elastic security labs

2024

Elastic 全球威胁报告

SOC 领导者应了解的威胁趋势

旨在为安全团队和 CISO 等管理者提供切实可行见解的 2024 Elastic 全球威胁报告给出了对超过 10 亿个数据点进行数月分析后得出的重要结论，这些数据点来自公共和 Elastic 特定的遥测数据。基于总结出的要点，报告还提供了来自数据的见解和针对贵组织的行动建议。

首要洞见

01 各企业错误配置了云环境

我们关于云安全态势管理 (CSPM) 的新章节将环境与互联网安全中心 (CIS) 的基准进行了比较，发现平均约有 50% 的环境未能通过检查，该数据与云服务提供商 (CSP) 无关。

02 防御规避仍然是最常见的终端战术

防御规避占终端行为的 38%，这表明攻击者可以轻松穿越安全系统。值得注意的是，这一数字比去年下降了 6%，表明防御工具正在有效发挥作用。

03 凭据访问告警持续增加，特别是在云中

在云环境中，凭据访问活动占 23%。此外，终端环境显示使用这些技术的年同比增长率为 3%。这可归因于信息窃取者和凭据经纪人的日益盛行，以及安全工具的可见性日益增强的事实。

04 攻击者正在滥用防御工具以高效进入系统

在观察到的恶意文件中，有 53% 被认定为攻击性安全工具；企业利用这些工具来发现弱点，而攻击者则滥用这些工具实施攻击。这些攻击性安全工具拥有庞大的研发团队，以创建进程注入等新功能 — 这是一种防御规避形式，占今年 Windows 告警事件的 53%。

05 生成式 AI 没有增加我们观察到的攻击数量或影响

安全团队一直担心可能出现生成式 AI 攻击大爆发。虽然我们看到威胁数量略有增加，但生成式 AI 在很大程度上加强了防御技术，这主要得益于告警汇总和任务自动化等功能。

关键建议

01 经常审核您的环境

攻击者依靠宽松或错误配置的安全控制来渗透到环境中，一旦进入环境，他们就会着力篡改传感器和数据。基准测试和风险评估可帮助您确定是否采用了最佳实践和行业标准来有效控制企业内部的访问。

02 通过调整安全控制为生成式 AI 做好准备

生成式 AI 使用的增加将导致社交工程尝试的增加。虽然培训用户群识别此类尝试和其他攻击手段始终是个好主意，但安全团队也应该验证自己的控制措施和权限，以确保成功的网络钓鱼尝试不会造成长期损害。

03 实施交互式终端代理，化解防御规避攻击

防御规避攻击是近年来的主要战术。虽然呈下降趋势，但攻击者仍在利用这些方法来渗透和侵入环境。Elastic Agent 等终端技术能提供可见性和能力，同时减少所需的工具数量。

04 为暴露的凭据创建稳健的响应计划

我们观察到暴力破解和从可疑内存中访问浏览器凭据等技术经常被使用。轮换暴露的凭据并为泄露响应建立快速工作流将产生明显效果。如果还没有，安全团队现在应强制执行多因素身份验证。

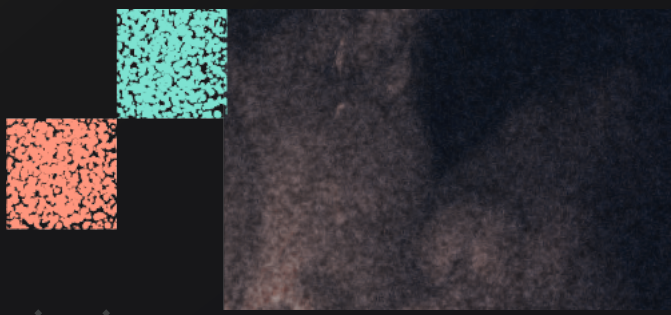
05 将您的云环境与 CIS 基准进行比较

CIS 基准是行业标准，可帮助您快速确定需要关注的领域。您的团队应制定一项计划来监控和提高您的得分，从长远来看，这将提高威胁检测能力并降低风险。

把握威胁态势

为此类及其他威胁的演变做好准备。获取我们的全部建议，并在 2024 Elastic 全球威胁报告中查看当今威胁形势的完整详述。您还可以关注我们的专家帐号 @ElasticSecLabs。

了解 Elastic Security 如何实现您安全运营的现代化。



elastic security labs