فصل اول

۱-۱- مقدمه

۱-۲- تشریح و بیان موضوع :

ما در عصر اطلاعات زندگی می‌کنیم که در آن هر شخصی که به اینترنت متصل است، تمام اطلاعات جهان را در دستان خود دارد. در حالی که اینترنت امکان اشتراک‌گذاری اطلاعات را گسترش داده است، بسیاری از کاربران را نگران کرده است که اطلاعات خصوصی آنها، از جمله فعالیت و مرور آنها، بدون اجازه و اطلاع‌شان مورد ردیابی قرار گیرد. با افزایش نگرانی ها در مورد حریم خصوصی و امنیت، کاربران اینترنت به دنبال راه‌هایی برای ناشناس کردن ترافیک شبکه خود هستند.

ذکر Tor به سال ۱۹۹۵ بر می‌گردد، زمانی که دفتر تحقیقات نیروی دریایی ایالات متحده[1] به همراه آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی[2] (DARPA) روی توسعه نوع جدیدی از فناوری کار کردند که ردیابی ترافیک به آنها را دشوار می‌کرد. این ایده مبتنی بر عبور ترافیک از طریق گره‌های تصادفی قبل از رسیدن به مقصد بود. هدف از این کار ایجاد سردرگمی در مورد اینکه فرستنده و مقصد مورد نظر چه کسی است، و از این طریق شناسایی مقصد نهایی ارتباط را دشوار می‌کرد. هدف از توسعه این فناوری در ابتدا تقویت حریم خصوصی نبود، بلکه ایجاد امکان برای پرسنل مخفی جهت برقراری ارتباط ناشناس بدون ترس از دستگیری بود.

[1] US Office of Naval Research
[2] Defense Advanced Research Projects Agency

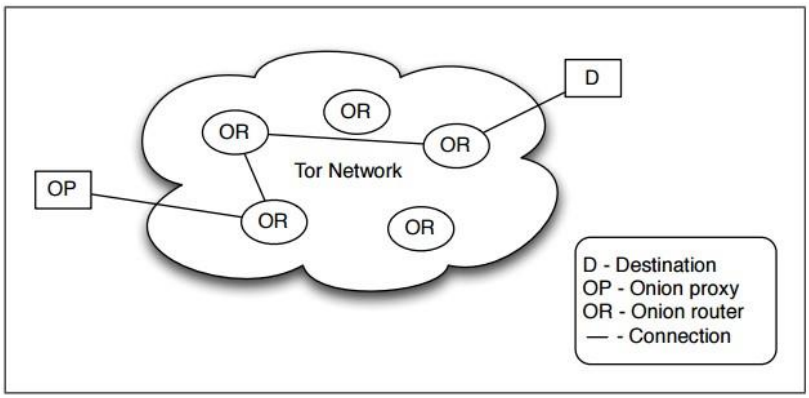
امروزه Tor یک پروژه منبع باز[3] است که برای اهداف مختلف توسط ارتش، روزنامه نگاران، سازمان های مجری قانون، فعالان و بسیاری دیگر استفاده می‌شود. ناشناس بودن شبکه Tor برای هر کسی که می‌خواهد از ارتباطات خود در برابر دیگران محافظت کند، موضوعات حساس را جستجو کند، از نظارت اجتناب کند، سانسور را دور بزند و از حریم خصوصی خود در برابر سارقان هویت محافظت کند، جذاب است [۲].

این واقعیت که Tor صددرصد ایمن نیست را نمی‌توان کتمان کرد و کمتر از آن چیزی که مردم فکر می‌کنند ایمن است. یعنی در این محیط ممکن است کاربری که برای انجام کاری وارد این فضا می‌شود مورد حمله قرار گیرد، و از اطلاعات شخصی او سوء استفاده شود.

برای ارائه یک سرویس ارتباطی ناشناس گسترده، محققان سیستم مبتنی بر مسیریابی پیاز تور [۲] را توسعه دادند.

این بزرگترین شبکه ارتباطی ناشناس موجود است، با بیش از ۷۰۰۰ سرور مجزا در سراسر جهان [3] خدمات ارتباطی ناشناس را برای صدها هزار کاربر اینترنت فراهم می‌کند و هر روز ترابایت‌ها ترافیک را حمل می‌کند [4].

شکل زیر نمای کلی از طراحی مسیریابی پیاز Tor را نشان می‌دهد.

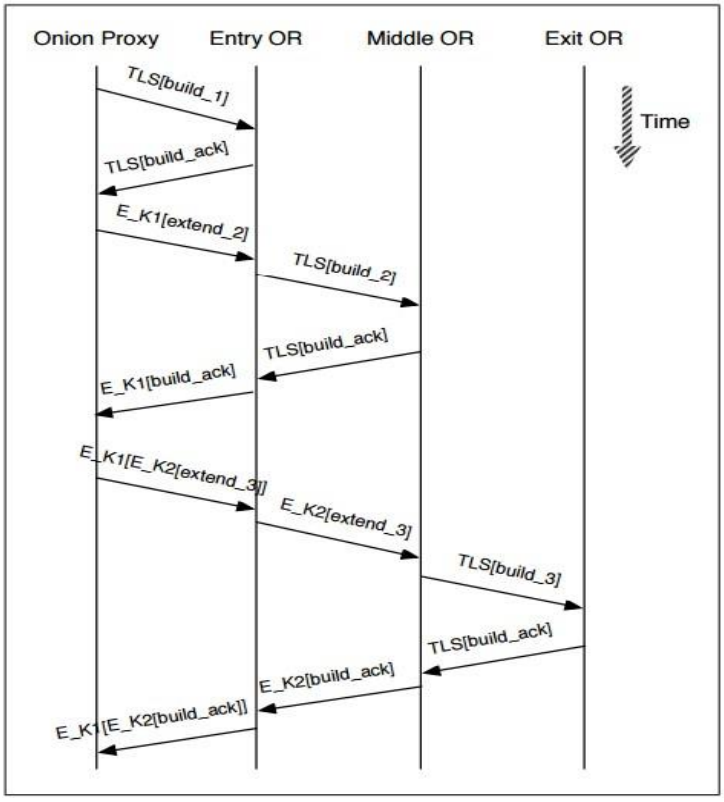


شکل ۱: مروری بر طراحی مسیریابی پیاز تور [108]

مسیریابی پیاز تلاشی است برای ناشناس ساختن ارتباطات با افزودن چندین لایه به بسته‌ها به همانند پیاز که چندین لایه دارد. معمولاً در اینترنت، ارتباطات بین دو نهاد با ارائه آدرس‌های IP مبدا و مقصد به بسته‌ها به روشی مشابه با یک سرویس پستی برقرار می‌شود. بیشتر داده‌ها نیز رمزگذاری شده‌اند، که تشـخیص اینکه این دو نهاد دقیقاً چه چیزی را به یکدیگر منتقل می‌کنند، برای برخی از اسـتراق

[3] Open-source

سمع‌کنندگان دشوار می‌سازد. با این حال، یک استراق سمع می تواند به راحتی متوجه شود که نهادها در حال ارتباط هستند، که می‌تواند قبلاً توسط برخی یک مسئله امنیتی در نظر گرفته شود. مسیریابی پیاز با معرفی گره‌های اضافی در مدار ارتباطی که بسته‌ها قبل از رسیدن به مقصد از بین آنها عبور می‌کنند، این مشکل را حل می‌کند. هنگامی که کاربر می خواهد از یک وب سایت خاص بازدید کند، ابتدا یک مدار راه اندازی می‌کند. این مدار از چند سلول رله تشکیل شده است که کاربر با آنها یک کلید مخفی مشترک تولید می‌کند. هر سلول رله دارای کلیدهای متقارن متفاوتی است که با کاربر مشترک است. هنگامی که کاربر می‌خواهد داده‌ها را از طریق مدار به هدف نهایی ارسال کند، با رمزگذاری داده‌ها با کلید آخرین سلول شروع به کار می‌کند و به طور مکرر بسته را با کلید از سلول رله دوم تا آخرین سلول رمزگذاری می کند و غیره. تا زمانی که بسته دارای یک لایه رمزگذاری برای هر سلول رله در زنجیره باشد. شکل زیر یک مدار را نشان می‌دهد [1].



شکل ۲: ایجاد مدار [۱۴۲]

بسته‌های ارسال شده در شبکه Tor معمولاً سلول نامیده می‌شوند. هر سلول Tor دارای طول ثابتی برابر با ۵۱۲ بایت است و از هر دو هدر و بارگذاری تشکیل شده است. هدر ضروری است زیرا از یک

شناسه مدار تشکیل شده است که برای شناسایی مداری که یک سلول معین متعلق به کدام مدار است استفاده می‌شود. این مهم است زیرا چندین مدار را می توان در یک اتصال TLS مالتی پلکس کرد. همچنین در هدر یک فیلد دستوری وجود دارد که توضیح می‌دهد که با بار سلولی چه باید کرد [11]. سلول‌ها را می‌توان به سلول‌های کنترل یا سلول‌های رله طبقه بندی کرد. سلول‌های کنترلی برای ارسال دستورات، ایجاد یا تخریب استفاده می‌شوند، جایی که می‌توان از padding برای نگه‌داشتن و پیوند استفاده کرد، از create برای راه‌اندازی یک مدار جدید و از بین بردن مدار قبل استفاده می‌شود. سلول‌های رله سلول‌هایی هستند که حاوی داده‌های واقعی هستند که به سمت نقاط انتهایی جریان هدایت می‌شوند [10]. این سلول‌ها دارای یک هدر اضافی به نام هدر رله هستند که شامل یک شناسه جریان به منظور چندگانه‌سازی جریان‌های متعدد، یک جمع کنترلی برای بررسی یکپارچگی انتها به انتها، یک فیلد طول بار و یک فرمان رله است. همانند دستورات کنترلی، این دستورات رله اهداف مشابهی را انجام می دهند، اما چند دستور دیگر مانند گسترش به منظور گسترش مدار توسط یک رله، و همچنین دستوراتی برای باز کردن و بستن مدار و ارسال اعلان ها نیز دارند.

ضرورت انجام تحقیق :

باتوجه به در دسترس بودن شبکه وب تاریک و همچنین ناشناس بودن هویت کاربر، این شبکه می‌تواند محلی جهت انجام کارهای غیر قانونی و غیر انسانی اعم از آدم ربایی، قتل، نقشه‌های جاسوسی و امنیتی، مسائل یا فسادهای اخلاقی و ... باشد. لذا سازمان‌ها و نهادهای قانونی مرتبط، بدنبال راهی جهت شناسایی و پیشگیری از رخداد مسائل ذکر شده هستند.

چنانچه این حضور و شناسایی در وب تاریک به درستی انجام نشود و نهادهای قانونی نتوانند ارتباطات تبهکارانه در آن را کنترل و رهگیری کنند، با توجه به احساس امنیت مجرمین و تبهکاران در این فضا، اقبال آنان به استفاده از وب تاریک بیشتر و بیشتر می‌شود و در نهایت توانایی کشف جرائم و اعمال قانون توسط نیروهای امنیتی و انتظاماتی به صورت بحرانی کاهش پیدا می‌کند.

حضور نیروی انسانی پلیس و دیگر نهادها در وب تاریک و انجام امور قانونی به صورت سنتی در آن، مانند ماموران مخفی و یا ایجاد سرویس‌های تله برای مجرمین، یکی از راه‌های کنترل این فضا است. اما این به تنهایی کافی نیست، چرا که هزینه اینگونه عملیات و نیروی انسانی حاضر در آن بسیار بالا است، و از طرف دیگر اینگونه روش‌های سنتی محدودیت‌های خاص خود را دارند و توانایی پوشش تمام اتفاقات در حال وقوع در وب تاریک را ندارند. بنابراین تحقیق و توسعه روش‌های فنی و خودکار برای شناسایی و نفوذ به وب تاریک تبدیل به یک ضرورت شده است تا نهادهای قانونی بتوانند همانند دهه‌های گذشته،

امنیت را در جامعه فراهم کنند.

مدل تهدید

در مقالات و مطالعات انجام شده قبلی تهدیدات را در انواع مختلفی تقسیم بندی کرده‌اند و دیدگاه‌های متفاوتی در این مورد وجود دارد. در این قسمت به یکی از این دیدگاه‌ها پرداخته می‌شود.

محبوبیت زیاد Tor منجر به توسعه تعداد زیادی از حملات غیرگمنام سازی در شبکه شده است. این حملات با گذشت زمان به طور فزاینده‌ای پیشرفته تر و مؤثرتر می‌شوند. از جمله قابل توجه‌ترین حملات، حمله سایبل[۴] است که بر این ایده استوار است که هر سیستمی که به نهادهای اعتماد توزیع شده متکی باشد می‌تواند هویت‌های متعددی را جعل کند. این شامل افزودن حدود ۱۱۵ سرور کامپیوتری جاسوسی شده به Tor که به کاربران اطمینان می‌دهد تا استفاده کنند. سرورها بیش از ۶ درصد از ظرفیت محافظت شبکه را در اختیار گرفتند. این حمله سبب جلب توجه بیشتر به شبکه Tor شد، زیرا اطلاعات به دست آمده توسط حمله کننده اطلاعات کاربران را که به چه سایت‌های مخفی متصل شده‌اند را شناسایی کرد.

