Dark web

Produced by:

Atousa Tohghyani

مقدمه:

- ممکن است بسیاری اینترنت و شبکه جهانی وب را مترادف بدانند؛ در صورتی که این طور نیست.
- وب بخشی از اینترنت است که به واسطه ی آن می توان به آن دسترسی پیدا کرد .
- برخی وب را ، فقط وب سایت های قابل دسترسی از طریق یک موتور جستجوی سنتی ، مانند Google میدانند.
- با این حال ، این محتوا – معروف به "Surface Web" – تنها یک بخش از وب است.
- Deep Web به کلاسی از محتوا در اینترنت اشاره دارد که به دلایل مختلف فنی توسط موتورهای جستجوگر فهرست بندی نمی شوند و بنابراین از طریق موتور جستجوی سنتی قابل دسترسی نخواهد بود.
- Dark Web بخشی از Deep Web است که عمداً پنهان شده است.

مقدمه:

- در سال ۲۰۰۵ تعداد کاربران اینترنت در سراسر جهان به ۱ میلیارد نفر رسید.
- این تعداد در سال ۲۰۱۰ از ۲ میلیارد عبور کرد.
- در سال ۲۰۱۴ بیش از ۳ میلیارد نفر بود.
- از ژوئیه سال ۲۰۱۶ ، بیش از ۴۶٪ از جمعیت جهان به اینترنت وصل شدند.
- محتوایی که در اختیار ما قرار دارد تنها ۵٪ از وب است.
- در طرف دیگر بخش بزرگی به نام دیپ وب وجود دارد که موتور های جست و جو نمیتوانند انها را پیدا و در انها جست و جو کنند.که این بخش بیش از ۹۵٪ فضای وب را تشکیل می دهد.

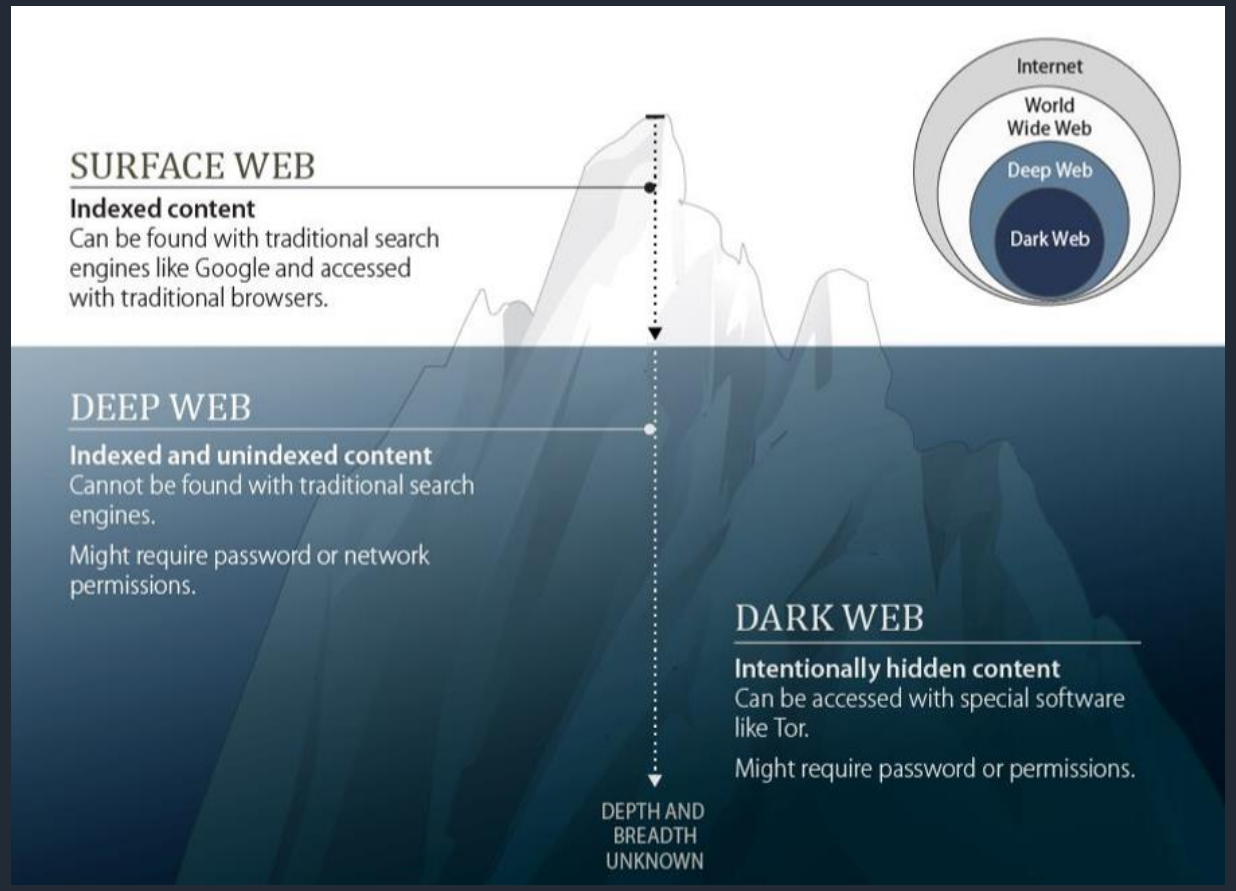
Layers of the Internet:

