ISBN : 000-00-000-0000-0

Samba 취약점 및 토렌트 보안위협 사례분석 보고서

2015년

한국과학기술정보연구원
과학기술사이버안전센터

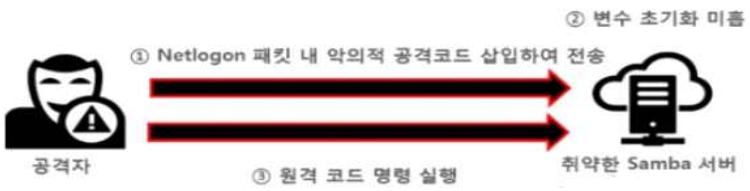
1. 공격 과정 및 특징

가. Samba 원격코드 실행(Remote-Code-Exectuion) 취약점

Samba Remote-Code-Execution(CVE-2015-0240) 취약점은 Samba*에 구현되는 "Server PasswordSet" 함수의 NetLogin RPC API를 사용하여 공격자는 특수하게 조작된 Net Login 패킷을 전송하여 임의의 코드를 실행 가능한 취약점이다.

* Samba : 시스템 간 파일·프린터를 공유할 수 있도록 제작된 오픈소스 기반 소프트웨어

⇒ 접근이 허용되지 않은 원격 사용자가 Samba 서버에서 루트(Root) 권한을 획득 가능



< 공격 시나리오 >

① 공격자가 *_netr_serverPasswordSet* 취약코드를 지닌 취약한 Samba 서버에 Netlogin 패킷을 조작하여 원격명령 실행 공격코드를 삽입하여 전송

② 취약한 코드는 *_netr_server/netlogin/srv_netlog_nt.c* 내 *_netr_serverPasswordSet*

③ 취약한 Samba 서버는 ServerPasswordSet RPC 요청 처리 시 특정 변수를 초기화하지 않아 메모리 스택에 존재하는 코드를 원격 명령 실행 가능

Samba 원격코드 실행 취약점에 영향을 받는 시스템은 <다음>과 같다.

◦ Samba 3.5.x ~ 4.2.0rc4 버전

나. 토렌트를 통한 보안위협 사례 분석(가위바위보.zip)

’15. 3·4 국내 특정 토렌트 사이트에 **가위바위보.zip.torrent 파일이 게시**되었다. 등록된 게시 글은 “19禁 가위바위보 옷벗기기 토렌트”라는 제목으로 실제 일본에서 만들어진 음란한 플래시 기반의 게임파일이 포함되어 있다.

노출수위가 높은 유해성 게임이 미성년자를 포함해 불특정 다수에게 무차별 배포된 점과 함께 더욱 큰 문제점은 이 게임파일 내부에 원격제어를 통해 미상의 악의적인 해커가 감염된 이용자 컴퓨터에 몰래 접속할 수 있는 악성코드까지 몰래 숨겨져 있다.

공격자는 주도 면밀하게 악성코드를 제작하여 처음 토렌트에 등록할 때부터 관심 유발을 높이기 위해 음란한 자료에 악성코드를 추가하였다.

< 토렌트 음란게임과 악성코드 유포 절차 >

악성코드는 마치 정상적인 게임 파일로 공유되어 여러 토렌트 사이트를 통해 확산되었다. 토렌트 사이트 특성상 여러 곳에서 동시다발적으로 배포 되었다.

2. 대응 방법 및 해결 방안

가. Samba 원격코드 실행(Remote-Code-Exectuion) 취약점

① 취약점 확인 방법

CVE-2015-0240 POC 링크

⇒ https://gist.github.com/worawit/33cc5534cb555a0b710b/download

※ Ubuntu 12.04 x86 버전에서만 실제 공격이 가능

<스크립트 사용법>

◦ 명령어 : cve-2015-0240_samba_poc[점검 IP]

<스크립트 점검 결과 확인>

```
[root@localhost /]# smbstatus

Samba version 3.6.23-12.el6
PID     Username      Group         Machine
-------------------------------------------------------------------

Service      pid     machine       Connected at
-------------------------------------------------------

No locked files

[root@localhost /]# python cve-2015-0240_samba_poc localhost
connection lost!!!
might be vulnerable
```

