

黑客首次启动“僵尸物联网”攻击

美国超过1200家网站“中招”

“帮凶”可能是家里的录像机、摄像头、温控器,甚至智能烤箱

新华社北京10月24日电(记者彭嵩)恐怕很多人难以料到,家里安装的网络摄像头或是联网的智能冰箱不仅会被黑客轻易控制,还可能成为他们发动网络攻击的新一代“武器”。

近日造成美国上千家大网站集体“掉线”的大规模DDOS攻击的源头,正是中了木马病毒的智能家居产品所组成的“僵尸物联网”。成千上万的物联网设备发送大量通信请求,使域名服务器瘫痪。这可能是首次借助物联网设备发动的大规模网络攻击。

遭受攻击的美国网络服务提供商迪恩公司的首席战略官凯尔·约克对媒体表示,很多看似无害的物联网设备正成为大范围黑客袭击的“帮凶”,它们可能是家里的录像机、摄像头、温控器,甚至智能烤箱。

其实,早在2013年专家就已指出智能家居、可穿戴器件等物联网设备的安全漏洞。《福布斯》杂志记者克什米尔·希尔曾通过网络远程打开了陌生人家的电灯、电视和其他智能设备。而惠普公司2015年的调研报告显示,10种物联网硬件中有6种存在网络安全隐患。



目前全球物联网安全状况非常令人担忧,全世界有数以百万计的联网摄像头,相当高比例的摄像头存在弱口令等很多安全问题。 新华社发

什么样的攻击让美国上千网站“沦陷”

新华社北京10月24日电(记者张莹)当地时间本月21日早晨,美国东海岸地区网民一觉醒来后发现,许多常用网站如网上支付系统贝宝、社交媒体网站推特、美版大众点评Yelp、在线视频网站奈飞以及美国有线电视新闻网等主流媒体网站突然全部无法登录。

这是美国境内遭受的最新一次网络攻击,超过1200家网站“中招”。

为上述网站提供网络域名服务的美国迪恩公司随后在官网发布消息说,该公司的域名服务器遭受三波“分布式拒绝服务”(DDOS)攻击。第一波始于美国东部时间21

日7时10分,受影响的主要是东海岸网民,约两个小时后服务恢复正常。第二波始于美国东部时间21日11时50分,受影响范围“更加全球化”,不局限于美国东海岸,1个多小时后服务恢复。此后,黑客又试图发起第三波攻击,但公司迅速采取遏制措施,使第三波攻击没有造成太大影响。

那么DDOS攻击是怎样发生的?为何这次攻击会造成大量主流网站同时瘫痪?

DDOS是目前较常见的黑客攻击手法,其特点是通过大量种植了木马的“傀儡机”(也被称为“肉鸡”)发送通信请求来占用网

络资源,最终使网络过载、服务器瘫痪。

位于美国新罕布什尔州曼彻斯特市的迪恩公司是美国DNS(域名系统)服务提供商。DNS可以看做互联网“交通管理中心”,作用是将数字组成的IP地址转换成人们容易记住的域名。用户在网络浏览器输入网址后,通过DNS的地址解析服务,就可以前往要访问的页面。一旦DNS服务器遭到攻击而瘫痪,地址解析无法完成,“交通管理”失灵,大量网站就无法访问了。

迪恩公司首席战略官凯尔·约克22日在公司官网发文说,公司正在对这次攻击的来源和性质进行调

查,目前已知这是一次精心策划的攻击,攻击的一个重要来源是感染了“未来”(Mirai)病毒程序的僵尸网络,该网络涉及了数以千万的IP地址。

“未来”病毒是一种以感染物联网设备方式发起DDOS攻击的恶意软件,它可以高效扫描物联网系统设备,感染采用出厂密码设置或弱密码加密的脆弱物联网设备。

网络安全专家认为,此次网络攻击使物联网安全问题再次浮出水面,而以“未来”病毒组织的僵尸网络已逐渐发展为DDOS网络攻击的主力。

美国网络安全技术供应商赛门

铁克今年9月曾发布报告说,随着物联网发展,利用路由器、调制解调器、网络连接或存储设备、闭路电视系统和工业控制系统等物联网设备作为“傀儡机”发动DDOS攻击越来越普遍。这些设备可以通过互联网访问,但由于硬件和软件的局限性,安全等级较低。

