第 1 章　关键基础设施安全概述

1.1　关键基础设施含义

关键基础设施是指公共通信和信息服务、能源、交通、水利、金融、化学、关键制造、食品和农业、政府设施和服务、公共卫生、国防军工、电子政务等重要行业和领域的重要信息和物理设施。作为经济、社会运行的神经中枢，这些设施一旦遭受来自物理和网络空间的破坏、丧失功能或者数据泄露，就可能严重危害国计民生、公共利益和国家安全。

1.1.1　中国政府高度重视关键信息基础设施安全

党的十八届三中全会通过了《关于全面深化改革若干重大问题的决定》(简称《决定》)[1]。《决定》明确指出，“加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全。设立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全。”为了贯彻落实十八届三中全会精神，健全公共安全体系，领导中国从网络大国迈向网络强国，中央网络安全和信息化领导小组于 2014 年 2 月 27 日宣告成立。中共中央总书记、国家主席、中央军委主席习近平担任组长，国务院总理李克强和中央书记处书记刘云山担任副组长。自中央网络安全和信息化领导小组成立以来，中国领导人高度重视关键信息基础设施网络安全问题，在小组全体会议、座谈会等重要场合发表了一系列重要讲话，分析了如何正确处理网络安全和发展的关系，阐述了网络强国战略及其实施举措。

1. 中央网络安全和信息化领导小组第一次会议[2]

习近平总书记在 2014 年 2 月 27 日，主持召开了中央网络安全和信息化领导小组第一次全体会议，并发表了重要讲话。讲话指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济。”习总书记本次讲话提到的信息基础设施，主要

指在政治、经济、文化、社会、军事等领域用于信息采集、处理、传播和利用的信息系统和网络。

2. 习近平总书记4·19讲话[3]

习总书记在2016年4月19日网络安全和信息化座谈会上讲话指出,“加快构建关键信息基础设施安全保障体系。金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢,是网络安全的重中之重,也是可能遭到重点攻击的目标。‘物理隔离’防线可被跨网入侵,电力调配指令可被恶意篡改,金融交易信息可被窃取,这些都是重大风险隐患。不出问题则已,一出就可能导致交通中断、金融紊乱、电力瘫痪等问题,具有很大的破坏性和杀伤力。我们必须深入研究,采取有效措施,切实做好国家关键信息基础设施安全防护。”

3. 习近平主持召开国家安全工作座谈会[4]

习总书记在2017年2月17日召开的国家安全座谈会上强调,“要准确把握国家安全形势,牢固树立和认真贯彻总体国家安全观,以人民安全为宗旨,走中国特色国家安全道路,努力开创国家安全工作新局面,为中华民族伟大复兴中国梦提供坚实安全保障。”在部署对当前和今后一个时期国家安全工作时,明确提出,“要筑牢网络安全防线,提高网络安全保障水平,强化关键信息基础设施防护,加大核心技术研发力度和市场化引导,加强网络安全预警监测,确保大数据安全,实现全天候全方位感知和有效防护。”习总书记将关键信息基础设施安全问题作为国家安全问题来看待。由此可见,国家领导人高度重视关键信息基础设施安全。

4. 2016年3月政府工作报告[5]

李克强总理2016年3月5日在第十二届全国人民代表大会第四次会议上做的政府工作报告中多次提到了基础设施建设工作。在“十三五”时期主要目标任务和重大举措的推进新型城镇化和农业现代化,促进城乡区域协调发展方面指出:“加强重大基础设施建设,高铁营业里程达到3万公里、覆盖80%以上的大城市,新建改建高速公路通车里程约3万公里,实现城乡宽带网络全覆盖。”在2016年重点工作中的改善农村公共服务方面指出:“加大农村基础设施建设力度,新建改建农村公路20万公里,具备条件的乡镇和建制村要加快通硬化路、通客车。抓紧新一轮农村电网改造升级,两年内实现农村稳定可靠供电服务和平原地区机井通电全覆盖。实施饮水安全巩固提升工程。推动电子商务进农村。

