国盟信息安全通报

2019 年 9 月 30 日第 202 期

国盟信息安全通报

（第 202 期）

国际信息安全学习联盟

2019 年 9 月 30 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 405 个，其中高危漏洞 88 个、中危漏洞 281 个、低危漏洞 36 个。漏洞平均分值为 5.68。本周收录的漏洞中，涉及 0day 漏洞 57 个（占 14%），其中互联网上出现“WordPressquotes-collection 插件跨站脚本漏洞、FlameCMS login.php 文件 SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2794 个，与上周（2276 个）环比增长 23%。

主要内容

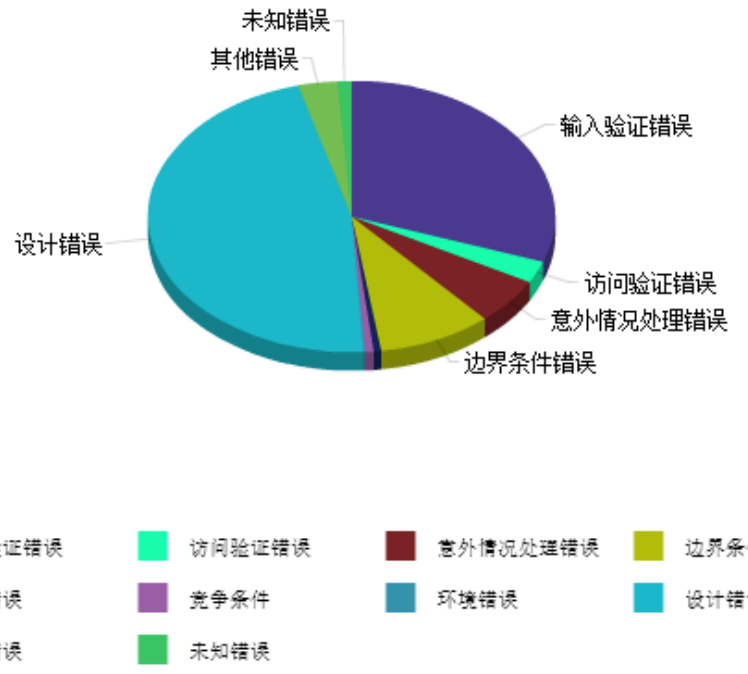
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

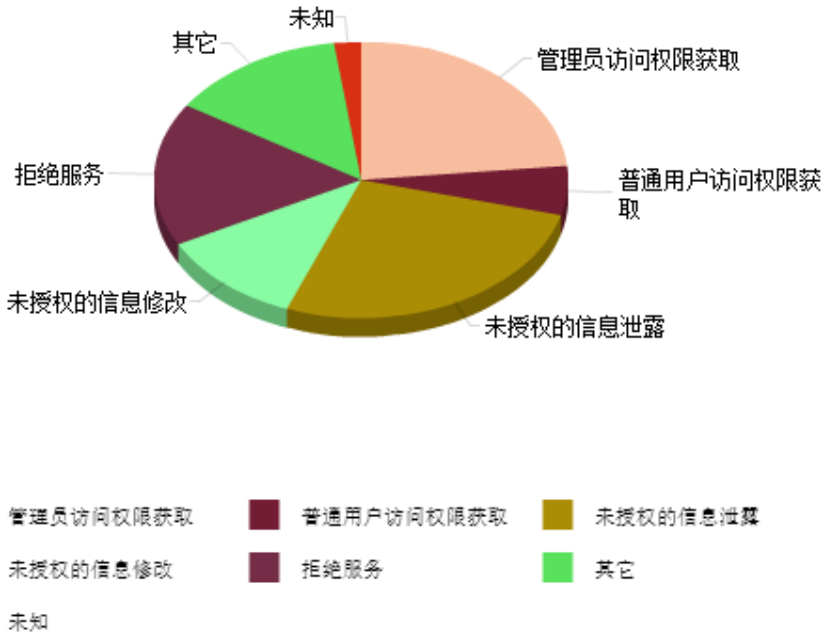
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 405 个，其中高危漏洞 88 个、中危漏洞 281 个、低危漏洞 36 个。漏洞平均分值为 5.68。本周收录的漏洞中，涉及 0day 漏洞 57 个（占 14%），其中互联网上出现“WordPressquotes-collection 插件跨站脚本漏洞、FlameCMS login.php 文件 SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2794 个，与上周（2276 个）环比增长 23%。

二、安全漏洞增长数量及种类分布情况

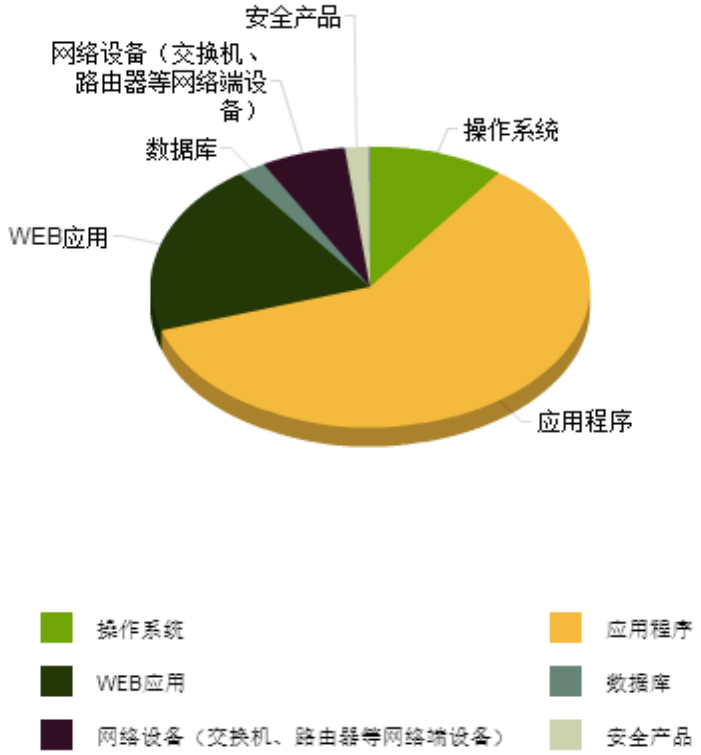
➢ 漏洞产生原因（2019 年 9 月 16 日—2019 年 9 月 30）



➢ 漏洞引发的威胁（2019 年 9 月 16 日—2019 年 9 月 30）



➢ 漏洞影响对象类型（2019 年 9 月 16 日—2019 年 9 月 30）



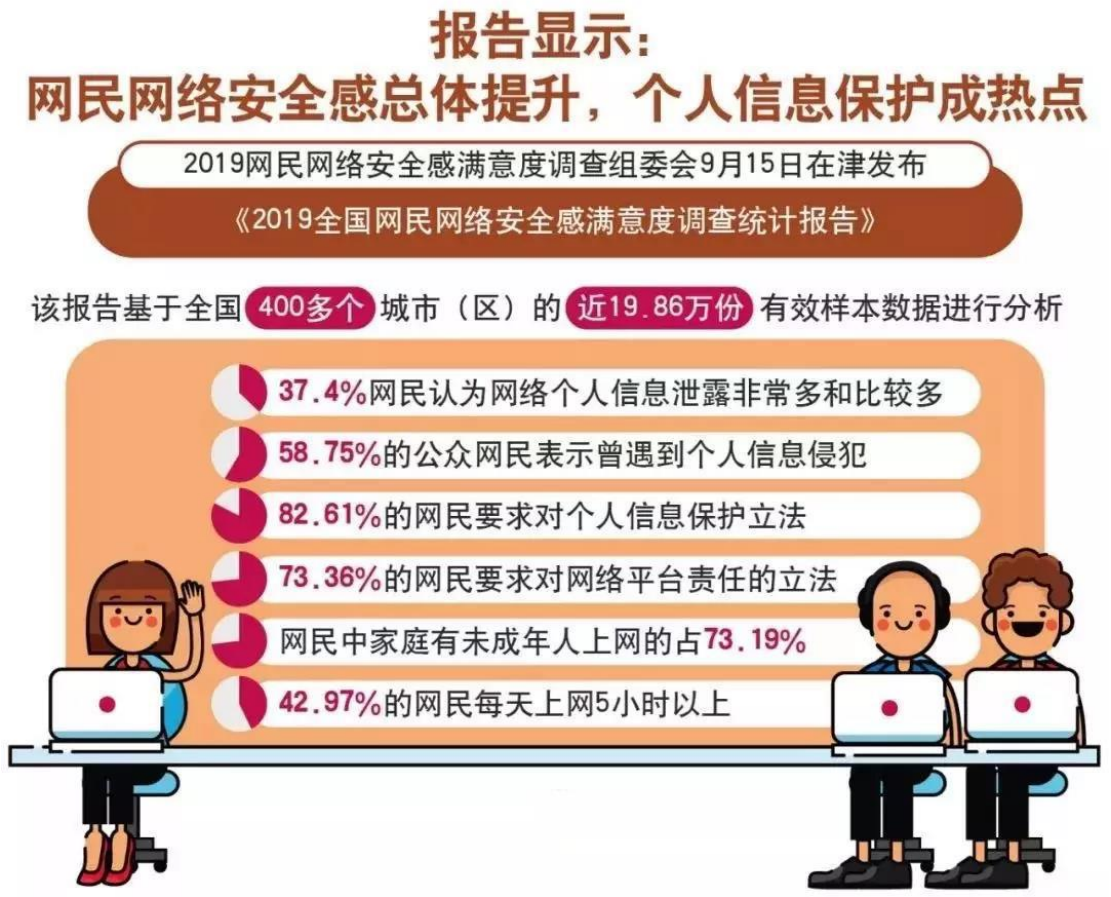
三、安全产业动态

➢ 移动互联时代，我们这样打赢个人信息保卫战

“移动互联时代，该怎样保护个人信息？”2019 国家网络安全宣传周刚刚结束，关于如何切实保障网络个人信息安全的讨论引来各方聚焦。哪些不良使用习惯会导致手机防护尽失、网络用户个人信息被“劫”？加固网络个人信息“城防”有何关键词？哪些隐患仍在威胁网络个人信息安全？

