Camera Cyber Lockdown

March 2017

Eagle Eye Networks, Inc. | 4611 Bee Caves Rd, #200 | Austin, TX 78746
www.EagleEyeNetworks.com | +1-512-473-0500 | sales@EagleEyeNetworks.com

Overview

Eagle Eye Camera Cyber Lockdown is a set of cyber security features that has been released as part of the Eagle Eye Cloud Security Camera Video Management System (VMS). The purpose of Eagle Eye Camera Cyber Lockdown is to significantly reduce or eliminate the impact of camera cyber security issues.

Protecting network video surveillance cameras is important because many cameras have multiple cyber security issues:

1. Cameras are manufactured by many companies located all over the world. Many of these companies have unknown political and governmental affiliations.
2. Many cameras are manufactured by one company, then labeled and sold by different companies. It can be difficult to determine the manufacturer and country of origin.
3. Many camera suppliers and manufacturers are lax on cyber security—they do not perform adequate testing of their cameras, and do not have the knowledge required to make their cameras truly cyber secure. It is hard to determine camera cyber security profiles when selecting cameras.
4. Manufacturers may have accidentally or on-purpose included secret “backdoor” access to cameras.
5. Many camera manufacturers do not address discoveries of camera cyber security flaws in a timely manner, by providing firmware upgrades addressing the security problems. Some do not provide firmware upgrades at all.
6. Often the published factory default passwords are not changed when cameras are installed, or easily-guessed passwords are used, leaving cameras wide open to individual hacker intrusions and automated network-based attacks.
7. Passwords are often transmitted in plain text and thus are discoverable.
8. Upgrading firmware on a large quantity of surveillance cameras is generally labor-intensive and costly.
9. Many surveillance camera customers (end users) do not have processes in place to monitor the discovery of camera cyber vulnerabilities and to perform camera firmware upgrades when they are released. Their cameras remain vulnerable.

