فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
فصلنامهٔ علمی ـ ترویجی
سال دوازدهم، شمارهٔ چهل‌وسوم، تابستان ۱۳۹۶

تاریخ دریافت: ۱۳۹۶/۰۳/۱۰
تاریخ پذیرش: ۱۳۹۶/۰۶/۱۴

تهدیدهای پیش‌روی حفاظت اطلاعات‌ها در رابطه با وب عمیق شبکه‌های پیازی

حسن نجفی[۱]

از صفحهٔ ۵۱ تا صفحهٔ ۸۸

چکیده

زمینه و هدف: امروزه زیرساخت‌های حیاتی در زمینه‌های مختلف، وابستگی زیادی به اینترنت پیدا کرده و مزیت‌های زیادی نصیب بشر گردیده؛ اما آسیب‌پذیری‌ها، تهدیدها و مشکلات جدید و خطرناکی ایجاد نموده است. بُعدی از اینترنت دیدنی نیست و برای دیده نشدن برنامه‌ریزی شده است؛ و با کمال تعجب خواهید دید که این بُعد، شامل بیش از ۹۵ درصد اطلاعات موجود بر روی اینترنت می‌شود که برای شما قابل دسترسی نیست. وب عمیق[۲] یکی از کامل‌ترین مراجع اطلاعاتی محسوب می‌شود که البته این اطلاعات توسط افراد غیر قابل شناسایی نگهداری می‌شوند؛ تارشگرها و رخنه‌گرها بخشی از این افراد را تشکیل می‌دهند. **هدف:** این پژوهش با هدف شناسایی تهدیدهای پیش‌روی حفاظت اطلاعات‌ها در رابطه با «وب عمیق» و «شبکه‌های پیازی» انجام شده است.

روش‌شناسی: این تحقیق از لحاظ هدف کاربردی و از حیث ابزار گردآوری به‌صورت اسنادی و کتابخانه‌ای و روش توصیفی؛ همچنین با بهره‌گیری از تجارب عملی محقق تدوین شده است.

یافته‌ها و نتیجه‌گیری: یافته‌های تحقیق حاکی از آن است که موتورهای جست‌وجو مانند گوگل[۳] و بینگ[۴] تنها حدود ۵درصد از محتوای اینترنت را پوشش می‌دهند و ۹۵ درصد مابقی فضای وب، مانند کوه یخی در زیر آب، مربوط به بخش‌های «وب عمیق» و «وب تاریک» است؛ یعنی جایی که کمتر کسی توانایی و حق دسترسی به آن را دارد. بخش عمده‌ای از فعالیت‌هایی که در فضای مجازی صورت می‌پذیرد، قابل شناسایی نیست و هیچ سازمان یا موتور جست‌وجویی توانایی ردیابی این فعالیت‌ها را ندارد؛ به همین دلیل از این بخش وب، بیشتر برای انجام کارهای غیرقانونی نظیر: خرید و فروش مواد مخدر، سلاح، قتل و... استفاده می‌شود؛ بنابراین، با شناسایی دنیای نادیده اینترنت می‌توان نسبت به بهبود انجام مأموریت حفاظت اطلاعات‌ها اقدام کرد.

کلید واژه‌ها: آسیب، امنیت اطلاعات، تهدید، فضای مجازی، موتورهای جست‌وجو، وب تاریک، وب عمیق.

---

۱. دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات (رایانامه: H61.najafi@chmail.ir).

2. Dark Web.
3 .Google.
4 .Bing.

مقدمه

امروزه اطلاعات به‌منزلهٔ خونی است که باید در رگ‌های جامعه متناسب با هر بخش جریان داشته باشد و حفظ سلامت آن برای در امان ماندن از هرگونه آلودگی از ضرورت‌ها است؛ اما به موازات آن، باید بسترهای جابه‌جایی اطلاعات که همان ارتباطات است هم امن شود. بدیهی است در این مرحله، با توجه به اولویت بسترهای ارتباطی، باید میزان امنیت تأمین گردد و تأمین امنیت رگ اصلی که اطلاعات را به حوزهٔ فرماندهی کل می‌رساند، از اهم موارد است.

محافظت و تأمین امنیت اطلاعات که امروزه بر مرکب سریع و پیچیدهٔ فنّاوری اطلاعات سوار است، چگونه باید انجام شود؟ اختیار این مرکب تا چه اندازه با ماست؟ چه کسی تضمین می‌کند که در این خونِ گرفته شده از حوزهٔ فعالیت دشمن، سلول‌های خاموش سرطانی نباشد تا به اشارهٔ آنها فعال شوند و وجود ما را نابود کنند؟

آیا تهدید اصلی ما رخنه‌گرها یا کرَکرها هستند؟ آیا مشکل ما مقابله با ویروس‌ها، کرم‌ها، تروجان‌ها و... است؟

اسب تروای واقعی در کجا سنگر گرفته و در کدام نرم‌افزار در کمین نشسته است؛ به‌طور حتم آنجایی که عوامل حریف سعی در القای امنیت صددرصد آن دارند، آن محل امن کجاست؟ آیا غیر از سیستم عامل است؟

این فنّاوری اطلاعات که بر شاهرگ حیاتی جریان اطلاعات خیمه زده و پنجه‌های نافذ خود را در تمامی ارکان سامانه‌های فرماندهی و واپایش اعم از نرم‌افزارها، سخت‌افزارها، بسترهای ارتباطی و... فرو برده، تا چه اندازه تابع تصمیم‌گیری‌های ماست و چقدر تأثیرپذیر است؟ چه کسی تضمین می‌کند که تجهیزات الکترونیکی و رایانه‌های مجهز به اجزای هوشمند قابل برنامه‌ریزی به‌محض به‌کارگیری، اطلاعات مربوط به موقعیت مکانی ما را به نزدیک‌ترین پایگاه دشمن اطلاع ندهند؟

همهٔ اطلاعات ما را می‌برند و عدم توجه به این مهم یا ناشی از خواب‌آلودگی است! ویا اینکه خود را به خواب زده‌ایم! این روشنایی ضعیفی که از دور به‌نظر می‌رسد، از چشمان گربه‌ای بی‌آزار ساطع نمی‌شود؛ بلکه گرگی است که وقتی نزدیک شود با دندان‌های

تیزش حیات ما را مورد تهدید قرار می‌دهد و مسئولیت آشکارسازی و افشاگری میزان تهدید برعهدهٔ اصحاب فن است که باید شب و روز در فکر مقابله باشند و اقدام لازم را به‌عمل آورند (نجفی، ۱۳۹۲: ۱).

افزایش روزافزون منابع اطلاعاتی و نیاز شدید افراد در دسترسی به این اطلاعات در سراسر دنیا از یک‌سو و در دنیای شگفت‌انگیز ارتباطات رایانه‌ای از سوی دیگر، موجب پیدایش شبکهٔ جهانی اینترنت در اواخر دههٔ ۱۹۶۰ گردید (اردلان،۱۳۸۲: ۵) ولی تا سال ۱۹۹۰ هیچ‌گونه ابزاری برای کاوش اطلاعات موجود در آن وجود نداشت. در سال ۱۹۹۰ شبکهٔ جهانی وب در «آزمایشگاه فیزیک ذره‌ای اروپا»[1] واقع در سوئیس توسط «تیم برنرزلی» ابداع شد. پس از ابداع شبکهٔ جهانی وب، ابزارها و موتورهای کاوش نیز پا به عرصهٔ ظهور نهادند. در سال ۱۹۹۰ «آلان امتیج» در دانشگاه «مک گیل» نخستین ابزار کاوش را با عنوان «آرکی» ابداع کرد (اردلان، ۱۳۸۲:۲۰). «آرکی» از طریق نمایه‌سازی فایل‌های موجود در وب‌گاه‌های اف‌تی‌پی (پروتکل انتقال فایل) امکان جست‌وجو و بازیابی فایل‌ها در محیط اینترنت را فراهم ساخت. برای سهولت جست‌وجو و دسترسی به اطلاعات در اینترنت، امکاناتی به نام موتورهای کاوش ابداع شدند اما با وجود پیشرفت‌ها و تحولات در حوزهٔ ذخیرهٔ اطلاعات در اینترنت که یکی از امتیازهای بارز این پدیدهٔ جدید است، باید یادآور شد که ذخیرهٔ اطلاعات به‌تنهایی کافی نیست و به‌طور قطع اطلاعات تولید شده، زمانی ارزش واقعی می‌یابد که مورد استفاده قرار گیرد. مشکلات موجود در زمینهٔ جست‌وجو و بازیابی اطلاعات در اینترنت، سبب شده است که حجم زیادی از اطلاعات ذخیره شده در آن، قابل دسترس نباشد (Sherman and price,۱۹۹۹). به موازات گسترش ابزارهای کاوش، پژوهش دربارهٔ جنبه‌های مختلف این موتور نیز شروع شد. بیشترین مباحث مطرح شده، موضوع دامنهٔ جست‌وجو و میزان سودمندی و کارایی موتورهای کاوش بود که در این‌باره بحث‌های زیادی نیز صورت گرفته است؛ اما از موضوع‌هایی که کمتر به آن توجه شده، موضوع وب نامرئی است. از آنجا که بین وب

1. European Particle Laboratory.

نامرئی و موتورهای کاوش در اینترنت ارتباط تنگاتنگی وجود دارد، لازم است نخست به‌صورت مختصر به سازوکار موتورهای کاوش اشاره شود.

به‌طور نسبی همهٔ ابزارهای کاوش، خود را بهترین، کارامدترین و قدرتمندترین وسیله برای جست‌وجو و بازیابی اطلاعات در محیط وب معرفی می‌کنند؛ اما تحقیقات نشان می‌دهد که بهترین موتورهای جست‌وجو فقط ۱۶درصد از اطلاعات موجود بر روی وب را به کاربران عرضه می‌کنند (منصوریان، ۱۳۸۲). دلیل‌های متعددی در این زمینه وجود دارند که بخشی از این مشکلات و دشواری‌ها به حجم عظیم و روزافزون اطلاعات موجود در اینترنت مربوط می‌شود. بخش دیگر به میزان مهارت‌های اطلاع‌یابی کاربران و تجربهٔ آنان در کاوش برمی‌گردد و بخش دیگری نیز به‌دلیل وجود وب نامرئی یا وب پنهان است که موتورهای کاوش، به ادله‌ای که در این مقاله شرح داده خواهد شد قادر به انجام عمل بازیابی در آن نیستند. همان‌طور که گفته شد گوشه‌های رازآلود اینترنت را به‌عنوان «وب پنهان» می‌شناسند و تحقیقات نشان می‌دهد که اکثر به اتفاق ترافیک رد و بدل شده در این بخش، مربوط به سوءاستفاده‌های جنسی از کودکان، خرید و فروش مواد مخدر، قتل و... است.

بیان مسئله: چرا انسان‌ها برای نگهداری از دارایی‌های با ارزش خود از هیچ کوششی فروگذاری نمی‌کنند؟ آیا می‌توان کسی را برای مراقبت از اشیای گران‌بها سرزنش نمود؟ چرا الماس‌ها، طلا و جواهرات را در مکان‌های مطمئن قرار می‌دهیم و از آنها محافظت می‌کنیم؟ آیا آنهایی را که از حریم و ناموس خود دفاع می‌کنند می‌توان محکوم کرد؟ آیا جوانمردان و شیرزنانی که در دفاع از ارزش‌ها، استقلال، آزادی و... جان خود را نثار می‌کنند در نظر جامعه محترم و جایگاه والایی ندارند؟

برای پاسخ دادن به موارد بالا و موارد مشابه هیچ‌کس منتظر استدلال نیست؛ چون همهٔ اینها از امور بدیهی است. مقولهٔ امنیت ملی چگونه است و محافظت از آن چه؟ همان‌طور که بقای آحاد موجودات به‌ویژه انسان‌ها، به هوایی است که درآن اکسیژن باشد، استمرار حیات ملت‌ها نیز وابسته به جامعه‌ای است که در آن امنیت باشد. تأمین و حفظ امنیت باید

فراگیر باشد و در تمامی حوزه‌های فعالیت انسان جاری گردد. به‌یقین پاره شدن یک رگ هر موجود زنده در صورت ترمیم نشدن، منجر به مرگ او خواهد شد؛ حال اگر رگ اصلی که خون را به مغز موجود زنده می‌رساند، بریده شود اگر در زمان کوتاهی امکان مداوا و مرمت وجود نداشته باشد، به‌طور حتم حیات فرد خاتمه می‌یابد. پس محافظت از شریان‌های حیاتی در اولویت است و برای حفظ امنیت باید اهم را بر مهم ترجیح داد. با توجه به رشد روزافزون استفاده از شبکه‌های پیازی برای هدف‌های مجرمانه، بایستی کارکنان در این زمینه توجیه شوند و راه‌های شناسایی فعالیت‌های مجرمانه در این فضا را کسب و نسبت به ناامن نمودن فضای مزبور برای مجرمان اقدام کنند.

