BitSquatting

BitSquatting

...or the infinite monkeys theorem...

"Three monkeys hitting keys at random on typewriters for an infinite amount of time will almost surely produce Hamlet."

-- David Ives in "Words, Words, Words"

Explanation...

Explanation...

www.twitter.com:

ASCII	**t**	**w**	**i**	**t**	**t**	**e**	**r**
Binary	01110100	01110111	01110100	01110100	01110100	01100101	01110010

Explanation...

www.twitter.com:

ASCII	**t**	**w**	**i**	**t**	**t**	**e**	**r**
Binary	01110100	01110111	01110100	01110100	01110100	01100101	01110010

www.4witter.com:

ASCII	**4**	**w**	**i**	**t**	**t**	**e**	**r**
Binary	0~~0~~110100	01110111	01110100	01110100	01110100	01100101	01110010

Explanation...

www.twitter.com:

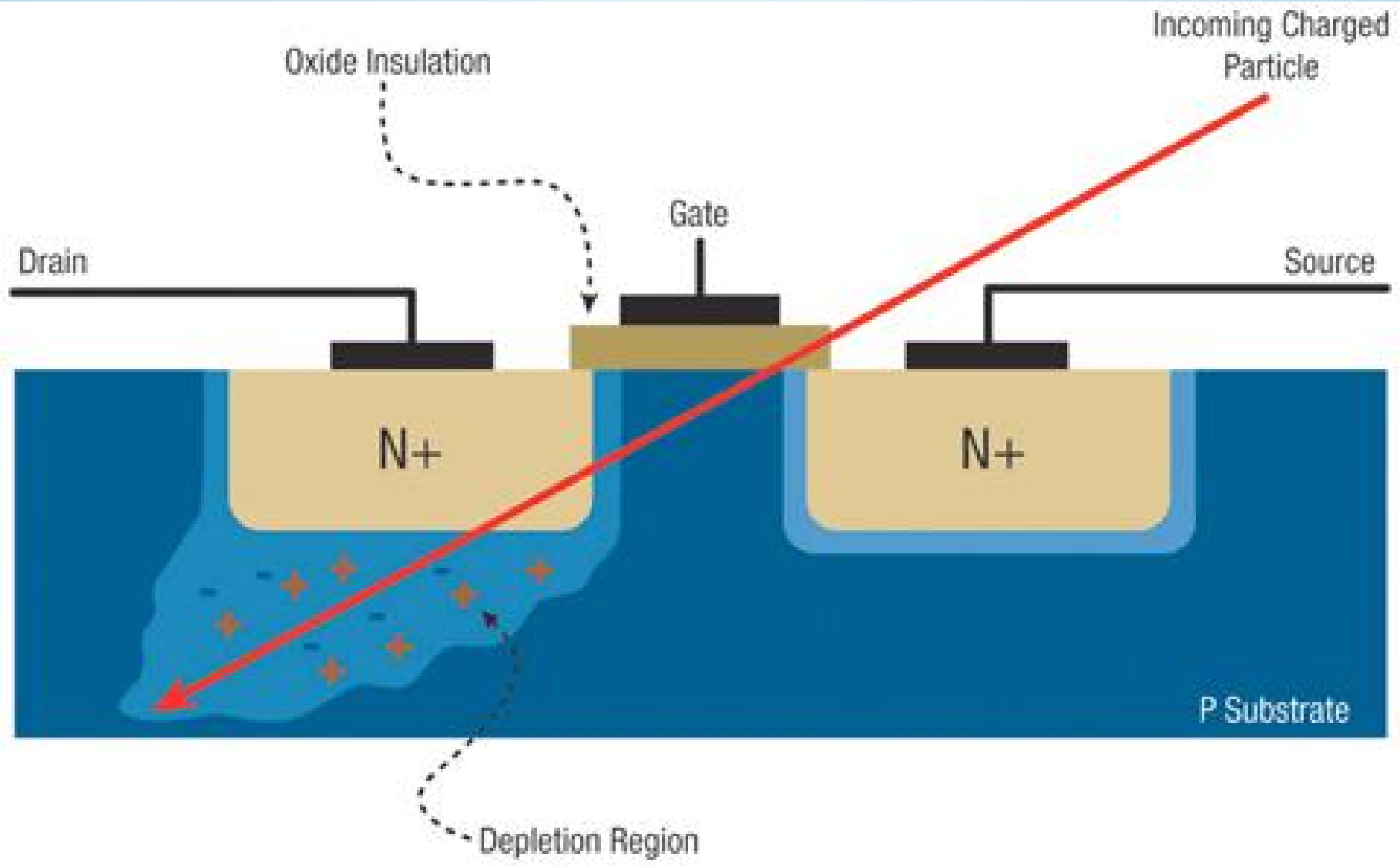
ASCII	t	w	i	t	t	e	r
Binary	01110100	01110111	01110100	01110100	01110100	01100101	01110010

www.4witter.com:

ASCII	4	w	i	t	t	e	r
Binary	00110100	01110111	01110100	01110100	01110100	01100101	01110010

```
~/src/code/python/bit-squat  git master  ./compare_characters_binary.py twitter.com 4witder.com
Domain 1  : |   t    |   w    |   i    |   t    |   t    |   e    |   r    |   .    |   c    |   o    |   m    |
Domain 2  : |   4    |   w    |   i    |   t    |   d    |   e    |   r    |   .    |   c    |   o    |   m    |
Difference: |01000000|00000000|00000000|00000000|00010000|00000000|00000000|00000000|00000000|00000000|00000000|
```

Srsly?!....

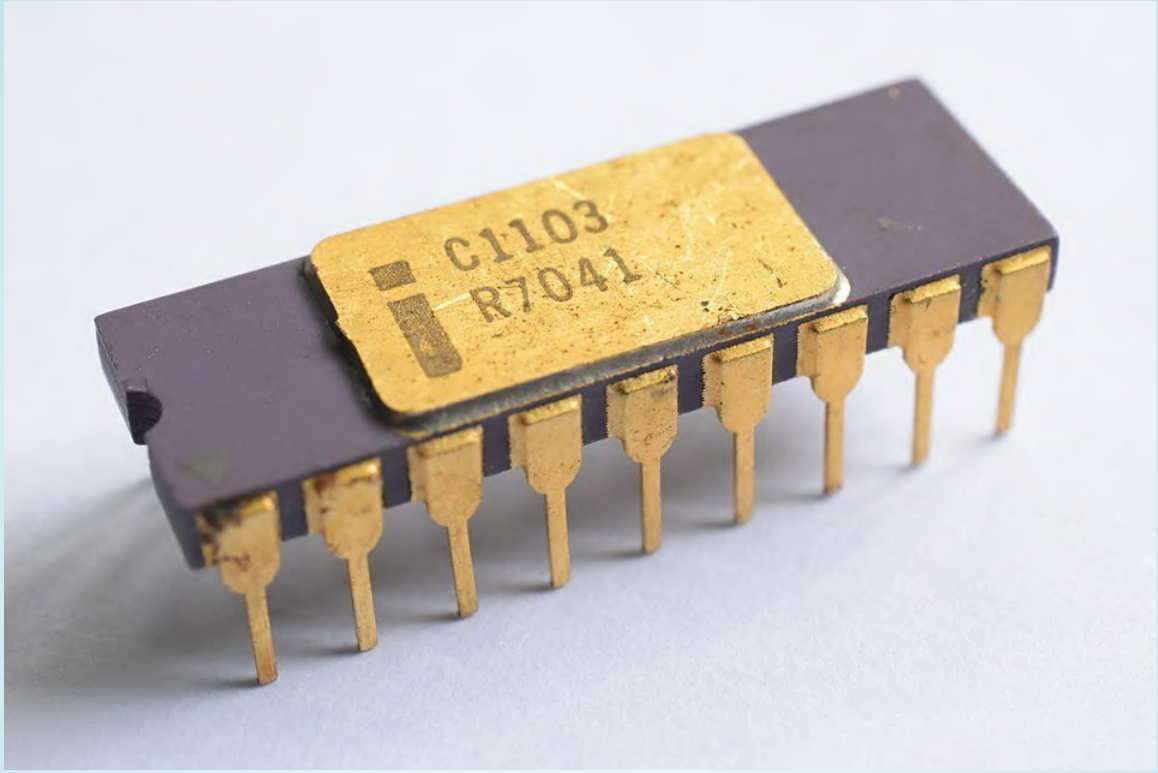


https://semiwiki.com/eda/3604-single-event-upsets/

Srsly?!....

