360数字安全
数字安全的领导者

360
高级威胁研究院

2023 RESEARCH REPORT

全球高级
持续性威胁
研究报告

CONTENTS | 目录

PART 01

2023年高级可持续性威胁概览

2023 ADVANCED PERSISTENT THREAT

PART.01

2023年全球高级可持续性威胁概览

Advanced Persistent Threat

2023年，全球政治格局和国际关系日益复杂，俄乌冲突持续胶着，中东地区又爆发新一轮巴以冲突，全球秩序面临前所未有的变革和挑战，传统安全问题变得更加严峻和复杂。全球所面临来自网络空间的威胁日益增加，高级持续性威胁（APT）形势也更加严峻复杂，成为国家网络空间安全战略需要应对的突出风险。

全球网络安全厂商和机构在2023年累计公开发布APT报告731篇，报告中涉及APT组织135个，其中首次披露的APT组织46个。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，攻击目标主要分布于政府、国防军工等行业领域。

我国是APT攻击活动主要受害国之一。截至目前，360依托全网安全大脑“看见威胁”的能力，已累计发现54个境外APT组织，2023年最新捕获到两个境外组织：APT-C-57（沃尔宁）、APT-C-68（寄生虫）。全年360监测到13个境外APT组织针对我国的APT攻击活动1200多起，相关APT组织主要归属北美、南亚、东南亚和东亚地区。受影响重点目标涉及16个行业领域，受影响行业TOP 5为：教育、政府、科研、国防军工、交通运输。

360一直以来持续监测和跟进美国的APT组织针对我国的网络攻击活动：今年3月，360对 APT-C-39（CIA）组织网络攻击武器和技战术细节进行了揭秘；7月，国家计算机病毒应急处理中心和360联合处置了美国组织对武汉市地震中心的网络渗透攻击；9月，国家计算机病毒应急处理中心和360披露了APT-C-40（NSA）组织网络间谍武器“二次约会”的技术分析报告。

2023年APT组织在攻击活动中利用的0day漏洞数量继续保持高位，东亚地区组织APT-C-06（DarkHotel）和APT-C-68（寄生虫）组织多次利用0day漏洞，针对特定行业软件供应商展开攻击。针对移动平台的APT攻击愈加频繁且复杂，移动平台的0day漏洞增长明显，这以APT-C-40（NSA）组织利用一系列漏洞针对苹果iOS系统的“Triangulation”攻击活动最具代表性。

纵观2023年，APT组织在攻击活动中呈现出一系列新态势：我国半导体芯片、5G等高科技领域成为北美方向组织攻击新重点；多个地区组织对我国地理、地质测绘信息相关目标攻击活动持续升温；另外我国驻外机构和企业遭受的APT攻击，无论从频次还是受影响程度都明显升高。全球范围APT组织针对能源行业攻击活跃度增加；网络攻击组织不仅以窃取军事情报方式介入地区冲突，还逐渐开展实际破坏性攻击。

网络空间对抗的重要性在地缘政治博弈和地区冲突中的作用日益突出，网络空间逐渐成为地缘政治较量的制高点。未来在在人工智能、神经网络等新技术的加持下，来自网络空间的威胁将成为所有国家共同需要面对的严峻挑战。

PART 02

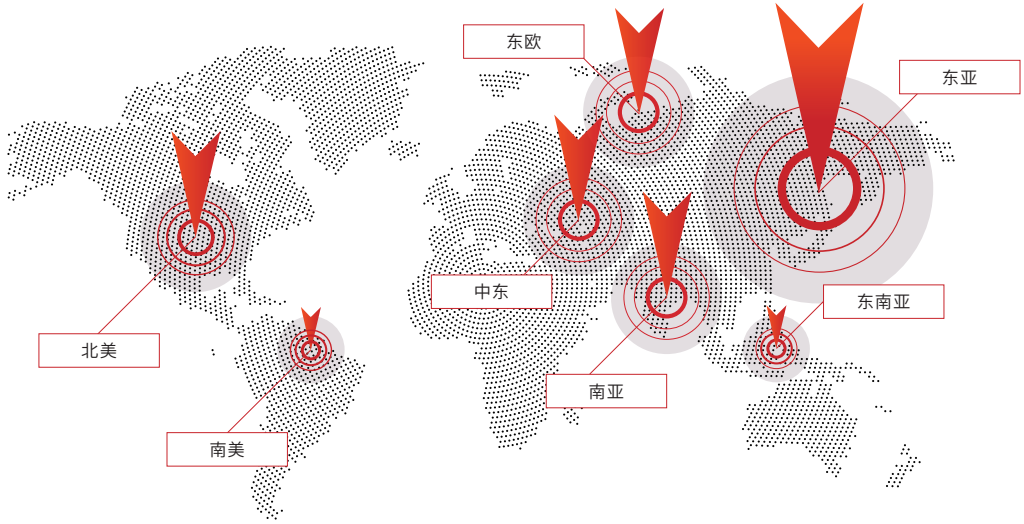
2023年全球活跃APT组织

2023 ADVANCED PERSISTENT THREAT

2023年全球活跃APT组织

Advanced Persistent Threat

进入2023年，全球政治格局和国际关系的日益复杂，全球秩序面临着前所未有的变革和挑战，全球化的消极互动成为一段时期内全球经济与政治互动的主要特征。在此形势下全球APT组织的攻击活动继续保持着高活跃度。截止2023年12月，全球网络安全厂商以及机构，公开发布APT报告累计731篇，报告中涉及APT组织135个，其中属于首次披露的APT组织46个。



北美	组织名称	活跃程度
	APT-C-39 (CIA)	★★★
	APT-C-57 (沃尔宁)	★★★
	APT-C-40 (NSA)	★★

东亚	组织名称	活跃程度
	APT-C-01 (毒云藤)	★★★★
	APT-C-26 (Lazarus)	★★★½
	APT-C-55 (Kimsuki)	★★★½
	APT-C-68 (寄生虫)	★★★
	APT-C-06 (DarkHotel)	★★★
	APT-C-28 (ScarCruft)	★★½

中东	组织名称	活跃程度
	APT-C-63 (沙鹰)	★★★
	APT-C-51 (APT35)	★★
	APT-C-23 (双尾蝎)	★★
	APT-C-49 (OilRig)	★

南亚	组织名称	活跃程度
	APT-C-09 (摩诃草)	★★★½
	APT-C-08 (蔓灵花)	★★★½
	APT-C-48 (CNC)	★★★½
	APT-C-24 (响尾蛇)	★★★
	APT-C-56 (透明部落)	★★½
	APT-C-61 (腾云蛇)	★★

东南亚	组织名称	活跃程度
	APT-C-00 (海莲花)	★★★★

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

南美	组织名称	活跃程度
	APT-C-36 (盲眼鹰)	★½

▶ 2023年全球典型APT组织活跃度情况

根据360全网安全大脑监测：2023年对中国发起攻击活动的APT组织，主要为归属南亚、东南亚、东亚等地区的13个组织。目标单位集中分布于教育、政府、科研、国防军工、交通运输等16个重点行业领域。从地域分布看，我国受APT攻击影响的单位，集中分布于东南沿海和政治经济中心区域。这与我国关基行业、教育科研重点资源、国防军工核心单位地域分布情况存在相关性。

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2023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	教育、政府、交通运输等
TOP2	APT-C-09（摩诃草）	南亚	教育、国防军工、科研等
TOP3	APT-C-00（海莲花）	东南亚	政府、教育、科研等
TOP4	APT-C-08（蔓灵花）	南亚	政府、教育、能源等
TOP5	APT-C-48（CNC）	南亚	教育、科研、国防军工等
TOP6	APT-C-06（DarkHotel）	东亚	制造、政府等
TOP7	APT-C-39（CIA）	北美	制造、科研等
TOP8	APT-C-24（响尾蛇）	南亚	政府、国防军工等
TOP9	APT-C-68（寄生虫）	东亚	国防军工、科研等
TOP10	APT-C-60（伪猎者）	东亚	教育等


2023
ADVANCED
PERSISTENT
THREAT

北美 | Advanced Persistent Threat

来自美国的网络黑客组织针对全球的网络攻击行为早已呈现出自动化、体系化和智能化的特征，其网络武器技术先进，攻击手法复杂，几乎可以覆盖全球所有互联网和物联网资产，攻击者为达到军事、政治侦察目的，可以随时随地控制他国网络，窃取关键数据。

继2022年6月，美国APT-C-40 (NSA) 组织针对西北工业大学的网络攻击活动披露后，2023年7月，国家计算机病毒应急处理中心和360公司再次处置和披露和处置了美国方向黑客组织针对武汉市地震监测中心的网络攻击活动[1]。地震检测中心的地震烈度数据与国家安全息息相关，通过地震烈度数据可以还原出我交通、能源、军事等重要领域特定区域的三维地貌图，如果数据泄露将严重威胁我国军事安全和国家安全。

2023年，360高级威胁研究院通过持续监测发现来源于北美方向针对我国的最新攻击活动。进一步综合研判溯源将此次攻击归属为一个全新APT组织：APT-C-57 (沃尔宁) 。该组织擅长利用重点目标专用应用软件进行复杂的供应链攻击。其攻击活动最早可追溯到2018年，2021年至2023年间持续活跃。

APT-C-39 (CIA)

APT-C-39 (CIA) 组织长期针对中国航空航天、科研机构、石油、大型互联网公司以及政府等关键领域进行网络渗透攻击。2023年360先是在《“黑客帝国”调查报告——美国中央情报局 (CIA) (之一)》[2]报告中，对CIA组织网络攻击武器主要细节进行了揭秘，随后在对CIA组织的持续跟踪中，再次捕获到该组织针对我国芯片、5G通信等领域目标的最新攻击活动。结合当前美国针对我国芯片、5G等高科技领域的打压态势，其用心不言而喻。

APT-C-39 (CIA) 组织对中国和其他国家实施的网络攻击窃密活动，大量使用0day漏洞，其中包括大批至今未被公开披露的后门和漏洞，在世界各地建立“僵尸”网络和攻击跳板网络，针对网络服务器、网络终端、交换机和路由器，以及数量众多的工业控制设备分阶段实施攻击入侵行动。APT-C-39 (CIA) 组织针对全球发起的网络攻击行为早已呈现出自动化、体系化和智能化的特征。

360高级威胁研究人员在APT-C-39 (CIA) 组织针对中国境内目标实施的网络攻击行动中，成功提取了多个“Vault7”(穹顶7) 网络攻击武器样本。通过对样本进行分析发现：CIA组织使用的后门程序和攻击组件大都以无实体文件的内存驻留执行方式运行。这使得对相关样本的发现和取证难度极大。我们将捕获的APT-C-39 (CIA) 组织攻击武器按类别，分为框架平台类、攻击模块投递类、远程控制类、横向移动类、信息收集窃取类、漏洞利用类、伪装正常软件类、安全软件攻防类、第三方开源工具类9个类别。

应对APT-C-39 (CIA) 组织高度体系化、智能化、隐蔽化的网络攻击，如何快速“看见”并第一时间对威胁进行“处置”尤为重要。我们在采用自主可控国产化设备的同时，应针对APT攻击威胁开展自检自查，逐步建立起长效防御体系，实现全面系统化防治，以抵御此类高级威胁攻击。

▶ APT-C-39 (CIA) 组织攻击武器类别

APT-C-40 (NSA)

2022年，国家计算机病毒应急处理中心会同360公司配合侦办西北工业大学被APT-C-40（NSA）组织网络攻击事件过程中，成功提取了NSA组织使用的“二次约会”网络间谍软件的多个样本，并通过样本分析，锁定了一系列网络攻击行动背后美国国家安全局（NSA）工作人员的真实身份。

2023年9月，国家计算机病毒应急处理中心和360公司对NSA组织使用的“二次约会”网络间谍软件技术分析报告进行了披露[3]。该间谍软件可实现网络流量窃听劫持、中间人攻击、插入恶意代码等恶意功能，它与其他恶意软件配合可以完成复杂的网络“间谍”活动。

技术分析发现，“二次约会”间谍软件是一款高技术水平的网络间谍工具。“二次约会”间谍软件长期驻留在网关、边界路由器、防火墙等网络边界设备上，可针对海量数据流量进行精准过滤与自动化劫持，实现中间人攻击功能。其主要功能包括网络流量嗅探、网络会话追踪、流量重定向劫持、流量篡改等。

2023年6月，国外安全厂商披露了NSA组织使用多个iOS平台0day漏洞针对iOS移动设备的攻击活动。攻击者通过iMessage平台使用0-click漏洞进行感染，先后利用多个漏洞获得对设备和用户数据的完全控制。

