26th annual **FIRST** conference

BOSTON

MASSACHUSETTS

JUNE 22—27, 2014

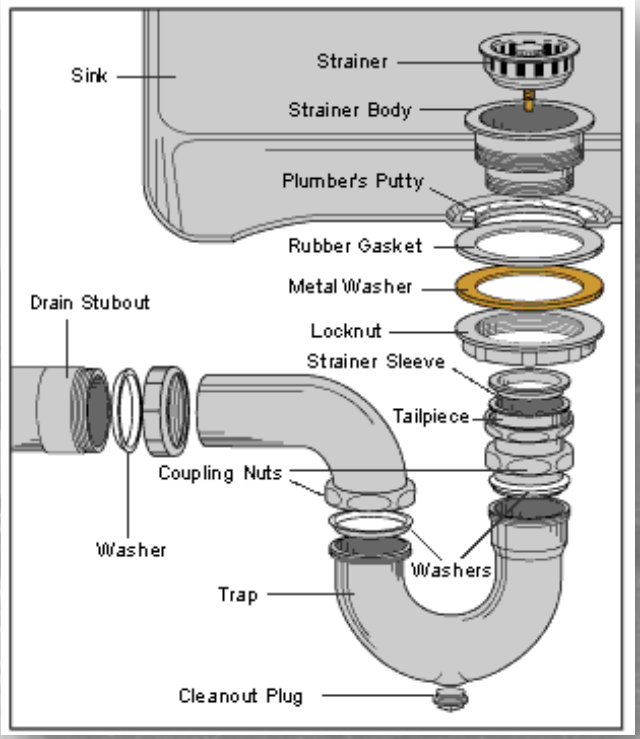
Back to the 'root' of Incident Response

Boston Park Plaza Hotel | June 22-27, 2014

The art of sinkholing

Tomasz Bukowski

CERT Polska / NASK



About

WHOIS

- Name:Tomasz Bukowski (tomasz.bukowski@cert.pl)
- Works in CERT Polska/NASK
- 5 years in IRT
- Fight malware && monitor botnets

- Linux user and sysadadmin
- Programmer
- Member of Dragon Sector CTF team ☺

CERT.PL

Introduction

CERT.PL

So, you want fight botnets ?

Botnet lifecycle:

1. write/buy malware
2. write/buy exploit pack
3. buy/hack VPS/hosting for (1) and (2)
4. buy domain for (3)
5. spred malware using exploit pack
6. $ profit $

CERT.PL

So, you want fight botnets ?

Life of security researcher:

1. monitor spam/social media/internets
2. see malware spreding using exploit pack
3. gather samples
4. monitoring / analysis / incubation
5. locate CnC domains
6. locate rest of infrastructure
7. << action required ! >>

CERT.PL

Fighting botnets ...

Malware domain takedown:

+ cut off botmaster from his flock of sheep

- devices still infected, no one get noticed

Malware domain takeover:

+ cut off botmaster from his flock of sheep
+ malware will keep talking to CnC
+ can gather and share infrmation on infections!

→ make cyberspace better place

CERT.PL

Sinkholing

CERT.PL

Sinkholing ?

Sinkholing – let me google it for you ...

Sinkholing is a technique that researchers use to redirect the identification of the malicious command-and-control (C&C) server to their own analysis server. This way, the malicious traffic that comes from each client goes straight to the research box, ready to be analyzed.

source: the internet

CERT.PL

Sinkholing

Scope : global

- **Take over CnC domain**
  - Point to researcher box (directly or by nameserver)
  - Doable
  - Need to provide evidence
  - Good will from domain operator (TLD)
- **Take over CnC IP :**
  - Hard to do - need persuade IP owner (ISP/Hosting)
- **Take over CnC infrastructure (server)**
  - Physicaly takeover
  - Often can be done only by law enforcements

CERT.PL

Sinkholing

Scope : global

- **Take over CnC domain**
  - Point to researcher box (directly or by nameserver)
  - Doable
  - Need to provide evidence
  - Good will from domain operator (TLD)
- **Take over CnC IP :**
  - Hard to do - need persuade IP owner (ISP/Hosting)
- **Take over CnC infrastructure (server)**
  - Physicaly takeover
  - Often can be done only by law enforcements

a lot of legislation problems

CERT.PL

Sinkholing

„Local” sinkholing (LAN) - redirect CnC traffic:

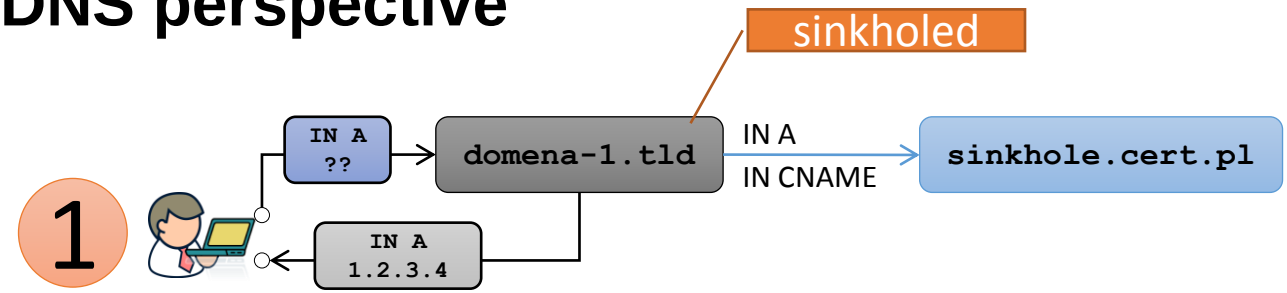
- By DNS : local DNS redirection
- By destination IP: traffic redirection

- Provide usefull information on infected workstations
  - Especially when you run multi-layered big internal company network ☺

