بسم الله الرحمن الرحیم

عنوان تحقیق

DNS Security & Sockets & Cashes

استاد محترم :جناب آقای مهندس منصوری

نگارنده : یوسف رشیدی

جهت درس: MCSA 2016

مجتمع فنی تهران

هدف کلی تحقیق

امنیـــت در DNS (DNS Security)

اهداف جزئی

۱. آشنایی با Zone file compromise

۲. آشنایی با Zone information leakage

۳. آشنایی با Compromised dynamic updates

۴. آشنایی با DNS client flooding (denial of service)

۵. آشنایی با Cache poisoning

۶. آشنایی با DNS Cache

۷. آشنایی با DNS Socket Pool

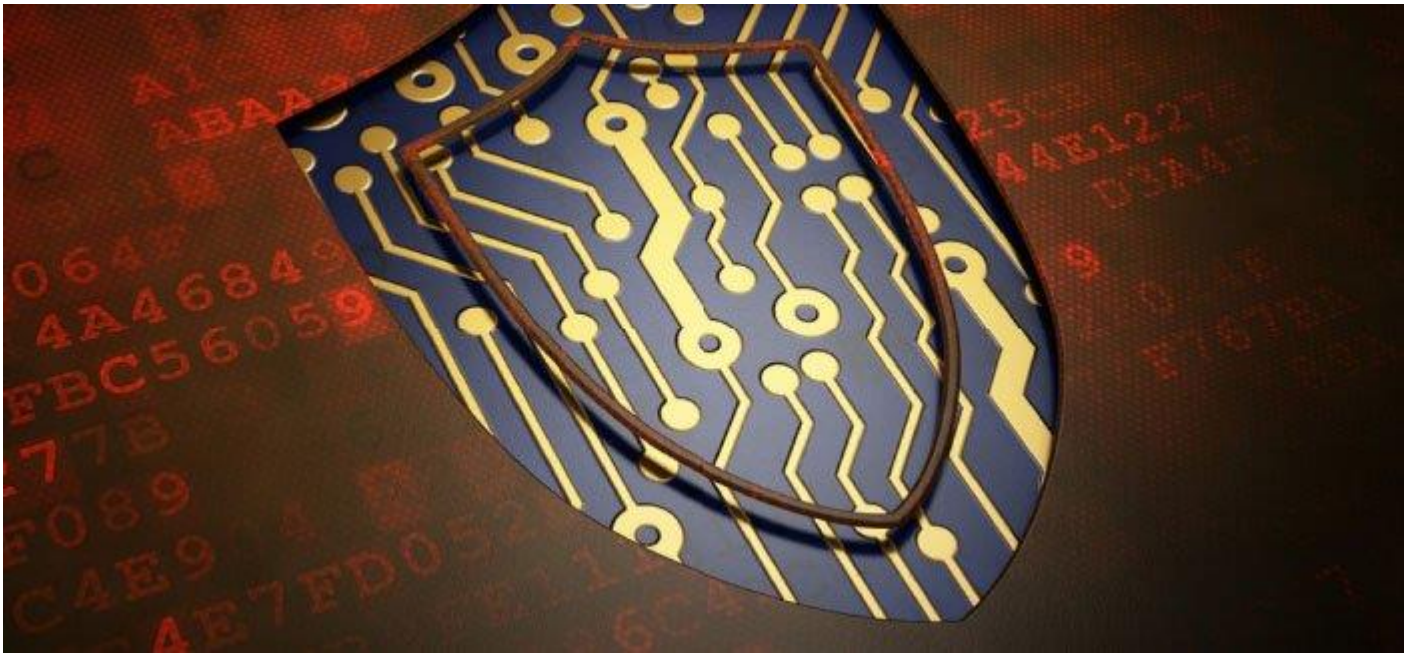
۸. آشنایی با Free DNS Servers

۹. آشنایی با Fishing Attack

هدف کاربردی

آشنایی با انواع حمله به سرور DNS و کارایی کش DNS در سرعت

امنیـت در DNS (DNS Security)



مقدمه

بسیاری از کاربران و نه تمام آن‌ها با مفاهیم امنیت نرم‌افزار آشنا هستند، اما راه‌های پایه‌ای بیش‌تری برای محافظت از کاربر در مقابل حملاتی چون فیشینگ، بات‌نت‌ها، تبلیغات ناخواسته و مواردی از این دست وجود دارد. یکی از مؤثرترین آن‌ها سرویس‌های DNS است. استفاده از تنها یکی از این خدمات می‌تواند از خانواده یا کسب و کار شما در مقابل حملات فیشینگ و سایر نفوذهای ناخواسته حفاظت کند.

فرآیند تبدیل نام دامنه به IP متناظر با آن را Domain name resolution می‌نامند. به‌طور کلی، دو نوع اصلی از DNS سرورها وجود دارند؛ Recursive و Authoritative. از این دو نوع، معمولاً از DNS سرورهای Recursive برای شرکت‌ها و سازمان‌های کوچک استفاده می‌شود.

اغلب فراهم‌کنندگان خدمات اینترنت (ISP یا Internet Service Providers) نیز از همین نوع DNS سرورها استفاده می‌کنند. تمام شرکت‌هایی که در این مقاله به بررسی آن‌ها خواهیم پرداخت نیز از سرورهای Recursive استفاده می‌کنند. اگرچه در میان آن‌ها برخی دیگر از شرکت‌ها هستند که از نوع دیگر DNS سرورها یا سرورهای Authoritative استفاده می‌کنند که به دارندگان وب‌سایت‌ها یا شرکت‌های ارائه خدمات میزبانی این امکان را می‌دهد تا یک IP برای وب سرور خود ایجاد کنند و دامنه آن‌ها برای مدیریت تنظیمات DNS به این IP اشاره کند.

از آنجا که DNS سرورها نقش واسطی را میان مرورگر و محتویات وب سایت بازی می‌کنند، بسیاری از خدمات DNS دیگر هستند که می‌توانند خدمات بیش‌تری را هم به کاربر و هم به مدیران شبکه ارائه دهند. خدماتی که نمونه‌هایی از آن در ادامه آورده شده است.

