通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

王 志,蔡亚运,刘 露,贾春福.基于覆盖率分析的僵尸网络控制命令发掘方法[J].通信学报,2014,(1):156~166

基于覆盖率分析的僵尸网络控制命令发掘方法

Using coverage analysis to extract Botnet command-and-control protocol

投稿时间： 2013-03-14

DOI：10.3969/j.issn.1000-436x.2014.1.018

中文关键词：恶意代码分析 僵尸网络 命令与控制协议 基本块 覆盖率

英文关键词:malware analysis Botnet command-and-control protocol code block code coverage

基金项目:国家自然科学基金资助项目(61300242，61272423，60973141)；国家重点基础研究发展计划(“973”计划)基金资助项目(2013CB834204)；中央高校基本科研业务费专项基金资助项目(65121012)；南开大学—腾讯联合基金资助项目(2011-11)

作者	单位
王 志，蔡亚运，刘 露，贾春福	南开大学 计算机与控制工程学院，天津 300071

中文摘要:

从僵尸程序执行轨迹对二进制代码块的覆盖规律出发，提出了一种僵尸网络控制命令发掘方法。通过分析执行轨迹对代码块的覆盖率特征实现对僵尸网络控制命令空间的发掘，根据代码空间是否被全覆盖来验证发现的僵尸网络命令空间的全面性。对僵尸网络Zeus、SdBot、AgoBot的执行轨迹进行了代码块覆盖率分析，结果表明，该方法能够快速准确地发掘出僵尸网络的控制命令集合，时间和空间开销小，且该命令集合所对应的执行轨迹可以覆盖僵尸程序95%以上的代码空间。

英文摘要:

There are some inherent patterns in the bot execution trace coverage of basic blocks. Using these patterns, an approach was proposed to infer Botnet command-and-control protocol (C&C protocol). Without intermediate representation of binary code and constraints solving, this approach has a lower time and space overhead. This coverage analysis approach was evaluated on 3 famous Botnet: Zeus, Sdbot and Agobot. The result shows that this approach can accurately and efficiently extract the Botnet control commands. And the completeness of the extracted control commands could be verified by checking whether all available basic blocks in bot are covered by the traces triggered by the control commands.

查看全文 查看/发表评论 下载PDF阅读器

关闭