بسم الله الرّحمن الرّحيم

دانشگاه صنعتی اصفهان

عنوان:

شبکه‌ی عمیق و شبکه‌ی تاریک

استاد راهنما:

دکتر محمدحسین منشئی

پژوهشگر:

جابر دانش‌آموز

تاریخ ارائه‌ی پروژه:

اردیبهشت 1396

فهرست عناوین

مقدمّه:

شبکه‌ی عمیق، به شبکه‌ایی است که به راحتی در دسترس عموم قرار نمی‌گیرد واز جستجوگرهای متداول بهره نمی‌برد. برای دسترسی به آن، از ابزارهای خاصی مانند TOR استفاده می‌شود. شبکه تاریک، بخشی از شبکه‌ی عمیق است که در قسمت عمیق‌تر آن قرار دارد. مجرمین، از این شبکه‌ی تایک، برای پنهان سازی هویتشان در فضای سایبری استفاده می‌کنند.

موضوع انتخاب شده به به این دلیل دارای اهمیّت است که بیش از 90 درصداز حجم اینترنت را شبکه‌ی عمیق تشکیل می‌دهد. این شبکه، بستر بیشتر جرایم و فعالیت‌های ضداخلاقی در فضای سایبری می‌باشد و به مشکل بزرگی برای مردم و دولت‌ها تبدیل شده‌است، اما کاربردهای مناسب بسایر زیادی نیز دارد.

این مقاله با چهار سرفصل کتاب در ارتباط مستقیم است:

- اخلاق برای کارکنان و کاربران فناوری اطلاعات(فصل 2)
- جرایم کامپیوتری و اینترنتی(فصل 3)
- حریم خصوصی(فصل 4)
- آزادی بیان(فصل 5)

به دلیل این که سومین مرجع ارائه شده در پروپوزال[1]، که در بانک اطلاعاتی اسکوپوس[2] یافت شده بود، قابلیت دسترسی به آن وجود نداشت، و می‌بایست آن را از راههای غیراخلاقی تهیه می‌کردم، از این کار صرف نظر کرده و از دیگر منابع، استفاده شده‌است.

[1] Proposal
[2] Scopus

تاریخچه شبکه‌ی عمیق:

بنا بر عقیده‌ی بسیاری، شبکه عمیق از همان اوایل که سرویس HTTP وارد کار شد، به گونه‌ای وجود داشت، اما از وقتی شهرت عمومی پیدا کرد که مدیر وراه‌انداز شبکه فروشگاهیِ جاده ابریشم، Ross Ulbricht، توسط FBI، شناسایی و در سال 2013، به همراه چندین تن از دیگر همکاران خود، دستگیر شدند [1] [2].

درسال 1995، یک دانشجوی ایرلندی به نام ایِین کلارک[3]، با ویژگی‌های برجسته‌ای مانند هوش و استعداد بالا، برای تحصیل در زمینه‌ی هوش مصنوعی و علوم کامپیوتر، وارد دانشگاه ادینبرگ[4] شد. او برای پروژه‌ی پایان‌نامه خود، یک حافظه و سیستم بازیابی غیرمتمرکز و گسترده[5] ایجاد کرد. به طور غیردقیق و غیرعلمی‌تر، می‌توان گفت که او یک راه جدید انقلابی برای مردم ایجاد کرد تا بتوانند بدون این که هویتشان تشخیص داده شود، از اینترنت استفاده کنند[3] .

بنابر گفته کلارک، از همان ابتدا خیلی واضح به‌نظر می‌آمد که شبکه(اینترنت)، قرار بود در ضمینه ارتباطات و آزادی چگونه باشد، اما در اواخر دهه‌ی 90 میلادی، این موضوع، مسئله‌ی مهمی به شمار نمی‌آمد. بنابرگفته‌ی او، پیش بینی می‌شد که اینترنت می‌تواند بسیار سریع‌تر و در دسترس‌تر، مفهومی‌تر، و ارزان‌تر از روش‌های ارتباطی قدیمی و از مد افتاده مانند نامه و تلفن باشد. با وجود تمام اون مسائل، پروژه‌ی او نمره B گرفت زیرا اساتید اعتقاد داشتند که او در پروژه‌اش، به اندازه‌ی کافی به کارهای دیگران ارجاع[6] نداده است[3] .

او نرم‌افزار خود را به صورت رایگان در اختیار دیگران گذاشت که با استفاده از آن، هر شخصی می‌توانست بدون این که هویتش شناسایی شود_با ضریب اطمینان بالا_، به صورت آنلاین گفتگو کند، صفحه وب راه‌اندازی یا بازدید کند و فایل به اشتراک بگذارد[3] .

کلارک، نرم‌افزار خود را در سال 2000 به صورت عمومی و برای همگان منتشر کرد که امروزه آن را با نام Freenet می‌شناسند. او در سال 2009 ادعا کرد که بیش از دو میلیون نسخه از این نرم‌افزار توسط کاربران استفاده می‌شود که عمده‌ی آن در اروپا و آمریکاست. وب سایت او که این نرم‌افزار را در اختیار عموم قرار می‌دهد، در کشورهای استبدادی مانند چین بلاک شده‌است. در این کشورها، مردم این نرم‌افزار را روش‌های دیگر مانند گرفتن از دوستان یا سایر سایت‌ها تهیه می‌کنند. کلارک با ارتقاء نرم‌افزار خود توانست جلوی تشخیص افرادی که این نرم‌افزار را نصب کرده‌اند و از آن استفاده می‌کنند را نیز بگیرد[3] .

---

[3] Ian Clarke
[4] Edinburgh
[5] Decentralized
[6] Citation

معرفی اجمالی شبکه‌های سطحی، عمیق و تاریک:

وب سطحی:

وب سطحی[7] عموماً به تمام سایت‌ها و محتواهایی گفته میشود که می‌توانند توسط یکی از موتورهای جستجوی متداول مانند گوگل، یاهو، بینگ و ... فهرست بندی[8] شوند. موتورهای جستجوی متداول مانند گوگل، برای پیدا کردن لینک و تشخیص محتوای سایت‌ها و صفحات وب[9]، به صفحاتی که شامل این لینک‌ها هستند متکی می‌باشند. این تکنیک، یک روش بسیار مناسب برای جستجو و پیدا کردن محتوای جدید در شبکه اینترنت می‌باشد، اما بسیاری از محتواها و سایت‌ها توسط این تکنیک نادیده گرفته شده و دسترسی به آنها از این روش غیر ممکن میباشد[4] .

