정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

Active Directory 환경에서의 침해사고 동향 분석 및 활용방안

이 슬 기*, 김 가 영*, 김 동 욱*, 이 태 우*, 이 재 광*

요 약

기업 내부 전산망을 관리하는데 용이한 Active Directory(AD) 환경이 보편적으로 사용되는 가운데, 적절치 않은 정책 설정으로 대형 침해사고로 이어지는 경우가 발생하고 있다. AD는 다수 시스템과 사용자 등 자원을 관리하기 효율적이라는 장점이 있지만, 핵심 권한을 탈취당하면, 모든 자원에 접근할 수 있다는 반작용도 존재한다. 한국인터넷진흥원은 기업의 보안성 제고를 위하여 AD 환경에서 발생하는 침해사고를 상세히 분석하고 최신 동향을 지속적으로 공유하고 있다. 하지만, 침해사고 보고서는 사업 특성 및 구축환경의 다양성으로 인하여 획일화된 대응 전략을 제시할 수 없으며, 기업에 특화된 적용방안은 각자 마련해야 한다. 본고에서는 공개된 보고서를 기업 환경에 적용하기 어렵다는 문제를 해결하기 위하여 최근 발생한 AD 환경에서의 침해사고를 분석하고, 각 기업에서 어떻게 활용할 수 있는지 방안을 제시한다.

Ⅰ. 서 론

최근 대형 침해사고로 이어지는 대부분의 사이버 공격은 필연적으로 정보가 유출될 경우 사업영역에 막대한 악영향을 미칠 수 있으며 다수의 자원을 보유하는 특징을 보인다. 그러므로 공격대상은 다수의 자원을 관리할 수 있는 환경을 사용하는데, 그 중 대표적인 관리 환경이 Microsoft Windows Server에서 제공하는 Active Directory(AD)이다. 다수의 전산 자원을 소수의 IT 부서에서 관리하기 위해서는 일률적인 제어기능이 필요하기 때문에 핵심적인 단말기 또는 서버가 장악되면, 전사 리소스가 위협에 노출되게 된다. 공격자 혹은 공격그룹은 이러한 특성을 이용하여, 기업 내부로 침투한 후 측면이동(Lateral Movement)을 통해 서버 관리자의 권한을 획득하려 노력한다. 이후, 전사 자원에 대한 유출 및 랜섬웨어 감염을 수행하는 방식으로 공격이 진행된다.

유출된 기업 내부정보의 공개 및 암호화 해제를 인질로 삼아 가상자산을 취득하는 사이버 범죄 생태계 구축 이후, 랜섬웨어를 이용한 침해사고는 점차 확산하는 추세를 보인다. 탈취한 전산 자원의 질과 양이 많을수록 피해액이 늘어나는 구조는 침해사고의 대형화 트렌드와 연관 지어 생각해 볼 수 있다. 이러한 배경 속에서 보안업계에서는 적극적인 정보공유 활동을 통해 위협에 대응하려 노력하고 있다. 그 노력의 하나로 침해사고에 사용된 IoC(Indicator of Compromise) 수준의 공유에서 공격그룹의 전술 및 전략을 분석하여 공유할 수 있는 MITRE ATT&CK 도입까지, 공유하는 정보도 고도화되고 있다. 하지만, 발표되는 보고서를 기업이 어떻게 적용해야 하는지에 대한 요구사항도 언급되고 있다. 분석 결과의 효용성은 결국 수요자의 활용 수준에 따라 결정되기 때문에, 본고에서는 대형 침해사고를 유발할 수 있는 네트워크 환경에서 공격그룹이 어떻게 공격을 수행하는지 분석하고, 분석 결과를 기업이 어떤 방식으로 활용할 수 있는지에 대한 방안을 제시한다.

우선, 높은 점유율을 가진 만큼 대형 침해사고로 빈번하게 사용되는 Active Directory 환경과 최근 사이버 공격을 설명하기 위한 MITRE ATT&CK에 대하여 2장에서 설명한다. 이후, 최근 AD 환경을 공격하는 그룹에 대한 분석 및 분석 결과를 어떻게 적용하는지에 대하여 3장과 4장에서 구체적으로 제시한다.

* 한국인터넷진흥원 (선임연구원, sglee@kisa.or.kr; 주임연구원, kimky91@kisa.or.kr; 선임연구원, kimdw777@kisa.or.kr; 선임연구원, heavyrain@kisa.or.kr; 팀장, leejk@kisa.or.kr)

