Malware u CZ a SK ISP

Robert Šefr (CTO, Whalebone)

whalebone

Whalebone a viditelný vzorek provozu

- DNS provoz
- 150k přípojek
- Česká republika a Slovensko
- Různé typy připojení uživatelů

Životní cyklus malwaru

Infekce

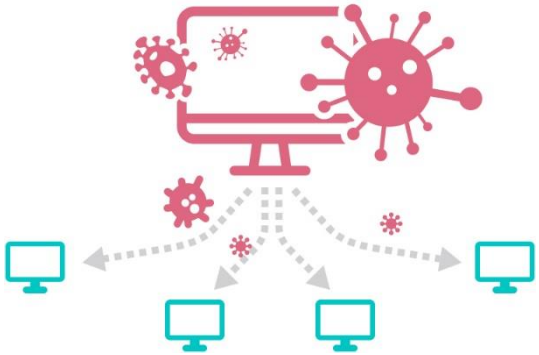
1

Instrukce od C&C

2

Aktivita malwaru

3



Hrozby v číslech

60 tisíc domén / den

Je zařazeno do naší databáze hrozeb

2,5 milionu domén

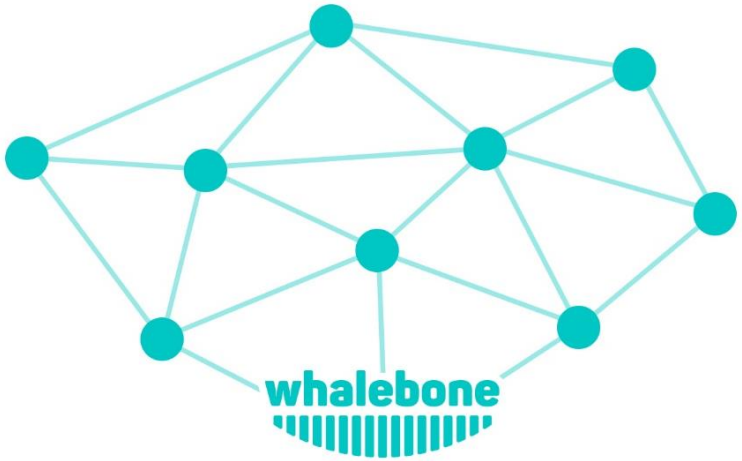
Je celkový počet závadných domén aktivních v naší databázi

30 tisíc incidentů / den

Je průměrný počet detekovaných incidentů ve všech zákaznických stítích

Neuronové sítě použité pro Zero-day detekci

- Neuronová síť rozpoznává náhodně vypadající (Domain Generation Algorithm) doménu od normálních domén
- Zero-day detekce neznámého malwaru a komunikace botnetů – např. komunikace infikovaného CCleaner
- Pokračujeme ve výzkumu automatizované blokace dalších typů hrozeb



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Nasazení

Cloud DNS resolver

- Pět minut - změna konfigurace DNS resolverů
- Bez nutnosti jakékoliv instalace ve vlastní infrastruktuře

On-premise DNS resolver

- Maximálně jednotky hodin
- Software pro Linux
- Viditelnost na lokální IP

1. Infekce

whalebone

Co mají tyto domény společného?

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

Distribuční domény Locky ransomware

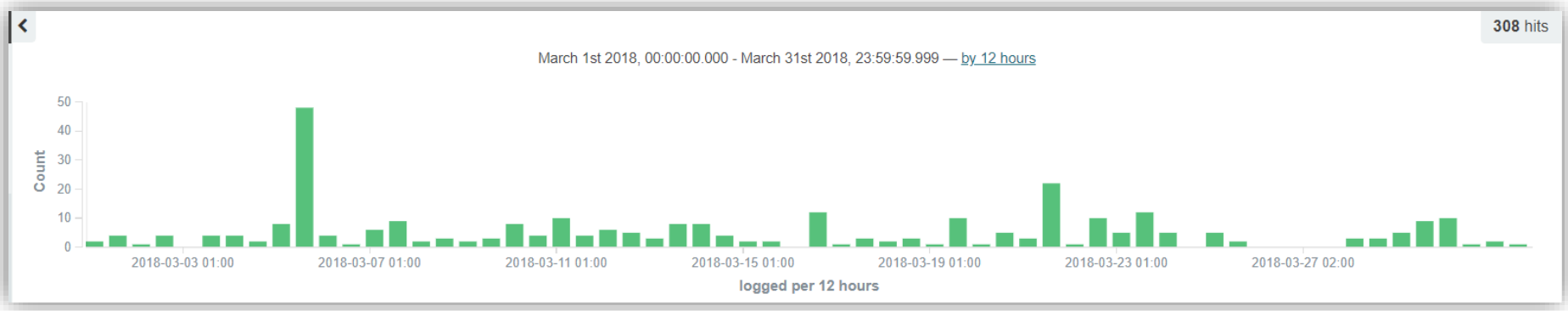
- Březen 2018
- Přístupy k distribučním doménám (infekce)

