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
06

SK 쉴더스

Contents

Headline

위협 중심 보안 전략의 핵심 도구: Rule Framework

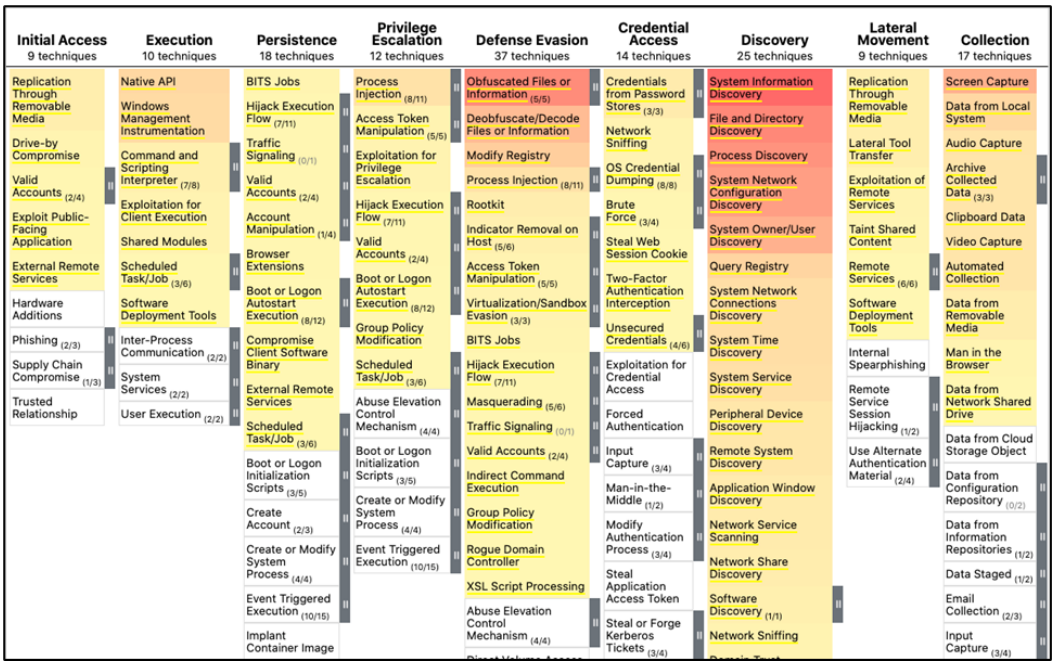
MSS 사업그룹 관제 CERT 팀 서기택 팀장

■ 지능형 위협의 시대

사이버 보안은 이제 단순한 IT 이슈가 아니라 조직의 생존과 직결된 전략적 과제가 되었다. 특히 지능형 지속 위협(APT : Advanced Persistent Threat), 공급망 공격, 랜섬웨어(Ransomware)와 같은 고도화 된 공격은 전 세계의 주요 기업과 공공 기관을 위협하고 있다. 이에 따라 보안 패러다임은 전통적인 예방 중심의 모델에서 위협 탐지 및 대응 중심으로 정보보안을 위한 전략적 이동이 이루어지고 있다. 이 변화의 중심에 탐지룰(Detection Rule-Set) 또는 방법론의 고도화가 큰 비중을 차지하고 있으며, 대표적인 보안 전략 모델로 MITRE ATT&CK 프레임워크가 존재한다. ATT&CK 프레임워크는 공격자의 실제 행위를 기반으로 구성된 지식 베이스로 위협 중심 보안 전략을 효과적으로 수립할 수 있는 기반을 제공한다.

■ MITRE ATT&CK 프레임워크란 무엇인가?

MITRE ATT&CK 는 Adversarial Tactics, Techniques and Common Knowledge 의 약자로 공격자들이 실제로 사용하는 전술(Tactics), 기술(Techniques), 절차(Procedures)을 체계적으로 분류한 지식 기반 매트릭스이다.



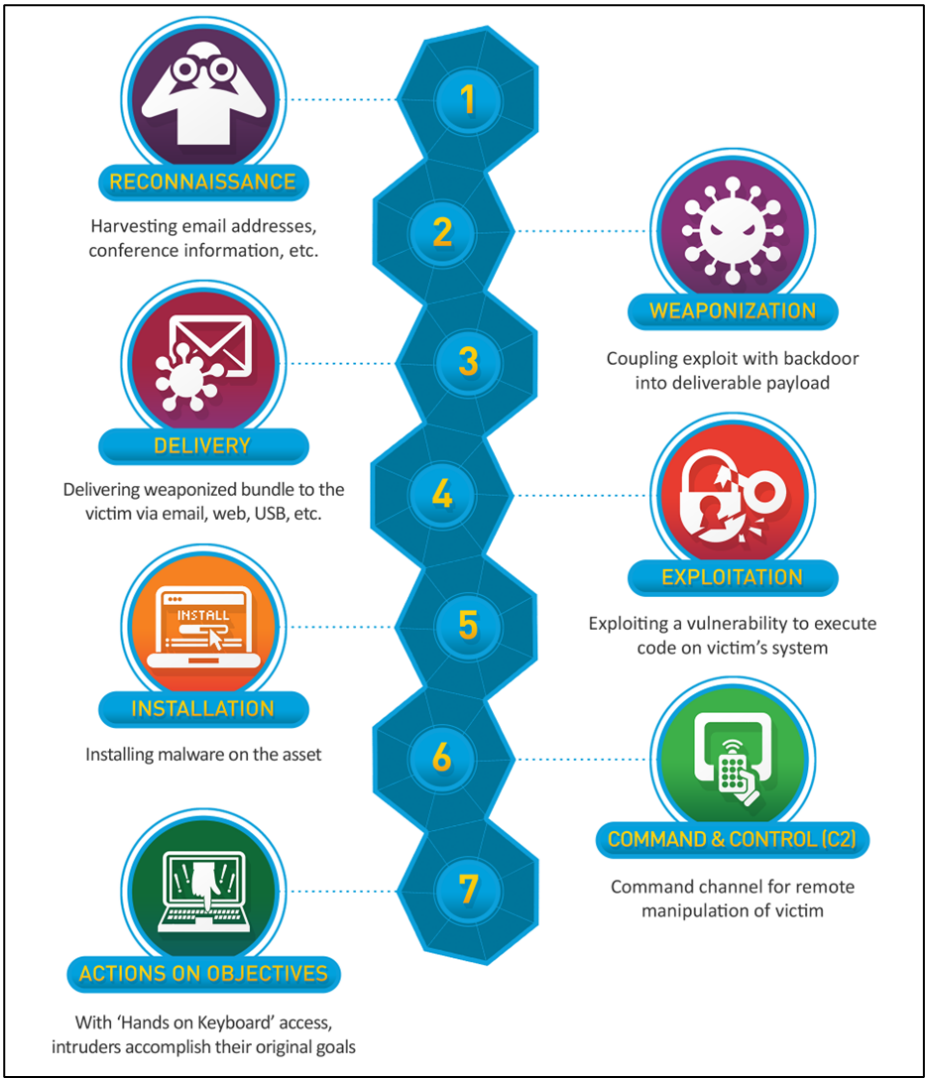
* 출처: MITRE ATT&CK 공식 홈페이지

그림 1. MITRE ATT&CK Metrix - Navigator 중 일부 발췌

공격은 일반적으로 일련의 단계적 행위를 기반으로 진행되며 각 단계는 특정한 전술과 기술로 구분된다. 예를 들어, 공격자는 먼저 초기 접근을 시도하고 그 다음 권한 상승, 내부 정찰, 명령 및 제어(C2), 데이터 유출 등의 단계를 거친다. MITRE ATT&CK 프레임워크는 이러한 각 단계에 따라 공격을 분류하고 기술에 대한 상세 설명과 탐지 지표, 완화 전략 등을 제공한다. 현재 Enterprise, Mobile, ICS 세 가지의 매트릭스를 제공하며 기업 보안, 산업 제어 시스템 보안, 모바일 보안 등 다양한 환경에 적용이 가능하다.

■ MITRE ATT&CK 프레임워크 전술과 기술(TTPs)의 구성

MITRE ATT&CK 프레임워크의 핵심은 공격자의 행동을 단계적으로 모델링한 전술(Tactics)과 그 단계에서 사용되는 구체적인 기술(Techniques)로 구성되어 있다는 점이다. 이 프레임워크는 공격자가 사이버 공격을 수행할 때, 어떤 목표를 가지고 어떤 방식으로 접근하는지를 설명하며 이를 통해 조직은 실제 위협 시나리오를 구조적으로 분석할 수 있다.



* 출처: Lockheed Martin 공식 페이지

그림 2. Lockheed Martin 에서 공개한 Cyber Kill Chain 모델

위 [그림 2]와 같이 사이버 위협 행위는 단계적으로 진행된다. 각 단계에 대해 조금 더 자세히 살펴보면, 가장 먼저 공격자는 시스템에 접근하기 위한 '초기 접근(Initial Access)' 단계를 시도한다. 이는 피싱 이메일, 악성 링크, 알려진 사용자 권한 등 사용자의 행위나 외부 접점의 취약점을 노리는 방식으로 나타난다. 이 단계의 목적은 내부 네트워크로 진입할 수 있는 발판을 마련하는 것이다. 다음은 '실행(Execution)' 단계로 공격자가 진입한 후 악성 코드를 실행하여 시스템 제어권을 확보하려는 시도이다. 여기에는 스크립트 실행, 명령어 삽입, 프로세스에 대한 오용 등이 포함된다. 이 과정은 시스템 내에서 공격자가 실제로 악성 행위 등을 동작하도록 만드는 관문이다.

'지속성(Persistence)'은 공격자가 시스템에 장기적으로 머물기 위해 설정하는 메커니즘을 의미한다. 시스템 재부팅이나 사용자 로그아웃 이후에도 공격 코드가 계속 작동할 수 있도록 서비스 등록이나 자동 실행 프로그램 설치 등의 방법이 사용된다. 다음 단계로는 '권한 상승(Privilege Escalation)'으로 정의되며 일반 사용자 권한을 관리자 또는 루트 권한으로 상승시켜 더 넓은 범위의 시스템 접근을 가능하게 만든다. 이후 '방어 회피(Defense Evasion)' 단계에서는 보안 솔루션이나 로그 시스템 등을 우회하거나 무력화시키는 기술이 사용된다. 예를 들어, 악성 파일을 난독화 한다거나 백신 우회를 위한 코드 인젝션 등의 기술이 여기에 해당된다. 이는 탐지를 피하고 지속적인 공격을 가능하게 만드는 중요한 단계이다. '자격 증명(Credential Access)' 단계에서는 공격자가 시스템 내에서 사용자 ID 나 비밀번호를 수집하여 다른 시스템으로 이동하거나 권한을 획득하려고 한다. 이는 메모리에서 비밀번호 해시를 추출하거나 키로거 등을 설치하여 수행된다. '발견(Discovery)' 단계는 내부 네트워크의 구조, 사용자 목록, 시스템 정보 등을 파악하는 과정이다. 공격자는 이 정보를 활용해 다음 공격 단계를 계획하거나 측면 이동(Lateral Movement)의 경로를 설정한다.

악성 행위가 본격적으로 확산되는 단계가 '측면 이동(Lateral Movement)' 단계이다. 이는 공격자가 하나의 시스템에서 다른 시스템으로 이동하는 행위로 자격 증명 도용이나 원격 명령어 실행 등이 주요 수단으로 사용된다. 이 과정을 통해 공격자는 핵심 시스템에 점차 접근하게 된다. 공격의 목적이 구체화되면, '수집(Collection)' 단계가 시작된다. 이때 공격자는 특정 데이터 예컨대 문서, 고객 정보, 인증서, 로그 파일 등을 수집하여 향후 유출이나 조작을 위해 저장한다. 수집된 정보를 외부로 보내는 과정이 '명령 및 제어(Command and Control, C2)' 단계다. 공격자는 악성 소프트웨어를 통해 외부 C2 서버와 연결하고 명령을 주고받거나 데이터를 전송한다. 보통 암호화 된 통신이나 정식 프로토콜을 위장한 전송 방식이 사용된다.

공격의 최종 단계는 '영향(Impact)'으로 이는 시스템의 가용성 저해, 데이터 훼손, 랜섬웨어 감염 등 실제 피해를 일으키는 부분이다. 공격자는 이 시점에 데이터 삭제, 시스템 파괴, 금전 요구 등의 목적을 달성하려 한다.

이처럼 MITRE ATT&CK 의 전술(Tactics)과 기술(Techniques) - TTPs 은 공격의 각 단계를 논리적으로 설명하며 실제 공격자들의 사고방식과 행동 양식을 추적하고 분석할 수 있도록 돕는다. 이를 통해 위협 대응 조직은 각 단계별 방어 전략을 수립하고 탐지 룰, 대응 시나리오 등을 보다 정교하게 구성할 수 있다.

■ APT 공격 사례 분석

실제 공격 사례를 통해 ATT&CK 프레임워크의 전략과 기술을 실무에 적용하여 이해할 수 있다.

- APT29 (Cozy Bear)

SolarWinds 공급망 공격에서 DLL Side-Loading(T1574.002), 정당한 프로세스 내 악성 코드 삽입(T1055) 등의 기술 사용

- Lazarus Group

금융 기관 공격에 피싱(T1566.001), 권한 탈취(T1003), SMB 를 통한 측면 이동(T1021.002) 등 전술적 조합 수행

- FIN7

POS 시스템 대상 악성 문서 배포(T1203), 정보 수집(T1005), 외부 서버로 데이터 전송(T1041)

위의 사례에서 각 공격 흐름은 MITRE ATT&CK 기술과 전술로 상세하게 매핑되며 이를 바탕으로 공격 재현 또는 탐지 정책 수립이 가능하다. 단순히 공격자 그룹이 사용한 기술을 나열하는 데 그치지 않고 그들의 공격 흐름 전체를 '전술-기술(TTPs) 체계'로 매핑하여 각 단계에서 어떤 탐지와 대응이 가능했는지를 시각화 할 수 있다.

- Lazarus Group: 금융기관 및 암호화폐 거래소 공격

북한과 연계된 것으로 알려진 Lazarus Group 은 금융기관 및 암호화폐 거래소를 집중적으로 노려온 APT 조직이다. 이들은 피싱 메일, 소셜 엔지니어링, 웹 취약점 등을 통해 초기 접근(Initial Access)에 성공한 후 자격 증명(Credential Access)을 탈취하고 측면 이동(Lateral Movement)을 통해 주요 자산 시스템에 접근하는 방식으로 활동한다.

MITRE ATT&CK 프레임워크로 분석해보면, Lazarus 의 피싱 공격은 T1566.001 (Spear phishing Attachment) 기술로 식별된다. 이후 권한 상승은 T1068 (Exploitation for Privilege Escalation), 자격 증명 탈취는 T1003 (Credential Dumping) 기술로 분류된다. 이 그룹은 또한 RDP 연결을 통해 내부 시스템에 접근(T1021.001)하고 외부 C2 서버로 민감 정보를 유출(T1041)했다. 실제 정보보안 실무에서는 이러한 연계 분석을 통해 Lazarus 가 사용하는 전술 및 기술의 시퀀스를 탐지 정책에 반영할 수 있으며, 위협 헌팅(Threat Hunting)의 기준점으로 삼을 수 있다.

표 1. 공격 사례에 대한 MITRE ATT&CK 프레임워크 적용 분석의 예

APT 사례에서 보듯이 MITRE ATT&CK 프레임워크는 이러한 복잡한 공격 흐름을 전술적으로 구조화함으로써 어디서부터 공격이 시작되었고 어떤 기술이 사용되었는지 그리고 어떤 단계에서 탐지 및 방어가 가능했는지를 명확히 파악할 수 있도록 돕는다. 또한 과거 공격 사례를 기준으로 사전 탐지 룰을 구성하거나 위협 헌팅(Threat Hunting) 시나리오를 개발하는 데 효과적인 도구로 활용 가능하다.

■ 시큐디움 센터(Secudium Center) – Rule Framework

Rule Framework 는 단순한 이론적 도구를 넘어 실제 보안 조직이 공격자의 행동을 체계적으로 이해하고 대응 역량을 강화하는데 매우 중요한 역할을 한다. SK 쉴더스 원격관제 서비스를 담당하고 있는 Secudium Center 에서는 관제 플랫폼 “Secudium v2.0”에 MITRE ATT&CK 프레임워크를 이용한 독자적인 Rule Framework 를 적용하였다. 적용된 프레임워크 구조는 큰 카테고리에서 9 단계로 구성되며, 필수 정보와 선택 정보로 수집 정보를 분류하여 위협 식별 및 대응에 유기적으로 적용 가능한 탐지 전략을 채택하였다.