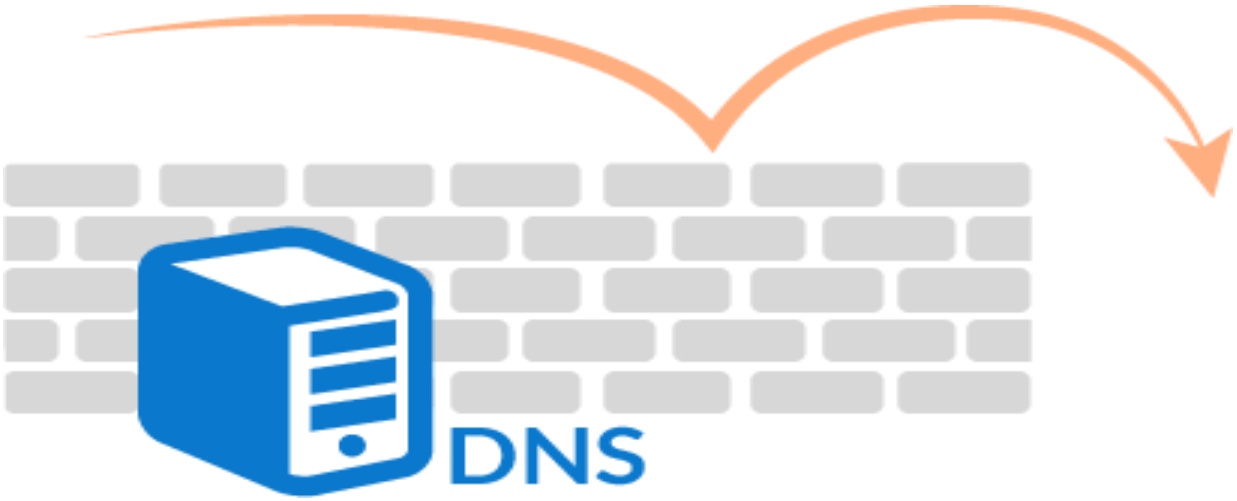
1. **فیلتر کردن داده‌ها : می‌توان به‌راحتی از این ابزار برای فیلتر کردن سایت‌های هرزه نگاری و سایر داده‌های ناخواسته و نامناسب استفاده کرد، بدون این‌که به نرم‌افزار خاصی روی کامپیوترهای کاربران نیازی داشته باشیم.**
2. **مسدود کردن بدافزارها و حملات فیشینگ: می‌توان این کار را با فیلتر کردن داده نیز انجام داد و سایت‌هایی را که ویروس، اسکمرها و سایر داده‌های خطرناک دارند، فیلتر کرد.**
3. **محافظت در مقابل بات نت ها: این سرویس می‌تواند ارتباطات ناخواسته را که اغلب بات نت با سرور مولد خود دارد مسدود کند؛ بنابراین، کمک زیادی به ارتقای امنیت کاربر می‌کند.**
4. **مسدود کردن تبلیغات: در واقع، این نیز نوع دیگری از فیلتر کردن داده‌ها است که می‌توان آن را با استفاده از برخی سرویس‌های DNS انجام داد.**

همانطور که می دانید DNS یکی از سرویس‌های زیرساختی شبکه‌های کاربردی به شماره می‌رود. بطوری که نبود این سروریس و یا اختلال در کارکرد آن به راحتی می‌تواند ارتباطات درون شبکه و برون شبکه‌ای را مختل سازد. وظیفه اصلی DNS تبدیل نام به آدرس IP است چرا که در دنیای انسانی از یک طرف ارتباطات بر اساس نام صورت می‌پذیرد و از سویی دیگر به خاطر سپردن نام‌ها بسیار ساده‌تر از آدرس‌های IP است.

بنابراین از سرویسی استفاده خواهیم کرد که آگاهی کاملی از تمامی نام‌های موجود در شبکه به همراه آدرس‌های آی‌پی آنها داشته باشد و بتواند درخواست‌های مورد نظر در خصوص تبدیل و ترجمه نام به آدرس آی‌پی را به درستی انجام دهد. کمی به جمله قبل دقت کنید: "سرویسی که آگاهی کاملی از نام‌ها و آدرس‌های IP موجود در شبکه دارد" دقیقا به همین دلیل که DNS از تمامی نام‌ها (اعم از نام‌های سرور و نام‌های کلاینت) و آدرس‌های آی‌پی آگاه است امنیت آن نیز مهم و حیاتی جلوه می‌کند.

این سرویس مهم در صورت بروز شکست امنیتی، برای نفوذگران اطلاعات مهمی را در بر خواهد داشت:

۱. ساختار آدرس‌های IP و آدرس‌های IP فعال
۲. آدرس‌های IP سرویس‌های حساس و حیاتی شبکه و نیز اسامی آنها
۳. هدایت ترافیک شبکه به مقصدی خاص با وارد نمودن اسم و آدرس تقلبی
۴. استفاده از آدرس‌های سایر افراد در شبکه در جهت مقاصد غیر قانونی
۵. ایجاد اختلال در سرویس و یا توقف آن به منظور مختل نمودن ارتباطات شبکه



DNS service and its security

با توجه به مقدمه بالا بنابراین آشنایی با خطراتی که سرویس DNS را تهدید می‌کند و نحوه رفع این خطرات و در نهایت ایمن‌سازی سرویس DNS امری مهم به نظر می‌رسد. پیش از آنکه به بحث امنیت در سرویس DNS بپردازیم ابتدا به خطرات موجود اشاره می‌کنیم:

- Zone file compromise
- Zone information leakage
- Compromised dynamic updates
- DNS client flooding (denial of service)
- Cache poisoning

