2025年
全球高级持续性威胁（APT）
研究报告

RESEARCH
REPORT

360数字安全
数字安全的领导者

360
高级威胁研究院

360数字安全
数字安全的领导者

360
高级威胁研究院

ADVANCED PERSISTENT THREAT

2025

全球高级持续性威胁(APT)研究报告

2025

全球高级持续性威胁
研究报告

2025

GLOBAL ADVANCED PERSISTENT THREAT
Research Report

360数字安全
数字安全的领导者

360 高级威胁研究院

2025

全球高级持续性威胁
研究报告

2025

GLOBAL ADVANCED PERSISTENT THREAT
Research Report

360数字安全
数字安全的领导者

360 高级威胁研究院

CONTENTS /目录

CONTENTS /目录

PART 1

概述

1、2025年度全球高级可持续性威胁形势概览

2025年，世界政治经济格局进入深刻演变期，传统秩序加速调整，新兴力量加快崛起。全球范围内冲突与博弈显著增多，地缘冲突在多地区凸显，多极化进程在曲折中持续向前。与此同时，网络安全态势正经历深刻演进，已从“技术层面对抗”升级为关乎国家生存与发展的战略博弈。我国网络空间安全面临复杂严峻挑战：境外国家级APT攻击持续不断，人工智能驱动的新型攻击与供应链渗透风险集中显现，黑色产业链助推勒索攻击与数据泄露趋于产业化，网络空间防御体系承受全方位压力。

2025年，全球网络安全厂商和机构累计发布APT报告700多篇，报告涉及APT组织140个，其中属于首次披露的APT组织42个，比2024年同期均呈现一定程度增加。从全球范围看，APT组织攻击活动聚焦地区政治、经济等时事热点，攻击目标集中分布于政府机构、国防军工、信息技术、金融、教育等十几个重点行业领域。当前，国家层面的网络攻防对抗不再局限于传统安全范畴，已经逐渐成为国家战略体系中不可或缺的组成部分。

我国历来是APT组织攻击的重点区域。依托360安全大模型，360高级威胁研究院在2025年，累计捕获到1300余起针对我国的APT攻击活动。相关APT组织主要来自北美、东亚、南亚、东南亚等地区。我国受攻击活动影响的单位主要分布于政府机构、教育、科研、国防军工、制造等15个重点行业领域。

2025年，北美和我国台湾省地区的APT组织活跃度较往年明显增加，这与中美政博弈、台海局势发展密切相关。来自北美地区的APT攻击技战术水平高超，主要针对我国重点科研和关基单位，造成的影响和危害极大；来自我国台湾省地区的APT组织主要针对我国政府机构和教育科研等领域展开钓鱼攻击，从而进行渗透和窃密。

2025年，360再次捕获并披露了到4个全新APT组织，分别为北美地区的APT-C-78、东亚地区的APT-C-64（匿名者64）、APT-C-67（乌苏拉）和南亚地区的APT-C-76（银环蛇）。截至2025年底，360已累计率先发现并披露了60个境外APT组织。

2025年，全球APT组织攻击技战术向规模化与战略化演进，供应链安全成为关键防线。在未来攻防两端对抗中AI技术的运用中，使得“AI对战AI”成为常态。网络空间的攻防对抗步入智能驱动、攻防前置、全域联动的新阶段。

PART 1

概述

1、2025年度全球高级可持续性威胁形势概览

2025年，世界政治经济格局进入深刻演变期，传统秩序加速调整，新兴力量加快崛起。全球范围内冲突与博弈显著增多，地缘冲突在多地区凸显，多极化进程在曲折中持续向前。与此同时，网络安全态势正经历深刻演进，已从“技术层面对抗”升级为关乎国家生存与发展的战略博弈。我国网络空间安全面临复杂严峻挑战：境外国家级APT攻击持续不断，人工智能驱动的新型攻击与供应链渗透风险集中显现，黑色产业链助推勒索攻击与数据泄露趋于产业化，网络空间防御体系承受全方位压力。

2025年，全球网络安全厂商和机构累计发布APT报告700多篇，报告涉及APT组织140个，其中属于首次披露的APT组织42个，比2024年同期均呈现一定程度增加。从全球范围看，APT组织攻击活动聚焦地区政治、经济等时事热点，攻击目标集中分布于政府机构、国防军工、信息技术、金融、教育等十几个重点行业领域。当前，国家层面的网络攻防对抗不再局限于传统安全范畴，已经逐渐成为国家战略体系中不可或缺的组成部分。

我国历来是APT组织攻击的重点区域。依托360安全大模型，360高级威胁研究院在2025年，累计捕获到1300余起针对我国的APT攻击活动。相关APT组织主要来自北美、东亚、南亚、东南亚等地区。我国受攻击活动影响的单位主要分布于政府机构、教育、科研、国防军工、制造等15个重点行业领域。

2025年，北美和我国台湾省地区的APT组织活跃度较往年明显增加，这与中美政博弈、台海局势发展密切相关。来自北美地区的APT攻击技战术水平高超，主要针对我国重点科研和关基单位，造成的影响和危害极大；来自我国台湾省地区的APT组织主要针对我国政府机构和教育科研等领域展开钓鱼攻击，从而进行渗透和窃密。

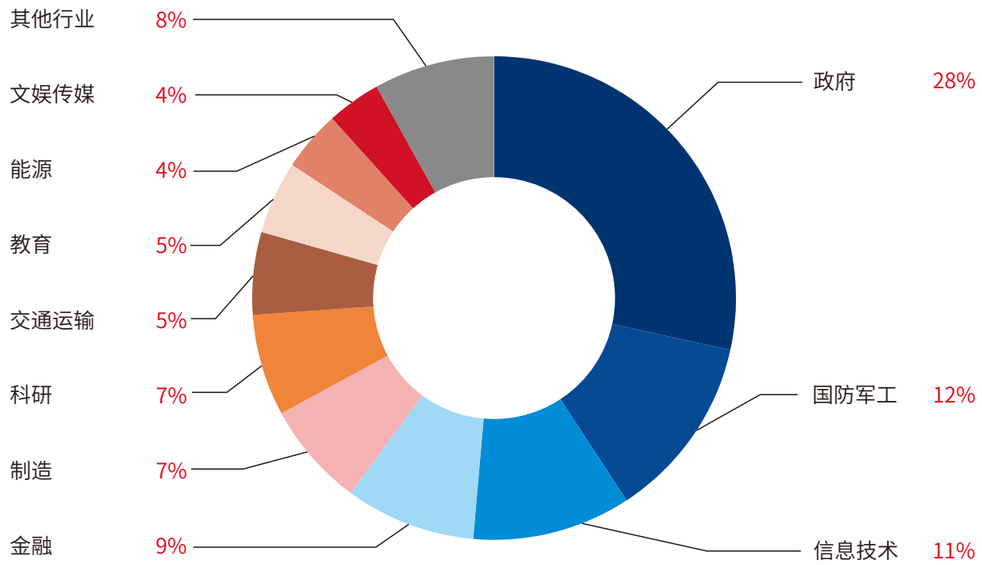
2025年，360再次捕获并披露了到4个全新APT组织，分别为北美地区的APT-C-78、东亚地区的APT-C-64（匿名者64）、APT-C-67（乌苏拉）和南亚地区的APT-C-76（银环蛇）。截至2025年底，360已累计率先发现并披露了60个境外APT组织。

2025年，全球APT组织攻击技战术向规模化与战略化演进，供应链安全成为关键防线。在未来攻防两端对抗中AI技术的运用中，使得“AI对战AI”成为常态。网络空间的攻防对抗步入智能驱动、攻防前置、全域联动的新阶段。

2、2025年度活跃APT组织统计

2025年，全球大国竞争呈现白热化，在军事、政治、经济等领域的博弈进一步深化，“国家级”背景的APT组织的攻击活动更加贴近的于地缘政治势力在地区博弈和竞争的战略。尤其在地缘军事行动中，国家级APT攻击已经成为战争战略战术的重要一环。

在此形势下，全球APT组织继续保持高活跃度。截止2025年底，全球网络安全厂商以及机构累计发布APT报告700多篇，报告涉及APT组织140个，其中属于首次披露组织42个。从全球范围看APT组织攻击比较集中的行业为政府机构、国防军工、信息技术、金融、制造等领域。



▲图：2025年全球范围APT攻击活动影响行业分布 TOP 10

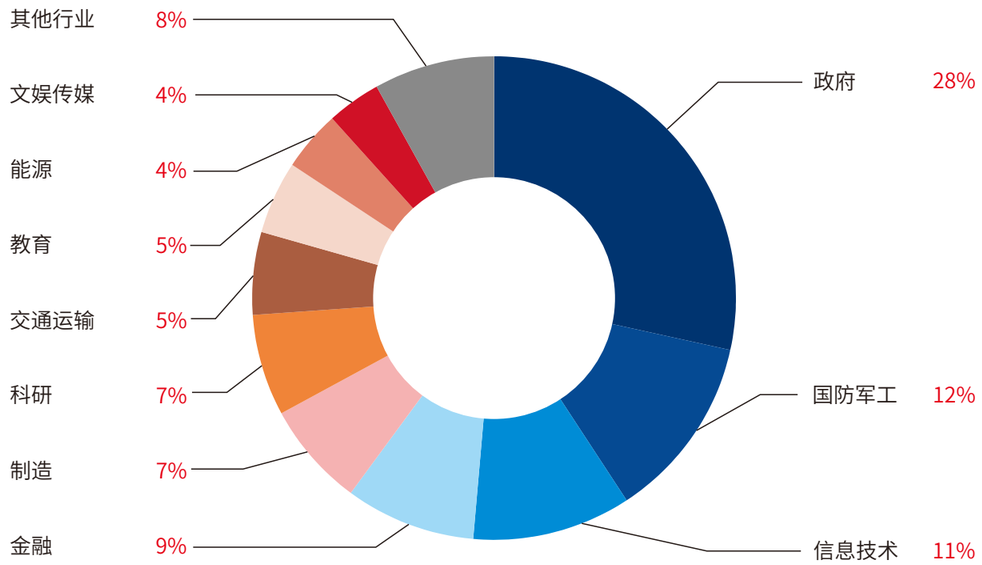
区域	组织名称	活跃程度
东亚	APT-C-01（毒云藤）	★★★★
	APT-C-65（金叶萝）	★★★★
	APT-C-26（Lazarus）	★★★★
	APT-C-55（Kimsuky）	★★★½
	APT-C-06（DarkHotel）	★★★
	APT-C-60（伪猎者）	★★½
	APT-C-64（匿名者64）	★★
	APT-C-28（ScarCruft）	★★
	APT-C-67（乌苏拉）	★★
南亚	APT-C-08（蔓灵花）	★★★★
	APT-C-09（摩诃草）	★★★½
	APT-C-48（CNC）	★★★
	APT-C-56（透明部落）	★★★
	APT-C-76（银环蛇）	★★½
	APT-C-24（响尾蛇）	★★½
	APT-C-70（独角犀）	★★
	APT-C-35（肚脑虫）	★★
北美	APT-C-78	★★★½
	APT-C-40（NSA）	★
东南亚	APT-C-00（海莲花）	★★★★
东欧	APT-C-20（APT28）	★★★½
	APT-C-53（Gamaredon）	★★★
	APT-C-13（Sandworm）	★★★
	APT-C-25（APT29）	★★
	APT-C-29（Turla）	★★
中东	APT-C-51（APT35）	★★★
	APT-C-49（OilRig）	★★½
南美	APT-C-36（盲眼鹰）	★★

▲图：2025年全球典型APT组织活跃度情况

2、2025年度活跃APT组织统计

2025年，全球大国竞争呈现白热化，在军事、政治、经济等领域的博弈进一步深化，“国家级”背景的APT组织的攻击活动更加贴近的于地缘政治势力在地区博弈和竞争的战略。尤其在地缘军事行动中，国家级APT攻击已经成为战争战略战术的重要一环。

在此形势下，全球APT组织继续保持高活跃度。截止2025年底，全球网络安全厂商以及机构累计发布APT报告700多篇，报告涉及APT组织140个，其中属于首次披露组织42个。从全球范围看APT组织攻击比较集中的行业为政府机构、国防军工、信息技术、金融、制造等领域。



▲图：2025年全球范围APT攻击活动影响行业分布 TOP 10

区域	组织名称	活跃程度
东亚	APT-C-01（毒云藤）	★★★★
	APT-C-65（金叶萝）	★★★★
	APT-C-26（Lazarus）	★★★★
	APT-C-55（Kimsuky）	★★★½
	APT-C-06（DarkHotel）	★★★
	APT-C-60（伪猎者）	★★½
	APT-C-64（匿名者64）	★★
	APT-C-28（ScarCruft）	★★
	APT-C-67（乌苏拉）	★★
南亚	APT-C-08（蔓灵花）	★★★★
	APT-C-09（摩诃草）	★★★½
	APT-C-48（CNC）	★★★
	APT-C-56（透明部落）	★★★
	APT-C-76（银环蛇）	★★½
	APT-C-24（响尾蛇）	★★½
	APT-C-70（独角犀）	★★
	APT-C-35（肚脑虫）	★★
北美	APT-C-78	★★★½
	APT-C-40（NSA）	★
东南亚	APT-C-00（海莲花）	★★★★
东欧	APT-C-20（APT28）	★★★½
	APT-C-53（Gamaredon）	★★★
	APT-C-13（Sandworm）	★★★
	APT-C-25（APT29）	★★
	APT-C-29（Turla）	★★
中东	APT-C-51（APT35）	★★★
	APT-C-49（OilRig）	★★½
南美	APT-C-36（盲眼鹰）	★★

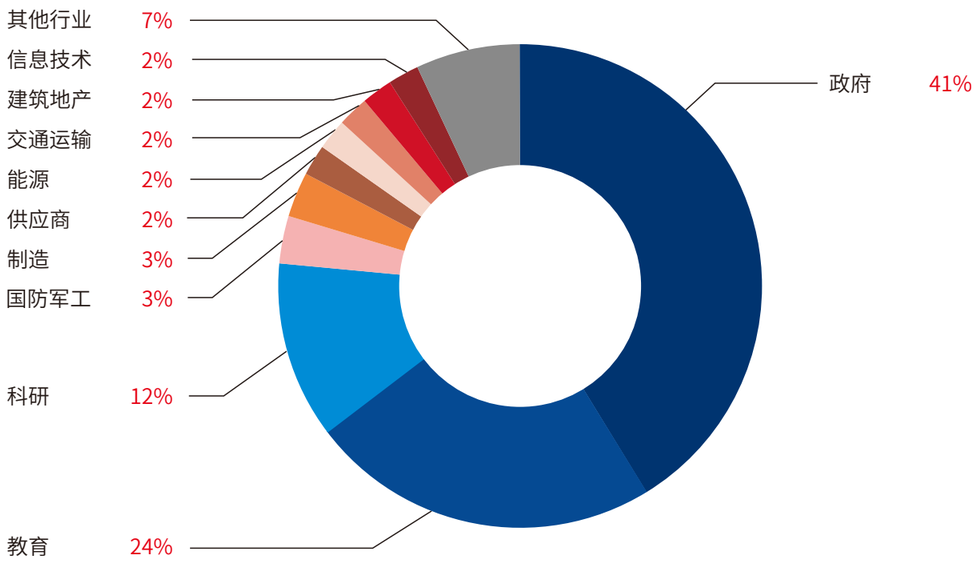
▲图：2025年全球典型APT组织活跃度情况

我国历来是地缘周边APT组织攻击的重点区域。依托360安全大模型，360高级威胁研究院在2025年，累计捕获到1300余起针对我国的APT攻击活动。APT组织攻击源主要来自南亚、东南亚、东亚以及北美等地区。我国受攻击活动影响的单位主要分布于政府机构、教育、科研、国防军工、制造等15个重点行业领域。

基于APT组织攻击活动频次、攻击活动影响单位和终端数量、攻击技战术水平等多个指标，我们对2025年攻击活动影响我国的APT组织活跃度进行综合评估，得出下表。

排名	攻击来源组织分布	所在地域	目标行业领域
TOP1	APT-C-01（毒云藤）	东亚地区	政府、教育、科研等
TOP2	APT-C-00（海莲花）	东南亚地区	教育、科研、政府等
TOP3	APT-C-65（金叶萝）	东亚地区	政府、国防军工、科研等
TOP4	APT-C-08（蔓灵花）	南亚地区	政府、教育、供应商等
TOP5	APT-C-09（摩诃草）	南亚地区	教育、科研、政府、制造等
TOP6	APT-C-06（DarkHotel）	东亚地区	贸易、科研、政府等
TOP7	APT-C-48（CNC）	南亚地区	教育、国防军工、科研等
TOP8	APT-C-78	北美地区	国防军工、制造、能源等
TOP9	APT-C-60（伪猎者）	东亚地区	政府、贸易等
TOP10	APT-C-64（匿名者64）	东亚地区	政府、国防军工、科研等

APT组织对我国政府、教育、科研行业攻击占比超过七成，其危害远超普通网络攻击，直接关系国家安全与科技发展命脉。针对我国政府、教育和科研机构的高级持续性威胁攻击呈现出高频次、高隐蔽性、高战略意图的特征，已成为危害我国国家安全、科技主权与数据主权的核心风险之一。这些攻击的背后往往是由境外情报机构主导、具备国家级资源支持的系统性网络间谍活动，其目的远超经济窃密，直指国家核心竞争力与战略安全。



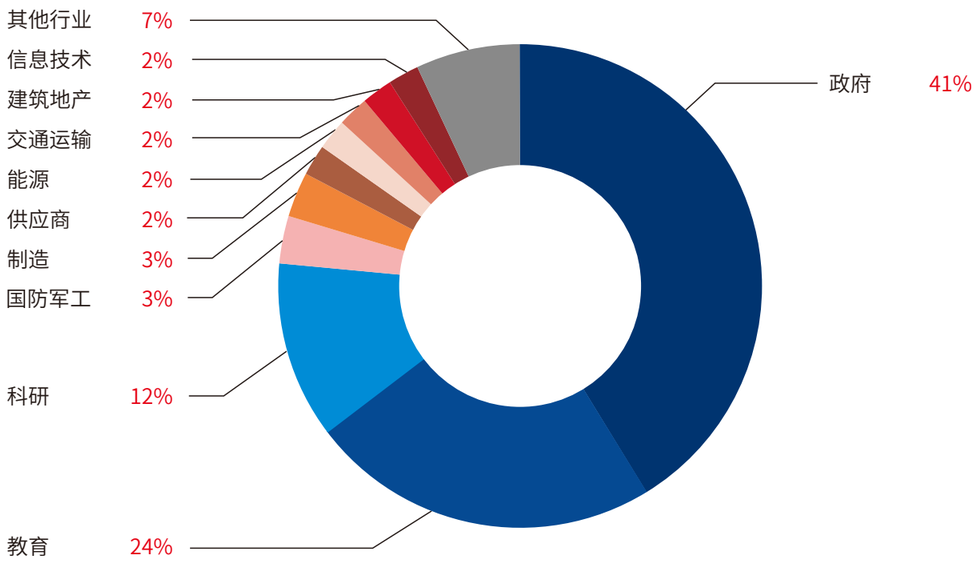
▲图：2025年我国受APT攻击影响单位行业分布TOP 10

我国历来是地缘周边APT组织攻击的重点区域。依托360安全大模型，360高级威胁研究院在2025年，累计捕获到1300余起针对我国的APT攻击活动。APT组织攻击源主要来自南亚、东南亚、东亚以及北美等地区。我国受攻击活动影响的单位主要分布于政府机构、教育、科研、国防军工、制造等15个重点行业领域。

基于APT组织攻击活动频次、攻击活动影响单位和终端数量、攻击技战术水平等多个指标，我们对2025年攻击活动影响我国的APT组织活跃度进行综合评估，得出下表。

排名	攻击来源组织分布	所在地域	目标行业领域
TOP1	APT-C-01（毒云藤）	东亚地区	政府、教育、科研等
TOP2	APT-C-00（海莲花）	东南亚地区	教育、科研、政府等
TOP3	APT-C-65（金叶萝）	东亚地区	政府、国防军工、科研等
TOP4	APT-C-08（蔓灵花）	南亚地区	政府、教育、供应商等
TOP5	APT-C-09（摩诃草）	南亚地区	教育、科研、政府、制造等
TOP6	APT-C-06（DarkHotel）	东亚地区	贸易、科研、政府等
TOP7	APT-C-48（CNC）	南亚地区	教育、国防军工、科研等
TOP8	APT-C-78	北美地区	国防军工、制造、能源等
TOP9	APT-C-60（伪猎者）	东亚地区	政府、贸易等
TOP10	APT-C-64（匿名者64）	东亚地区	政府、国防军工、科研等

APT组织对我国政府、教育、科研行业攻击占比超过七成，其危害远超普通网络攻击，直接关系国家安全与科技发展命脉。针对我国政府、教育和科研机构的高级持续性威胁攻击呈现出高频次、高隐蔽性、高战略意图的特征，已成为危害我国国家安全、科技主权与数据主权的核心风险之一。这些攻击的背后往往是由境外情报机构主导、具备国家级资源支持的系统性网络间谍活动，其目的远超经济窃密，直指国家核心竞争力与战略安全。



▲图：2025年我国受APT攻击影响单位行业分布TOP 10

PART 2

地区

1、北美

2025年的中美两国在政治、经济、贸易等多个领域激烈博弈，中美关系逐渐形成“竞争为主、对抗可控、合作局部”的新平衡。在此背景下，2025年北美地区APT组织对我国的网络攻击活动，呈现“国家级统筹、定向关键基础设施、战术隐蔽化”的核心特征。

2025年年初，北美地区APT组织，针对我国智慧能源和数字信息大型高科技企业展开网络攻击，意图窃取核心技术与商业机密，影响高科技产业竞争；2月，以APT-C-40（NSA）组织为核心执行机构，联合美高校作为“学术掩护体”，针对我国亚冬会相关服务展开攻击活动，威胁亚冬会赛事系统与黑龙江地区关键基础设施，美方3名TAO特工因此次攻击事件被我国通缉；10月，我国国家安全机关再次披露了APT-C-40（NSA）组织对我国国家授时中心实施的重大网络攻击活动。

PART 2

地区

1、北美

2025年的中美两国在政治、经济、贸易等多个领域激烈博弈，中美关系逐渐形成“竞争为主、对抗可控、合作局部”的新平衡。在此背景下，2025年北美地区APT组织对我国的网络攻击活动，呈现“国家级统筹、定向关键基础设施、战术隐蔽化”的核心特征。

2025年年初，北美地区APT组织，针对我国智慧能源和数字信息大型高科技企业展开网络攻击，意图窃取核心技术与商业机密，影响高科技产业竞争；2月，以APT-C-40（NSA）组织为核心执行机构，联合美高校作为“学术掩护体”，针对我国亚冬会相关服务展开攻击活动，威胁亚冬会赛事系统与黑龙江地区关键基础设施，美方3名TAO特工因此次攻击事件被我国通缉；10月，我国国家安全机关再次披露了APT-C-40（NSA）组织对我国国家授时中心实施的重大网络攻击活动。

披露时间	报告名称	发布机构
2025-1-17	美网络攻击我国某先进材料设计研究院事件调查报告	国家互联网应急中心
2025-1-17	美网络攻击我国某智慧能源和数字信息大型高科技企业事件调查报告	国家互联网应急中心
2025-3-25	美情报机构针对全球移动智能终端实施的监听窃密活动	中国网络安全产业联盟
2025-4-3	“2025年哈尔滨第九届亚冬会”赛事信息系统及黑龙江省内关键信息基础设施遭境外网络攻击情况监测分析报告	国家计算机病毒应急处理中心
2025-4-15	央视新闻报道:360揭批美国NSA针对亚冬会发起网络攻击	360
2025-4-16	公安机关公开悬赏通缉3名美国特工美国国家安全局组织实施亚冬会网络攻击活动	中华人民共和国公安部
2025-4-28	美情报机构利用网络 攻击中国大型商用密码产品提供商事件调查报告	中国网络空间安全协会
2025-7-3	APT-C-78组织Exchange内存自检工具发布	360
2025-8-1	美情报机构频繁对我国防军工领域实施网络攻击窃密	中国网络空间安全协会
2025-10-19	守护“北京时间”!国家安全机关破获美国国家安全局重大网络攻击案	国家安全部
2025-10-19	关于国家授时中心遭受美国国家安全局网络攻击事件的技术分析报告	国家互联网应急中心
2025-10-22	深度复盘美国NSA渗透攻击授时中心,360安全智能体蜂群引领政企防护升维	360

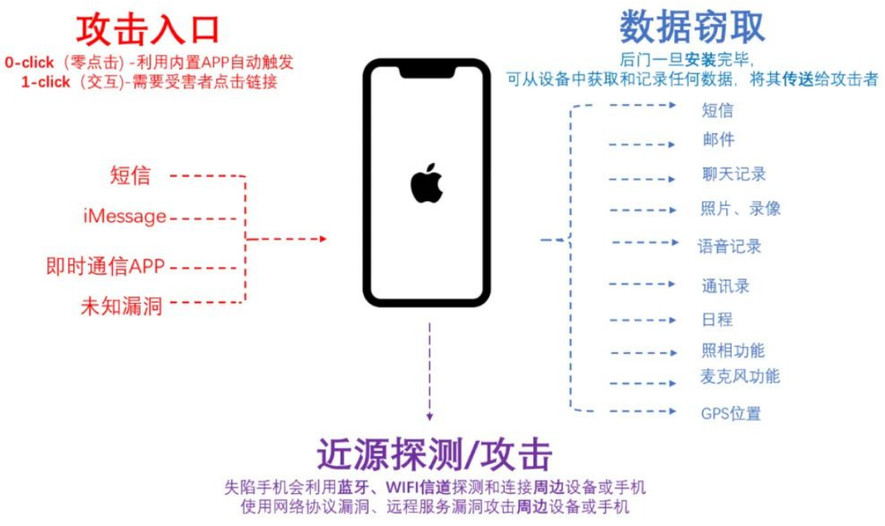
360高级威胁研究院在2025年捕获到多起北美地区APT组织对我国关基单位的重大网络攻击活动。这些网络攻击活动聚焦在关键基础设施(能源、电信、交通、授时)、高科技(半导体、量子、先进材料)、重大赛事与政府机构领域。其战略意图是期望通过技术遏制,窃取核心技术,延缓中国高科技产业的发展和突破;同时在关键基础设施植入后门,形成“战时破坏”能力,实现战略威慑。

1.1、APT-C-40(NSA)

APT-C-40(NSA)组织持续针对我国以及全球的网络攻击和渗透,其攻击技战术复杂,攻击武器储备丰富,技战术水平大幅领先于已知的网络攻击组织。在2025年,我国国家安全机关披露了该组织对国家授时中心实施的网络攻击活动。

APT-C-40(NSA)组织在此次攻击中使用了多达42款网络攻击武器,在2022年3月至2024年6月期间,攻击者利用境外网络资产作为主控端服务器持续实施了千余次攻击,严重破坏我国关键信息基础设施安全,对国家安全造成系统性、持续性危害。

在本次攻击活动中,攻击者在手机端成功获取办公计算机的登录凭证后,进一步通过手机端作为跳板取得了计算机端点的远程控制权限,并依次完成特种网络攻击武器的植入与升级。



随后,攻击者通过多款网络攻击武器协同作业,在目标内网构建起一个包含四层加密隧道的窃密攻击平台,具备高度隐蔽性与完整攻击功能,进而以此实施内网横向渗透,非法窃取关键数据信息。

整个过程中,攻击者在计算机终端上部署的攻击模块总计达42个。这些模块均采用内存加载、解密执行的方式运行,有效规避了常规安全软件的检测与查杀。

其中,前哨控守类武器(eHome_0cx)作为核心加载调度模块,由四个组件共同构成,负责协调并调用

▲图:APT-C-40(NSA)组织攻击渗透示意图

披露时间	报告名称	发布机构
2025-1-17	美网络攻击我国某先进材料设计研究院事件调查报告	国家互联网应急中心
2025-1-17	美网络攻击我国某智慧能源和数字信息大型高科技企业事件调查报告	国家互联网应急中心
2025-3-25	美情报机构针对全球移动智能终端实施的监听窃密活动	中国网络安全产业联盟
2025-4-3	“2025年哈尔滨第九届亚冬会”赛事信息系统及黑龙江省内关键信息基础设施遭境外网络攻击情况监测分析报告	国家计算机病毒应急处理中心
2025-4-15	央视新闻报道:360揭批美国NSA针对亚冬会发起网络攻击	360
2025-4-16	公安机关公开悬赏通缉3名美国特工美国国家安全局组织实施亚冬会网络攻击活动	中华人民共和国公安部
2025-4-28	美情报机构利用网络 攻击中国大型商用密码产品提供商事件调查报告	中国网络空间安全协会
2025-7-3	APT-C-78组织Exchange内存自检工具发布	360
2025-8-1	美情报机构频繁对我国防军工领域实施网络攻击窃密	中国网络空间安全协会
2025-10-19	守护“北京时间”!国家安全机关破获美国国家安全局重大网络攻击案	国家安全部
2025-10-19	关于国家授时中心遭受美国国家安全局网络攻击事件的技术分析报告	国家互联网应急中心
2025-10-22	深度复盘美国NSA渗透攻击授时中心,360安全智能体蜂群引领政企防护升维	360

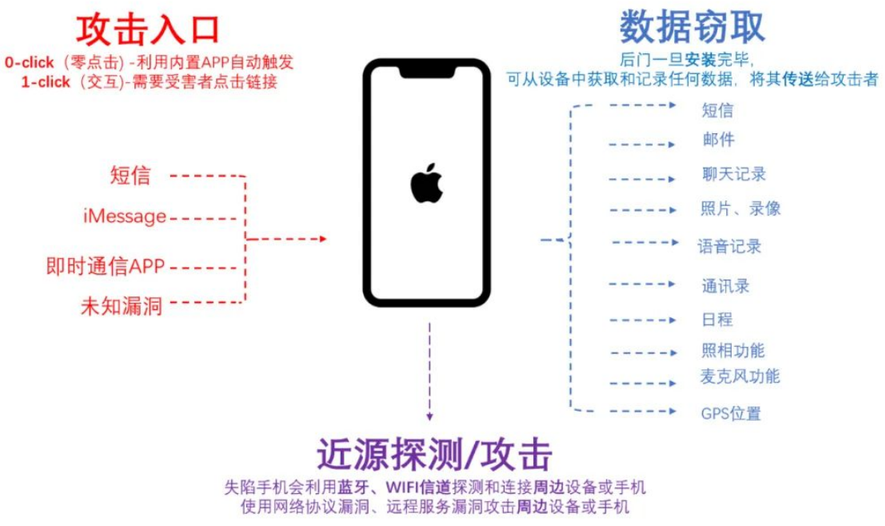
360高级威胁研究院在2025年捕获到多起北美地区APT组织对我国关基单位的重大网络攻击活动。这些网络攻击活动聚焦在关键基础设施(能源、电信、交通、授时)、高科技(半导体、量子、先进材料)、重大赛事与政府机构领域。其战略意图是期望通过技术遏制,窃取核心技术,延缓中国高科技产业的发展和突破;同时在关键基础设施植入后门,形成“战时破坏”能力,实现战略威慑。

1.1、APT-C-40(NSA)

APT-C-40(NSA)组织持续针对我国以及全球的网络攻击和渗透,其攻击技战术复杂,攻击武器储备丰富,技战术水平大幅领先于已知的网络攻击组织。在2025年,我国国家安全机关披露了该组织对国家授时中心实施的网络攻击活动。

APT-C-40(NSA)组织在此次攻击中使用了多达42款网络攻击武器,在2022年3月至2024年6月期间,攻击者利用境外网络资产作为主控端服务器持续实施了千余次攻击,严重破坏我国关键信息基础设施安全,对国家安全造成系统性、持续性危害。

在本次攻击活动中,攻击者在手机端成功获取办公计算机的登录凭证后,进一步通过手机端作为跳板取得了计算机端点的远程控制权限,并依次完成特种网络攻击武器的植入与升级。



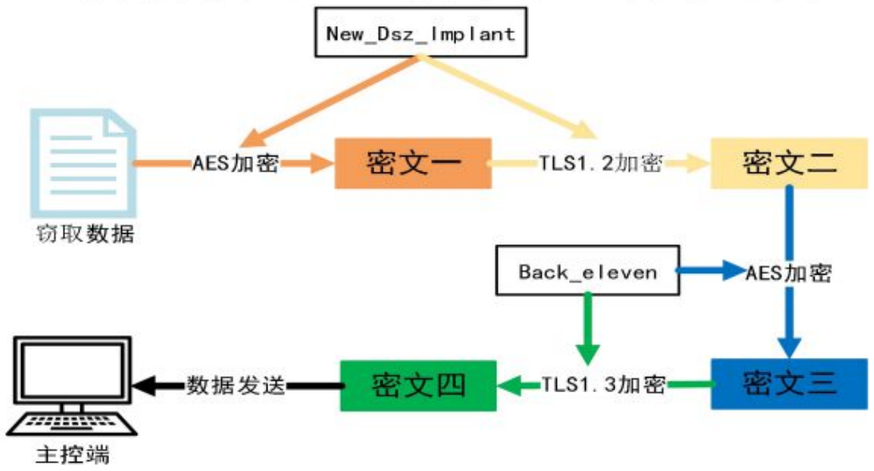
随后,攻击者通过多款网络攻击武器协同作业,在目标内网构建起一个包含四层加密隧道的窃密攻击平台,具备高度隐蔽性与完整攻击功能,进而以此实施内网横向渗透,非法窃取关键数据信息。

整个过程中,攻击者在计算机终端上部署的攻击模块总计达42个。这些模块均采用内存加载、解密执行的方式运行,有效规避了常规安全软件的检测与查杀。

其中,前哨控守类武器(eHome_0cx)作为核心加载调度模块,由四个组件共同构成,负责协调并调用

▲图:APT-C-40(NSA)组织攻击渗透示意图

其他各类网络攻击武器，包括隧道搭建类武器（Back_Eleven）以及数据窃取类武器（New-Dsz-Implant），形成一个层次清晰、功能完备的攻击体系。



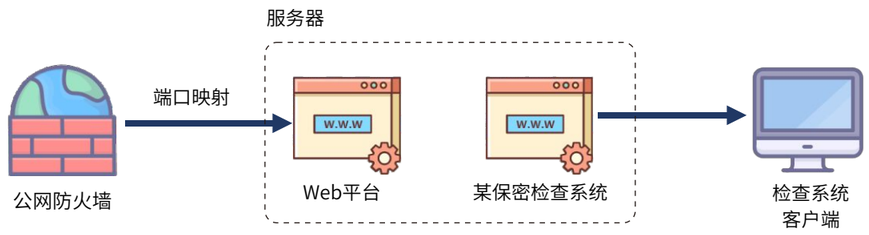
图①

我们通过深入分析发现，相比“飞马”等间谍软件针对苹果手机的窃密攻击，“三角测量”攻击活动针对苹果手机的攻击复杂度与隐蔽性更高。该类攻击通常采用多阶段、高集成的漏洞利用链，并植入极难检测的持久化后门，从而给防御与检测工作带来极大挑战。

1.2、APT-C-78

APT-C-78是360高级威胁研究院在2025年捕获并披露的北美地区APT组织。该组织表现活跃，针对我国国防军工、科研、信息技术、能源、汽车制造等几个领域重点目标策划了针对性攻击活动。

APT-C-78组织在2025年的攻击活动中对目标单位针对性的挖掘Web漏洞，并利用漏洞展开攻击活动。该组织在针对我国某国防军工背景相关单位的攻击活动中，针对受害企业自行开发的Web服务进行漏洞挖掘，继而利用漏洞展开攻击；在获得内网相关权限后，进一步利用某国产安全软件的服务端更新机制，分发专项后门程序，实现了对受害单位员工主机的批量控制。



图②

▲ 图①：APT-C-40（NSA）组织攻击流程示意图　　图②：APT-C-78组织攻击流程示意图

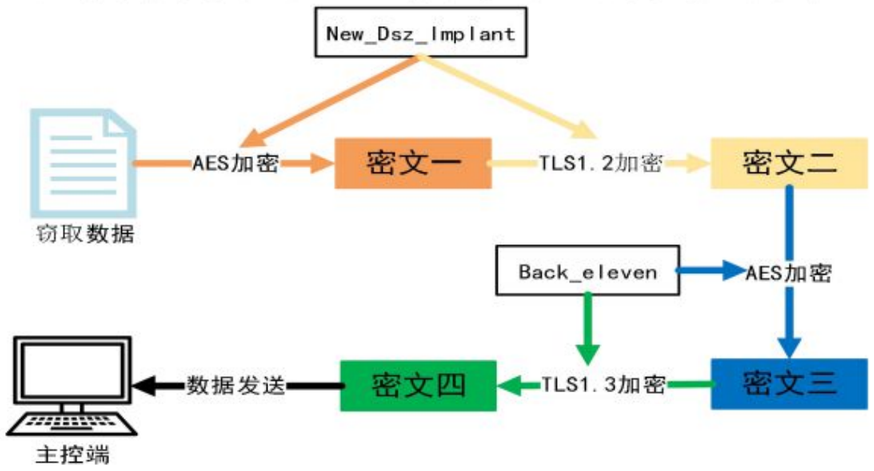
2、朝鲜半岛

2025年朝鲜半岛的网络攻击活动频繁，其活动具有高度组织性、隐蔽性和战略性。

朝鲜半岛的APT组织攻击目标广泛，涉及金融、能源、政府机构等基础设施，以及通过攻击外交、国防相关机构获取战略情报；APT-C-06（DarkHotel）、APT-C-60（伪猎者）等组织主要针对我国政府机构、驻外机构以及涉朝相关目标，擅长基于供应链攻击，尤其是利用目标环境特定应用0day漏洞进行突破；APT-C-26（Lazarus）、APT-C-55（Kimsuky）等组织除了对朝鲜半岛周围政府组织、涉朝机构等目标关注，更多攻击是针对虚拟加密货币的窃取活动，对全球金融与地缘安全构成持续冲击。

朝鲜半岛地区APT组织的网络攻击已成为“国家级融资工具”，战术从0day漏洞利用、多阶段攻击链等复杂手法延伸出“社会工程 + 内部渗透”，AI深度伪造与供应链攻击成为新趋势，对全球金融安全与地缘稳定构成重大威胁。

其他各类网络攻击武器，包括隧道搭建类武器（Back_Eleven）以及数据窃取类武器（New-Dsz-Implant），形成一个层次清晰、功能完备的攻击体系。



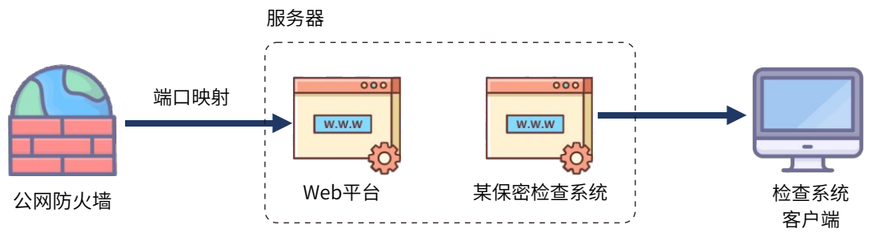
图①

我们通过深入分析发现，相比“飞马”等间谍软件针对苹果手机的窃密攻击，“三角测量”攻击活动针对苹果手机的攻击复杂度与隐蔽性更高。该类攻击通常采用多阶段、高集成的漏洞利用链，并植入极难检测的持久化后门，从而给防御与检测工作带来极大挑战。

1.2、APT-C-78

APT-C-78是360高级威胁研究院在2025年捕获并披露的北美地区APT组织。该组织表现活跃，针对我国国防军工、科研、信息技术、能源、汽车制造等几个领域重点目标策划了针对性攻击活动。

APT-C-78组织在2025年的攻击活动中对目标单位针对性的挖掘Web漏洞，并利用漏洞展开攻击活动。该组织在针对我国某国防军工背景相关单位的攻击活动中，针对受害企业自行开发的Web服务进行漏洞挖掘，继而利用漏洞展开攻击；在获得内网相关权限后，进一步利用某国产安全软件的服务端更新机制，分发专项后门程序，实现了对受害单位员工主机的批量控制。



图②

▲ 图①：APT-C-40（NSA）组织攻击流程示意图　　图②：APT-C-78组织攻击流程示意图

2、朝鲜半岛

2025年朝鲜半岛的网络攻击活动频繁，其活动具有高度组织性、隐蔽性和战略性。

朝鲜半岛的APT组织攻击目标广泛，涉及金融、能源、政府机构等基础设施，以及通过攻击外交、国防相关机构获取战略情报；APT-C-06（DarkHotel）、APT-C-60（伪猎者）等组织主要针对我国政府机构、驻外机构以及涉朝相关目标，擅长基于供应链攻击，尤其是利用目标环境特定应用0day漏洞进行突破；APT-C-26（Lazarus）、APT-C-55（Kimsuky）等组织除了对朝鲜半岛周围政府组织、涉朝机构等目标关注，更多攻击是针对虚拟加密货币的窃取活动，对全球金融与地缘安全构成持续冲击。

朝鲜半岛地区APT组织的网络攻击已成为“国家级融资工具”，战术从0day漏洞利用、多阶段攻击链等复杂手法延伸出“社会工程 + 内部渗透”，AI深度伪造与供应链攻击成为新趋势，对全球金融安全与地缘稳定构成重大威胁。

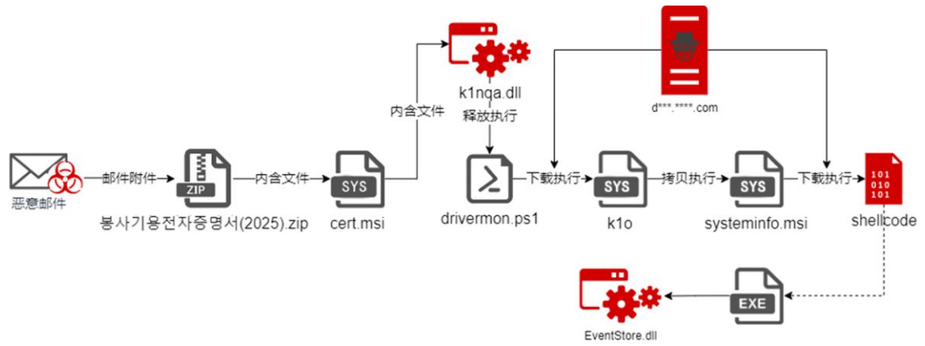
2.1、APT-C-06（DarkHotel）

APT-C-06（DarkHotel）组织在2025年攻击活动有所增加，技战术迭代升级。该组织的攻击行业未有明显变化，对我国的攻击活动受地缘因素影响，集中在朝鲜半岛附近地区的对朝贸易相关单位。

2025年上半年，APT-C-06（DarkHotel）组织在攻击活动中，利用钓鱼邮件分发包含恶意安装包的附件。攻击者使用的诱饵文件为“봉사기용전자증명서(2025).zip”（服务用电子证书）。执行该文件将引发一系列恶意行为，最终导致恶意载荷在用户机器驻留。

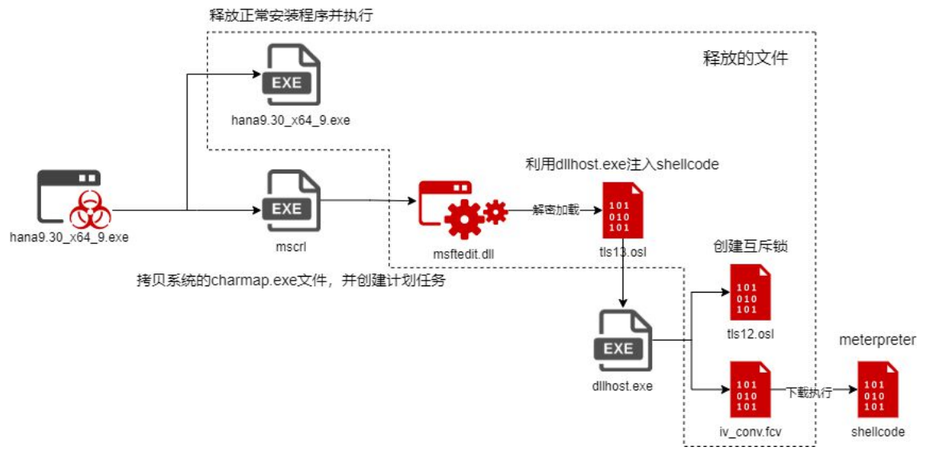
▲ APT-C-06（DarkHotel）伪造的证书程序

载荷的执行流程如下图所示：



图①

在我们捕获的另外一起攻击活动中，攻击者通过网盘工具、聊天工具和U盘等方式投递伪装成输入法以及伪装成压缩工具的恶意程序，受影响用户分布在朝鲜半岛周边地区。经360高级威胁研究院分析，这两种恶意程序均与APT-C-06（DarkHotel）组织在历史攻击活动中使用的攻击载荷高度相似。



图②

▲ 图①：APT-C-06（DarkHotel）组织攻击流程图 1　图②：APT-C-06（DarkHotel）组织攻击流程图 2

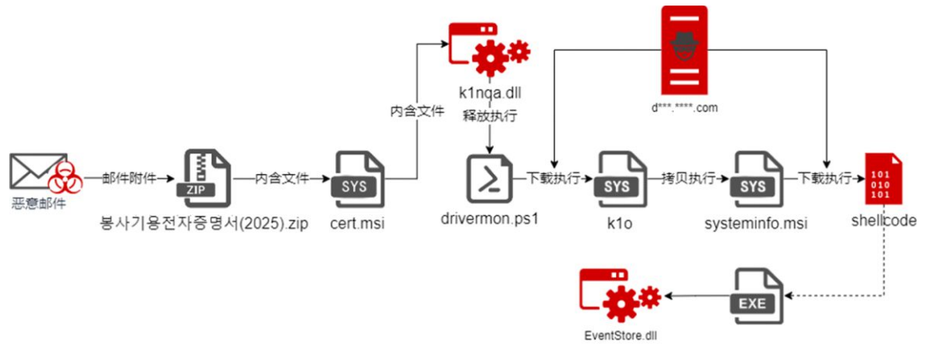
2.1、APT-C-06（DarkHotel）

APT-C-06（DarkHotel）组织在2025年攻击活动有所增加，技战术迭代升级。该组织的攻击行业未有明显变化，对我国的攻击活动受地缘因素影响，集中在朝鲜半岛附近地区的对朝贸易相关单位。

2025年上半年，APT-C-06（DarkHotel）组织在攻击活动中，利用钓鱼邮件分发包含恶意安装包的附件。攻击者使用的诱饵文件为“봉사기용전자증명서(2025).zip”（服务用电子证书）。执行该文件将引发一系列恶意行为，最终导致恶意载荷在用户机器驻留。

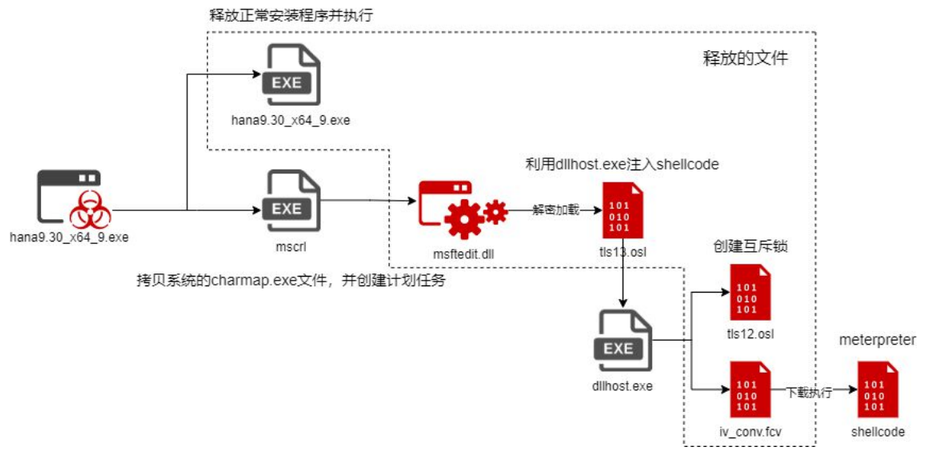
▲ APT-C-06（DarkHotel）伪造的证书程序

载荷的执行流程如下图所示：



图①

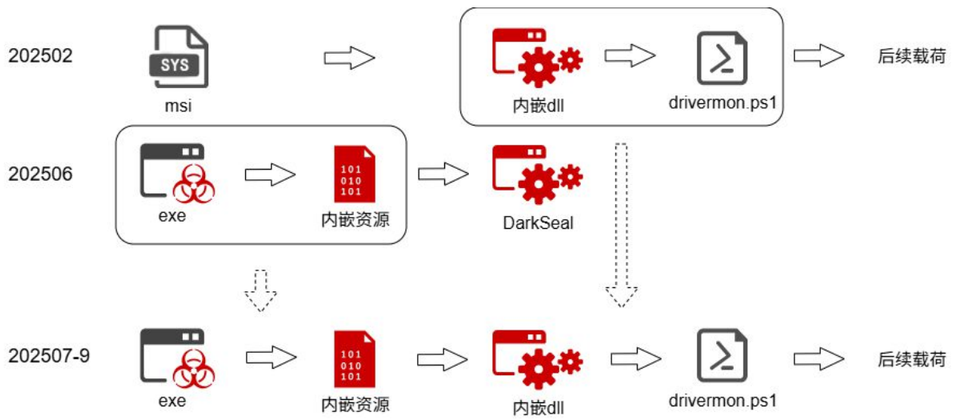
在我们捕获的另外一起攻击活动中，攻击者通过网盘工具、聊天工具和U盘等方式投递伪装成输入法以及伪装成压缩工具的恶意程序，受影响用户分布在朝鲜半岛周边地区。经360高级威胁研究院分析，这两种恶意程序均与APT-C-06（DarkHotel）组织在历史攻击活动中使用的攻击载荷高度相似。

