



分析师报告

# 托管检测和响应



# 目录





# 行动概要



每天发生的高严重性事件超过两起

按客户数量划分的关键地区：

- ◆ 欧洲 — 40%
- ◆ CIS\* — 21%
- ◆ 中东、土耳其和非洲 — 15%

关键欧洲国家：

- ◆ 意大利 — 31%
- ◆ 西班牙 — 15%
- ◆ 瑞士 — 13%



最常见的 MITRE ATT&CK 技术：

**T1566: 网络钓鱼**

TA0001: 初始访问

通过 24% 的事件可以观察到

**T1204: 用户执行**

TA0002: 执行

通过 19% 的事件可以观察到

**T1098: 账户操纵**

TA0003: 持久性

通过 18% 的事件可以观察到

\* CIS — 独立国家联合体 (亚美尼亚、阿塞拜疆、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、摩尔多瓦、俄罗斯、塔吉克斯坦、乌兹别克斯坦)

1 一种借助恶意软件实施且无明显人为介入痕迹的攻击

77% 的事件在首个相关安全警报接收后得到成功补救



所报告事件数量最多的行业：

工业 — 26%



金融 — 14%



政府 — 12%



高严重性事件中最常见的攻击者特征：

APT — 43%



安全评估 — 17%



犯罪<sup>1</sup> — 12%



最常见的离地攻击工具：

powershell.exe



rundll32.exe



comsvcs.dll



按严重性划分的报告事件分布情况：

■ 高 — 5%

■ 中 — 69%

■ 低 — 26%



高严重性事件的平均报告时间 — 54 分钟，中严重性事件的平均报告时间 — 41 分钟，低严重性事件的平均报告时间 — 38 分钟。



# 建议

- ◆ 相较于 2023 年，2024 年的高严重性事件数量降低了 34%。然而，调查和报告的平均时间增加了 48%，表明攻击的平均复杂程度有所上升。这些结论是通过检测规则和 IoA 的分析得出的，而这些规则和 IoA 大多源自专业的扩展检测与响应 (XDR) 工具。这意味着与往年相比形势有所变化，过去操作系统日志在检测中占据重要地位。在这种情况下，像 **XDR<sup>3</sup>这类专业工具** 对于成功检测和调查现代威胁而言至关重要。
- ◆ 2024 年，人为驱动的定向攻击在高严重性事件中的占比达 43%，较 2023 年增长 74%，比 2022 年高出 43%。尽管自动化检测工具不断进步，但心怀不轨的攻击者仍能设法绕过。为应对人为驱动的攻击，像 **托管检测和响应<sup>4</sup>** 这类以人为主导的解决方案不可或缺。对于拥有内部安全运营团队的组织而言，其内部流程与技术需具备应对现代威胁形势的能力。全面的 **SOC 咨询服务<sup>5</sup>** 可助力达成这一目标。
- ◆ 统计数据持续表明，攻击者在成功实施攻击后常会再次发动攻击。这一现象在政府组织中尤为突出，攻击者意图长期潜伏开展间谍活动。在此情形下，将配备 XDR 的内部 SOC 或外包 MDR 与定期 **损害评估<sup>6</sup>** 相结合，是检测并调查现有安全措施遗漏事件的有效方法。攻击者经常在缺乏适当系统配置控制的基础设施中使用离地攻击 (LotL) 方法<sup>7</sup>。大量事件与未经授权的更改相关，例如向特权组添加账户、弱化安全配置等。为了降低此类情形下的误报率，有效的配置管理以及用于执行变更和管理访问权限的正式流程至关重要。
- ◆ 2024 年，用户执行<sup>8</sup> 和网络钓鱼<sup>9</sup> 技术再次位列前三大威胁之列，近 5% 的高严重性事件涉及成功的社交工程攻击。用户依旧是最薄弱的环节，这让 **安全意识<sup>10</sup>** 成为企业信息安全规划的核心要点。

3 卡巴斯基新一代安全  
XDR 专家版

4 卡巴斯基托管检测和响应

5 卡巴斯基 SOC  
咨询

6 卡巴斯基损害评估

7 卡巴斯基百科全书离地攻击

8 MITRE ATT&CK T1204 用  
户执行

9 MITRE ATT&CK T1566  
网络钓鱼

10 卡巴斯基安全意识



# 卡巴斯基容器安全解决方案

年度托管检测和响应 (MDR) 分析师报告依托卡巴斯基 SOC 团队对 MDR 事件的分析, 给出相关见解。

报告披露了最常见的攻击者战术、技术与工具, 以及所检测到事件的特征, 还有这些事件在 MDR 客户所在地区和行业的分布情况。

该报告解答了一系列关键问题, 包括:

他们当下采用何种方法?

潜在的攻击者是谁?

如何有效检测其活动?





# 关于卡斯基 MDR

MDR 提供全天候的监控和威胁检测服务。端点保护平台 (EPP) 会传送遥测数据, 以供机器学习和 SOC 团队进行分析。在威胁检测方面, 运用攻击指标 (IoA), 同时结合专业的手动威胁搜寻策略。响应操作由 SOC 团队制定, 若用户批准, 则由 EPP 执行。

T1566: 网络钓鱼 — 24%

T1098: 账户操纵 — 18%

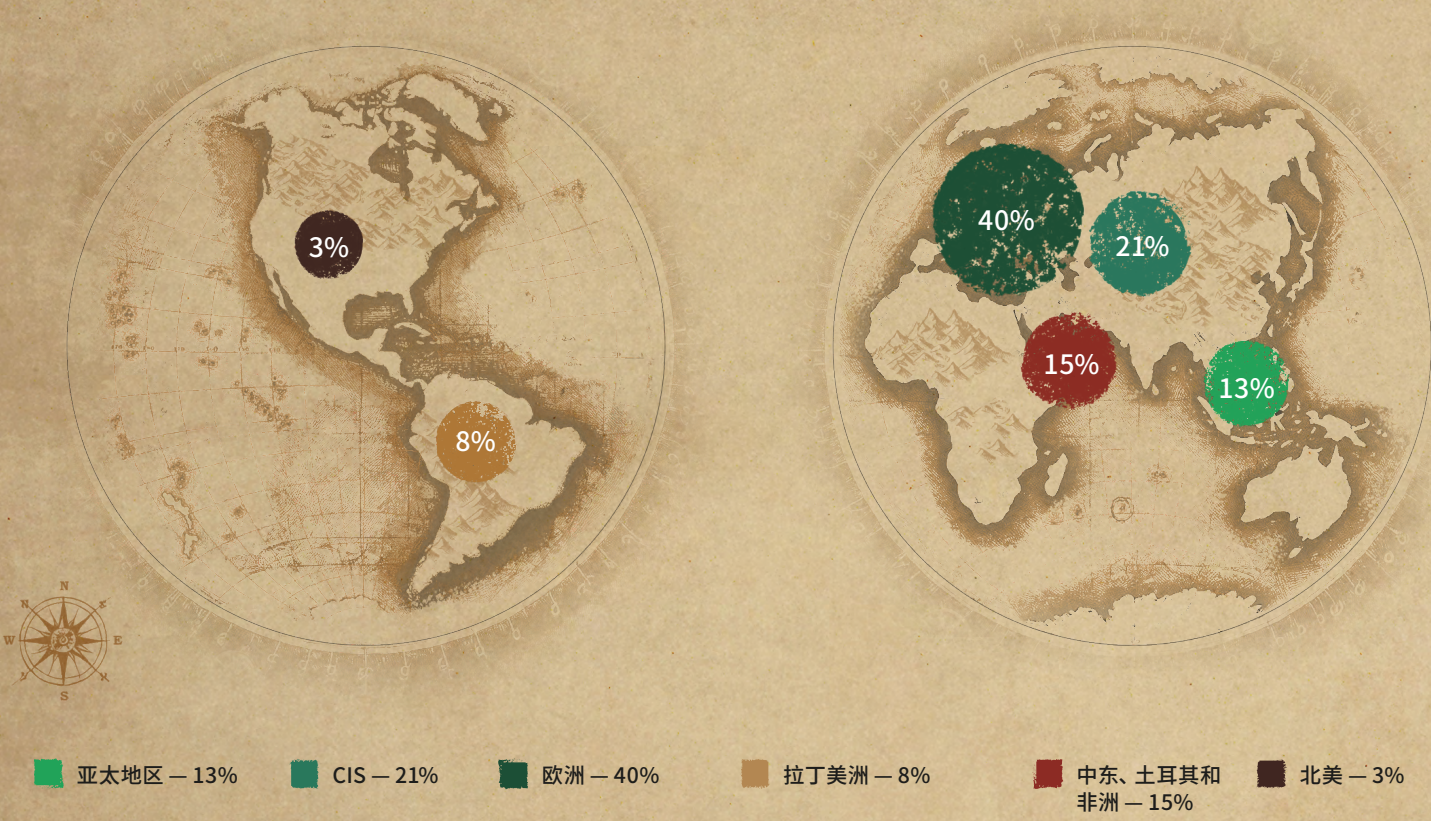
T1204: 用户执行 — 19%





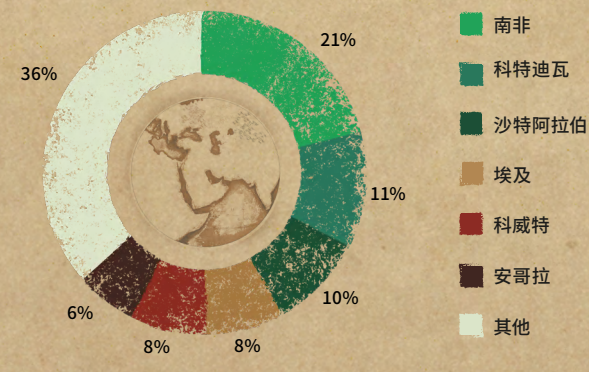
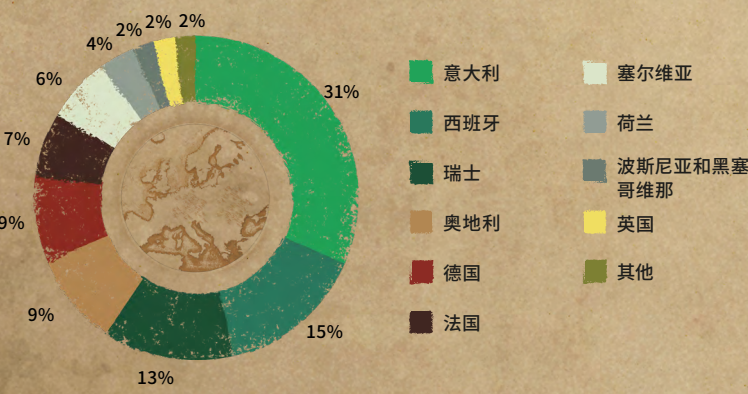
# 卡巴斯基 MDR 服务覆盖范围

卡巴斯基的 MDR 客户遍布全球，这让我们得以全面且客观地洞察各地区的攻击行为与战术。下方图表呈现了 MDR 客户的地理分布状况。其中，最大的客户群体位于欧洲、独联体 (CIS) 以及中东、土耳其和非洲地区。



