샤오치잉(晓骑营) 공격 그룹 침해사고 및 대응방안 보고서

등록일	@2023년 4월 10일 오전 9:43
최종수정일	@2023년 4월 10일 오후 2:26
저자	강동화 윤민아 윤수진 임정호
감수	김광연 박용규 최광희

1. 개요

해킹은 금전적 목적 외에 정치적, 외교적 공격 도구가 되기도 한다. 우크라이나를 대상으로 한 러시아의 공격, 대한민국을 대상으로 한 북한발 공격 등이 대표적이다.

올해 1월 샤오치잉*(晓骑营) 해커조직은 대한민국을 겨냥하는 도발적인 메시지와 함께 해킹을 예고했다. 이후 연구소, 학회 웹사이트 등의 메인 홈페이지가 변경되고 개인정보가 텔레그램을 통해 유포되는 등의 피해가 있었다.

* 샤오치잉(晓骑营) : 중국어로 새벽의 기병대라는 뜻

한국인터넷진흥원은 지난 1월부터 2월까지 샤오치잉 해커조직에 의한 침해사고를 대응해왔다. 본 보고서는 샤오치잉 해커조직에 의해 일어났던 침해사고들의 공격 기법을 소개하고, 대응 방안을 안내한다.

2. 타임라인

샤오치잉 해커조직(이하 샤오치잉)은 2023년 1월부터 2월까지 국내 웹사이트를 대상으로 웹페이지 변조, 정보유출 등의 공격을 수행하고 그 결과를 샤오치잉 홈페이지, 텔레그램, 해킹포럼 등을 통해서 공개하였다. 아래는 샤오치잉이 직접 언급하거나, 한국인터넷진흥원에서 대응한 이력을 정리한 타임라인이다.

- **2023년 1월 7일**
  - A社 내부자료를 샤오치잉 Github Pages에 공개(개인정보 160여명)
- **2023년 1월 20일**

    - B社 홈페이지 웹페이지 변조 후 샤오치잉 텔레그램 채널에 공개(개인정보 70여명)
- **2023년 1월 21일**
    - B社 내부정보를 샤오치잉 홈페이지에 공개
    - C社 서버의 내부 정보(디렉터리 및 파일 목록) 일부를 샤오치잉 텔레그램 채널에 공개
- **2023년 1월 22일**
    - KISA 보안공지: 국내 홈페이지 변조 관련 민간부문 보안 강화 권고 안내
- **2023년 1월 24일**
    - 샤오치잉 텔레그램 채널에 한국인터넷진흥원 공격 예고
- **2023년 1월 24일 ~ 26일**
    - C社 서버에서 DB 삭제, 웹페이지 변조 후 확보한 DB Dump 파일을 샤오치잉 텔레그램 채널에 공개
- **2023년 2월 14일**
    - WebLogic 취약점을 악용해서 D社, E社, F社 홈페이지 침투 후 웹페이지 변조
- **2023년 2월 18일**
    - A社 내부자료를 추가 확보 후 샤오치잉 홈페이지에 공개(개인정보 22,000여명)

3. 공격 기법

한국인터넷진흥원은 샤오치잉 해커조직과 관련된 침해사고를 피해기업으로부터 신고접수받고 원인분석하였다. 각 피해기업별로 침투경로, 피해유형, 공격시점을 정리한 결과는 아래와 같다.