※ 점검 시스템 정보 : Centos 6.6, samba 3.6.23-12.e16

② Samba 버전 확인 방법

Redhat Enterprise Linux / CentOS 경우 ↵

◦ rpm -qa | grep samba

Debian / ubunt 및 기타 제품 ↵

- dpkg -l | grep samba

③ Samba 보안 업데이트 방법

Redhat Enterprise Linux / CentOS 경우 ↵

- yum update samba // Samba 업데이트
- /etc/init.d/smbd restart // Samba 데몬 재시작

Debian / ubunt 및 기타 제품 ↵

- sudo apt-get update && sudo apt-get install samba // Samba 업데이트
- /etc/init.d/smbd restart // Samba 데몬 재시작

운영 환경으로 인해 업데이트가 불가능한 경우 ↵

- sudo apt-get update && sudo apt-get install samba // Samba 업데이트
- /etc/init.d/smbd restart // Samba 데몬 재시작

3. 상세 분석 및 기타

가. Samba 원격코드 실행(Remote-Code-Exectuion) 취약점

※ 취약 코드(librpc/gen_ndr/srv_netlogon.c)

```
1  NTSTATUS _netr_ServerPasswordSet(struct pipes_struct *p, struct netr_ServerPasswordSet *r)
2  {
3      NTSTATUS status = NT_STATUS_OK;
4      int i;
5      struct netlogon_creds_CredentialState *creds;
6          [...]
7      status = netr_creds_server_step_check(p, p->mem_ctx,
8                                            r->in.computer_name,
9                                            r->in.credential,
10                                           r->out.return_authenticator, &creds);
11     unbecome_root();
12
13     if (!NT_STATUS_IS_OK(status)) {
14             [...]
15         TALLOC_FREE(creds);
16         return status;
17     }
```

취약코드 내 _netr_ServerPasswordSe()는 Samba의 NetLogin RPC API(api_netr_Server PasswordSet)에 의해 호출되고 위 <그림> 1번라인으로 초기화 과정없이 netr_creds_server_step_check() 함수의 creds 포인터로 전달된다.

공격자는 이를 악용하여 creds 값을 제어할 수 있으며, 초기화되지 않고 스택에 남아 있는 값을 TALLOC_FREE 함수를 이용하여 실행 가능하다.

참고 링크

* https://securityblog.redhat.com/2015/02/23/samba-vulnerability-cve-2015-0240/
* https://gist.github.com/worawit/33cc5534cb555a0b710b
* https://www.us-cert.gov/ncas/current-activity/2015/02/24/Samba-Remote-Code-Execution-Vulnerability
* http://blog.trendmicro.com/trendlabs

나. 토렌트를 통한 보안위협 사례 분석(가위바위보.zip)

① 유포 과정

공격자는 이용자들이 많은 특정 토렌트 사이트에 성인용을 뜻하는 '19禁'이라는 특정 키워드와 노출수위가 높은 음란성 이미지를 포함시켜, 정상적인 게임파일처럼 위장한 악의적인 토렌트 파일을 등록했다. 이후 이 토렌트 파일은 여러 사이트를 통해 지속적으로 공유되기 시작해 현재 다수의 토렌트 사이트에서 배포되었다.

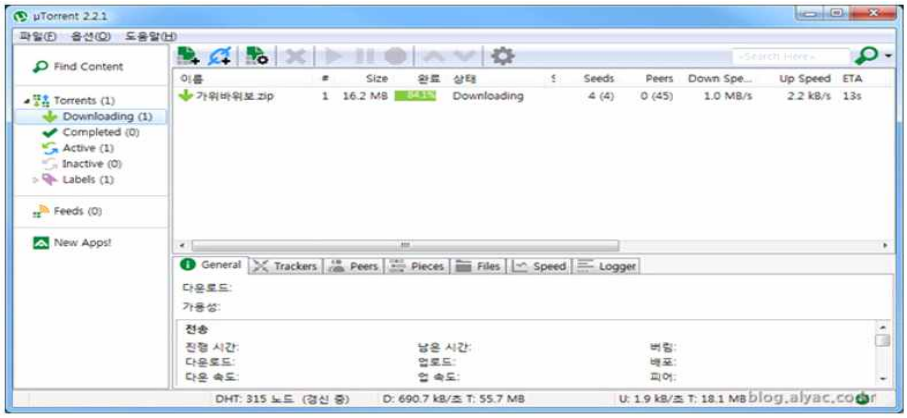
국내에서 운영 중인 토렌트 사이트를 살펴보면 도메인이 상이해도 하위 주소들이 비슷하다는 점을 알 수 있습니다. 현재 이 토렌트 사이트들은 공통적으로 동일한 악성코드를 배포하는데 악용되고 있다.

```
http://www.tog    .org/bbs/board.php?bo_table=torrent_game&wr_id=3
http://www.gong    .net/bbs/board.php?bo_table=torrent_game&wr_id=8
http://www.torrentt    .net/bbs/board.php?bo_table=torrent_game_tt&wr_id=1
http://tort    .com/bbs/board.php?bo_table=tr_game&wr_id=5
http://nate.to    /bbs/board.php?bo_table=game&wr_id=3
http://www.won    .com/bbs/board.php?bo_table=torrent_game&wr_id=3
http://www.torrentb    .net/bbs/board.php?bo_table=torrent_game&wr_id=6
```