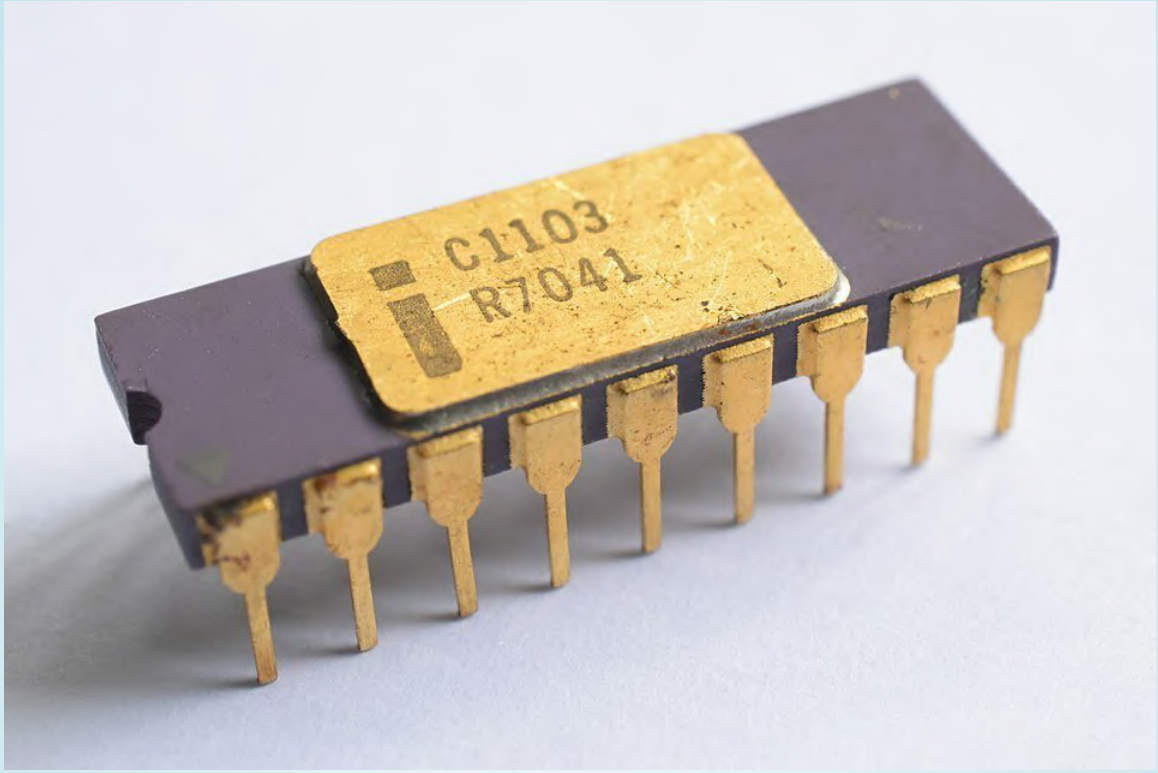
Similar chip - Thomas Nguyen, CC - https://commons.wikimedia.org/wiki/File:Intel_C1103.jpg

Srsly?!....



Similar chip - Thomas Nguyen, CC - https://commons.wikimedia.org/wiki/File:Intel_C1103.jpg

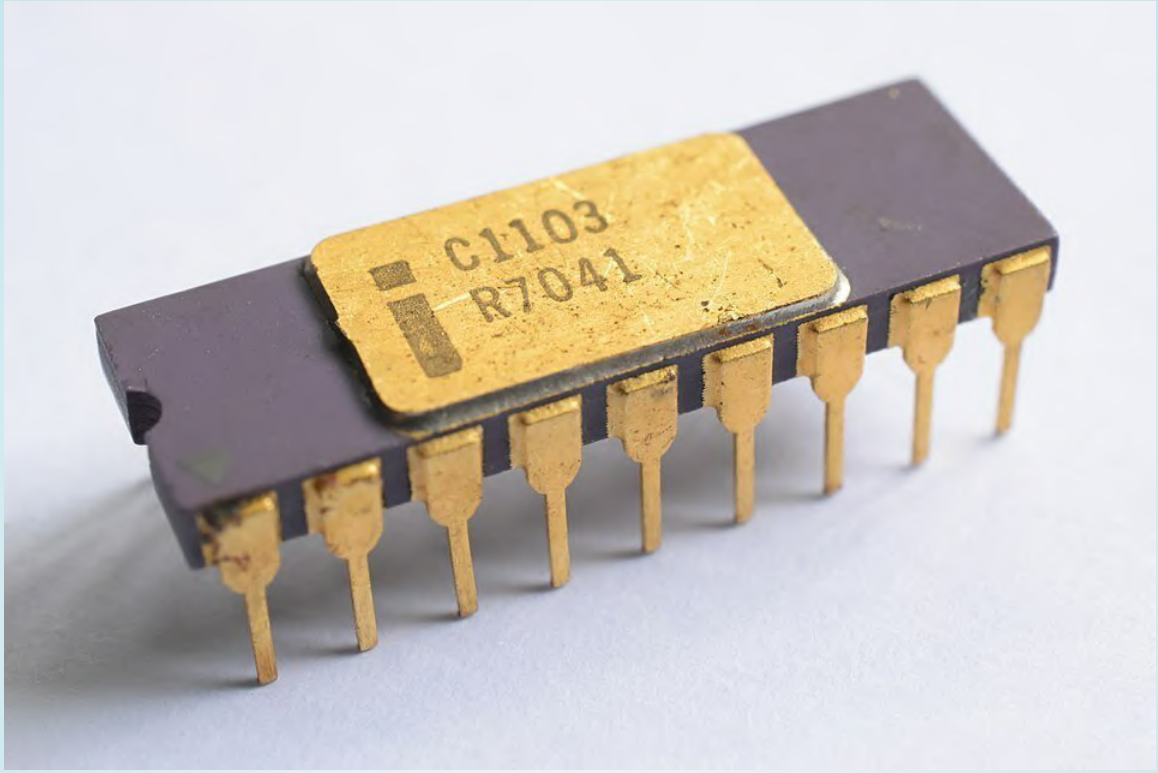
Srsly?!....



Intel 4K 2107 DRAM (~1974)

Similar chip - Thomas Nguyen, CC - https://commons.wikimedia.org/wiki/File:Intel_C1103.jpg

