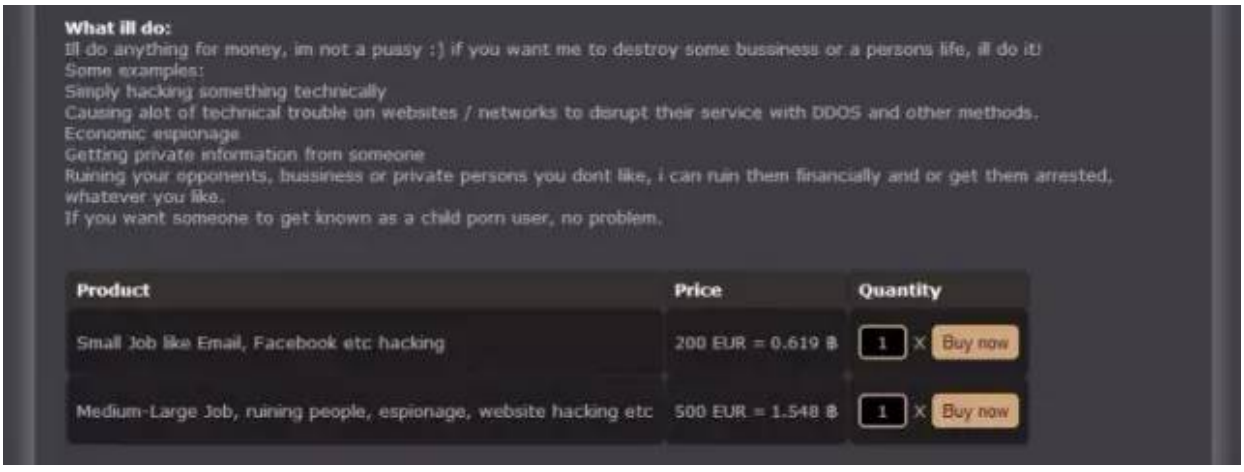
暗网那些事儿

2017-04-26 letshome 计算机与网络安全

> 为了钱我可以做任何事。不要误会，我不是鸡。如果你让我毁掉一桩生意或者毁掉一个人的生活，我很乐意效劳。

这是一名黑客在网上的独白，他在出租自己的黑客技术。黑进个人电子邮箱收费200欧元，而让一个人名誉扫地只要500欧元。这个帖子得以赤裸裸地招摇过市，是因为它处在不见天日的暗网之中。暗网的世界游离于标准互联网和搜索引擎之外，像你我这样的普通人可能永远不会看到它。



在暗网世界里，这算是口味最轻的一笔买卖。

暗网的存在并不是什么新闻。了解它的人，醉心于这里的自由放荡；不了解它的人，可能一生都不会踏进这扇门。

如同电影大师库布里克人生的最后一部作品《Eyes Wide Shut》（大开眼戒）中所描述，无论身份显赫或平庸，从进入古堡的一刻起，都必须头戴面具。而这个古堡在网络世界中的翻版，就是暗网。就算你会“科学上网”，用谷歌、百度等引擎也绝对搜索不到暗网中那些网站的蛛丝马迹。要进入这个世界，你需要一本特殊的“护照”，你的浏览器也需要学另一种“语言”。因为一旦踏入这些“暗室”，你的相貌、身份、地位、地理位置、联系方式、道德和底线，全部坍缩成一个词——匿名者。

Tor（The Onion Router）可以说是目前最为流行的网络匿名访问技术，用户的请求会在分布全球的主机随机跳转三次，最终才到达服务器，这就造成了溯源的极其困难，从而使得所有的访问者完全没有身份区别。大多数的暗网就建立在这样的技术之上。

通俗地讲，进入一个赤裸的世界，唯一需要遮挡的地方就是你的脸。如果你已经带好了面具，那么欢迎你进入这个充满“想象力”的国度。

肮脏的市集

人在什么时候需要完美的匿名呢？看看暗网中“电商”们出售的商品，你也许会有答案。

暗网“商店”中出售的美金伪钞

贩卖假钞、枪支、毒品的商店赫然在目。而往往每家店铺只出售一类商品，可谓“又专又精”。

- 只要5900美金可以获得包括美国护照、身份证、驾照等全套的证件。
- 伪造的英国护照价值2000英镑。甚至卖家还会承诺把你的个人信息添加到官方数据库之中，保证你的护照可以走遍世界。
- 一把沙漠之鹰手枪，需要1450欧元。当然，你可能还需要花45欧元买50发子弹。
- 一个新鲜出炉的用户信用卡信息（账户、密码、CVV码）要14美元。你可以用来随意消费。
- 如果你“缺钱”，可以花一半的价格买到伪钞。

