DOI 10.15302/J-SSCAE-2016.06.017

当前网络安全形势与应急响应

刘欣然[1]，李柏松[2]，常安琪[2]，鲁辉[3]，田志宏[4]

（1. 国家计算机网络应急技术处理协调中心，北京 100029；2. 安天实验室，哈尔滨 150000；
3. 中国科学院微电子研究所，北京 100029；4. 中国工程物理研究院计算机应用研究所，四川绵阳 621900）

摘要：随着互联网应用的迅速发展，各种网络安全威胁不断出现。本文介绍了网络安全所呈现的特点以及目前所面临的形势。攻击方法的更新、攻击技术的提升以及攻击范围的扩大给应急工作带来了考验。应急工作的管理现状存在一定的问题，在核心技术、安全保障方面都比较落后。借鉴传统领域的应急体系，改善当前应急技术措施成为网络安全工作的重要部分。针对新时期的网络安全应急工作环境，提出了调动体系力量，多方联动的消除方法，从体制和机制等方面来进行保证，以防止网络威胁产生的巨大影响。

关键词：网络安全；威胁；信息安全；应急响应；应急体系

中图分类号：TP393　　**文献标识码：**A

The Current Network Security Situation and Emergency Network Response

Liu Xinran[1], Li Baisong[2], Chang Anqi[2], Lu Hui[3], Tian Zhihong[4]

(1. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China;
2. Antiy Labs, Harbin 150000, China; 3. Institute of Microelectronics, Chinese Academy of Sciences, Beijing 100029, China;
4. Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, Sichuan, China)

Abstract: Considering the emergence of recent network security threats, this article presents network security features and the current situation. Updated attack methods, enhanced attack technology, and expanded attack scope have changed emergency work. Some problems exist in emergency management of the status quo; the core technology and security assurance are relatively backward. Learning from the emergency response system in traditional areas in order to improve current emergency technical measures becomes an important part of network security. In this paper, the author proposes a multi-linkage elimination method that can mobilize system strength and protect against network threats based on the system and the mechanism.

Key words: network security; threat; information security; emergency response; emergency system

一、前言

随着信息技术的不断发展进步，网络安全面临的问题增多，企业对安全的重视程度逐渐增加，应急响应工作显得举足轻重。新时期网络安全应急的定位已发生了变化，应急的范围不仅仅包括网络，

收稿日期：2016-10-08；**修回日期：**2016-10-20

作者简介：刘欣然，国家计算机网络应急技术处理协调中心，研究员，博士生导师，研究方向为网络与信息安全，分布式计算等；
E-mail: lxr@cert.org.cn

基金项目：中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)

本刊网址：www.enginsci.cn

同时也有重要的信息内容。随着威胁的不断演化，网络安全应急也面临着考验。

从总体上看，网络安全事件的处置分为包括国家级政府、国家级非政府和地方级非政府在内的三个层面。下层安全应急体系例如各家安全厂商的应急响应中心，互联网公司、电商的应急响应中心纷纷建立。即便如此，新一代网络安全威胁的传播速度很快，攻击面很广，其威胁覆盖面已超乎我们的想象，移动电话、个人电脑、网站、应用、社交媒体无一幸免。突发事件的发生给应急工作带来巨大的困难与考验。

进入 21 世纪，网络安全这一问题变得更加突出。如 2000 年雅虎网站的大规模拒绝服务攻击，2001 年的红色代码事件，2001 年全球根域名服务器遭到大规模拒绝服务攻击，2003 年的 SQL Slammer 蠕虫病毒，2004 年的震荡波 ，2006 年的熊猫烧香病毒，2010 年的震网事件 [1]，2015 年利用 Cobalt Strike 平台的 APT-TOCS[2] 事件、Hacking-Team 数据泄露事件、Biige 等商业手机木马利用事件，以及 2016 年日趋活跃的勒索软件的出现，使信息安全事件种类越来越多，呈现出如下特点。

（一）攻击组织化、趋利化

网络攻击不仅仅是单个黑客的炫技行为，也体现为许多有组织的以获取经济利益为目的的商业行为。其攻击行为的实施都有清晰分工，攻击组织化大大增强了攻击者对各类网站和信息系统的攻击能力，而目标趋利化则使得攻击所造成的危害进一步加大。