美国网络安全公司Imperva近日发布报告称,全球范围内受“未来”病毒感染物联网设备IP数量超过60万,遍布160多个国家。市场研究机构加特纳预计,到2020年全球物联网设备将从目前的60亿台增至200亿台,届时可能出现更多这类攻击。

对国家基础设施的危害会更大

目前联网摄像头存在弱口令等很多安全问题

“目前全球物联网安全状况非常令人担忧,大量物联网设备接入、暴露在互联网上,很多物理设备存在弱口令、缓冲器溢出等安全漏洞,极易被攻击,并作为攻击其他设备或系统的平台,”中科院信息工程研究所物联网信息安全技术北京市重点实验室主任孙利民接受新华社记者采访时说,“特别是目前全世界有数以百万计的联网摄像头,相当高比例的摄像头存在弱口令等很多安全问题。”

他们分析发现,一些存在安全漏洞的摄像头不仅能被操纵窥探用户的个人空间,还可能被黑客当做袭击其他目标的攻击平台。

为何网络黑客会选择物联网设备作案?原因就在于,这些设备常常缺乏基本的杀毒软件、反垃圾邮件软件等防护工具以及安全监控、警报手段,用户本身的安全意识也比较单薄,只知道给传统计算机加装安全防护,并未意识到新兴的智能硬件会

威胁自身信息安全,甚至互联网等基础设施。

孙利民认为,此次美国遭受大规模黑客袭击会让全世界对物联网安全的重要性认知上一个层次。网络摄像头等物联网设备已广泛应用在智慧城市、基础设施建设中,水利、能源、电力、交通等领域的物联网设备安全一旦被破坏,对国家基础设施的危害会更大。

记者彭茜新(新华社北京10月24日电)

专家:物联网如何做好防护

那么,面对日益严重的物联网安全隐患,人们该如何防护?

专家指出,首先,物联网智能设备厂商应从研发阶段就加强产品安全测试,预先根据物联网设备的特点和黑客可能的攻击点,从网络协议、加密算法、应用系统等方面提高产品整体安全性。孙利民说,从国家角度看,还应结合不同行业和类型的物联网设备,出台更细化的行业安全标准。

其次,有条件的用户要对现有物联网设备进行安全评估,查出有哪些安全漏洞,并配备相应防护手

段。孙利民认为,用户单位要加强物联网设备在使用过程中的监管,对发现流量异常、非法操作、异常行为等及时告警,同时配备防护设备及时切断非法操作。

美国加利福尼亚大学圣迭戈分校超级计算机中心网络安全专家金伯利·克拉非说,总体来看,目前尚无有效手段帮助用户及时发现自己的物联网设备是否被黑客攻击,因此互联网服务提供商也应提升安全监控力度。

记者彭茜新(据新华社北京10月24日电)

我国血脂异常患者约4.3亿人

冠心病死亡率以每十年30%的增幅上升

新华社北京10月24日电(记者毛伟豪)国家心血管病中心24日在京发布《中国成人血脂异常防治指南(2016年修订版)》,从生活方式干预、控制危险因素和规范诊疗入手,指导医护人员和公众提高对血脂异常防治的知晓率、治疗率和控制水平。据测算,2012年我国血脂异常患者约4.3亿人,冠心病死亡率以每十年30%的增幅上升。

依据国人长期队列研究流行病学数据和临床循证研究进展,新修订的指南对人群的心血管病危险分层做了重大更新,对缺血性心血管病极高危人群提出更严格的控制目标。指南坚持以预防为主、防治结合的方针,提出通过定时血脂检测,早期发现高胆固醇患者,从生活方式干预、控制危险因素和规范诊疗入手,努力提高人群血脂异常防治的知晓率、治疗率和控制率水平。

