

国家自然科学基金委员会网络安全现状与展望

李东¹, 郝艳妮¹, 彭升辉¹, 訾瑞杰², 刘西蒙^{1,3}

(1. 国家自然科学基金委员会信息中心, 北京 100085; 2. 北京北龙云海网络数据科技有限责任公司, 北京 100190;
3. 福州大学计算机与大数据学院, 福建 福州 350116)

摘要: 国家自然科学基金委员会(以下简称自然科学基金委)负责根据国家发展科学技术的方针、政策和规划, 有效运用国家自然科学基金, 支持基础研究, 坚持自由探索, 发挥导向作用, 发现和培养科学技术人才, 促进科学技术进步和经济社会协调发展。随着以信息化技术为代表的新生产力不断发展, 自然科学基金委一直致力于推动基金管理工作的信息化与智能化。业务种类愈加复杂, 在信息化建设中遇到信息泄露攻击等各类网络攻击, 使得网络安全面临严峻挑战。以自然科学基金委网络安全建设为主线, 介绍现有平台网络安全建设情况, 目前已建成以科学基金项目为核心的网络安全体系架构, 保障网络系统的安全稳定运行。分析介绍自然科学基金委主要的信息系统(自然科学基金共享服务网、业务部门网站、电子邮件系统)及其面临的主要威胁情况, 给出后续信息化与网络安全建设中的思考与建议。自然科学基金委将开启新一代网络安全的建设, 在充分考虑科学基金评审、管理及开放共享特点前提下, 达到“更智能、更安全、更完善”的总体目标, 为相关单位开展网络安全系统建设提供借鉴。

关键词: 信息化建设; 网络安全; 自然科学基金; 大数据

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022076

Network security of the National Natural Science Foundation of China: today and prospects

LI Dong¹, HAO Yanni¹, PENG Shenghui¹, ZI Ruijie², LIU Ximeng^{1,3}

1. Information Center of National Natural Science Commission, Beijing 100085, China

2. Beijing Beilong Yunhai Network Data Technology Co., Ltd., Beijing 100190, China

3. School of Computer and Data Science, Fuzhou University, Fuzhou 350116, China

Abstract: The National Natural Science Foundation of China (hereinafter referred to as the Natural Science Foundation of China) is responsible for effectively utilizing the National Natural Science Foundation of China,

收稿日期: 2022-02-28; 修回日期: 2022-10-31

通信作者: 刘西蒙, liuxm@nsfc.gov.cn

基金项目: 国家自然科学基金(62072109, U1804263); 福建省自然科学基金(2021J06013)

Foundation Items: The National Natural Science Foundation of China (62072109, U1804263), The Natural Science Foundation of Fujian Province (2021J06013)

引用格式: 李东, 郝艳妮, 彭升辉, 等. 国家自然科学基金委员会网络安全现状与展望[J]. 网络与信息安全学报, 2022, 8(6): 92-101.

Citation Format: LI D, HAO Y N, PENG S H, et al. Network security of the National Natural Science Foundation of China: today and prospects [J]. Chinese Journal of Network and Information Security, 2022, 8(6): 92-101.

supporting basic research, adhering to free exploration, playing a guiding role, and discovering and cultivating science and technology in accordance with the national guidelines, policies and plans for the promotion of scientific and technological progress and coordinated economic and social development. With the continuous development of new productive forces represented by information technology, the Natural Science Foundation of China has been committed to promoting the informatization and intelligence of fund management. With the increasing complexity of business types, various types of network attacks, such as information leakage attacks, are encountered in the construction of informatization and make network security face severe challenges. The network security construction of the Natural Science Foundation of China was took as the main line and the network security construction of the existing platform was introduced. At present, a network security system structure with the science fund project management as the core has been established to ensure the safe and stable operation of the network system. The main information systems of the Natural Science Foundation of China (Natural Science Foundation Shared Service Network, business department website, email system) and its main threats were analyzed and introduced. Then the thoughts and suggestions in the follow-up informatization and network security construction were given. The Natural Science Foundation of China will start the construction of a new generation of secure network. Under the premise of fully considering the characteristics of science fund review, management, and open sharing, it will achieve the overall goal of “smarter, safer, and better” and carry out network security system construction for relevant units.