بیشتر حملات به Tor بر روی شناسایی رابطه بین یک کلاینت و سروری که از شبکه Tor برای برقراری ارتباط استفاده می‌شود، تمرکز می‌کنند [6]. این فرآیند به عنوان غیرگمنام‌سازی[۵] [7] شناخته می‌شود. کلاینت یک مدار در شبکه Tor به یک گره خروجی ایجاد کرده است و گره خروجی با سرور ارتباط برقرار می‌کند. مهاجم می‌خواهد تأیید کند که کلاینت و سرور در حال ارتباط هستند و می‌خواهد یک نام مستعار (که در آن یک سرویس مخفی ارائه می‌شود) را به هویت واقعی اپراتور، مستقیماً یا از طریق مرحله‌ای میانی (مثلاً یک مکان فیزیکی یا آدرس IP) به هویت واقعی اپراتور مرتبط کند [12]. متداول‌ترین تهدید بر اساس یک دشمن منفعل است که می‌تواند بخشی از شبکه Tor را مشاهده کند و می‌تواند مسیریاب‌های پیاز خود را به خطر بیاندازد و راه‌اندازی کند. چنین مهاجمی به سادگی ورودی‌ها و خروجی‌های شبکه را مشاهده می‌کند و الگوهای آن‌ها را به هم مرتبط می‌کند، به اصطلاح تحلیل ترافیک انجام می‌دهد[۸]. مهاجم سعی می‌کند شباهت‌های ترافیکی را که مشتری ارسال می‌کند و ترافیکی که سرور دریافت می‌کند اندازه‌گیری کند. تجزیه و تحلیل ترافیک معمولاً در حملات به سرویس‌های مخفی که سعی در بی‌نام کردن کاربران دارند استفاده می‌شود [۱۴]. Tor در برابر یک دشمن منفعل جهانی محافظت نمی‌کند. تمرکز آن جلوگیری از حملاتی است که در آن مهاجم سعی

[4] Sybil attack

[5] de-anonymization

می کند تعیین کند که در کدام نقاط شبکه یک حمله مبتنی بر الگوی ترافیک باید اجرا شود. با دشوار کردن کار برای یک مهاجم جهت تعیین محل حمله، یک حمله دقیق دشوار است [9].

یک دشمن فعال نیز یک فرض رایج در مدل تهدید Tor است [6]. چنین مهاجمی حدس می‌زند که چه کسی با چه کسی ارتباط برقرار می‌کند و می‌تواند پیوندهای شبکه‌ای را تجزیه و تحلیل کند تا این ظن را تأیید کند [12]. آنها توانایی تزریق، حذف یا اصلاح ترافیکی را دارند که از طریق OR در خطر منتشر می شود. از آنجایی که دشمنان فعال آسان‌تر شناسایی می‌شوند، تلاش‌های تحقیقاتی متعددی برای توسعه اقدامات متقابل مختلف برای دفاع در برابر این تهدیدها صورت گرفته است.

در سیستم‌هایی مانند Tor، که توسط داوطلبان تحت کنترل محدود اداره می‌شود، همچنین یک نگرانی وجود دارد که یک مهاجم بخشی از شبکه ناشناس را کنترل کند [8]. با این حال، غیر واقعی است که چنین شخصی همه گره‌ها را کنترل کند. بنابراین این نوع حملات در تمرکز مدل تهدید Tor نیست [9]. توسعه‌دهندگان Tor مراقب هستند، اما همچنان به کاربران خود در مورد استفاده از Tor در موقعیت‌های حیاتی از طریق پیامی هنگام راه‌اندازی Tor هشدار می‌دهند: «این نرم‌افزار آزمایشی است. برای ناشناس ماندن قوی به آن تکیه نکنید.» [4]

دسته‌بندی تکنیک‌ها و حملات غیر گمنام سازی

با توجه به تکنیک‌های غیرگمنام‌سازی موجود در شبکه Tor، می‌توانیم این تکنیک‌ها را از دو دیدگاه مختلف به دو گروه دسته‌بندی کنیم:

- حملات غیرفعال و فعال دشمن می‌تواند به طور منفعلانه ترافیک شبکه را مشاهده کند یا به طور فعال ترافیک را دستکاری کند.
- حملات لایه انتها و انتها به انتها مهاجم می تواند ناشناس بودن شبکه را با نظارت یا کنترل مدارهای Tor در سمت رله ورودی یا رله خروجی یا در هر دو لبه مدار تحمیل کند.

بر اساس روش و هدف، حملات را می‌توان به هفت گروه طبقه بندی کرد:

حملات همبستگی حمله غیرفعال انتها به انتها[6]

حملات همبستگی، حملات غیر گمنام‌سازی معروف هستند. در این دسته از حملات فرض بر این است که مهاجم هم گره ورودی و هم گره خروجی مدار بین مشتری و سرور را کنترل می‌کند. مهاجم به

[6] Correlation Attacks End-to-end Passive Attack

دنبال ارتباطی در ترافیک بین گره ورودی و گره خروجی است، زیرا در این صورت می‌تواند نتیجه بگیرد که گره ورودی و گره خروجی در مدار مشارکت دارند. گره ورودی مشتری را می‌شناسد، گره خروجی سرور را می‌شناسد، بنابراین مهاجم می‌تواند تایید کند که کلاینت و سرور در حال ارتباط هستند.

حملات تراکم حمله فعال سرتاسر[7]

در یک حمله تراکم، یک حریف سعی می‌کند هویت مسیریاب‌های پیازی را که مداری را تشکیل می‌دهند که توسط مشتری هدفمند Tor ساخته شده است، تعیین کند. برای دستیابی به این هدف، حریف رله‌ها را یکی یکی متراکم می‌کند و به تفاوت‌های تاخیر در جریان ترافیک هدف گوش می‌دهد. یک دشمن می‌تواند تفاوت‌های تاخیر را با ازدحام رله‌ها اندازه‌گیری کند، در حالی که یک کلاینت در حال دانلود یک فایل بزرگ از a توسط وب‌سایت تحت کنترل دشمن است، تا زمانی که دشمن تشخیص دهد که سرعت دانلود کاهش یافته است. روش دیگر تزریق اسکریپتی است که به صورت دوره ای درخواست های HTTP را انجام می دهد و رله های متراکم را شروع می کند تا زمانی که فرکانس درخواست کاهش یابد. هدف از این حمله نشان دادن برخی یا همه OR هایی است که مدار ایجاد شده توسط یک کلاینت را برای یک سرور خراب تشکیل می‌دهند [13].

حملات زمان بندی حمله فعال انتها به انتها[8]

حملات زمان‌بندی شکل دیگری از حملات غیرگمنام‌سازی هستند. در طول یک حمله زمان‌بندی، حریف هم ورودی و هم رله خروجی مشتری هدف را دستکاری می‌کند. با همبستگی الگوهای جریان در ترافیک جریان از گره ورودی به ترافیک جریان به گره خروجی، دشمن می‌تواند تعیین کند که یک کلاینت با کدام سرور در ارتباط است.

حمله غیرمستقیم کاهش نرخ گیلاد و هرزبرگ این حمله زمان بندی را در سال ۲۰۱۲ معرفی کردند. این حمله از قابلیت پیش بینی گره‌های خروجی که یک OP انتخاب می‌کند و الگوریتم کنترل تراکم در پروتکل به نفع خود استفاده می‌کند. گیلاد و هرزبرگ خاطرنشان کردند که این حمله به طور کامل آزمایش نشده است، اما آنها برخی آزمایشات اولیه را انجام دادند که به خوبی انجام شد.

حملات اثرانگشتی حمله غیرفعال یک طرفه[9]

در یک حمله اثر انگشتی، دشمن از این واقعیت استفاده می کند که ترافیک اغلب دارای ویژگی های

[7] Congestion Attacks End-to-end Active Attack
[8] Timing Attacks End-to-end Active Attack
[9] Fingerprinting Attacks Single-end Passive Attack

بسیار متمایز است. این اثرانگشت های ترافیکی را می توان برای شناسایی صفحه وب مورد درخواست مشتری، اینکه آیا یک کلاینت به یک سرویس مخفی متصل است یا برای به دست آوردن دانش در مورد مسیری که ترافیک از طریق شبکه در حال حرکت است استفاده کرد.

حملات انکار سرویس حمله فعال تک پایانی[10]

حملات انکار سرویس (DoS) برای گمنام کردن کاربران استفاده نمی‌شوند، بلکه منابع شبکه قربانی را پر می‌کنند که منجر به اتصال بسیار کند یا غیرقابل دسترس شدن آن می‌شود. همچنین می‌توان از آن برای وادار کردن کاربران صادق به استفاده از رله‌های مخرب استفاده کرد، زیرا می‌توان رله‌های صادق را در دسترس قرار داد. به طور معمول قربانی یک حمله انکار سرویس توزیع شده (DDoS) سوء استفاده از بات نت هنگامی که فرمان و کنترل[11] (C&C) یک بات نت به عنوان یک سرویس پنهان Tor در آگوست ۲۰۱۳ اجرا شد، تعداد کاربران متصل از ۱ میلیون به ۶ میلیون افزایش یافت. هدف این حمله قربانیان خاصی نبود، بلکه بر کل شبکه Tor تأثیر داشت. در حالی که میزان ترافیک افزایش چشمگیری نداشت، به دلیل افزایش بار پردازش روی رله ها، زمان دانلود فایل های کوچک را دو برابر کرد. گلوگاه پروتکل تبادل کلید بود که برای ساخت مدارهای رمزگذاری شده مورد نیاز است. از آنجایی که C&C به عنوان یک سرویس مخفی اجرا می شد، همه سیستم‌های تحت کنترل بات نت به طور دوره‌ای مدارهایی را برای سرویس مخفی ایجاد می کردند.بسته های UDP زیادی را از منابع بسیاری ارسال می کند، اما از آنجایی که Tor فقط جریان‌های TCP را انتقال می‌دهد، این نوع DDoS در Tor امکان پذیر نیست.

حملات حمایتی طبقه بندی نشده است[12]

این نوع از حملات مستقیماً هدفشان غیرگمنام کردن کاربران Tor یا مختل کردن شبکه Tor نیست، بلکه برای انجام یک حمله غیرگمنام‌سازی یا یک حمله مخرب در زمان مناسب است.

تأثیرگذاری بر انتخاب گارد Tor بیشتر حملات به Tor حملات همبستگی ترافیکی هستند، جایی که هم گره ورودی و هم گره خروجی برای انجام حمله مورد نیاز هستند، برای مهاجم می‌تواند مفید باشد که مشتری را مجبور کند یک گره مخرب را به عنوان گره نگهبان انتخاب کند، یا نگهبان ورودی یک کلاینت فقط از گره های محافظ به عنوان گره‌های ورودی Tor استفاده می‌کند. این بدان معنی است

[10] Denial of Service Attacks Single-end Active Attack
[11] command & control
[12] Supportive Attacks Not classified

که اگر هیچ یک از گره‌های محافظ مخرب نباشد، کاربر هرگز نمی‌تواند به یک گره ورودی مخرب متصل شود. گره‌های نگهبان معمولاً پس از ۳۰ یا ۶۰ روز تعویض می‌شوند[13]. جایگزینی در یک دور انتخاب گارد به اصطلاح انجام می‌شود، که در آن مجموعه‌ای از گره‌های نگهبان انتخاب نشده انتخاب می‌شوند تا در لیست نگهبان قرار گیرند. احتمال اینکه یک گره نگهبان در لیست نگهبان گنجانده شود برای گره‌های طولانی مدت یا با پهنای باند بالا بیشتر است.

افشای حملات سرویس‌های پنهان طبقه بندی نشده است[۱۳]

در این مورد، برچسب "طبقه بندی نشده" به این معنی است که حملاتی که به دسته مربوطه تعلق دارند، اغلب هر دو نوع تکنیک را با هم ترکیب می‌کنند.

ممکن است برای یک مهاجم جالب باشد که یک سرویس مخفی را فاش کند. این نوع حمله به ویژه برای دولت‌هایی که سعی می‌کنند مکان یک سرویس مخفی را مشخص کنند بسیار جالب است.

جدول زیر حملات منتشر شده به Tor و نوع آنها را در سال‌های متوالی نشان می‌دهد.

جدول ۱: جدول زمانی سیزده سال حمله به تور

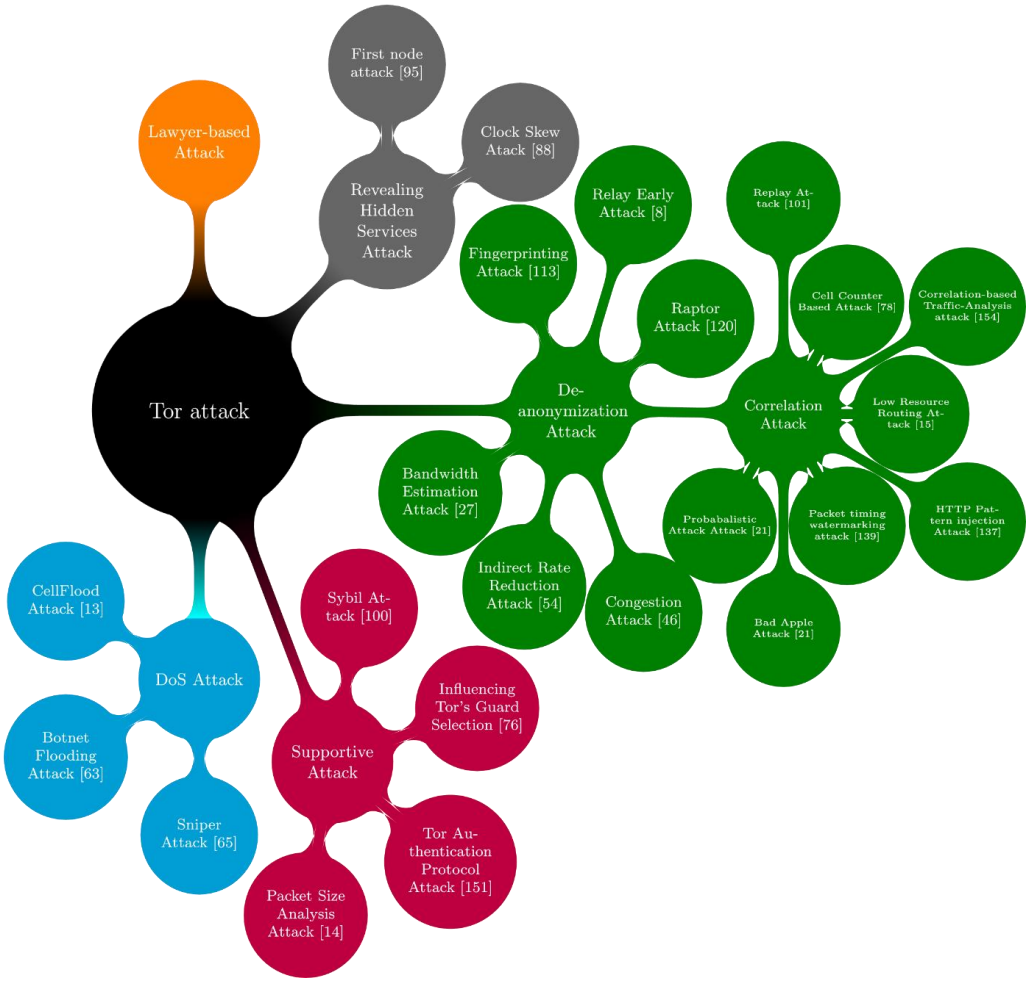
Year	Attack	Category
2016	Sybil Attack	Supportive Attack
2015	Guard Selection Attack	Supportive Attack
2015	RAPTOR Attack	Correlation Attack + Supportive Attack
2015	Torben Attack	Correlation Attack/ Side-channel Attack
2015	Circuit Fingerprinting	Fingerprinting Attack
2014	The Sniper Attack	DoS attack
2014	BotNet Flooding Attack	DoS Attack
2014	Relay Early Attack	Correlation Attack
2013	CellFlood Attack	DoS Attack
2013	Hidden Service Attack	DoS Attack
2012	Indirect Rate Reduction Attack	Timing Attack
2012	HTTPOS Website Fingerprinting	Fingerprinting Attack
2012	StegoTorus Attack	Supportive Attack
2011	HTTP-based application-level attack	Correlation Attack
2011	Packet Size Attack	Supportive Attack
2011	Bad Apple Attack	Correlation Attack
2011	Loop Attack	DoS Attack
2011	Throughput Fingerprinting	Fingerprinting Attack
2010	Traffic Analysis Attack	Correlation Attack
2010	Bandwidth Estimation Attack	Correlation Attack + Timing Attack
2010	Passive Linking Attack	Correlation Attack
2010	Client Location Attack	Correlation Attack
2010	Adaptive Surveillance Attack	Correlation Attack
2009	Cell Counter Based Attack	Correlation Attack

