



网络安全新威胁下我国面临的安全挑战和对策建议^{*}

马明杰¹, 孙奉刚¹, 翟立东¹, 杜跃进^{1,2,3}

(1. 中国科学院信息工程研究所 北京 100093;

2. 国家网络信息安全技术研究所 北京 100029;

3. 国家计算机网络应急技术处理协调中心 北京 100029)

摘要:随着互联网以及周边网络产品的发展,信息安全越来越受到重视,“棱镜门”事件爆发后,国家级信息安全不仅引起了全球领导人的重视,更引起了全世界人民的广泛关注。分析了在网络安全新威胁下我国面临的安全挑战,并针对我国在信息安全领域存在的问题提出未来网络发展的对策建议。

关键词:高级持续性威胁;安全事件;安全挑战;对策建议

doi: 10.3969/j.issn.1000-0801.2014.07.002

Security Challenges Facing Our Country and Countermeasure Recommendations Under New Network Security Threats

Ma Mingjie¹, Sun Fenggang¹, Zhai Lidong¹, Du Yuejin^{1,2,3}

(1. Institute of Information Engineering, CAS, Beijing 100093, China;

2. National Institute of Information Security Technology, Beijing 100029, China;

3. CNCERT/CC, Beijing 100029, China)

Abstract: With the development of the internet and peripheral network products, information security draw more and more attention, after the outbreak of the prism, the national information security is not only caused the attention of world leaders, has attracted wide attention from people around the world. The security challenges in the new network security threats which our country was facing were analyzed and recommendations for future network development in China in the field of information security were put forward.

Key words: advanced persistent threat, security issue, security challenge, countermeasure recommendation

1 网络安全新威胁下的安全事件

信息化高速发展的同时也给个人、企业以及国家带来了信息安全风险。近年来,频发的安全事件越来越引起人们对信息安全的重视。为能更好地认清网络安全新威胁,先看几个典型的网络安全事件。

极光行动(Operation Aurora)是一个典型的国家级信

息安全对抗的案例。2010年,Google的一名雇员因点击了一条恶意链接,导致Google网络被渗透数月、各种系统的数据被窃取。在该事件中,遭受攻击的除了Google外,还有20多家公司,其中包括Adobe Systems、Juniper Networks、Rackspace、雅虎、赛门铁克、诺斯洛普·格鲁门和陶氏化工等。赛门铁克分析此次行动攻击目标包括机构组织和制造业供应链,最主要目标是国防承包商。极光行动

^{*} 国家高技术研究发展计划(“863”计划)基金资助项目(No.2011AA01A103)

利用 Oday 漏洞,通过钓鱼邮件和网站漏洞传播恶意程序。具体攻击流程如图 1 所示。

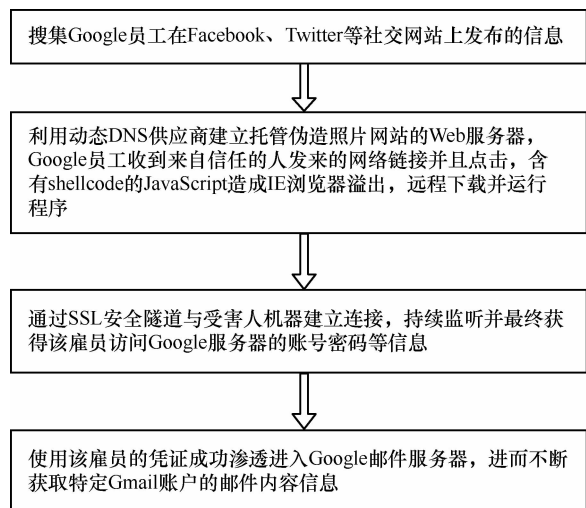


图1 极光行动攻击过程

2010年9月,“震网”蠕虫病毒攻击了伊朗的工业基础设施,病毒渗透进微软“视窗”操作系统,对其进行重新编程,从而造成系统破坏。该病毒结构非常复杂,其传播方式如图2所示。

