

一种拟态构造的 Web 威胁态势分析方法

李卫超, 张 铮, 王立群, 刘镇武, 刘 浩

(数学工程与先进计算国家重点实验室, 郑州 450001)

摘 要: 基于裁决差异性判别进行威胁推测是拟态防御系统屏蔽和阻断攻击威胁的重要机制, 然而现有的拟态裁决机制无法对拟态防御系统安全态势进行有效归纳分析和威胁管控。为此, 以拟态 Web 服务系统为例, 将网络态势感知技术融入到拟态防御架构中, 提出一种改进的 Web 威胁态势分析方法。对多层次的拟态裁决告警日志进行数据关联, 挖掘及分类融合提取的特征数据信息, 并对不同类型的分类数据进行可视化展示。实验结果表明, 该方法能够显示拟态防御系统的安全状态, 及时获悉异常执行体的运行情况, 从而实现对拟态防御系统的安全态势进行分析与评估。

关键词: 拟态防御; Web 服务系统; 数据关联; 威胁分类; 可视化技术

开放科学(资源服务)标志码(OSID):



中文引用格式: 李卫超, 张铮, 王立群, 等. 一种拟态构造的 Web 威胁态势分析方法[J]. 计算机工程, 2019, 45(8): 1-6.

英文引用格式: LI Weichao, ZHANG Zheng, WANG Liqun, et al. A Web threat situation analysis method for mimic structure[J]. Computer Engineering, 2019, 45(8): 1-6.

A Web Threat Situation Analysis Method for Mimic Structure

LI Weichao, ZHANG Zheng, WANG Liqun, LIU Zhenwu, LIU Hao

(State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

[Abstract] Threat adjudication based on the judge method of ruling difference is an important mechanism for the mimic defense system to shield and block the threat of attacks. However, the existing mimic adjudication mechanism cannot conduct effective inductive analysis and threat control on the security situation of the mimic defense systems. Therefore, taking the mimic Web service system as an example, and integrating the network situation awareness technology into the mimic defense architecture, this paper proposes an improved Web threat situation analysis method. The data association is performed on the multi-level mimic adjudication alarm log. The feature data information extracted by fusion is deeply mined and classified. Different types of classification data are visually displayed. Experimental results show that the method can display the security state of the mimic defense systems, and is informed of the running state of the abnormal execution body in time, so as to realize the analysis and evaluation of the security situation of the mimic defense systems.

[Key words] mimic defense; Web service system; data association; threat classification; visualization technology

DOI: 10.19678/j.issn.1000-3428.0054221

0 概述

根据国家信息安全漏洞共享平台最新整理资料发现, 网络安全漏洞数量累计达到 14 216 个, 其中高危漏洞 4 899 个, 程序漏洞和 Web 应用漏洞之和占比高达 85%^[1]。由于网络空间环境难以彻底避免未知漏洞、未知后门、未知攻击带来的安全威胁, 因此

研究人员提出拟态防御技术, 以期在应用系统存在漏洞后门的情况下, 通过拟态防御架构的动态异构冗余特性达到抵抗潜在漏洞威胁攻击的目的^[2]。网络空间拟态防御技术作为网络空间安全的新兴技术, 其仲裁方法^[3]、执行体调度算法^[4]、异构环境构造方法^[5]等发展十分迅速。Web 服务系统作为重要的服务载体和提供平台, 面临网络空间安全严重威

基金项目: 国家重点研发计划“网络空间安全”重点专项(2018YFB0804003); 上海市科学技术委员会科研计划项目(16DZ1120502)。

作者简介: 李卫超(1994—), 男, 硕士研究生, 主研方向为网络空间安全; 张 铮, 副教授; 王立群, 硕士研究生; 刘镇武, 硕士; 刘 浩, 硕士研究生。