建设美丽宜居乡村”。在安全生产和公共安全方面指出:“加强安全基础设施和防灾减灾能力建设,健全监测预警应急机制,提高气象服务水平,做好地震、测绘、地质等工作。完善和落实安全生产责任、管理制度和考核机制,实行党政同责、一岗双责、失职追责,严格监管执法,坚决遏制重特大安全事故发生,切实保障人民生命财产安全。”

分析政府工作报告中与基础设施相关的内容可知,基础设施的范围比信息基础设施要大,基础设施不仅包括用来保障金融、能源、电力、交通等领域系统正常运作的电信和广播电视等网络空间的系统和网络,还包括为人民生产生活提供公共服务的工程设施,如公路、铁路、电网、水利等物理空间设施。即基础设施既包括网络空间的信息基础设施,也包括物理空间的工程设施。

5. “一带一路”推进能源基础设施互联互通[6]

李克强总理在 2016 年 11 月 17 日主持召开的国家能源委员会会议上指出,“能源战略是国家发展战略的重要支柱,保障国家能源安全需要统筹国内国际两个大局,既要立足国内,又要深化国际合作,形成多元稳定的供给格局。要巩固与传统资源国家的互利合作,优化能源贸易结构,抓住‘一带一路’建设重大机遇,推进能源基础设施互联互通,加大国际产能合作,带动有竞争优势的能源装备出口。积极参与全球能源治理,推动国际能源秩序和治理体系朝着更加公正合理的方向发展。”

能源指煤炭、石油、天然气、生物质能和电力、热力以及其他直接或者通过加工、转换而取得有用能的各种资源[7]。作为基础设施的一个重要领域,能源是国民经济发展的重要物质基础。中国政府高度重视能源基础设施互联互通建设工作。

1.1.2　中国政府相关文件

1. 国务院

国务院办公厅于 2007 年 9 月 18 日发布了《关于开展重大基础设施安全隐患排查工作的通知》(国办发〔2007〕58 号)[8],通知要求,重点做好“公路交通设施、铁路交通设施、水运交通设施、民航交通设施、大型水利设施、大型煤矿、重要电力设施、石油天然气设施、城市基础设施”九个对象的安全隐患排查工作。国务院办公厅指出的上述九类基础设施都属于重大、关键基础设施范畴,都是指那些关乎国计民生的核心基础设施。

国务院办公厅于2012年6月28日发布了文件《关于大力推进信息化发展和切实保障信息安全的若干意见》(国发〔2012〕23号)[9]。该文件在健全安全防护和管理,保障重点领域信息安全的保障工业控制系统安全方面指出:“加强核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统,以及物联网应用、数字城市建设中的安全防护和管理,定期开展安全检查和风险评估。重点对可能危及生命和公共财产安全的工业控制系统加强监管。对重点领域使用的关键产品开展安全测评,实行安全风险和漏洞通报制度。”工业控制系统广泛应用于上述领域的基础设施中,实现设施和系统的自动化控制和运行操作,是基础设施的核心组成部分。这些基础设施的安全防护重点就是保障工业控制系统的网络和物理安全。

国务院于2013年9月6日发布了文件《关于加强城市基础设施建设的意见》(国发〔2013〕36号)[10]。文件指出,城市基础设施是城市正常运行和健康发展的物质基础,并建议,“加强城市道路交通基础设施建设,加大城市管网建设和改造力度,加快污水和垃圾处理设施建设,加强生态园林建设。”城市基础设施是国家关键基础设施的缩影和典型代表,城市中的道路、水/电/天然气管网、污水和垃圾处理系统等组成了城市的骨架,这些基础设施的完善程度影响着城市的承载能力及人民的生活质量。

