

BitSquatting

...or 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"

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*

Explanation...

www.twitter.com:

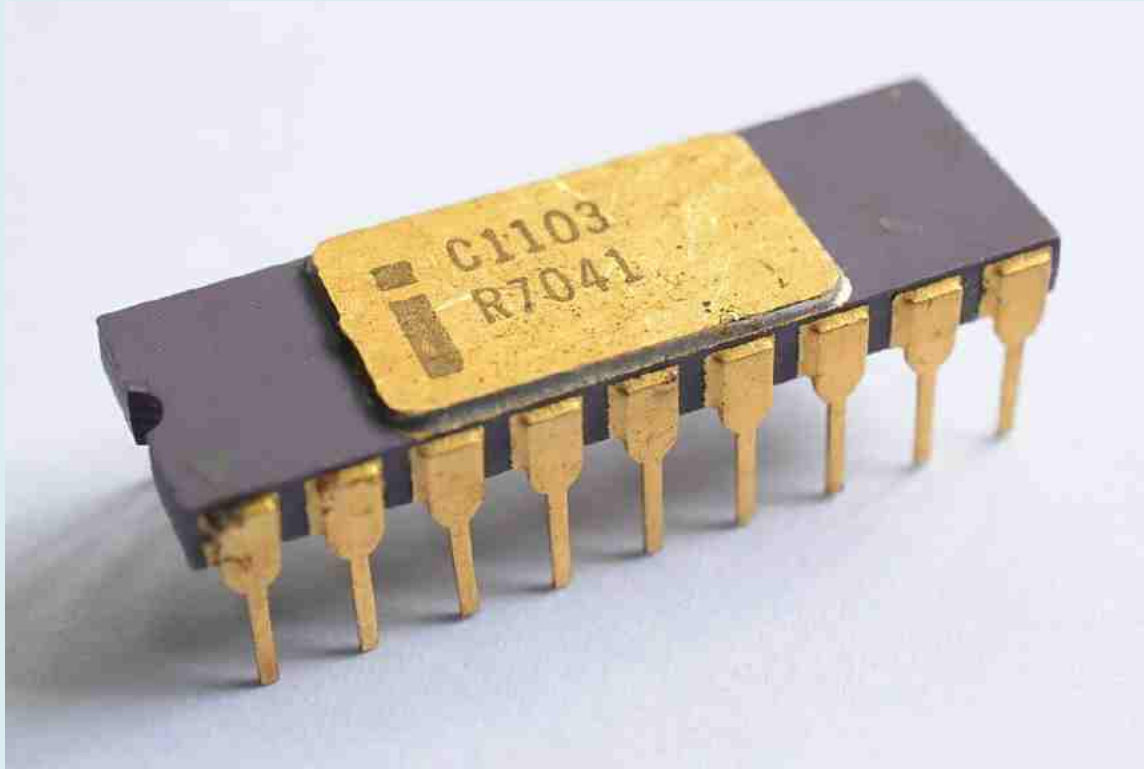
ASCII	t	w	i	t	t	e	r
Binary	01110100	01110111	01110100	01110100	01110100	01100101	01110010

