

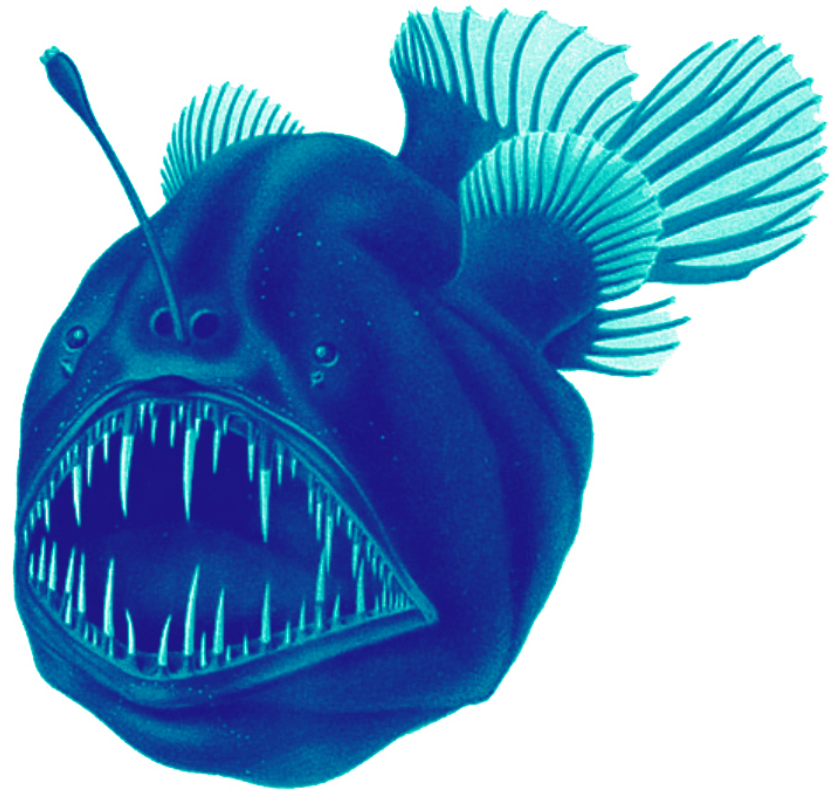


Filter online threats off your network

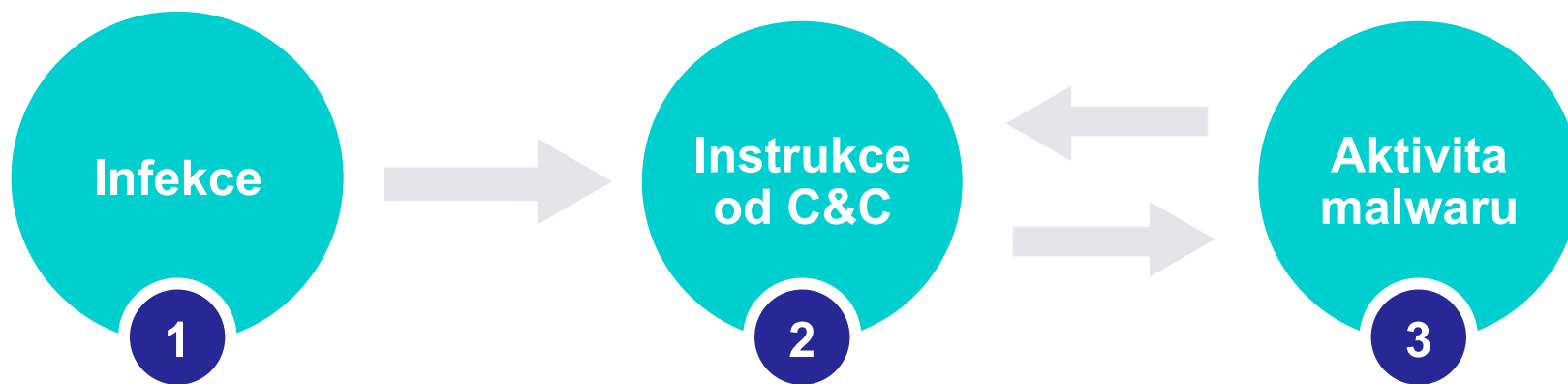
3dakademie.cz
5psdecin.cz
achb.cz
affilservis.cz
agsa.cz
airgym.cz
altere.cz
amen.cz
anamcara-podbrdy.cz
archiv-zlin.cz
atpic.cz
attigente.cz
autokarem.cz
autozabal.cz
bach-rek.cz
bazinga.sifruje.cz
bemarketing.cz
bereka.cz
berghauer.cz
bizaca.cz
blog.znamylekar.cz
bmobil.cz
bobsck.cz
bohumilice.cz
bulldoggym.cz
burgerspot.cz
calvero.cz
canalboating.cz
causavivendi.cz
cdfc.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

