War games: Live security DDoS drills

Jan Včelák

28. května 2019, CSNOG, Brno

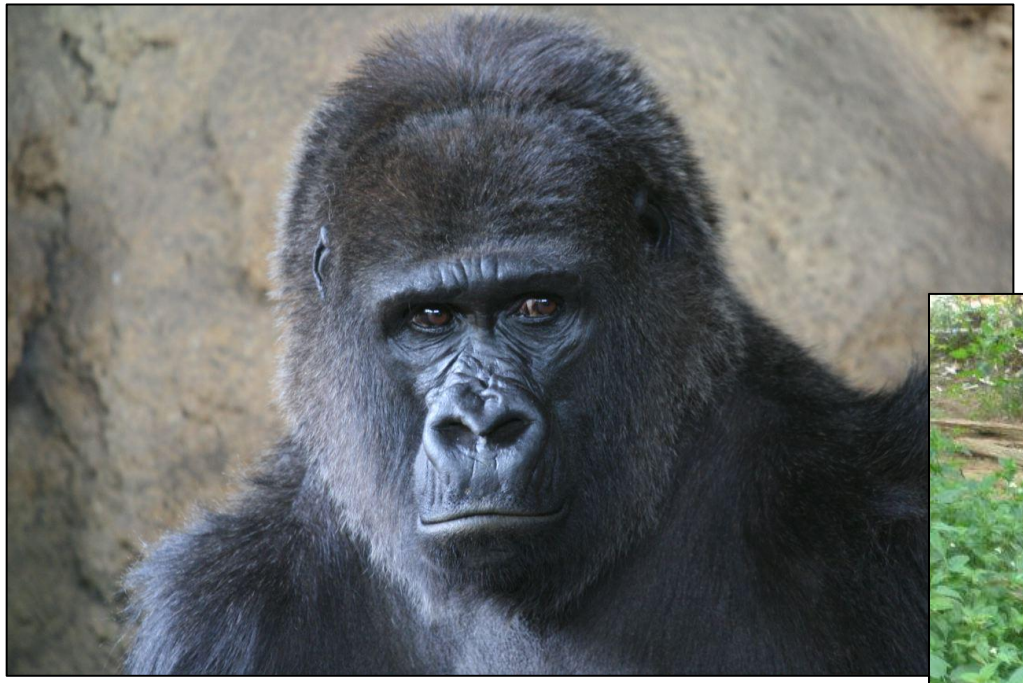
NS1.