[13] Revealing Hidden Services Attacks Not classified

2009	Protocol-level Attacks	Correlation Attack + Supportive Attack
2009	FortConsult Security Attack	Correlation Attack
2009	Bayesian Traffic Analysis Attack	Correlation Attack + Supportive Attack
2009	Practical Congestion Attack	Congestion Attack
2009	Website Fingerprinting	Fingerprinting Attack
2009	Bridge Deanonymization Attack	Supportive Attack
2009	Link-Based Relay Selection Attack	Supportive Attack
2009	Tor Authentication Protocol Attack	Supportive Attack
2009	AS Awareness Attack	Correlation Attack + Supportive Attack
2008	Route Fingerprinting	Fingerprinting Attack
2008	Package Spinning Attack	DoS Attack
2008	Replay Attack	Correlation Attack
2008	Passive logging Attack	Correlation Attack
2007	Low Resource Routing Attack	Correlation Attack
2007	Connection Start Tracking attack	Correlation Attack
2007	Packet Counting Attack	Correlation Attack
2007	Stream Correlation Attack	Correlation Attack
2007	Packet Timing Watermarking Attack	Correlation Attack + Timing Attack
2006	Clock Skew Attack	Revealing Hidden Services
2006	First Node Attack	Revealing Hidden Services
2005	Congestion Attack	Congestion Attack
2004	Predecessor Attack	Supportive Attack
2004	Intersection Attack	Correlation Attack
2003	Active n - 1 Attack	Correlation Attack
2003	Website Fingerprinting	Fingerprinting Attack
2003	Robust Watermark Correlation Attack	Correlation Attack + Timing Attack
2003	Statistical Disclosure Attack	Correlation Attack

همینطور که از جدول ارائه شده مشخص است زمان اولین حمله به Tor در سال ۲۰۰۳ و از نوع حمله همبستگی می‌باشد، و آخرین حمله نیز در سال ۲۰۱۶ و از نوع حمله حمایتی می‌باشد. و همچنین در سال‌های آخر حملات حمایتی و ترکیب حملات حمایتی با حملات همبستگی بیشتر مورد توجه قرار گرفته‌اند.

شکل زیر یک نقشه ذهنی را نشان می‌دهد که حملات را دسته بندی کرده است. چنانچه در شکل هم مشخص می‌باشد بیشترین نوع حملات از نوع حملات همبستگی و حملات غیرگمنام‌سازی می‌باشد.



شکل ۲: نقشه ذهنی که شامل تمام حملات مهم بر روی شبکه تور است که منتشر شده است.

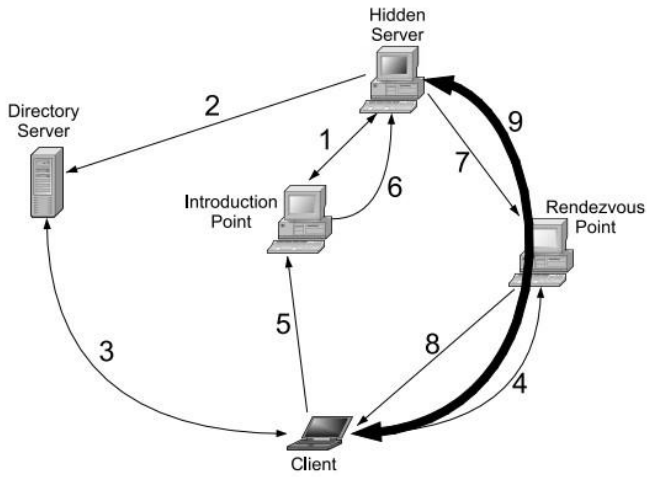
مسئله و اهداف اصلی تحقیق :

وب‌تاریک بخشی از اینترنت است که به صورت ساده و آشکار مورد دسترسی کاربران قرار ندارد. در این زیربخش از اینترنت ارتباطات بین کاربران و سرورها به صورت ناشناس برقرار می‌شود، به این معنی که کاربر و سرور هیچ‌یک به آدرس واقعی یکدیگر دسترسی پیدا نمی‌کنند. در ابتدا هدف از این شبکه‌ها، برقراری ارتباط غیرقابل شناسایی با اهداف نظامی و اطلاعاتی بوده است اما به مرور به یک ابزار عمومی برای کسانی که نیاز به ارتباط گمنام دارند تبدیل شده است.

با گذشت زمان و در اختیار قرار گرفتن این ابزار برای عموم، توانایی آن در گمنام‌سازی باعث توجه اقشار مختلفی از جوامع به آن گردید. علاوه بر استفاده‌های مفیدی که می‌توان برای گمنام‌سازی درنظر گرفت، تبهکاران و خلافکاران نیز تمایل زیادی به استفاده از ارتباطات ناشناس دارند که باعث سوء استفاده‌های زیادی از جمله فروش مواد مخدر، عملیات تروریستی، تجارت و مفاسد غیراخلاقی و ... از آن گردید. بنابراین سازمان‌های قانونی نیز مجبور به ورود به این فضا و رصد آن گشتند که منشاء تحقیقات بسیاری

در مورد راه‌های نفوذ به وب تاریک و جمع‌آوری اطلاعات از آن گردید.

Tor بزرگترین شبکه ارتباطی در وب تاریک است که از آن برای گمنام‌سازی (پنهان‌سازی) ارتباط بین کاربر و سرور استفاده می‌شود. تاکنون تحقیقات بسیاری آسیب‌پذیری‌های Tor's Onion Router را مورد بررسی قرار داده‌اند و کارایی و موفقیت آن را به چالش کشیده‌اند. سرویس مخفی[14] (HS) یک سرویس شبکه است که مکان سرورهای آن توسط شبکه Tor مخفی می‌شود. با ظهور سرویس‌های مخفی تور، امکان راه‌اندازی سایت‌هایی که قابل ردیابی نباشند فراهم گردید و در واقع گمنام‌سازی دو طرفه گردید. این سایت‌ها محل اصلی قرارگیری کسب و کارهای تبهکارانه هستند و یکی از نیازهای اصلی سازمان‌های قانونی، شناسایی و در واقع غیرگمنام‌سازی این سایت‌ها است. با وجود اینکه گمنام‌سازی هدف اصلی راه‌اندازی سرویس‌های مخفی است، اما مانند هر سرویس امنیتی دیگری آنها نیز آسیب‌پذیری‌هایی دارند. آسیب‌پذیری‌های سرویس‌های مخفی Tor به طور فزاینده‌ای با حملات غیرگمنام‌سازی مورد حمله قرار می‌گیرد. با گذشت زمان، حملات پیچیده‌تر و مؤثرتر شده‌اند و نیاز به حملات ترکیبی افزایش یافته است که می‌تواند در لایه شبکه، لایه پروتکل یا لایه برنامه انجام شود. شکل زیر مراحل اتصال به یک سرویس مخفی بر اساس پروتکل آن را نشان می‌دهد [5]:



شکل ۳: تنظیم عادی ارتباطات سرویس مخفی در [تور ۹۵]

هدف از این تحقیق بررسی حملات انجام شده به سرویس‌های مخفی تور، دسته‌بندی و تجزیه و تحلیل حملات منتشر شده به آن از نظر تاریخچه و میزان اثر بخشی، و نهایتا ارائه یک روش جدید برای حمله به سرویس‌های مخفی تور است.

[14] Hidden Service

فصل دوم

۲-۱- مقدمه

وب تاریک[۱۵] بخشی از شبکه وسیع جهانی (وب جهانی) است که برای دسترسی به آن به نرم افزارهای خاصی نیاز خواهیم داشت که بعد از وارد شدن به این بخش، وبسایت‌ها وسایر خدمات موجود در آن از طریق یک مرورگر همانند وب معمولی در دسترس قرار خواهند گرفت. در دارک وب وبسایت‌هایی وجود دارند که کاملا پنهان هستند، به طوری که حتی موتورهای جستجو هم نمی‌توانند صفحات این وبسایت‌ها را ایندکس کنند وتنها راه دسترسی داشتن به آن‌ها آدرس جهانی[۱۶] می‌باشد.

در دارک وب فروشگاه‌های خاصی در حال فعالیت هستند که اصطلاحاً "دارک‌نت مارکت[۱۷]" (فروشگاه-های دارک نت) نامیده می‌شوند که عمده محصولات این فروشگاه‌ها غیر قانونی می‌باشند که مواد مخدر وسلاح‌های گرم هم در این فروشگاه‌ها به فروش می‌رسد. پرداخت‌ها در فروشگاه‌های دارک نت معمولا با استفاده از پول‌های مجازی مانند بیت کوین انجام می‌گیرد.

۲-۲- فضای وب

امروزه بدون اغراق تمامی اطلاعاتی که بیشتر افراد کسب می‌کنند با واسطهٔ یا بدون واسطهٔ از طریق اینترنت وموتورهای جستجو می‌باشد. اما این چیزی که در دسترس کاربران قرار دارد تنها ۴٪ تمام

---

[۱۵] dark web

[۱۶] international

[۱۷] Darknet Markets

اطلاعات می‌باشد که به اصطلاح به اینها اطلاعات وب آشکار می‌گویند. وبقیه اطلاعات که در دسترس موتور جستجو قرار ندارد واین موتورها نمی‌توانند آنها را به اصطلاح کاوش کنند وب عمیق نام دارد. این وب عمیق یا به تشخیص موتورهای جستجو کاوش نمی‌شود مانند مشخصات شخصی، نام وشماره تلفن ویا توسط برنامه نویسان برای انجام کارهای مخفی مورد استفاده قرار می‌گیرد که در این صورت به آن وب تاریک می‌گویند.

در واقع قسمتی از اینترنت که به صورت عمدی توسط موتورهای جستجو سرچ نمی‌شود ویا توسط ایجاد کننده این اطلاعات از دسترس خارج شده است، مانند حساب ایمیل شخصی دیگران، حساب کاربری شبکه‌های اجتماعی، حساب کاربری بانکی آنلاین، و صفحات برندینگ از این جمله می‌باشند. که از مهمترین وب‌های عمیق، پایگاه داده‌های دانشگاهی وبانکی می‌باشد که هرگونه دسترسی به این اطلاعات جرم محسوب می‌شود و با فرد به عنوان مجرم برخورد خواهد شد. این قسمت از اینترنت بخش مخوف وخطرناک اینترنت نمی‌باشد ولی بسیاری از مردم وب عمیق را با قسمتی که توضیح داده‌ایم یعنی وب تاریک اشتباه می‌گیرند.

این قسمت از اینترنت در واقع زیر شاخه‌ای از وب عمیق می‌باشد که از دسترس موتورهای جستجو و افراد عادی خارج شده است. این وب‌ها با اهداف خاص که معمولا خطرناک هستند ایجاد می‌شوند. البته یکسری وب تاریک جاسوسی نیز وجود دارد که بسیار پیچیده است و دسترسی به اطلاعات آنها اصلا کار راحتی نمی‌باشد.

تمامی جرم‌های سایبری در این قسمت از اینترنت صورت می‌گیرد. این وب‌ها توسط موتورهای جستجو ایندکس نمی‌شود و فقط افراد خاص با روش‌های خاصی که آموزش دیده‌اند می‌توانند به این صفحات دسترسی پیدا کنند. البته وب‌های تاریک تنها ۰/۰۱٪ وب عمیق را تشکیل می‌دهند. در نظر داشته باشید برای دسترسی به این وب‌ها از مرورگرهای ساده و معمولی نمی‌توان استفاده کرد. و بایستی از نرم افزاری مانند Tor استفاده کنید که تمامی اطلاعات شخصی و مکانی فرد را رمزنگاری می‌کند.

نیمی از فعالیت‌هایی که در وب تاریک اتفاق می‌افتد غیر قانونی است مانند: خرید و فروش مواد مخدر و اسلحه، خرید و فروش برده‌های جنسی و حتی آزار جسمی و جنسی انسان‌ها به صورت آنلاین در این بُعد از اینترنت بدون جا گذاشتن ردی از افراد صورت می‌پذیرد. البته در بعضی مواقع این وب تاریک کاربردی نیز می‌باشد به عنوان مثال: فعالان خبرنگاری و فعالان سیاسی در کشورهایی که تحت سانسور شدید اینترنتی قراردارند می‌توانند بدون جا گذاشتن هیچ رد پایی از خود از این روش بهره‌مند شوند. این بُعد از اینترنت در ابتدا توسط نیروی دریایی ایالات متحده آمریکا مورد استفاده قرار گرفت.

وب تاریک برای به اشتراک گذاشتن اطلاعات ناشناس بدون هیچ نوع سانسور ایجاد شده است، به همین دلیل است که در بسیاری موارد در کشورهایی که آزادی بیان در آنها وجود ندارد و سانسور بخشی از زندگی روزمره است، مورد استفاده قرار می‌گیرد. به دلیل خصوصیات حفظ حریم خصوصی و ناشناس بودن، تبدیل به پناهگاه برای مجرمان می‌شود و به نظر می‌رسد که استفاده از آن فقط به این نوع افراد محدود می‌شود.