APT组织对我国国防科技背景高校单位的网络攻击活动，实则目标是针对我国国防军工和科技创新体系的渗透和窃密。我国政府机构、重点企业、教育科研等关基单位，应实现自身网络安全隐患和威胁的排查，对网络攻击威胁做到有效防御，即时发现溯源、实时阻断处置。

南亚 | Advanced Persistent Threat

2023年，南亚地区APT组织依旧以中国、巴基斯坦、孟加拉国等周边国家为攻击重心。攻击活动主要围绕国防军工、政府、能源、科研等关键行业领域。

2023年下半年，南亚地区APT组织针对我国的攻击活动频次均呈现出不同程度的增加。其中APT-C-08（蔓灵花）和APT-C-24（响尾蛇）组织针对我国驻外使馆、驻外合作等外事机构攻击活跃。

APT-C-08（蔓灵花）

APT-C-08（蔓灵花）组织在2023年的攻击活动十分活跃，攻击目标集中在我国驻外机构、驻外企业中涉及科技、商贸合作的相关单位，除此之外其攻击活动还影响国防军工、教育、科研相关单位。

在2023年的威胁狩猎中360监测到蔓灵花组织在部分攻击活动更新了技战术：起始阶段payload，除常用的CHM文件外，还利用lnk文件进行投递，进而用wscript调用系统SyncAppvPublishingServer.vbs文件执行下载命令。与以往攻击流程区别在于，msi文件不再作为最后阶段的远程控制工具，而是用于创建任务计划和持久化阶段的工具，具体攻击流程如下：

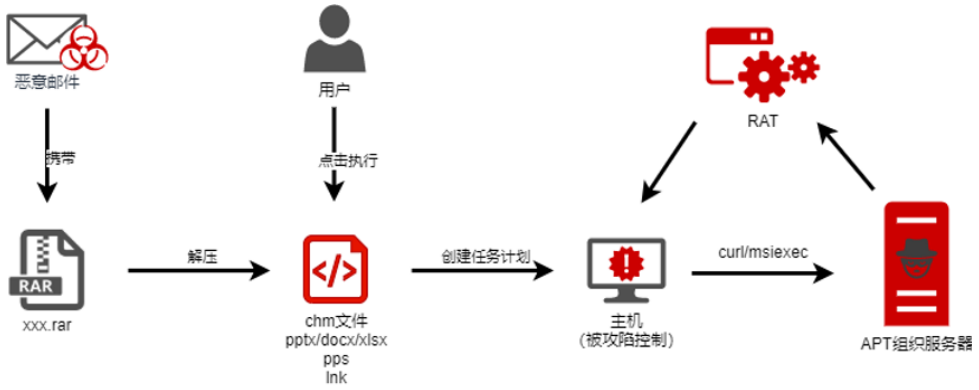


图1

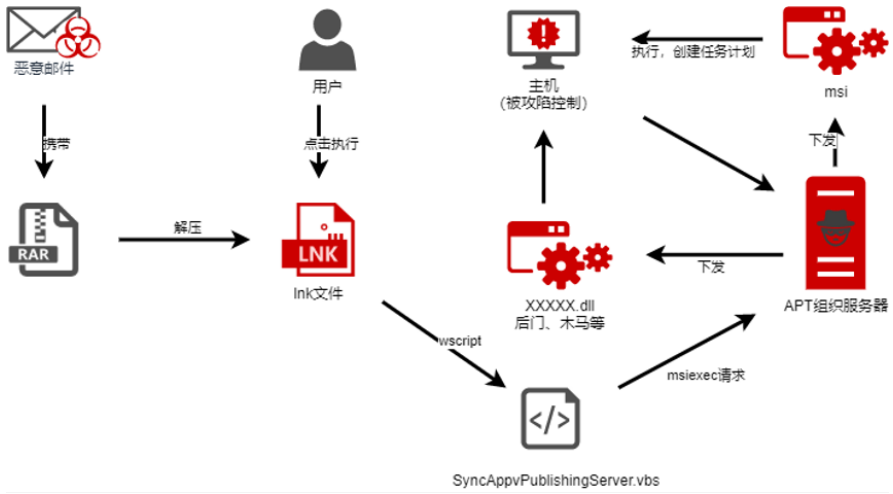


图2

▶ 图1 蔓灵花组织利用不同恶意附件类型，展开攻击的基本流程

▶ 图2 蔓灵花组织利用lnk文件的攻击流程

APT-C-09 (摩诃草)

APT-C-09 (摩诃草) 组织在2023年的攻击活动突然活跃。通过监测发现，摩诃草组织全年攻击活动主要针对教育、科研以及国防军工等领域。攻击重点存在间歇性更替变化，其中针对教育领域的攻击活动贯穿全年，针对气象类科研机构的攻击活动，集中在5月和10月展开；另外该组织针对几个重点目标，会在一段时间内，进行集中大规模攻击。

摩诃草组织一直处于不活跃状态，2022年底开始短暂活跃，进入2023年以来的持续攻击，是摩诃草组织组织持续时间最久，攻击影响范围最广的一次攻击活动。

摩诃草组织在本轮活跃攻击中不断更新攻击组件。攻击手法主要以投递恶意lnk文件为主，后续阶段投放的木马程序不仅包含BADNEWS组件，还利用多种开源远控工具或者开源loader加载其远控工具，并在一些组件中使用数字签名和强”壳“保护。其使用的攻击流程如下。

▶ 摩诃草组织用于攻击活动的诱饵文档截图

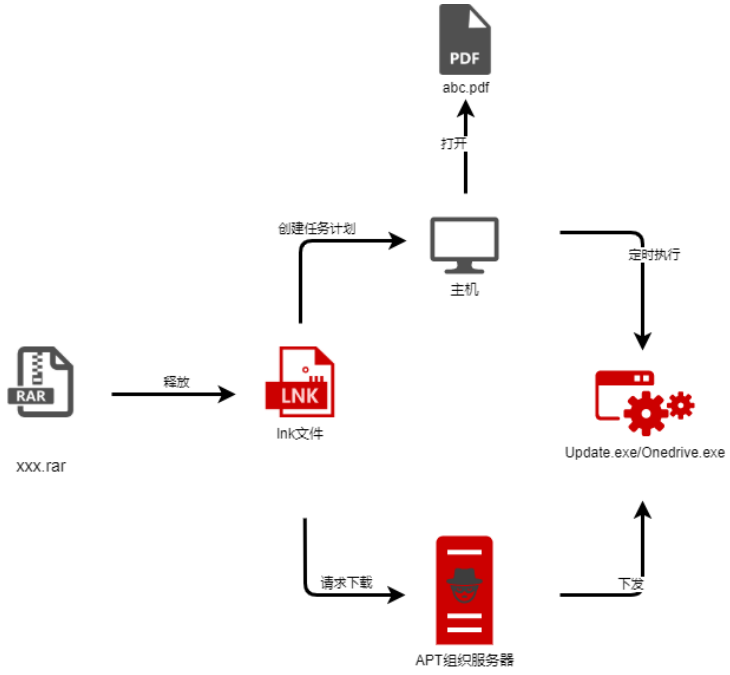


图1

APT-C-48 (CNC)

2023年APT-C-48 (CNC) 组织针对我国的攻击活动，攻击目标集中在我国教育、科研领域相关单位，依旧以窃取重点科研单位机密数据和文件为目的。受CNC组织攻击影响的重点高校和科研单位，大都具有国防军工背景。在2023年下半年，CNC组织攻击活动明显活跃，在11月、12月达到高峰。

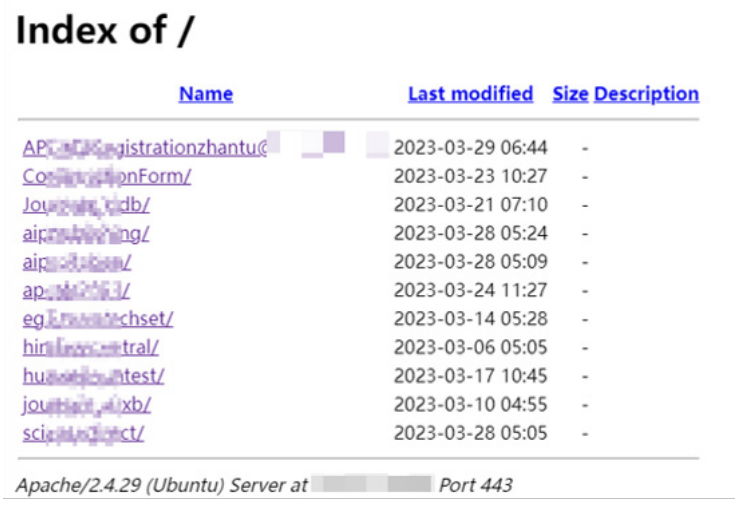


图2

▶ 图1 摩诃草组织攻击活动流程图

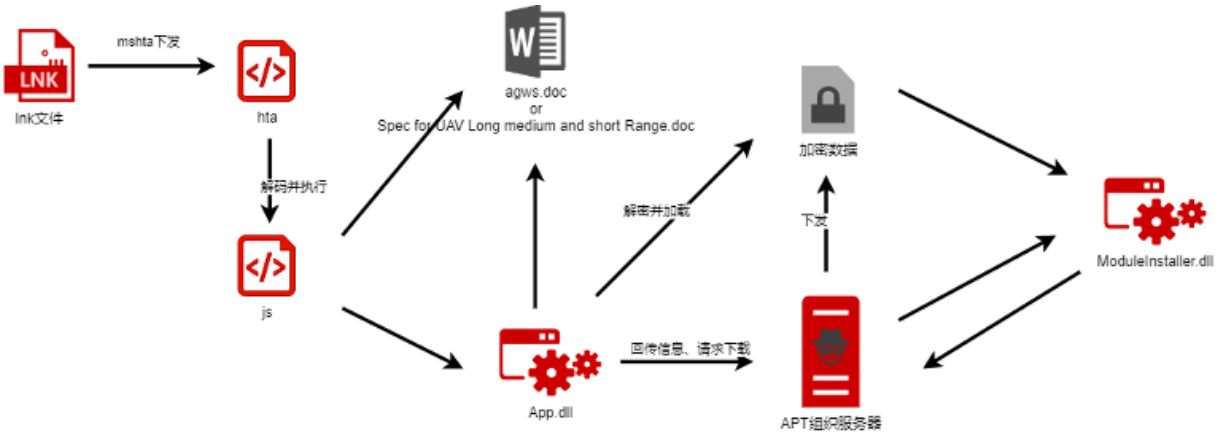
▶ 图2 360捕获到的CNC组织攻击使用的基础设施信息

南亚·其他组织 | Advanced Persistent Threat

APT-C-24（响尾蛇）

2023年，APT-C-24（响尾蛇）组织延续了对我国以及南亚地区周边国家外交事务相关人员的攻击活动。我国受其攻击影响的单位主要为外事机构以及驻外商贸相关单位，此外360高级威胁研究院还捕获到该组织针对我国高校相关目标的攻击。

响尾蛇组织在2023年部分攻击活动中，对攻击流程做了更新：url使用了新的混淆伪装手法，在起始阶段的lnk文件中对URL做了新的伪装。



APT-C-35（肚脑虫）

APT-C-35（肚脑虫）组织一直以来主要针对巴基斯坦、斯里兰卡、孟加拉国等地区的政府等领域进行网络间谍活动，以窃取敏感信息为主要目的。

360高级威胁研究院捕获到肚脑虫组织在2023年对攻击手法进行了更新。一是利用历史inp文档漏洞进行后续阶段的RAT下发，在此步骤中改用了商业版的Remcos RAT，之后沿用其历史攻击所用组件，攻击流程如下：

