Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 6 pp. 267-273, 2023

https://doi.org/10.5762/KAIS.2023.24.6.267
ISSN 1975-4701 / eISSN 2288-4688

중국 해킹그룹 샤오치잉 사이버 무기체계 대응방안 연구: SQL Injection 및 OSINT기반 Known Vulnerability 공격

유도진
극동대학교 해킹보안학과 교수

Research on Countermeasures Against the Cyber Weapon System of the Chinese Hacking Group Xiao Qi-ying: SQL Injection and OSINT-Based Known Vulnerability Attacks

Do-Jin Yoo
Assist. Professor, Department of Hacking & Security, Far East University

요 약 러시아-우크라이나 전쟁 이후의 국제 정세 변화의 영향으로 사이버 무기체계의 확산이 국가 안보와 국제 사이버 안전에 점점 더 중요한 요소가 되고 있다. 중국은 사이버 강대국으로 분류되며, 중국의 지원을 받는 것으로 의심되는 해킹그룹 샤오치잉(晓骑营)의 사이버 공격은 전 세계적인 도전으로 대두되고 있다. 본 연구에서는 2023년 1월 21일 샤오치잉의 공격개시 선포 이후 약 2달간 전개된 샤오치잉의 사이버 공격을 분석하여, 공격 양상과 대응 방안을 살펴보고 시사점을 제시한다. 샤오치잉은 주로 SQL Injection과 공개정보(Open Source Intelligence, 이하 OSINT)를 활용한 알려진 취약점 공격(이하, Known Vulnerability)을 공격기법으로 활용하였으며, 이를 고려한 종합적인 대응 방안과 사이버 보안 강화를 제안하고, 이를 통해 기업과 국가 차원에서 사이버 위협에 효과적으로 대응할 수 있는 전략 도출에 기여하고자 한다.

Abstract The spread of cyber weapons systems is becoming an increasingly important factor in national security and international cyber safety because of the changes in the international political climate following the Russia-Ukraine war. China is classified as a cyber superpower, and the cyber-attacks of the hacking group "Xiao Qi-ying" (晓骑营), suspected of receiving support from China, poses a global challenge. This study analyzed the cyber-attacks conducted by Xiao Qi-ying for approximately two months after its declared attack commencement on January 21, 2023, to examine the patterns of attacks and response measures and to present implications. Xiao Qi-ying primarily utilized techniques, such as SQL Injection and Known Vulnerability attacks utilizing Open Source Intelligence (OSINT). This paper proposes a comprehensive response plan considering these, enhancing cyber security, and contributing to the derivation of effective strategies to counter cyber threats at the corporate and national levels.

Keywords : Xiao Qi-ying, Cyber weapons, SQL Injection, OSINT, Known Vulnerability

*Corresponding Author : Do-Jin Yoo(Far East Univ.)
email: dhy8906@naver.com
Received May 2, 2023 Revised May 19, 2023
Accepted June 2, 2023 Published June 30, 2023