شبکه‌ی عمیق:

بر خلاف عقیده عموم که فکر می‌کنند بسیاری از اطلاعات موجود در اینترنت، توسط موتورهای جستجوی متداول مانند گوگل، شناسایی و فهرست بندی می‌شوند، بخش عظیمی از دنیای آنلاین خارج از دسترس این موتورهای جستجو میباشد. به این بخش عظیم، شبکه عمیق[10] گفته می‌شود. در واقع، به طور کلی می‌توان گفت که به هر محتوای اینترنتی که توسط موتورهای جستجوگر متداول، فهرست بندی نمی‌شود، شبکه عمیق گفته می‌شود[2] .

شبکه‌ی تاریک:

شبکه‌ی تارک[11]، به عنوان بخش کوچکی از شبکه عمیق طبقه‌بندی می‌شود که به صورت عامدانه، طوری طراحی شده است که ضمن مخفی بودن، توسط تمامی موتورهای جستجوی استاندارد، غیر قابل دسترسی باشد[4]. در اصطلاح، به بخش عمیق‌تر شبکه عمیق، شبکه تاریک گفته می‌شود که برخلاف شبکه عمیق، بیشتر برای فعالیت های مجرمانه از آن استفاده می‌شود و از ابتدا نیز برای همین کار طراحی شده بود، اما کاربردهای مناسب نیز دارد[1] .

بنا برتعریفی دیگر، شبکه‌ی تاریک، به مجموعه‌ی شبکه‌ها و صفحاتی گفته می‌شودکه در یک شبکه‌ی بزرگترِ رمزنگاری شده وجود دارند و در این شبکه، برای پنهان کردن هویت افراد و سایت‌ها، از ابزار رمزنگاری TOR[12] استفاده

---

[7] Surface web
[8] Index
[9] Web page
[10] Deep web
[11] Dark net
[12] The onion router

می‌شود و در واقع، این شبکه، در زیرِ شبکه‌ای با دسترسی محدود قرار دارد که برای استفاده از آن باید از ابزارها و روش‌های خاص مانند TOR و I2P[13] و Freenet استفاده کرد[1] [5] .

از شبکه‌ی تاریک، با عناوینی چون: وب تاریک[14]، وب نامرئی[15]، فضای آدرس تاریک[16]، فضای آدرس تیره[17] و فضای آدرس کثیف[18] نیز یاد میشود. اما همه‌ی این‌ها معنی یکسان و درستی از شبکه‌ی تاریک را نمی‌رسانند. به عنوان مثال، فضای آدرس تاریک، عموماً به آدرس‌های اینترنتی گفته می‌شود که به دلیل ضعف تکنیکی، از ادامه‌ی کار بازمانده‌اند. هم-چنین می‌دانیم شبکه‌ی تاریک استفاده‌های مفید زیادی دارد و مانند بسیاری از ابزار دیگر، می‌تواند به عنوان ابزاری برای انجام اعمال نادرست نیز مورد اسفاده قرار گیرد[3] .

همانطور که می‌بینید، تعاریف شبکه‌ی عمیق و تاریک، بسیار شبیه یکدیگرند و بسیاری از اوقات، نام شبکه‌ی عمیق و شبکه‌ی تاریک، به اشتباه به جای یکدیگر استفاده میشوند که در ادامه راجع به آن صحبت خواهیم کرد.

محتویات و کاربردهای شبکه‌ی عمیق و حجم آن :

محتویات شبکه‌ی عمیق:

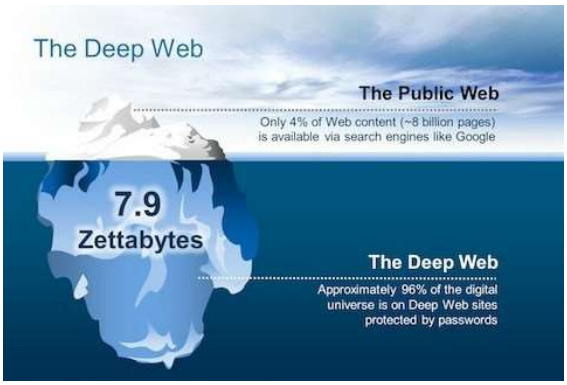
شبکه تاریک، فقط بخش کوچکی از شبکه‌ی عمیق است . تمام صفحات وب پویا[19]، سایت های بلاک شده، سایت-های لینک نشده، شبکه‌ها و سایت‌های خصوصی با دسترسی محدود(نیاز به ثبت نام و login دارند)، محتواهای غیر HTML و اسکریپت[20] نشده، پایگاه‌های داده‌ی دولتی و شخصی، کتابخانه‌های آنلاین، سایت‌های حاوی مقالات غیرقابل دسترس برای عموم، صفحات پنهان در ورای سایت‌های پرداخت، بیت های محافظت شده‌ی اطلاعات بانکی هنگام استفاده از حساب‌های بانکی برخط[21]، web mail ها ماند Gmail، اینترانت_انترنت داخلی که آن هم توسط موتورهای جستجوی متداول قابل دسترسی نیست_ همگی جزئی شبکه‌ی عمیق به حساب می‌آیند[5] [2] [1] .

حجم شبکه‌ی عمیق:

بنابر عقیده کارشناسان، به ازای هر صفحه وب موجود در شبکه سطحی، یک یا چند صفحه در شبکه عمیق وجود دارد[3]. بر اساس ارزیابی‌های انجام شده و گمانه‌زنی‌ها، تعداد سایت‌ها و صفحات موجود در شبکه‌ی تاریک، 400 الی 500

---

[13] Invisible Internet project
[14] Dark web
[15] Invisible web
[16] Dark address space
[17] Murky address space
[18] Dirty address space
[19] Dynamic web page
[20] Script
[21] Online



برابر شبکه‌ی سطحی می‌باشد. همچنین، گفته می‌شود بیش از 90 درصد از محتوای اینترنت، در شبکه‌ی عمیق قرار دارد. بسیاری، این اندازه شبکه عمیق و شبکه‌ی سطحی را به کوه یخ تشبیه می‌کنند که بخش عظیمی از آن در زیر آب قرار دارد و خارج از دید ما می‌باشد و فقط بخش کوچکی از آن روی آب بوده و در معرض دید ما قرار دارد[1] .