2011年9月22日,Lurid攻击被TrendMicro的研究人员公布。这是一起针对前独联体国家、印度、越南和中国等国家的重要部门,例如政府部门、外交部门、航天部门,还有科研机构的APT(advanced persistent threat,高级可持续威胁)事件。攻击者主要利用了被压缩成.rar文件的带有恶意代码的屏幕保护程序以及 CVE-2009-4324 和 CVE-2010-2883 这两个已知的 Adobe Reader 漏洞。用户一旦打

开恶意屏幕保护程序或阅读恶意 PDF 文件,其电脑就会被植入木马。木马程序会为了在受害电脑中保持存在而采取不同的方法。木马程序与 C&C 服务器进行通信,通常将收集的信息通过 HTTP post 上传给 C&C 服务器。攻击者借助 C&C 服务器对木马下达各种指令,不断收集受害企业、部门的敏感信息。

上述的安全事件发生时,被害企业或者国家很长时间都没有察觉到其受到攻击。很多病毒在其潜伏工作几年后才被发现,给受害企业或国家造成了很大的损失。

2 浅析网络安全事件

分析这几个典型网络安全事件的背景、攻击手段、影响等因素,不难看出,现在所处的网络空间安全环境是国际对抗环境,新威胁呈现 APT 的特征,即持续、高级、隐蔽等。分析每个安全事件,抽离其共性可发现,安全事件主要包括 3 方面要素:主体、方法和客体。

主体,是指主动发起攻击的人、企业或国家,是攻击的源头。现如今网络空间存在 4 类不同动机的攻击者:一是随意选择攻击目标,可能造成严重危害的“白开心”者;二是主要以经济利益为目的的“淘黑金”者;三是通过互联网窃取各类信息的“纯小偷”;四是从国家博弈角度选择目标,具备国家意志,包含政治动机的“大玩家”。“大玩家”的登场,是造成今天网络安全演变成国家间安全对抗新形势的主要原因。

客体,是指攻击目标。在国际对抗环境下,主体选择的目标一般具有高价值或高信息量,如重要信息系统、金融

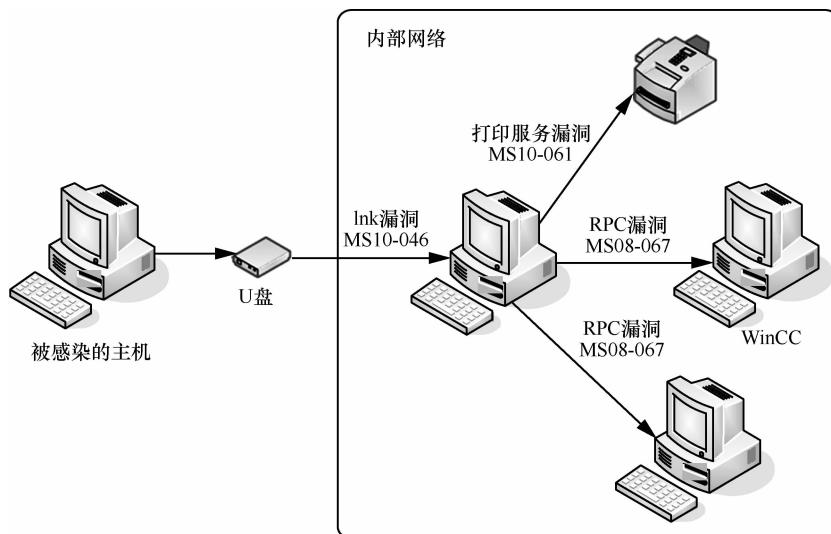


图2 “震网”病毒传播方式



产业、能源系统、政府和涉密信息系统、军事、高科技企业、工业控制系统等。这些目标一旦被攻击就会产生不可估量的损失甚至能引起世界级的恐慌。

方法,是指发动攻击事件所采取的手段。手段主要利用了客体的脆弱性,包括技术脆弱性和运营管理脆弱性两方面。技术脆弱性反映的是系统存在的后门程序或漏洞,包括系统网络结构、系统软件、数据库软件、应用中间件和应用系统几个方面。系统的技术漏洞还包括异常行为,异常行为是安全威胁的一个方面。狭义的异常行为包括病毒、木马、蠕虫和僵尸网络等;广义的异常行为包括异常操作、异常地址、异常时间和异常群体等。必须找到相应的手段来发现这些异常行为,才能避免安全威胁的发生。运行管理脆弱性主要是由于组织结构管理或人员配置上的不合理安排造成的安全隐患。网络的运行管理存在的隐患,例如身份盗用、责任分配不清晰、疏于防范、安全人员安全意识薄弱等都可能给攻击者以可乘之机。