< 여러 토렌트 사이트에 공통 등록된 주소 >

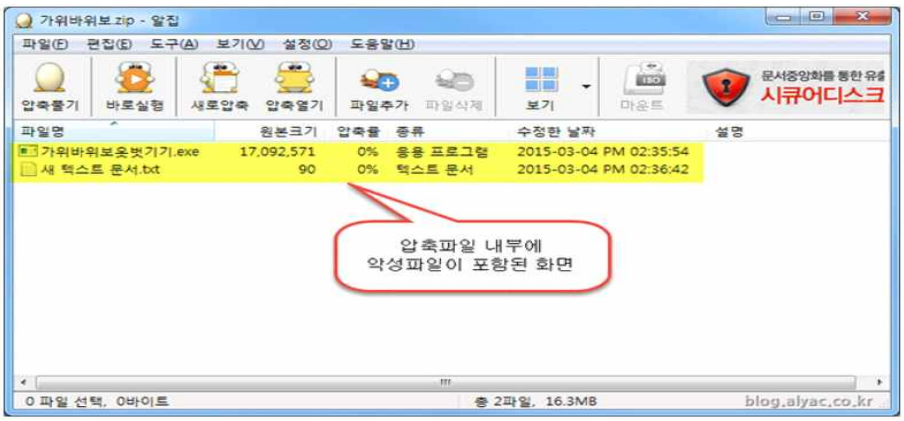
<다음>은 '15. 3 · 4 국내 특정 토렌트 사이트에 올려진 실제 화면이다.

토렌트 이용자가 *가위바위보.zip.torrent* 이름의 파일을 받아 파일을 실행할 경우 <다음>과 같이 *가위바위보.zip* 파일이 다운로드되게 된다. 가위바위보.zip 압축파일 내부에는 *가위바위보옷벗기기.exe* 실행파일과 새 *텍스트 문서.txt 문서파일*이 포함되어 있다.

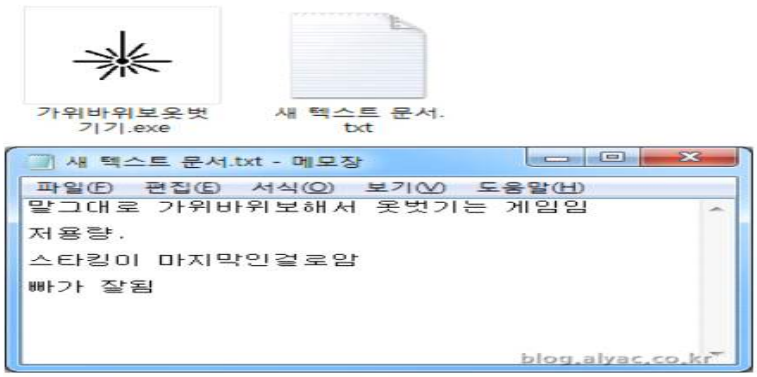


< 토렌트를 통해서 배포 중인 화면 >

압축된 날짜를 확인해 보면 '15. 3·4 오후 2시 35분경이라는 점을 알 수 있다. **공격자는 토렌트 파일을 먼저 배포**하고, 이후에 압축된 파일을 제작했던 것으로 추정할 수 있다.



