中国改革报 CHINA REFORM DAILY
2021.11.26 星期五
本版编辑：孟佳惠 Email：crd_xyzhg@163.com 热线：(010)56805187

印度黑客频繁“过界” 网络安全治理势在必行

□ 曹思琦 郭媛丹

“南亚地区的邪恶之花”“游荡在喜马拉雅山脉的幽灵战象”“来自美色的诱惑”……对大多数人来说，这些神秘的代码名称一般出现在烧脑刺激的黑客电影里。然而，《环球时报》记者近日从多家中国网络安全企业获悉，这些代码的背后揭示了一张精密、复杂的真实网络：来自南亚大陆——以印度为主要代表的顶尖黑客组织，他们在国家和情报机构的强大支持下，在过去几年里不断攻击中国、尼泊尔和巴基斯坦的国防、军事单位以及国有企业。

近些年，印度军政高层和媒体不断炒作“中国网攻威胁”，每次都遭到中方驳斥。事实证明，中国才是黑客攻击的主要受害国之一。安天科技集团、360政企安全集团和奇安信三大中国网络安全企业相关人士给记者提供了大量翔实的一手资料，从中可以发现印度对我国重要部门频密发动网络攻击的重要信息。相关专家也提醒，针对境外网络攻击，中国要提升自身免疫力，不管是来自印度还是美国的攻击都需要专业的团队分析对手，并采取相应的反制方式。

不仅利用“钓鱼”邮件，还擅长社会工程学手段

作为引领威胁检测与防御能力发展的网络安全国家队，安天科技集团一直在跟踪对我国发起的“钓鱼”攻击。安天科技副总工程师李柏松表示，今年3月以来，安天已捕获多起针对我国和南亚次大陆国家的“钓鱼”攻击活动。这些活动涉及网络节点数目众多，主要攻击目标为中国、巴基斯坦、尼泊尔等国家的政府、国防军事以及国企单位。安天科技发现，这一批次“钓鱼”攻击的最早时间可追溯至2019年4月份，攻击组织来自印度。

记者也从360政企安全集团获悉，2020年，360监控并捕获到的初始攻击载荷共有上百个。来自以印度为主要代表的南亚地区的网络攻击有活跃趋势，从2020年下半年开始一直持续至目前，并呈大幅上升趋势。尤其在2021年上半年的攻击活动中，针对时事热点的跟进频次和细分粒度已明显超过去年同期，主要针对我国和其他南亚地区国家，围绕地缘政治相关的目标，涉及教育、政府、航空航天和国防军工等多个领域。

从技术方面讲，以印度为代表的南亚地区网络攻击组织具有明显的特征，其主要利用“钓鱼”邮件，且擅长使用社会工程学手段——通过利用受害者的本能反应、好奇心、信任等心理进行欺骗或攻击。据介绍，这些顶级黑客组织攻击者将自身伪装成目标国家的政府或军队人员，向对方邮箱投递挂有“钓鱼”附件或嵌有“钓鱼”链接的攻击邮件，并诱导目标通过链接访问攻击者通过各种方式搭建的“钓鱼”网站，收集受害者输入的账号密码以供情报搜集或横向攻击所用。

360安全专家表示，来自印度等南亚国家的网络攻击涉及题材丰富多样，紧跟时事热点，且目标针对性极强，可以推断其背后有专门针对目标国家相关领域时事新闻的情报分析，同时以此来指导其进行网络攻击活动。

据了解，2021年境外针对中国的网络攻击目标不仅涉及教育、政府、航空航天和国防军工多个领域，更是通过紧密围绕政治、经济等热点领域及事件，瞄准涉及相关时事热点的重点机构或个人。

“国家级APT”瞄准政府机构、军工企业、核能行业等

此类黑客团伙被称为“国家级APT”（Advanced Persistent Threat，高级持续性威胁）组织。在国家背景的支持下，他们专注于针对特定目标进行长期和持续性的网络攻击，且一直处于十分活跃的状态。

