

基于模糊层次分析的木马攻击效果评估技术研究

曾辰熙, 吴泉源, 李爱平, 江荣

(国防科学技术大学计算机学院, 湖南 长沙 410073)

摘要: 现有的网络攻击效果评估系统主要针对 DDoS 和蠕虫进行分析, 缺乏对木马病毒的针对性。少数针对木马的危害度测量系统的指标值由人工标注, 且都为定性值, 稍欠客观性和全面性。基于该现状, 从木马特性分析出发, 建立针对木马病毒的层次化指标体系, 设计指标值可定性也可定量, 可人工标注也可系统采集。提出基于模糊层次分析的评估模型对木马攻击效果进行评估。同时, 提出一种多对一的权重综合技术, 对多组权重进行了合理的综合。最后, 通过对比已有评估系统的评估结果, 验证了所提评估技术的合理性。

关键词: 木马; 攻击效果评估; 模糊层次分析; 指标权重

中图分类号: TN915.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00073

Research on FAHP based Trojan attack effect evaluation

ZENG Chen-xi, WU Quan-yuan, LI Ai-ping, JIANG Rong

(School of Computer Science, National University of Defense Technology, Changsha 410073, China)

Abstract: The particular characters of Trojan are not fully taken into consideration by existed network attack effect evaluation systems which mainly focus on DDoS and Warm. A few Trojan harm measurement systems is somewhat short for objectivity and completeness as the result of that its indicator values is confined to manually marked and qualitative values. Under the circumstances, the analysis of Trojan's features were started from, and a hierarchical index system which accepted both quantitative and qualitative values, and both manually marked and system collected values was built. Then, a FAHP based evaluation model was proposed to evaluate the Trojan attack effect. Meanwhile, a many-to-one method to ensemble multiple weight vectors was proposed. Finally, the rationality of proposed evaluation system was verified by comparison with others.

Key words: Trojan, attack effect evaluation, fuzzy analytic hierarchy process, indicator weight

1 引言

拥有强隐蔽性和目的性的木马病毒相较于其他恶意软件来说, 对用户的隐私和财富具有更大的威胁。在 2015 年 9 月爆发的 XcodeGhost 风波中, 有超过 4 000 款 App 程序受感染, 波及实时通信、金融服务等多个领域^[1]。

对木马攻击效果的准确评估为新木马的危害预判工作带来强有力的保障。新木马出现后, 研究者可对该木马进行攻击效果评估, 评定其危害程度。依据不同的危害程度, 采取成本有别的预防措施, 以期达到网络安全维护工作的效益最大化。同时, 基于评估结果的自省, 本文更深入地认识木马病毒的特征, 了解木马设计者的动机,

收稿日期: 2016-05-17; 修回日期: 2016-06-24。通信作者: 江荣, jiangrong@erangelab.com

基金项目: 国家重点研发计划网络空间安全专项基金资助项目 (No.2016YFB0800803, No.2016YFB0800804, No.2016YFB0800303)

Foundation Item: The National Key Research and Development Program of China (No.2016YFB0800803, No.2016YFB0800804, No.2016YFB0800303)

把握木马技术的发展脉络和趋势。

对木马攻击效果评估技术的研究主要分为 2 部分, 对评估指标体系的研究以及对评估模型的研究。

韩兰胜等^[2]提出针对计算机病毒的危害性度量模型, 从病毒的共性出发建立了指标体系, 但并不适合直接用于木马评估。李渊等^[3]提出针对木马危害性度量模型, 其从木马的传播能力、隐藏能力、攻击能力、顽固度等方面考虑建立指标体系, 该指标体系的指标取值皆为定性值, 且由人工标注, 因此稍欠客观性和全面性。

网络攻击效果评估与网络安全态势评估紧密相连, 攻击效果本身就是通过靶标系统的完备性、安全性等指标的变化来体现的, 故可以从网络安全态势评估模型的设计中提取相关理论来对网络攻击效果评估建模。张建锋等^[4]将评估方法依照其原理分为 3 大类: 基于模式识别的方法、基于知识推理的方法和基于数学模型的方法。

基于模式识别的方法主要依靠从已标记的样本数据中挖掘模式进行评估, 如基于粗糙集理论的评估法、基于神经网络的评估法等, 该类模型的局限在于样本的标记难度及合理性。

以贝叶斯网为代表的评估法是当前基于知识推理的评估法的研究热点。其核心思想在于建立基于概率图模型, 以攻击各方的效益期望来近似表示网络安全态势。Cui 等^[5]提出基于隐马尔可夫博弈模型两角色网络安全态势评估模型, 而后在该模型中引入用户的中立角色^[6]。图模型的建立以及概率表的确定均需要大量的专业知识, 这是基于知识推理的评估法面临的最严峻的挑战。

