# The Traffic Amplifiers Great Hunt:

## Helping Network Operators to Bring Down DDoS Sources

*Pierre Lorinquer,* ***Florian Maury***

**November 19, 2015**

# ANSSI

## French Network and Information Security Agency

**ANSSI**:

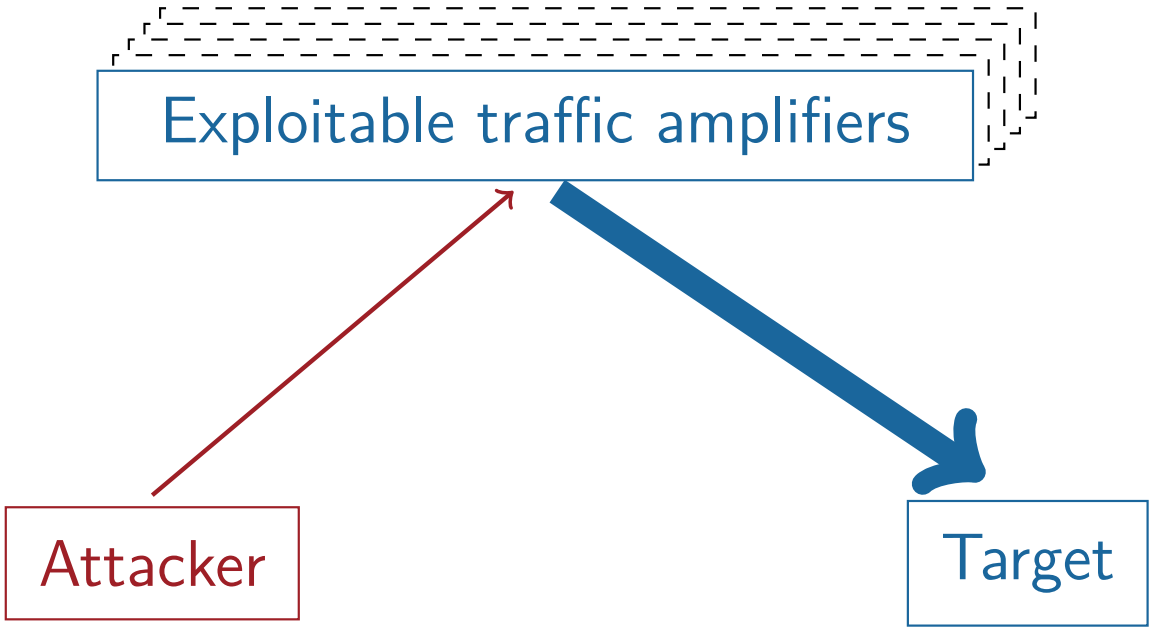
- national authority for the defence and security of information systems
- main missions: **Prevention**, **Defence**, **Information**
  - tranversal actions covering French governmental organizations, critical operators and the general public
  - guidance provider on network security topics (DNS, BGP, DDoS prevention. . . )
  - academic research, Internet Resilience Observatory in France, CVE. . .
  - coordinated response thanks to our CERT

# Amplification DDoS Attack Reminder

# Amplification Attack Principle

Threat: on IP networks, sender address **can be spoofed**

**Some UDP-based protocols do not make up for it**




Real IP: 192.0.2.66

**Spoofed IP: 198.51.100.42**

Real IP: 198.51.100.42

# Amplification Attack Fingerprint

Attacks traits:

- bandwidth-based or packet-based

Exploitable protocols:

- are unauthenticated or with well-known credentials
- must be widely deployed
- can be preloaded to improve amplification factor

# Identifying the Amplifiers:

# as easy as an Internet Sweep

# ANSSI Internet Scan Monitoring

Monitoring of a /22 IP address block shows that **many hosts scan the Internet**.

Some are **scanning projects**:

- academic / research projects (University of Michigan, University of Washington, Ruhr University Bochum . . . ) ;
- well-known scanning projects (Shadowserver, Shodan, Rapid7, Open * Project).

# Open * Projects Presentation

Four projects:

- Open (DNS) **Resolver** Project: http://www.openresolverproject.org/
- Open **NTP** Project: http://www.openntpproject.org/
- Open **SNMP** Project: http://www.opensnmpproject.org/
- Open **SSDP** Project: http://www.openssdpproject.org/

Project characteristics:

- powered by **Jared Mauch** (NTT)
- perform weekly scans of Internet address space
- provide **raw scan results** to researchers (thanks!)