- surface web

می توان با موتورهای جستجوگر سنتی مانند گوگل یافت و با مرورگرهای سنتی قابل دسترسی است.

- deep web

با موتور جستجوی سنتی یافت نمی شود.
ممکن است به گذرواژه یا مجوزهای شبکه احتیاج داشته باشد.



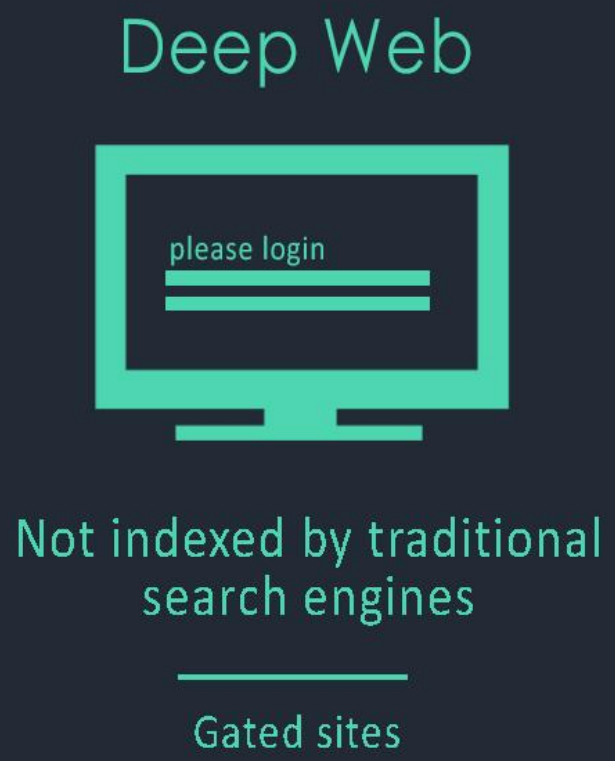
- dark web

با نرم افزارهای ویژه مانند "تور" قابل دسترسی است.
ممکن است به گذرواژه یا مجوز احتیاج داشته باشد.

: Surface Web

این بخشی از وب است ، که برای ما قابل مشاهده است.
تنها ۵٪ از فضای وب را شامل میشود.
تعداد ۳۳۴,۶ میلیون نام دامنه اینترنتی سطح جهانی در سه ماهه دوم سال ۲۰۱۶ ثبت شده اند .
این افزایش ۱۲,۹٪ از تعداد نام دامنه های ثبت شده در مدت مشابه سال ۲۰۱۵ است.
از فوریه ۲۰۱۷ ، بیش از ۱,۱۵۴ میلیارد وب سایت تخمین زده شده است.
همانطور که محققان خاطرنشان کردند ، این اعداد "فقط به اندازه وب اشاره می کنند" ، زیرا تعداد کاربران و وب سایت ها دائماً در حال نوسان هستند.

: Deep Web



دیپ وب به طور کلی به هر چیزی در اینترنت گفته میشود که توسط موتور های جست وجو رایج همچون گوگل ، یاهو و بینگ قابل (ایندکس شدن) نیست.
از این دست موارد میتوان به ایمیل شخصی ، دیتابیس شرکت های بزرگ وکوچک ، فضای شخصی ، ظرفیت ابری ، حساب های بانکی و وب سایت های غیر قانونی اشاره کرد.
بخش بزرگی از دیپ وب کاملا قانونی بوده و بنا به دلایل کاملا صحیح از دید مردم عادی پنهان شده است.
همین فضا باعث شکل گیری بخشی کاملا مجزا شده که ، در ان افرادی که نمی خواهند به هر دلیلی هویتشان فاش شود از این فضا استفاده میکنند.
اطلاعات در اینجا استاتیک نیستند و به صفحات دیگر لینک دارند.
برخی تخمین های اولیه اندازه دیپ وب را ۴۰۰۰-۵۰۰۰ برابر بزرگتر از شبکه سطح قراردادند.

