漏洞相关 极速快车手 2024-06-28 发表

组网及说明

DNS基于UDP 53号端口,诞生于1983年并沿用至今。如今DNS流量占比不足1%但是其中的攻击流量却占比90%以上。根据思科年度报告近91.3%的恶意软件被发现使用DNS作为主要手段。

因此如果你的办公电脑被审计到软件自动访问恶意域名,就需要引起重视。

Windows PC中的防火墙通常只支持限制ip的安全策略,无法实现恶意域名拦截。 修改host文件可以实现恶意域名黑名单功能。

配置步骤

1. 打开windows的资源管理器(快捷键:win + E), 进入 C:\Windows\System32\drivers\etc 文件夹

(把上面这个路径复制以后,粘贴在地址栏再按回车就可以快捷进入了)

:\Windows\System32\drivers\e			
C:\Windows\System32\drivers\6	etc		
名称	修改日期	类型	大小
hosts 🗋	2024/5/26 23:48	文件	1 KB
hosts.ics	2024/5/26 14:54	Calendar	1 KB
hosts_lg_bak	2023/3/31 15:08	文件	1 KB
Imhosts.sam	2022/5/7 13:22	SAM 文件	4 KB
🗋 networks	2021/6/5 20:08	文件	1 KB
D protocol	2021/6/5 20:08	文件	2 KB
services	2021/6/5 20:08	文件	18 KB

2. 我们可以看到这个文件夹里有一个叫 hosts 的文件, 双击打开它



3. 打开以后, 在最后一行添加

127.0.0.1 www.bilibili.com

注意前面不要加空格, 井号。ip地址和网址之间有一个空格

9	127.0.0.1 account.acronis.com
10	127.0.0.1 gateway.acronis.com
11	# Added by Docker Desktop 前面不要加空格和井号
12	192.168.1.105 host.docket.internal
13	192.168.1.105 gateway.docker.internal
14	# To allow the same kube context to work on the host and the container:
15	t End of section
16	127.0.0.1 www.bilibili.com
	这里有一个空格

如果你是想实现访问不了其它恶意域名,请将<u>bilibili.com</u>改为目标恶意域名,例如softdown.365xiaz ai.com,这样这台电脑就无法进行百度搜索了。并且可以输入多行内容,每写完一个IP+网址以后,另 起一行继续输入就行了。

例如下面这样:

4.内容书写完以后一定要保存,或者按快捷键 ctrl + s进行保存

	hosts		×	+				
文件	编辑	查看						
新建	标签页	Ctrl+N	ate ac	ronis	s.com			
新建	窗口	Ctrl+Shift+N	on.ac	ronis	.com			
打开		Ctrl+O	-tih.a	croni	is.com			
保存		Ctrl+S	ad.ac	ronis	com			
另存	为	Ctrl+Shift+S	Acron	15.COI	m			上安 点体计丹返山
全部	保存	Ctrl+Alt+S	onis.c	com				
页面	设置		onis.c	om				
打印		Ctrl+P	.acro	nis.c	om			
			'.acro	nis.c	om			

5. 🕯	然后按win	+	R	输入cmd代开终端
------	--------	---	---	-----------

回 运行	×
	Windows 将根据你所输入的名称,为你打开相应的程序、文件 夹、文档或 Internet 资源。
打开(O):	cmd ~
	确定 取消 浏览(B)
6. 在命令行	理输入 ipconfig /flushdns 点击回车即可



好了,**现在再去访问,你就会发现无论如何也打不开了。**就算重**连网络,更换浏览器**也不行。而且因为我们的做法是修改系统文件内容,也不会被杀毒软件检测到。

无法访问此网站 www.billbill.com 意外终止了连接。 请试试以下办法: - 检查网络维接 - 检查代理服务解和防火墙 - 运行 Windows 网络诊断 ERR_CONNECTION_CLOSED 運動加報	ß	
www.billbili.com 意外终止了连接。 请试试以下办法: • 检查网络连接 • 检查内理服务器和防火墙 • 运行 Windows 网络诊断 ERR_CONNECTION_CLOSED 難新加税	无法访问此网站	
请试试以下办法: • 检查网络连接 • 检查内理服务 瞬和防火墙 • 运行 Windows 网络诊断 ERR_CONNECTION_CLOSED 難新加税	www.bilibili.com 意外终止了连接。	
err_connection_closed 運動加税	请试试以下办法:	
E State Stat	ERR_CONNECTION_CLOSED	
	重新加報	洋橋

当然如果还可以访问的话,可能是浏览器缓存问题,进入浏览器的设置清除一下就可以了

隐私和安全	♥ Chrome 找到了一些安全建议需要您审核 密码、权限	前往"安全检查"可
性能		
外观	隐私和安全	
搜索引擎	清徐测览数据	
默认浏览器	清除测觉记录、Cookie、缓存及其他数据	
启动时	御私保护指南 检查重要的關格控制设置和安全控件	
语言	第三方 Cookie	
载内容	- 已相正尤混模式下图第三万 Cookie	

最后再说一下撤销的方法,那就是把刚才在 hosts 文件里写的内容删除就行了

配置关键点

在我们访问网站时,域名解析的优先级是: DNS缓存 > hosts文件 > 找网关,访问DNS服务器

假设b站的ip地址是119.84.174.66,在我们访问某域名时,正常情况下会找先DNS缓存,再找hosts 里的信息,最后找路由器来获取web的ip地址。总之正常情况下获取到的肯定是正确的ip地址,但是 如果将hosts文件修改为127.0.0.1对应恶意域名时在系统解析时就会定位到的ip地址为127.0.0.1,这 是系统的环回地址,所以肯定无法访问到了。另外为了防止DNS缓存先人一步匹配到正确的ip地址, 于是我们在cmd中删除了DNS缓存,这样就万无一失了。