在欧洲，意大利、西班牙和瑞士拥有最高的 MDR 覆盖率。

南非在中东、土耳其和非洲地区处于领先地位。

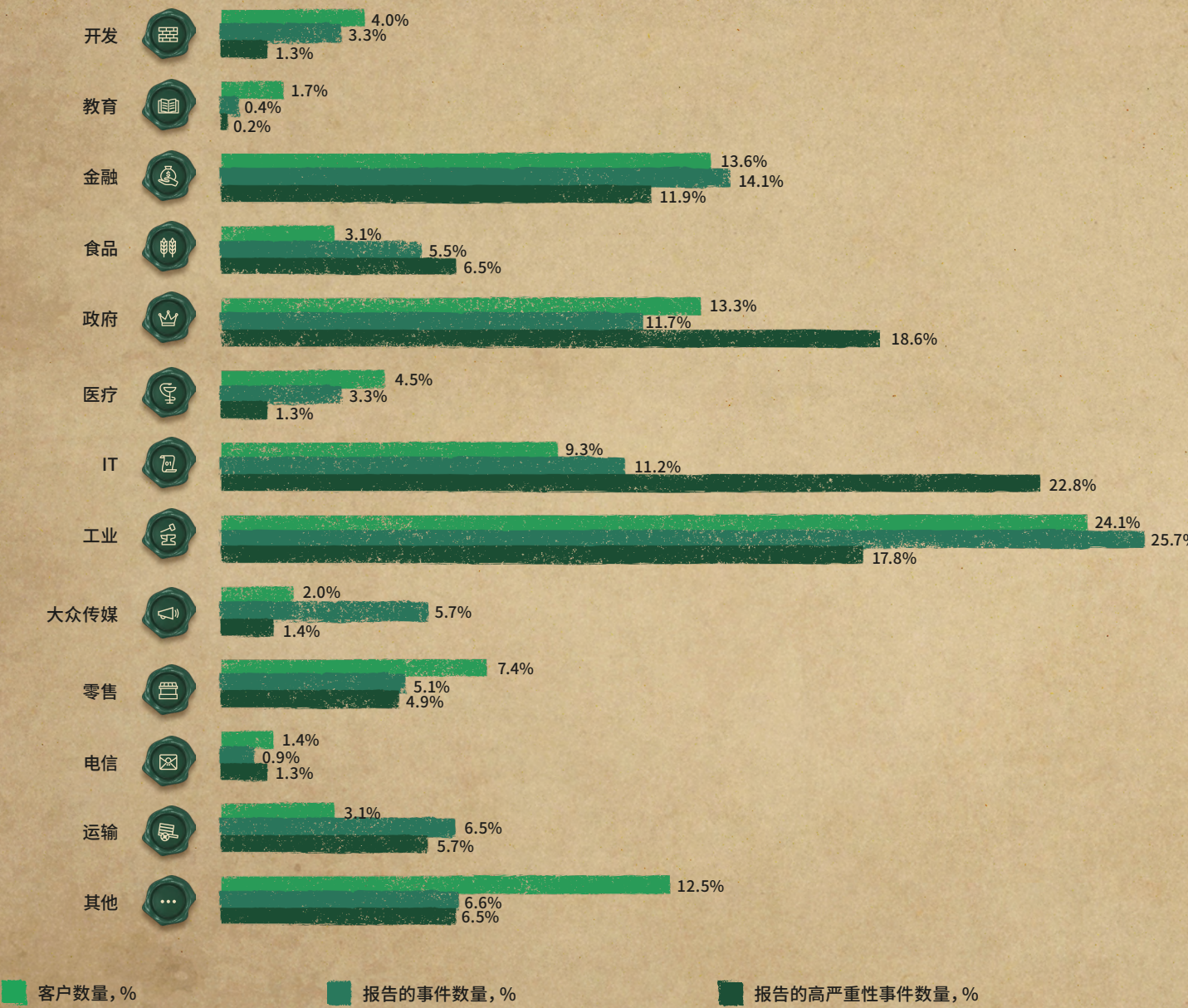




# 行业分布

2024 年, MDR 团队在工业企业 (占比 25.7%)、金融 (占比 14.1%) 以及政府 (占比 11.7%) 行业观测到的事件数量最多。

图 1 受攻击最多的行业



该图表按客户数量呈现了 MDR 在各相关行业的覆盖情形。将其与按事件数量的分布情况进行对比, 我们便能大致推断出各行业发生事件的频次。

若仅聚焦高严重性事件, 分布情形则有所差异: IT 行业占比 22.8%, 政府行业占比 18.3%, 工业行业占比 17.8%, 金融行业占比 11.9%。





# 事件数量

2024 年，MDR 基础设施每天均会收到并处理遥测事件，进而生成安全警报。这些警报中，大约 26% 的警报由机器学习算法处理，13% 经 SOC 团队分析后确认为实际事件。MDR 客户通过 MDR 门户获知这些事件信息。

图 2

## 卡巴斯基 MDR 警报处理漏斗

~ 270,000

个安全事件被接收到



~ 15,000

个来自主机的遥测事件

此数字可能会因主机活动和传感器类型的不同而有很大差异

~ 200,000

个警报经由 SOC 分析师进行分析

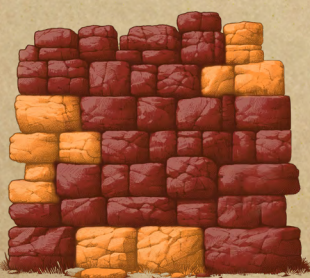


> 70,000

个警报由 AI 技术自动处理

~ 87%

的警报被 SOC 分析师识别为误报



> 26,000

个警报被分析

~ 13,000

起事件已报告给客户



警报数量的显著减少得益于团队针对检测逻辑效率提升所开展的大量工作，使得整体 IoA 转换率从 10% 增加到 13%，同时 SOC 在分析处理过程中的误报数量亦大幅降低。





# 事件检测时间

事件检测过程包含以下步骤。首先，由专门的机器人将生成的警报分配给空闲的 SOC 分析师个人队列。然后，分析师会根据警报的严重性以及服务水平协议 (SLA) 所规定的威胁检测时间对警报进行处理。若分析判定为误报，该警报会被忽略，并在客户或全球层面创建相应过滤器。若非误报，系统会把警报导入新事件或现有事件中，经深入调查后，可能再次作为误报关闭，也可通过 MDR 门户向客户报告并给出建议响应。若客户批准建议响应，端点代理将自动执行这些响应。

表 1

检测到事件的时间

| 严重性                                                                                  | 报告时间<br>(以分钟为单位)                                                                                                                                            | 注释                                                                                                    |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|  高  | <br>53.99 分钟<br>2023 年: 36.37 分钟<br>2022 年: 43.75 分钟<br>2021 年: 41.45 分钟  | 最为复杂的事件需要投入更多时间来收集额外信息并梳理建立事件时间线。<br>2024 年，这一耗时相较以往增加了约 48% <sup>2</sup> ，体现出该年高严重性事件的特点。            |
|  中 | <br>41.03 分钟<br>2023 年: 32.55 分钟<br>2022 年: 30.92 分钟<br>2021 年: 34.88 分钟 | 中严重性事件是最常见的严重级别。此类事件大多由恶意软件活动引发，而全自动补救措施已被证实有效。不过，与 2024 年相比，所需的处理时间增加了 26%，这是由于 2024 年中严重性事件的数量略有增加。 |
|  低 | <br>37.85 分钟<br>2023 年: 48.01 分钟<br>2022 年: 34.15 分钟<br>2021 年: 40.24 分钟 | 低严重性事件大多与潜在有害软件造成的影响相关。在多数情况下，此类事件的处理基本可实现自动化处理。                                                      |



# 事件严重性

在 MDR 服务中, 仅上报需客户方采取行动的事件。



这类事件虽不会对客户IT系统造成显著影响, 但仍需采取一定措施。



没有证据表明存在人为直接参与攻击的迹象, 此类情况虽可能对客户IT系统产生影响, 但不会引发严重后果。



由人为驱动的攻击或恶意软件威胁, 对客户的IT系统构成潜在或实际的重大影响。

2024 年, 平均每两天就会发生三起以上严重事件。尽管 2021 年发生的高严重性事件数量最多, 但此后的趋势表明, 高严重性事件占比有所下降, 中低严重性事件占比有所上升。

图 3

事件严重性

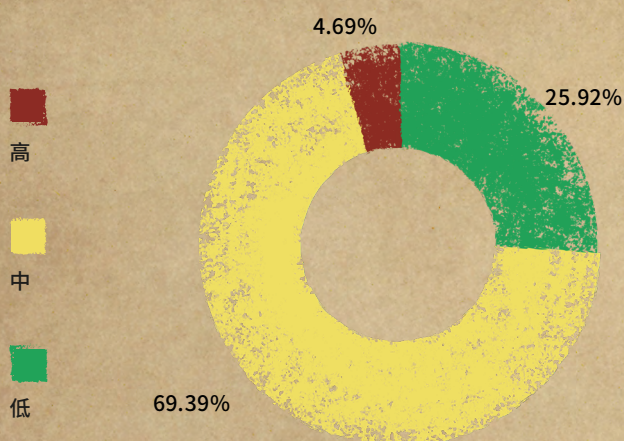
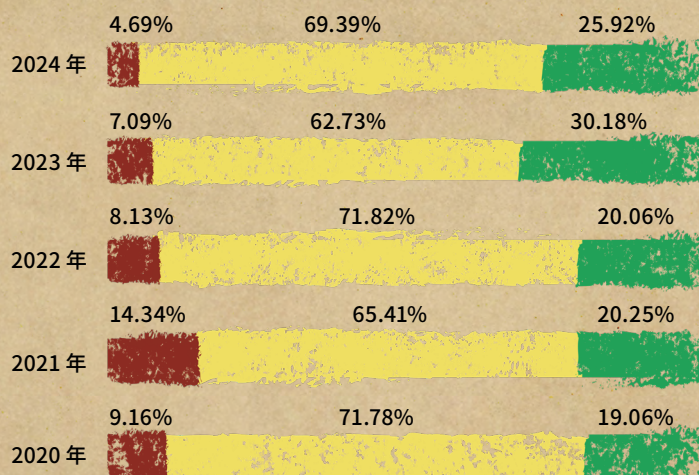


