


链接投毒



概览

试图攻击某些 P2P 下载软件。
用于测试的文件：
<https://raw.githubusercontent.com/songsammy/link-poisoning/master/Test.txt>
如果使用浏览器直接点击链接，那么会返回 404 错误。
但是，如果你用下载器下载，则会得到一个虚假文件。由于这只是一个测试，所用文件只是一个文本文件（不包含病毒）。但这足以证明攻击是可行的。
受影响的软件：

图标	名称
	迅雷 10.1.14.438

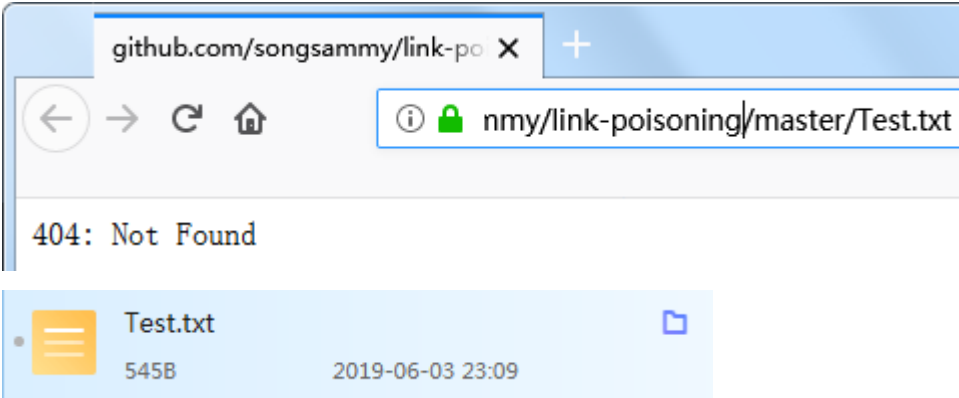
预防措施

尽量避免使用迅雷进行下载。
如有必要，则下载后一定要验证哈希[验证方法](#)

测试

开始时间： 2019-06-03 23:07:05

结果

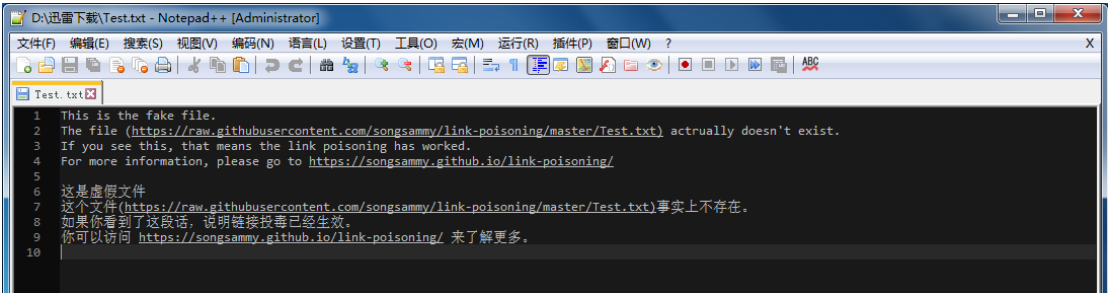


github.com/songsammy/link-po X +

← → ↺ 🏠 ⓘ 🛡️ nmy/link-poisoning/master/Test.txt

404: Not Found

Test.txt 545B 2019-06-03 23:09



D:\迅雷下载\Test.txt - Notepad++ [Administrator]

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?

Test.txt

```
1 This is the fake file.
2 The file (https://raw.githubusercontent.com/songsammy/link-poisoning/master/Test.txt) actually doesn't exist.
3 If you see this, that means the link poisoning has worked.
4 For more information, please go to https://songsammy.github.io/link-poisoning/
5
6 这是虚假文件
7 这个文件(https://raw.githubusercontent.com/songsammy/link-poisoning/master/Test.txt)事实上不存在。
8 如果你看到了这段话，说明链接投毒已经生效。
9 你可以访问 https://songsammy.github.io/link-poisoning/ 来了解更多。
10
```