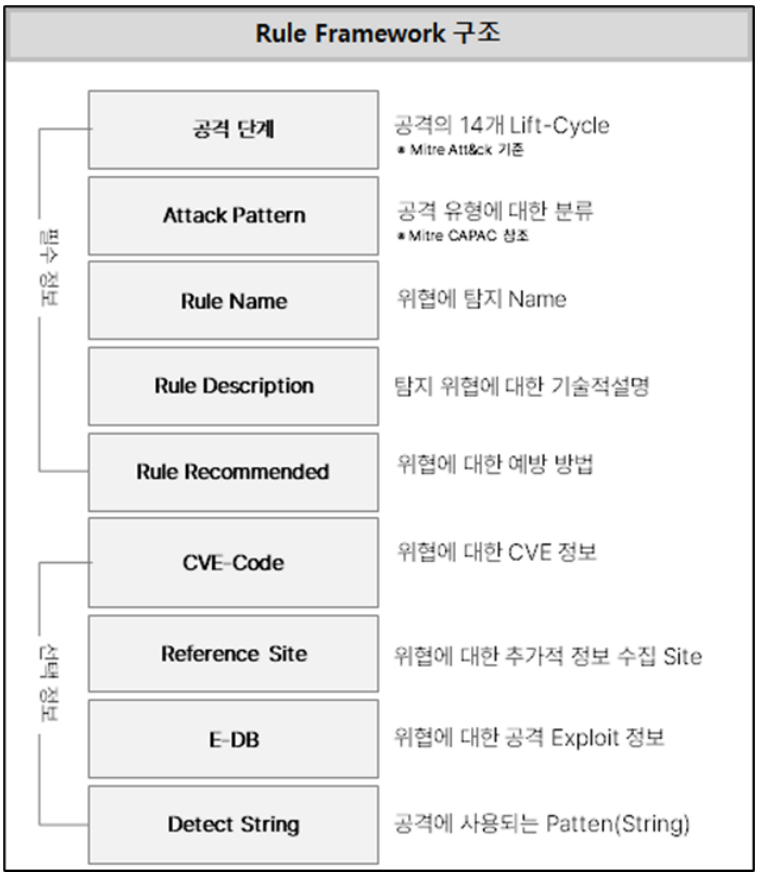


그림 3. Secudium 관제 플랫폼에 적용된 Rule Framework 구조

해당 Rule Framework 를 통해 수집되는 위협 로그를 탐지/분류하여 적절한 대응 기술이 적용된 위협 대응 체계를 구축하는 것이 해당 프레임워크를 활용하는 것의 핵심이다. 또한 위협 헌팅(Threat Hunting)의 구체적인 Feature 를 선정하여 공격자가 사용하는 기술을 선제적으로 탐지해 피해 확산을 방지하고 공격 초기 단계에서 대응 가능성을 높이는데 활용할 수 있다.

지능화 된 사이버 공격에 대항하는 정보 보안의 성공 열쇠는 '체계적 통합과 반복 개선'이다. 이런 관점에서 Rule Framework를 활용한 탐지 방법론을 정의하는 것은 단순히 새로운 도구를 추가하는 것이 아니라, 보안 운영 전반을 위협 중심의 대응 체계로 재설계하는 과정이다. 전략과 기술을 활용하여 체계적으로 분류 운영하고 반복적인 위협 가능성을 탐색하는 활동을 병행 할 때, 공격자보다 한 발 앞서 방어하는 "능동적 보안 체계"를 구축 할 수 있을 것이다.

■ 참고 자료

[1] MITRE ATT&CK: https://attack.mitre.org

[2] Red Canary: https://redcanary.com

[3] Mandiant Threat Intelligence Reports

[4] Atomic Red Team: https://github.com/redcanaryco/atomic-red-team

[5] Lockheed Martin – cyber kill chain: https://www.lockheedmartin.com

Keep up with Ransomware

Devman: 하나의 그룹, 여러 랜섬웨어

■ 개요

2025 년 5 월 랜섬웨어 피해 사례 수는 지난 4 월(550 건)에 비해 약 12% 감소한 484 건을 기록했다. 지난 3 월부터 매달 꾸준히 피해 사례 수가 감소하고 있는 추세지만, 5 월에 Vanhelsing 랜섬웨어의 소스코드가 공개돼 이를 악용한 변종이나 그룹이 등장할 가능성이 높아졌다.

5 월 초, LockBit 의 다크웹 유출 사이트가 "Don't do crime CRIME IS BAD xoxo from Prague"라는 문구와 함께 변조됐다. LockBit 의 경우 다크웹 유출 사이트가 변조뿐만 아니라 관리자 패널도 해킹을 당해 내부 데이터베이스 파일 일부가 유출됐다. 유출된 데이터베이스에는 가상화폐 지갑 주소, 랜섬웨어 버전 별 사용된 구성 정보, 제휴사 계정 정보, 채팅 내역 등이 포함되어 있었으며 복호화에 사용되는 개인키는 포함되어 있지 않았다. 이번 해킹 사태로 인해 평판이 훼손됐음은 물론, 6 월 초까지 다크웹 유출 사이트가 오픈 되지 않고 있는 상태로 보아 운영에 큰 차질이 생긴 것으로 보인다.

러시아 해킹 포럼 RAMP 에서 Vanhelsing 랜섬웨어의 소스코드가 공개됐다. 이전 멤버인 th30c0der 가 Vanhelsing 랜섬웨어의 소스코드를 판매한다는 글을 포럼 관련 사이트에 업로드한 것이다. Vanhelsing 운영진이 이를 인정하며 자신들의 기존 랜섬웨어와 패널 페이지 소스코드 일부를 공개했다. 하지만 th30c0der 는 자신이 패널부터 결제 시스템, 랜섬웨어를 개발한 핵심 인물이라고 소개하며, 공개된 코드가 전체 코드가 아니며 자신이 판매하고 있는 소스코드가 최신 버전이라고 주장하고 있다.

한편 Qilin 랜섬웨어의 복호화 도구로 추정되는 파일이 발견되기도 했다. 해당 샘플은 암호화된 파일을 AES 알고리즘이나 ChaCha20 알고리즘으로 복호화하는 기능을 제공한다. 다만, 모든 Qilin 랜섬웨어를 대상으로 복호화를 제공하진 않고, 특정 버전 혹은 특정 암호화 키로 암호화된 경우에만 정상적으로 복호화되는 것으로 확인됐다.

5 월에는 국내 침해 사례가 여러 건 확인됐다. RaLord 로 활동을 시작해 5 월에 리브랜딩한 Nova 그룹이 국내 대학교를 공격해 내부 문서, 보고서, 포털 사이트 소스코드, 데이터베이스, 학생 정보 등을 탈취했다고 주장했다. 6 월에는 탈취한 데이터가 공개됐으나, 개인 정보는 포함되지 않았으며, 포털 사이트 소스코드와 데이터베이스 관련 정보만 확인됐다.

TCR Team 은 국내 금융과 제조 분야의 기업 2 곳을 공격했다. 다크웹 유출 사이트에선 협상에 실패한 기업으로 분류되어 일부 데이터가 함께 공개됐다. 확보한 정보에는 내부 문서와 직원 개인 정보가 포함되어 있는 것으로 확인되었으나 약 2 주뒤에 공개된 데이터는 내려갔으며, 5 월 말에는 다크웹 유출 사이트가 비활성화 되어 접속이 불가능한 상태이다.

SAP 의 애플리케이션 통합 및 실행 플랫폼 NetWeaver 에서 발생한 파일 업로드 취약점(CVE-2025-31324)을 악용한 랜섬웨어 그룹이 확인됐다. 해당 취약점은 4 월 24 일 패치 됐으나 BianLian 그룹과 RansomEXX 그룹이 이를 악용한 정황이 확인됐다. 두 그룹 모두 랜섬웨어를 배포하진 않았으나, 취약점을 악용해 BianLian 의 C2[1] 서버와 통신하거나 RansomEXX 가 주로 사용하는 백도어[2] PipeMagic 을 배포하는 등의 행위가 포착됐다.

[1] C2: 악성코드에 감염된 PC 나 서버를 대상으로 공격자가 원하는 행위를 하도록 하는 명령을 하달하는 서버

[2] 백도어: 보안 시스템이나 인증 절차를 우회하여 대상 시스템에 접근할 수 있도록 하는 악성코드

■ 랜섬웨어 뉴스

LockBit 그룹, 내부 데이터베이스 유출

- 유출된 정보에 따르면 4월 말 해킹됐으며 5월 초 정보 공개
- “Don’t do crime CRIME IS BAD xoxo from Prague” 문구와 함께 내부 데이터베이스 일부 유출
- Everest 그룹의 해킹과 동일한 자의 소행으로 추정

Qilin 랜섬웨어 복호화 도구 발견

- Qilin 랜섬웨어로 암호화된 파일을 AES / ChaCha20 알고리즘 중 해당하는 알고리즘으로 복호화
- 모든 버전의 Qilin 랜섬웨어를 대상으로 복호화가 가능하진 않으며, 특정 버전 혹은 키에 해당하는 경우만 정상 동작

Vanhelsing 랜섬웨어 소스코드 공개

- “th30c0der”라는 유저가 5월에 RAMP 포럼에서 소스코드 판매
- Vanhelsing 운영진은 실제 함께 일한 유저임을 인정했으며, 자신들의 랜섬웨어 소스코드를 공개
- “th30c0der”는 공개된 코드가 v1에 해당하며, 자신은 최신 버전인 v2를 판매하고 있다고 주장

TCR Team 그룹, 국내 기업 2곳 공격

- 금융 및 제조업에 해당하는 기업을 공격해 데이터 탈취 및 공개
- 내부 문서와 직원 개인 정보가 포함된 데이터가 일부 공개
- 5월 말에 다크웹 유출 사이트가 비활성화되며 더 이상 접근 불가

Nova 그룹, 국내 대학교 공격

- 국내에 소재한 대학교를 공격해 내부 문서, 소스코드, 학생 정보 등을 탈취했다고 주장
- 6월 초 데이터가 공개됐으나 개인 정보는 포함되지 않았으며, 포털 사이트 소스코드와 데이터베이스가 포함

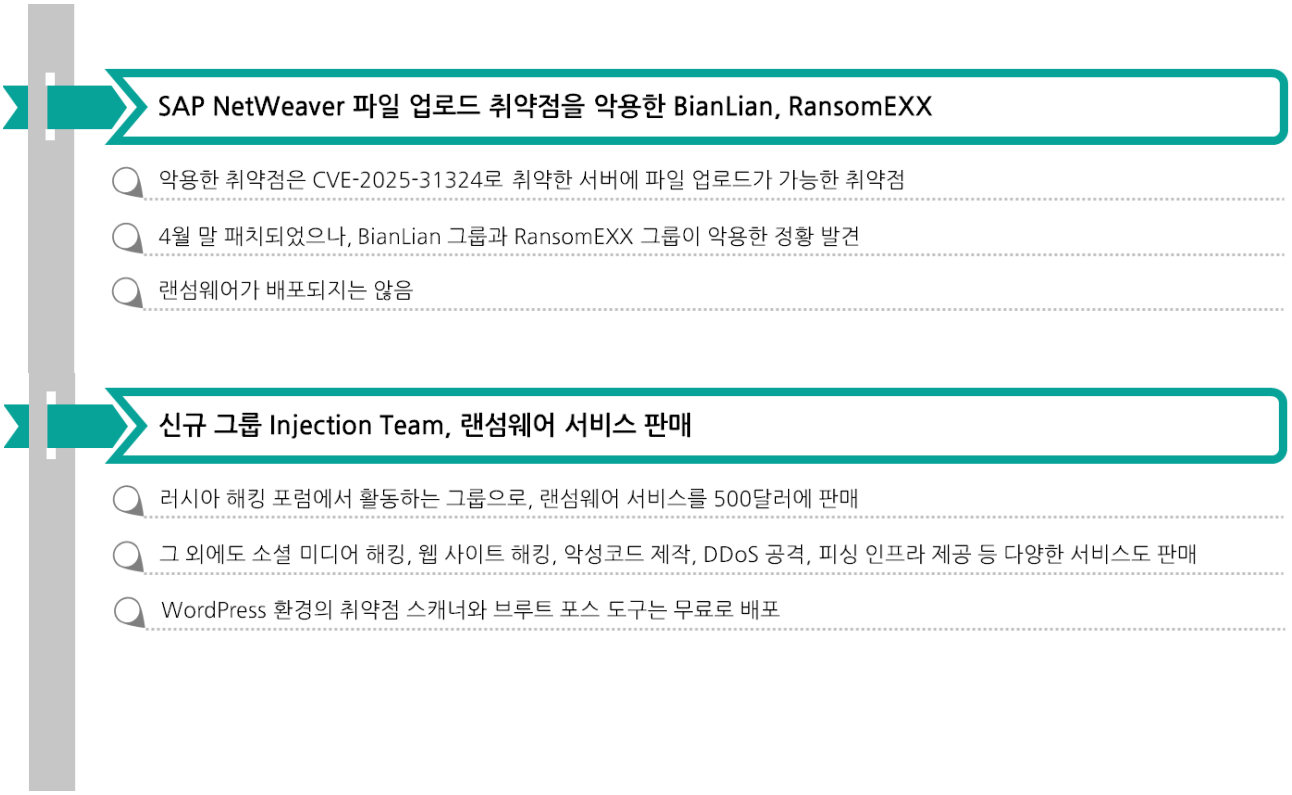

SAP NetWeaver 파일 업로드 취약점을 악용한 BianLian, RansomEXX
악용한 취약점은 CVE-2025-31324로 취약한 서버에 파일 업로드가 가능한 취약점
4월 말 패치되었으나, BianLian 그룹과 RansomEXX 그룹이 악용한 정황 발견
랜섬웨어가 배포되지는 않음
신규 그룹 Injection Team, 랜섬웨어 서비스 판매
러시아 해킹 포럼에서 활동하는 그룹으로, 랜섬웨어 서비스를 500달러에 판매
그 외에도 소셜 미디어 해킹, 웹 사이트 해킹, 악성코드 제작, DDoS 공격, 피싱 인프라 제공 등 다양한 서비스도 판매
WordPress 환경의 취약점 스캐너와 브루트 포스 도구는 무료로 배포

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

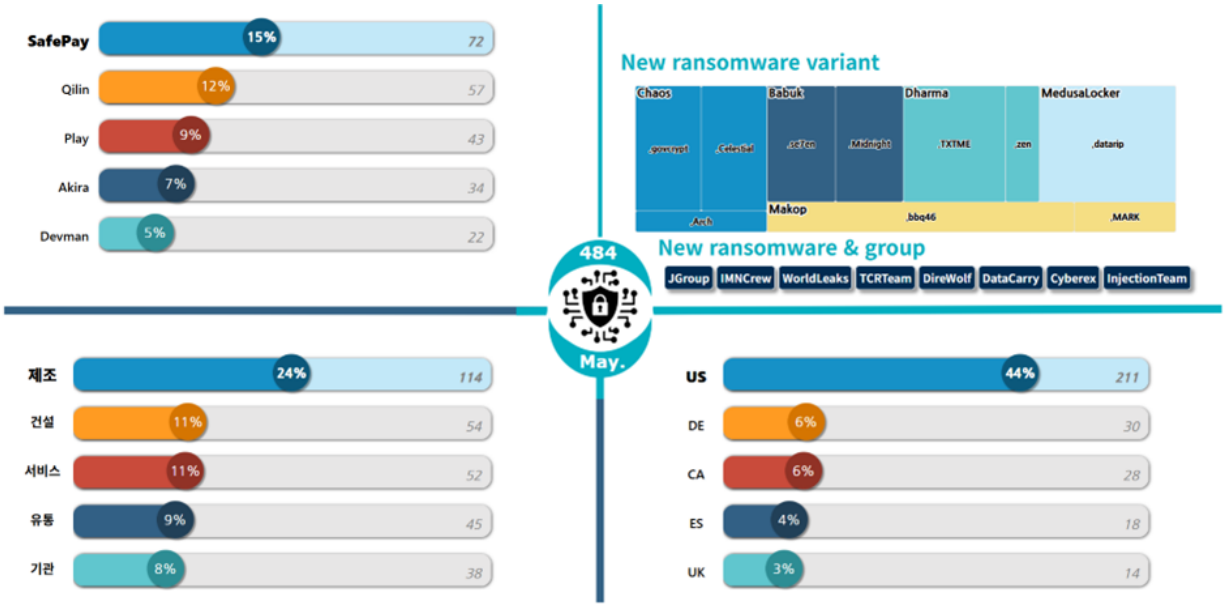


그림 2. 2025 년 5 월 랜섬웨어 위협 현황

새로운 위협

5 월에는 총 8 개의 신규 랜섬웨어 그룹이 확인됐다. JGroup 은 18 건, Imncrew 는 8 건, WorldLeaks 는 14 건, Direwolf 는 11 건, DataCarry 는 10 건 등 자체 다크웹 유출 사이트에 신규 피해자를 각각 업로드한 것이 확인됐다. 또한 Cyberex 그룹은 별도의 유출사이트를 운영하지 않고 채팅 사이트만 존재해, 감염된 피해자에게 몸값 협상을 진행하고 있다.

