全球威胁研究报告

执行摘要

耐心、隐秘攻击的时代正在让位于高速威胁的新时代。

我们的年度分析揭示了一个明显的战略转变：对手正在转型以提高速度，利用 AI 武器化以大规模制造新型威胁，并优先考虑立即执行而非长期隐蔽。这种加速迫使防御者适应以分钟而非以月为单位的攻击生命周期，在这种情况下，从实时和历史数据中快速做出背景丰富的决策已成为有效防御的关键。

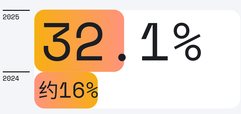
Elastic Security Labs 发布的《2025 年 Elastic 全球威胁报告》对这一新态势进行了剖析。

根据我们对全球威胁遥测的分析，我们已经确定了最重要的对手行为和防御创新。以下是您将学习的内容预览：

#01

Windows 上的攻击者优先级已经发生了变化

策略类别 **"执行"** 目前占恶意行为的 **32.1%**，其份额较先前的约 16% 翻了一番，并超过了 **防御规避** 成为最主要的策略。这打破了持续三年的趋势，表明战略重点已从初始隐蔽转向即时有效载荷部署。

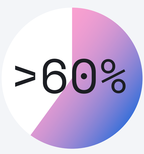


这对您意味着什么

→ 攻击者不再伺机隐藏，而是在进入后立即运行恶意代码。这使得运行时内存保护和防止初始访问比以往任何时候都更重要。

#02

云攻击面高度集中



超过 60% 的云安全事件 都可归结为三个攻击者目标：

攻击者目标

/初始访问
/持久化
/凭证访问

这对您意味着什么

→ 在所有主要云平台上，这种对 **基于身份的攻击** 的高度关注是一个明确的信号，即强化身份验证流程和监控异常特权访问是保护云工作负载的最有效方法。

#03

AI 武器化正在呈上升趋势

我们发现 **"通用"** 威胁增加了 **15.5%**，这一趋势很可能是攻击者利用 LLM 快速生成简单但有效的恶意加载程序和工具所致。

这对您意味着什么

→ AI 生成的威胁日益增多，这使得您所面临的恶意软件的数量和种类大幅增加。这意味着要减少对静态签名的依赖，更多地依靠 **行为分析和 AI 驱动的检测**，以自动识别并阻止大量新型威胁。

#04

窃取浏览器凭据是一笔大生意

我们对超过 **150,000 个恶意软件** 样本的分析显示，**超过八分之一的恶意软件旨在窃取浏览器数据。** 这些数据并非孤立使用；这些凭据是推动 **访问代理经济** 的原材料，为其他攻击者提供稳定的密钥供应，以危及企业云账户。

这对您意味着什么

→ 浏览器是组织中最敏感数据的主战场。信息窃取者已经适应了浏览器内置的保护措施，这意味着传统的身份控制手段已不再足够。

这些趋势是紧密相关的。

攻击者可以使用 AI 生成的恶意软件窃取浏览器凭据，然后利用这些凭据获得对云帐户的初始访问权限。一旦进入系统，他们就会立即专注于执行操作，部署勒索软件或窃取数据。本报告将这些要点联系起来，展示了这些 TTP 如何形成现代攻击链，更重要的是，说明了如何在多个环节打破这种攻击链。

威胁形势错综复杂，但只要了解恶意软件和威胁行为，并利用先进的防御手段，组织就能显著提高其应变能力。

第 1 步
专注于执行

第 2 步
获得云帐户的初始访问权限

第 3 步
使用 AI 生成的恶意软件

第 4 步
窃取浏览器凭据

Elastic Security 提供您所需的共享情报、高级功能和见解，助您应对当今威胁，构建更安全的未来。