Ⅱ. 운영 환경 및 MITRE ATT&CK 소개

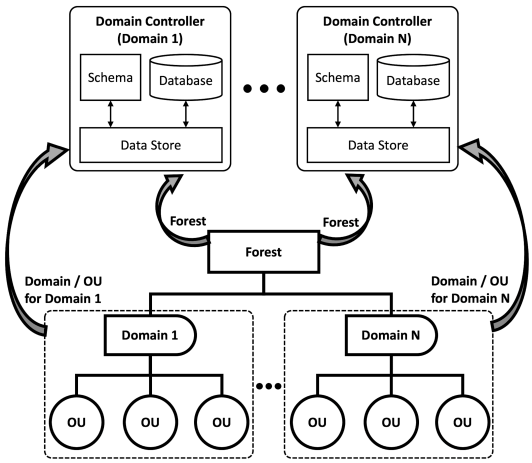
2.1. Active Directory

Active Directory는 Microsoft사에서 만든 디렉터리 서비스이다[1]. 디렉터리 서비스는 전산화하여 관리할 수 있는 모든 요소(파일, 사용자, 단말기, 네트워크 등)를 관리하고 구성하기 위한 서비스이다. 이러한 목적을 달성하기 위하여 다양한 플러그인 혹은 서비스들이 제공되며, 대다수의 기업들이 MS 윈도우 서버를 이용하여 Active Directory를 구성, 활용하고 있다. Windows Server는 기업 내부 전산망에서 약 72.1%가 사용하고 있으며[2], Active Directory 서비스는 Fortune 선정 상위 500개 기업의 95%가 사용하는 것으로 알려져 있다. AD 외 디렉터리 서비스로는 Redhat Directory Server, Apache Directory, OpenLDAP 등이 있으며, 윈도우 환경에서는 AD 환경에 가장 널리 쓰이고 있다.

Active Directory는 다음과 같은 논리적 구조와 기능으로 구성되어 있으며 일반적으로는 소수의 관리자가 다수의 사용자를 관리하는 중앙집중형과 같은 특성을 보유하고 있다[3].

AD에서 사용하는 논리적인 구조 중 대표적인 구조는 리소스를 지정하는 객체(Object), 현실에서의 조직을 전산화하여 관리를 용이하게 만들기 위한 구조인 OU(Organizational Unit), 도메인(Domain), 트리(Tree), 포레스트(Forest) 등이 있다. 특히, 트리, 포레스트, 도메인은 AD 네트워크를 그룹화하기 위한 요소로서, 그림 1과 같이 다수의 도메인이 트리를 이루고, 다시 다수의 트리가 포레스트를 구성하는 형식으로 관계된다.

위의 환경과 특성으로 인해 AD 환경에서는 소수에게 집중된 관리자의 권한을 공격자에게 탈취당한다면, 전사 리소스가 외부에 노출될 수 있다는 취약성을 보유하고 있다. AD 환경에서 발생할 수 있는 보안취약점을 보완하고 공개하고 있지만, 기업 내부에서 이를 적용하고 반영하는데 어려움이 있는 기업이 많다. 제로데이 취약점이 존재하는 서비스를 이용하는 기업이 공격받을 수는 있지만 공개된 취약점을 패치하지 못한 기업이 공격당할 확률이 더 높을 것이다. 또한, 취약점이 존재하는 것을 알더라도 비즈니스 효율성을 위하여 레거시 시스템을 운영하는 기업 또한 위협에 노출되어 있다.



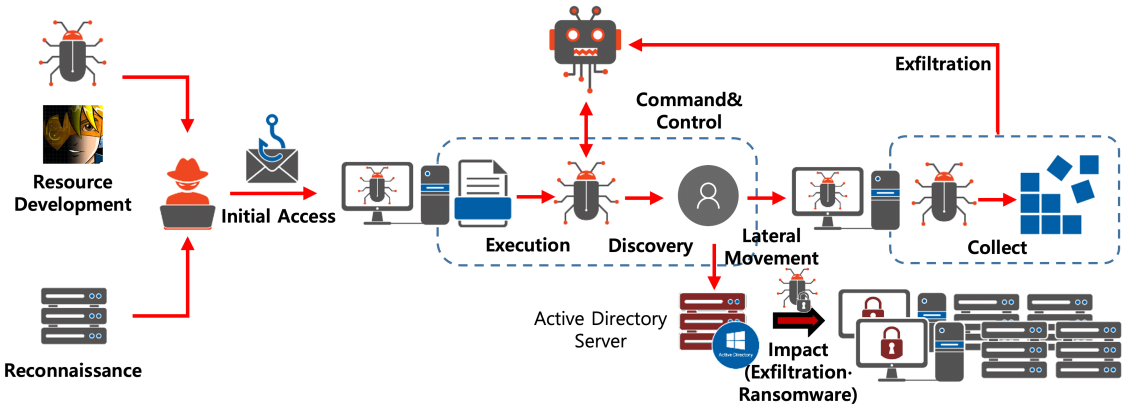
〔그림 1〕 Active Directory 데이터 구조 및 스토리지 설계

최근 발생하는 대형 침해사고는 직접적으로 관리자를 공격하는 것이 아니더라도, 일반 임직원의 단말기로 접근하여 '측면이동'을 이용, 관리자에게 접근한다. 이후, 관리자 권한을 탈취, 최종적으로는 전사 네트워크의 핵심 자산을 탈취하고, 랜섬웨어로 감염시키고 비용지불을 청구하는 방식으로 진행된다. 이러한 대형 침해사고를 방지하기 위하여, 기본적인 취약점 패치 등 보안 업데이트를 수행함과 동시에 내부 시스템의 보안정책 재점검이 필요하다.