3 个不良习惯或丢光全部个人信息

《2019 全国网民网络安全感满意度调查统计报告》显示，近四成网民认为，网络个人信息泄露非常多和比较多；近六成网民更曾遭遇过个人信息被侵犯。不仅如此，专家表示，个人信息遭泄露人群中，手机网民是“重灾区”。记者调查发现，这与几种手机不良使用习惯直接相关。



- **掉以轻心，随意扫描二维码，下载可疑应用软件。**“这是我们的创业项目，您扫描一下二维码填写个人信息，就可以获得我们的小礼品。”如此“地推”场景，相信并不陌生。

一些人或为支持年轻人创业热情或认为领取小礼品“有利可图”而同意扫描。殊不知，无论动机如何不同，他们手机上的个人信息都面临相同的泄露风险。网络安全专家告诉记者，一些二维码包含木马病毒，可窃取和修改设备内重要信息。不法分子还可能以此远程遥控用户手机，实现开启摄像头、麦克风、定位等操作。

- **因小失大，轻信“试睡”“体验”等“免费套路”。**酒店免费试睡体验类项目推广文章一度在微信朋友圈中流行。文中称，用户只要转发相应内容，并在文内链接留下自己的真实姓名、手机号等个人信息，就有机会获得免费试睡五星级酒店机会，有的甚至索要身份证号等个人敏感信息。记者从网络安全专家处得知，事实上，填写此类信息的用户获得“免费”体验机会微乎其微，但丢失个人敏感信息的风险却十分巨大。
- **被逼无奈或盲目授权，忽视手机 App 用户协议和隐私政策。**“如要继续使用本软件，请提供相应授权。”不少 App 通过“不同意就不准用”的“霸王条款”过度索权，给用户个人信息造成重大风险。比如记者发现某手电筒 App，安装时却要求获取阅读手机通讯录的权限。此外，一些用户嫌麻烦，使用 App 前不阅读用户协议和隐私政策，导致个人信息大量泄露还不自知。

标准模糊、霸王条款、隐蔽收集等潜在风险仍存

多位专家学者和相关部门负责人向记者表示，当前在网络个人信息保护方面“发力”已成常态，但仍有潜在风险有待排除。

相关保护措施的标准是什么？如何把握？中央网信办相关负责人认为，移动互联时代的个人信息保护应该“标准先行”，既不能“没标准”，也不能“标准总变”。他认为，App 收集和使用个人信息涉及到手机制造商、手机应用开发商、应用商店等多主体，因此有必要打通各环节，做到行业协调、综合治理。

中国消费者权益保护法学研究会副秘书长陈音江认为，当前经营者通过“不同意就不准用”等“霸王条款”变相强制采集用户信息问题泛滥，消费者个人信息泄露后往往存在举证难、维权难等问题。对此，不仅需要有关部门加强实际监管、严格执行现有法律法规，保护消费者权益，国家更应针对侵权“顽症”制定完善相关规则。

另据记者调查，还存在一些 App 隐蔽收集和使用用户个人信息的问题。中国信息通信研究院安全研究所所长魏亮指出，例如用户已经关闭了 GPS 权限，因此默认 App 不再收集我的地理位置信息，但实际上 APP 仍在通过用户所连接的 WiFi 来获取用户位置，这种收集和使用用户个人信息的行为已超出一般用户心理预期。

他建议，行业相关主体应切实以个人信息保护理念直接指导研发、编码过程，同时加强

对防窃密、防篡改、防泄露、数据脱敏、关键数据审计、流动追溯和数据备份等安全技术的研发和商业部署，让安全机制与安全技术落地、落实。

强化保护 3 个关键词：机构协同、精细立法、严厉打击

今年 1 月 25 日，中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》。有关方面开始从机构协同、精细立法、刑事打击等几个关键方面加大网络个人信息保护力度。

全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会成立 App 违法违规收集使用个人信息专项治理工作组，具体推动评估打击整治 App 违法违规收集使用个人信息。

据专项治理工作组专家何延哲介绍，专项治理工作组选取近 600 款用户数量大、与民众生活密切相关的 App 进行评估，督促问题严重的 200 余款 App 进行整改，涉及整改的问题点达 800 余个，无隐私政策、强制索权、超范围收集个人信息等问题得到显著改善。

另一方面，今年 5 月以来，国家网信办就《数据安全管理办法》面向全社会公开征求意见，并出台《儿童个人信息保护规定》。其中，《数据安全管理办法（征求意见稿）》明确提出，网络运营者以经营为目的收集重要数据和个人敏感信息的，应向所在地网信部门备案。记者从全国人大常委会法制工作委员会得到消息，个人信息保护法已列入本届全国人大常委会的立法规划。

此外，公安部在今年的“净网 2019”专项行动中，将打击 App 违法违规收集使用个人信息作为行动重点，各地公安机关侦破一批典型案件并向社会通报，相关违规企业被依法依规处理。 （来源：新华社）

➢ 网络生态环境治理的里程碑

近日，国家互联网信息办公室发布《网络生态治理规定（征求意见稿）》（以下简称《征求意见稿》），并向社会公开征求意见。《征求意见稿》以网络信息内容为主要治理对象，以营造文明健康的良好生态为目标，突出了“政府、企业、社会、网民”等多元主体参与网络生态治理的主观能动性，重点规范网络信息内容生产者，网络信息内容服务平台，网络信息内容服务使用者以及网络行业组织在网络生态治理中的权利与义务。这是我国网络生态治理领域的一项里程碑事件，而且以“网络生态”作为网络空间治理立法的目标，在全球也属首

创。

《征求意见稿》集中体现了习近平总书记提出的“我们要本着对社会负责、对人民负责的态度，依法加强网络空间治理”的重要指示精神，符合“以人民为中心”的发展理念，为我国实施网络生态治理法治化奠定了坚实的基础。

《征求意见稿》突出了网络生态治理主体的多元化

网络生态治理，应当明确多元参与协同共治的治理模式，要突破市场和政府二元对立和单一的主导模式。在数字经济时代，要以平台思维和社会化思维重新审视政府、企业、社会、网民四大主体在网络生态治理中的功能和作用。他们已经不是主体支配和被支配的关系，而是基于共同利益和目标的伙伴式关系。

《征求意见稿》第二条第二款明确了网络生态治理的定义，即“本规定所称网络生态治理，是指政府、企业、社会、网民等主体，以网络信息内容为主要治理对象，以营造文明健康的良好生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。”

网络生态是由多种文明要素组成的系统，这些要素主要包括网络主体、网络信息、主体行为、技术应用、基础设施保障、网络政策法规和网络文化等方面。笔者认为，在参与网络生态治理的四大主体中，政府的作用是监管、企业的义务是履责、社会的功能是监督、网民的义务是自律。

重点规制三大管理相对人

在网络生态治理行政法律关系中，与行政主体相对应一方的公民、法人和其他组织是网络生态治理的行政管理相对人。鉴于网络生态治理的对象是网络信息内容，而信息内容的生态治理主要涉及三类主体，即内容的生产者、内容的服务平台和内容服务的使用者，为此《征

求意见稿》重点规制这三大行政管理相对人。

首先，作为制作网络信息内容的组织或者个人，在遵守法律法规的前提下，还要遵循公序良俗，加强网络文明建设。其次，作为提供信息内容复制、发布、传播等服务的网络信息服务提供者（信息内容服务平台），必须切实履行网络生态治理的主体责任，重点加强本平台的生态治理工作，积极培育向上向善的网络文化。再次，作为使用网络信息内容服务的组织或者个人，是网络生态治理的主力军，对网上的违法和不良信息有义务以投诉、举报等方式行使监督权。

网络信息内容服务使用者禁止触碰的红线

我国网络信息内容服务使用者构成了一个庞大的网络群体。据腾讯官方数据显示，2018 年仅微信月活跃人数就保持在 10.8 亿用户上下，每天有 450 亿条消息在微信里传输。《征求意见稿》规定了网络信息内容服务使用者不得触碰的几条“红线”：不得利用网络和相关信息技术，实施侮辱、诽谤、威胁以及恶意泄露他人隐私、散布谣言、人肉搜索等网络侵权、网络暴力行为，侵害其他组织或者个人名誉权、财产权等合法权益；不得通过发布、删除信息等干预信息呈现的手段谋取不正当利益；不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动；不得通过人力或者技术手段实施流量造假、流量劫持以及虚假注册账号、批量买卖账号、操纵用户账号等行为，破坏网络生态秩序；不得利用党徽、国旗、国徽等代表党和国家形象的标识，或者借党和国家领导人名义及国家重大活动、重大纪念日等，违法违规开展网络商业营销活动。

《征求意见稿》体现了国家在网络生态治理领域的主权价值取向，展示了网络空间的自由和秩序、开放和自主、管理和服务的辩证关系，重点突出了网络生态治理的统筹协调。随着《网络生态治理规定》的出台，我国网络的生态治理将正式纳入法治轨道，并将依法形成合力。（来源：中国青年报客户端　作者：王春晖）

➢ 做好新时代网络安全工作四个要素

2019 年 9 月 16 日，2019 年国家网络安全宣传周在天津梅江会展中心开幕。本届宣传周以“网络安全为人民，网络安全靠人民”为主题。中央网信办副主任、国家网信办副主任刘烈宏出席了网络安全技术高峰论坛并发表致辞，他表示，当前，网络安全风险和挑战也不断增大，网络攻击、网络窃密、网络诈骗、网络黑产、个人信息泄漏等现象频发，关键信息