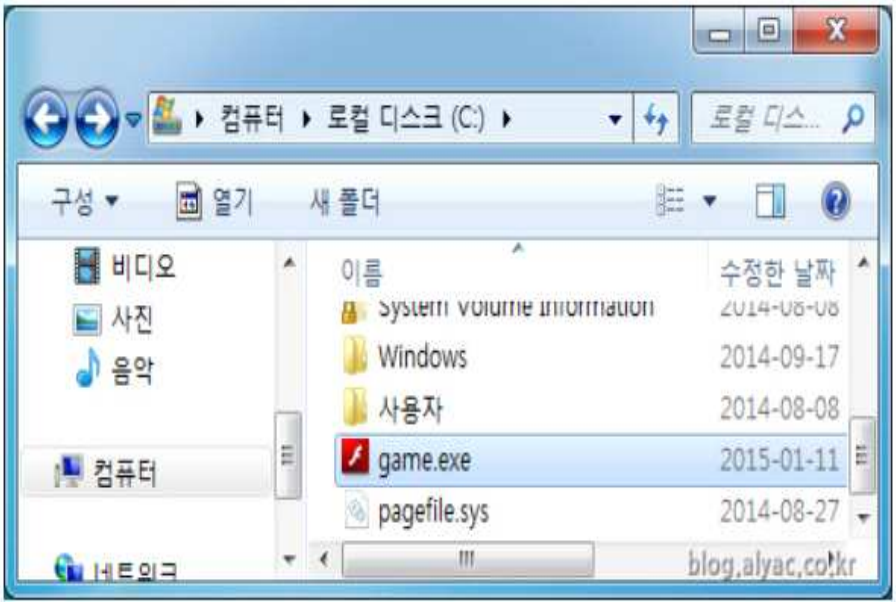
< 가위바위보.zip 압축파일 내부 화면 >



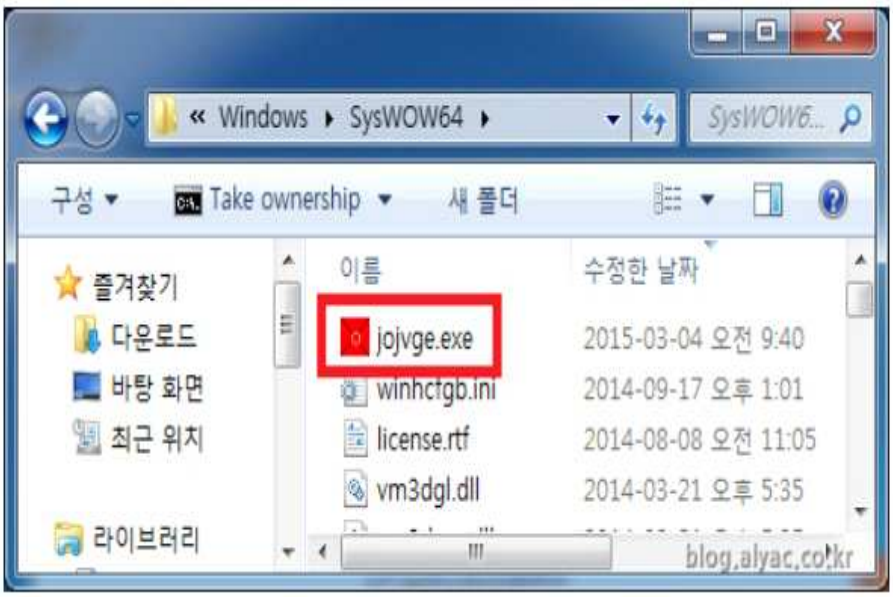
< 압축 내부에 있는 파일 화면 >

가위바위보옷벗기기.exe 파일이 실행되면 먼저 시스템 드라이브 루트경로(C:\)에 *qwe.exe, game.exe* 파일을 생성하고 실행한다. 여기서 qwe.exe 파일이 악성코드이며, game.exe 파일이 플래시 기반의 음란 게임파일이다.

악성코드는 이후 시스템 폴더 경로에 랜덤한 파일명으로 복사본을 만들어 작동하고, 루트 드라이브에 존재하던 원본은 삭제한다.



