AhnLab

安全月刊

2015.10 Vol. 36

嵌入式 Linux 安全性探析

IoT及嵌入式Linux系统的安全威胁

CSI纽约第六季第二集“黑名单(Blacklist)”中，犯人因患有疾病而不能外出只能在家生活。犯人就在家里通过攻击联网的汽车、POS系统、电梯等杀害平时怀恨在心的人们。该剧的内容刚好反应了万物互联IoT时代的网络安全问题。电视剧有可能夸张了一点，但是现实中也开始出现了利用联网设备的犯罪事件。随着越来越多的设备联网使用，黑客已开始了针对这些设备制作恶意软件并试图攻击。目前，物联网有多样的平台在竞争。其中，嵌入式Linux平台最为广泛使用。本刊，着重介绍针对嵌入式Linux平台的恶意软件。

由于最近上市的产品大部分可以联网使用，物联网(Internet of Things)术语也开始流行。可以分为IoT的物品有很多种，其中利用嵌入式Linux平台的物品最为多样。

基于嵌入式Linux平台的设备

目前，有很多操作系统为掌握IoT的主导权而展开着激烈的竞争。其中，嵌入式Linux最为广泛使用。尤其广泛利用在“网络路由器（被称为家用路由器、Wi-Fi路由器或无线路由器）”、“机顶盒（Set-top box）”和“网络附加存储（Network Attached Storage，NAS”）等。

网络路由器和网络附加存储（NAS）是最为常见的基于嵌入式Linux平台的系统之一。网络路由器广泛利用在家庭和小规模的办公室。通过网络路由器捕获无线网络中传输的数据信息的网络监听（Sniffing）技术已众所周知，但是网络路由器本身被恶意软件入侵是个重大的问题。

尤其，网络路由器和网络附加存储（NAS）为了网络共享或资料共享，通常24小时运行，这就给攻击者提供了有机可乘。尽管这种系统比起桌面系统性能低下，但是与物联网产品比较的话，接近于电脑，因此成为了攻击者首选的攻击目标。

基于嵌入式Linux平台的设备的安全问题

基于嵌入式Linux平台的设备大多数没有考虑到安全而设计和制造，或者内置了制造商提供的后门程序功能。

没有考虑安全的设计

很多物联网设备没有考虑安全而设计并制造。一些网络路由器和IP摄像机很多端口是开放的，攻击者可以通过这些端口访问。访问需要ID和密码，但是很多用户使用固定的初始密码，攻击者便很容易访问这些设备。这种设备通常内置BusyBox程序，可以利用该程序运行Linux命令。如果支持wget命令的话，就很容易下载恶意软件到设备并运行。

```
user@ubuntu:~$ telnet [redacted]
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
(none) login: admin
Password:
warning: cannot change to home directory


BusyBox v1.8.2 (2013-07-02 14:46:30 KST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# wget
BusyBox v1.8.2 (2013-07-02 14:46:30 KST) multi-call binary

Usage: wget [-csq] [-O file] [-Y on/off] [-P DIR] [-U agent] url

# 
```

【图 1】通过telnet访问物联网设备并运行wget命令

内置后门功能

很多设备发现内置了后门程序，从外部可以访问。内置后门程序的目的可能是为了软件工程师的调试等，但有时候是制造商有意制作的。从外部访问设备是很严重的安全问题，尤其一般的人根本就找不到设备内置的后门程序。

网络连接带来的安全威胁

多样的设备连接到互联网面临着各种安全威胁。尤其为了用户方便，很多连接互联网的设备允许外部的访问，这使得攻击者有机可乘。

侵犯隐私和信息泄漏

许多人的家中设有IP安全监控摄像机是为了提升家庭安全，用户可以随时随地通过手机监控家里的情况。然而，这种IP摄像机存在重大的安全隐患，摄像机不再照看你的安全，而是通过摄像机偷看你的隐私或将你的隐私曝光在网络上。实际在美国发生过通过IP摄像机（如婴儿监视器）偷看家庭内部的事件，攻击者甚至还试图与主人谈话。

