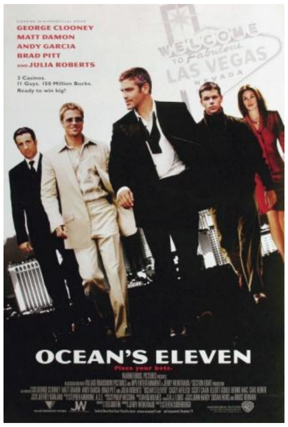
Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=surveillance-cameras-always-keep-company-safer-youll-surprised

Do Surveillance Cameras Always Keep Your Company Safer? You'll Be Surprised

Posted February 20, 2015

You probably remember the 2001 blockbuster remake of *Ocean's Eleven* starring George Clooney and Brad Pitt. While George and Brad's grand scheme—robbing a secret multi-casino vault underneath the Las Vegas Strip—may have been pure Hollywood, a key element of the plot is actually quite realistic, if not frighteningly simple: commandeering live surveillance video feeds, anywhere from ultra-secure government facilities to your company's server room.



We learned the true scope of this problem from cyber-vulnerability analyst (and former NSA specialist) Craig Heffner's highly informative presentation at the annual Black Hat security conference in 2013, which is posted on YouTube here.

We don't expect you to sit through the entire 30-minute video (it gets pretty technical pretty quickly), but Heffner reports how he examined the wide range of embedded surveillance cameras on the market today, from standard off-the-shelf products by trusted name brands (typically under $1,000 per unit) to top-end, "contact-us-for-pricing" equipment relied upon by schools, hotels, casinos, prisons, and many other high-security applications—including essential enterprise IT facilities.

While most vendors focus on the hardware quality of their cameras, they allow a surprising number of vulnerabilities on the backend… the kind of vulnerabilities a moderately skilled hacker can easily exploit.

The Achilles Heel: Unsecure Firmware

Almost all embedded surveillance cameras operate using web-based firmware provided by their manufacturer. Heffner points out that most vendors structure their firmware code in a similar fashion—while hardly updating it for newer model cameras. By simply *substituting a few characters on a single line of code*, he demonstrates how shockingly easy it is to hack into a camera's web server and view its existing factory default password—which most users never get around to changing—and gain full access to that server's admin interface.

Once inside admin mode, that hacker can do any of the following:

- Eavesdrop on your live video feed
- Freeze or loop that feed to mask any intruders (as the *Ocean's Eleven* gang did)
- Remotely reboot the system to gain full "root access"—literally the backdoor key to your entire IT network

George and Brad won't be tunneling into your secret vault anytime soon, but a hacker can unleash havoc throughout your entire company.

Try Before You Buy?

As we said, Heffner's full presentation is code-heavy and may be difficult to follow, but do scroll ahead to the last three minutes. Before choosing a new camera, he recommends doing your homework: investigate that model's existing online firmware for any glaring security bugs. A knowledgeable cyber-security expert will know how to download that code and literally "think like a hacker" to keep you as safe as possible from these types of attacks.