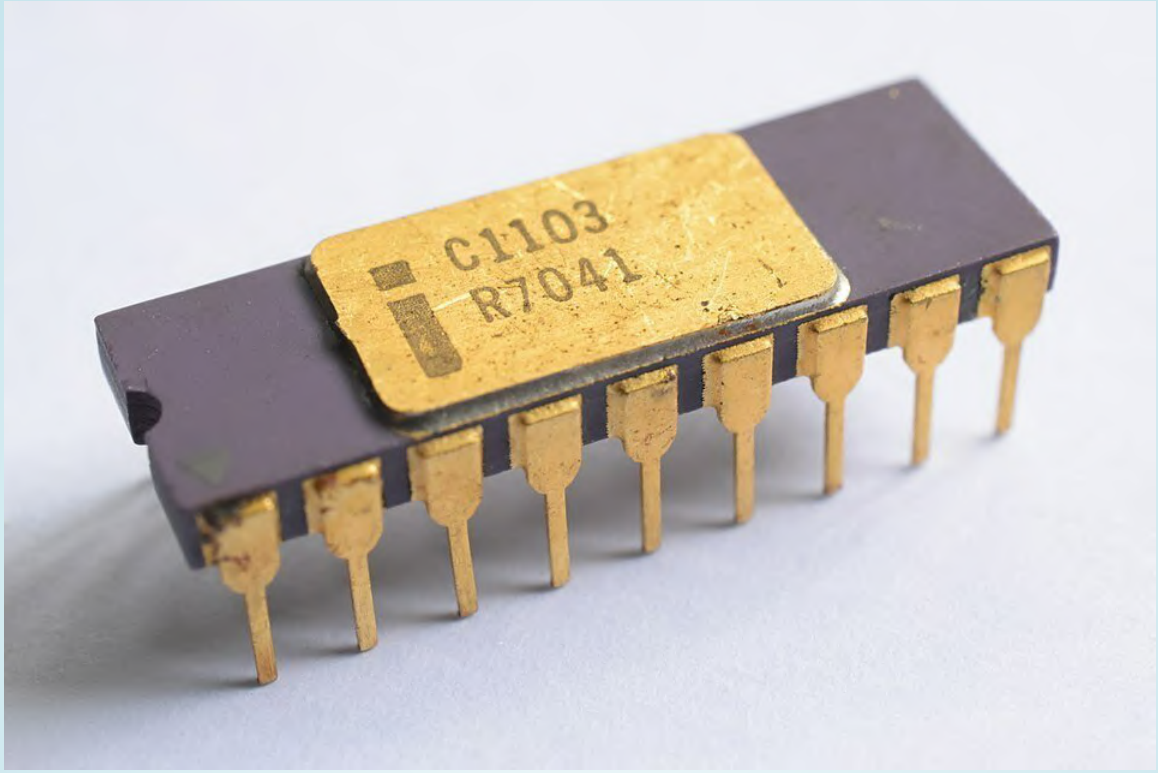
Srsly?!....



Intel 4K 2107 DRAM (~1974)

Ceramic from new factory on the Green River in Colorado...

Srsly?!....

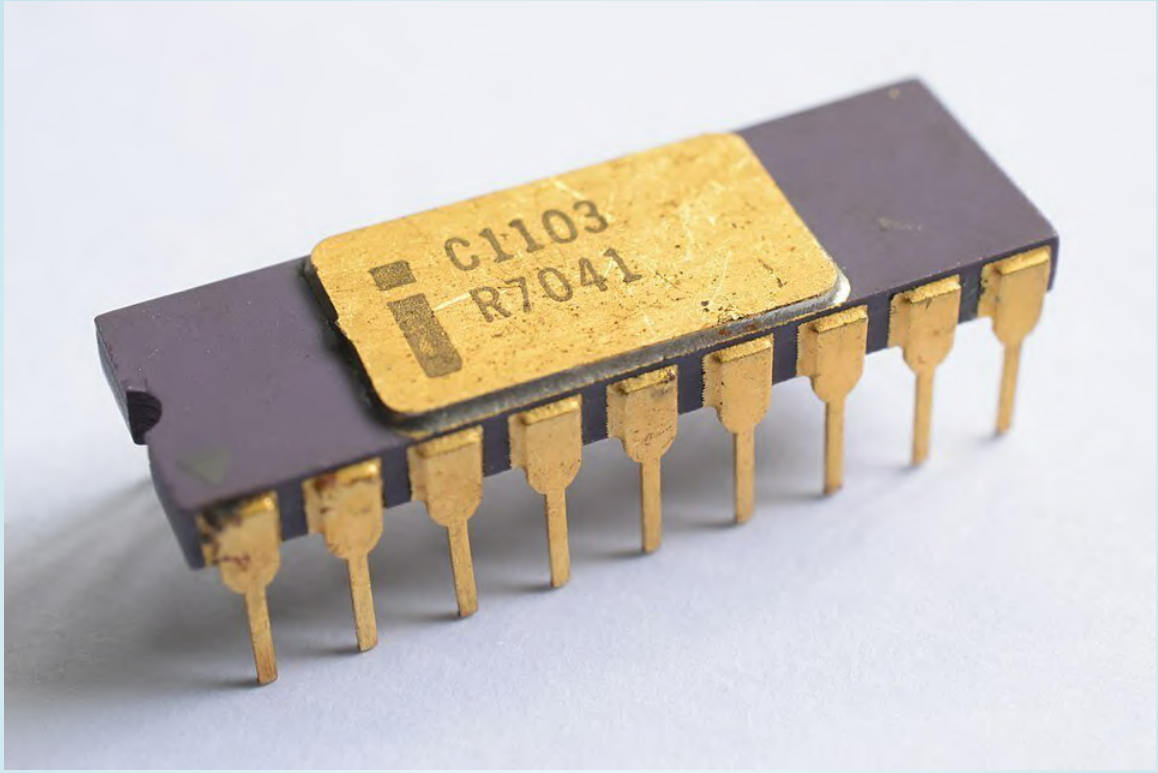


Intel 4K 2107 DRAM (~1974)

Ceramic from new factory on the Green River in Colorado...

built downstream from an old uranium mine.

Srsly?!....



Intel 4K 2107 DRAM (~1974)

Ceramic from new factory on the Green River in Colorado...

built downstream from an old uranium mine.

Water contaminated with U238, Th232 and daughter products

Qantas Flight 72 - 7 October 2008

https://en.wikipedia.org/wiki/Qantas_Flight_72

Qantas Flight 72 - 7 October 2008

- Flight from Singapore (SIN) -> Perth (PER) - Airbus A330-303

https://en.wikipedia.org/wiki/Qantas_Flight_72

Qantas Flight 72 - 7 October 2008

- Flight from Singapore (SIN) -> Perth (PER) - Airbus A330-303
- Bitflip in Air Data Inertial Reference Units - Alt -> AOA
  8.4 degrees pitch down and rapidly descending 200m, −0.8 g