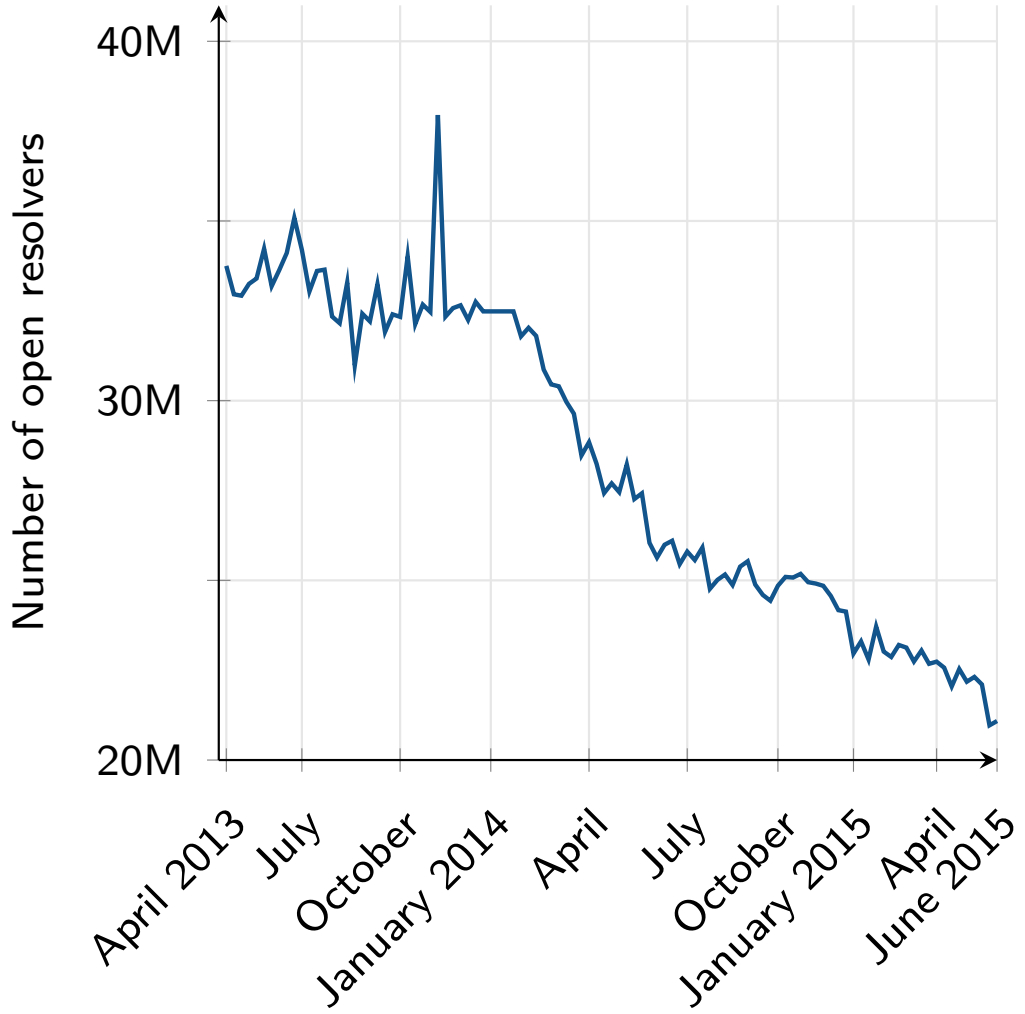
# ANSSI Initiative Regarding These Data Sources

We:

- requested access to Open * Projects raw results
- analyzed data and focused on French ASes
- summarized information and alerted French network operators
- monitored the development, both worldwide and in France