308

Unikátních incidentů v DNS provozu

83 IP adres

Pokus o stažení ransomwaru



Coin Miner - noblock.pro

- Doména hostující ApplicUnwnt.JS/CoinMiner.F
- JavaScript, který těží kryptoměnu pro útočníka

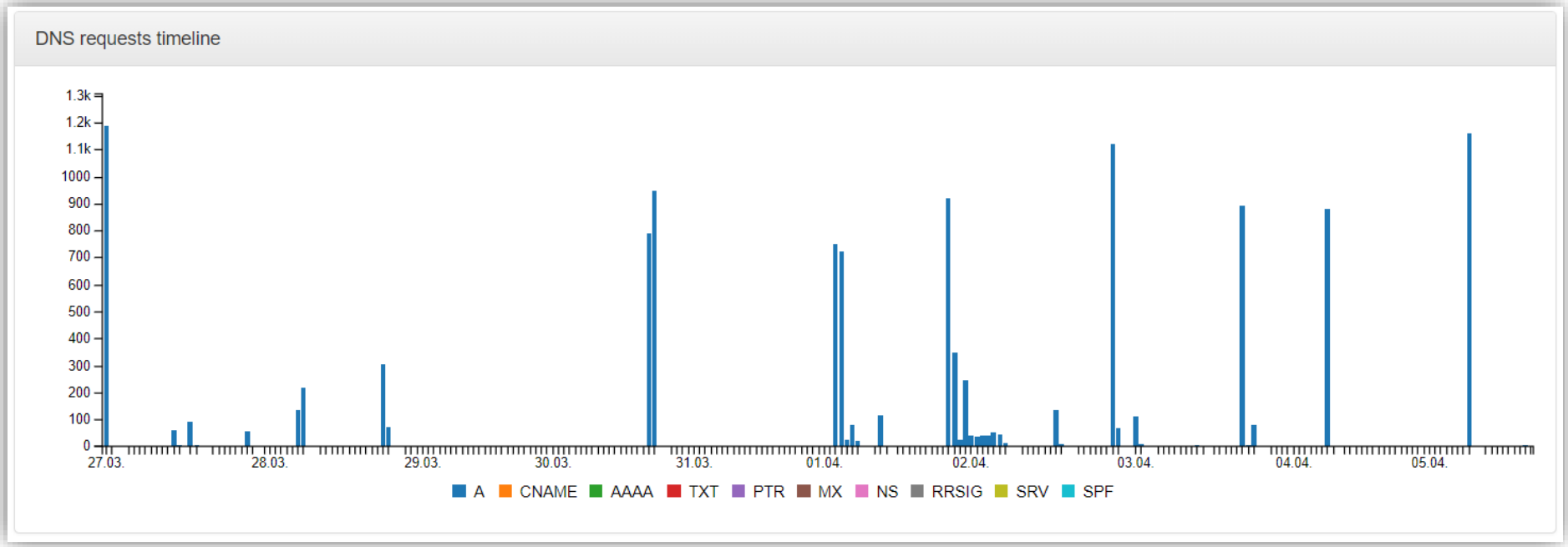
6,5% IP adres

Bylo cíleno tímto útokem během Q1 2018

2. Command & Control

whalebone

Necurs – Domain Generation Algorithm



25 infikovaných IP

Zkoušelo komunikovat s botnetem Necurs pomocí DGA dotazů

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

Cosiloon – Android malware

- Popsán v březnu 2018 společností Avast
- Předinstalovaný malware na Android zařízeních od následujících výrobců
  - ZTE
  - Archos
  - myPhone
- Agresivní podsouvání reklamy (adware)

