Distributing delivery of large Security Challenge payloads

ISGC 2019

Nikhef

Who Am I?

Jouke Roorda

Nikhef

Software Engineer @ Nikhef

Red Team for EGI SSC

SSC

We Want Large Files

Nikhef

Large as in >50MB

Tor Browser

Anything really

Job Submission Systems Can’t Cope

Grid Storage Is Too Much Work

So What Does Work?

We Need Redundancy

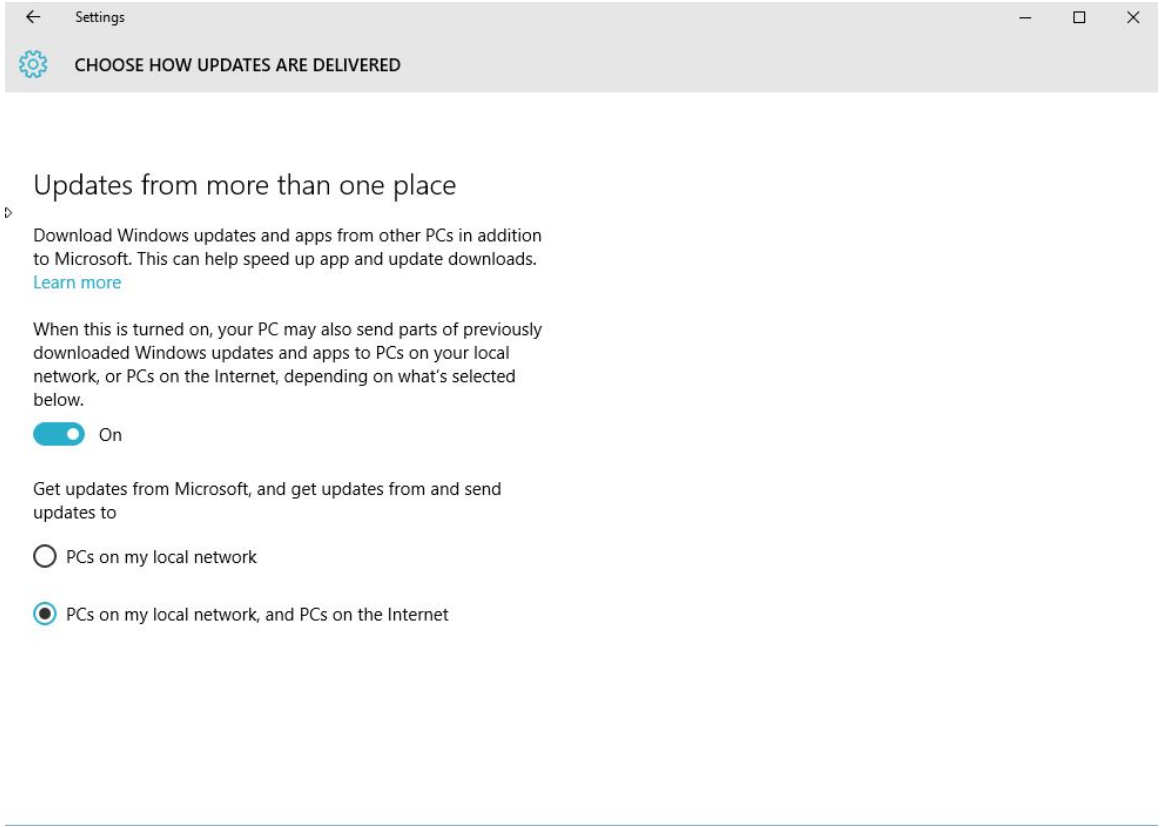
We Need Agility

We Need Ease of Use

BitTorrent

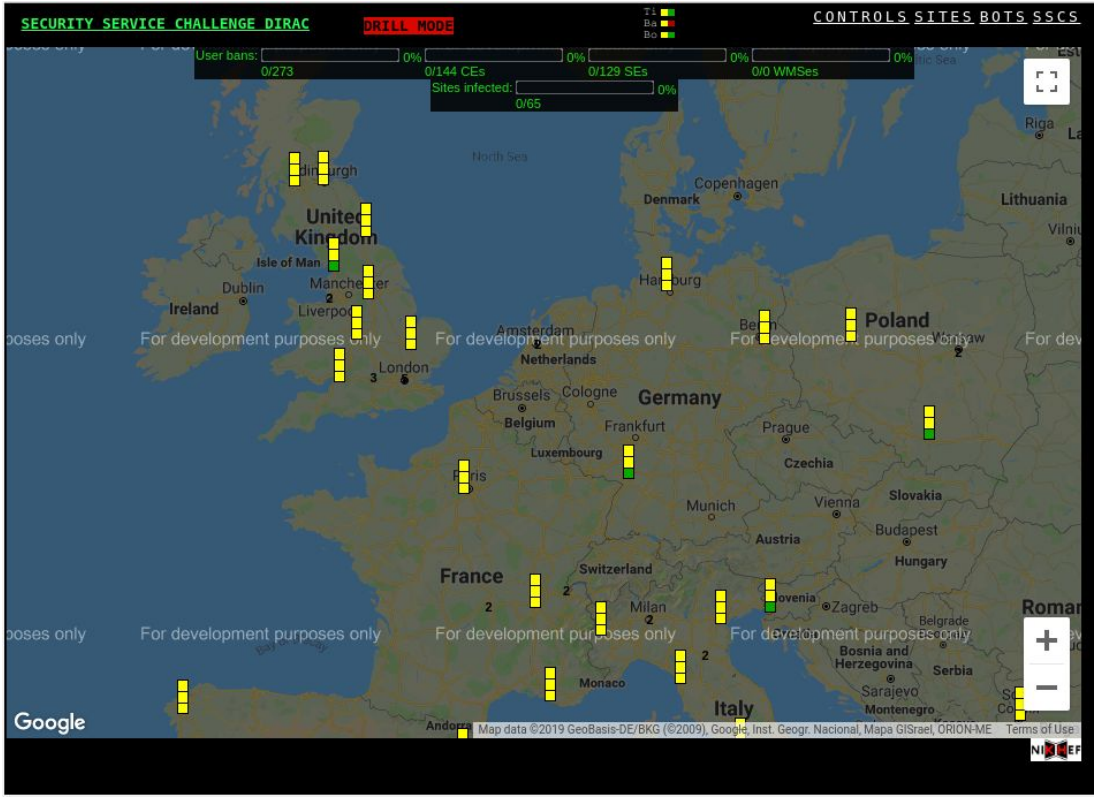
—

Works for pirates



Works for Microsoft

So Does It Work for Us?



Tor

Critical ⟶ Must be downloaded

Web Seeds as redundancy

x86 and x64 client

Nikhef

Seed Box(es)

20GBit+ Transit Connection

No Firewall (except to limit access to the torrent UI)

Transmission

Nikhef

aria2 on Grid Nodes

“aria2 is a lightweight multi-protocol & multi-source command-line download utility.”

Nikhef

Has BitTorrent

Has Web Seeds

Written in C++

No strange dependencies

Sounds good right?