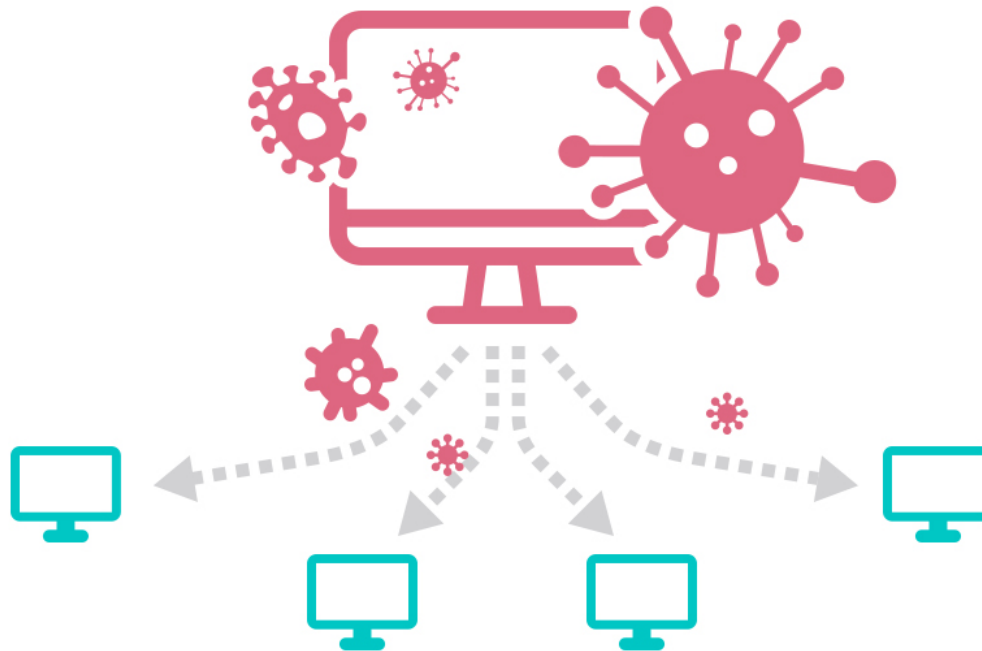
- Malware vyčkává s aktivitou až do prvních instrukcí od C&C serveru
- Pro komunikaci používá DNS překlad 91.3% malwaru (*2016 Annual Security Report, Cisco*)



