国盟信息安全通报

2019 年 11 月 25 日第 206 期

国盟信息安全通报

（第 206 期）

国际信息安全学习联盟

2019 年 11 月 25 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 541 个，其中高危漏洞 142 个、中危漏洞 334 个、低危漏洞 65 个。漏洞平均分值为 5.67。本周收录的漏洞中，涉及 0day 漏洞 212 个（占 39%），其中互联网上出现“TP-LINK TL-WR940N 和 TL-WR941ND 缓冲区溢出漏洞、Belkin Linksys EA6500 路径遍历漏洞”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 3140 个，与上周（7452 个）环比减少 58%。

主要内容

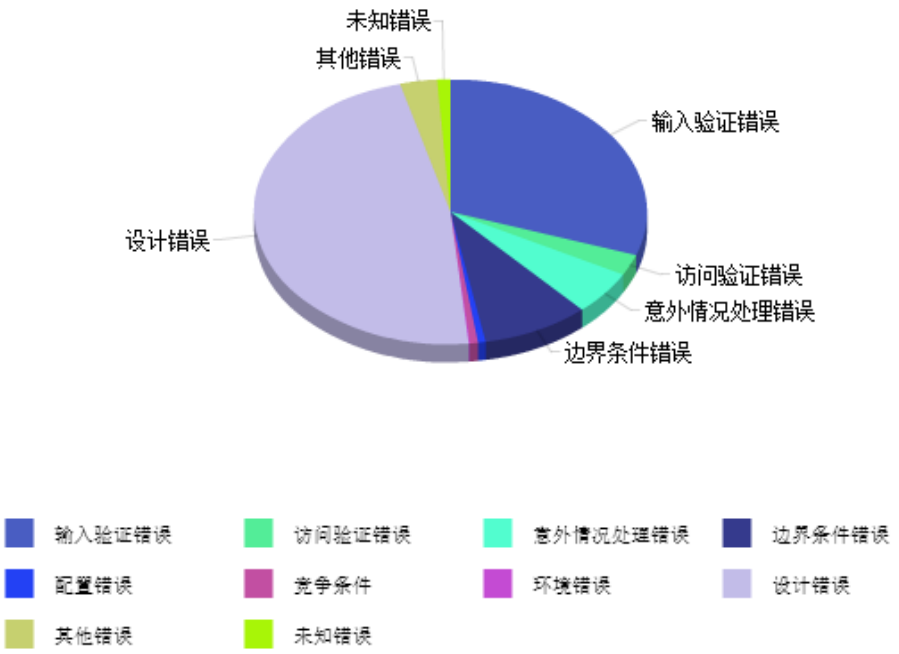
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

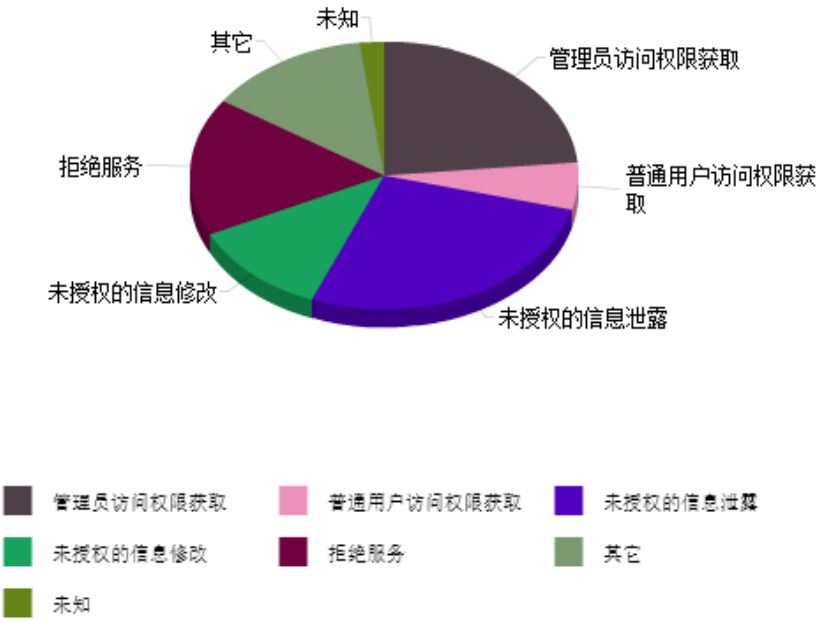
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 541 个，其中高危漏洞 142 个、中危漏洞 334 个、低危漏洞 65 个。漏洞平均分值为 5.67。本周收录的漏洞中，涉及 0day 漏洞 212 个（占 39%），其中互联网上出现“TP-LINK TL-WR940N 和 TL-WR941ND 缓冲区溢出漏洞、Belkin Linksys EA6500 路径遍历漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3140 个，与上周（7452 个）环比减少 58%。

二、安全漏洞增长数量及种类分布情况

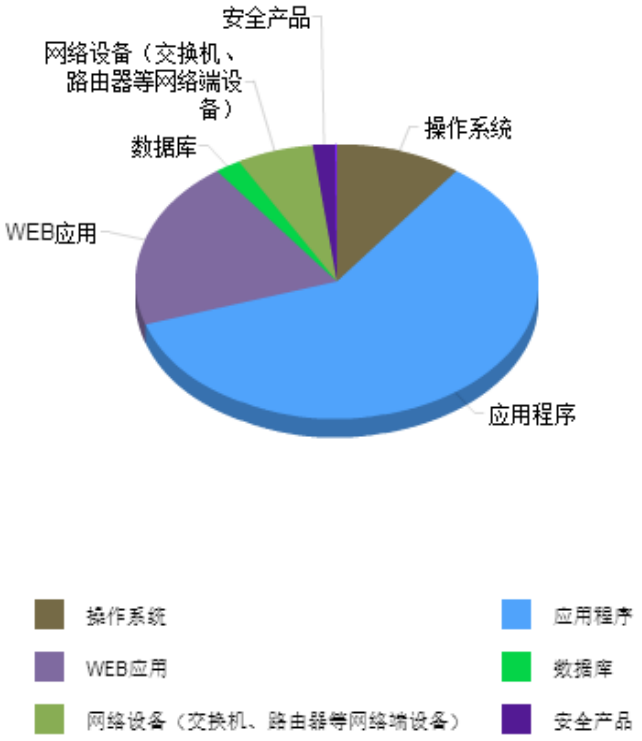
➢ 漏洞产生原因（2019 年 11 月 11 日—2019 年 11 月 25）



➢ 漏洞引发的威胁（2019 年 11 月 11 日—2019 年 11 月 25）



➢ 漏洞影响对象类型（2019 年 11 月 11 日—2019 年 11 月 25）



三、安全产业动态

➢ 共筑网络安全防线的四重路径

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，网络安全牵一发动全身。党的十八大以来，以习近平同志为核心的党中央准确把握时代潮流，立足我国互联网发展与治理实践，站在战略高度和长远角度，在维护网络安全、培养网络人才、创新网络技术等方面作出一系列重要部署，为做好网络安全工作提供了根本遵循和强大动力。当前，随着新一轮科技革命和产业变革加速演进，人工智能、大数据、物联网等新技术新应用新业态快速发展，互联网迎来了更加强劲的发展动能和更加广阔的发展空间。网络安全领域也面临着更多、更新、更复杂的挑战，安全发展任重而道远。

不久前，习近平总书记对国家网络安全宣传周作出重要指示，强调要坚持安全可控和开放创新并重，提升广大人民群众在网络空间的获得感幸福感安全感。这一重要指示，为共筑网络安全防线指明了方向。

1、保障个人信息网络安全

网络空间并非“虚拟”，而是与民众生活息息相关。习近平总书记强调，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。

保障个人信息网络安全，关键是要明确主体的社会责任。对于网络治理，习近平总书记一直非常注重党政、企业齐抓共管，良性互动，他明确要求，“企业要承担企业的责任，党

和政府要承担党和政府的责任，哪一边都不能放弃自己的责任”，“要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任”。企业越大，责任越大。习近平总书记多次强调要压实互联网企业的主体责任，决不能让互联网成为传播有害信息、造谣生事的平台。要建立健全企业网络安全、数据安全审查制度，提升网络安全防护综合能力，加大与公安、工信等部门联动，依法保障个人信息网络安全。

保障个人信息网络安全，基础是要提升全民网络安全意识和防护能力。各级党委、政府和领导干部应依托各级网络平台，以人民群众通俗易懂、喜闻乐见的形式，进行网络安全宣传教育，充分调动广大人民群众的力量，增强他们的责任感、使命感、紧迫感，让人人成为网络安全的维护者，个个争当网络安全的建设者；鼓励人民群众参与到网络安全的工作中，借助广大群众的力量发现网络安全隐患、识别网络安全问题、举报网络违法分子、应对网络安全风险；依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，切断网络犯罪利益链条，持续形成高压态势，维护个人信息网络安全。

2、构建网络安全良性生态

网络空间是亿万民众共同的精神家园。网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。习近平总书记强调，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。

构建网络安全良性生态，需要营造清朗的网络空间。当前，互联网已经成为各种政治信息、思想文化快速传播、扩散的主渠道，各种思想文化碰撞的平台、利益诉求的集散地和意识形态较量的战场，拓展了人们政治生活的新空间，冲击着人们的思想观念。习近平总书记指出，要加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间。因此，要做强网上正面宣传，推进网上宣传理念、内容、形式、方法、手段等创新，把握好时度效，运用网络传播规律，培育积极健康、向上向善的网络文化，用社会主义核心价值观和人类优秀文明成果滋养人心、滋养社会，做到正能量充沛、主旋律高昂，主动抢占网上制高点，引导互联网向着积极、健康的方向发展。

构建网络安全良性生态，需要核心技术和人才的支撑。网络安全的核心是技术安全。网络千变万化，网络安全是技术更新最快的领域，要进一步推动信息领域核心技术突破，攻破技术堡垒，占领网络安全制高点。习近平总书记强调：“网络空间的竞争，归根结底是人才竞争。建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。念好了人才经，才能事半功倍。”为此，应研究制定网信领域人才发展整体规划，

推动人才发展体制机制改革，培养网络安全人才，夯实网络安全根基，更好地推动技术创新和产业发展。

3、依法加强网络空间治理

网络空间的虚拟性不能遮盖参与主体的现实性，网络空间不是“法外之地”。习近平总书记强调，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。

法规建设是规范网络空间治理的重要基础。法律是治国之重器，良法是善治之前提。立足长远发展，扭住现实急需，做好网络立法工作，明确网络主体的发展责任，规范网民的网络信息行为，引导网络新技术应用，是依法治理网络空间的出发点和落脚点。近年来，我国加快了互联网立法进程，相继制定出台了《中华人民共和国网络安全法》《国家网络空间安全战略》《网络空间国际合作战略》等一系列法律法规，为推动依法治网奠定了法律基础。但面对依然严峻的网络安全形势，仍需要积极构建包括国家法律、地方法规、行业管理办法等多层面的网络安全立法体系框架，全面推进规范网络空间的法规建设，加强重点领域立法，坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。

打造良好的网络空间环境离不开法治保障。依托法治，促进科学技术与立法体系相融合，持续提升有效治理网络空间的各项能力。协调政府、企业、社会团体以及个人等多方力量参与网络空间治理，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。同时，注重发挥法治的引领和规范作用，大力培育有高度的安全意识、文明的网络素养、守法的行为习惯、必备的防护技能的中国好网民，确保共建共治共享。

4、共建网络空间安全共同体

网络安全，已经成为困扰各国的世界性难题，加强国际合作，共同推进网络空间全球治理，努力推动构建网络空间命运共同体，是行稳致远之道。习近平总书记强调，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。

共建网络空间安全共同体，需要坚持走互信共治之路。网络空间作为“第五疆域”，治理边界最广，治理难度最大，治理挑战最多，需要各国携手应对风险挑战，齐心共担治理责任。习近平总书记指出，中国是网络安全的坚定维护者。中国也是黑客攻击的受害国。国际社会应该本着相互尊重和相互信任的原则，共同构建和平、安全、开放、合作的网络空间。当前，新技术发展为各国合作应对网络风险、开展共同治理提供了坚实保障。各国应加强网