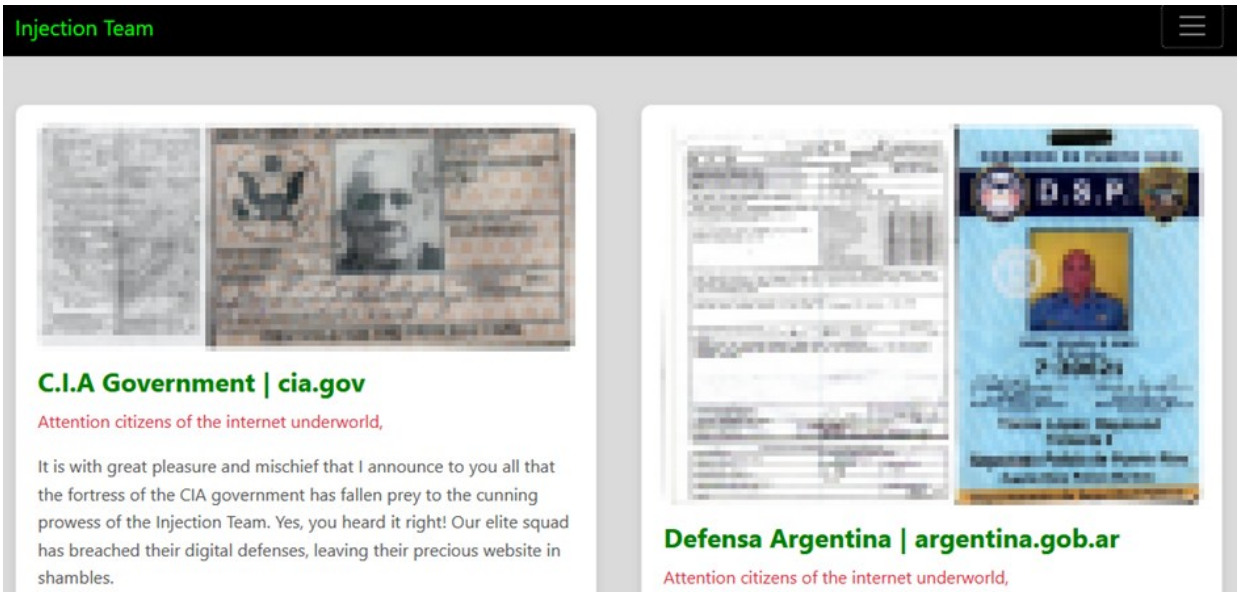


그림 3. InjectionTeam 다크웹 유출 사이트

신규 Injection Team 그룹은 러시아 해킹 포럼에서 자신들을 홍보하고 있는 그룹이다. 랜섬웨어 서비스는 물론 소셜 미디어 해킹, 웹 사이트 해킹, 악성코드 제작, DDoS[3] 공격, 피싱 인프라 제공 등의 각종 서비스를 1,000 달러 내외로 제공하고 있다. 이러한 유료 서비스 외에도 WordPress 환경의 취약점 스캐너와, 브루트 포스[4] 도구를 무료로 배포하고 있다.

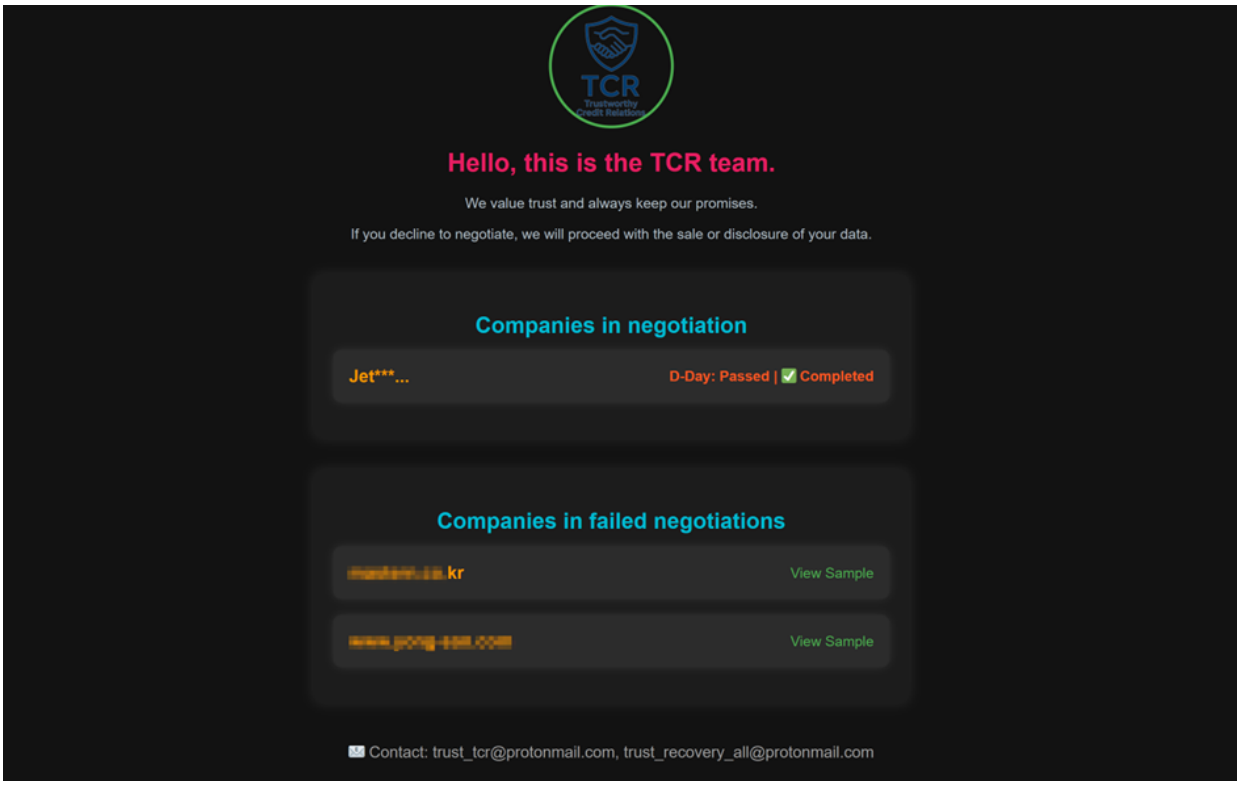


그림 4. TCR Team 다크웹 유출 사이트

국내를 공격한 신규 그룹도 확인됐다. TCR Team 그룹의 공격은 5 월 발견됐으며 국내 기업 2 곳을 공격해 일부 데이터를 공개했다. 피해 기업은 각각 금융 투자 기업과 자동차 부품 제조 기업으로 기업 내부 문서와, 직원 개인 정보가 포함된 문서들로 확인됐다. 5 월 말에는 샘플 데이터에 접근이 불가능해졌으며, 순차적으로 다크웹 유출 사이트 자체도 비활성화 됐다.

[3] DDoS (Distributed Denial of Service): 악의적으로 대상 네트워크, 서버, 온라인 서비스 등에 많은 트래픽을 발생시켜 해당 시스템의 기능을 정상적으로 사용하지 못하도록 하는 공격

[4] 브루트 포스(BruteForce): 조합 가능한 모든 경우의 수를 대입해보는 공격 기법

Top5 랜섬웨어

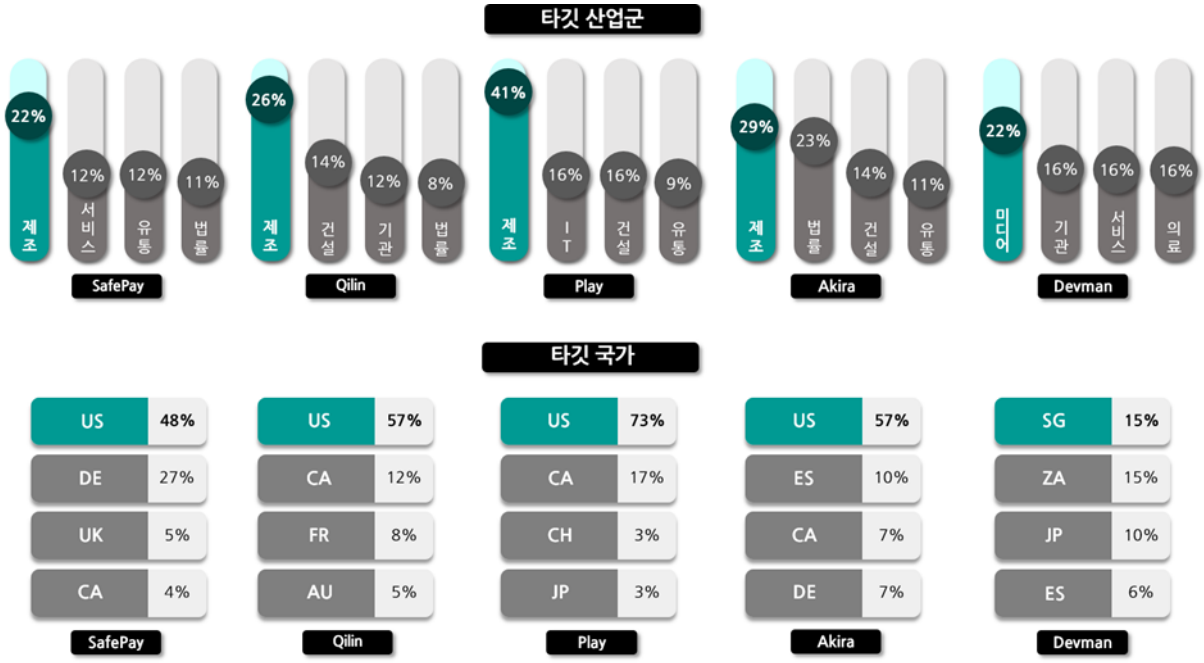


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

SafePay 그룹은 체코에 위치한 공립 고등학교 Gymnázium a Jazyková škola Zlín 을 공격해 30GB 가량의 내부 데이터를 공개했다. 해당 데이터에는 학교 내부 기록은 물론 학생의 정보가 일부 포함되어 있었다. 또한 호주의 법률 회사 RTB Legal 을 공격해 200GB 규모의 데이터를 탈취했으며, 이로 인해 법원 문서, 고객 정보, 이메일, 계약서, 유언장 등 다양한 법률 및 행정 문서가 유출됐다.

Qilin 그룹은 미국 조지아주 Cobb 카운티 정부를 공격해 약 150GB 크기의 40 만개의 문서를 탈취했다. 탈취한 데이터에는 주민 및 공무원 개인정보는 물론 사망자 이미지가 포함되어 있었다. 또한 미국의 컨트리 클럽 Army Navy Country Club 을 공격해 300GB 규모의 데이터를 탈취했으며, 이로 인해 회원의 이름, 주소, 신용카드 정보, 자격증명 등 민감 정보가 유출됐다.

Play 그룹은 미국의 기업을 집중적으로 공격하는 모습을 보이고 있다. 5 월에는 미국의 건설업체 W.E. Bowers 를 공격해 고객 문서, 예산, 급여 명세서, 회계 자료, 신분증, 재무 정보 등 다양한 데이터를 유출했으며, 구체적인 피해 규모는 공개되지 않았다. 또 다른 미국 건설업체 Greater Seattle Concrete 도 공격당했으며, 이로 인해 내부 문서와 기밀 정보가 포함된 데이터가 5 월 말 공개됐다.

Akira 그룹은 미국 에너지업체 Pacific Summit Energy 를 공격해 약 160GB 규모의 데이터를 탈취했다. 직원 개인 정보, 재무 감사 자료, 내부 업무 문서 등이 포함되어 있으며, 해당 데이터는 전부 공개됐다. 또한 미국의 금융 기관 Flagship Bank 를 공격해 고객 정보, 세부 재무 자료, 계약서 등이 포함된 40GB 규모의 데이터를 탈취해 공개했다.

4 월에 등장한 신규 그룹 Devman 은 케냐의 공공 연금 기구 NSSF Kenya 를 공격해 2.5TB 가량의 데이터를 탈취했다고 주장하고 있다. 자신의 X(트위터)를 통해서 인증 스크린샷을 지속적으로 업로드하고 있으며, 다크웹 유출 사이트에 정찰, 데이터 탈취, 파일 암호화 방식을 설명하기도 했다. 탈취한 데이터에는 이름, 주소, 사회보장번호와 같은 개인정보가 포함되어 있으며 몸값으로는 450 만 달러(한화 약 61 억원)을 요구하고 있다. 필리핀 매체 GMA Network 도 내부 서버가 암호화됐으며 65GB 가량의 데이터가 유출됐다. 몸값으로는 250 만 달러(한화 약 34 억원)을 요구하였으나 GMA Network 는 유출 데이터에 민감 정보나 개인 정보가 포함되지 않았다고 주장했다.

■ 랜섬웨어 집중 포커스

Welcome to Devman's Place

Soon there will be some news. Thanks for waiting.

WE ARE ACTIVELY BUYING ACCESS TO COUNTRIES(UK, FRANCE, CANADA). THESE COUNTRIES ARE OUR MAIN PRIORITY.

P.S sorry for being offline

My Victims

Company	Status	Ransom Amount
Doumen.fr(QILIN)	Negotiating	800k USD
Optimax Technology(QILIN)	Whaitng	590k USD
Texas Construction Firm(QILIN)	Pending	Amount TBD
Tawasol (APOS Attack)	Pedning	150k USD
Feel Four (QILIN Attack)	Pedning	60k USD
China Harbour (s) Engeneiring Company (Dragon Force Attack) FILE SAMPLE 1 avaliable /CHEC/CHECsample.zip	Ecnrypted(we encrypted every signle device on the network and downloaded 50gb of sensitive files)	450k USD
Honk Kong Victim (To be discoled)	(To be discoled)	(To be discoled)

그림 6. Devman 다크웹 유출 사이트

Devman 그룹은 25 년 4 월부터 활동을 시작한 그룹으로, 지금까지 총 44 건의 피해자를 게시했다. 처음 등장했을 때에는 “My Writeups” 페이지에 공격에 사용한 소프트웨어 취약점이나 취약한 패스워드 등을 공격 단계별로 상세하게 설명하는 독특한 모습을 보였다. 또한 자체 랜섬웨어가 아니라 다른 그룹의 랜섬웨어를 공격에 적극적으로 활용하며, 피해자가 Devman 유출 사이트뿐만 아니라 다른 랜섬웨어 그룹의 유출 사이트에도 함께 게시되기도 했다. 공격에 활용한 다른 그룹의 랜섬웨어는 Apos, Qilin, DragonForce, RansomHub 가 있으며, 5 월부터는 자체 랜섬웨어인 Devman 랜섬웨어를 악용한 피해자를 게시하기 시작했다.

Devman 그룹은 주로 X(트위터)에서 활동한다. 개발중인 랜섬웨어 서비스 페이지나, 공격 예고 글, 자체 제작 랜섬웨어 테스트 동영상 등 자신들을 과시하기 위한 용도로 주로 활용하고 있다. 또한 유출 규모가 큰 기업의 경우, 피해자의 X 계정을 직접적으로 언급하면서 확보한 샘플 이미지를 공개하거나 침투한 환경의 스크린샷을 공개하며 조롱하고 협박하는 모습도 확인됐다.

TBD GREECE	ALL FILES ENCRYPTED 120gb of data stollen	NEGOTIATION STARTED
TBD HONK KONG	ALL FILES ENCRYPTED	PAYED
TBD KOREA	ALL FILES ENCRYPTED	PAYED

그림 7. 일부 정보만 공개된 피해자 리스트

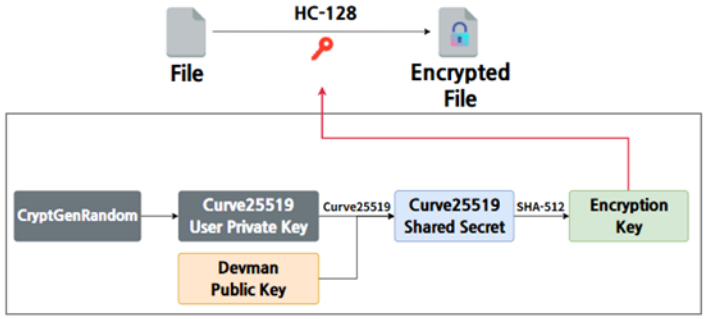
이들은 피해자를 공개할 때, 기업명을 바로 공개하지 않고 기업의 소속 국가나, 어떤 분야의 기업인지 우선적으로 공개하고 있다. 그 중에는 국내 기업도 포함되어 있으나, 정확한 피해 규모나 요구한 몸값은 공개되지 않고 이미 비용을 지불한 것으로 확인된다.

5 월에는 Devman 그룹의 자체 랜섬웨어로 추정되는 샘플이 발견됐으며, Devman 그룹이 자신들의 X 계정을 통해 해당 랜섬웨어가 v1 버전임을 인정하기도 했다. 다만 랜섬웨어가 지난 3 월 해킹당한 Mamona 랜섬웨어와 매우 유사해 비교 분석한 결과, 일부 기능이 추가된 버전으로 확인됐다. 6 월부터는 자체 랜섬웨어 서비스를 공개해 활동이 더 왕성해질 것으로 보여 이에 대비하고자 Devman 랜섬웨어를 분석한 내용을 공유하고자 한다.

Devman Ransomware

암호화 키

Curve25519 알고리즘으로 암호화 키를 생성하며 HC-128 알고리즘으로 암호화

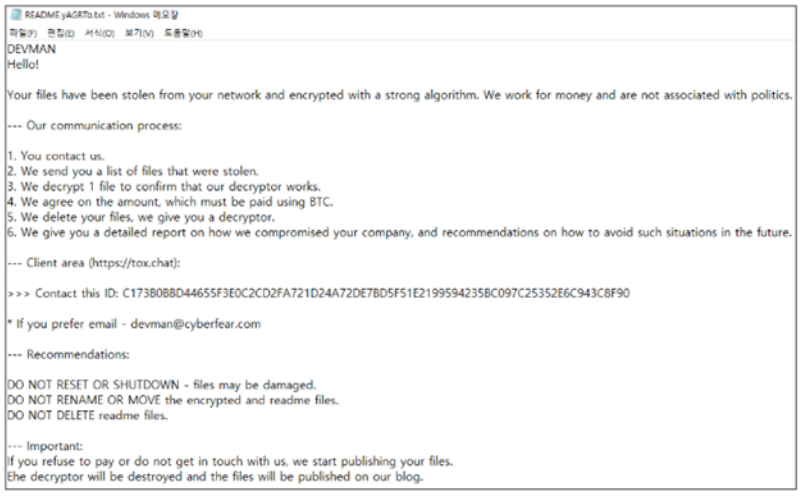


암호화 방식

* 암호화 방식 1.
1MB 이하: 전체 암호화
1MB 초과 5MB 이하: 파일의 첫 1MB 암호화
5MB 초과: 파일의 처음부터 파일 전체 크기의 N% 만큼 암호화(최대 70MB)
* 암호화 방식 2.
64Bytes 이하: 전체 암호화
64Bytes 초과 5MB 이하: 파일의 처음부터 전체 크기의 10%만큼 암호화
5MB 초과 20MB 이하: 파일 크기의 1/6 마다 첫 4KB 암호화
20MB 초과: 10MB 마다 첫 4KB 암호화

특징

랜섬노트



README.yAGRTb.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

DEVMAN
Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics.

