360漏洞研究院
VULNERABILITY RESEARCH INSTITUTE

360数字安全
数字安全的领导者

2025 年度网络安全漏洞分析报告

360 数字安全集团 ● 漏洞情报服务

目录

01 引言

Executive Summary

2025 年 1 月，DeepSeek 遭遇的大规模境外网络攻击，为这一年定下了激进的基调。这不仅是一次针对 AI 基础设施的流量冲击，更标志着 AI 正式从“辅助工具”进化为网络对抗的“风暴中心”。如果说 2022 年是生成式 AI 走近大众的起点，那么 2025 年则是其全面武器化与防御自主化的引爆点。

在这份年度报告中，我们将深入剖析过去一年重塑全球威胁版图的关键趋势。

- **AI 资产成为攻击“新皇冠”**

从 Langflow 到 SGLang 的远程代码执行漏洞，攻击者的目标已不再局限于传统服务器，而是直指企业核心的 AI 编排平台与模型数据。我们观察到，针对大模型的“零点击”提示注入攻击已成常态，攻击者正试图通过接管 AI Agent 来绕过传统的身份验证。

- **物理边界防御的全面坍塌**

2025 年是边缘设备与物联网资产失陷的重灾区。从思科 IOS XE 遭到恶意软件“BADCANDY”的规模化接管，到宇树机器人因底层协议漏洞导致集群受控，攻击者正利用这些补丁更新滞后、监控虚弱的“黄金入口”实施持续性渗透。这一年，全球边缘设备的受攻击频率较往年增长了数倍，意味着传统的内网隔离策略必须向零信任架构彻底转型。

- **软件供应链的深度投毒**

攻击面已从开源包管理系统（如 npm/PyPI）下沉至 React 和 Next.js 等现代 Web 框架的底层协议。这意味着，即便开发者的业务逻辑毫无瑕疵，底层的通信机制也可能被恶意利用。同时，机器身份（API 密钥、服务账号）的滥用已成为新的身份债务，导致数据泄露事件频发。

- **从人工响应到 AI 自主防御**

面对毫秒级的自动化攻击，传统的安全运营中心（SOC）正面临重构。OpenAI 发布基于 GPT-5 的自主修复 Agent 标志着防御方开始利用大模型进行实时加固。这种“以 AI 对垒 AI”的局面，使得实时、智能的自动化攻防闭环成为组织生存的唯一选择。

02 态势综述

Overview

1. 漏洞总量与趋势

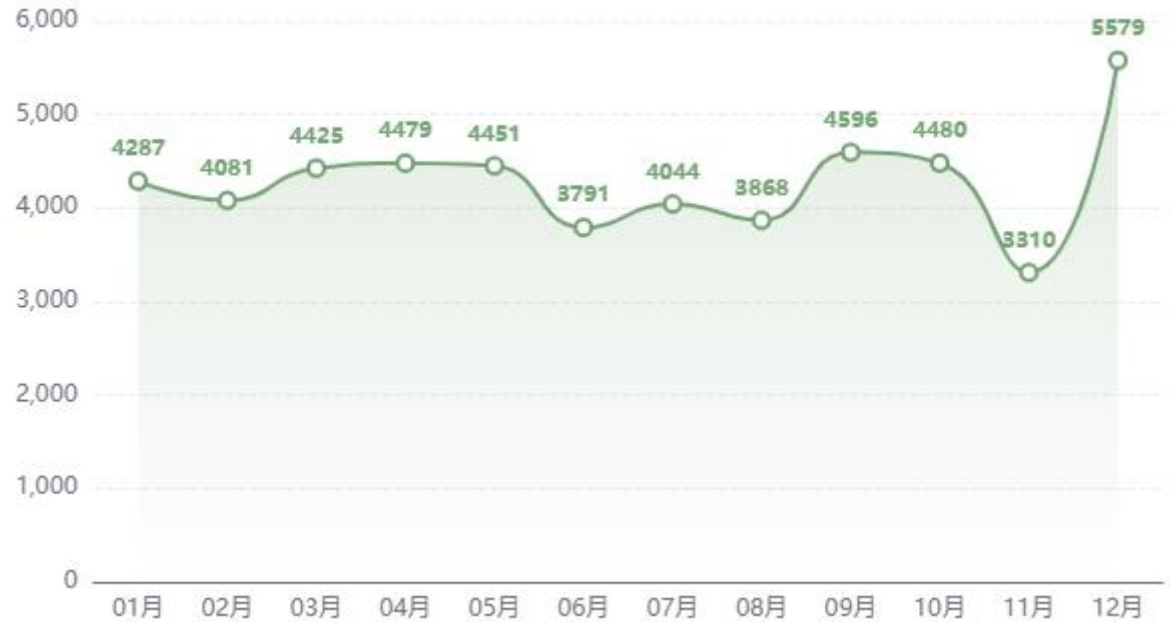

图 1. 漏洞总量月度趋势图

2025 年漏洞总量整体呈现波动上升的趋势，年度平均每月发现漏洞 4283 个。从月度变化来看，漏洞数量在 3 月至 5 月期间维持在较高水平（4400+），随后在 6 月出现显著下降至 3791 个，7-8 月回升至 4000 左右，9 月再次攀升至 4596 个，10 月略有回落。值得注意的是，11 月出现了年度最低值 3310 个，但紧接着 12 月出现了爆发式增长，达到 5579 个，创下年度新高，环比增长率达到 68.55%，远超其他月份的变化幅度。12 月的漏洞数量不仅显著高于年度平均水平（高出 30.27%），也达到了历史最高点，表明年末可能是漏洞披露的高峰期，建议相关组织在此期间加强安全防护措施和漏洞响应准备。

2. 全量漏洞严重程度分析

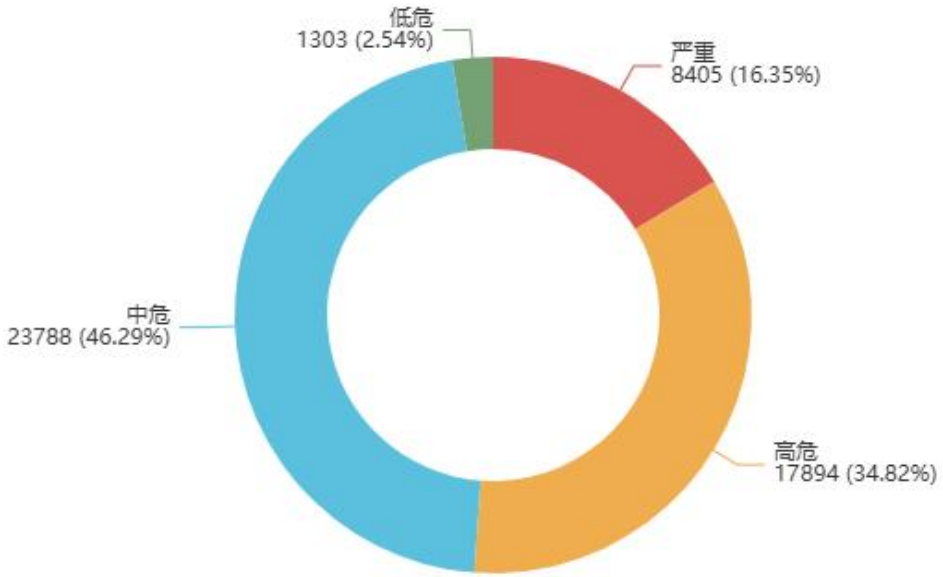

图 2. 漏洞严重性等级占比图

2025 年全网通用型漏洞的等级统计分析，中危漏洞占比最高，达到 46.29%（23788 个），高危漏洞次之，占 34.82%（17894 个），严重漏洞占 16.35%（8405 个），低危漏洞占比最少，仅为 2.54%（1303 个）。从累积分布来看，中危和高危漏洞合计占比达 81.11%，构成了年度漏洞的主要部分。虽然严重和高危漏洞对网络安全构成直接威胁，但中危漏洞的数量优势使其在整体风险暴露面上占据主导地位。建议相关组织在优先处置严重和高危漏洞的同时，不能忽视中危漏洞的累积效应，特别是在资源有限的情况下，应建立基于风险评估的分级处置策略，确保关键系统不受高等级漏洞影响，同时通过系统性修复降低中危漏洞的整体暴露风险。

