doi:10.3969/j.issn.1002-0802.2017.10.034

SOHO 路由器后门分析与检测研究综述 *

谭云木，王轶骏，薛 质

（上海交通大学 电子信息与电气工程学院，上海 200240）

摘 要：SOHO 路由器是家庭和小型办公网络中的关键组成部分，其生产和使用过程中面临被植入后门的威胁。SOHO 路由器后门可能造成通信监听、信息泄漏、拒绝服务等危害，给网络安全带来极大的挑战。在系统介绍 SOHO 路由器后门概念基础上，总结 SOHO 路由器后门的定义与分类方法，结合多个具体样本，分析后门的设计方法与技术特点，并对目前的后门检测技术进行分析比较，阐述各类方法的优缺点，最后展望了 SOHO 路由器后门未来的研究方向。

关键词：SOHO 路由器后门；概念；实例分析；检测技术

中图分类号：TP393 **文献标志码**：A **文章编号**：1002-0802(2017)-10-2324-09

Analysis and Detection of SOHO Router Backdoor

TAN Yun-mu, WANG Yi-jun, XUE Zhi

(School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: SOHO Router, as the key component of home or small-size office network, now faces the threat of backdoor implantation in its production and operation process. The backdoor of SOHO Router would bring great challenge to the security of network involving communication monitor, information leakage and denial of service. Based on systematical introduction of its backdoor concept, the backdoor definition and common classification of SOHO Router is summarized. And in combination of several specific samples, the backdoor design methods and technical characteristics are discussed. Then the general detecting methods as well as their advantages and disadvantages are compared and expounded. Finally, the future research direction for the backdoor of SOHO router is forecasted.

Key words: SOHO router backdoor; concept; case analysis; detecting methods

0 引 言

伴随着网络技术的高速发展，越来越多的个人电脑、手机、平板甚至智能电视等 IoT（Internet of Things）设备需要接入网络 [1]。智能设备的轻量化和处理能力的进一步提升，使得用户可以更加轻易地通过各类 IoT 设备检测和控制自身和周边的事物 [2]。稳定、可靠的网络环境是实现网络互联的基础，因此 SOHO（Small Office/Home Office）路由器作为互联网和 IoT 设备通信的中转节点和传输媒介，是物联网的中心，直接关系着网络质量和其他 IoT 设备的信息安全 [3-4]。SOHO 路由器的重要意义和庞大基数催生了针对 SOHO 路由器的后门，且由于路由器的中心地位和用户的长期忽视 [5]，较之一般计算机后门而言，SOHO 路由器后门的隐蔽性、破坏性都更高。

具体而言，如果 SOHO 路由器设备中有后门潜伏，那么攻击者便可以获取路由器的控制权限，从而对设备的核心设置进行篡改，监听和劫持用户流量，进而窃取用户敏感信息 [6]。同时，考虑到 SOHO 路由器是网络服务的基础，因而任何一个接入该路由器网络中的 IoT 设备节点都将面临类似的安全威胁 [7-8]。此外，SOHO 路由器等 IoT 设备的巨

* 收稿日期：2017-06-07；修回日期：2017-09-11 Received date:2017-06-07;Revised date:2017-09-11

大数量，是现阶段该类设备后门的另一大特点，其庞大的基数为攻击者提供了更多利用方式，甚至发起了 DDoS（Distributed Denial-of-Service）攻击，使目标网络陷入瘫痪，给国民经济带来巨大损失[9]。对于路由器后门造成的危害，已不乏先例可循。据国家互联网应急中心（CNCERT）发布的《2013 年我国互联网网络安全态势综述》显示，2013 年涉及通信网络设备的软硬件漏洞 505 个，数量较 2012 年增长 1.5 倍。分析验证后发现，D-LINK、Cisco、Linksys、Netgear、Tenda 等多个厂商的路由器产品存在后门漏洞，攻击者可由此直接控制路由器，进一步发起 DNS 劫持、窃取信息、网络钓鱼等攻击。2016 年 10 月，美国位于东海岸的 DNS 基础设施遭到了由名为“Mirai”的恶意代码感染的 IoT 设备僵尸网络发起的 DDoS 攻击，导致包括 Dyn、Github 等众多网络服务受影响，甚至一度无法访问。据统计，在这次 DDoS 攻击中，涉及到的 IP 地址遍及全球，数量达到千万级，其中大多数是 SOHO 路由器等 IoT 设备[10-12]。研究表明，Mirai 通过字典攻击破解设备上运行的 Telnet/SSH 服务密码，从而植入后门程序，随后等待攻击者发出指令进行 DDoS 攻击。

SOHO 路由器后门本身具有较高的隐蔽性和破坏性，其分析和检测技术的研究对保障信息安全具有重要意义，已经成为信息安全研究领域中备受关注的课题。

1　SOHO 路由器后门的概念

1.1　定义

SOHO 路由器后门指的是任何用于秘密绕过路由器系统中正常身份认证流程而获取访问权限的方法。SOHO 路由器后门的产生方式一般分为两种情况。一是攻击者利用漏洞、密码爆破等方式获得路由器控制权限后植入的恶意代码，用于维持访问。例如，安全公司 FireEye 在 2015 年 9 月报告的名为“SNYful Knock”的新型 Cisco 路由器后门，即攻击者通过弱口令登录并替换固件的方式植入后门[13]。另一种后门则是在 SOHO 路由器厂商在系统开发过程中用于快速修改和测试设备的隐秘通道，在产品发布后没有去除而遗留下来形成。2013 年，Heffner 在博客中披露的 D-Link 特殊 User-Agent 后门是其中的代表。攻击者仅需要将浏览器 User-Agent 标志修改为 xmlset_roodkcableoj28840ybtide，即可无需经过验证而访问路由器的 Web 管理界面，进而可修改路由器设备设置[14]。图 1 为该后门在全球范围内感染的 SOHO 路由器设备分布。