source: the internet

Sinkholing

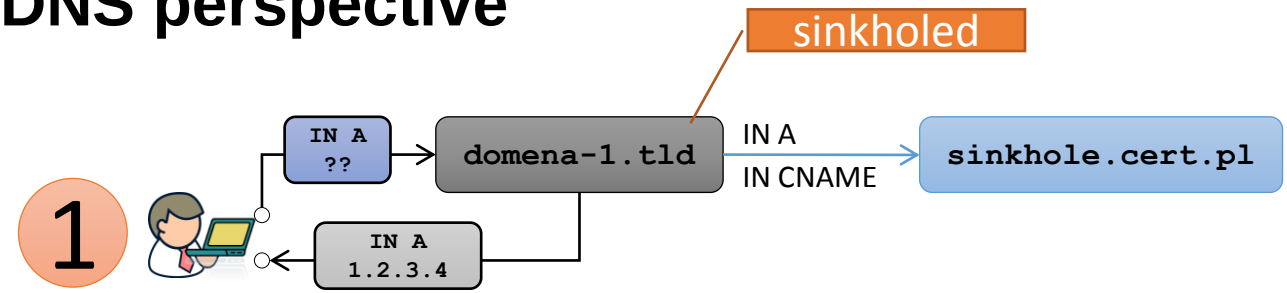
DNS perspective

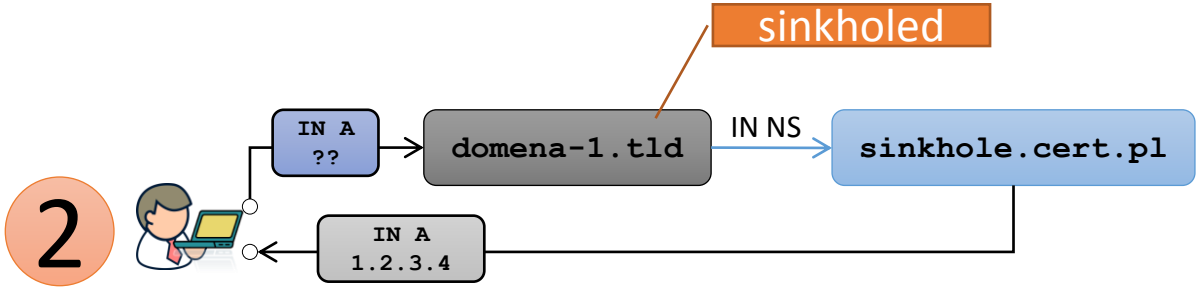


CERT.PL

Sinkholing

DNS perspective

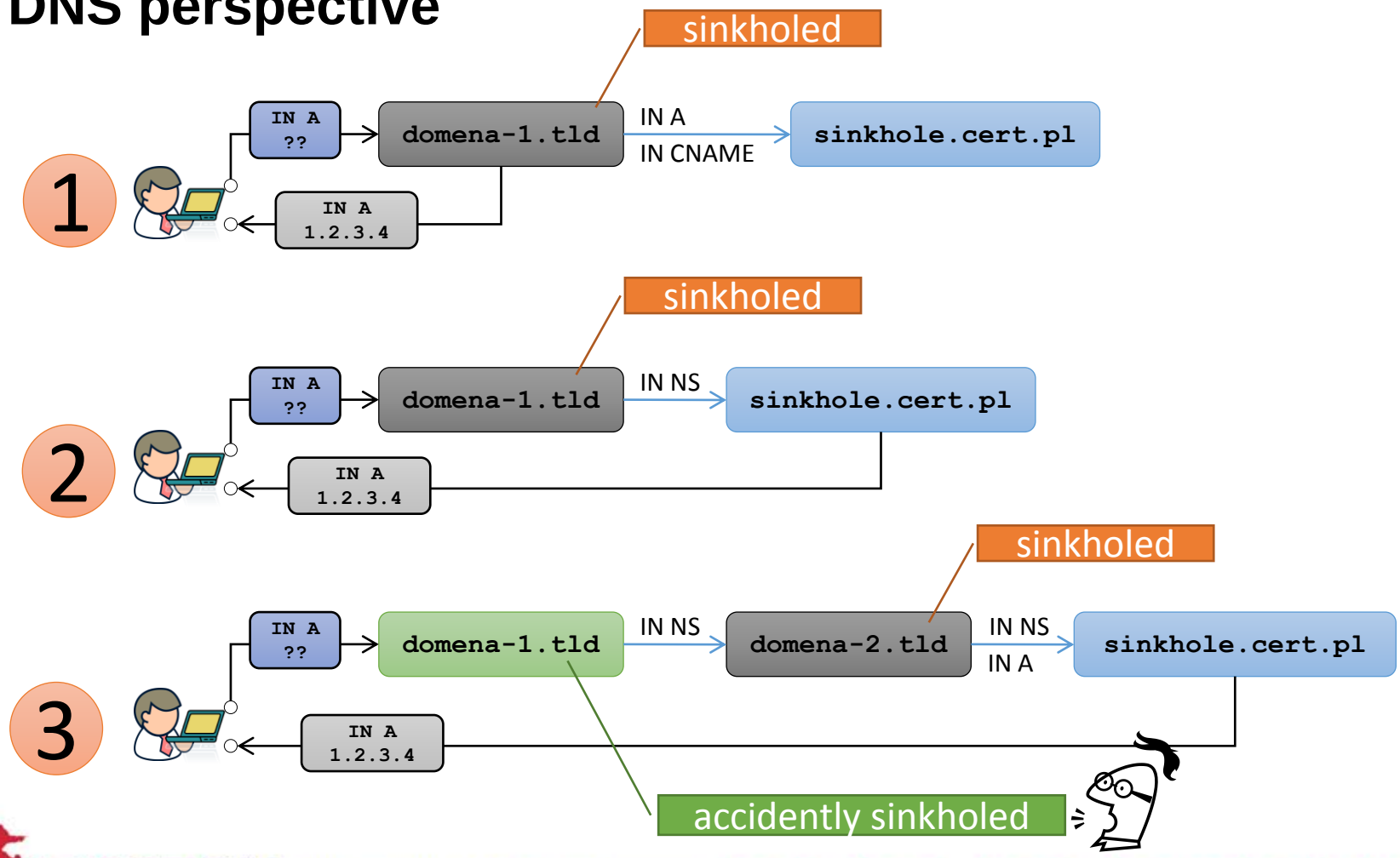




CERT.PL

Sinkholing

DNS perspective



CERT.PL

Sinkholing

„the goal”

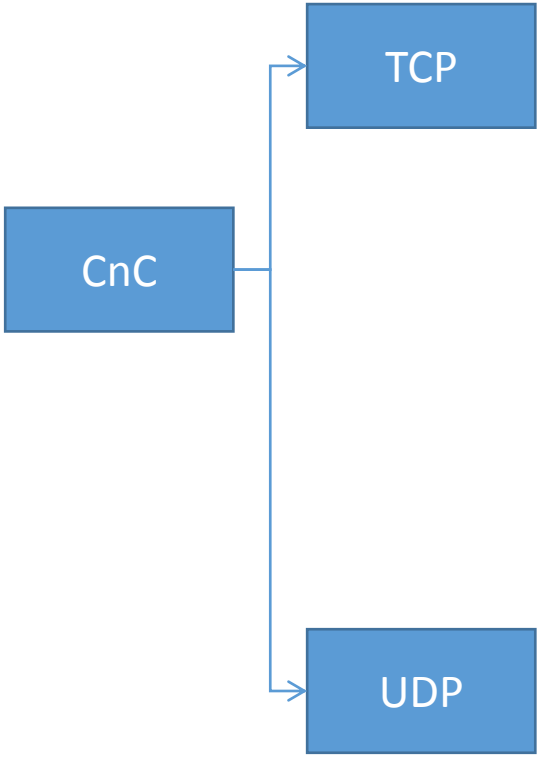
- Allow malware to connect to your box
- Keep malware connected to your sinkhole as long as possible
- Prevent malware from using alternative/bacup communication channels