ns1.com · @fcelda @ns1 · jvcelak@ns1.com

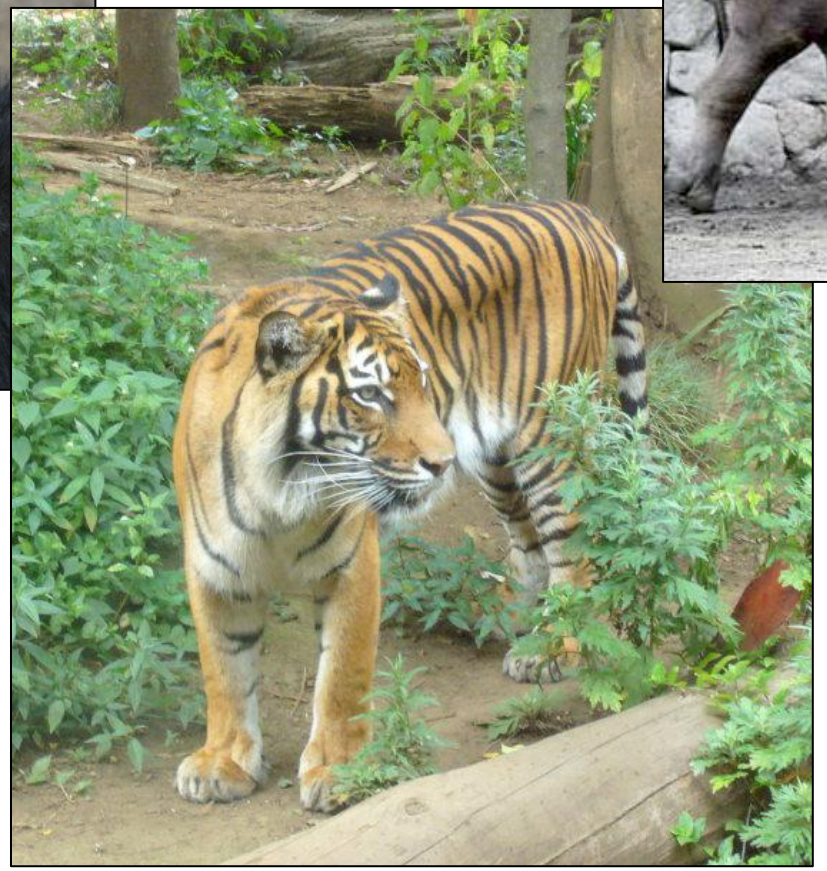
Ueno Zoo
Tokyo, Japan

NS1.

https://www.gojapango.com/places/tokyo/tokyo/zoo/ueno-zoo/



http://www.wikiwand.com/ja/%E6%81%A9%E8%B3%9C%E4%B8%8A%E9%87%8E%E5%8B%95%E7%89%A9%E5%9C%92



http://yourholidayhomes.com/things-to-do/ueno-zoo_495.html

http://latimesblogs.latimes.com/unleashed/2009/06/black-rhinoceros-calf-at-japans-ueno-zoo.html

