2025. 12

AhnLab

2025年网络威胁趋势
2026年展望

概述

目录

概述

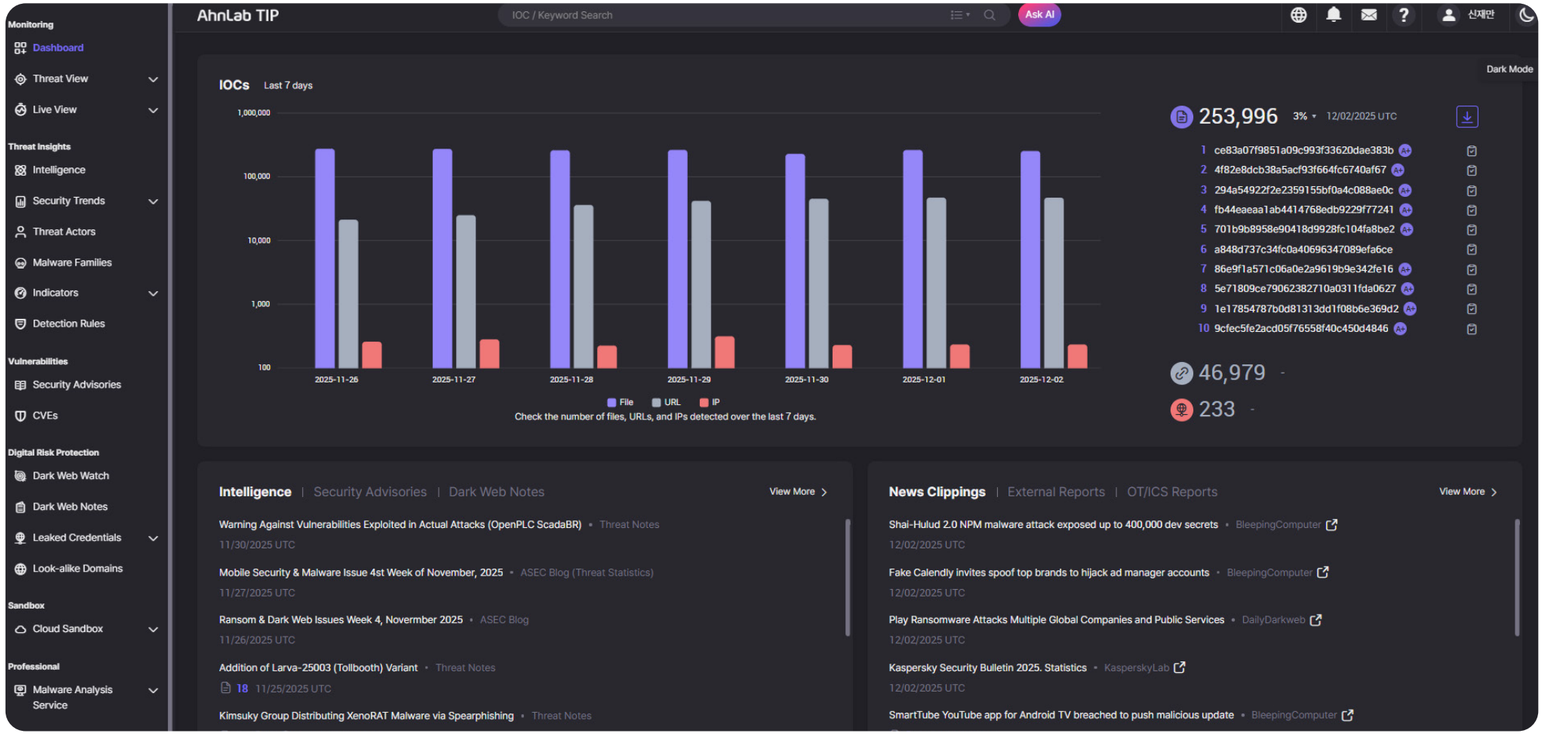
报告介绍

本报告基于 AhnLab 威胁情报平台 AhnLab TIP 提供的安全内容，对 2024 年第四季度至2025年第三季度期间的各类安全议题与趋势进行分析，并展望 2026 年网络安全威胁态势。

AhnLab TIP 从多渠道收集、分析并分类各类威胁情报，包括恶意软件、入侵事件、威胁行为者、漏洞、入侵指标（IoC）及安全新闻等。通过这些情报，帮助客户基于威胁情报制定安全策略并做出有效决策。

有关 AhnLab TIP 的更多详情，可访问 AhnLab 官网或 AhnLab TIP 门户网站进行了解。

→ 前往 AhnLab 官网
→ 前往 AhnLab TIP 门户



【图】AhnLab TIP 仪表板

概述

用数字解读 AhnLab 威胁情报

2,258条
威胁情报发布量

AhnLab TIP 的“Intelligence”栏目在过去一年共发布了 2,258 条内容。主要类型如下：

- **ASEC Notes**: 最快速传递威胁情报
- **ASEC Blog**: 对最新威胁进行快速分析
- **Dark Web Notes**: 提供深网/暗网威胁及高风险信息
- **趋势报告**: 分析恶意代码、暗网等多类趋势
- **分析报告**: 对 APT 组织、攻击手法等进行深度分析

661条
安全公告

安全公告针对软件漏洞及威胁组织安全的问题，提供快速的信息与应对指南。

每日数千至数万条 IoC
其中 30% 为 AhnLab 独家 IoC

AhnLab TIP 每日提供数千至数万条 IoC（如恶意文件、URL、IP、域名等），支持客户在威胁响应中直接使用。

AhnLab 拥有韩国最大规模的威胁检测与响应传感器网络。因此，**在 AhnLab 的IoC 中，约 30% 的 IoC 属于 OSINT 难以获取的独家情报。**

404个 – 威胁行为者
1,051个 – 恶意软件家族

AhnLab 持续追踪威胁行为者与恶意软件家族，并通过 AhnLab TIP 平台提供分析信息。

“Threat Actors”栏目不仅提供威胁行为者的详细信息，还可查看相关的战术、技术与流程（TTP）、入侵指标（IoC）以 及最新资讯。

“Malware Families”栏目基于恶意软件特征、技术、开发者等维度，对恶意软件家族进行分类并提供分析内容。

2,216条
新闻剪辑

收录来自国内外主流媒体与安全厂商发布的安全新闻与技术文档。每条新闻都附带相关 IoC 信息，便于企业安全负责人直接用于威胁应对。

2,970份 – 外部报告
19,679条 – 社交媒体帖子

提供来自国内外主要安全企业和专家的分析报告，以及从 X（原 Twitter）等社交媒体筛选的最新威胁趋势信息。内容中附带相关 IoC，帮助客户快速识别威胁并制定应对策略。

2025年主要网络安全趋势

→ 重大事件

→ 攻击组织趋势

- 暗网 Top 8
- 各国 APT 组织

→ 勒索软件趋势

- 主要组织活动 Top 10
- 主要受害行业
- 主要受害国家

→ 主要威胁趋势

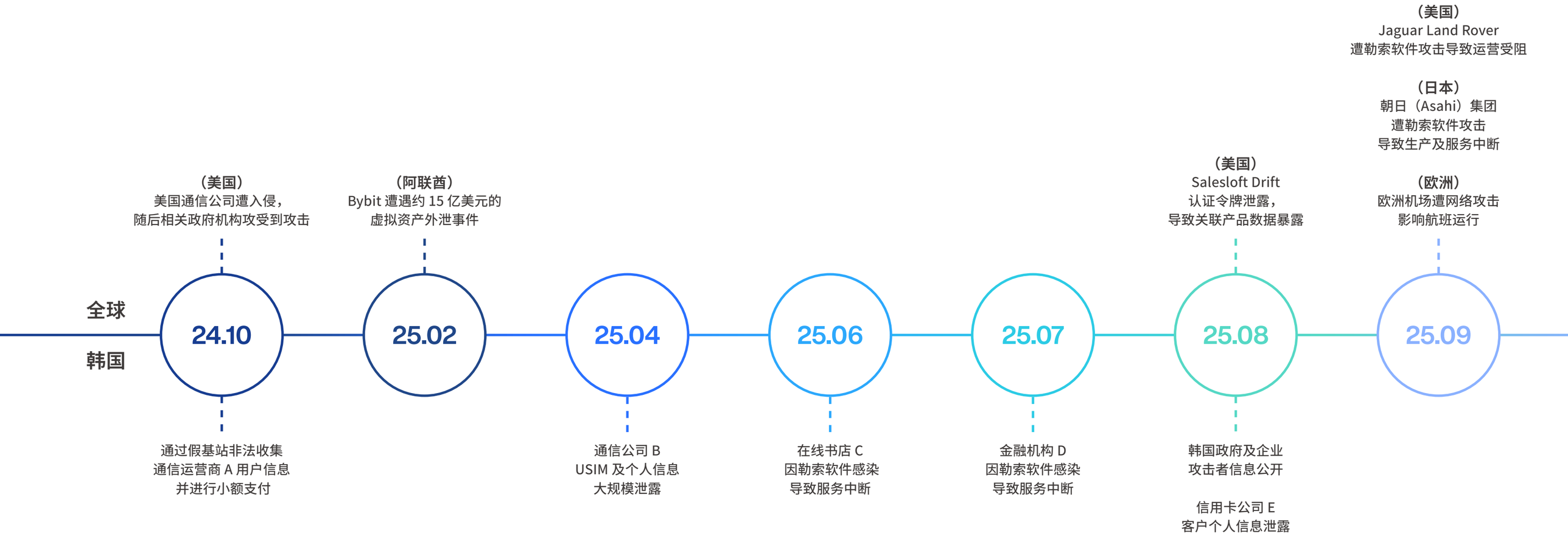
- 恶意代码 Top 9
- 攻击技术 Top 10
- 漏洞 Top 10
- 移动端 Top 6

→ 攻击统计

- 攻击类型

2025年网络威胁趋势

重大事件



2025年网络威胁趋势

重大事件: 全球

2025年10月：美国通信公司遭入侵，随后相关政府机构攻受到攻击

黑客组织 Salt Typhoon 入侵了美国至少 8 家主要通信公司，并成功访问执法机构的通信监听系统及敏感通信基础设施。

攻击者利用以下漏洞进行渗透：
Ivanti VPN（CVE-2023-46805、CVE-2024-21887）、Fortinet EMS（CVE-2023-48788）、Sophos Firewall（CVE-2022-3236）、Microsoft Exchange ProxyLogon。

通过受控通信网络，攻击者不仅窃听美国政府机构的通信，还疑似访问了 法院命令下的监听数据。

在攻击过程中，黑客部署了 GhostSpider、SnappyBee、Masol RAT 等高级后门工具，长期隐蔽驻留在目标网络中。此外，有消息称部分政府网站也遭到攻击。

2025年2月：Bybit 遭遇约 15 亿美元虚拟资产外泄事件

位于迪拜的虚拟资产交易所 **Bybit 遭遇重大安全事件，约 15 亿美元的加密货币被黑客窃取。**此次攻击**被怀疑由 Lazarus 黑客组织策划。**

攻击者针对冷钱包（Cold Wallet）向热钱包（Hot Wallet）转账的过程实施攻击，可能通过以下手段实现：入侵内部开发者系统；操纵 Safe Wallet 平台签名接口，伪造多重签名（Multisig）钱包交易。

在攻击过程中，黑客将恶意 JavaScript 代码注入签名主机，伪装合法地址，最终将资产转入攻击者控制的钱包。
被窃取的资产包括：以太坊（ETH）、质押以太坊（stETH）。
事件发生后，Bybit 已启动用户补偿计划及相关安全措施。

2025年8月：Salesloft Drift 认证令牌泄露，导致联动产品数据暴露

Salesloft 的 Drift AI 聊天机器人集成功能遭黑客攻击，导致 OAuth 令牌泄露，影响范围涉及包括 Salesforce 在内的 7**00余家企业客户数据。**

攻击细节：
黑客首先入侵 Salesloft 的 GitHub 账户，获取内部源代码；随后转向 Drift 的 AWS 环境，收集 OAuth 令牌；利用这些令牌访问 Salesforce 实例，窃取客户信息、账户数据等； 攻击者还收集了 AWS 密钥、密码、Snowflake 令牌等敏感凭证。

事件发生后，Salesforce 与 Salesloft 已将 Drift 应用从 AppExchange 下架，并切断所有连接，同时通知受影响企业并执行令牌失效处理。

主要内容（要点）

- Salt Typhoon 入侵美国通信公司，访问执法机构监听系统及敏感通信基础设施
- Bybit（迪拜） 遭黑客攻击，约 15 亿美元加密资产被窃取，疑似 Lazarus 所为
- Salesloft Drift AI 聊天机器人遭入侵，OAuth 令牌泄露，导致 700余家企业客户数据外泄

2025年网络威胁趋势

重大事件: 全球

2025年9月：朝日（Asahi）集团遭勒索软件攻击

日本知名食品饮料企业 朝日（Asahi）集团遭到 **Qilin 勒索软件组织攻击，导致全国 30家工厂的生产及物流系统瘫痪。**

攻击细节：
黑客加密了 Asahi 在日本的 IT 基础设施系统，并外泄部分数据后索要赎金；Asahi Super Dry、Draft Beer、Dry Zero 等核心产品的生产与出货全面中断；客服中心及订单系统长期离线，严重影响业务运营。

Qilin 勒索软件组织特点：
- 采用 Golang 与 Rust 开发的高级勒索软件；
- 属于“勒索软件即服务（RaaS）”模式；
- 使用“双重勒索（Double Extortion）”手法，既加密数据又威胁公开泄露。

目前，Asahi 集团正与外部专家合作进行系统恢复，部分工厂已于10月初开始部分恢复生产。

2025年9月：英国 Jaguar Land Rover 遭勒索软件攻击

英国汽车制造商 Jaguar Land Rover（JLR） 遭受疑似 Scattered Spider 与 Lapsus$ 关联组织的勒索软件攻击，导致全球生产全面停摆。

攻击影响：
黑客瘫痪 JLR 内部 IT 系统，使英国主要工厂及全球生产线中断超过 5 周； 超过 3 万名员工及 约 20 万名供应链人员受到影响；经济损失估计约 19 亿英镑（约合 3.3 万亿韩元）。

JLR 表示客户数据未泄露，但生产停工、交付延迟及零部件供应中断造成严重经济冲击。英国政府已提供 15 亿英镑紧急贷款担保，以稳定产业运营。

2025年9月：欧洲机场发生大规模故障

多家欧洲航空公司遭遇针对 Collins Aerospace 的 MUSE 软件的勒索软件攻击，导致大范围服务中断。该软件负责机场电子值机、行李处理、登机牌发放等关键功能。

攻击影响：
此次攻击导致伦敦希思罗、布鲁塞尔、柏林、都柏林等主要机场数百架航班延误或取消；
攻击者疑似通过 Collins Aerospace 欧洲数据中心入侵。

部分系统在恢复过程中再次感染，导致修复进度延迟，数千名旅客被迫手动值机并长时间等待，造成不便。

主要内容（要点）

- 日本 Asahi 集团遭 Qilin 勒索软件攻击，导致 30家工厂系统瘫痪
- Jaguar Land Rover（JLR）遭勒索软件攻击，英国及全球生产线中断超 5 周，损失约 19 亿英镑
- Collins Aerospace 遭勒索软件攻击，导致欧洲主要航班延误及取消

2025年网络威胁趋势

重大事件: 韩国

2025年10月：通信公司 A 遭假基站攻击，用户信息泄露并发生小额

通信公司 A 部分用户遭遇假基站攻击，导致约 2.2 万名用户个人信息泄露，其中 368 名用户遭受数亿韩元规模的小额支付欺诈。

攻击细节：

黑客自 2024年10月起通过假基站强制连接受害者手机，窃取 IMSI 等用户识别信息；随后制作 克隆手机，绕过认证流程，实施小额支付欺诈；

应对措施：

警方已抓获部分嫌疑人并查获部分设备；政府成立民官联合调查组，开展原因调查；

通信公司已采取措施：

阻断新型 Femtocell；降低小额支付限额；扩大 USIM 保护服务；为受害者提供退款及赔偿

2025年4月：通信公司 B 遭遇大规模 USIM 与个人信息泄露事件

通信公司 B 遭遇重大网络攻击，约 2300 万名客户个人信息被泄露。泄露数据包括：用户电话号码、IMSI、IMEI、USIM 认证密钥（K 值）。这些信息属于 USIM 核心识别数据，引发 SIM 卡调包（SIM Swapping）、身份盗用等二次风险担忧。

攻击细节：

黑客使用 Linux 平台 BPFDoor 后门，该后门通过内核级数据包过滤实现隐蔽，并仅在接收特定“魔术包”时激活；攻击者利用 WebShell 与远程代码执行（RCE）漏洞入侵内部系统；在 HSS 服务器部署 BPFDoor 后门，窃取 USIM 信息。

2025年6月：韩国最大在线书店 C 遭勒索软件攻击，服务中断 4 天

韩国第一大在线书店兼票务平台 C 公司**遭遇勒索软件攻击，导致网站与移动应用瘫痪长达 4 天。**攻击者加密了核心内部文件及管理员账户，锁定整个系统并索要赎金。

攻击影响：

约 2000 万用户无法正常进行图书购买、演出订票及社区互动；多场演唱会及粉丝见面会被取消或延期，造成严重经济与用户体验损失

主要内容（要点）

- 通信公司 A 遭假基站攻击 —— 黑客强制连接用户手机，窃取 IMSI 等用户识别信息
- 通信公司 B 客户 2300 万人个人信息泄露 —— 使用 Linux 平台 BPFDoor 恶意程序实施攻击
- 韩国最大在线书店 C 遭勒索软件感染 —— 网站与移动应用瘫痪 4 天，影响图书购买与演出订票

2025年网络威胁趋势

重大事件: 韩国

2025年7月：金融机构 D 遭 Gunra 勒索软件攻击，导致服务中断

韩国某大型金融机构 D 公司**遭遇 Gunra 勒索软件攻击，导致核心 IT 系统瘫痪，引发大规模业务中断。**

攻击细节：

黑客通过 SSL VPN 设备的 SSH 端口尝试登录进入内部网络；获取管理员权限后分发勒索软件；勒索软件采用 ChaCha8 + RSA 加密算法，并在加密文件添加 .ENCRT 后缀，实现条件化、精细化加密。

攻击影响：

住房贷款担保、手机开户、贷款担保等关键金融服务全面停摆；部分网点被迫采用手工处理，严重影响客户体验。

安全团队成功开发专用解密工具，完成系统恢复，避免长期停机风险。

2025年8月：APT Down 攻击韩国政府与企业的细节曝光

在全球黑客大会 DEF CON 33 上发布的报告《APT Down: The North Korea Files》揭示了针对韩国的 APT 组织攻击活动。

报告核心内容：基于从黑客工作站提取的 8.9GB 数据，**确认该组织长期渗透韩国政府机构、选举委员会、媒体及通信企业；**

攻击者使用了网络钓鱼攻击、证书窃取、横向移动（Lateral Movement）等高级技术。

报告还指出存在 朝鲜与中国联合攻击迹象。韩国政府已通过部分机构启动防御与调查。

AhnLab 发布了针对该攻击的深度分析报告：《Larva-25010 – APT Down 攻击者 PC 分析》。

2025年8月：信用卡公司 E 客户数据泄露，涉及敏感支付信息

韩国某信用卡公司 E **遭遇重大数据泄露事件，影响 297 万名客户。**其中 28 万名客户的敏感支付信息（卡号、有效期、CVC、安全密码）被窃取，可直接用于交易。

