이일구 교수 지도

석사학위 청구논문

랜섬웨어 방어를 위한 Active Directory 기만 기술 연구

2025

성신여자대학교 대학원

미래융합기술공학과

박 정 수

렌섬웨어 방어를 위한 Active Directory 기만 기술 연구

이일구 교수 지도

이 논문을 석사학위논문으로 제출함

2025

성신여자대학교 대학원
미래융합기술공학과
박 정 수

인 준 서

박정수의 석사학위 논문으로 인준함

2025년 6월

심사위원장 김 성 민 (서명 또는 인)

심 사 위 원 임 연 섭 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

성신여자대학교 대학원

논문 개요

랜섬웨어는 최근 사이버 보안 위협 중 가장 큰 피해를 야기하는 공격 유형으로 자리 잡고 있다. 사용자의 데이터를 암호화하여 금전을 갈취하는 방식의 이 공격은 기업과 공공기관뿐 아니라 개인 사용자까지도 직접적인 피해 대상이 되고 있다. 특히, 랜섬웨어 공격은 단순히 악성코드의 유포에 그치지 않고 사회 기반 시설, 의료 시스템, 제조업 등 주요 산업 분야를 마비시키며 그 피해 범위와 규모가 날로 커지고 있다. 미국의 컬러니얼 파이스라인사의 대한 공격 사례에서 볼 수 있듯이, 랜섬웨어는 국가 안보에 영향을 미칠 수 있는 수준의 위협으로 평가받고 있다.

이러한 랜섬웨어 공격이 점점 더 차단하기 어려운 이유는, 전통적인 바이러스와 달리 지속적으로 진화하며, 과거의 다양한 악성코드 기법들을 결합한 형태로 나타나기 때문이다. 파일 암호화 기능 외에도, 정보 탈취, lateral movement(측면 이동), 백도어 설치 등의 고급 기능을 탑재하고 있으며, 공격자는 피해자 시스템 내에 장시간 은밀히 잠복하며 타이밍을 조율하는 경우도 많다. 이로 인해 탐지 및 방어는 점점 더 어려워지고 있으며, 전통적인 보안 솔루션만으로는 대응에 한계가 있다.

더불어, Ransomware as a Service 형태로 랜섬웨어를 서비스화한 해킹 그룹의 활동이 활발해지면서 누구나 손쉽게 공격을 실행할 수 있는 여건이 조성되고 있다. 개발자는 공격 툴을 제작하고, 사용자는 이를 구매 또는 대여하여 공격을 실행하는 구조로, 범죄가 조직화·산업화되고 있다. 이 과정에서 가상화폐를 통해 금전을 거래하기 때문에 익명성이 보장되고, 이는 공격자 식별과 추적을 더욱 어렵게 만든다. 실제로 다수의 해킹 그룹이 비트코인 또는 모네로(Monero)와 같은 암호화폐를 통해 몸값을 요구하고 있으며, 피해자가 이를 지불해도 데이터 복호화가 이루어지지 않거나, 2차 공격이

이어지는 경우도 있어 심각한 문제로 대두되고 있다.

한편, 대부분의 기존 보안 솔루션은 시그니처 기반 또는 패턴 기반으로 동작하는 구조이기 때문에, 알려진 악성코드에 대해서는 대응이 가능하지만, 조금이라도 변형된 새로운 변종에 대해서는 탐지에 실패하는 경우가 많다. 랜섬웨어는 이 점을 악용하여 파일의 페이로드 일부를 변경하거나, 암호화된 쉘코드를 사용하여 보안 시스템을 우회한다. 최근에는 악성코드가 사용자 행동을 모니터링하면서, 보안 프로그램이 실행되지 않는 특정 시간대를 노려 활동하는 등 탐지를 피하는 방식도 점점 더 정교해지고 있다.

이러한 고도화된 랜섬웨어 위협에 대응하기 위해서는 새로운 보안 패러다임이 필요하다. 기만 기술은 공격자의 심리를 이용하여 가짜 정보를 통해 공격을 유도하고, 이를 통해 침입 여부를 조기에 탐지할 수 있도록 설계된다. 예를 들어, 엔드포인트에 해커가 흥미를 가질 만한 유인 정보를 의도적으로 배포하고, 해당 정보를 탐색하거나 접근하는 행위를 통해 실시간으로 위협을 감지할 수 있다. 또한, 운영 시스템과는 별도로 존재하는 디코이 시스템으로 해커의 접근을 유도함으로써, 실제 시스템에 대한 피해를 최소화하고 동시에 해커들의 Tactics, Techniques 및 Procedures를 수집할 수 있는 이점이 있다.

본 논문에서는 랜섬웨어 위협의 주요 특징과 공격 방식의 진화 양상을 분석하고, 현재 상용화되어 있는 보안 솔루션의 한계를 살펴본다. 나아가, 기존 대응 방식의 한계를 극복하기 위한 방안으로서 기만 기술의 개념과 활용 전략을 제안하고, 이를 통한 효과적인 랜섬웨어 탐지 및 대응 방안을 연구한다.

목 차

표 차 례

그림 차례

Ⅰ. 논문 서론

1. 연구 배경

랜섬웨어는 단순한 악성코드로 분류하기에는 그 복잡성과 정교함이 매우 뛰어난 위협이 되고 있다. 이는 다양한 유형의 악성코드가 지닌 핵심적인 기능들을 포괄적으로 결합하고 있어, 일정의 '복합형 악성코드(Hybrid Malware)'로 분류하는 것이 더 적절하다. 예를 들어, 트리어 목마(Trojan)의 은밀한 침투 방식, 웜(Worm)의 자가 복제 및 전파 능록, 스파이웨어(Spyware)의 정보 수집 기능, 루트킷(Rootkit)의 은폐 기술 등을 통합적으로 활용함으로써 보안 체계를 우회하고, 피해자의 데이터를 암호화한 뒤 금전을 요구하는 방식으로 진화하고 있다. 이러한 특성으로 진화하고 있다. 이러한 특성으로 인해 랜섬웨어는 단순한 감영 행월르 넘어, 지속적이고 전략적인 사이버 공격 수단으로 자리 잡고 있다. 아니다.

최근에는 특정 기관이나 기업의 IT 운영 시스템 공격, 평판 훼손 및 재정적 피해가 급증하고 있다[1][2]. 4차 산업 기술이 발전하고 IT 시스템에 대한 의존도가 증가함에 따라 랜섬웨어 공격의 위험 및 피해 규모가 기하급수적으로 증가하고 있다. 최근 랜섬웨어는 단순히 PC의 파일을 암호화하는데 그치지 않고 비즈니스 마비, 서비스 중단, 데이터 손상을 초래하여 막대한 금전적 손실을 발생시키고 있다[3]. 이로 인해, 사이버 범죄자들은 지속적으로 기술을 발전시키며 RaaS 형태로 진화하고 있다[4][5]. 공격자들은 보안이 취약하고, 재무 안정성이 높으며 디지털 인프라에 의존하는 기관을 표적으로 삼는다. 들은 자동화 도구, 다크웹의 정보 교류, 유출된 계정정보 및 보안 패치가 미흡한취약점 등을 통해 접근한다[6][7]. 일단 침투에 성공하면 측면 이동(Lateral Movement)하여 내부 시스템으로 공격을 확장한다. 이 과정에서 Active Directory 관리자 계정이 주요 타깃이 된다[8]. Ryuk, Conti, Hive 등의 고도화된 랜섬

웨어 그룹들이 실제 이 경로를 활용하여 대규모 피해를 발생시킨 바 있다[9][10].

본 논문은 현재 사용되고 있는 다양한 레거시 랜섬웨어 대응 솔루션의 기술적 한계를 분석하고, 랜섬웨어 공격 초기 단계에서 해커들의 공격 시도를 내부 시스템이 아닌 디코이 시스템으로 유도하여 내부 자산을 보호하는 기만 기술 기반 대응 방안을 제안한다[11].

2. 연구 목적

시그니처 및 제한적 차단 기술의 레거시 보안 솔루션의 기술적 한계를 확인한다. 램섬웨어의 침입 경로 및 공격 기법에 대해 확인하고 기술적인 새로운 대안을 제시한다.

레거시 보안 솔루션의 경우 알려지지 않은 제로데이 공격 및 내부자의 이상 행위를 탐지할 수 없는 기술적 제약이 존재한다[12]. 운영 중인 인프라의 구성 변경 및 에이전트 추가 설치 없이 Credential Lure 계정만 삽입하여 구성이 가능하다. 특히 백신 및 EDR이 탐지하지 못하는 Lateral Movement 및 내부자 공격을 탐지할 수 있는 기만 기술 기반의 방안을 제시하고자 한다[13][14]. SIEM, 백신 및 EDR 등 도입된 보안 솔루션과 연계해 탐지, 분석, 대응 보안 운영 환경을 자동화 할 수 있다. 연구를 통해 백신, EDR 대비 공격 탐지율을 수치하여 랜섬웨어 대응에 기여하고자 한다.

Ⅱ. 기술 현황

1. 랜섬웨어의 진화

랜섬웨어는 과거 단순한 파일 암호화에서 탈피해, 조직적인 범죄 형태로 진화하고 있다. 최근에는 RaaS 생태계를 기반으로 다양한 비전문 해커들도 공격이 가능해졌고, 공격자들은 데이터 탈취 후 유출 협박까지 하는 이중 협박 전략을 활용한다[15][16].

Maze, DarkSide, LockBit, Clop 등은 전 세계 주요 기업을 공격하여 수백만 달러의 피해를 입혔다. 이들은 탐지 회피, 정찰, 권한 상승, 내부 이동, 데이터 탈취 후 암호화까지 전체 공격 체인을 자동화된 도구로 구현하고 있다[17][18].

2. 주요 공격 벡터

랜섬웨어는 다양한 공격 벡터를 통해 조직 내 시스템에 침투하며, 그 중에서도 피싱(Phishing), 소프트웨어 취약점 악용, 원격 데스크톱 프로토콜(RDP) 취약점, 공급망 공격(Supply Chain Attack), 이동식 저장장치, 드라이브 바이 다운로드 및 내부자 위협이 주요 경로로 꼽힌다.

피싱은 이메일이나 메시지를 통해 악성 링크 또는 파일을 전달함으로써 사용자가 스스로 악성코드를 실행하게 만드는 사회공학적 기법이다. RDP는 취약하게 설정된 원격 접속 포트를 대상으로 무차별 대입 공격이나 취약점 이용을 통해 시스템에 원격 접속을 시도하는 경우가 많다.

또한, 운영체제나 자주 사용되는 응용 프로그램의 보안 취약점을 악용하는 방식, 또는 공급망을 통해 감염된 소프트웨어를 배포함으로써 다수의 사용자에게 동시에 전파되는 방식도 주요한 공격 수단이다. 이 외에도 이동식 저장

장치를 통한 물리적 전파, 사용자가 단순히 악성 웹사이트에 접속하는 동시에 감염되는 드라이브 바이 다운로드, 그리고 내부자의 실수 또는 악의적 행위로 인한 감염 사례 역시 꾸준히 보고되고 있다.

1) 스피어 피싱 이메일

스피어 피싱(spear-phishing)은 개인 및 특정 조직을 정밀하게 표적 삼아 진행되는 사회공학적 공격 기법으로, 랜섬웨어의 초기 침입 벡터 중 가장 빈번하게 사용되는 수단 중 하나이다. 공격자는 수신자의 직책, 업무 내용, 조직 내 관계 등을 기반으로 정교한 이메일을 제작하여 악성 링크 또는 첨부파일을 통해 공격을 수행한다 [19].

Barracuda Networks의 2023년 보고서에 따르면, 조사 대상 조직의 약 50%가 스피어 피싱 공격의 영향을 받았고, 24%는 이메일 계정이 실제로 탈취된 경험이 있다고 보고되었다. ReliaQuest는 2023년 보안 경고 분석에서, 유틸리티 산업 부문에서 탐지된 보안 경고 중 81%가 스피어 피싱과 관련되었음을 밝혀 해당 기법의 실질적인 위협 수준을 강조하였다.

Verizon의 2022 데이터 침해 보고서는 전체 침해 사고 중 약 36%가 피싱 공격과 관련되었으며, 이메일을 통한 침투로 시작되었다고 언급한다. IBM의 2022년 보고서에 따르면, 피싱 기반 공격은 데이터 유출 중 가장 비용이 많이 드는 벡터로, 평균 피해 비용이 약 491만 달러에 이른다.

APT(Advanced Persistent Threat) 공격 시나리오 내에서 초기 침입 수단으로서 스피어 피싱의 사용 빈도가 가장 높다는 점을 실증적으로 입증하였으며, 첨부파일 또는 URL 기반 악성코드 배포가 초기 단계에서 광범위하게 활용된다고 보고하였다 [20].

2) 원격 데스크탑 프로토콜(RDP) Brute Force 공격

원격 데스크톱 프로토콜(Remote Desktop Protocol)은 원격지에서 네트워크를 통해 윈도우 시스템에 접근할 수 있도록 설계된 프로토콜로, 특히 원격 근무 및 서버 유지 관리 환경에서 널리 사용되고 있다. 그러나, RDP는 보안 설정이 미흡한 경우 공격자에게 시스템 접근의 경로를 제공할 수 있으며, 랜섬웨어 공격의 대표적인 초기 침투 벡터 중 하나로 악용되고 있다 [1].