وب‌تاریک بخشی از اینترنت است که به صورت ساده و آشکار مورد دسترسی کاربران قرار ندارد. در این زیربخش از اینترنت ارتباطات بین کاربران و سرورها به صورت ناشناس برقرار می‌شود، به این معنی که کاربر و سرور هیچ‌یک به آدرس واقعی یکدیگر دسترسی پیدا نمی‌کنند. در ابتدا هدف از این شبکه‌ها، برقراری ارتباط غیرقابل شناسایی با اهداف نظامی و اطلاعاتی بوده است اما به مرور به یک ابزار عمومی برای کسانی که نیاز به ارتباط گمنام دارند تبدیل شده است.

در اغلب موارد شبکه دارک وب با دیپ وب همسان شمرده می‌شود اما در حقیقت این دو شبکه با هم تفاوت‌هایی دارند و هر دو در یک موضوع و زمینه خاصی فعالیت نمی‌کنند. به طور خلاصه وب عمیق (دیپ وب[۱۸]) به تمام وبسایت‌هایی گفته می‌شود که از طریق موتورهای جستجوگر نمی‌توان به آن‌ها دسترسی پیدا کرد به بیان ساده تمام وبسایت‌هایی که موتورهای جستجو قادر به بایگانی کردن صفحاتشان نیستند در دسته وب عمیق قرار می‌گیرند. بنابراین دارک وب را در حقیقت باید زیر مجموعه‌ای از وب عمیق دانست. اما دارک وب به طور کل از نظر تکنیک‌های ارائه شده در این شبکه با وب عمیق متفاوت است، در اینجا منظور از تکنیک‌ها مجموعه‌ای از محصولات و خدمات می‌باشد که برای همه کاربران اینترنت مورد استفاده قرار نمی‌گیرد و فقط بخشی از کاربران خواهان دستیابی به این محصولات و خدمات هستند که برای مثال می‌توان به وبسایت‌های خرید و فروش مواد مخدر، شرط‌بندی‌های غیر قانونی، وبسایت‌های کودک آزاری، خرید و فروش سلاح‌های جنگی و ... اشاره کرد. پس در واقع وبسایت‌های حاوی خدمات و محصولات غیر مجاز در دیپ وب را با نام دارک وب معرفی می‌کنند.

برای نمونه وبسایت اسلایک‌روآد[۱۹] در شبکه دیپ وب را جزئی از شبکه دارک وب می‌دانند، چرا که این وبسایت در زمینه خرید و فروش مواد مخدر در حال حاظر به فعالیت می‌پردازد! شبکه دیپ وب در کشورهای تمامیت‌خواه معمولا برای دسترسی آزاد و بدون مشکل به شبکه جهانی وب و همچنین به

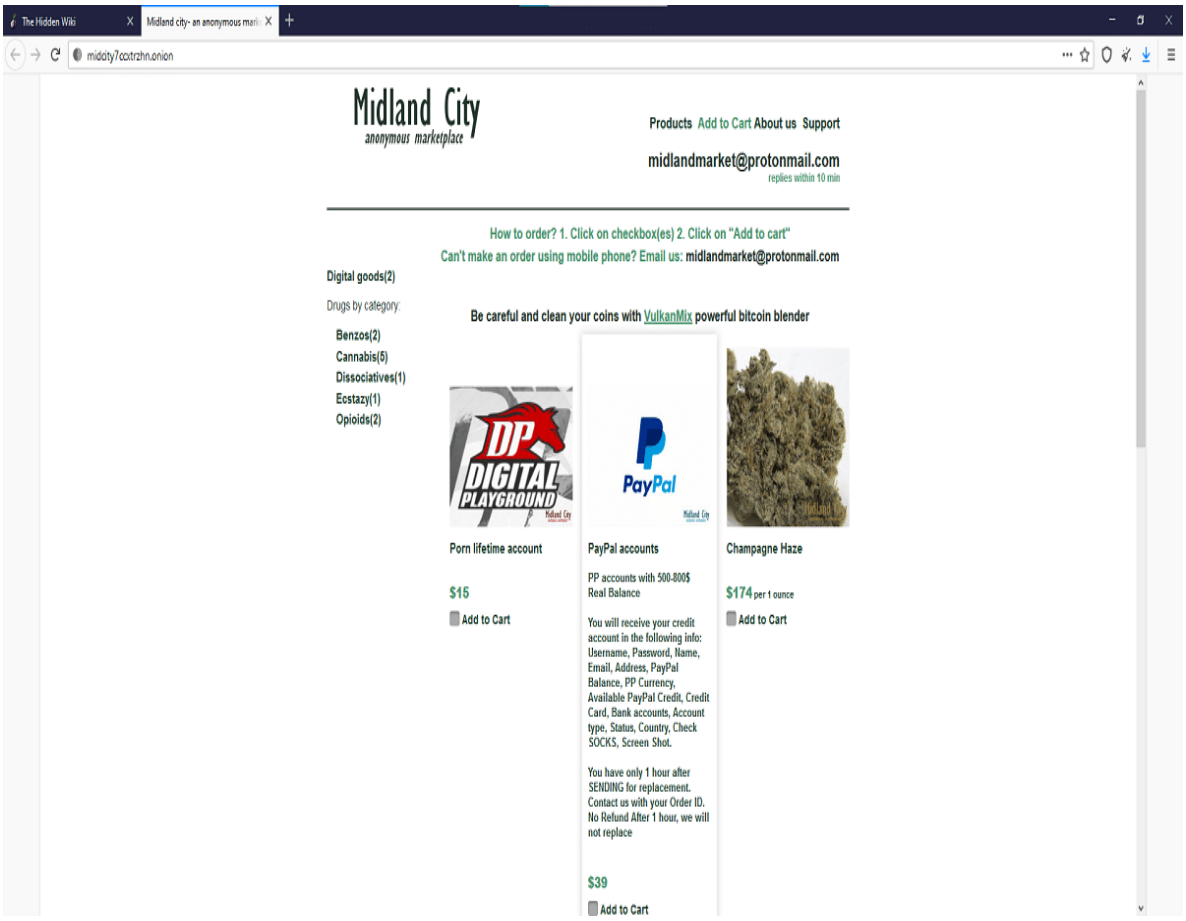
---

[۱۸] Deep Web

[۱۹] Slik Road

منظور شناسایی نشدن مورد استفاده قرار می‌گیرد ولی این موضوع بدین معنا نیست که این شبکه فقط در چنین جوامعی مورد استفاده قرار می‌گیرد، بلکه در کشورهای دموکراتیک نیز این شبکه حتی از جوامع توتالیته هم بیشتر کاربرد دارد که یکی از مهمترین دلایل استفاده از این سرویس در چنین کشورهایی، افشاگری‌های مختلف در خصوص شنود و زیر پا گذاشتن حریم خصوصی کاربران توسط دولت‌ها است.

با گذشت زمان و در اختیار قرار گرفتن این ابزار برای عموم، توانایی آن در گمنام‌سازی باعث توجه اقشار مختلفی از جوامع به آن گردید. علاوه بر استفاده‌های مفیدی که می‌توان برای گمنام‌سازی درنظر گرفت، تبهکاران و خلافکاران نیز تمایل زیادی به استفاده از ارتباطات ناشناس دارند که باعث سوء استفاده‌های زیادی از جمله فروش مواد مخدر، عملیات تروریستی، تجارت موضوعات غیراخلاقی و ... از آن گردید. بنابراین سازمان‌های قانونی نیز مجبور به ورود به این فضا و رصد آن گشتند که منشاء تحقیقات بسیاری در مورد راه‌های نفوذ به وب تاریک و جمع‌آوری اطلاعات از آن گردید.



شکل ۱. صفحات وب تاریک

در وب عمیق می‌توان همه محتواهایی را که در موتورهای جستجو قابل فهرست نباشد پیدا کرد، از آنجا که آنها اطلاعات عمومی نیستند، مانند پرونده‌های میزبانی شده در سرویس‌های ذخیره‌سازی، ایمیل‌ها، نمایش داده‌ها، داده‌های میزبانی شده در خدمات پرداخت مانند اسپوتیفی[۲۰]، نیت‌فلیکس[۲۱]، صفحات روزنامه با پای‌وَلز[۲۲]، درخواست‌هایی که یک صفحه وب با نتایج ایجاد می‌کنند.

وب عمیق با نام اینوسیبل‌وب[۲۳] یا هیدن‌وب[۲۴] نیز شناخته می‌شود، اصطلاحاتی که نحوه کار و نمایندگی آن را توصیف می‌کنند. درون وب عمیق، وب تاریک است. وب تاریک شبکه‌ای است که اطلاعاتی را دسترس ما قرار می‌دهد که برای دسترسی به این اطاعات نیاز به مرورگرهای ویژه می‌باشد.

با توجه به توضیحات داده شده در خصوص وب عمیق و وب تاریک به این نتیجه خواهیم رسید که استفاده از هر موردی نیاز به سواد مخصوص آن مورد را دارد. در میان این حجم افسار گسیخته اطلاعات و دسترسی به اینترنت شاید طوری هدایت شویم که یکی از ابزارهای بازی برای دارک وبی‌ها باشیم حتی بدون اینکه اطلاعی از آن داشته باشیم. این روزها جرائم به سمت سایبری شدن می‌رود چنانچه جنگ‌ها هم به این سو رفته به همین منظور داشتن سواد دیجیتال برای هر رده سنی و شغلی بسیار مهم است. بنابراین در این بخش هدف آن است که بتوانیم با ساختار وب تاریک و ابزارهایی که برای استفاده از این فضا مورد استفاده قرار می‌گیرند آشنا شویم و در نهایت بتوانیم به کمک هوش مصنوعی به اطلاعات مناسبی از این فضا دسترسی پیدا کنیم.

---

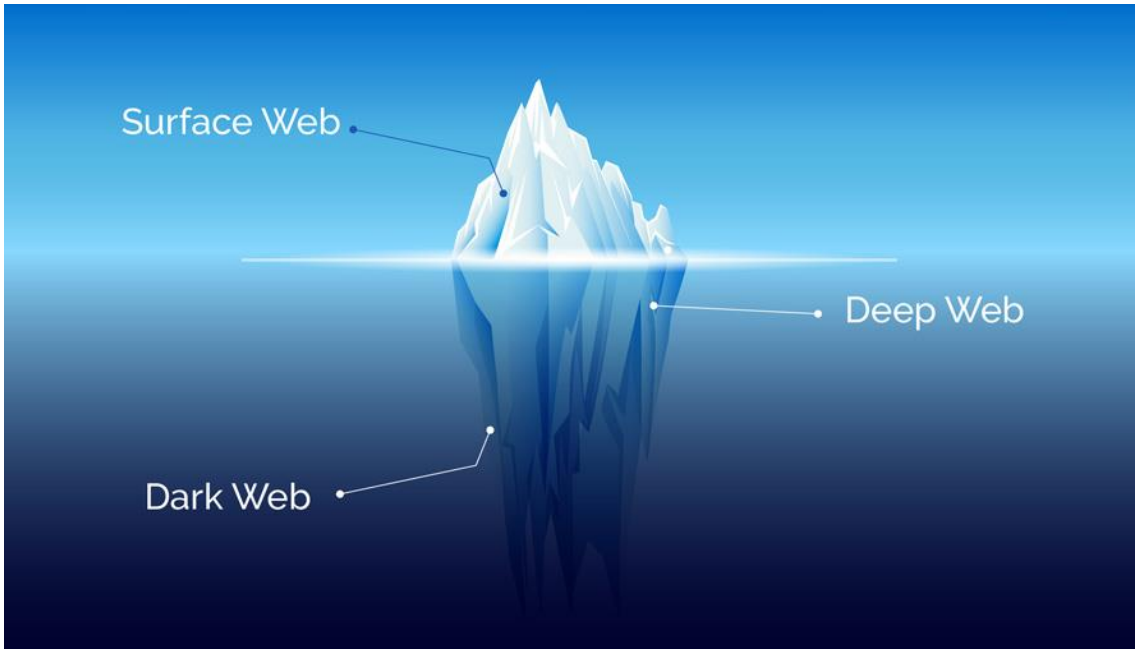
[۲۰] Spotify

[۲۱] Netflix

[۲۲] paywalls

[۲۳] Invisible Web

[۲۴] Hidden Web



شکل ۲. فضای وب

۳-۲- بررسی سه شبکه وب تاریک شامل آی‌توپی[۲۵] – فرینت و تور

در این بخش به بررسی سه شبکه وب تاریک پرداخته می‌شود که در مورد فرینت و آی‌توپی بصورت مختصر اشاره می‌کنیم چرا که بحث و هدف مطالعه ما در این پایان نامه شبکه تور می‌باشد و به همین علت این شبکه بیشتر از دو شبکه دیگر مورد مطالعه و بررسی قرار می‌گیرد.

۱-۳-۲- بررسی شبکه آی۲پی

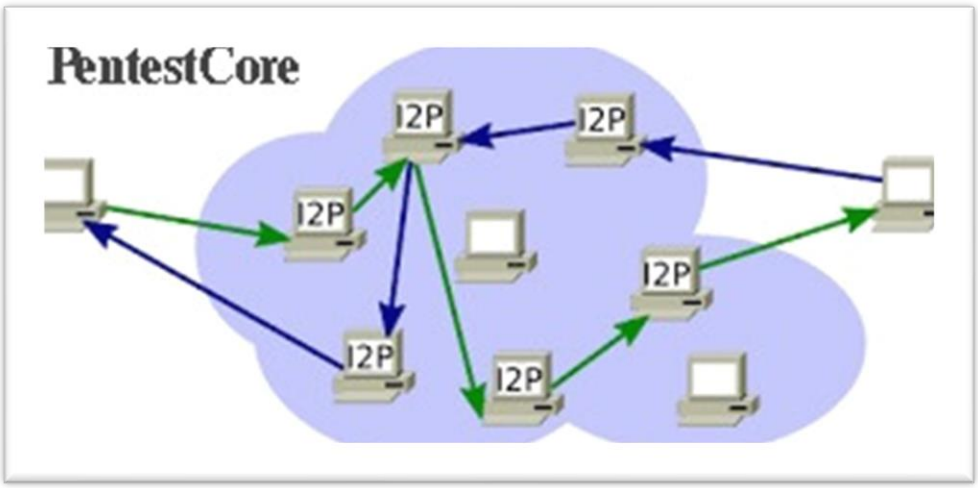
آی۲پی نام پروژه‌ای است تحت عنوان اینترنت پنهان یا نامرئی که شامل یک لایه ناشناس از شبکه است که به کاربران خود این توانایی را می‌دهد که از ارتباطات سانسور شده بصورت عمومی و همگانی بازدید کنند. این ارتباط مخفی و ناشناس از طریق رمز کردن ترافیک فرد (اِند۲اِند[۲۶]) برقرار می‌شود و همچنین ارسال آن از طریق یک شبکه‌ی گسترده در سراسر نقاط جهان صورت می‌گیرد و با وجود مسیرهای بسیار زیاد و متفاوت حمل نقل ترافیک صورت می‌گیرد. اگر بخواهیم به زبان ساده‌تر بیان کنیم آی‌توپی مسیری هموار برای نرم افزارهای کاربردی ایجاد می‌کند تا با نام و آدرس‌های غیر واقعی و امن بتوانند

---

[۲۵] Invisible Internet Project (I2P)

[۲۶] End2End

وبگردی، وبلاگ‌نویسی، چت و انتقال فایل داشته باشند.



