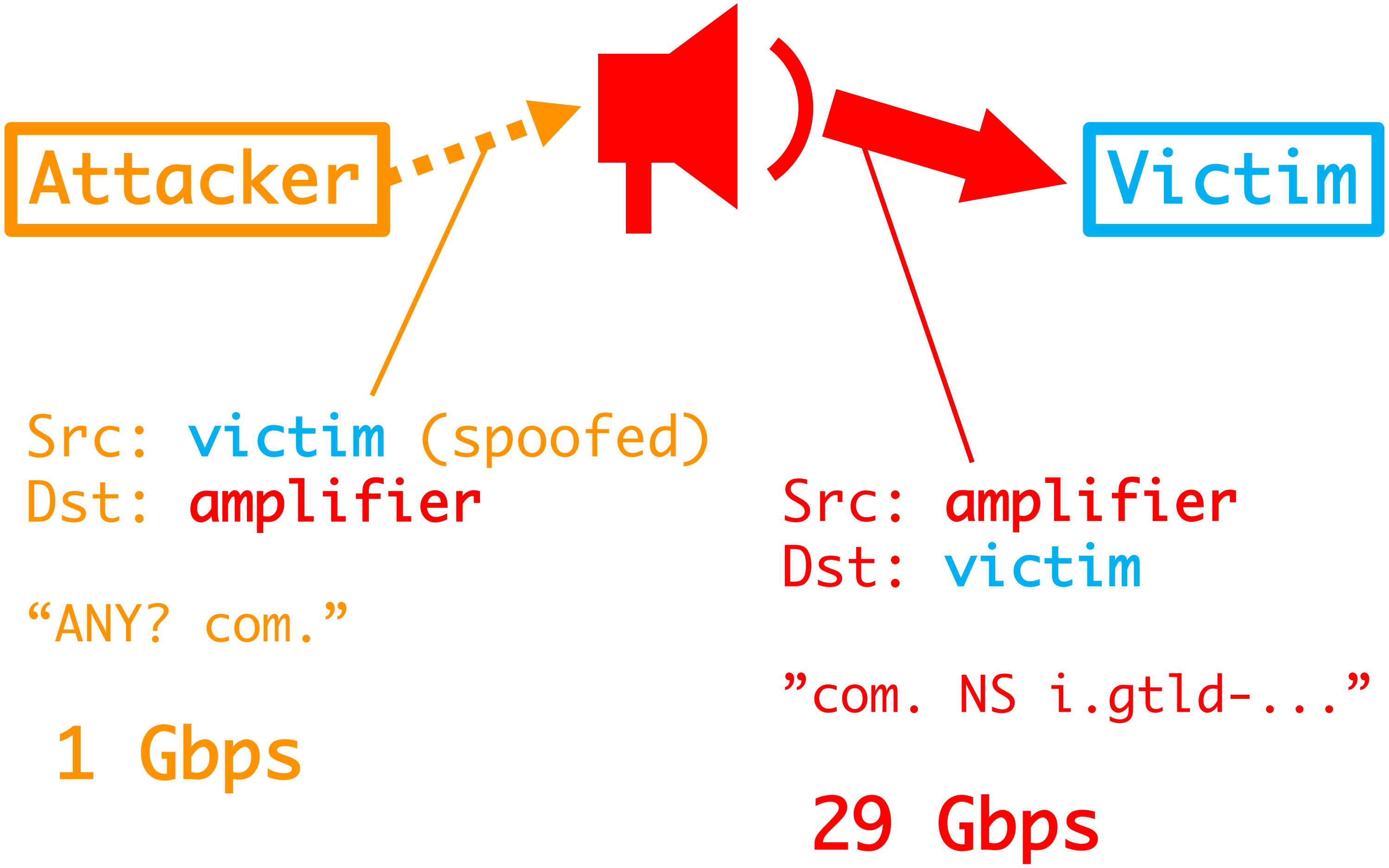
Memcached amplification: lessons learned

Artyom Gavrichenkov <ag@qrator.net>

1.7

Typical amplification attack

- Most servers on the Internet send more data to a client than they receive
- UDP-based servers generally do not verify the source IP address
- This allows for amplification DDoS



Attacker

Victim

Src: victim (spoofed)
Dst: amplifier

“ANY? com.”

1 Gbps

Src: amplifier
Dst: victim

”com. NS i.gtld-...”

29 Gbps

Proof of Source Address Ownership

E.g., QUIC:

- Initial handshake packet padded to 1280 bytes
- Source address validation

Other protocols?