# Monitoring the Number of Traffic Amplifiers Per Protocol

# Open Resolver Worldwide Count

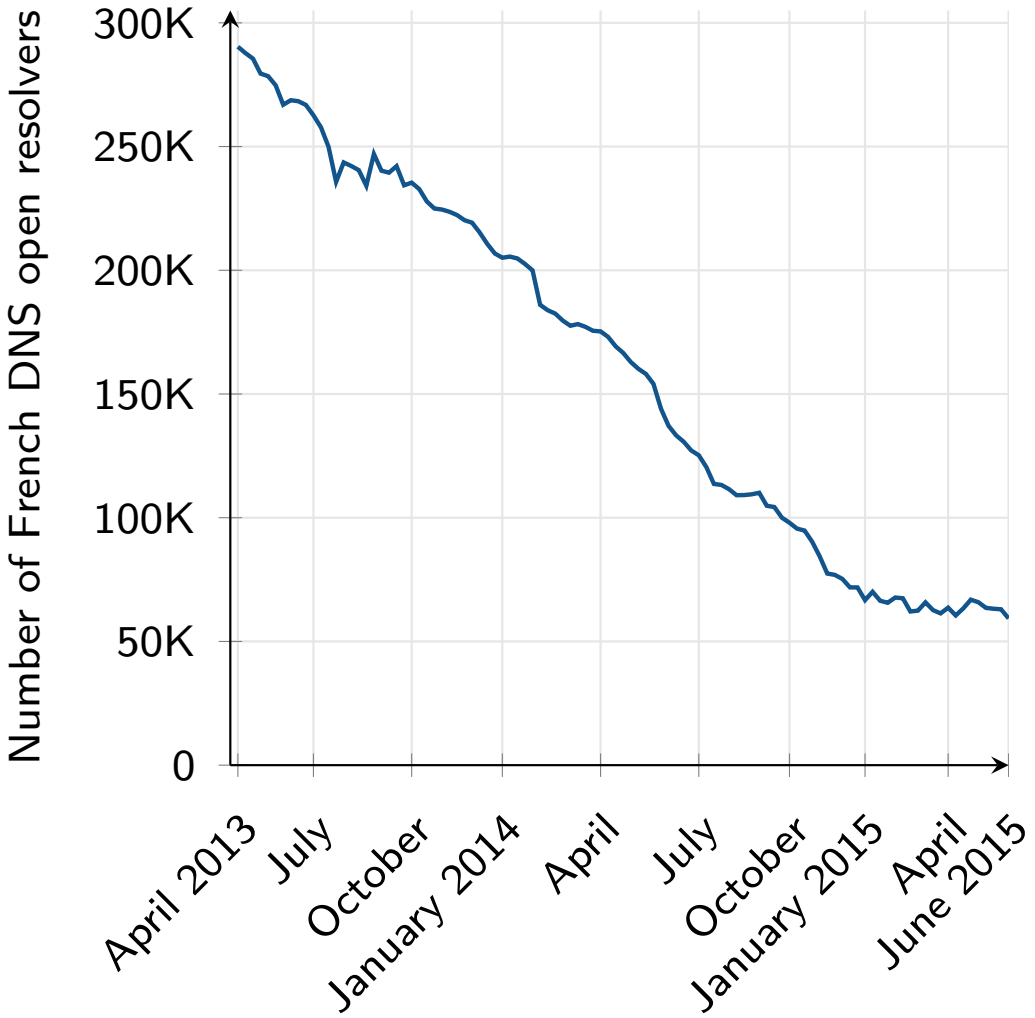



Reduction by a 3rd over the period

Very large DDoS use **only hundred of thousands of nodes**

**Open DNS resolvers remain a significant threat**

# French Open Resolver Count




Reduction by 80 % over the period

Slow trend: takes a lot of efforts/huge expenses to replace no longer supported devices

70 % of French open resolvers under one AS in 2013

# Random Qname Attacks: an additional risk

Hosting open resolvers may cary DoS risks: **random qname attack**

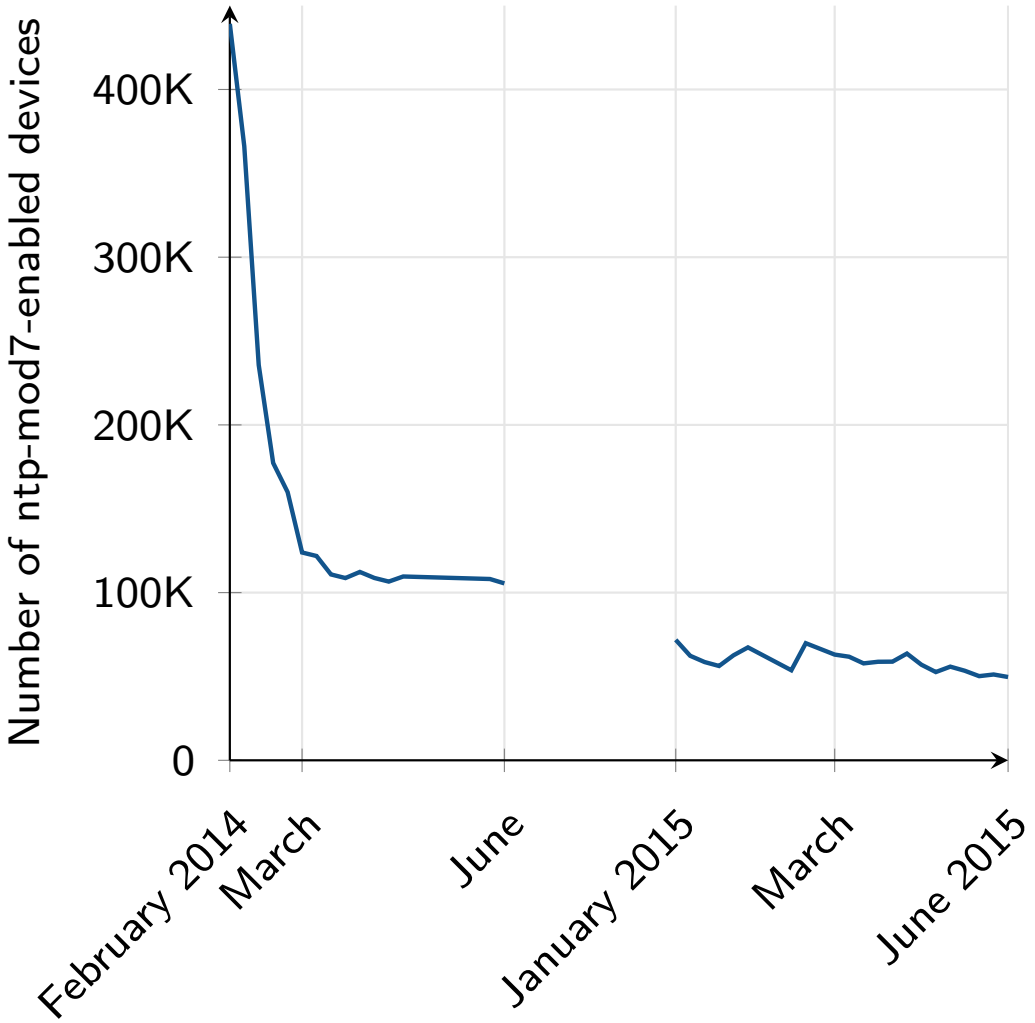
One operator was targetted by this attack:

- had prepared in lab a countermeasure for the DDoS attack
- rolled it out for this incident
- firewall rule to drop incoming DNS traffic

Results: almost no client complaints and open resolvers threat thwarted

# Amplifying NTP Server Worldwide Count

## Mod7 - Monlist



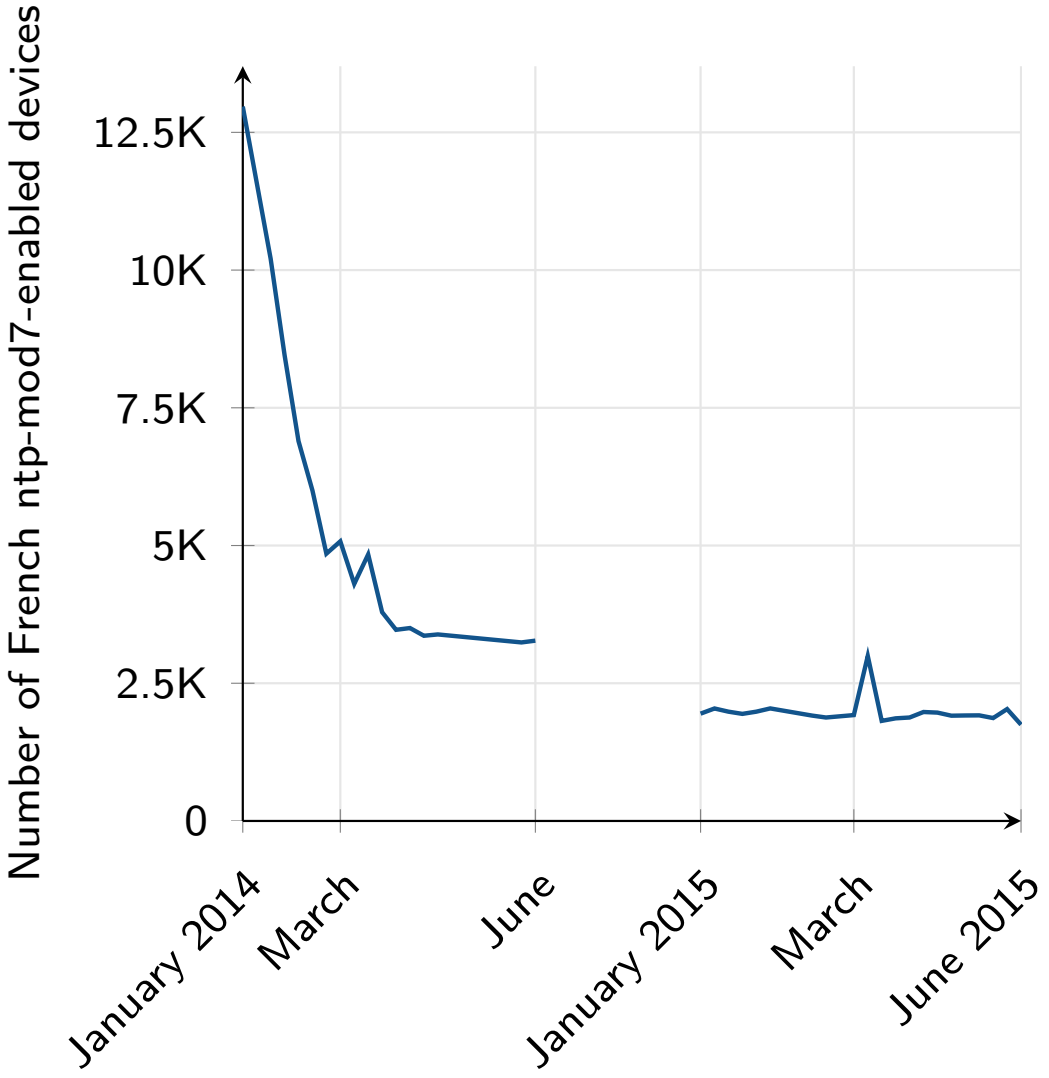

Operators already knowledgeable about amplification attacks: **quick response**

**NTP problem easier** to solve than the DNS one: upgrade to a **ntpd** version with safe default values, tweak configuration or block traffic with almost no side-effect

