

Analýza otrávené DNS cache

Ondřej Caletka



7. února 2017

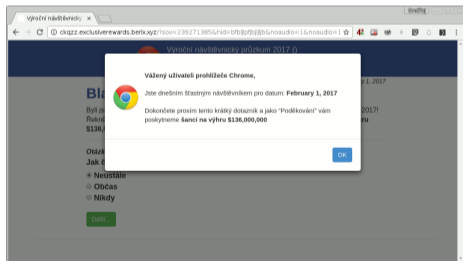


Uvedené dílo podléhá licenci Creative Commons Uvedte autora 3.0 Česko.

- real-time blacklist uceprotect.net
- zřízen za účelem potírání spamů
 - zaznamenává IP adresy serverů, které rozesílají spam
 - případně přilehlých síťových bloků
 - případně celých autonomních systémů
- dotazuje se převrácenou IPv4 adresou doplněnou příponou listu
- pro zalistované adresy vrací obvykle 127.0.0.x
- samostatně nepříliš účinné a bezpečné
 - použitelné jako jeden ze zdrojů reputačních systémů

Problém

- 1. listopadu 2016 00:11 CET
- Nagios: všechny e-mailové servery se ocitly na blacklistu UCEprotect
- stránky uceprotect dostupné
- ruční kontrola neukazuje žádný problém
- podivná adresa vrácená z blacklistu: 176.107.178.7



Otrávená DNS cache

- na hlavních DNS resolverech vše funguje bez problému
- nagios server používá svůj vlastní resolver
- stejný dotaz, různé odpovědi
- obdobný problém i v xDSL síti T-Mobile
- vyprázdnění cache problém vyřešilo

```
$ host www.uceprotect.net  
www.uceprotect.net has address 217.23.49.178
```

```
$ host www.uceprotect.net  
www.uceprotect.net has address 176.107.178.7
```

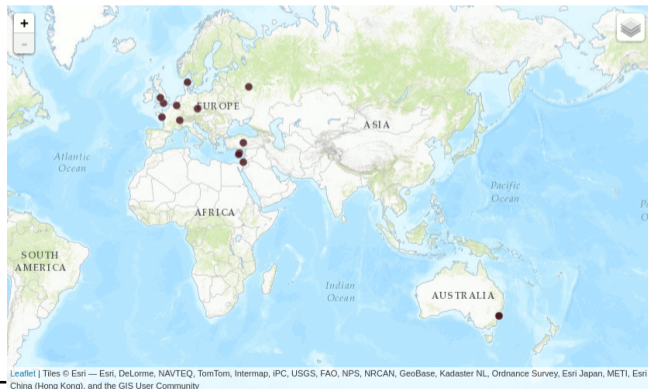
- šlo o cílený útok?
- jedná se o lokální, nebo globální problém?
- jakým způsobem nejspíše otrávení proběhlo?
- je možné tomu do budoucna předejít?

- systém aktivního měření Internetu
- budován od roku 2010
- používá hardwarové sondy hostované u dobrovolníků
- více než 9000 připojených sond (250 v ČR)
- vestavěná a uživatelsky definovatelná měření
- všechna měření veřejná
- API přístup k výsledkům i zadáním
- zaměřeno na nejnižší úroveň funkce IP sítí
 - ping
 - traceroute
 - DNS



Hledání sond s podobným problémem

- spuštěno měření na všech českých a slovenských sondách a dále na 500 sondách ze zbytku světa
- úkol: přeložit `www.uceprotect.net` na IP adresu
- 758 odpovědí, z toho 14 otrávených

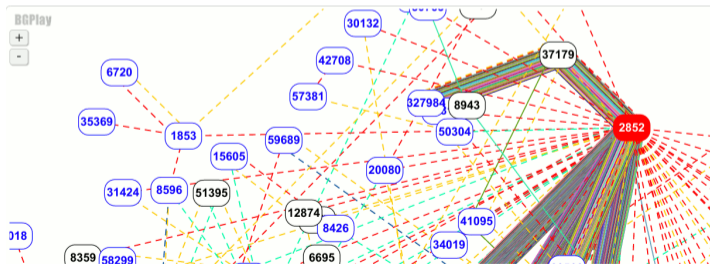


Problém nejspíše na autoritativní straně

- nelze vystopovat žádnou spojitost mezi jednotlivými sondami
- reálný případá únos autoritativních serverů
 - 1 únos všech současně (jsou-li v jedné síti)
 - 2 únos master serveru a vynucení přenosu zóny na slave servery
 - 3 změna delegace v nadřazené zóně