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 |
```

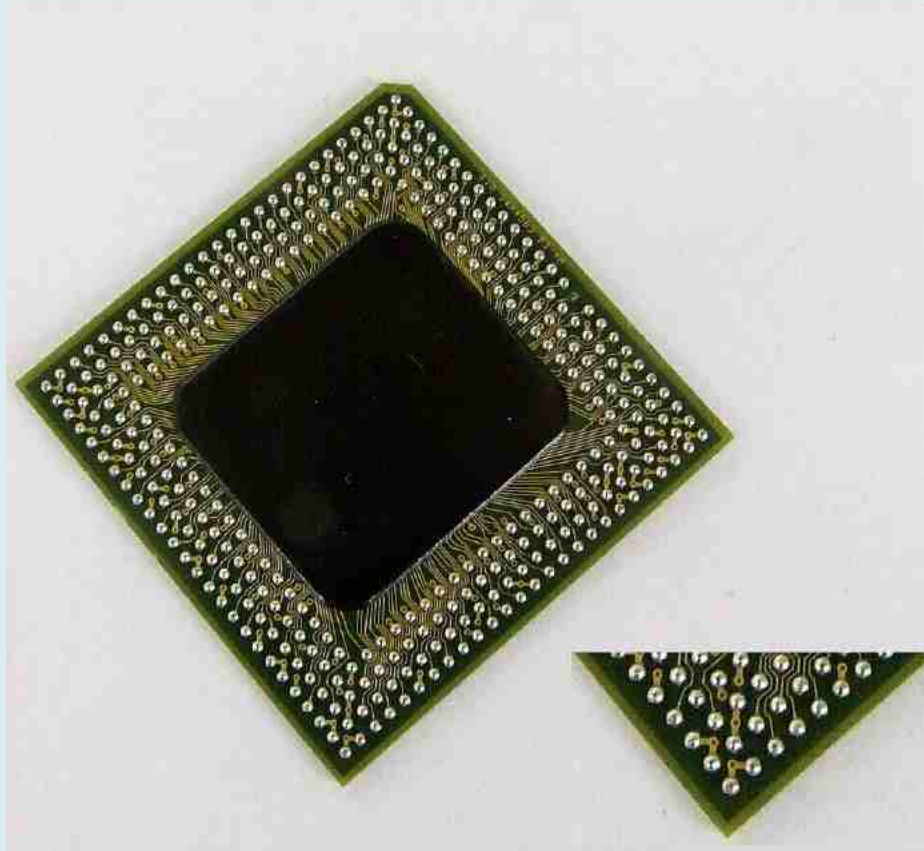
Srsly?!....



Intel 4K 2107 DRAM (~1974) - Ceramic from new factory on the Green River in Colorado, built downstream from tailings of an old uranium mine.

Water contaminated with U238, Th232 and daughter products

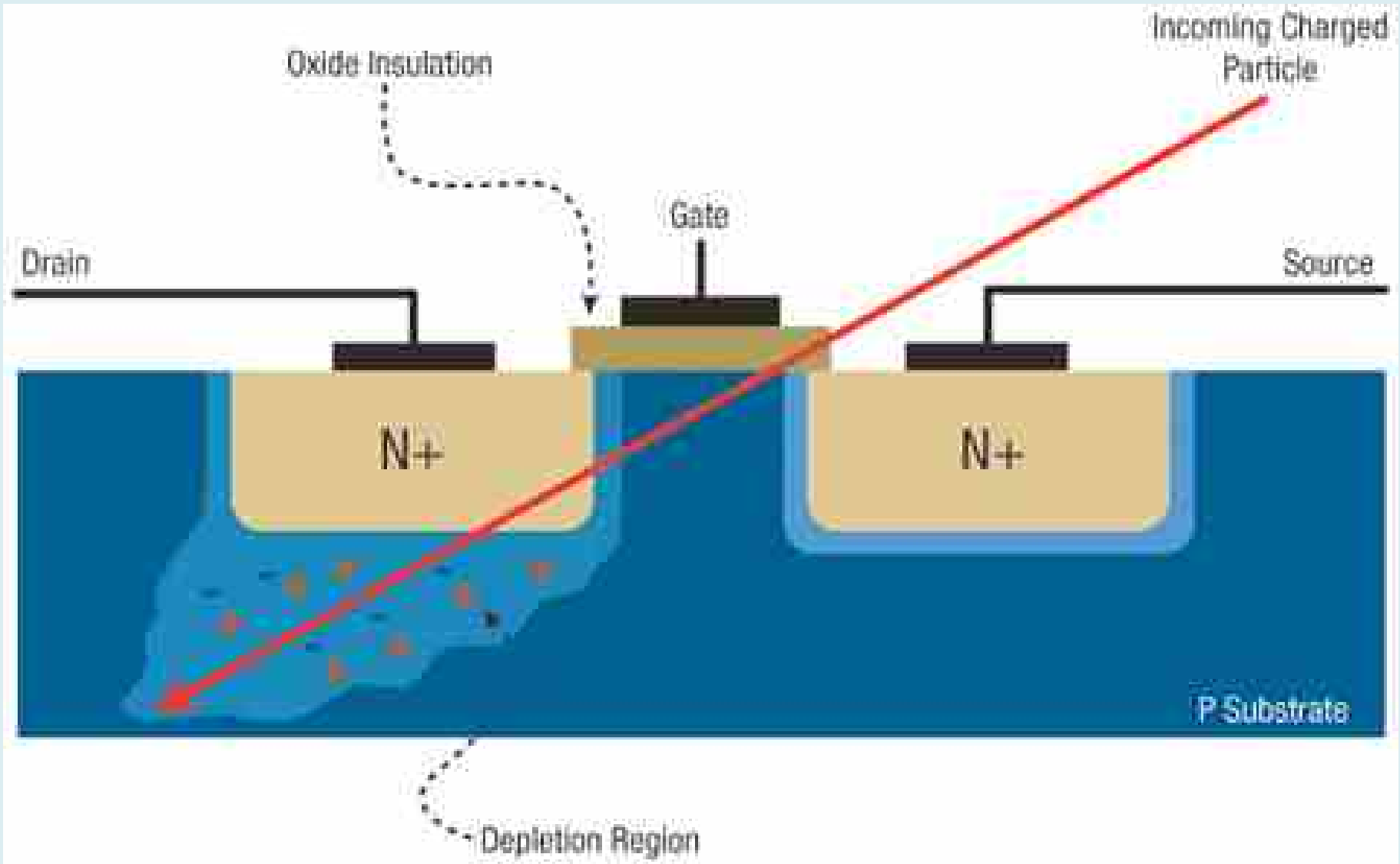
Srsly?!....



Lead in solder contains Pb-210 $\rightarrow$ (Bi-210 $\rightarrow$ Po-210) $\rightarrow$ Pb-206

Less of an issue with lead-free (e.g: Sn-Ag-Cu-Zn)