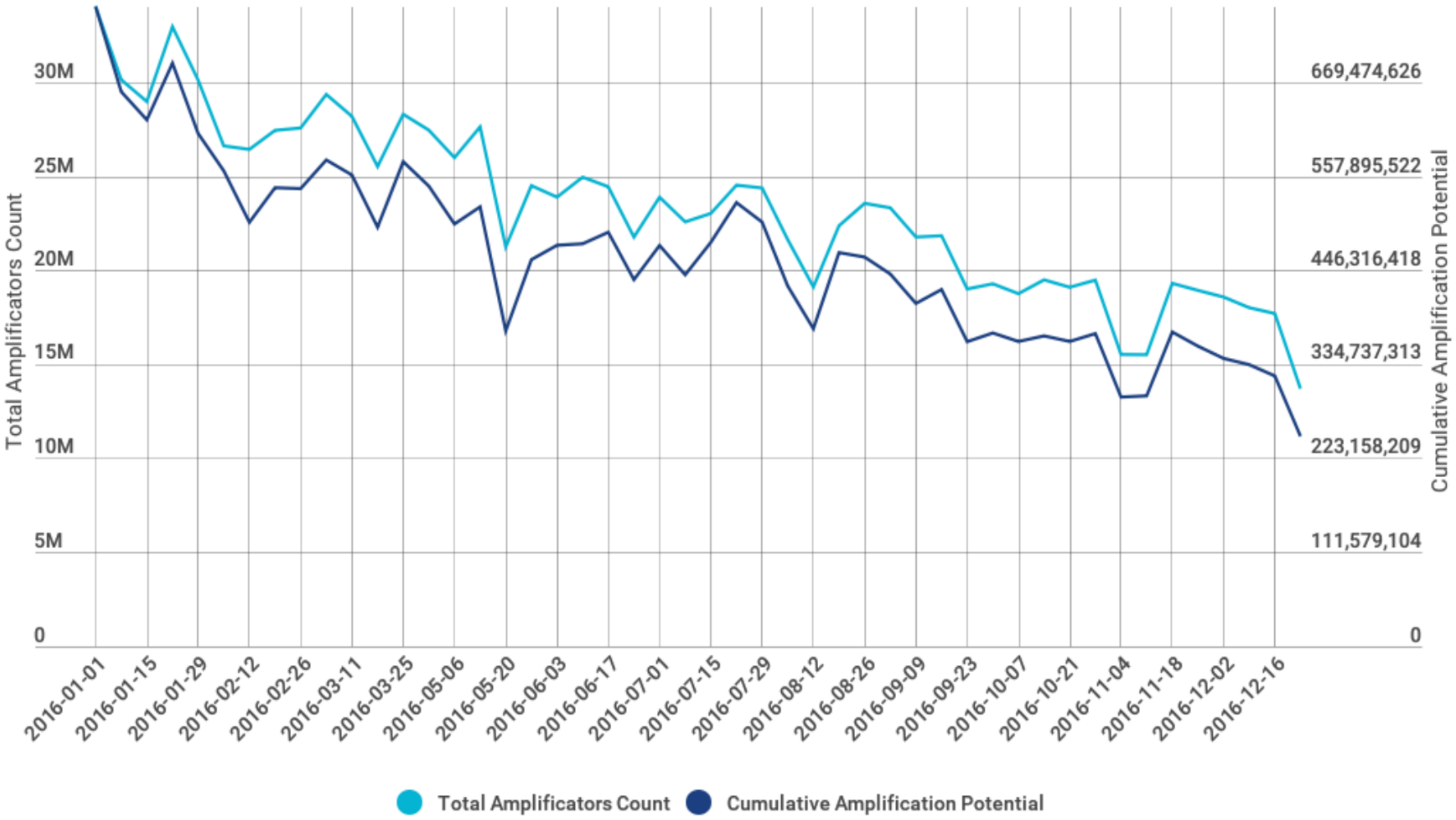
Vulnerable protocols

- A long list actually
- Mostly obsolete protocols (RIPv1 anyone?)
- Modern protocols as well: gaming

- NTP
- DNS
- SNMP
- SSDP
- ICMP
- NetBIOS
- RIPv1
- PORTMAP
- CHARGEN
- QOTD
- **Quake**
- …

Vulnerable servers

- As it's mostly obsolete servers, they eventually get updated
  - or replaced
  - or just trashed
- Thus, the amount of amplifiers shows steady downtrend

