国盟信息安全通报

2019 年 11 月 11 日第 205 期

国盟信息安全通报

（第 205 期）

国际信息安全学习联盟

2019 年 11 月 11 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 478 个，其中高危漏洞 92 个、中危漏洞 339 个、低危漏洞 47 个。漏洞平均分值为 5.36。本周收录的漏洞中，涉及 0day 漏洞 101 个（占 21%），其中互联网上出现“Apache Solr 基于 Velocity 模板远程命令执行漏洞、ACTi ACM-5611 Camera 远程命令执行漏洞”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 8002 个，与上周（9602 个）环比减少 17%。

主要内容

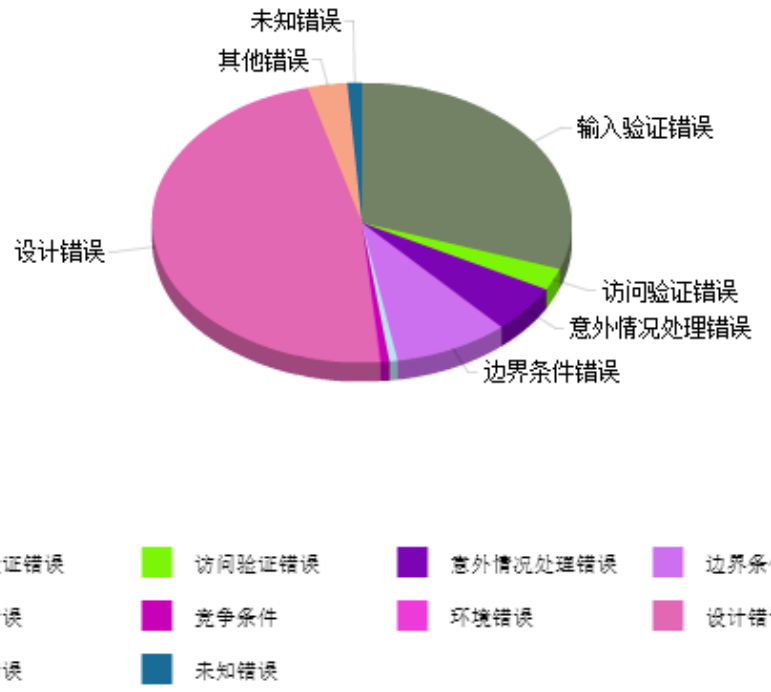
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

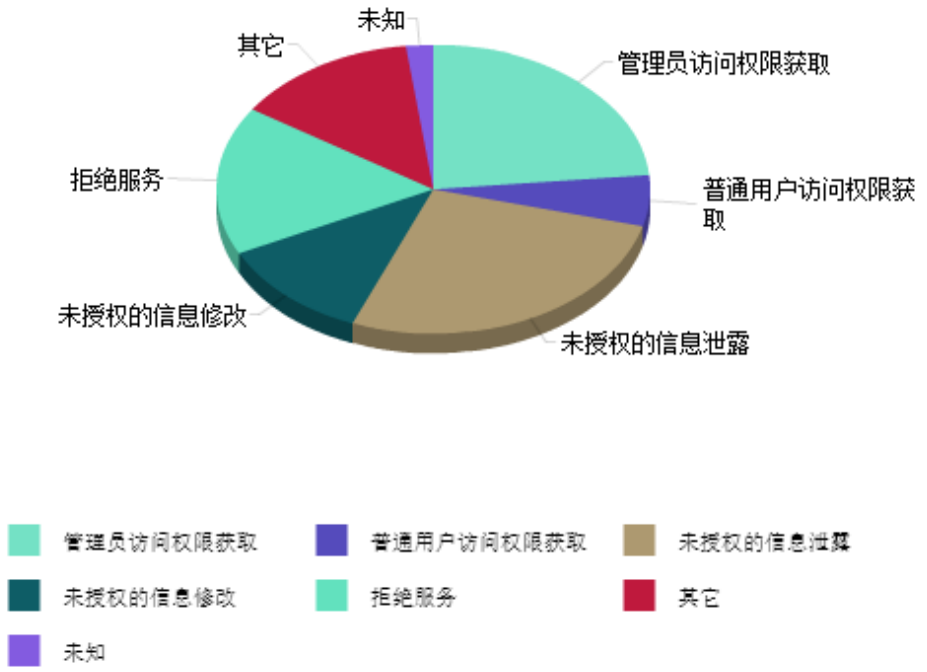
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 478 个，其中高危漏洞 92 个、中危漏洞 339 个、低危漏洞 47 个。漏洞平均分值为 5.36。本周收录的漏洞中，涉及 0day 漏洞 101 个（占 21%），其中互联网上出现“Apache Solr 基于 Velocity 模板远程命令执行漏洞、ACTi ACM-5611 Camera 远程命令执行漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 8002 个，与上周（9602 个）环比减少 17%。

二、安全漏洞增长数量及种类分布情况

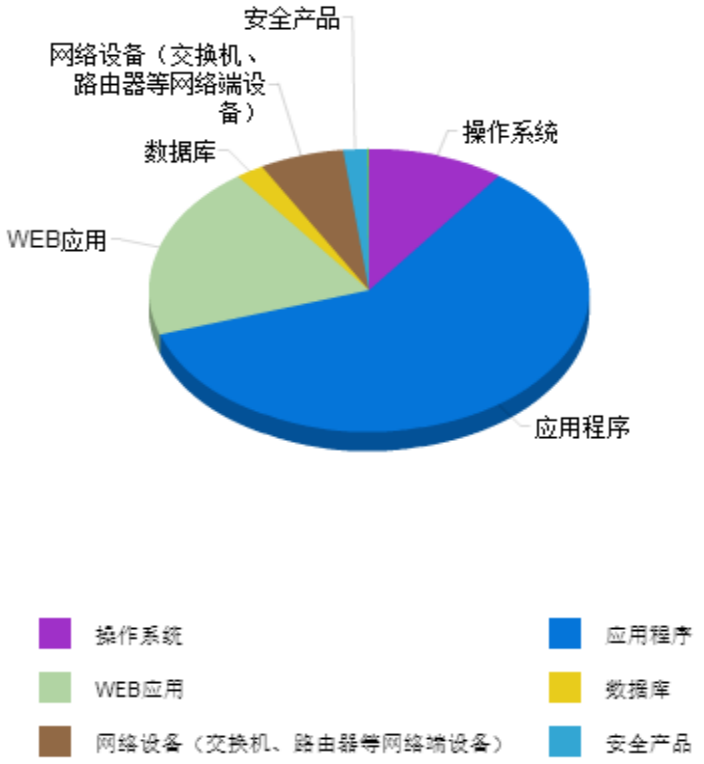
➢ 漏洞产生原因（2019 年 10 月 28 日—2019 年 11 月 11）



➢ 漏洞引发的威胁（2019 年 10 月 28 日—2019 年 11 月 11）



➢ 漏洞影响对象类型（2019 年 10 月 28 日—2019 年 11 月 11）



三、安全产业动态

➢ 述构建网络空间命运共同体 造福全人类

2019 年 10 月 20 日至 22 日，全世界的眼光又一次聚焦中国，世界互联网再次进入“乌镇时间”。国家主席习近平向第六届世界互联网大会致贺信，他指出：“发展好、运用好、治理好互联网，让互联网更好造福人类，是国际社会的共同责任。各国应顺应时代潮流，勇担发展责任，共迎风险挑战，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。”新时代的最强音回荡在中华大地和国际社会。

习近平主席倡导的构建网络空间命运共同体理念，从思想孕育、发展完善到逐渐成熟，为全球互联网发展治理贡献了中国智慧，赢得了广泛认同和高度赞誉。中国政府在互联网领域从落后时代、赶上时代到引领时代历程中提出的伟大倡议、付诸的伟大行动、经历的伟大事件、获得的伟大成就、凝结的伟大智慧，将激励全球人民在互联网发展征程中不断创造丰功伟业。

勇担互联网发展责任

网络空间命运共同体的理论建构、实践探索、成功经验和国际认同，意味着自诞生之日

起，久经互联网发展不平衡、规则不健全、秩序不合理“三座大山”压迫的全球网络成员迎来了从思想孕育、发展完善到逐渐成熟的伟大飞跃，迎来了擘画新时代互联网最大同心圆的光明前景。

思想孕育。网络空间命运共同体理念的提出，得益于中国对全球互联网治理生态和治理体系的战略思考，特别是以习近平同志为核心的中国共产党以勇立潮头、心系全球、敢为天下先的气概和胸襟，注重把握互联网时代的新特征、新规律、新趋向，高度关注网络空间对经济、政治、文化、社会、生态等领域产生的深刻影响。理论来源于丰厚的实践沃土。中国接入国际互联网 20 多年来，互联网发展取得了举世瞩目的历史性成就，溢出效应明显，新技术、新业态催生出“增量市场”，中国数字经济日益在全球舞台上发挥重要影响力。网络空间命运共同体理念正是在中国互联网发展的沃土中孕育，在致力解决全球互联网现实问题的伟大实践中开始萌芽。

发展完善。党的十八大以来，习近平主席高瞻远瞩地提出了网络强国战略思想，为完善网络空间命运共同体、强化国际社会相互尊重和相互信任奠定了重要基础，也成为推动构建网络空间命运共同体的坚实积淀。2014 年，首届世界互联网大会落户中国乌镇，搭建了中国与世界互联互通互信的国际平台和国际互联网共建共享共治的中国平台。这个平台怎么建？2015 年，习近平主席在出席第二届世界互联网大会开幕式时给出了答案：“网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体。”这一重要论述精准阐明了网络空间命运共同体建构的内在逻辑关系和发展路径，深刻描绘了深化全球互联网治理的当代价值。习近平主席向全世界发出的构建网络空间命运共同体的理念，不仅顺应了历史潮流，而且反映了全世界人民的共同心愿。

