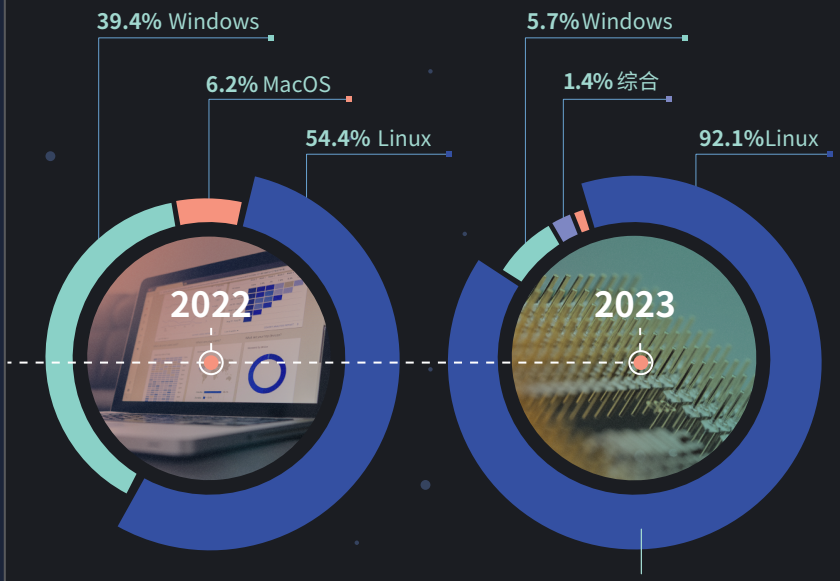
elastic security labs

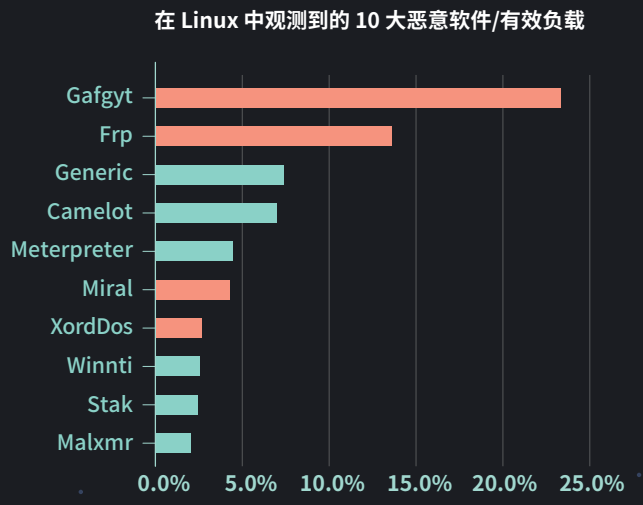
# 《2023 年 Elastic 全球威胁报告》中观测到的对手方法

我们的报告源于对超过 **10 亿个数据点**的分析

## Linux 基础架构引起对手的关注

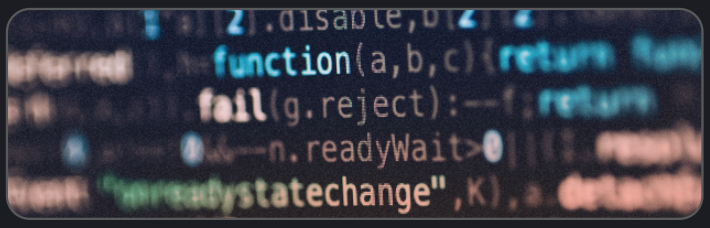



对 Linux 服务器的依赖导致恶意软件信号大幅增加。




在这个操作系统中，僵尸网络非常流行；在所观测到的 Linux 攻击中，约有 **44%** 利用了连接。

## 终端中对防御规避的依赖表明了对反制环境的适应性



在所有终端中观测到的 **MITRE ATT&CK** 战术

| | HITS |
|---|---|
| 防御规避 | 43.88% |
| 执行 | 29.20% |
| 持久化 | 7.98% |
| 权限提升 | 6.93% |
| 凭据访问 | 5.60% |

对手利用 **BYOVD** 等操作系统设计缺陷来避开检测。

## 对手在云环境中利用凭据访问技术成功实施了攻击

在云服务提供商中观测到的 **MITRE ATT&CK** 战术

| | 信号 % |
|---|---|
| 凭据访问 | 44.98% |
| 防御规避 | 23.02% |
| 执行 | 11.58% |
| 发现 | 6.04% |
| 持久化 | 5.81% |

易于收集或缺乏对冒用的可见性，因此使用这种方法可屡屡得逞。

## 通过《Elastic 全球威胁报告》了解威胁态势

深入了解我们对恶意软件签名、终端行为和云提供商的观测结果，并查看我们在《2023 年全球威胁报告》中给出的建议。在 X 上关注 Elastic Security Labs **@ElasticSecLabs**，并查阅我们的博客，以了解最新的威胁发展情况和研究等！