SK 쉴더스

Threat Intelligence Report

EQST INSIGHT

EQST(이큐스트)는 'Experts, Qualified Security Team' 이라는 뜻으로
사이버 위협 분석 및 연구 분야에서 검증된 최고 수준의 보안 전문가 그룹입니다.

2025
05

SK 쉴더스

Contents

Headline

망분리의 한계를 넘는 새로운 보안 패러다임: 국가 망 보안체계(N²SF) 도입과 시사점

관제사업그룹 관제사업 3 팀 고광진 팀장

■ 개요

2003 년 1 월 25 일 발생한 분산 서비스 거부(DDoS) 공격은 대한민국의 초고속 인터넷망을 마비시켜 국가 전체를 혼란에 빠드린 사건이었다. 이 사건이 발생하기 전까지 우리나라는 세계적인 초고속 인터넷 강국으로 평가받고 있었다. 빠른 인터넷 기술을 기반으로 1,000 만 명이 넘는 보급률이라는 인상적인 수치도 나왔지만, 화려한 타이틀과 통계 이면에 숨겨진 취약한 정보보호 수준은 '1.25 인터넷 대란'을 계기로 '모래 위의 성'에 불과했음이 드러났다.

이후 2006 년 국가사이버안전전략회의에서 국가기관의 업무망과 인터넷망을 분리하는 정책이 보고되었고, 국가정보원과 안전행정부(현 행정안전부), 한국정보화진흥원(NIA)이 역할을 분담해 '국가기관망분리 구축 가이드'를 배포함으로써 각 부처와 기관들이 참고하도록 했다.

망분리는 지난 18 년여 동안 업무망과 인터넷망을 분리해 사고 발생 시 피해를 최소화하는 국가 공공기관의 핵심 네트워크 보안 정책으로 자리잡아 왔다. 이는 내부 자산을 보호하기 위한 최적의 보안 모델로 기능해왔으나, 경계망 기반의 구조로 인해 보안 영역과 비보안 영역을 평면적으로만 분리하는 한계가 있었다. 구조가 단순하다는 장점이 있는 반면, 물리적 또는 논리적으로 망을 분리함에 따라 고비용, 낮은 유연성, 불편한 사용성 등의 단점도 존재했다.

국가정보원은 이러한 IT 환경의 변화와 현장 애로사항을 반영해 망분리 정책을 시대 상황에 맞게 지속적으로 보완해왔다. 그러나 코로나 19 이후 원격근무, 클라우드, 생성형 AI 등으로 대표되는 IT 환경의 급격한 변화는 기존 망분리 환경에서는 효율적인 업무 수행을 어렵게 만들었다. 이에, 기존 망분리 정책의 한계를 보완하고 변화하는 기술과 환경, 위협에 유연하게 대응할 수 있도록 『국가 망 보안정책 개선 합동 TF』가 구성됐으며, 국가정보원은 이 TF 와 함께 보안통제를 업무의 중요도에 따라 차등 적용하는 '국가 망 보안체계(National Network Security Framework, N²SF)'를 수립했다.

본 리포트에서는 국가 망 보안체계(N²SF)의 추진 목표, 적용 절차, 등급 분류, 보안 대책 등에 대해 자세히 살펴본다.

■ 국가 망 보안체계(N²SF) 추진 목표

국가정보원이 추진한 망분리 정책 개선 다섯 가지를 살표보면 아래와 같다.

첫째, 획일적인 망분리에서 탈피하여 국가 망 보안체계(N²SF) 기반으로 보안 정책의 패러다임을 전환한다.

둘째, 제약 없는 정보유통으로 신기술 융합을 강화하고 스마트 업무 환경을 조성한다.

셋째, 산·학·연·관 전문가와 함께 국내 실정에 최적화된 정책을 개발한다.

넷째, 새로운 보안 정책으로 공표함으로써 각급 기관의 제반 여건을 고려하면서 자율적으로 추진하되, 제도는 점진적으로 변화함으로써 안정적으로 정책이 안착되도록 한다.

다섯째, 공공 정보의 보안성과 활용성을 높이는 것과 함께 보안 기술 및 AI·데이터 산업 등 다양한 산업 발전· 육성으로 디지털 경제 창출에도 기여한다.

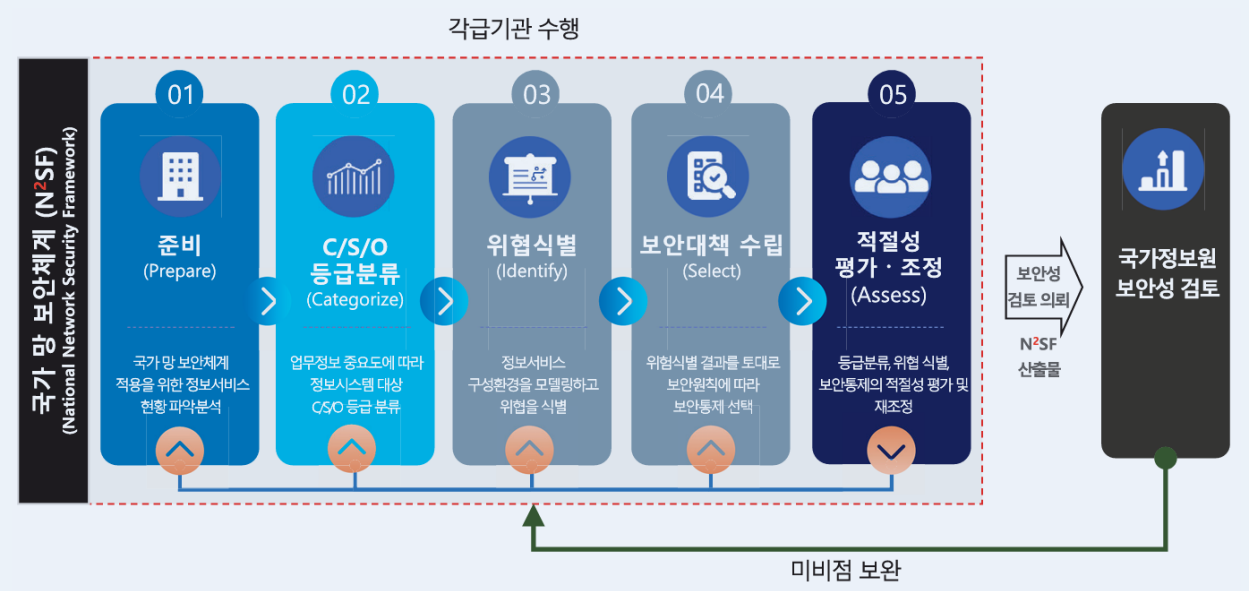
* 출처: 2024 정보보호 공시 현황 분석 보고서

그림 1. 망분리 정책 개선 추진 목표

또한, 국가 망 보안체계는 국가·공공기관의 업무 정보와 정보 시스템을 대상으로 법령 근거(정보공개법, 공공데이터법)에 따라 기밀(Classified), 민감(Sensitive), 공개(Open) 3 개 등급으로 분류하고, 등급별로 차등적인 보안통제를 적용하여 ①보안성 확보와 ②원활한 데이터 공유라는 두 가지 목적을 달성하는 정책이다.

■ 국가 망 보안체계(N²SF) 적용 절차

N²SF(국가 망 보안체계)는 총 5 단계의 절차로 구성된다. 이는 국가 및 공공기관이 정보화 사업을 계획하고 시행할 때, 해당 사업에 포함된 정보서비스에서 발생할 수 있는 보안 위협을 사전에 식별하고 위험 수준을 평가한 후, 이에 적절한 보안 대책을 수립하는 일련의 과정을 포괄한다. 각 단계에서 산출되는 결과물은 국가정보보안 기본지침에 따라 국가정보원의 보안성 검토 시 제출해야 한다.



* 출처: 2024 정보보호 공시 현황 분석 보고서

그림 2. 국가 망 보안체계 적용 절차

① 준비(Prepare) 단계에서는 기관의 업무정보 및 정보서비스 현황을 식별하고 분석하여, 이후 단계 수행에 필요한 기초적인 정보를 확보한다. 이를 바탕으로 국가 망 보안체계(N²SF) 적용 계획을 수립한다.

② C/S/O 등급 분류(Categorize) 단계에서는 기관의 업무정보 및 정보시스템의 중요도를 기준으로 C(Classified:기밀), S(Sensitive:민감), O(Open:공개) 등 3 단계로 등급을 분류한다.

③ 위협식별(Identify) 단계에서는 정보시스템을 포함한 서비스 환경 전체를 대상으로 한 모델링 기법을 활용해 위협을 식별하고, 보안 대책 적용이 필요한 대상을 선정한다.

④ 보안대책 수립(Select) 단계에서는 위협식별 결과를 기준으로 필요한 보안통제를 선택하고 구현계획을 수립한다.

⑤ 적절성 평가·조정(Assess) 단계에서는 준비 단계부터 보안 대책 수립 단계까지의 전 과정을 대상으로 적절성을 평가하고, 재조정·승인을 수행한다.

이처럼 국가 망 보안체계(N²SF)는 국가 및 공공기관이 자산(업무정보·정보시스템·정보서비스)을 분석해 위협을 식별하고 적절한 보안대책을 수립하도록 절차가 구성되어 있다.

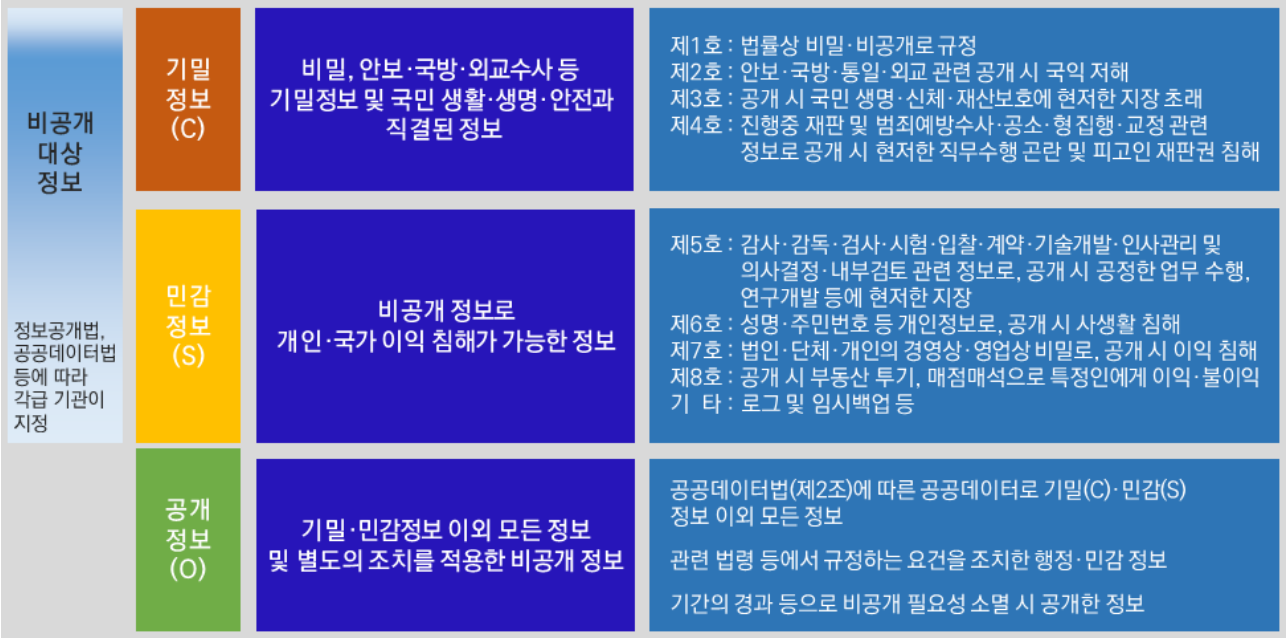
■ 국가 망 보안체계(N²SF) 등급 분류

국가 망 보안체계(N²SF)는 업무 정보와 정보시스템에 대해 각각 C/S/O 로 등급을 분류할 수 있으며, 분류의 기준은 관련법령의 근거에 따라 이루어진다.

기밀정보(Classified)는 비밀, 안보·국방·외교·수사 등의 기밀정보와 국민 생활·생명·안전과 직결된 정보로서 정보공개법 제 9 조(비공개 대상 정보)의 제 1 호부터 제 4 호까지를 포함한다.

민감정보(Sensitive)는 비공개 정보 등 개인·국가의 이익 침해가 가능한 정보로서 정보공개법 제 9 조(비공개 대상 정보)의 제 5 호부터 제 8 호까지의 정보 및 로그, 임시 백업 등의 기타 정보를 포함한다.

공개정보(Open)는 기밀정보(C) 및 민감정보(S) 이외의 모든 정보를 포함한다. 또한, 관련 법령 등에서 규정하는 요건을 조치한 비공개 정보를 포함해 기간의 경과 등 비공개 필요성이 소멸된 정보를 공개정보(O)로 분류한다.



* 출처 : 공공데이터법 및 정보공개법 참조

그림 3. 업무정보에 대한 C/S/O 분류 기준

■ 국가 망 보안체계(N²SF) 보안대책 수립

국가 망 보안체계(N²SF)는 정보서비스 모델링 단계에서 식별된 위협요소와 보안대책 적용지점에 관한 정보를 토대로 실시된다. 각 업무정보·정보시스템에 대한 보안통제 항목을 선택·조정한 후, 보안통제 구현계획을 수립해야 한다.

* 출처 : 국가 망 보안체계 보안 가이드 라인(Draft)

그림 4. 보안대책 수립 단계의 주요활동 연계도

또한, 보안대책 수립 단계의 주요 활동 및 산출물은 업무정보와 정보시스템에 대한 보안통제 항목에서 참고할 수 있다.

이처럼 N²SF의 준비단계부터 적절성 평가단계까지의 각 단계로 데이터 보안성과 활용성을 실현하는 것은 물론 공공기관의 업무 효율성을 높일 수 있게 됐다. 특히, 데이터 공유와 협업이 필요한 환경에서 효율성이 극대화될 것이다.

■ 주요국가 보안정책 동향

2014년 영국 정부가 수립한 GSCP(Government Security Classifications Policy, 정부 보안분류 정책)는 정보를 OFFICAL, SECRET, TOP SECRET 세가지 등급으로 분류한다. 각 등급은 정보 노출 시 국가안보, 경제적 이익, 국제 관계에 미칠 수 있는 피해의 심각성에 따라 결정한다.

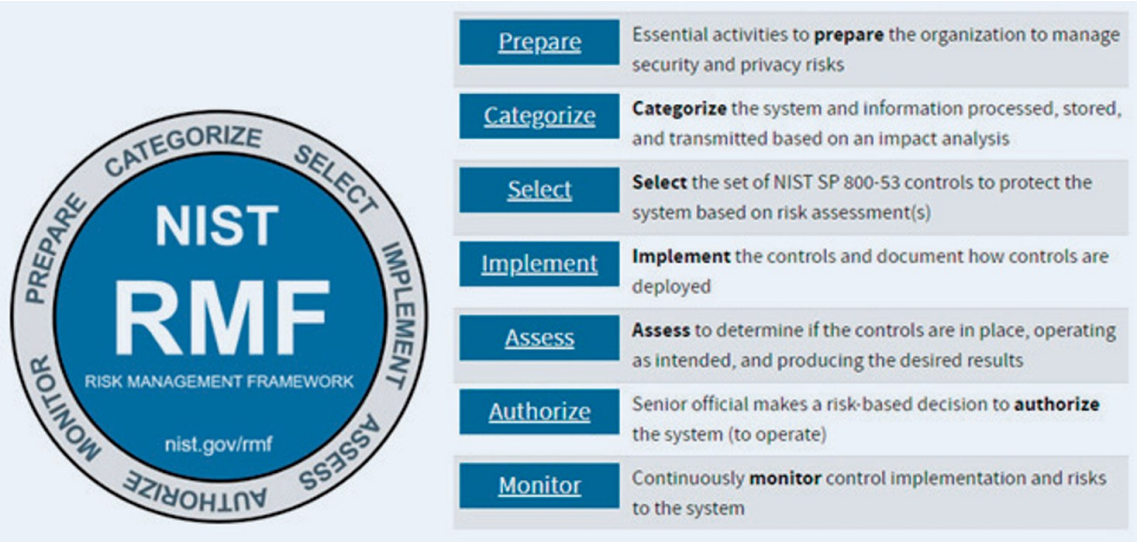
분류	정의 (정보 노출 시 파급력 수준)	보안 요구사항(개요)
TOP SECRET	국가안보와 직결되는 극도로 민감한 정보 (국가안보에 직접적이고 치명적인 피해)	적성국 국가배후 해킹조직 수준의 공격에 대한 보호
SECRET	고도의 보호가 필요한 민감한 정보 (국가의 안전과 운영에 심각한 피해)	국가배후 해킹조직, 고도화된 범죄조직 수준의 공격에 대한 보호
OFFICIAL	생산, 처리, 송수신되는 대부분의 공공정보 (피해가 없거나 미약한 피해)	내부자위협, 핵티비즘, 압력단체, 범죄조직 수준의 공격에 대한 보호

* 출처 : 영국정부 웹사이트 gov.uk

그림 5. 영국 GSCP(정부 보안분류 정책)

N²SF 역시 업무정보와 정보시스템을 기밀, 민감, 공개 등급으로 분류하는 등 관리하는 측면에서 GSCP와 매우 유사하다고 볼 수 있다.