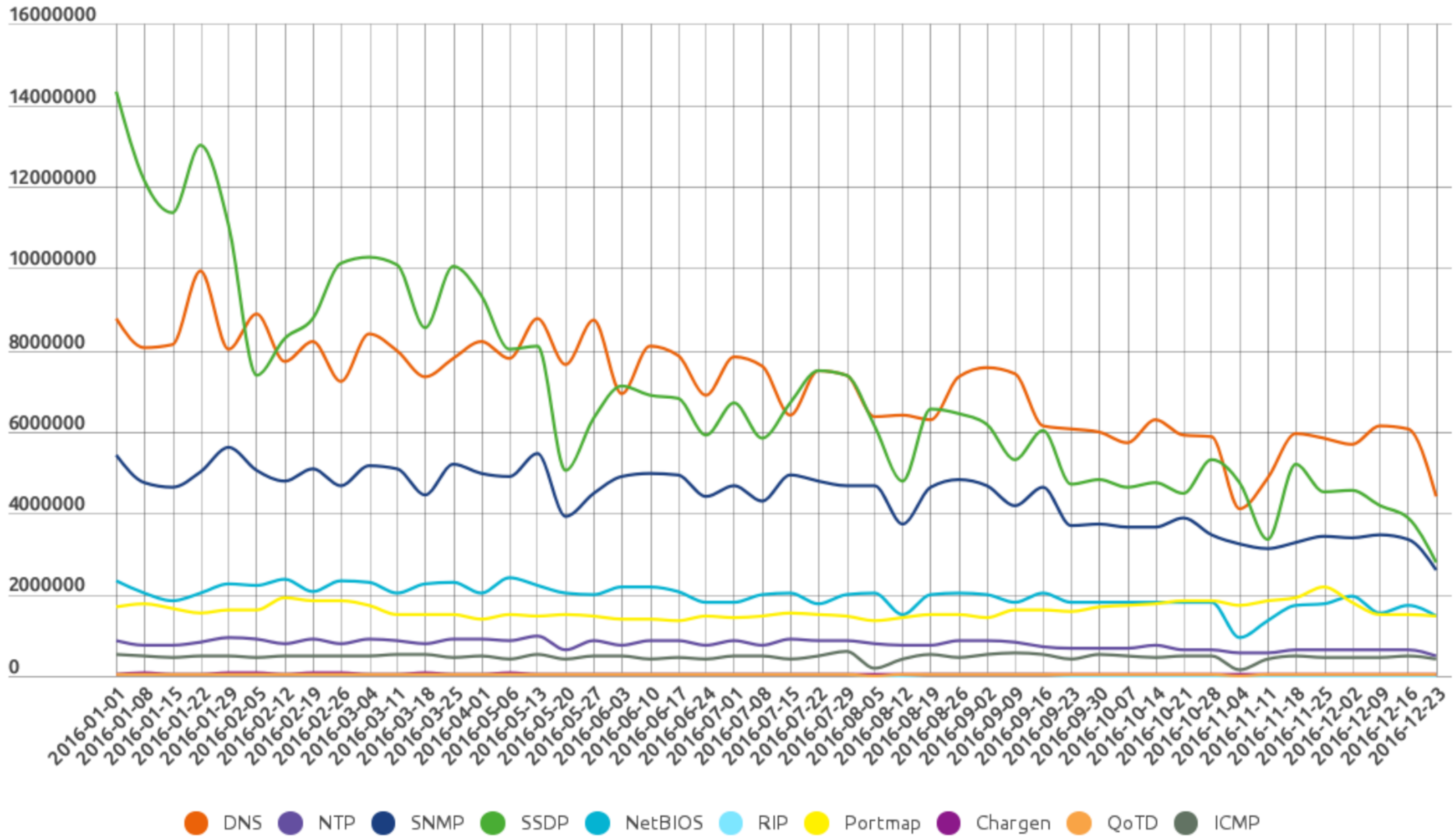


Source: Qrator.Radar network scanner

Amp power

- Downtrend in terms of the amount – and a downtrend in terms of available power

- However, once in a while, a new vulnerable protocol is discovered



Source: Qrator.Radar network scanner

Mitigation

- Most amplification attacks are easy to track, as the source UDP port is fixed

- NTP
- DNS
- SNMP
- SSDP
- ICMP
- NetBIOS
- RIPv1
- PORTMAP
- CHARGEN
- QOTD
- **Quake**
- …

BGP Flow Spec solves problems?

Mitigation

- Most amplification attacks are easy to track, as the source UDP port is fixed
- Two major issues:
  - ICMP
  - **Amplification without a fixed port**