基础设施面临较大的安全风险，网络安全问题日益成为影响国家安全、社会稳定和人民群众切身利益的重大战略问题。

刘烈宏认为，做好新时代网络安全工作，应该注意以下几个方面：

一是加强宣传教育和个人信息保护，切实维护公民在网络空间的合法权益。牢固树立以人民为中心的发展思想，提升人民群众在网络空间的获得感、幸福感、安全感，是网络安全工作的根本宗旨。要坚持网络安全为人民、网络安全靠人民，以办好国家网络安全宣传周为抓手，组织开展多种形式的宣传、教育和培训，提升全民网络安全意识和防护技能。同时深入开展 APP 违法违规收集个人信息专项治理，规范企业和机构采集利用的行为，依法严厉打击利用个人信息的违法犯罪活动，切实保障个人信息安全。

二是加快网络安全人才培养和技术产业的发展，努力形成人才培养、技术创新、产业发展的良好生态。网络空间的竞争归根到底是人才的竞争，强大的技术和产业是国家网络安全的重要支撑，要坚持网络安全教育、技术、产业融合发展。一方面加强网络安全一级学科和专业建设，实施好一流网络安全学院建设示范项目，加快建设国家网络安全人才与创新基地，着力培养急需的网络安全人才。另一方面加强网络安全技术产业统筹规划和整体布局，完善支持网络安全技术产业发展的政策措施，培育组织一批具有国际竞争力的网络安全企业。广大网络安全企业也要加强核心技术攻关，加快网络安全技术成果产业化的步伐，真正成为维护网络安全的重要力量。

三是大力培育新技术、新应用，积极利用法律法规和标准进行规范引导。当前新技术、

新应用不断涌现，带来的新问题、新挑战层出不穷。要加强技术创新，大力培育互联网、人工智能、5G、区块链等新技术、新应用，审时度势、精心谋划、超前布局，加快发展。同时要加强新技术、新应用相关法律法规和标准规范的研究制订，从技术自身安全、网络安全、隐私伦理等方面引导规范及健康发展，确保安全、透明、可控的服务于全人类的利益。

四是积极开展国际交流合作，立足开放环境，维护网络安全。网络是开放的，网络安全也是开放的，维护网络安全要树立全球视野和开放心态，正确处理开放和自主的关系，坚持安全可控和开放创新并重。关键核心技术突破既要立足自主创新、自立自强，也要互相借鉴、互相学习，借鉴国际先进的经验和技术成果，安全可控的使用世界范围先进的信息技术和产品。最大程度利用网络空间发展潜力提升网络安全发展水平，通过积极有效的国际交流、合作互动，建立多边、民主、透明的国际互联网治理体系，共同构建和平、安全、开放、合作、有序的网络空间，携手构建网络空间命运共同体。

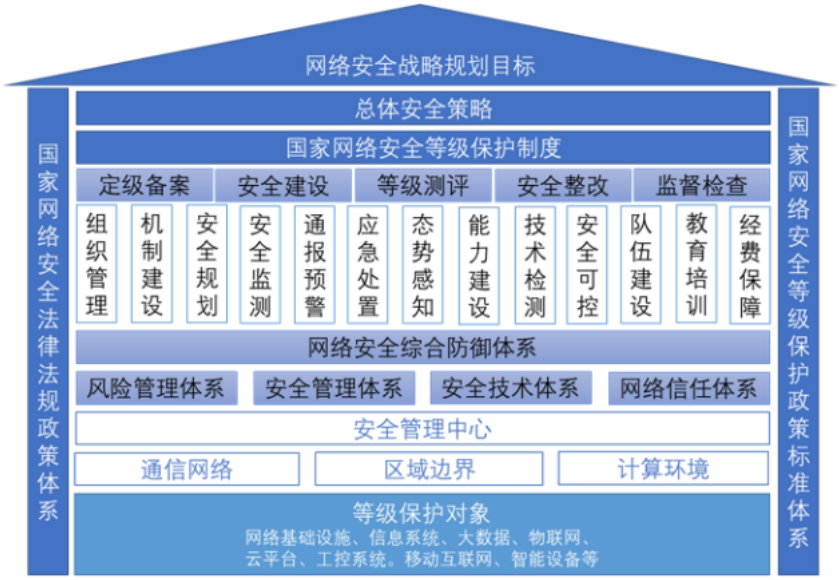
刘烈宏强调，关键信息基础设施是经济社会运行的神经中枢，是网络安全防护的重中之重。要加快出台关键信息基础设施安全保护相关的法律法规，建立健全标准体系，明确运营单位的主体责任和行业主管部门的监管责任，要强化动态、整体、综合的防护理念，健全完善网络完全态势感知和监测预警体系，加强网络安全应急工作，有效防范和应对不断变化的安全风险，要强化工业控制系统的安全保护，深入开展互联网网站安全专项的整治，严防重大网络安全事故的发生，要全面排查网络安全隐患，及时整改并进行安全加固，全力做好网络安全保障工作。（来源：人民网）

➢ 公安部张宇翔：须知等保 2.0 主要标准的调整

没有网络安全就没有国家安全。从 1.0 到 2.0，我国等级保护制度走过了十几年。等级保护 2.0 是网络安全的一次重大升级，等级保护对象范围在传统系统的基础上扩大了云计算、移动互联、物联网、大数据等，对等级保护制度提出了新的要求。近日，公安部信息安全等级保护评估中心常务副主任张宇翔对安全等级保护 2.0 主要标准的调整进行了简明扼要的介绍。

标准名称的变化

由原来的“信息系统安全等级保护××××”变为“网络安全等级保护××××”，这背后是两个战略的调整。主要特点如下：



对象范围扩大： 新标准将云计算、移动互联、物联网、工业控制系统等列入标准范围，构成了“安全通用要求+新型应用安全扩展要求”的要求内容。

分类结构统一： 新标准“基本要求、设计要求和测评要求” 分类框架统一，形成了“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心” 支持下的三重防护体系架构。强化可信计算： 新标准强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求。

强化可信计算技术使用

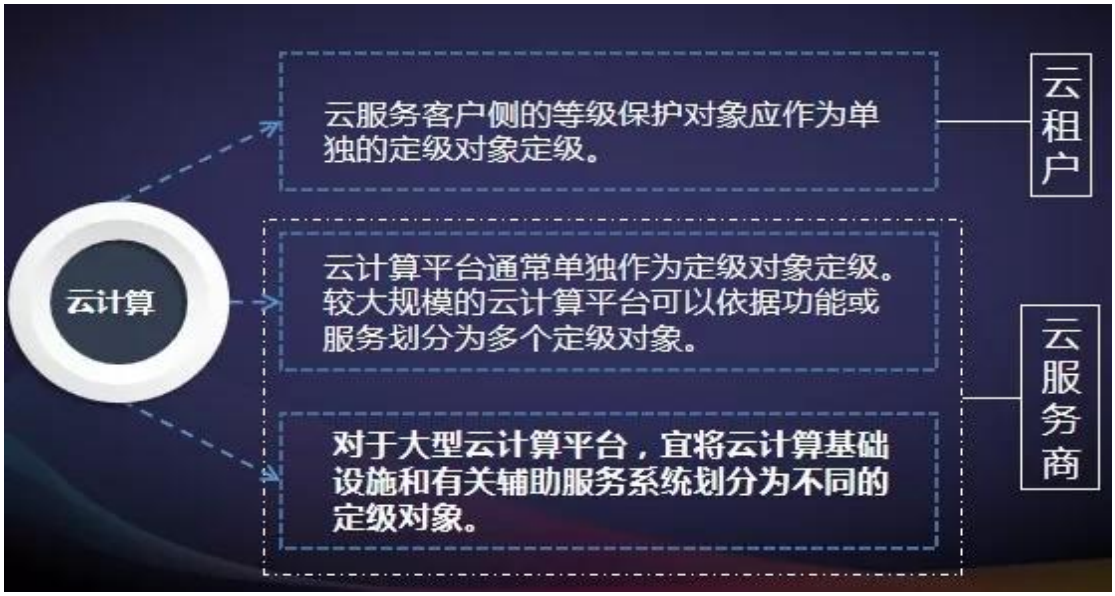
从一级到四级均在“安全通信网络”、“安全区域边界”和“安全计算环境”中增加了“可信验证”控制点。

- 一级：设备的系统引导程序、系统程序等进行可信验证
- 二级：增加重要配置参数和应用程序进行可信验证，并将验证结果形成审计记录送至安全管理中心
- 三级：增加应用程序的关键执行环节进行动态可信验证
- 四级：增加应用程序的所有执行环节进行动态可信验证

