恶意代码取证

恶意代码取证_下载链接1_

著者:(美)奎林娜|译者

出版者:科学

出版时间:2009-7

装帧:

isbn:9787030250667

《恶意代码取证》旨在提出一套完整的恶意软件取证方法和流程，并以Windows和Linux两种操作系统为平台详细介绍了恶意软件取证过程的5个主要的阶段：易失性数据取证保存和检查、内存检查、硬盘检查、恶意软件静态分析、恶意软件动态分析。《恶意代码取证》可用作高等院校信息安全专业及计算机专业本科生、研究生的教材。同时，对于信息安全特别是网络司法取证学界的广大教师、研究人员以及公安网侦人员，《恶意代码取证》同样是不可多得的重要参考资料。

网络犯罪是信息时代的产物。近年来随着计算机以及互联网的普及，尤其是各类金融业务通过因特网不断得到拓展，全球的网络犯罪案件迅速增长。如何有效防范并打击网络犯罪不但是各国立法机关、司法机关及行政机关迫切要解决的问题，而且是计算机技术领域、法学及犯罪学研究领域中最引人关注的课题。

作者介绍:

James M.Aquilina是Stroz Friedberg的行政主管兼代理常驻辩护律师，Stroz Friedberg是一家专门从事计算机取证，电子数据的保存、分析和生产，计算机欺诈响应，滥用响应以及计算机安全的服务与咨询公司。Aquilina先生为了公司的管理经营及其法律事务的处理而劳心劳力，另外全面负责整个洛杉矶办事处的工作。他曾为政府部门、重要法律部门、公司管理和信息系统等部门指导、完成了很多数字取证和电子侦查任务，处理了很多刑事、民事、管理以及内部的公司纠纷案件，如电子伪造、擦除、大面积删除或其他形式的电子数据窃取，机密信息泄露，通过计算机盗窃商业机密和非法电子监视等。他曾经担任第三方中立专家对电子证据进行法院认可的取证检查。Aquilina先生还带头开展了该公司的在线欺诈和职权滥用调查，并定期组织技术和战略磋商会议，以保护计算机网络免受间谍软件和其他入侵软件、恶意软件和恶意代码、网络欺诈以及其他形式的非法因特网活动的侵害。他博学多知，对僵尸网络、分布式拒绝服务攻击以及其他自动化网络入侵等都有深入了解，这使他能为企业提供解决计算机欺诈和职权滥用事件等问题的咨询和解决方案，以加强其基础设施的保护。

目录: 第1章 恶意软件事件响应：易失性数据收集与实时Windows系统检查第2章 恶意软件事件响应：易失性数据收集与实时Linux系统检查第3章 内存取证：分析物理内存和进程内存获取取证线索第4章 事后取证：从Windows系统中搜索并撮恶意软件以及相关线索第5章 事后取证：从Linux系统中搜索并撮恶意软件以及相关线索第6章 法律规范第7章 文件识别和构型：Windows系统中可疑文件的初步分析 第8章 文件识别和构型：Linux系统上可疑文件的初步分析 第9章 Windows平台下可疑软件分析第10章 Linux平台下可疑程序分析
・・・・・・(收起)

恶意代码取证_下载链接1_

标签

取证

security

安全

计算机

信息安全

eBook

Security

Owned

评论

取证入门书，包括Windows和Linux两大平台

恶意代码取证_下载链接1_

书评

恶意代码取证_下载链接1_