英特尔芯片漏洞发酵 消极应对数据安全引舆论风暴

□特约撰稿 马振贵

〉〉图说新闻

近日,福建福州一退休老人被诈骗分子冒充“公检法机关办案人员”,几个电话骗走账户资金300万元。调查发现,岁末年初,多地发生老年人遭诈骗的案件,这些案件单笔涉及资金少则几万元,多则数十万元甚至上百万元。图为民警在福建省晋江市公安局刑侦大队反诈骗中心工作,民警提醒老人,要提高警惕,了解新型诈骗手法。

新华社 魏培全/摄

〉〉资讯

首批社会安全大数据国家工程实验室主任基金申报指南发布

由中国电科院联合多单位组建的社会安全风险感知与防控大数据应用国家工程实验室,近日面向高等院校、科研机构及高科技公司优秀研究团队或个人,发布首批(2017—2018年度)3000万元“社会安全大数据”国家工程实验室主任基金申报指南。

基金将面向国家社会安全重大战略需求,以“国家大数据战略”“新一代人工智能发展规划”等顶层战略为指导,以提升对潜在社会安全事件的主动发现、提前预警和及时防范能力为目标,围绕大数据与人工智能技术在社会治理与风险感知防控应用中面临的关键科学问题与技术瓶颈,开展基础理论和核心技术研究。

(据1月4日国家国防科技工业局网站消息)

网络借贷将有征信统一平台

中国人民银行4日发布公示称,已受理百行征信有限公司(筹)的个人征信业务申请。随着百行征信的成立,网络借贷等领域将有征信服务统一平台。

根据央行公示的信息,百行征信由芝麻信用、腾讯征信、前海征信、考拉征信、鹏元征信、中诚信征信、中智诚征信、华道征信等8家市场机构和中国互联网金融协会共同发起组建。

业内认为,不隶属于某一家企业集团的百行征信的组建,将有利于共享个人征信信息,化解信息孤岛困局,缓解个人征信产品有效供给不足问题;有利于防范系统性金融风险,遏制“过度多头借贷”“诈骗借贷”等乱象;有利于贯彻个人信息隐私权益保护原则,防止个人信息被过度采集、不当加工和非法使用。

(据1月4日新华社消息)

百度2017年处置451.2亿条有害信息

全球最大的中文搜索引擎公司百度近日发布2017年度信息安全综合治理报告。该信息安全报告中统计了淫秽色情类、毒品类、赌博类、非法信息交易类、危险物品类、制假贩假类、诈骗类、暴恐类、侵权类、其他等10类危害社会安全及公民人身财产安全相关的有害信息。

报告披露,,2017年全年百度通过全方面手段处置的有害信息共达451.2亿余条,仅仅在上线前,机器就已拦截超过99%的有害信息。值得关注的是,所有类型中淫秽色情类占比高达68%,制假贩假类、赌博类紧随其后位列前三,占比分别为8.6%和7.2%。

(据1月2日中新网消息)

其实对于苹果、英特尔、微软来说,都曾经遭遇过很多安全问题,如果说以前我们在意的是软件企业本身存在的设计BUG等缺陷,人们很容易存在一个误解,就是只有系统级的软件才容易出现漏洞,也更容易遭受到黑客等攻击。而随着移动互联网时代的来临和火爆发展,很多在非软件应用层面的漏洞或许会带来更加致命的危机。比如苹果之前爆发的云数据泄露以及近期的“降频门”事件,再比如眼下火上浇油的英特尔芯片漏洞问题等等,我们看到更多的服务和硬件厂商带来的安全隐患或许给用户的危害更加“触目惊心”。

英特尔“漏洞门”震惊全球

近日,英特尔CEO科再奇表示,该公司不会召回受Meltdown(熔断)和Spectre(幽灵)漏洞影响的芯片产品。众所周知,早在1994年,英特尔就曾经召回过价值数千万美元的奔腾处理器,原因是该处理器中含有FDIV bug。不过,英特尔显然这次是不愿意召回的,科再奇表示,Meltdown和Spectre要比1994年的FDIV容易解决,而且英特尔已经开始在解决这个漏洞。英特尔表示,过去5年中他们生产的9成处理器都将会在近日迎来软件更新来解决漏洞。

英特尔表示,他们与许多计算机制造商以及操纵系统提供商展开了合作,本周他们会为过去5年内生产的芯片提供补丁程序。在未来几周内,他们还将会为生产时间更早的处理器提供补丁程序。另外英特尔还将在未来生产的芯片中解决这一漏洞。英特尔表示,该公司“已经针对过去5年推出的处理器产品发布了更新”。英特尔还指出,“很多操作系统厂商、公共云服务提供商、设备制造商和其他公司都表示,他们已经更新了产品和服务。”