▶ 响尾蛇组织基本攻击流程

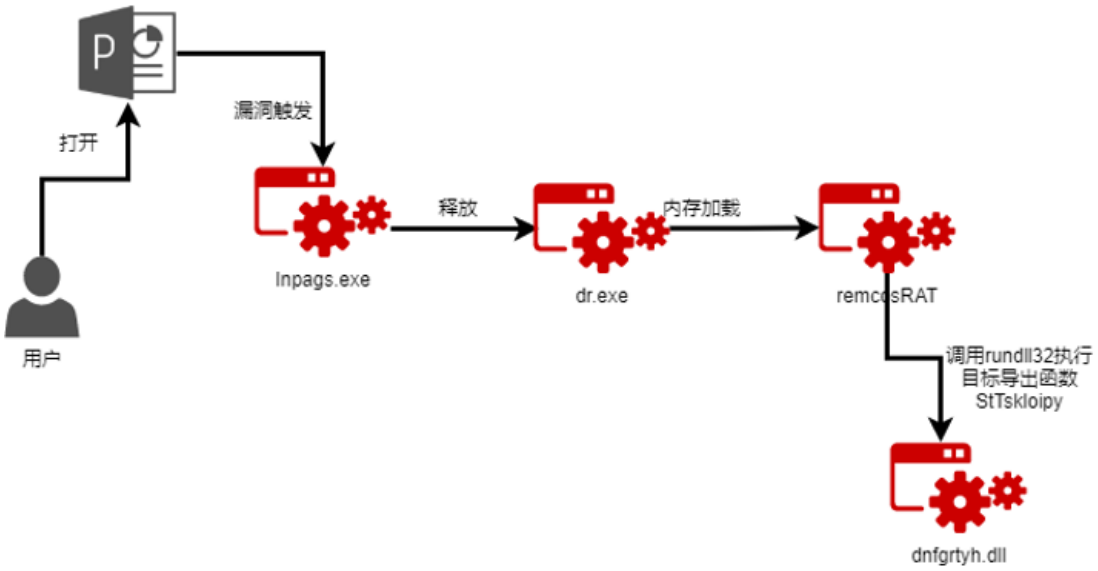


图1

二是借助恶意lnk文件下发hta文件，进而利用powershell下发Remcos RAT，攻击流程如下:

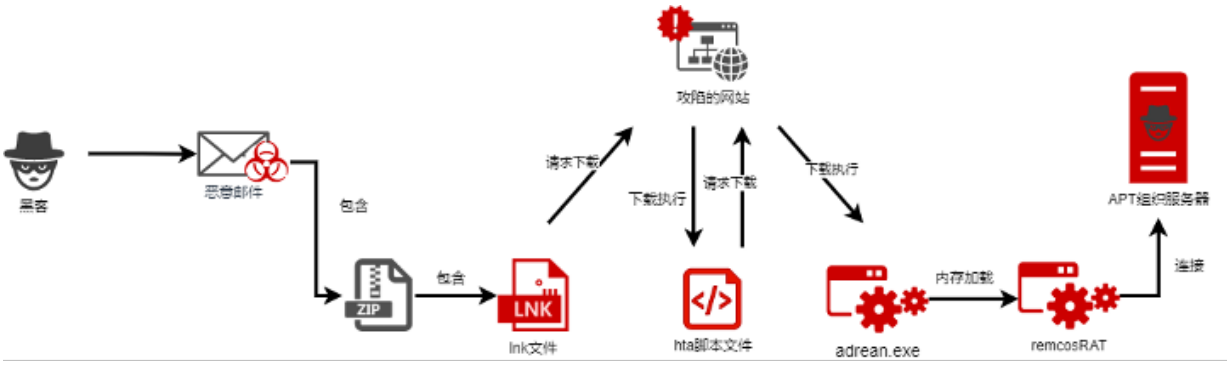


图2

▶ 图1 肚脑虫利用inp漏洞文档攻击流程

▶ 图2 肚脑虫利用lnk攻击流程

APT-C-56（透明部落）

APT-C-56（透明部落）组织长期针对南亚周边国家和地区，尤其是印度的政治、军事目标进行定向攻击活动。该组织具备在Windows、Android和Linux多平台开展攻击活动的能力。

2023年，透明部落组织主要通过投递恶意LNK快捷方式文件和携带恶意宏代码的诱饵文档的方式，投放CrimsonRAT后门程序针对印度的政府、军队、国防、医疗、电力、金融等单位进行攻击[4]。

360高级威胁研究院在2023年首次监测到透明部落通过伪造印度国家奖学金门户、印度陆军福利教育学会钓鱼网站向受害用户投放三平台木马进行攻击[5]。

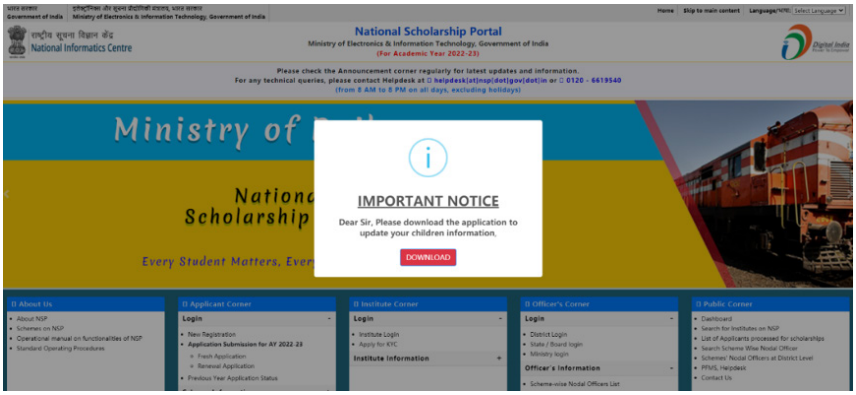


图1

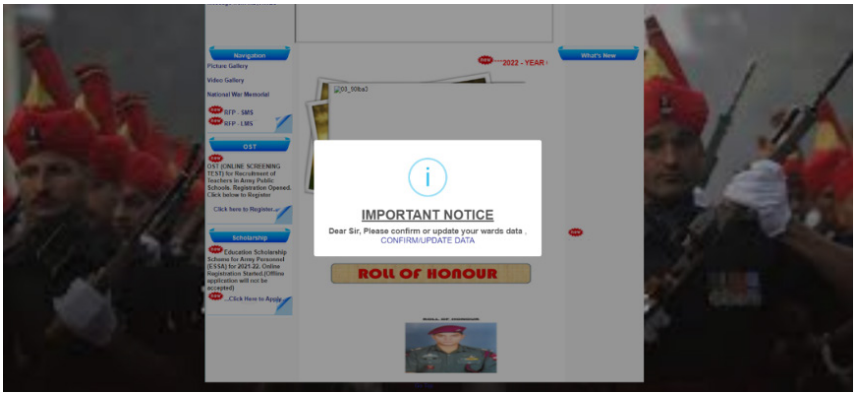


图2

▶ 图1 APT-C-56组织伪造印度国家奖学金网站

▶ 图2 APT-C-56组织伪造印度陆军福利教育学会网站

东亚 | Advanced Persistent Threat

2023年，东亚地区APT组织在攻击活动和攻击技战术更新上均保持着活跃态势。主要活跃组织如：APT-C-01（毒云藤）、APT-C-26（Lazarus）、APT-C-06（DarkHotel）、APT-C-55（Kimsuky）等。此外，360高级威胁研究院还捕获了东亚地区的新的活跃APT组织：APT-C-68（寄生虫）。

APT-C-01（毒云藤）组织依旧主要针对我国教育、政府、科研、国防军工领域展开大规模钓鱼攻击；APT-C-06（DarkHotel）在攻击活动中不断更新其前期载荷投递文件；APTC-26（Lazarus）下属组织具有更广泛的攻击目标，受其攻击影响的用户地域分布广泛，常进行网络间谍或以经济目的为驱动的网络攻击活动；APT-C-55（Kimsuky）和APT-C-28（ScarCruft）组织常以窃密为目的发起攻击，偶尔也以经济目的发起攻击。从现阶段我们捕获的APT-C-68（寄生虫）组织攻击活动看，该组织主要关注我国科研、教育、军工等行业。

APT-C-01（毒云藤）

2023年，APT-C-01（毒云藤）组织保持着针对我国教育、政府、国防军工、科研等领域的活跃攻击态势。毒云藤组织通过使用紧跟时事热点的诱饵文档和伪装性较强的钓鱼网页，发起大规模钓鱼攻击，主要以窃取受害者邮箱账号等信息为目的。

通过监测发现：与以往相比，毒云藤组织降低了通过钓鱼网站投递恶意附件进行攻击的倾向。受害者输入邮箱账户密码后，网站跳转下载附件或访问链接，多为正常文件和官方白链接。

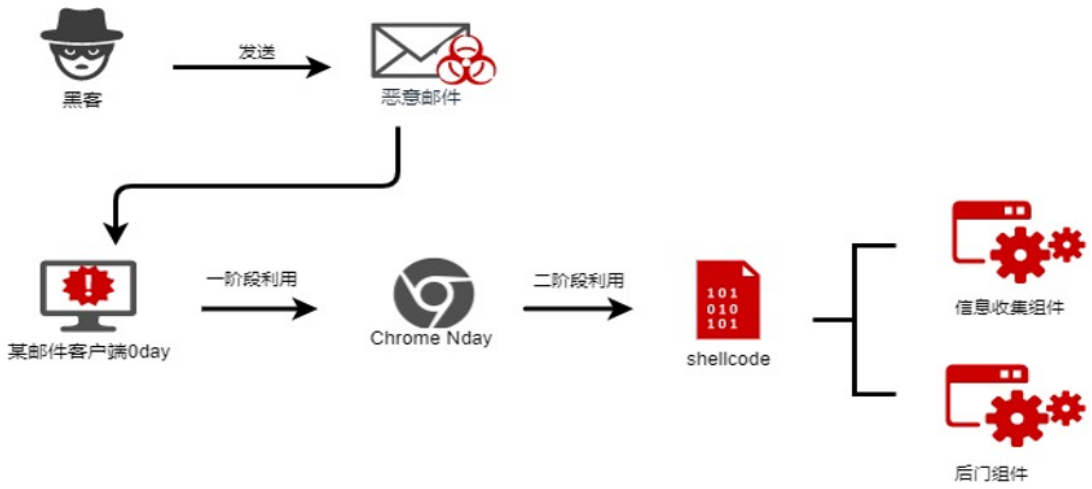
毒云藤组织主要的钓鱼手法为鱼叉邮件配合钓鱼链接，向目标群体发送带有钓鱼链接的邮件进行广撒网式的钓鱼，使用的诱饵文件具有很强的针对性，例如，针对高校教职工，使用主题为“稿件审核”的诱饵文档；针对航空航天领域人员，使用带有“航天”、“航站楼”等字眼的诱饵文档；针对我国海事机构或沿海地区目标，则是利用“海洋强区”，“海洋经济”等主题的诱饵文档。用户点击邮件附带的伪装钓鱼链接后，往往提示用户需要重新登录或者验证。

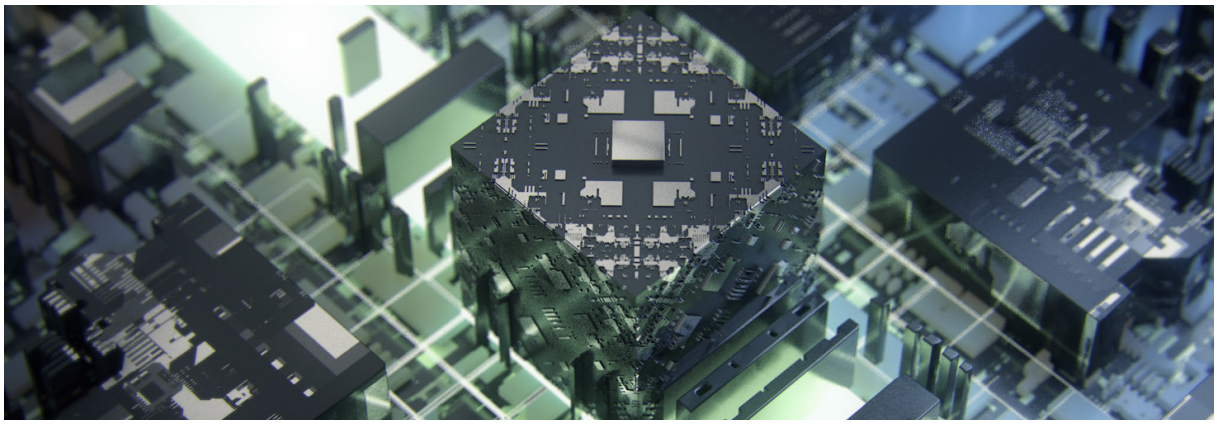
▶ 毒云藤组织使用的部分诱饵文档截图

APT-C-06 (DarkHotel)

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。受其攻击影响用户主要分布于我国近朝鲜半岛和东南沿海部分地区。360高级威胁研究院监测发现，2023年DarkHotel组织针对我国国防军工、政府机构等领域的攻击活跃度，较往年有所提升。