其中着重强调了三级：可基于可信根对设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

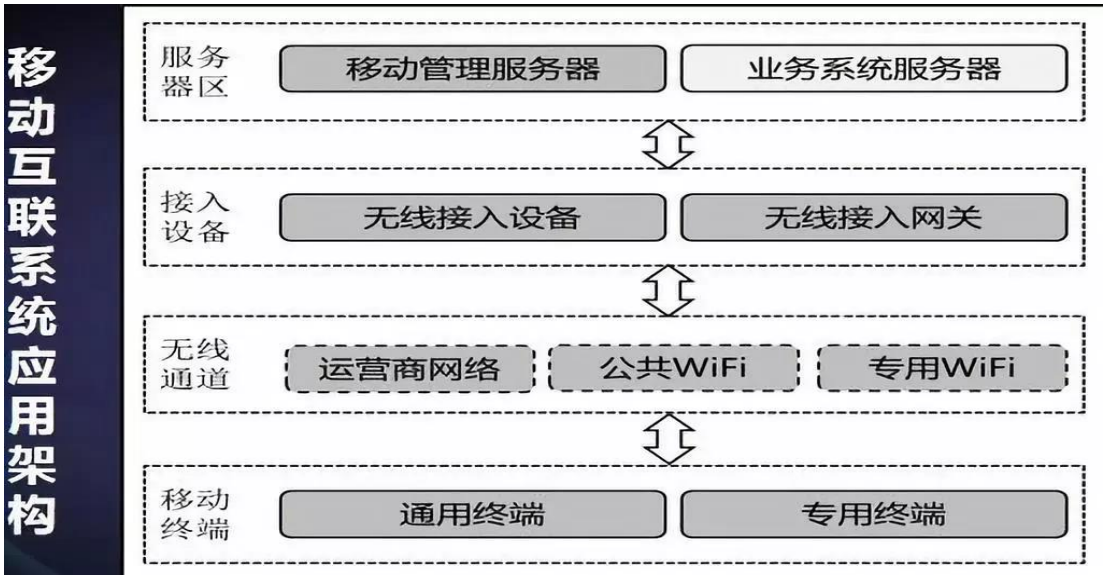
等级保护对象的扩展

增加了云计算安全扩展要求



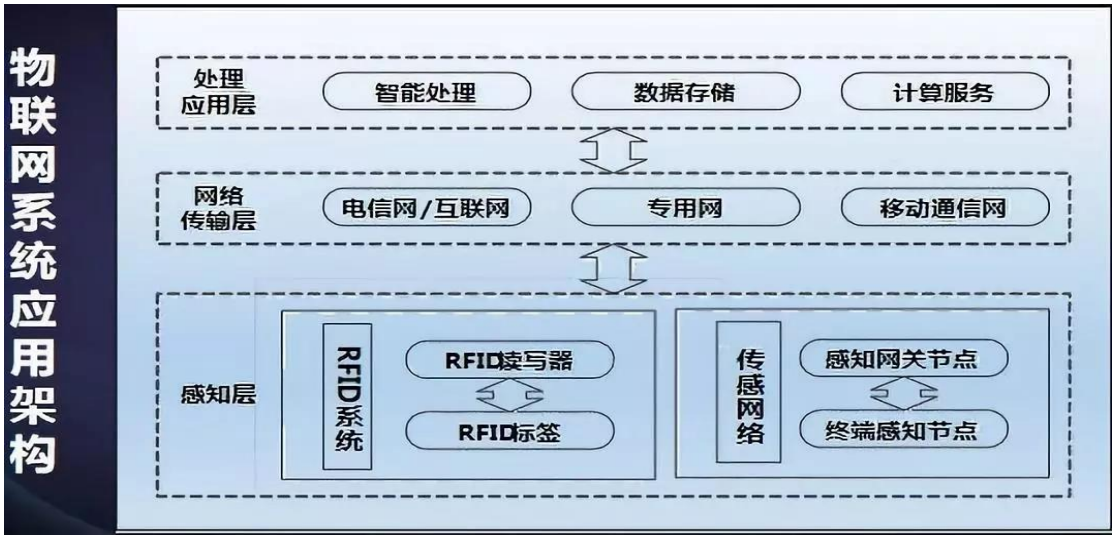
云计算安全扩展要求章节针对云计算的特点提出特殊保护要求。对云计算环境主要增加的内容包括“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”和“云计算环境管理”等方面。

增加了移动互联安全扩展要求



注：采用移动互联技术的等级保护对象应作为整体对象定级，移动终端、移动应用和无线网络等要素不单独定级。

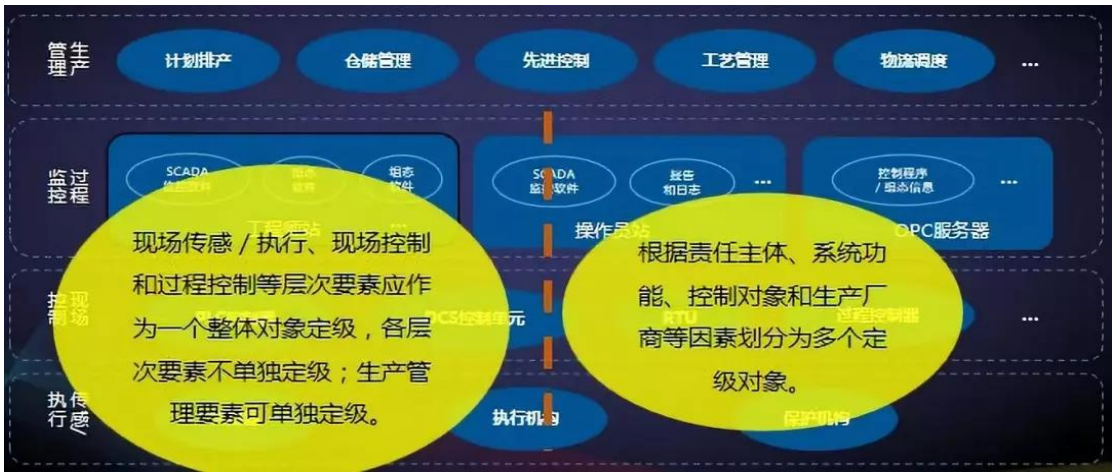
移动互联安全扩展要求章节针对移动互联的特点提出特殊保护要求。对移动互联环境主要增加的内容包括“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”等方面。增加了物联网安全扩展要求



注：物联网系统应将采集、感知、网络传输和处理应用等要素作为一个整体对象定级，各要素不单独定级。

物联网安全扩展要求章节针对物联网的特点提出特殊保护要求。对物联网环境主要增加的内容包括“感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理”和“数据融合处理”等方面。

增加了工业控制系统安全扩展要求



工业控制系统安全扩展要求章节针对工业控制系统的特点提出特殊保护要求。对工业控制系统主要增加的内容包括“室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制”和“控制设备安全”等方面。

增加了应用场景的说明

增加附录 C 描述等级保护安全框架和关键技术，增加附录 D 描述云计算应用场景，附录 E 描述移动互联应用场景，附录 F 描述物联网应用场景，附录 G 描述工业控制系统应用场景。（来源：信息安全与通信保密社）

四、政府之声

➢ 习近平对国家网络安全宣传周作出重要指示

2019 年 9 月 16 日，近日，中共中央总书记、国家主席、中央军委主席习近平对国家网络安全宣传周作出重要指示强调，举办网络安全宣传周、提升全民网络安全意识和技能，是国家网络安全工作的重要内容。国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。要坚持促进发展和依法管理相统一，既大力培育人工智能、物联网、下一代通信网络等新技术新应用，又积极利用法律法规和标准规范引导新技术应用。要坚持安全可控和开放创新并重，立足于开放环境维护网络安全，加强国际交流合作，提升广大人民群众在网络空间的获得感、幸福感、安全感。

2019 年国家网络安全宣传周开幕式 16 日在天津举行。中共中央政治局委员、中宣部部长黄坤明在开幕式上宣读习近平的重要指示并讲话。他说，要认真学习贯彻习近平总书记重要指示精神，深刻把握信息化发展大势，积极应对网络安全挑战，充分发挥广大人民在维护网络安全中的主体作用，把“四个坚持”的原则要求落到实处，有力维护人民群众在网络空

间的切身利益。

国家网络安全宣传周从 2014 年开始每年举办一届。本届宣传周以“网络安全为人民，网络安全靠人民”为主题，9 月 16 日至 22 日期间将举办网络安全博览会、网络安全技术高峰论坛、网络安全主题日等活动。（来源：新华社）

➢ 中国银保监会就《中国银保监会现场检查办法（试行）》公开征求意见

2019 年 9 月 18 日，为进一步完善现场检查制度框架，规范现场检查行为，提升现场检查质效，银保监会近日就《中国银保监会现场检查办法（试行）（征求意见稿）》（以下简称《办法》）公开征求意见。

《办法》共八章六十七条，主要章节包括总则、职责分工、立项管理、检查流程、检查方式、检查处理、考核评价和附则。《办法》突出了以下五个方面的主要内容。

一是明确现场检查定位。《办法》明确现场检查是监管流程的重要组成部分，通过发挥查错纠弊、校验核实、评价指导、警示威慑等作用，有效履行监管职责。

二是完善相关部门现场检查工作职责。明确承担现场检查职责的部门在现场检查工作中的牵头和归口管理作用，并进一步强调相关部门、各级监管机构之间的信息共享和联动机制，形成监管合力。

三是严格规范现场检查立项程序。确立“未经立项审批程序，不得开展现场检查”原则，突出现场检查立项的严肃性、科学性和公平性。

四是丰富现场检查方式方法。《办法》新增和规范了部分检查手段和方式方法，强化信息技术手段的运用，并根据工作需要，探索线上检查、函询稽核等新型检查方法。

五是鼓励自查自纠，促进机构合规经营。对于被查机构在现场检查前反馈的自查情况中主动发现并及时纠正相关问题，符合《中华人民共和国行政处罚法》第二十七条规定的相关情形，将依法提出从轻、减轻或不予行政处罚的意见建议。

《办法》的出台将进一步提升银保监会现场检查的科学性、规范性和有效性，有助于更好发挥现场检查的独特优势，督促和推动银行业和保险业机构全面贯彻落实国家宏观政策，在有效防范金融风险的同时，更好地支持实体经济持续稳健发展，更好地维护金融安全稳定大局。（来源：银保监会网站）

- **《中国银保监会现场检查办法（试行）（征求意见稿）》全文：**

- http://www.cbirc.gov.cn/cn/doc/9105/910502/91050201/26CCCE6312B34F5FA824E11984E763BC.html

➢ 水利部就网络安全渗透测试和现场检查发现的问题约谈相关单位责任领导

2019 年 9 月 23 日，近日，水利部副部长叶建春就 2019 年水利部网络安全渗透测试和现场检查中发现较多问题的单位，集体约谈松辽水利委员会主要负责人和黄河水利委员会、海河水利委员会、珠江水利委员会、太湖流域管理局、中国水利水电科学研究院等 5 家单位网络安全分管领导。

8 月中旬，根据鄂竟平部长抓住用务实手段查找问题这一“关键”和处罚这一“要害”的要求，水利部网信办采取不事先通知、不限定渗透路径的形式，对 6 个直属单位进行网络安全渗透测试。8 月底到 9 月中旬，水利部网信办组织对 8 个直属单位进行了网络安全现场检查。

叶建春首先对照《水利网络安全管理办法》逐个指出各单位存在问题，以及适用的问责条款，并指出通过渗透测试和现场检查可以看出，大多数单位网络安全重视程度有所提高，网络安全强监管初显成效，但反映出的问题不容乐观，水利行业部分单位仍然存在较多问题。

