DNS Amplification

حمله DNS Amplification

سیستم های مورد حمله :

سرورهای DNS(Domain Name System)

مقدمه :

در روزهای اخیر گزارشی از یک CERT بین المللی در مورد یک حمله DNS Amplification از طریق یک DNS آسیب پذیر در کشور به سیستم های آن کشورگزارش گردیده است. جهت آشنایی با این نوع حملات، در ادامه به بررسی این حمله و روش های جلوگیری و مقابله با آن می پردازیم.

حمله DNS Amplification چیست؟

حمله DNS Amplification یک فرم معمول از حمله انکار سرویس توزیع شده (DDoS) است که مبتنی بر استفاده عمومی از سرورهای open DNS برای ارسال ترافیک بسیار بالای پاسخ به DNS به سیستم های قربانی است. تکنیک اصلی مهاجم این است که درخواست lookup از DNS را به سرور open DNS با آدرس مبدا جعلی(spoofشده) به عنوان آدرس هدف ارسال می کند. وقتی سرور DNS رکوردهای پاسخ DNS را ارسال می کند، همه آنها به هدف می رسد. مهاجم معمولاً درخواستی را انتخاب می کند که اطلاعات zone آن آنچنان زیاد باشد که اثر amplification را تشدید کند. در بیشتر موارد بررسی شده درخواست های spoof شده توسط مهاجم بصورت ANY انتخاب می شود. که به این معناست که تمامی اطلاعات شناخته شده در مورد یک DNS zone در یک درخواست ساده برگردانده می شود. بدلیل آنکه سایز جواب در مقایسه با درخواست ارسال شده بسیار بیشتر است، لذا مهاجم قادر است مقدار ترافیک ارسالی به سمت قربانی را افزایش دهد. با نفوذ به یک بات نت و تولید تعداد زیادی درخواست DNS، spoofشده مهاجم قادر است مقدار بسیار زیادی از ترافیک را با یک تلاش کوچک ایجاد نماید. به علاوه چون پاسخ ها در حقیقت داده های قانونی از سرورهای معتبر هستند، جلوگیری از این نوع حملات بسیار مشکل است. درحالی که متوقف کردن این گونه حملات بسیار دشوار است، اپراتورهای شبکه با استراتژی های گوناگون، می توانند اثر آن را کاهش دهند.

تاثیر

عدم پیکربندی درست سرورDNS، می تواند موجب سوء استفاده از آن در حملات DDoS گردد.

راه حل

روش شناسایی

این مشکل را مشخصاً نمی توان به عنوان آسیب پذیری در حملات بازتابی[1] DNS شناخت، بلکه در حقیقت عدم پیکربندی مناسب در سرورهای DNS است. در این زمینه گزینه های مختلفی برای تشخیص open recursive resolvers وجود دارد. تعدادی سازمان ها و شرکت‌های معتبر امنیتی ابزارهای اسکن مبتنی بر وب و رایگان را برای جستجوی یک شبکه و شناسایی open DNS resolver پیشنهاد کرده اند. این ابزارها تمامی محدوده شبکه را اسکن و آدرس هر open resolver شناسایی شده را لیست می کنند.

- **پروژه Open DNS Resolver**

http://openresolverproject.org

پروژه Open DNS Resolver لیستی از سرورهای DNS که به عنوان Open Resolver های قابل دسترس در سطح جهان شناخته شده اند، را تهیه کرده است. اینترفیس این سایت به مدیران شبکه اجازه می دهد تا محدوده IP را در قالب CIDR وارد نمایند[1].

- **Measurement Factory**

http://dns.measurement-factory.com

مانند پروژه Open DNS Resolver، Measurement Factory نیز لیستی از سرورهای DNS قابل دسترس در اینترنت را تهیه کرده است و به مدیران شبکه اجازه می دهد تا openهای recursive resolver را جستجو کنند [2].

به علاوه این شرکت یک ابزار رایگان را برای تست یک DNS resolver پیشنهاد کرده است تا مشخص کند، آیا یک سرور اجازه open recursion می دهد یا نه. این ابزار مدیران شبکه را برای تعیین لزوم تغییرات در سرور یا درست بودن تغییرات انجام شده در پیکربندی یاری می رساند.[4,3].

- **DNSInspect**

http://www.dnsinspect.com

این سایت نیز مانند سایت های دیگر ذکر شده، برای ارزیابی یک resolver خاص برای آسیب پذیری ذکر شده بکار می رود، اما توانایی تست کل DNS Zone برای دیگر پیکربندی های ممکن و موارد امنیتی آن را نیز دارد[5].

کاهش اثرات

[1] reflection

متاسفانه با توجه به حجم بالای ترافیک ایجاد شده در این نوع حملات، در سیستم های با مقیاس بزرگ اغلب شانس کمی برای فرار قربانی از حمله DDoS باقی خواهد ماند.