逐渐成熟。党的十九大以来，国际国内形势复杂多变，以习近平同志为核心的中国共产党不断深化对互联网建设规律、互联网发展规律和互联网治理规律的认识。习近平主席在致第四届世界互联网大会贺信中敏锐地指出，“全球互联网治理体系变革进入关键时期，构建网络空间命运共同体日益成为国际社会的广泛共识”，提出“深化互联网和数字经济交流合作，让互联网发展成果更好造福世界各国人民”。2017 年，中国政府发布《网络空间国际合作战略》，以和平发展、合作共赢为主题，以构建网络空间命运共同体为目标，就推动网络空间国际交流合作首次全面系统地提出了中国主张，为破解全球网络空间治理难题贡献了中国方案。2018 年，习近平主席向第五届世界互联网大会致贺信，提出“以共进为动力、以共赢为目标，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”。2019 年 10 月

16日，世界互联网大会组委会发布《携手构建网络空间命运共同体》概念文件，积极回应各方期待，全面阐释构建网络空间命运共同体理念的时代背景、基本原则、实践路径和治理架构。

共同推进网络空间全球治理

网络空间命运共同体为什么能？

构建网络空间命运共同体既是国际互联网治理的客观需要，也是构建互联网新秩序的必然要求。当今世界，正在经历一场更大范围、更深层次的科技革命和产业变革。互联网让世界变成了“鸡犬之声相闻”的地球村，也给世界各国主权、安全、发展利益带来了新挑战。个人隐私侵害、知识产权侵犯、网络犯罪、网络监听、网络攻击、网络恐怖主义活动等全球公害，已形成国际社会共识；互联网领域发展不平衡、规则不健全、秩序不合理等问题，被各国提上议事日程。基于互联网所具有的高度全球化特征，在面对上述风险挑战时，没有哪个国家能够置身事外、独善其身。

推进全球互联网治理体系变革是大势所趋、人心所向。世界各国虽然国情不同、互联网发展阶段不同、面临的现实挑战不同，但给经济社会发展插上互联网翅膀、造福本国人民福祉的愿望却完全相同。也正是基于这些国际共识，世界各国才更应该紧紧抓住新一轮技术创新、新工业革命、数字经济等新要素新业态带来的重大机遇，携手共建网络空间命运共同体，打造互联网和数字经济的新增长点，更好地造福于全世界人民。构建网络空间命运共同体，是构建人类命运共同体在网络空间发展演变的逻辑必然。

网络空间命运共同体理念的提出，表明中国站在全人类和全世界角度的思考，在观瞻、理念、思想上体现了中国作为国际大国的全球担当。习近平主席高屋建瓴地指出，“互联网发展是无国界、无边界的，利用好、发展好、治理好互联网必须深化网络空间国际合作，携手构建网络空间命运共同体”。这是推进全球互联网治理体系变革的中国理念、共同构建网络空间命运共同体的中国倡议，系统阐述全球网络空间治理新秩序的中国路径，清晰勾勒出了“中国网络观”的蓝图，充分表达了国际社会要求以新的理念引领互联网发展、以新的模式强化国际合作、以新的路径增强全世界人民福祉的共同心声。

国际社会对网络空间命运共同体理念发自肺腑的广泛认同，是推进网络空间命运共同体理念落地生根的根本保证。法国前总理多米尼克·德维尔潘在第四届世界互联网大会上强调，数字经济也创造了机遇，通过不断扩展的互联网基础设施，可以给边远的国家和地区提供卫生和教育等服务，今天各国需要做的就是建立一个集体的、合作的环境，将数据从信息流变成充满活力的资源。联合国网络安全高级专家尼尔·沃尔什在第六届世界互联网大会上表示：

“我们应该充分利用乌镇峰会这一平台，使其发挥出更大价值。中国通过世界互联网大会表明了打造互信共治的网络空间的主张，这应该成为世界各国的共识。”大道之行，从者云集。中国提出的网络空间命运共同体理念正在世界范围内得到越来越多的认同，逐渐成为全球共识。

可见，网络空间命运共同体是适应时代发展进步要求的网络治理新理念。集世界人民之智慧、聚世界各国之力量，才能有效破解互联网治理难题。网络空间命运共同体以增进全球福祉、促进共同繁荣作为最终归宿。中国始终倡导求同存异、休戚与共、平等尊重，构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的全球互联网治理体系。倾听每一种声音，尊重每一个合理化建议，尊重彼此在不同发展阶段采取的有区别的管理方式，在处理国际互联网治理事务中，中国总是站在历史的正确一边。网络空间命运共同体理念充分彰显了中国政府的合作精神和对人类、对世界的责任。

让互联网更好造福人类

当前，我们正面临世界百年未有之大变局，国际利益格局调整与国际秩序转型速度加快，世界多极化、经济全球化、社会网络化是当今世界的基本特征。国际社会要主动顺应互联网发展带来的历史机遇，致力于利用好、发展好、治理好互联网，让互联网发展成果更好造福世界各国人民。

坚持尊重维护网络空间主权。坚持尊重维护网络空间主权，就必须尊重网络空间管辖权，允许各国在自己的网络主权空间范围内依法管网，保护本国基础设施、信息系统、数据资源和空间活动不受侵犯。加快建立网络空间国际关系基本准则，防止网络空间成为新的战场。

坚持完善网络治理体系。网络空间是人类共同的活动空间，网络空间治理的话语权应由世界各国共同掌握。构建网络空间命运共同体，就要消除缠斗不止的零和思维、赢者通吃的垄断思维和一家独大的丛林思维，深化网络空间治理和参与机制规则，推动在联合国框架下制定各国普遍接受的网络空间国际规则和国家行为规范，确立国家及各行为主体在网络空间应遵循的基本准则，加快使“信息安全国际行为准则”得到国际理解与支持。

坚持强化网络空间国际合作。随着网络空间国际合作不断深化，相隔万里的人们不再“老死不相往来”。“单丝不成线，独木不成林”。深化在世界互联网大会（乌镇峰会）、东盟地区论坛、博鳌亚洲论坛、上合组织、金砖国家、亚信会议、中非合作论坛等多框架下交流合作，拓展网络对话合作平台。加快消弭不同国家、地区、人群间的信息鸿沟，架起横亘全球的网上之路。合作打击网络监听、网络攻击、网络恐怖主义活动“三大公害”，建设文明诚信的网络环境，打造人类共同的网上家园。

坚持推动数字经济发展和数字红利普惠。随着互联网时代的到来，数字经济蓬勃发展，数字红利潜能巨大。中国正积极推进数字产业化、产业数字化，引导数字经济和实体经济深度融合，推动经济高质量发展。助推全球互联网合作创新，推动世界各国共同搭乘互联网和数字经济发展的快车，使互联网真正成为推动全球经济变革、效率变革和动力变革的加速器，撬动经济社会发展的新杠杆，增进民生福祉的新引擎。

我们有理由相信，随着网络空间命运共同体的逐步构建，互联网必将迎来更加强劲的发展动能和更加广阔的发展空间，也必将更好造福全人类。（来源：光民日报）

➢ 互联网金融风险分析及监管建议

在互联网技术迅速发展的大背景下，互联网金融得到了快速的发展，关于传统金融与互联网金融的唇枪舌战一直就没有消停过。任何新生事物的发展都会伴随着新的风险发生，互联网金融也不会例外，近几年来频繁爆发的 P2P 平台倒闭、老板携款潜逃给民众带来了巨大的伤害。为防范互联网金融风险，笔者从互联网金融的概念出发，揭示了互联网金融的本质特征，分析互联网金融风险所在，提出了防范互联网金融的措施建议。

互联网金融概念及其特征

所谓互联网金融（ITFIN）就是互联网技术和传统金融功能的有机结合，主要指依托大数据和云计算在开放的互联网平台上形成的功能化金融业态及其服务体系，包括基于网络平台的金融市场体系、金融服务体系、金融组织体系、金融产品体系以及互联网金融监管体系等。互联网金融突破了传统金融时间和空间的限制，呈现出成本低、监管弱、效率高、覆盖面广和风险大等主要特征，最受新生代年轻人所喜爱。目前互联网金融主导者来自两个方面，一是传统金融机构的信息网络化，指传统金融业务的互联网化及电商化创新、金融业务 APP 软件等；二是非金融机构依托互联网开展的金融电商业务，指大的互联网公司利用互联网技术优势进行金融监管套利，开展金融业务。目前互联网金融主要业务模式有 P2P 模式的网络借贷平台，众筹模式的网络投资平台，理财模式的手机理财 APP，货币模式的数字货币，以及第三方支付平台等。

互联网金融风险分析

1.传统金融风险

尽管互联网金融有着华丽的外衣、网络的特质，但其资金融通、价格发现、支付清算等方面的金融本质还没有改变，必然有着传统金融的相同风险。一是市场风险，由于市场因素(如利率，汇率，股价以及商品价格等)的波动而导致的金融参与者的资产价值变化的风险。二是信用风险，由于借款人或市场交易对手的违约(无法偿付或者无法按期偿付)而导致损失的风险。三是流动性风险，当金融参与者无法通过变现资产或者减轻资产方式筹集现金等价物来偿付债务时，流动性风险发生。

2.网络技术风险

互联网金融是以互联网为平台的金融，是以互联网形式表现的金融服务。如果网络技术出现问题，那互联网金融就失去了赖以生存与发展的基础，因此网络技术的风险是互联网金融的首要风险。尽管经过多年的发展，互联网技术已经是比较成熟了，但其风险依然不可避免。一是物理网络并非坚不可摧的，因自然灾害、电力因素、人为因素等原因，物理网络可能完成失效。二是基于物理层的互联网传输可能出现故障、网络平台系统可能因黑客攻击、计算机病毒等因素完成瘫痪。一旦网络软硬件或基础协议出现故障，整个互联网金融交易将面临网络全面瘫痪的风险。

3.法律合规风险

一是互联网金融是新兴业态，对于参与主体及其网络交易行为法律界限不明。现有法律法规对互联网金融平台公司和平台交易市场主体的法律定位尚不明确，到底什么样的自然人和企业法人才具有参与合法参与资格，法律上还有待明确。金融主体有不能触碰的两条底线：