공격자들은 인터넷에 노출된 RDP 포트(기본 3389번)를 대상으로 포트 스캐닝을 수행한 뒤, 무차별 대입(brute-force attack) 기법이나 이미 유출된 계정 정보를 통해 인증을 우회하여 시스템에 접근한다 [3]. 공격자는 인증 이후 관리자 권한을 확보하여 시스템 내부에서 권한 상승, 내부망 전파(lateral movement), 백업 파일 삭제 및 최종적으로 랜섬웨어를 실행하여 데이터를 암호화하는 공격을 수행하게 된다 [21].

RDP 기반 공격은 피싱 공격과 비교하여 상대적으로 탐지하기 어렵고, 공격자가 장기적으로 은밀하게 활동할 수 있어 더욱 치명적이다. 공격자의 RDP 기반 침입이 전체 APT(Advanced Persistent Threat) 공격의 70% 이상을 차지한다고 보고하였다 [21].

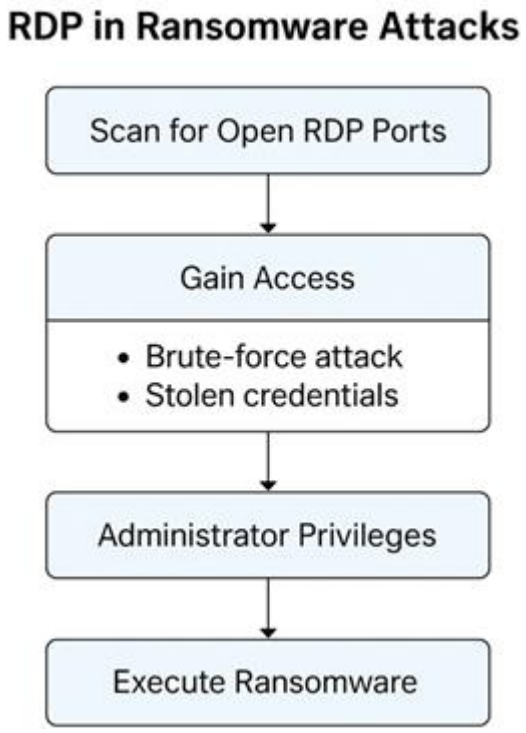

FIGURE 1. RDP 공격 흐름도

3) AD 관리자 계정 탈취를 통한 Lateral Movement

액티브 디렉토리(AD: Active Directory)는 조직 내 사용자 계정과 권한을 중앙에서 관리하는 핵심 시스템으로, 대다수 기업 환경에서 널리 사용된다. 그러나 공격자가 AD 관리자 계정을 탈취할 경우, 내부 네트워크 전체에 대한 접근 권한을 손쉽게 확보하여 lateral movement(측면 이동)를 수행할 수 있게 된다 [22].

공격자는 주로 피싱이나 RDP 침해와 같은 초기 침투 방법을 통해 시스템에 접근한 후, 관리자 계정의 자격 증명을 탈취하는 공격을 수행한다. 자격 증명 탈취는 메모리 내 해시(dumping hashes), 키로깅(keylogging), 자격 증명 재사용 공격(pass-the-hash attack)과 같은 다양한 기법을 통해 이루어지며, 이를

통해 획득한 관리자 계정을 활용하여 네트워크 전반으로 공격 범위를 확장하게 된다 [23].

AD 관리자 계정을 통한 lateral movement는 탐지가 어려우며, 공격자는 이를 통해 보다 광범위한 피해를 야기할 수 있다. Ullah 등의 연구에 따르면, 랜섬웨어 공격자들이 AD 계정 탈취 후 lateral movement를 통해 조직의 핵심 서버 및 백업 시스템을 장악하고, 랜섬웨어를 배포하여 최대 피해를 유발하는 것으로 나타났다 [21].

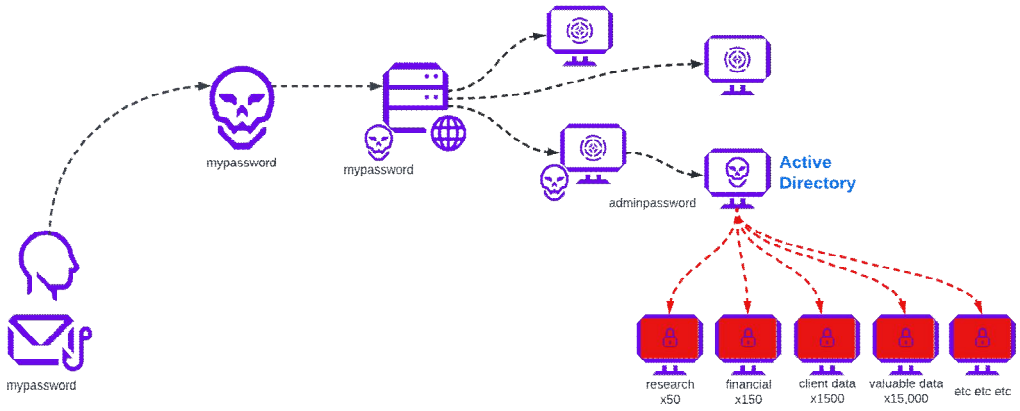

FIGURE 2. AD 관리자 계정을 통해 내부 시스템 랜섬웨어 감염

3. 레거시 방어 기술의 한계

기존의 보안 체계는 시그니처 기반 안티바이러스, 방화벽 및 침입 탐지 시스템(Intrusion Detection System) 등으로 구성되어 있으며, 이는 알려진 위협을 식별하고 차단하는 데 효과적인 방어 수단으로 오랫동안 활용되어 왔다. 그러나 이러한 레거시 보안 기술은 빠르게 진화하는 랜섬웨어 공격 방식에 효과적으로 대응하기 어렵다는 구조적 한계를 지닌다.

시그니처 기반 탐지 방식은 알려진 악성 코드에 대한 식별에는 유용하지만, 코드가 변형되거나 난독화(Obfuscation)된 경우에는 탐지가 어렵다. 특히,

현대의 랜섬웨어는 다형성(Polymorphic) 또는 파일리스(Fileless) 형태로 동작하여 기존 시그니처 데이터베이스에 등록되지 않은 상태에서도 시스템에 침투할 수 있다.

또한, 네트워크 기반의 전통적인 보안 장치는 내부 확산을 방지하기에 취약한 구조를 갖고 있다. 초기 침투 이후 공격자가 합법적인 사용자 권한을 탈취하여 내부 시스템을 순차적으로 감염시키는 행위는 기존 보안 체계로는 식별이 어렵다. 이러한 측면 이동(lateral movement)는 공격자의 행위를 정상적인 관리 활동으로 가장할 수 있기 때문에 탐지가 더욱 어렵다.

방화벽이나 접근제어 시스템 또한 정적인 룰 기반 정책에 의존하기 때문에, 동적으로 변화하는 공격 행위나 정상적인 트래픽을 위장한 악성 행위를 효과적으로 차단하는 데 한계가 존재한다.

결과적으로, 레거시 보안 기술만으로는 지능화된 랜섬웨어 공격에 선제적으로 대응하기 어렵고, 이는 탐지 지연, 대응 실패, 그리고 피해 확산으로 이어질 수 있다. 따라서 보다 정교하고 적응적인 대응 기술의 도입이 요구된다.

1) 시그니처 기반 안티바이러스 한계: 다형성 공격에 취약

랜섬웨어 공격에 대응하는 방어 수단으로 백신 소프트웨어(안티바이러스, Antivirus)는 오랜 기간 동안 널리 사용되고 있지만, 최근 공격 형태가 고도화됨에 따라 기존 백신 솔루션의 탐지 능력과 방어 역량에 한계가 드러나고 있다 [1].

전통적인 백신 솔루션은 주로 알려진 악성코드의 시그니처(signature) 기반 탐지 기법을 사용하기 때문에, 신종 또는 변형된 랜섬웨어에 대해서는 효과적으로 대응하기 어렵다. 공격자들은 지속적으로 악성코드를 변형하거나 암호화하여 백신의 탐지를 우회할 수 있으며, 이는 '제로데이(Zero-day)' 공격과 같은 신속한 대응이 필요한 상황에서 더욱 뚜렷한 문제로 나타난다 [2].

최근의 랜섬웨어 공격은 파일리스(fileless) 공격이나 메모리 기반 공격(memory-based attacks)과 같이 디스크에 흔적을 남기지 않고 메모리나 정당한 프로세스에 숨어 실행되는 방식을 사용하고 있어, 시그니처 기반의 백신 소프트웨어로는 탐지 및 대응이 불가능하다 [24].

백신 솔루션은 대부분 공격 발생 후 대응적인 성격이 강하여, 이미 시스템 내부에서 랜섬웨어가 활성화된 상태에서는 피해를 방지하는 데 한계가 있다. 즉, 실시간으로 시스템 내부의 이상 행위를 식별하거나 행위 기반(behavior-based)의 선제적 대응을 수행하지 못할 경우, 감염 확산과 데이터 암호화를 막기 어렵다 [25].

2) EDR 기술 한계: 침투 이후 대응 집중

최근 랜섬웨어 공격이 정교화되고 피해 규모가 증가함에 따라, 기존의 안티바이러스 솔루션의 한계를 보완하기 위해 EDR(Endpoint Detection & Response) 기술이 널리 도입되고 있다. EDR은 엔드포인트에서 이상 행위를 탐지하고 위협에 실시간 대응하는 능력을 제공하지만, 랜섬웨어 공격에 대한 완벽한 방어를 보장하지는 못하는 몇 가지 근본적인 한계를 지니고 있다 [26].

EDR의 탐지 및 대응 능력은 주로 행위 기반(behavior-based)의 이상 탐지 기법에 의존하고 있다. 그러나 최근 랜섬웨어는 정상적인 운영 체제의 프로세스나 허용된 애플리케이션을 악용하여, 정상 행위와 구분하기 어려운 은밀한 공격 기법을 사용하고 있다. 이러한 합법적 도구의 악의적 사용(Living-off-the-land, LOTL)으로 인해 EDR이 탐지하기 어렵다는 문제점이 나타난다 [27].

실시간 탐지 및 분석을 위해 막대한 양의 데이터를 수집하고 처리하는데, 이 과정에서 수집된 데이터의 과다나 탐지 모델의 복잡성으로 인해 오탐(False positive) 및 미탐(False negative)이 발생할 수 있다. 특히, 오탐이 자주 발생할 경우, 보안 담당자들이 실질적인 위협을 구별하고 대응하는데

오히려 방해가 되는 상황이 벌어진다 [28].

대부분 랜섬웨어의 초기 침투 후 탐지 및 대응을 중심으로 설계되어 있어, 공격 자체를 근본적으로 차단하거나 사전에 완벽히 예방하는 능력에는 한계가 있다. 다시 말해, EDR은 공격이 발생한 이후 대응 중심의 솔루션이며, 공격이 매우 빠르게 진행될 경우 랜섬웨어 감염과 암호화 피해를 미리 방지하기 어렵다 [29].

3) 이메일 보안 기술 한계 : 제한적 차단 및 속도 저하

이메일 보안 솔루션은 랜섬웨어의 주요 유포 경로 중 하나인 이메일을 통한 피싱 공격을 차단하는 데 효과적으로 활용되고 있다. 그러나 최근 랜섬웨어 공격의 고도화된 특성으로 인해 기존 이메일 보안 솔루션의 차단 능력에도 명확한 한계점들이 존재한다 [30].

대부분 알려진 악성 이메일을 차단하는 데 효과적이나, 표적형 스피어 피싱(spear-phishing)이나 비즈니스 이메일 침해(Business Email Compromise)와 같은 정교한 공격 형태에 대해서는 탐지 및 방어가 어렵다. 공격자들이 합법적인 이메일 계정 또는 도메인을 탈취하거나, 이메일 내용을 정밀하게 위장하는 경우가 많아, 기존 시그니처 기반 이메일 보안 필터를 쉽게 우회할 수 있다 [20].

일반적으로 이메일 본문 및 첨부파일에 대한 콘텐츠 분석을 수행하지만, 최근 공격자들은 클라우드 스토리지 서비스에 악성 파일을 올리고, 이메일에는 정상적인 링크를 첨부하여 보안 필터링을 우회하는 공격을 수행하고 있다. 이는 이메일 보안 솔루션이 이메일 내 정상적인 링크를 차단할 수 없다는 근본적인 한계를 노린 것이다[31].

이메일 자체만을 검사하고, 이메일을 통해 다운로드되는 악성 콘텐츠의 사후 행위는 실시간으로 탐지하기 어렵다. 즉, 사용자가 이메일 링크를 클릭하거나

첨부파일을 다운로드한 이후에 발생하는 시스템 내 악성행위는 이메일 보안 솔루션의 탐지 범위를 벗어나기 때문에, 이메일 보안 솔루션만으로 랜섬웨어 감염을 완전히 방지하는 데는 명확한 한계가 있다 [32].

