DOI: 10.3969/j.issn.1671-0673.2018.05.017

基于指标体系信息融合的恶意代码威胁程度评估方法研究

师 炜[1,2],庞建民[1,2],梁光辉[1,2],周 鑫[1,2]

(1. 信息工程大学,河南 郑州 45001;2. 数学工程与先进计算国家重点实验室,河南 郑州 45001)

摘要: 针对当前恶意代码威胁程度评估方法的局限性,研究基于信息融合的恶意代码威胁程度评估方法,提出针对恶意代码资源消耗、破坏能力、抗检测能力、自启动能力、扩散能力、隐蔽能力、自我保护能力等 7 个指标的评估体系,是一种融合上述 7 个指标的二进制恶意代码威胁性评估方法。实验表明,该体系可以用以判定可疑代码的威胁类别,量化危害程度,不仅可以使相应工作具有针对性,而且可以降低成本,提高效益。

关键词: 恶意代码; 指标体系; 信息融合

中图分类号: TP309 **文献标识码:** A **文章编号:** 1671-0673(2018)05-0598-05

Research on Evaluation Method of Malicious Code Threat Degree Index System Based on Information Fusion

SHI Wei[1,2], PANG Jianmin[1,2], LIANG Guanghui[1,2], ZHOU Xin[1,2]

(1. Information Engineering University, Zhengzhou 45001, China; 2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 45001, China)

Abstract: In view of the limitation of the current malicious code threat assessment method, this paper studies the evaluation method of the degree of malicious code threat based on information fusion, and puts forward an assessment system of the following seven indicators: malicious code resource consumption, destruction ability, anti-detection ability, self-starting ability, diffusion ability, concealment ability and self-protection ability. Experiments show that the system can be used to determine the threat category of suspicious code and quantify the degree of harm, which can not only make the corresponding work targeted, but also reduce costs to improve efficiency.

Key words: malicious code; index system; information fusion

0 引言

恶意代码从出现到发展至今,无论是数量的规模还是采用的技术都发生了一系列的进化演变,其主要表现为恶意代码的数量以惊人的速度增长,根据 Mcafee 实验室报道,2014 第 4 季度,有超过 350M 的恶意代码样本,相比第 3 季度增长了 17%[1],赛门铁克报道,在 2015 年 5 月,有超过 4450 万的新恶意代码生成;为了躲避检测,恶意代码作者采用多态,变形,混淆等技术,意味着一些恶意代码样本属于同一恶意代码家族;恶意代码攻击目标越来越多地针对政治,军事以及经济,根据 2015 年赛门铁克公司旗下诺顿公司发布的《诺顿

收稿日期: 2017-08-05; 修回日期: 2017-10-19

基金项目: 国家自然科学基金资助项目(61472447)

作者简介: 师 炜(1993-),男,硕士生,主要研究方向为信息安全。

网络安全调查报告》[2],我国是新兴市场中遭受网络攻击最严重的国家,2015 年 12 月 23 日,乌克兰电力系统遭受到恶意代码攻击,2016 年,美国东部网络遭到 Mirai 等恶意代码攻击、希拉里“邮件门”等事件,都深刻地改变着世界政治经济生活的方方面面。

因此,建立一套合理的恶意代码威胁评估指标体系,用以判定可疑代码的威胁类别,量化危害程度,不仅使相应工作具有针对性,还可以降低成本提高效益。

当前,恶意代码威胁性评估主要存在以下问题: ①评估指标少,对恶意代码威胁性的描述不够全面; ②评估选取特征比较单一,恶意代码的行为往往通过不同方式体现,单一的特征不足以描述恶意代码的威胁性; ③评估模型比较单一,难以细粒度地刻画评估要素之间的关系。

本文提出一种针对恶意代码威胁程度评估的指标体系,采用一种评估方法,对资源消耗、破坏能力、抗检测能力、自启动能力、扩散能力、隐藏能力、自我保护能力等 7 个指标进行评估。

