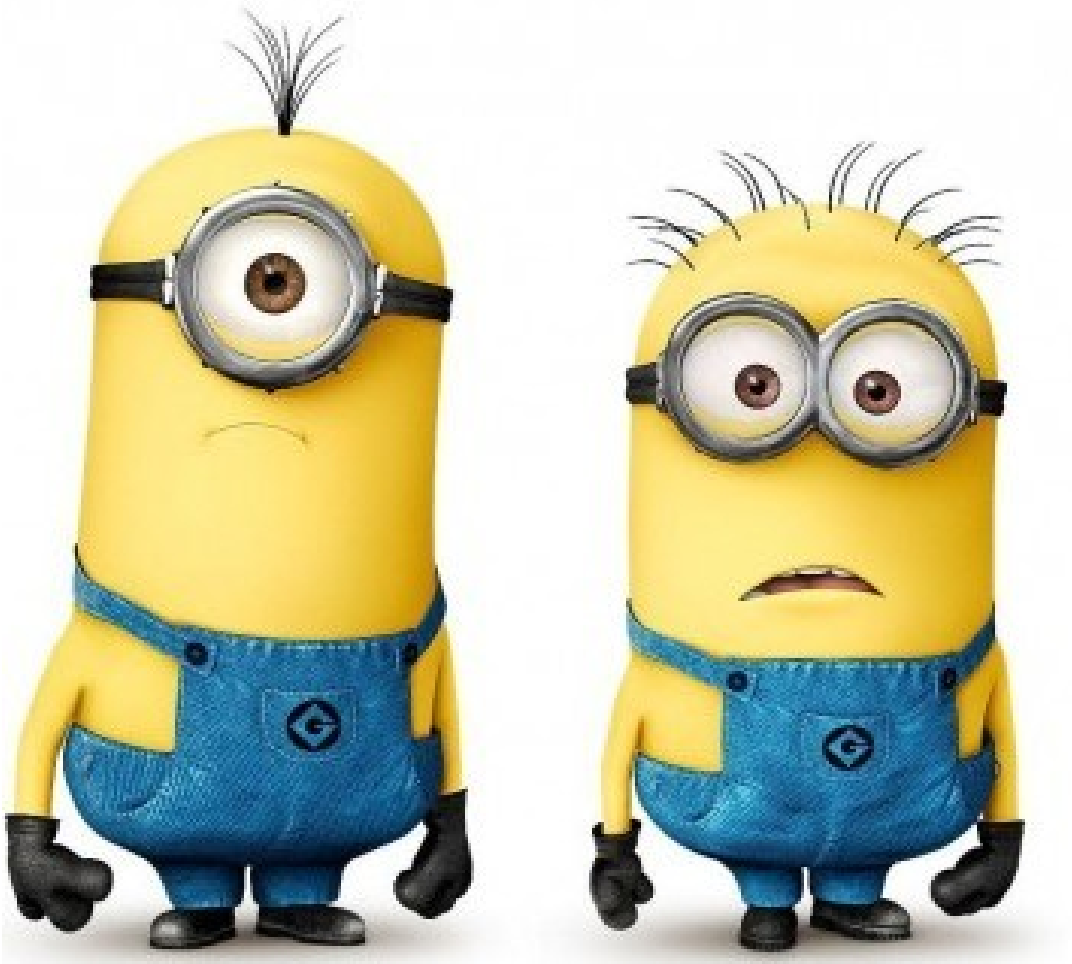
How we broke Let's Encrypt

Marian Marinov
mm@siteground.com
Chief System Architect
Head of the DevOps department

❖ Who am I?