2.2. MITRE ATT&CK

보안성을 향상시키기 위해서는 기업이 사용하는 환경에 대하여 지속적인 보안조치를 수행함과 동시에 현재 진행 중인 침해사고에 대한 전략·전술을 구체적으로 파악하고 적용하려는 노력이 수반되어야 한다. 과거부터 현재까지 공개되고 있는 침해사고에 대한 분석 보고서는 침해사고에 대한 전반적인 흐름을 신속하게 확인할 수 있다는 장점이 존재하지만, 그만큼 실무자가 참고하여 적용하기 어렵다는 단점 또한 존재한다. 이러한 단점을 보안하기 위하여 MITRE ATT&CK(이하 ATT&CK)이 공개되어 사고분석 보고서에 적용되기 시작하였다.

ATT&CK은 록히드마틴社의 Cyber Kill Chain에 이어서, 최근 침해사고에 대한 보고서를 작성하는데 있어서 널리 활용되는 일종의 Framework이다. ATT&CK은 공격자가 사용하는 전술과 기법을 체계적으로 정리하여 구성하였으며, Tactics는 공격자가 달성



〔그림 2〕 Active Directory 공격 개요도

하고자 하는 목적이며, 해당 목적을 달성하기 위하여 사용되는 기법이 Techniques이다. 이러한 요소들을 사용하여 전체적인 침해사고를 표현하면 TTP(Tactics, Techniques, Procedure)로 정리될 수 있다.

ATT&CK은 지속적으로 업데이트가 되고 있으며, Tactics와 Techniques, 악성도구 및 공격그룹에 대한 정보의 지속적인 추가, Sub-techniques 도입 등 큰 범주에서의 프레임워크 변화 또한 진행되고 있다.

과거에는 침해사고에 사용된 악성코드, IP, 도메인 등을 침해지표(IoC; Indicator of Compromise) 형태로 공유하여 건별로 차단하였다. 하지만, 위의 ATT&CK과 같이 공격자의 전략 및 전술을 공유하여 반영함으로써 일부만 변형한 공격을 일괄적으로 차단할 수 있다면 더 큰 활용 가치가 존재한다. 이러한 장점으로 인해, ATT&CK이 더 널리 활용되고 있다.

