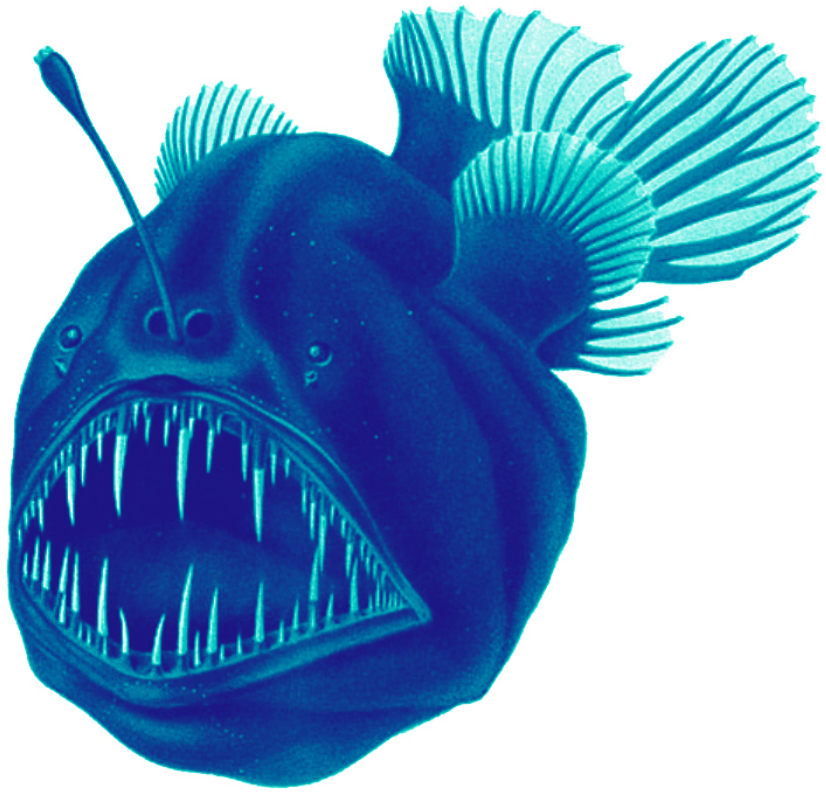
Filter online threats off your network

3dakademie.cz
5psdecin.cz
achb.cz
affilservis.cz
agsa.cz
airgym.cz
altere.cz
amen.cz
anamcara-podbrdy.cz
archiv-zlin.cz
atpic.cz
attigente.cz
autokarem.cz
autozabal.cz
bach-rek.cz
bazinga.sifruje.cz
bemarketing.cz
bereka.cz
berghauer.cz
bizaca.cz
blog.znamylekar.cz
bmobil.cz
bobsck.cz
bohumilice.cz
bulldoggym.cz
burgerspot.cz
calvero.cz
canalboating.cz
causavivendi.cz
cdfe.cz
centralgolf.cz
craftbox.cz
crazycow.cz
cus.cz
dawood.cz
decormag.cz
domovo.cz
doubleweb.cz
dovolena-letecky.cz
dragonflybeer.cz
drevenicezuberec.cz

Angler Exploit Kit

- **1** malware
- **90 559** domén
- **166** .cz domén
- **29 531** IP adres
- **50%** úspěšnost infekce



