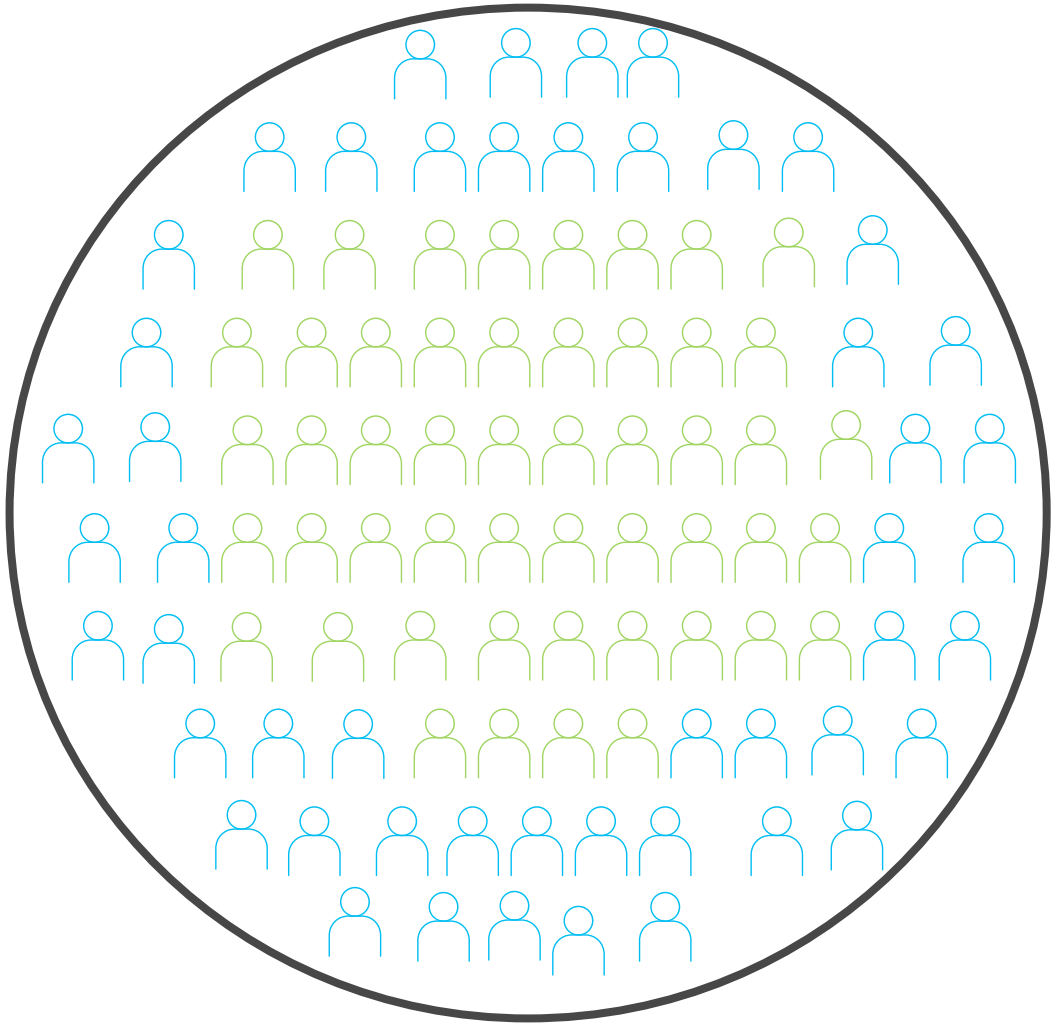
The Power of Community