NS1.

Koichi Kamoshida/Getty Images

NS1.

Koichi Kamoshida/Getty Images

NS1.

Yuriko Nakao/Reuters

NS1.

Reuters

NS1.

Chengdu Zoo
Sichuan, China

Reuters/China Daily

NS1.

Taiyuan *Zoo*
Shanxi, *China*

Reuters/China Daily

NS1.

Hello!

I’m Jan. I work at NS1.

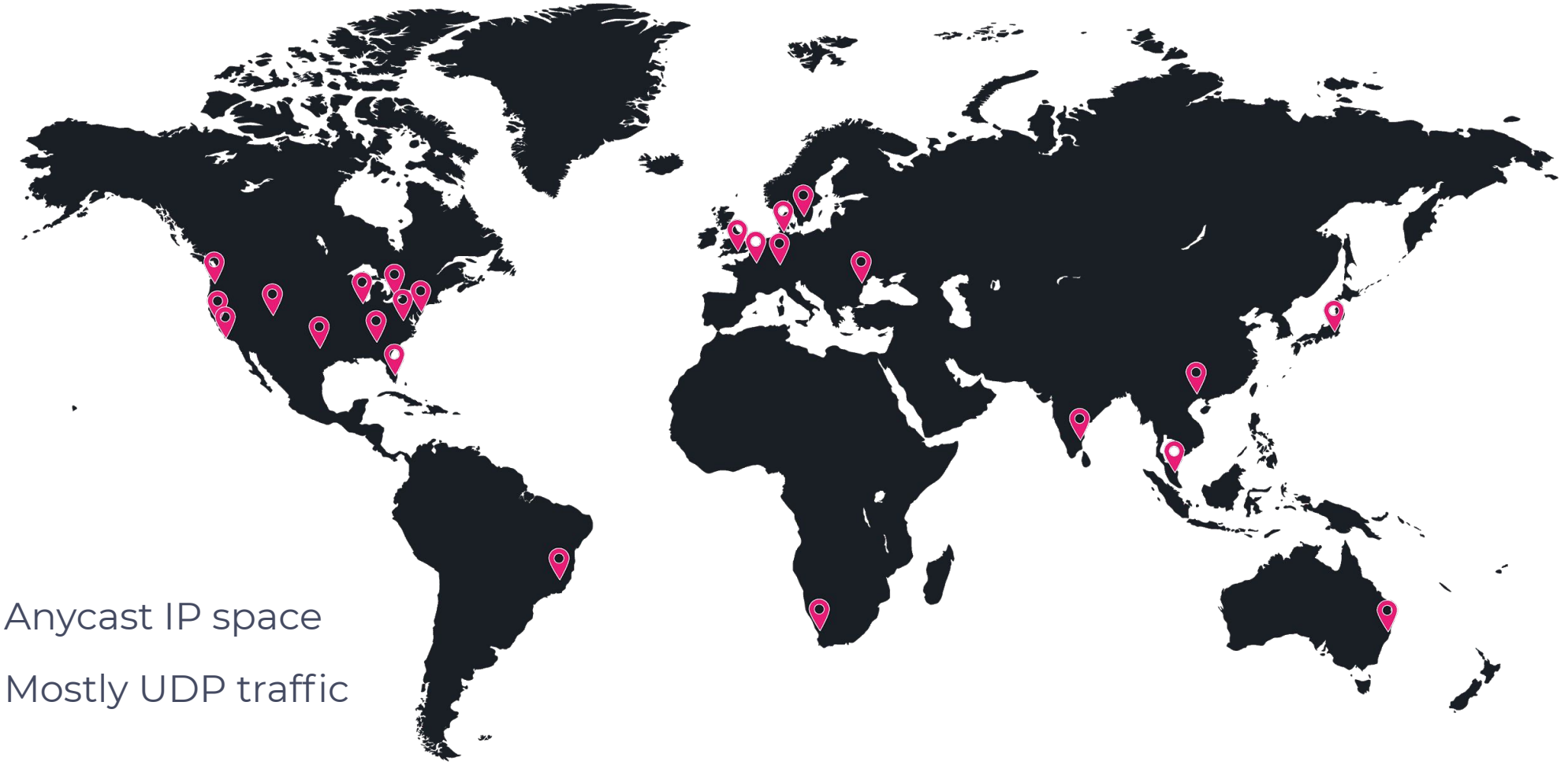
We run a global network of authoritative DNS servers that have to deal with attacks.