--- 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 avoid such situations in the future.

--- Client area (https://tox.chat):

>>> Contact this ID: C173B0BBD44655F3E0C2CD2FA721D24A72DE78D5F51E2199594235BC097C25352E6C943C8F90

* If you prefer email - devman@cyberfear.com

--- Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

--- Important:
If you refuse to pay or do not get in touch with us, we start publishing your files.
Ehe decryptor will be destroyed and the files will be published on our blog.

README.yAGRTb.txt

변경 확장자

.yAGRTb

제작 언어

C/C++

그림 8. Devman 랜섬웨어 개요

Devman 랜섬웨어 전략

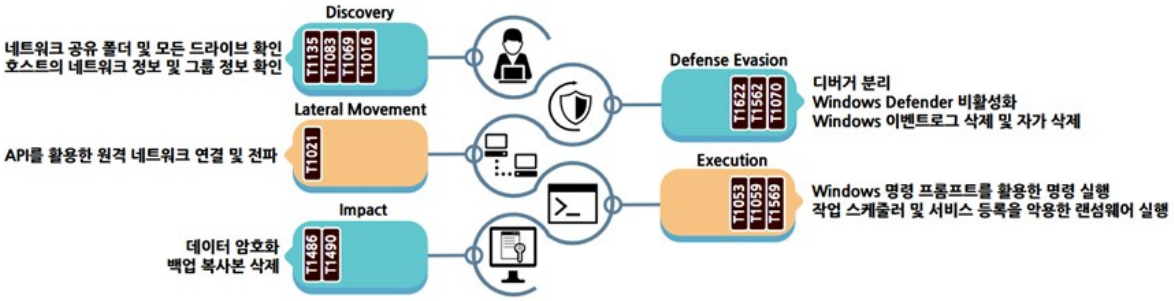


그림 9. Devman 랜섬웨어 공격 전략

Devman 랜섬웨어는 Mamona 랜섬웨어와 대부분의 기능이 동일하다. 차이점이 있다면 아이콘을 지정한 이미지 파일로 변경하거나, 디버거 분리를 위해 랜섬웨어를 재실행하는 기능 추가 그리고 대폭 개선된 네트워크 전파 부분이다. 변경점은 실행 인자에도 일부 반영됐다. Mamona 버전에서는 네트워크 인증을 위해서 NTLM[5] 해시를 전달하기 위한 인자 -H 가 Devman 버전에서는 삭제됐다. 또한 네트워크 전파 활성화를 위한 -ldap 인자와 네트워크 전파 대상을 지정하기 위한 -host, 디버거 분리 기능을 비활성화 하기 위한 -detached 인자가 함께 추가됐다.

구분	설명
-log	로그 출력
-keep	자가 삭제 비활성화
-skip-net	로컬 디스크만 암호화
-skip-local	네트워크만 암호화
-code {32Bytes key}	랜섬웨어 실행에 필요한 비밀번호
-sub {subnet}	네트워크 암호화 대상 네트워크 대역
-p {password}	네트워크 로그인 비밀번호
-u {username}	네트워크 로그인 이름
-time {HH:MM}	지정한 시각(HH:MM)까지 대기 후 실행
-delay {ss}	지정한 시간동안 대기 후 실행
-threads {int}	암호화 스레드 수 설정
-path {path}	특정 폴더 암호화
-host {ip_addr}	**특정 호스트 암호화**
-ldap	**네트워크 전파 활성화**
-detached	**랜섬웨어 재실행 비활성화**

표 1. Devman 랜섬웨어 실행 인자

[5] NTLM: 보안 인증 프로토콜 중 하나로, 인증을 위해 실제 암호 대신 해시를 전달해 권한 부여 및 인증을 제공하는 기능

Devman 랜섬웨어는 실행인자 외에도 암호화 관련 설정이나, 랜섬노트 내용, 키 생성에 필요한 공개키 등 각종 정보를 암호화한 채로 특정 세션에 저장하고 있으며, 이를 복호화해 사용한다. 확인된 정보는 아래와 같다.

오프셋	설명
config[0]	부분 암호화 비율
config[4]	랜섬노트 내용
config[2056]	자가 삭제 여부
config[2057]	이벤트 로그 삭제 여부
config[2058]	서비스 종료 여부
config[2059]	프로세스 종료 여부
config[2060]	랜섬웨어 비밀번호 검증 여부
config[2061]	암호화 모드 설정
config[2062]	랜섬노트 프린터 출력 여부
config[2064]	아이콘 변경 여부
config[2065]	네트워크 공유 자원 마운트 여부
config[2066]	랜섬웨어 비밀번호 (32Bytes)
config[2098]	암호화 확장자
config[2114]	Curve25519 공개키 (32Bytes)

표 2. Devman 랜섬웨어 설정값

랜섬웨어는 또한 복구 방지와 분석 방해를 위해 각종 기록이나 흔적을 삭제한다. 휴지통에 있는 데이터를 모두 삭제하며, 설정 값에 따라 Windows 환경의 모든 이벤트 로그를 삭제한다. 또한 명령 프롬프트 명령어를 활용해 백업 복사본을 삭제하며, 모든 파일 암호화가 끝난 뒤에는 랜섬웨어를 자체적으로 삭제한다.

명령어	설명
cmd.exe /c vssadmin delete shadows /all /quiet	백업 복사본 삭제
cmd.exe /C ping 127.0.0.7 -n 3 > Nul & Del /f /q \"%s\	자가 삭제

표 3. 삭제 관련 명령어

설정값에 서비스 종료나 프로세스 종료 관련 설정이 되어 있다면 원활한 파일 암호화를 위해 특정 서비스와 프로세스를 우선적으로 종료한다. 종료 대상 서비스 및 프로세스는 아래 표와 같다.

서비스	프로세스
WinDefend, SecurityHealthService, wscsvc, Sense, WdNisSvc, WdNisDrv, WdFilter, WdBoot, wdnisdrv, wdfilter, wdboot, mpssvc, mpsdrv, BFE, MsMpSvc, SepMasterService, wscsvc, SgrmBroker, SgrmAgent, EventLog	MsMpEng.exe, NisSrv.exe, SecurityHealthService.exe, smartscreen.exe, SecHealthUI.exe, MpCmdRun.exe, MSASCui.exe, MpUXSrv.exe, SgrmBroker.exe, MsSense.exe, SenseIR.exe, SenseCE.exe, SenseSampleUploader.exe, SenseNdr.exe,

표 4. 종료 대상 서비스 및 프로세스

서비스와 프로세스를 종료한 이후에는 네트워크에 랜섬웨어를 전파한다. 이는 -ldap 인자를 사용해야 실행되며, 추가적으로 -host 인자를 사용해 특정 호스트에만 전파를 시도하거나 -sub 인자를 사용해 특정 서브넷 대역의 모든 호스트에 전파할 수 있다. 기존 Mamona 버전에서는 IPC$[6] 를 통해서 네트워크 연결을 시도하며, 이를 위해서 -u, -H, -p 인자에 각각 로그인 아이디와 인증용 NTLM 해시, 로그인 비밀번호를 입력받는다. -H 로 인증용 해시 값을 받지만 실제 NTLM 인증은 진행하지 않으며, -u 인자와 -p 인자를 통해서 로그인을 시도한다. 만약 접속이 가능하다면, 별도의 랜섬웨어 전파 없이 해당 네트워크 공유 자원에 있는 파일을 암호화하는 방식을 사용한다.

```
  if ( log_flag )
  {
    print_log_sub_402730(Format: L"attempting hash auth to %s with user %s", v10, v11 + 568);
    v13 = v11 + 1608;
  }
  if ( !auth_ntlm_sub_406570(v10, lpUserName: (v11 + 568), v13) )
  {
    if ( log_flag )
      print_log_sub_402730(Format: L"hash auth failed, trying password auth");
LABEL_20:
    lpUserName = (v11 + 568);
    if ( !*(v11 + 568) || (lpPassword = (v11 + 1088), !*lpPassword) )
    {
      lpPassword = 0;
      lpUserName = 0;
    }
    if ( WNetAddConnection2W(lpNetResource: &cp, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0) )
      return HeapFree_wrp(lpMem: *(v1 + 4));
    WNetCancelConnection2W(lpName: Name, dwFlags: 0, fForce: 1);
  }
  if ( log_flag )
    print_log_sub_402730(Format: L"found accessible host: %s", *(v1 + 4));
```

그림 10. Mamona 랜섬웨어의 네트워크 인증 방식

[6] IPC$: 네트워크를 통해 다른 컴퓨터에 접근하려 할 때, 인증을 수행하기 위한 제어용 공유 폴더

Devman 랜섬웨어에서는 IPC$를 통해 네트워크 암호화를 시도하는 것이 아니라, LDAP[7] 을 활용해서 랜섬웨어를 전파하는 방식을 사용한다. -u 인자로 전달받은 로그인 아이디가 id@domain 형태라면 여기서 도메인 정보를 추출해서 사용하며, 해당 도메인 정보를 기반으로 AD[8] 에 연결된 모든 호스트의 정보를 가져온다. 이후 각 호스트에 -u 인자의 아이디와 -p 인자의 비밀번호로 인증이 가능한지 확인한 후, 인증된 모든 호스트에 랜섬웨어를 전파한다.

```
vsprintf_sub_409070(NewFileName, 260, L"%s\\Temp\\cleanup.exe", Name);
NetResource.dwType = 1;
NetResource.dwScope = 0;
memset(&NetResource.dwDisplayType, 0, 12);
NetResource.lpComment = 0;
NetResource.lpProvider = 0;
NetResource.lpRemoteName = Name;
if ( log_flag )
  print_log_sub_409040("[+] Connecting to share: %ws\n", Name);
v6 = WNetAddConnection2W(lpNetResource: &NetResource, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0);
if ( v6 )
{
  if ( log_flag )
    print_log_sub_409040("[!] Failed to connect to share: %ws (Error: %d)\n", Name, v6);
  return 0;
}
if ( log_flag )
  print_log_sub_409040("[+] Connected to share, copying binary\n");
if ( CopyFileW(lpExistingFileName: Filename, lpNewFileName: NewFileName, bFailIfExists: 0) )
{
  TickCount = GetTickCount();
  vsprintf_sub_409070(sc_name, 32, L"Radio_%d", TickCount);
  vsprintf_sub_409070(
    CommandLine,
    520,
    L"sc \\\\%s create %s binPath= \"%%windir%%\\Temp\\cleanup.exe %s\" start= demand",
```

그림 11. Devman 랜섬웨어 전파 및 실행

연결된 호스트의 임시 폴더에 cleanup.exe 파일명으로 랜섬웨어를 복제하며, 서비스로 등록하거나 작업 스케줄러로 랜섬웨어를 실행한다. 또한, 같은 네트워크에서 전파가 여러 번 시도되는 것을 방지하기 위해 원격 호스트에서는 -skip-net 인자를 추가하여 랜섬웨어를 실행한다. 사용하는 명령어는 아래 표와 같다.

명령어	설명
sc \\{host_ip} create Radio_[0-9]{32} binPath= "%%windir%%\Temp\cleanup.exe -skip-net" start= demand	원격 호스트에 서비스 생성
sc \\{host_ip} start Radio_[0-9]{32}	서비스 실행
schtasks /create /s {host_ip} /u {username} /p {password} /tn "CoolTask" /tr "%%windir%%\Temp\cleanup.exe -skip-net" /sc once /st 00:00	작업 스케줄러 작업 생성
schtasks /run /s {host_ip} /u {username} /p {password} /tn	작업 스케줄러 작업 실행
schtasks /delete /s {host_ip} /u {username} /p {password} /tn	작업 스케줄러 작업 삭제

표 5. 종료 대상 서비스 및 프로세스

[7] LDAP: 네트워크 상에서 사용자, 그룹, 장비, 인증 정보 등의 데이터를 저장하고 조회 가능하게 하는 프로토콜

[8] AD (Active Directory): LDAP 기반의 Windows 통합 디렉터리 시스템으로 사용자와 컴퓨터를 일괄적으로 관리 가능

네트워크 전파 이후에는 현재 로컬 시스템 암호화를 진행한다. -skip-local 을 사용하면 네트워크 공유 폴더만 암호화하며, -skip-net 을 사용하면 로컬 디스크만 암호화한다. 또한 -path 인자를 사용하면 특정 디렉터리와 그 하위 디렉터리만 암호화한다. 암호화 대상을 설정했으면, 각 디렉터리를 순회해 예외 항목에 해당하는지 확인한다. Devman 버전의 예외 확장자에 .bin 이 추가된 것을 제외하고, 두 버전의 암호화 예외 대상이 동일하다. 확인하는 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
Windows, Program Files, Program Files (x86), AppData, ProgramData, All Users, NETLOGON, SYSVOL	PrintMe22.pdf, .exe, .dll, .msi, .sys, .ini, .ink, .bin

표 6. 암호화 예외 대상

파일 암호화 방식은 설정값에 따라 두가지 암호화 모드로 구분된다. 설정값에는 암호화 모드를 결정하는 값과, 부분 암호화 비율을 결정하는 두 개의 옵션이 존재한다. 첫 번째 방식은 크기가 큰 파일의 경우 앞부분 일부만 암호화하는 방식이다. 1MB 이하의 파일은 전체 암호화를 진행하며, 5MB 이하의 파일은 처음 1MB 만큼만 암호화한다. 5MB 보다 큰 파일은 공격자가 지정한 비율만큼 파일의 첫 부분을 암호화하는데, 그 크기가 최대 70MB 로 제한되어 있다.

그림 12. 크기 별 파일 암호화 방식 - 1

두 번째 방식은 크기가 큰 파일의 경우 일정 간격마다 암호화하는 방식이다. 64Bytes 이하의 파일은 전체 암호화를 하며, 5MB 이하의 파일은 전체 크기의 10%만큼만 암호화한다. 20MB 이하의 파일은 전체 크기의 1/6 만큼 구간을 나누어 각 구간의 첫 4KB 만 암호화하고, 20MB 보다 큰 파일은 10MB 마다 처음 4KB 를 암호화한다.

그림 13. 크기 별 파일 암호화 방식 - 2

두 암호화 방식 모두 동일한 알고리즘을 사용한다. 암호화 키는 Curve25519 를 통해서 생성한 공유 비밀을 이용한다. 각 파일마다 랜덤한 개인키를 하나 생성한 다음, 하드코딩된 Devman 의 공개키를 사용해 공유 비밀을 생성할 수 있다. 자신의 개인키와 상대방의 공개키로 만든 공유 비밀이 자신의 공개키와 상대방의 개인키로 만든 공유 비밀과 동일한 값을 가지는 Curve25519 의 특성을 이용한 것이다. 해당 공유 비밀을 SHA-512 알고리즘으로 해시를 생성해 해쉬의 뒷 32 바이트를 키로 이용해 HC-128 알고리즘으로 파일을 암호화한다. 파일의 끝에는 키 복구에 필요한 Curve25519 공개키를 함께 저장한다.

파일 암호화가 끝나면, 각 암호화 대상 경로에 랜섬노트를 생성한다. 만약 랜섬노트를 출력하는 옵션이 활성화되어 있다면, 랜섬노트 내용을 PDF 형태로 저장한 뒤, 이를 연결된 모든 프린터에 출력한다. 랜섬노트는 임시폴더에 PrintMe22.pdf 이름으로 저장된다.