定期检查血脂是防治心血管病的重要措施。指南建议20岁至40岁成年人至少每5年测量一次血脂,40岁以上男性和绝经后女性每年检测血脂,动脉粥样硬化性血管病患者及其高危人群每3至6个月检测血脂。

采取健康生活方式是防治血脂异常和动脉粥样硬化性血管疾病的基本策略。指南提出良好的生活方式包括坚持心脏健康饮食、规律运动、远离烟草和保持理想体重,建议血脂正常者每日饮食应包含25至40克以谷类、薯类为主的膳食纤维,摄入胆固醇应小于300mg。

《中国居民营养与慢性病调查报告》显示,2012年我国成人血脂异常患病率达40.4%,较2002年的患病率水平出现大幅度增加,呈现为国民血脂异常的普遍暴露状态,且成人血脂异常患者的知晓率和治疗率仍处于较低水平,对我国血脂异常防治工作提出更为严峻的挑战。

血脂异常与心血管病发病增加关系密切。心血管病已成为我国城乡居民第一位死亡原因,严重消耗医疗和社会资源,给家庭和社会造成沉重的疾病负担。血脂异常(主要是高胆固醇血症)是心血管病的主要危险因素。国内外研究和临床实践证明,预防和控制血脂异常,降低人群胆固醇水平,可明显减少心肌梗死、缺血性卒中事件和心血管死亡,显著改善心血管病患者的生活质量并有效降低疾病负担。

陕西府谷发生爆炸事故

目前10人死亡147人受伤



图为爆炸现场。

据新华社西安10月24日电(记者毛海峰张骏贺)记者从现场救援处置领导小组获悉,截至24日23时,陕西府谷爆炸事故死亡人数已上升至10人。爆炸已造成157人伤亡,其中113人住院(重症11人),门诊救治34人。据初步掌握情况,仍有人被困未获救,现场仍在救援中。24日14时许,府谷县新民镇一居民院落的临时建筑彩钢房发生爆炸,波及旁边建筑受损,人员伤亡。

海南省地方税务局第一稽查局

税务文书送达公告

(琼地税一稽公[2016]24号)

南海海世界旅行社有限公司:

纳税人识别号:460100693150684

事由:你公司在规定期限内未履行已经生效的《海南省地方税务局第一稽查局税务处理决定书》(琼地税一稽处[2015]20号)及《海南省地方税务局第一稽查局税务行政处罚决定书》(琼地税一稽罚[2016]4号),应纳税款15,399,180.26元、滞纳金2,888,738.02元、

罚款7,594,379.75元,共计25,882,298.03元。

因你公司不在注册地办公,且无法联系你公司法定代表人及相关人员,采取其他方式均无法送达你公司,根据《中华人民共和国税收征收管理法实施细则》第一百零六条规定,现依法向你公司公告送达《海南省地方税务局第一稽查局催告通知书》(琼地税一稽催通[2016]13号),自本公告发出之日起满30日,即视为送达。

附件:《海南省地方税务局第一稽查局催告通知书》(琼地税一稽催通[2016]13号)

海南省地方税务局第一稽查局
2016年10月25日

中国银行股份有限公司海南省分行全辖安防监控设备维护商选型入围项目邀请招标公告

一、项目名称:中国银行股份有限公司海南省分行全辖安防监控设备维护商选型入围项目。

二、供应商的基本条件:

(一)供应商必须具备安防工程二级及以上从业资质证书;

(二)供应商的注册资金一百万元以上,有大型或全省视频监控联网项目实施、运维经验;

(三)供应商在海南本地设立机构,具备10名以上有相关监控维护专业的技术人员,并配备至少1辆工程维修车辆;

(四)供应商管理体制规范,2013年至今无违法违规行为。

海南省地方税务局第一稽查局催告通知书

琼地税一稽催通[2016]13号

南海海世界旅行社有限公司:

(纳税人识别号:460100693150684)

本局于2015年12月3日作出的《海南省地方税务局第一稽查局税务处理决定书》(琼地税一稽处[2015]20号)及《海南省地方税务局第一稽查局税务行政处罚决定书》(琼地税一稽罚[2016]4号)现已生效,你公司在规定期限内未履行相应的义务。现根据《中华人民共和国行政强制法》第三十五条的规定对你公司进行催告,请你公司将应纳税款15,399,180.26元、滞纳金2,888,738.02元、罚款7,594,379.75元,共计25,882,298.03元立即缴纳入库。若你公司仍不履行相应义务,本局将作出强制执行决定。

海南省地方税务局第一稽查局
2016年10月25日

海南新城拍卖有限公司拍卖公告

(第20161117期)

受委托,我公司定于2016年11月17日16:00在海南省陵水黎族自治县椰林镇建设路建设银行八楼拍卖大厅按现状进行公开拍卖:

1、陵水黎族自治县粮食储备公司2014年入库县级早灿稻358吨;2、陵水黎族自治县粮食储备公司2015年入库县级晚灿稻7吨。

整体拍卖,竞买保证金54万元,参考价77.548万元。

标的展示时间:2016年11月02日至2016年11月03日。

展示地点:第1项标的存放在陵水黎族自治县粮食储备公司的光坡库点2仓、3仓;第2项标的存放在提蒙库点2仓3廩。

报名时间:自公告之日起至2016年11月15日17:00前交纳竞买保证金,并办理报名手续。

联系人:李小姐 张先生 联系电话:0898-83333322

联系地址:海南省陵水黎族自治县椰林镇建设路208号老法院二楼201室(陵水友好医院旁)。

海南金鼎拍卖有限公司拍卖公告

(2016)海中法拍委字第140号

经海口市中级人民法院电脑随机选定确认并委托,由我公司对以下涉案财产进行公开拍卖:位于海口市滨涯湖开发区11309.85平方米土地使用权中40%土地使用权【证号:海口市国用(籍)字第S0176号】。参考价:1579.77万元,竞买保证金200万元。现将第一次拍卖相关事项公告如下:1.拍卖时间:2016年11月11日10:00;2.拍卖地点:海口市滨海新村588号海景湾大厦主楼20层拍卖厅;3.标的展示咨询及办理竞买手续时间:见报之日起至2016年11月10日17:00止,逾期将不予办理竞买手续;4.收取竞买保证金时间:以2016年11月8日17:00前到账为准;5.收取竞买保证金单位名称:海南省海口市中级人民法院;开户行:海口市农村信用合作社联社营业部;账号:1009454890000809;6.缴款用途须填明:竞买保证金(如代缴注明代某某缴款);7.特别说明:按现状净价整体拍卖,所有费用由买受人承担。拍卖机构电话:0898-3632621613006080999;法院监督电话:0898-66501619

海南金鼎拍卖有限公司拍卖公告

受海南省地方税务局第一稽查局委托,我公司定于2016年11月10日上午10:00在海口市海景湾大厦主楼20层拍卖下列资产:

委托拍卖标的物名称:海南义隆实业有限公司一间车库,产权证号:HK083562;房号102-3,建筑面积25.48平方米,参考价:2.5万元。

展示时间:2016年11月2日至2016年11月3日。收取保证金单位:海南金鼎拍卖有限公司,开户行:农行海口市龙昆支行,账号:21-139001040001861。缴款用途处须填明:竞买保证金(如代缴必须注明代某某缴款)。竞买保证金数额为1万元,保证金必须在2016年11月9日17:00前到账,逾期不予办理竞买手续。净价拍卖,产权过户应缴纳的税、费由买受人承担。

地址:海口市滨海新村588号海景湾大厦主楼20层

电话:0898-36305012 13876355557

委托方监督电话:0898 66725332