Srsly?!....



Srsly?!.....

Table 1: Memory errors per year:

Platf.	Tech.	Per machine				
		CE Incid. (%)	CE Rate Mean	CE Rate C.V.	CE Median Affet.	UE Incid. (%)
A	DDR1	45.4	19,509	3.5	611	0.17
B	DDR1	46.2	23,243	3.4	366	–
C	DDR1	22.3	27,500	17.7	100	2.15
D	DDR2	12.3	20,501	19.0	63	1.21
E	FBD	–	–	–	–	0.27
F	DDR2	26.9	48,621	16.1	25	4.15
Overall	–	32.2	22,696	14.0	277	1.29

Platf.	Tech.	Per DIMM				
		CE Incid. (%)	CE Rate Mean	CE Rate C.V.	CE Median Affet.	UE Incid. (%)
A	DDR1	21.2	4530	6.7	167	0.05
B	DDR1	19.6	4086	7.4	76	–
C	DDR1	3.7	3351	46.5	59	0.28
D	DDR2	2.8	3918	42.4	45	0.25
E	FBD	–	–	–	–	0.08
F	DDR2	2.9	3408	51.9	15	0.39
Overall	–	8.2	3751	36.3	64	0.22

Type	Failures In Test/Mbit	Hours until error (128MB)	Hours until error (16GB)
Mfg1,4GB DIMM	4,100	240	1.92
Mfg6,4GB DIMM	11,000	89	0.71
Micron Est., 256MByte	120 (- 240)	8,100	64

Qantas Flight 72 - 7 October 2008

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



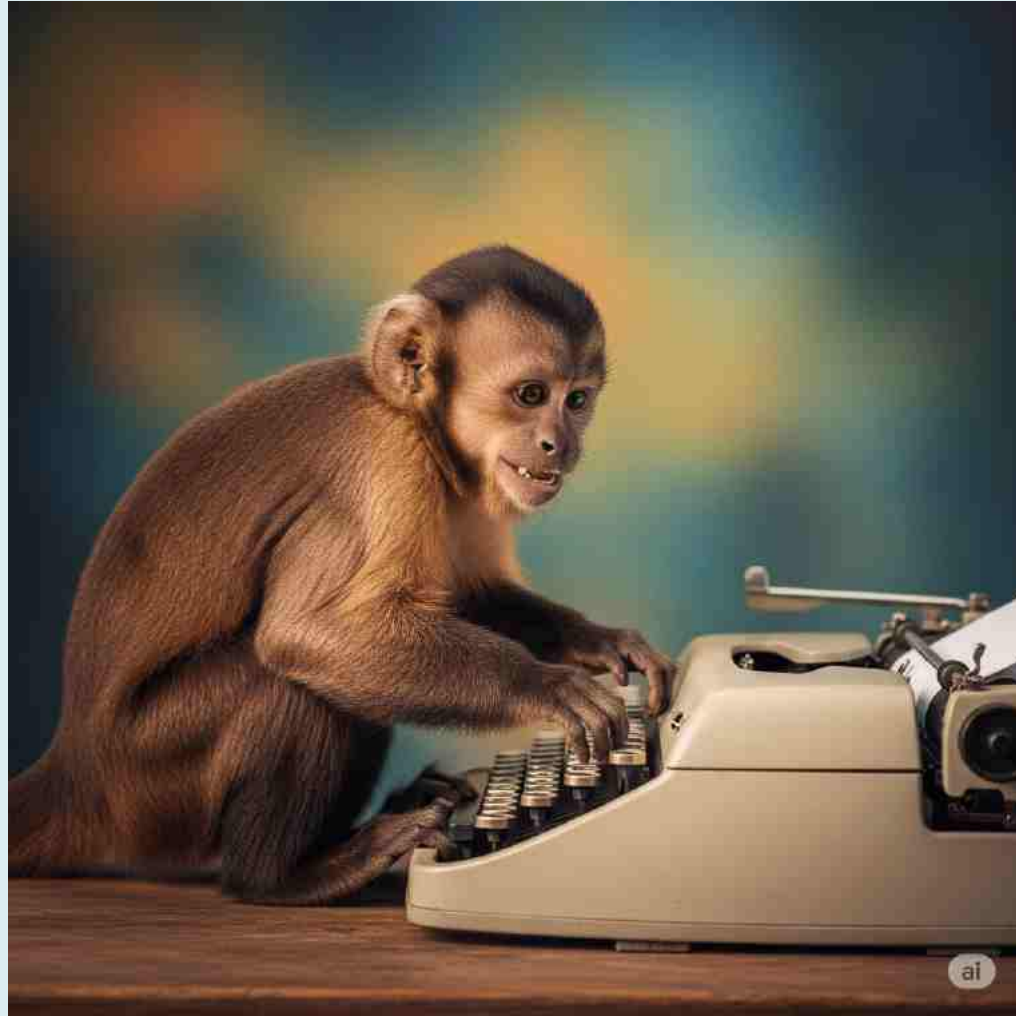
So what? I'm not a plane!

