APT攻防之使用图片暗藏shellcode实现无文件攻击和Edr绕过

DX安全实验室 • 2023-04-21 09:10 • 本文共 1028 字 • 阅读完需 4.5 分钟

> 远程白名单加载shellcode是钓鱼攻击的一种常见APT手法，在很多针对APT组织的分析报告中也有体现。

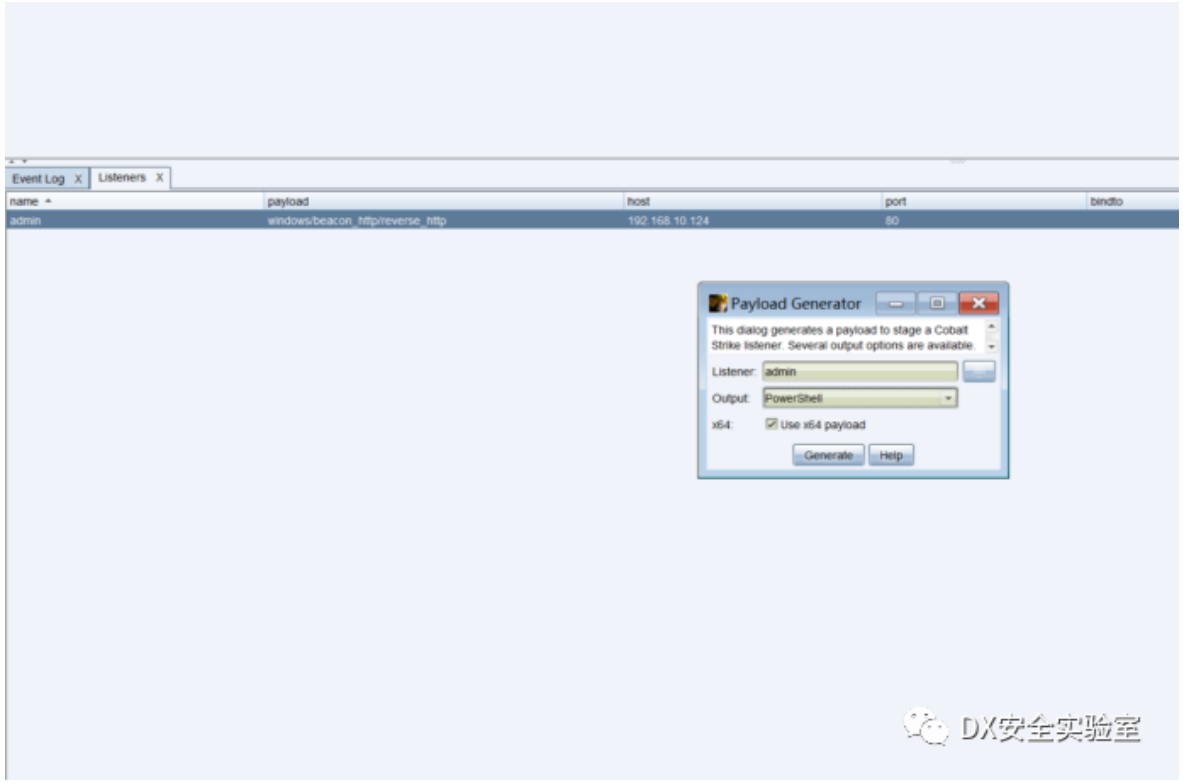
Part1原理

远程白名单加载shellcode是钓鱼攻击的一种常见APT手法，在很多针对APT组织的分析报告中也有体现。母体程序是一个经过编译的可执行程序，诱导用户点击之后，恶意程序会首先会去访问带有shellcode的图片，然后将图片加载到内存中。用户看到的就是一张图片，实际上已经完成了对目标主机攻击操作