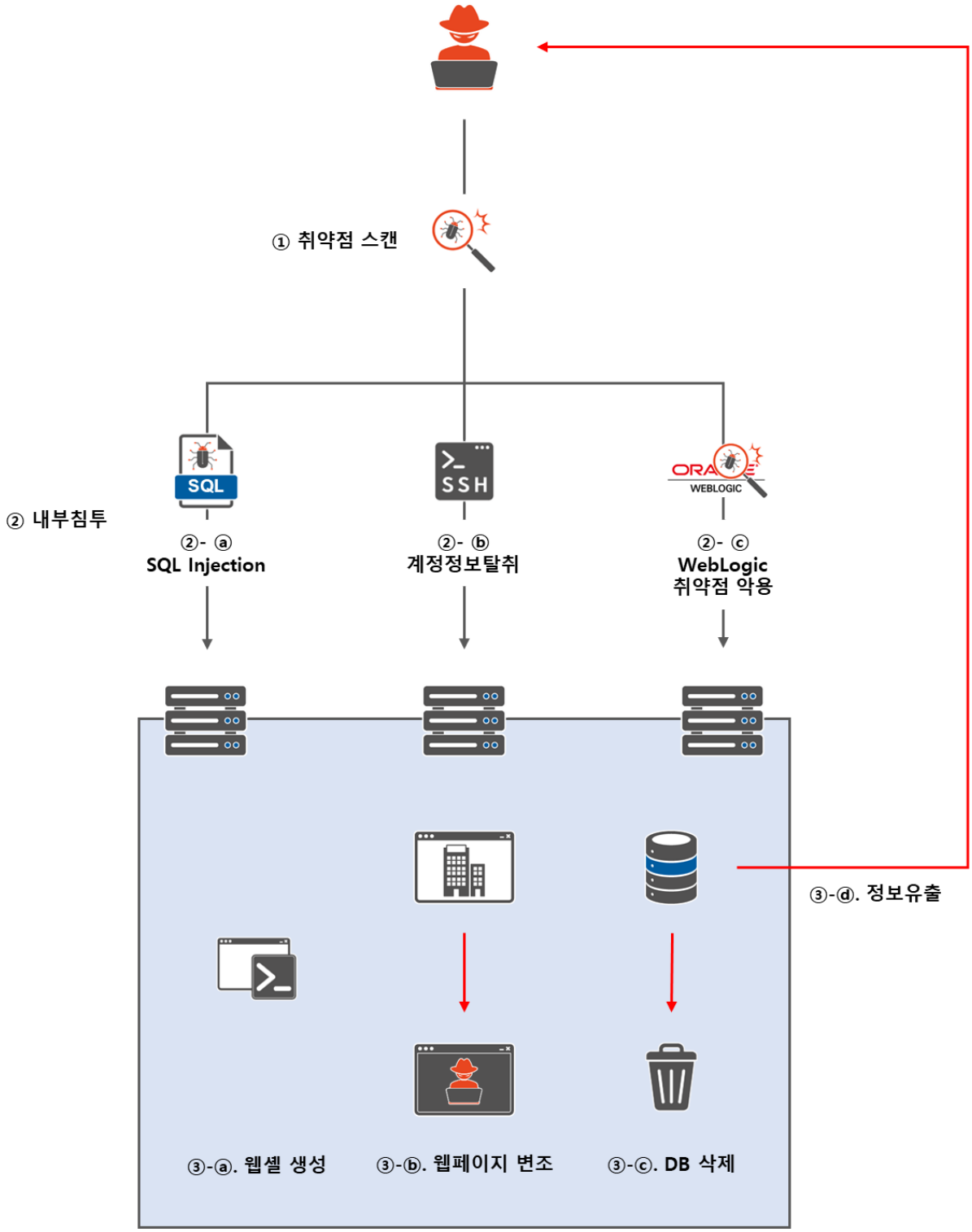
1월에는 SQL Injection이나 외부에 노출된 계정정보를 사용해서 침투해서 정보유출까지 수행했지만, 2월은 1건을 제외하고 WebLogic 취약점을 악용했으며, 다른 악성행위 없이 웹페이지 변조만 수행하였다.

웹페이지 변조의 경우 웹페이지 유형에 따라 A,B,C로 구분하였으며, A와 B의 경우는 기존의 메인 페이지를 교체하였고, C의 경우는 메인 페이지와 무관한 경로에 웹 페이지를 업로드하였다.

피해기업	침투경로	피해유형	공격시점
A社(1차)	확인 불가	정보유출	확인 불가
B社	SQL Injection	웹페이지 변조 A, 정보유출, 웹셸	2023년 1월 20일
C社	계정정보 노출	웹페이지 변조 B, 정보유출, DB 삭제, 웹셸	2023년 1월 20일(정보유출) 2023년 1월 24일(웹페이지 변조) 2023년 1월 24일(DB삭제)
D社	WebLogic 취약점	웹페이지 변조 C	2023년 2월 14일
E社	WebLogic 취약점	웹페이지 변조 C	2023년 2월 14일
F社	WebLogic 취약점	웹페이지 변조 C	2023년 2월 14일

피해기업	침투경로	피해유형	공격시점
A社(2차)	SQL Injection	정보유출	2023년 2월 18일

피해기업 6곳에서 발생한 침해사고의 침투경로와 피해유형을 종합한 구성도는 아래와 같다.



3-1. 취약점 스캔

샤오치잉은 웹사이트를 대상으로 취약점 스캔을 수행해서 공격대상들을 선별했던 것으로 확인된다. 특히 인터넷에서도 쉽게 확보할 수 있는 대표적인 해킹 툴인 Sqlmap 과 Nuclei 등이 확인되었다.