Keywords: information construction, network security, natural science fund, big data

0 引言

国家自然科学基金委员会（以下简称自然科学基金委）作为我国科研资助体系的重要组成部分之一，坚持以支持基础研究为主线，以深化改革为动力，确立了依靠专家、发扬民主、择优支持、公正合理的评审原则，建立了科学民主、平等竞争、鼓励创新的运行机制，健全了决策、执行、监督、咨询相互协调的管理体系，形成了以《国家自然科学基金条例》为核心，包括组织管理、程序管理、资金管理、监督保障在内的规章制度体系，形成了包括探索、人才、工具、融合四大系列组成的资助格局^[1]。国家自然科学基金聚焦基础、前沿、人才，注重创新团队和学科交叉，为全面培育我国源头创新能力做出了重要贡献，成为我国支持基础研究的主渠道。根据国家发展科学技术的方针、政策和规划，按照与社会主义市场经济体制相适应的自然科学基金运作方式，运用国家财政投入的自然科学基金，资助自然科学基础研究和部分应用研究，发现和培养科技人才，发挥自然科学基金的导向和协调作用，促进科学技术进步和经济、社会发展。

自然科学基金委着力促进信息化与科研活

动、科研管理体系的融合，充分挖掘信息化对科研资助业务和科研资金管理的主动支撑作用。信息化发展已成为推进全球政府、企业发展的综合实力的重要标志。根据《2020 联合国电子政务调查报告》^[2]，我国电子政务发展指数国际排名从2018 年的第 65 位上升到 2020 年的第 45 位。随着信息技术和网络的快速发展，国家安全的边界已经超越地理空间的限制，拓展到信息网络空间，网络安全成为事关国家安全的重要问题。根据国家工业信息安全发展研究中心发布的《2020 年工业信息安全态势报告》^[3]，国家工业信息安全监测预警网络全年捕获来自境外的恶意网络攻击累计 200 余万次。根据国家互联网应急中心《2021 年上半年我国互联网网络安全监测数据分析报告》显示，我国境内感染计算机恶意程序的主机数量约 446 万台，同比增长 46.8%。即使面临各类网络安全挑战，我国在网络安全、数据安全和个人信息保护的轨道上迈得越来越稳健，相继出台《中华人民共和国网络安全法》（2016 年）、《中华人民共和国数据安全法》（2021 年）、《中华人民共和国个人信息保护法》（2021 年）等法律法规，正式提出了多项旨在保障网络与数据安全的制度，为我国网络安全法律体系的建立和完善

搭建了基础框架。

随着自然科学基金委业务种类的不断增加,网络与数据安全面临着更严峻、更复杂的形势。在复杂性方面,网络空间对抗趋势更加突出,大规模针对自然科学基金委的网络攻击行为增加,安全漏洞、数据泄露、网络诈骗等风险增加。根据统计,2021 年 1 月至 12 月,自然科学基金委各信息系统共受到攻击 16 830 894 次,较 2020 年攻击数(2020 年 4 213 993 次)增长了 3.4 倍。在重要性方面,自然科学基金委目前建成了 10 余个重要的信息系统,每个系统都包含大量核心数据,其中包括专家数据、评审数据等敏感信息。为了防护各类攻击,自然科学基金委在网络安全防护方面构建了完善的网络安全体系架构,并在《国家自然科学基金“十四五”发展规划》^[4]、《2021—2035 年科学基金中长期发展规划》^[5]中提出:“持续加强安全保密管理,保障科学基金管理的高效运转”。自然科学基金委存储的数据极度敏感、应用系统构成极为复杂,相比其他部委/高校更具有代表性,因此,本文以自然科学基金委为研究对象,介绍现有建设现状,分析现有网络安全建设中的不足与挑战,并讨论如何运用人工智能等智能化技术不断提升自然科学基金相关系统的网络安全水平。

1 自然科学基金委网络安全架构现状

1.1 网络模型

自然科学基金委目前已建成以科学基金项目为核心的网络安全体系架构,共有各类型网络安全设备 30 余台,保障网络系统的安全稳定运行。依据自然科学基金委实际业务需求及《网络安全等级保护制度》的相关要求,根据网络安全敏感级别对网络区域进行了划分,分为核心链路区、三级核心业务区、二级业务区、其他/测试业务区、运维管理区、隔离业务区、运维管理区和用户终端网络区,各区域之间均通过防火墙设备进行隔离。其中,核心链路区为其他区域提供了纵深的基礎网络防护;三级核心业务区是为了满足等保 2.0 三级“关键网络设备的硬件冗余”的需求,部署了相关的三级业务系统;二级业务区部署了具备区域拦截能力的防火墙设备,

主要运行着相关等保二级的业务系统;其他/测试业务区提供相关应用的测试环境,供相关工作人员开发和测试使用;隔离业务区部署了具备区域拦截能力的防火墙设备,主要部署着需对外提供服务的相关网站;运维管理区部署了相关运维服务管理相关的设备和系统,负责对其他区域进行监控和管理;用户终端网络区为独立的网段,主要放置着用户的终端计算机设备,仅提供基础的上网服务。

自然科学基金委的核心链路区和三级核心业务区均采用了双链路部署的方式,这两个区域下的所有网络设备、安全设备均采用双机热备的方式部署,当一条链路出现故障时,将在 3 s 内自动进行切换。自然科学基金委网络安全整体架构如图 1 所示。