کابران شبکه‌ی عمیق و شبکه‌ی تاریک:

شبکه‌ی تاریک به گونه‌ای طراحی شده است که پنهان ماندن هویت را برای کاربران خود فراهم می‌کند. البته رعایت نکردن برخی مسائل می‌تواند باعث شناسایی هویت شما شود که در بخش‌های بعدی راجع به این موضوع و راه‌کار های آن و این که این شبکه چگونه طراحی شده تا این امر را امکان‌پذیر سازد،صحبت خواهیم کرد.

از جمله کاربران اصلی این شبکه، می‌توان روزنامه‌نگاران، سیاست‌مداران، فعالان حقوق بشر، دانشمندان_عموماً برای نگهداری داده‌های خام و نتایج تحقیقات و آزمایشات_، جنایتکاران و افراد خلاف‌کار، قاچاقچیان و فروشندگان مواد مخدر، خریداران مواد مخدر، فروشندگان اسلحه، خریداران اسلحه، هکرها، تروریست‌ها، قماربازها، جویندگان و سازندگان پورنوگرافی، کلاه‌برداران کارت‌های اعتباری، افرادی که میخواهند ارتباطات و مکالمات و مکاتباتشان از دید دولت‌ها مخفی بماند، فروشندگان و خریداران اسناد تقلبی و ... را نام برد که به پنهان ماندن هویت و اطلاعات شخصی و کاری در شبکه اینترنت نیاز دارند[6] [2] .

اغراق در مورد شبکه‌ی عمیق:

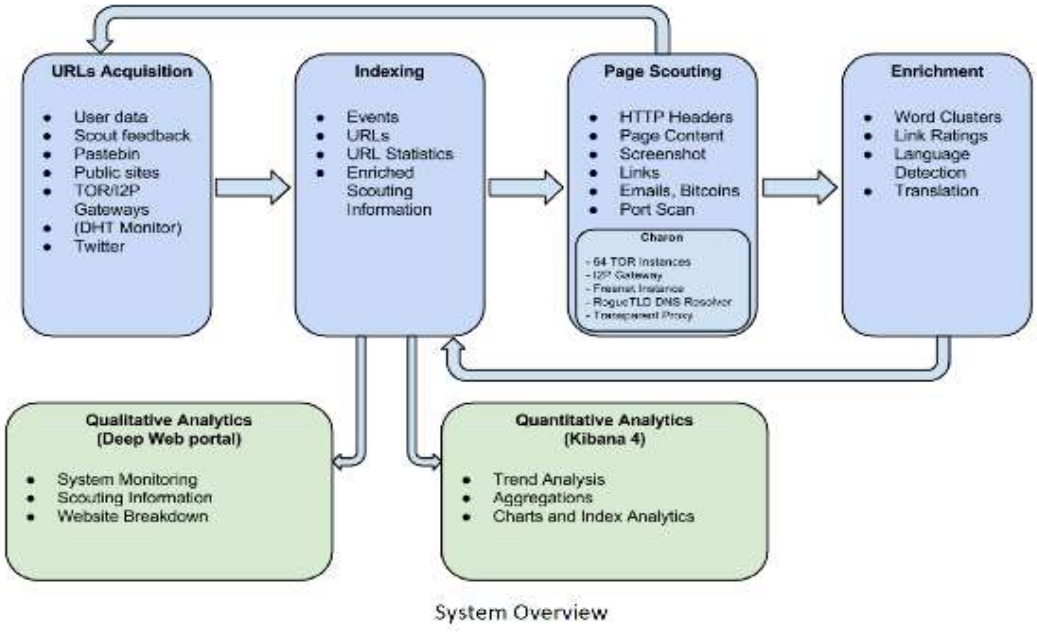
غالباً، روزنامه‌ها و اخبار، مطالب اغراق‌آمیزی در مورد شبکه‌ی پنهان ذکر می‌کنند. بسیاری از آن‌ها نیز نام شبکه‌ی تاریک و شبکه‌ی پنهان را به اشتباه به جای یکدیگر استفاده میکنند. داستان‌های خطرناک و مخوفی که این رسانه‌ها در مورد این که این شبکه 90 درصد حجم اینترنت را تشکیل می‌دهد، با شنیدن این که چه محتواهایی جزو شبکه‌ی عمیق حساب

می‌شوند_مانند انترانت و پایگاه‌های داده و ایمیل و ..._ کمی مسخره به نظر می‌آیند[5] . شبکه‌ی تاریک که بیشتر تخلفات در آن‌جا رخ می‌دهد، به صورت خوشبینانه، 0/01 درصد از محتوای اینترنت را به خود اختصاص میدهد[7] .

آمار کاربران و محتوای شبکه‌ی عمیق:

پی بردن به این که چه افرادی با چه ملیتی و چه زبانی و به چه میزان از شبکه عمیق استفاده می‌کنند، به دلیل سطح ناشناخته ماندن هویت که این سرویس ارئه می‌دهد، بسیار دشوار است. تنها با بررسی محتوای سایت‌های این شبکه، می‌توان دیدی نسبی به این قضیه پیدا کرد. در ادامه نمودار های ارزیابی‌های مجله Trend Micro که حاصل نتایج سیستمی است که برای این منظور طراحی کرده‌است، ارائه می‌شود. این سیستم URL[22] هایی که به آن لینک شده‌اند، شامل TOR، سایت‌های مخفی I2P، Freenet، و دامنه‌هایی که TLD[23] غیر استاندارد دارند را مورد کاوش و بررسی قرار می‌دهد[2] .

