僵尸永远不死：大型僵尸网络AIRASHI近况分析

blog.xlab.qianxin.com/large-scale-botnet-airashi/

January 15, 2025

概述

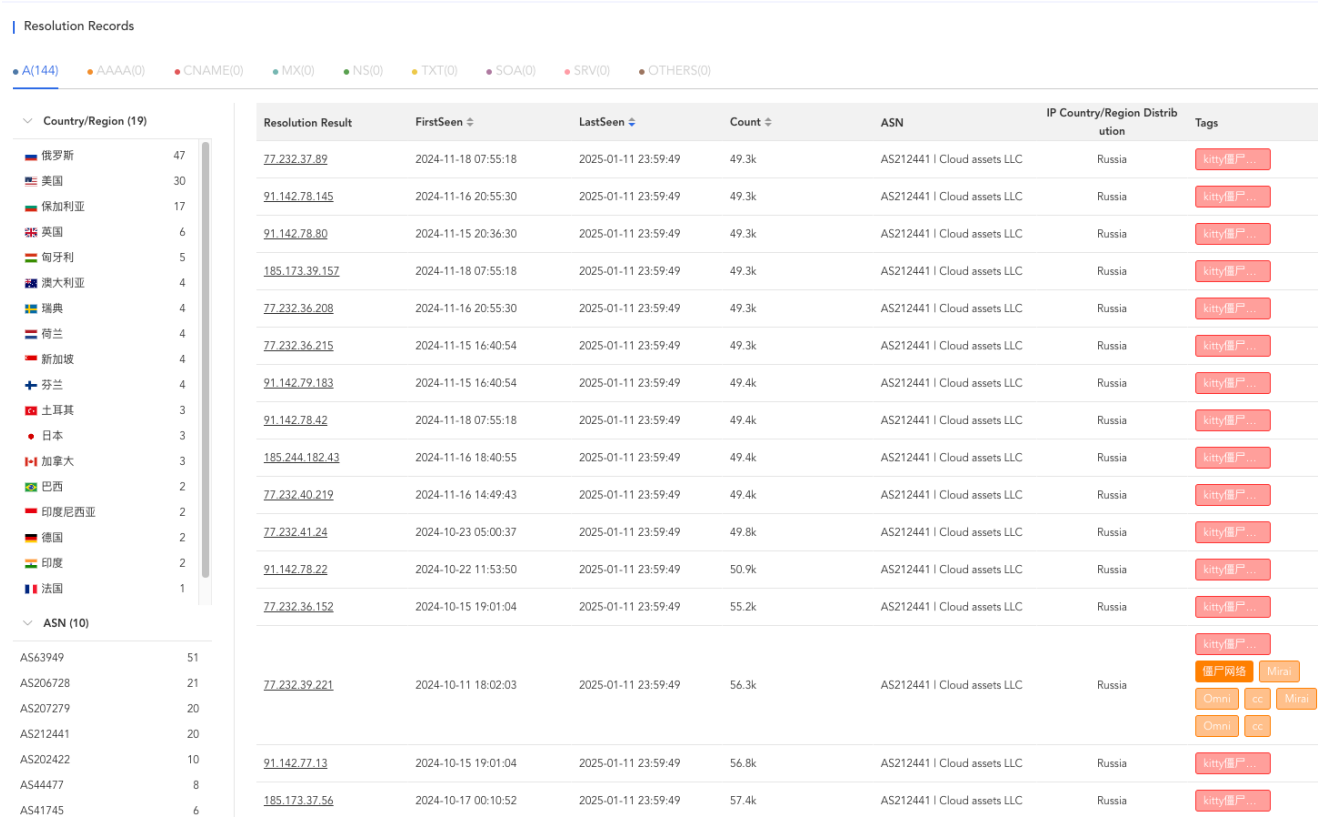
2024年8月XLab观察到一次有预谋的针对国产游戏《黑神话悟空》发行平台 Steam 和 完美世界的大规模DDoS攻击事件。此次攻击行动分为四个波次，攻击者精心挑选在各个时区的游戏玩家在线高峰时段发起长达数小时的持续攻击。并且同时攻击Steam和完美世界分布在全球13个地区的上百个服务器，以实现最大的破坏效果。而参与此次攻击行动的僵尸网络当时自称为`AISURU`。本文将要分析的正是`AISURU`僵尸网络的变种版本`AIRASHI`。