由于你懂的原因，交易的货币清一色折算为BTC（比特币）。由于比特币很值钱，所以14美金的信用卡信息只相当于0.04141413BTC。而面值2000美金伪钞也只需要5.535BTC。和淘宝一样，大多数卖家都会强调：“英国/美国直邮，包邮哦亲”；和淘宝类似，某些店铺的留言板上也有一些用户点评。和淘宝不同的是，没有支付宝这类支付平台对双方的信誉负责。交易方式千奇百怪，但“先交钱，再发货”这个铁律没得商量；和淘宝不同的是，这里也没有旺旺可以让买卖双方扯皮砍价。购买咨询往往会通过网站上公布的保密邮箱，有些卖家还会在邮箱地址之后加上一句：“别问脑残的问题，我们会直接无视。”

暗网集市中出售的手枪

在这个屏蔽了法律的黑暗森林，交易的天平往往变得倾颓，在暗网专用的某搜索引擎中输入“scam（诈骗）”会看到有论坛的帖子专门罗列“骗子网站”。甚至还有人开帖专门交流受骗的经验，好让后来者防止踩坑。在这些五花八门的“商店”中，究竟有多少商店做了多少交易，又是谁从中获得了多少利益，全部不得而知。而暗网商店的层出不穷，甚至繁荣蔓延，却给某些论断提供了铁证。

“Torshop”是一家专门为暗网电商建站的服务商，很多商家的网页底端都会标注：“Powered by Torshop”而在Torshop的“官网”上也会不断更新“合作电商”的地址，并且用自己的信用保证名单里的电商都不是骗子。雷锋网记者看到，在其上“注册”的商家有几十家，并且不断有人进出名单，持续更新这个黑暗的榜单。

苹果设备是暗网商店青睐的产品

暗网中出售的商品，可能是一个普通人一生都不会接触到的违法物品，然而有一类产品，却是人们日常生活中最为常用的。那就是以iPhone等苹果设备为主的电子产品。以电子产品为主营的暗网电商不在少数，网页精美，价格公道，一部iPhone的价格往往是官方售价的4-6折，这比你在中国电商上找到的水货价格更加低廉。

如果仔细研究，你会发现暗网上的商家大多很“nice”，比如他们会在页面上向你解释iPhone如此便宜的原因：

- 我们通过非法渠道得到了大量的信用卡信息，但是这些钱无法取出来，我们必须用这些卡购物，然后再卖掉这些东西变现。所以iPhone是最好的选择。

- 不要担心，iPhone不会直接邮寄到你家，而是会先邮寄到我们的地址，再由我们给你发货，这样你就绝对安全了。

这正好解释了信用卡信息的用途，一条购买信息、销赃套现的产业链逐渐被打捞。但是，先交钱再收货的铁律仍然颠扑不破。在暗网这个黑暗森林中，如果一个骗子想要骗你的钱，相信这也是他能想到的最让人信服的理由。

丝绸之路和“暗网大亨”

一个个闪烁着欲望的网页背后，究竟是什么人在维持这个冷酷的体系运转呢？五大三粗、描龙画凤的黑社会？西装革履、不怒自威的“教父”？还是衣着邋遢、目空一切的嬉皮士？

暗网在现实世最显赫的声名恐怕是由“丝绸之路”创造的。如果你还没有听过，那么这个以绿色驼队为LOGO的网站会让你对这条古老商道所有浪漫的想象化为齑粉。毒品是这个交易平台上最著名的商品，其类目之细致让人瞠目，九大类目中，八类为毒品、致幻剂和处方药，每一大类下还有5-6个子类，每个子类下有上百家供应商。而诸如信用卡信息、0-Day漏洞等其他交易被统一分配在“other”一栏中。

