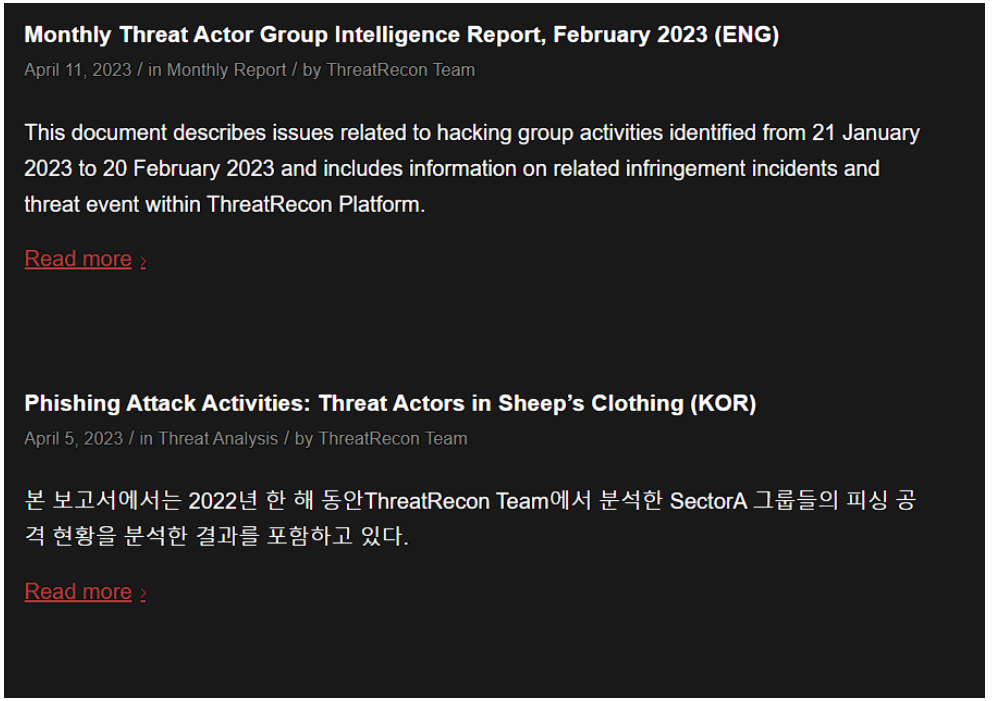
피싱 공격 활동
양의 탈을 쓴 해킹 그룹

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

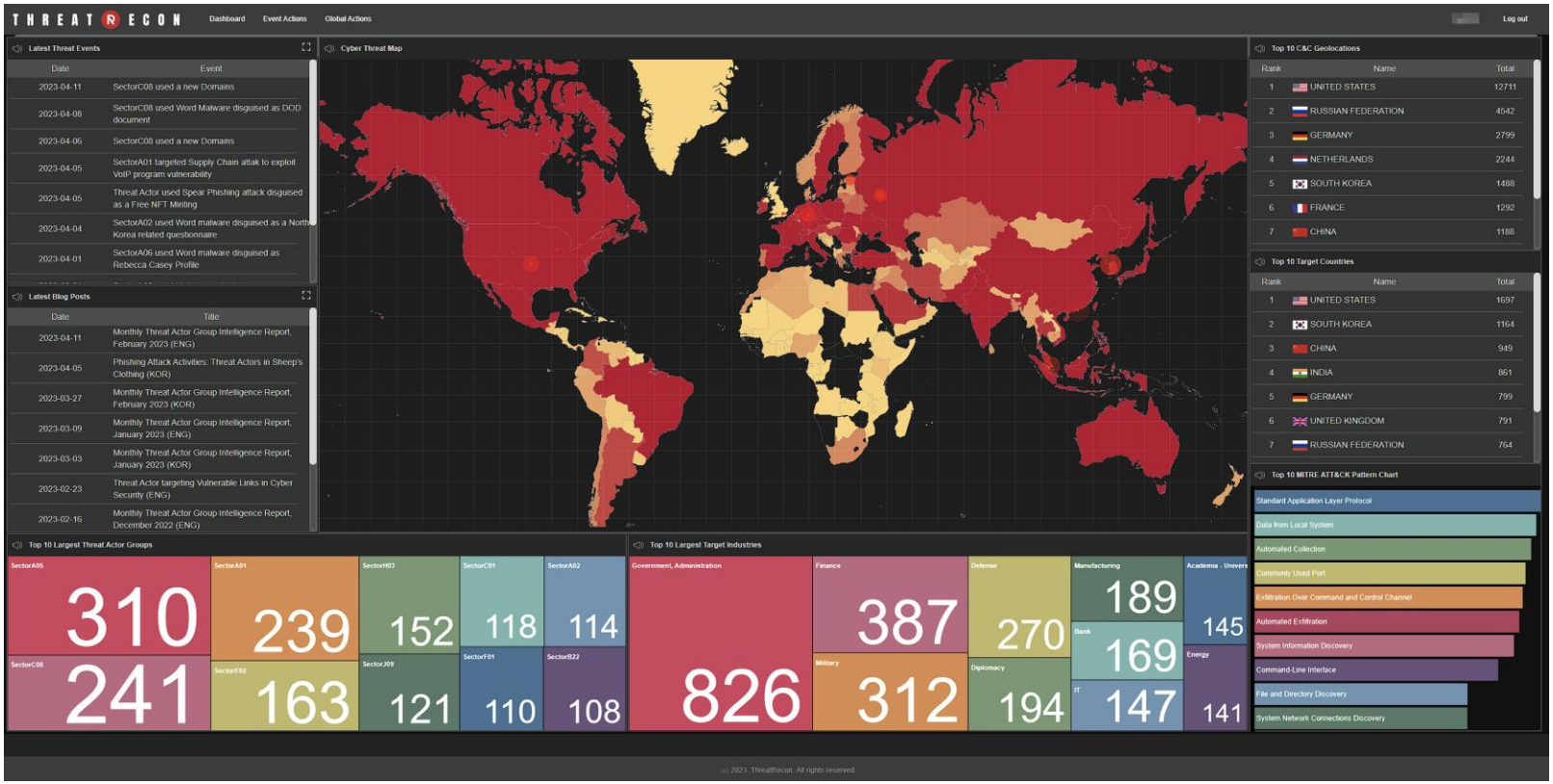
NSHC Threat Research Lab

- NSHC Threat Research Lab은 사이버 위협 분석 및 연구를 담당
- 전 세계에서 활동하는 **해킹 그룹들의 해킹 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