络空间的相互信任，深化务实合作，以共进为动力，共赢为目标，走出一条互信共治之路，让网络空间命运共同体更具生机活力。

共建网络空间安全共同体，需要建立和完善网络空间国际规则。网络安全是全球性挑战，没有哪个国家能置身事外、独善其身。习近平总书记率先提出了推进全球互联网治理体系变革应坚持的“四项原则”（尊重网络主权、维护和平安全、促进开放合作、构建良好秩序）和“五点主张”（加快全球网络基础设施建设，促进互联互通；打造网上文化交流共享平台，促进交流互鉴；推动网络经济创新发展，促进共同繁荣；保障网络安全，促进有序发展；构建互联网治理体系，促进公平正义）。他旗帜鲜明地指出，中国愿同各国一道，加强对话交流，有效管控分歧，推动制定各方普遍接受的网络空间国际规则。为此，应实现互联网技术、法律和政策等诸领域的协调与融合；妥善处理网络空间冲突，彼此尊重网络主权，有效应对网络恐怖主义、网络犯罪、网络诈骗等跨国性难题，加强网络安全合作；推动互联网全球治理体系变革，建立多边、民主、透明的全球互联网治理体系。（来源：光民日报 作者：周爱民，系湖南省中国特色社会主义理论体系研究中心研究员、中共湖南省委党校教授）

➢ 我国网络安全的特点、成就、趋势

我国的网民数量和网络规模均居世界第一，网络已经深度融入人们的学习、生活、工作。大数据、云计算、物联网、移动互联等技术的发展融合，导致安全风险复杂叠加并快速演化。维护我国网络安全，对于保障我国改革、发展和稳定，维护国家网络空间主权、安全和利益，都极其重要。

网络安全形成中的特点

从互联网建设开始，安全即登上网络舞台。我国网络安全工作在遵循普遍性要求基础上，体现了自身的特点。

网络安全主要靠技术和服务来治理。我们更多借助安全软件、安全硬件等技术和产品来保障网络安全，运用建设和服务的手段维护网络安全，初期运用中难免技术欠缺，管理较粗放，很难保证网络运用中数据的完整、保密、可用。针对问题，创新技术，加强维护，保障安全。技术的改进和网络质量的提高，弥补了网络安全漏洞，改善了网络安全环境。我国网络建设没有完全以资本、利润、市场来决定，而是照应边远贫困地区和广大农村的需要，正是网络技术共享的理念和实践，避免了网络贫富鸿沟，保持了网络秩序和安全。

网络安全立足发展中大国的实际。我国比一些发达国家铺的网络广、建的基站多，城镇、乡村一样建，从网络角度改善了农村、边疆的教育和医疗条件，提高了边远地区人口素质和文明水平，促进了扶贫事业的发展，减少了因贫穷发生各种风险的可能，更好地维护了安全和稳定。电商渗透到城乡村落，解决了大量就业，缩小了购物成本，从网络建设角度保障了人们的生存权和发展权。这些有益于群众的事业自然得到群众拥护，其实维护群众和国家的利益本身就是网络安全的目的。政府和企事业单位的信息公开和自媒体的发达，拓宽了获取信息和社交沟通的渠道，保障了基层群众的知情权。政府持续力推网络提速降费，让利于民，增强了公民网络权益的获得感。网络成为群众生活的一部分，群众成了网络安全最大的防护力量，防范了信息不公开、不对等引起的各种猜忌、思想混淆和恶意利用。

网络安全发展中的成就

遵循国家网络安全战略，防范风险，管技结合，加强防护，保障了经济社会发展和国家安全。

技术上打造坚实的网络安全基础。网络高度依赖技术，维护网络安全必须采取技术手段。一是夯实网络主权和安全的技术基础。在网络信息、网络安全和网络人权保护技术方面，我们取得了一定成效，但是核心技术和关键基础设施受制于人，成为我国网络安全的软肋。这些年实施网络信息核心技术设备攻坚战略，推动高性能计算、移动通信、量子通信等研发和应用取得重大进展，改进了我国网络安全的状况。二是建立常态化网络安全的技术漏洞修补机制。技术的局限性只有通过技术进步的方式克服，而不是通过否定技术本身的方式进行。

在充分吸收技术成果中，消除技术运用中的垃圾堆积、隐私泄露等安全问题，形成良性循环系统。我国的网络设备制造商、运营商和互联网企业，创新各自涉及的技术，加强关键网络设施维护，有效利用和安全处理网络数据，降低违反安全法规的风险。政府积极主导建立信息安全和数据管理体系，促进了信息安全和开放共享标准更加规范，解决了数据失控带来的风险。三是探索用大数据和区块链实施监管的技术问题。互联网、物联网、云计算、大数据、AI 等是生产力的新要素，而规划、市场、考核等管理手段仍然陈旧。一些信息互联网企业和平台，尝试将大数据、区块链纳入监管手段体系，为生产关系注入新要素，运用大数据让过去把握不准的东西变得更加清楚。发挥区块链去中心、多节点、防抵赖的特点，在电子商务、地图导航、快递外卖等方面，尝试解决传统管理出现的安全问题。

监管上致力于防范和打击网络侵权。解决网络安全问题多措并举，打防结合，净化网络，持续建设。一是对党政机关和重要行业的木马僵尸、恶意程序、网站安全、安全漏洞等网络安全事件，加强网络防护和治理。开展对计算机恶意程序的打击，关闭控制规模较大的僵尸网络，切断黑客对境内感染主机的控制。二是对公民网络隐私权问题，关注用户投诉，督促处理和整改，由监督机构和司法部门处理网络侵权行为。三是针对网络传播盗版影视作品、传播色情、鼓吹暴力等问题，开展网络安全教育，引导文明上网。查办网络盗版案件，实施行政处罚和刑事打击。打击制售、传播非法有害出版物及信息的活动，净化网上文化环境，维护未成年人权益。四是针对网络诈骗，侦查网络诈骗案件，查处违法犯罪人员，努力避免和挽回群众损失。

规范上推进网络文化基础上的建制立法。在网络安全实践基础上，形成了包括虚拟、匿名、交互、广域、迅捷等网络秉赋的文化，开放、平等、角色多重、媒体性质的网络社群礼仪观念，网络空间、网络公民、网络人权、网络权利的网络法治理念。在吸收网络文化思想基础上，形成了网络方面的两类规范性内容。一是网络安全的法律法规，如网络安全法、网络信息保护决定等。二是网络安全监管的行政法规和政策性文件，如信息网络传播权保护条例、计算机软件保护条例、推动资本市场服务网络强国建设的指导意见、政府网站集约化试点工作方案等。网络法律法规的体系化建设，保障了网络安全的规范和维护。

网络安全展望中的趋势

信息互联网技术正从人人互联向万物互联演进，现实世界和数字世界日益融合，需要把握网络趋势，争取自主权，创造安全有序的网络未来。

网络安全将在全球化与逆全球化的矛盾中曲折推进。全球化和互联网发展是时代潮流。各国主权范围内的网络事务应由各国人民自己做主。我们要与各国分享发展机遇、共享发展

成果、参与网络空间治理，加大在技术交流、打击网络恐怖和网络犯罪等领域的密切合作，健全多边、民主、透明的国际互联网治理体系，推进建设网络空间命运共同体。

网络安全将在与经济科技文化社会的交融中前行。要统筹网络安全和经济社会发展，不能以经济利益、科技创新、文化差异挤压网络安全。安全是发展的前提，任何以牺牲安全为代价的发展都难以持续。网络上的技术、监管、执法、维权等问题，反映了网络安全与经济、文化、科技、社会等方面的关系状况，我们要在网络安全与各方面关系上，把握好整体与局部、长远与短期的适度，加强网络伦理和文明建设，发挥道德教化作用，打击网络诈骗、网络盗窃、侵害公民信息、传播淫秽色情、黑客攻击、侵犯知识产权等违法犯罪行为。

网络安全在线上线下的配合和交互作用中改进。网络更新换代呈现出一波波新现象，需要我们借鉴传统安全的维护经验。把网络安全作为社会共同责任，网络安全工作者要注重客户体验，以产品和服务融合的方式解决问题；网络用户要经常检查自己的数据和分类，以防在动态中失去对数据的控制。建立线上线下配合交互的网络安全机制，防止有人利用线上线下不同的特点和间隙搞投机，维护全方位安全。

网络安全在人工智能和机器人的挑战中发展。随着人工智能和机器人技术的飞速发展和广泛运用，要关注其带来生活便利和经济效益中忽视网络安全的情况，要把人工智能也应用到网络安全上，使其自动检测，整合问题信息，并在处置基础上，推送疑难问题，提醒专业人员分析解决。要高度重视人工智能涉及人类进化的问题，把人脑与计算机、人脑与网络的连接作为重要网络安全问题。

网络安全在开放共享与管理秩序中博弈互动。网络的开放共享与网络的管理秩序互为条件。没有秩序就没有平等、民主和共享，为此，要依照有关规章制度监管网络，依法治理网络，鼓励公民拿起法律武器，捍卫自己的权利，维护网络秩序，促进公平利用和共享网络资源。（来源：光明网，北京大学中国战略发展研究中心常务理事 邵春保）

➢ 把更多精力放在打击网络犯罪上

日前，最高法发布《司法大数据专题报告之网络犯罪特点和趋势》。据统计，2016 年至 2018 年，网络犯罪案件已结 4.8 万余件，案件量及在全部刑事案件总量中的占比均呈逐年上升趋势。2018 年，微信超过 QQ 成为网络诈骗犯罪中使用最为频繁的犯罪工具，超半数网络诈骗案件中均有涉及应用微信实施诈骗的犯罪情节。

互联网就像一种中性“吸附剂”，优劣、良莠、善恶都会被它吸上来，网络犯罪就是恶的代表。随着互联网的普及与发展，传统违法犯罪不断向网上转移、渗透、蔓延，网络犯罪已成为许多国家第一大犯罪类型。据公安部透露，网络犯罪已占我国犯罪总数的三分之一，且呈不断上升态势。网络黄赌毒、盗窃、诈骗、传销、贩枪、传授制爆技术、窃取公民个人信息等违法犯罪增多，严重影响公共安全。

相对于传统违法犯罪，用大数据“画”出的网络犯罪，轮廓更加清晰、特征更加明显。比如说，犯罪主体低龄化，年龄在 18~30 岁之间的占了多数；犯罪方法智能化，网络犯罪分子往往具备专业技能；犯罪行为隐蔽化，网络的开放性和虚拟性使得网络犯罪具有极高的隐蔽性；犯罪结果扩散化，跨地域、跨国界特征非常明显；犯罪目的牟利化，非法敛财是主要目的；犯罪组织团伙化，与以往“简单结伙”“单兵作战”不同，如今的网络犯罪，组织化特点日益明显。

以“杀猪盘”诈骗为例，它就是一种集上述诸多特征于一身的网络犯罪。诈骗分子往往在各大婚恋交友网站或社交平台先寻找目标，然后以婚恋交友为幌子把他们诱骗到早已设计好的境外网络平台进行赌博或投资，从而进行“杀猪”（诈骗）。此类犯罪分子多半是年轻人，通过团伙操作，且网络平台设在境外，手段高明、行为隐蔽。

传统违法犯罪逐渐向网上转移，新型网络犯罪不断涌现，双重不利因素叠加，让网络安全形势日益严峻。鉴于此，外部监管也要将更多精力放在网上，在打击网络犯罪上投入更多

人力、物力、财力，保障网络一方平安。针对网络犯罪方法智能化，打击网络犯罪要注重智力投入，与犯罪分子斗智斗勇。公安机关必须提升侦查整体能力，实现技术的全面革新，引入更高阶的技术侦查手段，以专治专，以快制快，彻底扭转反制网络犯罪工作中“猫鼠不同步”的被动局面。

针对网络犯罪存在跨地区、跨国界问题，打击网络犯罪要突破体制机制障碍，建立起更广泛、更高效的合作机制。在跨地区执法上，以条块架构组织起来的传统执法模式，难以适应网络犯罪的流动性与扩散化特点，导致打击网络犯罪过程中存在效率较低、成本较高、时效性较差等问题；在国际合作过程中，由于各国及地区的法律不同、国际合作不顺畅、审批程序烦琐，导致沟通不力、协作效率低下。打击网络犯罪要“内”“外”兼修，在两个维度都有所突破，从而整体提升打击效率。

