

一个由荷兰国家警察、欧洲刑警组织联合创办的网站！

小小莫理 [莫理](#)



关注莫理！每天获取稀奇古怪的好东西

//

前言

说起勒索病毒，莫理想起了17年发生的趣事，那时候勒索病毒风波席卷全球，可一位外国小哥仅花了几十美金就制止了这场灾难。

<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>

上面这个域名不管是看似还是实际，都是杂乱无章，毫无规律可言。

但它的出现非同一般，是从病毒文件里分析而来！

```
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0); // ; "http://www.iuqerfsodp9ifjaposdfjhgosur
if ( v5 )
{
    InternetCloseHandle(v4);
    InternetCloseHandle(v5);
    result = 0;
}
else
{
    InternetCloseHandle(v4);
    InternetCloseHandle(0);
    sub_408090();
}
```

于是这位小哥就注册了这个域名并解析到了自己的服务器。

离奇的是出现了成千上万的访问者，ip地址更是来源世界各地！

域名 [iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com](#) 的信息 [求购此域名](#) 以下信息更新时间: 2021-01-13 19:46:14

域名	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com [whois 反查] 申请删除隐私 其他常用域名后缀查询: cn com cc net org
注册商	CloudFlare, Inc
更新时间	2019年04月06日
创建时间	2017年05月12日
过期时间	2024年05月12日
域名服务器	whois.cloudflare.com
DNS	BRUCE.NS.CLOUDFLARE.COM SARA.NS.CLOUDFLARE.COM



