高校网络安全事件应急处置策略研究

王海涛
（黑龙江林业职业技术学院信息工程学院，黑龙江 牡丹江 157011）

摘 要：本文对网络安全事件的类别进行了初步的分类，对总体处置策略进行了探讨，对病毒事件、木马事件、勒索病毒事件的处置策略进行了简要的分析。

关键词：木马；病毒；应急处置
【DOI】10.12231/j.issn.1000-8772.2021.02.312

1 引言

我国的高校正在成为信息安全泄露的高发区，据有关方面做了一个统计显示，从2014年的4月到2015年的3月份的一年的时间内，补天台上发现了多达3495个高校网站漏洞，统计有1088个高校网站，其中，高危漏洞2611个，占74.7%;中危漏洞691个，占19.8%;低危漏洞193个，占5.5%。这其中包含一些国内顶级名校。如何对网络安全事件进行响应、预防和处置，成为网络运营者的一项重要研究课题。

2 网络安全事件的分类

根据网络安全事件产生的原因，网络安全事件可分为以下几类：(1)恶意代码：木马、蠕虫、感染式病毒、僵尸网络等·WannaCry·劫持“驱动人生”的蠕虫挖矿病毒·LPK感染式病毒。(2)网络攻击：拒绝服务攻击、漏洞攻击、网络扫描窃听、网络钓鱼等。(3)信息破坏：篡改事件、信息假冒、信息泄露、信息窃取、信息丢失。(4)设备设施故障：软件自身故障、外围保障设施故障、人为破坏事故。(5)灾难破坏：水灾、台风、地震、雷击、火等。

3 网络安全事件的处置策略

(1)判定事件级别及是否需要上报：了解故障问题反应情况。(2)综合分析：分析安全设备流日志；分析应用系统监控日志；分析网络流量；分析终端状态；分析病毒服务器日志。(3)隔离受影响的业务系统：关闭网络接口。(4)隔离受影响的终端系统：开启终端防火墙；关闭上联接口。(5)隔离受影响的网络：关闭网络端口。(6)获取病毒特征码：特征码提取；特征码发送。(7)专杀工具开发：专杀工具下发。(8)处置方案制定：系统安全配置方案；网络安全配置。(9)病毒处置方案执行：病毒查杀；网络策略配置；安全策略配置。

4 网络安全事件的处置流程

4.1 计算机病毒事件、网页内嵌恶意代码事件处置

(1)对受感染业务系统进行镜像备份，以免后续处理过程中丢失重要数据；(2)防病毒厂商与网络管理员对文件系统、网络流量、注册表、系统进程、系统配置以及系统其他关键位置进行查看分析，初步评估病毒的危害；(3)对被感染重要业务系统服务器进行初步处理，杀死可疑进程，清理业务系统文件，初步评估业务系统损失情况；(4)防病毒厂商人员提取样本文件及特征码，通过网络发往厂商后台研发中心，研发制作完成并下发专杀工具或更新病毒库；(5)病毒库更新后，安全管理员在防病毒厂商协助下进行策略设置，使感染病毒终端自动更新病毒库并进行病毒查杀；(6)如自动查杀失败，到各被感染主机进行手工病毒查杀，查杀后重新开机观察5分钟，观察病毒文件是否存在、病毒进程是否存活；(7)分析病毒感染原因、传播路径，如果通过可移动介质传入则加强管理；(8)待检测终端运行正常后，应用管理员恢复业务应用。

4.2 蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件处置

(1)通过防火墙管理界面关闭对受感染业务系统的访问，并通过终端管理界面查找到运行异常的终端，电话通知责任人后，远程禁止该终端连接网络；(2) 通过网管软件关闭大范围受感染网段的上联端口；(3)对受感染业务系统进行镜像备份，以免后续处理过程中丢失重要数据；(4)对文件系统、网络流量、注册表、系统进程、系统配置以及系统其他关键位置进行查看分析，初步评估危害情况；(5)对被感染重要业务系统服务器进行初步处理，杀死可疑进程，清理业务系统文件，初步评估业务系统损失情况；(6) 防病毒厂商人员提取样本文件及特征码，通过网络发往厂商后台研发中心，研发制作完成并下发专杀工具或更新病毒库；(7)病毒库更新后，在防病毒厂商协助下进行策略设置，使感染病毒终端自动更新病毒库并进行病毒查杀，或者使用专杀工具清除；(8)如自动查杀失败，对感染主机进行手工清除查杀，查杀后重新开机观察5分钟，观察相应有害程序文件是否存在、可疑进程是否存活、可疑网络流量是否存在；(9)分析响应有害程序感染原因、传播路径，如果通过可移动介质传入则加强管理，如果是蠕虫、特洛伊木马等通过系统漏洞或应用漏洞传播则打好漏洞补丁；(10)待检测终端运行正常后，开通受感染系统端口及所关闭网络上联端口，恢复防火墙策略，恢复业务应用。

4.3 勒索软件事件的处置

(1)通过防火墙管理界面关闭对受感染业务系统的访问，并通过终端管理界面查找到运行异常的终端，电话通知责任人后，远程禁止该终端连接网络；(2) 通过网管软件关闭大范围受感染网段的上联端口；(3)对受感染业务系统进行镜像备份，以免勒索软件倒计时将所有文件删除；(4)防病毒厂商与网络管理员对文件系统、网络流量、注册表、系统进程、系统配置以及系统其他关键位置进行查看分析，初步评估被勒索软件加密的文件是否有备份和相应的损失；(5) 对被感染重要业务系统服务器进行初步处理，杀死可疑进程，清理业务系统文件，初步评估业务系统损失情况；(6) 防病毒厂商人员提取样本文件及特征码，通过网络发往厂商后台研发中心，研发制作完成并下发勒索软件专杀工具或更新病毒库；(7)使用专杀工具清除勒索软件；(8)分析勒索软件感染原因、传播路径，如果通过可移动介质传入则加强管理，如果是蠕虫通过系统漏洞或应用漏洞传播则打好漏洞补丁，补丁没有发布的，可以按照安全厂商的临时解决方案处理，例如封闭某传播用的端口；(9) 在相应勒索软件的解密办法未公布之前暂时不恢复被感染系统的网络且不重启系统，等待解密办法的发布。解密办法发布后，使用相应解密程序还原全部数据。

5 结束语

网络安全事件层出不穷，需要针对不同的事件制定不同的处置策略和风险预防策略，才能造就一片清朗的校园网络环境，为提高教学质量提供基础服务。

参考文献

[1]中华人民共和国网络安全法.2017.
[2]中央网信办.国家网络安全事件应急预案.2017.
[3]信息安全技术，信息系统安全等级保护，指南.GB-T22240-2012.

课题：本论文为黑龙江省教育厅2019年度高等职业教育教学改革研究项目《网络安全等级保护2.0制度下智慧校园网络安全防护措施与制度建设研究》(课题编号：SJGZZ2019030)阶段性成果。