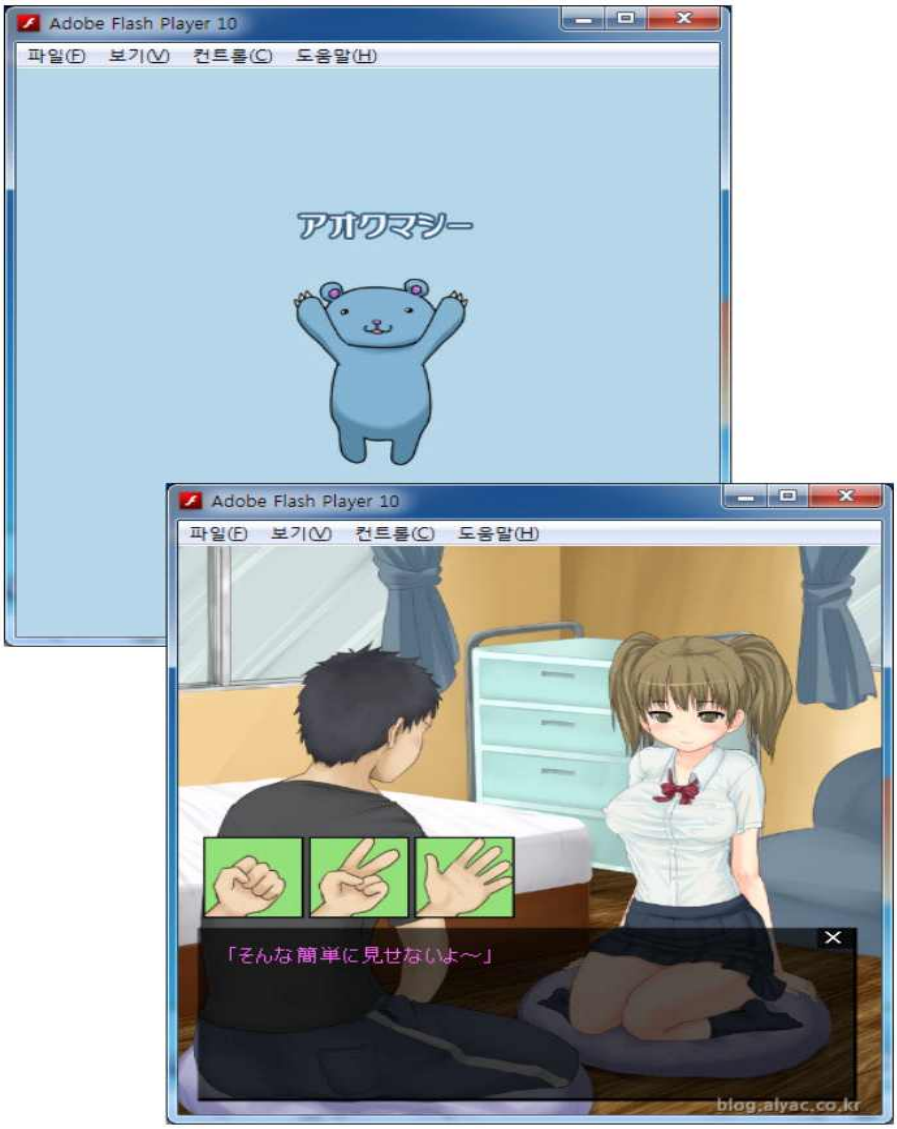
< 루트 드라이브 경로에 생성된 게임 파일 >



< 시스템 폴더 경로에 생성된 악성코드 >

② 분석 정보

game.exe 플래시 게임파일이 실행되면 <다음>과 같이 일본에서 제작된 음란 게임이 시작된다.