1. 서론

러시아-우크라이나 전쟁으로 인해 사이버 무기체계의 확산은 국가 안보 및 국제적 사이버 안전에 큰 영향을 미치고 있다는 것이 표면적으로 드러나고 있다. 특히 사이버 강대국으로 분류되는 중국의 경우, 2021년 1월부터 마이크로소프트社의 E-mail 서버 Zero-Day 취약점을 이용하여 침입 후 백도어를 심어 공격하여 미국 각급 정부부처와 기업 등 30,000곳 이상 피해를 입히는 등 위력을 과시한 바 있다. 또한 이러한 중국의 지원을 받는 해킹그룹이 다수 존재하는 것으로 의심되며[1, 2], 중국의 사이버 무기체계 확산은 국가안보에 있어 전 세계적인 도전으로 대두되고 있다. 특히, 23년 1월 21일 중국 해킹그룹중 하나인 샤오치잉이 국내 다양한 기관의 약 2천여개 웹사이트를 대상으로 사이버 공격을 예고하고 개인정보 유출 및 공격 등을 감행한 뒤 이러한 내용을 해킹포럼 등을 통해 공개한 바 있다. 이들의 공격예고와 실행에서 특징 및 동기를 유추해보면 주로 소규모의 기관 및 기업, 학회 등을 표적으로 선택하였는데, 이러한 표적 선정의 주된 이유는 중소기업 등 소규모 조직의 경우 보안에 대한 투자와 인식이 상대적으로 부족하여 공격에 성공할 확률이 높기 때문이었던 것으로 판단된다. 또한 샤오치잉은 공격에 성공한 후 획득한 관련 정보를 공개하였는데, 이는 피해 기관 및 기업에 추가적 부담을 주고, 자신들의 사회적 영향력을 확장하고자 하려는 목적이 있었던 것으로 보인다. 즉, 이러한 사이버 공격을 통해 주로 경제적 이익과 더불어 정치적 목적의 달성, 영향력 과시를 꾀한 것으로 분석할 수 있다. 한편 샤오치잉은 23년 2월 18일 마지막으로 식별된 공격 이후 우리나라에 대한 사이버 공격 중지를 발표했으나, 2023년 4월 24일 텔레그램 통해 국내 IT인프라 구축 관련 기업을 표적으로 개인정보 탈취 및 홈페이지 변조 공격을 감행한 사실을 공개하였다[3]. 이처럼 샤오치잉을 비롯하여 중국의 국가지원 해킹그룹으로 의심되는 국제적 사이버 공격 조직의 위협은 지속될 것으로 보이므로, 본 연구는 이와 같은 중국 해킹그룹 사이버 무기체계의 공격양상과 대응 전략을 살펴보고, 이에 대한 시사점을 도출하여 우리나라의 사이버 안보에 기여하고자 하며, 본 연구는 다음과 같은 구성으로 진행하였다. 2장에서는 사이버 무기체계의 개념과 함께 샤오치잉이 선택한 표적의 특성 및 이유를 파악하고자 하였다. 3장은 샤오치잉이 샤오치잉이 주로 활용한 공격기법에 대해 분석하였으며, 이들의 공격 방식을 이해하고 그들이 선택한 취약점을 파악하는 것은 효과적인 대응 전략 수립에 요구된다. 4장에서는 샤오치잉의 공격 방식을 바탕으로 대응방안을 논의하였다. 각 공격별 대응 방안은 공격 방식에 따라 맞춤화되어야 하며, 이를 통해 새로운 대응방안을 논의하였다. 마지막으로 5장 결론에서는 본 연구의 요약과 함께 시사점 및 한계점을 제시하고, 이를 바탕으로 향후 연구방향에 대해 제언하였다.

2. 사이버 무기체계

2.1 사이버 무기체계의 개념

사이버 무기체계는 사이버 공간에서 다양한 목표를 달성하기 위한 사이버 공격 및 방어 기술들을 통합한 체계이며, 소프트웨어 및 하드웨어 무기체계로 구분할 수 있다[4]. 소프트웨어 무기체계와 사이버 공격 기법은 서로 연관되어 있지만, 두 개념에는 차이점이 존재한다. 사이버 공격 기법은 사이버 공간에서 시스템, 네트워크, 데이터에 대한 공격이나 침투를 실행하는 데 사용되는 특정한 방법이나 기술로서, WannaCry, NotPetya, Bad Rabbit 등의 랜섬웨어, SQL Injection, Zero-day, APT, DDoS 등이 여기에 해당한다. 이러한 기법들은 사이버 공격을 수행하는 동안 취약점을 이용하거나 시스템 조작에 사용된다[5]. 반면 소프트웨어 무기체계는 공격기법을 포함하고 있는 더 큰 시스템이자 프레임워크로, 공격자들이 목표를 달성하기 위해 계획, 조직, 실행, 유지보수를 수행하는데 필요한 다양한 요소를 포함한다. 또한 소프트웨어 무기체계는 다양한 사이버 공격 기법 뿐 아니라 공격자의 전략, 인프라, 자원, 지식 등의 개념이 포함된다. 즉, 사이버 공격 기법은 소프트웨어 무기체계 내에서 사용되는 도구 또는 기술로, 이러한 기법을 효과적으로 전개하기 위한 전체적 구조와 전략을 의미한다. 한편 하드웨어 무기체계는 표적이 하드웨어 기반이 되며, 전력 인프라 공격을 위한 전자파(Electromagnetic Pulse, EMP) 무기, 드론을 이용한 무선 네트워크 공격이 포함된다. 이러한 공격은 특정 인프라, 통신 등을 무력화시키는데 사용되지만, 징후 및 식별이 비교적 뚜렷하고 일반적으로 국가간 적대적 상황이 조성되어야 발발하는 특징이 있다. 반면 소프트웨어 무기체계는 오늘날 국제적 해킹그룹의 주요 공격수단으로 사용되고 있며, 샤오치잉의 공격도 여기에 기반하였다.