3. 漏洞类型分析

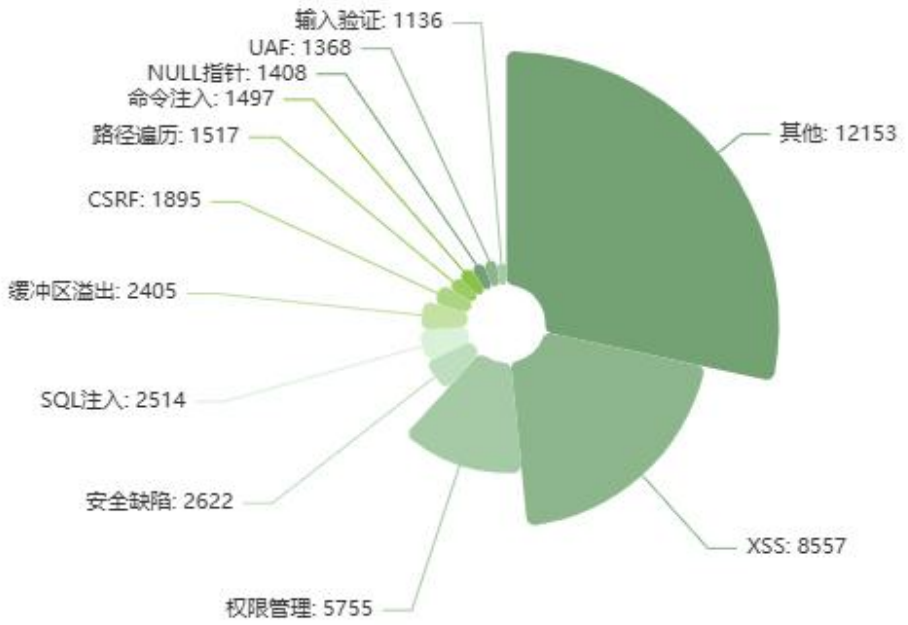

图 3. 漏洞类型占比图

根据 2025 年全网通用型漏洞类型的统计分析，Web 应用安全问题仍然是最主要的安全威胁，其中"其他"类型漏洞占比最高，达到 28.38%（12153 个）。跨站点脚本攻击(XSS)以 19.98%的占比（8557 个）位居第二，权限管理不当类漏洞占 13.44%（5755 个）位列第三。SQL 注入、缓冲区溢出等传统安全问题依然占据一定比例，分别为 5.87%和 5.62%。从累积分布来看，前三类漏洞合计占比已达 61.80%，构成了年度漏洞的主要部分。值得注意的是，OWASP Top 10 中的主要 Web 安全风险（如 XSS、权限管理不当、SQL 注入、CSRF 等）合计占比超过 50%，表明 Web 应用程序仍是网络安全防护的重点领域。建议相关组织重点关注 Web 应用安全防护，加强输入验证、访问控制和安全编码实践，同时建立完善的漏洞管理机制，优先处置高风险漏洞类型。

4. 行业漏洞数据分析

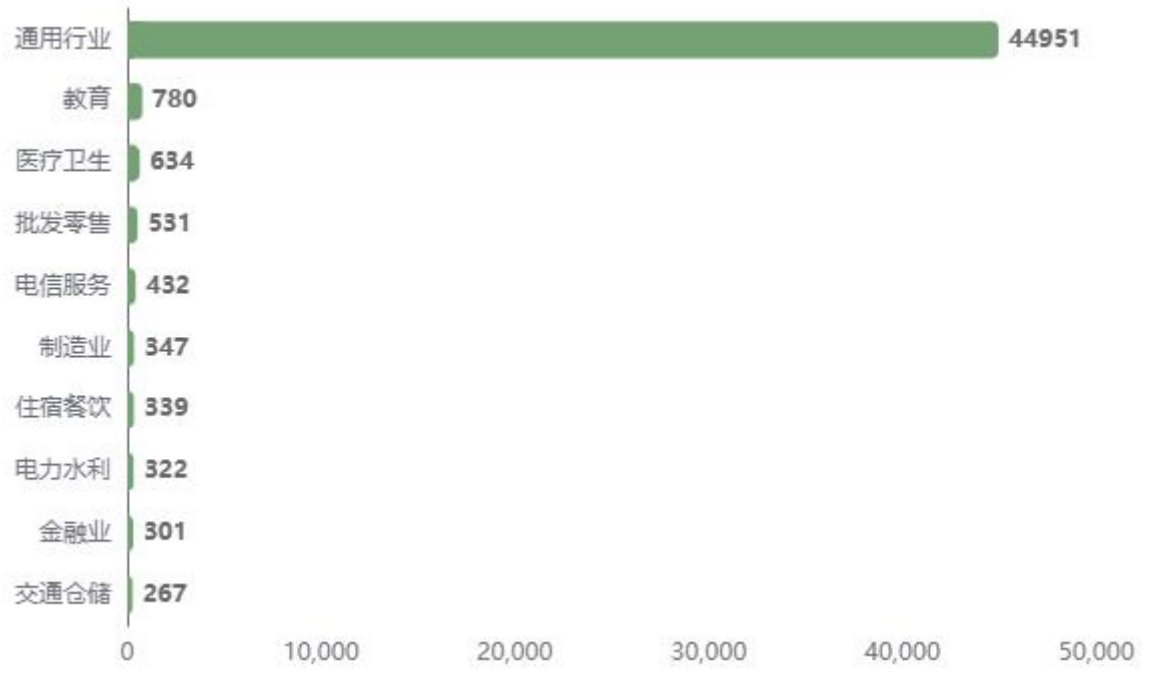

图 4. 漏洞行业分布图

2025 年全网通用型漏洞行业分布的分析来看，漏洞主要集中在“通用行业”，其记录占比高达 87.5%（44,951 个），表明绝大多数漏洞为跨行业通用的软件或组件漏洞，具有广泛的潜在影响面。在具体行业中，教育（780 个）、医疗卫生和社会工作（634 个）以及批发和零售业（531 个）成为漏洞数量最多的三大垂直领域。这一分布特征凸显了数字化进程较快、线上业务密集且系统复杂度高的民生服务行业正面临显著的安全压力。电信、广播电视和卫星传输服务（432 个）及制造业（347 个）紧随其后，表明关键信息基础设施和实体经济的重要支柱同样存在大量安全隐患。值得注意的是，尽管金融业通常被视为安全重镇，但其上报漏洞数量（301 个）仍位居前列，提示其面临持续威胁。整体而言，漏洞风险呈现出“普遍性基础风险”与“行业性集中风险”并存的局面。建议在持续推进通用组件安全治理的同时，必须重点加强对教育、医疗、零售等漏洞高发行业的针对性防护与漏洞消减支持。

03 月度全景

Monthly Timeline

一月 | AI 时代的“斯普特尼克时刻”：大模型基建化与边界防御的初步坍塌

核心焦点：DeepSeek DDoS 攻击、Windows LDAP 零点击 RCE、VPN 供应链连环劫持

DeepSeek 遭受大规模境外网络攻击事件

2025 年 1 月底，国产 AI 大模型 DeepSeek 突然遭遇大规模境外 DDoS 攻击，攻击手段在除夕前夜显著升级并持续发酵，引发了全球对 AI 技术博弈下网络安全的高度关注。此次事件不仅涉及针对 AI 基础设施的流量冲击，还诱发了大量以 DeepSeek 为诱饵的欺诈和网络钓鱼活动，迫使安全机构发布全面分析指南以应对这一复合型的安全挑战。其影响范围从技术层面的服务可用性延伸至社会层面的反欺诈防御，凸显了新兴 AI 平台在成为全球焦点后所面临的严峻地缘政治与黑产威胁环境。

Ivanti 产品系列漏洞链利用与 CISA 紧急告警

2025 年 1 月，Ivanti Connect Secure 及 CSA 设备被爆出存在严重的代码执行与缓冲区溢出漏洞（CVE-2025-0282）。CISA 与 FBI 联合发出警告，指出黑客正通过漏洞攻击链（Chained Attacks）利用这些缺陷入侵网络，甚至部分旧漏洞仍被持续利用。此类针对 VPN 和云服务网关的攻击性质极其恶劣，攻击者一旦得手即可获取企业内网的完整访问权，导致大规模的数据泄露或勒索病毒植入。

SonicWall SMA1000 零日漏洞利用事件

SonicWall 的安全设备在 2025 年初面临严峻挑战，CISA 确认其 SMA1000 系列漏洞已被攻击者在野利用。随后，厂商又紧急发布了关于 CVE-2025-23006 等关键漏洞的补丁，指出这些漏洞可能导致认证绕过，让未经授权的攻击者非法访问 VPN 资源。由于此类设备处于网络防御的最前沿，漏洞的武器化直接导致了多起针对企业边界的入侵事件，目前该漏洞已被正式列入 CISA 的“已知利用漏洞目录”中。

