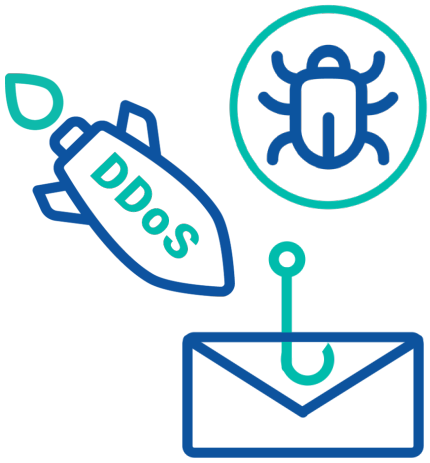
Attack Library
攻击库



确保网络安全&弹性

- ✓ 超过10,000个关键攻击、恶意软件和CVE的资料库
- ✓ 始终对新的和不断变化的威胁进行更新
- ✓ 混合有效的应用流量和恶意攻击
- ✓ 衡量网络安全设备的性能
- ✓ 为网络靶场生成现实的威胁场景
- ✓ 构建和维护具有抗威胁能力的网络

Apposite的攻击库由我们专业的安全团队持续更新，包括新的和不断发展的网络威胁

概览

Apposite的攻击库是一个最新的、不断发展的库，包括病毒、恶意软件和其他攻击的10k+网络安全威胁，用于全面的网络安全测试。

通过大规模模拟真实世界的攻击，企业可以优化下一代防火墙等安全设备，验证DDoS防御，提高安全性能，并确保网络的弹性。

将Apposite攻击库与我们的AppStorm和AppPlayback解决方案一起使用，可同时生成恶意攻击和合法应用流量，创造最真实和有效的测试环境。

我们独特的设计包括一个直观的搜索引擎，使您能够轻松地搜索和配置特定测试场景的确切攻击组合。模拟被攻击的设备和指挥中心，然后使用我们的向导驱动的测试配置过程，在短短的几个步骤中选择攻击的速率、长度和规模。

威胁类别

Viruses:在可执行文件和文件类型中发现的病毒和恶意软件。可执行文件和文件类型。
Spyware: 指挥与控制（C2C）活动。间谍软件从受感染的用户那里收集数据并与远程攻击者进行通信。
Ransomware: 来自恶意软件的流量 在支付赎金之前对文件进行加密。
Vulnerabilities: 攻击者可以利用的应用程序、网络和设备中的系统缺陷。
Backdoor: 绕过安全措施的攻击，以获得对一个应用程序或网络的根的未经授权的访问。
CVEs:由Mitre和其他公司维护的目录中公开披露和提供的常见漏洞利用。
Denial of Service (DoS): 使目标系统不可用的攻击，暂时破坏系统和依赖的应用程序和服务。
Fuzzing: 在源代码中插入大量的随机数据以发现漏洞的自动化过程。
Zero-day Attacks:利用供应商或用户未知的软件漏洞的攻击。