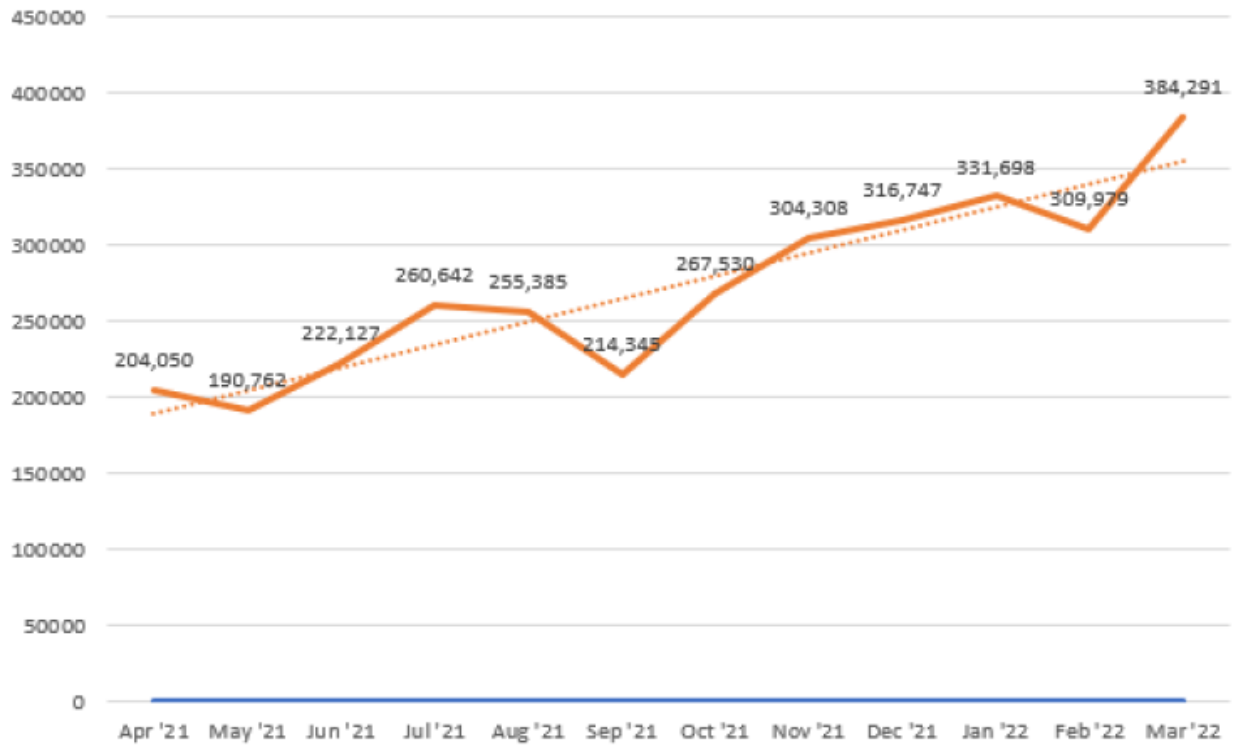
- **해킹 그룹들의 해킹 활동 관련 정보와 위협 데이터 수집 및 분석**
  - 전 세계 다양한 지역에서 발생하는 해킹 그룹들의 해킹 활동 관련 정보와 데이터 수집 및 분석
  - ThreatRecon Platform은 **총 18개 특성(Sector) 308개 해킹 그룹** 관련 위협 데이터 제공 (2023년 4월 16일 기준)
  - 현재 **5,168건 이상 위협 이벤트**와 **441,401건 이상 위협 데이터 제공** (2023년 04월 16일 기준)