值得关注的是,这次带来的危害或许涉及面更广,不管是PC、平板电脑、智能手机还是其它智能电子设备,只要里面使用了Intel的CPU,那么都有可能已经中招了。据了解,此次曝光的两个漏洞目前尚未被黑客利用,但是它们属于“根本性”的设计缺陷,包括Windows、Linux、Android和macOS等系统无一幸免,对于Meltdown漏洞,几大系统均推出了针对性补丁,但Spectre漏洞尚未得到有效修复。英特尔建议用户关注后续的芯片组更新和主板BIOS更新。

有意思的是,AMD表示,由于他们的基础架构不同于其他芯片,所以其相信AMD芯片目前受到的威胁几乎为零。鉴于AMD使用了不同的架构,目前尚未发现漏洞,AMD可能会把它作为一项营销优势,特别是在数据中心市场,前者市场份额占据了99%。而高通公司近日也宣布,针对近期曝光芯片级安全漏洞,正在全力开发更新,在受影响的产品中部署解决方案,并继续加强产品安全。但高通并未透露具体哪些产品受到了影响。

用户安全如何保障?媒体解读过分了吗?

众所周知,移动互联网时代,用户对自身数据的安全性要求越来越高,尤其是大量的隐私和商业数据等颇具价值的内容都会在移动互联网端进行呈现,如果说以前在PC时代,我们还有一些内容可以屏蔽PC存在,但进入到移动互联网时代之后,每个用户的大量数据和信息都离不开网络和应用的支撑。这时候用户数据的安全性无疑是非常巨大的。对国内市场而言,之前关于对微信安全的持续发酵,以及支付宝钱包2017年数据中默认勾选蚂蚁金融服务许可等等的解读,都说明媒体正在引导用户持续关注自己的数据安全。因为这部分内容出现问题之后,带来的危害或许是持续和致命的。

对于媒体对英特尔漏洞的解读,英特尔方面认为媒体是过分解读了,其实不然,这恰恰是媒体在督促企业持续关注信息安全和用户安全的一个重要的表现,同时也是对用户的一种警醒。就如同当初爆发的“勒索”病毒一样,谁能想到一夜之间数以百万计的电脑遭受攻击,再加上比特币等虚拟资产的引入,对于黑客的跟踪反而变得更加艰难。虽然我们都不愿意看到漏洞,但是漏洞确实因为科技本身的能力问题也不可避免,尤其对于硬件产品而言,出现漏洞更是“底层级”的,带来的影响更是巨大。

本次英特尔数据安全问题发酵是源于科技媒体The Register的一篇报道:英特尔的部分处理器有一个“根本性的设计缺陷”,导致本来单独用于保护密码等重要信息的存储区,可能会让一些软件程序获取权限。过去十年间所有使用英特尔芯片的电脑都受到影响,包括微软公司的Windows和苹果公司的OS X操作系统。这个信息也直接使英特尔的股价出现下跌。英特尔认为是媒体的过分解读,让自己的股价下跌。而且,英特尔认为这些漏洞不具有破坏、修改或删除数据的潜力。

虽然英特尔更新了补丁程序,但是有报告认为,这个芯片级安全漏洞的修补程序不是很完善,安成了修复,也会对性能造成严重的影响,“可能导致5%到30%的性能下降”,造成速度下降是由于处理器必须转储暂存的数据并重新加载存储器中的讯息。有意思的是,英特尔对此也不认可,英特尔表示,任何性能影响都由工作负载决定,对于一般用户来说,并不显著,并且会随着时间的推移得到缓解。

安全问题正成为业界共识

对于安全问题,其实涉及所有人和所有的企业,因为无论哪个环节出现问题带来的影响都是巨大的,尤其是在海量信息时代,大数据应用之后,信息安全意味着庞大的产业链,也预示着更多的技术支撑能力,这在以往是难以想象的。

或许未来涉及应用安全问题,并不是单一企业就可以解决的。这次英特尔芯片安全漏洞问题也是如此。我们看到,英特尔表示,它正在与包括AMD、ARM和操作系统供应商在内的其他几家技术公司合作,“开发一种适应于全行业的方法”,以便“迅速并具有建设性地解决问题”。

据悉,英特尔目前已经在美国加州、俄勒冈州和印第安纳州遭到三起诉讼,且都是集体诉讼。消费者的指控主要集中在英特尔披露漏洞问题迟缓,有消费者称,英特尔在几个月前就已经发现了处理器漏洞,但迟迟未对外发布消息。

(本文系作者个人研究之观点,不代表本报立场。作者系IT分析师小刀马)