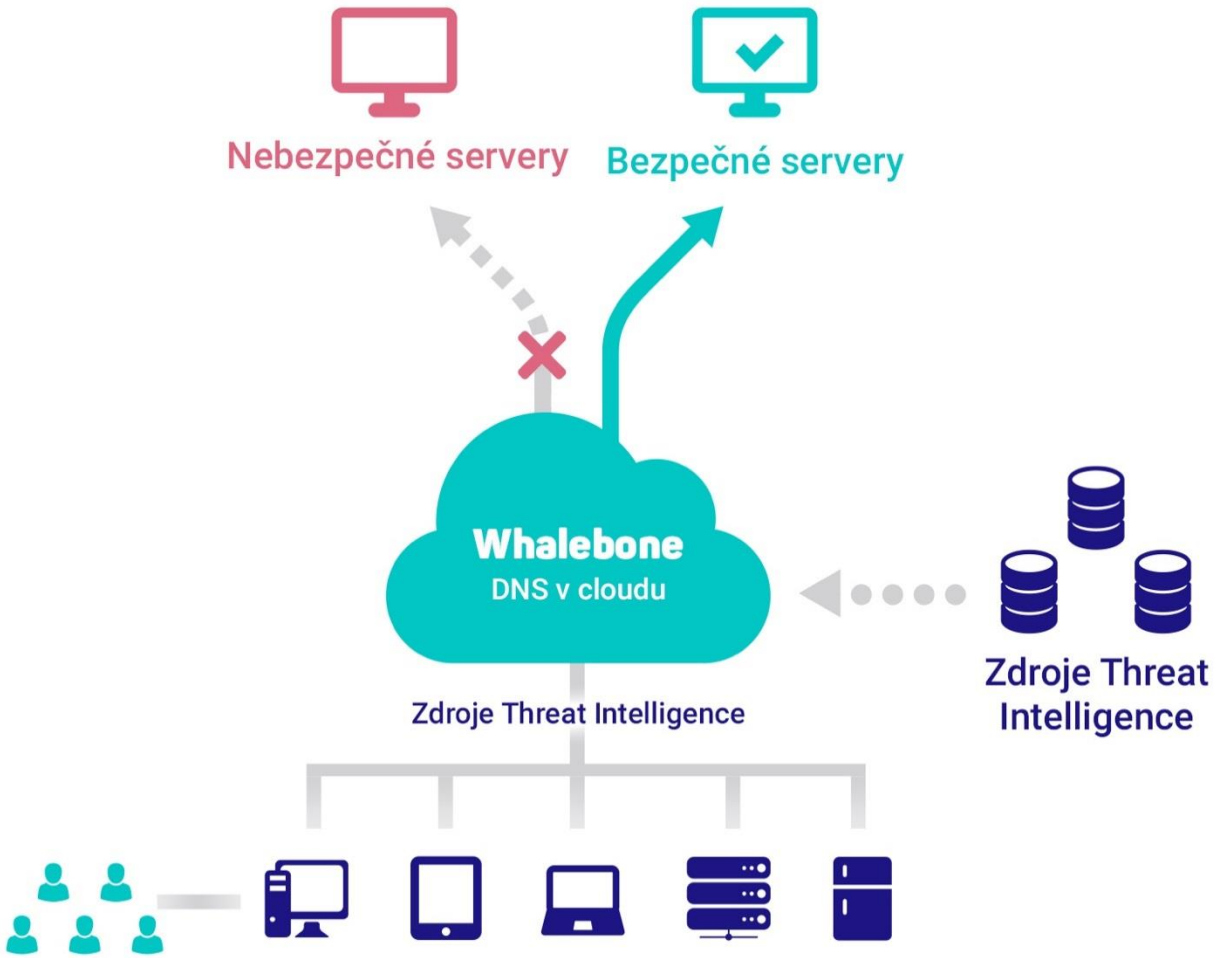
Filter online threats off your network

Co děláme?


