Bitsquatting

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is **VERY** easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don’t do it until you are able to confirm you are allowed to.

Code of Conduct

- Before proceeding past this point you must read and agree our Code of Conduct, this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.

- Code of Conduct can be found at https://wiki.shefesh.com/doku.php?id=code_conduct

Introduction

Bitsquatting - An intro

- Known as DNS Hijacking without exploitation
- Similar in principle to typosquatting
- Leads to the users receiving attacker supplied content
- Utilises bit errors

Bit Errors

Bit Errors - What are they?

- Data is stored as bits / transferred in bit-streams
- Bits can flip, aka change from 0 -> 1 or 1 -> 0
- 1 0 1 0 0 1 1 0 could become 1 0 0 0 0 1 1 0
- Caused by hardware issues, noise, heat etc
- Can occur in data transfer or in storage
- Changes the meaning of the data

Bitsquatting

Bitsquatting - How?

- If a bit error occurs in memory containing a URL
- The new data may represent another valid URL
- Can occur anywhere a URL ends up in memory
  - DNS requests
  - HTML links
    - On click
    - When link added to DOM
  - HTTP requests
    - Initial request
    - Following redirects
- And that’s just a few!

Bitsquatting - What?

- Register a domain which is 1-bit off another domain
- If bit error occurs in memory containing the original domain
- It can become a domain owned by the attacker
- Similar to typo squatting
- Except this time the user didn't do anything wrong!
- Relies on hardware errors
- So more popular domains are better (CDNs are good)
- More traffic, more chances of error

DOMAIN.COM

01100100 01101111 01101101 01100001 01101001 01101110 00101110
01100011 01101111 01101101 00001010

DOMCIN.COM

01100100 01101111 01101101 01100011 01101001 01101110 00101110
01100011 01101111 01101101 00001010

Bitsquatting - Attacks

- What can we do with it?
- Phishing sites
  - An identical site designed to steal data from the user
- Proxy as MITM
  - Replace internal links with links to squatting domain to keep on site
  - Can steal creds, inject ads, a crypo currency miner etc
- Host alternative files
  - If real site loads example.com/script.js
  - Host a malicious script on uxample.com/script.js (uxample.com bitsquats on example.com)
  - If bit error occurs wrong js file could be loaded to user

Bitsquatting - Protections

- There are various ways of protecting against this
- Using ECC memory
  - Corrects single bit errors
  - Can still occur if non-ECC is used upstream (router, proxy server, etc)
- Pre-registering the domains that bitsquat on yours
- Use sub-resource integrity checks on script loads

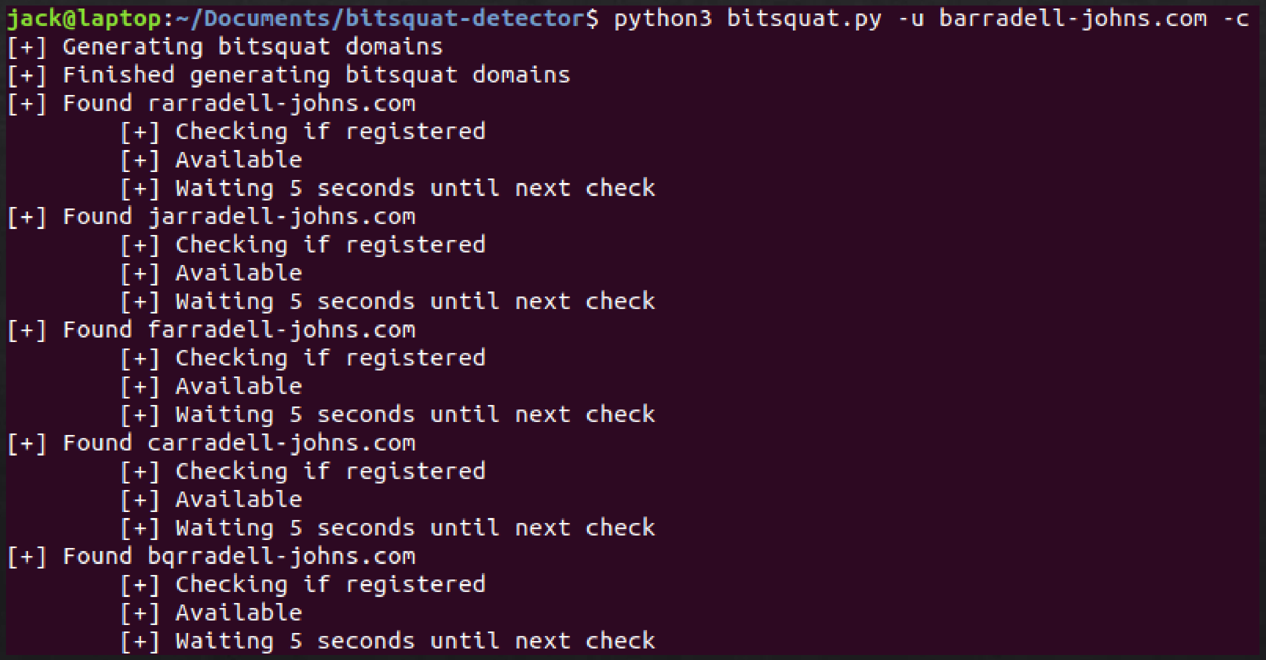
Bitsquatting - What makes it interesting?