피싱 공격 활동
양의 탈을 쓴 해킹 그룹

안티 피싱 워킹 그룹의 최근 피싱 공격 활동 현황

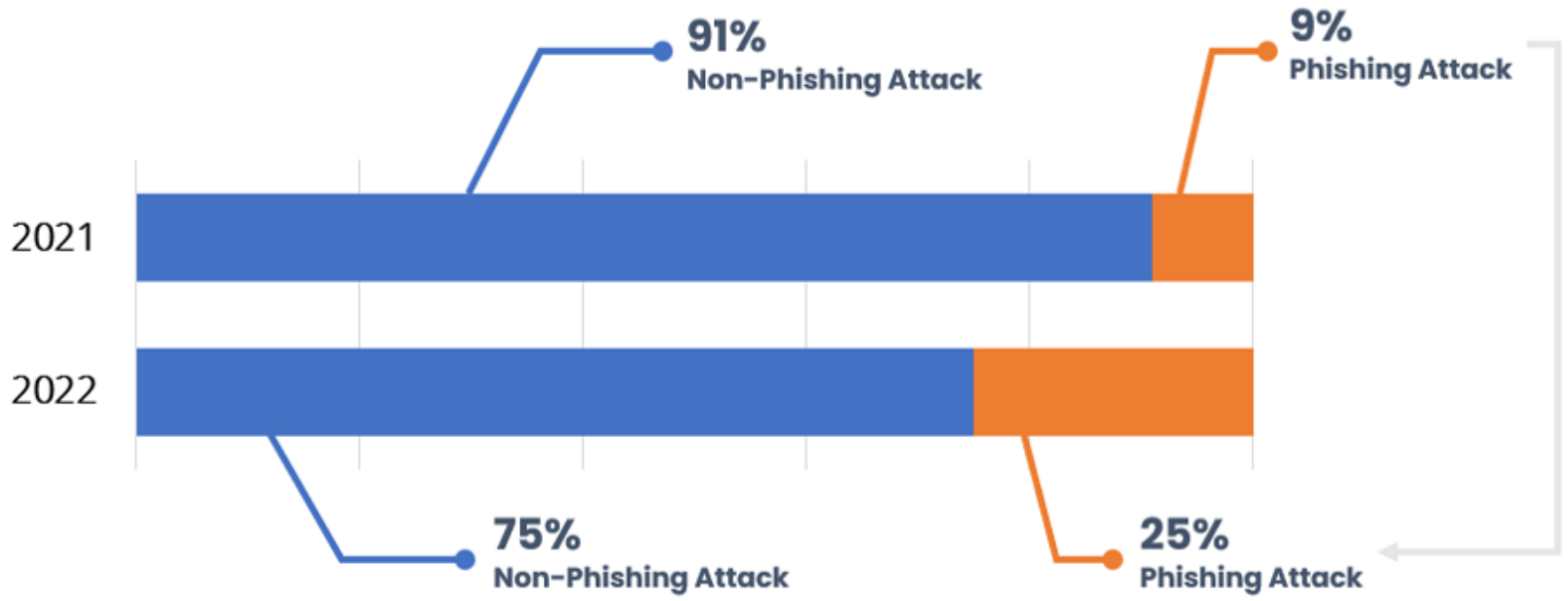
- **국제 피싱 대응 협의체 안티 피싱 워킹 그룹 (Anti-Phishing Working Group) 분석 보고서**
  - 전 세계에서 발생하는 피싱 공격은 2022년 1분기에만 100만 건 이상 발생
  - 전 세계적으로 발생하는 피싱 공격은 2021년 대비 67% 이상 증가 추세



[안티 피싱 워킹 그룹(APWG) 2022년 3월까지의 피싱 공격 추세]

북한 정부 지원 해킹 그룹들의 피싱 공격 활동 현황

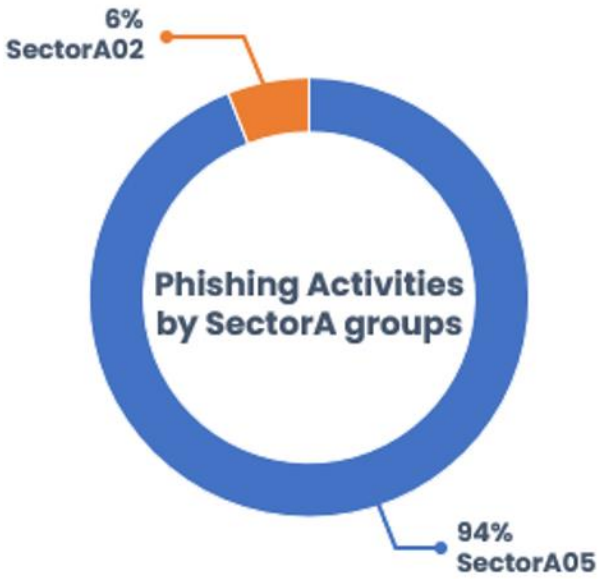
- **북한 정부 지원 해킹 그룹들의 피싱 공격 활동은 약 2.5배 증가**
  - 피싱 공격 활동은 2021년 전체 해킹 활동의 9%에서 2022년 25%로 약 2.5배 증가
  - 피싱 공격은 다른 해킹 기법에 비해 상대적으로 기술적 난이도가 낮음
  - 피싱 공격에 필요한 공격 자원이 다른 해킹 활동 대비 상대적으로 적게 소모