常见的基于数学模型的方法有层次分析法及其派生方法、模糊综合评估法等。这些方法多通过借鉴经典的多目标决策理论中的方法来解决网络安全态势评估问题。模糊层次分析法作为对层次分析法的改进, 提出一种实现简单且较好地解决了一致性校验及调整问题的方法, 成为广为使用的网络攻击效果评估模型。

当前, 在指标赋权的研究中, 基于判断矩阵的主观赋权法以及基于熵值法的客观赋权法是广为使用的赋权法。鲜明等^[7]提出使用相乘平均法来组合主观权重法和客观权重, 其局限在于对小权重的偏向。故在网络攻击效果评估领域, 仍缺

少行之有效的权重综合方法。

基于上述情况, 本文提出一套针对木马攻击效果的评估指标体系, 该体系中指标值可定性也可定量, 可人工标注也可系统采集。同时, 采用模糊层次分析法对指标赋权, 计算评估结果。进一步地, 本文提出一种多对一的权重综合技术, 将多个非纯客观权重及与单个客观权重进行综合。最后, 实现了木马攻击效果评估系统, 并使用第三方木马样本及其评估结果进行实验与对比分析。

2 木马攻击效果评估指标体系

2.1 木马分类及行为分析

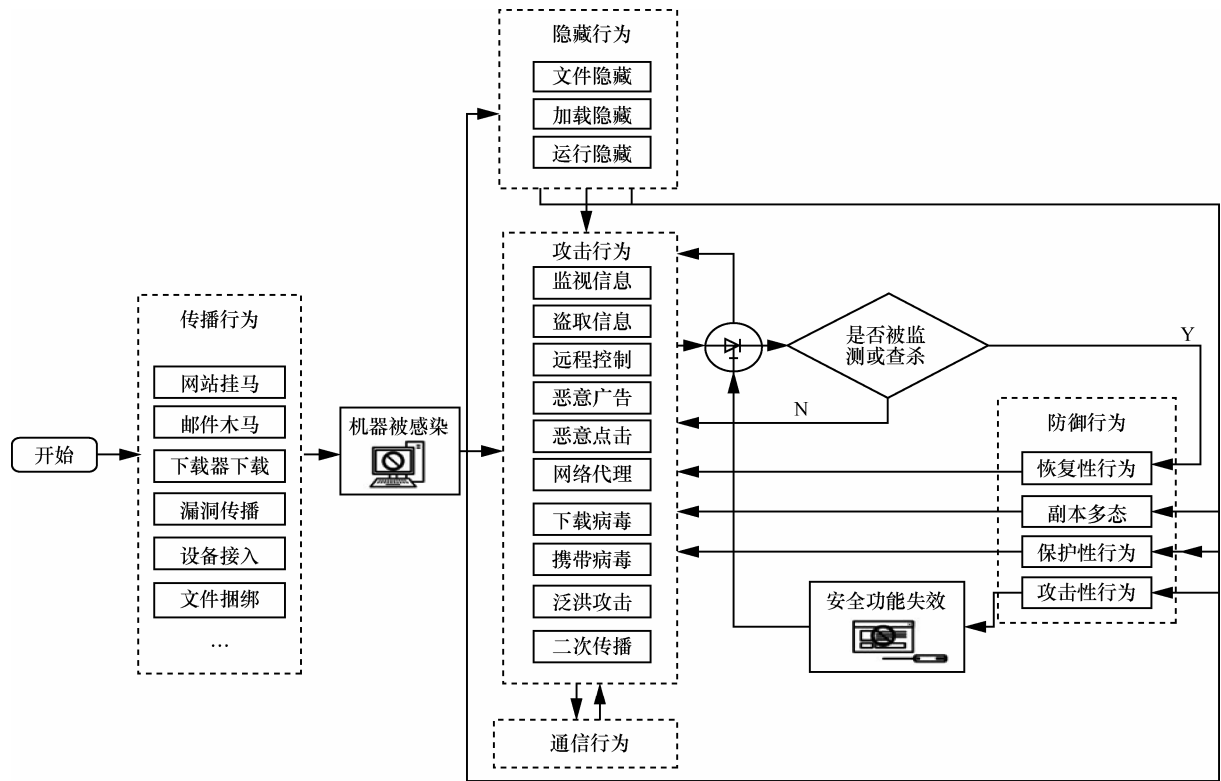
根据卡巴斯基实验室对木马病毒的定义, 可以按照其行为特征将常见的木马病毒分为表 1 中若干类别。