Windows LDAP 零点击远程代码执行漏洞

2025 年 1 月间，针对 Windows 轻量级目录访问协议（LDAP）的多个高危漏洞（涉及整数溢出及拒绝服务）接连曝光，并有相关的 PoC 工具发布。其中最令安全界担忧的是具备“零点击”（Zero-click）特性的 RCE 漏洞，攻击者无需用户交互即可通过构造恶意请求导致域控制器 LSASS 进程崩溃甚至执行任意指令。这一漏洞链条不仅严重威胁企业身份认证核心的安全，更可能导致整个 Windows 域环境的沦陷，其潜在的破坏力使其成为近期攻防演练和实战威胁情报中的核心焦点。

2025 年初国产大模型爆发不仅是中国 AI 的“斯普特尼克时刻”，更是全球网络安全对抗模式的一个里程碑，它标志着大模型已正式从单纯的生产力工具跃升为地缘政治博弈中的核心战略基础设施。这场波及全球、峰值达 3.2Tbps 的超大规模 DDoS 攻击，辅以从 API 接口渗透、Open ClickHouse 数据库误配置泄露到 PyPI 供应链投毒的复合攻势，暴露出在 AI 竞速的狂热下，高达 90%的私有化部署服务器仍处于“裸奔”状态的严峻现实。对于安全工程师而言，这既是机遇也是毁灭性的挑战：一方面，AI 规模经济正在极大降低安全防御的边际成本，GPT-5 级自主修复 Agent 的出现让我们看到了毫秒级响应的曙光；但另一方面，AI 资产的高度集权化也使其成为了极易被针对的“单一故障点”，攻击者正利用模型推理层与底层协议的黑盒特性，将漏洞利用从代码层下沉至认知与供应生态层。2025 年的开篇大戏警示我们，安全防线必须从“围墙式外挂”转向“模型级内生”，否则技术红利的喷涌将不可避免地伴随着难以承受的系统性安全债务。

二月 | “零点击”间谍阴云：雇佣兵式网络武器与高价值目标的精准“狩猎”

核心焦点：WhatsApp 零交互监控、塔塔科技勒索危机、PDF 诱饵间谍活动

WhatsApp 零点击（Zero-click）间谍软件攻击

2025 年初，以色列间谍软件公司 Paragon 被爆出利用 WhatsApp 的零点击漏洞发起秘密监控，Meta 随后确认约 90 名用户因此遭受定向攻击。该攻击的恐怖之处在于受害者无需任何操作即可被植入间谍软件，导致个人隐私和敏感通讯被彻底窃取，这一事件再次引发了全球对高价值个人、政府官员及记者面临的顶级雇佣兵式网络武器威胁的恐慌，并对即时通讯软件的安全性提出了根本性质疑。

印度科技巨头塔塔科技（Tata Technologies）遭勒索软件攻击

2025 年 1 月至 2 月期间，印度跨国公司塔塔科技连续多次出现在安全新闻快报中，确认其 IT 系统遭到勒索软件入侵。该事件导致这家工程服务巨头的全球业务运营出现显著中断，大量敏感企业数据面临泄露风险，其作为供应链核心环节的地位使得攻击影响波及了汽车、航空等多个下游客户行业，成为 2025 年初大型企业防御勒索软件产业化升级的典型受害案例。

由“肚脑虫（APT-C-35）”发起的 PDF 诱饵攻击

2025 年初，安全机构分析并披露了 APT 组织“肚脑虫”利用特定 PDF 文档作为诱饵的新一轮攻击活动。该组织通过精心设计的社会工程学手段，利用 PDF 渲染或处理漏洞植入木马，旨在进行精准的间谍活动，这一持续性的攻击态势表明针对敏感目标的定向文档渗透依然是高级持续性威胁中的主流手段。

三月 | 算力夺权与框架之殇：当 AI 工具链沦为攻陷全球巨头的“数字特洛伊”

核心焦点：Bybit 巨额加密劫案、Apache Tomcat RCE、迪士尼 AI 工具投毒事件

Bybit 交易所巨额加密资产劫案

2025 年 2 月至 3 月期间，加密货币交易所 Bybit 遭遇了史上规模最大的黑客攻击之一，导致约 14 亿至 15 亿美元的以太坊被盗。黑客在短短 10 天内通过去中心化交易所将数百万美元资金洗白，迫使 Bybit 首席执行官宣布进入冻结黑客资金的关键周，该事件不仅重创了 Bybit 的资产储备，更引发了对冷钱包安全性和链上 UI 防御机制的全球性反思。

Apache Tomcat 远程代码执行漏洞 (CVE-2025-24813)

2025 年 3 月，CNNVD 与各大安全机构对 CVE-2025-24813 发布紧急通报，指出该漏洞允许远程攻击者在满足特定配置的 Tomcat 服务器上执行任意代码。由于 Tomcat 是企业级 Java Web 应用的主流中间件，该漏洞的披露引发了金融、政府等行业对资产风险排查的高度重视。

木马化人工智能工具导致迪士尼黑客攻击

2025 年 3 月，一起极具前瞻性的攻击事件被披露，攻击者通过投放带有木马的伪造 AI 开发工具，诱使迪士尼内部人员下载并最终实现了内网渗透。这一事件标志着“AI 工具供应链攻击”已正式进入实战阶段，展示了黑客如何利用当下的 AI 热潮作为社工诱饵，对全球知名媒体巨头进行精准的数字资产窃取。

四月 | 攻防演进的“点杀”时代：国家级黑客的底层渗透与开发环境的“灯下黑”

核心焦点：亚冬会溯源反制、Vite 开发工具漏洞、Oracle 老旧资产失陷

以“亚冬会”为目标的国家级黑客攻击与溯源

2025 年初，随着哈尔滨亚冬会的举办，360 安全团队监测到并成功溯源了一起针对赛会基础设施的大规模网络攻击。分析显示，攻击源头指向了美国 NSA 关联的特工及相关高校实验室，攻击者利用了精密设计的恶意载荷试图窃取赛事组织数据，此次事件不仅是网络空间对抗的体现，更标志着针对大型国际体育赛事的数字间谍活动已进入高度组织化阶段。

Vite 开发工具任意文件读取漏洞 (CVE-2025-32395/31486)

2025 年 4 月，流行的前端开发工具 Vite 被曝出多个高危的任意文件读取漏洞，且相关 PoC（概念验证）已在社区公开流传。该漏洞允许攻击者通过精心构造的请求，越权访问开发服务器上的敏感配置文件或源代码。由于 Vite 在现代 Web 开发中极其普及，该漏洞的爆发导致大量处于开发或调试阶段的项目面临源码泄露风险，迫使开发者紧急升级版本以修补供应链前端防线。

Oracle 季度关键补丁更新与老旧服务器被黑事件

2025 年 4 月，Oracle 发布了年度第二次关键补丁更新，修复了涉及 WebLogic、数据库等产品的数百个漏洞。几乎同一时间，甲骨文确认两台老旧服务器遭黑客入侵，虽然未波及核心云数据，但这一“灯下黑”的讽刺性事件揭示了即使是顶级安全厂商，其非核心生产环境的防御短板也极易成为攻击者的突破口，再次警示了全量资产排查的重要性。

Samsung 德国大规模客户数据泄露

2025 年 4 月，三星德国分公司确认遭受数据泄露攻击，约 27 万名客户的敏感信息被非法获取。攻击者利用了第三方服务商的配置漏洞实施了入侵，尽管未涉及支付信息，但大规模的客户资料泄露导致了严重的品牌声誉受损及后续针对性的电信诈骗风险，再次敲响了大型跨国公司全球供应链安全管理的警钟。

SourceForge 平台沦为恶意软件分发跳板

2025 年 4 月，传统软件托管平台 SourceForge 被监测到遭到黑客滥用，攻击者通过在合法项目中插入混淆代码或直接上传仿冒软件来传播恶意病毒。利用开发者对知名托管平台的信任，黑客成功避开了部分杀毒软件的静态扫描，导致大量下游用户在更新常用软件时被植入窃信木马或勒索软件。

国家级攻击事件的深度分析揭示了 挑战 的极端性：攻击方如美国 NSA（TAO）不再满足于外围的流量冲击，而是转而激活预置的操作系统底层后门，并结合特定应用系统的零日漏洞实施精准“点杀”，这种从供应链末端向上渗透的 TTPs（战术、技术与路径）让传统基于规则的防火墙形同虚设。然而，挑战中蕴含的 机遇 同样具有跨时代意义：我国安全机构首次实现对国家级黑客组织个人身份的精准溯源与通缉，验证了“安全大模型+全网大数据”在毫秒级对抗中化解复杂伪装、捕捉跳板轨迹的能力，标志着防御范式正从被动的“封堵补丁”转向主动的“威胁狩猎”与实体化反制，为未来高强度对抗下的关键基础设施防护树立了实战标杆。