（二）攻击方法推陈出新

传统攻击通常采用 rootkit、感染式病毒等方式，而如今网络攻击的新思路、新技术、新方法不断出现，如网络钓鱼、社会工程、网页挂马、0day 漏洞、重定向等攻击。不断出现的种种新的攻击方法也增加了网络与信息安全事件原因分析和技术处置的难度。

（三）攻击技术工具化、平台化

纵观全球，传统意义的高级持续性威胁（APT）攻击更多地让人联想到精干的作业团队、用于攻击的基础设施、0day 漏洞挖掘小组以及恶意代码的编写小组等。但 APT-TOCS 事件攻击者依托自动化攻击测试平台 Cobalt Strike 实现了对目标主机进行远程控制的能力，用一种新的方式为一些技术能力和资源相对有限的国家和组织提供一种新的示范选择。这种方式降低了攻击的成本，而这种高度“模式化”的攻击也会让攻击缺少鲜明的基因特点，从而更难追溯，应急工作更难有效执行。

（四）攻击目标范围广泛化

除传统的网站、信息系统外，域名系统等互联网基础设施、邮件系统、工业控制系统、个人终端、智能手机、无线网络等都已经成为网络攻击的目标。这两年，除了熟悉的漏洞 Windows、Linux 和其他类 Unix 系统、iOS、Android 等操作系统及其应用软件漏洞外，安全威胁在小到智能汽车、智能家居、智能穿戴，大到智慧城市都无所不在。

二、应急响应的管理现状与存在问题

多年来，信息化发展已经深入到政府管理、企业运作、群众生活等方面，成为支撑社会正常运转的重要基础。当作为基础设施的信息系统出现故障时，将会直接影响正常的社会管理和服务。

（一）复杂的国内外环境

当今世界正发生着复杂深刻的变化。国际金融危机深层次影响继续显现，世界经济缓慢复苏、发展分化，国际投资贸易格局和多边投资贸易规则酝酿深刻调整，各国面临的发展问题依然严峻。我国“一带一路”顶层战略充分依靠与有关国家既有的双多边机制 [3]，借助既有的、行之有效的区域合作平台，积极发展与沿线国家的经济合作伙伴关系。

国际经济贸易战略交叉，互联网应用水平增高，使各国在合作的同时也体现出激烈的国际竞争与网络力量的博弈。

（二）核心技术和设备的缺失

国内网络与信息系统包括重要部门的信息系统使用国外技术和产品的比率居高不下，技术水平与基础设施供应不能很好匹配，与大国还有差距。如美国具备强大的技术力量，包括监控硬件生产、制造，操作系统、芯片在世界范围内的占有

率，其所具备的强大的信息获取能力是其他国家无法比拟的。

（三）信息安全保障工作比较落后

我国信息安全整体水平还相对比较落后，各级地方政府虽然已经开始认识到信息安全的重要性，但在具体工作的实施过程中仍存在问题，如应急响应工作的开展相对滞后，很多单位未能较好地落实国家要求，人才与投资显现出不足等问题。国家计算机网络应急技术处理协调中心（CNCERT/CC）自主监测的数据显示，2015 年已发现 10.5 万余个木马和僵尸网络控制端，控制了我国境内 1 978 万余台主机，抽样监测的恶意程序转发的用户邮件数量超过 66 万封 [2]，个人信息泄露事件频发，网络设备安全漏洞风险较大，并有增加趋势。

2014 年，我国成立了中央网络安全和信息化领导小组，统筹协调涉及各个领域的网络安全和信息化重大问题。国务院重组了国家互联网信息办公室，授权其负责全国互联网信息内容管理工作，并负责监督管理执法。2016 年 4 月 19 日，中共中央总书记习近平召开网络安全和信息化座谈会探讨网络安全措施与办法 [4]，强调在“十三五”开局之年网络安全和信息化工作是“十三五”时期的重头戏；在考察东北老工业基地期间，他来到了哈尔滨本地网络安全企业安天科技股份有限公司，突显了国家对于网络安全方面的重视。

纵观网络安全形势，去年由网络攻击引发的数据泄露依旧猖獗。信息泄露的背后已经形成一条完整的利益链，这些用户信息或被用于团伙诈骗、钓鱼，或被用于精准营销。因恶意代码导致的信息泄露事件中，极为值得反思的是 XcodeGhost 事件 [5]，截至 2015 年 9 月 20 日，各方累计发现已确认共 692 种 APP 曾受到污染，受影响的包括微信、滴滴、网易云音乐等流行应用 [6]。这次事件采用了非官方供应链污染的方式，反映了我国互联网厂商研发存在缺陷和安全意识薄弱的现状。