- Relies on random hardware errors
- There's no direct exploitation of victims
- The cause can happen at any point in the connection
- Upstream machines can cause it
- The victims don’t do anything wrong

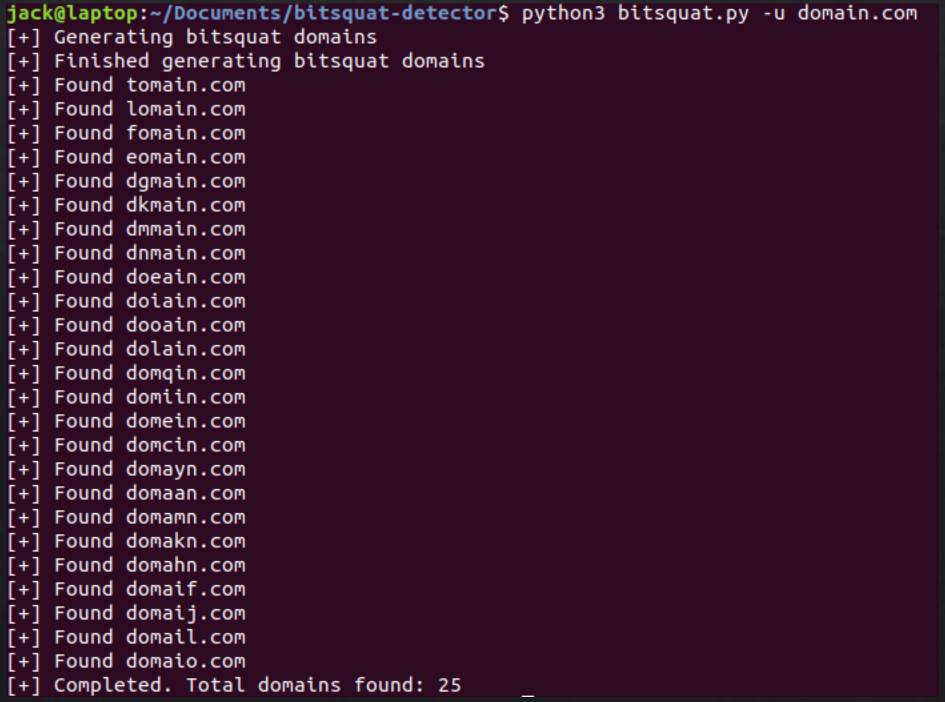
Bitsquatting Tool

Bitsquatting Tool

- I developed a tool in python to calculate domains that bitsquat on others
- Can use whois to find out if domains are available
- Full source at https://github.com/Jack-Barradell/bitsquat-detector
- Takes each byte, finds other 1-bit off bytes which are also valid URL characters



```
jack@laptop:~/Documents/bitsquat-detector$ python3 bitsquat.py -u barradell-johns.com -c
[+] Generating bitsquat domains
[+] Finished generating bitsquat domains
[+] Found rarradell-johns.com
        [+] Checking if registered
        [+] Available
        [+] Waiting 5 seconds until next check
[+] Found jarradell-johns.com
        [+] Checking if registered
        [+] Available
        [+] Waiting 5 seconds until next check
[+] Found farradell-johns.com
        [+] Checking if registered
        [+] Available
        [+] Waiting 5 seconds until next check
[+] Found carradell-johns.com
        [+] Checking if registered
        [+] Available
        [+] Waiting 5 seconds until next check
[+] Found bqrradell-johns.com
        [+] Checking if registered
        [+] Available
        [+] Waiting 5 seconds until next check
```



```
jack@laptop:~/Documents/bitsquat-detector$ python3 bitsquat.py -u domain.com
[+] Generating bitsquat domains
[+] Finished generating bitsquat domains
[+] Found tomain.com
[+] Found lomain.com
[+] Found fomain.com
[+] Found eomain.com
[+] Found dgmain.com
[+] Found dkmain.com
[+] Found dmmain.com
[+] Found dnmain.com
[+] Found doeain.com
[+] Found doiain.com
[+] Found dooain.com
[+] Found dolain.com
[+] Found domqin.com
[+] Found domiin.com
[+] Found domein.com
[+] Found domcin.com
[+] Found domayn.com
[+] Found domaan.com
[+] Found domamn.com
[+] Found domakn.com
[+] Found domahn.com
[+] Found domaif.com
[+] Found domaij.com
[+] Found domail.com
[+] Found domaio.com
[+] Completed. Total domains found: 25
```

Bitsquatting Experiment

Bitsquatting Experiment

- A server set up logging incoming requests to it
- Has a domain which bitsquats another pointing to it
- Planning to analyse the data over Christmas
- Have to dig through and filter out all the automated scan tools!