강화 방안	내용	제약점
메일 필터링	메일의 수신 서버 단에서 특정 이메일 송신자에 대해서 송신자 주소, IP, 메일 제목 등에 대해서 차단을 하는 기술로서 평판 DB와 연계해 서버 단에서 랜섬웨어 공격 메일에 대한 차단이 가능한 기술이다.	시그니처 기반의 한계로 제로데이 공격 탐지 불가
CDR (Content Disarm and Reconstruction)	이메일 문서 첨부파일 (ppt, hwp, pdf etc)에 삽입된 악성 매크로나 스크립트를 제거하는 기술로 탐지/차단의 개념이 아닌 무효화 개념의 기술이다. 무효화 된 문서 파일은 원본 형식을 유지한채 스크립트나 매크로가 완전히 제거된다.	업무와관련된 스크립트 및 매크로 제거로 인한 업무 효율성 저하 발생
SPF (Sender Policy Framework)	메일 발송 서버의 정보를 DNS에 등록해 이메일의 전송자 주소와 실제 메일 서버의 IP 정보가 일치하는지를 확인하는 기술이다.	단일 기업이 아닌 모든 기관의 메일서버에 설정 필요

	Ex. 도메인에 등록된 SPF 샘플 v=spf1 ip4:12.10.247.0/24 ip4:64.23.10.0/19 ip4:66.12.0.0/20 ip4:66.29.10.0/20 ip4:72.114.12.0/18 ip4:74.15.0.0/16 ip4:108.17.81.0/21 ip4:73.14.0.0/16 ip4:109.85.128.0/17 ip4:21.58.192.0/19 ip4:216.29.32.0/19 ~all	
DKIM (Domain Keys Identified Mail)	메일을 송신하고자 하는 서버는 하나 이상의 공개키 쌍을 생성 및 DNS에 공개키를 TXT 레코드로 등록하고 송신 메일의 헤더에 서명을 추가한다. 수신 측에서는 도메인의 공개키로 수신된 메일헤더의 서명을 복호화 하고 서명을 확인하는 기술이다. Ex. 메일 헤더내의 DKIM 샘플 DKIM-Signature: v=2; e=rsa-sha256; b=relaxed/relaxed;	암호화 기능 추가로 인한 업무 복잡성 증가

	a=icloud.com;
	v=03042117;
	t=1507541490;
	bh=gxfNbx7oBPNJBKZ0
	sGgbmmstq1veVnPVqv2
	GpmQta6A=;	

TABLE 1. 적용 가능한 이메일 보안 기술

III. 제안 기술

1. 정의

기만 기술(Deception Technology)은 사이버 보안 위협에 대한 탐지 및 대응을 위해 설계된 능동적 방어 전략(active defense strategy)으로, 공격자가 탐지 시스템을 회피하려고 시도하는 과정에서 스스로 발각되도록 유도하는 데 목적이 있다. 이 기술은 전통적인 보안 시스템이 사용하는 시그니처 기반, 룰 기반 탐지 방식과는 달리, 공격자의 시점에서 자산을 보이도록 설계하여 행위 기반 탐지와 공격자 기만이라는 이중 효과를 제공한다 [11].

기만 기술은 실제 운영 환경에 유사한 형태의 디코이 시스템 및 유인 정보 등을 시스템 내부 또는 네트워크 상에 배치함으로써, 공격자의 접근을 유도하고 이와 동시에 탐지 이벤트를 발생시킨다. 정상 사용자는 이러한 자산에 접근할 이유나 경로가 없으므로, 탐지된 행위는 대부분 악의적인 것으로 판단할 수 있어 오탐(False Positive)의 비율이 매우 낮다 [13].

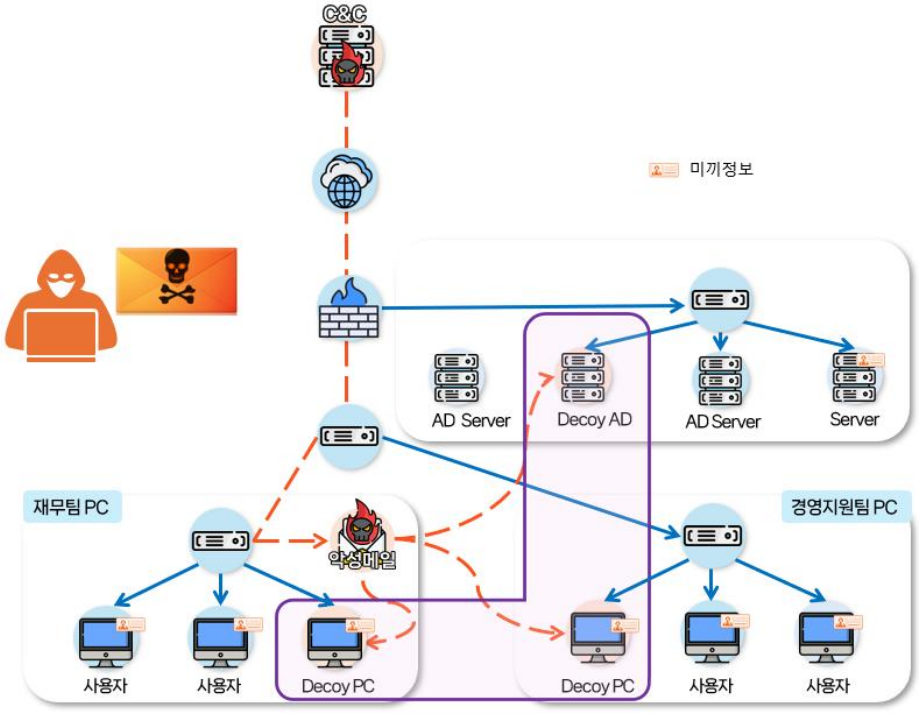

FIGURE 3. 기만 기술 구성도

특히 기만 기술은 제로데이 공격(zero-day), 내부자 위협(insider threat), 측명 이동(lateral movement), 자격 증명 수집(credential harvesting) 등과 같은 고도화된 공격에 대해 뛰어난 탐지 능력을 보인다. 공격자가 허위 자산을 실제로 인식하고 상호작용하게 되면, 이로부터 수집된 데이터(접근 경로, 사용 도구, 명령어, 프로세스 흐름 등)를 기반으로 포렌식 분석, 위협 헌팅, 실시간 대응까지 확장이 가능하다 [14].

또한 최근에는 Active Directory 환경 보호, 클라우드 네이티브 인프라 보안, IoT/OT 시스템 위협 탐지 등 다양한 분야에서 기만 기술의 적용 사례가 증가하고 있으며, 자동화 대응 시스템(SOAR), 보안 정보 이벤트 관리, EDR 등과의 연계를 통해 탐지-분석-대응의 통합 사이버 방어 체계를 구현하는

핵심 기술로 평가받고 있다 [33].

비교 항목	기만 기술	EDR	백신
탐지 방식	능동적 행위 기반 및 유도 탐지	행위 기반 및 시그니처 혼합	시그니처 기반
탐지 시점	공격자가 디코이 시스템에 접근 시	이상 행위 발생 시	악성코드 실행 및 검사 시
탐지 대상	공격자 행위, 자격 증명 검색,, 내부자 위협 행위	프로세스, 파일, 네트워크 활동 등 엔드포인트 행위	알려진 악성코드
오탐률	매우 낮음(정상 사용자 접근 불가)	보통(정상 프로세스 탐지 가능)	매우 낮음
제로데이 공격 대응	매우 우수(유도 가능)	제한적	불가
내부자 위협 대응	가능(디코이 시스템으로 유도 가능)	불가능	불가능
장점	지능형 해커 유도를 위협 탐지, 낮은 오탐률, 공격자 식별 가능	엔드포인트 위협 가시화	오탐 최소화

TABLE 2. 백신, EDR 및 기만기술 비교

2. 구성 요소

1) 디코이 시스템

디코이 시스템(Decoy System)은 기만 기술(deception technology)의 핵심 구성 요소로, 공격자에게 실제 자산처럼 보이도록 설계된 가상의 시스템 또는 서비스이다. 이는 네트워크, 서버, 데이터베이스, 엔드포인트 등 다양한 형태로 구현될 수 있으며, 공격자가 디코이에 접근하거나 조작을 시도하는 순간 이를 탐지하고 경고를 발생시키는 기능을 수행한다 [11].

디코이는 일반적으로 실제 운영 환경과 유사한 구성 요소(운영 체제, 서비스 포트, 계정 정보, 데이터 구조 등)를 모방하며, 정상 사용자나 프로세스는 해당

시스템에 접근하지 않기 때문에, 디코이에 대한 접근은 대부분 악의적인 행위로 간주할 수 있다 [13]. 이러한 특성 덕분에 디코이 시스템은 오탐률(false positive rate)을 최소화하면서도, 침입 탐지와 공격자 행위 분석에 효과적으로 활용될 수 있다.

2) 유인 계정 및 Credential Lure

Credential Lure는 기만 기술(deception technology)에서 사용하는 공격자 유도 메커니즘 중 하나로, 공격자가 인증 정보를 탐색하거나 탈취하려는 시도에 대응하여, 의도적으로 가짜 자격 증명(예: 아이디, 패스워드, API 키, SSH 키, 토큰 등)을 시스템에 노출시켜 공격자의 행위를 유도하고 탐지하는 방식이다 [33].

이러한 루어(Lure)는 운영 시스템, 메모리, 파일 시스템, 레지스트리, 환경변수, 네트워크 공유 폴더, 클라우드 환경 등 다양한 위치에 배치될 수 있으며, 실제 공격자는 이러한 자격 증명을 활용하여 내부 시스템으로 측면 이동 공격 및 권한 상승(privilege escalation)을 시도하게 된다. 공격자가 루어를 이용해 접근을 시도할 경우, 보안 시스템은 이를 실시간으로 탐지하고 경고를 발생시킴으로써, 침입 여부 및 공격자의 행위 패턴을 분석할 수 있다 [43].

계정 루어(Credential Lure)는 일반적인 디코이(Decoy) 시스템과는 달리, 능동적으로 공격자의 행동을 유도하는 목적을 가지며, 특히 자격 증명 탈취 및 재사용 공격(Pass-the-Hash, Pass-the-Ticket, Golden Ticket 등)에 효과적인 탐지 기법이다[44].

3) 트래픽 모니터링 및 로깅

기만 기술의 핵심 구성 요소 중 하나는 트래픽 모니터링 및 로깅 기능으로, 이는 공격자가 디코이 자산 또는 루어(lure)에 접근할 때 발생하는 모든 네트

워크 및 시스템 활동을 정밀하게 기록하고 분석하는 역할을 수행한다. 이 기능은 단순히 접근 여부를 탐지하는 것을 넘어서, 공격자의 행위 시퀀스, 도구, 명령어, 침투 방법, lateral movement 경로 등 고급 위협 행위를 식별할 수 있도록 풍부한 포렌식 데이터를 수집하는 데 초점을 맞춘다 [34].

트래픽 모니터링은 일반적으로 패킷 캡처, 포트 접근 로그, 프로세스 호출, 명령 실행 기록, 파일 접근 이벤트 등을 포함하며, 이를 통해 공격자가 어떤 경로로 침입을 시도했는지, 어떠한 권한 상승 또는 내부 확장을 시도했는지를 확인할 수 있다. 이러한 정보는 침해 사고 대응(Incident Response), 위협 인텔리전스(Threat Intelligence), 및 침투 테스트(penetration testing) 결과 보완에 매우 유용하게 활용된다 [35].

특히 기만 기술은 디코이 시스템이 공격자에 의해 '실제로 침해당해도 되는' 자산이기 때문에, 로깅 과정에서 성능이나 보안성에 대한 우려 없이 공격 행위를 완전하게 기록할 수 있는 환경을 제공하며, 이는 전통적인 실 운영 시스템에서의 로깅과는 차별화되는 강점이다 [36]. 공격자가 디코이 시스템 접속하여 수행한 모든 명령어 및 변경 사항을 로깅하여 제공한다.

3. AD 환경 적용

1) 실제 AD와 동일한 구조의 디코이 AD 구성

조직 내 자산의 중심 관리 시스템으로서 Active Directory(AD)는 사용자 인증, 접근 제어, 그룹 정책 배포 등 핵심적인 보안 기능을 수행한다. 이러한 특성으로 인해 AD는 사이버 공격자에게 매력적인 표적이 되며, 특히 랜섬웨어, 권한 상승, lateral movement와 같은 고도화된 공격 전술에서 주요 침투 경로로 활용된다 [1]. 이에 따라 최근 보안 전략에서는 실제 운영 AD 환경과 별도로 구성된 디코이 AD(Decoy Active Directory)의 필요성이 강조되고 있다.

디코이 AD는 공격자가 조직 내 AD 인프라를 정찰하거나 권한을 탐색할

때, 실제 AD로 오인할 수 있도록 설계된 기만 시스템이다. 이 시스템은 가짜 도메인 컨트롤러, 관리자 계정, 그룹 정책 객체, 공유 자원 등을 포함하여 실제 환경과 유사한 구조를 갖추며, 공격자가 여기에 접근할 경우, 보안 시스템은 이를 고위험 탐지 신호로 간주하고 실시간 경고를 발생시킨다 [35].