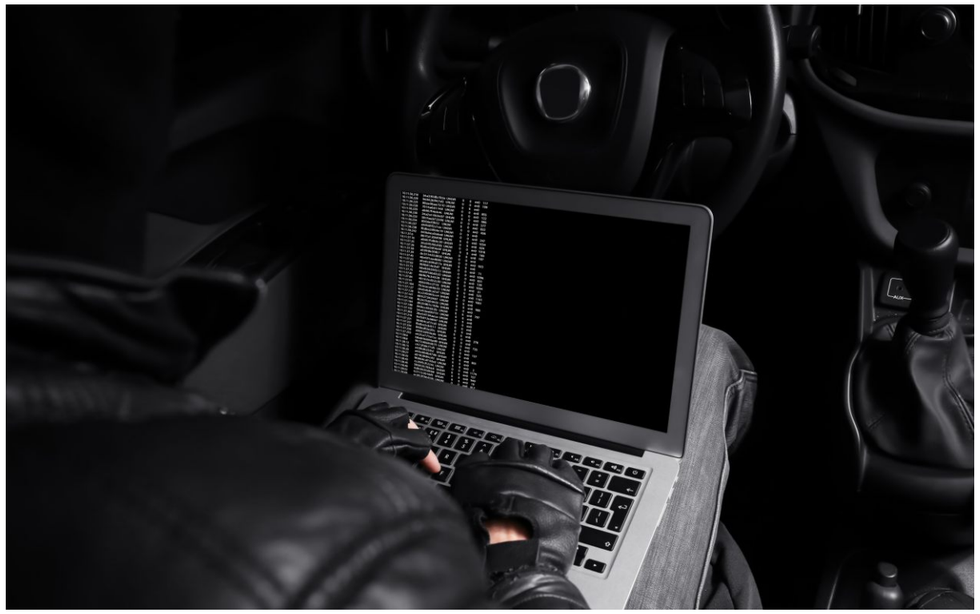


图②

▲ 图①：APT-C-06（DarkHotel）组织攻击流程图 1　图②：APT-C-06（DarkHotel）组织攻击流程图 2

在2025年下半年，APT-C-06（DarkHotel）在6月份使用恶意软件展开一波攻击后，我们又监测到另一波相似的攻击活动。在这次攻击活动中，更多类型的恶意软件出现。这些软件通过U盘接入，进而部署攻击载荷。此次攻击的受影响用户仍是我国和俄罗斯等周边地缘国家的涉朝相关人员。





▲图：APT-C-06（DarkHotel）攻击过程示意图

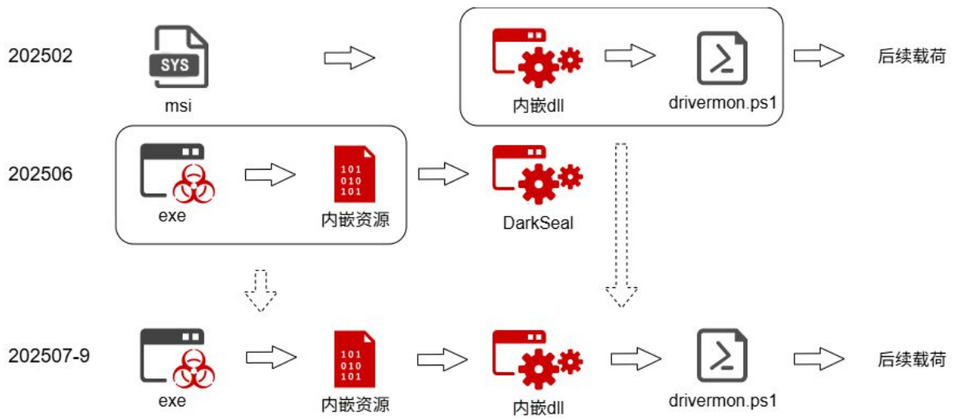
2.2、APT-C-26（Lazarus）

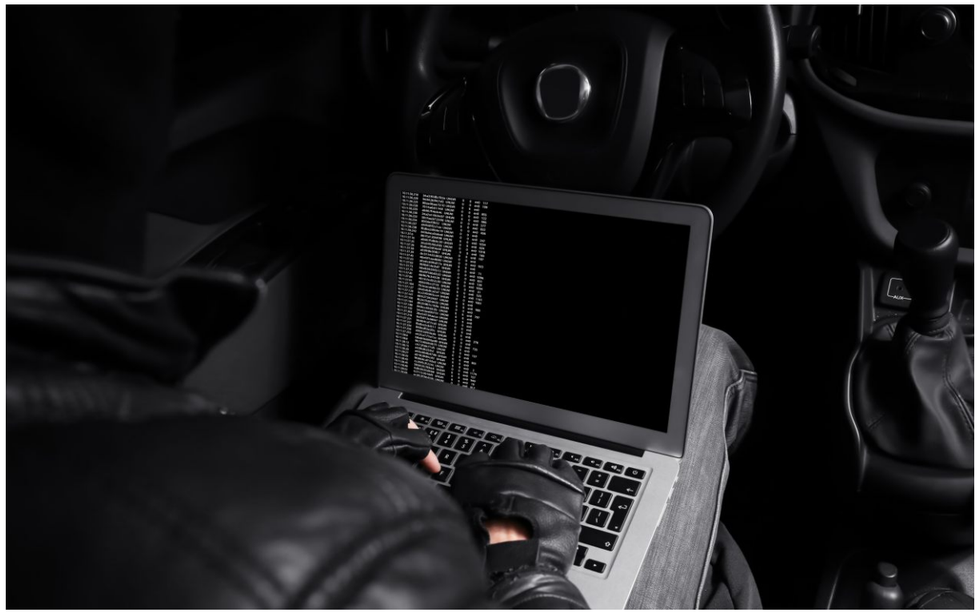
2025年，APT-C-26（Lazarus）组织在全球范围内实施了高度复杂且多元化的网络攻击活动，核心目标聚焦于加密货币盗窃与国防、关键基础设施等战略情报收集。整体攻击战术呈现技术融合化、行动全球化，深度集成AI技术提升社会工程调研和攻击效率。同时利用跨平台恶意软件框架实现全场景覆盖，该组织基础设施覆盖全球多地，通过深度匿名，规避溯源。

2025年，APT-C-26（Lazarus）组织针对加密货币的攻击频繁，影响极大。在2025初，APT-C-26（Lazarus）组织实施了近年来最大的加密货币盗窃案，盗窃Bybit公司超过14.6亿美元，其中包括401,347个以太币。

时间戳（UTC）	事件描述
2025-02-02 01:50:18	攻击者通过Namecheap注册域名getstockprice.com；
2025-02-04 08:55:45	Safe（Wallet）开发者遭到社会工程攻击，账户被入侵；
2025-02-05 08:36:51	攻击者使用获取的AWS访问令牌首次访问Safe（(Wallet)的AWS环境；
2025-02-05 14:06:25	攻击者尝试注册自己的MFA设备，但操作失败；
2025-02-05 至 2025-02-17	攻击者在Safe（Wallet）的AWS环境中进行侦察活动；
2025-02-17 03:22:44	攻击者开始在AWS环境中执行命令和控制活动；
2025-02-19 15:29:25	攻击者在Safe（Wallet）网站中植入恶意JS代码；
2025-02-21 14:13:35	Bybit平台发生恶意交易；
2025-02-21 14:15:13	攻击者删除了Safe（Wallet）网站上的恶意JS代码；
2025-02-21 14:16:11	Bybit平台发生资金盗窃交易。

在2025年下半年，APT-C-06（DarkHotel）在6月份使用恶意软件展开一波攻击后，我们又监测到另一波相似的攻击活动。在这次攻击活动中，更多类型的恶意软件出现。这些软件通过U盘接入，进而部署攻击载荷。此次攻击的受影响用户仍是我国和俄罗斯等周边地缘国家的涉朝相关人员。





▲图：APT-C-06（DarkHotel）攻击过程示意图

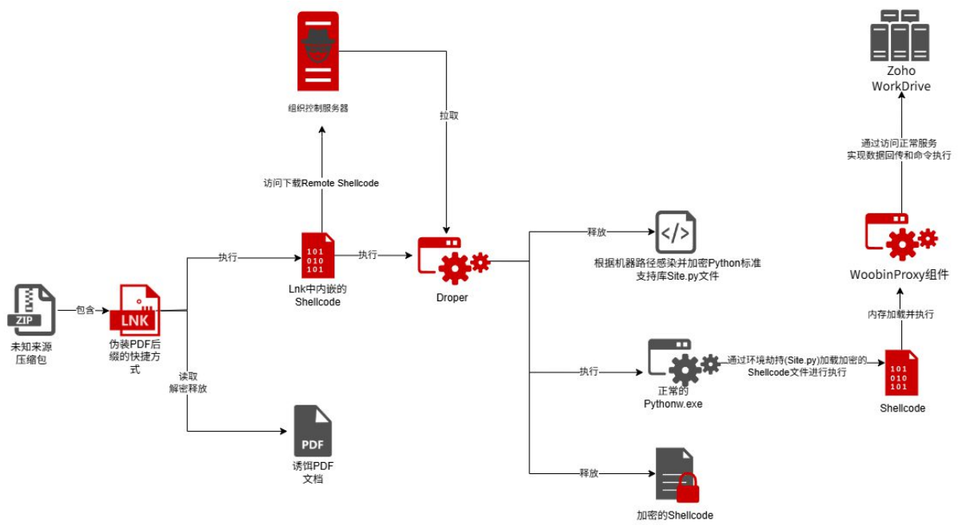
2.2、APT-C-26（Lazarus）

2025年，APT-C-26（Lazarus）组织在全球范围内实施了高度复杂且多元化的网络攻击活动，核心目标聚焦于加密货币盗窃与国防、关键基础设施等战略情报收集。整体攻击战术呈现技术融合化、行动全球化，深度集成AI技术提升社会工程调研和攻击效率。同时利用跨平台恶意软件框架实现全场景覆盖，该组织基础设施覆盖全球多地，通过深度匿名，规避溯源。

2025年，APT-C-26（Lazarus）组织针对加密货币的攻击频繁，影响极大。在2025初，APT-C-26（Lazarus）组织实施了近年来最大的加密货币盗窃案，盗窃Bybit公司超过14.6亿美元，其中包括401,347个以太币。

时间戳（UTC）	事件描述
2025-02-02 01:50:18	攻击者通过Namecheap注册域名getstockprice.com；
2025-02-04 08:55:45	Safe（Wallet）开发者遭到社会工程攻击，账户被入侵；
2025-02-05 08:36:51	攻击者使用获取的AWS访问令牌首次访问Safe（(Wallet)的AWS环境；
2025-02-05 14:06:25	攻击者尝试注册自己的MFA设备，但操作失败；
2025-02-05 至 2025-02-17	攻击者在Safe（Wallet）的AWS环境中进行侦察活动；
2025-02-17 03:22:44	攻击者开始在AWS环境中执行命令和控制活动；
2025-02-19 15:29:25	攻击者在Safe（Wallet）网站中植入恶意JS代码；
2025-02-21 14:13:35	Bybit平台发生恶意交易；
2025-02-21 14:15:13	攻击者删除了Safe（Wallet）网站上的恶意JS代码；
2025-02-21 14:16:11	Bybit平台发生资金盗窃交易。

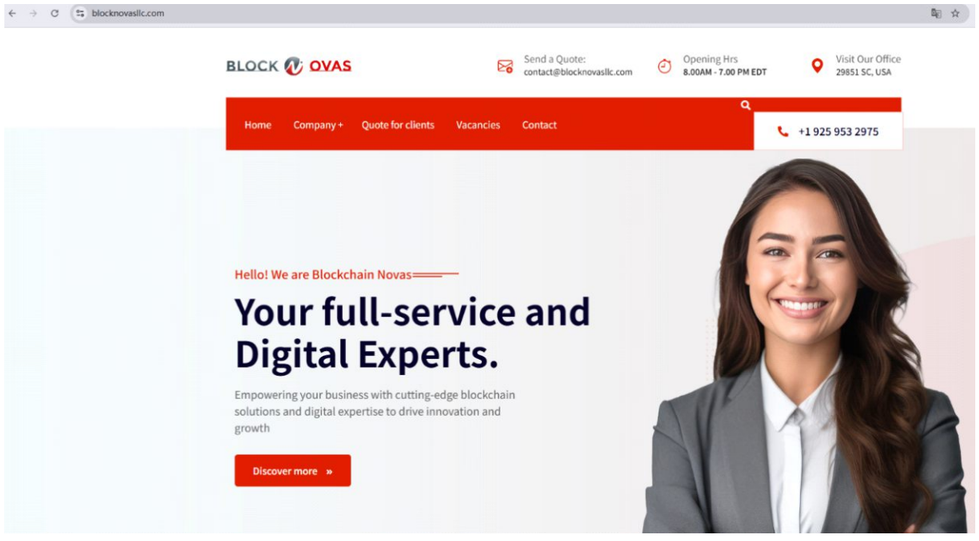
360高级威胁研究院捕获到了APT-C-26（Lazarus）组织从2025年10月开始，针对加密货币行业从业人员投递的一款名为WoobinProxy的复杂多功能后门组件。攻击者通常利用伪装成招聘文档的恶意LNK文件进行初始投递，通过多层Shellcode加载与远程下载技术释放载荷。该组件具备极高的隐蔽性，功能上集成了系统信息收集、键盘记录、屏幕监控、浏览器数据窃取及全盘文件枚举等全面的后门能力，并滥用Zoho WorkDrive等合法云服务作为C2通信通道，规避安全检测。



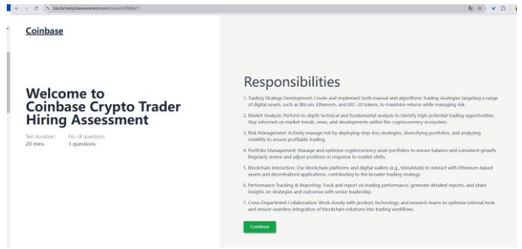
图①

▲图：APT-C-26（Lazarus）组织对加密货币的攻击流程示意图

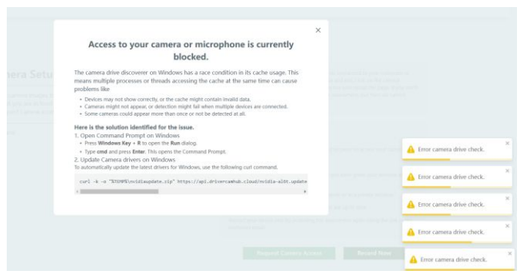
APT-C-26（Lazarus）组织极为擅长伪装，构造的虚假企业足以以假乱真。他们在攻击活动中投递虚假的项目库、NPM库，伪造虚假的面试邀约向目标软件开发人员投放恶意载荷。



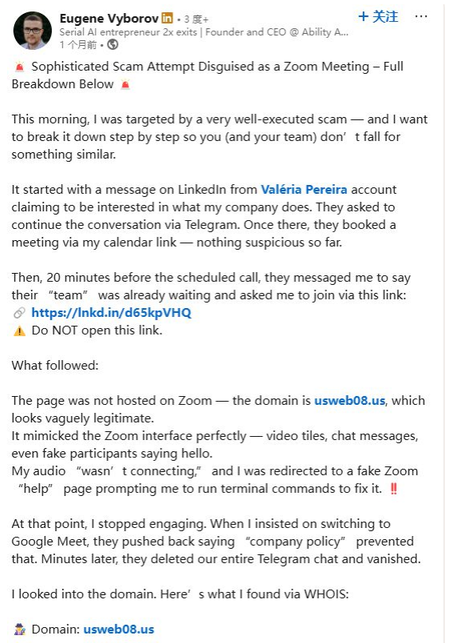
图①



图②



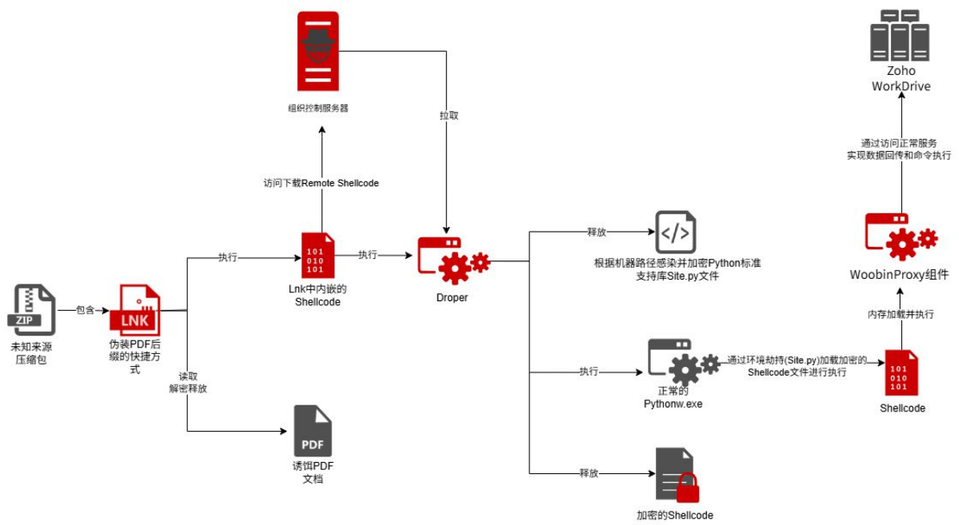
图③



图④

▲图①：APT-C-26（Lazarus）组织伪造的虚假公司官网　图②：APT-C-26（Lazarus）组织虚假的招聘网站
图③：APT-C-26（Lazarus）组织诱导面试人员执行恶意命令　图④：被攻击者自述

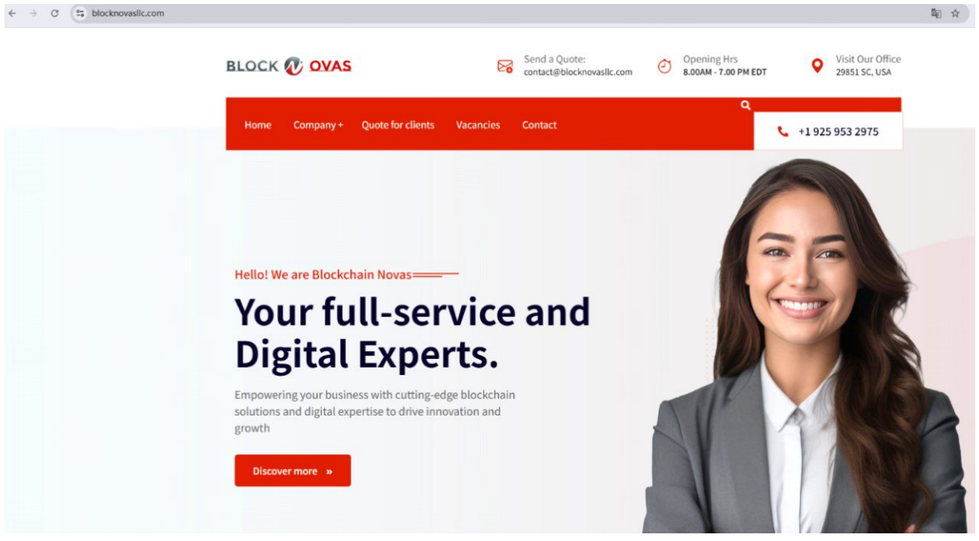
360高级威胁研究院捕获到了APT-C-26（Lazarus）组织从2025年10月开始，针对加密货币行业从业人员投递的一款名为WoobinProxy的复杂多功能后门组件。攻击者通常利用伪装成招聘文档的恶意LNK文件进行初始投递，通过多层Shellcode加载与远程下载技术释放载荷。该组件具备极高的隐蔽性，功能上集成了系统信息收集、键盘记录、屏幕监控、浏览器数据窃取及全盘文件枚举等全面的后门能力，并滥用Zoho WorkDrive等合法云服务作为C2通信通道，规避安全检测。



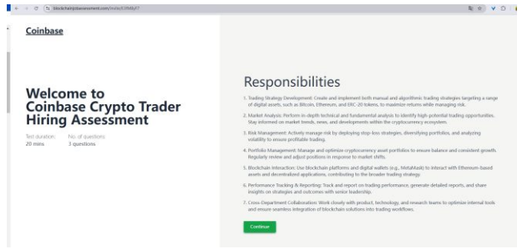
图①

▲图：APT-C-26（Lazarus）组织对加密货币的攻击流程示意图

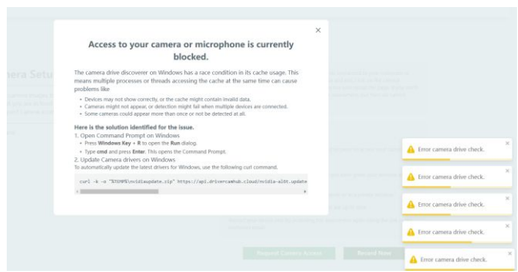
APT-C-26（Lazarus）组织极为擅长伪装，构造的虚假企业足以以假乱真。他们在攻击活动中投递虚假的项目库、NPM库，伪造虚假的面试邀约向目标软件开发人员投放恶意载荷。



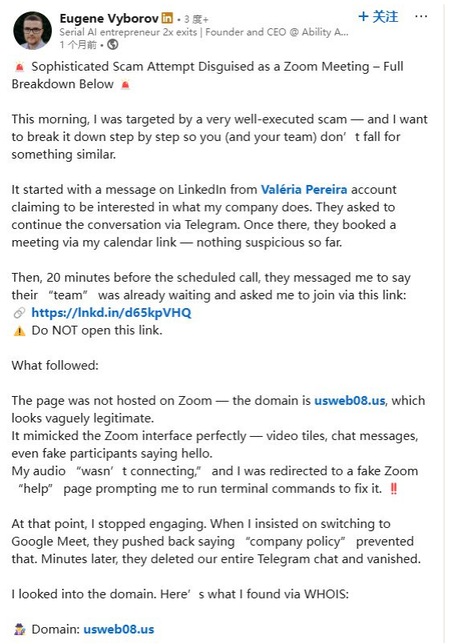
图①



图②



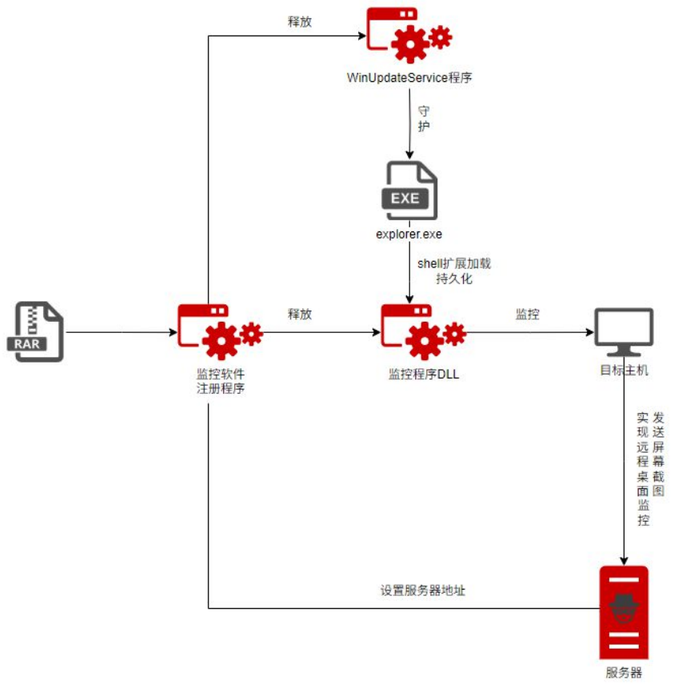
图③



图④

▲图①：APT-C-26（Lazarus）组织伪造的虚假公司官网　图②：APT-C-26（Lazarus）组织虚假的招聘网站
图③：APT-C-26（Lazarus）组织诱导面试人员执行恶意命令　图④：被攻击者自述

我们在追踪该组织的过程中捕获到该组织使用的一款功能完备的定制化监控程序，具备完整的远程桌面控制能力。通过分析发现，该组织中这些被派遣的远程IT人员在成功入职目标企业后，极有可能利用此类监控工具，在不触发警报的前提下，对所在企业的敏感数据进行隐蔽窃取。此类行为不仅威胁企业数据安全，更可能为该组织的后续网络攻击行动积累战略资源。



2.3、APT-C-47（旺刺）

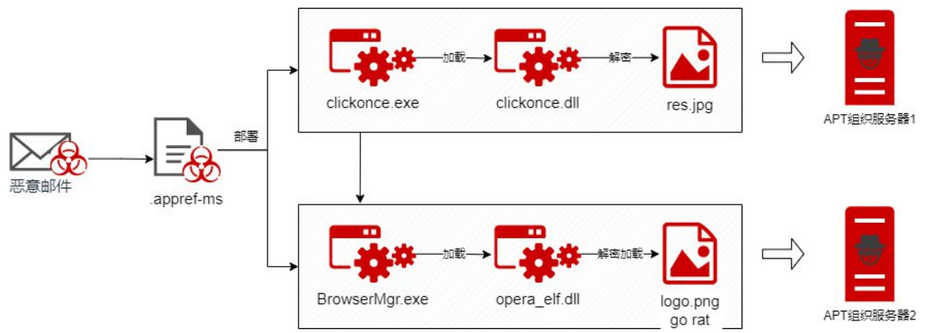
2025年4月，我们监测到APT-C-47（旺刺）组织新的攻击活动。攻击者使用ClickOnce技术投递下一阶段载荷。

我们监测发现APT-C-47（旺刺）组织在攻击活动使用了知识产权行业相关的专利和商标律师事务所的收费表，以及英国某知识产权监管委员会的仿冒内容。由此推断APT-C-47（旺刺）组织疑似以知识产权为支点，对科研相关领域进行有计划地攻击渗透。

▲图：APT-C-26（Lazarus）组织攻击流程示意图

图①

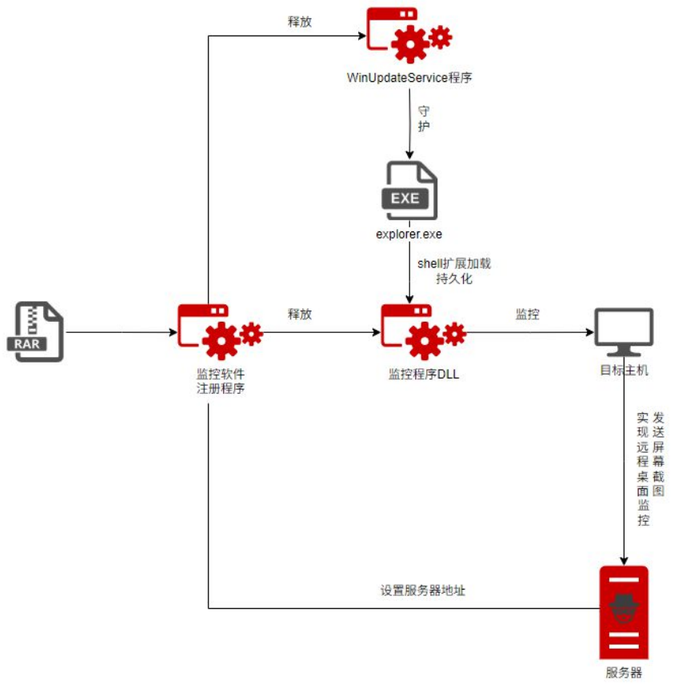
此次攻击活动中，攻击者通过ClickOnce部署了两部分载荷，第一组载荷的主要功能是将第二组攻击组件拷贝到特定目录下，然后执行、设置持久化、上传主机信息。第二组载荷通过白利用于内存中装载远控木马。



图②

▲图①：APT-C-47（旺刺）组织仿冒律师机构广告　图②：APT-C-47（旺刺）组织攻击流程示意图

我们在追踪该组织的过程中捕获到该组织使用的一款功能完备的定制化监控程序，具备完整的远程桌面控制能力。通过分析发现，该组织中这些被派遣的远程IT人员在成功入职目标企业后，极有可能利用此类监控工具，在不触发警报的前提下，对所在企业的敏感数据进行隐蔽窃取。此类行为不仅威胁企业数据安全，更可能为该组织的后续网络攻击行动积累战略资源。



2.3、APT-C-47（旺刺）

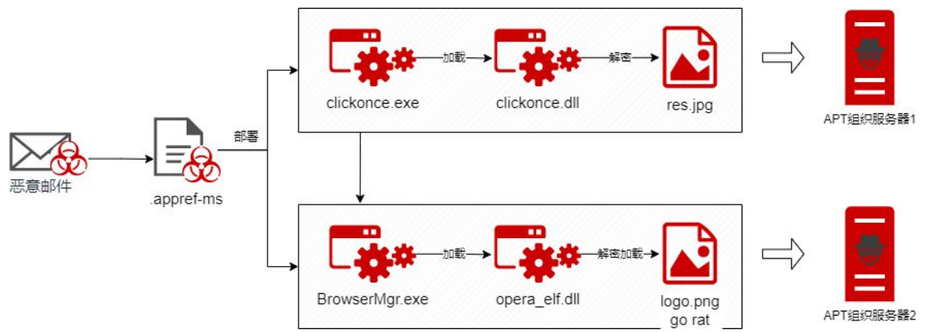
2025年4月，我们监测到APT-C-47（旺刺）组织新的攻击活动。攻击者使用ClickOnce技术投递下一阶段载荷。

我们监测发现APT-C-47（旺刺）组织在攻击活动使用了知识产权行业相关的专利和商标律师事务所的收费表，以及英国某知识产权监管委员会的仿冒内容。由此推断APT-C-47（旺刺）组织疑似以知识产权为支点，对科研相关领域进行有计划地攻击渗透。

▲图：APT-C-26（Lazarus）组织攻击流程示意图

图①

此次攻击活动中，攻击者通过ClickOnce部署了两部分载荷，第一组载荷的主要功能是将第二组攻击组件拷贝到特定目录下，然后执行、设置持久化、上传主机信息。第二组载荷通过白利用于内存中装载远控木马。



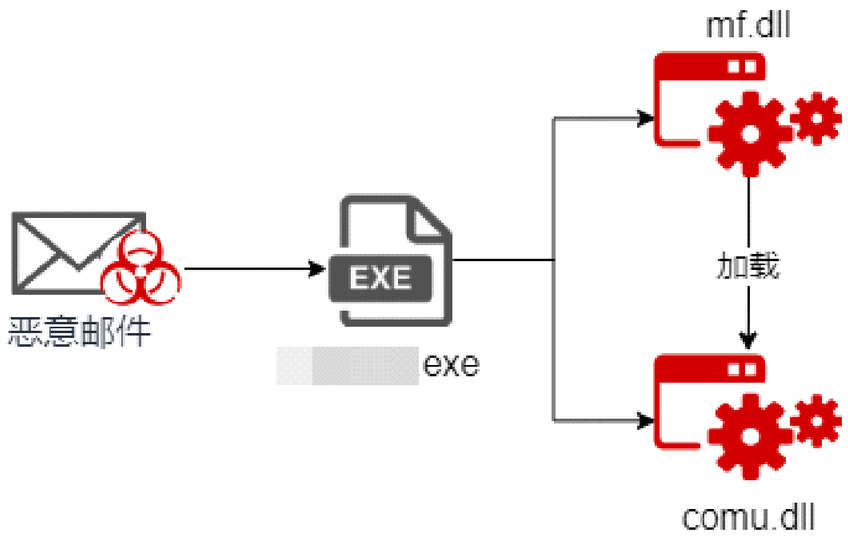
图②

▲图①：APT-C-47（旺刺）组织仿冒律师机构广告　图②：APT-C-47（旺刺）组织攻击流程示意图

2.4、APT-C-60（伪猎者）

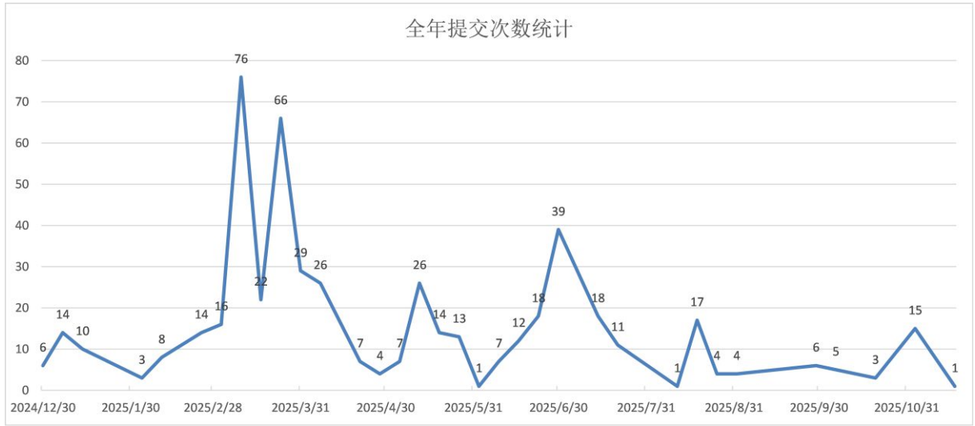
在2025年，APT-C-60（伪猎者）组织主要使用诱饵文档，对我国驻外相关机构，以及科研单位等目标展开钓鱼攻击；尤其在一些重大国际活动中，针对性攻击明显增加。该组织储备了大量的0day漏洞，历史上多次使用0day漏洞开展网络攻击。

我们通过监测发现APT-C-60（伪猎者）在2024年，该组织利用国产文档编辑软件的0day漏洞开展了钓鱼攻击；同年，我们还捕获到利用某邮件客户端0day漏洞针对我国涉朝目标展开攻击；在2025年9月初，我们又发现该组织利用国内某邮件服务商0day漏洞对目标人员开展攻击。这些针对国产应用软件漏洞开展的攻击，对国产应用软件环境造成不良影响。



▲图：APT-C-60（伪猎者）利用邮件漏洞攻击流程示意图

APT-C-60（伪猎者）组织在2025年攻击活动的一大特点是使用了GitHub作为载荷托管的主要站点。截止2025年底我们观测到该组织涉及的27个仓库，进行了524次提交。



2.5、其他APT组织

朝鲜半岛地区APT组织众多、攻击活跃，APT-C-28（ScarCruft）组织、APT-C-55（Kimsuky）组织长期针对韩国政府机构及朝鲜半岛事务相关部门进行网络攻击。

2.5.1、APT-C-28（ScarCruft）

2025年，APT-C-28（ScarCruft）组织将韩国作为核心作战目标，重点针对涉朝政治、外交、人权与学术研究领域个体以及学者、研究员、活动人士、心理辅导师、脱北者支援人员等小圈层；以韩文政治/招聘为主题诱饵，仿冒公共机构提升可信度，并逐渐将诱饵主题延伸至国家安全与情报相关主题。此外，360高级威胁研究院还捕获了APT-C-28（ScarCruft）组织持续使用的GoldBackDoor组件针对我国驻外机构相关目标进行网络攻击。

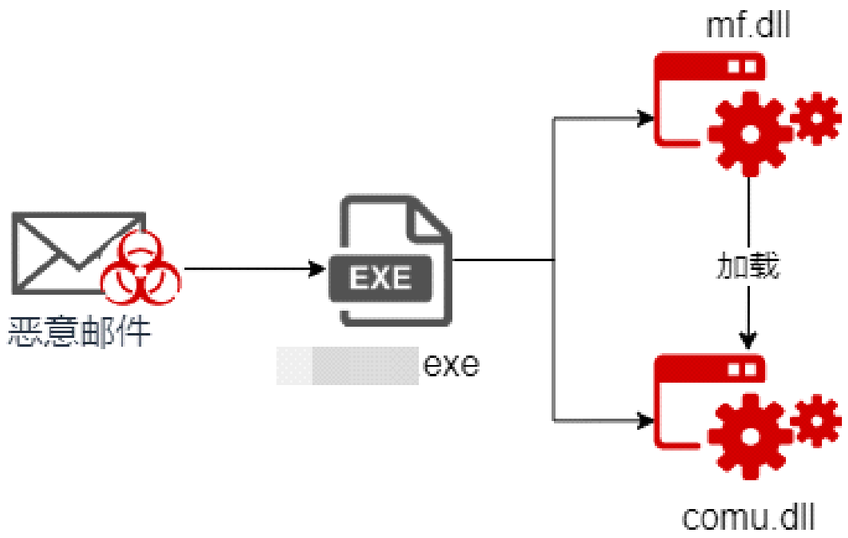
在攻击手段方面，该组织显著提升跨平台攻击能力，利用云服务分发恶意负载，并动态更新C2指令，有效规避IP黑名单。另外，在攻击过程中还采用无文件攻击、多阶段混淆及虚拟机检测机制躲避安全工具检测。

▲图：APT-C-60（伪猎者）组织载荷托管更新统计

2.4、APT-C-60（伪猎者）

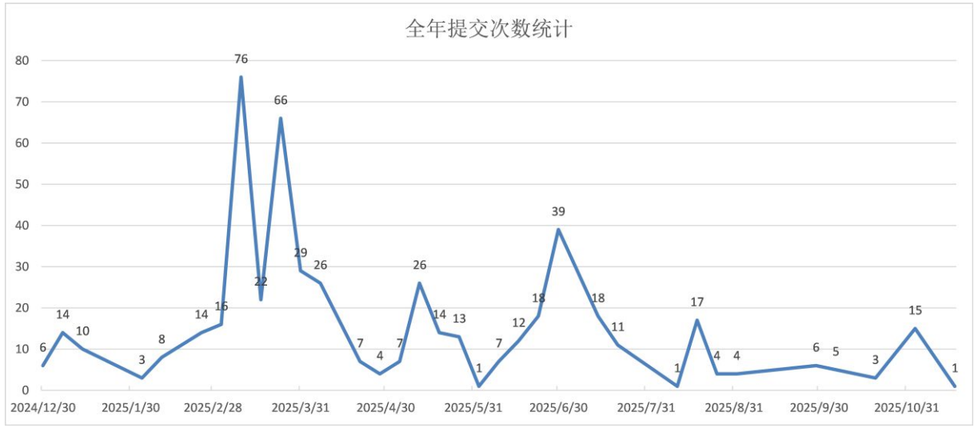
在2025年，APT-C-60（伪猎者）组织主要使用诱饵文档，对我国驻外相关机构，以及科研单位等目标展开钓鱼攻击；尤其在一些重大国际活动中，针对性攻击明显增加。该组织储备了大量的0day漏洞，历史上多次使用0day漏洞开展网络攻击。

我们通过监测发现APT-C-60（伪猎者）在2024年，该组织利用国产文档编辑软件的0day漏洞开展了钓鱼攻击；同年，我们还捕获到利用某邮件客户端0day漏洞针对我国涉朝目标展开攻击；在2025年9月初，我们又发现该组织利用国内某邮件服务商0day漏洞对目标人员开展攻击。这些针对国产应用软件漏洞开展的攻击，对国产应用软件环境造成不良影响。



▲图：APT-C-60（伪猎者）利用邮件漏洞攻击流程示意图

APT-C-60（伪猎者）组织在2025年攻击活动的一大特点是使用了GitHub作为载荷托管的主要站点。截止2025年底我们观测到该组织涉及的27个仓库，进行了524次提交。



2.5、其他APT组织

朝鲜半岛地区APT组织众多、攻击活跃，APT-C-28（ScarCruft）组织、APT-C-55（Kimsuky）组织长期针对韩国政府机构及朝鲜半岛事务相关部门进行网络攻击。

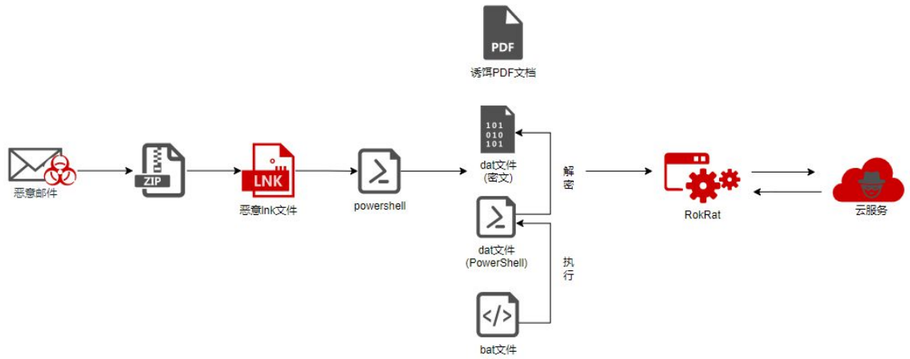
2.5.1、APT-C-28（ScarCruft）

2025年，APT-C-28（ScarCruft）组织将韩国作为核心作战目标，重点针对涉朝政治、外交、人权与学术研究领域个体以及学者、研究员、活动人士、心理辅导师、脱北者支援人员等小圈层；以韩文政治/招聘为主题诱饵，仿冒公共机构提升可信度，并逐渐将诱饵主题延伸至国家安全与情报相关主题。此外，360高级威胁研究院还捕获了APT-C-28（ScarCruft）组织持续使用的GoldBackDoor组件针对我国驻外机构相关目标进行网络攻击。

在攻击手段方面，该组织显著提升跨平台攻击能力，利用云服务分发恶意负载，并动态更新C2指令，有效规避IP黑名单。另外，在攻击过程中还采用无文件攻击、多阶段混淆及虚拟机检测机制躲避安全工具检测。

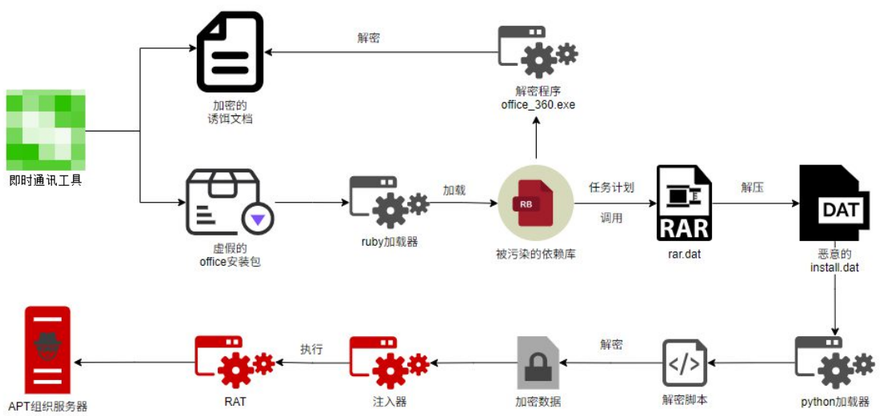
▲图：APT-C-60（伪猎者）组织载荷托管更新统计

我们还捕获了APT-C-28（ScarCruft）组织针对韩国政府及企业人员、朝鲜人权组织和脱北者的多次威胁活动。在这些活动中攻击者通过分发LNK恶意文件，采用无文件技术，向目标系统植入RokRat恶意软件。



图①

我们同时监测到APT-C-28（ScarCruft）组织利用虚假的Office安装包对受害者展开攻击活动。攻击者通过通信工具与目标用户建立联系，在取得信任后，发送加密诱饵文件和虚假安装包。这些诱饵文件在用户执行恶意安装包后被解密，同时恶意安装包会释放后门程序，窃取用户信息。



图②

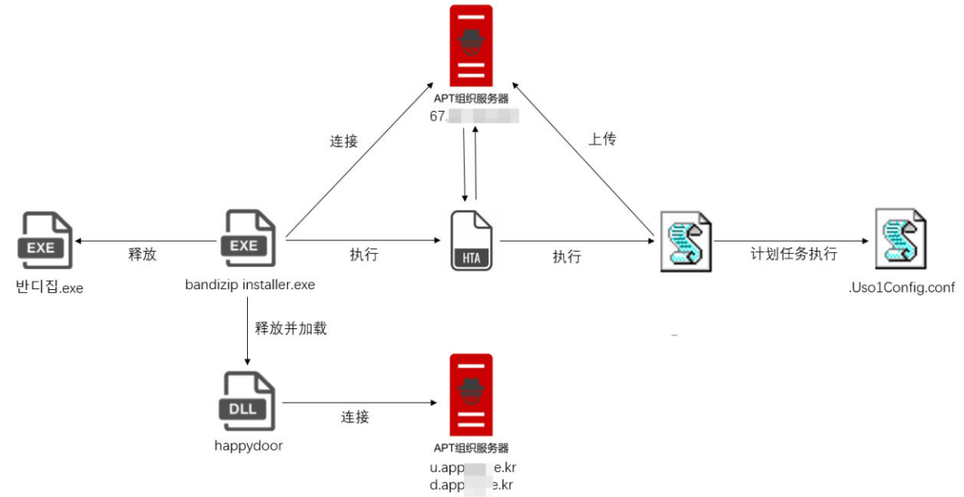
▲图①：APT-C-28（ScarCruft）组织攻击流程示意图　图②：APT-C-28（ScarCruft）组织攻击流程示意图

2.5.2、APT-C-55（Kimsuky）

2025年，APT-C-55（Kimsuky）组织主要攻击目标行业涉及韩国政府及与朝鲜半岛事务相关的政府、外交、国家安全机构、教育与研究机构、企业与金融等机构，以及加密货币领域。攻击目标从高价值机构人员逐步横向扩展到大众平台用户与加密货币生态。同时，我们还观察到该组织长期针对我国学术、外交等领域实施定向渗透，攻击活动隐蔽且持续。

在2025年，APT-C-55（Kimsuky）组织攻击武器显著更新。在移动端，APT-C-55（Kimsuky）组织以短信与二维码为入口，并结合物流、拍卖、VPN、空投等高可信度场景诱导安装，辅以门户登录仿冒与招聘站点钓鱼，实现凭证批量收集。在战术上延续鱼叉式邮件与LNK/HTA链路相结合的方式，C2服务采用HTTP POST与ID指令协议、Base64+XOR通信混淆实现通信保护；同时，还利用GitHub/Dropbox等云基础设施作为访问跳板。

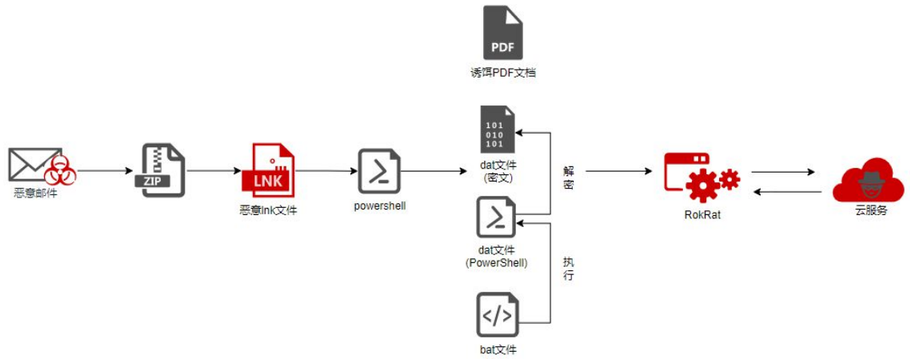
在360高级威胁研究院捕获到的APT-C-55（Kimsuky）针对韩国地区的攻击行动中。该组织通过下发伪装成bandizip的安装包远程加载恶意代码执行，释放VMP壳的HappyDoor木马用于窃密行动。



我们整理并总结了APT-C-55（Kimsuky）组织的三条主要攻击链路，发现其在战术手法、基础设施与载荷特征上高度关联，具备统一的行动模式与技术传承，因此我们对其进行统一归因与持续追踪。

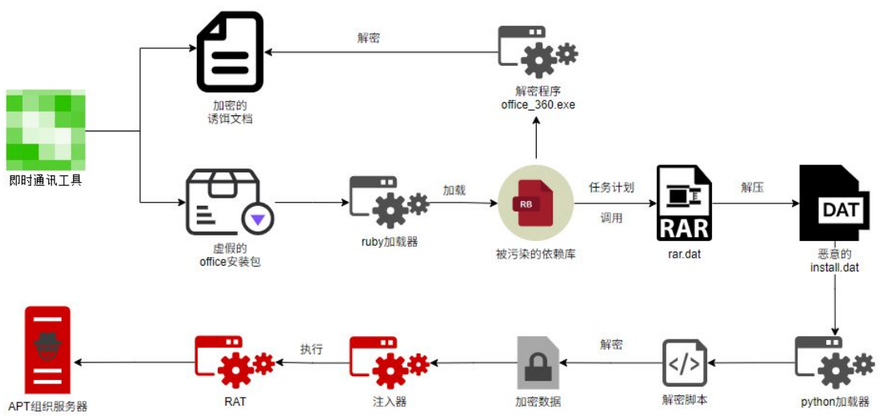
▲图：APT-C-55（Kimsuky）组织攻击流程示意图

我们还捕获了APT-C-28（ScarCruft）组织针对韩国政府及企业人员、朝鲜人权组织和脱北者的多次威胁活动。在这些活动中攻击者通过分发LNK恶意文件，采用无文件技术，向目标系统植入RokRat恶意软件。