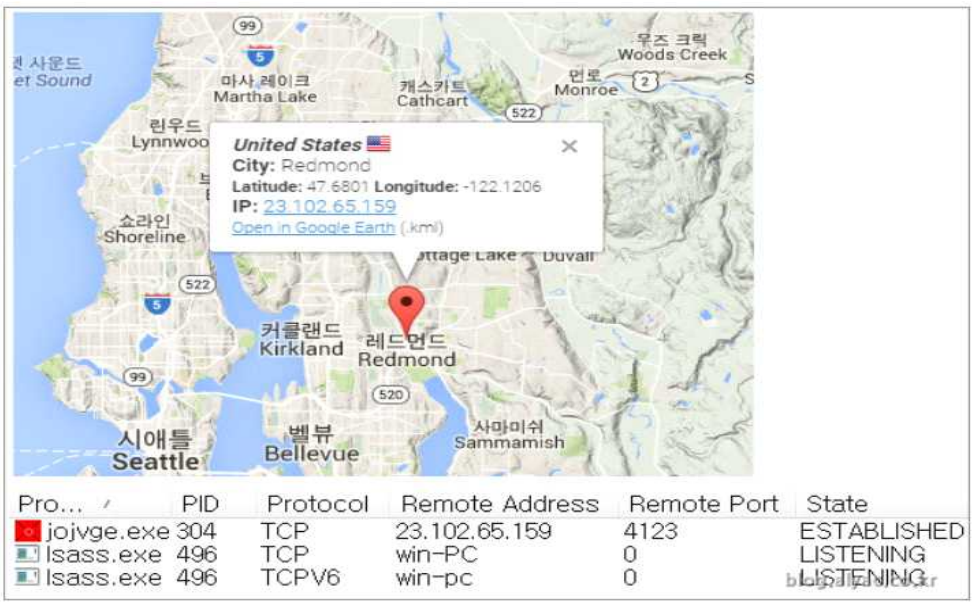
< 플래시 게임이 실행된 화면 중 일부 >

악성코드는 분석을 방해하기 위해서 'Themida' 프로그램으로 실행 압축되어 코드 내부적으로 사용된 언어가 중국어(zh-cn)로 설정된 것을 알 수 있다.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000017D0   54 5C 43 75 72 72 65 6E 74 56 65 72 73 69 6F 6E  T\CurrentVersion
000017E0   0D 0A 4B 45 52 4E 45 4C 33 32 2E 64 6C 6C 0D 0A  ..KERNEL32.dll..
000017F0   47 65 74 53 79 73 74 65 6D 44 69 72 65 63 74 6F  GetSystemDirecto
00001800   72 79 41 0D 0A 47 45 54 20 25 73 20 48 54 54 50  ryA..GET %s HTTP
00001810   2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 69 6D  /1.1..Accept: im
00001820   61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65 2F 78  age/gif, image/x
00001830   2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67 65 2F  -xbitmap, image/
00001840   6A 70 65 67 2C 20 69 6D 61 67 65 2F 70 6A 70 65  jpeg, image/pjpe
00001850   67 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78  g, application/x
00001860   2D 73 68 6F 63 6B 77 61 76 65 2D 66 6C 61 73 68  -shockwave-flash
00001870   2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 76 6E  , application/vn
00001880   64 2E 6D 73 2D 65 78 63 65 6C 2C 20 61 70 70 6C  d.ms-excel, appl
00001890   69 63 61 74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 70  ication/vnd.ms-p
000018A0   6F 77 65 72 70 6F 69 6E 74 2C 20 61 70 70 6C 69  owerpoint, appli
000018B0   63 61 74 69 6F 6E 2F 6D 73 77 6F 72 64 2C 20 2A  cation/msword, *
000018C0   2F 2A 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75  /*..Accept-Langu
000018D0   61 67 65 3A 20 7A 68 2D 63 6E 0D 0A 41 63 63 65  age: zh-cn..Acce
000018E0   70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69  pt-Encoding: gzi
000018F0   70 2C 20 64 65 66 6C 61 74 65 0D 0A 55 73 65 72  p, deflate..User
00001900   2D 41 67 65 6E 74 3A 4D 6F 7A 69 6C 6C 61 2F 34  -Agent:Mozilla/4
00001910   2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20  .0 (compatible;
00001920   4D 53 49 45 20 25 64 2E 30 3B 20 57 69 6E 64 6F  MSIE %d.0; Windo
00001930   77 73 20 4E 54 20 25 64 2E 31 3B 20 53 56 31 29  ws NT %d.1; SV1)
00001940   0D 0A 48 6F 73 74 3A 20 25 73 3A 25 64 0D 0A 43  ..Host: %s:%d..C
00001950   6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D  onnection: Keep-
00001960   41 6C 69 76 65 0D 0A 47 45 54 20 25 73 20 48 54  Alive..GET %s HT
00001970   54 50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20  TP/1.1..Accept:
00001980   69 6D 61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65  image/gif, image
00001990   2F 78 2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67  /x-xbitmap, imag
```

< 악성코드 내부에서 포함된 언어 설정 >

악성코드에 감염된 경우 <다음>과 같이 호스트 23.102.65.159 주소로 접속하여 공격자의 추가 명령을 대기한다.



Pro...	PID	Protocol	Remote Address	Remote Port	State
jojvge.exe	304	TCP	23.102.65.159	4123	ESTABLISHED
lsass.exe	496	TCP	win-PC	0	LISTENING
lsass.exe	496	TCPV6	win-pc	0	LISTENING

< 미국의 조정서버(C&C)로 접속한 화면 >

다수의 토렌트 사이트를 통해 원격제어와 개인정보 유출 피해를 입을 수 있는 악성코드가 은밀하게 유포되고 있다. 특히, 음란한 내용으로 이용자들을 현혹시키고 있어 보다 각별한 주의가 필요하다.