Home Routers for Fun & Profit

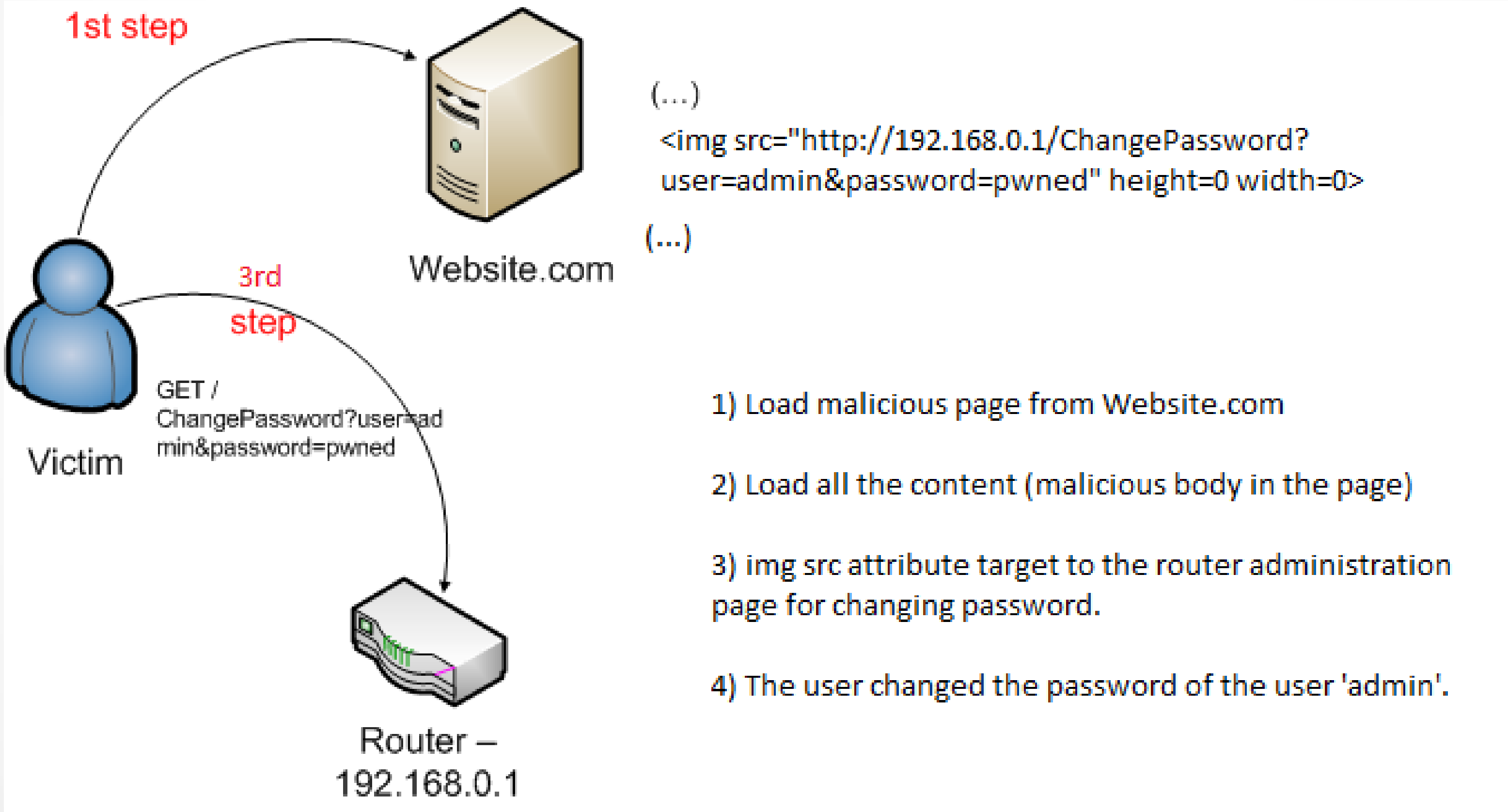
GreHack Conference - Paul AMAR

Context

- ISP Manufacturers provide routers
- Users don’t modify default settings
  - Pirates can predict attacks on those systems

- Possible weaknesses in those platforms ?