针对网络犯罪团伙化、专业化，打击网络犯罪要多方形成合力，公安机关、司法部门、网络服务提供者、社会组织、用户个人都有合作义务。尤其是网络服务提供者，它是网络生态环境的主要创建者、网络活动规则的主要制定者，与包括违法犯罪者在内的服务接受者共生互利，有责任也有能力向社会提供安全的网络产品和服务，而不是秉持所谓的“中立”。既然超半数网络诈骗案件中均有涉及应用微信实施诈骗的犯罪情节，那么腾讯公司就该更好履行早前的承诺，以更高阶的技术对抗与防御，让网络犯罪从“事后防御”“事中拦截”扩展到“事先预警”，从而降低犯罪发生率。

打击网络犯罪，事关网络安全、社会稳定、百姓幸福，必须众志成城、同心协力，打一场以正压邪的人民战争。（来源：广州日报）

➢ 落实“四个坚持” 创新人才培养模式

中共中央总书记、国家主席、中央军委主席习近平对今年国家网络安全宣传周作出重要指示，强调：“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。”习近平总书记还曾提出：“网络空间的竞争，归根到底是人才的竞争”。在网络强国建设的过程中，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以想象的。

目前，我国最大的短板和主要问题困难是：一是没有全面掌握网络的核心关键技术，二是网络安全人才严重缺乏。这必然会影响建设网络强国、维护和保障国家网络安全和网络主

权。随着大数据、5G 技术、移动网络、人工智能、物联网等快速发展，网络安全问题日益突出，保障网络安全、维护国家网络主权显得更加重要和紧迫。

要解决我国网络安全人才严重短缺和提高网络安全人才的全面素质问题，既要加强加速高等学校对高素质网络安全专门人才的培养，更要加强加快加大对网络安全人才的岗位技能培训。因为高校每年只能招收 3 万多人，远远解决不了网络安全人才短缺和社会急切需求的问题。要加强加快加大对网络安全人才的岗位技能培训。要充分发挥高校、科研机构、企业和社会民间力量对网络安全人员培训的作用，加强对网络安全岗位人员的培训，是解决网络安全人才短缺和提高素质的重要举措，否则，在很长的时间内这个问题都无法得到解决。

根据目前社会对网络安全人才的需求,以及网络安全人才教育培训的现状和困难，既要加强学历教育，加强高素质高级专门人才的培养,必须加强网络安全基础理论、学科专业体系的构建，制定特色鲜明的人才培养方案，设置好核心骨干课程和实验实训课目，编写好相关教材。网络安全是一门交叉学科，涉及理、工、法、管等学科，理论性、技术性、应用性、实践性、敏捷性等非常强，必须培养复合型人才。同时，又要加强对网络安全岗位人员的岗位培训，要积极认真地研究探讨如何做好网络安全人才岗位技能培训的模式和方法。经过思考，我们设想，可以建设“网络安全培训创新综合基地”，设定九个功能平台。

培训平台。以提高网络安全岗位业务知识和实战动手能力为目标，坚持以解决问题为导向，强调针对性、实战性、实效性、灵活多样性的教学培训。强调干什么学什么，缺什么补什么练什么，强化培训质量，建立标准化培训体系；以“动手操作＋案例”分析为主，通过

在实验室实训上网操练提高实战能力，通过建立案例库及案例分析，提高学员发现问题、提出问题、分析问题、解决问题的能力。为解决网络攻防竞赛和培训靶场出现模式化、固定化等问题，要创建综合性、高仿真的网络靶场，建设“固定靶标+移动靶标+红蓝攻防对抗”的竞赛训练培训模式；要做到数据信息攻防、设备设施攻防，以提高培训学员“基本功＋灵活机动战术”的能力；在网络受到不同木马病毒等各种方法的攻击时，能够灵活机动地应对处置；通过固定靶标训练学习掌握网络攻防基础知识和基本功，通过移动靶标和红蓝攻防对抗训练，让学员学习掌握攻击方如何明确攻击目标和达到实现目标的路径方法，防守方如何侦测攻击路径并做好防守，阻止（止血）攻击并控制损害范围；攻防对抗操练不设固定条件环境，任由红蓝双方运用网络攻防技术手段自由进行攻防对抗训练，在设定的时间内考核决定胜负，改变由单方攻击设置好条件环境的固定靶标的训练竞赛模式。通过“移动靶标＋红蓝攻防对抗”的培训模式，主要培养学员练就具备灵活多样和会静默潜伏、持久作战的思维意识、敏捷快速、机动灵活、攻防兼备应对处置网络安全风险问题的思想素质、技术能力和水平。

在教学培训方式方法上，强调“短、平、快”。“短”就是培训学习时间短，在较短的时间内为学员解决一个问题，学会一个技术方法，掌握一项技能；“平”就是平等，教师与学员、学员与学员之间平等相待，互教互学，共同学习、共同提高；“快”就是让学员能够快速地掌握能够实用、发挥实效的技术方法和技能。要通过产教融合，双导师制等，培养政治可靠、攻防兼备的具有网络安全特色的实战应用性强的复合型人才。

为了实现以上目标，要建好教学、实验实训的软件和硬件场地环境，建好案例库和攻防对抗实训靶标环境。要根据不同网络安全岗位对人才知识、技术能力的需求，编写不同的案例、教材和实训操练大纲，力争打造出具有网络安全培训鲜明特色的“网络安全朱日和”训练综合基地。

展示平台。建设一个展览大厅，将国内外网络安全产品、系统进行展示介绍，包括研发制造的企业厂家，产品的技术性能和应用功能等，达到较全面地了解网络安全产品、系统的现状，交流信息，互相学习，取长补短。为供需双方提供交易网络安全产品、系统实物的信息平台。

查询平台。建设网络安全数据信息库和人才库。通过查询平台能够查询涉及网络安全领域的文献资料摘要，网络安全产品、系统的企业厂家，技术性能、应用功能等信息,从事网络安全人才的有关简要信息等。

检测平台。建设网络信息安全产品、系统安全检测实验室，购建相关检测仪器设备和建

设检测环境，重点检测信息安全产品、系统的安全可靠性及性能和功能是否真实可靠，安全检测重点放在如何有效发现软硬件设计缺陷导致的安全漏洞和后门上。要将网络安全等级保护标准纳入产品及系统检测之中，通过等级保护标准检测对网络信息安全产品进行定级。要研究解决对网络安全产品如何进行量化标准化检测的世界性难题。对网络信息安全产品的检测实行自愿送检的原则，尤其是对一些企业研发的网络信息安全产品，在未进入市场之前委托进行安全可靠性检测。

交流平台。打造提供一个良好的进行学术思想和产品及技术交流的环境场所，建设大、中、小各种各样的自由交流的环境场所。架起党政军民学、政产学研用在网络安全方面进行交流沟通的桥梁，做好穿针引线工作。

创新平台。充分发挥培训、展示、查询、检测、交流等平台的作用，紧紧围绕“网络技术安全+管理安全”做好研发创新，突出网络安全理论、网络安全技术及方法、网络安全管理和法律法规的研究创新，为企业和个人提供创新服务,为国家维护网络安全建言献策。

创业平台。为微小企业和个人进行网络安全的创业提供场所环境和相关服务。

宣传平台。配合国家网络安全宣传活动，做好网络安全宣传的有关工作。网络安全为人民，网络安全靠人民。要充分发挥综合基地内各个平台在网络安全宣传教育方面的作用，综合基地可以对大中小学生和群众开放参观学习，使其成为向社会进行宣传教育网络安全知识的窗口和基地，提高维护国家网络安全思想意识和能力的阵地。

服务平台。网络安全培训创新综合基地树立服务至上的理念，为进入基地的企业和人员提供高效优质服务，做到工作效率高，服务质量好，基地内做到信息共享、互联互通，搞好一条龙服务。

希望通过这九个平台，把网络安全培训创新等工作做细做扎实，实实在在做人，扎扎实实做事，愉愉快快做成事。因为网络安全涉及国家安全、经济社会发展和人民群众的切身利益，来不得半点儿浮躁虚假。政府有关部门、企业单位和个人应参与到网络安全培训创新综合基地建设中来，使蓝图能够变为现实，为维护国家网络安全贡献力量！（来源:《中国信息安全》杂志 2019 年第 10 期））

四、政府之声

➢ 国家网信办发布《网络安全威胁信息发布管理办法（征求意见稿）》

2019 年 11 月 20 日，国家互联网信息办公室向社会公开征求对《网络安全威胁信息发布管理办法(征求意见稿)》(以下简称《办法》)意见，国家互联网信息办公室有关负责人接受采访，就《办法》相关问题回答了记者提问。

1.问：请您介绍一下制定《办法》的背景？

答：当前，网络安全产业迅猛发展，许多网络安全研究者和网络安全企业出于提高公民网络安全意识、交流网络安全技术、增强用户网络安全防范能力、促进网络安全产业发展等目的，积极向社会发布网络安全威胁信息，为维护国家网络空间安全做出很大贡献。但是也应看到，网络安全威胁信息的发布仍存在很多问题，有关单位、网络运营者反映强烈。例如，有组织或个人打着研究、交流、传授网络安全技术的旗号，随意发布计算机病毒、木马、勒索软件等恶意程序的源代码和制作方法，以及网络攻击、网络侵入过程和方法的细节，为恶意分子和网络黑产从业人员提供了技术资源，降低了网络攻击的门槛；有组织或个人未经网络运营者同意，公开网络规划设计、拓扑结构、资产信息、软件代码等属性信息和脆弱性信息，容易被恶意分子利用威胁网络运营者网络安全，特别是关键信息基础设施的相关信息一旦被公开，危害更大；部分网络安全企业和机构为推销产品、赚取眼球，不当评价有关地区、

行业网络安全攻击、事件、风险、脆弱性状况，误导舆论，造成不良影响；部分媒体、网络安全企业随意发布网络安全预警信息，夸大危害和影响，容易造成社会恐慌。

2.问：制定《办法》的依据是什么？

答：《网络安全法》第二十六条规定，“开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。”目前，尚无规范网络安全威胁信息发布活动的法律法规。因此，为了进一步规范网络安全威胁信息发布行为，国家互联网信息办公室会同公安部等有关部门依据职责制定了《办法》。

3.问：为什么禁止发布恶意程序源代码、制作方法，能够完整复现网络攻击、网络侵入过程的细节信息等网络安全威胁信息？

答：上述网络安全威胁信息容易被恶意分子或网络黑产从业人员直接利用，降低了网络攻击的门槛，因此从维护网络安全的角度，要求发布网络安全威胁信息时不得包含上述内容。网络安全从业者、爱好者仍可通过多种方式加强原理和技术研究，提高网络安全能力水平。

4.问：禁止发布第四条规定的信息，是否会导致这些信息流入地下黑市？

答：为网络犯罪提供技术支持是法律明确禁止的违法犯罪行为，依法要承担相应的法律责任。我们相信，作为遵纪守法、有道德操守的网络安全工作者、爱好者，以前不会为网络黑产提供技术支持，今后同样也不会。

5.问：是否会对网络安全产业发展造成影响？

答：我们鼓励和支持网络安全企业向社会展示技术能力，促进网络安全意识提升，传播普及网络安全防护技术知识，提供网络安全服务。要求安全企业不向社会发布恶意程序的制作技术、网络攻击技术，并不意味着企业不能研究网络攻击技术，企业仍可通过研究网络攻防技术，不断提升网络安全防护能力，不但不影响安全产业发展，对提高网络安全产业发展水平还产生积极的促进作用。

6.问：媒体今后还能报道网络安全事件新闻吗？

答：媒体可以正常报道网络安全事件新闻，但需满足两个条件，一是如果属于办法第五条提到的网络和信息系统网络安全事件，首次披露前要向所在地区地市级以上公安机关报告，以便有关部门及时掌握事件情况，采取处置措施，降低危害；二是不得包含网络安全事件泄露的数据内容本身，以免扩大事件的危害。

7.问：向网信部门、公安机关、行业主管部门等报告是否属于行政许可？

答：不属于行政许可，完成报告即为履行义务。

8.问：为什么发布具体网络和信息系统存在风险、脆弱性的情况时，需要事先征得其运营者书面同意?