اهمیت و ضرورت تحقیق: با توجه به اینکه متأسفانه به‌دلیل نداشتن آگاهی و ضعف اشراف در حوزهٔ فضای مجازی، برخی از کارکنان و خانواده‌های آنان به دام شبکه‌های اطلاعاتی و یا مفاسد اخلاقی گرفتار می‌شوند، ضرورت دارد حفاظت اطلاعات‌ها ضمن شناخت تهدیدها و آسیب‌پذیری‌های فضای موصوف، نسبت به آگاه‌سازی کارکنان به‌منظور پیشگیری از تخلف‌های احتمالی و یا جلوگیری از نفوذ شبکه‌های اطلاعاتی اقدام نمایند و همچنین قادر به رصد وب عمیق و شبکه‌های پیازی باشند تا بتوانند آسیب‌پذیری‌های موصوف را احصا کنند.

هدف‌های تحقیق

هدف اصلی: شناسایی تهدیدهای پیش‌روی حفاها در حوزهٔ وب عمیق و شبکه‌های پیازی.

هدف‌های فرعی

- بررسی وب عمیق و راه‌های شناسایی شبکه‌های پیازی؛
- بررسی تأثیرهای وب عمیق بر فعالیت‌های مجرمان.

سؤال‌های تحقیق

سؤال اصلی: تهدیدهای پیش‌روی حفاها در حوزهٔ وب عمیق و شبکه‌های پیازی کدامند؟

سؤال‌های فرعی

- راه‌های شناسایی وب عمیق یا شبکه‌های پیازی چیست؟

- آشنایی با وب عمیق یا شبکه‌های پیازی تا چه اندازه می‌تواند از آسیب‌ها و تهدیدهای کارکنان در بستر موصوف جلوگیری نماید؟
- نقش وب عمیق یا شبکه‌های پیازی در انجام کارهای غیرقانونی مانند: خرید و فروش مواد مخدر، قاچاق سلاح گرم، قتل و... چیست؟

روش تحقیق: روش گردآوری داده‌ها در این تحقیق به‌صورت بررسی میدانی و کتابخانه‌ای (مطالعه کتاب‌ها، مقاله‌های مرتبط و مستندات قانونی و اینترنت با رعایت اصل امانتداری) است. این تحقیق از نظر نوع «کاربردی» است.

پیشینهٔ تحقیق: تاکنون تحقیقات زیادی در حوزهٔ وب عمیق یا شبکه‌های پیازی صورت نگرفته است و منابع مطالعاتی به زبان فارسی پیرامون موضوع فوق موجود نیست و اکثر منابع موجود به زبان لاتین است و ضرورت دارد در این‌باره تحقیقات بیشتری انجام شود.

تعریف‌ها و اصطلاحات

سخت‌افزار[1]: به مجموعه ابزار و اجزای فیزیکی و مدارهای الکترونیکی رایانه اطلاق می‌شود.

نرم‌افزار[2]: به برنامه‌هایی که برنامه‌نویس به‌منظور بهره‌گیری از سخت‌افزار رایانه می‌نویسد می‌گویند؛ در واقع نرم‌افزار، پل ارتباطی بین کاربر و سخت‌افزار رایانه است.

تهدید[3]: از نظر لغوی، به‌معنای ترساندن، رعب و وحشت یا بیم و عقوبت دادن است (فرهنگ عمید). از نظر اصطلاحی، امری است که از سوی دشمنان داخلی و خارجی به‌منظور براندازی نظام مطرح می‌شود. از دیدگاه سازمانی نیز به‌معنای مجموعه خطرهای بالقوه برون سازمانی است که امنیت سازمان و کارکنان آن را به مخاطره می‌اندازد.

از نظر لغوی، ترسانیدن، بیم دادن (فرهنگ دهخدا) و از نظر اصطلاحی به مجموع خطرهای بالقوه و برون سازمانی که امنیت سازمان و کارکنان را به مخاطره می‌اندازد، اطلاق می‌شود. به عبارت دیگر، هرگونه فعل، حادثه، وضعیت و حالتی است که بالقوه موجب ایجاد اختلال، نابودی یا دسترسی غیرمجاز به موضوع‌های حفاظتی شود (پورمراد: ۵۷۱).

---

1. Hardware.
2 .Software.
3 .Threat.

خطر: هرگونه بستر و شرایطی که بالفعل موجب نقض حفاظت شود و در نهایت منجر به بروز شکست حفاظتی (نابودی، اختلال و دسترسی یا تصاحب غیرمجاز) گردد (تعریف‌ها و اصطلاحات آیین‌نامهٔ جامع امنیت فاوا ن.م مصوب ستاد کل ن.م). تهدید بالفعل را خطر گویند.

آسیب: از نظر لغوی به‌معنی آزار، گزند، رنج، زیان، خسارت، عیب و نقص، صدمه و زخم است. در فرهنگ دهخدا، آسیب به‌معنای زخم، کوب، صدمه، عیب و نقص آمده است.

از نظر اصطلاحی، به آثار و پیامدهای ناشی از تهدیدها و خطرهای مترتب بر موضوع‌های حفاظتی آسیب گویند.

آسیب‌پذیری امنیتی: آسیب‌پذیری امنیتی یکی از ارکان اصلی امنیت ملی است. «جان کالینز» آسیب‌پذیری را میزان حساسیت یک ملت یا یک نیروی نظامی به‌گونه‌ای که بتوان با به‌کارگیری توان و ابزار نظامی و غیره از توان و کارایی آن ملت و نیروی نظامی کاست، تعریف کرده است (منصوری، ۱۳۸۷: ۷۲).

نفوذگران: یکی از مهم‌ترین تهدیدهای اینترنت، نفوذگران هستند. نفوذگران همواره درصدد استفاده از نقاط ضعف و آسیب‌پذیر موجود در نرم‌افزارها هستند. با اینکه در برخی از حالت‌ها ممکن است هدف‌های آنها غیرمخرب و با انگیزه‌ای صرفاً کنجکاوانه باشد اما حاصل عملیات می‌تواند آثار جانبی منفی بر جای بگذارد. تا چندی پیش برنامه‌نویسان برنامه‌های کوچکی می‌نوشتند که شوخی‌های بی‌ضرر، دسترسی‌های بی‌اجازه و برگرفته از احساس بود؛ اما اکنون تبدیل به زیان‌های جدی شده است. به هرحال برخی وقت‌ها، نفوذگرها برای سازمان‌ها مفید هستند و به‌عنوان محافظ عمل می‌کنند. بنا به تعریف، آنها افراد یا گروه‌هایی از افراد با انگیزه‌های متفاوت هستند که امنیت سامانه‌های رایانه‌ای یک سازمان یا یک فرد را به‌خطر می‌اندازند (گروه امداد امنیت رایانهٔ ایران) [1].

شنود[2]: هرگاه در اینترنت به یک اتاق گفت‌وگو وارد می‌شوید و مخاطب خود را انتخاب می‌کنید با فعال‌سازی میکروفن، بلندگو و دوربین به مشاهدهٔ یکدیگر و گفت‌وگو

1. http://www.ircert.com.
2. Sniff.

می‌پردازید؛ در این حالت احتمال دسترسی غیرمجاز نفوذگران به صوت و تصویر شما وجود دارد. اما قصه به همین‌جا پایان نمی‌یابد، اگر رایانهٔ شما دارای میکروفن، بلندگو و دوربین باشد، به‌احتمال زیاد، نفوذگران منتظر شما نخواهند ماند که آنها را فعال کنید و به ایشان مجوز شنود و مشاهدهٔ محل استقرار خود را بدهید، بلکه پنهانی و بدون مجوز نسبت به فعال‌سازی سامانه‌های شما اقدام و از آن بهره‌برداری می‌کنند؛ بنابراین هرگاه شما رایانهٔ خود را روشن می‌کنید امکان شنود محیطی را نیز برای نفوذگران فراهم می‌سازید[1].

علاوه بر آن، در مواردی که شما دارای اطلاعات ارزشمندی هستید یا از پایگاه اجتماعی والایی برخوردارید، امکان تجهیز رایانهٔ شما به ابزارهای جاسوسی وجود دارد. به‌عنوان مثال: نصب میکروفن و دوربین‌های مخفی در رایانهٔ شما[2]، در این‌حالت سخت‌افزارهای جاسوسی از قبل بر روی رایانهٔ شما به‌طور ماهرانه نصب شده و کافی است به اینترنت متصل شوید تا نفوذگر علاوه بر سرقت اطلاعات موجود در رایانهٔ شما، نسبت به سرقت صدا و محل استقرارتان نیز اقدام کند؛ هر چند برخی از کارشناسان خوش‌باور این اقدام‌ها را بعید می‌دانند ولی هیچ‌گاه نباید در این قضیه به استقبال خطر رفت.

مهاجم[3]: به کاربر یا به‌طور کلی بازیگران در سامانه گفته می‌شود که برای رسیدن به مقاصد خود از آسیب‌پذیری‌های موجود بهره‌برداری می‌کنند.

حمله[4]**:** یک حمله مجموعه‌ای از اقدام‌های از پیش تعریف شده است که چنانچه با موفقیت انجام شود می‌تواند منجر به تخریب دارایی‌ها و یا انجام عملیاتی نامطلوب گردد.

وب نامرئی[5]**:** با بررسی فرهنگ‌ها و دایره‌المعارف‌ها، هیچ‌گونه تعریفی برای این اصطلاح یافت نشد (sherman and price,۱۹۹۹). مرور نوشتارها حاکی از آن است که به احتمال قریب به یقین «ژیل السورث»[6] در سال ۱۹۹۴ نخستین بار عبارت «وب نامرئی» را ابداع

---

۱. درحالتی که رایانه شما مجهز به میکروفن و دوربین است.

۲. مستنداتی وجود دارد که برخی از سازمان‌های اطلاعاتی، حتی لوازم خانگی سوژه‌های خود را با این ابزارها تجهیز کرده‌اند.

3. Attacker.
4. Attack.
5. Invisible web.
6. Jill Ellsworth.

کرده است. البته معدودی از منابع نیز شخص دیگری به نام «متیوکل»[1] را مبدع این اصطلاح معرفی می‌کنند (منصوریان، ۱۳۸۲).

وب عمیق[2]: بخش دیگری از وب نامرئی، به مجموعه‌ای از اطلاعات الکترونیکی پیوسته اطلاق می‌شود که بسیاری از پایگاه‌های اطلاع‌رسانی، آنها را از طریق شبکهٔ جهان گستر وب در دسترس عموم قرار داده‌اند. برخی این اطلاعات را به رایگان و برخی دیگر، با دریافت هزینه در دسترس عموم قرار می‌دهند. مندرجات این پایگاه‌ها معمولاً خارج از حوزهٔ جست‌وجوی موتورهای کاوش قرار دارند؛ هریک از این پایگاه‌ها صفحهٔ جست‌وجوی مبتنی بر وب دارند که امکان جست‌وجو در آنها را برای کاربران فراهم می‌کند اما خزنده‌های موتورهای جست‌وجو توان ورود به آنها را ندارند و در نتیجه حجم انبوهی از اطلاعات، نمایه نشده باقی می‌ماند. به‌عنوان نمونه اگر یک متخصص موضوعی (مثل یک دانشجوی رشته پزشکی) بخواهد خود را به موتورهای کاوش معمولی محدود کند و نتواند به پایگاه‌های اطلاعاتی تخصصی مراجعه نماید یا از وجود آنها آگاه نباشد، از دسترسی به حجم انبوهی از اطلاعات محروم خواهد ماند؛ بنابراین، کاربر باید در این موارد از طریق موتورهای جست‌وجو، پایگاه‌های مرتبط با موضوع خود را شناسایی کند و سپس جداگانه به جست‌وجو در آنها بپردازد تا از دسترسی به وب عمیق باز نماند.