Životní cyklus botnetu

1 Infekce

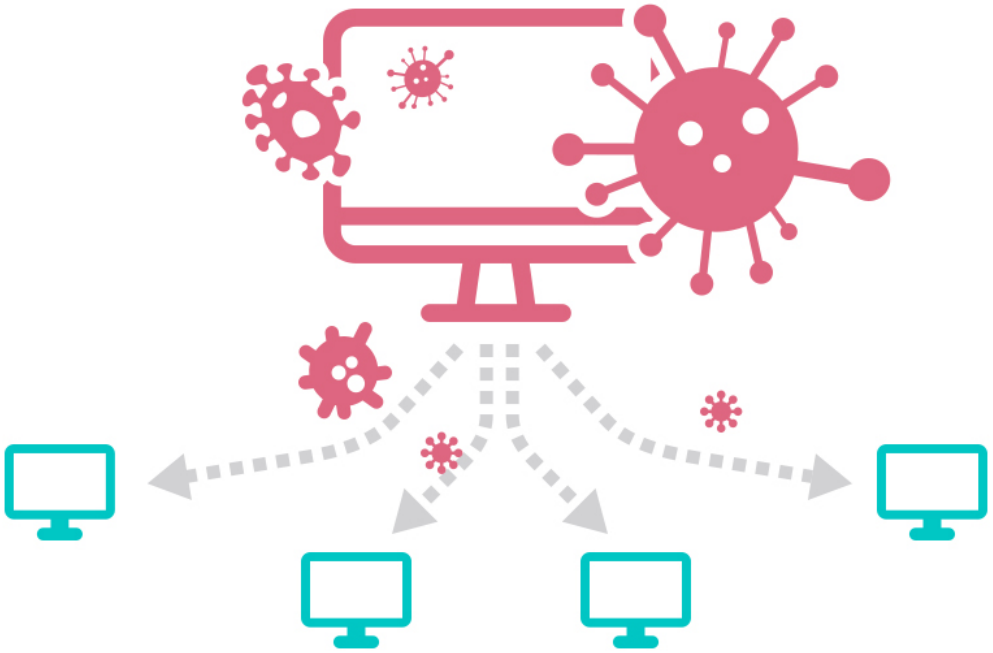
- Emailem rozesílaný downloader
- Infekce (exploit) hostovaná na webu

2 Instrukce od C&C

- Malware vyčkává s aktivitou až do prvních instrukcí od C&C serveru
- Pro komunikaci používá DNS překlad 91.3% malwaru (*2016 Annual Security Report, Cisco*)

