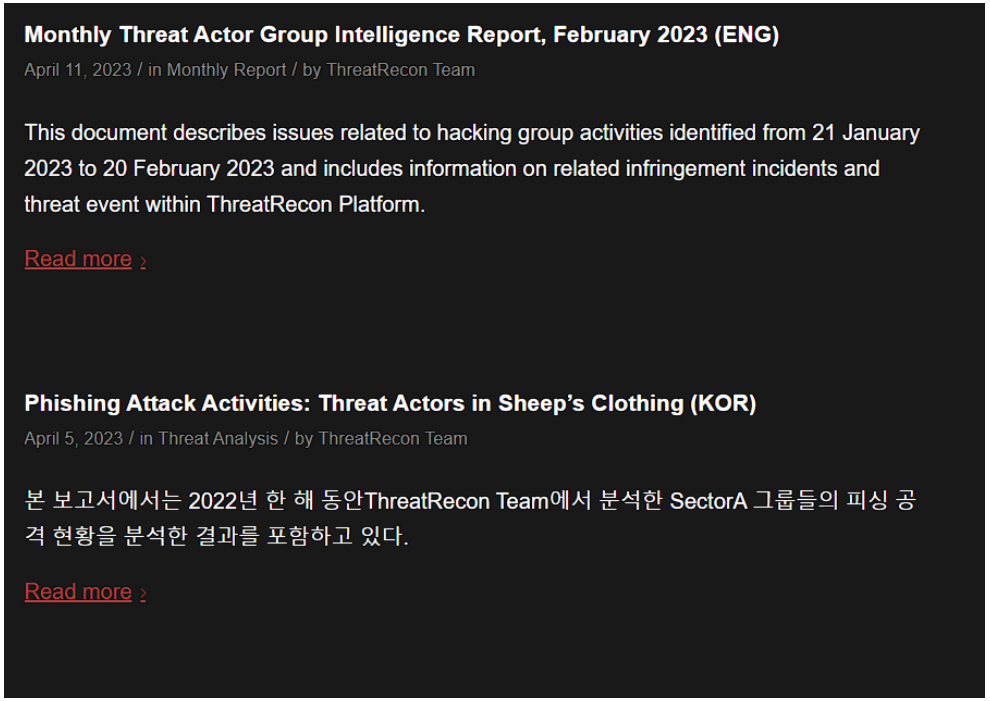
2022년 사이버 해킹 그룹 동향 및 특징 분석

장 영 준 수석
cyj@nshc.net
NSHC Threat Research Lab

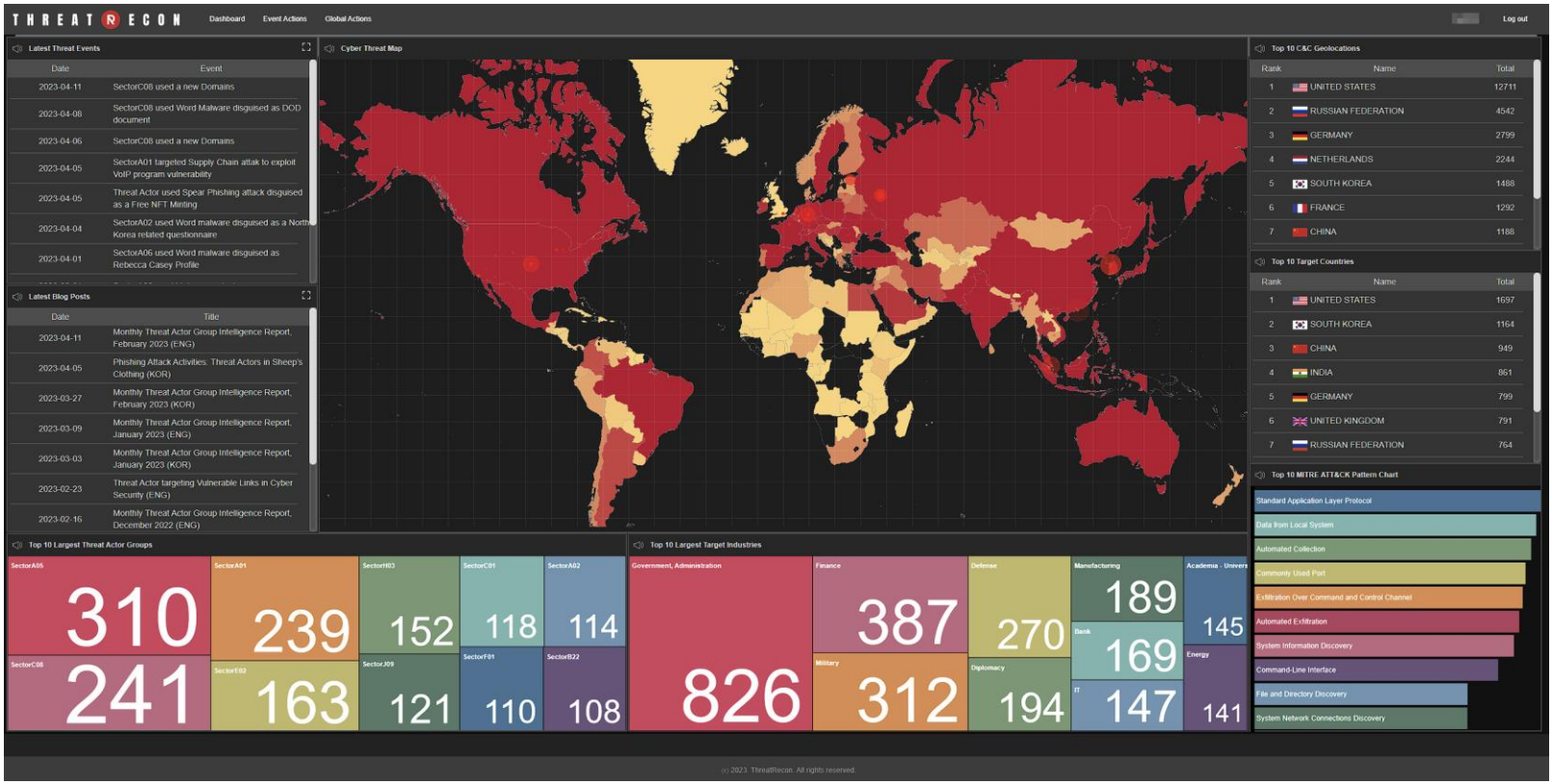
NSHC Threat Research Lab

- NSHC Threat Research Lab은 사이버 위협 분석 및 연구를 담당
- 전 세계에서 활동하는 **사이버 해킹 그룹들의 활동 관련 정보와 위협 데이터 수집 및 분석**
- 수집한 정보 및 위협 데이터 분석 결과를 **ThreatRecon Platform으로 CTI 서비스 제공**
- **트위터(twitter.com/nshcthreatrecon)와 블로그(redalert.nshc.net/blog) 운영**



ThreatRecon Platform 위협 데이터 현황

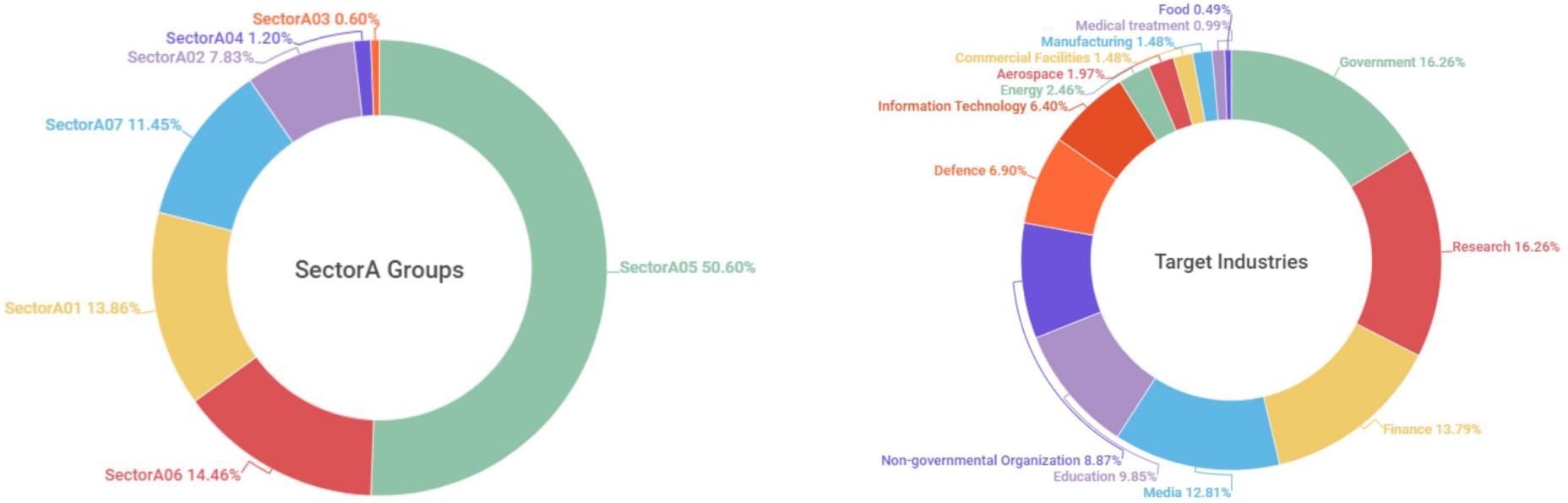
- **해킹 그룹들의 해킹 활동 관련 정보와 위협 데이터 수집 및 분석**
  - 전 세계 다양한 지역에서 발생하는 사이버 해킹 그룹들의 활동 관련 정보와 데이터 수집 및 분석
  - ThreatRecon Platform은 **총 18개 특성(Sector) 308개 해킹 그룹** 관련 위협 데이터 제공 (2023년 4월 16일 기준)
  - 현재 **5,168건 이상 위협 이벤트**와 **441,401건 이상 위협 데이터 제공** (2023년 04월 16일 기준)