We do live security drills to help us prepare for them.

Toshifumi Kitamura/AFP/Getty Images

NS1.

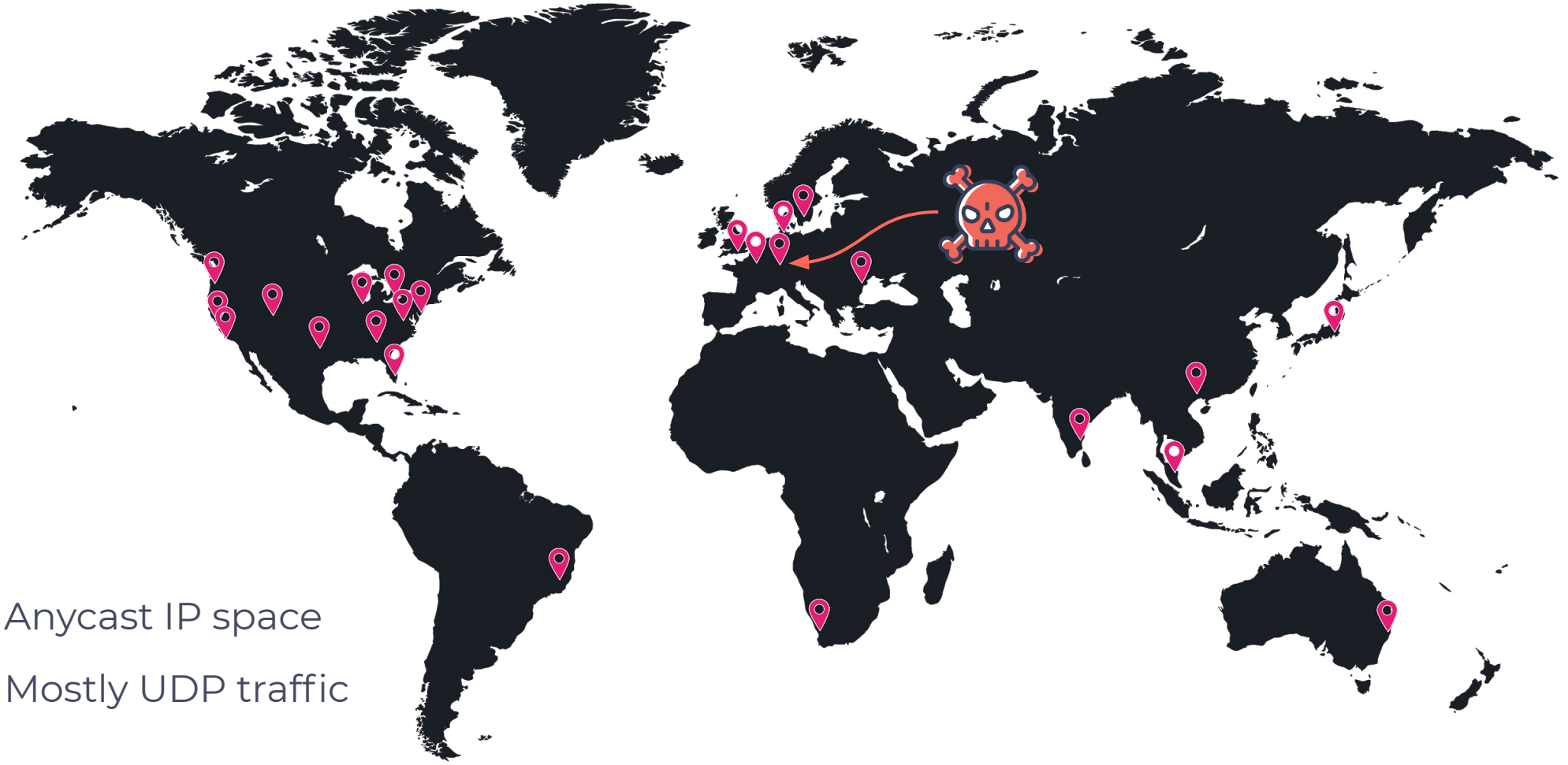
DNS Delivery Network



- Anycast IP space
- Mostly UDP traffic

NS1.

