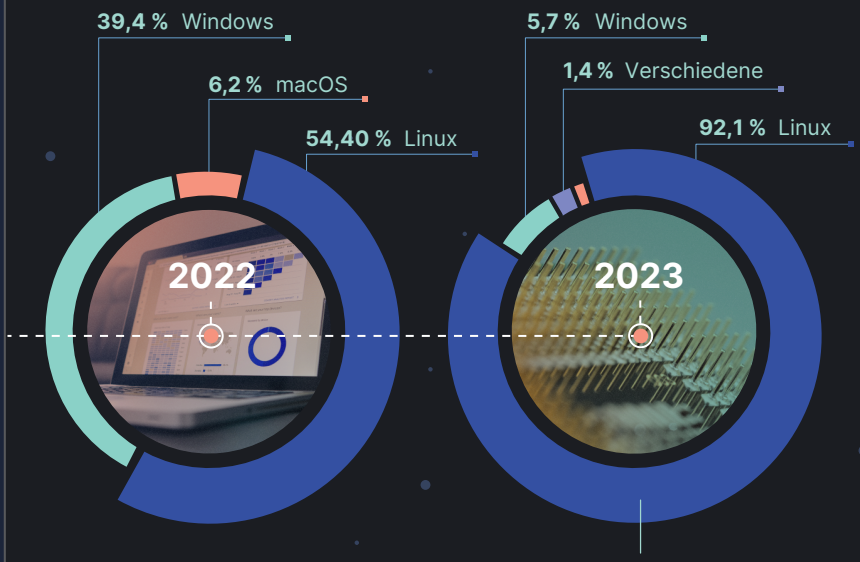
elastic security labs

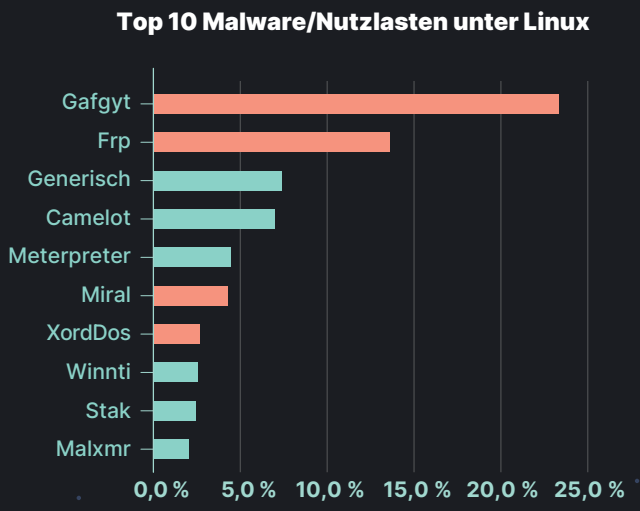
Angreifertechniken im Elastic Global Threat Report 2023

Unser Bericht beruht auf mehr als **einer Milliarde Datenpunkte**

Linux-Infrastrukturen im Fokus der Angreifer

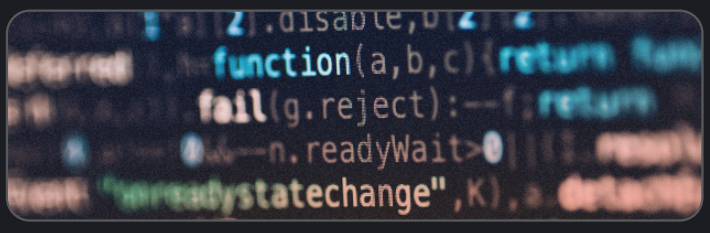


Der umfangreiche Einsatz von Linux-Servern Starker hat zu einem Anstieg an Malware-Signalen geführt.



Botnets sind unter diesem BS beliebt und nutzen die Konnektivität bei **ca. 44 %** der beobachteten Linux-Angriffe.

Der Einsatz von Tarnmechanismen auf Endpoints zeigt die Vertrautheit mit den angegriffenen Umgebungen.



Auf allen Endpoints beobachtete **MITRE ATT&CK**-Taktiken	**TREFFER**
Tarnung	**43,88 %**
Ausführung	**29,20 %**
Persistenz	**7,98 %**
Rechteausweitung	**6,93%**
Zugriff mit Anmeldeinformation	**5,60 %**

Angreifer nutzen BS-Designlücken wie **BYOVD**, um sich zu tarnen.

Angreifer nutzen immer häufiger Zugriffe mit Anmeldeinformation in Cloud-Umgebungen.

Bei Cloud-Dienstanbietern beobachtete **MITRE ATT&CK**-Taktiken	**% der Signale**
Zugriff mit Anmeldeinformation	**44,98 %**
Tarnung	**23,02 %**
Ausführung	**11,58 %**
Discovery	**6,04 %**
Persistenz	**5,81 %**

Zuverlässige Methode, weil Daten leicht zu beschaffen sind und Betrug oft nicht erkannt wird.

Bedrohungslandschaft kennenlernen mit dem Elastic Global Threat Report

Entdecken Sie unsere Beobachtungen zu Malware-Signaturen, Endpoint-Verhaltensweisen und Cloud-Anbietern und lesen Sie unsere Empfehlungen im Global Threat Report 2023. Folgen Sie den Elastic Security Labs auf X **@elasticseclabs** und lesen Sie unseren Blog über die neuesten Bedrohungsentwicklungen, Forschungsergebnisse und vieles mehr!