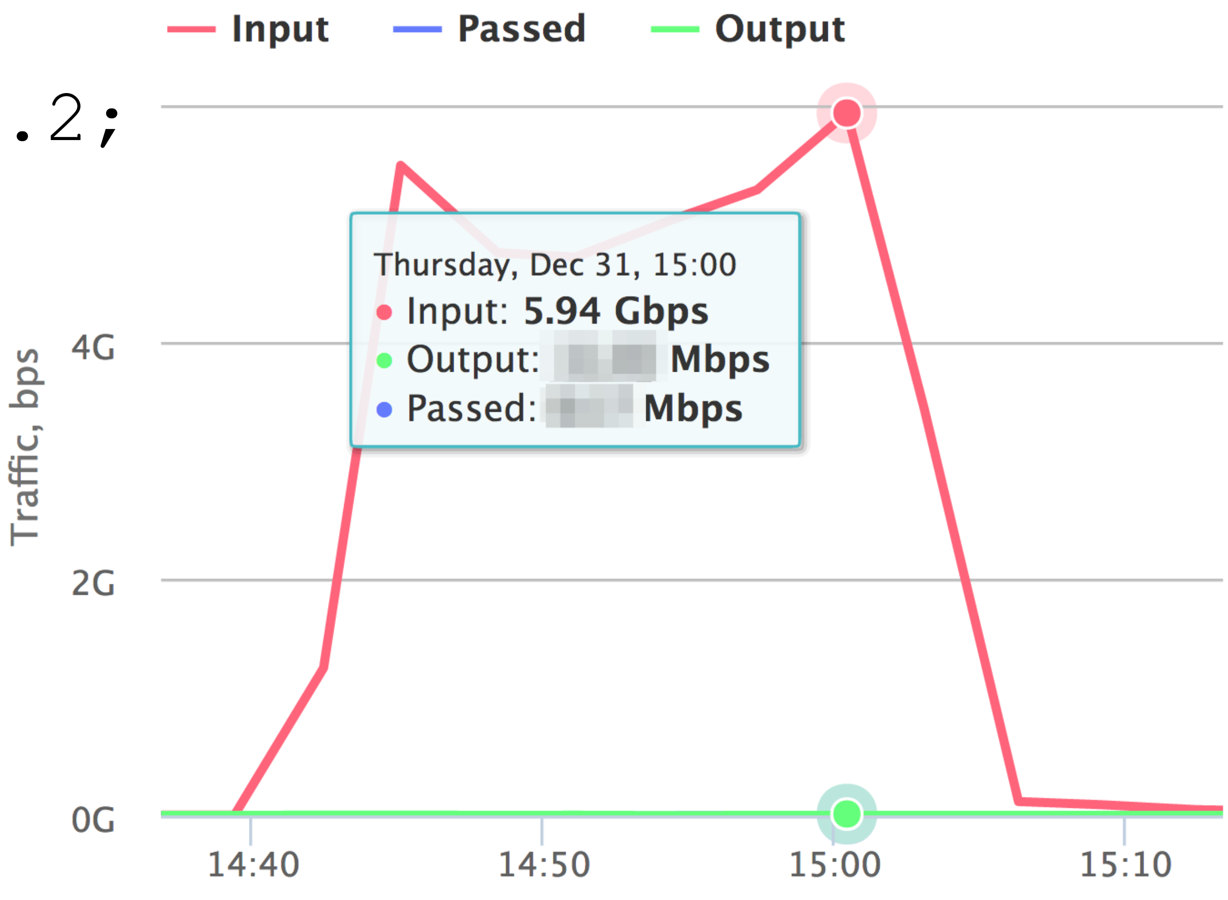
- NTP
- DNS
- SNMP
- SSDP
- ICMP
- NetBIOS

- RIPv1
- PORTMAP
- CHARGEN
- QOTD
- **Quake**
- …

Wordpress Pingback

```
GET /whatever
User-Agent: WordPress/3.9.2;
 http://example.com/;
 verifying pingback
 from 192.0.2.150
```

