广西科学院学报
Journal of Guangxi Academy of Sciences

2012,28(1):38~40
Vol. 28, No. 1 February 2012

基于"震网"病毒的物理隔离网络的风险控制措施
Risk Control Analysis of the Physical Isolated Network Based on the Stuxnet

饶跃东,熊 瑜
RAO Yue-dong, XIONG Yu

(桂林空军学院,广西桂林 541003)
(Guilin Airforce Academy, Guilin, Guangxi, 541003, China)

摘要:阐述"震网"病毒对物理隔离网络带来的安全威胁,并从内网终端的安全防护、准入控制、内网安全应急响应、安全防护理念以及自主可控技术创新等五个方面探讨物理隔离网络的风险控制措施。

关键词:病毒 震网病毒 物理隔离 风险控制
中图法分类号:TP309.5 **文献标识码**:A **文章编号**:1005-9164(2012)01-0038-03

Abstract: This paper analyzes the security threats of the Stuxnet for physical isolated network. The risk control measures of the physical isolated network are stated including the intranet terminal protection, access control, intranet security emergency response, security protection ideas and independent controllable technology innovation.

Key words: virus, Stuxnet, physical isolated, risk control

"震网"病毒,英文名称"Stuxnet",是世界上首个针对工业控制系统编写的破坏性蠕虫病毒,它利用微软操作系统中至少4个漏洞,其中有3个全新的零日漏洞,伪造驱动程序的数字签名;利用西门子SIMATIC WinCC系统的多个漏洞,特别是针对西门子公司的监控与数据采集系统(SCADA)进行攻击。一旦运行该系统的服务器感染了"震网"病毒,工业控制指令和数据等信息就可能被病毒拦截,窃取和修改[1]。"震网"病毒的主要攻击途径:一是通过U盘利用Windows Shell中的远程代码执行漏洞(MS10-046)攻击;二是通过局域网或者利用打印机后台服务中的远程代码执行漏洞(MS10-061),或者利Windows服务器中的远程代码执行漏洞(MS08-067)向计算机发送恶意RPC请求,一旦攻击成功,即可完全控制被攻击计算机,进行感染,从而进行破坏系统运行、甚至控制系统运行等攻击。

"震网"病毒除了具有极强的攻击力和破坏力外,还具有病毒结构复杂、攻击目标明确等特点。从病毒传播的情况来看,其攻击目标主要集中在工业专用计算机系统。由于这类系统自身的特殊性和重要性,往往是与互联网物理隔离,独立于外部网络而自成体系运行的。"震网"病毒攻击工业专用计算机系统,造成隔离网络内部计算机无法及时获得最新的操作系统补丁,防病毒软件也可能无法及时升级更新,给病毒带来可乘之机。"震网"病毒给物理隔离网络安全带来了新的启示。本文从风险控制角度,就五个方面探讨物理隔离网络的安全防护措施。

1 加强内网终端的安全防护

物理隔离网络的终端安全往往被忽视。很多用户认为自己处于隔离网络的"内部",对外有整体网络的区域防护就已经很安全了。但是我们知道,根据木桶原理的短板效应,网络的安全性是取决于其最弱环节,终端的每一台主机都有可能成为病毒攻击的入口,因此必须强化终端的安全防护。

内网终端的安全防护可以采用的措施主要包括:在终端设备上开启防火墙功能;及时安装操作系统和各种应用程序的最新补丁;安装杀毒软件,开启

收稿日期:2011-12-19
作者简介:饶跃东(1981-),男,讲师,主要从事计算机网络安全和智能算法研究。

实时监控功能,并及时更新病毒库升级到最新版本;关闭默认共享,阻止病毒在局域网中传播;使用强口令,以保护系统免受攻击;关闭主机中不必要的网络服务端口;关闭计算机的自动播放功能,使用可移动设备前先进行病毒扫描,使用专用的 U 盘病毒查杀工具等等。