Zone File Compromise

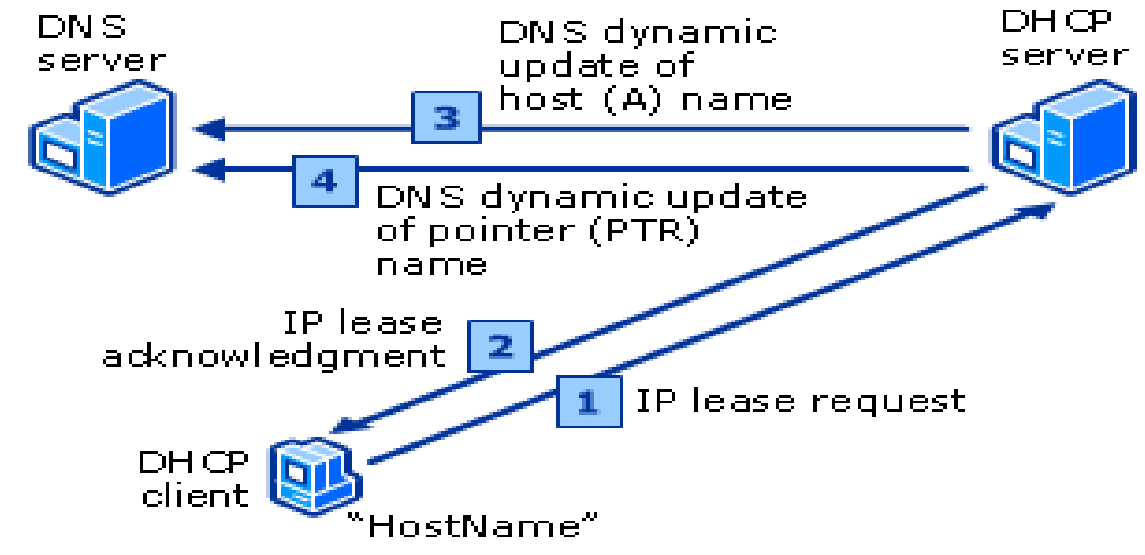
در ساختار DNS مبتنی بر ویندوزهای سرور، سرویس دهنده DNS حاوی یک Zone یا ناحیه‌ای است که مسئول معتبر پاسخ‌دهی در آن ناحیه محسوب می‌شود. به عبارت دیگر این Zone حاوی اطلاعات و یا رکوردهایی است که نشانگر نام و آدرس IP کامپیوترهای داخل شبکه خواهد بود. بطور پیش‌فرض Administrator می‌تواند سرویس DNS را با استفاده از کنسول مدیریتی آن و یا دستور متناسب مدیریت نموده و Resource Recordها را ویرایش

نماید. یکی از خطراتی که ساختار DNS را تهدید می‌کند این است که نفوذگر بتواند مستقیماً و یا از راه دور به کنسول مدیریتی DNS دسترسی پیدا کرده و آن را به دلخواه خود تغییر دهد. نکته مهم امنیتی در این بخش این است که سرویس DNS تنها برای افراد دارای صلاحیت (Authorized) فعال بوده و سایر افزاد مجوز دسترسی به آن را نداشته باشند. این مجوز دسترسی بهتر است هم بصورت لوکال و هم بصورت ریموت و نیز برای کاربر و حتی ماشین تعریف گردد.