进一步分析国家间安全事件过程,可概括为5个阶段,分别为定、接、攻、潜、行,如图3所示。

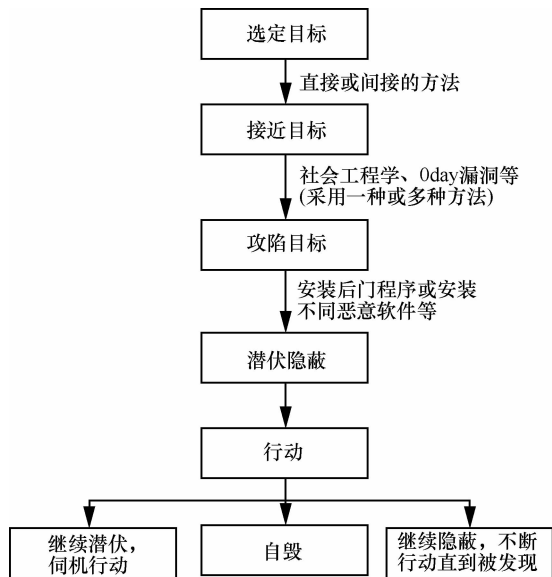


图3 新威胁下的安全事件过程

具体分析如下。

(1)定

即选定目标。攻击者首先选定要攻击的目标,即客体。国家间信息对抗一般从国家博弈的角度出发,包含有政治动机、经济动机等因素。

(2)接

即接近目标。攻击者会采取直接或者间接的方法接近目标。直接的方法为直接接近目标;若攻击的目标防御较严密,不易从正面攻击,攻击者则会采用间接的方法,采用曲线方式接近目标,例如选择合适的跳板,通过跳板接近目标且跳板有可能不只一个,有可能有多个。

(3)攻

即攻陷目标。该目标可以包括阶段目标以及最终目标,阶段目标即跳板。攻陷目标的方法可能包含了社会工程学、0day漏洞等。比如利用目标虚荣等缺点,发送一些中奖、免费赠送商品的邮件或者网址,或者发送带有恶意链接的电子邮件或者虚假的Web站点诈骗;或者通过一定的手段给目标制造网络或计算机的问题等,骗取用户的信任;利用常用软件的安全漏洞;利用后门程序等。有的攻击只采用了其中一种手段就可以达到目的,有的为达到目的采用了几种手段的组合。

(4)潜

即潜伏隐蔽。攻击者为确保能在外部网络的环境中对主要系统进行持续控制,常在目标的网络环境中安装新的后门程序或者在多台计算机上安装不同的恶意软件,有的攻击者采用建立不涉及后门程序的网络访问方法,例如使用有效PKI或VPN证书,允许入侵者伪装成一个合法用户进入企业网络和内部资源等,这样即使网络安全人员发现并删除他们的恶意软件,也能使他们保持存在。在某些情况下,APT攻击者可以绕过身份验证以保持对受害网络和它的资源的访问。潜伏的周期不定,有的可能几年或者几十年才会进入下一阶段,有的可能不经历潜伏阶段直接进入下一阶段。

(5)行

即行动。行动不仅仅包括窃密还包括破坏,若国家级安全对抗中行动的目的为破坏,一般会给受害者造成巨大的损失,比较著名的例子就是“震网”攻击,“震网”病毒可能感染并破坏了伊朗的核设施,并最终导致伊朗的布什尔核电站推迟启动。但一般的APT旨在窃取机密。APT攻击者一旦发现感兴趣的文件,就会将其打包成归档文件并传送。

行动后攻击程序的动态也不一样。例如行动后有的攻击程序继续隐蔽自己,只要没被发现便会伺机再行动;有的攻击程序行动后会自毁以保证其他攻击程序的正常运行。有的攻击程序在隐蔽自己的同时会不断地行动直到被发现。