2022년 주요 사이버 해킹 그룹 동향 분석

북한 정부 지원 해킹 그룹들의 공격 활동 현황 (1)

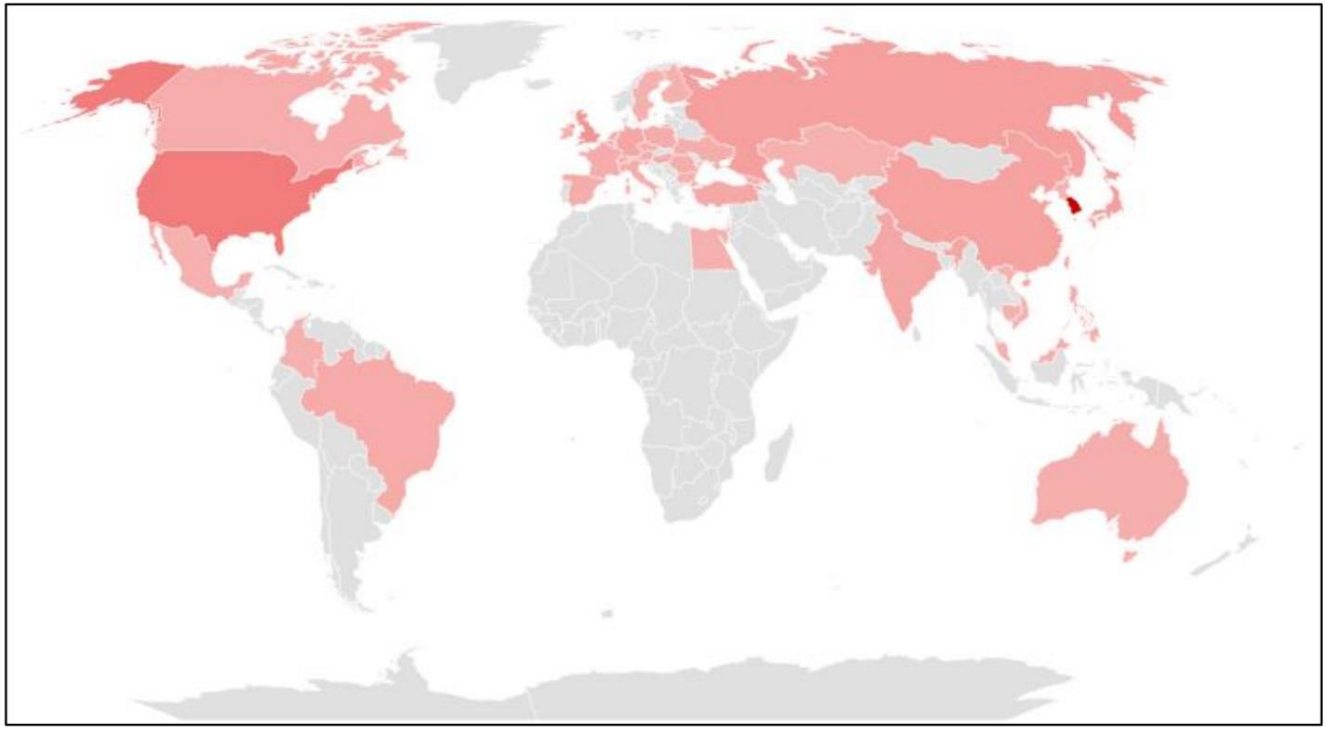
- **북한 정부 지원 해킹 그룹 SectorA 그룹들 활동**
  - 2022년 북한 정부 지원 해킹 그룹들은 총 7개 그룹들의 활동 발견
  - SectorA05 그룹의 활동이 전체의 50%를 차지, 그 다음은 SectorA06 및 SectorA01 그룹 차지
  - 주요 공격 대상 산업군은 정부 기관과 연구 기관 그리고 금융 산업 차지



[2022년 SectorA 그룹들의 활동 분포 및 공격 대상 산업군]

북한 정부 지원 해킹 그룹들의 공격 활동 현황 (2)

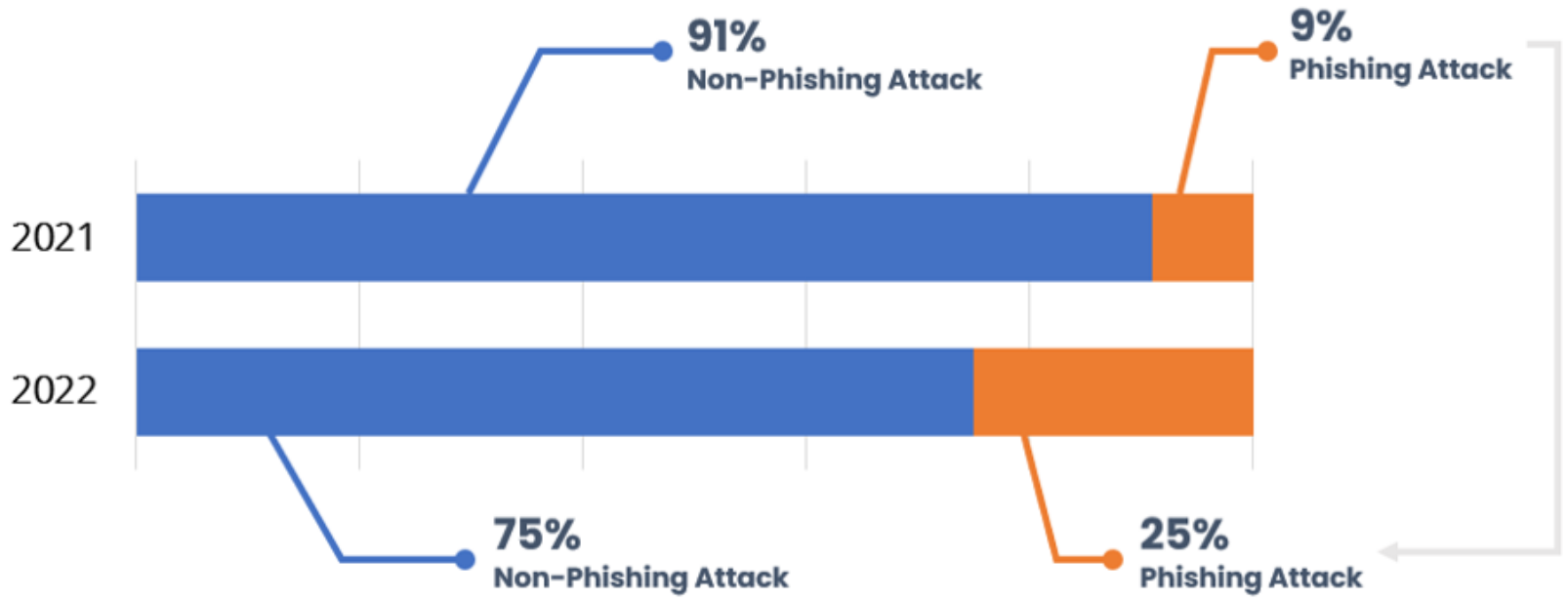
- **북한 정부 지원 해킹 그룹 SectorA 그룹들 공격 대상 국가**
  - 주요 해킹 대상 국가는 한국, 미국, 영국 그리고 러시아 순서를 차지
  - 북한 정부와 정치적 경쟁 국가들의 활동과 관련된 정보 수집 활동
  - 경제 제재로 인해 현금화 가능한 디지털 자산 정보 탈취 활동



[2022년 SectorA 그룹들의 공격 대상 국가]

북한 정부 지원 해킹 그룹들의 공격 활동 현황 (3)

- **북한 정부 지원 해킹 그룹들의 피싱 공격 활동은 약 2.5배 증가**
  - 피싱 공격 활동은 2021년 전체 해킹 활동의 9%에서 2022년 25%로 **약 2.5배 증가**
  - 피싱 공격은 다른 해킹 기법에 비해 상대적으로 기술적 난이도가 낮음
  - 피싱 공격에 필요한 공격 자원이 다른 해킹 활동 대비 상대적으로 적게 소모