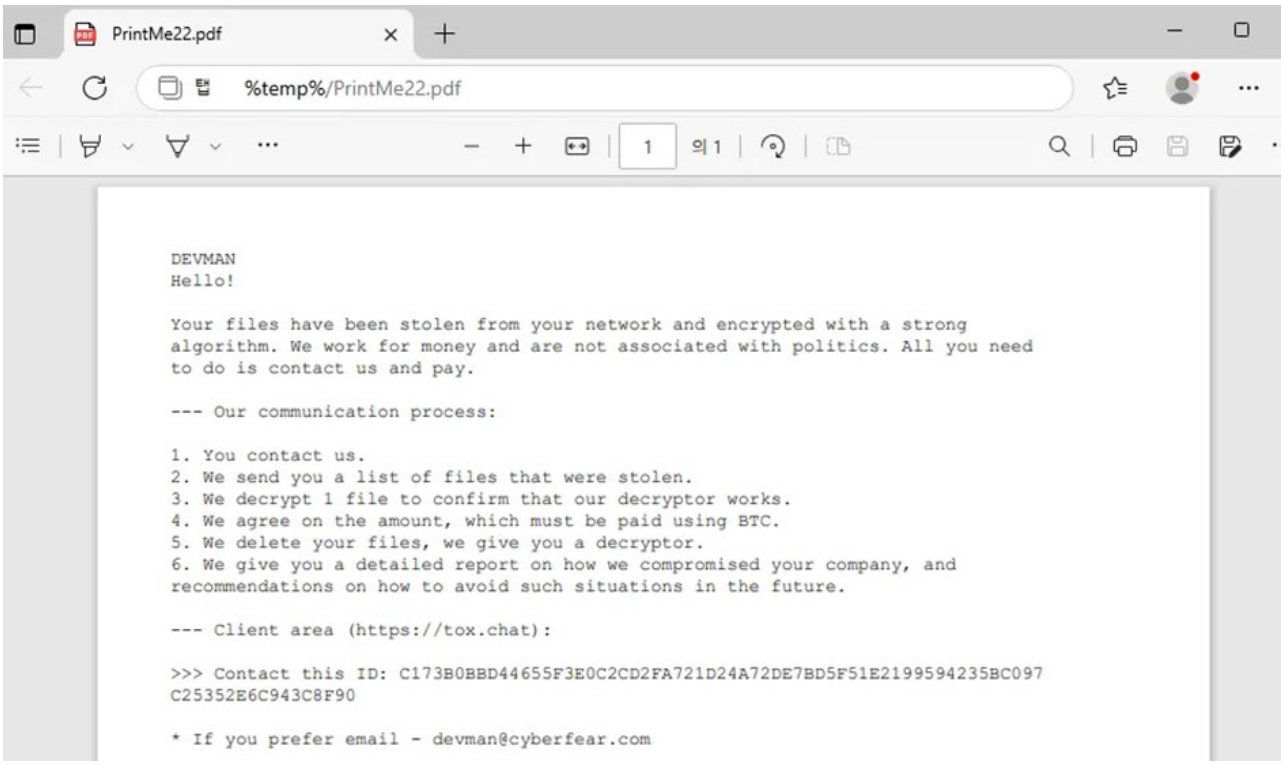


그림 14. 출력용 랜섬노트

그 외에도 암호화된 파일의 아이콘을 변경하기 위해 Base64 형태로 저장된 아이콘 이미지 파일을 임시폴더에 저장한 후, 레지스트리 설정 변경을 통해서 아이콘을 임의로 변경한다. 또한 “YOUR FILES HAVE BEEN ENCRYPTED! CHECK README.yAGRTb.txt” 라는 문구가 적힌 이미지로 배경화면을 변경한다.

그림 15. 변경된 배경화면

DragonForce 랜섬웨어 대응방안

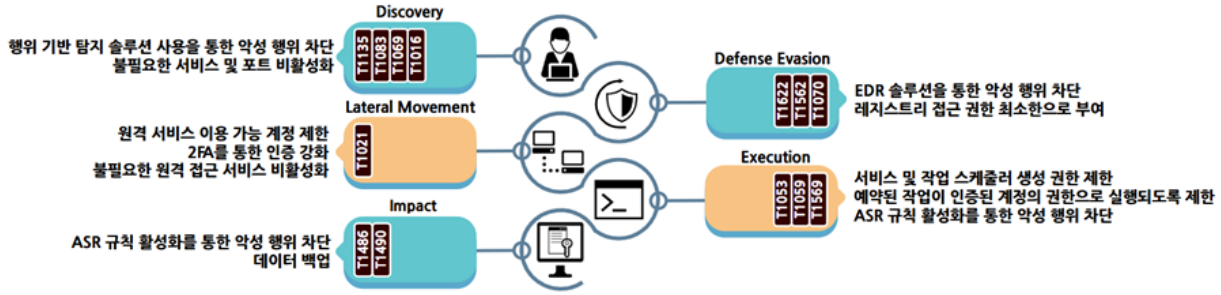


그림 16. Devman 랜섬웨어 대응방안

Devman 랜섬웨어는 파일 암호화 및 네트워크 전파를 위해서 네트워크 공유 폴더나 시스템이 속한 도메인 등 각종 정보를 활용한다. 따라서 행위 기반 탐지 솔루션을 사용해 악성 행위를 차단할 수 있으며, 불필요한 네트워크 서비스를 제거하거나 비활성화해 네트워크로 피해가 확산되지 않게 할 수 있다.

랜섬웨어의 악성 행위가 탐지되는 것을 회피하기 위해 Windows Defender 를 비활성화하며, 디버거를 분리하고 각종 이벤트 로그를 삭제한다. EDR[9] 솔루션을 사용해 Windows Defender 비활성화나 이벤트 로그 삭제와 같은 악성 행위를 차단할 수 있다. 특히 이벤트 로그 삭제의 경우 레지스트리에 접근이 필요한데, 레지스트리 접근 권한을 최소한으로 부여하면 공격자가 임의로 이벤트 로그를 삭제하지 못하게 할 수 있다.

또한 네트워크 환경으로 랜섬웨어를 전파하기 위해서 로그인 ID 와 비밀번호를 이용해 네트워크 환경에 접근을 시도한다. 별도의 ID 및 비밀번호 수집 과정은 확인되지 않았으나, 공격 준비 과정에서 계정 정보를 수집하거나 유출 혹은 취약한 계정을 악용할 수 있기 때문에 2FA[10] 를 이용해 인증을 강화해야 한다. 또한 원격 서비스를 이용할 수 있는 계정을 제한하거나 불필요한 원격 서비스 자체를 비활성화해 공격자가 네트워크 환경에 접근하지 못하도록 할 수 있다.

앞서 설명한 악성 행위는 대부분 Windows 명령 프롬프트를 활용하거나 작업 스케줄러 및 서비스 등록을 통해 이루어진다. 따라서 ASR[11] 규칙 활성화로 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 파일 격리도 가능하다. 그 외에도 서비스 및 작업 스케줄러의 생성 권한을 제한하여 복제된 랜섬웨어가 원격으로 실행되지 않도록 제한해야 하며, 예약된 작업이 실행되더라도 인증된 계정의 권한으로 실행되도록 설정하여 피해를 최소화할 수 있다.

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

[10] 2FA (2-factor Authentication): ID/PW 인증 외에도 휴대전화나 OTP 등을 활용한 추가 인증 수단으로 인증하는 방식

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

암호화된 파일을 사용자가 임의로 복구하는 것을 방지하기 위해서는 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.

IoCs

Hash(SHA-256)
1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e
c5f49c0f566a114b529138f8bd222865c9fa9fa95f96ec1ded50700764a1d4e7

■ 참고 사이트

• GMA Network (https://www.gmanetwork.com/news/topstories/nation/945481/gma-network-statement-on-cybersecurity-incident)

• RELIAQUEST (https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/)

Special Report

제로트러스트 보안전략 : 기기 및 엔드포인트 (Device/Endpoint)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

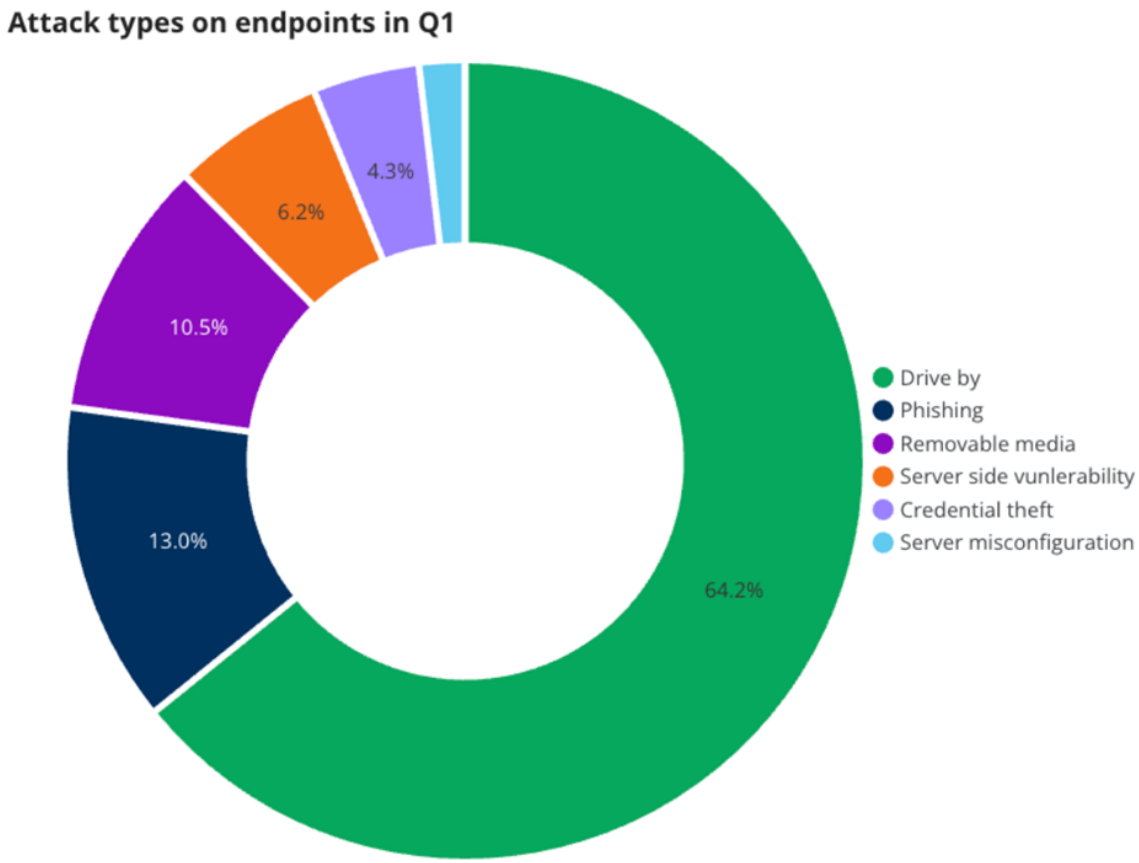
■ 기기 및 엔드포인트 (Device/Endpoint) 필러 개요

제로트러스트 아키텍처에서 기기(Device) 및 엔드포인트(Endpoint) 필러는 식별자·신원(Identity) 필러와 긴밀하게 연계되어, 사용자가 민감한 리소스에 접근하기 전에 디바이스 상태와 보안 신뢰도를 기반으로 최종 접근 여부를 판단하는 핵심 통제 지점으로 작동한다. 사용자의 신원이 확인되더라도, 해당 디바이스가 검증되지 않았거나 보안 기준을 충족하지 못할 경우, 접근은 제한되어야 한다. 이는 CISA 의 가이드라인에서 강조하는 사용자와 디바이스의 상태, 위치, 행위 등의 다양한 요소를 기반으로 접근 정책을 동적으로 조정하는 체계를 적용해야 함을 의미한다.

코로나 19 팬데믹 이후 업무 환경은 급격히 변했다. 이에 따라 조직의 주요 정보들은 사용자들이 일상적으로 사용하는 PC, 노트북, 태블릿 등 다양한 디바이스에 분산되어 저장돼 사용하는 형태로 전환되었다. 이러한 디바이스들은 내부망과 외부 망, 클라우드 환경 등 여러 보안 경계를 넘나들며 연결되고 있으며, 특히 재택근무, 출장, 외부 고객 미팅 등으로 기업 소유 또는 개인 소유(BYOD)의 디바이스를 공공장소나 외부 네트워크로 빈번하게 활용하고 있다.

특히 국내의 경우, 물리적 망분리를 중심으로 설계된 기존 보안 환경이 원격·유연 근무 확대로 구조적 제약으로 작용하고 있다. 이를 해소하기 위해 국가정보원 주도의 '국가 망 보안체계 가이드라인(N2SF)', 금융위원회의 '금융분야 망분리 개선 로드맵' 등에서 망 분리 환경의 단계적 완화와 제로트러스트 기반 보완책을 함께 제시하고 있다. 이러한 흐름은 디바이스 및 엔드포인트 수준에서의 실질적인 보안 검증과 제어 체계를 더욱 정교하게 요구하고 있다.

디바이스 및 엔드포인트 환경의 다변화와 더불어, 엔드포인트를 노리는 공격은 꾸준히 증가하고 있다. 최근 Expel 의 "2025 년 1 분기 엔드포인트 위협 보고서"에 따르면, 조직을 대상으로 한 전체 보안 사고 중 68%가 엔드포인트에서 발생하였으며, 아래 그림을 보면 '드라이브 바이(Drive by)', 피싱(Phishing), 이동식 저장매체(Removable media), 서버 취약점(Server side vulnerability) 등 다양한 공격 유형이 확인됐다. 특히, '드라이브 바이' 공격이 전체 엔드포인트 공격의 64.2%로 가장 높은 비중을 차지하고 있어, 기존 네트워크 중심의 수동적 방어만으로는 대응에 한계가 있음을 보여준다.



출처 : Expel "2025 년 1 분기 엔드포인트 위협 보고서"

그림 1. 2025 년 1 분기 엔드포인트 공격 유형

"Expel, CrowdStrike 등 글로벌 리포트에서 말하는 디바이스와 엔드포인트에는 시스템(서버)까지 포괄하는 경우가 많지만, 국내 제로트러스트 실무에서는 사용자 디바이스 중심의 엔드포인트 관점으로 해석할 필요가 있다."

이처럼 디바이스 및 엔드포인트에 대한 위협이 고도화·지능화됨에 따라, 단순한 방화벽·백신 중심의 대응만으로는 충분하지 않다. 행위 기반 탐지(EDR/XDR), 통합 엔드포인트 관리(UEM), 지속적인 보안 상태 모니터링, 정책 기반 접근 통제 등 다양한 대응 전략을 동시에 적용하는 다층적 방어 체계가 필요하다. 제로트러스트 관점에서는 디바이스 및 엔드포인트의 신뢰성을 동적으로 평가하고, 위협을 실시간으로 탐지·차단하는 체계 구축이 핵심이다.

특히 제로트러스트 환경에서는 사용자의 신원을 검증할 때, 해당 사용자가 실제로 접근하는 디바이스의 신뢰성과 보안 상태 또한 연계하여 함께 확인하는 것이 필수다. 예를 들어, 동일한 자격을 가진 사용자라 하더라도, 미승인 혹은 위험도가 높은 디바이스(패치 미적용, 악성코드 감염, 이상 행위 탐지 등)로는 기업 내 중요 시스템이나 데이터에 대한 접근을 자동으로 제한해야 된다. 이처럼 식별자와 디바이스 필러의 연계적 통제는 조직 내 민감 자산이 실질적으로 보호받을 수 있도록 하며, 단일 인증 체계의 취약점을 보완하는 결정적 역할을 수행하게 된다.

디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처 내에서 단순한 접속 수단을 넘어, 조직 접근 정책과 실시간 위험 평가의 핵심 축으로 기능한다. 특히 디바이스는 실제 사용자가 업무에 활용하는 실질적 접근 주체이기 때문에, 정책 판단 과정에서 각종 속성 정보와 보안 상태를 제공하는 PIP(Policy Information Point, 정보제공지점)로서의 역할이 강조된다.

결과적으로 디바이스 및 엔드포인트 영역을 제로트러스트 아키텍처 관점으로 고도화할 때, 조직은 점차 정교해지는 위협에 효과적으로 대응하는 것은 물론, 핵심 자산과 정보를 안전하게 보호할 수 있는 기반을 만들 수 있다.

■ 기기 및 엔드포인트 (Device/Endpoint) 필러의 주요 요소

디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처에서 사용자 신원(Identity)과 더불어, 실제 리소스 접근의 전 단계에서 적용되는 핵심 보안 통제 영역이다. 디바이스는 사용자가 업무에 활용하는 실질적 접점이자, 조직 자산 및 데이터에 대한 다양한 위협이 현실적으로 발생하는 지점이다.

특히, 제로트러스트 환경에서는 모든 디바이스와 엔드포인트를 신뢰할 수 없는 대상으로 간주하고, 디바이스의 상태·신뢰도·위험 수준 등을 기반으로 실시간 검증과 세분화된 정책 적용이 요구된다. 이를 위해, 디바이스 인벤토리(자산 목록화), 디바이스 인증, BYOD 관리, 취약점 및 패치 관리, 위험 평가 등 다양한 요소별 통합 관리 체계가 마련되어야 한다.

아래에서는 디바이스 및 엔드포인트 필러의 주요 요소들과, 이를 구현하기 위한 관리적·기술적 방안을 구체적으로 살펴본다.

1. 디바이스 인벤토리

제로트러스트 환경에서 디바이스 인벤토리는 조직 내 리소스에 접근 가능한 모든 기기를 체계적으로 식별·관리하는 기반이 된다. 관리 대상은 데스크톱, 노트북, 스마트폰, 태블릿은 물론, IoT 기기와 프린터, 이동식 저장장치 등으로 확장된다. 이에 따라 조직은 디바이스의 형태, 운영체제, 하드웨어·소프트웨어 특성 등 세부 속성을 기준으로 식별 정책을 마련하고, 각종 인벤토리 정보를 통합적으로 관리해야 한다.

디바이스 인벤토리는 단순 목록화가 아닌, 네트워크에 새로 연결되는 기기의 자동 등록, 디바이스 상태 변화·위치 이동·폐기 등 라이프사이클 관리가 포함된다. 자동화된 자산관리 시스템이나 UEM(Unified Endpoint Management), AD 등과 연계해 인벤토리 정보의 정확성과 최신성을 유지하는 것이 중요하다.

