

知 某局点wips反制不生效经验案例

WIPS 范书珩 2023-07-13 发表

问题描述

某局点使用wips反制，但是发现wips针对安卓终端开启的热点反制效果比较好，针对苹果终端开启的热点反制效果差，苹果终端已经关闭了随机mac，ios系统为16.5

过程分析

首先检查wips的基本配置，现场针对Test测试信号进行反制，检查基本配置没有发现问题

```
wips
#
ap-classification rule 1
  ssid equal Test
#
classification policy 1
  apply ap-classification rule 1 rogue-ap severity-level 100
#
countermeasure policy 1
  countermeasure rogue-ap
  countermeasure enhance
#
detect policy 1
  ap-spoofing quiet 360
  client-spoofing
  client-association fast-learn enable
#
virtual-security-domain vsd1
  apply classification policy 1
  apply countermeasure policy 1
#
client-proximity-sensor random-mac-report enable
```

随后在AC上查看反制记录，发现AC上存在对苹果热点的反制记录，但是终端可以正常连接苹果手机释放的热点。

```
[DX-NH-WX3520X-AC1-wips-dtc-1]display wips virtual-security-domain vsd1 device | include 5c1d
d272-907b-5c1d AP Rogue 00h 00m 28s 6 6 Inactive
```

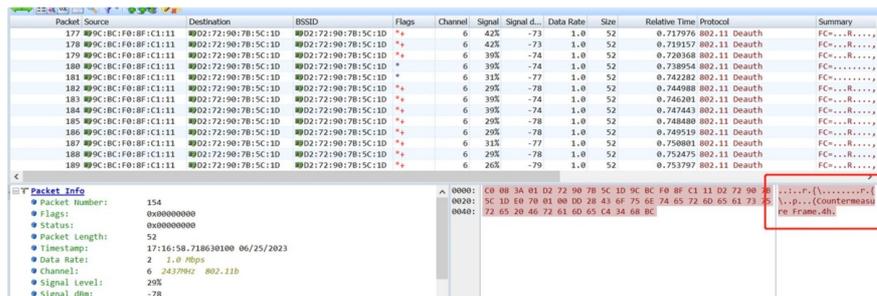
```
[DX-NH-WX3520X-AC1-wips-dtc-1]dis wips virtual-security-domain vsd1 countermeasure record | in
5c1d
```

```
d272-907b-5c1d AP Class AP2 2 2023-06-25/16:57:12
d272-907b-5c1d AP Class AP3 2 2023-06-25/17:11:42
d272-907b-5c1d AP Class AP2 2 2023-06-25/17:11:42
d272-907b-5c1d AP Class AP3 2 2023-06-25/17:11:42
d272-907b-5c1d AP Class AP2 2 2023-06-25/17:14:24
d272-907b-5c1d AP Class AP2 2 2023-06-25/17:14:24
d272-907b-5c1d AP Class AP2 2 2023-06-25/17:14:24
```

虽然AC上存在反制记录，但是究竟是否真正执行了反制，还需要空口抓包进行确认，如下为苹果热点空口抓包

苹果热点mac: d272-907b-5c1d 测试手机mac:9cbc-f08f-c111

空口抓包看AP伪装手机终端的mac不断的在给苹果热点发death报文，但是实际上终端依然可以稳定连接



| Packet | Source | Destination | BSSID | Flags | Channel | Signal | Signal d... | Data Rate | Size | Relative Time | Protocol | Summary | |
|--------|-------------------|-------------------|-------------------|-------|---------|--------|-------------|-----------|------|---------------|----------|---------|-------------|
| 177 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 42% | -73 | 1.0 | 52 | 0.717976 | 802.11 | Deauth | FC...R..... |
| 178 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 42% | -73 | 1.0 | 52 | 0.719157 | 802.11 | Deauth | FC...R..... |
| 179 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 39% | -74 | 1.0 | 52 | 0.720368 | 802.11 | Deauth | FC...R..... |
| 180 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 39% | -74 | 1.0 | 52 | 0.738954 | 802.11 | Deauth | FC...R..... |
| 181 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 31% | -77 | 1.0 | 52 | 0.742282 | 802.11 | Deauth | FC...R..... |
| 182 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 29% | -78 | 1.0 | 52 | 0.746088 | 802.11 | Deauth | FC...R..... |
| 183 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 39% | -74 | 1.0 | 52 | 0.746281 | 802.11 | Deauth | FC...R..... |
| 184 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 39% | -74 | 1.0 | 52 | 0.747443 | 802.11 | Deauth | FC...R..... |
| 185 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 29% | -78 | 1.0 | 52 | 0.748480 | 802.11 | Deauth | FC...R..... |
| 186 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 29% | -78 | 1.0 | 52 | 0.749519 | 802.11 | Deauth | FC...R..... |
| 187 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 31% | -77 | 1.0 | 52 | 0.750801 | 802.11 | Deauth | FC...R..... |
| 188 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 29% | -78 | 1.0 | 52 | 0.752475 | 802.11 | Deauth | FC...R..... |
| 189 | 9C:BC:F0:8F:C1:11 | D2:72:90:7B:5C:1D | D2:72:90:7B:5C:1D | * | 6 | 26% | -79 | 1.0 | 52 | 0.753797 | 802.11 | Deauth | FC...R..... |

Packet Info for packet 189:

- Packet Number: 189
- Flags: 0x00000000
- Status: 0x00000000
- Packet Length: 52
- Timestamp: 17126.59.718630100 06/25/2023
- Data Rate: 2 1.0 Mbps
- Channel: 6 2437MHz 802.11b
- Signal Level: 29%
- Signal dBm: -78

Hex dump of the selected packet:

```
0000: C0 08 3A 01 02 72 90 7B 5C 1D 9C BC F0 8F C1 11 02 72 90 7B 5C 1D 00 00 00 00 00 00 00 00 00 00
0040: 72 65 20 46 72 61 60 65 C4 34 68 BC
```

理论上在wips反制过程中，AP不仅会伪装终端mac发death给热点，也会伪装热点发death给终端，而现场的AP只伪装终端发death给热点，怀疑是AP没有伪装热点给终端发death报文导致的反制不成功，在经过确认后发现配置了countermeasure enhance后反制报文只有单方向的，随后删除countermeasure enhance进行测试，空口抓包看到AP不仅伪装终端mac发death给热点，也伪装热点发death给终端，但是反制依然没有生效，终端依然可以稳定连接。

由于现场用的苹果手机系统版本是最新版本，经验来看wips针对之前版本的苹果手机热点是可以正常反制的，于是让现场找了一台老版本ios 15.6.1的手机测试，发现反制效果比较明显，那么问题可以基本确认为ios的新版本对wips反制做了一些保护措施，经过研究后发现ios16以上的版本默认使用了WPA3加密方式，如果连接热点的客户端也支持WPA3，那么客户端和苹果热点的管理帧在协议上被增加了保护措施，其中的管理帧被加密后就无法被终端识别出现就是因为反制报文对终端设备之前实际是相致报文种组能安姐果释放黑点南终端和连接热点的终端都使用WPA3的加密方式h0则无法针对使消反制A3的热点连接度的反制效果明显是因为客户端终端没有使用WPA3加密方式即客户端的版本释放也是A3的热点所以wips反制没有问题。

