Introdução à engenharia reversa de códigos maliciosos
Parte II

Apresentador: Marcus Botacin
Monitores: Lucas Galante & Giovanni Bertão

UNICAMP

Agosto/2018

Roteiro

Roteiro

Revisitando o `crackme`.

Analise o binário

- Files/crackme2

Revisitando o `crackme`.

O que você (provavelmente) deve ter feito.

```
......  ;****************************************
......  ; function passwd (global)
......  ;****************************************
......  passwd:                                 ;xref o4
......    push        rbp
4007a7    mov         rbp, rsp
4007aa    sub         rsp, 10h
4007ae    mov         [rbp-8], rdi
4007b2    mov         rax, [rbp-8]
4007b6    mov         esi, strz_The_Pass_400a64
4007bb    mov         rdi, rax
4007be    call        wrapper_602040_400660
4007c3    test        eax, eax
4007c5    nop
4007c6    nop
4007c7    mov         edi, strz_Oh_Yeah__400a6d
```

Revisitando o `crackme`.

O que você (provavelmente) não fez.

```
.....  ! main:                                    ;xref o40
.....  !   push    rbp
4007d5 !   mov     rbp, rsp
4007d8 !   sub     rsp, 120h
4007df !   mov     rax, fs:[28h]
4007e8 !   mov     [rbp-8], rax
4007ec !   xor     eax, eax
4007ee !   mov     edx, 21h
4007f3 !   mov     esi, passwd
4007f8 !   mov     edi, 0
4007fd !   call    Crc32_ComputeBuf
400802 !   mov     [rbp-118h], rax
400809 !   cmp     qword ptr [rbp-118h], 1fb61
400814 !   jnz     loc_400820
400816 !   mov     edi, 0
40081b !   call    wrapper_602050_400680
```

Roteiro

Anti-Análise 1.

Analise o binário

- Files/context

Anti-Análise 1.

Malware sensível a contexto.

```
if(strcmp(argv[0],MYNAME)!=0)
```

Anti-Análise 2.

Analise o binário

- Files/context2

Anti-Análise 2.

Malware sensível a contexto.

```
#define EXPECTED_PARENT "bash\n\x7f"
int parent = getppid();
sprintf(comm,"/proc/%d/comm",parent);
fread(buf,1,BUF_SIZE,f);
if(strcmp(buf,EXPECTED_PARENT)!=0)
```

Anti-Análise 3.

Analise o binário

- Files/disappear

Anti-Análise 3.

Remoção de evidência.

```
#define MYPATH "/proc/self/exe"
readlink(MYPATH, buf, BUF_SIZE);
remove(buf);
```

Anti-Análise 4.

Analise o binário

- Files/time

Anti-Análise 4.

Evasão por tempo.

```
sleep(100000000);
```

Anti-Análise 4.

Injeção de código

```
unsigned int sleep(unsigned int seconds){
        return 0;
}
```

LD_PRELOAD

```
LD_PRELOAD=./awake.so ./infinite
```

Injeção de código.

Hooking e funções trampolim.

- O que mais posso fazer ?

Rootkit

Fake readdir

```
struct dirent *readdir(DIR *dirp){
```

Calls original readdir

```
orig_readdir_type orig_readdir;
orig_readdir = (orig_readdir_type)dlsym(RTLD_NEXT,"
valueOfReturn = orig_readdir(dirp);
```

Ommits HIDDEN file

```
if(strcmp(HIDDEN, valueOfReturn->d_name) == 0){
   return NULL;
}
```

Rootkit `ls`

Antes

```
galante@galante-VirtualBox:~/Documents/secomp2018/Files/preload/rootkitls$ ls -l
ah
total 80K
drwxrwxr-x 2 galante galante 4,0K Ago  3 11:52 .
drwxrwxr-x 5 galante galante 4,0K Ago  2 23:00 ..
-rw-rw-r-- 1 galante galante   24 Jan 12  2018 benign
-rw-rw-r-- 1 galante galante  837 Ago  2 23:32 fake.c
-rwxrwxr-x 1 galante galante 8,0K Ago  3 11:52 fake.so
-rw-rw-r-- 1 galante galante  238 Ago  2 22:58 Makefile
-rw-rw-r-- 1 galante galante    9 Jan 12  2018 malware
-rw-rw-r-- 1 galante galante  45K Jan 12  2018 output.txt
```

Depois

```
galante@galante-VirtualBox:~/Documents/secomp2018/Files/preload/rootkitls$ make
runlah
LD_PRELOAD=./fake.so /bin/ls -lah
total 72K
drwxrwxr-x 2 galante galante 4,0K Ago  3 11:52 .
-rw-rw-r-- 1 galante galante   24 Jan 12  2018 benign
-rw-rw-r-- 1 galante galante  837 Ago  2 23:32 fake.c
-rwxrwxr-x 1 galante galante 8,0K Ago  3 11:52 fake.so
-rw-rw-r-- 1 galante galante  238 Ago  2 22:58 Makefile
-rw-rw-r-- 1 galante galante  45K Jan 12  2018 output.txt
```

Rootkit ps

Antes

```
11899 ?        00:00:03 atom
11911 ?        00:04:01 atom
11951 ?        00:00:00 atom
12294 ?        00:01:00 nautilus
15302 pts/17   00:00:00 bash
16733 ?        00:00:00 cupsd
17062 ?        00:00:00 polkitd
19611 pts/1    00:00:00 bash
20300 ?        00:13:30 Web Content
20637 ?        00:01:32 gnome-terminal-
22169 ?        00:00:00 dhclient
22770 pts/1    00:00:19 evince
22777 ?        00:00:00 evinced
23141 ?        00:00:03 notify-osd
```

Depois

```
 2732 ?        00:00:00 deja-dup-monito
 3914 ?        00:00:00 gvfsd-network
 3934 ?        00:00:00 gvfsd-dnssd
 4305 ?        00:00:00 gconfd-2
 9512 ?        00:00:27 Web Content
11869 ?        00:00:00 atom
16733 ?        00:00:00 cupsd
20300 ?        00:13:31 Web Content
20637 ?        00:01:33 gnome-terminal-
22169 ?        00:00:00 dhclient
22770 pts/1    00:00:19 evince
23141 ?        00:00:03 notify-osd
23306 ?        00:00:00 kworker/0:2
23356 ?        00:00:00 kworker/u4:1
```

Roteiro

Outros Comportamentos.

O que faz o binário ?

- Files/files1

Ransomware.

Como Reverter ?

- Files/files1

Ransomware.

Reversão da "encriptação"

- **Propriedade**: XOR(XOR(X,k),k) = X

Ransomware.

Como Reverter ?

- Files/files2

Roteiro

Java.

Analise a classe

- Files/java/

Java.

Analise da classe

- **Descompilação**: ./jad classe
- **Compilação**: javac classe
- **Execução**: java classe

Roteiro

Dúvidas, Críticas e Sugestões.

Contato

- **mfbotacin@inf.ufpr.br**
- **marcus@lasca.ic.unicamp.br**