So we set it up

But...

Problem #1

No two sites offer the same environment

Nikhef

Some sites have CentOS 7

Some sites have SLC6

Solution #1

CVMFS

Nikhef

Consistent

Offers a more modern environment

Available on all target sites (LHCb)

Problem #2

aria2 compilation takes 15 minutes on a good day

Nikhef

15 minutes on a 2018 EPYC

30 minutes on my 2017 laptop

Solution #2

Static builds

Nikhef

Available on GitHub

Certificate checking had to be disabled

Torrents check some integrity

Problem #3

aria2 static builds segfault at CERN

Nikhef

This we found out during the SSC launch

Solution #3

None

Nikhef

We do not know why this happened

Fallbacks implemented, using wget

We could have sent a signal

Everything worked, bots came online

Some statistics

223

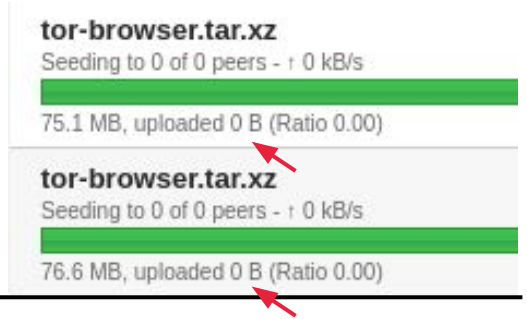
Number of unique aria2 IPs our tracker saw

1031

The number of tracker hits by aria2 clients

0

The number of bits our seedbox uploaded



Why?