2 建立完善的内网终端准入控制

在加强内网终端自身安全防护的同时,对于外来终端进入内网的准入控制,也是构建一个安全网络,有效控制安全风险的关键[2]。终端准入控制是一个系统工程,它具有统一目标和统一策略,能够有效控制、监视和跟踪分散的内网终端。从功能上,可以将终端准入控制分为 6 个方面:(1)准入认证。通过准入认证,形成有效的权限控制机制,完成用户名与 IP、MAC、VLAN、接入端口、接入设备 IP、SSID 等多元素绑定。目前常见认证协议包括 802.1X 协议、Web 认证、PPPoE 协议等。(2)安全评估。终端安全控制评估主要包括对终端系统补丁管理、防病毒软件检查、注册表监控、异常流量和连接数监控等方面。(3)权限控制。主要包括对不同角色、不同用户的权限策略控制,对移动存储介质以及其它外设的安全策略控制。(4)行为审计。主要是对用户网络访问行为的审计和移动硬盘、打印机等其它外设使用行为的监控和审计,帮助管理员追踪定位非法用户。(5)协助管理。包括用户进入内网需安装的客户端软件部署和安装方式,以及客户端定制、软件分发、用户拓扑管理等功能。(6)可扩展性。应考虑到实现终端准入控制的可用性和扩展性,例如实行两机冷、热备份,用户分权管理、服务分级管理等。

3 提高内网安全应急响应能力

物理隔离使得内部网络遭受攻击的风险大大降低,也正因如此,容易使管理人员疏忽大意,一旦有攻击发生便手忙脚乱。因此,应大力加强内网安全应急响应体系建设,提高应急响应处理能力。目前,内网建设仍然存在不少安全问题,如:用户安全意识欠缺,安全管理过程不完善,缺乏科学规范的应急预案等等。建设合理的内网安全应急响应体系,一方面能够对内网进行全局范围内的监控,降低网络被侵害的风险,可以通过以入侵检测为核心,联合防火墙、漏洞扫描、违规外联监控等其它安全产品进行入侵管理,对发生的安全事件进行应急响应,建立整个系统"一体化"的安全预警与响应体系;另一方面能够及时发现安全事件,快速定位安全问题,充分利用各种网络安全设备,以最快的速度响应和处理突发的安全事件。

提高应急响应处理能力的关键是加强内网安全自身的软硬件建设,在处理各种突发事件时,管理人员能够及时采取行动和措施,阻止和减小事件带来的影响。(1)做到事前有准备。在突发事件发生前做好准备,比如在管理上进行风险评估、制订安全策略和应急预案、开展安全培训、安全通告进行预警等;在技术上则要增加系统安全性,如合理备份数据、安装防火墙、入侵检测工具等。(2)做到事后能处理。在突发事件发生后能及时采取抑制、清除和恢复等措施,把事件造成的损失降到最小且尽快恢复正常运行。这些行动措施部分来自于人,部分来自于系统,比如系统备份、病毒检测、后门检测、病毒清除、隔离限制或关闭服务器、系统恢复、反击追踪、调查总结等一系列操作。

4 提升内网信息安全防护理念

物理隔离网络的直接目的是防止外网的攻击和威胁,最大限度地保护内部网络安全。但是内网安全不仅仅只是来自于外部,内部攻击、非法外联、"摆渡"攻击等等,都在不断威胁着物理隔离的内网安全。"震网"病毒的出现,再一次突破了物理隔离的屏障,给位于内部网络的各种工业控制系统带来灾难性破坏。因此,加强物理隔离网络的风险控制,必须从安全防护理念上抓起。(1)强化安全意识,严禁非法操作。"震网"的主要传播方式是通过 U 盘等移动存储设备进入网络内部,因此,必须加强内部人员安全意识,规范操作流程,严禁非法外联、一机跨两网等违规操作,严格控制移动存储介质在内网和外网之间交叉使用。同时建立完善内网安全管理制度,深入开展信息安全人员专业技术培训,防止网络安全事件反复发生,从源头上杜绝安全威胁。(2)转变防护观念,加强技术研究。初级的安全防护是被动的,总是在威胁来临之后。应积极转变防护观念,在建立可信网络连接,构建可信系统并提供可信服务的基础上,从被动防御为主转向到主动防范为主,从以脆弱性分析为主转变为以真实性判别为主。同时要紧贴信息技术发展趋势,不断加强创新技术研究,例如数字签名、密钥交换、无线移动网络等等,为内网安全防护提供可靠的技术保障。