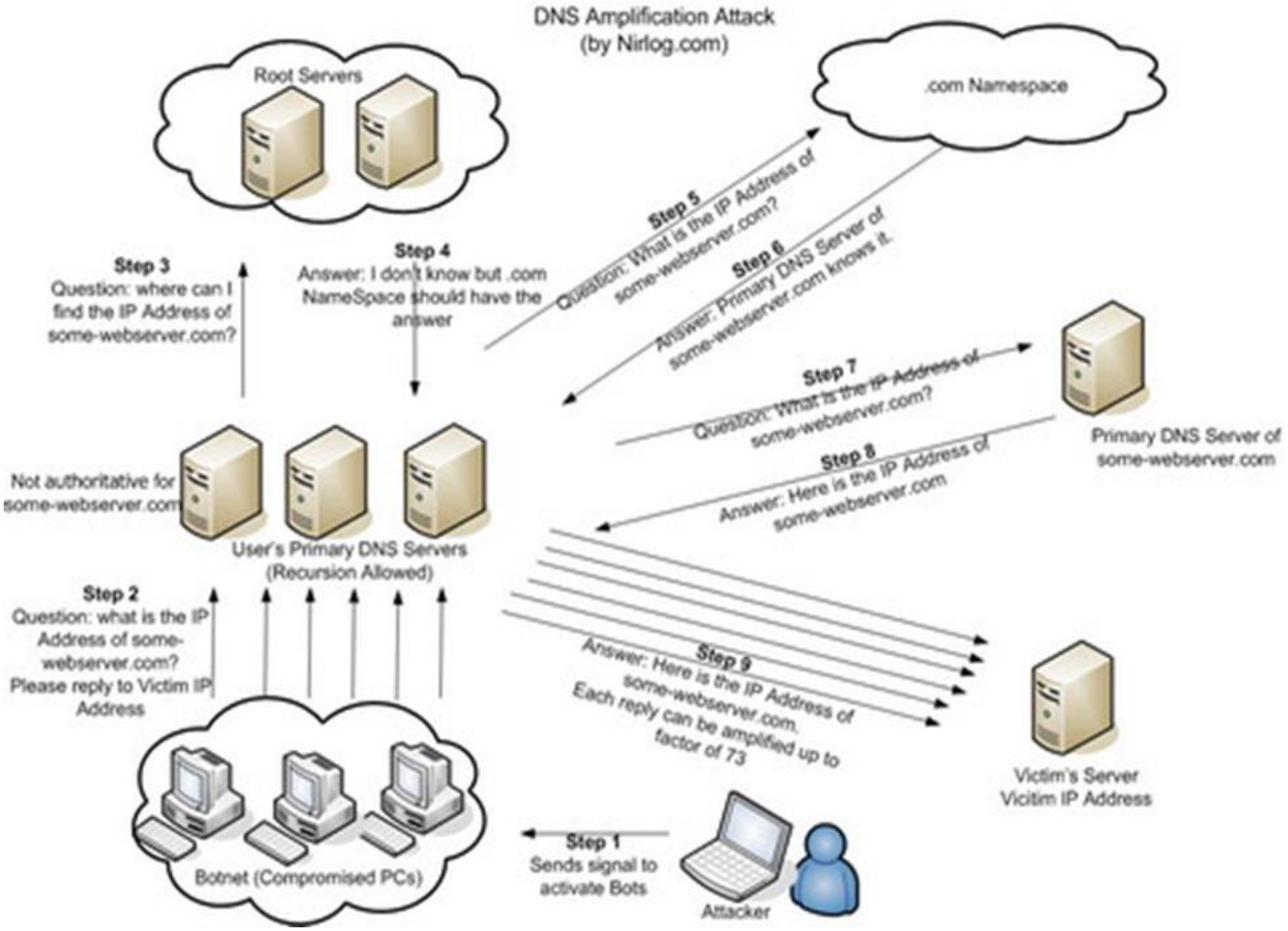
Zone Information Leakage

Zone در یک DNS حاوی اسامی کامپیوترها و آدرس‌های IP متناظر با آنهاست. این Resource Recordها فارغ از این که بصورت دستی در DNS ثبت شده باشند و یا اینکه ثبت آنها با استفاده از Dynamic Update باشد می‌تواند اطلاعات مهمی‌را در اختیار نفوذگر قرار دهند. نشت اطلاعات از Zone زمانی اتفاق می‌افتد که نفوذگر بتواند بر اساس نام یک سرور به Role یا نقش آن در شبکه پی ببرد. به عنوان مثال DCSRV می‌تواند نامی باشد که به سرور Domain Controller اشاره دارد. مسلم است که این اطلاعات ساده می‌تواند به نفوذگر در اقدامات بعدی کمک موثری داشته باشد! نفوذگر به طرق مختلفی می‌تواند اسامی کامپیوترهای موجود در شبکه را بدست آورد. بعنوان مثال چنانچه Zone Transfer بر روی سرور DNS فعال باشد مکانیسم تبادل Zone براحتی می‌تواند اطلاعات شما را در اختیار نفوذگر قرار دهد. حتی اگر Zone Transfer نیز فعال نباشد اما نفوذگر کمی‌حوصله کار داشته باشد می‌تواند بر اساس Queryهایی از نوع Reverse DNS به ساختار نام شبکه دسترسی پیدا کند. در کنار این موضوع، آگاهی از آدرس‌های IP فعال در شبکه نیز می‌تواند نفوذگر را در کار خود چند قدمی به جلو حرکت دهد. به عنوان مثال دیگر نیازی نیست Range زیادی از آدرس‌های IP را برای آگاهی از آدرس‌های فعال اسکن کند. همچنین با آگاهی از آدرس‌های IP غیر فعال می‌تواند با استفاده از همان آدرس‌ها سرویس‌های تقلبی به نفع خود در شبکه راه اندازی کند.

Compromised Dynamic Updates

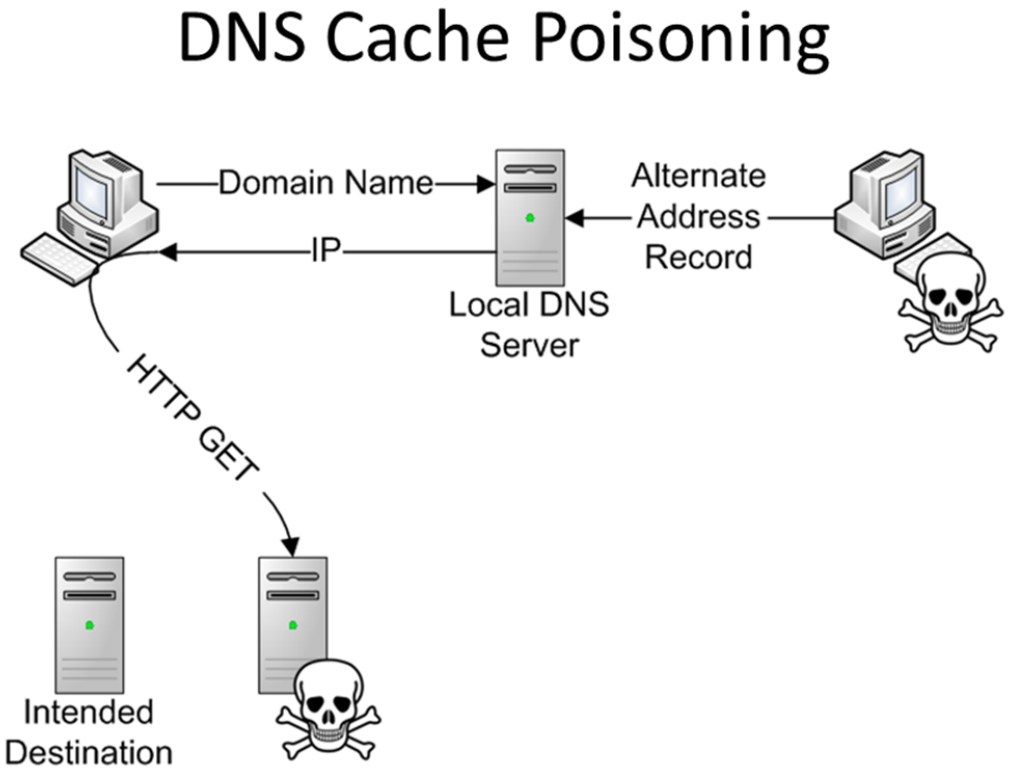


همانطور که می‌دانید DNS Dynamic Update مزیت بسیار بزرگی برای راهبران شبکه محسوب می‌شود چراکه این راحتی را در اختیار راهبر قرار می‌دهد که بدون نیاز به ثبت اسامی و آدرس‌های IP کامپیوترها بصورت دستی، ثبت و به روز رسانی آنها بصورت پویا و اتوماتیک صورت پذیرد. بطور کلی Dynamic Update به دو صورت Secure و Unsecure انجام می‌شود. در حالت ایمن، کلاینت موظف است عملیات Authentication را (مثلا با استفاده از نام کامپیوتر خود که پیش از این در Active Directory ثبت شده است) انجام دهد. در حالت غیر ایمن نیز عملیات Authentication انجام نمی‌شود و هر کلاینتی می‌تواند رکورد خود را در DNS ثبت نماید. البته این را نیز باید بدانید که Secure Dynamic Updateها همیشه و در هر شبکه ای یکسان نیستند. به عنوان مثال تصور کنید که در شبکه‌ای تنها کاربران گروه Administrator اجازه Join کردن کامپیوتر به شبکه را داشته باشند. در این حالت ایمنی از حالت نرمال بالاتر خواهد رفت چراکه راهبر شبکه حتما توانایی تشخیص کامپیوتر مطمئن را از غیر مطمئن خواهد داشت. در همین حال اگر سایر کاربران نیز توانایی Join به شبکه را داشتن باشند قطعاً امنیت پایین تری را خواهید داشت. هنگامیکه پروسه Dynamic Update در معرض خطر قرار گرفته و شکسته می‌شود آنگاه نفوذگر می‌تواند اطلاعات موجود در Resource Recordهای کلیدی و حساس را تغییر دهد. به عنوان مثال با وارد نمودن یک اسم تقلبی ترافیک را به سمت مقصد خاص هدایت کند.



