证券代码：002415　　证券简称：海康威视　　公告编号：2015-025 号

杭州海康威视数字技术股份有限公司

关于部分监控设备遭到网络攻击的后续说明

本公司及全体董事、监事、高级管理人员保证公告内容真实、准确和完整，没有虚假记载、误导性陈述或者重大遗漏。

2015 年 3 月 30 日，杭州海康威视数字技术股份有限公司（以下简称“海康威视”或者“公司”）收到国家计算机网络应急技术处理协调中心《关于近期部分互联网设备被入侵控制情况的调查说明》，现公告如下：

国家计算机网络应急技术处理协调中心依据《木马和僵尸网络监测与处置机制》文件（工信部保[2009]157 号）的工作要求，对 Backdoor.Linux.Gafgyt 恶意代码（该恶意代码可感染嵌入式设备）在我国境内的感染情况进行了监测和分析。经分析，我国境内互联网上感染该恶意代码的活跃被控 IP 地址中部分可确认为视频监控类智能设备的联网 IP，涉及包括海康威视在内的至少 5 家国内知名视频监控类设备生产企业。

上述“Backdoor.Linux.Gafgyt 恶意代码”，就是海康威视 3 月 1 日晚间发布的《关于部分监控设备遭到网络攻击的情况说明》（公告编号：2015-008）中所述网络攻击的源头。公司积极配合国家计算机网络应急技术处理协调中心识别受感染的海康威视设备，根据监测，3 月 1 日以来新发现的感染设备数量极小。公司已经基本完成受感染设备的修复和潜在风险设备的加固。

公司高度重视产品和系统的安全性能提升，已于 2014 年 3 月成立海康威视安全响应中心（Hikvision Security Response Center），目前已完成和正在推动的工作主要包括：

1、通过聘请专业信息安全顾问，组建专业团队，促进产品及系统安全的持

续改进。

2、持续加大互联网应用安全投入。针对互联网视频监控应用特点，专门构建萤石云系统，为小微企业、家庭和个人用户提供安全可靠的互联网视频应用服务。

3、继续加强与行业主管部门的联系，在视频监控系统前端安全、网络安全、主机安全、应用安全、运维安全等方面，提供全方位建议，规避和降低视频监控系统安全风险。

4、将联合政府相关部门以及业内领先的安全公司，成立“嵌入式设备网络安全联合实验室”，专注于视频监控产品及系统的安全提升。

风险提示：

随着互联网应用的普及，由恶意网络攻击引发的网络安全问题日益严峻，所有互联网从业企业都将面临极大挑战。尽管公司已投入资源提升产品或系统的安全性能，但仍可能存在第三方（包括计算机病毒、恶意软件、黑客攻击等）刻意尝试破坏公司产品或系统，此类破坏未必能够被提前发现、阻止，故公司可能遭受攻击导致产品或系统被侵入、破坏等风险。请广大投资者注意风险，谨慎投资。

特此公告。

杭州海康威视数字技术股份有限公司

董 事 会

2015 年 3 月 31 日