非法集资和非法吸收公众存款，在互联网上该如何界定触碰底线的交易行为，法律也没有给出明确的答案。二是互联网企业内控制度不健全，合规性易被突破。合理的内控制度是互联网企业的“防火墙”，能有效防范经营风险。实践中，一些互联网金融企业片面追求业务拓展和盈利能力，创新推出一些有争议、高风险的交易模式，但并没有建立客户身份识别、交易记录保存和可疑交易分析报告机制，容易为不法分子利用平台进行洗钱等违法活动创造条件;也有一些互联网企业不注重内部管理，信息安全建设水平低下，客户信息泄露事件常常发生。

4.道德与信用风险

中国互联网金融信用体系建设仍处于起步阶段，网络平台信用体系并不完善，平台爆雷、老板跑路、欺诈交易行为不时发生。目前存在几个主要问题：一是互联网金融交易主体身份认定问题。部分交易主体在身份认定上并非实名制，关键信息缺失或不真实，而且缺少有效的网络安全防范措施，客户信息安全无法得到保障；二是互联网金融交易过程虚拟化程度高，交易全过程透明度低下，交易真实性不易考察验证。三是互联网金融的交易资金管理不规范。部分互联网金融的线下资金的第三方存管制度缺失，资金管理不规范，存在较大的道德风险。例如，现在一些 P2P 网络借贷平台没有建立资金第三方托管机制，会有大量投资者资金沉淀在平台账户里，如果没有外部监管，就存在着资金被挪用甚至携款“跑路”的道德风险。

互联网金融风险的监管建议

1.加强互联网金融知识宣传，提高风险防范意识

对于普通百姓来说，互联网金融还是新兴的事物，对互联网金融的认知还需要一个过程。互联网金融的风险管理需要从知识的普及与宣传教育开始。对互联网金融风险来说，防范重于监管，管理部门必须强化日常知识普及宣传、专栏风险防范宣传，推进互联网金融知识及风险防范警示教育工作制度化、常态化。让日常宣传进学校、进社区、进乡村、进商圈，向社会公众广泛普及互联网金融知识，树立科学理性的投资意识，增强社会公众的对互联网金融风险的防范意识和自我保护能力。

2.完善互联网金融相关法律法规

互联网金融离不开法律法规的保障，应尽快完善互联网金融法律体系，以立法的形式明确互联网金融机构的性质和法律地位，对其组织形式、准入资格、经营模式、风险防范、监督管理和处罚措施等进行规范。一是对现有法律法规进行互联网补充。我国现行法律法规多数都是出台于互联网兴起之前，由于历史的局限性，当时没有考虑互联网因素，因此我们需要对现有相关金融管理法律、法规、办法进行修订与完善，弥补监管法规的互联网金融空白，

增加前瞻性和开放性，充分考虑未来的发展和业态变化。二是加快互联网金融技术规则和国家标准的制定，互联网金融涉及的技术环节较多，如物理网络、网络协议、系统软件、数据保护、密钥管理、客户识别、身份验证等，对于互联网金融的技术标准和业务规范标准必须尽快制定。

3.加强互联网金融征信体系建设

信用是金融的基础和根本，互联网金融的良性发展离不开市场主体的信用体系建设。一是加强全国征信信息系统在互联网金融平台的应用，由于互联网金融是基于网络平台的交易，交易双方互不认识，不存在资产抵押的可能，交易者完全是基于对平台的信任而交易，因此，互联网金融平台必须公开其信用信息，市场参与主体必须向平台提供其信用信息；二是加强互联网金融平台信用信息采集，把互联网金融交易主体及平台全部纳入信用信息采集范围，让不良信用行为付出相应的代价；三是建立统一的互联网金融信息披露平台，对于互联网金融交易中的不诚信主体进行公开曝光，加强交易主体与平台方的相互监督，减少欺诈交易的发生率，促进互联网金融市场健康良性发展。

4.建立自律机制，增强互联网金融信息透明度

互联网金融风险的主要原因之一就是信息不对称，而来自同行的信息是最有参考价值的。想要有效监管互联网金融风险，首先要成立互联网金融行业协会，建立自律机制，加强行业内部相互监督，从源头上防范不诚信行为。其次，增强互联网金融平台的透明度也非常重要，要求互联网金融产品与服务者提供通俗易懂、真实准确、系统全面的信息，使普通投资者能够正确理解相关的互联网金融信息，避免盲目投资而引发风险。（来源:《金融电子化》2019 年 9 月刊）

➢ 网络安全与国家安全关系的五个特点

在全球从传统经济社会向数字经济社会转型的过程中，网络空间和物理空间高度融合使原有社会规则和秩序面临重大变革甚至重构需求。各国在网络空间主权、网络治理目标、网络安全规则等方面的分歧，给全球网络治理和构建数字世界新秩序带来挑战，同时，新技术新应用“突飞猛进”，带来更多不确定性和新的安全风险，亟需要各国共同探寻并构建数字世界新秩序。

所谓国家安全，是个综合概念，包括政治、经济、军事及其他各领域。随着新技术的发

展，特别是网络技术的发展，很多国家的不安全因素越来越多。那么，网络安全与国家安全是什么关系？

第一，网络安全的基础性。随着高新技术的发展，国际物联网的发展，万物互联、新技术不断推动人类社会的发展，第四次工业革命也是以信息技术革命为龙头，越来越成为国家关键基础设施的龙头。从这个角度说，网络安全以及网络新技术确实是国家安全问题。

第二，网络安全的技术性。新技术的发展，行业的不断创新，使人类对于网络的发展寄予越来越大的希望。网络，相对于现实空间、人类社会以及军事等各个方面，都有实质性的发展。但是，人类的监管以及技术的规范，永远跟在技术发展的后面，而不可能走在前面。从这个角度说，现在一些国家强调所谓的“绝对安全”，这个理念实际上是不成立的。网络安全永远是以相对安全为基础，处理技术进步的问题。换句话说，技术进步的问题不一定都是国家安全问题。

国家安全这个概念泛化的问题，实际上和技术发展有很大的关系。举个例子，在 4G 之前，美国在无线技术领域占有最强的优势。无论从技术规范、设备等等，都在世界前列。在 4G 之前，美军从来没有提出过无线通讯的问题，而到了 5G，由于标准选择的问题，出现了两条道路，因此，美军就面临在国际上要与其他规范，即中欧的规范，进行接口连接的问题。自然产生了所谓安全关注的问题，所谓国家安全的问题。如果从合作的角度去考虑这个问题

的话，完全可以有办法把这个问题从技术的角度解决，而不用与其他国家进行技术切割，对人员的交流往来进行切割，对国际合作进行切割，这样做的后果将导致技术发展碎片化。

第三，主权性的问题。网络安全是有主权的，这一点过去西方国家不太承认。但是，自从 2016 年美国大选受到所谓“通俄门”事件的影响，西方世界也开始重视网络主权性。网络安全不应该影响国家的稳定、安定。

第四，网络安全的伦理性。信息技术的发展、跨境的信息流动以及网络生物技术识别，还有知识产权问题，都事关网络伦理的问题。

最后，可追溯性。由于技术性，自然造成所谓“电子痕迹”的问题。可追溯性是强调网络安全一个非常重要的特点，是区别于任何的所谓安全问题的一个标志。当用国家安全的概念指责某一种技术的发展、某一个国家政策方向的时候，在网络安全的角度必须要有证据，而不是莫须有。

所以，这五个特性决定了两个方面：第一，网络安全要有一个所谓的国家安全利益；第二，网络安全一定要促进数字经济的发展，也就是国家发展利益。这两个支柱加上能够确保一个国家的社会、政治稳定，这三个支柱加起来，才可以构成所谓的国家安全的概念。

在目前整个世界形势发展这么快的情况下，人类社会出现动荡不定的趋势。今年 6 月，G20 峰会大阪宣言，专门讲到数字经济问题。各国政府都很关注数字经济的发展，要确保数字经济的安全、稳定、可持续，而并没有要用国家安全的概念阻碍数字经济的发展。

因此，安全利益、发展利益、国家稳定，这三大支柱是能够确保国家安全最基础的东西，也是促进国际合作中需要关注的问题。（来源：《中国信息安全》杂志 2019 年第 9 期）

➢ 新时代密码工作的坚强法律保障

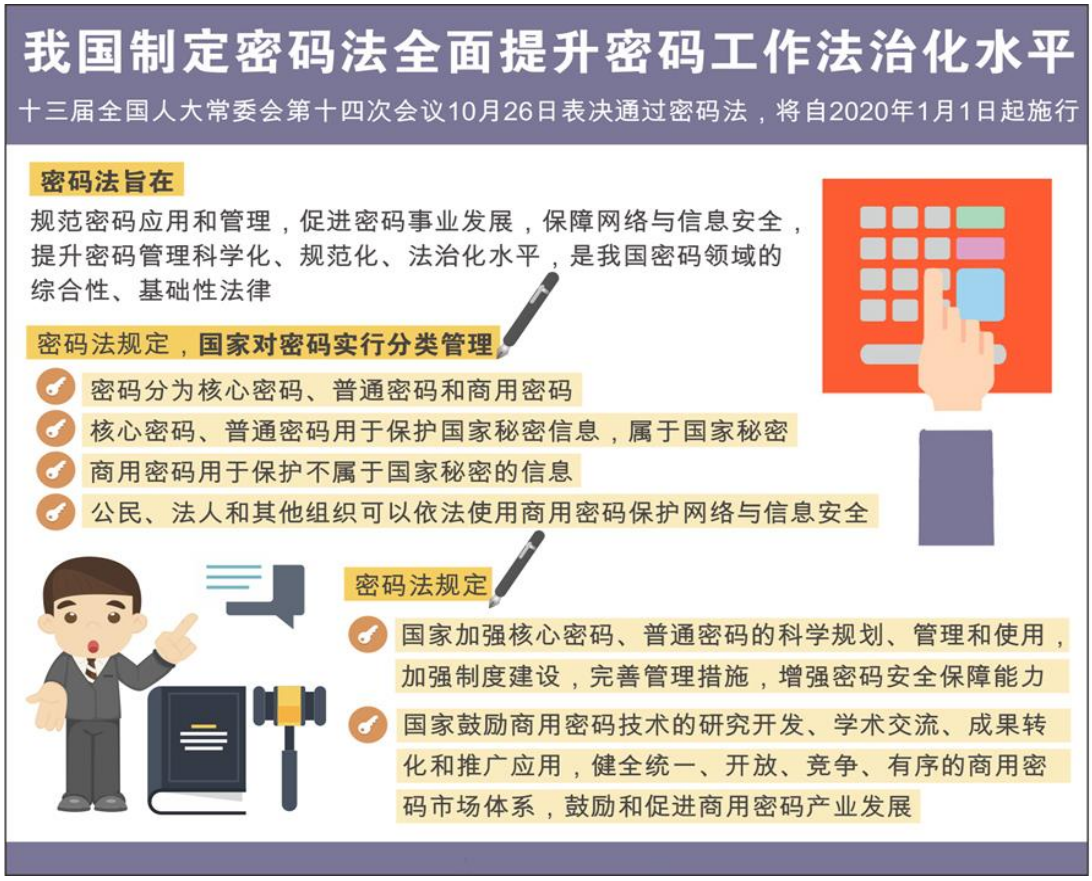
2019 年 10 月 26 日，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，习近平主席签署主席令予以公布，将于 2020 年 1 月 1 日起正式施行。密码法的颁布实施，是密码工作历史上具有里程碑意义的大事，必将对密码事业发展产生重大而深远的影响。