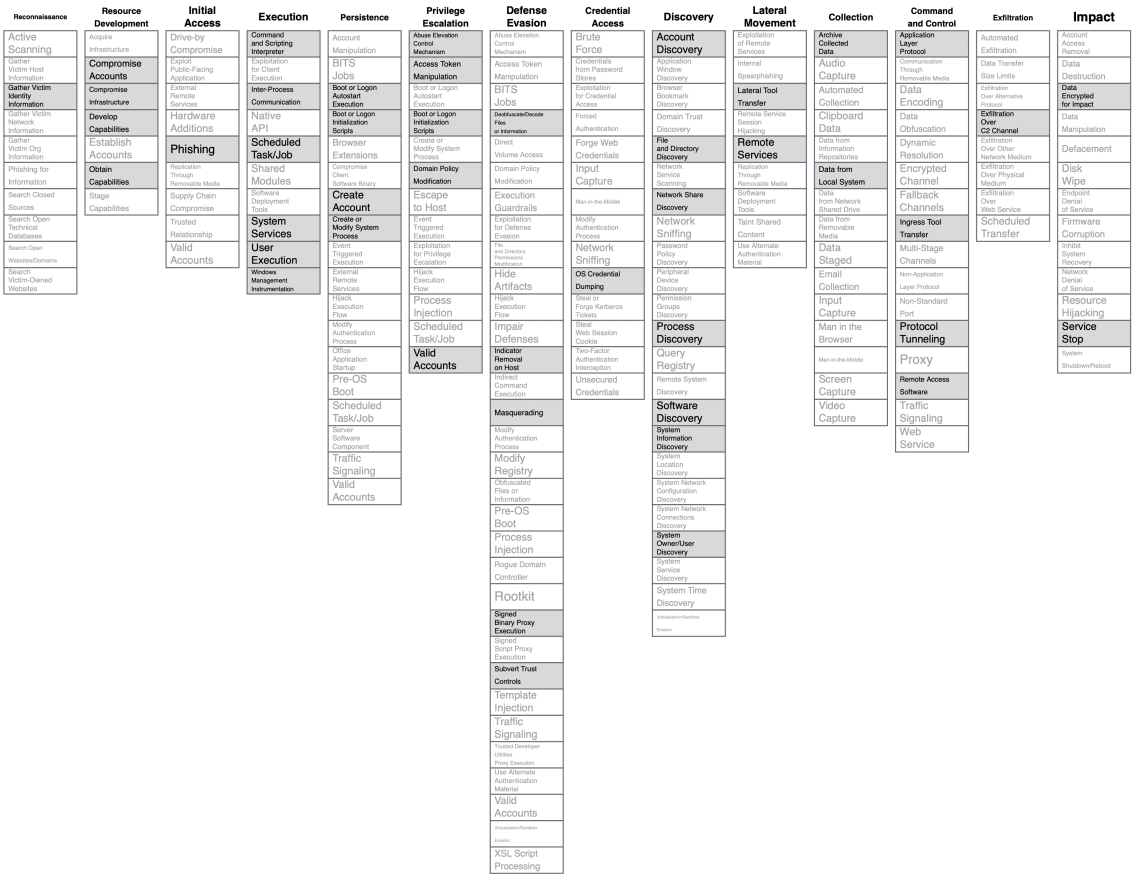
Ⅲ. Active Directory 환경을 위협하는 공격

Cyber Kill Chain과 마찬가지로 ATT&CK은 발생한 보안위협을 체계적으로 분석하여 정리할 수 있도록 도와준다. ATT&CK을 이용한 침해사고 분석 보고서, 시스템들이 적극적으로 공개되고 있으며 ATT&CK의 Tactic 별로 공격의 대략적인 개요를 설명하고, 본문에서는 Technique을 통해 동작을 서술하는 형식으로 기술된다.

다음 그림 2는 최근 AD 환경을 대상으로 발생한 침해사고들을 분석하여 공통적으로 사용된 기법과 전술들의 특징을 정리한 개요도이다. 해당 TTP를 통해 중소기업부터 중견·대기업에 이르기까지 많은 기업들이 피해를 입었다.

최근 AD 환경을 지속적으로 공격한 공격그룹은 사전준비 단계에서 자체적으로 개발한 악성코드 및 침투도구를 개발하고, 외부에 공개된 도구를 수집한다. 이후 공격목표에 따라 아웃룩 데이터 파일 통해 이메일 정보를 수집하여 공격대상을 결정한다. 또한 명령제어 서버와 유포지로 사용하기 위한 인프라를 확보하고 공격 준비를 마무리한다. 관찰한 공격대상의 관심사항과 비즈니스로 인해 열람할 수밖에 없는 주제로 구성한 스피어 피싱은 공격자를 내부로 접근할 수 있도록 구성된다. 이후 공격자는 원격제어 악성코드를 통해 다양한 원격 명령을 수행한다. 기업 내부로 침투한 후에는 공개된 여러 취약점과 도구를 이용하여 손쉽게 측면이동이 가능하다. 공격자는 보편적으로 활용되는 측면이동의 기법인 SMB 포트를 통해 다른 시스템에 명령을 실행하고, 도메인 컨트롤러를 장악한다. 동시에 추가 악성코드 다운로드 및 실행을 통해 정보 수집·유출, 악성코드·이벤트 로그 흔적삭제 등 다양한 악성행위를 수행할 수 있다. 관리자 권한을 획득한 시점에서 전사 네트워크는 감염되어 공격자의 목적에 따라 피해가 발생한다.

AD 환경을 위협하는 최근 공격은 큰 범주에서 최초 침투, 측면이동, 관리자 권한 획득, 악성행위 수행의 순으로 진행된다. 공격자는 다수의 AD 공격경험으로 인해 방어자의 취약한 점을 습득하고 있으며, 이를 하나의 TTP로 구성하여 다수의 침해사고를 발생시키고 있다. 따라서 침해지표 수준의 기계식 대응보다 계속 사용되는 TTP를 이해하고 보안정책에 적용, 방어하는 것이 더욱 큰 효과를 보일 수 있다.



〔그림 3〕 AD 환경을 위협한 특정 공격그룹의 TTP

Ⅳ. 기업에서의 침해사고 보고서 활용 방안

과거 공유된 침해지표를 단순 차단하는 것은 공격자가 손쉽게 우회할 수 있다. 공격에 사용되는 도구 제작 및 침투기법을 연구·습득하고, 실제로 공격을 수행하는데 있어서, 침해지표 차단은 공격자에게 큰 위협이 되지 않는다. 악성코드 내부의 문자열 변경만으로 악성코드 해쉬는 변경되며, 도메인, IP 주소는 직접 작은 규모의 웹서버를 해킹하여 구성하거나 구매가 가능하다. David J Bianco가 제안한 고통의 피라미드는 바로 이러한 공격자가 대응하기 어려운 수준을 피라미드 형태로 구성한 그림이며, 가장 고통을 주는 대상은 TTP로 알려져 있다[4].