شکل ۴: شبکه آی۲پی

مزایایی آی۲پی به شرح زیر است:

- برای مشاهده خدمات پنهان به صورت ناشناس طراحی شده است.
- همسالان فقط بر اساس نمایه‌سازی قوی و عملکرد رتبه‌بندی انتخاب می‌شوند.
- حتی وقتی یک مهاجمی وارد تونل می‌شود، فعالیت را تشخیص می‌دهد.
- تونل‌هایی که حامل پیام هستند کوتاه مدت هستند که از حمله مهاجمان به آن جلوگیری می‌کند.
- همه همسالان و کاربران در مسیریابی شرکت می‌کنند.

شبکه آی۲پی از برنامه‌های کاربردی زیادی جهت انجام بسیاری از فعالیت‌های معمولی مانند مرور اینترنت بصورت ناشناس، چت، اشتراک‌گذاری فایل، ایمیل، وبلاگ‌نویسی و پیوند محتوا، گروه‌ها و کانال‌های خبری و... پشتیبانی می‌کند.

۲-۳-۲- بررسی شبکه تور

تور شبکه‌ای است که امکان مخفی‌سازی هویت کاربران را در فضای اینترنت فراهم می‌کند و از دسترسی سیستم‌های نظارتی، مکان‌یاب و غیره به حریم خصوصی کاربران جلوگیری می‌کند که برای اتصال به این شبکه امنیتی نیاز به نسخه‌ای خاص و تغییریافته از مرورگر فایرفاکس خواهید داشت که تحت‌عنوان

توربروزر[۲۷] شناخته می‌شود.

با استفاده از تور می‌توانید در فضای وب بدون شناخته شدن به گشت‌وگذار بپردازید و این در حالی است که تور برای محافظت از کاربران خود در برابر جاسوسی این امکان را می‌دهد تا هویت واقعی خود را پنهان نگه دارند. توسعه و نگهداری تور توسط یک سازمان شخصی به نام تورپروجکت[۲۸] انجام می‌شود و این در حالی است که کمک‌های مالی هم غالباً از سمت دولت‌های آمریکا، سوئد و برخی اسپانسرهای دیگر ارائه می‌شود.

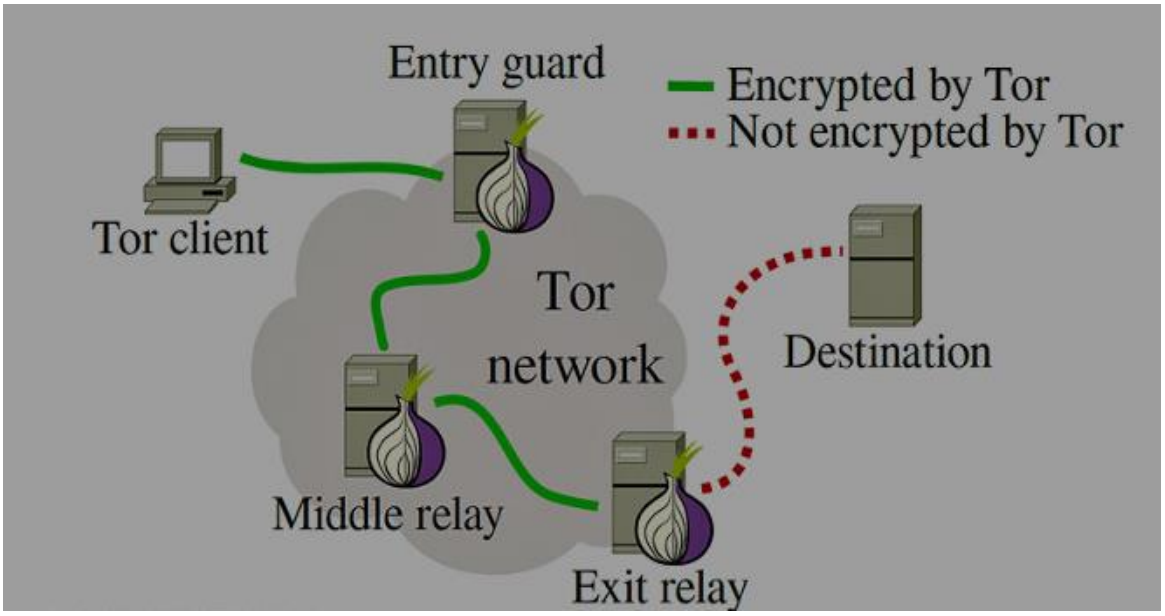
تور بر اساس ایده مسیریاب پیاز که توسط Paul Syverson، Micheal G Reed و David Goldschlag در آزمایشگاه‌های Naval آمریکا در دهه ۹۰ میلادی توسعه داده شده بود، بنا گردیده است. نسخه آلفای پروژه The Onion Router یا به صورت خلاصه TOR توسط Roger Dingledin و Nick Mathewson توسعه داده شد و در بیستم سپتامبر ۲۰۰۲ منتشر شد و همچنین لازم به ذکر است که توسعه این پروژه نیز زیر چتر مالی Electronic Frontier Foundation یا به اختصار EFF ادامه دارد.

نحوه کارکرد تور بدین صورت است که با مفهومی تحت‌عنوان Onion Router (روتر پوست‌پیازی) ابتدا اطلاعات کاربر به اصطلاح رمزنگاری می‌شود سپس در بین رِله‌های مختلفی که در شبکه تور وجود دارد جابه‌جا می‌شود. همچنین رمزنگاری چندلایه باعث امنیت هویت کاربر می‌شود که برای درک بهتر سازوکار تور، همان‌طور که در تصویر زیر ملاحظه می‌کنید، می‌توانید لایه‌های مختلف یک پیاز را در نظر بگیرید:

---

[۲۷] Tor Browser

[۲۸] Tor Project



شکل ۳. ساختار شبکه TOR

در هر رله تور، یک لایه رمزنگاری - رمزگشایی وجود دارد و باقی اطلاعات به رله بعدی، که کاملاً تصادفی انتخاب می‌گردد، ارسال می‌شود تا به مقصد نهایی برسد و آخرین رله، که اطلاعات را به سرور مورد نظر می‌دهد، به عنوان منبع اصلی اطلاعات خواهد بود که در نتیجه پیگیری هویت کاربر یا سرور برای هرگونه سرویس نظارتی کار مشکل و پیچیده‌ای خواهد بود. (جدای از اینکه سرویس Tor به کاربران امکان گمنامی و ناشناس بودن می‌دهد، این سرویس را می‌توان برای سرویس‌های به اصلاح P2P مثل BitTorrent برای دانلود تورنت در بستر اینترنت نیز تنظیم کرد.)

بهبودهای تور نسبت به نسخه قدیمی اونیون روتینگ به شرح زیر می‌باشد:

- **رازداری کامل:** در طرح اصلی اونیون روتینگ، یک گره متخاصم می‌تواند ترافیک را ثبت کند و بعداً گره‌های متوالی را در مدار به خطر بیاندازد و آنها را مجبور به رمزگشایی کند. به جای استفاده از یک ساختار داده چندگانه رمزگذاری شده (یک پیاز) برای قرار دادن هر مدار، Tor اکنون از یک طراحی مسیرسازی افزایشی یا تلسکوپی استفاده می کند، جایی که آغازگر کلیدهای جلسه را با هر پرش متوالی در مدار مذاکره می‌کند. هنگامی که این کلیدها حذف می‌شوند، گره‌های در معرض خطر بعدی نمی‌توانند ترافیک قدیمی را رمزگشایی کنند. به عنوان یک مزیت جانبی، تشخیص پخش مجدد پیاز دیگر ضروری نیست، و فرآیند ساخت مدارها قابل اعتمادتر است، زیرا آغازگر می‌داند چه زمانی یک هاپ از کار می‌افتد و سپس می‌تواند به یک گره جدید گسترش یابد.

- **جداسازی "پاکسازی پروتکل" از ناشناس بودن:** مسیریابی پیاز در اصل به یک " برنامه پراکسی " جداگانه برای پشتیبانی هر برنامه نیاز داشت – که اکثر آنها هرگز نوشته نشدند، بنابراین بسیاری از برنامه‌ها هرگز پشتیبانی نمی‌شدند. Tor از رابط پروکسی استاندارد SOCKS که تقریباً همه جا کاربرد دارد [۳۰] استفاده می‌کند و به ما این امکان را می‌دهد تا از اکثر برنامه‌های مبتنی بر TCP بدون تغییر پشتیبانی کنیم. برای پاکسازی پروتکل HTTP و HTTPS، Tor به Tor button [۳۶] (افزونه فایرفاکس) و تغییراتی که در نسخه فایرفاکس که به عنوان بخشی از بسته مرورگر Tor به کاربران تحویل داده شده است، وابسته است.
- **بدون ترکیب، لایه‌گذاری یا تغییرشکل ترافیک (تاکنون):** Onion Routing در ابتدا خواستار دسته‌بندی و مرتب‌سازی مجدد سلول‌ها به محض ورود آنها بود، و در طراحی‌های بعدی، لایه‌گذاری بین پروکسی‌های پیاز (کاربران) و ORها را اضافه می‌کرد [۲۵، ۳۹]. مبادله بین حفاظت از لایه و هزینه مورد بحث قرار گرفت و الگوریتم‌های تغییرشکل ترافیک [۴۷] برای ارائه امنیت خوب بدون لایه‌های گران‌قیمت تئوری شد، اما هیچ طرح لایه‌گذاری محکمی پیشنهاد نشد.
- **توانایی به اشتراک گذاری یک مدار مشترک به وسیله بسیاری از جریان‌های TCP:** Onion Routing در ابتدا یک مدار مجزا برای هر درخواست سطح برنامه ایجاد کرد، اما این به چندین عملیات کلید عمومی برای هر درخواست نیاز داشت، و همچنین تهدیدی برای ناشناس ماندن از ساخت مدارهای بسیار بود. Tor چندین جریان TCP را در امتداد هر مدار چندگانه می‌کند تا کارایی و ناشناس بودن را بهبود بخشد، اما به کاربر اجازه می‌دهد تا کنترل کند که کدام جریان ممکن است مداری را با کدام جریان‌های دیگر به اشتراک بگذارد تا از پیوند ناخواسته نام‌های مستعار جلوگیری کند.
- **توپولوژی نشتی مسیر مدار:** از طریق سیگنال‌دهی در باند درونی مدار، آغازگرهای Tor می‌توانند ترافیک را به سمت گره‌های موجود در قسمتی از مدار هدایت کنند. در صورت مشاهده ترافیک مختل شده در انتهای مدار این رویکرد جدید به ترافیک اجازه خروج از مدار را می‌دهد.
- **کنترل تراکم:** طرح‌های ناشناس قبلی به تنگناهای ترافیکی نمی‌پردازند. متأسفانه، روش‌های معمول برای متعادل‌سازی بار و کنترل جریان در شبکه‌های همپوشانی شامل ارتباطات کنترل بین گره‌ای و نماهای کلی از ترافیک است. کنترل ازدحام غیرمتمرکز Tor از آک‌های انتها به انتها برای حفظ ناشناس بودن استفاده می‌کند و در عین حال به گره‌های کناری شبکه اجازه

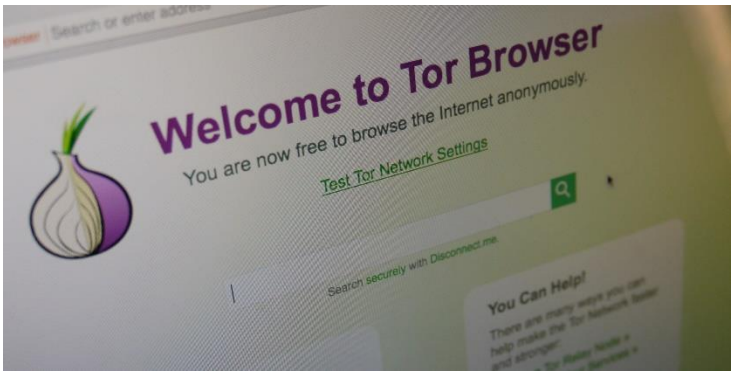
می‌دهد تا تراکم و حرکت حجم زیاد ترافیک را تشخیص دهند و داده‌های کمتری ارسال کنند تا زمانی که ازدحام فروکش کند.