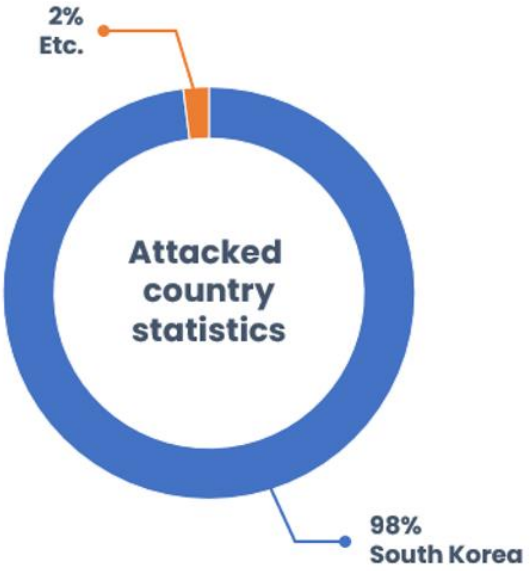
[최근 2년 북한 정부 지원 해킹 그룹 SectorA 그룹들의 피싱 공격 활동 추이]

SectorA 해킹 그룹들의 피싱 공격 활동

- **북한 정부 지원 해킹 그룹을 SectorA로 하위 총 7개 그룹으로 관리**
- **2022년 발생한 피싱 공격은 북한 정부 지원 해킹 그룹들 중 2개 그룹 식별**
  - SectorA05 그룹이 전체의 94%로 피싱 공격 활동을 가장 활발히 수행
  - SectorA 그룹들의 피싱 공격 활동은 전체 98%가 한국을 대상으로 발생



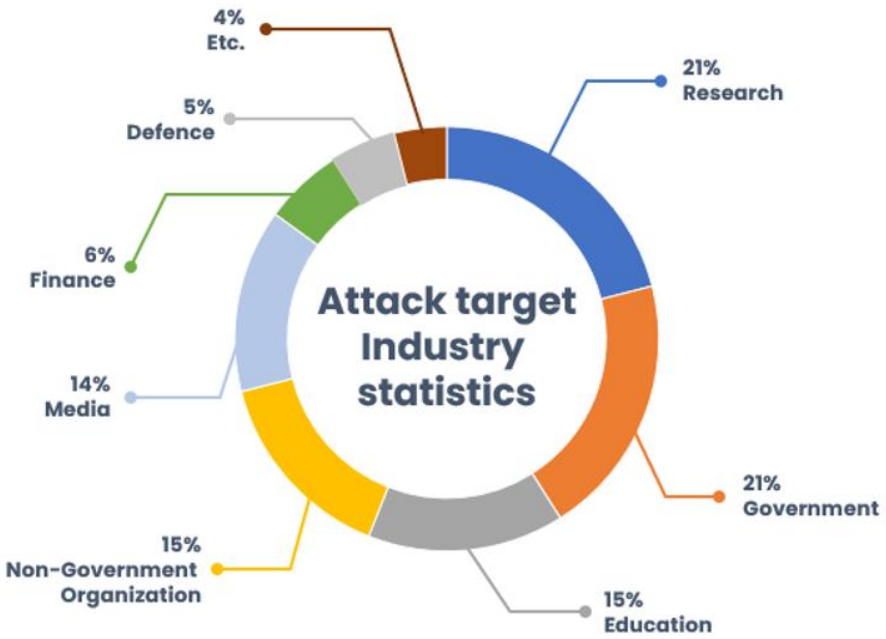
[SectorA 그룹들의 피싱 공격 활동 분포]



