elastic security labs

2022 年全球威胁报告

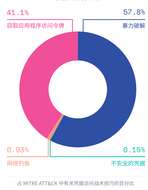
信息图表

威胁来自何处？

基于解决方案遥测数据，Elastic Security Lab 发布的《2022 年全球威胁报告》揭示了多种威胁现象和趋势，并相应提出了多项建议，旨在帮助组织为未来做好准备。研究结果包括……

当管理员手动实施比默认设置更多的安全控制时，真实环境中的云是最安全的

将近 41% 的凭据访问告警曾试图窃取应用程序访问令牌与其他凭据材料。

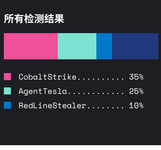


攻击者一旦进入内部，第一件事就是使用凭据进行访问

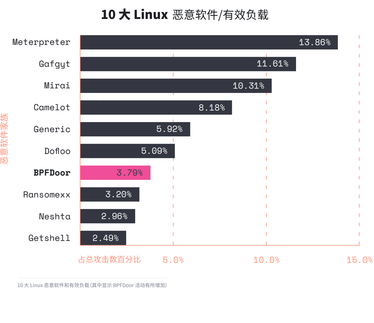
商务软件正在被改造为实施攻击的工具

为红队设计的恶意软件正在被用来攻击组织。

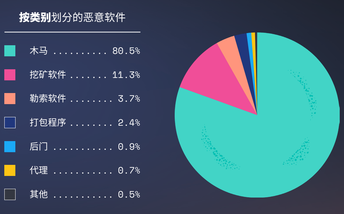
CobaltStrike 是 Windows 终端最常见的恶意二进制文件或有效负载，其次是 AgentTesla 和 RedLineStealer。



开源软件并不像大家想象的那么安全



木马仍然是一种利用交付物实施攻击的常用方式



好消息 — Endpoint Security 正在发挥作用

为了绕过防御措施，终端攻击方式变得越来越多样化。今年，我们监测到有 50 种不同的终端渗透技术没有取得成功。

技术	信号百分比
伪装	44.29%
系统二进制代理执行	30.00%
访问令牌操控	12.32%
进程注入	7.62%
BITS Jobs	4.74%
可信开发者实用程序代理执行	0.90%
XSL 脚本处理	0.66%
削弱防御	0.65%
防御规避利用	0.64%
系统脚本代理执行	0.13%
修改注册表	0.03%
移除主机指示器	0.01%

阅读《2022 年全球威胁报告》，全面了解 Elastic Security Labs 研究人员的研究结果