Web Seeds

~35 vs 1

Nikhef

Theory: Web Seeds pushed out the actual torrent traffic

P2P is more complicated than just a request

So is this useful?

For widely available files: No...

And for specific files?

Not really, in my opinion*

Fundamental issues

Unsuitable Networks

Not vulnerable enough

Nikhef

No UPnP

No NAT-PMP

(But yes firewalls)

No seeding, or you'll get caught

Politically Problematic

Hosting ‘Hacking Pirates’ is apparently not very popular

Too much work

Tracker (or DHT)

Seed Box(es)

Generating Torrents

Nikhef

Software

Nikhef

Less portable than expected

Mainly aimed at desktops

Mainly aimed at home environments

aria2 is nice, *once it works*...

In Short:
Save yourself some time, use a cheap web CDN

SSC: Detection and Artifacts

In chronological order

Nikhef

DIRAC kills idle jobs

CPU/time is monitored

Setting up tor is not intense enough

Our bots wait for instructions

Nikhef

DIRAC kills idle jobs

Should we burn CPU for nothing?

Nikhef

Luckily...

Undocumented feature

```
self.log.verbose('Initializing Watchdog instance')
watchdog.initialize()
self.log.verbose('Calibrating Watchdog instance')
watchdog.calibrate()
# do not kill Test jobs by CPU time
if self.jobArgs.get('JobType', '') == 'Test':
  watchdog.testCPUConsumed = False

if 'DisableCPUCheck' in self.jobArgs:
  watchdog.testCPUConsumed = False

if exeThread.isAlive():
  self.log.info('Application thread is started in Job Wrapper')
  watchdog.run()
else:
  self.log.warn('Application thread stopped very quickly...')

if exeThread.isAlive():
  self.log.warn('Watchdog exited before completion of execution thread')
  while exeThread.isAlive():
    time.sleep(5)
```

Nikhef

Major Indicators

Detecting Strange Jobs

DIRAC / Site perspective

Nikhef

Jobs with check-evading flags

Jobs are idle for days

Detecting Torrents

Should you?