收稿日期: 2019-03-14

修回日期: 2019-05-05

E-mail: 010liweichao@163.com

胁。因此,将拟态防御理论应用在 Web 服务环境中,设计出拟态防御构造的 Web 服务器,期望能够通过内生安全的动态异构冗余架构技术来抵御复杂多变的 Web 攻击手段^[6]。为验证拟态防御构造 Web 服务器的安全防御能力,多家权威测试机构于 2016 年对拟态防御构造 Web 服务器进行了完整的测试,充分验证了拟态防御构造 Web 服务器的安全防御能力^[7]。然而,目前拟态防御系统与传统基于规则检测的防御方法的目的和手段有所不同,拟态防御并不依赖于规则进行威胁检测,而是依赖于构造动态异构冗余的内生威胁感知环境,通过多模裁决的方法进行威胁推测。因此,对于拟态裁决产生的威胁告警数据只包括多个服务执行结果的差异信息,相对于传统方法产生的威胁告警数据存在归纳分析和威胁管控的困难。此外,由于拟态防御的动态异构冗余特性,会产生多源异构的源数据,为处理多维数据带来了困难。对于拟态裁决的差异性判别产生的告警数据,大部分异常告警中只有少部分为真正的攻击威胁,即较大部分的攻击威胁中只有少数是真正起到作用的。因此,需要将网络安全态势感知技术、拟态 Web 威胁感知环境和基于拟态裁决的威胁推测方法相结合,以实现拟态 Web 服务系统的风险评估和态势展示。

本文将网络态势感知技术融入到拟态防御架构中,以实现拟态裁决的威胁告警数据关联分类和可视化展示,并基于拟态防御架构的 Web 服务系统,提出一种拟态构造的 Web 威胁态势分析方法,以达到对潜在的漏洞威胁进行管控的目的。

1 网络空间态势感知技术

目前,网络空间态势感知技术的研究方法已经在众多网络空间基础设施中应用并取得了成功。早在 1999 年, Bass 提出了网络态势感知(Cyberspace Situational Awareness, CSA)的概念,并且指出了多维数据融合将是未来网络空间态势感知技术的发展方向^[8]。网络态势的概念是指网络整体的运行状态和变化趋势,它由各种网络设备的运行状态、网络传输行为和用户在网络空间中的操作组成。网络态势描述了网络空间中空间、时间和实体之间的复杂关系,这可以理解为是一种由连续状态集构成的趋势。因此,网络空间态势感知技术则会通过将网络态势的变化趋势进行获取、分析、评估和展示,并对未来发展趋势做出预测。近年来,对于网络空间态势感知技术的研究正处于多元发展的阶段。文献[9]结合网络空间应用系统的具体实际问题,提出网络空间态势感知的基础模型。文献[10]提出基本的攻击树构造方法,并将其应用于网络态势分析研究。文献[11]论述了以渐进或递归的方式来表示攻击树,从而利用攻击变化的趋势来生成网络态势。文献[12]提出基于图的网络弱点分析方法,利用攻击

成功概率指出风险性较高的攻击路径,从而对网络态势进行评估。文献[13]提出利用加权图的方法来应用系统漏洞攻击者对应用系统访问控制权限变化的影响,并基于加权图对网络态势进行了安全评估。文献[14]提出用风险度和危害度描述攻击目标的重要性和攻击危害程度来量化网络安全态势。文献[15]提出由网络风险传播算法构成的网络态势的风险传播模型。文献[16]提出一种层次化的方法来表述网络安全态势感知。文献[17]提出基于攻防博弈模型的最优主动防御模型和网络安全态势测评方法。文献[18]从网络安全态势的觉察、理解和投射这 3 个层面综述讨论了网络安全态势感知的研究现状和存在的问题。

对拟态防御系统的非特异性安全增益进行安全态势感知,依赖于网络安全态势感知技术,从服务系统的运行过程中获得原始数据,识别出各类网络活动中的关键要素以及其中异常反应的真实意图,并对其风险性按照攻击类型、攻击威胁程度、攻击目标关键性、异构冗余组件的可信程度以及拟态防御架构的异构化差异程度等指标进行综合评估,合理地进行拟态容器执行环境和裁决推理策略的变换^[19]。

2 拟态告警数据关联分析

基于拟态裁决的威胁推测方法产生的异常告警信息,通过数据流量的不一致程度产生异常报警,但产生的报警信息过于单一,导致攻击行为的辨识度低下以及攻击溯源困难等问题。为增强告警信息的准确性和有效性,便于对普遍存在的恶意攻击进行分析,将裁决日志和执行体容器中的日志记录进行融合,以更加有效地对攻击威胁进行分析^[20]。图 1 所示为拟态防御系统生成异常告警流程示意图。

