

# Internet Abuse

Real-life tips & tricks for reporting an handling

Jurrian van Iersel

NLNOG-day, september 8th, 2017



@JurrianVI



[linkedin.com/in/jurrianvaniersel](https://www.linkedin.com/in/jurrianvaniersel)

# Who am I?

- IT Developer at Infopact
- Volunteer at Coloclue (developer, system- & network admin)
- Contributions to several Open Source projects
- This talk is about a personal project in spare time

# Project history

- Started in 2012
- Noticed high number of login attempts
- 1 report took me > 30 minutes
  - Find abuse-contact
  - Copy-paste relevant lines from logfiles to textfile
  - Write an email
- I am a developer, this can be automated

# Abuse Indexing & Reporting

- Parse logfiles hourly, add abuse to database
  - Webserver (PhpMyAdmin, WordPress, .asp, .cfm, .cgi)
  - Mailserver (SMTP-auth, relaying, non-existing domains)
  - Port scans (portsentry)
  - Failed SSH logins
  - DNS unauthorized zone transfers and queries
- Catch-all on unused domains, import spam
  - Also report to Spamcop
- Independent, non-manipulated analytics
- Send aggregated report per IP once a day
  - Use X-ARF standard, planning to add IOdef
  - This is where the problems starts...

# Independent statistics

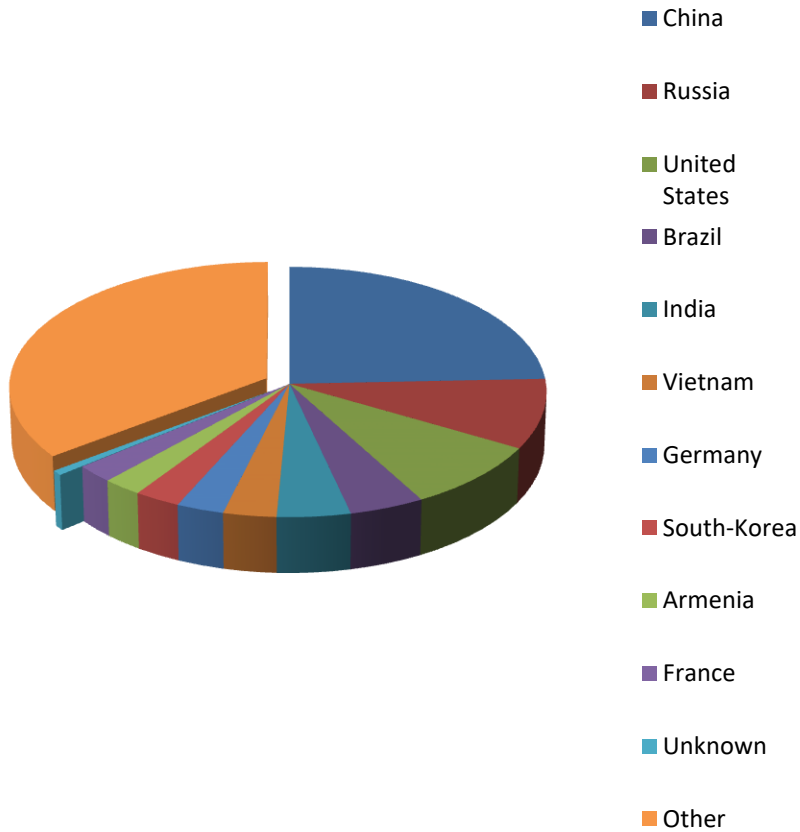
I am not...

- a salesman for security products
- payed by a company selling security products
- forced by a government or company to silence about certain security incidents

Data is collected from personal (virtual) servers in multiple countries

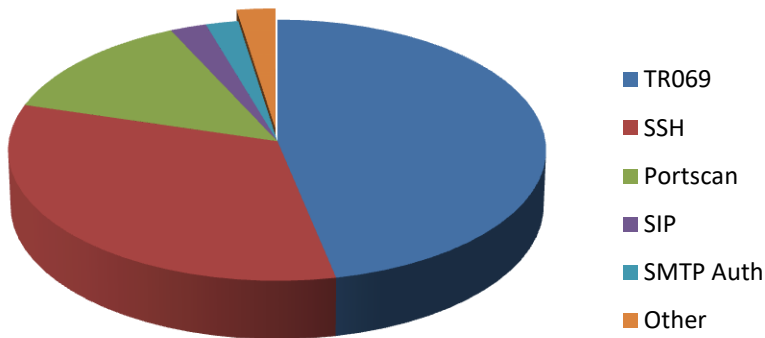
# Top 10 originating countries of abuse

- Data from 2017-01-01 till 2017-09-01



# Top 5 type of abuse

- Data from 2017-01-01 till 2017-09-01
- Multiple incidents from same IP-address counted as one