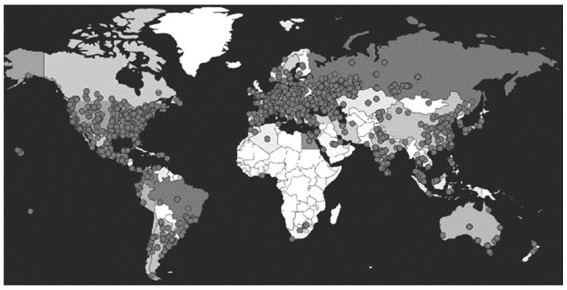

图 1　D-Link 特殊 User-Agent 后门全球范围影响

攻击或开发者在路由器设备植入后门后，即保留了一条进入系统的隐秘通道。该通道可以实现以下目的[15]：

（1）绕过安全性控制，简化渗透或测试过程。后门植入后，可在路由器系统中长期秘密隐藏运行。即使系统环境已经发生变化，如在配置修改、口令变更后，攻击者都能凭借植入的后门再次渗透系统，从而无需再次寻找新的攻击方式。

（2）隐藏自身以及攻击者操作痕迹。考虑到后门是作为隐秘通道而存在的，如果失去了隐蔽性，后门的功能也就无从谈起[16]。因此，后门还会通过相应手段来隐藏自己和入侵者的活动痕迹来躲避日志及检测系统，从而降低被发现的可能。

（3）传播和植入恶意代码。对于很多攻击者，通过后门可以远程控制系统，从而简化分发和植入恶意代码的流程[17]。病毒、木马、网络蠕虫等恶意代码均可以通过后门来快速传播和感染。

1.2　分类

根据 SOHO 路由器后门的不同功能和特点，可以从不同角度对其进行分类。本文试从功能实现、隐藏技术、活动方式三个方面对其分类进行总结，如图 2 所示。

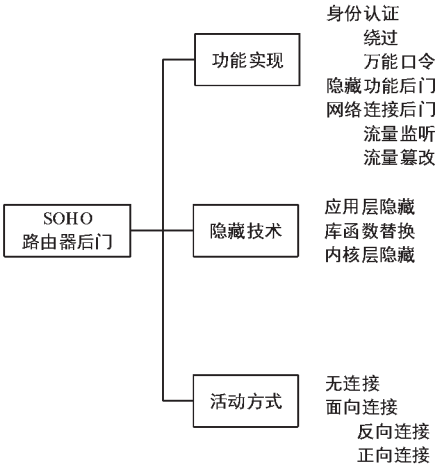

图 2　SOHO 路由器后门分类

按照功能实现进行分类。SOHO 路由器后门可以按照设计目的和功能的不同进行划分，参照 C Wysopal 等对一般后门的分类，最常见的几种后门功能包括 [15]：

（1）身份认证后门，即植入于 SOHO 路由器身份认证系统的后门，允许硬编码的特殊口令绕过认证系统来实现登陆；或者攻击者替换原有的正常登陆程序，在不影响原有身份验证功能基础上，提供触发特殊认证流程的方式进入系统。

（2）隐藏功能后门。此类后门通过在路由器固有功能的正常执行流程上添加额外操作，并通过特殊参数触发这些操作，以实现原本不应该执行的程序逻辑。

（3）网络连接后门。后门程序可以借助 iptables 等功能，在 SOHO 路由器和攻击者之间建立隐秘信道，从而镜像或劫持系统网络流量，发起中间人（Man-in-the-Middle Attack）攻击 [18]。

按隐藏方式进行分类。隐藏方式的不同直接影响后门的隐蔽效果。在应用层，后门主要表现为单独的可执行文件（Executable and Linking Format），在程序执行期间完成窃取隐私数据等功能。但是，后门的活动局限于程序执行周期，容易被发现，隐蔽性不高。一种更好的应用层后门技术是替换合法的路由器系统程序，或者在合法程序中嵌入后门代码以实现额外的功能，并借助于合法程序的伪装来增强后门的隐蔽性。库函数后门是另一种依据操作系统动态链接库的特点而设计的后门。由于几乎所有基于类 Unix 系统的路由器设备都通过动态链接库的方式减少可执行文件体积和运行期间的内存占用，因此可以通过替换系统共享库中关键函数来植入后门 [19]。内核级后门是利用可加载内核模块完成植入，或者路由器内核设计中已经植入了后门。内核是操作系统的核心，内核级后门不仅有非常好的隐藏性，而且借助于内核的控制权限，内核级后门能完成许多应用层后门无法完成的工作 [20]。

还可以按照活动方式划分 SOHO 路由器后门。面向连接型后门首先需要与控制端建立连接，随后传输数据以收发命令、上传敏感信息。无连接型后门是指后门在植入路由器系统后，不会建立数据传输信道，而是等待满足触发条件后（例如收到特定格式的网络数据包、路由器 Telnet 或配置管理页面中特殊字符串输入等），后门再进行身份认证绕过、用户权限提升等工作。无连接型后门需要特定条件才能触发，避免了客户端 / 服务器模式中的信道建立，一定程度上减少了被发现的可能。