五月 | 零售业的“散布之影”：医疗与商业关键基础设施的韧性大考

核心焦点：英国零售业系统性受袭、Ascension 医疗二度失陷、Llama-Index AI 漏洞

英国大型零售商（哈罗德、玛莎百货等）连续遭袭

2025 年 5 月，英国零售业遭遇系统性网络冲击，哈罗德百货（Harrods）确认遭受企图性网络攻击，紧接着玛莎百货（Marks & Spencer）也被爆出与黑客组织“散布的蜘蛛（Scattered Spider）”有关的入侵事件。由于这已是短期内第三家遭受重创的大型零售商，英国政府特工及 NCSC 已介入调查，事件导致大量客户数据安全受疑，并引发了对供应链防御漏洞和关键商业基础设施韧性的广泛担忧。

医疗巨头 Ascension 连续遭受第二次网络攻击

2025 年 5 月初，医疗保健集团 Ascension 披露其遭受了针对患者数据的第二次重大网络攻击，事件涉及第三方服务商的防御崩溃。攻击者利用了外包环节的脆弱性深度渗透，导致敏感的患者医疗记录面临泄露，迫使集团进入紧急通报流程，该事件标志着针对医疗系统的攻击已从单纯的勒索演变为针对性极强的、具有持续破坏性的数据窃取活动。

防勒索巨头 Hitachi Vantara 遭 Akira 团伙攻破

2025 年 5 月，以“防勒索专家”著称的 Hitachi Vantara 被勒索软件组织 Akira 成功入侵，陷入了“医者不能自医”的尴尬处境。Akira 团伙通过利用未公开的边界漏洞获取了权限，不仅加密了核心业务数据，更可能获取了其安全方案的技术细节，这一具有讽刺意味的事件严重打击了行业信心，凸显了顶级安全服务商在专业黑客团伙面前同样存在被渗透的高风险。

Llama-Index CLI 远程命令执行高危漏洞 (CVE-2025-1753)

2025 年 5 月，人工智能开发领域的关键工具 Llama-Index 被爆出存在 CLI 命令行注入漏洞，其 CVSS 评分显示为极高危。攻击者可以通过精心构造的输入在受影响的服务器上直接执行任意指令，由于该工具是目前构建大模型应用的核心组件，该漏洞的发现意味着大量 AI 生产环境处于“裸奔”状态，引发了 AI 开发者群体的一场紧急修补竞赛。

Npm 与 PyPI 供应链中的“土耳其代码”恶意软件

2025 年 5 月，安全机构监测到一场针对开源生态系统的深层供应链攻击，新的恶意软件操作正在疯狂袭击 Npm 和 PyPI 仓库，目标直指全球数百万开发者。攻击者通过伪装成合法工具包或利用拼写偏差植入恶意代码，一旦开发者在构建过程中引入这些包，其敏感凭据及 CI/CD 信息将被立即窃取。此事件导致大量下游应用面临“先天性”染毒风险，再次重创了全球软件供应链的信任体系，迫使开发者对自动化依赖更新策略进行紧急审计。

六月 | 邮件即入侵，协议即跳板：老旧 IoT 设备与科研机构的“全网大沦陷”

核心焦点：WebDAV 与 Roundcube 邮件 RCE、新型 Mirai 变体、摩诃草科研窃密

Windows WebDAV 客户端远程代码执行漏洞 (CVE-2025-33053)

微软针对 Windows WebDAV 客户端发布了紧急安全预警，修补了代号为 CVE-2025-33053 的远程代码执行漏洞。攻击者通过构造恶意的网络资源并诱导用户访问，可以在无需授权的情况下在受害者机器上执行任意指令。由于 WebDAV 协议在企业协作环境中被广泛调用，该漏洞的披露引发了全球管理员的“补丁竞赛”，以防止勒索软件利用该路径进行横向传播。

Roundcube Webmail 代码执行漏洞 (CVE-2025-49113)

流行的开源邮件系统 Roundcube 确认存在 CVE-2025-49113 高危代码执行漏洞，且被复发现存在在野利用。攻击者只需发送一封特定格式的恶意邮件，即可在邮件服务器上执行系统命令，这种“邮件即入侵”的攻击模式对政府、高校及中小型企业的自建邮件服务器造成了毁灭性威胁。

新型 Mirai 僵尸网络利用 DVR 漏洞扩张

一种新型 Mirai 僵尸网络变体正通过命令注入漏洞疯狂感染 TBK DVR 设备。攻击者利用此类 IoT 设备普遍存在的固件弱点实施远程入侵，并将其纳入庞大的僵尸网络集群，用于发起更大规模的 DDoS 攻击或作为内网渗透的跳板。该事件凸显了老旧联网设备在面对现代化僵尸网络攻击时的脆弱性，也使得针对关键基础设施的流量防御压力在 2025 年年中达到峰值。

摩诃草 (APT-C-09) 针对高校的定向窃密行动

APT 组织“摩诃草”被监测到正通过仿冒高校官方域名的手段，针对科研人员实施精准的钓鱼与窃密行动。攻击者通过高度仿真的登录页面获取受害者的办公账号权限，进而渗透实验室网络获取核心科研数据。这一持续性的定向攻击不仅反映了 APT 组织在社工手段上的精进，也凸显了高校及科研机构在数字化转型中面临的严峻地缘政治情报威胁。

巴黎迪士尼乐园 64GB 机密文件泄露事件

黑客组织公开曝光了从巴黎迪士尼乐园窃取的 64GB 机密文件，涉及大量内部运营细节和潜在的敏感数据。此次泄露事件起源于针对其内部办公系统的深度渗透，不仅让这家全球知名娱乐巨头面临严峻的隐私合规挑战，更在品牌声誉和企业核心资产保护方面造成了难以估量的负面影响。目前，相关的地下黑产交易已针对这部分数据展开，进一步加剧了其员工和客户的个人风险。

七月 | 信任链的“静默污染”：Slopsquatting 幻觉投毒与软件供应链的信用破产

核心焦点：AI 助手生成代码投毒、npm “is”库被接管、AT&T 天价数据和解案

新型“Slopsquatting”供应链攻击威胁

一种针对 AI 编码助手的全新供应链攻击方式——“Slopsquatting”被曝光。攻击者利用 AI 助手在生成代码时产生的“幻觉”，预先注册这些幻觉生成的虚假软件包名并植入恶意载荷，导致开发者在不知情中引入中毒代码。这种利用 AI 工具逻辑缺陷的新型攻击手段，直接绕过了传统的代码审计，对全球正在快速普及的 AI 驱动型开发模式构成了基础性的安全挑战。

Microsoft 365 Direct Send 伪造邮件精准钓鱼

黑客被监测到正在疯狂滥用 Microsoft 365 的 Direct Send 功能，通过伪造内部员工身份向美国企业发送精准的钓鱼邮件。攻击者巧妙利用了该功能在邮件验证机制上的盲点，使得欺诈邮件能够完美绕过企业的 SPF 和 DKIM 检查，直接进入受害者收件箱并极具迷惑性。这起事件显著提升了企业防御社交工程攻击的成本，证明了即使是成熟的云协作平台也存在被恶意利用的协议级风险。

JavaScript 库“is”遭 npm 供应链投毒

拥有数百万周下载量的热门 JavaScript 库“is”被发现遭到了 npm 供应链攻击并植入后门。黑客通过接管维护者权限或复杂的社工手段，在合法版本中插入了敏感凭据窃取脚本，导致无数依赖该库的前端项目面临资产失窃风险。该事件再次暴露了现代 Web 开发中过度依赖小型开源软件包所潜伏的系统性危机。

AT&T 达成 1.77 亿美元数据泄露和解协议

电信巨头 AT&T 就其跨越 2019 年至 2024 年的两次重大数据泄露事件（涉及超 1 亿用户）达成了高达 1.77 亿美元的和解协议。这些泄露多由第三方云数据库配置不当和系统漏洞被利用所致，导致海量公民身份及通话记录流入黑市。这起天价和解案标志着法律监管机构对电信巨头数据保护不力的严厉惩治，同时也反映了大型企业在长期资产管理中的安全积弊。