- **مقامات دایرکتوری:** طراحی قبلی Onion Routing برای انتقال وضعیت اطلاعات از طریق شبکه برنامه ریزی شده بود – که می‌تواند رویکردی غیرقابل اعتماد و پیچیده باشد. Tor دیدگاهی ساده نسبت به توزیع این اطلاعات دارد. گره‌های مورد اعتماد بیشتری به‌عنوان مقامات دایرکتوری عمل می‌کنند: آنها برای تولید اسناد دایرکتوری امضاشده که روترهای شناخته شده و وضعیت فعلی آنها را توصیف می‌کنند، همکاری می‌کنند. کاربران به صورت دوره‌ای این اسناد را مستقیماً از مقامات یا یک مشابه از طریق HTTP تنظیم شده روی مدار Tor دانلود می‌کنند.
- **سیاست‌های خروج متغیر:** Tor یک مکانیسم ثابت برای هر گره فراهم می‌کند تا سیاست میزبان‌ها و پورت‌هایی که به آن‌ها متصل می‌شود را توصیف کند. این سیاست‌های خروج در زیرساخت‌های توزیع‌شده مبتنی بر داوطلبان حیاتی هستند، زیرا هر اپراتور به راحتی به انواع مختلف ترافیک اجازه می‌دهد از گره خود خارج شود.
- **بررسی یکپارچگی انتها به انتها:** طرح اصلی Onion Routing هیچگونه بررسی یکپارچگی روی داده‌ها را انجام نمی‌داد. هر گره در مدار می‌تواند محتویات سلول‌های داده را در حین عبور تغییر دهد – برای مثال، تغییر درخواست اتصال به وب سرور که باعث شود به سرور دیگری وصل شود، یا ترافیک رمزگذاری شده را "برچسب" کند و به دنبال ترافیک خراب مربوطه در لبه‌ها شبکه بگردد [۱۳]. Tor با تأیید صحت داده‌ها قبل از اینکه از شبکه خارج شوند، مانع از این حملات می‌شود.
- **مقاومت در برابر سانسور:** تعداد فزاینده‌ای از کاربران Tor نه تنها به ارتباطات ناشناس نیاز دارند، بلکه به مقاومت در برابر سانسور نیز نیاز دارند. Tor تلاش‌هایی را که برای مسدود کردن دسترسی به شبکه انجام می‌شود از طریق یک "پل" که یک گره در Tor است دور می‌زند و به کاربر اجازه دسترسی به شبکه را می‌دهد، که آدرس IP پل در لیست دایرکتوری سرویس Tor وجود ندارد و تعداد کمی از افراد آدرس IP آن را می‌دانند تا احتمال مسدود شدنش کاهش یابد. پروتکل Tor نیز شبیه به HTTPS طراحی شده است به طوری که مسدود کردن Tor، بدون مسدود کردن HTTPS، دشوارتر می‌شود.
- **معماری مدولار:** برنامه Tor فقط بخشی از یک سیستم ارتباطی ناشناس تاثیر گذار است و قابلیت ادغام شدن Tor با سایر اجزاء سازنده سیستم باعث می‌شود طیف گسترده‌ای از نیازهای

کاربر برآورده شود. رابط کاربر گرافیکی یک برنامه جداگانه است (Vidalia، در بسته مرورگر Tor، اما گزینه‌های جایگزین وجود دارد) که از طریق یک سوکت محلی - "پورت کنترل" با Tor ارتباط برقرار می‌کند. محققان برای تجزیه و تحلیل و اصلاح نمونه اولیه تور کنترل کننده-های ویژه‌ای را طراحی کردند. مقاومت بیشتر در برابر پروتکل انگشت نگاری، با هدف مقاومت در برابر سانسور، ممکن است توسط یک مبهم کننده خارجی «یک اتصال قابل حمل و نقل» ارائه شود.

مزایای tor:

- تعداد دنبال کننده و جامعه آماری کاربرانش زیاد است.
- در جوامع هکری محبوبیتزیادی دارد.
- TOR بیشتر توسط جامعه استفاده می‌شود زیرا توسعه دهندگان بیشتری دارد.
- TOR تا حد زیادی با انسداد محتوا و حملات DOS سازگار شده است.
- پهنای باند کم دارد.



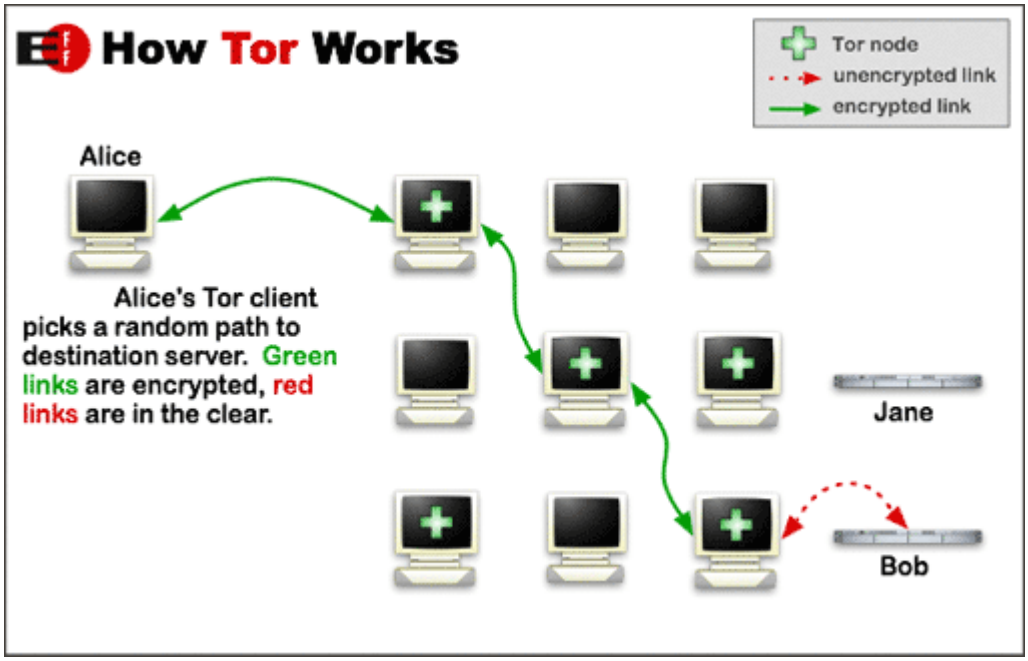
شکل ۴. مرورگر tor

هم‌اکنون «تور» امن‌ترین سامانه ارتباطی جهان و بهترین نرم‌افزار برای ناشناس ماندن در فضای سایبری است. به گونه‌ای تاکنون که هیچ سازمان و نهاد امنیتی قادر به شکستن کدهای آن نبوده‌است.

شکل ۵. شبکه Tor (یا فقط "Tor") اجرای برنامه ای است که در ابتدا توسط نیروی دریایی ایالات متحده در اواسط دهه ۱۹۹۰ توسعه یافت. با رمزگذاری ترافیک اینترنت و عبور آن از یک سری گره، کاربران را قادر می سازد ناشناس ماندن بیشتری به صورت آنلاین داشته باشند.

Tor چیست و چگونه کار می کند؟

شبکه Tor که اغلب به آن فقط "Tor" گفته می‌شود، یک سیستم داوطلبانه است که به ناشناس‌تر کردن استفاده از اینترنت کمک می‌کند. هنگامی که کاربر به Tor (اغلب از طریق مرورگر Tor) متصل می‌شود، ترافیک اینترنتی خروجی او قبل از رسیدن به مقصد (وب سایتی که کاربر می‌خواهد از آن بازدید کند) از طریق یک سری تصادفی حداقل سه گره (به نام رله) تغییر مسیر می‌دهد. کامپیوتر ما به یک گره ورودی متصل است و ترافیک گره نهایی که از آن عبور می‌کند، گره خروجی است و پس از آن به مقصد می‌رسد (وب‌سایتی که می‌خواهید از آن بازدید کنید). ترافیک ورودی به روشی مشابه تغییر مسیر داده می‌شود.



شکل ۶. یک نسخه ساده شده از نحوه کار Tor (منبع: EFF از طریق Wikimedia)

علاوه بر اینکه با عبور از چندین گره، ترافیک در واقع چندین بار رمزگذاری می‌شود. در هر گره سطحی از رمزگذاری را از دست می‌دهد، اما هرگز به طور کامل رمزگشایی نمی‌شود تا زمانی که گره خروجی را به مقصد خود ترک کند. هر گره یک آدرس IP شناسایی دارد که رمزگذاری شده است. تنها آدرس IP قابل مشاهده برای وب سایت مقصد، آدرس آخرین گره است که به عنوان گره خروجی شناخته می‌شود. در مجموع، شبکه Tor در حال حاضر از حدود ۷۰۰۰ رله (گره) و ۸۰۰ پل تشکیل شده است. پل‌ها شبیه رله‌ها هستند، اما در Tor فهرست نشده‌اند. اینها معمولاً توسط هر کسی که قادر به دسترسی به شبکه Tor با وسایل عادی نیست، برای مثال، اگر مسدود شده باشد، استفاده می‌شود. همچنین ممکن است از آنها استفاده شود که یک وب سایت یا برنامه ترافیک را از گره Tor شناسایی شده مسدود می‌کند.

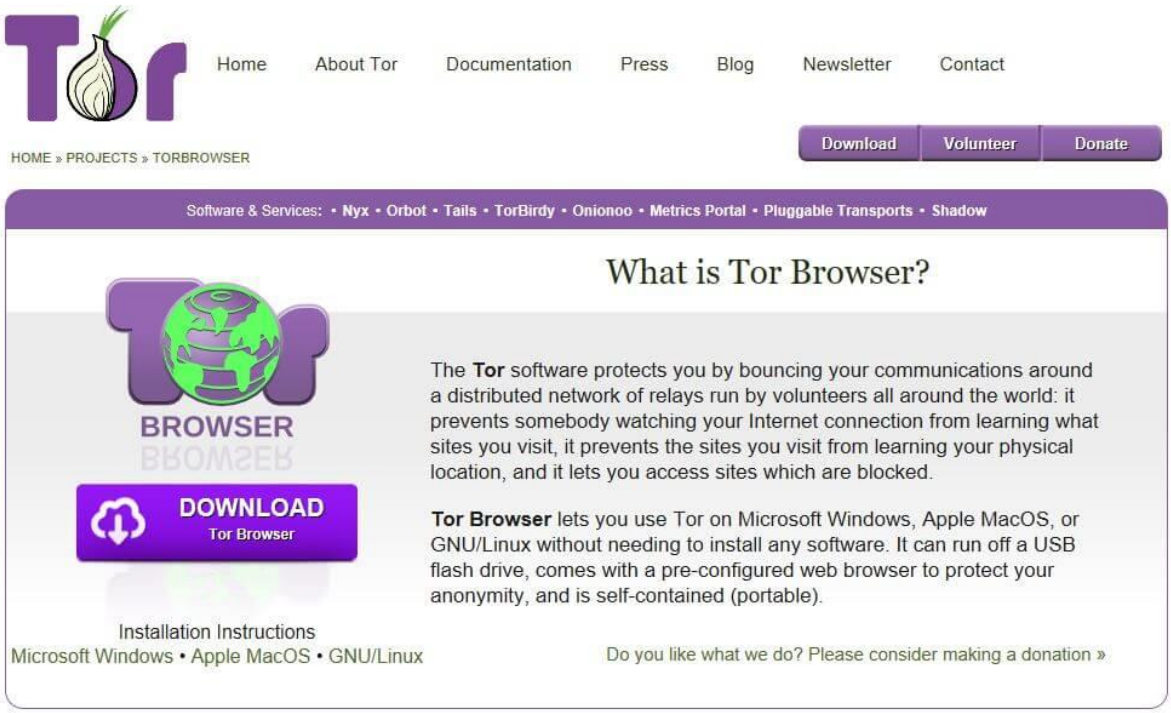
آیا Tor آدرس IP را پنهان می‌کند؟

هنگامی که به شبکه Tor متصل هستید، فعالیت هرگز به آدرس IP ما قابل ردیابی نخواهد بود. به همین ترتیب، ارائه‌دهنده خدمات اینترنتی (ISP) ما نمی‌تواند اطلاعات مربوط به محتوای ترافیک ما، از جمله وب‌سایتی را که بازدید می‌کنیم، مشاهده کند.ISP ما می بیند که به یک گره ورودی Tor متصل هستید و وب سایتی که بازدید می‌کنید به سادگی آدرس IP گره خروج Tor را می‌بینند.

نحوه استفاده از Tor: شروع به کار

ساده‌ترین راه برای استفاده از Tor از طریق مرورگر Tor است. این یک برنامه مبتنی بر فایرفاکس است

که می‌توانید آن را دانلود و بر روی رایانه خود نصب کنید.



شکل ۷. تصویری از وبسایت tor

نسخه‌ها برای MacOS، Windows و Linux در دسترس هستند. پس از دانلود و نصب، می‌توانید از طریق مرورگر به سایت‌های clearnet و .onion دسترسی داشته باشید. در برخی موارد، استفاده از مرورگر Tor ممکن است مسدود شود. همانطور که قبلا ذکر شد، استفاده از پل باید بر این مشکل غلبه کند. در گذشته اینکار نسبتاً پیچیده بود، اما در آخرین نسخه بسیار ساده‌تر است. ابتدا باید یک پل را پیدا کنید و سپس آن را با مرورگر Tor پیکربندی کنید.

آیا Tor واقعاً ما را ناشناس می‌کند؟

ناشناس شدن آنلاین غیرممکن نیست اما کار بسیار دشوار است، ولی Tor مطمئناً می‌تواند به ما کمک کند تا به آن دست پیدا کنیم. با استفاده از تور اینطور به نظر می‌رسد که تمام ترافیک ما که به مقصد می‌رسد از یک گره خروجی تور دارد ارسال می‌شود، بنابراین آدرس آی‌پی آن گره به اطلاعات ارسالی اختصاص داده می‌شود. از آنجایی که ترافیک در حین رمزگذاری از چندین گره اضافی عبور کرده است، نمی‌توان آن را ردیابی کرد. یعنی فقط آدرس IP گره آخر که مربوط به گره خروجی Tor است قابل شناسایی است و کاربر اولیه ناشناس می‌ماند.

با این حال، یکی از مسائل در اعتماد به اپراتور گره خروجی است. اگر از یک وب سایت رمزگذاری نشده (غیر HTTPS) بازدید می‌کنیم، ممکن است اپراتور گره بتواند فعالیت ما را ردیابی کند و اطلاعات ما را

مشاهده کند. آنها می‌توانند داده‌هایی مانند صفحات وبی که مشاهده می‌کنیم، اطلاعات ورود به سیستم، محتوای پیام‌ها یا پست‌ها و جستجوهایی که انجام می‌دهیم را جمع‌آوری کنند. اگرچه، هیچ راهی برای ردیابی آن اطلاعات به ما یا حتی بازگشت به گره ورودی وجود ندارد.