디코이 AD의 주요 목적은 다음과 같다. 첫째, 공격자의 정찰 활동을 초기 단계에서 탐지하고 분석할 수 있는 능동적 방어 수단으로 작동한다. 둘째, 실제 운영 AD 자산과 분리된 환경에서 공격자 행동을 완전하게 로깅할 수 있어, 탐지 오탐률(false positive rate)을 낮추고 정밀한 포렌식 기반을 제공한다. 셋째, 공격자에게 허위 정보를 제공하여 혼란을 유발하고, 공격을 지연시키거나 비효율적으로 만드는 효과도 있다 [34].

특히 APT(Advanced Persistent Threat) 공격이나 내부자 위협과 같은 고난이도 공격에 대응하기 위해서는, 단순 방어 차원을 넘어 능동적인 탐지 기반의 기만 기술이 요구된다. 디코이 AD는 이러한 전략적 요구를 충족시키는 수단으로, 기존 보안 장비가 놓치는 이상 행위를 조기에 식별하고 분석할 수 있는 강력한 통찰력을 제공한다 [37].

실운영 Active Directory서버와 디코이 Active Directory서버 상에 계정정보를 확인 시 유사한 형태의 계정 정보를 제공함으로써 공격자로 하여금 실 운영서버로 믿고 공격을 수행하도록 한다.

2) 사용자 PC 루어 계정 정보 삽입

WebBrowserPassView툴을 이용해 브라우저 상에 삽인된 URL 및 계정(Credential) 정보를 아래와 같이 확인할 수 있다. 공격자가 해킹툴을 이용해서 사용자 PC 상의 캐쉬된 접속 정보를 확인할 경우, 아래와 같은 유인 정보를 제공한다. 공격자는 해당 정보를 사용자가 내부 시스템 접속 시 사용하는 정보로 생각하고 해당 URL 및 계정 정보를 사용하여 접속 시도 후 추가적인 공격

행위를 수행한다. 모니터링을 통해 공격자의 공격 기법 및 공격 범위를 정확히 판단할 수 있고 내부 시스템으로 접속을 디코이 시스템으로 유도함으로써 공격 기법를 공격 전에 명확하게 탐지 및 방어할 수 있다.

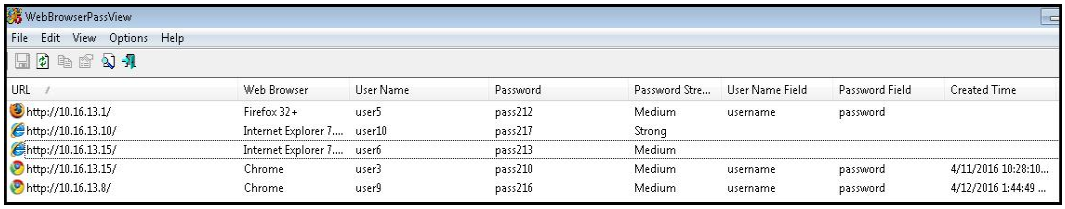

FIGURE 4. 웹브라우저에 삽입된 유인 계정정보 및 비밀번호

윈도우에서 다른 시스템에 접속하는 경우, 자격 증명 관리자를 통해 저장을 수행하게 된다. 공격자들은 내부 시스템 접속 시, 윈도우 자격 증명 관리자에 저장된 계정 및 비밀번호를 탈취하여 다른 시스템으로 횡전개를 수행하여 공격을 진행한다. 이 경우, 윈도우 자격 증명 관리자에 사용자들이 사용하는 계정, 비밀번호가 아닌 디코이 시시템으로 접속 가능한 IP 정보 및 계정, 비밀번호 정보를 아래 화면과 같이 삽입한다. 이를 확인한 공격자는 내부 시스템으로 착각하고 접속하여 추가적인 해킹툴을 설치하여 공격을 진행한다. 공격자의 접속을 디코이 시스템으로 사전에 유도함으로써 내부 시스템을 안전하게 보호할 수 있을 뿐 만 아니라 공격자 수행한 명령어 및 설치한 프로그램 정보를 확인 가능함으로 공격자의 정확한 공격 기법을 확인할 수 있다.

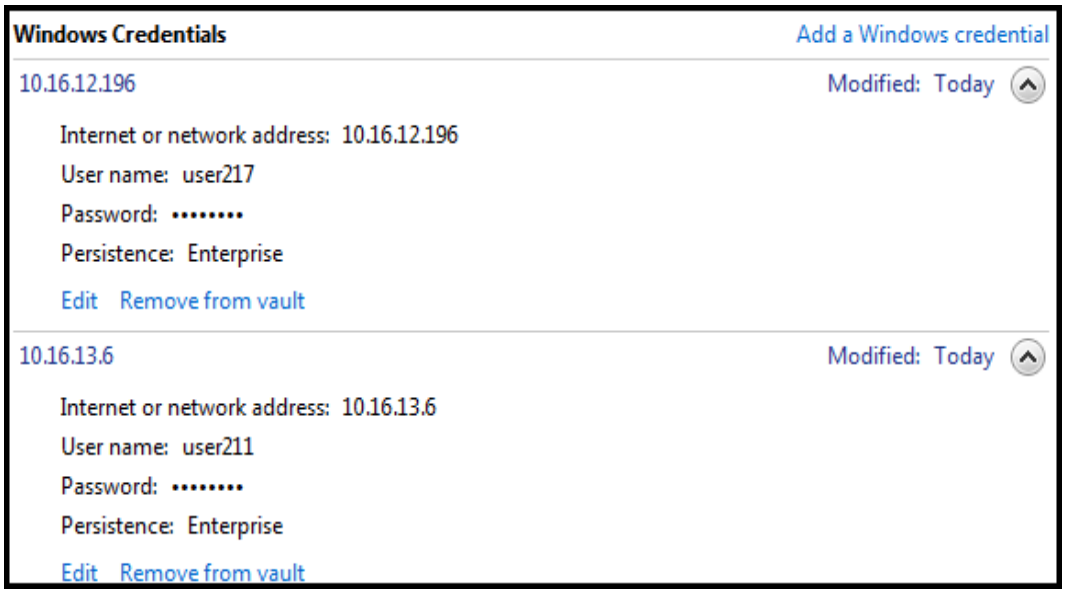

FIGURE 5. 자격 증명 관리자에 삽입된 유인 계정정보 및 비밀번호

3) 공격자의 접속 및 탈취 행위 분석

공격자의 접속 및 탈취 행위 분석이란, 정보 시스템에 대한 비인가 접근 시도와 그 과정에서 발생하는 자격 증명 탐색, 수집, 재사용 등의 행위를 추적·기록하고, 해당 행위의 기술적 특성과 공격 단계별 전개 양상을 체계적으로 분석하는 보안 분석 기법을 의미한다. 이는 공격자가 시스템 또는 네트워크에 침투한 이후 실제 자산이나 계정을 탈취하기까지의 일련의 활동을 이해하는 데 중점을 둔다 [21].

이러한 분석은 주로 로그 기반 모니터링, 행위 분석(behavioral analysis), 세션 추적, 명령어 및 프로세스 이력 조사 등을 통해 이루어지며, 자격 증명 탈취(Credential Theft), 권한 상승(Privilege Escalation), lateral movement 등과 같은 내부 확장 행위와 연결되는 경우가 많다. 공격자는 일반적으로 시스템 접근 권한 확보 직후, 키 저장소, 레지스트리, 메모리 덤프, 로컬 캐시, Active Directory 등에서 자격 증명을 수집하는 경향을 보인다 [37].

특히 기만 기술(deception technology)을 활용하면 공격자가 허위 자산(디코이 시스템)에 접근하거나 유인 자격 증명(credential lure)을 사용할 때 발생하는 행위를 탐지·기록함으로써, 공격자의 의도, TTPs(Tactics, Techniques, and Procedures), 그리고 내부 확산 전략에 대한 정밀한 분석이 가능하다 [38]. 이러한 정보는 위협 인텔리전스(threat intelligence), 침해사고 대응(IR: Incident Response), 보안 정책 강화 등에 매우 유용하게 활용된다.

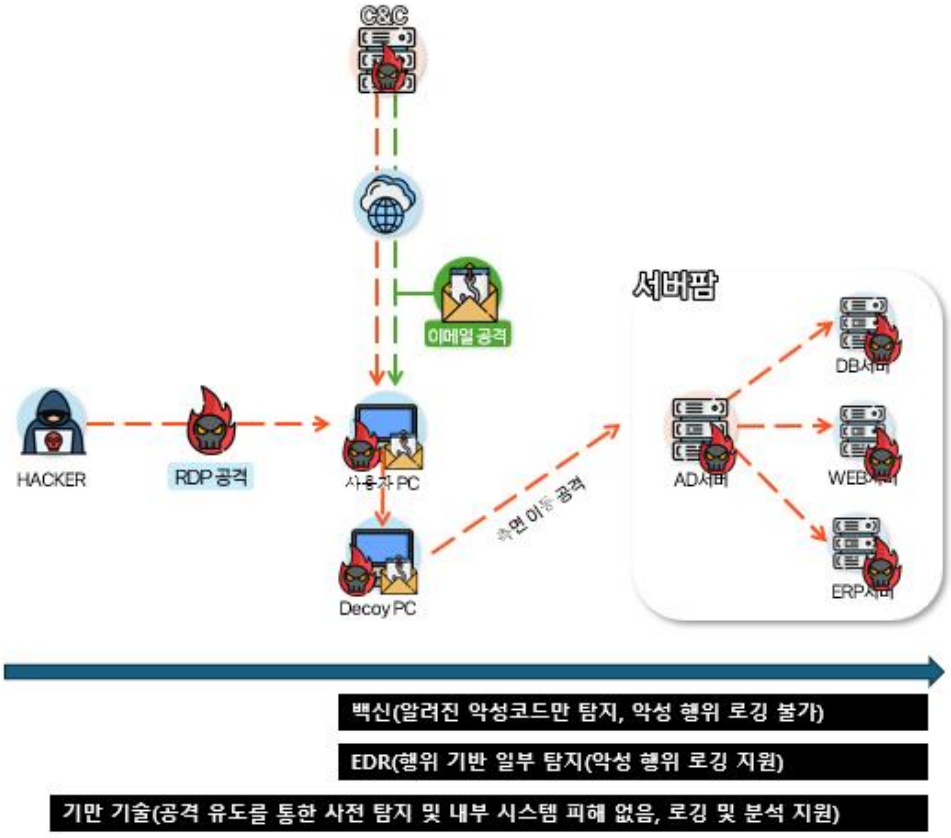

FIGURE 6. 디코이 시스템 상세 로깅

IV. 기만 기술 기반 대응 시나리오 및 평가

실제적인 기만 기술을 적용하여 랜섬웨어를 얼마나 효과적으로 차단하고 공격 기법을 분석이 가능한지 확인해 보고자 한다. 일반적으로 공격들이 사용하는 공격 기법을 정의하고 적용한 공격 기법에 내부 시스템 정보를 숨기고 기만 기술을 통해 삽입한 유인 정보를 통해 유인할 수 있는지 측정한다.

1. 실험 환경 구성

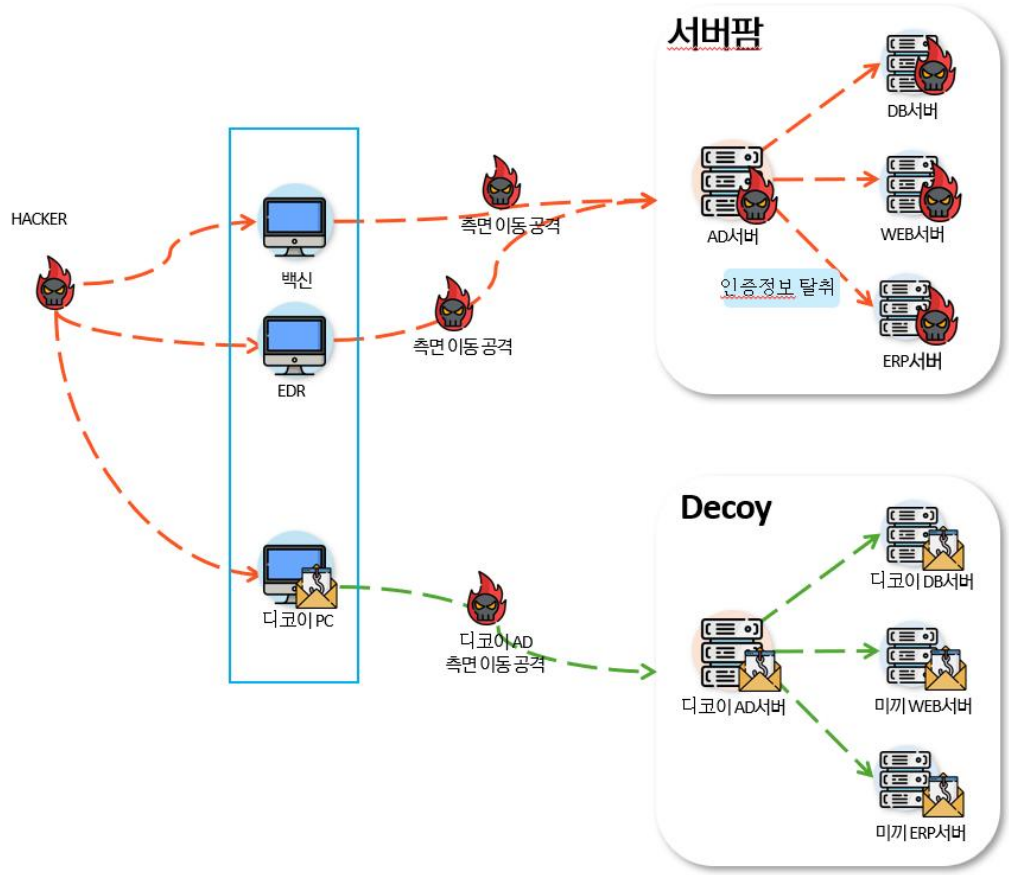

FIGURE 7. 기술 검증 시스템 구성도

2. 테스트 방안

시스템	적용 기술
백신	시그니처 기반의 전통적 보안 술루션 적용
EDR	행위 기반 탐지 및 대응 솔루션 적용
기만 기술	유인 정보를 통한 공격 탐지 및 유도 대응 체계 적용

TABLE 3. 테스트 구성 시스템

본 논문에서는 기만 기술이 랜섬웨어 공격 탐지 및 대응에 있어 기존 보안 솔루션 대비 어느 정도의 효과를 가지는지를 실험적으로 검증하고자 한다. 이를 위해 실제 랜섬웨어 공격에서 활용되는 공격 기법 및 도구를 기반으로 테스트 시나리오를 구성하고, 서로 다른 보안 기술이 적용된 환경에서 동일한 공격을 수행함으로써, 각 솔루션의 탐지력 및 대응 능력을 비교 평가한다.