534 infikovaných IP

A do dnešního dne stále velmi aktivní

Infikovaný CCleaner

- Odhalen v září 2017
- Okamžitě byl zařazen do antivirových databází prakticky všech vendorů
- CCleaner aktualizace infekci také odstranila
- Přes všechny tyto mechanismy stále vidíme na sítích několik infikovaných zařízení

6 infikovaných IP

stále aktivních v září 2018

DGA v DNS provozu

1,01% of IPs 

Vykazuje známky aktivity přítomnosti malwaru komunikujícího pomocí Domain Generation Algorithm

0,28% ze všech DNS dotazů

Je označeno jako náhodných pomocí naší neuronové sítě

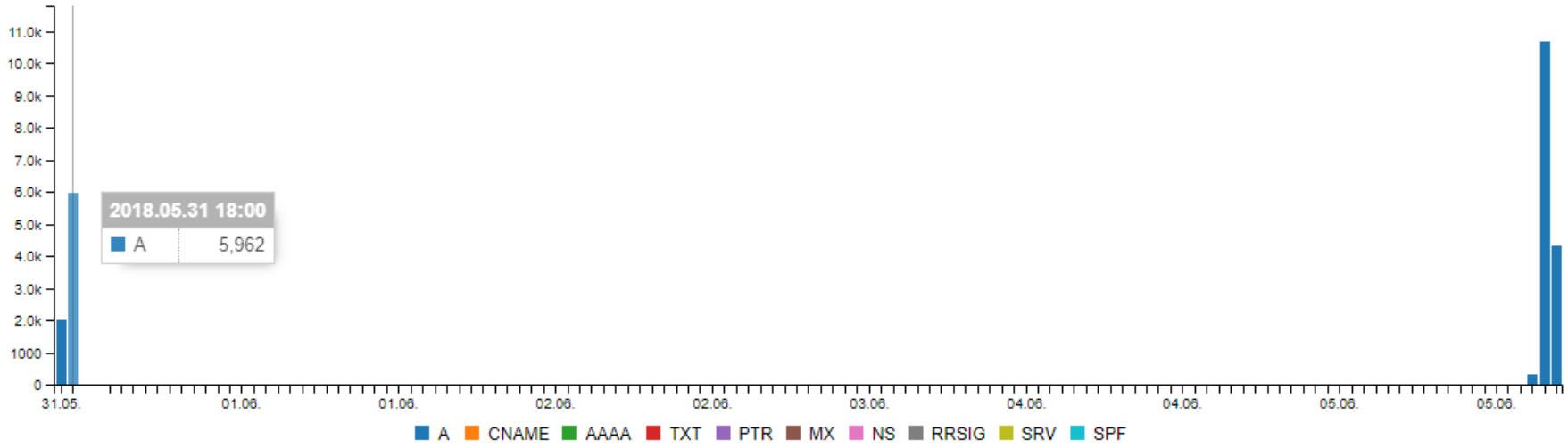
3. Aktivita malwaru

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

Detekce spamu pomocí MX dotazů

4. Závěr

whalebone

Whalebone statistiky – srpen 2018

22,68%

Adres s podezřelým provozem

1,69%

Adres komunikujících s C&C servery

732 581

Unikátních incidentů v DNS provozu

Kvalitní a vždy dostupný DNS překlad

- Základem je **Knot Resolver** předkonfigurovaný společností Whalebone a přidaným modulem pro bezpečnostní filtraci
- Upgrade a rekonfigurace bez výpadku DNS provozu
- Podpora aktuálních standardů DNSSEC
- Prefetching zajišťuje neustále aktuální cache
- Resolver přeloží i domény, které mají přechodné technické problémy

20 tisíc dotazů / s

Úspěšně odbaveno v produkčním nasazení

Otestujte Whalebone (za hodinu)

1. Požádejte si o testování: https://whalebone.io/cs/zkusebni-verze/
2. Nainstalujte Whalebone resolver (copy-paste): http://docs.whalebone.io/cs/latest/local_resolver.html#instalace-noveho-resolveru
3. Nasměrujte na Whalebone resolver DNS provoz

Měsíc testování zdarma s kódem:

KKTS-PLZEN-2018

Odfiltrujte hrozby ze své sítě

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

https://whalebone.io

whalebone