Agatha 纯净生存服务器

1 月 29 日非官方压力测试攻击

分析报告

一、事件概要

2023 年 1 月 29 日下午，Agatha 纯净生存服务器（正线）遭到大批量 Minecraft Bot 压测。

二、详细经过

当天 13:27:22，第一个 Bot 进入服务器，此后直到 13:30:22，共有 Bot 请求 1376 次，其中 1316 次命中运营商金盾防火墙，但没有被拦截。根据数据包记录，Bot 进服后会在服内快速移动刷取区块，因此在 13:27:29 系统启用了限速。13:30:22 起直到 13:31:55，Fiona 系统启动应急处理，将 Bot 移出服务器。

截至 13:31:59，Fiona 系统以 DMS-CCE-4903（非人类请求）移除了 Bot 总计 19941 次。

13:32:19，服务器软件系统启动 AntiBot 模式，程序通报硬件防火墙，金盾系统开始全量清洗海外请求。

13:33:04，值班管理员登录后台重新挂载磁盘，清除了任务负载。

13:34:50，最后一只 Bot 离开服务器。

三、应急处置

硬件系统（金盾）拦截总数	23508
软件系统（AntiBot / Fiona）拦截总数	351
后期分析 Bot 总次数	24119

13:27:22，Fiona 程序控制金盾系统开展清洗，13:34:55 结束。

四、数据分析

根据后期数据分析发现：

1. 攻击呈现明显的两批次，第一批以随机命名的一串字母数字组合为用户名，在攻击开始时频繁加入服务器，并成功触发金盾。第二批次以正版用户名为组合，因金盾风控未解除，第二批被以接近 100%的成功率拦截。
2. 攻击 IP 地址总量超过 5,000，并以海外 IP 为主，导致攻击效果极差。
3. 攻击为程序操纵肉鸡触发，余量收尾用时 17 秒左右，收尾效果差，流量洪峰时间短，显著低于该产业平均水平。
4. 攻击会触发磁盘系统文件限制，导致 Bot 无法正常进服刷图。
5. 攻击无法欺骗 Fiona 系统，导致后台快速接入人工处理。

根据 IP 地址数据库发现：

1. 攻击 IP 地址以东南亚国家为主，缺少中国大陆境内访问，可以通过封控海外访问请求解决。
2. 攻击 IP 地址以 IDC 为主，可以通过特定运营商屏蔽规则解决。
3. 攻击 IP 未做伪装，直接命中金盾风控库，与 Fiona 云数据接近 70%吻合。
4. 攻击 IP 有军用地址。

五、溯源处理

本次攻击的数据已转交托管机房溯源风控处理。