CERT.PL

CnC

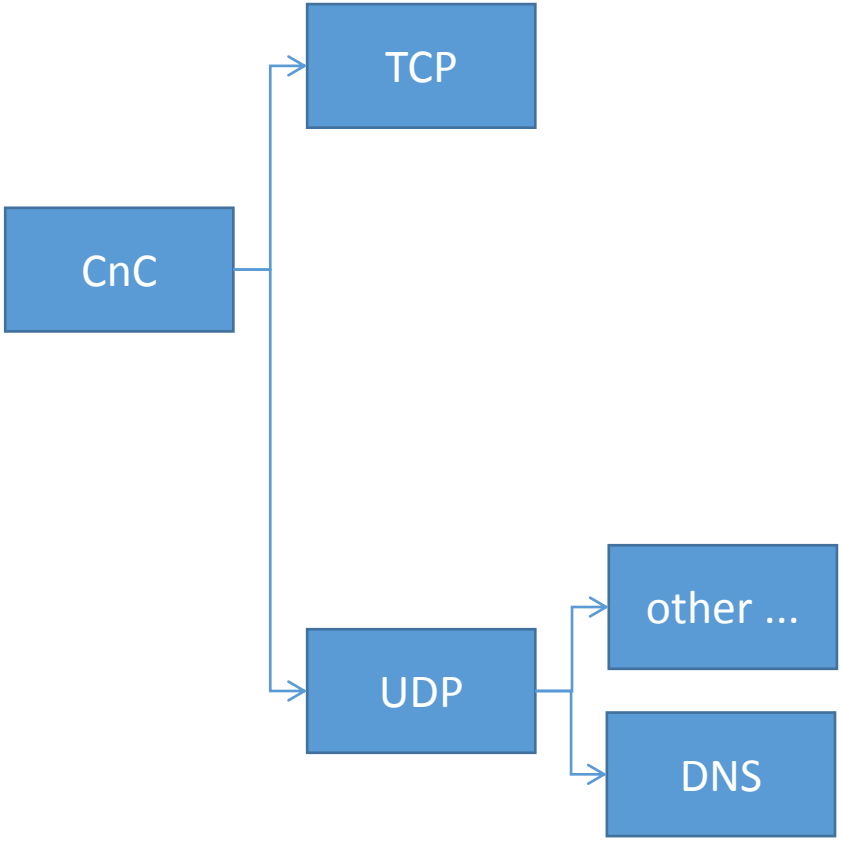
CERT.PL

CnC Types



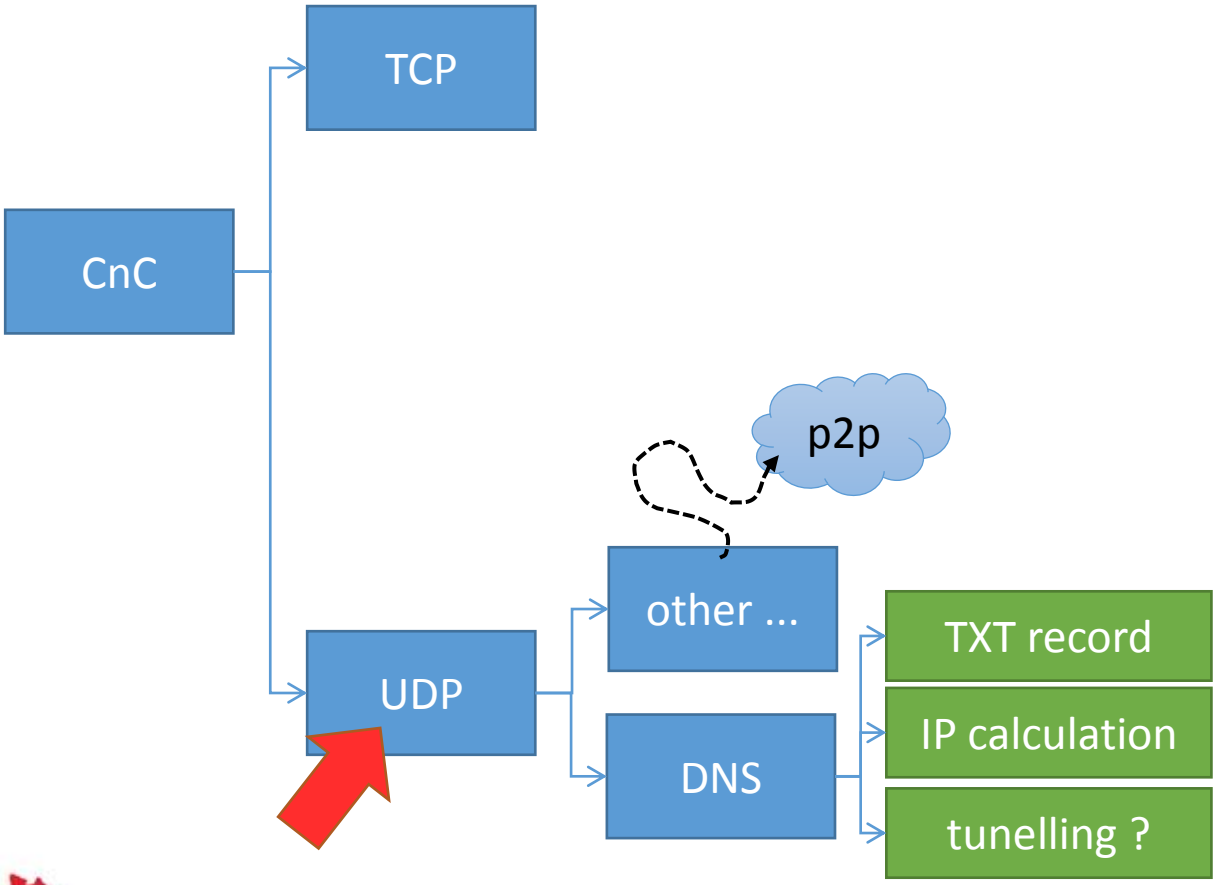
CERT.PL

CnC Types



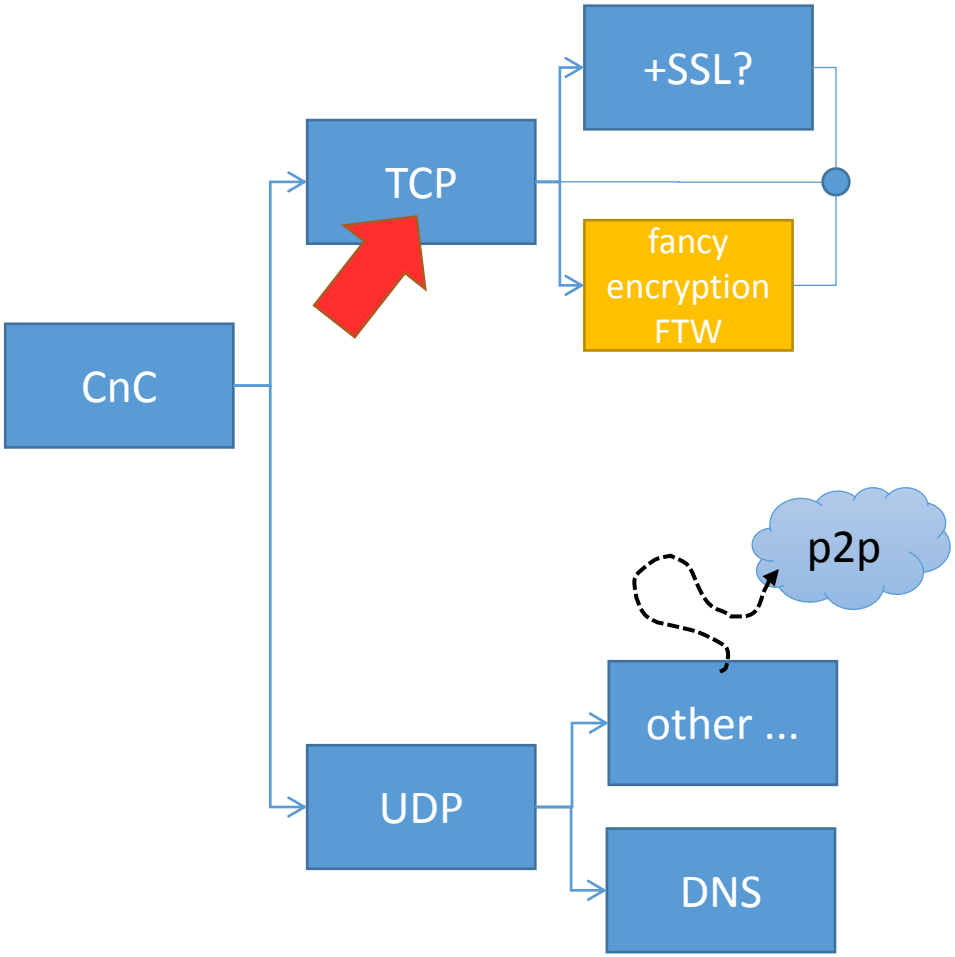
CERT.PL

CnC Types



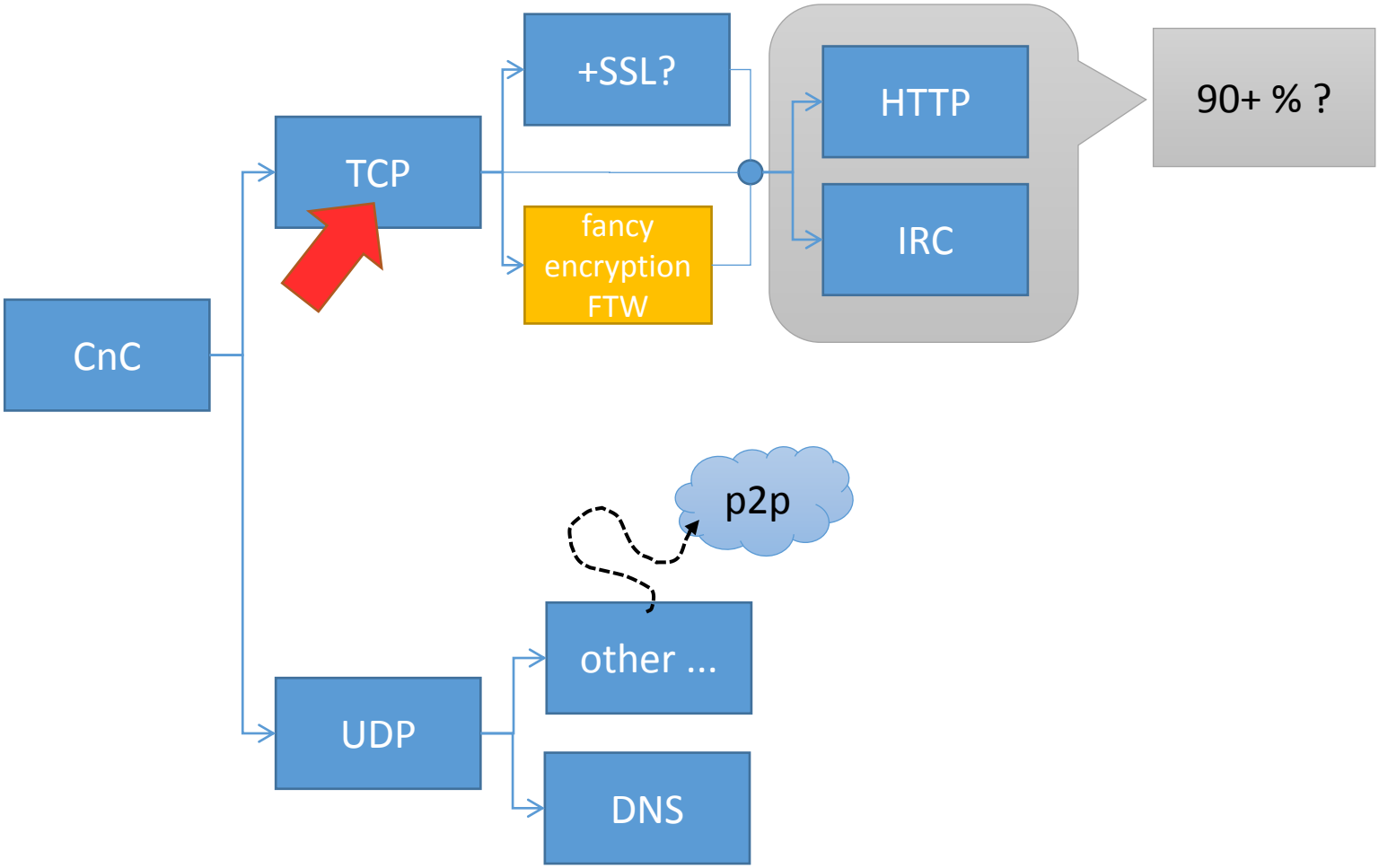
CERT.PL

CnC Types



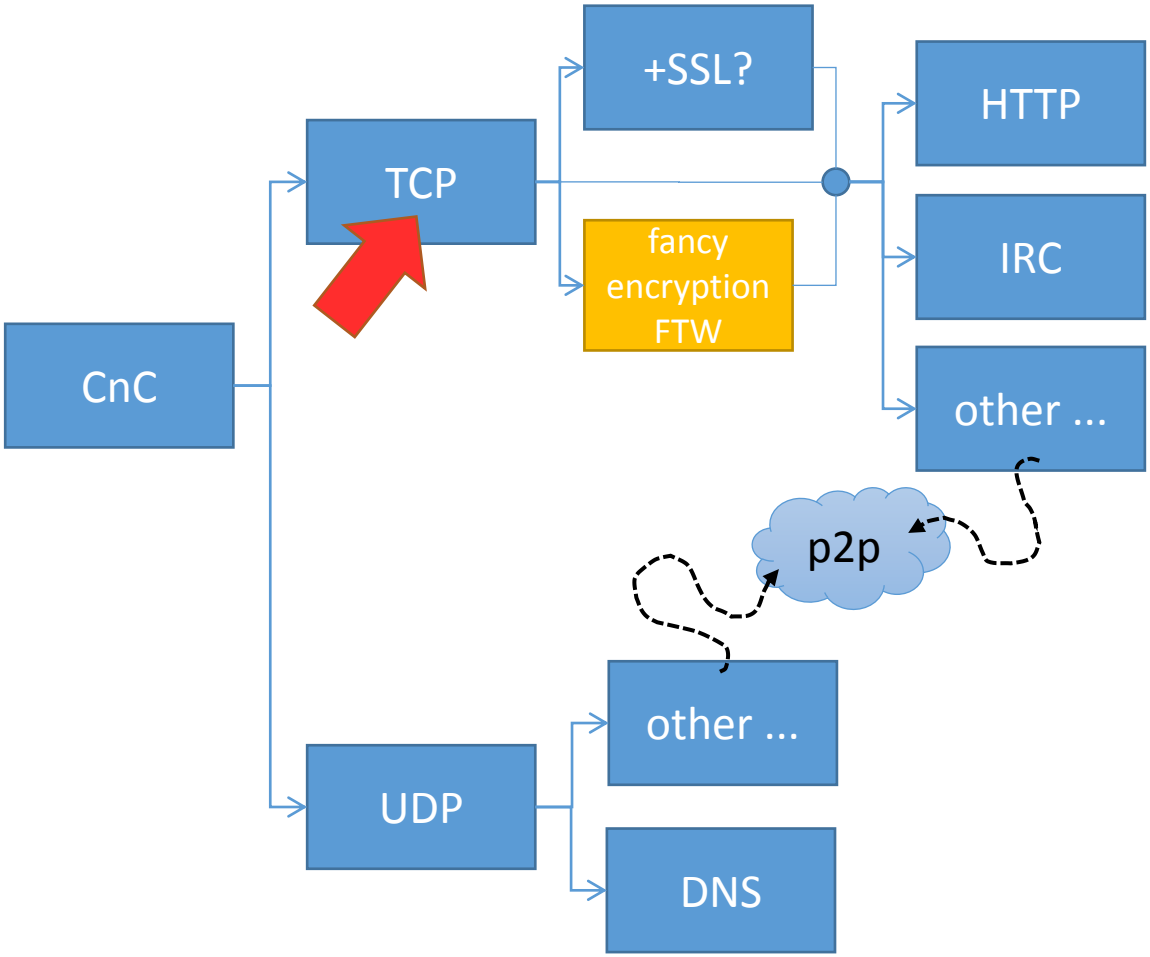
CERT.PL

CnC Types



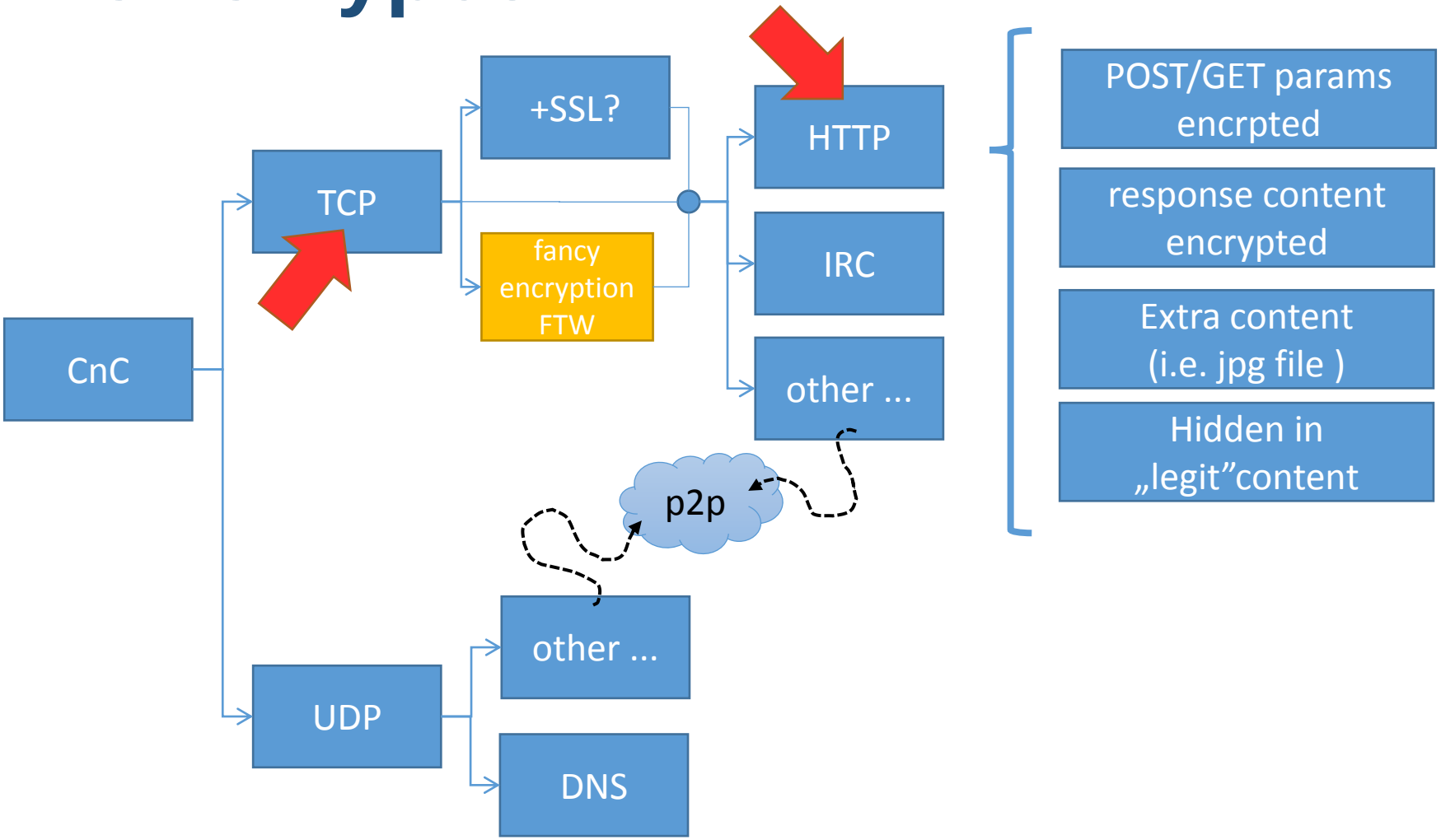
CERT.PL

CnC Types