从我国现阶段来看，信息安全突发事件应急管理工作取得了一定的进展，但从总体来看，应急预案不够完善，在实际应用上，缺乏实用性和可操作性。除了中国外，世界上网络大国或网络发达国家都制定了网络安全国家战略 [7]。各国网络安全战略之所以如此密集地出台，主要是因为随着互联网的迅速发展和普及，各国政府、关键基础设施、企业和公民均严重依赖于网络的可靠功能；网络安全出现问题，将严重危及政府和企业的运转，极大影响公众的社会生活，可以说网络安全是一国繁荣发展的“生命线”。因此，合理建立信息安全突发事件的应急响应体系，实现有限投入下最大程度地降低信息安全突发事件的负面影响，就成为一个迫切需要解决的问题。

我国在互联网网络安全应急保障体系方面，已经初步形成了在工业和信息化部互联网应急工作办公室领导下，以 CNCERT/CC 为核心、以各种互联网骨干网运营企业为依托、以应急服务支撑单位为后援的国家级网络安全应急处理体系 [8]。

随着我国经济的发展，在信息安全的法律法规方面，我国已经进行了初步尝试，但相对发达国家来讲距离还不小。互联网的复杂性和跨地域性决定了网络安全事件的应急处置应该是多个部门和单位协同的过程，这便要求各主管部门和应急机构要不断整合各自的优势，最终形成合力，并根据各部门在应急响应中所发挥的作用，确定一个应急响应牵头部门，负责统一指导整个应急响应工作，以改变目前各自为政的局面。不规范的网络行为，是造成网络风险最重要的因素。然而，仅仅依靠打击网上犯罪和违法行为来解决问题也是远远不够的，要充分做到网络安全监管的关口前移，发挥行政管理措施的职能。目前整个网络安全应急响应工作仍存在诸多问题，如应急响应的时间滞后性问题，应急响应工作有效落实的问题，应急计划操作性不强、部门联动性差、应急培训演练次数不足、应急技术人员的专业性不足、过分依赖国家应急平台等问题 [9,10]。

三、传统领域的应急内容参考

传统领域的应急体系包括企业安全生产事故应急体系、公共灾害安全事故应急体系、公共卫生领域传统安全事件应急体系等，各领域均已建立起相应的法律法规和相关工作技术，并取得了一定的技术创新。传统领域的安全是真实环境下的国家公共基础设施应急体系建设的安全，而网络安全方面的防范重点表现为计算机病毒与黑客犯罪。网络安全除了保护设备与系统安全外，要保护数据安全。网

络安全与其他领域安全均要做到在应急事件来临时快速、高效、全面的响应。从针对传统领域应急体系的建设中，总结出网络安全应急在组织机制、指挥体系以及救援队伍方面需要借鉴之处，为从高位（国家机构）、中位 [互联网数据中心（IDC）、内容分发网络机构（CDN）、电商、行业主管] 到低位（网民）三方面建立网络安全应急体系提供指导。网络安全应急体系建设过程中需要考虑以下几个方面——组织体系：需要建立国家层面的安全应急指挥部门和应急管理部门，在各省市、自治区及地方区域建立相应的应急机构；指挥体系：需要建立各级应急指挥系统、通信指挥系统；建立监测和预防预警系统；建立信息共享机制、事件上报机制、通报机制；建立专业的应急队伍：国家队、省级队和各单位建立应急队伍，并加强演练和培训。四大应急体系差异分析情况见表 1。

四、采取的措施

综上所述，当今网络安全形势严峻，网络威胁发展迅速，应急响应工作面临重大考验。互联网网络安全应急保障体系在稳步建设的同时仍存在许多问题，通过应急响应工作的加强与改善来解决网络安全问题成为行之有效的服务手段之一，并具有一定的迫切性。

针对新时期的网络安全应急工作，因其定位已发生变化，应急的对象也在不断扩充，需要调动体系的力量，多方联动及时消除隐患，从体制和机制等方面来进行保证，防止产生巨大的恶劣影响。具体包括以下几方面内容。