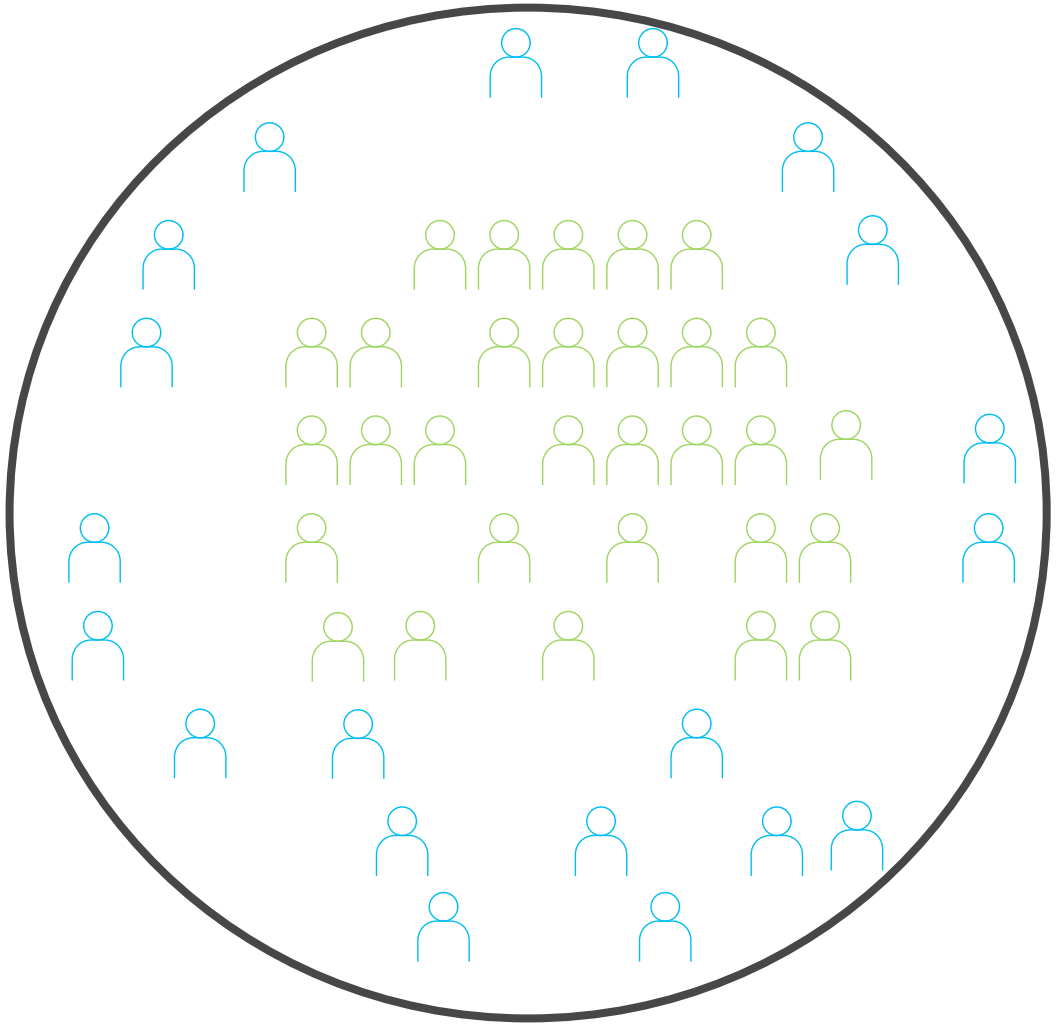
Robert Haynes



Take 100 people

