<<恶意代码取证>>

图书基本信息

书名：<<恶意代码取证>>

13位ISBN编号：9787030250667

10位ISBN编号：7030250664

出版时间：2009-7

出版时间：科学

作者：(美)奎林娜|译者:彭国军//陶芬

页数：542

<<恶意代码取证>>

内容概要

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。
　本书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。
本书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，本书同样是不可多得的重要参考资料。

作者简介

作者：(美)奎林娜(AquilinaJamesM.) Eoghan Casey Cameron H.Malin 等 译者：彭国军 陶芬James M．Aquilina是Sttoz Friedberg的行政主管兼代理常驻辩护律师，StrozFriedberg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。
在加入Stroz Friedberg之前，Aquilina先生是美国加利福尼亚州中部地区联邦检察官办公室刑事司的一名助理检察官，在那里他主要负责网络和知识产权犯罪科与计算机和电子通信方面相关的工作。
他还担任了洛杉矶电子犯罪特遣部队成员和计算机入侵工作组（一个机构间的网络犯罪响应组织）负责人。
在担任助理检察官期间，．Aquilina先生负责调查并监督与计算机入侵犯罪、拒绝服务攻击敲诈、计算机和因特网欺诈、侵权犯罪、盗窃商业机密以及其他涉及盗窃和滥用个人职权等行为相关的起诉案件。
Aquilina先生主持参与过很多著名的网络犯罪调查案例，例如美国第一例起诉利用僵尸网络进行牟利的犯罪案例，“地下僵尸管理者”通过转卖其所控制的受感染计算机大军用以发动攻击、发送垃圾邮件或秘密安装广告软件来牟利：他曾推进陪审团就第一起与数码摄像机使用相关的刑事版权侵犯案件进行定罪；他曾负责监督指导政府对网络犯罪打击活动[Opreation Cyberslam]（一项国际入侵犯罪调查，主要调查雇佣黑客针对在线商业竞争者进行计算机攻击等犯罪行为）的起诉；他也曾协助美国洛杉矶相关检察机关收集和分析当地恐怖组织的相关电子证据。
在其于美国联邦检察官办公室工作期间，Aquilina先生同时也任职于重大欺诈和恐怖主义，有组织犯罪科，调查和审判了很多复杂案件，例如他曾审判过一起重大的国税局税务官和会计师联合腐败案件；他曾起诉法国里昂信贷银行欺诈一家现已解散的保险公司的赔偿，并为之昭雪：他还以勒索和绑架罪审判过一个亚美尼亚有组织犯罪集团。
随着2001年9月11日袭击事件的发生，Aquilina先生开始协助联邦调查局紧急行动中心法律科的组建和运作。
Aquilina先生在从事公共服务之前，曾在纽约的Richards、Spears、Kibbe＆Orbe律师事务所工作，当时主要负责解决联邦白领工作问题和纽约州的刑事、管理问题。
Aquilina先生也曾担任过十分受人尊敬的加利福尼亚州南部的美国地方法院法官Irma E．Gonzalez的法律助理。
他是乔治敦大学的优秀学士，美国加利福尼亚大学伯克利分校法学院的法学博士，当时他还是理查德厄斯金的学术研究员，担任了《加利福尼亚州法律审查》（califomiaLawReview）的文章编辑和执行委员会成员。
他目前担任国际电子商务顾问理事会（电子商务理事会）网络法律问题的名誉理事会会员，该组织提供CEH（道德黑客认证）和CHFI（黑客法医调查员认证）认证，引领世界各地的安全行业专家。
Eoghan Casey是一位事件响应和数字取证分析专家，经常在大面积的调查范围（包括国际范围内的网络入侵）内开展安全漏洞响应和数字证据分析工作。
他在数字取证方面有丰富的经验，能够根据安全漏洞响应确定计算机入侵的起源、性质和范围，并利