有关丝绸之路的故事甚至可以写成如魔戒三部曲般厚的书，分别对应丝绸之路1.0、2.0和3.0时代。没错，这个隐秘的世界已经悄然历尽无数“劫波”了。

丝绸之路的创建者 乌布利希

乌布利希是丝绸之路的创建者，一个名副其实的“暗网大亨”。这个看上去如加州阳光一样灿烂的大男孩有两个身份：冷血的瘾君子、自由主义哲学家。在数学和自然科学方面的天才让他可以制造出一切需要的东西，包括毒品和“丝绸之路”平台。2010年，他在LinkedIn中宣布将“打造一个经济模拟体，让人们亲身体验在一个没有系统性力量的世界生活。”无疑，系统性力量正是指“警察和法律”。之后他便在正常的网络中消失。他在“丝绸之路”出售自己生产的“迷幻蘑菇”，依靠良好的“信用”吸引了大批毒贩和瘾君子。

> 网站发布没几天就有了第一批注册用户，然后收到了首条信息。我激动得不能自已。逐渐地人们开始注册，卖方注册，然后我的首个订单就来了，我永远不会忘记它。
>
> 之后几个月我通过网站卖了大约十英磅迷幻蘑菇。

乌布利希的日记里如此写道。

整个计划，只有他的大学老友贝茨和女友知晓。接下来的剧情，就是标准的好莱坞大片模式。乌布利希生意火爆，联邦调查局根据物流顺藤摸瓜，由于“丝绸之路”的五

个“员工”企图索要封口费导致乌布利希试图买凶灭口，FBI骗过乌布利希顺利成为一名“员工”，老友贝茨在重压之下选择背叛。

乌布利希从暗网浮出水面之后，有两个瞬间给人们留下了深刻的烙印：

> 1、在乌布利希简朴的住所附近的图书馆里，他正在和FBI伪装的“员工”在电脑上聊天，两名特工扮演的路人在他身后突然争吵，在他回头的一瞬间，便被另一名特工按倒在地，他再也没能碰到自己的电脑。如果再晚一秒，让他有机会关上电脑，或许所有扳倒他的证据都将灭失。
>
> 2、在审判阶段，他重复了无数次在网上发出的宣言：“丝绸之路远非买卖毒品那么简单，它是要夺回我们的自由、我们的尊严和对公正的追求。”然后平静地地聆听有罪判决，转向坐席上憔悴的父母和他的支持者，淡然一笑。

被捕时乌布利希无法关闭的电脑上显示着他的账户

暗网的惊人之处，也是恐怖之处在于它强大的自愈能力。2013年10月，乌布利希被捕，仅仅一个月以后“丝绸之路2.0”上线。创建者自称“Defcon”，用强大的品牌号召力瞬间重组了涣散的毒品大军。FBI故技重施，特工成功得到Defcon的信任，并且还赚了相当于32000美元比特币的工资。2014年，Defcon被捕，他的真实身份是一名SpaceX前员工，火箭专家和比特币痴迷者本特霍尔。

就在FBI的发言人正气凛然地表示“那些藏在键盘背后的人，将最终被发现”的时候，丝绸之路3.0上线，Slogen是：“王者归来。”

事实证明，FBI除了改变丝绸之路的版本号以外，最重要的工作是证明了：暗网并不是密不透风的避风港。

改变世界的漏洞天堂

即使你是一个遵纪守法的好公民，并且根本不知道这个鬼魅网络的存在。暗网对你生活的影响， 也远超你的想象。

早些时候，著名的网络军火商HackingTeam被黑客侵入，证明了它的大量漏洞收购和网络军火交易都通过暗网进行。而HackingTeam的客户中，包括大量国家的政府机关，他们采购网络军火用以维护自身的国家利益。而这些军火究竟是用在了正义的事业上还是邪恶的勾当中，取决于你的国籍和政治态度。

有资料显示，韩国和哈萨克斯坦都运用了这些网络军火对中国进行了攻击，对于这两国公民来说，暗网在捍卫他们国家利益中立了大功。在网络战争中，没有国家可以独善其身。根据业内人士透露，漏洞作为一个国家重要的网络军火资源，是每个国家都在积极储备的。在这些资源的流动过程中，暗网的身影不时显现。