答：如果随意发布上述信息，恶意分子有可能利用这些信息入侵相关网络和信息系统，导致网络和信息系统运营者利益受损。但如果根据发布的网络安全威胁信息，无法定位到具体网络和信息系统，如不涉及网络和信息系统的名字、位置、域名、IP 地址等信息，就不需要征求其运营者同意。此外，如果相关风险、脆弱性已被消除或修复，或已提前 30 日向网信、电信、公安或相关行业主管部门举报，发布上述信息也可不经其运营者同意。

9.问：为什么发布网络安全威胁信息，标题中不得含有“预警”字样?

答：根据《国家网络安全事件应急预案》，网络安全预警是一种特定信息，具有权威性，应由政府部门按权限发布。但目前有的组织和个人随意发布预警，夸大事实，进行炒作，事实上破坏了预警的效力和权威性，所以我们要求发布网络安全威胁信息，标题中不得含有“预警”字样。相关组织和个人可通过风险提示、威胁情报等方式提醒公众加强风险防范。

（来源：国家互联网信息办公室）

- **《网络安全威胁信息发布管理办法（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2019-11/20/c_1575785387932969.htm

➢ 工业和信息化部关于印发《携号转网服务管理规定》的通知

2019 年 11 月 11 日，工业和信息化部发布了《携号转网服务管理规定》（下称《管理规定》）。为了更好地理解和执行《管理规定》，现就有关内容解读如下：

一、《管理规定》的制定背景

为贯彻落实 2019 年国务院《政府工作报告》在全国实行“携号转网” 的要求，践行以人民为中心的发展思想，加强“携号转网”服务管理，切实提升行业服务质量，不断增强人民群众的获得感。工业和信息化部依据《中华人民共和国电信条例》《电信服务规范》及相关法规和规章，制定本规定。

二、《管理规定》的重要作用

《管理规定》是维护用户合法权益的重要保障。“携号转网”是由基础电信业务经营者提供的一项电信服务，用户可以依据本规定向电信业务经营者提出申请，办理“携号转网”。电信业务经营者应明确服务办理条件和流程并向社会公开，以保障用户在办理“携号转网”

过程中规则更加透明，流程更加顺畅。

《管理规定》是规范企业经营行为的重要指引。“携号转网”服务是一项惠民服务举措。《管理规定》通过明确企业在提供“携号转网”服务过程中的红线，进一步规范企业经营行为，为共同维护有序的市场环境，促进行业健康发展提供有力保障。

《管理规定》是加强行业监管的重要依据。管理规定明确指出，电信业务经营者在提供“携号转网”服务过程中，不得存在的 9 类禁止性行为，为电信监管机构实施监督检查提供重要依据。

三、《管理规定》的制定过程

2019 年 3 月，工业和信息化部在前期充分论证基础上，启动了《管理规定》的制定工作。在《管理规定》制定过程中，一是梳理总结了试验五省（市）“携号转网”服务管理经验；二是征求了电信企业和全国各通信管理局相关意见，对规定涉及内容、操作实用性等问题进行了反复研究；三是 7 月 31 日至 8 月 14 日，通过工业和信息化部门户网站向社会公开征求了意见。

四、《管理规定》的制定思路和原则

在前期征求意见基础上，根据意见情况，工业和信息化部进一步提高政治站位，紧扣行业监管职责定位，在《管理规定》制定过程中，重点把握以下三点原则：

一是坚持以人民为中心。严格落实党中央、国务院的决策部署，要求电信企业遵循用户方便、公平公正、诚实守信、协同配合的原则，建立健全服务体系，为用户提供高质量的“携

号转网”服务。

二是落实企业主体责任。强化企业责任担当，要求电信企业制定“携号转网”服务实施细则，实施过程中加强协同，不断优化服务。

三是注重风险防范。要求电信企业明确告知用户面临的风险和损失，并获得用户确认。

五、《管理规定》共 15 条，主要内容包括：

一是提出“携号转网”服务基本原则和总体要求。电信业务经营者应当遵循方便用户、公平公正、诚实守信、协同配合的原则，建立健全服务体系，落实企业主体责任，为用户提供高质量的“携号转网”服务。

二是明确“携号转网”服务适用的地域范围和号段范围。“携号转网”服务是指在同一本地网范围内，蜂窝移动电话用户变更签约的基础电信业务经营者而用户号码保持不变的一项服务。现阶段该服务不包含物联网用户号码、卫星移动用户号码和移动通信转售用户号码。

三是明确电信管理机构、电信业务经营者和用户的权责关系。电信业务经营者应当为用户提供便捷的“携号转网”服务。电信管理机构对电信业务经营者的“携号转网”服务实施监督检查。用户可以向电信业务经营者申请、办理“携号转网”服务，同时应当配合电信业务经营者开展身份信息一致性验证。

四是规定电信企业九类禁止性行为。电信业务经营者不得有妨碍服务、干扰用户选择、阻挠携转、降低通信服务质量、比较宣传、虚假宣传等违规行为。

五是要求电信企业向用户做好风险告知。明确告知用户办理“携号转网”服务可能面临的风险和损失，并获用户确认。（来源：工业和信息化部）

- **工业和信息化部关于印发《携号转网服务管理规定》的通知全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c7513621/content.html

➢ 公安部通报“净网 2019”专项行动工作情况及典型案例

2019 年 11 月 14 日，公安部在京召开新闻发布会，通报全国公安机关开展“净网 2019”专项行动工作情况及典型案例。发布会上，公安部网络安全保卫局巡视员、副局长张宏业，北京市公安局网络安全保卫总队副总队长刘尚奇，黑龙江省七台河市公安局常务副局长朱孔勤，浙江省公安厅通报中心主任黄海涛，山东省烟台市公安局党委委员陈斌就相关工作回答了记者提问。

持续强化对“暗网”犯罪的打击力度

记者：请介绍一下当前“暗网”犯罪的一些特点？

刘尚奇：所谓“暗网”，简单地说就是隐藏的网络，普通网民无法通过常规手段搜索访问，需要使用一些特定的软件、配置或者授权等才能登录。由于“暗网”匿名性等特点，容易滋生以网络为勾联工具的各类违法犯罪，比如买卖各类枪支弹药、毒品、公民个人信息、提供黑客工具、传授黑客技术教程、网络攻击、制作贩卖淫秽物品等。但是“暗网”并非“法外之地”，近年来，我国公安机关不断研究“暗网”相关违法犯罪问题，持续强化对“暗网”犯罪的打击力度，成功侦破多起利用“暗网”实施违法犯罪的案件。

继续对“套路贷”违法犯罪高压严打

记者：少数科技信息公司、数据服务公司、第三方支付公司成为网络“套路贷”犯罪工具和帮凶。对此，公安机关将采取哪些有效措施？

朱孔勤：公安机关将对“套路贷”违法犯罪活动继续保持高压严打态势，对网络“套路贷”犯罪涉及的技术服务商、数据支撑服务商、支付服务商、推广服务商等进行生态式、全链条打击。特别是对涉及的明知是“套路贷”却仍为其研发系统平台和 App 的科技公司、为“套路贷”进行网上推广的网站和平台、为非法获取公民个人信息提供数据支撑的数据公司、为“套路贷”开通资金结算渠道和提供支付服务的第三方支付公司，公安机关将依法查处、严厉打击，绝不姑息。同时，将进一步加强对各类网站和互联网企业的日常监管，依法规范其运营，确保网络空间天朗气清、生态良好。另外，在这里也提醒广大网民，要对网上现金借贷服务增强辨别力，不要陷入“套路贷”的陷阱。

全链条打击窃听、窃照类违法犯罪

记者：针孔摄像头等窃听、窃照器材为何屡打不绝、屡禁不止？公安机关在打击查处这类案件上有什么样的举措？

黄海涛：这类违法犯罪活动屡打不绝、屡禁不止的原因有三点：

第一，这类违法犯罪有利可图。据了解，在市面上售价三四百元的针孔摄像头，其成本不过百元，却在黑市上销路非常好。这样的高额回报，吸引了不法分子铤而走险“捞金”。

第二，针孔摄像头制作并不复杂，技术含量也不高，前期公安机关所收缴的大量针孔摄像头有相当部分源于手工作坊，这样的低门槛为不法分子“入行”提供了可能。

第三，打击和监管的难度在增加。从现在的情况来看，越来越多的针孔摄像头的销售方式从网下搬到了网上，不法分子想通过网络销售的方式来躲避监管。同时，在具体的销售方式上，他们采取了“挂羊头卖狗肉”或者把针孔摄像头的主要部件和伪造部件分开销售的方

式进行，这为监管和打击工作带来一定的难度。

在办理此类案件时，公安机关要做到对针孔摄像头的生产、销售、使用等各环节开展全链条式打击。浙江公安机关前期主要是从三个维度入手。

一是紧盯源头，直捣非法生产针孔摄像头的上层团伙。我们从一起偷窥案件入手，追根溯源，最终打掉了一条由方案设计商、硬件生产商、二级生产商、代理经销商等 4 个层级构成的非法生产、销售针孔摄像头的黑色产业链条，共抓获犯罪嫌疑人 26 名。

二是重拳出击，严查非法使用针孔摄像头的行为。我们根据前期打击上层团伙所掌握的线索，对非法使用针孔摄像头用户逐一落地排摸，尽快处置，以消除现实危害。截至目前，浙江共查处非法安装使用针孔摄像头的点位 684 个，查扣摄像头 714 个，查处刑事案件 2 起，违法案件 35 起。

三是上下结合，斩断多层级的针孔摄像头网络销售链路。从生产团伙以及下游的使用人员两端入手，我们“自上而下”或“自下而上”对销售中间环节进行逐一追查，扩线深挖。截至目前，我们已经查处非法销售针孔摄像头的刑事案件 24 起，抓获犯罪嫌疑人 32 名。

为人民群众创造更加美好的网络生态环境

记者：当前网上贩售迷奸类药物犯罪有什么特点？

陈斌：我们在案件侦办过程中发现，当前犯罪嫌疑人主要是通过医院、医药公司和境外代购这些渠道非法大量购入国家管制的精神类、麻醉类的药品，利用“黑卡”注册网络虚拟身份，大量组建 QQ 群、微信群，同时不断拉人入伙，入伙者以 20 岁左右的年轻人居多。嫌疑人在网上使用暗语贩卖迷奸类药物，并且在群内向买家传授使用方法，教唆实施迷奸犯罪，甚至相约共同实施迷奸犯罪。为改良配方，犯罪嫌疑人还要求买家向其反馈使用效果。下游买家一般会选择亲朋好友、同事熟人这一类人作为迷奸犯罪的侵害对象，积累经验以后再扩大到其他的女性甚至是幼女，犯罪嫌疑人还利用约会网友、与女同事加班独处等机会伺机下药，实施犯罪，并且拍摄视频图片，甚至上传到黄色网站获利，严重冲击了社会伦理及道德法律的底线。

记者：“净网 2019”专项行动下一阶段工作重点是什么？

张宏业：当前，随着互联网的快速发展，传统犯罪加速向以互联网为媒介的非接触式犯罪转移，涉网犯罪数量、受害人规模和社会危害性持续激增。借助互联网非接触式的特点，各种传统犯罪的组织方式、外在表现形式、范围、影响都发生了深刻变化，且持续交织、动态变化，构成了错综复杂的网络违法犯罪生态。针对当前网络违法犯罪高发多发的严峻形势，公安机关网安部门将继续深化“净网 2019”专项行动，按照整体作战、生态打击的总体思

路，聚焦网络违法犯罪高发频发的深层次原因，进一步研究打击策略、打击方法、法律适用和防范措施，抓住网络违法犯罪生态的关键环节，打准打断网络黑灰产业链条。同时，建立打防管控一体化工作模式，深入推进“一案双查”制度，逐步完善管理措施，逐项覆盖监管对象，压制萎缩网络违法犯罪生存空间，不断提高网络生态治理水平，积极构建网络社会共建、共治、共享体系，为人民群众创造更加美好的网络生态环境。（来源：公安部）