图①

我们同时监测到APT-C-28（ScarCruft）组织利用虚假的Office安装包对受害者展开攻击活动。攻击者通过通信工具与目标用户建立联系，在取得信任后，发送加密诱饵文件和虚假安装包。这些诱饵文件在用户执行恶意安装包后被解密，同时恶意安装包会释放后门程序，窃取用户信息。



图②

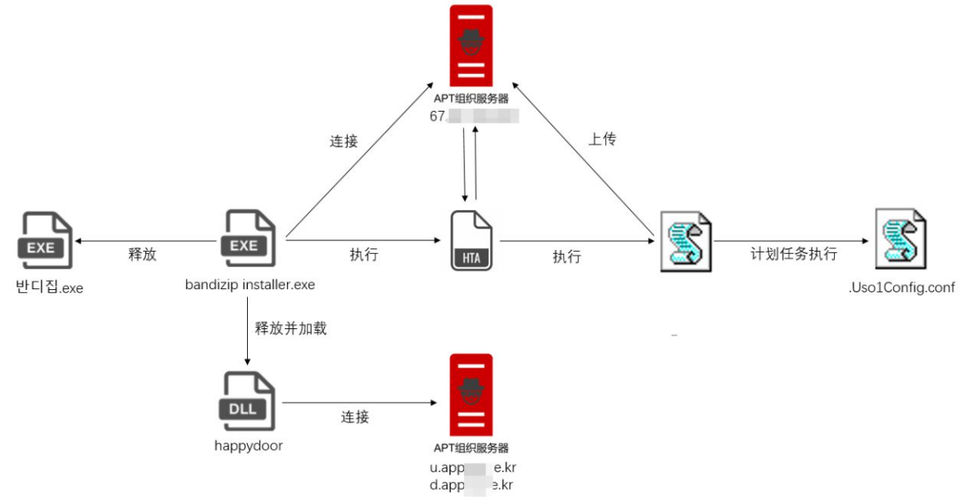
▲图①：APT-C-28（ScarCruft）组织攻击流程示意图　图②：APT-C-28（ScarCruft）组织攻击流程示意图

2.5.2、APT-C-55（Kimsuky）

2025年，APT-C-55（Kimsuky）组织主要攻击目标行业涉及韩国政府及与朝鲜半岛事务相关的政府、外交、国家安全机构、教育与研究机构、企业与金融等机构，以及加密货币领域。攻击目标从高价值机构人员逐步横向扩展到大众平台用户与加密货币生态。同时，我们还观察到该组织长期针对我国学术、外交等领域实施定向渗透，攻击活动隐蔽且持续。

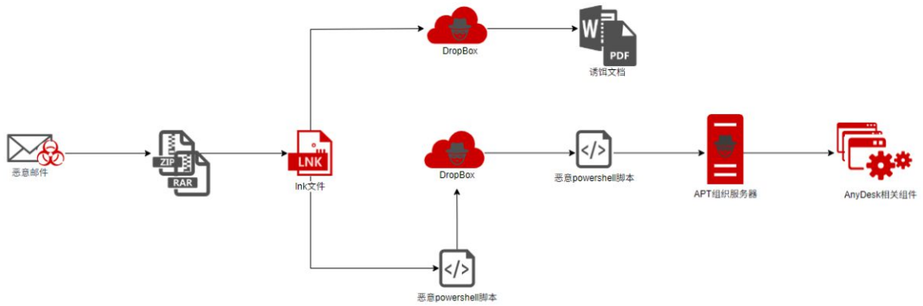
在2025年，APT-C-55（Kimsuky）组织攻击武器显著更新。在移动端，APT-C-55（Kimsuky）组织以短信与二维码为入口，并结合物流、拍卖、VPN、空投等高可信度场景诱导安装，辅以门户登录仿冒与招聘站点钓鱼，实现凭证批量收集。在战术上延续鱼叉式邮件与LNK/HTA链路相结合的方式，C2服务采用HTTP POST与ID指令协议、Base64+XOR通信混淆实现通信保护；同时，还利用GitHub/Dropbox等云基础设施作为访问跳板。

在360高级威胁研究院捕获到的APT-C-55（Kimsuky）针对韩国地区的攻击行动中。该组织通过下发伪装成bandizip的安装包远程加载恶意代码执行，释放VMP壳的HappyDoor木马用于窃密行动。

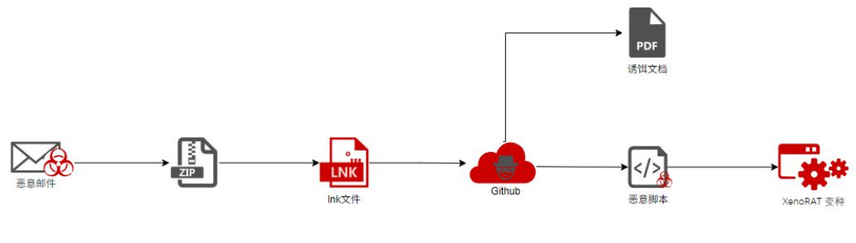


我们整理并总结了APT-C-55（Kimsuky）组织的三条主要攻击链路，发现其在战术手法、基础设施与载荷特征上高度关联，具备统一的行动模式与技术传承，因此我们对其进行统一归因与持续追踪。

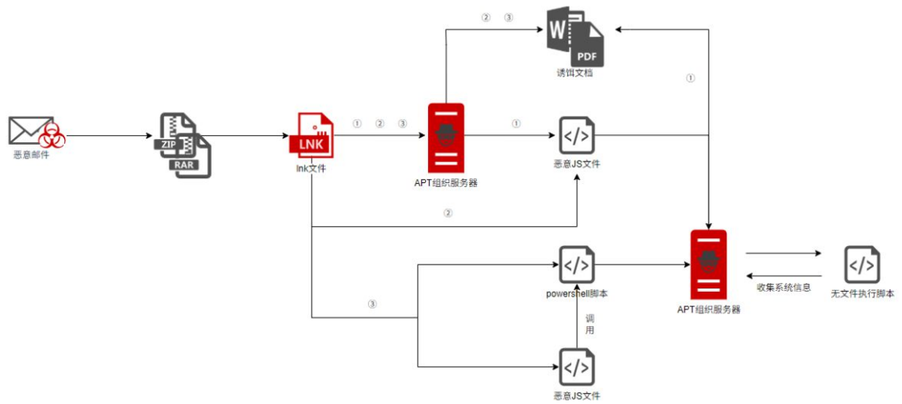
▲图：APT-C-55（Kimsuky）组织攻击流程示意图



图①



图②



图③

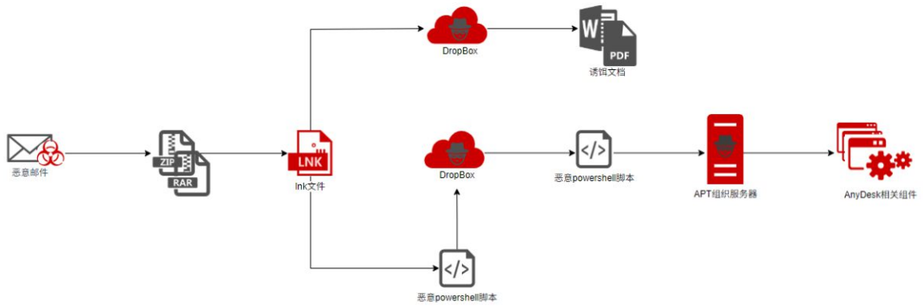
▲图①：DropBox链路攻击流程示意图　图②：Github链路攻击流程示意图　图③：服务器链路攻击流程示意图

3、中国台湾省

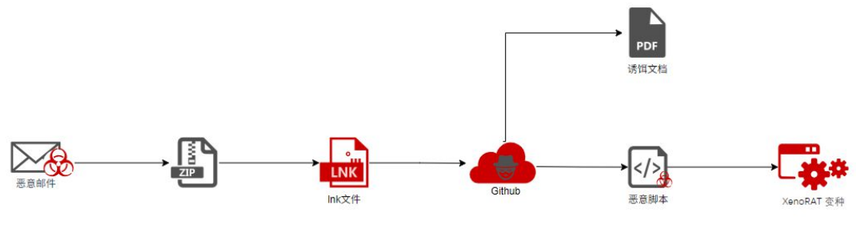
2025年6月，国家计算机病毒应急处理中心在《“蚍蜉撼树”——台民进党当局“资通电军”黑客组织网络攻击活动调查报告》中披露了中国台湾省民进党当局支持的黑客组织，充当反华势力爪牙，长期针对我国政府机构、科研单位、高等院校、国防科技企业等实施网络间谍活动。网络攻击渗透成为“台独”和外部干涉势力的政治工具，对我国网络空间安全构成多重威胁。

2025年台海局势复杂严峻，充满挑战。在此期间，我国台湾省地区APT-C-01（毒云藤）、APT-C-67（乌苏拉）等网络组织持续活跃，意图通过网络攻击窃取国家重要政策、国防军工技术、尖端科技成果、国民经济运行数据等敏感数据信息；APT-C-64（匿名者64）组织还妄图通过攻击数字媒体服务系统，破坏社会公共秩序，制造混乱。

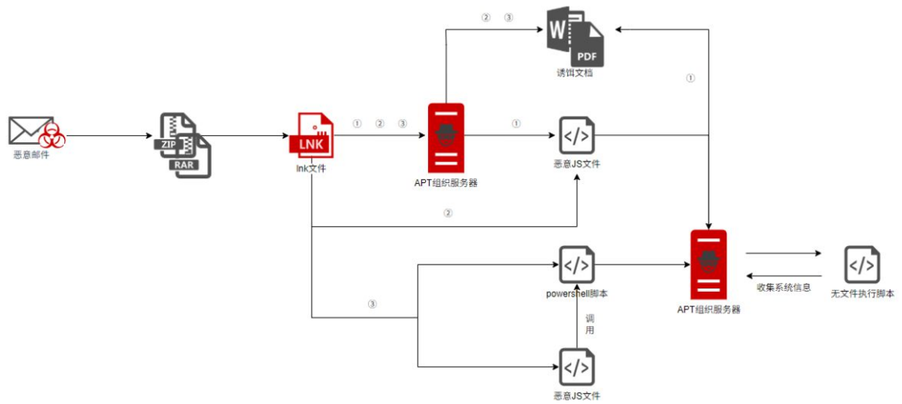
我国统一的大势不可阻挡，在通过法律、军事等手段坚决反制“台独”分裂行径的同时，也需不断警惕和防御来自网络空间的渗透与攻击活动。



图①



图②



图③

▲图①：DropBox链路攻击流程示意图　图②：Github链路攻击流程示意图　图③：服务器链路攻击流程示意图

3、中国台湾省

2025年6月，国家计算机病毒应急处理中心在《“蚍蜉撼树”——台民进党当局“资通电军”黑客组织网络攻击活动调查报告》中披露了中国台湾省民进党当局支持的黑客组织，充当反华势力爪牙，长期针对我国政府机构、科研单位、高等院校、国防科技企业等实施网络间谍活动。网络攻击渗透成为“台独”和外部干涉势力的政治工具，对我国网络空间安全构成多重威胁。

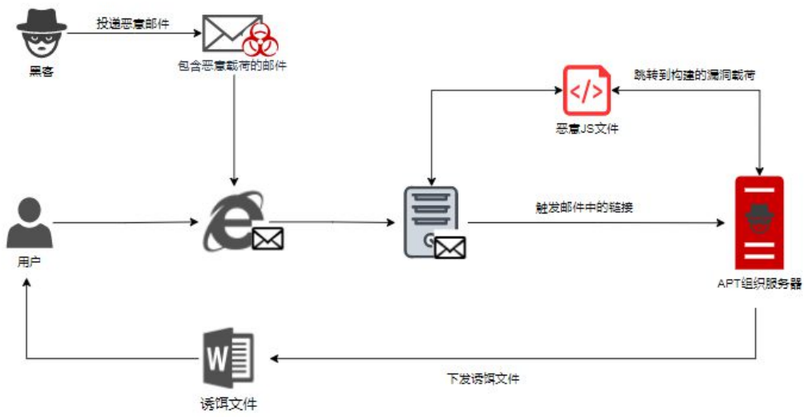
2025年台海局势复杂严峻，充满挑战。在此期间，我国台湾省地区APT-C-01（毒云藤）、APT-C-67（乌苏拉）等网络组织持续活跃，意图通过网络攻击窃取国家重要政策、国防军工技术、尖端科技成果、国民经济运行数据等敏感数据信息；APT-C-64（匿名者64）组织还妄图通过攻击数字媒体服务系统，破坏社会公共秩序，制造混乱。

我国统一的大势不可阻挡，在通过法律、军事等手段坚决反制“台独”分裂行径的同时，也需不断警惕和防御来自网络空间的渗透与攻击活动。

3.1、APT-C-01（毒云藤）

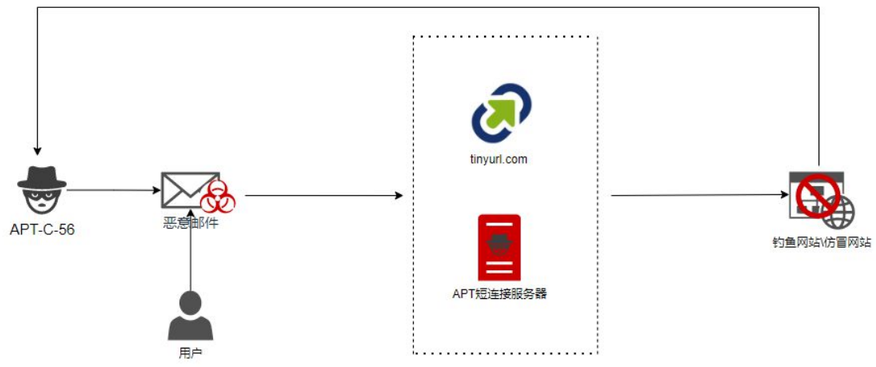
2025年，APT-C-01（毒云藤）组织持续通过针对性钓鱼攻击，对我国政府机构、国防军工、科研教育等多个重要行业领域展开攻击窃密。

在《反分裂国家法》颁布20周年之际，360监测到APT-C-01（毒云藤）组织利用国内某头部邮箱平台0day漏洞实施网络钓鱼攻击。当用户访问相关钓鱼页面链接后无需用户其他操作，目标用户邮箱登录凭证等信息即被攻击者窃取。该攻击手法较之前传统钓鱼窃密更加隐蔽，成功率更高。



图①

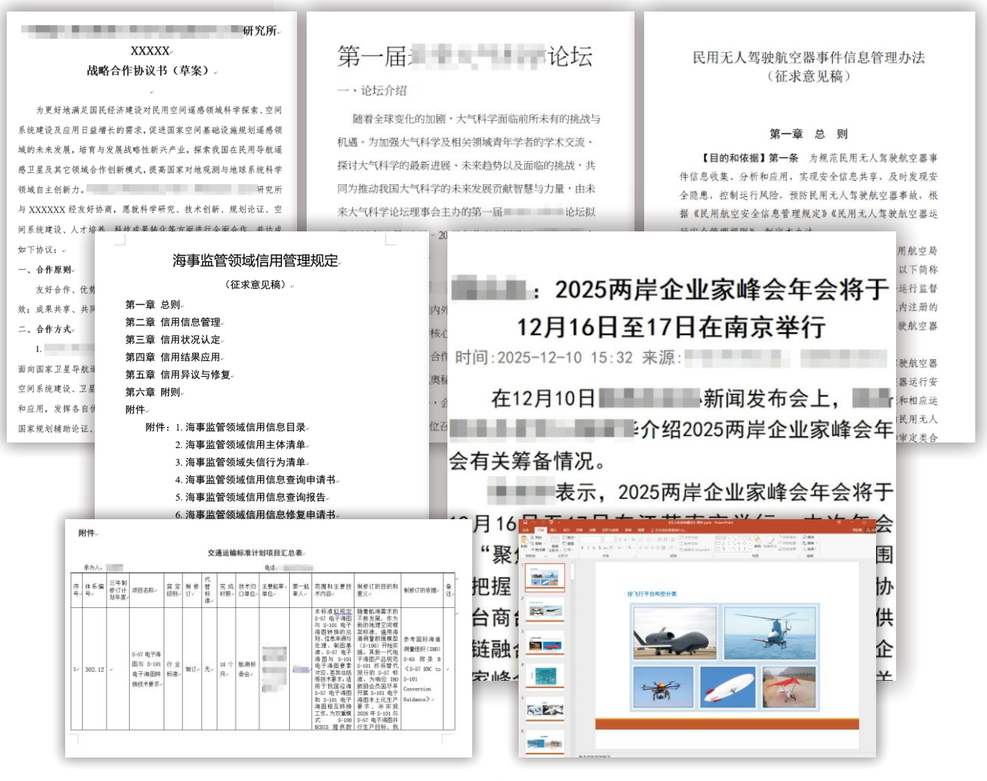
2025年里，我们观测到APT-C-01（毒云藤）组织钓鱼攻击活动中，钓鱼网站部署变得更加隐蔽。攻击者使用短链接服务进行中转，以短链接服务的时效性让攻击者的服务器更加隐蔽。



图②

▲图①：APT-C-01（毒云藤）组织攻击流程示意图1　图②：APT-C-01（毒云藤）组织攻击流程示意图2

图①



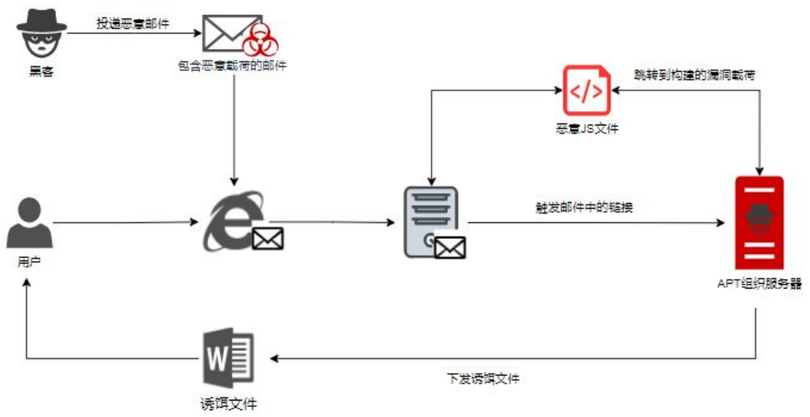
图②

▲图①：APT-C-01（毒云藤）组织近期使用钓鱼文档主题关键词　图②：APT-C-01（毒云藤）组织近期使用的钓鱼文档

3.1、APT-C-01（毒云藤）

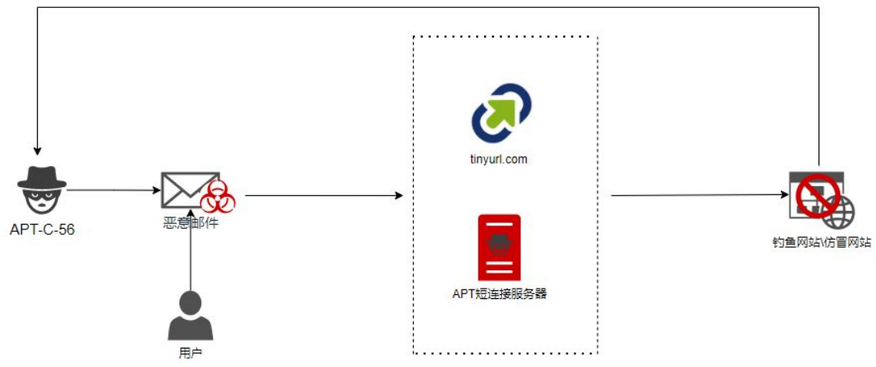
2025年，APT-C-01（毒云藤）组织持续通过针对性钓鱼攻击，对我国政府机构、国防军工、科研教育等多个重要行业领域展开攻击窃密。

在《反分裂国家法》颁布20周年之际，360监测到APT-C-01（毒云藤）组织利用国内某头部邮箱平台0day漏洞实施网络钓鱼攻击。当用户访问相关钓鱼页面链接后无需用户其他操作，目标用户邮箱登录凭证等信息即被攻击者窃取。该攻击手法较之前传统钓鱼窃密更加隐蔽，成功率更高。



图①

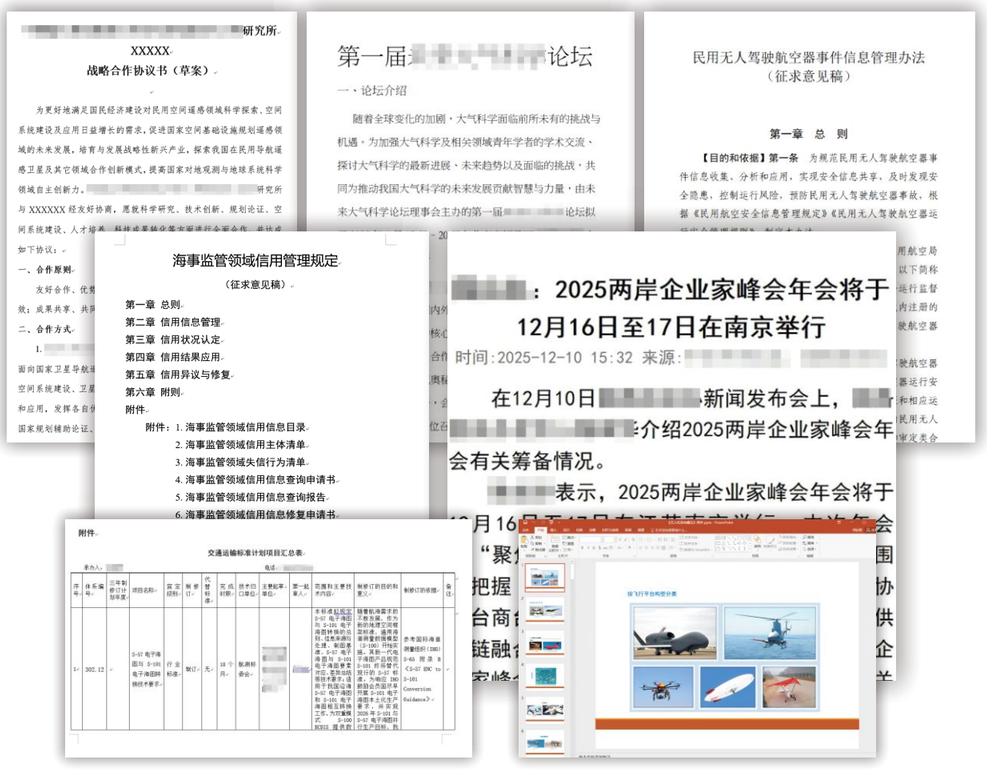
2025年里，我们观测到APT-C-01（毒云藤）组织钓鱼攻击活动中，钓鱼网站部署变得更加隐蔽。攻击者使用短链接服务进行中转，以短链接服务的时效性让攻击者的服务器更加隐蔽。



图②

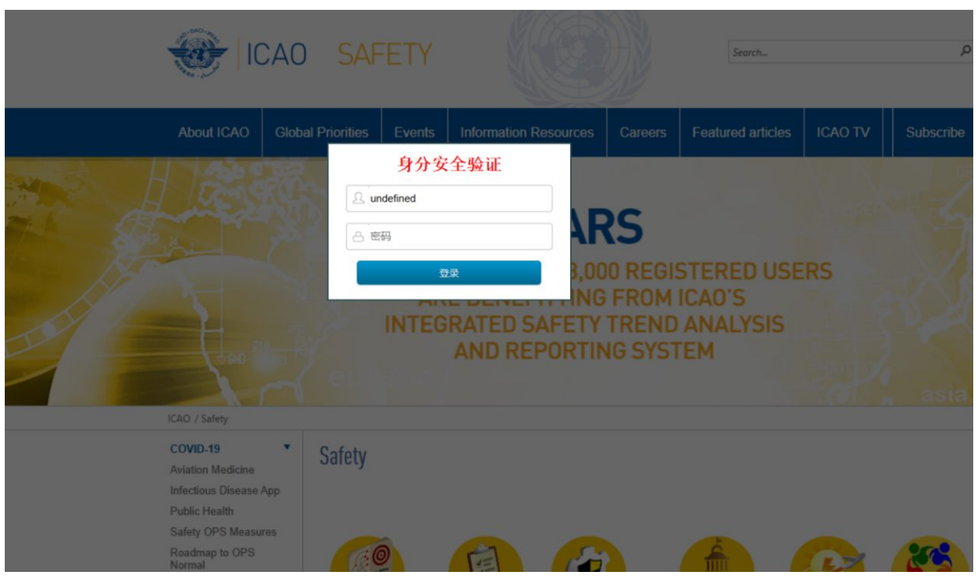
▲图①：APT-C-01（毒云藤）组织攻击流程示意图1　图②：APT-C-01（毒云藤）组织攻击流程示意图2

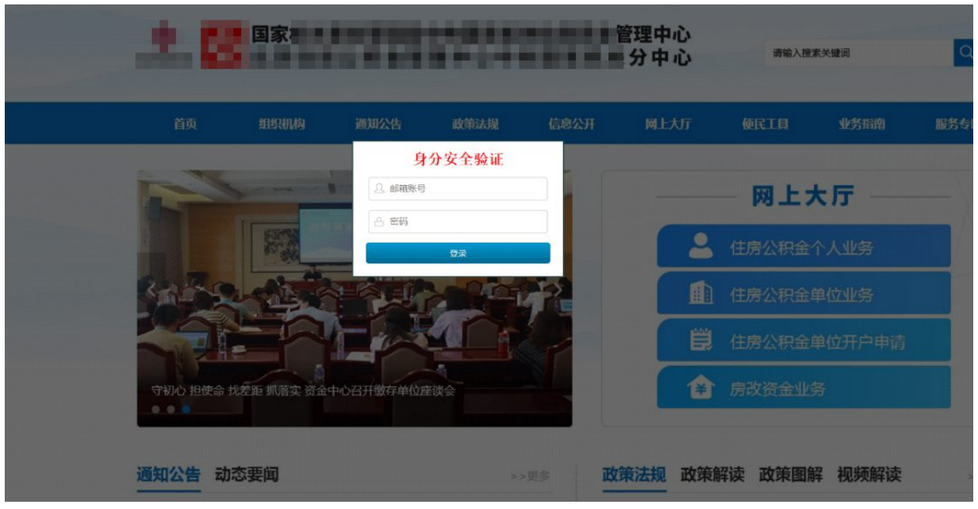
图①



图②

▲图①：APT-C-01（毒云藤）组织近期使用钓鱼文档主题关键词　图②：APT-C-01（毒云藤）组织近期使用的钓鱼文档





▲ 图：APT-C-01（毒云藤）组织近期使用的钓鱼网站

3.2、APT-C-64（匿名者64）

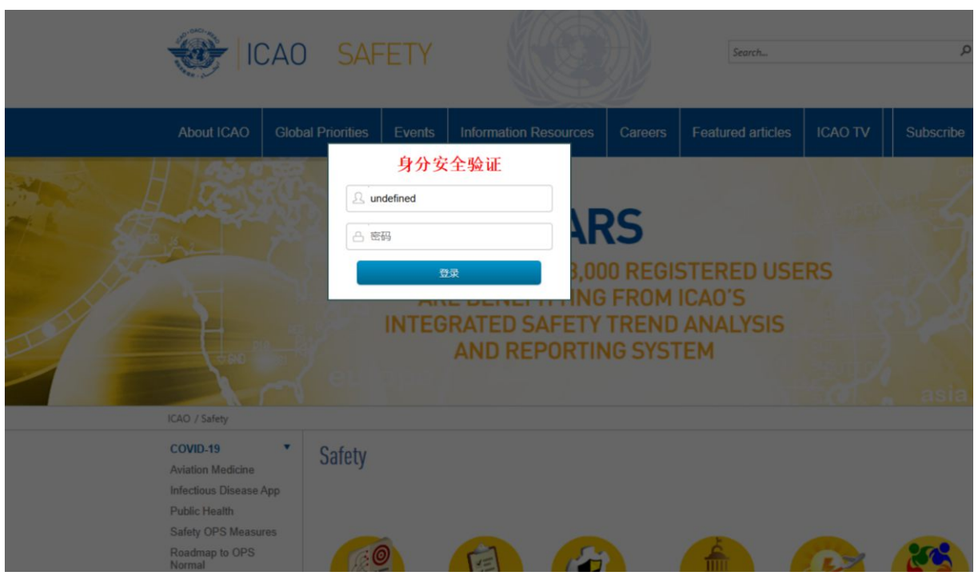
APT-C-64（匿名者64）组织攻击目标主要涉及我国大陆及港澳地区政府和企事业单位的数字媒体服务系统，以及相关网站、户外电子屏幕、网络电视等，攻击目的是通过篡改系统播放政治敏感内容，制造舆论效果，进而扰乱社会公共秩序。

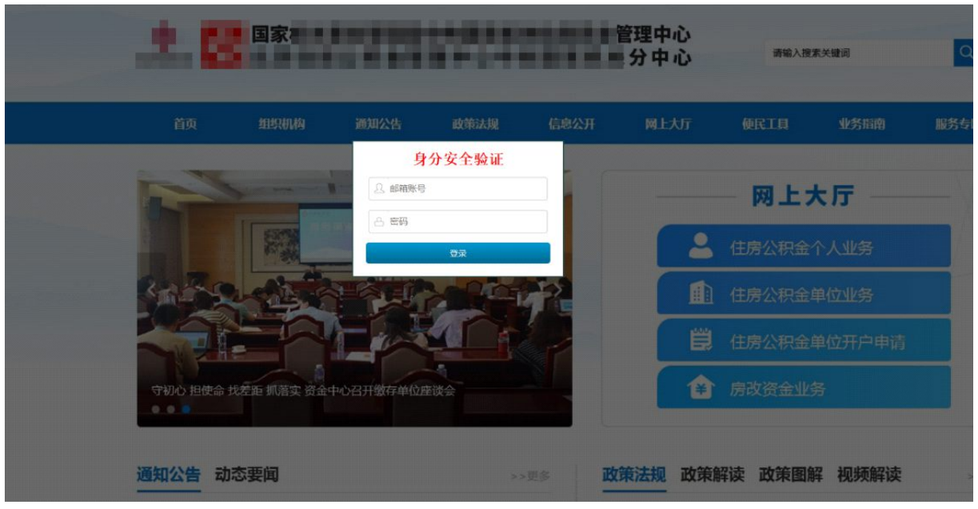
攻击者首先对特定数字媒体发布管理系统（Digital Media System，简称DMS）服务的端口进行扫描探测，识别我国大陆以及港澳地区单位的DMS系统进行攻击，在获取控制权限后将有政治目的的煽动和诋毁视频发布到网页。

目前该组织声称已经攻破的“官方网站”实际大都为山寨版的官方网站或长期无人运营的子网站，暂未发现gov.cn、edu.cn、ac.cn、mil.cn等一级域名网站被攻击。

其典型攻击技战术下图所示：

▲ 图：APT-C-64（匿名者64）组织攻击流程图





▲ 图：APT-C-01（毒云藤）组织近期使用的钓鱼网站

3.2、APT-C-64（匿名者64）

APT-C-64（匿名者64）组织攻击目标主要涉及我国大陆及港澳地区政府和企事业单位的数字媒体服务系统，以及相关网站、户外电子屏幕、网络电视等，攻击目的是通过篡改系统播放政治敏感内容，制造舆论效果，进而扰乱社会公共秩序。

攻击者首先对特定数字媒体发布管理系统（Digital Media System，简称DMS）服务的端口进行扫描探测，识别我国大陆以及港澳地区单位的DMS系统进行攻击，在获取控制权限后将有政治目的的煽动和诋毁视频发布到网页。

目前该组织声称已经攻破的“官方网站”实际大都为山寨版的官方网站或长期无人运营的子网站，暂未发现gov.cn、edu.cn、ac.cn、mil.cn等一级域名网站被攻击。

其典型攻击技战术下图所示：

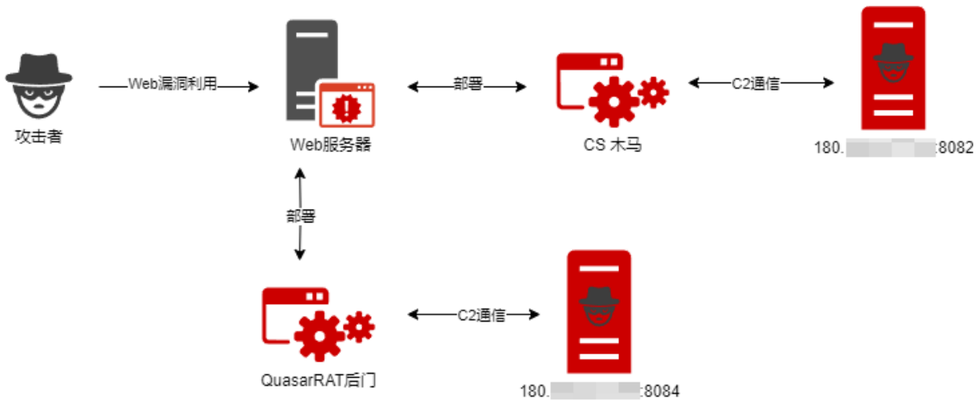
▲ 图：APT-C-64（匿名者64）组织攻击流程图

3.3、APT-C-65（金叶萝）

APT-C-65（金叶萝）组织自2020年以来，持续针对我国防军工、航空航天、能源等关基单位进行网络攻击渗透，目标窃取我关键信息基础设施重要数据。

APT-C-65（金叶萝）组织攻击活动与台当局领导人的所谓“外事活动”时间紧密关联。360通过对该组织持续监测发现，该组织分别在2022年8月美国国会众议长南希·佩洛西窜访中国台湾、2023年8月民进党代表赖清德窜访美国、2024年4月台湾省数字事务部参加美国网络安全演习期间，以及2024年12月初赖清德再次窜美几个时间节点前后，对我国防军工、政府机构、能源、交通运输等领域，特别其中的航空航天、港口、海事等相关单位，实施了密集的网络攻击和情报刺探活动。

APT-C-65（金叶萝）组织典型攻击手段是通过Web系统漏洞利用进行渗透，然后部署恶意软件窃取敏感数据。主要涉及国产电子文档安全管理系统、国产OA系统、国产ERP系统和国产办公系统等相关软件漏洞。攻击活动流程先是通过Web应用系统漏洞控制相关主机系统；然后通过调用Windows系统程序InstallUtil.exe来规避进程白名单检查，以隐藏恶意代码的执行。



▲图：APT-C-65（金叶萝）组织攻击流程示意图

3.4、APT-C-67（乌苏拉）

APT-C-67（乌苏拉）是一个在中国台湾省地区近年来逐渐活跃的APT组织。该组织主要针对中国大陆和港澳地区的物联网系统，特别是视频监控系统，妄图通过控制大量视频监控设备，持续窃取我网络及地理空间情报数据。该组织典型网络攻击技战术如下图所示。

APT-C-67组织常态化借助公开网络资产测绘平台或通过批量网络地址扫描探测，获取我国境内暴露在互联网上存在已知漏洞的网络安防系统、网络摄像机等物联网系统的网络地址；进一步尝试利用已知漏洞非法获取监控系统后台控制权限，部署远程控制工具或木马，逐步完成内网渗透，最终获得安防系统的全面控制权限和数据访问权限，利用安防系统的实时视频和历史数据对目标所在区域实施情报收集。

2025年4月，该组织对我国某科技公司实施了网络攻击，通过绕过该公司网络防护装置，入侵自助设备后台系统，通过横向移动渗透，控制了该公司多台内网设备，进一步向这些设备后台系统上传多份恶

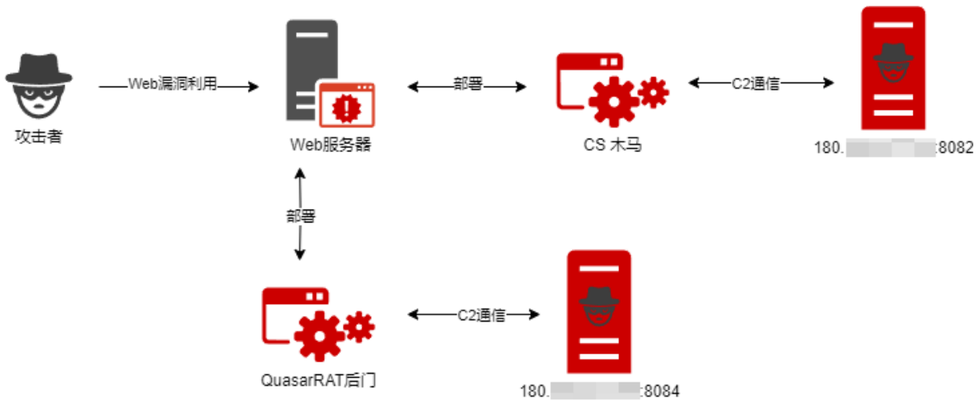
▲图：APT-C-67（乌苏拉）组织攻击流程图

3.3、APT-C-65（金叶萝）

APT-C-65（金叶萝）组织自2020年以来，持续针对我国防军工、航空航天、能源等关基单位进行网络攻击渗透，目标窃取我关键信息基础设施重要数据。

APT-C-65（金叶萝）组织攻击活动与台当局领导人的所谓“外事活动”时间紧密关联。360通过对该组织持续监测发现，该组织分别在2022年8月美国国会众议长南希·佩洛西窜访中国台湾、2023年8月民进党代表赖清德窜访美国、2024年4月台湾省数字事务部参加美国网络安全演习期间，以及2024年12月初赖清德再次窜美几个时间节点前后，对我国防军工、政府机构、能源、交通运输等领域，特别其中的航空航天、港口、海事等相关单位，实施了密集的网络攻击和情报刺探活动。

APT-C-65（金叶萝）组织典型攻击手段是通过Web系统漏洞利用进行渗透，然后部署恶意软件窃取敏感数据。主要涉及国产电子文档安全管理系统、国产OA系统、国产ERP系统和国产办公系统等相关软件漏洞。攻击活动流程先是通过Web应用系统漏洞控制相关主机系统；然后通过调用Windows系统程序InstallUtil.exe来规避进程白名单检查，以隐藏恶意代码的执行。



▲图：APT-C-65（金叶萝）组织攻击流程示意图

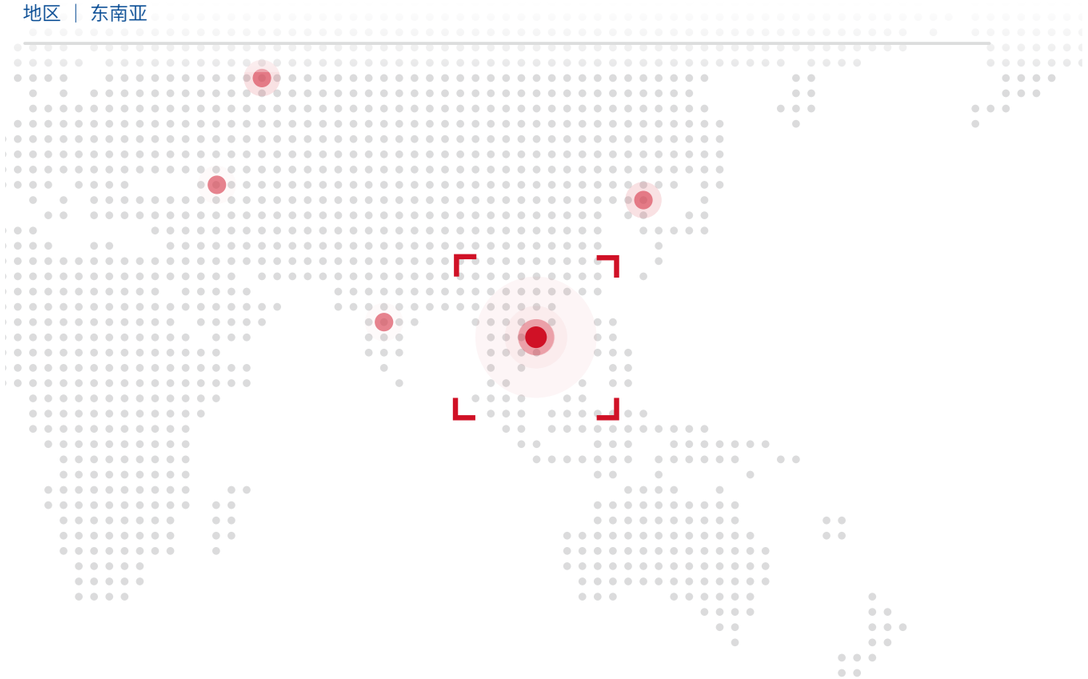
3.4、APT-C-67（乌苏拉）

APT-C-67（乌苏拉）是一个在中国台湾省地区近年来逐渐活跃的APT组织。该组织主要针对中国大陆和港澳地区的物联网系统，特别是视频监控系统，妄图通过控制大量视频监控设备，持续窃取我网络及地理空间情报数据。该组织典型网络攻击技战术如下图所示。

APT-C-67组织常态化借助公开网络资产测绘平台或通过批量网络地址扫描探测，获取我国境内暴露在互联网上存在已知漏洞的网络安防系统、网络摄像机等物联网系统的网络地址；进一步尝试利用已知漏洞非法获取监控系统后台控制权限，部署远程控制工具或木马，逐步完成内网渗透，最终获得安防系统的全面控制权限和数据访问权限，利用安防系统的实时视频和历史数据对目标所在区域实施情报收集。

2025年4月，该组织对我国某科技公司实施了网络攻击，通过绕过该公司网络防护装置，入侵自助设备后台系统，通过横向移动渗透，控制了该公司多台内网设备，进一步向这些设备后台系统上传多份恶

▲图：APT-C-67（乌苏拉）组织攻击流程图



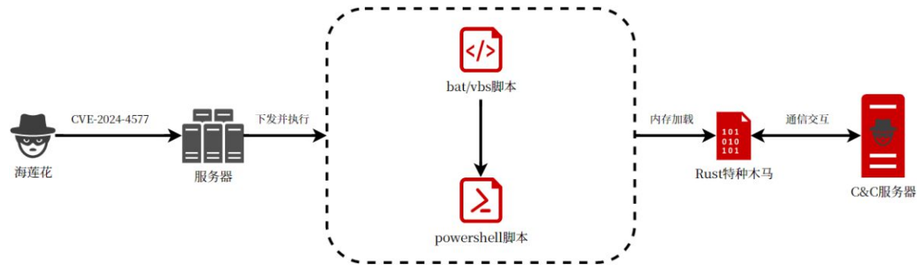
4、东南亚

2025年中国与东南亚国家命运共同体建设进入务实推进的新阶段。东南亚各国对海洋问题的政治态度强调对话合作、反对域外干涉的总体特征。个别国家虽拥有广泛海洋权益诉求，但近年明显转向经济优先、安全谨慎策略。区域APT组织的攻击方向也是以窃取我国国际关系、海事研究、经济贸易情报为主。

4.1、APT-C-00（海莲花）

APT-C-00（海莲花）组织攻击频繁，以我国国际关系、海事研究、经济贸易相关的科研及教育工作者作为主要攻击目标。

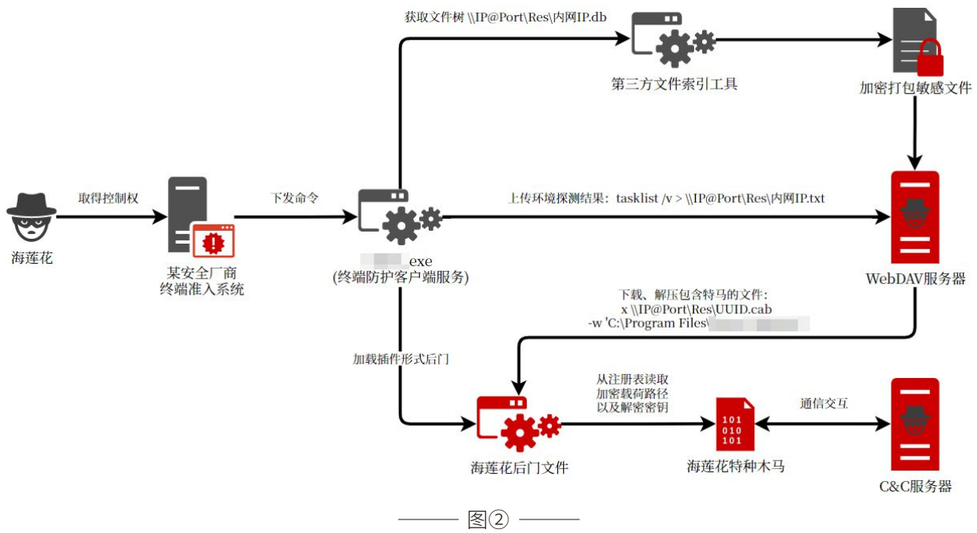
2025年我们监测到APT-C-00（海莲花）组织对存在可利用PHP-CGI RCE漏洞（CVE-2024-4577）的服务器展开批量攻击。攻击者通过此漏洞上传后门并实现长期驻留。



图①

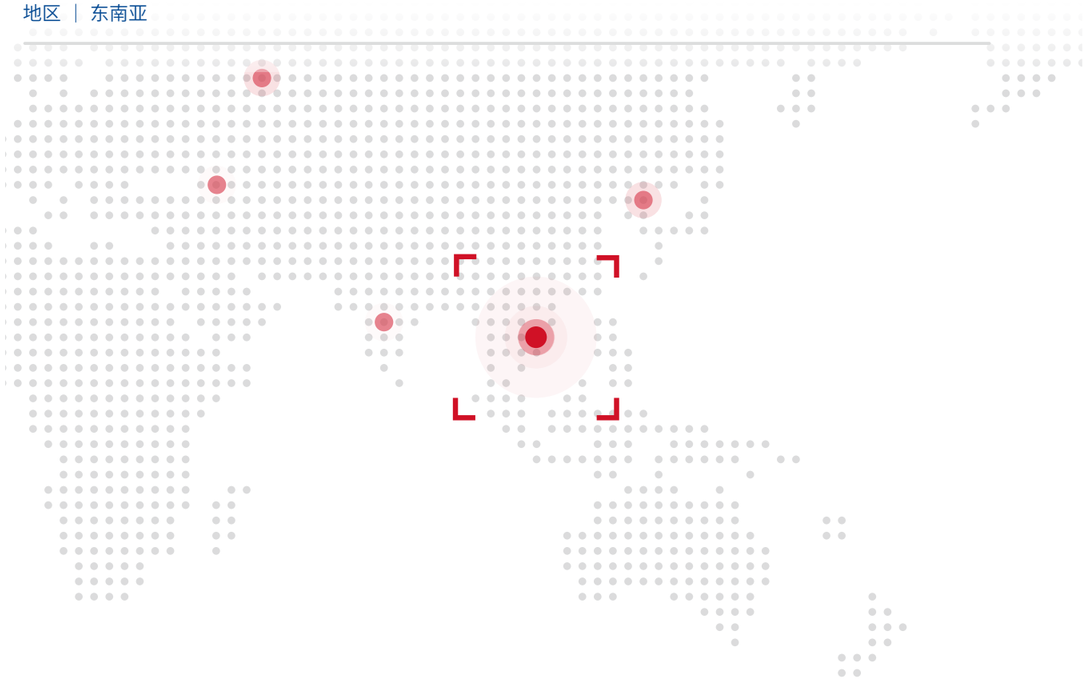
APT-C-00（海莲花）组织在利用某安全厂商终端防护程序的攻击活动中，在攻克的终端准入系统服务器上，基于终端服务程序执行安全管理命令的渠道下发后门模块，然后加载APT-C-00（海莲花）的特种木马。

本次攻击自5月持续至12月期间，APT-C-00（海莲花）曾多次投递第三方文件索引工具，挑选所需文件加密打包回传至服务器。同期，我们还观察到APT-C-00（海莲花）组织为躲避安全软件查杀而下发的轻量化Python后门。



图②

▲ 图①：APT-C-00（海莲花）组织利用RCE漏洞攻击流程示意图　　图②：APT-C-00（海莲花）组织利用终端防护漏洞攻击流程图



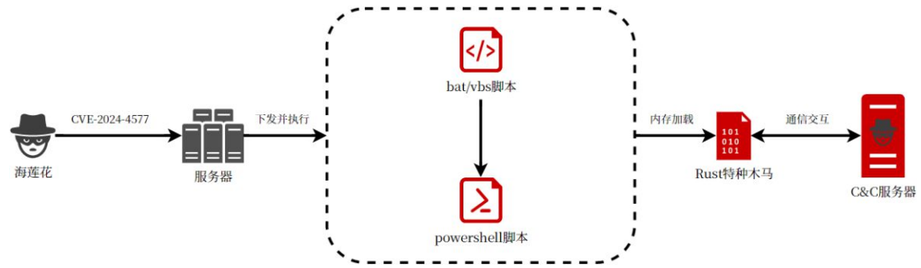
4、东南亚

2025年中国与东南亚国家命运共同体建设进入务实推进的新阶段。东南亚各国对海洋问题的政治态度强调对话合作、反对域外干涉的总体特征。个别国家虽拥有广泛海洋权益诉求，但近年明显转向经济优先、安全谨慎策略。区域APT组织的攻击方向也是以窃取我国国际关系、海事研究、经济贸易情报为主。