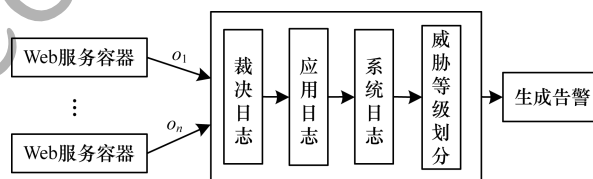


图 1 异常告警流程示意图

首先系统输入将请求分发至具有 n 个执行体容器集合,所述的 n 个构件体容器对请求进行解析并计算,将各自计算结果发送至裁决模块。然后裁决模块对所述 n 个执行体容器的计算结果进行多模裁决,根据多模裁决的不一致程度,将不一致程度较高的计算结果标记为异常告警数据。当裁决日志中记录了异常信息后,根据该裁决日志中所记录的执行体容器索引和失效类型,从具体应用的日志中确定该异常是否存在应用日志中出现,在系统日志中确定是否存在该异常进程运行的相关记录,并根据在应用层次出现的情况下进行威胁等级划分。最后将经过多重确定的攻击威胁生成告警信息。告警数据关联示意图如图 2 所示。

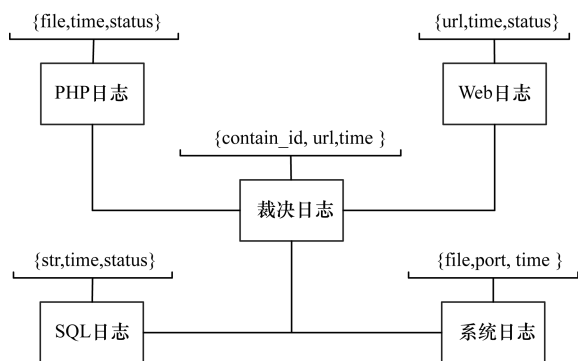


图2 告警数据关联示意图

在裁决日志中记录裁决不一致程度、执行体索引、裁决访问 url、执行裁决时间等裁决信息数据;在 PHP 应用日志中记录响应时间、执行文件、PHP 解析结果状态等程序代码执行数据;在 Web 服务日志中记录响应时间、响应 url 等字段、响应状态等应用服务运行数据;在 SQL 应用日志中记录响应时间、SQL 执行语句、SQL 执行结果状态等 SQL 语句处理结果数据;在系统日志中记录系统运行文件、运行端口、运行时间等系统调用过程数据。通过在多个层次中确定威胁产生情况来确立威胁等级。例如,若 Web 服务采用 3 个执行体容器的拟态防御架构,每个执行体具有 4 层:应用逻辑层、Web 服务层、数据存储层和系统架构层。获取异构执行体容器在不同层次产生的异常告警数据,根据威胁产生的层次,威胁等级从高到低依次为系统架构层、数据存储层、Web 服务层和应用逻辑层。根据裁决日志中记录的响应输出不一致程度进行具体的威胁等级划分。

若 3 个执行体处理得到的 3 个执行结果均相同,则认为无攻击威胁,威胁等级为 0;若 3 个执行体处理得到的 3 个执行结果互不相同,则认为攻击在 3 个执行体上均不生效,只在应用逻辑层发现威胁,视为 1 级威胁;在 Web 服务层发现威胁,视为 2 级威胁;在数据存储层发现威胁,视为 3 级威胁;在系统架构层发现威胁,视为 4 级威胁;若 3 个执行体处理得到的 3 个执行结果中有 2 个执行结果相同,并且所述相同的 2 个执行结果与另一个执行结果不同时,则认为攻击在一个执行体上生效,从系统的应用逻辑层至系统架构层则依次视为 5 级~8 级威胁。威胁等级的划分根据拟态防御架构和裁决策略选取的不同进行适应性调整。

3 拟态威胁分类预测方法

将裁决日志和多层次的系统日志融合后,在日志记录中将会存在 contain_id、url、time、ip、port、file 等大量的数据信息。因此,为达到对攻击威胁进行分析分类预测的目的,根据融合日志提取的特征字段,构建历史信息知识库。通过深度学习的方法对深层的数据信息进行挖掘和学习,从而实现对威胁的分类预测^[21]。