表 1 木马病毒的分类

类型	说明
Backdoor	后门木马, 恶意用户可通过后门程序远程控制感染机器
Exploit	漏洞木马, 专指利用系统或用户软件漏洞进行感染的木马
Rootkit	该木马使用 Rootkit 工具设计, 具有非常强的隐藏能力
Trojan-Downloader	木马下载器, 主要用来下载并安装新的恶意软件
Trojan-Dropper	木马携带者, 能够阻止安全软件的探测, 安装新的恶意软件
Trojan-Spy	间谍型木马, 通过监视屏幕、键盘等盗取系统或用户信息
Trojan-Psw	盗号木马
Trojan-Gamethief	专指盗取在线游戏账号信息的木马
Tojan-Banker	专指盗取在线金融系统账号信息的木马
Trojan-Mailfinder	收集感染机器中的邮箱地址
Trojan-Clicker	机器感染该木马后, 在用户不知情的情况下对网页广告或恶意网页进行点击
Adware	在用户未允许的情况下, 以弹窗形式弹出广告
Trojan-Proxy	恶意用户通过感染机器作为匿名代理访问网络
Trojan	综合性木马, 包含多种攻击手段

尽管不同种类木马在行为上存在差异, 但是均具有传播性、攻击性、防御性、隐藏性和交互性共 5 种特性, 并且在 5 种特性上表现出不一样的性能。通过对木马运行流程的解读 (如图 1 所示), 可以对以上特性有进一步的了解。

木马的运行流程以传播行为为起点, 可同时



执行隐藏行为、攻击行为和防御行为。其中，攻击行为是其他行为的目的，若没有攻击行为，木马病毒谈不上危害。隐藏行为是攻击行为能够成功执行的前提，而防御行为进一步保证了攻击行为的持久性。绝大多数木马攻击行为的最终目的都在于窃取数据，而数据需要通过网络进行传输，通信行为是攻击质量的保证。

通过以上分析，可以依据木马在 5 种特性上性能的好坏来评价木马攻击效果，表 2 对木马病毒在以上特性上表现的性能及其重要程度描述如下。

表 2 木马病毒性能分析		
性能	说明	对攻击效果的重要度
传播能力	决定是否被感染	稍微重要
攻击能力	木马病毒的核心	非常重要
隐藏能力	攻击成功与否的前提	最重要
防御能力	攻击持久化的保证	非常重要
通信能力	攻击质量的保证	一般重要

2.2 传播能力分析

木马病毒通常通过网站挂马、邮件木马、

下载其下载、系统或软件漏洞等方式传播，可从传播的广度和易感染度来分析木马病毒的传播能力。首先，木马程序能够运行的平台种数决定了最大传播半径，对于可通过漏洞进行传播的木马来说，所含漏洞的软件或系统的热门程度进一步限制了该种木马的传播范围。

对于传播半径以内的计算机，木马病毒对用户行为的依赖程度定义了最基础的易感染度。同时，对于那些强依赖用户行为的木马病毒，还需关注其伪装度对用户行为的诱导，如伪装为正常软件的图标和名称诱使用户点击。表 3 对影响木马传播能力的要素进行了总结。

表 3 影响木马传播能力的要素		
要素	说明	对传播能力的重要度
感染平台种数	传播的最大半径	一般重要
对用户行为的依赖程度	最基本感染度指标	非常重要
伪装性	用诱导能力描述易感染度	稍微重要
漏洞利用能力	用漏洞的广度描述传播广度	最重要

表4 影响木马攻击能力的要素

要素	说明	对攻击能力的重要度
下载软件数量	提升了攻击效果的深度	最重要
二次传播能力	提升了攻击效果的广度	最重要
远程控制能力	能够最大限度窃取数据	非常重要
监视信息能力	通用窃取数据的手段	非常重要
盗取信息能力	专用窃取数据的手段	非常重要
携带软件能力	由于具有强隐蔽性, 攻击性能比较稳定	稍微重要
泛洪攻击能力	高危害的新型攻击	稍微重要
恶意点击能力	低危害的新型攻击	一般重要
恶意广告能力	低危害的新型攻击	一般重要
网络代理能力	低危害的新型攻击	一般重要

表5 影响木马防御能力的要素

要素	说明	对防御能力的重要度	对保护性的重要度	对顽固度的重要度	对副本能力的重要度	对恢复能力的重要度
保护性	保护静态的文件和动态的程序	最重要	/	/	/	/
静态防御能力	保护静态的文件	/	最重要	/	/	/
动态防御能力	保护动态的程序	/	一般重要	/	/	/
攻击性	攻击安全软件、防火墙等	最重要	/	/	/	/
顽固度	被监测或查杀后的顽固性	一般重要	/	/	/	/
副本能力	副本多态	/	/	最重要	/	/
静态副本数	静态的文件副本数	/	/	/	一般重要	/
动态副本数	动态的程序副本数	/	/	/	最重要	/
恢复能力	被查杀后恢复	/	/	非常重要	/	/
动态恢复能力	恢复动态的进程、线程等	/	/	/	/	非常重要
静态恢复能力	恢复静态的文件	/	最重要	/	/	一般重要
更新能力	对自身进行更新	最重要	一般重要	一般重要	/	/

