Fighting malware during DNS resolution

Robert Šefr (CTO, Whalebone)

whalebone

Whalebone traffic visibility

- DNS traffic “only”
- 100k of households
- Czech Republic and Slovakia (few computers in Austria)
- Representative sample (all kinds of users)

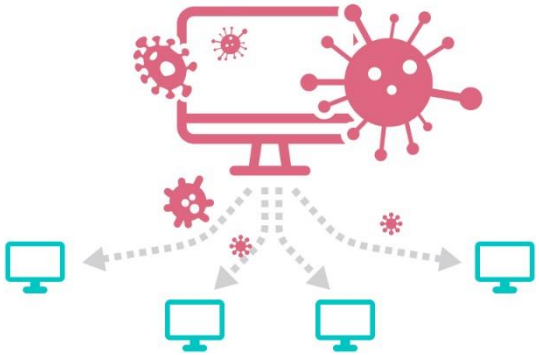
The story, all domains, malware, and incidents portrayed in this production are **real**. Identification with actual malware (living or deceased) is intended and should be inferred. No animals were harmed in the making of this presentation.

Malware lifecycle

Infection 1

C&C 2

Malware activity 3



1. Infection

whalebone

Infection vectors

- Web
  - Exploit kit (Drive-by Download)
  - Conscious download of malicious software
- Email
  - Binary or scripted downloaders
- Remote exploits
  - Payload downloaded from external source

What do these domains have in common?

0668.com
administrategia.com
adsnight.com
atriym-stroy.ru
aurea-art.ru
auwm.ru
babyparka.ca
basarteks.com
bobtheprinter.com
btkdevelopment.ru
canstore.ca
cmt.ro
codezigns.com
cpugame.com
dbatee.gr
decoracionbebes.com
delreywindows.com
dfl210.ru
dienmayhonghung.com
dnp9.com
dowfrecap.net
dulich.me
environment.ae
expert-as.ru
fashioncheer.com
flexdeal.net
frembud.pl
gadget24.ro
gebrauchtkauf.at
gigabothosting.com
hrbqcc.com
ichinoyado.com
ict-net.com
ijiyo.com
infomazza.com
ingesof.com
innoservtest.in
ist-profy.ru
kayju.com
kvnysoho.com
masterimob.ro
mk-4.ru
mvco.de
nerfetyv.org
orthanna.com
p-g-a.org
polgraf.eu
pornovizion.com
pwmsteel.com
rdsc-seminar.com
relive-clean.ru
satherm.pt
satyagroups.in
senabel.com
sendat.vn
silverhand.eu
spazioireos.it
statikwerk.de
stav-reporter.ru
system-inka.de
terrabit.ro
theamericanwake.com
thetravelbug.org

Locky ransomware distribution sites statistics

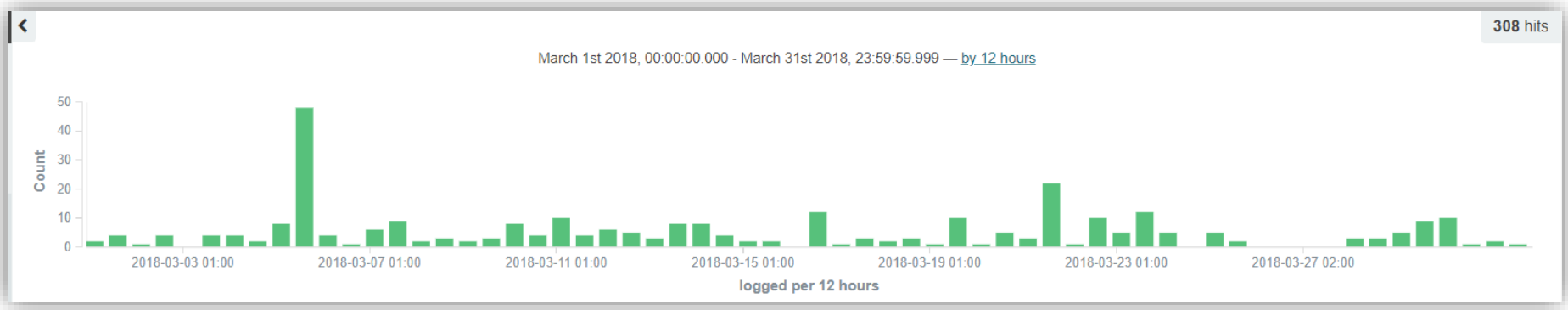
- March 2018
- Access to distribution sites (infection phase)

308

Unique incidents in DNS traffic

83 IPs

Tried to download Locky ransomware



Coin Miner - noblock.pro

- Hosting ApplicUnwnt.JS/CoinMiner.F
- JavaScript misusing the computational power of the machine to mine cryptocurrency for the attacker