1　研究现状

关于恶意代码危害性的评估通常组织专家进行人工评估,国内相关的研究有,文献[3]提出针对计算机病毒的传播情况、攻击破坏性、传染性以及复杂性 4 个基本要素分别制定相应指标体系进行级别划分的评估方法; 文献[4]提出基于证据推理的程序恶意性判定方法,对二进制进行逆向分析得到恶意行为,通过证据推理融合行为特征,进而判定程序的恶意程度。

文献[5]提出一种基于行为分析的代码危害性评估技术,分析恶意代码常见行为,并利用系统调用序列及相关参数信息为各种恶意代码行为建立特征模式,以传染能力、破坏能力和生存能力构建代码危害评估指标体系,设计并实现基于行为的代码危害评估系统原型。文献[6]提出通过实时监测主机的文件系统的修改、远程进程的注入、特定 API 函数的调用等行为来判定程序是否为木马程序属于基于主机行为的检测方法。文献[7]提出一种基于安全事件分类的动态风险评估指标体系框架,将静态评估和动态评估结合起来。文献[8]提出以趋利性和破坏性为恶意代码的主要特征,研究恶意代码危害性评估要素和指标体系,制定了恶意代码危害性评估标准。

文献[9]提出一种基于信息融合的二进制恶意代码威胁性评估方法,通过对恶意代码威胁性的评估过程逐层分解,针对各层不同的特点采用不同的算法,避开了采用单一算法的缺陷,提高了恶意代码威胁性评估的适应性与可扩展性。

本文在文献[9]的基础上,参考国家标准《信息安全技术信息安全风险评估规范》[10],结合研究现状对恶意代码威胁性评估进一步完善。首先,文献[9]提出了资源消耗、自启动能力、隐藏能力、自我保护能力 4 个指标,而在恶意代码对用户的威胁方面,恶意代码是否会通过移动载体等方式进行传播,是否会检测到是虚拟机环境,对目标会造成哪些方面的破坏,即恶意代码的扩散能力、抗检测能力、以及破坏能力都应作为恶意代码威胁程度的评估指标之一; 其次 API 调用序列是反映恶意代码动态行为的重要参考信息之一; 第三,恶意代码评估结果应该清晰直观,本文采用图示法描述评估结果。

与文献[9]相比,本文主要做了以下改进:

①对恶意代码威胁性的指标描述更全面,增加了扩散能力、抗检测能力、破坏能力等指标; ②增加了恶意代码 API 调用序列作为恶意代码行为特征; ③对恶意代码威胁程度的描述更加直观,采用示例图的形式,对各个指标给出分数,便于比较不同恶意代码各个指标的能力,对恶意代码行为描述更详细。

2　恶意代码威胁程度评估框架

通过对恶意代码结构,传播机制,自我保护机制和危害性的分析,本文总结出判断恶意代码威胁程度的 7 个关键指标。本章给出恶意代码评估的指标定义、分析原理、实现流程和评估方法。

2.1　基于恶意代码行为的分析方法

本文根据文献[5,9],结合实际工作经验,总结出恶意代码在实际运行过程中重要的威胁行为,恶意代码威胁性评估流程如图 1 所示。

如表 1 所示,恶意代码破坏能力指其对目标机的系统造成的破坏程度,例如修改系统配置,删除或修改文件等行为造成的破坏等; 恶意代码抗检测性指其是否能感知运行环境是虚拟机,沙盒等的能力,例如虚拟机识别包括对系统的注册表、文件系统、进程识别。虚拟机的注册表中会记录虚拟机信息相关的键值,文件系统中有与虚拟机相关的文件和文件夹,任务进程中,也会运行一些特殊的进程,

这类进程名可作为识别虚拟机检测的依据。恶意代码扩散能力指恶意代码的扩散速度和扩散途径，例如是否具有写入U盘并传播的行为等。启动能力指其自启动的能力，即开机自启的能力。隐藏能力指恶意代码隐藏自身的能力，如设置隐藏属性，代码注入等能力。自我保护能力指恶意代码的加密技术，反跟踪技术。资源消耗指恶意代码运行所占有的CPU，内存等资源情况。