攻击细节：

黑客在在线支付服务器植入恶意代码与 WebShell；窃取并外传约 200GB 数据。

应对措施：

为受影响客户提供卡片重发、年费减免、免息分期、全额赔偿；承诺未来 5 年投入 1100 亿韩元加强安全防护。

主要内容（要点）

- 金融机构 D 遭 Gunra 勒索软件攻击 —— 导致金融服务全面中断，但最终通过专用解密工具成功恢复
- APT Down 攻击组织长期渗透韩国企业与政府机构 —— AhnLab 发布深度分析报告
- 信用卡公司 E 客户 297 万人个人信息泄露 —— 约 200GB 数据外传，涉及敏感支付信息

2025年网络威胁趋势

攻击组织趋势 - 暗网 Top 8

AhnLab 持续在暗网监控并分析网络威胁相关议题，并通过 AhnLab TIP 提供情报内容。以下是基于过去一年暗网动态分析所得出的攻击组织相关洞察：

1. 勒索软件生态碎片化与小型组织激增

2025年，勒索软件生态发生了根本性的结构变化。大型组织如 LockBit 因执法机构的集中打击而大幅削弱，RansomHub 也因内部矛盾而停止官方活动。

作为反作用，超过 40 个小型和新兴组织大量涌现。过去由少数大型组织主导的格局，已被 Akira、Qilin、Play、Gunra 等重新改写。这些小型组织利用泄露的 LockBit 3.0、Conti 源代码进行再开发，并以独立品牌开展活动。它们采用比大型攻击组织更具攻击性、更不可预测的谈判策略，部分甚至不提供解密工具，导致受害者损失进一步加重。

勒索软件生态正从集中化向去中心化演变。在传统基于 IoC（入侵指标） 的检测面临瓶颈的情况下，现有防御策略也亟需全面重构。

2. 基于 RaaS 和白标模式的勒索软件“卡特尔”

2025 年勒索软件生态最大的变化，是基于白标模式的“勒索软件卡特尔”的出现。**在这种模式下，中央平台提供加密工具、数据泄露基础设施和谈判工具，而旗下加盟成员则以各自品牌实施攻击，并仅需上缴 20% 收益。**相比传统 RaaS 需要分成 30%~40%，该模式对攻击者而言更具吸引力。目前，该模式已在 Global Group、Anubis 等多个勒索软件生态圈中迅速扩散。

这种“加盟”形式降低了攻击门槛，使攻击者无需具备深厚的技术能力或自建基础设施即可开展攻击。随之而来的是攻击频率与手法的多样性显著提升，仅通过攻击品牌名称已难以识别具体攻击组织。

主要内容（要点）

- 勒索软件生态碎片化 —— LockBit 等大型勒索软件组织被削弱，导致众多小型组织崛起
- 基于白标模式的勒索软件“卡特尔” —— 有利的收益分成，轻松实现“加盟”式攻击

2025年网络威胁趋势

攻击组织趋势 - 暗网 Top 8

3.国家背景 APT 与勒索软件生态的深度融合

2025年，**具有国家背景的 APT 组织正式加入民用勒索软件生态体系。**这意味着国家级网络间谍活动与以牟利为目的的网络犯罪之间的界限正在被彻底打破。

Microsoft 披露，朝鲜 APT 组织 Moonstone Sleet 已放弃自研勒索软件 FakePenny，转向部署俄罗斯系的 Qilin 勒索软件。另有案例显示，朝鲜背景的组织 Andariel 在植入 Dtrack 后门后，部署了 Play 勒索软件。**这些事件表明，一种新的“分工模式”正在形成：APT 组织负责初始入侵，RaaS 加盟组织则负责加密和勒索。**

当 APT 的高阶渗透能力与 RaaS 的高效勒索机制结合时，攻击成功率与破坏规模将大幅提升。这不仅加剧防守方的分析与溯源难度，也使受制裁国家可能将此类攻击作为体系化、持续性的收入来源，风险进一步扩大。

4.国际协作调查与生态系统重组

2025 年，各国执法机构的国际协作对网络犯罪生态造成了重大打击。**所谓 Endgame 行动（Operation Endgame） 于 2024 年 5 月启动，并于 2025 年 5 月扩展至第二阶段，重点打击 DanaBot、Qakbot、Trickbot 等主要恶意代码基础设施。**

仅在 2025 年 5 月，就封锁了约 300 台服务器和 650 个域名。对 20 名网络犯罪嫌疑人发出国际逮捕令，并查扣约 405 万美元的加密货币，使总查扣金额达到约 2,453 万美元。

同时，行动还针对暗网基础设施进行了打击，包括逮捕 BreachForums 的 5 名运营者及 XSS 论坛管理员，**这直接导致 LockBit、RansomHub 等大型攻击组织的瓦解。**

5.勒索软件集团内部割裂

2025 年，勒索软件生态因内部信任崩塌而遭受重大打击。其中最具代表性的事件是 5 月发生的 **LockBit 管理面板被黑事件。导致约 6 万个比特币钱包地址、208 份受害企业与加盟者谈判记录及加盟者账户信息泄露。**Qilin 与 Black Basta 的内部工具及聊天记录也被泄露，使其运营模式被竞争对手知晓。

此外，许多受害企业即便支付赎金，也无法获得正常工作的解密工具，或根本未收到解密工具。这导致勒索软件加盟公司运营者间的不信任加剧，部分成员开始独立运营或跳槽至竞争集团，内部信息泄露与背叛行为成为常态。结果是，大型 RssS 平台快速崩溃，大量小型、临时型勒索软件组织涌现。

主要内容（要点）

- 国家背景的 APT 与勒索软件联盟——APT 组织负责初始入侵，勒索软件组织负责勒索
- 国际执法机构协作，重击网络犯罪生态——LockBit、RansomHub 等组织被瓦解
- 勒索软件组织之间互相攻击并出现内部分裂，导致小型组织大量涌现

2025年网络威胁趋势

攻击组织趋势 - 暗网 Top 8

6.供应链攻击的高级化与扩大

2025 年的供应链攻击相比 2024 年更加精细化，规模也进一步扩大。攻击目标已从软件延伸至云服务、MSP（托管服务提供商）、安全解决方案供应商。最典型的案例是攻击组织 Clop 利用 Cleo MFT 平台的零日漏洞。今年 1 月，CLOP 通过一次攻击同时渗透 182 家企业，发动了大规模的连锁攻击。此外，Clop 对 Oracle EBS 漏洞的利用也在增加。CISA 已正式警告，由于 Oracle Cloud 凭证泄露引发的连锁入侵风险。

攻击组织 DragonForce 和 Scattered Spider 直接将目标锁定在云 MSP，利用 SimpleHelp 漏洞并通过社交工程手段欺骗 IT 管理员，获取远程访问权限。结果，一个 MSP 被攻破，导致数十家客户企业同时受害，实现了“连锁供应链攻击”。

7.暗网生态系统不稳定性加剧

2025 年，暗网生态系统经历了前所未有的不稳定。从过去的“执法机构 vs 犯罪组织”格局，演变为犯罪组织之间的攻击常态化，整个生态陷入混乱。

今年 3 月，攻击组织 DragonForce 入侵了竞争阻止 RansomHub 的数据泄露站点（Data Leak Site，DLS）。4 月，他们又篡改（deface）了 BlackLock 和 Mamona 的 DLS，并泄露内部聊天记录和后端配置。研究人员指出，DragonForce 利用了竞争组织 AI 生成的后端代码漏洞。值得注意的是，Everest 和 LockBit 的站点被同一条消息篡改：“Don't do crime CRIME IS BAD xoxo from Prague”。这暗示了针对多家攻击组织的系统性攻击的可能性。

8.地缘政治冲突驱动的黑客主义活动激增

2025 年，相比 2024 年，地缘政治冲突在网络空间的扩散更加激烈。亲俄攻击组织 NoName057(16) 持续攻击北约国家，而 Dark Storm Team 针对北约能源基础设施的攻击已经达到能产生物理影响的程度。反对阵营中，IT Army Ukraine 对俄罗斯运营商 UIS 发动 DDoS 攻击，导致其服务中断长达 72 小时。

在中东地区，随着伊朗—以色列冲突加剧，黑客主义活动明显上升。Holy League 和 313 Team 等攻击组织针对以色列医院和中央银行展开攻击。“#OpIsrael 2025” 活动预告大规模网络攻击，实际也有多家医疗机构遭到 DDoS 冲击。此外，在印度—巴基斯坦冲突局势中，Indian Cyber Force 声称入侵巴基斯坦的银行和警察机构。

主要内容（要点）

- 供应链攻击从软件扩展至云服务、MSP —— 单一企业被攻破，导致大量客户受害
- DragonForce 入侵竞争组织 RansomHub 的 DLS —— 暗示攻击组织间存在有组织攻击的可能
- 黑客激进主义活动激增，涉及俄罗斯 vs 乌克兰+北约、伊朗-以色列、印度-巴基斯坦 等地缘冲突

2025年网络威胁趋势

攻击组织趋势 - APT：整体动向

2025 年延续去年趋势，朝鲜 APT 组织的活动依然十分活跃。被提及最多的组织是 Lazarus，共公开 31 条相关信息。由于该组织包含多个子组织，因此提及次数较多；如果按子组织区分，统计结果可能有所不同。其次是 Kimsuky（27 起）和 TA-RedAnt（17 起）。中国和俄罗斯的 APT 组织活动同样频繁。Mustang Panda 有 11 起公开信息，APT28 有 10 起，Gamaredon 也有 10 起。此外，印度和巴基斯坦的 APT 组织也保持活跃，原因可能与**地缘政治紧张局势**有关。其中，巴基斯坦的 Transparent Tribe 以 17 起表现突出。

同期按国家统计 APT 组织活动数量，朝鲜以 86 起位居首位。中国 27 起，俄罗斯和印度各 18 起，巴基斯坦为 17 起。伊朗相对较少，为 9 起。除这些主要国家之外，其他攻击组织也有 32 起活动记录。这表明在全球威胁环境中，多国背景的 APT 组织正在积极运作。需要注意的是，报告公开次数少并不意味着活动少。一些 APT 组织行动隐秘，相关信息未被确认，且针对政府机构的攻击可能因政策原因不予公开。

	APTs	10/24	11/24	12/24	01/25	02/25	03/25	04/25	05/25	06/25	07/25	08/25	09/25
North Korea (86)	Andariel	2		1	1	1							
	Kimsuky	3	4	6	2	2	2			2	2	2	2
	Konni	2					2	1	1				
	Lazarus	5	2	2	4	3	4	1		2	2	4	2
	TA-RedAnt	2	1		2	1	4		1		2	3	1
China (27)	APT41	1	1					1	1	1	1	1	
	MirrorFace		2		1		1	1					
	Mustang Panda				2	2		3		1			3
	Salt Typhoon		1			1			1	1			
Russia (18)	APT28	2	1						3	1	2		1
	Gamaredon			4			1	1			1	1	
Iran (9)	Charming Kitten		2	1					1				
	MuddyWater		1			1					1	1	1
India (18)	Bitter	1	1	1					1	1		1	
	SideWinder	1					1		2			1	2
	Viceroy Tiger	1	1		1	1					1		
Pakistan (17)	Transparent Tribe		1	1			1	1	4	4	2	3	

[表] 各国 APT 组织月度活动次数（2024 年 10 月 ~ 2025 年 9 月）

2025年网络威胁趋势

攻击组织趋势 - APT：整体动向

APT 组织通常围绕地缘政治冲突区域展开活动。韩国—朝鲜、印度—巴基斯坦、中国—东南亚、俄罗斯—乌克兰、以色列—中东等区域出现网络攻击集中的现象。这些组织主要以政府、军方、外交、国防工业、金融、能源、通信、教育、NGO 等高价值机构为目标。

初始入侵方式方面，电子邮件钓鱼仍然是主要手段，使用带有恶意附件的邮件，附件格式包括 LNK、ISO、MSC、PDF、CHM、ZIP 等。攻击者利用社会工程学伪装成虚假招聘、政策文件、安全通知、公文，并使用定制化的诱饵文档和事件进行攻击。

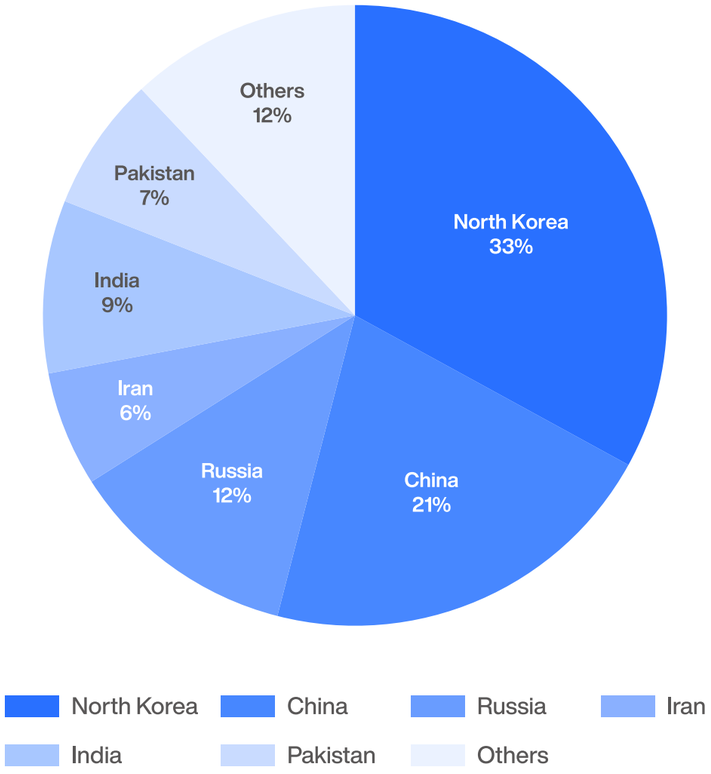
同时，APT 组织使用多种恶意代码和合法工具。恶意代码多为远程控制、后门、键盘记录、信息窃取类型。PowerShell、VBS、Batch 脚本以及 Sliver、Mimikatz 等开源工具也常被纳入攻击流程。为了实现多平台攻击，它们还会根据需要使用适用于 Windows、Linux、macOS、Android 的恶意代码。

此外，这些组织采用多种高级技术实现持久化和规避检测。以下是 APT 组织常见的攻击技术：

- 任务计划程序 / 注册表持久化
- 服务 / 对象模型（COM）劫持
- UAC（用户账户控制）绕过
- 无文件执行
- DLL 侧载
- JPEG 隐写
- VM / 沙箱环境检测与规避
- 日志清除

APT 组织还利用 GitHub、Dropbox、Google Drive、Telegram、Cloudflare、Outlook 等合法服务与云基础设施来进行 C2 通信与数据泄露，并通过 DNS/DoH、TOR、VPN 等方式隐匿攻击活动。

其最新攻击趋势包括：利用 AI 制作深度伪造（Deepfake）、MFA 绕过（AiTM、OTP 窃取）、供应链攻击、水坑攻击（Watering Hole）、IoT 设备渗透、攻击自动化与规模化、伪装成合法服务等。同时，它们会混合使用公开工具与自研恶意代码。

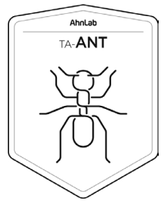


[图] 各国 APT 组织活动占比（2024 年 10 月 ~ 2025 年 9 月）

2025年网络威胁趋势

攻击组织趋势 - APT：朝鲜

朝鲜 APT 组织针对政治、外交、金融、加密货币等多个行业，目的包括获取经济利益和情报。其特点是使用高度复杂的攻击技术，如鱼叉式钓鱼、供应链攻击、 多平台恶意代码、权限提升、MFA 绕过等。此外，它们通过滥用合法文档和签名、隐写术、无文件执行、多层混淆来规避检测，建立长期渗透基础。



朝鲜

Kimsuky

2025 年，Kimsuky 组织针对多个国家和行业实施高级网络攻击。它们**伪装成演讲邀请或采访请求，利用鱼叉式钓鱼传播 ISO、LNK、MSC 等多种文件格式。**使用 MSC 文件的 Google Drive 钓鱼攻击，以及滥用 VbsEdit 签名的手法尤为突出。

使用 GitHub、Facebook、Telegram 等多渠道进行多阶段攻击，以及使用 AI 生成的伪造身份证件的攻击也首次被确认。此外，通过 PebbleDash、RDP Wrapper、Proxy 恶意代码强化远程控制，并在针对日本的攻击中使用 AsyncRAT 变种。

Kimsuky 下属多个子组织：
Larva-24005：使用 Kimalogger 收集用户键盘输入内容。
Larva-24009：实施基于 LNK 的攻击，使用 QuasarRAT、UltraVNC 等工具。
Larva-25001：通过伪装成合法文档的 LNK 文件传播 HttpSpy、Memload 等恶意代码。

Andariel

Andariel 组织持续针对多个国家实施以经济利益为目的的攻击。即使在 2024 年被美国司法部起诉后仍未停止活动。**它们曾针对美国民企，利用 Preft 和 Nukebot 后门进行渗透。**该组织使用 Sliver、Chisel、PuTTY 等开源工具，以及键盘记录器、Mimikatz 等窃取凭证，**并通过 Play 勒索软件基础设施分发勒索软件。**

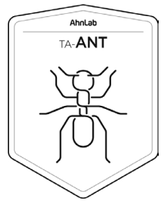
在韩国，它们针对资产管理和文档集中化解决方案，分发 ModeLoader 和 SmallTiger 恶意代码。并通过 RDP 访问和隐藏账户创建来建立长期渗透基础。此外，还确认其利用 Apache Tomcat 漏洞安装 WebShell，使用 Advanced Port Scanner 进行网络探测等。尤其值得注意的是，该组织使用 RID Hijacking 技术将低权限账户提升为管理员权限，并使用 CreateHiddenAccount 工具添加后门账户。他们还通过 PsExec 执行远程命令，利用 REGINI 操控 SAM 注册表等技术实施精细的内部渗透。甚至曾窃取韩国某安全企业 S 公司的证书，为恶意代码签名，滥用信任机制。

主要内容（要点）

- Kimsuky 通过鱼叉式钓鱼传播多种恶意代码，持续利用伪装域名和恶意文档
- Kimsuky 下属多个子组织，实施更广泛的网络攻击
- Andariel 针对美国民企，利用后门进行渗透
- 通过 Play 勒索软件基础设施分发勒索软件

2025年网络威胁趋势

攻击组织趋势 - APT：朝鲜



朝鲜

Konni

自去年底至 2025 年，**Konni 组织针对包括乌克兰在内的高价值目标，集中实施基于 LNK 文件的鱼叉式钓鱼攻击。**攻击中利用了以“税务”、“市场分析”等为主题的社会工程学手法，并结合 PowerShell 与 AutoIt 脚本以隐蔽方式执行恶意载荷。尤其是，他们在 ZIP 压缩包中插入伪装的快捷方式文件，使受害者执行后触发多阶段加载以投放恶意代码。