图 4

多年来 MDR 检测到的事件严重性



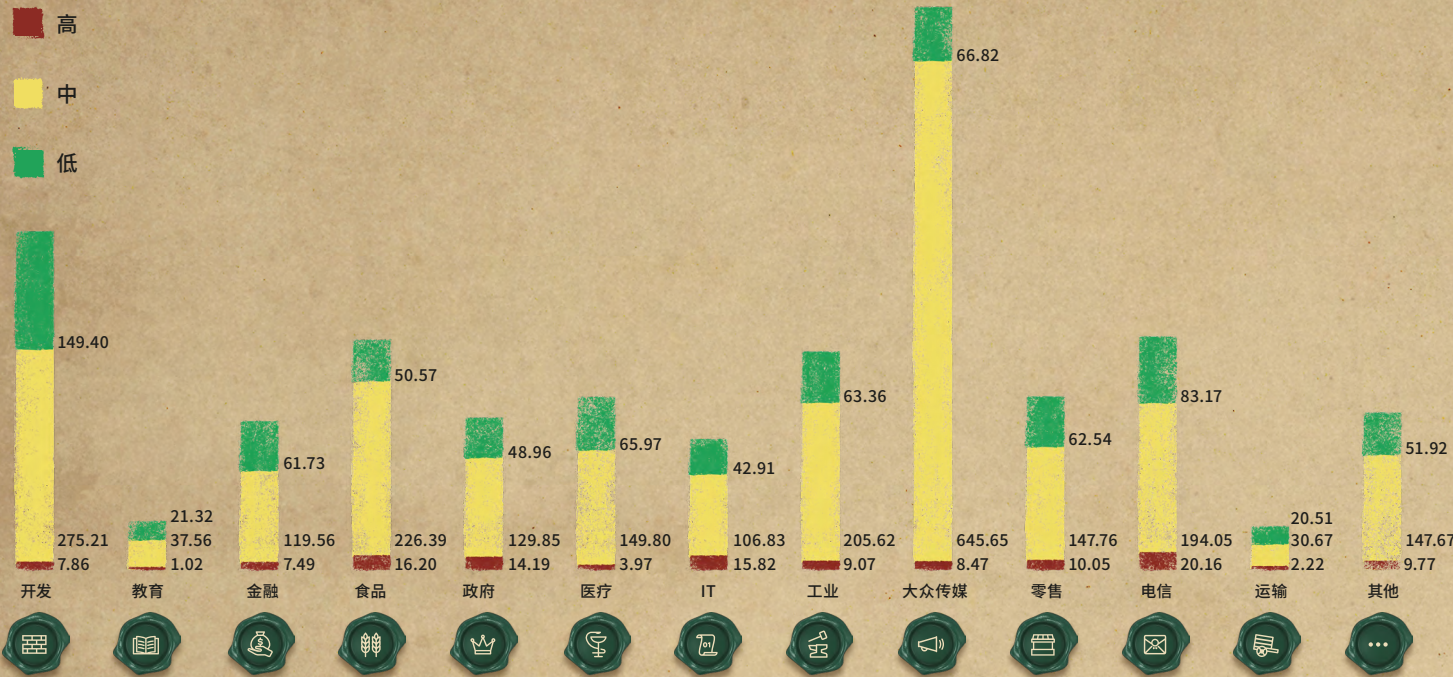
从高严重性事件向中严重性事件的转变, 可归因于早期检测与工具补救措施。在检测到攻击时, 往往缺乏足够证据表明有人为直接参与。在这类情况下, 检测到的活动包括恶意电子邮件活动、路过式下载攻击、连接至潜在恶意互联网资源、网络侦察、暴力破解尝试或漏洞利用等。不过, 卡斯基 MDR 团队判定, 这些活动的性质及其关联风险, 尚不足以将其归为高严重性事件。



事件数量的多少在很大程度上由监控范围所决定。下图展示了在按行业划分的 10,000 个受监控端点里，各类严重性事件的预估数量。

图 5

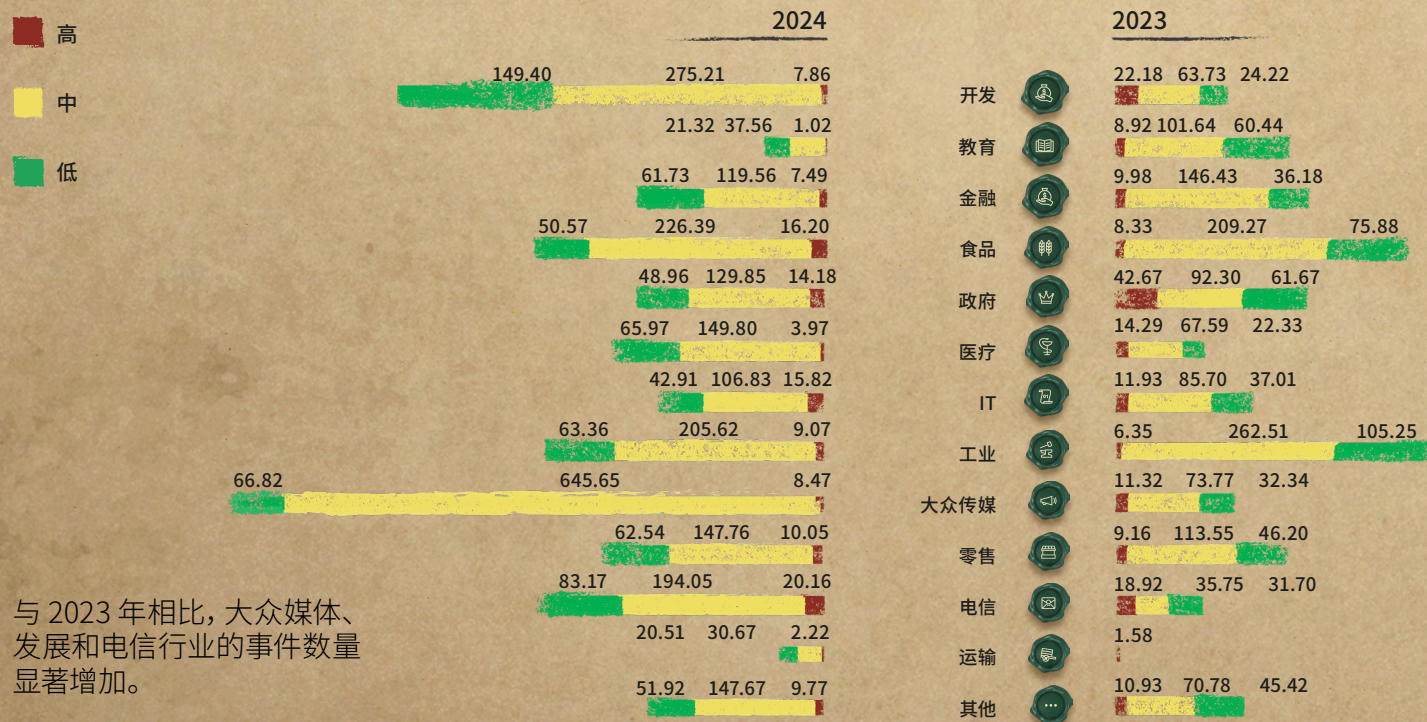
按行业分类的 10,000 个端点中不同严重级别的预期事件数量分布



该图表显示，大众媒体、发展和电信行业发生的事件数量相对最多。

图 6

与上一年相比，按行业分类的 10,000 个端点中不同严重级别的预期事件数量分布



与 2023 年相比，大众媒体、发展和电信行业的事件数量显著增加。



2024 年，高严重性事件在总数中所占比例不到 5%，在整体事件量中并不突出。下图仅聚焦于高严重性事件。

图 7

与上一年相比，按行业分类的 10,000 个端点中不同严重级别的预期事件数量分布



该图表揭示，政府与发展领域的高严重性事件明显减少，而工业领域的事件数量则维持稳定或有所上升。食品行业的事件数量出现了相对显著的增长，IT 与电信行业的事件数量也略有攀升。尽管大众媒体领域的事件数量大幅增长，但这一趋势并未在高严重性事件中体现出来。这进一步印证了之前的观察，即许多攻击企图被及时发现并得以缓解，从而避免了其升级为更高级别的严重事件。





# 响应效率

图 8

按相关警报数量划分的事件分布情况

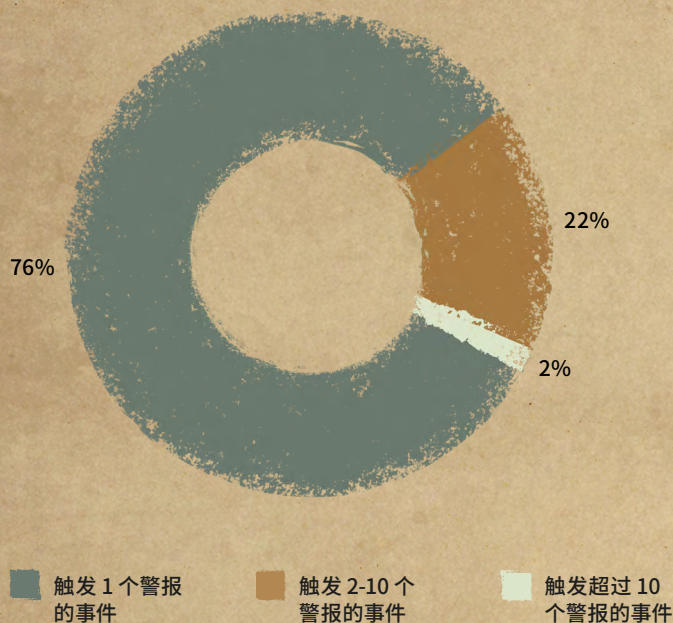
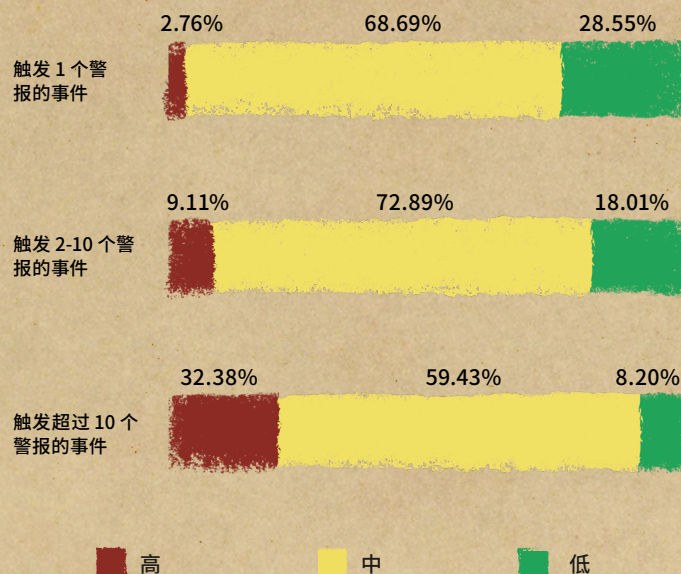


图 9

按相关警报的严重性和数量划分的事件分布情况



大约 76% 的事件是基于**单一警报检测出**的。如果没有生成进一步的相关警报，便认定攻击已被成功拦截。此类事件还包含那些有明确应对方案的典型情况。严重事件占比不到 3%，大部分为中（69%）和低（29%）严重性事件。

大约 22% 的事件是基于**2-10 个警报检测出**的。为了使其难以绕过检测，我们采用一组技术针对同一威胁创建不同的警报。例如，EPP 可以同时根据威胁二进制文件及其行为检测到工具的使用。在 MDR 一侧，检测可能基于特定的命令行以及对某些注册表配置单元的访问。此类别反映的是首个警报出现后未自动处理的事件，即要么有人介入响应，要么首个相关警报被归类误判。