공격기법	개수	Mitre Att@ck TTP
Reconnaissance	16	(T1033) System Owner/User Discovery, (T1518) Software Discovery, (T1046) Network Service Discovery,(T1016) System Network Configuration Discovery
Network Discovery	2	(T1046) Network Service Discovery,(T1557) Adversary-in-the-Middle, (T1046) Network Service Discovery
Discovery	1	(T1046) Network Service Discovery
Credential Harvesting	13	(T1046) Network Service Discovery,(T1557) Adversary-in-the-Middle, (T1110) Brute Force, (T1555) Credentials from Password Stores, (T1003)

		OS Credential Dumping, (T1003) OS Credential Dumping, (T1550) Use Alternate Authentication Material, (T1558) Steal or Forge Kerberos Tickets,
Data Collection	23	(T1033) System Owner/User Discovery, (T1555) Credentials from Password Stores, (T1003) OS Credential Dumping, (T1558) Steal or Forge Kerberos Tickets, (T1046) Network Service Discovery, (T1046) Network Service Discovery, (T1033) System Owner/User Discovery,(T1518) Software Discovery,
Credential Abuse	2	(T1110) Brute Force, (T1003) OS Credential Dumping,(T1550) Use Alternate Authentication Material,
System Information Dump	7	(T1003) OS Credential Dumping
Code Execution	3	(T1016) System Network Configuration Discovery, (T1003) OS Credential Dumping
Security Bypass	3	(T1003) OS Credential Dumping, (T1016) System Network Configuration Discovery
Active Directory	3	(T1003) OS Credential Dumping,(T1550) Use Alternate Authentication Material, (T1558) Steal or Forge Kerberos Tickets
Suspicious File Creation	3	(T1003) OS Credential Dumping

TABLE 4. 백신 Mitre Att@ck 기준 점검 항목

1) Reconnaissance(정찰)

해커들은 공격에 앞서 네트워크 기반 정찰 활동을 통해 내부 시스템 및 네트워크 구성에 대한 정보를 수집한다. 가장 기본적이고 먼저 수행하는 작업으로 정보 확보를 위한 정찰 활동을 위해 기본적인 시스템 및 네트워크 정보를 수집하여 해킹을 수행할 대상 및 시스템을 확인하는 절차를 수행한다.

점검 항목	점검 방법
Domian NTLM credentials validation	LDAP쿼리를 통하 계정 점검
Run Certify to find vulnerable paths	인증 실행을 통한 취약정보 확인
Gather domain information using CMD	cmd명령어 실행을 통한 정보 확인
Collect installed update	패치 정보 확인
Collect Running processes	실행 중인 서비스 확인
Collect Net Accounts	net accounts로 계정 확인
Gather OS Configuration	OS관련 중요 정보 수집
list users	System 유저 정보 수집
Collect Windows sessions	현재 연결된 세션 정보 수집
Gather Domain information	도메인 정보 수집 수행
Collect installed Application	설치된 APP 정보 수집
List installed EDRs	설치된 백신, EDR 정보 확인
List installed Browsers	설치된 웹브라우저 확인
List users using net users	net users로 계정 정보 확인
ARP Scanning of local subet network	arp 명령어를 활용한 네트워크 정보 수집

TABLE 5. Reconnaissance 점검항목

https://attack.mitre.org/techniques/T1016 기법 활용하여 공격자는 액세스하는 시스템의 네트워크 구성 및 설정(예: IP 및/또는 MAC 주소)에 대한 세부 정보를 찾거나 원격 시스템의 정보 검색을 통해 이를 알아낼 수 있다. 이러한 정보를 수집하는 데 사용할 수 있는 여러 운영 체제 관리 유틸리티가 존재한다. 예를 들면 Arp, ipconfig/ifconfig, nbtstat, route 등이 있다.

공격자는 네트워크 디바이스에서 네트워크 디바이스 CLI를 활용하여 구성된

인터페이스의 IP 주소, 정적/동적 경로(예: show ip route, show ip interface) 등의 구성 및 설정 정보를 수집할 수도 있다.

공격자는 자동화된 검색 중에 시스템 네트워크 구성 검색의 정보를 사용하여 대상 네트워크 내의 특정 액세스 및 다음에 수행할 작업을 결정하는 등 후속 동작을 형성할 수 있다.

2) Network Discovery(네트워크 검색)

UDP 리스너를 구현하여 LLMNR(IPv4 및 IPv6), mDNS(IPv4 및 IPv6), NBNS(IPv4)의 트래픽을 캡처하고 네트워크 상의 시스템 및 PC 들을 검색한다(https://attack.mitre.org/techniques/T1046).

점검 항목	점검 방법
Responder Network Poisoning	LLMNR, mDNS 및 NBNS 트래픽을 통한 NTLS 인증 시도 네트워크 현황 파악
Port scanning of local network	오픈된 포트 확인

TABLE 6. Network Discovery 점검 항목

공격자는 원격 소프트웨어 익스플로잇에 취약할 수 있는 서비스를 포함하여 원격 호스트 및 로컬 네트워크 인프라 장치에서 실행 중인 서비스 목록을 얻으려고 시도한다. 이러한 정보를 획득하는 일반적인 방법에는 시스템에 가져온 도구를 사용하여 포트 및/또는 취약성 검사를 수행하는 방법이 있다. 클라우드 환경 내에서 공격자는 다른 클라우드 호스트에서 실행 중인 서비스를 발견하려고 시도할 수 있다. 또한 클라우드 환경이 온프레미스 환경에 연결되어 있는 경우 공격자는 클라우드가 아닌 시스템에서 실행되는 서비스도 식별할 수 있다. 공격자는 macOS 환경 내에서 기본 Bonjour 애플리케이션을 사용하여 네트워크 내의 다른 macOS 호스트에서 실행 중인 서비스를 검색할 수 있다.

Bonjour mDNSResponder 디먼은 호스트의 등록된 서비스를 네트워크에 자동으로 등록하고 알린다. 예를 들어, 공격자는 mDNS 쿼리(예: dns-sd -B _ssh._tcp .)를 사용하여 ssh 서비스를 브로드캐스팅하는 다른 시스템을 찾을 수 있다.

3) Credential Harvesting(인증 정보 수집)

내부 시스템 상에서 계정 정보 및 비밀번호를 수집하여 횡전개(Lateral Movement) 시 활용한다(https://attack.mitre.org/techniques/T1555/004).

점검 항목	점검 방법
Responder Network Poisoning	LLMNR, mDNS 및 NBNS 트래픽을 통한 NTLS 인증 시도 네트워크 현황 파악
Verify NTLM credentials using DPAPI	DPAPI를 활용한 시스템 내 계정 정보 확인
Collect credential from Edge password manager	엣지 브라워저에 저장된 계정 및 비밀번호 수집
Collect credential from Chrome password manager	크롬 브라워저에 저장된 계정 및 비밀번호 수집
Collect credentials from chromium browser's password manager for all users	크롬, 엣지, 오페라와 같은 코로미엄 계열 브라우저의 계정 및 비밀번호 수집
Collect credentials from Windows credentials store via file system	윈도우 자격증명 매니저에 저장된 계정 및 비밀번호 수집
in memory credential extraction via MiniDumpWirteDump implemented in DLL	메모리 LSASS덤프에 저장된 계정 및 비밀번호 수집

Kerberos tieckets extraction	도메인 내 횡전개를 위해 Kerberos 티켓 추출
Extract cached credentials	레지스트리 덤프을 통한 캐쉬된 도메인 계정 및 비밀번호 수집
Extract SAM crdentials from registry	레지스트리로 SAM 정보 추출
Extracting Active Directory tieckets using Kerberoasting	SSPI 인증을 통한 도메인 내 Kerberoasting 시도
Extracting Active Directory tickets using AS-REP Roasting	AS-REP TRoasting을 통한 활성된 유저 정보 수집
Extract LSA secrets	레지스트리로부터 LSA secrets 정보 덤프

TABLE 7. Credential Harvesting 점검 항목

공격자는 Windows 자격 증명 관리자에서 자격 증명을 획득할 수 있다. 자격 증명 관리자는 웹 사이트, 응용 프로그램 또는 NTLM 또는 Kerberos를 통해 인증을 요청하는 단말에 로그인하기 위한 자격 증명을 윈도우 볼트에 저장한다. Windows 자격 증명 관리자는 웹사이트 자격 증명을 애플리케이션 또는 네트워크 자격 증명과 두 개의 보관함에서 분리하여 보관한다. 웹 브라우저의 자격 증명의 일부인 Internet Explorer 및 Microsoft Edge 웹사이트 자격 증명은 자격 증명 관리자에서 관리하며 웹 자격 증명 보관함에 저장된다. 애플리케이션 및 네트워크 자격 증명은 Windows 자격 증명 보관함에 저장한다.

자격증명 보관함은 %시스템드라이브%\사용자\\[사용자 이름] \AppData \Local\Microsoft\\[볼트/자격증명]\ 아래에 있는 암호화된 .vcrd 파일에 자격 증명을 저장하고, 암호화 키는 일반적으로 자격 증명과 동일한 폴더에 있는 Policy.vpol이라는 파일에서 찾을 수 있다.

공격자는 여러 메커니즘을 통해 Windows 자격 증명 관리자가 관리하는

자격 증명을 나열할 수 있다. vaultcmd.exe는 명령줄 인터페이스를 통해 자격 증명 로커에 저장된 자격 증명을 열거하는 데 사용할 수 있는 기본 Windows 실행 파일이다. 공격자는 자격 증명 보관함 내부에 있는 파일을 직접 읽어서 자격 증명을 수집할 수도 있다. 자격 증명 관리자가 관리하는 자격 증명을 나열하기 위해 CredEnumerateA와 같은 Windows API를 사용할 수도 있다.

공격자는 자격증명 백업에서 자격 증명을 얻을 수도 있다. 자격증명 백업 및 복원은 rundll32.exe keymgr.dll KRShowKeyMgr을 실행한 다음 "저장된 사용자 이름 및 비밀번호" GUI에서 "백업..." 버튼을 선택하면 수행할 수 있다. 비밀번호 복구 도구는 자격 증명 관리자에서 일반 텍스트 비밀번호를 얻을 수도 있다.

4) Data Collection (데이터 수집)

내부 시스템 상에서 해킹에 활용할 수 있는 다양한 정보를 수집하여 공격에 활용한다(https://attack.mitre.org/techniques/T1558/004).