Konni 使用基于 WordPress 的 C2 基础设施投放 Konni RAT、Amadey、Lilith RAT、AsyncRAT 等多种远程控制型恶意代码。为保持感染持久性，采用了 Avast 杀毒绕过、启动目录自动运行、隐藏目录创建、注册表项值注册等技术。此外，还通过自动生成大量恶意样本，在不同时间点投放，并结合混淆与加密的载荷实现检测规避。

在社会工程方面，已确认其使用伪装成韩国政府邮件以及针对乌克兰政府的攻击。他们利用 PHPMailer 伪造发件人信息，并将合法文档与恶意脚本结合，使受害者误以为安全。Konni 的活动不仅限于信息窃取，还包括系统控制、凭证收集、网络侦察，并强化长期渗透的持久性策略。这些行为被认为是朝鲜关联网络行动的一部分，未来可能出现更复杂的攻击扩散。

Lazarus

2024 至 2025 年，Lazarus 组织将攻击范围扩展至加密货币、金融、IT、国防等多个行业。尤其开发了大量支持 macOS 和 Linux 的多平台恶意代码，并推出基于 Electron 和 Tauri 框架的新型后门及信息窃取工具。主要恶意代码包括 InvisibleFerret、BeaverTail、OtterCookie、CookiePlus、FrostyFerret 等，这些恶意代码具备键盘记录、剪贴板监控、浏览器缓存及加密货币钱包信息窃取功能。攻击技术方面，供应链攻击和水坑攻击尤为突出。

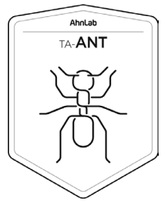
在韩国，Lazarus 通过利用软件漏洞的 Operation SyncHole 行动入侵了至少 6 个行业组织。同时，还通过 npm、PyPI、GitHub 等开源生态分发恶意软件包，感染开发者和企业。社会工程手法也在持续演进，如 ClickFix & ClickFake Interview 等虚假面试活动，结合高级心理战术诱导受害者。技术层面，采用多阶段混淆、VMProtect 和 Confuser 混淆、扩展属性（xattr）隐藏、JPEG 隐写、无文件执行、DLL 侧加载、基于 TxF 的 Process Doppelganging 等检测规避与持久化技术。此外，还出现了 MFA 绕过、OTP 窃取、云基础设施滥用等重要变化。

主要内容（要点）

- Konni 集中实施基于 LNK 文件的鱼叉式钓鱼攻击
- 利用基于 WordPress 的 C2 基础设施分发多种远程控制型恶意代码
- Lazarus 开发大量支持 macOS 和 Linux 的多平台恶意代码
- 在韩国通过利用软件漏洞的 Operation SyncHole 活动，入侵至少 6 个行业组织

2025年网络威胁趋势

攻击组织趋势 - APT：朝鲜



朝鲜

TA-RedAnt

自 2024 年至 2025 年，TA-RedAnt 组织将攻击范围扩展至东亚、南亚、中东、欧洲等多个地区，**目标涵盖政治、外交、国防、金融、医疗、能源、教育等多个行业。**TA-RedAnt 同样包含多个子组织，如 ScarCruft（APT37）、SideWinder、Transparent Tribe（APT36）、UNC3886（Fire Ant）等。

其采用的攻击手法多种多样，包括鱼叉式钓鱼、水坑攻击、伪装招聘、恶意文档（HWP、PDF、ISO、LNK 等）、恶意安装包及压缩文件（EGG、ZIP）、云端链接，以及基于 GitHub/Dropbox 的 C2 等。尤其值得注意的是，他们新引入了多项高级隐蔽与持久化技术，如 JPEG 隐写术、无文件执行、DLL 侧加载、基于 TxF 的 Process Doppelganging、Transacted Hollowing 等。

新确认的内容包括：Rust 编写的后门（Rustonotto、CHILLYCHINO）、VCD 勒索软件、PubNub/Ably 消息通信 C2、基于 LLM 的恶意代码（LAMEHUG）、MFA 绕过（AiTM、OTP 窃取）、AI 图像与语音伪造、Python 代码混淆等。此外，利用 .desktop 文件的 Linux 攻击、基于 WebSocket 的 C2、通过 Google Drive 传递载荷等多平台攻击也呈现增长趋势。

他们的社会工程手法也在不断演进，通过冒充真实人物、伪装学术活动与新闻简报、利用即时通讯群组、发送无链接邮件等方式以最大限度降低怀疑。攻击自动化与检测规避能力也进一步增强。同时，还使用合法文档、应用程序、签名程序伪装，构建基于云和合法服务器的 C2，采用多阶段解密与混淆、自删除及临时文件夹隐藏等技术。

TA-RedAnt 利用多种恶意代码和工具窃取凭证、系统信息、加密货币、文档、音频、USB/MTP 数据，**并在部分受害组织中投放勒索软件造成经济损失。**未来，TA-RedAnt 将持续演进其攻击技术，成为全球主要威胁之一。

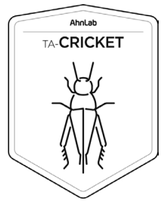
主要内容（要点）

- 针对政治、外交、国防、能源等多个行业目标
- 使用鱼叉式钓鱼、恶意安装包、云端 C2 等多种攻击手法
- 高级隐蔽与持久化技术，包括 JPEG 隐写术、无文件执行、DLL 侧加载
- 部分受害组织遭勒索软件感染，造成经济损失

2025年网络威胁趋势

攻击组织趋势 - APT：中国

中国 APT 组织以政府机构、外交、军事、工业领域为目标，开展长期且战略性的情报收集与监控。他们利用零日漏洞、供应链攻击、多平台恶意代码、云基础设施滥用等高级技术，并不断强化其检测规避能力。通过结合社会工程学与基于 AI 的自动化工具，大规模开展定制化钓鱼与攻击活动，同时追求地缘政治与经济利益。



中国

APT41

过去一年间，APT41 持续针对全球政府机构及各类产业开展高度复杂的攻击。该组织利用 Google Calendar 的 TOUGHPROGRESS 活动、基于 ClickOnce 的 OneClik 攻击、RunnerBeacon 后门、Anatsa（TeaBot）木马等多种技术，重点攻击政府机构、能源/石油/天然气行业及金融机构。同时，他们向日本企业投放侦察工具与加密 WebShell，并针对非洲政府 IT 基础设施发动攻击。**尤其在 2024 年 7 月，利用 Fortinet VPN 客户端（FortiClient）认证后残留在内存中的凭证提取零日漏洞进行攻击。**

APT41 通过 WordPress 基础 C2 架构、加密 HTTPS 流量、伪装的 TLS 协议规避检测，并通过自动化生成大量恶意样本，在不同时间点投放。其特点是同时开展供应链攻击与移动平台渗透，尤其在 iOS 和 Android 设备上投放定制恶意应用以窃取信息，并通过窃取云服务账户进一步向企业内部网络扩散。APT41 使用结合语言和文化特性的社会工程学手法，并利用 AI 自动化工具批量生成钓鱼内容，这一趋势已被研究人员捕获。

MirrorFace

自 2024 年 6 月以来，MirrorFace 将攻击目标从日本扩展至台湾、印度以及欧洲的外交机构。**其初始入侵主要通过鱼叉式钓鱼邮件以及利用 OneDrive 链接传播的 ZIP 压缩包实现。**ZIP 文件中通常包含宏文档（ROAMINGMOUSE）、快捷方式文件（LNK）以及 SFX 可执行文件等。同时，该组织还利用 SSL VPN 和文件存储服务的零日漏洞（CVE-2023-28461、CVE-2023-27997 等）获取初始访问权限，随后通过 MirrorStealer、Lodeinfo、Cobalt Strike 等工具窃取凭据并进一步渗透 Active Directory（AD） 服务器。其恶意代码基于最新版本的 ANEL 后门，并结合使用 NOOPDOOR、NOOPLDR 等新型恶意程序。为实现攻击自动化，MirrorFace 结合使用 PowerShell 脚本和基于 WMI 的命令执行。同时强化检测规避技术，如 Base64/HEX 编码、WMI 执行、UAC 绕过、沙箱规避等。

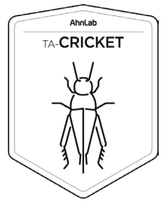
此外，该组织还针对日本政界人士和媒体开展定制化钓鱼活动。攻击基础设施利用云服务和 CDN（内容分发网络）伪装成正常流量。日本警方警告，该组织的活动很可能是有组织的信息收集企图。

主要内容（要点）

- APT41 利用 FortiClient 提取凭据的零日漏洞攻击案例已被报告
- 通过 WordPress 构建的 C2、加密 HTTPS 流量、TLS 协议伪装实现检测规避
- MirrorFace 通过鱼叉式钓鱼等手段进行初始访问，并利用零日漏洞尝试渗透
- 在日本针对政界人士和媒体开展定制化钓鱼活动

2025年网络威胁趋势

攻击组织趋势 - APT：中国



中国

Mustang Panda

自 2024 年至 2025 年，Mustang Panda 将攻击范围扩大至东南亚、东北亚、欧洲、南美等多个地区的政府、外交、军事、非政府组织（NGO）、学术机构等目标。**初始入侵通过鱼叉式钓鱼邮件和恶意文档（LNK、CHM、OneNote、PDF、HTML、ISO 等）实现，并引入多种攻击技术，如 HTML Smuggling、USB 蠕虫（SnakeDisk）、基于云的钓鱼等。**

恶意代码方面，攻击者使用了 PlugX、TONESHELL、Bookworm、PUBLOAD、MQsTTang、CCoreDoor、ShadowPad 等多种后门和 远控木马（RAT）。此外，还发现了 StarProxy、PAKLOG/CorKLOG、SplatCloak、Yokai 等大量新工具。这些工具具备横向移动、键盘记录、EDR 绕过、USB 传播功能。其规避检测技术也进一步提升，包括：通过合法进程（如 MAVInject.exe）进行 DLL 注入；基于 WriteProcessMemory 的反射式 DLL 注入（Reflective DLL Injection）；利用 FakeTLS 和 TLS-like 头隐藏 C2 流量；使用 Cloudflare CDN、Google Drive、Box 等云基础设施传递载荷。社会工程学手法也有所强化，使用与地区热点相关的定制诱饵文档，例如台湾大选、蒙古洪灾、东盟会议、西藏活动等。WebSocket C2、基于 AES/DES 的多阶段加密、通过窃取 Kavach OTP 绕过 MFA 等，也是在近期出现的新技术。

Salt Typhoon

自 2024 年至 2025 年，Salt Typhoon 针对美国、亚洲、中东、非洲地区的电信公司、政府、军事及非政府组织（NGO），开展长期监控和情报收集活动。**攻击者利用公开的服务器和网络设备漏洞（CVE-2018-0171、CVE-2023-20198 等）获取初始访问权限，**并在内部通过 WMIC.exe、PSEXEC.exe 执行横向移动。为提升 AD 环境权限，攻击者采用 Kerberos 凭证伪造及 Pass-the-Hash 技术，并**强化利用合法管理工具的 Living-off-the-land（LOTL）策略以规避检测。**

恶意代码方面，主要使用 GHOSTSPIDER、SNAPPYBEE、MASOL RAT。其中，GHOSTSPIDER 采用模块化设计并结合 TLS 加密，提高分析难度；SNAPPYBEE 通过调用云端 API 实现数据泄露；MASOL RAT 则结合无文件执行与 PowerShell 混淆以规避检测。2025 年 5 月，该组织利用 Commvault Metallic SaaS 平台的零日漏洞（CVE-2025-3928）入侵 Microsoft 365 环境。此外，他们采用 ShadowPad、SoftEther VPN 隐藏 C2 流量，改进利用 CAB 文件安装 DEMODEX Rootkit 的方式，并通过合法进程注入实现持久化。攻击基础设施利用 CDN 和云存储伪装正常流量。还发现其结合 Python 脚本与 AI 生成钓鱼内容实现攻击自动化的迹象。

主要内容（要点）

- MustangPanda 利用鱼叉式网络钓鱼邮件和恶意文档进行初始入侵。引入 HTML Smuggling 等多种攻击技术。
- 在重复使用现有工具和基础设施的同时，采用新的恶意代码和隐匿技术以增强精细化。
- Salt Typhoon 利用公开的服务器及网络设备漏洞获取初始访问权限。
- 为规避检测，强化 LOTL 策略，并推进恶意代码开发、流量伪装、攻击自动化等多种战术升级。

2025年网络威胁趋势

攻击组织趋势 - APT：俄罗斯

俄罗斯 APT 组织利用地缘政治冲突，对政府、军事、外交及战略机构开展长期且有组织的攻击。采用高级技术，如电子邮件钓鱼、公开漏洞利用、基于云基础设施的 C2 隐匿、无文件执行等，具备卓越的规避检测能力。为扩大心理战和政治影响力，开展定制化活动，不仅窃取信息，还企图攻击关键基础设施。

俄罗斯

APT28

APT28 持续针对乌克兰、北约及东欧的政府、军事、防务产业和技术领域发动攻击。该组织利用地缘政治冲突开展定制化钓鱼活动，**并以俄乌战争及北约峰会相关文件作为诱饵。**初始入侵主要通过电子邮件钓鱼及漏洞利用（CVE-2023-38831、CVE-2023-23397 等），并积极利用 Outlook、Roundcube、Zimbra 等邮件服务器漏洞。

该组织引入基于 LLM 的恶意代码（LAMEHUG），用于自动生成命令及信息收集，在持久化方面强化了 MFA 绕过（AiTM）、COM 劫持、UAC 绕过等技术。此外，利用 Google Drive 等云基础设施隐藏 C2 通信，通过伪装成正常流量实现规避检测。他们结合 Python 脚本与 PowerShell 混淆技术，大量生成恶意样本以实现攻击自动化。主要恶意代码包括 HeadLace、GooseEgg、MASEPIE，具备凭证窃取、网络侦察及横向移动功能。此外，该组织还使用 Cobalt Strike、Sliver 等开源攻击框架以提升攻击链复杂度。近期引入 HTML Smuggling、无文件执行及 JPEG 隐写等载荷隐藏技术。

Gamaredon

Gamaredon 组织针对乌克兰及俄语用户开展高级鱼叉式钓鱼和信息收集活动。初始入侵通过利用 LNK、HTA、XHTML 文件的钓鱼活动实现。文件执行后，会加载基于 PowerShell 的恶意代码，用于收集系统信息并下载额外载荷。该组织利用 Cloudflare Tunnels、DNS over HTTPS（DoH）等外部基础设施规避 C2 检测。同时结合 Python 脚本与 PowerShell 混淆实现攻击自动化。**新型恶意代码 GammaDrop、GammaLoad、GammaSteel 使用了混淆、注册表隐藏、USB 驱动器武器化等复杂技术。**其中，GammaSteel 通过无文件执行和多层加密增加分析难度。

移动平台攻击也在加强。通过 BoneSpy、PlainGnome 等**安卓监控恶意软件针对俄语用户，**其中部分伪装成三星 Knox 渗透企业。恶意应用可收集通话记录、消息、位置信息，并远程控制摄像头和麦克风。2025 年，该组织针对驻乌克兰的西方军队实施基于 PowerShell 的信息窃取。其活动已超越单纯间谍活动范畴，还结合军事、外交情报收集与心理战攻击。推测与俄罗斯联邦安全局（FSB）下属第 18 信息安全中心存在关联。

主要内容（要点）

- APT28 开展钓鱼活动，并以俄乌战争及北约峰会相关文件作为诱饵。
- 引入基于 LLM 的恶意软件（LAMEHUG），尝试自动生成命令并进行信息收集。
- Gamaredon 使用恶意软件，采用混淆、注册表隐藏、USB 驱动器武器化等复杂技术。
- 加强移动平台攻击，通过安卓监控恶意软件针对俄语用户。

2025年网络威胁趋势

攻击组织趋势 - APT：伊朗

伊朗 APT 组织以中东和欧洲为中心，针对外交、媒体、人权组织及政府机构开展长期攻击行动。他们使用鱼叉式钓鱼、HTML Smuggling、无文件执行、MFA 绕过、OTP 窃取等高级技术手段。还通过云基础设施和隐写术（Steganography）进一步增强规避检测能力。此外，他们将安卓恶意代码与 AI 生成的钓鱼内容相结合，将攻击范围扩展至移动设备。

伊朗

Charming Kitten

Charming Kitten 以中东和欧洲为中心，针对外交、媒体及人权组织开展攻击。初始入侵主要利用基于社会工程的钓鱼与恶意文档投放，**并新增 LNK 文件与 PowerShell 结合的多阶段加载方式。**该组织通过在 JPEG 图像中利用隐写术隐藏恶意代码，并大量使用无文件执行技术以规避检测。

Charming Kitten 通过 **MFA 绕过与 OTP 窃取技术破坏认证体系，**并运营基于 AiTM（Adversary-in-the-Middle）的钓鱼站点，以实时劫持会话。其云端 C2 通信利用 Dropbox、Google Drive、Telegram API 等平台伪装成正常流量，同时结合 TLS 加密与 DNS over HTTPS（DoH）规避网络检测。主要使用的恶意代码包括 POWERSTATS、NokNok、CharmPower，具备键盘记录、浏览器 Cookie 窃取及系统信息收集等功能。

MuddyWater

MuddyWater 持续针对中东、欧洲、南亚地区的政府、外交、通信与工业组织实施攻击。该组织**积极利用 LOTL（Living-off-the-land）技术，通过 PowerShell、MSHTA 等合法工具实现初始入侵与命令执行。**攻击中使用鱼叉式钓鱼邮件分发恶意 LNK 文件，并结合正常文档与恶意脚本以规避检测。同时扩大使用 Ligolo、SimpleHelp、Venom Proxy 等**开源工具进行 C2 通信，并通过 VPN 与远程管理工具（RMM）在内部横向移动。**尤其值得注意的是，MuddyWater 使用 BugSleep（MuddyRot） 后门替代传统的 Atera RMM，并结合 Python 脚本与 PowerShell 混淆实现攻击自动化。无文件执行与内存加载恶意代码是其典型特征之一，规避检测时还采用正常进程注入与 UAC 绕过。

主要恶意代码包括 MuddyC2Go、BugSleep、SimpleHelp RAT，具备凭证窃取、键盘记录及网络侦察功能。此外，MuddyWater 利用 DNS over HTTPS（DoH）与 TLS 加密隐藏 C2 流量，并使用云服务（Google Drive、Dropbox）投递有效载荷。
在攻击基础设施方面，他们还利用 CDN 与合法网站实施水坑攻击。

主要内容（要点）

- Charming Kitten 基于社会工程的钓鱼和恶意文档投放，新增结合 LNK 文件与 PowerShell 的多阶段加载方式。
- 通过 MFA 绕过和 OTP 窃取技术破坏认证体系。
- MuddyWater 利用 LOTL 技术，通过合法工具实现初始入侵和命令执行。
- 扩大使用开源工具进行 C2 通信，并通过 VPN 和远程管理工具实现内部扩散。

2025年网络威胁趋势

攻击组织趋势 - APT：印度

印度 APT 组织主要针对南亚和中东地区的政府、军事及外交机构开展长期攻击。他们使用鱼叉式钓鱼、HTML Smuggling、PowerShell 混淆、DLL 侧加载等高级技术手段，并通过云基础设施和隐写术提升规避检测能力。此外，他们使用安卓恶意代码开展多平台攻击，并结合 AI 生成的钓鱼内容进一步提升社会工程技术。