神经网络在许多分类任务中取得了较好的结果。在不同的应用任务中,例如手写数字识别、目标分类、语音识别等都具有较好的分类效果,且始终优于其他方法^[22]。对于网络服务中的数据信息,信息整体的逻辑序列有着大量的内容,并且信息之间存在着复杂的时间关联性。循环神经网络(Recurrent Neural Network, RNN)通过将输出的一部分重新输入,可以从以往发生的事件中推理出后续可能发生的事情,能够很好地发现网络数据中的时间关联关系,但是 RNN 在复杂情况下难以得到合理的结果。LSTM(Long Short-Term Memory)模型是一种 RNN 的变型。在 LSTM 网络中能够通过增加单元状态和门限结构的方法,解决距离增长导致 RNN 记忆失效的问题,使 RNN 具备学习长期依赖的能力。在拟态构造的 Web 服务中使用 LSTM 进行分类预测,设立的层次模型包括 Embedding 层、Dropout 层、LSTM 层、Dense 层。通过将拟态裁决产生数据信息附加数据标签的方法进行监督学习。因此,将告警信息作为训练数据集,数据集中每个日志条目将会被描述为正常的访问请求,标记为 0;或是异常的攻击尝试,标记为 1。应用的神经网络分类模型如图 3 所示。

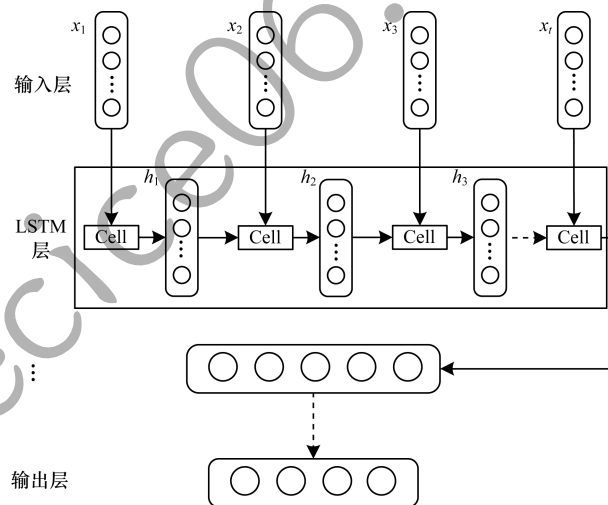


图3 神经网络分类模型

对于生成训练数据的方法,则可以采用模拟用户访问的实际情况进行数据获取。例如,模拟访问“/index.html”“/admin”“/search”等。由于用户访问的数据量是有限的,因此需要将积累够一定数量的日志数据进行训练,才能获得更好的效果。由于使用模拟访问生成训练数据集的方法存在着一些限制,并且为了保证分类结果的应用范围更加广泛,在预处理期间仅提取几个必要的日志字段。这些属性包括“url”“ip”“status”“requestPayload”等。另外,对于请求内容的分析可以采用额外的数据信息、预处理方法和单独分类器来进行分析。为了减少分类预测误差,生成的数据集中包含了大约 10 000 条正常请求日志记录和 10 000 条恶意请求日志记录。将

75% 的数据集作为训练子集,25% 数据集作为验证子集,进行分类预测。经过几轮迭代后,能够获得较高精度的分类预测模型。

4 拟态威胁态势可视化展示

早在 1977 年,文献[23]就详细阐述了可视化对数据的分析具有深刻的影响。对于威胁等级划分后的告警数据,需要借助图形与图像化的手段,将信息更加清晰有效地表达出来。因此,利用数据可视化技术,将每一项数据表示为系统态势元素,大量的数据集构成系统态势展示图,同时以多维数据的形式表示系统态势的各个属性值,从不同维度层面观察分析数据,从而对数据进行更加深入的观察和分析^[24]。拟态威胁态势的可视化采用生成态势展示图的方法,主要包括总体威胁趋势图、平均威胁趋势图、总体请求趋势图、平均请求趋势图、威胁来源分布图和威胁等级排名图等。通过将威胁数据进行威胁等级分类并按照不同的显示要求,将特征聚合,根据需要进行统计的内容的不同,生成不同的特征聚合结果,并进行可视化展示,如图 4 所示。