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

Nasazení

Cloud DNS resolver

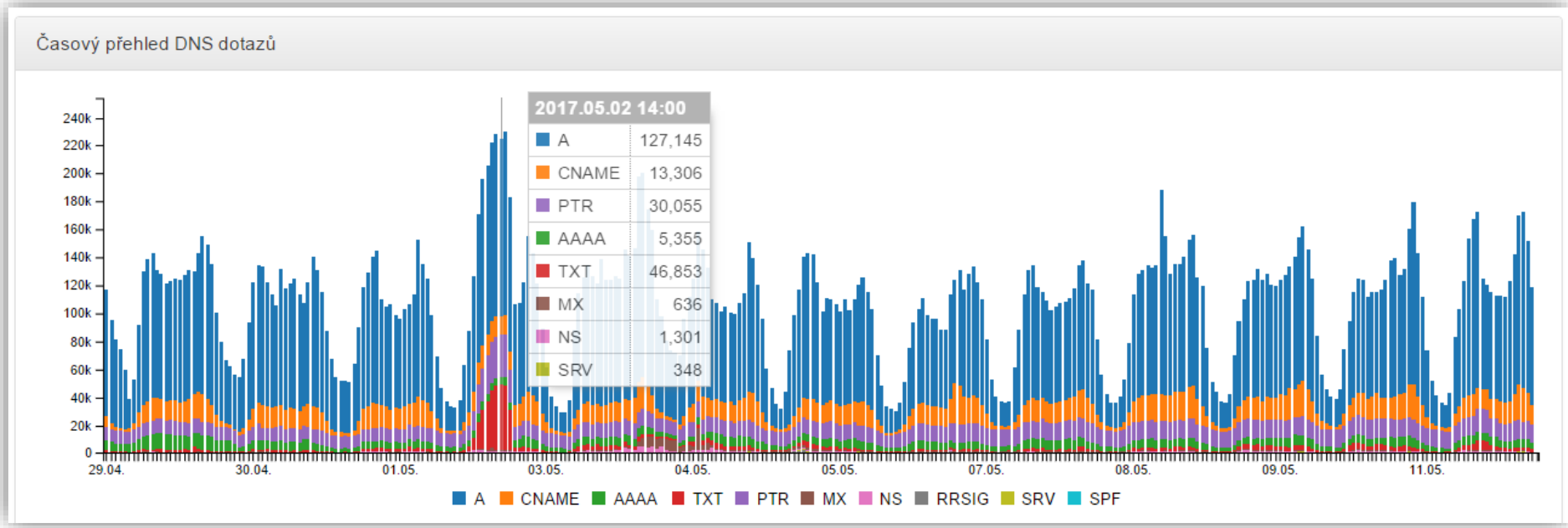
- Pět minut - změna konfigurace DNS resolverů
- Bez nutnosti jakékoliv instalace ve vlastní infrastruktuře

On-premise DNS resolver

- Maximálně jednotky hodin
- Software / virtuální appliance
- Viditelnost na lokální IP

Kompletní DNS audit

- Až na úroveň konkrétních DNS dotazů
- Nad auditem se dá dělat rozsáhlý výzkum a přinést mnohem víc informací



Výzkum: Neuronové sítě a klasifikace provozu

Výzkum - Neuronové sítě

- Tým tří výzkumníků spolupracuje s týmem Whalebone
- Detekce **Domain Generation Algorithm** v DNS provozu. Soustředíme se na pokus o kontakt C&C serverů hostovaných na algoritmicky generovaných doménách

Research team

Czech Technical University in Prague

Sebastian Garcia (@eldracote)

- Malware network security researcher and Teacher
- Machine Learning in security for the civil society
- Stratosphere IPS project https://stratosphereips.org

Carlos A. Catania (Aka Harpo), Ph.D. in Computer Science

- Associated professor at National University of Cuyo - Argentina
- Machine Learning, Network Security, Distributed Computing
- Member of the Stratosphere project since 2015

Pablo Torres

- Software Engineer
- Neural Networks Expert
- AI Cybersecurity Warrior

Detekční mechanismus

- Neuronové sítě se používají k rozpoznávání vzorů v obrázcích, zvucích, videu, ale také v jazyce
- Naše neuronová síť má za úkol rozpoznat náhodně vypadající doménu od normálních
- Další komponenty vyhodnocují kontext a zpřesňují detekci

1. Neural Network

- Počítá pravděpodobnost „náhodnosti“ na škále 0-1 (více než 0.95 považujeme za podezřelou doménu)
  - google.com -> 0.006
  - y9uj6ikyre2a.ru -> 0.998
- **0.1%** celkového provozu je označeno jako podezřelé