4.1、APT-C-00（海莲花）

APT-C-00（海莲花）组织攻击频繁，以我国国际关系、海事研究、经济贸易相关的科研及教育工作者作为主要攻击目标。

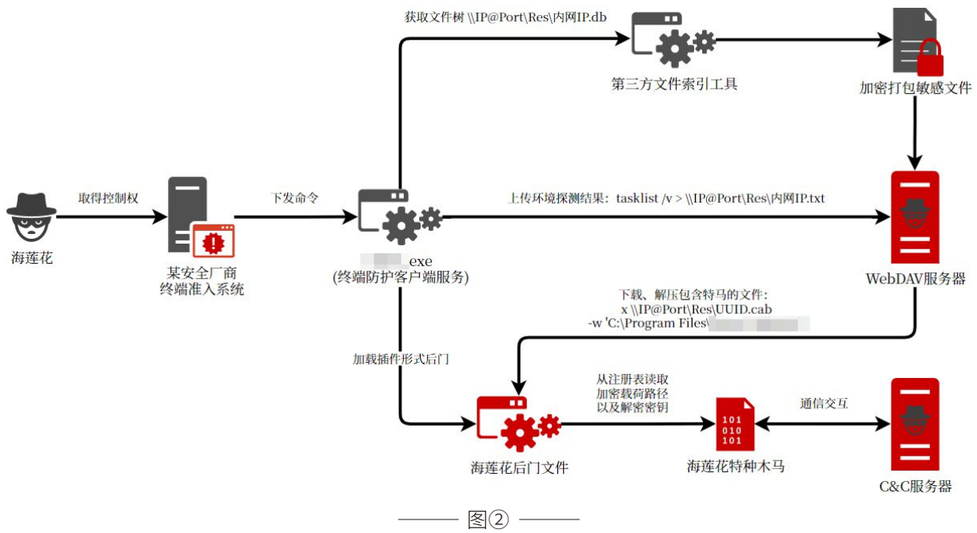
2025年我们监测到APT-C-00（海莲花）组织对存在可利用PHP-CGI RCE漏洞（CVE-2024-4577）的服务器展开批量攻击。攻击者通过此漏洞上传后门并实现长期驻留。



图①

APT-C-00（海莲花）组织在利用某安全厂商终端防护程序的攻击活动中，在攻克的终端准入系统服务器上，基于终端服务程序执行安全管理命令的渠道下发后门模块，然后加载APT-C-00（海莲花）的特种木马。

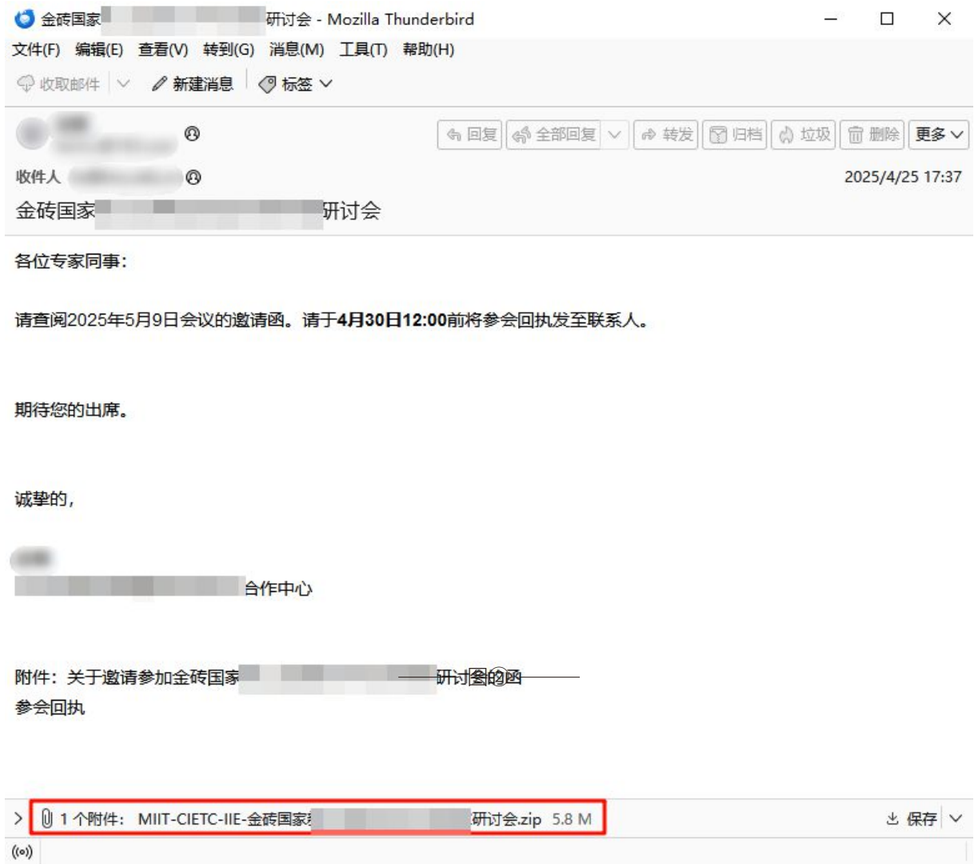
本次攻击自5月持续至12月期间，APT-C-00（海莲花）曾多次投递第三方文件索引工具，挑选所需文件加密打包回传至服务器。同期，我们还观察到APT-C-00（海莲花）组织为躲避安全软件查杀而下发的轻量化Python后门。



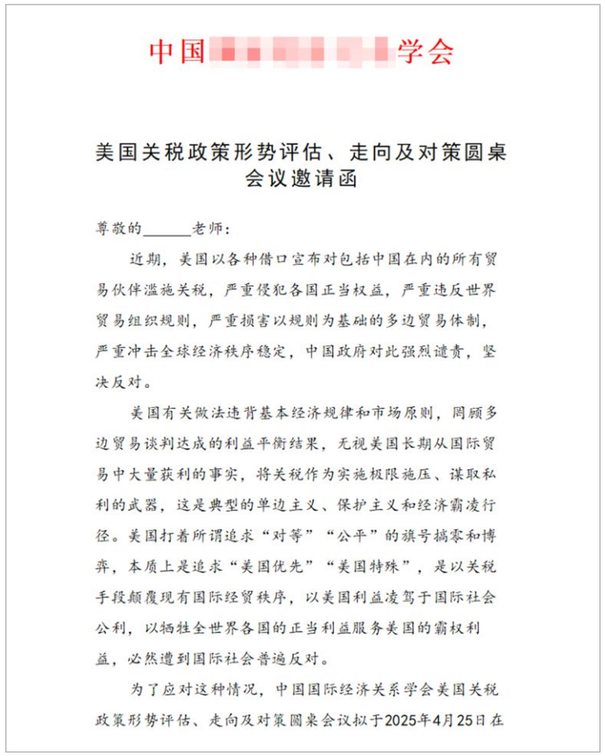
图②

▲ 图①：APT-C-00（海莲花）组织利用RCE漏洞攻击流程示意图　　图②：APT-C-00（海莲花）组织利用终端防护漏洞攻击流程图

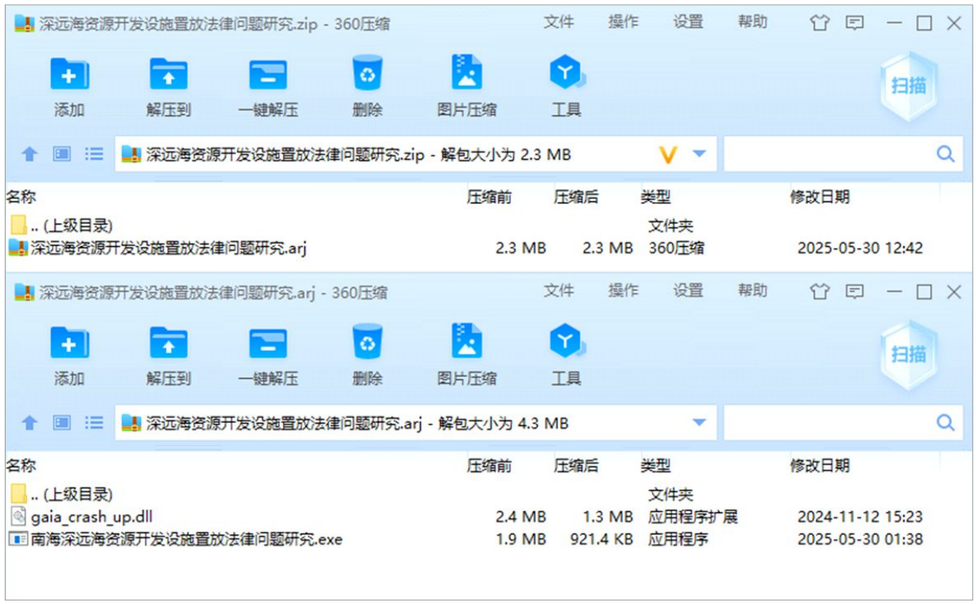
2025年，APT-C-00（海莲花）组织将我国国际关系、海事研究、经济贸易相关的科研及教育工作者作为主要攻击目标，制作和投递与之相关会议通知、技术资料、行业报告等钓鱼诱饵文件。受害用户在运行诱饵文件后，攻击者会根据目标价值决定是否保持长期控制权或横向移动。被该组织长期驻留的机器会被定期窃取重要文件。



▲图：APT-C-00（海莲花）组织使用的钓鱼邮件



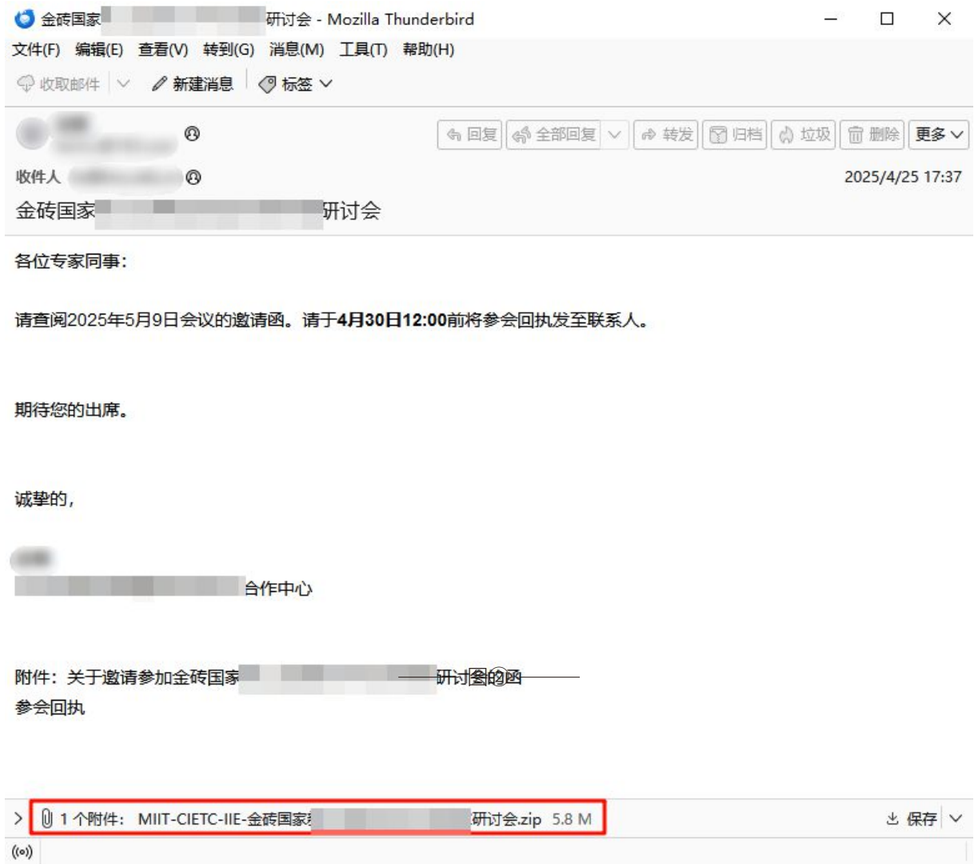
图①



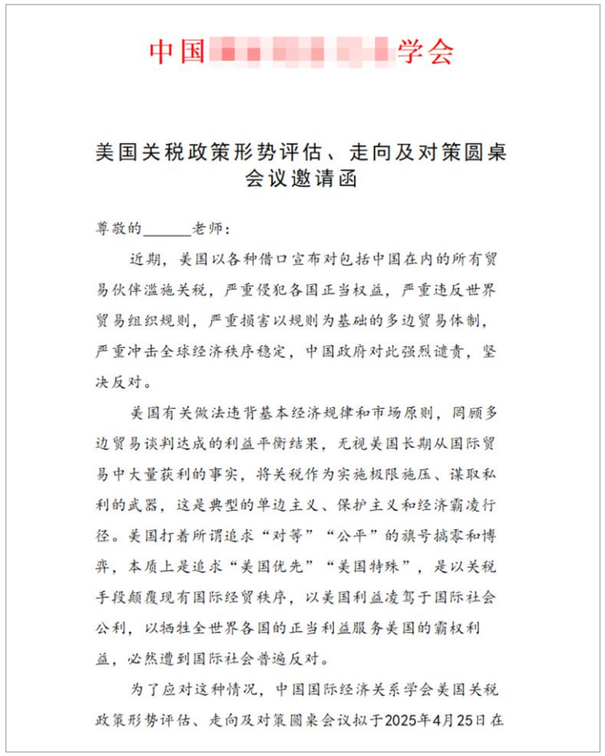
图②

▲图①：APT-C-00（海莲花）组织使用的诱饵文档　图②：APT-C-00（海莲花）组织攻击载荷文件

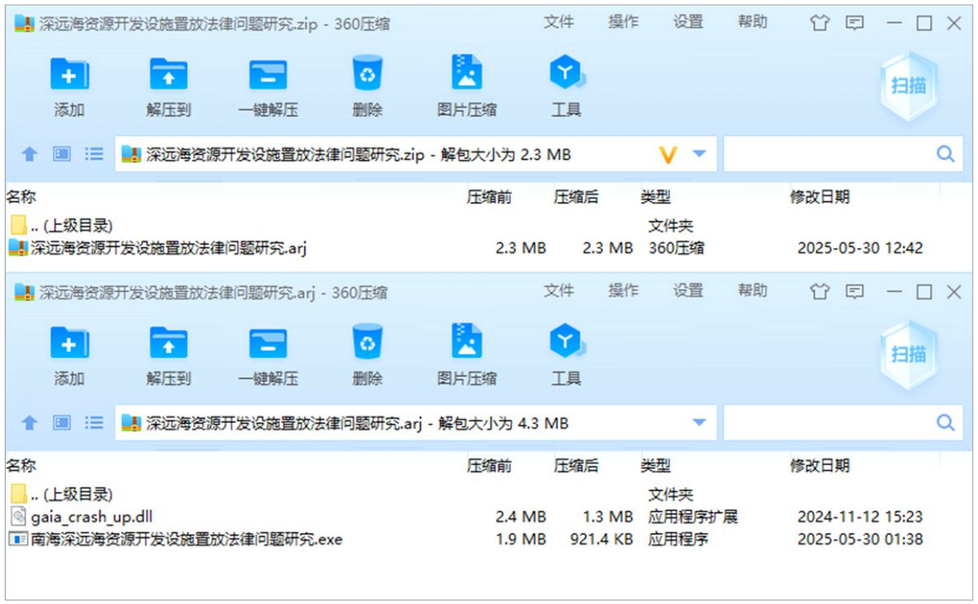
2025年，APT-C-00（海莲花）组织将我国国际关系、海事研究、经济贸易相关的科研及教育工作者作为主要攻击目标，制作和投递与之相关会议通知、技术资料、行业报告等钓鱼诱饵文件。受害用户在运行诱饵文件后，攻击者会根据目标价值决定是否保持长期控制权或横向移动。被该组织长期驻留的机器会被定期窃取重要文件。



▲图：APT-C-00（海莲花）组织使用的钓鱼邮件



图①



图②

▲图①：APT-C-00（海莲花）组织使用的诱饵文档　图②：APT-C-00（海莲花）组织攻击载荷文件

自2024年APT-C-00（海莲花）组织在GitHub平台发布包含后门的安全工具项目钓鱼后，2025年APT-C-00（海莲花）组织则将目标转向PyPI平台，发布模仿常用模块包名的项目试图感染开发人员。本次投毒最早可追溯至2025年3月，攻击者上传的测试项目包含针对Windows和Linux双平台的后门模块。

近年来随着国家信创战略的深入推进，党政机关及关键行业的信息系统国产化替代加速落地。国产化进程在提升自主可控能力的同时，也吸引了APT-C-00（海莲花）组织的高度关注，针对国产化系统的定向攻击呈现显著上升趋势。

```
public b() {
  this.a = "大国竞争与全球治理交织下的联合国：机遇、挑战和前景.docx";
  this.b = ".report-scheduler-1.0-SNAPSHOT.jar";
  this.c = "12";
  Random random = new Random();
  String str = Paths.get(System.getProperty("java.io.tmpdir"), new String[0]).r
  if (a(this.a, str)) {
    if (!a(str)) {
      JOptionPane.showMessageDialog(null, "File is corrupted", "Error", 0);
      return;
    }
  } else {
    JOptionPane.showMessageDialog(null, "File is corrupted", "Error", 0);
    return;
  }
  if (!(str = System.getProperty("os.name")).toLowerCase().contains("linux"))
    return;
  str = Paths.get(a(), new String[0]).resolve(this.b).toString() + ".lock";
  try {
    RandomAccessFile randomAccessFile = new RandomAccessFile(str, "rw");
```

图①

大国竞争与全球治理交织下的联合国：机遇、挑战和前景

【内容提要】在百年变局和新型全球化推动下，国际社会形成大国竞争和全球治理并存和交织的新态势。一方面，联合国在维护国际安全中的权威性和有效性受到质疑和挑战；另一方面，联合国在全球治理中的地位和作用不断上升。如何通过变革，推动大国协调，有效应对全球挑战，是联合国面临的重大课题。

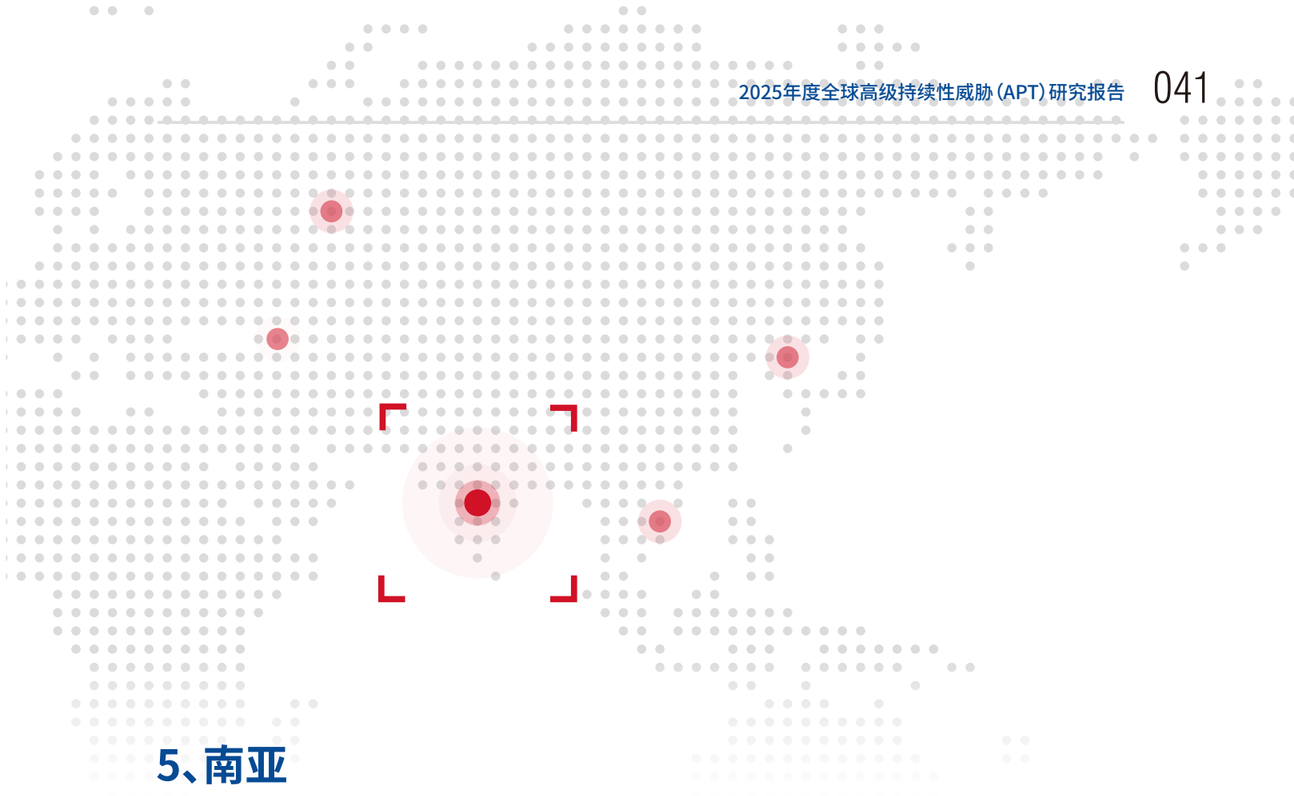
一、大国竞争和全球治理的新态势

冷战时期，大国竞争主要体现为东西方对抗和美国苏霸，形成两极格局。无论是朝鲜战争、越南战争、阿富汗战争，还是中东和非洲地区的大量冲突，大国直接卷入或在其代理人之间进行。美苏两个超级大国之间形成政治、经济、军事和意识形态的全方位对抗。尽管冷战时期不同阶段这种对抗的方式有所不同，但强对抗大致构成了战后40多年国际关系的基本内容和特点。另一方面，真正的全球治理尚未形成。尽管成立了联合国及其众多附属机构和专门机构，关税及贸易总协定、世界银行、国际货币基金组织等世界经济组织，但许多国家并没有加入国际组织。国际组织的领导权和主导权也掌握在美西方几个主要大国等大国竞争和全球治理形成。更主要的是，跨国问题还不突出，或尚未成为全球性议题。即使如联合国开展的维和行动，以及推动的四个发展十年战略，从其内容和过程来看也还缺乏治理意义。如果说有治理，也是以西方国家为主的部分国家开展的国际治理，还没有形成"全球"的治理。可见，冷战时期的大国竞争和全球治理表现为"强对抗、弱治理"的态势。

冷战结束后，随着苏联解体和东欧剧变，东西方之间的对抗消退，大国竞争转变为大国协调。大国之间的力量对比则表现为美国独大的单极格局。尽管俄罗斯未能被融入到西方体系，但与美西方国家的关系总体上处于比较协调状态。中美之间出现过象台海危机、撞机、使馆被炸等突发事件，但两国较好地进行了管控。随着"911"事件的发生和中国加入世界贸易组织，中美关系特别是在经贸和人文交流领域取得巨大进展。大国协调为联合国发挥更大作用和开展全球治理提供了有利的条件和环境。联合国维和行动转向国内冲突解决和冲突后重建，千年发展目标成为联合国会员国共同努力的方向，人权和国际法治得到更多的重视。这些进展都具有显著的治理意义。2015年，《巴黎协定》的签订和2030年可持续发展目标的提出，标志着全球治理进入一个"黄金时期"。全球性和地区性国际组织非常活跃，多边主义和国际合作获得前所未有的动力和支持。可以说，大国竞争和全球治理出现弱对抗、强治理的态势。

图②

▲ 图①：APT-C-00（海莲花）组织针对国产化系统的脚本　　图②：APT-C-00（海莲花）组织针对国产化系统的钓鱼文档



5、南亚

2025年南亚呈现“政治动荡加剧、经济分化明显、军事对抗升级”的格局，印巴冲突全域化、多国政局洗牌、经济复苏乏力与军备竞赛提速叠加，外部势力深度介入，地区稳定性显著下滑。同时，我国在南亚地区的一带一路相关项目建设，以及能源基础设施的重大工程对区域经贸关系有重大影响，南亚地区APT组织对我国在区域水利能源、驻外机构也极为关注。

2025年南亚方向APT组织攻击表现依旧十分活跃。其结合实时热点话题，针对周边国家持续进行了多种攻击活动。在2025年，360高级威胁研究院披露了一个新的南亚区域背景APT组织，APT-C-76（银环蛇）。该组织先后对我国国内文娱产业、教育领域发起攻击。

5.1、APT-C-08（蔓灵花）

2025年，APT-C-08（蔓灵花）组织的整体活动保持活跃，主要围绕我国外交、政府及国际关系实体等展开渗透，不断进行情报窃取攻击。特别是在国际热点事件期间，该组织对我国驻外相关机构的攻击活动明显。尤其2025年7、8月份期间，针对我国中印边境相关地区省市政府机构发起大规模集中攻击活动，以水利能源、工程建设等基础设施建设相关单位为首要目标。

APT-C-08（蔓灵花）组织在常用的攻击手法外，还不断地更新攻击手段，持续扩充自己的武器库。我们在2025年公开披露了该组织的新的攻击武器“gmRAT”。

自2024年APT-C-00（海莲花）组织在GitHub平台发布包含后门的安全工具项目钓鱼后，2025年APT-C-00（海莲花）组织则将目标转向PyPI平台，发布模仿常用模块包名的项目试图感染开发人员。本次投毒最早可追溯至2025年3月，攻击者上传的测试项目包含针对Windows和Linux双平台的后门模块。

近年来随着国家信创战略的深入推进，党政机关及关键行业的信息系统国产化替代加速落地。国产化进程在提升自主可控能力的同时，也吸引了APT-C-00（海莲花）组织的高度关注，针对国产化系统的定向攻击呈现显著上升趋势。

```
public b() {
  this.a = "大国竞争与全球治理交织下的联合国：机遇、挑战和前景.docx";
  this.b = ".report-scheduler-1.0-SNAPSHOT.jar";
  this.c = "12";
  Random random = new Random();
  String str = Paths.get(System.getProperty("java.io.tmpdir"), new String[0]).r
  if (a(this.a, str)) {
    if (!a(str)) {
      JOptionPane.showMessageDialog(null, "File is corrupted", "Error", 0);
      return;
    }
  } else {
    JOptionPane.showMessageDialog(null, "File is corrupted", "Error", 0);
    return;
  }
  if (!(str = System.getProperty("os.name")).toLowerCase().contains("linux"))
    return;
  str = Paths.get(a(), new String[0]).resolve(this.b).toString() + ".lock";
  try {
    RandomAccessFile randomAccessFile = new RandomAccessFile(str, "rw");
```

图①

大国竞争与全球治理交织下的联合国：机遇、挑战和前景

【内容提要】在百年变局和新型全球化推动下，国际社会形成大国竞争和全球治理并存和交织的新态势。一方面，联合国在维护国际安全中的权威性和有效性受到质疑和挑战；另一方面，联合国在全球治理中的地位和作用不断上升。如何通过变革，推动大国协调，有效应对全球挑战，是联合国面临的重大课题。

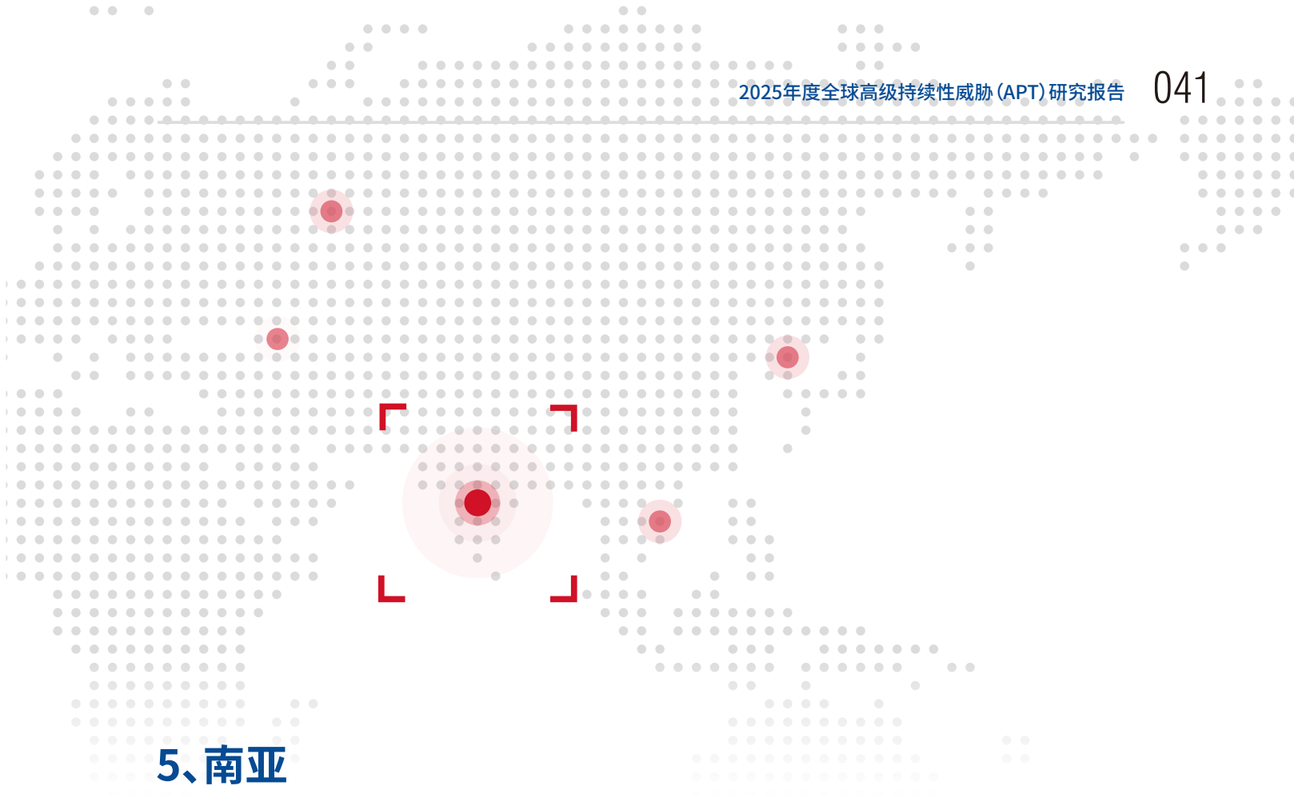
一、大国竞争和全球治理的新态势

冷战时期，大国竞争主要体现为东西方对抗和美国苏霸，形成两极格局。无论是朝鲜战争、越南战争、阿富汗战争，还是中东和非洲地区的大量冲突，大国直接卷入或在其代理人之间进行。美苏两个超级大国之间形成政治、经济、军事和意识形态的全方位对抗。尽管冷战时期不同阶段这种对抗的方式有所不同，但强对抗大致构成了战后40多年国际关系的基本内容和特点。另一方面，真正的全球治理尚未形成。尽管成立了联合国及其众多附属机构和专门机构，关税及贸易总协定、世界银行、国际货币基金组织等世界经济组织，但许多国家并没有加入国际组织。国际组织的领导权和主导权也掌握在美西方几个主要大国等大国竞争和全球治理形成。更主要的是，跨国问题还不突出，或尚未成为全球性议题。即使如联合国开展的维和行动，以及推动的四个发展十年战略，从其内容和过程来看也还缺乏治理意义。如果说有治理，也是以西方国家为主的部分国家开展的国际治理，还没有形成"全球"的治理。可见，冷战时期的大国竞争和全球治理表现为"强对抗、弱治理"的态势。

冷战结束后，随着苏联解体和东欧剧变，东西方之间的对抗消退，大国竞争转变为大国协调。大国之间的力量对比则表现为美国独大的单极格局。尽管俄罗斯未能被融入到西方体系，但与美西方国家的关系总体上处于比较协调状态。中美之间出现过象台海危机、撞机、使馆被炸等突发事件，但两国较好地进行了管控。随着"911"事件的发生和中国加入世界贸易组织，中美关系特别是在经贸和人文交流领域取得巨大进展。大国协调为联合国发挥更大作用和开展全球治理提供了有利的条件和环境。联合国维和行动转向国内冲突解决和冲突后重建，千年发展目标成为联合国会员国共同努力的方向，人权和国际法治得到更多的重视。这些进展都具有显著的治理意义。2015年，《巴黎协定》的签订和2030年可持续发展目标的提出，标志着全球治理进入一个"黄金时期"。全球性和地区性国际组织非常活跃，多边主义和国际合作获得前所未有的动力和支持。可以说，大国竞争和全球治理出现弱对抗、强治理的态势。

图②

▲ 图①：APT-C-00（海莲花）组织针对国产化系统的脚本　　图②：APT-C-00（海莲花）组织针对国产化系统的钓鱼文档



5、南亚

2025年南亚呈现“政治动荡加剧、经济分化明显、军事对抗升级”的格局，印巴冲突全域化、多国政局洗牌、经济复苏乏力与军备竞赛提速叠加，外部势力深度介入，地区稳定性显著下滑。同时，我国在南亚地区的一带一路相关项目建设，以及能源基础设施的重大工程对区域经贸关系有重大影响，南亚地区APT组织对我国在区域水利能源、驻外机构也极为关注。

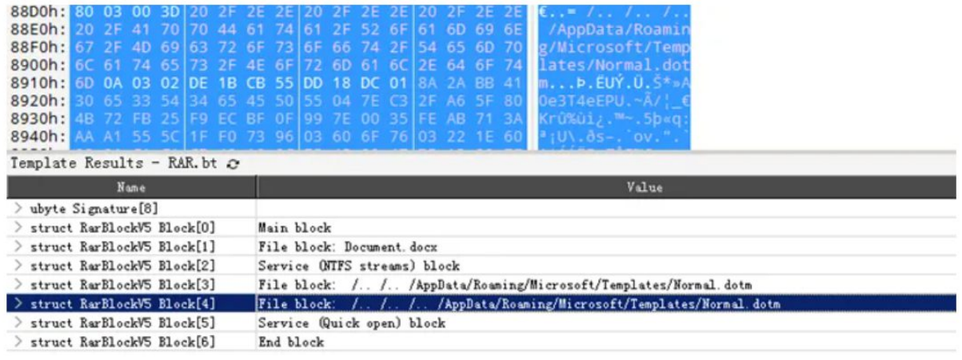
2025年南亚方向APT组织攻击表现依旧十分活跃。其结合实时热点话题，针对周边国家持续进行了多种攻击活动。在2025年，360高级威胁研究院披露了一个新的南亚区域背景APT组织，APT-C-76（银环蛇）。该组织先后对我国国内文娱产业、教育领域发起攻击。

5.1、APT-C-08（蔓灵花）

2025年，APT-C-08（蔓灵花）组织的整体活动保持活跃，主要围绕我国外交、政府及国际关系实体等展开渗透，不断进行情报窃取攻击。特别是在国际热点事件期间，该组织对我国驻外相关机构的攻击活动明显。尤其2025年7、8月份期间，针对我国中印边境相关地区省市政府机构发起大规模集中攻击活动，以水利能源、工程建设等基础设施建设相关单位为首要目标。

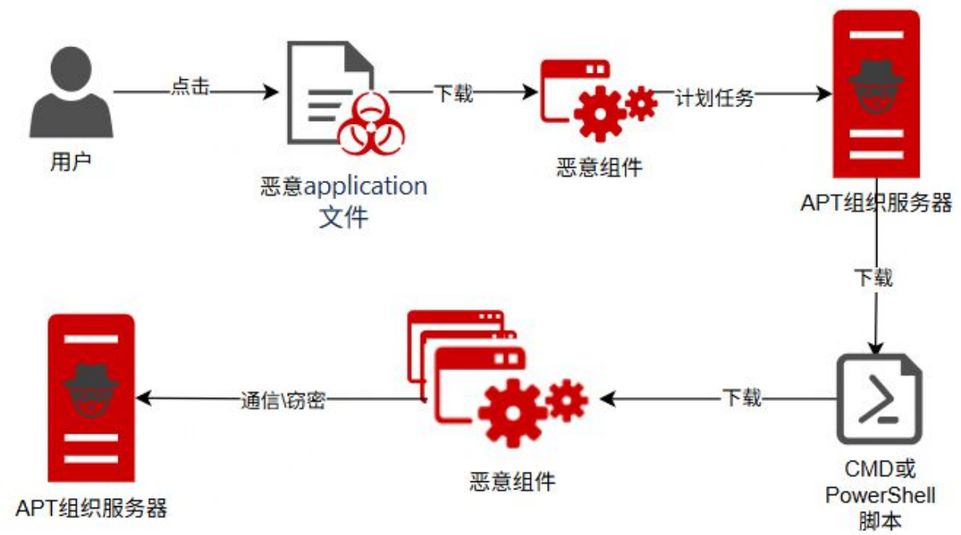
APT-C-08（蔓灵花）组织在常用的攻击手法外，还不断地更新攻击手段，持续扩充自己的武器库。我们在2025年公开披露了该组织的新的攻击武器“gmRAT”。

2025年还首次发现APT-C-08（蔓灵花）组织利用WinRAR漏洞CVE-2025-6218（WinRAR目录穿越漏洞）实施网络攻击。通过构造特殊的文件路径，将恶意文件Normal.dotm释放到Office模板目录下，当用户打开任意word文档时，便会加载“Normal.dotm”文件，从而触发恶意代码。



图①

除了上述的攻击手法外，APT-C-08（蔓灵花）组织还会通过伪造应用程序进行网络钓鱼行动。用户点击恶意应用程序之后，该应用可远程下载后续的恶意载荷。这些恶意载荷会利用“计划任务”周期性地回传受影响用户的机器信息，通知远程服务器下发后续攻击组件。



图②

▲图①：dotm样本片段示意图　图②：APT-C-08（蔓灵花）攻击流程示意图

5.2、APT-C-09（摩诃草）

APT-C-09（摩诃草）组织在2025年攻击活动频繁，针对我国发起多次钓鱼邮件攻击。其主要攻击方向为高校、科研机构、气象与灾害研究实验室等单位，覆盖了教育、科研、政府等相关单位和工作人员


2025年度
可持续社会价值全球开放研究计划
开放申请！

可持续社会价值全球开放研究计划（简称“SSV开放计划”）由清华大学可持续社会价值研究院发起并主办。SSV开放计划旨在推动全球学术界在可持续社会价值领域的合作与研究。该计划面向全球学者（学术研究人员、研究机构及非营利组织），邀请他们提交关于可持续社会价值核心理念及实践应用的研究课题，并资助入选计划的项目开展研究工作。

研究院将重点支持该领域具有前沿性、交叉性、创新性及开发应用前景的原创性研究，并通过探索可持续社会价值的共创路径，为实际社会问题提供创新解决方案。

2025年度申报即日启动。

一、重点议题

SSV开放计划邀请申请者围绕以下11个重点议题进行研究：

- 可持续社会价值的基础理念研究
- 企业社会价值在具体领域的研究
- 科技向善与数字伦理
- 人工智能在善惠社会中的应用


重载无人机机载探地雷达大深度探测
与快速识别

[redacted]

2025.8.6

汇 报 提 纲

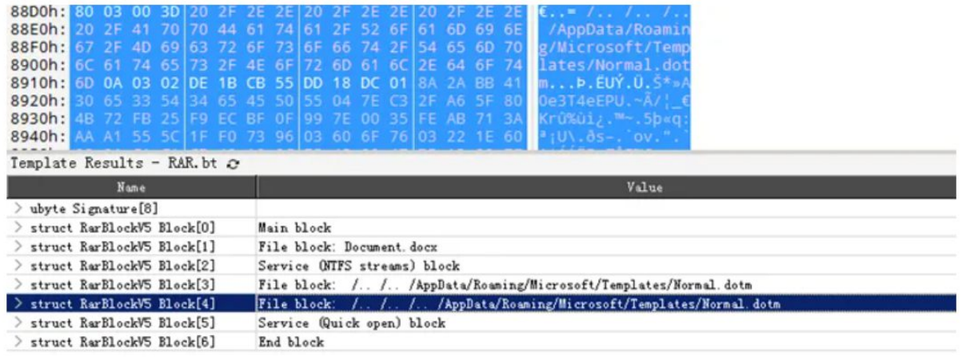
附件1

2025年“硕博连读”选拔评审成绩 [redacted]

序号	姓名	报考单位	报考专业	综合成绩	评审成绩	最终成绩	排名	评审意见
1	[redacted]	[redacted]	[redacted]	82.95	92.20	89.425	1	通过
2	[redacted]	[redacted]	[redacted]	80.81	92.20	88.783	2	通过
3	[redacted]	[redacted]	[redacted]	77.14	93.40	88.522	3	通过
4	[redacted]	[redacted]	[redacted]	78.43	91.60	87.649	4	通过
5	[redacted]	[redacted]	[redacted]	75.71	89.40	85.293	5	通过
6	[redacted]	[redacted]	[redacted]	66.45	89.80	82.795	6	通过
7	[redacted]	[redacted]	[redacted]	62.15	88.60	80.665	7	通过
8	[redacted]	[redacted]	[redacted]	51.78	88.40	77.414	8	通过
9	[redacted]	[redacted]	[redacted]	59.23	85.20	77.409	9	通过

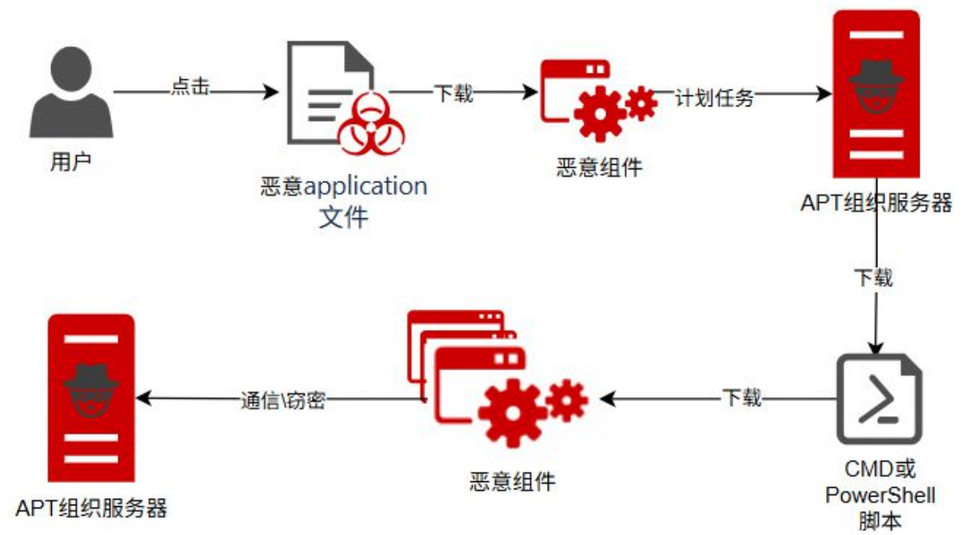
▲图：APT-C-09（摩诃草）组织诱饵文档示例

2025年还首次发现APT-C-08（蔓灵花）组织利用WinRAR漏洞CVE-2025-6218（WinRAR目录穿越漏洞）实施网络攻击。通过构造特殊的文件路径，将恶意文件Normal.dotm释放到Office模板目录下，当用户打开任意word文档时，便会加载“Normal.dotm”文件，从而触发恶意代码。



图①

除了上述的攻击手法外，APT-C-08（蔓灵花）组织还会通过伪造应用程序进行网络钓鱼行动。用户点击恶意应用程序之后，该应用可远程下载后续的恶意载荷。这些恶意载荷会利用“计划任务”周期性地回传受影响用户的机器信息，通知远程服务器下发后续攻击组件。



图②

▲图①：dotm样本片段示意图　图②：APT-C-08（蔓灵花）攻击流程示意图

5.2、APT-C-09（摩诃草）

APT-C-09（摩诃草）组织在2025年攻击活动频繁，针对我国发起多次钓鱼邮件攻击。其主要攻击方向为高校、科研机构、气象与灾害研究实验室等单位，覆盖了教育、科研、政府等相关单位和工作人员


2025年度
可持续社会价值全球开放研究计划
开放申请！

可持续社会价值全球开放研究计划（简称“SSV开放计划”）由清华大学可持续社会价值研究院发起并主办。SSV开放计划旨在推动全球学术界在可持续社会价值领域的合作与研究。该计划面向全球学者（学术研究人员、研究机构及非营利组织），邀请他们提交关于可持续社会价值核心理念及实践应用的研究课题，并资助入选计划的项目开展研究工作。

研究院将重点支持该领域具有前沿性、交叉性、创新性及开发应用前景的原创性研究，并通过探索可持续社会价值的共创路径，为实际社会问题提供创新解决方案。

2025年度申报即日启动。

一、重点议题

SSV开放计划邀请申请者围绕以下11个重点议题进行研究：

- 可持续社会价值的基础理念研究
- 企业社会价值在具体领域的研究
- 科技向善与数字伦理
- 人工智能在善惠社会中的应用


重载无人机机载探地雷达大深度探测
与快速识别

[redacted]

2025.8.6

汇 报 提 纲

附件1

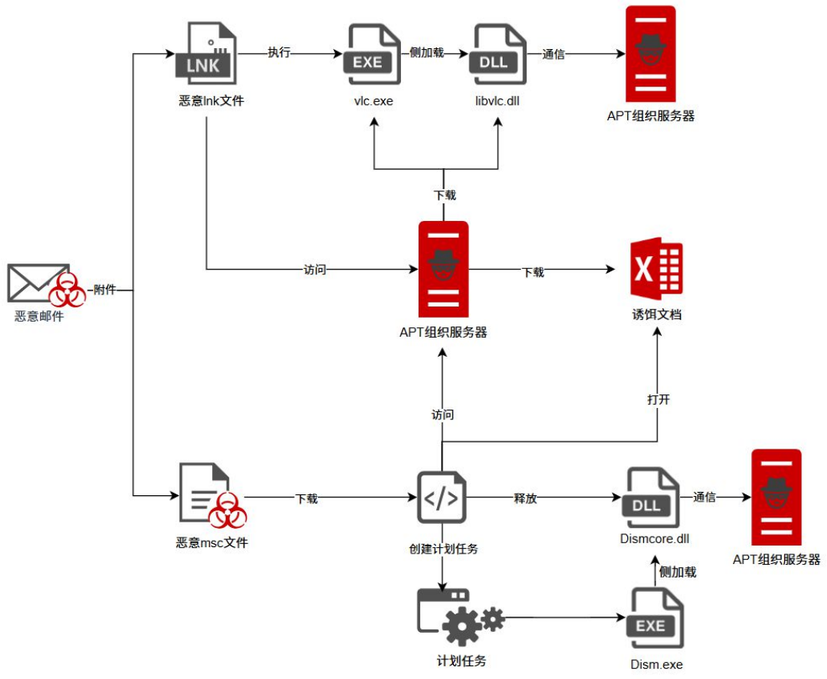
2025年“硕博连读”选拔评审成绩 [redacted]

序号	姓名	报考单位	报考专业	综合成绩	评审成绩	最终成绩	排名	评审意见
1	[redacted]	[redacted]	[redacted]	82.95	92.20	89.425	1	通过
2	[redacted]	[redacted]	[redacted]	80.81	92.20	88.783	2	通过
3	[redacted]	[redacted]	[redacted]	77.14	93.40	88.522	3	通过
4	[redacted]	[redacted]	[redacted]	78.43	91.60	87.649	4	通过
5	[redacted]	[redacted]	[redacted]	75.71	89.40	85.293	5	通过
6	[redacted]	[redacted]	[redacted]	66.45	89.80	82.795	6	通过
7	[redacted]	[redacted]	[redacted]	62.15	88.60	80.665	7	通过
8	[redacted]	[redacted]	[redacted]	51.78	88.40	77.414	8	通过
9	[redacted]	[redacted]	[redacted]	59.23	85.20	77.409	9	通过

▲图：APT-C-09（摩诃草）组织诱饵文档示例

其钓鱼攻击手法是通过钓鱼邮件下发伪装成PDF的LNK文件，当用户运行文件后会执行内嵌的PS指令下载后续恶意载荷，并创建计划任务来保持感染链稳定。

除上述的攻击手段外，我们还捕获到一类基于Mythic C2框架的新型载荷。该组织通过钓鱼邮件下发MSC文档；当用户打开MSC文档后会远程加载一个html文件；文件内嵌混淆的JScript代码，JScript脚本执行时会从远程下载诱饵文档，同时释放恶意dll，并通过白利用的方式加载Mythic C2框架组件构建的恶意dll。



▲图：APT-C-09（摩诃草）组织攻击流程示意图

5.3、APT-C-48（CNC）

APT-C-48（CNC）组织在2025年的主要攻击手法为使用“XXX的简历”为话题的钓鱼活动。如果受害者通过移动设备打开相关钓鱼连接，还会提示“设备不支持”等相关提示。