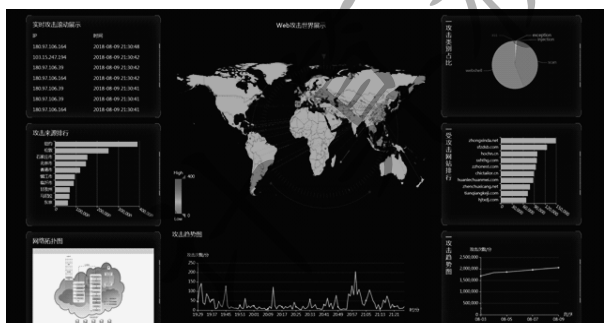


图 4 Web 威胁态势可视化展示

在拟态威胁态势可视化展示中,可将数据类型分为以下 5 类:

1) 对于具有分类属性的数据,每个分类属性都有一个数值。因此,对数据进行分类能够很轻易地掌握数据集的范围。以受攻击网站排行图为例,将威胁感知日志中的网站域名信息进行聚类统计,得出所有不同网络所产生的威胁数量,通过柱状图可明显地观察到各分类的数值大小以及分类中的最值。

2) 对于包含整体和部分关系的数据而言,需要能够清晰地表达出数据的层次结构,并将所有的分组保持在一起进行分析。以攻击类别占比图为例,将威胁感知日志中记录的攻击类别进行分类汇总,计算出攻击分类数量与攻击总量,并通过饼状图将各攻击分类的占比关系进行显示。

3) 对于包含子分类嵌套关系的数据,通常需要引入多维度的数据进行观察,从而得到更加丰富的内涵信息。以执行体状态图为例,如果想要获悉多

个执行体容器的受攻击情况,那么就需要在攻击分类数据中增加执行体容器类别的数据维度,通过多组环形图显示各攻击类型在各执行体容器中运行状态的占比情况。

4) 对于随时间变化的数据,数据什么时间发生的变化,数据变化的程度为多少,以及数据趋势发生变化的原因,都是时序数据需要重点关注的内容。以攻击趋势图为例,将一段时间内的威胁数量进行汇总,然后按照时间顺序将各时间点的威胁数量连接形成曲线图,从而能够清晰地观察攻击发生的数量和攻击发生的趋势。

5) 对于受空间变化影响的数据,数据中所表达的空间位置信息是最为重要的。以攻击世界地图展示为例,将攻击来源地的经纬度信息映射到二维的世界地图中,用不同的颜色在地图上标记攻击来源,通过色彩的差异可以明显地观察到不同攻击来源的数量大小。

5 实验结果与分析

5.1 实验环境

为保证实验的真实性和有效性,在互联网服务环境中实现拟态防御架构的搭建。将访问流量通过负载均衡器分发给拟态网关设备,然后拟态网关设备将请求分发至拟态容器集群中,通过对集群中异构的执行容器进行裁决,并将裁决产生的告警信息发送至信息处理设备进行分类与可视化得到最后的威胁态势。其中,负载均衡设备负责将请求流量分发至拟态防护容器集群中,采用 F5 硬件和 HAProxy 集群相结合的方式,为应用提供更加完善的可用性、加速性和安全性;拟态 Web 服务网关负责提供 Web 服务的安全防护,通过旁路模式接入负载均衡对后端拟态防护容器集群进行安全防护,并以双机热备的形式提高系统容灾能力;信息处理设备与拟态网关设备相接,在其中应用了告警数据关联、威胁分类预测和态势可视化展示方法来对告警数据进行处理。拟态威胁分类与可视化的实验部署架构如图 5 所示。