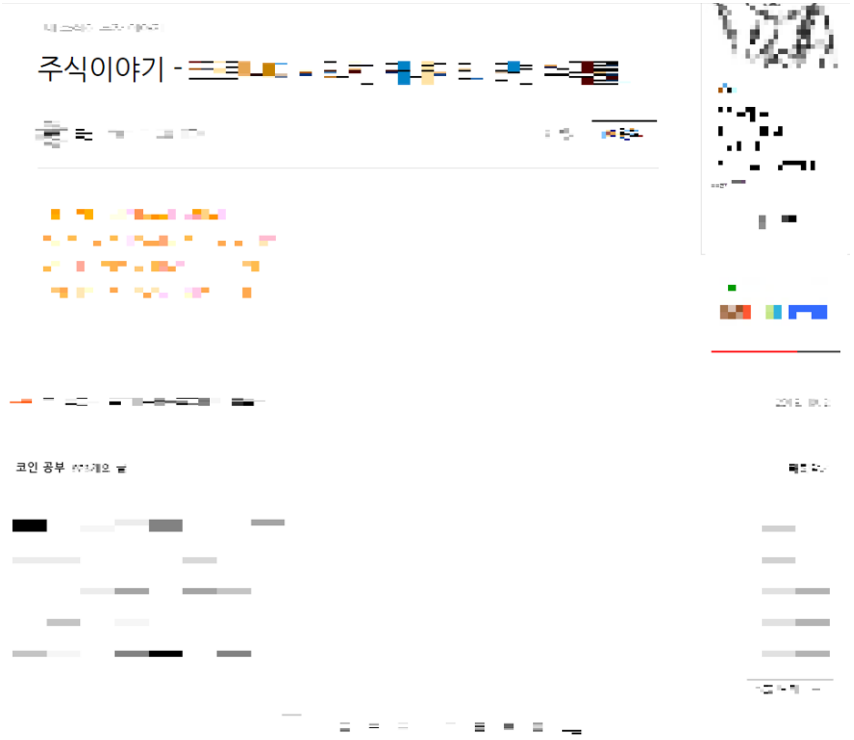
[SectorA 그룹들의 피싱 공격 활동 국가]

SectorA 해킹 그룹들의 피싱 공격 대상

- **피싱 공격 대상은 대북 관련 연구 기관 및 정부 기관 종사자들이 21% 차지**
  - 대북 관련 분야 연구 기관 및 유관 분야 관련 기관 종사자들이 주요 공격 대상
  - 주식, 부동산 및 가상 화폐 등과 관련된 개인 투자자들 역시 주요 공격 대상
  - 개인 투자자들은 주로 한국 내 유명 포털 웹사이트에서 금융 투자 관련 블로그 운영



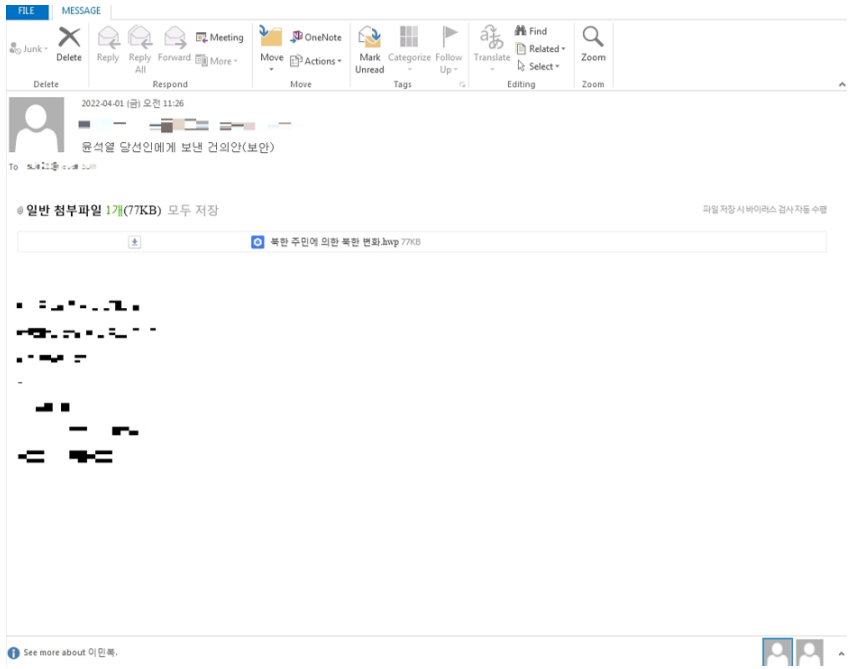
[SectorA 그룹들의 피싱 공격 대상 산업군]

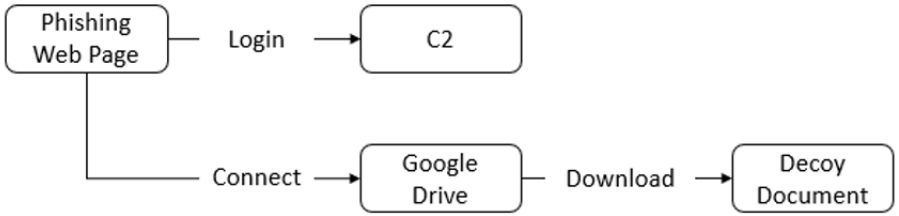


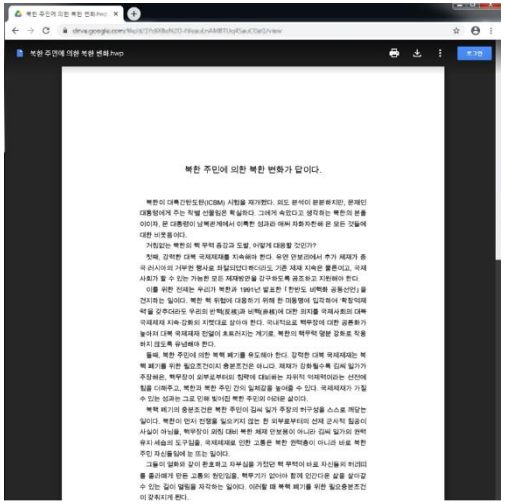
[SectorA 그룹들의 피싱 공격 대상 개인투자자 블로그]