2023年，APT-C-06 (DarkHotel) 组织利用国内某邮件系统0day漏洞进行大规模攻击。攻击活动主要针对要我国政府、科研以及涉朝相关单位。

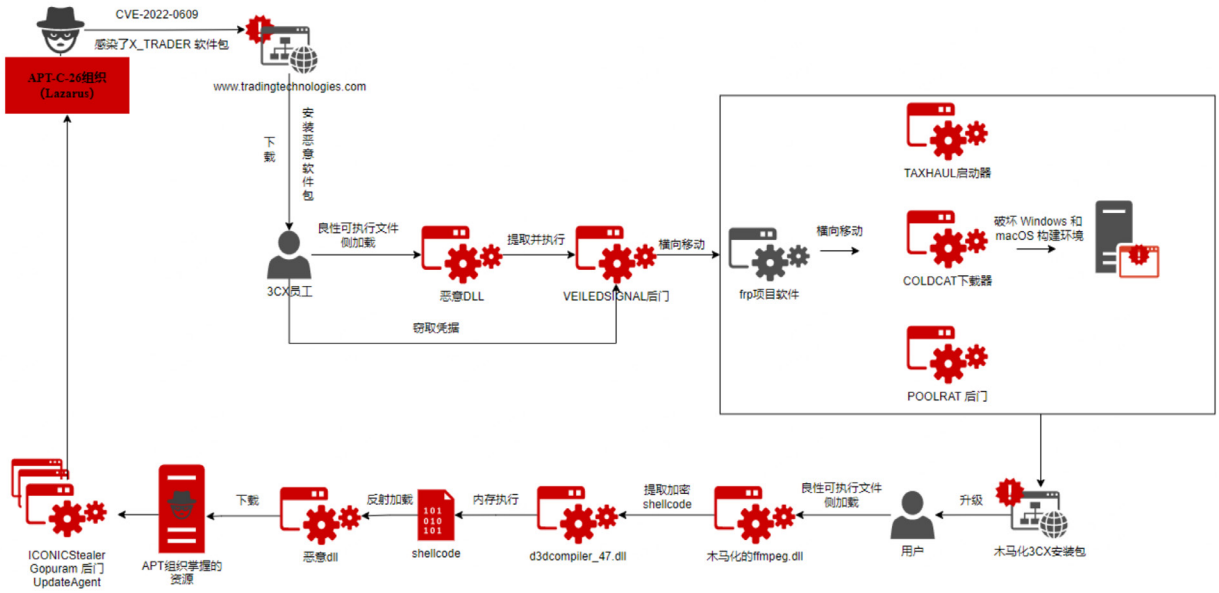




▶ DarkHotel组织利用某邮件系统0day攻击流程示意图

APT-C-26 (Lazarus)

2023年，APT-C-26 (Lazarus) 组织在全球范围内开展了一系列网络攻击。这些攻击活动涉及医学研究、技术部门到金融安全等多个领域，展示了其技术多样性和攻击手段的创新性。Lazarus组织还不断更新攻击手法，在攻击活动中不仅利用了Windows IIS Web服务器漏洞[6]，还通过伪装成安全更新安装程序分发恶意代码，甚至利用韩国金融安全解决方案漏洞展开攻击。



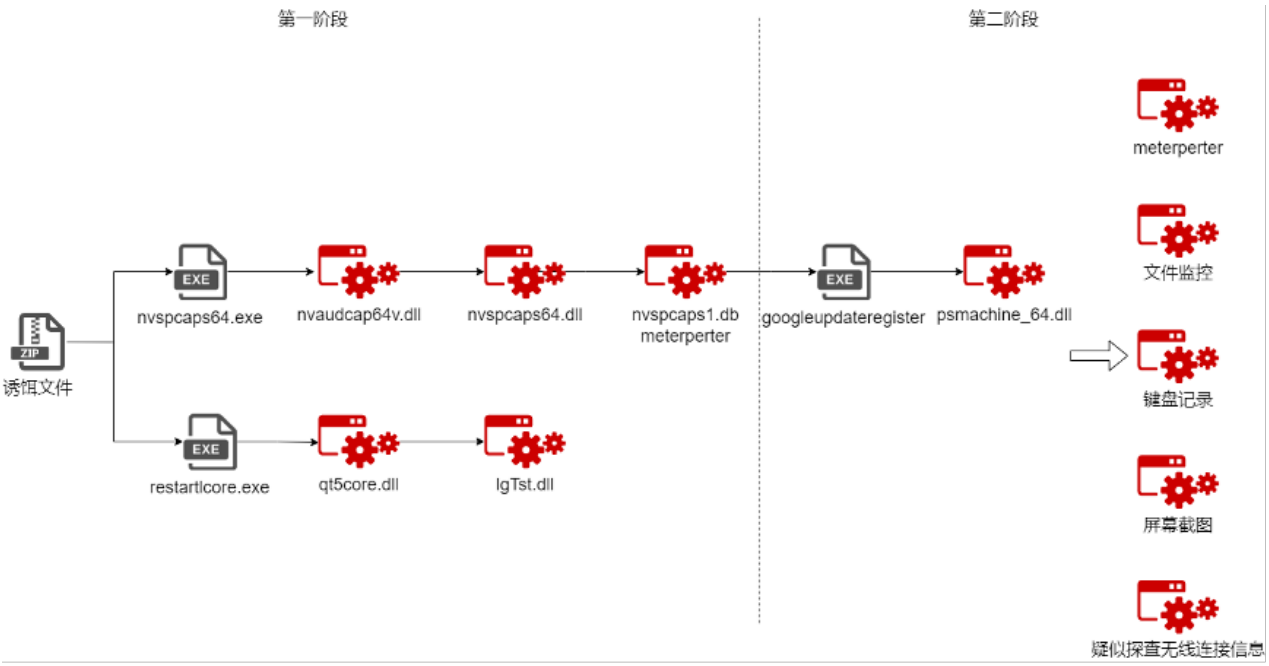
2023年3月，Lazarus组织发起了一场针对3CX桌面应用程序的供应链攻击。攻击者首先利用Chrome浏览器的远程代码执行漏洞CVE-2022-0609成功攻击目标网站，并感染X_TRADER软件包。接下来在Windows和macOS构建环境中部署了TAXHAUL启动器、COLDCAT下载器和POOLRAT后门。当用户进行3CX软件升级时，会下载3CX MSI Installer安装器，释放并执行3CX Desktop APP (3CXDesktopApp.exe)，完成下载和执行后门程序，从而构成完整攻击链。

▶ Lazarus组织3CX攻击流程图

APT-C-68 (寄生虫)

APT-C-68 (寄生虫) 组织是360高级威胁研究院在2023年最新捕获的活跃APT组织。现阶段寄生虫组织攻击活动主要影响我国国防军工、科研、教育等行业。其最早攻击活动可以追溯到2021年7月。

寄生虫组织在2023年攻击十分活跃，我们监测到该组织集中利用某行业软件0day漏洞攻击了我国科研、国防军工相关单位。该组织在另一起针对我国某军工背景企业展开攻击中，疑似利用chm文件作为诱饵文件进行恶意载荷投递，并通过某终端防护软件的漏洞来进一步部署恶意载荷。



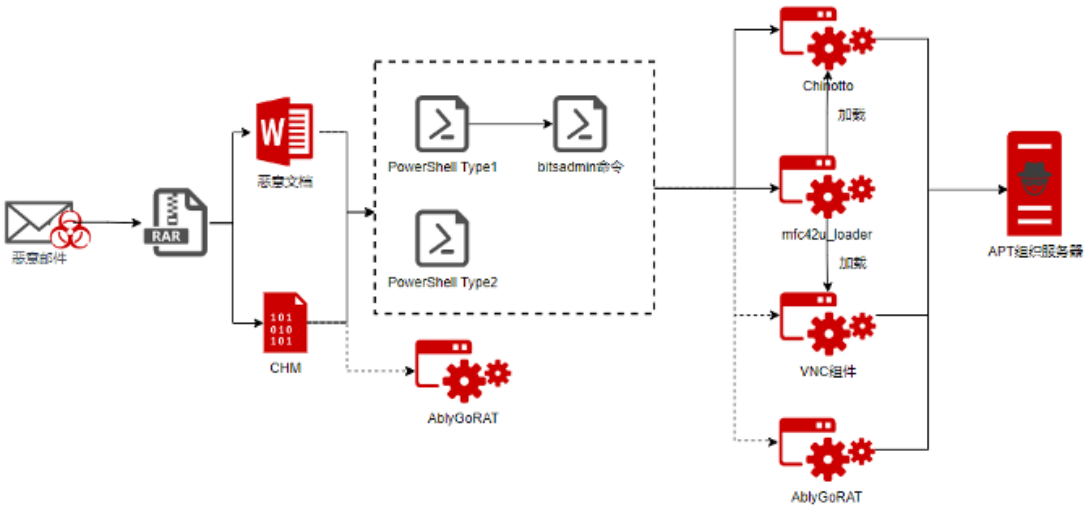
▶ 寄生虫组织现阶段攻击流程示意图

东亚·其他组织 | Advanced Persistent Threat

APT-C-28 (ScarCruft)

APT-C-28 (ScarCruft) 组织在2023年主要通过发送伪装成来自官方或信任机构的电子邮件和使用多样化的恶意软件发起攻击活动，邮件中通常包含HTML类型文件或CHM恶意软件，以窃取信息或破坏目标系统为主要目的。

360高级威胁研究院在上半年捕获到ScarCruft组织窃密攻击活动，该攻击活动至少从2022年11月开始。攻击者通过鱼叉式钓鱼邮件诱导用户执行附件内的诱饵文档或CHM恶意文件，加载远程C2上的PowerShell脚本，通过PowerShell脚本攻击者可以执行任意命令以及下发其他恶意载荷。我们对此次攻击活动相关信息进行整合，攻击流程总结如下。



▶ ScarCruft组织定向攻击活动流程图

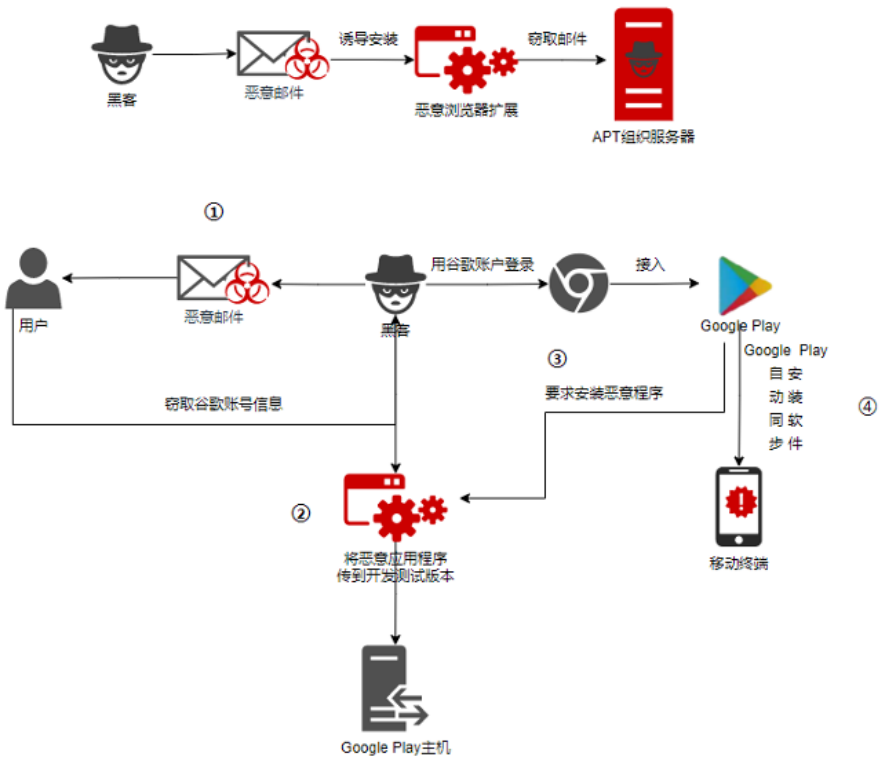
此外ScarCruft组织在2023年还在攻击活动中尝试通过伪装成重要国际意义材料、韩文图标APP以及知名域名服务器来针对韩国的MacOS用户发起钓鱼攻击；利用CVE_2023_38831漏洞针对加密货币领域发起攻击。

APT-C-55 (Kimsuky)

2023年，APT-C-55 (Kimsuky) 组织攻击活动呈现活跃态势。采用了多种攻击策略，展现了其多样化的攻击手段。这些活动包括伪装成金融和投资相关内容的恶意软件分发；通过模仿进口申报文件等形式，针对东北亚地区的研究机构实施攻击，并利用混淆的PowerShell脚本和后门文件进行信息窃取。同时Kimsuky组织在针对智库、学术界和媒体实施的定制化钓鱼攻击，使了与目标兴趣和当前事件相关的主题来提高攻击的成功率，体现了其在社会工程学方面的技战术水平。