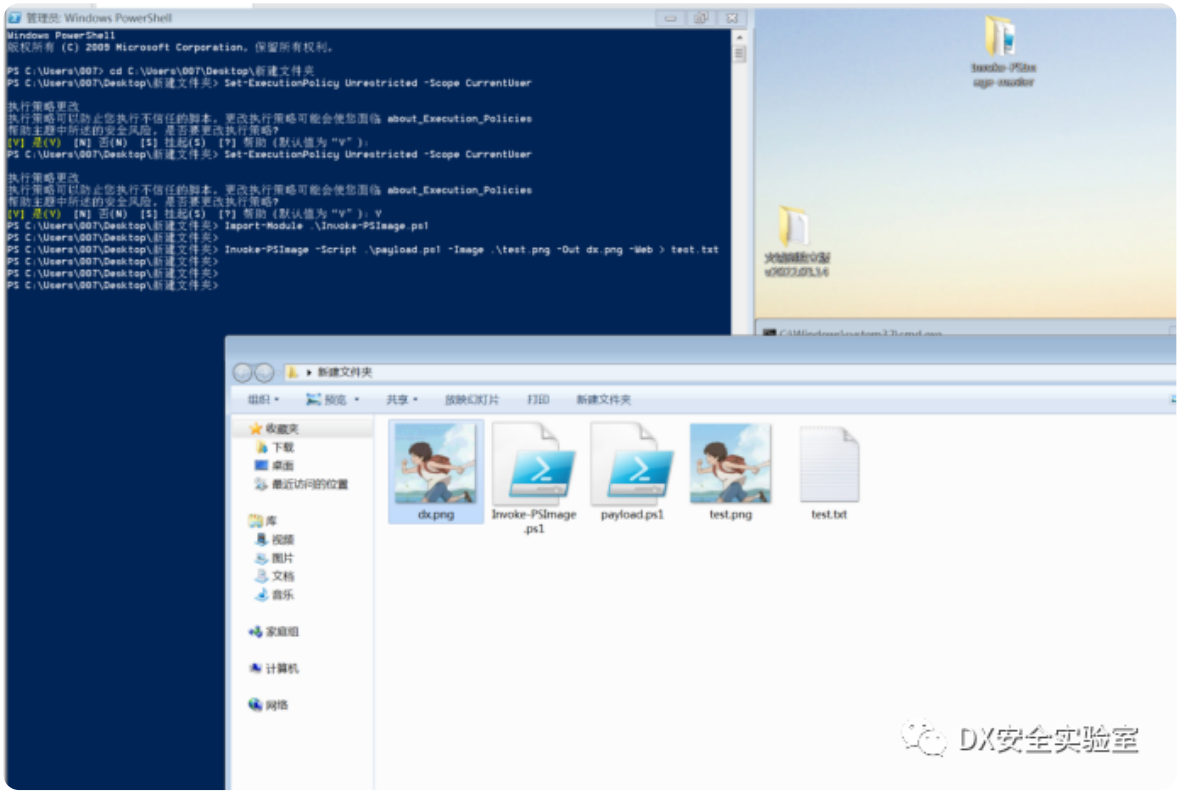
实验概述：由于涉及到敏感的绕过技术， 所以实施过程部分细节未写详尽，望理解

Part2过程

0x01：使用cs生成一个 Powershell 类型的shellcode



用Invoke-PSImage， 去将生成的shellcode写入到图片里面



设置执行策略:

```
Set-ExecutionPolicy Unrestricted -Scope CurrentUser
```

导入Invoke-PSImage文件:

```
Import-Module .\Invoke-PSimage.ps1
```

生成带有 Shellcode 的图片,并且将输出到test.txt：

```
Invoke-PSImage -Script .\payload.ps1 -Image
.\test.png -Out .\dx.png -Web> test.txt
```