미국의 NIST RMF는 미국 연방정보보안현대화법(FISMA)의 요구사항을 충족하는 모든 조직이 정보보안 및 개인정보보호에서의 위험을 관리하는데 사용하는 포괄적이고 유연한 위험관리 프레임워크다. NIST RMF는 7단계 절차로 구성되며 지속적인 보안강화를 위해 순화되는 개념을 담고 있다. 현재는 미국뿐만 아니라 캐나다, 호주, 뉴질랜드, 대한민국 등 많은 국가들이 이를 기반으로 한 자국의 위험관리 프레임워크를 개발하는 등 정보보안에 관한 위험관리 지침 및 표준으로 삼고 있다.



* 출처 : NIST CSRC

그림 6. NIST RMF 개요

캐나다 정부는 ITSG-33를 통해 자국의 정보보안 위험관리 프레임워크를 제공한다. ITSG-33은 NIST RMF를 바탕으로 캐나다 정부의 특정 요구사항을 반영해 개발되었다. 2009년 캐나다 정부의 보안정책에 따라 2010년 위험관리 프레임워크의 기본 틀을 개발하였고, 이후 2012년 프레임워크를 구체화한 기본 가이드라인을 발표했다.

년도	구분	관련문서 (지침, 가이드라인)	주요내용
2009	캐나다 정부 보안정책 수립	Policy on Government Security	
2010	위험관리 프레임워크	Framework for the Management of Risk	위험관리 개요 및 원칙
2012	가이드라인	ITSG-33 부록1	부서별 IT 보안 위험관리 활동
		ITSG-33 부록2	정보시스템 보안 위험관리 활동
		ITSG-33 부록3	보안통제 카탈로그
		ITSG-33 부록4	보안통제 프로파일
		ITSG-33 부록5	용어집

* 출처 : Canadian Centre for Cyber Security

그림 7. 캐나다 ITSG-33 연혁

ITSG-33은 위험관리 활동을 크게 부서별 IT보안 위험관리 계층과 정보시스템 보안 위험관리 계층으로 나누고, 두 개의 상·하위 계층을 유기적으로 연계할 수 있도록 했다.

ITSG-33의 보안통제는 NIST RMF의 보안통제를 기반으로 하기 때문에 보안통제 패밀리를 기술, 운영, 관리 등 3개의 클래스로 분류하고 있는 것이 특징이다. 각각의 클래스는 보안 매커니즘, 운영 절차, 관리 활동에 관한 보안 통제를 포함하고 있다.

호주 정부의 ISM(Information Security Manual, 정보보안 매뉴얼)은 ISMS 를 기반으로 정부 기관의 정보보안 가이드라인을 제공하며 거버넌스, 식별, 보호, 탐지, 대응의 영역으로 구성된다. 호주 사이버보안센터는 사이버보안 사고감소 전략의 일환으로 사이버공격으로부터 네트워크를 보호하기 위해 실행해야 할 8 가지 기본적인 보안조치를 명시했다. 이 8 가지 기본 보안조치는 주로 예방적인 조치를 강조하며, 비교적 간단하게 측정하고 구현할 수 있도록 구성했다.

* 출처 : 호주 사이버보안센터

그림 8. 호주 ACSC 의 Essential Eight 의 보안통제 영역

국내에서는 국가·공공기관을 대상으로 국가 망 보안체계(N²SF)를 확산하려는 움직임이 보이고 있다. 이런 흐름에 대응하기 위해 여러 솔루션 업체들이 관련된 제품을 발빠르게 내놓고 있다. 국가정보원은 지난 18년간 국가·공공기관을 대상으로 추진하였던 망분리 환경을 완화하면서 보안은 강화시켰다. 새로운 방안으로 제시되고 있는 N²SF를 통해, 신기술 도입과 데이터 활용을 촉진하며 국가 사이버 보안 방어에 기여할 것으로 보고 있다.

■ 국가 망 보안체계(N²SF) 관련 주요 가이드라인

국가 망 보안체계(N²SF)의 실질적 보안요소는 NIST-800-207(Zero Trust Architecture), NIST-800-53(Cyber Security Framework), MITRE ATT&CK V14,15를 참고해 만들어졌다. 다만, N²SF의 모태가 되는 ZTA는 국가·공공기관 보다는 기업을 고려해 만들어진 만큼 국가·공공기관이 실질적인 환경과 위협에서 대응이 어려울 것으로 판단해, 국가정보원에서는 ZTA와 ZTMM의 오버레이를 통해 자연스럽게 신기술이 적용되도록 N²SF를 만들었다. 올해 국정원에서 배포된 가이드라인과 해설서는 Draft 버전으로 금년 3분기에 정식 버전이 배포될 전망될 것으로 예상된다.

1. NIST, SP 800-207, ZTA

NIST(National Institute of Standards and Technology)는 미국 상무부 산하의 정부 기관으로, 다양한 기술 분야에서 표준과 모범 사례를 개발하는데 중요한 역할을 하고 있다. 특히 사이버 보안 분야에서 NIST는 정보 시스템 보안을 위한 권장 사항과 지침을 제공하는 800 시리즈로 전 세계에 널리 알려져 있다.

이 중 2020년 8월에 발표된 NIST SP 800-207은 제로트러스트 아키텍처(ZTA)에 대한 구체적인 가이드라인을 제공하는 문서로, 조직이 제로트러스트 모델을 도입하고 운영하도록 가이드라인을 제시한다. 해당 가이드라인은 제로트러스트 아키텍처에 대해서 정의한 최초의 표준 문서다. 이 후 발간된 가이드라인들은 NIST 800-207에서 정의한 제로트러스트 개념과 원칙을 참고하여 작성되었다.

2. NIST, SP 800-53

NIST, SP 800-53 (Cyber Security Framework)은 미국 상무부 산하 국립표준기술연구소(NIST)에서 개발한 정보보안 표준으로, 정보 시스템의 보안 및 개인정보 보호를 위한 통제(controls) 카탈로그를 제공한다.

미국 연방 정부 기관(국가안보 관련 기관 제외)을 대상으로 시행했으나, 5차 개정 이후로는 공공 및 민간 조직 모두가 사용할 수 있도록 변경돼 국제적으로 인정받는 사이버보안 프레임워크로 자리잡았다.

주요 특징은 정보시스템의 기밀성, 무결성, 가용성 보호와 위험 기반 접근법을 통해 보안 통제의 기준선을 선정하고 조직환경에 맞춰 조정할 수 있다는 점이다.

3. MITRE ATT&CK V14, 15

MITRE ATT&CK 프레임워크는 사이버 공격자의 전술(Tactics), 기술(Techniques), 절차(Procedures)를 체계화한 지식 베이스로, 보안 전문가들이 위협을 탐지하고 대응하는데 활용된다. 최신 버전인 v14와 v15에는 탐지 기능 강화와 새로운 공격 패턴이 반영됐다.

v14 주요 업데이트 내용은 ①측면 이동, ②ICS 자산 추가, ③모바일 위협 대응 확장, ④탐지 노트 개선 등이 있다.
v15 주요 업데이트 내용은 ①분석 형식 개편, ②토큰 보호 완화 조치, ③크로스 도메인 통찰력, ④클라우드 매트릭스 강화 등이 있다.

두 버전 모두 실제 공격 사례를 반영한 지속적인 진화가 특징이며, 특히 v15에는 토큰 기반 공격 방어와 크로스 도메인 분석 기능에서 기술적 도약을 했다. 각 기관의 보안을 담당하는 조직은 이러한 업데이트 내용을 활용해 공격 수명 주기 전반에 걸친 예방·탐지·대응 전략을 수립할 수 있다.

결과적으로 국가 망 보안체계(N²SF)는 선택이 아닌 필수가 돼야 한다. 다만, 아직까지 시행한 사례가 없기 때문에 국가·공공기관에서 국가 망 보안체계(N²SF) 도입에 대해 의문이 많은 것은 사실이다. 국가정보원은 국가·공공기관이 국가 망 보안체계(N²SF)를 보다 쉽게 도입하고 운영할 수 있도록 필요한 ①가이드라인과 ②통제항목, ③정보서비스 해설서를 제공하고 있다. 다음 장에서는 국가 망 보안체계(N²SF) 주요 통제 항목에 대해서 알아보도록 하겠다.

■ 국가 망 보안체계(N²SF) 통제 항목

국가 망 보안체계(N²SF)는 업무 정보, 정보시스템을 대상으로 정보공개법과 공공데이터법에 따라 등급을 분류하여 위협을 도출하고, 통제 항목을 통해 보호 대책을 수립한다. 또한, 국가 망 보안체계(N²SF)에서 제공되는 통제 항목은 6개분야 약 180여개 항목으로 구성되어 있다. 각 기관은 이 통제 항목을 선별적으로 적용하여 유연성 있게 보호 대책을 수립하면 된다.

따라서 통제 항목 별로 요구되는 보안 조치와 이를 지원하는 주요 시스템(솔루션)은 N²SF 를 성공적으로 구현하기 위한 핵심 요소가 된다. 아래 주요 통제 항목을 간략하게 설명하고자 한다.

1. 권한

시스템 및 정보 접근 권한을 최소화하고, 철저한 신원 검증을 통해 인증된 사용자만 접근할 수 있도록 한다. 최소 권한 원칙을 적용해 불필요한 접근을 차단한다.

1-1. 최소권한(Least Privilege, LP)

최소권한은 사용자나 프로세스가 특정 업무를 수행하는 데 필요한 최소한의 권한만을 부여하는 보안 원칙으로 내부 및 외부 위협으로부터 보호하고, 내부 정보로의 불필요한 접근을 방지하기 위한 통제항목이다. 제한하는 방식으로 운영되는 이 권한의 식별자 필러에 연관된 주요 시스템은 아래와 같다.

1-2. 신원검증(Identity Verification, IV)

신원증명은 시스템 접근을 위한 자격 증명을 설정할 목적으로 대상 사용자의 신원 정보를 수집, 검증 및 확인하기 위한 통제항목이다.

1-3. 식별자관리(Identifier Management, IM)

식별자관리는 기관의 IT자산 및 인적 자원을 식별할 수 있는 고유한 식별자를 생성, 관리하여 접근 통제를 강화하고 인증 프로세스를 지원하기 위한 통제항목이다.

1-4. 계정관리(Account Management, AC)

계정관리는 시스템 내에서 사용자와 관련된 계정을 생성, 관리, 모니터링, 비활성화 및 삭제 기능을 수행하여 불필요한 계정 사용을 방지하고, 비 인가된 사용자 접근을 통제하여 보안성을 유지하기 위한 통제항목이다.

2. 인증

다중요소 인증(MFA)과 외부 인증수단 연계 등 다양한 인증 방식을 도입해 보안성과 편의성을 강화한다. 이를 통해 비인가자의 접근을 효과적으로 방지한다.

2-1. 다중요소 인증(Mutl-Factor Authentication, MA)

다중요소 인증은 기관 내부 사용자의 정보시스템 등에 접근 시 사용자 인증을 위해 두 개 이상의 인증 요소를 사용하여 보안성을 강화하기 위한 통제항목이다.

2-2. 외부 연계(External Integration, EI)

외부 연계 인증은 외부 기관 사용자에 대한 접근 시스템을 식별하고 시스템에 대한 접근 권한을 부여하기 위한 통제항목이다.

2-3. 식별(Identification, ID)

식별은 기관 정보시스템 및 시스템 구성장비에 대한 비인가 단말의 접속을 차단하기 위한 통제항목이다.

2-4. 인증보호(Authentication Protection, AU)

인증보호는 계정 인증 보안 강화 및 불법적인 계정 로그인 시도 방지, 생체 인증 공격 방지, 대체 보안수단 강구 등 인증 과정에서의 보안성 강화 및 다양한 위협에 대응하기 위한 통제항목이다.

2-5. 인증정책(Authentication Policy, AP)

인증정책은 기관 사용자 증명, 인증 프로파일, 그룹계정 사용자 인증 등 기관 내 사용자의 신원을 지속적으로 확인하고 보호하기 위한 통제항목이다.

2-6. 인증수단(Authentication Method, AM)

인증수단은 시스템 접근에 사용되는 인증의 생성, 변경, 보호, 갱신 등을 관리하기 위한 통제항목이다.

2-7. 로그인 (Login, LI)

로그인은 인증 피드백 보호, 로그인 시도 제한, 시스템 사용 알림, 인증 결과 처리 등 사용자 계정 인증 과정에서의 보안 위협 방지를 위한 통제항목이다.

3. 분리 및 격리

하드웨어와 소프트웨어를 활용한 물리적·논리적망분리 및 접근통제 기술을 적용한다. 필요 시 외부 연결을 제한하여 보안을 유지한다

3-1. 분리(Segregation, SG)

정보서비스 및 업무정보가 보안 등급에 따라 서로 다른 보안 도메인으로 구분되도록 하드웨어, 소프트웨어, 운영체제 분리 또는 인프라, 사용자 기능 분리를 통해 각 영역에 대한 보안을 강화하기 위한 통제항목이다.

3-2. 격리(Isolation, IS)

정보시스템은 각 프로세스를 독립된 공간에서 실행하여 상호 간섭을 차단하고, 일반 사용자에게 관리 기능 및 인터페이스의 노출을 제한하며, 애플리케이션 접근을 통제하여 데이터의 무단 접근을 방지하기 위한 통제항목이다.

4. 통제

데이터 전송 방식 및 유형을 통제해 중요 정보의 유출을 방지한다. 데이터 이동 경로와 전송 방법을 엄격히 관리한다.

4-1. 정보흐름(Information Flow, IF)

정보시스템 간에 정보가 이동할 수 있는 경로에 대한 관리 제어를 통해 비정상 동작, 외부 공격, 암호화된 정보의 흐름, 일방향 데이터 전송 및 차단, 메타데이터 활용, 정보전송 방식 제한, 보안 및 프라이버시 규칙 등을 통제하여 민감한 정보의 유출을 방지하고 안전한 정보흐름을 보장하기 위한 통제항목이다.

4-2. 외부경계(External Boundary, EX)

정보시스템 경계에서는 외부 네트워크와의 연결 접점을 제한하고, 승인된 통신만 허용할 수 있도록 경계 보호 장치를 활용하여 트래픽을 필터링하며, 이를 통해 외부로부터의 무단 접근을 차단하고 내부 정보시스템 구성요소 및 데이터 유출 방지, 개인 식별 정보에 대한 보호조치를 위한 통제항목이다.

4-3. 원격접속(Remote Access, RA)

원격접속 환경에서의 기밀성과 무결성 강화를 위한 접속 통제 및 통신구간 암호화, 관리자·사용자의 접속 위치 및 권한 사용에 대한, 무단 정보 유출 방지 및 일정 시간 이후 세션 자동 종료와 같은 안전한 원격접속을 위한 통제항목이다.

4-4. 세션(Session, SN)

세션 관리 및 보안은 각 세션의 고유 식별자를 할당하여 비정상 종료나 비활성 상태 시 즉시 종료하고 사용자의 요청 또는 조건에 따라 동시 세션 수 제한 자동 세션 종료, 알람 메시지 제공 등 세션의 보안통제를 통해 비인가 사용자 무단 접근과 정보 유출을 방지하기 위한 통제항목이다.