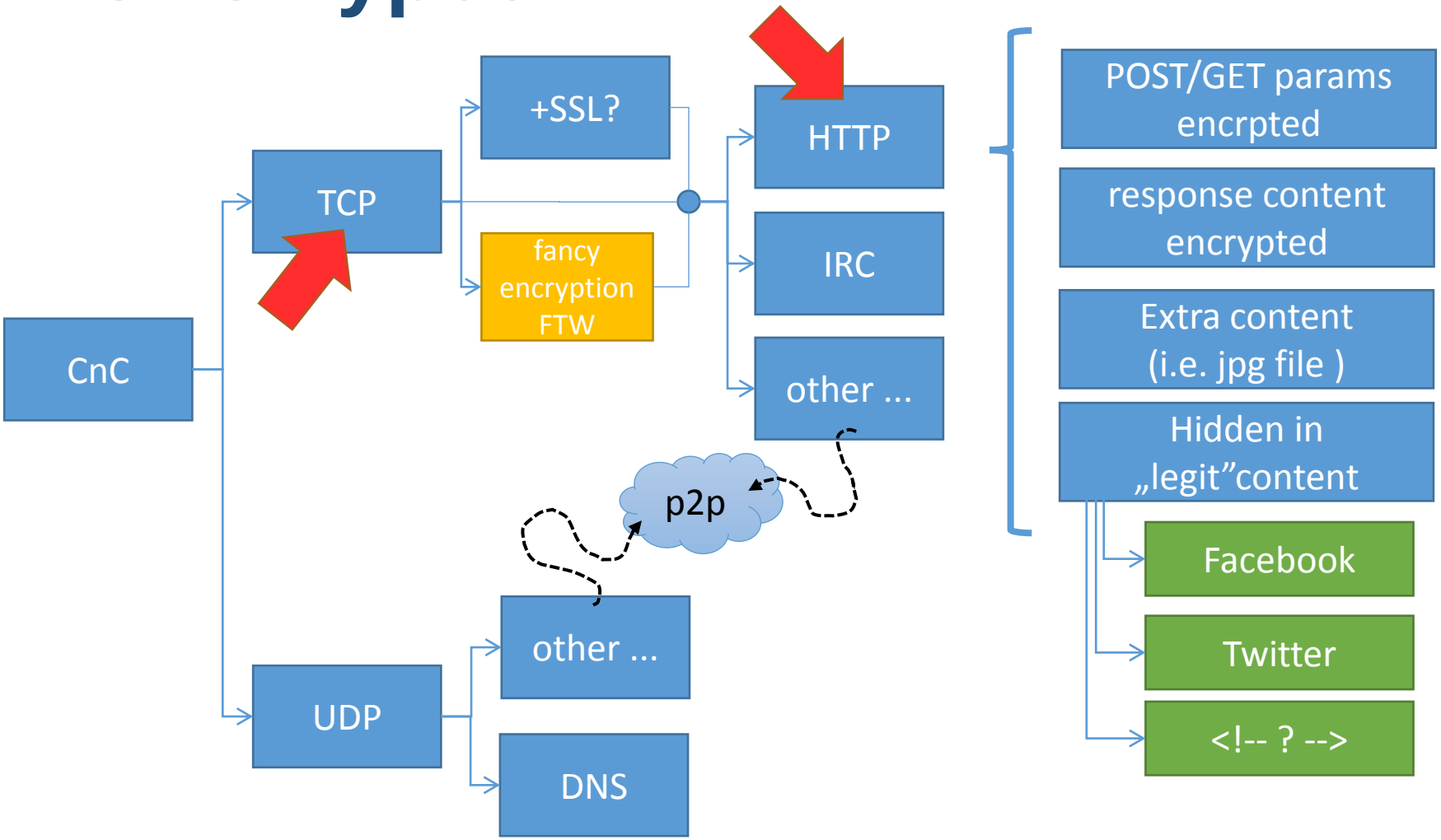
CERT.PL

CnC Types



CERT.PL

CnC Types



CERT.PL

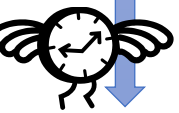
CERT .PL story (1)

CERT.PL

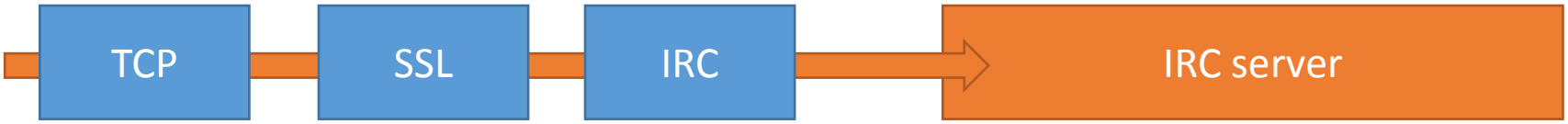
Timeline

end of 2012 – dorkbot

- Yet another malware using .pl domain as CnC
- Yet did not have TLD sinkhole procedure (in progres)
- Registrar decided to help (after abuse report)
- Am... but we do not have sinkhole !?



