Camera Cyber Lockdown

Technical White Paper

Overview

Eagle Eye Camera Cyber Lockdown is a cyber security feature that has been released as part of the Eagle Eye Security Camera VMS. Camera Cyber Lockdown blocks cameras from communicating with the Internet, blocks attacks from reaching the cameras, and will not allow any Trojans which may have been implanted in the cameras to communicate with the Internet. This feature greatly increases the cyber security of video surveillance systems and reduces the amount of cyber security maintenance required.

The overall effect of Eagle Eye Camera Cyber Lockdown is protection from cyber security breaches and reduction in cyber security issues generated by cameras. Performing firmware updates on cameras is normally crucial for cyber security, but since the cameras are locked down, these maintenance needs are reduced.

Surveillance cameras have a number of cyber security issues associated with them:

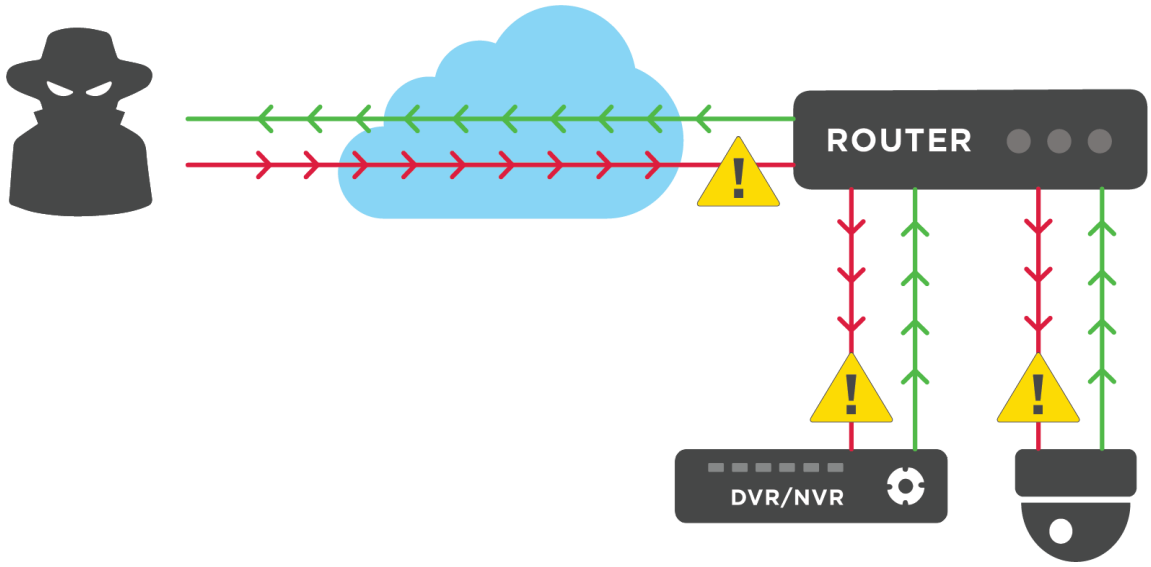
1. Cameras are manufactured by a large number of companies located all over the world. Many of these companies have unknown political and governmental influences.
2. Many cameras are manufactured by one company and labeled and sold by different companies. It is often difficult to know who and where cameras are manufactured. Tracing the true source of a camera can be difficult.
3. Many camera suppliers and manufacturers are lax on their cyber security and do not perform adequate testing or have the knowledge to make their cameras truly cyber secure. It's hard to know this when selecting cameras.
4. Many camera suppliers do not provide adequate firmware upgrades addressing cyber security flaws in a timely manner. Some do not provide any firmware upgrades at all.
5. Upgrading firmware on surveillance cameras when you have a large quantity of them can be extremely time consuming.
6. Many surveillance camera users do not have processes in place to perform camera firmware upgrades when cyber vulnerabilities are discovered. Most do not have a process in place to track cyber security vulnerabilities and then respond to them.

Given the variety of vendors involved, the lack of firmware upgrades, and the lack of attention to cyber security by some manufacturers, Eagle Eye Camera Cyber Lockdown solves a serious cyber security issue.

The Problem

Part 1: Internet Connections

Traditional DVRs provide little or no protection from cyber attacks. Very few have integrated firewalls. Very few have adequate cyber security testing. Very few have adequate firmware upgrades. Very few patch OS vulnerabilities as they are discovered. Very few provide firmware upgrades for security vulnerabilities. The root of the problem is that traditional DVRs require a connection directly FROM the Internet (see red lines in drawing below) to the DVR to view live or recorded video. This is how the video is transferred to the mobile device or the remote viewer. If the DVR does not have this connection video can only be viewed when on the premise and few customers are willing to accept only local viewing.



Because the DVR can be contacted directly from the Internet, the DVR can be easily attacked and exploited by cyber criminals and other attackers. Users will need constant vigilance to avoid being compromised. Anything connected to the Internet is typically attacked or probed over 100 times per day.