4-5. 무선망 접속(Wireless Network Access, WA)

무선 통신망 보안은 사용자 및 기기 인증, 통신 구간 암호화, 송수신 출력 제어, 승인되지 않은 무선망 차단, 그리고 외부인 전용 무선망 분리 및 무선망 관리 기능 보호를 통해 무선망의 기밀성과 무결성을 유지하는 통제항목이다.

4-6. 블루투스 연결(Bluetooth Connection, BC)

정보시스템에서 블루투스 사용 시 키보드, 마우스와 같이 사용자 입력을 위한 HID(Human Interface Device) 프로파일과 데이터 전송을 위한 FTP(File Transfer Profile) 기반의 통신을 구분하여 정보유출 위협이 발생할 수 있는 데이터 통신을 제한하는 통제항목이다.

5. 데이터

저장 및 전송 과정에서 암호화 기술과 키 관리 시스템을 적용해 데이터 보호 수준을 향상시킨다. 데이터의 안전한 저장과 처리를 보장한다.

5-1. 암호 키 관리(Encrytion Key Management, EK)

암호 키 관리는 암호 키의 생성, 배포, 저장, 사용 및 폐기 등 키의 전체 수명 주기를 안전하게 관리 하기 위한 프로세스로 키의 무단 접근과 오용을 방지하고, 데이터 기밀성과 무결성을 유지하기 위한 통제항목이다.

5-2. 암호기술 적용(Encrytion Technology Application, EA)

암호기술을 사용할 경우 보안등급과 용도에 따라 국가정보원장이 인증한 검증필 암호모듈 및 국가용 암호자재·장비를 사용하거나 특수목적용 암호자재·장비의 선택적 사용에 대한 통제항목이다.

5-3. 데이터 전송(Data Transmission, DT)

데이터 전송은 시스템 간 데이터 및 정보를 안전하게 전송하기 위한 보안 요구사항을 명확히 하고, 이를 관리하는 절차를 포함한다. 전송 중인 정보가 허가되지 않은 사람이나 시스템에 의해 읽히거나 변경, 손상되지 않도록 전송 기밀성과 전송 무결성을 보호하기 위한 통제항목이다.

5-4. 데이터 사용(Data Usage, DU)

데이터 사용은 검색, 연산 또는 기타 데이터 처리 활동과 같이 데이터가 정보시스템 내부에서 사용되는 동안에도 데이터에 대한 보호조치를 구현하는 통제항목이다.

6. 정보자산

모바일 기기, 하드웨어, 정보시스템 등 정보자산에 대한 보호 방안을 마련하고, 최신 기술을 반영해 지속적으로 관리한다.

6-1. 모바일 단말(Mobile Device, MD)

모바일 단말은 시스템에서 허용 및 금지할 모바일 코드와 모바일 코드 기술을 정의하고 허용할 모바일 코드와 모바일 코드 기술의 사용 제한 사항과 구현 가이드를 수립하여 내부 혹은 외부에서 모바일 단말의 사용인가, 모니터링을 위한 통제항목이다.

6-2. 하드웨어(Device, DV)

하드웨어 보안 항목은 정보시스템과 하드웨어의 무결성을 유지하기 위해 펌웨어 및 하드웨어 구성 요소 검증, 그리고 실행 환경의 무결성 보장을 위한 통제항목이다.

6-3. 정보시스템 구성요소(Information System Component, IN)

정보시스템의 구성요소는 중앙화된 저장소를 통해 목록화하고, 설치·제거·업데이트 시 이를 정기적으로 갱신, 자동화된 매커니즘으로 최신성, 완전성, 정확성을 유지하여 불필요한 기능, 포트, 프로토콜, 소프트웨어를 비활성화 또는 제거하기 위한 통제항목이다.

위에서 간략하게 살펴본 봐와 같이 국가 망 보안체계(N²SF)의 보안통제 항목은 6개 영역의 180여개 항목으로 구성이 되어 있고, 현재 공식적으로 배포된 자료는 Draft버전으로 지속적으로 최신 기술과 기관·기업들의 목소리를 반영할 예정이다.

국가·공공기관에서 국가 망 보안체계(N²SF) 환경을 구현하기 위해서는 권한, 인증, 분리 및 격리, 통제, 데이터, 정보자산 등 통제항목에 대해 다양한 보안대책 작업들이 필요하다. 이러한 보안통제 항목을 업무정보와 정보시스템에 적용시켜 실시간으로 위협을 탐지하며, 동적 정책을 생성함으로써 조직의 보안 운영을 효율화하고 인적 자원의 부담과 보안 사고에 대한 문제를 완화시킬 수 있다.

국가 망 보안체계(N²SF)가 제공하는 통제항목을 통해 국가·공공기관은 업무 운영 환경을 효과적으로 구현할 수 있도록 해야 한다. 국가 망 보안체계(N²SF)의 성공적인 구현은 조직의 보안 전략과 기술적 역량의 조화에 있다. 조직은 해당하는 통제 항목을 적용하면 더욱 강력하고 유연한 보안체계를 마련할 수 있을 것이다.

■ 시사점

국가 망 보안체계(N²SF)는 기존의 획일적인 망분리 정책이 가진 한계를 극복하고, 보안성과 데이터 활용성을 동시에 고려한 새로운 보안 패러다임이다. 디지털 전환의 가속화와 함께 AI, 클라우드 등 첨단 기술이 빠르게 확산되는 현시점에서, 공공기관과 국가 차원의 정보보호는 단순한 방어 중심 접근만으로는 한계에 직면하고 있다. 안전한 데이터 활용과 효율적인 업무 환경을 동시에 충족해야 하는 시대적 요구에 따라, 국가 망 보안체계(N²SF)는 망의 등급별 분류와 차등화된 보안 통제를 기반으로 한 혁신적인 방식을 제시하고 있다.

국가 망 보안체계(N²SF)의 도입은 다음과 같은 시사점을 지닌다.

첫째, 보안과 업무 효율성 간의 균형이 가능하다. 망을 기밀(Classified), 민감(Sensitive), 공개(Open) 등급으로 세분화하고, 각 등급에 적합한 보안 대책을 적용함으로써 불필요한 업무 지연이나 비효율을 최소화하는 동시에, 국가 핵심 정보의 안정성을 확보할 수 있다.

둘째, 신기술 도입에 대한 유연성이 향상된다. AI, 빅데이터, 클라우드 등 혁신 기술을 보다 적극적으로 활용할 수 있는 기반이 마련되어, 공공서비스의 품질 제고 및 미래 경쟁력 강화에 기여할 수 있다.

셋째, 보안 위협의 고도화·다변화에 대응하는 체계적인 관리가 가능해진다. 각 망의 특성과 위협 수준을 고려해 맞춤형 보안 정책을 수립함으로써, 사이버 공격에 대한 선제적 대응 역량이 강화된다.

향후 국가 망 보안체계(N²SF)는 국가 및 공공기관뿐 아니라 민간 부문으로도 확산되며, 글로벌 사이버 보안 표준으로 자리매김할 가능성이 높다. 이를 위해서는 제도적 지원뿐 아니라 실무자 교육, 기술 표준화, 정책의 지속적 개선이 병행되어야 한다. 국가 망 보안체계(N²SF)는 단순한 보안 정책을 넘어, 디지털 시대 국가 경쟁력을 좌우하는 핵심 인프라로서 그 중요성이 더욱 커질 것으로 기대된다.

■ 참고문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] NIST SP 800-253, “Cyber Security Framework”, 2020.08

[3] MITRE ATT&CK v14, v15, 2023.10

[4] 국가 망 보안체계 보안 가이드라인(Draft), 2025.01

[5] 국가 망 보안체계 보안 가이드라인(Draft) 부록1, 2025.01

Keep up with Ransomware

카르텔 모델을 도입한 DragonForce 랜섬웨어

■ 개요

2025 년 4 월 랜섬웨어 피해 사례 수는 지난 3 월(773 건)에 비해 약 29% 감소한 550 건을 기록했다. 4 월에 피해 사례가 감소한 이유는 지난 3 월까지 매달 70 건 내외의 피해자를 발생시키던 RansomHub 그룹이 더 이상 활동하지 않는 것에 영향을 받은 것으로 보인다. 신규 그룹도 많이 등장했지만, 기존에 많은 활동을 보이던 그룹들이 주춤하고 있는 것이 가장 큰 요인으로 작용했다.

4 월에도 랜섬웨어 그룹이 해킹 당한 사례가 확인됐다. 20 년부터 활동하기 시작한 Everest 그룹은 4 월 초 “Don’t do crime CRIME IS BAD xoxo from Prague”라는 문구와 함께 다크웹 유출 사이트가 변조되어 비활성화됐다. 법 집행 기관에 의해 인프라를 압수당했을 때, 설정되는 페이지와는 상이해 사용자가 해킹 후 변조했을 것으로 예상된다. 4 월 말 Everest 그룹의 다크웹 페이지는 복구됐으며 다시 피해자를 게시하며 활동 재개를 시작했다.

이러한 해킹 사건은 4.0 버전을 출시하며 부활을 노리던 LockBit 그룹에게도 발생했으며, 그로 인해 내부 데이터가 유출된 것으로 확인됐다. 5 월 초, LockBit 의 다크웹 유출 사이트가 Everest 그룹 해킹 건과 동일한 문구로 함께 변조됐다. LockBit 의 경우 다크웹 유출 사이트 변조뿐만 아니라 관리자 패널도 해킹으로 인해 내부 데이터베이스 파일 일부가 유출됐다. 유출된 데이터베이스에는 가상화폐 지갑 주소, 랜섬웨어 버전 별 사용된 구성 정보, 제휴사 계정 정보, 채팅 내역 등이 포함되어 있었다. 유출된 정보에는 복호화에 사용되는 개인키가 포함되어 있진 않았지만, 이번 해킹 사태로 인해 평판이 훼손되어 운영에 큰 영향을 받을 것으로 보인다.

3 월까지 왕성한 활동을 보이던 RansomHub 그룹이 3 월 31 일에 돌연 다크웹 유출 사이트를 비활성화 하며 활동을 중단했거나 중단했다. 이전부터 자주 다크웹 유출 사이트 접속에 문제가 있었지만, 이번에는 계열사들도 인프라 접근에 문제가 생겨 다른 그룹의 플랫폼에서 피해자와 협상을 진행하는 등 운영에 차질이 발생했다. 이에 더불어 4 월에는 DragonForce 그룹이 RansomHub 의 인프라를 운영하게 되었다고 주장하며 혼란이 가중됐다. 이에 따라 RansomHub 가 리브랜딩을 위해 활동을 중단했거나 DragonForce 가 RansomHub 를 인수했다는 등 다양한 의견이 제시되는 만큼 추후 움직임을 지켜볼 필요가 있다.

Play 랜섬웨어 그룹이 제로데이 취약점을 활용해 공격을 시도한 정황이 확인됐다. 이들은 공격 정에서 Windows 권한 상승 취약점인 CVE-2025-29824 를 악용해 공격에 필요한 권한을 확보했다. 비록 랜섬웨어를 배포하진 않았으나, 정보 탈취 도구 Grixba 를 이용해 정보를 수집한 정황이 발견됐다.

DragonForce 그룹이 새로운 브랜드 모델을 선보이며 확장 전략에 박차를 가하고 있다. 이들은 “카르텔”이라는 조직명을 사용하며 제휴사들에게 자체 브랜드를 런칭할 수 있는 권한을 부여하기 시작했다. DragonForce 는 악성 도구, 관리 패널 등 인프라를 제공하고, 계열사는 자체 랜섬웨어를 사용하는 독립적인 브랜드로 활동할 수 있는 구조다. 기존 랜섬웨어 서비스는 공격에 필요한 각종 도구 지원을 통해 기술력이 부족한 해커들이 쉽게 접근할 수 있었지만, 이번 서비스 모델은 특정 도구 사용을 강제하지 않으면서 독립적인 브랜드를 운영할 수 있기 때문에 숙련된 공격자들까지 유입되는 유연한 구조를 갖추고 있다.

■ 랜섬웨어 뉴스

LockBit 그룹, 내부 데이터베이스 유출

- 유출된 정보에 따르면 4월 말 해킹된 것으로 추정
- “Don’t do crime CRIME IS BAD xoxo from Prague” 문구와 함께 내부 데이터베이스 일부 유출
- Everest 그룹의 해킹과 동일한 자의 소행으로 추정

RansomHub 비활성화

- 3월 31부터 다크웹 유출 사이트 접속 불가
- 계열사도 접속 불가능한 상태로, 다른 그룹으로 다수 이탈
- 4월 말 인프라가 복구 됐지만, “RansomHub R.I.P. (03.03.2025)”라는 문구만 남겨두어 활동 종료 추정

DragonForce 그룹, 신규 서비스 모델 출시

- 카르텔이라고 불리는 신규 모델 출시
- 제휴사에 인프라를 제공하며, 제휴사는 독립적인 브랜드를 가질 수 있는 형태
- 4월부터 RansomBay라는 그룹이 해당 서비스를 이용하기 시작

Everest 그룹, DLS 해킹

- 4월 초 DLS가 변조되며 비활성화
- LockBit의 변조 페이지와 동일한 문구로 변조되어, 동일 인물의 소행으로 추정

DragonForce 그룹, RansomHub 인프라 관리 주장

- 4월부터 RansomHub의 인프라를 관리하게 되었다고 러시아 해킹 포럼에서 주장
- RansomHub를 인수했거나, 광고 수단으로 활용했을 가능성 존재


신규 Devman 그룹, RaaS 출시 예고
4월에 등장한 신규 그룹으로, 다른 그룹의 랜섬웨어를 사용하고 자신들의 공격 전략을 일부 공개
5월부터는 Devman 그룹 자체 랜섬웨어도 공격에 사용
6월 말에는 자체적인 RaaS 플랫폼을 공개할 예정
RaLord 그룹, Nova로 리브랜드
3월 등장한 RaLord 그룹, 4월에 Nova로 리브랜딩 후 활동 재개
Rust 기반의 랜섬웨어 사용
Play 그룹, Windows 권한 상승 취약점 (CVE-2025-29824) 악용
취약한 Cisco ASA를 통해 침투 후 권한 상승 취약점 악용
랜섬웨어를 배포하진 않았으나, 인포스틸러를 활용해 정보를 수집한 정황 발견

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

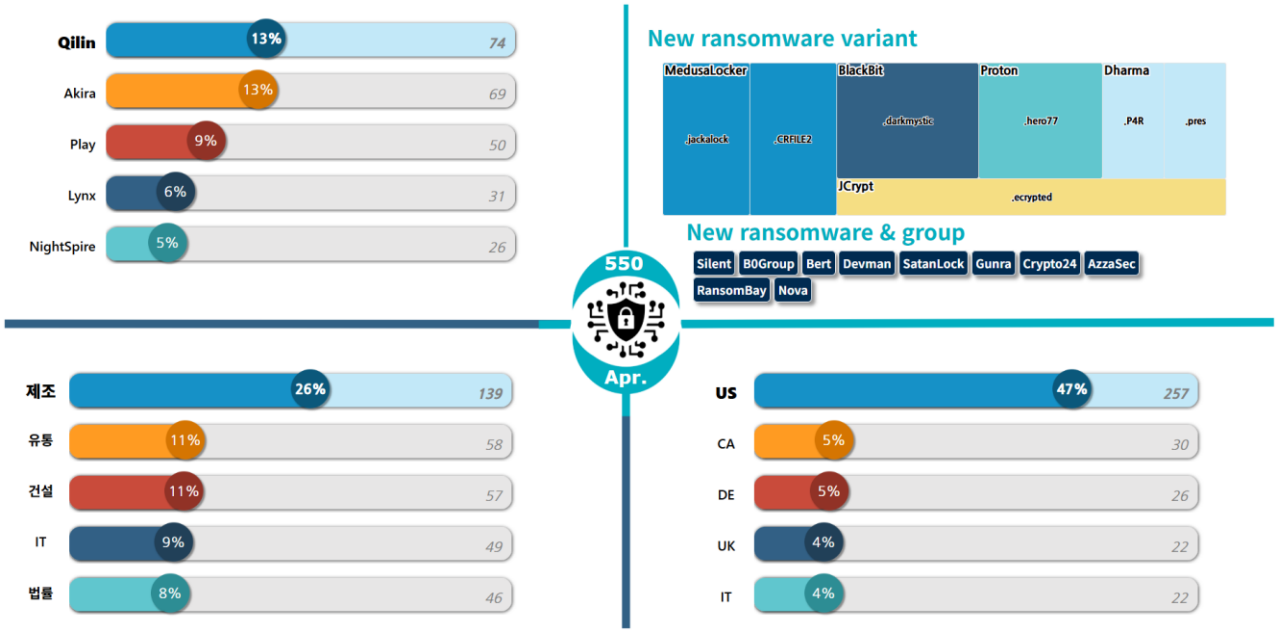


그림 2. 2025 년 4 월 랜섬웨어 위협 현황

새로운 위협

4 월에는 기존 랜섬웨어 그룹의 업데이트 소식이 있었다. 총 5 개의 신규 랜섬웨어 그룹이 확인됐다. 그 중 4 개의 그룹 Silent, BERT, Devman, Gunra 그룹은 4 월에 신규로 등장해 5 월까지 정상적으로 활동하고 있으며, SatanLock 그룹은 5 월까지 지속적으로 활동하고 있으나 다크웹 유출 사이트가 빈번하게 비활성화 되는 모습을 보이고 있다.