ISIS在暗网上的视频网站

事实证明，在一些影响世界的重大事件中，暗网承担了重要的作用。

- 阿拉伯之春中，埃及的革命者正是通过在暗网上的串联，才成功躲避政府的追踪，最终导致穆巴拉克下台。

- 恐怖组织ISIS的网站，几乎全部建立在暗网之上，躲避打击，持续招募成员。向其宣战的“匿名者”组织和ISIS交战的主战场也在暗网之上。

漏洞交易在商业竞争中同样扮演重要角色。在暗网上，几乎每个大型交易网站都会为漏洞交易开辟“专区”，即所谓的“H/P/A/W/V/C”：Hack, Phreak, Anarchy, Warez, Virus, Crack（黑客、窃听、无政府、盗版、病毒、破解）。

暗网上的黑客技术和漏洞交易

> 如果你把一个Win10的致命漏洞提交给微软，可能拿到几万美金，如果你拿到漏洞黑市上交易，你可以得到几倍、几十倍、几百倍的利润。撇开道德因素，一个理智的黑客一定会在黑市中交易他手中的漏洞。

> 根据HackingTeam泄露的数据，一个普通的漏洞交易价格大约在3.5-4.5万美元之间，如果独家销售给Hacking Team，价格至少会翻三倍。一个有价值的iOS漏洞交易价格可能在几十万美金。

显然，这些高价的漏洞被购买者用在了他认为能够产生更大价值的地方。有“中国黑客教父”之称的万涛曾经说，真正高级的黑客从不会让别人意识到他的存在，因为他们从不失手。如果按照这个观点来推演，人们甚至无法证伪，因为一些漏洞借助暗网的传播，悄然改变了诸多事件的走向。

> 暗网是隐藏在文明世界的无政府领地。你可能永远不知道我们熟悉的互联网还有狰狞的另一面，这里充斥着性、毒品和杀戮。这里的一切都明码标价：一把沙漠之鹰价值1450美金、一个伪造的英国护照价值2000英镑、一克纯可卡因价值80美金、一张个人信用卡信息价值14美金、黑入邮箱的服务价值200美金，而一个人的生命值10000美金。

如果你做好了准备，就最后一次仰望一下湛蓝的天空，屏住呼吸，潜入沸腾着欲望的暗网世界吧。

地下的维基百科

由于暗网的隐蔽性，导致无法通过大规模的宣传来获得表层网站这么庞大的用户群。所以精准定位的分类导航成为了流行的形式。例如：一个名为“UnderDir”的分类导航网站，收录了11000多家暗网站。分为12类，包括商务、政治、科技、色情、宗教等很多类目，甚至还专有搜索引擎一项。

Under Dir 暗网分类导航引擎

在暗网的世界里，没有形成一家独大的搜索引擎。各类引擎分庭抗礼，使用同样的关键词搜索到的内容也不尽相同。然而，暗网的搜索体验，远远谈不上愉悦。不论是通过分类导航还是搜索引擎，进入的网站有很大可能是无法访问。在“UnderDir”收录的11000多家网站中，有7545处于离线状态。几乎所有的搜索引擎都会提供“网页最后一次被成功访问”的时间信息。如果证明已经掉线，会在本条搜索结果中标注“Offline”。之所以搜索引擎会保留这些死链接，是因为暗网站经常受到追踪或者干扰，非常不稳定。可能根据情况随时下线，也可能瞬间起死回生。对于有“抱负”的网站（例如丝绸之路）来说，保持时时在线是“良好信誉”的保证。

虽然暗网的网站有相当一部分是涉及非法活动的，不过也有一些技术网站或主题论坛是并不违法的。能够在“The Hidden Wiki”上拥有自己的词条，恐怕是网站实力的重要“背书”。这个暗网版维基百科收录了一些著名的词条，有权限的用户也可以创建新的词条。然而，相比维基百科的全面精确，这里的词条混乱不堪，“圣经的真相”“如何打扫浴室”“买房的注意事项”等等奇葩的词条赫然其上。如果用户搜索了没有被创建的词条，网站就会自动提供搜索引擎的结果。