另外，联网的闭路电视（Closed Circuit Television, CCTV）有时候还利用在其他犯罪活动，用来确认犯罪场所周边的环境。

【图 2】通过闭路电视偷看收银台

更改设置及篡改数据

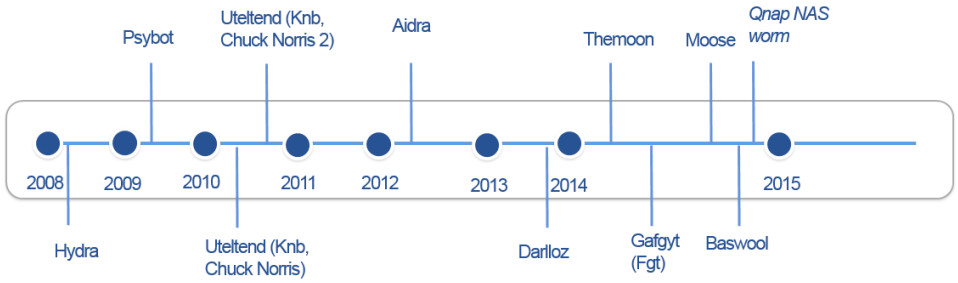
黑客攻击联网设备后，更改内部设置输出意外的结果或篡改保存的数据。如界面显示用户不情愿的广告或者诱导用户访问钓鱼网站或恶意软件网站。如果医疗设备被黑客攻击后数据被操作的话，有可能威胁患者的生命。

感染恶意软件

嵌入式Linux系统为了支持Telnet或Web服务器功能，打开多样的端口来使用。攻击者推测登录信息或利用漏洞制作访问设备的恶意软件。目前为止，发现的恶意软件大部分利用在“DDos攻击”、“显示广告”、“诱导钓鱼网站”和“开采虚拟货币”等目的。

主要嵌入式Linux恶意软件

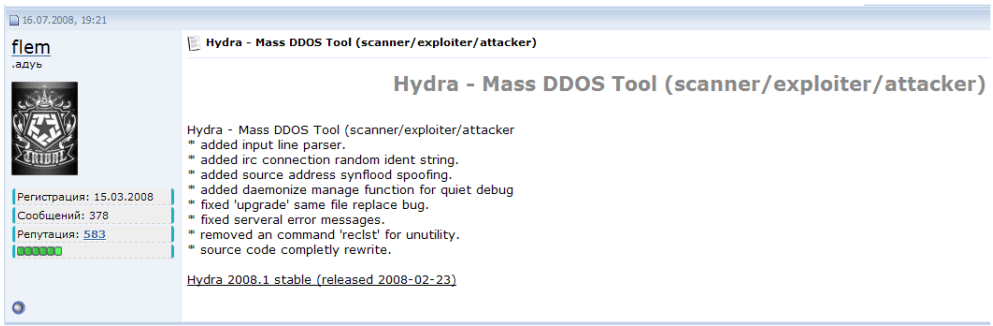
嵌入式Linux恶意软件最初2008年被报告第一事例后，至今陆续被发现。初期的嵌入式Linux恶意软件只能感染使用MINPS进程的网络路由器，但是2012年发现的Aidra蠕虫除了MIPS之外支持多样的进程，不仅在网络路由器，还可以在机顶盒（Set-top box）等多样的嵌入式Linux平台活动。很多恶意软件具有DDos攻击功能，但在2013年发现的Darlloz蠕虫主要目的是开采比特币之类的虚拟货币。2014年圣诞节当天，黑客集团Lizard Squad发起大量由Gafgyt恶意软件变形的DDoS攻击，使得一些网络游戏网站瘫痪。Lizard所使用的攻击软件名为Lizard Stresser。Lizard Stresser是一款强大的DDoS工具，它主要利用被感染的家用路由器的网络带宽流量发起对目标的攻击。



【图 3】主要嵌入式Linux恶意软件

Hydra

最初发现的网路路由器恶意软件是Hydra，是用于进行DDoS攻击的恶意软件。2008年在地下论坛就出现了有关Hydra的恶意软件的信息，由此可见，该恶意软件可能在2008年以前出现。


16.07.2008, 19:21

flem

.адуь

Регистрация: 15.03.2008

Сообщений: 378

Репутация: 583

Hydra - Mass DDOS Tool (scanner/exploiter/attacker)

Hydra - Mass DDOS Tool (scanner/exploiter/attacker)

Hydra - Mass DDOS Tool (scanner/exploiter/attacker
* added input line parser.
* added irc connection random ident string.
* added source address synflood spoofing.
* added daemonize manage function for quiet debug
* fixed 'upgrade' same file replace bug.
* fixed serveral error messages.
* removed an command 'reclst' for unutility.
* source code completly rewrite.

