Dear Valued partner,

It has come to our attention recently that a small amount of DVR's / NVR's supplied by Weston Distribution may have been infected with a version of the Mirai Botnet. This whilst not fatal to any equipment could potentially stop the recording / take the unit off line (internet based). To determine if your device has been infected "Hacked" will be shown across channel names 1-4.

To overcome this issue the following steps, need to be taken. A firmware patch is available from us to heighten the security settings on the devices, once the firmware has been installed a full factory reset must be done and finally a "STRONG" password must also be deployed on all devices.

The Mirai or versions of this botnet has so far infected over 1.4 million devices throughout Europe and the USA with the world largest CCTV manufacturers being hardest hit. It first came to light in 2015 and we then strengthened our security protocols on devices, but it has now evolved and a further update is necessary. Whilst we apologise for any inconvenience this may have caused we are seeing that all devices infected so far have been left with default username and passwords and the Mirai botnet (or variant) feeds on devices where security is low. Also, so far all the devices infected have been behind freely issued routers from ISP's that have low security on them, so far no device behind a professional firewall has been infected. Just resetting the device without the security patch will still allow the botnet to re-infect and the patch is necessary.

Please contact us on 0113 323 8572 and the correct version of firmware will be offered, please have to hand your model number of device that you are requesting firmware for. Even if your units have not been infected we strongly advise that firmware and strict security settings are checked to ensure future proofing.

We expect this botnet to re surface again in the future and urge all installers to check any equipment, whilst we strive to make sure security is at our forefront, unexpected or new botnets are always evolving and you can play your part by tightening your security protocols on all devices to stem the spread of such malware. Most IoT (internet of things) devices are subjected to attacks every single day and his will only get worse as more devices are connected / integrated into our lives. We will be running free to attend sessions on internet security (related to CCTV) with our valued distribution partners, to attend these sessions please contact your local dealer.

Weston Communications (Networks) Limited T/A Weston Distribution
Registered Office: Networks house, 2 Whitehall Industrial Estate, Whitehall Road, Leeds LS12 5JB
Tel: 0113 323 8572 Fax: 0113 3238574
Company Number: 3944371

Stats:

Analysis this week by Symantec concluded the average an IoT device is scanned every two minutes. This means that a vulnerable device, such as one with a default password, could be compromised within minutes of going online.

Analysis by Symantec of recent Mirai samples has found the malware is configured to use a list of at least 62 user name and password combinations, most of which are commonly used default credentials for IoT devices.

Q: What can I do to protect my devices and prevent them from becoming infected?

A: We have the following tips to protect any IoT device from becoming infected with malware.

- Perform an audit of IoT devices used on your / customers networks
- Change the default credentials on devices. Use strong and unique passwords for device accounts and Wi-Fi networks.
- Use a strong encryption method when setting up Wi-Fi network access or check your customers have done this. (WPA)
- Disable features and services that are not required
- Disable Universal Plug and Play (UPnP) on routers unless absolutely necessary, use proper port forwarding when possible, we can offer this service free of charge to aid installation.
- Modify the default privacy and security settings of IoT devices according to your requirements and security policy
- Disable or protect remote access to IoT devices when not needed
- Use wired connections instead of wireless where possible
- Regularly check our website for firmware updates
- Ensure that a hardware outage does not result in an unsecure state of the device

If you require more information please do not hesitate to contact one of our team we are glad to help.