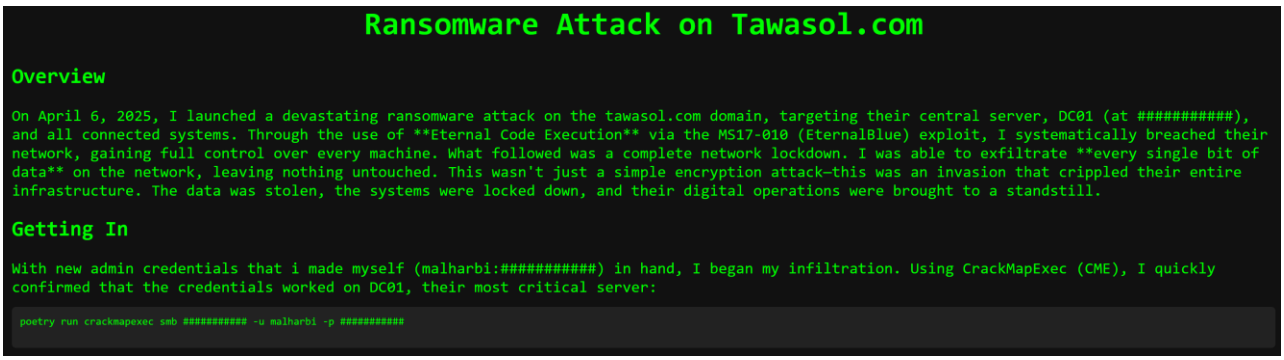


그림 3. Devman 랜섬웨어 공격 방식 설명

신규 Devman 그룹은 활동 초기 자신들의 공격 방식을 순차적으로 정리해서 다크웹 유출 사이트에 업로드하는 독특한 모습을 보여줬다. 활동 초기에는 공격에 자체적인 랜섬웨어를 사용하는 것이 아닌, 다른 그룹의 랜섬웨어를 사용한 것이 확인됐다. 그로 인해서 다른 그룹과 동일한 피해자를 다크웹 유출 사이트에 업로드 하는 경우도 발견됐다. 5 월 초부터는 자체 랜섬웨어로 공격하기 시작했으며, 6 월 20 일에 자체적인 RaaS[1] 플랫폼을 출시할 것이라고 예고한 바 있다.

신규 그룹 외에도 리브랜딩을 한 그룹도 확인됐다. Nova 그룹은 25 년 3 월에 RaLord 라는 그룹으로 활동을 시작했으며 4 월에는 Nova 라는 이름으로 리브랜딩했다. 또한 Azzasec 그룹은 작년 6 월에 자체 랜섬웨어 기반의 RaaS 를 공개한적 있는 그룹으로, DoubleFace 로 리브랜딩 후 다시 Azzasec 으로 변경한 뒤 활동을 이어가고 있다.

[1] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 쉽게 랜섬웨어를 만들고 공격할 수 있도록 하는 비즈니스 모델

Top5 랜섬웨어

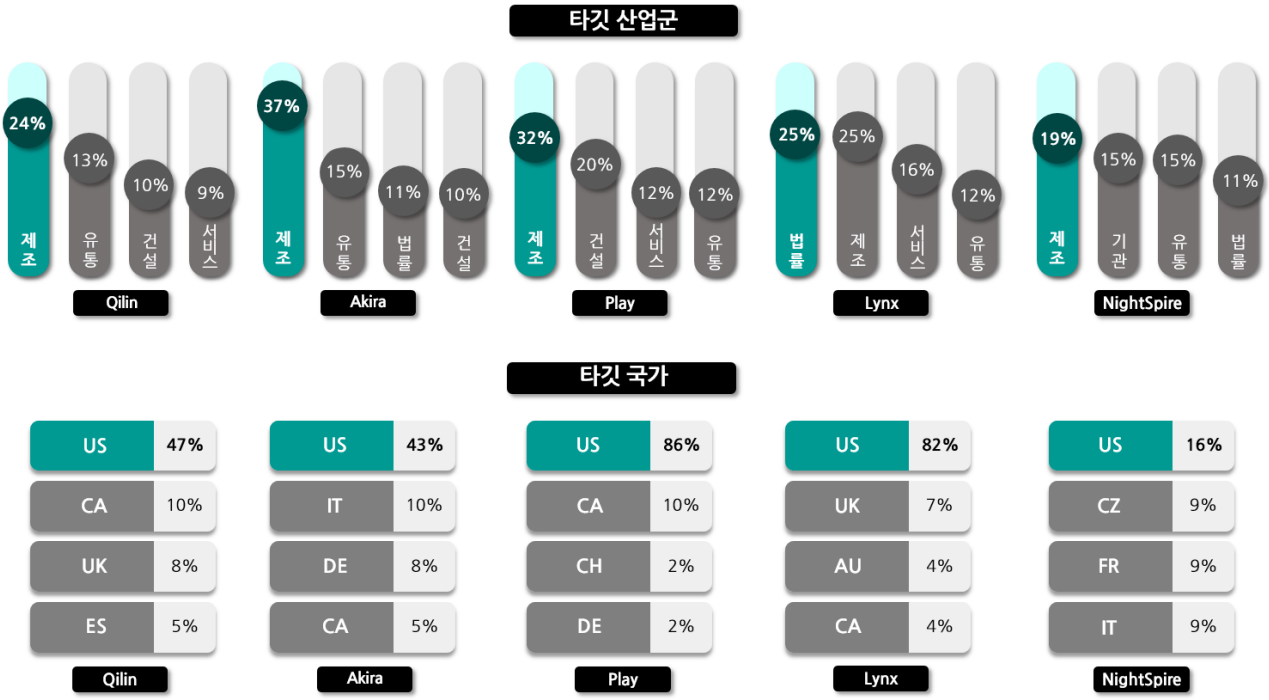


그림 4. 산업/국가별 주요 랜섬웨어 공격 현황

4 월에 미국의 회계 법인 Richmond CPA 를 공격해 약 183GB 분량의 계약서, 세금 계산서, 급여 명세서 등의 내부 자료를 유출한 Qilin 그룹은 4 월에만 총 74 건의 피해자를 게시했다. 4 월 초 RansomHub 서비스가 중단되자 다수의 제휴 공격자들이 Qilin 진영에 합류해 공격이 급증한 것으로 사료된다. 북한 연계 위협 그룹 Moonstone Sleet 와의 연관성도 제기되고 있으며, 특히 Moonstone Sleet 이 과거 사용했던 FakePenny 랜섬웨어와 유사한 배포 방식이 확인되고 있어 주의가 필요하다.

Akira 그룹은 4 월에 미국의 제조 및 조립 서비스 업체 TrussWorks International 을 공격해 직원 및 고객 연락처, 전화번호, 주소와 같은 개인정보는 물론 재무 기록, 비밀 유지 계약 등 내부 문서 13GB 를 유출했다. 또 다른 사례로, 부동산 서비스 업체인 Santa Cruz Properties 를 공격해 재무 문서, 계약서가 포함된 15GB 데이터를 유출한 것으로 알려졌다.

Play 그룹은 Windows CLFS 권한상승 취약점(CVE-2025-29824)을 악용해 침투하려는 시도가 포착되었다. 공용 Cisco ASA[1] 장비 취약점을 공격한 뒤 자체 제작 정보탈취 악성코드 Grixba 를 심어 내부 네트워크 정보를 수집하고 흔적을 삭제했던 시도 정황이 확인됐다. 랜섬웨어를 배포하진 않았지만, 해당 취약점이 패치되기 전에 Play 그룹뿐만 아니라 다른 그룹도 해당 취약점을 악용했을 가능성이 있기 때문에 꾸준히 지켜볼 필요가 있다.

[1] Cisco ASA: Cisco 의 네트워크 보안 장비로, 방화벽, 침입 탐지/방지, VPN 등의 보안 기능을 제공

Lynx 그룹은 4 월에 미국의 농업 컨설팅 기업인 Southern Ag LLC 를 공격해 내부 운영 시스템을 공격해 재무 문서, 고객 데이터, 기밀 문서 등 50GB 의 데이터를 유출했다. 또 다른 피해 사례로는 영국의 법률 서비스 업체 Vicaraga Court Solicitors 로, 이 회사의 메일과 일부 계약서가 다크웹 유출 사이트에 게시됐다. 해당 그룹은 과거 INC 랜섬웨어의 소스코드를 구매해 활용하고 있으며, 최근 공격에서는 Lumma 인포스틸러를 함께 사용하는 등 정보 탈취 도구와 결합된 형태로 진화하고 있다.

NightSpire 는 4 월 일본의 세라믹 제조업체 Nippon Ceramic 을 공격해 45GB 의 기술 설계 문서 및 생산 관련 파일을 탈취했다고 밝혔다. 탈취된 데이터는 다크웹 유출 플랫폼에 공개됐으며, 4 월 말에는 싱가포르의 금융 서비스 기업인 Melco Capital 을 공격해 약 1.8TB 의 재무 정보 및 내부 문서를 유출했다. NightSpire 는 2025 년 3 월부터 활동을 시작한 신규 그룹으로, 최근 몇 주 사이 빠르게 피해 범위를 확장하고 있다.

■ 랜섬웨어 집중 포커스

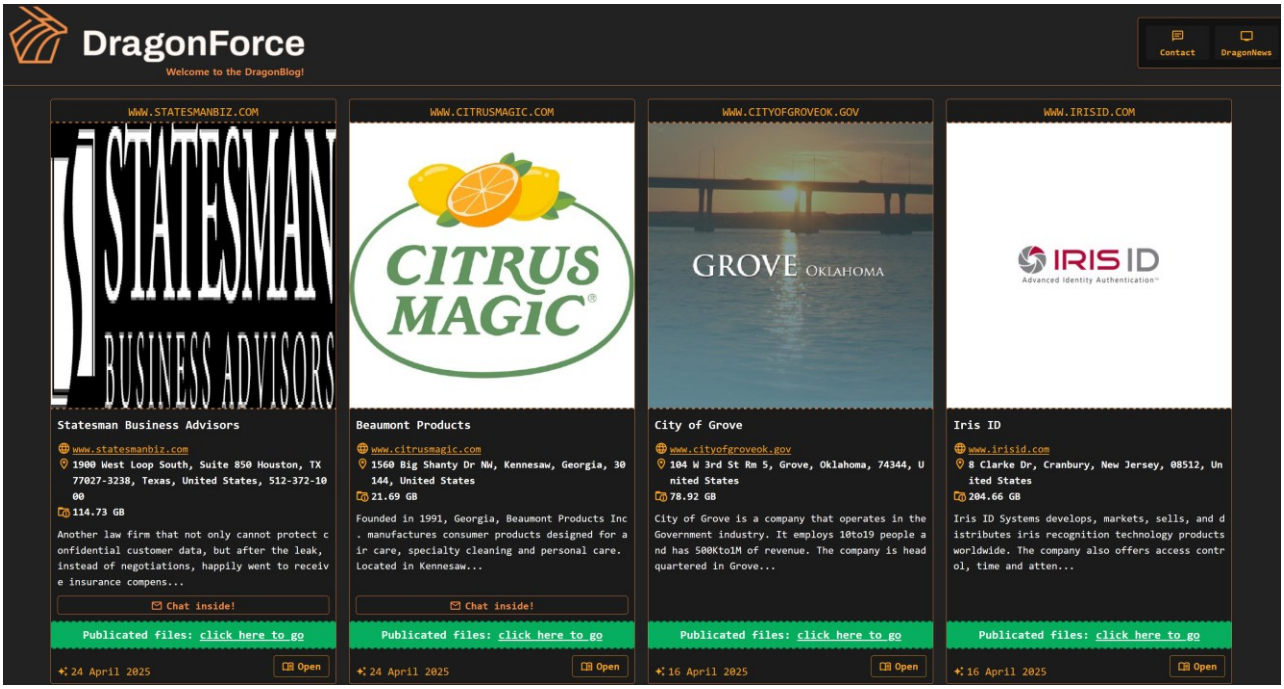


그림 5. DragonForce 다크웹 유출 사이트

DragonForce 그룹은 23 년 12 월부터 활동을 시작해 매월 10 건 이내의 피해자를 꾸준히 게시하는 그룹이다. 24 년 6 월에는 러시아 다크웹 해킹 포럼인 RAMP 포럼에 파트너 모집 글을 업로드했으며, 지금까지도 해당 글을 업데이트하며 랜섬웨어의 버전 업데이트 내용이나 새로운 서비스를 소개하고 있다.

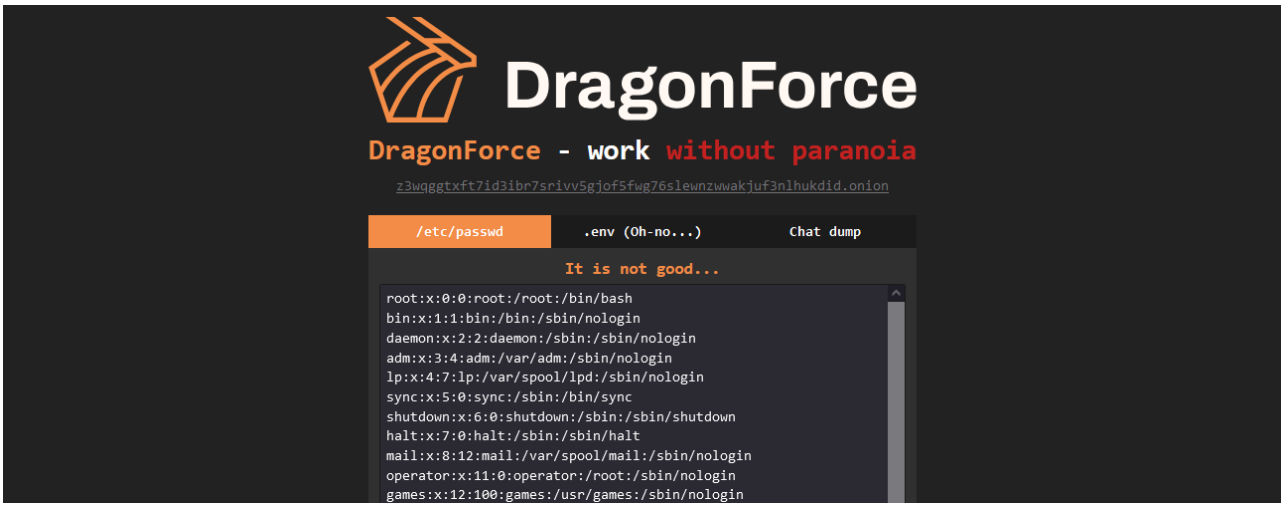


그림 6. 해킹된 BlackLock 유출 사이트

2025 년 3 월, DragonForce 는 경쟁 그룹의 인프라 보안 취약점을 활용해 BlackLock 과 Mamona R.I.P 의 다크웹 유출 사이트를 해킹했다. 당시 BlackLock 의 운영 환경은 보안 구성이 허술한 것으로 알려져 있었으며, 여러 포럼 유저는 물론 DragonForce 가 이를 노려 해킹을 시도했다고 보고 있다. 해킹 이후 Mamona 의 유출 사이트는 완전히 비활성화되었고, BlackLock 의 사이트는 변조되어 DragonForce 를 홍보하는 메시지와 로고가 게시되었다.