➢ 中国中国互联网金融协会下发通知 强化互联网金融个人信息保护

2019 年 11 月 6 日，中国互联网金融协会发布《关于增强个人信息保护意识依法开展业务的通知》，通知提到，近期国家监管部门发现，社会上有一些互联网机构以“大数据”为名，通过“爬虫”业务涉嫌违法违规收集个人信息，或窃取、滥用、买卖、泄露个人信息，侵犯了消费者个人隐私，造成了不良的社会影响。

为引导会员机构增强个人信息保护意识，坚持合规、审慎经营，防范并纠正违反个人信息保护规定的行为，现就增强个人信息保护意识、依法开展业务的有关事项通知如下：

一、各会员机构应严守法律底线，依法合规开展个人信息的收集、处理、使用和对外提供等活动，不断加强个人信息保护工作力度、未经消费者授权同意，各会员机构不收集、处理使用和对外提供消费者个人信息。

二、未经消费者授权同意，各会员机构不收集、处理、使用和对外提供消费者个人信息。各会员机构不以默认授权、概况授权、功能捆绑等误导、强迫消费者的方式收集个人信息，不与违规收集和使用个人信息的第三方开展数据合作，不滥用、非法买卖和泄露消费者个人信息。

三、各会员机构应建立健全收集、处理、使用、对外提供等全生命周期的个人信息保护制度，采取有效技术措施保障个人信息安全，加强对员工的教育和培训，对个人信息的收集、使用等活动加强监督管理。

四、各会员机构应及时就个人信息保护工作开展自查，并对数据合作方进行排查，对于存在的问题应立即整改，并及时将有关情况报告协会。

五、各会员机构应履行消费者教育义务，加强对消费者的风险提示。（来源：中国互联网金融协会）

五、本期重要漏洞实例

➢ Microsoft 发布 2019 年 11 月安全更新

发布日期：2019-11-12

更新日期：2019-11-12

受影响系统：

11 月 12 日，微软发布了 2019 年 11 月份的月度例行安全公告，修复了其多款产品存在的 322 个安全漏洞。受影响的产品包括：Windows 10 1903 & WindowsServer v1903（46 个）、Windows 10 1809 & WindowsServer 2019（46 个）、Windows 10 1803 & WindowsServer v1803（46 个）、Windows 8.1 & Server 2012 R2（37 个）、Windows RT 8.1（32 个）、WindowsServer 2012（37 个）、Windows7 and Windows Server 2008 R2（35 个）、WindowsServer 2008（31 个）、MicrosoftEdge（4 个）、InternetExplorer（2 个）和 Microsoft SharePoint-related software（6 个）。

利用上述漏洞，攻击者可以提升权限，欺骗，绕过安全功能限制，获取敏感信息，执行远程代码或发起拒绝服务攻击等。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

描述：

ID: CNTA-2019-0037

CVE 编号	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2019-1384	**NETLOGON 安全功能绕过漏洞** NETLogon 消息能够获得会话密钥并签署消息时，存在安全功能绕过漏洞。要利用此漏洞，攻击者可以发送精心编制的身份验证请求。成功利用此漏洞的攻击者可以使用原始用户权限访问其他计算机。通过更改 NTLM 验证网络身份验证消息的方式解决该问题。	重要 绕过安全功能	Windows 10 Windows 7 Windows 8.1 Server 2008 Server 2008 R2 Server 2012 Server 2012 R2 Server 2016 Server, version 1803 Server 2019 Server, version 1903
CVE-2019-1397	**Windows Hyper-V 远程代码执行漏洞** 当主机服务器上的 Windows Hyy-V 未能正确验证来自客户操作系统上的身份验证的用户的输入时，存在远程代码执行漏洞。要利用此漏洞，攻击者可以在客户操作系统上运行构建的应用程序，可能会导致 Hyper-V 主机操作系统执行任意代码。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。安全更新通过更正	严重 远程执行代码	Windows 10 Server, version 1803 Server 2019 Server, version 1903 Server 2016 Windows 7 Windows 8.1 Server 2008 Server 2008 R2

	Hyper-V 如何验证客户操作系统用户输入来解决该漏洞。		Server 2012 Server 2012 R2
CVE-2019-1419	**OpenType Font Parsing 远程代码执行漏洞** 当 Windows Adobe 类型管理器库未能正确处理精心制作的 OpenType 字体时，在 Microsoft Windows 中存在远程代码执行漏洞。对于除 Windows 10 以外的所有系统，成功利用此漏洞的攻击者都可以远程执行代码。攻击者有多种方法可以利用此漏洞进行攻击，例如说服用户打开精心编制的文档，或者说服用户访问包含巧尽心思构建的嵌入 OpenType 字体的网页。	严重 远程执行代码	Windows 10 Server, version 1803 Server 2019 Server, version 1903 Server 2016 Windows 7 Windows 8.1 Server 2008 Server 2008 R2 Server 2012 Server 2012 R2
CVE-2019-1429	**Internet Explorer 脚本引擎内存破坏漏洞** Internet Explorer 脚本引擎处理内存对象的方式存在远程代码执行漏洞。该漏洞可破坏内存，使得攻击者可以在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。	重要 远程执行代码	Internet Explorer 10 Internet Explorer 9 Internet Explorer 11
CVE-2019-1448	**Microsoft Excel 远程代码执行漏洞** 当软件未能正确处理内存中的对象时，Microsoft Excel 软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。将帐户配置为在系统上拥有较少用户权限的用户可能比使用管理用户权限操作的用户受影响更小。 安全更新通过更正 Microsoft Excel 如何处理内存中的对象来解决此漏洞。	重要 远程执行代码	Office 2019 Office 2019 for Mac Office 365 ProPlus Excel 2016 Office 2016 for Mac Excel 2010 Excel 2013
CVE-2019-1443	**Microsoft SharePoint 信息泄漏漏洞** 当微软向 SharePoint 服务器上传专门制作的文件时，ShareSharePoint 中存在信息泄露漏洞。成功利用此漏洞的经过身份验	重要 信息泄露	SharePoint Enterprise Server 2016 SharePoint Server 2019 SharePoint Foundation 2010 SharePoint Foundation 2013

	证的攻击者可能会利用 SharePoint 功能获取 SMB 哈希。 安全更新通过更正 SharePoint 如何检查文件内容来解决该漏洞。		

➢ IBM Rational Quality Manager 跨站脚本漏洞

发布日期：2019-11-21
更新日期：2019-11-21
受影响系统：
IBM Rational Quality Manager（RQM） >=6.0，<=6.0.6
描述：

CVE(CAN) ID: CVE-2019-4251
BM Rational Quality Manager（RQM）是美国 IBM 公司的一套协作的、基于 Web 的质量管理解决方案。该方案在软件开发的整个生命周期之内，提供了测试规划与测试评价管理方法，并能够共享信息、自动化加快项目进度以及报告制定的发布决策。
IBM Rational Quality Manager 6.0 版本至 6.0.6.1 版本中存在跨站脚本漏洞。远程攻击者可利用该漏洞在 Web UI 中执行任意的 JavaScript 代码。
<*来源：IBM
建议：

厂商补丁：
IBM
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://www.ibm.com/support/pages/node/1076637

➢ Symantec Endpoint Protection (SEP) 权限提升漏洞

发布日期：2019-11-14
更新日期：2019-11-19
受影响系统：
Symantec Endpoint Protection < 14.2 RU2
Symantec Endpoint Protection < 12.1 RU6 MP10
Symantec Endpoint Protection Small Business Edition (SEP SB < 12.1 RU6 MP10d (12.1.7510.70
描述：

BUGTRAQ ID: 110786
CVE(CAN) ID: CVE-2019-12757

Symantec Endpoint Protection (SEP) 是由赛门铁克开发的安全软件包，包括杀毒软件、入侵检测系统和防火墙，适用于服务器和台式计算机，在端点安全产品中拥有最大的市场份额。
Symantec Endpoint Protection (SEP)14.2 RU2 & 12.1 RU6 MP10 之前版本，Symantec Endpoint Protection Small Business Edition (SEP SBE) 12.1 RU6 MP10d (12.1.7510.7002)之前版本，在实现中存在权限提升漏洞，攻击者利用此漏洞可获得提升的权限，访问受保护资源。
<*来源：Symantec
*>
建议：

厂商补丁：
Symantec
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.symantec.com/us/en/article.SYMSA1488.html

➢ Apache Flink 任意 Jar 包上传漏洞

发布日期：2019-11-15
更新日期：2019-11-18
受影响系统：
Apache Group Flink <= 1.9.1
描述：

Apache Flink 是开源流处理框架，可用于对流数据进行分布式处理，在大数据领域中应用广泛。
Apache Flink 在 jar 包上传功能实现中存在安全漏洞，此漏洞源于 Dashboard 在默认状态下无需认证即可访问，如果有攻击者探测到目标存在 Apache Flink Dashboard，利用该威胁可未授权上传 jar 包，上传包含恶意代码的 jar 包，从而控制目标服务器。
<*来源：anonymous
*>
建议：

临时解决方法：
目前官方暂未发布针对此威胁的修复方案，相关用户可采取以下临时防护建议进行防护：
禁止对公网开放 Flink
在内网中限制对 8081 端口（Flink Dashboard 默认端口）的访问
为 Flink 的访问增加认证策略
厂商补丁：
Apache Group
目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：
https://flink.apache.org/
https://www.apache.org/security/projects.html

六、本期网络安全事件

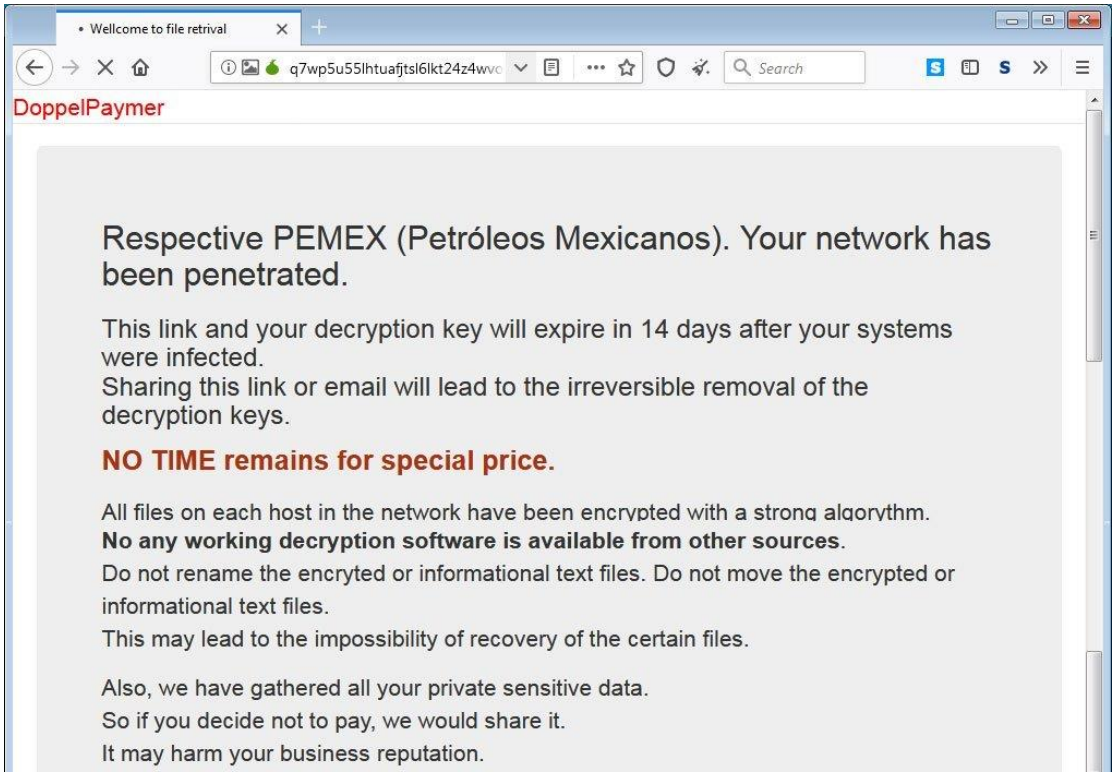
➢ 墨西哥国有石油公司 Pemex 遭遇勒索软件打击

2019 年 11 月 13 日，周日，DoppelPaymer 勒索软件感染并破坏了墨西哥国有石油公司 PetróleosMexicanos（Pemex）的系统。黑客向 Pemex 提出的金额为 565 比特币。此外，DoppelPaymer 的 TOR 网站更新后的文字如下：“我们还收集了所有的私人敏感数据。如果你拒绝付款，我们会将这些数据传播给其他人，这可能会损害您的商誉。”

pic.twitter.com/BoHi1lVigF

— MalwareHunterTeam（@malwrhunterteam），2019 年 11 月 12 日

据该公司称，公司只有不到 5%的计算机感染了勒索软件。



“和其他国际政府以及金融公司和机构一样，Pemex 经常收到威胁和网络攻击。” 该公司发布的安全公告中写道。“11 月 10 日星期日，这家国有生产公司遭遇了网络攻击，这些攻击最终被及时消除，并且只影响了不到 5%的个人计算机设备的运行。此次事件过后，Pemex 重申其燃料生产，供应和库存是有安全保障的。”