CnC – example: Dorkbot



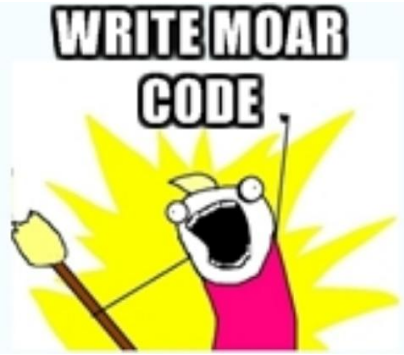
CERT.PL

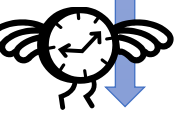
Timeline

end of 2012 – dorkbot

-> Take this old unused server and do somethink
(4 GB RAM, 2x 3.0 Ghz CPU, 160 GB HDD , decend 1U !)

-> We need TLS IRC
->Take charybdis irc server, remove 80 % functions





CERT.PL

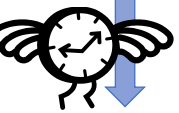
Timeline

end of 2012 – dorkbot

begin of 2013 – virut

- Realy long-living malware still sitting on .pl domains ☹

- TLD sinkhole procedure in progres
- Promising results from sinkholing dorkbot ☺
- Decistion : we need to do this !



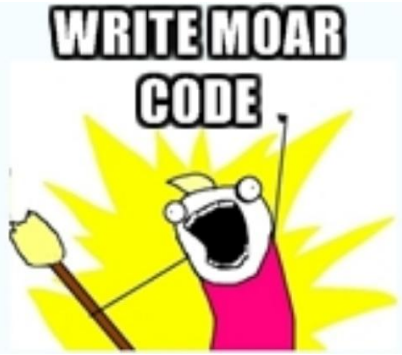
CERT.PL

Timeline

end of 2012 – dorkbot

begin of 2013 – virut

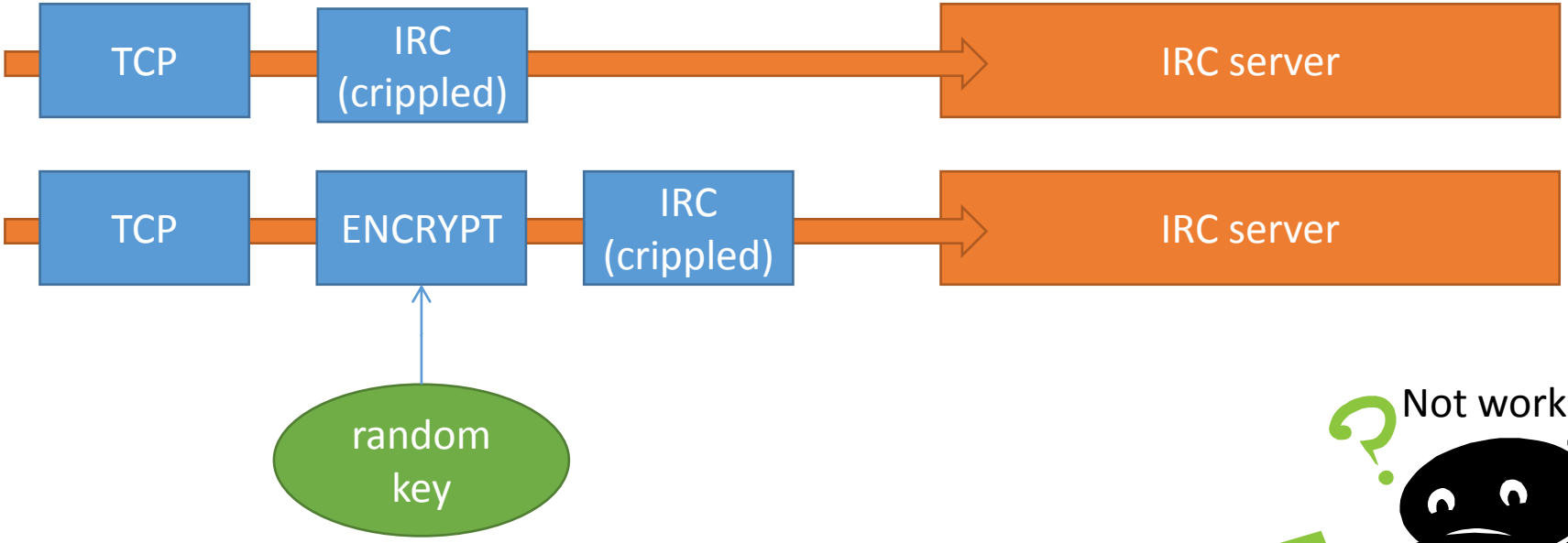
- We already got hadrware (+)
- We need (a lot) more software



CERT.PL

CnC – example: Virut

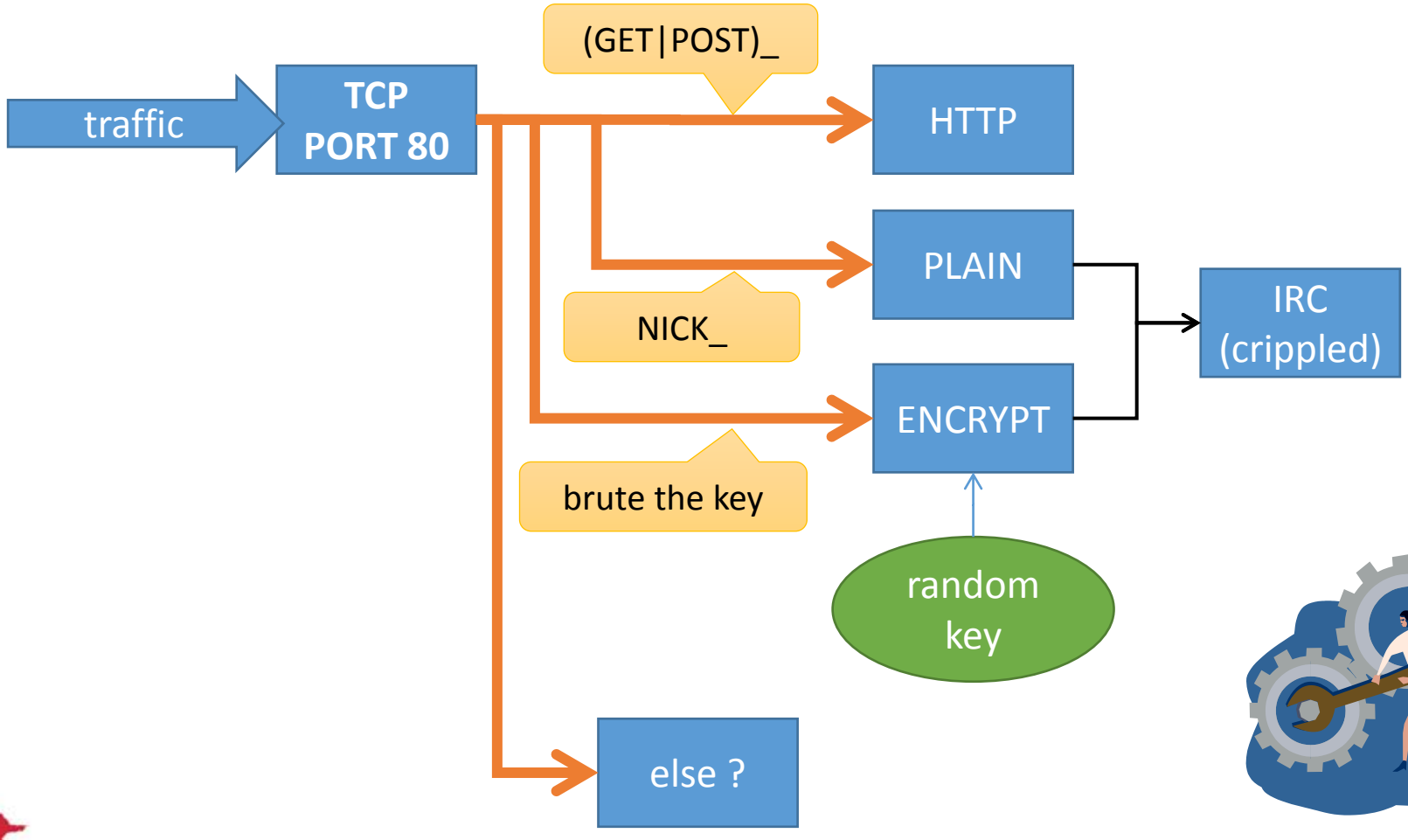
(expectations)



CERT.PL

CnC – example: Virut - reality

(reality)



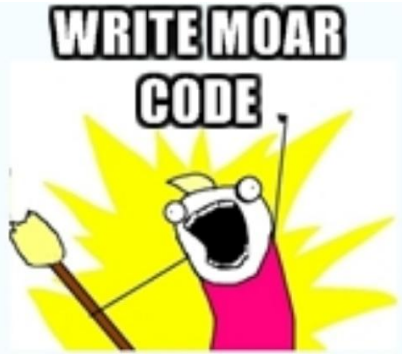
CERT.PL

Timeline

end of 2012 – dorkbot

begin of 2013 – virut

- Write python script
  - peek first 5 bytes (decision: irc/http/crypted)
  - keep TCP connection as long as possible