印度

Bitter

Bitter 持续针对南亚和中东地区的政府、军事及外交机构发动攻击。初始入侵通过夹带恶意文档和 LNK 文件的电子邮件攻击实现。**该组织新增使用 HTML Smuggling 和基于 PowerShell 的恶意代码，以增强规避检测能力。**通过将正常文档与恶意脚本结合来获取受害者信任，并采用多阶段加载方式隐藏有效载荷。

Bitter **还利用安卓恶意代码将攻击范围扩展至移动设备。其恶意应用可窃取金融信息、短信、地理位置数据，并具备远程控制摄像头与麦克风的功能。**其云端 C2 通信利用 Dropbox、Google Drive、Telegram API 等平台伪装成正常流量，同时结合 TLS 加密与 DNS over HTTPS（DoH）规避网络检测。通过基于 AiTM（中间人攻击）的钓鱼网站及 OTP 窃取绕过 MFA。主要使用的恶意代码包括 AridViper 变种、BitterRAT、VajraSpy，具备键盘记录、浏览器 Cookie 窃取及系统信息收集功能。他们结合 Python 脚本与 PowerShell 混淆技术，大量生成恶意样本以实现攻击自动化。社会工程诱饵文档也更加多样化，尤其是伪装成政府政策文件、外交谈判资料、军事报告的邮件被大量发现。

Sidewinder

SideWinder 组织将攻击范围扩展至南亚、东南亚和中东地区的政府、军事、外交、能源、教育机构。**该组织围绕 WarHawk 系列恶意代码开发了多种模块，包括 USB 蠕虫、键盘记录、信息窃取等功能。**通过结合多阶段加载与无文件执行，其规避检测能力进一步提升。初始入侵主要通过鱼叉式钓鱼邮件分发恶意 LNK 文件，以及采用 HTML Smuggling 技术。

该组织利用 PowerShell 混淆、DLL 侧加载、基于 TxF 的 Process Doppelganging 等高级技术规避检测。同时通过 Cloudflare CDN 和 Google Drive 隐藏 C2 通信，并结合 TLS 加密与 DNS over HTTPS（DoH）规避网络检测。主要使用的恶意代码包括 WarHawk、SideWinder RAT、SplatCloak，具备键盘记录、浏览器 Cookie 窃取、系统信息收集、USB 传播等功能。**社会工程手法持续进化，如冒充真实人物、伪装学术活动及利用群组消息平台。**攻击者还会与受害者进行多轮邮件往来，以建立信任关系。此外，还发现其结合 Python 脚本与 AI 生成钓鱼内容实现攻击自动化的迹象。

主要内容（要点）

- Bitter 新增使用 HTML Smuggling 和基于 PowerShell 的恶意代码，强化规避检测能力。
- 安卓恶意应用窃取金融信息、消息、位置信息，并远程控制摄像头和麦克风。
- SideWinder 以 WarHawk 系列恶意软件为核心，开发包含 USB 蠕虫、键盘记录及信息窃取功能的多种模块。
- 社会工程技术演进：冒充真实人物、伪装学术活动、利用群组消息平台。

2025年网络威胁趋势

攻击组织趋势 - APT：巴基斯坦及其他

巴基斯坦 APT 组织针对印度、巴基斯坦、中东及非洲的政府、军事、教育及 NGO 开展长期攻击。他们利用多种恶意代码同时攻击 Windows、Linux 和 Android 环境。通过 MFA 绕过和基于 WebSocket 的 C2 通信规避检测。利用云端基础设施与隐写术隐藏恶意载荷，并通过定制化钓鱼、AI 生成内容等方式不断强化社会工程技术。

巴基斯坦及其他

Transparent Tribe

Transparent Tribe 持续针对印度、巴基斯坦、中东及非洲地区的政府、军事、教育及 NGO 开展攻击。该组织使用 CapraRAT、CrimsonRAT、ObliqueRAT 等**多种 RAT，同时攻击 Windows、Linux、Android 环境。**尤其在 Linux 环境中，了首次采用基于“.desktop”文件的攻击方式。通过 WebSocket 实现 C2 通信以增强规避检测能力，并通过窃取 Kavach OTP 绕过 MFA，还利用 AiTM 钓鱼网站执行实时会话劫持。

Transparent Tribe 积极利用云端基础设施。Transparent Tribe 积极使用云基础设施，扩大通过 Google Drive、Slack、Telegram API 的 C2 通信，并结合 TLS 加密与 DNS over HTTPS（DoH）规避网络检测。主要使用恶意代码包括 CrimsonRAT、CapraRAT、ObliqueRAT，还发现其使用安卓恶意应用。攻击者以正常应用为伪装分发恶意应用，并在 APK 文件中使用隐写术隐藏恶意载荷。社会工程技术多样化，使用定制化诱饵文档，如伪装成外交谈判资料、学术活动邀请函的电子邮件，并通过多轮邮件往来建立信任关系。此外，发现其结合 Python 脚本与 AI 生成的钓鱼内容实现攻击自动化的迹象。

其他

被归类为“其他”的 APT 组织，其活动模式复杂多变，难以按照国家维度进行分类。这些组织以政府、国防、金融、通信、教育、NGO 等多种行业为目标，活动范围遍及亚洲、中东、欧洲、美洲等全球地区。它们**普遍采用基于社会工程的鱼叉式钓鱼，并利用多种文档格式开展初始入侵。**同时，通过 PowerShell 等脚本型恶意代码进行多阶段加载。积极利用云服务和开源基础设施，尤其是 GitHub、Dropbox、Google Drive、Telegram 等作为 C2 通信渠道。此外，它们还使用 Rust、Go、Python 等**多种语言开发恶意代码，同时攻击 Windows、Linux、macOS、Android 等多平台环境。**

其使用的检测规避技术高度先进，包括混淆、加密、无文件执行、DLL 侧加载、COM 劫持、日志清除、时间戳篡改等多种方式。尤其是，LLM 驱动的恶意代码（LAMEHUG）、ClickFix、HTML Smuggling 等最新社会工程技术，以及 MFA 绕过、会话 Cookie 窃取等认证体系破坏技术也被广泛使用。部分组织甚至会控制其他组织的基础设施，或通过“假旗（False Flag）”策略制造混乱。

主要内容（要点）

- Transparent Tribe 利用多种 RAT，同时攻击 Windows、Linux、Android 环境。
- 利用云端基础设施扩大 C2 通信，并规避网络检测。
- 其他组织普遍采用基于社会工程的鱼叉式钓鱼及多种文档格式进行初始入侵。
- 通过多种语言开发的恶意代码，同时攻击 Windows、Linux、macOS、Android 等多平台环境。

2025年网络威胁趋势

勒索软件趋势

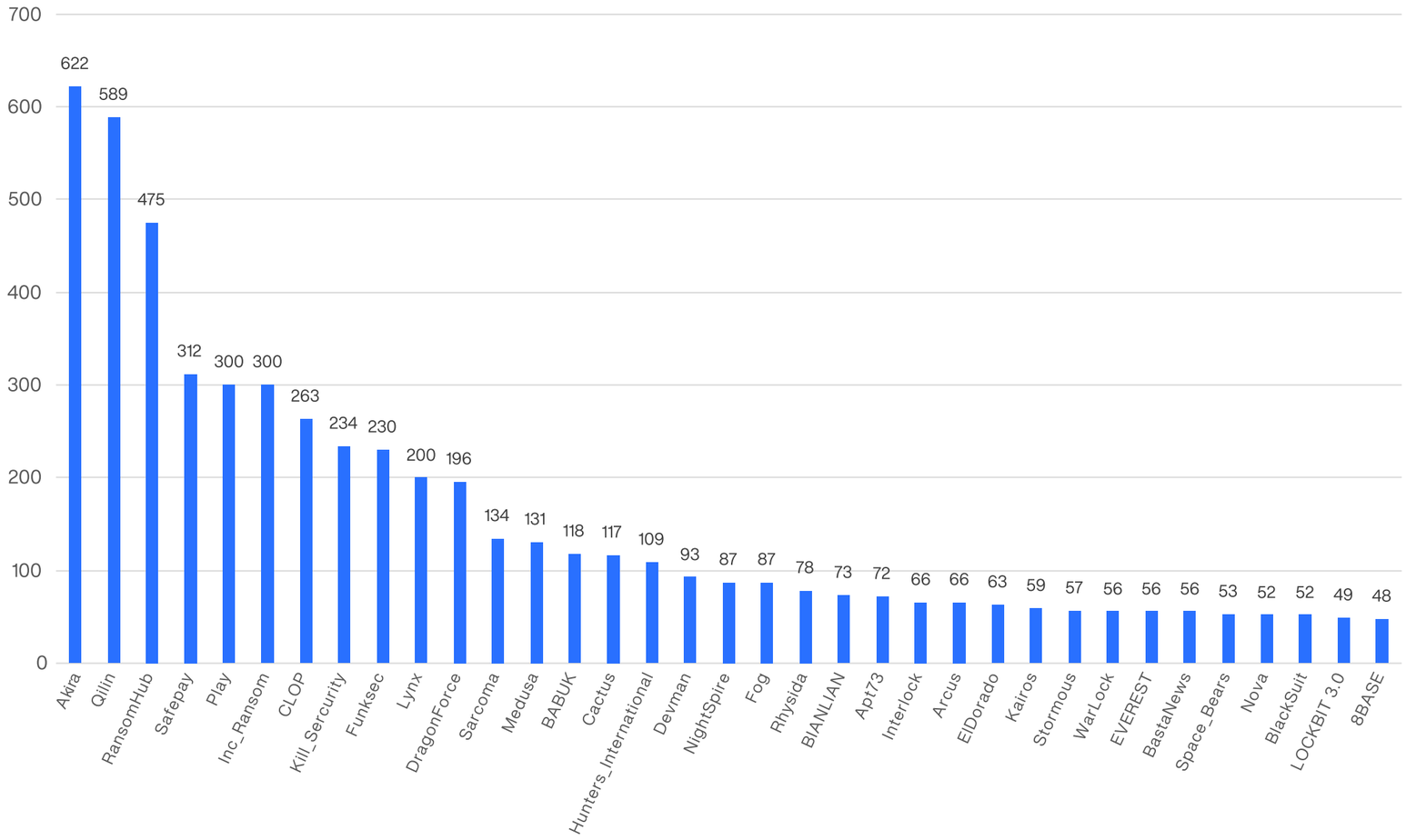
概况及动向

2025 年勒索软件生态系统相比去年扩大了 38%，呈现爆发式增长。尽管执法打击部分主要组织受挫，但活跃的攻击组织数量仍增长至 96 个，同比上升 26%，生态系统碎片化进一步加速。

攻击组织排名也发生了显著变化：造成 622 起受害事件的 Akira **从去年第 4 位跃升至第 1 位；**Qilin 以 589 起事件从第 11 位跃升至第 2 位；CLOP 也从第 43 位升至第 7 位；相比之下，2024 年排名第 1 的 LockBit 因 Operation Cronos 行动受到重创，跌出前 30 名。

此外，朝鲜背景的 Andariel 和 Moonstone Sleet 开始分发 Play 和 Qilin 勒索软件，**显示出国家支持的攻击组织正逐步并入 RaaS（勒索软件即服务）体系，呈现“卡特尔化”趋势，**为追求经济利益及规避国际制裁提供新的运作模式。

2025 年各勒索软件组织公布受害企业数量



2025年网络威胁趋势

勒索软件趋势

执法机构的打击及其局限性

今年，执法机构加强了对勒索软件的打击力度，但整体效果仍有限。在 Operation Cronos 受挫后，LockBit 于 2025 年 9 月发布 LockBit 5.0 宣布“复活”，并明确允许攻击核电站、火力发电站等关键基础设施，回归更具攻击性的战术。

2025 年 4 月，曾在 2024 年攻击次数排名第一的 RansomHub 突然宣布停止活动。 尽管 DragonForce 声称已吸收 RansomHub，但 RansomHub 指控 DragonForce 与执法机构合作，引发分裂。

ヨ生态系统随之重组，再次展现了 RaaS 体系具有极强的恢复力与适应性。

主要攻击战术

勒索软件攻击技术已演变为 “三重勒索” 策略：数据加密、数据外泄及联系受害组织的客户和合作伙伴施压。
该策略在医疗、金融行业中被广泛使用，以最大化声誉损害。

另一个值得关注的趋势是从零日漏洞转向 1-Day 漏洞的利用。
- CLOP 利用 Cleo MFT 零日漏洞攻陷了超过 400 家机构；
- Akira 集中攻击 SonicWall SSL VPN 漏洞MFT 平台与 VPN 设备成为新的关键攻击向量。

应对方案及展望

预计勒索软件将继续向 AI 自主攻击系统与 LLM 辅助战术演进，“无加密、纯数据泄露型”攻击也将持续增加。以朝鲜案例为开端，国家支持黑客与网络犯罪组织的合作将进一步加强。

有效应对勒索软件需要构建多层防御体系：引入零信任架构、 对 VPN 和 RDP 实施多因素认证（MFA）、加强 VMware ESXi 等虚拟化环境安全，并通过网络微分段防止横向扩散同样重要。
基于威胁情报的 24/7 持续监控、利用 IAB（初始访问经纪人）交易与实际攻击之间 18 天窗口进行早期检测，以及使用物理隔离的离线备份和不可变备份是也是必不可少的。

主要内容（要点）

- 尽管大型勒索软件组织受到打击，但 RaaS 生态展现出极强的恢复能力
- 勒索软件攻击技术演变为“三重勒索”——在数据泄露威胁之外，进一步向客户与合作伙伴施压
- 应对不断演变的勒索软件，需要采用多层防御体系：零信任、MFA、基于情报的监控等

2025年网络威胁趋势

勒索软件趋势 - Top 10 主要组织活动分析

1.Gunra -入侵韩国金融业

Gunra 是于 2025 年 4 月首次发现的新型勒索软件组织，主要针对韩国、日本、巴西、土耳其及台湾等国家和地区，值得注意得是受害国家中没有美国。该组织的勒索软件基于 Conti v2 源代码开发。

其最大特点是仅 5 天极短谈判期限，对受害组织施加强烈心理压力。在暗网中，Gunra 运营类似 WhatsApp 风格的谈判门户，并设有专门的“经理”角色，运营十分体系化。

Gunra 勒索软件可同时攻击 Windows 和 Linux 环境，尤其拥有支持最多 100 个并发加密线程的高性能 Linux 变种。Linux 版本使用 ChaCha20 加密算法，但在实现过程中出现了加密弱点，这使得韩国保证保险机构成功实现了解密。

2.Qilin - 建立压倒性统治力

Qilin 在 2024 年韩国和日本的攻击记录为零，但在 2025 年却在两国发动了数十起攻击，成为最活跃的勒索软件组织之一。在 RansomHub 消失后，Qilin 快速填补空白，大量吸收了流散的附属成员（affiliate）。**在韩国，Qilin 发起 “Korean Leak” 活动，通过攻击 IT 供应链，攻击 29 家中小资产管理公司。**

值得关注的是，**具有朝鲜背景的 Moonstone Sleet 自 2025 年 2 月开始分发 Qilin 勒索软件，逐渐演变为国家支持的威胁组织。**2025 年 9 月，Qilin 还与 DragonForce、LockBit 形成“卡特尔式联盟”，建立市场支配型合作体系。

3.Play -与朝鲜 Andariel 的结合

2024 年 10 月确认，Play 勒索软件组织与具有朝鲜背景的 Andariel 建立合作关系，**这是国家背景攻击组织首次利用 RaaS 基础设施的案例。**Andariel 在 2025 年 5 月渗透受害组织后，部署 Sliver C2 框架和 DTrack 后门，并长期潜伏，最终于 9 月分发 Play 勒索软件。

2025 年上半年，FBI 公布约 900 家机构遭受 Play 勒索软件攻击。自 WannaCry 以来，朝鲜一直利用勒索软件作为资金筹措手段，与 Play 的合作被视为规避国际制裁的新策略。

主要内容（要点）

- Gunra 勒索软件同时攻击 Windows 与 Linux；其 Linux 版本存在加密实现弱点
- 具有朝鲜背景的 Moonstone Sleet 自 2 月起分发 Qilin 勒索软件，向国家支持型威胁组织演进
- Play 勒索软件与朝鲜 Andariel 合作——国家背景攻击组织首次利用 RaaS 基础设施

2025年网络威胁趋势

勒索软件趋势 - Top 10 主要组织活动分析

4.Akira - 攻击 SSL VPN 设备

Akira 在 2025 年保持了稳定的增长率，攻击次数位居首位。该组织改变了战术，从 2024 年零星的大规模数据泄露模式转向 2025 年第一季度开始的定期小规模泄露。

最引人注目的事件是自 7 月份以来集中攻击 SonicWall SSL-VPN 设备。他们利用 CVE-2024-40766 漏洞在全球范围内发动了攻击。8 月，美国组织中连续观测到网络扫描、横向移动、权限提升和数据泄露。

该组织还专门针对 Vmware ESXi 虚拟化环境发动攻击，具备广泛加密云基础设施的能力。他们开发了基于 Rust 的新变种（Akira v2），并采用了高级混淆技术。此外，他们还使用了滥用 PowerTool、删除日志等多种规避 EDR (端点检测与响应) 的技术。该组织将制造业、教育和医疗领域作为主要目标，在 2025 年上半年攻击了数十个组织，确立了代表性攻击组织的地位。

5.Lynx - 集中攻击制造业

Lynx 于 2024 年 7 月出现，是 INC 勒索软件代码的品牌重塑。其受害者数量从 2025 年 1 月的 96 个急剧增加到 8 月的 300 个。该组织从 6 月份开始以 Sinobi 的名义实施多品牌战略。**他们主要针对制造业和建筑业，美国占了所有受害国家的 60%**。

1 月，他们攻击了一家美国律师事务所，窃取了客户敏感信息；12 月，瘫痪了一家罗马尼亚能源供应商。该组织声称是道德黑客，但实际上采用双重勒索战术，发动机会主义且无差别的攻击。

6.LockBit - 以 5.0 版本复苏

LockBit 在 2024 年 2 月的 “Cronos 行动”之后遭受了严重打击。随后，在 2025 年 9 月，该组织借其成立六周年之际，宣布以 LockBit 5.0 复苏。**新版本加强了跨平台战略，同时针对 Windows, Linux 和 VMware ESXi 进行攻击。**此外，还应用了 DLL 反射加载、ETW 修补等高度复杂的反分析技术。

最值得注意的是，该组织明确允许附属成员攻击此前对外宣称克制的核电站、火电站等关键基础设施。

主要内容（要点）

- Akira 勒索软件，利用 SonicWall SSL-VPN 设备漏洞在全球范围内发动攻击。
- Lynx 勒索软件，主要针对制造业和建筑业进行攻击 — 美国占所有受害国家总数的 60%。
- LockBit 5.0，加强了同时针对 Windows、Linux 和 VMware ESXi 的跨平台战略。