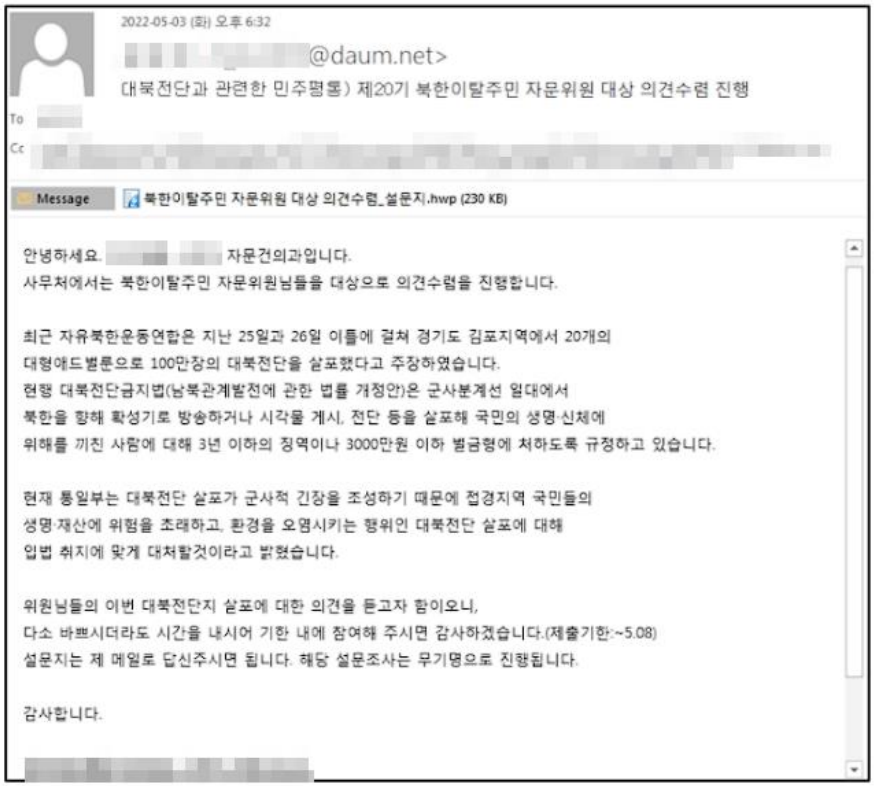


[최근 2년 SectorA 그룹들의 피싱 공격 활동 추이]

북한 정부 지원 해킹 그룹들의 공격 활동 현황 (4)

- **북한 정부 지원 해킹 그룹들의 공격 기법과 사이버 공격 무기**
  - MS 오피스 및 한글(HWP) 파일 형태, 윈도우 도움말(CHM) 파일 및 윈도우 바로가기(LNK) 등 활용
  - 웹 브라우저, 외부 접점 시스템 및 한국에서 광범위하게 사용하는 소프트웨어 취약점 악용

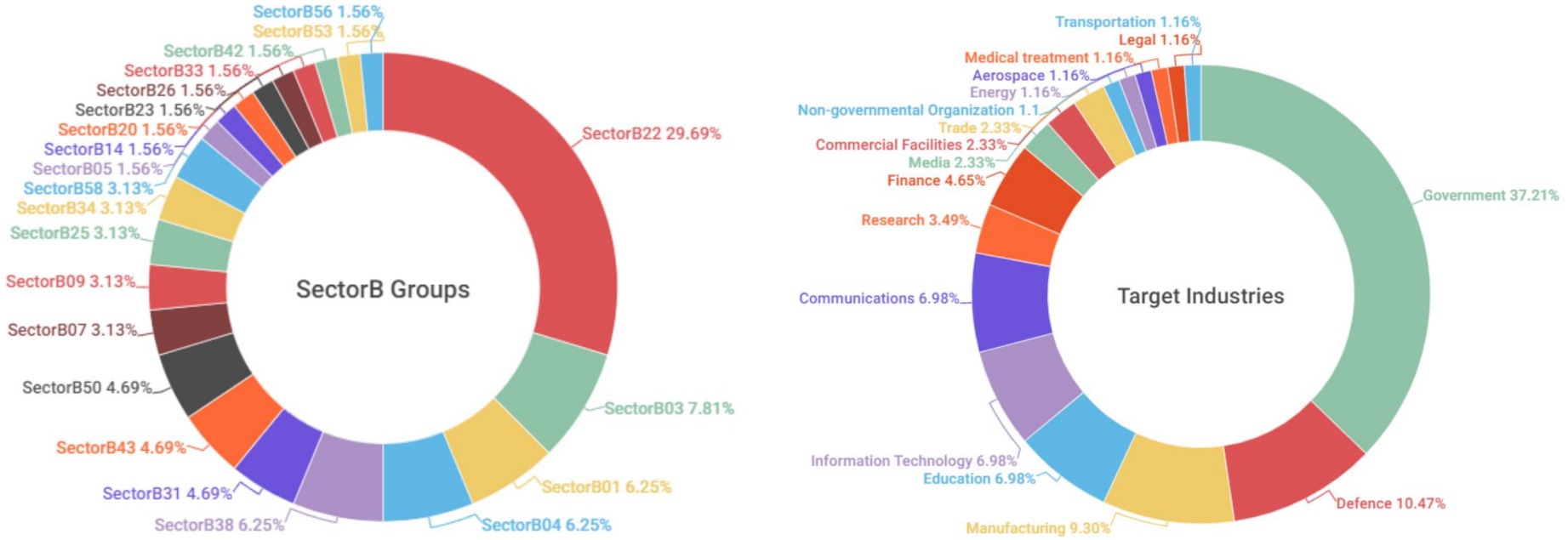
[SectorA06 그룹의 가상화폐 거래소 대상 해킹 활동]



[SectorA02 그룹의 탈북자 대상 해킹 활동]

중국 정부 지원 해킹 그룹들의 공격 활동 현황 (1)

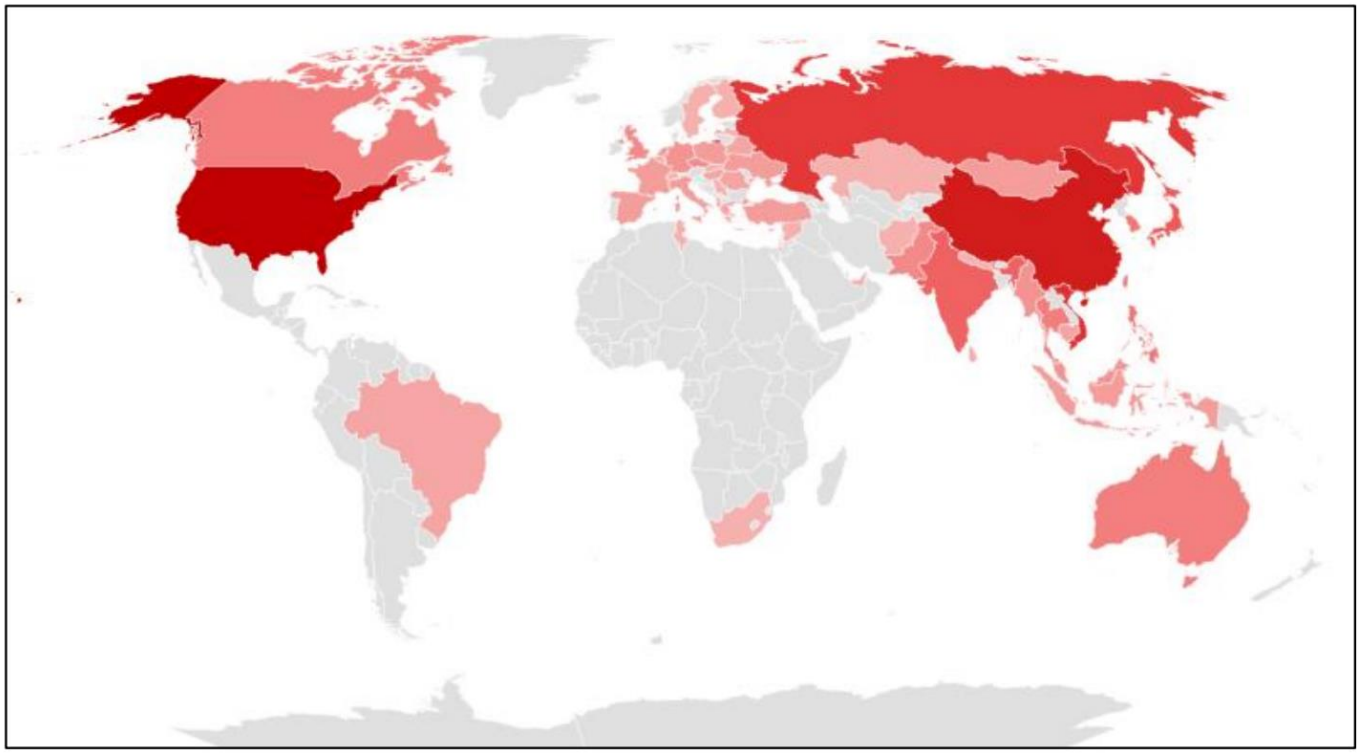
- **중국 정부 지원 해킹 그룹 SectorB 그룹들 활동**
  - 2022년 중국 정부 지원 해킹 그룹들은 총 22개 그룹들의 활동 발견
  - SectorB22 그룹의 활동이 전체의 30%를 차지, 그 다음은 SectorB03과 SectorB01 그룹 순서를 차지
  - 주요 공격 대상 산업군은 정부 기관과 방위 산업체 그리고 제조 산업 순서를 차지