2 SOHO 路由器后门举例

从分类来看，SOHO 路由器的设计没有统一的模式。根据不同的应用环境，它的设计方法也有不同。以下通过一些具体的典型 SOHO 路由器后门来说明其设计流程和实现的具体功能。

2.1 Netcore/Netis igdmptd

Yeh 在文献 [21] 中披露，Netcore/Netis 系列路由器在 /bin 目录下内置了一个名为 igdmptd 的后门程序。此程序在路由器上电后自动运行，并在广域网（WAN）端口上监听 UDP 53413 端口。由于该程序在广域网上监听端口，攻击者可以从任何位置对接入互联网的这些 SOHO 路由器设备发起攻击。趋势科技（TrendLabs）通过 Zmap 扫描发现，全球范围内有 200 余万个 IP 地址向互联网开放 UDP 53413 端口，其遍布多个国家和地区 [21]。

通过反编译逆向分析样本可以发现，该 SOHO 路由器后门主要逻辑代码主要包括 [22]：

（1）端口监听。后门程序开始运行后，首先通过 create_server 函数监听 UDP 端口 53413。汇编代码显示，函数首先发起 ioctl 请求，以获取 br0 网络接口绑定的 IP 地址，并将用于监听的网络嵌套字也绑定在这个地址上。

（2）命令接收与执行。这是后门程序的主要工作函数。后门在成功监听端口后，将循环调用该函数直到发生错误退出。在循环内部，首先使用 recvfrom 函数调用接收外部发来的命令数据包，之后根据预定义的命令数据协议解析命令选项，经过对函数流程逆向分析，可得到该后门的通信协议，如图 3 所示。

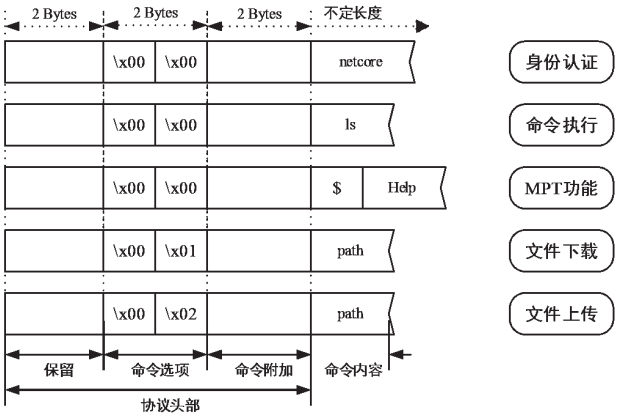

图 3 igdmpt 后门通信协议

成功解析命令后，后门程序将根据命令头部选择相应的函数流程执行命令，最后通过 UDP 协议回传执行结果。通过对该函数的逆向分析可以发现，

该后门可以完成身份验证、任意命令执行、任意文件上传下载和预定义 MPT 命令功能。通过字符串交叉引用、参数分析和函数关联分析，该后门几乎可以读取和篡改路由器系统所有的核心设置，图 4 为分析识别的部分 MPT 功能。

```
LOAD:004138D8  00000006  C  $Help
LOAD:004138E0  0000000A  C  $WriteMac
LOAD:004138EC  00000009  C  $ReadMac
LOAD:004138F8  0000000B  C  $WriteSsid
LOAD:00413904  0000000A  C  $ReadSsid
LOAD:00413910  0000000C  C  $GetVersion
LOAD:0041391C  0000000F  C  $ReadRegDomain
LOAD:0041392C  00000010  C  $WriteRegDomain
LOAD:0041393C  0000000F  C  $ReadWwwPasswd
LOAD:0041394C  00000010  C  $WriteWwwPasswd
LOAD:0041395C  0000000D  C  $ReadChannel
LOAD:0041396C  0000000E  C  $WriteChannel
LOAD:0041397C  00000014  C  $ReadChannelBonding
LOAD:00413990  00000015  C  $WriteChannelBonding
LOAD:004139A8  00000009  C  $TestUsb
LOAD:004139B4  00000009  C  $SetSsid
LOAD:004139C0  00000009  C  $GetSsid
LOAD:004139CC  0000000F  C  $GetGpioStatus
LOAD:004139DC  0000000A  C  $Ifconfig
```

图 4　igdmpt 后门 MPT 功能

2.2　SYNful Knock

文献 [13] 指出，网络安全公司火眼（FireEye）于 2015 年检测出一种名为“SYNful Knock”的路由器植入后门。该后门主要针对思科（Cisco）路由器设备，包含在经过篡改的路由器固件中允许攻击者匿名登陆并从网络中动态加载其他攻击模块，或者进行自我更新。同时，后门还允许攻击者通过特殊构造的 TCP 数据包获得路由器管理员权限。研究表明，该后门没有使用零日攻击（Zero-day exploit），而是借助于默认或其他手段获取的口令合法登陆系统，以固件更新方式来完成后门植入。

SYNful Knock 对路由器固件的修改主要包括：页表缓存（Translation Lookaside Buffer）读写属性修改、挂钩合法函数初始化后门、替换合法函数、替换合法字符串四个部分，如图 5 所示。