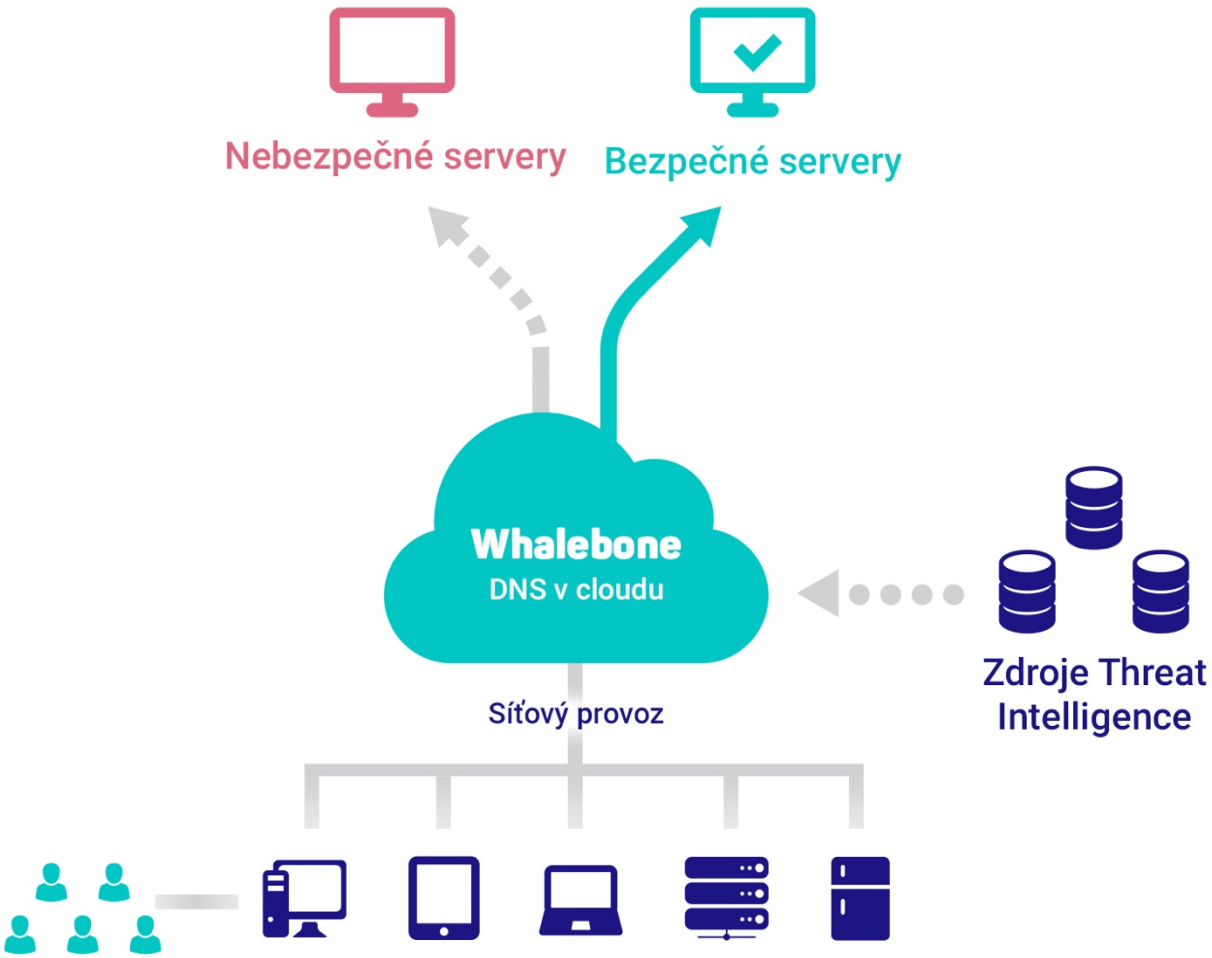
3 Aktivita malwaru

- Rozesílání spamu
- DDoS útoky
- Skenování online služeb
- Bruteforcing online služeb
- Keylogging
- Vydírání uživatelů



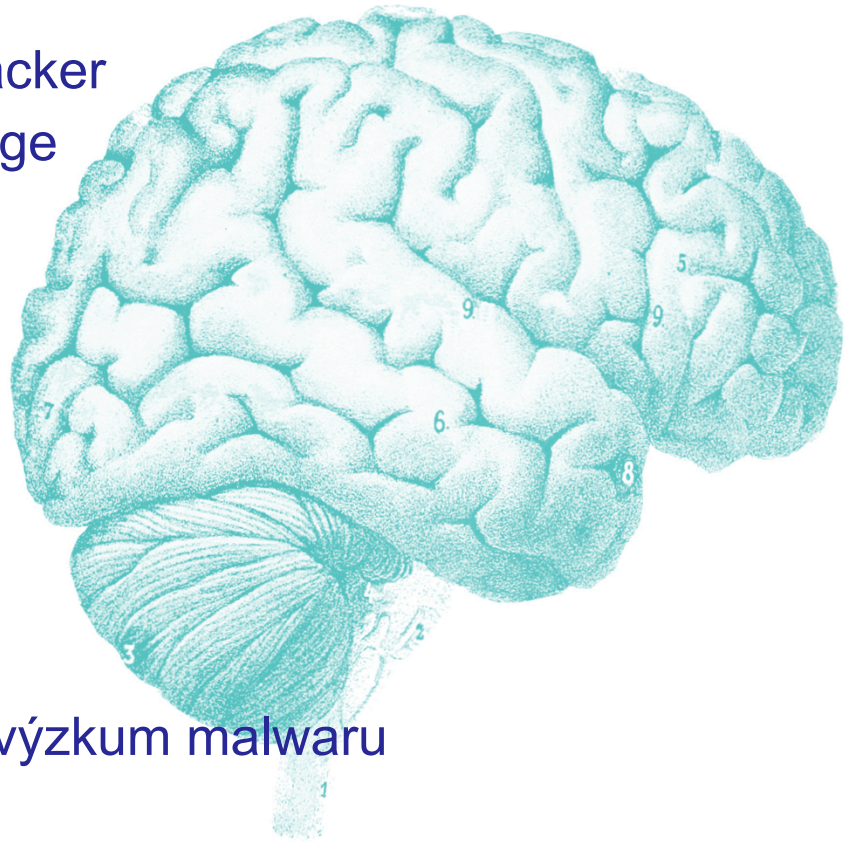
Whalebone / Tým z Brna

Co děláme?


Nebezpečné servery
Bezpečné servery
Whalebone
DNS v cloudu
Zdroje Threat Intelligence
Síťový provoz