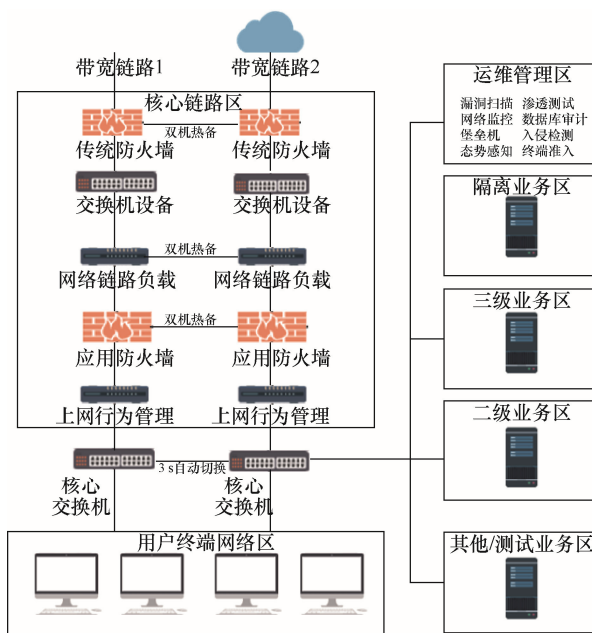


图 1 自然科学基金委网络安全整体架构示意
Figure 1 Schematic diagram of the overall network security architecture of the Natural Science Foundation of China

针对自然科学基金委员信息系统的主要攻击手段如下。

结构化查询语言 (SQL, structured query language) 注入攻击^[6]: 黑客对数据库进行攻击的常用手段之一。由于在编写代码时,程序员没有对用户输入数据的合法性进行判断,攻击者通过把 SQL 命令伪装成正常的 HTTP 请求参数,传递到服务端,欺骗服务器最终执行恶意

的 SQL 命令,达到入侵目的。通过利用 SQL 注入漏洞,攻击者可以查询非授权信息,修改数据库服务器的数据,改变表结构,甚至获取服务器系统权限。

系统命令注入:一个 Web 安全漏洞,使攻击者可以在运行应用程序的服务器上执行任意操作系统(OS)命令,并且通常会完全破坏该应用程序及其所有数据。攻击者可以利用 OS 命令注入漏洞来破坏托管基础结构的其他部分,利用信任关系将攻击转移到组织内的其他系统。

Webshell 与文件上传漏洞^[7]:文件上传漏洞通常是代码中对文件上传功能所上传的文件过滤不严或 Web 服务器相关解析漏洞未修复而造成的。Webshell 的功能比较强大,被网站管理员用于网站管理、服务器管理,可以上传/下载文件,查看数据库,甚至可以调用一些服务器上系统的相关命令(如创建用户、修改删除文件)。但是,攻击者可以将自己编写的 Webshell 上传到 Web 服务器的页面的目录下,然后通过页面访问的形式进行入侵,或者通过插入一句话连接本地的一些相关工具直接对服务器进行入侵操作。

目录遍历攻击:Web 服务器或者应用程序对用户输入的文件名称的安全性验证不足而导致的一种安全漏洞,攻击者通过利用一些特殊字符可以绕过服务器的安全限制,访问任意的文件,甚至执行系统命令。

1.2 研究现状

高尚省等^[8]从数字政府面临的网络安全风险分析出发,从安全管理、安全建设、安全运营、安全效果 4 个方面对数字政府网络安全防护工作进行了评估,提出了评估工作中发现的各地市数字政府网络安全防护工作现状,并对未来整体安全防护工作进行了展望。赵志岩等^[9]针对当前网络安全态势感知模型数据分析的深度和广度的局限性,以及协作联动能力不足等问题,提出了一种智能化网络安全威胁感知融合模型,可根据不同组合的模型应用实现数据安全服务与信任评估服务,有效提升网络安全态势感知系统的监测预警能力。王惠莅等^[10]针对我国网络安全人才存在数量缺口较大、能力素质不高、结构不尽合理等问题,分析了美国、英国和我国网络安全人才方

面相关的标准情况,提出我国网络安全人才建设标准化建议。王丹等^[11]围绕加强农业科研单位信息安全管理的内容进行探讨,介绍了信息等级保护的重要性,详细分析了中国农业科学院的网络安全管理制度体系和网络安全管理技术等,并对加强农业科研单位信息安全建设的有效策略提出了相关建议。李艳等^[12]介绍了国内外研究现状及网络安全态势感知与传统态势感知之间的区别与联系,提出了网络安全态势感知的逻辑分析框架,将整个过程分解为要素采集、模型表示、度量确立、求解分析和态势预测 5 个连续的处理阶段,为网络安全的产业化方案提供辅助思想。

2 自然科学基金委主要系统面临的网络安全攻击趋势与分析

本节介绍自然科学基金委主要的信息系统(自然科学基金共享服务网、业务部门网站、电子邮件系统)及面临的主要威胁情况。

2.1 自然科学基金共享服务网和基础研究知识库系统

自然科学基金共享服务网^[13]系统提供资助项目、结题项目、项目成果的检索与统计,提供结题报告的全文浏览,旨在提高科学基金资助工作的透明度,促进基础研究学术信息资源的共享和利用,全面反映科学基金资助绩效。自然科学基金基础研究知识库^[14]作为我国学术研究的基础设施,收集并保存科学基金资助项目成果的研究论文的元数据与全文,向社会公众提供开放获取。为了抵御“软件扫描类”“非人为试探类”等相关爬虫软件对系统数据的爬取,2021 年 8 月起对相关的防护策略进行了优化,并在相关防护设备中开启了“人机主动防御”的功能,最终实现了通过自动化的手段抵御爬虫软件的非正常获取信息的行为。