图①

用户根据提示使用Windows设备点击钓鱼链接，则会下载钓鱼木马。

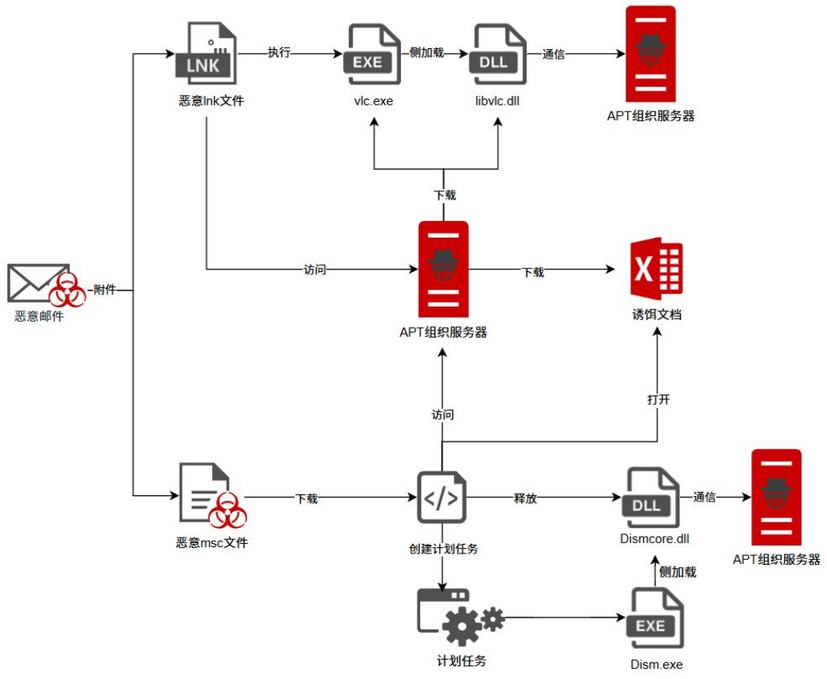
图②

该组织在2025年钓鱼攻击活动中的钓鱼链接使用了仿冒国内外知名邮箱、云盘（云）等常见应用的域名，以增加其点击成功率。

▲图①：非Win设备点击钓鱼连接提示　　图②：木马示例

其钓鱼攻击手法是通过钓鱼邮件下发伪装成PDF的LNK文件，当用户运行文件后会执行内嵌的PS指令下载后续恶意载荷，并创建计划任务来保持感染链稳定。

除上述的攻击手段外，我们还捕获到一类基于Mythic C2框架的新型载荷。该组织通过钓鱼邮件下发MSC文档；当用户打开MSC文档后会远程加载一个html文件；文件内嵌混淆的JScript代码，JScript脚本执行时会从远程下载诱饵文档，同时释放恶意dll，并通过白利用的方式加载Mythic C2框架组件构建的恶意dll。



▲图：APT-C-09（摩诃草）组织攻击流程示意图

5.3、APT-C-48（CNC）

APT-C-48（CNC）组织在2025年的主要攻击手法为使用“XXX的简历”为话题的钓鱼活动。如果受害者通过移动设备打开相关钓鱼连接，还会提示“设备不支持”等相关提示。

图①

用户根据提示使用Windows设备点击钓鱼链接，则会下载钓鱼木马。

图②

该组织在2025年钓鱼攻击活动中的钓鱼链接使用了仿冒国内外知名邮箱、云盘（云）等常见应用的域名，以增加其点击成功率。

▲图①：非Win设备点击钓鱼连接提示　　图②：木马示例

恶意域名	仿冒的目标应用
cloudauwei[.]com	华为云
cloudhauwei[.]com	华为云
mailcloud163[.]com	163邮箱
coremailcloucl[.]com	Coremail邮箱
mailcloucl[.]com	MailCloud邮箱
qq.ernailcloud[.]com	qq邮箱

5.4、APT-C-76（银环蛇）

APT-C-76（银环蛇）是2025年360最新披露的具有南亚背景的APT组织。该组织于2024年年末开始针对我国和巴基斯坦等地缘周边国家展开攻击活动，目前呈现高度活跃状态。其主要通过投递鱼叉钓鱼邮件的方式诱导用户自行打开恶意攻击载荷以建立落脚点，对受影响设备进行持续控制与窃密。

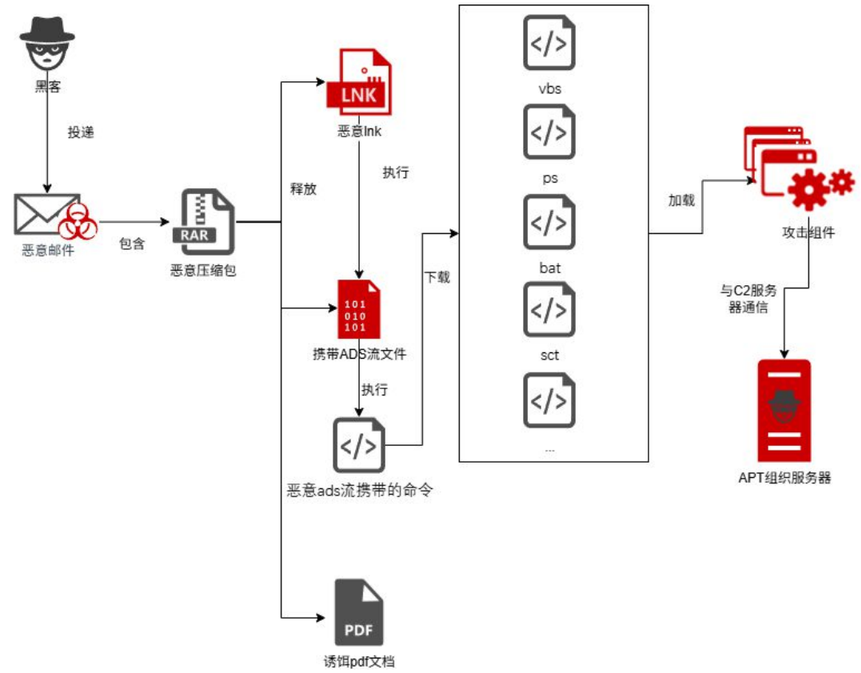
依托于360安全大模型，我们发现APT-C-76（银环蛇）组织先后对我国国内文娱产业、教育领域发起攻击。其中对教育领域的攻击使用了WinRAR在野0day漏洞。

目前发现该组织有三种主要攻击手法。三种手法主要的不同之处是攻击初始的攻击载荷投递和加载过程。

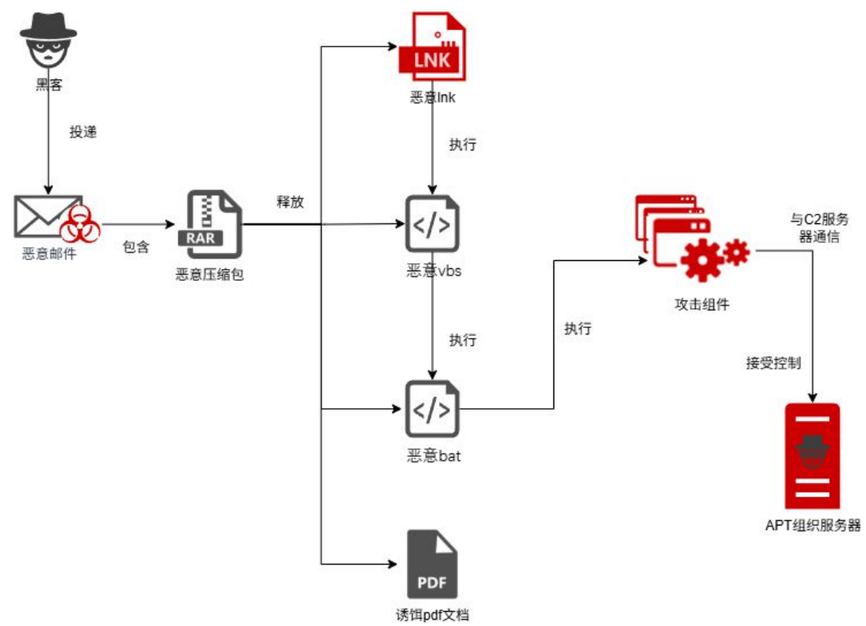
第一种攻击手法中，攻击者通过投递带有伪装为pdf文档的恶意LNK文件、具备ADS流的恶意文件的压缩包作为初始访问阶段攻击载荷以诱导用户执行恶意LNK文件以触发具有ADS流的恶意文件执行。

第二种攻击手法中，攻击者通过投递带有恶意LNK文件、VBS脚本、诱饵pdf文档以及白加黑组件的压缩包作为初始访问阶段攻击载荷诱导用户打开。

第三种攻击手法中，攻击者充分表现出对新型攻击技术的快速实战转化能力，利用披露不久的CVE-2025-8088漏洞构建恶意压缩包作为初始访问阶段攻击载荷，诱导用户打开并解压该压缩包以触发漏洞利用。



图①



图②

▲图①：APT-C-76（银环蛇）攻击流程示意图一　　图②：APT-C-76（银环蛇）攻击流程示意图二

恶意域名	仿冒的目标应用
cloudauwei[.]com	华为云
cloudhauwei[.]com	华为云
mailcloud163[.]com	163邮箱
coremailcloucl[.]com	Coremail邮箱
mailcloucl[.]com	MailCloud邮箱
qq.ernailcloud[.]com	qq邮箱

5.4、APT-C-76（银环蛇）

APT-C-76（银环蛇）是2025年360最新披露的具有南亚背景的APT组织。该组织于2024年年末开始针对我国和巴基斯坦等地缘周边国家展开攻击活动，目前呈现高度活跃状态。其主要通过投递鱼叉钓鱼邮件的方式诱导用户自行打开恶意攻击载荷以建立落脚点，对受影响设备进行持续控制与窃密。

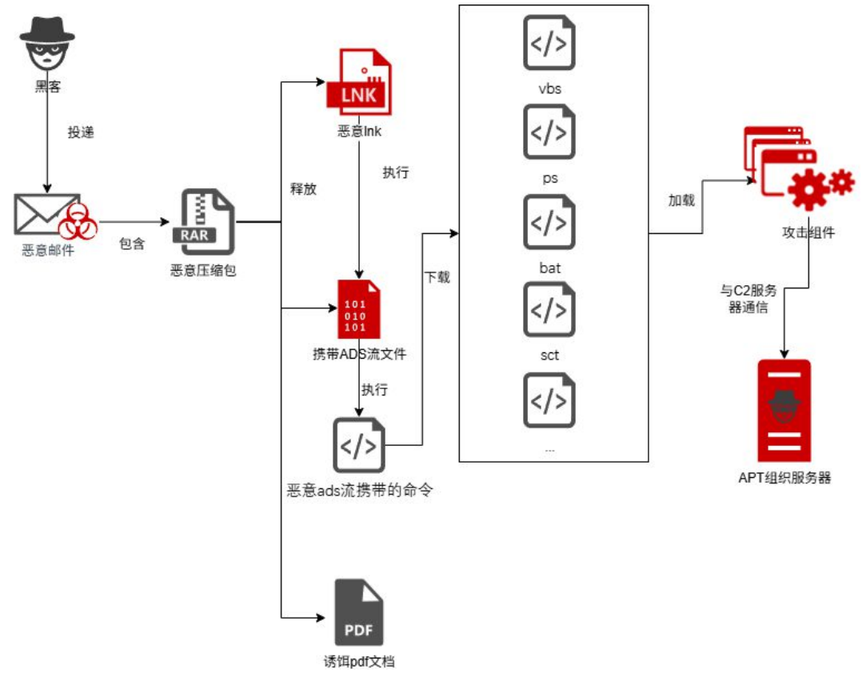
依托于360安全大模型，我们发现APT-C-76（银环蛇）组织先后对我国国内文娱产业、教育领域发起攻击。其中对教育领域的攻击使用了WinRAR在野0day漏洞。

目前发现该组织有三种主要攻击手法。三种手法主要的不同之处是攻击初始的攻击载荷投递和加载过程。

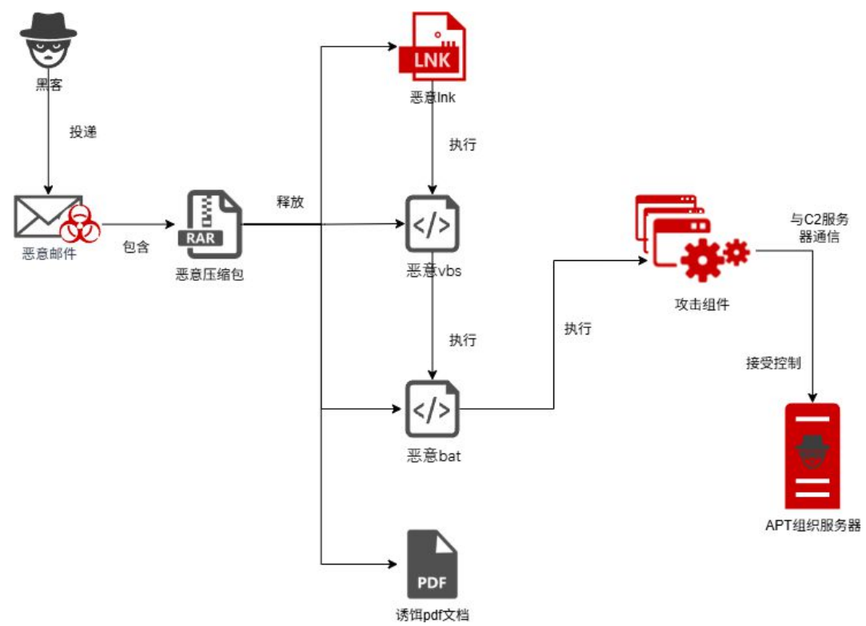
第一种攻击手法中，攻击者通过投递带有伪装为pdf文档的恶意LNK文件、具备ADS流的恶意文件的压缩包作为初始访问阶段攻击载荷以诱导用户执行恶意LNK文件以触发具有ADS流的恶意文件执行。

第二种攻击手法中，攻击者通过投递带有恶意LNK文件、VBS脚本、诱饵pdf文档以及白加黑组件的压缩包作为初始访问阶段攻击载荷诱导用户打开。

第三种攻击手法中，攻击者充分表现出对新型攻击技术的快速实战转化能力，利用披露不久的CVE-2025-8088漏洞构建恶意压缩包作为初始访问阶段攻击载荷，诱导用户打开并解压该压缩包以触发漏洞利用。

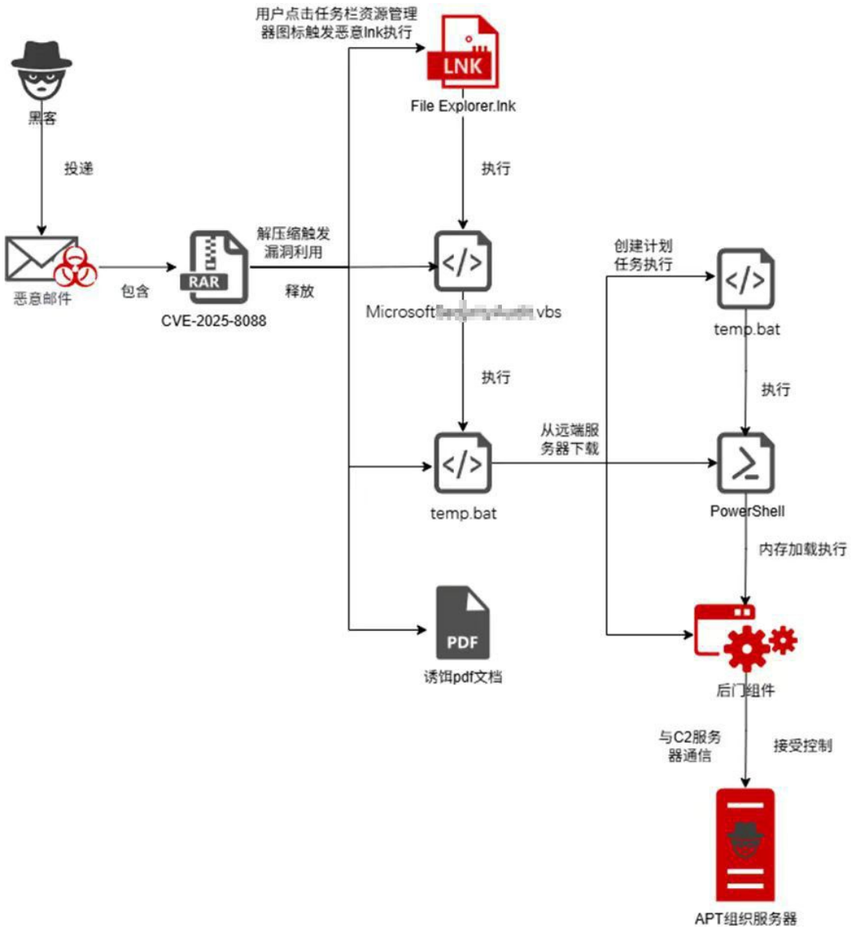


图①



图②

▲图①：APT-C-76（银环蛇）攻击流程示意图一　　图②：APT-C-76（银环蛇）攻击流程示意图二



5.5、其他APT组织

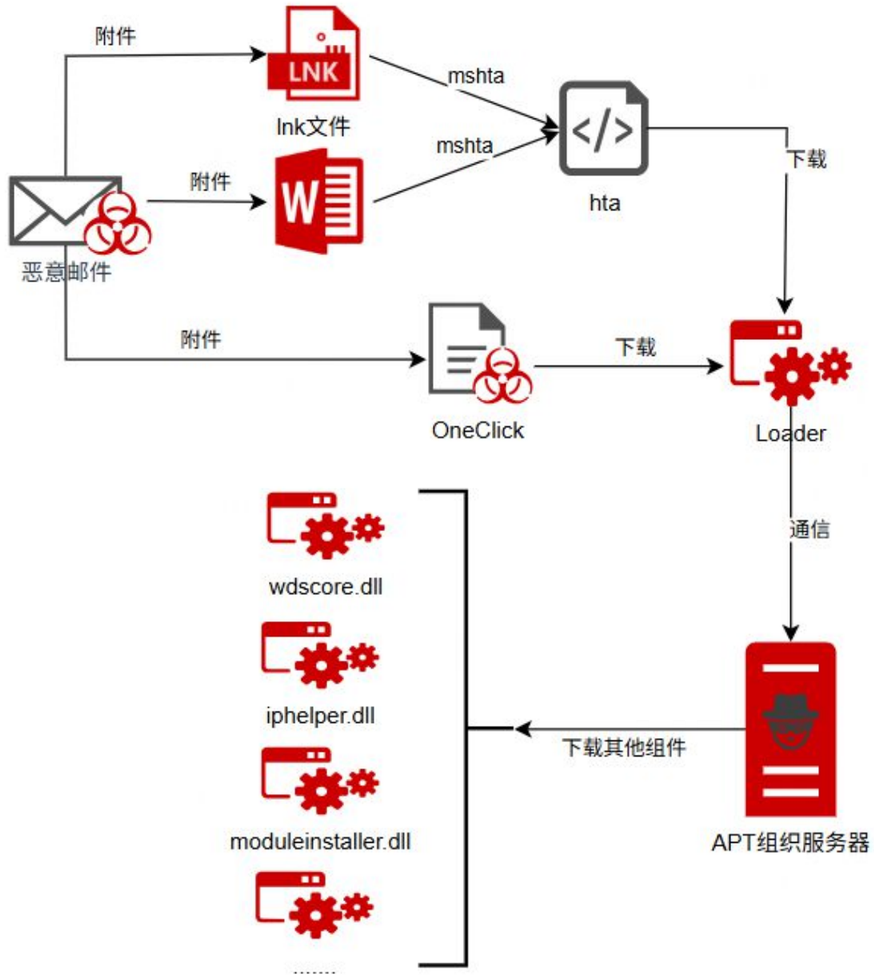
来自南亚地区的APT-C-24（响尾蛇）、APT-C-35（肚脑虫）、APT-C-56（透明部落）、APT-C-70（独角犀）等组织，在2025年对地缘周边国家的攻击活动持活跃。

▲图：APT-C-76（银环蛇）攻击流程示意图三

5.5.1、APT-C-24（响尾蛇）

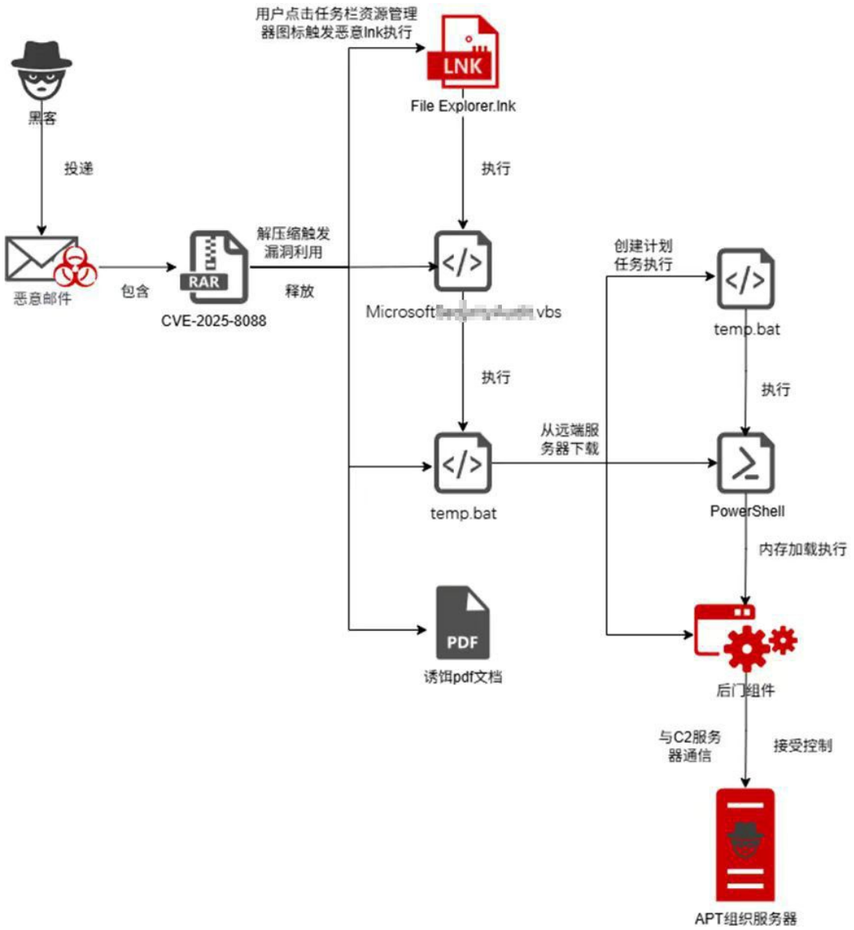
2025年，APT-C-24（响尾蛇）组织的主要攻击目标集中在孟加拉、巴基斯坦等地区。少量攻击针对国内的部分企业和机构。

2025年攻击活动中，APT-C-24（响尾蛇）组织多是使用LNK或包含早期的Office漏洞（如CVE-2017-11882）的文档，分多阶段下发攻击样本，最后实现服务驻留的目的。在下半年中，我们发现该组织部分活动还使用了OneClick文件作为初始载荷来下发攻击样本。



APT-C-24（响尾蛇）组织在钓鱼信息收集方面，会使用内嵌入钓鱼连接的pdf文件，受害者点击后跳转伪装成政府相关的钓鱼网站。

▲图：APT-C-24（响尾蛇）组织攻击流程示意图



5.5、其他APT组织

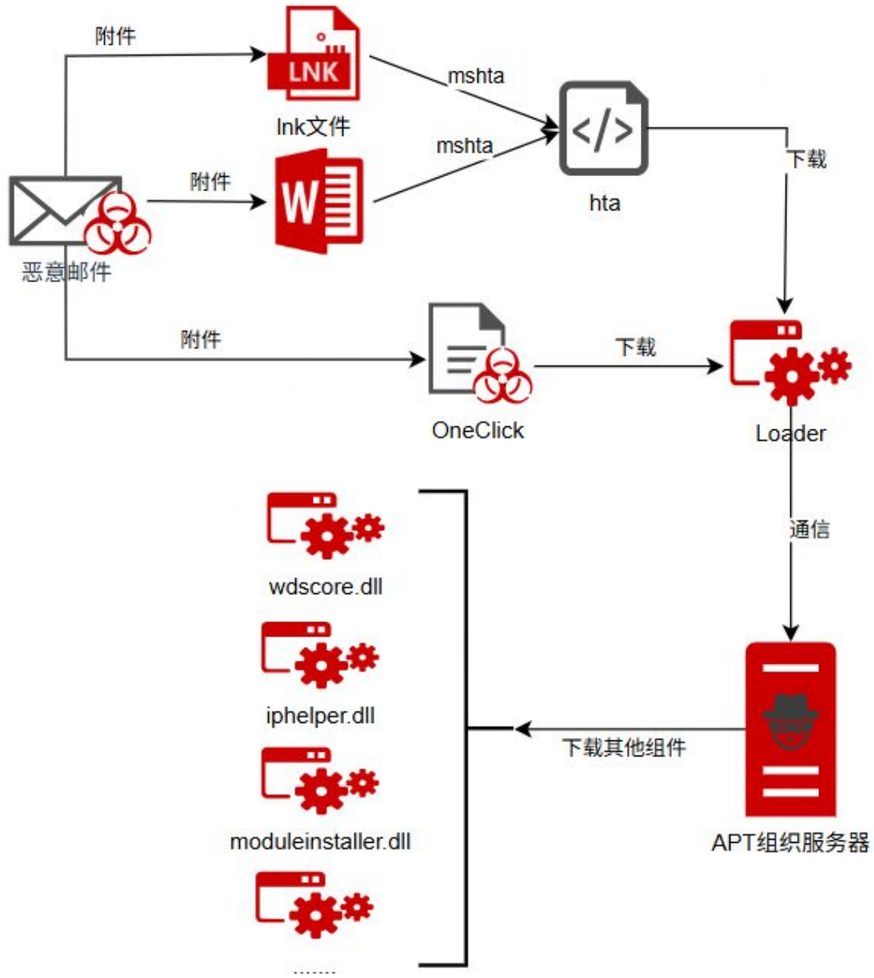
来自南亚地区的APT-C-24（响尾蛇）、APT-C-35（肚脑虫）、APT-C-56（透明部落）、APT-C-70（独角犀）等组织，在2025年对地缘周边国家的攻击活动持活跃。

▲图：APT-C-76（银环蛇）攻击流程示意图三

5.5.1、APT-C-24（响尾蛇）

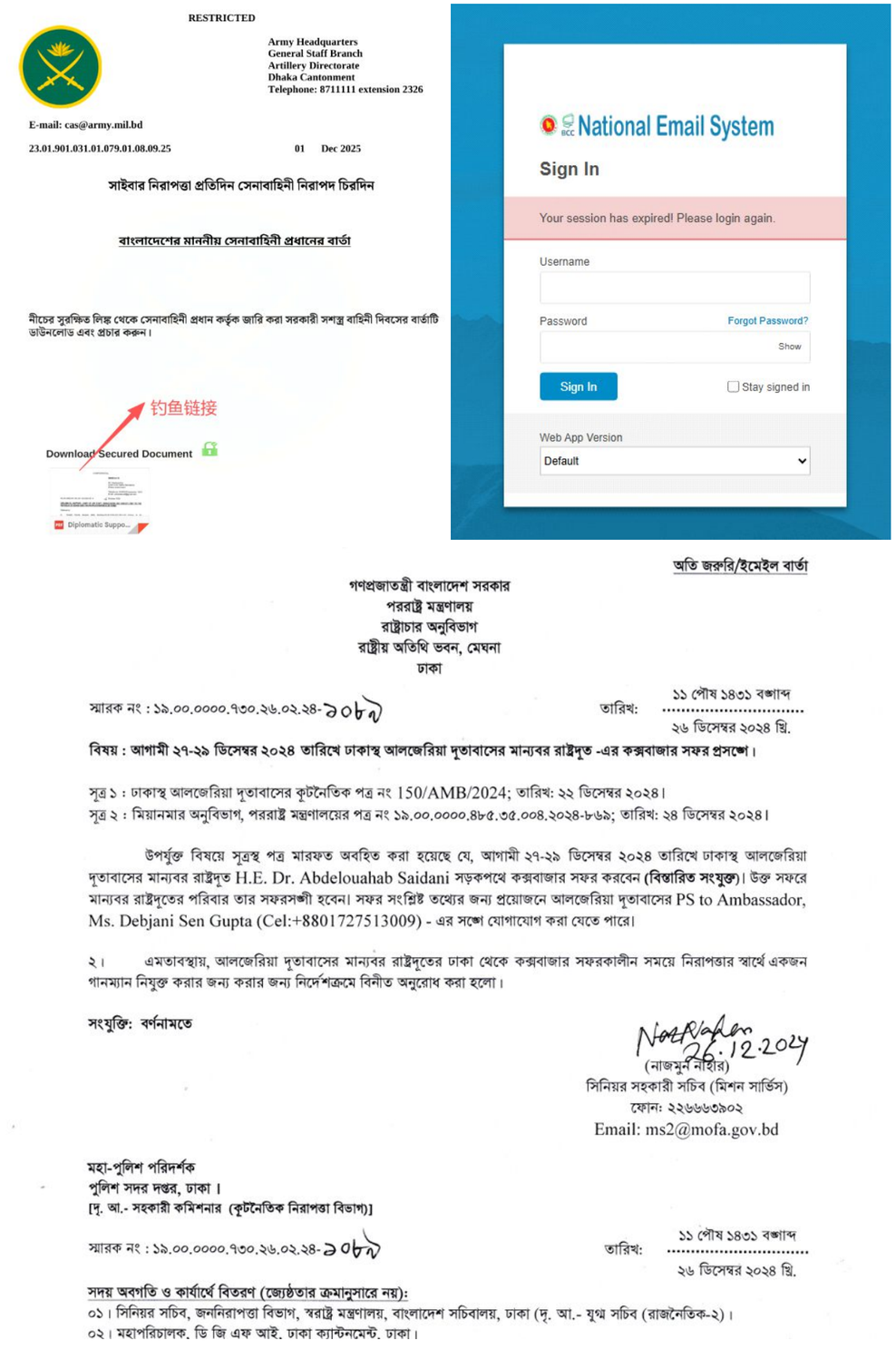
2025年，APT-C-24（响尾蛇）组织的主要攻击目标集中在孟加拉、巴基斯坦等地区。少量攻击针对国内的部分企业和机构。

2025年攻击活动中，APT-C-24（响尾蛇）组织多是使用LNK或包含早期的Office漏洞（如CVE-2017-11882）的文档，分多阶段下发攻击样本，最后实现服务驻留的目的。在下半年中，我们发现该组织部分活动还使用了OneClick文件作为初始载荷来下发攻击样本。



APT-C-24（响尾蛇）组织在钓鱼信息收集方面，会使用内嵌入钓鱼连接的pdf文件，受害者点击后跳转伪装成政府相关的钓鱼网站。

▲图：APT-C-24（响尾蛇）组织攻击流程示意图



RESTRICTED

Army Headquarters
General Staff Branch
Artillery Directorate
Dhaka Cantonment
Telephone: 8711111 extension 2326

E-mail: cas@army.mil.bd

23.01.901.031.01.079.01.08.09.25 01 Dec 2025

সাইবার নিরাপত্তা প্রতিদিন সেনাবাহিনী নিরাপদ চিরদিন

বাংলাদেশের মাননীয় সেনাবাহিনী প্রধানের বার্তা

নীচের সুরক্ষিত লিঙ্ক থেকে সেনাবাহিনী প্রধান কর্তৃক জারি করা সরকারী সশস্ত্র বাহিনী দিবসের বার্তাটি ডাউনলোড এবং প্রচার করুন।

钓鱼链接

Download Secured Document

Diplomatic Suppo...

National Email System

Sign In

Your session has expired! Please login again.

Username

Password Forgot Password?

Show

Sign In Stay signed in

Web App Version

Default

অতি জরুরি/ইমেইল বার্তা

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
পররাষ্ট্র মন্ত্রণালয়
রাষ্ট্রাচার অনুবিভাগ
রাষ্ট্রীয় অতিথি ভবন, মেঘনা
ঢাকা

স্মারক নং : ১৯.০০.০০০০.৭৩০.২৬.০২.২৪-৯০৮৭ তারিখ: ১১ পৌষ ১৪৩১ বঙ্গাব্দ / ২৬ ডিসেম্বর ২০২৪ খ্রি.

বিষয় : আগামী ২৭-২৯ ডিসেম্বর ২০২৪ তারিখে ঢাকাস্থ আলজেরিয়া দূতাবাসের মান্যবর রাষ্ট্রদূত -এর কক্সবাজার সফর প্রসঙ্গে।

সূত্র ১ : ঢাকাস্থ আলজেরিয়া দূতাবাসের কূটনৈতিক পত্র নং 150/AMB/2024; তারিখ: ২২ ডিসেম্বর ২০২৪।
সূত্র ২ : মিয়ানমার অনুবিভাগ, পররাষ্ট্র মন্ত্রণালয়ের পত্র নং ১৯.০০.০০০০.৪৮৫.৩৫.০০৪.২০২৪-৮৬৯; তারিখ: ২৪ ডিসেম্বর ২০২৪।

উপর্যুক্ত বিষয়ে সূত্রস্থ পত্র মারফত অবহিত করা হয়েছে যে, আগামী ২৭-২৯ ডিসেম্বর ২০২৪ তারিখে ঢাকাস্থ আলজেরিয়া দূতাবাসের মান্যবর রাষ্ট্রদূত H.E. Dr. Abdelouahab Saidani সড়কপথে কক্সবাজার সফর করবেন **(বিস্তারিত সংযুক্ত)**। উক্ত সফরে মান্যবর রাষ্ট্রদূতের পরিবার তার সফরসঙ্গী হবেন। সফর সংশ্লিষ্ট তথ্যের জন্য প্রয়োজনে আলজেরিয়া দূতাবাসের PS to Ambassador, Ms. Debjani Sen Gupta (Cel:+8801727513009) - এর সঙ্গে যোগাযোগ করা যেতে পারে।

২। এমতাবস্থায়, আলজেরিয়া দূতাবাসের মান্যবর রাষ্ট্রদূতের ঢাকা থেকে কক্সবাজার সফরকালীন সময়ে নিরাপত্তার স্বার্থে একজন গানম্যান নিযুক্ত করার জন্য করার জন্য নির্দেশক্রমে বিনীত অনুরোধ করা হলো।

সংযুক্তি: বর্ণনামতে

26.12.2024
(নাজমুন নাহার)
সিনিয়র সহকারী সচিব (মিশন সার্ভিস)
ফোন: ২২৬৬৬৩৯০২
Email: ms2@mofa.gov.bd

মহা-পুলিশ পরিদর্শক
পুলিশ সদর দপ্তর, ঢাকা।
[দৃ. আ.- সহকারী কমিশনার (কূটনৈতিক নিরাপত্তা বিভাগ)]

স্মারক নং : ১৯.০০.০০০০.৭৩০.২৬.০২.২৪-৯০৮৭ তারিখ: ১১ পৌষ ১৪৩১ বঙ্গাব্দ / ২৬ ডিসেম্বর ২০২৪ খ্রি.

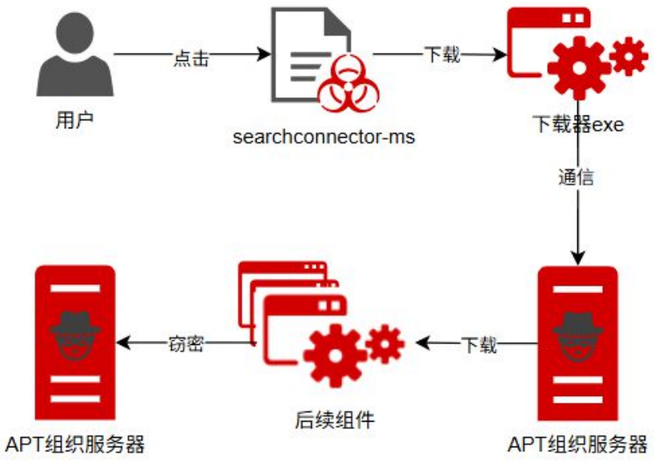
সদয় অবগতি ও কার্যার্থে বিতরণ (জ্যেষ্ঠতার ক্রমানুসারে নয়):
০১। সিনিয়র সচিব, জননিরাপত্তা বিভাগ, স্বরাষ্ট্র মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা (দৃ. আ.- যুগ্ম সচিব (রাজনৈতিক-২)।
০২। মহাপরিচালক, ডি জি এফ আই, ঢাকা ক্যান্টনমেন্ট, ঢাকা।

▲图：APT-C-24（响尾蛇）组织构造的含有钓鱼链接的pdf文档

5.5.2、APT-C-35（肚脑虫）

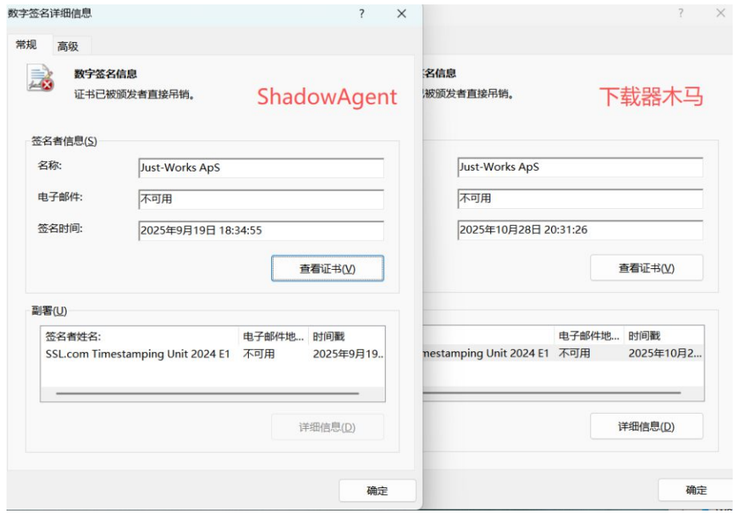
APT-C-35（肚脑虫）组织在2025年的活动与历史相比稍有变化，改为使用searchconnector-ms类型文件作为初始载荷。其核心攻击还是集中在巴基斯坦、孟加拉等地区。

当用户点击searchconnector-ms会远程连接到伪装成pdf文档的下载器样本；下载器样本会下载后续的攻击组件，并将其通过COM注册为计划任务。



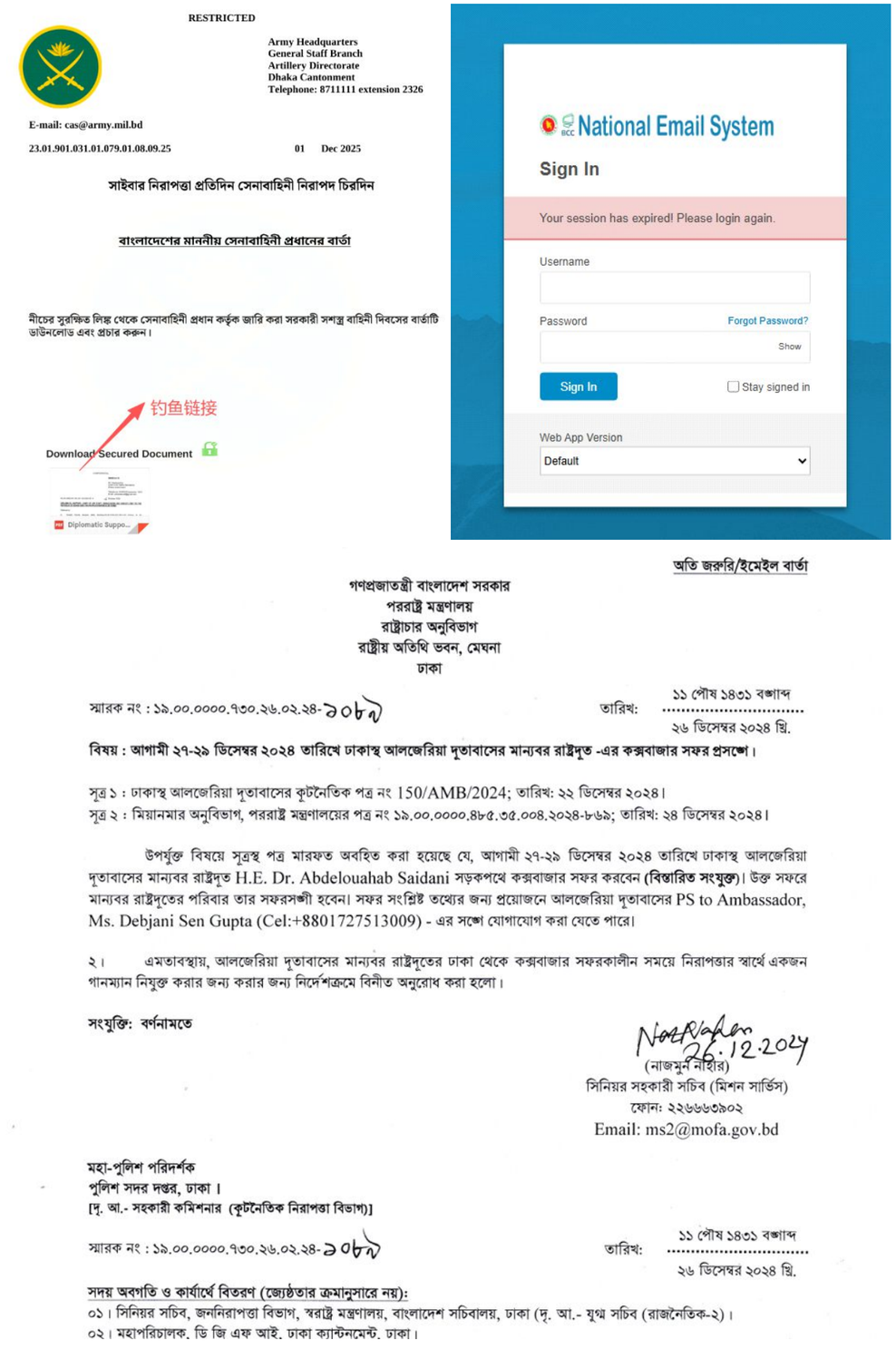
图①

我们在2025年中观测到多起spyder事件与APT-C-35（肚脑虫）活动有所关联。其中，有的事件是C2相关联，有的是数字签名相关联。在以往历史事件中spyder为APT-C-09（摩诃草）常用的组件之一，由此推测spyder可能成为APT-C-09（摩诃草）与APT-C-35（肚脑虫）共用组件。



图②

▲图①：APT-C-35（肚脑虫）组织攻击流程图示意图　图②：左为spyder相关样本、右为APT-C-35（肚脑虫）下载器木马



RESTRICTED

Army Headquarters
General Staff Branch
Artillery Directorate
Dhaka Cantonment
Telephone: 8711111 extension 2326

E-mail: cas@army.mil.bd

23.01.901.031.01.079.01.08.09.25 01 Dec 2025

সাইবার নিরাপত্তা প্রতিদিন সেনাবাহিনী নিরাপদ চিরদিন

বাংলাদেশের মাননীয় সেনাবাহিনী প্রধানের বার্তা

নীচের সুরক্ষিত লিঙ্ক থেকে সেনাবাহিনী প্রধান কর্তৃক জারি করা সরকারী সশস্ত্র বাহিনী দিবসের বার্তাটি ডাউনলোড এবং প্রচার করুন।

钓鱼链接

Download Secured Document

Diplomatic Suppo...

National Email System

Sign In

Your session has expired! Please login again.

Username

Password Forgot Password?

Show

Sign In Stay signed in

Web App Version

Default

অতি জরুরি/ইমেইল বার্তা

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
পররাষ্ট্র মন্ত্রণালয়
রাষ্ট্রাচার অনুবিভাগ
রাষ্ট্রীয় অতিথি ভবন, মেঘনা
ঢাকা

স্মারক নং : ১৯.০০.০০০০.৭৩০.২৬.০২.২৪-৯০৮৭ তারিখ: ১১ পৌষ ১৪৩১ বঙ্গাব্দ / ২৬ ডিসেম্বর ২০২৪ খ্রি.

বিষয় : আগামী ২৭-২৯ ডিসেম্বর ২০২৪ তারিখে ঢাকাস্থ আলজেরিয়া দূতাবাসের মান্যবর রাষ্ট্রদূত -এর কক্সবাজার সফর প্রসঙ্গে।

সূত্র ১ : ঢাকাস্থ আলজেরিয়া দূতাবাসের কূটনৈতিক পত্র নং 150/AMB/2024; তারিখ: ২২ ডিসেম্বর ২০২৪।
সূত্র ২ : মিয়ানমার অনুবিভাগ, পররাষ্ট্র মন্ত্রণালয়ের পত্র নং ১৯.০০.০০০০.৪৮৫.৩৫.০০৪.২০২৪-৮৬৯; তারিখ: ২৪ ডিসেম্বর ২০২৪।

উপর্যুক্ত বিষয়ে সূত্রস্থ পত্র মারফত অবহিত করা হয়েছে যে, আগামী ২৭-২৯ ডিসেম্বর ২০২৪ তারিখে ঢাকাস্থ আলজেরিয়া দূতাবাসের মান্যবর রাষ্ট্রদূত H.E. Dr. Abdelouahab Saidani সড়কপথে কক্সবাজার সফর করবেন **(বিস্তারিত সংযুক্ত)**। উক্ত সফরে মান্যবর রাষ্ট্রদূতের পরিবার তার সফরসঙ্গী হবেন। সফর সংশ্লিষ্ট তথ্যের জন্য প্রয়োজনে আলজেরিয়া দূতাবাসের PS to Ambassador, Ms. Debjani Sen Gupta (Cel:+8801727513009) - এর সঙ্গে যোগাযোগ করা যেতে পারে।

২। এমতাবস্থায়, আলজেরিয়া দূতাবাসের মান্যবর রাষ্ট্রদূতের ঢাকা থেকে কক্সবাজার সফরকালীন সময়ে নিরাপত্তার স্বার্থে একজন গানম্যান নিযুক্ত করার জন্য করার জন্য নির্দেশক্রমে বিনীত অনুরোধ করা হলো।

সংযুক্তি: বর্ণনামতে

26.12.2024
(নাজমুন নাহার)
সিনিয়র সহকারী সচিব (মিশন সার্ভিস)
ফোন: ২২৬৬৬৩৯০২
Email: ms2@mofa.gov.bd

মহা-পুলিশ পরিদর্শক
পুলিশ সদর দপ্তর, ঢাকা।
[দৃ. আ.- সহকারী কমিশনার (কূটনৈতিক নিরাপত্তা বিভাগ)]

স্মারক নং : ১৯.০০.০০০০.৭৩০.২৬.০২.২৪-৯০৮৭ তারিখ: ১১ পৌষ ১৪৩১ বঙ্গাব্দ / ২৬ ডিসেম্বর ২০২৪ খ্রি.