3

Aktivita malwaru

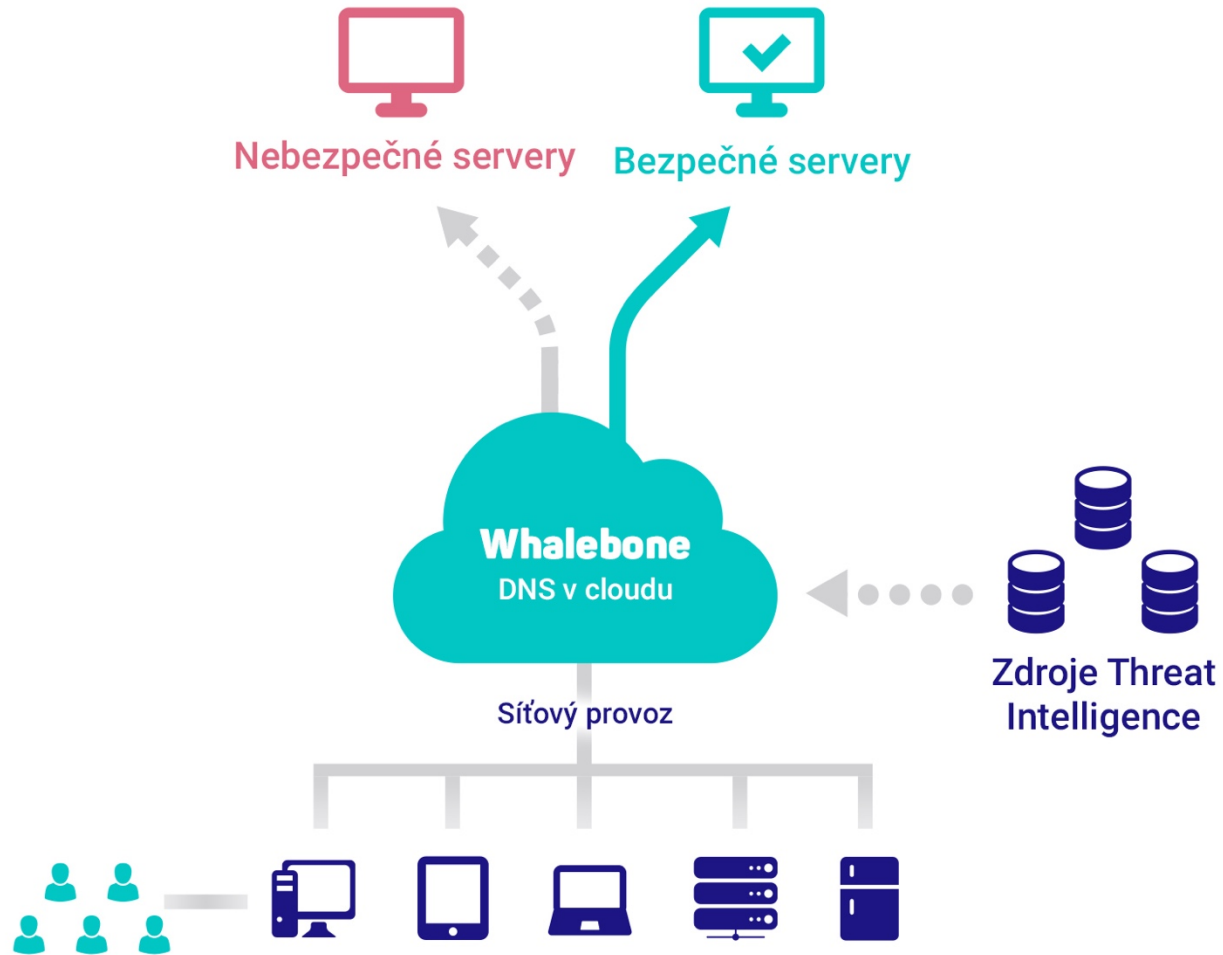
- Rozesílání spamu
- DDoS útoky
- Skenování online služeb
- Bruteforcing online služeb
- Keylogging
- Vydírání uživatelů



Whalebone / Tým z Brna

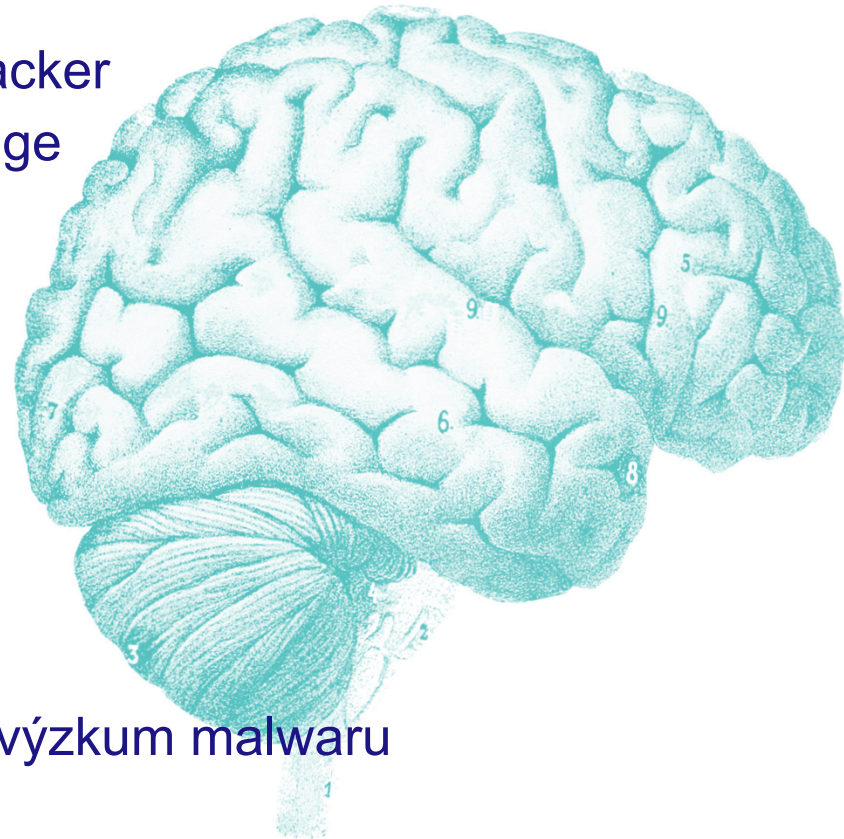


Co děláme?