2025年网络威胁趋势

勒索软件趋势 - Top 10 主要组织活动分析

7.DragonForce - “卡特尔”战略

DragonForce 于 2023 年底出现，并于 2025 年 3 月宣布成立“勒索软件卡特尔”（Ransomware Cartel），试图重塑勒索软件生态系统。**该组织引入了“白标”模式（White Label Model），允许附属成员使用自己的品牌进行活动，同时利用 DragonForce 的基础设施。**他们向附属成员分配 80% 的收入，并提供 PB 级存储、24 小时监控、博客和文件服务器。2025 年 4 月，DragonForce 声称已接管 RansomHub 的基础设施。然而，RansomHub 反驳称 DragonForce 正在与执法机构合作，双方冲突浮出水面。

8.CLOP - 攻击 Cleo MFT 解决方案

CLOP 在 2025 年第一季度强势回归。核心是**通过利用 Cleo MFT 解决方案的两个零日漏洞（CVE-2024-50623, CVE-2024-55956）进行攻击。**尽管 Cleo 在 10 月修补了第一个漏洞，但 CLOP 在 11 月成功绕过了补丁，并在 12 月发现了第二个零日漏洞，持续发动攻击。约 400 个组织受到侵害。CLOP 利用其在 2023 年攻击 MOVEit（导致超过 2,000 个组织受损）的经验，展现出针对 MFT 平台漏洞攻击的专业性。从 1 月开始，该组织按字母顺序公布了受害者名单，最终受害规模超过数百起。

9.RansomHub - 昔日强者的兴衰

RansomHub 以高达 90% 的附属成员收入分成比例以及超过 210 个组织受侵害的记录，在 2025 年第一季度保持了最高的活跃度。然而，在 4 月 1 日，该组织的活动突然完全停止。

RansomHub 的瓦解引发了数百名附属成员转向 Qilin, DragonForce, Lynx 等其他组织，从而推动了大规模的生态系统重组。这是继 2024 年 LockBit 的“Cronos 行动”之后最大的结构性变化，再次印证了勒索软件生态系统的不稳定性和动态性。

10.针对日本企业的攻击增加

在 2024 年 10 月至 2025 年 9 月期间，**日本遭受的勒索软件攻击比去年同期增加了 217%。**Qilin 是攻击次数最多的组织，Lynx, Nightspire, RansomHub, Akira 等组织也对安全防护薄弱的中小企业发起了攻击。

新的攻击组织 Kawa4096 于 6 月底出现后立即攻击了两个组织。该组织的 KaWaLocker 勒索软件具备 Salsa20 加密、多线程和文件名哈希功能，并在 7 月发布的 2.0 版本中进一步增强了功能。制造业受到的冲击最大，中小企业占了受害者的大多数。

主要内容（要点）

- DragonForce 引入“白标”模式，允许附属成员使用自有品牌进行活动，同时利用 DragonForce 的基础设施。
- CLOP 勒索软件，利用 Cleo MFT 解决方案的零日漏洞发动攻击 — 约 400 个组织受到侵害。
- 针对日本的勒索软件攻击增加了 217% — 制造业受到的冲击最大，中小企业占多数受害者。

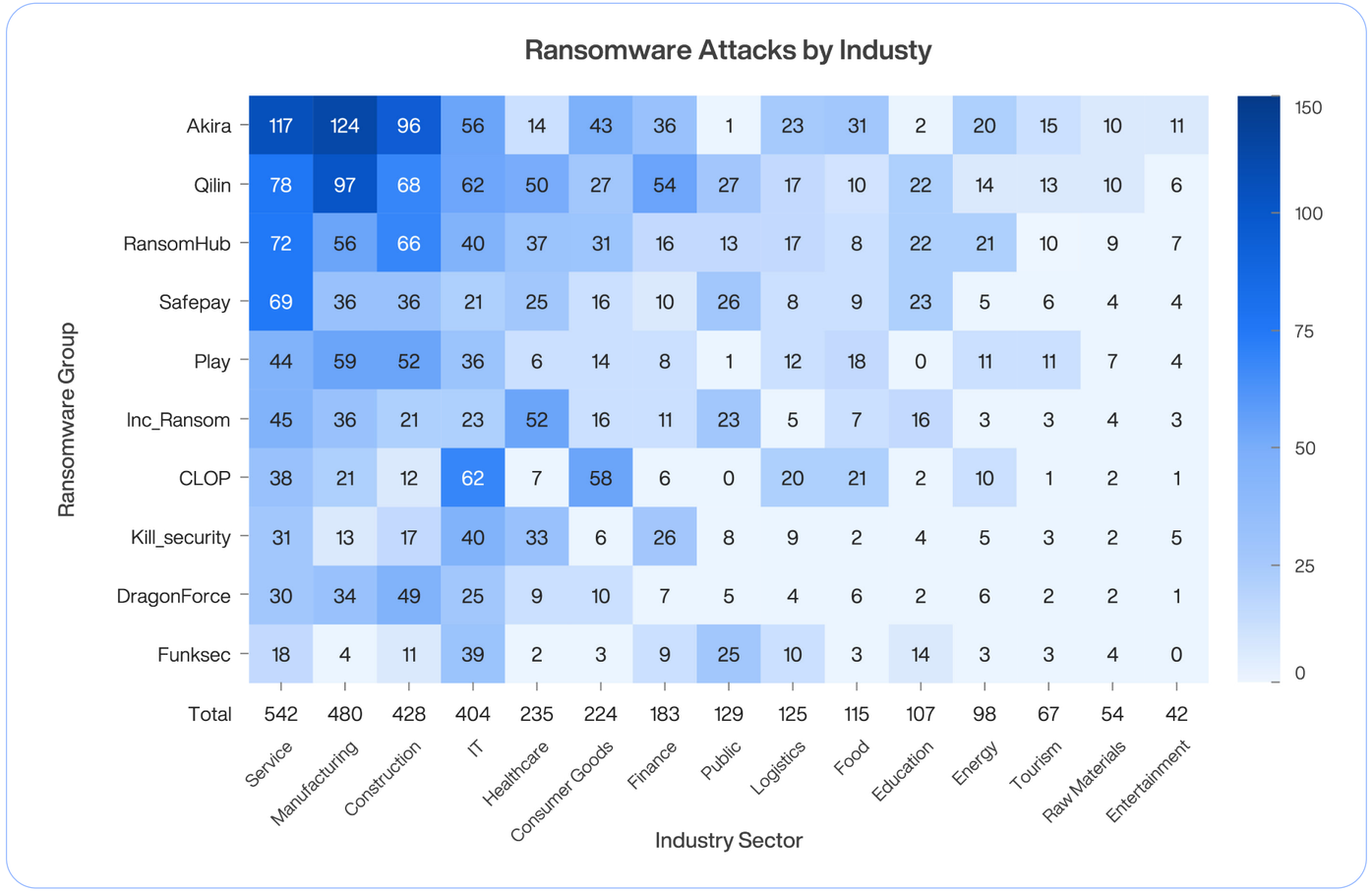
2025年网络威胁趋势

勒索软件趋势 - 主要受害行业

2025 年勒索软件攻击组织针对主要受害行业的分析结果显示，服务业、制造业、建筑业和 IT 领域是主要的攻击目标。**最值得关注的变化是服务业成为受害最多的行业。**因为新冠疫情后数字化转型，服务业对 IT 的依赖度提高，且系统中断时会立即遭受收入损失等影响。

制造业和建筑业仍然是主要目标。制造业因智能工厂和供应链管理系统的扩大而攻击面增加。生产线中断会造成巨大损失，因此支付恢复费用的可能性也高。建筑业因项目延期面临巨大的违约金和法律纠纷风险，因此恢复压力很大。IT 行业因拥有大规模客户数据，持续被攻击者盯上。

最令人担忧的变化是医疗领域的攻击增加。该领域曾被默认是攻击禁区，但在 2025 年这一界限被彻底打破。例如，BlackCat 在 2024 年被执法机构行动瓦解后复苏，解除了禁止攻击医院的禁令，并鼓励进行攻击。由于直接关系到患者生命，不可能延迟恢复，且敏感医疗信息泄露会带来巨大的法律和道德责任，使其成为攻击者青睐的高收益目标。另一方面，食品、旅游等行业的攻击频率较低。这被解读为由于其数字化依赖度较低，且倾向于传统的运营方式，因此未被攻击者列为主要目标。



[图] 勒索软件组织针对行业攻击的现状 (2024 年 10 月 ~ 2025 年 9 月)

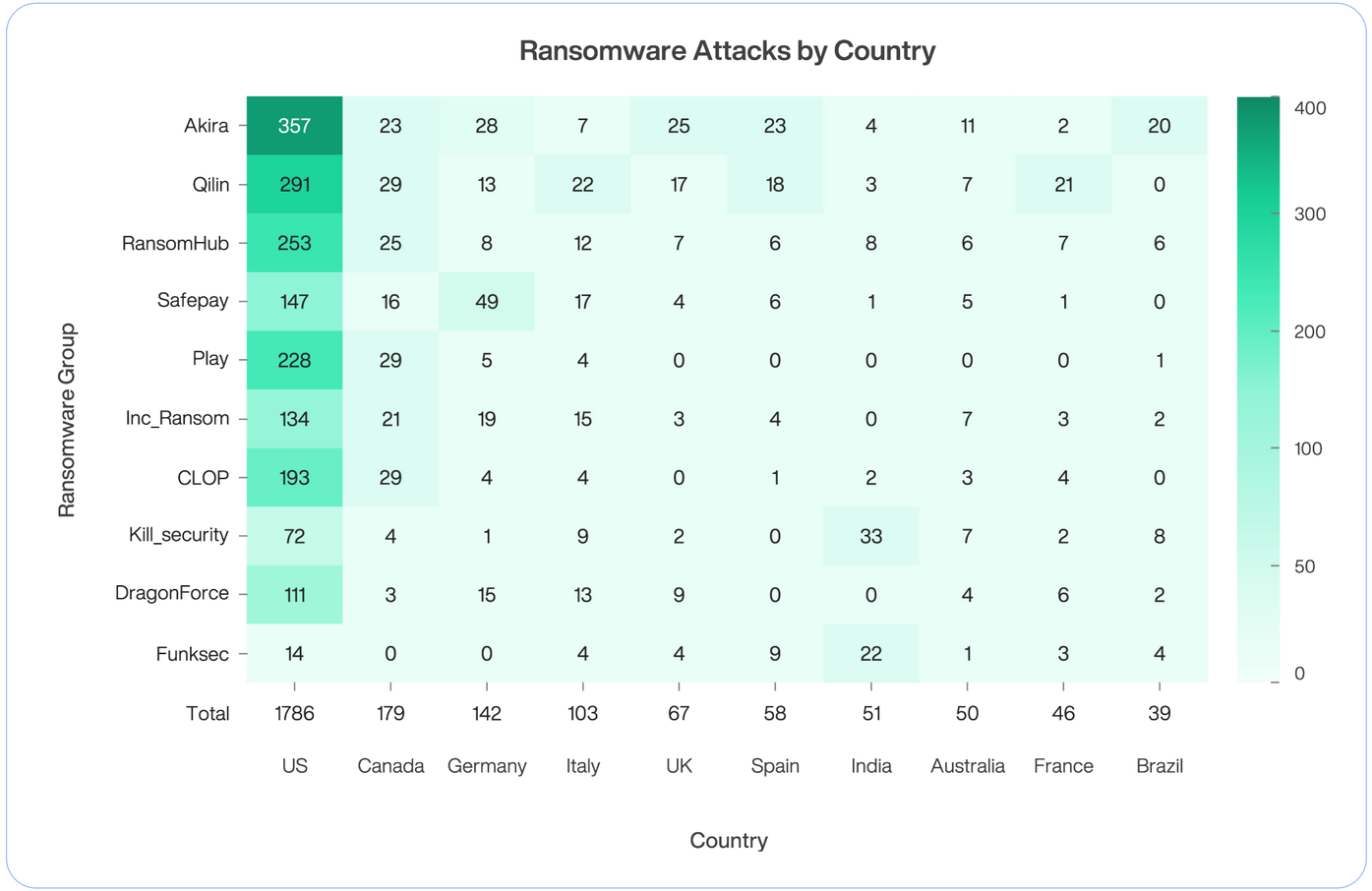
2025年网络威胁趋势

勒索软件趋势 - 主要受害国家：全球

根据 2025 年的统计数据，美国仍然是遭受勒索软件攻击最多的国家。**Akira 和 Qilin 持续发动攻击，RansomHub 在 4 月停止活动前也一直将美国企业/机构作为目标。**作为全球最大的经济体，美国高附加值产业（如制造、IT、医疗、金融）集中，且数字化依赖度高，具备易受网络威胁的结构性特点。大规模客户数据和敏感信息集中在云端，使其成为数据泄露和双重/三重勒索的主要目标。

欧洲和亚洲地区的攻击模式多样化也值得关注。德国遭受 Safepay 和 Akira 的集中攻击，受害程度同比增加。特别是数据泄露型勒索攻击尤为突出。法国和英国也持续遭受打击。**在亚洲，印度崛起成为 Kill_Security 和 Funksec 的基地，成为新的攻击目标。**加拿大因其地理位置邻近美国和相似的经济结构，受害仍然较多。

西班牙、意大利、巴西等国也成为主要受害国。在欧洲，Qilin 和 Akira 持续攻击西班牙和意大利。在南美洲，巴西遭受 Akira 的集中攻击。亚太地区确认澳大利亚和日本是主要受害国。美国政府及其盟友通过国际合作调查和制裁积极应对勒索软件生态系统。然而，攻击者利用法律管辖的漏洞，以海外基础设施为基础发动攻击，从而逃避制裁。



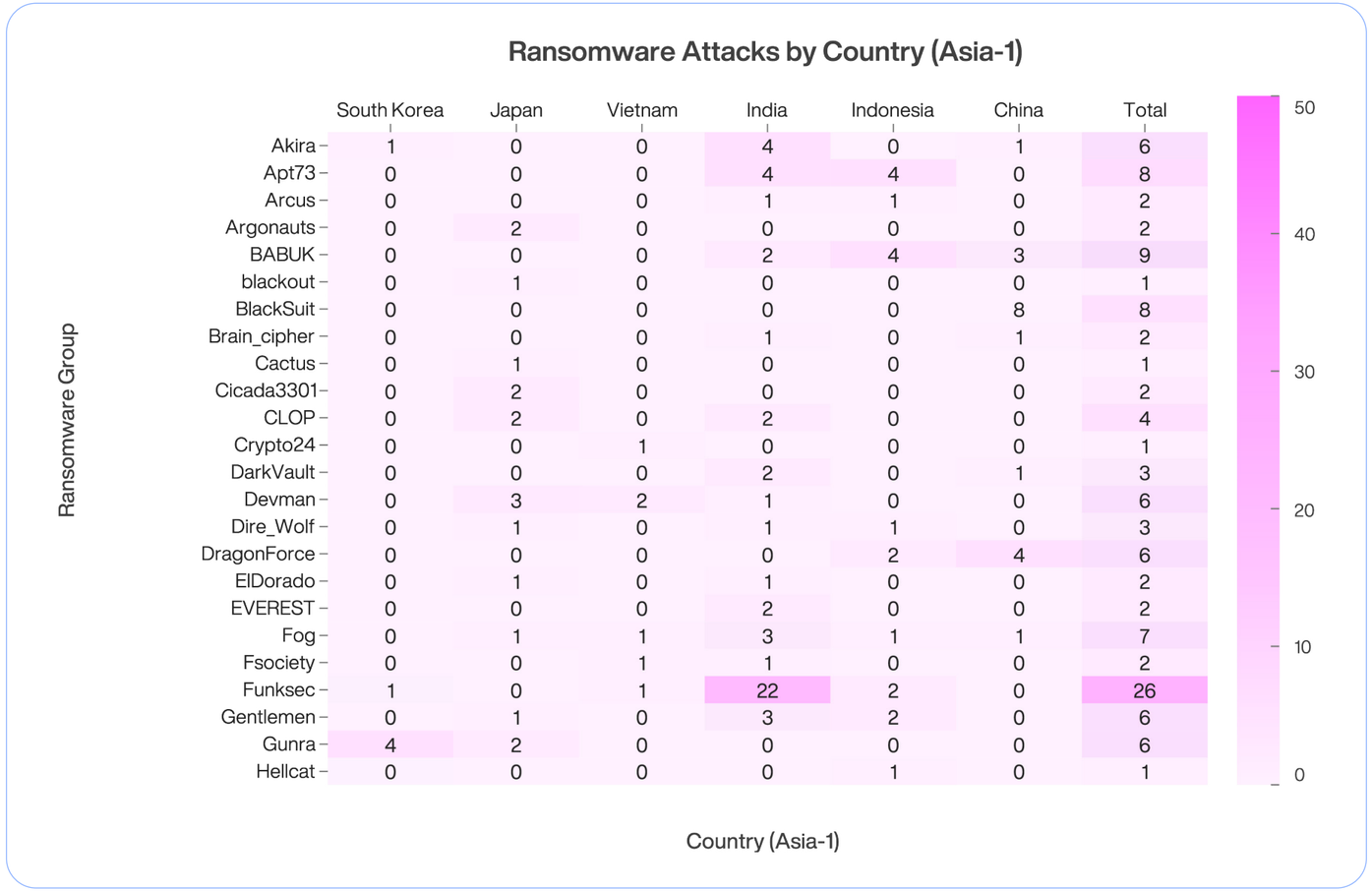
[图] 各国遭受勒索软件攻击的现状 (2024 年 10 月 ~ 2025 年 9 月)

2025年网络威胁趋势

勒索软件趋势 - 主要受害国家：亚洲（1）

2025 年亚洲各国勒索软件受害分析结果显示，**印度超越日本，迅速崛起为主要目标。**此外，台湾、韩国和日本的受害次数处于相似水平。总体事件数量较去年同期急剧增加。

值得注意的是，各国在威胁集中度上存在差异。**韩国和中国表现出集中于少数强大组织的倾向。**相比之下，日本和印度尼西亚则呈现出相对分散型的威胁结构。在这种情况下，需要针对各种攻击组织使用的渗透战术进行防御。



Ransomware Group	South Korea	Japan	Vietnam	India	Indonesia	China	Total
Akira	1	0	0	4	0	1	6
Apt73	0	0	0	4	4	0	8
Arcus	0	0	0	1	1	0	2
Argonauts	0	2	0	0	0	0	2
BABUK	0	0	0	2	4	3	9
blackout	0	1	0	0	0	0	1
BlackSuit	0	0	0	0	0	8	8
Brain_cipher	0	0	0	1	0	1	2
Cactus	0	1	0	0	0	0	1
Cicada3301	0	2	0	0	0	0	2
CLOP	0	2	0	2	0	0	4
Crypto24	0	0	1	0	0	0	1
DarkVault	0	0	0	2	0	1	3
Devman	0	3	2	1	0	0	6
Dire_Wolf	0	1	0	1	1	0	3
DragonForce	0	0	0	0	2	4	6
ElDorado	0	1	0	1	0	0	2
EVEREST	0	0	0	2	0	0	2
Fog	0	1	1	3	1	1	7
Fsociety	0	0	1	1	0	0	2
Funksec	1	0	1	22	2	0	26
Gentlemen	0	1	0	3	2	0	6
Gunra	4	2	0	0	0	0	6
Hellcat	0	0	0	0	1	0	1