叶建春对被约谈单位提出三点要求：一是提高认识，逐级问责。要从这次渗透测试和网络安全检查中吸取教训，引以为戒，提高认识，落实主体责任。贯彻落实《水利网络安全管理办法》，对发生问题的责任单位和责任人进行责任追究，起到警示、威慑作用，防止类似问题再次发生。二是举一反三，查改同步。要积极主动延伸拓展，再次排查网内是否仍存在

安全隐患，采取有效措施整改，9 月底前必须完成整改，无法整改的问题要采取有效措施，确保水利网络安全。三是筑牢防线，迎接国庆。要配备专门力量，加强监测预警和值班值守，强化应急处置和信息通报，扎实做好网络安全工作。

被约谈单位的领导分别作了表态发言，诚恳接受批评，表示要深刻反思，吸取教训，以问题为导向，压实责任，举一反三，严格按照《水利网络安全管理办法》要求，全面开展漏洞隐患排查和整改，切实做好新中国成立 70 周年庆祝活动期间网络安全保障工作。

水利部办公厅、人事司、监督司和网信办负责同志参加约谈。（来源：水利部网站）

➢ 工信部就《促进网络安全产业发展指导意见》征求意见

2019 年 9 月 27 日，工业和信息化部网络安全管理局，为贯彻落实《中华人民共和国网络安全法》，积极发展网络安全产业，工业和信息化部会同有关部门起草了《关于促进网络安全产业发展的指导意见（征求意见稿）》（见附件），现面向社会公开征求意见。如有意见或建议，请于 2019 年 10 月 11 日前反馈。

附：关于促进网络安全产业发展的指导意见（征求意见稿）全文

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。当前，各种形式的网络攻击、黑客入侵、恶意代码、安全漏洞层出不穷，对关键信息基础设施安全、数据安全、个人信息安全构成严重威胁。网络安全的本质是技术对抗，保障网络安全离不开网络安全技术和产业的有力支撑。近年来，我国网络安全产业规模快速增长、产品体系相对完善、创新能力逐步增强、发展环境明显优化，但与网络安全保障要求相比，还存在核心技术欠缺、产业规模较小、市场需求不足、产业协同不够等问题。为积极发展网络安全产业，提升网络安全技术支撑保障水平，制定本指导意见。

一、总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平总书记关于网络安全的系列重要讲话精神，坚持新发展理念，树立正确的网络安全观，贯彻落实《网络安全法》，以服务国家网络空间安全战略需求为导向，主动应对互联网、大数据、人工智能和实体经济深度融合伴生的新风险，积极应对 5G、工业互联网、下一代互联网、物联网等新技术新应用带来的新挑战，坚持市场主导、政府引导，着力突破关键技术、构建产业生态、优化发展

环境，推动我国网络安全产业高质量发展，为维护国家网络空间安全、保障网络强国建设提供有力的产业支撑。

（二）基本原则

创新驱动。大力推动技术、产品创新，突破技术瓶颈，着力提升网络安全核心技术能力。创新网络安全服务模式，提升网络安全专业化服务水平，实现产业发展逐步由产品主导向服务主导转变。协同发展。充分调动各方力量，加强产学研合作，鼓励技术成果转化，推动强强联合、协同攻关，构建多方参与、优势互补、融合发展的产业生态体系。推动产融合作，引导社会资本参与网络安全产业发展。需求引领。推动各行业各领域持续加大网络安全投入，坚持问题导向，加强供需对接，促使产业更好满足金融、能源、通信、交通、电子政务等重点领域网络安全需求。　开放合作。推动网络安全产业国际交流合作，学习借鉴国外产业发展模式，促进技术、人才交流和信息共享，积极参与“一带一路”建设，提升产业国际竞争力。

（三）发展目标

网络安全技术创新能力显著增强，网络安全产品和服务体系更加健全，网络安全职业人才队伍日益壮大，政产学研用资协同发展的网络安全产业格局不断巩固，产业发展环境更加优化，网络安全产业维护国家网络空间安全、保障网络强国建设的支撑能力大幅提升。到 2025 年，培育形成一批年营收超过 20 亿元的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，网络安全产业规模超过 2000 亿元。

二、主要任务

（一）着力突破网络安全关键技术

以构建先进完备的网络安全产品体系为目标，聚焦网络安全事前防护、事中监测、事后处置、调查取证等环节需要，大力推动资产识别、漏洞挖掘、病毒查杀、边界防护、入侵防御、源码检测、数据保护、追踪溯源等网络安全产品演进升级，着力提升隐患排查、态势感知、应急处置和追踪溯源能力。加强 5G、下一代互联网、工业互联网、物联网、车联网等新兴领域网络安全威胁和风险分析，大力推动相关场景下的网络安全技术产品研发。支持云计算、大数据、人工智能、量子计算等技术在网络安全领域的应用，着力提升威胁情报分析、智能监测预警、加密通信等网络安全防御能力。积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构，推动网络安全理论和技术创新。

（二）积极创新网络安全服务模式

针对网络安全专业性强、技术演进快、应用难度大的特点，倡导“安全即服务”的理念，

鼓励网络安全企业由提供安全产品向提供安全服务和解决方案转变。支持专业机构和企业开展网络安全规划咨询、威胁情报、风险评估、检测认证、安全集成、应急响应等安全服务，规范漏洞扫描、披露等活动。支持合法设立的认证机构依法开展网络安全认证。大力发展基于云模式的网络安全公共服务平台，提供远程实时在线的漏洞发现、网站防护、抗拒绝服务攻击、域名安全等服务。鼓励基础电信企业和云服务提供商发挥网络资源优势，面向客户提供网络安全监测预警、攻击防护、应急保障等增值服务。鼓励发展面向智慧城市建设、电子政务等领域的网络安全一体化运营外包服务。探索开展网络安全保险服务。

（三）合力打造网络安全产业生态

支持龙头骨干企业整合网络安全创新链、产业链、价值链，建立开放性网络安全技术研发、标准验证、成果转化平台，畅通创新能力对接转化渠道，实现大中小企业之间多维度、多触点的创新能力共享、创新成果转化和品牌协同。着力培育主营业务突出、竞争能力强、成长性好的网络安全中小企业，鼓励以专业化分工、服务外包、共享研发等方式与大企业相互合作，形成协同共赢格局。充分调动各类园区、企业、科研院所、金融机构等主体的积极性和主动性，鼓励集聚、集约、关联、成链、合作发展。培育建设一批网络安全技术、产品协同创新平台和实验室，开展共性重要问题和市场亟需方向的联合研究，充分发挥科技支撑引领作用，推动产业共性技术研发和推广应用，引导创新资源集聚。鼓励企业、研究机构、高校、行业组织等积极参与制定网络安全相关国家标准、行业标准。

（四）大力推广网络安全技术应用

充分发挥党政机关和相关行业主管部门作用，推动先进适用网络安全技术产品和服务在金融、能源、通信、交通、电子政务等重要领域的部署应用。加强工业互联网、车联网、物联网安全管理，督促指导相关企业采取必要的网络安全技术措施。大力促进商用密码技术在网络安全防护中的应用。财政投资的信息化项目应当同步配套建设网络安全技术设施，并单独开展安全验收。加大对网络安全技术应用试点示范项目的支持推广力度，鼓励示范企业将解决方案转化为标准指南并开展专题宣讲。鼓励开展网络安全技术论坛和产品服务展示活动。

（五）加快构建网络安全基础设施

推动相关行业主管部门、地方政府建设本行业、本地区网络安全态势感知平台，着力提升支撑网络安全管理、应对有组织高强度攻击的能力。鼓励重点行业、骨干企业建设漏洞库、病毒库等网络安全基础资源库，促进相关主体之间的信息共享。统筹建设国家网络安全信息共享平台和应急指挥平台，实现跨企业、跨行业、跨地区信息共享和协调联动。重点围绕工

业互联网、车联网、物联网新型应用场景，建设网络安全测试验证、培训演练、设备安全检测等共性基础平台。支持构建基于商用密码、指纹识别、人脸识别等技术的网络身份认证体系。

三、保障措施

（一）加强组织领导

各地相关部门要从网络强国战略高度充分认识发展网络安全产业的重要意义，加强组织领导和统筹谋划，强化部门合作，共同营造有利于网络安全产业发展的良好环境。深入贯彻落实《网络安全法》，加快制定配套法规政策，加大网络安全监管力度，督促网络运营者落实网络安全技术措施，带动网络安全市场需求。

（二）加大政策支持力度

中央网信办指导支持国家网络安全人才与创新基地建设，会同相关部委推动网络关键设备和网络安全专用产品认证和安全检测结果互认，避免重复认证、检测。工信部推动国家网络安全产业园区建设，建立网络安全产业运行监测体系，组织开展网络安全技术应用试点示范，指导举办中国网络安全产业高峰论坛。国家发展改革委加强网络安全领域规划、政策研究制定。中央财政统筹利用中国互联网投资基金等现有渠道，引导支持网络安全产业发展。各地可结合本地实际情况，在财政、人才引进、要素保障等方面研究制定有针对性的产业扶持政策。

（三）健全人才培养体系

推动高校设立网络空间安全学院或网络安全相关专业，加强一流网络安全学院和网络安全师资队伍建设。加强网络安全职业教育和技能培训，培养更多实用技能型人才。推动校企对接，支持设立网络安全联合实验室。鼓励举办高水平网络安全技能竞赛，健全人才发现选拔机制。支持职业技能鉴定机构、行业协会等开展网络安全人员技能鉴定和能力评定工作。

（四）推进国际交流合作

利用各种多边、双边对话机制或活动平台，加强网络安全技术、产业务实合作与交流。鼓励有实力的网络安全企业设立海外研发中心和联合实验室，引进海外高端人才和先进技术。鼓励参加和举办有影响力的网络安全国际论坛和展会，积极参与网络安全国际标准制定和协调。推动相关地方发挥区位优势，打造国际、区域性网络安全技术、产业、人才交流平台。（来源：工业和信息化部网络安全管理局）

