elastic security labs

# 《2023 年全球威胁报告》给首席信息安全官带来的十大启示

Elastic 的第二份年度《全球威胁报告》旨在提供威胁见解，公布了对超过 10 亿个数据点（由私人和公共遥测提供）进行数月分析后的重大发现。Elastic Security Labs 将这些见解归纳为了三个重要类别：态势预测、对手战术和系统。

## 态势预测

**1.开源工具将更加流行**

开源工具为威胁参与者提供了免费且便利的网络犯罪入口。Elastic 在我们的《全球威胁报告》分析中以及在此处调查结果之前的研究中都观测到了若干个开源恶意软件工具，例如 r77 rootkit 和 JOKERSPY。

**2.可供新威胁参与者利用的恶意软件即服务 (MaaS) 将会越来越多**

正如RaaS（勒索软件即服务）流行所证实的那样，对手正在利用即服务 (AaS) 模型来填补知识和产品方面的空白。提供恶意 AaS 的公司会将他们的产品组合进行多样化，以更好地迎合买家需求，而利用 MaaS 的对手将会依赖于混淆和伪装技术。

**3.对手将会更多地篡改环境，而不是隐藏起来**

由于对手面临的环境越来越强大，因此他们会更频繁地试图禁用或以其他方式篡改安全传感器。除《全球威胁报告》分析外，Elastic 还观测到，利用操作系统设计缺陷（例如，通过自带漏洞驱动程序 (BYOVD)，部署带有一个或多个可利用漏洞的驱动程序）发动的攻击也有所增加。

## 对手战术

**4.勒索软件正在不断蔓延和变得多样化**

在 WannaCry 和 NotPetya 等备受瞩目的示例中，勒索软件多年来已被证明是一种强大的威胁。在所有观测到的勒索软件中，勒索软件即服务 (RaaS) 活动占比 81%，这可能是因为新对手和老对手的进入门槛都较低的缘故。我们预测威胁参与者会在这一类别中进一步创新。

 

**5. 对手可轻松穿梭于各个系统**

在观测到的终端行为中，几乎一半 (43.89%) 属于防御规避。这个数字的意义表明，对手熟悉并可轻松规避安全系统。

**6. 通过内置操作系统实用程序执行恶意代码**

Elastic 观测到，在终端上运行的防御规避技术中，有 48% 采用的是系统二进制代理执行方法，这给威胁参与者提供了在本机操作系统程序内执行恶意代码的机会。这种技术之所以受欢迎，可能是因为分析这类告警非常耗时所致。

**7. 对手在云环境中依赖凭据访问技术实施攻击**

Elastic 观测到，凭据访问信号增加了 11%，这表明凭据已成为云入侵过程的重要部分。这可能意味着凭据易于收集，也可能是环境缺乏必要的可见性，在有效凭据被冒用之时无法及时识别。

## 系统

**8.更高的 Windows 可观测性揭示了 Azure 的受欢迎程度**

今年，Elastic 对 Windows 环境的可见性有所提高，相比去年的分析提高了 422%，其中包括对 Microsoft 365 新增的可见性。在对云服务提供商的分析中，我们观测到，Azure 活动从去年的 13.14% 提高到了 36%。虽然 AWS 仍然占大多数，但来自 AWS 环境的信号减少了约 10%。

**9. 虽然大部分终端信号仍来自 Windows，但 macOS 和 Linux 信号都有显著增加**

94% 的终端行为告警都指向了 Windows 系统，这在一定程度上是以 Windows 为重点的遥测增加所致。总体而言，Elastic 发现 Windows、Linux 和 macOS 的信号都有显著增加。随着 macOS 创新增加 118%，发现了 RUSTBUCKET 等新型恶意软件。

**10.观测到的大多数恶意软件感染都发生在 Linux 系统中**

在 Elastic 提高了对所有系统可观测性的情况下，Linux 仍占所观测到感染的 91.2%。值得注意的是，这些感染大多不涉及人为干预，都是自动执行的，可能是无差别的攻击。

## 把握威胁态势

为应对这些威胁及更多威胁的演变做好准备。查看 Elastic Security Labs 的专家在《2023 年 Elastic 全球威胁报告》中给出的建议。在 X（以前是 Twitter）上关注 Elastic Security Labs @ElasticSecLabs，并查阅我们的文章，以了解最新的威胁发展情况和研究等！

 