新型 Hpingbot 僵尸网络大规模爆发

安全机构监测到一种名为 Hpingbot 的僵尸网络正通过滥用 Pastebin 平台来分发恶意负载，并利用成熟的 Hping3 工具发起猛烈的 DDoS 攻击。攻击者利用合法的公共内容托管平台作为 C2 指令站，极大增加了溯源和封禁的难度，导致大量受害服务器因瞬时的高带宽流量冲击而瘫痪。

2025 年爆发的大规模 JavaScript 库遭 npm 供应链投毒事件，标志着攻击向量已从简单的“拼写劫持”演进为以“Slopsquatting（AI 垃圾包投毒）”为代表的精细化渗透，深刻揭示了现代开发生态中信任链条的极度脆弱。其挑战在于，随着 AI 生成代码的泛滥，海量低质且自带恶意逻辑的包碎片彻底湮灭了传统的人工审计防线，使开发者的本地环境（如 Vite 等构建工具）沦为进入企业内网的隐形跳板，这种“静默污染”正在透支开源社区的信用根基。然而，此危机亦带来了重塑行业标准的新机遇：它强制加速了从“事后漏洞扫描”向“原生准入控制”的范式转变，推动了具备行为监控能力的动态 SBOM（软件物料清单）和 AI 启发式沙箱审计技术的全面落地，迫使安全边界从生产环境彻底前移至开发者的每一行依赖引用，真正开启了软件供应链的“零信任”时代。

八月 | 勒索引擎的“AI 智能化”：PromptLock 现身与身份准入核心的门禁失守

核心焦点：AI 驱动勒索软件、Cisco ISE 未授权 RCE、GitHub 恶意游戏外挂分发

全球首例 AI 驱动勒索软件 "PromptLock" 现身

网络安全领域迎来了一个危险的里程碑，安全机构发现并确认了首个在真实攻击中利用 AI 驱动的勒索软件——"PromptLock"。不同于传统勒索软件，它利用大模型实时生成的动态加密逻辑和话术来对抗 EDR（端点检测与响应）系统的启发式扫描，实现了极高的静默感染率。该事件标志着自动化和智能化攻击手段正式进入实战阶段，迫使全球安全防御体系必须从基于特征的检测向基于行为的实时 AI 审计转型。

CrushFTP 零日漏洞 (CVE-2025-54309) 的在野利用

广泛使用的文件传输服务器 CrushFTP 被曝出存在一个严重的零日漏洞，相关 PoC（概念验证代码）迅速在网络公开并遭到了黑客团伙的野外利用。该漏洞源于系统对用户提供的路径处理不当，允许攻击者在无需身份验证的情况下进行任意文件读写或执行恶意代码。此次事件迫使大量依赖该平台进行跨境数据传输的企业紧急停机修补，暴露了企业级文件传输基础设施在面对突发零日威胁时的防御短板。

Cisco ISE/ISE-PIC 未授权远程代码执行漏洞 (CVE-2025-20281)

思科（Cisco）紧急通报了身份服务引擎（ISE）中的一个严重漏洞，其技术细节随之公开。该漏洞允许远程、未经身份验证的攻击者在底层操作系统上执行 root 级别的命令。由于 ISE 是企业网络准入控制的核心，该漏洞的爆发意味着企业内网的“门禁系统”可能彻底沦为黑客进入内网的坦途，其影响范围覆盖了全球多数顶级跨国企业的网络基础设施。

GitHub "SmartLoader" 恶意软件活动与游戏外挂投毒

安全研究人员曝光了一场利用 GitHub 平台分发恶意软件的持续性活动。攻击者通过伪装成流行的游戏外挂或辅助工具吸引用户下载，实则内置了名为 "SmartLoader" 的加载器。该恶意软件利用了多层混淆技术避开静态检测，一旦在玩家机器上运行，便会静默下载后续的窃信木马（Infostealer），导致大量个人游戏账户凭据及系统敏感数据被远程窃取，严重破坏了开源平台和玩家社区的互信环境。

新型 AI 工具革命性革新内网威胁防御体系

一批新型 AI 安全防御工具在行业内引发热议，它们通过深度学习流量模式来革新传统的内网威胁监测手段。这些工具能够识别出黑客利用逻辑漏洞实施的极其细微的横向移动行为，有效弥补了传统防火墙和入侵检测系统在应对内部人员或已受损凭据时的无能。该趋势表明，随着攻击手段的智能化，防御方正试图利用 AI 的大规模数据吞吐能力重新夺回在内网对抗中的主动权。

九月丨具身智能的物理冲击：从 s1ngularity 自动化扩散到朝日啤酒生产线停摆

核心焦点：GitHub 账号自动化劫持、制造业 OT 网络瘫痪

AI 驱动的 s1ngularity 攻击重创 GitHub 账户

一场代号为 "s1ngularity" 的攻击浪潮利用 AI 自动化工具感染了超过 2180 个 GitHub 账户。攻击者通过 AI 生成的高质量恶意代码库和自动化脚本进行大规模扩散，旨在窃取开发者的 SSH 密钥和 CI/CD 秘密。此事件标志着利用 AI 提升攻击吞吐量的产业化趋势日益明显，对全球软件源代码的安全性造成了系统性冲击。

WhatsApp 与 Apple 零日漏洞协同攻击事件

黑客组织正利用 WhatsApp 的一个未公开缺陷，配合苹果系统的零日漏洞，针对特定目标发起高度隐蔽的间谍软件攻击。攻击者通过构造特殊的媒体文件或诱导点击，在受害者毫无察觉的情况下绕过系统沙箱，实现远程代码执行。这一事件反映了顶级威胁行为者利用跨平台漏洞链进行协同渗透的复杂性，对全球移动端隐私安全构成了严峻威胁。

啤酒巨头朝日（Asahi）受攻击停产事件

全球啤酒酿造巨头朝日（Asahi）确认遭遇严重网络袭击，导致部分生产线被迫停摆。攻击者渗透进其 OT（运营技术）网络与生产管理系统，实施了破坏性活动，直接影响了全球供应链的供应能力。此次事件作为针对关键制造业的典型案例，展示了网络攻击从数字空间向物理生产环境渗透的巨大破坏力。



十月 | “影遁”提示词注入：AI Agent 逻辑资产泄露与电商生态的支付劫持

核心焦点：AI 代理参数注入攻击、Windows WSUS 补丁服务器 RCE、无印良品供应链断裂

AI 代理参数注入与“影遁”零点击攻击漏洞

随着人工智能的普及，针对 AI Agent 的新型攻击成为报道重点。多款流行 AI 代理（如 Copilot Studio 等）中存在关键参数注入和提示词注入漏洞，使攻击者能远程执行代码或窃取敏感的 OAuth 令牌。更具威胁性的是被称为“影遁（Shadow Escape）”的零点击攻击，这种手段无需用户交互即可通过 AI 助手的逻辑漏洞访问后端数据，致使数万亿条记录面临泄露风险。这些事件标志着网络攻击已从传统的软件代码层延伸至 AI 模型推理与指令层，对新兴的 AI 生产力工具提出了严峻的安全挑战。

Windows Server WSUS 远程代码执行漏洞 (CVE-2025-59287)

Windows Server 更新服务（WSUS）被发现存在远程代码执行漏洞，攻击者可以在未经身份验证的情况下，通过预身份验证阶段的逻辑缺陷实现远程代码执行（RCE）。2025 年 10 月下旬，微软发布了紧急修复程序，但随后安全研究人员发现黑客已开始利用该漏洞投放 Skuld 等信息窃取木马，导致数千个暴露在公网的收件箱和服务器面临被完全接管的风险。由于 WSUS 广泛应用于企业内网更新管理，该漏洞的爆发严重威胁了全球企业的内网安全生态。

Adobe Commerce 与 Magento 严重漏洞 (CVE-2025-54236)

漏洞涉及 Adobe Commerce 和 Magento 的嵌套反序列化问题，属于关键的远程代码执行漏洞。自 2025 年 10 月漏洞细节公开以来，全球已有超过 250 起针对该漏洞的活跃攻击，平均每 5 家相关商店中就有 3 家存在安全风险。攻击者利用此漏洞可以绕过身份验证并接管用户会话，进而窃取支付信息或控制整个电商后端。由于受影响版本广泛且攻击门槛较低，该事件促使 CISA 及多家安全机构紧急发布预警，要求零售商立即修补以防止大规模的财务数据泄露。