اینترنت پنهان[3]: بخش دیگری از وب پنهان وجود دارد که بنا به مسائل فنی و ناکارامدی ابزارهای جست‌وجو، از دسترسی کاربران دورمانده است. بسیاری از موتورهای جست‌وجو، قادر به بازیابی اطلاعات متنی «Html» هستند ولی توانایی بازیابی فایل‌های «Pdf» را ندارند یا به‌دلیل کمبود منابع مالی و فنی از جست‌وجوی فایل‌های غیرمتنی صرف‌نظر کرده‌اند؛ بنابراین منابع اطلاعاتی متنوعی نیز در وب وجود دارند که تنها به دلیل محدودیت‌های فنّاورانه یا مالی موتورهای جست‌وجو، از حوزهٔ کاوش آنها و در نتیجه از دسترس کاربران دور مانده‌اند (منصوریان، ۳۳:۱۳۸۲).

---

1. Matthew Koll.
2. Deep web.
3. The truly invisible web.

جامعهٔ مجـازی: جامعـهٔ مجـازی، سـومین جامعـه‌ای اسـت کـه جامعـهٔ غـرب پـس از جامعـهٔ صنعتی، به آن می‌رسد. بر اساس تحقیقاتی که در حـوزه‌هـای آینـده‌شناسـی رسـانه صـورت گرفته است، جامعهٔ مجازی شـامل مؤلفـه‌هـایی از جملـه وب، پاکدسـت، وبـلاگ، ویکـی، تجارت اجتماعی و جامعهٔ همراه می‌گردد (ارجمندی، ۱۳۹۳).

وب عمیق، شبکه‌های پیازی

وب نامرئی به بخشی از فضای شبکهٔ وب اطلاق می‌شود که ربات‌هـای موتورهـای کـاوش، قـادر بـه دسترسـی و شناسـایی آن نیسـتند و بـه‌همـین دلیـل در پایگـاه اطلاعـاتی آنهـا وارد نمی‌شوند، مثل: صفحاتی که برای دسترسی به آنهـا نیـاز بـه گـذرواژه[1] اسـت یـا فایـل‌هـای دیداری و شنیداری و تصاویر.

«شرمن» و «پرایس» به‌طور خلاصه وب نامرئی را این‌چنین تعریف نمودند: «وب پنهـان آن بخش از فضای شبکهٔ جهان‌گستر وب می‌باشد کـه عمـدتاً شـامل منـابع اطلاعـاتی غیرمتنـی و پویایی است که به هر دلیل، بـه‌طـور موقـت یـا دایـم خـارج از حـوزهٔ جسـت‌وجـو و بازیـابی موتورهای کاوش قرار دارند و بازیابی اطلاعات موجود در آن از طریق استفادهٔ مستقیم از ایـن موتورها میسر نمی‌باشد. امکان بازیابی منابع پنهان در وب نامرئی، یا بـرای موتورهـای کـاوش از نظر فنی میسر نیست یا محدودیت‌های مالی مانع از نمایه‌سازی این منابع شده است».

در خصوص وب نامرئی کلمه‌هایی نظیر: وب پنهان[2]، وب عمیق[3] و وب تاریک[4] به‌طـور مترادف در متون مختلف به‌کار برده شده‌اند؛ اما اینها در حقیقت معـادل یکـدیگر نیسـتند و هر یک به جنبه‌ای از نامرئی بودن اشاره می‌کنند.

بخش‌های مختلف وب نامرئی

وب مات یا تاریک: بخشی از فضای وب نامرئی به «وب مات» موسوم گردیـده اسـت کـه می‌تواند مورد استفاده کاربران قرار گیرد؛ اما به دلیل‌هـای زیـر ایـن اطلاعـات در خـارج از دسترس کاربران قرار گرفته است و موتورهای کاوش نمی‌توانند آنها را بازیابی کنند:

---

1. Password.
2 .Hidden web.
3. Deep web.
4. Opaque web.

- از آنجا که نخست محیط وب به‌طور دایم در حال تغییر است و هر روز منابع و اطلاعات جدید به آن افزوده می‌شود و دوم اینکه صفحه‌هایی در وب وجود دارد که هیچ پیوندی بین آنها با منابع دیگر برقرار نشده است، خزنده‌های موتورهای جست‌وجو قادر به یافتن این صفحه‌ها و همگام نمودن خود با این حجم عظیم اطلاعات نیستند؛
- به دلیل محدودیت توانایی، نرم‌افزارهای خزنده فرصت کافی برای روزآمدسازی صفحات جدید وب را ندارند. موتورهای کاوش نیز امکان روزآمدسازی حجم عظیمی از اطلاعات و منابع جدید را ندارند و به‌همین دلیل بسیاری از این اطلاعات از حوزهٔ موتورهای کاوش دور می‌مانند؛
- محدودیت توان مالی بسیاری از موتورهای کاوش سبب شده است که موتورهای کاوش نتوانند تمام صفحه‌های وب‌گاه‌ها را نمایه‌سازی کنند؛ چرا که برای آنها هزینه‌های زیادی دارد و بنابراین موتورهای کاوش بنا بر سیاست‌های خودشان، تنها بخشی از وب‌گاه‌ها یا لایه‌های بیرونی آنها را نمایه‌سازی می‌کنند؛ بنابراین همیشه بخش عظیم لایه‌های درونی وب‌گاه‌ها پنهان می‌مانند.

منابع موجود در وب نامرئی

با توجه به آنچه گفته شد، بخش بزرگی از وب وجود دارد که عنکبوت‌های موتورهای جست‌وجو آنها را نمایه نمی‌کنند یا نمی‌توانند نمایه کنند و عبارتند از: سایت‌های دارای رمز عبور، اسناد موجود در پشت سامانه‌های حفاظتی[1]، فایل‌های «pdf» از متون آرشیو شده و ابزارهای تعاملی نظیر: ماشین حساب‌ها و برخی واژه‌نامه‌ها و همچنین محتویات بعضی از پایگاه‌های اطلاعاتی، منابع محافظت شده از طریق اسم کاربر و گذرواژه، منابع و صفحه‌های وب بدون پیوند و صفحه‌های افزون بر حداکثر تعداد صفحه‌های قابل مرور در نتایج بازیابی.

اهمیت وب نامرئی[2]

به دو دلیل می‌توان گفت که وب نامرئی اهمیت دارد؛ نخست از نظر کمی، باید گفت که حجم اطلاعات موجود در این بخش خیلی بیشتر از سطح آشکار است. موارد زیر، اهمیت وب نامرئی را از نظر کمی نشان می‌دهند (Devine and Egger-sider,۲۰۰۱):

1. Firewalls.
2. Visible.

- بهترین موتورهای کاوش فقط قادر هستند که حدود ۱۶درصد از اطلاعات موجود در وب را بازیابی کنند و بنابراین ۸۴ درصد آنها جزو وب نامرئی به حساب می‌آیند؛
- اندازهٔ وب نامرئی تقریباً ۵۰۰ برابر وب مرئی است (وب نامرئی ۵۵۰ میلیون سند و وب مرئی تقریباً ۱ میلیون سند را داراست).

دوم اینکه از نظر کیفی، اطلاعات بخش‌های مختلف این مجموعه به‌ویژه منابع اطلاعاتی موجود در وب عمیق، معمولاً منابع ارزشمند و مفید و در بسیاری از موارد پاسخگوی نیاز کاربران هستند. به‌طور نسبی بیش از نیمی از وب نامرئی را پایگاه‌های اطلاعاتی موضوعی تشکیل می‌دهند.

سازوکار موتورهای کاوش

موتورهای کاوش، نرم‌افزارهای کاربردی هستند که برای جست‌وجوی منابع اطلاعاتی در اینترنت استفاده می‌شوند. (ابراهیمی، ۱۳۸۰) این نرم‌افزارهای کاربردی، تحت شبکه و در محیط وب قابل دسترس هستند و بر اساس کلیدواژه‌ها و عبارت‌های مورد نظر، جست‌وجو را بر روی یک پایگاه اطلاعاتی انجام می‌دهند و نتیجه را همراه با پیوندهایی به اصل موضوع ارائه می‌کنند. این موتورهای جست‌وجو با هدف سهولت دسترسی به اطلاعات ابداع گردیدند و به‌عنوان پایگاه اطلاعاتی، از ساختار محتوایی نوینی نسبت به پایگاه‌های اطلاعاتی سنتی برخوردارند. این در حالی است که تحقیقات دانشگاهی بسیاری در زمینهٔ ابزارهای کاوش در اینترنت صورت گرفته یا در حال انجام است (کوشا، ۱۳۸۲). اگرچه ابزارهای کاوش، حجم بسیار بالایی از اطلاعات (صفحه‌های وب) را در پایگاه‌های خود نمایه و با سرعت بالایی بازیابی می‌کنند؛ اما این پرسش مطرح می‌شود که آیا همهٔ اطلاعات موجود در وب توسط این ابزارها قابل بازیابی است؟ تقریباً همهٔ ابزارهای کاوش، خود را بهترین، کارامدترین و قدرتمندترین وسیله برای جست‌وجو و بازیابی اطلاعات در محیط وب معرفی می‌کنند؛ اما تحقیقات نشان می‌دهد که بهترین موتورهای جست‌وجو فقط ۱۶درصد از اطلاعات موجود بر روی وب را به کاربران عرضه می‌کنند (منصوریان،

۱۳۸۲). دلیل‌های متعددی در این زمینه وجود دارد که بخشی از این مشکلات و دشواری‌ها به حجم عظیم و روزافزون اطلاعات موجود در اینترنت مربوط می‌شود. بخش دیگر به میزان مهارت‌های اطلاع‌یابی کاربران و تجربهٔ آنان در کاوش برمی‌گردد و بخش دیگر نیز به‌دلیل وجود وب نامرئی یا وب پنهان است که موتورهای کاوش، به ادله‌ای که در این مقاله شرح داده می‌شود، قادر به انجام عمل بازیابی در آن نیستند. افزایش روزافزون منابع اطلاعاتی در اینترنت و مشکلات فنی و غیرفنی موتورهای کاوش موجب شده حجم زیادی از این اطلاعات از دید کاربران پنهان بماند و به‌عنوان وب نامرئی مورد بحث بسیاری از متخصصان قرار گیرد.

بخش‌های مختلف موتورهای کاوش

عنکبوت[1]: عنکبوت با وارسی و پویش صفحه‌های وب، پیوندهای موجود در هر صفحه و صفحه‌های مربوط به آن صفحه را دنبال می‌کند. این ربات‌ها معمولاً هرچند وقت یک‌بار در اینترنت به جست‌وجوی صفحه‌های وب و ارتباط آنها با صفحه‌های دیگر می‌پردازند و در پایان، آنچه را پیدا کرده‌اند به نمایه می‌افزایند. گستردگی و عمق دسترسی به اطلاعات در هر موتور جست‌وجو، بیش از هر چیز به ویژگی‌های نرم‌افزار خزندهٔ آن بستگی دارد.

نمایه[2]: یک پایگاه اطلاعاتی است که اطلاعات نمایه‌سازی شده و مرتبط با صفحه‌ها یا وب‌گاه‌ها در آنجا نگهداری می‌شود و قابل بازیابی است. ساختار نمایه و اندازه و حجم آن، در موتورهای جست‌وجو متفاوت است؛ به‌همین دلیل جست‌وجو با کلیدواژه‌های یکسان در موتورهای گوناگون، نتایج نسبتاً متفاوتی را در پی خواهد داشت.