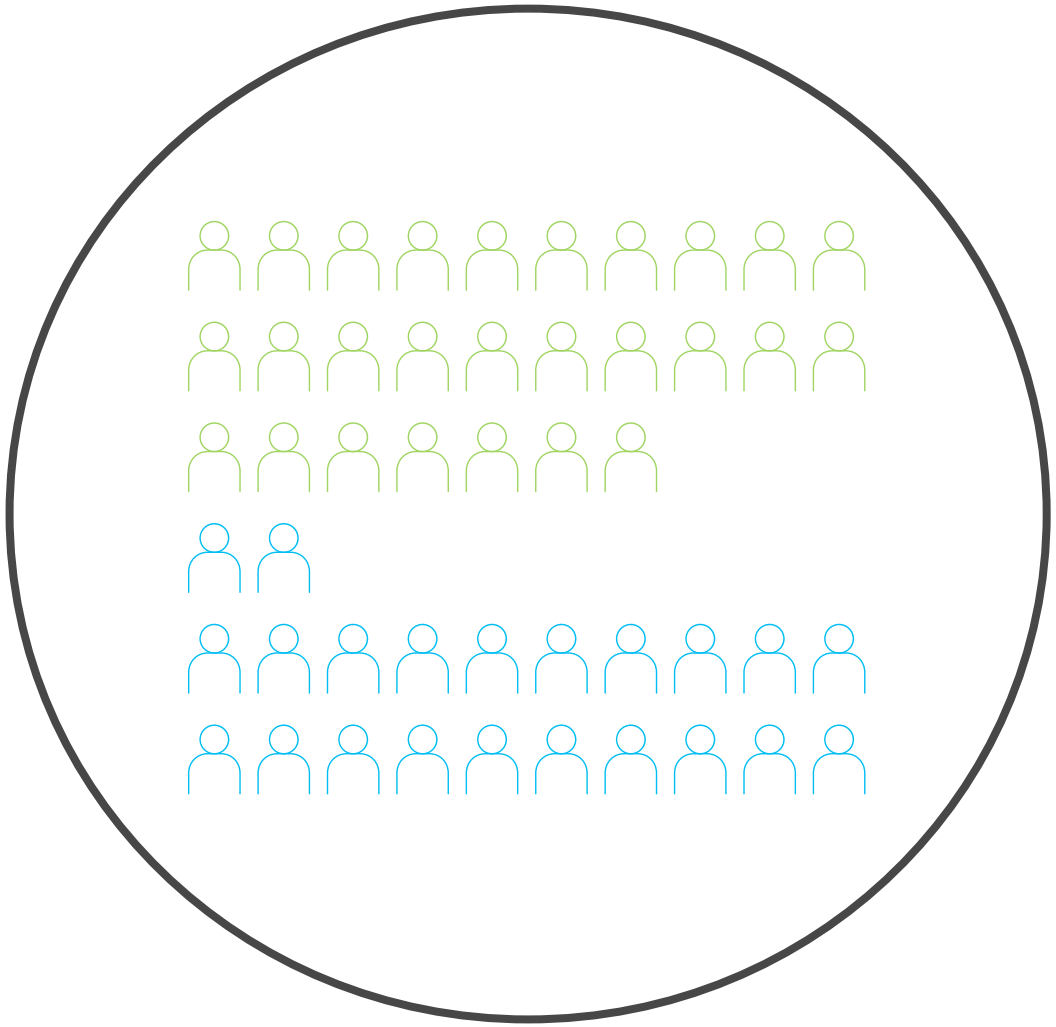
50 Have ‘strong community ties’, 50 don’t.