充分认识制定和实施密码法的重要意义

密码是我们党和国家的“命门”“命脉”，密码工作是党和国家的一项特殊重要事业，在我国革命、建设、改革的各个历史时期，都发挥了不可替代的重要作用。进入新时代，密码工作面临许多新的机遇和挑战。制定和实施密码法，对于深入贯彻落实党中央决策部署和习

近平总书记重要指示批示精神，全面提升密码工作法治化和现代化水平，具有十分重要的意义。

第一，这是构建国家安全法律制度体系的重要举措。党的十八届四中全会提出，贯彻落实总体国家安全观，加快国家安全法治建设，构建国家安全法律制度体系。密码工作直接关系国家政治安全、经济安全、国防安全和信息安全。党中央高度重视密码立法工作，将密码法作为国家安全法律制度体系的重要组成部分，强调要在国家安全法治建设的大盘子中研究制定密码法，把党对密码工作的最新要求通过法定程序转化为国家意志。制定和实施密码法，填补了我国密码领域长期存在的法律空白，对于加快密码法治建设，理顺国家安全领域相关法律法规关系，完善国家安全法律制度体系具有重要意义。



第二，这是维护国家网络空间主权安全的重要举措。密码是目前世界上公认的，保障网络与信息安全最有效、最可靠、最经济的关键核心技术。在信息化高度发展的今天，密码的应用已经渗透到社会生产生活各个方面，从涉及政权安全的保密通信、军事指挥，到涉及国民经济的金融交易、防伪税控，再到涉及公民权益的电子支付、网上办事等等，密码都在背后发挥着基础支撑作用。制定和实施密码法，就是要把密码应用和管理的基本制度及时上升为法律规范，推动构建以密码技术为核心、多种技术交叉融合的网络空间新安全体制，努力做到党和国家战略推进到哪里，密码就保障到哪里。

第三，这是推动密码事业高质量发展的重要举措。我们党的密码工作诞生于烽火硝烟的 1930 年 1 月，是毛泽东、周恩来等老一辈无产阶级革命家亲自领导创建的，已经走过了近 90 年的光辉历程。革命战争年代，党中央通过密码通信这一重要渠道运筹帷幄、决胜千里。仅在指挥三大战役期间，毛泽东同志就亲自起草密码电报 197 份，批签密码电报上千份。电影《永不消逝的电波》中李侠的人物原型——中共上海地下党员李白，以及被誉为“龙潭三杰”之一的钱壮飞等革命烈士都是密码战线的优秀代表。党的十八大以来，在以习近平同志为核心的党中央坚强领导下，在中央密码工作领导小组领导指挥下，密码事业取得历史性成就、实现历史性变革。制定和实施密码法，就是要适应新的形势发展需要，推进密码领域职能转变和“放管服”改革，建立健全密码法治实施、监督、保障体系，规范密码产业秩序，提升密码自主创新水平和供给能力，为密码事业又好又快发展提供制度保障。

准确把握密码法的精神实质和主要内容

密码法立法既注意总结我国密码管理中形成的一系列好传统、好经验、好做法，又适应新情况、新问题、新挑战，改革重塑了现行相关管理制度，体现了继承发展、守正创新精神。贯彻实施密码法，重点要领会把握好以下原则。

第一，坚持党管密码和依法管理相统一。党管密码原则是密码工作长期实践和历史经验的深刻总结，密码工作大权在党中央，密码工作大政方针必须由党中央决定，密码工作重大事项必须向党中央报告。密码法规定，坚持中国共产党对密码工作的领导，旗帜鲜明地把党管密码这一根本原则写入法律，同时明确中央密码工作领导机构统一领导全国密码工作，这是密码法最根本性的规定。随着全面依法治国基本方略的深入实施，依法管理已经成为党管密码的基本方式和内在要求。只有坚持党管密码，才能保证密码管理沿着正确的方向不偏离、不走样。只有依靠依法管理，才能将党管密码的具体制度纳入法治化轨道。

第二，坚持创新发展和确保安全相统一。安全是发展的前提，发展是安全的保障。密码法依法确立了促进密码事业发展的一系列制度措施，努力为密码科技创新、产业发展和应用推广营造良好环境。同时要看到，密码作为一种典型的“两用物项”，用得好会造福社会，用得不好或者被坏人利用，就可能给党和国家利益带来不可估量的损失。因此，密码法明令禁止任何组织或者个人窃取他人加密保护的信息，非法侵入他人的密码保障系统，或者利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

第三，坚持简政放权和加强监管相统一。党的十九大报告指出，转变政府职能，深化简政放权，创新监管方式。密码法明确了密码分类管理原则，规定核心密码、普通密码用于保护国家秘密信息，由密码管理部门实行严格统一管理。在商用密码管理方面，充分体现职能

转变和“放管服”改革要求，充分体现非歧视原则，大幅削减行政许可事项，进一步放宽市场准入，对国内外产品、服务以及内外资企业一视同仁，规范和加强事中事后监管，切实为商用密码从业单位松绑减负。

切实抓好密码法的宣传贯彻实施

密码法为做好新时代密码工作提供了强大法律武器。贯彻实施好密码法，必将有力地推动密码事业发展。我们一定要在贯彻实施上狠下功夫，做到有法必依、执法必严、违法必究。

第一，深入开展密码法宣传普及。要贯彻密码法要求，把密码安全教育纳入国民教育体系和公务员教育培训体系，充分利用“全民国家安全教育日”“国家网络安全宣传周”等平台，深入开展密码法宣传普及活动，推动密码进社会、进课堂、进教材、进网络，努力在全社会营造“知密码、懂密码、用密码”和尊法、学法、守法、用法的浓厚氛围。各级密码管理部门和涉及密码工作的机关单位要采取多种形式，组织好本部门本单位的学习、宣传和培训工作，让密码工作人员深刻理解密码法各项规定，不断提高依法从事密码工作的能力和水平。

第二，严格执行密码法各项规定。各级密码管理部门要切实抓好密码法的贯彻实施工作，把实施好这部法律作为落实党中央决策部署、加强和改进新时代密码工作的重要抓手。国家、省、市、县四级密码管理部门要依法确立行政主体地位，全面履行密码法赋予的行政管理职能，加快推动管理职能转变和管理方式创新。要积极配合市场监管、网信、商务、财政、发展改革等职能部门，在职责范围内履行好密码管理和保障职责，确保密码法各项制度措施落到实处。

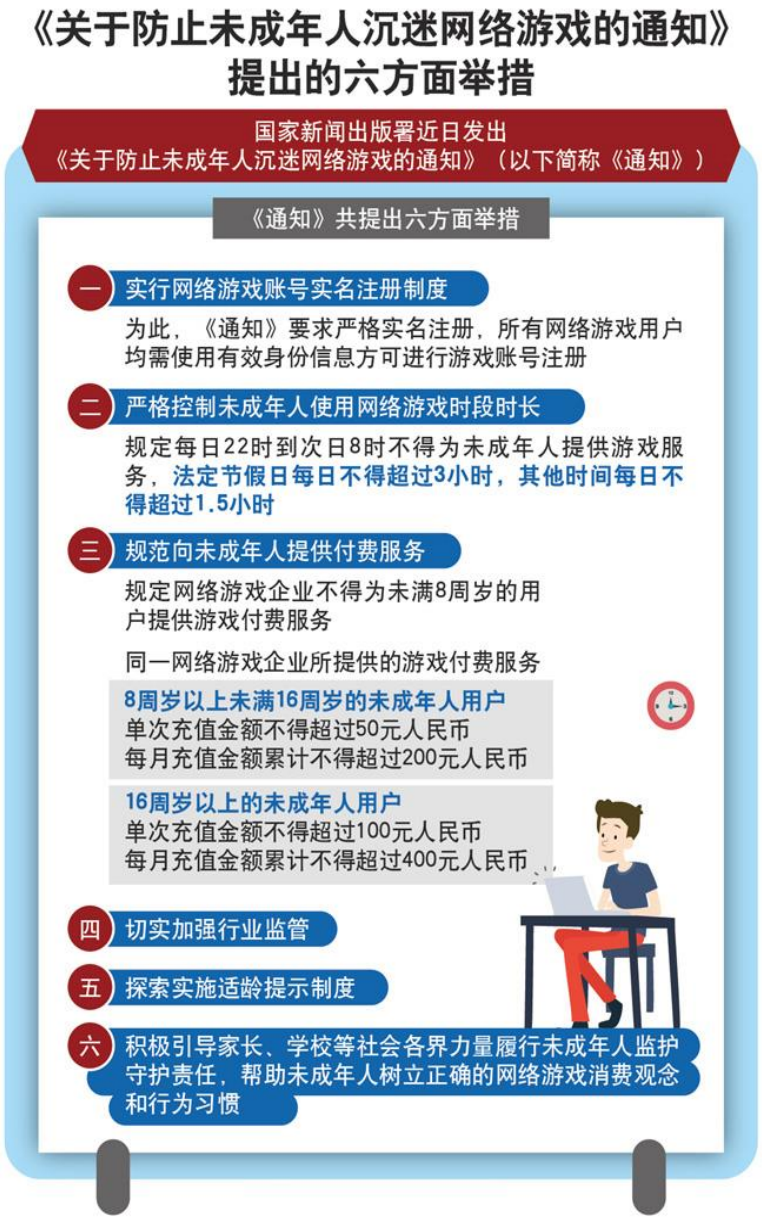
第三，抓紧完善密码法配套制度。国家密码管理局将紧紧抓住密码法出台的契机，加强密码法律制度的顶层设计和整体规划，统筹推进《商用密码管理条例》等配套法规制度的制定修订工作，确保密码法规制度符合密码法确定的立法原则和基本制度，与密码法的相关规定相互协调和衔接。地方各级密码管理部门也要根据密码法，及时清理和制定修订本地区出台的密码法规制度，不断推进本地区密码工作制度化、规范化。