نرم‌افزار جست‌وجو در نمایه[3]: برنامه‌ای است که در میان میلیون‌ها صفحهٔ نمایه شدهٔ موجود در یک موتور جست‌وجو، مطابق با پرسش جست‌وجوگر و راهبردهای جست‌وجو عمل می‌کند و اطلاعاتی را که با موضوع مرتبط باشد بازیابی می‌کند و نمایش می‌دهد.

---

1. Spider. Crawler.
2. Index.
3. Query processor.

ادلهٔ عدم بازیابی و نمایه‌سازی وب نامرئی توسط موتورهای کاوش

دلیل‌های فنی: بسیاری از موتورهای کاوش به‌دلیل محدودیت‌های نرم‌افزاری، توانایی روزامدسازی اطلاعات جدید وب را ندارند. گفتنی است، هنوز هیچ موتور کاوشی ادعا نکرده که قادر به گسترش حوزهٔ کاوش خود به تمام محیط وب است و همیشه این موتورها یک گام از سرعت روزافزون اطلاعات عقب‌تر هستند.

دلیل‌های بودجه‌ای: همان‌طور که پیش از این اشاره شد فرایند نمایه‌سازی تمام صفحه‌های وب، هزینه‌بَر خواهد بود و موتورهای کاوش نیز بنا به محدودیت بودجه، ناگزیرند فقط بخشی از وب‌گاه‌ها را نمایه‌سازی کنند.

دلیل‌های اجتماعی و حقوقی: از آنجا که اطلاعات موجود در وب در دسترس عموم قرار می‌گیرد، بسیاری از افراد و سازمان‌ها به دلیل صرف بودجه‌های کلان در راه‌اندازی وب‌گاه‌ها و پایگاه‌های اطلاعاتی خود، حاضر نیستند این اطلاعات را به‌صورت رایگان در اختیار همه بگذارند؛ البته این از لحاظ اجتماعی و حقوقی حق مسلم آنها است.

شیوه‌های اطلاع‌یابی در وب نامرئی

در حال حاضر ابزارهایی به‌وجود آمده‌اند که منابع وب نامرئی را شناسایی و کاربران را به وب‌گاه‌های مناسب راهنمایی می‌کنند. این رویکرد را بزرگراه‌های اطلاعاتی و کتابخانه‌های مجازی پذیرفته‌اند؛ به‌طوری که فقط توصیفی از پایگاه‌های اطلاعاتی و مجله‌های نامرئی را ارائه می‌کنند؛ مانند وب‌گاه «Invisibleweb» که فهرستی از منابع نامرئی و وب‌گاه «Completeplaset» که فهرستی حدود ۴۰۰۰۰ پایگاه اطلاعاتی وب نامرئی را ارائه می‌دهند. برخی دیگر از ابزارهای اطلاع‌یابی نیز که تاکنون معرفی شده‌اند و می‌توان با استفاده از آنها به این اطلاعات دسترسی پیدا کرد، به شرح زیر است:

پورتال‌ها یا پایگاه‌های اطلاعاتی خاص موضوعی: مجموعه‌ای از پایگاه‌های اطلاعاتی خاص موضوعی هستند که به یک موضوع خاص اختصاص دارند و به‌وسیلهٔ دانشمندان، محققان، متخصصان، مؤسسه‌های دولتی، شرکت‌های بازرگانی و کارشناسان موضوعی، افراد بسیار علاقه‌مند یا دارای دانش حرفه‌ای و اطلاعات وسیع در حوزهٔ خاص ایجاد

می‌شوند (Oxford uni. Libraries. 2000). از پورتال‌ها در هنگام جست‌وجو برای موضوع‌های خاص مانند: پیوندهای خبری، فایل‌های چندرسانه‌ای، بایگانی‌ها، فهرست‌های پستی اشخاص، شغل‌یاب‌ها و هزاران پایگاه اطلاعاتی که به موضوع‌های خاص اختصاص دارند استفاده می‌شود. از مزیت‌های عمدهٔ استفاده از دروازه‌های اطلاعاتی این است که برای ایجاد آنها، افرادی با دانش موضوعی خاص، در اینترنت جست‌وجو کرده‌اند و به پالایش اطلاعات مفید از غیرمفید پرداخته‌اند.

ابرموتورهای کاوش: گسترش‌پذیری حوزه‌های جست‌وجو نیز یکی از شیوه‌های دسترسی به وب نامرئی شمرده می‌شود که نمونهٔ آن، استفاده از ابرموتورهای کاوش است. این ابرموتورها خود، موتورهای جست‌وجوی واقعی نیستند؛ بلکه به کاربران این امکان را می‌دهند که کلیدواژه‌های خود را هم‌زمان توسط چند موتور، مورد کاوش قرار دهند و نتایج جست‌وجوی همهٔ آنها را با هم ببینند.

اینترنت با وب چه تفاوتی دارد؟

بسیاری افراد «اینترنت» و «وب» را دو مفهوم مترادف در نظر می‌گیرند؛ در حالی که این موضوع درست نیست. در واقع وب، یک جزء از اینترنت است. وب، یک محیط است که از طریق آن اطلاعات قابل دسترسی است. در تصور بسیاری از مردم، وب منحصراً به وب‌گاه‌هایی اطلاق می‌شود که از طریق موتورهای جست‌وجوی سنتی (همچون گوگل) قابل دسترسی و کاوش هستند. در حالی که این محتواها (که با عنوان لایهٔ سطحی[1] از آن یاد می‌شود) بخشی از وب هستند. «وب عمیق»[2] در واقع به مجموعه‌ای از محتواهای اینترنتی اشاره دارد که به دلیل‌های فنی بسیار، توسط موتورهای جست‌وجو، نشانه‌گذاری و آدرس‌دار نمی‌شوند و به‌همین دلیل است که با کمک این موتورهای جست‌وجوگر قابل ردیابی نیستند.

در حقیقت، موتورهای جست‌وجوگر تجاری همچون گوگل و بینگ[3]، از الگوریتم‌هایی برای نمایش دادن نتایج جست‌وجو استفاده می‌کنند که بر مبنای پرطرفدار

1. Surface Web.
2 .Deep Web.
3. Bing.

بودن و یا رتبهٔ وب‌گاه‌های مختلف استوار است. با وجود این، این موتورهـای جسـت‌وجـو، تنها حدود ۵ درصد از محتوای اینترنت را پویش می‌کننـد. آنچـه بیـان شـد، بخـش‌هـایی از یک گزارش با عنوان «وب تاریک» است که به تازگی (ژولای ۲۰۱۵) در مرکز پـژوهش‌هـای کنگرهٔ آمریکا[1] و توسط یکی از متخصصان امنیت داخلی امریکا[2] ارائه شده است. در ادامـه مهم‌ترین بخش‌های این گزارش، مرور خواهد شد.

در این گزارش، لایه‌های مختلف اینترنت، بسیار متفاوت با آن محتواهای سـطحی و ظـاهری که با یـک جسـت‌وجـوی اولیـه در دسـترس همگـان هسـتند، معرفـی شـده اسـت. در حقیقـت، محتواهای دیگری نیز در اینترنت وجود دارد کـه بـه‌عنـوان «وب عمیـق» شـناخته مـی‌شـوند. ایـن محتواها توسط موتورهای جست‌وجوی معمولی همچون گوگل، فهرست‌بندی نمـی‌شـوند و قابـل شناسایی نیستند. دورترین نقاط از وب عمیق نیز «وب تاریک» نام دارد که شـامل بخـش‌هـایی از وب می‌شود که در واقع به‌صورت خودخواسته و عامدانه، پنهان شده‌اند!

استفاده‌های دولت‌ها از وب تاریک

استفاده از وب تاریک به استفاده‌های غیرقـانونی محـدود نمـی‌شـود؛ بلکـه دولـت‌هـای مختلـف می‌توانند برای انتقال امن اطلاعات برای مقاصد امنیتی، نظامی و انتظامی از آن بهره‌برداری کنند.

در این گزارش، به این نکته اشاره شده است: «سوءاسـتفاده‌هـایی کـه از محـیط وب تاریـک شده، سـبب جلـب توجـه قـانون‌گـذاران و مقـام‌هـای رسـمی بـه ایـن موضـوع گردیـده اسـت». پژوهشگران و محققان حـوزهٔ امنیـت، همـواره در حـال کـار بـر روی وسـایلی هسـتند تـا بتواننـد خدمات و شبکه‌های مخفی را مشخص و افراد و کاربران این محیط را شناسایی کنند.

به عنوان نمونه در این گزارش به برخـی از راه‌کـنش‌هـای وزارت دفـاع امریکـا در ایـن راستا اشاره شده است:

به منظور مقابله با تحرک‌های داعش و گروه‌های تارشگری در فضای وب تاریـک، وزارت دفاع امریکا می‌تواند با مجموعه‌ای از راه‌کنش‌های مقابله‌ای، این فعالیت‌ها را تحت نظر بگیرد.

---

1. Congressional Research Service.
2. Kristin Finklea.

آژانس پروژه‌های پیشرفتهٔ دفاعی (DARPA) که از سازمان‌های تابع وزارت دفاع امریکاست، در حال کار بر روی یک پروژهٔ مطالعاتی موسوم به Memex است تا یک موتور جست‌وجوی جدید طراحی کند که الگوها و روابط میان داده‌های دیجیتال برخط را به‌دست آورد و به‌منظور تشخیص فعالیت‌های غیرمجاز و غیرقانونی، به نیروهای مختلف امنیتی کمک کند. در واقع هدف نهایی پروژهٔ Memex تشکیل یک نقشهٔ جامع از محتواهای موجود بر روی اینترنت است.

علاوه بر بخش‌های نظامی، در بخش‌های مختلف دیگر دولت آمریکا، پروژه‌های دیگری در همین راستا تعریف شده‌اند:

آژانس امنیت ملی آمریکا (NSA) برنامهٔ XKeyscore را در دستورکار خود دارد (این برنامه را «ادوارد اسنودن» فاش کرد) بر مبنای این برنامه، هر کاربری که نرم‌افزار خاص ورود به وب تاریک را از اینترنت دریافت کرده است، به‌طور خودکار، مورد پیگرد قرار خواهد گرفت و تمامی فعالیت‌های او ثبت خواهد شد.

سازمان‌های اطلاعاتی و امنیتی امریکا نیز این موضوع را در رأس فعالیت‌های خود قرار داده‌اند. مؤسسهٔ مطالعات پیشرفتهٔ جاسوسی در امریکا (IARPA) نیز برنامه‌ای با عنوان «حمله‌های سایبری، روش‌های پیش‌بینی، تشخیص، مقابله و دفاع در برابر آن» را توسعه داده است.

انواع محتوای وب عمیق

وب متنی[1]: صفحه‌هایی است که محتوای آنها با سطوح دسترسی متفاوت، تغییر می‌کند.

محتوای پویا[2]: شامل صفحه‌های پویای وب است.

محتوای وب با دسترسی محدود[3]: وب‌گاه‌هایی است که دسترسی به محتوای خود را به دلیل‌های فنی محدود کرده‌اند.

---

1 .Contextual Web.
2 .Dynamic content.
3 .Limited access content.

محتوای غیرمتنی[1]: شامل محتوایی است که به قالب‌های غیرمتنی مانند: قالب‌های چندرسانه‌ای رمزنگاری شده‌اند.

وب خصوصی[2]: بخشی دیگر از وب نامرئی وجود دارد که چون اطلاعات موجود در آن جزء دارایی‌های شخصی یا خصوصی سازمان‌ها یا افراد است، از حوزهٔ دسترسی موتورهای جست‌وجو پنهان است. به‌عنوان مثال: در برخی از سازمان‌ها و مؤسسه‌های خصوصی یا دولتی، به ادلهٔ امنیتی از اطلاعات مربوط به مسائل کاری و سازمانی و نیروی انسانی خود حفاظت می‌کنند، اجازهٔ دسترسی به دیگران نمی‌دهند و فقط کسانی که دارای اسم کاربر و گذرواژه هستند می‌توانند از آنها استفاده کنند؛ این بخش، وب خصوصی محسوب می‌گردد (منصوریان، ۱۳۸۲:۳۲).