3 我国面临的网络安全挑战

在国际网络安全对抗新形势下,在新威胁不断出现的情况下,我国信息安全保障体系尚不能完美地抵御所有攻击。我国管理体系还有待完善,管理部门职能定位有待细化;信息安全专业人才缺乏,复合型人才缺乏更甚,人员安全意识薄弱;国家网络基础设施主要依靠进口,自主创新能力有限,防范手段单一等现状,都使国家易遭受技术遏制与威胁。综上所述,我国存在的网络安全问题可以总结为3方面要素:管理、技术、人员。

(1)管理方面

管理方面的问题主要体现在以下两个方面。

- 机制体制方面。国家信息化高速发展,我国信息安全在政策立法、规章制度制定方面明显落后,显得力不从心。现如今攻击事件频繁发生,采用的攻击手段花样繁多,现有法律还不能完全概括所有信息安全问题,导致一些安全事件无法定性量刑。
- 组织结构方面。国家在设置组织机构上主要存在责任不明确、缺乏权威的立法机构等问题。责任不明确不仅会浪费人才而且容易出现争权或相互推卸责任的现象。缺乏权威的立法机构会导致立法缓慢。

(2)技术方面

技术方面存在的问题主要表现在以下3个方面。

- 威胁分析能力不足。威胁分析评估能够在事件发生前保障整个信息网络安全,是非常重要的预见性工作,可以很大程度上减少安全事件的发生。只有了解、分析、评估可能面临的威胁和被保护资源的价值,才能确定信息系统的安全保护等级,才能有效地配置有关技术、管理、人员等资源去实施科学合理的保护。我国在这方面还有待完善。
- 面对复杂威胁,应急响应能力不足。应急响应能力主要针对已经发生的网络安全事件,重视效率与速度。国家级应急预案以及应急机制与其他信息安全技术先进国家相比还有待改善与提高。
- 核心技术能力不足。国家针对信息安全的研究起步较晚,软硬件技术基础较为薄弱,采用的网络硬件设备和操作防护软件大多源于国外。在信息技术的软硬件领域均缺乏核心技术,关键性技术大多依赖于外国引进,对整体信息安全构成了重大威胁。

(3)人员方面

人员方面存在的问题主要表现在以下两方面。

- 复合型人才奇缺。目前国家在培养人才方面,虽然已经取得了一定成绩,给各行各业输送了大量的专业型人才,但是复合型人才的输送比较少,造成部分单位虽然想保障单位信息安全,但是无从下手的局面。
- 人员信息安全意识薄弱。由于安全宣传、教育或培训不到位或本身信息安全意识薄弱等原因,信息安全人员难以满足安全管理的要求。人员安全意识因素往往是最容易出现问题但又最容易被忽视的环节。

4 未来网络发展对策建议

针对国家新形势下存在的问题和所面临的威胁和挑战,国家应该从宏观层面完善政策法规建设、协调组织结构、大力培养安全人才、强化国家级核心能力研究与建设。

(1)进一步加强和完善法规建设

完善的法律法规是保障信息化高速健康发展的重要前提。国家政府部门应参考国际先进国家的法律法规,结合我国实际,加强和完善具有中国特色的法规建设。

(2)成立国家网络安全风险和威胁分析工作组,提升威胁分析能力

通过对威胁的分析,可得到国家网络情况的整体威胁分析量表,对所有系统面临的威胁进行一个综合的评判,依此进行下一步的工作。该量表可以从攻击难度和造成的破坏性两个方面加以考虑,进而将系统分为以下4类:

- 破坏性大且攻击难度小;
- 破坏性大且攻击难度大;
- 破坏性小且攻击难度小;
- 破坏性小且攻击难度大。

这4类系统需要受到的关注依次递减。

(3)成立信息安全人才培训中心

建立过程可分前提准备、中期试点、后期完善3个阶段。培训中心的职责不仅包括分领域地针对不同层次的从业人员进行培训,还包括对他们的能力进行评估。这种评估,与学校中的考试不同,更多的是对培训者具体行业的从业能力进行打分。