Nikhef

Mainly web traffic

Bencode tracker communication

Torrent files on the system

Detecting Unusual CPU Load

yes > /dev/null &

Nikhef

‘yes’ is highly optimized

No throughput

Miner-like activity

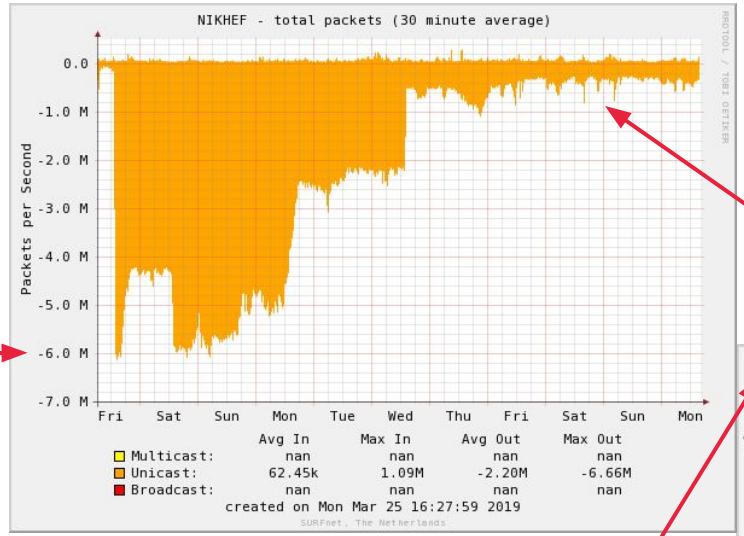
Detecting DDOSes

Nikhef

UDP Packet Flooding

Limited traffic

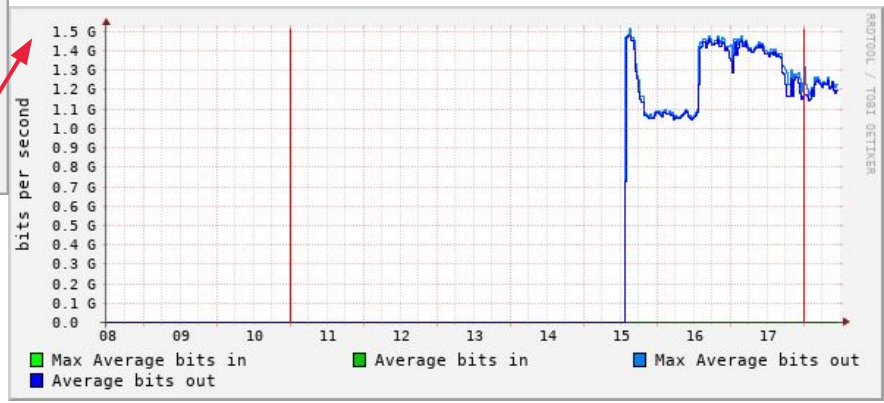
Detecting a (D)DOS attack



6 Mio packs

This is not a baseline

1,5Gb



Nikhef

Detecting a (D)DOS attack

SURFcert started complaining

Nikhef ‘complained’ to EGI

Nikhef

Detecting a (D)DOS attack

No machines were harmed in the process of this attack

Nikhef

Detecting Bot Characteristics

Using methods from the workshop on Sunday

Nikhef

UUIDs in the bot

egissc tor address

Makeself pilot-like initialization

SSC Fun Facts

Total Bots: ~250

Nikhef

Some in short queues ⟶ killed

Some glite, some DIRAC

Some were redeployed

First Ban: <12h

Nikhef

Tor was found

LHCb job on an ATLAS site

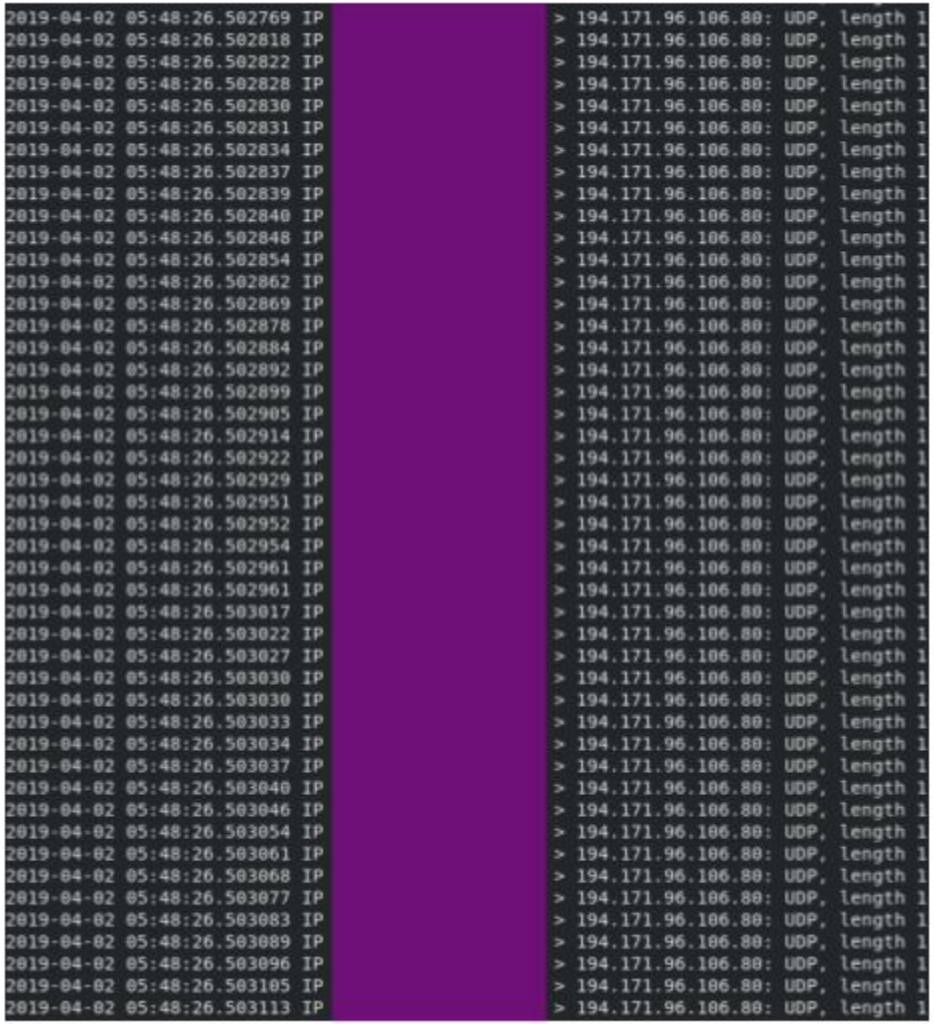
Longest DDOS

Still going on...

Nikhef

More than 3 weeks

Currently around 60 Mb/s


2019-04-02 05:48:26.502769 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502818 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502822 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502828 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502830 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502831 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502834 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502837 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502839 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502840 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502848 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502854 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502862 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502869 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502878 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502884 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502892 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502899 