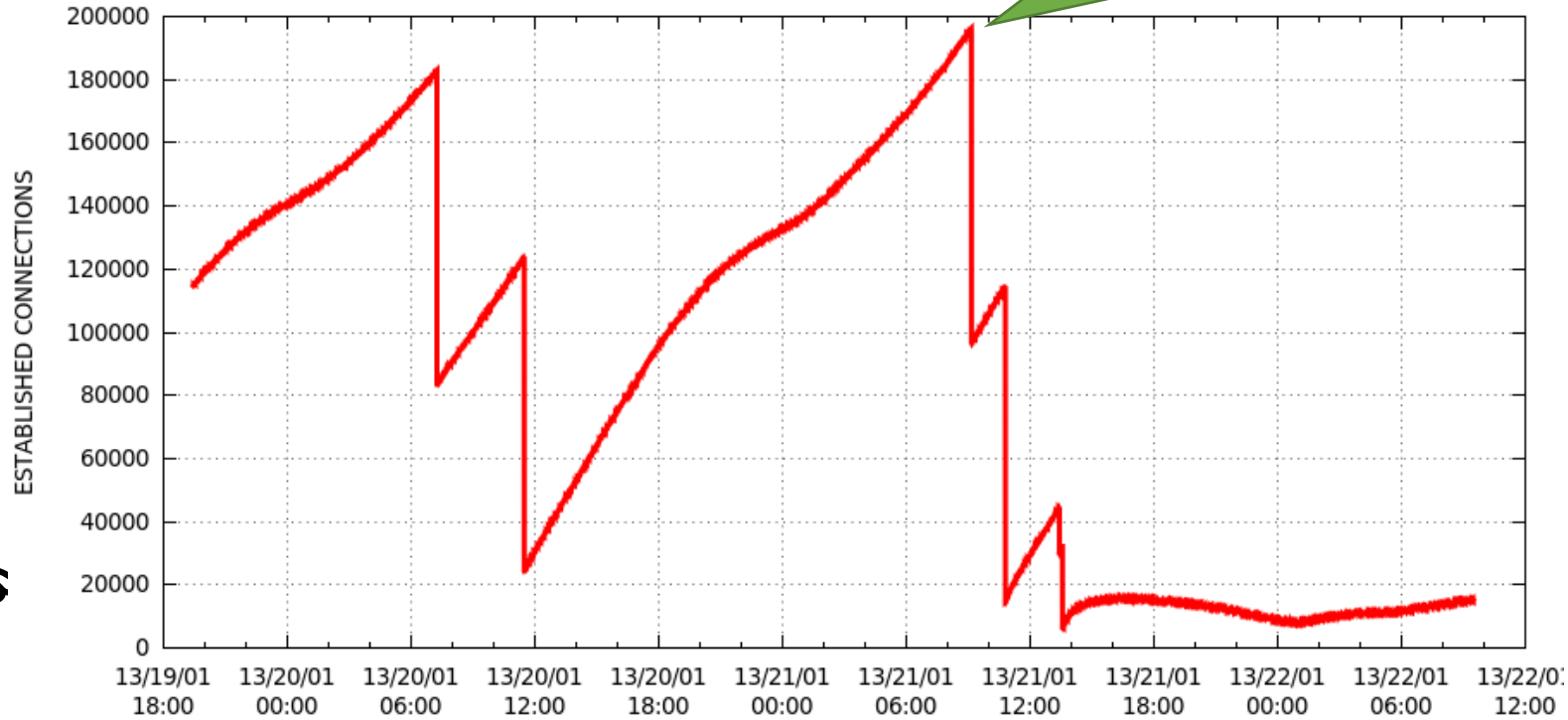
CERT.PL

Timeline

end of 2012 – dorkbot

begin of 2013 – virut

200 K connections in „established" state !?



CERT.PL

Timeline

Encountered problems: TCP timeouts

- close timeout = 10s
- close-wait timeout = 60s
- established timeout = 5 days
- fin-wait timeout = 120s
- last-ack timeout = 30s
- syn-received timeout = 60s
- syn-sent timeout = 120s
- time-wait timeout = 120s

srsly ! it is just waiting for RST

CERT.PL

Timeline

Encountered problems: software

(you know them when you hit the limit ☹)

Somewhere in code you need to „select()" over opened file descriptors. It uses limited size bit-fields !

Hint: on Linux use poll !

CERT.PL

Timeline

Encountered problems: default OS limits

(you know them when you hit the limit ☹)

- max opened file descriptors (each tcp connection=new FD)
  - ➢ can be easily fixed : **`ulimit -n 999999`** ☺

- max entries in contract table
  - ➢ requires kernel param tweak, fixable ☺

CERT.PL

Timeline

Conclusion (1)

Establishing TCP connection and leaving it with default settins is <u>bad idea</u> !

Use SO_KEEPALIVE socet option ☺ (obvious ?)

CERT.PL

Timeline

Conclusion (2)

~~**SELECT()**~~

POLL()