2.2 사이버 무기체계의 표적

표적은 공격의 목표가 되는 자산 및 인프라로, 다양한 형태가 존재하며, 국가 차원에서는 중요 IT인프라, 정부 및 국방 시스템, 통신 및 에너지 시설 등 핵심 및 고가치 자산이 해당되며, 민간은 영업기밀 등의 지식 재산, 고객 정보, 중요 데이터 등이 표적이 될 수 있다. 한국인터넷진흥원(이하 KISA)의 관련 보고서에 따르면 '23년 1월부터 전개된 샤오치잉의 주요 표적은 대부분 소규모 기관 및 기업, 학회 등으로 분석된다[6]. 이러한 조직의 특성은 보안에 대한 적극적 투자가 제한되어, 규모가 큰 조직에 비해 보안전문가의 채용이 어렵고 이로 인해 보안인식 및 교육이 부족하여 임직원이 관련 위협에 대해 충분히 인지하지 못하거나 적절한 대응이 어려울 가능성이 높다. 이러한 주요 표적의 특성을 정리하면 아래 Table 1과 같다.

Table 1. Theorem of the properties of the main targets

Class	Features
Scale	Many affected organizations are small, leading to insufficient security budgets.
Business type	Industries like finance, healthcare, and manufacturing contain crucial information.
Security awareness	Low security awareness can leave employees unprepared for threats.
Security personnel	Small organizations struggle to hire security personnel and implement measures.

3. 공격기법

KISA에 따르면 올해 1월부터 약 2달간 전개된 샤오치잉의 사이버 공격을 분석하면 이들은 주로 SQL Injection과 Known Vulnerability 기법을 사용하였다[4]. 이를 통해 조직의 고가치 정보를 유출하고 웹페이지의 변조 및 DB 삭제 등을 감행하였다. 이에 표적에 대한 공격기법 및 각 전개양상을 분석한다.

3.1 SQL Injection

SQL Injection은 데이터베이스(Data Base, 이하 DB) 관련 애플리케이션에서 발생하며, 공격자가 악의적 SQL 구문을 주입하여 DB에 직접 접근하거나 조작한다. 이를 통해 공격자는 표적이 가진 중요 정보를 무단으로 조회하거나 삭제, 수정한다[7]. 샤오치잉이 SQL Injection을 활용한 공격 수행 절차를 정리해보면, 우선 표적 선정 및 취약점 스캔을 논의해야 한다. 보안 인프라가 취약한 조직을 표적으로 선정한 뒤 기본적인 정보수집과 희생자의 취약한 SQL 쿼리를 찾기 위해 Sqlmap 등 관련 Tool을 활용한 것으로 보인다. 이 때 사용자 입력값을 처리하는 코드에 SQL 쿼리가 안전하게 필터링되지 않은 경우 표적으로 적절하다. 샤오치잉이 국내 기업에 대해 감행한 취약점 스캔의 일부를 살펴보면 아래의 Fig. 1과 같으며, 이는 KISA 보고서의 그림 일부를 재구성하였다[6].