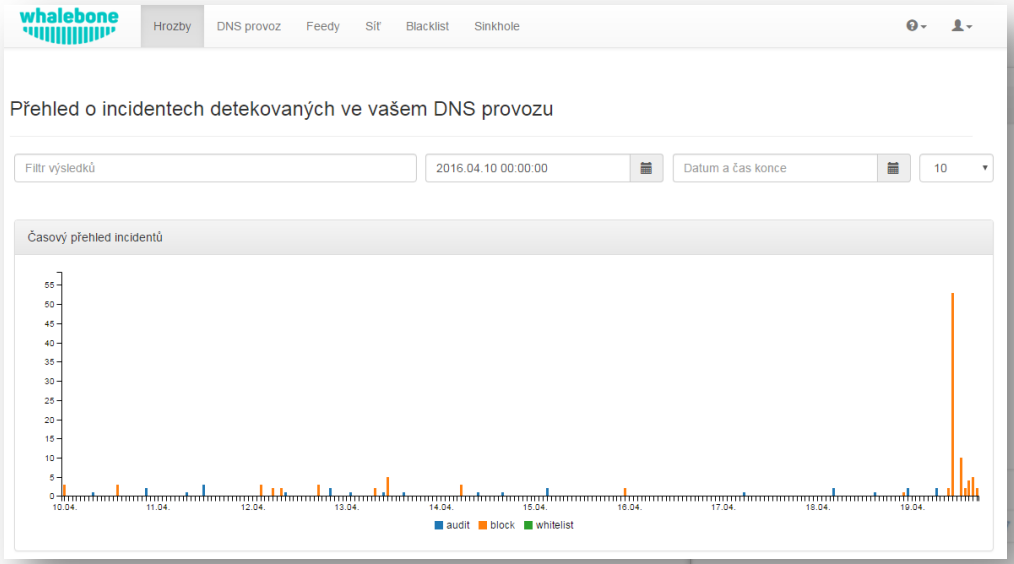
Threat Intelligence Feeds

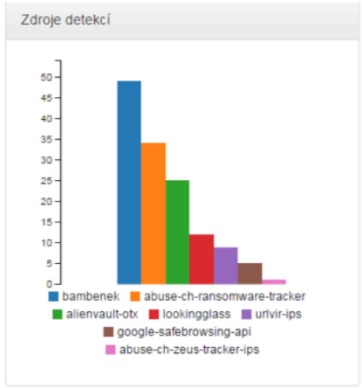
- **Kombinace mnoha open source zdrojů**
  - Tinba, Bedep, Ramnit, apod.
  - Ransomware Tracker, Zeus Tracker
  - Alienvault Open Threat Exchange

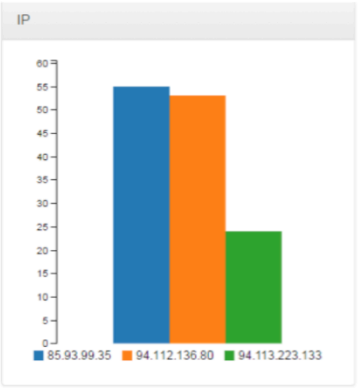


- **Proprietární zdroje**
  - Data od AntiVirus vendorů
  - Google Safebrowsing API
  - Společnosti specializované na výzkum malwaru

Use Case

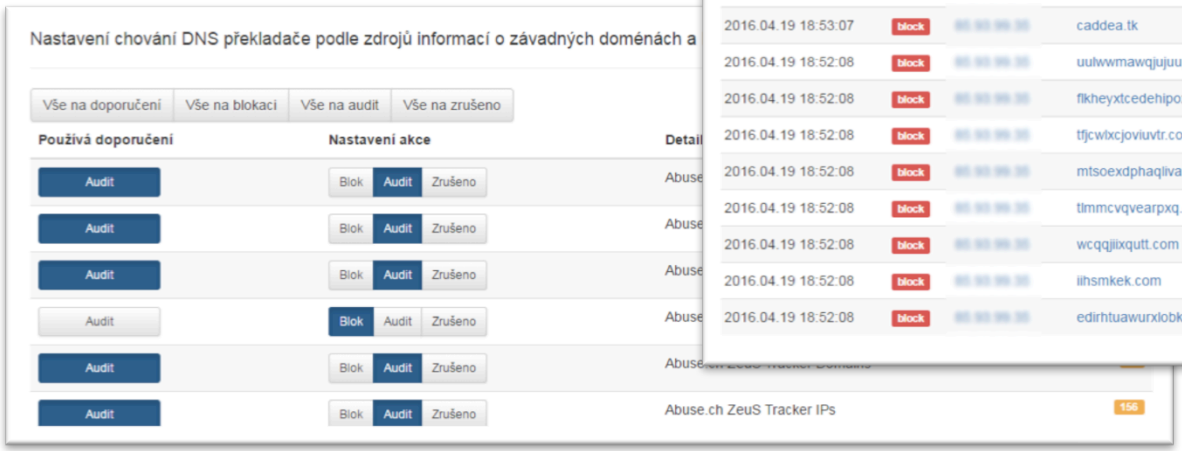






8 ... 11 ... 14 Next »