- 150 000 – 170 000 vulnerable servers at once
- SSL/TLS-enabled

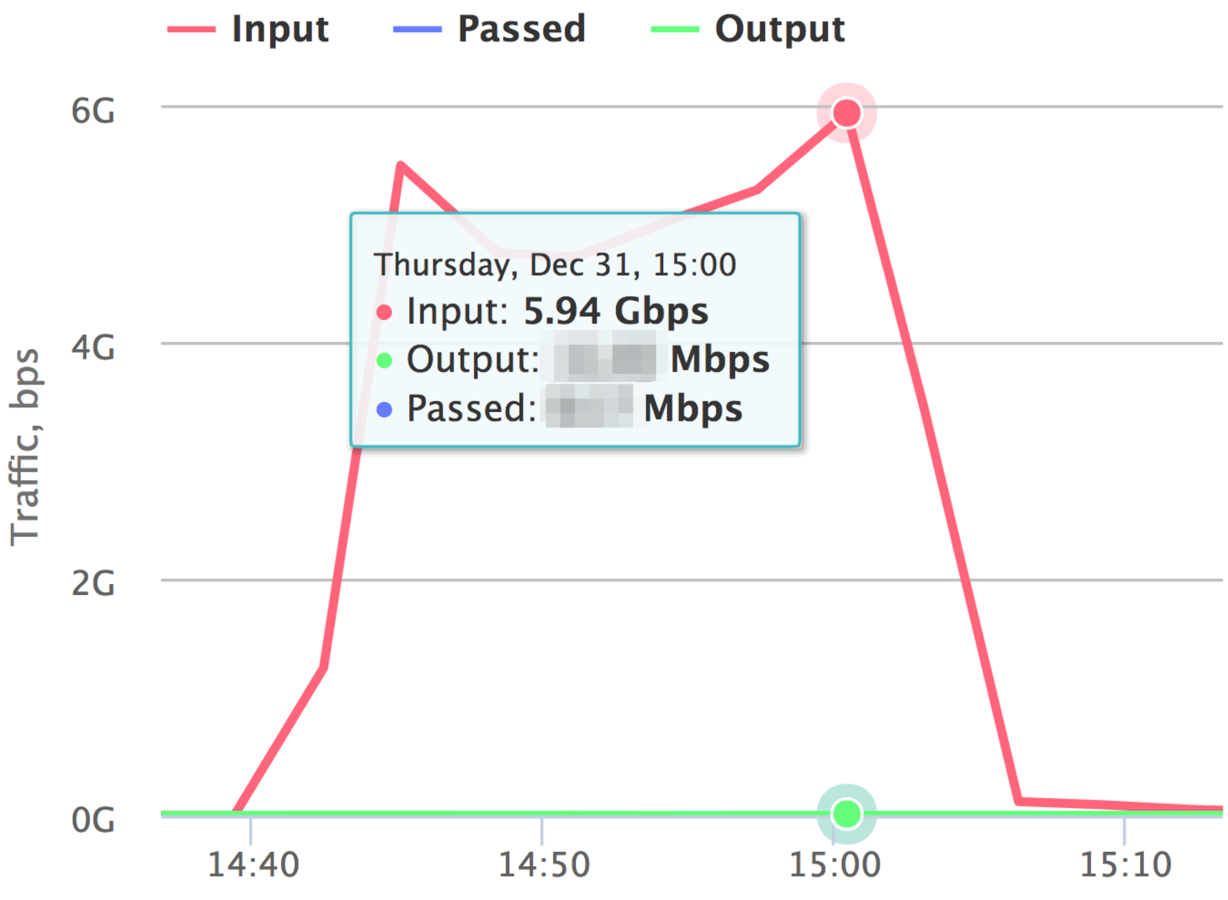


Data from Qrator monitoring engine

Wordpress Pingback

- SSL/TLS-enabled
- No port data available for filtering

- Also, network operators **hate** giving FlowSpec to anyone

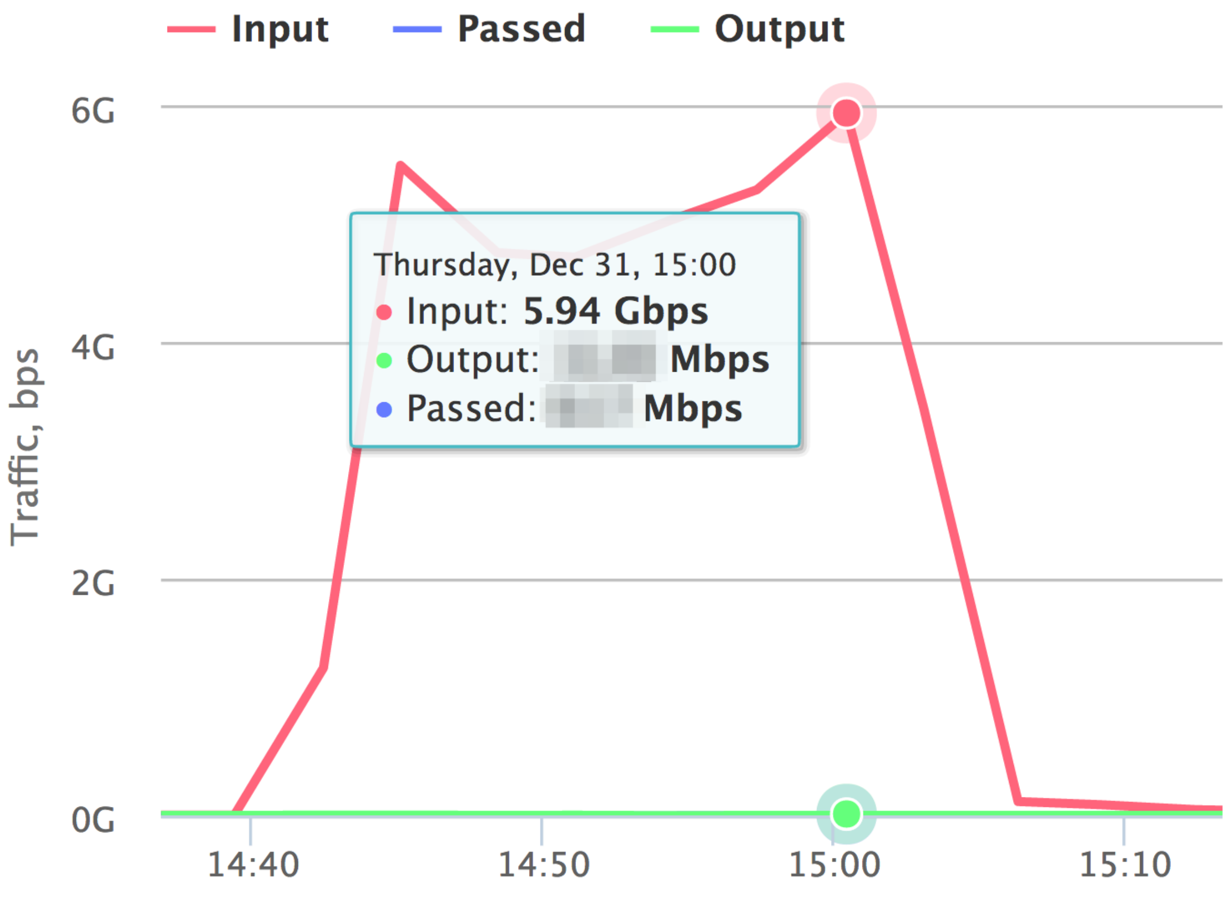


Data from Qrator monitoring engine

Wordpress Pingback

- Pingback was the first case of Web dev causing DDoS problems to ISPs

(has anyone really thought it would be the last case)



Thursday, Dec 31, 15:00
● Input: **5.94 Gbps**
● Output: [redacted] **Mbps**
● Passed: [redacted] **Mbps**

Data from Qrator monitoring engine

memcached

- A **fast** in-memory cache
- Heavily used in Web development

memcached

- A **fast** in-memory cache
- Heavily used in Web development

- Listens on all interfaces, port 11211, by default

memcached

- Basic ASCII protocol doesn’t do authentication
- 2014, Wallarm, Blackhat USA:
  “An attacker can inject arbitrary data into memory”

memcached

- Basic ASCII protocol doesn't do authentication
- 2014, Wallarm, Blackhat USA:
  "An attacker can inject arbitrary data into memory"

- **2017, 360.cn, Power of Community:**

  "An attacker can send data from memory to a third party via spoofing victim's IP address"

```
import memcache
m = memcache.Client([
    ‘reflector.example.com:11211’
])
m.set(’a’, value)
```

– to inject a value of an arbitrary size under key “a”

```
print ’\0\x01\0\0\0\x01\0\0gets a\r\n’
```