[图] 亚洲主要国家勒索软件组织攻击现状 (2024 年 10 月 ~ 2025 年 9 月, 跨页展示 32-33页)

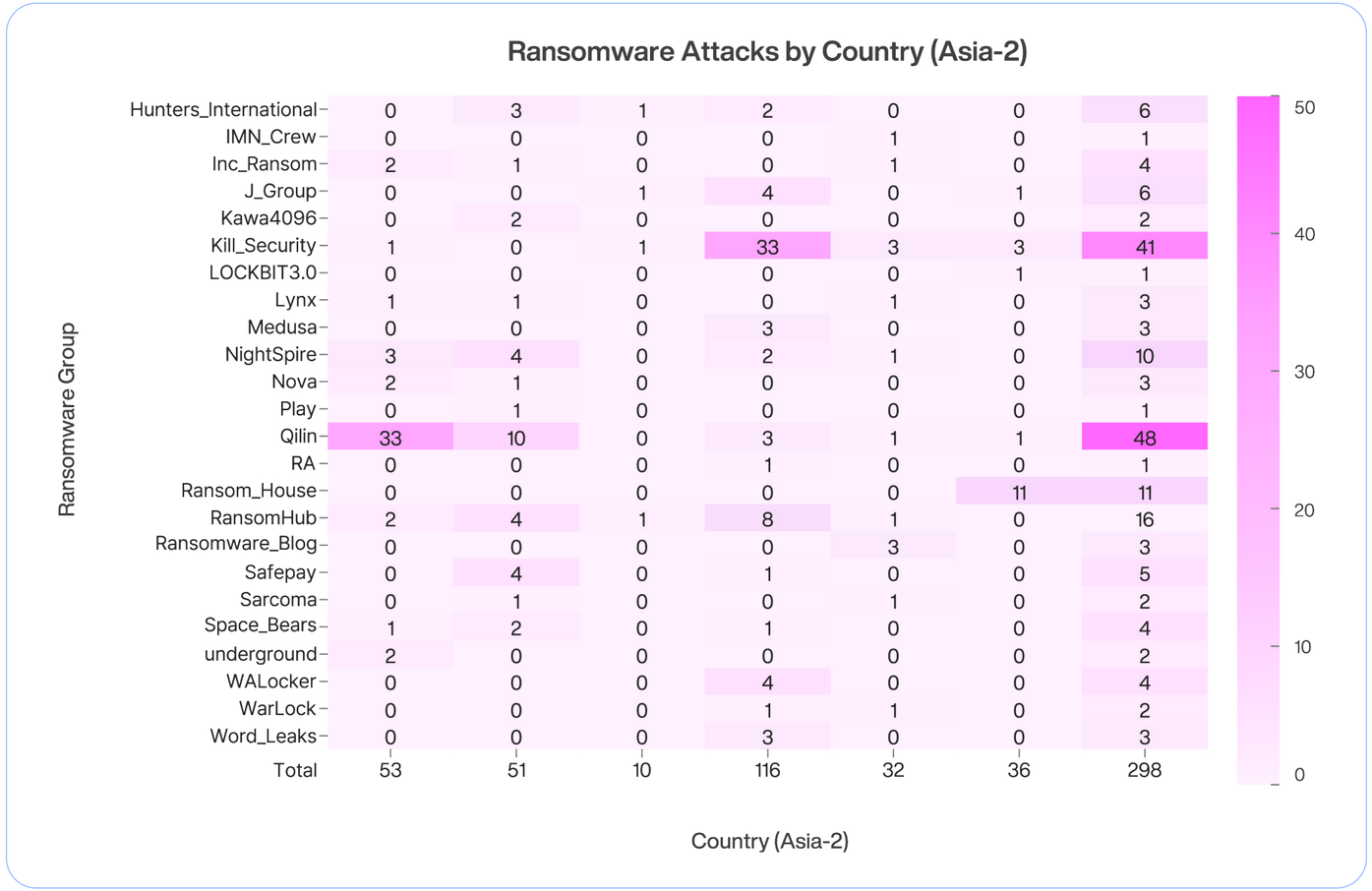
2025年网络威胁趋势

勒索软件趋势 - 主要受害国家：亚洲（2）

从攻击组织的活动来看，**Qilin 是今年在亚洲地区最为活跃的组织。**尤其在韩国和日本确认有集中活动。Qilin 在韩国的活动激增，是因为他们渗透了 IT 服务供应商，并执行了供应链攻击，同时打击了该供应商管理的多个资产管理公司。紧随其后的 Kill_Security 则强烈集中于印度。

2025 年亚洲地区的勒索软件攻击可总结为 ▲ 受害次数增加 ▲ 攻击目标转移 (日本 · 印度) ▲ 各国威胁组织集中度差异。

包括韩国、印度、日本在内的亚洲国家正持续遭受各种攻击，需要持续监控和强化的安全体系。此外，还需迅速反映 RansomHub 瓦解后重组的 Qilin、Kill_Security 等主要攻击组织的战术变化，并制定相应的应对方案。



[图] 亚洲主要国家勒索软件组织攻击现状 (2024 年 10 月 ~ 2025 年 9 月, 跨页展示 32-33页)

2025年网络威胁趋势

主要威胁趋势 - 恶意代码 Top 9

2025 年，报告了多种类型的恶意代码，针对通信、金融和 Linux 基础设施的攻击尤为突出。勒索软件和利用认证结构的恶意代码被积极传播，且传播手法多样化，包括基于 USB 的传播或通过社交媒体广告窃取信息等。
发现与朝鲜 APT 组织相关的新型恶意代码，且现有恶意代码也在持续传播。

1. BPFDoor 恶意代码 针对通信公司的隐秘入侵者

BPFDoor 是一款针对 Linux 系统运行的后门恶意代码。它利用网络过滤技术 BPF 绕过安全设备的监控，隐秘地进入系统内部。

该恶意代码仅在接收到特定数据包时才会激活。它利用多种通信协议接收外部命令，并泄露内部信息。在执行过程中，它伪装成正常的系统进程，并通过复制文件后删除原文件的方式，最大限度地减少痕迹。它试图通过 /dev/shm 路径进行基于内存的执行。

2025 年，在韩国通信公司黑客事件中使用了该恶意代码。尤其是针对用户认证服务器的攻击被报告后，整个行业的安全检查需求被提出。

2. Qilin 勒索软件 针对资产管理公司的双重勒索者

Qilin 是以 RaaS 方式运营的勒索软件。与大多数用 C 语言编写的传统勒索软件不同，**它使用 Rust 语言开发，支持 Windows 和 Linux 环境。**普通勒索软件通常只加密文件一次，但 Qilin 在 Linux 环境下会对同一文件进行三次加密。它还包括删除备份和妨碍恢复的功能。该组织拥有系统化的运营结构，甚至为攻击者提供法律和公关支持。

2025 年，该组织攻击了韩国一家资产管理公司。由于多家资产管理公司共用的电算管理公司云服务器被感染，客户信息和内部文件被泄露到暗网。

3. Gunra 勒索软件 无需谈判的恢复案例

Gunra 勒索软件也以 RaaS 形式运营。据悉，它基于 Conti 勒索软件的源代码制作。它支持 Windows 和 Linux 环境，其特点是通过排除影响操作系统的文件，选择性地加密企业的核心资产，从而最大限度地扩大损害。

2025年，**它接连攻击了金融机构和制造业。**受害企业的内部文件和客户信息被泄露到暗网，引发了整个行业的不安。不过，在 Linux 版本中发现了加密密钥生成方式的结构性缺陷。因此，得以提取解密密钥并恢复了数据。

主要内容（要点）

- BPFDoor 被用于韩国电信公司黑客事件 — 仅在接收特定数据包时激活，泄露内部信息。
- Qilin 勒索软件，使用 Rust 语言开发，支持 Windows 和 Linux 环境 — 攻击了韩国资产管理公司。
- Gunra 勒索软件，攻击多家企业 — Linux 版本加密密钥存在结构性缺陷，可被解密。

2025年网络威胁趋势

主要威胁趋势 - 恶意代码 Top 9

4. Plague 恶意代码 针对 Linux 认证结构

Plague 恶意代码**通过劫持 Linux 系统的登录流程来窃取用户账户信息。**它在系统启动时自动运行，收集用户通过 SSH 或终端登录时输入的 ID 和密码。

Linux 通过名为 PAM 的认证模块来验证登录信息，Plague 恶意代码利用 LD_PRELOAD 技术，设置自身优先于系统本应执行的认证功能运行。

也就是说，当用户登录时，Plague 恶意代码以静默插入的方式窃取信息。它通过删除登录记录和修改系统设置，被配置为重启后仍能持续运行。最近，它进化为增强了检测规避和隐藏功能的形式。

5. 通过 USB 传播的挖矿恶意代码

通过 USB 传播恶意代码在可进行物理访问的环境中仍然是有效的手段。**最近也发生了通过 USB 介质传播加密货币挖矿恶意代码的案例。**

攻击者在被感染的 USB 中隐藏快捷方式 (.lnk) 文件，用户执行该文件后，通过 PowerShell 脚本安装挖矿程序 XMRig。它不仅仅是安装，而是通过直接连接到 PostgreSQL 数据库的方式进行命令收发。它拥有比一般恶意代码更精密的通信结构，允许从外部控制或监控挖矿活动的状态。此外，它通过 GitHub 下载恶意文件，并利用 Windows 注册表的 Run 键设计为重启后自动运行。因此，可以进行持续挖矿。

6. 通过虚假交易所广告传播的信息窃取程序

攻击者在 Facebook 上投放冒充 Binance 等**知名交易所的广告，用户点击后被引导至虚假交易所网站，并被诱导下载 installer.msi 文件。**该文件不会在执行后立即开始恶意行为，仅在受害者不是处于虚拟环境且符合攻击者设定的条件时，才会注册恶意调度程序，随后下载并执行信息窃取程序恶意代码。

仅访问恶意代码传播地址不会导致感染，非目标用户会被重定向到正常网站，从而逃避检测。恶意代码通过 PowerShell 获取额外的有效载荷，并收集系统信息、浏览器存储数据、屏幕截图、Telegram 账户等敏感信息。

主要内容（要点）

- Plague 恶意代码，劫持 Linux 系统的登录流程，窃取用户账户信息。
- 在韩国发生了通过 USB 介质传播加密货币挖矿恶意代码的案例。
- 虚假交易所广告 — 冒充知名交易所的 Facebook 广告 > 引导至虚假交易所网站 > 下载恶意文件。

2025年网络威胁趋势

主要威胁趋势 - 恶意代码 Top 9

7. Proxyware 恶意代码的隐秘渗透如果你的电脑在偷偷共享带宽?

Proxyware 是一种合法程序，用户可以通过共享自己的互联网带宽来获得收益。但近期出现了利用该程序的恶意代码，成为安全威胁。

攻击者**在未经用户同意的情况下安装 Proxyware，使其偷偷共享网络资源。**通过这种方式获取经济利益的 Proxyjacking 已被多次发现。它以与 Mimo 挖矿程序一同传播，或在免费软件安装过程中通过广告页面自动安装的方式被使用。受害者会遭受系统性能和网络速度下降的影响。

Proxyware 持续与外部服务器通信，并根据攻击者设定的方式利用资源，因此很难察觉到已被感染。它类似于 Cryptojacking，但区别在于利用网络带宽而非 CPU，并通过规避杀毒软件检测的方式秘密运行。

8. BeaverTail & Tropidoor 恶意代码 Lazarus 的招聘邮件攻击

BeaverTail 和 Tropidoor 是据称由朝鲜支持的 ‘Lazarus’ 组织使用的恶意代码，通过伪装成招聘的钓鱼邮件传播。攻击者冒用真实公司名义接近开发者或 IT 从业人员。他们通过在邮件中嵌入包含恶意项目的 Bitbucket 链接来尝试感染。

恶意代码 BeaverTail 具有信息窃取程序功能，用于收集浏览器中存储的登录信息和加密货币钱包数据。Tropidoor 是基于内存的后门，通过系统信息收集、命令执行、屏幕截图等多种功能，实现长期入侵。

9.EndRAT，Kimsuky 的新型恶意代码

EndRAT 是据称由朝鲜支持的 ‘Kimsuky’ 组织从 2025 年 7 月开始使用的一款基于 AutoIt 的新型 RAT (远程访问木马) 恶意代码。

EndRAT 包含用于与服务器通信的独特字符串 “endServer9688” 和 “endClient9688”，并以此标识符命名。它通常通过诱导执行 LNK 文件的方式传播。2025 年 9 月，也确认了通过伪装成名为 “Stress Clear” 的程序的 MSI 安装程序进行分发的案例。它基于 AutoIt 脚本制作，在执行条件和通信结构中使用特定字符串的方式，与现有恶意代码有所不同。

主要内容（要点）

- 未经用户同意安装 Proxyware，偷偷共享网络资源的攻击方式。
- Lazarus，接近开发者或 IT 从业人员，传播 BeaverTail 和 Tropidoor 恶意代码。
- Kimsuky 组织，开始使用新型 RAT (远程访问木马) 恶意代码 ‘EndRAT’ 。

2025年网络威胁趋势

主要威胁趋势 - 攻击技术 Top 10

1. 软件供应链攻击

2025 年以来，软件供应链攻击的规模和复杂性有所扩大。**攻击者直接渗透到开源软件包仓库 (如 npm, PyPI)，或篡改流行库和开发工具，通过正常的更新和依赖安装过程广泛传播恶意代码。**此类攻击感染开发和 CI/CD 环境，导致源代码窃取、植入后门和凭证收集。结果是金融、加密货币、云、公共机构等各种行业遭受了连锁损害。特别是，2025 年确认了多起利用正常签名和自动部署体系的供应链攻击。

2. 凭证窃取及 MFA 绕过 (T1078)

2024 年下半年以来，通过鱼叉式网络钓鱼和信息泄露进行的凭证窃取急剧增加。攻击者**获取有效账户，渗透 VPN、SSO、云环境，并利用 EvilProxy 等基于代理的中间人认证攻击工具绕过 MFA，**或反复向用户终端发送大量认证请求，诱导用户错误批准。APT29、Scattered Spider 等组织成功利用该技术实现了长期潜伏和内网据点扩展。

3.云环境入侵与回迁 (Cloud Repatriation)

云回迁（Cloud Repatriation）是一种将核心数据或工作负载迁回本地，以实现成本优化、性能提升和合规应对的策略。然而，由于 CSP 缺乏安全功能，可能伴随安全配置遗漏、配置错误等风险。尤其在云环境中，OAuth 令牌窃取、凭证滥用导致的横向移动、权限扩展等入侵事件不断增加。因此，在回迁过程中，需要强化认证、权限和可视性，并重新制定安全策略。

4. AI and LLM-Powered Attack

攻击者**利用 AI 和大型语言模型 (LLM) 实现恶意代码自动生成、规避检测、制作复杂的网络钓鱼文案和深度伪造（Deepfake）内容等自动化操作。**结果，攻击的准确性和效率显著提升，传统的威胁检测技术越来越难以阻止此类攻击。此外，攻击者借助自动化工具快速设计并发起大规模定向攻击，防御方的响应时间进一步缩短。随着这一趋势，基于 AI 的攻击预计将更加多样化并持续升级。

2025年 攻击技术 Top 10

1. 软件供应链攻击
2. 凭证窃取及 MFA 绕过
3. 云环境入侵与回迁
4. AI/LLM 驱动的攻击升级
5. 远程访问和边界安全渗透
6. MoTW 绕过与压缩格式滥用
7. Web 服务和云滥用
8. 鱼叉式网络钓鱼附件利用
9. DLL 搜索顺序劫持
10. 操作系统内置工具滥用 – LOTL

2025年网络威胁趋势

主要威胁趋势 - 攻击技术 Top 10

5. 远程访问和边界安全渗透 (T1133)

利用 RDP、VPN、VDI 等外部远程访问服务的渗透尝试正在增加。特别是位于网络边界的防火墙、VPN 等的漏洞成为主要的入口点。攻击者通过暴露的端口、脆弱的凭证和认证配置执行初始入侵。随后，通过窃取 SSO 会话和绕过认证进行内部网络的横向移动。Ivanti、Fortinet、Cisco ASA、Palo Alto Networks 设备的零日漏洞被用作 APT 攻击的主要攻击载体，并报告了多起绕过认证和进入内部网络的案例。

6. MoTW 绕过与压缩格式滥用 (T1553.005)

攻击者**持续利用绕过 Windows 安全功能 MoTW（网页标记）的攻击手法。**MoTW 会为从互联网下载的文件添加 Zone.Identifier 元数据，以便通过 SmartScreen 和 Office 保护功能进行验证。攻击者利用 ISO、ZIP 等压缩格式，使 MoTW 无法传递到内部文件，或通过篡改 LNK 文件结构以及利用 7-ZIP 漏洞（CVE-2025-0411）来移除 MoTW，从而在无警告的情况下执行恶意文件。

7. Web 服务和云滥用 (T1071.001)

攻击者**为规避检测，利用 GitHub、Dropbox、Google Drive、Telegram 等正常 Web 服务和云平台进行 C2 通信。**网络流量被伪装成普通用户活动，难以被防火墙或 IDS 识别。2024 年，CloudSorcerer 攻击组织曾在 GitHub 上隐藏加密命令，并通过 Microsoft Graph API 和 Yandex Cloud 与受害系统进行通信。Gamaredon, Kimsuky, PteroBox 等 APT 组织也利用了该技术。

8. 鱼叉式网络钓鱼附件滥用 (T1566.001)

自 2024 年下半年以来，攻击者**主要采用基于社会工程学的鱼叉式钓鱼作为渗透手段。**LNK、CHM、ZIP/RAR 文件仍被频繁使用。近期还出现通过恶意 URL 和二维码替代附件的方式。此外，攻击者还利用 ClickFix 技术诱导用户点击、输入认证信息并安装恶意文件。根据 CrowdStrike 和 Microsoft 的案例，此类 ClickFix 型攻击被用作内网访问和窃取凭证的主要途径。

9. DLL 搜索顺序劫持 (T1574.001) DLL 侧加载 (T1574.002)

DLL 搜索顺序劫持**是一种通过操纵程序加载 DLL 时的 Windows 搜索顺序，使攻击者创建的恶意 DLL 代替正常 DLL 被加载的攻击技术。**它被滥用于权限提升、远程代码执行和确保持久性。实际上，它被用于与 ShadowPad 相关的勒索软件活动和 NI LabVIEW 的未受控搜索路径漏洞 (CVE-2025-2630) 等。攻击者通常将恶意 DLL 放置在易受攻击的路径上或操纵安装/更新进程的行为，以长期规避检测并维持权限。

10. 操作系统内置工具滥用 – LOTL (T1059)

攻击者**使用 LOTL (利用现有资源) 技术，利用 PowerShell、WMI、rundll32、mshta 等 Windows 正常文件，最大限度地减少恶意代码痕迹。**该技术规避杀毒软件、EDR 等防御体系，并将恶意行为隐藏在正常进程中。根据 Microsoft 的调查，Volt Typhoon 等中国背景的 APT 组织在针对美国国防、通信、能源基础设施的渗透中，使用 wmic、netsh、PowerShell 等工具进行权限获取、凭证收集、内网侦察。