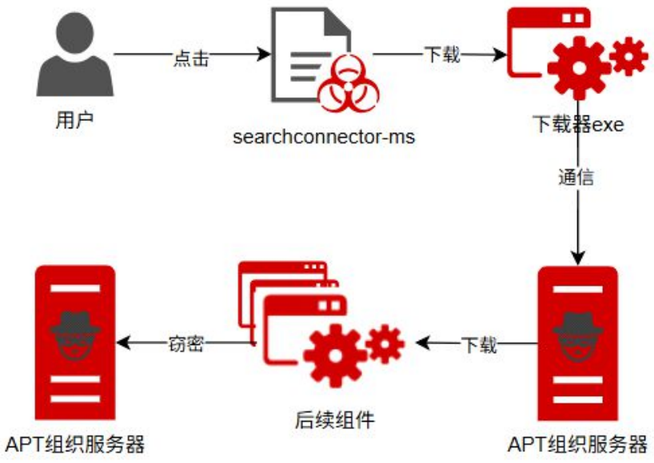
সদয় অবগতি ও কার্যার্থে বিতরণ (জ্যেষ্ঠতার ক্রমানুসারে নয়):
০১। সিনিয়র সচিব, জননিরাপত্তা বিভাগ, স্বরাষ্ট্র মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা (দৃ. আ.- যুগ্ম সচিব (রাজনৈতিক-২)।
০২। মহাপরিচালক, ডি জি এফ আই, ঢাকা ক্যান্টনমেন্ট, ঢাকা।

▲图：APT-C-24（响尾蛇）组织构造的含有钓鱼链接的pdf文档

5.5.2、APT-C-35（肚脑虫）

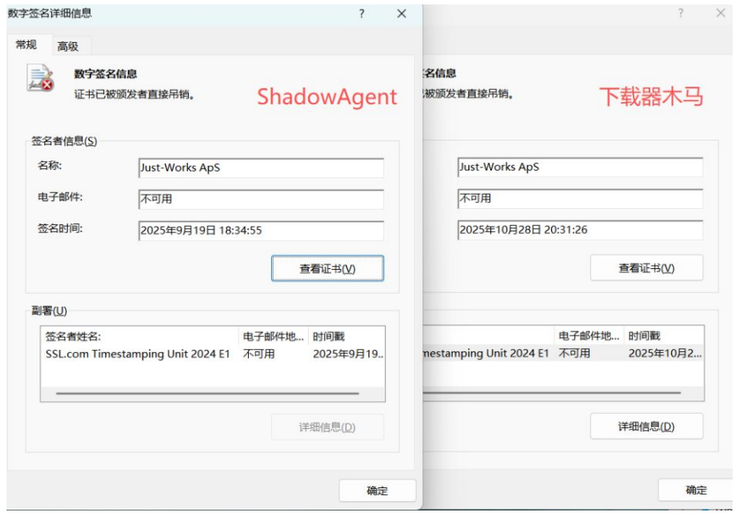
APT-C-35（肚脑虫）组织在2025年的活动与历史相比稍有变化，改为使用searchconnector-ms类型文件作为初始载荷。其核心攻击还是集中在巴基斯坦、孟加拉等地区。

当用户点击searchconnector-ms会远程连接到伪装成pdf文档的下载器样本；下载器样本会下载后续的攻击组件，并将其通过COM注册为计划任务。



图①

我们在2025年中观测到多起spyder事件与APT-C-35（肚脑虫）活动有所关联。其中，有的事件是C2相关联，有的是数字签名相关联。在以往历史事件中spyder为APT-C-09（摩诃草）常用的组件之一，由此推测spyder可能成为APT-C-09（摩诃草）与APT-C-35（肚脑虫）共用组件。



图②

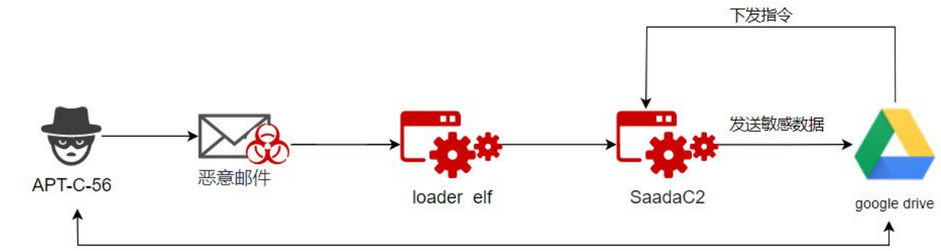
▲图①：APT-C-35（肚脑虫）组织攻击流程图示意图　图②：左为spyder相关样本、右为APT-C-35（肚脑虫）下载器木马

5.5.3、APT-C-56（透明部落）

APT-C-56（透明部落）组织长期针南亚地区，尤其是印度相关的政府、医疗、电力、金融、制造业等行业领域目标，进行高强度的以信息窃取为主要目的的攻击活动。

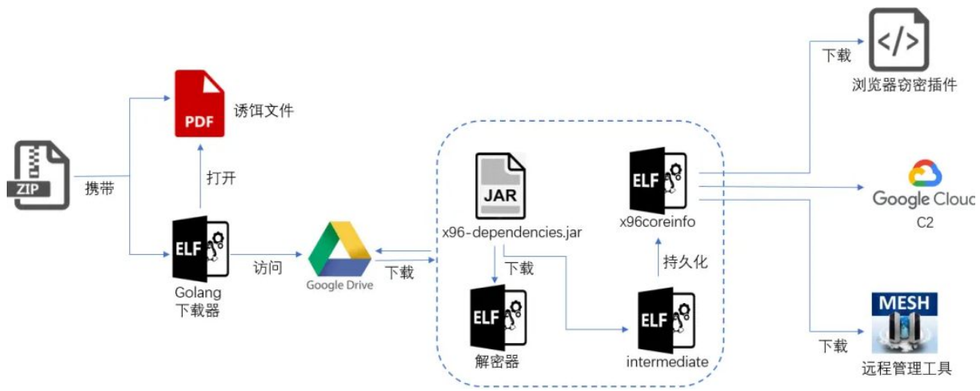
2025年，APT-C-56（透明部落）组织使用的攻击手法是通过钓鱼邮件将Windows快捷方式文件和Linux快捷方式文件投递到目标群体，诱使用户运行快捷方式文件，下载木马进行后续攻击。

透明部落组织投递的SaadaC2后门程序主要功能是窃取用户浏览器密码、窃取文档文件、下载MeshAgent后门、窃取指定网站的Cookie信息，此后门程序在执行过程中大量使用了Google Drive云服务。



图①

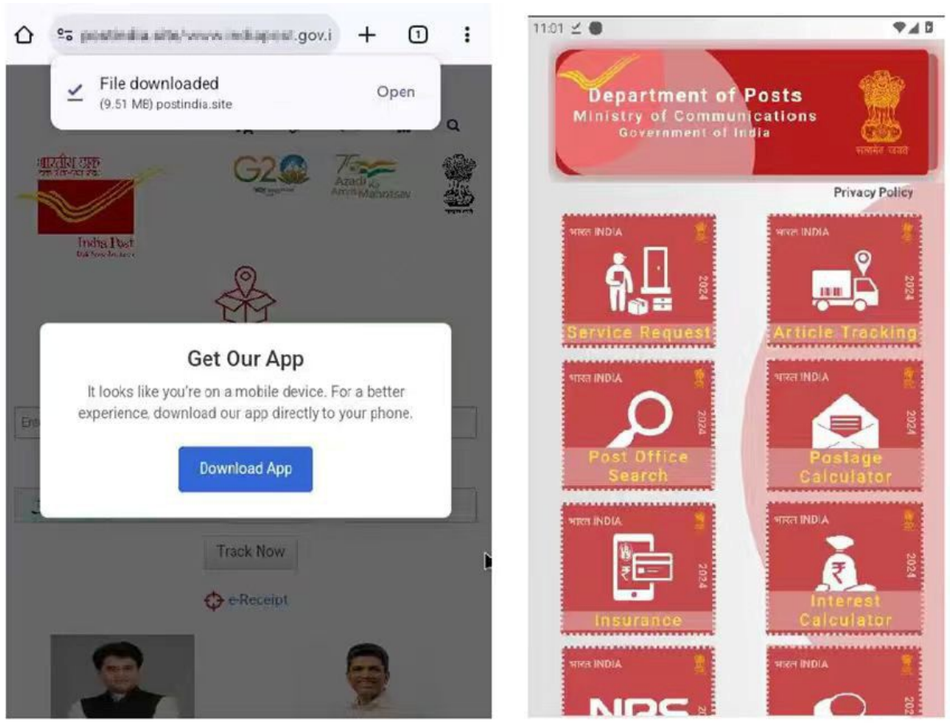
360高级威胁研究院捕获到了一起透明部落组织使用DISGOMOJI恶意软件变体的攻击活动，该软件是基于Golang编写的ELF可执行程序，其借助谷歌云盘（Google Drive）进行下发，并且数据回传到谷歌云服务（Google Cloud Platform），此外还会下载浏览器窃密插件和远程管理工具以实现进一步的窃密行动和远程控制。



图②

▲图①：APT-C-56（透明部落）组织攻击流程示意图（一）　图②：APT-C-56（透明部落）组织攻击流程示意图（二）

APT-C-56（透明部落）组织针对移动平台的依旧以建立仿冒网站诱使用户下载伪装的后门程序为主要攻击手段，攻击频率有所降低。安卓后门程序具备窃取用户移动设备中敏感文件的功能，根据不同的手机型号选择不同自启动方式。该后门运行后还会对自身的程序的图标进行替换，以实现隐藏。



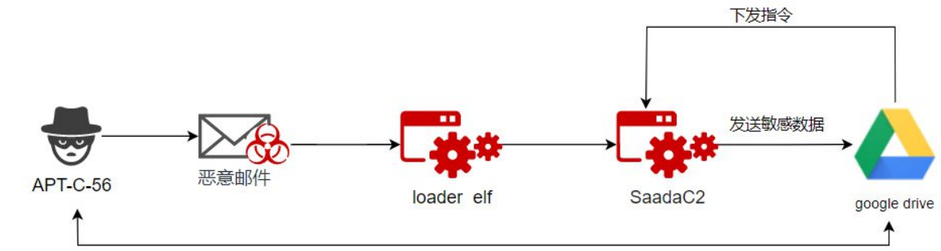
▲图：APT-C-56（透明部落）组织仿冒网站截图

5.5.3、APT-C-56（透明部落）

APT-C-56（透明部落）组织长期针南亚地区，尤其是印度相关的政府、医疗、电力、金融、制造业等行业领域目标，进行高强度的以信息窃取为主要目的的攻击活动。

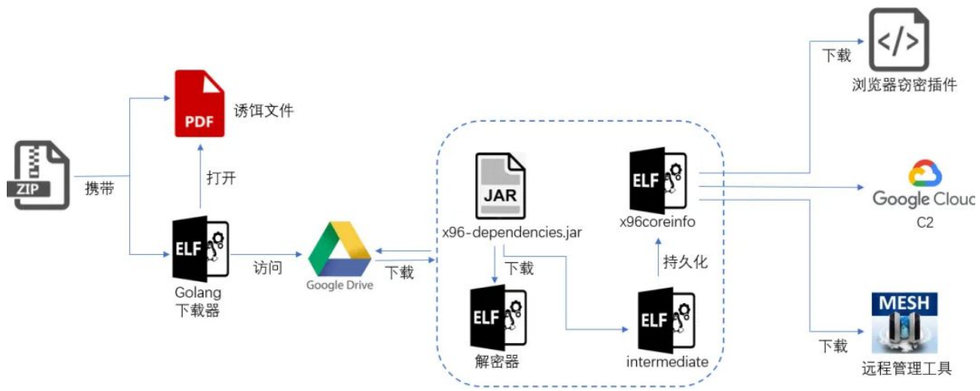
2025年，APT-C-56（透明部落）组织使用的攻击手法是通过钓鱼邮件将Windows快捷方式文件和Linux快捷方式文件投递到目标群体，诱使用户运行快捷方式文件，下载木马进行后续攻击。

透明部落组织投递的SaadaC2后门程序主要功能是窃取用户浏览器密码、窃取文档文件、下载MeshAgent后门、窃取指定网站的Cookie信息，此后门程序在执行过程中大量使用了Google Drive云服务。



图①

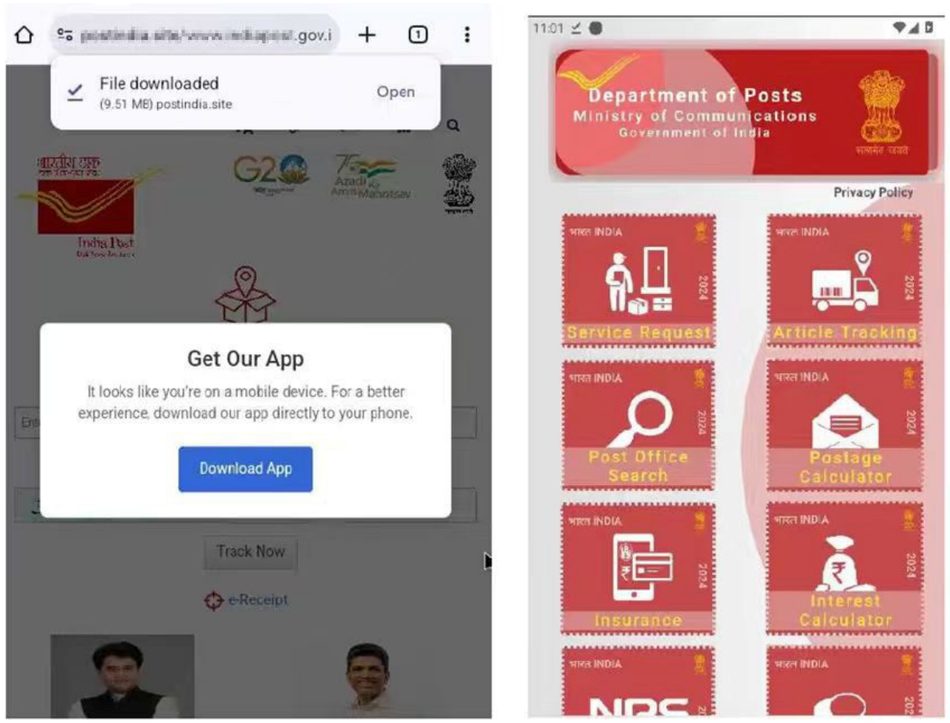
360高级威胁研究院捕获到了一起透明部落组织使用DISGOMOJI恶意软件变体的攻击活动，该软件是基于Golang编写的ELF可执行程序，其借助谷歌云盘（Google Drive）进行下发，并且数据回传到谷歌云服务（Google Cloud Platform），此外还会下载浏览器窃密插件和远程管理工具以实现进一步的窃密行动和远程控制。



图②

▲图①：APT-C-56（透明部落）组织攻击流程示意图（一）　图②：APT-C-56（透明部落）组织攻击流程示意图（二）

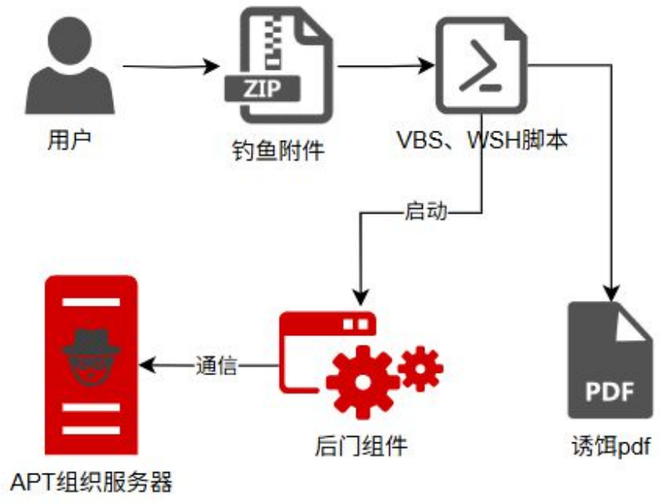
APT-C-56（透明部落）组织针对移动平台的依旧以建立仿冒网站诱使用户下载伪装的后门程序为主要攻击手段，攻击频率有所降低。安卓后门程序具备窃取用户移动设备中敏感文件的功能，根据不同的手机型号选择不同自启动方式。该后门运行后还会对自身的程序的图标进行替换，以实现隐藏。



▲图：APT-C-56（透明部落）组织仿冒网站截图

5.5.4、APT-C-70（独角犀）

APT-C-70（独角犀）组织近期主要通过投递带有“学位”、“代码”相关主题的钓鱼诱饵文件进行钓鱼攻击。攻击者在钓鱼邮件附件内嵌入多个pdf文件和伪装成pdfviewer的脚本，诱骗用户点击恶意脚本，从而执行后续木马组件。攻击流程如下图所示。

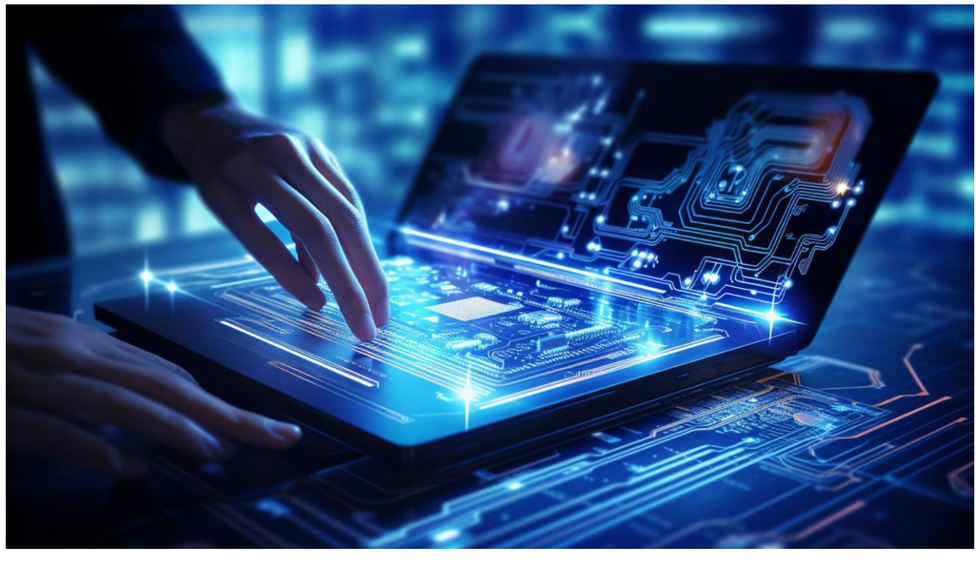


▲图：APT-C-70（独角犀）组织攻击流程示意图

6、东欧

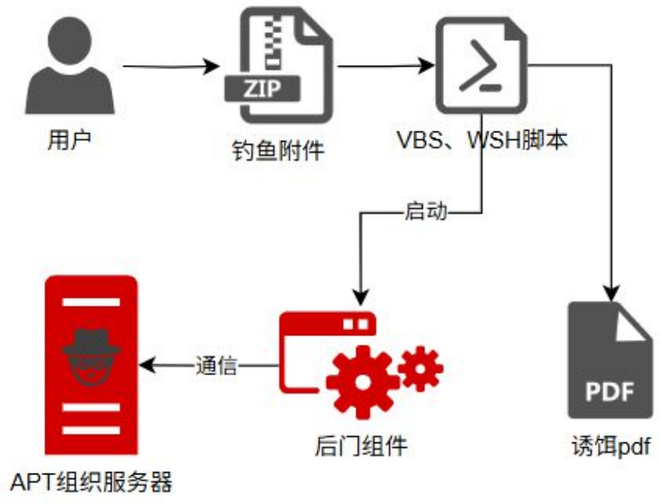
2025年是俄乌冲突进入“高强度消耗战常态化”与“战略僵局深化”的关键一年，其核心特征可概括为：低速推进、高成本消耗、外交停滞、技术升级、全球外溢加剧。地缘政治冲突的持续让这里成为网络对抗的“前沿阵地”，网络攻击已从早期的“辅助手段”演变为战略级作战武器，地区APT组织的攻击技术和目标都呈现出鲜明的“实战化”特征。

地区APT组织凭借国家资源与技术储备占据规模优势，攻击活跃。APT组织将网络攻击能力深度嵌入军事与经济消耗战，攻击动机聚焦于情报窃取和系统破坏，成为混合战争的核心组成部分。



5.5.4、APT-C-70（独角犀）

APT-C-70（独角犀）组织近期主要通过投递带有“学位”、“代码”相关主题的钓鱼诱饵文件进行钓鱼攻击。攻击者在钓鱼邮件附件内嵌入多个pdf文件和伪装成pdfviewer的脚本，诱骗用户点击恶意脚本，从而执行后续木马组件。攻击流程如下图所示。

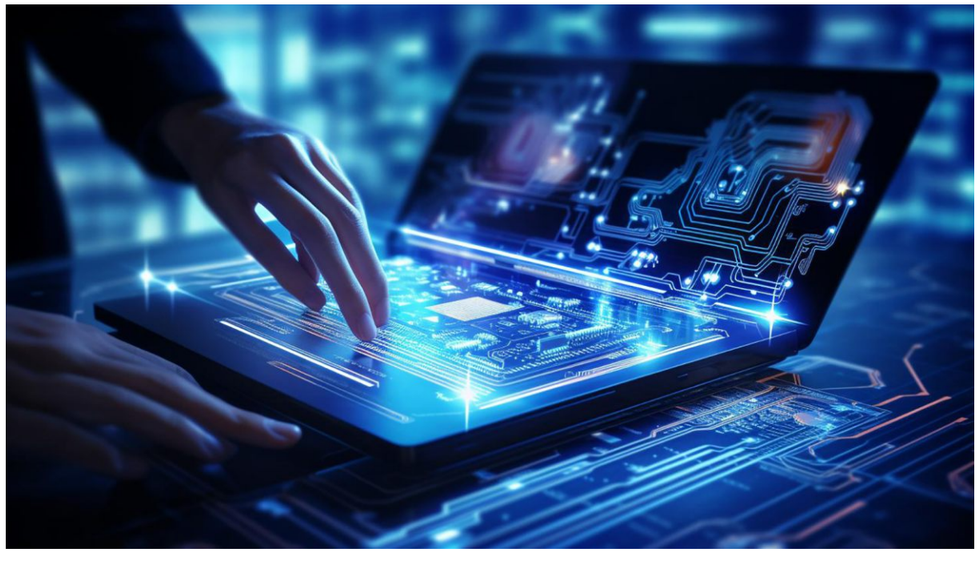


▲图：APT-C-70（独角犀）组织攻击流程示意图

6、东欧

2025年是俄乌冲突进入“高强度消耗战常态化”与“战略僵局深化”的关键一年，其核心特征可概括为：低速推进、高成本消耗、外交停滞、技术升级、全球外溢加剧。地缘政治冲突的持续让这里成为网络对抗的“前沿阵地”，网络攻击已从早期的“辅助手段”演变为战略级作战武器，地区APT组织的攻击技术和目标都呈现出鲜明的“实战化”特征。

地区APT组织凭借国家资源与技术储备占据规模优势，攻击活跃。APT组织将网络攻击能力深度嵌入军事与经济消耗战，攻击动机聚焦于情报窃取和系统破坏，成为混合战争的核心组成部分。

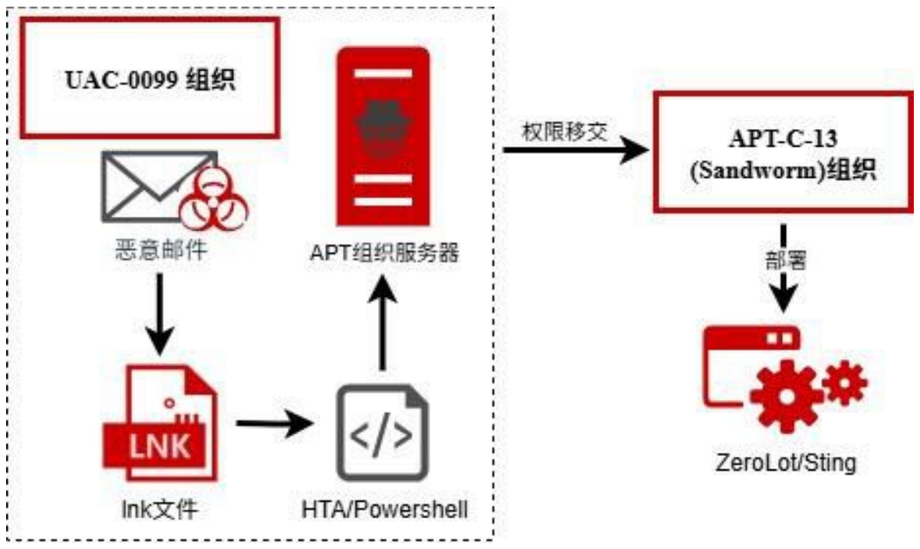


6.1、APT-C-13（Sandworm）

2025年，APT-C-13（Sandworm）组织的攻击活动灵活多变，展现出了极高破坏性。他们利用盗版软件和供应链漏洞进行大范围的底层渗透。

APT-C-13（Sandworm）组织针对乌克兰开展的持续性破坏行动还重点攻击了政府、能源、物流等行业。特别是利用新型擦除器对乌克兰的重要的粮食经济产业和教育体系实施精准的毁灭性打击 。这种“广泛撒网控制”与“精准定点爆破”相结合的模式，对乌克兰国家生存能力造成重大威胁。

APT-C-13（Sandworm）组织的部分“精准攻击”是通过与UAC-0099组织合作代理获取了初始访问权限，之后伪装成Windows计划任务方式来部署“ZeroLot”和“Sting”等多种恶意数据擦除软件。这些攻击活动旨在通过破坏文件系统和主引导记录来不可逆地销毁关键数字资产，从而削弱乌克兰的经济来达成其战略目的。

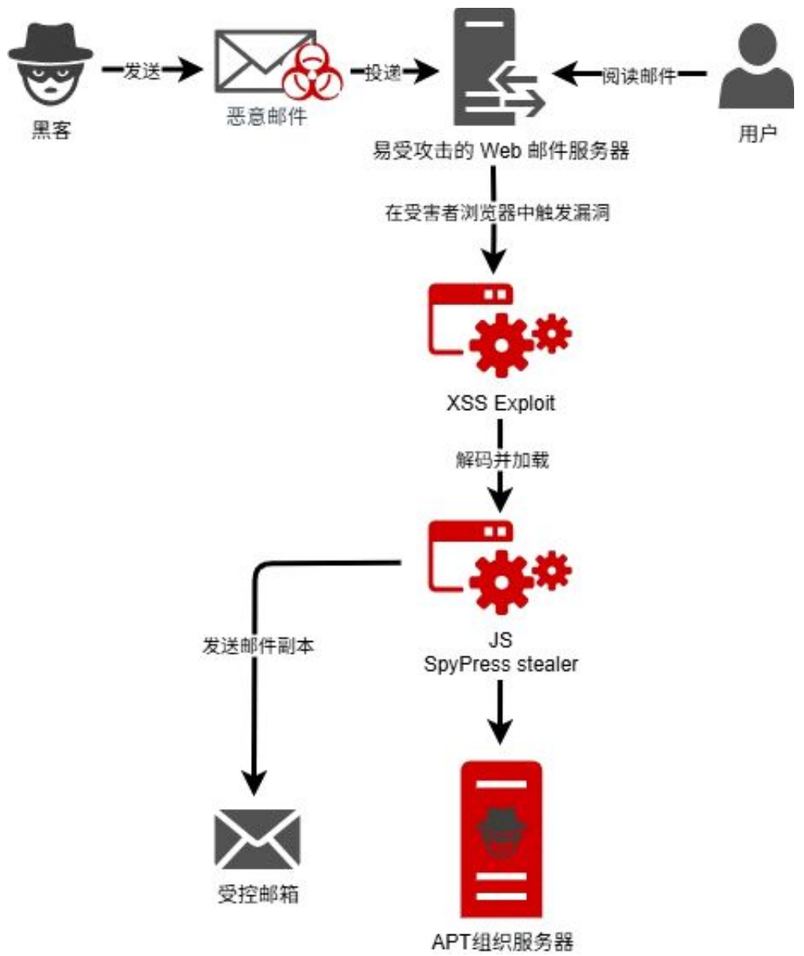


▲图：APT-C-13（Sandworm）组织攻击流程示意图

6.2、APT-C-20（APT28）

2025年，APT-C-20（APT28）组织在攻击武器库的快速迭代和攻击面的多样化方面动作明显。其核心目标依然是服务于地缘政治利益，通过使用Nday和0day漏洞，对乌克兰及其西方盟友实施深度情报窃取。

在APT-C-20（APT28）组织发起的一场针对高价值Web邮件服务器的持续性网络间谍活动。攻击者通过鱼叉式网络钓鱼利用Web邮件平台中的XSS漏洞，向受害者页面注入定制的“SpyPress”恶意JavaScript代码，从而实现对凭据、联系人列表及邮件内容的窃取。攻击者甚至还利用0day漏洞绕过MDaemon多因子认证开展攻击。该行动将攻击范围从最初的Roundcube邮件平台扩展至Horde、Zimbra和MDaemon等多个邮件平台，主要目标锁定在与乌克兰战争密切相关的东欧政府部门及国防关联的公司，攻击行动造成的影响也波及到非洲、欧洲和南美洲的部分政府部门。



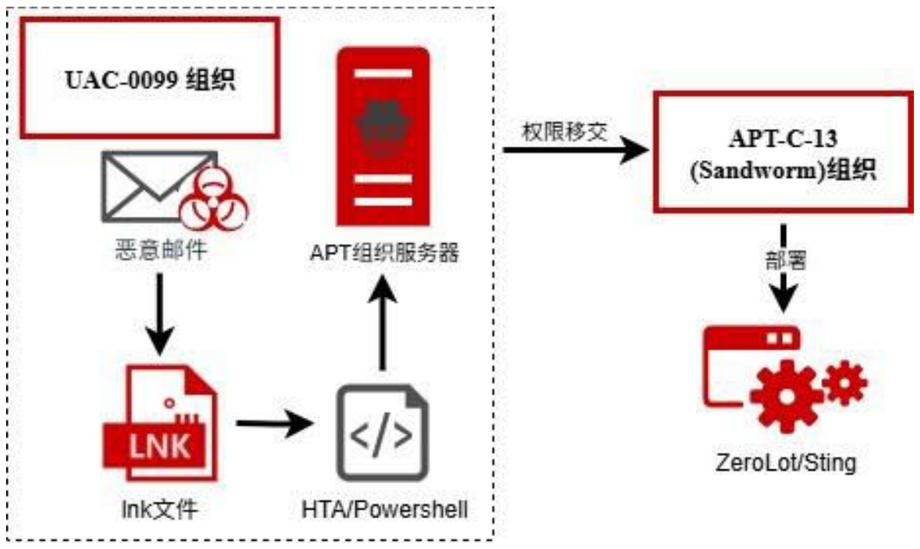
▲图：APT-C-20（APT28）组织攻击流程示意图

6.1、APT-C-13（Sandworm）

2025年，APT-C-13（Sandworm）组织的攻击活动灵活多变，展现出了极高破坏性。他们利用盗版软件和供应链漏洞进行大范围的底层渗透。

APT-C-13（Sandworm）组织针对乌克兰开展的持续性破坏行动还重点攻击了政府、能源、物流等行业。特别是利用新型擦除器对乌克兰的重要的粮食经济产业和教育体系实施精准的毁灭性打击 。这种“广泛撒网控制”与“精准定点爆破”相结合的模式，对乌克兰国家生存能力造成重大威胁。

APT-C-13（Sandworm）组织的部分“精准攻击”是通过与UAC-0099组织合作代理获取了初始访问权限，之后伪装成Windows计划任务方式来部署“ZeroLot”和“Sting”等多种恶意数据擦除软件。这些攻击活动旨在通过破坏文件系统和主引导记录来不可逆地销毁关键数字资产，从而削弱乌克兰的经济来达成其战略目的。

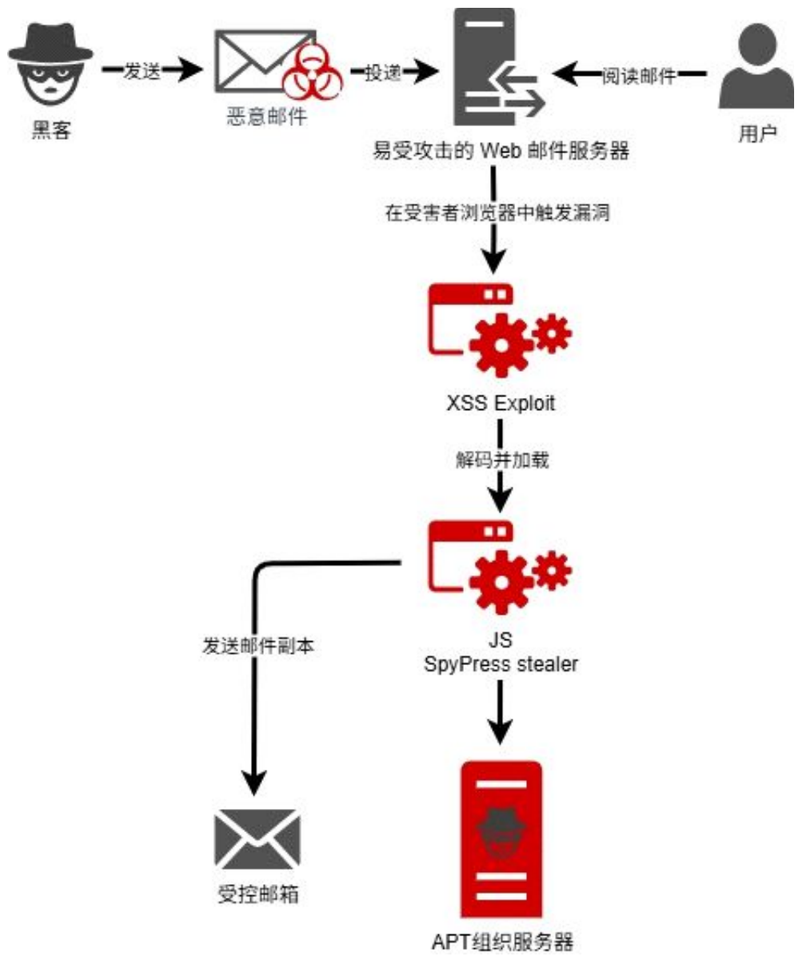


▲图：APT-C-13（Sandworm）组织攻击流程示意图

6.2、APT-C-20（APT28）

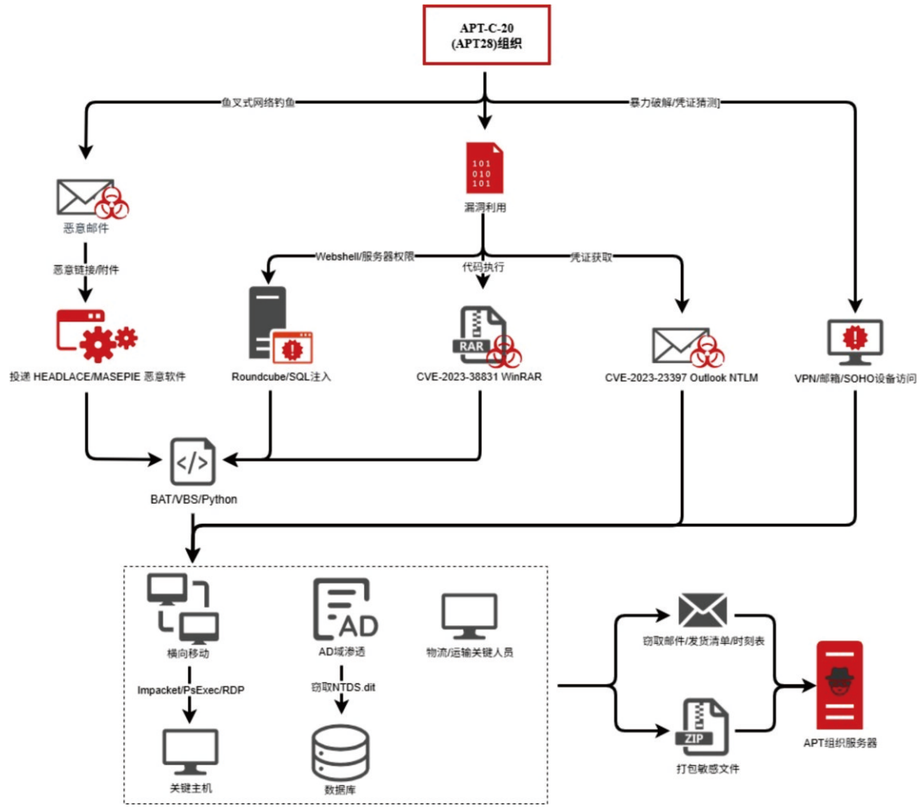
2025年，APT-C-20（APT28）组织在攻击武器库的快速迭代和攻击面的多样化方面动作明显。其核心目标依然是服务于地缘政治利益，通过使用Nday和0day漏洞，对乌克兰及其西方盟友实施深度情报窃取。

在APT-C-20（APT28）组织发起的一场针对高价值Web邮件服务器的持续性网络间谍活动。攻击者通过鱼叉式网络钓鱼利用Web邮件平台中的XSS漏洞，向受害者页面注入定制的“SpyPress”恶意JavaScript代码，从而实现对凭据、联系人列表及邮件内容的窃取。攻击者甚至还利用0day漏洞绕过MDaemon多因子认证开展攻击。该行动将攻击范围从最初的Roundcube邮件平台扩展至Horde、Zimbra和MDaemon等多个邮件平台，主要目标锁定在与乌克兰战争密切相关的东欧政府部门及国防关联的公司，攻击行动造成的影响也波及到非洲、欧洲和南美洲的部分政府部门。



▲图：APT-C-20（APT28）组织攻击流程示意图

APT-C-20（APT28）组织针对援乌后勤供应链及关键基础设施实施长期网络间谍行动。该组织利用Outlook NTLM（CVE-2023-23397）漏洞、Roundcube及WinRAR等已知漏洞，以及凭证撞库、鱼叉式网络钓鱼在内的多种初始访问技术，渗透了北约成员国及乌克兰的物流实体、运输枢纽及IT服务公司；旨在窃取发货清单、运输时刻表等敏感数据，以追踪军事援助物资的流向。除了传统的网络渗透，攻击者还大规模入侵了约10,000个位于乌克兰边境及关键节点的联网摄像头，通过暴力破解RTSP协议获取实时监控画面来追踪物资运输；还进一步渗透欧洲、美国及澳大利亚的多个工业控制系统与企业网络，对关键基础设施构成了潜在的破坏威胁。

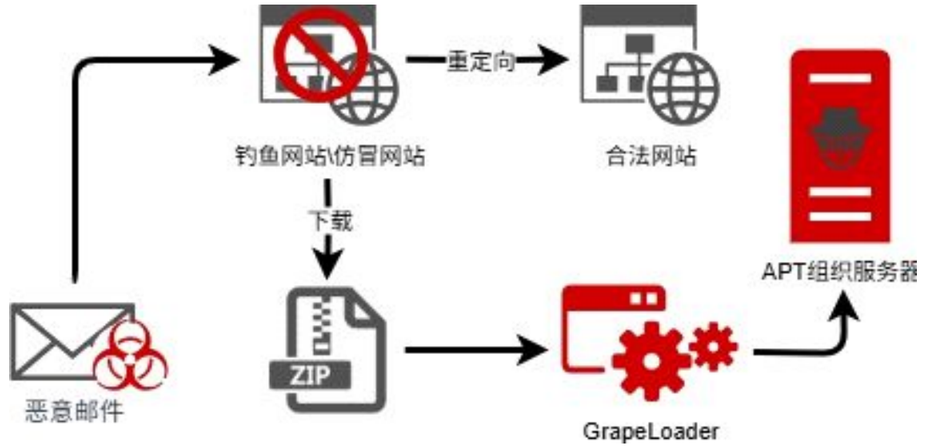


▲图：APT-C-20（APT28）组织攻击流程示意图

6.3、APT-C-25（APT29）

2025年，APT-C-25（APT29）组织展现了极高的战术灵活性和针对性，采取了“传统间谍技术”与“现代云身份攻击”双轨并行的攻击战术。根据目标环境精准切换武器，在需要深潜控制的欧洲外交网络投放新型木马，在防御严密的美国云环境实施无恶意软件的身份接管。其核心目标依然服务于地缘政治利益，聚焦于西方国家的外交、政府及相关供应链体系。

APT-C-25（APT29）组织在攻击活动中冒充某欧洲国家外交机构，向目标人员发送葡萄酒品鉴活动邀请，诱使受害者点击网页链接，从而导致受害者主机被部署名为GRAPELOADER的新后门。此次攻击活动主要针对分布于欧洲地区的外交机构。

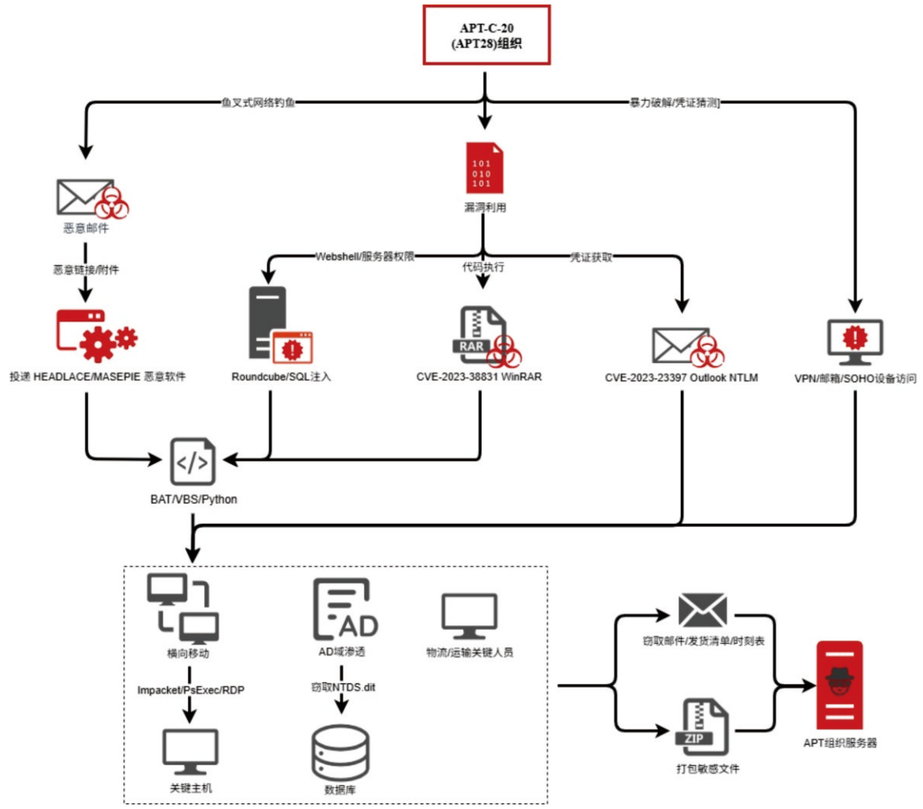


图①

APT-C-25（APT29）组织利用美国移动网络代理IP以及经过深度混淆编码处理的Gmail账户，伪装成美国国务院，发送“关于加入Microsoft 365 Tenant外部用户”或“Measuring Influence Operations Teams群组”的虚假邀请函。一旦受害者中招，攻击者即可在无需窃取密码的情况下获得账户的OAuth授权访问权限。

▲图：APT-C-25（APT29）组织攻击流程示意图

APT-C-20（APT28）组织针对援乌后勤供应链及关键基础设施实施长期网络间谍行动。该组织利用Outlook NTLM（CVE-2023-23397）漏洞、Roundcube及WinRAR等已知漏洞，以及凭证撞库、鱼叉式网络钓鱼在内的多种初始访问技术，渗透了北约成员国及乌克兰的物流实体、运输枢纽及IT服务公司；旨在窃取发货清单、运输时刻表等敏感数据，以追踪军事援助物资的流向。除了传统的网络渗透，攻击者还大规模入侵了约10,000个位于乌克兰边境及关键节点的联网摄像头，通过暴力破解RTSP协议获取实时监控画面来追踪物资运输；还进一步渗透欧洲、美国及澳大利亚的多个工业控制系统与企业网络，对关键基础设施构成了潜在的破坏威胁。

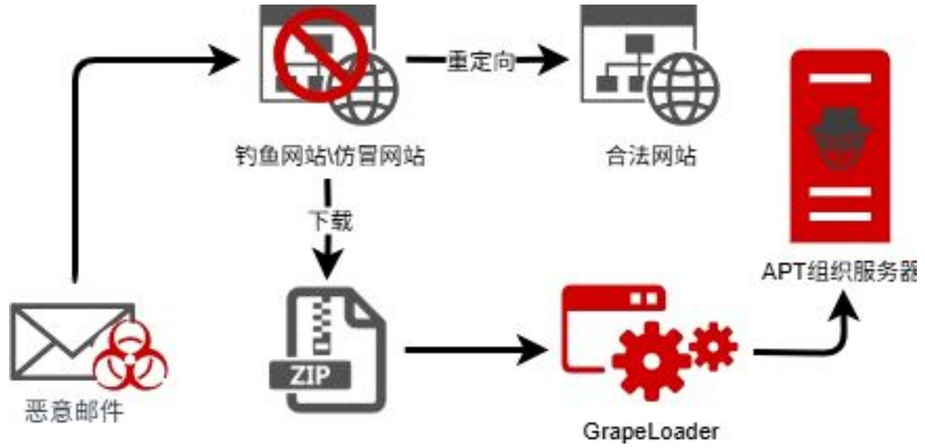


▲图：APT-C-20（APT28）组织攻击流程示意图

6.3、APT-C-25（APT29）

2025年，APT-C-25（APT29）组织展现了极高的战术灵活性和针对性，采取了“传统间谍技术”与“现代云身份攻击”双轨并行的攻击战术。根据目标环境精准切换武器，在需要深潜控制的欧洲外交网络投放新型木马，在防御严密的美国云环境实施无恶意软件的身份接管。其核心目标依然服务于地缘政治利益，聚焦于西方国家的外交、政府及相关供应链体系。

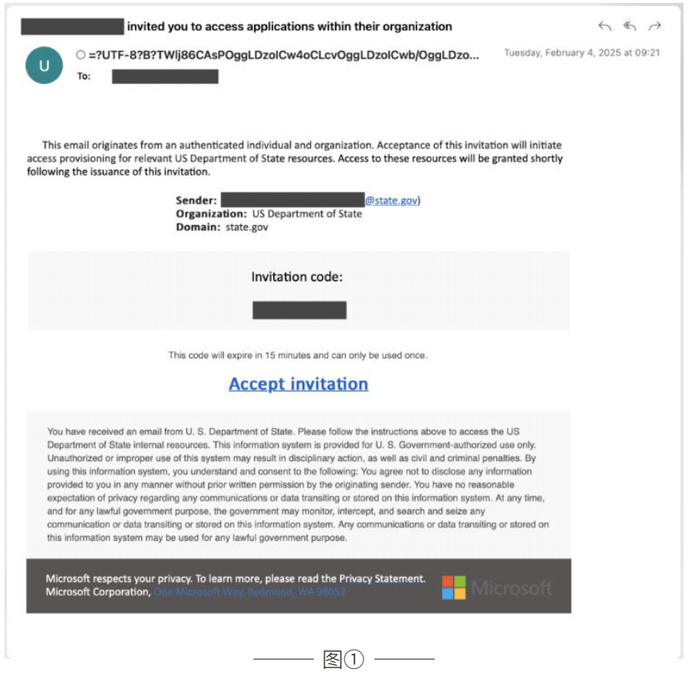
APT-C-25（APT29）组织在攻击活动中冒充某欧洲国家外交机构，向目标人员发送葡萄酒品鉴活动邀请，诱使受害者点击网页链接，从而导致受害者主机被部署名为GRAPELOADER的新后门。此次攻击活动主要针对分布于欧洲地区的外交机构。



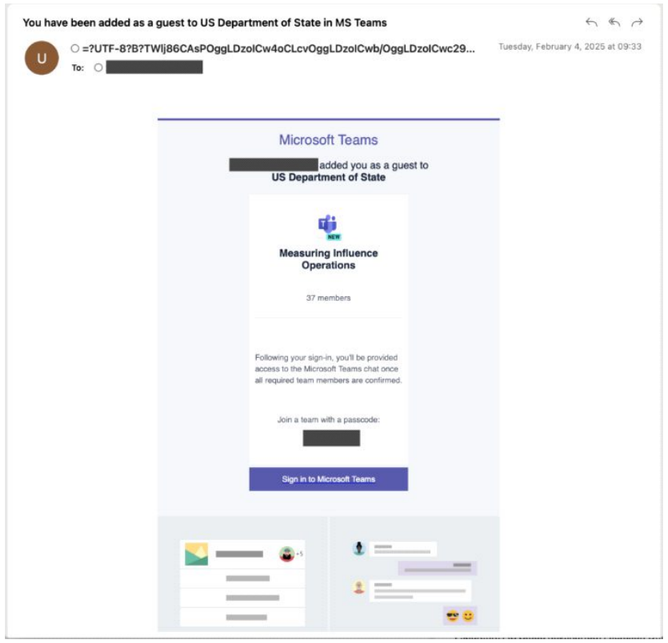
图①

APT-C-25（APT29）组织利用美国移动网络代理IP以及经过深度混淆编码处理的Gmail账户，伪装成美国国务院，发送“关于加入Microsoft 365 Tenant外部用户”或“Measuring Influence Operations Teams群组”的虚假邀请函。一旦受害者中招，攻击者即可在无需窃取密码的情况下获得账户的OAuth授权访问权限。

▲图：APT-C-25（APT29）组织攻击流程示意图



图①

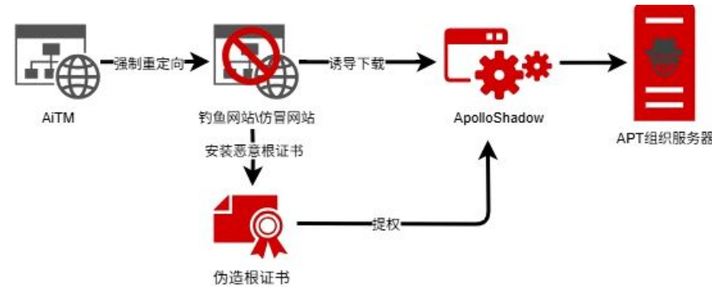


图②

▲ 图①：加入Microsoft365 Tenant的外部用户虚假邀请　图②：Microsoft Teams虚假聊天邀请

6.4、APT-C-29（Turla）

2025年，APT-C-29（Turla）组织通过中间人（AiTM）攻击，对驻莫斯科的外国大使馆进行网络间谍活动。在此攻击活动中，攻击者利用合法拦截手段安装伪装成Kaspersky反病毒软件的根证书，之后使用TLS/SSL剥离技术解密目标流量窃取凭证和令牌，进而部署“ApolloShadow”恶意软件实现持久化控制。此类远程控制窃取情报的攻击手段延续了该组织此前对东欧外交部开展的伪造的Flash安装程序木马的中间人攻击战术。



图①

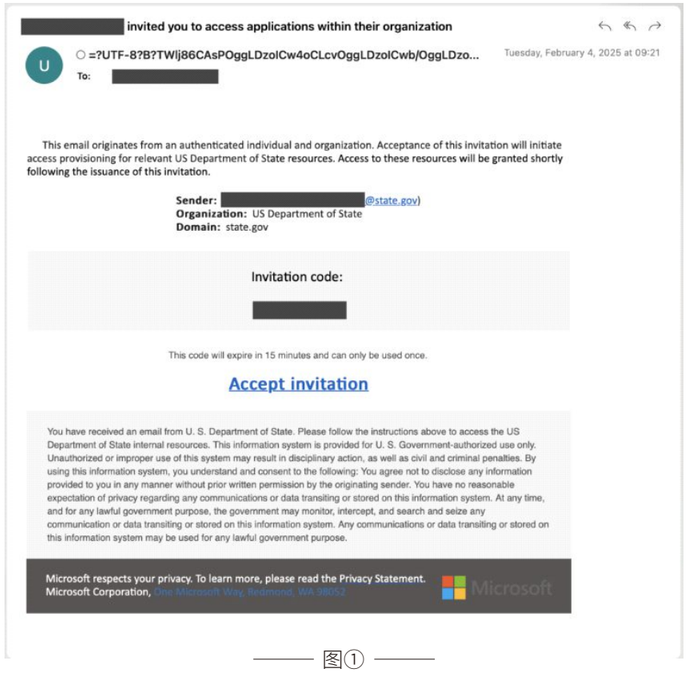
6.5、APT-C-53（Gamaredon）

2025年，APT-C-53（Gamaredon）组织依旧以乌克兰的政府部门、军事等重要机构为主要目标，涉及政府部门、军事部门、民生部门、警务部门。该组织采用多种复杂的技术和策略，使用恶意LNK文件、HTA文件以开展复杂的网络钓鱼。