2.3 攻击能力分析

木马病毒的攻击行为按攻击过程可分为直接攻击和间接攻击, 其中, 直接攻击又可按攻击目标分为传统攻击和新型攻击。传统攻击的首要目的在于窃取数据, 不限于远程控制、监视键盘、盗取账号等手段。新型攻击包括泛洪攻击、恶意点击、恶意广告等。直接攻击的危害度是有上限的, 通常认为间接攻击的潜在威胁更大。通过下载恶意软件或二次传播, 木马病毒攻击效果的深度和广度都得到了提升。在表4中, 可以看到各要素对木马攻击能力的影响。

2.4 防御能力分析

最好的防御是攻击, 木马病毒对安全软件、防火墙等安全系统的攻击是最强力的防御行

为。其次, 防御行为又可按保护的对象分为静态防御和动态防御, 静态防御旨在保护静态的程序文件、配置信息等, 动态防御旨在保护在内存中运行的木马程序。另外, 具有副本多态或强恢复能力的木马不能被彻底查杀, 具有更新能力的木马能够实时地提高防御能力。表5列举了影响木马防御能力的要素。

2.5 隐藏能力分析

木马病毒的隐藏行为按隐藏对象可分为静态隐藏、动态隐藏及通信隐藏。静态隐藏旨在隐藏木马程序文件、配置信息等。动态隐藏旨在隐藏木马的加载过程和运行过程。通信隐藏旨在隐藏通信方式和通信内容。成功的加载是木马运行的前提, 故加载隐藏的重要程度高于

运行隐藏，同时，动态隐藏是隐藏工作的重中之重。通过表 6 可以看到各要素对木马隐藏能力的重要性。

2.6 通信能力分析

通信能力决定了木马攻击的质量，早期木马程序采用 CS 模式设计，病毒在宿主主机上运行服务端程序，开启监听端口，由客户端主动向服务端发起连接从而实现通信。现代操作系统的安全策略、防火墙技术及实时监控技术飞速发展，经典的通信方式基本无法进行。因此，端口寄生技术和端口反弹技术被采用到木马程序设计当中。

2.7 层次化指标体系建立

通过对木马特性的分析，建立如表 7 所示的层次化的指标体系。

3 基于模糊层次分析的评估模型

3.1 模糊层次分析法

Satty 等^[8]提出层次分析法 (AHP, analytic hierarchy process)，该方法可在层次结构的指标体系中，依据专家对相邻层中下层准则对上层准则的重要度打分，计算出底层，即指标的绝对权重。该方法的核心工作为构建判断矩阵，准则数为 n 的层次对其上层准则 P 的判断矩阵 J 定义如下。

$$J = \left\{ a_{i,j} = k \in \left(\frac{1}{9}, \frac{1}{8}, \dots, \frac{1}{2}, 1, 2, \dots, 9 \right) \right\} \quad (1)$$

专家将下层第 i 个准则与第 j 个准则对准则 P 的重要性进行比较，打分为式(1)中 $a_{i,j}$ 的值。所取的分值 k 为 1 表示同等重要，从 2~9 数值

增大表示第 i 个准则比第 j 个准则重要度增加，反之，数值的倒数表示第 j 个准则比第 i 个准则的重要度。通过对判断矩阵 J 求最大特征根，可得到下层各准则对准则 P 的权重。通过对层次的广度遍历，可计算出底层相对总目标的权重。

使用层次分析法的难点在于对判断矩阵 J 的一致性判断，若一致性不满足则需要专家再次打分，调整判断矩阵。

Chang 等^[9]提出模糊层次分析法 (FAHP, fuzzy analytic hierarchy process)，在层次分析中引入了模糊理论。其最大的优势在于不用对判断矩阵 J 进行一致性判断，而计算权重的过程中就包含了一致性处理^[10]。模糊层次分析法对判断矩阵 J 定义如下。

$$J = \{ a_{i,j} = k \in (0.1, 0.2, \dots, 0.9) \} \quad (2)$$

同样采取专家打分的形式，所取分值 k 为 0.5 表示同等重要，从 0.6~0.9 数值增大表示第 i 个准则比第 j 个准则重要度增加，反之同理。基于判断矩阵，计算权重向量的方法为

$$W = \left\{ W_i = \frac{\sum_j a_{i,j} + \frac{n}{2} - 1}{n(n-1)} \right\} \quad (3)$$

3.2 指标权重计算及量化方法

通过对木马特性的分析，基于模糊层次分析法可以计算出指标的权重，同时，可以更进一步采用模糊层次分析法对定性指标值进行量化。相比现有的木马危害测量模型，指标取值可定量也可定性，其中，定性指标取值更合理（不同等级