大约 2% 的事件包含超过**10 个警报**。通常在客户拒绝响应或响应无效的情况下会出现此类状况。比如，面对需要深入调查后才能响应的新型定向攻击，或是客户要求在不采取主动防御措施的前提下对攻击进行监控（如网络演习场景）。在此类情况中，高严重性事件占比最高，超过 32%。该类别里大约 8% 的低严重性事件，是由 MDR 用户因内部因素或事件危害程度较低而未采取优先响应行动所导致。尽管这些未响应行为不会致使攻击进一步恶化，但 MDR 基础设施仍会持续接收到与所报告事件相关的警报。



# 高严重性事件的性质

## 高严重性事件的主要原因

图 10

按类型划分的严重事件数量

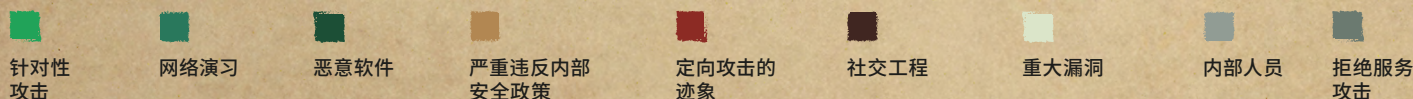
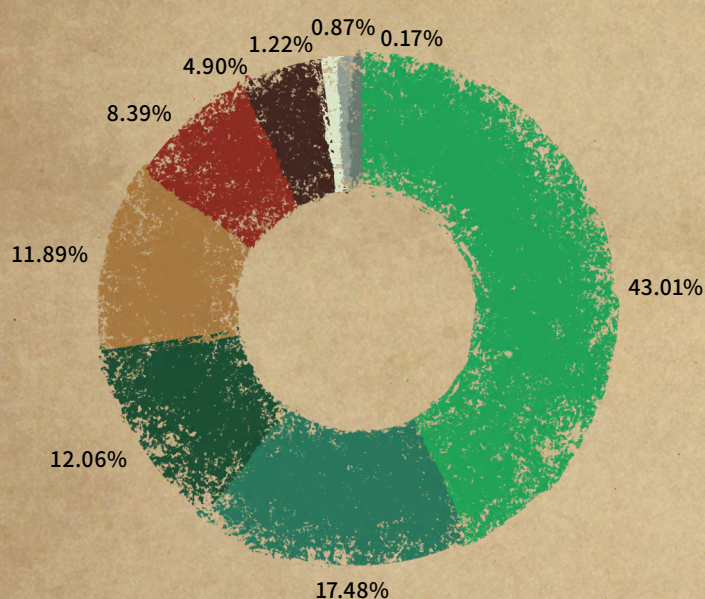
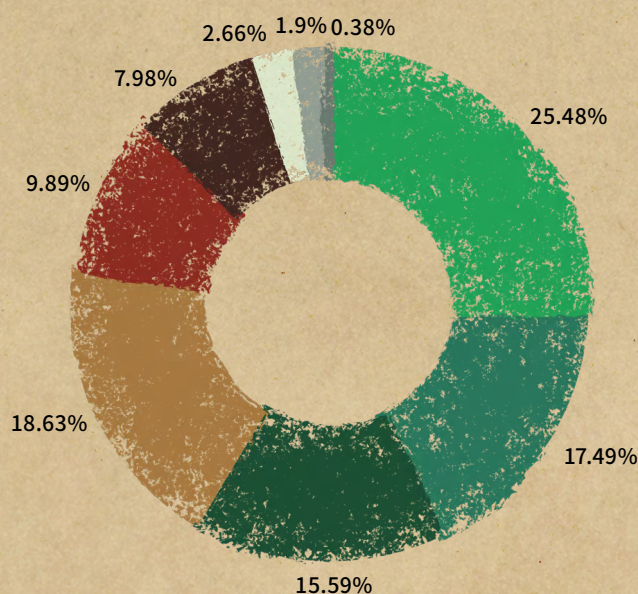


图 11

按类型划分的遭受严重事件的公司数量



2024 年，卡巴斯基在四分之一的客户中检测到由人为驱动的攻击（APT）。此类攻击在所有高严重性事件中占比超 43%。经客户确认为网络演习的人为驱动攻击，在事件中占比超 17%，且在超 17% 的客户中均有观察到。约 12% 的事件涉及严重违反安全政策，超 18% 的客户报告了这类情况。2024 年，与恶意软件相关的安全事件位列第三，不到 16% 的客户报告了略超 12% 的高严重性事件。

超过 8% 的事件与检测过往人为驱动攻击的痕迹有关，这些攻击在检测时已不再活跃，受影响的客户比例不足 10%。虽然漏洞检测不是 MDR 的核心重点，不过相关技术能力已经具备。超过 1% 的此类高严重性事件是由不到 3% 的客户发现的。合法用户的可疑行为会通常被归为违反安全政策。如果客户确认是蓄意恶意行为，这些事件会重新被归类为内部活动。这种极为罕见的情况在高严重性事件中占比不到 1%，且发生在不到 2% 的基础设施中。

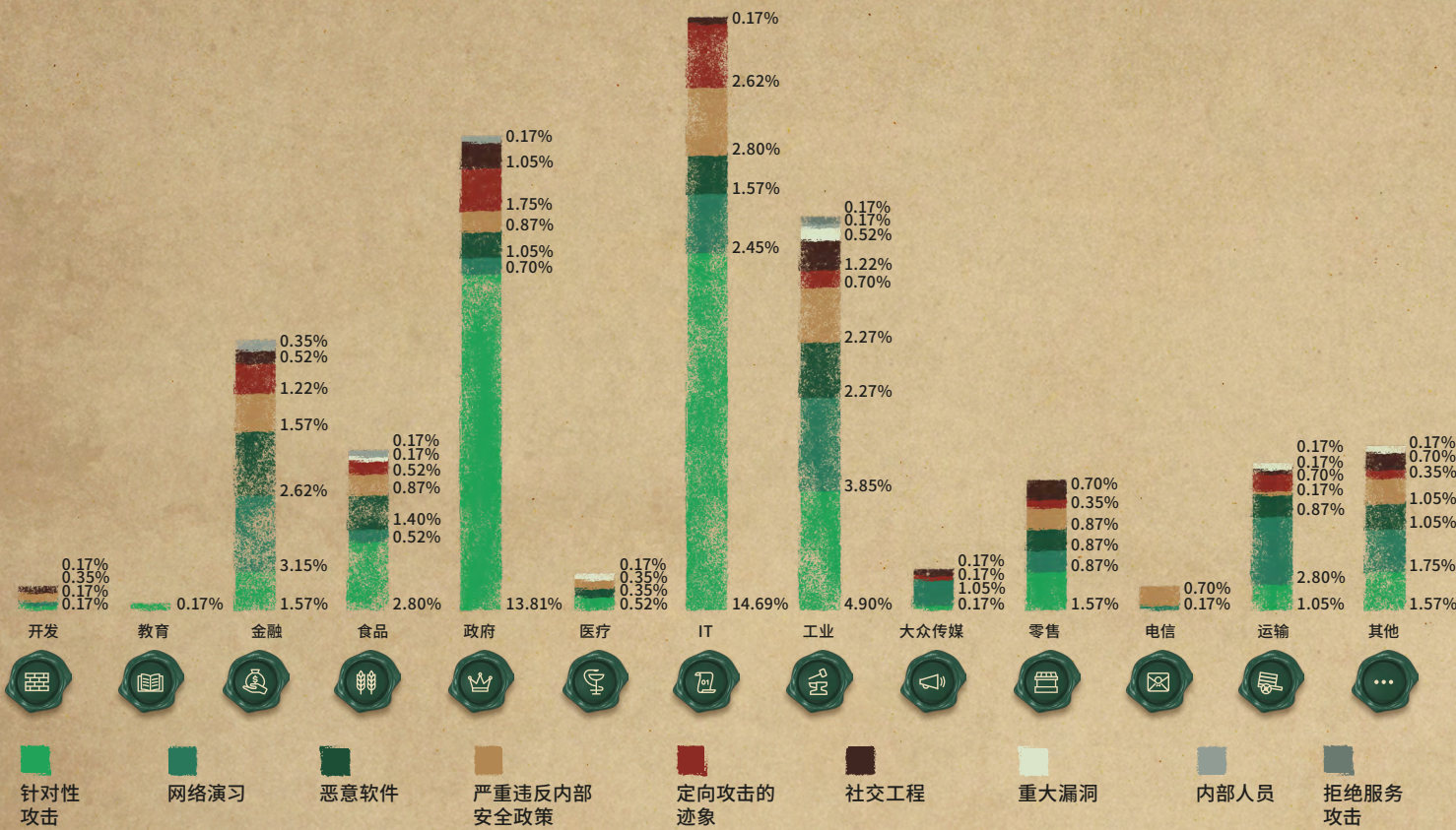


# 按行业划分的高严重性事件数量

下图显示了按类型和行业划分的高严重性事件的分布情况。

图 12

## 按类型和行业划分的高严重性事件数量



## 从统计数据中可以得出以下结论：

- ◆

除电信行业外，其他所有行业均观察到了人为驱动的定向攻击。IT 和政府行业分别以 14.7% 和 13.8% 占比领先。
- ◆

工业领域观察到了所有类型的事件，在 2024 年高严重性事件总数中位列第三，其中包括检测到的 0.17% 的 DoS 攻击。
- ◆

金融行业在高严重性事件总数中排名第四，受到所有 MDR 事件类型的影响。
- ◆

安全评估仍属于一种常见做法，除教育和医疗保健领域外，其他经济领域均有此类事件发生。
- ◆

与恶意软件相关的高严重性事件主要集中于金融（2.6%）、工业（2.3%）和 IT（1.6%）领域。
- ◆

涉及过往 APT 攻击迹象的事件，反映了活跃人为驱动攻击的分布情况。在发展和教育领域，检测到活跃的人为驱动攻击，但未报告出涉及过往攻击迹象的事件。
- ◆

除教育和大众媒体行业外，其他所有行业均观察到了严重违反内部安全政策的情况。IT（2.8%）、工业（2.3%）和金融（1.6%）行业受影响最为严重。在金融、食品、政府和工业领域，观察到已确认的恶意内部行为。
- ◆