DNS Client Flooding

اگر تا به حال بر روی سرور DNS حمله DOS را تجربه نکرده‌اید باید بگوییم که جزو افراد خوش شانس محسوب می‌شوید. Queryهای DNS، Authenticate نمی‌شوند و DNS همواره سعی بر این دارد که درخواست‌های واصله را پاسخ دهد. این بدین معنی است که به راحتی می‌توان حمله‌ای بصورت Distributed Denial of Service بر علیه سرویس DNS راه اندازی کرده و بعد از مدتی مناسب سرویس را از کار انداخت. پس از غیرفعال شدن سرویس، نفوذگر زمان کافی در اختیار خواهد داشت تا یک سرویس تقلبی DNS را راه اندازی کرده و درخواست‌های واصله را به دلخواه نفوذگر پاسخ دهد. در این حالت کاربران به هیچ طریقی نمی‌توانند از تقلبی بودن سرویس دهنده DNS آگاهی پیدا کنند. حال به راحتی نفوذگر می‌تواند بعنوان مثال ترافیک را به سمت سایت‌های تقلبی و مشابه با سایت‌های اصلی هدایت کرده و حساب‌های کاربری و رمز عبور کاربران را بدست آورد.



Cache Poisoning

سرویس دهنده DNS گاهی به منظور ارایه پاسخ به درخواست‌های واصله موظف است از دیگر سرویس دهنده‌های DNSای پرسش نموده و اطلاعات بدست آمده را برای ارایه در درخواست‌های بعدی در حافظه موقت (Cache)خود ذخیره نماید. این اطلاعات برای مدتی معین در حافظه ذخیره شده و در زمان دریافت درخواست بعدی که پاسخ آن

در Cache موجود است، کارآیی DNS در ارایه پاسخ افزایش خواهد یافت. در کنار افزایش کارآیی سرویس DNS، مشکل امنیتی نیز ممکن است بوجود آید. DNS Cache Poisoning زمانی اتفاق می‌افتد که سرویس‌های DNS از یک سرویس دهنده دیگر سوال کرده و سرویس دهنده دوم اطلاعات غلط در اختیار DNS قرار می‌دهند. در اغلب اوقات سرویس دهنده DNS دوم که اطلاعات غلط در اختیار قرار داده، قبلا توسط نفوذگر تسخیر شده است. DNS Cache Poisoning به این دلیل اتفاق می‌افتد که سرویس دهنده اصلی DNS از صحت اطلاعات بدست آمده آگاهی نداشته و همچنین خود به بررسی و اعتبار سازی آن نیز نمی‌پردازد. در این حالت اطلاعات غلط در Cache قرار گرفته و درخواست‌های کلاینت‌ها در نوبت‌های بعدی با این اطلاعات پاسخ داده خواهد شد.

What is DNS cache ?

در این بخش اطلاعاتی در مورد کش DNS و روش پاک کردن کش dns کسب خواهید کرد. کش dns که بعضی اوقات به نام dns resolver cache شناخته می‌شود، یک پایگاه داده موقت است که توسط سیستم عامل کامپیوتر نگه‌داری می‌شود. این پایگاه داده موقت حاوی اطلاعات تمام بازدیدهای اخیر و تلاش برای بازدید از وب سایت‌ها و سایر دامنه‌های اینترنتی است.

به عبارت دیگر کش dns حافظه‌ای از جستجوهای اخیر dns است که کامپیوتر هنگامی‌که تلاش می‌کند تا نحوه بارگذاری وب‌سایت را بفهمد، می‌تواند به سرعت به آن اشاره کند.اغلب مردم عبارت "DNS cache" را تنها زمانی می‌شنوند، که می‌خواهند برای حل مسئله اتصال به اینترنت پاک کردن کش dns را انجام دهند.

هدف از کش dns چیست؟

اینترنت بر پایه Domain Name System (DNS) متکی است تا فهرستی از تمام وب‌سایت‌های عمومی و آدرس‌های IP مربوطه را نگهداری کند. شما می‌توانید آن را مانند یک دفترچه تلفن فرض کنید. با کمک یک دفترچه تلفن، ما مجبور نیستیم شماره تلفن همه را به خاطر بسپاریم. در دنیای وب نیز از DNS استفاده می‌شود تا ما از حفظ آدرس IP هر وب سایت بی‌نیاز باشیم. همانطور که برقراری ارتباط با تلفن‌ها متکی بر شماره تلفن است، برقراری ارتباط تجهیزات شبکه با وب‌سایت‌ها نیز بر اساس آدرس IP می‌باشد.

این فرآیند زمانی‌که می‌خواهید با استفاده از مرورگر وب، یک وب‌سایت را بارگیری کنید، در پشت پرده اتفاق می‌افتد. شما یک آدرس URL مانند Google.com را تایپ می‌کنید و مرورگر وب از روتر آدرس IP را می‌پرسد. روتر سرور dns است که آدرس‌ها در آن ذخیره شده است، بنابراین سرور dns آدرسIP میزبان هاست را می‌پرسد.

سرور dns آدرس IP متعلق به Google.com را پیدا می‌کند. بنابراین می‌تواند بداند وب‌سایت مورد نظر شما چیست، پس مرورگر شما می‌تواند صفحه مناسب را بارگذاری کند.

این مراحل برای هر وب‌سایتی که می‌خواهید بازدید کنید، انجام می‌شود. هر بار که کاربر با نام میزبان هاست از یک وب سایت بازدید می‌کند، مرورگر وب یک درخواست برای اینترنت را آغاز می‌کند. اما این درخواست تا زمانی که نام سایت "تبدیل" به یک آدرس IP شود، تکمیل نمی‌شود.

مشکل این است که حتی اگر تعداد زیادی سرور dns عمومی وجود داشته باشد تا شبکه بتواند برای سرعت بخشیدن به فرآیند تبدیل میزبان هاست به IP از آن استفاده کند، باز هم استفاده از کپی محلی از آدرس‌های IP سرعت بیشتری خواهد داشت. در این جاست که DNS Cacheها وارد بازی می‌شوند. کش dns تلاش می‌کند تا قبل از ارسال درخواستِ تماشای میزبان هاست به اینترنت، با جستجو در آدرس نام‌های تازه بازدید شده، سرعت بارگیری را افزایش دهد.

