|  |  |
| --- | --- |
| 特征编号 | 1 |
| 行为描述 | 设备接收控制信息（设置/通用/报警/响铃/夜灯/联动） |
| 源ip:port | 192.168.137.197：49164 |
| 目的ip:port | 49.4.47.2：5685 |
| 数据包  （加密后） | 80090000201605180000000000000000001402034fe81372278037cb66ce000000000000 |
| 加密方式 | 未知 |
| 数据包  （解密） | 数据采用基于TCP未知加密算法无法解密 |
| 返回的数据包  （加密后） | 005a5245bbd4e206f878acff893d9754295811fc820648c8b9c645e158cae342f9109f381ddc963f0b7ae9d8858b8788c933a0945f1c43d9e994fab6f5425db69b8e3b94ee87878e0a72d5fb967429909f0cd7ff7c899b25459720e6 |
| 返回数据加密方式 | 未知 |
| 返回的数据包  （解密） | 数据采用基于TCP未知加密算法 无法解密 |

|  |  |
| --- | --- |
| 特征编号 | 2 |
| 行为描述 | 设备与云端交互(上线离线) |
| 源ip:port | 192.168.137.197：49165 |
| 目的ip:port | 118.194.33.150：8089 |
| 数据包  （加密后） |  |
| 加密方式 | 未知 |
| 数据包  （解密） | 数据采用基于HTTP未知加密算法无法解密 |
| 返回的数据包  （加密后） | [truncated]x\001\001\003d�{"CONTENT":[{"SAID":[{"RT":4456606,"II":327680,"CT":"8LBIKEa2lV6tD/lRyxWPnmECitkd4SpqT2Y6M1gwW8vXfXz2xIf6rv+y884oFMpGa5VvXIZGojyRXonzRbIKX6HUSwLZ3dQUBktQ9FZc+b2oRP8tcrP5tZqEekAE5LDfpKxEZaj7WaM8dyspnhUSKLIj0zs/ |
| 返回数据加密方式 | 未知 |
| 返回的数据包  （解密） | 数据采用基于emuiv2似乎是华为定制HTTP无法解密 |

|  |  |
| --- | --- |
| 特征编号 | 3 |
| 行为描述 | 设备配网过程 |
| 源ip:port | 192.168.137.197 |
| 目的ip:port | 192.168.137.1 路由器地址 |
| 数据包  （加密后） |  |
| 加密方式 | 未知 |
| 数据包  （解密） | 数据采用基于HTTP未知加密算法无法解密 |
| 返回的数据包  （加密后） | [truncated]x\001\001\003d�{"CONTENT":[{"SAID":[{"RT":4456606,"II":327680,"CT":"8LBIKEa2lV6tD/lRyxWPnmECitkd4SpqT2Y6M1gwW8vXfXz2xIf6rv+y884oFMpGa5VvXIZGojyRXonzRbIKX6HUSwLZ3dQUBktQ9FZc+b2oRP8tcrP5tZqEekAE5LDfpKxEZaj7WaM8dyspnhUSKLIj0zs/ |
| 返回数据加密方式 | 未知 |
| 返回的数据包  （解密） | 数据采用基于emuiv2似乎是华为定制HTTP无法解密 |

|  |  |
| --- | --- |
| 特征编号 | 4 |
| 行为描述 | 网关发布CoAP |
| 源ip:port | 192.168.137.17 |
| 目的ip:port | 238.238.238.238（广播地址？） |
| 数据包  （加密后） |  |
| 加密方式 | 未知 |
| 数据包  （解密） |  |
| 返回的数据包  （加密后） | 934 42.183770 192.168.137.17 238.238.238.238 CoAP 80 NON, MID:29870, GET, TKN:00 0c, /.well-known/core?st=homeCenter |
| 返回数据加密方式 | CoAP协议 应该未加密 |
| 返回的数据包  （解密） | ?well-known/core?st=homeCenter |