```
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
```

2025 Updates...

...are there still monkeys?!



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 if 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
- mhicrosoft.com
- mkicrosoft.com
- mmicrosoft.com

Doing this again...

```
Apple ~/tmp ./compare_characters_binary.py icann.org iaann.org
Domain 1 : | i | c | a | n | n | . | o | r | g |
Domain 2 : | i | a | a | n | n | . | o | r | g |
Difference: | 00000000 | 00000010 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 |
```

- bankofamermca.com
- chage.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
- mmicrosoft.com
- you4ube.com

Doing this again...

Setup webserver to capture:

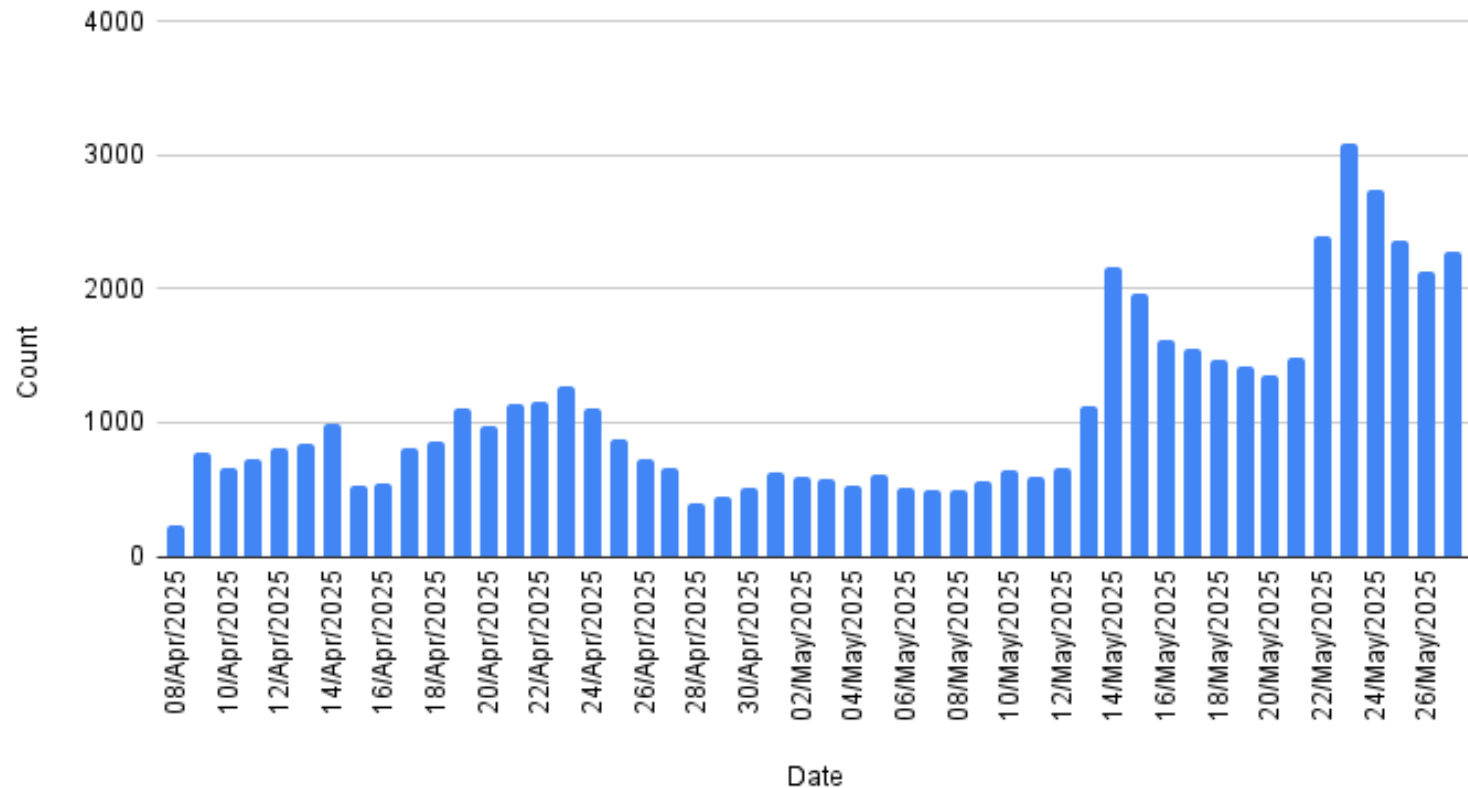
- "Expanded names"
- SNI information
- Cookies
- URLs

Boring... these are just typos...