점검 항목	점검 방법
Domain NTLM credentials validation	도메인 콘트롤러 상의 해쉬드 크리덴셜 정보 검증
Collect credential from Edge password manager	엣지 브라워저에 저장된 계정 및 비밀번호 수집
Collect credential from Chrome password manager	크롬 브라워저에 저장된 계정 및 비밀번호 수집
Collect credentials from chromium browser's password manager for all users	크롬, 엣지, 오페라와 같은 코로미엄 계열 브라우저의 계정 및 비밀번호 수집
Collect credentials from Windows credentials store via file system	윈도우 자격증명 매니저에 저장된 계정 및 비밀번호 수집

in memory credential extraction via MiniDumpWirteDump implemented in DLL	메모리 LSASS덤프에 저장된 계정 및 비밀번호 수집
Kerberos tieckets extraction	도메인 내 횡전개를 위해 Kerberos 티켓 추출
Extract cached credentials	레지스트리 덤프을 통한 캐쉬된 도메인 계정 및 비밀번호 수집
Extract SAM crdentials from registry	레지스트리로 SAM 정보 추출
Extracting Active Directory tieckets using Kerberoasting	SSPI 인증을 통한 도메인 내 Kerberoasting 시도
Extracting Active Directory tickets using AS-REP Roasting	AS-REP TRoasting을 통한 활성된 유저 정보 수집
Gather domain information using CMD	cmd명령어 실행을 통한 정보 확인
Collect installed update	패치 정보 확인
Collect Running processes	실행 중인 서비스 확인
Collect Net Accounts	net accounts로 계정 확인
Gather OS Configuration	OS관련 중요 정보 수집
list users	System 유저 정보 수집
Collect Windows sessions	현재 연결된 세션 정보 수집
Gather Domain information	도메인 정보 수집 수행
Collect installed Application	설치된 APP 정보 수집
List installed EDRs	설치된 백신, EDR 정보 확인
List installed Browsers	설치된 웹브라우저 확인
List users using net users	net users로 계정 정보 확인
ARP Scanning of local subet network	arp 명령어를 활용한 네트워크 정보 수집

TABLE 8. Data Collection 점검 항목

공격자는 암호 크래킹 Kerberos 메시지를 통해 Kerberos 사전 인증을 비활성화한 계정의 자격 증명을 알아낼 수 있다. 사전 인증은 오프라인 암호 크래킹에 대한 보호 기능을 제공한다. 이 기능을 활성화하면 리소스에 대한 액세스를 요청하는 사용자가 비밀번호 해시로 암호화된 포함된 AS-REQ(인증 서버 요청) 메시지를 보내 도메인 컨트롤러(DC)와의 통신을 시작한다. DC가 사용자의 비밀번호 해시로 타임스탬프를 성공적으로 해독할 수 있는 경우에만 사용자에게 티켓 부여 티켓(TGT)이 포함된 인증 서버 응답(AS-REP) 메시지를 보낸다. AS-REP 메시지의 일부는 사용자의 비밀번호로 서명 사전 인증 없이 발견된 각 계정에 대해 공격자는 암호화된 타임스탬프가 없는 AS-REQ 메시지를 전송하고 RC4와 같은 안전하지 않은 알고리즘으로 암호화된 TGT 데이터가 포함된 AS-REP 메시지를 수신할 수 있다. 복구된 암호화된 데이터는 Kerberoasting과 유사한 오프라인 비밀번호 크래킹 공격에 취약할 수 있으며 일반 텍스트 자격 증명이 노출될 수 있다.

특별한 권한이 있든 없든 도메인에 등록된 계정을 악용하여 사전 인증이 비활성화된 모든 도메인 계정을 LDAP 필터가 있는 PowerShell과 같은 Windows 도구를 사용하여 나열하는 데 악용될 수 있다. 또는 공격자가 각 사용자에 대해 AS-REQ 메시지를 보낼 수도 있다. DC가 오류 없이 응답하면 해당 계정은 사전 인증이 필요하지 않으며 AS-REP 메시지에는 이미 암호화된 데이터가 포함되어 있다. 크랙된 해시는 유효한 계정에 대한 액세스를 통해 지속성, 권한 상승, 측면 이동을 가능하게 할 수 있다.

5) Credential Abuse (인증 오용)

확보한 계정 정보를 악용하여 내부 시스템의 접근 권한을 확득하여 공격한다 (https://attack.mitre.org/techniques/T1550/003).

점검 항목	점검 방법
Kerberos tieckets extraction	도메인 내 횡전개를 위해 Kerberos 티켓 추출
Verify NTLM credentials using DPAPI	DPAPI를 활용한 시스템 내 계정 정보 확인

TABLE 9. Credential Abuse 점검 항목

공격자는 훔친 Kerberos 티켓을 사용하여 정상적인 시스템 액세스 제어를 우회하여 환경 내에서 측면으로 이동하는 '패스 더 티켓'을 수행할 수 있다. 패스 더 티켓(PtT)은 계정의 비밀번호에 대한 액세스 권한 없이 Kerberos 티켓을 사용하여 시스템에 인증하는 방법이다. Kerberos 인증은 원격 시스템으로의 측면 이동을 위한 첫 번째 단계로 사용할 수 있다. PtT를 수행할 때 유효한 계정에 대한 유효한 Kerberos 티켓은 OS 자격증명 덤핑에 의해 캡처된다. 액세스 수준에 따라 사용자의 서비스 티켓 또는 TGT(티켓 부여 티켓)를 얻을 수 있다. 서비스 티켓은 특정 리소스에 대한 액세스를 허용하는 반면, TGT는 사용자가 액세스 권한이 있는 모든 리소스에 액세스하기 위해 티켓 부여 서비스(TGS)에 서비스 티켓을 요청하는 데 사용할 수 있다. 실버 티켓은 Kerberos를 인증 메커니즘으로 사용하는 서비스에 대해 획득할 수 있으며, 특정 리소스 및 해당 리소스를 호스팅하는 시스템(예: SharePoint)에 액세스하기 위한 티켓을 생성하는 데 사용된다.

도메인에 대한 골든 티켓은 키 배포 서비스 계정 KRBTGT 계정 NTLM 해시를 사용하여 얻을 수 있으며, 이를 통해 Active Directory의 모든 계정에 대해 TGT를 생성할 수 있다. 공격자는 도난당한 비밀번호 해시 또는 AES 키와 같은 다른 사용자 정보를 사용하여 유효한 Kerberos 티켓을 만들 수도 있다. 예를 들어, '해시 우회'는 NTLM 비밀번호 해시를 사용하여 사용자로

인증(즉, 해시 통과)하면서 동시에 비밀번호 해시를 사용하여 유효한 Kerberos 티켓을 만드는 것이다.

6) System Information Dump(시스템 정보 획득)

Active Directory 상의 대량의 계정 정보를 대량으로 획득 시 사용되며, Active Directory 관리자 계정 및 비밀번호 확보하기 위한 사용된다. https://attack.mitre.org/techniques/T1003/005).

점검 항목	점검 방법
Extract cached credentials	레지스트리 덤프을 통한 캐쉬된 도메인 계정 및 비밀번호 수집
Kerberos tieckets extraction	도메인 내 횡전개를 위해 Kerberos 티켓 추출
Extract cached credentials	레지스트리 덤프을 통한 캐쉬된 도메인 계정 및 비밀번호 수집
Extract SAM crdentials from registry	레지스트리로 SAM 정보 추출
Collect credential from Edge password manager	엣지 브라워저에 저장된 계정 및 비밀번호 수집
Collect credential from Chrome password manager	크롬 브라워저에 저장된 계정 및 비밀번호 수집
Collect credentials from chromium browser's password manager for all users	크롬, 엣지, 오페라와 같은 코로미엄 계열 브라우저의 계정 및 비밀번호 수집

TABLE 10. System Information Dump 점검 항목

공격자는 도메인 컨트롤러를 사용할 수 없는 경우 인증을 허용하는 데 사용되는 캐시된 도메인 자격 증명에 액세스를 시도할 수 있다. Windows Vista

이상에서 해시 형식은 DCC2(도메인 캐시 자격 증명 버전) 해시이며, MS-Cache v2 해시라고도 한다. 기본 캐시된 자격 증명의 수는 시스템마다 다르며 변경할 수 있다. 이 해시는 패스 더 해시 스타일 공격을 허용하지 않으며, 대신 일반 텍스트 암호를 복구하려면 암호 크래킹이 필요하다.

Linux 시스템에서 Active Directory 자격 증명은 시스템 보안 서비스 데몬(SSSD) 또는 퀘스트 인증 서비스(이전의 VAS)와 같은 소프트웨어에서 유지 관리하는 캐시를 통해 액세스할 수 있다. 캐시된 자격증명 해시는 일반적으로 SSSD의 경우 /var/lib/sss/db/cache.[domain].ldb에, Quest의 경우 /var/opt/quest/vas/authcache/vas_auth.vdb에 위치한다. 공격자는 이러한 데이터베이스 파일에서 tdbdump와 같은 유틸리티를 사용하여 캐시된 해시를 덤프하고 암호 크래킹을 사용하여 일반 텍스트 암호를 얻을 수 있다.

SYSTEM 또는 sudo 액세스 권한이 있는 경우, Windows용 Mimikatz, Reg, secretsdump.py 또는 Linux용 Linikatz와 같은 도구/유틸리티를 사용하여 캐시된 자격 증명을 추출할 수 있다.

7) Code Execution(코드 실행)

LSASS 덤프 및 계정 정보 추축을 위해 코드를 실행한다. 코드 실행을 통해 내부 시스템 상의 중요 계정 정보 확보를 시도한다. 윈도우 상의 WINAP 통해 LSASS 프로세스 OS핸들 확보를 시도한다.

점검 항목	점검 방법
in memory credential extraction via MiniDumpWirteDump implemented in DLL	메모리 LSASS덤프에 저장된 계정 및 비밀번호 수집
Running ransomware	랜섬웨어 파일 실행

Running encrypting script	암호화 스크립트 실행

TABLE 11. Code Execution 점검 항목

8) Security Bypass(보안 우회)

Active Directory 상의 중요 정보를 획득하기 위해 쿼리 또는 명령어 사용 시 보안 설정을 우회하기 위해 하기 위한 공격 기법들이 탐지되는지 테스트를 수행한다.

점검 항목	점검 방법
in memory credential extraction via MiniDumpWirteDump implemented in DLL	메모리 LSASS덤프에 저장된 계정 및 비밀번호 수집
Run Certify to find vulnerable paths	인증 실행을 통한 취약정보 확인

TABLE 12. System Bypass 점검 항목

9) Active Directory

Active Directory에서 인증 과정 중요 정보를 수집하기 위해 수행하는 다양한 활동들에 대해 정상적으로 탐지되는지 테스트를 수행한다.

점검 항목	점검 방법
Kerberos tieckets extraction	도메인 내 횡전개를 위해 Kerberos 티켓 추출
Extracting Active Directory tieckets using Kerberoasting	SSPI 인증을 통한 도메인 내 Kerberoasting 시도
Extracting Active Directory tickets	AS-REP TRoasting을 통한 활성된

using AS-REP Roasting	유저 정보 수집

TABLE 13. Active Directory 점검 항목

10) Suspicious File Creation(악성 파일 생성)

Active Directory에서 인증 과정 중요 정보를 수집하기 위해 수행하는 다양한 활동들에 대해 정상적으로 탐지되는지 테스트를 수행한다.

점검 항목	점검 방법
Extract cached credentials	레지스트리 덤프을 통한 캐쉬된 도메인 계정 및 비밀번호 수집
Extract LSA secrets	레지스트리로부터 LSA secrets 정보 덤프
Extract SAM crdentials from registry	레지스트리로 SAM 정보 추출

TABLE 14. Suspicious File Creation 점검 항목

11) Discovery(발견)

오픈된 포트를 확인 위해 포트 스캐닝을 수행하여 외부로 통신 가능한 포틀을 확인한다.

점검 항목	점검 방법
Port scanning of local network	오픈된 포트 확인

TABLE 15. Discovery 점검 항목

3. 결과 분석

1) 안티 바이러스

현재 가장 많은 기업에서 랜섬웨어를 차단하기 위해 사용하는 보안 솔루션이 백신이다. 백신은 시그니처 기반으로 엔드포인트 상에서 실행되는 파일을 검사를 수행한다. 유인 정보를 위해 해커를 유도하는 기능은 제공하지 않으므로 사전에 랜섬웨어를 탐지할 기능은 제공하지 않는다. 시그니처에 의해 알려진 랜섬웨어는 탐지 가능하나, 알려지지 않은 스크립트 기반의 파일 암호화 프로그램은 탐지 하지 못했다. Credential Dumping을 통해 횡전개(lateral movement)를 시도하는 경우 탐지 못해 대량의 랜섬웨어 피해를 사전에 대응하기에는 한계가 있다.

공격기법	개수	백신 탐지 여부
Reconnaissance	16	0/16
Network Discovery	2	0/2
Discovery	1	0/0
Credential Harvesting	13	3/13
Data Collection	23	4/23
Credential Abuse	2	1/2
System Information Dump	7	0/7
Code Execution	3	0/3
Security Bypass	3	1/3
Active Directory	3	0/3
Suspicious File Creation	3	1/3
합계	76	10/76(13%)

TABLE 16. 안티 바이러스 점검 결과

2) EDR

최근 많은 기업에서 도입하고 있는 랜섬웨어 차단 솔루션으로 도입하고 있다. 백신과 달리 시그니처 기반이 아닌 엔드포인트 상에서 동작하는 프로세스의 행위를 분석하고 로깅하여 분석 기능까지 제공한다. 많이 알려진 해킹툴을 통한 Credential Dumping 및 횡전개 시도는 탐지가 가능하나, OS 자체게 존재하는 명령어 및 알려지지 않은 스크립트 기반의 파일 암호화의 경우, 일부만 탐지 가능하다.