등록된 인벤토리 정보에는 소유자, 소속 부서, 용도, 보안 등급, 연결 이력 등 다양한 데이터가 포함되며, 이러한 정보는 보안 정책 적용, 이상행위 감지, 사고 대응의 핵심 자료로 활용된다. 또한, 중요도·위험도·업무 유형 등에 따라 디바이스를 그룹화하고, 그룹별로 차등화된 접근통제 및 보안 정책이 적용될 수 있다. 예를 들어, 관리용 디바이스와 일반 사용자, 외부 협력업체 디바이스를 구분해 관리함으로써, 불필요한 권한 확산과 내부 위협을 효과적으로 통제 가능하다.

2. 디바이스 인증

제로트러스트 환경에서 디바이스 인증은, 단순히 기기가 등록되어 있다는 사실만을 신뢰하지 않는다. 조직은 접근 요청이 들어오는 각 디바이스에 대해 고유 식별 정보(예: MAC 주소, 디지털 인증서, 시리얼 등)를 활용해 신뢰할 수 있는 기기인지 여부를 반드시 확인해야 한다. 이 과정에서는 단순 인증 정보뿐만 아니라, 소유자, 등록 이력, 관리 상태 등의 교차 검증 절차를 반드시 병행해야 한다. 미승인·비인가 디바이스에 대해서는 네트워크 접근을 원천적으로 차단할 수 있도록 정책을 설계하는 것이 중요하다.

디바이스 인증은 일회성 절차에 머물러서는 안 된다. 조직은 디바이스의 네트워크 연결 현황, 운영체제 및 소프트웨어 최신화 여부, 물리적 위치와 사용자의 접속 이력, 행위 패턴 등 다양한 요소를 종합적으로 평가해 신뢰도 점검을 주기적으로 해야 한다. 예를 들어, 패치 미적용 기기, 악성코드 감염, 비정상적인 위치·시간의 접근 등이 감지되는 경우, 추가 인증 또는 접근 제한 등의 추가 절차를 반드시 반영해야 한다. 이러한 신뢰도 평가는 UEM, EDR 등 보안 시스템과 연계해 실시간으로 자동화하는 것이 효과적이다.

조직은 디바이스 신뢰도 평가 결과를 기반으로, 각 디바이스에 대해 접근 허용, 제한, 격리, 추가 인증 등 세분화된 대응 정책을 마련해야 한다. 신뢰도가 낮은 기기에 대해서는 민감 자산 접근을 자동으로 차단하거나, 별도의 관리 체계로 이관하는 방안을 검토해야 한다. 이러한 모든 과정은 ICAM, SSO, EDR, UEM 등과의 통합 운영 체계를 통해 보안 정책과 연동하여, 조직 전반의 위험 대응 능력을 향상시키는 데 기여해야 한다.

3. BYOD(Bring Your Own Device) 관리

제로트러스트 환경에서 BYOD 관리는 개인이 소유한 노트북, 스마트폰, 태블릿 등 각종 디바이스가 업무 목적으로 조직 리소스에 접근할 수 있도록 허용하는 대신, 반드시 적정 수준의 보안통제와 정책 준수가 병행되어야 한다. 개인 디바이스를 통한 업무는 사용 편의성과 생산성을 크게 높일 수 있지만, 한편으로는 조직의 민감 정보가 외부 환경에 노출될 가능성을 상존하게 만든다.

따라서 조직은 BYOD 도입 여부 및 허용 범위, 승인 절차, 보안 수준, 운영체제와 관리 플랫폼(MDM/UEM) 등을 명확히 정책으로 정의해야 한다. 허용된 디바이스 유형, 플랫폼, 소프트웨어 목록, 필수 보안 앱 설치 여부 등 기준을 구체적으로 마련하는 것이 중요하다.

BYOD 정책에는 디바이스 등록과 주기적 보안상태 점검, 접속 이력 기록, 중요 리소스 접근 시 강화된 인증(MFA), 클라우드·네트워크 분리 등 다양한 보안요건이 반영되어야 한다. 또한, BYOD 사용자의 개인정보 보호와 프라이버시 침해 방지 측면도 중요하게 다뤄져야 하므로, 최소한의 모니터링 범위와 용도, 접근 가능 정보에 대해 사용자에게 사전 고지 및 동의를 받는 절차를 마련해야 한다.

BYOD 위험도 평가는 기기 보안상태, OS 취약점, 악성코드 감염 여부, 백신·MDM 설치 여부, 정책 위반 이력 등을 종합적으로 반영해 주기적으로 실시하는 것이 필요하다. 이러한 평가는 UEM, MDM, EDR 등 통합관리 솔루션을 통해 자동화하는 것이 효율적이다. 위험도가 높게 평가된 디바이스는 민감 데이터 접근 제한, 추가 인증 요구, 조직 네트워크 격리 등 차등화된 대응 정책으로 관리할 수 있다.

BYOD 환경의 실시간 모니터링 역시 필수적이다. 운영체제·제조사·설치, 소프트웨어·네트워크 접속 이력 등 기초 정보뿐만 아니라, BYOD 정책 위반 여부, 비정상 접속 패턴, 의심 활동 발생 시 자동 경고 등 다양한 요소를 관리 시스템에서 수집·분석하도록 한다. BYOD 를 모니터링할 때에는 업무 중단이나 과도한 사생활 침해가 발생하지 않도록 업무 관련 데이터와 개인 데이터의 논리적 분리 원칙이 반드시 보장되어야 한다.

4. 디바이스 취약점 관리

제로트러스트 환경에서 디바이스 취약점 관리는 단순히 소프트웨어나 운영체제의 최신 패치를 적용하는 수준을 넘어, 조직 내에 존재하는 모든 기기(PC, 노트북, 모바일, IoT 등)에 대한 취약점 탐지와 영향 평가, 신속한 대응까지 전 주기를 포괄해야 한다.

우선, 조직은 정기적이고 체계적인 취약점 식별 및 평가 정책을 수립해야 하며, 이를 통해 기기별 취약점 진단 절차와 평가 기준, 자동화된 점검 주기, 발견 시 조치 프로세스 등 일련의 관리체계를 구체적으로 마련해야 한다.

취약점 진단 단계에서는 UEM, MDM, EDR 등 보안 시스템을 활용해 네트워크 상에 연결된 모든 디바이스를 주기적으로 스캔한다. 이 과정에서 운영체제 미 패치, 취약한 애플리케이션, 불필요한 서비스 구동 등 다양한 취약 요소를 식별하며, 위험 등급 및 우선순위에 따라 신속한 조치가 이루어져야 한다. 최신 보안 패치 배포, 취약 소프트웨어 제거, 설정 변경, 네트워크 격리 등 자동화된 대응을 병행하는 것이 바람직하다.

취약점이 발견되면, 해당 취약점의 영향도와 악용 가능성을 분석해 우선순위별로 대응 전략을 세워야 한다. 예를 들어, 내부 주요 시스템 침해, 데이터 유출, 랜섬웨어 감염 등 실질적 피해 가능성이 높은 취약점은 즉시 차단·패치·격리 등 강력한 대응 조치를 실행한다. 취약점 영향 분석 결과와 대응 과정은 별도의 보고서로 기록해, 향후 유사한 위협 발생 시 신속한 참고자료로 활용한다.

취약점 관리 결과는 디바이스 위험도 평가에 직접 반영할 수 있다. 반복적으로 취약점이 발견되거나, 미조치 상태가 지속되는 기기는 민감 데이터 접근 제한, 추가 인증 요구, 네트워크 분리 등으로 연동해 실질적 리스크를 줄일 수 있다.

종합적으로, 디바이스 취약점 관리체계는 디바이스 인벤토리·인증·신뢰도 평가와 연계해 운영함으로써, 조직 내에 존재하는 모든 단말의 보안 수준을 일관성 있게 유지하고, 침해사고 가능성을 선제적으로 차단할 수 있는 기반이 된다.

5. 디바이스 패치 관리

제로트러스트 환경에서 디바이스 패치 관리는 조직 내 모든 기기의 보안 수준을 일관되게 유지하기 위한 핵심 요소다. 패치 관리는 단순한 소프트웨어 업데이트가 아니라, 체계적인 정책 수립과 절차 정의, 그리고 패치 배포·검증·사후 관리까지 전 주기에 걸쳐 관리 체계를 갖추는 것이 중요하다.

조직은 먼저, 디바이스 운영체제와 디바이스 내에서 사용되는 애플리케이션, 펌웨어 등에 대한 패치 적용 원칙과 절차를 구체적으로 정의하는 패치 관리 정책을 마련해야 한다. 해당 정책에는 관리 대상 기기의 목록화, 패치 우선순위 산정, 패치 배포·설치 프로세스, 백업 및 복구 방안, 패치 적용 이력 관리와 같은 핵심 항목들이 포함되어야 한다. 패치 관리 정책은 실제 보안 환경의 변화와 기술 발전을 반영해 정기적으로 검토·갱신하는 것이 필요하다.

패치 배포 시에는 각 디바이스의 특성, 운영 환경, 업무 중요도 등을 종합적으로 고려하여, 자동화된 시스템(AD, PMS 등)을 적극 활용해야 한다. 모든 단말에 일괄 적용하는 방식이 아닌, 네트워크 환경이나 사용자 편의성, 업무 영향도를 반영해 배포 일정과 방식에 유연성을 두는 것이 효과적이다. 패치의 정확성, 완전성, 일관성, 확장성 등을 관리 지표로 삼아, 최신 패치가 신속하고 누락 없이 적용될 수 있도록 설계해야 한다.

패치 적용 이후에는, 설치 현황과 누락 여부를 실시간으로 모니터링할 수 있는 체계가 필요하다. 누락되거나 실패한 패치에 대해서는 신속하게 추가 조치를 수행하고, 예외 상황이나 실패 이력은 별도의 보고 체계를 통해 관리하는 것이 바람직하다. 또한, 패치 관리 결과와 이력은 정기적인 보안 점검, 위험도 평가, 내부·외부 감사 및 규제 대응 등에 적극적으로 활용할 수 있도록 체계적으로 기록·보관해야 한다.

디바이스 패치 관리는 디바이스 인벤토리, 취약점 진단, 신뢰도 평가와 연계해 운영함으로써, 조직 내 모든 단말의 보안 취약점을 선제적으로 차단하고, 일관된 보안 수준을 유지하는 기반이 된다.

6. 디바이스 위험 관리

제로트러스트 아키텍처에서 디바이스 위험 관리는 조직 내 모든 업무용 기기의 물리적·논리적 위협에 대한 보호를 핵심 목표로 한다. 디바이스는 분실, 도난, 탈취, 비인가 접근과 같은 직접적인 물리적 위협뿐만 아니라, 내부자 위험이나 악성코드 감염, 데이터 유출 등 다양한 리스크에 노출될 수 있다.

먼저, 모든 디바이스는 자산 목록에 등록해 소유자와 위치, 사용 이력 등 주요 정보를 체계적으로 관리해야 한다. 물리적 분실이나 도난 사고에 대비해, 노트북이나 태블릿 등 주요 장비에는 시건장치(잠금장치) 등의 물리적 보호조치를 도입한다. 이동이 잦은 장치에는 GPS 기반 위치 추적 기능이나 분실 시 원격 잠금·데이터 삭제 등 즉각적 대응체계를 마련해야 한다.

디바이스 사용자는 분실·도난 등 사고 발생 시 즉각적으로 조직 내 IT 담당자나 보안 관리자에게 신고할 수 있는 절차를 숙지해야 하며, 조직은 이를 위해 정기적인 보안 교육과 가이드라인을 제공해야 한다.

이러한 다층적 관리·운영 체계를 기반으로, 조직은 단순히 기술적 보호조치에만 의존하지 않고, 사람과 정책, 프로세스가 결합된 통합적 보안 환경을 구현해야 한다. 디바이스 위험 관리는 결과적으로 정보 유출, 자산 손실, 내부자 위협 등 다양한 리스크를 최소화하고, 업무 연속성과 정보보호 수준을 실질적으로 강화하는 기반이 된다.

7. 통합 엔드포인트 관리(UEM)

조직 내 엔드포인트 환경이 PC, 노트북, 모바일, IoT 등으로 다변화됨에 따라, UEM(Unified Endpoint Management)은 단일 플랫폼에서 다양한 기기의 등록, 인증, 정책 배포, 보안 관리, 데이터 보호까지 통합적으로 지원해야 한다. 단순히 모바일 단말의 원격 제어에 머무는 기존 MDM 에서 진화해, 업무 현장의 모든 엔드포인트에 대해 일관성 있는 보안 정책과 운영 효율성을 동시에 추구하는 것이 핵심이다.

UEM 정책은 조직의 정보보호 방침, 디바이스 관리 원칙과 연동되어야 하며, 디바이스 등록과 인증, 엑세스 제어, 보안 위협 감지 및 대응, 데이터 보호 등 주요 보안 요구사항을 세부적으로 포함해야 한다. 이때, UEM 은 단독으로 운영되지 않고 ICAM, 통합 모니터링 시스템 등과 연계하여, 조직 내 디바이스 영역에 제로트러스트 보안체계의 실질적 실행 플랫폼 역할을 수행해야 한다.

엑세스 제어 측면에서, UEM 은 각 디바이스가 조직 리소스에 접근하는 경로와 수준을 세밀하게 관리해야 한다. 네트워크 기반의 접근제어와 더불어, ICAM 연동을 통해 RBAC, ABAC 등의 정책을 적용할 수 있다. 또한, UEM 은 사용자 행동 분석 결과를 반영하여 위험도가 높거나 이상 징후가 탐지된 기기에 대해 별도의 제한 또는 추가 인증 절차를 적용하는 등, 동적이고 자동화된 엑세스 제어 체계를 마련해야 한다.

데이터 유출 방지 역시 UEM 의 중요한 기능이다. 디바이스 내 민감 데이터는 자동 식별과 암호화해 보호되어야 하며, 데이터 손실 방지(DLP) 기능과 연계하여 의도적, 비의도적 유출 모두를 효과적으로 차단해야 한다. 조직은 정기적으로 UEM 정책과 시스템의 효과성을 평가·개선하며, 새로운 유형의 디바이스와 위협에 능동적으로 대응할 수 있도록 관리체계를 지속적으로 고도화해야 한다.

8. 엔드포인트 확장 탐지 및 대응 (EDR)

최근 사이버 위협의 지능화로 전통적인 시그니처 기반 보안 방식만으로는 모든 위협을 감지하고 대응하는 데 한계가 있다. 이에 따라 EDR(Endpoint Detection & Response)은 실시간 탐지, 사용자 행동 분석, 지속적 모니터링 등 다층적인 접근으로 조직의 디바이스 및 엔드포인트 보안의 핵심 축으로 자리잡고 있다.

EDR 의 실시간 위협 탐지 및 차단 기능은 다양한 유형의 악성 코드, 내부자 위협, 익명 공격, 사회공학 기반 공격 등 폭넓은 위협을 신속하게 감지하고, 자동화된 정책에 따라 사전에 설정된 차단 조치를 수행할 수 있도록 한다. 이 과정에서는 행동 기반 탐지, 파일 및 네트워크 트래픽 분석, 프로세스 감시 등 다양한 기법을 조합해 알려진 위협과 미지의 공격까지 아우르는 대응 체계를 마련할 수 있다. 또한, 위협이 감지될 경우 파일 삭제, 네트워크 연결 차단, 응용 프로그램 실행 제한 등 자동화된 방어 조치가 신속하게 이뤄져야 한다.

EDR 은 단순한 위협 탐지를 넘어, 엔드포인트 사용자 및 행동을 분석하는 고도화된 기능을 제공해야 한다. 정상적인 사용 패턴을 학습·정의한 후, 이와 다른 비정상적인 행위나 정책 위반 징후를 실시간으로 감지해 이상 행위 발생 시 즉각적인 대응이 이뤄질 수 있도록 한다. 사용자별로 세분화된 정보 수집과 통계 분석을 통해, 잠재적 내부자 위협이나 계정 탈취와 같은 고위험 사건에 효과적으로 대응할 수 있다.

지속적인 디바이스 상태 모니터링 역시 EDR 의 중요한 역할 중 하나다. 단순히 위협 발생 시에만 작동하는 것이 아니라, 사용자 행동, 시스템 설정, 네트워크 접속, 소프트웨어 설치 현황 등 다양한 요소를 실시간으로 모니터링해 정책 위반이나 취약점 노출을 조기에 탐지해야 한다. 수집된 데이터와 이상 행위 정보는 ICAM, 통합 관제 시스템 등 조직 내 타 보안 시스템과 연계되어, 보다 통합적이고 신속한 대응 체계 구축의 기반이 된다.

9. 정책 및 프로세스

디바이스 및 엔드포인트의 효과적인 관리와 보호를 위해서는 명확한 정책 수립과 체계적인 관리 프로세스가 필수적이다. 제로트러스트 보안 모델을 기반으로 한 관리 정책에는 기기 승인 절차, 인벤토리 등록 및 온보딩, 암호화 범위와 방식, 정기 백업 및 복구, 소프트웨어 관리, 보안 로그 모니터링, 감사 및 정책 검토 등 다양한 관리 항목이 포함되어야 한다. 이러한 항목들은 세부적인 운영지침과 실행 절차로 구체화되어야 하며, 조직 내 모든 구성원이 일관되게 준수할 수 있도록 체계적으로 관리할 필요가 있다.