그림 7. RansomHub DLS 호스팅 설정

4 월에도 DragonForce 는 타 랜섬웨어 그룹을 통해 자신들을 홍보하려는 정황이 포착됐다. 당시 RansomHub 가 DragonForce 측에 인프라 운영을 위임하기로 결정했다며 관련 설정 페이지가 공개했으며, 이는 양측이 실제 협력 관계를 맺고 인프라를 재정비하고 있는 것으로 해석되었다. 이러한 해석에는 같은 시기 RansomHub 의 다크웹 유출 사이트가 비활성화된 사실이 영향을 미쳤다. 그러나 이후 복구된 RansomHub 유출 페이지에는 "RansomHub R.I.P. (03.03.2025)"라는 문구만 남겨졌고, 'hexcat'이라는 유저가 "RansomHub 는 DragonForce 에 합병됐다"고 주장하면서, 단순한 협력이 아닌 DragonForce 의 인수였다는 가능성도 제기됐다.

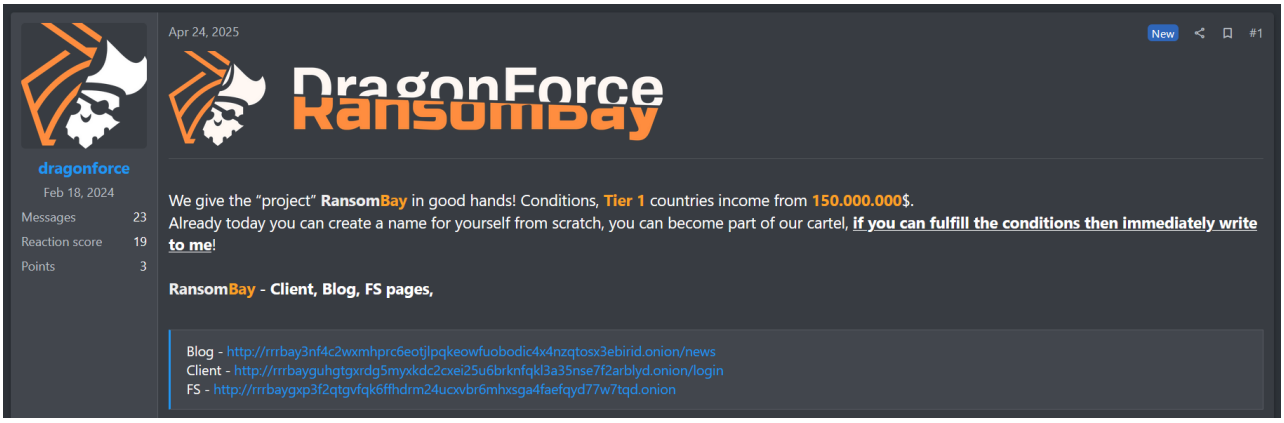
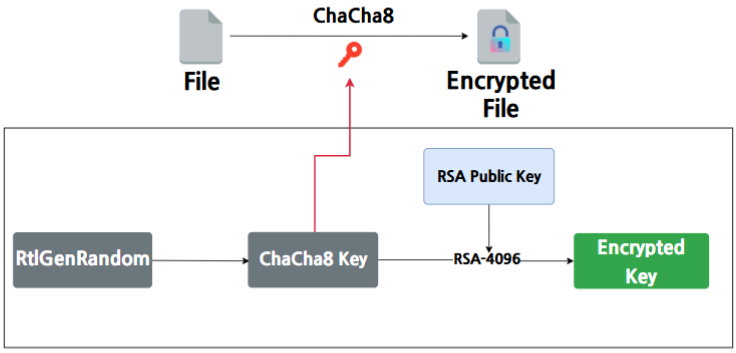


그림 8. RansomBay 홍보글

DragonForce 랜섬웨어 그룹은 활동 영역을 넓히기 위해 자신을 “카르텔”이라고 지칭하기 시작했다. 자신의 계열사는 동일한 인프라를 사용하지만 브랜드로 활동할 수 있다고 밝혔으며 새로운 RansomBay 라는 브랜드가 4 월부터 활동하기 시작했다. 최근 경쟁 그룹의 인프라를 해킹해 자사 홍보 수단으로 악용하거나 새로운 사업 구조를 공개하는 등, 단순 금전 갈취를 넘는 전략적 활동을 보이며 사이버 위협 생태계 내에서 빠르게 입지를 넓히고 있다. 본 보고서는 이러한 배경을 토대로 다가오는 위협에 대비하기 위한 DragonForce 랜섬웨어의 분석 내용을 공유하고자 한다.

암호화 키

ChaCha8 알고리즘으로 암호화를 하고, 해당 키를 RSA-4096으로 보호

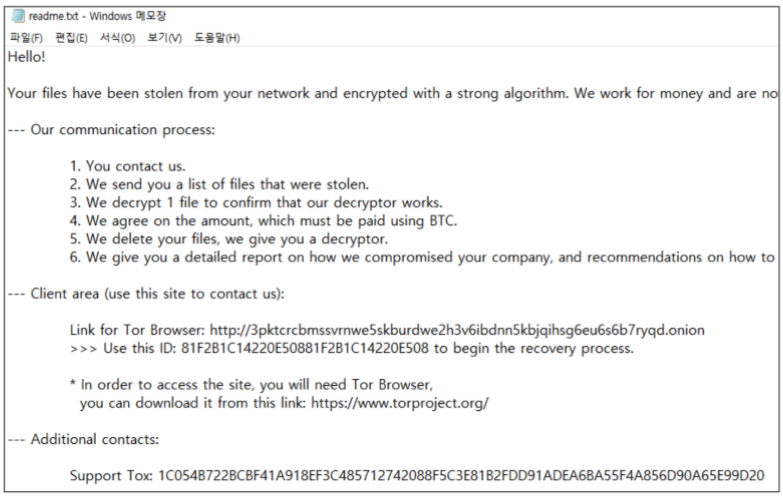


암호화 방식

2MB 이하: 전체 암호화
2MB 초과 10MB 이하: 파일의 첫 3MB만 암호화
10MB 초과: 파일의 50%만 암호화

특징

랜섬노트



readme.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are no

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to

--- Client area (use this site to contact us):

Link for Tor Browser: http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
>>> Use this ID: 81F2B1C14220E50881F2B1C14220E508 to begin the recovery process.

* In order to access the site, you will need Tor Browser,
you can download it from this link: https://www.torproject.org/

--- Additional contacts:

Support Tox: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

readme.txt

변경 확장자

.dragonforce_encrypted

제작 언어

C/C++

그림 9. DragonForce 랜섬웨어 개요

DragonForce 랜섬웨어 전략

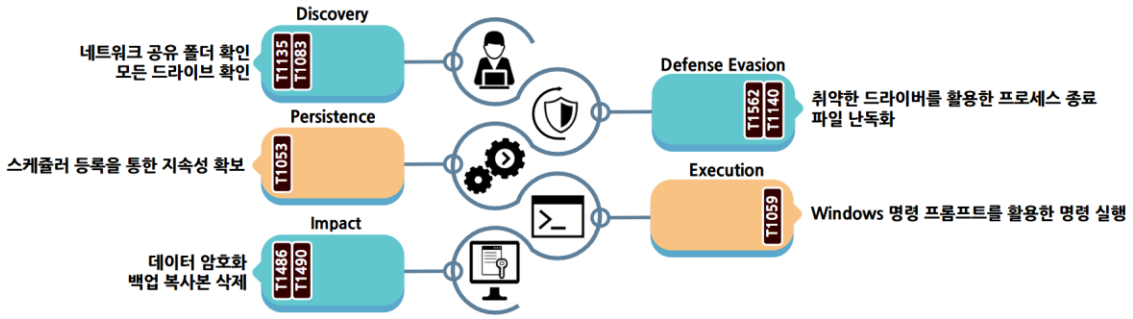


그림 10. DragonForce 랜섬웨어 공격 전략

DragonForce 랜섬웨어는 로그에 사용하는 문자열이나 백업 복사본에 사용하는 명령어 등 각종 문자열을 인코딩해 저장하며, 필요할 때마다 디코딩해 활용하는 방식을 사용한다. 뿐만 아니라 바탕화면, 아이콘 등 실행에 필요한 각종 데이터와 설정 값을 암호화해서 저장해두며, 랜섬웨어 실행 시 이를 복호화하여 사용한다. 랜섬웨어의 기능은 복호화된 설정값과 랜섬웨어 실행 시 입력한 실행 인자를 기반으로 정해진다.

DragonForce 랜섬웨어는 다양한 실행 인자를 사용해 암호화 대상이나 방식을 설정할 수 있으며, 로그 파일 생성이나 중복 실행을 허용할 수 있다. 다만, 랜섬웨어 내부에 암호화되어 있는 기본 설정값에 따라 일부 인자는 확인만 하고 사용하지 않는 경우가 있다. 실제 확인하는 인자와 기능은 아래 표와 같다.

인자	설명
-p <path>	특정 경로만 암호화
-m [all/local/nt/backups]	암호화 모드 설정
-log <path>	특정 경로에 로그 파일 생성
-size <percent>	부분 암호화 비율 설정
-nomutex	중복 실행 허용

표 1. DragonForce 랜섬웨어 실행 인자

실행 인자 중 일부 적용되지 않는 경우는 대부분 랜섬웨어 내부에 저장된 설정값 때문이다. 랜섬웨어는 ChaCha8 알고리즘으로 암호화된 설정값을 가지고 있으며, 이를 복호화해 랜섬웨어의 실행 옵션을 정한다. 이렇게 저장되는 설정값을 활용해 파일 암호화나 프로세스 종료 등에 활용한다. 또한 로그 파일의 맨 처음에 해당 랜섬웨어의 설정값을 우선적으로 저장하며, 저장된 로그 파일에 따른 설정 값은 아래 표와 같다.

구분	설명
build_key	로그 파일 암호화 키
custom_icon	암호화 파일 아이콘 변경 여부
custom_wallpaper	바탕 화면 변경 여부
custom_extension	암호화 확장자
time_sync	시스템 시간 동기화 여부
encrypt_mode	기본 암호화 모드(all, local, nt, backups)
full_encrypt_threshold	전체 암호화 파일 기준
header_encrypt_threshold	파일 헤더 암호화 기준
header_encrypt_size	파일 헤더 암호화 크기
other_encrypt_chunk_percent	부분 암호화 비율
encrypt_file_names	원본 파일명 Base32 인코딩 여부
schedule_job	작업 스케줄러 등록 여부
job_executable	작업 스케줄러 실행 파일 경로
job_title	스케줄러 작업 이름
job_description	스케줄러 작업 설명
job_start	스케줄러 작업 시작 시각
kill	프로세스 종료 여부
use_sys	BYOVD[1] 기법 활용 여부
priority	프로세스 종료 대상
whitelist	암호화 예외 여부
path	암호화 예외 폴더
ext	암호화 예외 확장자
filename	암호화 예외 파일명

표 2. DragonForce 랜섬웨어 설정값

[1] BYOVD: 합법적인 서명이 되어 있지만, 취약점을 가진 드라이버를 악용해 보안 솔루션을 우회해 악성 행위를 하는 기법

원활한 파일 암호화를 위해 설정값에 저장된 프로세스를 우선적으로 종료한다. 분석을 진행한 랜섬웨어에는 아래 표에 해당하는 프로세스 리스트가 확인됐다.

프로세스
MsMpEng.exe, sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe,isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, encsvc.exe, firefox.exe, tbirdconfig.exe, mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe, calc.exe, wuauclt.exe, onedrive.exe, SQLAGENT.exe, sqlservr.exe, SQLWriter.exe

표 3. 종료 대상 프로세스

단순히 프로세스 핸들을 가져와 종료하는 방식도 있지만, 설정에 use_sys 옵션이 활성화되어 있다면 취약한 드라이버 truesight.sys 와 rentdrv2.sys 를 악용해 프로세스를 종료한다. 각 드라이버의 임의 프로세스 종료 기능을 통해 보안 솔루션의 탐지를 우회하고 프로세스 종료를 시도한다. truesight.sys 는 Adlice Software 의 멀웨어 제거 도구 RogueKiller Antirootkit 에서 루트킷 탐지 및 제거 기능을 제공하는 드라이버 모듈로, v3.4.0 이하의 버전에서 임의의 프로세스를 종료시킬 수 있는 취약점이 발견됐다. rentdrv2.sys 는 중국의 네트워킹 플랫폼 기업 Hangshou Shunwang Technology 에서 사용하는 드라이버로, truesight.sys 와 동일하게 임의의 프로세스를 종료시킬 수 있는 취약점이 발견됐다. rentdrv2.sys 의 경우 세부 버전이 공개되지 않았으나 24 년 12 월 개발 업체는 취약점 조치가 완료됐다고 주장했으며, 두 취약한 드라이버는 모두 취약 드라이버 차단 정책에 적용됐다.

```
switch ( use_sys_flag )
{
  case 0:
    goto LABEL_26;
  case 1:                                   // truesight.sys | terminate process (0x22E044)
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E044u, lpInBuffer: &InBuffera, nInBufferSize: 4u, lpO
    break;
  case 2:                                   // rentdrv2.sys | terminate process (0x22E010)
    lpInBuffer[1] = InBuffera;
    lpInBuffer[0] = 1;
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E010u, lpInBuffer: lpInBuffer, nInBufferSize: 0x808u,
    break;
  default:
    goto LABEL_26;
```

그림 11. BYOVD 를 활용한 프로세스 종료

또한 암호화된 파일을 사용자가 임의로 복구하지 못하도록 백업 복사본을 삭제한다. 백업 복사본을 삭제하기 위해 사용하는 명령어는 아래와 같다.

```
cmd.exe /c C:\\Windows\\System32\\wbem\\WMIC.exe shadowcopy where "ID='%s'" delete
```

표 4. 백업 복사본 삭제 명령어

백업 복사본 삭제 이후에는 -m 실행 인자로 설정한 암호화 모드에 따라 암호화 대상을 설정한다. 모드에는 연결된 드라이브를 암호화하는 local, 네트워크 공유 자원 중 “ADMIN$” 폴더를 암호화하는 nt, 그리고 드라이브와 네트워크 공유 자원을 모두 암호화하는 all 모드로 구분된다. 이 외에도 backups 라는 모드도 존재하지만, 해당 옵션을 사용하면 어떤 파일도 암호화하지 않고 종료된다. -p 실행 인자를 사용하면 특정 폴더만 암호화할 수 있으며, -m 혹은 -p 인자를 사용하지 않으면 설정 값에 기본으로 지정된 방식을 사용한다.

암호화 대상을 설정했으면, 각 디렉터리를 순회해 예외 항목에 해당하는지 확인한다. 예외 항목은 설정값에 저장되어 있으며, 이를 기준으로 대상 디렉터리가 예외 항목인지 확인하고 디렉터리 확인이 끝났다면 각 디렉터리에 존재하는 파일이 예외 항목인지 확인한다. 확인하는 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, perflogs, Public	.exe, .dll, .lnk, .sys, .msi, .bat, .dragonforce_encrypted, readme.txt

표 5. 암호화 예외 대상

파일 암호화 방식은 파일의 확장자와 크기에 따라 결정된다. 데이터베이스와 관련된 파일은 크기와 상관없이 전체 암호화를 진행하고, 가상 머신과 관련된 파일은 파일의 크기와 상관없이 처음 20%만 암호화한다. 각각 해당하는 파일 확장자는 아래 표와 같다.