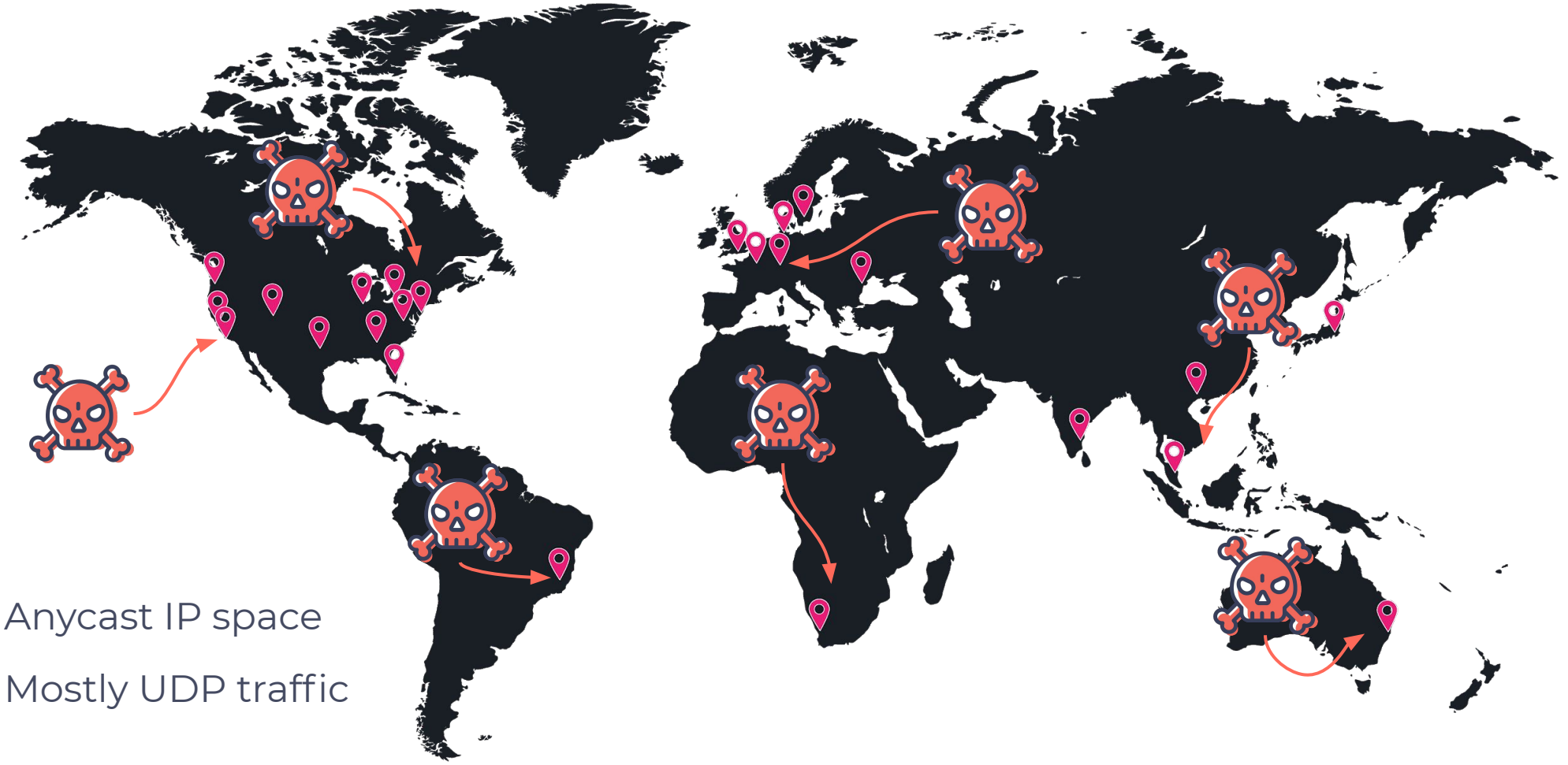
DoS Attacks



- Anycast IP space
- Mostly UDP traffic

NS1.

Distributed DoS Attacks



- Anycast IP space
- Mostly UDP traffic

NS1.

DNS Attacks

- Attacks targeting:
  - Network resources (switches, uplinks, …)
  - Computational resources (CPU, memory)
- Volumetric and flood attacks
- Reflection and amplification (DNS and NTP)
- DNS random label attacks

  (o8dnc638d.foo.com, bu7vyf52x.foo.com, …)
- Very distributed botnets (e.g. Mirai)

https://www.kotaku.com.au/2014/02/when-murderous-rampaging-animals-are-fake-and-look-goofy/

NS1.

Dealing With Attacks

Michael Caronna/Reuters

- **Visibility**
  - Packet inspection
  - Metrics and dashboards
  - Alerting
- **Mitigation** (filtering and limiting)
  - Upstream filtering
  - BPF/netfilter at servers
- **Automation**
  - Traffic flow classification
  - Automatic filtering rules
  - Moving traffic to POPs with more resources

NS1.

WarGames (1983) directed by John Badham

NS1.

Motivation For Drills

- Continually **evolving platform** and **attack methods**
- Tools will break or we **won't remember** how to use them
- Operators need to be **confident** knowing which tools and dashboards to pull up at a moments notice, under stress
- Realistically **stress our system** to understand failure scenarios
- Introduce **new engineers** to mitigation
- Do something **different and fun**

NS1.

What Goes Down

- **Every two weeks**, 1-2 hour session
- On **real production** infrastructure
- Run by technical and network **operations teams**
- Representative from **customer support**
- Communicate in **shared video call** and **Slack channel**
- We **take notes**
- We **recap**, update documentation, create tickets

NS1.