表 6 影响木马隐藏能力的要素

要素	说明	对隐藏能力的重要度	对动态隐藏能力的重要度	对通信隐藏能力的重要度
静态隐藏能力	隐藏静态的文件	稍微重要	/	/
动态隐藏能力	隐藏加载过程和运行过程	最重要	/	/
加载隐藏能力	隐藏加载过程	/	最重要	/
运行隐藏能力	隐藏运行过程	/	非常重要	/
通信隐藏能力	隐藏通信方式和通信内容	一般重要	/	/
通信方式隐藏能力	隐藏通信方式	/	/	最重要
通信内容隐藏能力	隐藏通信内容	稍微重要	/	一般重要

表 7

木马攻击效果评估指标体系

目标	一级准则	二级准则	三级准则	四级准则
木马攻击效果评估	传播能力	可感染平台种数	/	/
		对用户行为的依赖程度	/	/
		伪装性	/	/
		漏洞利用能力	/	/
	攻击能力	下载软件数量	/	/
		二次传播能力	/	/
		远程控制能力	/	/
		监视信息能力	/	/
		盗取信息能力	/	/
		携带软件能力	/	/
		泛洪攻击能力	/	/
		恶意点击能力	/	/
		恶意广告能力	/	/
		网络代理能力	/	/
	防御能力	保护性	静态防御能力	/
			动态防御能力	/
		攻击性	/	/
			副本能力	静态副本数 动态副本数
		顽固度	恢复能力	静态恢复能力 动态恢复能力
			更新能力	/
		静态隐藏能力	/	/
			加载隐藏能力	/
		动态隐藏能力	运行隐藏能力	/
			通信方式隐藏能力	/
		通信隐藏能力	通信内容隐藏能力	/
			/	/
	通信能力	/	/	/

值的差异更符合现实情况),同时取值方式也更灵活(可人工标注也可系统采集)。

3.3 构建评估模型

综上所述,通过对木马特性进行分析,设计层次化的指标体系,使用模糊层次分析对指标权重进行计算,对指标值进行量化,从而构建木马攻击效果评估模型。

4 权重综合技术

4.1 多对一的权重综合技术

相乘平均法与可信权重法是常用的权重综合技术,但是前者对小权重具有倾向性,而后者在定义可信度的同时又加入了主观因素。同时,两者对客观权重采取直接组合的方式,对样本的依

赖性较大。本文提出一种多对一的权重综合技术,认为非纯客观权重与客观权重越接近,则具有更高的可信度,在评估计算时占到更大的比重,该技术并不是直接对客观权重进行组合,因此对样本的依赖性较小。定义含 S 组非纯客观权重的权重矩阵 W_s 为

$$W_s = \{w_{s_{i,j}}\} \quad (4)$$

其中, $w_{s_{i,j}}$ 为第 i 个非纯客观权重的第 j 个分量。基于客观权重 W_o , 计算权重分量近似度矩阵 S 为

$$S = \{s_{i,j} = 1 - |w_{s_{i,j}} - w_{o_j}|\} \quad (5)$$

基于近似度矩阵计算可信的权重矩阵 W_t 为

$$W_t = \{w_{t_{i,j}} = w_{s_{i,j}} \times s_{i,j}\} \quad (6)$$

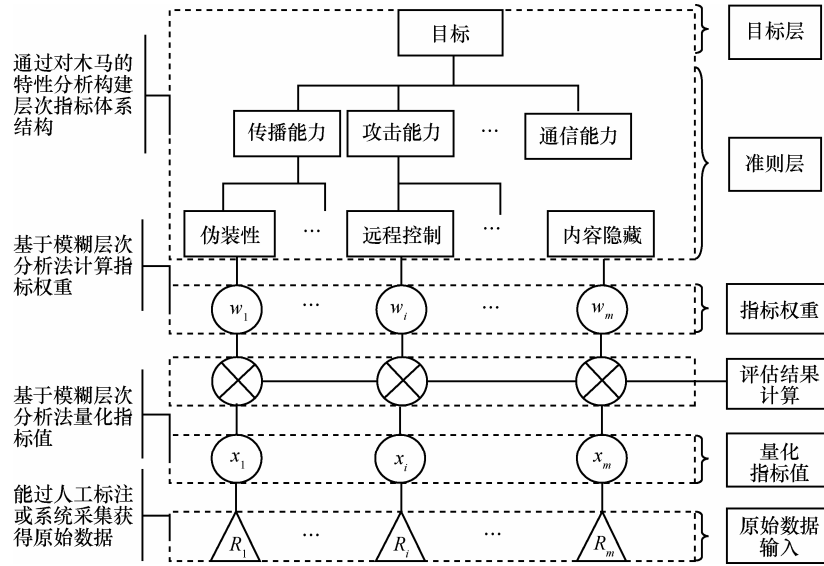


图2 木马攻击效果评估模型

基于可信的权重矩阵计算综合权重向量 W' 为

$$W' = \left\{ w'_j = \sum_i w_{i,j} \right\} \quad (7)$$

最后通过归一化，得到最终的权重向量 W

$$W = \left\{ w_j = \frac{w'_j}{\sum_j w'_j} \right\} \quad (8)$$

4.2 基于灰色关联度的赋权法

谭学瑞等^[11]提出基于曲线几何相似原理的灰色关联理论，钱吴永等^[12]基于该理论，通过计算指标的关联度来表示指标权重。在容量为 n 、指标个数为 m 的样本中，该方法通过式(9)计算指标值对参考值的关联系数，通过式(10)计算指标的关联度，通过式(11)计算归一化的指标权重。