**Team Cymru provides safe configuration templates:**
`http://www.team-cymru.org/secure-ntp-template.html`

# French Amplifying NTP Server Count

## Mod7 - Monlist

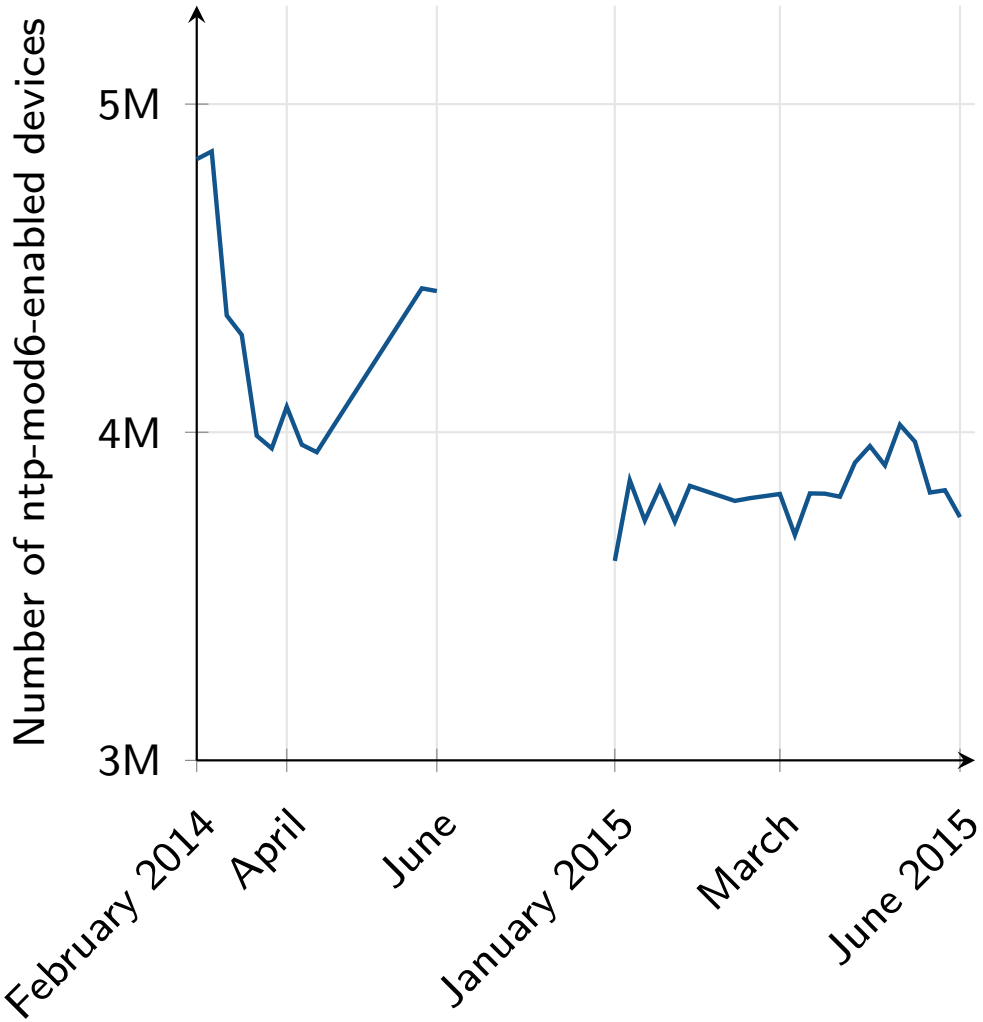



France results similar to world-wide results

Spike in March 2015 from a new operator deployment that quickly handled the issue