: Dark Web

دارک وب به بخشی از اینترنت نامرئی گفته میشود که در ان اکثرا فعالیت های غیر قانونی صورت میگیرد.
فعالیت هایی مثل فروش مواد مخدر ، فروش غیرقانونی اسلحه ، قاچاق حیوان و انسان ، قمارهای کلان که سرنوشت یک بازی ورزشی را مشخص میکند.
با توجه به اینکه این فضا قابل دسترسی عموم نیست و هویت کاربران هم در ان مخفی است ،کسب و کار در ان بسیار رونق دارد.
دارک وب مثل هر چیز دیگری ، دو روی مثبت ومنفی دارد که حداقل جنبه های منفی ان بسیار اشکارتر است زیرا پرطرفدارترین بخش دارک وب ، بازارهای غیرقانونی ان است.
در دیپ وب ، دارک وب نیز در حال رشد است.
مشخص نیست که میزان دیپ وب ، توسط محتوای دارک وب چقدر است و میزان دارک وب برای فعالیتهای قانونی یا غیرقانونی چقدر است.

Tor

برای ورود به سطح نامرئی اینترنت به نرم افزاری به نام Tor نیاز دارید که بتواند نقش پل ارتباطی را برای شما ایجاد کند.
از بین این نرم افزار ها تور مشهورترین انهاست.
واژه تور مخفف "Thin Onion Routing" است.
خوده این نام برگرفته از Onion Routing (مسیریابی پیازی) است. روشی که در ان تبادل اطلاعات به صورت ناشناس انجام میشود.
علت انتخاب این نام استفاده از الگوهایی با عملکرد لایه ایی و رمزنگاری پیازی شکل است که در دسته بندی الگوهای ناشناختی قرار دارد.
بنابراین لوگو پیازی که رنگ اصلی ان بنفش است. علامت همین سرویس و تداعی کننده لایه های متعدد برای رسیدن به هسته اصلی است.
ایالات متحده(۱۹/۲٪) بیشترین میانگین مصرف کنندگان روزانه Tor را دارد و پس از آن روسیه (۹/۱۱٪) ، آلمان (۹/۹٪) و امارات متحده عربی (۹,۲٪) قرار دارند

Tor

در بیشتر متدولوژی های فضای تاریک ، ادرس سرویس کاربران از طریق درهم سازی (Hashing) کیلد عمومی با الگوریتم SHA-1 و درهم سازی ۱۰ کاراکتر (۸۰ بیت) اول با الگوریتم Base32 به دست می اید که یک رشته ۱۶ کاراکتری است.
ترجمه و شناسایی این نوع ادرس دهی برای دیگر موتور های جست وجو قابل شناسایی و ردیابی نیست.
از طرف دیگر ساده ترین مسیر ارتباطی بین کاربر و سرور از طریق توزیع پخشی بین حداقل ۶۰۰۰ سرور تعریف میشود که عملا کشف و رهگیری را غیر ممکن میسازد.
خود تور دارای مرورگر است ، هرچند کاربران برای ورود به دارک وب میتوانند از مرورگرهای مخصوص استفاده کنند.
اکثر کاربران به هیدن ویکی (Hidden Wiki) مراجعه میکنندکه میتوان ان را ویکی پدیای تخصصی وب تاریک دانست.
و به صورت یکی از سرویس های تور ارائه میشود.

Tor

تاریخچه:

مهندسان نیروی دریایی ایالت متحده در اواسط دهه ۹۰ مشغول توسعه نرم افزاری شدند که بتواند از اطلاعات CIA محافظت کرده و قابلیت ارتباط بدون شناسایی را در اختیار مقام های بالادستی خود قراردهند.
مدتی بعد دارپا (سازمان پروژه های تحقیقاتی پیشرفته دفاعی) توسعه این نرم افزار را ادامه داد و درنهایت اواسط سال ۲۰۰۳ اولین ورژن از نرم افزار تور در اختیار کاربران عادی قرار گرفت.
اکنون کار به جایی رسیده که اکثر سایت های غیرقانونی برای مخفی کردن هویتشان از رمزگذاری تور استفاده کرده و از پسوند Onion بهره می برند.
سال ۲۰۱۰ این پروژه توسط بنیاد نرم افزار های ازاد به عنوان پروژه آزاد نمونه، انتخاب شد.