https://en.wikipedia.org/wiki/Qantas_Flight_72

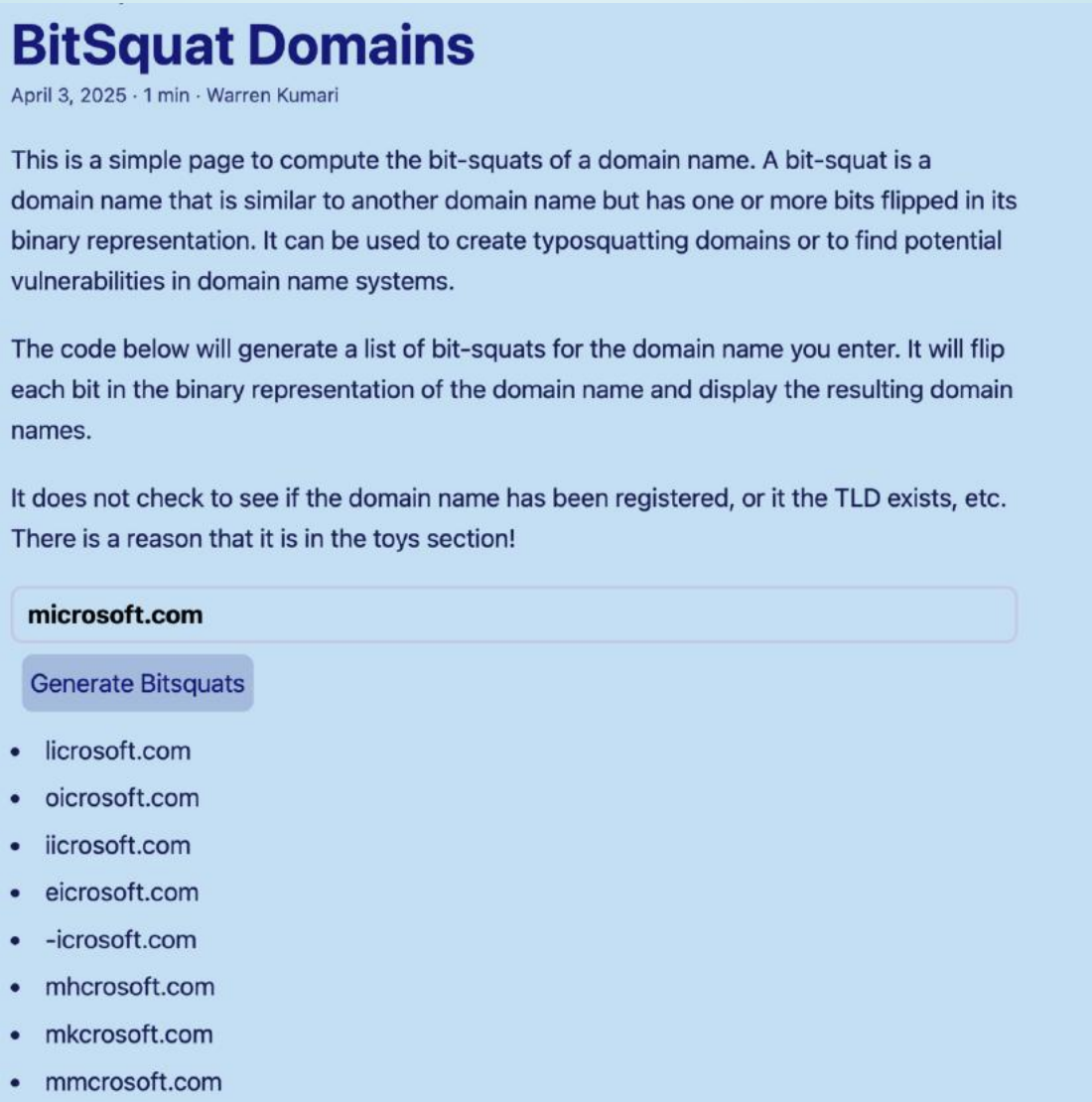
Qantas Flight 72 - 7 October 2008

- Flight from Singapore (SIN) -> Perth (PER) - Airbus A330-303
- Bitflip in Air Data Inertial Reference Units - Alt -> AOA
  8.4 degrees pitch down and rapidly descending 200m, −0.8 g
- 110 total injuries
  - 53 people hospitalized, 14 people airlifted

https://en.wikipedia.org/wiki/Qantas_Flight_72

Doing this again...

- Original work and attention mostly 2011, I presented in 2018



BitSquat Domains

April 3, 2025 · 1 min · Warren Kumari

This is a simple page to compute the bit-squats of a domain name. A bit-squat is a domain name that is similar to another domain name but has one or more bits flipped in its binary representation. It can be used to create typosquatting domains or to find potential vulnerabilities in domain name systems.

The code below will generate a list of bit-squats for the domain name you enter. It will flip each bit in the binary representation of the domain name and display the resulting domain names.

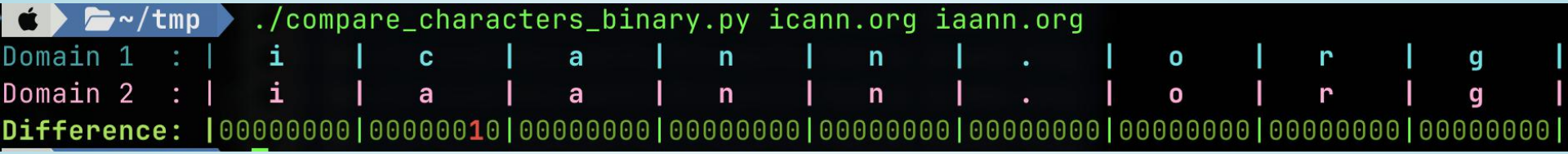
It does not check to see if the domain name has been registered, or it the TLD exists, etc. There is a reason that it is in the toys section!

microsoft.com

Generate Bitsquats

- licrosoft.com
- oicrosoft.com
- iicrosoft.com
- eicrosoft.com
- -icrosoft.com
- mhcrosoft.com
- mkcrosoft.com
- mmcrosoft.com

Doing this again...



- bankofamermca.com
- chaqe.com
- chasg.com
- cxase.com
- fbkdn.net
- googneapis.com
- iaann.org
- ibann.org
- icafn.org
- icaln.org
- licrosoft.com
- microroft.com
- microsmft.com
- microsofv.com
- microsont.com
- mmcrosoft.com
- you4ube.com

Doing this again...

Setup webserver to capture:

- "Expanded names"
- SNI information
- Cookies
- URLs

Boring... these are just typos...

- Tried to choose names which are "far" on the keyboard.

Boring... these are just typos...

- Tried to choose names which are "far" on the keyboard.
- Expanded names:
  - microsont.com ->
  - msedge.b.tlu.dl.delivery.mp.microsont.com

Boring... these are just typos...

- Tried to choose names which are "far" on the keyboard.
- Expanded names:
  - microsont.com ->
  - msedge.b.tlu.dl.delivery.mp.microsont.com
- API / "System" names:
  - access-point.cloudmessaging.edge.microsont.com

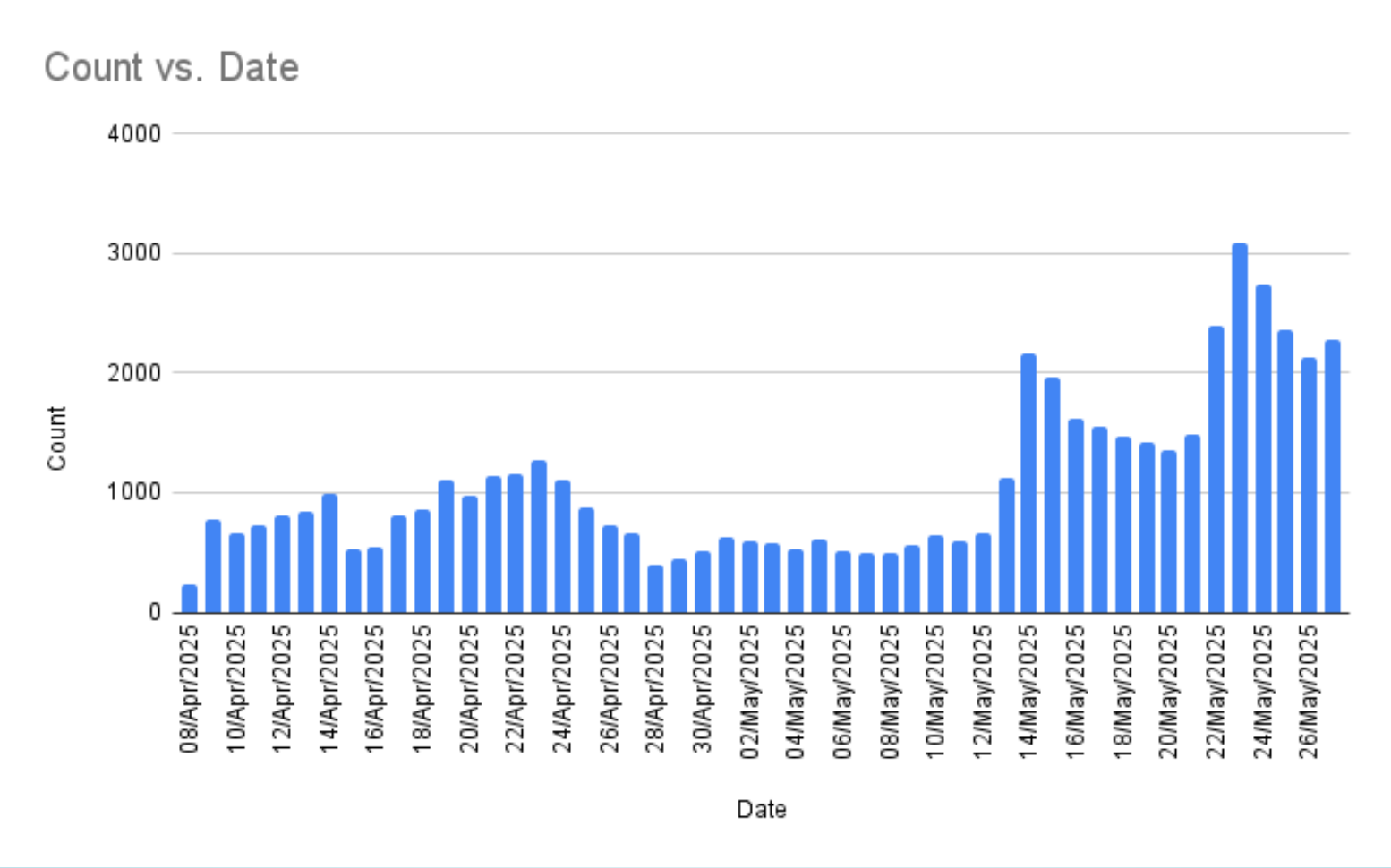
Boring... these are just typos...