通过对攻击情况分析,共享服务网和基础研究知识库系统 2021 年全年共受到各类型攻击 3 671 052 次,峰值出现在 8 月,单月攻击数为 1 249 076 次,当月占比约 34.02%。主要的攻击方式为“SQL 注入”“系统命令注入”“Webshell 上传”“代码注入”“目录遍历攻击”“软件扫描类”“非

人为试探类”等，具体攻击趋势情况如图 2 所示。

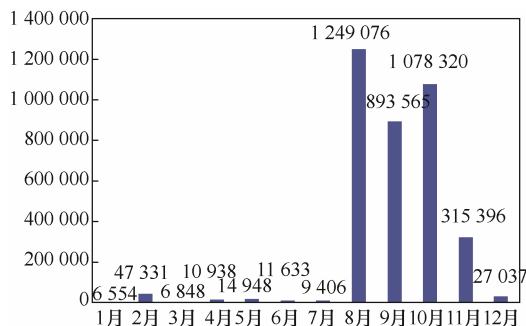


图 2 共享服务网和研究知识库攻击趋势
Figure 2 Shared services network and research repository attack trend graph

2.2 自然科学基金业务部门网站

业务部门网站作为自然科学基金委信息发布重要渠道的组成部分，负责发布其部门相关的项目指南、受理与申请政策、资助信息与成果信息等。以自然科学基金委独立部署的一个部门网站为例，2021 年该网站共受到各类型攻击 301 025 次，攻击峰值出现在 8 月，单月攻击数为 88 176 次，主要的攻击类型为“SQL 注入”“系统命令注入”“Webshell 上传”“人机主动防御”“目录遍历攻击”等，业务部门网站攻击趋势如图 3 所示。

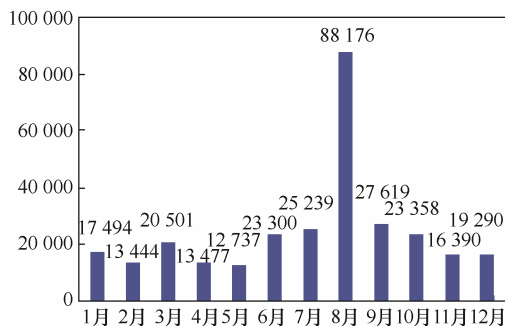


图 3 业务部门网站攻击趋势
Figure 3 Trends in website attacks of business departments

2.3 自然科学基金委电子邮件系统

电子邮件系统作为自然科学基金委日常对外进行信息交流和文件传输的工具，为日常的办公提供重大的保障性和支撑性作用。以 2021 年为例，全年电子邮件系统共受到各类型攻击 180 429 次，峰值出现在 10 月，攻击次数为 29 072 次。从对各月的攻击情况分析来看，整体攻击情况相对比较平稳，无异常波动的情况发生，主要的攻击方式相对比较单一，即“口令暴力破解攻击”，电子邮

件系统攻击趋势如图 4 所示。

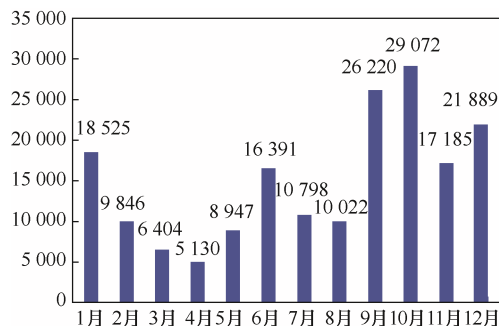


图 4 电子邮件系统攻击趋势
Figure 4 E-mail system attack trend chart

2.4 攻击数量与地域分析

针对外部非法组织频繁对相关业务系统进行信息爬取的行为，自然科学基金委开启了“人机主动防御”的功能，将共享服务网、业务部门网站和电子邮件系统 3 个网站或系统纳入了防护的范畴。2021 年 8 月，自然科学基金委共受到各类型攻击 1 933 167 次（7 月为 400 504 次），攻击数突破历史峰值，防火墙全部成功记录与拦截。

从 2021 年 8 月 1 日开始，自然科学基金委整体攻击数量呈上升的态势，峰值攻击数出现在 8 月 27 日，单日攻击次数突破 12 万次。其中，自然科学基金共享服务网的占比最高，共受到各类型攻击 1 249 076 次，占比约 64.61%，自然科学基金系统受攻击情况如图 5 所示。