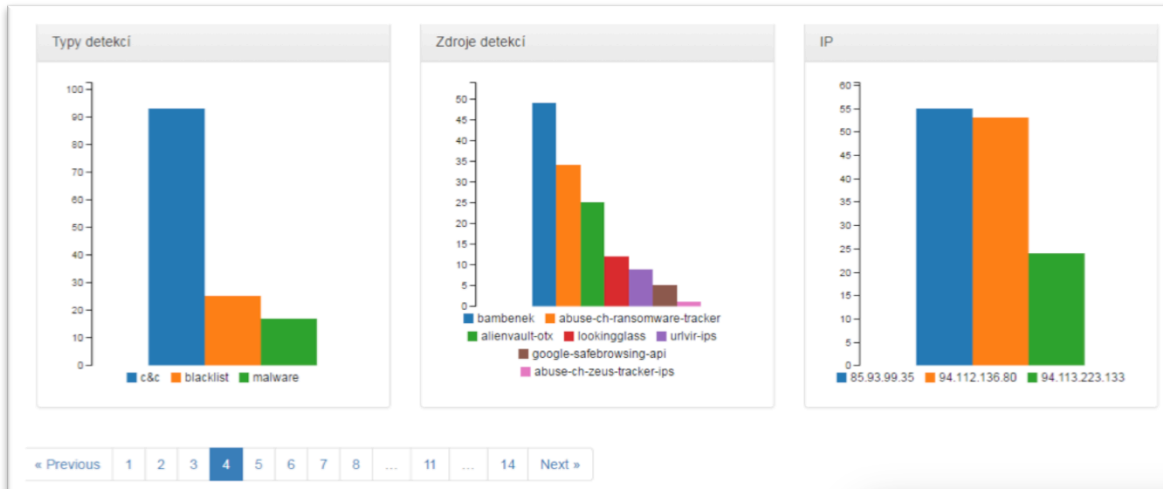


Threat Intelligence Feeds

- **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



Detekce C&C komunikace



« Previous 1 2 3 4 5 6 7 8 ... 11 ... 14 Next »

| Datum | Akce | IP požadavku | DNS Dotaz | Kategorie |
|---------------------|-------|--------------|-----------------------|----------------------|
| 2016.04.19 18:53:07 | block | 85.93.99.35 | caddea.tk | blacklist alienvaut- |
| 2016.04.19 18:53:07 | block | 85.93.99.35 | caddea.tk | blacklist alienvaut- |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | uulwvmawqujuuprpp.com | c&c bambenek |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | flkheytxcedehipox.com | c&c bambenek |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | tfcwxcjoviuivr.com | c&c bambenek |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | mtsoexdphaqlva.com | c&c bambenek |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | timmvcvqearpqx.com | c&c bambenek |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | wcqjlixqutt.com | c&c bambenek |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | liismkek.com | c&c bambenek |
| 2016.04.19 18:52:08 | block | 85.93.99.35 | edirhtuawurxiobk.com | c&c bambenek |