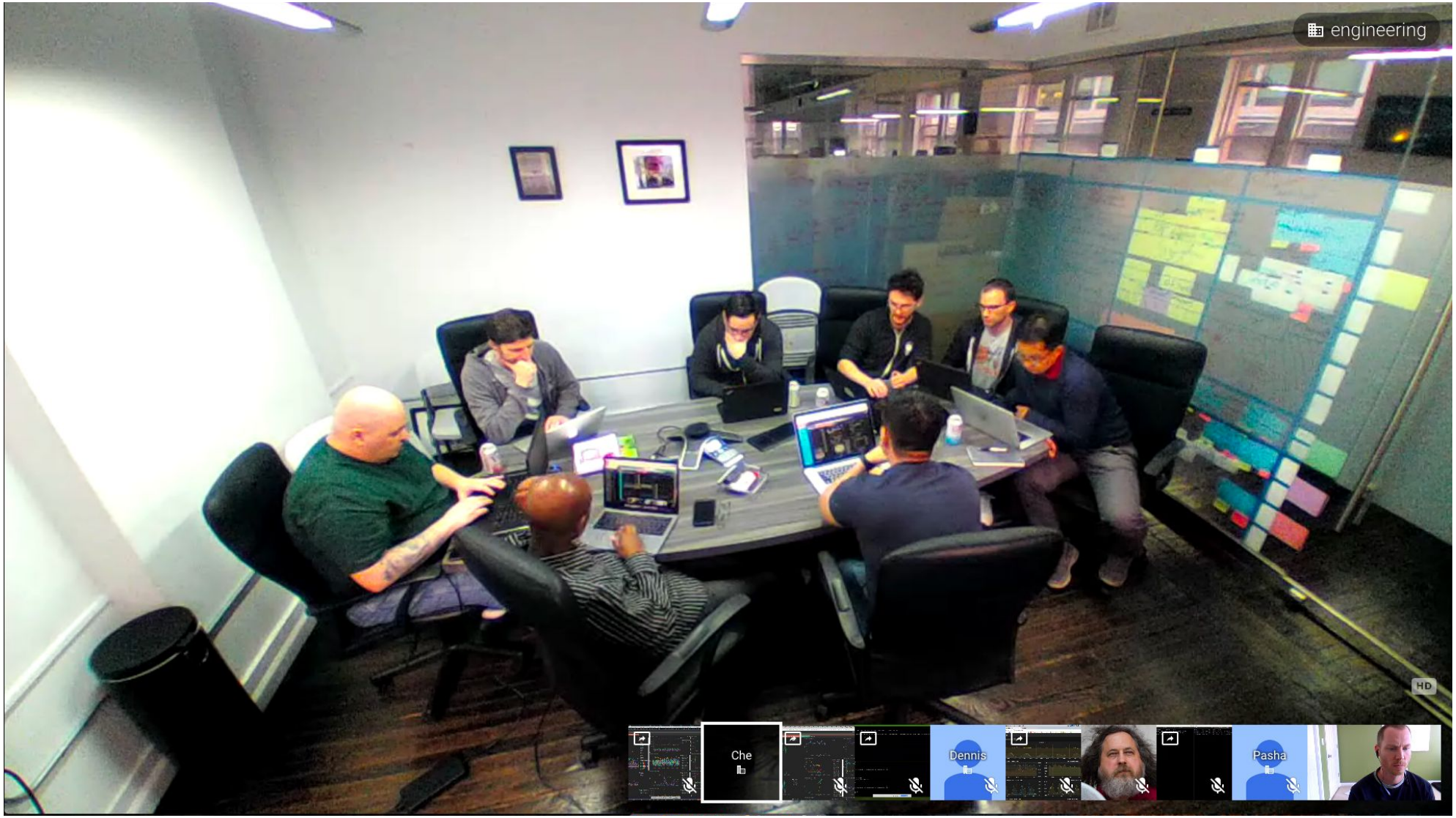
What Goes Down

- **Attacker**
  - Prepares ahead of time
  - Brings up attack infrastructure
  - Tries to throw defenders for a loop
  - Mutates attack over time
- **Defenders**
  - Exercise visibility tools
  - Exercise mitigation tools
  - Exercise critical communication