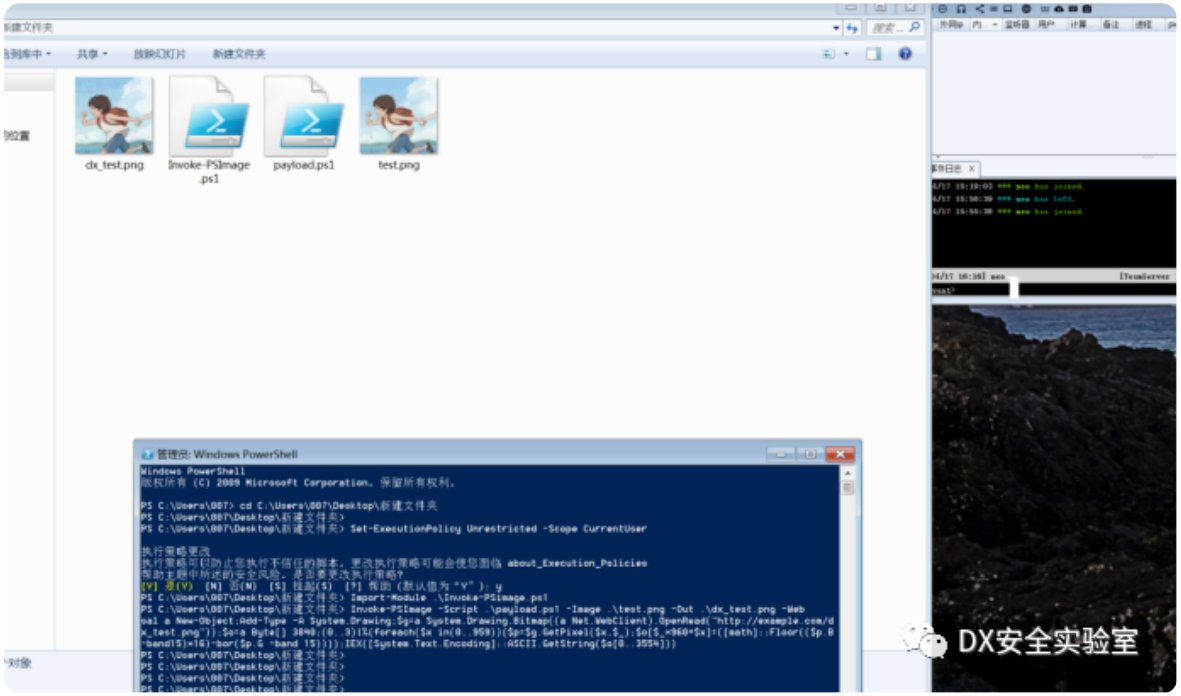
-Script为要转化为图片马的powershell脚本

-Image是一张正常的图片

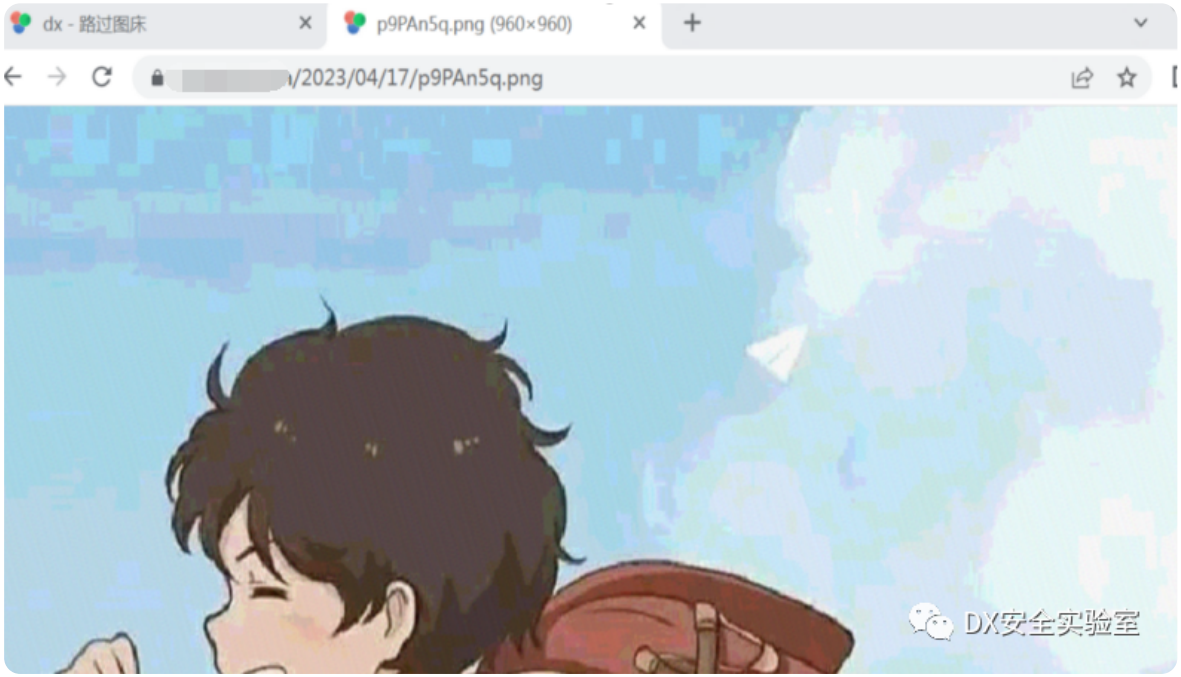
—Out生成的带图片的shellcode

——web将读取的命令显示出来