$$\xi_{i,j} = \frac{\min_i \min_j (|x_{0j} - x_{i,j}|) + \rho \max_i \max_j (|x_{0j} - x_{i,j}|)}{|x_{0j} - x_{i,j}| + \rho \max_i \max_j (|x_{0j} - x_{i,j}|)} \quad (9)$$

$$W' = \left\{ w'_j = \sum_i \xi_{i,j} \right\} \quad (10)$$

$$W = \left\{ w_j = \frac{w'_j}{\sum_j w'_j} \right\} \quad (11)$$

4.3 常见的客观赋权法

变异系数法与熵值法为常见的客观赋权法，其核心思想均认为离散程度越大的指标对评估结果越重要，不同之处在于两者分别以变异系数和熵值来描述指标值的离散程度。

在容量为 n ，指标个数为 m 的样本中，变异系数法通过式(12)和式(13)计算各指标的均值和方差，通过式(14)计算各指标的变异系数，通过式(15)对变异系数归一化作为指标权重。

$$\bar{x}_j = \frac{1}{n} \sum_i x_{i,j} \quad (12)$$

$$s_j = \sqrt{\frac{1}{n-1} \sum_i (x_{i,j} - \bar{x}_j)^2} \quad (13)$$

$$cov_j = \frac{s_j}{|\bar{x}_j|} \quad (14)$$

$$w = \left\{ w_j = \frac{cov_j}{\sum_j cov_j} \right\} \quad (15)$$

熵值法通过式(16)计算个体的概率，通过式(17)计算各指标的熵值，通过式(18)将熵值转换为权重，通过式(19)将权重归一化。

$$p_{i,j} = \frac{x_{i,j}}{\sum_i x_{i,j}} \quad (16)$$

$$entropy_j = -\sum_i^n p_{i,j} \ln(p_{i,j}) \quad (17)$$

$$w'_j = \ln(n) - entropy_j \quad (18)$$

$$w = \left\{ w_j = \frac{w'_j}{\sum_j w'_j} \right\} \quad (19)$$

5 木马攻击效果评估实验与分析

5.1 样本与实验设计

本实验选取 57 个木马病毒样本，其中，50 个样本由东方微点公司进行危害度评级，另外 7 个样本由李渊等^[3]的木马危害测量模型进行评估，共覆盖 14 种木马类型。

实验分为 2 个部分：第 1 部分使用基于模糊层次分析的评估模型对这 57 个样本进行评估，并将评估结果与其他评估系统进行对比分析；第 2 部分使用多对一的权重综合技术对非纯客观权重及客观权重进行综合，将综合评估结果与未综合评估结果进行对比，以说明该权重综合技术的合理性。

5.2 评估实验与分析

在实验的第 1 部分中，本文根据模糊层次分析法对指标进行了主观赋权，在此基础上对木马病毒样本进行评估。

东方微点公司将 50 个样本评为高度危害和中度危害 2 种级别，如图 3 所示。通过对比可以看到，评估结果与之基本吻合。有 2 个高度危害的木马病毒比 2 个中度危害的木马病毒评估结果低，如图 4 所示，这 2 个高度危害木马病毒在各自的类型中仍然为攻击效果最好的。

通过对以上 2 个中度危害的木马进行进一步分析，可以看到即使被评为中度危害，具有高隐藏型的 Rootkit.Win32.Agent.fd 仍有不错的攻击效果。而中度危害的 Trojan-Downloader.Win32.Antiav.f 与高度危害的 Trojan-Dropper.Win32.Flystud.d 相比，隐藏能力稍强，下载能力明显较弱，但评估结果更高，这正是由于模糊层次分析法缺少对样本离散度的考虑造成的。