印度是一个可能被世界情报界忽视的有威胁的国家，甚至南亚的一些国家可能也没有完全意识到它先进的网络能力。正如一些网络安全观察人士经常提到的，“下一场世界大战将不是在地面、空中或水下进行，而是在虚拟的网络空间进行”。多年来，中国一直是网络攻击的受害国，中国网安企业捕捉到的来自印度的加强攻击也再次表明中国网络安全形势的严峻性和加快构建网络安全保障体系的紧迫性。例如：2020年新冠肺炎疫情暴发初期，一个名为“APT-C-48（CNC）”的组织通过伪造体检表格文档对我国医疗相关行业发起攻击；2021年4月，360捕获到CNC组织针对我国重点单位发起的新一轮攻击；2021年6月中旬，CNC组织在我国航天时事热点前后，针对我国航空航天领域相关的重点单位突然发起集中攻击。

记者从中国知名网络安全公司奇安信旗下的高级威胁研究团队红雨滴获悉，目前已知这些主要瞄准政府机构、军工企业、核能行业等领域的国家级顶级黑客团伙集中在“蔓灵花”（BITTER）、“摩诃草”（Patchwork）、“魔罗桫”（Confucius）和“肚脑虫”（Donot）四大组织中。

首先说说“蔓灵花”，这是一个据称有南亚背景的APT组织。该组织至少从2013年11月以来就开始活跃，但一直未被发现，直到2016年才被国外安全厂商Forcepoint首次披露。同年，奇安信威胁情报中心发现国内也遭受相关攻击，并将其命名为“蔓灵花”。该组织具有强烈的政治背景，主要针对巴基斯坦、中国两国，2018年也发现过其针对沙特阿拉伯的活动，攻击瞄准政府部门、电力、军工等相关单位，意图窃取敏感资料。据了解，2019年该组织还加强了针对我国进出口行业的攻击。

其次是“魔罗桫”，该组织的攻击活动最早可以追溯到2013年，被首次公开披露的时间则是2016年。相关专家认为，“魔罗桫”组织疑似来自印度地区，长期以中国、巴基斯坦、尼泊尔等国家及周边地区为主要攻击区域，并瞄准政府机构、军工企业、核能行业、商贸会议、通信运营等领域发起攻击。

再次是“摩诃草”，该组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，主要攻击领域为政府、军事、科研、教育等。2020年2月，“摩诃草”便发起以“新冠疫情”为主题针对国内的攻击活动。该组织利用“武汉旅行信息收集申请表.xlsm”“卫生部指令.docx”等诱饵对我国进行攻击活动。2021年8月，“摩诃草”借助美女图片为诱饵发起“来自美色的诱惑”的恶意程序攻击。

最后是“肚脑虫”，该组织由360和奇安信威胁情报中心联合发现，并在全球率先披露。2017年“肚脑虫”攻击活动首次被曝光，但它的攻击活动可追溯到2016年。“肚脑虫”组织一直处于活跃状态，主要针对巴基斯坦、克什米尔地区、斯里兰卡、泰国等南亚、东南亚国家和地区发起攻击，对政府、军队以及商务领域重要人士进行网络间谍活动。

没有网络安全就没有国家安全

随着中国互联网行业的快速发展，网络安全风险迅速增加。多年来，中国、俄罗斯等国一直是网络攻击的主要受害者。网络已成为美国及其“盟友”在信息战中压制其他国家的新武器。中国国家互联网应急中心数据显示，2020年位于境外的约5.2万个计算机恶意程序控制服务器，控制了中国境内约531万台主机，就控制中国境内主机数量来看，控制规模排名前三位的控制服务器均来自北约成员国。

此外，相关报道显示，美国中央情报局的网络攻击组织APT-C-39，曾对中国航空航天科研机构、石油行业、大型互联网公司以及政府机构等关键领域进行了长达11年的网络渗透攻击。

“这告诉中国人一个很简单的道理：在网络攻击中，有一种东西叫作国家级的网络攻击。”复旦大学网络空间国际治理研究基地主任沈逸说，“我们在网络空间开展活动，所发布、拥有的信息又是具有国家安全意义和影响的，天然就会成为国家情报机构进行网络搜集的目标。”他认为，网络安全是国家安全的重要组成部分，要从国家安全领域理解网络安全，树立安全意识。

沈逸表示：“我们一开始认为我们是一个落后国家，或者说发展中国家，在网上好像我们的信息不值钱，没什么值得你偷的。但我们现在已经是经济体量全球排第二的国家，有些周边国家把你视为对手，会发动国家级的网络攻击。印度对我们的攻击是长期持续存在的，是网络空间、国际局势和体系复杂性的具体表现。”在沈逸看来，尽管中国一直试图搞好和印度的关系，但印度一直受西方式的地缘政治思想和理念影响，在网络安全上和美方开展了大量合作。