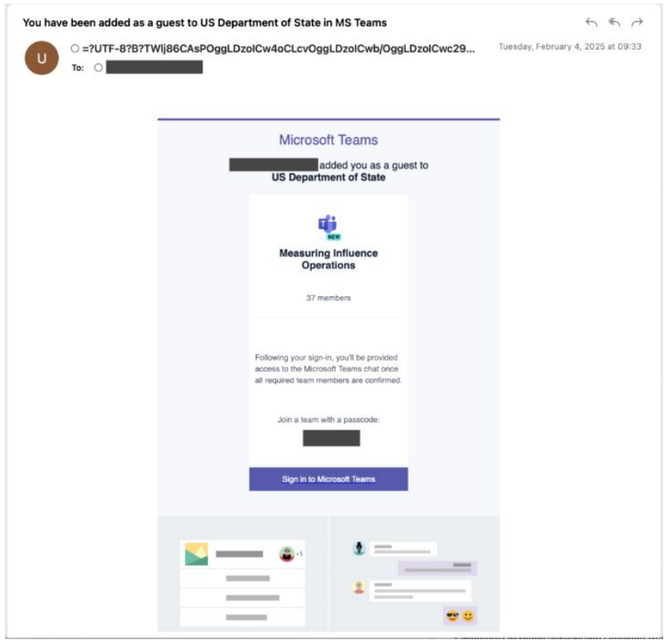
在APT-C-53（Gamaredon）组织利用WinRAR漏洞（CVE-2025-8088）发起的鱼叉式网络钓鱼活动中，攻击者通过投递含有恶意数据流的特制RAR压缩包，在受害者解压诱饵文件时触发目录遍历漏洞，将恶意HTA下载器静默写入Windows启动目录以实现初始持久化；系统重启后将触发该HTA文件，之后使用mshta.exe从C2服务器拉取伪装成PDF文档的多层混淆的VBScript核心载荷，该载荷进一步创建伪装的计划任务以巩固持久化状态，并建立稳定的命令控制通道。APT-C-53（Gamaredon）组织在此次攻击活动中将新漏洞利用与其成熟的VBScript攻击框架相结合。

图②

▲ 图①：APT-C-29（Turla）组织攻击流程示意图　图②：APT-C-53（Gamaredon）组织攻击流程示意图



图①

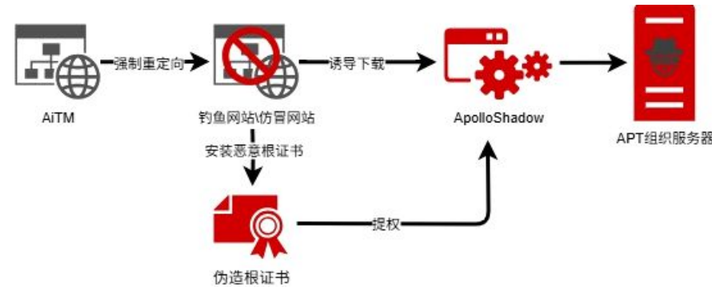


图②

▲ 图①：加入Microsoft365 Tenant的外部用户虚假邀请　图②：Microsoft Teams虚假聊天邀请

6.4、APT-C-29（Turla）

2025年，APT-C-29（Turla）组织通过中间人（AiTM）攻击，对驻莫斯科的外国大使馆进行网络间谍活动。在此攻击活动中，攻击者利用合法拦截手段安装伪装成Kaspersky反病毒软件的根证书，之后使用TLS/SSL剥离技术解密目标流量窃取凭证和令牌，进而部署“ApolloShadow”恶意软件实现持久化控制。此类远程控制窃取情报的攻击手段延续了该组织此前对东欧外交部开展的伪造的Flash安装程序木马的中间人攻击战术。



图①

6.5、APT-C-53（Gamaredon）

2025年，APT-C-53（Gamaredon）组织依旧以乌克兰的政府部门、军事等重要机构为主要目标，涉及政府部门、军事部门、民生部门、警务部门。该组织采用多种复杂的技术和策略，使用恶意LNK文件、HTA文件以开展复杂的网络钓鱼。

在APT-C-53（Gamaredon）组织利用WinRAR漏洞（CVE-2025-8088）发起的鱼叉式网络钓鱼活动中，攻击者通过投递含有恶意数据流的特制RAR压缩包，在受害者解压诱饵文件时触发目录遍历漏洞，将恶意HTA下载器静默写入Windows启动目录以实现初始持久化；系统重启后将触发该HTA文件，之后使用mshta.exe从C2服务器拉取伪装成PDF文档的多层混淆的VBScript核心载荷，该载荷进一步创建伪装的计划任务以巩固持久化状态，并建立稳定的命令控制通道。APT-C-53（Gamaredon）组织在此次攻击活动中将新漏洞利用与其成熟的VBScript攻击框架相结合。

图②

▲ 图①：APT-C-29（Turla）组织攻击流程示意图　图②：APT-C-53（Gamaredon）组织攻击流程示意图

7、中东

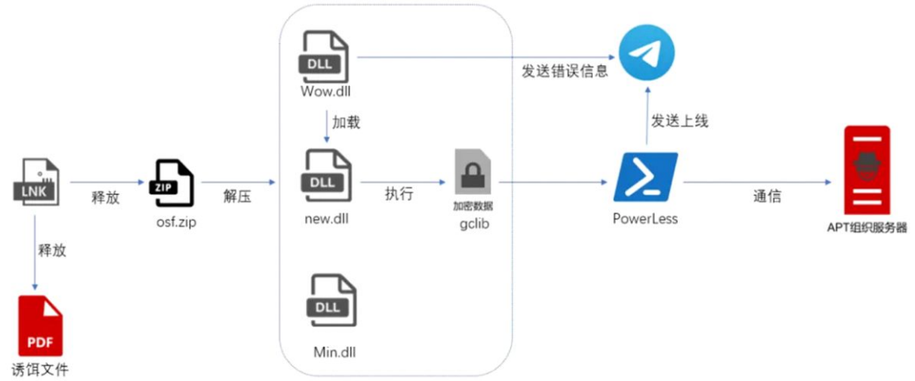
2025年，中东地区秩序重塑加速，该地区网络空间成为地区政治势力间博弈与代理人冲突前沿。针对能源、通信、金融、港口和军事指挥系统的网络攻击活动，多以情报搜集、基础设施破坏和心理震慑为目的。

3月，伊朗两大航运公司116艘油轮遭网络攻击，黑客通过VSAT终端弱密码入侵，切断船岸通信并删除导航配置；6月，伊朗加密货币交易所Nobitex被入侵，超过9000万美元从Nobitex钱包转入黑客地址；12月，伊朗核心通信服务商遭12万个攻击源DDoS攻击，防御及时未致大面积瘫痪。

7.1、APT-C-51（APT35）

APT-C-51（APT35）组织近期攻击方式主要使用鱼叉式钓鱼邮件攻击以及水坑攻击。

2025年6月，APT-C-51（APT35）组织被曝冒充技术高管或研究人员以电子邮件或WhatsApp消息针对以色列记者、安全专家以及大学教授发起鱼叉钓鱼攻击，被窃取的用户凭证和数据信息，在其他关联的攻击活动中为攻击者使用。此外，我们还捕获到了该组织针对中东的攻击行动，攻击组织通过恶意LNK下发后续恶意组件，然后层层加载最终实现PowerLess木马的部署，从而完成窃密活动。



▲图：APT-C-51（APT35）组织攻击流程图

7.2、APT-C-49（OilRig）

APT-C-49（OilRig）组织主要针对中东地区政府、能源、化工等行业展开网络间谍行动，大多以网络侦察和窃密为目的。

2025年，APT-C-49（OilRig）组织在攻击活动中使用了新的后门程序：Whisper和PrimeCache。

Whisper后门程序通过登录已失陷的Microsoft Exchange邮件账户，使用邮件附件与攻击者建立交互，Whisper会定期向攻击者发送窃密数据。PrimeCache是作用于IIS服务器的后门程序，通过解析传入的HTTP请求进行文件执行、文件创建、文件删除、命令执行等恶意操作。

7、中东

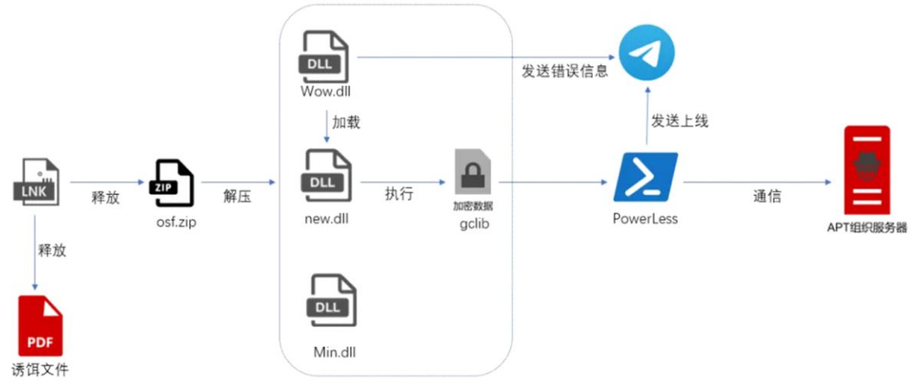
2025年，中东地区秩序重塑加速，该地区网络空间成为地区政治势力间博弈与代理人冲突前沿。针对能源、通信、金融、港口和军事指挥系统的网络攻击活动，多以情报搜集、基础设施破坏和心理震慑为目的。

3月，伊朗两大航运公司116艘油轮遭网络攻击，黑客通过VSAT终端弱密码入侵，切断船岸通信并删除导航配置；6月，伊朗加密货币交易所Nobitex被入侵，超过9000万美元从Nobitex钱包转入黑客地址；12月，伊朗核心通信服务商遭12万个攻击源DDoS攻击，防御及时未致大面积瘫痪。

7.1、APT-C-51（APT35）

APT-C-51（APT35）组织近期攻击方式主要使用鱼叉式钓鱼邮件攻击以及水坑攻击。

2025年6月，APT-C-51（APT35）组织被曝冒充技术高管或研究人员以电子邮件或WhatsApp消息针对以色列记者、安全专家以及大学教授发起鱼叉钓鱼攻击，被窃取的用户凭证和数据信息，在其他关联的攻击活动中为攻击者使用。此外，我们还捕获到了该组织针对中东的攻击行动，攻击组织通过恶意LNK下发后续恶意组件，然后层层加载最终实现PowerLess木马的部署，从而完成窃密活动。



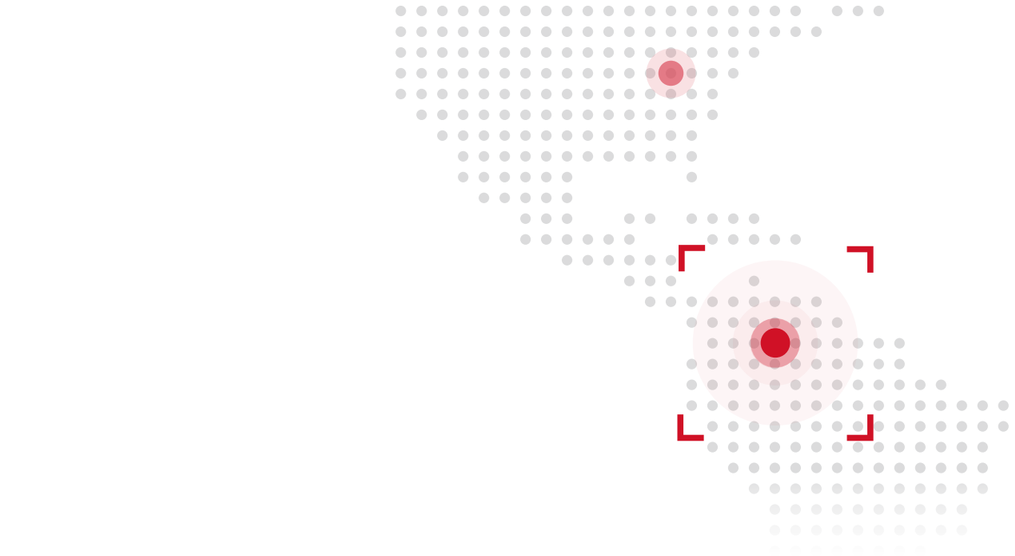
▲图：APT-C-51（APT35）组织攻击流程图

7.2、APT-C-49（OilRig）

APT-C-49（OilRig）组织主要针对中东地区政府、能源、化工等行业展开网络间谍行动，大多以网络侦察和窃密为目的。

2025年，APT-C-49（OilRig）组织在攻击活动中使用了新的后门程序：Whisper和PrimeCache。

Whisper后门程序通过登录已失陷的Microsoft Exchange邮件账户，使用邮件附件与攻击者建立交互，Whisper会定期向攻击者发送窃密数据。PrimeCache是作用于IIS服务器的后门程序，通过解析传入的HTTP请求进行文件执行、文件创建、文件删除、命令执行等恶意操作。



8、南美

2025年，受地缘政治摩擦影响，南美地区逐渐成为网络攻击活动的热点区域。从巴拉圭全国公民个人数据被勒索，到巴西、秘鲁、哥伦比亚等国金融系统遭遇网络攻击，再到委内瑞拉的系统性数据泄露与能源基础设施被攻击，该地区网络攻击活动规模和破坏性显著增加。

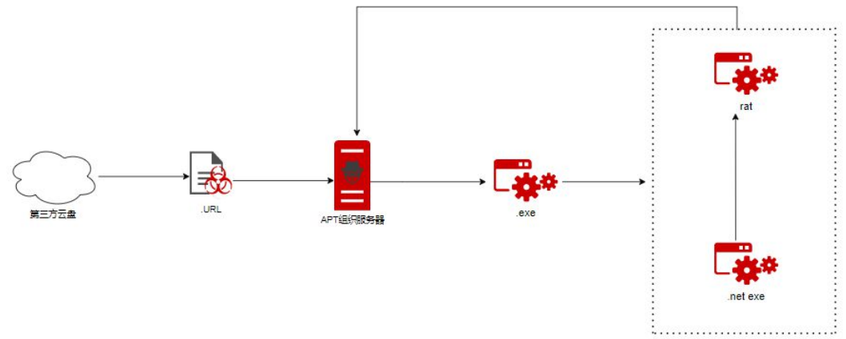
南美地区最活跃的APT-C-36（盲眼鹰）组织在攻击活动中组合使用2024年11月披露的Windows系统漏洞和第三方云平台服务，大大提升了攻击效率。同时我们发现该组织在最新的攻击活动中引入了成熟的加载器程序以丰富其攻击手段。

8.1、APT-C-36（盲眼鹰）

APT-C-36（盲眼鹰）组织近期攻击活动主要针对哥伦比亚、委内瑞拉、厄瓜多尔、巴拿马和阿根廷等南美地区国家。

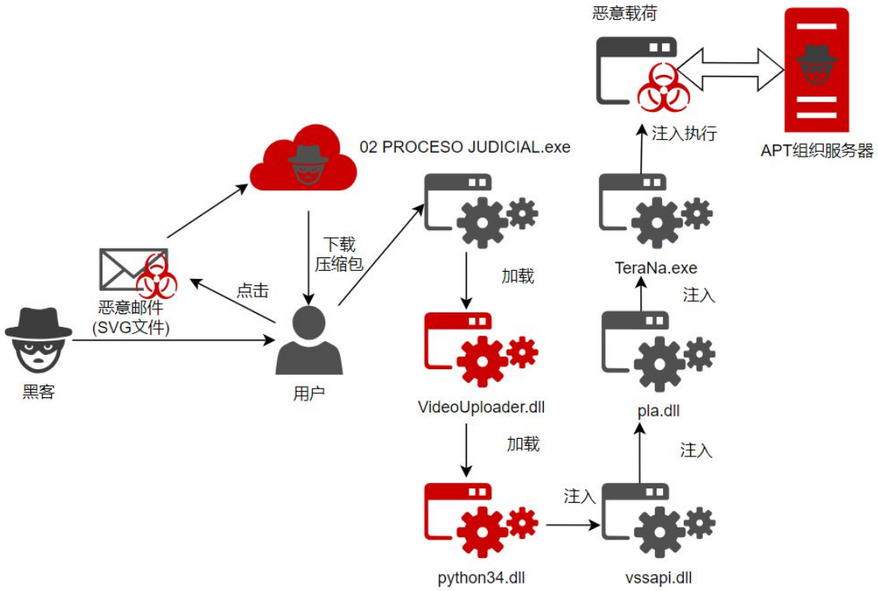
2024年11月12日，微软披露了Windows系统漏洞CVE-2024-43451，该漏洞载荷文件被触发后，会下载并执行恶意文件。APT-C-36（盲眼鹰）组织在随后的攻击活动中对未修复该漏洞的终端进行攻击。

攻击者使用钓鱼邮件向哥伦比亚政府以及司法系统人员投递钓鱼邮件，诱使用户从Google Drive和Dropbox第三方云平台下载恶意.url文件并执行Remcos RAT木马。



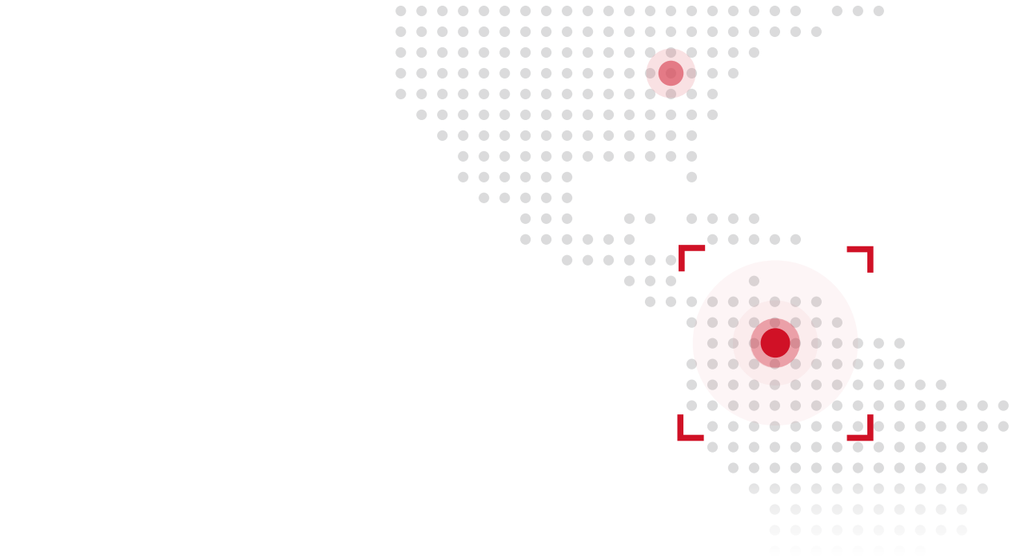
图①

APT-C-36（盲眼鹰）组织在2025年10月份实施了新一轮攻击活动。攻击者使用Hijackloader加载器加载恶意载荷。该加载器使用各类注入手段，多阶段、反复进行shellcode注入，最终加载Pure远程控制木马，实现对受害者计算机的控制。



图②

▲图①：APT-C-36（盲眼鹰）组织攻击流程示意图　图②：APT-C-36（盲眼鹰）组织攻击流程示意图



8、南美

2025年，受地缘政治摩擦影响，南美地区逐渐成为网络攻击活动的热点区域。从巴拉圭全国公民个人数据被勒索，到巴西、秘鲁、哥伦比亚等国金融系统遭遇网络攻击，再到委内瑞拉的系统性数据泄露与能源基础设施被攻击，该地区网络攻击活动规模和破坏性显著增加。

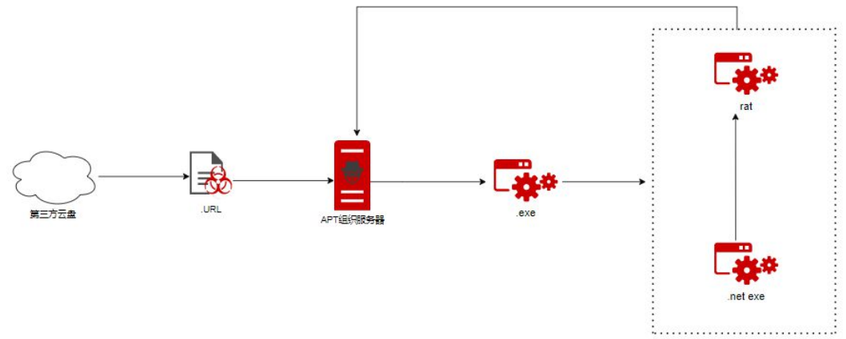
南美地区最活跃的APT-C-36（盲眼鹰）组织在攻击活动中组合使用2024年11月披露的Windows系统漏洞和第三方云平台服务，大大提升了攻击效率。同时我们发现该组织在最新的攻击活动中引入了成熟的加载器程序以丰富其攻击手段。

8.1、APT-C-36（盲眼鹰）

APT-C-36（盲眼鹰）组织近期攻击活动主要针对哥伦比亚、委内瑞拉、厄瓜多尔、巴拿马和阿根廷等南美地区国家。

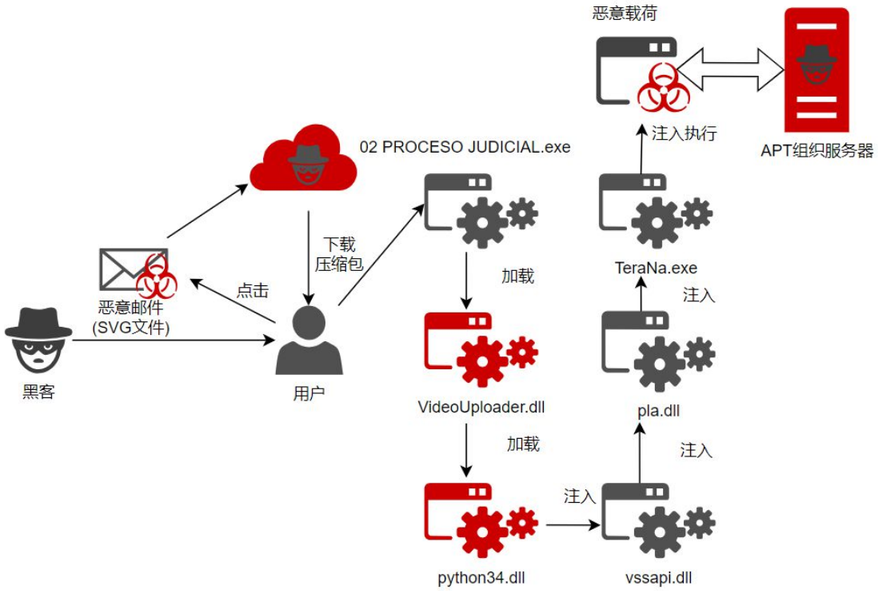
2024年11月12日，微软披露了Windows系统漏洞CVE-2024-43451，该漏洞载荷文件被触发后，会下载并执行恶意文件。APT-C-36（盲眼鹰）组织在随后的攻击活动中对未修复该漏洞的终端进行攻击。

攻击者使用钓鱼邮件向哥伦比亚政府以及司法系统人员投递钓鱼邮件，诱使用户从Google Drive和Dropbox第三方云平台下载恶意.url文件并执行Remcos RAT木马。



图①

APT-C-36（盲眼鹰）组织在2025年10月份实施了新一轮攻击活动。攻击者使用Hijackloader加载器加载恶意载荷。该加载器使用各类注入手段，多阶段、反复进行shellcode注入，最终加载Pure远程控制木马，实现对受害者计算机的控制。



图②

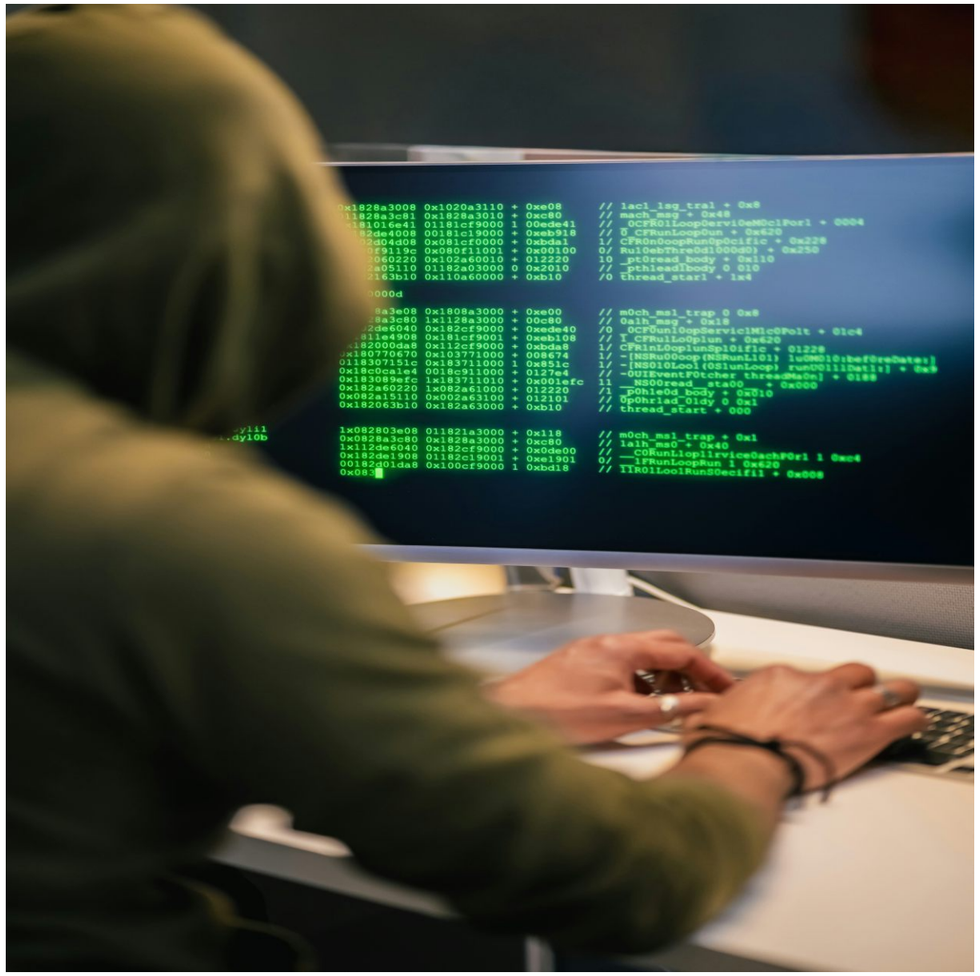
▲图①：APT-C-36（盲眼鹰）组织攻击流程示意图　图②：APT-C-36（盲眼鹰）组织攻击流程示意图

PART 3

2025年 APT攻击发展趋势分析

1、攻击活动使用的ATT&CK技战术 TOP20

360高级威胁研究院综合分析了2025年全球安全机构和厂商公开披露的APT攻击技术报告，对其中符合ATT&CK知识标准的攻击活动和技战术使用情况进行统计，给出了APT组织在2025年攻击活动过程中使用最多的TOP20 ATT&CK技战术。

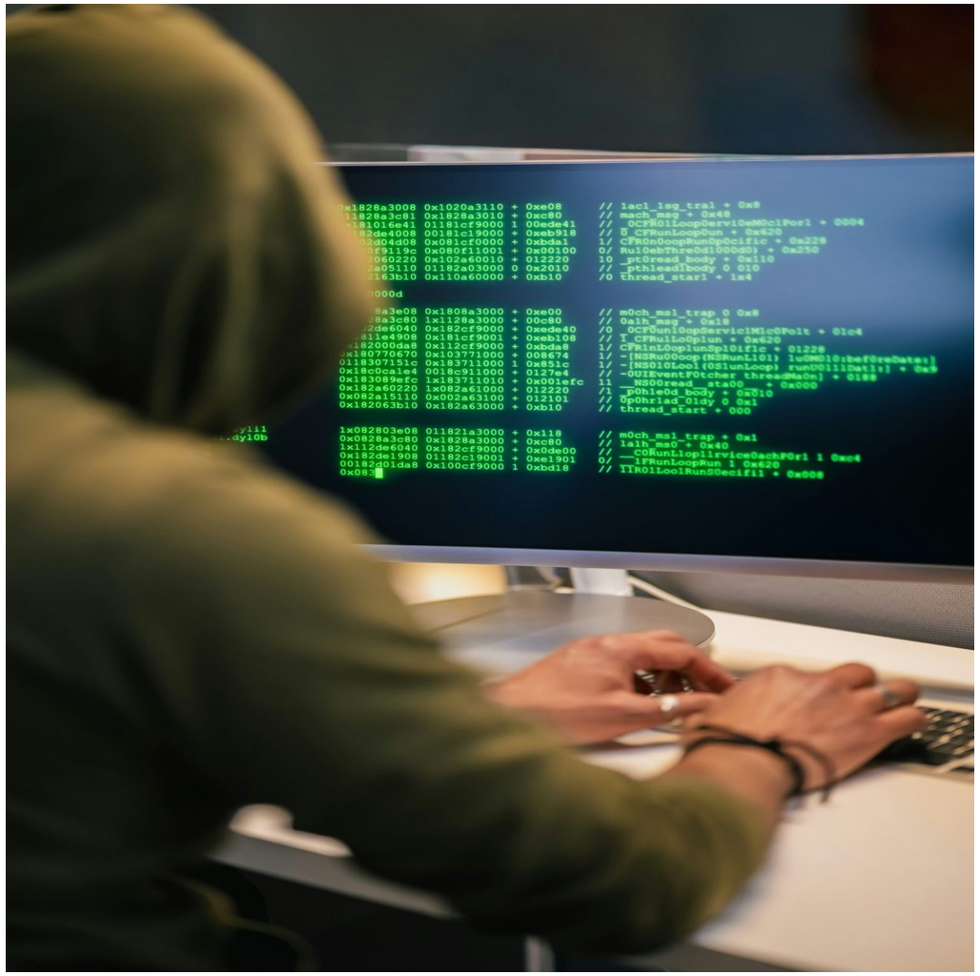


PART 3

2025年 APT攻击发展趋势分析

1、攻击活动使用的ATT&CK技战术 TOP20

360高级威胁研究院综合分析了2025年全球安全机构和厂商公开披露的APT攻击技术报告，对其中符合ATT&CK知识标准的攻击活动和技战术使用情况进行统计，给出了APT组织在2025年攻击活动过程中使用最多的TOP20 ATT&CK技战术。



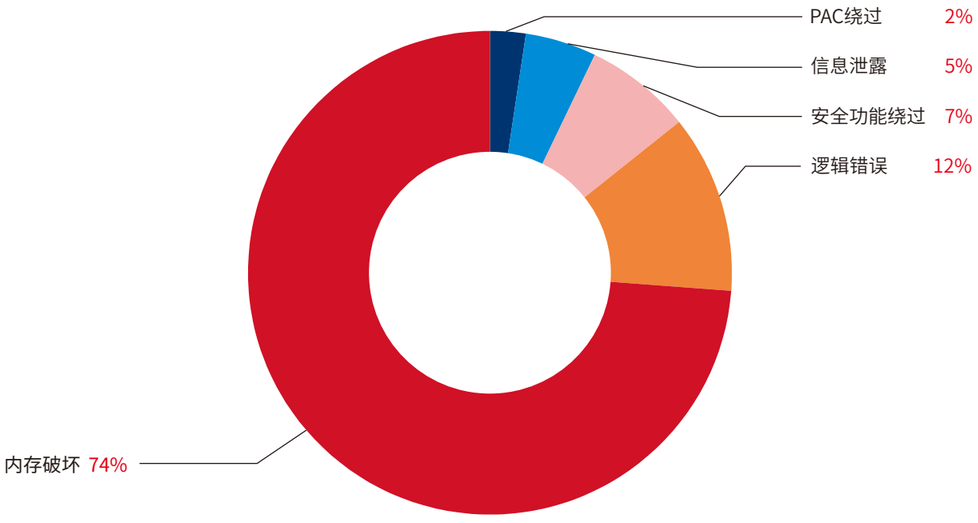
技术ID	技战术名称(英文)	技战术名称(中文)	热度变化
T1566	Phishing	网络钓鱼	-
T1027	Obfuscated Files or Information	混淆文件或信息	↑1
T1105	Ingress Tool Transfer	从外部系统转移文件	↑1
T1059	Command and Scripting Interpreter	滥用命令和脚本解释器	↓2
T1071	Application Layer Protocol	应用层协议	-
T1204	User Execution	诱导用户执行	-
T1082	System Information Discovery	检测操作系统和硬件的信息	↑1
T1070	Indicator Removal	删除痕迹	↑4
T1573	Encrypted Channel	信道使用加密算法	↑10
T1036	Masquerading	伪装	↓1
T1053	Scheduled Task/Job	计划任务	↓4
T1547	Boot or Logon Autostart Execution	启动或登录时自动执行	↓2
T1041	Exfiltration Over C2 Channel	通过C2通道渗透	↓2
T1055	Process Injection	进程注入	-
T1574	Hijack Execution Flow	劫持执行流程	↓2
T1140	Deobfuscate/Decode Files or Information	解码加密/混淆的文件信息	↓1
T1083	File and Directory Discovery	收集文件和目录信息	↑1
T1056	Input Capture	捕获用户输入	↓1
T1132	Data Encoding	数据编码	↑7
T1190	Exploit Public-Facing Application	利用面向公网服务的漏洞	↓4

通过与2024年TOP20 ATT&CK技战术相比，T1573（信道使用加密算法）和T1132（数据编码）热度上升明显，这一定程度反映出2025年APT组织在技战术变化趋势，说明攻击者会更多地用到对抗IDS检测的手段，信道加密的远控方式与加密载荷投递已经是APT组织攻击链条中的基准攻击技术。

2、APT攻击活动0day漏洞统计

2025年APT组织在攻击活动利用的0day漏洞数量，较2024年全年有所增加。其中，针对我国境内网络设施的0day攻击同样上升明显，仅通用型漏洞就涉及到压缩工具、邮件软件、多个邮件平台、网络安全终端防护工具、办公软件系统等多种类别应用软件。

根据统计2025年，全球APT组织在攻击活动利用的影响较大的0day漏洞共计42个，涉及IOS、Windows、Android、Chrome以及VMware等多个平台。



在这些漏洞当中，针对iOS系统的PAC绕过漏洞影响面较大。在过去PAC绕过漏洞主要是“越狱”社区关注的核心攻击手段，而在2025年披露的CVE-2025-31201（PAC绕过漏洞）已被用于针对特定iOS用户发起攻击。其与CVE-2025-31200组合形成“用户态RCE→内核权限提升→持久化”的零交互攻击链，无需用户点击，仅需接收iMessage即可触发，隐蔽性极强。

▲图：APT攻击活动利用新增0day漏洞分布

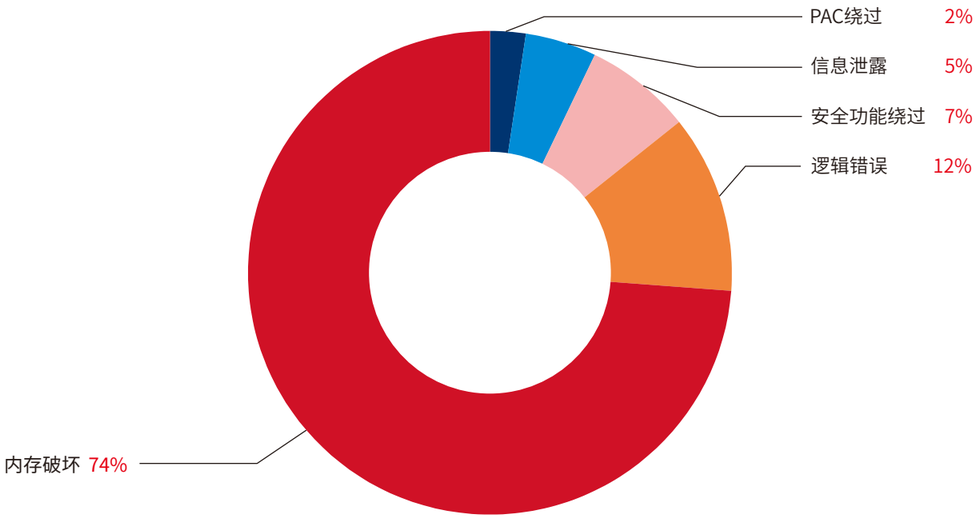
技术ID	技战术名称(英文)	技战术名称(中文)	热度变化
T1566	Phishing	网络钓鱼	-
T1027	Obfuscated Files or Information	混淆文件或信息	↑1
T1105	Ingress Tool Transfer	从外部系统转移文件	↑1
T1059	Command and Scripting Interpreter	滥用命令和脚本解释器	↓2
T1071	Application Layer Protocol	应用层协议	-
T1204	User Execution	诱导用户执行	-
T1082	System Information Discovery	检测操作系统和硬件的信息	↑1
T1070	Indicator Removal	删除痕迹	↑4
T1573	Encrypted Channel	信道使用加密算法	↑10
T1036	Masquerading	伪装	↓1
T1053	Scheduled Task/Job	计划任务	↓4
T1547	Boot or Logon Autostart Execution	启动或登录时自动执行	↓2
T1041	Exfiltration Over C2 Channel	通过C2通道渗透	↓2
T1055	Process Injection	进程注入	-
T1574	Hijack Execution Flow	劫持执行流程	↓2
T1140	Deobfuscate/Decode Files or Information	解码加密/混淆的文件信息	↓1
T1083	File and Directory Discovery	收集文件和目录信息	↑1
T1056	Input Capture	捕获用户输入	↓1
T1132	Data Encoding	数据编码	↑7
T1190	Exploit Public-Facing Application	利用面向公网服务的漏洞	↓4

通过与2024年TOP20 ATT&CK技战术相比，T1573（信道使用加密算法）和T1132（数据编码）热度上升明显，这一定程度反映出2025年APT组织在技战术变化趋势，说明攻击者会更多地用到对抗IDS检测的手段，信道加密的远控方式与加密载荷投递已经是APT组织攻击链条中的基准攻击技术。

2、APT攻击活动0day漏洞统计

2025年APT组织在攻击活动利用的0day漏洞数量，较2024年全年有所增加。其中，针对我国境内网络设施的0day攻击同样上升明显，仅通用型漏洞就涉及到压缩工具、邮件软件、多个邮件平台、网络安全终端防护工具、办公软件系统等多种类别应用软件。

根据统计2025年，全球APT组织在攻击活动利用的影响较大的0day漏洞共计42个，涉及IOS、Windows、Android、Chrome以及VMware等多个平台。



在这些漏洞当中，针对iOS系统的PAC绕过漏洞影响面较大。在过去PAC绕过漏洞主要是“越狱”社区关注的核心攻击手段，而在2025年披露的CVE-2025-31201（PAC绕过漏洞）已被用于针对特定iOS用户发起攻击。其与CVE-2025-31200组合形成“用户态RCE→内核权限提升→持久化”的零交互攻击链，无需用户点击，仅需接收iMessage即可触发，隐蔽性极强。

▲图：APT攻击活动利用新增0day漏洞分布

3、利用开源代码仓库方式进行供应链攻击

在2025年，APT-C-00（海莲花）的钓鱼攻击、APT-C-26（Lazarus）的虚假面试行动等多个APT组织的攻击活动中，都发现其利用开源代码仓库作为攻击环节之一。APT组织在代码仓库中精心构建含有后门的恶意软件项目和软件包，诱导开发人员引用这些项目或软件包到开发者的项目中，从而实现供应链投毒。此外，攻击者还通过入侵开发者主机，使用攻击武器自动感染开发者维护的软件包，然后强制发布这些包补丁，使攻击产生级联感染效应，在整个生态系统中造成连锁式入侵。

GitHub和NPM等代码仓库由于开发者用户众多，受影响最大，甚至一些拥有百万下载量的软件包也同样被入侵。代码仓库投毒是开源生态快速发展下的恶性安全威胁，本质是对开发者信任的滥用。

此类攻击伪装性极强，诱导性突出，让开发者难以察觉；攻击链条隐蔽，影响面广，投毒不仅针对终端开发者，还会渗透CI/CD流水线，一旦恶意组件被引入，可能导致从开发环境到生产系统的全链路污染，引发大规模数据泄露或系统失控；危害后果严重，连锁反应明显，轻则造成服务中断、经济损失，重则窃取企业机密、用户凭证甚至影响国家安全。

究其背后的关键诱因，主要是开源生态的信任红利被滥用，开源仓库的开放注册特性降低了攻击门槛；开发效率与安全校验的失衡，开发者为追求迭代速度，缺乏审查、未建立完善的依赖管理流程，给投毒攻击留下可乘之机。

企业应构建全周期安全体系，部署私有镜像仓库隔离公共源风险，集成自动化安全检查，通过SBOM（软件物料清单）跟踪组件来源，使用最小权限构建环境配置。

4、AI技术已被攻击者应用在深度伪造和诱饵制作等场景

AI技术的应用，无疑会提高APT组织在社会工程学调研和攻击的效率，提升攻击者构造跨语言、跨文化、跨行业领域诱饵文档的水平。尤其在大模型技术的深度应用方面，深度伪造已经开始被APT组织在攻击活动中用于快速构建仿冒或伪造的目标服务。

2025年，APT-C-26（Lazarus）组织不仅在攻击活动中投递虚假的项目库、NPM库，伪造虚假的面试邀约，还通过伪造Zoom会议实施深度欺诈。攻击者为了获得远程工作机会，他们创建、租用或获取与目标组织地理位置相匹配的被盗身份，创建电子邮件账户和社交媒体资料，并创建虚假的作品集、GitHub和LinkedIn等开发者平台上的个人资料。同时，使用AI工具增强运营，包括虚假简历制作、图像创建、使用语音转换软件等。在人工智能的帮助下，减少语法错误，使伪造的简历看起来更加真实。

另外从APT-C-47（旺刺）针对知识产权行业进行有计划的攻击渗透，到APT-C-01（毒云藤）组织相关诱饵文档的制作。在大模型技术应用普及之后，这些跨地缘、跨文化背景、针对特定行业的钓鱼攻击明显增多。

攻击者使用AI技术结合钓鱼攻击，已从早期的“广撒网”式诈骗，进化为针对性极强的“精准制导”型攻击，成为个人、企业乃至国家层面网络安全的主要威胁之一。特别是结合AI技术的智能化升级，进一步降低了高级钓鱼攻击的门槛。攻击者可利用大模型快速生成符合目标人群语言风格的钓鱼文案，规避基于关键词的垃圾邮件检测；通过AI图像生成工具制作高度逼真的伪造文件、界面截图，提升内容可信度；甚至利用AI驱动的对话机器人，在即时通讯中模拟真人交互，逐步诱导目标泄露敏感信息，这种“交互式钓鱼”的欺骗性远超传统静态钓鱼内容。应对这一新形势，需要利用AI技术来驱动自动化防御，做到以模型制约模型、以AI对抗AI，提升威胁防御能力。

3、利用开源代码仓库方式进行供应链攻击

在2025年，APT-C-00（海莲花）的钓鱼攻击、APT-C-26（Lazarus）的虚假面试行动等多个APT组织的攻击活动中，都发现其利用开源代码仓库作为攻击环节之一。APT组织在代码仓库中精心构建含有后门的恶意软件项目和软件包，诱导开发人员引用这些项目或软件包到开发者的项目中，从而实现供应链投毒。此外，攻击者还通过入侵开发者主机，使用攻击武器自动感染开发者维护的软件包，然后强制发布这些包补丁，使攻击产生级联感染效应，在整个生态系统中造成连锁式入侵。

GitHub和NPM等代码仓库由于开发者用户众多，受影响最大，甚至一些拥有百万下载量的软件包也同样被入侵。代码仓库投毒是开源生态快速发展下的恶性安全威胁，本质是对开发者信任的滥用。

此类攻击伪装性极强，诱导性突出，让开发者难以察觉；攻击链条隐蔽，影响面广，投毒不仅针对终端开发者，还会渗透CI/CD流水线，一旦恶意组件被引入，可能导致从开发环境到生产系统的全链路污染，引发大规模数据泄露或系统失控；危害后果严重，连锁反应明显，轻则造成服务中断、经济损失，重则窃取企业机密、用户凭证甚至影响国家安全。

究其背后的关键诱因，主要是开源生态的信任红利被滥用，开源仓库的开放注册特性降低了攻击门槛；开发效率与安全校验的失衡，开发者为追求迭代速度，缺乏审查、未建立完善的依赖管理流程，给投毒攻击留下可乘之机。

企业应构建全周期安全体系，部署私有镜像仓库隔离公共源风险，集成自动化安全检查，通过SBOM（软件物料清单）跟踪组件来源，使用最小权限构建环境配置。

4、AI技术已被攻击者应用在深度伪造和诱饵制作等场景

AI技术的应用，无疑会提高APT组织在社会工程学调研和攻击的效率，提升攻击者构造跨语言、跨文化、跨行业领域诱饵文档的水平。尤其在大模型技术的深度应用方面，深度伪造已经开始被APT组织在攻击活动中用于快速构建仿冒或伪造的目标服务。

2025年，APT-C-26（Lazarus）组织不仅在攻击活动中投递虚假的项目库、NPM库，伪造虚假的面试邀约，还通过伪造Zoom会议实施深度欺诈。攻击者为了获得远程工作机会，他们创建、租用或获取与目标组织地理位置相匹配的被盗身份，创建电子邮件账户和社交媒体资料，并创建虚假的作品集、GitHub和LinkedIn等开发者平台上的个人资料。同时，使用AI工具增强运营，包括虚假简历制作、图像创建、使用语音转换软件等。在人工智能的帮助下，减少语法错误，使伪造的简历看起来更加真实。

另外从APT-C-47（旺刺）针对知识产权行业进行有计划的攻击渗透，到APT-C-01（毒云藤）组织相关诱饵文档的制作。在大模型技术应用普及之后，这些跨地缘、跨文化背景、针对特定行业的钓鱼攻击明显增多。

攻击者使用AI技术结合钓鱼攻击，已从早期的“广撒网”式诈骗，进化为针对性极强的“精准制导”型攻击，成为个人、企业乃至国家层面网络安全的主要威胁之一。特别是结合AI技术的智能化升级，进一步降低了高级钓鱼攻击的门槛。攻击者可利用大模型快速生成符合目标人群语言风格的钓鱼文案，规避基于关键词的垃圾邮件检测；通过AI图像生成工具制作高度逼真的伪造文件、界面截图，提升内容可信度；甚至利用AI驱动的对话机器人，在即时通讯中模拟真人交互，逐步诱导目标泄露敏感信息，这种“交互式钓鱼”的欺骗性远超传统静态钓鱼内容。应对这一新形势，需要利用AI技术来驱动自动化防御，做到以模型制约模型、以AI对抗AI，提升威胁防御能力。

5、破坏背后的逻辑，网络攻击成为地缘政治工具

2026年1月3日，美国悍然对委内瑞拉境内目标实施军事打击。在军事行动发生前，美国已在加勒比地区强化军事部署，扣押委方油轮，制造了紧张地缘局势；而在网络空间中，美国政府通也通过网络攻击破坏委内瑞拉石油能源企业的正常运营。