https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000316



Eventually 50 die

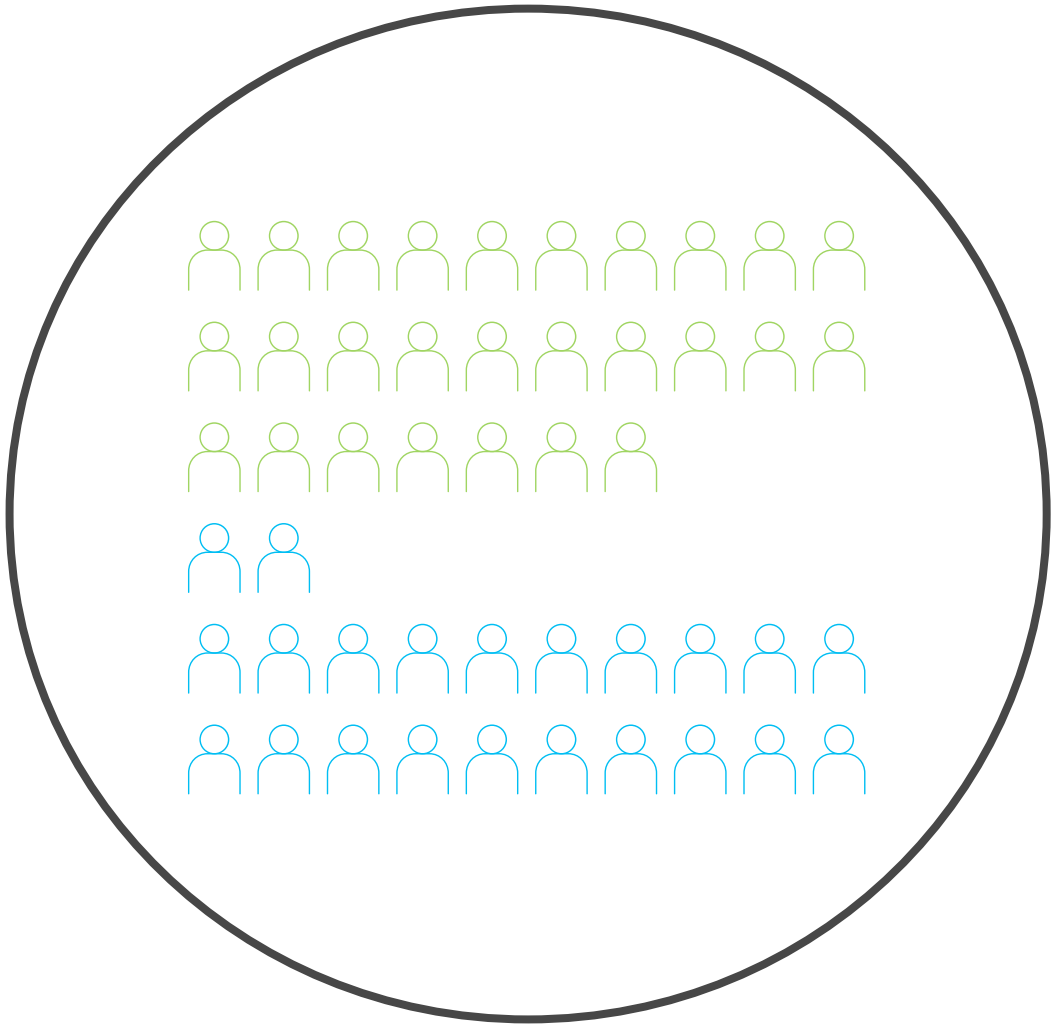
https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000316

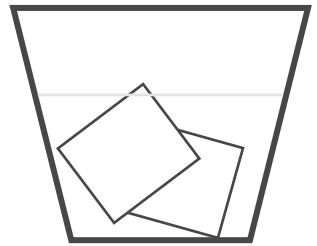


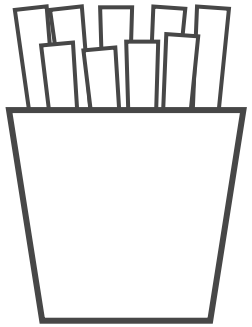
5 more

Community people live.