وب ملکی[3]: بخش دیگر، منابع اطلاعاتی از قبیل نشریه‌های الکترونیکی مبتنی بر وب هستند که دسترسی به آنها از طریق پرداخت حق اشتراک و خرید محصولات اطلاعاتی شرکت‌های مختلف صورت می‌گیرد و «وب ملکی» نامیده می‌شود.

محتوای اسکریپت[4]: شامل صفحه‌ها و منابعی است که از طریق «جاوا اسکریپت» پیوند می‌شوند.

محتوای پیوند نشده[5]: صفحه‌ها و منابعی از وب هستند که توسط صفحه‌های دیگر پیوند نشده‌اند.

محتوای بایگانی شده[6]: شامل صفحه‌های وب بایگانی شده است که به کاربر اجازهٔ دسترسی نسخه‌های صفحه‌های وب مورد نظر را در طول زمان می‌دهد. خدماتی نظیر Machine Wayback نمونه‌ای از منابع محتوای بایگانی شدهٔ اینترنتی است.

وب مات یا تاریک[7]: بخشی از فضای وب نامرئی، وب مات یا تاریک نامیده می‌شود که یک نوع شبکهٔ پوششی[8] است و تنها از طریق یک نرم‌افزار، پیکربندی و یا مجوز خاصی

---

1 .Non-HTML/text content.
2 .Private Web.
3 .Proprietary Web.
4 .Scripted content.
5 .Unlinked content.
6 .Web archives.
7 .Dark Web.
8 .Overlay Network.

قابلیت دسترسی به آن وجود دارد. وب تاریک اغلب از قراردادها و پورت‌های غیراستاندارد برای برقراری ارتباط استفاده می‌کند.

شبکه‌های فعال نرم‌افزاری وب تاریک

- Tor؛
- I2P؛
- Freenet؛
- RetroShare؛
- GNUnet؛
- Zeronet؛
- Syndie؛
- OneSwarm؛
- Tribler.

اهمیت وب نامرئی

به دو دلیل می‌توان گفت که وب نامرئی اهمیت دارد؛ نخست از نظر «کمی» باید گفت که حجم اطلاعات موجود در این بخش خیلی بیشتر از سطح آشکار است. موارد زیر، اهمیت وب نامرئی را از نظر کمی نشان می‌دهد:

- بهترین موتورهای کاوش فقط قادر هستند که حدود ۶ درصد از اطلاعات موجود در وب را بازیابی کنند؛ بنابراین، ۸۴ درصد آنها جزء وب نامرئی به‌حساب می‌آیند؛
- در گزارشی نیز اندازهٔ وب مرئی را تقریباً ۱۶۷ ترابایت تخمین زده‌اند؛ و این در حالی است که اندازهٔ وب نامرئی را در حدود ۹۱۰۰۰ ترابایت پیش‌بینی می‌کنند.

دوم اینکه از نظر کیفی، اطلاعات بخش‌های مختلف این مجموعه به‌ویژه منابع اطلاعاتی موجود در وب عمیق، معمولاً منابع ارزشمند و مفید و در بسیاری از موارد پاسخگوی نیاز کاربران هستند. تقریباً بیش از نیمی از وب نامرئی را پایگاه‌های اطلاعاتی موضوعی تشکیل می‌دهند.

منابع موجود در وب نامرئی

پایگاه‌های اطلاعاتی دربردارندهٔ اطلاعاتی هستند که در جدول‌هایی که با برنامه‌هایی مانند: access، oracle، SQL server و DB2 ساخته شده‌اند، ذخیره گردیده است.

اطلاعات ذخیره شده در این پایگاه‌های اطلاعاتی تنها از طریق جست‌وجوی این پایگاه‌ها قابل استحصال هستند؛ بنابراین، این اطلاعات با صفحهٔ وب معمولی که به‌صورت اسنادی با امکان دسترسی مستقیم هستند، متفاوت‌اند. این پایگاه‌های اطلاعاتی معمولاً یک موضوع مشخص و یا جنبهٔ خاصی از یک موضوع مشخص را دربر می‌گیرند. عنکبوت‌های موتورهای جست‌وجو از فهرست کردن این‌گونه اطلاعات عاجزند. حجم قابل توجهی از اطلاعات باارزش روی وب را این پایگاه‌های اطلاعاتی ارائه می‌کنند. در واقع، تخمین زده می‌شود که حجم اطلاعات موجود در این پایگاه‌ها پانصد برابر اطلاعات موجود در صفحه‌های وب معمولی باشد.

منابع موجود در وب نامرئی به‌طور خلاصه عبارت‌اند از: «وب‌گاه‌های دارای رمز عبور، اسناد موجود در پشت سامانه‌های حفاظتی، فایل‌های pdf از متون آرشیو شده و ابزارهای تعاملی نظیر: ماشین حساب‌ها و برخی واژه‌نامه‌ها و همچنین محتویات بعضی از پایگاه‌های اطلاعاتی، منابع حفاظت شده از طریق اسم کاربر و گذرواژه، منابع و صفحه‌های وب بدون پیوند و صفحه‌های افزون بر حداکثر تعداد صفحه‌های قابل مرور در نتایج بازیابی».

در اینجا چند نشانی ارائه می‌شود که در دستیابی به وب نامرئی می‌توانند مفید باشند:

CompletePlanet	دارای یک سامانهٔ جست‌وجو برای دستیابی به هزاران موتور جست‌وجو
Direct Search	منبع بزرگی از آدرس‌ها و لینک‌های جمع‌آوری شده به منابع تحقیقاتی مختلف
Invisible-web.net	یک دایرکتوری از منابع عالی برای وب عمیق
ProFusion	یک متاموتور که بر اساس موضوع در وب عمیق به‌طور عمودی جست‌وجو در اعماق وب را انجام می‌دهد.

آشنایی با وب تاریک

«وب تاریک» به بخشی از دنیای وب گفته می‌شود که به‌صورت عمومی در اختیار همهٔ کاربران وب قرار ندارد. بخش عمده‌ای از فعالیت‌هایی که در این دنیای تاریک صورت می‌پذیرد، قابل شناسایی نیستند و هیچ سازمان یا موتور جست‌وجویی توانایی ردیابی این فعالیت‌ها را ندارد؛ به‌همین دلیل از این بخش وب، بیشتر برای انجام کارهای غیرقانونی مانند: خرید و فروش مواد مخدر و سلاح گرم استفاده می‌شود.

وب تاریک یکی از مراجع اطلاعاتی کامل به‌شمار می‌آید که البته افراد غیرقابل شناسایی، اطلاعات آن را نگهداری می‌کنند؛ تارشگرها و نفوذگرها، بخشی از این افراد را تشکیل می‌دهند.

در وب تاریک، فروشگاه‌های خاصی در حال فعالیت هستند که در اصطلاح فروشگاه‌های «دارک‌نت» نامیده می‌شوند که عمدهٔ محصولات این فروشگاه‌ها غیرقانونی هستند؛ به‌طوری که مواد مخدر و سلاح گرم هم در این فروشگاه‌ها به فروش می‌رسد. پرداخت‌ها در فروشگاه‌های وب تاریک معمولاً با استفاده از پول مجازی «بیت کوین» انجام می‌گیرد.

در واقع وب‌گاه‌های وب تاریک، توسط افراد عمومی قابل مشاهده هستند؛ اما برای اجرا شدن از «IP» نشانی‌های مخفی سرور استفاده می‌کنند؛ یعنی هر فردی می‌تواند از این وب‌گاه‌ها استفاده کند اما هیچ‌کس نمی‌تواند هویت واقعی گردانندگان این وب‌گاه‌ها را شناسایی کند. اطلاعات موجود در این وب‌گاه‌ها به‌صورت برخط توسط گذرواژه‌ها، رمزنگاری و محافظت می‌شوند که همین عامل دلیل پنهان بودن این بخش از دنیای وب به‌شمار می‌آید؛ به‌طوری که شناسایی وب‌گاه‌های موجود در وب تاریک، حتی برای موتورهای جست‌وجو نیز کاری بسیار دشوار است و کاربران نیز به کمک موتورهای جست‌وجوی معمولی نمی‌توانند به این قبیل وب‌گاه‌ها دسترسی داشته باشند. وب‌گاه‌هایی که موتورهای جست‌وجو نمی‌توانند آنها را شناسایی کنند در اصطلاح «دیپ وب» نامیده می‌شوند و برای پنهان ماندن از ابزارهای رمزنگاری قوی نظیر «Tor» بهره می‌برند.

براساس تخمین‌های صورت گرفته، شبکهٔ تاریک وب تقریباً ۵۰۰ برابر بزرگ‌تر از شبکهٔ جهانی وبی است که کاربران به‌صورت روزانه از آن بهره می‌برند.

گروه‌های تارشگری تبادل نظر، تبلیغات گسترده، استخدام نیرو و حتی طراحی حمله‌ها را از طریق وب تاریک انجام می‌دهند؛ به این دلیل که وب در همه جا و در هر لحظه در دسترس است و گروه‌های تارشگری بیشتر از قبل می‌توانند با یکدیگر ارتباط داشته باشند و از طریق گروه‌های مجازی با یکدیگر همکاری کنند. وب تاریک شامل اطلاعات زیادی دربارهٔ گروه‌های تاریک و اخبار مربوط به آنها می‌شود.

شبکهٔ تاریک، شبکه‌ای همپوشان با قابلیت دسترسی از طریق نرم‌افزار مخصوص به خود است. این شبکه، شبکه‌ای شخصی و پوشیده است که ارتباطات آن فقط به‌صورت ارتباط یک زوج معتمد یعنی کاربر به کاربر - گاهی می‌گویند دوستان به دوستان[1] - است که از پروتکل‌ها و پورت‌های غیراستاندارد استفاده می‌کند. شبکه‌های تاریک، متمایز از دیگر شبکه‌های رایج کاربر به کاربر هستند به‌طوری که اشتراک‌گذاری به‌صورت مخفی بودن نشانی IP است. شبکهٔ تاریک، به‌طور گسترده‌ای پذیرفته شده است و رسانه‌های بزرگ از جمله Rolling Stone و Wired آن را به‌کار می‌گیرند.

شبکه‌های تاریک می‌توانند استفاده‌های مختلفی داشته باشند از جمله:

- نگرانی‌های حریم خصوصی یا ترساندن توسط مخالفان سیاسی؛
- برای انتشار دستاوردهای مجرمانه؛
- برای اشتراک فایل‌های صوتی و تصویری (اغلب فایل‌هایی که قانون کپی رایت از آنها حمایت می‌کند).

شبکه‌های تاریک، یک طبقه‌بندی از شبکه‌ها است؛ بنابراین از لحاظ فنی می‌توان گفت که مجموعه‌ای از «IP ها» که در بُرد (رِنج) خاصی با هم کار می‌کنند و همچنین با یک «پراکسی» با هم هماهنگ شده‌اند و در یک فرمت بر اساس پروتکلی که مورد استفاده قرار گرفته رمزگذاری شده است.

---

1 .Frind 2 Frind.

بیشتر اطلاعات شبکهٔ تاریک در پایگاه داده‌هایی نظیر LexisNexis ذخیره می‌شود. در این شبکه، اطلاعات جامعی نهفته شده است که افراد ناشناس آنها را مدیریت می‌کنند. نفوذگرها، تارشگرها و افراد سودجو، اغلب این دسته از افراد را تشکیل می‌دهند؛ اگرچه این دو به‌جای دیگر به‌کار گرفته می‌شوند.

یک نمونه از وب‌گاه‌های شبکهٔ تاریک، Silk Road و مشتقات آن است که وب‌گاهی برای خرید و فروش مواد مخدر است. سامانهٔ «دیپ‌وب» در جوامع توتالیته ممکن است برای ارتباط بدون حد و حصر استفاده شود؛ اما این بدان معنا نیست که کشورهای به اصطلاح دمکراتیک جهان، مصون از این قضیه باشند؛ بلکه دقیقاً برخلاف تصور ما در این کشورها همچون امریکا یا انگلیس، استفاده از این روش محبوب‌تر شده است. یکی از ادلهٔ این موضوع را می‌توان افشاگری‌های مختلف در مورد استراق سمع مردم و رهگیری فعالیت آنها در اینترنت دانست.

