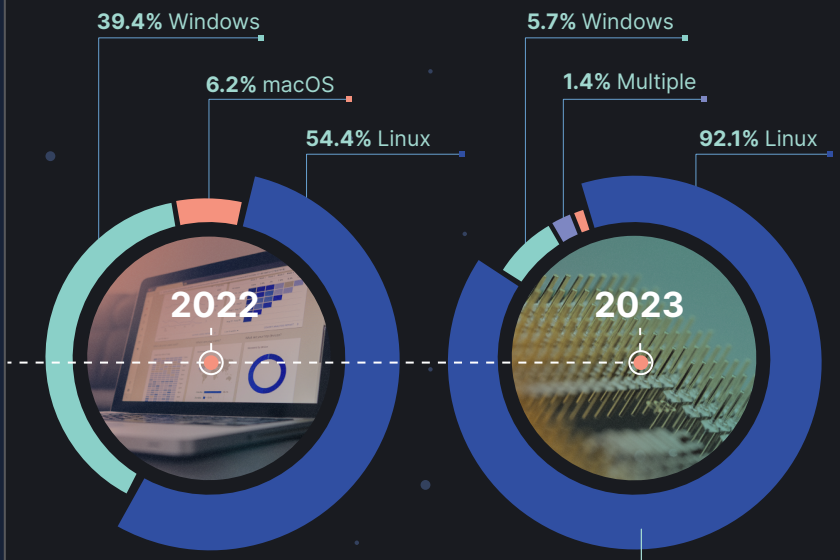
elastic security labs

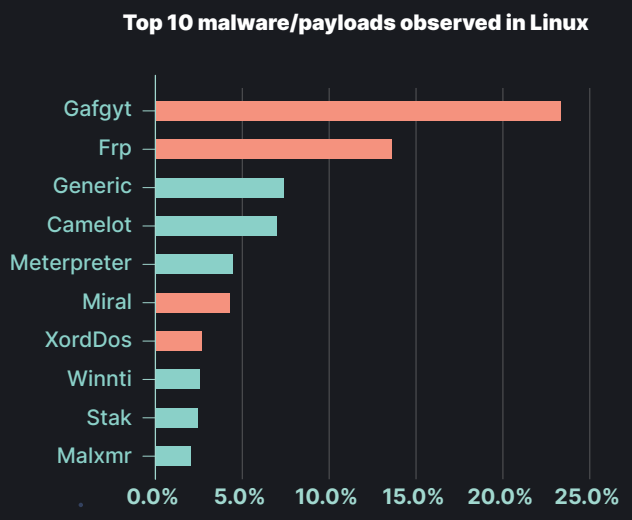
Adversary Methods in the 2023 Elastic Global Threat Report

Our report is derived from over **1 billion data points**

Linux infrastructure draws adversary attention

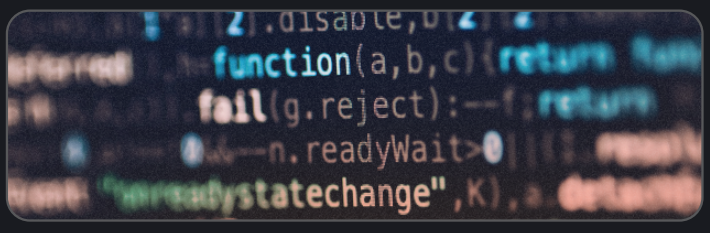


Reliance on Linux servers has resulted in a large increase in malware signals.



Botnets are popular within this OS, capitalizing on connectivity in **~44%** of Linux observed attacks

Reliance on Defense Evasion in endpoints indicates adaptation to hostile environments



MITRE ATT&CK tactics observed across all endpoints	**HITS**
Defense Evasion	**43.88%**
Execution	**29.20%**
Persistence	**7.98%**
Privilege Escalation	**6.93%**
Credential Access	**5.60%**

Adversaries are leaning on OS design flaws like **BYOVD** to prevent detection.

Adversaries are finding success with Credential Access techniques in cloud environments

MITRE ATT&CK tactics observed across cloud service providers	**Signal %**
Credential Access	**44.98%**
Defense Evasion	**23.02%**
Execution	**11.58%**
Discovery	**6.04%**
Persistence	**5.81%**

Ease of gathering or lack of visibility into fraudulent use make this method reliable.

Understand the threat landscape with the Elastic Global Threat Report

Drill deeper into our observations on malware signatures, endpoint behaviors, and cloud providers and see our recommendations in the 2023 Global Threat Report. Follow Elastic Security Labs on X **@elasticseclabs** and **check out our blog** for the latest threat developments, research, and more!