导致情况进一步恶化的成功社会工程攻击，在高严重性事件总数中位列第六。工业（1.2%）和政府（1.1%）领域受影响较大。
- ◆

工业、交通、食品和医疗保健领域报告了与2024年严重漏洞相关的事件。



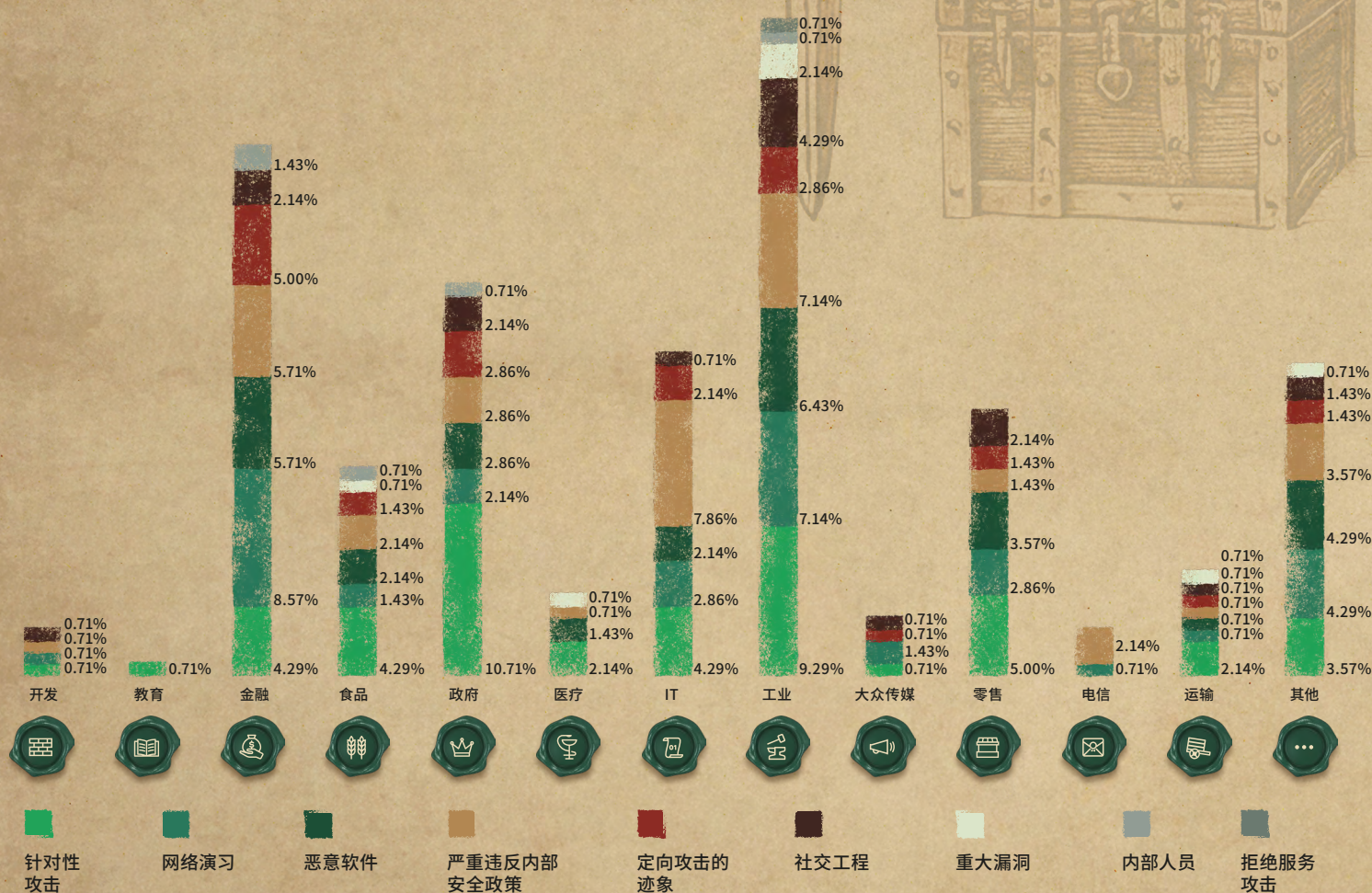


# 遭遇高严重性事件的组织数量

下图显示了各行业检测到特定类型高严重性事件的MDR客户总数占比情况。此图表有助于分析所有客户的整体情况。

图 13

按行业分布的经历过高严重性事件的 MDR 客户数量

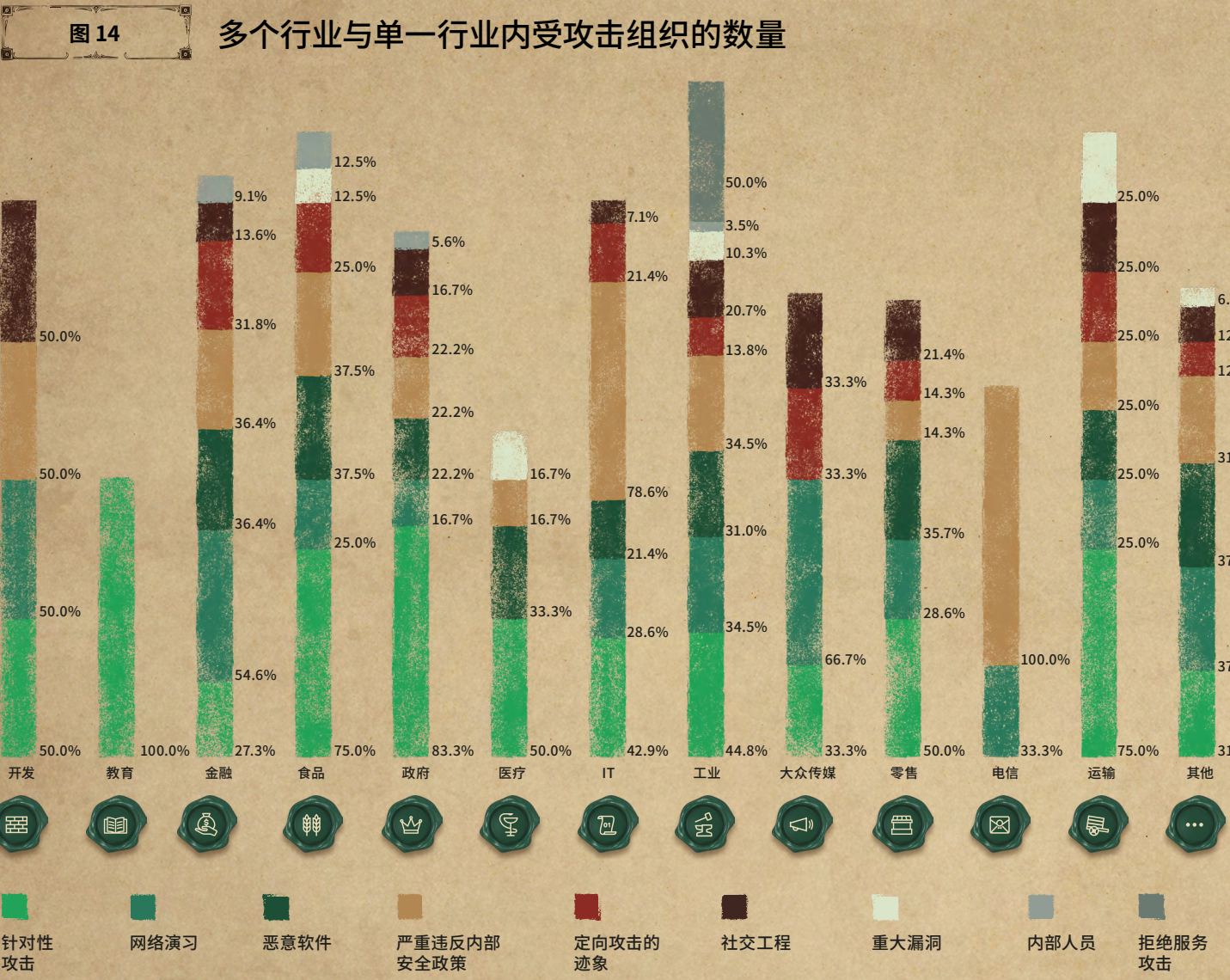


除了先前的发现，从该图还可以得出以下结论：

- ◆ 各行业均发现高严重性事件。
- ◆ 在受到人为驱动攻击的公司中，工业（9.3%）和政府（10.7%）行业占比居首。
- ◆ 就受影响组织数量而言，严重违反安全政策的事件排名第二。卡斯基基监控的近乎所有组织都出现此类事件，其中IT（7.9%）、工业（7.1%）和金融（5.7%）行业最为显著。
- ◆ 恶意软件攻击在工业（6.4%）和金融（5.7%）领域的企业中最为常见。
- ◆ 金融（8.6%）和工业（7.1%）领域经历的网络演习相关事件数量最多。



若需比较多个行业及单一行业内受攻击组织的数量,可参考下图。图中百分比代表发生相应类型事件的组织在特定行业组织总数中的占比。



### 该可视化图表中的关键点:

- 在教育领域,所观察到的唯一高严重性事件类型是人为驱动的攻击。此外,83% 的政府组织、75% 的交通与食品行业组织,以及一半的发展、医疗保健和零售行业组织报告了 APT 事件。
- 电信行业所有组织及 79% 的 IT 组织报告出现违反安全政策的情况。
- 一半的工业领域组织都报告遭受 DoS 攻击。
- 网络安全演习在大众媒体领域 (三分之二的组织)、金融领域 (55%)、发展领域 (50%) 尤为常见。
- 在 32% 的金融组织、33% 的大众媒体组织以及 25% 的食品和交通领域组织中,检测到先前人为驱动攻击的迹象。
- 成功的社会工程攻击影响了 50% 的发展组织、33% 的大众媒体组织和 25% 的交通运输组织。