확장자
.dadigrams, .sqlite, .db, .sas7bdat, .daschema, .sqlite3, .abcddb, .sqlite, .nrmlib, .db-wal, .db-shm, .dacpac, .accdw, .xmlff, .kexis, .kexic, .fmp, .sl, .accft, .accdt, .accdr, .accde, .accdc, .accdb, .fmp12, .temx, .rodx, .rctd, .nwd, .kexi, .itd, .grd, .epim, .dtsx, .dlis, .wmd, .mdn, .maw, .lut, .kdb, .icr, .icg, .hjt, .fm5, .db2, .adn, .abx, .abs, .xld, .xdb, .wrk, .wdb, .vvv, .vpd, .vis, .v12, .usr, .udl, .udb, .trm, .trc, .tps, .tmd, .sql, .spq, .sis, .sdf, .sdb, .scx, .sbf, .rsd, .rpd, .rod, .rbf, .qvd, .qry, .pnz, .pdm, .pdb, .pan, .p97w, .p96, .owc, .orx, .oqy, .odb, .wyn, .yf, .wnv2, .nsf, .ns4, .ns3, .ns2, .nnt, .ndf, .myd, .mwb, .mud, .mrg, .mpd, .mdf, .mdb, .mav, .mas, .mar, .maq, .maf, .lwx, .lgc, .kdb, .jtx, .jet, .itw, .ihx, .idb, .his, .hdb, .gwi, .gdb, .frm, .fpt, .fp7, .fp5, .fp4, .fp3, .fol, .fmp, .fic, .fdb, .fcd, .exb, .ecx, .eco, .dxl, .dsk, .dqy, .dp1, .ddl, .dcx, .dct, .dcb, .dbx, .dbv, .dbt, .dbs, .dbc, .db3, .dad, .cpd, .cma, .ckp, .cdb, .cat, .bdf, .btr, .ask, .alf, .ora, .arc, .adp, .adf, .ade, .adb, .4dl, .4dd, .mdt, .nv, .ib, .db, .te

표 6. 데이터베이스 관련 확장자

확장자
.vdi, .vhd, .vmdk, .pvm, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso

표 7. 가상 머신 관련 확장자

그 외의 파일은 설정값의 크기 기준 full_encrypt_threshold, header_encrypt_threshold 값에 따라서 전체 암호화와 부분 암호화를 결정한다. 각각 2MB 와 10MB 로 설정되어 있어, 2MB 이하의 파일은 전체 암호화를 하며, 2MB 초과 10MB 이하의 파일은 처음 3MB 만 암호화한다. 또한 10MB 보다 큰 파일은 전체의 50%만 암호화한다.

그림 12. 크기 별 파일 암호화 방식

암호화 알고리즘으로 ChaCha8 을 사용하며, 사용한 키와 IV 는 RSA-4096 공개키로 보호한 다음 암호화한 파일의 맨 뒤에 추가한다. 파일 암호화 이후에는 암호화 확장자를 추가하는데, encrypt_filenames 옵션이 활성화되어 있는 경우 암호화 확장자 추가뿐만 아니라 파일명을 인코딩한다. 인코딩 방식으로 Base32 를 사용하지만 기본 문자 집합이 아닌 “gwfn6l3bk45o2zecvi7xtyqrpsudmahj” 문자열 집합을 기준으로 원본 파일명을 인코딩 한 뒤 암호화 확장자를 추가한다.

그림 13. 변경된 바탕화면

파일 암호화 이후에는 랜섬웨어에 저장된 이미지와 아이콘 파일로 바탕화면과 암호화된 파일의 아이콘을 변경한다. 배경화면은 “C:\Users\Public\wallpaper_white.png” 경로에 저장하며, 아이콘 이미지는 “C:\Users\Public\icon.ico” 경로에 저장한다.

뿐만 아니라 랜섬웨어를 작업 스케쥴러에 등록해 실행하는 기능도 확인됐다. 해당 설정이 존재한다면, 현재 랜섬웨어를 job_executable 설정에 저장된 경로에 복사한다. 그 이후 job_title 에 저장된 값을 작업명으로, job_description 을 작업 설명으로 생성하며, job_start 에 저장된 시각을 기준으로 실행되도록 작업을 생성한다.

DragonForce 랜섬웨어 대응방안

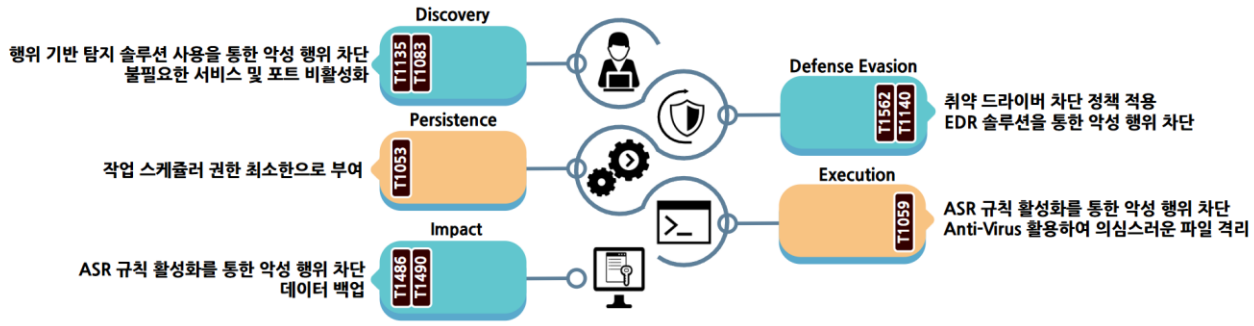


그림 14. DragonForce 랜섬웨어 대응방안

DragonForce 랜섬웨어는 Windows 명령 프롬프트를 활용해 백업 복사본 삭제를 진행한다. 따라서 ASR[1] 규칙 활성화를 통해서 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 랜섬웨어에 저장된 프로그램을 임시 폴더에 저장하거나 작업 등록을 위해 랜섬웨어를 특정 위치에 복제하기 때문에 Anti-Virus 를 활용하여 의심스러운 파일을 격리할 수 있다.

네트워크 공유 폴더 암호화를 위해서 현재 시스템의 내부 네트워크 대역을 탐색하고, 연결이 가능한 공유 폴더에 접근을 시도한다. 또한, 파일 암호화의 경우 모든 드라이브를 탐색한 뒤 실행 인자에 따라서 암호화할 드라이브를 구분하기 때문에 행위 기반 탐지 솔루션을 통해 공격자의 악성 행위를 막을 수 있다.

합법적인 서명이 되어있지만, 취약한 버전의 드라이버 truesight.sys 와 rentdrv2.sys 를 악용해서 보안 장비를 우회하여 프로세스 종료를 시도하기 때문에 취약한 드라이버가 실행되지 않도록 차단해야 한다. 이는 취약 드라이버 차단 정책을 통해 해결할 수 있으며, Microsoft 에서 제공하는 취약한 드라이버 차단 목록에 이미 취약한 두 드라이버가 추가되어 있어 가이드라인에 따라 이를 시스템에 적용하여 취약한 드라이버가 악용되는 것을 방지할 수 있다. 뿐만 아니라 악성 행위에 필요한 파일과 명령어들이 암호화되거나 인코딩 된 상태로 존재하며, 사용 직전에 복호화 및 디코딩을 진행해 사용하기 때문에, EDR[2] 솔루션을 통해 악성 행위를 차단해야 한다.

암호화된 파일을 사용자가 임의로 복구하는 것을 방지하기 위해 시스템에 존재하는 모든 백업 복사본을 삭제한 뒤 파일을 암호화한다. ASR 규칙 활성화를 통해서 백업 복사본을 삭제하는 프로세스와 파일을 암호화는 것을 차단할 수 있다. 뿐만 아니라 백업 복사본을 별도의 네트워크나 저장소에 소산 백업하여, 시스템이 암호화되더라도 복구할 수 있도록 조치해야 한다.

[1] ASR (Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

[2] EDR (Endpoint Detection and Response): 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션

IoCs

Hash(SHA-256)
d06b5a200292fedcfb4d4aecac32387a2e5b5bb09aaab5199c56bab3031257d6
70afd8efb34382badead93ae104d958256de6be8054227ccc85fe95d5c5f9db0

■ 참고 사이트

• Guide Point Security (https://www.guidepointsecurity.com/blog/ransomsnub-ransomhubs-affiliate-confusion/)

• The Hacker News (https://thehackernews.com/2025/05/play-ransomware-exploited-windows-cve.html)

• The Hacker News (https://thehackernews.com/2025/05/qilin-leads-april-2025-ransomware-spike.html)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/everest-ransomwares-dark-web-leak-site-defaced-now-offline/)

• Symantec (https://www.security.com/threat-intelligence/play-ransomware-zero-day)

• GitHub (https://github.com/keowu/BadRentdrv2)

• UNIT 42 (https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/)

• Microsoft (https://learn.microsoft.com/ko-kr/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules)

Special Report

제로트러스트 보안전략 : 식별자·신원(Identity)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

■ 식별자·신원(Identity) 필러 개요

식별자·신원(Identity) 필러는 제로트러스트 아키텍처의 핵심 요소 중 하나로 사용자, 서비스, IoT 기기 등 모든 엔터티를 고유하게 식별하고 보호하는 역할을 담당한다. 제로트러스트 원칙에 따라 모든 사용자는 신뢰할 수 없는 대상으로 간주되며, 네트워크와 시스템 등에 접근하기 전에 반드시 검증을 거쳐야 한다. 이는 단순히 초기 인증 단계에서의 검증에 그치지 않고, 지속적인 모니터링과 동적 정책 적용을 통해 사용자의 신뢰도를 평가하고 권한을 부여하거나 제한하는 방식으로 운영된다.

식별자·신원 필러는 조직 내 모든 엔터티를 명확히 식별하고, 이를 기반으로 보안 정책을 일관되게 적용할 수 있도록 한다. 사용자와 기기의 신원을 확인하는 과정은 단순한 인증 절차를 넘어, 지속적인 검증과 위험 평가를 포함한다. 이를 통해 조직은 내부 및 외부 위협으로부터 민감한 자산을 보호하고, 보안 사고를 사전에 예방할 수 있다.

제로트러스트 환경에서 식별자·신원 필러는 보안의 출발점이자 중심축으로 작용하며, 신원 관리와 접근 통제를 통해 보안 태세를 강화한다. 특히 사용자의 역할(Role), 부서, 직급 등의 속성을 기반으로 권한을 부여하거나 제한하는 정책은 최소 권한 원칙을 실현하는 데 중요한 역할을 한다. 이러한 정책은 조직 내 모든 시스템과 데이터에 대해 일관된 접근 제어를 가능하게 하며, 보안의 효율성과 신뢰성을 높인다.

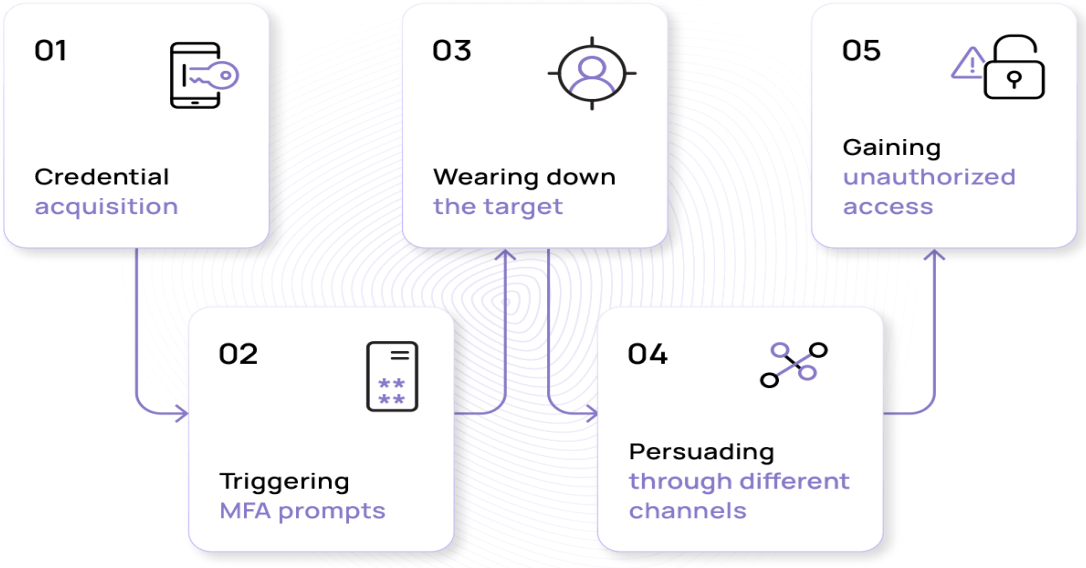
출처 : SK 쉴더스 EQST, "2025 보안 위협 전망 보고서"

그림 1. 2024 보안 이슈 Review

최근 글로벌 위협 보고서에 따르면, 아이덴티티(Identity)를 이용한 공격이 급격히 증가하는 등 공격자들의 주요 표적이 되고 있다. 특히, 크리덴셜 스터핑(Credential Stuffing)은 가장 널리 사용되는 공격 방식 중 하나로, 공격 트래픽의 상당 부분을 차지하고 있다. 크리덴셜 스터핑은 이전 데이터 유출에서 얻은 계정 정보를 자동화된 도구를 통해 여러 플랫폼에서 테스트하여 불법적으로 접근하는 방식으로 이루어진다. 다크웹에서는 이러한 계정 정보가 거래되고 있으며, 이는 공격자들이 초기 침투를 시도하는 데 주요 수단으로 활용된다.

SpyCloud 의 "2025 Identity Exposure Report"에 따르면, 2024 년 한 해 동안 533 억 개의 신원 데이터가 유출된 것으로 나타났다. 이는 전년 대비 22% 증가한 수치다. 이러한 데이터는 크리덴셜 스터핑과 같은 공격에 사용되어 기업과 개인 모두에게 심각한 위협을 초래하고 있다.

제로트러스트 아키텍처의 인증 강화 방안인 다단계 인증(MFA)은 오랫동안 아이덴티티(Identity) 보호를 위한 보안의 표준으로 여겨져 왔지만, 최근에는 이를 우회하려는 다양한 공격 기법들이 등장하면서 다단계 인증만으로는 아이덴티티(Identity)의 보안성을 보장할 수 없게 되었다. 잘못된 MFA 정보를 계속 보내는 MFA 피로공격, 리버스 프록시 아키텍처를 이용한 피싱도구, 중간자 (A.ItM) 피싱, MFA 정보를 보관하는 중간지점 공격 등 다양한 공격이 사용되고 있다.



출처 : Sosafe, "MFA Fatigue Attack"

그림 2. MFA 피로공격 절차

현 시점에서 가장 안전한 인증 방식으로 알려진 생체인증 또한 우회가 불가능한 것은 아니다. 가트너는 딥페이크 공격이 빈번해지면서 2026 년 기업의 30%가 생체 인증을 신뢰할 수 없을 것으로 예상했다. 가트너는 "2024 년 예측: A.I 및 사이버 보안" 보고서에서 신원확인 공급업체의 비공식 탐지 결과를 언급하면서 사기성 신원 인증 시도 중 15%가 딥페이크와 관련 있으며, 탐지되지 않은 것의 비중은 얼마나 될지 알 수 없다고 설명했다.

결론적으로 아이덴티티 기반 공격이 증가하는 상황에서 단순히 기존의 보안 기술에 의존하는 것은 더 이상 충분하지 않다. MFA 와 생체 인증은 여전히 강력한 보호 수단이지만, 이를 우회하려는 공격 기법 또한 정교해지고 있다. 따라서 제로트러스트 원칙을 기반으로 한 지속적인 모니터링과 동적 정책 적용이 필수적이다. 제로트러스트 원칙 중 "지속적인 검증"과 "최소 권한" 원칙을 통해 인증을 일회성으로 끝내는 것이 아닌 사용자의 행동 패턴, 접속 환경, 디바이스 상태 등을 지속적으로 평가하여 추가검증을 해야 한다. 예를 들어, 사용자가 평소와 다른 지역에서 접속하거나 비정상적인 활동을 수행할 경우, 추가 인증 절차를 요구하거나 접근 권한을 제한하는 것이다. 또한 MFA 및 생체 인증을 통한 사용자의 신원 확인 후에도, 업무 수행에 필요한 최소 권한만 부여함으로써 공격 표면을 줄이는 효과를 낼 수 있다. 이를 통해 사용자가 불필요하게 민감한 데이터나 시스템에 접근하지 못하도록 제한하는 것은 물론 내부자 위협이나 권한 남용 위험을 최소화할 수 있다.

궁극적으로 조직은 제로트러스트 기반의 패스워드리스(Passwordless) 인증 도입, 사용자 행동 분석 및 위험 평가 강화, 그리고 생체 인증의 보완과 같은 다층적인 접근 방식을 통해 아이덴티티 보호 체계를 강화해야 한다. 이를 통해 조직은 점점 더 정교해지는 위협 환경에서도 민감한 자산을 안전하게 보호하고, 신뢰할 수 있는 디지털 환경을 구축할 수 있을 것이다.

