警惕网络安全五大新风险

1月28日,深度求索(DeepSeek)官网显示,其线上服务受到大规模恶意攻击。1月30日凌晨,奇安信Xlab实验室监测发现,针对DeepSeek线上服务的攻击烈度升级,其攻击指令较1月28日暴增上百倍。Xlab实验室观察到,至少有2个僵尸网络参与攻击,共发起了两波次攻击。

近年来,随着一系列新技术的发展,网络安全也面临着新的挑战。网络攻击的规模和强度持续上升,网络攻击手段更加多样,造成的危害也愈加明显。其中,人工智能技术带来的影响最值得关注。

网络攻击危害性加剧

数字化转型加速,网络技术快速发展,恶意软件攻击也在不断升级。从简单的病毒木马事件到高级持续性威胁(APT),从黑灰产到勒索软件,网络攻击手段日益复杂化、专业化,互联网黑灰产业链日渐完善,经济利益更加明确,给网络安全构成较大威胁。

关键单位受攻击占比大。攻击方针对社会关键信息基础设施的攻击,已经组织化、产业化,所采用的攻击水平快速提升。业内人士介绍,近年来,我国电力、能源和科研机构等要害部位受到高等级威胁攻击频次处于高位,相关单位面临的网络安全风险较高。

北京知道创宇信息技术股份有限公司的数据显示,关键单位网站或业务系统的受攻击占比超过5%,是普通单位的2.5倍左右,2023年发现超过400个境内资产遭APT(高级持续性威胁)组织攻击和控制的事件,其中大部分资产为关键单位所有。

勒索类攻击频次高、范围广。勒索软件攻击通常是黑客进入用户计算机后,通过加密编码"锁定"数据后,要求用户支付赎金以获得释放数据所需的解密密钥。继2023年11月,中国工商银行股份有限公司在美全资子公司工银金融服务有限责任公司遭遇勒索软件攻击后,2024年又有印度尼西亚国家数据中心、美国联合健康集团子公司Change Healthcare等机构成为勒索软件的受害者。

据奇安信发布的《2023年中国企业勒索病毒攻击态势分析报告》显示,勒索病毒事件已连续多年位居恶意程序攻击类型的榜首,其中,医疗卫生、制造业、生活服务等行业受此类攻击的占比较高。

深信服安全业务运营总监訾然说,勒索软件攻击涉及行业领域更加广泛,赎金支付现象更为普遍,对企业的正常运营造成了巨大压力。

黑产团伙活跃度上升。大数据、云计算、物联网、人工智能等新技术迅猛发展和广泛应用带来便利的同时,也让非法数据交易团伙活跃度上升、非法交易行为更高频。

深圳永安在线科技有限公司发布的报告显示,2024年上半年共监测到3.4万个黑产团伙,其中有1973个黑产团伙经分析验证涉及真实数据泄露事件,较2023年下半年新增984个,增长近一倍。

人工智能的广泛应用降低了网络攻击的门槛,即使不具备深厚技术背景的黑客或民间力量也能发动复杂且有效的网络攻击。知道创宇公司CEO赵伟介绍,人工智能使得攻击工具更加智能化和自动化,黑客组织或民间力量可以利用这些工具来自动扫描目标、识别漏洞,并执行攻击。这种自动化攻击不仅提高了攻击效率,还降低了攻击成本。

五大新风险需警惕

当前,我国面临的网络安全威胁态势严峻,网络攻击事件从未间断,关键基础设施、关键科研场所、关键行业、关键数据、关键机构持续面临勒索软件、数据窃取和隐私泄密等攻击威胁。记者梳理近年来典型案例发现,网络安全事故频发暴露五类风险值得警惕。