وب تاریک به‌طور عام و شبکهٔ «TOR» به‌طور خاص، بستری امن را برای مجرمان فضای مجازی برای ارتکاب فعالیت‌های غیرقانونی از خرید و فروش محصولات مجرمانه تحت ارتباطات امن و غیرقابل ردیابی گرفته تا پیاده‌سازی بدافزارها و باتنت‌هایی که به سادگی قابل ردیابی و واپایش نیستند، فراهم می‌آورد؛ بدین لحاظ ردیابی و نظارت بر فعالیت‌های مجرمانه در این محیط (به ویژه شبکهٔ TOR) از اهمیت بسیار زیادی برای آژانس‌های امنیتی برخوردار است. در اینجا به معرفی و تحلیل فنّاوری جدیدی برای شناسایی و نظارت بر ترافیک سامانه‌های پنهان شبکه‌های وب تاریک به ویژه شبکهٔ TOR که محققان نیز در کنفرانس امنیتی، آن را در سال ۲۰۱۵ معرفی و بررسی کرده‌اند، پرداخته خواهد شد؛ این روش نشان می‌دهد که چگونه یک مهاجم می‌تواند از طریق به‌کارگیری نوعی حملهٔ همبستگی[1] به شناسایی و بررسی ترافیک دسترسی کاربران وب تاریک به سامانه‌های پنهان شبکه بپردازد.

نحوهٔ دسترسی به وب تاریک چگونه است؟

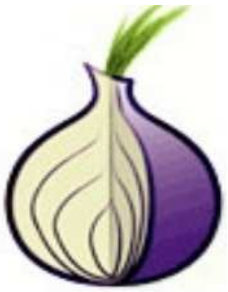
1 .Correlation Attack

به لحاظ فنی، دسترسی به این وب‌گاه‌ها چندان سخت نیست؛ به‌راحتی و با نصب Tor می‌توان زمینهٔ لازم برای دسترسی را فراهم کرد. برای این کار کافی است به نشانی www.torproject.org مراجعه و Tor Browser Bundle را دانلود نمایید که حاوی تمام ابزارهای لازم برای اتصال به شبکهٔ Tor است. بعد از نصب نرم‌افزار کافی است مرورگر مخصوص Tor را با فشردن Start Tor Browser باز کنید. بقیهٔ موارد به‌صورت خودکار بر روی شبکه اعمال می‌شود.

شکل شماره۱- نمای نرم‌افزار TOR

با دسترسی به شبکهٔ تاریک شما قادر خواهید بود به تمام محتواها و وب‌گاه‌های تابو دسترسی یابید که شامل مواد مخدر، فروش سلاح، نژاد پرستی، برده‌داری جنسی و موارد بدتر است. در وب‌گاه‌های اجتماعی همچون Reddit می‌توان فهرستی از آنها را پیدا کرد و برخی ویکی‌ها همچون http://thehiddenwiki.org سیاهه‌ای از این وب‌گاه‌ها را ارائه می‌کنند که می‌توانند مقصدهای خیلی بدی باشند که توصیه می‌شود از ورود به آنها پرهیز گردد. مورد مهمی که دربارهٔ این وب‌گاه‌ها باید مدنظر قرار داده شود این است که بسیاری از وب‌گاه‌های شبکهٔ تاریک، هر از چند گاهی و احتمالاً به دلیل محتواهای مجرمانه‌شان «داون[۱]» می‌شوند.

شبکهٔ پیازی Tor [۲]



Tor سامانه‌ای است که برای ناشناسی (ناشناس ماندن) کاربران در محیط اینترنت به‌کار می‌رود و از نرم‌افزار کارخواه و شبکه‌ای از خدمات‌دهنده‌ها (سرورها) تشکیل شده است و می‌تواند داده‌هایی از کاربران را مانند جایگاه و نشانی پروتکل اینترنت پنهان کند. بهره‌گیری از این سامانه، ردگیری و شنود داده‌های کاربر را به دست دیگران بسیار سخت می‌کند. این ردگیری و شنود می‌تواند در مورد بسیاری از فعالیت‌های کاربر مثل: بازدید از وب‌گاه‌ها، بارگیری و بارگذاری پرونده‌ها، ارسال یا دریافت پیام‌هایی که از طریق نرم‌افزارهای پیام‌رسان و هرگونه ارتباطاتی که در محیط اینترنت برقرار می‌کند، صورت پذیرد. این نرم‌افزار، یک نرم‌افزار آزاد است و استفاده از شبکهٔ آن نیز رایگان است.

Tor نخستین نسخهٔ خود را در ۲۰ سپتامبر ۲۰۰۲ عرضه کرد. این نرم‌افزار از سامانهٔ مسیریابی پیازی استفاده می‌کرد که آزمایشگاه تحقیقاتی نیروی دریایی امریکا آن را ایجاد کرده بود. وظیفهٔ اصلی آن ایجاد شبکه‌ای امن برای مکالمه‌های دولتی بود. پس از ایجاد

---

۱. داون یا Down اصطلاحی است که در دنیای مجازی به از کار افتادن وب‌گاه‌ها اطلاق می‌شود.

2. The Onion Router.

Tor این پروژه توسط خبرنگاران، مخالفان حکومت‌ها، سازمان‌های اطلاعاتی و پلیس مورد استفاده قرار می‌گیرد. پشتیبان‌های این نرم‌افزار، نیروی دریایی امریکا در سال‌های اولیه و سپس «ای‌اف‌اف» و بنگاه سخن‌پراکنی ایالات متحده در سال‌های کنونی بودند.

طرز کار: این نرم‌افزار از مسیریابی پیازی استفاده می‌کند. یک نرم‌افزار به‌جای اینکه به‌صورت مستقیم به ماشین مقصد متصل شود، به یک «پروکسی» مسیریاب پیازی وصل می‌شود. این پروکسی از طریق چند مسیریاب پیازی مسیر ناشناسی برای کاربر مبدأ ایجاد می‌کند. هر مسیریاب پیازی فقط رایانهٔ قبلی و بعدی خود را می‌شناسد. در عین حال رایانهٔ اول برای هر مسیریاب در راه یک لایهٔ رمزنگاری به دادهٔ ارسالی ماشین مبدأ اضافه می‌کند. پس از آن هر رایانه در راه، لایهٔ خود را از دادهٔ ارسالی کم می‌کند و در پایان دادهٔ ارسالی به ماشین مقصد، همان دادهٔ رمزنگاری نشده است. دادهٔ عبوری از مسیریاب‌ها برای هر مسیریاب متفاوت است و دلیل آن هم تفاوت در رمزنگاری است؛ دلیل دیگر تفاوت، جلوگیری از ورود مسیریاب‌های جعلی در میان راه است. اگر در میانهٔ راه ارتباط قطع شود، داده‌ها بدون هیچ تأخیری روی هر مسیریابی که باشند، حذف می‌شوند.

پل‌ها: رله‌های پلی (یا به‌صورت مخفف پل‌ها) مسیریاب‌هایی هستند که به‌صورت مستقیم در پوشهٔ اصلی Tor فهرست نشده‌اند. از آنجایی که یک فهرست جامع از آنها وجود ندارد، اگر حتی خدمات‌دهندهٔ اینترنت شما همهٔ این مسیریاب‌های فهرست شدهٔ Tor را ببندد، امکان بستن همهٔ پل‌ها وجود ندارد. اگر فکر می‌کنید که دسترسی شما به Tor مسدود شده‌است، می‌توانید از طریق سامانهٔ پل به شبکه وصل شوید.

اضافه شدن پل‌ها به شبکهٔ Tor برای افزایش مقاومت آن در برابر سانسورهای اینترنتی است. با وجود اینکه اینترنت شما ممکن است دارای فیلتر باشد، بهتر است Tor را بدون سامانهٔ پل آزمایش کرد و در صورت عدم اتصال به شبکه از سامانهٔ پل استفاده کرد. برای استفاده از پل‌ها باید شما یک پل را بیابید. سپس Tor خود را برای استفاده از این پل تنظیم نمایید. البته سامانهٔ Tor آدرس پل‌ها را با استفاده از پست الکترونیک برای شما ارسال می‌کند.

خروجی‌ها: یکی دیگر از مسیریاب‌های بسیار مهم در شبکهٔ Tor ، مسیریاب‌های خروجی هستند. این مسیریاب‌ها ظرفیت شبکه را مشخص می‌کنند. هر داده که از شبکه عبور می‌کند، باید از یکی از خروجی‌ها عبور کند و سپس به ماشین‌های خارج از شبکه انتقال پیدا می‌کند. خروجی‌ها به علت اینکه در پایان مسیر داده قرار دارند، به‌عنوان انجام دهندهٔ هر کاری که کاربران Tor انجام می‌دهند، شناخته می‌شوند. در واقع اگر کسی با استفاده از Tor کاری غیرقانونی انجام دهد، این شناسهٔ اینترنتی خروجی است که در پایان ثبت می‌شود. از این‌رو باید دقت عمل لازم برای تنظیم صحیح این مسیریاب‌ها انجام شود.

راه‌اندازی Tor: برای این کار می‌توان از برنامه‌های مختلف استفاده کنید و در غیر این صورت نسبت به توزیعی که استفاده می‌کنید می‌بایست مطابق با آن توزیع از دستورها و مخازن آن استفاده کنید. در اینجا ما از توزیع سامانهٔ عامل «اوبونتوبیس» استفاده می‌کنیم.

ابتدا این دستور را وارد می‌کنید: `$ sudo apt install tor` درصورتی که برای اتصال به شبکهٔ Tor محدودیت داشته باشیم، لازم است متن "get transportobfs4" را بدون موضوع به پست الکترونیک "bridges@bridges.torproject.org" ارسال کنیم بعد از مدتی نامهٔ الکترونیکی ارسال می‌شود که باید یکی از آنها را با نشانی پل موجود در پروندهٔ torrc عوض کنیم.

ابتدا با دستور زیر obsf4proxy را نصب می‌کنیم:

```
$ sudo apt install obfs4proxy
```

بعد از دستور بالا، فایل torrc را باز می‌کنیم:

```
$ gksudo gedit /etc/tor/torrc
```

و به انتهای فایل باز شده، خطوط زیر را اضافه می‌کنیم:

```
UseBridges 1
Bridge obfs4 69.162.169.229:7336
36366CA74CB5D7958A73BEB5681135F627DC4F05
cert=bxE0qAN4Um6XGBZ6beZGJM66vMRH/1uvf6hjwWWTO5rA
LH/bPkq9ktTVtyhhy1vO3YbwMA iat-mode=0
ClientTransportPlugin obfs4 exec /usr/bin/obfs4proxy
```

بعد از عملیات بالا، بایستی Tor را دوباره راه‌اندازی کنیم:

```
$ sudo systemctl restart tor.service
```

حال Tor در حال اجراست و با اتصال به socks به درگاه ۹۰۵۰ روی دامین محلی از آن استفاده کنیم. نکتهٔ قابل توجه این است که نخستین بار ممکن است مقداری زمان ببرد تا به شبکهٔ Tor متصل شویم.

برای دیدن گزارش از دستور زیر استفاده می‌کنیم:

```
Bootstrapped 100%: Done
```

در صورتی که در خروجی ظاهر شد به معنی این است که به تور متصل شدیم.

```
$ tail -f /var/log/tor/log
```

ایجاد پل خصوصی در تور

برای این امر می‌بایست یک سرور در خارج از کشور داشته باشیم و کشور میزبان نیز مشکل فیلترینگ نداشته باشد.