# Amplifying NTP Server Worldwide Count

## Control Messages (Mod6) - ReadVar

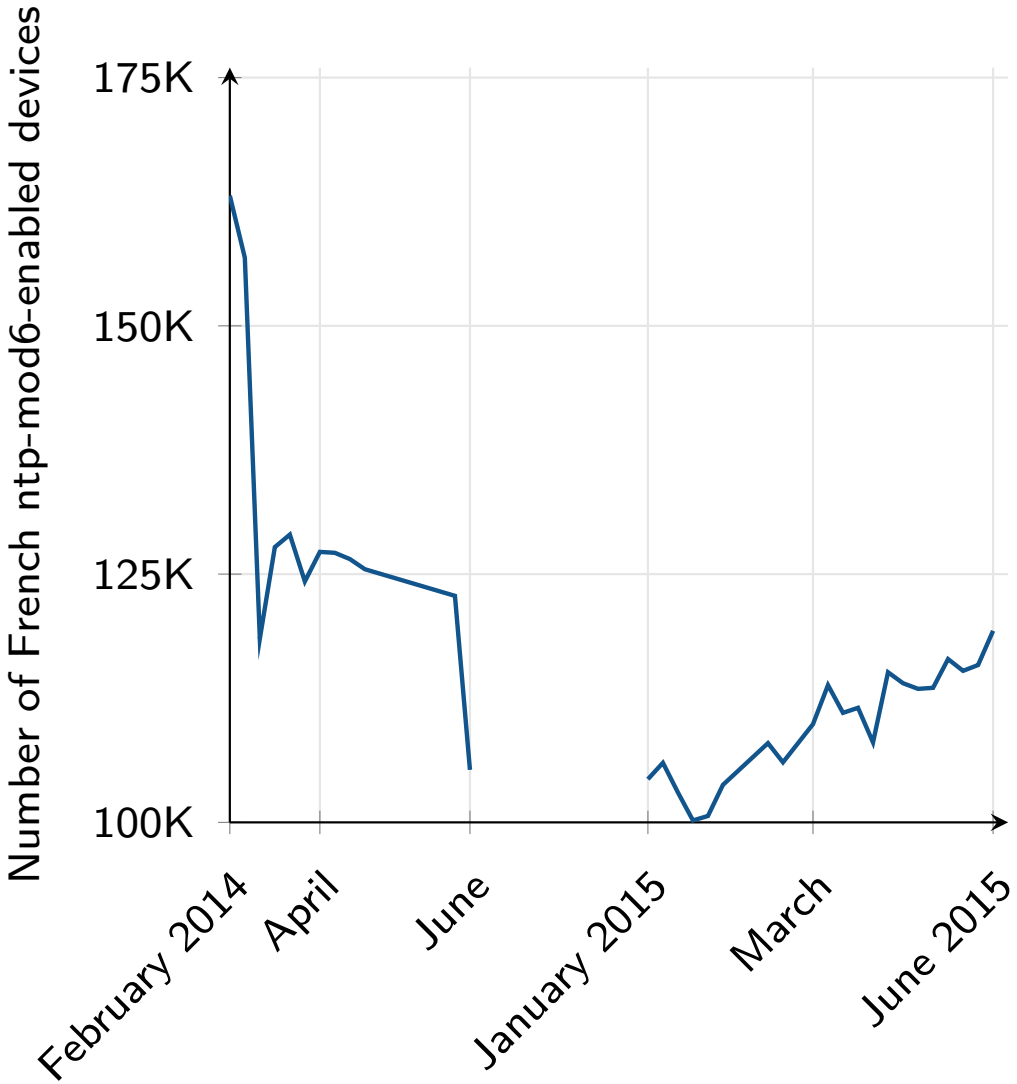



Mod6 messages amplify traffic but **amplification factor is less dramatic**

Mod6 is a RFC-standard message: **not only a ntpd issue**

# French Amplifying NTP Server Count

## Control Messages (Mod6) - ReadVar

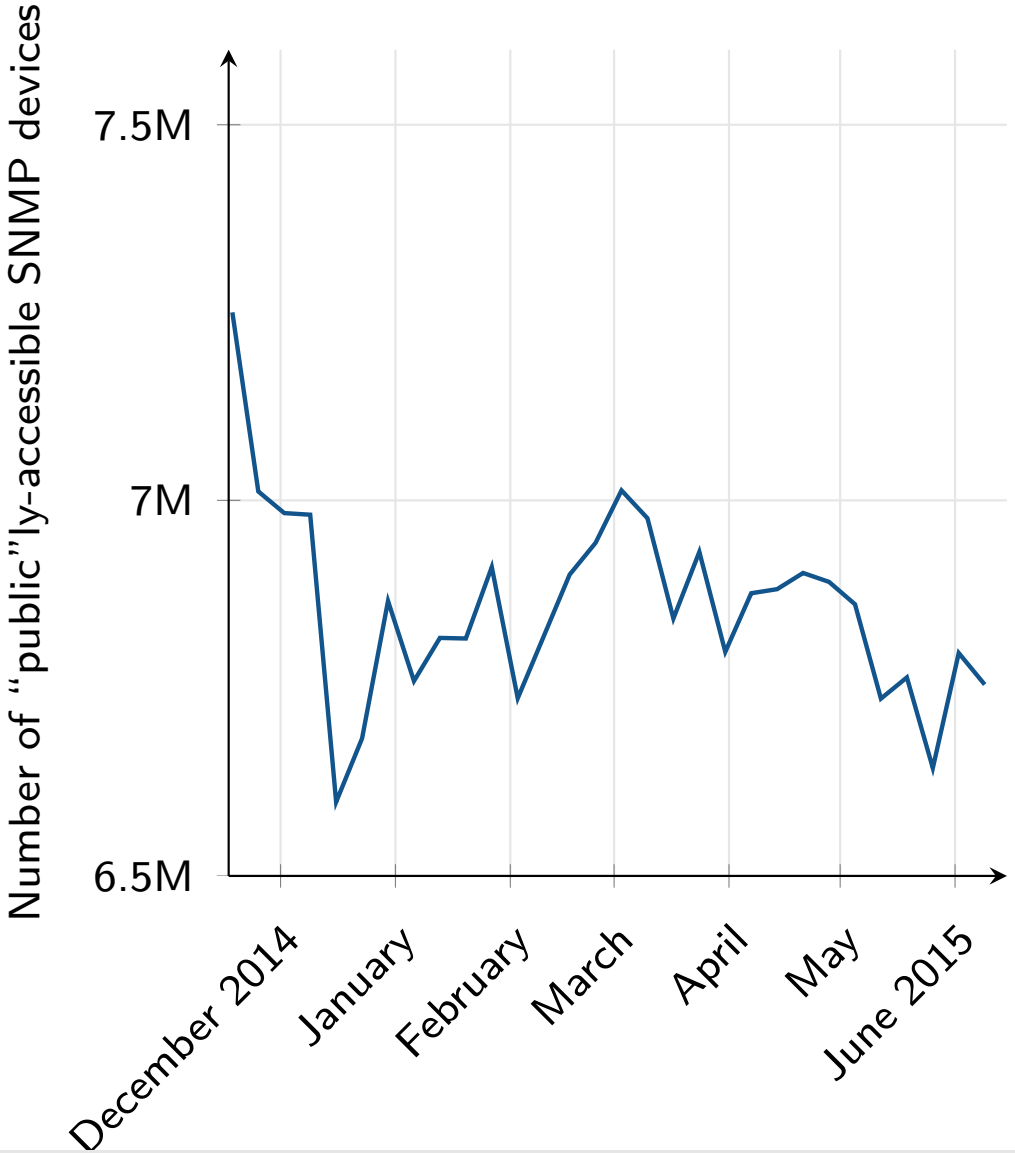



One AS responsible for **47 % of NTP mod6 amplifiers, in May 2014**

This AS reduced its amplifier count by a third in June 2014

**Two operators rolled out amplifiers during 2015**

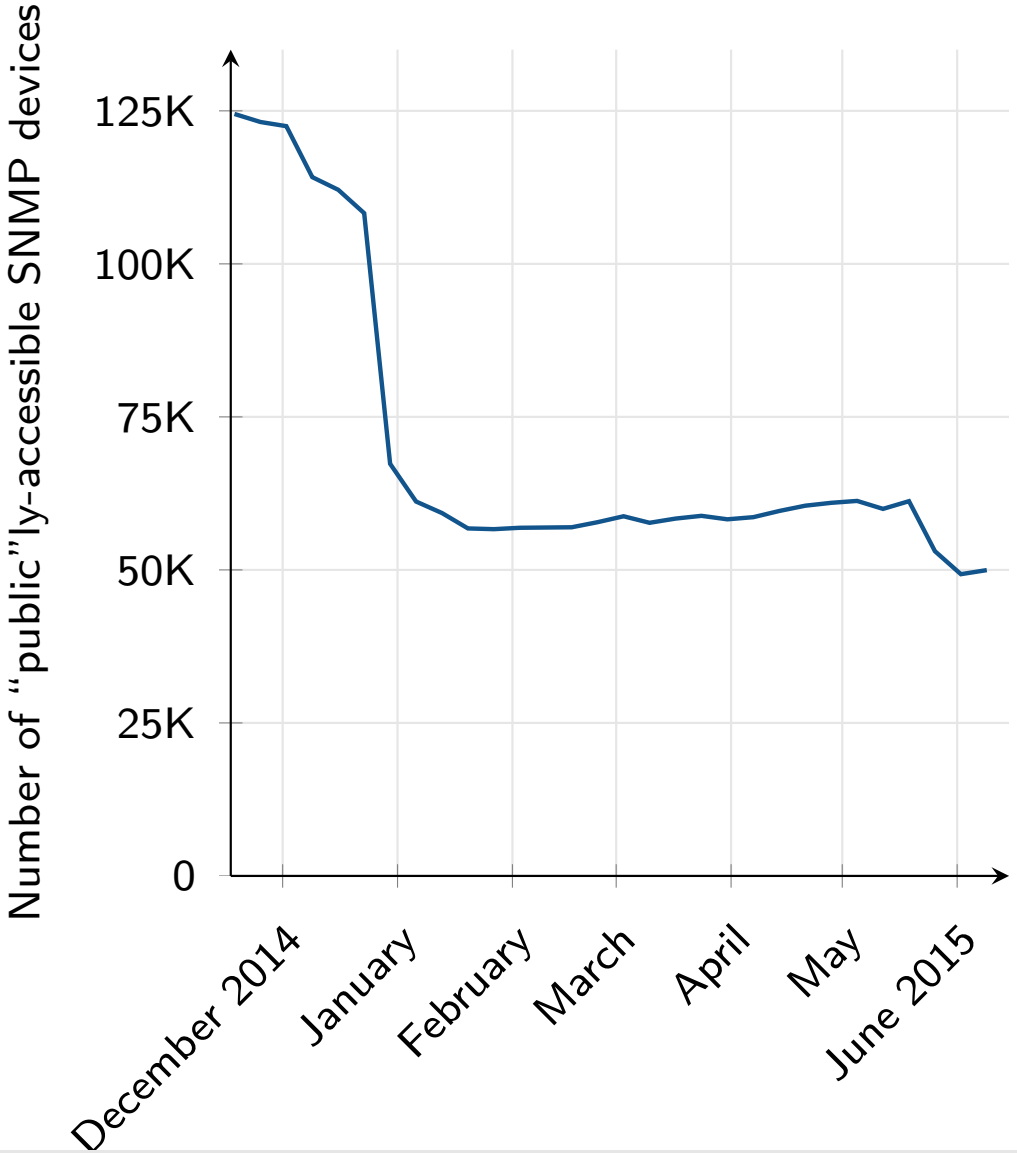
# Responding SNMP Device Worldwide Count




More than 6,750,000 devices identified worldwide

**There was no significant decrease of the number of devices since December, 2014**

# French Responding SNMP Device Count




Around 50 000 devices in France (0.7 % of the total number of devices) in June, 2015

**The number of devices in France has fallen by nearly 60 % since the beginning of the process**

This improvement is mainly due to the decrease of the number CPEs, but also network devices such as routers, switches. . .