6,5% IPs

Targeted with this attack during Q1 2018

Mikrotik oriented malware

- **VPNFilter**
- Overlap with BlackEnergy
- Probably aiming Ukraine

`toknowall.com`

2 IPs

Seen in June 2018

- **Luabot variant**
- Deployed through 0-day exploit
- Downloads payload from following domains

`marchdom4.com`
`march10dom5.com`

1 IP

Seen in June 2018

2. Command & Control

whalebone

Locky C&C servers

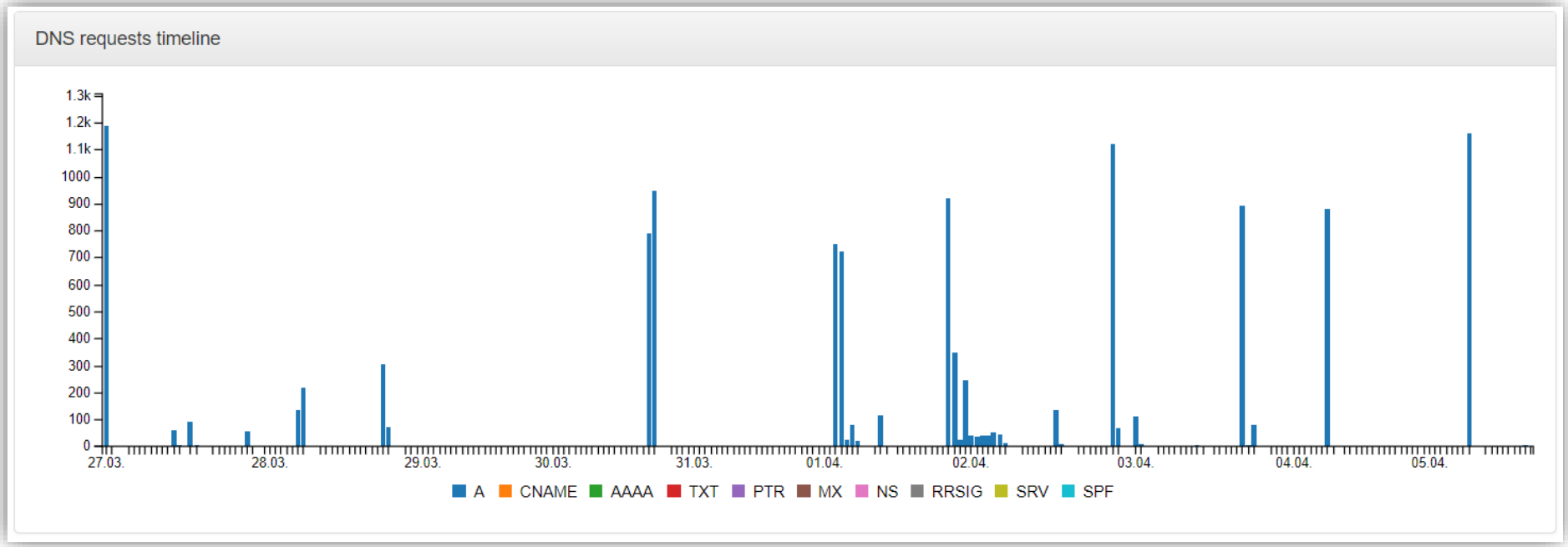
- Legitimate looking ones (“legitimate”)

  `pornohd24.com`

- Domain Generation Algorithm

  `rbwubtpsyokqn.info`
  `qvdgqayo.pw`
  `qsbfwgtedexirbyoq.pw`
  `qlwnvdjwro.pw`
  `qfuxosx.eu`
  `qdesslfdcmd.pw`
  `qdvkdyvrtpjc.pw`
  `qcwbrevxrotoepsp.pw`
  `qbqrfyeqqvcvv.pw`
  `pvwinlrmwvccuo.eu`
  `preeqlultgfifg.pw`

Necurs – Domain Generation Algorithm



23 IPs

In 2018 infected with Necurs and trying DGA

```
netbwdeyuxswfpdels.pw
qabilhpihvesr.com
egcsmclqwabbua.com
abnnmxfqohvsybo.la
sibtlsbcjecvapgfw.pw
unxojswfkobafrohbg.net
crdbvabhxucgbiuufsy.pw
ptuoauttnujdwfbp.net
```

Trojan OSX "Flashback"