با وجود اینکه تنها راه حل موثر در خصوص حل مشکل حملات این چنینی، حذف DNS های نا امن می باشد اما این کار تلاش و همکاری ارگان های بسیاری را نیازمند می باشد – بر طبق گزارش پروژه ی Open DNS Resolver از ۲۷ میلیون DNS شناخته شده تقریبا ۲۵ میلیون، حداقل یک تهدید استفاده شده در حملات را داشته اند- با این حال چندین روش جهت کاهش مخاطرات این دسته حملات موجود می باشد از جمله آنها می توان به لینک های تنظیمات تهیه شده جهت ایجاد تغییرات توصیه شده برای کمک به مدیران شبکه ها اشاره نمود[1]. لازم به ذکر است این تنظیمات تنها برای سرورهای DNS پرکاربرد در شبکه ها یعنی BIND9 و Microsoft تهیه گردیده است، در صورتی که شما از سرور DNS دیگری استفاده می نمایید از مستندات تهیه شده توسط سازنده خود، جهت انجام تنظیمات اقدام نمایید.

- **تایید و بازبینی آدرس IP مبدا**

از آنجایی که درخواست ارسالی به DNS توسط مهاجمین، نیازمند داشتن آدرس IP ساختگی به منظور شبیه سازی سیستم قربانی می باشد، اولین گام جهت کاهش موثر این تهدید فیلترینگ آدرسهای تقلبی توسط ISP ها می باشد که مستندات نحوه ی فیلترینگ آدرسهای تقلبی برای ISP ها در سالهای ۲۰۰۰ و ۲۰۰۴ ارائه گردیده است. تغییرات توصیه شده در این مستند بررسی آدرسهای مبدا توسط روترها می باشد[7].

- **غیرفعال نمودن recursion در سرورهای اختصاصی DNS**

برخی از سرورهای DNS بر روی اینترنت منحصراً جهت یک دامین مشخص تنظیم گردیده اند، پس در این موارد نیازی به فعال بودن گزینه ی Recursion نخواهیم داشت.

- **BIND9**

گزینه های زیر را در Global Options اضافه نمایید[8].

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

- **Microsoft DNS Server**

در Microsoft DNS console Tool مراحل زیر را انجام دهید [9]:

۱- بر روی DNS server راست کلیک نموده و properties را انتخاب نمایید.
۲- بر روی Advanced Tab کلیک کنید.
۳- در بخش Server options گزینه ی Disable recursion را انتخاب و Ok نمایید.

- **محدود کردن recursion برای کاربران مجاز**

برای سرورهای DNS که درون یک سازمان یا ISP بکار گرفته می شوند، resolver تنها باید برای انجام درخواست های بازگشتی از طرف کاربران مجاز پیکربندی شود. این درخواست ها بایستی فقط از کاربران درون محدوده آدرس شبکه سازمان باشد. لذا پیشنهاد می شود که مدیران شبکه recursion را محدو د به کاربران درون سازمان خود نمایند.

- **BIND9**
  - گزینه های زیر را در Global Options اضافه نمایید[10]:

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

- **Microsoft DNS Server**

در حال حاضر امکان محدود کردن درخواست های DNS برای یک محدوده آدرس خاص وجود در سرور DNS ماکروسافت وجود ندارد. برای نزدیک کردن عملکرد لیست های کنترل دسترسی BIND، یک caching-only name server متفاوت بایستی برای تامین recursive resolution راه اندازی گردد. لذا برای این کار بایستی یک rule در فایروال جهت بلوکه کردن دسترسی ورودی از شبکه خارج از سازمان به سمت caching-only server ایجاد گردد. اما برای سرویس دهی به عنوان authoritative name server لازم است که روی سرور جداگانه ای host شود ولی قابلیت recursion همان طور که در قبل ذکر شد، غیرفعال نمایید.

- **محدود سازی زمان پاسخ (RRL)[۲]**

در حال حاضر این مورد یک ویژگی آزمایشی بر روی سرورهای BIND9 می باشد که بصورت مجموعه ای از وصله ها[۳] در دسترس می باشند که به مدیر شبکه قابلیت محدود سازی حداکثر تعداد پاسخ های ارسالی به یک کلاینت از سمت سرور را می دهد[11].

نحوه ی انجام تنظیمات :

- **BIND9**

۱- وصله های موجود برای سرور BIND9 را نصب نمایید. (BIND9 9.10 or later)

۲- موارد ذیل را در بلاک options در authoritative-only اضافه نمایید[12].

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

[۲] Response Rate Limiting (RRL)

[۳] patches

- **Microsoft DNS Server**

این گزینه فعلاً در سرور DNS ماکروسافت وجود ندارد.

توجه: RRL در پاسخ های DNS ممکن است موجب شود میزبان های قانونی ، پاسخی دریافت نکنند. در چنین میزبان هایی احتمال افزایش ریسک حملات DNS cache poisoning بیشتر خواهد بود.

References

- [1] http://openresolverproject.org/
- [2] http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl
- [3] http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl
- [4] http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/latest.html
- [5] http://www.dnsinspect.com/
- [6] http://tools.ietf.org/html/rfc1034
- [7] http://tools.ietf.org/html/bcp38
- [8] Chapter 3. Name Server Configuration
- [9] http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch03.html#id2567992
- [10] http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access_Control_Lists
- [11] http://ss.vix.su/~vixie/isc-tn-2012-1.txt
- [12] http://www.redbarn.org/dns/ratelimits
- [13] http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/latest.html
- [14]http://technet.microsoft.com/en-us/library/cc754941.aspx
- [15] https://www.us-cert.gov/ncas/alerts/TA13-088A