The cameras may be connected to the DVR/NVR or the router. If the cameras are connected to the router or a switch directly, they have the potential to be directly attacked. If they are

connected via the DVR, depending on the DVR, they may be attacked either directly or once the DVR is compromised.

Part 2: Trojans/Spyware/Virus Pre-Installed

There is a significant concern that cameras, DVRs, and NVRs may be provided by the manufacturer with spyware, trojans, or viruses already installed. This happens when the supplier sells a piece of hardware that is already compromised, whether it is intentional or accidental. There are many documented cases of this having occurred.

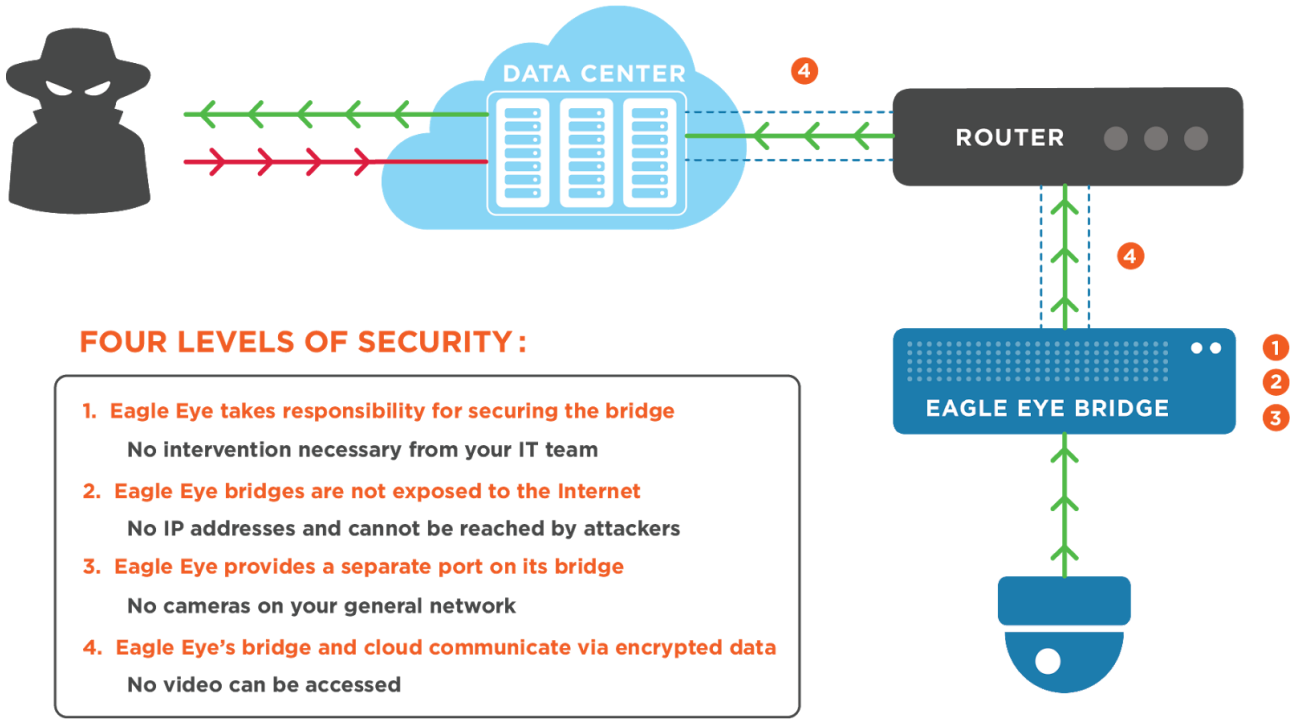
In this case, the camera is running software that will either immediately, or at some predetermined point in time, attempt to contact a "command and control server" (CCS) on the Internet for additional code and instructions. For example, the compromised camera could have a trojan that will attempt to contact its CCS on Jan 15, 2019. On that date, the camera will try and use the network connection to reach out and obtain instructions. Most networks allow outbound connections from any device. More sophisticated network configurations utilizing VLANS or firewalls will attempt to block outbound connections, but this is not the norm. In a normal network, the encrypted outbound connections to a CCS would be allowed. Files from your local network, video images, and passwords could easily be transferred out to the hackers by this camera. The camera could then receive instructions or additional programs to hack into other computers on your network, attack databases, transfer out credit card information, or take part in a denial of service (DDoS) attack. See the section on “Why They Are Attacking” below for more information.

The primary issue is that the camera, NVR, or DVR, may be provided by a manufacturer that is not taking responsibility for its cyber security. In the case of the trojan or pre-installed virus, the device simply needs ANY access to the Internet to be a serious threat.