5 加强自主可控技术创新

信息技术自主可控是建立可信体系,实现网络

安全的关键。物理隔离网络信息安全不仅是网络边界安全，更重要的是隔离网络内部软硬件信息安全。目前我国包括水利、交通、钢铁等部分大型项目和工程都采用的是国外品牌的自动化软件，一旦“震网”病毒突破物理隔离网络屏障进入内部，就有可能因为没有掌握核心技术而无法及时排除故障，从而带来巨大的损失。因此，必须加大信息安全领域软硬件技术和产品的自主研发力度，加强自主可控技术创新。特别是对关系到国计民生和国家安全的重大项目，能自主的就要尽可能实现技术自主；以目前技术还无法实现完全自主的，也必须要保证它可知可控[3]。

6 结束语

“震网”的出现，改变了人们对传统计算机病毒的认识和看法，给原本认为“很安全”的物理隔离网络敲响了警钟，使人们意识到，物理隔离网络并非牢不可破，必须在加强网络安全软硬件建设的同时，采取防护控制措施，有效控制风险，变被动为主动，才能使网络遭受攻击的风险和损失降到最低，信息安全才能得到更加可靠的保障。

参考文献：

[1] 严霄凤.“震网”引发网络安全新思考[J].信息安全与技术，2011(2)：17-19.

[2] 王春莲.内网网络安全解决方案研究[J].硅谷，2011(4)：59-59.

[3] 陈梁.“震网”病毒敲响自动化系统安全警钟[J].自动化技术与应用，2010(10)：138-138.

（责任编辑：邓大玉）

（上接第37页）

表2 视频文件加解密所需时间

序号	文件名	加密时间(ms)	解密时间(ms)
1	1m.flv	72.00	75.00
2	2m.avi	142.20	159.30
3	29m.avi	1701.50	1767.20
4	100m.mp4	4790.60	5229.70
5	156m.rmvb	7304.70	9584.40
6	302m.mp4	15667.20	24326.50
7	471m.rmvb	23543.60	33309.40
8	893m.rmvb	46806.10	66042.30
9	1300m.AVI	98932.00	100328.00

表3 加密解密对文件占用存储空间大小和损失率的影响

序号	文件名	加密文件平均大小	解密文件平均大小	平均膨胀率(%)	平均损失率(%)
1	1m.flv	1085263.80	1035623	4.793	0
2	2m.avi	2346039.30	2238362	4.811	0
3	29m.avi	31606300.70	30116286	4.948	0
4	100m.mp4	107805147.00	102677258	4.994	0
5	156m.rmvb	167657337.20	159724405	4.967	0
6	302m.mp4	324986231.90	309518868	4.997	0
7	471m.rmvb	507222659.30	483064211	5.001	0
8	893m.rmvb	960637114.70	914884087	5.001	0
9	1300m.AVI	1471983714.33	1401879740	5.001	0

表3的实验结果表明，医学视频文件经过加密之后文件的膨胀率在5%左右，解密之后不影响视频文件的使用，文件在加解密过程中没有损失，系统能够满足实际应用的需求。说明我们提出的解决方法能够满足系统运行性能的要求，而且实现了Web环境下系统的安全认证。

参考文献：

[1] 彭和平，高德远，姜刚，等.计算机信息安全防拷贝系统研究与实现[J].微电子学与计算机，2005，22(8)：12-16.

[2] Kathleen Reavis Conner，Richard P Rumelt. Software piracy：an analysis of protection strategies[J]. Management Science，1991，37：125-139.

[3] 林路丝.在线授权认证平台的设计与实现[D].广州：华南理工大学，2010：1-62.

[4] 袁春，钟玉琢，贺玉文.基于混沌的视频流选择加密算法[J].计算机学报，2004，27(2)：257-263.

[5] 陈道敏，王正华，彭宇行，等.流媒体技术安全研究与实现[J].计算机工程，2005，31(6)：137-139.

[6] Qao L，Nahrstedtk. A new algorithm for MPEG video encryption[C]. In：Proceeding of the First International Conference on Imaging Science，Systems and Technology (CISST' 97)，Las Vegas，Nevada，1997：21-29.

（责任编辑：邓大玉）