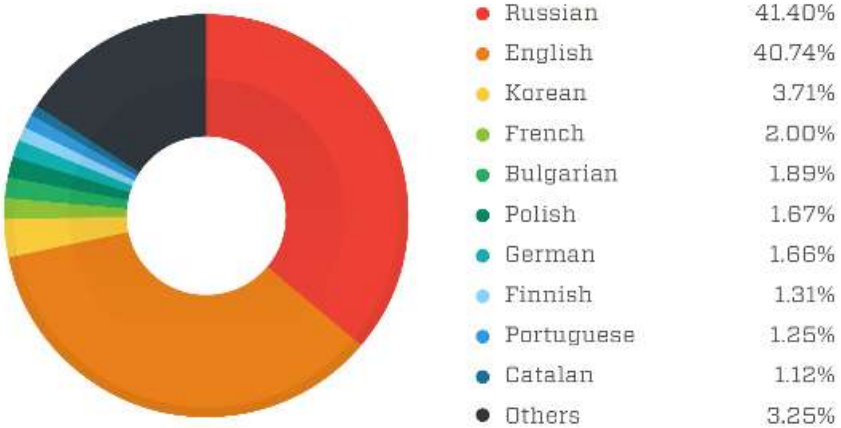
[22] Uniform resource locator
[23] Top level domain



شمای الگوریتم ارزیابی شبکه‌ی عمیق

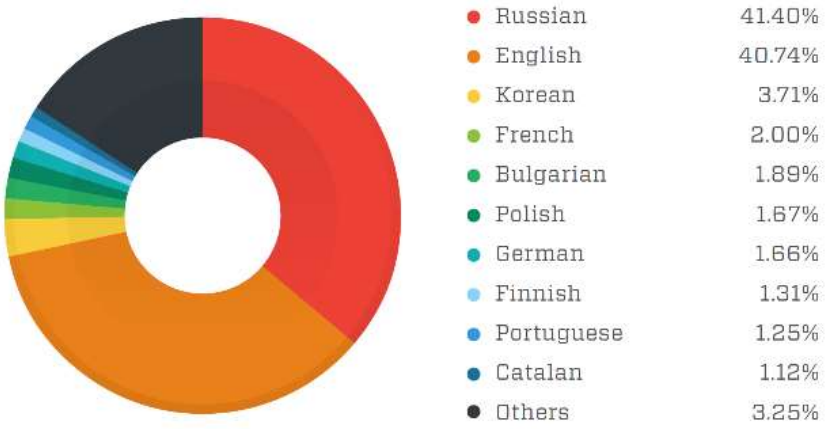
ارزیابی بر اساس زبان:

از لحاظ تعداد دامنه‌ها، زبان انگلیسی بیش از 2154 سایت از 3454 سایت که به صورت موفقیت‌آمیز مورد جاسوسی و ارزیابی قرار گرفته‌اند را به خود اختصاص می‌دهد که با توجه به این که زبان انگلیسی، زبان بین‌المللی می‌باشد، تعجب برانگیز نیست. بعد از زبان انگلیسی، زبان روسی و فرانسوی بیشترین آمار را به خود اختصاص می‌دهند[2] .



Most popular languages based on the number of URLs with content using them

با بررسی تعداد زبان بر اساس تعداد URL ها، روسیه از انگلیس پیشی می‌گیرد. در حال حاضر، تعداد بسیار زیادی تالار گفتگوی[۲۴] روسی در TOR و I2P وجود دارند که به صورت مستقیم نیز به فعالیت‌های بدخواهانه ربطی ندارند که در این ارزیابی، آن‌ها نیز در نظر گرفته‌شده‌اند[2] .



Most popular languages based on the number of URLs with content using them

ازیابی بر اساس معاملات:

آنالیز 15 فروشنده‌ی بزرگ در شبکه‌ی عمیق نشان می‌دهد که مواد مخدر سبک_مانند مارجوانا_بیشترین اقلام مبادله شده در شبکه‌ی عمیق می‌باشند. بعد از آن، اقلام دارویی مثل ریتالین و مواد مخدر سنگین_مانند کراک_ در رده‌های بعدی قرار می‌گیرند[2] .

[24] Forum

Cannabis	27.28%
Pharmaceuticals	22.39%
MDMA	14.43%
LSD	7.47%
Meth	3.93%
Mushrooms	3.41%
Heroin	3.31%
Seeds	3.92%
Video games	6.93%
Accounts	6.93%

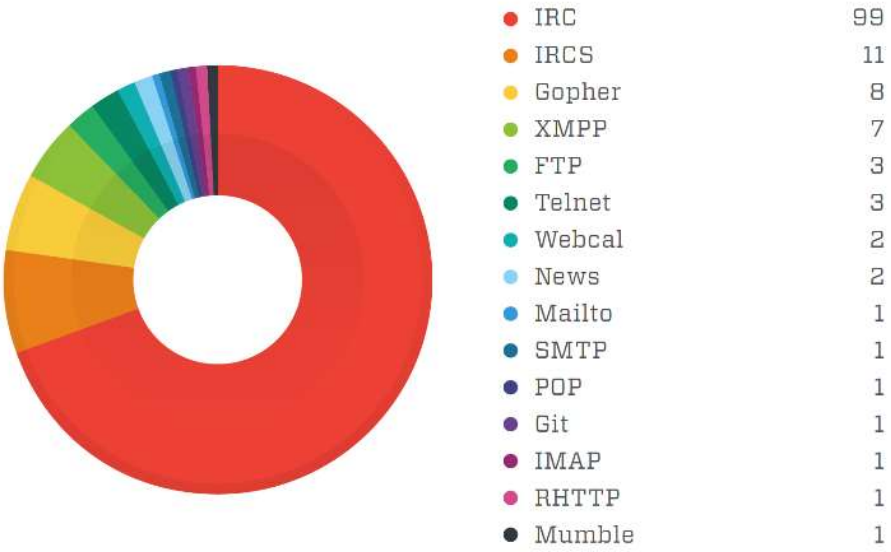
Buyer breakdown based on data pulled on 3 June 2015

Cannabis	31.60%
Pharmaceuticals	21.05%
MDMA	10.53%
LSD	5.26%
Meth	5.26%
Mushrooms	5.26%
Heroin	5.26%
Seeds	5.26%
Video games	5.26%
Accounts	5.26%

Vendor breakdown based on data pulled on 3 June 2015

ارزیابی بر اساس پروتکل‌های مورد استفاده:

بر اساس تحقیقات انجام شده، می‌توان URL ها را بر اساس شمای آن‌ها_HTTP,[26]FTP,HTTPS[۲۵] و ..._ دسته‌بندی کرد. بنابر نتایج این تحقیقات، بیش از 22000 دامنه یا از HTTP و یا از HTTPS استفاده می‌کنند. اگر این دو پروتکل را کنار بگذاریم، به آمار و ارقام زیر در مورد سایر پروتکل‌ها[۲۷] می‌رسیم. به‌طور معمول، سرورهای گفتگویی[۲۸] که به عنوان پاتوق برای عاملان کارهای بدخواهانه، صرف انجام ملاقات و مبادله‌ی کالاها یا ایجاد شبکه ارتباطی برای botnet تشکیل می‌شودند، از IRC[29] و IRCS[30] استفاده میکنند[2] .