Camera vulnerabilities include:

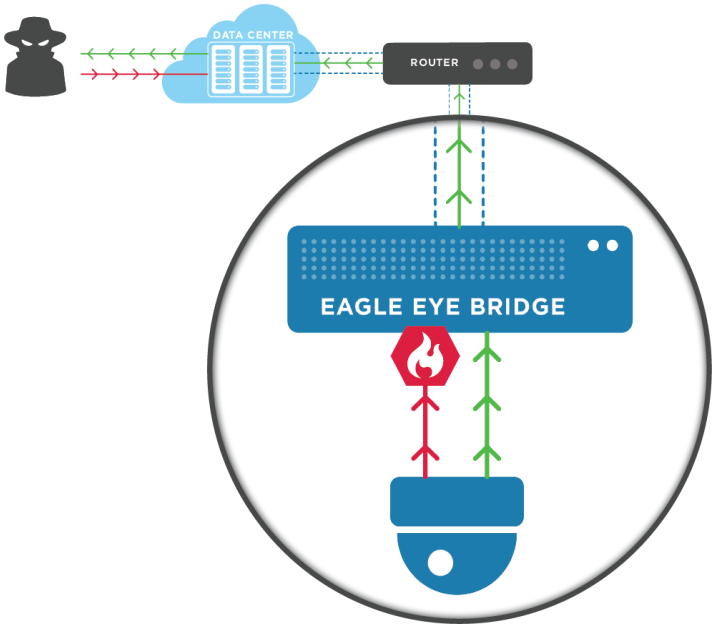
- Possible trojans from factories in a malevolent country
- Lack of attention and testing for cyber security by the manufacturer
- Possible backdoor accounts from the manufacturer either accidentally or on purpose
- Lack of firmware upgrades during operational life of the camera from the manufacturer
- Difficulty in applying firmware upgrades across all of the cameras
- High probability of misconfiguration by installers (typically passwords)

The Solution: Eagle Eye Camera Cyber Lockdown



Eagle Eye Networks takes multiple steps to ensure the cyber security of your Eagle Eye Security Camera VMS:

1. Eagle Eye takes responsibility for patching and securing the Eagle Eye Bridge which is located on the network and connects to the Internet. Eagle Eye patches this quickly and efficiently for any and all security issues.
2. Eagle Eye Bridges and CMVRs are not exposed directly to the Internet. They are not open to general attacks because they do not have any exposed IP Addresses and cannot be directly reached by attackers.
3. Eagle Eye provides a physically



separate port on the Eagle Eye Bridge to connect cameras. This means that the cameras are not on your general network and cannot be reached by employees or other people with access to the network. It also means that the cameras cannot be directly reached by hackers from the outside.

4. Eagle Eye use AES encryption to protect video data being communicated between the Bridge and the cloud to insure that a hacking effort never results in usable video.

With Camera Cyber Lockdown and use of Eagle Eye's dedicated CAMLAN the IP Cameras used in your surveillance system are far more secure and safe.

Why They are Attacking

The days of kids having fun by hacking are long gone. It is now big business that takes the form of selling stolen information, and holding websites hostage using compromised systems. These can be anything from public facing websites, gaming systems, e-Commerce sites, and in some cases even government systems.

Hackers are interested in hacking IP cameras for a few reasons:

1. To obtain confidential personal information such as credit card numbers, social security numbers and other personal identification information (PII)
2. To obtain confidential company-related information such as customer information, financial statements, etc.
3. To bring down a website or network via a distributed denial-of-service attack (DDoS) by utilizing numerous compromised devices (often distributed globally) in what is referred to as a botnet.

DDoS attacks are quickly becoming the most prevalent types of attacks, growing rapidly in the past year in both number and volume. IP cameras connected to Internet devices, such as DVRs and NVRs, are an ideal target. These vulnerabilities make for a highly insecure system that is simple to exploit. Between August and October of 2016, the Mirai malware was used in a number of DDoS attacks, which exploited a range of IoT devices, including security cameras[1]. Once a system becomes a DDoS pawn, and you're a member of a botnet, the attackers will eventually look for confidential information.

[1] https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

Conclusion

The market for surveillance cameras is very competitive and includes many suppliers from different countries. It is difficult to know the source of the camera and the level of attention the manufacturer has and will continue to give to cyber security. Low cost cameras are often preferred, but the vendors who provide them might cut corners on cyber security to deliver a product at a lower price point.

There are many ways to turn your camera into a weapon, a doorway into internal networks, or a hackers paradise if the camera can be accessed via the Internet.

Yes, it is possible to securely configure and maintain your network, but in our experience keeping a network of 20 cameras secure using traditional methods will take an average of 25 hours per year. In addition, the initial setup and configuration will take at least 8 hours.

Eagle Eye Camera Cyber Lockdown eliminates nearly all ways for the camera to be contacted via the Internet or to contact the Internet -- making the surveillance system far more cyber secure.