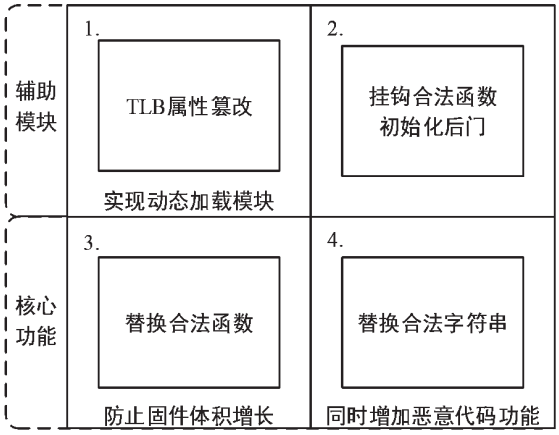

图 5　SYNful Knock 后门修改内容

SYNful Knock 后门的 CnC 功能隐蔽性非常高，需要一系列精心构造的 TCP 报文才能触发，具体的触发流程如下 [23]：

（1）攻击者首先需要向植入后门的路由器设备 80 端口发送特殊的 TCP SYN 数据包，其中序列号（SEQ）和确认号（ACK）之间的差值为 0xC123D。

（2）后门程序收到握手请求后，将序列号与确认号的差值设置为 0xC123E，同时，TCP 中可选字段被硬编码为“02 04 05 B4 01 01 04 02 01 03 03 05”，紧急指针（Urgent Pointer）被设置为 0x01，但 URG 标志并不置位。最后，将 SYN 请求报文中的确认号设置为相应序列号，并返回 SYN-ACK 响应报文。随后的流程与正常三次握手过程无异。图 6 为上述连接建立过程。

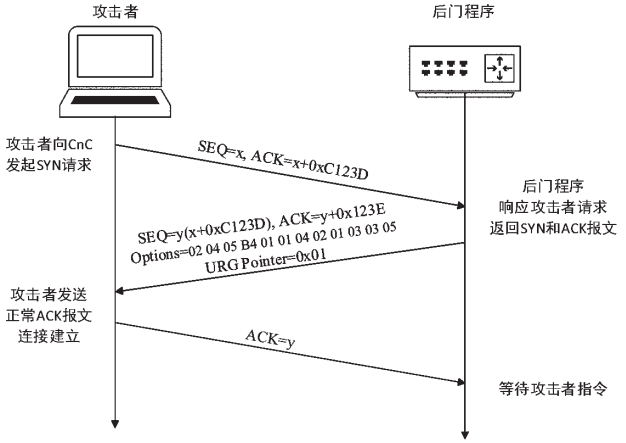

图 6　连接建立

（3）一旦连接建立，CnC 将同样通过特定的 TCP 流发送命令与回传结果。其中，包括置位 TCP 报文的 PSH 与 ACK 标志，在 TCP 报头偏移 0x62 位的地址写入特殊字符串“text”，最后将异或后的控制命令写入距报头 0x67 位的位置。后门的响应值包含在静态 HTTP/HTML 页面中。图 7 为上述命令执行与回传过程。

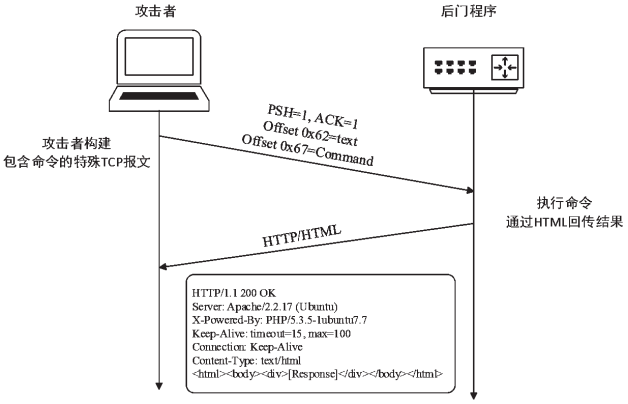

图 7　命令执行

通过以上实例不难发现，SOHO 路由器后门的设计与实现方式众多，其功能也根据设计者需要不一，可用于权限获取、命令执行、恶意代码加载以及其他一些功能。研究现阶段不同 SOHO 路由器后门样本，有利于掌握其植入、隐藏等相关技术特点，从而更好地把握SOHO路由器后门未来的发展方向。

3 检测方法

鉴于 SOHO 路由器后门对网络安全的威胁日益凸显，对其检测方法的研究也成为密切关注的重要议题。但是，由于 SOHO 路由器后门种类繁多，其具体实现没有统一标准，给检测工作带来了相当的难度。同时，就现阶段而言，SOHO 路由器作为一种嵌入式设备，包含文件系统在内的核心内容均以固件的形式存储在闪存（Flash）中。因此，对固件文件的获取和解析是 SOHO 路由器后门检测的基础 [24]。

固件文件的获取主要有两种途径，一是从路由器厂商技术支持网站直接下载，另一种是以硬件接入方式直接从路由器闪存中提取。文献 [25] 中详细介绍了利用 JTAG（Joint Test Action Group）连接 SOHO 路由器主板并提取闪存的方法。

SOHO 路由器的固件一般为二进制数据流文件形式。不同路由器固件的文件布局有所不同，但通常由以下几部分组成：固件头部、引导程序（bootloader）、系统内核、文件系统等，解析流程如图 8 所示。针对固件中二进制流中信息不同偏移量以及魔数（magic number）签名构成的特征，可以实现固件不同主体之间的分离，从而解析出路由器文件系统 [26]。