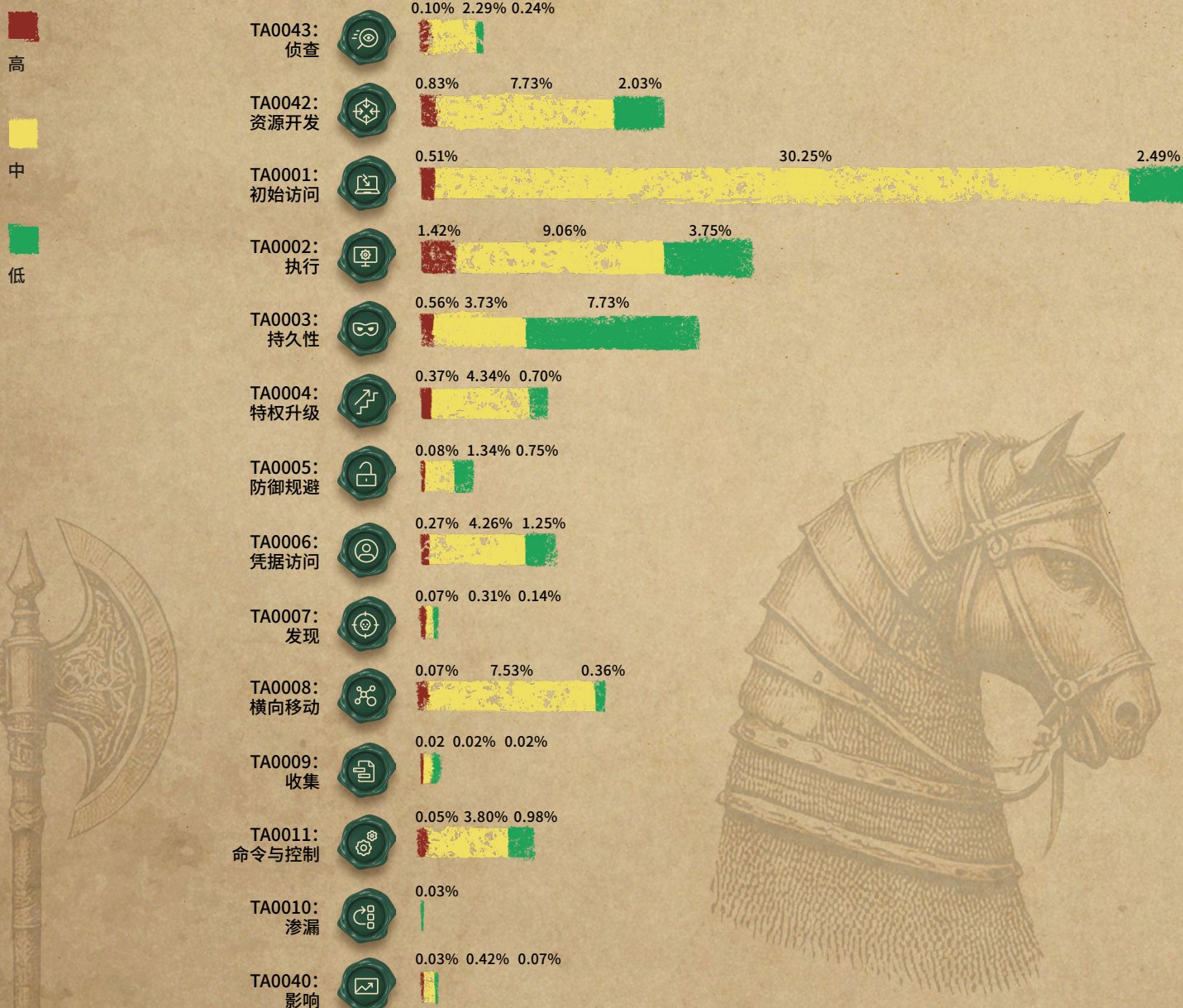


# 检测技术对抗战术、技术和程序

MDR 具备检测不同攻击阶段事件的能力。尽管在实际情况中，多数事件往往会历经 MITRE ATT&CK® 战术所涵盖的全部攻击阶段，但下方图表聚焦于呈现与每个事件警报相关联的最初战术，旨在提供更具针对性的洞察视角。

图 15

## 对抗战术





## 卡巴斯基用于检测事件的攻击者战术：



### TA0043： 侦查

此阶段检测到的事件大多与各种类型的扫描有关。这些事件的严重性取决于扫描目标。被归类为高严重性的事件通常与成功的鱼叉式网络钓鱼有关，会导致攻击进一步升级。在此阶段还观察到与已知 APT 活动相关的事件。



### TA0042： 资源开发

归因于该战术的事件主要与检测恶意软件或不需要的软件有关，即使在没有执行迹象的情况下也是如此。这些事件的严重性取决于所检测到工具的分类。



### TA0001： 初始访问

在此阶段检测到的绝大多数事件与网络钓鱼电子邮件相关，这些邮件包含各类被归为中等严重性的恶意对象。高严重性事件涵盖成功的社会工程攻击、导致攻击进一步演进的远程服务入侵，以及可归因于已知定向攻击的活动。低严重性事件一般是用户点击后报告的网络钓鱼尝试，因为自动补救成功而未造成任何影响。



### TA0002： 执行

由于启动专门的攻击工具往往会产生较大动静，因此此阶段检测到的高严重性事件数量居多。一般而言，事件的严重性取决于所执行恶意工具的分类。



### TA0003： 持久性

此阶段的事件包括替换无障碍功能、可疑或不安全的网络资源配置以及 Bootkit。若有明显证据表明有活跃的人为攻击者参与，则被判定为高严重性事件。中低严重性事件基于潜在影响进行判定。此处检测到的大多数低严重性事件涉及账户操纵，如启用本地管理员或外部来宾账户。



### TA0004： 特权升级

绝大多数事件采用这种最早的战术——向各种特权组添加账户，如域管理员、企业管理员等。这涵盖与使用专门工具进行权限提升相关的事件，这些工具被 EPP 检测为单独文件或已加载至系统内存中。还包括检测易受攻击的驱动程序、更改 UAC 配置或试图绕过 UAC 的情况。



### TA0005： 防御规避

在此阶段检测到的事件占比相对较小，但检测到的活动种类繁多。例如，主机上的可疑 SPN 设置、伪装成合法 Windows 组件的计划任务、日志删除、更改驱动程序数字签名检查、使用不同的 LOLBins<sup>11</sup> 以及试图修改端点配置等。此处的误报比例最低，因为检测到的技术和工具很少与合法活动存在关联。

<sup>11</sup> 离地二进制文件、脚本和库







## TA0006: 凭据访问

与此战术相关的大多数事件都企图访问 LSASS 进程内存、转储敏感注册表配置单元、检测不同类型的键盘记录器、进行暴力破解或密码喷洒尝试。与前一种情况类似，除了某些已确认的网络演习之外，此阶段识别出的事件很少为误报。



## TA0007: 发现

该阶段的检测中存在大量误报，所以相关的 IoA 很少会转化为警报。现有事件主要与各种类型的内部网络扫描、Active Directory 配置发现或检测专门工具（例如 Bloodhound<sup>12</sup>）的使用有关。



## TA0008: 横向移动

鉴于横向移动的误报率较低，它是规划开发新 IoA 的理想战术。2024 年，大多数事件都与网络远程利用尝试有关。借助不同的基于异常的检测方法，所检测到的使用合法凭据的可疑网络登录，同样归属于此类事件。



## TA0009: 收集

此阶段所观察到的活动是基于对特殊工具的检测。部分事件还借助机器学习支持的异常检测引擎得以识别。



## TA0010: 渗漏

2024 年，仅有少数事件达到这一阶段。检测到的事件很难和 TA0011 区分开来，因为最为常见的情况是运用标准应用层协议的 T1041：通过 C2 通道实施渗漏<sup>13</sup>。当证据明确时，便会将事件归因于这种战术，比如出现能表明某个操作涉及渗漏的特定命令行活动。



## TA0011: 命令与控制

此阶段的绝大多数检测是基于威胁情报开展的，即检测访问恶意资源的情况。事件的严重性取决于 C2 的已知用途：如果与 APT 相关，该事件就会被归为高严重性。检测已知的 C&C 框架，如 Cobalt Strike<sup>14</sup>、Sliver<sup>15</sup>、MSF<sup>16</sup> 等，同样属于这一类别。



## TA0040: 影响

在这种战术中，大多数事件是在早期检测和响应难以开展的情况下，通过检测特定的恶意软件来识别。2024 年，绝大多数发展到该阶段的事件，都与检测加密货币挖矿程序或勒索软件有关。

<sup>12</sup> MITRE ATT&CKS0521 BloodHound

<sup>15</sup> MITRE ATT&CKS0521 BloodHound

<sup>13</sup> MITRE ATT&CKT1041 通过 C2 通道进行渗漏

<sup>16</sup> MITRE ATT&CKT1041 通过 C2 通道进行渗漏

<sup>14</sup> MITRE ATT&CKS0154 Cobalt Strike





# 对抗战术和检测技术

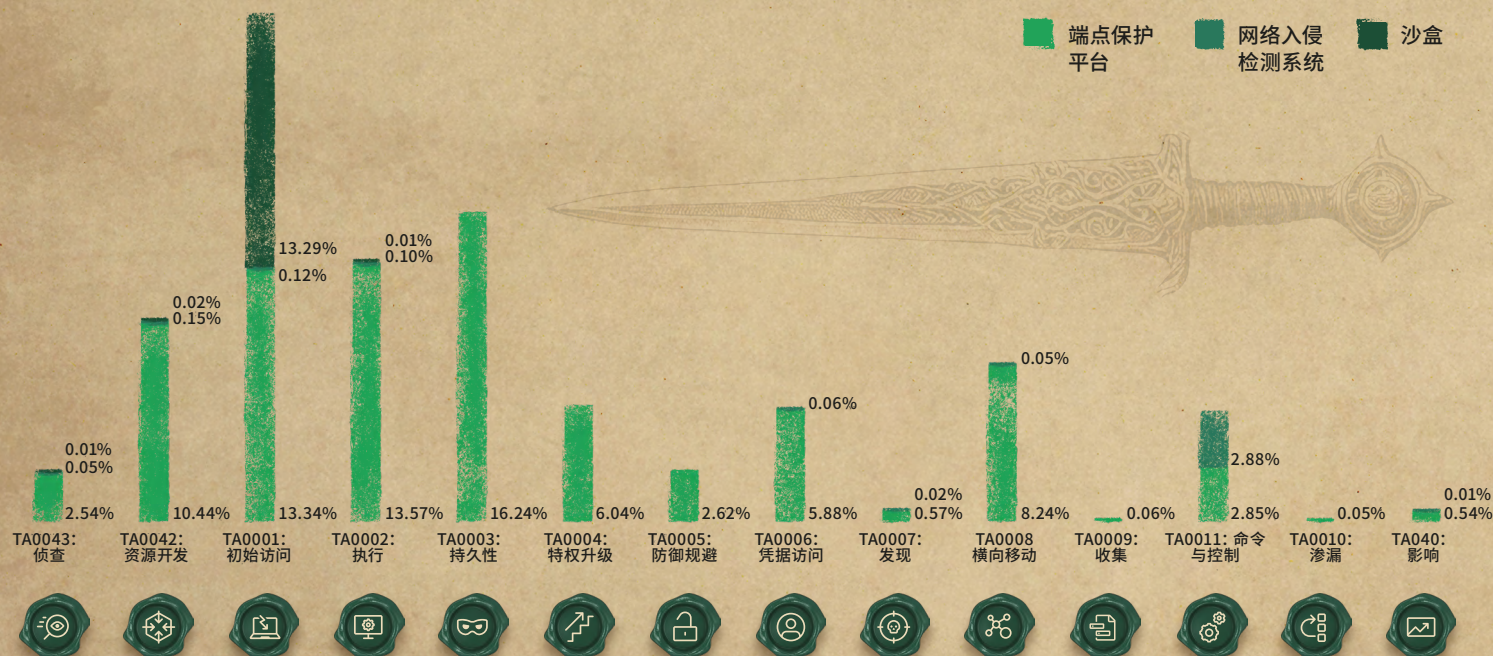
卡斯基 MDR 运用了多种传感器，包括端点保护平台 (EPP)、网络入侵检测系统 (NIDS) 以及沙盒 (SB)。其中，后两种传感器是卡斯基反针对性攻击 (KATA) 的组成部分。

在本报告里，作为 EPP 一部分的 IDS 裁定被视为端点警报。

在诸多情况下，会采用多种类型的传感器来检测事件。然而，就下述图表而言，我们仅统计首先被检测到且被 SOC 分析师用于构成事件的警报。因此，EPP 检测到的事件占多数，并不意味着这些事件无法被作为 KATA 一部分的 IDS 或沙盒检测到。事件统计数据表明，即便端点传感器看似是最为直观的检测手段（比如针对 TA0040：影响或 TA0006：凭据访问的情况），网络 IDS 也同样能够作为 EPP 的有效补充。下方的图表展示了不同类型传感器最初检测到的事件的占比：