2. 工业和信息化部

工信部于2014年8月29日发布了《关于加强电信和互联网行业网络安全工作的指导意见》(工信部保〔2014〕368号)[11],在加强新技术新业务网络安全管理重点工作中指出:“加强对云计算、大数据、物联网、移动互联网、下一代互联网等新技术新业务网络安全问题的跟踪研究,对涉及提供公共电信和互联网服务的基础设施和业务系统要纳入通信网络安全防护管理体系,加快推进相关网络安全防护标准研制,完善和落实相应的网络安全防护措施。”提供公共电信和互联网服务的网络和系统都属于信息基础设施的范畴。

工信部于2011年10月27日发布了《关于加强工业控制系统信息安全管理的通知》(工信部协〔2011〕451号)[12]。通知指出:“数据采集与监控(SCADA)、分布式控制系统(DCS)、过程控制系统(PCS)、可编程逻辑控制器(PLC)等工业控制系统广泛运用于工业、能源、交通、水利以及市政等领域,用于控制生产设备的运行。一旦工业控制系统信息安全出现漏洞,将对工业生产运行和国家经济安全造成重大隐患。加强工业控制系统信息安全管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、

城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。”上述关键基础设施都是指事关国家、经济发展命脉的重要工业控制设备、网络和系统。

3. 网络安全法

2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》（简称《网络安全法》）[13]。该法案专门设立了一节对关键信息基础设施的运行安全做出了具体的法律规定，对关键信息基础设施运行安全不仅给出了定义，规定了如何实施安全保护，而且还从国家相关部门、行业、关键基础设施/网络运营者等不同层面分别规定了国家网信部门、行业主管单位、运营单位或企业等各自的义务与责任。

其中，《网络安全法》的第三章网络运行安全的第二节关键信息基础设施的运行安全的第三十一条规定：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。”与其他定义相比，《网络安全法》对关键信息基础设施的定义又新增加了网络安全等级保护和重点保护的要求。

4. 国家互联网信息办公室

经中央网络安全和信息化领导小组批准，国家互联网信息办公室于 2016 年 12 月 27 日发布了《国家网络空间安全战略》（简称《战略》）[14]，将保护关键信息基础设施作为一项重点战略任务。《战略》指出：“国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。坚持技术和管理并重、保护和震慑并举，着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。”《战略》不仅给出了关键信息基础设施较为全面的定义，还重点强调了信息基础设施和其关键数据的同等重要性。

经中央网络安全和信息化领导小组批准，2016 年 7 月 8 日，首次全国范围的关键信息基础设施网络安全检查工作启动[15]。检查时间截至 2016 年 12 月底。本次检查给出了关键信息基础设施的如下定义："关键信息基础设施指的是面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，这些系统一旦发生网络安全事故，可能影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境及人民生命财产造成严重损失。"本次安全检查给出的关键信息基础设施定义，将关键信息基础设施定义为提供网络信息服务或支撑重要行业运行的信息系统或工业控制系统。该定义突出强调了信息系统和工业控制系统在关键信息基础设施中的同等重要性。

国家互联网信息办公室于 2017 年 7 月 11 日发布了《关键信息基础设施安全保护条例(征求意见稿)》[16]。该条例是依据《网络安全法》，专门针对关键信息基础设施安全制定的条例。在该条例的第三章第十八条给出了关键信息基础设施保护范围："下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：(一)政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；(二)电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；(三)国防科工、大型装备、化工、食品药品等行业领域科研生产单位；(四)广播电台、电视台、通讯社等新闻单位；(五)其他重点单位。"此外，该条例也在关键信息基础设施运营者安全保护、产品和服务安全、监测预警、应急处置和检测评估等方面给出了具体要求及法律责任规定。

1.1.3 美国政府关键基础设施安全布局

随着关键基础设施行业中越来越多的系统网络接入公共网络，基础设施系统面临着越发严峻的网络安全问题。美国也已经将关键基础设施安全提升为国家战略问题。美国自克林顿政府就开始重视关键基础设施安全问题。克林顿、小布什、奥巴马和特朗普政府在国家安全战略、机构设置、安全保护计划及项目、标准规范等方面持续开展并推动了关键基础设施安全保护工作布局，通过一系列政策文件从法律、政府层面引导、促进关键基础设施安全建设工作。关于这些具体政策文件的介绍请参见 1.4 节内容。