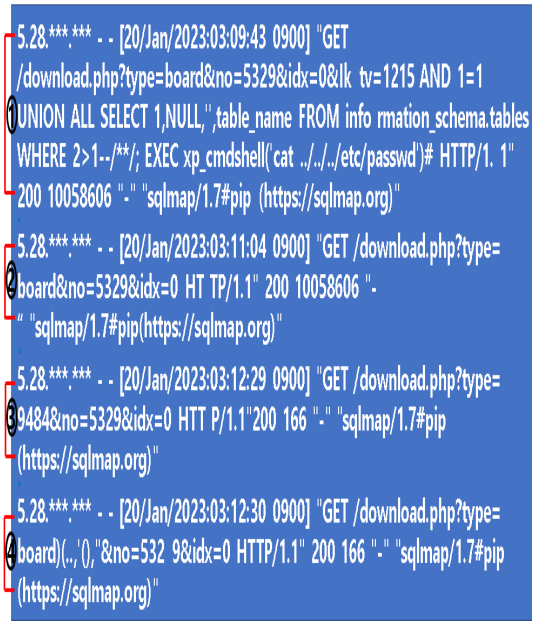

Fig. 1. Scan for vulnerabilities using Sqlmap

위 Fig. 1에서 ①번 항목을 보면 request에서 공격자는 UNION ALL SELECT 문을 사용하여 정보 추출을 시도하였으며, EXEC xp_cmdshell을 통해 원격 명령을 시도하였다. 또한, 요청에서 사용된 User-Agent을 통해 Sqlmap을 사용했음을 유추할 수 있다. ②번의 경우 request는 정상적으로 보이나 User-Agent에 여전히 Sqlmap이 사용되었다. 이전 공격 시도 이후 정상 request를 보내는 것처럼 가장하려는 시도이다. ③번 항목에서는 다른 type 값이 사용되었지만, 여전히 Sqlmap을 사용한 것으로 보이며, ④번 항목에서는 인코딩된 문자를 사용하여 SQL Injection을 시도한 것을 알 수 있다. 여기서도 User-Agent는 Sqlmap을 사용하였다. 다음으로 SQL Injection(악성구문 주입)이다. 예를 들어,

로그인 폼에서 입력받은 사용자 이름과 비밀번호를 이용하는 SQL 쿼리가 있을 때, 공격자는 사용자 이름 또는 비밀번호 입력란에 악성 SQL 구문을 입력하여 원래의 쿼리를 변경하는 방식을 사용할 수 있다. 샤오치잉도 동일한 기법을 활용하였는데, KISA에서 제공한 샤오치잉의 SQL Injection을 살펴보면 아래 Fig. 2와 같다[6].

No	Xiao Qi-Ying's SQL Injection statement used (Source: Web Log)
①	AND ORD(MID((SELECT IFNULL(CAST(table_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.TABLES WHERE table_schema=**** LIMIT 0,1),1,1))>64&idx=0
②	AND ORD(MID((SELECT IFNULL(CAST(COUNT(column_name) AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name=admin AND able_schema=****),1,1))>48&idx=0
③	AND ORD(MID((SELECT IFNULL(CAST(admin_id AS NCHAR),0x20) FROM ****.admin ORDER BY admin_id LIMIT 0,1),1,1))>64&idx=0
④	AND ORD(MID((SELECT IFNULL(CAST(admin_pwd AS NCHAR),0x20) FROM ****.admin ORDER BY admin_id LIMIT 0,1),1,1))>64&idx=0

Fig. 2. SQL Injection using by Xiao Qi-Ying

위 Fig. 2의 ①번 항목의 내용에서 분석해보면 “INFORMATION_SCHEMA Table”에서 Table 이름을 찾아 1글자씩 추출하여 공격 대상이 되는 Table을 확인하였음을 알 수 있다. ②번 항목의 구문은 해당 Table에 속한 Column(열)의 개수 확인이다. 이를 통해 추출하려는 데이터를 포함하는 열을 찾을 수 있다. ③번 항목의 구문은 admin Table에서 admin_id 컬럼의 값을 1글자씩 추출이다. 이를 통해 관리자 테이블에서 관리자 ID를 획득할 수 있으며, ④번 항목의 구문은 admin Table에서 admin_pwd 컬럼의 값을 1글자씩 추출이다. 이를 통해 시스템 관리자의 비밀번호를 획득할 수 있다. 주입 이후에는 DB조작 및 정보 유출로 이어지는데, 이는 SQL Injection 성공으로 시스템 조작 및 정보의 위변조가 가능해져 이를 통해 핵심정보를 획득하였다. 예로, 공격자가 관리자 권한을 부여받아 고객의 개인정보 등을 획득하였으며, 이렇게 획득한 정보는 유출, 위변조 등에 악용될 수 있다. 또한 추가 공격 수행의 빌미도 제공하게 되는데, 공격중 획득한 정보로 조직의 네트워크에 침투하거나 타 조직에 대한 공격을 계획할 수 있다. 상기 4가지 과정을 요약해서 정리하면 아래 Table 2와 같다.