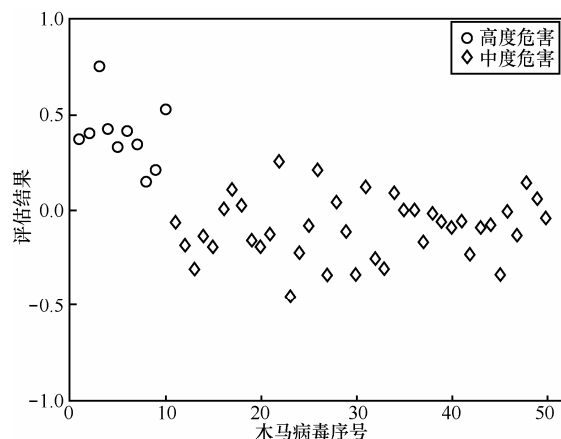


图 3 评估结果与东方微点病毒危害度评级对比

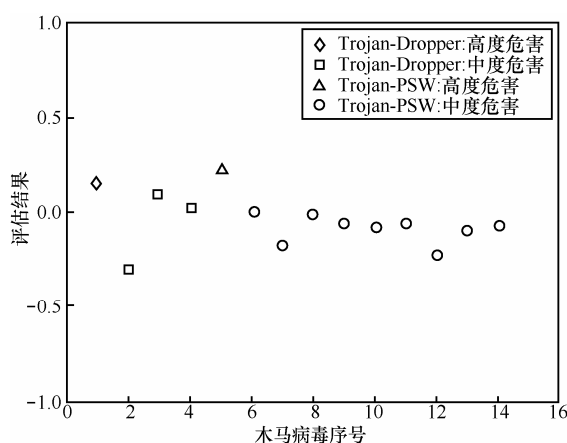


图 4 Trojan-Dropper 和 Trojan-PSW 类型木马的评估结果

东方微点的病毒危害度评级方式具有如下特性。1) 相对性，对不同类型的病毒有不同的评级方式，故 Rootkit.Win32.Agent.fd 未被评高度危害；2) 粗糙性，无法对同危害级别的木马进行粒度更细的评估。本文所提评估模型计算出来的评估结果，既能够反映不同类型木马的攻击效果的差异，又能够对同类型木马进行正确的评估，同时提供细粒度的量化评估结果。

本文所提评估模型对指标值的变化也是敏感的，实验样本中后门程序 Backdoor.Win32.Wintu.j 与 Backdoor.Win32.Krafcot.h 具有类似的传播能力、攻击能力、防御能力和攻击能力。但由于前者通过 UPX 方式加壳，具有更强的隐藏性。这两者的评估结果仍能够敏感地反映其隐藏性能上的差异：前者评估结果为-0.185 4，而后者为-0.300 1。

本文将另外 7 个样本的评估结果与李渊等^[3]的评估实验结果进行了对比，如表 8 所示，2 份评估结果具有一定的相似性：样本 A 因其卓越的

表 8 评估结果与木马危害测量模型评估结果对比

序号	木马名称	说明	本文提出的模型的评估结果	木马危害测量模型的评估结果
A	Trojan-GameThief.Win32.Magania.dlip	以设备驱动、文件劫持等多种方式加载启动，破坏多种安全软件，盗取游戏账号	0.462 3	1.847 0
B	Trojan-GameThief.Win32.OnLineGames.tnys	无加载隐藏能力，低防御能力，盗取指定游戏账号	-0.381 0	1.032 8
C	Trojan-GameThief.Win32.Ganhame.cn	修改注册表方式启动，攻击安全软件，盗取多种账号	0.082 9	1.318 4
D	Trojan-Downloader.Win32.Nurech.bg	修改注册表方式启动，攻击安全软件，下载多种恶意软件	-0.058 1	1.038 7
E	Trojan-Dropper.Win32.Delf.grq	修改注册表方式启动，盗取多种账号	-0.022 4	1.447 1
F	Trojan-Banker.Win32.Delf.bz	修改注册表方式启动，攻击安全软件，盗取指定金融系统账号	-0.150 5	1.280 4
G	Trojan-Mailfinder.Win32.MagPlayer.a	修改注册表方式启动，低防御能力，盗取邮件地址信息	-0.326 0	1.197 0

表 9 Trojan-Downloader.Win32.Antiav.f 与 Trojan-Dropper.Win32.Flystud.d 评估结果比较

木马名称	未经权重综合的评估结果	经权重综合的评估结果
Trojan-Dropper.Win32.Flystud.d	0.155 4	0.104 3
Trojan-Downloader.Win32.Antiav.f	0.210 5	0.109 9

隐藏能力和防御能力，排名第一；由于隐藏能力及防御能力皆弱，样本 B 排名最后；样本 C 与 E 均能够盗取多种类型账号，故排名靠前。然而，在评估结果中，样本 A 与其他样本的评估结果差异更大，能够正确反映木马病毒的核心性能隐藏能力对攻击效果的重要性。同时，样本 C 的评估结果比 E 稍高，这是因为前者能够攻击安全软件，防御力更强。另外，样本 D 相比 F 与 G 获得了更高的评估得分，这是因为其既能够攻击多种安全软件，又具有下载恶意软件的能力，攻击潜力不可忽视。

在实验的第 2 部分中，本文以基于模糊层次分析的赋权法及基于灰色关联度的赋权法构建非纯客观权重矩阵，以熵权法计算客观权重，最后通过多对一的权重综合技术，计算各样本的评估结果。再次对中度危害的 Trojan-Downloader.Win32.Antiav.f 与高度危害的 Trojan-Dropper.Win32.Flystud.d 进行比较，如表 9 所示，两者间评估结果近似，综合权重体现了指标离散度对评估结果的影响。