导致这么多访问者的主要原因是WanaCrypt病毒模块运行时，会通过因特网访问这个域名。

若能正常连接则停止工作，不执行加密程序。若连接失败，则会继续执行加密。

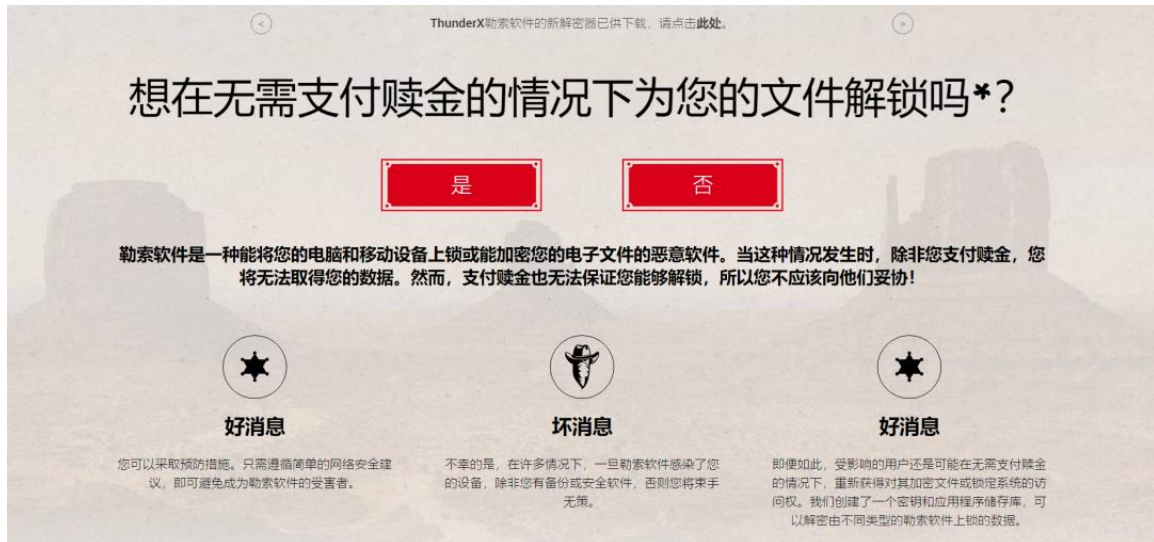
如今打开这个杂乱无章的域名，提示如下：



不过被火绒贴上了恶意网址，自动拦截 🤖



拒绝勒索病毒



网址：

<https://www.nomoreransom.org/zh/index.html>

拒绝勒索病毒网站是由荷兰国家警察高科技犯罪单位、欧洲刑警组织下属欧洲网络犯罪中心、卡巴斯基实验室和英特尔安全网络公司所创力的计划。

旨在帮助勒索软件的受害者重新免费取回其加密数据，无需向犯罪者支付赎金。



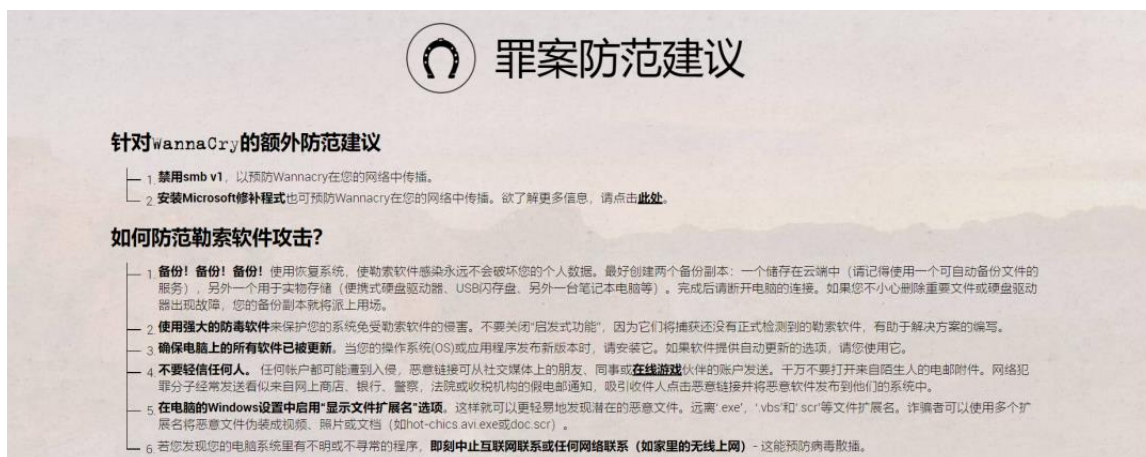
如果你的电脑不幸中了勒索病毒，该网站或许对你有所帮助，首先可以利用它查看勒索软件的类型。

如果有相对应的解密工具，则会提供给你。根据网站提供的操作指南进行解密操作。


此外还科普了许多勒索软件的相关知识，起源以及发展，感染的症状以及应对措施等等。

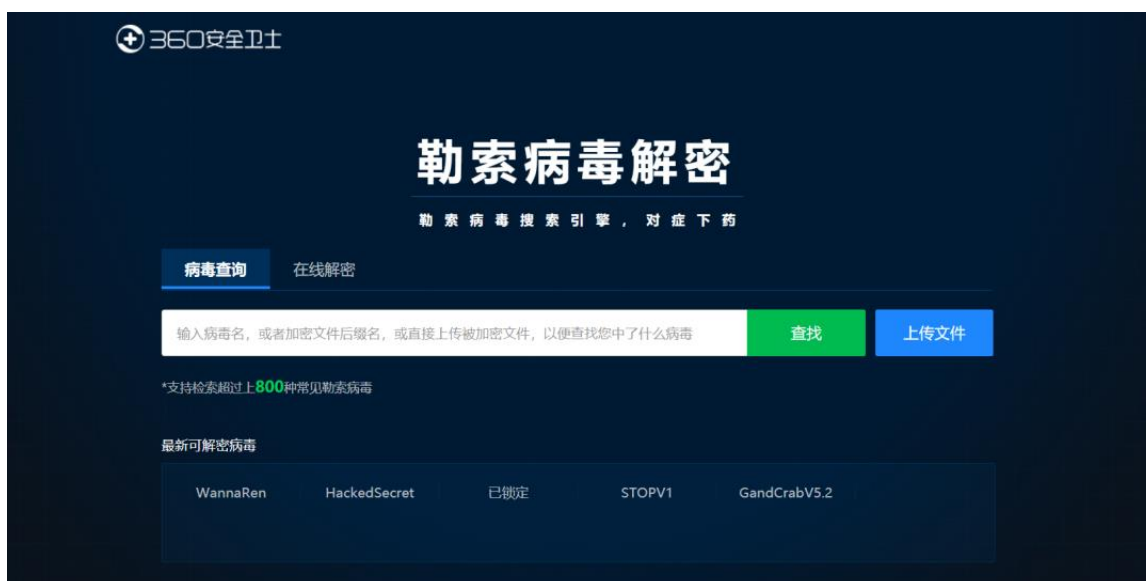


你可以进行举报罪案，根据相应的地区进行操作。



网站特别强调：我们一般建议您不要支付赎金。支付赎金只会让网络犯罪分子确认勒索软件是有效的，并不能保证您会得到所需的解锁密钥。

国内360安全卫士旗下也有同类型的勒索病毒解密产品 



网址：<https://lesuobingdu.360.cn>

其实在某宝上也有很多“专家”，自称能破解任何勒索病毒。但要价比原赎金还要高。

不得不怀疑那些“专家”仅仅是询问病毒作者价格后加价反馈给我们，此乃“中间商” 🐼

有小伙伴说可以先发一个于你而言非常重要的文件给某宝卖家或者病毒作者，让他恢复证明确实有解锁能力，若是真的咱们就白嫖走人。

歌故事里

汪峰《在雨中》官方版

由网友“Y”点歌

视频来源：腾讯视频

可能喜欢

[真以为靠手速抢到茅台吗？](#)

[逆天的开源神器，简直不要太方便！](#)

[找到了！！四年前的版本用着才最爽！](#)

[鹅厂两款良心听歌神器，共享曲库版权！](#)

[两款珍藏好久神器，安卓苹果都有！](#)

[还开大会员？快白嫖大佬开发的神器！](#)

到底了，顺手打个卡趴