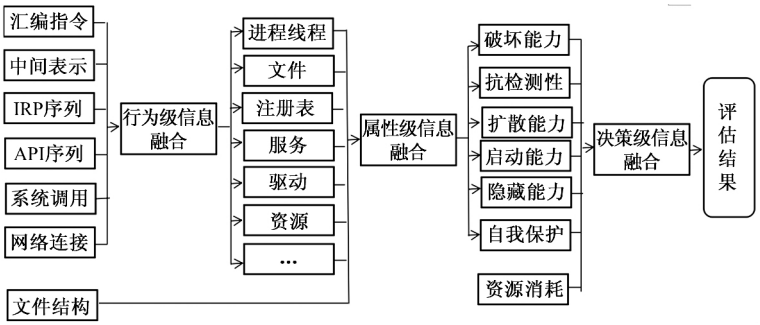


图1 恶意代码威胁程度评估流程图

表1 指标定义表

指标	定义
资源消耗	运行占有的CPU、内存等资源
破坏能力	修改系统配置，删除/修改文件，网络阻塞，获取敏感信息等
抗检测性	感知在虚拟机中运行的能力等
扩散能力	扩散速度，摆渡攻击等
启动能力	开机自启动等
隐蔽能力	设置隐藏属性的能力等
自我保护能力	加壳，加密，反跟踪等

2.2 基于信息融合的二进制恶意代码威胁性评估方法

如图1所示，基于信息融合的二进制恶意代码威胁性评估方法步骤如下:

2.2.1 行为级信息融合

利用静态或者动态方法分析恶意代码对进程，线程、文件、注册表、服务、网络、系统资源等对象的操作，通过分析得到上述对象对应的的文件结构、反汇编指令、系统调用，IRP序列、API序列等信息进行融合，对恶意代码行为做出判断，即确定代码特征、实现方法、代码行为三者之间一一对应关系，属性的某种实现方式可以有多种实现方法，例如，启动属性可以通过加载系统服务，可以通过注册表启动等多种实现方法，定义 $Type_i$ 为某种实现方式，$Behavior_{in}$ 为该方式实现过程中所涉及的行为，当实现方式 i 所涉及的行为均满足时，判定代码采用了该方式，即

$$Type_i = Behavior_{i1} \& \cdots \& Behavior_{in}。$$

对于 $Behavior_{in}$，$\boldsymbol{I}_{ASM}$ 表示代码的反汇编指令序列，$\boldsymbol{I}_{FUN}$ 表示代码的函数调用序列，$\boldsymbol{I}_{API}$ 表示代码的 API 调用序列，$\boldsymbol{I}_{IRP}$ 表示代码执行过程中的 IRP 序列，则

$$\mathrm{Behavior}_{ij} = \boldsymbol{I}_{ASM} \mid \boldsymbol{I}_{FUN} \mid \boldsymbol{I}_{API} \mid \boldsymbol{I}_{IRP}。$$

2.2.2 属性级信息融合

$Attribute_i$ 代表恶意代码第 i 个关键属性，

$$Attribute_i = \sqrt{\sum_{i=1}^{n} \left(w_{ij} . Type_{ij} \right)^2}。$$

其中，W_{ij} 代表第 j 种实现方式在第 i 个关键属性影响中所占的权重，由专家经验获得，且第 i 个关键属性所有实现方式的权重之和为1，即 $\sum_{j=1}^{n} w_{ij} = 1$，$Type_{ij}$ 表示第 i 个关键属性的第 j 种实现方式，如果该属性采用第 j 种实现方式实现，则 $W_{ij} = 1$，反之为0。

2.2.3 决策级信息融合

采用层次分析法对各属性的相对重要性进行计算，确定权重的步骤如下:

步骤① 以恶意代码关键属性两两比较的结果构造判断矩阵:

$$\boldsymbol{M} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ . & \cdots & . \\ . & \cdots & . \\ . & \cdots & . \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$，其中 $a_{ij} > 0$，$a_{ji} = \frac{1}{a_{ij}}$，$a_{ii} = 1$，

i 为数列的行数，j 为数列的列数，a_{ij} 的值由表2确定。

表2 a_{ij} 量化赋值表

因素比因素	量化值
同等重要	1
稍微重要	3
较强重要	5
强烈重要	7
极端重要	9
两相邻判断的中间值	2,4,6,8

步骤② 计算重要性排序，根据判断矩阵，求出最大特征根 λ_{max} 所对应的特征向量 $\boldsymbol{\omega}$，$M \cdot \omega =$

$\lambda_{max} \cdot \omega, \omega = (w_1, w_2, \cdots, w_n)$。

步骤③　一致性检验,如果满足一致性,则恶意代码评估结果:

$S = (w_1, w_2, \cdots, w_n) \cdot (Attribute_1, Attribute_2, \cdots, Attribute_n)^T$。

3　实验与分析

3.1　实现流程

恶意代码威胁程度评估系统的评估流程,如下图 2 所示。

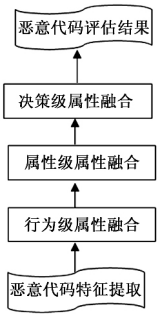
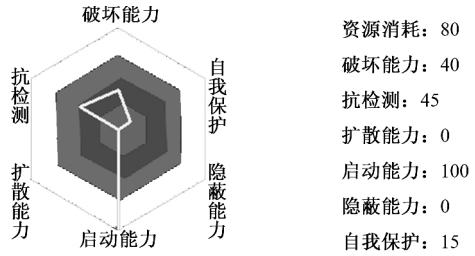


图 2　恶意代码评估流程图

3.2　实验分析

文中分析的恶意代码均为 PE 格式,恶意代码特征的提取在 Windows 7 x86 的 VMware 虚拟机中进行,并且每评估完一个样本即将虚拟机恢复到新安装时的状态。

本文数据集共收集了 2 176 个 PE 格式样本,实验样本均来自于 Virusshake 网站。其中对于样本 A,本文实验分析结果如图 3 所示,样本 A 是一种远程控制型的木马,通过修改系统权限,设置启动项,连接指定网站,使系统下载和安装文件,从而远程控制并窃取用户资料。



恶意代码检测-评分

图 3　恶意代码评估结果图

利用本文决策级信息融合中的层次分析法,计算该样本的评估结果步骤如下:

①该样本的判断矩阵为

$$\begin{pmatrix} 1 & 1/9 & 1/7 & 1/6 & 1/4 & 1/3 & 1/5 \\ 9 & 1 & 3 & 3 & 5 & 7 & 5 \\ 7 & 1/3 & 1 & 2 & 4 & 6 & 3 \\ 6 & 1/3 & 1/2 & 1 & 4 & 5 & 3 \\ 4 & 1/5 & 1/4 & 1/4 & 1 & 3 & 1/2 \\ 3 & 1/7 & 1/6 & 1/5 & 1/3 & 1 & 1/3 \\ 5 & 1/5 & 1/3 & 1/3 & 2 & 3 & 1 \end{pmatrix},$$

求得其最大特征根 $\lambda_{max} = 7.4067$**,归一化后特征向量** $\omega = (0.0236, 0.3841, 0.2212, 0.1742, 0.0675, 0.0390, 0.0903)$。

②一致性检测。根据判断矩阵检测原理,检测以上得到的权重是否合理,使用检测公式: C. R. = C. I. /R. I. **,其中** C. R. **为判断矩阵的随机一致性比率;** C. I. **为判断矩阵的一般一致性目:**

$$C.I. = (\lambda_{max} - n) / (n-1),$$

即 $C.I. = (7.4067-7) / (7-1) = 0.6778$**,** R. I. **为判断矩阵的平均随机一致性目标,1 ~ 9 阶的判断矩阵如表 3 所示。**