Nástroj RIPEstat

- kolekce statistik internetových prostředků
- IP adresy, čísla autonomních systémů, geolokace, data ze senzorů
- webová aplikace s widgety
- automatické vyhledávání abuse kontaktů
- API přístup k surovým datům v JSON




Geolokace autoritativních serverů

Geoloc (217.23.48.85)




▶ Geoloc details

 Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)


Showing results for 217.23.48.85 as of 2016-11-02 20:00:00 UTC

[source data](#) [embed code](#) [permalink](#) [info](#)

Geoloc (208.77.218.116)



▶ Geoloc details


 Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for 208.77.218.116 as of 2016-11-02 20:00:00 UTC

[source data](#) [embed code](#) [permalink](#) [info](#)

Geolokace autoritativních serverů

Geoloc (67.212.83.77)




▶ Geoloc details

i Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for 67.212.83.77 as of 2016-11-02 21:00:00 UTC

source data embed code permalink info

Geoloc (96.43.138.38)



▶ Geoloc details

i Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for 96.43.138.38 as of 2016-11-02 21:00:00 UTC

source data embed code permalink info

- diverzitní rozmístění – únos všech nepravděpodobný
- kolektory BGP nezaznamenaly žádné změny v ohlašování daných IP adres
- pro synchronizaci blacklistů se nejspíše nepoužívají zónové přenosy
- zbývá hypotéza se změnou delegace v nadřazené zóně

Whois uceprotect.net

Domain Name: uceprotect.net
Registry Domain ID: 97889633_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.psi-usa.info
Registrar URL: http://www.psi-usa.info
Updated Date: 2016-10-31T16:58:08Z

...

Registrant Name: Sebastian Müller
Registrant Organization: Privacy Guard
Registrant Street: Freiligrathstr. 2
Registrant City: Magdeburg
Registrant State/Province: DE
Registrant Email: _contact_@privacy-guard.de



From: Claus von Wolfhausen <c.v.wolfhausen@uceprotect.net>

Hi,

We are aware that someone seems to have poisoned multiple COM, NET, EDU Domains at Internic Rootservers by Monday... Our DNS had the correct Informations and also the datas at our registrar are fine. Registrar told us, they recommend to retransmitt our DNS to the Rootservers so we did an Update at Monday Since that the Problem should be fixed. If you still experience problems please delete your DNS-Cache or request your provider to do so.

Regards

Claus



Hacknutý registrátor?

- nejpravděpodobnější vysvětlení
- webové stránky PSI-USA nevypadají jako stránky registrátora
- nejspíš jde o *skořápkovou společnost* – registrátora, který je plně ovládán jinými subjekty v pozadí

Fraud Reports Wikia

PSI-USA Inc is an ICANN accredited registrar in Germany, also offering its services as InterNetX. Early in 2013 InterNetX suffered the highest abuse rate from the Russian fake pharmacy fraud, EvaPharmacy and has tried to tackle the problem.

Zdroj: <http://fraud-reports.wikia.com/wiki/PSI-USA>

Servery hostující unesenou doménu

- e-mail v konferenci Spamassasin ukazuje IP adresy NS při únosu
- tyto servery jsou stále funkční!
- hostují velké množství zón

Passive DNS analýza

- na stejné adrese hostováno asi 1000 domén
- některé jsou dodnes delegovány
- některé vypadají velmi podivně:
`drophishost-0c4705e8-ecbf-4c0d-a773-888b51c30b87.biz`

- proti změně dat po cestě: **DNSSEC**
- proti injektování obsahu do zóny při přenosu: **TSIG**
 - podepisování zónových přenosů sdíleným tajemstvím
- proti hacknutí registrátora: **zamykání na úrovni registru**
 - u domény .cz snadno a rychle pomocí Doménového prohlížeče
 - u jiných problematické, zařizuje se prostřednictvím registrátora (!)
- proti dlouhodobému otrávení cache resolveru
 - volba max-cache-ttl v konfiguraci
 - standardně 7 dní pro BIND, 1 den pro Unbound

- útok byl nejspíše cílený na slabě zabezpečeného registrátora
- znefunkčnění DNS blacklistu nejspíše nebyl cíl, ale **vedlejší efekt**
- registrátor je hodně podezřelý a nedůvěryhodný
 - zvláště po incidentu
 - vhodné přemigrovat jinam, pokud nejsou k registrátorovi jiné vazby
- únosy IP adres se zřejmě nestávají
 - což je dobrá zpráva

Root.cz: Za výpadek známého blacklistu mohla unesená doména

Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<https://Ondrej.Caletka.cz>



Prezentace je již nyní k dispozici ke stažení.