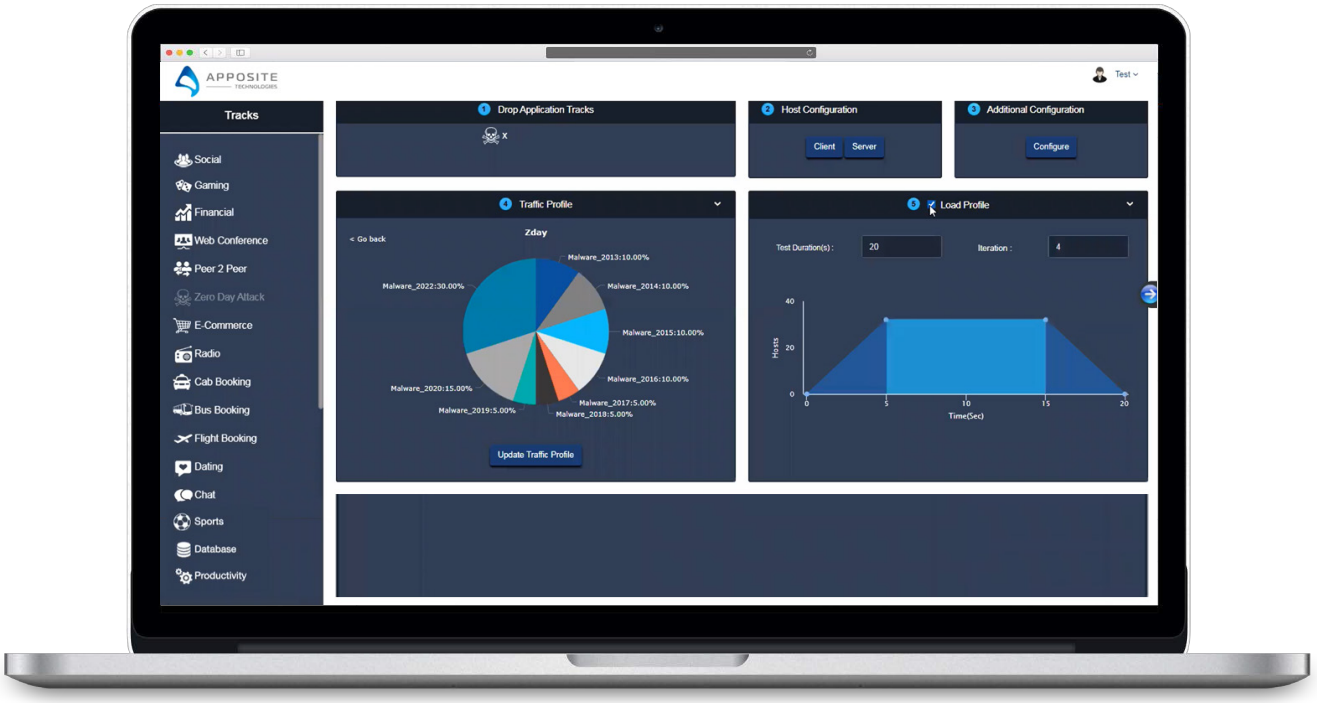
产品性能

Apposite的攻击库由一个专门的安全团队提供支持，该团队不断研究最新的漏洞、威胁和攻击方法，以确保我们的解决方案始终是最新的。通过每月发布更新，攻击库提供了保护您的网络和设备免受不断变化的网络安全威胁所需的最先进的情报。我们的图书馆包括超过10,000次攻击--而且还在不断增加--以及数以千计的真实世界应用流量，从社交媒体到商业经济、VoIP和金融服务。

使用攻击库与我们的AppStorm和AppPlayback解决方案，你可以：

- 强化安全防御措施，衡量网络和安全设备的性能
- 建立能抵御网络攻击的网络和基础设施
- 同时产生合法的应用流量和恶意攻击，以衡量应用感知设备和网络的性能
- 验证DoS防御，防止零日攻击，并提高攻击准备度
- 优化安全设备和系统，如下一代防火墙、IPS和IDS系统，以及SD-WAN网关
- 模拟大规模僵尸网络攻击，对你的网络进行压力测试，发现隐藏的弱点
- 模拟真实的流量场景，以获得最佳的网络靶场培训环境
- 提供一个永远在线的用户体验
- 从1000个预定义的应用流中选择视频流、社交媒体、SaaS、电子商务、金融、游戏、聊天、网络会议和其他许多应用。
- 捕获您的精确生产网络流量，并以巨大的规模进行回放

用户界面



特征

Apposite的攻击库与我们的流量生成解决方案无缝集成，提供无与伦比的易用性。AppStorm和AppPlayback都在同一平台上运行，并共享相同的现代、向导驱动的测试配置过程，使您能够利用授权流量和攻击库中的恶意攻击快速设置复杂的测试。

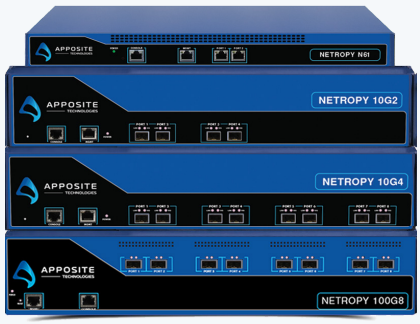
- 配置攻击，使其按顺序或平行运行
- 如果攻击在第一次尝试时被阻止，通过设置重试来模拟暴力攻击
- 通过设置每秒的数据包来控制攻击的速度
- 配置2013年以来每年CVEs的恶意软件的百分比
- 模拟被攻击的设备和指挥中心
- 使用我们直观的搜索引擎，根据供应商名称、CVE编号或攻击类型轻松搜索特定的CVEs
- 指定攻击的持续时间和使用负载配置文件的周期数量
- 通过我们的离线分析器，实时或在测试完成后查看每个应用程序和每个攻击的统计数据
- 捕获端口级别的统计数据，如传输的总数据、吞吐量、每秒的数据包和延时