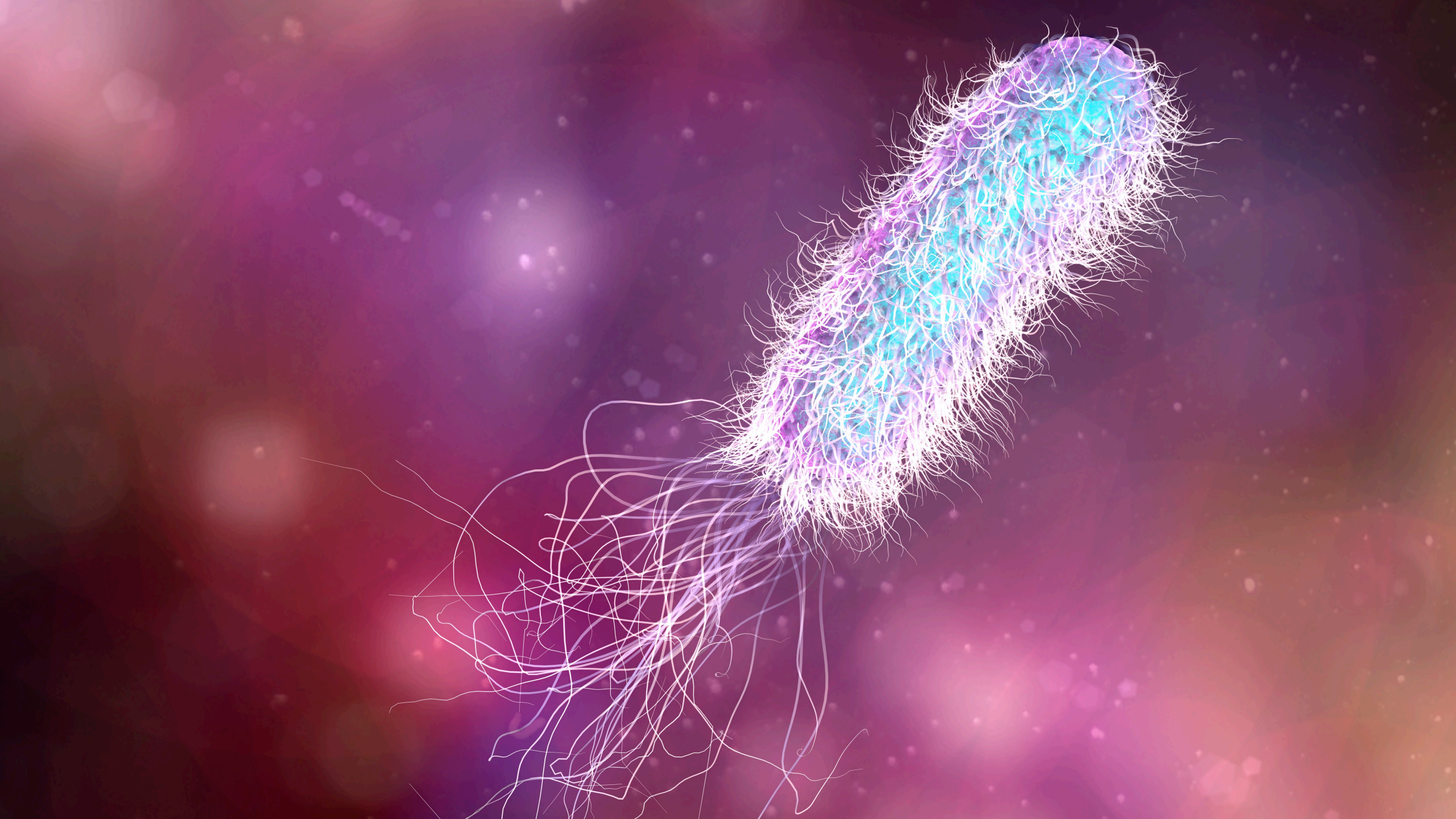
https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000316







https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000316



Good news: IT is (mostly) not life or death

1

2

3

4

5

(Whatever the logos might suggest)

[1]By Leena Snidate / Codenomicon - http://heartbleed.com/heartbleed.svg, CC0, https://commons.wikimedia.org/w/index.php?curid=32089280
[2]By Lepidum Co. Ltd. - http://ccsinjection.lepidum.co.jp/, CC0, https://commons.wikimedia.org/w/index.php?curid=51826364
[3]By Qihoo 360 Co. Ltd. - http://security.360.cn/cve/CVE-2016-6304/, CC0, https://commons.wikimedia.org/w/index.php?curid=52346391
[4]By CrowdStrike Inc. - https://web.archive.org/web/20150513104122/http://venom.crowdstrike.com/, CC BY-SA 4.0,
[5]By Natascha Eibl - https://meltdownattack.com/, CC0, https://commons.wikimedia.org/w/index.php?curid=65235937

A long time ago

Security

'Devastating' Apache bug leaves servers exposed

Devs race to fix weakness disclosed in 2007

By Dan Goodin 24 Aug 2011 at 18:05 42 SHARE ▼

Maintainers of the Apache webserver are racing to patch a severe weakness that allows an attacker to use a single PC to completely crash a system and was first diagnosed 54 months ago.