暗网中的维基百科 The Hidden Wiki

大量的色情网站（包括儿童色情网站）可以通过分类网站或者搜索引擎被找到。和表层网络不同的是，这里鲜有赌场广告等变现形式。大多数网站需要直接支付比特币才能获得会员资格，进行资源下载。不得不说，暗网的商业形态相当落后。而这种封闭的生态结构也注定不会有复杂的交易形态产生。一手交钱、一手交货，从原始社会就形成的交易规则在这里成为标准玩法。

天堂向左，影网向右

> 我们是3人一组的杀手，在美国（包括加拿大）和欧洲接受任务，一旦收到你的付款，我们会在1-2天内联系你。根据你要消灭的目标不同，我们会和你持续联系1-3周。唯一的准则就是：不杀16岁以下的孩子，还有排名前十的政治人物。

这同样是一个“Powered by Torshop”的页面。其中的商品是人的生命。10000美元取一个人的性命，杀手说得如此冷静从容，就好像一次无聊的家政服务。暗网的残忍在这一点开始不可遏制地滑向了深渊。

暗网中杀手的杀人价码

在暗网中，仍然有一扇扇暗门，通向更加黑暗的地下室。这里如《盗梦空间》的Limbo一般，让毒枭和恋童癖都不忍直视。这就是传说中的影网。

一切有关影网的传说都缘起于Reddit用户的一个帖子：《A warning to those thinking about accessing the shadow web》（警告那些想要进入影网的人）。帖子中细致地描述了作者——一位加油站员工如何在一个偶然的机会得到了一张卡片，上面详细描述了如何进入这个影网：下载一款特别的浏览器，在浏览器中设定特别的参数。一个在正常浏览器，甚至Tor浏览器中都毫无意义的链接发出清脆的“Click”声音，展现出这家网站的真容。

宣称可以进入影网的网站入口

根据作者的描述，他不明就里地充值了比特币，进入了一个直播房间——Redroom。而房间里的内容让他终生难忘：

> 一个强壮的男人根据“Master”（主人）的指示，用各种手段，一步一步残忍地虐杀了一名阿拉伯女性。“Master”甚至多出500美元，让施暴者在镜头前挖出了她的双眼。

凄厉的尖叫和残忍的杀戮让作者不敢看屏幕上发生的一切，跑到厕所呕吐不止。而当喊叫声终于结束，他才敢回到电脑前，看到受害者横尸镜头前，双眼只剩下两个空洞，不断涌出鲜血。而管理员却平静地说：感谢观赏，下一场将在一小时后开始。

这个故事甚至还有后续，有很多人留言质疑作者所言的真实性，其中一个设法联系到了帖子的作者。作者将这个卡片翻拍给他，他根据卡片指引果然进入了影网，并且在Reddit上发文证实，奉劝大家千万不要试图进入影网。再后来，据说发帖作者再也没有在网上出现，而同一时间，某个原本平静小镇发生了离奇的凶杀案。

这次事件涉及的所有帖子中没有任何网页截图，也为整个事件蒙上了真假难辨的黑雾。然而这件事如鬼魅一般久久不散的原因在于：影网在技术上是完全可以实现的。只要采用特别的网络协议和特定的浏览器参数，影网的服务器便可以面向特定的人开放浏览。与其说这是影网，不如说是既处在网络之中，却又与世隔绝的残忍直播间。最让人不寒而栗的是，在某些动荡的阿拉伯或非洲国家，仇杀和虐杀频繁发生，只要这些变态杀人狂选用影网的技术，就可以让Redroom在事实上成为可能。而根据网上自称“知情人士”的用户爆料，某些ISIS成员正在利用死亡秀的方式筹集资金。

记者以“Redroom”为关键词在暗网各搜索引擎进行搜索，得到的结果令人吃惊。

某Redroom网站入口

> 你已经来到了影网的Redroom，每隔一周这里都会上演死亡秀（只要参与人数达到标准）。我们定制了火狐浏览器，并且应用SPDY协议保证你的匿名访问。你需要付0.5比特币就可以得到“安全浏览器”的下载链接，在秀开始之前24小时，我们会通知你。欢迎来到俱乐部。

记者按照要求专门申请了匿名邮箱，向其发信请求网站的比特币钱包地址，但是两天过去了，没有收到来自网站的任何回复。仔细研读这个声明的日期：2015年10月27日，距今只有一个月。按照网站公布的“隔周一次”的频率，这里已经进行了至少两场死亡秀。而网站会员的收费标准，和Reddit帖子中的价格几乎完全相同。