Kazuhiro Nogi/AFP/Getty Images

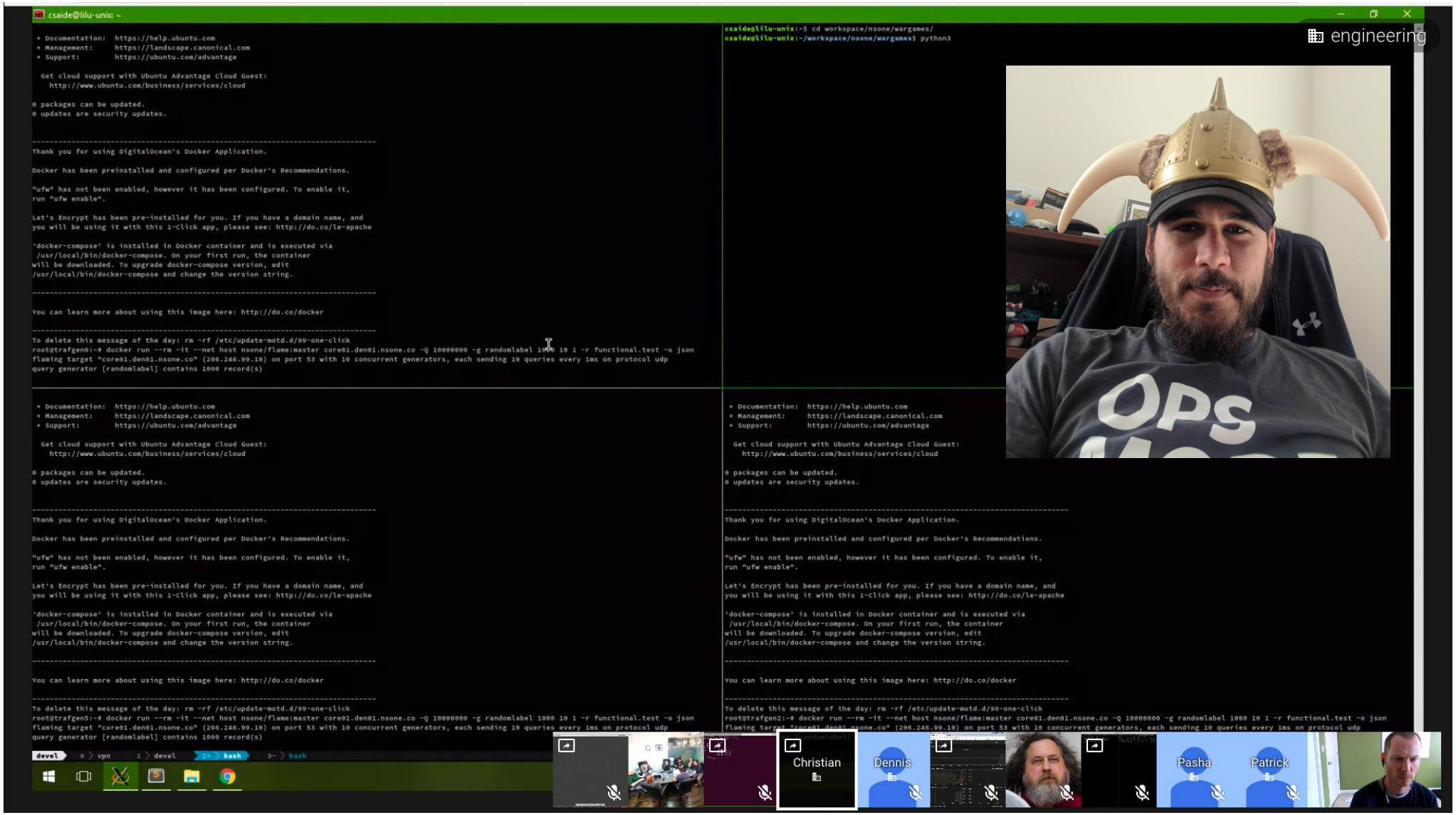
NS1.