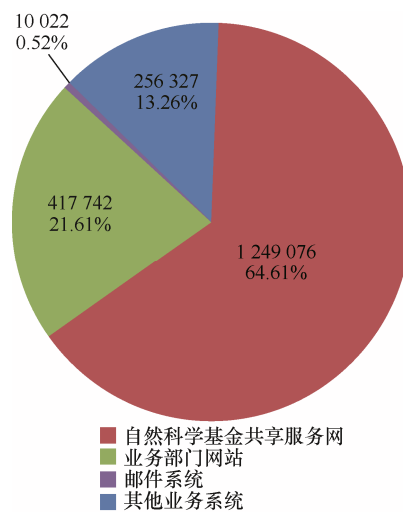


图 5 自然科学基金系统受攻击情况
Figure 5 Attacks on the Natural Science Foundation of China

以对自然科学基金共享服务网攻击地址源的

分布情况为例，攻击者区域分布相对比较分散，无固定的攻击源。攻击源 IP 前 5 位分别来自北京、四川乐山、贵州贵阳等地区，攻击源 IP 最高

来自北京，攻击数为 19 418 次，占比为 1.55%，无明显集中的攻击情况发生，海外攻击情况相对偏少，攻击源前 5 位分布情况如表 1 所示。

表 1 攻击源前 5 位分布情况
Table 1 Distribution of the top five attack sources

序号	攻击来源	攻击类型	IP 归属地	攻击次数	拦截次数	拦截率
1	36.112.128.12	人机主动防御 (19418)	中国北京	19 418	19 418	100%
2	36.112.134.189	人机主动防御 (19288)	中国北京	19 288	19 288	100%
3	182.151.7.184	人机主动防御 (19167)	中国四川乐山	19 167	19 167	100%
4	106.38.75.162	人机主动防御 (18972)	中国北京	18 972	18 972	100%
5	140.246.217.179	人机主动防御 (18408)	中国贵州贵阳	18 408	18 408	100%

2.5 攻击类型分析

从 2021 年 8 月统计的数据来看，信息系统遭受的主要攻击类型包括人机主动防御攻击、SQL 注入、系统命令注入、Webshell 上传、代码注入、目录遍历攻击、跨站脚本攻击 (XSS) 等，其中，人机主动防御攻击占比最高，各系统中攻击源前 5 位的攻击类型均为人机主动防御攻击。对比 2020 年 8 月各业务系统的攻击和拦截数据，单月攻击次数为 322 423 次，主要的攻击类型有 SQL 注入、系统命令注入、Webshell 上传、目录遍历攻击、XSS 攻击等，而对于主动防御攻击 (自动化爬虫或探测性软件) 均采用流量放行的状态，没有采取任何防御性的措施。数据异常升高的主要原因是自然科学基金委部署了人机主动防护系统，针对一些自动化爬虫或探测性软件通过一定的算法规则 (每分钟的访问次数、访问频率的间隔时间) 自动进行拉黑处理，同时将此类爬取行为列入整体安全防御的范畴，故 2021 年 8 月的攻击数据有了近百倍的增长。

从外部攻击源方面来看，外部攻击者原有的自动化攻击行为失效后，会尝试通过其他手段来展开攻击，而更换攻击源的 IP 地址是最有效的方式，导致攻击源分布比较分散。从业务层面的范畴来看，自然科学基金共享服务网是基础研究成果的共享平台，包含了大量成果相关的数据，攻击者为了获取相关的成果信息，会将此系统作为主要的攻击对象，也会尝试不

同的攻击手段，导致该系统攻击数占比过高。2021 年 8 月，单月攻击次数为 1 249 076 次，其中人机主动防御攻击类型占比超过 99%；而 2020 年 8 月的攻击数仅为 10 132 次，主要的攻击类型为网站扫描，占比超过 90%，具体如图 6 所示。通过上述分析表明，自然科学基金委的业务数据备受外界关注，通过网络信息安全的不断建设，以获取驱动为主的攻击类型已被成功防御。

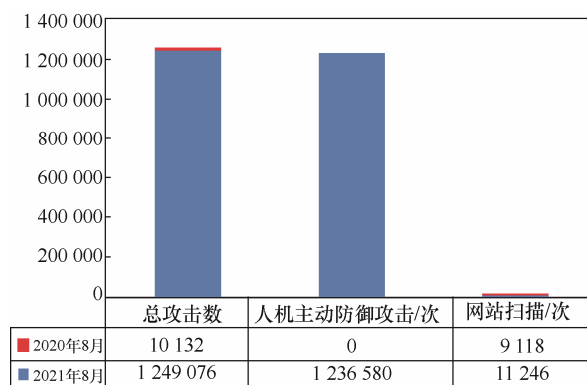


图 6 自然科学基金共享服务网按年度受到攻击情况
Figure 6 The Natural Science Foundation of China shared service network attacked by year