为应对来自网络空间的挑战，中国政府推出一系列法律措施，以建立一个网络安全治理系统。自2017年以来，中国几乎从零开始建立起一套完善的网络安全法律保障机制。沈逸还建议，中国应从提升网络安全防御能力和威慑能力两方面来进行网络安全建设。中国的网络空间要有在开放环境、数据跨境流动、基本零信任条件下的有效防御能力。同时，要建立信息的通报机制，如美国经常写报告，把矛头指向中国，以此制约中国的网络空间国际治理，而中国也要采取相应的反制方式。

中国网络空间战略研究所所长秦安表示，现在网络空间军事化的大趋势已形成，一些国家开始加强对外网络攻击。秦安认为，对中国来说，要提升自己的免疫力，“洪水、污水都是水，不管是来自印度还是美国的攻击都需要专业的团队分析对手，专门应对”。

美国10月零售销售额环比增加1.7%

美国商务部近日公布数据显示，美国10月零售销售额环比增加1.7%，是自今年3月以来最高增幅，也高于市场普遍预期。图为民众在首都华盛顿周边家得宝（HomeDepot）购物。 沙晗汀 摄

海外传真

印度要立法禁止私人加密货币

本报讯 印度政府11月23日表示，印度正寻求在议会冬季会议上推出加密货币监管法案，禁止除个别情况外的所有私人加密货币。

据《印度斯坦时报》报道，印度政府将在冬季议会会议上引入“2021年加密货币和官方数字货币监管法案”。该法案旨在为印度央行发行官方数字货币建立促进性框架，并禁止几乎所有私人加密货币。

这份加密货币法案是印度政府即将在冬季议会上提出的26项新法案之一。《今日印度》报道称，印度储备银行有意推出自己的加密货币，但尚未宣布。该报从印度政府获得的初步文件显示，法案对于私人加密货币的禁止将有“少数例外”，以促进加密货币技术及应用。

近来，不仅印度在加密货币方面有所动作，萨尔瓦多作为世界上第一个采用比特币作为法定货币的国家，11月22日被国际货币基金组织（IMF）“婉言相劝”。IMF表示，考虑比特币价格的高波动性，将其作为法定货币会对消费者保护、金融诚信与金融稳定带来重大风险，萨尔瓦多不应将这种加密货币列为法定货币，建议缩小比特币的法律适用范围，并加强对这种新支付生态系统的管理与监督。 （郝爽言）

谷歌同意向法新社新闻内容付费

本报讯 据德新社消息，美国谷歌公司近日宣布，其与法新社签署了5年合作关系协议，其中包括将向法新社新闻内容付费。这也是法国新法律下科技巨头达成的最大授权协议之一。

上述合作关系协议还包括开发一个订阅平台、通过谷歌广告技术服务分享广告收入、发展音频新闻和通过谷歌旗下社交平台投资视频新闻等内容。新闻集团首席执行官罗伯特·汤姆森表示，协议确立了优质新闻应享有溢价的规则，将给全球新闻业带来积极影响。

法新社首席执行官法布里斯·弗莱斯表示，这笔交易是对“信息价值的认可”。谷歌法国分部负责人塞巴斯蒂安·米索夫表示：“与法新社达成的协议表明，我们愿意与法国的出版商和新闻机构就邻接权(与著作权相关的权利)问题达成共识。”

据法新社消息，这项为期五年的协议标志着新闻机构首次根据2019年欧洲版权指令就所谓的邻接权达成协议。欧盟的这项修正案旨在更新在数字时代过时的欧盟版权法，并确保作者从网上发布的内容中获得更多的报酬。

据德新社消息，谷歌公司最初拒绝为转载内容付费，但是2020年10月谷歌在巴黎上诉法院遭遇败诉。谷歌公司最近表示，已开始同法国、匈牙利、丹麦和荷兰等欧洲版权法所管辖国家的数百家新闻出版商进行谈判。今年1月，这家互联网巨头和法国出版商就共同的报酬标准达成一致，结束了一场旷日持久的版权纠纷，尽管这笔交易不包括来自杂志报业联盟的新闻机构和媒体。