whalebone Hrozby DNS provoz Feedy Sit Blacklist Sinkhole

Přehled o incidentech detekovaných ve vašem DNS provozu

Filtr výsledků 2016.04.10 00:00:00 Datum a čas konce 10

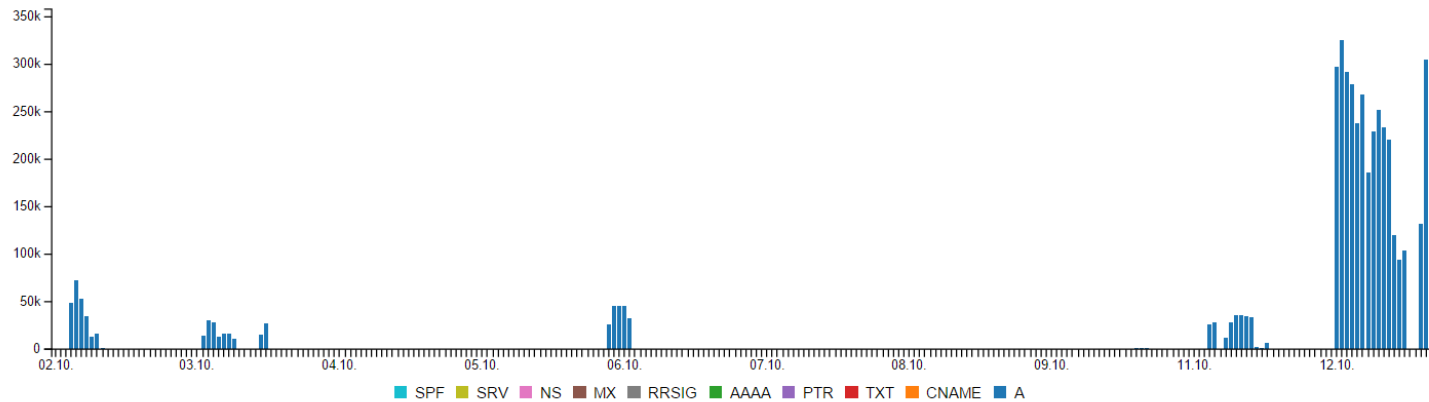
Časový přehled incidentů

| Datum | audit | block | whitelist |
|-------|-------|-------|-----------|
| 10.04 | 0 | 0 | 0 |
| 11.04 | 0 | 0 | 0 |
| 12.04 | 0 | 0 | 0 |
| 13.04 | 0 | 0 | 0 |
| 14.04 | 0 | 0 | 0 |
| 15.04 | 0 | 0 | 0 |
| 16.04 | 0 | 0 | 0 |
| 17.04 | 0 | 0 | 0 |
| 18.04 | 0 | 0 | 0 |
| 19.04 | 0 | ~55 | 0 |

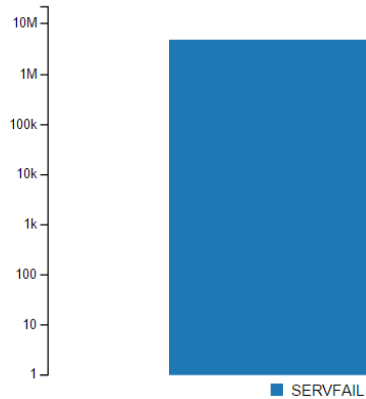
Detekované odchozí DoS útoky

answer:SERVFAIL

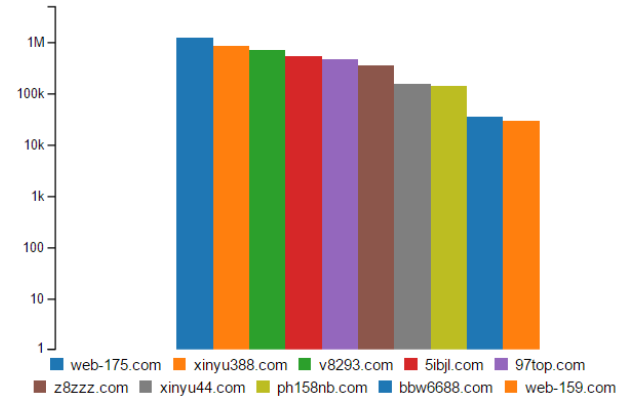
Časový přehled DNS dotazů



Odpovědi



Domény 2. řádu



Nastavení feedů a sítí

Nastavení chování DNS překladače podle zdrojů informací o závadných doménách a IP adresách

Vše na doporučení Vše na blokaci Vše na audit Vše na zrušení

| Používá doporučení | Nastavení akce | Detaily feedu | |
|--------------------------|--|---------------------------------|-----|
| <input type="checkbox"/> | <input type="checkbox"/> Blok <input checked="" type="checkbox"/> Audit <input type="checkbox"/> Zrušeno | Abuse.ch Feodo Tracker IPs | 608 |
| <input type="checkbox"/> | <input type="checkbox"/> Blok <input checked="" type="checkbox"/> Audit <input type="checkbox"/> Zrušeno | Abuse.ch Palevo Tracker Domains | 15 |
| <input type="checkbox"/> | <input type="checkbox"/> Blok <input checked="" type="checkbox"/> Audit <input type="checkbox"/> Zrušeno | Abuse.ch Palevo Tracker IPs | 12 |
| <input type="checkbox"/> | <input type="checkbox"/> Blok <input checked="" type="checkbox"/> Audit <input type="checkbox"/> Zrušeno | Abuse.ch Ransomware Tracker | 558 |
| <input type="checkbox"/> | <input type="checkbox"/> Blok <input checked="" type="checkbox"/> Audit <input type="checkbox"/> Zrušeno | Abuse.ch Zeus Tracker Domains | 65 |
| <input type="checkbox"/> | <input type="checkbox"/> Blok <input checked="" type="checkbox"/> Audit <input type="checkbox"/> Zrušeno | Abuse.ch Zeus Tracker IPs | 156 |

Brno

85.93.99.35/32



62.245.116.45/32



Praha

195.39.4.0/24



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 blokáce 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 „**SIETE JASNA**“

Kontaktní formulář Whalebone

Jméno *

Společnost

Email *

Telefon

Zpráva

Odeslat

Odfiltrujte hrozby ze své sítě

Richard Malovič

richard.malovic@whalebone.io

+420 608 252 312

<https://whalebone.io>