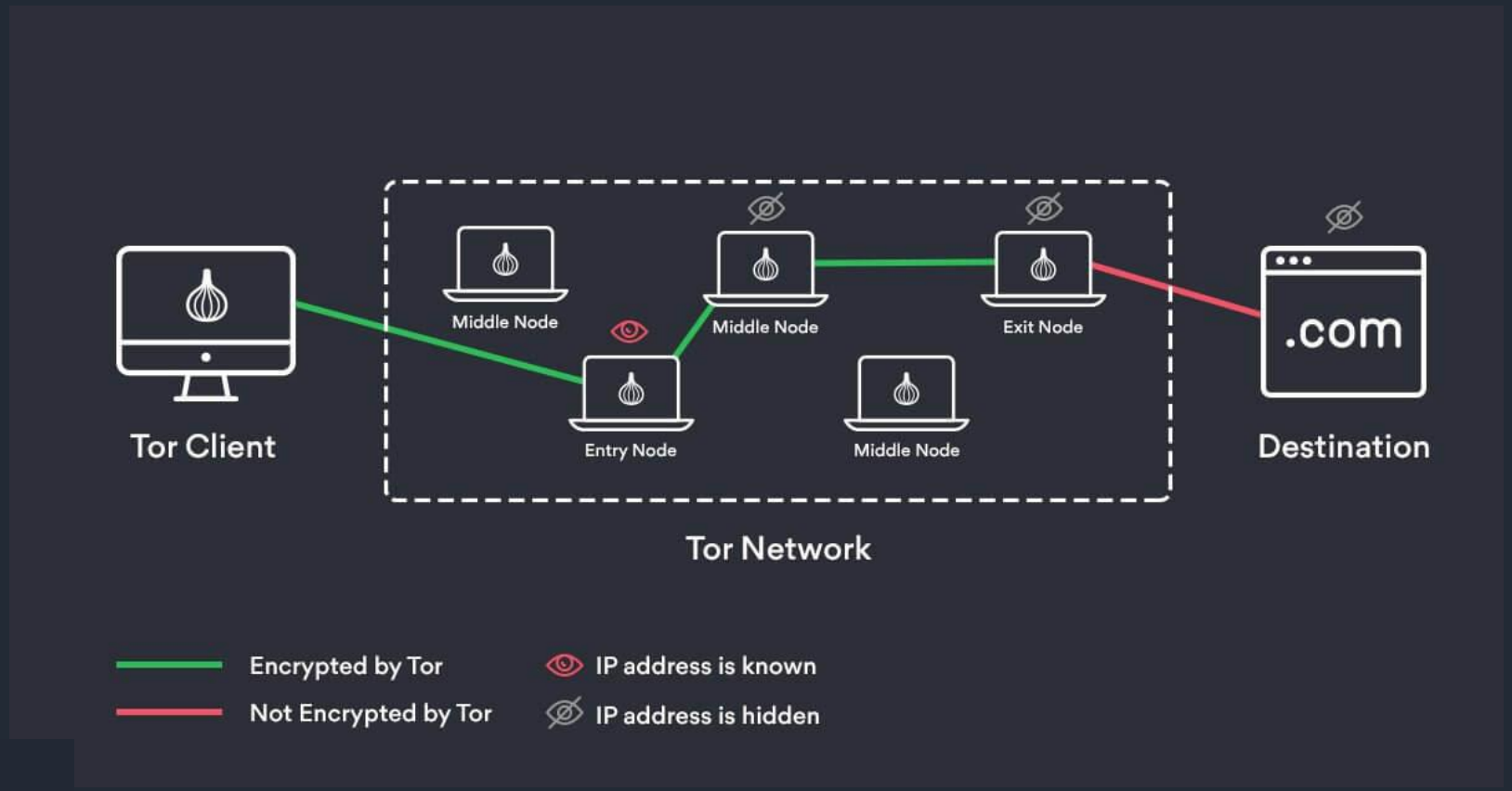
Tor

طرز کار:

در این شیوه پیام های رمز نگاری شده به وسیله تعداد زیادی گره شبکه با نام مسیر یاب های پیازی فرستاده میشود.
هر مسیریاب یک لایه رمز را برای خواندن دستورهای مسیریابی رمز گشایی میکند و پیام را به مسیریاب بعدی میفرستد که همین روند را تکرار میکند .این روش باعث میشود که محتوا و مبداء و مقصد پیام مخفی بماند.
برای دریافت لایه به لایه ، Tor، "رله(relays)" را در رایانه های سراسر جهان مستقر کرده است که از طریق آن اطلاعات منتقل می شود.
اطلاعات بین رله ها رمزگذاری شده اند ، و کل ترافیک Tor حداقل قبل از رسیدن به مقصد ، حداقل از سه رله عبور می کند.
رله نهایی "رله خروجی" نامیده می شود و آدرس IP این رله به عنوان منبع ترافیک Tor مشاهده می شود.
هنگام استفاده از نرم افزار Tor، آدرس های IP کاربران پنهان می ماند.
به این ترتیب ، به نظر می رسد که اتصال به هر وب سایت داده شده از آدرس IP رله خروجی Tor، که می تواند در هر نقطه دنیا باشد ، ناشی می شود.

Tor

طرز کار:

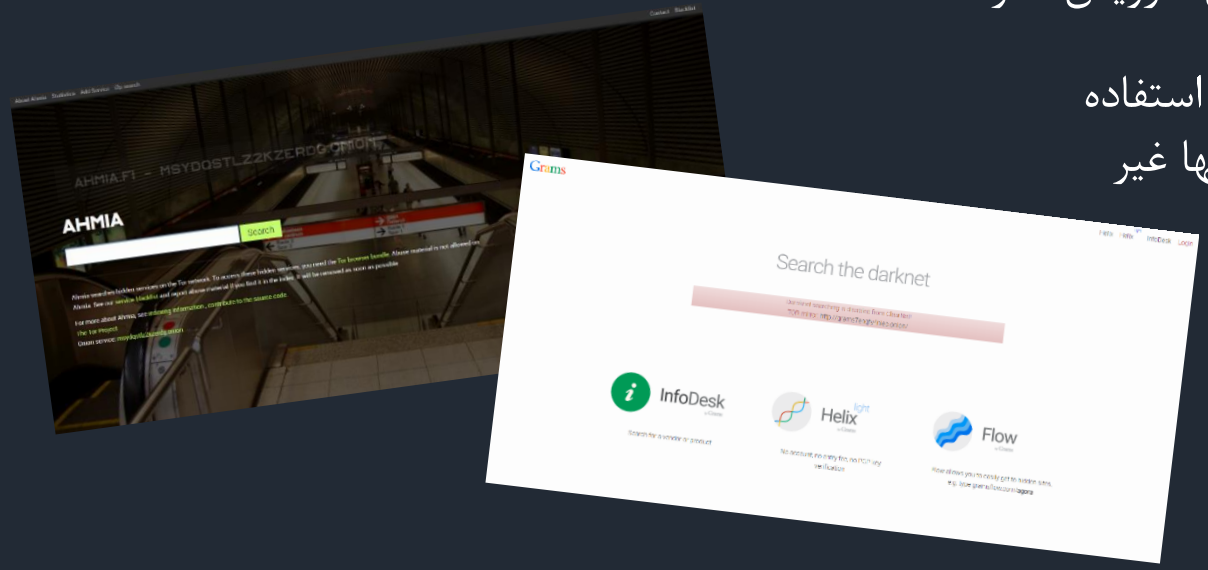

Middle Node
Middle Node
Exit Node
.com
Tor Client
Entry Node
Middle Node
Destination
Tor Network
Encrypted by Tor
Not Encrypted by Tor
IP address is known
IP address is hidden