Protocols found in the Deep Web apart from HTTP/HTTPS

[25] Hypertext transfer protocol
[26] File transfer protocol
[27] Protocol
[28] Chat
[29] Internet relay chat
[30] Internet relay chat safe

محتویات نامناسب و کاربردهای غیراخلاقیِ شبکه‌ی عمیق و تاریک:

محتویات نامناسب و غیر اخلاقی زیادی در شبکه‌ی تاریک و عمیق وجود دارند که در این‌جا، فقط به بررسی اجمالی مهم‌ترین آن‌ها می‌پردازیم.

البتّه، بنابر گفته‌ی پلیس مبارزه با جرایم اینترنتی آمریکا، بسیاری از فعالیّت‌های مجرمانه، نه در شبکه‌ی پنهان، بلکه در تالارهای گفتگوی غیرمخفی هستند. شما فقط باید بدانید که کجا دنبال آن‌ها بگردید. مردم، ممکن است پس از کلیک بر روی لینک مورد نظر در تالار گفتگو، به یک صفحه‌ی نامربوط حاوی عکس گل‌ها هدایت شده، سپس با کلیک بر روی هجدهمین گل، و پس از انجام چندیدن مرحله‌ی مشابه، به سایت مورد نظر هدایت شوند[3] .

تجارت بدافزارها:

بنابر دلایل مختلف، می‌توان گفت که شبکه‌ی عمیق و بدافزارها، کاملاً مناسب یکدیگرند، خصوصا زمانی که بحث میزبانیِ زیر ساخت دستور و کنترل[۳۱] پیش می‌آید. طبیعت سیستم‌های پنهان مانند TOR این است که مکان سرور را با استفاده از رمزنگاری‌های پیچیده، مخفی نگه‌می‌دارد. این دو مسئله، بسیاری از شرایط را برای حملات سایبری و بدافزارها فراهم می‌کند[1] .

بدافزار VAWTRAK، یک تروجان بانکی است که به وسیله‌ی ایمیل‌های phishing، منتشر شد. هر نمونه از آن، با لیستی از C&C سرورها ارتباط برقرار میکرد. IP[32] این سرورها، به وسیله دانلود یک فایل آیکون رمزنگاری شده از برخی سایت‌های TOR به دست می‌آمد. این بدافزار، با استفاده از برتری ناشناخته ماندن سرور کار خود را انجام می‌داد [2].

یکی از بدافزارهای مهم و اصلی دیگر که از شبکه پنهان بهره می‌برد، باج‌افزار Crypto Locker است. این باج‌افزار، اسناد شخصی قربانیان را قبل از این که آن‌ها را به سایت خود، برای پرداخت هزینه به منظور به‌دست آوردن دوباره‌ی اطلاعاتشان هدایت کند، رمزنگاری می‌کند. این باج‌افزار به اندازه‌ی کافی هوشمند می‌باشد که می‌تواند سایت پذیرنده برای دریافت باج را متناسب با زبان ملی فرد قربانی تنظیم کند [2].

مواد مخدر:

بنابر آمارهای گزارش شده که در قسمت‌های قبل نشان داده‌شده، مواد مخدر اصلی ترین کالای مبادله شده در شبکه‌ی تاریک می‌باشد. از بزرگ‌ترین فروشندگان مواد مخدر، می‌توان فروشگاه جاده ابریشم را نام برد که پیش‌تر راجع به آن توضیحاتی داده شد.

---

[31] Command and control(C&C)
[32] Internet protocol

علاوه بر فروشگاه‌ها و تالارهای گفتگوی[۳۳] اختصاص یافته به مواد مخدر، سایت مشهور Grams و بسیاری از سایت‌های دیگر مانند Hiddenwiki، این امکان را به مردم می‌دهند تا مواد مخدر خود را به سادگی جستجو کرده و سایت-های فروش مواد مواد مخدر را برای آن‌ها فهرست بندی می‌کنند. سایت Grams، با داشت لوگوی شبیه به لوگوی گوگل، این موضوع را تداعی می‌کندکه بسیار شبیه گوگل عمل کرده، منتها برای دسترسی به محتواهای این چنینی طراحی شده‌است [2].

بیت کوین:

برای انجام مبادلات غیرقانونی در شبکه‌ی تاریک و عمیق، شدیداً به این مسئله نیازمندیم که کسی نتواند در هنگام مبادله‌ی پول، هویت پرداخت کننده و دریافت کننده را تشخیص دهد. به این منظور، واحد پول الکترونیکی بیت‌کوین[۳۴] ایجاد شده است. مانند سایر موارد قبل، فقط به معرفی اجمالی این موضوع می‌پردازیم.

سرویس پول‌شویی بیت‌کوین، به ناشناخته مانند هویت هنگام مبادله‌ی پول از طریق این سیستم بیت‌کوین، کمک می‌کند. در نهایت، استفاده‌کنندگان از بیت‌کوین، نیاز دارند که پول نقد خود را به بیت‌کوین تبدیل کرده و برعکس. سایت-های بسیاری هستند که این کار را برای شما انجام می‌دهند. سایت‌هایی مانند WeBuyBitcoins ، تبدیل پول واقعی به بیت‌کوین هم‌چنین تبدیل بیت‌کویت به پول واقعی را انجام می‌دهند. میزان مبادلات این سایت‌ها با سایت‌های مشابه در وب-سطحی قابل مقایسه است [2].

تعداد قابل توجهی از فروشندگان در شبکه‌ی تاریک، کلاه‌بردار بوده و در قبال دریافت بیت‌کوین، محصول یا خدمت مورد نظر را در اختیار شما نمی‌گذارند و شما نیز نمی‌توانید بابت این موضوع، از آن‌ها شکایت شکایت کنید [4] [5].

