“防弹”主机服务提供商：网络犯罪基础设施的防线出现裂痕

网络犯罪分子的得逞依赖于安全、隐蔽且强韧的基础设施。每一次网络入侵、凭证被盗、勒索软件攻击、数据被盗并在非法论坛上出售的背后，都隐藏着为网络犯罪分子的行动和隐匿提供便利的基础设施。

然而，对于网络犯罪分子来说，保持隐蔽和难以追踪正变得越来越具有挑战性。各国政府、执法部门和私营部门之间的全球合作正在让网络犯罪分子在网上保持匿名变得更加困难。此外，具备自行管理和维护安全基础设施所需技能与专业知识的网络犯罪分子少之又少。因此，他们会寻找非法的基础设施提供商，由其代为提供此类服务，使网络犯罪分子能够专注于攻击受害者并牟利

“网络犯罪即服务”（Cybercrime-as-a-service）指的是为各类恶意网络行为者提供支持而发展起来的地下市场。这个地下市场包含日益增多且不断演变的可供购买的工具、服务和信息，帮助网络犯罪分子对线上目标实施攻击。潜在的网络犯罪分子可以购买网络访问权限、购买帮助其规避安全防护措施的工具，还可以购买恶意软件来攻击受害者并窃取个人信息。防弹主机（BPH）服务提供商是该生态系统的一部分，为网络犯罪分子提供安全的基础设施。重要的是，一个BPH服务提供商就可以直接让数百名网络犯罪分子能够针对全球范围内的受害者发起攻击。

什么是“防弹”主机服务提供商？

简单来说，BPH 服务提供商向网络犯罪分子出租虚拟和/或实体基础设施，供其开展犯罪活动。BPH 服务提供商是一类特殊的互联网基础设施服务，允许恶意行为者（包括网络犯罪分子）将非法内容托管在其主机上，并通过互联网开展相关活动。

“防弹”这个术语纯粹是一种营销说法。实际上，这些服务与其他基础设施提供商一样容易遭到打击。不过，BPH 服务提供商拒绝配合执法部门及其他内容下架请求，并无视受害者针对滥用的投诉和订阅者发出的请求通知。这意味着网络犯罪分子可以进行通信、运行非法论坛和网站、部署恶意软件和网络钓鱼活动，以及进行洗钱，而无需担忧运营商会因执法部门的要求或其他要求而终止其租约。

BPH 服务提供商明知故犯地参与网络犯罪生态系统，助长了以经济为目的的严重的网络犯罪。影响澳大利亚组织及其客户的重大网络安全事件都是由于犯罪分子利用了BPH 服务提供商而发生的。这些事件的后果包括破坏性的勒索软件攻击、数据勒索和敏感信息盗窃。

以下为地下论坛中某个防弹主机服务提供商的广告示例：

BPH 服务提供商是如何运作的？

不同BPH服务提供商的业务模式各不相同。最常见的方式是向网络犯罪分子客户出租IP地址，并采用复杂的网络交换方法来帮助掩盖他们的位置、身份和活动。在许多情况下，BPH服务提供商会从其他合法的主机服务商、数据中心或互联网服务提供商（ISP）处转售或租赁IP地址和服务器。这些“上游”服务提供商可能并没有意识到他们正在向BPH服务提供商提供基础设施，而后者再向网络犯罪分子提供“下游”服务。

BPH服务提供商会对其网络和系统架构进行配置，以增加识别其客户的难度。例如，他们经常更改与客户活动相关的面向互联网的标识符——例如分配给他们的IP地址和域名。这类手段使得将某一事件与行为者或客户在任何特定时间使用的 IP 地址联系起来变得更加困难，因此给防御者和调查人员带来了挑战。此外，BPH服务提供商通常会使用网络制度宽松的国家的基础设施，这些国家要么没有正式的措施来调查和预防恶意网络活动，要么这些措施较为宽松。

针对 BPH 服务提供商的打击如何影响网络犯罪威胁

BPH服务提供商为一次性打击数百至数千名网络犯罪分子提供了宝贵的机会。许多网络犯罪分子和其他恶意网络行为者使用这些服务来使他们的犯罪行为更加容易——他们相信，在面临下架请求或滥用投诉时，他们的活动依然能够保持隐蔽并持续运作。

然而，执法部门、政府机构和私营部门正在合作针对并打击这些非法的基础设施提供商，包括采取防御措施，例如主动封锁来自已知BPH服务提供商的互联网流量。这些活动有助于减少与澳大利亚及其盟友网络互动的网络犯罪数量，其中包括那些可能在不知情的情况下帮助BPH服务提供商接入互联网并为网络犯罪分子提供安全基础设施的合法“上游”基础设施提供商和互联网服务提供商（ISP）。

BPH服务提供商并非“网络犯罪即服务”生态系统中唯一的一类基础设施提供商。这些服务通过积极支持网络犯罪活动并故意阻碍合法调查和应对措施，持续助长并促成了针对澳大利亚的网络犯罪威胁。针对 BPH服务提供商采取行动，能够揭示这些服务的弱点以及利用它们的恶意网络行为者。