그림 2가 기존 침해사고 보고서에서 공격흐름을 신속히 파악할 수 있는 개요도라면, 그림 3은 체계적으로 공격자의 전략·전술을 분석한 결과이다. 그림 2는 침해사고가 발생하고 분석결과를 정리할 때 가장 앞에 표현되는 그림이다. 공격 개요를 신속히 확인할 수 있다는 장점이 존재하기 때문에 앞으로도 계속 사용될 것이다. 이에 덧붙여 그림 3은 그림 2보다 실무자 관점에서 보다 상세하게 분석된 결과이다. 침해사고의 개괄적인 내용 파악보다 어떠한 공격기법과 전략으로 침해사고가 발생하였는지 분석할 수 있으며, 대응 전략 마련에 최적화되어 있다. ATT&CK은 최종적으로 공격자의 TTP에 맞추어 자동으로 대응할 수 있도록 연구를 진행하고 있지만, 아직 그 단계까지 발전하지 않은 상황이다. 또한, 자동대응 수준으로 개선되더라도 최적화가 필요하기 때문에 TTP에 대한 이해와 적용은 기업에 필수적이다. 기존에는 그림 2의 개요도를 보고 추상적으로 대응방안을 마련해야 된다는 어려움이 존재하였지만 ATT&CK이 널리 활용되면서 점차 개선되고 있다. 하지만, 프레임워크가 침해사고 보고서에 적용되기 시작하고 현재까지, 기업에서는 TTP를 어떻게 활용해야 되는지 어려움을 가지고 있다.

4.1. AD 환경을 위협하는 공격에 대한 대응 전략

공격개요를 제공하는 수준에서 공격자의 TTP를 공유하는 수준으로 침해사고 보고서가 진화함에 따라, 실무자가 기업 정보보호 수준을 제고하기 위한 활동이 구체적으로 변화하고 있다. 기업 정보보호전문가는 침해사고 보고서의 사례 별로 공격 개요를 파악하고 기업 환경에 맞는 시나리오를 수립하여 자체적인 점검을 수행할 수 있다. 또한, ATT&CK을 이용하여 공격자의 목표달성을 위해 어떠한 기법들이 사용되었는지를 확인하여 구체적으로 완화전략(Mitigations)을 수립할 수 있다. AD 환경에서 발생한 많은 침해사고들을 분석하였을 때 공통적으로 사용된 기법과 전술들의 특징을 대응방안으로 정리하면 대형 침해사고로 이어지는 피해를 줄이거나 예방할 수 있다. AD 환경에서의 침해사고는 세 가지의 대표적 특징을 보인다.

첫 번째 특징은 측면이동을 진행할 때 나타나는 특징이다. AD 환경의 특성 상 중앙에서 정책 배포 등을 용이하게 만들기 위하여 SMB 포트를 사용한다. 공격자들이 SMB 포트를 이용하여 악성코드를 실행하는 기법은 서비스 설치 및 실행, 작업 스케줄러 등록, WMIC 기능 이용, PSEXEC 프로그램 사용 등으로 한정지어 고려해야 한다. 공격자의 이러한 기법에 대응하기 위해 모니터링 할 수 있는 포인트는 다음과 같다. 서비스 설치 및 실행 기법은 시스템 이벤트 로그에 서비스 설치 흔적(Event ID 7045)이 남게 되며, 작업 스케줄러를 통한 악성코드 실행은 이벤트로그-응용프로그램 및 서비스 로그-Microsoft Windows-TaskScheduler-Operational에 생성 흔적(Event ID 106)이 남게 된다. 위의 이벤트 로그는 기본적으로 비활성화 되어 있기 때문에 모니터링을 위해서는 활성화가 필요하다. PSEXEC 도구를 사용하는 경우 서비스 설치를 통해 실행되기 때문에 이벤트로그 7045를 탐지해야 한다. 서비스 설치 로그 및 스케줄러 설치 로그는 이미 운영 중인 상태의 서버에서는 해당 로그가 자주 발생하지 않는다. 따라서 AD 환경에서 주요 점점이라고 생각되는 서버에서 로그 모니터링 정책을 설정해둔다면 첫 번째 SMB 포트 사용을 통한 악성코드 실행 기법을 대응하는데 효과적일 수 있다.

두 번째는 측면이동 기법을 사용함에 있어서 파생되는 특징이다. 위의 이벤트로그에 공격흔적이 남기 때문에 공격자들은 이벤트 로그를 삭제한다. 따라서 삭제 이벤트인 Event ID 104, 1102를 탐지하여 비정상적인 로그 삭제를 모니터링 할 수 있다.

세 번째로 대규모 감염을 시도할 때 나타나는 특징이다. AD 환경의 특성상 대규모로 일괄적인 감염을 시도하게 되며, 도메인 컨트롤러의 정책배포 기능을 이용한다. 공격자는 그룹정책템플릿(GPT) 경로인 \\Windows\SysVol\{DomainName}\Policies\{PolicyGUID}\Machine\Scripts\Startup\에 악성코드를 생성하여 유포에 이용한다. 따라서 도메인 컨트롤러의 그룹정책의 추가 생성을 모니터링 해야 한다.