在上述攻击事件被曝光后，`AISURU`僵尸网络在9月短暂收手，停止了攻击活动。但在利益的驱使下10月对他们的僵尸网络进行了更新，根据样本特征我们命名为`kitty`。11月底，新的变种再次出现并在样本中11月底再次更新，并将僵尸网络更名为：`AIRASHI`。

当前AIRASHI僵尸网络主要有以下几个特点:

- 使用美国Cambium Networks公司的cnPilot路由器0DAY漏洞传播样本

- 样本字符串使用RC4加密，CNC通信协议部分新增了HMAC-SHA256校验，使用chacha20加密
- CNC域名使用`xlabresearch`, `xlabsecurity`，`foxthreatnointel`等关键字，调侃XLAB和安全研究人员。
- 稳定的T级别DDoS攻击能力
- 控制端的IP资源较为丰富，域名解析的IP将近60个，分布多个在不同的国家和服务商。可能是为了承载更多的BOT端和增加摧毁僵尸网络的困难程度。下图是AIRASHI CNC `xlabsecurity.ru` Passive DNS记录。可以看到`xlabsecurity.ru`这个CNC 曾经解析到144个IP，这些IP分布在19个国家，10个AS号（Autonomous System Number, ASN）。



xlabsecurity.ru Passive DNS records

样本传播

依托于XLab大网威胁感知系统的能力，我们观察到AIRASHI样本主要通过NDAY漏洞和TELNET弱口令传播，同时具备0DAY漏洞的利用能力。我们观察到AIRASHI自去年6月开始使用美国Cambium Networks公司的cnPilot路由器0DAY漏洞传播样本，关于该0DAY漏洞去年6月份我们联系了厂家，但是没有得到厂家任何回应。为防止漏洞滥用，本文也不会涉及此漏洞信息。AIRASHI 使用的漏洞如下：

VULNERABILITY

AMTK Camera cmd.cgi Remote Code Execution

VULNERABILITY
Google Android ADB Debug Server - Remote Payload Execution
AVTECH IP Camera / NVR / DVR Devices
cve_2013_3307
cve_2016_20016
cve_2017_5259
cve_2018_14558
cve_2020_25499
cve_2020_8515
cve_2022_40005
cve_2022_44149
cve_2023_28771
Gargoyle Route run_commands.sh Remote Code Execution
LILIN Digital Video Recorder Multiple Remote Code Execution
CVE-2022-3573
cnPilot 0DAY
OptiLink ONT1GEW GPON 2.1.11_X101
Shenzhen TVT Digital Technology Co. Ltd & OEM {DVR/NVR/IPC} API RCE

攻击能力与攻击活动

攻击能力

僵尸网络运营者通常通过社交媒体（如 Telegram、Discord 或论坛）展示其攻击能力，目的是吸引潜在客户或威慑竞争对手。为了证明僵尸网络的攻击能力，一些僵尸网络运营者会使用第三方提供的僵尸网络攻击能力测量服务来证明。他们驱动僵尸网络去攻击这些测量服务方提供的服务器，测量服务方会统计这些僵尸网络的攻击流量大小、包速率，攻击源地理位置信息、ASN，攻击方式等信息。僵尸网络运营者获得这些统计信息后将这些信息发布到他们的社交媒体以证明他们的攻击能力。

AIRASHI僵尸网络正是通过这种方式来证明他们的攻击能力。下图是他们的一次攻击能力证明：

可以看到图上的统计

- 当前攻击峰值: 3.11Tbps (270.52Mpps)
- 测试用户ID: 66XXXXXXXX (此ID正是AIRASHI僵尸网络Telegram运营频道管理员的ID)
- 更新时间: 2025-01-13 20:20:04 UTC
- 攻击来源