Kimsuky组织在钓鱼攻击活动，巧妙利用各种诱饵文档型恶意软件，如“调查问卷”、“半岛相关问题”和“邀请函”等主题诱饵文档，通过执行额外的恶意宏来实现攻击。360高级威胁研究院监测发现，Kimsuky组织在攻击中，通过使用诱饵主题发送CHM类型文件和投递QuasarRat恶意软件，以窃取用户信息。

Kimsuky组织在2023年的攻击活动中，还启用了两种新的攻击模式：通过恶意浏览器扩展程序窃取谷歌邮件，以及利用Google Play同步功能向移动端同步恶意应用程序。这两种攻击模式，充分利用了谷歌的浏览器扩展程序和Google Play同步功能，使得攻击更加隐蔽和难以防范。

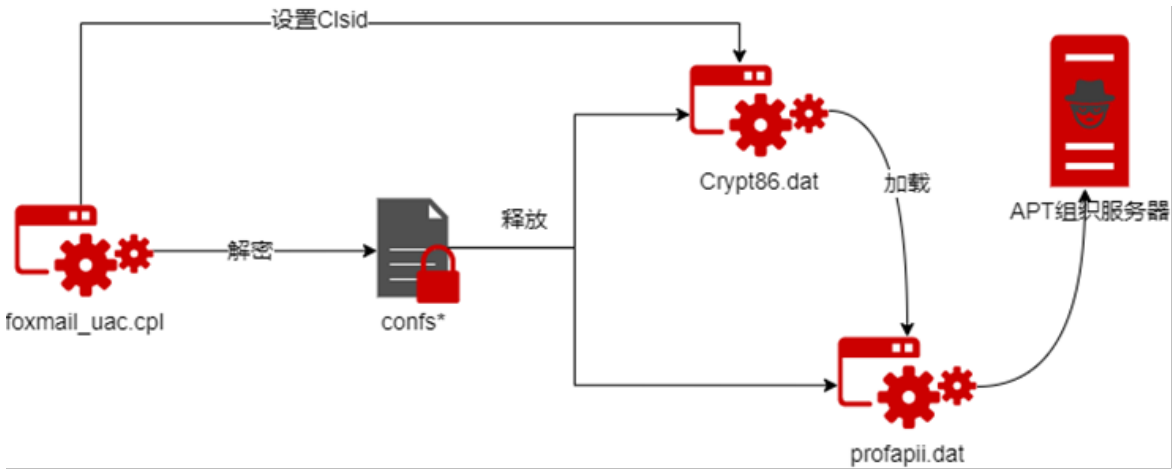


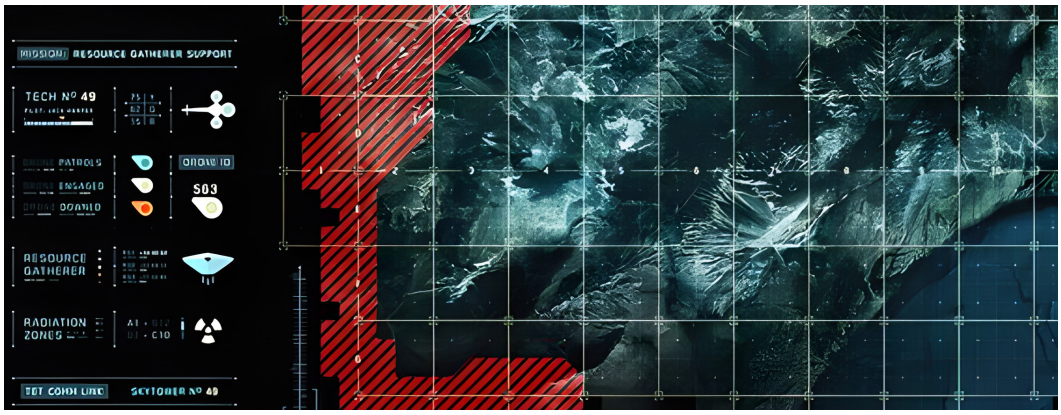
▶Kimsuky利用谷歌浏览器扩展程序和Google Play同步功能攻击流程图

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，该组织主要针对我国涉韩政府机构、贸易、文化交流相关单位展开攻击。

攻击者向受害用户foxmail邮箱发送“foxmail_uac.cpl”以及加密的恶意载荷文件文件。cpl文件是Windows中的控制面板项文件，在用户被诱导双击运行cpl文件后，该文件由系统应用程序control.exe加载执行，并解密恶意载荷文件，实现信息回传和远程控制。载荷执行流程如下图。





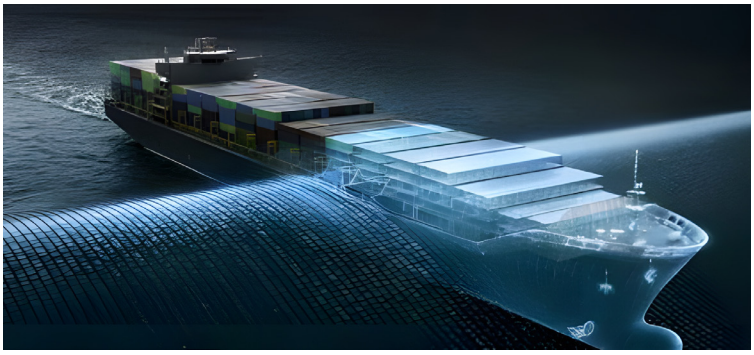
▶ 伪猎者组织载荷加载执行流程图

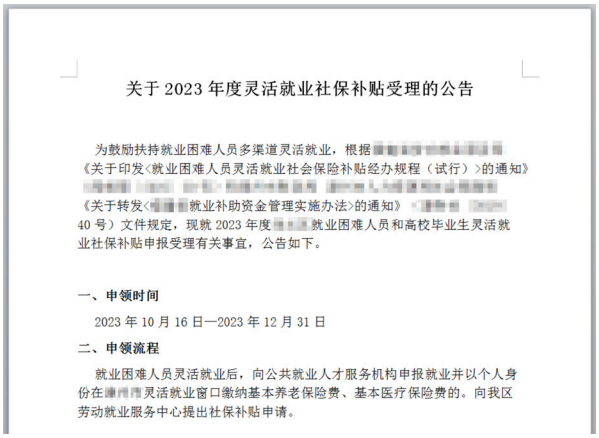
东南亚 | Advanced Persistent Threat

2023年，APT-C-00（海莲花）为东南亚地区主要活跃APT组织。海莲花组织长期以来针对我国重点行业领域进行渗透攻击。我国受其攻击活动影响较为严重的是政府、教育、科研、国防军工、能源、信息技术等行业领域。

APT-C-00（海莲花）

APT-C-00（海莲花）组织在2023年重新启用了鱼叉式钓鱼的攻击手段，攻击成功后对高价值目标进行内网横移。通过对海莲花组织攻击活动的追踪和监测，我们发现该组织会利用以往攻击获取到的情报信息，针对下一轮攻击目标构造诱饵文档或钓鱼邮件，以此来增加成功率。此外，海莲花在攻击流程中也做了部分改进，例如：与安全软件对抗方面，在攻击活动中检测到自身攻击被拦截时，会立即删除其木马组件；在持久化方面，海莲花会将白文件的Lnk快捷方式投递到开始菜单的开机自启动目录中，以保持对目标主机的长久控制。





关于 2023 年度灵活就业社保补贴受理的公告

为鼓励扶持就业困难人员多渠道灵活就业，根据[redacted]《关于印发〈就业困难人员灵活就业社会保险补贴经办规程（试行）〉的通知》[redacted]《关于转发〈[redacted]就业补助资金管理实施办法〉的通知》[redacted]40 号）文件规定，现就 2023 年度[redacted]就业困难人员和高校毕业生灵活就业社保补贴申报受理有关事宜，公告如下。

一、申领时间

2023 年 10 月 16 日—2023 年 12 月 31 日

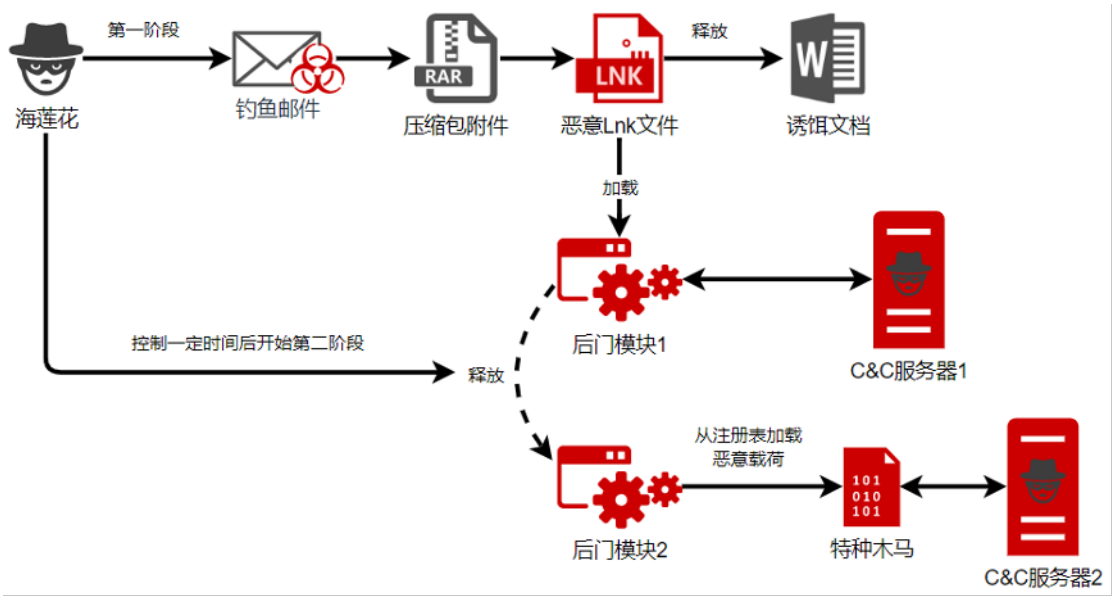
二、申领流程

就业困难人员灵活就业后，向公共就业人才服务机构申报就业并以个人身份在[redacted]灵活就业窗口缴纳基本养老保险费、基本医疗保险费的。向我区劳动就业服务中心提出社保补贴申请。

▶ 海莲花组织投放的诱饵文档

2023年年初，360捕获到海莲花组织利用国内某安全厂商防火墙0day漏洞，对部署该品牌防火墙的高价值目标进行了渗透攻击。同时使用了一种采用多种通信协议进行数据加密传输的新型Linux特种木马，增加了目标与C&C服务器之间通信的隐蔽性和灵活性，使得攻击更加难以追踪。另外2023年下半年，海莲花组织使用漏洞攻击了国内多款OA系统的服务器，显示该组织在漏洞挖掘方面的能力以及目标多平台化的野心。

值得重点关注的是，360高级威胁研究院通过对海莲花组织攻击活动的持续跟踪和监测发现，该组织在2023年几乎完全抛弃了先前的网络资产和近三年使用的后门模块，同时还采用“假旗行动”的策略，旨在干扰和误导安全人员对攻击归属的判断，以进一步掩盖其真实身份，假旗行动模仿对象以东欧地区的APT组织为主[7]。



▶ 海莲花组织攻击活动中两个攻击阶段示意图

东欧 | Advanced Persistent Threat

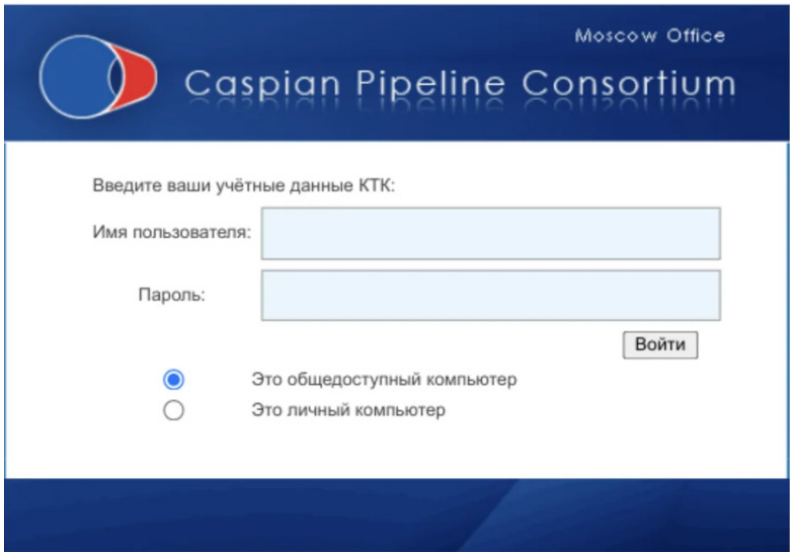
2023年俄乌地区冲突进入相持阶段，东欧地区APT组织在网络空间的对抗依旧热度不减。具有东欧背景的APT-C-13 (Sandworm) 、APT-C-20 (APT28) 和APT-C-25 (APT29) 等组织在2023年将乌克兰的政府、军事设施和关键基础设施作为主要攻击目标，进行了一系列精心策划的网络攻击。

