

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO



**GHID CU PRIVIRE LA DETECȚIA ȘI REMEDIEREA
ATACURILOR DE TIP "DNS AMPLIFICATION"**

Versiunea 1.0 – 10 iulie 2013

- Pagină albă -

Cuprins

1. INTRODUCERE	5
2. DESCRIEREA ATACULUI.....	5
3. METODE DE DETECȚIE	5
4. METODE DE REMEDIERE	6
BIBLIOGRAFIE:	10

- Pagină albă –

1. INTRODUCERE

Un atac „DNS amplification” este o formă populară de atac de tip DDoS (Distributed Denial of Service) care se bazează pe utilizarea unor servere de tip „open recursive DNS resolver”, accesibile în mod public, pentru a supraîncărca un sistem informatic victimă cu trafic de tip răspuns DNS.

2. DESCRIEREA ATACULUI

Serverele de tip „open recursive DNS resolver” sunt de obicei servere DNS legitime care însă au fost configurate în mod necorespunzător să răspundă la cererile recursive provenite de la orice sistem, în loc să restrângă răspunsurile doar la sistemele informatice locale sau cele autorizate în mod explicit.

Tehnica de bază utilizată constă în transmiterea de către un atacator, către un server de tip „open recursive DNS resolver”, a unei cereri de tip „DNS name lookup” special astfel încât să conțină adresa IP a victimei ca și adresă IP sursă creată (tehnică denumită „spoofing”). Astfel, răspunsul serverului DNS la cererea primită este transmis către adresa IP a sistemului victimă, chiar dacă în realitate sistemul respectiv nu a făcut o astfel de cerere DNS. Deoarece mărimea unui astfel de răspuns este de obicei considerabilă mai mare decât cea a cererii, atacatorul este în măsură să amplifice volumul de trafic îndreptat către sistemul victimă prin transmiterea unui număr cât mai mare de cereri.

Adesea atacatorii utilizează sisteme informatice infectate, care fac parte dintr-o rețea botnet controlată de aceștia, pentru a transmite cât mai multe cereri DNS de tipul celor menționate anterior. Astfel, atacatorul poate genera o cantitate impresionantă de trafic direcționat către sistemul victimă, obținând astfel supraîncărcarea acestuia și implicit blocarea serviciilor oferite de acesta (Denial of Service).

Dificultatea blocării unor astfel de atacuri constă în faptul că traficul generat prin tehnica descrisă anterior este văzut de sistemul victimă ca trafic legitim provenit de la servere DNS valide.

3. METODE DE DETECȚIE

Deși prevenirea unor astfel de atacuri este destul de dificilă, operatorii de rețea pot implementa totuși câteva strategii de diminuare a afectelor unor astfel de atacuri. Un prim obiectiv, ce poate fi considerat și ca o soluție eficientă pe termen lung, este detectarea și eliminarea sistemelor de tip „open recursive DNS resolver”, reducând astfel numărul potențialelor resurse pe care un atacator le poate utiliza în cadrul unui atac de acest tip.

3.1. Indicatori utilizați pentru detecție

Într-o cerere DNS recursivă tipică, un sistem client transmite o cerere către un server DNS local prin care solicită rezolvarea unui nume de domeniu („domain name resolution”) sau rezolvarea inversă a unei adrese IP („IP reverse resolution”). Serverul DNS local transmite mai departe cererea DNS în numele clientului și răspunde printr-un pachet de date care conține informația solicitată de client sau un mesaj de eroare.

Specificațiile DNS nu permit răspunsuri DNS nesolicitate și astfel un indicator cheie în detecția sistemelor de tip „open recursive DNS resolver” îl reprezintă detecția unor răspunsuri DNS pentru care nu există cererile DNS aferente.

Mai multe organizații oferă unelte gratuite de scanare a unei rețele pentru identificarea serverelor DNS vulnerabile precum cele de tip „open recursive DNS resolver”. Printre acestea enumerăm:

- Open DNS Resolver Project, <http://openresolverproject.org/>;
- The Measurement Factory, <http://dns.measurement-factory.com/>;
- DNSInspect, <http://www.dnsinspect.com/>.

Conform datelor publicate pe site-ul web al Open DNS Resolver Project, din cele peste 33 de milioane de servere din Internet care răspund într-o anumită măsură la cereri DNS recursive, aproximativ 28 de milioane reprezintă o amenințare semnificativă (date valabile la 26.05.2013).

4. METODE DE REMEDIERE

În cele ce urmează se regăsesc diferite tehnici ce pot fi utilizate pentru reducerea eficienței unor atacuri, informațiile de configurare fiind limitate la servere DNS de tip BIND9 și Microsoft DNS Server, fiind 2 tipuri de servere DNS cu răspândire largă. Pentru servere DNS de alt tip se recomandă studierea detaliilor de configurare din cadrul documentației puse la dispoziție de producător.

4.1. Verificarea adresei IP sursă

Având în vedere că cererile DNS transmise de către atacator conțin ca și sursă adrese IP ale sistemelor informatice țintă („spoofing”), prima măsură pentru reducerea eficienței atacului de tip „DNS amplification” este filtrarea de către ISP a traficului DNS către adresele IP țintă.