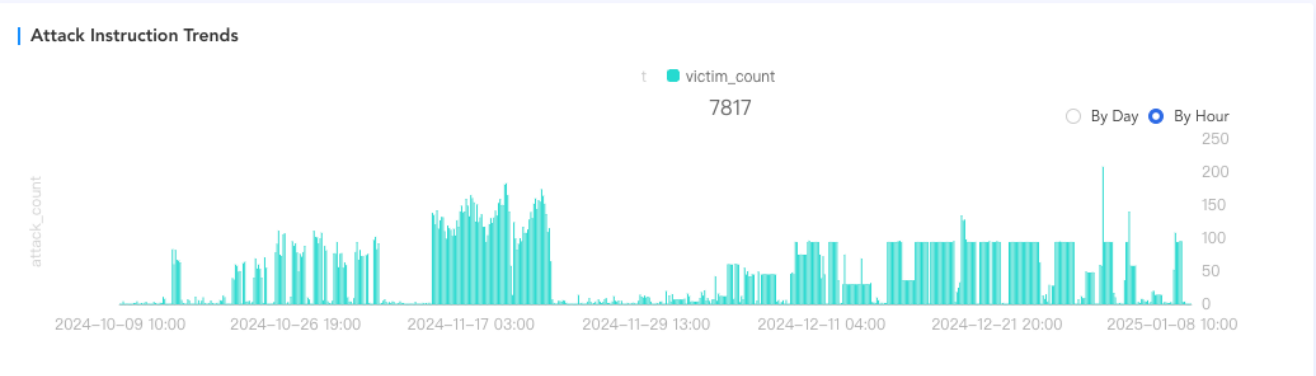
Country	Network
Brazil	30.01%
Russian Federation	24.51%
Viet Nam	22.79%
Indonesia	22.7%