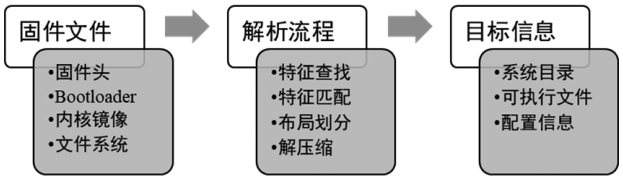

图 8 SOHO 路由器固件解析流程

除手动提取 SOHO 路由器固件外，还可以建立特征值提取规则，实现自动化分析与提取。文献 [27] 中设计并实现了 Binwalk 这一全自动固件分析工具。它的基本原理是：利用 libmagic 动态库获取所有魔数签名列表，同时分段扫描路由器固件文件的内存镜像，对比列表判断每一段是否含有文件魔数标识，最后根据记录的偏移量确定固件文件布局，整体流程如图 9 所示。Zaddach 等在文献中亦介绍了 firmware-mod-kit、FRAK、ERESI framework、signsrch、TrID 等众多可用于SOHO路由器固件分析、提取和逆向工程的工具 [28-30]。

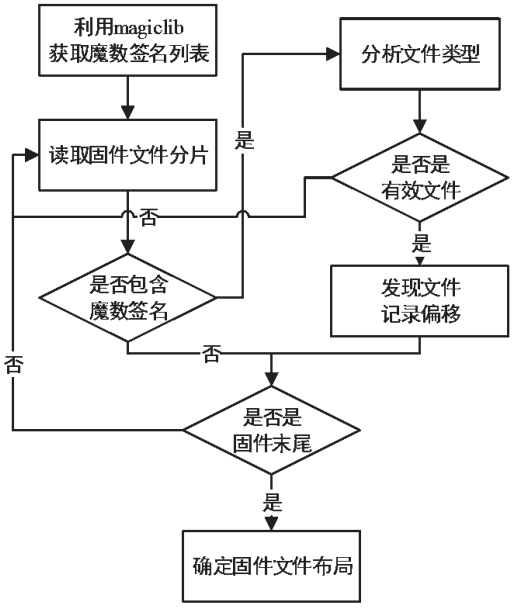

图 9 固件文件系统提取流程

SOHO 路由器固件的核心内容是文件系统，其中包含路由器的全部可执行程序、配置文件等信息。因此，在得到文件系统后，可以尝试进行路由器的后门检测。目前，检测方法主要分为静态检测和动态检测。

3.1 静态检测

静态检测是指在测试源程序或系统在非运行的情况下，通过分析程序的结构和功能信息发现后门特征 [31]。SOHO 路由器后门程序本质上是由计算机指令构成的恶意代码，因此根据是否考虑代码语义，又可以将静态检测分为基于代码特征的分析和基于代码语义的分析。

基于代码特征的分析方法是指采用签名特征匹配、统计特性等算法规则进行分析检测，而不考虑其具体语义。例如，有网络连接功能的 SOHO 路由器后门，在执行期间一般需要监听特定端口或者主动向控制端发起连接请求。对于这种情况，通过交叉引用分析和调用参数分析，可以在后门的代码段（Text）检测到对特定端口的函数调用，或者在代码数据段（Rodata）发现预定义的控制端网络地址。但是，部分后门在设计过程中采用混淆手段对代码进行处理，以对抗特征检测 [32]。这种情况需要进一步对代码进行语义分析。

SOHO 固件中的程序一般为编译后的二进制代码，需要对二进制程序进行语法分析、程序指令

的语义分析，以生成由低级汇编代码组成的控制流图，最后根据获得的控制流图对程序进行语义分析检测 [33]。Christodorescu 等针对恶意代码的重排、加壳和花指令插入等混淆技术，提出了三元操作符检测手段，以排除混淆干扰。该方法对混淆后的 SOHO 路由器后门检测同样有参考意义 [34]。忽朝俭等针对网络套接字和字符串 / 内存操作函数，在 IDA Pro 生成的反汇编代码基础上，提出了一种启发式规则与逆向分析结合的检测技术，讨论了多种典型嵌入式固件后门类型的检测方法，包括非预期功能、隐藏功能、主动网络连接以及非授权的监听，具体流程如图 10 所示 [35]。文献 [36] 研究了内核级 Rootkit 技术的实现趋势，提出了一组以量化特征评估的方法来检测可加载内核模块 LKM（Loadable Kernel Module）型 Rootkit 后门技术，可用于对基于 LKM 实现的 SOHO 路由器后门进行检测。该方法速度较快，但误报率较高，多需要辅以人工分析来进一步判断。

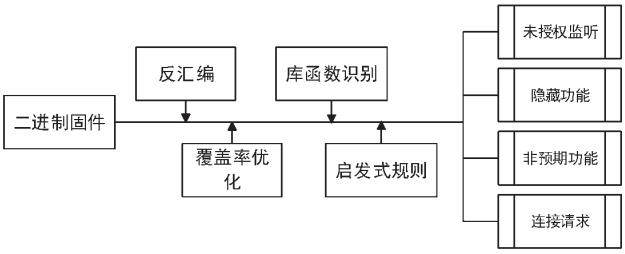

图 10　启发式规则与逆向分析结合的后门检测

3.2　动态检测

动态检测指在被测 SOHO 路由器工作期间，通过监视运行过程中相关信息，从而发现潜在的后门行为。同样地，根据是否考虑代码语义特征，动态检测有行为检测和跟踪调试两种。

