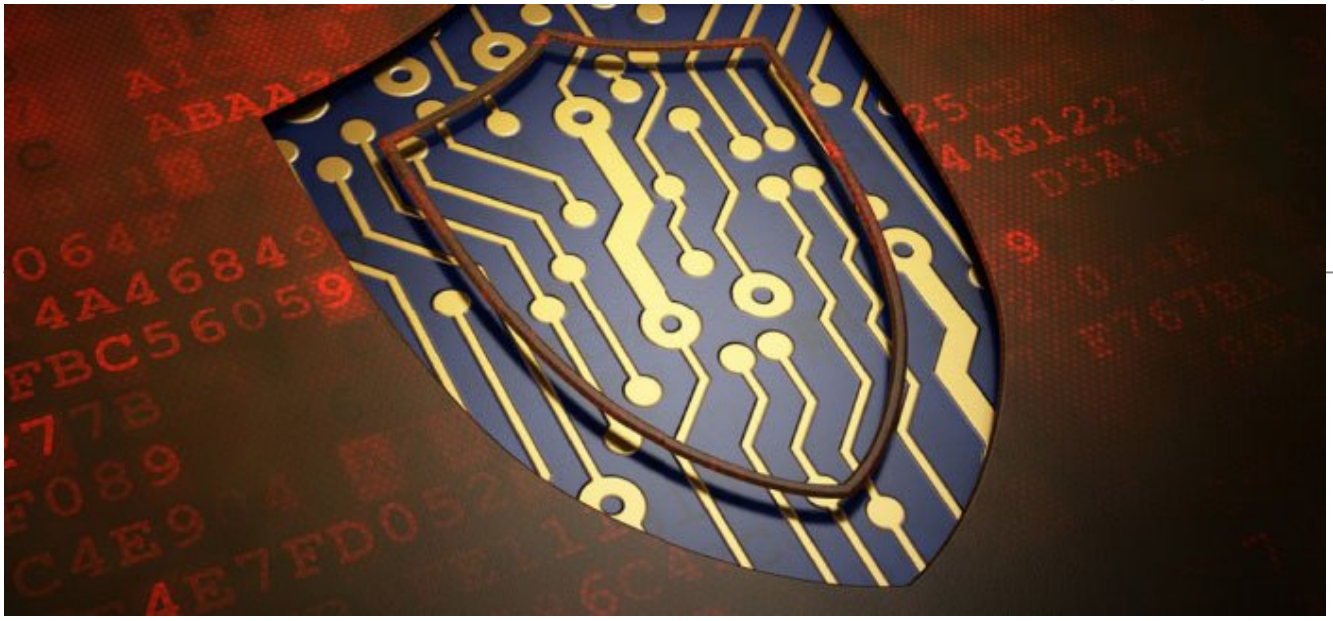
6 سرویس برای مقابله با بدافزارها

امنیـت در مـرز DNS



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.

نخست، برای افرادی که با DNS آشنایی ندارد، مرور کوتاهی بر آن خواهیم داشت. در واقع، هر زمانی که وب‌گردی می‌کنیم، از DNS (سرنام Dynamic Name Server) استفاده می‌کنیم. هر زمان که کاربر نام سایتی را در مرورگر وارد می‌کند، DNS درخواستی را برای دریافت IP متناظر با نام آن سایت به سروری ارسال می‌کند که به همین منظور در شبکه قرار داده شده است. بر همین اساس، مرورگر می‌تواند وب‌سرور مربوط به وب‌سایتی که کاربر می‌خواهد آن را ببیند پیدا کند و وب‌سایت را به کاربر نشان دهد (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 (که در این مقاله هم به‌تفصیل به آن‌ها خواهیم پرداخت).
اغلب فراهم‌کنندگان خدمات اینترنت (ISP سرنام 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 وب‌سرور 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 وب‌سایت 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.

ـ فیلتر کردن داده‌ها : می‌توان به‌راحتی از این ابزار برای فیلتر کردن سایت‌های هرزه‌نگاری و سایر داده‌های ناخواسته و نامناسب استفاده کرد، بدون این‌که به نرم‌افزار خاصی روی کامپیوترهای کاربران نیازی داشته باشیم.

ـ 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.

ـ محافظت در مقابل بات‌نت‌ها: این سرویس می‌تواند ارتباطات ناخواسته را که اغلب بات‌نت با سرور مولد خود دارد مسدود کند؛ بنابراین، کمک زیادی به ارتقای امنیت کاربر می‌کند.

ـ 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.

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. در این مقاله، به بررسی و معرفی این سرویس‌ها خواهیم پرداخت. 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 Namebench استفاده کنید) تا بتوانید کارایی را در محل مشخصی بررسی کنید.

Comodo Secure DNS

رایگان فقط برای کاربری شخصی

نشانی دی‌ان‌اس: 8.26.56.26 و 8.20.247.20

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 آی‌اس‌پی‌ها 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

رایگان برای کاربری‌های شخصی و تجاری

نشانی دی‌ان‌اس: 216.146.35.35 و 216.146.36.36

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 Authoritatives 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 25 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

رایگان برای کاربری‌های شخصی و تجاری
نشانی دی‌ان‌اس: 87.118.111.215 و 213.187.11.62
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 20 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.