关键基础设施业务中断风险

2024年7月,全球数百万台装有Windows操作系统的计算机出现"蓝屏"死机现象,造成航班停飞、医疗设备瘫痪、金融系统中断等问题。

麒麟软件有限公司李震宁等业内人士表示,此类事件频发反映出网络安全防范能力和应对能力不足问题,特别是涉及国计民生的航空、医疗、能源等关键基础设施,一旦核心系统出现问题造成业务中断,将造成巨大损失。

关键基础设施合作商的安全防护同样不容忽视。2022年11月,网络攻击造成丹麦最大铁路公司列车全部停运,连续数个小时未能恢复。看似是对该公司运营信息系统的攻击,但实际上遭受攻击的是为铁路、交通基础设施和公共客运提供资产管理解决方案的外包供应商。专家建议,应以此为鉴,提升关键基础设施的全链条网络安全防护。

关键科研场所应急响应缺位风险

近年来,我国关键信息基础设施成为境外网络攻击的重要目标,如西北工业大学和武汉市地震监测中心遭受的网络攻击事件,这些攻击具有明显的政治、军事或情报收集目的,频度高、隐匿性强。

山东师范大学公共管理学院副院长、教授刘芳认为,没有事先规划好的应急响应计划意味着组织在危急时刻无法迅速做出反应,事故发生后缺乏有效应急响应机制,导致损失扩大。

关键行业敏感信息泄露风险

大数据、云计算、物联网、人工智能等新技术迅猛发展和广泛应用带来便利的同时,数据泄露与数据窃取渠道、手段也更加多样,安全风险持续加大。

深圳永安在线科技有限公司旗下品牌威胁猎人发布的《2024年上半年数据泄露风险态势报告》显示,2024年上半年全网监测并分析验证有效的数据泄露事件16011起,较2023年下半年增长59.58%,数据泄露事件数量前五名行业分别为银行、电商、消费金融、保险和快递。

业内人士表示,金融、电商等行业的信息通常会被下游黑产团伙用于精准营销和电信诈骗,因其包含大量高价值用户数据且靠近交易环节,成为个人信息泄露的重灾区。

关键领域数据泄露带来的危害显而易见。2022年,有研究人员通过漏洞远程入侵了13个国家的25辆电动汽车,成功控制了车辆的方向盘、车窗等系统。

根据研究机构Upstream发布的《2023年全球汽车行业网络安全报告》显示,全球汽车行业在过去5年因网络攻击而遭受的损失超过了5000亿美元,其中近70%的汽车安全威胁都是由远程网络攻击行为引发的。

奇安信集团车联网安全业务负责人付海涛表示,智能网联汽车平均安装多达150个ECU,运行着约1亿行软件代码,若存在安全缺陷漏洞或被黑客利用攻击,可能给驾乘人员、周边人员带来严重的安全威胁。此外,车辆运行过程中的行驶轨迹、采集的车周环境数据等信息,被泄露后也会给公共安全带来隐患。

关键数据跨境安全保障风险

2024年8月,荷兰数据保护局宣布,对美国网约车服务运营商优步公司处以2.9亿欧元(约合人民币23亿元)罚款,理由是优步将欧洲地区司机的个人数据传送至美国。该机构表示,优步在欧洲地区收集司机的敏感信息,包括账户详情、位置信息、照片、支付信息、身份证件等,甚至在某些情况下还涉及犯罪记录和医疗数据。在长达两年多的时间里,这些数据未经适当的传输机制就被传送到优步位于美国的总部,导致数据未能得到充分保护。这一行为"严重违反"欧盟《通用数据保护条例》。

受访专家认为,此类案件为中国关键数据跨境安全敲响了警钟。虽然各国对数据隐私保护的法律要求和标准并不完全一致,但在中国坚持扩大对外开放的大背景下,如何在跨境活动中保护好对外数字贸易领域主体的数据安全,是亟待研究和解决的问题。

关键机构内部权限滥用风险

2022年1月,国际红十字会遭受了网络攻击,大量数据泄露,包括超过50万的病患信息流出。这起攻击后续被查明是借助权限上升技术实现,这说明权限系统的正确性与完备性需要得到更多重视。