The Problem

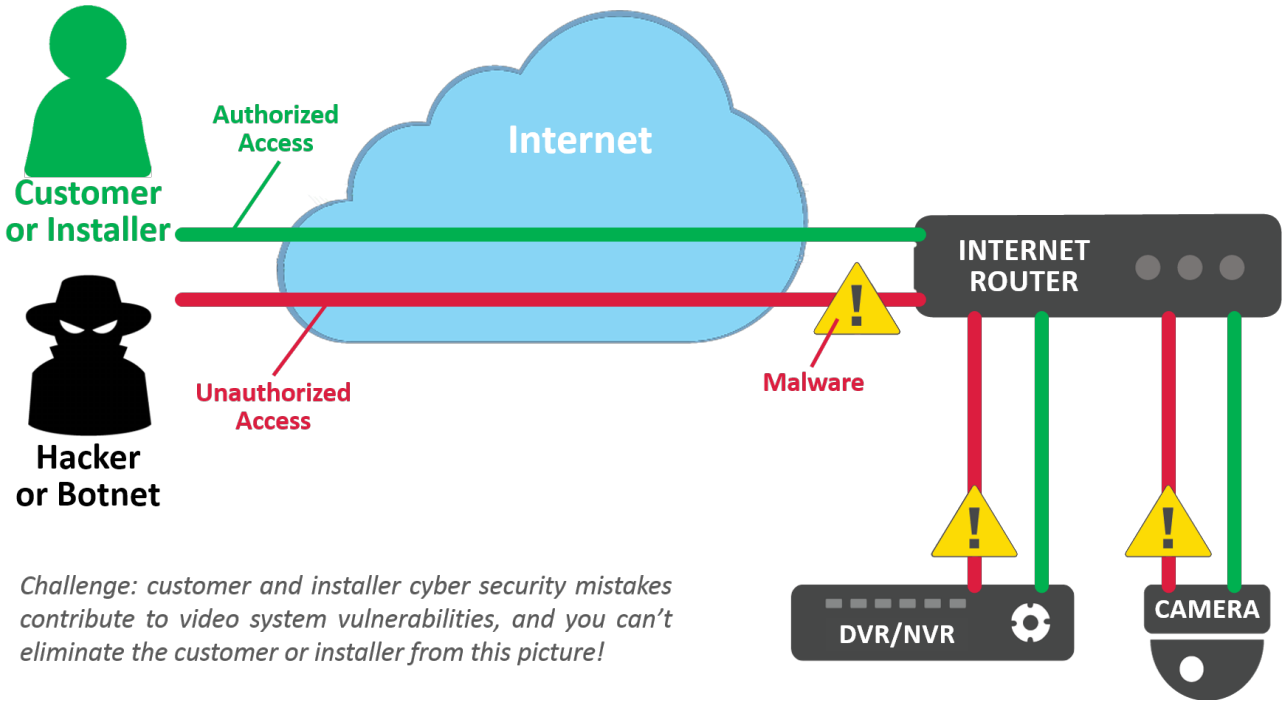
Part 1: Internet Connections

A “bot”, short for robot, is a software program that performs automated tasks. A botnet is a network of computers, each of which is running one or more bots. Hackers have coopted the term “botnet” to refer to a network of internet-connected devices, including PCs, servers, mobile devices and internet-of-things devices, that are infected and controlled by a common type of malware, with the device owners usually unaware of the malware infection. Internet-connected security video cameras and recorders have become a favored target for hacker botnet infections.

In September and October of 2016, the two largest global botnets attacks to date were launched using several hundred thousand infected cameras, digital video recorders (DVRs) and network video recorders (NVRs). Researchers have reported that in 2016 about one million web-connected video cameras and DVRs were infected by malware, with most of the camera and DVR owners unaware that their devices are infected.

The root of the problem is the desire of individuals and businesses to remotely view security video using a desktop or laptop computer, tablet, or smartphone. Traditional DVRs and NVRs require a connection FROM the Internet to the recorders (see the red lines in **Figure 1** below). If the recorder does not have an Internet connection, video can only be viewed at the recorder's location, and few customers are willing to accept a restriction to local viewing only.

Figure 1. Security cameras and traditional DVR and NVR recorders are vulnerable to cyber attack.



Cameras, DVRs and NVRs have little to no protection from cyber attacks, very few have built-in firewalls. Most have not undergone adequate cyber security testing by their manufacturers or installers. Most have major password vulnerabilities. Few receive adequate firmware upgrades to fix security vulnerabilities, or have their operating system (OS) vulnerabilities patched as updates are released.

In July 2017, cyber security researchers discovered a serious flaw, which they named "Devil's Ivy", that exists in nearly all cameras supporting the popular ONVIF specification. The flaw allows hackers to take full control of ONVIF-compliant cameras. Most camera makes and models are vulnerable, including top brand high-quality cameras. Within days a few major manufacturers issued firmware updates that correct the flaw. It is up to camera owners and servicing contractors to update the cameras. There is no telling which manufacturers will make firmware corrections for their cameras, or how many of the millions of vulnerable installed cameras will actually be updated.

When vulnerable cameras and recorders can be contacted directly from the Internet, they can be easily attacked and exploited by cyber criminals and other attackers. Strong cyber security controls and constant vigilance are needed to avoid recorders being compromised. Any device connected to the Internet is typically attacked or probed hundreds of times per day, especially DVRs and NVRs, as they are a high-value target.

Part 2: Trojans, Spyware, & Pre-Installed Viruses

There is a significant concern that cameras, DVRs, and NVRs may be provided by the manufacturer or the installer with spyware, Trojans, or viruses already installed. There are many documented cases of this having occurred.

When that occurs, the device is running software that will either immediately, or at some predetermined future point in time, attempt to contact a "command and control server" (CCS) on the Internet to retrieve additional software code and instructions. For example, a compromised camera could have a Trojan that will attempt to contact its CCS on January 15, 2019. On that date, the camera will use the Internet connection to obtain instructions from the server.

