EASA
European Aviation Safety Agency

Is it safe? How many known vulnerabilities are still in the wild?

High Level Conference Cybersecurity in Civil Aviation

Kraków, Poland

9 November 2017

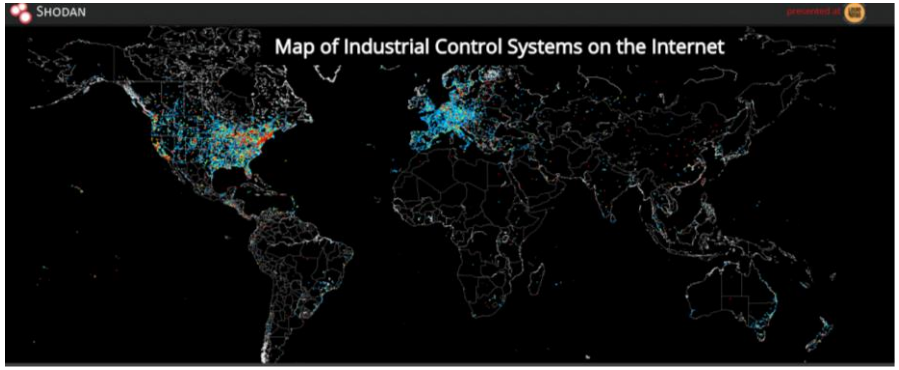
Your safety is our mission.

An agency of the European Union

do you know shodan?

When people don't see stuff on Google, they think no one can find it.

That's not true. John Matherly



Anything connected to the internet and having open port(s) is known to shodan.

The entire IP range is regularly scanned by powerful IP scanners (zmap: 45 min)

from fridges to nuclear power plants

and now ships

Let’s take a (well) known vulnerability

- Heartbleed is a security flawn (improper input validation that allows a buffer-over-read: you read more data than allowed) in the OpenSSL library (which is a widely used implementation of the Transport Layer Security protocol).
- Means the attacker can read the credentials of previous sessions
- Registered in the Common Vulnerabilities and Exposures database as CVE-2014-0160
- It was disclosed in April 2014

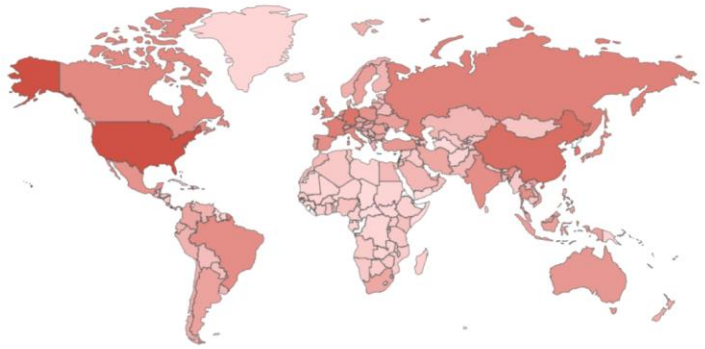
… 2014 … that 3 years an a half. How many systems still vulnerable?

Shodan analysis of CVE-2014-0160

SHODAN | Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account | Upgrade

heartbleed October 2017

Search for vuln:cve-2014-0160 returned 145,778 results on 17-10-2017

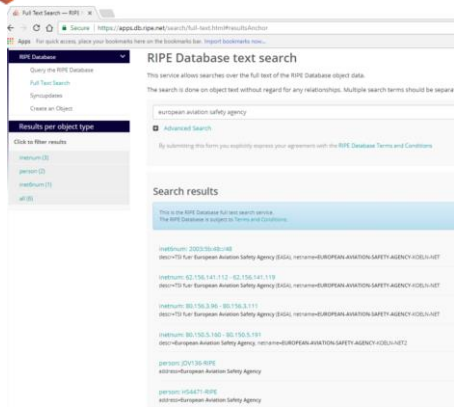


Top Countries

1.	United States	36,122
2.	China	12,353
3.	Germany	9,476
4.	Korea, Republic of	7,582
5.	France	6,192
6.	Russian Federation	5,454
7.	United Kingdom	4,146
8.	Italy	3,703
9.	Canada	3,624
10.	Japan	3,520

Data mining with OSINT

RIPE NCC
RIPE NETWORK COORDINATION CENTRE



1) Target range

MALTEGO

```
//Put the sequence of transforms to run in here
run("FileToAS")
type("maltego.AS", scope:"global")
paths{
    run("ASToBGPTweets")
    path{
        run("ASToNetblocks")
        type("IPNetblock", scope:"global")
        run("NetblockToIPs")
        type("ipaddress", scope:"global")
        run("IPToShodanInfo")
    }
}

setLayout("Interactive Organic")
```