Organizația „Network Working Group of the Internet Engineering Task Force” a emis un document de tip „Best Current Practice” (<http://tools.ietf.org/html/bcp38>) în Mai 2000 în care este descris modul în care un ISP poate filtra traficul în cadrul propriei rețele prin blocarea pachetelor pentru care adresa IP sursă nu este accesibilă prin intermediul traseului de rețea extras din pachetul respectiv. Astfel, un dispozitiv de rețea cu rol de rutare a traficului va testa dacă poate comunica cu adresa IP sursă din cadrul unui pachet prin intermediul aceleiași interfețe prin care a sosit

pachetul. Dacă comunicarea nu este posibilă, este evident că pachetul respectiv are ca sursă o adresa IP „spoofată” (setată în mod intenționat de atacator).

4.2. Dezactivarea recursivității pentru serverele DNS autoritare („Authoritative Name Servers”)

Multe dintre serverele DNS din Internet la momentul actual sunt destinate exclusiv furnizării serviciului de rezolvare de nume pentru un singur domeniu. Aceste sisteme nu necesită să suporte rezolvarea altor domenii în numele unui client și în consecință trebuie configurate cu dezactivarea recursivității.

4.2.1. Bind9

Adăugați următoarele linii în opțiunile globale:

```
options {  
    allow-query-cache { none; };  
    recursion no;  
};
```

Pentru detalii suplimentare vizitați:

<http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch03.html#id2567992>

4.2.2. Microsoft DNS Server

Utilizând consola Microsoft DNS parcurgeți următorii pași:

1. Executați click dreapta pe serverul DNS și accesați „Properties”;
2. Selectați secțiunea „Advanced”;
3. În secțiunea „Server options” bifați opțiunea „Disable recursion” și apoi click pe „OK”.

4.3. Limitarea recursivității la clienții autorizați

Serverele DNS din cadrul unei organizații sau ISP ar trebui să fie configurate astfel încât să transmită cereri recursive doar în numele unor sisteme client autorizate. Aceste cereri, în mod normal, ar trebui să sosească de la sisteme client din spațiul de adrese IP alocat organizației.

4.3.1. Bind9

Adăugați următoarele linii în opțiunile globale:

```
acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };
options {
    allow-query { any; };
    allow-recursion { corpnets; };
};
```

Pentru detalii suplimentare vizitați:

http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access_Control_Lists

4.3.2. Microsoft DNS Server

În momentul de față, în sistemele Microsoft DNS Server, nu este posibilă restricționarea cererilor DNS la un spațiu de adrese IP . Pentru a obține totuși un rezultat aproximativ echivalent trebuie utilizat un alt server DNS, de tip „caching-only”, pentru a furniza serviciul de rezolvare recursivă. Apoi trebuie creată o regulă de firewall care să blocheze traficul din afara rețelei organizației către serverul DNS de tip „caching-only”. Serviciul de server DNS autoritar („authoritative name server”) va trebui să fie găzduit pe un server separat, însă configurat prin dezactivarea recursivității conform ghidului de la secțiunea secțiunea 3.2.2. de mai sus.

4.4. Limitarea ratei de răspuns (Response Rate Limiting - RRL) pentru serverele DNS recursive

În momentul de față există o facilitate experimentală, sub forma unui set de patch-uri pentru BIND9, care-i conferă administratorului posibilitatea de a limita numărul maxim de răspunsuri pe secundă ce se transmit către un sistem client de la serverul DNS. Această funcționalitate este destinată a fi folosită doar pentru serverele DNS autoritare deoarece ar afecta performanța celor recursive.

Pentru o protecție eficientă se recomandă ca serverele DNS autoritare să fie găzduite pe mașini diferite de cele pe care sunt găzduite serverele DNS recursive, cu implementarea RRL pe cele autoritare și configurarea de liste de control acces (Access Control Lists - ACL) pe cele recursive.

4.4.1. Bind9

În momentul de față sunt disponibile patch-uri pentru 9.8.latest și 9.9.latest care oferă suport pentru RRL în sistemele UNIX. Într-o implementare BIND9 care rulează patch-urile RRL introduceți următoarele linii în blocul de opțiuni corespunzător perspectivei autoritare:

```
rate-limit {  
    responses-per-second 5;  
    window 5;  
};
```

4.4.2. Microsoft DNS Server

Această opțiune nu este disponibilă la momentul actual pentru sistemele Microsoft DNS Server.

ATENȚIE! Implementarea RRL pentru răspunsurile DNS poate împiedica un sistem client să primească răspunsuri la cererile DNS. Acest fapt crește expunerea sistemului client respectiv la atacuri de tip „DNS cache poisoning”.

BIBLIOGRAFIE:

1. <https://www.us-cert.gov/ncas/alerts/TA13-088A>;
2. <http://www.team-cymru.org/Services/Resolvers/instructions.html>;
3. <http://openresolverproject.org/>;
4. <http://tools.ietf.org/html/rfc1034>;
5. <http://tools.ietf.org/html/bcp38>;
6. <http://dns.measurement-factory.com/>;
7. <http://www.dnsinspect.com/>;
8. <http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch03.html#id2567992>;
9. [http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access Control Lists](http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access_Control_Lists).