

# Your Freedom

Arash Taher-Kalateh

882980

برنامه Your-Freedom خود را در درجه اول به عنوان یک Connectivity Service معرفی می کند که اجازه دور زدن محدودیت ها را به ما میدهد. این امر با تبدیل کامپیوتر مبدأ به یک Web-proxy و Socks-proxy صورت می گیرد. این برنامه میتواند روی Web-proxy ، Firewall و امثال آن تونل بزند. این برنامه VPN نیست، برای افزایش امنیت طراحی نشده و امکان کامل ناشناس ماندن را هم فراهم نمیکند.

قسمت اول این برنامه، به صورت یک برنامه جاوا برای سمت Client نوشت شده است. این برنامه توسط یکی از پروتکل هایی که سمت Client هنوز باز است به سرورهای Your-freedom متصل میشود. این ارتباط معمولاً به صورت یک HTTP Connection انجام می پذیرد. با این حال امکان اتصال از طریق HTTPS ، FTP و یا UDP هم وجود دارد. معمولاً تمام آنچه که نیاز است آدرس Proxe Server است، Client بقیه موارد را سر و سامان میدهد و روش مناسب برا برقرای ارتباط را پیدا می کند.

این برنامه در حال حاضر از ۳۱ سرور در ۹ کشور مختلف استفاده می کند ( در برخی نقاط، با محدودیت روی ارتبا P2P ). برای برقراری امنیت سطحی، امکان رمزگذاری ساده هم وجود دارد که چندان مطمئن نیست.

اما بگذارید کمی ریز تر شویم و روش های مختلف اتصال Client به Server را بررسی کنیم. یکی از این روش ها CGI-Relay است. معمولاً Client برنامه YF به صورت مستقیم به سرورها متصل میشود. بستن چنین ارتباطی برای ادمین چندان مشکل نیست، تمام آنچه که نیاز دارد انجام دهد داشتن یک لیست از آی پی سرورها و بلاک کردن آنهاست. یک روش برای رد شدن از این سد عوض کردن هر از چند گاه سرورها و آی پی آدرس هاست که بیشتر موش و گربه بازی است. برای حل این موضوع YF از CGI-Relay ها استفاده می کند. به این صورت که در میان راه، یک اسکریپت ساده php قرار می گیرد که ارتباط بین کلینت و سرور را رله می کند. به این ترتیب برای هر کدام از سرورها می توان تعداد زیادی URI و آی پی داشت، به نحوی که عملاً بستن همه آنها غیر ممکن میشود. همین الان هم YF با دادن مشوق افرادی که وب سرور دارند را به نصب اسکریپت برای رله کردن ترافیک ترغیب می کند ).

یکی دیگر از راه های اتصال DNS-Mode است. در اینجا از سرویس dns برای تونل زدن استفاده

میشود. سرویس dns تقریبا در اختیار همه قرار دارد. شاید این راه پایداری کمتری داشته باشد، اما در بسیاری از شرایط جواب میدهد. چنانچه نتوانیم مستقیما به سرور وصل شویم، از nameserver برای برقراری ارتباط استفاده میشود.

یک راه حل دیگر برای وصل شدن به سرور ECHO-Mode است که از بسته‌های ICMP ECHO یا همان ping استفاده می‌کند. مناسب برای زمانی که دسترسی کامل نداریم، اما امکان Ping کردن داریم. این روش، به دلیل اینکه از Raw Socket استفاده می‌کند و در نتیجه کد جاوا باید از JNI استفاده کند، بر روی همه پلتفرم‌ها قابل استفاده نیست. علاوه بر آن، دسترسی روت هم مورد نیاز است.

در ادامه این مسیر، اشاره می‌کنیم به PPTP. این روش مناسب افرادی است که میخواهند ناشناس بمانند و مکان آنها مشخص نشود. PPTP یک VPN-tunnel است که توسط مایکروسافت طراحی شده. این روش استاندارد است و نسبتا در بین PC و دستگاه‌های جانبی به خوبی گسترش داشته است، امنیت آن هم خوب است. اما چه زمانی مناسب است که از روش استفاده کنیم :

زمانی که به Hot-Spot متصل شده‌ایم و می‌خواهیم ناشناس بمانیم.

زمانی که می‌خواهید کشور شما ناشناس مانده و با یک کشور دیگر شناخته شوید.

زمانی که مهیا کنند سرویس اینترنت شما بر روی بعضی سایت‌ها محدودیت سرعت قرار داده ( مثل Youtube )

علاوه بر همه اینها روش‌های دیگر چون SOCKS 5 و IPv6-Teredo هم وجود دارد.