零售巨头无印良品（MUJI）供应商遭勒索软件攻击

由于关键物流合作伙伴遭受勒索软件袭击，零售巨头无印良品被迫暂停了其在日本等地的在线销售业务和发货服务。虽然攻击并非直接针对无印良品自身系统，但供应商系统的瘫痪导致其核心电商链路中断。此类“间接打击”不仅造成了巨大的直接经济损失，还迫使企业在数字化转型中重新审视第三方风险管理。该事件与同期发生的雷诺英国数据泄露、凯帕（Capita）创纪录罚款等事件共同揭示了勒索软件对现代商业供应链的摧毁性影响。

三星 Galaxy S25 与移动端零日漏洞攻击

三星最新旗舰机型 Galaxy S25 被爆出存在零日漏洞。文档披露，黑客已能在野外利用该漏洞远程启用手机摄像头并持续追踪用户的地理位置信息。此外，新闻还提到了针对 Android 免接触支付的 NFC 中继恶意软件，以及伪装成 Minecraft 等应用的 Python 木马。这些事件反映出针对个人隐私和移动金融的攻击手段正变得愈发隐蔽且高效，攻击者正利用系统底层漏洞和社交工程学相结合的方式，对高端移动设备用户实施全方位监控。

十一月丨闪电贷逻辑坍塌与 BADCANDY 逆袭：金融合约与基础设施的极速渗透

核心焦点：Balancer 协议 1.28 亿损失、思科 IOS XE 持久化控制、Linux 内核 UAF 提权

大型语言模型（LLM）“零点击”与提示注入漏洞

针对生成式人工智能的安全研究成为焦点，多份报告指出 GPT-4o、GPT-5 以及 Microsoft 365 Copilot 存在严重的零点击攻击漏洞和提示词注入风险。通过构造特殊的输入指令，攻击者可以绕过 AI 模型的安全护栏机制，诱导 AI 泄露用户的隐私数据、OAuth 令牌，甚至在某些集成环境中执行恶意代码。随着 AI 代理（Agent）的广泛普及，此类攻击标志着网络威胁已从传统软件层延伸至模型推理层，对现代企业的 AI 应用安全提出了全新的挑战。

Balancer 协议遭大规模黑客攻击导致 1.28 亿美元损失

去中心化金融协议 Balancer 的 V2 池遭受了精心策划的多轮攻击，在短短 30 分钟内被抽干了价值约 1.28 亿美元的加密资产。调查显示，这是一场经过数月准备的高级渗透行动，攻击者利用了智能合约中的闪电贷逻辑缺陷实施非法套利。此次事件不仅造成了巨额的直接经济损失，更重创了投资者对 DeFi 协议安全性的信心，引发了金融科技领域对区块链底层代码审计及实时威胁监控机制的深度反思。

Cisco IOS XE 系列产品遭 BADCANDY 恶意软件攻击

多个国家安全机构（如澳大利亚 ASD）发布紧急警报，称黑客正在大规模利用思科 IOS XE 操作系统的零日漏洞实施攻击。攻击者通过该漏洞在受害设备中部署名为“BADCANDY”的 Web Shell，从而获取对网络设备的持久控制权。这一事件对全球网络基础设施构成了直接威胁，大量路由器和交换机面临被非法接管的风险，可能导致大规模的流量劫持或内网渗透，思科已发布相关补丁并督促管理员进行全面漏洞扫描与系统加固。

Linux 内核 UAF 漏洞被勒索软件组织利用

Linux 内核中一个严重的 Linux 内核“释放后重用漏洞正在被多个勒索软件团伙积极利用，用以在 Linux 服务器上提升权限并实施加密攻击。CISA 也就此发布了针对 CVE-2024-1086 等相关漏洞的警报，指出黑客已成功利用此类底层缺陷突破系统防御。随着企业关键业务逐渐向 Linux 和容器化环境迁移，针对内核层面的漏洞攻击已成为勒索病毒破坏供应链、瘫痪数据中心的核心手段，安全专家建议运维人员必须强制执行内核版本升级计划。

十二月丨 满分漏洞与架构重塑：Web 框架底层协议级坍塌与 AI 语音诈骗的终极进化

核心焦点：React/Next.js 满分漏洞、Aisuru 创纪录流量攻击、哈佛大学语音钓鱼

React 与 Next.js 远程代码执行漏洞 (CVE-2025-55182)

安全研究人员发现 React 服务器组件（RSC）和 Next.js 框架中存在严重的远程代码执行缺陷，CVSS 评分高达 10.0，在未经身份验证的情况下实现远程接管服务器。漏洞细节披露后数小时内，已有黑客组织开始尝试武器化利用，其波及范围涵盖了全球大量使用 React 架构的现代 Web 应用。

Aisuru 僵尸网络发起创纪录的 DDoS 攻击

由全球约 400 万台受感染设备组成的 Aisuru 僵尸网络发起了峰值达 29.7 Tbps 的大规模攻击，刷新了历史记录。该攻击主要针对跨国企业及互联网基础设施，旨在通过海量流量瘫痪其业务系统。尽管 Cloudflare 等云安全机构成功缓解了此次冲击，但该事件暴露出物联网设备漏洞（如 Mirai 衍生变种）在构建超大规模网络武器方面的巨大破坏力，引发了对全球带宽安全防线的深刻担忧。

Coupang 大规模数据泄露影响 3400 万用户

韩国一起严重的内部威胁引发的数据灾难，引发了社会性震动。2025 年 11 月至 12 月间，韩国电商巨头 Coupang 确认其 3400 万客户的个人隐私信息遭非法泄露，导致近七成韩国民众面临电信诈骗风险。调查指出，涉事者为一名与境外势力有关联的前雇员，利用权限管理漏洞窃取了海量数据库记录。该事件不仅让 Coupang 面临巨大的法律诉讼，也凸显了大型科技公司在内部人员审计与数据防泄露（DLP）体系上的重大短板。

哈佛大学语音钓鱼与数十万校友数据泄露

哈佛大学遭遇了一场结合了社会工程学与语音伪造技术的高级攻击。黑客通过语音钓鱼手段骗取了内部人员的认证凭据，导致数十万名校友及捐赠者的敏感个人信息和财务记录泄露。该事件在学术界和高净值人群中引起了极大恐慌，因为它展示了 AI 语音合成技术在突破传统身份验证流程中的实战威力。哈佛大学被迫升级其全校范围内的多因素认证体系，并向受影响个人发布了长期的信用保护方案。

React 与 Next.js 远程代码执行漏洞（CVE-2025-55182）标志着攻击面已从传统的业务逻辑层正式下沉至现代 Web 框架的底层通信协议级，揭示了全栈集成架构下防御边界的系统性坍塌。挑战在于，React Server Components (RSC) 等技术的引入使前后端信任链深度耦合，这种“架构级”缺陷让传统的 WAF 拦截或简单的输入审计在面对复杂的框架内部序列化逻辑时几近失灵，为那些过度依赖现代框架“原生安全性”的企业留下了难以在短期内清偿的防御债务。然而，这一危机也孕育了深刻的机遇：它正强力倒逼行业告别“外挂式”的安全补丁模式，推动 Web 开发向“安全即设计（Secure by Design）”的范式转型，并加速了具备上下文感知能力的下一代软件物料清单及自动化协议深度审计技术的实战化应用，迫使我们在智能化的攻防对抗中，必须重新定义现代 Web 应用的信任根基。

04 重点漏洞

Key Vulnerabilities

1. Langflow 未授权代码注入漏洞 (CVE-2025-3248)

2025 年 4 月，AI 工作流构建平台 Langflow 曝出严重未授权代码注入漏洞。该平台未对 Python 执行环境进行有效沙箱隔离，且用户输入过滤机制缺失，致使其逻辑校验失效。攻击者可通过 API 接口直接注入并执行恶意代码。由于 Langflow 多部署于企业内部 AI 环境，该漏洞易导致服务器失陷，进而威胁 AI 模型、API 密钥等核心资产安全。

2. Microsoft SharePoint Server 远程代码执行利用链 (CVE-2025-53770、CVE-2025-53771)

2025 年 7 月，微软 SharePoint 中曝出名为“ToolShell”的复杂漏洞链。攻击者通过操作 ToolPane 接口规避身份验证，并结合不安全反序列化漏洞，能够从系统中提取加密密钥（ValidationKey）。一旦获取密钥，攻击者即可构造完全有效的 ViewState 数据，在系统层面获得完全控制权。该漏洞通常用于针对政府和大型金融机构的 APT 攻击，可导致其内部网络被深度渗透、敏感文档库被整体窃取。