Petróleos Mexicanos 声称它迅速解决了此事件，同时强调其运营和生产系统没有受到影响。Pemex 确认其基础设施与所有主要的国家和国际政府以及金融组织一样，正不断面对来

自黑客的攻击，因此公司正在持续加强安全措施。

DoppelPaymer 勒索软件是 BitPaymer 勒索软件的 forked 版本，它可能是由某些网络犯罪团伙以 TA505 身份开发的。（来源：ZDNet）

➢ 迪士尼流媒体平台"Disney+"用户账号遭攻击流入"暗网"

2019 年 11 月 12 日，迪士尼集团流媒体平台 Disney+在美国、加拿大、荷兰正式上线。Disney+一经上线，就气势磅礴的为用户推出了超过 500 部电影，7500 集电视剧集，10 部原创电影。其 IP 资源内容覆盖了迪士尼动画、皮克斯动画、漫威影业、卢卡斯影业、国家地理等。其会员费用为每月 6.99 或每年 69.99 美元，明显低于 Netflix(305.16, 2.56, 0.85%)等竞争对手，后者最受欢迎的标准高清电视月套餐售价为 12.99 美元。

难以忽视的技术问题

在上线首日，就有用户在实际访问迪士尼庞大的内容目录时遇到了一系列技术上的问题。虽然一些用户体验到了较慢的流媒体速度，但其他用户却根本无法连接到服务上。

迪士尼将这些问题解释为“消费者需求的膨胀”。“用户对 Disney+的热情超出了我们的最高预期。虽然我们对这一令人难以置信的反应感到高兴，但我们也意识到了当前的用户问题并正在努力迅速解决这些问题。对你们的耐心我们深表感谢。”随即，迪士尼很快就解决了上述问题。

但近日，Disney+面临更严重的技术问题

据英国广播公司报道，数千个 Disney+账户遭到黑客攻击。自从上周这个流媒体服务上线以来，成千上万的用户报告说他们的账户被黑了，这些账户后来被卖到“暗网”上。尽管很多人联系了迪士尼公司，但很多人的问题还没有得到解决。

事实上，11 月 12 日“Disney+”上线几个小时后，有已经有用户账号的账号被盗，并开始出现在“暗网”上销售。

虽然“Disney+”只在美国、加拿大和荷兰上线，但许多人在上线当天就被锁定了自己的账号，并在社交媒体上抱怨。其中一些人说，迪士尼还没有给他们回复。一些分析人士推测，其不稳定的推出部分是由于那些被锁定的账户，这些账户可能就在当天遭到了黑客攻击。

根据 ZDNet 的一项调查，许多用户的账户信息在服务推出几小时后就在“暗网”上出售了，有些甚至只卖 3 美元至 11 美元之间，甚至还有免费登出账户信息，这意味着你可以花极低的价钱，就可以观看“Disney+”的庞大资源库。

CyberInt 的首席研究员贾森·希尔表示，许多账户遭到黑客攻击，是因为许多人在不同的网站上使用相同的密码。迪士尼用户现在更为担心的是，因为黑客可以使用他们 Disney+的登录访问其他迪士尼产品，如迪士尼商店和娱乐公园。（来源：界面）

➢ 这个“李鬼”很危险！小心高仿手机 App

2019 年 11 月 20 日，为方便打理财务，济南市民韩先生下载了一款名为“××银行信用卡”的 App，不久后却发现银行卡被盗刷、莫名被贷款等情况。到银行营业网点核实，被告知所安装的客户端是高仿的。

网上转账缴费、处理罚单、买火车票……随着移动互联网的发展，越来越多的人习惯用手机 App 处理各种事务。“新华视点”记者调查发现，在手机应用市场中，一些通过相近名称、类似图标制作的高仿 App 令人难辨真假，给不少用户造成财产损失。

高仿 App“鬼”影重重大设陷阱

济南市民成栋前不久为网上处理汽车交通罚单，试图在手机应用商店下载公安部推出的“交管 12123”App。搜索结果第一位的为一款名为“12123”的软件，且 App 图标为一个“违”字。下载使用后才发现，这款 App 功能和页面都极其简陋，是一款高仿 App，不仅无法处理违章，还含有大量广告。

记者在多个应用商店检索发现，此类 App“李鬼”并不少见。例如，北京公交集团推出

的“北京公交”App，可用来刷码乘公交。但在安智网、酷安网等应用市场中检索“北京公交”，排名前几位的应用多为“北京实时公交”“北京公交在线”等 App，下载量最高的达 30.8 万次。打开上述 App 后，界面非常简单，也不具备刷码乘车功能，且都包含不少广告。在这些 App 的用户评论区，许多使用者留言“根本用不了”“软件是骗人的”等。

值得警惕的是，一些高仿 App 还通过伪装成官方软件窃取用户个人信息。济南市民罗腾告诉记者，他此前为在济南一家医院挂号，在应用市场中下载了这家医院的 App，并填写了电子病历，其中包含家庭住址、联系方式、职业等个人信息。但之后发现，所下载的并不是官方 App。“这款 App 的下载量近 10 万，窃取了大量个人信息，侵犯个人隐私。”罗腾说。

记者发现，高仿 App 除了集中在垂直的生活服务类软件，同时在电商平台的应用中也较为普遍。烟台市民马翘楚告诉记者，她曾在某应用市场搜索“淘宝”时，下载了一款名为“淘宝特卖”的 App，进入后发现，平台内不少商家销售价格低廉的山寨货品，并且购物的“三包”“退换货”等条款都不齐全。

记者联系了北京公交部门、山东交警部门以及淘宝服务热线，分别核实高仿 App“12123”“北京公交在线”“淘宝特卖”等是否与官方推出的应用有关联。相关工作人员均告诉记者，这些 App 与官方应用无任何关系；类似的高仿 App 很多，的确在一定程度上干扰了使用者，不少用户无法第一时间下载到官方应用。

5 万元即可开发一个高仿 App

记者调查发现，不少高仿 App 开发者为第三方公司。以“北京实时公交”为例，开发者

为江苏一家商贸有限公司，在国家企业信用信息公示系统中，该公司经营范围为“化妆品、服装、日用百货销售”。此外记者还发现，应用市场中的一些高仿应用，开发者甚至为个人，网络上无法查询更多开发者信息。

业内人士告诉记者，高仿 App 盈利主要靠应用内的大量广告赚取广告费，这类 App 开发难度并不高。记者联系了一个 App 开发团队，并向对方提出想开发图标和名字都模仿一款学习类应用的高仿 App。对方表示，只要不是要求“一模一样”，就都可以实现。费用在 5 万元左右，开发周期大约一个月。

业内人士表示，开发一款高仿 App，花费数万元可以长期赚取广告收益。应用市场在对上架的 App 进行审核时，机器审核只进行病毒和兼容性测试，人工审核一般只审核名称、内容是否存在违规，对 App 名称、图标、宣传语等内容是否存在模仿，多数应用市场都疏于甄别。记者查询了多个应用市场的相关条款，只有“华为应用商店”等极个别应用市场在相关条款中要求，上架应用不得与其他开发者应用具有相同或相似的外观、名称、主题等。

高仿 App 已形成危害用户网络安全的产业链

360 发布的《2018 年双十一购物安全生态报告》显示，一个月时间内虚假仿冒主流购物 App 的数量接近 4000 个，覆盖设备超过 30 万个，高仿 App 已形成危害用户网络安全的产业链。记者调查发现，近期福建、河北等地网信部门关停下架的应用中不乏高仿类 App。福建泉州网信办今年 8 月下架的 43 款违规 App 中，就有模仿“天天快报”等 App 的应用。

北京师范大学法学院副教授吴沈括说，高仿 App 对于正版应用的模仿，已经涉嫌侵权，同时对用户产生了实质性危害。但是，目前在打击高仿 App 的过程中，存在多方协调难、举报下架过程漫长、相关法律政策不完善等因素，给一些不法企业从事违规行为提供了空间。

多位专家建议，公安、市场监管、网信等部门应进行联合执法，严肃查处高仿 App 给使用者造成经济损失、个人信息泄露等情况。北京京师律师事务所律师张新年说，相关部门应通过案例发布、防范建议等形式提高用户保护个人信息和预防网络诈骗的能力。

吴沈括说，各大应用市场作为平台方，应进一步完善自身内部审核机制，对入驻应用软件提交的信息尽到法定和约定的审查、登记、检查监控义务，从源头治理高仿 App 问题。

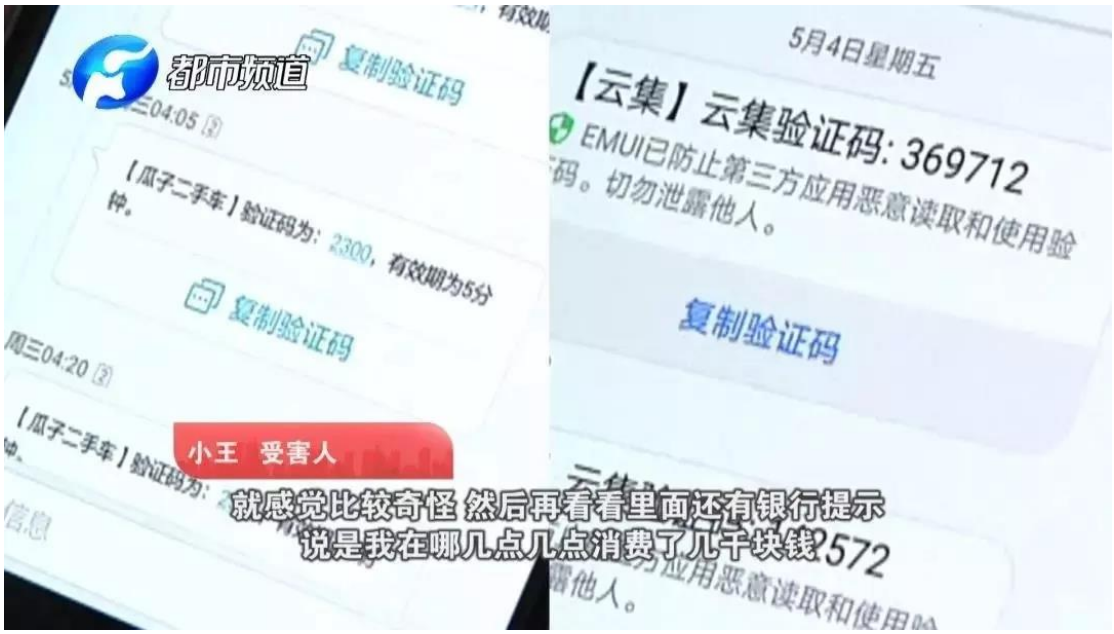
多位专家提醒：用户在使用 App 过程中，尤其遇到要求转账汇款等情况时，应仔细分辨应用真伪，不轻易接受对方指令。此外，App 中要求点击的不明链接，用户也要谨慎甄别，尽量不在不明链接里输入个人信息，以免信息遭泄露。（来源：北京青年网）