做好新时代密码工作，责任重大，使命光荣。让我们紧密团结在以习近平同志为核心的党中央周围，增强“四个意识”，坚定“四个自信”，做到“两个维护”，不忘初心、牢记使命，坚持党管密码不动摇、创新发展不动摇、服务大局不动摇，全力以赴推动密码法贯彻落实，以优异成绩迎接党的密码工作创建 90 周年，为开创新时代密码工作新局面、实现中华民族伟大复兴中国梦作出新的更大贡献！（来源：人民日报 作者：密码管理局局长：李兆宗）

四、政府之声

➢ 国家新闻出版署发布《关于防止未成年人沉迷网络游戏的通知》

2019 年 11 月 5 日，国家新闻出版署近日发出《关于防止未成年人沉迷网络游戏的通知》（以下简称《通知》）。国家新闻出版署有关负责人就《通知》有关情况，接受了记者专访。



问：请介绍一下《通知》出台的背景和意义。

答：近年来，我国网络游戏业发展迅速，在满足群众休闲娱乐需要、丰富人民精神文化生活的同时，也出现部分未成年人沉迷游戏、过度消费等一些值得高度关注的问题。这些问

题影响未成年人身心健康和正常学习生活，社会各界反映强烈。为积极回应社会关切，解决行业发展中的突出问题，我们开展相关调研，多方听取意见，制定具体措施，形成了本《通知》。《通知》以习近平新时代中国特色社会主义思想为指导，充分体现社会效益优先、未成年人保护优先的原则，坚持问题导向，针对当前防沉迷存在的重点难点问题，精准施策、靶向治疗，提出了关于防止未成年人沉迷网络游戏的工作要求和具体安排，明确了网络游戏行业为未成年人提供服务应遵循的原则和规范。《通知》在集中解决突出问题基础上，强调严格落实企业主体责任，依法履行政府监管职责，推动社会各界协同治理、有效参与，形成政府、企业、社会共管共治。《通知》的制定和实施，对于加强和改进网络游戏管理，切实保护未成年人身心健康，营造风清气朗的网络空间，具有重要意义和切实作用。

问：《通知》提出了哪些具体要求？主要考虑是什么？

答：《通知》共提出六方面举措，一是实行网络游戏账号实名注册制度。目前，游戏用户实名注册方式包括手机号、微信号、身份信息等多种方式。但实际使用中，不少未成年人使用家长手机号、微信号注册游戏账号，导致针对未成年人的管理制度难以真正落地。为此，《通知》要求严格实名注册，所有网络游戏用户均需使用有效身份信息方可进行游戏账号注册。二是严格控制未成年人使用网络游戏时段时长。规定每日 22 时到次日 8 时不得为未成年人提供游戏服务，法定节假日每日不得超过 3 小时，其他时间每日不得超过 1.5 小时。具体标准主要是从合理分配未成年人日常作息时间角度提出，除去正常睡眠、学习、用餐及文体活动时间外，区分节假日和其他时间，对游戏时段时长予以限定。这一规定既是对网络游戏企业和平台的要求，也是对监护人履行未成年人监护义务的指导。三是规范向未成年人提供付费服务，规定网络游戏企业不得为未满 8 周岁的用户提供游戏付费服务；同一网络游戏企业所提供的游戏付费服务，8 周岁以上未满 16 周岁的未成年人用户，单次充值金额不得超过 50 元人民币，每月充值金额累计不得超过 200 元人民币；16 周岁以上的未成年人用户，单次充值金额不得超过 100 元人民币，每月充值金额累计不得超过 400 元人民币。主要参考《民法》总则中对民事行为能力的区分，以及有关方面就家长对孩子使用网络游戏消费限额意愿进行的抽样调查，并适当考虑目前未成年人实际付费状况。四是切实加强行业监管。要求对未落实本通知要求的网络游戏企业，各地出版管理部门应责令限期改正；情节严重的，依法依规予以处理，直至吊销相关许可。五是探索实施适龄提示制度。随着网络游戏类型越来越多样化，在题材、内容、玩法等各方面都可能存在不适宜未成年人体验的问题。《通知》要求网络游戏企业从多维度综合衡量，探索对网络游戏予以适合不同年龄段用户的提示，帮助未成年人、家长和老师等更好区分网络游戏，引导未成年人更好使用网络游戏。需要特别

说明的是，适龄提示并不等同于西方的分级制度，决不允许色情、血腥、暴力、赌博等有害内容存在于面向成年人的游戏中。六是积极引导家长、学校等社会各界力量履行未成年人监护守护责任，帮助未成年人树立正确的网络游戏消费观念和行为习惯。没有监护人的有效监督约束和陪伴陪护，有关制度的落实必然会大打折扣。

问：如何抓好《通知》的贯彻落实？

答：一分部署，九分落实。《通知》印发后，关键要认真贯彻和严格执行，把各项规定落实到位，让防沉迷的要求落地见效。一是做好宣传解读。国家新闻出版署将通过组织研讨、培训等形式，向各地新闻出版管理部门和相关企业做好阐释解读，组织各地各单位认真学习《通知》，准确把握相关内容和要求。二是强化督查落实。各地各单位要统一认识，严格落实《通知》要求，切实建立健全相关工作机制。《通知》明确规定各属地管理部门要认真履行属地监管职责，加强对贯彻执行情况的监督检查，并协调有关执法机构做好监管执法工作。对《通知》落实过程中出现的问题，各属地管理部门要及时发现和纠正，对落实情况要及时报告。三是完善配套制度。防止未成年人沉迷网络游戏的工作是一项复杂的系统性工程，需要各方面共同努力、积极推进，不断研究完善相关做法。目前，相关方面正抓紧推动《未成年人保护法》、《未成年人网络保护条例》的立法与修订工作，将防止未成年人沉迷网络游戏的要求写入法律法规，为各项具体工作提供更加有力的支撑。同时，国家新闻出版署正与公安部对接，牵头建设统一的身份识别系统，为游戏企业提供游戏用户身份识别服务，以准确验证未成年人身份信息。我们还将逐步完善和丰富身份识别系统的功能，实现跨平台使用网络游戏时间的数据互通，以掌握每一个未成年人跨平台使用游戏的总时间并予以约束。随着网络游戏载体形式和服务方式的不断发展变化，我们将继续探索创新制度设计，不断总结好经验好做法，让防沉迷工作取得更大成效，为广大青少年健康成长保驾护航。（来源：新华社）

➢ 工业和信息化部开展 APP 侵犯用户权益专项整治行动

2019 年 10 月 31 日，工业和信息化部发布《关于开展 APP 侵害用户权益专项整治工作的通知》工信部信管函〔2019〕337 号。

1、整治工作的背景

当前，APP 违规收集个人信息、过度索权、频繁骚扰、侵害用户权益的问题突出，群众反映强烈。工业和信息化部高度重视 APP 用户权益保护工作，始终贯彻以人民为中心的发

展思想，坚决把群众利益放在首位，不断完善 APP 治理体系，提升 APP 治理能力。此次组织开展的 APP 侵害用户权益专项整治行动，是对前期四部委开展 APP 违法违规收集使用个人信息专项治理行动成果的巩固和深化，是紧扣部行业管理职责定位，在信息通信行业行风纠风工作体系下，重点解决群众关心问题的主动作为。

2、整治工作的主要做法

此次组织开展的 APP 侵害用户权益专项整治工作，坚持问题导向，聚焦人民群众反映强烈和社会高度关注的侵犯用户权益行为，重点对用户关心的八类问题进行监督检查和规范整治。一方面，推动 APP 服务提供者和 APP 分发服务提供者自查自纠，及时整改；另一方面，技管结合，综合运用技术检测和检查、社会监督、用户和专家评议等手段，充分发挥第三方机构、媒体和用户的共同监督作用，构建政府管理、社会协同、公众参与、媒体监督、行业自律、科技支撑的全方位综合监管体系。

3、整治工作的法律依据

专项整治工作依据《网络安全法》《电信条例》和《规范互联网信息服务市场秩序若干规定》《电信和互联网用户个人信息保护规定》《移动智能终端应用软件预置和分发管理暂行

规定》等法律法规和规范性文件要求开展。

4、整治工作的主体对象

本次专项整治工作，主要面向两类主体对象，一是 APP 服务提供者。二是 APP 分发服务提供者，包含具备分发功能的应用商店、网站、应用软件和基础电信企业营业厅等各类企业。

5、整治工作的重点内容

本次专项整治工作重点检查是否存在人民群众反映强烈和社会高度关注的四个方面 8 类重点问题。

违规收集用户个人信息方面，重点针对私自收集个人信息、超范围收集个人信息等问题进行监督检查和规范整治。

违规使用用户个人信息方面，重点针对私自共享给第三方、强制用户使用定向推送功能等问题进行监督检查和规范整治。

不合理索取用户权限方面，重点针对不给权限不让用、频繁申请权限、过度索取权限等问题进行监督检查和规范整治。

为用户账号注销设置障碍方面，重点针对账号注销难进行监督检查和规范整治。

APP 分发服务提供者应落实《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等有关要求，组织对其所分发的 APP 进行全面检查，对存在问题的违规应用软件予以督促整改，拒不改正的应组织予以下架处理。

