Arecont Vision®

Leading the Way in Megapixel Video™

ARECONT VISION TECHNICAL UPDATE

Issued 21 November 2016

Number: TU-11/21/16 Cybersecurity

Cybersecurity Attacks and Arecont Vision

On October 21, 2016, a major Distributed Denial of Service (DDoS) attack was launched on New Hampshire-based Dyn, a network monitoring and DNS routing company. The cyberattack heavily impacted up to 85 web services, including Amazon, the Financial Times, Netflix, PayPal, Reddit, Spotify, and Twitter. Users across the United States and Europe were unable to access these web services during this cyberattack and it was later reported that the eleven-hour incident resulted in an estimated $100M loss in revenue.

A wide variety of Internet connected devices, including surveillance cameras, web cams, DVRs, and many other IoT (Internet of Things) connected devices such as home appliances and thermostats, may have been used as "bots" or robotic attackers in the October attack. The devices were taken over by hackers and used to launch repeated DDoS waves of cyberattacks.

Due to the severity of the cyberattack, both the FBI and Homeland Security became involved in the investigation. Frustrated social media users and worldwide news agencies alike reported concerns and outrage over the incident: see https://goo.gl/mtyrp8.

Unfortunately, the October 21st attack is not an isolated incident. Verisign, a Virginia-based network infrastructure and security company, reports that the frequency of cyberattacks is increasing by 75% year over year: see https://goo.gl/tHVZKR. Another major DDoS attack had already occurred in September 2016 -- a month prior to the one involving Dyn -- targeting Krebsecurity.com and French hosting firm OHV. This cyberattack involved over 140,000 network cameras and DVRs: see https://goo.gl/Df4Mkr.

We are proud to state that **Arecont Vision megapixel cameras were not used in any of these cyberattacks.**

At the core of each Arecont Vision camera is our custom-designed FPGA (field programmable gate array) integrated circuit on which we run our proprietary firmware. We do not use Linux, which is an operating system often found in network cameras, computers, DVRs, and many other electronic devices. Linux has security vulnerabilities that can be used to gain root access, making cyberattacks much easier.

For example, when a hacker accesses an Internet connected device running the Linux operating system, the attacker can load and run a bot shell script. This script can then be used to launch various cyberattacks on other networked devices.

Arecont Vision megapixel cameras do not have these vulnerabilities. Should a hacker gain access to an Arecont Vision camera or obtain the user ID and 16-digit ASCII password to log into a camera, anything they do would solely impact that particular device. A hacker would not be able to remotely repurpose an Arecont Vision camera into a bot for the types of DDoS attacks mentioned earlier.

The choice is simple: if a customer wants to ensure cybersecurity protection, Arecont Vision cameras should be their first choice.