AD 환경의 대규모 악성코드 유포를 위해서 공격자는 도메인 컨트롤러 탈취를 목표로 한다. 도메인 컨트롤러에 침투하기 위해 가장 많이 사용되는 것이 관리자 계정의 탈취이다. 따라서 관리자 계정의 경우 한정된 시스템에만 사용해야 하며 관리자 계정을 최소한으로 사용하여 주요 관리 모니터링 대상을 줄이는 것이 필요하다. 관리자 계정을 사용하는 시스템이라면 위의 세 가지 방안에 대한 모니터링을 적용했을 때 공격이 진행되는 중간에 침해사고를 발견하여 공격자의 최종 목적(랜섬웨어 감염, 정보유출 등)을 막을 수 있다.

위의 대응전략을 실제 기업 환경에 적용하기 위하여 이용하는 보안장비의 설정방법에 따라 적절한 정책을 생성해야 한다. 보안이벤트를 통합·관리하는 SIEM (Security Information and Event Management) 장비의 공통 사용 포맷으로 Sigma 룰이 활용되고 있다. Sigma 룰은 로그를 기반으로 동작할 수 있도록 구성이 되어 있으며, 네트워크 트래픽의 Snort, 파일의 YARA와 같다고 할 수 있다 [5]. 침해사고를 표현함에 있어서 악성코드는 YARA를 이용하여 패턴을 탐지할 수 있으며, 단말기에서 발생하는 로그는 Sigma 룰을 이용하여 탐지할 수 있다.

방어자는 Sigma 룰을 이용해 침해사고 분석 보고서에서 공유되는 TTP의 각 기법 별로 탐지규칙을 표현할 수 있다. 또한, 이 탐지 규칙을 보안장비에 적용하여 내부에서 발생하는 위협을 탐지 할 수 있다. 아래 그림 4는 그림 2,3에서 분석한 AD 환경을 위협한 특정 공격그룹의 TTP를 탐지하기 위하여 구성한 Sigma 룰 예시이다. 위에서 설명한 것과 같이 탐지해야 하는 이벤트 로그가 어떠한 것인지와 그룹정책템플릿 경로를 통한 악성코드 유포를 탐지하기 위한 규칙을 정의할 수 있다.

```
action: global
title: Target Active Directory
status: experimental
description: Detect Attack in Active Directory.
author: KRCert RyanKDW
date: 2021/05/24
references:
tags:
    - attack.t1569.002
    - attack.t1053.005
    - attack.t1070.001
    - attack.t1037.003
    - attack.t1484.001
    - attack.t1036.005

falsepositives:
    - Software installation
level: high
---
logsource:
    product: windows
    definition : 'Detect Service Execution and ScheduleTask Creation.'
detection:
    service_powershell:
        EventID: 7045
        ServiceFileName|contains:
         - 'powershell.exe'
    service_cmd:
        EventID: 7045
        ServiceFileName|contains:
         - 'cmd.exe'
    service_bat:
        EventID: 7045
        ServiceFileName|contains:
         - '.bat'
    schedule_create:
        EventID: 106
    delete_system_log:
        EventID: 104
    delete_secure_log:
        EventID: 1102
    condition: 1 of them
---
logsource:
    product: windows
    definition : 'Detect EventLog Delete'
detection:
    delete_system_log:
        EventID: 104
    delete_secure_log:
        EventID: 1102
    condition: 1 of them
---
logsource:
    product: windows
    defination : 'Detect Group Policy Object Creation. Apply to Domain Controller'
detection:
    GPO_Create_log:
        EventID: 1502
    GPO_File_creation:
        TargetFilename|contains: '\\SYSVol\\*\\Policies\\*\\Machine\\Scripts\\*'
    condition: GPO_Create_log and GPO_File_creation
---
logsource:
    product: windows
    category: file_event
    defination : 'Detect Masquerading malware'
detection:
    malware_path:
        TargetFilename|contains:
         - 'C:\ProgramData\Adobe\'
         - 'C:\Intel\'
         - 'C:\hp\'
         - 'C:\ProgramData\Microsoft Help\'
         - 'C:\Windows\tasks\'
    condition: malware_path
```

〔그림 4〕 AD 환경을 위협한 공격그룹을 탐지하기 위한 Sigma 룰

4.2. Adversary Emulation 적용

최근 ATT&CK에서 정의하는 TTP를 에뮬레이션 하여 분석하는 Adversary Emulation이 활발히 연구되고 있다. ATT&CK 모델을 기반으로 공격자의 전략과 전술, 기법을 분석하여 규칙을 생성하고, 공격이 실제 발생하는 것처럼 시뮬레이션이 가능하다. 이러한 활동을 통해 방어자는 기업 환경에서 공격을 탐지·대응할 수 있는지 자가진단해볼 수 있다. Atomic Red Team [6], CALDERA [7] 등 새로운 솔루션이 등장하고 있으며, 사용하는 포맷 및 동작환경, 세부 기능에 차별성이 존재하나 에뮬레이션이라는 핵심 기능은 동일하다. 자가진단의 효과 외에도 시뮬레이션 결과를 통해 보안 제품이 효과적으로 공격에 대응할 수 있는지 평가하는 용도로 활용이 가능하여 향후 공격자 에뮬레이션 솔루션 시장의 성장이 예상된다.