Datum	Akce	IP požadavku	DNS Dotaz	Kategorie
2016.04.19 18:53:07	block	[redacted]	caddea.tk	blacklist alienvault-otx malware google-safebrowsing-api
2016.04.19 18:53:07	block	[redacted]	caddea.tk	blacklist alienvault-otx malware google-safebrowsing-api
2016.04.19 18:52:08	block	[redacted]	uulwwmawqjujuuprpp.com	c&c bambenek
2016.04.19 18:52:08	block	[redacted]	flkheyxtcedehipox.com	c&c bambenek
2016.04.19 18:52:08	block	[redacted]	tfjcwlxcjoviuvtr.com	c&c bambenek
2016.04.19 18:52:08	block	[redacted]	mtsoexdphaqliva.com	c&c bambenek
2016.04.19 18:52:08	block	[redacted]	tlmmcvqvearpxq.com	c&c bambenek
2016.04.19 18:52:08	block	[redacted]	wcqqjiixqutt.com	c&c bambenek
2016.04.19 18:52:08	block	[redacted]	iihsmkek.com	c&c bambenek
2016.04.19 18:52:08	block	[redacted]	edirhtuawurxlobk.com	c&c bambenek



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 / virtuální appliance
- Viditelnost na lokální IP

Využití v síti ISP

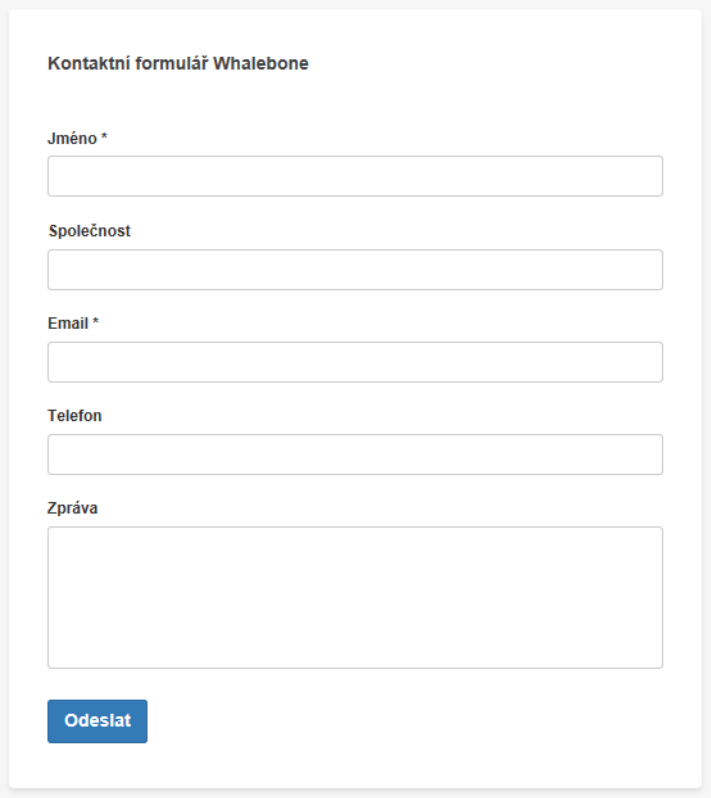
- **Detekce infikovaných a rizikových přípojek**
  - Možnost notifikace uživatelů a firem
  - Automatická blokace opravdu závadného provozu
- **Jednoduchý nástroj na blokaci vybraných domén**
  - Na přání zákazníka (např. školy)
  - Na základě legislativního nařízení
- **Výsledky použitelné pro marketing**
  - „Ochránili jsme naše zákazníky před XYZ útoky“
- **Přehledy o trendech provozu a anomáliích**

Výhody čisté sítě

- **Snížení objemu spamu, DDoS a bruteforce útoků**
- **IP adresy a sítě nebudou zařazovány na blacklisty**
- **Zvýšení dostupnosti služeb zákazníkům**
- **Snížení počtu abuse hlášení a nutnost jejich řešení**
- **Méně klientů dožadujících se nápravy řádění malwaru**

Testovací účet

1. Zaregistrujte se na **https://whalebone.io**
2. Do zprávy nám napište „**SÍTĚ PLZEŇ**“



Odfiltrujte hrozby ze své sítě

Richard Malovič
richard.malovic@whalebone.io
+420 608 252 312

Michal Karm
karm@whalebone.io
+420 737 778 560

https://whalebone.io

whalebone