Table 2. Summary of SQL Injection Attacks

Procedure	Content
Scanning	Select vulnerable organizations in the security infrastructure, gather information, and use related tools to scan for vulnerable SQL queries in the victim's system.
SQL Injection	A input malicious SQL statements into the username or password fields to alter the original query.
Leakage	Once the system can be manipulated and information tampered with, attackers can acquire critical data.
Additional attacks	Use the obtained information to infiltrate the organization's network or plan attacks on other organizations.

3.2 Known Vulnerability

Known Vulnerability 공격은 잘 알려진 보안 취약점을 이용하여 시스템에 침입하거나 정보를 탈취하는 것을 의미한다. 공격자는 OSINT를 활용하여 취약점 정보를 찾아낸 뒤 이를 공격 기회로 활용한다[8]. 여기에는 SNS, 공개된 소프트웨어 버전 정보를 포함해서 인터넷상의 모든 정보가 포함될 수 있다. KISA보고서에 따르면 샤오치잉이 Known Vulnerability 공격을 활용한 이유는 소규모 조직의 경우 보안 패치를 적용하지 않거나, 업데이트를 미루는 경우가 많기 때문으로 판단된다. 이를 통해 공격자는 시스템 접근 기회를 확보한다. Known Vulnerability 공격 절차를 정리해보면 다음과 같다. 첫째, 공개된 취약점 정보를 수집하는데, 이 정보는 과거에 발견되었지만 아직도 많은 시스템에서 사용되고 있는 취약점인 경우가 많다. 또한 보안 취약점 코드(Common Vulnerabilities and Exposures, 이하 CVE) DB와 같은 오픈소스를 통해 정보를 수집할 수 있다. 이후 스캐닝 도구를 사용하여 대상 네트워크를 분석한다. 활용되는 Tool로 잘 알려진 Snort, Nmap, Wireshark, Metasploit, Nikto, Nessus 등이 있다[9]. 둘째, 취약점 검증을 위한 테스트 수행이다. 이 과정에서 시스템이 예상되는 취약점을 가지고 있음을 확인할 수 있다. 셋째, 계획 수립이다. 공격자는 시스템에 액세스하고, 데이터를 조작하거나, 추가적인 악성 코드를 실행하는 방법을 결정한다. 넷째는 실제 공격으로, 시스템의 정보를 획득하거나 위변조하여, 다른 시스템을 공격할 수 있는 통로로 활용한다. 이후 로그 파일을 삭제하거나 수정하여 공격 흔적을 은폐한다. 구체적인 예로 23년 2월 샤오치잉에게 공격받은 모 기업은 웹 서버에 개발 환경과 동기화

를 위한 SFTP 계정 설정 파일인 sftp.json 파일이 외부에 노출되도록 업로드하였다[6]. 이에 샤오치잉은 웹 로그를 확인하여 아래 Fig. 3과 같이 접근하였다.

```
[{
    "name": "***",
    "host": "222.2**.***.***",
    "protocol": "sftp",
    "port": ****,
    "username": "***",
    "password": "***",
    "remotePath": "/home/***",
    "uploadOnSave": true
}]
```

Fig. 3. Sftp.json file accessed by Xiao Qi-Ying

샤오치잉은 이 파일을 통해 획득한 계정정보를 악용하여 아래 Fig. 4와 같이 SSH 접속을 시도하였으며, Fig. 5와 같이 Secure Log에서 확인된 것처럼 접속에 성공하였다.

```
8.213.***.*** - - [20/Jan/2023:21:08:53 +0900] "GET /.config/sftp.json HTTP/1.1" 404 215
8.213.***.*** - - [20/Jan/2023:21:08:53 +0900] "GET /.vscode/sftp.json HTTP/1.1" 200 352
...(중략)...
8.213.***.*** - - [20/Jan/2023:21:08:53 +0900] "GET /.vscode/sftp.json HTTP/1.1" 200 352
5.28.***.*** - - [20/Jan/2023:23:02:35 +0900] "GET /.vscode/sftp.json HTTP/1.1" 200 3 52
```

Fig. 4. Access History by Xiao Qi-Ying

```
Jan 20 23:03:13 n***n sshd[39407]: Accepted password for %username% from 5.28.***.*** port 61924 ssh2
Jan 20 23:03:13 n***n sshd[39407]: pam_unix(sshd:session): session opened for user %u sername% by (uid=0)
Jan 20 23:09:30 n***n sshd[39407]: pam_unix(sshd:session): session closed for user %u sername%
```