دارک وب از چه زمانی بر سر زبان ها افتاد؟

اواخر سال ۲۰۱۳ که FBI از بستن سایت Silk Road خبر داد سایتی که گفته میشود ، بزرگترین وب سایت فروش مواد مخدر در دارک وب بود و در طول فعالیت دوساله اش بیش از ۱ میلیون و ۳۰۰هزار معامله غیر قانونی (خرید و فروش مواد مخدر) در ان انجام گرفت که از این حیث میتوان ان را بزرگترین کارتل انلاین تاریخ نامید.
این سایت در فوریه سال ۲۰۱۱ افتتاح شد.
در ابتدا افراد بسیار کمی توانایی فروش مواد را داشتند و اکثر کاربران مشتری بودند ، اما این روند طی مدت کوتاهی تغییر کرد ، طوری که تا تابستان سال ۲۰۱۳(چند ماه پیش از بسته شدنش) این فروشگاه نزدیک به ۳۹۰۰ فروشنده داشت و ۱۴۰ هزار خریدار داشت.
در این مدت ارزش معاملاتی که در این سایت صورت گرفت ، به بیش از ۱/۲میلیارد میرسید.
تمامی این معاملات با استفاده از بیت کوین انجام می شد.
وقتی در نوامبر سال ۲۰۱۳ پلیس فدرال امریکا خبر دان (Down) کردن سایت و دستگیر شدن مالک ان را اعلام کرد ، بخش زیادی از مخاطبان تازه با پدیده ترسناک دارک وب اشنا شده بودند.
این موضوع باعث شد حتی نمایندگان مجلس سنای امریکا در نوبت های مختلف ، در مورد دارک وب اظهارنظر کنند.
این سر و صدای رسانه ای به مدت ۶ ماه ادامه داشت ، تا در نهایت میلیون ها نفر از وجود این بخش تاریک اینترنت خبردار شدند.

پیمایش در Deep Web و Dark Web :

- اکثر کاربران از موتور جست وجوی Hidden Wiki برای استفاده از دارک وب استفاده میکنند اما موتور های جست وجوی دیگری نیز وجود دارد ، از جمله:
  - Ahmia : جستجوها و فهرستهای موجود در فهرست خدمات پنهان Tor را فهرست بندی می کند.
  - Grams : یک موتور جستجوی خاص تر است "با الگوبرداری از Google " که در آن کاربران می توانند مواد مخدر، اسلحه ، پول تقلبی و سایر مواد منع مصرف را پیدا کنند.
- هنگام استفاده از Tor، URL وب سایتها تغییر میکنند ، به عنوان مثال :
به جای وب سایتهایی که به ".net" or ".org" or ".com" و.. غیره ختم می شوند ، دامنه ها معمولاً با پسوند " onion " پایان می یابند و یک " hidden service " را مشخص می کنند.
Tor بسیار کند است و این به عنوان یکی از اشکالات استفاده از این سرویس ذکر شده است.
- Dark Web همچنین از یک ساختار نامگذاری scrambled استفاده می کند که URL هایی را ایجاد می کند که به خاطر سپردن آنها غیر ممکن است. به عنوان مثال ، یک سایت بازرگانی محبوب به نام Dream Market توسط آدرس غیرقابل توصیف "noino.۷۶lcca۲z۳eajwlvm" می رود.



ایا میتوان به Dark Web اعتماد کرد؟

حتی با وجود تور و سایت های غیر قانونی باز هم هرکسی نمیتواند از تمامی خدمات موجود در دارک وب استفاده کند ، زیرا افرادی که مشتری دائم دارک وب هستند نمیخواهند کسی از کار انها سر دراورد.
قوانین دارک وب تفاوت زیادی با بازی Hitman دارد !
هیچ راهی وجود ندارد که مخاطب دریابد ایا سایت های دارک وب واقعا در ازای پولی که به انها پرداخت میشود ، خدمانی انجام میدهند یا به قول معروف سرکاری است.
بسیاری از فعالیت هایی که در دارک وب انجام میشود توسط خلافکاران بزرگ و کارتل ها سازماندهی میشود.

به نظر شما ،ایا کاربر عادی میتواند به راحتی و تنها با استفاده از تور به شبکه عظیم خرید و فروش انها دسترسی پیدا کنند؟

قطعا خیر

بسیاری از سایت ها تنها از طریق رابط غیرقابل دسترس بوده و خود گردانندگان سایت روی ورود شخص به شبکه گسترده انها بسیار حساس هستند.
موضوعی که پس از بسته شدن سایت Silk Road بسیار تشدید شد.