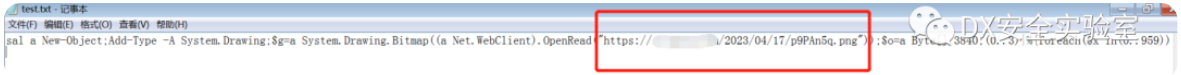
>test.txt将读取的命令放到test.txt里面去，方便修改复制



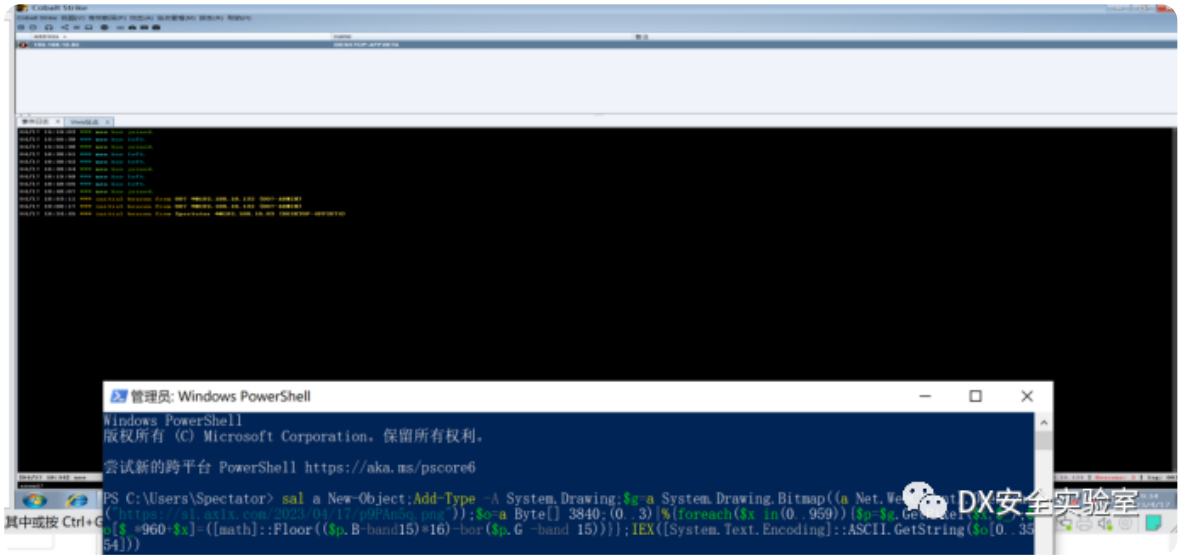
可以把带有shellcode的图片传到一些并上传至存放图片的公共图床中，甚至是任意网站上（网站头像处、百度图片等）