- sqlmap(https://sqlmap.org) 사용

  sqlmap은 SQL Injcetion 공격을 탐지하여 데이터베이스 서버 침투 과정을 자동화한 오픈 소스 침투테스트 도구로 공격자가 주로 악용한다.

```
5.28.***.*** - - [20/Jan/2023:03:09:43  0900] "GET /download.php?type=board&no=5329&idx=0&Iktv=1215 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')# HTTP/1.1" 200 10058606 "-" "sqlmap/1.7#pip (https://sqlmap.org)"
5.28.***.*** - - [20/Jan/2023:03:11:04  0900] "GET /download.php?type=board&no=5329&idx=0 HTTP/1.1" 200 10058606 "-" "sqlmap/1.7#pip (https://sqlmap.org)"
5.28.***.*** - - [20/Jan/2023:03:12:29  0900] "GET /download.php?type=9484&no=5329&idx=0 HTTP/1.1"200 166 "-" "sqlmap/1.7#pip (https://sqlmap.org)"
5.28.***.*** - - [20/Jan/2023:03:12:30  0900] "GET /download.php?type=board)(..,'(),"&no=5329&idx=0 HTTP/1.1" 200 166 "-" "sqlmap/1.7#pip (https://sqlmap.org)"
```

- Nuclei(https://github.com/projectdiscovery/nuclei) 사용

  Nuclei는 yaml Template을 기반으로 공격 대상 스캔을 위해 사용하는 취약점 점검 도구로 공격에 악용되었다.

```
8.213.***.*** - - [20/Jan/2023:20:56:44 +0900] "POST /clients/editclient.php?action=update&id=2KaUszFpjGzjXVdCO1V8SaRwz2K HTTP/1.1" 404 220
8.213.***.*** - - [20/Jan/2023:20:56:44 +0900] "GET /logos_clients/1.php HTTP/1.1" 404 217
8.213.***.*** - - [20/Jan/2023:21:08:53 +0900] "GET /sftp.json HTTP/1.1" 404 207
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
```

  - Nuclei를 이용해서 스캔할때 .yaml 형식의 Template을 사용할 수 있으며, 이번 공격(sftp.json 탐색)에는 아래 Template을 사용한 것으로 추정된다.
    - Nuclei Templates(geekniklabs): https://github.com/geeknik/the-nuclei-templates/blob/main/vscode-sftp.yaml

3-2. 취약한 웹 서비스를 통한 내부 침투

샤오치잉은 외부에 공개된 웹 사이트를 정찰하여, 취약한 설정 및 WAS(Web Application Server) 취약점을 악용하였다. 샤오치잉이 악용한 취약점은 아래와 같다.

A. SQL Injection

SQL Injection은 많이 알려진 취약점으로, 웹을 통해 SQL 명령어를 전달하는 취약점이다. 여전히 많은 웹사이트들이 보안조치 없이 구축되어, SQL Injection은 공격 수단으로 많이 사용된다. 샤오치잉도 SQL Injection 공격을 통해서 DB에 저장되어 있는 웹 관리자 계정정보 탈취에 성공하였다.

No	**샤오치잉이 사용한 SQL Injection 구문(출처: 웹로그)**	**설명**

No	**샤오치잉이 사용한 SQL Injection 구문(출처: 웹로그)**	**설명**
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	Table 이름 확인
2	AND ORD(MID((SELECT IFNULL(CAST(**COUNT(column_name)** AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS WHERE **table_name=admin** AND **table_schema=******),1,1))>48&idx=0	Column 개수 확인
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	admin Table에서 웹 관리자 계정 ID 검색
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	admin Table에서 웹 관리자 계정 패스워드 검색

B. 계정 설정 파일 접근

관리자의 실수로 계정 정보나 민감 정보가 외부에서 접근 가능하도록 웹 서버에 업로드 되기도 한다. C社도 그런 사례 중 하나이다. sftp.json은 개발환경과 웹 서버 동기화를 위한 SFTP 계정 정보를 담고 있다. 본래는 개발 환경에만 존재해야하는 파일이나, 부주의로 인하여 웹 서버에 업로드되었고, 샤오치잉은 이를 악용하여 접속 정보를 획득하였다.

샤오치잉이 접근한 계정 설정 파일 (/.vscode/sftp.json)

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

💡 **샤오치잉 접근 내역(웹로그, /.vscode/sftp.json)**

```
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
```

💡 **SSH 접근 성공한 로그(출처 : Secure Log)**

```
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%
```

C. 오래된 버전의 WebLogic 악용

샤오치잉은 Oracle에서 배포하는 WAS(Web Application Server) WebLogic의 오래된 버전의 취약점을 악용해서 3개의 피해기업을 침투한 것으로 분석되었으며 근거는 아래와 같다.

- **샤오치잉 공격그룹이 공개했던 공격도구**
  - 아래 그림은 샤오치잉이 2월 15일에 텔레그램에 공유한 취약점 공격 도구들이다. WebLogic 과 관련된 도구가 포함되어 있다.