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

Some stats... (~1 month)

Count vs. Date

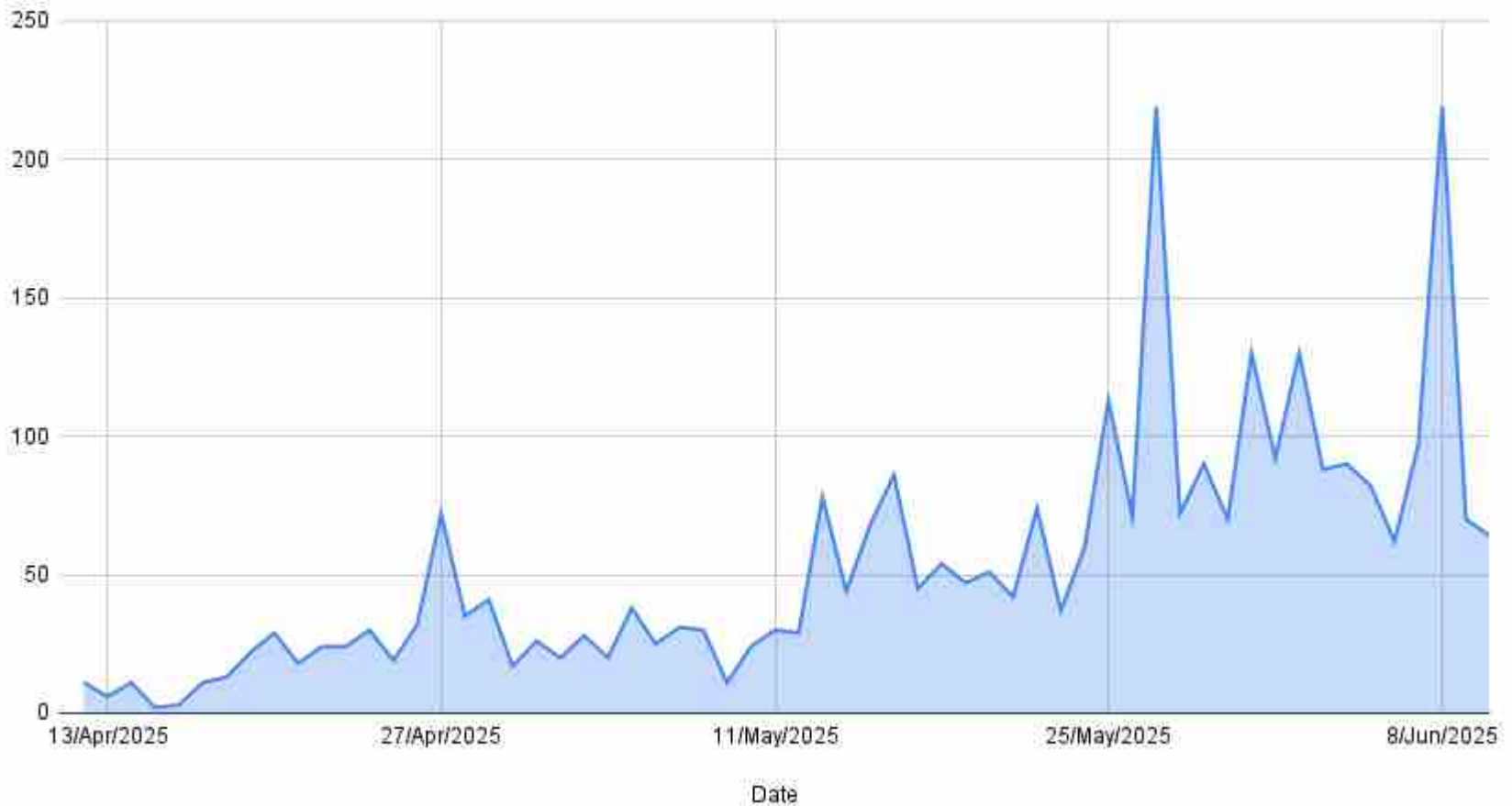


Total: 54146

Ignoring scrapers, cxase.com, etc.

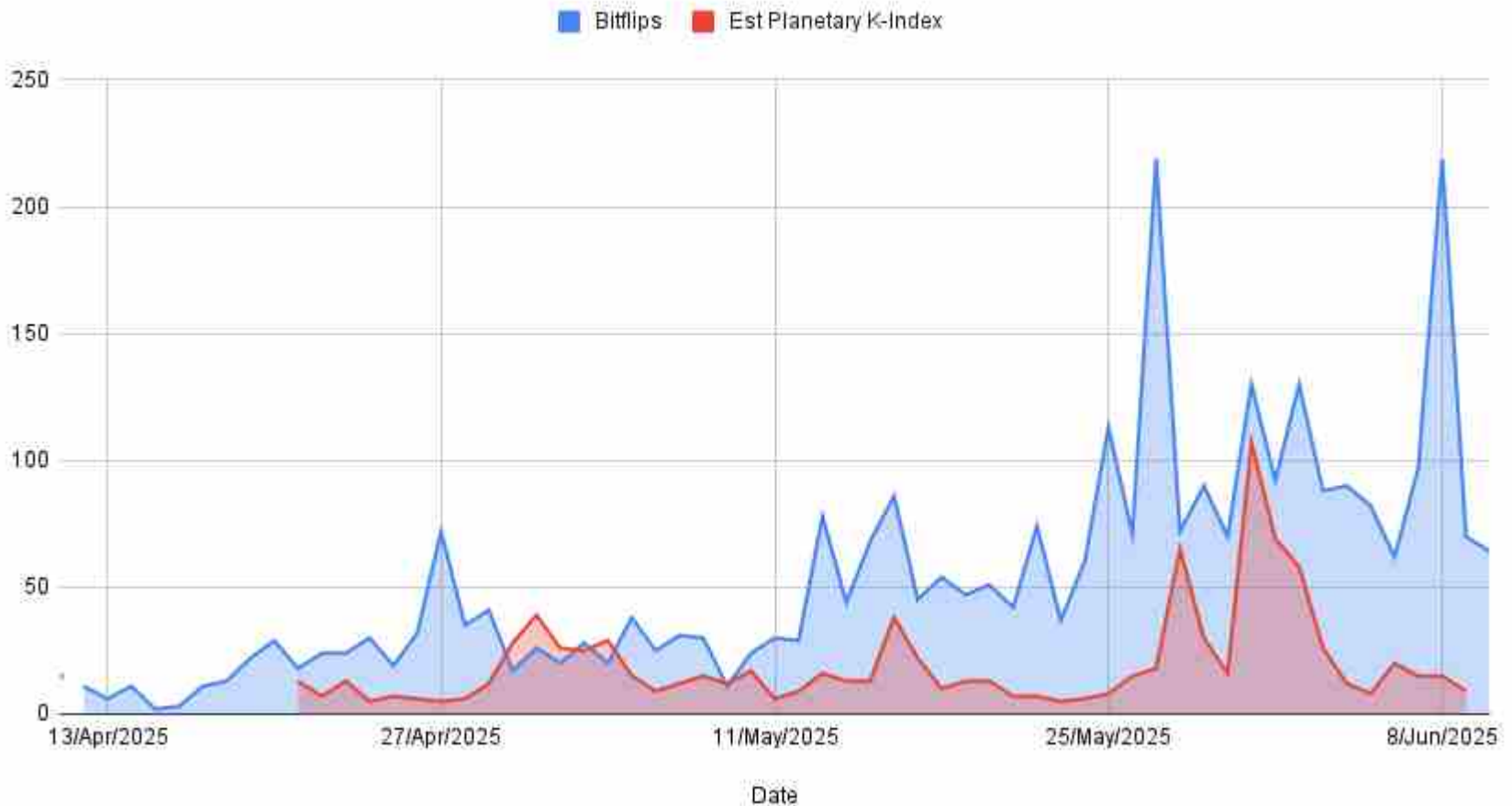
Some stats... (1 month)

Bitflips Over Time



Some stats... (1 month)

Bitflips and Est Planetary K-Index



Expanded names...

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