Attack code dubbed “Apache Killer” that exploits the vulnerability in the way Apache handles HTTP-based range requests was published Friday on the Full-disclosure mailing list. By sending servers running versions 1.3 and 2 of Apache multiple GET requests containing overlapping byte ranges, an attacker can consume all memory on a target system.

madi 56757 asked a question.
August 25, 2011 at 5:09 AM

Apache Killer

hello all,

I need help for following rule

We need an irule to avoid an exploit on Apache

Apache syntax

RewriteEngine On

RewriteCond %{REQUEST_METHOD} ^(HEAD|GET) [NC]

RewriteCond %{HTTP:Range} ([0-9]*-[0-9]*)(\s*,\s*[0-9]*-[0-9]*)+

RewriteRule .* - [F]

dlg 23340
8 years ago

```
when HTTP_REQUEST {
  if { [HTTP::header exists "Range"] and ([HTTP::header "Range"] matches_regex {(,.*?){40,}}) } {
    log local0. " Range attack CVE-2011-3192 detected from [IP::client_addr].  [llength [split [HTTP::header "Range"], ","]] ranges requested."
```

Show More
Upvote · Reply

madi 56757
8 years ago

it seem to work

thank you very much for your help

Show More
Upvote · Reply

naladar 65658
8 years ago

Cool iRule dlg! :)
Upvote · Reply

dlg 23340
8 years ago

After another announcement from the apache folks and little help from smp offline, we have this:

```
when HTTP_REQUEST {
  HTTP::header remove Request-Range
```

Show More
Upvote · Reply

zero 39359
8 years ago

May I know is there any difference for"(,.*?){40,}" on irule and "(,.*?){5,}" on CVE-2011-3192, it seem the counter is difference, your irule is count for 40 and the CVE-2011-3192 is count for 5 range, thanks!
Upvote · Reply

dlg 23340
8 years ago

zero, the 5 from the CVE seemed too restrictive, given the legitimate uses of the Range header. It ends up we could withstand quite a few simultaneous attacks at 40, so it seemed like a good balance between blocking bad traffic and allowing good traffic.

Meanwhile…..