■ 식별자·신원(Identity) 필러의 주요 요소

제로트러스트 아키텍처에서 식별자·신원(Identity) 필러는 사용자와 관련된 모든 보안 요소를 다루는 핵심 영역으로, 제로트러스트 원칙을 구현하는 데 있어 필수적인 역할을 한다. 사용자는 단순히 사람뿐만 아니라 서비스 계정, IoT 기기 등 다양한 형태로 존재하며, 이들에 대한 신원 확인과 검증은 보안 체계의 출발점이 된다.

특히, 제로트러스트 환경에서는 모든 사용자를 신뢰할 수 없는 대상으로 간주하고, 지속적인 검증과 최소 권한 부여를 통해 접근을 통제해야 한다. 이를 위해 식별자·신원 필러는 사용자 인벤토리 관리, 계정 및 권한 관리, 인증 강화, 위험 평가 등 다양한 요소를 포함하며, 각 요소는 조직의 보안 태세를 강화하는데 중요한 역할을 한다.

아래에서는 식별자·신원 필러의 주요 요소와 이를 구현하기 위한 관리적 및 기술적 방안을 구체적으로 살펴본다.

1. 사용자 인벤토리

사용자 인벤토리는 조직 내 모든 사용자를 식별하고 관리하는 기본적인 출발점이다. 제로트러스트 환경에서는 사용자를 명확하게 식별하고, 이들의 신원을 최신 상태로 유지하는 것이 매우 중요하다. 사용자 인벤토리는 조직 내에서 누가 어떤 자산에 접근할 수 있는지에 대한 정보를 제공하며, 이를 통해 접근 통제 및 권한 부여를 효율적으로 관리할 수 있다.

사용자는 지속적으로 업데이트되는 목록화된 정보로 관리한다. 이 목록은 사용자의 기본 정보뿐만 아니라 신원 정보까지 포함해야 한다. 초기 단계에서는 파일이나 수기로 관리될 수 있지만, 성숙도가 높아짐에 따라 자동화된 시스템을 통해 사용자 정보가 실시간으로 업데이트되고, 신뢰도 있는 데이터를 기반으로 권한이 자동으로 변경될 수 있어야 한다.

사용자는 부서, 직급, 역할 등에 따라 그룹핑되어야 하며, 이러한 그룹 정보는 사용자의 상태가 변경될 때마다 자동으로 업데이트되어야 한다. 이를 통해 특정 그룹에 속한 사용자들이 필요로 하는 자산에만 접근되도록 제한한다.

2. 사용자 계정관리

사용자 계정 관리는 각 사용자가 보유한 계정을 통해 리소스에 접근할 수 있도록 하는 체계다. 계정 관리는 단순히 계정을 생성하고 삭제하는 것을 넘어, 계정의 수명주기 전체를 중앙에서 통제하고 관리해야 한다.

각 사용자는 고유한 계정을 부여받아야 하며, 해당 계정은 중앙에서 목록화하여 관리한다. 초기 단계에서는 단순히 파일이나 수기로 계정을 관리할 수 있지만, 점차 ICAM(Identity Credential Access Management)과 같은 통합 시스템을 도입해 모든 계정을 중앙에서 일괄적으로 관리하는 방식으로 발전해야 한다.

사용자 계정의 생성부터 삭제까지의 모든 과정이 자동화될 수 있도록 해야 하며, 이를 통해 불필요한 권한이 남용되지 않게 주의한다. 특히 A.I 및 머신러닝을 활용해 사용자의 신뢰도 데이터를 기반으로 계정의 상태를 지속적으로 검증하고, 필요 시 자동으로 권한을 조정하는 체계를 구축하는 것이 필요하다.

3. 사용자 패스워드 관리

패스워드는 많은 시스템에서 기본적인 인증 수단으로 사용되고 있다. 그렇기 때문에 패스워드 관리는 매우 중요한 요소다. 패스워드 정책은 주기적인 변경 요구와 복잡성 규정을 포함해야 하며, 패스워드 유실이나 도용을 방지하기 위한 추가적인 보안 조치도 필요하다. 사용자는 주기적으로 패스워드를 변경해야 하며, 이러한 변경 요구는 시스템에서 자동으로 알림을 제공해야 한다. 성숙도가 높은 조직에서는 패스워드가 자동으로 변경되고, 사용자는 인증 절차를 통해 새로운 패스워드를 확인하는 방식으로 운영될 수 있다.

패스워드는 정책에 따라 복잡성 요구사항이 설정되어야 한다. 이러한 정책이 준수되도록 모든 사용자를 강제한다. 또한 패스워드 유실 시에는 잠금 정책을 통해 추가적인 보안을 제공해야 하며, 이상 행위가 감지되면 즉시 대응할 수 있는 체계를 마련해야 한다.

제로트러스트 아키텍처에서는 패스워드 관리뿐만 아니라 사용자 행위에 따라 추가 인증이나 다중 인증 요소(MFA)를 적극적으로 활용하는 것을 권장한다. 이는 단순히 비밀번호를 사용하는 것만으로는 부족한 보안성을 강화하기 위해 사용자의 접속 환경과 행동 패턴을 지속적으로 평가하고, 필요 시 추가 인증 절차를 요구하는 방식이다. 예를 들어, 사용자가 평소와 다른 위치에서 접속하거나 비정상적인 활동을 수행할 경우 MFA 를 통해 보안을 강화할 수 있다.

궁극적으로 제로트러스트 아키텍처는 Passwordless 방식으로 전환하는 것을 목표로 한다. 이는 생체 인증(지문, 얼굴 인식), FIDO2 토큰 또는 물리적 키와 같은 강력한 인증 기술을 활용하여 비밀번호의 재사용 문제와 유출 위험을 근본적으로 해결한다. Passwordless 방식은 사용자 경험을 개선하면서도 보안을 강화하는 데 효과적이며, 제로트러스트 환경에서 점점 더 중요해지고 있다.

4. 사용자 권한 관리

제로트러스트 아키텍처에서는 최소 권한 원칙이 매우 중요하다. 사용자 권한 관리는 각 사용자가 업무 수행에 필요한 최소한의 리소스에만 접근할 수 있도록 제한하는 것을 목표로 한다.

각 시스템과 리소스에 대한 접근 권한은 개별적으로 설정되어야 하며, 이러한 권한은 주기적으로 검토되고 업데이트되어야 한다. 또한 각 시스템에서 운영자와 관리자 등 다양한 역할에 따라 접근 권한을 구분한다. 리소스별로 접근 및 수정 권한이 명확하게 정의되어야 가능하다.

사용자가 리소스에 접근하여 수행하는 모든 활동은 실시간으로 모니터링되고, 이상 징후가 발견되면 즉시 차단하거나 경고를 제공하는 체계가 필요하다.

5. 사용자 증명

제로트러스트 환경에서는 단순히 ID 와 비밀번호만으로는 충분하지 않다. 사용자 증명(User Authentication)은 다단계 인증(MFA)을 포함하여 더욱 강력하게 이루어져야 하며, 이를 통해 신뢰성을 강화할 필요가 있다.

ID 페더레이션은 한 번의 로그인으로 여러 서비스에 접근할 수 있도록 하는 체계다(SAML, OAuth 등 표준 활용). 전사적인 ID 페더레이션 체계를 구축하면 모든 시스템과 애플리케이션에서 일관된 인증 절차를 거칠 수 있다.

다중 인증(MFA)을 통해 추가적인 보안 레이어를 제공하며, 신뢰도 판단 데이터를 기반으로 인증 절차를 강화해야 한다. MFA 는 지식 기반(비밀번호), 소유 기반(OTP), 생체 기반(지문) 등을 결합하여 보다 안전하게 사용자 인증을 수행한다.

6. 통합 ICAM 플랫폼

통합 ICAM(Identity Credential Access Management) 플랫폼은 제로트러스트 아키텍처의 핵심 구성 요소 중 하나로, 모든 리소스에 대한 접근 제어와 자격 증명을 중앙에서 통합적으로 관리하는 역할을 수행한다. ICAM 은 기존 IAM(Identity and Access Management)의 확장 개념으로, 단순히 신원(Identity) 관리에 그치지 않고 자격 증명(Credential)까지 포함하여 사용자와 엔터티의 신뢰도를 더욱 정교하게 평가한다.

ICAM 플랫폼은 모든 사용자와 관련된 정보를 중앙에서 일괄적으로 관리하며, 이를 통해 자격 증명과 인증 절차를 자동화한다. 역할 기반 제어(Role-Based Access Control) 기능으로 각 사용자의 역할에 따라 리소스 접근 권한이 자동으로 부여되거나 제한된다. 또한, 속성 기반 접근 제어(Attribute-Based Access Control)를 활용하여 사용자의 위치, 디바이스 상태, 행동 패턴 등 다양한 컨텍스트를 고려한 동적 정책 적용이 가능하다.

ICAM 은 PIP(Policy Information Point)를 활용하여 SIEM(Security Information and Event Management), EDR(Endpoint Detection and Response), UEM(Unified Endpoint Management) 등에서 전달된 정보를 바탕으로 사용자의 신원(Credential)을 판단한다. 이러한 정보는 사용자의 행동 패턴과 디바이스 상태를 실시간으로 분석하여 위험도를 평가하고, 이를 기반으로 지속적인 인증 및 검증을 수행한다. 예를 들어, 사용자가 비정상적인 네트워크 활동을 수행하거나 보안 정책을 위반한 경우, ICAM 플랫폼은 즉시 경고를 생성하거나 추가 인증 절차를 요구할 수 있다.

ICAM 은 또한 PAM(Privileged Access Management)과 연계되어 특권 계정의 접근을 제어하고 모니터링함으로써 Identity 기반의 자격 증명을 더욱 강화한다. PAM 과의 통합은 민감한 시스템과 데이터에 대한 접근을 엄격히 제한하며, 내부자 위협이나 권한 남용을 방지하는 데 중요한 역할을 한다.

7. 사용자 위험평가

제로트러스트 환경에서는 각 사용자의 위험도를 평가하고 이를 바탕으로 보안 정책을 동적으로 조정하는 것이 중요하다. 각 사용자의 위험도는 컴플라이언스 준수 여부나 이상 행위 탐지에 따라 정량화하여 평가된다.

위험도 평가는 인증 강화 및 권한 부여 시 중요한 데이터로 활용되며, 실시간 모니터링을 통해 즉각적인 대응이 가능하도록 해야 한다.

식별자·신원 필러는 이러한 주요 요소들을 통해 조직 내 민감한 자산을 보호하고 내부자 위협과 외부 공격 모두를 효과적으로 차단할 수 있다. 나아가 변화하는 위협 환경에 적응할 수 있는 유연성과 신뢰성을 제공하며, 제로트러스트 환경에서 일관된 보안 정책 적용과 지속 가능한 디지털 보안 체계를 구축하는 데 핵심적인 역할을 한다. 이를 통해 조직은 더욱 강력하고 신뢰할 수 있는 보안 태세를 유지하며, 안전한 디지털 환경을 조성할 수 있을 것이다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행할 수 있는 시스템은 필수적이다. 제로트러스트 아키텍처는 "신뢰하지 않고 항상 검증한다"는 원칙을 기반으로 한다. 이를 실현하기 위해 사용자와 엔터티의 신원을 확인하고, 지속적으로 검증하며, 최소 권한 접근을 보장을 수행할 수 있는 시스템이 필수적이다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 식별자(Identity) 관점으로 중요한 역할을 담당하며, 이들 시스템은 상호 연계되어 조직의 보안 태세를 강화할 수 있다. 각 시스템 별로 제로트러스트 환경 구현을 위해 수행해야 할 기능과 이를 통해 조직이 얻을 수 있는 보안 강화 효과를 구체적으로 살펴보고자 한다.

출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

그림 3. 식별자·신원 주요 시스템

1. SSO(Single Sign-On)

SSO 는 하나의 인증으로 여러 애플리케이션과 시스템에 접근할 수 있도록 하는 통합 인증 시스템으로, 사용자 편의성과 운영 효율성을 동시에 확보할 수 있는 인증 기술이다. 하지만 제로트러스트 환경에서는 단순한 사용자 편의성만으로는 충분하지 않으며, 지속적인 검증과 동적 통제가 가능한 보안 역량이 필수적으로 요구된다.

제로트러스트 환경에서 SSO 는 더 이상 단일 포털 인증 수준에 머물지 않는다. 웹 환경은 물론 클라우드 서비스(AWS, Azure, GCP)와의 연계, 그리고 C/S 기반 내부 시스템까지 포함하여 다양한 접근 경로에 대한 통합 인증을 지원해야 하며, 각 환경에서의 인증 요구사항을 만족할 수 있도록 표준 인증 프로토콜(SAML, OAuth, OIDC 등)에 기반한 상호 운용성과 확장성을 갖추는 것이 기본 전제가 된다.

제로트러스트 원칙에서 SSO 는 단순히 최초 인증을 처리하는 시스템이 아니라, 최초 인증 이후에도 지속적으로 세션의 유효성, 사용자 행동 변화, 접속 단말과 위치, IP 주소, 접속 시간 등의 컨텍스트 정보를 실시간으로 분석하여 인증 값의 변조 가능성을 탐지하고 필요 시 재인증이나 세션 차단 등 후속 조치를 수행할 수 있어야 한다. 이 과정에서 인증 토큰에 대한 암호화는 기본이며, 인증값 위·변조 방지 기술을 통해 세션 하이재킹 등 공격 시도에 선제적으로 대응할 수 있는 구조가 요구된다.

더불어, 사용자 인증 시 단순한 정적 규칙 기반 접근이 아니라, 다중 요소(단말 유형, 접속 위치, 시간대, IP 특성 등)를 기반으로 리스크 스코어링을 수행하여 동적으로 인증 수준을 조정하거나 인증 경로 자체를 변경할 수 있는 유연한 정책 구성이 필요하다. 예컨대 동일한 자격 증명을 보유하더라도 평소와 다른 지역, 의심스러운 시간대, 새로운 디바이스로 접속 시 추가 인증(MFA)이나 접근 제한 조치가 병행되어야 한다.

이러한 모든 인증 활동과 접근 흐름은 시각화된 대시보드를 통해 실시간 모니터링되어야 하며, 인증 성공·실패 이력, 사용자별 접속 이력, 리스크 이벤트 발생 현황 등을 체계적으로 리포트할 수 있어야 한다. 이는 단순한 보안 감시를 넘어서, 사용자 행동 기반의 이상 탐지(UEBA)나 보안 정책 강화에도 활용될 수 있는 주요 기반 데이터로 작용한다.

결국 SSO 는 제로트러스트 환경의 '초기 관문'으로서 단순한 인증 시스템의 범주를 넘어, 사용자와 엔터티에 대한 지속 가능한 검증 체계를 제공하는 실시간 보안 운영 인프라로 자리매김하고 있다. 제대로 된 SSO 구현 없이는 제로트러스트 아키텍처의 출발점조차 성립하기 어려운 만큼, 해당 시스템에 대한 기술적·관리적 완성도는 제로트러스트 환경에서 매우 중요한 요소이다.

2. IAM(Identity and Access Management)

IAM 은 제로트러스트 아키텍처의 핵심 구성요소로, 사용자 계정과 권한을 중앙에서 통합 관리하고 다양한 업무 시스템과의 연동을 지원함으로써 보안 통제력을 강화하는 역할을 한다. IAM 은 단순한 계정 등록과 삭제를 넘어, 사용자의 신원과 권한을 연계한 세분화된 접근 제어를 실현하며, 이를 통해 최소 권한 원칙을 지속적으로 유지할 수 있도록 한다.

제로트러스트 환경에서의 IAM 은 인사 정보나 사용자 속성 같은 다양한 데이터를 연계하기 위해 LDAP, AD, DB File 등과 같은 디렉터리 시스템과의 연동 기능을 갖추고 있어야 하며 웹 기반, C/S 환경, 클라우드 플랫폼 등 이기종 시스템과 유연하게 통합되도록 표준 프로토콜(SAML) 및 API 연동을 지원해야 한다. 이를 통해 조직은 모든 업무 시스템에 대한 사용자 계정과 권한을 중앙에서 통합적으로 관리할 수 있으며, 정책 위반 계정 탐지, 휴면 계정 정리 등의 작업도 자동화하여 지속적인 권한 적정성을 유지할 수 있다.