图 16

不同类型的传感器检测到的事件比例：



沙盒在 TA0001：初始访问阶段的高效率是由 KATA 在网络边界检测网络钓鱼攻击的常见用例驱动的。网络 IDS 在 TA0011：命令和控制阶段非常高效。除了这些情况外，IDS 在检测网络扫描方面也运行良好，这解释了它在 TA0043：侦查、TA0006：凭据访问和 TA0007：发现等阶段能发挥作用的原因。IDS 在 TA0040：影响阶段检测到的少量事件是恶意软件检测，基于已知的与其远程 C2 的典型通信。C2 检测也解释了 IDS 在 TA0047：资源开发战术中的存在。

在端点上发生的阶段，从 TA0002：执行到 TA0006：凭据访问，端点传感器是主要的检测机制。但是，如果使用具有典型网络流量的攻击工具，这些事件也可以通过 IDS 检测到。例如，检测加密货币挖矿程序 (TA0040：影响)、网络密码暴力破解尝试 (TA0006：凭据访问)、网络服务远程利用尝试 (TA0001：初始访问)。

由于用作端点传感器的 Kaspersky Endpoint Security 配备了内置网络 IDS，因此它在通常与 IDS 相关的阶段（例如 TA0011：命令和控制、TA0008：横向移动和 TA0010：渗漏）也能高效运行。



# 对抗技术

## 攻击中使用的工具

攻击者会使用内置的操作系统工具，以便在向被入侵系统实施攻击时尽量减少被检测到的风险。

表 2

最流行的 LOLBins 及其使用频率

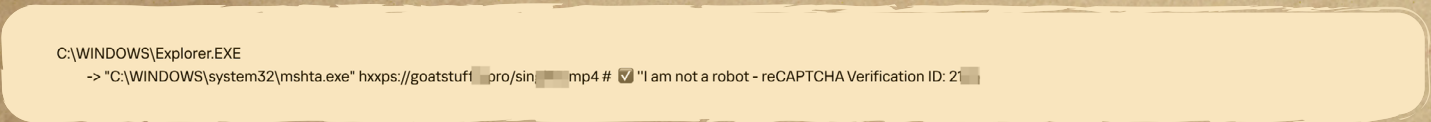
|                | 所有事件  | 高严重性事件 |
|----------------|-------|--------|
| powershell.exe | 1.64% | 10.51% |
| rundll32.exe   | 0.81% | 6.85%  |
| comsvcs.dll    | 0.26% | 3.82%  |
| reg.exe        | 0.23% | 2.07%  |
| msiexec.exe    | 0.67% | 1.59%  |
| certutil.exe   | 0.15% | 1.59%  |
| mshta.exe      | 0.22% | 1.43%  |
| msbuild.exe    | 0.07% | 1.27%  |
| esentutil.exe  | 0.07% | 1.27%  |

几乎在每起事件都能发现的最流行的 LOLBins 是 **powershell.exe**、**rundll32.exe** 和 **reg.exe**。2023 年 MDR 报告中重点提及了 PowerShell.exe、rundll32.exe、reg.exe、comsvcs.dll、msiexec.exe 和 certutil.exe 等例子<sup>17</sup>。

**Mshta.exe** 用于代理恶意执行，如 T1218.005: Mshta 中所述<sup>18</sup>。以下是 2024 年最常见的例子之一：

图 21

Mshta.exe 下载恶意有效载荷



执行 mshta 导致随后启动 PowerShell，而 PowerShell 下载并执行恶意有效载荷<sup>19</sup>。

17 2023 年卡巴斯基 MDR 分析师报告

19 Qualys社区揭开 Lumma 窃取者的面纱：分析使用虚假 CAPTCHA 的欺骗策略

18 MITRE ATT&CK T1218.005 系统二进制代理执行: Mshta





**Msbuild.exe** 用于编译并执行代理它的有效载荷，如 T1127.001: MSBuild 中所述<sup>20</sup>。下面是一个典型示例，演示了通过一个系统服务 (T1543.003: Windows 服务<sup>21</sup>) 实现的恶意持久性，该系统服务指定了用于执行 msbuild.exe 的二进制路径。

图 22

## Msbuild.exe 用于作为 Windows 服务恶意执行

注册表项: HKLM\SYSTEM\ControlSet001\Services\██████.cbxC  
ImagePath (命令): cmd.exe /c start cmd /v: on /c "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Msbuild.exe C:\ProgramData\██████\ZIPp.csproj"

**Esentutl.exe**<sup>22</sup> 二进制文件与 Microsoft JET 数据库配合使用，用于复制和下载二进制文件，包括 NTFS 替代数据流。下面的示例命令演示了复制文件 ..\Network\Cookies，该文件包含打开的浏览器会话数据。攻击者可以使用该文件拦截与在线资源的身份验证通信。

图 23

## Esentutl.exe 从 1.bat 启动，用于文件复制

c:\windows\svcbatch.exe c:\windows\1.bat  
L--> esentutl.exe /y /vss C:\Users\██████\AppData\Local\Google\Chrome\userdata~1\profil~1\Network\Cookies /d c:\users\public\██████

2024 年，**msedge.exe**<sup>23</sup> 继续频繁出现在报告的事件中，表明有相当数量的事件涉及用户点击网络钓鱼链接或成为路过式下载攻击的受害者。

以下是一个典型的源自网络钓鱼电子邮件的执行示例。

图 24

## 来自 Outlook 电子邮件客户端的恶意附件中的 Msedge.exe 试图访问恶意网站

(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"  
└─(PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\██████\AppData\Local\Microsoft\Windows\NetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PPRA User ID details.pdf"  
└─(PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/scf/rf/r03vub4463xluyb65whot/PPRA\_Letters.zip?rlkey=vl19sdakfxmsp4k  
cendo8qzgxe=2&st=d0e86ec1&dl=0

图 25

## 用户试图通过 msedge.exe 访问的恶意网站示例

hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044  
类别: 恶意软件网站

20 MITRE ATT&CKT1127.001 受信任的开发者实用程序代理  
执行: MSBuild

22 MITRE ATT&CKS0404 esentutl

21 MITRE ATT&CKT1543.003 创建或修改系统进  
程: Windows 服务

23 GithubMsedge.exe



# MITRE ATT&CK® 事件分类

MDR 中使用的 IoA 被映射到 MITRE ATT&CK® 技术。为确保检测质量，检测工程团队会评估每个 IoA 的转化率和影响，从而也能够为 MITRE ATT&CK® 技术计算这些指标。下面列出了转化率最高的八种技术，热图显示了观察到技术的影响。转化率低是由于在实践中采用了防御性安全措施，即使攻击者尝试实施已识别技术，但并非所有尝试都能导致实际的事件。

| 表 3 转化率最高的技术            |        |                                                                                         |
|-------------------------|--------|-----------------------------------------------------------------------------------------|
| T1078: 有效账户             | 34.82% | 攻击者经常使用域和本地账户来绕过安全解决方案，并在被入侵的系统中获得持久性。最近，窃取程序变得越来越流行，这可能是这种技术如此常见的原因，尤其是在准备充分的定向攻击中。    |
| T1098: 账户操纵             | 30.30% | 尽管特权账户和特权组通常受到良好的控制，但攻击者经常会激活已禁用的账户和/或向组中添加成员。                                          |
| T1566.002: 鱼叉式网络钓鱼链接    | 24.50% | 网络钓鱼仍然是最流行的获取初始访问权限的技术。2024 年，其流行程度延续了 2023 年的水平，转化率甚至更高。附件比前几年更加常见。                    |
| T1110.001: 密码猜测         | 22.18% | 虽然网络传感器和端点代理都能有效检测到密码猜测，但这种技术在安全评估项目和真实攻击中仍然很流行。                                        |
| T1210: 利用远程服务漏洞         | 20.62% | RCE 漏洞利用尝试在事件中非常常见，既能获得初始访问权限，又能促进横向移动。                                                 |
| T1547.001: 注册表运行项/启动文件夹 | 17.58% | 这是最流行的持久性技术，无论事件严重性如何。它利用了与 LotL <sup>24</sup> 工具相结合的标准操作系统机制，由于没有额外的上下文，很难将其与合法配置区分开来。 |
| T1021: 远程服务             | 17.14% | 这是第二流行的横向移动技术，经常与 T1078: 有效账户一起在各种类型的事件中被使用。                                            |
| T1071.002: 文件传输协议       | 14.78% | 2024 年，该技术首次出现在前 8 名热门话题列表中。FTP 和 SMB 通常用于合法目的，这使得它们成为隐藏恶意活动的诱人选择。                      |

24 卡巴斯基百科全书离地 (LotL) 攻击





# 触发最频繁的检测规则

2024 年，MDR 检测到 803 个具有非零转化的独特情况。在本节中，我们将研究最常触发的情况（加起来占有所有检测的 37% 以上），并根据事件严重性分析它们的影响。

在我们的 2023 年报告中，我们将 IoA 分为两部分列出：基于操作系统的事件和 XDR 遥测。但是，今年绝大多数触发的规则基于 XDR 遥测，而基于操作系统的 IoAs 主要用作附加上下文，而不是主要的检测方法。

表 4

转化率最高的技术

| 检测场景                    | 注释                                           | 所需的遥测数据和<br>数据丰富操作                                                                              | 按严重性划分<br>的影响                      |
|-------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------|
| 转储敏感注册表配置单元             | 此活动被 EDR 遥测以及 EPP 对可疑活动的裁定检测到                | <div><div>注册表访问</div><div>EPP 可疑活动检测</div></div>                                                | 高: 26.91%<br>中: 1.21%<br>低: 1.59%  |
| EPP 内存检测                | EPP 检测系统进程或内存中的某个部分                          | <div><div>EPP 检测</div></div>                                                                    | 高: 17.04%<br>中: 2.45%<br>低: 0.66%  |
| 作为服务执行的系统进程             | 创建或执行了包含任意代码的可疑服务                            | <div><div>自动运行条目</div><div>操作系统事件</div><div>进程启动</div></div>                                    | 高: 16.88%<br>中: 0.58%<br>低: 0.12%  |
| 尝试访问可疑主机                | 尝试访问信誉不佳的主机                                  | <div><div>EPP 检测</div><div>HTTP 连接</div><div>网络连接</div><div>DNS 请求</div><div>目标主机信誉</div></div> | 高: 12.26%<br>中: 7.96%<br>低: 13.21% |
| 可疑的系统内存转储               | 转储系统内存以获取凭据访问权限（即 LSASS 内存转储 <sup>25</sup> ） | <div><div>EPP 检测</div><div>LSASS 进程访问</div><div>任何包含命令行的遥测事件</div></div>                        | 高: 11.94%<br>中: 0.99%<br>低: 1.24%  |
| 启动信誉不佳的对象 <sup>26</sup> | 任何启动文件和命令脚本以及打开信誉不良的办公文档的场景                  | <div><div>任何包含启动事件的进程的遥测事件</div><div>文件/脚本/办公文档信誉</div></div>                                   | 高: 10.83%<br>中: 6.51%<br>低: 1.62%  |
| 用户添加到特权域组               | 基于操作系统事件。关键组成员资格被更改                          | <div><div>操作系统账户操纵事件</div></div>                                                                | 高: 8.76%<br>中: 7.05%<br>低: 0.87%   |