- **《关于促进网络安全产业发展的指导意见（征求意见稿）》的意见全文：**
- http://www.miit.gov.cn/n1278117/n1648113/c7449603/content.html

五、本期重要漏洞实例

➢ ImageMagick Studio ImageMagick 内存泄露安全漏洞

发布日期：2019-09-23
更新日期：2019-09-25
受影响系统：
ImageMagick ImageMagick 7.0.8-35
描述：

CVE(CAN) ID: CVE-2019-16710
ImageMagick Studio ImageMagick 是一套开源的图像处理软件。该软件可读取、转换或写入多种格式的图片。
ImageMagick Studio ImageMagick 7.0.8-35 版本，在 MagickCore/memory.c/AcquireMagickMemory 中存在内存泄露安全漏洞。攻击者可利用该漏洞获取敏感信息。
<*来源：butterflyhack
*>

建议：

厂商补丁：
ImageMagick

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://github.com/ImageMagick/ImageMagick/issues/1528

➢ Microsoft Internet Explorer 远程代码执行漏洞

发布日期：2019-09-23
更新日期：2019-09-25
受影响系统：
Microsoft Internet Explorer 9
Microsoft Internet Explorer 11
Microsoft Internet Explorer 10
描述：

CVE(CAN) ID: CVE-2019-1367

Internet Explorer，是微软所开发的图形用户界面网页浏览器。
Internet Explorer 在脚本引擎处理内存中对象的方式中存在一个远程代码执行漏洞。该漏洞可以破坏内存，使攻击者可以在当前用户的上下文中执行任意代码。

<*来源：Microsoft
*>

建议：

厂商补丁：
Microsoft

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://support.microsoft.com/zh-cn/help/4522007/cumulative-security-update-for-internet-explorer

➢ Linux kernel 信息泄露漏洞

发布日期：2019-09-23
更新日期：2019-09-25
受影响系统：
Linux kernel < 5.2.14
描述：

CVE(CAN) ID: CVE-2019-16714
Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。
Linux kernel 5.2.14 之前版本，由于 tos 及 flags 字段没有未初始化，net/rds/recv.c/rds6_inc_info_copy 存在信息泄露漏洞，攻击者可利用漏洞获取内核栈内存的敏感信息。

<*来源：vendor
*>

建议：

厂商补丁：
Linux

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.2.14
https://github.com/torvalds/linux/commit/7d0a06586b2686ba80c4a2da5f91cb10ffbea736

➢ Adobe Flash Player 释放后重利用漏洞

发布日期：2019-09-12
更新日期：2019-09-20
受影响系统：
Adobe Flash Player Desktop Runtime <= 32.0.0.238
Adobe Flash Player for Google Chrome <= 32.0.0.238
Adobe Flash Player for Microsoft Edge and IE <= 32.0.0.207
描述：

CVE(CAN) ID: CVE-2019-8070
Adobe Flash Player 是一款跨平台、基于浏览器的多媒体播放器产品。
Adobe Flash Player 32.0.0.238 及更早版本, 32.0.0.207 及更早版本在实现中存在释放后重利用漏洞，成功利用后可在当前用户上下文中执行任意代码。
<*来源：anonymous
*>

建议：

厂商补丁：

Adobe

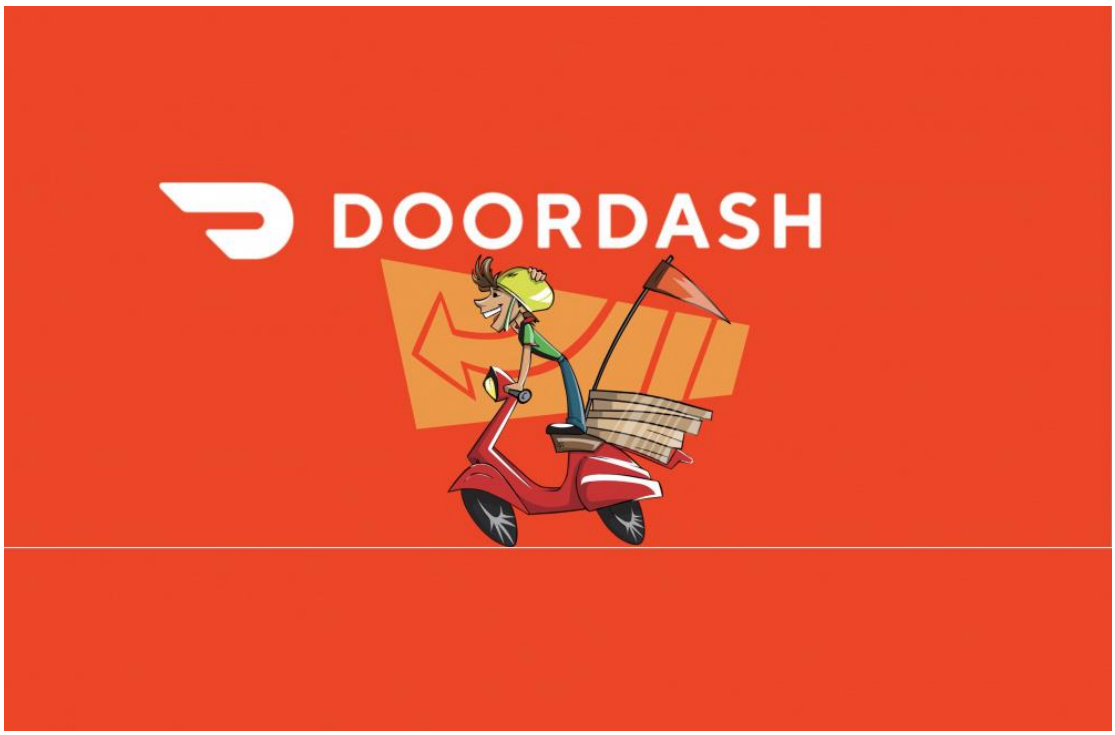
目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

https://get.adobe.com/flashplayer/
https://www.adobe.com/products/players/flash-player-distribution.html
https://chromereleases.googleblog.com/
https://portal.msrc.microsoft.com/en-US/security-guidance
https://get.adobe.com/flashplayer/
https://helpx.adobe.com/security/products/flash-player/apsb19-46.html

六、本期网络安全事件

➢ 美国外卖服务 DoorDash 数据泄露：影响 490 万人

2019 年 9 月 27 日，美国外卖服务 DoorDash 周四宣布，一项安全漏洞暴露了该公司大约 490 万客户、商家和送货员的个人数据。



这家总部位于旧金山的公司在一份声明中说，此次泄露的信息可能包括大约 10 万名送货工人的驾驶执照号码，其他数据可能包括“姓名、电子邮件地址、交货地址、订单历史记录、电话号码”等。

该公司还在声明说，一些消费者支付卡的最后四位数字也可能被暴露出来，但其中没有包含足够的数据来进行欺诈性收费。送货员和商家的银行帐号最后四位数可能已被他人访问。但该公司表示，该信息不足以进行欺诈性提款。

DoorDash 表示已采取其他措施来保护存储在其系统中的数据。该公司称，此次泄露的数据仅限于在 2018 年 4 月 5 日或之前加入公司平台的客户、商家和送货员。

DoorDash 表示，他们本月初已意识到该漏洞，并于 5 月 4 日确定“未经授权的第三方访问了 DoorDash 的某些用户数据”。

DoorDash 的一位发言人表示，该数据泄露行为涉及第三方服务提供商，目前正在进行调查。（来源：新浪科技）

➢ 电信诈骗手段翻新 制作“安全防护”冒充北京警方 App

2019 年 9 月 14 日，从北京警方处获悉，近来有一款名为“安全防护”的软件冒充北京警方的官方 App。该 App 一般与“冒充公检法”的电话捆绑出现，迷惑市民输入银行卡信息。新京报记者搜索发现，该 App 无法在应用商店下载，只能通过链接下载。对此，北京警方提示，遇到可疑电话不要轻信，更不要下载不明 App 进行操作，要尽快拨打 110 核实情况。

市民被“安全防护”骗走 6.5 万元

9 月初，林女士接到电话，对方自称是北京刑侦队的民警，查到林女士涉嫌参与多起诈骗案件，需要其配合警方调查。林女士按要求添加了对方的 QQ 号，并告诉对方自己的招商银行卡号和密码。对方称林女士名下的招商银行借记卡在几分钟前有 1.9 万余元进账，怀疑是一笔赃款。

林女士一开始并不相信对方，但查看银行账户后发现的确多出了 1.9 万余元，便以为自己真的被卷入了某起诈骗案件，只好答应对方“清查”的要求。

为了自证清白，林女士通过对方发来的链接，下载了一款号称是“北京警方官方”的 App“安全防护”，并根据提示填写了银行卡号、密码、验证码等信息。

填写完信息后，林女士发现自己的银行卡余额被人分三次转走了 6.5 万余元，这才反应过来自己被骗，随即报警。此后，林女士仔细查询交易明细发现，其招商银行借记卡多出的 1.9 万余元，其实从自己招行信用卡账户转账而来。

手机应用商店无法找到作案 App

通过警方提供的截图，新京报记者看到，该 App 制作十分粗糙。页面中有各大银行的标识，并写着“网银加密”。点击银行进入界面后，会要求填写卡号和登录密码以及交易密码等信息。新京报记者在多个应用商店搜索，均没有找到该款 App。

民警介绍，以往“冒充公检法”的诈骗案件，不法分子总是通过电话实施诈骗。但随着广大市民防范意识的提升，很多人在接到自称是警方的电话时，会直接挂掉。不法分子为了提高诈骗成功率，让受害人在短时间内相信其警察身份，会要求添加 QQ 好友。然后在 QQ 上通过捏造照片、聊天记录等信息，营造出以假乱真的形象。还会发给受害人“帮人追回欠款”的聊天记录。

在取得信任后，不法分子会要求受害人下载 App。此类 App 只能通过链接下载，迷惑性极强。在获得账户信息后，不法分子再通过名下银行卡互转等方式，让账户看起来“钱多了”。“不法分子冒充公检法的最终目的就是骗钱。警方根本没有所谓的‘安全账户’。”民警称，遇到可疑电话千万不要轻信，尽快拨打 110 核实情况。（来源：京新报）