基于行为检测是在路由器设备运行过程中，通过监听网络流量、系统环境、输入输出流来判断是否存在后门程序。由于功能需要，SOHO 路由器后门在运行过程中通常会进行为网络交互、日志记录、敏感文件读取等行为。因此，通过监视系统运行过程中系统文件、网络连接的变化，可以捕获后门程序的可疑行为。以 SOHO 路由器运行过程中网络行为为例，通过端口扫描工具、网络数据包分析软件，对运行期间的 SOHO 路由器进行扫描和监听，确定系统开放的监听端口和通信流量 [37]。行为检测方法又常常与模糊测试（Fuzzing）相结合，充分利用计算机的运算能力，随机构造输入向量，以激活 SOHO 路由器系统中需要满足特定条件才能触发的后门 [38]。以网络行为检测为例，如图 11 所示。对于路由器系统授权开放的端口，可以根据特定端口通信协议的特点，产生随机的数据作为输入向量发往路由器，并记录每一次的请求和相应内容。在得到足够数量的请求 / 响应数据对后，根据协议规范和预期网络行为流量，找出偏差的数据集合，筛选并作进一步分析。Xin Xu 等介绍了一种基于敏感流量跟踪和混合执行的技术，能有效发现包括窃取信息和数据库注入之类的后门行为，可以对 SOHO 路由器后门产生的异常流量进行有效检测 [39]。总体而言，行为检测获得的是路由器系统真实的执行信息，因此准确度较高。但是，随着对 SOHO 路由器的更高需求，造成路由器软件和系统的复杂度进一步提高，运行和采集过程的信息熵增加，导致代码覆盖率不高，可能会遗漏部分系统隐藏的后门。

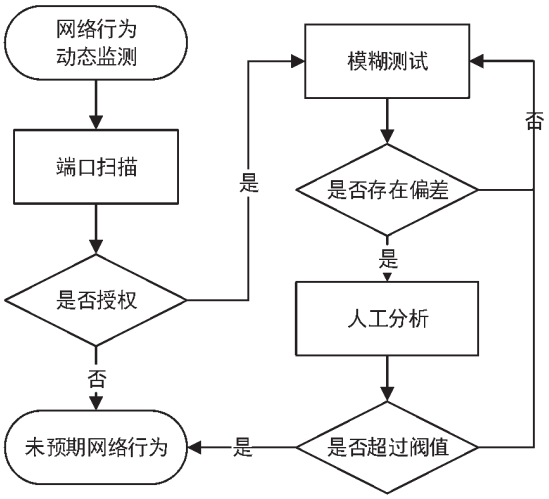

图 11　基于网络行为的后门检测

基于跟踪调试的检测包括利用 GDB 等工具对 SOHO 路由器系统中的可执行程序或代码片段进行单步跟踪执行，以及通过挂钩（Hook）、插桩等方式监视关键的系统调用和返回 [40]。Zaddach 等设计完成了一套名为 Avatar 的框架，以模拟器和真实硬件共同执行的方式，完成对嵌入式设备的复杂动态测试，以找出包括后门在内的多种安全问题 [41]。系统结构如图 12 所示，其中包括基于 KLEE 和 Qemu 模拟器的符号执行和分析框架 S²E、连接 SOHO 路由器等嵌入式设备和分析框架的通信接口以及用于辅助固件执行分析的 Python 脚本框架。用于固件代码执行的模拟器，经过修改能够拦截并转发全部的 I/O 操作至路由器设备。同时，系统将采集设备在处理 I/O 操作过程中真实的信号和中断信息，再注入到模拟器，避免了因为特殊 I/O 操作带来的代码执行错误。得益于框架基于事件的特性，用户可以

自定义插件以接入数据流，甚至直接修改模拟器与SOHO 路由器设备之间的数据。跟踪调试可以全面监视程序系统的执行过程，但由于插桩等信息采集过程加入，检测速度较慢，且程序或系统的完整执行分析相当费时，因此确定需要监视代码片段和挂钩的函数调用范围非常重要。