Most networks allow outbound connections from any device on the network. More sophisticated network configurations utilizing VLANS or firewalls will attempt to block outbound connections, but this is not the norm. In a typical network, encrypted outbound connections to a CCS would be allowed. Files from computers on a local network, video images, and passwords could easily be transferred out to hackers by an infected camera. The camera could then receive instructions and additional software to execute, to hack into other computers on the network, attack databases, transfer out credit card information, or take part in a denial of service (DDoS) attack.

In the case of the Trojan or pre-installed virus on a camera, NVR, or DVR, the infected device simply needs ANY access to the Internet to become part of a botnet and pose a serious threat to the systems the controlling hacker has targeted.

Why Hackers Attack

The days of kids hacking websites just for fun are long gone. Hacking is now a big business that steals information to sell it, and uses encryption to hold websites hostage for ransom. These websites can be of any type, including public-facing websites, gaming systems, e-Commerce sites, and in some cases even government systems.

Key hacker objectives include:

1. Obtain confidential personal information such as credit card numbers, social security numbers and other personal identifiable information (PII).
2. Obtain confidential company-related information such as customer information, financial statements, etc.
3. Bring down a website or network via a distributed denial-of-service attack (DDoS) by utilizing a botnet of tens or hundreds of thousands of compromised devices (often distributed globally).

DDoS attacks have become the most prevalent type of attack, growing rapidly in the past year in both number and volume. Network cameras, DVRs and NVRs are an ideal target. Their vulnerabilities make for a highly insecure system that is simple to exploit.

The Solution: Eagle Eye Camera Cyber Lockdown

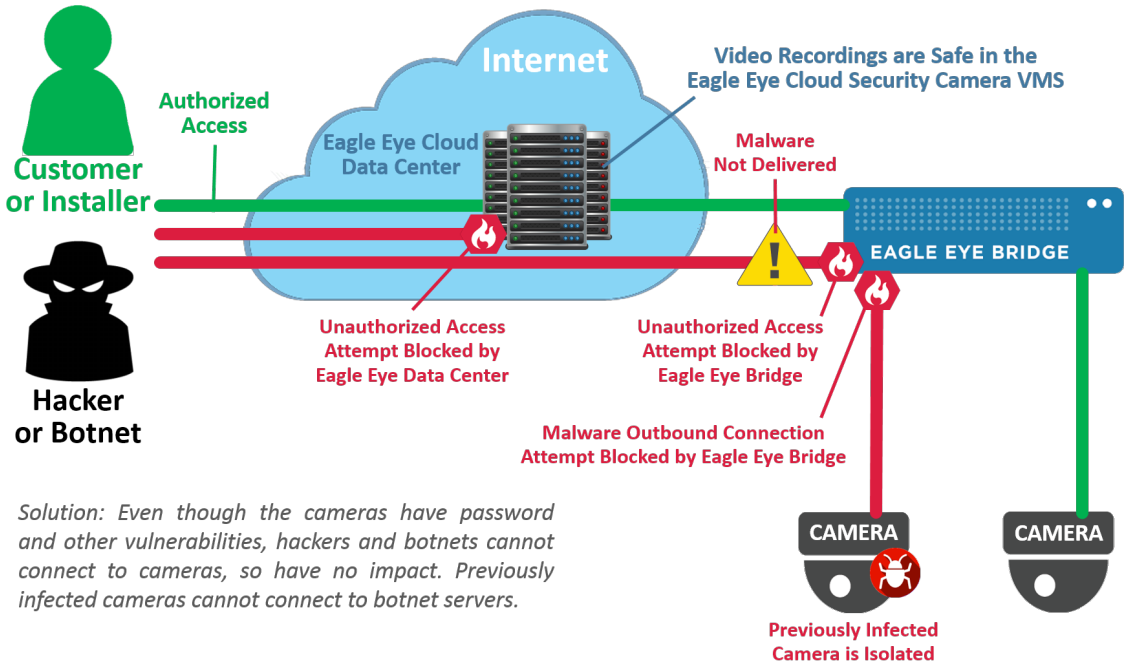
The Eagle Eye Cloud Security Camera VMS is a cyber-secure cloud-based system that replaces traditional DVRs and NVRs with:

- **Eagle Eye video appliances:** *Bridges*, for receiving and buffering video, audio, alarm and event data from cameras and video encoders, and sending it to the Eagle Eye Cloud Data Center, and *Cloud-Managed Video Recorders* (CMVRs), which perform all the Bridge functions plus store video locally. The required networking, routing and firewall functionality is built into the appliances to ensure the integrity of the on-premise portion of the system. Third-party network routers, firewalls and switches are not needed.
- **Eagle Eye Cloud Security Camera Video Management System (VMS):** The *Cloud Security Camera VMS* is designed and built as a modern redundant cloud architecture that provides a web browser-based interface and comprehensive mobile applications for iOS and Android smartphone and tablet devices. It is provided as a managed service, including automatic security and feature updates for the Eagle Eye video appliances.

Secure Encrypted Connections

Eagle Eye appliances do not accept inbound connections; thus, hackers and botnets are not able to access the appliances or the cameras connected to them. All connection attempts are blocked, as shown in **Figure 2**.

Figure 2. Eagle Eye Camera Cyber Lockdown protects cameras from cyber threats.



The firewall functionality in the Eagle Eye appliances blocks any outgoing connection attempts from cameras. Thus, if a camera is infected with malware and tries to connect to a command and control server on the Internet, that connection attempt is blocked.

The only connection the appliances make is an outbound connection to the Eagle Eye Cloud Security Camera VMS. That connection is authenticated using digital certificates, and is encrypted using Transport Layer Security (TLS) version 1.1 or higher, using the SHA-256 secure hash algorithm with a 2048-bit RSA encryption key.

Strong User Two-Factor Authentication

Two Factor Authentication is used to provide strong security by establishing trusted user devices (PCs, laptops, tablets and smartphones) and only allowing users to access cameras and video from those trusted devices. Attempts to sign in using a non-trusted device result in access being denied.
Two-factor authentication utilizes the following mechanisms:

- **Trusted Device.** A trusted device is a mobile device or a browser on a specific computer that has previously registered using two-factor authentication ice that is known to be associated with that Eagle Eye User.
- **Security Code.** A security code is a one-time-use code sent to a trusted device or phone number when the user logs in for the first time using a new device or browser.

Camera and Data Isolation

Cameras are never directly connected to the internet. Eagle Eye Bridge appliances aggregate and buffer the video data for secure encrypted transmission to the Eagle Eye Networks Cloud Data Center. For local recording, Eagle Eye CMVRs continue to ensure that cameras have no direct link to the Internet. Both the Eagle Eye Bridge and the CMVR provide a physically separate network port for cameras, so that cameras are not directly connected to the general business network or the Internet.

Simple Secure Deployment

Securely deploying Eagle Eye appliances is simple because they are all designed as “locked down” devices, have no open ports, accept no inbound communications, and are pre-configured to automatically authenticate and connect to the Eagle Eye Cloud Security Camera VMS. No configuration is required to establish network connections. Cameras are auto-discovered, and must be manually approved before they are enrolled in the system. Bridges and CMVRs act as DHCP servers for network cameras, so that it is not necessary to manually set camera IP addresses.

Assuring Cyber Security Protection

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

1. The Eagle Eye Cloud Security Camera VMS performs security and feature updates automatically for Eagle Eye video appliances, with no installer or end user action required.
2. Eagle Eye provides a physically separate port for cameras on the Eagle Eye video appliances (Bridges and CVMRs), thus the cameras do not reside on the general business network and cannot be reached by employees or other personnel with access to the network. It also means that cameras cannot be directly reached by hackers from the outside.
3. Eagle Eye uses 256-bit AES encryption for video data stored on Bridges and CMVRs, as well as in the Eagle Eye Cloud Data Center.
4. Eagle Eye use TLS version 1.1 or higher to protect video data being communicated between Eagle Eye video appliances and the Cloud Security Camera VMS to ensure the confidentiality and integrity of video data.
5. Eagle Eye video appliances use digital certificates to authenticate themselves to the Eagle Eye Cloud Security Camera VMS.
6. Eagle Eye video appliances do not accept any inbound connections, have no open network ports, and automatically self-configure their connections to the Eagle Eye Cloud Security Camera VMS.
7. Eagle Eye video appliances auto-discover cameras, which must be manually approved before they are enrolled in the system.