SectorA 해킹 그룹들의 피싱 공격 사례 (1)

- **SectorA05 그룹은 대북 관련 미디어 분야 종사자 대상 피싱 메일 발송**
  - 탈북자 출신의 대북 분야 관계자가 발송한 메일로 위장
  - 피싱 이메일에는 첨부파일이 아닌 피싱 웹페이지로 이동하는 하이퍼링크(Hyperlink) 포함
  - 피싱 웹페이지에서 구글 드라이브에 존재하는 정상 문서 파일을 다운로드



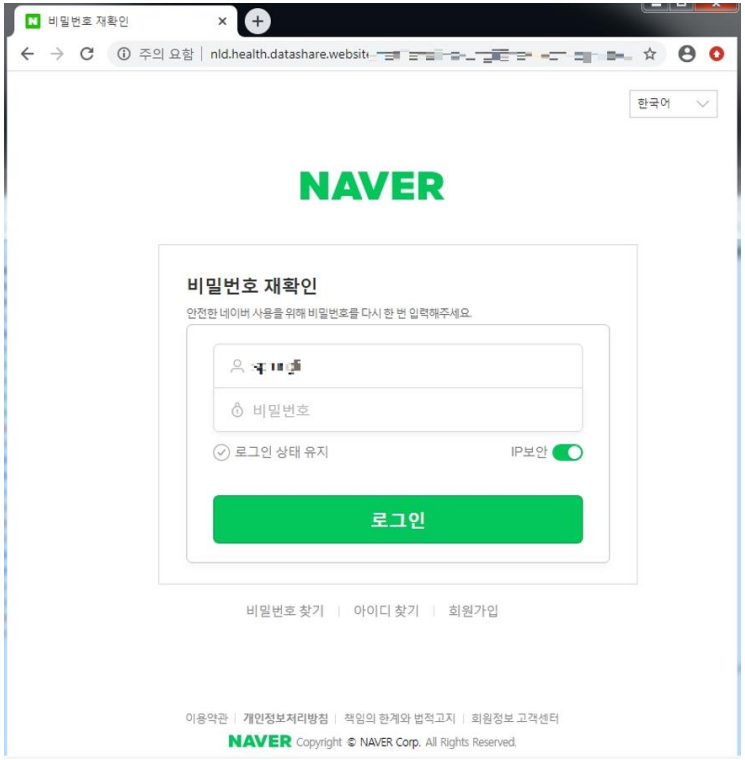




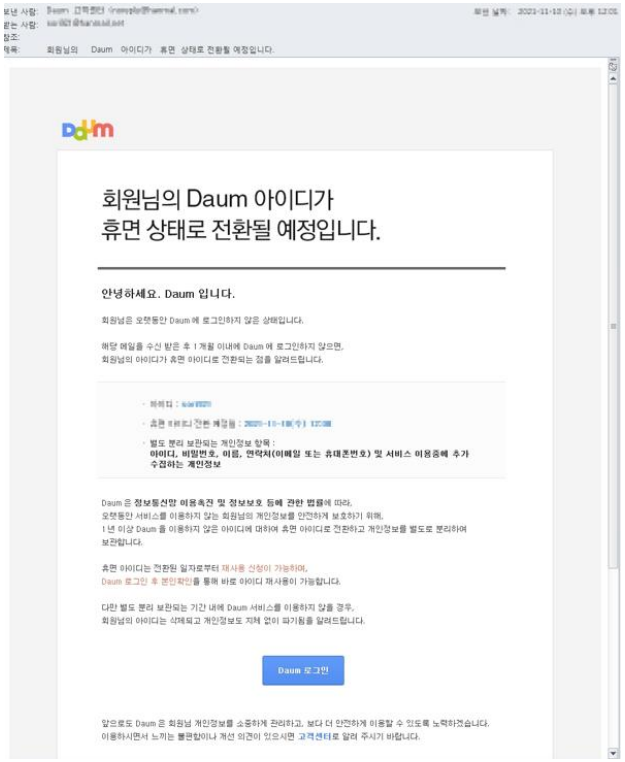
[SectorA05 그룹의 피싱 이메일과 정상 문서 파일]

SectorA 해킹 그룹들의 피싱 공격 사례 (2)