[2022년 SectorB 그룹들의 활동 분포 및 공격 대상 산업군]

중국 정부 지원 해킹 그룹들의 공격 활동 현황 (2)

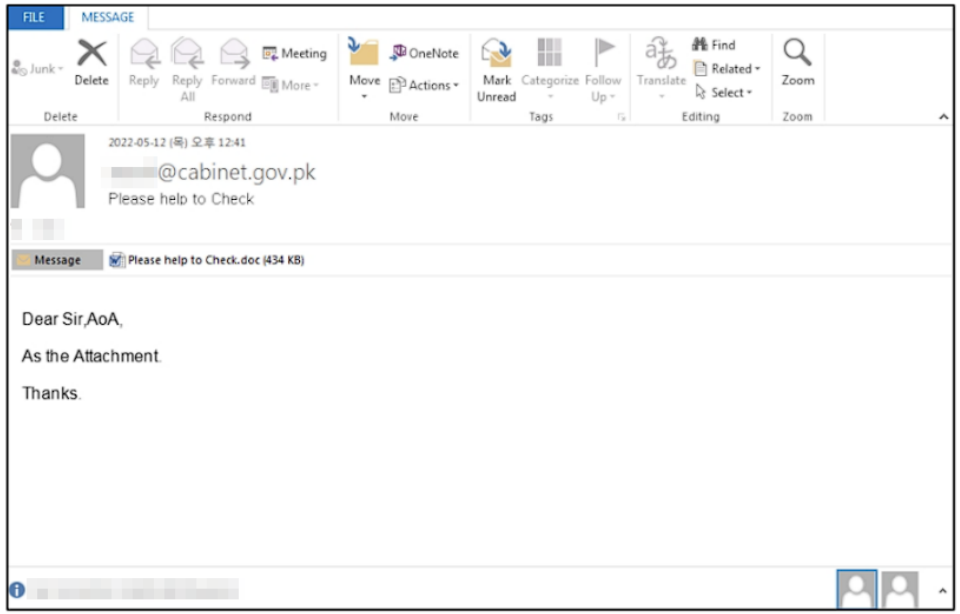
- **중국 정부 지원 해킹 그룹 SectorB 그룹들 공격 대상 국가**
  - 주요 해킹 대상 국가는 미국, 홍콩 그리고 베트남과 러시아 순서를 차지
  - 중국 정부와 정치적 경쟁 국가들 및 소수민족 정치가들의 활동 정보 수집과 고급 군사 기술 탈취 활동
  - 남중국해 인접한 동남아시아 국가들의 활동 정보 수집 활동

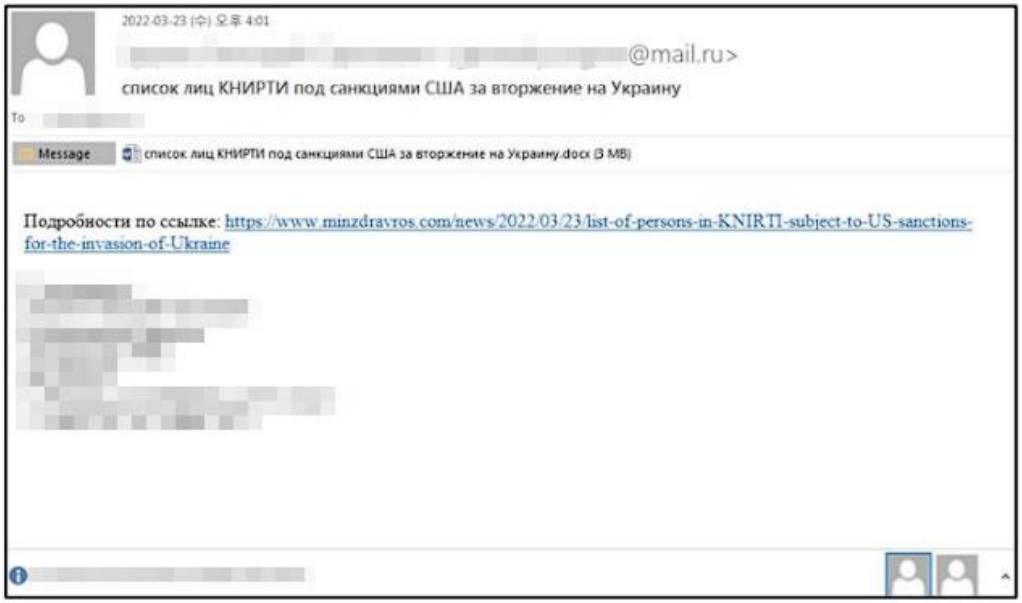


[2022년 SectorB 그룹들의 공격 대상 국가]

중국 정부 지원 해킹 그룹들의 공격 활동 현황 (3)

- **중국 정부 지원 해킹 그룹들의 공격 기법과 사이버 공격 무기**
  - MS 오피스 파일 형태, 윈도우 도움말(CHM) 파일 및 윈도우 바로가기(LNK) 등 활용
  - 정상 파일이 실행 될 때 악성코드를 동반 실행하는 사이드 로딩(Side Loading) 기법 적극 활용
  - 다른 정부 지원 해킹 그룹들과 비교해 다수의 취약점 및 오픈소스 기반 도구들을 적극적으로 활용



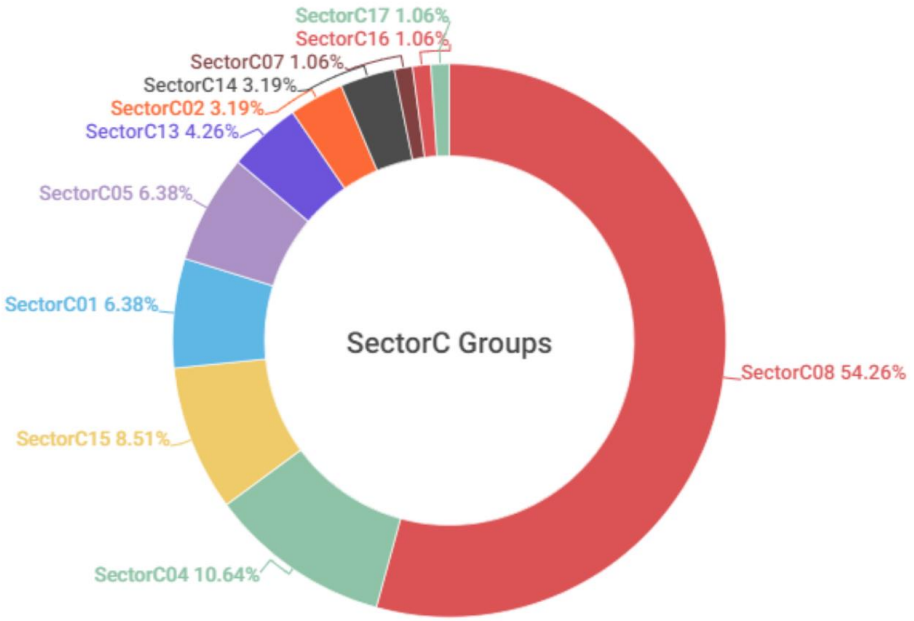


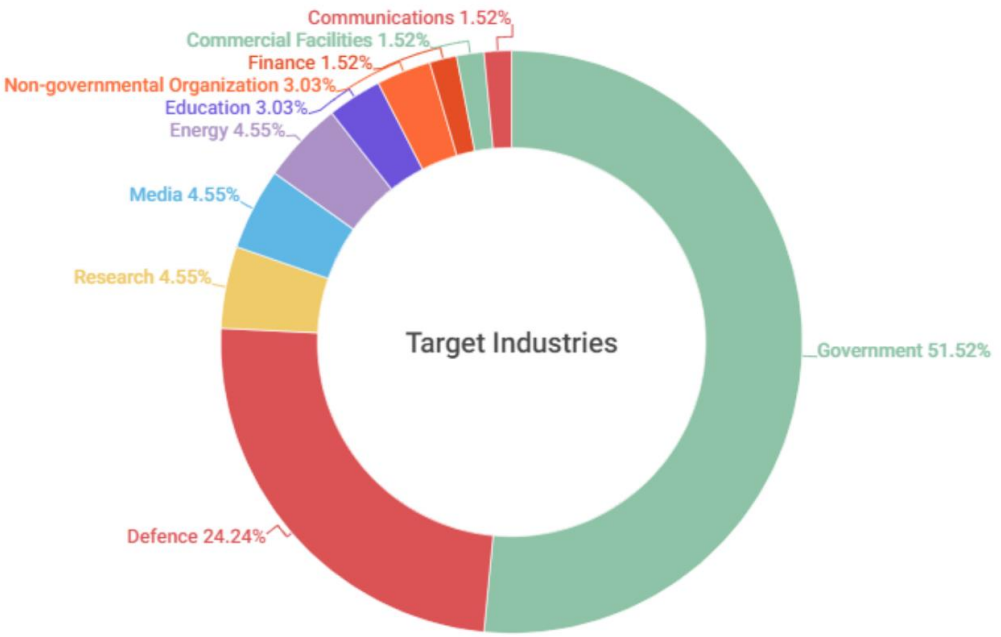
[SectorB25 그룹의 파키스탄 통신국 대상 해킹 활동]