- Chief System Architect of SiteGround.com
- Sysadmin since 1996
- Organizer of OpenFest, BG Perl Workshops, LUG-BG and others
- Teaching Network Security and Linux System Administration courses in Sofia University and SoftUni

SiteGround



Google

Sep 8, 2016 in the end of Jan.2017 it will mark sites with CC data or passwords without HTTPS as "Not secure"

Jan 31, 2017 it happened

Apr 27, 2017 http sites which have forms will be added to "Not secure" in October

Feb 8, 2018 it will mark all HTTP sites that don't have HTTPS as "Not secure"

Let's Encrypt

- Announced in the beginning of 2016
- Lunched on April 12, 2016
- SiteGround is one of the first sponsors of Let's Encrypt
- Wildcard certificates were introduced in March 2018

SiteGround

- In the beginning 2016 we started working on cPanel plugin for Let's Encrypt

- In Oct 2017 we started work on wildcard certs

SiteGround

- In the beginning of **Dec 2017** we decided to issue certs to every host that is hosted on our infrastructure...

SiteGround

Let the failures

begin!!!

SiteGround

❖ We first decided to create account for every client that we have, so everyone can take their own Let's Encrypt account with them if they are leaving...

Creating that many accounts:

- it was slow... so we decided to do it in parallel
  - about 10 requests per server
  - but all servers in the same time

- We broke the infrastructure of Let's Encrypt

SiteGround

- We got a call from Let's Encrypt :)

SiteGround

- They had one **SIMPLE** request:

Implement a global limit(across all of our Data Centers) to create max 2 accounts per second

- Implementing such lock, with performance and reliability in mind is not simple...
- We decided to use HashiCorp's Consul locking for that

- We have a lot of customers... such a limit was never going to be enough...
- So we decided to go with a single account for all servers (proposed by Let's Encrypt)

- At that point everything started to work...
- But we issued certs only to people that wanted SSL, not everyone

- Using certbot it took around 1min to issue a single certificate

- Using certbot it took around 1min to issue a single certificate
- But we had millions of hosts...

- Using certbot it took around 1min to issue a single certificate
- But we had millions of hosts...
- 1,000,000 min ~ 16,667h ~ 694 days

- Using certbot it took around 1min to issue a single certificate
- But we had millions of hosts...
- 1,000,000 min ~ 16,667h ~ 694 days
- No problem :) We have thousands of machines...

- Using certbot it took around 1min to issue a single certificate
- But we had millions of hosts...
- 1,000,000 min ~ 16,667h ~ 694 days
- No problem :) We have thousands of machines...
- We will issue them in parallel from all servers :)

SiteGround

- I don't remember why, but we decided to issue all certs between Christmas and New year :)

Can you imagine the DDoS we caused?

SiteGround

- 6 Data Centers on 3 continents

SiteGround

- 6 Data Centers on 3 continents
- Every server trying to issue up to 6 certificates in parallel

SiteGround

- 6 Data Centers on 3 continents
- Every server trying to issue up to 6 certificates in parallel
- Let's Encrypt did not had limits for this...

- Needless to say... we had a call from Let's Encrypt :)

- They had one **SIMPLE** request:

Implement a global limit(across all of our Data Centers) to issue less then 10 certificates at the same time

- While we were again implementing Consul lock for this...
- Let's Encrypt implemented specific limits, because of us :)
- for a week there were intermittent issues with Let's Encrypt, but it was between Christmas and New year... so both we and Let's Encrypt didn't had the people to address the issue

In March renewing became a problem :)

- we hit different limits

- number of issues of a cert with the same hosts

- number of errors per-server

- number of new certs

❖ unintentionally one of my DevOps guys switched from single account to one account per server

- now, we had a new challenge, when moving an account, we also had to move its certs, because otherwise it reaches the limit of issues

- the certs were still slow to issue

- we had to do some changes to certbot in order to be able to finalize some interrupted issue of certs

I wrote our own certbot, called acmebot, based on Net::ACME2.

Next 2 months we spent adding the same limits that LE have

While doing that...

The next wave of renewals came...
Again we had issues.

SiteGround

We implemented per LE account limit for every server that had its own account.

We implemented a sliding window limit for all servers that use the big account.

Marian Marinov
mm@siteground.com