특히 제로트러스트 원칙에 따라 ABAC(속성 기반 접근 제어), RBAC(역할 기반 접근 제어) 등의 정책 모델을 정교하게 구현해야 하며, 사용자의 직무, 부서, 위치, 접속 환경 등 다양한 속성을 기반으로 한 권한 제어가 가능해야 한다. 이러한 역할 기반·속성 기반 권한 설정은 단순히 관리자에 의해 수동으로 구성되기에는 한계가 있으며, A.I 나 머신러닝을 통한 정책 자동화 기능이 함께 도입되어야 한다.

예측 기반의 접근 권한 추천, 권한 충돌 감지, 이상 행위 기반의 정책 재구성 등은 단순히 이론적 기능이 아닌, 최근 상용 IAM 제품들이 실제로 구현하고 있는 핵심 기능이다. 예를 들어, 일부 글로벌 IAM 솔루션은 사용자의 과거 접근 패턴과 직무 이력을 학습하여 새로운 업무 시스템 연동 시 자동으로 적절한 권한을 추천하거나, 유사 직무자와의 권한 비교를 통해 초과 권한 여부를 탐지한다.

또한 머신러닝 기반의 이상행위 탐지 엔진은 사용자 행위가 통상적인 업무 흐름과 벗어날 경우 경고를 생성하거나 권한을 자동 축소하는 정책을 실시간 적용한다. 이러한 기능들은 IAM 을 단순한 계정 관리 시스템이 아닌 '지능형 접근 제어 허브'로 진화시키며, 제로트러스트 보안 체계의 실행력을 강화하는 데 실질적으로 기여하고 있다.

IAM 은 확장될 경우 기존 IAM 시스템에서 신원(Credential)을 포함한 ICAM(Identity, Credential and Access Management)으로 확장 구성될 수 있으며, 이는 제로트러스트 기반의 핵심 통합 시스템으로 작동한다. ICAM 은 EDR, UEM, Micro-Segmentation, SIEM/SOAR, DLP, DSPM 등의 다양한 PIP(Policy Information Point)와 연동되어 사용자와 기기의 신뢰 수준을 실시간으로 평가하고 이를 기반으로 동적 접근 정책을 적용하는 역할까지 수행하게 된다. 따라서 IAM 은 단순한 인증 및 계정 관리 체계를 넘어, 제로트러스트 환경의 기반이 되는 '핵심 시스템'으로 기능해야 한다.

* 근거 문서

1. "NIST SP 800-207" (NIST)
2. "Automating Access Governance for Zero Trust" (KuppingerCole) 3."The Importance of Least Privilege in a Zero Trust World" (SANS Institute)
4. "User and Entity Behavior Analytics (UEBA) for Zero Trust" (Gartner) 5."The Role of SIEM in a Zero Trust Architecture" (Forrester)

그림 4. 제로트러스트 기반 SSO/IAM 의 주요기능

3. MFA (Multi-Factor Authentication)

다중 인증(MFA)은 제로트러스트 환경에서 '지속적인 검증' 원칙을 실현하는 핵심 수단으로, 사용자 인증에 있어 단일 수단에 의존하지 않고 다양한 인증 방식을 조합해 보안성을 강화하는 역할을 수행한다. 특히 해외에서는 MFA 가 SSO 기능과 통합되어 하나의 인증 플랫폼으로 운영되는 경우가 많지만, 국내 보안 환경에서는 MFA 를 별도의 독립된 인증 시스템으로 구축하고 관리하는 경우가 일반적이다. 이러한 구조는 시스템 구성의 유연성과 보안정책의 분리 운용 측면에서 각각의 장단점을 가지고 있으며, 제로트러스트 환경에서는 양쪽 모두에 대한 고려가 필요하다.

MFA 시스템은 기본적으로 SSO, IAM 에서 사용자 이상행위가 탐지되었을 때 추가 인증 수단을 수행하는 역할을 하며, OTP(일회용 비밀번호), 하드웨어/소프트웨어 토큰, 휴대폰 기반 생체 인증(FIDO2 기반 지문·얼굴 인식) 등의 다양한 방식이 사용된다. 이때 인증 수단은 정보보안 인증의 기본 개념인 Type1(지식), Type2(소유), Type 3(존재)을 조합하여 구성되며, 다중 요소 인증의 본질은 바로 이 복합 인증 요소들의 상호 보완성을 통해 인증 위협을 차단하는 데 있다.

최근 MFA 기술은 단순한 인증 수단 제공을 넘어 진화하고 있다. 예를 들어, FIDO2 이후에는 브라우저·디바이스 간 인증 연계성, 생체 인증의 보안성 강화, 인증 절차 단순화 등을 중심으로 한 차세대 기술 개발 논의가 지속되고 있으며, 특히 생체 인증 과정에서의 라이브니스 감지(Liveness Detection) 기술은 딥페이크나 녹화 영상 등의 위조 시도를 탐지하는 데 활용되고 있다. 또한 인증 토큰 발급 및 전달 과정에서 PQC(Post-Quantum Cryptography, 양자 내성 암호) 등 차세대 암호 알고리즘을 적용하려는

움직임도 나타나고 있다. 이처럼 MFA 는 고도화된 인증 위협에 대응하기 위한 핵심 기술로 자리매김하고 있으며, 단순한 인증 절차를 넘어 제로트러스트 아키텍처의 정밀한 인증 관문으로서의 역할을 강화하고 있다.

결과적으로 MFA 는 사용자의 인증을 일회성으로 처리하지 않고, 위험 기반 인증(RBA: Risk-Based Authentication), 행위 기반 재인증, 컨텍스트 기반 정책 적용 등을 통해 지속적이고 동적인 인증 체계를 제공한다. 이는 단순한 로그인 절차를 넘어서 지속적으로 신뢰를 평가하고 강화하는 제로트러스트 모델의 핵심 구성 요소로 기능하며, SSO, IAM 과의 긴밀한 연동을 통해 사용자 신원을 정교하게 검증하는 보안 인프라로 자리매김하고 있다.

4. AD(Active Directory)

Active Directory(AD)는 마이크로소프트가 제공하는 디렉터리 서비스로, 가장 많이 사용되는 Windows 기반 인프라 환경에서 사용자 계정, 그룹, 장치, 정책 등을 중앙에서 관리하는 핵심 시스템이다. 오랜 역사를 가진 레거시 시스템이지만, 현재도 대다수의 기업 환경에서는 여전히 중심적인 사용자 인증 및 접근 제어 인프라로 활용되고 있으며, 특히 온프레미스 AD 와 Microsoft 의 클라우드 기반 디렉터리 서비스인 Entra ID(구 Azure AD)의 연동을 통해 하이브리드 환경을 구성하는 사례가 빠르게 확산되고 있다.

AD 는 단순한 사용자 저장소를 넘어, 조직 내 다양한 시스템(SaaS 애플리케이션, 파일 서버, ERP 등)과 연계되어 사용자 신원 정보와 그룹 속성, 권한 정책을 실시간으로 제공하는 정보 허브 역할을 수행한다. 특히 SSO, IAM, EDR, UEM 등 다수의 보안 시스템들은 AD 를 기반으로 사용자 권한을 해석하고 동적으로 접근 제어 정책을 적용하기 때문에, AD 정보의 정확성과 최신성은 전체 보안 체계의 신뢰성을 좌우하는 요소로 작용한다.

제로트러스트 환경에서 AD 는 그 자체로 보안 대상이며 동시에 공격 표적이 된다. 공격자는 초기 침입 이후 권한 상승을 위해 AD 를 우선적으로 노리고, 관리자 계정 탈취, 권한 확장, 서비스 접근 경로 확보 등의 행위를 AD 내부에서 수행하려 한다. 실제로 다수의 침해 사고 사례에서 AD 가 권한 탈취의 통로로 활용된 바 있으며, 이로 인해 AD 는 제로트러스트 보안 전략 내에서 최우선 보호 대상 자산으로 간주된다.

따라서 AD 는 단순한 운영 관리 대상이 아니라 보안 인프라로서 기능해야 하며, 이를 위해 다양한 보안 솔루션이 함께 적용되어야 한다. 예를 들어, AD 내부의 이상 행위를 실시간으로 탐지하는 보안 로그 분석 시스템, 관리자 권한의 위임 및 승인 체계를 적용하는 PAM 연계, 불필요한 그룹 정책이나 계정 설정을 탐지하고 정리하는 정책 감사 도구 등이 대표적인 보안 기술이다. 이외에도 AD 자체에 대한 정기적인 위협 분석 및 강화 설정 점검이 필수적으로 수행되어야 한다.

AD 는 제로트러스트 환경에서 사용자의 실시간 상태, 디바이스 연결 여부, 로그인 시도 기록 등을 기반으로 리스크 기반 인증 정책이나 세분화된 접근 통제를 수행하는 데 기초 데이터를 제공한다. 따라서 AD 와 연계되는 보안 시스템은 AD 로부터 제공되는 정보를 토대로 지속적인 사용자 신뢰 평가와 권한 검증을 수행해야 하며, 이를 위해 AD 는 항상 최신의 정확한 데이터를 유지해야 한다.

결과적으로 AD 는 더 이상 단순한 사용자 관리 시스템이 아니라, 제로트러스트 환경을 구현하기 위한 보안 기반 플랫폼 중 하나로서 기능하며, 그 운용 수준에 따라 전체 보안 아키텍처의 완성도 또한 달라질 수 있다.

5. HR 시스템 (Human Resources System)

HR 시스템은 조직 내 모든 사용자에 대한 신원, 직무, 소속 부서, 고용 상태 등의 인사 정보를 관리하는 핵심 시스템으로, 제로트러스트 환경에서는 사용자 신뢰 수준 판단과 권한 정책 적용의 기초 데이터 소스로서 기능한다. 기존 보안 아키텍처에서는 HR 시스템이 단순한 행정 시스템으로 여겨졌으나, 제로트러스트 체계에서는 사용자 검증과 접근 통제를 위한 핵심 연동 대상 시스템으로 그 중요성이 재조명되고 있다.

이처럼 HR 시스템은 사용자 라이프사이클 전반에 걸쳐 보안 정책을 연계·적용하기 위한 '권한 정책의 출발점'으로 작동하며, 특히 부서 이동, 직무 변경, 장기 휴직 등 사용자 속성의 변화가 발생할 경우 이를 신속하게 연동 시스템에 반영할 수 있어야 한다. 이를 통해 불필요한 권한 유지, 휴면 계정 방치 등으로 발생할 수 있는 보안 리스크를 사전에 차단할 수 있다.

또한, HR 시스템은 사용자 데이터를 기반으로 한 RBAC(역할 기반 접근제어) 및 ABAC(속성 기반 접근제어) 정책 설계의 핵심 기반이 되며, 이는 제로트러스트의 '최소 권한 원칙'을 실현하는 데 필수적인 요소다. 특히 최근에는 HR 시스템에 저장된 데이터를 기반으로 머신러닝을 활용한 권한 적정성 평가, 초과 권한 자동 탐지 등 지능형 접근 제어 기능의 정확도를 높이는 데 사용하고 있다.

결과적으로 HR 시스템은 보안 시스템과 별도로 존재하는 관리 시스템이 아니라, 제로트러스트 보안 체계 전반에 데이터를 공급하고 사용자 행위를 통제하는 핵심 정보 연계 시스템으로 기능해야 한다. HR 정보의 정확성과 시의성은 사용자 권한 설정의 정확도뿐 아니라 전체 보안 정책의 실효성을 결정짓는 요인으로 작용하며, 이를 위한 체계적인 연동 구조와 지속적 데이터 정합성 확보가 무엇보다 중요하다.

식별자·신원 필러의 각 시스템은 단순한 기능 단위를 넘어, 제로트러스트 아키텍처를 기술적으로 구현하는 실질적인 수단으로 작동한다. SSO, IAM, MFA, AD, HR 시스템은 서로 독립된 기능을 수행하면서도 상호 유기적으로 연계하여, 사용자 식별부터 인증, 권한 부여, 활동 모니터링에 이르기까지 전 과정에 걸친 통합 보안 통제를 가능하게 한다.

이로써 조직은 물리·가상·클라우드 등 다양한 환경에서도 일관되고 정밀한 신원 기반 접근 제어를 구현할 수 있으며, 다양한 보안 위협 환경 속에서도 신뢰 중심의 보안 전략을 지속 가능하게 유지할 수 있다.

결국 제로트러스트의 핵심 원칙인 '지속적인 검증'과 '최소 권한 부여'는 이러한 시스템들을 통해 구체적으로 구현되며, 이는 조직의 보안 전략을 이론적 구상에 머물게 하지 않고, 실제 환경에서 적용 가능하고 운영 가능한 수준으로 끌어올리는 기반이 된다.

■ 맺음말

제로트러스트 아키텍처에서 식별자(Identity)는 모든 보안 전략의 시작점이자, 사용자와 엔터티에 대한 신뢰를 평가하고 검증하는 중심 축이다. 사용자, 기기, 서비스 계정 등 다양한 주체에 대한 정확한 식별과 지속적인 신뢰 평가가 수반되지 않는다면, 제로트러스트의 핵심 원칙인 '지속적인 검증'과 '최소 권한'은 형식적인 구호에 그칠 수밖에 없다.

식별자 필러의 주요 시스템인 SSO, IAM, MFA, AD, HR 시스템은 단순히 개별 기능을 수행하는 시스템이 아니라, 식별자 기반 통제 체계를 구성하는 유기적이고 상호 보완적인 보안 인프라다. 이들 시스템은 사용자 정보를 생성하고 검증하며, 이를 바탕으로 접근 권한을 부여하고, 이상 행위를 탐지해 실시간으로 정책을 조정하는 등, 제로트러스트 환경에서 요구되는 핵심 보안 통제 기능을 분산 수행한다.

특히 식별자 필러는 사용자 신원과 권한에 대한 데이터 흐름을 제어하고 연결하는 '허브' 역할을 수행하며, 다른 모든 필러의 기반을 제공한다. 식별자 필러가 정교하게 설계되고 운영될 경우, 조직은 사용자 단위의 통제는 물론, 디바이스, 네트워크, 애플리케이션, 데이터 등 제로트러스트 아키텍처 전 영역에 걸쳐 일관된 보안 정책을 적용할 수 있는 구조적 기반을 확보하게 된다. 반대로 식별자 필러가 허술하게 구축되면, 권한 오남용, 비인가 접근, 내부자 위협에 대한 감시가 어려워지고, 전체 보안 체계의 연속성 역시 약화될 수 있다.

또한 식별자·신원 기반 통제가 견고하게 작동할수록, 조직은 보안 사고에 대해 보다 안전한 상태를 유지할 수 있다. 이는 단순히 사고를 예방하는 수준을 넘어, 사고 발생 시 원인 분석과 사용자 이력 추적, 포렌식까지 신속하게 수행할 수 있는 기반이 된다는 점에서 중요하다. 이러한 정보는 사고 대응과 재발 방지, 정책 보완 등 보안 운영 전반에 실질적인 효과를 제공한다.

식별자 필러는 단순한 인증 기능이 아니라, 제로트러스트 아키텍처 전반을 실질적으로 작동시키는 '기반 필러'이자 '보안 전략의 관문'이다. 조직은 이 영역을 전략적으로 우선 구축하고, 이를 토대로 다른 필러로 확장하는 단계적 접근을 통해 리스크를 통제 가능한 수준으로 줄이고, 신뢰 기반의 디지털 보안 환경을 실현할 수 있을 것이다.

■ 참고 문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] DoD, “Zero Trust Overlays”, 2024.06

[3] 과학기술정보통신부/KISA, “제로트러스트 가이드라인 V1.0”, 2023.06

[4] 과학기술정보통신부/KISA, “제로트러스트 가이드라인 V2.0”, 2024.12

[5] SK쉴더스, “2025 보안 위협 전망 보고서”

[6] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” - 브로슈어

[7] SpyCloud, “2025 Identity Exposure Report”

[8] Gatner, "Predicts 2024: AI & Cybersecurity - Turning Disruption Into an Opportunity"

[9] SC Media, "How attackers outsmart MFA in 2025"

[10] Sosafe, "MFA Fatigue Attack"

EQST INSIGHT

2025.05

SK쉴더스

SK쉴더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 SK쉴더스 EQST사업그룹
제 작 SK쉴더스 마케팅그룹