- **오래 된 WebLogic 사용**
  - 피해기업 3곳(D社, E社, F社)은 오래된 버전의 WebLogic을 사용 중이었다. 설치된 버전은 공개 된지 10년 이상 지났으며 보안업데이트 적용한 적이 없는 것으로 확인되었다. 샤오치잉은 위에 언급된 도구를 사용해서 침투했을 것으로 추정된다.

피해 기업	D社	E社	F社
운영체제 버전	Solaris 10	IBM AIX 7.1	Red Hat Enterprise Linux 5.5
WebLogic Version	10.3.6	10.3.5	10.3.5
WebLogic 마지막 업데이트	2014년	2016년	2013년

- **업로드 된 웹페이지 경로**
  - 피해기업 3곳(D社, E社, F社)의 웹서버에는 같은 웹페이지가 비슷한 경로에 무단 업로드 되었다.

피해 기업	업로드 경로

피해 기업	업로드 경로
D社	[Domain Directory]/servers/*****/tmp/_WL_internal/wls-wsat/a16ls0/war/index.html
E社	[Domain Directory]/servers/*****/tmp/_WL_internal/wls-wsat/5y8uhv/war/index.html
F社	[Domain Directory]/servers/*****/tmp/_WL_internal/wls-wsat/tdm5og/war/index.html

3-3. 피해 발생

샤오치잉은 취약점을 악용해서 서버에 침투 후 웹셸 생성, 내부 정보 탈취, 웹 사이트 변조, 자료 삭제를 하였다. 1월에 침투했던 피해 기업으로부터는 내부 자료를 탈취했으며, 2월에 침투했던 피해 기업에는 1개 기업을 제외하고는 웹페이지 변조만 수행하였다.

A. 내부 정보 탈취

SQL Injection, 서비스 계정 설정 파일, 오래된 버전의 Weblogic을 악용하면, 서버 내부 자료에 접근이 가능하다. 샤오치잉은 이러한 취약점을 통해 내부 정보에 직접 접근하거나 웹셸, 백도어 등을 업로드하여 내부 정보를 탈취했다.

💡 **내부 자료 조회 (출처 : MySQL Slow Query Log)**

```
# Time: 230121  2:29:03
# User@Host: n***n [n***n] @  [5.28.***.***]
# Query_time: 109.358440  Lock_time: 0.000014 Rows_sent: 75916  Rows_examined: 75916
use %databasename%;
SET timestamp=1674235743;
SELECT * FROM `IN_BOOK_INFO`;
# Time: 230121  2:29:57
# User@Host: n***n[n***n] @  [5.28.***.***]
# Query_time: 205.455409  Lock_time: 0.171085 Rows_sent: 75224  Rows_examined: 75224
use %databasename%;
SET timestamp=1674235797;
SELECT * FROM `IN_ARTICLE_INFO`;
```

💡 **자료 탈취 확인(출처 : DB Dump 파일)**

```
/*
 Navicat Premium Data Transfer

 Source Server         : 韩国***-k***
 Source Server Type    : MySQL
 Source Server Version : 50156
 Source Host           : localhost:3306
 Source Schema         : submit_k***

 Target Server Type    : MySQL
 Target Server Version : 50156
 File Encoding         : 65001

 Date: 21/01/2023 02:30:14
*/

SET NAMES utf8;
SET FOREIGN_KEY_CHECKS = 0;

-- ----------------------------
```

B. 웹사이트 변조 및 무단생성

샤오치잉은 해킹사실을 과시하거나 새로운 멤버를 모집하는 목적의 웹페이지를 메인페이지와 교체하거나 추가로 업로드 하였다. 한국인터넷진흥원은 피해기업의 서버를 분석하면서 샤오치잉이 무단 업로드한 3가지 웹페이지를 확인할 수 있었다.