APT-C-13 (Sandworm)

APT-C-13 (Sandworm) 组织在2023年聚焦俄乌冲突，利用凭证钓鱼、恶意软件和外部服务等多种手法展开攻击活动。攻击目标瞄准政府、国防、能源等关键领域，以广泛的信息情报收集以及大规模的数据泄露为目的。

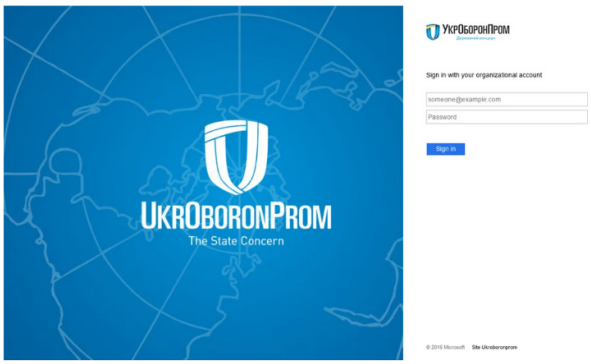
Sandworm组织通过持续利用EXIM邮件服务器漏洞展开攻击活动，并将被入侵的主机整合进其网络中。被控主机已被确认用于访问受害者网络、与受害者账号互动、发送恶意电子邮件等。

2023年第一季度，Sandworm组织针对里海油管联合公司 (CPC) 及其他欧洲能源行业组织展开攻击活动[8]。攻击者通过发送假Windows更新包链接等方式，试图使用Rhadamanthys恶意软件窃取相关机构的凭证和信息。



▶ Sandworm组织仿冒能源组织CPC的钓鱼网站

Sandworm组织针对乌克兰国防军工及Ukr.net网络邮件用户发起的大规模钓鱼攻击[9]，使用的钓鱼邮件大多伪装成系统管理员通知，试图窃取受害者登录凭证。



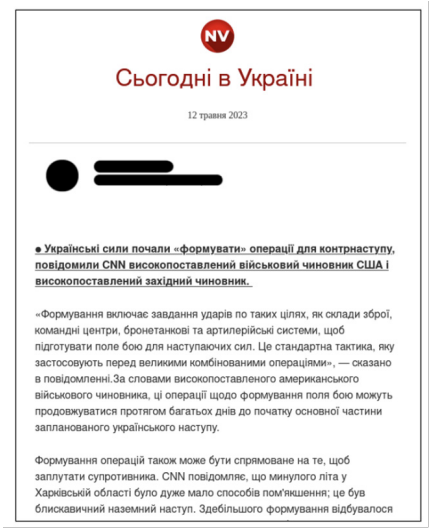
国外网络安全机构披露，Sandworm组织在2022年10月对乌克兰一处能源设施发动复杂的攻击[10]，导致电力中断，随后乌克兰各地的关键基础设施遭到广泛的导弹袭击。此次攻击是罕见的破坏目标物理设施运行的网络攻击事例，也是自俄乌冲突以来第一起已知的因网络攻击导致断电的公开案例，还是首次与导弹袭击同时发生的此类网络攻击事件。此次攻击事件显示了该组织APT组织攻击能力的最新演变。

APT-C-20 (APT28)

在2023年，APT-C-20 (APT28) 组织主要针对乌克兰相关实体发起以钓鱼攻击为主的攻击活动。2023年4月期间，乌克兰CERT捕获到一系列伪装成“Windows更新”通知，针对乌克兰政府的电子邮件钓鱼攻击[11]。

2023年5月，APT28组织针对乌克兰政府发起了一起精心策划的攻击活动[12]。攻击者首先从乌克兰媒体获取新闻报道，在新闻报道最初发布的几小时内制作成诱饵，并转化为有效的攻击工具，随后利用一系列漏洞成功下发侦查和窃密脚本，进一步加深对目标的渗透。这一行动揭示了APT28组织技战术的高度专业化。

▶ 钓鱼网站冒充乌克兰国防公司Ukroboronprom



Сьогодні в Україні

12 травня 2023

[redacted]

● Українські сили почали «формувати» операції для контрнаступу, повідомили CNN високопоставлений військовий чиновник США і високопоставлений західний чиновник.

«Формування включає завдання ударів по таких цілях, як склади зброї, командні центри, бронетанкові та артилерійські системи, щоб підготувати поле бою для наступаючих сил. Це стандартна тактика, яку застосовують перед великими комбінованими операціями», — сказано в повідомленні.За словами високопоставленого американського військового чиновника, ці операції щодо формування поля бою можуть продовжуватися протягом багатьох днів до початку основної частини запланованого українського наступу.

Формування операцій також може бути спрямоване на те, щоб заплутати супротивника. CNN повідомляє, що минулого літа у Харківській області було дуже мало способів пом'якшення; це був блискавичний наземний наступ. Здебільшого формування відбувалося

图1

Разумков
центр

№ 33/(1-7)
04.08.2023

Dear colleagues!

We invite you to take part in the expert discussion **"War of Attrition: Comparison of Potentials and Assessment of Prospects"**, which will be held on **August 9, 2023** in online and offline formats.

Questions for discussion:
- Intermediate results and prospects for the further course of the Russian-Ukrainian war.
- Assessment of existing potentials and forecasts of their changes.
- How to avoid a "stalemate" under conditions of approximate parity of combat potentials.

Representatives of government, civil society, scientific institutions, and donor organizations are invited to participate in the event.

The discussion will be held on the basis of the Zoom platform of the Razumkov Centre from 12:00 to 1:30 p.m. Working languages: **Ukrainian, English.**

Connection of participants - from 11:45. **Pre-registration of participants via the link:** https://us06web.zoom.us/meeting/register/tZ0vduGupzkoEtQGzp6AADIObMgYJJUQepiU#/registration

The live broadcast of the event will be carried out on the YouTube channel of the Razumkov Centre as part of its project implemented under the USAID/ENGAGE activity, which is funded by the United States Agency for International Development (USAID) and implemented by Pact. The contents of this event are the sole responsibility of Pact and its implementing partners and do not necessary reflect the views of USAID or the United States Government.

Analytical materials which will be presented during the discussion have been made within the frameworks of the MATRA Programme supported by the Embassy of the Kingdom of the Netherlands in Ukraine.

Best regards,

President of the Razumkov Centre **Yuriy Yakymenko**

图2

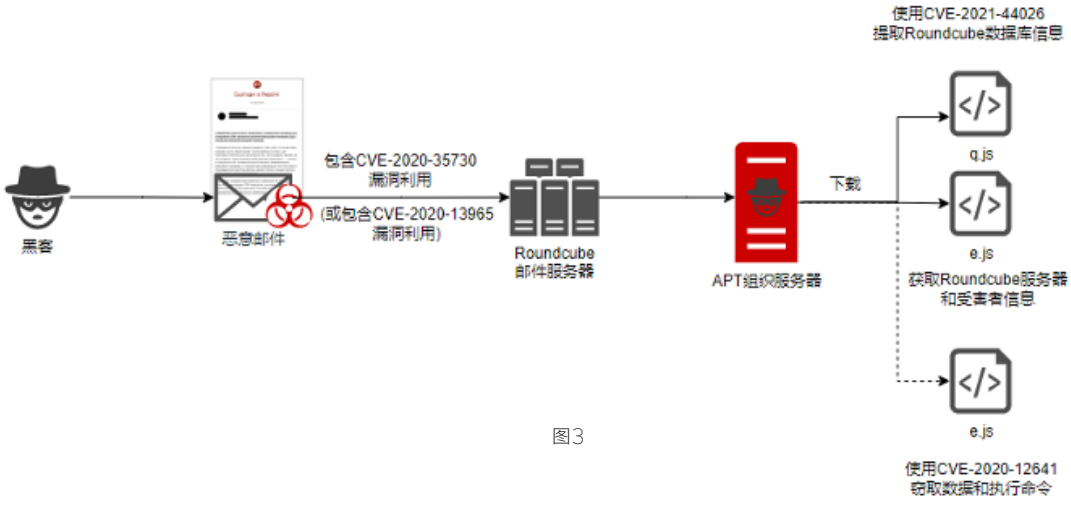


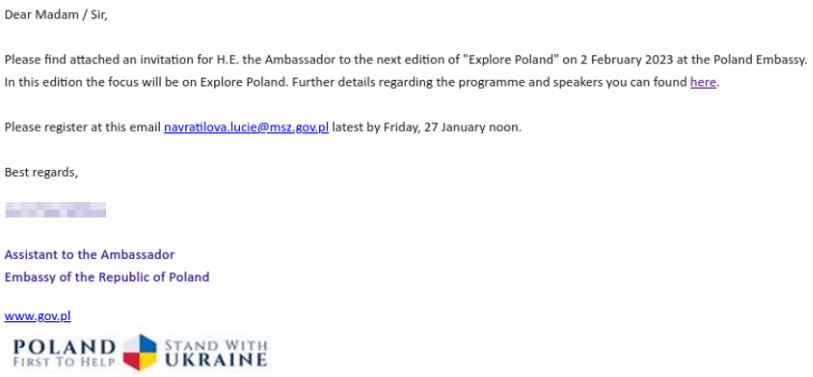
图3

在2023年下半年，APT28组织精心策划了一系列针对乌克兰关键能源基础设施的网络攻击。攻击者通过伪装成正规邮件，巧妙地利用Microsoft Edge浏览器的“无头”模式 (headless mode) 来隐蔽地创建和执行CMD文件，除此之外，还运用PowerShell脚本来获取账户的密码哈希值，增强其在网络空间的控制力。

▶ 图1 APT28组织利用新闻报道制作的诱饵文档 ▶ 图2诱饵文件冒充乌克兰公共政策智囊团 ▶ 图3 APT28组织攻击流程图

APT-C-25 (APT29)

APT-C-25 (APT29) 组织2023年显示出更高的活跃度和更强的威胁性，在攻击活动中不断投入使用新的攻击组件：如SnowyAmber、Halfrig和Quarterrig，以及新的C2通信方式[13]。


Dear Madam / Sir,

Please find attached an invitation for H.E. the Ambassador to the next edition of "Explore Poland" on 2 February 2023 at the Poland Embassy.
In this edition the focus will be on Explore Poland. Further details regarding the programme and speakers you can found here.

Please register at this email navratilova.lucie@msz.gov.pl latest by Friday, 27 January noon.