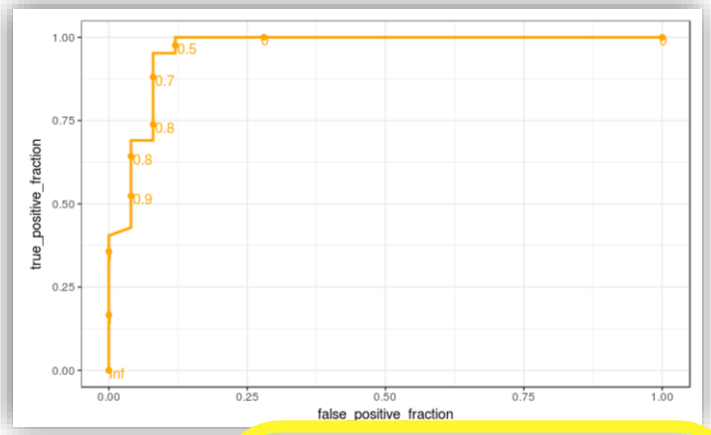
- Učení probíhalo na milionech standardních domén a domén generovaných desítkami botnetů

2. Classifier

- Dostává informace o detekovaných doménách
- Vyhodnocuje časování okolních DNS dotazů
- Kontext eliminuje občasné chyby neuronové sítě
  - Při falešné detekci neuronové sítě není nalezen korespondující historický provoz
  - Pokud byla v sérii podezřelých domén kategorizována pouze část, Classifier se postará o doplnění ostatních, které těsně unikly detekci

3. Profiler

- Udržuje informace o tom, zda je některá z IP adres infikovaná
- Vyhodnocuje pravděpodobnost svého úsudku, při překročení prahové hodnoty 0.8 je IP prohlášena za infikovanou



1. Neural Network → 2. Classifier → 3.Profiler

Detekce v provozu

Conficker

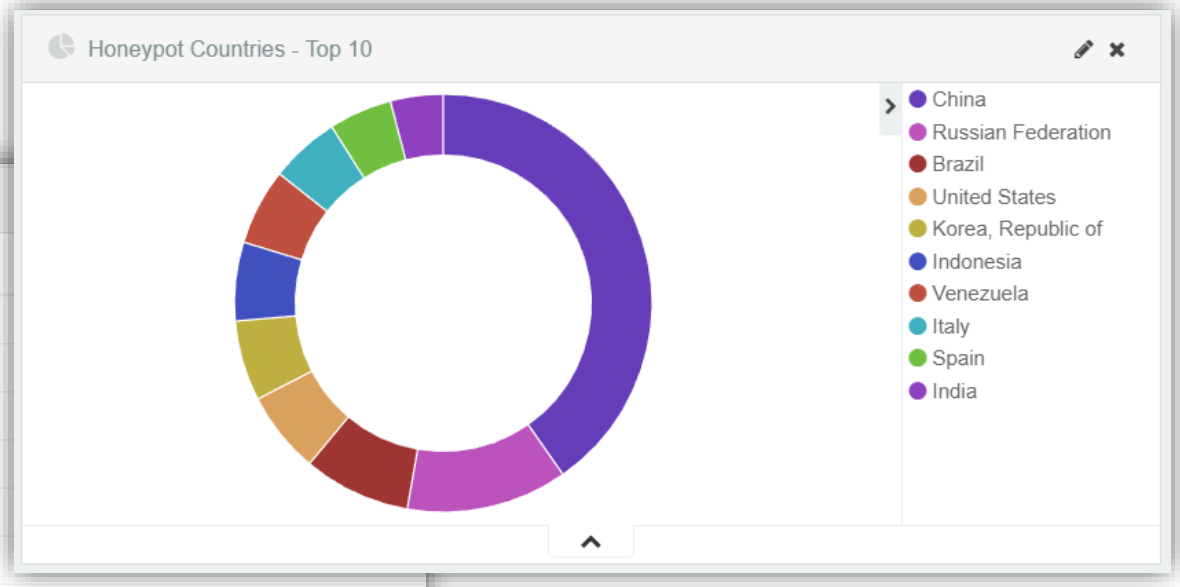
- Stále mnoho infikovaných strojů, přestože zanedlouho oslaví deset let
- Botnet nebyl nikdy pořádně „využit“ svými tvůrci
- Prakticky neustále detekovaný botnet