تجارت در Dark Web:

ناشناس بودن ذاتی مکان ، نظرکلاهبرداران و سارقان را به خود جلب می کند ، **اما شما هنگام خرید اسلحه یا مواد مخدر هدفتان چیست؟**

- سایت های تجارت وب تاریک دارای ویژگی های مشابه با هر عملیات خرده فروشی الکترونیکی از جمله رتبه بندی / بررسی ، سبد خرید و تالار گفتگو هستند ، اما تفاوت های مهمی وجود دارد: یکی کنترل کیفیت.
- هنگامی که خریداران و فروشندگان ناشناس هستند ، اعتبار هر سیستم رتبه بندی مشکوک است.
- رتبه بندی ها به راحتی دستکاری می شوند و حتی فروشندگان با سابقه طولانی نیز ناگهان با رمزهای مشتری های خود ناپدید می شوند ، بعداً با یک نام مستعار دیگر اقدام به راه اندازی فروشگاه می کنند.
- بیشتر ارائه دهندگان تجارت الکترونیکی نوعی خدمات سپردن ارائه می دهند که بودجه مشتری را تا زمان تحویل محصول ، نگه می دارد.
- اما در صورت بروز اختلاف ، لبخند انتظار نداشته باشید.
- هر ارتباط رمزگذاری می شود ، بنابراین حتی ساده ترین معامله به یک کلید PGP نیاز دارد.
- حتی تکمیل معامله هیچ تضمینی برای ورود کالا نیست.
- بسیاری نیاز به عبور از مرزهای بین المللی دارند و مقامات گمرک بسته های مشکوک را خراب می کنند.
- وب سایت تاریکی اخبار Deep.Dot.Web با داستان هایی از خریدارانی که به دلیل تلاش برای خرید دستگیر شده اند یا به زندان افتاده اند ، روبرو است.

پرداخت در Dark Web:

بیت کوین ، ارزی است که اغلب در معاملات در وب تاریک مورد استفاده قرار می گیرد.
هنگامی که یک بیت کوین در یک معامله مالی استفاده می شود ، معامله در یک دفترچه عمومی به نام زنجیره بلوک ثبت می شود.
اطلاعات ثبت شده در زنجیره بلوک آدرس های بیت کوین فرستنده و گیرنده است.
یک آدرس، بیت کوین خاصی را منحصر به فرد نمی کند. آدرس صرفاً یک معامله خاص را مشخص می کند.
آدرس کاربران با کیف پول همراه بوده و در آنها ذخیره می شود.
کیف پول حاوی کلید خصوصی یک فرد است ، که یک شماره مخفی است و به آن امکان می دهد بیت کوین را از کیف پول مربوطه ، مانند رمز عبور ، خرج کند.
کیف پول و کلید خصوصی در دفترچه عمومی ثبت نمی شود.
اینجاست که استفاده از بیت کوین باعث افزایش حریم خصوصی شده است.
وب سایت تاریک به لطف بیت کوین رونق گرفته است که به دو طرف امکان می دهد بدون اطلاع از هویت یکدیگر ، یک معامله مطمئن را انجام دهند.

"بیت کوین عامل اصلی رشد وب تاریک بوده است و وب تاریک عامل بزرگی در رشد بیت کوین بوده است."

Red Room:

مقدمه:

اعتقاد بر این است که اتاق های سرخ حاوی محتوای شکنجه صریح است که توسط یک مدیر که دستورالعمل های بیننده را دریافت می کند ، در معرض دید افراد قرار میگیرد.
به عبارت ساده ، اتاق های قرمز فقط مانند حراج هایی عمل می کنند که مزایده ها مربوط به شکنجه مردم هستند.
کاربران می توانند هزینه تماشای شکنجه را به صورت آنلاین بپردازند ، در حالی که سرپرست هر کاری که بالاترین میزان پرداخت از طرف کاربران را داشته باشد ، روی اسیر انجام می دهد.

ظهور :

اصطلاح "اتاق قرمز" ده ها سال است که وجود دارد. تصور می شود که این فیلم ، از فیلم ترسناک " Videodrome " در ۱۹۸۳ سرچشمه گرفته است. در این فیلم شکنجه در اتاقی رخ داده است که به رنگ قرمز رنگ شده و به صورت زنده از تلویزیون نشان داده شده است.

محبوبیت:

اعتقاد بر این است که اتاق قرمز پس از انیمیشن ژاپنی محبوب شد و در آنجا تبلیغی pop-up روی صفحه نمایش افراد با این سؤال که " اتاق قرمز را دوست دارید؟ "نمایش داده میشد ، اگر کسی سعی میکرد آن را ببندد ، یک پنجره تمام اندازه با نام افراد باز میشد.
داستان ها حاکی از آن است که این اسامی متعلق به افرادی است که قبلاً به اتاق سرخ دسترسی پیدا کرده بودند و مرده بودند.