فروش حساب‌های بانکی مسروقه و اسناد تقلبی و مسروقه:

خرید و فروش حساب‌های بانکی مسروقه:

این موضوع، فقط مربوط به شبکه‌ی تاریک و عمیق نیست، بلکه در بسیاری از تالارهای گفتگو در شبکه‌ی سطحی نیز این کار انجام می‌شود. این حساب‌ها به طور کلی بنابر دو روش به فروش می‌روند. روش اول، حساب‌هایی هستند که با درصد کیفیت بالایی، راستی‌آزمایی شده‌اند و مقدار دقیق موجودی آن‌ها معلوم است و قیمت بالاتری نسبت به نوع دوم دارند. دسته‌ی دوم، حساب‌های حجمی هستند که در آن‌ها، چندین حساب راستی‌آزمایی نشده وجود دارند، اما معمولاً این تضمین را می‌دهند که درصد خاصی از آن‌ها، معتبر هستند. هم‌چنین، در شبکه‌ی عمیق، کارت‌های اعتباری فیزیکی نیز به فروش می‌رسند [2].

---

[33] Forum
[34] Bitcoin

اسناد تقلبی و مسروقه:

پاسپورت‌ها و شناسنامه‌ها به دلیل این که اسناد معتبری و یکتایی هستند، اهمیّت و ارزش زیادی دارند. آن‌ها، اسنادی هستند که برای عبور از مرزها، بازکردن حساب بانکی، گرفتن وام بانکی، خرید املاک، اقامت در کشورها و بسیاری از کارهای دیگر مورد نیاز هستند. سایت‌های اندکی در شبکه‌ی تاریک هستند که اقدام به فروش این اقلام می‌کنند و قیمت آن‌ها، بسته به فروشنده و کشور و ... متفاوت است [2].

اطّلاعات فاش شده افراد:

در آگوست 2015، بسیاری ار روزنامه‌ها گزارش دادند که 10GB اطلاعات از سایت Ashley Madison به سرقت رفته‌است. این سایت کانادایی، برای فراهم کردن زمینه خیانت و آشنا کردن زن و مردهای متعهّل با یکدیگر طراحی شده بود. هکرها، با دزدیدن اطلاعت کاربران، تهدید کردند که در صورتی که سایت، فعالیت خود را متوقف نکند، این اطّلاعات را بر روی شبکه سطحی منتشر خواهندکرد. پس از این که سایت به درخواست آن‌ها عمل کرد، هکرها برای کاربران این شبکه ایمیل‌های سیاهی فرستادند که از آن‌ها درخواست 2500 دلار پول بیت‌کوین، برای فاش نکردن اطّلاعاتشان کردند [5].

این امر که هکرها، افراد خاص مانند افراد مشهور و سیاست‌مداران و بازیگران هالیوود و ... را مورد هدف برای سرقت اطلاعات شخصی قرار دهند، موضوعی رایج است. در بسیاری از موارد، تشخیص درست یا غلط بودن این اطلاعات، کاری دشوار است. این اطّلاعات، معمولاً شامل شماره ملی، تاریخ تولّد، ایمیل شخصی، آدرس فیزیکی و شماره تلفن می‌باشند. تعدادی از افرادی که اطّلاعات آن‌ها به سرقت رفته است [2]:

- چند مأمور FBI
- اشخاص سیاسی مانند باراک و میشائیل اوباما، بیل و هیلاری کلینتون، سناتور سارا پِلین و قاضی کاترین رولان فارست
- افراد مشهور مانند بیل گیتس، آنجلینا جولی، بیانسه، تام کروز و دنیس رادمن

محتویّات مناسب و کاربردهای خوب شبکه‌ی عمیق و تاریک:

مطالب بسیاری در این مورد وجود دارد که برای خارج نشدن از کلیّت موضوع و طولانی نشدن مطلب، از آوردن تمامی آن‌ها خودداری کرده و صرفا به ذکر برخی از آن‌ها اکتفا می‌کنیم.

آزادی بیان:

شبکه‌ی تاریک، این امکان را به افراد می‌دهد تا بدون سانسور و بدون ترس از شکنجه و مجازات غیرقانونی، آزادی بیان داشته باشند. بنابر گزارش Tor Project، ناشناخته ماندن در سرویس‌های پنهان، پناه‌گاهی برای معترضان سیاسی در کشورهایی نظی لبنان و موریتانی و کشورهای بهار عربی بوده‌است. این شبکه، میزبان وبلاگ‌های ابراز عقیده و تبادل ایده‌ها درکشورهایی بوده‌است که در آن‌ها ابراز عقاید موردغضب واقع می‌شود. و همچنین، سایت‌هایی مانند Global leaks، Indymedia و WikiLeaks که موجب جلب توجه دولت‌ها و نگرانی عمومی شده‌اند، بازتابی از سایت‌های موجود در همین شبکه است [6].

در استفاده سودمند از Freenet، می‌توان به این نکته اشاره کرد که این برنامه، در جواب به درخواست[35] شما برای جستجوی مطالب مفید، صدهای سایت آزادی‌خواه و سایت‌های مربوط به اخبار داخلی کشورهایی مانند ایران و کره‌شمالی و بسیاری سایت‌های مفید دیگر را فهرست می‌کند [3].

:Whistleblowing

در شبکه تاریک، معترضان در بهار عربی می‌توانستند ردپای دیجیتال خود رو مخفی کرده و امنیت خود را حفظ کنند. در این شبکه، اخبار مربوط به خطرهای امنیتی سایبری جدید منتشر می‌شود. هم‌چنین، whistleblower ها می‌توانند بدون اینکه هویتشان فاش شده و در معرض خطر قرار گیرند، اطلاعات خود را فاش کنند [6].

از بارزترین نمونه‌های whistleblowing در سال‌های اخیر، می‌توان افشاگری‌های ادوارد اسنودن[36] و جولیان آسانژ[37] و چلسی منینگ[38] را نام برد که به صورت عمده، به شبکه‌ی تاریک متکی بودند. هر سه این افراد، از TOR برای اشتراک‌گذاری فایل‌های طبقه‌بندی شده‌ی با ارزش دولت آمریکا استفاده کردند، قبل از این که بخواهند آن‌ها را به صورت آنلاین منتشر کنند [1].