GreenTeam Internet

رایگان برای کاربری‌های شخصی و تجاری
نشانی دی‌ان‌اس: 81.218.119.11 و 209.88.198.133
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 47 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 GreenTeam 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. GreenTeam 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 ConnectSafe

رایگان برای کاربری‌های شخصی
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 1 (Security): این سطح که در واقع سطح پایه‌ای آن هم است، می‌تواند بدافزارها، سایت‌های فیشینگ و

اسکمر را مسدود کند و از IP نشانی 119.85.126.10 و 199.85.127.10 استفاده می‌کند.
سطح 2: قابلیت‌های مسدودسازی سایت‌های با محتوای هرزه‌نگاری را نیز به سطح Security اضافه می‌کند که با IP نشانی 119.85.126.20 و 199.85.127.20 در دسترس است.
سطح 3: با مسدود کردن وب‌سایت‌های آسیب‌رسان دیگر سطح بیش‌تری از امنیت داده را برای کاربر مهیا می‌کند که با IP نشانی 199.85.126.30 و 199.85.127.30 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.
این خدمات شامل دسترسی‌های دو سطح اولی است که به کاربران رایگان نیز اختصاص دارد، اما با نشانی DNS متفاوت و سطح سوم خدمات می‌تواند سیستم به اشتراک‌گذاری فایل P2P را غیر فعال کند. وقتی کاربر وارد یک سایت مسدود می‌شود، صفحه‌ای را می‌بیند که دلیل مسدود شدن وب‌سایت مورد نظر را برای وی توضیح داده است و یک لینک نیز برای ارسال ایمیل به Norton ConnectSafe وجود دارد تا کاربر درخواست رفع مسدودی را برای آن‌ها ارسال کند. البته تبلیغاتی برای سایر محصولات Norton نیز در این صفحه دیده می‌شود. صفحه مربوط به دامنه‌هایی که وجود ندارند یا سرور مربوط به آن‌ها پاسخ‌دهی ندارد هم دارای تبلیغات نیست، اما یک کادر جست‌وجو دارد که از موتور جست‌وجوی ASK.com استفاده می‌کند تا نتایج جست‌وجو را به کاربر نمایش دهد.

OpenDNS

رایگان برای استفاده شخصی و تجاری برای Enhanced DNS و استفاده شخصی تنها برای کاربری خانگی امکان‌پذیر است.
نشانی دی‌ان‌اس: 208.67.222.222. و 208.67.220.220 (نشانی DNS مخصوص سرویس FamilyShield: 208.67.222.123 و 208.67.220.123).
این برنامه از محبوب‌ترین ارائه‌کنندگان خدمات DNS است. این سرویس نیز خدمات رایگان و تجاری دارد که برای کاربران خانگی و کسب و کارها طراحی شده است.
پایه‌ای‌ترین سرویس آن Enhanced DNS است که توسط سرورهای اصلی شرکت ارائه می‌شوند و تنظیماتی از پیش اعمال شده برای مسدود کردن بدافزارها و سایت‌های فیشینگ دارد. اما OpenDNS سرویس‌های دیگری برای کاربران شخصی و خانگی نیز دارد.
OpenDNS FamilyShield: درست مثل Enhanced DNS است، با این تفاوت که کاربر می‌تواند فیلترها و تنظیمات امنیتی بیش‌تری داشته باشد که از جمله آن‌ها می‌توان به داشتن فهرست‌های سفید و سیاه، پیام‌های قابل سفارشی‌سازی برای صفحات مسدود و دریافت آمار و لاگ‌های اولیه اشاره کرد. این سرویس از همان IP نشانی مربوط به Enhanced DNS استفاده می‌کند، اما برای استفاده از آن باید حساب کاربری داشته باشید.
OpenDNS Home VIP: سرویس Premium مشابه با سرویس خانگی دارای آمارها و گزارش‌های نحوه استفاده از آن و پشتیبانی است که برای استفاده از آن باید سالانه 19.95 دلار پرداخت کنید. این سرویس نیز از IP نشانی سرویس Enhanced DNS استفاده می‌کند، اما برای استفاده از آن باید حساب کاربری ایجاد کنید. سرویس پایه‌ای مربوط به کسب و کارهای کوچک OpenDNS به‌نام Umbrella تنظیمات مدیریتی و امنیتی پیش‌رفته دارد که برای شبکه‌های بزرگ بسیار سودمند است. زمانی که کاربر می‌خواهد به یک وب‌سایت مسدود دسترسی داشته باشد، یک صفحه ساده را روبه‌روی خود خواهد دید که هشدار مسدود بودن و دلیل آن را به او نمایش می‌دهد.
مدیران شبکه که از هریک از سرویس‌های رایگان یا تجاری OpenDNS استفاده می‌کنند، می‌توانند متن‌های دلخواه خود را به این صفحات اضافه کنند. همچنین، در همین صفحات کاربر می‌تواند درخواست رفع مسدودی وب‌سایت مورد نظر را به مدیر شبکه ارسال کند. زمانی که از Umbrella روی یک شبکه تجاری استفاده می‌کنید، مدیر شبکه می‌تواند به‌سرعت با استفاده از کدهایی که در اختیار دارد، وب‌سایت‌ها را از حالت مسدودی خارج کند. برای کاربرانی که از سرویس‌های خانگی OpenDNS استفاده می‌کنند نیز امکاناتی مشابه در دسترس است، اما باید از روترهای Netgear برای دسترسی به DNS سرور استفاده کنند (بر اساس اعلام Netgear بیش‌تر روترهای جدید این شرکت از OpenDNS پشتیبانی می‌کنند). کاربرانی که دامنه‌های ناموجود یا دامنه‌هایی را که سرور آن‌ها پاسخ‌دهی ندارد فراخوانی می‌کنند، صفحه خطای پیش‌فرض مرورگر را خواهند دید. البته در سرویس‌های رایگان OpenDNS تبلیغاتی در این صفحات به کاربر نمایش داده می‌شد که از ابتدای ژوئن سال 2014 نمایش این تبلیغات نیز متوقف شده است.

منبع:

کامپیوتر ورلد
تاریخ انتشار:
24 اسفند 1393

نشانی منبع: https://www.shabakeh-mag.com/networking-technology/416