[SectorB04 그룹의 러시아 국방 연구소 대상 해킹 활동]

러시아 정부 지원 해킹 그룹들의 공격 활동 현황 (1)

- **러시아 정부 지원 해킹 그룹 SectorC 그룹들 활동**
  - 2022년 러시아 정부 지원 해킹 그룹들은 총 11개 그룹들의 활동 발견
  - SectorC08 그룹의 활동이 전체의 55%를 차지, 그 다음은 SectorC04 그룹과 SectorC15 그룹 순서를 차지
  - 주요 공격 대상 산업군은 정부 기관과 군 기관 그리고 연구 기관 순서를 차지

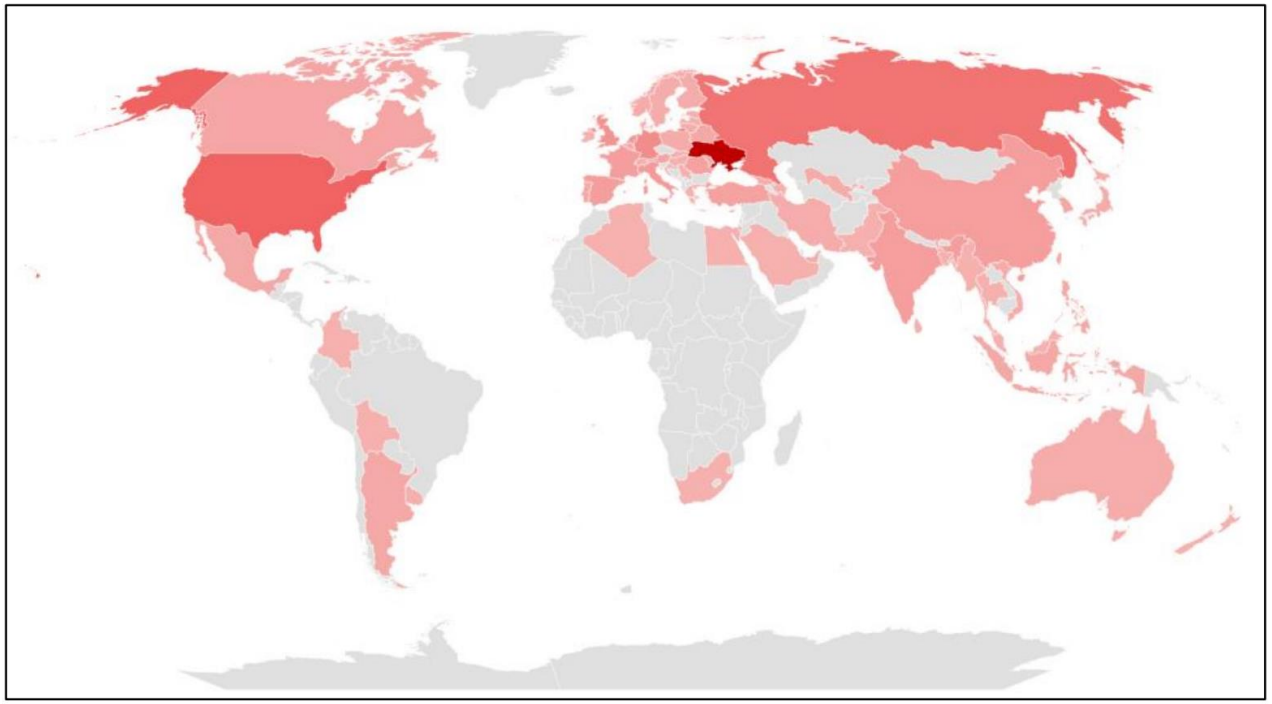




[2022년 SectorC 그룹들의 활동 분포 및 공격 대상 산업군]

러시아 정부 지원 해킹 그룹들의 공격 활동 현황 (2)

- **러시아 정부 지원 해킹 그룹 SectorC 그룹들 공격 대상 국가**
  - 주요 해킹 대상 국가는 우크라이나, 미국, 캐나다 순서를 차지
  - 우크라이나 전쟁 발발 후 나토(NATO) 회원국들과 그 우방국들에 대한 정보 수집 활동
  - 우크라이나에 대한 전방위적 사이버 전쟁으로 군사 정보 수집과 사회 기반 시설 파괴 활동 병행

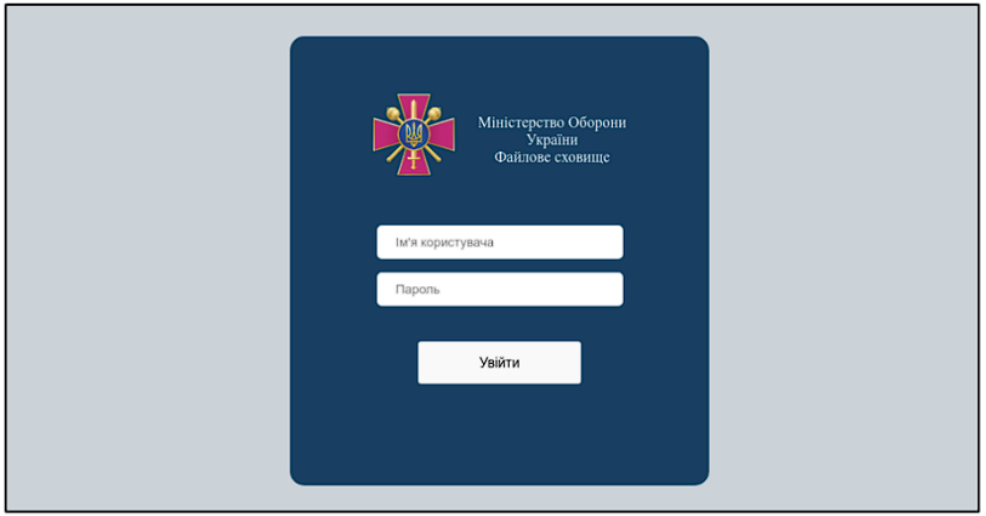


[2022년 SectorC 그룹들의 공격 대상 국가]

러시아 정부 지원 해킹 그룹들의 공격 활동 현황 (3)

- **러시아 정부 지원 해킹 그룹들의 공격 기법과 사이버 공격 무기**
  - 피싱 공격, 문서형 악성코드와 프리웨어 기반의 원격제어 도구까지 다양한 공격 기법과 무기 활용
  - 윈도우 OS, 외부 접점 시스템 및 전력 시스템 자동화 소프트웨어 등 고급 취약점 악용

[SectorC04 그룹의 이탈리아 군사 기관 대상 해킹 활동]