Fig. 5. SSH Access Successful Logs by Xiao Qi-Ying

샤오치잉은 이렇게 노출 계정정보를 악용하여 시스템에 침입, 정보를 획득 및 변조하였다. 이 외에 샤오치잉은 오래된 버전의 WebLogic 취약점도 악용하였으며, 이 취약점을 악용해 해당 조직의 웹페이지를 변조하고 시스템에 남아있는 로그 파일을 삭제 및 수정하여 공격 흔적의 은폐를 시도하였다. 이 사례를 통해 볼 수 있듯이, 민감정보가 노출되거나, 시스템에 알려진 취약점이 존재할 경우 공격자에게 시스템 침입의 기회를 제공하게 된다. 따라서, 조직은 보안 정책을 철저히 관리하고, 시스템의 취약점을 지속적으로 점검하며, 적절한 패치 및 업데이트를 실시하여 공격자로부터 시스템을 보호할 수 있도록 노력이 요구된다. 상기 Known Vulnerability 공격 순서를 정리해보면 아래 Table 3과 같다.

Table 3. Summary of Known Vulnerability Attacks

Procedure	Content
Gathering information	Utilize public sources or scanning tools to gather target system information.
Exploring	Identify vulnerabilities using gathered information, databases, or scanning tools.
Prepare	Choose an attack technique based on attack objectives.
Attack	Execute the attack using necessary tools or code.
Concealment of traces	Evaluate attack results and take additional actions, or retry with alternate methods.

4. 대응방안

사이버 무기체계에 대응하기 위한 기존의 대응 방안들이 있지만, 이러한 방안들에는 일부 한계가 있다. 이는 대부분 웹 서버 보안 강화와 관련된 것으로, 공격이 발생한 후의 피해 복구와 향후 공격 대비를 위한 철저한 보안 대책이 부족하며, 다음과 같은 한계점을 가지고 있다. 소규모 조직은 예산의 제약이나 인력 부족으로 인해 전문적인 보안 인력을 고용하거나 교육하기 어려운 상황이다. 이러한 이유로 상기 논의한 것과 같이 웹 서버에 계정정보를 노출하는 등 낮은 보안인식이 취약할 가능성이 높아진다. 또한 상대적으로 보안교육 빈도가 낮은 기관 및 기업의 보안 정책 실패로 내부자 위협 등이 존재한다거나, 혹은 적절한 PMS(Patch Management System, 이하 PMS)이 적용되지 않아 취약할 수 있다. 이로 인해 기회를 노리는 공격자들의 표적이 될 가능성이 존재한다. 또한 사전 대응 부족도 초래한다. 이러한 대응방안은 공격이 발생한 후에 대응하는 교정통제에 초점을 맞추고 있어, 사전에 공격을 예방하거나 조기에 탐지하는데 한계가 있다. 이로 인해 공격자들이 시스템에 침투하고 피

해를 입히는 데 충분한 시간을 확보할 수 있다. 이에 샤오치잉이 공격개시를 선포한 23년 1월 21일부터 2월 18일까지 이뤄진 공격을 토대로 새로운 대응방안에 대해 논의한다.

4.1 SQL Injection 대응

웹 서버 시큐어 코딩과 웹 방화벽 설치와 더불어 런타임 어플리케이션 셀프 보호(Runtime Application Self Protection, 이하 RASP)를 도입하면 입력값 검증의 정확성과 효율성을 높일 수 있으며, 개발자 교육 및 코드 리뷰를 강화하여 Prepared Statement 사용의 정확성과 일관성을 향상시킬 수 있다. 또한 시대적 요구에 따라 인공지능 기반 보안솔루션 도입을 고려해야 한다[9]. 이는 사이버 무기체계와 공격기법이 지속적으로 발전하기 때문에, 실시간 공격을 감지하고 대응을 위해 필요하다. 이러한 솔루션은 이상 탐지(Anomaly Detection) 기능을 사용하여 웹 애플리케이션의 정상적인 트래픽 패턴과 다른 요청을 식별하고 이를 통해 SQL Injection 공격과 관련된 요청을 차단할 수 있으며, 자연어 처리(Natural Language Processing) 기능을 활용하여 사용자 입력값을 분석하고, SQL Injection을 시도하는 입력값을 식별할 수 있다. 이를 통해 악성 구문 주입 차단 및 예방·탐지가 가능하다. 또한 머신러닝(Machine Learning)을 통해 과거 SQL Injection 사례를 학습하고, 이와 관련된 Zero-Day 등 새로운 공격 기법을 더 빠르게 탐지할 수 있으며, 공격자가 필터링을 우회하는 기법을 사용하더라도 시스템이 적응할 수 있다. 이 외에도 연속적 모니터링을 통해 발생하는 이벤트를 실시간으로 분석하여 공격에 대한 대응이 가능하고 보안 정책의 자동 최적화로 새로운 공격 기법에 대한 대응 전략을 제안할 수 있다. 이를 통해 기관 및 기업들은 더 효과적으로 SQL Injection 대응 전략을 구축할 수 있다.