在生成的Powershell的命令里面替换一下自己的图片地址

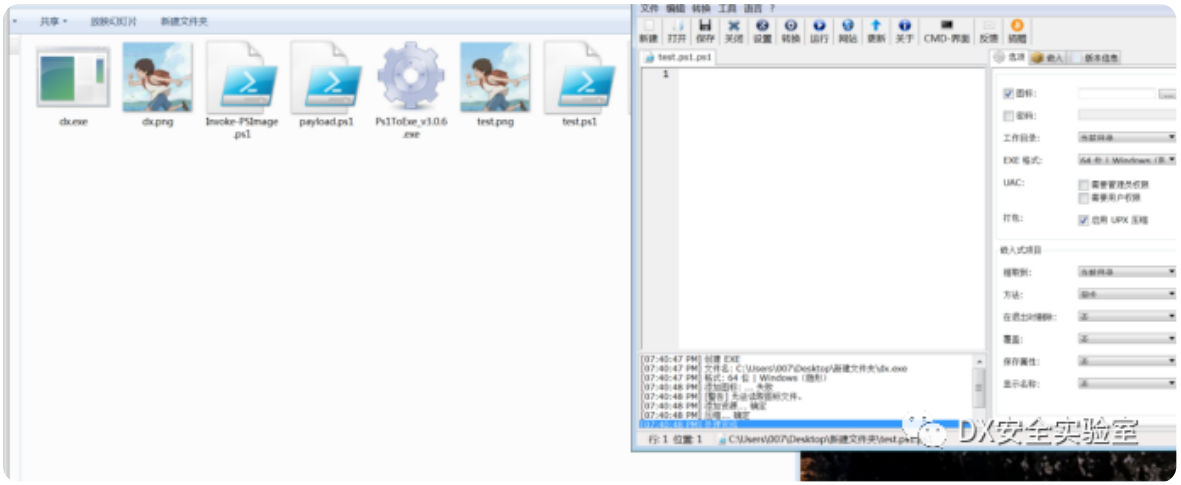


打开powershell运行代码，成功上线

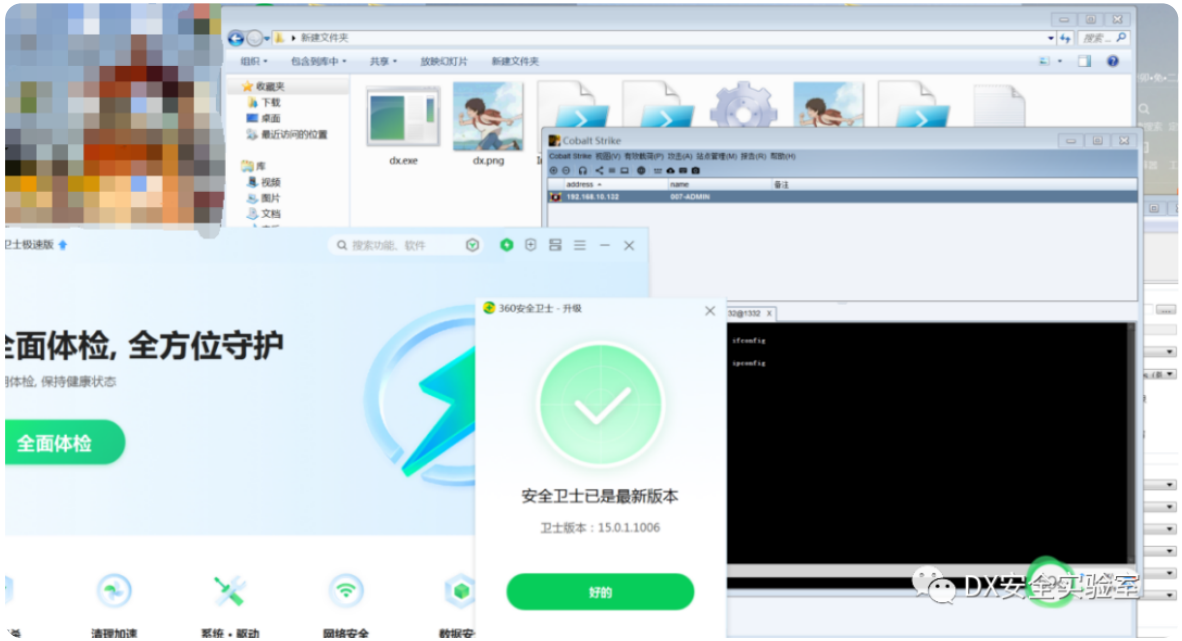


编译成可执行文件

使用Ps1 To Exe 将上面那段加载的命令编译生成可执行文件

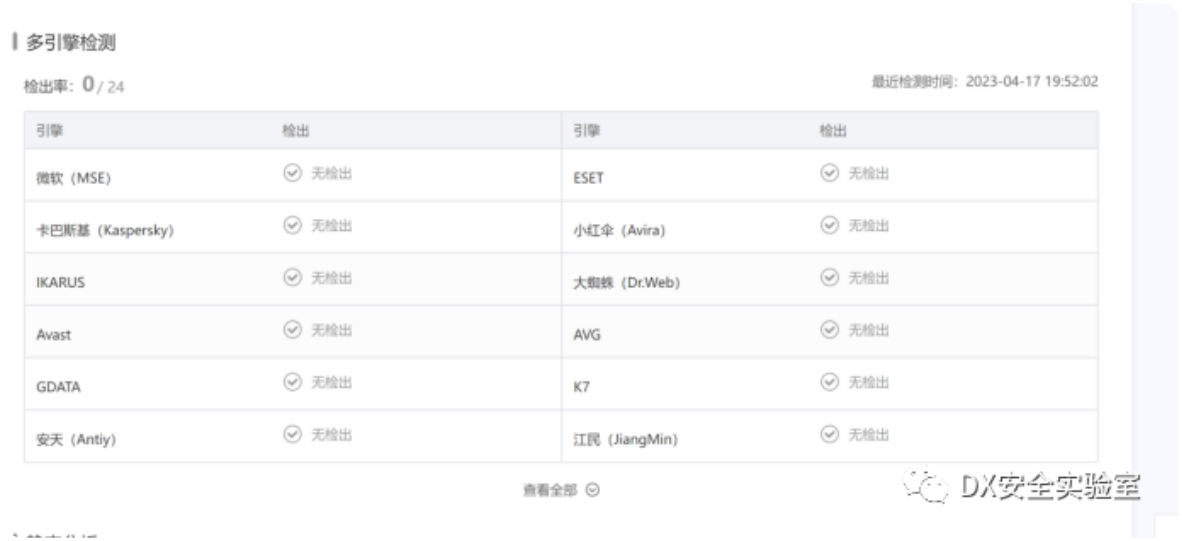


Ok，可以看到已经编译成了.exe的windows可执行文件，运行一下看看