با دستور SSH به سرور متصل می‌شویم؛

بسته‌های tor و obfs4proxy را با استفاده از دستور زیر نصب می‌کنیم:

```
$ sudo apt install tor obfs4proxy
```

فایل torrc را ویرایش می‌کنیم:

```
$ sudo vim /etc/tor/torrc
```

مقادیر زیر را به انتهای فایل اضافه و ذخیره می‌کنیم:

```
SocksPort 0
ORPort auto
BridgeRelay 1
Exitpolicy reject *:*
## CHANGEME_1 -> provide a nickname for your bridge, can be anything you like
#Nickname CHANGEME_1
## CHANGEME_2 -> provide some email address so we can contact you if there's a problem
```

```
#ContactInfo CHANGEME_2
ServerTransportPlugin obfs4 exec /usr/bin/obfs4proxy managed
```

سامانه را re start می‌کنیم؛

```
$ sudo systemctl restart tor.service
```

بعد از صبر برای برقراری ارتباط با پل می‌توان با دستور زیر پل‌های ایجاد شده را دید:

```
$ cat /var/lib/tor/pt_state/obfs4_bridgeline.txt
```

خروجی به شکل زیر است:

```
Bridge obfs4 <IP ADDRESS>:<PORT> <FINGERPRINT>
cert=EQQDSR2PqQXnRvvY89HLVB3RQ2Kcc9i46IvEsWefjAFu58a
kKNMaHpA5PhzOdHynuW5beQ iat-mode=0
```

در صورت استفاده از سرور و دسکتاپ ابونتو (Ubunto) مشکل «apparmor» ممکن است رخ دهد.

در صورتی که دچار مشکل «apparmor» شویم، چنین متنی را در گزارش مشاهده خواهیم کرد که منجر به عدم راه‌اندازی می‌گردد:

```
[warn] Could not launch managed proxy executable at
'/usr/bin/obfs4proxy' ('Operation not permitted').
```

برای رفع این مشکل فایل زیر را ویرایش می‌کنیم:

```
$ gksudo gedit /etc/apparmor.d/abstractions/tor
```

و خط زیر را

```
$ gksudo gedit /etc/apparmor.d/abstractions/tor
```

جایگزین این خط می‌کنیم:

```
/usr/bin/obfs4proxy PUx,
```

در انتها می‌بایست apparmor را آبدیت کرد:

```
$ sudo apparmor_parser -r -v /etc/apparmor.d/system_tor
```

و شبکهٔ تور را re start کنیم:

```
$ sudo apparmor_parser -r -v /etc/apparmor.d/system_tor
```

برای اطمینان خاطر از اینکه سامانه به‌درستی کار می‌کند دستور زیر را وارد می‌کنیم:

```
$ tail -f /var/log/tor/log
```

راه‌های دسترسی به شبکهٔ تاریک وب

برای دسترسی و ورود به شبکهٔ تاریک وب، کاربران به نرم‌افزارهای خاصی نیاز دارند که البته تعداد زیادی از این نرم‌افزارها را توسعه دهندگان مختلف تولید کرده‌اند؛ در واقع، راه‌های زیادی برای ورود به شبکهٔ تاریک وجود دارد که مهم‌ترین آنها استفاده از نرم‌افزارهای Tor وFreenet و i2P است. از میان این سه نرم افزار، محبوب‌ترین آن Tor است که نام اصلی آن «پیاز روتر» می‌باشد و دلیل محبوب بودن آن ساده بودن کار با این نرم‌افزار نسبت به سایر هم‌نوعان خود است. دلیل نام‌گذاری «پیاز روتر» بر روی این نرم‌افزار آن است که Tor برای عبور اطلاعات همانند پیاز از یک شبکهٔ چندلایه استفاده می‌کند. اطلاعاتی که از طریق تور منتشر می‌شوند به‌گونه‌ای رمزگذاری شده‌اند که فقط توسط رایانه‌های مقصد قابل دسترسی هستند که این ویژگی یک راه امن را برای ایجاد ارتباط پنهان در شبکهٔ اینترنت فراهم می‌کند. یکی از راه‌های رمزگذاری بر روی صفحه‌ها توسط Tor استفاده از آدرس‌های اختصاصی خود است؛ به این معنی که این نرم‌افزار به‌جای آنکه از دامنه‌های پرکاربرد موجود نظیر com، net، org و... استفاده کند، از یک دامنهٔ اختصاصی onion بهره می‌برد. موتورهای جست‌وجو مانند «بینگ» و «داک داک گو» خدماتی را برای ارسال نشانی‌های مربوط به نرم‌افزار Tor به کاربران ارائه می‌دهند.

دسترسی به اطلاعات در شبکهٔ تاریک

از آنجا که یافتن اطلاعات و صفحه‌ها در شبکهٔ تاریک کار دشواری است و حتی موتورهای جست‌وجوگر معمولی قادر به نمایش اطلاعات این بخش از دنیای وب نیستند، به‌همین دلیل یکی از مشکلات در وب تاریک، یافتن اطلاعات و صفحه‌های مورد نظر است. بعد از ورود به دنیای تاریک وب، حال باید به برنامه‌ها و امکانات جداگانه‌ای برای یافتن اطلاعاتی که در پی آن هستیم، مراجعه کنیم. در ادامه به معرفی شاخص‌ترین راه‌ها برای دستیابی به اطلاعات در شبکهٔ تاریک اشاره می‌شود.

مرورگر ناشناس Tor: پیش از این اشاره شد که یکی از راه‌های دسترسی به شبکهٔ تاریک، بهره‌گیری از نرم‌افزار Tor است که دربارهٔ روش کار این نرم‌افزار نیز توضیحاتی

داده شد. نرم‌افزار یاد شده علاوه بر فراهم آوردن امکان ورود به وب تاریک، به ما در دستیابی به اطلاعات مورد نظرمان نیز کمک می‌کند. این نرم‌افزار در کنار رمزگذاری اطلاعات حین اتصال، یک مرورگر اختصاصی را در اختیار کاربر قرار می‌دهد که همانند خود نرم‌افزار، ردگیری اطلاعات در آن کاری دشوار است؛ چرا که از همان پروتکل‌های موجود برای یافتن اطلاعات استفاده می‌کند و همچنین برای مخفی ماندن کاربران از بیش از ۶۰۰۰ سرور بهره می‌برد. از آنجا که نشانی‌های ارائه شده Tor فقط دارای پسوند onion هستند، به همین دلیل این نشانی‌ها نیز تنها با استفاده از مرورگر اختصاصی این نرم‌افزار قابل دسترسی می‌باشند.

موتورهای جست‌وجوی مخفی: از آنجایی که دسترسی موتورهای جست‌وجوی معمولی به اطلاعات در شبکهٔ تاریک امکان‌پذیر نیست، به همین دلیل گردانندگان این بخش از دنیای وب، به راه‌اندازی موتور جست‌وجوی اختصاصی خود اقدام کرده‌اند که همانند سایر سامانه‌های شبکهٔ تاریک مخفی است و قابل شناسایی نیست و همچنین فقط از طریق دسترسی به وب تاریک می‌توان از آن بهره برد. نخستین موتور جست‌وجوی اختصاصی شبکهٔ تاریک را یک هکر در اواسط سال ۲۰۱۴ طراحی کرد که به کاربران امکان جست‌وجو در شبکهٔ تاریک وب را در میان اطلاعات منتشر شده می‌دهد. کاربران شبکهٔ تاریک به کمک این موتور جست‌وجو می‌توانند همهٔ خدمات و محصولات موجود در این بخش از وب، مانند: سلاح گرم، مواد مخدر، حساب‌های بانکی لو رفته و... را بیابند.

ویکی‌های جنایی: یکی دیگر از راه‌های دستیابی به اطلاعات در شبکهٔ تاریک، مراجعه به ویکی‌های موجود در آن است. ویکی‌هایی که به‌صورت غیرقانونی و به‌منظور ارائهٔ خدمات ممنوع طراحی شده‌اند که در اصطلاح «ویکی‌های جنایی» یا جنایتکارانه نام دارند. دلیل اصلی استفاده از ویکی‌ها در شبکهٔ تاریک، این است که بیشتر اطلاعات موجود در شبکهٔ تاریک در قالب صفحه‌های ویکی دسته‌بندی شده‌اند که حتی برای هر دسته‌بندی توضیحاتی نیز ارائه شده است. مهم‌ترین اطلاعات قابل دسترس در ویکی‌های شبکهٔ تاریک، بازارهای سیاه، مراجع فروش مواد مخدر، وب‌گاه‌های ارائه دهندهٔ بدافزارهای

رایانه‌ای، ارتباط با نفوذگرها و... هستند. در حقیقت مطالب و صفحه‌های قابل دسترس در شبکهٔ تاریک به‌صورت ویکی دسته‌بندی می‌شوند و به این منظور صفحه‌های وب تاریک را بیشتر به‌عنوان ویکی می‌شناسند؛ همین دلیل استفاده از مراجع ویکی، وب تاریک را به یکی از مرسوم‌ترین کارها برای دستیابی به اطلاعات مورد نظر تبدیل کرده است. برای نمونه صفحهٔ Hidden Wiki به‌عنوان مرجع اصلی اطلاعات وب تاریک استفاده می‌شود.

اتاق‌های گفت‌وگوی مخفی: در وب تاریک نیز همانند وب معمولی اتاق‌های گفت‌وگو برای ارتباط برقرار کردن میان کاربران آن وجود دارد اما برخلاف اتاق‌های گفت‌وگوی معمولی، ردیابی کردن کاربران اتاق‌های گفت‌وگوی تاریک به مراتب سخت‌تر و تا حدی غیرممکن است؛ به‌همین دلیل کاربران این بخش از دنیای وب برای یافتن نفوذگرها و افراد تبهکار مانند دزدهای اینترنتی، قاتل‌ها و... به این اتاق‌های گفت‌وگو مراجعه می‌کنند.

معاملات بانکی در شبکهٔ تاریک: از آنجا که محیط وب تاریک، برای ناشناس ماندن به‌وجود آمده است، برای انجام معامله‌ها و پرداخت‌ها نمی‌توان از حساب‌های بانکی واقعی و همچنین تبادل پول‌های معمولی استفاده کرد. به‌همین دلیل پول‌های مجازی به وجود آمده‌اند که در صدر آنها «بیت کوین» قرار دارد. این پول مجازی به‌گونه‌ای رمزگذاری شده است که قابل شناسایی و ردیابی نیست؛ از این‌رو، در فضاهایی نظیر شبکهٔ تاریک وب، بهترین گزینه برای پرداخت‌ها و خرید و فروش است. برای نمونه طبق مطالعات انجام شده، هر ساله بیش از ۱۰۰میلیون دلار در کشور امریکا برای انجام معامله‌های خرید و فروش مواد مخدر در وب تاریک تبادل می‌شود که همهٔ این پول در قالب «بیت کوین» مورد استفاده قرار می‌گیرد.

در وب تاریک، کاربران معمولاً از Hidden Wiki که وب‌گاه‌های اینترنتی را به صورت موضوعی دسته‌بندی می‌کند و مشابه ویکی پدیاست، استفاده می‌کنند. در این لایه از وب، افراد می‌توانند با راه‌های مختلفی با یکدیگر ارتباط برقرار کنند و به جست‌وجوهای گسترده‌تری در طول وب عمیق بپردازند.

دسترسی به آنچه که در لایه‌های پایین می‌گذرد زیاد ساده نیست؛ چرا که بیشتر ارتباط‌ها و خرید و فروش‌های اصلی توسط لینک ارتباطی امن بین طرفین برقرار می‌شود. ارتباطی که از نظرگاه همهٔ موتورهای جست‌وجوگر، فرسنگ‌ها فاصله دارد. اما وب‌گاه‌هایی هم هستند که عموم مردم آماج آنهاست. این وب‌گاه‌ها بر روی سرورهای Tor راه‌اندازی شده‌اند و از طریق مرورگرهای معمولی قابل دستیابی نیستند. root name این وب‌گاه‌ها اغلب onion است که در DNS های root ثبت نشده و فقط بر روی سرورهای Tor تعریف شده است. همچنین URL آنها، به‌سادگی به یاد سپردنی نیست و هرچند وقت یک‌بار به کل تغییر می‌کند. اغلب این وب‌گاه‌ها دارای صفحه‌های سیاه رنگی حاوی چند متن مختصر هستند.

وب‌گاه رسمی که آدرس وب‌گاه‌های ساخته شده را به نمایش می‌گذارد "https://onion.cab/list.php" است.

نرم‌افزارهای شبکهٔ تاریک

در حال حاضر Tor امن‌ترین سامانهٔ ارتباطی جهان و بهترین نرم‌افزار برای ناشناس ماندن در فضای مجازی است؛ به‌گونه‌ای که تاکنون هیچ سازمان و نهاد امنیتی قادر به شکافتن کدهای آن نبوده است.