- **SectorA05 및 SectorA02 그룹은 대북 분야 연구 기관 및 대학 관계자 대상 피싱 메일 발송**
  - SectorA05 그룹은 대북 분야 연구 기관 및 탈북자 출신의 대북 분야 관계자 대상 피싱 메일 발송
  - SectorA02 그룹은 대북 분야 대학 관계자 대상으로 피싱 메일 발송
  - 피싱 공격들은 공통적으로 피싱 웹페이지를 포털 웹사이트 로그인 페이지로 위장



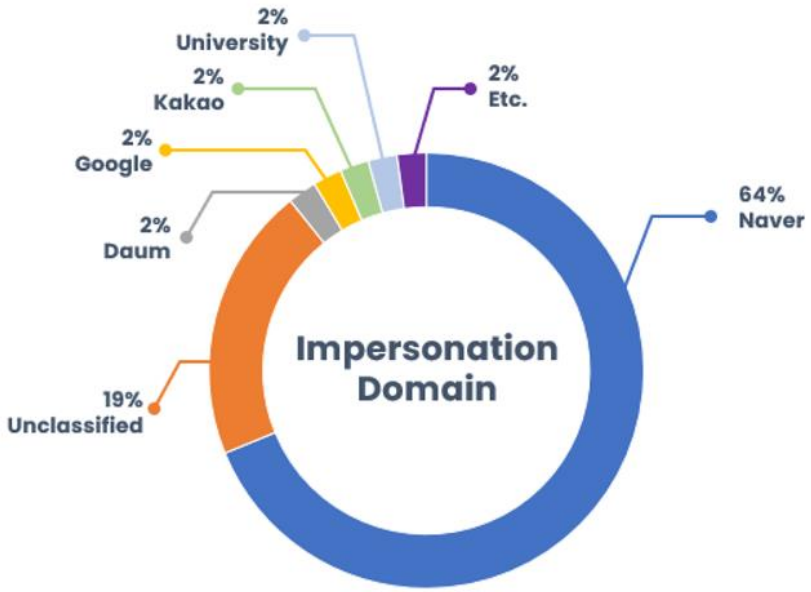
[SectorA05 그룹의 피싱 웹페이지]

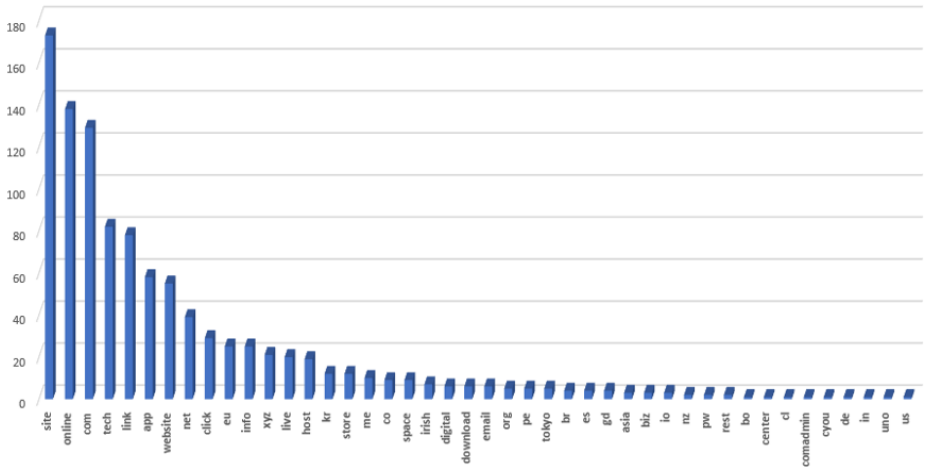


[SectorA02 그룹의 피싱 이메일]

SectorA 해킹 그룹들의 피싱 공격 특징 (1)

- **SectorA 그룹들은 피싱 웹페이지를 인터넷 서비스 웹사이트로 위장**
  - 한국인들의 사용 빈도가 높은 포털 웹사이트들로 위장한 피싱 웹페이지 및 주소로 제작
  - 피싱 웹페이지 주소에서 총 44개의 최상위 도메인(Top-Level Domain, TLD) 식별
  - 피싱 웹페이지는 포털 웹사이트, 대학교, 금융기관 및 공공기관 등과 관련된 주소들로 위장