- Tried to choose names which are "far" on the keyboard.
- Expanded names:
  - microsont.com ->
  - msedge.b.tlu.dl.delivery.mp.microsont.com
- API / "System" names:
  - access-point.cloudmessaging.edge.microsont.com
- SNI names:
  - tlu.dl.delivery.mp.microsoft.com

Boring... these are just typos...

- Tried to choose names which are "far" on the keyboard.
- Expanded names:
  - microsont.com ->
  - msedge.b.tlu.dl.delivery.mp.microsont.com
- API / "System" names:
  - access-point.cloudmessaging.edge.microsont.com
- SNI names:
  - tlu.dl.delivery.mp.microsoft.com
- Full URLs:
  - https://dotnet.microsmft.com/en-us/download/dotnet/thank-you/runtime-desktop-6.0.12-windows-x64-installer

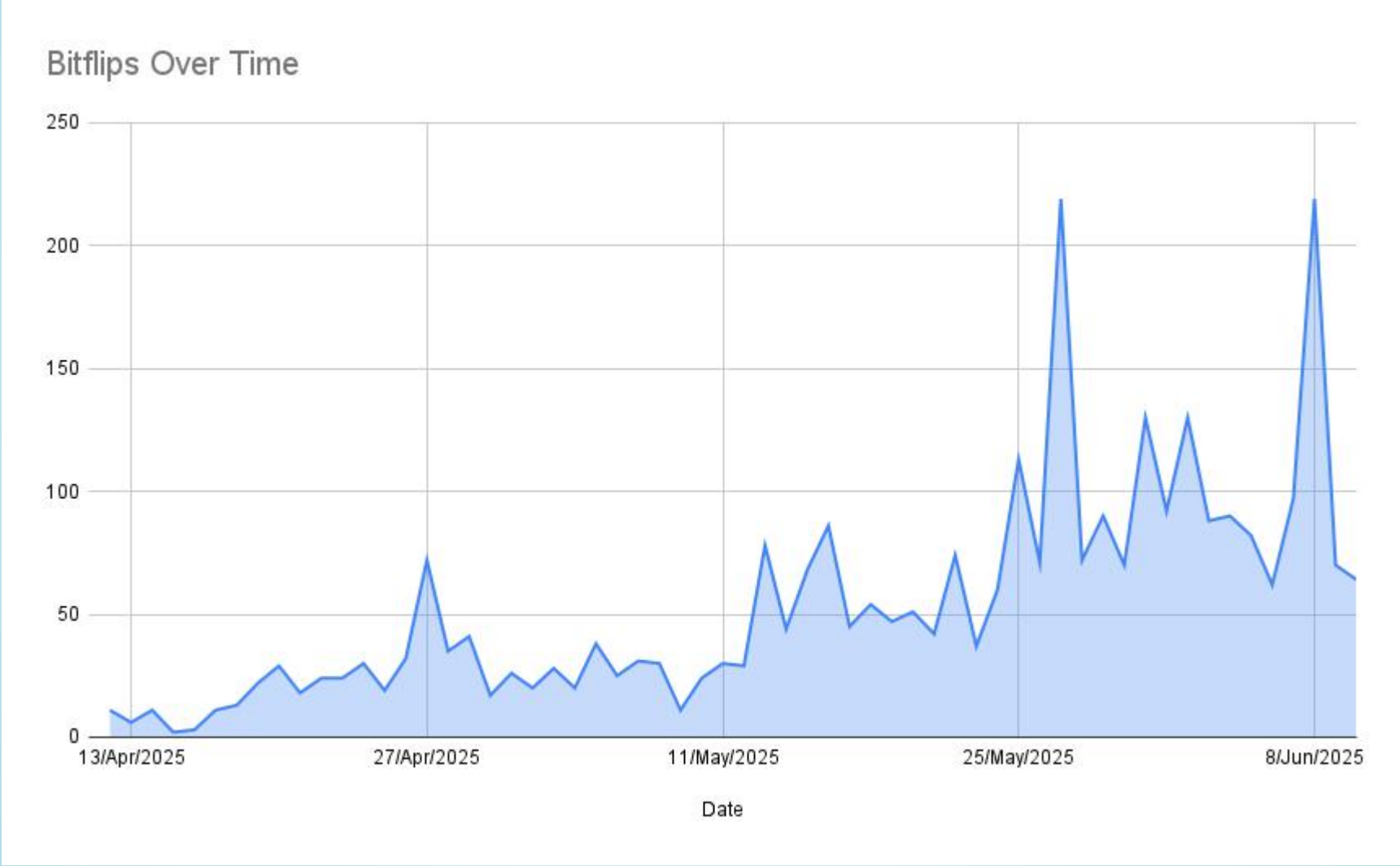
Some stats... (~1 month)