---

[35] Request
[36] Edward Snowden
[37] Julian Assange
[38] Chelsea Manning

ارتباط پیامی امن، ابزار انتقال فایل امن، جلسات سیاسی فوری و تالارهای گفتگوی امن، از دیگر کاربردهای مثبت این شبکه می‌باشند که البته می‌توانند برای انجام کارهای نادرست نیز استفاده شوند [6].

حریم خصوصی:

بسیاری از مردم، برای جلوگیری از فاش شدن هویتشان حتّی در انجام وب‌گردی‌های روزانه و خریدهای معمولی اینترنتی، از این شبکه استفاده می‌کنند تا به نحوی مانع نقض حریم خصوصی خود شوند. بسیاری از سیاستمداران و افراد مشهور نیز که به شدت در معرض نقض شدن حریم خصوصی قرار دارند، از استفاده کنندگان شبکه‌ی تاریک هستند.

داده‌های محرمانه و شخصی:

سازمان‌های دولتی و گاهاً نظامی و همچنین بانک‌ها، کتابخانه‌ها و پژوهش‌کده ها و آزمایشگاه‌ها، برای جلوگیری از فاش شدن اطاعات خود و کاربرانشان از این شبکه برای ذخیره و بازیابی اطلاعات خود استفاده می‌کنند. بسیاری از دانشمندان نیز داده‌های خام خود رو در این شبکه نگه‌داری می‌کنند.

ابزارهای استفاده از شبکه‌ی عمیق و تاریک:

نحوه‌ی کار شبکه‌ی عمیق و تاریک:

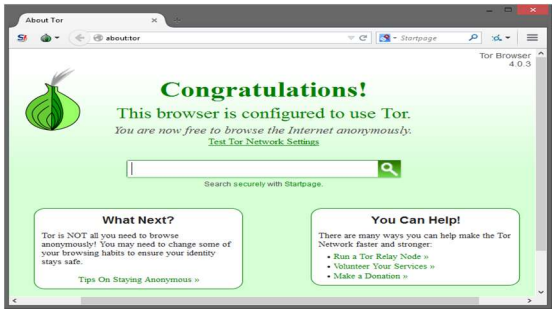
شبکه‌ی عمیق و تاریک، حاوی سایت‌هایی هستند که در سرچشمه‌های DNS سرورها ثبت شده‌اند، اماتوسط ICNANN مدیریّت نمی‌شوند. بنابراین از ویژگی‌های URL به همراه TLD های غیراستاندارد، بهره می‌برند. برای مثال، سرویس بیت‌کوین، از دامنه‌ی bit. استفاده می‌کند. این شبکه، با استفاده از طبیعت DNS های جایگزین شونده و غیرمتمرکز، کار ردیابی و از بین بردن این دامنه‌ها را بسیار سخت می‌کند[1]. شانس پیدا کردن و دسترسی به این شبکه‌ها به صورت اتفاقی

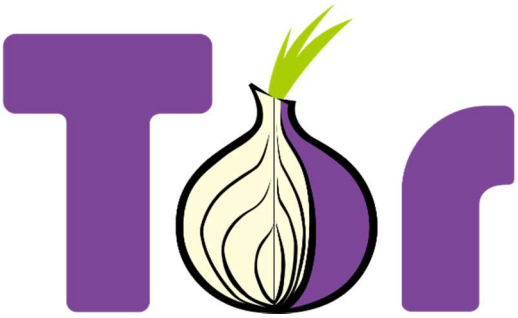
توسط افرد عادی، تقریباً صفر است. فقط افرادی که از وجود این شبکه‌ها با خبر بوده و عامدانه و با ابزار خاص، به سراغ آن‌ها می‌روند، می‌توانند دسترسی پیدا کنند [6].

TOR:

این پروژه که توسط نیرویی دریای وزارت دفاع آمریکا راه‌اندازی شده‌است، یک برنامه‌ی بدون سود است و به همین دلیل، به طور مداوم توسط ارتقاء دهندگان داوطلب، پیشرفت داده می‌شود. بودجه‌ی اصلی این برنامه، توسط دولت آمریکا و بیاد ملّی علوم آمریکا تأمین می‌شود. در حال حاضر، معروف‌ترین و گسترده‌ترین ابزار استفاده از شبکه‌ی عمیق، برنامه TOR می‌باشد. این برنمه در سال 2002 معرفی شد [8] [9].

TOR، سرواژه عبارت مسیریاب پیازی[39] می‌باشد. صفحه‌ی خانه‌ی[40] TOR، Onionland نام دارد. Onionland، به وسیله‌ی سرویس‌های مخفی و ناپدیدشدن‌های ناگهانی، مدام تغییر مکان می‌دهد. علاوه بر این، بسیاری از فهرست‌های راهنما[41] نیز مدام URL خود را تغییر داده و شما باید برای پیدا کردن آن‌ها، از Onionland یا Reddit استفاده کنید. بسیاری از URL ها و فهرست‌های راهنمای موجود در Onionland، اکنون وجود ندارند [6].





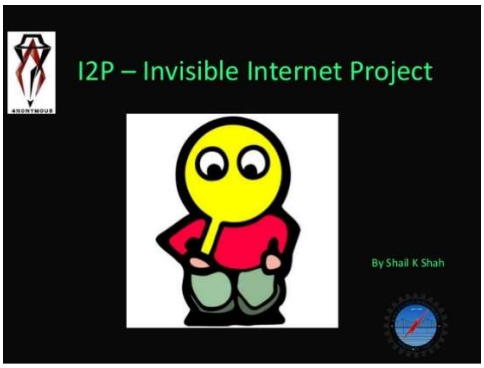
I2P:

I2P، به عنوان لایه‌ای برای ارتباطات بی‌نام[42] گسترده‌ی فردبه‌فرد[43] طراحی شد که می‌تواند همه‌ی سروریس‌های اینترنت قدیمی را نیز اجرا کند. این پروژه از سال 2003 به عنوان نسخه‌ی کامل‌تری از Freenet شروع به کار کرده است و هدف آن این است که به چندین سرویس، اجازه‌ی اجرا شدن در کنار HTML را بدهد. برخلاف TOR که از ابتدا قرار بود

---

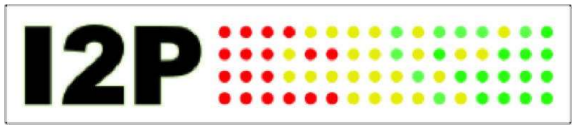
[39] The onion router
[40] Homepage
[41] Directory
[42] Anonymous
[43] Peer to peer

ناشناختگی را هنگام ارتباط با اینترنت حفظ کند، هدف اصلی I2P این است که راهی دزدکی و مخفی بین کاربران و سرویس-های میزبان ایجاد کند [9].



