Bitsquatting – An introduction

Nigel Roberts

Chief Xenobehaviourist
CHANNELISLES.NET

nigel@roberts.co.uk
@nigelrbrts
http://nigel.je
http://roberts.gg

What is bitsquatting

- *“Typosquatting is a subset of cybersquatting: bitsquatting is a subset of typosquatting.”* - Arends

- In bitsquatting:
  - a squatted identifier
    - differs from the intended victim
    - by one bit

Why do we care?

- It turns out
  - That, in in some circumstances
  - traffic addressed for a victim
    - can be intercepted by a attacker
    - by utilising an address identifier
    - that differs
      - by one bit
      - from the victim's principal address

Bitsquatting

- First described in 2011
- by **Artem Dinaburg** of Raytheon.
  - *Bitsquatting: DNS Hijacking without exploitation*

  http://gg.gg/bs-dinaburg

What is the science?

- Working Hypothesis
  - Hardware not humans
  - Devices make single bit errors
  - which
    - In the case of certain identifiers
    - to which there is a very large quantity of traffic
    - are statistically significant

      e.g www.facebook.com

What's the cause?

- Speculation
  - Heat
  - Poor quality memory
  - Background radiation (e.g. radon) and/or nuclear explosions
  - Cosmic rays
  - Aliens playing Halo 2 with live ammunition.

Empirical evidence

- Is there any evidence for bitsquatting?
  - Yes
- described by Duane Wessels of Raytheon
  - *Evidence of Bitsquatting In COM/NET Queries*

  http://gg.gg/bs-wessels

Implications

- What are the implications?
- Investigated by Jaeson Schulz of Cisco
  - *Examination of the bitsquatting attack surface*

http://gg.gg/bs-schulz

Detection of enemy activity

- The qualified question.
- Is it being used in the wild by hostile forces?
- If so, how do we detect it?

The contention:

- “Domain registries and registrars have unique tools available to them to investigate and detect whether bit-squatting is being actively pursued by bad guys” - Roberts
- Corollary: There are other good guys able to do this too, perhaps with different tools.
  - Google
  - Who else?

How?

- Easy to make a list of all bitsquatting collisions of all registered domains.
- SMOP
- But there's a lot of them
  - Mostly either legitimate, or “ordinary typosquatting”
- Need to reduce them further
  - Various possible tools to do this
    - DNS data, registry data (WHOIS), IP registry data (RIPE/ARIN etc), MD5 hash of spidered data
  - Are there any characteristics of domain names and registration that give us extra information?

Conclusion

- “You have more work to do”
  - Houston, Floyd, Carnicero, Tennant *(Spy the Lie)*