美国有线通信和话音通信提供商威瑞森通信公司发布的《2024年数据泄露调查报告》显示,特权滥用是指组织内部具有合法访问权限的员工窃取数据的模式。在该报告所分析的所有事件中,属于该模式的有897起,其中854起确认有数据泄露的情况。

抢建人工智能时代网络安全优势

供应链数智化转型后,信息安全风险敞口迅速累积:泛终端安全工作全面深入程度不够,终端容易被攻陷控制;网络边界防护能力不足,导致网络边界易被突破;内网防护手段欠缺,导致攻击内网扩展迅速;安全运维工作体系化、规范化、流程化等严谨程度不够,安全隐患无法杜绝……

"在人工智能时代的前夜,我们尚未熟练利用自动化、智能化、工程化的方式,去解决网络安全复杂的场景化问题。"北京华顺信安科技有限公司CEO赵武说,对防守者与攻击者而言,现在是格外宝贵的窗口期,谁先熟练掌握新工具谁就占得先机。

国内多位网安领域从业者与专家认为,国内相关行业应从理念认知、人才梯队、技术装备等方面加快布局,尽快适应新的网络攻防环境,在应急预案、数据备份上留出安全冗余。

加强新兴威胁预研。山东省泉城实验室杨波、刘芳等认为,需重点研究人工智能防御与对抗技术。同时建立完善的应急预案,定期演练,切实提高威胁发生时的应急响应能力。建立国际合作机制,推动统一的网络安全标准建设与跨国合作机制。天津社会科学院舆情研究所研究员王建明认为,应激活多元主体共同参与网络生态治理机制,积极参与全球互联网治理,构建共建、共治、共享的网络空间命运共同体。

针对关键机构场所,一方面要通过定期的安全审计和漏洞扫描来识别和修补潜在的安全漏洞,最大限度防止数据泄露;另一方面要对数据进行有效脱敏或加密,确保使用权、管理权、所有权的严格分离,提升相关机构部门抗风险能力。

针对智能网联车等重点领域,应尽快完善法律法规体系、建立具有包容度、审慎监管的治理格局。

王建明建议,加快制定和完善智能网联汽车网络安全的法律法规体系,探索开展自动驾驶系统的网络安全管理,强化自动驾驶系统数据安全顶层设计,健全网联车网络安全管理要求、数据安全管理保护要求、个人信息和重要数据保护、数据传输共享等一系列安全标准制度体系,明确企业主体责任、监管职责和法律责任,为智能网联汽车网络安全提供坚实的法律保障。

基础软件协同安全机制需尽快成形。李震宁说,要做好操作系统等基础软件的内生安全机制,并解决国产操作系统与网络安全软件的协同机制,形成操作系统内生安全与网络安全产品深度协同防御的产业底座。

在此基础上,加快建立全流程风险管理机制。对供应商和合作伙伴进行严格的安全审查和管理,确保第三方软件和服务的安全性。业内人士建议,特别是对于与操作系统深度耦合且需要频繁升级的网络安全专用产品,应做好产品质量管控,建立全流程的风险跟踪控制机制。

避免落入先建设系统、后做安全加固的窠臼。启明星辰集团副总裁王健斌等业内专家表示,应推动可解释人工智能研究,增加模型决策过程的透明度。通信、民航、能源等关键行业要从规划、设计、实施以及预算编制角度,明确行业转型中的网络安全建设规格和要求,建立面向未来的网络安全保障体系,确保持续护航数智化安全稳定运行。

工联领创(北京)科技有限公司工控安全专家刘建兵认为,近年来网络安全标准的局限性,制约网络安全技术和产品创新,创新性的网络安全产品,无标可循、无据可依,应当为创新性的网络安全产品提供相对开放的发展渠道,助力国家网络安全的自主可控和创新。

《瞭望》新闻周刊记者**萧海川 孙飞**