（一）坚持战时协助攻防、急时快速掌控、平时侧重服务的应急方针

战时协助攻防：网络应急工作应该以保障军事网络安全运行为核心，协助我国军事网络部队进行网络战的方案制定等，必要时可以切断公共互联网网络。急时快速掌控：在发生大规模网络攻击事件时，能够在最短时间内控制事件的扩散，掌握事件的发展动态，准确判断事件的影响范围，制定应急响应措施，将损失降低到最小。平时侧重服务：应急响应的平时工作是保障互联网的安全运行，及时应对一般性网络安全事件。

（二）在应急处理中开展体系化对抗

从法制、机制、人员、资金、技术等多个层面建立立体对抗体系，用国家机器去完成网络应急。应急的目标不局限于把境外有害言论的源头挖出来，而是震慑一大批有企图的人，从而达到降低宏观指数的目的。

（三）明确危害网络信息安全的责任和义务

现实空间的每个主体都具有各自的权利与义务，同样，网络空间也如此，每个主体都为维护所处空间的正常运行而努力。每个网络主体有权要求国家提供一个正常、安全的网域空间，同时也有义务来维护其安全。

表 1　四大应急体系差异分析

应急体系	通报机制	事故性质	指挥体系
公共卫生应急	1. 通报内容：事件波及范围，防护措施等 2. 通报对象：各级政府部门，医疗机构和个人	范围一般较广，需要全国动员，容易引起恐慌	从国家到省级到地方都有应急指挥平台
消防应急	1. 通报内容 : 事件波及范围，事件造成的损失等 2. 通报对象：全社会	一般波及范围小，局部事件种类众多	只有省级地方级应急指挥平台
电力应急	1. 通报内容：事件波及范围，故障排除需要的时间等 2. 通报对象：各级政府部门和个人	波及范围较大，主要造成经济损失	1. 建成预防预测和监控预警系统 2. 应急信息指挥系统
核安全应急	1. 通报内容：事件波及范围，造成的损失，影响的范围等 2. 通报对象：各级政府部门，医疗机构和个人	波及范围小，但是影响时间长，对环境、公共健康造成危害	1. 建立国家核应急指挥中心 2. 核电所在省、地区、核电厂都建立有应急指挥中心

在网络信息安全立法中，必须对危害国家和公共网络安全的行为明确法律责任，为追究违法者创造法律条件。一是对于违法行为，应当相应地规定其民事责任、行政责任和刑事责任，明确各自的责任界限；二是要解决好民事责任、行政责任和刑事责任之间的衔接问题，对于尚不构成犯罪的违法行为，应当依法承担民事责任或行政责任；三是建立移送制度，对于危害性较大且已经构成犯罪的行为，应依法移送司法机关追究刑事责任，避免“以罚代刑”；四是所有网络运营商都有维护用户信息安全的义务，这些义务主体在未履行保护网络信息安全义务时，应当承担相应的法律责任。

（四）完备网络安全组织体制，强化应急救援体系

建议成立专门机构，作为中央政府应对特别重大突发公共事件的应急指挥机构，统一指导、协调和督促网络基础设施应急、公共基础设施信息系统应急、网络内容管理应急等网络安全应急工作，建立不同网络、系统、部门之间应急处理的联动机制，对分散在各部门的网络安全应急管理职能适当加以整合。

（五）机制上落实应急处理主体的行政执行能力和执法权

第一，强制要求网站拥有者配备安全人员、安全设备。安全人员如首席安全官（CFO）等需具备相关资历，在相关安全应急培训组织进行过专业培训，并可提供其能力的官方证明材料。

第二，将“gov”和“edu”等国字头网站做统一托管，将流量数据大集中，便于进行安全检测。

（六）将事后应急向事前和事中应急转变

第一，平时发出探针，发现异常就针对关键目标监控，对来源 IP 分析，通过运营商查询通联日志，有针对性地搭建蜜罐，当攻击者攻击蜜罐时，不仅可以记录下详细的攻击过程，还有希望伺机利用漏洞来反制。

第二，不仅是网络设备，QQ、淘宝、乌云等常用应用要进行监测，收集数据，尽可能地发现非正常现象，从中找出攻击者的某些可识别信息、资金链等，并及时将信息共享。

（七）定期开展国家级网络安全应急演练

互联网是一个高度军民融合的环境，一方面要坚持军民共建共享，另一方面要统筹平战需求。为了实现“战时协助攻防，平时侧重服务，急时快速掌控”的目标，需要加强应急演练，保证网络空间安全体系处于应急态时可以高效运转，形成科学有效、反应迅速的应急工作机制，保障重要信息系统的稳定运行。需要成立国家级和省市级的网络安全应急演练工作组，制定网络安全的规章制度；组织安全排查，及时消除网络安全隐患；组织制定并实施各级网络安全事故应急预案，能够及时、准确地报告网络安全事故。