특히, 디바이스 및 엔드포인트 관리 프로세스는 각 기기의 전체 라이프사이클을 아우르는 단계별 관리 체계를 수립하는 것이 중요하다. 신규 기기의 도입·배포, 사용 중 보안 유지, 운영 소프트웨어의 정기적 업데이트 및 취약점 관리, 사용 종료 후 반납과 폐기, 외부 반출이나 이동식 매체 사용에 대한 별도 절차까지, 각 단계별로 표준화된 운영 프로세스를 마련해야 한다. 조직은 이러한 프로세스 정립을 통해 보안 수준을 높이고, 실시간 자산 현황 파악 및 효율적인 리소스 배포·운영을 달성할 수 있다.

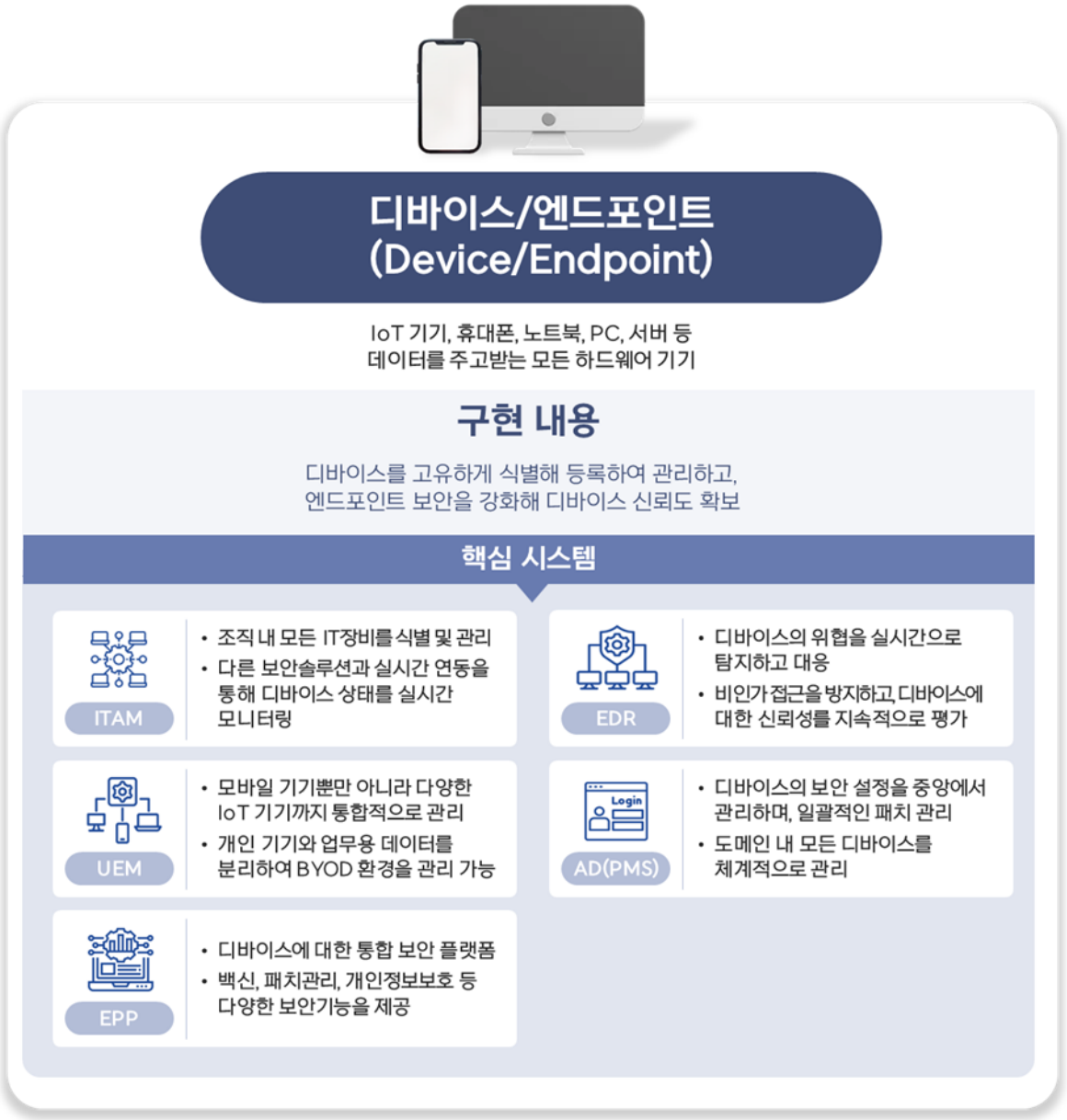
정책과 프로세스의 정교화는 디바이스 및 엔드포인트 영역의 일관된 보안 태세 유지와, 변화하는 업무 환경에서의 신속한 위험 대응에 반드시 필요한 과정이다.

이러한 주요 요소들을 기반으로, 디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처의 실질적인 보안 통제 축이 된다. 조직 내 모든 디바이스의 신뢰성과 보안 상태를 정밀하게 관리하고, 실시간으로 검증함으로써 사용자의 신원뿐만 아니라 실제 접속에 활용되는 기기의 위험까지도 일관성 있게 통제할 수 있다. 내·외부 위협으로부터 핵심 자산을 효과적으로 보호하며, 변화하는 업무 환경과 진화하는 사이버 위협에 신속하게 대응할 수 있는 유연성과 확장성을 제공한다. 디바이스 및 엔드포인트 필러의 고도화는 조직의 보안 정책과 관리 프로세스가 실질적으로 구현되는 기반이 된다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행하는 시스템이 필수적이다. 제로트러스트 아키텍처는 "신뢰하지 않고 항상 검증한다"는 원칙을 기반으로 한다. 이를 실현하기 위해 사용자와 엔터티의 신원을 확인하고, 지속적으로 검증하며, 최소 권한 접근 보장을 수행하는 시스템이 반드시 갖춰져야 한다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 중요한 역할을 담당하며, 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 2. 디바이스/엔드포인트 주요 시스템

1. ITAM (IT Asset Management, IT 자산관리시스템)

ITAM(IT 자산관리) 시스템은 제로트러스트 아키텍처에서 디바이스 및 엔드포인트의 인벤토리로서 출발점이자 기반 인프라로 기능해야 한다. 조직은 모든 IT 및 OA 자산(PC, 노트북, 모바일, 서버, 프린터, IoT 장비 등)에 대해 도입, 등록, 사용, 이동, 반출, 폐기 등 전 라이프사이클을 아우르는 관리 체계를 마련해야 하며, 자산 정보가 실시간으로 정확하게 반영될 수 있도록 자동화된 등록·변경·삭제 프로세스를 구축해야 한다. ITAM 은 각 조직의 업무 환경에 따라 별도의 상용 솔루션을 커스터마이징 후 도입하거나, 자체 SI(시스템 통합) 개발을 통해 구축할 수 있다.

ITAM 은 각 디바이스에 대한 자산번호, 바코드, 소유자, 소속 부서, 위치, 용도, 운영체제, 소프트웨어 설치 현황, 보안 등급, 연결 이력 등 다양한 속성 정보를 통합 관리할 수 있어야 한다. 신규 자산이 도입되거나 반출·폐기 등 상태 변경이 발생할 경우, 인벤토리 시스템에 자동 반영되어 관리 공백이나 정보 누락 없이 전체 현황을 한눈에 파악할 수 있도록 해야 한다. 특히 네트워크 접근이 가능한 디바이스에 대해서는 미등록 자산이 조직 네트워크에 접속하는 경우 자동으로 탐지·차단하거나, 보안 담당자에게 즉시 알림이 전달되도록 해야 한다.

ITAM 은 자산관리 고유 기능을 넘어서, EDR, UEM, AD, ICAM, ZTNA 등 주요 보안 솔루션과 연동하여, 인벤토리 정보의 최신성과 정합성을 유지하고, 실제 네트워크 환경에서 일어나는 변화까지 실시간으로 반영할 수 있어야 한다. 자산별 보안 상태(예: 패치 적용 현황, 취약점 점검 결과, 위험 등급, 접근 이력 등)는 ITAM 과 보안 시스템 간 데이터 교환을 통해 지속적으로 업데이트되며, 이를 기반으로 디바이스의 접근 통제·격리·추가 인증 등 동적 정책이 적용될 수 있다.

제로트러스트 환경에서는 등록되지 않은 디바이스의 네트워크 접근을 원천적으로 차단해야 하며, 반입·반출·폐기 등 주요 자산 흐름에 대해서는 추적성과 기록 관리를 통해 감사 및 사고 대응에도 활용할 수 있도록 해야 한다. 또한 ITAM 은 자산 반입 시 기본 보안점검(초기 상태 확인, 악성코드 탐지 등), 사용 중 정기 상태 점검, 반출·폐기 시 데이터 완전 삭제 및 인증 기록 보관 등 전체 라이프사이클에 걸쳐 보안 요건이 내재화될 수 있도록 연계되어야 한다.

관리자는 ITAM 을 통해 자산의 사용 현황, 이상 징후, 보안 정책 위반 사례 등을 한눈에 파악하고, 조직 내 어디에서 어떤 디바이스가 어떤 목적으로 운영되고 있는지 실시간으로 관리할 수 있다. ITAM 시스템은 내부·외부 보안 감사, 규제 대응, 침해사고 분석 등 다양한 요구사항에도 즉시 대응할 수 있도록 정확성, 추적성, 신뢰성을 갖춘 관리 환경을 제공해야 한다.

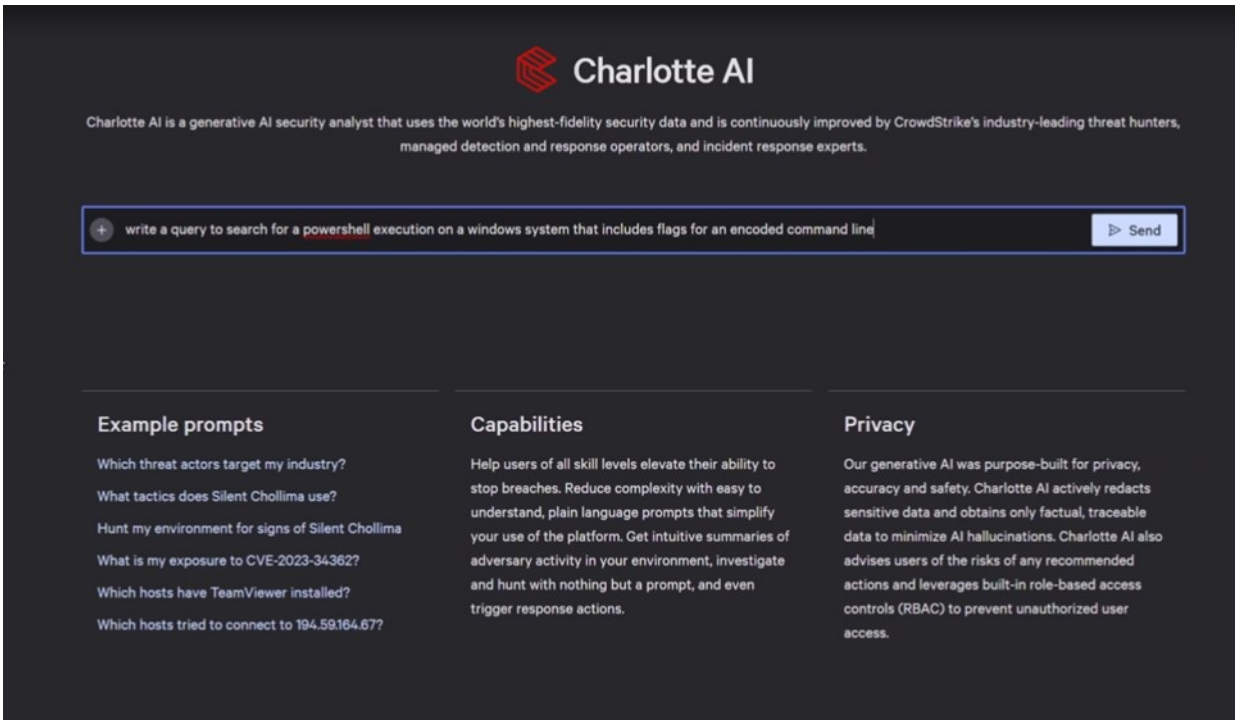
ITAM 의 고도화는 조직이 디바이스 및 엔드포인트 신뢰성 검증을 실질적으로 수행하는 기반이 되며, 네트워크 접근 통제 및 자산 보호 정책의 출발점으로 작동해야 한다. 이를 통해 조직은 제로트러스트 원칙에 따라 모든 디바이스에 일관된 접근 정책을 적용하고, 내부·외부 위협에 대한 실시간 대응력을 크게 향상시킬 수 있다.

2. EDR(EndPoint Detection & Response, 엔드포인트 탐지 및 대응)

EDR 은 PC, 노트북, 서버 등 조직의 모든 엔드포인트 단말에 설치되어, 실행 중인 프로세스, 파일 변경, 사용자 행위, 네트워크 활동 등 다양한 정보를 실시간으로 수집·분석하고, 이상 행위나 침해 징후를 탐지하여 신속한 대응까지 아우르는 고도화된 보안 시스템이다. 기존에는 안티바이러스(Anti-Virus) 알려진 악성코드 차단에 집중했었다. EDR 은 알려지지 않은 위협이나 내부자 이상행위, 제로데이 공격 등까지 대응 범위를 확장하며 엔드포인트 보안의 핵심으로 자리 잡고 있다.

EDR 은 단순한 위협 탐지 기능을 넘어, 실제 업무 환경에서 발생하는 다양한 보안 이벤트를 실시간으로 상관분석하고, 각 단말별 보안 상태와 취약점, 이상 행위, 비인가 소프트웨어 실행 등 복합적인 위협 징후를 한눈에 파악할 수 있는 통합 대시보드를 제공한다. 주요 EDR 제품은 프로세스 간 행위 추적, 메모리 기반 공격 탐지, 파일 및 네트워크 포렌식, 취약점 자동 탐지, 사용자별 행동 패턴 분석 등 고도화된 기술을 적용하여, 보안 담당자가 이상 상황을 신속히 인지하고, 자동 또는 수동으로 적절한 대응조치를 취할 수 있도록 지원한다. 또한, 자동화된 인시던트 대응 플레이북, 감염 단말 자동 격리, 위협 지표(IOC) 실시간 업데이트, 샌드박스 연동 분석 등 고급 대응 기능까지 점차 표준화되고 있다.

글로벌 EDR 솔루션들은 인공지능(AI)과 머신러닝 기반 탐지 및 분석, 프롬프트(자연어) 입력을 통한 정책 자동화 등 최신 기술을 적극적으로 도입하고 있다. 예를 들어 아래 '그림 3'과 같이 관리자가 영어로 "특정 명령 줄 플래그가 포함된 PowerShell 실행 탐지 정책을 생성해줘"라고 프롬프트를 입력하면, AI 가 관련 탐지 룰을 자동 생성·적용한다. 또한, AI 기반 위협 인텔리전스와 연동하여 실시간으로 신규 공격 유형이나 공격자의 행동 패턴을 반영하고, 정책 수정 및 룰 등록이 훨씬 직관적으로 이루어질 수 있다. 이와 함께, 위협 사냥(Threat Hunting) 기능과 자동화된 포렌식, 경보 우선순위 조정, 행위 기반 위험 점수 할당, 대응 프로세스 최적화 등 조직 규모와 환경에 따라 맞춤형 보안 운영을 지원하는 다양한 기능도 제공되고 있다.



출처 : CrowdStrike, "Conversations with Charlotte AI Demo"

그림 3. 프롬프트 입력을 통한 정책 쿼리 생성 화면

제로트러스트 아키텍처에서는 EDR 이 각 디바이스 및 엔드포인트의 신뢰성 검증을 위한 필수 수단으로 기능해야 한다. EDR 은 단순히 위협 탐지에 머무르지 않고, 감지된 위험 요소에 따라 접근 제한, 네트워크 격리, 추가 인증 요구 등 다양한 대응 정책을 자동화할 수 있어야 한다. 또한 SSO, IAM, MFA, ICAM 등 접근제어 시스템과 연동하여, 위협이 발생한 기기나 사용자의 접근 권한을 즉시 조정하고, 사고 확산을 효과적으로 차단할 수 있는 체계 마련이 중요하다.

최근 EDR 의 탐지·대응 범위를 사용자·네트워크·시스템·클라우드 등으로 확장하는 XDR(eXtended Detection and Response) 개념이 부상하고 있으나, 실제로는 데이터 연계 범위, 벤더 종속성, 표준 부재 등의 한계로 완전한 XDR 구현이 쉽지 않은 상황이다. 이에 따라 많은 조직은 EDR, NDR, SIEM/SOAR 등 각 필러별 전문 시스템을 별도로 구축하고, 상호 연동을 통해 현실적인 제로트러스트 보안 체계를 실현하는 방식을 택하고 있다.

EDR 도입을 통해 조직은 단순한 악성코드 차단을 넘어, 다양한 위협 유형과 공격 벡터에 실시간으로 대응하고, 디바이스 및 엔드포인트의 보안 신뢰도를 효과적으로 관리할 수 있다. 또한, AI 기반 자동화와 직관적 정책 관리, 상호 연동성 향상 등 기술 고도화를 바탕으로, 제로트러스트 환경에서 필요한 실시간 보안 검증과 대응 능력을 갖출 수 있다.