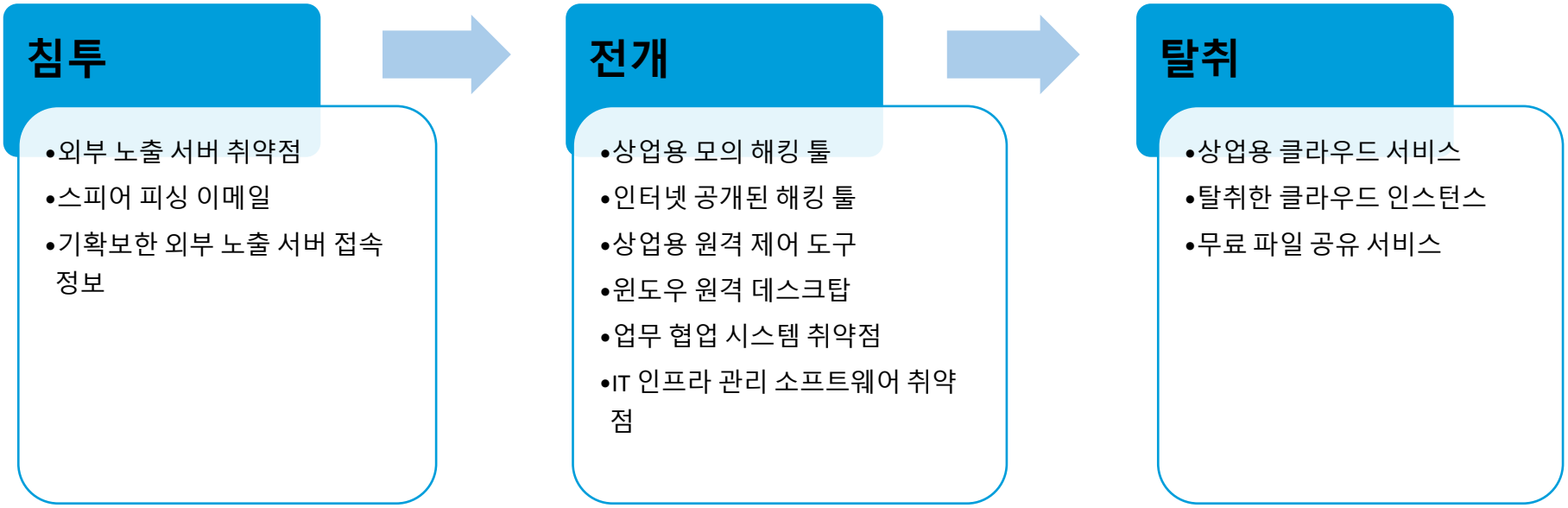
[SectorC14 그룹의 우크라이나 국방부 위장 피싱 사이트]

[SectorC15 그룹의 우크라이나 에너지 기업 대상 해킹 활동]

2022년 사이버 해킹 그룹 활동 특징

사이버 해킹 그룹 활동 관련 주요 특징

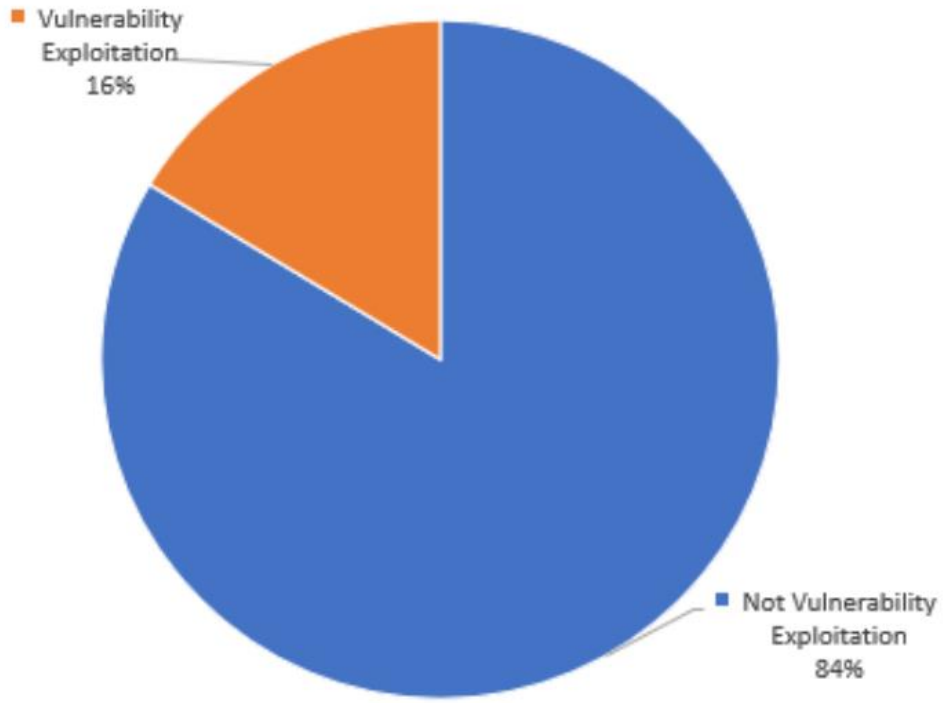
- 침투 단계에 활용 가능한 공격 접점 증가, 악성코드는 비실행형 파일 활용
- 전개 단계는 상업용 또는 공개된 해킹 툴이나 시스템 관리 툴 활용
- 탈취 단계는 수집한 정보들을 상업용 클라우드 서비스 등으로 전송



[사이버 해킹 그룹 활동 관련 해킹 단계별 주요 특징]

사이버 해킹 그룹 활동 관련 주요 특징 – 침투 (1)

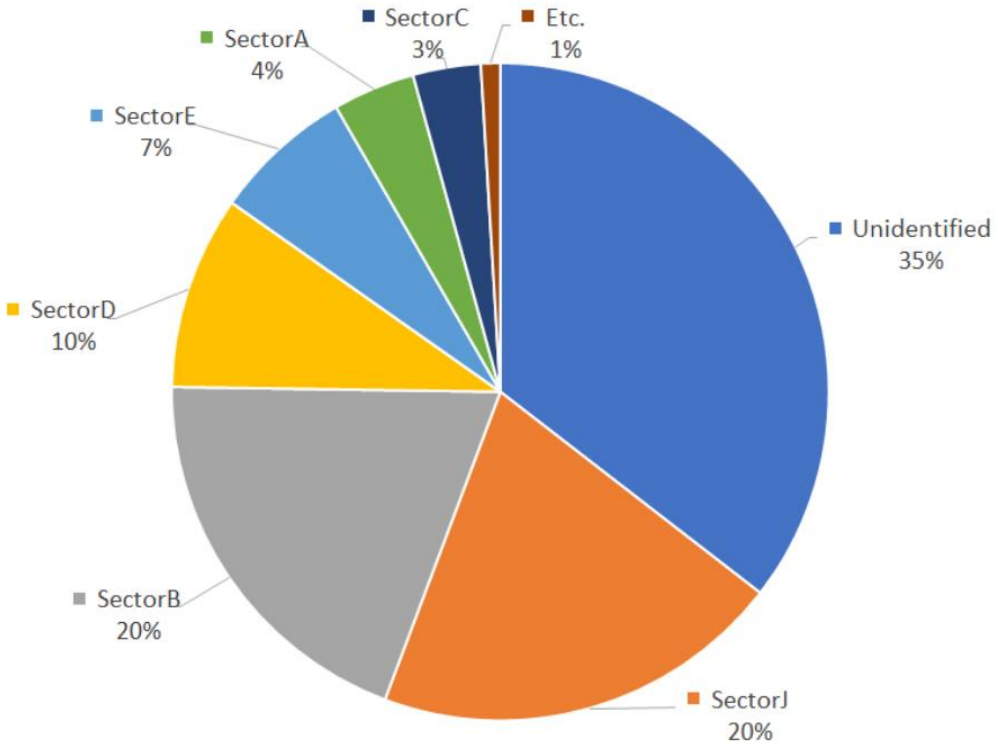
- 2022년 Threat Research Lab 에서 식별한 사이버 공격 활동 중 취약점 악용 비율
- 취약점을 악용한 사이버 공격 활동은 전체 사이버 공격의 16% 차지
- 84%를 차지하는 대부분의 사이버 공격은 취약점 악용하지 않음



[2022년 발생한 사이버 공격 활동 중 취약점 악용 비율]

사이버 해킹 그룹 활동 관련 주요 특징 – 침투 (2)

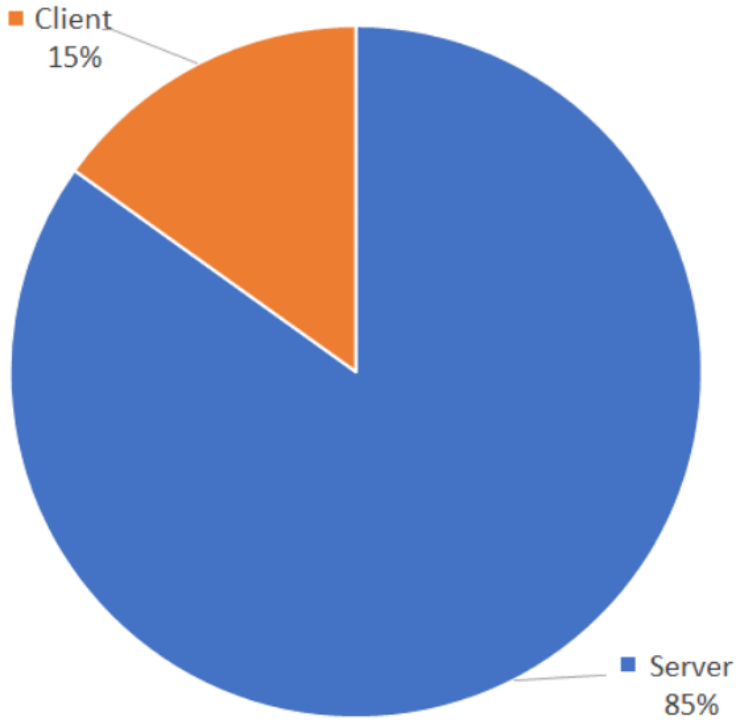
- 미식별(Unidentified) 해킹 그룹과 사이버 범죄(SectorJ) 그룹의 취약점 악용 비중 높음
- 전반적으로는 사이버 범죄 해킹 그룹들의 취약점 악용 비중이 높음
- 취약점 발굴 및 구매에 대한 충분한 활동 지원 여부가 취약점 악용과 인과관계 발생



