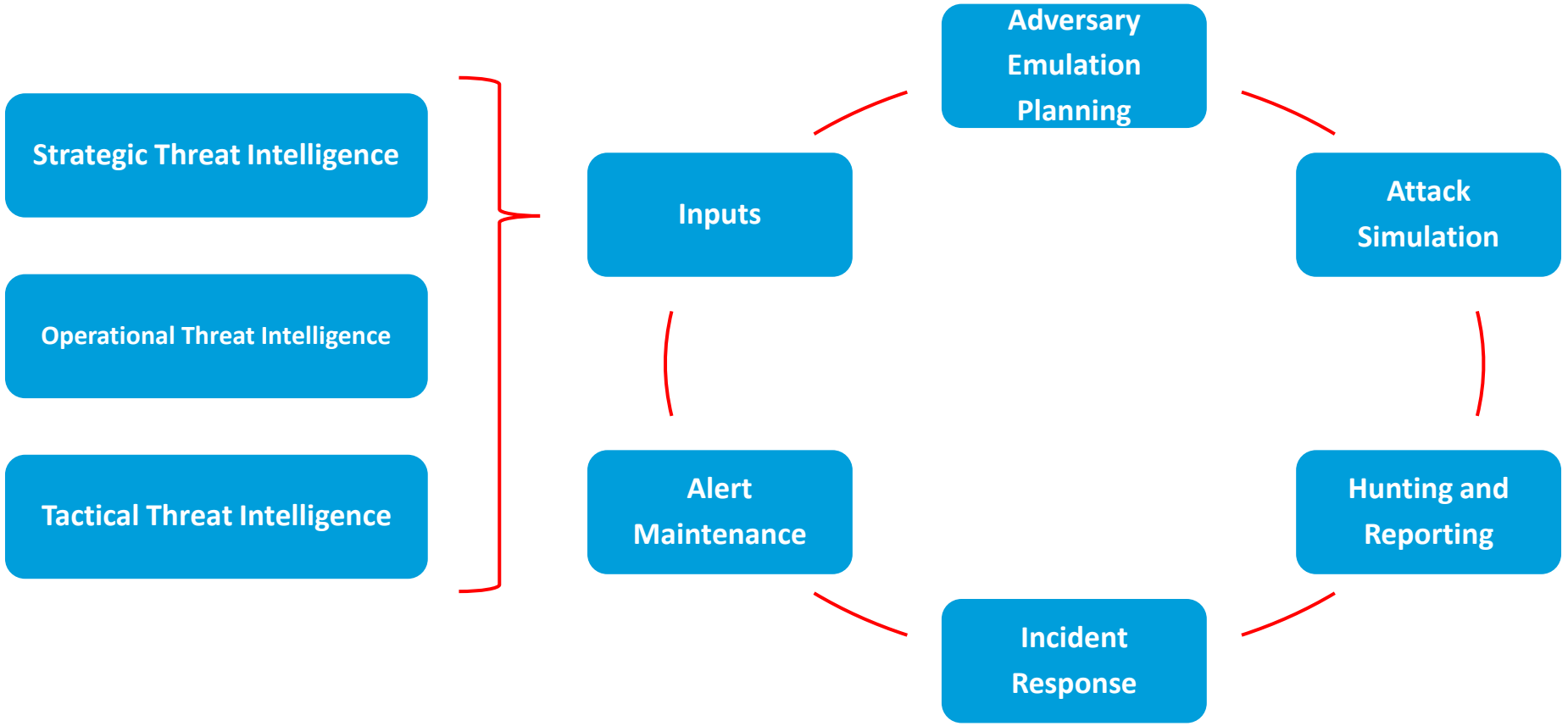
- 전반적인 해킹 활동 동향과 기법 설명
- 조직 보안 전략과 방향성 수립

- MITRE ATT&CK Matrix 기반 공격 과정 설명
- 실제 공격 진행 시 탐지 및 대응 가능성 점검

- IOC의 SIEM 적용으로 실제 공격 탐지 및 대응
- 정기적 위협 헌팅(Threat Hunting) 활동에 활용

사이버 위협 인텔리전스 기반 보안 운영 체계

- 사이버 위협 인텔리전스 기반으로 조직 보안 운영 역량 점검 및 검토
  - 최신 해킹 활동과 유사 해킹 상황(Adversary Emulation Planning과 Attack Simulation) 연출
  - 최신 해킹 활동에 대해 효과적 탐지 및 대응(Hunting and Reporting과 Incident Response) 여부 점검
  - 기술적, 정책적 그리고 프로세스 상의 문제점 검토 후 이를 개선(Alert Maintenance)



THANK YOU

Contact Us

대표 메일 : **RA.global@nshc.net**
NSHC : 서울시 금천구 가산디지털로 1길 186, 제이플라츠 806 (우) 16108
RedAlert 연구소 : 15850 경기도 군포시 당정동 1045 군포아이티밸리 B동 414호