6 结束语

本文基于对木马特性的分析，建立了一套针对性的层次化指标体系，指标值可定性也可定量，

可人工标注也可系统采集。在此基础上，构建了基于模糊层次分析的评估模型，对木马病毒样本进行了评估实验。将实验结果与现有木马危害测量模型及安全公司的危害度评级进行了对比，本文提出的指标体系符合正确性、单调性及敏感性，评估结果符合客观事实。最后，本文引入了结合主客观权重的多对一权重综合技术，进一步提升了评估结果的合理性。下一步工作将结合指标体系合理性评估的相关研究，优化指标体系构建技术及权重综合技术。同时，结合更多机构对木马攻击效果评估实验，扩充木马病毒样本数据，进一步完善对比实验。

参考文献：

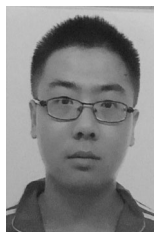
[1] XcodeGhost 入侵,大量 iOS 知名应用中中招[J]. 中国信息安全, 2015(10):14.
XcodeGhost invades a large number of well-known IOS applications[J]. China Information Security, 2015(10):14

[2] 韩兰胜, 郑聪, 邹梦松, 等. 计算机病毒危害性的模糊评价模型[J]. 小型微型计算机系统, 2010, 31(7):1297-1301.
HAN L S, ZHENG C, ZOU M S, et al. Fuzzy evaluation model for harms of computer virus[J]. Mini-Micro Systems, 2010, 31(7): 1297-1301.

[3] 李渊. 基于层次分析法的木马危害测量分析系统[D]. 武汉: 华中科技大学, 2012.
LI Y. AHP based evaluation model for harms of Trojan[D]. Wuhan: Huazhong University of Science and Technology, 2012.

- [4] 张建锋. 网络安全态势评估若干关键技术研究[D]. 长沙: 国防科学技术大学, 2013.
ZHANG J F. Key technologies research on large scale network security evaluation[D]. Changsha: National University of Defense Technology, 2013.
- [5] CUI X, TAN X, ZHANG Y, et al. A Markov game theory-based risk assessment model for network information system[C]//International Conference on Computer Science and Software Engineering. c2008:1057-1061.
- [6] 张勇, 谭小彬, 崔孝林, 等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3):495-508.
ZHANG Y, TAN X B, CUI X L, et al. Network security situation awareness approach based on markov game model[J]. Journal of Software, 2011, 22(3):495-508.
- [7] 鲜明. 网络攻击效果评估导论[M]. 长沙: 国防科技大学出版社, 2007:172-173.
XIAN M. Introduction to network attack effect evaluation[M]. Changsha: National University of Defense Technology, 2007: 172-173.
- [8] SATTY T L. How to make a decision:the analytic hierarchy process[J]. European Journal of Operational Research, 1990, 1(48):9-26.
- [9] CHANG D Y. Applications of the extent analysis method on fuzzy AHP[J]. European Journal of Operational Research, 1996, 95(3): 649-655.
- [10] 张吉军. 模糊层次分析法(FAHP)[J]. 模糊系统与数学, 2000, 14(2):80-88.
ZHANG J J. Fuzzy analytic hierarchy process(FAHP)[J]. Fuzzy Systems and Mathematics, 2000, 14(2):80-88.
- [11] 谭学瑞, 邓聚龙. 灰色关联分析:多因素统计分析新方法[J]. 统计研究, 1995(03):46-48.
TAN X R, DENG J L. Grey relational analysis: a new method of multivariate analysis[J]. Statistical Research, 1995(3):46-48.
- [12] 钱吴永, 党耀国, 熊萍萍, 等. 基于灰色关联定权的 Topsis 法及其应用[J]. 系统工程, 2009(8):124-126.
QIN W Y, DANG Y G, XIONG P P, et al. Topsis based on grey correlation method and its application[J]. System Engineering, 2009(8):124-126.

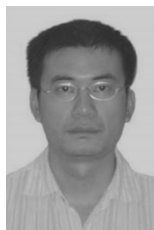
作者简介:



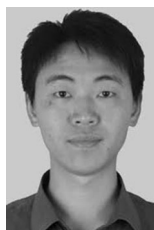
曾辰熙 (1987-), 男, 湖南长沙人, 国防科学技术大学硕士生, 主要研究方向为网络安全。



吴泉源 (1942-), 男, 上海人, 博士, 国防科学技术大学教授, 主要研究方向为人工智能与分布计算。



李爱平 (1974-), 男, 山东诸城人, 博士, 国防科学技术大学研究员, 主要研究方向为语义网络、数据挖掘和网络空间安全。



江荣 (1984-), 男, 福建连城人, 博士, 国防科学技术大学助理研究员, 主要研究方向为隐私保护和网络空间安全。