(4)强化国家级核心能力研究与建设

鼓励走自主创新道路,增强国家核心能力,并以之带



动人才培养、研究实验、产业发展、服务水平,全面提高国家网络安全水平建设和防护水平。

(5)建立网络信息安全应急演练机制

为提高国家应急处置能力,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,需成立国家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;组织制定并实施关系国计民生单位的网络安全事故应急预案;总负责国家应急指挥工作,及时、准确地报告网络安全事故。

(6)建立主要安全产品和信息系统抗攻击的演练测试环境,组织社会力量检验国家网络安全能力

例如针对微软公司的 Windows XP 系统停服现状,为了解 Windows XP 用户安全情况,可将 Windows XP 系统环境作为演练测试环境的一部分,通过组织相关安全竞赛,组织参赛者挑战 Windows XP 平台上的安全产品,通过实践来检验国家具体网络安全能力以及网络安全人员的水平,为未来的网络安全技术决策提供基础。

5 结束语

互联网不断发展,网络安全新威胁层出不穷,其手段也在不断更新变化,这对完美有效地保障个人、企业、国家的信息安全提出了严峻的考验。在国家对抗的新形势下,具有影响力的安全事件一般涉及的是对国家有高价值、高数据量、对国家发展有着重要影响的企业、部门,一般出于政治、经济等目的,采用高科技手段、社会工程学或者 0day 漏洞等进行攻击,一旦攻击成功,后果将不堪设想。因此要切实有效地保障国家信息安全,需要深刻认知我国网络安全存在的问题,发展适合我国信息安全发展的技术且找寻合适的对策。

参考文献

- 1 王柏松.中国新安全观及其安全战略选择研究.东北师范大学博士学位论文,2013
- 2 Baize E. Developing secure products in the age of advanced persistent threats. IEEE Security & Privacy, 2012, 10(3):88~92
- 3 Virvilis N, Gritzalis D, Apostolopoulos T. Trusted computing vs advanced persistent threats: can a defender win this game. Proceedings of 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing, Autonomic and Trusted Computing (UIC/ATC), Vietri Sul Mare, 2013: 396~403
- 4 Li F, Lai A, Ddl D. Evidence of advanced persistent threat: a

case study of malware for political espionage. Proceedings of the 6th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, 2011: 102~109

- 5 Mustafa T. Malicious data leak prevention and purposeful evasion attacks: an approach to advanced persistent threat (APT) management. Proceedings of 2013 Saudi International Electronics, Communications and Photonics Conference (SIEPCPC), Riyadh, 2013:1~5
- 6 Symantec Security Response. The Elderwood Project (Infographic). <http://www.symantec.com/connect/blogs/elderwood-project-infographic>
- 7 杜跃进. 国际对抗环境下的网络安全防护能力建设. 信息网络与安全, 2013(3):86~88
- 8 杜跃进. 陌生的危机: 我国的网络安全形势. 中国金融电脑, 2014(1):32~35
- 9 Symantec Security Response. The Elderwood Project (Infographic). <http://www.symantec.com/connect/blogs/elderwood-project-infographic>, 2014
- 10 吴正龙.“震网”的警示. 解放日报, 2011-02-10
- 11 启明星辰. 八大典型 APT 攻击过程详解. http://netsecurity.51cto.com/art/201308/408470_7.htm, 2013
- 12 安天实验室, 安全研究与应急处理中心. 对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告, 2010
- 13 让我们一起来案例分析 第五期 (极光行动). <http://bbs.51cto.com/thread-1062449-1.html>, 2014

[作者简介]



马明杰,女,现就职于中国科学院信息工程研究所,主要研究方向为工业控制系统信息安全。

孙奉刚,男,现就职于中国科学院信息工程研究所,主要研究方向为移动互联网。

翟立东,男,博士,中国科学院信息工程研究所副研究员,主要研究方向为移动互联网。

杜跃进,男,博士,国家网络信息安全技术研究所教授、网络安全应急技术国家工程实验室主任、国家网络信息安全技术研究所所长、国家计算机网络应急技术处理协调中心(CNCERT/CC)副总工程师,主要研究方向为基础网络、移动智能终端。

(收稿日期:2014-06-22)