Hydra 2008.1 stable (released 2008-02-23)

【图 4】2008年Hydra信息

Psybot

Psybot是在2009年1月由Teny Baume发现。在网络路由器中首次被一般人广泛所知，并具有DDoS攻击功能。

Uteltend

Uteltend是在2009年捷克的马萨里克大学发现，又被称为Chuck Norris Bot。该恶意软件先寻找攻击对象系统后，利用“Telnet暴力攻击法（Telnet brute force attack）”来感染目标系统。据说源代码中包含了意大利语‘[R]anger Killato：in nome di Chuck Norris!’。而且使用UPX加壳，躲避杀毒软件的查杀，并存在 字符串‘Knb Keep nick bot 0.2.2’ 。

Aidra, Lightaidra

Aidra于2012年2月面世，在韩国也有感染事例。之前的嵌入式Linux恶意软件的攻击对象是使用MIPS进程的网络路由器的话，该恶意软件不仅在MIPS，还可在ARM、MIPSEL、Power PC和SuperH等多样的进程中运行。Aidra恶意软件主要用途是利用IRC Bot进行DDoS攻击，其源代码在2012年12月在网上公布，即是说已存在多样的Aidra变种。

Darlloz, Zollard

Darlloz发现于2013年10月，是一种不仅可以感染x86芯片的Linux系统设备，还可以感染搭载ARM芯片及PPC、MIPS架构的Linux设备的物联网蠕虫病毒。该恶意软件具有挖掘比特币之类的虚拟货币的功能。根据赛门铁克的报道，全世界有31,000台系统被感染，而其中17%的系统所在地是韩国。

Gafgyt

Gafgyt恶意软件发现于2014年8月。2014年末，黑客组织Lizard Squad对索尼和微软的游戏网络发动了DDoS攻击，该攻击利用的即是Gafgyt恶意软件。2015年1月，公开了恶意软件源代码，此后存在多样的变种。

嵌入式Linux恶意软件的预防

到目前为止，当网络路由器或NAS被恶意软件感染，并没有专门的防病毒产品来诊断和治疗。即使存在，如果没有制造商的帮助，则无法安装。这就需要做出努力来预防被恶意软件感染。首先，网络路由器或NAS安装后必须更改初始密码。密码必须组合英文、数字和特殊符号，而且最好是定期变更。
攻击者一旦发现网络路由器的漏洞便进行攻击。制造商针对与此，需要定期提供固件更新。如果是联网的产品，则必须更新为最新的固件。攻击者大部分利用设备的“从外部访问设备内部”的功能。因此，如果不是必要的情况，则禁用外部访问功能。
尽管采取了预防措施，仍然有可能被恶意软件感染。但是，大部分的嵌入式Linux系统不存在防病毒软件。一旦被感染，需要手动删除。还有很多用户还不知道固件需要更新为最新版本，甚至不知道固件更新的方法。为解决这些问题，需要制造商考虑固件自动更新功能，就像计算机操作系统的自动更新。

最近连接互联网的产品越来越增加。其中，一些网络路由器或NAS已具备了计算机的性能。黑客已在数年前开始针对这些系统不断地展开攻击，但是没有广泛所知。加上有些恶意软件的源代码已在网上公开，出现了多样的变种。对这些恶意软件和变种，还没有确实的预防方法。即使被感染，也没有适当的治疗方法。随着联网设备越来越多样且系统性能越来越提高，将要面对的恶意软件问题也越来越增加。

目前，嵌入式Linux恶意软件的攻击目标主要局限在网络路由器等家庭使用的联网设备。但是，恶意软件制作者正在努力制作更多样的恶意软件，欲感染除了家庭联网设备以外的更多的联网设备。一旦黑客的攻击目标扩展到更多的联网设备，则问题会变得很严重。在问题变得严重而无法收拾之前，需要政府、设备制作商和网络安全提供商联手来考虑这些问题并导出解决方案。另外，个人用户和企业在购买联网设备时，最好选择可以信任并持续提供固件更新的厂家。

参考文献

[1] Marta Janus/Kaspersky, ‘Heads of the Hydra, Malware for Network Devices’, 2011
[2] Marta Janus/Kaspersky, ‘State of play: network devices facing bulls-eye’, 2014
[3] Son, Kijong/韩国互联网振兴院, ’通过路由器攻击事例的物联网设备面临的安全威胁‘, 2015

http:// cn.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com