1996 年 7 月 15 日，在克林顿政府颁布的第 13010 号行政令《关键基础设施防护》[17]中指出，关键基础设施包括电信、电力、天然气石油存储和运输、银行和

金融、交通、水利供应、应急服务(如医疗、警务、火警和救援)及其他保障政府持续运作 8 类系统。由于许多关键基础设施都是由私营企业拥有和经营的,因此,13010 号行政令还宣布成立总统关键基础设施保护委员会,要求政府部门与相关私营企业一起合作来研发、部署安全防护技术。

1998 年 5 月 22 日,克林顿总统颁布了第 63 号总统决策指令《关键基础设施防护》[18]。该指令在明确关键基础设施定义和范畴的基础上,进一步明确了财政部、司法部、国防部、商业部、交通部、能源部等相关部门的责任与义务。

小布什总统上任后不久便发生了"9·11"恐怖袭击事件,因此,为了应对恐怖袭击活动,加强基础设施安全防护措施,2001 年 10 月 16 日,小布什政府颁布了第 13231 号行政令《信息时代的关键基础设施防护》[19]。该行政令指出,信息时代的商业交易、政府运作和国家防御都依赖的关键信息基础设施涉及电信、能源、金融服务、制造业、水利、交通、医疗保健和应急服务等行业和领域。第 13231 号行政令还宣布成立总统关键基础设施保护管理委员会,并要求委员会关于关键基础设施保护工作、安全项目建设等方面定期提出发展建议和政策。

为了进一步组织开展具体安全防护项目,2002 年 11 月 25 日,小布什总统签署了《国土安全法案》[20],宣布成立国土安全部,专门负责国土安全事务,具体包括防止发生针对关键基础设施的恐怖袭击事件,加强安全防范能力,保卫网络空间安全,增强自然灾害应对能力等。国土安全部自成立以来针对关键基础设施网络安全,设计了专门的机构,开展了一系列安全实践和研发项目,如设计了工业控制系统网络应急响应小组,开展了"网络风暴"系列演习,发起了"国家基础设施保护计划"和"下一代网络基础设施"项目等。

为了动员和组织全国上下共同抵御恐怖袭击活动,小布什政府于 2002 年 7 月 16 日发布了《国土安全国家战略》第一版[21]。随后,在 2003 年 2 月,小布什总统发布了《关键基础设施和重要资产物理保护国家战略》[22],将农业和食品、水利、公共健康、应急服务、国防工业基础、电信、能源、交通、银行和金融、化学工业和危险材料、邮政和航运等设施作为关键基础设施,将国家古迹和建筑、核电站、大坝、政府设施、商业设施作为重要资产。2006 年,国土安全部发起了《国家基础设施保护计划》[23]。该计划的目标是通过加强对国家关键基础设施和重要资产的保护,来建立一个物理上、信息网络上更安全以及故障恢复能力更强的美国,以此来阻止、减缓或消除由恐怖袭击所带来的蓄意破坏影响。

奥巴马总统上任后,继续加强了关键基础设施安全防护力度。2013 年 2 月 12 日,奥巴马政府同时颁布了第 13636 号行政令《提高关键基础设施的网络安全》[24]和第 21 号总统决策指令《提高关键基础设施的安全性和恢复力》[25]。前

者旨在指导行政部门设计一个技术中立的网络安全框架。后者则明确定义了16个关键基础设施行业,包括化学、商业设施、通信、关键制造、大坝、国防军工、应急服务、能源、金融服务、食品和农业、政府设施、公共卫生、信息技术、核反应堆材料和废物、交通、城市供水和废水处理系统。

