DNS tunneling  با استفاده از درخواست های DNS برای پیاده سازی یک مسیر فرمان و کنترل برای بدافزار استفاده می کند. ترافیک DNS ورودی می تواند دستورات را به بدافزار منتقل کند، در حالی که ترافیک خروجی می تواند داده های حساس را استخراج کند یا به درخواست های اپراتور بدافزار پاسخ دهد. به دلیل اینکه DNS یک پروتکل بسیار انعطاف پذیر است ، می تواند به راحتی مورد حمله تانلینگ قرار گیرد. همچنین محدودیت های بسیار کمی در مورد داده هایی که یک درخواست DNS را شامل می شود وجود دارد زیرا برای جستجوی نام دامنه وب سایت ها طراحی شده است و تقریباً هر چیزی می تواند یک نام دامنه باشد. از فیلدهای نام دامنه می توان برای حمل اطلاعات حساس استفاده کرد. این درخواست‌ها به گونه‌ای طراحی شده‌اند که به سرورهای DNS کنترل‌شده توسط مهاجم بروند و اطمینان حاصل کنند که می‌توانند درخواست‌ها را دریافت کنند و در پاسخ‌های DNS مربوطه پاسخ دهند.

## شناسایی حملات تونل زنی DNS

برخی از شاخص های DNS tunneling در یک شبکه می تواند شامل موارد زیر باشد:

1. درخواست‌های غیرمعمول دامنه: بدافزار تونل زنی DNS داده‌ها را در یک نام دامنه درخواستی (مانند DATA\_HERE.baddomain.com) رمزگذاری می‌کند. بررسی نام‌های دامنه درخواستی در درخواست‌های DNS ممکن است سازمان را قادر سازد تا ترافیک قانونی را از تلاش برای تونل‌سازی DNS متمایز کند.
2. درخواست ها برای دامنه‌های غیرمعمول: تونل‌سازی DNS تنها در صورتی کار می‌کند که مهاجم ، مالک دامنه هدف باشد. به طوری که درخواست‌های DNS به سرور DNS آنها برود. اگر سازمانی با افزایش ناگهانی درخواست ها برای یک دامنه غیرمعمول مواجه شود، ممکن است نشان دهنده حمله DNS Tunneling باشد، به خصوص اگر آن دامنه به تازگی ایجاد شده باشد.
3. حجم بالای ترافیک DNS: نام دامنه در یک درخواست DNS حداکثر اندازه (253 کاراکتر) دارد. بدین معنی که یک مهاجم احتمالاً به تعداد زیادی درخواست DNS مخرب برای  استخراج داده یا اجرای یک پروتکل فرمان و کنترل بسیار تعاملی نیاز دارد. جهش حاصل در ترافیک DNS می تواند نشانگر حمله تونل سازی DNS باشد.

## نحوه محافظت در برابر  DNS Tunneling

1. **بروزرسانی نرم افزار DNS:**از آخرین نرم افزارهای DNS که شامل جدیدترین پچ های امنیتی هستند، استفاده نمایید.
2. **Multi-factor authentication یا احراز هویت چند عاملی (MFA):** برای تمام حساب‌های کاربری که در زیرساخت DNS سازمان شما تعریف شده، MFA را تنظیم نمایید.
3. **Domain Name System Security Extensions یا پروتکل‌های امنیتی سیستم نام دامنه (DNSSEC):** استفاده از امضاهای دیجیتال مبتنی بر رمزنگاری کلید عمومی، امنیت DNS را تضمین می کند. بنابراین DNSSEC یک لایه امنیتی به DNS سازمان شما اضافه خواهد کرد.
4. **زیرساخت DNS مطمئن:** این زیرساخت، پایه و اساس یک محیط امن و حفاظت شده برای حضور آنلاین سازمان شما است. اگر درخواست های DNS زیادی دریافت می‌کنید، شبکه Anycast DNS، ضروری خواهد بود.
5. **DNS محافظت شده در مقابل DDoS یا DDoS protected DNS:** این سرویس به طور خاص برای کاهش یکی از مضرترین حملات سایبری یعنی DDoS، طراحی شده است.
6. **نظارت مداوم:**ثبت گزارش و نظارت بر کوئری های DNS ورودی و خروجی، می‌تواند به طور قابل توجهی در تشخیص رفتارهای غیرعادی کمک کند.
7. **DNS resolver خصوصی:**DNS resolver را به کاربران داخل شبکه محدود نمایید تا از آلودگی کش DNS توسط هکرها، جلوگیری کنید.

## عملکرد DNS Tunneling

حملات تونل سازی DNS از پروتکل DNS برای افزودن بدافزار و سایر داده ها از طریق مدل سرور-کلاینت، سوء استفاده می کنند. مهاجم دامنه ای مانند example.com را ثبت می نماید. نام دامنه به سرور مهاجم اشاره می کند، جایی که یک بدافزار تونل سازی نصب شده است.

مهاجم کامپیوتری را که اغلب پشت فایروال یک شرکت قرار دارد، با بدافزار آلوده می کند. از آنجایی که درخواست‌های DNS همیشه مجاز به جابجایی و خروج از فایروال هستند، رایانه آلوده مجاز است درخواستی را به "مترجم DNS" یا DNS resolver ارسال کند. DNS resolver سروری است که درخواست‌های آدرس IP را به سرورهای دامنه اصلی و سطح بالا ارسال می‌کند.

DNS resolver کوئری را به سرور تحت کنترل مهاجم هدایت می کند، جایی که برنامه تونل سازی نصب شده است. اکنون ارتباطی بین قربانی و مهاجم از طریق DNS resolver برقرار شده است. از این تونل می توان برای استخراج داده ها یا سایر اهداف مخرب استفاده کرد. از آنجایی که هیچ ارتباط مستقیمی بین مهاجم و قربانی وجود ندارد، ردیابی رایانه مهاجم دشوارتر است. نمودار زیر نحوه عملکرد DNS Tunneling را نشان می دهد.



DNS tunneling تقریباً 20 سال است که وجود دارد. دو بدافزار Morto و Feederbot برای تونل سازی DNS استفاده می شوند. حملات اخیر تونل سازی توسط این بدافزارها، مربوط به گروه DarkHydrus می شود که نهادهای دولتی خاورمیانه را در سال 2018 هدف قرار داد و هنوز فعال است.