2025年网络威胁趋势

主要威胁趋势 - 漏洞 Top 10

1. Ivanti Connect Secure VPN (CVE-2024-21887, CVE-2025-22457)

APT 组织在初始渗透中利用防火墙、SSL VPN 等网络安全产品漏洞的案例越来越多。特别是 Ivanti Connect Secure VPN 的认证绕过漏洞 (CVE-2023-46805) 和命令注入漏洞 (CVE-2024-21887) 至今仍是攻击者的主要目标。2025 年 4 月公开的缓冲区溢出导致远程代码执行漏洞（CVE-2025-22457）被确认由 APT 组织 UNC5221 使用。攻击者通过漏洞投放 WebShell 和后门，渗透政府机构及金融企业。

2. FortiOS and FortiProxy (CVE-2025-24472)

2025 年初，FortiOS 和 FortiProxy 的认证绕过漏洞 (CVE-2025-24472) 被披露。**攻击者利用该漏洞获取超级管理员 (Super Admin) 权限，从而可以控制整个网络。**报告了在初始渗透阶段利用该漏洞的案例，大型企业和金融机构遭受了严重损失。漏洞 PoC 公开后，攻击尝试急剧增加。

3. PAN-OS and GlobalProtect (CVE-2024-0012)

在 Palo Alto Networks 的 PAN-OS 管理 Web UI 中，认证绕过漏洞（CVE-2024-0012、CVE-2025-0108）与权限提升漏洞（CVE-2024-9474）及认证后文件读取漏洞（CVE-2025-0111）**被链式利用，导致管理员或 root 权限控制、配置篡改及敏感信息访问。**GlobalProtect 方面，CVE-2024-3400 零日漏洞是典型案例，已确认攻击者建立远程 Shell 并进行内部网络横向移动。对此，美国卫生与公众服务部（HHS）下属安全团队 HC3 将医疗保健行业列为主要攻击目标行业。

4. Cisco ASA and Firepower (CVE-2025-20333, CVE-2025-20362)

在 Cisco ASA 和 Firepower 设备中发现了与 ArcaneDoor 系列活动相关的零日和 N 日漏洞。CVE-2025-20333 允许通过 VPN Web 服务器漏洞实现远程代码执行。CVE-2025-20362 允许在未认证的情况下访问受限 URL。这两个漏洞在实际攻击中被链式利用。美国 CISA 要求联邦机构进行资产识别、取证收集、快速缓解并应用补丁。Cisco 还确认了通过 ROMMON 和引导链篡改实现持久化的战术。

2025年 漏洞 Top 10

1. Ivanti Connect Secure VPN
2. Fortinet – FortiOS/FortiProxy
3. Palo Alto - 防火墙/GlobalProtect
4. Cisco ASA/Firepower
5. 文件传输解决方案
   （如 MOVEit、Cleo）
6. Sitecore RCE
7. 网页浏览器零日漏洞
8. Android 权限提升
9. 压缩程序
10. 开源软件供应链

2025年网络威胁趋势

主要威胁趋势 - 漏洞 Top 10

5. 文件传输解决方案漏洞（如 MOVEit、Cleo 等）

Cleo Harmony, VLTrader 等 MFT 产品中确认了远程代码执行和认证绕过漏洞。CLOP 勒索软件利用这些漏洞对多个组织造成了损害。其中，CVE-2024-50623 通过利用无限制的文件上传和下载功能来执行远程代码。CVE-2024-55956 则利用了 Autorun 目录设置漏洞，允许在未经身份验证的情况下执行命令。此外，MOVEit Transfer 的 CVE-2024-5806 漏洞由于 SFTP 身份验证处理问题，导致可以绕过身份验证。这进一步导致了 Safe Wallet 前端资产受损及资金被盗。美国联邦调查局（FBI）指出，此活动与朝鲜攻击组织 TraderTraitor 有关。

6. Sitecore RCE (CVE-2025-534690)

Sitecore 的 ViewState 反序列化漏洞（CVE-2025-534690）允许攻击者在无需身份验证的情况下执行远程代码（RCE）。据分析，攻击的起因是旧版部署指南中提供的示例 machineKey 被重复使用。该漏洞的利用迹象自 2024 年底起便被观测到，正式安全公告于 2025 年 9 月发布。攻击者通过暴露在互联网上的 Sitecore 实例获取初始访问权限，随后安装远程 Shell，进行系统和域侦察、收集凭证和内部横向移动。随后窃取了配置和秘密密钥等敏感信息。

7. 浏览器零日漏洞 (Chrome: CVE-2024-4947, Firefox CVE-2024-9680)

在 Web 浏览器中发现的零日漏洞（Zero-day Vulnerability）已被用于实际攻击。Chrome V8 引擎漏洞（CVE-2024-4947）**仅需访问精心制作的网页即可执行代码，拉撒路（Lazarus）系列攻击组织曾利用该漏洞针对金融领域发起攻击。**Firefox 的释放后使用（Use-After-Free, CVE-2024-9680）漏洞则被俄罗斯 APT 组织 RomCom 利用，在针对欧洲和北美的间谍行动中安装后门。这些漏洞的共同特点是：通过窃取凭据、执行载荷（Payload）以及确保持久性来完成整个攻击流程。

主要内容（要点）

- Cleo Harmony、VLTrader 等 MFT 产品中确认了远程代码执行和认证绕过漏洞。
- Sitecore 的 ViewState 反序列化漏洞 (CVE-2025-534690$) 的原因是重复使用了旧的 machineKey。
- Chrome V8 引擎漏洞 (CVE-2024-4947) 仅通过访问网页即可执行代码，并被 Lazarus 用于攻击。

2025年网络威胁趋势

主要威胁趋势 - 漏洞 Top 10

8. 安卓权限提升漏洞
(Android CVE-2025-38352)

Android CVE-2025-38352 被用于通过本地权限提升来扩大恶意应用的设备权限。特别是，观察到它在整个攻击流程中与网页浏览器零日漏洞结合，在初始控制设备后进行凭证窃取和执行额外有效载荷。恶意应用可以扩大权限，进行系统设置更改、访问敏感数据、禁用安全功能。在针对移动用户的目标攻击中，存在被用于窃取金融信息或间谍活动的风险。

9. 压缩程序漏洞
(CVE-2025-0411, CVE-2025-8088)

攻击者也将压缩程序用作攻击手段。在此背景下，**已确认多起利用在个人和企业环境中广泛使用的 7-Zip 和 WinRAR 漏洞的攻击案例。**7-Zip 的 MoTW 绕过漏洞 (CVE-2025-0411) 被俄罗斯攻击组织用于向乌克兰政府机构和民间组织分发 SmokeLoader 恶意软件。在 WinRAR 中发现了路径遍历 (Path Traversal) 漏洞 (CVE-2025-6128, CVE-2025-8088)。特别是 CVE-2025-8088，据报道已被攻击组织 RomCom 用于攻击欧洲和加拿大的物流、制造、金融及国防企业。

10. 开源软件供应链漏洞
(例如: npm package)

在 JavaScript npm 包等**广泛使用的开源库中，接连发生了结合维护人员账户窃取和恶意代码注入的供应链攻击。**2025 年 9 月，npm 因维护人员钓鱼和令牌窃取导致多个流行软件包被污染。同期，PyPI 正式警告针对开发者的邮件钓鱼活动，并公布了账户窃取风险。在容器领域，确认了大量包含 XZ 后门的 Docker Hub 镜像仍然存在，供应链暴露持续发生。此外，在 Rust 生态系统中也发现了窃取钱包密钥的恶意 crate 并被立即删除。

主要内容（要点）

- Android CVE-2025-38352 被用于通过本地权限提升来扩大恶意应用的设备权限。
- 确认了攻击者利用 7-Zip 和 WinRAR 漏洞的攻击案例。
- 在广泛使用的开源库中，接连发生了结合账户窃取和恶意代码注入的供应链攻击。

2025年网络威胁趋势

主要威胁趋势 - 移动 Top 6

1. 基于社会工程学技术的移动端犯罪升级

2025 年，利用社会工程学技术的移动端犯罪进一步升级。其特点是制作和分发时反映了传播当时的社会热点问题。**移动端社会工程学技术，利用冒充电信公司、AI 应用、公共机构等吸引受害者注意的伪装应用。**此外，还发现了多款诈骗应用 (Scam App)，它们假借飙升股、首次公开募股 (IPO) 投资或情侣关系来建立亲密感，随后诱导投资。这些应用以保证高收益为名目迷惑受害者，并要求安装恶意应用。

受害者存入投资金后，通过应用查看实时伪造的收益率。出现多起在要求提现时，以各种理由拒绝返还投资金并潜逃的案例。此外，还持续发现裸聊诈骗案例，即以可以进行私密对话为名诱导安装应用，随后窃取受害者的联系人信息和照片，并以此威胁传播，索要资金。

2. 搭载新攻击功能的恶意应用

利用安卓 HCE (主机卡模拟) 劫持 NFC 通信技术的恶意应用正在升级。名为 NGate 的应用除了劫持 NFC 通信功能外，还包含显示虚假屏幕窃取用户凭证信息的功能。

这些应用会在与基于 NFC 的设备接触时，将产生的通信信息发送给攻击者。攻击者基于 NFC 通信信息进行ATM 非法提款等活动。还新发现了利用 OCR (光学字符识别) 库窃取加密货币信息的恶意应用。该应用利用了用户为备份加密货币钱包而将助记词 (Mnemonic) 相关信息以图片形式存储的特点。攻击者利用 OCR 技术，自动分析、提取并窃取图片中包含的助记词和加密货币相关信息。

3. 官方商店内恶意应用类型多样化

官方应用商店也持续发现多种类型的恶意应用。最近发现了金融信息窃取 (Banker)、高息贷款 (SpyLoan)、加密货币信息窃取 (SparkCat, SparkKitty)、隐藏广告执行 (HiddenAds)、投资诈骗 (ScamFX) 等多种应用。

特别是 Banker 类型的应用，由于包含恶意功能时被应用商店安全检查检测到的可能性高，因此**已进化为伪装成正常应用注册后安装，再从外部下载恶意有效载荷执行的方式。**某些恶意应用经常智能地运行，例如根据用户环境有条件地激活恶意功能，或仅在特定国家和语言设置下执行恶意行为。

主要内容（要点）

- 移动端社会工程学技术，利用冒充电信公司、AI 应用、公共机构等吸引受害者注意的伪装应用。
- 出现了利用安卓 HCE (主机卡模拟) 劫持 NFC 通信的恶意应用
- 进化为以正常应用注册到应用商店后，再从外部下载恶意有效载荷执行的方式。

2025年网络威胁趋势

主要威胁趋势 - 移动 Top 6

4. 利用多种漏洞的攻击

除了**已公开的 远程代码执行 (RCE) 和 权限提升 (EoP) 等 CVE 漏洞外，利用未公开漏洞的攻击也在持续被发现。**由于这些漏洞在报告前不为人所知，攻击者将其用作“零日漏洞 (Zero-Day)”来制作和传播恶意应用。在安全补丁发布之前，受害者可能处于毫无防御的状态。

典型的有 Pixnapping 漏洞。利用该漏洞，在 Android 13~16 版本的特定终端设备上，可以利用半透明覆盖和精确时序来提取像素数据。通过这种方式窃取 MFA 认证码等敏感信息。CVE-2024-43093 漏洞是一个利用 ContactsDirectory 的权限提升漏洞，允许在无需用户交互的情况下自动运行应用程序。攻击者可以借此在用户不知情的情况下运行恶意应用或在后台激活恶意功能。事实上，已经发现了具备此类功能的恶意应用案例。

5. 朝鲜关联的网络攻击组织活动

与朝鲜有关联的攻击组织正持续针对韩国分发用于窃取敏感信息的间谍应用 (Spyware)。**这些应用主要伪装成文件管理器、软件更新、安全文档查看器等实用程序，**以规避用户的怀疑，并精心地设计了 UI（用户界面） 和功能，使其看起来与正常应用无异。

此外，为了干扰安全分析，攻击者采用了代码混淆、加密、动态加载、条件执行等多种技术。应用还包含通过 C2 服务器（控制服务器） 接收指令并将窃取的信息发送至外部的功能。在部分恶意应用的 C2 服务器中，甚至还发现了虚拟货币钓鱼网站。这表明其攻击范围已扩展至窃取加密货币等相关资产。

6. 预装恶意代码的设备传播

最近，发现了一些基于 Android OS 的智能手机、机顶盒 (set-top box) 等**设备在制造商出厂前就被预装了恶意代码进行流通的案例。**这些设备以低于正常产品的价格来迷惑消费者。设备内部包含执行 DDoS 或撞库攻击的 Mirai 恶意代码，以及以广告收益为目标的 HiddenAds 类型恶意代码。恶意代码在用户不知情的情况下长期运行。可能导致网络流量增加、电池消耗、个人信息泄露等损害。

此外，通过 USB 线缆进行的黑客攻击案例也持续被报告。线缆内部包含滥用数据传输功能的恶意芯片，设计用于在连接设备上实现文件访问、命令执行和信息窃取等功能。

主要内容（要点）

- 除了已公开的 CVE 外，持续发现利用未注册的未公开漏洞的移动端攻击。
- 朝鲜关联组织 - 主要伪装成文件管理器、软件更新、安全文档查看器等实用工具应用。
- 发现智能手机、机顶盒等部分设备在制造商出厂前就被预装了恶意代码进行流通的案例。

2025年网络威胁趋势

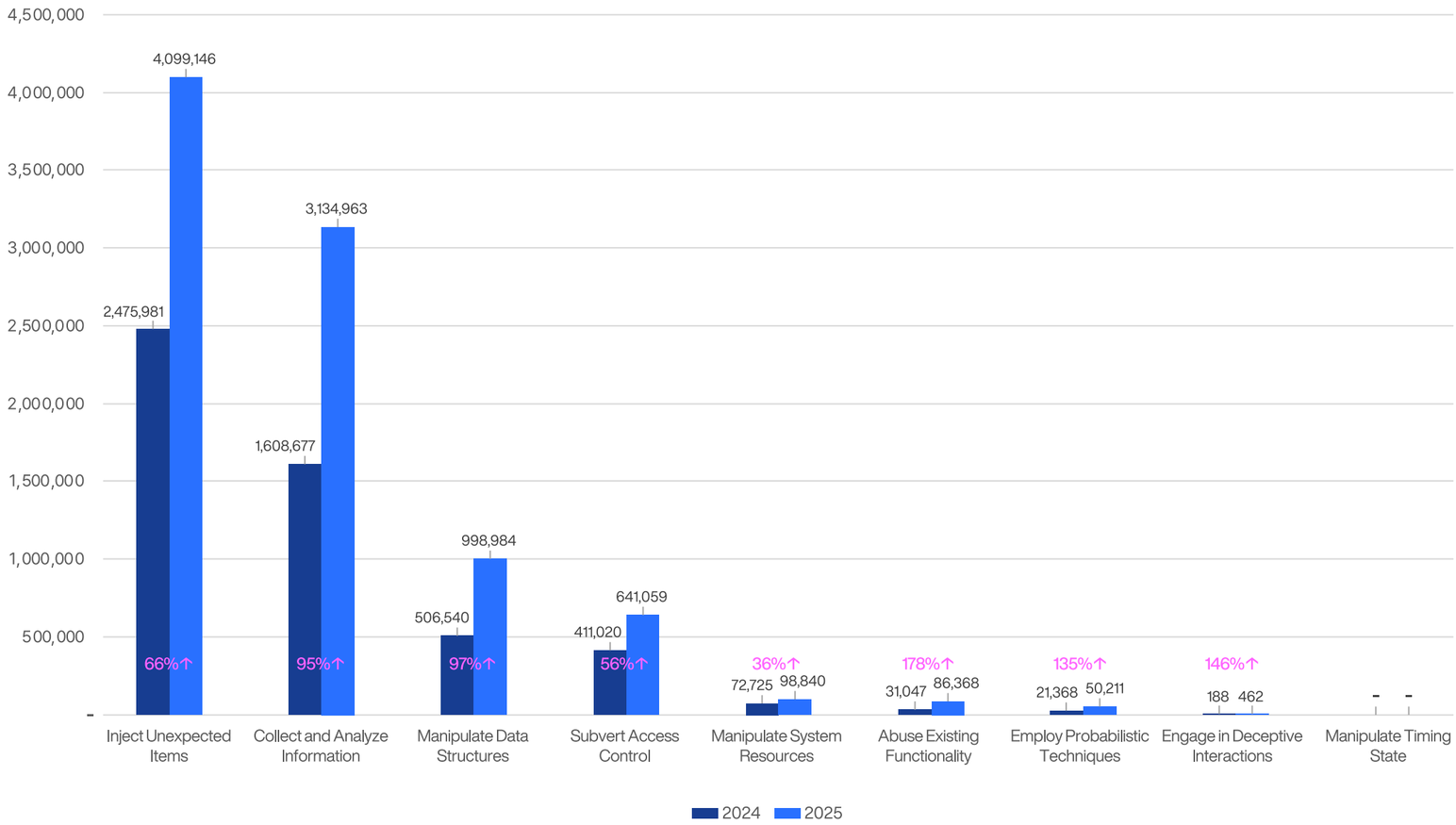
攻击类型统计

AhnLab 的入侵响应专业团队 CERT (Computer Emergency Response Team) 每月都会发布分析网络威胁趋势的《CERT 月报》。以下是基于该报告整理的 2025 年网络攻击类型统计数据。

2025 年，**攻击检测总数较去年增加了 78%。**所有类型的攻击均较去年呈现两位数以上的增长，部分类型的增幅甚至超过了 100%。据分析，这是由于 AI 驱动的攻击高级化、云环境扩大以及利用供应链漏洞等多种因素综合作用的结果。

发生次数最多的攻击类型是注入意外项 (Inject Unexpected Items)，继 2024 年之后再次位居第一。紧随其后的是信息收集与分析 (Collect and Analyze Information)、数据结构操纵 (Manipulate Data Structures)、访问控制篡改 (Subvert Access Control)、系统资源操纵 (Manipulate System Resources)。

2025 年攻击类型排名



2025年网络威胁趋势

攻击类型统计 - 类型说明

1. 注入意外项目（Inject Unexpected Items）

攻击者通过系统的输入接口注入异常或异常的数据，从而控制或干扰系统运行。此类攻击通常发生在输入验证不足或处理逻辑薄弱的情况下。系统可能因注入值而出现运行异常、绕过安全策略或泄露信息。

2. 收集与分析信息（Collect and Analyze Information）

攻击者通过主动查询或被动观察获取并分析目标系统信息。通过收集系统配置、用户账户等详细信息，攻击者可以设计后续攻击路径或识别潜在漏洞。此过程通常作为初始渗透的准备阶段。

3. 篡改数据结构（Manipulate Data Structures）

攻击者**蓄意修改系统内部数据结构，破坏正常的数据处理流程。**通过干扰或篡改内部数据流，诱导系统产生异常结果。这种操纵不仅会导致意外错误，还会损害数据的可靠性。

4. 破坏访问控制（Subvert Access Control）

攻击者**绕过或使访问控制机制失效，从而获取未授权的权限并非法访问系统。**通过这种方式，攻击者可以获得管理员或高级用户权限，进而访问敏感数据或操纵特定功能。

5. 篡改系统资源（Manipulate System Resources）

该方式旨在**过度消耗受害者的 CPU、内存等系统资源，导致性能下降或资源耗尽。**这使得系统难以提供正常服务，用户会感到响应速度变慢甚至系统停机。从长远来看，资源耗尽会造成类似于拒绝服务（DoS）的攻击效果，损害系统可用性。