3. Sudo 外部资源引用不当漏洞 (CVE-2025-32463)

2025 年 7 月，权限管理工具 sudo 在处理--chroot 选项时被发现存在设计漏洞。该程序会错误地采用用户可控目录下的/etc/nsswitch.conf 配置文件，导致权限提升过程受控。本地低权限用户可以借此诱导 Sudo 加载恶意的动态库或配置，从而直接获取超级用户（root）权限。这在多用户服务器或容器环境中极具杀伤力，直接摧毁了类 Unix 系统的权限防御基石。

4. Docker Desktop 访问控制不当漏洞 (CVE-2025-9074)

2025 年 8 月，Docker Desktop 修复一处访问控制不当漏洞。该漏洞允许本地 Linux 容器通过默认 Docker 子网（192.168.65.7:2375）直接访问 Docker 引擎 API，从而执行各类特权命令，如操控其他容器、创建新容器及管理镜像等。在特定配置下（使用 WSL 后端的 Windows 版 Docker Desktop），攻击者还能以当前用户权限挂载主机驱动器，致使大量个人电脑面临容器逃逸风险。

5. WhatsApp 授权校验漏洞与苹果 Image I/O 越界写漏洞组合利用 (CVE-2025-55177、CVE-2025-43300)

2025 年 8 月，WhatsApp 授权校验漏洞（CVE-2025-55177）与苹果 Image I/O 框架零日漏洞（CVE-2025-43300），形成高效“零点击”攻击链——前者可静默远程加载恶意内容，后者通过解析特制图像触发内存越界写，实现无交互远程控制。该漏洞链已被用于对记者、人

权维护者等群体实施定向监控。鉴于 WhatsApp 用户基数庞大，事件引发全球安全震动。一旦感染，设备通信、位置及媒体数据均可被窃。

这标志着 2025 年“零点击”攻击技术已步入成熟阶段，也暴露了即时通讯应用与系统底层深度耦合所带来的严峻安全风险。

6. SGLang 大模型推理框架远程代码执行漏洞 (CVE-2025-10164)

2025 年 9 月，开源 AI 推理框架 SGLang 曝出高危 RCE 漏洞（CVE-2025-10164）。该漏洞源于其动态权重更新接口/update_weights_from_tensor 存在 Pickle 反序列化缺陷，攻击者可构造恶意 Base64 载荷植入系统命令，在默认配置下实现“零交互”接管目标 GPU 服务器。

作为 AI 领域的“地震级”威胁，该漏洞波及 Meta、谷歌、百度等机构部署的数百万个推理节点，涉及资产超万亿。一旦被利用，攻击者可窃取模型权重与机密数据，甚至将其作为跳板渗透企业内网，引发全球 AI 服务瘫痪。所幸得益于 360 与相关单位的极速协同，通过资产清点与访问控制等手段，在补丁窗口期内成功实现了全球“野外零利用”，有效捍卫了 AI 基础设施的底层安全。

7. 宇树机器人 BLE 漏洞（CVE-2025-35027、CVE-2025-60017、CVE-2025-60250、CVE-2025-60251）

2025 年 9 月，宇树（Unitree）机器人被曝存在一系列代号为“UniPwn”的高危安全漏洞。该漏洞源于其低功耗蓝牙（BLE）配置接口使用硬编码密钥，允许攻击者近距离伪造管理员身份并植入恶意代码，从而获取系统最高权限。尽管漏洞已于 5 月上报，厂商迟至 9 月才发布修复补丁，响应滞后引发业界担忧。

这一漏洞让具身智能设备彻底暴露在物理威胁面前：攻击者可完全接管机器人动作、实时窃取环境监控数据，甚至阻断固件更新使其永久受控。蓝牙传播特性可能引发“僵尸网络”式连锁感染，导致机器人集群集体失控。

8. FortiWeb 远程代码执行漏洞(CVE-2025-64446、CVE-2025-58034)

2025 年 11 月，网络安全领军厂商 Fortinet 旗下 Web 应用防火墙 FortiWeb 曝出高危漏洞链，涉及身份认证绕过（CVE-2025-64446）与命令注入（CVE-2025-58034）。攻击者可借此绕过认证创建持久化管理员账户，并在配置 SAML 时注入指令，最终实现未授权的远程代码执行。

由于漏洞链支持未授权利用且已在野活跃，众多部署该产品的企业面临直接威胁。一旦防线失守，攻击者不仅能窃取 Web 流量与后台数据，还可将其作为内网渗透跳板，甚至引发大规模网络瘫痪。此事件表明，关键安全设备本身正成为攻击入口，对企业边界防御构成了严峻挑战。

9. 三星移动设备 Quram 图像解析库远程代码执行漏洞(CVE-2025-21042)

2025 年 11 月，Unit 42 安全研究团队披露了三星 Quram 图像解析库的在野攻击。该漏洞源于其 DeltaPerColumn 在处理 DNG 格式图片时存在索引越界逻辑错误。攻击者可通过 WhatsApp 发送伪装成 JPEG 的恶意 DNG 图像，在系统 AI 服务扫描时触发堆溢出，实现远程代码执行。

作为典型的“一键式”攻击，用户仅需查看图片即可触发，隐蔽性极强，该漏洞被间谍软件组织用于静默植入监控程序。尽管三星已于 2024 年 4 月发布补丁，但由于 Android 生态的碎片化，仍有数千万旧设备处于风险之中。此事件暴露出移动设备闭源第三方库在供应链安全中的系统性脆弱，以及“一键式”利用对移动安全的持续威胁。

10. React Server Components 代码注入漏洞 (CVE-2025-55182)

2025 年 12 月，React 及其生态框架（如 Next.js）遭遇了 CVSS 评分为 10.0 的严重安全挑战。该漏洞源于 React 服务器组件在反序列化 Flight 格式数据时缺乏关键检查，使得恶意请求可直接在服务端触发代码执行，攻击者通过构造特定 payload 即可完全接管 Web 应用服务器。鉴于 React 19 及其后续版本在现代化互联网架构中处于关键地位，该漏洞影响从初创公司到大型互联网企业的众多业务系统。

05 关键趋势

Key Trends

1. AI 武器化与反制 (AI Weaponization & Defense)

AI 已从辅助工具演变为攻防体系的核心引擎，“武器化”与“自动化反制”并行发展。

在攻击侧，生成式 AI 极大提升了漏洞挖掘与利用代码生成的响应速度，而大模型服务器频繁曝出的高危 RCE 漏洞事件则表明，模型自身已成为高价值攻击目标。AI 驱动的自动化攻击日趋复杂，AI Agent 不仅能自主探测漏洞，更能动态模拟对抗行为。

在防御侧，反制技术也在走向自主化。以 OpenAI 基于 GPT-5 构建的“Aardvark”自主修复 Agent 为代表，防御方正运用大模型实现漏洞的毫秒级修复与系统加固。

这场“AI 对垒 AI”的范式变革，正在倒逼传统依赖人工的响应体系全面重构，构建智能化、自动化的攻防闭环已成为 2025 年漏洞治理的核心挑战与方向。

2. 边缘设备与物联网失陷 (Edge & IoT Compromise)

传统边界防护体系正在失效，路由器、摄像头及其他智能终端日益成为攻击者渗透内网的“黄金入口”。

攻击者对网络边界基础设施的锁定与利用速度空前加快：例如，Salt Typhoon 组织利用已知旧漏洞大规模入侵思科边缘设备，Juniper MX 系列路由器亦频遭定向攻击。同时，民生相关 IoT 设备风险凸显——数百万台冰箱、冰柜因控制器漏洞面临远程失控风险，SunPower 能源设备中曝出的高危漏洞可导致设备完全失陷。

边缘设备往往因补丁更新滞后、安全监控薄弱，已成为国家级黑客组织与犯罪团伙渗透内网的重要跳板。面对这一态势，政企机构必须推动从单一内网防护，转向覆盖异构边缘及 IoT 资产的全生命周期漏洞管理与持续行为审计。

3. 供应链信任危机 (Supply Chain Fragility)

软件生态“毛细血管”被毒化，开发者信任链受严峻挑战。

从实际案例看，底层组件与分发渠道成攻击首选：nPM、PyPI 生态的新型恶意软件操作威胁数百万人；VS Code 插件领域，自传播蠕虫“GlassWorm”利用供应链致近 3.6 万台设备受影响。

2025 年攻击不止针对单一组织，更在毒化开发者工具与共享组件。企业须清醒：信任链任一环断裂都可能引发系统灾难，建立 SBOM 透明化治理与第三方风险动态评估迫在眉睫。

4. 漏洞利用“零日化”与高速化 (Rapid Exploitation)