➢ 多人中招手机“自动”消费，最高损失十几万

2019 年 11 月 15 日，没丢手机也没丢银行卡，没扫二维码也没点短信链接，一觉醒来银行卡里的钱竟然没了!最近,河南郑州、新乡等地多个小区的居民遇到了这样的离奇事件，他们绑定手机支付平台的银行卡，半夜三更被神秘消费、莫名盗刷。

“嗅探” 三公里内刷爆所有银行卡

小王：“正睡觉了，听见手机短信一直响，说我在哪哪哪几点消费了几千块钱。”2018 年 5 月的一个深夜，短短几分钟，几十条短信提示声，把河南新乡的小王从睡梦中惊醒。短信的内容是消费扣款的通知。新乡市延津县公安局陈亭介绍说，跟小王住在同一小区的多名受害人，都有同样的遭遇：都是在凌晨的两三点、三四点钟，手机接到大量的类似于带有验证码的付款短信。



通过追踪资金流向，警方很快锁定了以孙某为首的五名犯罪嫌疑人，操纵盗刷他人银行卡的“黑科技”也浮出水面。警方介绍说，作案工具一个是采集设备，用来采集移动、联通手机号，还有个是“嗅探”设备，用来专门拦截手机短信。

根据孙某的供述，他们在福建龙岩还有一个上线，盗刷银行卡的“嗅探”设备就是从那里购买的。随后办案民警赶往福建龙岩，将犯罪嫌疑人张某抓获。至此，一个遍布全国、利用“短信嗅探”拦截验证码，进而盗刷他人银行卡的犯罪团伙被连根拔起。

“嗅探”到底是一个什么样的网络“黑科技”，竟然能拦截他人的信息、验证码，再实施盗刷？犯罪嫌疑人张某向警方交代：“这个手机号在我的设备范围之内，我们可以拦到它

的验证码，用它的手机号登录一些 APP、网站、网页，可以查询到机主的一些个人信息，然后通过这些盗刷。”

卖家：嗅探一开，钱哗哗进账

经过多方联系，记者匿名进入到一个名为“嗅探”的 QQ 群，群里一个名为“创富力电子嗅探”的群成员推销说：”我们最新款的有手机型短信嗅探器，可以直接嗅探附近的手机短信。”记者明确表达了购买“嗅探”设备的意向，然后根据卖家提供的接头地点，来到位于广州的一栋破旧大楼里，这里到处都是放风的人，一名二十多岁的的年轻人接待了记者：

卖家：“你好，想看什么产品？”

记者：“想看一看短信嗅探那个设备。”

卖家：“要范围拦截还是做指定拦截？”

记者：“就是附近的拦截的那种。”

卖家：“方圆附近就是拦截一到五公里，看你距离多远。”

除了单位拦截，卖家表示还能提供定制服务，也就是特定号码拦截，只要知道对方的电话号码，就能拦截他的短信、验证码，进而盗刷他绑定在手机上的银行卡：

记者：“指定号码拦截有没有距离限制？”

卖家：“那就没有，知道他的号码，把号码导进去就可以了。”

记者：“假如我知道他号码，他人在北京，我也可以拦截么？”

卖家：“没错，指定号码拦截没有限制这个距离。”

随后卖家拿出设备供记者查看，并表示只要把“嗅探”放在合适的位置，可以不停的有

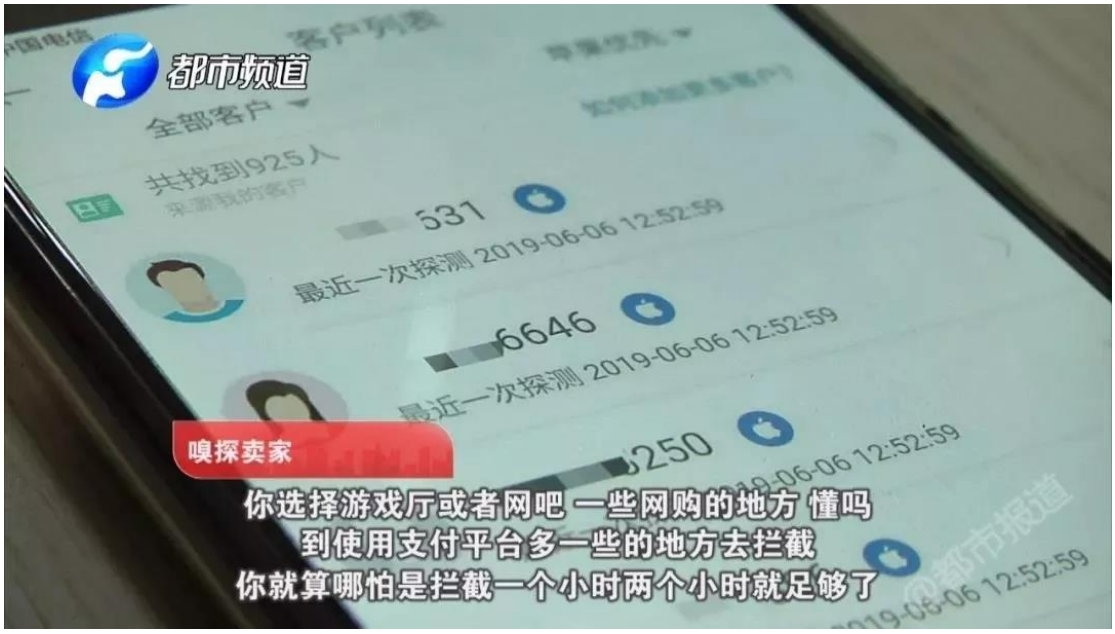
钱进账：

记者：“这还带个手机？”

卖家:“就是到时你拦截到的信息都是在这个手机里面搜集的，哪怕你就是转手给人家，也是通过电脑导出去。到使用支付平台多的一些地方去拦截，哪怕拦截一个小时两个小时也足够了。

记者实验：手机被“嗅探”操控

达成交易后，卖家通过快递从上海将一套“嗅探”设备寄给了记者，包裹里还隐藏了一个小小的 U 盘。在记者收到包裹的同时，一个自称是“嗅探技术员”的电话打了过来，远程指导设备安装：



嗅探技术员：“把这个 U 盘系统插上电脑，然后开机直接进入这个 U 盘的系统。”通过安装人员的介绍，“短信嗅探”的指挥系统，其实就是那个 U 盘，卖家把设置好的“拦截程序”隐藏在 U 盘里。操作流程简单说，就是利用“嗅探”扫描周围用户的手机号，然后再拦截用户的短信，与此同时用户仍可正常收取短信，不易被察觉。拦截到的信息包括收发短信双方的手机号码，以及信息的内容。而只要“嗅探”开始扫描，附近一到五公里内几乎所有的手机收到短信的同时，他们的电脑上也会显示同样的短信。卖家“技术员”给记者做了一个演示：

嗅探技术员：“第一条拦截是红颜色，第二第三条是蓝颜色，这两边都能看到，显示是一样的。频点出来了，一共扫描到 12 个，然后我们要的就是这个等号后面这些数字。”“嗅探”对手机隐私侵害到底有多强？来看记者的实验，看完让人脊背发凉！

安全黑洞，百万隐私信息已泄漏

更可怕的是，购买设备，卖家还赠送了他们搜集来的“个人信息”材料，包括姓名、电话号码、家庭住址，甚至还有家庭成员的姓名和电话。还有一种更高级的个人信息，就是银行卡号、开户行，甚至还包括银行卡密码。

记者留意到，普通的个人信息大多是通过快递单号搜集来的，在其中一些信息上，还有“签收”两个字。而这几百万条信息上的地址，有河南、广东、湖南、四川等等，涵盖全国多个省份。

如何防止手机被“嗅探”

凌晨时分实施更改密码的盗刷，设备异地邮寄规避警方检查，再加上非法搜集获取个人信息，“短信嗅探”盗刷已经形成了完整的黑色利益链，每个环节各自分工，相互配合。

今年 5 月，在河南郑州也发生多起盗刷案件，受害者被盗取金额最大的有十几万元。和新乡延津的盗刷案件一样，受害者也几乎都是住在同一个小区，盗刷时间也集中在凌晨。办案民警发现，一旦被“嗅探”设备盯上，手机信号可能会出现异常，迅速从 4G 变成 2G，接着就会频繁收到带有验证码的短信，然后银行卡、支付宝就被盗刷了。郑州市公安局二路岗分局案侦大队副大队长史非介绍说：

史非：“它使用了一个伪基站的原理，相当于您的这个手机连接这个基站，接收或者发送一条短信的时候，我这边机器也能够接收到这个短信，他获取这个信息之后，晚上再做这个撞库的操作。”

史非说，很多人的支付宝账号就是本人的手机号码，犯罪嫌疑人通过这个手机号在支付

宝或者其他第三方支付平台操作，如更改密码，然后手机会接到一条更改密码的动态密码短信，这个时候“嗅探”设备则会同步看到这一密码，通过密码实施盗刷：

虽然“嗅探”听起来很吓人，但并不代表不法分子可以为所欲为，我们也可以进行有效的防范。

史非：“居民在日常工作和生活当中，如果发现本来 4G 网络信号很稳定，突然手机信号降网了，降到了 2G 工作状态，就有可能在我们身边有伪基站或者是短信嗅探设备开机。这个时候要高度重视。减小损失的最安全的方式，就是（手机）要么关机，要么进入飞行状态，这样的话能保证我们的财产安全。”

警方重要提醒：防止被“嗅探”盗刷，一定做好以下几点：

1、平时要做好手机号、身份证号、银行卡号、支付平台账号等敏感的私人信息保护。

2、如果自己的手机信号忽然从 4G 降到 2G，有可能手机会受到攻击，请马上暂时启动飞行模式。

3、假如收到不明短信验证码，要马上意识到可能已被劫持攻击，可考虑暂时关机。

4、如果早上起来，看到半夜收到奇怪的验证码短信，一定要想到可能是遇到短信嗅探攻击，如果发现钱被盗刷了，火速冻结银行卡，保留短信内容并报警。（来源：中国之声）

➢ 7 家科技公司盗取身份证信息，4.68 亿个人信息泄露

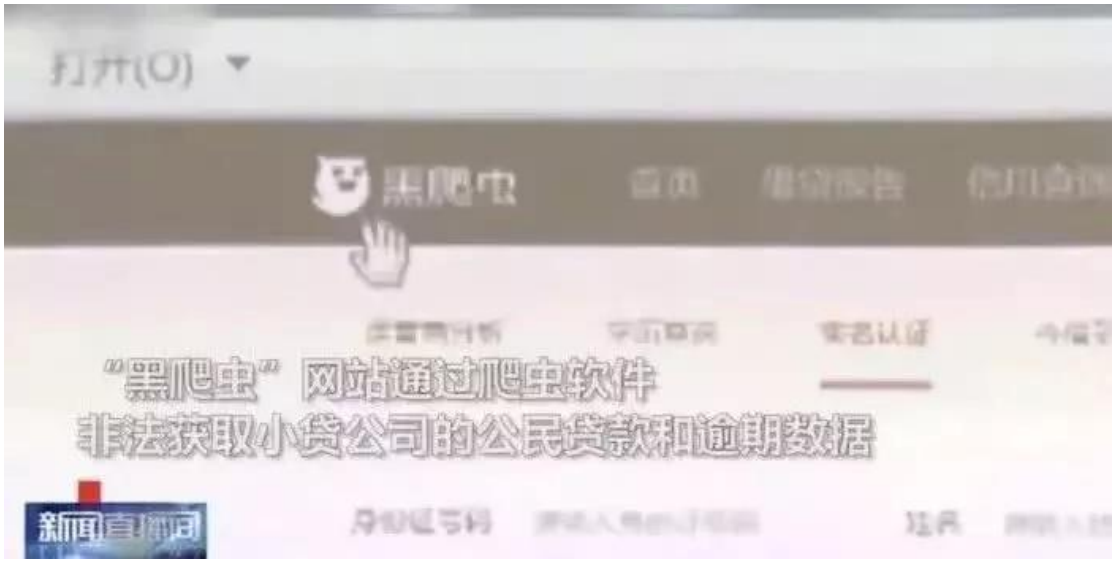
2019 年 11 月 19 日，江苏淮安警方破获了一起信息泄露案件，7 家科技公司涉嫌非法缓存公民个人信息超 1 亿条。其中，每天有 2500 万人次使用的支付软件拉卡拉，因为旗下公司考拉征信涉嫌非法提供身份证返照查询 9800 多万次、获利 3800 万元，已经有 20 名涉案人员被警方抓捕。

