Spyware on IoT

Infection Methods

- Physical debug ports (JTAG, UART)
- UDP/TCP network ports
- Software security vulnerabilities
- Software logic flaws

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-10-07 15:02 PDT
Nmap scan report for 192.168.43.59
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
```

First Mirai Variant

- Physical debug ports (JTAG, UART)
- UDP/TCP network ports
- Software security vulnerabilities
- Software logic flaws

Specifically port 23 and 2323

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-10-07 15:02 PDT
Nmap scan report for 192.168.43.59
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
```

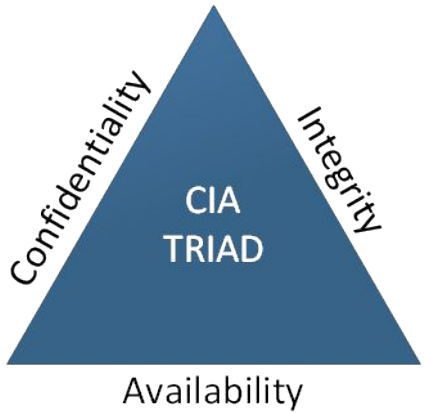
Wyze Cam

- Physical debug ports (JTAG, UART)
- UDP/TCP network ports
- Software security vulnerabilities
- Software logic flaws

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-10-07 15:02 PDT
Nmap scan report for 192.168.43.59
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
```

CIA Triad

- Wyze Cam does not provide Integrity
  - The software logic for updating new firmware does not check for firmware's authenticity, allowing an adversary to upload their own firmware onto Wyze



Custom Wyze Firmware

- Physical debug ports (JTAG, UART)
- UDP/TCP network ports
- Software security vulnerabilities
- Software logic flaws

We open up a new infection method on Wyze through logic flaw in its firmware update

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-10-07 15:02 PDT
Nmap scan report for 192.168.43.59
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
```

Steal Images

- A spyware can be installed on Wyze over-the-air from the opened port to steal camera's images