شایان ذکر است که استفاده از مرورگر Tor تنها از ترافیک عبوری از طریق آن اتصال محافظت می‌کند و دیگر برنامه‌ها را روی رایانه ما ناشناس نمی‌کند (اگرچه بسیاری از آنها را می‌توان از طریق روش‌های دیگر در شبکه Tor پیکربندی کرد). همچنین، ISP ما همچنان می‌تواند ببیند که از Tor استفاده می‌کنیم یا نه. و همچنین برای بهبود حریم خصوصی، می‌توانیم از VPN در کنار مرورگر Tor استفاده کنیم.

دارک نت چیست و Tor چگونه با آن ارتباط دارد؟

اگر با اصطلاح «شبکه شفاف» آشنا باشید، می‌دانید به بخشی گفته می‌شود که از اینترنت می‌توان آزادانه به آن دسترسی داشت، یعنی بدون Tor یا روش های دیگر بتوان به آن درسترسی داشت. در طرف دیگر وب عمیق را داریم. این بخش شامل محتوایی می شود که توسط موتورهای جستجو فهرست نشده است، از جمله محتوای قدیمی، فایل های خصوصی، و صفحات وب که موتورهای جستجو را از خزیدن در آنها منع کرده‌اند.

همچنین در وب عمیق، دارک نت وجود دارد. این محتوا معمولاً فقط با استفاده از ابزارهای خاصی مانند Tor قابل دسترسی است. دارک نت برخی از وب سایت های قانونی را در خود جای داده است، اما بیشتر به دلیل مکانی مملو از فعالیت های غیرقانونی شناخته شده است.

ما می توانیم با Tor به شبکه شفاف دسترسی داشته باشیم ، اما همچنین می توانیم به وب سایت های دارک نت، به ویژه سایت های .onion دسترسی داشته باشیم. اینها سایت هایی هستند که فقط افرادی که از مرورگر Tor استفاده می کنند می توانند به آنها دسترسی داشته باشند و .onion را به عنوان بخشی از URL خود دارند. آنها همچنین به عنوان "خدمات پنهان Tor" شناخته می شوند.

آنها توسط موتورهای جستجو ایندکس نمی شوند و اگر ندانید کجا را جستجو کنید پیدا کردن آنها دشوار است. Tor از ناشناس ماندن اپراتورهای سایت‌های onion محافظت می‌کند، بنابراین تشخیص اینکه چه کسی آنها را اجرا می‌کند دشوار است. البته، ترکیبی از ناشناس بودن اپراتور و کاربر چیزی است که دارک نت را برای فعالیت های مجرمانه ایده آل می کند.

شکل ۸ .وب سایت (اکنون توقیف شده) بازار بدنام AlphaBay یک سایت پیاز بود. (منبع: وزارت دادگستری ایالات متحده از طریق ویکی پدیا)

همانطور که گفته شد، بسیاری از وب سایت های قانونی وجود دارند که نسخه های .onion دارند. به عنوان مثال، VPN ها برای کاربران آگاه به حفظ حریم خصوصی طراحی شده اند و برخی از آنها نسخه های پیازی سایت خود را ارائه می دهند که ExpressVPN یک نمونه است. حتی می توانید از طریق مرورگر Tor یک سایت .onion خودتان راه اندازی کنید.

دلایل استفاده از تور

همانطور که گفته شد، Tor اغلب با فعالیت غیرقانونی و کاربرانی که مایل به دسترسی به وب تاریک هستند مرتبط است. به همین دلیل، اغلب این فرض وجود دارد که هرکسی که از Tor استفاده می‌کند باید به هیچ وجه خوب نباشد. برعکس، Tor به سادگی می‌تواند توسط کاربران آگاه به حریم خصوصی برای مرور روزانه در سایت‌های cleannet استفاده شود تا به حفظ ناشناس بودن و حفظ حریم خصوصی کاربران در زمان آنلاین کمک کند.

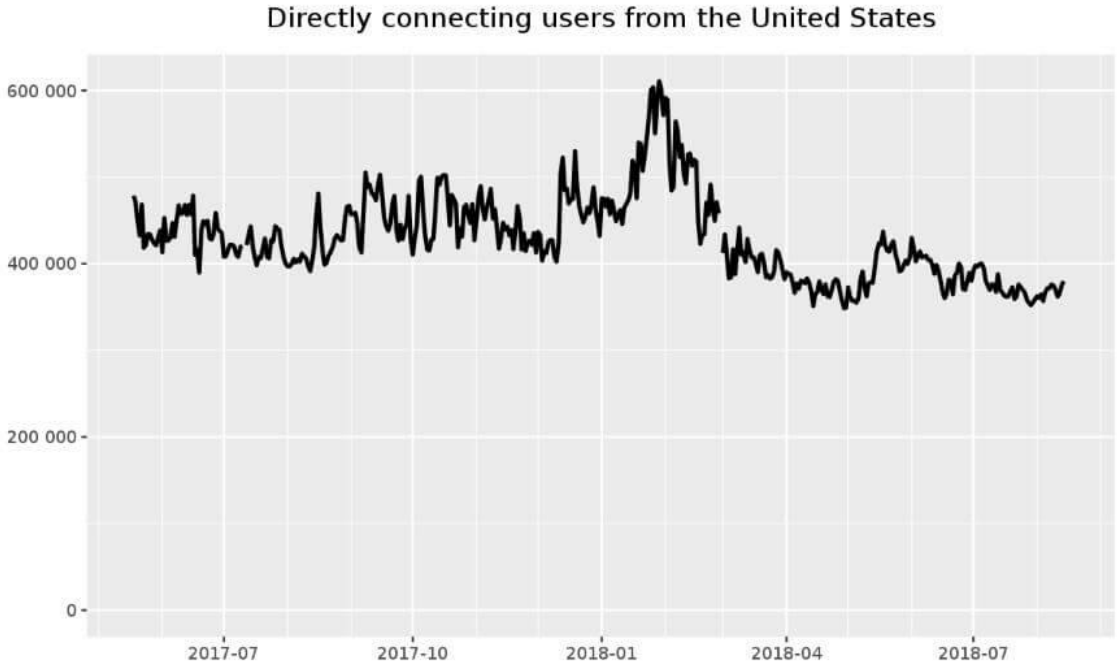
دلایل زیادی وجود دارد که کاربر معمولی اینترنت ممکن است بخواهد ناشناس‌تر باشد. اینها شامل توقف ISPها و اشخاص ثالث در جمع‌آوری داده‌ها در مورد فعالیت آنلاین، دور زدن سانسور، محافظت از حریم خصوصی کودکان، یا تحقیق در مورد موضوعاتی مانند کنترل تولد یا مذهب است.

همچنین بسیاری از مشاغل وجود دارند که در آنها حفظ یک نمایه آنلاین ناشناس ضروری یا مفید

است. برخی از کسانی که به طور قانونی از Tor استفاده می کنند عبارتند از:

- خبرنگاران
- افسران مجری قانون
- فعالین
- افشاگران
- مدیران تجاری
- وبلاگ نویسان
- نظامیان
- متخصصان فناوری اطلاعات

اگرچه Tor کارهایی که کاربران آنلاین انجام می‌دهند را ردیابی نمی‌کند، اما آماری را ارائه می‌دهد که به ما می‌گوید کاربران در کجا قرار دارند. که میتاون نمودارها را بر اساس کشور دید و درباره رویدادهایی که ممکن است به تغییرات شدید در تعداد کاربران کمک کرده‌اند، مطالعه کرد.



شکل ۹. نمودار تعداد کاربران ایالات متحده

به عنوان مثال، نمودار بالا تعداد کاربران ایالات متحده را نشان می دهد که در طول سال گذشته متصل شده اند. در تفسیر تاریخ‌دار زیر هر نمودار، Tor یادداشت‌هایی درباره مواردی مانند به‌روزرسانی‌ها،

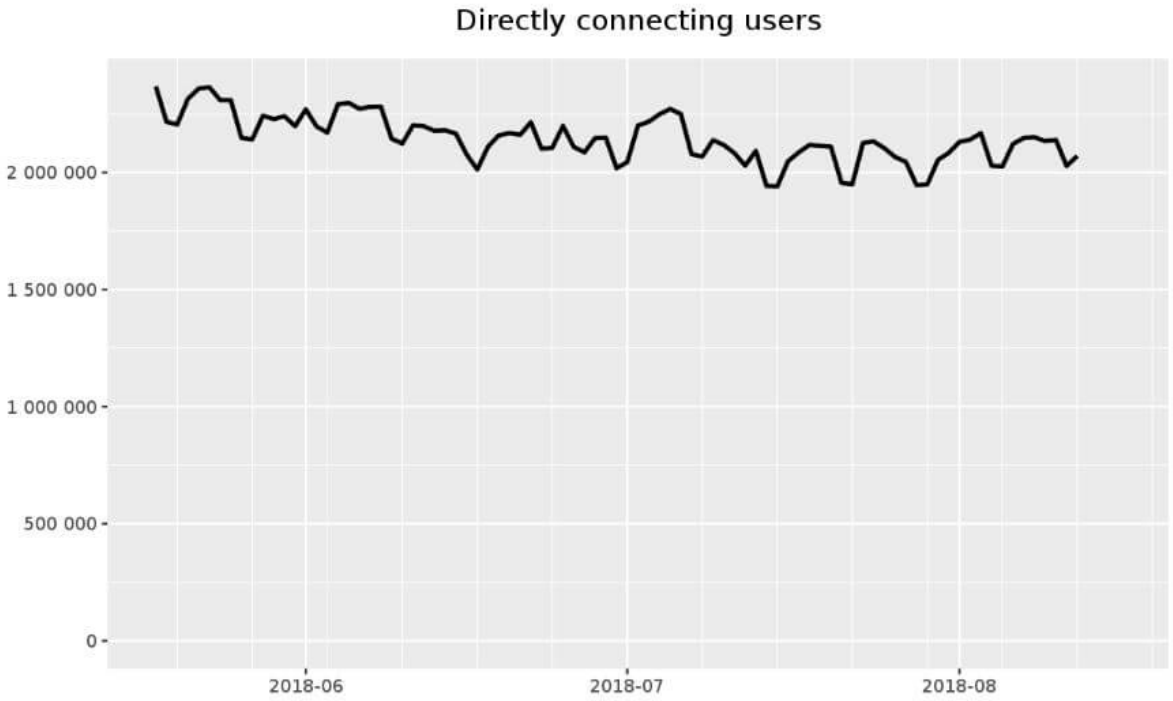
خاموشی‌ها و رویدادهای مهم مانند مسدود شدن دولت ارائه می‌دهد.

آیا استفاده از Tor قانونی است؟

درست است که ماهیت Tor آن را به یک انتخاب محبوب در میان مجرمانی تبدیل می کند که می خواهند به برخی از قسمت های سایه دار دارک نت دسترسی داشته باشند و فعالیت های مجرمانه انجام دهند. این شامل خرید یا فروش محصولات یا خدمات غیرقانونی، یا شرکت در انجمن هایی است که سخنان نفرت پراکنی می کند و افراط گرایی را تشویق می کند.

با این حال، همانطور که در بالا ذکر شد، دلایل زیادی وجود دارد که غیر مجرمان بخواهند از Tor استفاده کنند. در واقع، استفاده از Tor کاملاً قانونی است، اگرچه در برخی کشورها مسدود شده یا در حال حاضر مسدود شدن است. به علاوه، هنوز یک انگ وجود دارد، بنابراین احتمالاً نباید تصور کنید که می توانید بدون دردسر از آن استفاده کنید. گزارش شده است که ISP ها پهنای باند کاربران Tor را کاهش می دهند و حتی با مشتریان تماس گرفته اند تا از مرورگر Tor استفاده نکنند. کاربران ممکن است توسط ISP ها در مورد اینکه به کدام وب سایت ها از طریق Tor متصل می شوند، سؤال شوند. خود مقامات ممکن است به کاربران Tor مشکوک شوند و تنها بر اساس این دلایل در مورد فعالیت های آنها تحقیق کنند. اگرچه، در واقع گزارشی مبنی بر جریمه یا هزینه های مربوط به استفاده از Tor وجود ندارد.

تور در میان بسیاری از کاربران محبوب است، در حال حاضر حدود ۲ میلیون کاربر به صورت همزمان به رله‌های تور متصل می‌شوند.



شکل ۱۰. تعداد کاربران شبکه tor

اما تور هم معایب خود را دارد. در اینجا معایب اصلی استفاده از Tor آمده است:

۱. سرعت کم

۲. قابل تشخیص توسط ISP ها

۳. مسدود سدن توسط مدیران شبکه

۴. آسیب‌پذیر بودن در برابر حملات

هریک از موارد گفته شده رو به صورت دقیق‌تر بررسی می‌کنیم:

سرعت کم

نقطه ضعف اصلی استفاده از Tor کند بودن آن است. ترافیک مستقیماً به مقصد نمی رود، بنابراین سرعت کار را کاهش می دهد. به علاوه، سرعت جریان ترافیک بین گره‌ها می‌تواند کمتر از اتصال معمولی اینترنت ما باشد و سرعت کلی را بیشتر کاهش دهد.

علاوه بر این، تعداد گره‌های داوطلب در دسترس در مقایسه با میزان ترافیکی که در شبکه جریان دارد بسیار کم است. ازدحام ناشی از آن، ترافیک را به خصوص در زمان اوج مصرف کاهش می دهد . با توجه به این مسائل، کاربرد اصلی Tor مرور عمومی است. برای استریم یا تورنت یا هر چیز دیگری که به پهنای باند زیادی نیاز دارد مناسب نیست.

قابل شناسایی توسط ISP ها

نکته منفی دیگر این است که ISP می تواند ببیند که از Tor استفاده می کنید. نمی‌تواند محتویات ترافیک ما را بخواند، اما این واقعیت که تشخیص می‌دهد ما از Tor استفاده می‌کنیم می‌تواند عواقبی داشته باشد. همانطور که قبلا ذکر شد، استفاده از Tor به تنهایی برای ایجاد شک از سوی ISPها و مقامات کافی است. یکی از راه‌های حل این مشکل استفاده از VPN با Tor است

مسدود شدن توسط مدیران شبکه

Tor اغلب توسط مدیران شبکه های خاص مسدود می شود. یکی از راه ها استفاده از پل هایی است که نباید به عنوان گره های Tor قابل شناسایی باشند. اگر انسداد پیچیده‌تر است و از بازرسی عمیق بسته استفاده می‌کند، ممکن است لازم باشد از یک ابزار اضافی مانند Pluggable Transports استفاده کنید. این کار ترافیک Tor ما را به عنوان ترافیک معمولی برای دور زدن بلوک پنهان می کند.