AIRASHI的运营者一直在Telegram发布自己的DDoS能力测试结果，从历史数据可以看到AIRASHI僵尸网络的攻击能力稳定在1-3Tbps左右。

```
Attack Peak: 3.11Tbps (270.52Mpps)  User ID:: 660(      6  Time: 2025-01-13 20:20:04 UTC  UDP 100%
Attack Peak: 1.82Tbps (158.04Mpps)  User ID:: 660(      6  Time: 2025-01-13 19:39:04 UTC  UDP 100%
Attack Peak: 1.16Tbps (726.42Mpps)  User ID:: 660(      6  Time: 2025-01-13 19:14:04 UTC  UDP 100%
Attack Peak: 2.3Tbps (198.61Mpps)  User ID:: 6606       Time: 2025-01-13 19:00:04 UTC  UDP 100%
Attack Peak: 1.93Tbps (168.96Mpps)  User ID:: 660(      6  Time: 2025-01-13 02:25:04 UTC  UDP 100%
Attack Peak: 2.12Tbps (185.42Mpps)  User ID:: 660(      6  Time: 2025-01-12 06:22:04 UTC  UDP 99.99%
Attack Peak: 1.07Tbps (751.08Mpps)  User ID:: 660(      6  Time: 2025-01-11 04:22:04 UTC  UDP 100%
Attack Peak: 2.02Tbps (175.94Mpps)  User ID:: 660(      6  Time: 2025-01-11 04:16:04 UTC  UDP 100%
Attack Peak: 2.12Tbps (184.15Mpps)  User ID:: 660(      6  Time: 2025-01-11 04:10:04 UTC  UDP 100%
Attack Peak: 2.76Tbps (238.92Mpps)  User ID:: 660(      6  Time: 2025-01-04 16:50:04 UTC  UDP 99.99%
Attack Peak: 2.43Tbps (210.23Mpps)  User ID:: 660(      6  Time: 2025-01-04 12:34:04 UTC  UDP 99.99%
Attack Peak: 1.27Tbps (118.7Mpps)  User ID:: 6606       Time: 2025-01-02 12:46:04 UTC  UDP 100%
Attack Peak: 1.39Tbps (121.5Mpps)  User ID:: 6606       Time: 2024-12-21 18:35:03 UTC  UDP 100%
Attack Peak: 1.25Tbps (109.47Mpps)  User ID:: 660(      6  Time: 2024-12-09 07:59:03 UTC  UDP 100%
Attack Peak: 1.25Tbps (116.64Mpps)  User ID:: 660(      6  Time: 2024-12-07 04:34:03 UTC  UDP 100%
Attack Peak: 1.69Tbps (149.37Mpps)  User ID:: 722       5  Time: 2024-12-03 05:56:22 UTC  UDP 100%
Attack Peak: 1.69Tbps (157.84Mpps)  User ID:: 660(      6  Time: 2024-11-26 11:23:41 UTC  UDP 100%
Attack Peak: 1.73Tbps (161.07Mpps)  User ID:: 660(      6  Time: 2024-11-26 11:23:28 UTC  UDP 100%
Attack Peak: 1.91Tbps (178.13Mpps)  User ID:: 660(      6  Time: 2024-11-11 09:28:17 UTC  UDP 100%
Attack Peak: 1.89Tbps (165.85Mpps)  User ID:: 722       5  Time: 2024-11-10 14:20:16 UTC  UDP 100%
Attack Peak: 1.73Tbps (161.52Mpps)  User ID:: 660(      6  Time: 2024-11-04 14:58:50 UTC  UDP 100%
Attack Peak: 1.65Tbps (155.42Mpps)  User ID:: 660(      6  Time: 2024-11-02 18:23:17 UTC  UDP 100%
Attack Peak: 1.39Tbps (130.04Mpps)  User ID:: 660(      6  Time: 2024-10-23 03:09:14 UTC  UDP 100%
Attack Peak: 1.66Tbps (144.41Mpps)  User ID:: 660(      6  Time: 2024-10-14 11:28:14 UTC  UDP 100%
Attack Peak: 1.75Tbps (152.24Mpps)  User ID:: 6606      6  Time: 2024-10-12 10:36:14 UTC  UDP 100%
Attack Peak: 1.17Tbps (108.99Mpps)  User ID:: 7222      5  Time: 2024-10-11 17:29:14 UTC  UDP 100%
```

攻击活动

AIRASHI僵尸网络的攻击目标遍布全球，分布在各个行业，主要攻击目标分布在中国、美国、波兰、俄罗斯等地区。并无明显的强针对性。每日攻击目标几百个左右。



样本分析

AIRASHI僵尸网络样本更新频繁，拥有多个版本，部分版本除了支持主要的DDoS功能和操作系统命令执行外还支持代理服务，下文以kitty 和 AIRASHI为主要分析对象，从**字串解密，C2获取，通信协议，以及支持的指令**等方面入手，剖析僵尸网络的技术细节。

Part1: kitty-socks5 分析

kitty在2024年10月初开始传播，和Aisuru之前的样本相比，在网络协议方面进行精简；而在10月底使用socks5代理与C2通信，在字符串表中加密编码了250个代理和55个C2。

0x1: 字串解密

字符串解码方面变化不大，解密方法仍使用xor_bytes，仅修改了key为`DEADBEEFCAFEBABE1234567890ABCDEF`，字符串表项数缩减为7。

```
int table_init()
{
  add_entry(1, &unk_1FE8C, 330);
  add_entry(2, &unk_1FFD8, 1500);
  add_entry(3, &unk_205B8, 8);
  add_entry(4, &unk_205C4, 12);
  add_entry(5, &unk_205D4, 3);
  add_entry(6, &unk_205D8, 5);
  return add_entry(7, &unk_205E0, 17);
}
```