نرم‌افزار Tor به دلیل «متن باز» بودن برای بیشتر سکوهای نرم‌افزاری رایانه‌های رومیزی و همراه طراحی شده‌است. در حال حاضر این نرم‌افزار بر روی همهٔ رایانه‌های رومیزی با سیستم عامل‌های «ویندوز»، «مک اواس ایکس» و «لینوکس» قابل اجرا است. در عین حال نسخه‌های «بتا» برای «اندروید» ایجاد شده است. همچنین تلاش‌هایی برای ایجاد بسته‌هایی برای آیفون اپل انجام می‌شود.

در سال ۲۰۱۳ مرورگر Tor ۱۵۰ میلیون بار دانلود شده است و در حال حاضر به ۲.۵میلیون کاربر در روز خدمات ارائه می‌دهد.

موارد استفاده وب تاریک توسط مجرمان و سازمان‌های اطلاعاتی در زیر آمده است:

- **پول‌های مجازی:** در وب تاریک، یکی از مهم‌ترین خدمات تحت وب قابل ارائه، تهیهٔ پول‌های دیجیتال مانند «بیت کوین» و «دارک کوین» برای انجام معامله‌های مجازی است. کسانی که در وب تاریک قصد انجام مبادله‌های پولی را دارند، می‌توانند با تهیهٔ پول‌های مجازی به خرید و فروش محصولات و خدمات موجود در این شبکه اقدام کنند[1]؛
- **میزبانی وب غیرقابل شناسایی:** در وب تاریک، شرکت‌هایی فعالیت می‌کنند که بدون شناسایی هویت واقعی کاربران در دنیای وب، سرورهایی برای ذخیرهٔ اطلاعات در اختیار آنها قرار می‌دهند. در چنین خدماتی که به کاربران خود ارائه می‌دهند، تعدادی از شرکت‌های ارائه دهندهٔ میزبانی وب در کشورهای اوکراین و روسیه بدون آنکه مشخصات فردی کاربر را دریافت کنند، فضاهایی را در وب به کاربران اجاره می‌دهند؛
- **فضاهای ابری مخفی:** شبکهٔ تاریک وب، فضاهای ابری مخفی را در اختیار کاربران مختلف و به‌ویژه نفوذگرها قرار می‌دهد تا این افراد بتوانند بدون شناسایی شدن، اطلاعات خود را در فضای اینترنت ذخیره کنند. این اطلاعات می‌تواند هر چیزی اعم از: اسناد و مدارک مهم سیاسی (مانند اسنادی که ادوارد اسنودن افشاگر برنامهٔ جاسوسی امریکا منتشر کرد) یا فایل‌ها و کدهای مخرب که نفوذگرها می‌سازند، باشد؛
- دسترسی به نرم‌افزارهای مخرب: یکی از بهترین مکان‌ها برای یافتن نرم‌افزارهای مخرب و جاسوسی، شبکهٔ تاریک وب است؛ برای نمونه در سال ۲۰۱۳ یک نفوذگر به کمک بسته‌های نرم‌افزاری که در وب تاریک وجود داشت، توانسته بود عملیات سایبری مخرب و بزرگی را به اجرا درآورد؛
- **استخدام نفوذگرها:** در شبکهٔ تاریک وب‌گاه‌هایی وجود دارند که می‌توان انجام فعالیت‌های سایبری مخرب را در ازای پرداخت مبلغی به نفوذگرها سپرد. این نفوذگرهای در حال فعالیت در این شبکه معمولاً افراد بسیار حرفه‌ای هستند؛

---

1. http://www.popsci.com/dark-web-revealed.

- **خرید و فروش مواد مخدر:** یکی از مهم‌ترین فعالیت‌های در حال انجام در شبکهٔ تاریک وب، خرید و فروش مواد مخدر است؛
- **پول‌های تقلبی:** یکی از آسان‌ترین راه‌ها برای دستیابی به پول‌های تقلبی استفاده از شبکهٔ تاریک وب است؛ در این شبکه، هر نوع پولی اعم از: یورو، دلار، پوند و... در دسترس است؛
- اسناد جعلی؛
- اسلحهٔ گرم و مهمات جنگی؛
- **جاسوسی:** یکی از مهم‌ترین فعالیت‌های سازمان‌های اطلاعاتی در شبکهٔ تاریک وب، ارتباط‌گیری با جاسوسان است.

تجزیه و تحلیل

پیشرفت فنّاوری، دسترسی غیرمحسوس و مؤثر سازمان‌های اطلاعاتی دشمن را به اطلاعات رایانه‌ها ممکن کرده است. این عبارت را بارها شنیده‌اید که اطلاعات شما بر روی وب امنیت ندارد و همهٔ اطلاعات شما در نهایت توسط خبرگان عرصهٔ اینترنت قابل روئیت خواهد بود. این گزاره‌ای است که کارشناسان امنیت فضای مجازی، به عموم مردم در استفاده‌های رایج از اینترنت نظیر: حضور در شبکه‌های مجازی و وب‌گاه‌های خبری یا تفریحی، وبلاگ‌ها و... هشدار می‌دهند. رشد قارچ گونهٔ جرایم در حوزهٔ فضای تولید و تبادل اطلاعات، مثل: کلاهبرداری اینترنتی، جعل داده‌ها و عنوان‌ها، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، رخنه و نفوذ به سامانه‌های رایانه‌ای و اینترنت، هرزنگاری و جاسوسی شبکه‌ای و از طرفی مأموریت سازمان‌های نظامی و انتظامی برای کشف و شناسایی این موارد، ایجاب می‌کند همهٔ کارکنان حفاظت اطلاعات‌ها، اشراف کامل به فضای مجازی و جرایم موجود در آن داشته باشند؛ لذا در این مقاله کارشناسان با بُعد جدیدی از دنیای نادیده اینترنت آشنا شدند و راه‌های شناسایی وب تاریک نیز بررسی شد.

نتیجه‌گیری و پیشنهاد

شبکهٔ تاریک وب یکی از گسترده‌ترین بخش‌های شبکهٔ وب به‌شمار می‌آید که رازهای پنهانی را در دل خود جای داده است. این مقاله سعی کرده است مرجعی برای آشنایی کاربران با این بخش از دنیای وب باشد؛ بنابراین به معرفی کامل وب تاریک، راه‌های دسترسی به آن و همچنین دسترسی به اطلاعات در این شبکه، فعالیت‌ها و خدمات قابل ارائه در آن و در نهایت راه‌های شناسایی آن پرداخته شده است. این دنیای بزرگ، گسترده‌تر از آن است که در حوصلهٔ این مقاله بگنجد، این شبکه به اندازه‌ای بزرگ است که هر بخش اشاره شده را می‌توان به‌صورت جداگانه در قالب پژوهشی جامع‌تر تهیه و گردآوری کرد.

با این توضیحات، لازم است همهٔ کارشناسان حوزهٔ امنیت با این موضوع آشنا شوند و در کارگاه‌های آموزشی نیز به‌صورت عملی به این موضوع‌ها پرداخته شود.

با توجه به اهمیت و نقش به‌سزای «وب عمیق» در امور جاسوسی و خرابکاری در فضای تولید و تبادل اطلاعات، موارد زیر پیشنهاد می‌شود که پیوسته باید مدنظر کاربران و مدیران و فرماندهان باشد:

- توجه به فرصت‌های موجود در وب عمیق از طریق دستگاه‌های نظارتی برای استفاده در راستای مبارزه و مقابله با گروه‌های تارشگری و مجرمان فضای مجازی و فعالیت سازمان‌های اطلاعاتی؛
- ایجاد تشکیلات سازمانی از طریق دستگاه‌های نظارتی برای رصد، بهره‌گیری و واپایش وب عمیق؛
- طراحی بدافزارهایی توسط دستگاه‌های نظارتی به‌منظور ایجاد اختلال در وب‌گاه‌های گروه‌های تارشگر و نفوذگر؛
- فراگیری دقیق آموزش‌ها، توجیهات، قوانین و مقررات مرتبط با وب عمیق برای کارشناسان دستگاه‌های نظارتی؛
- برگزاری کارگاه‌های آموزشی از طریق ساحفاها در خصوص وب عمیق برای کارشناسان واپایش امنیت؛
- جلوگیری از اقدام‌های مجرمانه با شناسایی فعالیت‌های غیرقانونی تبهکاران، مانند: خرید و فروش مواد مخدر، سلاح گرم، قتل و... در وب عمیق.

منابع و مآخذ

ارجمندی، اسماعیل (۱۳۹۳)، «سیر تطور رسانه‌های مجازی»، تهران: همایش آینده‌نگاری فناوری اطلاعات.

ابراهیمی، مهدی (۱۳۸۰)، «اینترنت»، تهران: نشر کتابدار.

اردلان، رضا (۱۳۸۲)، «بازیابی اطلاعات از طریق اینترنت»، مجموعه مقالات ششمین همایش کتابداران سازمان مدیریت و برنامه‌ریزی کشور، یزد ۱۸ـ۱۶ بهمن ۱۳۸۰، تهران: سازمان مدیریت و برنامه‌ریزی کشور.

پورمراد، مجید (۱۳۸۸)، «حفاظت فناوری اطلاعات»، تهران: نشر حدیث کوثر.

حاجی زین‌العابدینی، محسن (۱۳۸۱)، «بررسی مسائل فهرست‌نویسی منابع اینترنتی و ارائه دستنامهٔ پیشنهادی برای کتابخانه‌های ایران»، پایان‌نامه کارشناسی‌ارشد علوم کتابداری و اطلاع‌رسانی پزشکی دانشگاه علوم پزشکی ایران.

کوشا، کیوان (۱۳۸۱)، «ابزارهای کاوش در اینترنت: اصول، مهارت‌ها و امکانات جست‌وجو در وب»، تهران: نشر کتابدار.

کوشا، کیوان (۱۳۸۲)، «معیارهای ارزیابی موتورهای کاوش در اینترنت، رویکردی متن پژوهی برای ارائه سیاهه وارسی». اطلاع‌شناسی، شماره ۱۰۶.

منصوریان، یزدان (۱۳۸۲)، «اینترنت پنهان و منابع اطلاعاتی نهفته در اعماق نامرئی شبکه جهان‌گستر وب»، کتابداری و اطلاع‌رسانی آستان قدس رضوی.

منصوریان، یزدان (۱۳۸۲)، «نگاهی به جنبه‌های مختلف وب نامرئی، مرور پژوهش‌ها» ارائه شده در همایش وب سایت کتابخانه‌ها، تهران.

منصوری، مرتضی (۱۳۸۷)، «حفاظت اطلاعات کارشناسی ارشد رسته انتظامی»، دانشگاه علوم انتظامی امین.

نجفی، حسن (۱۳۹۲)، «ارزیابی امنیتی برنامه‌های کاربردی تحت وب»، تهران: نشر حدیث کوثر.

Anthony, s. "Anxicty and rumor. Journol of Social Psychology", 1993, PP91-8.

Ashbourn, A, "The rumor mill", In the Guardian. 2003, P.27.

Christopher J. Lamb, "Review of Psychological Operations: Lessons Learned from Recent Operational Experience", Washington D. C. National Defense University press, 2005, P.25.

D. Stuttard, M. Pinto, "The web application hackers handbook", Wiley, 2008.

Web Application Security Consortium, ” The Web Security Threat Classification", 2010.
http://www.theguardian.com/technology/silk-road-ross-ulbricht-sentenced 2015 /may/۲۹
http://www.nist.org
http://www.lexisnexis.com
www.whitehatsec.com
http://www.idsco.ir/Dark-web-Secret-network-for-Internet-criminals
https://freenetproject.org
https://getip.net/en
http:// cwe.mitre.org
https://en.wikipedia.org/wiki/Onion_routing
https://www.torproject.org
http://www.iflscience.com/technology/what-dark-web
http://www.popsci.com/dark-web-revealed
http://www.iflscience.com/technology/what-dark-web
https://nakedsecurity.sophos.com/fbi-again-thwarts-tor-to-unmask-visitors-to-a-dark-web-child-sex-abuse-site