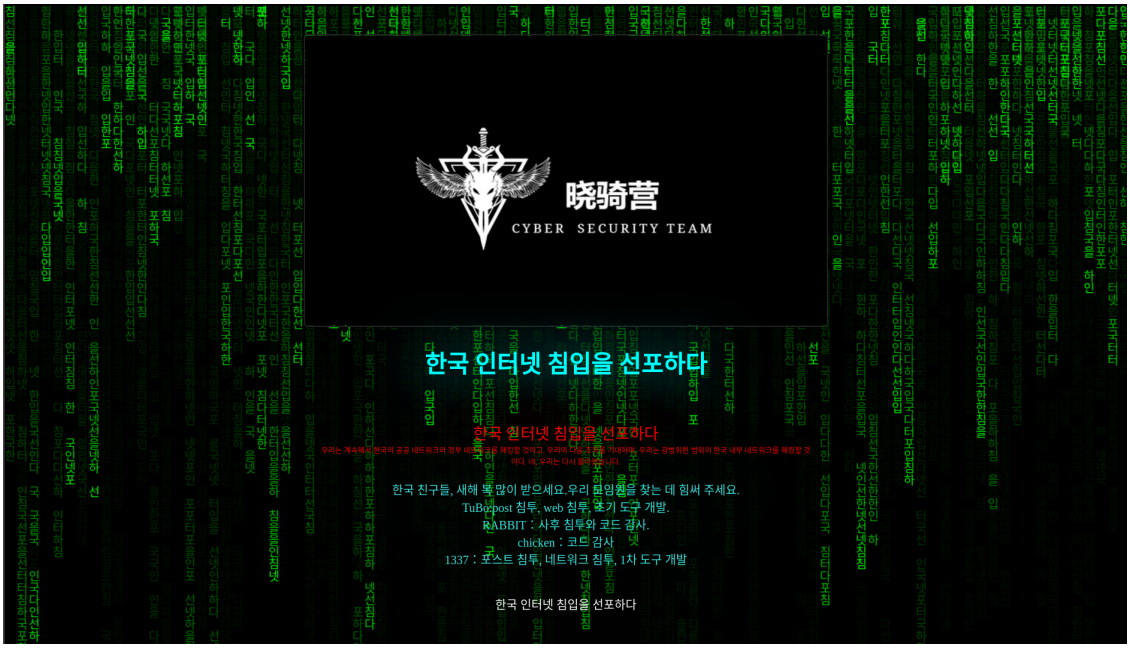
샤오치잉이 업로드한 첫번째 웹페이지 유형

우리는 계속해서 한국의 공공 네트워크와 정부 네트워크를 해킹할 것이고, 우리의 다음 트워크를 해킹할 것이다. 네, 우리는 다시 돌아왔습니다.

晓骑营

CYBER SECURITY TEAM

샤오치잉이 업로드한 두번째 웹페이지 유형



샤오치잉이 업로드한 세번째 웹페이지 유형

Announced voluntary joining members? Saint Michael

[I voluntarily joined the Dawn Cavaliers and announced that I voluntarily joined the South Korean action plan.]

My ID is: Saint Michael

I am coming from? Dark networkDawn Cavalry

C. 자료 삭제

샤오치잉은 C社 서버에 있는 DB를 탈취한 후 마지막으로 삭제도 하였다.

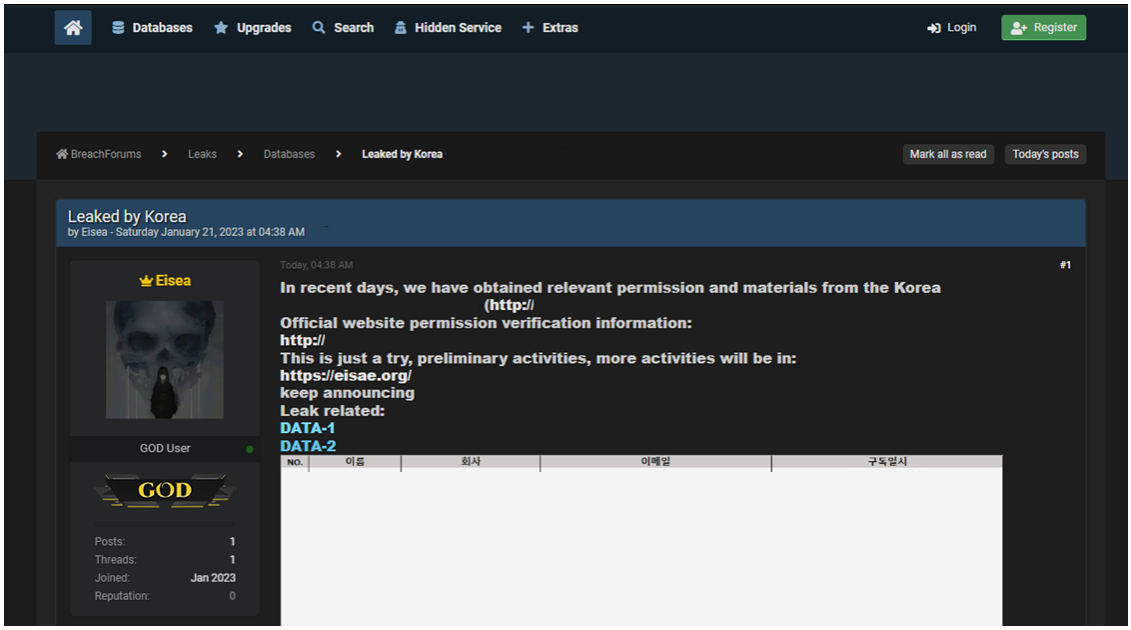
DB 삭제 (출처 : MySQL Binary Log)

```
#230124 22:57:28 server id 1  end_log_pos 67928024  Query thread_id=629978 exec_time=
1 error_code=0
SET TIMESTAMP=1674568648/*!*/;
DROP DATABASE `%databasename%` /*!*/;
# at 67928024
#230124 22:57:32 server id 1  end_log_pos 67929472  Query thread_id=629989 exec_time=
1 error_code=0
SET TIMESTAMP=1674568652/*!*/;
DROP DATABASE `%databasename%` /*!*/;
# at 67929472
```