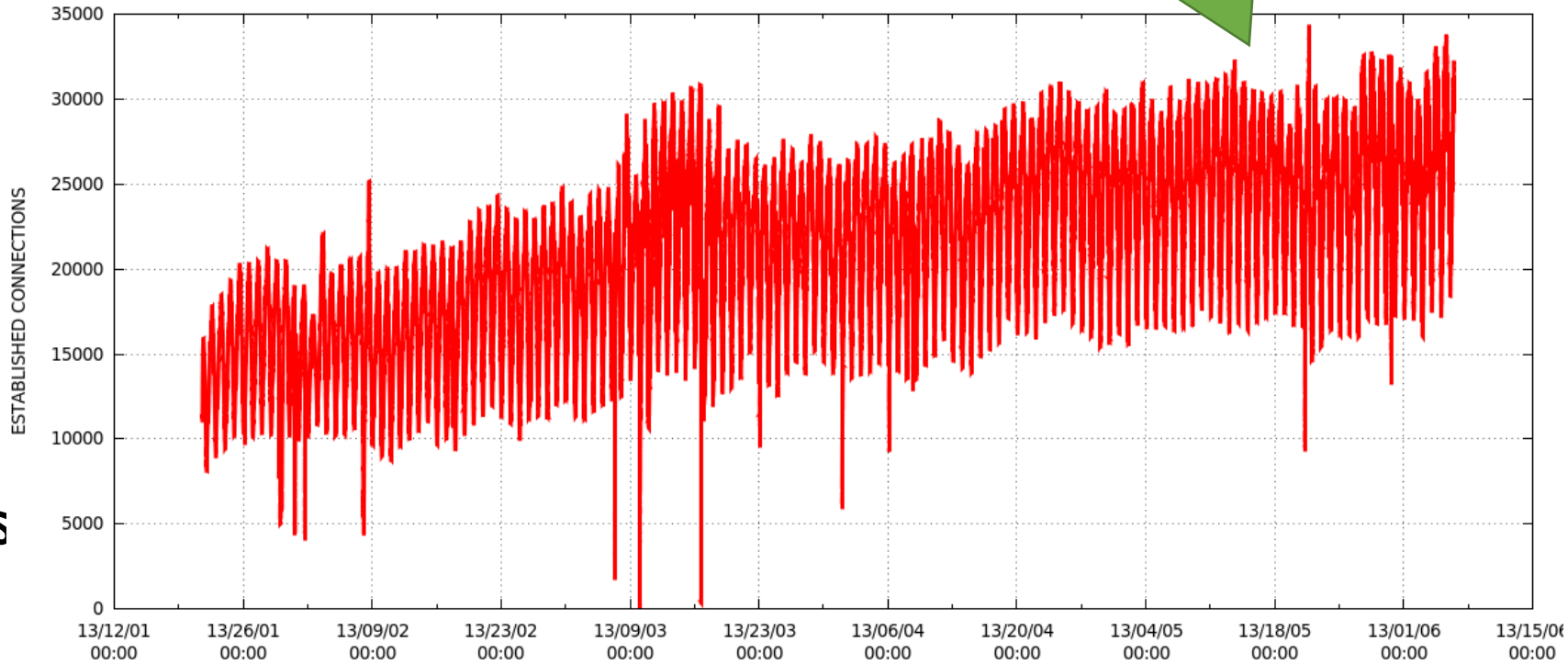
CERT.PL

Timeline

end of 2012 – dorkbot

begin of 2013 – virut

30K simultanious connections ☺



CERT.PL

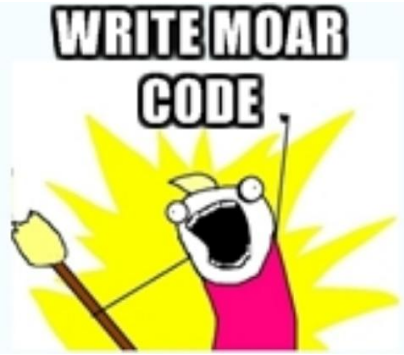
Timeline

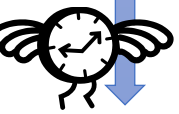
end of 2012 – dorkbot

begin of 2013 – virut

spring 2013 – few ZueS domains

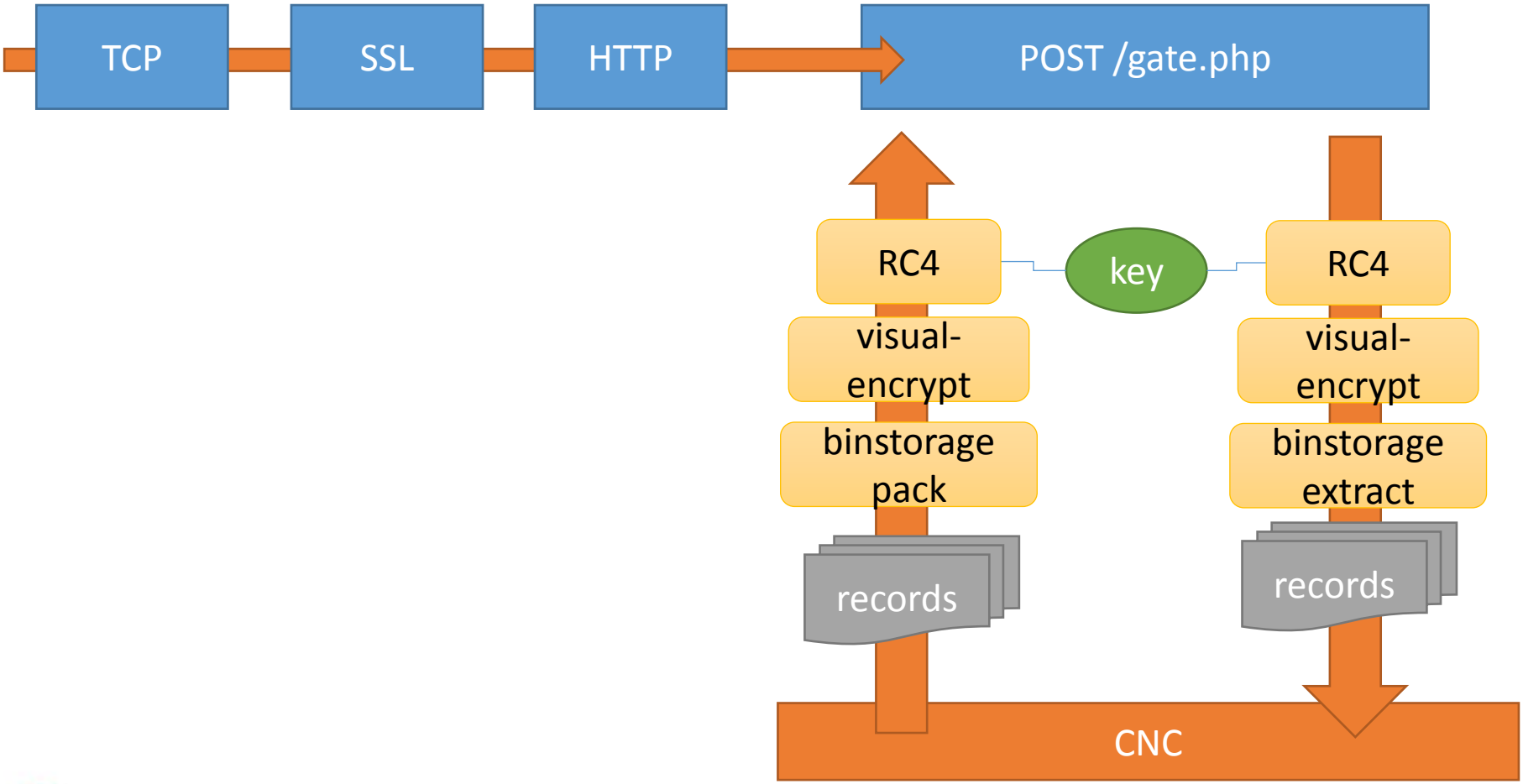
- Write python script that will understand HTTP and decode incoming zeus data ...





CERT.PL

CnC – example: ZeuS



CERT.PL

Timeline

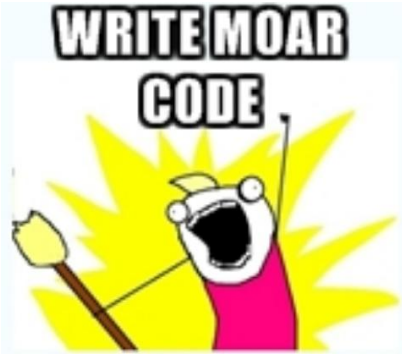
end of 2012 – dorkbot

begin of 2013 – virut

spring 2013 – few ZueS domains

summer 2013 – domainsilver takedown

- A LOT of various malware domains
- Write python scripts .... ?



CERT.PL

Timeline

Encountered problems:

we already got numerous different python scripts running different CnC

CERT.PL

Timeline

Conclusion (3)

Need decent sinkhole software ☺

(obvious ?)

CERT.PL

CERT.PL
sink-soft ☺

CERT.PL

Requirements

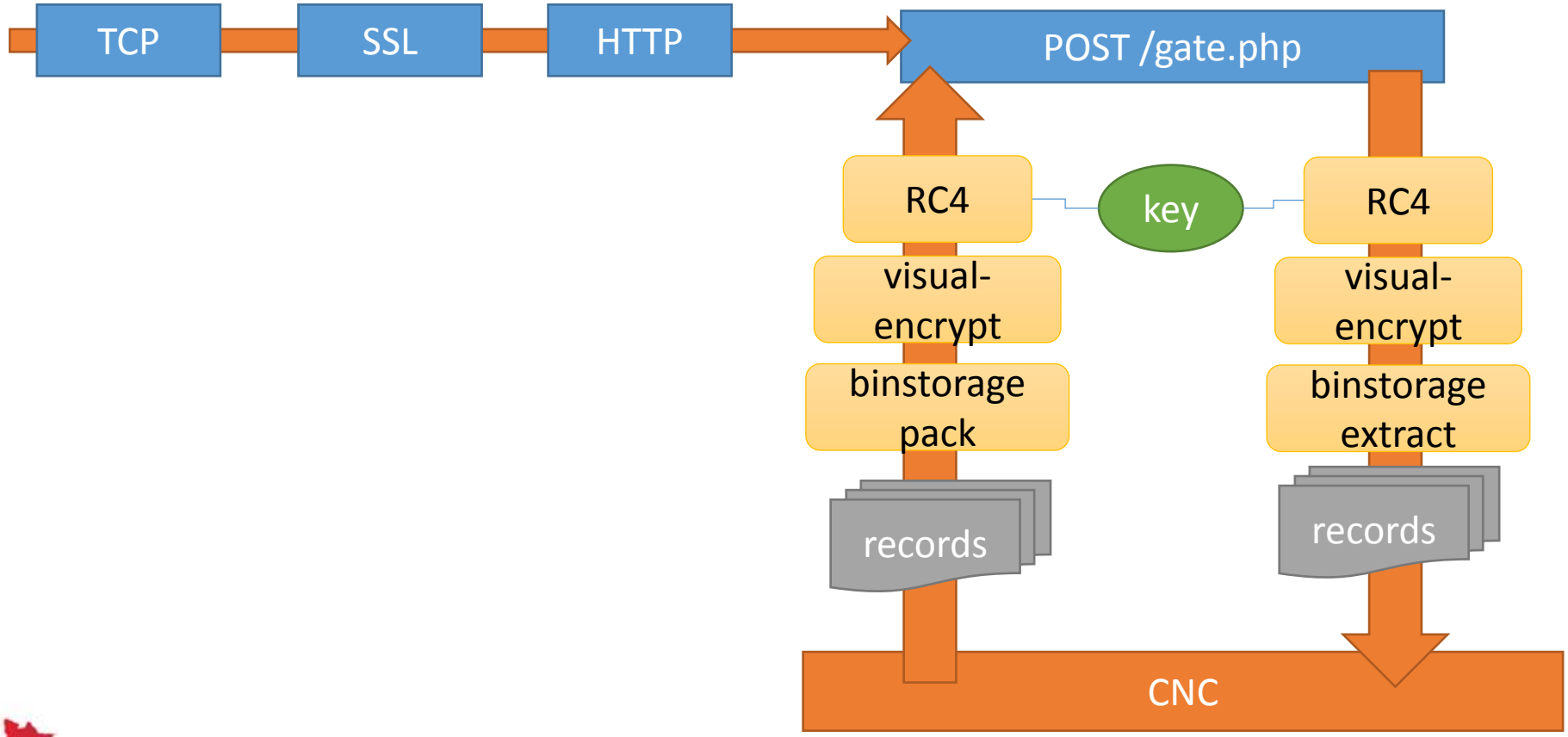
- Build consistent framework for sinkholing
- Make event logging/sharing easy
- Identify common content processing functions
- Handle undret of TCP connections from
- Be as elastic as possible
- Implement any fancy encryption/encoding anywhere