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502905 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502914 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502922 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502929 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502951 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502952 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502954 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502961 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.502961 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503017 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503022 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503027 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503030 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503030 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503033 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503034 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503037 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503040 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503046 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503054 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503061 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503068 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503077 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503083 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503089 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503096 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503105 IP > 194.171.96.106.80: UDP, length 1
2019-04-02 05:48:26.503113 IP > 194.171.96.106.80: UDP, length 1

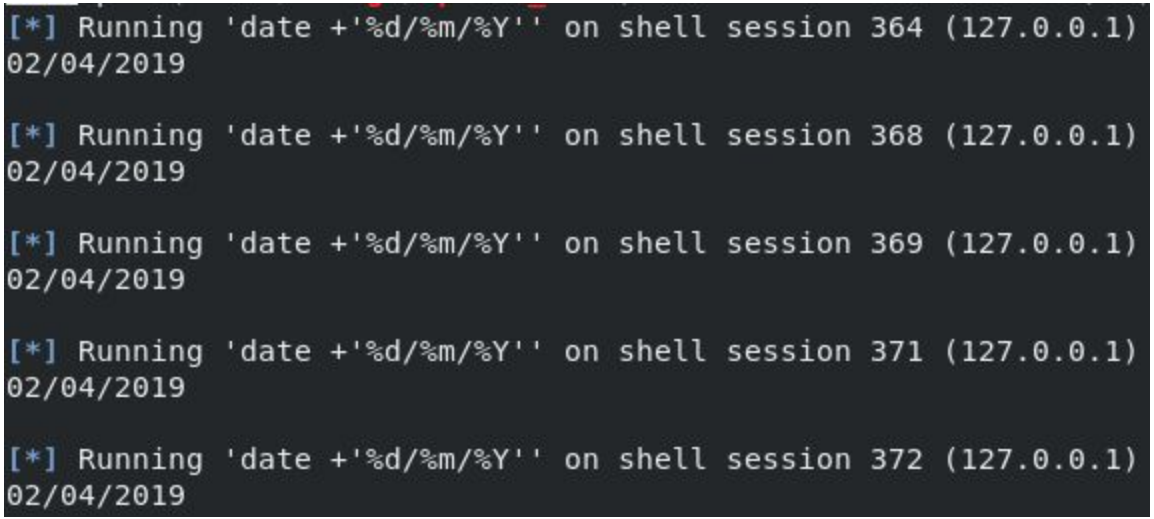
Bots still responding: 5

Excluding the DDOSing bots

Not currently doing anything

Nikhef

—



(127.0.0.1) is a Tor side-effect

Debug sessions: ~4

Nikhef

All gave up

Voluntarily infecting more hosts?

Pilot Users Banned: many

Basically every site banned the LHCb Pilot User, more or less crippling DIRAC

Nikhef

Timing of the SSC: Very Bad

(for LHCb)

Nikhef