```
1073 msdn.microsoft.com
738 go.microsoft.com
727 xevbaplay.googleapis.com
719 teredo.ipv6.microsoft.com
352 self.events.data.microsoft.com
347 msedge.b.tlu.dl.delivery.mp.microsoft.com
102 internal.revenue.service.62528.cxase.com
46 bk.bankofamerica.com
42 video.fcmb11-1.fna.fbcdn.net
41 content.office.microsoft.com
39 storage.googleapis.com
39 delivery.mp.microsoft.com
37 android.googleapis.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.bankofamerica.com/login/sign-in/signOnScreen.go/login.html HTTP/1.1](#)
- [/common/oauth2/v2.0/authorize?client_id=18fbca16\[...\]](#)
- [login.microsoft.com](#)

"login" URLs



Javascript...

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

Javascript...



Executables...

- <https://dotnet.microsoft.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
```

47



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!

```
Apple ~/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|00000000|
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|
```

~_(\ツ)_/~

Questions?!

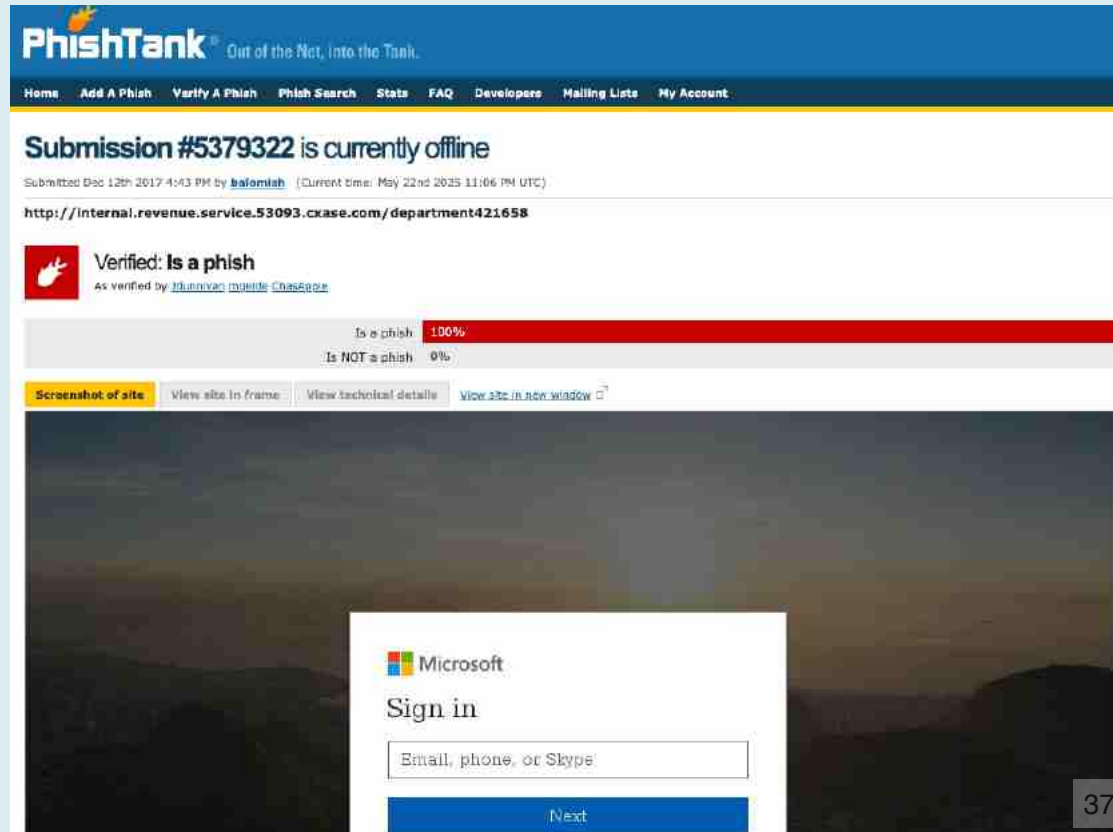


This is why we can't have nice things.

- Found lots of lookups for things like:

`http://internal.revenue.service.53093.cxase.com/departments421658`

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

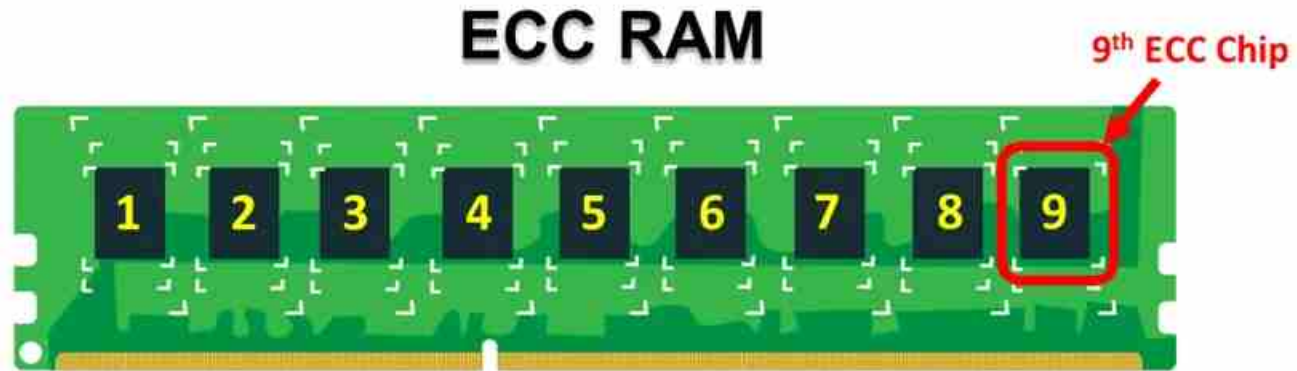


The screenshot shows the PhishTank website interface. At the top, the PhishTank logo is displayed with the tagline "Out of the Net, Into the Tank." Below the logo is a navigation bar with links: Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. The main content area displays the submission status for Submission #5379322, which is currently offline. It shows the submission was made on Dec 12th 2017 at 4:43 PM by user bafomiah, and the current time is May 22nd 2023 at 11:06 PM UTC. The URL being verified is `http://internal.revenue.service.53093.cxase.com/departments421658`. A red PhishTank logo icon is shown next to the text "Verified: Is a phish". Below this, it says "As verified by idunivas mobile ChasePage". A progress bar indicates that the site is 100% verified as a phish. Below the progress bar, there are buttons for "Screenshot of site", "View site in frame", "View technical details", and "View site in new window". The screenshot of the site shows a Microsoft sign-in page with the text "Sign in" and a field for "Email, phone, or Skype". A blue "Next" button is visible at the bottom of the sign-in form.

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-desktd=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...

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 8192,000 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

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.