五、结语

本文详细介绍了在互联网大背景下网络安全形势的严峻性与应急响应工作的重要性，分析了威胁的主要来源与其攻击方式所呈现的特点，总结了当前网络应急工作的管理现状与存在的问题，并列举了所要采取的措施。与以往的网络威胁相比，当前网络攻击方法正不断推陈出新，应急响应工作更应随时做出调整与完善，以应对各种威胁。

参考文献

[1] 国家计算机网络应急技术处理协调中心. 西门子宣布修复被 Stuxnet 蠕虫利用的漏洞[EB/OL]. (2012-07-25) [2016-10-08]. http://www.cert.org.cn/publish/main/98/2012/20120725152801904458081/20120725152801904458081_.html.
National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). Siemens announced to repair the vulnerability utilized by Stuxnet [EB/OL]. (2012-07-25) [2016-10-08]. http://www.cert.org.cn/publish/main/98/2012/20120725152801904458081/20120725152801904458081_.html.

[2] 国家计算机网络应急技术处理协调中心. 2015 年中国互联网网络安全报告[R]. 北京: 邮电出版社, 2016.
National Computer Network Emergency Response Technical Team/Coordination Center of China. China Internet network security report of 2015 [R]. Beijing: Posts & Telecom Press, 2016.

[3] 储殷. 中国“一带一路”战略定位的三个问题[J]. 国际经济评论,2015(2):12–13.
Chu Y. Three issues on the strategic orientation of China “One Belt One Road”[J]. International Economic Review, 2015(2):12–13.

[4] 新华通讯社. 习近平在网络安全和信息化工作座谈会上的讲话[J]. 中国信息安全,2016(5):2–9.
Xinhua News Agency. Speech by Xi Jinping at the symposium on network security and information work [J]. China Information Security, 2016(5):2–9.

[5] 国家计算机网络应急技术处理协调中心. 关于使用非苹果官方XCODE 存在植入恶意代码情况的预警通报[EB/OL]. [EB/OL]. (2015-09-30) [2016-10-08]. http://www.cert.org.cn/publish/main/12/2015/20150914152821158428128/20150914152821158428128_.html.
National Computer Network Emergency Response Technical Team/Coordination Center of China. Alert about unofficial apple XCODE contain malicious code [EB/OL]. (2015-09-30) [2016-10-08]. http://www.cert.org.cn/publish/main/12/2015/20150914152821158428128/20150914152821158428128_.html.

[6] Antiy CERT. 非官方版本恶意代码污染事件(XcodeGhost) 的分析与综述[EB/OL]. (2015-09-30) [2016-10-08]. http://www.antiy.com/response/xcodeghost.html.
Computer Emergency Response Team of Antiy. Analysis and review of Xcode unofficial supply chain pollution incident (XcodeGhost) [EB/OL]. (2015-09-30) [2016-10-08]. http://www.antiy.com/response/xcodeghost.html.

[7] 袁春阳, 杜跃进, 周威, 等. 美国政府国家网络应急响应计划及其借鉴意义[J]. 保密科学技术,2012(5):35–37.
Yuan C Y, Du Y J, Zhou W, et al. US national network emergency response plan and its reference significance [J]. Secrecy Science and Technology, 2012(5): 35–37.

[8] 刘玉龙. 我国网络与信息安全应急响应体系建设[J]. 能源技术与管理,2012,3(3):164–165.
Liu Y L. Network and information security emergency response system construction of China [J]. Energy Technology and Management, 2012,3(3):164–165.

[9] 网络安全课题组. 中国网络安全应急体系的问题与对策[J]. 电子政务,2014,139(7):20–25.
Research Group of Network Security. Problems and solutions of network and information security emergency response system of China [J]. E-Government, 2014,139(7):20–25.

[10] 解旭红. 基于网络空间的应急动员信息管理能力建设管见[J]. 国防科技,2015,36(1):55–57.
Xie X H. Construction of emergency mobilization information management capabilities based on cyberspace [J]. National Defense Science & Technology, 2015,36(1):55–57.