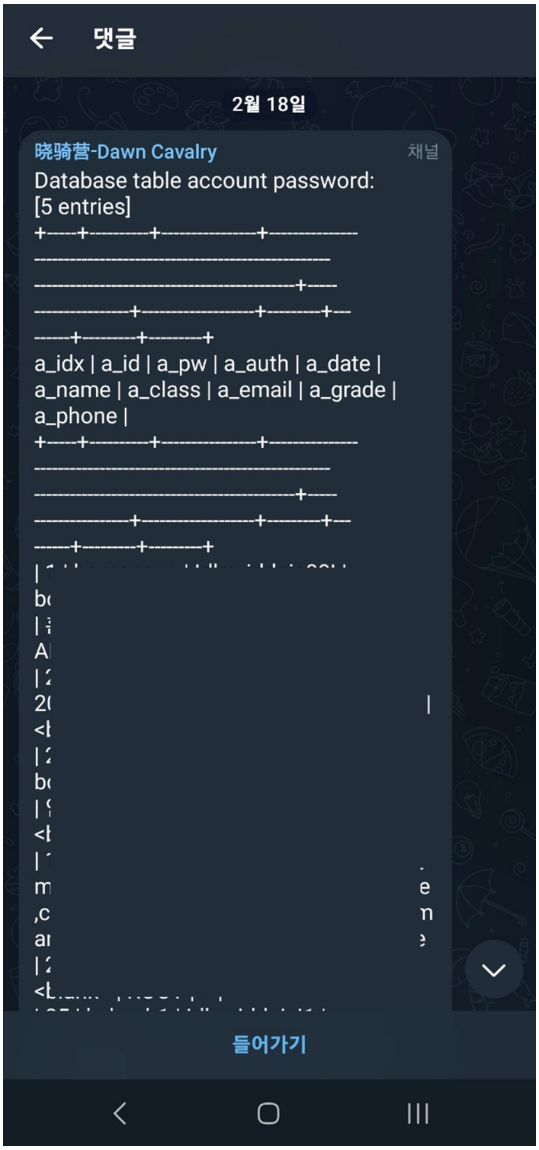
3-4. 해킹 사실 공개

샤오치잉은 해킹 사실을 입증하기 위해서 탈취한 정보를 공개하였고, 일부 웹페이지를 변조하였다. 또한 피해기업들로 부터 탈취한 개인정보나 변조된 화면 사진을 여러 채널(해킹포럼, 텔레그램, Gihub Pages등)을 통해 실시간 공개하였는데 이는 국내언론 및 정부기관 등에 자신들의 해킹 실력을 입증하거나 과시하기 위한 목적으로 풀이되며 금전적 목적이나 핵티비즘의 성격으로 보이기는 어려웠다.

해킹포럼(breached)에 공개한 탈취 정보



텔레그램에 공개한 탈취 정보



Github Pages(Github에서 제공하는 웹 호스팅서비스)에 공개한 탈취 정보

4. 대응 방안

샤오치잉의 공격을 방어하고, 피해를 최소화하기 위한 방법은 아래와 같이 소개한다.

4-1. SQL Injection 공격 예방

웹 서버 시큐어 코딩

시큐어 코딩은 안전한 소프트웨어 개발을 위해 소스 코드에 잠재한 보안 취약점을 제거하고, 보안과 관련된 기능을 구현하는 등의 활동을 나타낸다. SQL Injection 대응을 위하여, 한국인터넷진흥원이 배포하는 웹 서버 보안 강화 안내서, 소프트웨어 개발 보안 가이드, JavaScript 시큐어코딩 가이드를 참고하길 바란다. 해당 가이드에는 SQL Injection을 대응하기 위한 방법과 예제 코드 등이 있다.

웹 방화벽 설치

웹 방화벽은 웹 서버를 안전하게 보호하기 위해 웹 공격을 탐지하고 차단하는 보안 솔루션이다. 웹 방화벽은 SQL Injection뿐 아니라 XSS(Cross Site Scripting), CSRF(Cross Site Request Forgery) 등의 웹 공격 방어에 특화되어있다. 전반적 웹 취약점 대응을 위해 웹 방화벽 사용을 권장한다. 중소기업의 경우, 한국인터넷진흥원에서 지원하는 웹 방화벽(캐슬)을 사용할 수 있다.