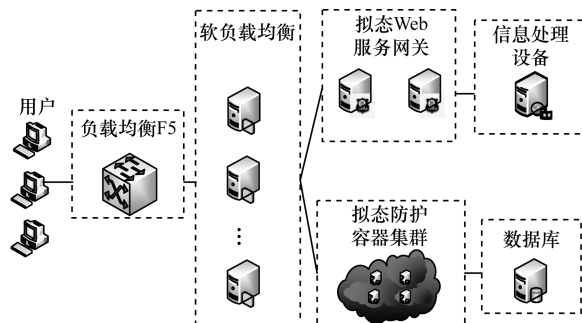


图 5 拟态威胁分类与可视化部署架构

5.2 实验分析

在整个现网运行过程中,通过负载均衡将访问流量和拟态网关设备记录访问流量信息。访问日志

显示每天 100 000 条以上访问记录,负载均衡日志抽样显示 2 GB/h 流量信息以及 6 000 条访问数据信息。具体的日志记录信息包括:

1) 负载均衡流量监测数据,负载均衡设备通过开启访问记录模式记录网站访问流量,以及具体报文信息。

2) 拟态防御威胁感知日志,在拟态设备中记录了通过网站服务的访问数据流量,记录内容存放在访问日志;对网站进行扫描嗅探产生的异常访问记录以及漏洞威胁引起的攻击威胁则记录到威胁感知日志。

对网站运行数据进行分析,根据线上运行期间记录的数据日志,依据数据统计、分类聚合、数据可视化等方法,在去除测试访问记录前提下,对比负载均衡流量监测日志、拟态防御威胁感知入侵检测设备日志记录,分析拟态设备和信息处理设备的威胁数据关联、威胁数据分类和威胁数据可视化的运行效果,如表 1 所示。

表 1 拟态 Web 威胁态势展示功能测试

测试项	测试用例	测试结果
威胁数据关联	1) Web 服务多层间数据关联与拟态各执行容器数据关联; 2) 负载均衡流量监测数据与入侵监测设备日志比对	1) 对拟态 Web 发起攻击,查看到拟态威胁感知日志记录,包含 contain_id、url、time、ip、port、file 字段; 2) 对比拟态设备、负载均衡设备和入侵检测设备的运行数据均一致
威胁数据分类	1) 标记正常数据和异常数据; 2) 构造威胁数据分类器; 3) 预测威胁分类结果	人为进行攻击测试,包括 webshell、SQL 注入、目录爆破、恶意黑页、系统致瘫等多种攻击方法,威胁分类结果和预测结果准确率能够达到 90% 以上
威胁数据可视化	1) Web 实时攻击滚动展示; 2) Web 攻击来源排行展示; 3) Web 攻击世界地图展示; 4) Web 近日攻击量统计展示; 5) Web 平均威胁次数趋势展示; 6) Web 总威胁次数趋势展示; 7) Web 攻击类别占比展示	1) 对拟态 Web 发起攻击,查看到攻击产生的威胁数据; 2) 通过数据调用接口传送数据,测试威胁数据能够正常传输; 3) 访问拟态 Web 威胁态势展示平台,查看页面显示结果均为正常

针对信息处理设备的处理结果,以 2018 年 7 月 30 日—2018 年 8 月 6 日一周内的抽样访问数据为例,一周内拟态 Web 服务网关的总访问量为 1 311 918 次,一周内日访问量从第一天的访问量 153 052 次,通过 2 天逐渐上升至 175 359 次,并于后续 2 天中基本持平,最后在剩余 2 天中又下降至 15 000 次左右。一周内的日访问量变化趋势如图 6 所示。

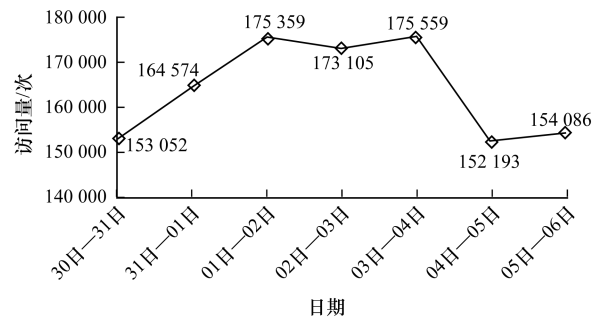


图 6 日访问量变化趋势

一周内拟态 Web 服务网关的日均访问量为 163 990 次。平均每小时访问量在每日 10 时—17 时访问量相对较高,约每小时 10 000 次左右;在每日 17 时后访问量逐渐减少直至次日凌晨 4 时左右达到最小值,约每小时 1 000 次左右,最后在凌晨 5 时—6 时访问量由最小值逐渐恢复。每日平均访问量变化趋势如图 7 所示。