آسیب پذیر بودن در برابر حملات

در حالی که تایید نشده است، گزارش هایی وجود دارد که تجزیه و تحلیل ترافیک در Tor با موفقیت برای یافتن شواهد مجرمانه استفاده شده است. یکی از موارد برجسته، حذف جاده ابریشم در سال ۲۰۱۳ است. جاده ابریشم بازاری بود که از طریق شبکه Tor اداره می شد و در فروش مواد مخدر به ارزش تخمینی ۱ میلیارد دلار، همراه با سایر کالاها و خدمات غیرقانونی شرکت داشت. تئوری های مختلفی در مورد چگونگی شناسایی جنایتکاران دخیل توسط FBI وجود دارد، اما این مورد نشان می دهد که آسیب پذیری هایی در شبکه Tor به عنوان ابزار ناشناس وجود دارد.

آیا Tor روی موبایل کار می کند؟

مرورگر Tor فقط برای سیستم‌عامل‌های Windows، MacOS و Linux در دسترس است که اگر به دنبال اتصال به شبکه Tor از یک دستگاه تلفن همراه هستید، ممکن است ناامید کننده باشد. اما برای کاربر اندروید Orbot، یک برنامه پراکسی رایگان است که ترافیک ما را از طریق شبکه Tor ارسال می کند.

شکل ۱۱. شبکه tor در آندروید

همچنین یک مرورگر اندرویدی به نام Orfox وجود دارد که بر روی فایرفاکس ساخته شده است.

شکل ۱۲. مرورگر شبکه tor در آندروید

اگر کاربر iOS هستید، همه چیز به این سادگی نیست. یک برنامه رایگان و نسبتاً محبوب Onion Browser برای iOS وجود دارد، اما این برنامه به اندازه Orfox ایمن در نظر گرفته نمی شود و تجربه کاربری عالی را ارائه نمی دهد. اتصال دستی به شبکه Tor امکان پذیر است، اما ابتدا باید دستگاه خود را تنظیم کنید.

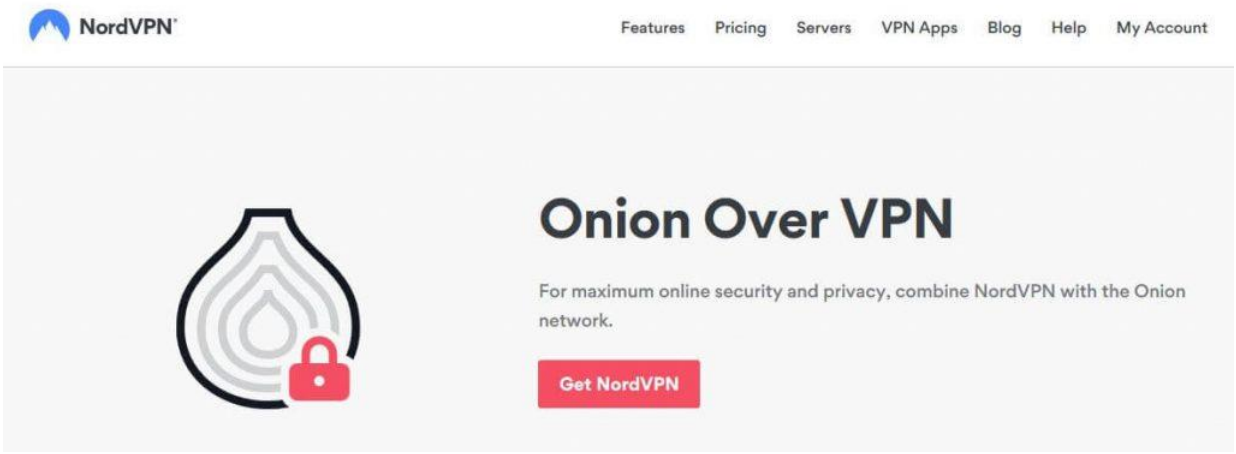
آیا هنگام استفاده از Tor هنوز به VPN نیاز دارم؟

به عبارت ساده تر ، Tor بیشتر در مورد ناشناس بودن است، در حالی که VPN بیشتر به حفظ حریم خصوصی می پردازد. با استفاده از Tor، تمام ترافیک ما رمزگذاری می شود، اما ISP ما همچنان می تواند ببیند که به Tor متصل هستیم. علاوه بر این، گره ورودی Tor می تواند آدرس IP واقعی ما را ببیند. با استفاده از VPN، تمام ترافیک ما رمزگذاری می شود و ISP ما نمی تواند ببیند که از کدام وب سایت ها بازدید می کنیم . فقط می بیند که ترافیک رمزگذاری شده به و از یک سرور VPN می رود. با این حال، ارائه دهنده VPN ما این قابلیت را دارد که ترافیک ما را بخواند، حتی اگر بگوید این کار را نمی کند. بنابراین همیشه مقدار مشخصی از اعتماد وجود دارد که باید در هر ارائه دهنده VPN قرار گیرد، در حالی که Tor "بی اعتماد" است.

در دنیای ایده‌آل، ما نمی‌خواهیم ISP ما ببیند که از Tor استفاده می‌کنیم ، گره‌های ورودی Tor آدرس IP ما را می‌بینند، یا مجبور نباشیم به ارائه‌دهنده VPN خود اعتماد کنیم تا فعالیت ما را مشاهده یا ثبت نکند. استفاده از VPN در کنار Tor می‌تواند این مشکلات را کاهش دهد. دو گزینه برای انجام این کار وجود دارد: Tor از طریق VPN یا VPN از طریق Tor. تفاوت اصلی در این است که ابتدا به کدام یک وصل می‌شوید.

Tor بر روی VPN

با Tor over VPN، ابتدا به VPN متصل می‌شویم، سپس از مرورگر Tor استفاده می‌کنیم. این ساده و موثر است. ترافیک ما قبل از اینکه به گره ورودی Tor برسد از سرور VPN عبور می‌کند. این بدان معنی است که سرور VPN فقط می‌تواند ببیند که ما به Tor متصل هستیم و نمی‌تواند ببیند ترافیک ما به کجا می‌رود. با بازگشت به ISP خود، فقط می‌بیند که به یک سرور VPN متصل هستیم و چیزی فراتر از آن نیست. این بدان معنی است که ISP ما نمی‌تواند ببیند که ما به یک گره ورودی Tor متصل هستیم.



شکل ۱۳. وی پی ان Nord

چندین VPN با رتبه برتر، از جمله NordVPN، دسترسی به شبکه Tor را در سرویس خود ادغام می کنند. ما به یک سرور تخصصی متصل می شویم و تمام ترافیک اینترنت ما از طریق شبکه Tor می رود. با این حال، این احتمالاً باید محدود به استفاده با برنامه هایی غیر از مرورگرهای وب باشد. مرورگرهایی مانند کروم و فایرفاکس آنقدر شناسه دارند که ناشناس ماندن حتی در صورت اتصال به شبکه Tor دشوار است. بنابراین، برای مرور، اتصال به VPN و سپس باز کردن مرورگر Tor احتمالا بهترین گزینه است.

VPN از طریق Tor

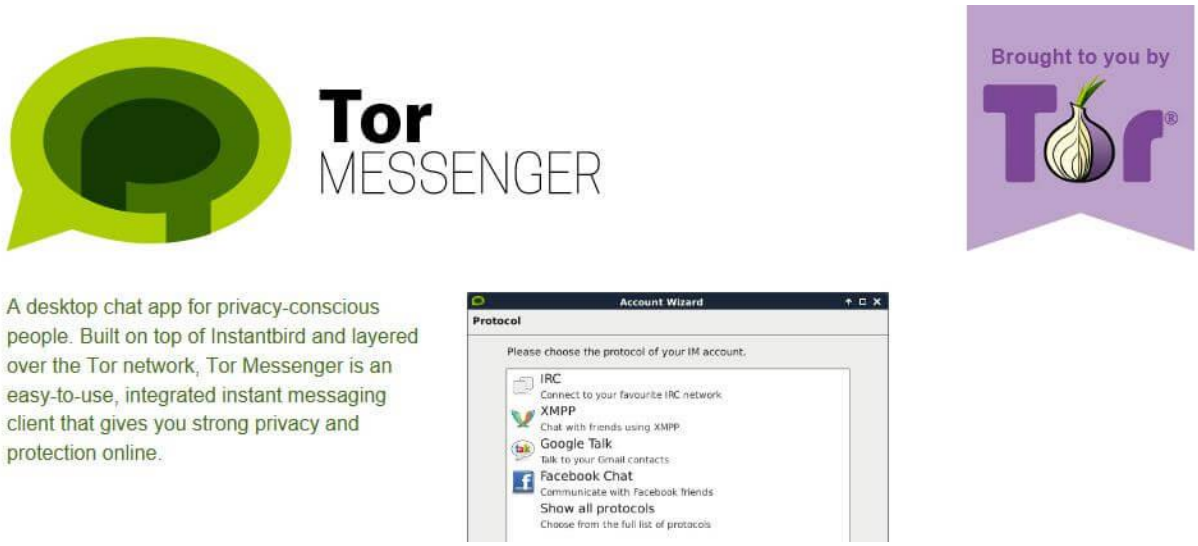
این تنظیم کمی پیچیده تر است و واقعاً ناشناس بودن اضافی را ارائه نمی‌دهد. در این حالت، ابتدا ترافیک از Tor عبور می‌کند. ISP ما همچنان می‌تواند ببیند که به شبکه Tor متصل هستیم ، گره ورودی Tor می‌تواند آدرس IP واقعی را ببیند، و همچنان باید به VPN اعتماد کنیم زیرا می‌تواند ببیند ترافیک به کجا می‌رود.

یکی از مشکلاتی که VPN از طریق Tor برطرف می کند این است که گره خروج Tor نمی تواند ببیند از کدام سایت بازدید می کنیم . در عوض، به سادگی می بیند که ما در حال اتصال به یک سرور VPN هستیم . یک نقطه ضعف این است که اطلاعات ورودی VPN ما توسط اپراتور گره خروج Tor قابل مشاهده است. یکی دیگر از مزایای این راه اندازی این است که وب سایت هایی که معمولاً ترافیک Tor را مسدود می کنند از حالت انسداد خارج می شوند.

سیستم پیام رسان تور چیست؟

یکی از پروژه های مرتبط با تور که ممکن است با آن آشنا باشید، پیام‌رسان تور است. این نرم افزار منبع باز برای استفاده در کنار شبکه‌های موجود مانند فیس بوک، توییتر و گوگل تاک طراحی شده است.

تمام ترافیک Tor Messenger از طریق Tor ارسال می‌شود و از چت Off-The-Record برای اعمال مکالمات رمزگذاری شده بین کاربران استفاده می‌شود.



شکل ۱۴. پیام رسان tor

Tor Messenger مبتنی بر Instabird است و رابط کاربری مشابهی دارد. اگرچه یکی از مشکلات اصلی Tor Messenger به این دلیل است که Instabird دیگر در حال توسعه نیست. این موضوع در کنار مسائل دیگر، از جمله نشت ابرداده و منابع محدود، منجر به توقف توسعه پروژه پیام‌رسان Tor شده است.

پروژه‌های مرتبط با Tor

شبکه Tor فقط مرورگر Tor نیست. پروژه های مختلف دیگری برای تکمیل شبکه توسعه یافته است. قبلاً به سایت‌های .onion، سیستم پیام‌رسانی فوری Tor و چند پروژه اندروید اشاره کردیم ، اما در اینجا برخی از پروژه‌های دیگری وجود دارد که ممکن است با آنها برخورد کنید:

• Atlas: این یک برنامه وب است که جزئیات مربوط به رله ها و پل های مختلف در شبکه Tor را به ما نشان می دهد. می‌توانید جستجوها را انجام دهید و اطلاعاتی مانند پهنای باند، سیاست‌های خروج و زمان کار را پیدا کنید.

• Nyx: که قبلاً Arm نامیده می شد، Nyx یک مانیتور خط فرمان برای کاربرانی است که رله ها را در شبکه Tor اجرا می کنند. این اطلاعات را در قالبی آسان برای مشاهده، مانند استفاده از پهنای باند و گزارش های اتصال ارائه می دهد.

• Onionoo: این یک پروتکل مبتنی بر وب است که داده های مربوط به رله ها و پل ها را در شبکه Tor ارائه می دهد. برخلاف اطلس، برای ارائه مستقیم داده ها به انسان طراحی نشده است، بلکه برای

ارائه اطلاعات به برنامه های کاربردی دیگر (مانند اطلس) و وب سایت ها طراحی شده است.

• OONI: رصدخانه باز تداخل شبکه (OONI) تست‌های نرم‌افزاری رایگان، از جمله آزمایش‌هایی برای شناسایی مسدود شدن وب‌سایت‌ها و برنامه‌های پیام‌رسانی فوری ارائه می‌دهد. همچنین می توانید مسدود شدن ابزارهای مورد استفاده برای دور زدن بلوک ها مانند Tor را شناسایی کنید.

• Pluggable Transports: Pluggable Transports (PTs) باعث می شود که ترافیک Tor بین مشتری و پل مانند ترافیک معمولی به نظر برسد. این برای دور زدن سانسورهایی که از بازرسی بسته عمیق برای تشخیص جریان ترافیک Tor استفاده می کنند مفید است.

• Shadow: این یک نرم افزار متن باز است که شبیه سازی Tor را برای اهداف آزمایشی در اختیار کاربران قرار می دهد.

• Tails: Amnesic Incognito Live System (Tails) یک سیستم عامل زنده است که می تواند از طریق DVD یا USB روی رایانه ما راه اندازی شود. این بر روی دبیان ساخته شده است و ترافیک را از طریق Tor ارسال می کند.

• TorBirdy: این به طور خاص برای استفاده با برنامه ایمیل Mozilla Thunderbird طراحی شده است. TorBirdy حریم خصوصی Thunderbird را بهبود می بخشد و آن را برای استفاده با Tor پیکربندی می کند.

• Tor2web: Tor2web به کاربران کمک می کند تا بدون استفاده از مرورگر Tor به خدمات Tor Onion دسترسی داشته باشند. با این حال، به ما ناشناس ماندن را نمی‌دهد، فقط اجازه دسترسی به سایت‌های onion. را می دهد.

فصل سوم

فصل چهارم

فصل پنجم