表 3　1 ~ 9 阶矩阵随机一致性指标表

n	R. I.	n	R. I.
1	0	6	1.26
2	0	7	1.41
3	0.52	8	1.46
4	0.90	9	1.49
5	1.12		

$C.I. = 0.6778 < 1.41$ **满足一致性,得到的权重是合理的,该样本的评估结果为** $S = (0.0236, 0.3841, 0.2212, 0.1742, 0.0675, 0.0390, 0.0903) \cdot (80, 40, 45, 0, 100, 0, 15)^T = 35.3105$**,即该样本评估结果分数为** 35.3105。

如图 4 所示,实验表明,本文所实现的系统能捕获样本各个指标的行为信息,并给出相应的分数,相较于哈勃文件系统给出的安全指数,本文所实现的系统更直观更便于理解,而对于该样本各个指标的能力,哈勃系统分析如图 4、图 5 所示,哈勃系统将恶意代码的行为分析划分为进程、文件、网络、注册表和其他行为,如图 3、图 6 所示,本文不仅能捕获恶意代码以上行为并能融合以上行为信息,按恶意代码资源消耗、破坏能力、抗检测能力、自启动能力、扩散能力、隐蔽能力、自我保护能力 7 个指标对上述行为进行评估给出分数,为相关部门进行恶意代码行为及能力的对比提供参考。

从实验结果看,系统对恶意代码各项能力使用百分制打分,评估结果清晰直观,对各行为指标能详细描述,为评估恶意代码提供较好的参考辅助

工具。

图4 哈勃行为分析结果图

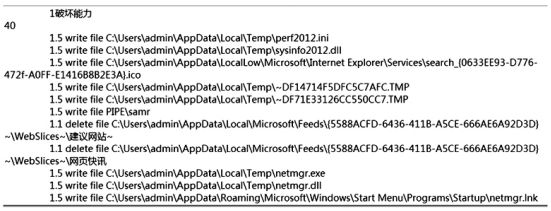


图6 本系统行为分析图

图5 哈勃指标行为分析结果图

4 结论

本文通过构建恶意代码威胁程度评估模型，准确地对恶意代码的威胁性做出评估，提高了对恶意代码危害程度评估能力，为相关部门制定相关政策和防治措施提供参考。在笔者研发的某项目中得到运用，取得了良好的实际效果。

参考文献:

[1] 迈克菲实验室. 迈克菲实验室威胁评估报告 [EB/OL]. [2015-05-14]. http://www.macafee.com/us/resorurces/reports/rp-quarterly-threat-q4-2014.pdf.

[2] 赛门铁克. 赛门铁克智能报告 [EB/OL]. [2015-05-14]. https://www.symantec.com/content/en/us/enterprise/other_resources/intelligence_report_05-2015.en-us.pdf.

[3] 张建，梁宏，陈建民，等. 计算机病毒危害评估 [J]. 信息网络安全，2005(1):39-41.

[4] 张一弛，庞建民，赵荣彩. 基于证据推理的程序恶意性判定方法 [J]. 软件学报，2012，23(12):3149-3160.

[5] 黄茜. 基于行为分析的代码危害性评估技术研究 [D]. 郑州: 信息工程大学，2010.

[6] 韩奕. 基于行为分析的恶意代码检测与评估研究 [D]. 北京: 北京交通大学，2014.

[7] 徐冰莹. 基于指标体系的网络安全风险评估研究 [D]. 长沙: 国防科学技术大学，2008.

[8] 张健，舒心，杜振华，等. 一种评估恶意代码危害性方法的研究 [J]. 信息网络安全，2009，24(10):7-9.

[9] 庞建民，戴超，单征，等. 一种基于信息融合的二进制恶意代码威胁性评估方法: 中国，CN201410361614 [P]. 2014-07-25.

[10] 全国信息与文献标准化技术委员会. 中华人民共和国国家标准 GB/T31509-2015 [S]. 2015-05-15.

(编辑: 颜峻)