0x2: C2获取

C2获取方面，10月初删除了原先通过http获取C2ip的方法，继续使用`|`分割C2字符串，和之前一样每个域名都有20多个IP映射。

eg:`dvrhelpers.su|ipcamlover.ru|xlabresearch.ru|xlabsecurity.ru`

但在10月底添加socks5后，字符串表添加代理项，并且C2和代理项都使用多组`IP-PORT`的字节序列编码。

eg:`\x7f\x00\x00\x01\x00\x50`代表`127.0.0.1:80`

0x3: 网络协议

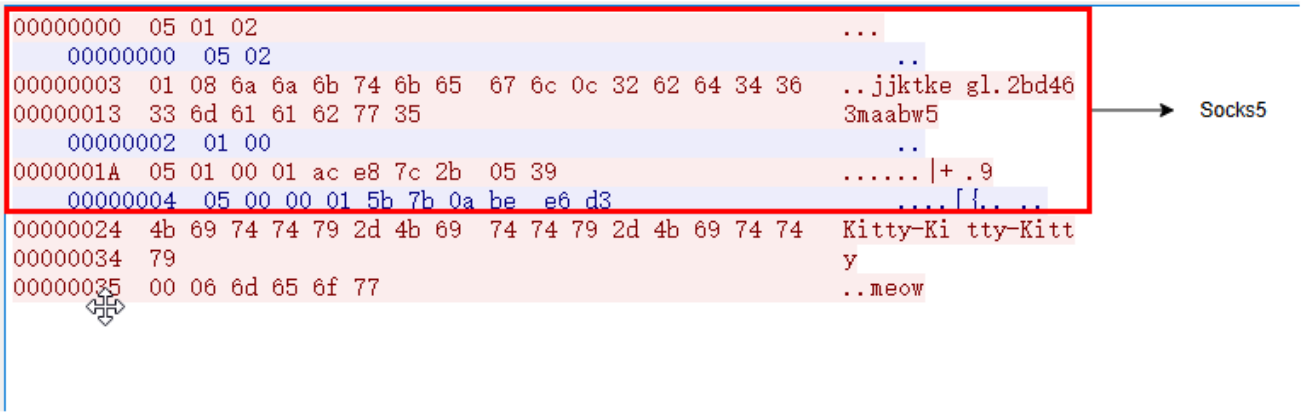
网络协议方面仍使用和Fodcha僵尸网络类似的switch-case进行各个阶段的处理

```
switch ( connect_stage )
{
  case 0:
    main_make_connection();
    break;
  case 1:
    if ( !v4 )
    {
      sleep(2);
      if ( authenticate(a1) )
        v4 = 1;
    }
    break;
  case 2:
    main_check_connection();
    break;
  case 3:
    main_read_connection();
    break;
  case 4:
    main_disconnect_connection();
    v4 = 0;
    break;
  default:
    break;
}
```

但在通信方面进行简化，最新样本使用socks5代理（使用身份验证）访问C2；

```
username: jjktkegl
password: 2bd463maabw5
```

取消原先的密钥协商过程，通信流量也不再加密，上线包替换为`Kitty-Kitty-Kitty`，每隔2分钟向C2发生心跳包`cat`，C2返回`meow!`作为响应。



指令类型仍以DDoS为主，添加了反向shell的功能，指令格式变化不明显，仍采用了`cmdtype+payload`的结构，只是cmdtype的值进行更新，而DDoS相关指令新增了AttckID字段。

cmdtype	desc
0x13	reverse shell
0x2c	stop attack
0x4b	start attack
0xaf	exit

Part2: AIRASHI 分析

目前发现了AIRASHI的3类样本：

1. AIRASHI-DDoS：最早发现于10月底，功能以DDoS为主，也可执行任意指令、获取反向shell。
2. Go-Proxisdk: 最早发现于11月底，由Go编写的基于muxado的代理工具。
3. AIRASHI-Proxy：最早发现于12月初，魔改AIRASHI-DDoS的同一套源码，使用私有协议实现代理功能。

AIRASHI和AISURU存在一些相似之处，如果说kitty是AISURU的精简版，AIRASHI更像是升级版。自10月开始持续更新，在开发了简单的`Go-Proxisdk`后，又开发了自定义协议的代理工具`AIRASHI-Proxy`，似乎想要用全新的东西惊艳我们。