6. 滥用现有功能（Abuse Existing Functionality）

攻击者**利用系统或应用程序的正常功能引发危害。**其特点是不添加新代码，而是恶意利用现有功能。 例如，利用客服系统的文件上传功能分发恶意文件，或利用搜索功能泄露内部信息。

7. 采用概率技术（Employ Probabilistic Techniques）

攻击者**通过概率性方法探索系统漏洞或逐渐提高攻击成功率。**代表性技术包括暴力破解（Brute Force）和计时攻击。通过猜测密码等手段，成功率随时间推移而增加。此类攻击对加密体系和身份验证程序薄弱的系统非常有效，往往在用户未察觉的情况下入侵。

8. 进行欺骗性交互（Engage in Deceptive Interactions）

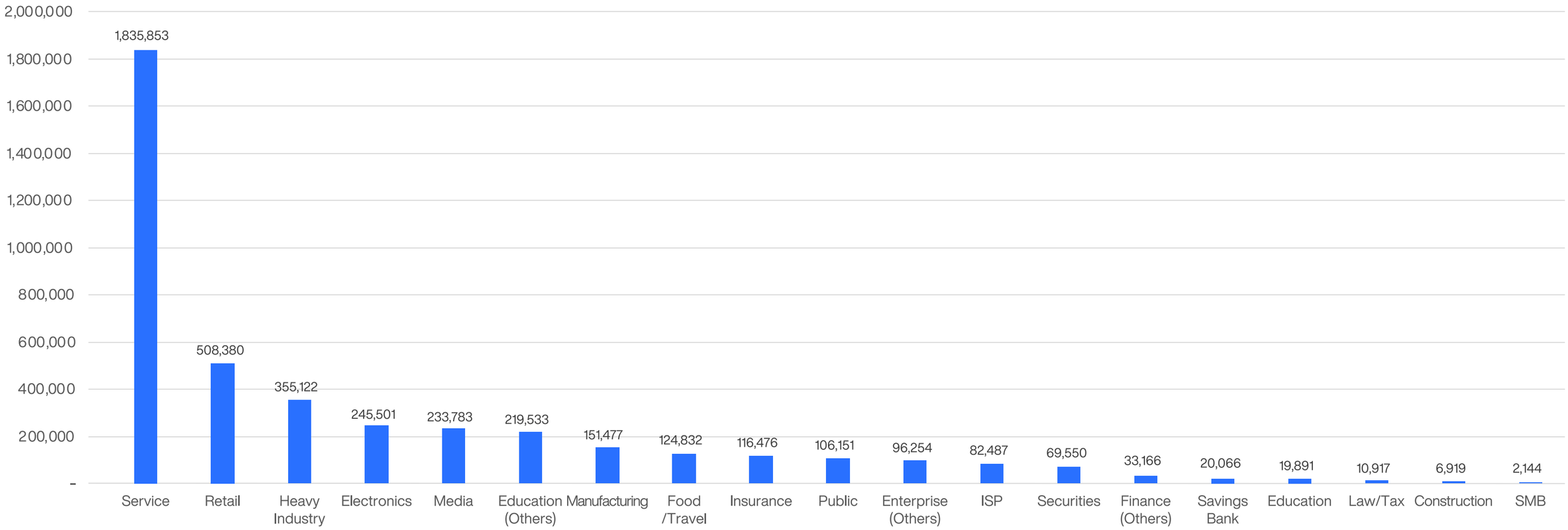
攻击者**在与系统或用户交互时，隐藏身份和真实意图，传递错误信息以获得所需结果。**代表性手段包括网络钓鱼、社会工程学、以及利用假冒网站和电子邮件进行的诈骗。此类方式通过欺骗用户获取信任，随后诱导其输入敏感信息或下载恶意文件。

2025年网络威胁趋势

攻击类型统计 - 各行业攻击次数

从 2025 年下半年的各行业攻击次数来看，服务业以 1,835,853 次位居首位。其后依次是零售业 (508,380次)、重工业 (355,122次) 以及电子/半导体行业 (245,501次)。

2025 年下半年各行业攻击次数



2025年网络威胁趋势

攻击类型统计 - 各行业攻击类型

2025 年下半年各行业攻击类型比例

	Inject Unexpected Items	Collect and Analyze Information	Manipulate Data Structures	Subvert Access Control	Manipulate System Resource
Service	43%	33%	12%	9%	1%
Retail	37%	50%	7%	3%	1%
Heavy Industry	51%	34%	8%	3%	1%
Electronics	48%	14%	20%	12%	1%
Media	38%	40%	9%	10%	2%
Education (Others)	28%	62%	6%	3%	1%
Manufacturing	48%	37%	11%	2%	1%
Food/Travel	41%	48%	6%	5%	0%
Insurance	30%	62%	4%	4%	0%
Public	40%	45%	7%	5%	1%
Enterprise (Others)	50%	41%	6%	2%	0%
ISP	38%	53%	6%	3%	0%
Securities	53%	30%	9%	3%	4%
Finance (Others)	44%	39%	12%	3%	1%
Savings Bank	41%	36%	10%	8%	0%
Education	49%	42%	6%	3%	1%
Law/Tax	50%	29%	13%	6%	0%
Construction	35%	51%	8%	4%	1%
SMB	80%	1%	9%	3%	0.0%

2026年展望

→ 2026年五大趋势展望

1. AI 驱动的网络攻击全面扩散
2. 勒索软件攻击扩大及受害加深
3. 利用开源生态系统的供应链攻击
4. 对国家核心基础设施的威胁扩大
5. 持续增加的 Linux 威胁

2026年展望

1. AI 驱动的网络攻击全面扩散

→ 深入了解 AhnLab AI 安全战略

利用 AI 的“定制化”攻击

2026 年，AI 能够实时分析受害者环境并生成精准打击目标的恶意代码，这种自适应攻击 (Adaptive Attack) 将进一步扩大。特别是 AI 能够生成多种变体代码以规避检测，从而绕过现有的安全系统。因此，超越以静态检测为中心的安全防御，动态分析和基于行为的检测的重要性将更加凸显。

此外，随着深度伪装 (Deepfake) 技术的高级化，精细模仿真实人物声音或面部的实时钓鱼攻击将滥用于视频会议或电话通话。随着深度伪装质量的不断提高，利用特定人物声音窃取金融信息等敏感数据的攻击，将进化到受害者难以辨别的水平。

利用 AI 的诈骗自动化也值得关注。预计攻击者将大量生成虚假投资网站、聊天机器人、购物中心等，并与受害者自然地进行交互。目前，攻击者已能利用 AI 制作肉眼难以区分的钓鱼网站和电子邮件，这种自动化和量产能力将直接导致攻击活动的爆发式增长。

除此之外，AI 也将大大助力攻击者开发新的黑客技术。通过漏洞检测和模式分析，AI 可能发现未知的安全漏洞，并将其用于零日（Zero-Day）攻击。最终，攻击者对 AI 的利用将降低黑客攻击的门槛，同时提高攻击的频率和准确性。

针对 AI 本身的攻击扩大

以 AI 模型本身为攻击目标的攻击技术也将进一步发展。主要的攻击手法包括：▲提示词注入 (Prompt Injection) 及数据投毒 (Data Poisoning)、▲提示词泄露 (Prompt Leaking) 以及▲模型逆向工程等。攻击者向聊天机器人、自动分析系统或安全 AI 注入恶意输入，或操纵训练数据，诱导其产生预期的误操作或信息泄露。这将对使用 AI 的系统及基于 AI 的安全解决方案的可靠性和完整性构成根本性威胁。

攻击者通过提示词泄露获取 AI 的 Prompt。如果提示词通过 GitHub 等代码共享平台泄露，攻击者可能利用其歪曲 AI 的输出。随着 AI 模型使用的增加，提示词泄露及相关的数据安全防护将备受关注。

攻击者通过对 AI 模型进行重复查询来分析其运行方式，并开展窃取训练数据的逆向工程。这种方式基于模型的响应来掌握训练数据和内部结构，从而泄露敏感信息。攻击者将针对存在安全漏洞的 AI 模型进行逆向分析，以扩大攻击范围。

主要内容（要点）

- AI 驱动的恶意代码、深度伪造、诈骗自动化、零日漏洞发现等定制化攻击增加。
- 随着 AI 模型使用量的增加，针对 AI 的攻击技术，如提示词注入、提示词泄露、模型逆向分析等也将升级。

2026年展望

2. 勒索软件攻击扩大及受害加深

→ 深入了解 AhnLab 的勒索软件综合安全战略

勒索软件组织碎片化及卡特尔化加速

2025 年，LockBit、RansomHub 等大型勒索软件组织的势力有所减弱或停止活动。然而，这并不意味着勒索软件生态系统本身的削弱。**作为大型组织缩减的反作用，Akira、Qilin、Play、Gunra 等大量小型及新兴组织如雨后春笋般出现。**正如在 2025 年趋势中所观察到的，这些新兴组织正活跃地发起攻击，预计这种重组后的勒索软件生态系统将在 2026 年持续存在。

APT 组织与勒索软件组织之间的合作以及基于 RaaS 的“勒索软件卡特尔化”预计将在 2026 年进一步加深。中央平台提供攻击所需的基础设施和工具，附属组织执行攻击后以 “80 比 20” 的比例分配收益的模式在勒索软件生态系统中已基本确立。此外，**随着 2026 年地缘政治冲突的加剧，APT 组织与勒索软件组织之间的合作将比 2025 年更加活跃。**

对于防御者而言，由于黑客攻击门槛降低，攻击者能够发起更多样、更频繁的攻击，安全防御的难度也将随之提升。特别是随着生态系统的碎片化和频繁协作，归因分析（特定攻击组织） 将变得更加困难。

针对中小企业的攻击增加

2025 年勒索软件趋势的主要特点是门槛降低和攻击多样化。对于以获取金钱利益为首要目标的攻击者来说，攻击一次就能获得更大收益的大企业是合理的，2026 年大企业仍将是勒索软件组织的主要目标。

然而，**在当前可以更容易地进行各种攻击的情况下，预计针对安全态势相对薄弱的中小企业的攻击将更快速地增加。**特别是，攻击者可以制造新型和变种的勒索软件持续攻击，针对难以构建系统化多层安全的中小企业的攻击成功率很可能会提高。

事实上，2025 年也捕捉到攻击者将主要目标转向中型企业而非大企业的战略转变。规模较小的企业需要格外警惕精密的定向攻击、内部人员收买以及社会工程学手段。此外，企业必须意识到类似攻击随时可能再次发生，并应建立能够预先识别并预防威胁的安全体系。

主要内容（要点）

- 勒索软件行业已成为犯罪分子的盈利模式，预计攻击将持续增加，尽管勒索软件名称可能会变。
- 勒索软件攻击将从系统内文件加密，扩展到针对数据库、备份解决方案、虚拟化环境等的精确攻击。
- 随着勒索软件攻击门槛的降低，预计针对安全态势薄弱的中小企业的攻击将增加。

2026年展望

3. 利用开源生态系统的供应链攻击

→ 深入了解 AhnLab 利用 XDR 和 ZTNA 构建的供应链安全战略

开源生态系统威胁扩大

2025 年，针对开源软件包注册中心的供应链攻击急剧增加。恶意软件库大规模扩散，并确认了多起开发者及 CI/CD 环境密码与令牌（Token）泄露的案例。考虑到现代软件开发中 90% 以上都依赖开源组件，单一软件包的受损可能导致数千个下游项目产生连锁受损。

预计 2026 年此类威胁将进一步加剧。特别是，**特别是攻击者在安装阶段或 CI 流水线中收集敏感信息以诱导连锁感染的手段将更加精细化。**拼写错误盗用 (Typosquatting)、接管合法软件包维护者账号、依赖项混淆攻击 (Dependency Confusion) 等多种手段可能会被综合利用。

对于遭受此类供应链攻击的企业来说，**实时监控开源使用情况和总体数据流，确保整个开源流水线的可见性是首要任务。**通过这样做，可以在漏洞发生时立即响应，最大限度地减少损失，并具备恢复能力。

从软件到云端及硬件

2025 年的供应链攻击展现了从软件扩展到云服务、MSP（管理服务提供商）、安全解决方案供应商的趋势。例如，攻击组织 DragonForce 和 Scattered Spider 曾攻击云 MSP，实现了对数十个客户同时造成损害的“连锁供应链攻击”。

此外，还确认了供应链攻击中不仅利用软件，还利用硬件的案例。2025 年，曾有基于 Android OS 的智能手机、机顶盒 (set-top box) 等部分设备在制造商出厂前就被预装了恶意代码进行流通的案例。如果这些设备被感染后大规模流通，损害规模将大到难以估量。

预计 2026 年攻击者将不分软件、云、硬件等领域进行攻击，以扩大损害规模。此外，由于供应链攻击现已成为跨国界的问题，预计 2026 年对基于跨国合作的供应链安全框架的需求将比以往更加突出。

主要内容（要点）

- 开源是现代软件开发的核心，但因其开放性和依赖性而成为攻击者的诱人目标。
- 为安全使用开源，需要确保整个开源流水线的可见性和控制力。
- 预计 2026 年将不分软件、云、硬件等领域进行供应链攻击。

2026年展望

4. 对国家核心基础设施的威胁扩大

→ 深入了解 AhnLab 的 CPS 综合安全战略

针对国家基础设施的打击扩大

数据显示，2025 年全球约一半的勒索软件攻击针对的是制造、医疗、能源等核心基础设施。这类设施之所以成为集中攻击目标，原因包括：运营中断带来的高额赔付压力、高价值数据以及相对不足的安全投入。

从今年的行业受损情况来看，服务业因数字化转型加速受损最重；制造业则随着智能工厂的普及，受攻击次数急剧增加。此外，以往被视为攻击禁区的医疗领域也持续遭到破坏，与患者生命直接挂钩的医疗机构已成为高收益攻击目标。这种针对基础设施的攻击趋势预计将在 2026 年持续。

明年攻击预计会增加的领域还包括铁路、海上、航空运输网络及通信网。随着这些设施数字化进程的推进，港口与船舶管理系统、飞机控制系统、机场安保系统等都可能成为攻击对象。而作为连接政府、企业和个人所有数据的核心基础，通信网受攻击的频率正在上升，预计 2026 年攻击范围将进一步扩大。

尽管大多数攻击者的动机是经济利益，**但在 2026 年，部分受国家支持的威胁组织可能因地缘政治冲突发起攻击。**在国际局势持续紧张的背景下，针对社会基础设施的网络攻击将更加精细化。

产业的数字化，将成为攻击者的目标

贯穿国家基础设施攻击的关键关键词是“数字化”。过去以模拟形式运行或在物理隔离的 OT（运营技术）环境中运行的工业系统，曾被认为比外部网络更安全。然而，随着数字化的加速，这些环境与外部的连接点（接点）不断增加，攻击面 (Attack Surface) 随之扩大，攻击者正利用这些新出现的攻击面开展行动。

工业设施数字化带来的最显著变化，是从传统 OT 向涵盖 OT 与 IT 的 “CPS（赛博物理系统，Cyber-Physical System）” 概念转变。**由于封闭的 OT 环境增加了外部接口，安全防护需求已扩展至涵盖 IT、IoT 及云连接的综合防御。**事实上，在最新的智能制造环境中，包含 IoT 在内的各种先进设备已被广泛应用。

针对 CPS 环境的攻击手法也在升级。

攻击者往往利用 OT 与 IT 环境相连的特性，先入侵 IT 环境再渗透进 OT 内部。目前已发现专门针对 OT 环境制作的恶意代码和勒索软件。这类针对 CPS 环境的攻击预计在 2026 年乃至未来将持续扩大。

主要内容（要点）

- 基础设施的数字化、地缘政治冲突、技术武器化加剧了 CPS 环境下对国家基础设施的威胁。
- 国家基础设施遭受攻击时，为实现快速恢复，加强网络恢复能力至关重要，包括备份体系、恢复流程、模拟演练等。

2026年展望

5. 持续增加的 Linux 威胁

→ 深入了解 AhnLab Linux 安全战略

增加的漏洞，升级的攻击

根据 AhnLab 的数据显示，仅 2025 年 6 月一个月内，针对 176 个 Linux 系统的攻击就高达 1.2 万余次。虽然各月数据有所差异，但平均每月有超过 100 个系统遭受数千至上万次的攻击。攻击类型也多种多样，包括 ▲DDoS 僵尸网络 ▲挖矿软件 ▲后门 ▲勒索软件等。Linux 漏洞也达到了数千个，仅 2025 年上半年就发现了超过 6 万个针对 Linux 环境的新型恶意代码。**预计 2026 年，针对 Linux 环境的攻击频率、漏洞数量、恶意代码数量仍将持续增长。**

2025 年，韩国某运营商的 Linux 服务器遭到黑客攻击，导致约 2300 万名客户的个人信息泄露。攻击中使用了基于 Linux 的 BPFDoor 后门。攻击者通过 WebShell 及远程代码执行 (RCE) 漏洞渗透内部系统，随后在 HSS 服务器上安装 BPFDoor 并窃取了 SIM 卡信息。**正如前文对 2026 年国家基础设施威胁扩大的展望，针对 Linux 服务器的攻击也将随之增加。**

为什么针对 Linux 服务器的攻击在增加？ 原因很简单：因为 Linux 服务器连接着大量客户端 PC，并存储着各种核心业务数据。**特别是随着大部分云基础设施基于 Linux 运行，攻击面正在迅速扩大。**AWS、Microsoft Azure、Google Cloud 等主流云环境以及 Docker、Kubernetes 等容器平台均以 Linux 为基础。一旦一个 Linux 系统被攻破，数百个虚拟机和容器可能同时面临威胁。

此外，**攻击者的策略正在发生转变，即直接瞄准海量虚拟化管理层 (Hypervisor) 而非客户操作系统 (Guest OS)。**2025 年 6 月，Akira 勒索软件成功加密了 Nutanix AHV (Acropolis Hypervisor) 虚拟机磁盘文件，其攻击范围已超越 VMware ESXi 和 Hyper-V。虚拟化平台的多样化导致了攻击面的扩大。仅需一次入侵，即可在数小时内使数百个虚拟机瘫痪，极大地提高了攻击效率。随着针对 Linux 系统的恶意代码增加，可能导致业务中断等严重后果。

面对高级化的 Linux 攻击，单一的安全手段难以应对。由于攻击可能始于终端、电子邮件等多个环节，且新变种恶意代码频发，**因此，建立像 AhnLab 安全架构那样跨多环节执行最佳安全功能的集成安全体系将变得至关重要。**

主要内容（要点）

- 为提高运营和性能效率，服务器环境中的 Linux 使用量正在增加，但安全管理相对不足。
- 预计针对虚拟化环境和 Linux 的攻击将增加 – 一次攻击可能入侵数百个虚拟机。
- 在多个环节执行最佳安全功能的集成安全体系的重要性将提高。

AhnLab

AhnLab China,
北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区新镇路1699弄E栋303室
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）
http://cn.ahnlab.com | cn.sales@ahnlab.com