# Open SSDP Project

**June, 2015**:

Almost 10 million devices identified by the scans

20 000 devices in France (0.2 %)

**There was no significant decrease since the beginning of the year (both in the world and in France).**

# Mitigation Challenges

# &

# Effective Countermeasures

# Challenge: a Wide Variety of Traffic Amplifiers

## Exploitable Devices Breakout

- numerous CPEs (Internet gateways)
  - some are no longer supported, or partly hard-coded
  - support contact required for device replacement
- some pseudo-savvy customers
- various types of PE devices (routers, switches, firewalls)
- Voice over IP / Video conferencing devices
- multimedia devices

# Effective Countermeasures

Mostly common sense countermeasures:

- **Apply security updates**
- **Stick to configuration best current practices**
- **Rate-Limit** traffic for protocols and services that can be exploited
- **Block** traffic coming from local services, when possible. For example, drop traffic that should not be seen on the Internet (SSDP)

# Take Aways

# Take Aways

1. Amplifiers are still a very real problem
2. New protocol regularly discovered vulnerable or specified!
3. Some scanning projects provide raw data to researchers and do-gooders
4. Tipping the balance can sometimes be done with the help of few operators
5. Fixing the damn things takes time = extensive work for operators
6. CERTs and governmental agencies can help (guidance, documentation, reports...)

**Thank you for your attention.**

**Q&A**

**Contact: florian.maury @ssi.gouv.fr**

# Open Resolver Project: Captured Probe

## Recursive Query

```
value {
  id: 17152 (0x4300)
  qr: false
  opcode: StandardQuery (0 = 0x0)
  aa: false
  tc: false
  rd: true
  ra: false
  z: 0 (0x0)
  rcode: NOERROR (0 = 0x0)
  qdcount: 1 (0x1)
  ancount: 0 (0x0)
  nscount: 0 (0x0)
  arcount: 0 (0x0)
  questions {
    questions[0] {
      qname: "f07b0a49.openresolverproject.org"
      qtype: A (1 = 0x1)
      qclass: IN (1 = 0x1)
    }
  }
  answers {}
  authority_answers {}
  additional_records {}
}
```

# Open NTP Project: Mod7 Captured Probe

## NTP Monlist Query (Mod7)

```
value {
  response: false
  more: false
  version: 2 (0x2)
  mode: 7 Reserved for private use (7 = 0x7)
  authenticated: false
  sequence: 0 (0x0)
  implementation: ntpd post IPv6 (3 = 0x3)
  reqcode: Return collected v1 monitor data (42 = 0x2a)
  errcode: No error (0 = 0x0)
  data_item_count: 0 (0x0)
  mbz: "0000" (4 bytes)
  data_item_len: 0 (0x0)
  data {}
}
```

# Open NTP Project: Mod6 Captured Probe

## NTP Readvar Query (Mod6)

```
value {
  null_magic: 0 (0x0)
  version: 2 (0x2)
  mode: 6 NTP control message (6 = 0x6)
  response: false
  error: false
  more: false
  opcode: Read variables command/response (2 = 0x2)
  sequence: 1 (0x1)
  unparsed_status: 0000 (2 bytes)
  association_id {
    association_id: 0 (0x0)
  }
  offset: 0 (0x0)
  len: 0 (0x0)
  data {
    VariablesRead: "" (0 byte)
  }
  padding: "" (0 byte)
}
```

# Open SNMP Project: Captured Probes (1)

## GetBulkRequest

```
###[ SNMP ]###
  version    = <ASN1_INTEGER[1L]>
  community = <ASN1_STRING['public']>
  \PDU        \
   |###[ SNMPbulk ]###
   |  id             = <ASN1_INTEGER[60461639L]>
   |  non_repeaters= <ASN1_INTEGER[0L]>
   |  max_repetitions= <ASN1_INTEGER[10L]>
   |  \varbindlist\
   |   |###[ SNMPvarbind ]###
   |   |  oid          = <ASN1_OID['.1.3.6.1']>
   |   |  value        = <ASN1_NULL[0L]>
```

# Open SNMP Project: Captured Probes (2)

## GetNextRequest

```
###[ SNMP ]###
  version   = <ASN1_INTEGER[0L]>
  community = <ASN1_STRING['public']>
  \PDU       \
   |###[ SNMPnext ]###
   |  id          = <ASN1_INTEGER[2122146261L]>
   |  error       = <ASN1_INTEGER[0L]>
   |  error_index= <ASN1_INTEGER[0L]>
   |  \varbindlist\
   |   |###[ SNMPvarbind ]###
   |   |  oid         = <ASN1_OID['.1.3.6.1']>
   |   |  value       = <ASN1_NULL[0L]>
```

# Open SSDP Project: Captured Probe

**ssdp:discover**

```
M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:ssdp:all
Man:"ssdp:discover"
MX:3
```