With Camera Cyber Lockdown the cameras in your surveillance system are far more secure and safe.

Conclusion

The market for surveillance cameras is very competitive and includes many suppliers from different countries. It is difficult to determine the source of many camera makes and models, and to discover the level of attention their manufacturers have given—and will continue to give—to camera cyber security.

Customers often prefer low-cost cameras, but the vendors who provide them typically do not have the technical knowledge or skills to deploy a cyber-secure video management system. Camera security is especially difficult for low-cost cameras, because they have the greatest number of cyber security vulnerabilities.

While it is technically possible to install and configure a cyber-secure video surveillance system, it does require that the selected video management system has features that allow it to be securely configured. For most brands of video management systems and video cameras, it also requires a high degree of cyber security expertise, due to ever-increasing cyber threats and the cyber vulnerabilities of most security video cameras.

Fortunately, thanks to its Camera Cyber Lockdown features, the Eagle Eye Cloud Security Camera VMS provides a cost-effective way to effectively address the cyber security vulnerabilities of Internet-connected security camera systems.

About Eagle Eye Networks

Founded in 2012, Eagle Eye Networks, Inc., (‘Eagle Eye’) is the leading global provider of cloud-based video surveillance solutions addressing the needs of businesses, alarm companies, security integrators, and individuals. Eagle Eye's 100% cloud managed solutions provides cloud and on-premise recording, bank level security and encryption, and broad analog and digital camera support - all accessed via the web or mobile applications. Businesses of all sizes and types utilize Eagle Eye solutions for operational optimization and security. All Eagle Eye products benefit from Eagle Eye’s developer friendly RESTful API platform and Big Data Video Framework ™, which allow for indexing, search, retrieval, and analysis of live and archived video. Eagle Eye's open Video API has been widely adopted for integration in alarm monitoring, third party analytics, security dashboards, and point of sale system integrations.

Eagle Eye sells its products through authorized global resellers and installation partners. Headquartered in Austin, Texas, USA, Eagle Eye has offices in Europe and Asia.

About Dean Drako

Founded by Dean, Eagle Eye Networks is the first cloud-based video surveillance company to provide both cloud and on-premise recording.

Dean has led, and continues to lead, remarkable security related firms throughout his impressive career. Concurrently with Eagle Eye Networks, Dean is the owner and Chairman of Brivo, a cloud access control company. Previously, as founder, president and CEO of Barracuda Networks, Dean created the industry’s first email security appliance. Prior to Barracuda Networks, Dean founded Boldfish, a leading provider of enterprise outbound email solutions that was acquired by Siebel Systems in 2003. Dean was founder, President and CEO of Design Acceleration, Inc. (DAI), a maker of superior design analysis and verification tools, which was acquired by Cadence Design Systems in 1998.

Dean was founder, Dean received his BSEE from the University of Michigan, Ann Arbor and MSEE from the University of California, Berkeley.

Goldman Sachs named Dean as one of the “100 Most Intriguing Entrepreneurs of 2014.”

Headquarters

Eagle Eye Networks
4611 Bee Caves Rd.
Suite 200
Austin, TX 7874
Tel: +1-512-473-0500
Web: www.EagleEyeNetworks.com
Sales: sales@EagleEyeNetworks.com

EMEA Office

Eagle Eye Networks B.V.
Hogehilweg 19
1101 CB
Amsterdam
The Netherlands
Tel: +31 (0) 88 00 68 450
Sales: EMEAsales@EagleEyeNetworks.com