- MacOS trojan
- Mostly active in 2012
- There is a **single** last instance in the sample at the moment

```
hzxwhzifyjewe.com
juifltdlpjjva.com
cdgssacqafewut.com
lwpuwdovuvpgtf.com
peclecgpwygqda.com
dppqqdmahihaly.com
rjuhnumyhderuy.com
moakzphcyysqst.com
pcjvhrwvrielyu.com
ofeogazqbxmqft.com
euxjnhxehfpeuy.com
rgerldgchahvj.info
qfywnsimhpxbkdx.kz
tgnqheyqmfogmgt.in
ocpyyfcaytqnpnw.info
```

Cosiloon – Android malware

- Discovered May 2018 by Avast
- Preinstalled on Android devices mainly from following manufacturers
  - ZTE
  - Archos
  - myPhone
- Aggressive advertsisement (adware)

59 infected IPs

Seen in May and June 2018

CCleaner infection

- Described during Septemeber 2017
- Very good antivirus coverage since that time
- CCleaner automatic update removes the infection
- Despite all this mechanisms, there are still infected machines

3 IPs

Still running infected Ccleaner in June 2018

DGA in the DNS traffic

1,01% of IPs

DGA like resolution patterns

0,28% of all DNS requests

Identified as random

DGA false positives

- Usage of abbreviations, or even combination of abbreviations results in awkward domain names
- Usually schools, public organizations and regional associations

- Such false positives are rare and be taken care of by the historical context for the same host