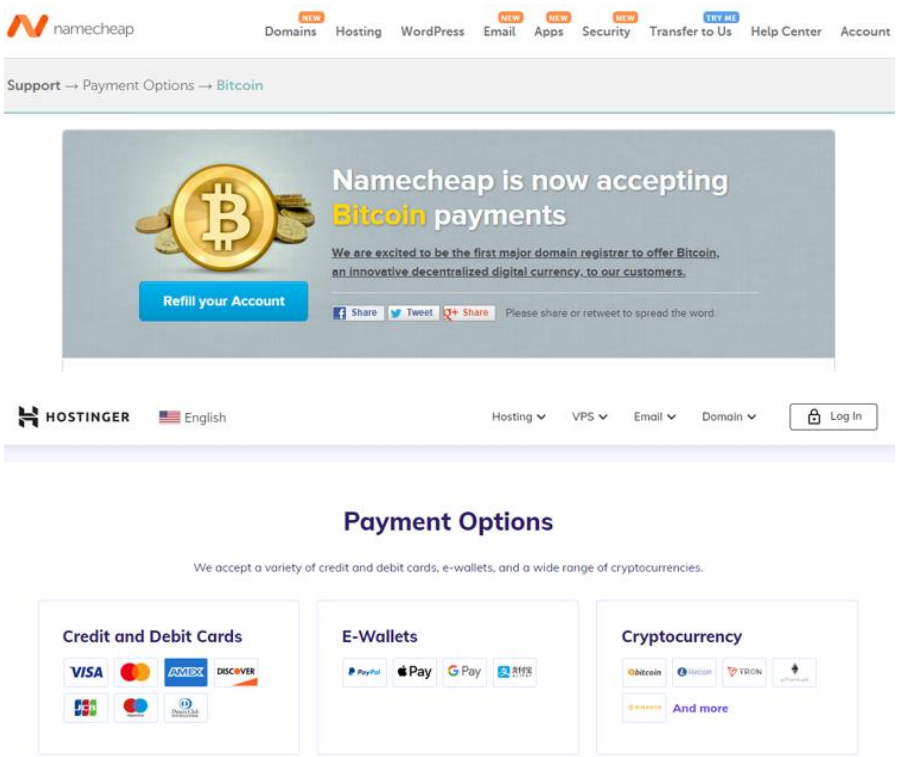


[SectorA 그룹들의 피싱 웹사이트 위장 형태와 사용한 최상위 도메인]

SectorA 해킹 그룹들의 피싱 공격 특징 (2)

- **SectorA 그룹들의 피싱 웹페이지는 웹 호스팅 서비스 활용**
  - 피싱 공격 활동에 사용한 피싱 웹페이지는 총 20개의 웹 호스팅 서비스 활용
  - 웹 호스팅 서비스는 온라인 비대면으로 활용해 피싱 웹페이지를 운영
  - 웹 호스팅 서비스 비용은 가상화폐 및 모바일 결제 등으로도 가능

	도메인 호스팅 서비스	서비스 위치
1	1API GmbH	독일(Germany)
2	Atak Domain	터키(Turkey)
3	Danesco Trading Ltd.	키프로스(Cyprus)
4	Endurance Domains Technology LLP	인도(India)
5	Enom	미국(United States)
6	Gabia	한국(South Korea)
7	Gandi SAS	프랑스(France)
8	GMO	일본(Japan)
9	GoDaddy	미국(United States)
10	Hosting Concepts	네덜란드(Netherland)
11	Hostinger	리투아니아(Lithuania)
12	INAMES	한국(South Korea)
13	Key-Systems GmbH	독일(Germany)
14	MarkMonitor	미국(United States)
15	Name.com	미국(United States)
16	NameCheap	미국(United States)
17	NetEarth One	미국(United States)
18	PublicDomainRegistry	인도(India)
19	Tucows Domains	캐나다(Canada)
20	Whois Corp	한국(South Korea)



[SectorA 그룹들이 활용한 웹 호스팅 서비스와 비용 결제 방식]

결론

결론

- **북한 정부 지원 SectorA 해킹 그룹들의 피싱 공격 증가 추세**
  - 2022년 발생한 전체 해킹 활동 중 25%가 피싱 공격 활동으로 분석
  - 다른 해킹 전략 및 기법들 대비 상대적으로 적은 공격 자원 필요
  - 적은 공격 자원으로 인해 목적에 따라 단기간 빠르게 동시 다발적인 해킹 활동 수행 가능
  - 전략적으로 다른 해킹 활동을 위한 기반 활동으로도 피싱 공격 기법 활용 가능

- **북한 정부 지원 SectorA 해킹 그룹들의 피싱 공격은 대남 정보 수집과 금융 정보 탈취 목적**
  - 피싱 공격의 대상이 대북 관련 연구 기관 및 정부 기관 종사자들이 주요 대상
  - 이는 한국 정부의 대북 관련 정책 및 외교 정책 관련 정보 등을 획득하기 위함
  - 주식, 부동산 및 가상 화폐 등과 관련된 개인 투자자들 역시 대상
  - 대북 경제 제재와 코로나 확산으로 인한 경제 위기를 벗어나기 위한 수단으로 활용

- **IOC(Indicator of Compromised)는 휘발적인 데이터**
  - 공격자가 단시간 언제든지 변경 가능한 데이터 형태들
  - 생명주기(Lifecycle)가 짧아 단발적인 사이버 공격에는 유효하나, 장기적인 관점에서는 비효율적
  - 지표(Indicator)는 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 특성화는 결국 TTP(Tactics, Techniques, Procedures)에 기반한 데이터들

THANK YOU

서비스 문의 - service@nshc.net