3. UEM (Unified Endpoint Management, 통합 엔드포인트 관리)

조직 내 디바이스와 엔드포인트는 한때 PC 와 노트북 등 전통적인 IT 기기에 국한되어 있었으나, 업무 환경의 변화에 따라 스마트폰, 태블릿, 웨어러블, IoT, 그리고 개인 소유의 BYOD(Bring Your Own Device)까지 다양한 형태로 빠르게 확장되었다. 이러한 변화는 디바이스 관리의 복잡성을 크게 높였고, 단일 플랫폼에서 모든 단말을 효과적으로 통합 관리해야 할 필요성이 대두됐다.

환경 변화에 대응하기 위해, 엔드포인트 관리 기술 역시 MDM(Mobile Device Management)에서 EMM(Enterprise Mobility Management), 그리고 UEM(Unified Endpoint Management)으로 진화해왔다.

MDM 은 모바일 단말(스마트폰, 태블릿 등)에 대한 원격 제어와 보안 관리 기능에 초점을 맞췄으나, 점차 모바일 업무가 확대되고 디바이스의 종류가 다양해지면서 한계가 드러났다.

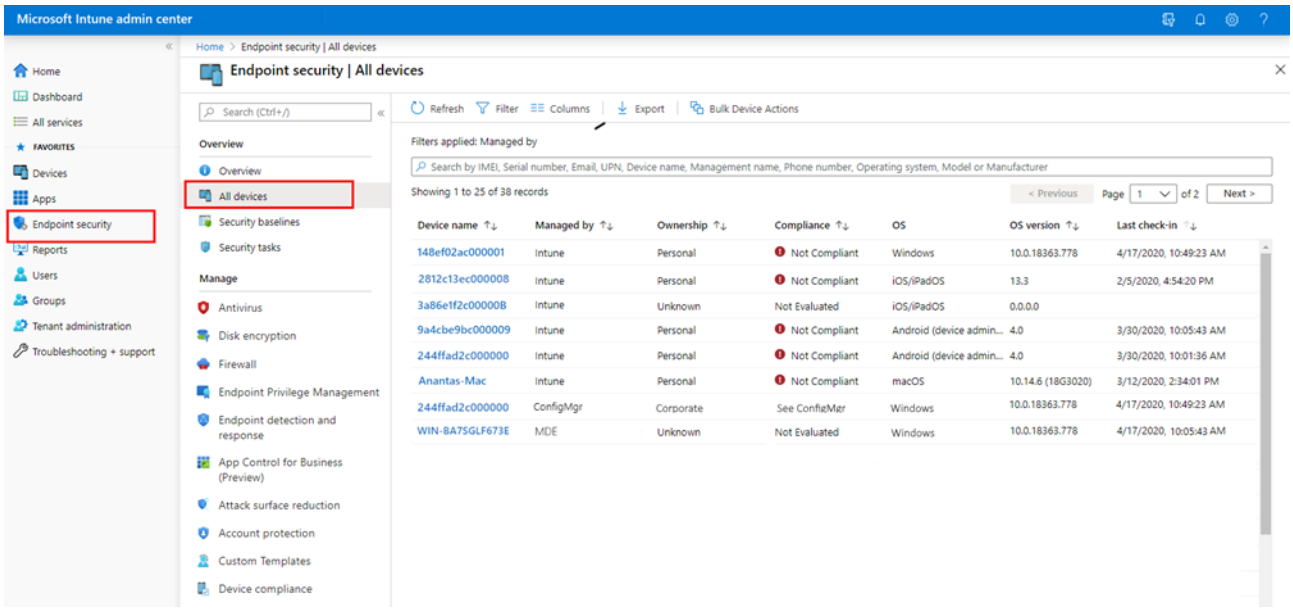
EMM 은 이러한 한계를 극복하기 위해 등장한 개념으로, 모바일 디바이스 관리(MDM)뿐만 아니라, 앱 관리(MAM), 콘텐츠 관리(MCM), 이메일·네트워크 보안 등 모바일 환경 전반을 포괄적으로 제어할 수 있게 기능이 확장됐다. 업무용·개인용 앱과 데이터의 분리, 정책 기반의 접근 제어, 클라우드 연계 등 EMM 을 통해 모바일 업무 환경의 보안성과 유연성이 한층 높아졌다.

UEM 은 EMM 의 기능을 더욱 확장하여, PC, 노트북, 스마트폰, 태블릿, 웨어러블, IoT, BYOD 등 조직 내 모든 IT 자산과 엔드포인트를 단일 플랫폼에서 통합 관리하는 체계를 제공한다. 단순한 모바일 관리 수준을 넘어, 운영체제와 장비 유형, 업무 환경을 불문하고 모든 디바이스의 등록·인증·정책 배포·보안 관리·애플리케이션 제어·취약점 점검·데이터 유출 방지·실시간 모니터링 등을 일원화한다.

UEM 은 제로트러스트 보안 아키텍처에서 모든 엔드포인트의 상태와 신뢰도를 실시간으로 검증하고, 미승인 또는 취약한 기기의 네트워크 접근을 제한하거나 격리할 수 있는 강력한 통제 기능을 제공해야 한다. 업무용·개인용, 내부·외부 소유를 불문하고 모든 디바이스의 보안 상태, 정책 준수 여부, 실시간 행위 분석 결과를 기반으로 접근 권한과 보안 정책을 동적으로 조정하는 것이 가능하다.

특히 UEM 은 기존의 EDR 이나 IT 자산관리 시스템만으로는 대응이 어려운 영역을 포괄적으로 통제할 수 있다는 점에서 차별성을 가진다. 예를 들어, EDR 이나 자산관리 솔루션은 PC, 서버 등 일반적인 IT 자산에 높은 수준의 통합·탐지·대응 역량을 제공하지만, 모바일 기기나 태블릿, BYOD, IoT 등 다양한 운영체제와 장비에는 에이전트 호환성 문제, 설치 제약, 통제 한계 등의 문제가 발생할 수 있다. UEM 은 이런 다양한 단말 환경과 보안 과제를 단일 플랫폼에서 통합적으로 관리할 수 있는 체계를 제공한다. 하지만, 국내외 실제 구축 사례는 아직 많지 않고, 조직 환경에 맞는 맞춤형 도입 및 운영이 쉽지 않다는 한계가 있다.

제로트러스트 아키텍처를 실질적으로 구현하기 위해서는 UEM 과 같은 통합 엔드포인트 관리 플랫폼의 도입과 고도화를 적극적으로 추진할 필요가 있으며, 엔드포인트 관리 체계 전반의 성숙도를 끌어올리는 노력이 병행되어야 한다.



출처 : Microsoft, “Technical documentation”

그림 4. MicroSoft Intune, UEM 콘솔 화면

4. AD(Active Directory/PMS, 패치 및 자산 관리)

Active Directory(AD)는 마이크로소프트 사가 제공하는 대표적인 디렉터리 서비스로, 조직 내 PC, 노트북, 서버 등 다양한 디바이스를 도메인 단위로 통합 관리하는 핵심 시스템이다. 기존에는 사용자 계정과 그룹 권한 관리에 주로 활용되었지만, 실제 기업 환경에서는 디바이스 등록·승인·삭제·정책 배포 등 엔드포인트 관리의 기반 인프라로 작동하고 있다.

AD 는 디바이스가 도메인에 가입되는 순간, 해당 기기의 보안 정책 적용, 접근 권한 부여, 패치·설정 일괄 배포, 인증 로그 집계 등 다양한 운영·보안 절차를 중앙에서 일괄 관리할 수 있도록 한다. 온프레미스 AD 뿐만 아니라, Microsoft Entra ID(구 Azure AD)와 연동된 하이브리드 환경에서도 동일하게 PC, 노트북, 태블릿, 일부 IoT 장비까지 디바이스의 통합 관리를 지원한다.

제로트러스트 관점에서 AD 는 단순한 디렉터리 서비스가 아닌, 엔드포인트 라이프사이클 전체를 관리하는 '디바이스 PMS(패치 및 자산 관리 시스템)'로 역할이 확장됐다 할 수 있다. 예를 들어, 도메인 가입된 모든 디바이스의 소유자, 위치, 사용 이력, 보안 상태(패치 적용 여부, 보안 정책 준수 등)를 실시간으로 집계·모니터링하고, 그룹 정책(GPO)이나 Intune(UEM) 등과 연동해 자동화된 보안 설정, 소프트웨어 배포, 이상 행위 탐지 및 격리 등 다양한 통제 체계를 일괄 적용할 수 있다.

또한, AD 와 연동된 UEM, EDR, ICAM, ZTNA 등 주요 보안 솔루션들은 AD 에서 제공하는 디바이스 속성 정보와 인증 기록을 활용해, 네트워크 접근 통제·격리·추가 인증 등 동적 정책을 구현한다. 이는 미승인·미등록 디바이스의 자동 탐지 및 네트워크 차단, 패치 미적용 기기 경고, 주요 자산 접속 기기 실시간 모니터링 등, 실질적인 엔드포인트 보안 통제의 기반이 된다.

최근에는 온프레미스 AD 뿐 아니라, 클라우드 기반 Entra ID 와 연동해 하이브리드 환경의 단말까지 통합 관리하는 사례가 빠르게 확산되고 있다. 디바이스 인벤토리, 패치 관리, 정책 배포, 위험도 평가 등 다양한 관리 기능을 점차 AD 기반으로 일원화하는 방향으로 발전할 것으로 보인다.

AD는 제로트러스트 아키텍처에서 사용자와 디바이스 모두를 아우르는 통합 인벤토리 및 정책 관리 엔진으로 기능해야 한다. AD 의 관리 범위와 데이터 정확성, 보안 통제력은 조직 내 모든 엔드포인트의 신뢰성 검증과 접근 통제, 정책 일관성 확보에 직결된다. AD 와 연계된 각종 보안 시스템이 제공하는 실시간 통합 관리는 조직 전체의 운영 효율성과 보안 수준을 한층 높일 수 있는 토대가 된다.

5. EPP (Endpoint Protection Platform, 엔드포인트 보호 플랫폼)

EPP 는 단일 플랫폼에서 엔드포인트(PC, 노트북, 서버 등)에 대한 다양한 보안 기능을 통합적으로 관리하고 제공하는 제품군을 의미한다. 본래 안티바이러스(AV)나 안티멀웨어를 중심으로 출발했지만, 최근에는 EDR, UEM, PMS, 취약점 진단 등 다양한 엔드포인트 보안 기능이 하나의 제품군으로 융합되는 방향으로 진화하고 있다.

EPP 는 통상적으로 하나의 콘솔에서 조직 내 여러 엔드포인트의 실시간 상태 모니터링, 정책 배포, 위협 탐지, 이상행위 분석, 취약점 점검, 패치 관리, 소프트웨어 설치 현황 파악 등 주요 보안 관리 업무를 일괄적으로 지원한다. 이런 통합적 관리 프레임워크는 운영 편의성과 가시성 측면에서 높은 효과를 제공하며, 실제 시장에서도 EPP 는 AV, EDR, PMS 등 다양한 엔드포인트 보안 솔루션을 통합해 라이선스를 판매하는 형태가 주류를 이룬다.

하지만, 실제 구현 단계에서 EPP 가 모든 엔드포인트 보안 시스템을 완전히 통합 관리하는 것은 제한적이다. 특히 대부분의 EPP 제품은 특정 벤더(제조사) 소프트웨어에 한정하여 통합 기능을 제공하며, 서로 다른 벤더의 보안 제품 간에는 연동의 한계가 존재한다. 이는 제로트러스트 환경에서 요구하는 '다양한 보안 시스템간 연동'이나, 조직 전반의 위협 정보, 정책, 인증 기반을 중앙에서 유연하게 다루는 데 있어 근본적 한계로 작용한다.

물론, 일부 조직에서는 다양한 벤더의 엔드포인트 보안 솔루션에서 제공하는 API 를 통합해 별도의 정보보안 포털이나 통합 관리 시스템을 자체적으로 구축하는 사례도 있다. 하지만, 시장에서 'EPP'라는 용어가 통용될 때는 대체로 벤더 중심의 제품군 혹은 솔루션을 의미하는 경우가 많다.

제로트러스트 환경에서 EDR, UEM, NDR, ZTNA, DSPM, SIEM&SOAR 등 필러별 주요 보안 시스템들은 각 필러별 영역에서 정책결정지점(PDP) 및 정책시행지점(PEP)의 역할을 수행할 수 있다. 하지만, 이러한 시스템들이 각각의 독립적 관점에서만 정보를 수집·통제하는 경우, 조직 전체에서 일관성 있는 정책 적용과 실시간 위험 대응, 보안 운영의 통합성이 저하될 수 있다.

제로트러스트 환경에서 궁극적으로 지향해야 할 것은, 각 필러별 보안 시스템이 제공하는 정보(PIP)를 ICAM(Identity, Credential and Access Management) 등 최상위 통합 플랫폼으로 연계하고, 식별자·엔드포인트·네트워크·데이터 등 조직 전반에 걸친 정보 기반의 통합 정책 및 접근 통제체계를 구현하는 것이다. ICAM 은 각 필러에서 전달되는 신원, 인증, 상태, 위험, 정책 이슈 등을 통합적으로 분석·판단하며, 조직 전체의 접근 정책(PDP)과 정책 집행(PEP) 역할을 중앙에서 일관되게 수행할 수 있어야 한다.

결국, EPP 를 비롯한 각종 영역별 보안 플랫폼을 개별적으로 운용하는 것은 제로트러스트의 전체론적 통합 아키텍처를 구현하는 데에 본질적 한계가 존재한다. 각 시스템이 정보를 제공하고 정책 집행에 참여할 수 있지만, 최상위 통합 관리체계인 ICAM 을 통해 조직 전체의 리스크와 정책을 통합적으로 통제하는 방향이 제로트러스트 보안 체계의 근간이 되어야 한다.

기기/엔드포인트 필러의 각 시스템은 단순한 기능 단위를 넘어, 제로트러스트 아키텍처를 기술적으로 구현하는 실질적인 수단으로 작동해야 한다. ITAM, EDR, UEM, AD, EPP 등은 각기 독립적으로 중요한 역할을 수행하되, 상호 유기적인 연동과 정보 공유를 통해 조직 내 모든 디바이스의 신뢰성 검증, 위험 탐지, 정책 집행이 일관되게 이뤄질 수 있도록 한다.

이러한 주요 시스템들의 기술적인 구현과 연계는 업무 환경과 디바이스 유형이 다양해지는 상황에서도, 일관된 보안 정책과 정밀한 통제를 구현할 수 있는 기반을 제공한다. 조직은 제로트러스트 환경 하에서 다양화되는 업무 환경과 디바이스 유형에 유연하게 대응하면서, 엔드포인트 보안의 신뢰성과 운영 효율성을 실질적으로 높일 수 있을 것이다.

■ 맺음말

제로트러스트 아키텍처에서 기기 및 엔드포인트(Device/Endpoint)는 단순한 업무 도구를 넘어, 조직의 모든 보안 전략을 실현하는 실질적이며 핵심적인 보안 요소이다. ITAM, EDR, UEM, AD, EPP 와 같은 주요 시스템들은 각각 독립적인 보안 기능을 수행하는 동시에, 상호 긴밀한 연계를 통해 모든 디바이스의 신뢰성을 평가하고, 실시간 위협을 탐지하며, 통합적인 정책 관리를 가능하게 한다.

디바이스 및 엔드포인트 필러의 정교한 설계와 운용은 조직의 모든 디바이스에 대한 철저한 보안 관리를 보장하는 동시에, 조직이 다양한 업무 환경과 지속적으로 진화하는 사이버 위협에도 유연하게 대응할 수 있는 '구조적 토대'를 제공한다. 특히 사용자의 신원과 디바이스의 신뢰성을 함께 검증하고 관리하는 접근 방식은 제로트러스트 환경에서 요구되는 일관되고 강력한 보안 통제를 구현하는 핵심 원칙이 된다.

제로트러스트 기반의 통합적 관리 체계는 디바이스의 유형과 사용 환경이 점차 다양화되고, 위협이 정교해지는 상황 속에서도 조직이 보다 효과적으로 위협을 예방하고 신속히 대응할 수 있도록 돕는다. 이는 단순히 개별 솔루션의 효용성을 넘어, 조직의 전반적인 보안 수준과 운영 효율성을 획기적으로 향상시키는 데 기여할 수 있다.

결론적으로 디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처의 핵심적이고 필수적인 구성요소이며, 조직의 디지털 자산 보호를 위한 실질적인 기술 기반을 마련한다. 조직은 이 필러를 중심으로 기술적 고도화와 관리 체계의 정교화를 지속적으로 추진함으로써, 디지털 환경의 복잡성과 리스크를 실질적으로 관리 가능한 수준으로 낮추고, 지속 가능한 디지털 보안 환경을 실현할 수 있을 것이다.

■ 참고 문헌

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

[2] NIST SP 1800-22, “Mobile Device Security: Bring Your Own Device (BYOD)”, 2023.09

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

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

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

■ 참고 자료

[1] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” – 브로슈어

[2] Gartner, “Best Endpoint Protection Platforms Reviews 2025”

[3] Expel, “Expel Quarterly Threat Report, Q1 2025: Endpoint threats”

[4] CrowdStrike, “CrowdStrike Falcon guides”

[5] SentinelOne, " SentinelOne Resource Center, Documentation"

[6] Microsoft, “Microsoft Defender for Endpoint”

EQST INSIGHT

2025.06

SK 쉴더스

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

발행인 SK쉴더스 EQST사업그룹
제 작 SK쉴더스 마케팅그룹