Solutions Now Available for Apache Killer

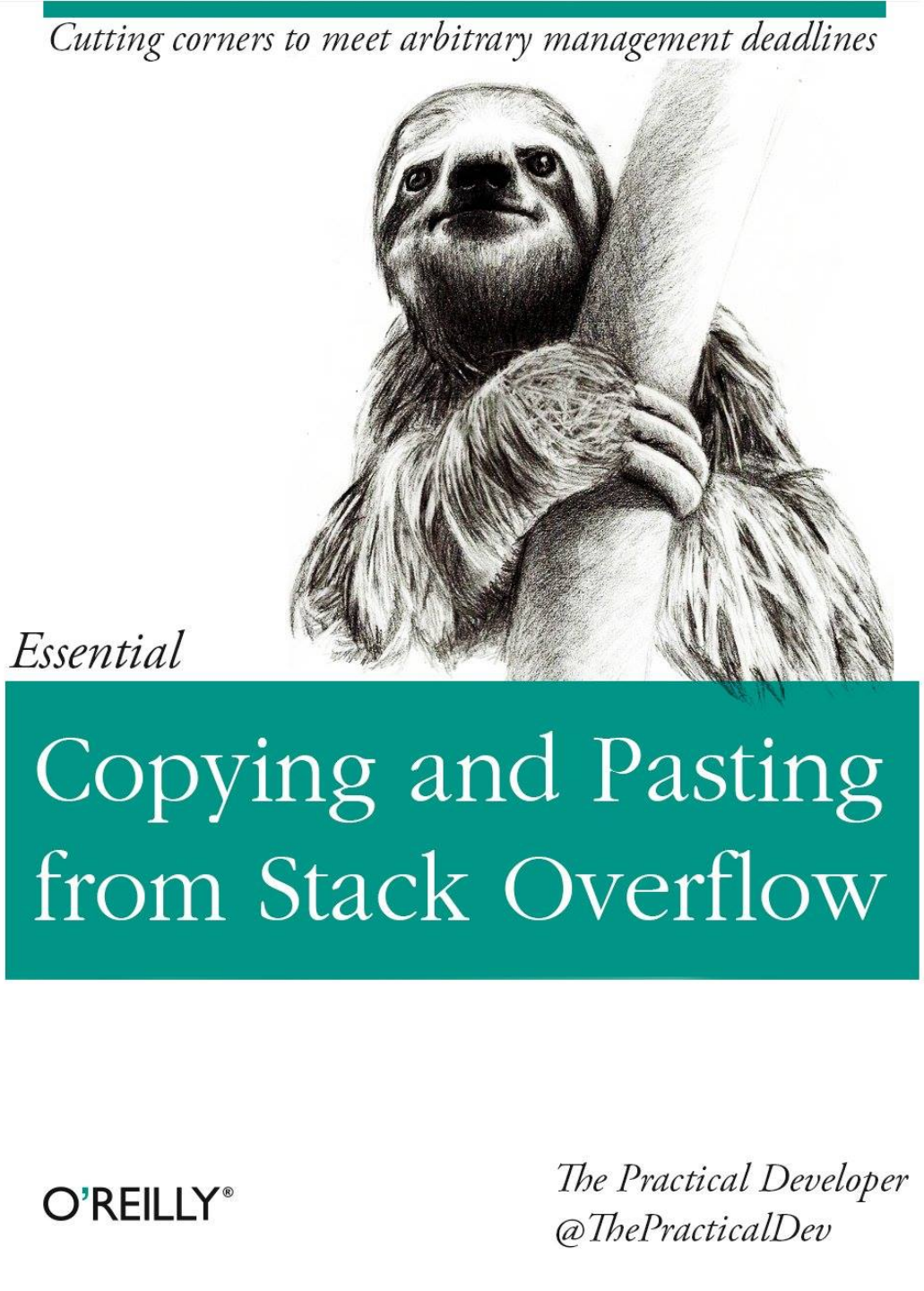
Posted on: September 7, 2011 at 3:54 am **Posted in:** Vulnerabilities
Author: Kim Chanwoo (Security Specialist)

If you are a frequent reader of this blog, you are more or less already familiar with denial-of-service (DoS) attacks. Such an attack typically targets specific systems or servers and "floods" it with information in order to prevent legitimate users from accessing information or services.

This time around, we observed a DoS attack exploiting a specific vulnerability. This is different from the usual known DoS attack methods. DoS attacks are typically done by flooding the target site with traffic (SYN flooding, UDP flooding, ICMP flooding). What makes this attack noteworthy, however, is that it does not require the use of a huge amount of traffic. All the attacker has to do is to send the especially crafted HTTP request, which will render the site inaccessible.

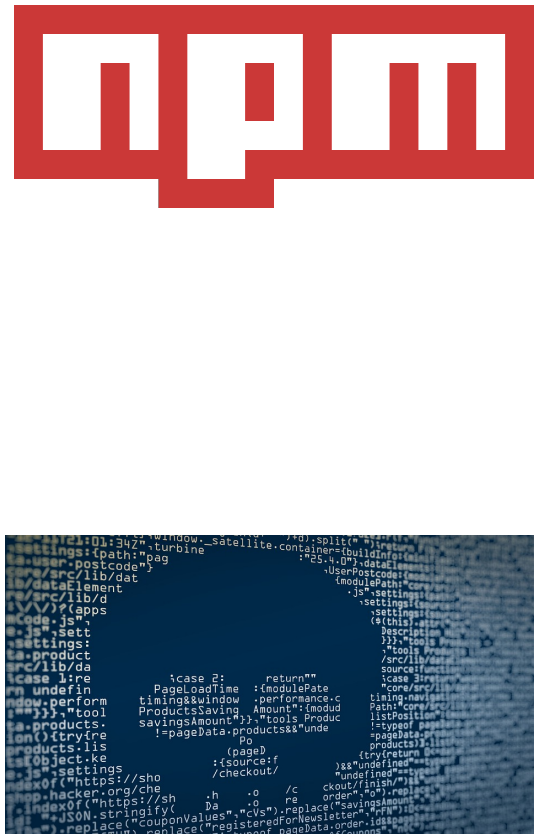
We recently did a deeper analysis of the said vulnerability *(CVE-2011-3192)* found in certain versions of *Apache HTTP Server* that allows a remote attacker to conduct a DoS attack by sending a small HTTP request.