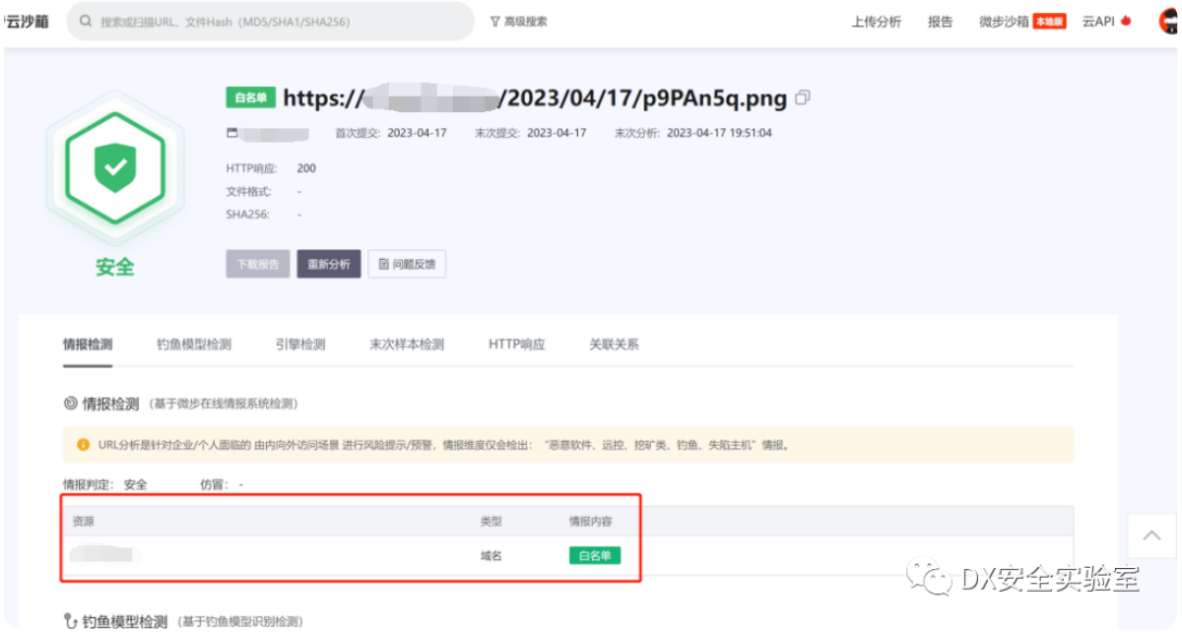
上线也没问题

云沙箱 shellcode图片文分析概况：



图片url分析概况：

可以看到shellcode文件地址处于威胁情报中的白名单



Part3总结

在整个过程中，powershell加载程序并不存在恶意代码，所以杀软和edr无法检出；shellcode从远程图片上面动态获取，整个过程无任何恶意文件落盘，所有操作均在内存中处理完成，所以成功绕过绝大多数的杀毒引擎，并通过计划任务达到持久稳定运行的目的。

“D&X 安全实验室”

专注渗透测试技术

全球最新网络攻击技术