0x1: RC4解密字符串解密

AIRASHI和AISURU在字符串解密方面有一些共性，继续使用长度为16字节的key，解密算法使用RC4；输出字符串`snow slide`；使用`|`分割特殊字符串。Prxoy版本和DDoS版本的解密方法相同，但Prxoy版本内的字符串数量很少。

有趣的是一些未被引用的字符串似乎在回应我们之前的blog：一首包含的conga舞曲的youtube链接和舞蹈邀请，此外还希望xlab和foxnointel命名该变种为AIRASHI

```
0 'snow slide'
1 'telnetd|upnpc-
static|udhcpc|/usr/bin/inetd|ntpclient|boa|lighttpd|httpd|goahead|mini_http|miniupnpd
|dnsmasq|sshd|dhcpd|upnpd|watchdog|syslogd|klogd|uhttpd|uchttpd|pppd|dhclient'
2 '/dvrEncoder|/dvrRecorder|/dvrDecoder|/rtspd|/ptzcontrol|/dvrUpdater'
3 'cve-2021-36260.ru'
4 'honeybooterz.cve-2021-36260.ru'
5 'stun.l.google.com:19302'
6 '/proc/'
7 '/proc/self/exe'
8 '/proc/net/tcp'
9 '/proc/mounts'
10 '/cmdline'
11 '/exe'
12 '/status'
13 '/fd/'
14 'PPid:'
15 '/bin/|/sbin/|/usr/|/snap/'
16 'wget|curl|tftp|ftpget|reboot|chmod'
17 '/bin/login'
18 '/usr/bin/cat'
19 'processor'
20 '/proc/cpuinfo'
21 '/bin/busybox echo AIRASHI > /proc/sys/kernel/hostname'
22 '/bin/busybox AIRASHI'
23 'AIRASHI: applet not found'
24 'abcdefghijklmnopqrstuvw012345678'
25 'come on, shake your body xlab, do the conga'
26 'i know you can't control yourself any longer'
27 'https://www.youtube.com/watch?v=ODKTITUPusM'
28 'dear researcher (xlab, foxnointel, ...), please refer to this malware as AIRASHI.
thank you!'
```

0x2: C2获取

AIRASHI共使用了3种不同的C2获取方法：

1. AIRASHI-DDoS，在开发初期（10月底），使用最普通的方法，通过DNS服务器解析C2的A记录。
2. AIRASHI-Proxy，通过DNS服务器获取C2的TXT记录，解析明文IP和端口。
3. AIRASHI-DDoS，在11月底，通过DNS服务器获取C2的TXT记录，base64解密、chacha20解密4字节的IP，端口硬编码在样本中。

解析结果	首次解析时间	最近解析时间	解析次数
"etf2FQ=="	2024-11-26 00:14:02	2024-11-26 02:04:14	4
"etf0Kw=="	2024-11-26 00:14:02	2024-11-26 02:04:14	4
"etf5HA=="	2024-11-26 00:14:02	2024-11-26 02:04:14	4
"etf1ew=="	2024-11-26 00:14:02	2024-11-26 02:04:14	4

DNS_TXT_CHACHA20_KEY: `8E12DF8893A638354D851BCB46B5B7DC451C6F52066305AC641DE60C80D11850`
DND_TXT_CHACHA20_NONCE: `941A247DDD53819F755FD59B`

值得注意的是，在12月3日`AIRASHI-DDoS`的C2解析A记录和TXT记录同时存在，且解密后存在对应关系，可能是为了兼容之前的版本，但这让加密编码都变得毫无意义。