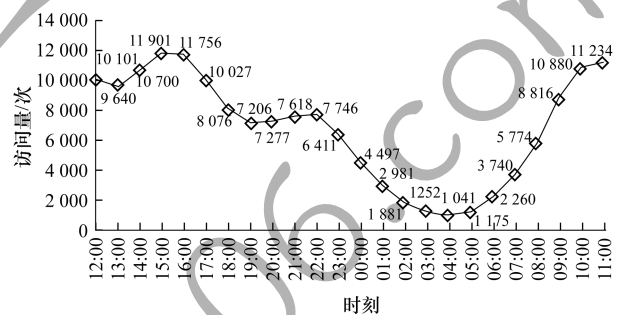


图 7 每日平均访问量变化趋势

通过对信息处理设备的访问流量趋势分析可知,拟态网关设备运行状态稳定正常,并且拟态网关设备能够记录服务自身的整体运行状态,一周内日访问量变化与人们的日常生活习惯相符合,工作时间访问量偏高,非工作时间访问量偏低。

为对拟态网关设备产生的异常访问流量进行分析,于 2018 年 7 月 30 日正式上线运行前进行了攻击测试。在保证拟态网关设备运行稳定正常并且真实准确的情况下,信息处理设备根据拟态防御威胁感知日志的数据记录,分析异常访问流量中的访问类别信息。在拟态网关设备记录的异常访问流量中,将其划分为 4 类,如图 8 所示。

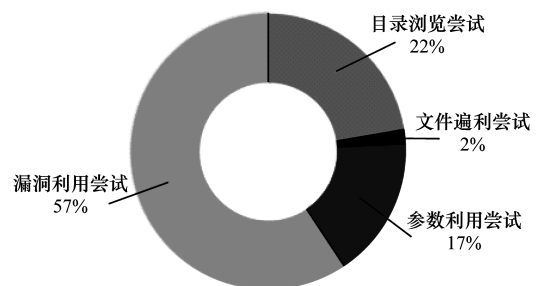


图 8 异常分类结果

拟态网关设备记录的异常访问流量分为以下 4 类:

1) 目录浏览尝试,包括尝试爆破和遍历网站目录的异常访问请求,例如“/test/”“/admin/”等。

2) 文件遍历尝试, 包括探测网站中存在的文件类型的异常访问请求, 例如“/robot.txt”“test.rar”“test/bulletin_2_0.xml”等。

3) 参数利用尝试, 包括尝试利用网站源码中的变量和参数的异常访问请求, 例如“test/search/65535? catId=4968374& type=4& action=list”等。

4) 漏洞利用尝试, 包括尝试利用 php、asp、jsp 类型网站漏洞的异常访问请求, 例如“/test/mytag_js.php”“/index.asp”等。

通过对信息处理设备的异常流量分类结果分析可知, 在 4 类异常访问中, 目录浏览尝试 2 839 次, 文件遍历尝试 237 次, 参数利用尝试 2 108 次, 漏洞利用尝试 7 547 次。容易发现, 漏洞利用尝试的异常访问比例明显多于另外 3 类异常访问。

6 结束语

本文提出一种拟态 Web 威胁告警分类与可视化分析方法, 通过拟态防御的裁决方法生成异常告警数据, 并按照裁决一致程度进行等级划分和分类预测, 进而生成各种拟态防御态势展示图。实验结果表明, 该方法可提高安全工作人员对拟态防御系统阻断的漏洞威胁的分析效率, 且通过对拟态防御系统的安全状态进行显示, 能够及时获悉异常执行体的运行状态, 从而有助于安全人员评估拟态防御效果。由于本文方法针对异常访问无法给出更准确的分析结果, 因此下一步将结合现场快照、文件追踪、数据还原等取证技术做进一步研判分析, 扩大其在产品研发与实践部署中的应用范围。