支持的SPYWARE类型	
Adware	显示可能不需要的广告的程序。一些广告软件修改浏览器，突出显示和超链接网页上最常搜索的关键词。这些链接将用户重定向到广告网站。广告软件还可以从命令和控制（C2）服务器检索更新，并将这些更新安装在浏览器或客户端系统上。
Autogen	这些基于有效载荷的签名检测命令和控制（C2）流量并自动生成。
Backdoor	允许攻击者获得对系统的未经授权的远程访问的程序。
Botnet	僵尸网络是由攻击者控制的被恶意软件感染的计算机（"僵尸"）组成的网络。攻击者可以集中指挥僵尸网络中的每台计算机同时进行协调行动（例如，发动DoS攻击）。
Browser Hijack	浏览器劫持者可能会接管自动搜索或跟踪用户的网络活动，并将这些信息发送到C2服务器。
Cyptominer	恶意程序产生的下载尝试或网络流量，旨在利用计算资源，在用户不知情的情况下挖掘加密货币
Data Theft	一个系统向一个已知的C2服务器发送信息
DNS Security	连接到恶意域的DNS请求
Hacktool	由软件工具产生的流量，用于进行侦察，攻击或获得对脆弱系统的访问，渗出数据，或创建一个命令和控制通道，未经授权偷偷地控制计算机系统
Keylogger	键盘记录器使用各种C2方法，定期向预定的电子邮件地址或C2服务器发送日志和报告。通过键盘记录器的监视，攻击者可以检索到能够访问网络的凭证
Networm	能自我复制并从一个系统传播到另一个系统的程序。网络蠕虫可能使用共享资源或利用安全故障来访问目标系统
Phishing	钓鱼网站诱使用户提交凭证，攻击者可以窃取这些凭证以获得对网络的访问
Spyware	外向型C2通信

支持的漏洞类型	
Brute Force	强制签名表明活动发生的频率和速度是可疑的。例如，在短时间内许多失败的FTP登录可能表明攻击者试图用密码组合来访问FTP服务器
Remote Code Execution	远程代码执行（RCE）攻击允许攻击者在别人的计算机设备上远程执行恶意命令，就像他们是登录的用户一样
Code Obfuscation	经过改造的代码，在保留其功能的同时隐藏了某些数据。被混淆的代码很难或不可能被阅读，因此不清楚该代码正在执行什么命令，或与哪些程序进行交互
DoS	拒绝服务（DoS）攻击是指攻击者试图使一个目标系统不可用，暂时破坏系统和依赖的应用程序和服务
Exploit Kits	攻击套件的登陆页面通常包含几个攻击，针对一个或多个常见的漏洞和暴露（CVE），适用于多个浏览器和插件
Overflow	溢出漏洞是指缺乏对请求的适当检查，可被攻击者利用。一个成功的攻击可能会导致远程代码执行，并获得应用程序、服务器或操作系统的权限。
Phishing	当用户试图连接到一个钓鱼网站的登陆页面（可能是在收到带有恶意网站链接的电子邮件后）。钓鱼网站诱使用户提交凭证，攻击者可以窃取这些凭证以获得对网络的访问。
Protocol Anomaly	协议异常是偏离标准和合规使用的协议行为。例如，一个畸形的数据包，写得不好的应用程序，或在非标准端口上运行的应用程序，都被认为是协议异常，可以作为规避工具使用。
SQL Injection	一种常见的黑客技术，攻击者在应用程序的请求中插入SQL查询，以便从数据库中读取或修改。这种类型的技术经常被用于那些没有全面净化用户输入的网站。

支持的病毒类型
Malicious APK (Android)
Malicious DMG (Apple)
Flash
Java-class
Macho (Mach Object files) for Mac
Office
PDF
便携式可执行文件（PE），如： • 对象代码，字体(FONs) • 系统文件 (SYS) • 驱动程序文件 (DRV) • 窗口控制板项目(CPLs) • DLLs (动态链接库) • OCXs（OLE自定义控件或ActiveX控件的库）SR • Cs(可用于执行其他文件的脚本) • 可视化固件接口（EFI）文件 • 程序信息文件（PIFs）

Netropy流量生成器解决方案



Netropy流量生成解决方案可用于高性能设备和虚拟机（VMWareESXi, KVM, Openstack）。在一个现代的、基于浏览器的用户界面上轻松配置测试，或使用全面的RESTfulAPI来提高自动化程度。一次性运行多个测试，并使其在后台运行，与你的团队协作，并从任何地方轻松连接和执行测试。

Apposite的Netropy流量生成解决方案可与Apposite的Netropy网络仿真器完全集成，以创造最终的真实世界测试环境。

虹科电子科技有限公司

电话：400-999-3848
邮箱：hocyber@hkaco.com

广州 | 北京 | 上海 | 西安 | 成都 | 苏州 | 香港 | 台湾 | 美国硅谷