6、都有哪些处置措施

针对存在问题的 APP，将依法依规予以处理，具体措施包括责令整改、向社会公告、组织 APP 下架、停止 APP 接入服务，以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等手段，对于问题突出、严重违法违规、拒不整改的 APP 主体，将从严处置。后续工业和信息化部还将以此次专项行动为契机，推动出台相关规定，为规范行业管理和建立长效机制奠定基础。（来源：工业和信息化部信息通信管理局 ）

- **《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知》全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c7506353/content.html
- **《关于开展 APP 侵害用户权益专项整治工作的解读》**
- http://www.miit.gov.cn/n1146295/n7281315/c7507241/content.html

➢ 国资委印发《关于加强中央企业内部控制体系建设与监督工作的实施意见》

2019 年 10 月 23 日，国资委印发《关于加强中央企业内部控制体系建设与监督工作的实施意见》的通知。**通知指出，**为深入贯彻习近平新时代中国特色社会主义思想和党的十九大精神，认真落实党中央、国务院关于防范化解重大风险和推动高质量发展的决策部署，充分发挥内部控制（以下简称内控）体系对中央企业强基固本作用，进一步提升中央企业防范化解重大风险能力，加快培育具有全球竞争力的世界一流企业，根据《中共中央、国务院关于深化国有企业改革的指导意见》（中发（2015）22 号）、《国务院关于印发改革国有资本授权经营体制方案的通知》（国发（2019）9 号）、《国务院办公厅关于加强和改进企业国有资产监督防止国有资产流失的意见》(国办发（2015）79 号）等规定，制定本实施意见。（来源：互联网）

➢ 上海市网信办发布上海市网络安全事件应急预案 （2019 年版）

2019 年 10 月 30 日，为贯彻落实中央和市委网信工作部署，进一步加强我市网络安全应急管理工作，上海市互联网信息办公室官方微信公号于 10 月 30 日向公众发布《上海市网络安全事件应急预案》(2019 年版)。

《上海市网络安全事件应急预案》(2019 年版)主要目得：建立健全本市网络安全事件应急工作机制，提高应对突发网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序，保障城市安全运行。

《上海市网络安全事件应急预案》(2019 年版) 编制依据：《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《突发事件应急预案管理办法》、《国家网络安全事件应急预案》、《上海市实施<中华人民共和国突发事件应对法>办法》、《上海市突发公共事件总体应急预案》和《信息安全技术 信息安全事件分类分级指南》(GB/Z 20986—2007)等,编制本预案。（来源：网信上海）

- **《上海市网络安全事件应急预案 （2019 年版）》全文：**
- https://mp.weixin.qq.com/s/HW-eMdWbBITh5z9k48Pu3w

五、本期重要漏洞实例

➢ 关于 Android-gif-Drawable 开源库存在远程代码执行漏洞的安全公告

发布日期：2019-10-28
更新日期：2019-10-28
受影响系统：
使用 Android-gif-Drawable 库进行 GIF 图像处理，且 Android-gif-Drawable 库版本在 1.2.18 以下的安卓 APP 受此漏洞影响。iOS 应用不受此漏洞影响。
腾讯安全玄武实验室阿图因系统分析结果显示，该 GIF 开源库被大量安卓 APP 使用，全球范围内 43619 个使用该 GIF 开源库开发的安卓 APP 可能受此漏洞影响。
描述：

ID: CNTA-2019-0036
2019 年 10 月 14 日，国家信息安全漏洞共享平台（CNVD）收录了由腾讯安全玄武实验室报送的 Android-gif-Drawable 开源库远程代码执行漏洞（CNVD-2019-35254）。攻击者利用该漏洞，可在未授权的情况下，在用户终端上远程执行代码或导致应用拒绝服务。目前厂商已发布补丁完成修复，漏洞相关细节已公开，漏洞影响范围和危害较大。
Android-gif-Drawable 是用于 Android 系统进行 GIF 图像解析的开源库（以下简称 GIF 开源库）。GIF 开源库通过 JNI 捆绑 Giflib 的方式对帧数进行渲染，与 WebView 类和 Movie 类相比渲染效率较高，因此得到了广泛应用。
2019 年 5 月，安全研究人员发现 Android 版本的 WhatsApp（2.19.244 版本之前）存在内存重复释放漏洞（CVE-2019-11932，对应 CNVD-C-2019-144833），攻击者通过向 WhatsApp 用户发送一个精心制作的恶意 GIF 文件，就可以获得 WhatsApp 的应用权限，在手机端进行 SD 卡读取、音频录制、摄像头访问、文件系统访问、WhatsApp 沙盒存储访问等操作。
腾讯安全玄武实验室研究发现，上述漏洞是由 GIF 开源库导致的。凡使用该 GIF 开源库进行 GIF 图像解析的安卓应用（APP）都可能受此漏洞影响。攻击者通过向受影响的 APP 用户远程发送恶意 GIF 文件，可在目标设备的 APP 应用权限环境下执行任意代码（安卓 8.0 版本及以上）或导致应用拒绝服务（安卓 8.0 版本以下）。
CNVD 对该漏洞的综合评级为“高危”。
建议：

厂商补丁：
GIF 开源库已发布新版本（1.2.18）修复此漏洞，CNVD 建议：

1、开发人员对使用的 GIF 开源库版本进行全面排查，发现问题后及时安装 Android-gif-Drawable 开源库更新应用补丁（https://github.com/koral--/android-gif-drawable/pull/673/commits/4944c92761e0a14f04868cbcf4f4e86fd4b7a4a9），或整体替换至最新版本（https://github.com/koral--/android-gif-drawable/releases/tag/v1.2.18 ），并向用户及时推送新版本的 APP。2、用户使用手机端 APP 时，不要浏览和存储来历不明的 GIF 文件。

➢ Microsoft Windows Hyper-V 远程代码执行漏洞

发布日期：2019-11-01
更新日期：2019-11-01
受影响系统：
Microsoft Windows 10
Microsoft Windows 10 1607
Microsoft Windows Server 2016
Microsoft Windows 10 1703
Microsoft Windows 10 1709
描述：

CVE(CAN) ID: CVE-2019-0709
Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Windows Hyper-V 是其中的一个虚拟化产品，支持在 Windows 中创建虚拟机。
Microsoft Windows Hyper-V 存在远程代码执行漏洞，攻击者可利用该漏洞执行任意代码。

<*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://www.cnvd.org.cn/patchInfo/show/188309

➢ Linux kernel 内存破坏漏洞

发布日期：2019-10-29
更新日期：2019-10-29
受影响系统：
Linux kernel <5.3.4
描述：

CVE(CAN) ID: CVE-2019-18198
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 5.3.4 之前版本中的 net/ipv6/fib6_rules.c 文件的‘fib6_rule_suppress()’函数存在内存破坏漏洞，本地攻击者可利用该漏洞造成内存损坏。

<*来源：Linux
*>

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://www.cnvd.org.cn/patchInfo/show/187537

➢ Cisco TelePresence Collaboration EndpointSoftware 任意文件写漏洞

发布日期：2019-10-28
更新日期：2019-10-28
受影响系统：
Cisco Cisco TelePresence Collaboration Endpoint (CE) Software < 9.8.1
描述：

CVE(CAN) ID: CVE-2019-15962

Cisco TelePresence 是思科网真解决方案。
Cisco TelePresence Collaboration Endpoint (CE) 9.8.1 之前版本存在安全漏洞，该漏洞是由于权限分配不当所致。攻击者可利于该漏洞通过登录为 remotesupport 可导致对/root 目录下的文件写操作。

<*来源：Cisco
*>

建议：

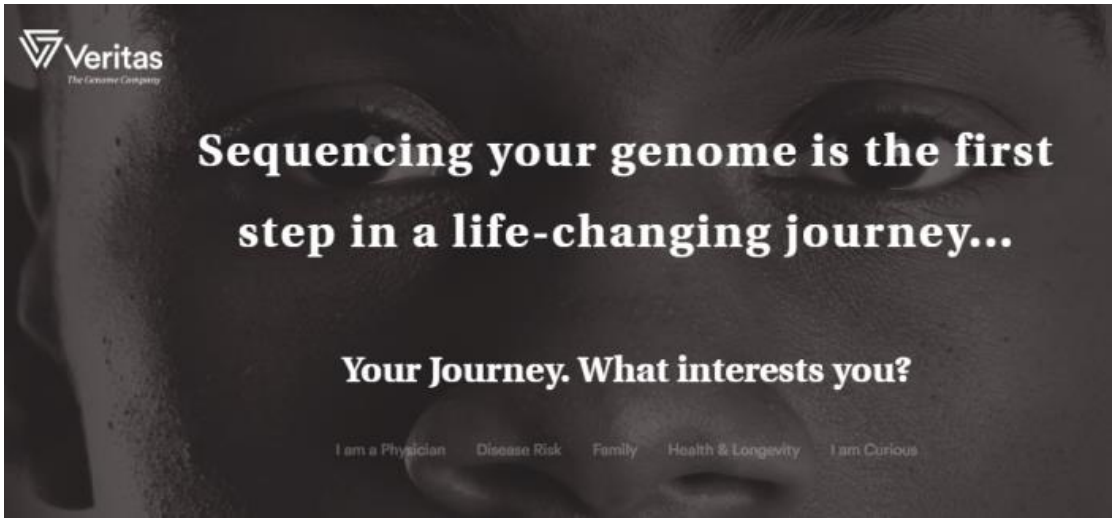
厂商补丁：
Cisco

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.cnvd.org.cn/patchInfo/show/187205

六、本期网络安全事件

➢ 美国基因检测公司 Veritas Genetics 客户数据遭泄露

2019 年 11 月 8 日，据国外媒体报道，美国 DNA 检测初创公司 Veritas Genetics 表示，该公司发生一起数据泄露事件，导致一些客户的信息被盗。这家总部位于美国马萨诸塞州丹弗市的公司承认，其面向客户的门户网站“最近”遭到了黑客攻击，但没有说明何时遭到攻击。该公司拒绝透露具体哪些信息被盗，只表示该门户网站不包含客户的检测结果或医疗信息，以及仅有少数客户受到了影响。