کش dns چگونه کار می‌کند؟

قبل از اینکه مرورگر درخواست‌های خود را به شبکه خارجی ارسال کند، کامپیوتر مانع مرورگر می‌شود و نام دامنه را در پایگاه داده کش جستجو می‌کند. پایگاه داده حاوی لیستی از تمام نام‌های دامنه تازه دیده شده و آدرس‌هایی است که dns در اولین درخواست برای آنها ایجاد کرده است.

محتویات کش dns محلی را می‌توان در ویندوز با استفاده از دستور ipconfig / displaydns تماشا کرد. نتایجی مشابه اطلاعات زیر نمایش داده خواهد شد.

```
docs.google.com
----------------------------------------
Record Name . . . . . : docs.google.com
Record Type . . . . . : 1
Time To Live . . . . : 21
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 172.217.6.174
```

درDNS ، رکورد "A" بخشی از ورودی dns است که حاوی آدرس IP برای میزبان هاست می‌باشد. کش dns این آدرس، نام وب سایت درخواست شده و چندین پارامتر دیگر را از ورودی میزبان dns ذخیره می‌کند.

آلوده شدن کش dns به چه صورت است؟

در مطالب بالا راجع به Cache Poisoning اطلاعاتی ارائه شد بنابراین یک کش dns هنگامی مسموم یا آلوده می‌شود که نام دامنه یا آدرس IP غیر مجاز در آن قرار بگیرد. گاهی اوقات ممکن است کش به دلیل آسیب‌های فنی یا مشکلات اجرایی خراب شود، اما آلوده شدن کش dns معمولا با ویروس‌های کامپیوتری یا سایر حملات شبکه مرتبط است که ورودی‌های dns نامعتبر را در کش قرار می‌دهند.

آلوده شدن کش باعث می‌شود درخواست‌های کاربر به مقصد اشتباه که معمولا وب سایت‌های مخرب و صفحات پر از تبلیغات هستند هدایت شوند.به عنوان مثال، اگر رکورد docs.google.comدارای یک رکورد متفاوت "A" باشد، پس وقتی وارد docs.google.com در مرورگر خود شوید، در آدرس دیگری قرار می گیرید.

این یک مشکل عظیم برای وب سایت‌های محبوب است. به عنوان مثال اگر یک مهاجم درخواست شما برای Gmail.comرا به یک وبسایتی مشابه Gmail جابجا کند، شما ممکن است با یک حمله فیشینگ مواجه شوید.

همچنین اگر شما مدیر یک وب‌سایت هستید ممکن هست با انتقال هاست خود از شرکت هاستینگی به شرکت هاستینگ دیگر که در نهایت منجر به تغییر IP می‌شود، مشکل باز نشدن سایت برای شما یا کاربران‌تان ایجاد شود.

پاک کردن کش dns چه اهمیتی دارد؟

هنگام رفع مشکلات مربوط به آلودگی در حافظه پنهان یا سایر مسائل مربوط به اتصال اینترنت، ممکن است نیاز به پاک کردن کش dns باشد. از آنجا که پاک کردن دایرکتوری dns تمام ورودی‌ها را حذف می‌کند، هر گونه سوابق نامعتبر نیز حذف می‌شود و کامپیوتر مجبور می‌شود تا آدرس‌ها را دوباره بارگذاری کند.

آدرس‌های تازه از سرور dns که شبکه برای استفاده از آن تنظیم شده گرفته می‌شود. بنابراین در نمونه بالا، اگر رکورد Gmail.comمسموم شده و شما را به یک وب‌سایت عجیب و غریب هدایت می‌کند، با پاک کردن کش dns، اقدام مناسبی برای به دست آوردن Gmail.comاصلی انجام خواهید داد.

تصحیح نشانی‌های URL

برای مثال، اگر کاربر در مرورگر خود به اشتباه تایپ کرد gogole.com سیستم به‌طور خودکار آن را به google.com اصلاح می‌کند. بیش‌تر سرویس‌هایی که در این مقاله به آن‌ها اشاره خواهیم کرد رایگان هستند یا بیش‌تر خدمات آن‌ها به رایگان قابل استفاده است. از آنجا که سرویس‌های DNS زیادی وجود دارند، آن‌هایی برای این مقاله انتخاب شده‌اند که تا حد امکان کارها را به‌صورت خودکار انجام دهند و نیازی به تنظیمات پیچیده توسط کاربر نباشد و به‌ویژه تنظیمات فیلتر کردن داده نیز از قبل روی آن‌ها انجام شده باشد. سوییچ کردن بین دو سرویس DNS سرور Recursive آسان است. تنها کافی است IP نشانی مربوط به DNS را در بخش تنظیمات اینترنت روتر تغییر دهید تا کل شبکه تحت تأثیر تنظیمات جدید قرار بگیرد یا این‌که روی هر کدام از کامپیوترها تک‌تک این کار را انجام دهید. برخی دیگر از این خدمات را می‌توان با ساخت یک حساب کاربری برای ایجاد سطوح مختلف دسترسی و نحوه دریافت پیام در مواجهه با داده فیلتر شده از آن‌ها استفاده کرد. به یاد داشته باشید که سرعت، اطمینان‌پذیری و کارایی DNS سرور می‌تواند متفاوت باشد. داشتن Domain resolution کم‌سرعت و ضعیف ممکن است به وب‌گردی کم‌سرعت و نامطمئن منجر شود. می‌توانید آزمون‌های سرعت را نیز روی DNS سرورها انجام دهید (برای این کار پیشنهاد می‌کنیم از Name bench استفاده کنید) تا بتوانید کارایی را در محل مشخصی بررسی کنید.

DNS Socket Pool

یکی از قابلیت های امنیتی موجود در سرویس DNS است که با DNS با انتخاب کردن پورت مبدا بصورت تصادفی از حملات DNS cache poisoning جلوگیری میکند. با تصادفی سازی پورت مبدا، سرویس DNS به طور تصادفی یک پورت مبدا را از Pool مربوط به سوکت های موجود یا باز که Socket Pool نام دارد، انتخاب میکند. سرویس DNS به جای استفاده از پورت پیشفرض برای پاسخ دهی به Query ها از این پورت ها استفاده میکند. همانطور که گفته شد Socket Pool حملات DNS cache poisoning را برای مهاجم بسیار دشوار میکند زیرا مهاجم باید شماره پورت مبدا DNS Query را به علاوه Transaction ID آن به طور صحیح حدس بزند تا بتواند حمله خود را با موفقیت انجام بدهد.