25 MITRE ATT&CKT1003.001 操作系统凭据转储: LSASS 内存

26 卡巴斯基在线文件信誉





| 检测场景                         | 注释                                                                      | 所需的遥测数据和<br>数据丰富操作         | 按严重性划分<br>的影响                     |
|------------------------------|-------------------------------------------------------------------------|----------------------------|-----------------------------------|
| 异常服务安装                       | 基于操作系统事件。安装某项服务，而该服务是使用攻击工具的标志                                          | 服务安装事件                     | 高: 6.69%<br>中: 0.23%<br>低: 0.09%  |
| 远程执行的进程                      | 进程在具有网络登录类型的账户下执行                                                       | 进程启动<br>部分加载               | 高: 5.57%<br>中: 0.17%<br>低: 0.17%  |
| 在命令行中发现恶意 URL                | 在任何遥测事件的任何事件字段（最常见的情况是用于解释规则名称的命令行），都会对 URL 进行解析，然后使用可用的 TI 检查其信誉和任何匹配项 | URL 信誉                     | 高: 4.94%<br>中: 5.24%<br>低: 1.47%  |
| 使用 impacket 执行 <sup>27</sup> | 使用 impacket 工具远程执行                                                      | 任何包含命令行的遥测事件<br>EPP 可疑活动检测 | 高: 4.62%<br>中: 0.13%              |
| APT 相关检测                     | 相关 EPP 裁定列表                                                             | EPP 检测                     | 高: 3.50%<br>中: 2.21%<br>低: 1.15%  |
| IDS 检测                       | 网络 IDS 作为 KATA 检测的一部分                                                   | 网络 IDS 检测                  | 高: 1.11%<br>中: 15.70%<br>低: 1.01% |
| 沙盒检测                         | 触发沙盒作为 KATA 检测的一部分。EPP 针对可疑对象没有任何确切的裁定                                  | 沙盒裁定<br>EPP 针对对象的裁定        | 中: 18.25%<br>低: 0.66%             |

关键 — 卡巴斯基

Ski xjt begl he oestne hx  
cirnkoqntsqtne?

Kaojgtqegx!Jtn HPN oenucse  
sjhacieo lnjksqcue qbnekq btiqciy,  
kpukisep qbnekq ciqeggcyaise kip  
nklcp qbnekq neoljioe qj pegcuen  
gekpciy-epye lnjqesqci qbkq feelo  
sxaensnchcikgo jtq kip xjtn atocieoo  
okre.

27 GithubImpacket



技术热图



2-4%

5-7%

8-11%

>12%





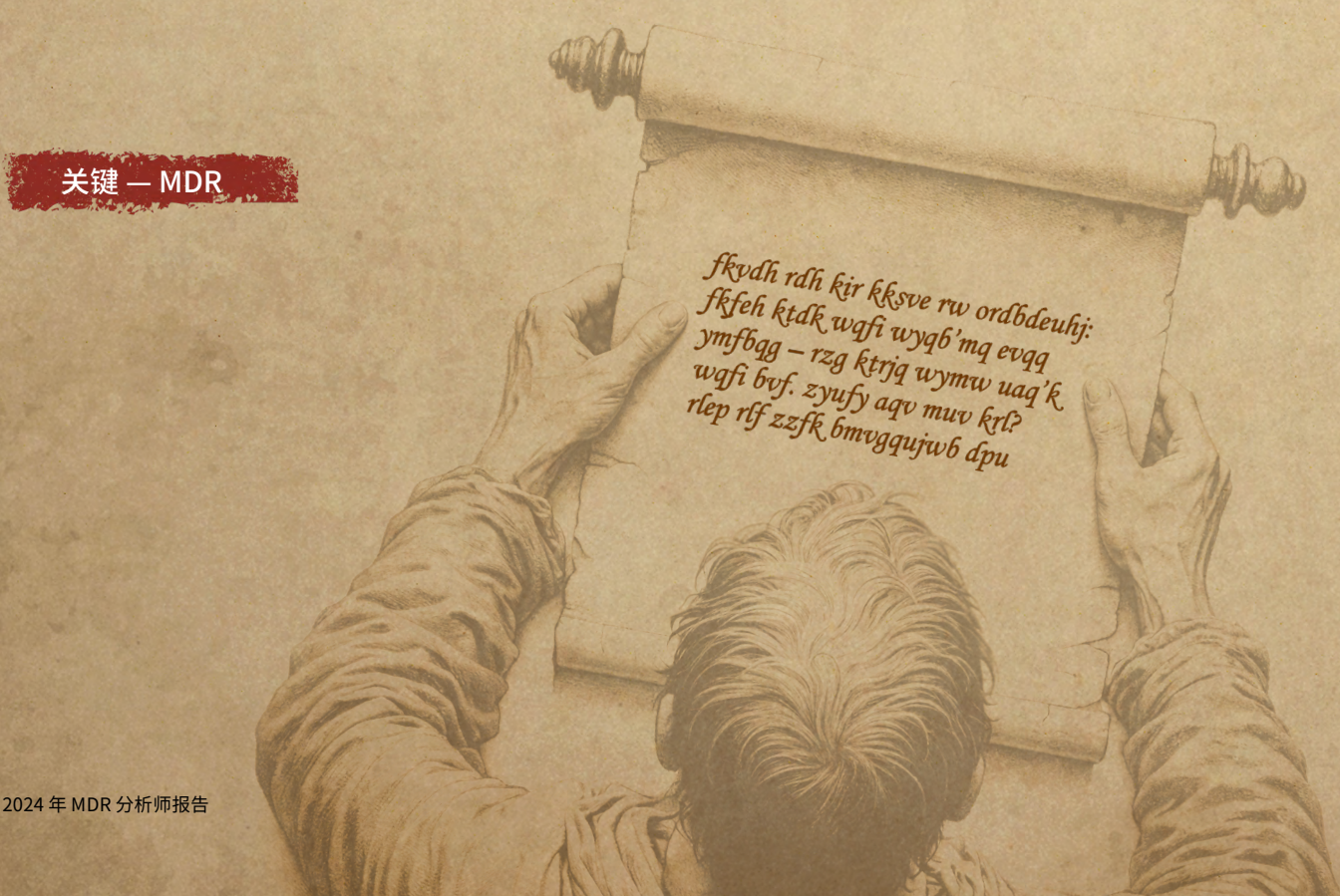
| TA0008:<br>横向移动  | TA0009:<br>收集       | TA0010:<br>渗漏       | TA0011:<br>命令与控制 | TA0040:<br>影响        | TA0042:<br>资源开发 | TA0043:<br>侦查     |
|------------------|---------------------|---------------------|------------------|----------------------|-----------------|-------------------|
| T1210: 利用远程服务漏洞  | T1560: 归档已收集的数据     | T1567: 通过网页服务进行渗漏   | T1071: 应用层协议     | T1565: 数据操纵          | T1588: 获取功能     | T1595: 主动扫描       |
| T1021: 远程服务      | T1005: 来自本地系统的数据    | T1041: 通过 C2 通道进行渗漏 | T1568: 动态解析      | T1561: 磁盘擦除          | T1587: 开发功能     | T1598: 通过网络钓鱼获取信息 |
| T1570: 横向工具转移    | T1114: 邮件收集         | T1048: 通过替代协议实现的渗漏  | T1572: 协议隧道      | T1496: 资源劫持          | T1608: 部署能力     | T1590: 收集受害者网络信息  |
| T1534: 内部鱼叉式网络钓鱼 | T1119: 自动收集         | T1011: 通过其他网络介质进行渗漏 | T1105: 入口工具传输    | T1486: 为了产生影响对数据进行加密 | T1583: 获取基础设施   | T1592: 收集受害者主机信息  |
| T1563: 远程服务会话劫持  | T1113: 屏幕捕获         | T1020: 自动化渗漏        | T1095: 非应用层协议    | T1485: 数据破坏          | T1584: 入侵基础设施   |                   |
| T1080: 污染共享内容    | T1115: 剪贴板数据        | T1029: 计划传输         | T1090: 代理        | T1489: 服务停止          | T1586: 入侵账户     |                   |
|                  | T1125: 视频捕获         | T1030: 数据传输大小限制     | T1219: 远程访问软件    | T1531: 账户访问权限移除      |                 |                   |
|                  | T1025: 来自可移动媒体的数据   | T1052: 通过物理介质进行渗漏   | T1092: 通过可移动介质通信 | T1499: 端点拒绝服务        |                 |                   |
|                  | T1039: 来自网络共享驱动器的数据 |                     | T1102: Web 服务    | T1498: 网络拒绝服务        |                 |                   |
|                  | T1074: 数据暂存         |                     | T1573: 加密通道      | T1490: 禁止系统恢复        |                 |                   |
|                  | T1530: 来自云存储的数据     |                     | T1571: 非标准端口     | T1529: 系统关闭/重启       |                 |                   |
|                  |                     |                     | T1001: 数据混淆      |                      |                 |                   |

2-4%

5-7%

8-11%

>12%





# 关于卡巴斯基

卡巴斯基是一家全球网络安全和数字隐私公司，成立于 1997 年。我们的深度威胁情报和安全专业技术正在不断转化为创新的安全解决方案和服务，可以为全球的企业、重要基础设施、政府和消费者保驾护航。我们提供全面的安全产品线，包括领先的端点保护以及专门的安全解决方案和服务，帮助您应对复杂多变的数字威胁。

## 卡巴斯基安全服务



卡巴斯基  
托管检测和响应



卡巴斯基  
事件响应



卡巴斯基  
SOC 咨询



卡巴斯基  
数字足迹情报



卡巴斯基  
安全评估



卡巴斯基  
损害评估

了解更多

## 享誉全球

卡巴斯基产品和解决方案不断接受独立测试和评审，屡屡斩获佳绩，赢得高度认可与众多权威奖项。我们的技术和流程定期接受全球最受推崇的分析机构的评估和验证，久经考验，屡获殊荣。

了解更多

5,000+

专业人士就在卡巴斯基

50%

的员工是研发专家

5

个独特的专业中心

467,000

卡巴斯基日均检测出的新恶意文件数量

200,000

全球企业客户

49 亿

卡巴斯基在 2024 年检测到的网络攻击数量





卡巴斯基

托管检测和响应

[www.kaspersky.com.cn](http://www.kaspersky.com.cn)

© 2025 AO Kaspersky Lab.  
注册商标和服务商标归其各自所有者所有。

#卡巴斯基  
#引领未来