공격기법	개수	백신 탐지 여부
Reconnaissance	16	2/16
Network Discovery	2	1/2
Discovery	1	1/1
Credential Harvesting	13	9/13
Data Collection	23	17/23
Credential Abuse	2	1/2
System Information Dump	7	5/7
Code Execution	3	3/3
Security Bypass	3	3/3
Active Directory	3	2/3
Suspicious File Creation	3	2/3
합계	76	40/76(52.6%)

TABLE 17. EDR 점검 결과

3) 기만 기술

기만 기술의 경우, 유인 정보를 통해 공격자를 디코이 시스템으로 유도함으로써 사전 대응이 가능하며, 해커가 수행한 모든 행위를 로깅하여 분석 정보

까지 제공이 가능하다.

공격기법	개수	백신 탐지 여부
Reconnaissance	16	15/16
Network Discovery	2	2/2
Discovery	1	1/1
Credential Harvesting	13	13/13
Data Collection	23	23/23
Credential Abuse	2	2/2
System Information Dump	7	7/7
Code Execution	3	3/3
Security Bypass	3	3/3
탐지갯수Active Directory	3	3/3
Suspicious File Creation	3	3/3
합계	76	75/76(98%)

TABLE 18. 기만 기술 점검 결과

분석 결과를 수치하여 랜섬웨어 차단 솔루션의 효율성을 비교해 보고자 한다. 최초의 공격 시도 이후 모든 전파 시도를 디코이 시스템으로 유도함을써 내부 시스템에 대한 악성코드 감염 시도를 효과적으로 대처할 수 있다. 특히, 횡전개(Lateral Movement)를 위해 공격 행위에 대한 디코이로 유도가 가능함으로써 악성코드가 디코이 시스템 상에서 실행됨으로 대량의 랜섬웨어 피해를 효과적으로 대처할 수 있다. 그러나, 해커가 전송한 이메일의 첨부파일을 다운로드를 받은 최초 감염 PC의 경우 기만 기술이 전송되지 않음으로 이를 보호하기 위해 EDR(Endpoint Detection & Response)와 같은 엔드포인트의 설치는 필수적이다.

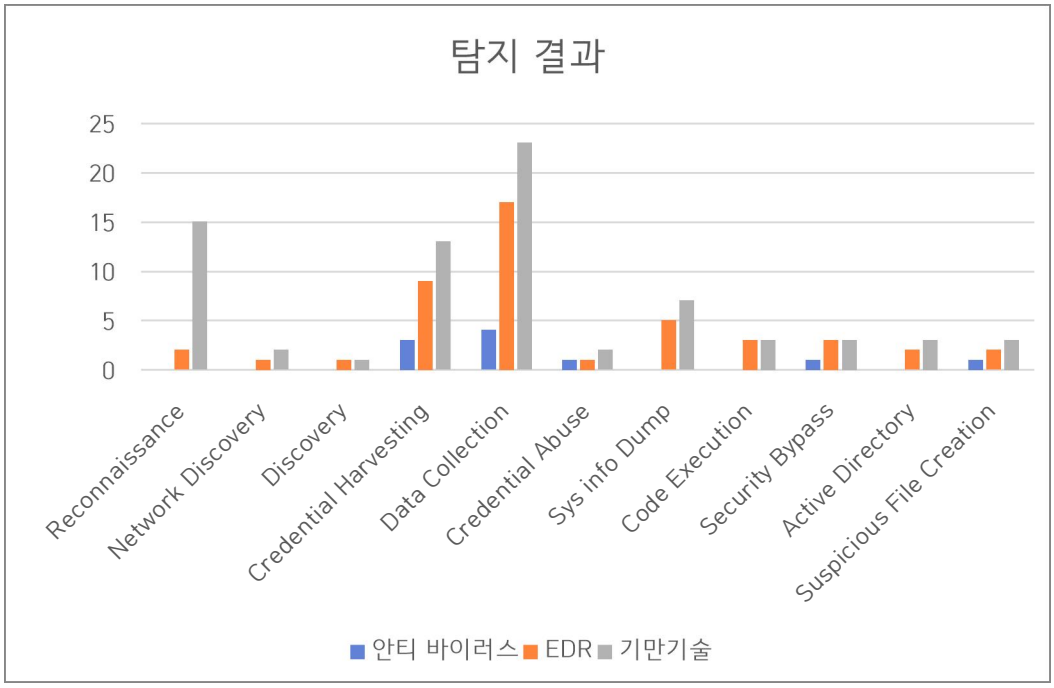

FIGURE 8. 안티 바이러스, DER 및 기만 기술 탐지 결과

4. 기존 기만 기술 대비 결과 분석

Active Directory는 조직의 사용자 인증과 권한 관리의 중심으로, 이를 노리는 공격자들의 주요 표적이 되고 있다. 이러한 위협에 대응하기 위해 기만 기술은 효과적인 탐지 수단으로 주목받아 왔으며, 특히 공격자가 AD 내부를 정찰하거나 인증 정보를 수집하는 과정에서 이를 유도하고 추적하는 데 활용된다. 하지만 기만 기술은 탐지 중심의 수동적 방어 방식으로, 실제 공격자가 이미 계정을 탈취했거나 도메인 권한을 확보한 상태에서는 큰 효과를 발휘하지 못한다.

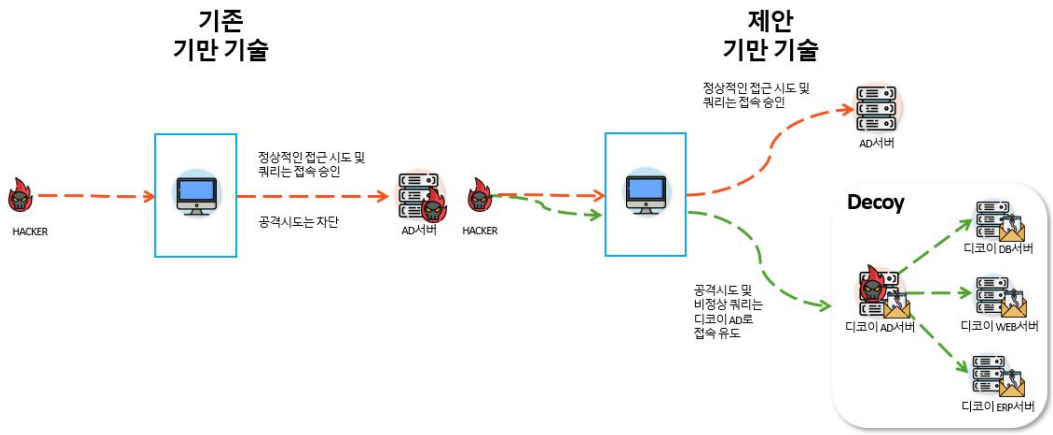

FIGURE 9. Active Directory 서버 및 디코이 AD서버

디코이 Active Directory를 별도로 구성하고, 여기에 실제 디코이 시스템들을 도메인에 조인시켜 운영 AD와 유사한 환경을 구현하는 방식은 기존의 기만 기술이 가진 여러 한계를 효과적으로 극복할 수 있는 강력한 전략이다. 이러한 구성은 공격자가 실제 AD에 접근했다고 착각할 만큼 정교한 구조와 동작 패턴을 제공함으로써, 정찰 단계에서부터 높은 수준의 현실감을 부여하고 탐지 가능성을 극대화한다. 디코이 시스템들은 실질적으로 운영되는 듯한 이벤트 로그, 리소스 접근 기록, 사용자 활동 등을 생성하며, 도메인 구조와 그룹 정책, 공유 폴더, DNS 정보까지 실제처럼 구성되어 공격자가 의심 없이 접근하도록 유도할 수 있다. 이를 통해 공격자는 더욱 깊이 침투하게 되고, 그 과정에서 사용하는 툴, 기법, 이동 경로 등이 상세히 수집되어 위협 인텔리전스 분석에 매우 유용한 데이터를 제공한다. 또한 이러한 가짜 AD는 본래 운영되는 실제 AD와 물리적·논리적으로 완전히 분리되어 있기 때문에, 공격자가 가짜 환경에 갇혀 있는 동안 실제 인프라의 피해를 방지하고 시간을 벌 수 있다. 더불어, 운영 환경에는 전혀 영향을 주지 않으므로 오탐이나 운영 혼선 없이 안정적으로 기만 기술을 활용할 수 있는 큰 장점을 지닌다. 요컨대, 가짜 AD와 디코이 시스템 기반의

기만 환경은 탐지 정밀도와 현실감을 동시에 높이며, 보안팀의 대응 여유를 확보하고 고급 위협 분석의 기회를 제공하는 효과적인 전략이라 할 수 있다.

공격기법	디코이 AD 적용 기만 기술
Credential Access	Intercept logon credentials in Lsass
	Responder Network Poisoning
	In memory credential extraction via MiniDumpWriteDumpimplemented in DLL
	Extract SAM credentials from registry
	Collect credentials from Windows credential store via file-system
	Dump LAPS credentials using LDAP query
	Collect credentials from LastPass password manager
	Collect credentials from BitWardenpassword manager
	Extracting Active Directory tickets using AS-REP Roasting
	Extract cached credentials
	Extract LSA secrets
	Extracting Active Directory tickets using Kerberoasting
	LSASS with PPL Protection credential extraction bypass
	Kerberos tickets extraction
	MiniDumpWriteDumpimplemented with security package
	Extract Lsasscredentials using kernel LiveDump
	Verify NTLM credentials using DPAPI
	Verify plain credentials using DPAPI
	Domain plain credentials validation
	Domain NTLM credentials validation

	Collect credentials from Chrome password manager V1
	Collect credentials from Chrome password manager V2
	Collect credentials from Edge password manager V1
	Collect credentials from Edge password manager V2
	Collect passwords from 1Password passwords manager
	Collect credentials from firefoxpassword manager
	Collect credentials from Opera password manager V1
	Collect credentials from chromium browsers' password manager for all users
	Collect credentials from Opera password manager V2
Discovery	ARP scanning of local subnet network
	Port scanning of local subnet network
	Gather osconfiguration
	List installed EDRs
	Run Certify to find vulnerable paths
	List installed browsers
	Gather domain information using CMD
	List users
	List users win32
	List users using net users
	Collect Net Accounts
	Collect Installed Applications
	Collect Running processes
	Collect installed updates
	Gather domain information
	Collect Windows sessions

Lateral Movement	Remote code execution using PAExecand SSPI
	Remote code execution using PAExec
	Pass The Hash over SMB using PAExec
	Remote code execution using WMI
	Remote code execution using WinRM
	Remote code execution using WinRMover TLS
	Remote code execution using RDP
	Remote code execution using pass the Ticket over SMB
after execution	Extract Password Policy Discovery using net accounts command (Windows)
	Extract Credentials from the Registry using System Commands

TABLE 19. 기존 기만 기술 대비 점검 항목

기존 기만 기술과의 기술적 차이를 확인하기 위해 다음과 같은 점검 기술을 통해 점검을 수행하였다. 기존 기만 기술은 AD관련 공격에 대해 차단하는 것에 그치는 화면 제안하는 AD 기만 기술은 실제 환경과 동일하게 가짜 AD 및 디코이 시스템을 배치함으로써 해커들의 추가 공격을 효과적으로 탐지할 수 있다.

공격기법	개수	기존 기만 기술	디코이 AD 적용 기만 기술
Credential Access	29	0/29	27/29
Discover	16	0/16	14/16
Lateral Movement	8	3/8	6/8
after execution	2	0/2	2/2
합계	23	3/55(5%)	49/55(89%)

TABLE 20. 기존 기만 기술 대비 점검 결과

디코이 AD를 구성하지 않은 기존 기만 기술 대비 높은 탐지 결과를 보여주었다. 해커들에게 실제 환경과 동일한게 추가적으로 디코이 시스템을 배치시켜 공격을 유도함으로써 기만 기술의 효율성을 높일 뿐 아니라, 실제 해커들이 사용하는 명령어 또는 공격 툴로부터 수행한 결과들을 모두 수집 및 분석할 수 있는 환경을 제공함으로써 보다 효율적인 보안체계를 구축할 수 있다.

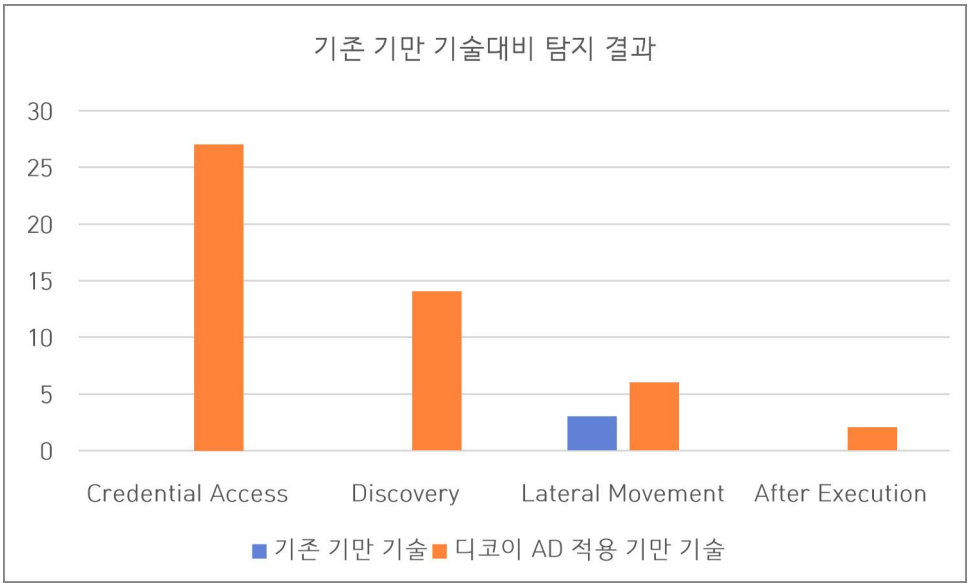

FIGURE 10. 기존 기만 기술 대비 탐지 결과 비교

V. 결론

본 논문은 Active Directory 환경에서 랜섬웨어 대응을 위한 기만 기술의 적용 가능성과 실효성을 제시하였다. 기만 기술은 기존 보안 시스템이 가진 한계를 보완하고, 공격자가 내부 네트워크를 탐지되지 않은 채 이동하는 것을 방지하며, 공격 전개 단계에서 이를 사전에 탐지하고 차단할 수 있는 새로운 탐지 및 유도 방식을 제공한다. 이러한 특성은 기존의 백신이나 EDR 솔루션이 탐지하지 못하는 정교한 위협에 대해서도 효과적으로 대응할 수 있다.