用取证与安全技术来维护受害网络的安全。
他曾研究过数百种数字取证过程中可获得的证据，包括电子邮件和文件服务器、手持设备、备份磁带、数据库系统和网络日志等。
Casey先生是其研究领域的权威，经常在美国和国外相关专业杂志或会议上撰写相关论文并发表演讲，如数字取证研究研讨会、高科技犯罪调查协会、搜索、IT安全和Infragard等会议。
他曾编写了一本十分流行的教科书：《数字取证和计算机犯罪：取证科学、计算机与网络》（学术出版社，2004年）。
他还是《计算机犯罪调查手册》的编辑，并且合著过《儿童剥削和色情调查》一书。
Casey先生现在担任国际期刊《调查取证》的总编辑，该期刊按季度出版数字取证和事件响应方面的文章。
作为Stroz Friedberg的数字取证调查总指导，Casey与其他人一起管理该公司在计算机取证、计算机犯罪响应和紧急事件响应领域的技术业务。
此外，他还积极参与待审民事和刑事案件的作证，并提交专家报告以为计算机和网络犯罪案件的审判而向大陪审团作证。
Casey先生还带头开展Stroz Friedberg公司外部和内部的各种取证培训项目并担任培训负责人。
在Casey到Stroz Friedberg公司工作之前，他曾作为顾问在许多涉及与凶杀、剥削儿童和其他类型案件相关的网上犯罪活动和数字证据的刑事调查中协助执法部门办案。
Casev于1999年至2002年间曾在耶鲁大学担任信息安全主管，并在后续咨询工作中负责脆弱性评估，处理关键安全漏洞，部署和维护入侵检测系统、防火墙和重要的公共基础设施，制定相关政策、规程和教育项目。
自1996年以来。
Casey先生一直通过在线和实地训练的方式提供培训服务，其课程涵盖了数字取证、事故响应和入侵调查。
Casey先生于1991—1995年间还曾在美国航天局的极端紫外线探测卫星项目中担任高级研究助理和卫星操作员，负责编写与自动执行日常、安全性要求很高的卫星操纵流程相关的计算机程序，建立并维护一个Sybase的sQL数据库。
Casey先生毕业于加州大学伯克利分校的机械工程专业，并获得纽约大学教育传播与技术专业硕士学位。
Cameron H．Malin是联邦调查局分配给美国加利福尼亚州洛杉矶的网络重案组的特别代理，主要负责调查计算机入侵和恶意代码等问题。
Malin先生是一位通过国际电子商务顾问理事会（电子商务理事会）认证的道德黑客（CEH认证），是一位通过国际信息系统安全认证协会（“（ISC）2”）认证的信息系统安装专家（CISSP），还是一位通过SANS研究机构认证的资深逆向工程恶意软件分析专家、资深系统入侵分析员、资深故障处理员和资深取证分析员。
Malin先生目前是数字取证国际期刊（UDE）的编委会成员和信息保障技术分析中心（IATAC）的主题专栏专家。
就职于美国联邦调查局之前，Malin曾是佛罗里达州迈阿密的国家检察官助理（ASA）和美国司法部长特别助理，专门从事计算机犯罪的起诉。
在其作为国家检察官助理的任职期间，Malin先生也担任了乔治华盛顿大学的硕士课程《计算机欺诈调查》的助理教授。
本书中由Cameron Matin所提及的相关技术、工具、方法、观点和意见都仅代表其个人意见，并不代表美国司法部、联邦调查局，甚至美国政府。
联邦政府或者任何联邦机构不以任何方式对此书或其内容进行支持。
译者简介：彭国军，男，1979年11月生，湖北荆州人。
武汉大学计算机学院教师、信息安全博士。
2001年起从事恶意软件及防护技术研究，曾协助公安机关进行多起网络犯罪案件的取证工作；2004年主编信息安全专业本科教材《计算机病毒分析与对抗》（“十一五”规划教材），参编和翻译的著作

包括《计算机网络管理实用教程》、《信息安全原理与实践》等。
主持多个省部级网络与安全科研项目，并参与多个国家“863”项目与国家自然科学基金项目。
目前已发表信息安全方向科研与教学论文近20篇，各类安全技术文章近20篇。
研究方向包括恶意代码、网络攻防、软件可信等。

<<恶意代码取证>>

书籍目录

章节摘录

插图：73．起草者充分地讨论这些设备是否应该限制为专为犯罪而设计的设备（因此不包括多功能设备）。
这样考虑太过狭窄，可能导致在犯罪诉讼中举证困难，不能实际适用或仅适用于少数案例。
包含所有设备的方案（即使它们是合法生产和分配的）也被拒绝。
只有主观因素有意进行计算机犯罪才会实行惩罚，这种在资金犯罪中常使用的方式未获通过。
对该协议一种合理的折中方法是根据各实例（实例中设备是客观设计且是专为犯罪行为设计的，因此多重功能的设备不被包括在其中）限定其范围。
74．第一段a．ii将生产、销售、获得使用权、进口、分发或获取电脑密码及类似的数据以使系统的某部分可以访问使用的行为定义为犯罪。
75．第一段b举出了占有第一段a．i，a．ii列举的条目的犯罪行为。
缔约方允许通过法律来要求拥有这类物品的数目必须达到一定限度。
拥有的数量直接体现了犯罪意图，因此缔约方需要谨慎决定所要求的条目数目。
76．犯罪需要证明它是故意且是非授权的。
为了避免对设备在生产和投放市场的合法用途的错判，如系统对攻击发起的反击，需要对犯罪进行更加严格的定义。
除了一般意图，也需要对特殊意图以确定设备用于犯罪的目的，见协议的第2～5章。
77．第二段中清楚的指出用于授权测试或保护计算机系统的工具并不在条款的保护之下。
这一概念已被标志为“没有权限”。
例如，企业用来控制信息可靠性和测试系统安全的测试设备和网络分析设备，这些用于合法目的的会被认为“拥有权限”。

<<恶意代码取证>>

编辑推荐

《恶意代码取证》特色：第一本详细描述恶意代码取证技术的作品，获得2008 Bejtlich最佳图书奖（Winner of Best Book Bejtlich Read in 2008），《恶意代码取证》作者参与了许多恶意入侵案件的调查审理工作，具有丰富的实践经验，全书结合实例对相关的技术和工具进行说明，同时给出相关法律思考、法律后果及必要的治理方法。

版权说明