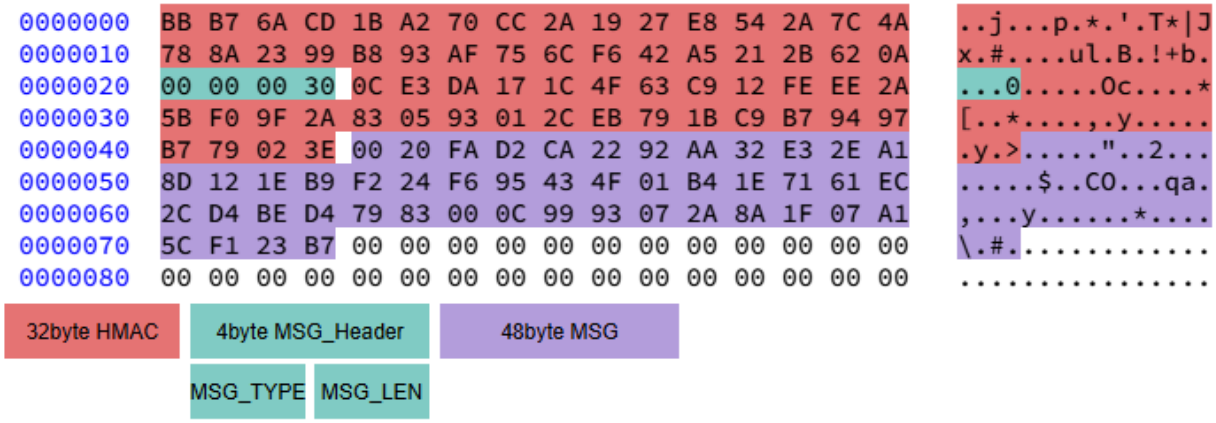
0x3: 网络协议

AIRASHI使用了全新的网络协议，用到的算法有HMAC-SHA256和CHACHA20，使用HMAC校验消息并使用协商后的CHACHA20_KEY加/解密消息。Proxy版本在协议部分没有使用HMAC进行消息验证，其他部分和DDoS版本保持一致。

- **通信过程**

  每条消息被分为2部分：32字节消息HMAC校验码、消息

  如下图首先会发送Header部分消息，确认消息类型和消息长度，若消息长度不为0，再发送Payload部分



  通信过程和之前一样使用状态码的switch-case结构控制，分为4步：

  1. 密钥协商

     获取32字节的CHACHA20_KEY和Nonce，之后的消息使用chacha20加密并使用CHACHA20_KEY作为HMAC-SHA256的密钥。
  2. 密钥确认

     使用chacha20加密发送消息类型为1的消息，验证返回消息类型是否为1
  3. 发送上线包

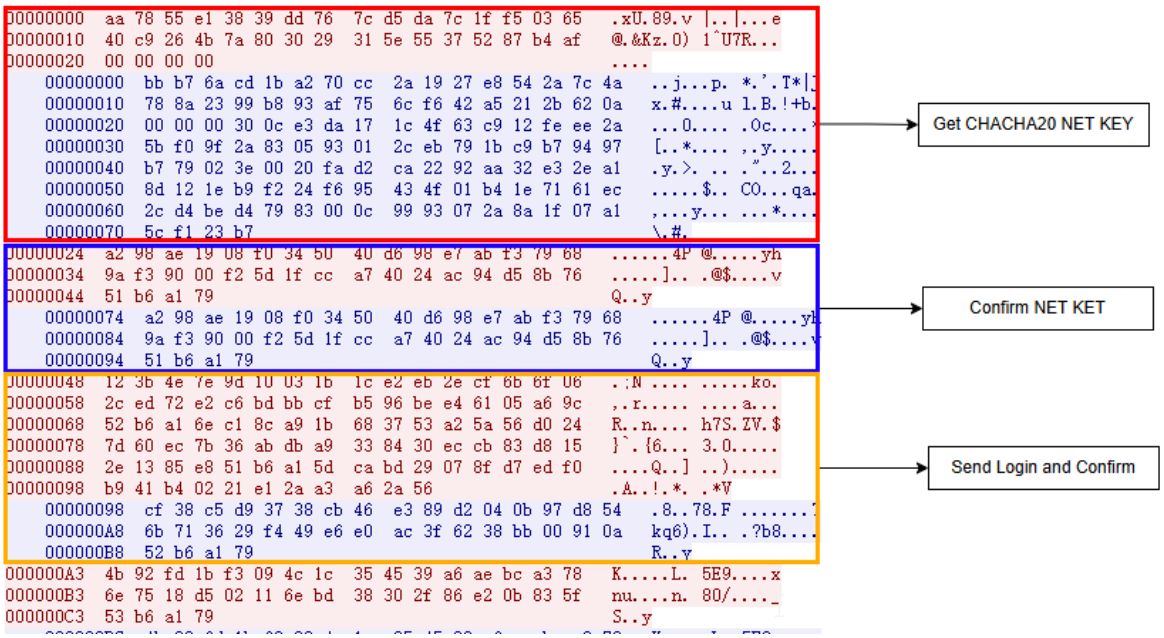
     通过读取ELF头获取arch类型，上线包结构体如下

```
struct login{
    uint8 uk1;
    uint8 uk2;
    uint8 uk3;
    uint32 stunIP;
    uint32 botid_len;
    char botid[botid_len];
    uint16 cpu_core_num;
    uint16 arch_type;
}
```