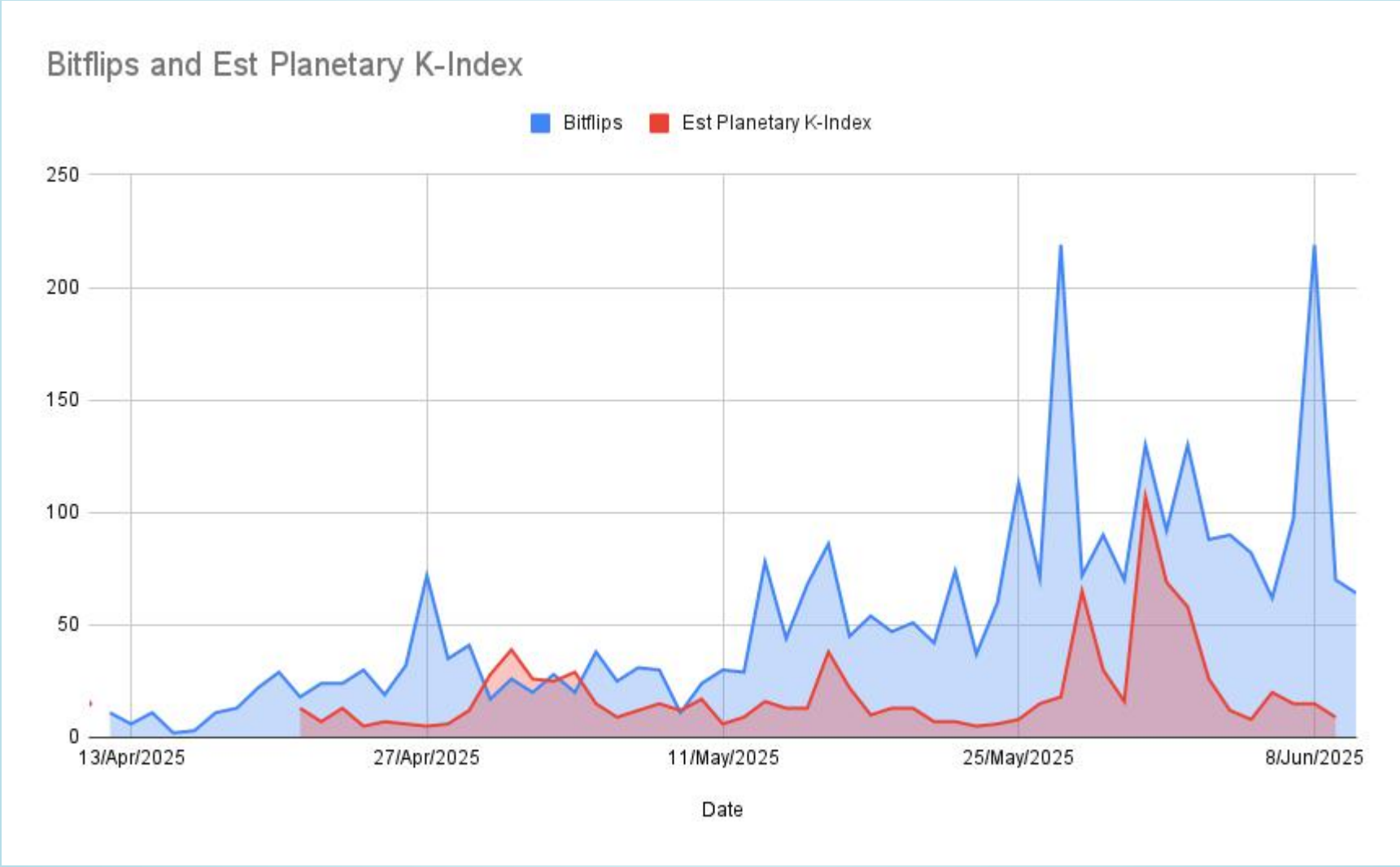
Total: 54146 - 1 month 18 days

Ignoring scrapers, cxase.com, etc.

Some stats... (1 month)



Some stats... (1 month)



Expanded names...

(<something>.<bitsquat>): 487 unique

```
1073 msdn.microsont.com
 738 go.microsont.com
 727 xevbaplay.googneapis.com
 719 teredo.ipv6.microsmft.com
 352 self.events.data.licrosoft.com
 347 msedge.b.tlu.dl.delivery.mp.microsmft.com
 102 internal.revenue.service.62528.cxase.com
  46 bk.bankofamermca.com
  42 video.fcmb11-1.fna.fbkdn.net
  41 content.office.microsont.com
  39 storage.googneapis.com
  39 delivery.mp.microsmft.com
  37 android.googneapis.com
```

Expanded names...

SNI: 48 unique "real" domains

- go-eu.trouter.teams.microsoft.com
- settings-win.data.microsoft.com
- video.fcmb11-1.fna.fbcdn.net
- geover.prod.do.dsp.mp.microsoft.com
- edge.microsoft.com
- scontent.xx.fbcdn.net
- mobileappcommunicator.auth.microsoft.com
- api-apac.flightproxy.teams.microsoft.com
- storage.googleapis.com
- geover.prod.do.dsp.mp.microsoft.com
- play.googleapis.com
- self.events.data.microsoft.com
- icann.org

SNI: 48 unique "real" domains

"login" URLs

"login URLs": 23 unique. E.g:

- secure.bankofamer**m**ca.com/login/sign-in/signOnScreen.go/login.html HTTP/1.1
- /common/oauth2/v2.0/authorize?client_id=18fbca16[...]
- login.microso**n**t.com

"login" URLs

Javascript...

- https://learn.microsont.com/static/third-party/adobe-target/at-js/2.9.0/at.js
- https://wcpstatic.licrosoft.com/mscc/lib/v2/wcp-consent.js
- https://learn.microsont.com/static/assets/0.4.030556769/scripts/en-us/index-docs.js
- https://www.chaqe.com/auth/fcc/js/channela.js?single

Javascript...

Executables...

- https://dotnet.microsont.com/zh-cn/download/dotnet/thank-you/runtime-desktop-6.0.12-windows-x64-installer?cid=getdotnetcorp

Executables...

Cookies!

Cookies!

```
Cookie:"PHPSESSID=gom[ELIDED]imkc3; _visitor_id=-
OP-kQ[ELIDED]B9F-q;
_auth_token=eyJ[ELIDED]CJ9.eyJ2a[ELIDED]Tl9.Y_SBEJG
GCRl_HB[ELIDED]QivY;
handl_landing_page=https%3A%2F%2Flivebh.com%2Fapart
ments%2Fconnection-at-buffalo-
pointe%2F%3Futm_medium%3Dredirect%26utm_campaign%3D
vanity%26original_referrer%3Dhttps%3A%2F%2Fliveatth
econnection.com; handl_ip=35.xxx.xxx.249;
handl_url_base=https%3A%2F%2Flivebh.com%2Fapartment
s%2Fconnection-at-buffalo-pointe%2F;
handl_url=https%3A%2F%2Flivebh.com%2Fapartments%2Fc
onnection-at-buffalo-
pointe%2F%3Futm_medium%3Dredirect%26utm_campaign%3D
vanity%26original_referrer%3Dhttps%3A%2F%2Fliveatth
econnection.com utm_campaign=vanity; "
```

Cookies!

```
Cookie:"FOTOGRAF=ae17[ELIDED]50b;GCs=CartItem1_92_0
3_87_UserName1_92_4_02_;MISCGCs=USERPC1_92_201463_8
7_USERLL1_92_39.0438%2C77.48793_87_USERST1_92_VA3_8
7_LOCST1_92_VA3_87_USERDMA1_92_5113_87_DT1_92_PC;
PHPSESSID=as[ELIDED]pf2;SignedIn=1;TS0133ea21=06[EL
IDED]0250cf07cd7f08e4ee976d8f593f1ab16f10962e1eabd0
6f75;_auth_token=eyJhbGc[ELIDED]Xo; _visitor_id=-
OP3[ELIDED]RJz-D;dergan=09cf3f[ELIDED]1d176937;
elegantsession=1129277[ELIDED]a6ea2adc3;handl_ip=3.
xxx.xxx.5;handl_landing_page=https%3A%2F%2Fatlantas
pecializedcare.com%2F; [...]"
```

Cookies!

```
$ less bitsquat_cookies_access.log | grep -v wp-log
|grep -v x.js | grep -Ei '(token|auth)' | wc -l
```

136

TLS will save us, right?! Right?!

TLS will save us, right?! Right?!

TLS will save us, right?! Right?!

```
127.0.0.1 - - [22/May/2025:20:58:34 +0000] "GET /
HTTP/1.1" 200 255 "-" "-" SNI:"microsoft.com"
Cookie:"esctx-[ELIDED]=AQ[ELIDED]AA;
fpc=Aj[ELIDED]AA; x-ms-gateway-slice=estsfd;
stsservicecookie=estsfd;"
```

TLS will save us, right?! Right?!

```
127.0.0.1 - - [22/May/2025:20:58:34 +0000] "GET /
HTTP/1.1" 200 255 "-" "-" SNI:"microsoft.com"
Cookie:"esctx-[ELIDED]=AQ[ELIDED]AA;
fpc=Aj[ELIDED]AA; x-ms-gateway-slice=estsfd;
stsservicecookie=estsfd;"
```

Let's prevent bitflips of TLDs!

Let's prevent bitflips of TLDs!

```
~/src/code/python/bit-squat  git master !1  ./closest_tlds.py --gtld
abb -> abc (1)          00000000|00000000|00000001|
aco -> eco (1)          00000100|00000000|00000000|
bar -> car (1)          00000001|00000000|00000000|
best -> rest (1)        00010000|00000000|00000000|00000000|
bio -> jio (1)          00001000|00000000|00000000|
bio -> rio (1)          00010000|00000000|00000000|
bms -> bmw (1)          00000000|00000000|00000100|
bom -> boo (1)          00000000|00000000|00000010|
bom -> com (1)          00000001|00000000|00000000|
boo -> foo (1)          00000100|00000000|00000000|
booking -> cooking (1)00000001|00000000|00000000|00000000|00000000|00000000|0
bot -> jot (1)          00001000|00000000|00000000|
box -> fox (1)          00000100|00000000|00000000|
cab -> car (1)          00000000|00000000|00010000|
cafe -> safe (1)        00010000|00000000|00000000|00000000|
```

Let's prevent bitflips of TLDs!

```
~/src/code/python/bit-squat  git master !1  ./closest_tlds.py --gtld
abb -> abc (1)          00000000|00000000|00000001|
aco -> eco (1)          00000100|00000000|00000000|
bar -> car (1)          00000001|00000000|00000000|
best -> rest (1)        00010000|00000000|00000000|00000000|
bio -> jio (1)          00001000|00000000|00000000|
bio -> rio (1)          00010000|00000000|00000000|
bms -> bmw (1)          00000000|00000000|00000100|
bom -> boo (1)          00000000|00000000|00000010|
bom -> com (1)          00000001|00000000|00000000|
boo -> foo (1)          00000100|00000000|00000000|
booking -> cooking (1)00000001|00000000|00000000|00000000|00000000|00000000|0
bot -> jot (1)          00001000|00000000|00000000|
box -> fox (1)          00000100|00000000|00000000|
cab -> car (1)          00000000|00000000|00010000|
cafe -> safe (1)        00010000|00000000|00000000|00000000|
```

... 60...