而这个网站只是无数自称Redroom网站其中之一。有更多的网站宣称只要付费就可以看到Redroom的血腥杀人秀，明确标明了做“Master”（施虐方式决定者）

和“Spectator”（观众）的价码，以及事无巨细的注意事项，甚至可以决定被害者的年龄是Preteen（-18）、Teen（18-30）还是Adult（30+）。所有的类似网站入口都有一句标志性的欢迎词：“玩得愉快，希望我们的房间让你快乐！”这句话像魔鬼一样让人不寒而栗。

还没有人和丝绸之路创建者乌布利希一样因为“杀人秀”而被捕，这或许可以给我们以安慰，让我们相信Redroom并不存在。

暗网里的中国人

> 人生几个秋，发家不用愁！

在暗网上看到如此对仗的中文，让人有种久违的亲切感。这个由署名“VIP”的用户发表在“暗网中文论坛”的帖子目的是找Carding（信用卡盗刷）同伙。要成为同伙首先需要交300元会费，再以每个150-300元的价格购买信用卡信息，承托提供完备的服务。并且留下了合作邮箱，特别强调邮件内容需要使用密文，因为不要“猪一样的队友”。

暗网中文站上的“买人帖”

在暗网上为数不多且略显萧条的中文站里，讨论发财致富的方法是主流思潮（这倒和“明网”遥相呼应），不断有人反复询问“来钱快的路子”，并且强调“不介意犯法”。银行卡盗刷、赃款套现、制毒、枪支贩卖成为了几大“研讨主题”。自称是台湾人，用繁体字的用户和用简体字的用户数量大致各占半壁江山，在这个社区里，两岸亲密无间的状态让人恍如隔世。

从Torbay深网论坛、深网中文第一页、暗网114论坛的活跃主题来看，大致可以想象出一条横跨台海两岸的枪支走私网络。甚至有声称是台湾人的用户发帖询问如何从越南芒街偷渡到中国，因为他已经进入了政府的禁止入境的“黑名单”。

这里并没有中文黑市，存在于各大中文论坛的交易区也并不活跃。很难计算究竟有多少人真正进行了非法交易，不过从各大站点中不时发出的对“VIP”的讨伐帖或追债贴，还有“VIP”跟帖回呛的状态来看，暗网上的中文圈有两个特点：

> 1、不大；
>
> 2、在不大的圈子里，现实世界的怀疑和欺诈呈现得更加直白且狗血。

暗网中文论坛的另一个特别之处在于，人们热衷于政治话题的讨论。有人回帖写道：“在这里发帖，起码不会被删。”让人回味良久，无语凝噎。

匿名者在暗网上的中文论坛中讨论枪支

尾声

说到暗网中游走的人，除了黑色产业参与者、骗子、猎奇者、无数匿名警察以外，还有一些让人印象深刻的角色。

> 有一名黑客专门黑进儿童色情网站，删除其中的图片和视频，并且表示这是他人生当中不多的有意义的事情。

> 有一名西班牙医生，专门为吸毒者无偿普及正确的吸毒方式。他表示，并不能阻止瘾君子吸毒，但至少可以用专业知识减轻毒品对他们的危害。

他们算是暗网之中的异类。

如果习惯了暗网当中对规则的肆意凌辱，回到现实难免会怅然若失。暗网因为无政府而显现出一套奇异的社会面貌。那些蔑视规则、向往自由的人最有可能成为暗网的死忠，而危险、复杂、欺诈，正是“自由”的代价。在纯匿名的网络中，最有可能获利的人无疑是把木马隐藏在网页中，俘获猎奇者的黑客，还有伪装自己有毒品、假钞、甚至是杀人直播的骗子们。如果你在暗网中流连多日，你会觉得暗网中流传的故事分为三类：

> 1、无数人背负自由之名，行苟且之事；
>
> 2、无数人拼死掩盖罪恶，却终究败露；
>
> 3、无数人目睹尸山血海，仍蠢蠢欲动。

暗网和现实这两个世界绝无可能完全隔绝。如你所想，暗网世界和每个人都有关，无论它让你自由还是蒙羞。

▼ 点击**阅读原文**，查看更多**精彩文章**。

阅读原文