방어자는 CALDERA는 세 가지 범주로 활용할 수 있다. 첫 번째는 위협을 정의하여 방어 환경에 영향을 미치는지 분석하는 공격 에뮬레이션이다. 이 활동을 통해 특정한 사이버 위협을 방어자가 대응할 수 있는지 자가 점검하고 기업 블루 팀을 훈련시킬 수 있는 효과를 얻을 수 있다. 두 번째는 자동화된 침해사고 대응이다. 호스트가 주어졌을 때 자동화된 위협을 식별하고 대응하는 활동을 경험할 수 있도록 지원한다. 마지막으로 레드 팀이 공격도구를 이용하여 수동으로 평가를 할 수 있도록 보조하는 기능이다. CALDERA의 다양한 활용방안에 따라 기업의 레드 팀과 블루 팀이 성장하고, 지능화되는 APT 공격에 자사 보안환경이 대응할 수 있는지 판단할 수 있다.

CALDERA에서는 공격자의 목표 달성하기 위한 전반적인 Procedure의 흐름을 사전조건(Pre-condition)과 사후조건(Post-condition)을 통해 제어하고 있으며, Technique을 실제로 동작할 수 있도록 동작 환경별로 정의하고 있다. 사용자는 기본적으로 제공하는 명령어를 수정하거나 함께 전송되는 페이로드를 추가함으로써 자사 환경에 최적화된 테스트 환경을 구축할 수 있다. 이러한 기능을 이용하여 기업은 침해사고 보고서의 내용을 이해하여 점검에 활용할 수 있다. 다음 그림 5는 AD 환경에서의 위협을 자사 환경에 맞추어 점검할 수 있도록 구성한 예시이다. 현재 지원하지 않은 명령어와 기법은 제외되어 있으나 공격도구를 추가, 페이로드 수정을 통해 공격을 명확하게 재현할 수 있다.

보고서를 기반으로 TTP를 재구성 하여 방어자는 자사 환경이 공격에 노출된 것처럼 실험할 수 있다. 그 결과는 그림 6과 같다. 순차적으로 TTP가 전개될 때, Technique 기반의 명령어가 성공했는지 여부를 확인하고, 어떤 단계에서 공격이 실패하였는지를 점검할 수 있다. 만약 Privilege Escalation 단계에서 공격이 실패

〔그림 5〕 AD 대상의 공격을 에뮬레이션하기 위한 규칙

하여 관리자 권한 확보가 누락된다면, 현재 구축된 환경에서는 해당 TTP를 이용한 대규모의 공격에 저항능력을 보유하고 있다고 평가할 수 있다.

Adversary Emulation 시장은 점차 성장할 것으로 기대되며, 추가적인 개념의 정립 및 상세한 동작 구성이 추가적으로 필요하다. 향후 공격그룹에 대한 프로파일링 결과를 에뮬레이션 할 수 있도록 규칙을 추가하여 각 기업에서 자가 진단할 수 있는 보고서가 공유될 것으로 예상된다.

V. 결 론

지금까지 AD 환경에서 사용된 공격기법을 TTP 형태로 정리하고 어떻게 기업에서 적용할 수 있는지에 대하여 알아보았다. 기존 침해지표 차단 수준의 대응전략이 효용성이 낮다는 문제가 예전부터 알려져 왔고, 이를 대응하기 위하여 TTP 공유의 형태로 변화하고 있다. 공격자의 전술·전략을 표현하는 프레임워크가 존재하지 않던 침해사고 보고서를 각 기업이 공격자의


```
"name": "AD_Threat_Operation_1",
"host_group": [
  {
    "available_contacts": [
      "http"
    ],
    "executors": [
      "psh"

    "origin_link_id": 0,
    "group": "red",
    "sleep_min": 30,
    "exe_name": "splunkd.exe",
    "username": "WIN-TD1L9SDINAM\\Administrator",
    "proxy_receivers": {},
    "location": "C:\\Users\\Public\\splunkd.exe",
    "platform": "windows",
    "privilege": "Elevated",
    "paw": "cxjmdz",
    "created": "2021-05-26 15:24:07",
    "last_seen": "2021-05-26 17:49:48",
    "contact": "http",
    "sleep_max": 60,
    "pid": 540,
    "host": "WIN-TD1L9SDINAM",
    "display_name": "WIN-TD1L9SDINAM$WIN-TD1L9SDINAM\\Administrator",
    "server": "http://10.10.2.40:8888",
    "ppid": 1072
        "uploads": [],
        "access": {},
        "platform": "windows",
        "code": null,
        "privilege": null,
        "repeatable": false,

    "steps": [
      {
        "ability_id": "1b47e726716362f535e47c9cd1051c6b",
        "command": "aWYgHC1ub3QoVGVzdC1QYXRoIEhLTE06U09GVFdBUkVcQ2xhc3NlcixFeGNlbCS8cHBsaWNhdGlvbikpezsgICByZXR1cmUgJ1Bs
        "delegated": "2021-05-26 17:43:28",
        "run": "2021-05-26 17:43:51",
        "status": 0,
        "platform": "windows",
        "executor": "psh",
        "pid": 1732,
        "description": "The macro-enabled Excel file contains VBScript which opens your default web browser and opens it
        "name": "Download Phishing Attachment - VBScript",
        "attack": {
          "tactic": "initial-access",
          "technique_name": "Phishing: Spearphishing Attachment",
          "technique_id": "T1566.001"
        }
      },
      {
        "ability_id": "523898649ff03b6f6051b5f92f24e9c9",
        "command": "IyBFbmNvZGVkIHBheWxvYWQgaWHgbmVidCBjb2ltYW5kIGlzIHRoZSBmb2xsb3dpbmcgIlNldC1Db250ZW50IC1wYXRoICIkZW52
        "delegated": "2021-05-26 17:43:53",
        "run": "2021-05-26 17:43:58",
        "status": 0,
        "platform": "windows",
        "executor": "psh",
        "pid": 2828,
        "description": "Execution of a PowerShell payload from the Windows Registry similar to that seen in fileless mal
        "name": "PowerShell Fileless Script Execution",
        "attack": {
          "tactic": "execution",
          "technique_name": "Command and Scripting Interpreter: PowerShell",
          "technique_id": "T1059.001"
        }
      },
    "group": "red",
    "sleep_min": 30,
    "exe_name": "splunkd.exe",
    "username": "WIN-TD1L9SDINAM\\Administrator",
    "proxy_receivers": {},
    "location": "C:\\Users\\Public\\splunkd.exe",
    "platform": "windows",
    "privilege": "Elevated",
    "paw": "cxjmdz",
    "created": "2021-05-26 15:24:07",
    "last_seen": "2021-05-26 17:49:48",
    "contact": "http",
    "sleep_max": 60,
    "pid": 540,
    "host": "WIN-TD1L9SDINAM",
    "display_name": "WIN-TD1L9SDINAM$WIN-TD1L9SDINAM\\Administrator",
    "server": "http://10.10.2.40:8888",
    "ppid": 1072
```