Allow to sinkhole new malware with lowest possible effort

CERT.PL

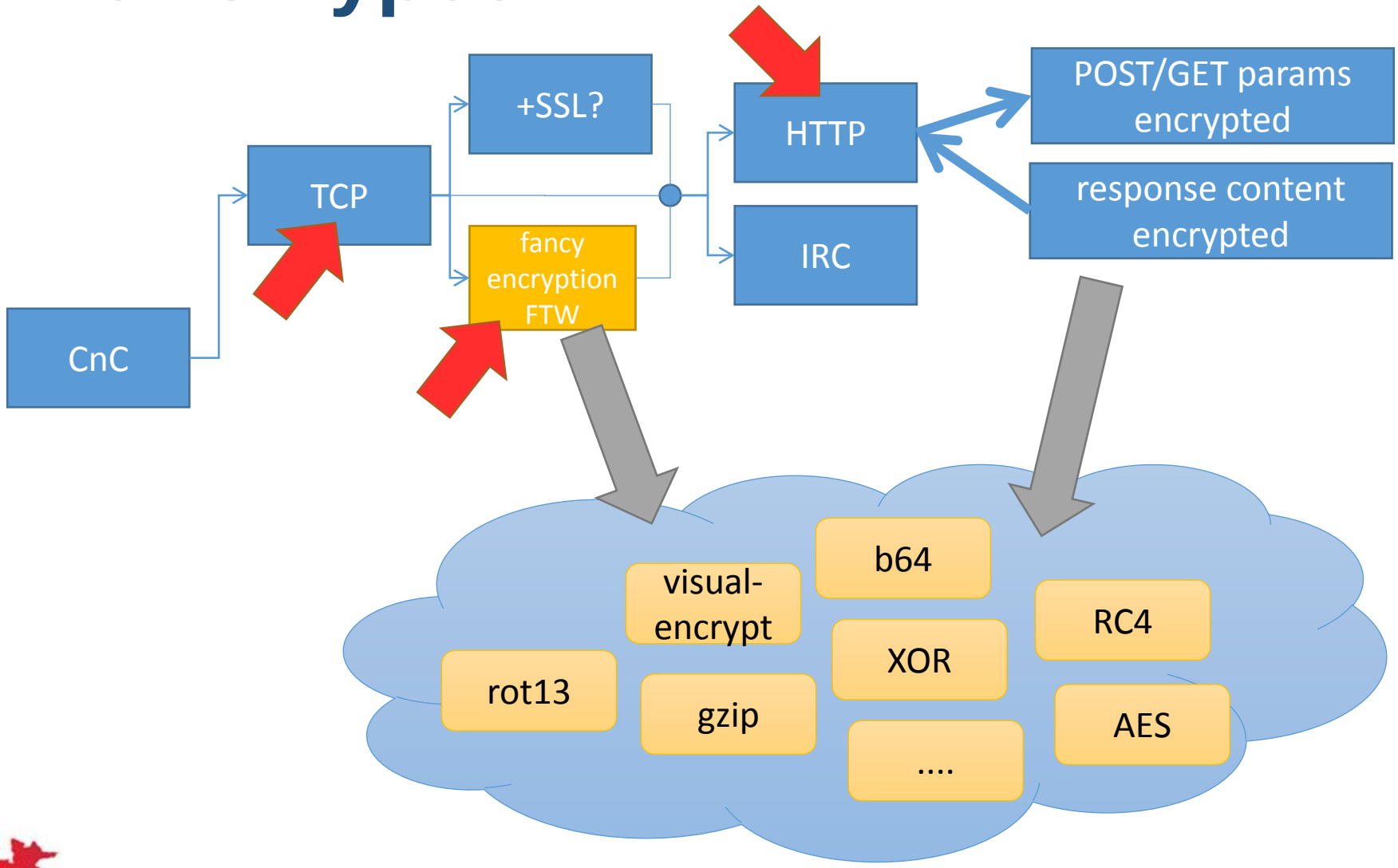
Design

Build your sinkhole out of blocks (modules) ☺



CERT.PL

CnC Types



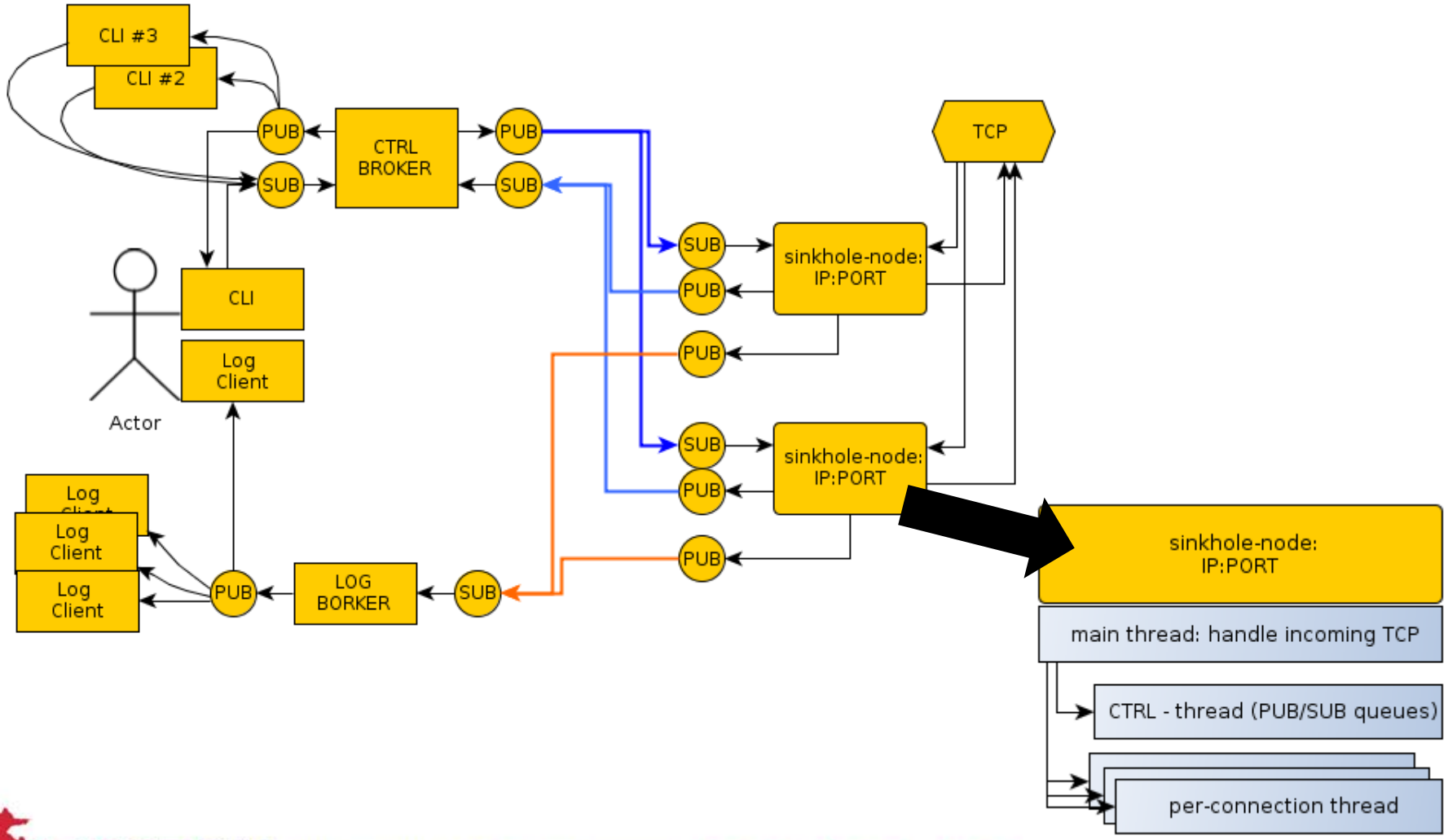
CERT.PL

Design

- Provide TCP conevtivity layer
- Use MQ – ZeroMQ (fast && simple)
- PUB-SUB messaging pattern
- Deployed as standalone package with lowest possible requirements (msgpack && zmq-python)
- Easy configuration (chose ip,port and modules chain)
- unpack & config & run

CERT.PL

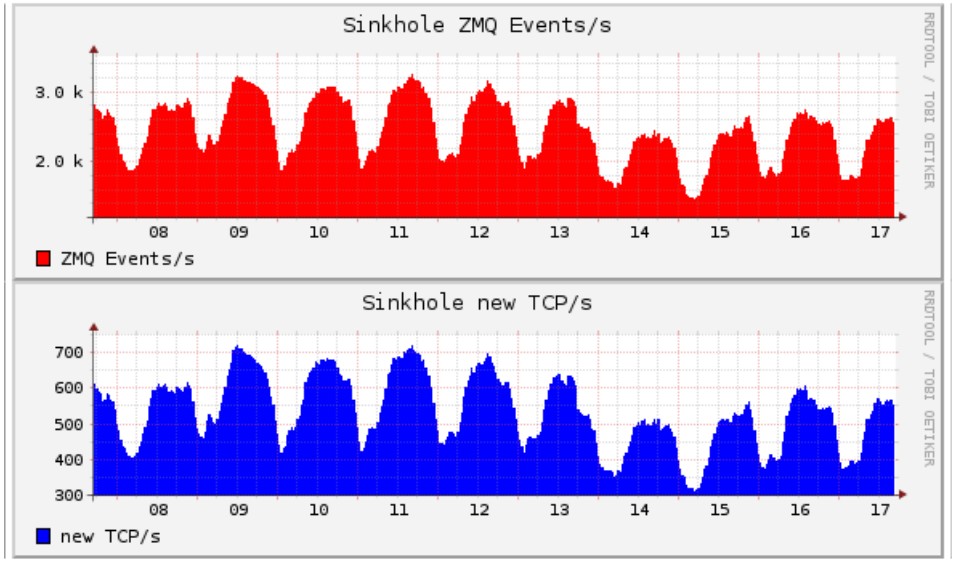
Design

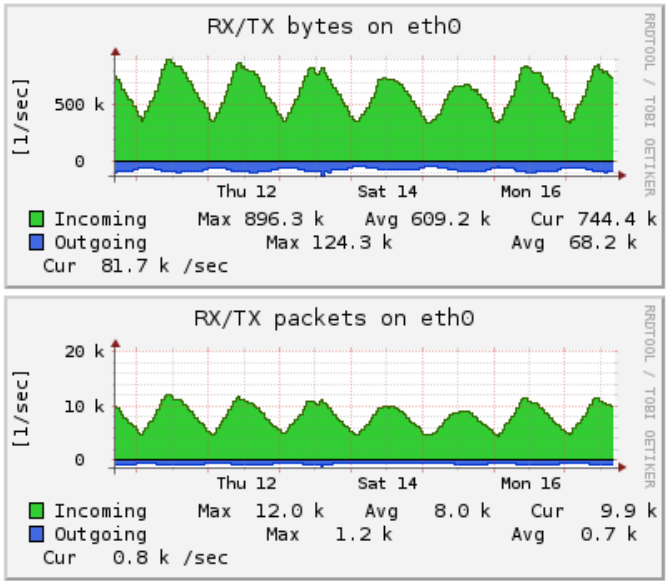


CERT.PL

Sink-soft

Sinkholing > 200 active malware domains






```
root@sinkhole:~# w
 14:20:38 up 561 days, 19:05,  4 users,  load average: 0.00, 0.00, 0.00
```

CERT.PL

Sink-soft

demo :)

Fin.

Tomasz Bukowski

tomasz.bukowski@cert.pl