该公司尚未发表正式的公开声明，也没有在其网站上承认此事。Veritas Genetics 的一位发言人没有回复记者的置评请求。美国彭博社首先报道了这一消息。

Veritas Genetics 的竞争对手包括 23andMe、Ancestry 和 MyHeritage。该公司表示，它可以利用个人的一小部分 DNA 来分析和理解人类基因组，从而让客户更好地了解他们今后生活中可能面临的健康风险，或将该风险遗传给子女的风险。

尽管此次被盗的数据不包括个人健康信息，但这可能会进一步加剧人们的担忧，即健康初创公司，尤其是处理敏感 DNA 和基因组信息的公司，可能无法保护好用户的数据。

在此之前，美国执法部门曾获得法律授权，要求 DNA 采集和基因检测公司帮助识别犯罪嫌疑人，从而使隐私成为基因检测领域的一个备受人们关注的问题。就在本周，有报道称，美国佛罗里达州颁发了一份具有“游戏规则改变者”性质的授权令，允许警方搜索本地 DNA 检测公司 GEDmatch 的全部数据库。去年，警方曾利用该公司的数据库帮助抓捕臭名昭著的“金州杀手”(Golden State Killer)。在美国，约有 2600 万消费者使用了家用遗传检测试剂盒。

（来源：网易科技）

➢ 台“金管会”：6 券商遭黑客攻击 无投资人受影响

2019 年 11 月 6 日，据台湾“中央社”报道，台股创 29 年新高，但 5 日却传出有 6 家券商通报遭黑客攻击，导致资安异常情况。台湾“金管会证期局”表示，受攻击的券商在启动流量清洗机制后，已立即解决问题恢复正常，没有任何投资人受影响。

台股 5 日上演开高走高戏码，终场上涨 87.18 点，收在 11644.03 点。不过，市场也传出，从 4 日开始，就有 10 多家券商遭到资安攻击。台湾“金融监督管理委员会证券期货局副局长”蔡丽玲证实，5 日共有 6 家证券商通报资安发生异常情况，但发生异常时间非常短，且启动流量清洗机制后，交易马上恢复正常，没有任何投资人受到影响。

依照规定，发生重大异常或资通安全事件，依照规定要在 30 分钟时限之内进行通报。蔡丽玲强调，这次的事件仅是流量受到影响，猜测应是随机攻击，不是只锁定小型券商；“金管会”会研议如何提升业者资安防护能力，并督导业者遵守资通安全相关规范。

她进一步表示，有请券商要留意黑客攻击事件，一旦发现受到攻击，要引导电子下单的投资人采用替代方案来下单，后续继续追踪，确保投资人权益。

“金管会”针对证券期货业者的信息安全规范共有 8 大防范措施，包括要求业者要按照资产规模大小要去配置资安专责单位及专责主管、要求业者使用电子凭证，以确保网络下单交易安全、要求业者建立资安通报机制及通报系统，以利掌握资安事件等。

另外，针对分布式阻断服务攻击(DDoS)攻击的因应，券商应提供网络下单交易服务业者，已导入流量清洗机制，并每年由证券期货单位办理 DDoS 攻击演练等。（来源：中新网）

➢ 脸书产品新漏洞至少 20 国官员手机被黑客控制

2019 年 11 月 1 日，援引 WhatsApp 内部调查的消息人士称，今年早些时候，脸书公司旗下社交软件 WhatsApp 存在安全漏洞，黑客曾借此“控制（take over）”使用该软件用户的手机。而本次事件中有一大部分的受害人，是分布在五大洲至少 20 国的高级政府官员及军方官员。很多受影响国家都是美国的盟国。


CYBER RISK NOVEMBER 1, 2019 / 12:04 AM / UPDATED 13 HOURS AGO

Exclusive: Government officials around the globe targeted for hacking through WhatsApp - sources

Christopher Bing, Raphael Satter

4 MIN READ

目前，黑客的身份还未确认，但观察者网注意到，10 月 29 日 WhatsApp 曾向美国当地法院控诉一家以色列企业，声称后者研发的程序，让黑客入侵 WhatsApp 的用户手机。

美国旧金山法院一份文件显示，WhatsApp 此次起诉的是一家名为 NSO 的以色列网络监控企业。诉讼文件显示，NSO 将恶意程序发送至目标用户的移动装置，该程序可秘密协助监视目标手机用户，并窃取资料。在 2019 年 4 月 29 日至 5 月 10 日之间，至少 1400 名 WhatsApp 用户手机遭到攻击，其中至包括 100 名外交官、记者、人权组织人士、高级官员等人士。

熟悉 WhatsApp 内部调查的消息人士表示，已知受害者中有“相当一部分”是分布在五大洲至少 20 个国家的政府高官和军方人士，如阿联酋、巴林、墨西哥、巴基斯坦和印度等。被黑手机用户很多是美国盟国的官员。

NSO 对此发表声明，否认该公司进行过任何不当行为，称其产品只是为了帮助政府抓获恐怖分子和罪犯。NSO 同时表示无法透露其客户的身份，也无法对其技术的具体用途进行说明。

在《金融时报》等媒体眼中，NSO 这家公司“劣迹斑斑”。该媒体曾曝料，这家公司曾研发一款名为“飞马座（Pegasus）”的程序，“可以攻克苹果手机的隐私保护功能”。苹果手机用户在设备上安装恶意软件后，Pegasus 功能可以从包括谷歌云服务软件 Google Drive、脸书通讯软件 Messenger 和苹果云服务软件 iCloud 在内的服务中复制身份验证密钥。

《金融时报》还暗示 NSO 和以色列政府有关联。报道称，“飞马座”是由以色列政府出售，仅提供给其他国家政府部门以协助进行犯罪调查。不过当时 NSO 和以色列政府均否认参与任何“黑客行动”。

如今对于 WhatsApp 方面的指控，以色列安全内阁部长埃尔金（Ze‘ev Elkin）于 11 月 1 日接受特拉维夫当地电台 102.FM 采访时撇清关系，称 NSO 是家私企，“以色列政府并没有参与本次事件，众所周知，这件事和以色列政府无关”。

脸书于 2014 年斥资 193 亿美元收购 WhatsApp。截至 2018 年 2 月，WhatsApp 用户已达 15 亿人，是全球范围内最流行的社交软件之一。“黑客事件”曝光后，脸书昨晚美股盘后略有下跌，跌幅 0.04%。

2018 年 3 月，脸书爆发“剑桥分析丑闻”，涉嫌泄露 8700 万用户数据。就此事，今年 7 月脸书与美国联邦贸易委员会（FTC）达成和解协议，需支付高达 50 亿美元，创下最高罚款记录。10 月 30 日，脸书又和英国政府达成和解，同意支付 50 万英镑罚单。“剑桥分析丑闻”发布后，脸书在全球范围内推进数据相关业务时不顺。今年脸书欲退出加密货币“Libra”项目，但欧盟因数据隐私保护上担忧，反对“Libra”在欧洲推进。除此以外，美国司法部 7 月宣布启动针对美国科技巨头的反垄断调查，其中就涉及脸书。（来源：观察者网）

➢ 疯狂攻击网站，这些黑客被“团灭”！

2019 年 11 月 5 日，日常生活中，人们上网有时会遇到“连接网站失败”“服务器无法访问”“网站自动跳转至其他页面”等类似问题。这不一定是网络连接的故障，很可能是登录的网站正在被黑客恶意攻击。近日，江苏睢宁警方破获了一起有组织的、谋取非法利益的网络黑客案。

服务器异常牵出“DDoS 攻击”团伙

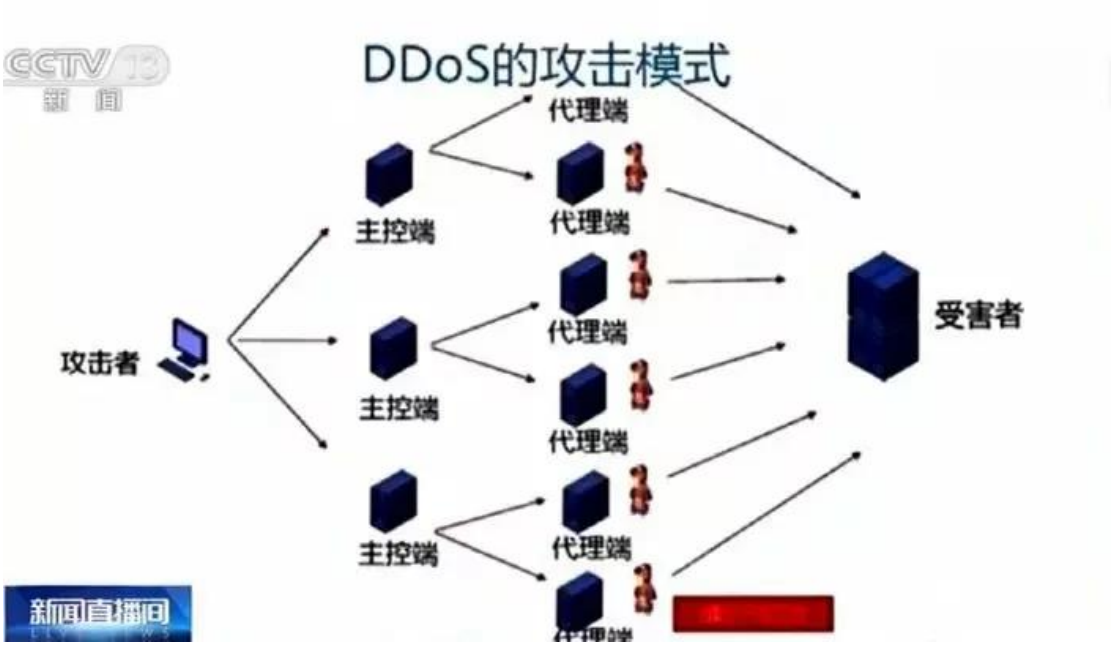
2018 年 5 月，江苏睢宁警方发现，徐州电信机房的一台网络服务器异常，疑似被人上传了“木马”控制程序。