  4. 上线确认

     由C2返回消息类型为2的消息

  实际产生的流量如下所示：



- **消息类型**
  AIRASHI-DDoS共支持13种消息类型，对应的处理函数在bot的代码中以数组的方式存储，一些消息类型的处理函数仍不完善，可能还在开发当中。

```
:0805B140 ; int msg_handler[12]
:0805B140 msg_handler     dd 0                    ;
:0805B144                 dd 0
:0805B148                 dd 0
:0805B14C                 dd offset sub_80511F0
:0805B150                 dd offset sub_8051410
:0805B154                 dd offset sub_80513E0
:0805B158                 dd 0
:0805B15C                 dd 0
:0805B160                 dd offset sub_8051290
:0805B164                 dd offset sub_8051370
:0805B168                 dd offset sub_80512F0
:0805B16C                 dd offset sub_8051200
```

AIRASHI-DDoS一共支持以下13种消息类型，还保留了一些类型用于后续开发：

MSG_Type	Desc
0	Get Net Key
1	Confirm Net Key
2	Confirm Login
3	Heartbeat

MSG_Type	Desc
4	Start Attack
5	Exit
6	Killer Report
7	unknown
8	unknown
9	Disable Killer
10	Enable killer
11	Exec Command
12	Reverse Shell

而`AIRASHI-Proxy`则只支持5种消息类型，可以看出它们前4种类型保持一致。

MSG_Type	Desc
0	Get Net Key
1	Confirm Net Key
2	Confirm Login
3	Heartbeat
4	Unknown
5	Prxoy

检测

鉴于cnPilot路由器漏洞正在被积极利用，我们不便提供更多细节。我们提供Snort规则来帮助防御方识别其环境中的漏洞尝试和可能的感染

```
alert tcp any any -> any any (msg:"cnPilot 0DAY exploit #1 attempt";
content:"execute_script"; content:"sys_list"; content:"ASPSSIONID"; sid:1000007;)
```

Contact Us

Readers are always welcomed to reach us on twitter.

IOC

C2

```
xlabresearch.ru
xlabsecurity.ru
foxthreatnointel.africa
```

SHA1

```
3c33aa8d1b962ec6a107897d80d34a5d0b99899e
0339415f8f3e2b1eb6b24ed08c3a311210893a6e
95c8073cc4d8b80ceddb8384977ddc7bbcb30d8c
12fda6d480166d8e98294745de1cfdcf52dbfa41
08b30f5ffa490e15fb3735d69545c67392ea24e9
c8b8bd5384eff0fe3a3a0af82c378f620b7dc625
```

Downloader

```
190.123.46.21   Panama|Panama|Panama    AS52284|Panamaserver.com
190.123.46.55   Panama|Panama|Panama    AS52284|Panamaserver.com
95.214.52.167   Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
162.220.163.14  United States|New Jersey|Secaucus       AS19318|Interserver, Inc
```