在第13636号行政令和第21号总统决策指令的指导要求下,美国国家标准与技术研究院起草,美国白宫于2014年2月12号公布了《提高关键基础设施网络安全的框架规范》(简称《规范》)[26]的第一个版本。该规范是自美国启动保护关键基础设施信息安全工作以来发布的第一个较全面的基础性指导文件。为了进一步加强网络安全法律、法规保护力度,奥巴马总统于2015年12月18日签署了《网络安全信息共享法案(2015)》[27],并将其标注为《2015年网络安全法案》。该法案第208条专门对"多重并发的关键基础设施网络事件"给出了法律规范。除了通过立法来促进改善国家网络安全以外,奥巴马政府还在2016年2月9日推行了《网络安全国家行动计划》[28],在提升国家整体网络安全水平方面,该行动计划明确指出,要增强关键基础设施的安全性和恢复力。

特朗普总统上任后开始全面加强网络安全建设。特朗普总统于2017年5月11日签署了网络安全行政令《增强联邦网路和关键基础设施的网络安全》[29],在联邦网络、关键基础设施和国家三个方面,规定了增强网络安全的措施。在关键基础设施网络安全方面,该项行政令要求应遵照奥巴马政府颁布的第21号总统决策指令所规定的关键基础设施行业进行安全评估,并于180日内提交其网络安全风险评估报告,今后每年度评估一次并更新报告。

小结:中国政府和美国政府都高度重视关键基础设施在网络空间所面临的安全威胁和攻击问题。二者分别通过领导人重要讲话、政府文件等形式在不同场合强调了开展关键基础设施安全防护工作的必要性,阐述了关键基础设施的含义和范畴,成立了专门的网络安全机构,发布了安全法律法规、国家安全战略及安全保护计划等重要文件。

1.2 典型安全事件

在现代战争时期,敌对双方首要摧毁目标必然是指挥机构,其次便是国家正常运行所依赖的电力、石油、天然气、交通以及水利等关键基础设施,从而实现以点破面,使整个国家陷入瘫痪的目的。目前较为突出的是在海湾战争和科索沃战争中,美军通过"斩首行动"迅速破坏了敌方的高级指挥机构和众多电力、能

源、通信、机场等关键基础设施，导致伊军和南联盟很快地失去了指挥权进而陷入一片混乱。

在目前总体和平的情况下，一些国家政府雇佣的高度组织化和专业化的黑客团体，以及一些以敲诈勒索为手段来营利的黑客团伙，这些组织和个人在近几年给各国的关键基础设施带来了不少的混乱和麻烦，也引起了业内业外的广泛关注。工业控制系统是关键基础设施的核心组成部分，因此，工控系统也就成了安全攻击的首要对象。目前发生在工控领域的安全事件得到了世界各国的广泛关注。下面就国内外发生在能源、水利、污水处理、交通以及制造业等领域的安全事件，分别叙述其起因、经过及影响。

1. 能源行业

(1) “震网”病毒

“震网”病毒于 2010 年 6 月席卷伊朗、印度尼西亚和印度，其中伊朗关键基础设施感染最为严重，尤其是核电站的浓缩铀设备的离心机遭到破坏，造成伊朗核电站推迟发电、重新更换设备、核泄漏等一系列重大安全后果。“震网”病毒可以自我复制，通过网络或 USB 等介质不断扩散。仅伊朗国内就有 500 万网民和多个行业的领军企业感染了“震网”病毒。

首先，“震网”病毒的入侵方式是精心设计的。这次事件的主要受害者 Natanz 工厂，负责着伊朗的核项目，拥有 15 层防火墙、3 个数据单向保护设备和入侵检测系统，这么强大的保护网之所以都未能阻止“震网”病毒的渗透攻击，是因为“震网”病毒采取了极为巧妙的攻击策略。“震网”病毒的编写人员在 2009 年创建之日起便定向攻击了和 Natanz 工厂相关联的几家电力设施、工业自动化系统及铀浓缩离心机供应商，设计者通过精心设计，悄无声息地渗透了这些企业网络，从中搜集和“Step 7”软件相关的信息，并利用在其中一家工控系统供应商为 Natanz 工厂系统升级改造的时机，通过移动介质将“震网”病毒引入了 Natanz 工厂系统中。