War Room



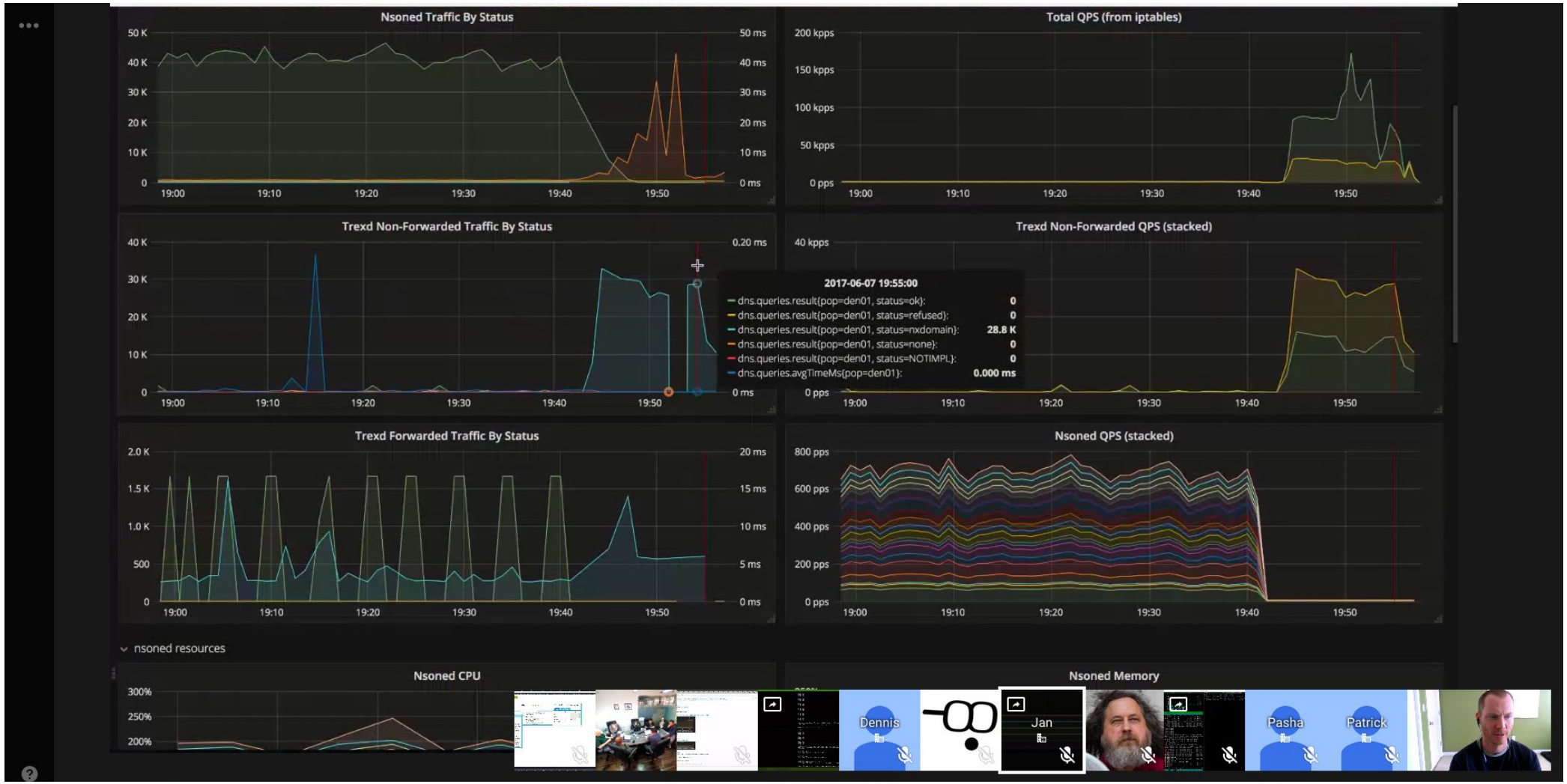
NS1.

Attacker



NS1.

Defenders


Nsoned Traffic By Status
Total QPS (from iptables)
Trexd Non-Forwarded Traffic By Status
2017-06-07 19:55:00
dns.queries.result{pop=den01, status=ok}: 0
dns.queries.result{pop=den01, status=refused}: 0
dns.queries.result{pop=den01, status=nxdomain}: 28.8 K
dns.queries.result{pop=den01, status=none}: 0
dns.queries.result{pop=den01, status=NOTIMPL}: 0
dns.queries.avgTimeMs{pop=den01}: 0.000 ms
Trexd Non-Forwarded QPS (stacked)
Trexd Forwarded Traffic By Status
Nsoned QPS (stacked)
nsoned resources
Nsoned CPU
Nsoned Memory
Dennis
Jan
Pasha
Patrick

Tools We Use

- Visibility
  - pktvisor, Packetbeat, ntopng
  - ELK, Grafana
- Attack Infrastructure
  - Terraform, cloud providers
  - Custom controller scripts
- Traffic generation
  - Flamethrower, dnsperf
  - hping3
  - tcpreplay

China Daily/Reuters

NS1.

Lessons Learned

- **Documentation** was wrong
- Could not **remember** tool syntax
- Mitigation commands **failed to work** properly
- Increased cache size we didn't **understand**
- Found attacks **invisible** to our monitoring
- Forces us to **improve** existing mitigation tools
- Keeps us **creative** and flexible

NS1.

Tips For Success

- Attacks have to be **realistic**, use production servers and data
- Record and **review** the sessions, get follow-up tasks in roadmap
- Put real time into **planning** for game day
- **Consistency** is important, pick a schedule and stick to it
- Keep it **fun**

Future Ideas

- Surprise unplanned attacks
- Introduce artificial constraints (e.g. no Slack or Zoom)

Thank you.

ns1.com

jvcelak@ns1.com

@fcelda @ns1

NS1.