– to retrieve a value

```
print ’\0\x01\0\0\0\x01\0\0gets a a a a a\r\n’
```

– to retrieve a value **5 times**

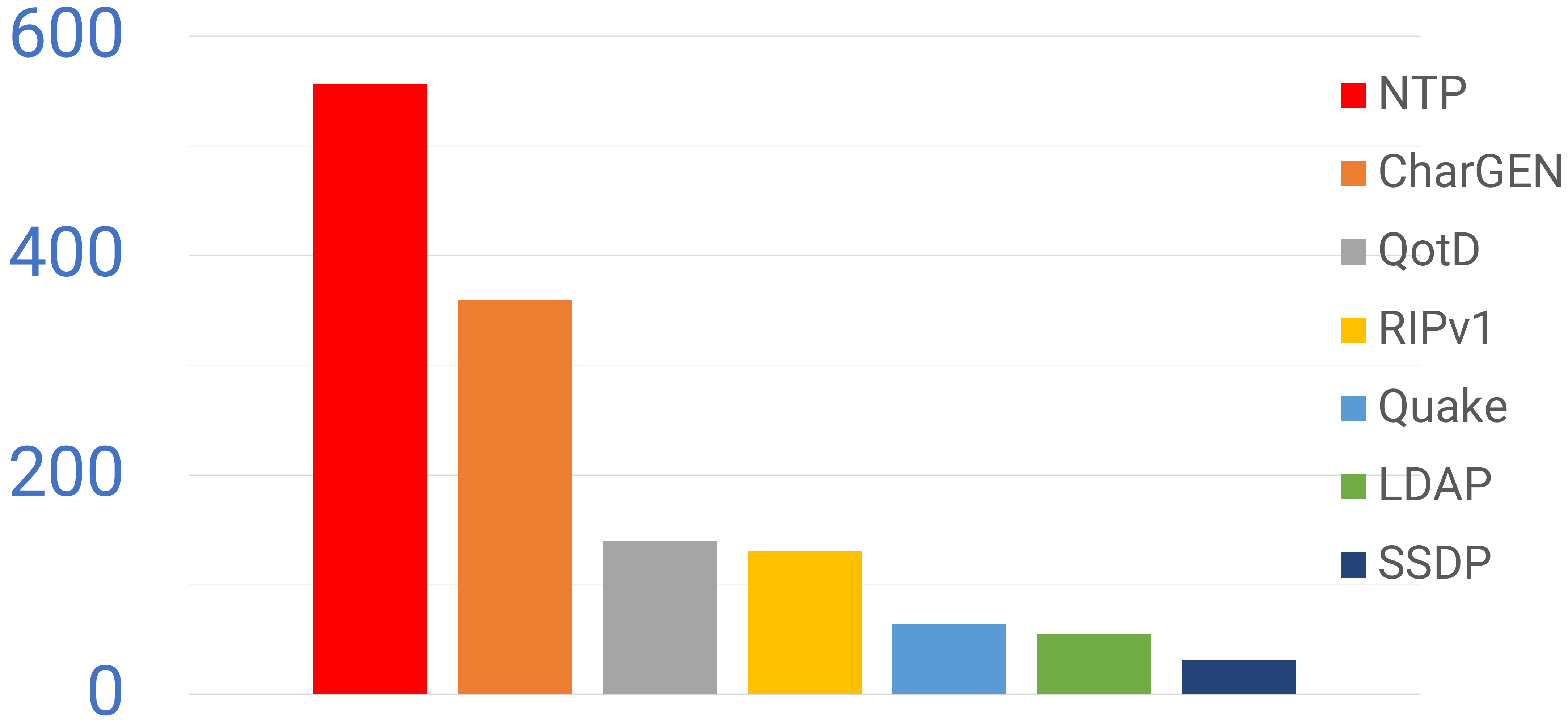
```
print ’\0\x01\0\0\0\x01\0\0gets a a a a a\r\n’
```

– to retrieve a value **5 times.**

Or 10 times.

Or a hundred.

Amplification factor



Source: https://www.us-cert.gov/ncas/alerts/TA14-017A

memcached

- Theoretical amplification factor is **millions**

memcached

- Theoretical amplification factor is **millions**

- Fortunately, all the packets aren't sent at once
- In practice, the amplification factor is 9000-10000

- **Still 20 times the NTP Amplification does.**

memcached

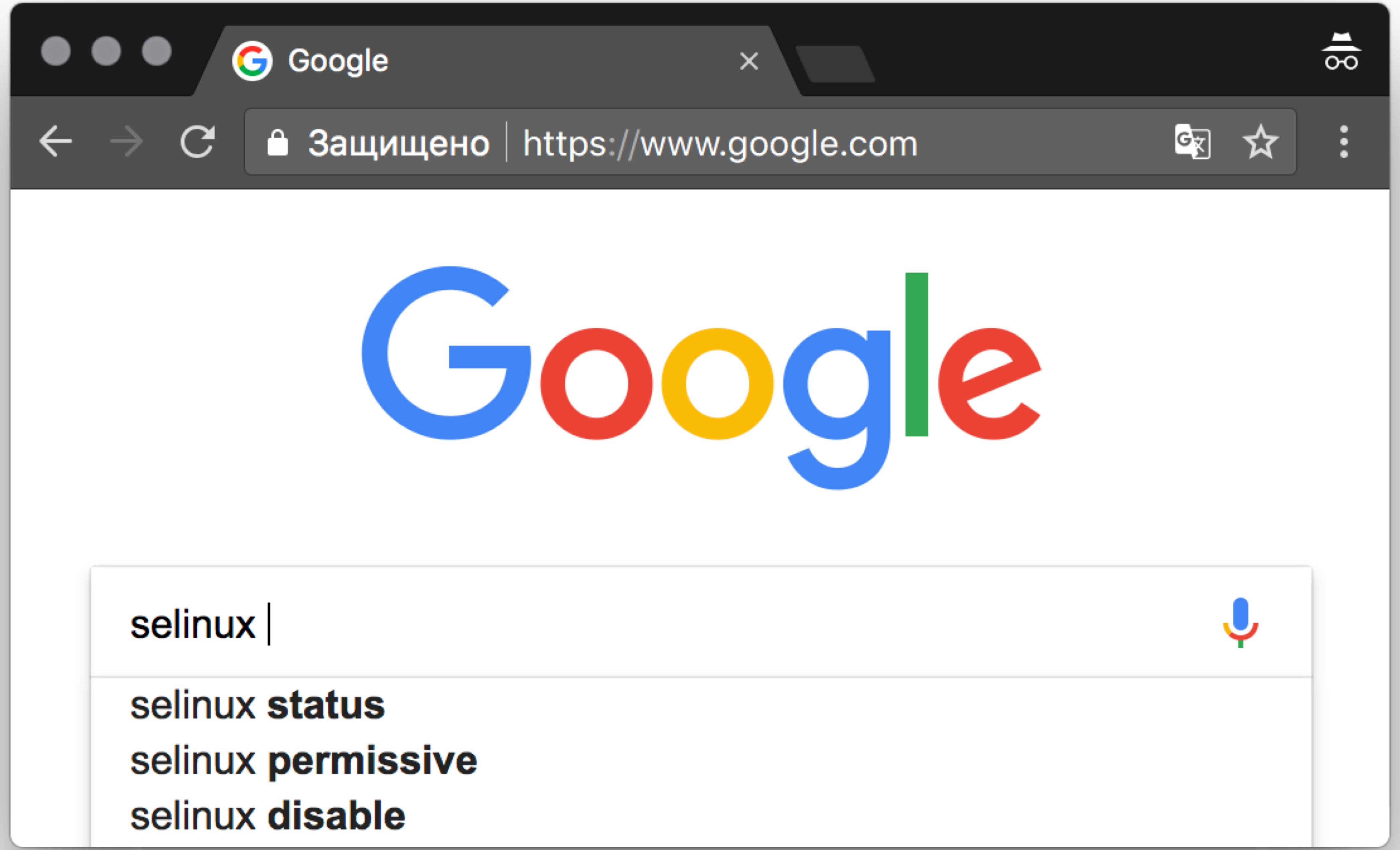
- Fortunately, all the packets aren’t sent at once
- In practice, the amplification factor is 9000-10000
- **Still 20 times the NTP Amplification does.**
- Seeing 200-500 Gbps, we projected **up to 1,5 Tbps** during APNIC 45 in February
- **1.7 Tbps happened**