➢ 我只想选个座，你却让我社交？航旅纵横又被曝泄露隐私

2019 年 9 月 21 日，有网友质疑航旅纵横 APP 泄露乘客隐私，称在上面选座后，陌生人可查看其姓名和头像，并受到陌生人骚扰。22 日，航旅纵横对此作出回应，但网友似乎并不买账。

女乘客使用 APP 选座后 收到陌生人骚扰信息

9 月 21 日晚，网友@喜乐喜囍 发布微博称，她在航旅纵横 APP 上选座后，有陌生人向其发送“可以约你吗”等骚扰信息。而她发现，自己也可以通过航旅纵横查看航班上其他乘客的名字和头像。

随后，多位网友在其微博下留言，表示航旅纵横 APP 上的“允许他人与我进行私聊”这一功能是默认开启状态。有些网友甚至不知道自己什么时候开启了这一功能。

9 月 24 日下午消息，针对航旅纵横 App 的社交新功能泄露用户隐私的新闻报道，航旅纵横在微博发布声明称近期个别媒体针对航旅纵横发表了泄露用户隐私等完全不符合事实的报道，对其产生了严重的负面影响，对不实报道将保留法律追诉权。

对于质疑，航旅纵横回应称出行互动功能是航旅纵横在 2018 年 6 月上线的一个探索性功能，至今未做更新迭代。该功能默认关闭，虚拟身份与真实身份也是完全隔离的。

在此次的微博声明中，航旅纵横表示一直高度重视信息安全工作，通过多种技术手段以严格保护用户信息安全，并通过了相关主管部门的审核认定。

以下是航旅纵横完整声明内容：关于个别媒体不实报道的声明

一直以来我司都欢迎社会各界提出意见和建议，对我们的工作进行监督与指导，但近期

个别媒体针对航旅纵横发表了泄露用户隐私等完全不符合事实的报道，对我司产生了严重的负面影响，严重损害了我司合法权益，我们深感遗憾，对不实报道我们将保留法律追诉权。我们特郑重澄清和声明如下：

一、出行互动功能是航旅纵横在 2018 年 6 月上线的一个探索性功能，至今未做更新迭代。该功能上线前，我们把用户隐私保护作为核心要点 进行了深入研讨，力求在用户隐私保护万无一失的基础上开展业务探索。通过建立虚拟身份开通提示确保用户在知情的情况下开启互动功能，通过用户自行设置虚拟身份信息确保用户隐私数据的绝对安全，通过建立完备的虚拟身份信息修改注销功能保证用户意愿得到充分尊重。用户间仅可以查看到虚拟信息，不存在个人隐私数据泄露问题。

二、该功能是默认关闭的，上线初始时所有用户的虚拟个人主页均默认为关闭状态。用户上线后点击该功能开通虚拟身份前，会弹窗增强式 告知明确提示虚拟身份用于与他人互动。只有用户同意建立后才会开启，用户不建立虚拟身份也不会影响任何其他功能的使用，截至目前仍 有很多用户根据个人需求未开启此项功能。

三、虚拟身份与真实身份是完全隔离的。虚拟身份不仅是由用户根据 自己的意愿自主选择是否开启，且所有包含的内容都需要用户逐项手动 添加或选择。用户也可以随时对填写的内容进行修改，用户对于功能的开启、使用及关闭都有充分的自主权。用户开通虚拟身份后，仅通过用户自主填写的内容他人才可见，而用户的个人真实信息他人是无法看到的，不存在任何用户个人隐私泄露的问题。

四、虚拟身份只需用户在底部菜单栏点击“我”进入账户信息页，在账户信息的授权管理中即可注销。航旅纵横致力于帮助用户建立一条获取 权威信息的智能通道，每一个真实用户只能注册一次，为保护用户权益，在注册过程中需进行严格的身份认证。如用户不再使用航旅纵横，希望注销航旅纵横主账号时，同样需要核实用户真实身份，以避免他人盗用，保护账号使用者的权益。

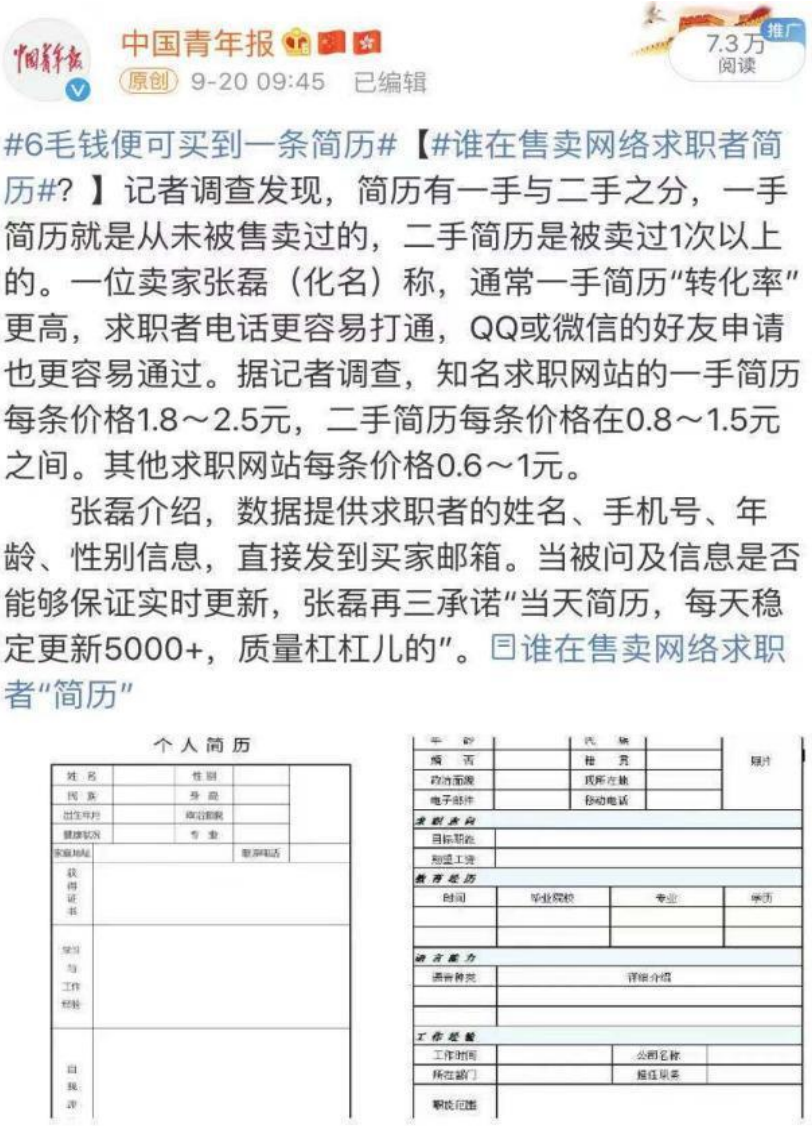
航旅纵横一直高度重视信息安全工作，通过多种技术手段以严格保护用户信息安全，并通过了相关主管部门的审核认定。航旅纵横始终致力于探索利用创新技术提升民航业整体服务水平，得到了行业和广大用户的高度认可，并被上级部门评价为改革开放 40 年国有企业在互联网领域 取得的重大突破。未来我们也将继续坚持以用户为核心，为广大用户提供更加高效、便捷的服务，为民航行业注入更多的科技元素。（来源：互联网综合整理）

➢ 冲上热搜大学生的简历，一份只值一块钱？

2019 年 9 月 21 日，刚大学毕业不久的郭某急于找工作，在网上向几家公司投递了简历，之后竟频繁接到陌生电话和短信，提供的都是一些莫名其妙的职位。记者调查发现，目前，网上简历售卖市场十分活跃，已形成“一条龙”产业。不法分子通过各种形式以正规企业身份入驻网络求职平台获得求职者简历，卖家出售的商品从简历获取的软件与账号、再到简历，一应俱全。

完整的“简历收集”产业链

记者在网络商贩手中购买了 100 份某知名求职网站的简历，求职意向涵盖美术指导、律师、翻译、缝纫、淘宝客服等多个行业。记者随机选取了 10 份简历，对其中信息进行核实。求职者中至少有 3 位曾受到过不同程度的信息骚扰。



中国青年报
原创 9-20 09:45 已编辑
推广 7.3万 阅读

#6毛钱便可买到一条简历#【#谁在售卖网络求职者简历#？】记者调查发现，简历有一手与二手之分，一手简历就是从未被售卖过的，二手简历是被卖过1次以上的。一位卖家张磊（化名）称，通常一手简历“转化率”更高，求职者电话更容易打通，QQ或微信的好友申请也更容易通过。据记者调查，知名求职网站的一手简历每条价格1.8～2.5元，二手简历每条价格在0.8～1.5元之间。其他求职网站每条价格0.6～1元。

张磊介绍，数据提供求职者的姓名、手机号、年龄、性别信息，直接发到买家邮箱。当被问及信息是否能够保证实时更新，张磊再三承诺“当天简历，每天稳定更新5000+，质量杠杠儿的”。#谁在售卖网络求职者“简历”

记者调查发现，简历有一手与二手之分，一手简历就是从未被售卖过的，二手简历是被卖过 1 次以上的。一位卖家张磊（化名）称，通常一手简历“转化率”更高，求职者电话更容易打通，QQ 或微信的好友申请也更容易通过。

据记者调查，知名求职网站的一手简历每条价格 1.8～2.5 元，二手简历每条价格在 0.8～1.5 元之间。其他求职网站每条价格 0.6～1 元。张磊介绍，数据提供求职者的姓名、手机号、年龄、性别信息，直接发到买家邮箱。当被问及信息是否能够保证实时更新，张磊再三承诺“当天简历，每天稳定更新 5000+，质量杠杠儿的”。