3 自然科学基金委面临的网络安全挑战

近几年，自然科学基金委一直致力于推动基金管理工作信息化与智能化。自然科学基金委在信息化发展的过程中面临如下挑战：攻击手段与环境复杂多样，攻击的隐蔽性越来越高，数据泄露风险加剧，业务部门网站管理分散，工作人

员防范意识需要提升。这些网络安全挑战都是自然科学基金委需要重点解决和关注的问题。

(1) 攻击手段与环境复杂多样

攻击工具与手法日趋复杂多样,单纯的防火墙策略已经无法满足对安全高度敏感的部门的需要。网络环境也变得越来越复杂,各式各样的复杂网络安全的设备与防火墙,需要不断升级、补漏的系统使得网络管理员的工作不断加重,不经意的疏忽便有可能造成安全的重大隐患。勒索病毒攻击更为频繁且破坏力更强,供应链攻击等新手段也在被高级持续性威胁(APT)组织持续利用,分布式拒绝服务(distributed denial of service, DDoS)攻击^[15]更为复杂多样。网络攻击的产业化发展趋势使得攻击工具和手法变得愈加复杂多样,传统的防火墙、入侵检测技术、恶意代码扫描、网络监控等被动防御手段显得捉襟见肘。面对日益严峻的网络空间安全威胁,研究网络安全威胁信息有助于自然科学基金委更好地“知己”“知彼”,了解自身的网络安全脆弱点,掌握已知、未知的网络安全风险点,不断提升自身在实战中的检测与响应能力,筑牢网络安全防御城墙。

(2) 网络攻击的隐蔽性越来越高

随着计算机网络知识的普及,攻击者越来越多,知识日趋成熟,传统的网络攻击行为会在系统中留下痕迹,容易被追溯;攻击行为的目标和意图比较明确,容易被发现。此外,利用智能化技术可以对复杂的攻击行为进行隐藏,如通过不同的终端设备实施攻击,在不同的时间发动攻击等。传统的恶意代码、恶意程序在发布以后,这些代码和程序的攻击目标、攻击意图往往是确定的,网络空间中的防御者可以通过逆向工程、网络监听等方式分析得知攻击的目标和意图。然而,在人工智能技术的助力下,恶意代码、恶意程序可以通过内嵌深度神经网络模型,实现在代码开源的前提下,依然确保攻击目标、攻击意图、高价值载荷三者的高度机密性,从而大幅度地提升攻击行为的隐蔽性。在这种高隐蔽攻击的环境下,需要不断提升自然科学基金委的网络防护智能化技术,实现在高隐蔽环境下对未知攻击进行发现

与溯源。

(3) 数据泄露风险加剧

数据是一项重要的资源和资产,自然科学基金委拥有着大量的申请数据、用户数据以及评审专家等敏感数据,系统一旦被攻击,很容易造成大规模的数据被窃取或破坏。此外,自然科学基金委的业务系统不断变复杂,随着自然科学基金委信息化与智能化进程的不断深入,部分应用数据被产生、传输,在受资助项目科研论文实行开放获取的政策声明下,受国家自然科学基金资助的科研项目产出的论文成果需要在互联网上公开、共享。与此同时,新一代应用通过网页、微信公众号等业务渠道接入,应用敞口风险和链条管控难度加大,各类针对数据的攻击模式变化多端,如撞库攻击、暴力破解、爬虫攻击,使得自然科学基金委面临越来越严峻的数据安全风险。未来需要不断提高网络安全抵御能力,进一步完善安全保障体系,为科学基金管理提供稳定可靠的信息化网络运行环境。

(4) 业务部门网站管理分散

自然科学基金委内设机构较多,各学部、处(室)职责分工比较细,各个学部分散建设各自网站,网站资源重复交织分散,缺乏整体的规划和统筹。

部分建设时间较久,系统安全性较弱,没有专人对网站的安全性进行评估与维护,服务体验的亲合力需进一步加强。现有的各方面已不能充分满足自然科学基金委网站网络安全的统一建设要求,亟须加紧改进。

(5) 工作人员防范意识需要提升

在自然科学基金委信息化运维工作中,采用核心管理+外包运维的服务模式。核心管理人员网络安全面临技术知识更新不够及时、难以适应网络安全高速变化的攻击模式等问题。大量服务人员面临人员更替频繁、业务理解难以深入和存在相关信息泄露风险等问题。因此,不断迭代更新网络安全相关知识,提升工作人员的防范意识、为不同的工作人员设置相对应细粒度的访问控制权限是面临的紧迫问题。

4 自然科学基金委信息化网络安全建设分析与建议

自然科学基金委信息化平台的建设,需要着眼于未来科学基金发展与深化改革需求,加强信息化安全建设的顶层设计。自然科学基金委新一代网络安全的建设,应在充分考虑科学基金评审、管理及开放共享特点的前提下,达到“更智能、更安全、更完善”的总体目标。具体而言,相比自然科学基金委员利用防火墙等传统设备的被动防御模式,“更智能”需要利用人工智能、大数据等新兴技术提升网络与信息安全的自动化治理水平,有效探查未知的网络安全风险点。现有的防护模式为先建设、再加固,在系统建设初期并未考虑到安全性的问题,“更安全”在新一代信息化平台建设初期就需要考虑数据安全、敏感信息泄露防护、关键信息基础设施免受大规模攻击等。针对外包人员防范意识较弱、人机协同分离的问题,“更完善”可以完善组织机构与相应的规章制度,提高信息中心工作人员网络安全相关能力和素质,打通人与机器之间的壁垒。