Best regards,

Assistant to the Ambassador
Embassy of the Republic of Poland

www.gov.pl

POLAND FIRST TO HELP STAND WITH UKRAINE

图1

SnowyAmber恶意攻击组件，也被称为GraphicalNeutrino，最早在2022年10月被观察到作为加载器使用，它同时具有基本的C2功能，并实现了多种反分析技术，包括API解钩、动态解析API、字符串加密和沙箱逃逸。Halfrig组件在2023年2月首次被观察到充当加载器来启动其中包含的Cobalt Strike后门工具包。Quarterrig于2023年3月首次被捕获，它与Halfrig共享部分代码，充当下载器，投递下一阶段攻击载荷。

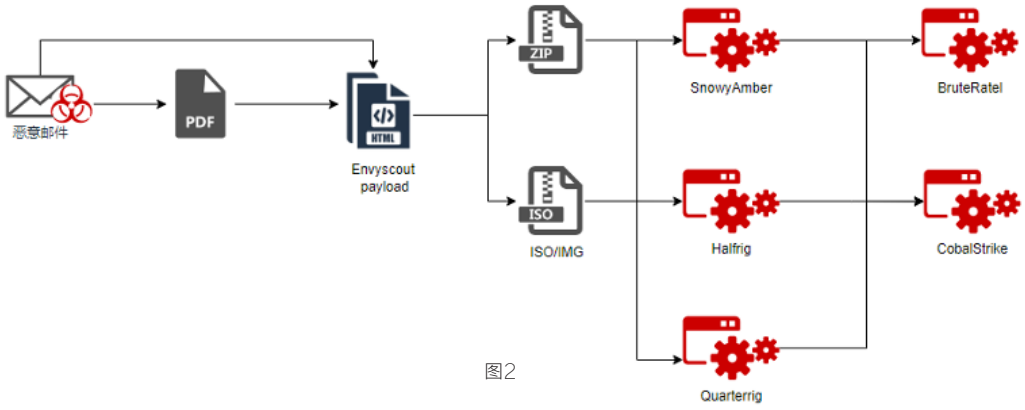


图2

在2023年下半年，APT29组织展现了其在全球范围内进行网络攻击的能力，特别是利用了JetBrains TeamCity的CVE-2023-42793漏洞，展开一系列包括权限提升、横向移动、部署额外的后门的网络活动。APT29组织还使用CVE-2023-38831漏洞发起针对大使馆机构的网络攻击渗透，攻击目标分布于多个欧洲国家。APT29组织的网络行动呈现出高度专业化和精细化特征。

▶图1 APT29组织冒充波兰大使馆的恶意电子邮件　▶ 图2 APT29组织攻击流程图

APT-C-53 (Gamaredon)

2023年，APT-C-53 (Gamaredon) 组织延续了2022年的活跃势头，除乌克兰政府相关目标外，还加强了针对对乌克兰军事和安全组织目标的攻击。Gamaredon组织具备专业化的自动化鱼叉式网络钓鱼攻击技术。依靠其精心设计的乌克兰政府组织官方文件诱饵和高度定制化的武器文件分发，来提高钓鱼攻击的成功率。

2023年，Gamaredon组织进行社会工程攻击时使用了多种诱饵主题。诱饵涵盖了包括检察官、军事服役、培训请愿、法律诉讼等广泛领域。这种多样化的诱饵策略表明，Gamaredon集团在社会工程方面具有高度的灵活性和创新能力，通过各种话题吸引不同目标群体，以此来实现其网络攻击目的。

在网络基础设施方面，Gamaredon组织依赖于多阶段的Telegram账号进行攻击目标分析和地理位置确认，然后引导被攻击目标连接到下一阶段服务器，以完成最终恶意载荷传递[14]。每个Telegram账户都会定期部署新的IP地址，同时采用多样化的C2获取方式，增加其攻击的复杂性和隐蔽性。

2023年1月，360高级威胁研究院捕获到Gamaredon组织在攻击活动中投放的vbs dropper样本。该样本在代码中掺入大量无用逻辑，伪装成普通程序，而恶意逻辑隐藏在大量垃圾代码中。vbs dropper样本功能为释放并执行vbs脚本。

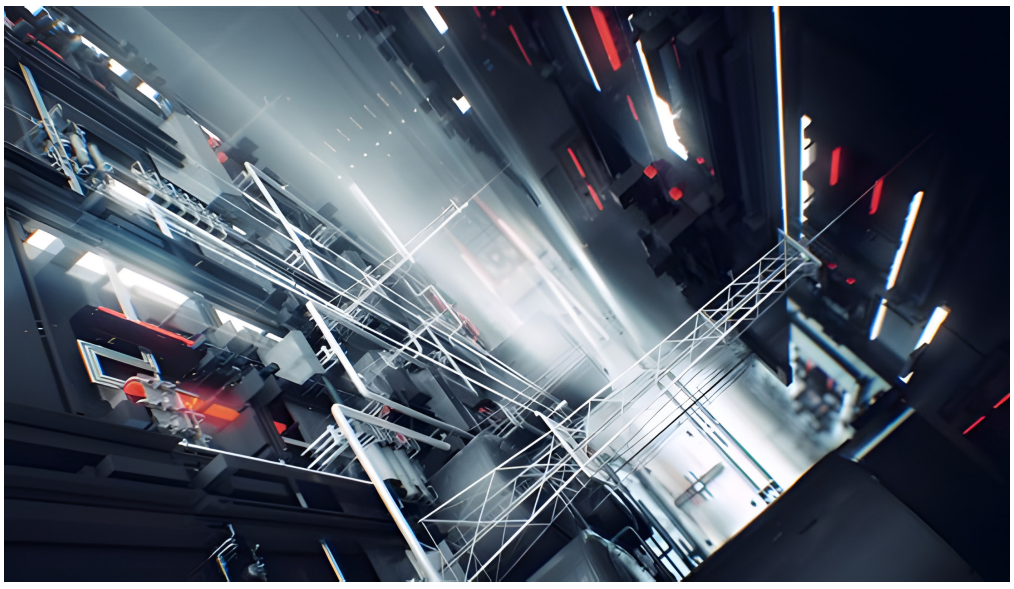
中东 | Advanced Persistent Threat

除上述地域范围外，2023年在巴以冲突矛盾升级的推波助澜下，中东地区地区的网络空间对抗活动热度也呈现爆发式增长，疑似拥有中东地区国家背景的APT组织，如APT-C-23（双尾蝎）、APT-C-51（APT35）等，针对冲突相关的政府、企业等攻击活跃度较往年明显增加。这期间也不乏一些全新APT组织的身影。与俄乌冲突相似，此次巴以冲突期间的网络攻击活动，也出现了数据擦除器攻击，恶意软件不仅会破坏文件，甚至破坏整个操作系统。

APT-C-23（双尾蝎）

APT-C-23（双尾蝎）组织同时具备Windows与Android双平台的攻击能力。通常使用鱼叉式钓鱼邮件和虚假社交媒体资料诱导用户安装恶意软件作为攻击手段。

2023年，APT-C-23（双尾蝎）组织被披露，使用更新后的工具集攻击巴基斯坦、埃及、土耳其等中东国家的政府、军事、金融、媒体、教育等目标，并按不同目标部门进行后门程序投放和指定文件类型窃取。同时在Android平台方向，我们监测发现双尾蝎组织伪造OPlayer以及Align It平台钓鱼网站，投放经重打包处理后的后门APK程序进行攻击。



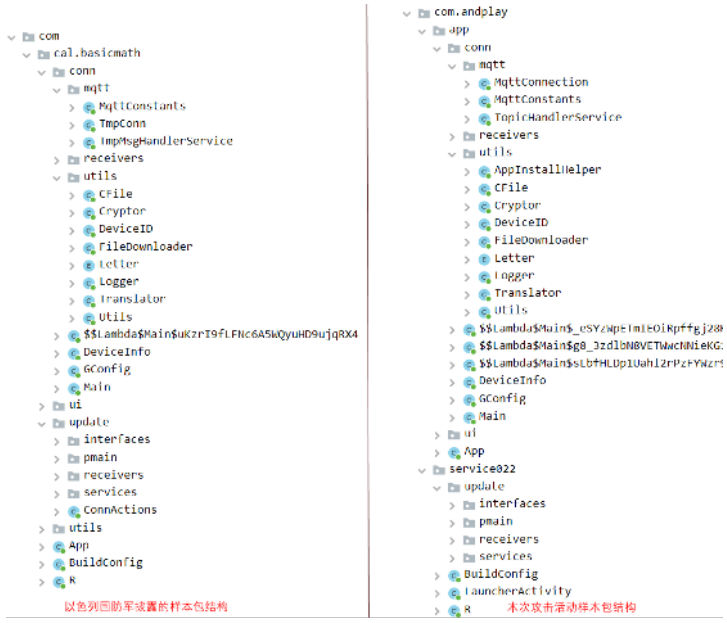


图1

2023年下半年，双尾蝎组织被披露将间谍软件伪装成非恶意Android应用更新程序针对阿拉伯语用户进行信息窃取[15]。11月，双尾蝎组织BARBWIRE后门木马持续活跃，BARBWIRE后门被伪装成Windows默认照片查看器程序 (ImagingDevices.exe) 向中东地区航空行业投递。

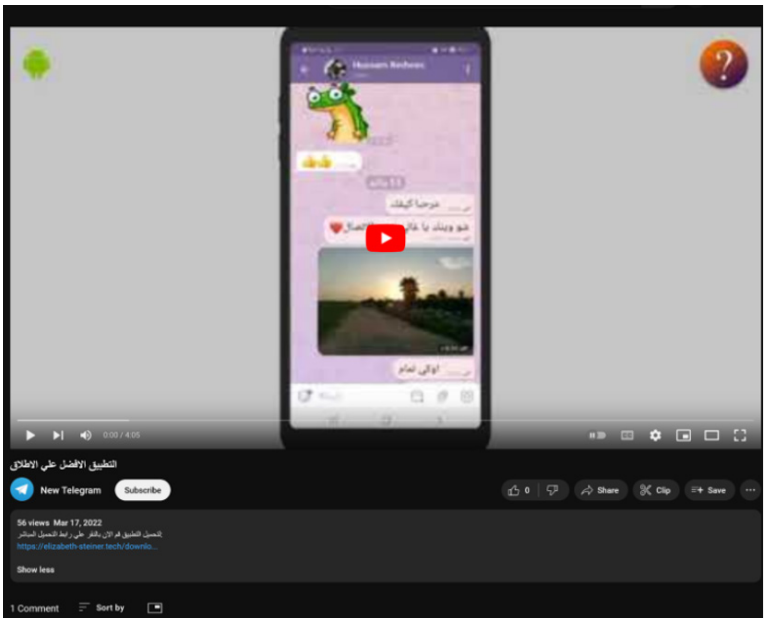
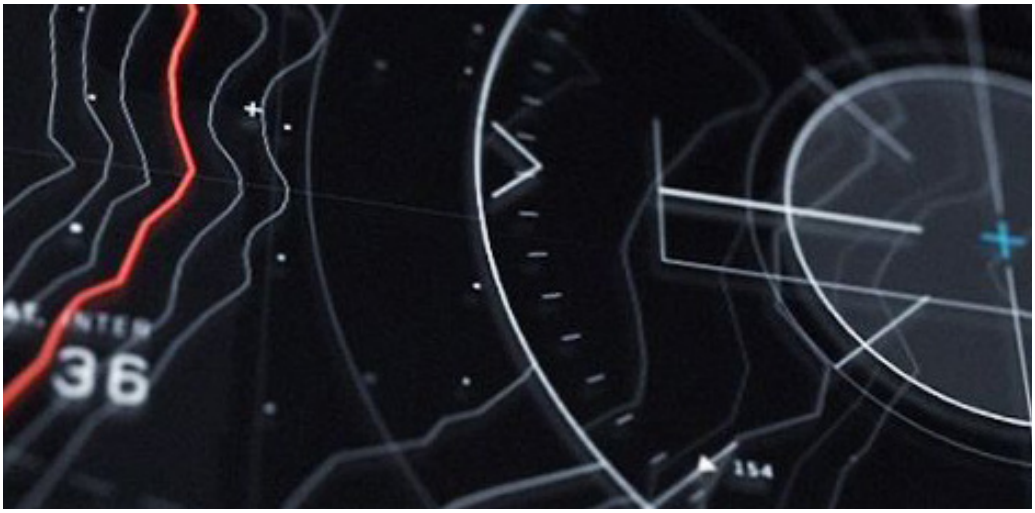


图2

▶ 图1 双尾蝎组织重打包APK资源对比 ▶ 图2在YouTube视频评论区下投放BARBWIRE后门木马下载链接



APT-C-49 (OilRig)

中东地区APT组织APT-C-49 (OilRig)，一直以来主要针对该地区的金融，政府，能源，化工和电信等行业领域展开攻击活动。

OilRig组织被曝在2023年2月至9月期间对中东地区政府机构进行了长达8个月的入侵。攻击者通过投递一个PowerShell后门 (PowerExchange) 用于窃取文件和密码。后门恶意软件通过受感染的邮箱帐户将被盗数据从内部邮箱发送到攻击者控制的外部邮件帐户。

APT-C-51 (APT35)

APT-C-51 (APT35) 组织又称CharmingKitten，通常以美国和中东地区的军事、政府、媒体组织、能源、电信服务等作为攻击目标。

2023年巴以冲突爆发后，APT35组织被曝使用新型Sponsor后门针对以色列用户开展攻击活动。Sponsor后门程序运行后，会收集计算机的敏感信息上传至攻击者服务器。