4.2 Known Vulnerability 대응

계정정보 관련 서버 내 계정정보 업로드 여부 점검 외의 새로운 대응 방안으로 다중 인증(Multi Factor Authentication, MFA)을 도입하는 방법을 고려할 수 있다. 이를 활용하면 계정정보 보안을 강화할 수 있다. 또한 사용자들에게 비밀번호 관리 도구를 사용할 것을 권고함으로써, 비밀번호 사용의 안전성을 높일 수 있다. 운영체제 및 소프트웨어 버전 업그레이드와 관련해서는 최신 보안 업데이트를 받을 수 있는 패치관리시스템 점검이 중요하다. 새로운 대응 방안으로는 자동화된 업데이트 및 패치 관리 도구를 도입하면 업데이트와 패치의 적용 시간을 단축하고, 호환성 문제를 최소화할 수 있다. 또한 가상 패치(Virtual Patching) 기술을 활용하여 취약점이 발견된 시스템을 신속하게 보호할 수 있으며, 중요한 자료를 오프라인으로 별도 백업해야 하는 것도 중요하다[10]. 그러나 새로운 대응방안으로 블록체인 기반의 분산 백업 시스템을 도입을 꼽을 수 있다. 이를 통해 데이터의 실시간 백업과 안전한 암호화 기술을 활용할 수 있다. 이를 통해 백업 데이터의 안전성과 신뢰성을 높일 수 있다. 한편 로그 파일의 주기적 점검이 어려워 공격의 발견이 지연될 수 있으므로, 웹 로그 및 WebLogic 로그의 주기적 점검 및 백업을 통해 보안을 강화할 수 있다. 이러한 새로운 대응 방안들을 적용함으로써 샤오치잉의 공격에 대해 보다 효과적으로 대응할 수 있다. 다만, 이러한 대응 방안들을 구체적으로 적용하는 과정에서 시스템의 특성, 비용, 인력 등의 요소를 고려해야 한다. 이에 따라 각 기업이나 기관별로 적합한 대응 방안을 선택하고 적용할 필요가 있다. 상기 설명한 대응 방안을 정리하면 아래 Table 4와 같다.

Table 4. SQL Injection, Known Vulnerability Countermeasures

Field of response	Content
SQL Injection	Existing countermeasures : Verifying inputs, using PreparedStatement, training developers, and reviewing code
	New proposal: Web server secure coding, web firewall installation, AI-based security solutions, runtime application self-protection (RASP)
Known Vulnerability	Existing countermeasures: Check for updates and patch management, check and backup log files, and upload account information within the server
	New proposal: Multiple authentication (MFA), virtual patching technology, blockchain-based distributed backup systems, password management tool recommendations, periodic checks and backups of web logs and WebLogic logs

5. 결론

본 연구에서는 중국 해킹그룹 샤오치잉의 사이버 공격 양상과 대응방안을 중심으로 논의하였다. 특히 샤오치잉의 SQL Injection 및 Known Vulnerability 공격에 대