نکته منفی که در رابطه با ویژگی DNS Socket Pool وجود دارد این است که این قابلیت Utilization یا بهره وری DNS را بالا می برد، بدین معنی که منابع سیستمی مانند CPU و حافظه RAM با وجود این قابلیت در DNS و البته فعال بودن آن بیشتر مصرف می شود. نکته قابل توجهی که در رابطه با این قابلیت در DNS هست این است که مقدار پیشفرض Socket Pool برابر ۲۵۰۰ می باشد. هنگام پیکربندی این قابلیت میتوانید مقدار Socket

Pool را از ۰ تا ۱۰۰۰۰ تنظیم کنید. بدیهی است که هر چه اندازه Socket Pool بزرگتر باشد بیشتر می تواند از سرویس DNS در برابر حملات DNS Spoofing محافظت به عمل آورد. به طور مثال اگر شما اندازه Socket Pool را برابر صفر در نظر بگیرید سرویس DNS از یک پورت تنها برای پاسخ گوئی به Query ها استفاده خواهد نمود.

در پایان این مقاله به تعدادی از DNS Server های رایگان با خدمات خواص اشاره می شود که عبارتند از :

1. Comodo Secure DNS IP Address = 8.20.247.20 & 8.26.56.26
2. Dyn Internet Guide IP Address = 216.146.36.36 & 216.146.35.35
3. FoolDNS IP Address = 213.187.11.62 & 87.118.111.215
4. Green Team Internet IP Address = 209.88.198.133 & 81.218.119.11
5. Norton Connect Safe IP Address = xxx%xxx%xxx%xxx

Comodo Secure DNS

این برنامه یک سرویس رایگان ساده را در اختیار شما قرار می‌دهد. همچنین، برای مسدود کردن وب‌سایت‌های خطرناک و آسیب‌رسان مانند آن‌ها که بدافزار، جاسوس‌افزار و... دارند، از پیش تنظیم شده است. به علاوه، این سرویس ادعا دارد می‌تواند بسیار سریع‌تر، مطمئن‌تر و هوشمندتر از بسیاری از سرورهای DNS باشد که به‌وسیله ISPها مورد استفاده قرار می‌گیرد. Comodo نیز درست مثل سرویس Dyn خدمات دیگری را شامل سرورهای Authoritative برای وب‌سایت‌ها، گواهی‌نامه‌های SSL، خدمات ایمیل امن و... ارائه می‌دهد.

در زمان مسدود شدن Comodo Secure DNS، یک صفحه هشدار نمایش داده می‌شود. در این صفحه، دلیل مسدود شدن وب‌سایت توضیح داده می‌شود و البته به کاربر اجازه می‌دهد تا آن را نادیده بگیرد و سایت را باز کند. زمانی که کاربر با نادیده گرفتن پیام هشدار وب‌سایت مظنون را باز می‌کند، می‌تواند مدت زمان دسترسی به آن را نیز مشخص کند.

درباره نبود دامنه‌های مورد نظر یا زمانی که دامنه مورد نظر پاسخی نمی‌دهد، کاربر صفحه‌ای به‌نام Comodo Secure DNS Search را می‌بیند. عبارت‌ها و جملات پیشنهادی نیز بر اساس نام دامنه‌ای که کاربر تایپ کرده است، به وی نمایش داده می‌شود. به علاوه، امکان جست‌وجوی مجزا نیز در آن وجود دارد. با وجود آن‌که نتایج جست‌وجو به‌وسیله موتور جست‌وجوی یاهو تولید و نمایش داده می‌شود، اما این نتایج تنها شامل نتایجی است که قبلاً برای آن‌ها پول پرداخت شده است و به هیچ وجه بیان‌کننده جست‌وجوی کامل نیست. این امر یکی از نقاط ضعف این سرویس قلمداد می‌شود.

همواره منتظر به‌روزرسانی‌های این سرویس باشید و در حال حاضر نسخه بتای آن به‌نام Comodo Secure DNS 2.0 که قابلیت سفارشی کردن نوع مسدود کردن داده را نیز دارد، قابل استفاده است.

Dyn Internet Guide

این برنامه یک سرویس رایگان برای استفاده‌های شخصی و تجاری است. تنظیماتی که از پیش روی آن اعمال شده است، باعث می‌شود تا به‌صورت خودکار بدافزارها و سایت‌های فیشینگ را مسدود کند و همچنین اصلاح تایپ نشانی غلط را نیز برای کاربر انجام می‌دهد. این سرویس از سرور Authoritative استفاده می‌کند که متشکل از Hostname برای دسترسی ریموت و راهکارهای جامع DNS برای وب‌سایت‌ها است.

به علاوه، Dyn سرویس فیلتر کردن با قابلیت سفارشی‌سازی را نیز ارائه می‌دهد، اما قبل از آن باید یک حساب کاربری ایجاد کنید. می‌توانید تا سی دسته‌بندی از پیش تعیین شده را برای فیلتر کردن انتخاب و فهرست‌های سفید و سیاه سفارشی ایجاد کنید. شرکت ارائه‌کننده این سرویس یک اشتراک Internet Guide را نیز ارائه می‌دهد که خود این اشتراک رایگان است، اما سرویس دسترسی ریموت آن هزینه‌بر است که هزینه آن بر اساس نوع خدمات ارائه شده به‌صورت سالانه از ۲۵ دلار شروع می‌شود. البته کاربران می‌توانند از دو هفته دسترسی آزمایشی رایگان نیز استفاده کنند. همچنین، کاربر باید هر ماه یک بار وارد حساب کاربری Internet Guide شود تا حساب کاربری فعال بماند.Dyn دو نوع اشتراک Internet Guide را ارائه می‌دهد؛ اشتراک Pro با هزینه ده دلار در سال و اشتراک Premium با هزینه بیست دلار در سال که هیچ کدام به استفاده از سرویس دسترسی ریموت را نیاز ندارند، به شرط این‌که شما نیز از یکIP استاتیک استفاده کنید. زمانی که کاربری تلاش کند تا به سایتی که با تنظیمات اعمال شده در Internet Guide مسدود شده است، دسترسی پیدا کند، یک صفحه هشدار به وی نمایش داده و دلیل مسدود شدن صفحه نیز به وی توضیح داده می‌شود. زمانی که در سایتی بدافزاری پیدا یا توسط تنظیمات خودکار امنیتی Internet Guide سایتی فیشینگ تشخیص داده شود، به کاربر این اجازه داده می‌شود تا هشدارها را نادیده بگیرد و وارد سایت شود مگر این‌که آن سایت خاص یا آن دسته‌بندی که این سایت در آن قرار می‌گیرد، به‌طور صریح از طریق تنظیمات موجود در Internet Guide مسدود شده باشد. درباره نبودن دامنه‌های مورد نظر یا زمانی که از سوی دامنه مورد نظر پاسخی داده نمی‌شود، کاربر صفحه‌ای به‌نام Internet Guide را می‌بیند. عبارت‌ها و جملات پیشنهادی نیز بر اساس نام دامنه‌ای که کاربر تایپ کرده است، به وی نمایش داده می‌شود.

