

liuyang

en

New Threat: ZHtrap botnet implements honeypot to facilitate finding more victims

Overview In the security community, when people talk about honeypot, by default we would assume this is one of the most used toolkits for security researchers to lure the bad guys. But recently we came across a botnet uses honeypot to harvest other infected devices, which is quite interesting. From



• Mar 12, 2021 • 11 min read

New Threat

新威胁：ZHtrap僵尸网络分析报告

ZHtrap，本文对其做一分析，文章要点如下：1. ZHtrap的传播使用了4个Nday漏洞，主要功能依然是DDoS和扫描，同时集成了一些后门功能。2. Zhtrap能将被感染设备蜜罐化，目的是提高扫描效率。3. Zhtrap感染受害主机后会禁止运行新的命令，以此实现彻底控制和独占该设备。4. 在C2通信上，ZHtrap借鉴了套娃，采用了Tor和云端配置。ZHtrap全情介绍 ZHtrap的代码由Mirai修改而来，支持x86, ARM, MIPS等主流CPU架构。但相对Mirai，ZHtrap变化较大，体现在如下方面：* 在指令方面，加入了校验机制 * 在扫描传播方面，增加了对真实设备和蜜

 · Mar 12, 2021 · 15 min read

en

New Threat: Matryosh Botnet Is Spreading

Background On January 25, 2021, 360 netlab BotMon system labeled a suspicious ELF file as Mirai, but the network traffic did not match Mirai's characteristics. This anomaly caught our attention, and after analysis, we determined that it was a new botnet that reused the Mirai framework, propagated through

 · Feb 2, 2021 · 8 min read

DDoS

新威胁：能云端化配置C2的套娃（Matryosh）僵尸网络正在传播

版权声明：本文为Netlab原创，依据 CC BY-SA 4.0 许可证进行授权，转载请附上出处链接及本声明。背景 2021年1月25日，360网络安全研究院的BotMon系统将一个可疑的ELF文件标注成Mirai，但网络流量却不符合Mirai的特征。这个异常引起了我们的注意，经分析，我们确定这是一个复用了Mirai框架，通过ADB接口传播，针对安卓类设备，主要目的为DDoS攻击的新型僵尸网络。它重新设计了加密算法，通过DNS TXT的方式从远程主机获取TOR C2以及和C2通信所必须的TOR代理。这个僵尸网络实现的加密算法以及获取C2的过程都是一层层嵌套，像俄罗斯套娃一样，基于这个原因，我们将它命名为Matryosh。每天都有脚本小子拿着Mirai的源码进行魔改，想着从DDoS黑产赚上一笔。Matryosh会是这样的作品吗？随着分析的深入，更多细节浮出水面，根据C2指令的相似性，我们推测它是当下非常活跃的Moobot团伙的又一个尝试。Matryosh没有集成扫描，漏洞利用的模块，主要功能为DDoS攻击，支持 tcpraw, icmpecho,

 · Feb 2, 2021 · 10 min read