Let's prevent bitflips of TLDs!

... 60...

Let's prevent bitflips of TLDs!

... 60...

¯_(ツ)_/¯

Let's prevent bitflips of TLDs!

Let's prevent bitflips of TLDs!

.com -> .bom

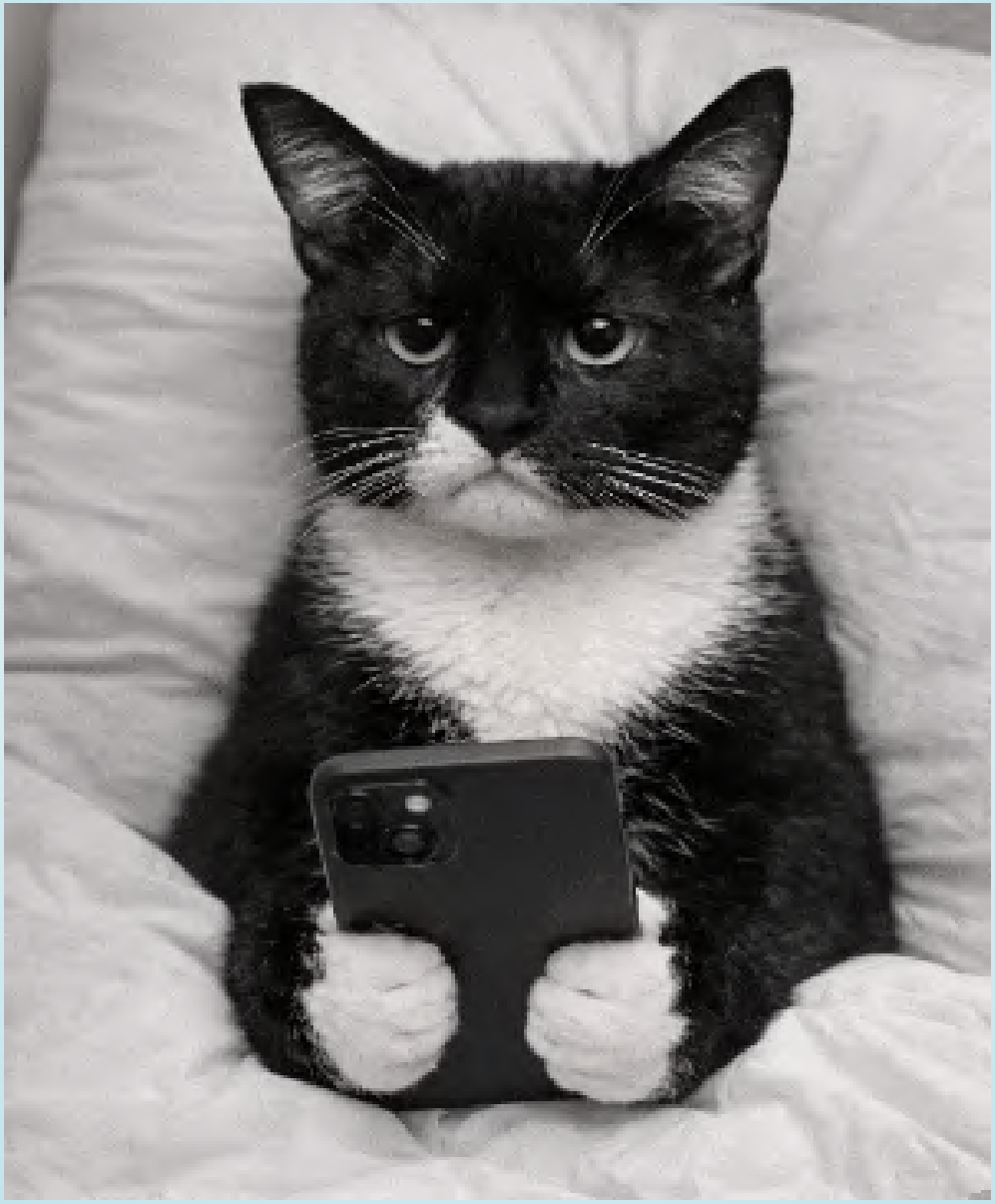
Let's prevent bitflips of TLDs!

.com -> .bom

Thanks to NIC.br for taking this seriously...

Conclusion?!

Conclusion ?!



Questions?!

This is why we can't have nice things.

This is why we can't have nice things.

- Found lots of lookups for things like:

```
http://internal.revenue.service.53093.cxase.com/department421658
```

This is why we can't have nice things.

- Found lots of lookups for things like:

```
http://internal.revenue.service.53093.cxase.com/department421658
```

- These seemed a: scary and b: fascinating...

This is why we can't have nice things.

- Found lots of lookups for things like:

```
http://internal.revenue.service.53093.cxase.com/department421658
```

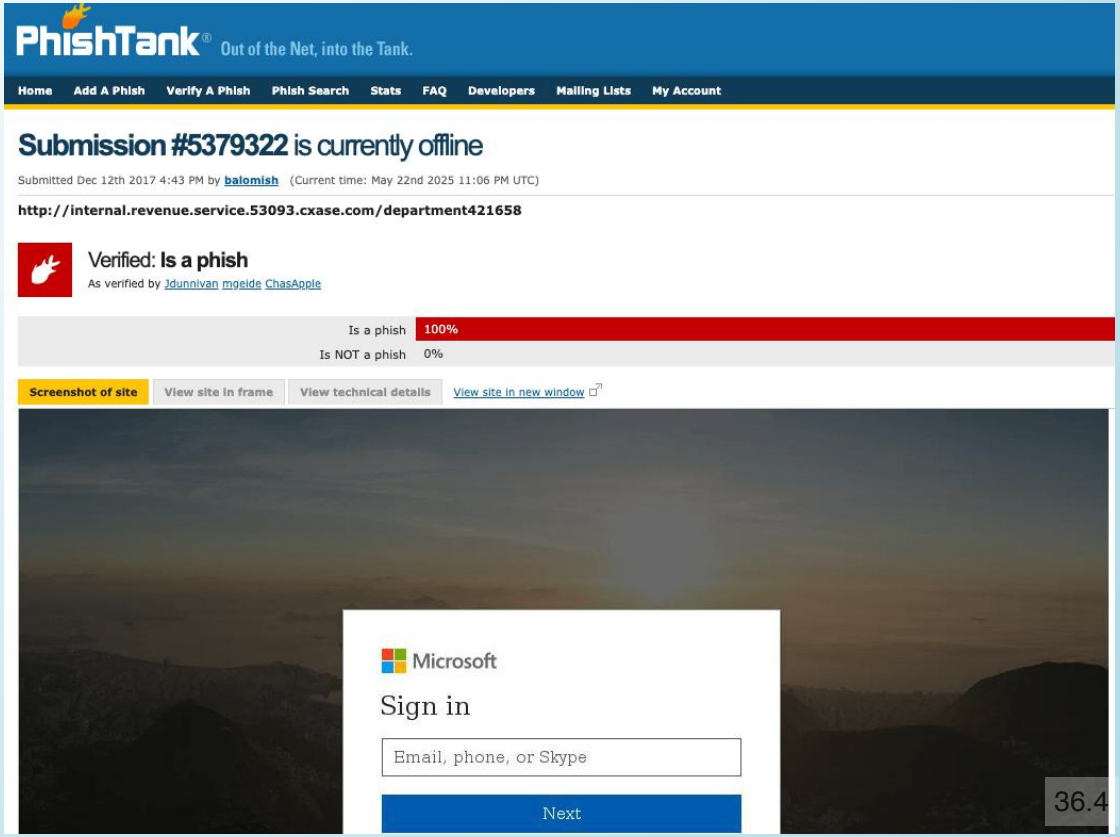
- These seemed a: scary and b: fascinating...
- ... just stumbled over old phishing campaign...