응하기 위한 다양한 솔루션을 제시하였다. 이러한 솔루션 중, SQL Injection에 대응하기 위해 웹 서버 시큐어 코딩, 웹 방화벽 설치, 인공지능 기반 보안솔루션, 런타임 어플리케이션 셀프 보호(RASP) 등의 적극적 도입을 제시하였다. 알려진 취약점과 관련하여 다중 인증, 가상 패치 기술, 블록체인 기반의 분산 백업 시스템, 비밀번호 관리 도구, 그리고 웹 로그 및 WebLogic 로그의 주기적 점검 및 백업 등을 제안하였다. 또한 인적 요소와 환경을 포함한 종합적 접근을 통해 사이버 보안 환경을 개선하려는 노력을 기록하였으며, 이는 샤오치잉과 같은 해킹그룹으로부터 보호할 수 있는 체계를 구축하는데 기여할 것으로 기대된다. 그러나 본 연구는 샤오치잉의 전체 공격 전략을 포함하지 않으며, 정량적 대응 효과 평가가 어렵다는 한계가 있다. 따라서 향후 연구 방향은 다음과 같다. 첫째, 다양한 해킹그룹의 공격기법 분석 및 전략을 포괄적으로 연구하여 보다 효과적인 대응 전략을 수립하는 것이 필요하다. 둘째, 대응 방안의 효과를 측정하고 평가할 수 있는 지표 개발 및 평가 방법론을 제시하여 보안 대책의 성과를 관리하고 개선할 수 있도록 해야 한다. 셋째, 인공지능, 딥러닝 등의 최신 기술을 활용하여 사이버 공격에 대응하는 자동화 시스템 및 솔루션을 응용하는 연구를 확대해야 한다. 이를 통해 사이버 보안 환경을 개선하고, 샤오치잉과 같은 해킹그룹으로부터 기업과 국민을 보호할 수 있는 체계를 구축하는데 기여할 것으로 기대된다.

References

[1] N. H. Park, J. H. Park, "Attribution of Cyber Operations by Non-State Actors under the Law of State Responsibility: With a Focus on the Cases of North Korea", *Korea Law Review*, 93, pp.1-38, Jun. 2019.
DOI: https://doi.org/10.36532/kulri.2019.93.1

[2] N. S. Chang, S. J. Kim, "U.S. Choices of Cyber Strategy and Their Security Implications", *The journal of political science & communication*, 19(3), pp.57-92, Oct. 2016.
DOI: https://doi.org/10.15617/psc.2016.10.19.3.57

[3] Money Today, Xiao Qi-Ying Returned..."The Korean security company's stock price will rise due to hacking"...What's the plan? [Internet]. Available From: https://news.mt.co.kr/mtview.php?no=2023042414544742992&utm_source=dable (accessed Apr. 20, 2023)

[4] J. H. Eom, An Introduction of Cyber Warfare: Attack and Security Techniques, p.284, hongpub, pp.18-24.

[5] H. G. Lee, J. I. Lim, K. H. Lee, "Analysis of Influencing Factors of Cyber Weapon System Core Technology Realization Period", *Journal of The Korea Institute of Information Security and Cryptology*, 27(2), 281-292, Feb. 2017.
DOI: https://doi.org/10.13089/JKIISC.2017.27.2.281

[6] D. H. Kang, M. A. Yoon, S. J. Yoon, J. H. Lim, Xiao Qi-iying Attack Group Infringement Accident and Response Plan Report, Korea Internet Security Agency, Republic of Korea, pp.4-10.

[7] N. Bharti, C. Naresh, S. Nanhay, "A Survey on the Detection of SQL Injection Attacks and Their Countermeasures", *Journal of Information Processing Systems*, 13(4), 689-702, Aug. 2017.
DOI: https://doi.org/10.3745/JIPS.03.0024

[8] H. S. Jang, "Vulnerability Analysis using the Web Vulnerability Scanner", *Journal of convergence security*, 12(4), 71-76, Sep. 2012.

[9] Y. O. Kwak, I. J. Jo, "Effective Defense Mechanism Against New Vulnerability Attacks", *The Journal of the Korea Contents Association*, 21(2), 499-506, Nov. 2021.
DOI: https://10.5392/JKCA.2021.21.02.499

[10] OWASP, Virtual Patching Best Practices [Internet]. Available From: https://owasp.org/www-community/Virtual_Patching_Best_Practices (accessed Apr. 28, 2023)

유 도 진(Do-Jin Yoo) [정회원]

- 2021년 8월 : 명지대학교 대학원 보안경영공학과 (공학박사)
- 2022년 9월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
사이버보안, 무기체계, 중국학