其次，“震网”病毒的设计也极为复杂。2010 年曝光于公众视野范围内的只是“震网”简单版本，然而，“震网”的复杂变种版本才是那个让伊朗政府极为不安的不定时炸弹。2007 年有人在 VirusTotal 上提交了段代码，这在后来被证实为“震网”的第一个变种，即复杂变种版本。大家所熟悉那个简单版本，其相较于复杂版本更为简单，也缺乏隐蔽性，只是能够控制离心机的转速使其周期性大幅改变，从而破坏离心机。但是，Natanz 工厂为了弥补离心机不稳定而配置的级联保护系统，能够防止离心机坏掉，防止发生生产流程终止情况。所以，“震网”病

毒简单版本并不是那个影响力最大的。复杂变种版本是最早入侵并潜伏在Natanz工厂工业控制系统中的,其主要目的并不是大肆破坏,而是通过伪装数字签名来表现为一个合法软件。在控制室、报警系统和操作员看来,系统运行状态一切正常。“震网”病毒复杂变种版本小心翼翼地控制着隔离阀,增大压力,慢慢减少转子的寿命,但不马上损坏离心机,从而增强了隐蔽性。

然而,“震网”病毒也不是完全隐蔽的。其开始是针对伊朗核设施设计的,但是在感染民用主机的同时,也将自身暴露于公众视野之下,许多安全公司都针对“震网”病毒的攻击模式和路径加固了安全防护措施。“震网”病毒无疑是网络空间的一枚核弹,其造成的影响和破坏不局限于伊朗,它刷新了人们对21世纪网络战争的认知,一个国家以较低的代价便可以在网络空间对另一方造成巨大的破坏。

(2)“火焰”蠕虫

2012年,美国和以色列为了破坏伊朗的核计划使用“火焰(Flame)”蠕虫进行了大量的恶意攻击。2012年5月,“火焰”蠕虫由于在以色列的策划下对伊朗的石油工业发起了一系列攻击,由此进入了公众视野。虽然,此次行动中,以色列成为了替罪羔羊,但“火焰”蠕虫据称是由美国和以色列共同研究设计而完成的,甚至有西方某官员称,策划者有NSA、CIA、以色列军队和Stuxnet的设计团队等,在如此强大的团队共同努力下,“火焰”蠕虫也就成为迄今为止最为复杂的恶意软件。即使是国家级的安全网络,仍然会感染“火焰”蠕虫。感染后果包括:用户的浏览器记录、键盘、账号密码、通话记录等敏感信息都会被回传到C&C服务器,摄像头和麦克风遭受非授权访问控制,地理位置信息数据遭受泄露等。下面从“火焰”的传播路径、复杂结构、隐蔽性三个特点描述这一蠕虫病毒。

“火焰”主要通过物理接触和远程感染两种方式在伊朗的关键基础设施领域扩散,安全研究人员在捕获的“火焰”样本中发现了“震网”病毒所使用的USB攻击模块。一些人会将感染了“火焰”蠕虫的USB插入到关键基础设施系统中的PC机中。另一种传播方式则是通过Windows Update,将冒用微软数字签名的“火焰”蠕虫从伪造的服务器下载安装到受害者电脑上,由此躲过杀毒软件的检测。

“火焰”蠕虫的复杂性体现在:拥有5种以上不同的加密算法,3种以上压缩技术,至少5种文件格式。“火焰”是用不太常见的LUA语言(一般用在游戏机上)编写的,其总体大小在30MB左右。“火焰”代码有大量的独立模块和攻击工具包,其中主模块文件大小在6MB之上,其他模块则有漏洞攻击代码、模块配置