elastic security labs

2022 Global Threat Report

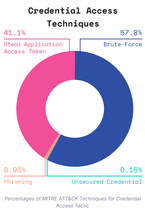
Infographic

Where are threats coming from?

Based on solution telemetry, the Elastic Security Labs' 2022 Global Threat Report reveals threat phenomena, trends, and recommendations to help organizations prepare for the future. Findings include...

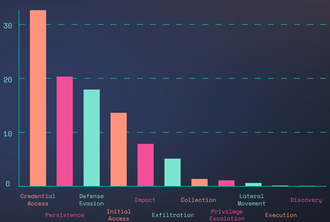
A secure cloud is one that rises above bad defaults

Nearly 41% of credential access alerts attempted to steal application access tokens versus other credentialed materials.



Percentages of MITRE ATT&CK Techniques for Credential Access Tactic

Once attackers are inside, credential access is priority one

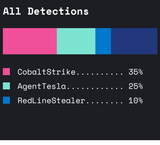


Percentages of total MITRE ATT&CK tactic names for cloud-based detection alerts

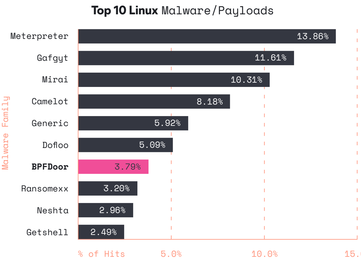
Commercial software is being weaponized

Malware designed for red teams is being used against organizations.

CobaltStrike was the most popular malicious binary or payload for Windows endpoints, followed by AgentTesla and RedLineStealer.

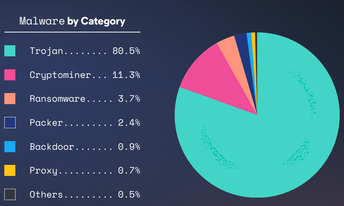


Linux isn't as secure as you think



Top 10 Linux malware and payloads depicting BPFDoor activity increasing

Trojans continue to be a favored way to weaponize deliverables



Good news – Endpoint security is working

Endpoint attacks are becoming more diverse in efforts to bypass defenses. This year we observed 50 different endpoint infiltration techniques that didn't work.

Technique	Signal Percentage
Masquerading	44.20%
System Binary Proxy Execution	30.00%
Access Token Manipulation	12.32%
Process Injection	7.02%
BITS Jobs	4.74%
Trusted Developer Utilities Proxy Execution	0.90%
XSL Script Processing	0.66%
Impair Defenses	0.65%
Exploitation for Defense Evasion	0.64%
System Script Proxy Execution	0.13%
Modify Registry	0.03%
Indicator Removal on Host	0.01%

Get full insight into Elastic Security Labs researchers' findings in the 2022 Global Threat Report