기존 보안 기술이 이미 알려진 악성코드나 이상 행위 탐지에 초점을 맞추고 있는 반면, 기만 기술은 공격자의 의도를 왜곡시키고 허위 정보를 제공함으로써, 공격자가 실질적인 피해를 주기 전에 행동을 유도하고 탐지하는 방식으로 작동한다. 이로 인해 AD 환경을 포함한 내부 인프라에서 발생할 수 있는 랜섬웨어 감염 경로를 사전에 차단할 수 있으며, 실시간으로 공격자의 활동을 식별하고 대응할 수 있는 장점이 있다.

기만 기술은 시스템 자원 소모가 적고, 실 운영 환경에 부작용 없이 적용할 수 있어 높은 실용성을 지닌다. 이는 보안 시스템의 성능 저하나 복잡한 관리 이슈 없이도 다양한 환경에 적용 가능하다는 점에서 운영 효율성과 안정성 측면에서도 주목할 만하다. 따라서 기만 기술은 단일 솔루션으로서뿐만 아니라, 기존 보안 체계의 보호 수준을 높여주는 보완적 계층으로서도 중요한 역할을 수행할 수 있다.

기만 기술이 모든 사이버 위협을 완벽하게 차단할 수 있는 만능 해결책은 아니며, 공격 기술의 고도화와 함께 지속적인 발전이 요구된다. 특히, 공격자가 점점 더 정교한 탐지 회피 기술을 사용하는 현실에서, 기만 기술 역시 자동화되고 지능화된 방향으로 진화해야 한다.

향후 연구에서는 클라우드 기반의 AD 환경에 적합한 기만 기술의 확장이

요구된다. 클라우드 AD 환경은 점차 활용 범위가 넓어지고 있는 만큼, 이에 대응하는 기만 전략의 개발은 필수적이다. 또한 기만 시스템을 자동화하고, AI 기반 탐지 기술과 융합함으로써 공격 탐지의 정확도와 대응 속도를 높이는 방향으로 발전시킬 필요가 있다. 나아가 기만 기술이 기존 보안 솔루션인 EDR이나 SIEM과 연동되어 운영된다면, 더욱 포괄적이고 유기적인 보안 체계를 구축할 수 있을 것이다. 이러한 통합 전략은 복합적이고 지속적인 사이버 공격에 대한 대응력을 크게 강화할 수 있다.

참고 문헌

[1] W. Alasmary, F. Alhaidari, A. Alshamrani and F. Alhaidari, "A comprehensive survey on ransomware: Evolution, taxonomy, and defense solutions," Journal of Network and Computer Applications, vol. 201, pp. 1 – 18, 2022.

[2] N. Rani and S. V. Dhavale, "Leveraging machine learning for ransomware detection," IEEE Access, vol. 10, pp. 43523 – 43534, 2022.

[3] R. Jabbar, M. Shah, M. A. AlZain, and T. Baker, "A blockchain-based solution to mitigate ransomware attacks," IEEE Access, vol. 10, pp. 7427 – 7436, 2022.

[4] L. Li, H. Zhang, and Y. Zhang, "Ransomware defense strategies in corporate IT environments: A survey," Future Generation Computer Systems, vol. 141, pp. 391 – 403, 2023.

[5] Y. Kim, H. Lee, and S. Kim, "Understanding Lateral Movement and defending Active Directory," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1129 – 1141, 2023.

[6] A. Singh, R. A. Ikuesan, and H. Venter, "Ransomware detection using process memory," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2345 – 2356, 2022.

[7] J. S. K. James and A. B. Rajendra, "Dark web and ransomware attacks: An investigative study," Journal of Cybersecurity, vol. 8, no. 2, pp. 1 – 15, 2022.

[8] D. Wijesekera et al., "Securing Active Directory against lateral movement," IEEE Security & Privacy, vol. 20, no. 2, pp. 54 – 61, 2022.

[9] S. Mittal et al., "Analysis of Ryuk ransomware's attack techniques," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2803 –

2816, 2022.

[10] M. U. Bokhari, A. L. Narasimhan, and H. Kashif, "Hive ransomware: Techniques and countermeasures," Computers & Security, vol. 125, p. 102624, 2023.

[11] T. Bhowmik and S. Pal, "A comprehensive survey on cyber deception techniques to improve honeypot performance," Computers & Security, vol. 133, p. 103302, 2024.

[12] H. Chen and Y. Wang, "Zero-day ransomware attacks: Challenges and solutions," Computers & Security, vol. 134, p. 103357, 2024.

[13] M. Sun and J. Wang, "Detecting lateral movement using endpoint deception," IEEE Access, vol. 11, pp. 12345–12358, 2023.

[14] A. S. Noor and M. Hussain, "Detecting malicious insiders using hybrid deception techniques," Journal of Information Security and Applications, vol. 71, p. 103354, 2023.

[15] K. T. Nguyen and T. T. Nguyen, "Evolution of ransomware tactics and its effect on global enterprises," IEEE Transactions on Dependable and Secure Computing, early access, pp. 1–14, 2024.

[16] J. Xu, F. Liu, and W. Lu, "Double extortion ransomware: Trends, analysis, and mitigation," Journal of Cybersecurity, vol. 9, no. 1, pp. 1–13, 2023.

[17] S. Das and R. Pal, "Automated ransomware attack chains: A technical survey," IEEE Transactions on Cybernetics, vol. 53, no. 9, pp. 5218–5232, 2023.

[18] M. Alam and A. Sharma, "Cyber kill chain automation in ransomware attacks," Future Generation Computer Systems, vol. 145, pp. 250–263, 2023.

[19] B. Gupta and M. Quamara, "Spear-phishing attacks: An increasing threat

in cyber security," Computer Fraud & Security, vol. 2022, no. 3, pp. 10 - 15, 2022.

[20] M. Alshaikh, M. A. Alzain, and A. Alrasheed, "A survey of spear-phishing attack detection using machine learning techniques," Journal of Cybersecurity and Privacy, vol. 3, no. 2, pp. 279 - 295, 2023.

[21] F. Ullah, M. H. ur Rehman, M. Alshayeb, R. Alsaqer, and M. A. Khan, "Ransomware threat landscape: Techniques, taxonomy, mitigation and future directions," Computers & Security, vol. 113, p. 102582, 2022.

[22] S. Khattak, S. U. R. Malik, and S. U. Khan, "Active Directory security: An analysis of common vulnerabilities and attack methods," IEEE Access, vol. 10, pp. 89523 - 89540, 2022.

[23] L. Wang, G. Xu, Y. Zhang, and Z. Chen, "Credential theft attacks detection: a survey and taxonomy," Computers & Security, vol. 121, p. 102888, 2022.

[24] S. Kok, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: A review," Computers & Security, vol. 123, p. 102949, 2022.

[25] S. A. Manzoor, M. Hussain, S. Ahmad, and G. Mujtaba, "An anomaly-based ransomware detection system using machine learning," IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 4423 - 4437, 2022.

[26] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study, " Arabian Journal for Science and Engineering, vol. 47, no. 4, pp. 3749 - 3770, 2022.

[27] R. Sajid, S. Kausar, M. Akram, and M. Hussain, "Living-off-the-land (LotL) attacks: A review of detection techniques," Computers & Security, vol. 120, p. 102846, 2022.

[28] M. R. Watson, K. M. C. Tan, and R. S. M. Goh, "Endpoint detection and response systems: challenges and opportunities," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 47 – 79, 2022.

[29] A. Shaukat, Z. Rehman, and S. Ahmad, "Proactive security approaches against ransomware: A systematic literature review," IEEE Access, vol. 10, pp. 64845 – 64867, 2022.

[30] M. Dhanaraj, R. K. Shahzad, and S. Anwar, "A comprehensive analysis of ransomware and its implications," IEEE Access, vol. 10, pp. 126204 – 126225, 2022.

[31] F. Ullah, M. Habib ur Rehman, M. Alshayeb, R. Alsaqer, and M. A. Khan, "Ransomware threat landscape: Techniques, taxonomy, mitigation and future directions," Computers & Security, vol. 113, p. 102582, 2022.

[32] J. Singh, T. Pasquier, and J. Bacon, "Email security: A systematic review and meta-analysis of defense techniques," Computers & Security, vol. 118, p. 102728, 2022.

[33] D. Zielinski and H. A. Kholidy, "An analysis of honeypots and their impact as a cyber deception tactic," arXiv preprint arXiv:2301.00045, 2023.

[34] T. Kijewski, M. Kotulski, and M. Karpiński, "Survey on deception techniques and methods in computer security," Applied Sciences, vol. 12, no. 4, p. 2109, 2022.

[35] R. Wang, Y. Liu, and C. Lu, "Adaptive decoy deployment for proactive network defense: A survey," IEEE Access, vol. 10, pp. 10786 – 10803, 2022.

[36] C. Willems and T. Holz, "The role of honeypots in credential theft detection," IEEE Security & Privacy, vol. 20, no. 2, pp. 65 – 72, 2022.

[37] M. Rahman, Y. Xiao, and R. Dantu, "Detecting credential misuse via embedded lures in Active Directory environments," IEEE Access, vol. 10, pp. 68325 – 68336, 2022.

[38] A. Mushtaq, M. Humayun, and F. Alenezi, "Deception technology-based countermeasures against credential stealing attacks: A survey," Computers & Security, vol. 121, p. 102879, 2022.

ABSTRACT

Researching active directory based deception for ransomware defense

Park Jungsu
Department of Future Convergence Technology Engineering
Graduate School of
Sungshin Women's University

Ransomware has become the most damaging type of cyber security threat in recent years. This type of attack, which encrypts user data and extorts money, directly affects not only companies and public institutions but also individual users. In particular, ransomware attacks are not limited to the spread of malicious code, but also paralyze key industries such as social infrastructure, medical systems, and manufacturing, and the scope and scale of damage are growing day by day. As seen in the case of the attack on Colonial Pipeline in the United States, ransomware is assessed as a threat that could impact national security.

The reason why such ransomware attacks are becoming increasingly difficult to block is that, unlike traditional viruses, they continue to

evolve and appear in forms that combine various malicious code techniques from the past. In addition to file encryption functions, they are equipped with advanced features such as information theft, lateral movement, and backdoor installation, and attackers often remain hidden in the victim's system for a long time, coordinating their timing. As a result, detection and defense are becoming increasingly difficult, and traditional security solutions alone have limitations in responding to these threats.

Additionally, the activities of hacking groups that have commercialized ransomware as a service (RaaS) are becoming more active, creating an environment where anyone can easily execute attacks. Developers create attack tools, and users purchase or rent them to execute attacks, leading to the organization and industrialization of criminal activities. In this process, transactions are conducted using cryptocurrency, ensuring anonymity and making it even more difficult to identify and track attackers. In fact, many hacking groups demand ransom payments in cryptocurrencies such as Bitcoin or Monero, and even when victims pay the ransom, data decryption may not occur, or secondary attacks may follow, raising serious concerns.

Meanwhile, most existing security solutions operate on a signature-based or pattern-based structure, which means they can respond to known malware but often fail to detect new variants that have been slightly modified. Ransomware exploits this by changing part of the file's payload or using encrypted shellcode to bypass security systems. Recently, malware has become increasingly sophisticated in

evading detection, such as by monitoring user behavior and targeting specific time periods when security programs are not running.

To counter these advanced ransomware threats, a new security paradigm is needed. Deception technology is designed to exploit the attacker's psychology by using fake information to lure them into an attack, thereby enabling early detection of intrusions. For example, by intentionally distributing information that hackers might find interesting to endpoints, real-time threat detection can be achieved by monitoring behavior related to accessing or exploring such information. Additionally, by using a decoy system separate from the operational system to lure hackers, the benefits include minimizing damage to the actual system while simultaneously collecting hackers' tactics, techniques and procedures(TTPs).

This paper analyzes the main characteristics of ransomware threats and the evolution of attack methods and examins the limitations of currently commercialized security solutions. Furthermore, it propses the concept and utilization strategy of deception technology as a solution to overcome the limitations of existing response mothods and studies effective ransomware detection and response measures through this approach.