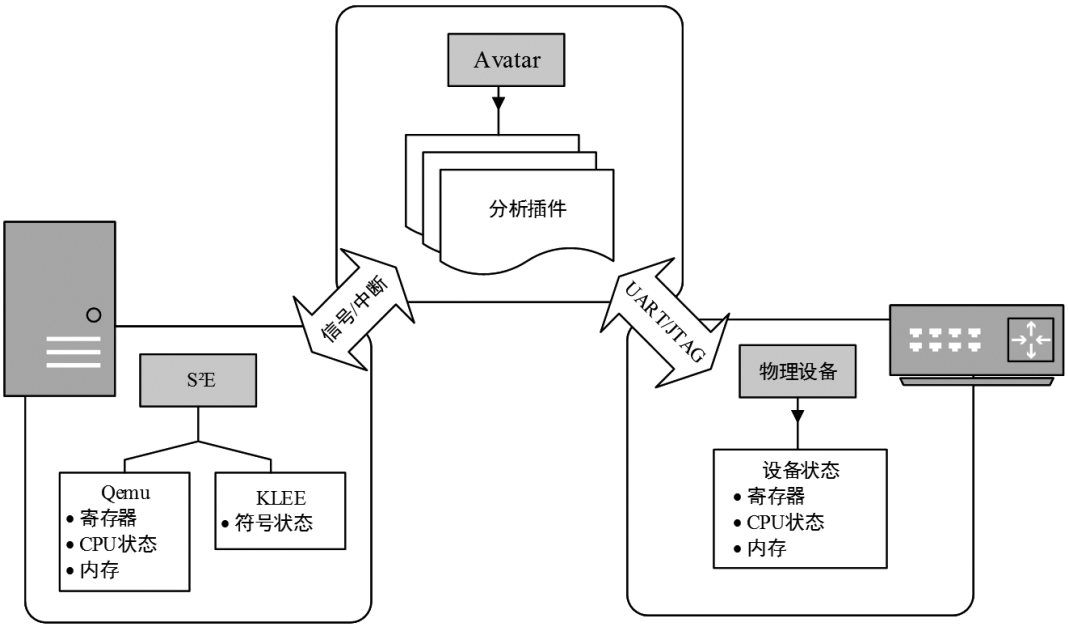

图 12 Avatar 体系结构

由于静态检测和动态检测各有优势，也有采用静态与动态结合的分析方法进行后门检测。A Damodaran 等通过同时训练静态和动态特征集的隐藏马尔可夫模型（HMM）方式来获得最佳的后门检出率[42]。E Salimi 等使用对系统和软件特征进行人工神经网络（ANN）和遗传算法（GA）来分类系统功能特性。这些方法可以用于分类 SOHO 路由器固件中各应用的功能，从而预测后门存在的可能性[43]。

4 结 语

随着人们对 SOHO 路由器等 IoT 设备安全需求的日益增长，对此类设备的后门检测技术越发受到重视。但是，与一般计算机在运行环境、操作系统、文件系统等多方面的差异，使得 SOHO 路由器后门功能更加灵活、隐蔽性更强、检测难度也更大。本文对 SOHO 路由器后门的定义和分类方法进行了系统性概述，详细分析了多个具有代表性的后门样本，并结合现阶段已有的研究成果，对比讨论了不同后门检测方法各自的技术特点。虽然目前 SOHO 路由器后门检测技术研究已经取得了一定成果，但是研究工作的开展时间较短，研究深度也受样本数量等客观条件的限制，尚未形成成熟的技术体系。因此，SOHO 路由器后门检测的关键技术、检测速率、智能化等方面的性能改进，还有待进一步研究和完善。

参考文献

[1] Xia F,Yang L T,Wang L,et al.Internet of Things[J]. International Journal of Communication Systems, 2012,25(09):1101–1102.

[2] Gubbi J,Buyya R,Marusic S,et al.Internet of Things (IoT):A Vision,Architectural Elements,and Future Directions[J].Future Generation Computer Systems,2013,29(07):1645–1660.

[3] Ning H,Liu H,Yang L T.Cyberentity Security in the Internet of Things[J].Computer,2013,46(04):46–53.

[4] Gan G,Lu Z,Jiang J.Internet of Things Security Analysis:Internet Technology and Applications (iTAP)[C].2011 International Conference on,2011.

[5] Davis M,Chow M.SOHO Router Security[EB/OL].(2012–12–12)[2017–03–28].http://www.cs.tufts.edu/comp/116/archive/fall2014/mdavis.pdf.

[6] Paganini P. Netgear, Linksys and many otherWireless Routers have a backdoor[EB/OL].(2014–01–04)[2017–05–02].http://securityaffairs.co/wordpress/20941/hacking/netgear–linkys–routers–backdoor.html.

[7] Waichal S,Meshram B B.Router Attacks–detection and Defense Mechanisms[J].International Journal of Food Science & Technology,2013,2(06):145–149.

[8] Costoya J,Flores R,Gu L,et al.Securing Your Home Routers[EB/OL].(2016–12–29)[2017–05–05].https://www.trendmicro.

com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-securing-your-home-routers.pdf.

[9] Zargar S T,Joshi J,Tipper D.A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks[J].IEEE Communications Surveys &Tutorials,2013,15(04):2046-2069.

[10] Zeifman I,Bekerman D,Herzberg B.Breaking Down Mirai:An IoT DDoS Botnet Analysis[EB/OL].(2016-09-20)[2017-05-08].https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html .

[11] Jerkins J A.Motivating a Market or Regulatory Solution to IoT Insecurity with the Mirai Botnet Code:Computing and Communication Workshop and Conference (CCWC)[C].2017 IEEE 7th Annual,2017.

[12] Moskvitch K.Securing IoT:In Your Smart Home and Your Connected Enterprise[J].Engineering & Technology,2017,12(03):40-42.

[13] Hau B,Lee T,Homan J.SYNful Knock a Cisco Router Implant[EB/OL].(2015-09-15)[2017-05-12].https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html.

[14] Heffner C.Reverse Engineering a D-Link Backdoor[EB/OL].(2013-10-12)[2017-05-12].http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/.

[15] Wysopal C,Eng C,Shields T.Static Detection of Application Backdoors[J].Datenschutz und Datensicherheit-DuD,2010,3(34):149-155.

[16] 孙淑华 , 马恒太 , 张楠等 . 后门植入、隐藏与检测技术研究 [J]. 计算机应用研究 ,2004,21(07):78-81.
SUN Li-hua,MA Heng-tai,ZHANG Nan,et al.Research on Backdoor Implantation,Concealment and Detection Techniques[J].Application Research of Computers,2004,21(07):78-81.