漏洞从披露到在野利用的时间窗口被极度压缩，构成威胁环境核心特征。

例如 Chrome V8 引擎、Windows WebDAV 客户端、SonicWall 防火墙等核心产品漏洞，PoC 发布后几乎立即遭攻击者锁定。此趋势不仅蔓延至传统软件，更侵入大模型架构与云原生组件。高速化攻击倒逼企业放弃“按月修补”，转向预测性威胁情报与自动化响应，应对 MTTE（平均利用时间）缩减的挑战。

5. 关键基础设施勒索常态化 (Critical Infrastructure Ransomware)

勒索软件的攻击目标正显著聚焦于支撑社会运转的核心命脉，其破坏性与民生关联度极高。

攻击已从加密、窃取数据，升级为通过入侵工业控制系统（ICS）及边缘网络设备（如思科、Juniper 网络设备），直接获取物理控制权。

面对关键设施极低的停机容忍度，攻击者借此施加“双重勒索”甚至“破坏性勒索”，迫使相关方在公共安全压力下妥协。应对 2025 年常态化的勒索威胁，防御重心须转向对高价值资产的实时行为监测与分级加固。

360漏洞研究院
VULNERABILITY RESEARCH INSTITUTE

360数字安全
数字安全的领导者

06 CISO 指南

CISO Insights

1. 从“AI 应用”转向“AI 治理”，构建模型级防御体系

2025 年，AI 不仅是生产力工具，更成为了高价值攻击目标。从 DeepSeek 遭受的复合型攻击，到 Langflow（CVE-2025-3248）和 SGLang（CVE-2025-10164）的远程代码执行漏洞，攻击者正通过注入攻击、反序列化缺陷直接接管 AI 基础设施。

- ✧ 建立 AI 资产清单（AIBOM）： 识别并审计所有内部部署及第三方集成的 AI 模型、推理框架（如 SGLang）和编排工具（如 Langflow）。
- ✧ 实施模型层访问控制： 针对 AI Agent 实施“影遁（Shadow Escape）”防御策略，严格限制 AI 代理的 OAuth 令牌权限，防止参数注入导致的敏感数据外泄。
- ✧ AI 原生安全审计： 将安全评估从代码层扩展到提示词（Prompt）层与推理逻辑层，防范针对 LLM 的“零点击”提示注入攻击。

2. 重塑身份边界，应对“零点击”与机器身份危机

2025 年是“零点击”漏洞的爆发年。WhatsApp、Windows LDAP 及 WSUS 的漏洞显示，攻击者无需用户交互即可实现内网渗透。由于机器身份（API 密钥、服务账号）的增速远超人类身份，这些疏于管理的机器凭证已成为企业防御体系中最薄弱的环节。

- ✧ 强制执行全量多因素认证（MFA）： 针对所有特权账号及关键基础设施（如 WSUS、SharePoint）实施抗钓鱼 MFA。
- ✧ 机器身份治理（MIG）： 建立自动化轮换机制，清理僵尸账号。针对第三方集成实施动态授权，防止类似 TransUnion 式的 API 权限滥用。

- ✧ 微隔离与零信任架构： 鉴于 LDAP 等核心协议的脆弱性，应通过微隔离技术限制域控等核心资产的横向移动路径。

3. 深化供应链透明度，防御“底层协议”坍塌

2025 年末 React/Next.js（CVE-2025-55182）满分漏洞的爆发，标志着攻击面已下沉至现代 Web 框架的底层协议。此外，npm/PyPI 的持续投毒与“Slopsquatting”新型攻击，使得开发者环境（如 Vite）成为内网渗透的新跳板。

- ✧ 全生命周期软件物料清单（SBOM）： 要求供应商提供动态更新的 SBOM，并建立针对 React、Next.js 等主流框架底层漏洞的快速响应机制。
- ✧ 开发环境加固： 针对 Vite 等开发工具实施严格的本地访问控制，防止开发机成为进入生产环境的“暗门”。
- ✧ 自动化依赖审计： 引入 AI 驱动的依赖项扫描工具，识别并阻断具有“拼写偏差”或异常行为的恶意软件包。

4. 强化边缘与 OT 韧性，应对关键基础设施勒索常态化

攻击者正以前所未有的速度锁定 VPN（Ivanti/SonicWall）、路由器（Cisco IOS XE）及机器人（宇树 BLE 漏洞）等边缘设备。朝日啤酒停产事件证明，针对 OT 网络的攻击已具备直接破坏物理生产的能力。

- ✧ 资产可见性与补丁提速： 边缘设备（VPN、防火墙）的补丁窗口必须缩短至 24 小时内。针对无法及时补丁的 OT 设备，实施物理隔离或协议转换代理。
- ✧ OT/IT 融合安全审计： 针对具身智能（机器人）及工业控制系统实施专项安全评估，重点排查硬编码密钥与不安全通信协议。
- ✧ 业务连续性演练： 针对勒索软件导致的“业务停摆”进行实战化模拟，确保在核心系统失陷时具备快速恢复能力。

5. 从“预防心态”转向“恢复能力”，构建安全行为文化

2025 年的攻击速度（Breakout Time）已压缩至分钟级。哈佛大学语音钓鱼事件显示，AI 深伪技术已能轻易突破传统的人工审核流程。

- ✧ 嵌入式安全教育： 针对 AI 生成的钓鱼邮件和语音深伪，开展实战化模拟演练，提升员工的“数字直觉”。
- ✧ 关注团队心理健康： 面对极速化的威胁环境，建立安全团队的“减压”机制，利用 AI 自动化工具减少警报疲劳，防止核心人才流失。
- ✧ 合规性前瞻布局： 密切关注《网络安全事件报告管理办法》等新规，建立符合监管要求的秒级事件报告与响应流程。

07 结语

Conclusion

2025 年，我们目睹了网络安全领域的一次范式转移。从年初针对 DeepSeek 的复合型冲击，到年末 React/Next.js 底层协议漏洞引发的全球震荡，攻击者的矛头已不再仅仅指向孤立的服务器或数据库，而是直指支撑现代社会的 AI 基础设施与软件供应链微循环。

回首过去一年，网络安全对抗的边界已被彻底重塑。边缘设备不再只是网络的末梢，而是成为了国家级威胁组织进入内网的“黄金入口”；生成式 AI 不再只是效率工具，而是成为了攻防双方在毫秒级博弈中的核心引擎。

我们必须承认，传统的“围墙式”防御已正式宣告失效。在“零点击”漏洞频发、机器身份数量远超人类身份的今天，任何组织都无法通过单纯的拦截来实现绝对安全。

安全不是一段代码的终点，而是一场永无止境的进化。2025 年的种种震荡提醒我们：在这个智能化的攻防时代，最坚固的屏障并非某种单一的技术，而是组织在面对未知威胁时，能够迅速识别、快速自愈、并持续进化的业务韧性。

360数字安全
数 字 安 全 的 领 导 者

360 数字安全集团(三六零数字安全科技集团有限公司)是数字安全的领导者，秉持“上山下海助小微”企业使命，确立安全和 AI 发展双主线。

在安全领域，为解决国家“看见”高级威胁的卡脖子问题探索形成一套以“看见”为核心的数字安全中国方案，并以“安全即服务”为核心发展理念全面升级 360 安全云，将近 20 多年被行业反复验证成功的数字安全运营体系框架，以云化、服务化方式赋能城市、大型企业、中小微企业，帮助其构建应对数字时代复杂威胁的安全能力。

在人工智能领域，360 积极布局 AI 战略。360 自研千亿参数认知型通用人工智能大模型“360 智脑”，并创新推出全球首个 L4 级别的企业智能体工厂-360SEAFactory(简称“SEAF”)。智能体工厂是一套满足企业生产、构建、运营智能体的全套基础设施与开发框架，聚焦领域专家、业务骨干需求，支持通过自然语言描述岗位流程定义智能体，无需编程能力，实现专家智能体协作团队搭建。

截至目前，360 累计捕获 58 个境外 APT 组织，监测到 6200 多次对我国 20000 多家重要机构单位的高级网络攻击事件；360 数字安全中国方案已落地超 20 个大中型城市，涵盖四大直辖市和部分省会城市，树立了标志性的城市级安全服务典范；同时，覆盖了超过 90%的中央部委、80%央企、95%大型金融机构和 100%的运营商，累计服务超 20000 家政企客户。

除此之外，360 已连续十年支撑国家级网络攻防实战演习，一直是国家重大政治、经济活动的核心网络安全保障力量。在两会、二十大、九三阅兵、“一带一路”峰会、G20、金砖会议、APEC、七十周年庆典、2022 年北京冬奥会等活动的重保工作，以及国家安全和国防安全相关工作中发挥了重要保障作用。