This is why we can't have nice things.

- Found lots of lookups for things like:

`http://internal.revenue.service.53093.cxase.com/department421658`

- These seemed a: scary and b: fascinating...
- ... just stumbled over old phishing campaign...



Moar...

- In the 2003 elections in Brussels's municipality Schaerbeek (Belgium), an anomalous recorded number of votes triggered an investigation that concluded an SEU was responsible for giving a candidate named Maria Vindevoghel 4,096 extra votes.

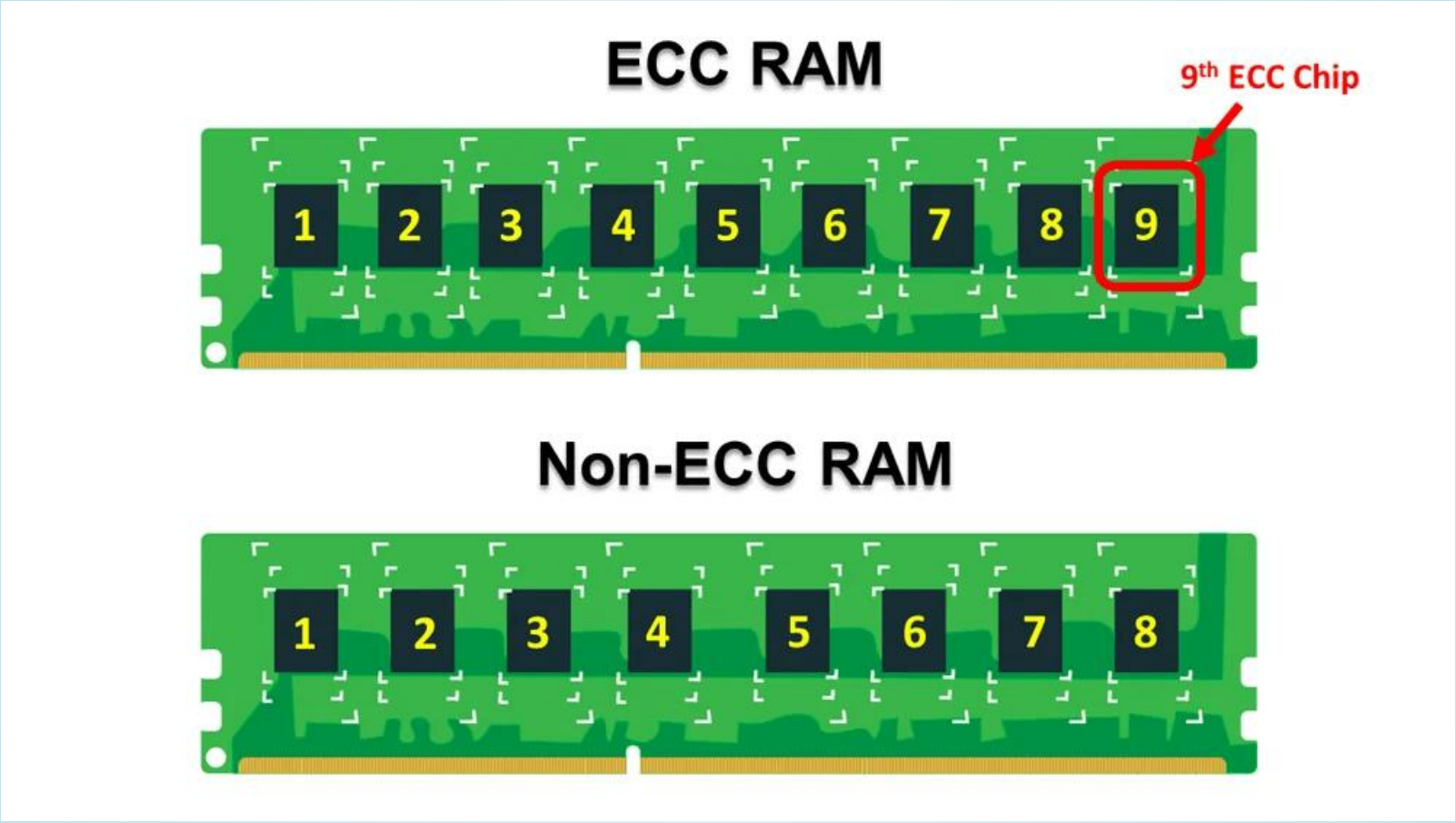
Maria Vindevoghel, Workers' Party of Belgium.

Source: nieuwsblad.be

When it rains, it pours...

- When one bit flips, often many do.
- E.g:
  - `https://dotnet.microsoft.com/zh-cn/download/dotnet/thank-you/runtime-desktop-6.0.12-windows-x64-installer?cid=getdotnetcorp`
- was actually:
  - `dotnet.microsont.com/zn-cn/downioad/dotnet/tnank-you/runtime-desktOD=6.0.12-windows-x64-installer?cid=getdotnetcorp`

Doesn't ECC solve this?!



- Kinda... But ECC RAM is expensive, and is only really deployed on server type devices, not phones and laptops...

Source: corsair.com

How often does this happen?!

- Soft Error Rate (SER) is measured in FIT units (failures in time). 1 FIT denotes one failure per billion device hours (114,077 years).
- SER of 1Mbit of SRAM [...], is typically in the order of 1,000 FIT for modern process technologies.
- 1GB = 8192Mbit. This is 8,192,000 FIT
- This is roughly once per 5 days!
- DRAM FIT is / was somewhat lower than SRAM, but lower voltages and cell capacitance / potential wells has made this flip

Data from: "SOFT ERROR ISSUE AND IMPORTANCE LOW ALPHA SOLDERS FOR MICROELECTRONICS PACKAGES"

Not new...

Based on work by Artem Dinaburg

- Paper: *Bitsquatting: DNS Hijacking without Exploitation - Blackhat 2011*
- Slides: BITSQUATTING
- Video: *Defcon 19: Artem Dinaburg - Bit-squatting: DNS Hijacking Without Exploitation*

Earlier work...

Earlier work...

```
138.246.253.5 - - [13/Sep/2018:04:27:52 +0000] SNI: twitter.com "HEAD /
HTTP/1.1" 200 0 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.85 Safari/537.36"
"_"
71.62.75.209 - - [13/Sep/2018:14:10:03 +0000] SNI: www.twitter.com "GET /
HTTP/1.1" 200 647 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
"_"
163.172.4.153 - - [14/Sep/2018:06:31:53 +0000] SNI: - "GET / HTTP/1.1" 200
647 "http://twitter.com/" "Mozilla/5.0 (Windows NT 6.3; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
"_"
```

Earlier work...

```
138.246.253.5 - - [13/Sep/2018:04:27:52 +0000] SNI: twitter.com "HEAD /
HTTP/1.1" 200 0 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.85 Safari/537.36"
"_"
71.62.75.209 - - [13/Sep/2018:14:10:03 +0000] SNI: www.twitter.com "GET /
HTTP/1.1" 200 647 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
"_"
163.172.4.153 - - [14/Sep/2018:06:31:53 +0000] SNI: - "GET / HTTP/1.1" 200
647 "http://twitter.com/" "Mozilla/5.0 (Windows NT 6.3; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
"_"
```

```
root@ron[0]:~/tmp/tmp# grep twitter * | wc -l
102
```