lvxing

Botnet

僵尸网络911 S5的数字遗产

概述 2024年5月29日，美国司法部发布通告，声称其执法活动摧毁了"史上最大的僵尸网络" 911 S5，查封了相关域名，并且逮捕了其管理员YunHe Wang。Wang及其同伙通过创建并分发包含恶意代码的免费VPN程序感染用户，并且在名为911 S5的住宅代理服务中出售对被感染设备构成的代理网络的访问权。 按照360威胁情报中心的分析，911S5从2014年开始运营，到2022年7月关停，在2023年10月又摇身一变，化名CloudRouter继续其肮脏生意，终于在2024年5月被多国联合执法摧毁。911S5的僵尸网络运行时间长、涉及多个国家的19M个IP地址、行为高调，虽然经过执法行动后大势已去，但是其数字遗产仍然对网络空间构成了现实且显著的威胁，下文是我们对威胁分析的结果。 “空手套白狼”的911 S5 911S5出售的代理服务背后是数千万被感染的设备。受害者主动或被动下载捆绑了恶意代码的软件、免费VPN程序等。在程序启动后，恶意代码将会创建持久化服务作为后门，为911S5客户提供代理服务。 在2023年以前，911S5使用的免费VPN包括:ProxyGate、Mas

· Jun 14, 2024 · 7 min read