- **Ze zvědavosti jsme jednu z domén koupili**

```
mbvtbiwylx.com
ysutzorwqvo.com
gejxmmgzjpe.biz
gqifzmdqxv.ws
qnbzxzl.net
yngxmaqko.com
hhgfnxgv.info
wzhofyuymkz.cn
osxknyfyyu.net
vblmfivps.info
akshfvxub.com
qxzglrqu.info
qlgqfuhkl.org
ofgjcesjgr.com
```

Conficker Sinkhole

- Více než 170 tisíc unikátních IP za den
- V ČR necelých 500



Honeypot ASN - Top 10

AS	ASN	
AS5610	O2 Czech Republic, a.s.	
AS5588	T-Mobile Czech Republic a.s.	
AS6830	Liberty Global Operations B.V.	
AS13036	T-Mobile Czech Republic a.s.	
AS34080	MIRAMO spol. s.r.o.	
AS39906	CoProSys a.s.	
AS44546	ALFA TELECOM s.r.o.	38
AS12767	T-Mobile Czech Republic a.s.	26
AS15614	Dragon Internet a.s.	25
AS29208	Dial Telecom, a.s.	24

Sality

- Agresivní a velmi dlouho aktivní virus
- První zmínky se datují do roku 2003, ale od té doby byl výrazně změněn
- Deaktivuje antivirová řešení

```
h7smcnrwlsdn34fgv.info
lukki6nd2kdnc.info
f5ds1jkkk4d.info
g1ikdcvns3sdsal.info
hkukud123ncs.info
```

Ramnit

- První detekce 2010, aktivní dodnes
- Botnet zaměřený na odcizení
  - Session cookies
  - Hesel k FTP klientům
  - Hesel k bankovním účtům
- Zároveň také poskytuje útočníkovi plný přístup k infikovanému stroji

```
rtvwerjyuver.com
tvrstrynyvwstrtve.com
wqerveybrstyhcerveantbe.com
```

Trojan OSX Flashback

- Trojský kůň mířený na MacOS
- Největší nárůst aktivity v roce 2012

```
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
```

A mnoho dalších nepojmenovaných

- Mnoho detekcí, které není jednoduché přiřadit konkrétnímu botnetu
- Je ale poměrně zjevné, že je klient infikovaný

```
7dkwdw.8zbbnaczgeyig1b.info
2go4dr.719y8g7czj70krr.info
2go4dr.vwn5rft7uycu0b.info
8ep4e5.tupwk35u6uz58gu.info
4ev2g1.uk4e56g1lysskxq.info
2go4dr.719y8g7czj70krr.info
2go4dr.vwn5rft7uycu0b.info
5dnkdk.tmw9n7gwb7pe.info
4ev2g1.z3r6bn90q6k5a80.info
```

```
ohyxgtmlgnqzs.com
rudgjefqzkvmvopmzy.com
itkxafypmpcvolmdy.com
stirkdehyvybgpk.com
pqvahqxodencrqrybo.com
volebczsjkhy.com
qnaxiludclqpilcfe.com
lkrchaparalglqlojg.com
chcvgrkdqfsvw.com
```

Zajímavosti

- Pochybné reklamní systémy (nejčastěji pop-up reklamy) rezervují velké množství náhodných domén kvůli blacklistům

```
doiljgzpurycgx.bid
ywwefdjjc.bid
wwfjhzut.bid
pcvdrjvku.bid
zeuwuxfzvaoqp.bid
mlntnugnalv.bid
pcvdrjvku.bid
oijvjlfjjb.bid
```

- Některé jednotlivé validní domény není jednoduché strojově odlišit od malwaru
  - Jedná se o samostatné výskyty, které nestačí k označení stroje jako infikovaného

```
csvnmnm.cz
vospaspsm.cz
zbkjmkcr.cz
zusjjrrozmitalptr.cz
zstgmlomnice.cz
odbrdkvltave.cz
```

Otestujte si Whalebone

- Vyplňte náš kontaktní formulář https://whalebone.io/plzen/

- Uveďte heslo „**SÍTĚ PLZEŇ 2017**“ pro získání delšího testovacího období zdarma

Odfiltrujte hrozby ze své sítě

Robert Šefr
robert.sefr@whalebone.io
+420 608 737 930
https://whalebone.io

whalebone