FoolDNS

این برنامه در دو نسخه رایگان و تجاری عرضه شده است که هر دو نسخه کاربران خانگی و کسب و کارهای کوچک را هدف گرفته‌اند. این سرویس اساساً به‌منظور مسدود کردن ردیابی‌های آنلاین و تبلیغات مزاحم طراحی شده است،

اما در کنار آن‌ها می‌تواند بدافزارها و سایت‌های فیشینگ را نیز مسدود کند. خدمات Premium این شرکت امکانات بیش‌تری دارد که در هر دو نسخه به کاربر پیشنهاد می‌شود. نسخه Audit امکاناتی مانند گزارش‌گیری، لاگ کردن رویدادها و امکان ساخت فهرست‌های سفید و سیاه را دارد. نسخه Business امکان فیلتر کردن بیش از دو میلیون دامنه غیر ایمن، قابلیت‌های پیش‌رفته‌تر گزارش‌گیری و توانایی ایجاد فیلترهای سفارشی با ۲۰ دسته‌بندی از پیش تعیین شده دارد. زمانی که صفحه‌ای مسدود می‌شود ــ به‌طور مثال وقتی که یک بدافزار کشف می‌شود ــ یک صفحه بسیار ساده نمایش داده می‌شود و بیان می‌کند که دامنه مسدود است.

Green Team Internet

این برنامه خدمات رایگان و تجاری برای کاربران خانگی و کسب و کارهای کوچک دارد. تنظیمات رایگان از پیش اعمال شده آن می‌تواند به‌طور خودکار بدافزارها و سایت‌های فیشینگ، تبلیغات و همچنین سایت‌های هرزه‌نگاری را مسدود کند. زمانی که از حساب کاربری رایگان آن استفاده می‌کنید، می‌توانید نوع فیلتر کردن داده را با انتخاب از بین سه سطح از پیش تعریف شده و ۴۷ دسته‌بندی که آن‌ها هم از پیش تعریف شده‌اند، تغییر دهید. همچنین، امکان ایجاد فهرست‌های سیاه و سفید سفارشی نیز وجود دارد. اما در حساب‌های کاربری که هزینه استفاده از آن را پرداخت می‌کنید، با توجه به نوع شرکت‌تان می‌توانید از تنظیمات و دسترسی‌های بیش‌تری بهره‌مند باشید. زمانی که سایتی که کاربر به آن مراجعه می‌کند مسدود است، به کاربر پیامی نشان داده می‌شود که بیان می‌کند سایتی که قصد ورود به آن را دارد مربوط به چه دسته‌بندی و چرا مسدود شده است. علاوه بر آن، در صفحه‌ای که این پیام را به کاربر نشان می‌دهد، کاربر می‌تواند با ارسال ایمیلی به Green Team از آن‌ها بخواهد سایت فوق را دوباره در دسترس قرار دهند. همچنین، کاربران می‌توانند ایمیل خود را نیز برای سیستم ارسال کنند تا زمانی که سایت مورد نظر آن‌ها در دسترس قرار گرفت، از طریق ایمیل آگاه شوند.

در هر دو حساب رایگان و تجاری این امکان برای مدیر شبکه وجود دارد تا بتواند پیام‌های مخصوص به خود را در صفحات مسدود وب‌سایت‌ها نمایش دهد. Green Team Internet برای دامنه‌هایی که وجود ندارند یا دامنه‌ای که پاسخ‌دهی از سمت سرور ندارد، دارای صفحه خاصی نیست و به‌جای آن به مرورگر اجازه می‌دهد تا پیام‌های مخصوص به خود را نمایش دهد.

Norton Connect Safe

نشانی DNS: متفاوت بسته به نوع سرویس

این برنامه برای استفاده‌های شخصی رایگان است و برای استفاده به حساب کاربری نیز نیازی ندارد. این سرویس سه دسته‌بندی را در سطوح مختلف به کاربر ارائه می‌دهد:

سطح ۱ (Security): این سطح که در واقع سطح پایه‌ای آن هم است، می‌تواند بدافزارها، سایت‌های فیشینگ و اسکمر را مسدود کند و از IP نشانی ۱۱۹,۸۵,۱۲۶,۱۰ و ۱۹۹,۸۵,۱۲۷,۱۰ استفاده می‌کند.

سطح ۲: قابلیت‌های مسدودسازی سایت‌های با محتوای هرزه‌نگاری را نیز به سطح Security اضافه می‌کند که با IP نشانی ۱۱۹,۸۵,۱۲۶,۲۰ و ۱۹۹,۸۵,۱۲۷,۲۰ در دسترس است.

سطح ۳: با مسدود کردن وب‌سایت‌های آسیب‌رسان دیگر سطح بیش‌تری از امنیت داده را برای کاربر مهیا می‌کند که با IP نشانی ۱۹۹,۸۵,۱۲۶,۳۰ و ۱۹۹,۸۵,۱۲۷,۳۰ در دسترس است. این سرویس خدمات مخصوص کاربران تجاری نیز دارد که برای استفاده از آن‌ها باید هزینه‌های مربوط به آن را پرداخت کنید تا بتوانید به عنوان مشترک از خدمات آن استفاده کنید.

باتشکر فراوان از توجه شما استاد عزیز