[17] Moore D,Shannon C.Code-Red:ACase Study on the spread and victims of an Internet worm[C].Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment,2002.

[18] Ornaghi A,Valleri M.Man in the Middle Attacks Demos[C].Blackhat Conference,2003.

[19] Wheeler D A.Program library howto[EB/OL].(2003-04-11)[2017-05-21].http://tldp.org/HOWTO/Program-Library-HOWTO/shared-libraries.html.

[20] Yuan Y.Survey on LKM Backdoors[J].Computer Science,2008,7(02):3.

[21] Yeh T.Netis Routers Leave Wide Open Backdoor[EB/OL].(2014-08-25)[2017-05-21].http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/.

[22] Stevens W R,Rago S A.Advanced Programming in the UNIX Environment[M].Boston:Addison-Wesley,2013.

[23] Allman M,Paxson V,Blanton E.TCP Congestion Control[R].2009.

[24] Zaddach J,Costin A.Embedded Devices Security and Firmware Reverse Engineering[C].Blackhat Conference,2013.

[25] 赵亚新 , 郭玉东 , 舒辉 . 基于 JTAG 的嵌入式设备固件分析技术 [J]. 计算机工程与设计 ,2014,10(01):3410-3415.
ZHAO Ya-xin,GUO Yu-dong,SHU Hui.Analysis Technology of Embedded Device Firmw are based on JTAG[J].Computer Engineering and Design,2014(10):3410-3415.

[26] 吴少华 , 赵旭 , 王炜 . 揭秘家用路由器 0day 漏洞挖掘技术 [M]. 北京 : 电子工业出版社 ,2015:368.
WU Shao-hua,ZHAO Xu,WANG Wei.Discovery of Home Router Zero-Day Vulnerability Mining Technology[M].Beijing:Publishing House of Electronics Industry,2015:368.

[27] Heffner C.Binwalk-Firmware Analysis Tool[EB/OL].(2014-07-22)[2017-05-21]https://github.com/devttys0/binwalk.

[28] Costin A,Zaddach J,Francillon A,et al.A Large-Scale Analysis of the Security of Embedded Firmwares[C].USENIX Security,2014.

[29] Desnos A,Roy S,Vanegue J.ERESI:AKernel-level Binary Analysis Framework[C].SSTIC08:Symposium sur la Securite des Technologies de l'Information et Communications,2008.

[30] Auriemma L.Signsrch Tool[EB/OL].(2016-06-23)[2017-05-22].http://aluigi.altervista.org/mytoolz.htm.

[31] Xie Y,Aiken A.Static Detection of Security Vulnerabilities in Scripting Languages[C].USENIX Security,2006.

[32] Sharif M I,Lanzi A,Giffin J T,et al.Impeding Malware Analysis Using Conditional Code Obfuscation[C].NDSS,2008.

[33] 蒋烈辉 . 固件代码逆向分析关键技术研究 [D]. 郑州 : 解放军信息工程大学 ,2007.
JIANG Lie-hui.Research on Key Techniques for Firm-Code Reverse Analysis[D].Zhengzhou:PLA Information

Engineering University,2007.

[34] Christodorescu M,Jha S.Static Analysis of Executables to Detect Malicious Patterns[R].Wisconsin Univ-Madison Dept of Computer Sciences,2006.

[35] 忽朝俭 , 薛一波 , 赵粮等 . 无文件系统嵌入式固件后门检测 [J]. 通信学报 ,2013(08):140-145.
HU Chao-jian,XUE Yi-bo,ZHAO Liang,et al.Backdoor Detection in Embedded System Firmware without File System[J].Journal on Communications,2013(08):140-145.

[36] Kruegel C,Robertson W,Vigna G.Detecting Kernel-level Rootkits Through Binary Analysis[C].Computer Security Applications Conference,2004.

[37] Orebaugh A,Ramirez G,Beale J.Wireshark & Ethereal Network Protocol Analyzer Toolkit[M].Syngress,2006.

[38] Wang K,Huang C,Lin S,et al.A Fuzzy Pattern-based Filtering Algorithm for Botnet Detection[J].Computer Networks,2011,55(15):3275-3286.

[39] Xu X,Wang J,Cheng S,et al.Software Backdoor Analysis based on Sensitive Flow Tracking and Concolic Execution[J].Wuhan University Journal of Natural Sciences,2016,21(05):421-427.

[40] Muniz S,Ortega A.Fuzzing and Debugging Cisco IOS[C].BlackHat,2011.

[41] Zaddach J,Bruno L,Francillon A,et al.AVATAR:A Framework to Support Dynamic Security Analysis of Embedded Systems´ Firmwares[C].NDSS,2014.

[42] Damodaran A,Di Troia F,Visaggio C A,et al.A Comparison of Static,Dynamic,and Hybrid Analysis for Malware Detection[J].Journal of Computer Virology and Hacking Techniques,2015,13(01):1-12.

[43] Salimi E,Arastouie N.Backdoor Detection System Using Artificial Neural Network and Genetic Algorithm[C].Computational and Information Sciences(ICCIS),2011.

作者简介：

谭云木（1992—），男，硕士，主要研究方向为信息安全；

王轶骏（1980—），男，硕士，讲师，主要研究方向为网络攻防及系统安全；

薛　质（1971—），男，博士，教授，主要研究方向为计算机通信及信息安全。