|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **时 间** | **作 者** | **文 章 题 目** | **对 抗 方 法** | **关 键 词** | **不 足** |
|  | 2002 | M. Shaw, S. D. Gribble | Reverse Firewalls in Denali | 阻止本机向未知的或未授权的地址发起连接 | reverse firewall | 不能区分正常的应用（P2P应用会向未知的地址发起连接）和间谍软件的区别[] |
|  | 2004 | Wang et al. | [Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management]((2004)%20Gatekeeper：Monitoring%20Auto-Start%20Extensibility%20Points%20(ASEPs)%20for%20Spyware%20Management.pdf) | 基于行为的方法。利用间谍软件（随操作系统或多数常用应用程序）自启动的行为特点检测 | ASEP | 单一行为检测，FP较高；检测由用户活动触发的间谍软件时效果不好[] |
|  | 2004-T | Wang et al. | [Strider GhostBuster: Why It’s a Bad Idea for Stealth Software to Hide Files]((2004-T)%20Strider%20GhostBuster：Why%20It's%20a%20Bad%20Idea%20for%20Stealth%20Software%20to%20Hide%20Files.pdf) | 基于行为的方法。使用“outside the box”的思想，分别从干净系统和感染（rootkit）系统中获取文件快照（利用“dir”命令），分析其中的差异，用来发现隐藏的文件 | outside the box |  |
|  | 2004 | Borders et al. | [Web Tap：Detecting Covert Web Traffic]((2004)%20Web%20Tap：Detecting%20Covert%20Web%20Traffic.pdf) | 基于行为/流的方法。根据正常的web请求模式（训练获得），分析主机外发的HTTP流量，发现潜在的间谍软件 | outbound HTTP traffic | 对不使用HTTP协议的间谍软件无能为力；对blend in with legitimate behavior的间谍软件无能为力[][6] |
|  | 2006 | Kirda et al. | [Behavior-based Spyware Detection]((2006)%20Behavior-based%20Spyware%20Detection.pdf) | 基于行为的方法。动静态分析结合检测利用IE的BHO或工具栏接口的间谍软件  1、动态分析：通过监测浏览器函数调用发现插件是否在收集信息  2、静态分析：分析可疑插件二进制码中是否出现导致信息泄露的库函数调用 | BHO, toolbar interface | 检测由用户活动触发的间谍软件时效果不好[] ；方法不具有一般性，局限于特殊的环境（IE的BHO）[] ；静态分析易被混淆技术逃避，且仅知道是否有信息泄露，不知道具体是什么信息泄露，去向是哪里[14] |
|  | 2006 | Borders et al. | [Siren: Catching Evasive Malware]((2006)%20Siren：Catching%20Evasive%20Malware.pdf) | 基于行为/流的方法。利用VM技术向待检测系统中注入honeytoken（已知的网络请求序列），并将这些序列与实际的网络负载进行比较。若实际的网络负载与预期的不符，则产生报警。利用白名单降低伪肯定率 | blend in, mimicry attack | 静态的honeytoken容易被间谍软件发现规律，并无视其刺激[]；不能发现不使用网络发送敏感信息的间谍软件[] |
|  | 2006 | H. Wang, S. Jha et al. | [NetSpy: Automatic Generation of Spyware Signatures for NIDS]((2006)%20NetSpy：Automatic%20Generation%20of%20Spyware%20Signatures%20for%20NIDS.pdf) | 基于行为/流的方法（白名单处理正常程序的流量）   1. 用预定输入获取干净系统的外发网络流量 2. 用同样的输入，从感染系统中获取流量 3. 差别分析（分离非可信程序生成的流量，并将其内容和用户输入关联），发现间谍软件 4. 自动生成间谍软件的网络级别的特征 | diﬀerential analysis, automatic signature generation | 仅能检测感染IE的基于HTTP的间谍软件 []；NetSpy在每个程序安装后运行，因此不能有效发现多个、时间触发的或特定输入触发的间谍软件[]；不能保证在获取参照点时系统是干净的 |
|  | 2006 | M. Wu, Y. Huang, Y. Wang et al. | [A Stateful Approach to Spyware Detection and Removal]((2006)%20A%20Stateful%20Approach%20to%20Spyware%20Detection%20and%20Removal.pdf) | 使用预设的规则监控系统所有进程的（注册表、文件、进程、网络）Win API调用，并将重新安装或恢复被删除的自启动扩展点（ASEP）作为关键事件，检测自我修复的间谍软件进程，并更新规则阻止间谍软件自恢复，最终终止间谍软件进程。 | ASEP, self-healing | 需与其它反间谍软件配合，由第三方反间谍软件提供首次发现间谍软件的信息 |
|  | 2007-J | M. Wu, Y. Wang et al. | [Self-Healing Spyware: Detection, and Remediation]((2007-J)%20Self-Healing%20Spyware：Detection,%20and%20Remediation.pdf) |  |  |  |
|  | 2007 | Lim | [Defeat Spyware with Anti-screen Capture Technology using Visual Persistence]((2007)%20Defeat%20Spyware%20with%20Anti-screen%20Capture%20Technology%20using%20Visual%20Persistence.pdf) | 使用抗截屏技术的虚拟键盘 | on-screen keypad | 仅能防御从用户输入设备获取敏感信息的间谍软件，不能防御类似于IE插件的间谍软件 |