参考文献

- [1] 中国信息安全测评中心. 国家信息安全漏洞通报[J]. 中国信息安全, 2018(3): 110-113.
- [2] 郭江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
- [3] 林森杰, 刘勤让, 王孝龙. 面向拟态防御系统的竞赛式仲裁模型[J]. 计算机工程, 2018, 44(4): 193-198.
- [4] 张杰鑫, 庞建民, 张铮, 等. 面向拟态构造 Web 服务器的执行体调度算法[J/OL]. 计算机工程, 2019-04-12. <http://www.ecice06.com/CN/10.19678j.issn.1000-3428.0053425>.
- [5] 王伟, 曾俊杰, 李光松, 等. 动态异构冗余系统的安全性分析[J]. 计算机工程, 2018, 44(10): 42-45, 50.
- [6] 全青, 张铮, 张为华, 等. 拟态防御 Web 服务器设计与实现[J]. 软件学报, 2017, 28(4): 883-897.
- [7] 张铮, 马博林, 郭江兴. Web 服务器拟态防御原理验证系统测试与分析[J]. 信息安全学报, 2017, 2(1): 13-28.
- [8] 龚正虎, 卓莹. 网络态势感知研究[J]. 软件学报, 2010, 21(7): 1605-1619.
- [9] TADDA G, SALERNO J J. Realizing situation awareness within a cyber environment [EB/OL]. [2018-10-21]. <https://doi.org/10.1117/12.665763>.
- [10] MAUW S, OOSTDIJK M. Foundations of attack trees[C]//Proceedings of ICICS'06. Berlin, Germany: Springer, 2006: 186-198.
- [11] MOORE A P, ELLISON R J, LINGER R C. Attack modeling for information security and survivability [EB/OL]. [2018-10-21]. <https://www.researchgate.net>.
- [12] SWILER L P, PHILLIPS C. A graph-based system for network-vulnerability analysis [C]//Proceedings of NSOW'98. Washington D. C., USA: IEEE Press, 1998: 71-79.
- [13] HAMID T K A. Attack graph approach to dynamic network vulnerability analysis and countermeasures [EB/OL]. [2018-10-21]. <https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.665736>.
- [14] NOVAK J, NORTHCUTT S. Network intrusion detection[J]. EDPACS, 2000, 27(7): 1-2.
- [15] 张永铮, 方滨兴, 迟悦, 等. 用于评估网络信息系统的风险传播模型[J]. 软件学报, 2007, 18(1): 137-145.
- [16] 陈秀真, 郑庆华, 管晓宏. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885-897.
- [17] 姜伟, 方滨兴, 田志宏, 等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报, 2009, 32(4): 817-827.
- [18] 龚俭, 臧小东, 苏琪. 网络安全态势感知综述[J]. 软件学报, 2017, 28(4): 1010-1026.
- [19] DUTT V, AHN Y S, GONZALEZ C. Cyber situation awareness: modeling the security analyst in a cyber-attack scenario through instance-based learning [C]//Proceedings of IFIP Annual Conference on Data and Applications Security and Privacy. Berlin, Germany: Springer, 2011: 280-292.
- [20] KARAGIANNIS T, PAPAGIANNAKI K, FALOUTSOS M. Blinc: multilevel traffic classification in the dark[J]. ACM SIGCOMM Computer Communication Review, 2005, 35(4): 229-240.
- [21] 李伟明, 雷杰, 董静, 等. 一种优化的实时网络安全风险量化方法[J]. 计算机学报, 2009, 32(4): 793-804.
- [22] RINZLER K, CINO R, SCULLY B. Situational awareness system security features [J]. Computers and Security, 2018, 46(1): 18-31.
- [23] WANG Yuyang, NARASIMHA M, HEATH J R W. MmWave beam prediction with situational awareness: a machine learning approach [C]//Proceedings of the 19th IEEE International Workshop on Signal Processing Advances in Wireless Communications. Washington D. C., USA: IEEE Press, 2018: 145-154.
- [24] KULLMAN K, CWLEY J, BEN-ASHER N. Enhancing cyber defense situational awareness using 3D visualizations [C]//Proceedings of International Conference on Cyber Warfare and Security. Washington D. C., USA: IEEE Press, 2018: 226-234.
- [25] LOPEZCUEVAS A, MEDINAPEREZ M A, MONROY R, et al. FiToViz: a visualisation approach for real-time risk situation awareness [J]. IEEE Transactions on Affective Computing, 2018, 9(3): 372-382.

编辑 索书志