警方围绕租用服务器的黄某展开侦查，发现其利用控制的计算机进行网络攻击，并牵出一个网络黑客犯罪团伙。

犯罪嫌疑人实施的犯罪行为叫做“DDoS 攻击”。这种攻击利用网络漏洞控制别人的计算机，并用这些被控制的计算机同时集中访问某个网站，或发送一些攻击性指令，致使目标网站瘫痪或无法使用。民警表示，这些犯罪嫌疑人按小时收费。一般而言，使目标网站瘫痪一小时，收几百元钱。网站的防御能力越强，收费越高。

经过 9 个多月的调查取证，警方梳理出一个黑客犯罪的链条。今年 1 月和 3 月，专案组奔赴广东、河南、云南等 16 个省份、20 个地级市，成功打掉这个“DDoS 攻击”团伙和获取、买卖网站服务器控制权限的犯罪团伙。抓捕行动共抓获 41 人，侦破“DDoS 攻击”案件 100 余起，查获各类网站非法控制权限 20 余万个，关闭涉案服务器 30 余台，涉案金额 1000

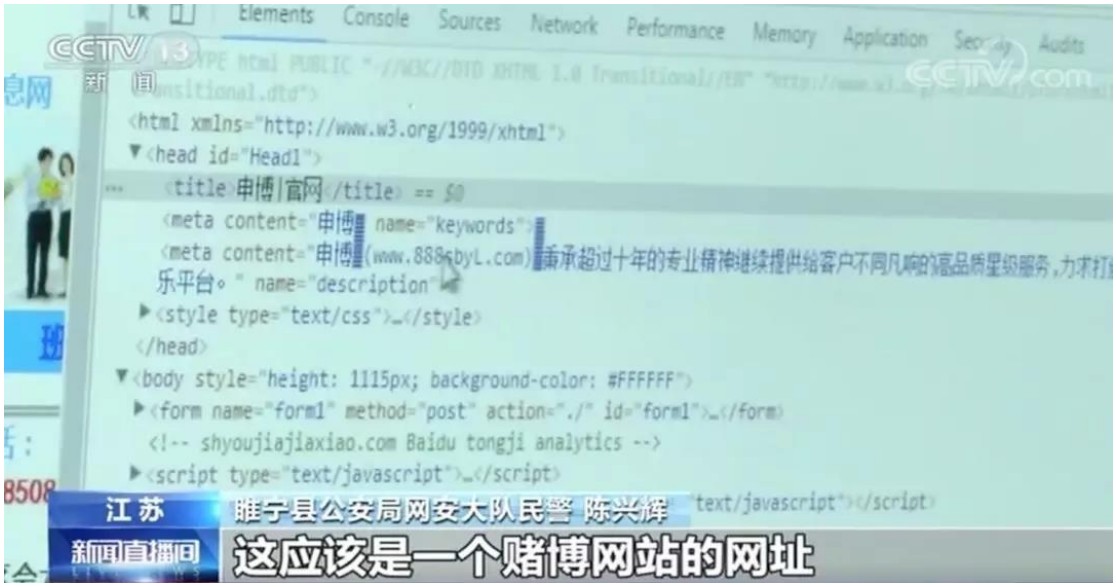
多万元。



驾校网站秒变赌博网站　黑客入侵无孔不入

民警介绍，这个黑客犯罪团伙利用黑客技术，入侵国内的政府、企业网站，获取网站控制权限。之后通过网络销售大量网站控制权，用于植入各类赌博、色情、诈骗链接。

睢宁县公安局网安大队民警陈兴辉：我们在犯罪嫌疑人的电脑里提取了一些文档。一个看上去正常的驾校网站，其标题被修改后，直接跳转到一个赌博网站。



警方提醒：各相关企业、部门一定要加强网站的安全措施，做好网站安全管理工作，一旦发现系统被入侵，应及时报案。根据刑法规定，对计算机信息系统实施非法控制，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，处以三年以上七年以下有期徒刑，并处罚金。（来源：央视新闻）

➢ 多家网站未履行网络安全保护义务遭黑客攻击，贵阳网警：罚

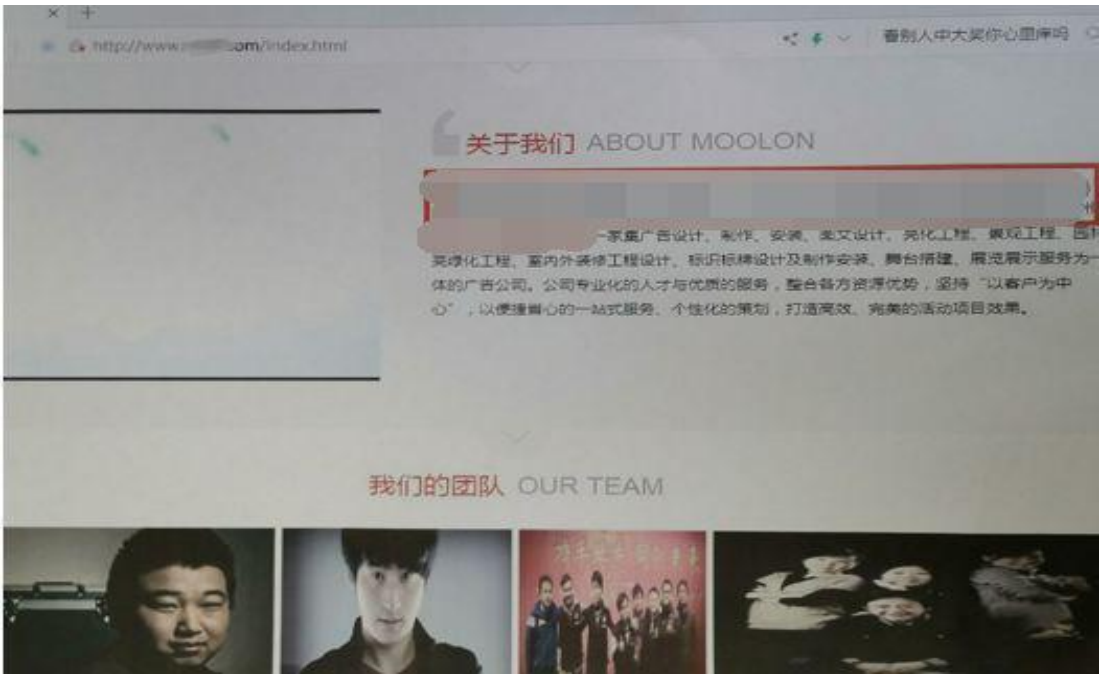
2019 年 10 月 31 日，近日，贵阳网警联合辖区公安分局，查处多家因未履行网络安全保护义务致使网站遭黑客攻击篡改、悬挂违法有害信息的单位。

高校网站遭黑客攻击

贵阳一高校网站主页遭遇黑客攻击，登录页面被非法篡改为违法有害信息，影响恶劣。贵阳网警获悉后，立即展开调查。经查，该高校网站平台未留存 web 访问日志，服务器系统日志、安全日志留存时间不满 6 个月留存时限，未开展网络安全检测，平台内共发现 10 余个木马后门，技术防护措施极为薄弱。2019 年 10 月 19 日，观山湖警方根据《中华人民共和国网络安全法》第 21 条、第 59 条之规定，依法对该高校及高校负责人分别处以 10 万元和 5 万元的行政罚款。

公司简介变赌博信息

贵阳一广告公司门户网站主页被不法分子悬挂赌博信息。经查，该公司未落实网络安全等级保护制度，未落实网络安全技术措施，导致网站被入侵篡改，造成不良社会影响。2019 年 9 月 23 日，南明警方根据《网络安全法》第 21 条、第 59 条之规定，依法对该公司及公司法人分别处以 1 万元和 5 千元的行政罚款。



网站发布涉政违法信息

贵阳某网站存在涉政违法信息。经查，该网站未落实实名制管理要求，未落实网络安全技术防护措施，未发现并删除违法信息。2019 年 10 月 16 日，云岩警方根据《网络安全法》第 21 条，第 59 条规定，对该网站予以行政警告并责令限期整改的处罚。

普法小贴士：《中华人民共和国网络安全法》第二十一条：

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露

或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

《中华人民共和国网络安全法》第五十九条第一款：

网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。（来源：贵阳网警巡查执法）

➢ 趋势科技员工将 68000 名客户信息出售给犯罪分子

2019 年 11 月 7 日，趋势科技近期宣布，一名员工窃取了 68000 名客户的敏感信息，并将其卖给第三方用于钓鱼诈骗。

在 2019 年 8 月，趋势科技了解到，旗下一些客户在使用家庭安全解决方案时，收到了冒充 TrendMicro 技术支持的诈骗分子的钓鱼电话。这些骗子在电话中的透露的信息，让趋势科技相信这不是一个普通的钓鱼电话，很可能有公司内部有勾结。“这些罪犯在这些诈骗电话中掌握的信息让我们有理由怀疑这是一起内外协同攻击。”

经过调查，趋势科技在 10 月份确定这些钓鱼电话和内部的一名员工非法访问客户支持数据库有关。他把大量客户信息转移出来，出售给犯罪分子。

趋势科技在博客中表示：“尽管我们立即展开了调查，但直到 2019 年 10 月底，我们才确定了内部威胁源。趋势科技的一名员工使用欺诈手段获取了客户支持数据库的访问权限，再把其中的姓名、电子邮件地址、趋势科技内部标号、电话号码非法出售给犯罪分子。不过该数据库并没有如财务或信用支付等金钱交易信息，也不含企业或政府客户的任何敏感数据。”

在找出内鬼后，趋势科技立刻终止了雇佣关系，并通报了执法部门。根据他们的调查，这一安全事件影响了趋势科技不到 1%的客户，且只针对说英语的用户。虽然没有财务信息被盗，但因此产生的针对性很强的钓鱼攻击可能会导致不少客户的财产遭受损失。

趋势科技也表示：他们永远不会给任何客户打电话，如果客户接到自称是趋势科技的人打来的电话，应该立即挂断。虽然这起安全事件的根源并不是在于外部黑客攻击，但这已经不是今年第一次有未经授权的用户访问趋势科技的系统了。在 2019 年 5 月，一名黑客据称获得了趋势科技测试实验室的访问权限，接触到超过 30TB 的源代码文件。（来源：趋势科技）