NOT FINISHED - PROTOTYPE

Doomed by default password

AUTOMATED ROUTER OWNING

NOT FINISHED - PROTOTYPE

Introductions

- TBD

NOT FINISHED - PROTOTYPE

The routers

- Edimax Routers Firmwares 1.40-2.52
  - ~50,000 according to shodan
  - Mainly Israel and Taiwan
  - Some in Poland and netherlands
- Others
  - Default router credentials all over
  - http://www.phenoelit.org/dpl/dpl.html or Google

NOT FINISHED - PROTOTYPE

The problems with them

- Default credentials
  - Admin :1234
  - Really high security
- HTTP management
  - Easy to fill out web forms
  - Silent to the router clients
  - Leaves no trace of who is running tool
    - We are admin, we control the logs
  - Externally accessible!

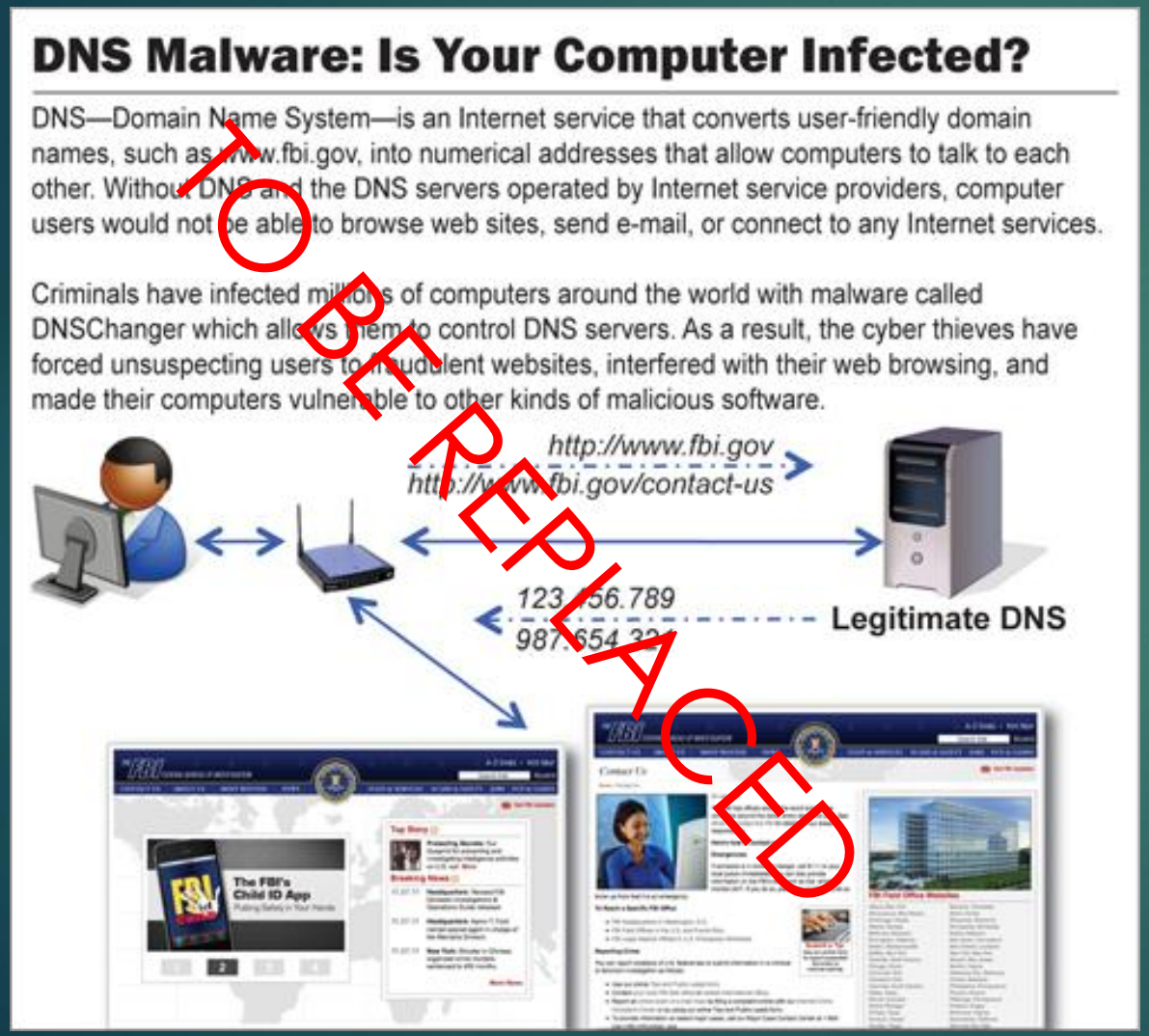
NOT FINISHED - PROTOTYPE

DNS changing attack

1. Bad guy hijacks your DNS to his boxes in some fishy eastern European country
2. Bad guy redirects some or all of the traffic to his fake HTTP servers
3. Bad guy either: Redirects you to a 0day, Sniffs your credentials or redirects traffic in a malicious way
4. He maintains access by using dynamic DNS account

NOT FINISHED - PROTOTYPE

Illustrated DNS changing attack



NOT FINISHED - PROTOTYPE

How to automate

1. Login using default credentials
2. Change DNS
3. Maybe enable a dynamic DNS service to maintain access.

- Provided tool “heasant” executes the first two steps using python and mechanize library for the models X,Y and Z.
- You should only use it to maintain your own routers as using it to do other things would be bad.

NOT FINISHED - PROTOTYPE

Demo

- I hope this works

NOT FINISHED - PROTOTYPE

Problems with the DNS attack

- HTTPS is done for so don't try anything that needs HTTPS
  - Redirect users to a custom page stripped of HTTPS
- DNS cache will have to clear for the user to actually use your DNS
  - Time?
- User DNS settings override router settings
  - Not very many casual people use these
- Easily detected/Traced to source by anyone with an internet browser
  - Attacker should really be more stealthy than this
- Not all that hard to remove
  - Keep running the tool?/DynamicDNS service to keep tabs on user
  - Maybe custom router Firmware (Michael Coppola DEF CON 20)

NOT FINISHED - PROTOTYPE

Other possible attacks

- Transparent request proxy
  - Monitor what everyone is doing on the internet silently using very little traffic
  - Used to keep tabs on a person/population
- Malicious ad injection
  - Redirect ads.adserver.com to badguy.com
  - Hijack all the ads and monetize

NOT FINISHED - PROTOTYPE

This actually happens

- http://news.cnet.com/8301-27080_3-57321844-245/seven-accused-in-$14-million-click-hijacking-scam/
  - $14 Million worth of malicious hijacking
  - Exploited from internal network
  - 2007-2011 lifespan
  - $3.5 million per year

NOT FINISHED - PROTOTYPE

Solutions

- No remote management enabled for the majority of routers
  - Why is this enabled by default?
  - Internal would be okay with a good password but external is a serious problem
- Use a better password
  - If you absolutely must have remote management then secure it.
- Use computer assigned DNS
  - Namebench will help you find some fast DNS

NOT FINISHED - PROTOTYPE

Credits

- Cite Images:
  - http.com
- Cite software used:
  - Burp
  - Python
  - Mechanize library
- Cite people:
  - People go here

NOT FINISHED - PROTOTYPE

Questions?