2019 年 11 月 20 日，拉卡拉股票跌停、市值已跌去 20 亿元；该公司回应称目前处于取证阶段，卡拉征信只是配合调查。尽管这一声明指出案件还未落实，但市场对个人信息泄露的反映仍在发酵。截至目前，警方已经立案侦查侵犯公民个人信息案件 29 起，缴获公民个人信息 4.68 亿余条。这些被泄露被贩卖至房车营销机构、网贷机构、催收机构甚至博彩机构，被泄露的人中不乏明星、上市公司高管、投资者等。这些个人信息全套的售价，最低竟然只卖一分钱！

都有哪些公司被查？

就在不久前的 10 月 21 日，51 信用卡被警方突击调查的一幕才刚发生。2019 年 11 月 19 日，江苏淮安警方就再次通报了一起骇人听闻的个人信息泄露案件，有 7 家公司涉嫌非法缓存公民个人信息超 1 亿条。警方是怎么发现这些线索的呢？

据通报，2018 年 4 月，江苏淮安警方在网上巡查时发现，有人非法购买公民个人信息，之后，嫌疑人高某主动到警方投案。



51 信用卡被突击现场

高某交代，他花 500 元从网名叫“过去、将来”的人手里购买了 317 条公民个人信息，这些信息包括手机号、姓名、身份证号和家庭地址。他买这些信息的目的是打电话，给网络小贷公司拉客户。

顺藤摸瓜之下，警方锁定了高某的上线申某。随后又通过申某的上线“挖”到了违法从事个人信息贩卖、小额贷款、软暴力催收等业务的广州诺涵科技公司。在进一步的侦查过程中，警方发现该公司的公民个人信息主要来自湖南九象信息有限公司。

锁定相关犯罪证据后，淮安警方在长沙、深圳分别将湖南九象公司的法定代表人和技术主管抓获。审讯得知，九象公司黑爬虫网站的“身份核验返照”业务端口来自北京黑格科技有限公司，而黑格公司是从北京考拉征信服务有限公司等四家公司购买的查询接口。

黑爬虫网站页面

随即，警方将北京黑格公司和考拉征信公司的法定代表人、董事长、销售、技术等 20 余名涉案人员抓获，并于今年 4 月在北京将他们上游公司的 5 名涉案人员抓获。

经查，北京考拉征信服务有限公司从上游公司获取接口后又违规将查询接口出卖，并非法缓存公民个人身份信息，供下游公司查询牟利，从而造成公民身份信息包括身份证照片的

大量泄露。

不查不知道，一查吓一跳。泄露个人信息谋取非法利益的考拉征信，正是仅次于支付宝、微信支付的全国第三大支付公司、有着 A 股市场“支付第一股”之称的拉卡拉的子公司。

支付场景中常见的拉卡拉 POS 机

拉卡拉本身作为支付巨头，截至到 2019 年 6 月 30 日，累计签约商户数 2100 万户，累计交易笔数达 36.7 亿笔、交易金额 1.7 万亿元；拉卡拉旗下各类主要 APP 用户总数也达到了 1500 万，公众号粉丝数合计约 2000 万，每天有 2500 万人次使用这一支付方式支付。

这些数据意味着，有上千万用户的个人信息，在使用拉卡拉的过程中面临着泄露风险。正因如此，考拉征信的涉嫌信息泄露的消息一出，拉卡拉的股票在 11 月 20 日开盘即迎来跌停，市值跌去了 20 亿元。

截止目前，该公司的相关人士回应称，“目前只是取证阶段，考拉征信是配合调查。拉卡拉只是考拉征信众多股东之一，拉卡拉与考拉征信之间的财务、业务、经营等都是各自独立的。”

个人信息黑产规模已超千亿

警方通报中提到，广州诺涵公司内部将公民个人信息称为“流量”。该公司开发了小贷平台“乐花管家”从事贷款业务，以所谓的“流量”作为其推销贷款和软暴力催收的基础。

广州诺涵公司获取“流量”的方式，除从湖南九象公司购买以外，还包括与其他公司交换，以及开发爬虫云等软件、利用技术手段爬取其他小贷公司的“流量”等等。在开展贷款、催收业务的同时，该公司也通过非法出售“流量”牟利。

广州诺涵公司内部的业绩会议照片

而广州诺涵的主要上线公司湖南九象公司，则是一家直接从事非法获取、贩卖公民个人信息的企业。与 51 信用卡涉嫌使用爬虫技术非法获取个人信息类似，该公司开发有一个黑爬虫网站，通过爬虫软件非法获取数十家小贷公司的公民贷款和逾期数据。

湖南九象公开提供收费查询服务，并提供“身份核验返照”业务，付费后任何人均可在其开发的网站输入公民姓名和身份证号码，查询获取公民身份证相片——这些照片由用户在使用拉卡拉等公司软件时上传。

由上述渠道泄露出去的个人信息，经不法分子或不法公司通过爬取、窃取等方式收集和贩卖后，导向了房地产、汽车、教育培训、游戏等行业的营销机构，甚至是网贷、催收、博彩等常年行走在灰色地带的不法公司。有媒体此前曾报道，泄露和贩卖个人信息产业已经发展成为一条产业规模超千亿元的黑色产业链。

被泄露的大量个人信息

“流量”只是这个黑色产业当中的“黑话”之一，黑产从业人员往往会用首字母指代某些业内专有名词。此前微博爆发过的明星个人信息泄露事件中，“sfz”“sjh”“hj”等分别用于代称“身份证（号码）”“手机号”“户籍”的暗语，就曾大量出现在网络上。

另外在大量贩卖个人信息的 QQ 群等社交媒体中，“WZ 加粉，CP 直推，QP 跑量，BC 引流”等暗语，也是黑产从业者常用的代号，用来指向个人信息的用途，分别代指“网赚”“彩票”“棋牌”和“博彩”。很多人手机上经常会收到“六合彩”等非法推销短信，就是泄露后被不法分子通过这些方式推送的。至于被贩卖的个人信息本身是极其廉价的，2019 年 8 月出现的“明星个人信息价格从几元到几十元不等，全套信息也只需要一百多元”实际上已经是卖出天价。

简历数据库公司巧达科技因涉爬被查封

媒体报道显示，此前曾有人在 QQ 群里售卖“2019 上市公司高管，新三板高管数万条”个人信息，售价也只有一万元——平均下来，一套上市公司高管个人的信息，价格也只有几

毛钱。股民的电话、住址、姓名等个人信息，价格最低更低至 1 分钱，它们主要被用于股票等证券产品推销。

据统计，近年警方已经立案侦查侵犯公民个人信息案件 29 起，缴获公民个人信息 4.68 亿余条，涉案金额 9400 余万元。在 51 信用卡被突击调查前后，已有巧达科技等多家爬虫公司被查。随着监管不断施压，未来还会有更多涉及个人信息黑产的公司“暴雷”。（来源：时代周报）

➢ 黑客发现电商平台漏洞在圈内炫耀：140 万被盗 33 人被抓

2019 年 11 月 19 日，据重庆市公安局渝中区分区官方微信公众号平安渝中消息，近日，在“2019 净网专项行动”期间，渝中区公安分局成功破获一起涉嫌利用某电商平台系统漏洞，疯狂实施盗窃其资金账户的“黑客”团伙犯罪案件，涉案金额高达 140 余万元。从今年 6 月开始至 11 月 9 日，渝中警方相继在全国十余省市抓获该案犯罪嫌疑人 33 名，平均年龄只有 20 岁左右。

“黑客”发现电商漏洞，篡改数据获利

今年 5 月，重庆渝中警方接到辖区内某商业管理公司报警，称他们的电商平台数据在 5 月 13 日 23 时至 14 日 6 时的 7 个小时内，出现异常，估计被黑客利用网站代码漏洞，恶意透支，通过第三方交易平台购买话费、油卡、实物等进行消费，共造成 140 余万元的资金损失。接到报警后，渝中区公安分局高度重视，经分局技术人员现场勘验、检查，发现

该电商平台存在支付流程逻辑漏洞，后通过民警的技术论证复原了嫌疑人整个作案经过。犯罪嫌疑人先在平台 APP 上注册 2 个账号，登录其中 1 个账号，向另一个账号进行转账操作，并在转账期间，使用抓包软件截取相关数据，然后修改转账数值(即把转账数值改成负数)，再将改好的参数，依原路径发送过去，在转账成功后转出的账号就是正数，而接收转账的账号就是负数。

通过不断重复以上操作，犯罪嫌疑人就完成了不花一分钱，使账号不断累积可变现的积分。接着再通过第三方交易平台，消费该平台账号资金，即不断为全国各地手机号码充值、办理充值加油卡、在大型电商平台上购物、在旅游网站上订酒店、预交旅行费用等多种方式进行套现。

圈内“炫技”一拥而上，终被一网成擒

在明确了嫌疑人作案手法后，渝中警方立即组织各警种成立专案组进行分析研判，开展侦查工作，查看比对相关信息。据介绍，警方通过涉案购买的话费充值手机号码、加油卡充值信息和网购平台的购物信息寻踪追线，主要犯罪嫌疑人，22 岁男子莫某某的真实身份终于浮出水面，接着专案组立即组织民警赶赴其所在地广西贺州，将嫌疑人成功抓获。

通过审讯，莫某某交代了其通过使用黑客软件扫描出该电商平台的系统漏洞后，利用从网上学来的黑客技术，盗取电商平台资金的犯罪事实。据莫某某交代，经过反复“实验”，5 月 13 日晚 23 时，他首次使用黑客技术，成功盗取了该电商平台内资金账户后，为炫耀“技术”，同时也为了掩盖自己的盗窃行为，立即将整个入侵盗窃过程，在自己的黑客圈子里进行发布传播，圈内“好友”们立即一拥而上，如法炮制，致使该电商平台在短短 7 个小时内损失 140 余万元，莫某某一人在其期间就盗窃走了 7 万多元。

从今年 6 月以来，截至 11 月 9 日，渝中警方专案组派遣精干力量，先后赶赴广西、广东、福建、黑龙江、山东、江西、四川、湖南、河北、河南、湖北、安徽、甘肃、重庆等全国 10 余省市，成功抓获本案的犯罪嫌疑人 33 人。据了解，该案中这些嫌疑人利用黑客技术盗取的资金从几千到数万元不等，其行为已经涉嫌盗窃罪，非法入侵计算机信息系统罪，以及非法破坏计算机信息系统罪。目前，其中 30 人已被刑事拘留，迎接他们的将是法律的严惩。

网络并非法外之地，如此“技术”不可效仿

“这起案件的涉案团伙成员，呈现出低龄化特征，被抓获的 33 名嫌疑人，平均年龄仅 20 岁左右。”据本案专案组负责人分析介绍，所有嫌疑人几乎都没有正当职业，还有部分是在校大学生。

他们就如同互联网中的“蛀虫”一般，学习到的计算机知识丝毫不用于正途，而是依靠扫描互联网上各平台系统漏洞，利用所学黑客技术非法入侵、破坏、控制计算机信息系统，并以此牟利。此外，这群人彼此间还会在一些社交软件平台上，相互“学习”、相互串联，交流黑客技术，以期达到分享信息，共同非法牟利的目的。

事实上，网络犯罪案件一直具有非接触、跨地域、跨时空、链条化、产业化、侦破难度大等特点。本案嫌疑人就广泛分布在全国 10 余省市，作案嫌疑人仅靠一台电脑、一根网线，就完成了从扫描平台漏洞，盗取账户资金，充值话费、油卡，购买机票、实物等，再到销赃变现各个犯罪环节的“一条龙”操作。（来源：IT 之家）