Figure 19: "AS Monitoring" Machine code

2) Check vulnerabilities

SHODAN

3) Eventually exploit

metasploit

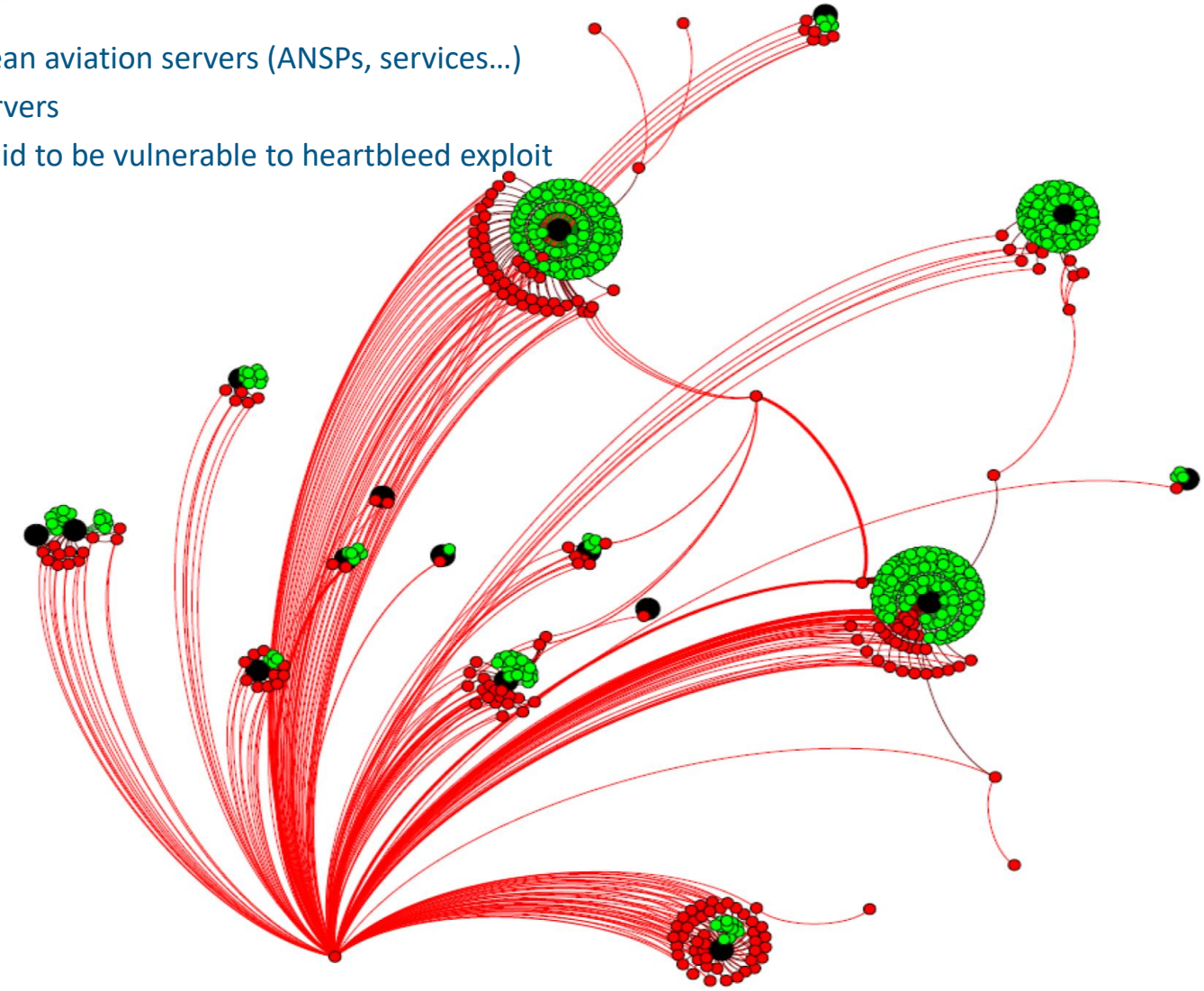
Credit: Florian Barbarin (DGAC/ENAC)

Result

Scan of some european aviation servers (ANSPs, services…)

Green spots: safe servers

Red spots: servers said to be vulnerable to heartbleed exploit



Conclusion

1) Check
2) Patch
3) In some cases consider changing all passwords

EASA
European Aviation Safety Agency

Questions?

Your safety is our mission.

An agency of the European Union