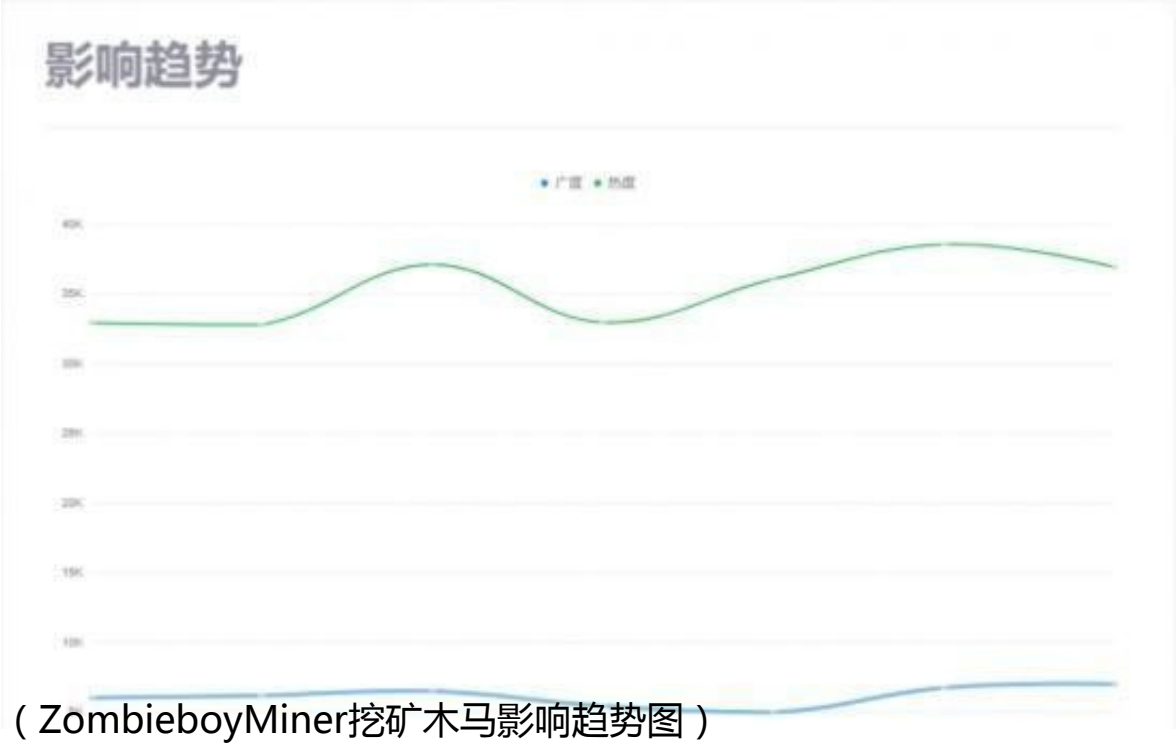
随着区块链技术的快速发展，以比特币为首的数字货币造就了一大批挖矿者的致富神话。在市场增速不断加快的背景下，不法黑客将目光锁定非法挖矿产业，也想趁机分一杯羹。近日，腾讯御见威胁情报中心监测到，不法黑客利用ZombieboyTools进行传播挖矿木马的最新活动。据了解，不法黑客对公开的黑客工具ZombieboyTools进行修改，利用NSA攻击包对用户网络进行攻击，植入挖矿及远程访问控制木马，对用户网络安全造成严重威胁。



（ZombieboyMiner挖矿木马影响趋势图）

据安全专家介绍，ZombieboyMiner挖矿木马运行后，将释放端口扫描工具、NSA利用攻击工具，以及payload程序到用户电脑。其入侵路径是先利用端口扫描工具，扫描局域网中开放445端口的机器，再通过NSA利用攻击工具，将payload程序注入到局域网内尚未修复MS17-010漏洞的机器，进而开展挖矿、远程控制等木马行为。

值得注意的是，ZombieboyMiner挖矿木马通过Las.exe程序释放svsohst.exe启动门罗币挖矿程序，使用注册的二级C2域名进行自建矿池挖矿门罗币。同时，该木马还会在“中招”电脑中植入远程控制木马程序，搜集用户敏感信息上传至木马服务器，给用户的信息安全带来威胁。目前，受ZombieboyMiner挖矿木马感染的电脑在全国各地均有分布，广东、江苏、浙江三省位居前三位。

（腾讯企业级安全产品御点）

据悉，腾讯智慧安全御点终端安全管理系统现将百亿量级云查杀病毒库、引擎库以及腾讯TAV杀毒引擎、系统修复引擎应用到企业内部，可有效防御企业内网终端的病毒木马攻击。同时，御点还具备终端杀毒统一管控、修复漏洞统一管控，以及策略管控等全方位的安全管理功能，可帮助企业管理者全面了解、管理企业内网安全状况、保护企业网络信息安全。