Red Room:

ایا واقعی است؟

گرچه برخی ادعا می کنند که آنها قادر به دسترسی به یک اتاق قرمز بودند ، اما همه سایت هایی که ادعا می کنند چنین نوع محتوا را ارائه می دهند ، تاکنون جعلی بوده اند.
سایتهایی مانند اتاق قرمز فقط به افراد کمک می کند تا فکر کنند که در قسمت پنهانی از اینترنت که قرار نیست در آن پیدا شود ، گیر افتاده است.
با این حال ، تقریباً تمام این سایت ها توسط کلاهبرداری هایی که می خواهند دست خود را به بیت کوین بکشند اداره می شوند.
علاوه بر این ، حتی اگر سایت های شکنجه "پرداخت به نمایش" وجود داشته باشد ، آنها مطمئناً از طریق شبکه Tor کار نمی کنند.
چون شبکه های Tor آهسته هستند و پخش کردن یک فیلم زنده در ان تقریبا غیرممکن است.
تحقیقات نشان می دهد که اتاق های قرمز یک اسطوره هستند. آنها به دلیل رسانه های سنتی و اجتماعی محبوب شدند.
مردم می توانند هر آنچه را که می خواهند در اینترنت بنویسند. میلیون ها نفر آن را می خوانند. و همین کافی است تا مردم باور کنند که چیزی وجود دارد حتی اگر اینگونه نباشد.
اتاق های قرمز چیزی فراتر از یک افسانه شهری نیست. تا به امروز ، هیچ مدرک واقعی پدید نیامده است که خلاف آن را مطرح کند.
با این حال ، هنوز هم افرادی در وب تاریک (و سطح) وجود دارند که ادعا می کنند وجود دارند.

برخی اصطلاحات در Dark Web :

Alias

- نام صفحه ای که به منظور مخفی نگه داشتن هویت واقعی آنها طراحی شده است.

Bitcoin

- بیت کوین اساساً ارز Dark Web است . بازدید کنندگان برای خرید اقلام از بازارهای آنلاین یا عضویت در سایت ها استفاده کنند.

Blockchain

- نوعی بانک اطلاعاتی است که از بلوک اطلاعات تشکیل شده است که یک سری معاملات را ثبت می کند. اطلاعات موجود در ان در یک سری از کاربران یا رایانه ها توزیع می شود.

Carding

- اصطلاحی است که برای توصیف روش سرقت اطلاعات کارت اعتباری و فروش آن در وب تاریک به کار می رود.

Clearnet

- اصطلاح دیگری برای اینترنت سنتی است که همه ما می شناسیم.

برخی اصطلاحات در Dark Web :

Cryptocurrency

- می توان ان را نوعی پول دانست،که معمولاً در وب تاریک استفاده می شود.

Doxing

- اغلب به عنوان نوعی انتقام جویی مورد استفاده قرار می گیرد.

Encryption

- هنگامی که داده ها رمزگذاری می شوند ، تقسیم می شوند ، و آن را غیر قابل تشخیص می کنند.

Firewall

- یک وسیله امنیتی شبکه است که بر ترافیک ورودی و خروجی نظارت می کند و تصمیم می گیرد اجازه دهد یا مسدود کند ..

Honeypot

- یکی از راههایی که کارشناسان امنیتی در مورد جرایم سایبری و حملات آنلاین مطالعه می کنند.

Spoofing

- کلاهبرداری از کارت اعتباری و شماره حسابهای بانکی را که بصورت آنلاین با انها خرید میکنید.

چند مورد از اتفاقات در دارک وب:

۱. ادم خواری
۲. اتاق شکنجه
۳. جعبه سیاه
۴. جارو برقی
۵. ابزار شکنجه
۶. جعل اسناد
۷. چرم طبیعی
۸. احضار روح
۹. اعدام
۱۰. مواد مخدر
۱۱. استخدام هکر
۲۱. جنگ جهانی دوم
۳۱. کودک ازاری
۴۱. ...

Reference:

1. Dark Web -Kristin Finklea Specialist in Domestic Security -March ۲۰۱۷,۱۰
2. https://youc.ir/dark-web/
3. https://www.tarafdari.com/
4. https://www.lifelock.com/learn-identity-theft-resources-what-is-the-dark-web.html
5. https://en.wikipedia.org/wiki/Dark_web
6. http://securityaffairs.co/wordpress/8719/cyber-crime/the-good-and-the-bad-of-the-deep-web.html

Thank You :)

for your attention!