（秦天弘）

欧洲议会通过《数字市场法》建议案

本报讯 欧洲议会内部市场和消费者保护委员会11月23日以42票赞成、2票反对、1票弃权的绝对多数通过了旨在限制国际互联网巨头不正当竞争行为的《数字市场法》建议案（以下简称“建议案”）。

建议案将市值超过800亿欧元、在欧洲年营业额超过80亿欧元的社交网络、搜索引擎、操作系统及电子商务运营商定性为“核心平台服务提供商”或“看门人”公司，其中显然包括了谷歌、脸书、亚马逊等国际互联网巨头。建议案规定，这类公司在欧盟范围内不允许利用数据优势向用户投放指向性广告，除非获得用户明确许可。同时，这类公司在欧盟范围内的同行业并购也将受到限制和监管，并购意向必须在事前获得欧盟委员会许可。如果这类公司有违反上述规定的行为，将被处以年营业额4%~20%的罚款。

欧盟委员会执行副主席维斯塔格高度赞扬这项建议案，他表示，这向着建立一个自由、公平和竞争性的科技市场迈出了一步，在这个市场中所有参与者都有机会成功。

欧洲议会全会计划在12月对《数字市场法》进行表决，如获通过将与欧盟各国政府展开进一步磋商，法案最终有望在明年上半年法国担任欧盟轮值主席国期间在欧洲落地实施。

（陶 冶）

国际观察

一场数据主权保卫战已然打响

□ 肖君拥

国家安全部日前就非传统领域危害我国重要数据安全问题公布了三起案例。从中可以看出，国外间谍组织在抢夺数据资源方面可谓无所不用其极，一场不见硝烟的数据主权保卫战已然打响。如何构建数据安全防控体系，在未来的数据主权保卫战中做到运筹帷幄，显得尤为重要。

一是要强化公民个人数据安全防范意识。实践中，一些公民依然没有认识到数据安全对于个人信息和国家安全的重要性，甚至为追求某些目的主动放弃了个人信息，导致个人数据安全受到威胁的同时，间接帮助外国间谍组织分析我国行业数据特征和国家重要数据。还有一些国外间谍组织擅于借助资本优势伪装目的，以利诱或哄骗的方式，诱使我国公民免费使用其提供的应用软件或科技产品，非法收集公民个人信息或窃取国家重要数据。因此，谨防个人信息泄露，保护国家重要数据安全，需要每个人的参与和支持。

二是要加强企业安全防范措施。从事数据相关业务的企业应提高对用户信息数据库的保护能力，履行保护用户个人信息安全的义务。首先，企业应当适用数据最小化原则，在确保用户正常使用的基础上，不得对用户个人数据进行额外采集，也不得利用优势地位强行收集用户个人信息，根据实际技术需求，明确采集用户数据的范围和保存时间、方式等，同时及时开展数据安全自查与评估，将不必要的数据按照销毁程序妥善处置。其次，企业应当加强数据安全保障能力。让隐私设计等数据安全的意识体现在产品的各个时期，从产品研发到上线运营再到升级更新，每个阶段都以数据安全为第一要务，制定符合企业长远发展的安全策略。针对数据采集、存储、传输、共享、销毁等环节，从安全技术创新、数据系统升级、人员结构配置、制度流程监控等方面侧重提升企业对用户数据的保护力度。最后，企业应当遵守数据安全相关法律法规。目前，我国数据安全法律体系已基本构建。与之配套的规章、制度等也已相继颁布，未来企业在运营过程中应结合行业领域特点和要求，严格按照法律法规进行数据操作与数据保护。

三是要完善国家数据安全治理体系。数据分类分级保护制度是数据安全治理的基础。建立健全交通、金融、卫生、科技等相关行业的重要数据判定标准，有助于实践厘清重要数据，提升可操作性。同时，加大网络安全审查力度也势在必行。以国家安全为立足点，适当扩大网络安全审查范围，尤其是信息基础设施运营者的审查还应包含一般数据审查。对于数据跨境流通更是要审慎审查，杜绝信息外泄。含有国家或公民信息的敏感数据、重要数据，出境前应申报安全评估，对国家核心数据应禁止跨境流通。

社址：北京市西城区月坛南街59号（邮政编码100045） 值班电话(010)56805051 广告发行部(010)56805116 广告经营许可证：京大工商广登字20180001号 零售价2.00元 印刷单位：经济日报印刷厂（地址：北京市西城区白纸坊东街2号）