4-2. 계정정보 관리

서버 내 계정정보 업로드 여부 점검

IDE(Integrated development environment, 통합 개발 환경)를 이용하여 개발하는 경우 개발의 편의성을 위해 서버와 개발PC를 동기화하는 플러그인을 사용하는 경우가 많다. 그 과정에서 생성되는 설정파일에는 접속정보가 평문으로 적혀있는데, 이 정보가 실수로 서버에 올라가는 경우 접속정보가 외부에 노출될 수 있다. 웹 취약점 도구는 이러한 실수들을 점검해주고 있는데, 샤오치잉은 해당 도구를 악용하여 서버 내 취약점을 찾고 공격에 이용하였다.

서버 관리자 및 개발자는 주기적으로 웹 서버 점검을 통해 의도하지 않은 접속정보가 공유되고 있는지 확인하는 것이 필요하다.

💡 **sftp.json 예시**

```
{
    "name": "Profile Name",
    "host": "name_of_remote_host",
    "protocol": "ftp",
    "port": 21,
    "secure": true,
    "username": "username",
    "remotePath": "/public_html/project",  <---- This is the path which will be downl
oaded if you "Download Project"
    "password": "password",
    "uploadOnSave": true
}
```

4-3. 운영체제 및 소프트웨어 버전 업그레이드

샤오치잉 관련 피해기업에서 운영하고 있던 서버에는 오래 된 버전의 운영체제와 WebLogic 등의 소프트웨어를 사용하고 있었다. WebLogic을 사용하는 3개 피해기업 모두 10년 이상 지난 버전을 사용중이었다. 운영체제의 경우 CentOS, Ubuntu, Solaris, AIX, Redhat 등 다양하게 사용중이었으나, 1개 피해기업을 제외하고는 모두 지원기간이 만료되었다. 지원기간이 만료된 운영체제는 최신 보안업데이트를 받을 수 없기 때문에 각종 취약점에 노출되어 있게 된다. 실제로 이번 피해기업 중 일부는 다양한 취약점 공격도구와 함께 최고 관리자로 생성 된 악성코드도 발견되었다. 따라서 이러한 취약점으로부터 보호하기 위해서는 사용중인 운영체제와 소프트웨어를 최신 버전으로 반드시 업그레이드 해야한다.

4-4. 중요자료백업

C社의 해킹 사고의 경우, 운영중인 DB가 삭제되었다. 샤오치잉의 랜섬웨어 공격 사례는 아직 발견되지 않았지만, 확보하게 되는 권한과 의지에 따라서 랜섬웨어 공격가능성은 충분히 존재하기 때문에 중요한 자료는 오프라인으로 별도 백업해 두는 것을 권장한다.

자세한 백업 방법은 한국인터넷진흥원에서 배포한 랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드를 참고하길 바란다.

4-5. 로그 설정

웹 로그 주기적 점검 및 백업

웹사이트를 통한 침투의 대부분 흔적은 웹 로그에 기록되며, 이번 사고의 침해사고 경로 및 원인 분석 등을 위해 중요한 증거 자료로 활용되었다.

다만 일부 피해 기관에서는 너무 짧은 로그 저장주기(일주일 이하)로 인해 분석에 어려움이 있었으므로 향후 침해사고 발생 시 신속한 원인 분석을 위해서 가급적 장기간의 로그 저장(최소 2년 이상)과 백업을 권장한다.

> 💡 **(개인정보보호위원회) 개인정보의 안전성 확보조치 기준, 제8조(접속기록의 보관 및 점검)**

WebLogic 로그 저장 연장

WebLogic은 기본설정으로 7개의 로그 파일 개수를 저장하도록 설정되어 있어서 비교적 매우 짧은 기간의 로그가 저장되고 있다. 침해사고를 뒤늦게 인지할 경우, 로그가 삭제되어서 원인 분석이나 침투 시점 확인이 어려워 질 수 있다.

WebLogic 로그는 WebLogic 콘솔을 통해서, 로그 저장 설정을 변경 할 수 있다. 각 환경에 맞춰 저장하되, 안정적인 운영을 위해 2년 이상의 로그가 저장되도록 설정 및 보관을 권장한다.

4-6. 한국인터넷진흥원 정보보호 서비스 활용

한국인터넷진흥원에서는 기업 보안에 도움이 될 수 있는 다양한 보안서비스, 보고서 및 가이드를 제공하고 있으며 보안 관련 중요한 이슈 발생시 보안공지를 통해서 공유하고 있다. 자세한 내용은 아래 한국인터넷진흥원 인터넷 보호나라 홈페이지에서 확인할 수 있다.