[최근 3개월 사이버 공격 대상 주요 산업군]

사이버 해킹 그룹 활동 관련 주요 특징 – 침투 (3)

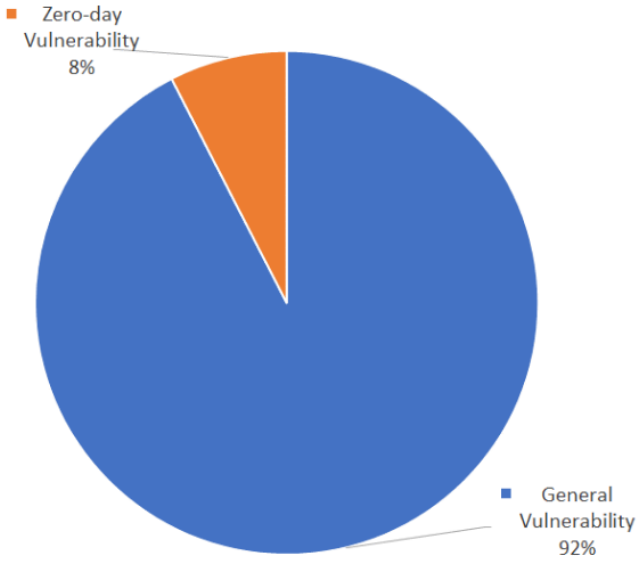
- 취약점이 발견된 소프트웨어 유형에 따라 서버(Server)와 클라이언트(Client) 구분
- 개인용 컴퓨터에 설치된 소프트웨어 취약점 악용은 15%, 서버 소프트웨어 취약점 85% 차지
- 시스템 접속 빈도가 높은 서버 형태의 컴퓨터에 설치된 소프트웨어 취약점 악용 비중 높음

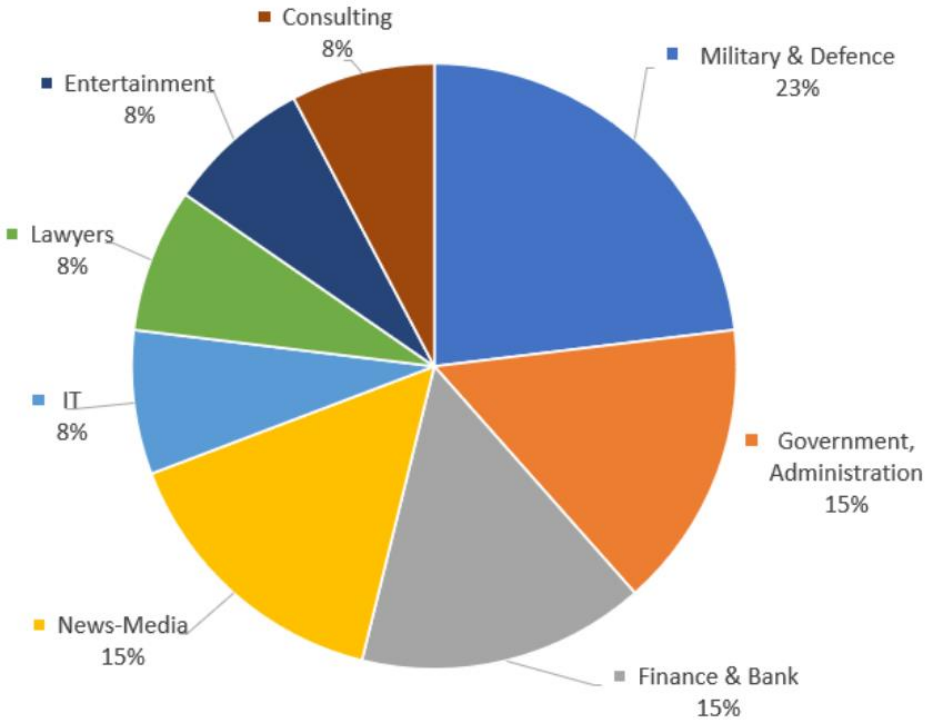


[2022년 취약점이 발견된 소프트웨어 유형 비율]

사이버 해킹 그룹 활동 관련 주요 특징 – 침투 (4)

- 제로 데이 취약점 악용한 사이버 공격 활동은 **전체 취약점 악용 사이버 공격의 8%**로 확인
- 제로 데이 취약점 발굴에는 시간과 자본 등이 필요함으로 활용 빈도 낮음
- 제로 데이 취약점은 군 및 방위 산업 관련 산업군에 악용 빈도가 높음

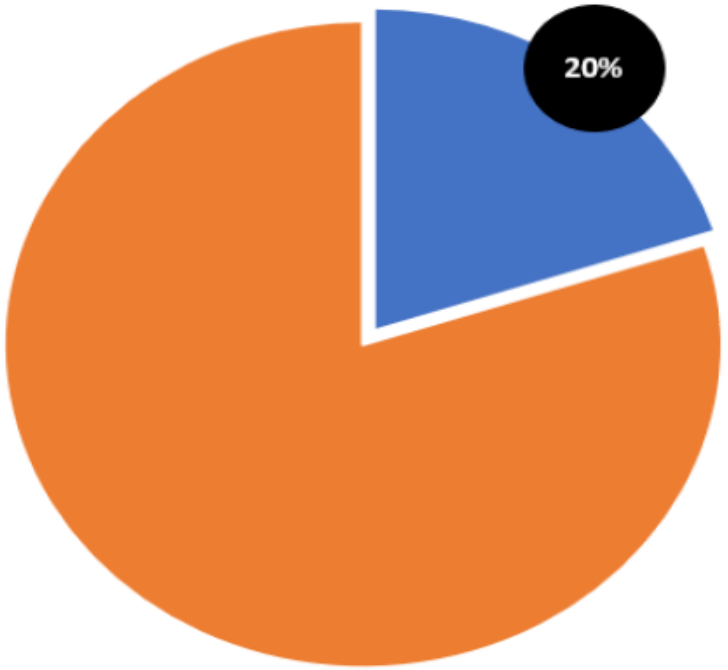




[2022년 발생 사이버 공격 활동 중 제로 데이 취약점 악용 비율과 공격 대상 산업군]

사이버 해킹 그룹 활동 관련 주요 특징 – 전개 (1)

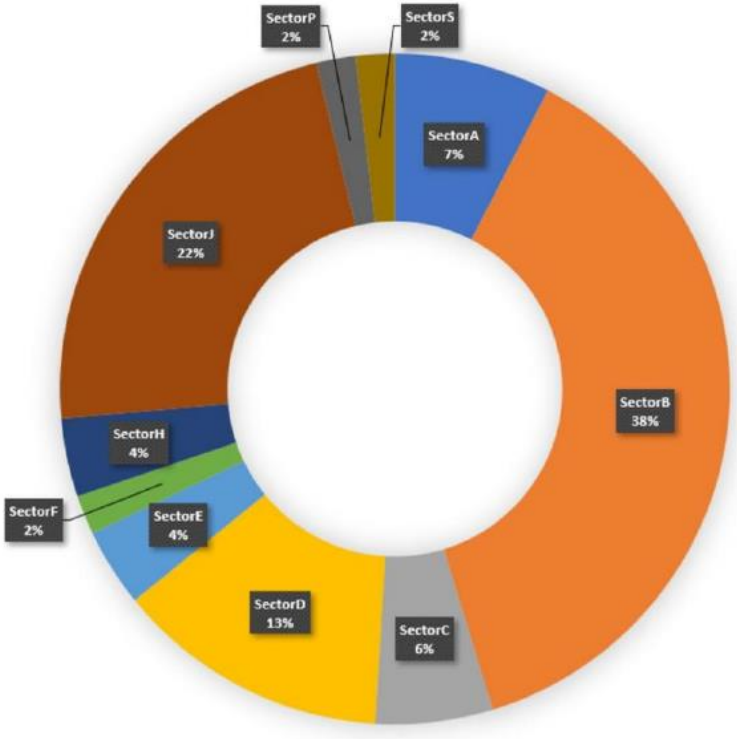
- **2021년 분석한 해킹 그룹 활동 관련 전체 위협 이벤트 중 20% 악용 사례 발견**
- **2021년 발견한 해킹 그룹이 활용한 오픈 소스 기반 도구와 프리웨어는 총 129개 식별**
  - 2022년 총 744개(웹 기반 서비스 106개, 시스템 툴 24개, 오픈소스 툴 391개, 프리웨어 223개) 식별
- **해킹 그룹이 악용한 오픈 소스 기반 도구와 프리웨어는 대부분 IT 인프라 관리 및 점검 용도**



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

사이버 해킹 그룹 활동 관련 주요 특징 – 전개 (2)