Default memcached conf. in Red Hat

  - memcached listens on all network interfaces
  - both TCP and UDP transports are enabled
  - no authentication is required to access Memcached

  - the service has to be manually enabled or started
  - the default firewall configuration
    does not allow remote access to Memcached

- Also Zimbra, etc.



selinux

selinux **status**
selinux **permissive**
selinux **disable**

Mitigation

- Think about fighting spoofed packets
- Make sure you don’t have open `memcached` port `11211/udp` on your network
- Use firewalls or FlowSpec to filter `11211/udp`

```
ipv4 access-list exploitable-ports
    permit udp any eq 11211 any
   !
   ipv6 access-list exploitable-ports-v6
    permit udp any eq 11211 any
   !
   class-map match-any exploitable-ports
    match access-group ipv4 exploitable-ports
    end-class-map
   !
   policy-map ntt-external-in
    class exploitable-ports
     police rate percent 1
      conform-action transmit
      exceed-action drop
     !
     set precedence 0
     set mpls experimental topmost 0
    !
...
```

Source: http://mailman.nlnog.net/pipermail/nlnog/2018-March/002697.html

```
...
    class class-default
     set mpls experimental imposition 0
     set precedence 0
    !
    end-policy-map
   !
   interface Bundle-Ether19
    description Customer: the best customer
    service-policy input ntt-external-in
    ipv4 address xxx/x
    ipv6 address yyy/y
    ...
   !
   interface Bundle-Ether20
    service-policy input ntt-external-in
    ...
   ... etc ...
```

Source: http://mailman.nlnog.net/pipermail/nlnog/2018-March/002697.html

What’s next?

- Web dev won’t stop here
- And gaming industry won’t

- This will happen again.

- Time to discuss possible threats with upstream providers

What’s next?

- In 2016, we’ve almost seen the Internet on fire due to an Internet of Things botnet
- Numerous working groups and nonprofits were launched to address *“**the IoT problem**”*

What’s next?

- In 2016, we’ve almost seen the Internet on fire due to an Internet of Things botnet
- Numerous working groups and nonprofits were launched to address ***“the IoT problem”***

- `memcached` is **not** IoT
- What should we expect then, a memcache WG? ;-)

What’s next?

- memcached:
  - Disclosure in November 2017
  - In the wild: February 2018

- Three months are an overly short interval
- With **Cisco Smart Install**, it was even shorter
- Meltdown/Spectre show: the “embargo” approach doesn’t work well for a community large enough

What’s next?

- Maybe our focus is wrong?

- Collaboration
- Proper and timely reaction
- RFC 2350: CERT/CSIRT for network operators?
    - No matter the name

Q&A

mailto: Artyom Gavrichenkov <ag@qrator.net>