〔그림 6〕 Adversary Emulation 결과 보고서(중략)

기법을 분석하고, 다시 정책 및 보안장비 룰을 생성하는데 어려움이 많았다. 본고에서는 현장에서 직접적으로 어떻게 보안장비로 ATT&CK 프레임워크 기반의 보고서를 적용해야 하는지 제시하였다. 또한, 최근 주목받고 있는 Adversary Emulation을 이용하여 어떻게 자가 진단에 활용할 수 있는지 가능성을 제안하였다. 향후 한국인터넷진흥원은 지속적으로 침해사고에 대한 프로파일링을 통해 공격자의 전략과 전술, 기법 등을 상세히 분석하여 공유할 예정이다.

참 고 문 헌

[1] Active Directory, https://en.wikipedia.org/wiki/Active_Directory, Wikipedia

[2] Thomas Alsop , “Share of the global server market by operating system in 2018 and 2019”, Statista, May 2020.
[3] Microsoft, Active Directory Structure and Storage Technologies, https://docs.microsoft. com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759186(v=ws.10)
[4] David J Bianco, https://detect-respond. blogspot.com/2013/03/the-pyramid-of-pain.html, Jan 2014.
[5] Sigma, https://github.com/SigmaHQ/sigma
[6] Atomic Red Team, https://atomicred team.io, Red Canary
[7] CALDERA, https://caldera.mitre.org, MITRE

〈저 자 소 개〉

이 슬 기 (Seulgi Lee)
정회원
2013년 2월 : 충남대학교 컴퓨터 공학과 졸업
2019년~현재 : 고려대학교 빅데이터응용및보안학과 석사과정
2012년 10월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 위협 프로파일링, 악성코드, AI 보안, SW 보안

김 가 영 (Kayoung Kim)
정회원
2016년 2월 : 가톨릭대학교 컴퓨터정보공학과 졸업
2020년~현재 : 고려대학교 소프트웨어보안학과 석사과정
2016년 4월~현재 : 한국인터넷진흥원 주임연구원
<관심분야> 사이버 위협 프로파일링, 악성코드 분석, 디지털 포렌식, 침해사고 대응

김 동 욱 (Dongwook Kim)
2014년 2월 : 한양대학교 컴퓨터공학과 졸업
2013년 12월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 사이버 위협 프로파일링, 악성코드 분석, 디지털 포렌식, 침해사고 대응

이 태 우 (Taewoo Lee)
2015년 2월 : 호서대학교 정보보호학과 졸업
2014년 6월~2016년 5월 : 하우리 침해대응센터 연구원
2016년 6월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 사이버 위협 프로파일링, 악성코드 분석, 침해사고 대응

이 재 광 (JaeKwang Lee)
2007년 2월 : 서울대학교 수학과 석사 졸업
2010년 2월~현재 : 한국인터넷진흥원 인터넷침해대응센터 근무(현 종합분석팀장)
<관심분야> 포렌식, 침해사고 조사 기법, 데이터 프로파일링