csvnmnm.cz
vospaspsm.cz
zbkjmkcr.cz
zusjjrrozmitalptr.cz

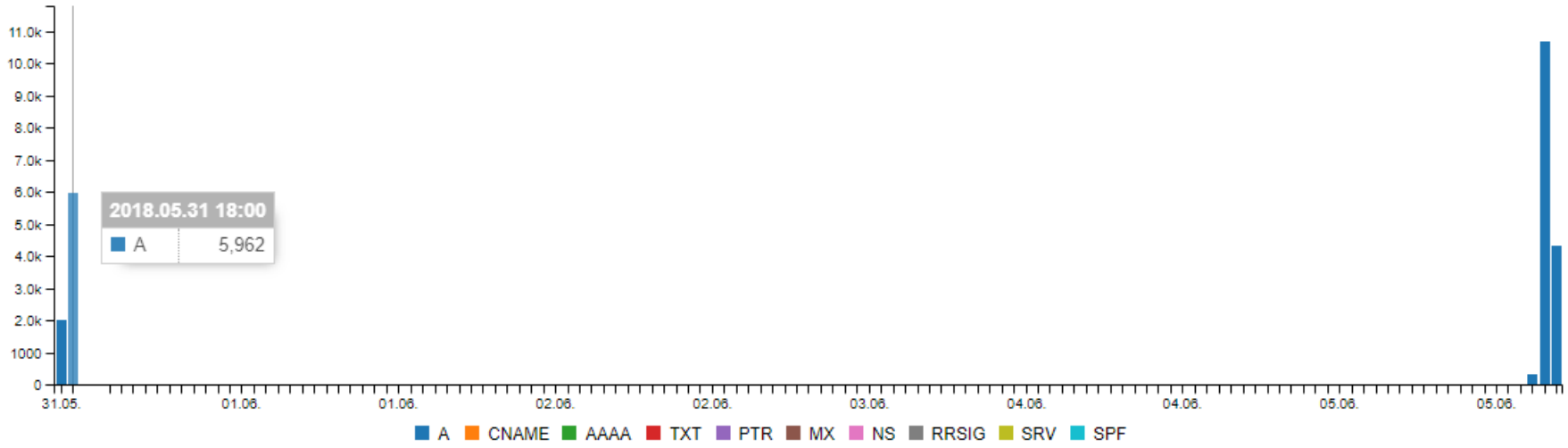
3. Malware activity

whalebone

Random Subdomain DDoS - SERVFAIL

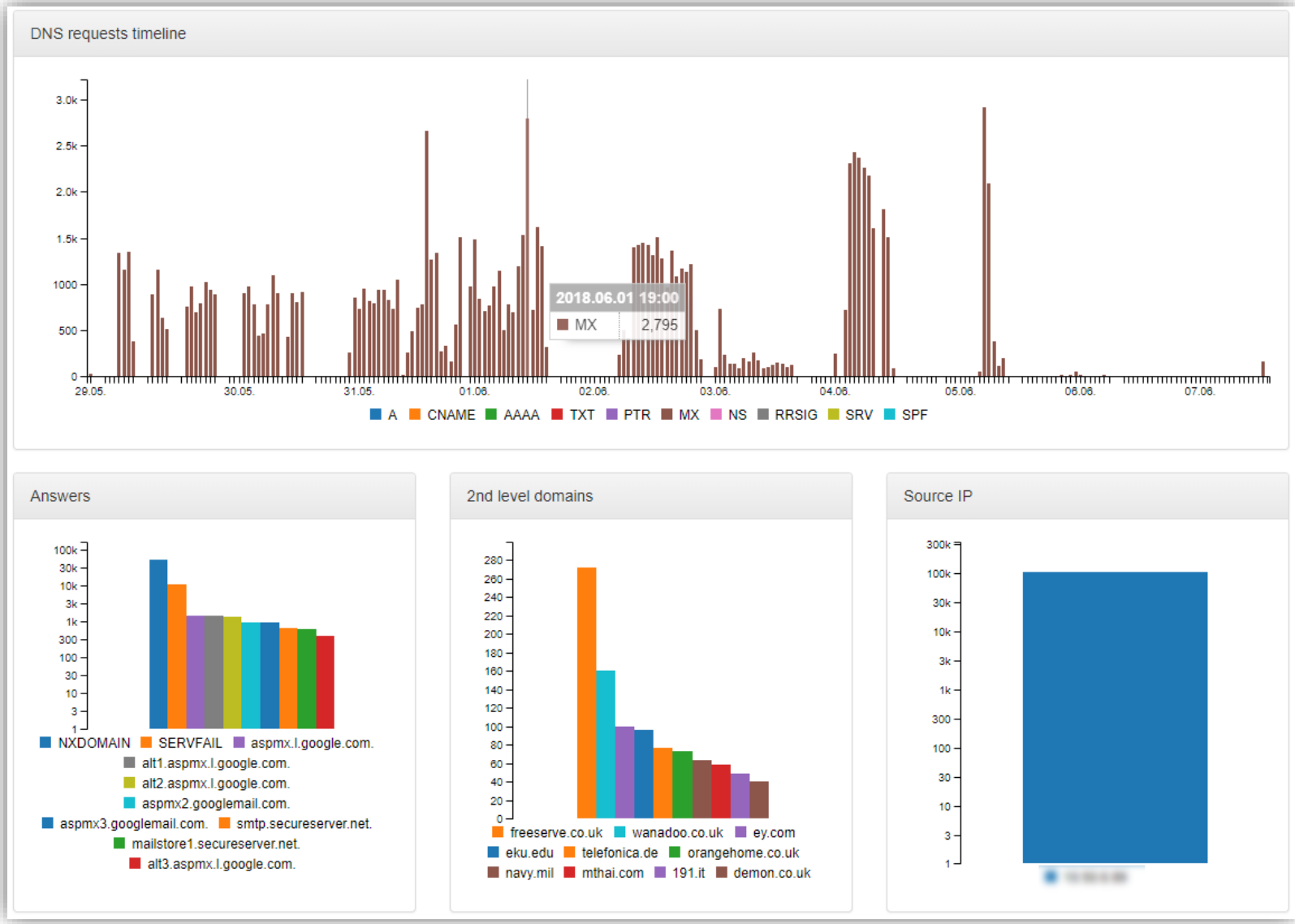
answer:SERVFAIL | dns_client_ip: [redacted] | domain:uber-help.ru

DNS requests timeline



Date	Request IP	Query type	Query	Level2 domain	Answer	TTL	Class
2018.06.05 21:36:44	[redacted]	A	xianggangsaimahuishiershengxiaobiao…	uber-help.ru	SERVFAIL	0	IN
2018.06.05 21:36:44	[redacted]	A	xinlijituan.uber-help.ru.	uber-help.ru	SERVFAIL	0	IN
2018.06.05 21:36:44	[redacted]	A	xianggangpaogoutu.uber-help.ru.	uber-help.ru	SERVFAIL	0	IN
2018.06.05 21:36:44	[redacted]	A	xianggangsaimahuishiershengxiaobiao…	uber-help.ru	SERVFAIL	0	IN
2018.06.05 21:36:44	[redacted]	A	xinlijituan.uber-help.ru.	uber-help.ru	SERVFAIL	0	IN
2018.06.05 21:36:44	[redacted]	A	xianggangpaogoutu.uber-help.ru.	uber-help.ru	SERVFAIL	0	IN
2018.06.05 21:36:43	[redacted]	A	xianggangcaipiaowangzhidaquan.uber-help…	uber-help.ru	SERVFAIL	0	IN
2018.06.05 21:36:43	[redacted]	A	xianshangjinpaiyulecheng.uber-help.ru.	uber-help.ru	SERVFAIL	0	IN

Observing spam through the MX queries



3. Summary

whalebone

Whalebone statistics – February 2018

19,95% 

Addresses with suspicious traffic

1,79% 

Addresses communicate with C&C

433 508 

Uníque incidents in DNS traffic

Filter online threats off your network

Robert Šefr, CTO
robert.sefr@whalebone.io
+420 608 737 930

https://whalebone.io

whalebone