최신 보안 트랜드 분석 및 취약점 분석 서비스 제공

배재석* 김가을* 김찬규* 김희연* 이시현* 김도훈**

Provide latest security trend analysis and vulnerability analysis service

Bae JaeSeok* Kim Gaeul* Kim Changyu* Kim HeeYeon* Lee sihyeon and Kim DoHoon**

WebSE

요약

해마다 증가하는 사이버 공격은 가상화폐의 출현으로 다양한 랜섬웨어 공격으로 이어지고 있다. 대기업이나 관공서는 KISA(한국인터넷진흥원)에서 제공하는 가이드에 맞추어 서비스를 운영하고 보안시스템을 유지하여 사이버 공격을 예방하지만, 중소기업이나 스타트업은 이러한 보안으로부터 취약한 상태이다. 본 연구에서는 이러한 사이버 공격에 취약한 기업들을 대상으로 취약점을 분석해주고 이를 통해 발생할 수 있는 여러 공격 시나리오를 제시해준다. 공격 시나리오는 사이버 킬체인을 기반으로 이루어지고 MITRE ATT&CK Framework를 사용하여 각 단계별에서 발생할 수 있는 공격들을 소개한다. 이러한 명시된 공격들을 통해 기존의 공격 시나리오와 다른 공격 시나리오를 발견하고 이에 대한 대응책을 제공함으로써 추가적인 피해를 막을 수 있다.

Abstract

Cyber attacks that increase every year are leading to various ransomware attacks with the emergence of virtual currency. Large companies and government offices operate services and maintain security systems in accordance with the guides provided by the Korea Internet & Security Agency (KISA) to prevent cyber attacks, but small and medium-sized companies and startups are vulnerable to such security. In this study, vulnerabilities are analyzed for companies vulnerable to these cyber attacks and various attack scenarios that can occur through them are presented. The attack scenario is based on the cyber kill chain and uses the MITRE ATT&CK Framework to introduce possible attacks at each stage. These stated attacks can prevent further damage by discovering attack scenarios that differ from existing attack scenarios and providing countermeasures.

Key words
ransomware, MITRE ATT&CK, cyber killchain, web hacking

---

*소속, Email, **소속, Email(,교신저자표시), ...

※ 감사의 글
본 연구는 과학기술정보통신부 및 정보통신기획 평가원의 SW중심대학지원사업의 연구결과로 수행되었음 (2021-0-01393)

정찰(reconnaissance)	정보 수집 및 공격대상 조사/식별
무기화 및 전달(Weaponization and Delivery)	공격할 요소를 찾고 권한을 획득
익스플로잇 및 설치(Exploitation and Installation)	공격 대상에 악성코드 설치
명령 및 제어(Command and Control)	원격으로 명령을 실행
목적 수행(Action on Objectives)	시스템 파괴 등 공격 수행

[표 1] 사이버 킬체인의 각 단계

Ⅰ. 서 론

국내 랜섬웨어 피해는 매년 급증하고 있다. 21년 기준 피해액은 약 2조 5천억에 이를거라는 조사가 그 결과이다. 한국 랜섬웨어침해 대응센터의 조사에 따르면 2015년부터 7년간 피해액을 모두 합치면 6억 8천 6백억에 달할 것으로 조사되었다. 랜섬웨어 피해를 당한곳은 중소기업이 (43%), 소상공인(25%), 개인 (22%)이 대부분을 차지했다. 반면 공공기관(2%)와 대기업(1%)은 상대적으로 피해를 적게 입은것으로 파악되었다. [1]

위의 통계와 같이 랜섬웨어 피해는 매년 늘고 있지만 소상공인과 중소기업은 이러한 공격에 쉽게 노출되어 있다. 중소기업은 대기업에 비해서 정보기술에 대한 의존도가 높지만, 재정적인 어려움과 한정된 자원 및 노하우의 부족 등의 이유로 인해서 정보보안에 투자하지 않기 때문이다. [2]

본 연구에서 진행하는 서비스는 랜섬웨어 공격에 쉽게 노출되는 중소기업 및 소상공인을 대상으로 이루어진다. 취약점 분석 서비스는 웹에서 랜섬웨어가 감염될 수 있는 경로를 탐색하고 탐색한 경로를 바탕으로 시나리오를 구성한다. 기존의 OWASP와 같은 취약점 공격 가능성을 보여주는 비영리 단체는 존재하지만, 정보가 산재해 있어 기업에 맞는 정보를 찾기에는 어려움이 존재한다. 이에 반해 해당 서비스는 보고서에 공격 시나리오를 작성하고 이를 요약하여 시각적으로 쉽게 보여줌으로써 중소기업만 아니라 개인까지도 해당 서비스를 이용할 수 있다. 이를 통해 사용자들은 자신들의 시스템이나 웹사이트에서 랜섬웨어 공격에 취약한 부분을 파악하고 이를 보완함으로써 공격으로부터 안전하게 보호될 수 있다.

Ⅱ. 공격 시나리오 사이버 킬체인 적용

본 연구에서 제작하는 보고서는 랜섬웨어를 감염되는 전반적인 과정을 공격 시나리오로 만든다. 이러한 공격 시나리오는 공격자가 공격 대상을 탐색하는 초반 단계부터 침투하여 공격 목표의 가용성과 무결성을 손상시키는 최종단계까지 이루어진다.