提取出来的简历都是真实信息，并且实时更新

除简历买卖外，企业 VIP 账号的子账号、辅助软件在网上均有出售。当下获取简历最主要方式是通过企业账号发布招聘信息，等待求职者投递简历，再将简历提取出来售卖或直接利用。

知情人士赵峰（化名）透露，在一些知名求职网站上，只有通过认证的企业账号才有权下载简历。认证企业需要准备营业执照和该网站没有认证过的账号，行话称为“白号”。一般来说，一张营业执照可认证 3～5 个白号。

记者调查发现，网上有专门出售用于注册白号的软件，可以帮助买家批量注册白号，价格在每月 100 元以上。另外，营业执照也可以批量购买。理论上，发的招聘信息越多，收到的简历数量就越多。赵峰说：“能否吸引到求职者，还要看话术。”网上还专门售卖“发帖机”

软件，价格在 300～400 元/月。另外还有软件可以将帖子刷新，使帖子排名更高。最后，根据平台服务，利用“简历提取器”，以文本形式提取出求职者简历信息。

“简历收集”产业链一经曝光，话题#1 元即可购买一条简历#迅速冲上微博热搜：不少网友都表示自己有过简历信息泄露的经历！

法学教授：平台方应担起责任

网络简历贩卖是窃取公民个人信息的违法行为。苏州大学王健法学院民商法学教研室张鹏教授指出，简历买卖涉及到多方面侵权问题。而求职简历软件开发和简历购买者的行为，已构成共同侵权。

张鹏还说：“平台应当承担一定的数据安全保障和严格审查的义务。”在网站设计、网站建设维护过程中，平台有义务保障用户信息安全。如果用户信息泄露，但平台无所作为，则要承担间接责任。

根据刑法第二百五十三条之一规定：“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。”（来源：人民日报）

➢ 黑客两周攻破 600 余网站 还未“领赏”就在十堰落网

2019 年 9 月 26 日，自学计算机网络技术,在国外“深造”黑客技术,回国组建“黑帽团队”,以广告推广为幌子,入侵数百家网站,预留后门、植入恶意脚本修改他人网站首页,妄图为赌博网站做推广牟利“发家致富”……

近日从湖北省公安厅获悉,今年 8 月,十堰市公安局网安支队在开展“净网 2019”专项行动中侦破一起破坏计算机信息系统案,打掉一黑客犯罪团伙,有效净化了网络空间。

据悉,今年 3 月底,十堰市公安局民警在十堰市茅箭区上海路一处住宅小区走访时,有居民反映居民楼内有几名租住小青年比较可疑。经检查,民警在住宅内发现 3 名男青年熊某学、龙某和吴某,房间配备有多台电脑,还散布着移动硬盘、U 盘、移动上网卡等大量电脑网络设备。

3 人自称是从事广告推广业务,但对经营模式和具体工作任务语焉不详。这引起了民警的怀疑,遂将 3 人传唤至公安机关进一步调查。经了解,熊某学等 3 人自称“黑帽黑客团队”,他们蜗居小区的目的是攻击境内正常网站,获取网站管理权后对原网站进行修改,植入早已准备好的境外赌博公司网页,向境内公民推广网络赌博业务,招揽“顾客”,进而赚取不法利益。

所谓“黑帽黑客”,是利用黑客技术,破解网站或软件,牟取私利的网络黑客。

熊某等人以“黑帽”自居,引起了公安机关的高度警惕。十堰市公安局迅速组成专班,提

取了这个窝点内的笔记本电脑、上网卡等相关物证,并对相关电子物证进行了鉴定、分析。

经深入侦查,办案民警发现,19 岁的熊某学是这个“黑帽团队”的技术骨干和核心。2018 年,熊某学在网络上结识了在境外从事网络赌博违法犯罪活动的李某海,他多年练就的黑客技术获得了李某海的“赏识”。应李某海的邀约,熊某学出境到某赌博公司供职,主要任务是为网络赌博提供技术支持、网站维护及广告推广等。

其间,熊某学学到了大量赌博网站推广技术,并窃取拷贝了多种黑客攻击软件工具及木马文件,还结识了从事同样工作的龙某等人。今年年初,李某海决心自立门户,开设网络赌场,他高薪邀约熊某学加入,并指使自己的表弟吴某加强与熊某学、龙某的联络,意欲在境内开展网络攻击,进而推广自己的网络赌场,招揽“业务”。

高薪聘请技术人员、提供食宿,配备高端电脑,租用高性能网络服务器……李某海精心“构筑”的窝点很快搭建起来了。

今年 3 月中旬,熊某学、龙某、吴某杰相继从外省齐聚十堰,开始启动他们的“业务”。安排妥当后,李某海离开境内,远赴国外。

熊某学和吴某、龙某分工协作,熊某学负责攻击、渗透目标网站,拿下网站或服务器的控制权,这个步骤称之为“拿站”。

在熊某学“拿站”成功后,龙某负责给受害网站植入木马或链接,使这些网站在被访问时跳转到他们指定的赌博公司广告页面。吴某则负责给二人打下手。

首次出击,熊某盯上一款用户常用网站建站模板,此建站模板在我国北方地区使用广泛,很多中小企业和个人选择使用此模板建设自己的网站,但此软件的低版本存在一些安全漏洞。

在高性能网络云服务器的帮助下,这个团伙的攻击效率很高。很短时间内,熊某就筛选出可以利用的目标网站 1.88 万个,并制成文档,存放在移动硬盘内备用。熊某学对筛选出的网站进行各个击破。据熊某学交代,短短两周,他就攻破了 600 多个网站。民警立即赶赴相关网络公司和单位开展调查取证。

经过仔细甄别,警方查明,一部分被攻击的网站已进行了修复,有证据证实被破坏的网站仍有 260 多家,涉及河北、吉林、辽宁 3 省 12 个地市。

因“工作”时间不足一个月,熊某学等 3 人还没来得及领取李某海承诺的高薪。8 月初,熊某学等 3 人被公安机关以破坏计算机信息系统罪依法移送审查起诉,李某海也被上网追逃。目前,十堰市公安局已与相关网络公司联系,以便及时堵塞网站漏洞,避免损失扩大或被再次入侵。

警方提醒：

- 黑客攻击极易导致公民个人信息泄露,进而被个别别有用心的犯罪分子利用,用于精准诈骗等违法犯罪活动。个人用户在使用互联网和计算机系统时,不要登录来历不明的网站,重要数据及时备份,定期对计算机进行安全扫描,修补漏洞；正确使用网络防火墙,封堵黑客攻击渠道；定期下载系统补丁,对计算机系统进行升级、打补丁,有效杜绝黑客入侵。
- 企业用户在建设网站和部署其它互联网项目时,应做好访问控制、入侵检测技术和安全扫描,尽量使用安全度较好的软件系统,并及时更新升级,有条件的可聘请专业人员进行网络安全管理。（来源：中国经济周刊）

➢ 全国 30 多万台手机被“控制”！手机没出厂就被装了木马

2019 年 9 月 19 日，你的手机号码被恶意注册了网络账号，成为犯罪团伙的“掩护马甲”，你还蒙在鼓里？昨日，省公安厅召开“净网 2019”专项行动发布会。广东警方重拳打击整治网络黑产犯罪，着力斩断为各类网络犯罪提供服务的引流支撑、技术支撑、账号支撑、支付支撑。

据了解，网络黑产主要分为四类：一是引流推广类，利用各类网络资源，为网络黄赌平台、网络诈骗网站等进行广告投放和信息推送，增加网络流量。二是技术服务类，提供恶意脚本编写、钓鱼网站搭建、网站攻击渗透、网络流量劫持等技术开发运维服务。三是账号支撑类，利用他人身份信息或手机号码恶意注册大量网络账号，为犯罪团伙提供“掩护马甲”。四是支付通道类，包括第四方支付平台、虚拟货币交易平台等，利用监管漏洞，为犯罪团伙提供隐蔽的资金流转、结算渠道。

今年以来，全省共侦破网络黑产案件 730 余起，刑事拘留 7460 余人，缴获被泄露窃取买卖的公民个人信息 40 亿余条，同比分别上升 20.55%、16.55%、447.94%。

案例：杂牌机植入木马黑客程序 全国被控制手机 30 余万部

今年 7 月，省公安厅网警总队侦获一非法获取计算机信息系统数据黑客线索。经侦查，深圳某科技有限公司为多家杂牌手机厂商提供终端系统方案，在还未出厂的手机操作系统底层植入木马黑客程序，只要用户买了手机插入电话卡，在不知情的情况下，其手机号码就被黑客程序控制。

同时，该公司搭建多个接收手机验证码平台，结合事先植入手机操作系统底层的木马黑客程序，把接收到的手机号码和短信验证码用于为下游黑产业团伙提供各类网络账号注

册服务，每次接码服务费用 0.4 至 2.5 元不等。

经腾讯守护者计划安全团队技术分析，短信验证码回传后，后台即删除、屏蔽相关短信，导致手机用户无法发现自身号码被他人利用注册网络账号。这些网络账号被提供给下游网络诈骗、网络水军、“薅羊毛”等黑产业犯罪团伙使用，形成“手机系统开发商-手机硬件厂商-接码平台-下游黑产业团伙”的犯罪链条，全国被控制手机 30 余万部，由此形成了规模庞大的手机“猫池”。

9 月 2 日，在摸清掌握了犯罪团伙的组织架构以及涉案人员的相关信息后，专案组在深圳、上海等地同时开展收网行动，抓获犯罪嫌疑人 63 人，查获涉案手机主板、电脑、手机、银行卡等物品一大批，实现对该犯罪团伙的手机系统开发商、手机硬件厂商、接码平台、下游黑产业团伙的全链条打击。该案是全国首例打击预装手机后门获取验证码注册网络账号的网络黑产案件。

警方提醒广大群众：购买手机时要通过正当渠道选择正规品牌的手机。如果发现手机号码有被盗用或者被利用实施违法犯罪活动时，应及时向公安机关报案。（来源：广州日报）

信息安全意识产品年服务

021-33663299