QVidium Technologies, Inc.
Web: http://www.qvidium.com
E-mail: Sales@qvidium.com
Phone: +1 858-792-6407

Application Note:

Internet Security: Hacking and Intrusion Detection and Prevention

Overview

Attaching your QVidium encoder or decoder to the raw Internet is frought with dangers of unwanted intrusions and the possibility of your QVidium device being hijacked or infected and being used by rogue agents for sending out spam and other uses that would compromise your network, the integrity of your QVidium device, and the video you are trying to send and receive. For this reason, it is best to place your QVidium device behind a firewall.

However, since it is not always possible to deploy your QVidium encoder and decoder behind firewalls, we have included free whitelist-based firewall functionality to the QVidium firmware. We strongly recommend that you configure and enable this firewall. We cannot guarantee the operation nor integrity of your QVidium product without firewall protection.

This application note will help you determine whether your QVidium QVENC or QVDEC has been affected by unauthorized intruders, what to do if it has been compromised to disinfect and secure it, and how to configure the firewall feature to prevent hacking and intrusion problems in the future.

1. Determining whether your QVidium device has been hacked

Click on Network/Status. Scroll to the **Active Connections** section. You should see something like this:

```
Active Connections

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.20:80         192.168.1.90:62406      TIME_WAIT
tcp        0      0 192.168.1.20:80         192.168.1.90:62403      TIME_WAIT
tcp        0    226 192.168.1.20:80         192.168.1.90:62409      ESTABLISHED
udp        0      0 0.0.0.0:7               0.0.0.0:*
udp        0      0 0.0.0.0:997             0.0.0.0:*
```

Inspect the column labeled **Foreign Address**. If there are addresses you do not recognize, then intruders have broken into your system. You should follow the procedures below to secure and disinfect your system.

2. Securing your QVidium Device

NOTE: Go to http://www.qvidium.com/qvpro/Firewall/ to install the firewall feature if you do not see it in the menu before starting the following procedure.

Please follow the following procedure to secure your QVidium device:

1) Under **Management/Configure**, Select **Disable** for **Secure Shell Access**.

2) Click on **System/Reboot** to reboot

3) Under **Firewall/Config**, enter Whitelist addresses and check the box to the left of each address. Be certain to include the IP address of the encoder on the decoder and vice versa. Also, be certain to enter any public IP address of devices for which you wish to give access.

   NOTE: You can include a range of addresses using the notation AAA.BBB.CCC.DDD/XX, where XX is in the number of most-significant bits in the IP address that must match for access. For example, enter 67.32.45.138/29, if you wish to provide access to a range of 8 addresses (calculated as 2^(32-XX), where XX=29 in this example) starting at 136 (calculated by replacing the last XX-29 bits of the IP address with 0).

4) Once you are certain that you have entered all the relevant public IP addresses in the list, click on the **Firewall On** checkbox and then click on **Change Firewall Configuration**. Click on **Firewall/Status** to make certain you still have access after enabling the firewall. If you are locked out, you can still connect from a PC on the same LAN as the QVidium device. There is also a Firewall Reset procedure at http://www.qvidium.com/reset to turn off the firewall.

5) Reboot the unit again using **System/Reboot**, and check the Network/Status page after rebooting to verify that there are no unwanted IP addresses accessing your device.

3. Disinfecting your QVidium device.

At this point, your QVidium device should be secure from new intruders. However, it would be prudent to re-install all the software to erase any possible malware that may have been installed by a foreign hacker. Please follow the Reset Software instructions: "To completely update of all firmware..." at http://www.qvidium.com/reset/. Your encoder/decoder profiles and Ethernet settings should not be affected by this reset. However, to be safe, please first export and save any Profiles you want to keep safe.