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

- 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

Severele 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 conţină adresa IP a victimei ca şi 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 reţea botnet controlată de aceştia, pentru a transmite cât mai multe cereri DNS de tipul celor menţionate anterior. Astfel, atacatorul poate genera o cantitate impresionantă de trafic direcţionat către sistemul victimă, obţinând astfel supraîncărcarea acestuia şi 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

Deşi prevenirea unor astfel de atacuri este destul de dificilă, operatorii de reţea pot implementa totuşi câteva strategii de diminuare a afectelor unor astfel de atacuri. Un prim obiectiv, ce poate fi considerat şi ca o soluţie eficace pe termen lung, este detectarea şi eliminarea sistemelor de tip „open recursive DNS resolver”, reducând astfel numărul potenţialelor resurse pe care un atacator le poate utiliza în cadrul unui atac de acest tip.

3.1. Indicatori utilizaţi pentru detecţie

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 şi răspunde printr-un pachet de date care conţine informaţia solicitată de client sau un mesaj de eroare.

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

Mai multe organizaţii oferă unelte gratuite de scanare a unei reţele pentru identificarea serverelor DNS vulnerabile precum cele de tip „open recursive DNS resolver”.

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 ameninţare 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 eficientei unor astfel de atacuri, informaţiile de configurare fiind limitate la servere DNS de tip BIND9 şi 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 documentaţiei puse la dispoziţie de producător.

4.1. Verificarea adresei IP sursă

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

Organizaţia „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 reţele prin blocarea pachetelelor pentru care adresa IP sursă nu este accesibilă prin intermediul traseului de reţea extras din pachetul respectiv. Astfel, un dispozitiv de reţea cu rol de rutare a traficului va testa dacă poate comunica cu adresa IP sursă din cadrul unui pachet prin intermediul aceleiaşi interfeţe 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 intenţionat de atacator).

4.2. Dezactivarea recursivităţii 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 şi în consecinţă trebuie configurate cu dezactivarea recursivităţii.

4.2.1. Bind9

Adăugaţi următoarele linii în opţiunile globale:

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

Pentru detalii suplimentare vizitaţi:
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 parcurgeţi următorii paşi:

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 recursivităţii la clienţii autorizaţi

Serverele DNS din cadrul unei organizaţii 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 spaţiul de adrese IP alocat organizaţiei.

4.3.1. Bind9

Adăugaţi următoarele linii în opţiunile globale:

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

Pentru detalii suplimentare vizitaţi:
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 faţă, în sistemele Microsoft DNS Server, nu este posibilă restricţionarea cererilor DNS la un spaţiu de adrese IP . Pentru a obţine totuşi 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 reţelei organizaţiei 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 recursivităţii conform ghidului de la secţiunea secţiunea 3.2.2. de mai sus.

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

În momentul de faţă 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 funcţionalitate este destinată a fi folosită doar pentru serverele DNS autoritare deoarece ar afecta performanţa celor recursive.

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

4.4.1. Bind9

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

```
rate-limit {
```

```
    responses-per-second 5;
window 5;
};
```

4.4.2. Microsoft DNS Server

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

ATENŢIE!: Implementarea RRL pentru răspunsurile DNS poate împiedica un sistem client să primească răspunsuri la cererile DNS. Acest fapt creşte expunerea sistemul 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/Open-Resolver-Challenge.html;
3. http://tools.ietf.org/html/rfc1034;
4. http://tools.ietf.org/html/bcp38;
5. http://dns.measurement-factory.com/;
6. http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch03.html#id2567992;
7. http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access_Control_Lists.