# Problem 1: find abuse contact

- Abuseix.org, lot of invalid information
- 5 RIR's, 5 different WHOIS-formats
  - Brazil has it's own organization / WHOIS
  - Most have field for abuse contact
    - RIPE NCC has a nice REST API
- Still lots of corrections by hand



# Problem 2: invalid information

- Delegations not registered in WHOIS
- Abuse-contact in free-text field (remark)
- Emailaddress does not exist (anymore)
  - Domainname isn't registered anymore
  - Employee left the company
  - RIRs: please start periodic validation
- Mailserver unreachable
  - My opinion: main problem in abuse from China

# Problem 3: wrong handling

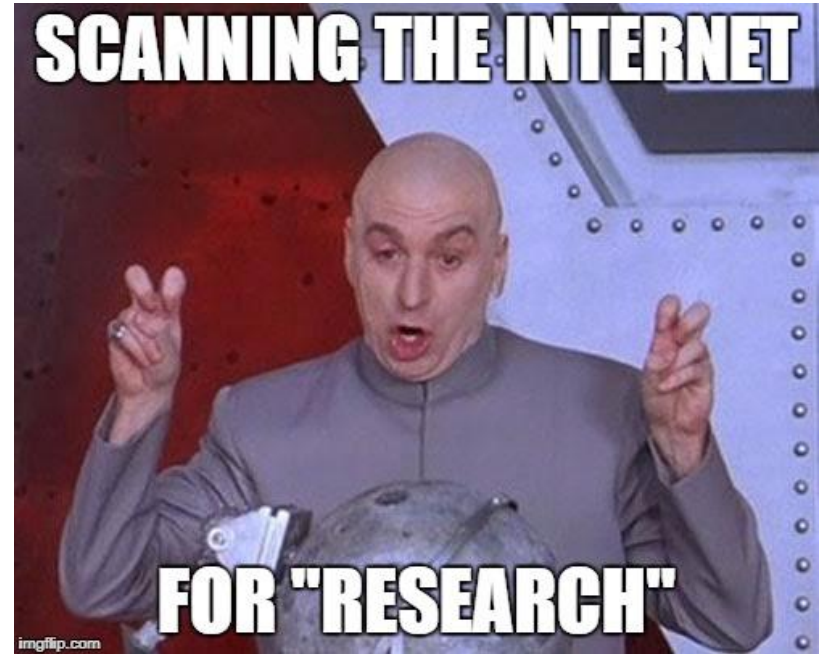
- Distribution list
  - Autoresponders
  - Mailbox does not exist anymore
  - Mailbox reached max. size
- Please use the form on our website
- Not allowed to open attachments
- Forward my own report to me, because I am also a customer

# Problem 4: ticketing systems

- Wrote a tool to handle replies, add your ticket-id to my next report
- Common problems:
  - Ticketing system replaces subject, incl. my ID
    - “Please do not remove our ID”
  - No follow-up on tickets
    - Reporting daily > 2 months, customer didn’t take action. Staff from abuse desk knows my name on conference...

# Problem 5: “research projects”

- Why not use shodan.io, shadowserver, etc.
- I don't believe you if my 10th report this week is again “research”
- Scans should be opt-in, not opt-out



Discuss these things with your “research”-customer

# Good news!

- Most ISP's take action on complaints
- Except 'bullet proof' hosters
- Some shut down customer's server immediately
- Most urge customers to solve it within 24 – 48 hours
  
- Some customers don't understand, think I am some kind of federal agent

Reporting does matter!

# Advice

- Use a dedicated email address and mailbox for abuse
- Ticketing
  - add ID to subject instead of replacing. Between [ ] or ( ) is common
  - Link report to affected customer, not the reporter
- Make sure correct address is in WHOIS
  - Schedule a (half)yearly check in your agenda
  - Until RIRs start periodic validation

# Advice

- Handle X-ARF and IOdev reports automatically
  - Saves time, notify customer faster
- Use automated reports like
  - Feedback loops
  - Spamcop
  - Project Honeypot
  - Microsoft SNDS
  - Shadowserver

Have a look at AbuseIO, <http://abuse.io>

Questions?