한국인터넷진흥원 보안공지

- 보안 관련 주요 이슈 발생시 한국인터넷진흥원에서 관련 내용을 공지하고 있으며, 샤오치잉 관련 보안공지도 포함되어 있음

보안공지 > 알림마당 : KISA 인터넷 보호나라&KrCERT

KISA https://www.krcert.or.kr/kr/bbs/list.do?menuNo=205020&bbsId=B0000133

한국인터넷진흥원 배포 가이드/보고서

- 한국인터넷진흥원에서 발간하는 각종 보안 가이드와 공격그룹 분석 보고서를 제공하고 있으며, 이번 샤오치잉 공격 관련으로는 웹 서버 보안 강화 안내서, 소프트웨어 개발 보안 가이드, JavaScript 시큐어코딩 가이드를 권장한다.

보고서/가이드 > 알림마당 : KISA 인터넷 보호나라&KrCERT

https://www.krcert.or.kr/kr/bbs/list.do?menuNo=205021&bbsId=B0000127

중소기업 대상 보안서비스

- 중소기업을 대상으로 한국인터넷진흥원에서 제공하는 보안서비스이며, 이번 샤오치잉 공격 관련으로는 내 서버 돌보미, 중소기업 홈페이지 보안강화 보안서비스를 권장한다.

기업 서비스 홈 > 기업 서비스 > 주요사업 소개 > 정보보호 서비스 : KISA 인터넷 보호나라&KrCERT

https://www.krcert.or.kr/kr/subPage.do?menuNo=205007

중소기업 침해사고 피해지원 서비스

- 중소기업에서 침해사고가 발생하는 경우 한국인터넷진흥원에서 원인분석 및 재발방지를 위한 원인제거, 예방컨설팅, 보안교육을 지원하고 있다.

중소기업 피해지원 > 정보보호 서비스 : KISA 인터넷 보호나라&KrCERT

https://www.krcert.or.kr/kr/subPage.do?menuNo=205004

5. 결론

샤오치잉은 한국정부를 향한 해킹예고, 국내 기업을 대상으로 한 해킹 및 결과 공개로 많은 주목을 받았다. 한국인터넷진흥원에 신고접수 된 피해기업은 대부분 보안에 많은 투자를 하기 어려운 소규모 기업이나 기관이었다. 그리고 신고접수 된 피해기업에 대해 원인분석을 해본 결과, 고전적인 기법(SQL Injection, 알려진 취약점 악용 등)을 사용한 것을 확인할 수 있었다.

한국인터넷진흥원에서는 보안에 많은 투자를 하기 어려운 중소기업을 대상으로 다양한 보안 서비스와 보고서를 제공하고 있으며, 침해사고 발생시 중소기업 침해사고 피해지원 서비스를 통해 침해사고 원인분석 및 후속 조치를 지원하고 있다.

본 보고서와 한국인터넷진흥원의 다양한 서비스를 통해 기본 보안을 강화하여, 향후 발생할 수 있는 침해사고를 대비하길 기대하며 보고서를 마무리한다.

Appendix

악성파일(웹셸)

MD5 Hash
88A630E0633045159CE0C0ACC01BD5F4
ACE2AEF7F6F03233AC9836977A82A276
E458DB1C3C1359A12A3D4C952022CB71

MD5 Hash
67EBA714F23EE4B7C9CAF7136CB983DB
0FBD87B813516942F0391D783F4F70F2
4C3866023B50AA90A7BAA30A49A7C06C

공격자 IP

> 💡 **IP 조회는 KISA WHOIS OpenAPI 활용**

IP	**국가코드(국가명)**
8.213.132.75	SG(싱가포르)
5.28.34.201	KH(캄보디아)
36.227.231.17	TW(대만)
114.43.86.96	TW(대만)
203.69.23.25	TW(대만)
114.43.86.96	TW(대만)
142.202.49.101	US(미국)
106.55.207.123	CN(중국)
218.190.235.118	HK(홍콩)
149.154.161.220	AG(안티구아 바부다)
218.190.235.135	HK(홍콩)
149.154.161.253	AG(안티구아 바부다)
114.246.35.136	CN(중국)
111.202.167.85	CN(중국)
114.255.249.182	CN(중국)
114.247.113.166	CN(중국)
103.142.65.131	IN(인도)
103.142.65.141	IN(인도)
156.251.145.233	SC(세이셸)
163.47.15.102	KH(캄보디아)
104.28.211.105	US(미국)
114.43.88.126	TW(대만)
203.69.23.25	TW(대만)
114.25.103.20	TW(대만)
192.109.205.229	US(미국)

IP	**국가코드(국가명)**
192.109.205.209	US(미국)
192.109.205.179	US(미국)