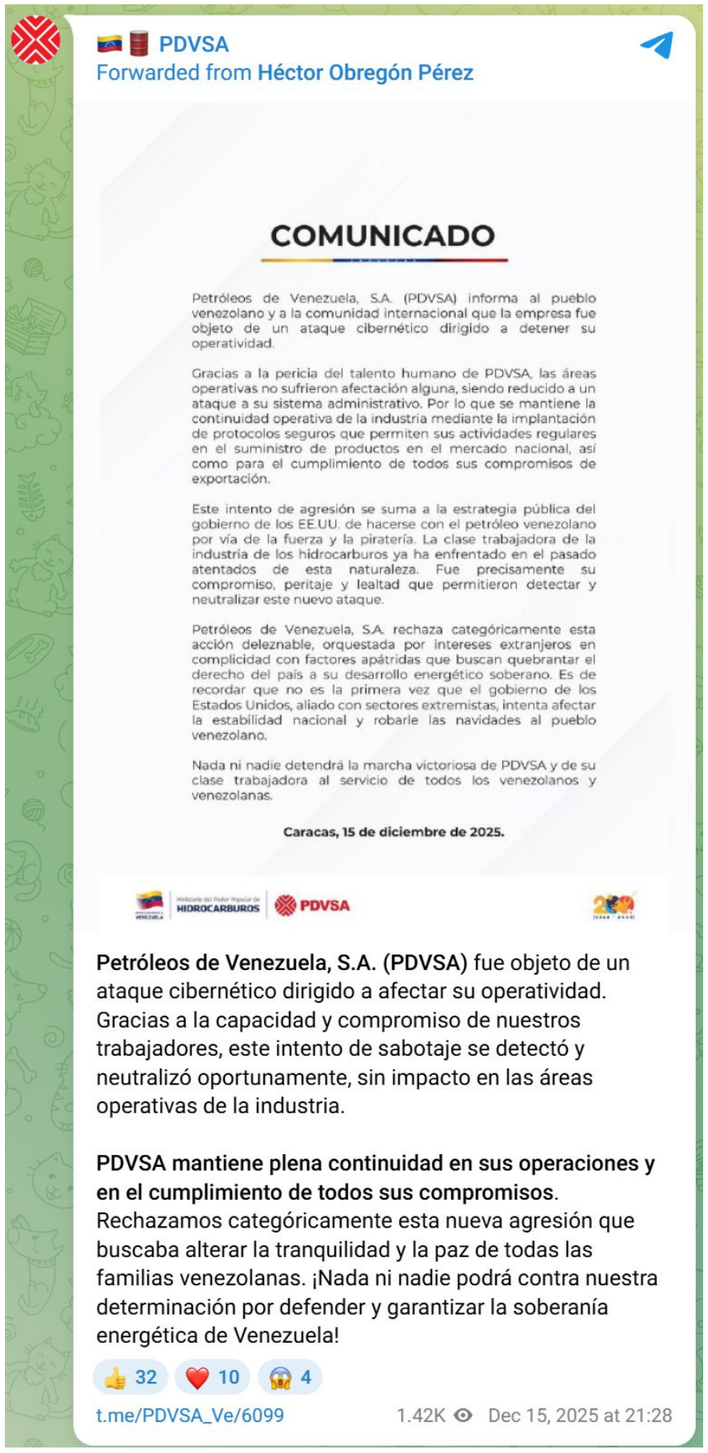
当地时间2025年12月15日，委内瑞拉国家石油公司发布声明，通报该公司遭遇了一起旨在中断其运营的“网络攻击”。声明中指出：2025年12月13日，委内瑞拉国家石油公司（PDVSA）遭遇针对性网络攻击，核心攻击手段为勒索软件侵袭管理系统。PDVSA出口调度等关键业务系统陷入离线状态，导致业务中断。

当前国际格局下，网络攻击已突破网络空间和技术层面，升级为国家战略核心高度，成为地缘政治势力间博弈的重要工具，通过“低成本、高隐蔽、强威慑”的网络行动，服务于国家政治、军事、经济等领域的战略目标。

在俄乌冲突初期，多个东欧背景的APT组织异常活跃，启用的网络资源数量也大幅增加，该地区多个网络组织使用包括擦除器等各种攻击技术手段，持续对东欧地区政府、媒体组织、互联网基础设展开攻击。旨在通过网络攻击，在敌对方制造混乱、阻碍通信、削弱军事反应速度，并借机窃取情报信息。在俄乌冲突相持阶段，东欧地区网络空间对抗成为该地区冲突的重要组成部分，APT-C-13（Sandworm）、APT-C-20（APT28）等APT组织通过网络攻击，在情报窃取、信息传播、舆论引导方面发挥作用，甚至部分组织通过网络攻击针对基础设施进行破坏。

在以色列与伊朗全面对抗中，伊朗高层领导人和核计划专家被执行定点清除，从打击的准度和精度看，攻击者事先早已通过各种技术手段掌握相关专家的身份和实时位置信息。当下地缘政治和军事冲突中，"攻城略地"的传统征服模式已经被取代，而定点打击已经成为一种高效的常态化战术。在万物互联的时代，网络空间对抗与地缘政治冲突的交汇点上，这不仅仅是一次简单的军事打击，它深层次地揭示了网络空间力量在现代冲突中，战略价值从幕后走向前台。这将会引发关于网络战规则、冲突升级阈值以及未来战争形态的深刻争议。

在现代战争中，网络安全的定位已从传统“后勤保障”跃升为“核心作战能力”，直接决定战争主动权归属、攻防成本高低与最终胜负走向。2026年1月4日，美国政府透露，在对委内瑞拉首都加拉加斯发动空袭并成功抓捕委总统尼马杜罗的行动中，美方或动用网络攻击等技术手段切断了当地电力供应。这一事件成为近年来美国对外公开使用网络战力的典型案例。可见，网络空间已成为大国博弈与现代战争的关键战场，网络攻防能力的强弱将持续影响国际格局与战争形态的演变。



▲图：PDVSA关于此次攻击的声明

5、破坏背后的逻辑，网络攻击成为地缘政治工具

2026年1月3日，美国悍然对委内瑞拉境内目标实施军事打击。在军事行动发生前，美国已在加勒比地区强化军事部署，扣押委方油轮，制造了紧张地缘局势；而在网络空间中，美国政府通也通过网络攻击破坏委内瑞拉石油能源企业的正常运营。

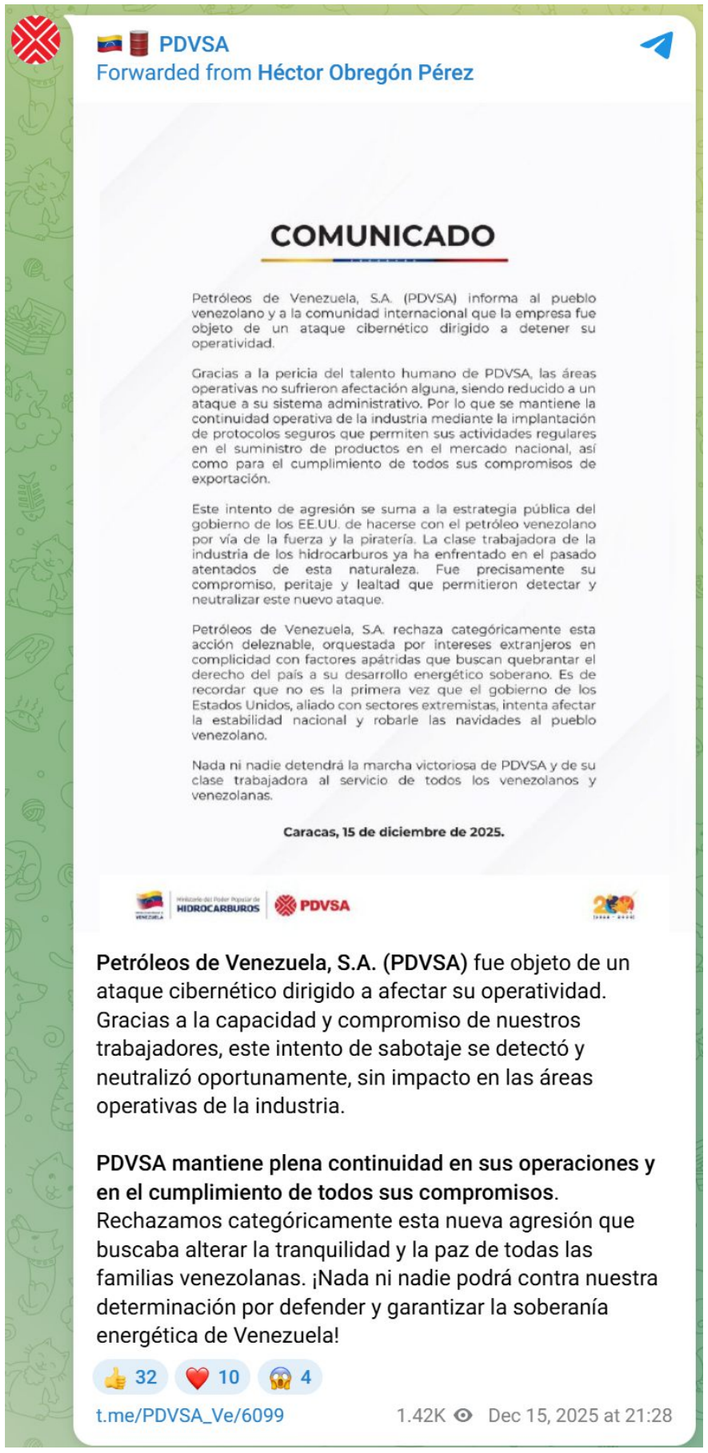
当地时间2025年12月15日，委内瑞拉国家石油公司发布声明，通报该公司遭遇了一起旨在中断其运营的“网络攻击”。声明中指出：2025年12月13日，委内瑞拉国家石油公司（PDVSA）遭遇针对性网络攻击，核心攻击手段为勒索软件侵袭管理系统。PDVSA出口调度等关键业务系统陷入离线状态，导致业务中断。

当前国际格局下，网络攻击已突破网络空间和技术层面，升级为国家战略核心高度，成为地缘政治势力间博弈的重要工具，通过“低成本、高隐蔽、强威慑”的网络行动，服务于国家政治、军事、经济等领域的战略目标。

在俄乌冲突初期，多个东欧背景的APT组织异常活跃，启用的网络资源数量也大幅增加，该地区多个网络组织使用包括擦除器等各种攻击技术手段，持续对东欧地区政府、媒体组织、互联网基础设展开攻击。旨在通过网络攻击，在敌对方制造混乱、阻碍通信、削弱军事反应速度，并借机窃取情报信息。在俄乌冲突相持阶段，东欧地区网络空间对抗成为该地区冲突的重要组成部分，APT-C-13（Sandworm）、APT-C-20（APT28）等APT组织通过网络攻击，在情报窃取、信息传播、舆论引导方面发挥作用，甚至部分组织通过网络攻击针对基础设施进行破坏。

在以色列与伊朗全面对抗中，伊朗高层领导人和核计划专家被执行定点清除，从打击的准度和精度看，攻击者事先早已通过各种技术手段掌握相关专家的身份和实时位置信息。当下地缘政治和军事冲突中，"攻城略地"的传统征服模式已经被取代，而定点打击已经成为一种高效的常态化战术。在万物互联的时代，网络空间对抗与地缘政治冲突的交汇点上，这不仅仅是一次简单的军事打击，它深层次地揭示了网络空间力量在现代冲突中，战略价值从幕后走向前台。这将会引发关于网络战规则、冲突升级阈值以及未来战争形态的深刻争议。

在现代战争中，网络安全的定位已从传统“后勤保障”跃升为“核心作战能力”，直接决定战争主动权归属、攻防成本高低与最终胜负走向。2026年1月4日，美国政府透露，在对委内瑞拉首都加拉加斯发动空袭并成功抓捕委总统尼马杜罗的行动中，美方或动用网络攻击等技术手段切断了当地电力供应。这一事件成为近年来美国对外公开使用网络战力的典型案例。可见，网络空间已成为大国博弈与现代战争的关键战场，网络攻防能力的强弱将持续影响国际格局与战争形态的演变。



▲图：PDVSA关于此次攻击的声明

6、跨平台攻击武器构造复杂攻击链

近些年，越来越多的APT组织开始开发跨平台攻击武器。表面上是攻击资源集约化、攻击覆盖面最大化、防御突破效率化的必然趋势，本质是攻击者针对“多终端协同办公、多系统混合部署”的现代IT架构，实施的精准战术适配。这种趋势不仅大幅提升了攻击的隐蔽性和杀伤力，也对传统“单点防御”体系提出了极大挑战，成为当前网络安全对抗的核心痛点之一。APT-C-28（ScarCruft）组织虚假的Office安装包攻击活动是典型的跨平台攻击行为，使用了多种跨平台脚本开展窃密攻击。

现代攻击武器不再局限于单一操作系统或终端类型，而是实现了对Windows、Linux、macOS、iOS、Android以及物联网（IoT）设备、工业控制系统（ICS）的全覆盖适配。跨平台武器的核心价值不在于“多平台运行”，而在于构建跨终端的协同攻击链条。攻击组织普遍采用“核心载荷 + 跨平台模块”的武器架构：核心恶意逻辑基于HTTP/HTTPS、TCP等通用网络协议实现，而针对不同平台的执行模块则通过调用开源组件（如Python的cross-platform库、Go语言的跨编译工具）快速开发。

这种模块化设计让攻击武器的开发、更新成本大幅降低，只需修改少量适配代码，就能快速支持新的操作系统或终端类型。

7、针对海外机构的APT攻击增多，威胁风险加大

近年来，我国驻外使领馆、经商处、中资企业、文化中心等驻外机构，正成为国家级APT组织的优先攻击目标；攻击威胁在频次、战术复杂度、情报窃取意图上显著升级。这一趋势在2023年至2025年间尤为突出。

在我国参与重大国际会议和重要外事活动期间，南亚、东南亚地区APT组织对我国驻外外交、驻外经贸合作、国际政策研究等相关单位的攻击活动明显活跃。目标直指驻外机构的邮件系统、内部文档与外交决策信息。其中中东、南亚、北美为攻击密度最高区域，与地缘冲突热点高度重合。目标不再局限于传统的使领馆核心网络，甚至延伸至驻外人员个人手机、电脑设备。

这些攻击动机主要瞄准“外交战略、双边谈判底线、军事信息”，“能源合作、基建项目、经贸谈判数据”，以及“制造外交压力、破坏我国国家形象”。其背后主因首先是中美博弈加剧，美国将我国视为“战略竞争对手”，通过APT-C-40（NSA）等组织对我国驻外机构实施常态化网络监控与渗透，试图获取外交、军事、经济情报，掌握博弈主动权；其次，区域冲突外溢，中东、南亚等地区冲突中，我国驻外机构成为各方势力获取情报的“窗口”，网络攻击成为地缘对抗的“低成本武器”；再次，我国在全球治理、“一带一路”倡议等领域的外交活动频繁，驻外机构成为情报收集的重点目标，攻击频次随外交活动密度同步上升。而IT架构复杂，设备与软件国产化不足，存在供应链安全隐患，防护碎片化缺乏统一安全管理平台，这些也使得驻外人员易成为攻击突破口。

我国驻外机构网络攻击威胁的增加，是地缘政治冲突、数字技术发展与防护体系不完善共同作用的结果。攻击的本质是情报窃取与地缘博弈，而非单纯的技术犯罪。

8、国家级APT攻击瞄准国产应用，信创基础设施威胁凸显

当APT组织针对性发起信创平台应用软件的网络攻击，当国产软件漏洞被APT组织利用，一场围绕信创基础设施的网络攻防战已然打响。自主可控软件和信创产业作为国家科技自立自强的核心载体，正成为国家级网络攻击的重点目标。

随着我国“2+8+N”信创体系加速落地，核心软硬件国产化替代进入关键期，在政务、金融、能源等关键领域构建起自主可控的数字基础设施与关键信息基础设施。这种技术突围打破了既有的全球科技格局，使得APT组织将信创体系视为战略竞争的“新战场”，通过国家级网络力量实施精准打击。

从利用国产软件漏洞制作钓鱼诱饵，到美情报机构通过OA系统供应链漏洞窃取密码和研发核心数据，攻击行为呈现出目标明确、手段专业、资源充沛的鲜明特征，本质上是通过破坏信创安全来遏制我国科技自主进程。

当前信创安全面临的挑战具有复杂性和系统性。一方面，部分信创软件产品处于快速迭代期，安全机制成熟度有待提升；另一方面，国产化应用软件迁移过程中存在底层架构重塑，安全策略响应 滞后放大了风险窗口。值得警惕的是，攻击者已形成精准打击能力：专门开发适配国产系统的木马，展现出对信创生态的深度研究。这些攻击手段精准击中了当前信创安全的薄弱环节。

信创产业的安全发展，从来不是单一企业或行业的独角戏，而是关乎国家数字主权的系统工程。面对日趋激烈的网络空间博弈，我们要将安全理念深植产业发展血脉。唯有技术创新与安全防护双轮驱动，才能让信创基础设施真正成为数字中国的“安全底座”，在全球科技竞争中牢牢掌握主动权。

6、跨平台攻击武器构造复杂攻击链

近些年，越来越多的APT组织开始开发跨平台攻击武器。表面上是攻击资源集约化、攻击覆盖面最大化、防御突破效率化的必然趋势，本质是攻击者针对“多终端协同办公、多系统混合部署”的现代IT架构，实施的精准战术适配。这种趋势不仅大幅提升了攻击的隐蔽性和杀伤力，也对传统“单点防御”体系提出了极大挑战，成为当前网络安全对抗的核心痛点之一。APT-C-28（ScarCruft）组织虚假的Office安装包攻击活动是典型的跨平台攻击行为，使用了多种跨平台脚本开展窃密攻击。

现代攻击武器不再局限于单一操作系统或终端类型，而是实现了对Windows、Linux、macOS、iOS、Android以及物联网（IoT）设备、工业控制系统（ICS）的全覆盖适配。跨平台武器的核心价值不在于“多平台运行”，而在于构建跨终端的协同攻击链条。攻击组织普遍采用“核心载荷 + 跨平台模块”的武器架构：核心恶意逻辑基于HTTP/HTTPS、TCP等通用网络协议实现，而针对不同平台的执行模块则通过调用开源组件（如Python的cross-platform库、Go语言的跨编译工具）快速开发。

这种模块化设计让攻击武器的开发、更新成本大幅降低，只需修改少量适配代码，就能快速支持新的操作系统或终端类型。

7、针对海外机构的APT攻击增多，威胁风险加大

近年来，我国驻外使领馆、经商处、中资企业、文化中心等驻外机构，正成为国家级APT组织的优先攻击目标；攻击威胁在频次、战术复杂度、情报窃取意图上显著升级。这一趋势在2023年至2025年间尤为突出。

在我国参与重大国际会议和重要外事活动期间，南亚、东南亚地区APT组织对我国驻外外交、驻外经贸合作、国际政策研究等相关单位的攻击活动明显活跃。目标直指驻外机构的邮件系统、内部文档与外交决策信息。其中中东、南亚、北美为攻击密度最高区域，与地缘冲突热点高度重合。目标不再局限于传统的使领馆核心网络，甚至延伸至驻外人员个人手机、电脑设备。

这些攻击动机主要瞄准“外交战略、双边谈判底线、军事信息”，“能源合作、基建项目、经贸谈判数据”，以及“制造外交压力、破坏我国国家形象”。其背后主因首先是中美博弈加剧，美国将我国视为“战略竞争对手”，通过APT-C-40（NSA）等组织对我国驻外机构实施常态化网络监控与渗透，试图获取外交、军事、经济情报，掌握博弈主动权；其次，区域冲突外溢，中东、南亚等地区冲突中，我国驻外机构成为各方势力获取情报的“窗口”，网络攻击成为地缘对抗的“低成本武器”；再次，我国在全球治理、“一带一路”倡议等领域的外交活动频繁，驻外机构成为情报收集的重点目标，攻击频次随外交活动密度同步上升。而IT架构复杂，设备与软件国产化不足，存在供应链安全隐患，防护碎片化缺乏统一安全管理平台，这些也使得驻外人员易成为攻击突破口。

我国驻外机构网络攻击威胁的增加，是地缘政治冲突、数字技术发展与防护体系不完善共同作用的结果。攻击的本质是情报窃取与地缘博弈，而非单纯的技术犯罪。

8、国家级APT攻击瞄准国产应用，信创基础设施威胁凸显

当APT组织针对性发起信创平台应用软件的网络攻击，当国产软件漏洞被APT组织利用，一场围绕信创基础设施的网络攻防战已然打响。自主可控软件和信创产业作为国家科技自立自强的核心载体，正成为国家级网络攻击的重点目标。

随着我国“2+8+N”信创体系加速落地，核心软硬件国产化替代进入关键期，在政务、金融、能源等关键领域构建起自主可控的数字基础设施与关键信息基础设施。这种技术突围打破了既有的全球科技格局，使得APT组织将信创体系视为战略竞争的“新战场”，通过国家级网络力量实施精准打击。

从利用国产软件漏洞制作钓鱼诱饵，到美情报机构通过OA系统供应链漏洞窃取密码和研发核心数据，攻击行为呈现出目标明确、手段专业、资源充沛的鲜明特征，本质上是通过破坏信创安全来遏制我国科技自主进程。

当前信创安全面临的挑战具有复杂性和系统性。一方面，部分信创软件产品处于快速迭代期，安全机制成熟度有待提升；另一方面，国产化应用软件迁移过程中存在底层架构重塑，安全策略响应 滞后放大了风险窗口。值得警惕的是，攻击者已形成精准打击能力：专门开发适配国产系统的木马，展现出对信创生态的深度研究。这些攻击手段精准击中了当前信创安全的薄弱环节。

信创产业的安全发展，从来不是单一企业或行业的独角戏，而是关乎国家数字主权的系统工程。面对日趋激烈的网络空间博弈，我们要将安全理念深植产业发展血脉。唯有技术创新与安全防护双轮驱动，才能让信创基础设施真正成为数字中国的“安全底座”，在全球科技竞争中牢牢掌握主动权。

PART 4

2026年 APT攻击发展趋势预测

1、AI驱动的攻击全面升级，智能体将大大提升攻击效率

AI技术已经深入IT领域，以AI为驱动的APT攻击会越来越普遍。在2025年，APT-C-26（Lazarus）组织的虚假面试攻击利用了AI的深度伪造技术进行钓鱼攻击。深度伪造诈骗将常态化，利用视频会议诈骗、高管语音/视频指令欺诈成功率将会激增，而AI模仿声音、样貌与神态，邮件仿冒将会升级为“实时交互钓鱼”，钓鱼攻击手段必将“花样百出”。

AI智能体已成为钓鱼攻击主力工具，未来自动化伪造流程使得攻击组织的钓鱼话题紧跟时事。生成式AI批量生产深度伪造钓鱼邮件为不同受害者“量身定制”，攻击周期压缩至分钟级。

在攻击侧，智能体正在颠覆传统的网络攻防格局。过去，高水平的攻击者的成长周期极长，攻击行为高度依赖个人经验和技能。如今，攻击者可以将多年积累的攻击手法、渗透经验、漏洞利用技巧等，全部训练进大模型，打造出“攻击者智能体”，可以自动完成一系列攻击任务。而且攻击者智能体易于批量复制，只要有算力，便可以复制成千上万个。一个人类攻击者可以管理几十个甚至上百个攻击者智能体，成为超级攻击者，将攻击者的攻击频率极大拓宽、攻击效率极大提升，进一步加剧网络攻防的不对称性。

2、云基础设施与供应链攻击更为频繁

在2025年，多个APT组织使用云基础设施提供的服务作为网络攻击节点，通过污染供应链的方式对云上服务展开攻击。

2026年，云基础设施与供应链攻击态势正经历深刻演变。随着企业全面拥抱混合云、多云架构和AI驱动的自动化运维，攻击者也同步升级战术，将目标从单点系统转向整个数字生态链。供应链与云基础设施成APT组织重点攻击目标，通过攻击供应商、合作伙伴、云服务商，实现“迂回包抄”，一旦攻击成功多云环境导致可见性碎片化，未授权访问、注入攻击与配置错误将会使攻击目标快速横向扩散。当攻击者不再攻城略地，而是污染水源，云基础设施与供应链的融合使得单点失守等价于全网崩溃。

PART 4

2026年 APT攻击发展趋势预测

1、AI驱动的攻击全面升级，智能体将大大提升攻击效率

AI技术已经深入IT领域，以AI为驱动的APT攻击会越来越普遍。在2025年，APT-C-26（Lazarus）组织的虚假面试攻击利用了AI的深度伪造技术进行钓鱼攻击。深度伪造诈骗将常态化，利用视频会议诈骗、高管语音/视频指令欺诈成功率将会激增，而AI模仿声音、样貌与神态，邮件仿冒将会升级为“实时交互钓鱼”，钓鱼攻击手段必将“花样百出”。

AI智能体已成为钓鱼攻击主力工具，未来自动化伪造流程使得攻击组织的钓鱼话题紧跟时事。生成式AI批量生产深度伪造钓鱼邮件为不同受害者“量身定制”，攻击周期压缩至分钟级。

在攻击侧，智能体正在颠覆传统的网络攻防格局。过去，高水平的攻击者的成长周期极长，攻击行为高度依赖个人经验和技能。如今，攻击者可以将多年积累的攻击手法、渗透经验、漏洞利用技巧等，全部训练进大模型，打造出“攻击者智能体”，可以自动完成一系列攻击任务。而且攻击者智能体易于批量复制，只要有算力，便可以复制成千上万个。一个人类攻击者可以管理几十个甚至上百个攻击者智能体，成为超级攻击者，将攻击者的攻击频率极大拓宽、攻击效率极大提升，进一步加剧网络攻防的不对称性。

2、云基础设施与供应链攻击更为频繁

在2025年，多个APT组织使用云基础设施提供的服务作为网络攻击节点，通过污染供应链的方式对云上服务展开攻击。

2026年，云基础设施与供应链攻击态势正经历深刻演变。随着企业全面拥抱混合云、多云架构和AI驱动的自动化运维，攻击者也同步升级战术，将目标从单点系统转向整个数字生态链。供应链与云基础设施成APT组织重点攻击目标，通过攻击供应商、合作伙伴、云服务商，实现“迂回包抄”，一旦攻击成功多云环境导致可见性碎片化，未授权访问、注入攻击与配置错误将会使攻击目标快速横向扩散。当攻击者不再攻城略地，而是污染水源，云基础设施与供应链的融合使得单点失守等价于全网崩溃。

3、关键基础设施成为破坏与勒索的首选目标

无论是在在俄乌冲突中、伊以冲突中、印巴对峙中，还是在美国对南美国家的威吓中，情报窃取和系统破坏一直是APT组织的核心战术手段。在涉及到地缘政治冲突时候，国家级APT攻击必将延伸至军事、通信，电力、交通、能源等国计民生核心行业。不管是核心情报泄露，还是物理层面的破坏将会给对手造成严重后果。

“擦除器”这类攻击武器永久破坏目标系统数据，使其丧失可用性。其攻击效果明显，攻击动机简单直接：多为地缘政治威慑、战略破坏或掩盖攻击痕迹；攻击过程体现出“快速、彻底、隐蔽”的特征，致力于快速达成战术目标，防止追踪溯源。

勒索攻击是对基础设施破坏的一个重要手段，不同于“擦除器”这类攻击武器，勒索攻击的核心目标是数据劫持，以获取高额赎金为核心目的。但在APT组织开展的勒索攻击中，往往有更为隐晦的攻击目的。在过去我们捕获的APT勒索事件中，有些攻击的牟利动机不显，攻击者真实意图不明；而在一些窃密攻击活动当中，勒索攻击发生在攻击中段，表现为较强的黑灰产特征，意图掩盖攻击者真实意图，干扰事件归因；此外，还有一些黑灰产攻击者在数据劫持成功之后，将劫持系统售卖给APT组织，随着“窃密+加密”的双重勒索模式越来越多，这种商业转让将会更多发生。勒索攻击使得攻击者的攻击效果可以在“破坏”和“窃密”之间随时切换，更方便攻击者随时适配其攻击动机。

4、量子计算威胁逼近，加密数据泄露不可不查

量子计算通过核心算法，从数学基础上瓦解传统密码体系，引发“现在存储、未来解密”的追溯性威胁，同时催生混合攻击与防御失衡，是对网络安全范式的根本性挑战。

量子计算对网络安全的威胁是“颠覆性”而非“渐进式”，一旦量子计算威胁实现工程化，必将成为APT组织的核心攻击手段。当前，全球范围内已出现大量针对敏感数据的“囤积式攻击”，攻击者通过窃取金融、医疗、政务等领域的加密数据，等待量子计算技术成熟后进行解密。这种攻击模式的隐蔽性极强，一旦量子计算突破，将导致历史数据的批量泄露，造成不可挽回的损失。美国已经相继出台多项法案及标准来应对即将到来的威胁。2026年的核心任务，应尽快识别敏感数据资产，建立量子迁移计划。

5、网络攻击是混合作战的重要组成部分

不管是在俄乌冲突这种大规模兵团作战中，特种部队的小规模斩首行动中，还是印巴战略对峙中，网络攻击已从传统作战的“辅助手段”升级为“核心赋能模块”，其重要性贯穿作战全流程、覆盖战略-战役-战术全层级，是实现“降维打击”和“体系破击”的关键抓手。

混合作战的核心是多域力量的协同联动，而网络空间是串联陆、海、空、天、电等作战域的“无形纽带”。网络攻击的首要价值在于抢占“制网权”，进而夺取制信息权、制空权、制海权等传统制权的前置优势。

未来战争的胜负，很可能在网络空间的无声较量中早已决定。因此，构建强大的网络防御体系、提升网络韧性，并发展网络反击能力，已成为国家综合安全战略的重中之重。

6、攻击技术持续升级、系统化攻击工程是必经之路

在2025年，几乎所有的APT组织都升级了他们的攻击武器、攻击策略。在近些年的APT攻击行动中可以看出，先进的攻击工具能突破更为严密的防守，而复杂的攻击链才能造成更大的影响。

在未来，APT攻击组织的攻击能力将体现在能否将“复杂情报分析、技术的快速变化、战术的迅速调整”整合成统一、连贯的整体，能够自适应场景的变化。网络攻击手段将从零散工具叠加转向全链路协同、模块化组装、AI驱动闭环、产业化分工的系统化形态，攻击链被拆解为可复用组件，从侦察到攻击的全流程实现标准化，攻击工具集成系统化。以北美地区的APT-C-39（CIA）和APT-C-40（NSA）组织为代表，这些APT组织的渗透程度最深、潜伏时间最长。

APT组织的动机往往能体现出国家政治利益，博弈层次已经从攻防技术演变为军事威慑力和经济安全的复合型战略博弈。IT技术先发地区的APT组织凭借技术积累，在网络武器研发、漏洞储备、网络资源掌控上占据优势；后发地区的APT组织，寄希望于网络空间中“弯道超车”，也投入资源加速网络军备竞赛。APT攻击已经从“单兵作战”升级为“体系化作战”，其复杂程度与组织性堪比一场小型“数字战争。

3、关键基础设施成为破坏与勒索的首选目标

无论是在在俄乌冲突中、伊以冲突中、印巴对峙中，还是在美国对南美国家的威吓中，情报窃取和系统破坏一直是APT组织的核心战术手段。在涉及到地缘政治冲突时候，国家级APT攻击必将延伸至军事、通信，电力、交通、能源等国计民生核心行业。不管是核心情报泄露，还是物理层面的破坏将会给对手造成严重后果。

“擦除器”这类攻击武器永久破坏目标系统数据，使其丧失可用性。其攻击效果明显，攻击动机简单直接：多为地缘政治威慑、战略破坏或掩盖攻击痕迹；攻击过程体现出“快速、彻底、隐蔽”的特征，致力于快速达成战术目标，防止追踪溯源。

勒索攻击是对基础设施破坏的一个重要手段，不同于“擦除器”这类攻击武器，勒索攻击的核心目标是数据劫持，以获取高额赎金为核心目的。但在APT组织开展的勒索攻击中，往往有更为隐晦的攻击目的。在过去我们捕获的APT勒索事件中，有些攻击的牟利动机不显，攻击者真实意图不明；而在一些窃密攻击活动当中，勒索攻击发生在攻击中段，表现为较强的黑灰产特征，意图掩盖攻击者真实意图，干扰事件归因；此外，还有一些黑灰产攻击者在数据劫持成功之后，将劫持系统售卖给APT组织，随着“窃密+加密”的双重勒索模式越来越多，这种商业转让将会更多发生。勒索攻击使得攻击者的攻击效果可以在“破坏”和“窃密”之间随时切换，更方便攻击者随时适配其攻击动机。

4、量子计算威胁逼近，加密数据泄露不可不查

量子计算通过核心算法，从数学基础上瓦解传统密码体系，引发“现在存储、未来解密”的追溯性威胁，同时催生混合攻击与防御失衡，是对网络安全范式的根本性挑战。

量子计算对网络安全的威胁是“颠覆性”而非“渐进式”，一旦量子计算威胁实现工程化，必将成为APT组织的核心攻击手段。当前，全球范围内已出现大量针对敏感数据的“囤积式攻击”，攻击者通过窃取金融、医疗、政务等领域的加密数据，等待量子计算技术成熟后进行解密。这种攻击模式的隐蔽性极强，一旦量子计算突破，将导致历史数据的批量泄露，造成不可挽回的损失。美国已经相继出台多项法案及标准来应对即将到来的威胁。2026年的核心任务，应尽快识别敏感数据资产，建立量子迁移计划。

5、网络攻击是混合作战的重要组成部分

不管是在俄乌冲突这种大规模兵团作战中，特种部队的小规模斩首行动中，还是印巴战略对峙中，网络攻击已从传统作战的“辅助手段”升级为“核心赋能模块”，其重要性贯穿作战全流程、覆盖战略-战役-战术全层级，是实现“降维打击”和“体系破击”的关键抓手。

混合作战的核心是多域力量的协同联动，而网络空间是串联陆、海、空、天、电等作战域的“无形纽带”。网络攻击的首要价值在于抢占“制网权”，进而夺取制信息权、制空权、制海权等传统制权的前置优势。

未来战争的胜负，很可能在网络空间的无声较量中早已决定。因此，构建强大的网络防御体系、提升网络韧性，并发展网络反击能力，已成为国家综合安全战略的重中之重。

6、攻击技术持续升级、系统化攻击工程是必经之路

在2025年，几乎所有的APT组织都升级了他们的攻击武器、攻击策略。在近些年的APT攻击行动中可以看出，先进的攻击工具能突破更为严密的防守，而复杂的攻击链才能造成更大的影响。

在未来，APT攻击组织的攻击能力将体现在能否将“复杂情报分析、技术的快速变化、战术的迅速调整”整合成统一、连贯的整体，能够自适应场景的变化。网络攻击手段将从零散工具叠加转向全链路协同、模块化组装、AI驱动闭环、产业化分工的系统化形态，攻击链被拆解为可复用组件，从侦察到攻击的全流程实现标准化，攻击工具集成系统化。以北美地区的APT-C-39（CIA）和APT-C-40（NSA）组织为代表，这些APT组织的渗透程度最深、潜伏时间最长。

APT组织的动机往往能体现出国家政治利益，博弈层次已经从攻防技术演变为军事威慑力和经济安全的复合型战略博弈。IT技术先发地区的APT组织凭借技术积累，在网络武器研发、漏洞储备、网络资源掌控上占据优势；后发地区的APT组织，寄希望于网络空间中“弯道超车”，也投入资源加速网络军备竞赛。APT攻击已经从“单兵作战”升级为“体系化作战”，其复杂程度与组织性堪比一场小型“数字战争。

PART 5

参考链接

参考链接

1. https://www.bleepingcomputer.com/news/security/sandworm-hackers-use-data-wipers-to-disrupt-ukraines-grain-sector/

2. https://www.welivesecurity.com/en/eset-research/operation-roundpress/#h2-6

3. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

4. https://research.checkpoint.com/2025/apt29-phishing-campaign/

5. https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/

6. https://mp.weixin.qq.com/s/zerWPti8aO8ymhOT1Ij-ig

7. https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/

8. https://harfanglab.io/insidethelab/uac-0057-pressure-ukraine-poland/

9. https://mp.weixin.qq.com/s/N-ut-NCAPdbdidb4Ng8hdw

10. https://mp.weixin.qq.com/s/CI1g4iaYxHhO925V15LvIQ

11. https://mp.weixin.qq.com/s/wxRSVugKHy7x1SmANQOrAA

12. https://mp.weixin.qq.com/s/ItcbKuoH0KjJjzSTG7YSrA

13. https://www.fortinet.com/blog/threat-research/confucius-espionage-from-stealer-to-backdoor

14. https://labs.k7computing.com/index.php/breakingdown-of-patchwork-apt/

15. https://www.trellix.com/blogs/research/from-click-to-compromise-unveiling-the-

PART 5

参考链接

参考链接

1. https://www.bleepingcomputer.com/news/security/sandworm-hackers-use-data-wipers-to-disrupt-ukraines-grain-sector/

2. https://www.welivesecurity.com/en/eset-research/operation-roundpress/#h2-6

3. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

4. https://research.checkpoint.com/2025/apt29-phishing-campaign/

5. https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/

6. https://mp.weixin.qq.com/s/zerWPti8aO8ymhOT1Ij-ig

7. https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/

8. https://harfanglab.io/insidethelab/uac-0057-pressure-ukraine-poland/

9. https://mp.weixin.qq.com/s/N-ut-NCAPdbdidb4Ng8hdw

10. https://mp.weixin.qq.com/s/CI1g4iaYxHhO925V15LvIQ

11. https://mp.weixin.qq.com/s/wxRSVugKHy7x1SmANQOrAA

12. https://mp.weixin.qq.com/s/ItcbKuoH0KjJjzSTG7YSrA

13. https://www.fortinet.com/blog/threat-research/confucius-espionage-from-stealer-to-backdoor

14. https://labs.k7computing.com/index.php/breakingdown-of-patchwork-apt/

15. https://www.trellix.com/blogs/research/from-click-to-compromise-unveiling-the-

sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/

16.https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis

17.https://fieldeffect.com/blog/zoom-doom-bluenoroff-call-opens-the-door

18.https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/saja-dprk-employment-scam-network.pdf

19.https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/

20.https://www.genians.co.kr/en/blog/threat_intelligence/android?hsCtaAttrib=255186951894

21.https://research.checkpoint.com/2025/iranian-educated-manticore-targets-leading-tech-academics/

22.https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/

23.https://unit42.paloaltonetworks.com/iranian-attackers-impersonate-model-agency/

24.https://mp.weixin.qq.com/s/nY2Hyg6ZsM7ViXW1lhO2Ag

25.https://hunt.io/blog/track-apt34-like-infrastructure-before-it-strikes

26.https://www.proofpoint.com/us/blog/threat-insight/call-it-what-you-want-threat-actor-delivers-highly-targeted-multistage-polyglot

27.https://securelist.com/bellacpp-cpp-version-of-bellaciao/115087/

28.https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/

29.https://www.group-ib.com/blog/muddywater-infrastructure-malware/#introduction

30.https://mp.weixin.qq.com/s/BHyqfnMMMAvDDX_LZVubyA

31.https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracing-blind-eagle-to-proton66/

32.https://x.com/Merlax/status/1919786735648833727

33.https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/#single-post

34.https://mp.weixin.qq.com/s/leEKONeK1JsAvPRF837Pow

35.https://www.recordedfuture.com/research/drat-v2-updated-drat-emerges-tag-140s-arsenal

36.https://hunt.io/blog/apt36-clickfix-campaign-indian-ministry-of-defence

37.https://www.seqrite.com/blog/goodbye-hta-hello-msi-new-ttps-and-clusters-of-an-apt-driven-by-multi-platform-attacks/

38.https://blog.xlab.qianxin.com/p/9a61b251-aa91-46df-b36a-dea00c3b8add/

39.https://mp.weixin.qq.com/s/88VDPssTV3LG9MHgAG5VsQ

40.https://mp.weixin.qq.com/s/nyxZFXgrtm2-tBiV3-wiMg

41.https://mp.weixin.qq.com/s/Cx-v95Ua8U7I77-yQFckpA

42.https://mp.weixin.qq.com/s/m2G9oLHv04HJDW8mB5rDA

43.https://3w.huanqiu.com/a/de583b/4MIDCq1bC5d

sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/

16.https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis

17.https://fieldeffect.com/blog/zoom-doom-bluenoroff-call-opens-the-door

18.https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/saja-dprk-employment-scam-network.pdf

19.https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/

20.https://www.genians.co.kr/en/blog/threat_intelligence/android?hsCtaAttrib=255186951894

21.https://research.checkpoint.com/2025/iranian-educated-manticore-targets-leading-tech-academics/

22.https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/

23.https://unit42.paloaltonetworks.com/iranian-attackers-impersonate-model-agency/

24.https://mp.weixin.qq.com/s/nY2Hyg6ZsM7ViXW1lhO2Ag

25.https://hunt.io/blog/track-apt34-like-infrastructure-before-it-strikes

26.https://www.proofpoint.com/us/blog/threat-insight/call-it-what-you-want-threat-actor-delivers-highly-targeted-multistage-polyglot

27.https://securelist.com/bellacpp-cpp-version-of-bellaciao/115087/

28.https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/

29.https://www.group-ib.com/blog/muddywater-infrastructure-malware/#introduction

30.https://mp.weixin.qq.com/s/BHyqfnMMMAvDDX_LZVubyA

31.https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracing-blind-eagle-to-proton66/

32.https://x.com/Merlax/status/1919786735648833727

33.https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/#single-post

34.https://mp.weixin.qq.com/s/leEKONeK1JsAvPRF837Pow

35.https://www.recordedfuture.com/research/drat-v2-updated-drat-emerges-tag-140s-arsenal

36.https://hunt.io/blog/apt36-clickfix-campaign-indian-ministry-of-defence

37.https://www.seqrite.com/blog/goodbye-hta-hello-msi-new-ttps-and-clusters-of-an-apt-driven-by-multi-platform-attacks/

38.https://blog.xlab.qianxin.com/p/9a61b251-aa91-46df-b36a-dea00c3b8add/

39.https://mp.weixin.qq.com/s/88VDPssTV3LG9MHgAG5VsQ

40.https://mp.weixin.qq.com/s/nyxZFXgrtm2-tBiV3-wiMg

41.https://mp.weixin.qq.com/s/Cx-v95Ua8U7I77-yQFckpA

42.https://mp.weixin.qq.com/s/m2G9oLHv04HJDW8mB5rDA

43.https://3w.huanqiu.com/a/de583b/4MIDCq1bC5d

44.https://www.cert.org.cn/publish/main/49/2025/20250117141306569102021/20250117141306569102021_.html

45.https://www.cert.org.cn/publish/main/49/2025/20250117141608670773438/20250117141608670773438_.html

46.https://www.cverc.org.cn/head/zhaiyao/news20250403-haerbinyadonghui.htm

47.https://www.cert.org.cn/publish/main/49/2025/20251019142622914870997/20251019142622914870997_.html

48.http://society.people.com.cn/n1/2025/0528/c1008-40489086.html

49.http://www.china.com.cn/opinion2020/2025-06/09/content_117916848.shtml

50.https://www.impriindia.com/insights/policy-update/space-security-cyber/

51.https://www.mea.gov.in/press-releases.htm?dtl%2F38924%2F

52.https://news.cnr.cn/native/gd/kx/20251019/t20251019_527401113.shtml

53.https://www.mps.gov.cn:8080/n2254098/n4904352/c10047273/content.html

54.https://mp.weixin.qq.com/s/ZtKjlaIoMVCSY-rXt2RP1Q

55.https://mp.weixin.qq.com/s/nFdDdsTVGR9LD4t5NW8VHw

56.https://www.china-cia.org.cn/WorkDetail/MCA-by-USIA.html

57.https://mp.weixin.qq.com/s/kzdSrLdejED3MxSKtszUnA

58.https://mp.weixin.qq.com/s/fm4Z9L0_b3w3A-QdqkB_7A

59.https://mp.weixin.qq.com/s/1uVaMzBvt1PlmMMXEZvuzg

60.https://mp.weixin.qq.com/s/AS3kRKDW63IzZCbxIb_MoA

61.https://cloud.tencent.com.cn/developer/article/2564920

62.https://www.toutiao.com/article/7590002044509930036/

63.https://www.51cto.com/article/819037.html

64.https://www.toutiao.com/article/7587234030123352617/

65.https://www.c114.com.cn/satellite/2514/a1286133.html

66.https://cloud.tencent.com.cn/developer/article/2577187

67.https://www.br-cn.com/static/content/news/br_news/2025-10-22/1430659388729757547.html

68.https://thehackernews.com/2025/08/blind-eagles-five-clusters-target.html

69.https://www.toutiao.com/article/7592393443097035279/

70.resecurity.com/blog/article/paraguay-is-being-targeted-by-cybercriminals-74-million-citizen-records-for-sale

71.https://blog.lacnic.net/en/the-perfect-storm-the-largest-cyberattack-on-brazils-financial-system/

72.https://www.crowdstrike.com/en-us/blog/2025-latam-threat-landscape-report-deep-dive/

73.https://mp.weixin.qq.com/s/43unkZrYzJ4Roo-2NuREZg

74.https://armedservices.house.gov/uploadedfiles/deterring_china.pdf

75.https://docs.house.gov/billsthisweek/20241209/RCP_HR5009_xml%5b89%5d.pd

44.https://www.cert.org.cn/publish/main/49/2025/20250117141306569102021/20250117141306569102021_.html

45.https://www.cert.org.cn/publish/main/49/2025/20250117141608670773438/20250117141608670773438_.html

46.https://www.cverc.org.cn/head/zhaiyao/news20250403-haerbinyadonghui.htm

47.https://www.cert.org.cn/publish/main/49/2025/20251019142622914870997/20251019142622914870997_.html

48.http://society.people.com.cn/n1/2025/0528/c1008-40489086.html

49.http://www.china.com.cn/opinion2020/2025-06/09/content_117916848.shtml

50.https://www.impriindia.com/insights/policy-update/space-security-cyber/

51.https://www.mea.gov.in/press-releases.htm?dtl%2F38924%2F

52.https://news.cnr.cn/native/gd/kx/20251019/t20251019_527401113.shtml

53.https://www.mps.gov.cn:8080/n2254098/n4904352/c10047273/content.html

54.https://mp.weixin.qq.com/s/ZtKjlaIoMVCSY-rXt2RP1Q

55.https://mp.weixin.qq.com/s/nFdDdsTVGR9LD4t5NW8VHw

56.https://www.china-cia.org.cn/WorkDetail/MCA-by-USIA.html

57.https://mp.weixin.qq.com/s/kzdSrLdejED3MxSKtszUnA

58.https://mp.weixin.qq.com/s/fm4Z9L0_b3w3A-QdqkB_7A

59.https://mp.weixin.qq.com/s/1uVaMzBvt1PlmMMXEZvuzg

60.https://mp.weixin.qq.com/s/AS3kRKDW63IzZCbxIb_MoA

61.https://cloud.tencent.com.cn/developer/article/2564920

62.https://www.toutiao.com/article/7590002044509930036/

63.https://www.51cto.com/article/819037.html

64.https://www.toutiao.com/article/7587234030123352617/

65.https://www.c114.com.cn/satellite/2514/a1286133.html

66.https://cloud.tencent.com.cn/developer/article/2577187

67.https://www.br-cn.com/static/content/news/br_news/2025-10-22/1430659388729757547.html

68.https://thehackernews.com/2025/08/blind-eagles-five-clusters-target.html

69.https://www.toutiao.com/article/7592393443097035279/

70.resecurity.com/blog/article/paraguay-is-being-targeted-by-cybercriminals-74-million-citizen-records-for-sale

71.https://blog.lacnic.net/en/the-perfect-storm-the-largest-cyberattack-on-brazils-financial-system/

72.https://www.crowdstrike.com/en-us/blog/2025-latam-threat-landscape-report-deep-dive/

73.https://mp.weixin.qq.com/s/43unkZrYzJ4Roo-2NuREZg

74.https://armedservices.house.gov/uploadedfiles/deterring_china.pdf

75.https://docs.house.gov/billsthisweek/20241209/RCP_HR5009_xml%5b89%5d.pd

f

76.https://www.congress.gov/bill/119th-congress/senate-bill/2296/text

77.https://www.congress.gov/bill/119th-congress/senate-bill/1071/text

78.https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view?gid=897725844#gid=897725844

79.https://nvd.nist.gov/vuln/detail/CVE-2025-31201

80.https://github.com/JGoyd/iOS-Attack-Chain-CVE-2025-31200-CVE-2025-31201

81.https://www.securitylab.ru/news/557556.php

82.https://www.elliptic.co/blog/iranian-crypto-exchange-nobitex-hacked-pro-israel-group

83.https://www.jpost.com/israel-news/article-857969

84.https://www.presstv.ir/Detail/2026/01/01/761673/Iran-cyberattacks-Sattar-Hashemi-communications-infrastructure-Behzad-Akbari-DDoS-

85.https://www.stepsecurity.io/blog/ctrl-tinycolor-and-40-npm-packages-compromised

2025年度
全球高级持续性威胁（APT）
研究报告

2025
GLOBAL ADVANCED PERSISTENT THREAT RESEARCH REPORT

f

76.https://www.congress.gov/bill/119th-congress/senate-bill/2296/text

77.https://www.congress.gov/bill/119th-congress/senate-bill/1071/text

78.https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view?gid=897725844#gid=897725844

79.https://nvd.nist.gov/vuln/detail/CVE-2025-31201

80.https://github.com/JGoyd/iOS-Attack-Chain-CVE-2025-31200-CVE-2025-31201

81.https://www.securitylab.ru/news/557556.php

82.https://www.elliptic.co/blog/iranian-crypto-exchange-nobitex-hacked-pro-israel-group

83.https://www.jpost.com/israel-news/article-857969

84.https://www.presstv.ir/Detail/2026/01/01/761673/Iran-cyberattacks-Sattar-Hashemi-communications-infrastructure-Behzad-Akbari-DDoS-

85.https://www.stepsecurity.io/blog/ctrl-tinycolor-and-40-npm-packages-compromised

2025年度
全球高级持续性威胁（APT）
研究报告

2025
GLOBAL ADVANCED PERSISTENT THREAT RESEARCH REPORT

2025年
全球高级持续性威胁（APT）
研究报告

RESEARCH
REPORT

360数字安全
数字安全的领导者

360
高级威胁研究院

360数字安全
数字安全的领导者

360
高级威胁研究院

ADVANCED PERSISTENT THREAT

2025

全球高级持续性威胁(APT)研究报告