:Freenet

در مورد Freenet، در بخش تاریخچه تا حدودی توضیح داده‌شد. بنابر عقیده‌ی کلارک، مواردی مانند پورنوگرافی کودک، نباید در این شبکه وجود داشته باشند. او گفته است که:"از لحاظ تکنیکی، این امکان‌پذیر است که ما بتوانیم ویروسی تولید کنیم که سایت‌های حاوی پورنوگارفی کودک را از بین ببرد. اما راه‌های بسیاری نیز برای دسترسی به آن‌ها، حتی در وب سطحی وجود دارد. ما همچین، به قانون کپی‌رایت احترام می‌گزاریم و هر چیزی که در Freenet، مضنون باشد را، با اعمال فشار، مجبور به متوقف کردن می‌کنیم. اصلاح Freenet، پایان کارFreenet خواهدبود [3].



نحوه‌ی استفاده:

در این بخش، صرفاً به طور اجمالی، نحوه‌ی استفاده از مشهورترین ابزار دسترسی به شبکه‌ی عمیق، یعنی TOR را بررسی میکنیم.

ابتدا بسته‌ی نرم‌افزاری TOR را از سایتwww.torproject.org دانلود کرده و سپس آن را نصب نمایید.پس از اجرای نرم‌افزار، Vidalia control panel به صورت خودکار، راه‌اندازی شبکه تصادفی[۴۴] را انجام میدهد و زمانی که TOR آماده‌ی کارب کار شد، صفحه‌ی مرور بازشده و شما می‌توانید جستجوی خود را انجام دهید. البته، تا این مرحله، شما صرفاً چیزی شبیه به یک ف_ی_ل_ت_ر شکن در اختیار دارید. مشکل اصلی این است که کجای شبکه‌ی تاریک و عمیق را بگردیم. سایت‌های زیادی مانند Redditو Grams و چند ویکی که معروف‌ترین آن‌ها، TheHiddenWiki.org می‌باشد، لینک‌های زیادی را به شما پیشنهاد می‌دهند [5].

دولت‌ها و قوانین اجرایی:

بسیاری دولت‌ها نظیر آمریکا و انگلیس، دو رویکرد متفاوت نسبت به شبکه‌ی عمیق و تاریک، بنابر نوع استفاده از آن اتخّاذ می‌کنند. رویکرد اوّل، حمایت از این شبکه در راستای احقاق آزدای بیان و حفظ حریم خصوصی و رویکرد دوم، مبارزه با مجرمان این شبکه ها می‌باشد.

در چند سال اخیر، حمایت دولت آمریکا از TOR افزایش یافته‌است. آزادی بیان در حوزه‌ی سایبری، که به عنوان بخشی از قوانین دولت‌های ایالتی آمریکا تعریف شده‌است، به دنبال این است که به مردم رژیم‌های سرکوبگر، کمک کند تا آن‌ها بتوانند به اطلاعاتی که توسط حکومت کشورشان سانسور می‌شود، دسترسی پیدا کنند. هم‌چنین، شرکت Facebook، در راستای این قوانین، به تازگی ورژنی از سایت خود را راه اندازی کرده‌است که مردم کشورهایی که این سرویس را محدود می‌کنند_مانند ایران و چین_ راحت تر بتوانند به آن دسترسی داشته باشند [10]

در مارس 2015، دولت انگلیس برای مبارزه با جرایم شبکه‌ی تاریک، خصوصاً در ضمینه‌ی پورنوگرافی کودک و قتل‌های زنجیره‌ای، یک واحد مجزّای جرایم اینترنتی را راه‌اندازی کرد. در همین را ستا، آژانش ملّی جرم انگلیس(NCA) و سرویس اطّلاعات انگلیس(GCHO)، با همکاری یکدیگر، سلول عملیّات مشترک(JOC) را تشکیل دادند [5].

نکات و راه‌کارهای امنیتی:

استفاده از شبکه‌ی عمیق، به تنهایی باعث محفوظ نگه‌داشتن ناشناختگی هویت شما نمی‌شود، بلکه باید در کنار آن، مراقب مسائل دیگری نیز بود. این که شماره حساب بیت‌کویت شما به هویت شما لینک شده باشد یا این که از هویت واقعی برای ثبت نام و عضویت در سایت‌های مختلف و خریدهایتان استفاده کنید، یا استفاده از آدرس ایمیلی که به وسیله‌ی آن در جای دیگری از وب سطحی استفاده کرده‌اید، همگی می‌توانند هویت شما را فاش کنند.

[44]Randomized

در ضمن، گفته می‌شود که حتماً روی دوربین رایانه‌ی خود را با برچسب بپوشانید تا کسی نتواند از طریق هک کردن دوربین رایانه شما، به هویت و مکان شما پی ببرد. مسدود کردن ورودی صدای رایانه نیز برای رعایت کردن جوانب احتیاط، لازم است.

منابع:

[1] The Deep Web and “ ,Daniel Sui, James Caverlee, Dakota Rudesill .2015 *,Wilson Center* ”,The Dark Net

[2] Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, Martin .2015 *,Trend Micro* ”,Exploring The Deep Web“ ,Rosler

[3] .2017 *,Tech Advisor* ”,What is the dark web and deep web“ ,M. Egan

[4] *Bright* ”,Cleaning up confusion Deep web VS Dark web“ ,M. Singh .2014 *,Planet Corporation*

[5] May 6 *,Dictionary* ”,The Deep web VS The dark Web“ ,J. Solomon .2015

[6] .February 2015 *,PCMagazine* ”,Inside The Dark Web“ ,M. Eddy

[7] The dark web, what is it, how it works, and why its not “ ,T. B. Lee *.vox* ”,going

[8] .August 2012 12 *,PCWorld* ”,Meet darknet“ ,B. Chacos

[9] 26 *,The Guardian* ”,The dark side of the internet“ ,A. Beckett .Novermber 2009

[10] Robert ,Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov *,Trend Micro* ”,Deepweb and cybercrime, its not all about TOR“ ,McArdle .2013