|  | 2007 | Provos et al. | [The Ghost in the Browser-Analysis of Web-Based Malware]((2007)%20The%20Ghost%20in%20the%20Browser%20Analysis%20of%20Web-Based%20Malware.pdf) | 通过在虚拟机中打开被挂马的网页，监测HTTP fetches（用其他反病毒引擎）及VM状态的变化（创建进程、注册表及文件改变），检测在用户不知情的情况下自动安装的基于web的恶意软件 | web-based malware | 主要是预防基于web的间谍软件感染；对隐蔽性强的间谍软件（模仿攻击）效果不好；依赖第三方反病毒引擎 |
|  | 2007 | Li et al. | [SpyShield: Preserving Privacy from Spy Add-Ons]((2007)%20Spyshield：Preserving%20Privacy%20from%20Spy%20Add-Ons.pdf) | 干扰而非检测：在敏感信息出现（敏感区域）时，通过实施用户定义的安全策略，保证敏感信息流向非可信的程序（组件），能防止间谍插件通过约定的接口（如API）获取敏感信息或直接读取主程序的内存以获取敏感信息。 | spy add-ons, spyware containment | 仅能干扰插件式的间谍软件，对独立的间谍软件（如keylogger）无能为力； |
|  | 2007 | Chandrasekaran et al. | [SpyCon: Emulating User Activities to Detect Evasive Spyware]((2007)%20SpyCon：Emulating%20User%20Activities%20to%20Detect%20Evasive%20Spyware.pdf) | 基于行为/流的方法。针对现有间谍软件blend in with legitimate behavior的特点，使用随机honeytoken模拟用户正常的网络活动，以此诱导间谍软件的网络活动，通过分析这些网络流量与干净系统网络流量的差异检测间谍软件 | honeytoken, user activity | 不能发现不使用网络发送敏感信息的间谍软件[] |
|  | 2007 | M. Egele, C. Kruegel, E. Kirda et al. | [Dynamic Spyware Analysis]((2007)%20Dynamic%20Spyware%20Analysis.pdf) | 基于行为的方法。使用动态污点分析的方法监控敏感信息的流动，当有插件试图将这些敏感信息泄露到浏览器地址空间之外时，将该插件视为间谍软件，同时继续追踪敏感信息，以获得该信息泄露的去向 | information flow, dynamic taint analysis | 方法不具有一般性，局限于特殊的环境（IE的BHO）； |
|  | 2007-M | J. Jensen | Detection of Hidden Software Functionality |  |  |  |
|  | 2008 | Saroiu et al. | [SpySaver: Using Incentives to Address Spyware]((2008)%20SpySaver：Using%20Incentives%20to%20Address%20Spyware.pdf) | 通过生成大量假冒的信息（利用VM模拟虚拟用户上网活动in design）降低间谍软件所窃取信息的价值，达到混淆的目的 | incentive | 由于能够验证信息，keylogger这样的间谍软件不太受影响 []；伪造信息产生于虚拟用户，容易被间谍软件识破[]；动机清除错误，系统会失效 |
|  | 2008 | Arastouie et al. | [Hunter: An Anti spyware for windows Operating System]((2008)%20Hunter：An%20Anti%20spyware%20for%20windows%20Operating%20System.pdf) | 收集系统资源的使用情况，并利用预先设置的静态规则，发现间谍软件 | policy | 静态方法；反隐能力弱；没有实验支撑 |
|  | 2008 | Han et al. | [HoneyID：Unveiling Hidden Spywares by Generating Bogus Events]((2008)%20HoneyID：Unveiling%20Hidden%20Spywares%20by%20Generating%20Bogus%20Events.pdf) | 使用伪造用户活动（多角度：键盘、鼠标、网络活动等）的方法，引诱间谍软件实施动作。基于引诱阶段和非引诱阶段动作的不同，计算伪造事件的响应比，进而发现潜在的间谍软件。 | enticement strategy, bogus events | 针对dialog spyware；正常的软件亦会有键盘、鼠标、网络等行为，而该方法采用的白名单方式不足以区分未知的软件是否属于间谍软件（且该方法必须有待检测间谍软件敏感的行为的先验知识），从而限制了该方法的应用范围 |
|  | 2009 | Wang et al. | [Interests-based Spyware Detection]((2009)%20Interests-Based%20Spyware%20Detection.pdf) | 根据发生在数据上的程序动作（复制粘贴和传送），使用逆向云发生器表达程序的兴趣。如果兴趣集中在敏感数据上，该程序很可能是间谍软件 | interest, cloud model | 数据的分类（根据关键词）要人为进行；监控动作不宜实施； |
|  | 2009 | Li et al. | [A Static Method for Detection of Information Theft Malware]((2009)%20A%20Static%20Method%20for%20Detection%20of%20Information%20Theft%20Malware.pdf) | 使用静态污点分析的方法，检测信息窃取恶意软件 | taint analysis |  |
|  | 2010-J | N.Lavesson, M. Boldt  et al. | [Learning to Detect Spyware using End User License Agreements]((2010-J)%20Learning%20to%20Detect%20Spyware%20using%20End%20User%20License%20Agreements.pdf) | 利用学习算法对软件发行商提供的软件附带的最终用户许可协议（EULA）进行学习（服务器训练，各主机定期下载知识），并利用训练好的分类器分类，以发现捆绑的间谍软件，使之无法安装 | EULA, document classification | 要求软件必须附带EULA，但许多软件（开源软件）不满足这个条件；无法应对未知/零日攻击 |
|  | 2010-J | 李佳静 et al. | [一种隐式流敏感的木马间谍程序检测方法]((2010-J)%20一种隐式流敏感的木马间谍程序检测方法.pdf) | 从隐式流的角度出发，使用静态污点传播分析方法检测截获用户按键信息的间谍软件（Keylogger） | 隐式流，污点分析 | 静态污点传播分析不能对抗混淆技术 |