사이버 킬체인(Cyber Kill Chain)이란 사이버 공격이 계획된 하나의 절차에 따라 시행된다는 점을 인지하고 공격의 시작부터 종단까지의 프로세스를 보여주는 모델이다. 일반적으로 사이버 킬체인은 정찰(Reconnaissance), 무기화 및 전달(Weaponization and Delivery), 익스플로잇 및 설치(Exploitation and Installation), 명령 및 제어(Command and Control), 목적 수행(Action on Objectives) 단계로 구성된다. [3]

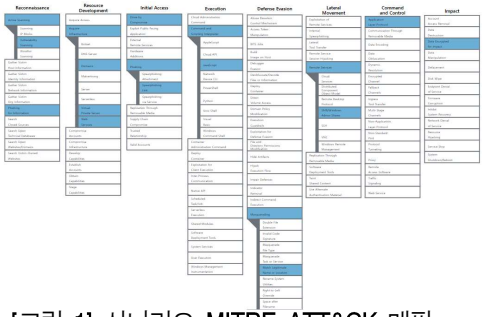
본 연구에서는 공격과정을 사이버 킬체인을 통해 공격자 관점에서 공격의 절차를 파악 및 분석하여 위협 요소를 단계별로 제거해나가 피해를 최소화할 수 있다. 또한 각 단계에서 시행가능한 공격기법을 분석한다면, 다양한 웹 기반 공격 시나리오를 찾아내고 대응책을 제시할 수 있다.

Ⅲ. MITRE ATT&CK Framework 기반 공격기법 매핑 및 도식화

기존의 취약점 보고서는 산재하여있는 정보를 모아 기존 서비스에 공격 가능한 취약점을 소개하고 이에 대한 대응책을 소개한다. 이러한 정보는 고객의 시각에서 해당 취약점의 위험성과 실현 가능성을 체감하기 힘들다는 한계가 존재한다.

본 연구에서는 이러한 문제를 방지하고자 사이버 킬체인으로 단계별 구성된 공격 시나리오를 MITRE ATT&CK Framework를 사용하여 각 단계에서 발생할 수 있는 공격을 매핑한다. 이는 공격과정을 시각적으로 보여주어 해당 취약점이 어느 단계에서 발생하는지 알 수 있다. 이를 통해 고객은 해당 공

격의 위험성을 인지하는데 도움이 된다.



[그림 1] 사나리오 MITRE ATT&CK 매핑

정찰(Reconnaissance)에서는 active scanning이 가능하다. active scanning 과정에서 스캐닝 도구를 활용하여 공격대상의 취약점을 찾아낼 수 있다.

무기화 및 전달(Weaponization and Delivery)에서는 Malvertising(악의적인 광고)를 통해 피해자를 유인하고 이후 Drive-by download 공격으로 이어진다. 다른 공격 방법으로는 Drvie-by target을 통해 공격대상을 확정하고 공격대상이 자주 이용하는 웹페이지에 Watering hole 공격을 시도하여 악성코드를 설치하는 시나리오이다.

익스플로잇 및 설치(Exploitation and Installation)에서는 Drive-by Compromise를 통해 사람들이 자주 이용하는 웹페이지에 Watering hole 공격을 시도한다.

명령 및 제어(Command and Control)에서는 SMB protocol을 통해 랜섬웨어 내부 전파를 시도한다.

마지막으로 목적 수행(Action on Objectives)에선 Data Encryotion(데이터 암호화)를 통해 파일 암호화 후 금전적인 요구를 수행한다.

MITRE ATT&CK을 통해 위의 시나리오를 각 단계에 맞게 구성하고 이에 해당하는 공격기법을 매핑할 수 있다.

또한 매핑과정에서 산출된 공격들을 통해 새로운 공격 시나리오를 구상하고 기존에는 발견하지 못한 새로운 취약점을 찾아낼 수 있다. 우리는 이를 분석하여 추가적인 서비스로 제공한다.

IV. 결론

본 연구에서는 웹기반 랜섬웨어 감염과정을 시나리오를 통해 취약점을 분석하는 서비스를 제공한다. 기존의 취약점 보고서와 달리 공격 시나리오를 사이버 킬체인에 기반하여 작성하고 이를 MITRE ATT&CK에 매핑함으로써 해당 취약점 공격이 어떠한 측면에서 필요한지 근거를 제공한다. 이를 통해 기존 보안시스템이 미흡한 중소기업 및 소상공인에게 자주 발생하는 랜섬웨어 감염을 사전에 방지한다. 이는 국내 중소기업의 성장을 촉진할 수 있다.

참고문헌

[1] 한국랜섬웨어침해대응센터 (2018.11.13) 2018년 랜섬웨어 침해분석 및 2019년 공격전망 https://rancert.com/bbs/bbs.php?bbs_id=news&mode=view&id=539

[2] Sangsoo Yeo, Suchul Hwang, “A Safe Operating Strategy for Information System of small and Medium Enterprises”, 2009.07, p.2~3

[3] Youngin Yoon, Jongwha Kim, Jaeyeon Lee, Sukdea Yu, Sangjin Lee, “A research on cyber kill chain and TTP by APT attack case study”, 2020.10, p2

한글제목	휴먼명조, 17, 장평:90, 자간: -7
저자명	돋움, 11, 장평:90, 자간: 5
영문제목	견명조, 15, 장평:90, 자간: -7
영문저자명	휴먼명조, 10, 장평:90, 자간: -5
본문	중고딕, 10, 장평:90, 자간: -6
참고문헌	영문:Times New Roman, 10, 장평:90, 자간:-6
요약본문	휴먼명조, 9, 장평:90, 자간: -5
영문요약문	중고딕, 10, 장평:90, 자간: -6
소제목	중고딕, 11, 장평:90, 자간: -6