1) 构建一站式科学基金智能防护系统。通过数据挖掘、机器学习、人工智能等新型的智能化技术,建设适用于自然科学基金委信息系统的智能化防御系统。对比现有的被动式防火墙,将人工智能技术应用到网络安全防护中,实现对网络威胁的预先研判、智能防护和自动抵御,有效提升安全威胁检测、态势感知、应急处置和追踪溯源能力,实现安全防护技术的与时俱进。利用人工智能技术构建一站式科学基金智能防护系统,具体而言可以分为以下3个方面。一是基于人工智能威胁监测,包括智能化漏洞利用的检测、数据爬取攻击、Web攻击的检测以及同源性分析,通过技术可以有效地发现现有防火墙无法发现的未知威胁。二是基于智能化的威胁感知和阻断,即通过自动化的手段提供威胁预警和应急防护措施阻止威胁事件,通过事件关联分析识别网络层、系统层、应用层的潜在威胁。三是智能化的安全运营运维托管,通过智能化的安全基线构建、安全风险检测、安全风险评估、动态安全策略防护服务,实现对安全事件的自

动响应。

2) 建设统一标准化的业务网站平台。以自然科学基金委现有的私有云服务器为基础,各业务部门、各行业主管部门等用户以及相关业务抽取到统一业务网站平台,实现统一认证、单点登录、集中授权。一是提供异构数据池数据安全共享和利用,实现多源异构数据的安全融合,并为各个网站与平台提供支撑数据。二是信息安全运维团队为各个网站提供统一集中的网络安全监管与服务,提供时效性强、准确度高的网络安全监测服务,确保网站不受各类攻击。三是建设网站集约化管理平台,统一管理、统一防护、统一监测,为各级网站管理员提供多级权限管理与灵活的访问控制策略。

3) 实现更安全的保障体系建设。完善自然科学基金委安全保障体系,从高发的安全事件中吸取经验教训,建设更加完善的安全保障机制,利用新型的防护策略与手段保证系统不被破解、坚固有效,具体措施如下。一是落实关键信息基础设施保护,严格按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《网络安全等级保护条例》以及等保2.0的要求^[16],开展关键信息基础设施的认定、报送、安全建设等工作。二是开展数据安全体系建设,聚焦数据安全生命周期,规划设计全局化和开放性的数据安全体系,提升数据安全融合能力,构建自然科学基金委数据安全运营场景落地,实现组织数据资产可视、数据血缘可溯、数据风险可控、数据威胁可管。三是加强运行安全制度保障建设,包括安全管理机制落实强化、开展态势感知体系建设、安全运行服务水平提升和开展数据级容灾体系建设。

4) 加强自然科学基金委网络安全人才支撑体系建设。从加强信息安全人才队伍建设和完善网络安全组织机构两个方面构建,具体措施如下。一是积极开展全员信息安全技术培训活动,对自然科学基金委工作人员,通过线上或线下开展培训,提高全员网络安全的能力和素质,强化全员安全意识,使自然科学基金委的网络安全防护水平不断提升。二是完善网络安全组织机构建设,建立统一的网络安全管理体制,增强对网络与信

息安全建设运行管理和维护能力,扩大服务模式,将更专业的技术力量参与到网络安全系统的建设和维护工作中。

综上所述,在信息化的过程中,自然科学基金委网络安全建设取得了一定的成绩。但是在大数据背景下,自然科学基金委在信息化的过程中将面临更多的网络安全事件与挑战,需要建设更智能的防护手段、更安全的保障体系,并加强面向未来技术与人员等各方面的储备。

参考文献:

- [1] 国家自然科学基金委员会. 国家自然科学基金委员概况[EB]. 2022.
National Natural Science Foundation of China. Overview of national natural science foundation of China[EB]. 2022.
- [2] 联合国经济和社会事务部. 2020 联合国电子政务调查报告: 数字政府助力可持续发展十年行动[R]. 2020.
United Nations Department of Economic and Social Affairs. 2020 United Nations E-government survey report: digital government for the decade of action for sustainable development[R]. 2020.
- [3] 国家工业信息安全发展研究中心. 2020 年工业信息安全态势报告[R]. 2020.
National Industrial Information Security Development Research Center. 2020 industrial information security situation report[R]. 2020.
- [4] 国家自然科学基金委员会. 国家自然科学基金“十四五”发展规划[EB]. 2020.
National Natural Science Foundation of China. The 14th five-year development plan of the national natural science foundation of China[EB]. 2020.
- [5] 国家自然科学基金委员会. 2021—2035 年科学基金中长期发展规划[EB]. 2020.
National Natural Science Foundation of China. 2021-2035 mid- and long-term development plan of the national natural science foundation of China[EB]. 2020.
- [6] 张卓. SQL 注入攻击技术及防范措施研究[D]. 上海: 上海交通大学, 2007.
ZHANG Z. Research on SQL injection attack technology and preventive measures[D]. Shanghai: Shanghai Jiaotong University, 2007.
- [7] 石刘洋, 方勇. 基于 Web 日志的 Webshell 检测方法研究[J]. 信息安全研究, 2016, 2(1): 66-73.
SHI L Y, FANG Y. Research on Webshell detection method based on web logs[J]. Information Security Research, 2016, 2(1): 66-73.
- [8] 高尚省, 郭勇, 高智伟, 等. 广东省数字政府网络安全评估体系与实践[J]. 大数据, 2021, 7(2): 182-188.
GAO S S, GUO Y, GAO Z W. Practice of digital government network security index evaluation system in Guangdong Province[J]. Big Data Research, 2021, 7(2): 182-188.
- [9] 赵志岩, 纪小默. 智能化网络安全威胁感知融合模型研究[J]. 信息网络安全, 2020, 34(4): 87-93.
ZHAO Z Y, JI X M. Research on the intelligent fusion model of network security situation awareness[J]. Netinfo Security, 2020, 34(4): 87-93.
- [10] 王惠苙, 王秉政, 杨杰. 网络安全人才政策及标准化研究[J]. 信息安全研究, 2021, 7(6): 520-526.
WANG H L, WANG B Z, YANG J. Research on standardization of cybersecurity workforce[J]. Journal of Information Security Research, 2021, 7(6): 520-526.
- [11] 王丹, 孙洋, 谢辉, 等. 基于网络安全等级保护 2.0 的农业科研单位网络安全体系研究——以中国农业科学院为例[J]. 农业图书情报学报, 2020, 32 (12): 97-103.
WANG D, SUN Y, XIE H, et al. Network security systems of agricultural research institutions based on hierarchical protection 2.0: taking the Chinese academy of agricultural sciences as an example[J]. Journal of Library and Information Science in Agriculture, 2020, 32 (12): 97-103.
- [12] 李艳, 王纯子, 黄光球, 等. 网络安全态势感知分析框架与实现方法比较[J]. 电子学报, 2019, 47(4): 927-945.
LI Y, WANG C Z, HUANG G Q, et al. A survey of architecture and implementation method on cyber security situation awareness analysis[J]. Acta Electronica Sinica, 2019, 47(4): 927-945.
- [13] 李东, 于笑丰, 杜一, 等. 国家自然科学基金资助成果开放共享平台: 现状与展望[J]. 中国科学基金, 2021, 35(5): 804-814.
LI D, YU X F, DU Y, et al. The open sharing platform of national natural science foundation of China: current situation and prospects[J]. Chinese Science Foundation, 2021, 35 (5): 804-814.
- [14] 姚畅, 王晓帆, 杜一, 等. 国家自然科学基金大数据知识管理服务总体方案及关键技术研究[J]. 中国科学基金, 2019(1): 55-61.
YAO C, WANG X F, DU Y, et al. Research on the overall plan and key technologies of the big data knowledge management service platform of the National Natural Science Foundation of China[J]. China Science Foundation, 2019(1): 55-61.
- [15] 何慧, 张宏莉, 张伟哲, 等. 一种基于相似度的 DDoS 攻击检测方法[J]. 通信学报, 2004, 25(7): 176-184.
HE H, ZHANG H L, ZHANG W Z, et al. A similarity-based DDoS attack detection method[J]. Journal of Communications, 2004, 25(7): 176-184.

- [16] 密码行业标准化技术委员会. GM/T0054-20186 信息系统密码应用基本要求[S]. 北京: 中华人民共和国密码行业标准, 2018.
- Technical Committee on Standardization of Cryptography Industry. GM/T0054-20186 basic requirements for cryptographic applications in information systems[S]. Beijing: Cryptography Industry Standards of the People's Republic of China, 2018.



彭升辉(1978-), 男, 河南潢川人, 国家自然科学基金委员会信息中心中级实验师, 主要研究方向为科研信息化和网络信息安全。

[作者简介]



李东(1970-), 女, 天津人, 国家自然科学基金委员会信息中心研究员, 主要研究方向为科技政策与科研信息化。



訾瑞杰(1985-), 男, 河北邯郸人, 北京北龙云海网络数据科技有限责任公司中级工程师, 主要研究方向为网络安全信息安全与智能化运维。



郝艳妮(1978-), 女, 山西平遥人, 国家自然科学基金委员会信息中心副研究员, 主要研究方向为数据库管理与使用、计算机架构分析、计算机软件应用与维护。



刘西蒙(1988-), 男, 陕西宝鸡人, 福州大学研究员、博士生导师, 主要研究方向为数据安全与密码学。