Cross Site Request Forgeries(1/2)



```
(...)
 <img src="http://192.168.0.1/ChangePassword?
 user=admin&password=pwned" height=0 width=0>
(...)
```

1) Load malicious page from Website.com

2) Load all the content (malicious body in the page)

3) img src attribute target to the router administration page for changing password.

4) The user changed the password of the user 'admin'.

Cross Site Request Forgeries (2/2)

- User has to be connected to the interface
  - Request forged with user's cookie

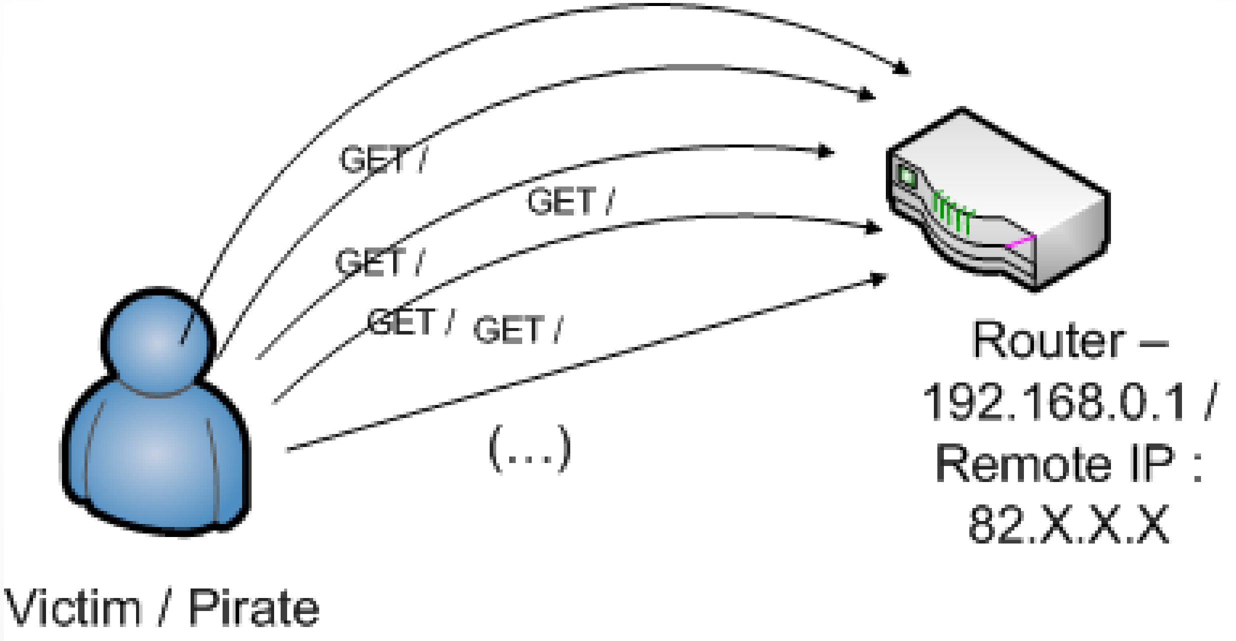
- Change any settings on the router :
  - Admin password
  - Router configuration
  - Remote access with public IP
  - Etc.

- Can disable his own access to his router

Demonstration !

Denial Of Service (DoS)

- DoS Attacks (attack can be done with private/public IP)



DoS Attack

- Private IP : Malicious script installed in the network
  - Attack coming from the internal network using private IP (ex: 192.168.0.1)

- Public IP : Knowing the (online) remote IP of the user
  - Can launch an attack on those devices with Botnet if necessary

- Internet / Phone down, victim is then unreachable

Attack Scenario

- Get victim’s network down (DoS, DNS Settings, Blacklist IP on the router)
- Attack his external websites (ex: company’s websites)
- Leak Personnal / Professional information

- No remote maintenance / monitoring during the attack

Limitations

- User has to be connected to the interface
- Have to know the public/private IP of the router
- Can’t work with custom network settings (192.168.1.254 instead of 102.168.0.1 for example)
- Plug-in which can block remote iframes, javascript, ..

Searching vulnerabilities..

- Many ways … BUT !

SHODAN

- Shodan (shodanhq.com)
- Computer Search Engine
  - Interrogates ports and grab the banner results
  - Then, it’s available on Shodan !
- Then, can access directly remote routers !

Thanks for your attention.