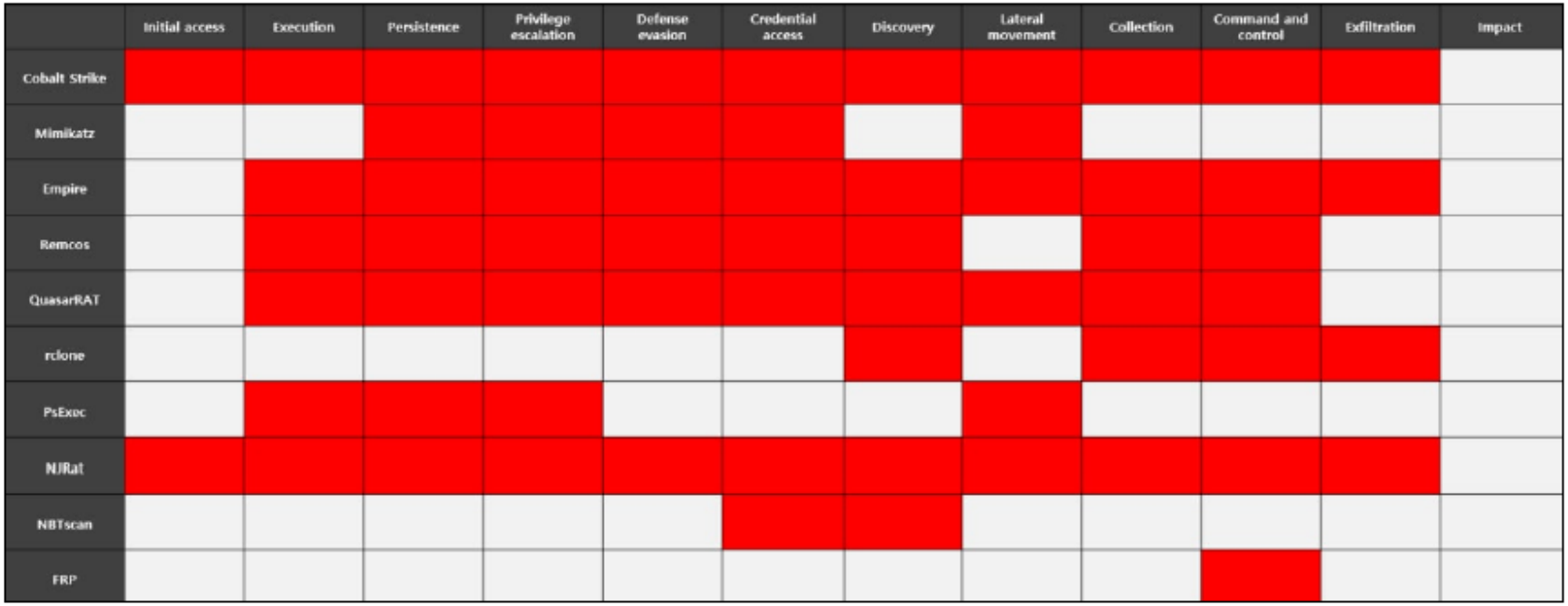
- 2021년 **총 53개 해킹 그룹들**이 해킹 활동에 오픈 소스 기반 도구와 프리웨어를 악용
- 중국 정부 지원 해킹 그룹인 SectorB의 20개 하위 해킹 그룹들이 악용 빈도 높음
- 사이버 범죄 목적의 해킹 그룹인 SectorJ의 12개 하위 해킹 그룹들이 악용



[2021년 오픈 소스 기반 도구와 프리웨어를 악용한 해킹 그룹들 분포]

사이버 해킹 그룹 활동 관련 주요 특징 – 전개 (3)

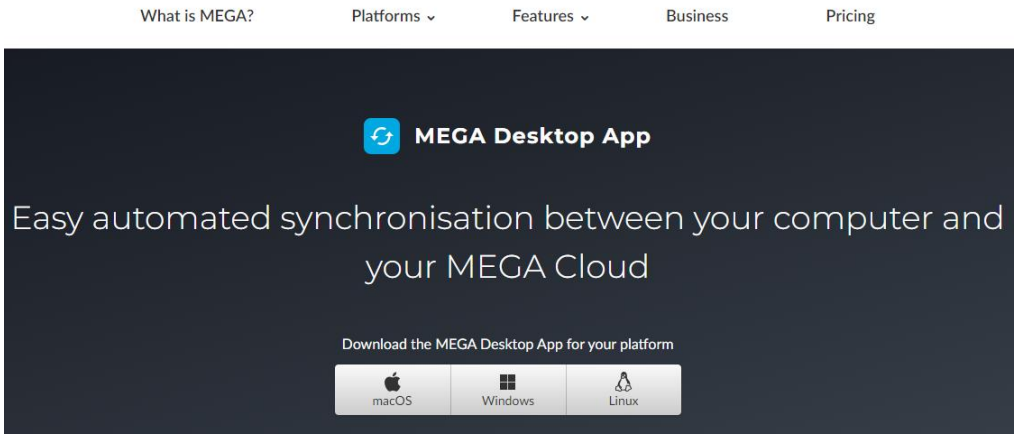
- 해킹 그룹의 악용 빈도가 가장 높은 10 개를 MITRE ATT&CK Matrix Tactics으로 구분
- 해킹 그룹은 오픈 소스 기반 도구와 프리웨어를 내부망 침입 이후 가장 활발히 악용
- 최초 침해 시스템에서 정보 및 권한 획득 후 인접 시스템 이동 그리고 데이터 유출 준비 단계



[2021년 오픈 소스 기반 도구와 프리웨어의 공격 진행 단계에 따른 구분]

사이버 해킹 그룹 활동 관련 주요 특징 – 탈취

- **상업용 클라우드 서비스 활용**
  - 탈취 한 데이터를 상업용 클라우드 서비스인 AWS, Azure 등으로 전송
  - 악성코드 유포 및 C2 서버 구축에 무료 호스팅 서비스(Free Hosting Service) 활용
- **무료 파일 공유 서비스 활용**
  - 구글 드라이브(Google Drive), 원드라이브(OneDrive), 메가 클라우드(MEGA Cloud) 등 활용
  - 악성코드 유포 및 탈취한 데이터 전송 등의 다목적으로 활용



[사이버 해킹 그룹이 활용한 상업용 클라우드 서비스]

결론

Know your Enemy ??

Know my Adversary !!

결론 – Know your Enemy

- **극동 아시아를 중심으로 주요 사이버 해킹 그룹들의 해킹 활동 증가 예상**
  - 우크라이나 전쟁으로 인해 자유 민주주의 동맹국들에 대한 광범위한 해킹 활동 증가 예상
  - 신 냉전 현상이 가시화 될 경우, 자유 민주주의 동맹국들과 사회주의 동맹국들 사이의 사이버 전쟁 발생도 가능
  - 대북 경제 제제와 북한 무력 시위 등으로 인한 정부 기관 및 민간 기업 대상 해킹 활동 증가 예상
  - 극동 아시아의 자유 민주주의 동맹 강화에 따른 정부 기관 정보 탈취 목적의 해킹 활동 증가 예상

- **해킹 그룹들의 취약점을 악용한 해킹 활동은 서버 중심으로 재편**
  - PC를 사용하는 엔드 유저(End User) 소프트웨어 환경보다는 서버 소프트웨어 공략에 집중
  - 취약점은 임의의 코드를 실행 할 수 있는 원격 코드 실행 취약점 선호
  - 원격 코드 실행 취약점 악용으로 초기 침투를 효과적으로 진행

- **오픈 소스 기반 도구와 프리웨어 악용으로 해킹 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 우회 용이

결론 – Know my Adversary

- **사이버 위협 인텔리전스(Cyber Threat Intelligence)는 위협 관련 의사 결정 도구**
  - 인텔리전스는 의사 결정을 위해 반드시 필요한 정보와 데이터들로 구성
  - 조직 형태와 업무 역할에 따라 필요한 정보와 데이터들은 서로 다름

- **IOC(Indicator of Compromised)는 휘발적인 데이터**
  - 공격자가 단시간 언제든지 변경 가능한 데이터 형태들
  - 생명주기(Lifecycle)가 짧아 단발적인 사이버 공격 탐지에는 유효하나 장기적인 관점에서는 비효율적인 데이터들
  - NSHC Threat Research Lab은 지표(Indicator)를 측정 가능하고, 비교 가능한 모든 형태의 데이터들로 재정의

- **사이버 해킹 그룹 행동 방식에 기반한 데이터 필요**
  - 공격자가 사용하는 기술(Technique), 무기(Software) 및 활용법(Procedures)에 대한 이해 필요
  - 공격자에 대한 TTP(Tactics, Techniques, Procedures)에 기반한 데이터들 필요
  - 공격자가 실제 악용하는 소프트웨어 취약점에 대한 대응 우선 순위 결정 필요

THANK YOU

서비스 문의 - service@nshc.net