The vulnerability exists in the *byterange* filter in *Apache HTTP Server 1.3.x, 2.0.x* through *2.0.64* and *2.2.x* through *2.2.19*. It can be exploited by a range header that expresses multiple overlapping ranges. The proof of concept for the exploit that abuses this vulnerability was published in August. A tool that conducts DoS attacks by exploiting this vulnerability was later created and dubbed as the "Apache Killer." Apache already patched this security hole last week.

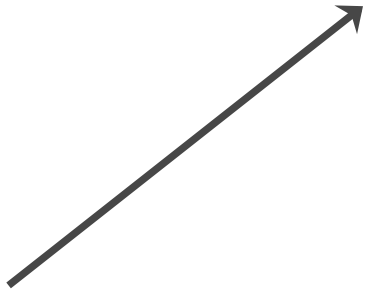


Who, me?

Source: @thePracticalDev (I think)



`event-stream`



2 Million
Downloads

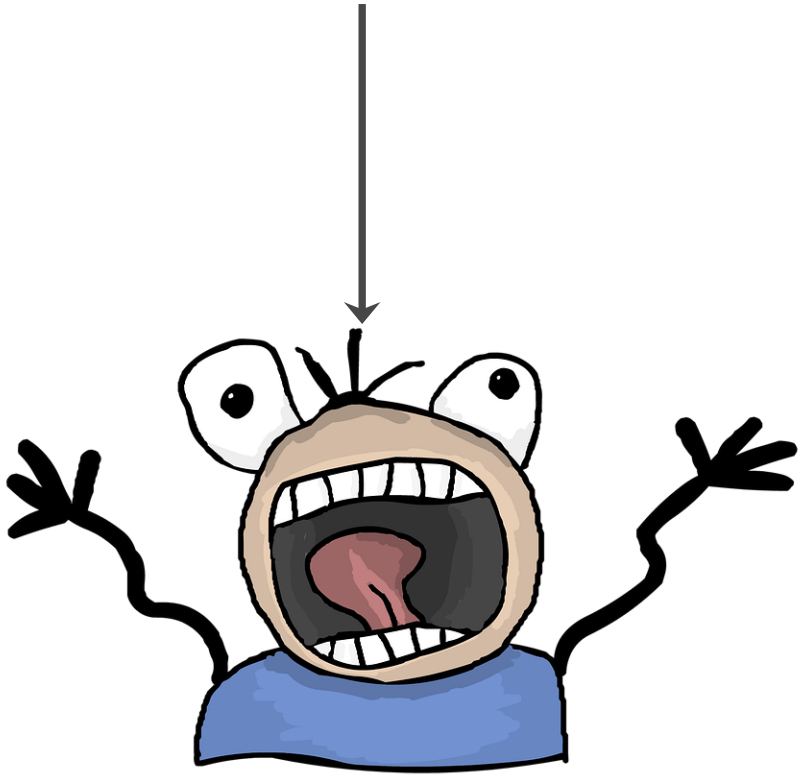


Image by Dmitry Abramov from Pixabay

"*You can buy every 'DevOps' tool in the market and end up further away from your DevOps goals than you are now.*"[1]

Without an empowered community who work together to deliver – you will fail[2]

[1] Somebody I read on the internet somewhere

[2] Me

The F5 and NGINX Community

dev/central

AN F5 COMMUNITY

NGINX

Forum

Our Commitment to Communities

300K Users

400M websites

>$500k donations