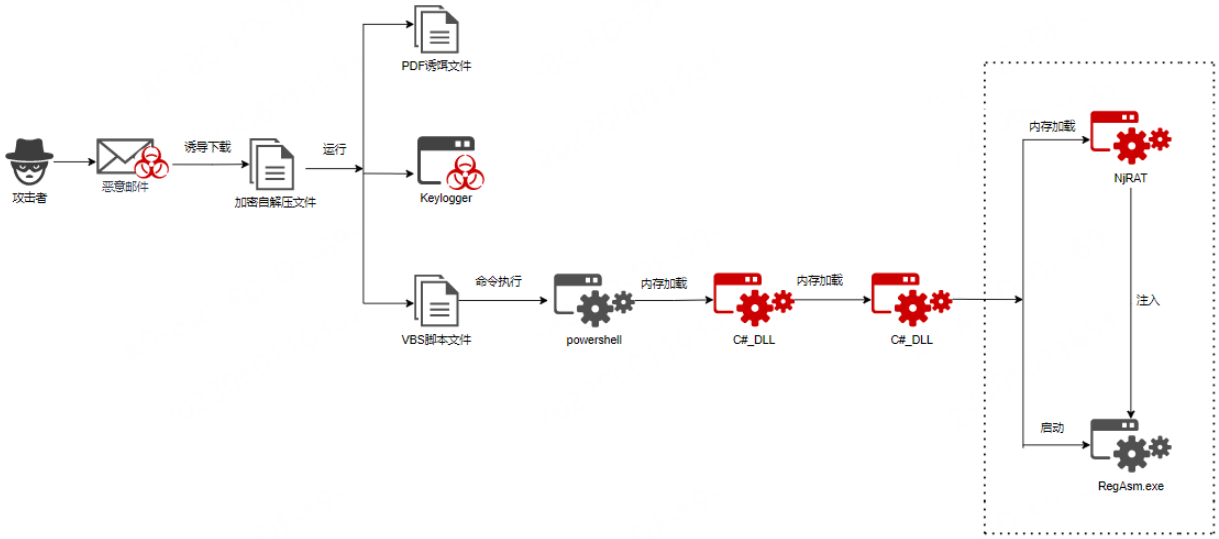
▶ BARBWIRE攻击流程图

南美 | Advanced Persistent Threat

APT-C-36 (盲眼鹰)

APT-C-36 (盲眼鹰) 组织主要针对哥伦比亚等南美地区政府机构，金融、保险等行业以及大型公司展开定向攻击。其惯用攻击手段为利用钓鱼邮件传播携带可下载恶意压缩包链接的PDF文件，对恶意载荷做加密压缩，诱导用户使用PDF文件中携带的密码解压并运行。

在2023年对盲眼鹰组织组织的监测中，我们发现该组织对原先使用的鱼叉钓鱼邮件投递手法进行了扩展，尝试使用teams投递、恶意文档投递和渗透攻击命令展开攻击活动。



▶ 盲眼鹰组织近期攻击流程

PART 03

关键行业攻击态势分析

PART.03

关键行业攻击态势分析

Advanced Persistent Threat

2023年全球网络安全机构披露的APT攻击活动中，政府、国防军工、信息技术、外交、教育等为主要受攻击影响行业。根据360全网安全大脑监测，我国受APT攻击影响单位，主要分布于教育、政府、科研、国防军工以及交通运输等行业。其中按职能看，政府机构下的海事机构、驻外机构、金融监管以及交通管理等是受APT攻击影响的重点。

政府机构历年来一直是APT攻击的核心目标领域，而受攻击的政府机构，其职能基本都涉及关键行业，后续会根据具体行业进行重点分析。

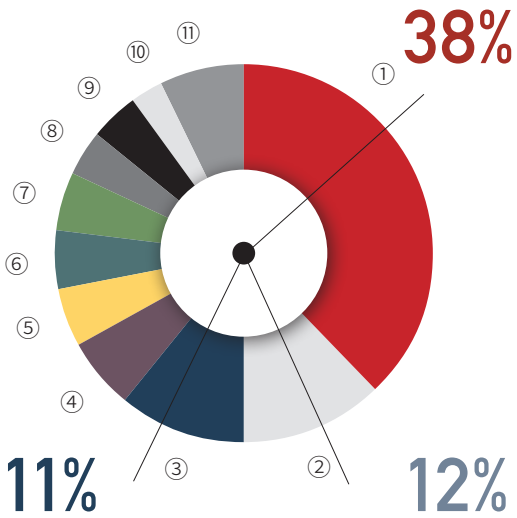


图1

①政府	38%	⑦制造	5%
②国防军工	12%	⑧能源	4%
③信息技术	11%	⑨文娱传媒	4%
④教育	6%	⑩交通运输	3%
⑤金融	5%	⑪其他行业	7%
⑥科研	5%		

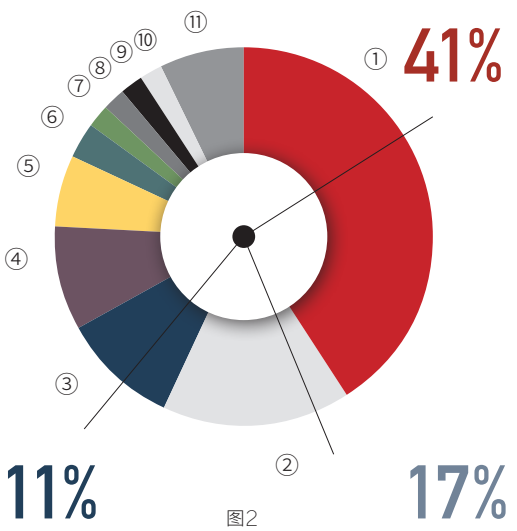


图2

①教育	41%	⑦自然资源	2%
②政府	16%	⑧贸易	2%
③科研	10%	⑨建筑地产	2%
④国防军工	9%	⑩能源	2%
⑤交通运输	5%	⑪其他行业	7%
⑥制造	3%		

▶ 图1 全球APT攻击影响TOP10行业分布　　▶ 图2 我国受APT攻击影响TOP10行业分布

1.教育和科研

在周边复杂地缘政治环境等多重因素影响下，2023年上半年，境外APT组织针对我国国防军工领域攻击非常活跃。尤其以南亚和东南亚地区的APT-C-48（CNC）、APT-C-08（蔓灵花）、APT-C-00（海莲花）等组织攻击活动最为频繁。

▶ 教育和科研是APT攻防对抗的核心战场

360全网安全大脑监测，2023年，对我国展开攻击活动的APT组织，攻击目标大都涉及我国教育和科研领域，我国受APT攻击影响单位中，教育科研行业占比超过50%。教育和科研单位作为APT攻击的重灾区，逐渐成为我国与境外APT组织攻防对抗的核心战场。

例如：APT-C-48（CNC）组织针对我国的攻击活动，目标集中分布在教育科研领域，其中受其攻击影响的高等院校，大部分具有国防军工背景；APT-C-09（摩诃草）组织从2023年2月开始，陆续以“某集团招聘计划”、“国际科学家研究基金”等主题，针对我国多个高校、科研机构发起多轮针对性攻击，受攻击目标包含我国多所重点高等院校。

▶ 利用前期攻击成果实施精准攻击活动频发

360高级威胁研究院通过分析APT组织针对教育科研领域的攻击活动发现：部分攻击活动中，攻击者出现利用已攻陷的资源，如使用窃取的文档数据、联系人信息等，实施对目标的进一步精准攻击，以扩大攻击成果。

攻击者在第一阶攻击活动中，针对目标行业领域投递诱饵文档，展开广泛钓鱼攻击，以窃取目标用户的邮箱账号密码、联系人以及其他敏感数据；在第二阶段，攻击者使用窃取的邮箱账号冒充受害者身份，向其他目标发送钓鱼邮件，并针对性的将窃取的目标环境中的内部文件制作成诱饵文档，通过一系列社工手段，降低了目标用户的防备，极大地提高了第二阶段攻击的成功率。

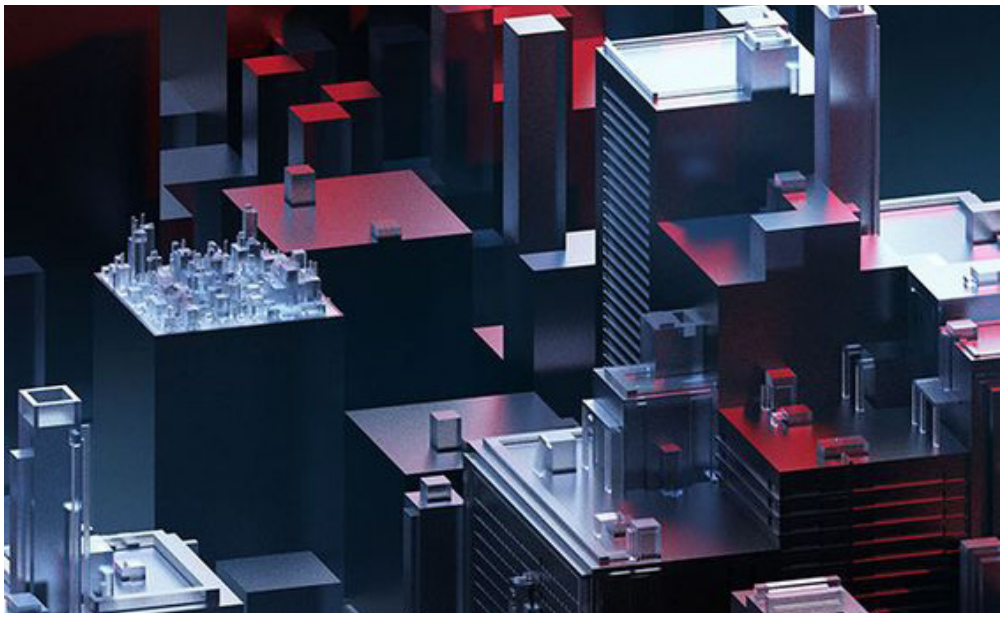
360高级威胁研究院通过研判分析南亚、东南亚等多个方向组织，如APT-C-09（摩诃草）、APT-C-00（海莲花）等，已在近期攻击活动运用了此类攻击手法。此攻击手法体现出APT组织针对特定人群攻击时，合理利用网情和社会工学的思路。这也提醒我国各重点关基行业单位提高网络安全意识，增强对此类攻击威胁的防范。

2.政府机构

▶ 针对我国驻外机构、驻外企业的攻击活跃度明显上升

“一带一路”是我国提出的重大国际合作倡议，旨在加强沿线国家的经济、科技合作以及互联互通。2023年是“一带一路”倡议提出10周年。10年来，共建“一带一路”倡议成果丰硕，成为极具影响力的国际合作平台。中国国际影响力也在逐渐提升，不断走近世界舞台中央。

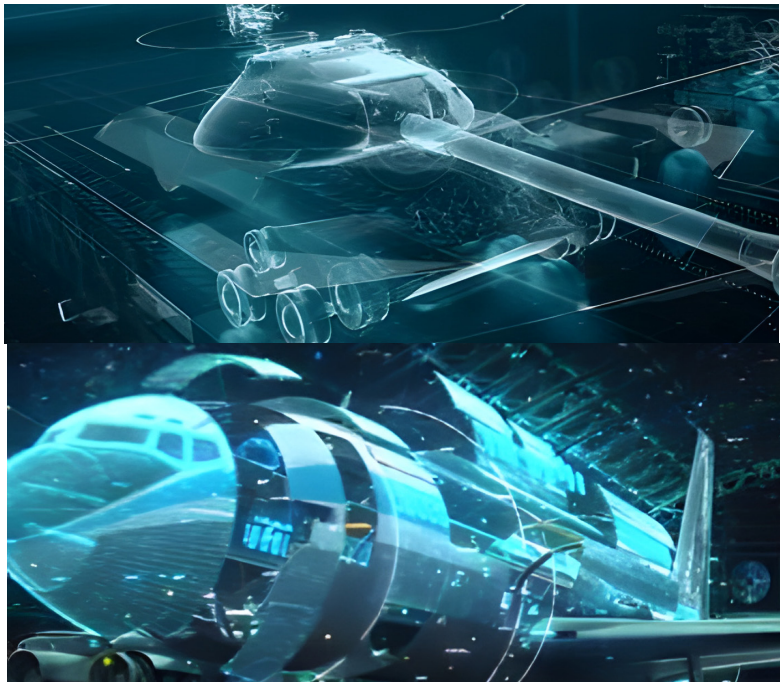
我们通过监测发现，2023年南亚、朝鲜半岛、中东地区的APT组织针对我国驻外机构、驻外企业攻击活跃，进一步重点涉及其中的科技、商务合作机构。这些组织尤其关注其所属国家周边地区的驻外机构。



我国外事和驻外机构是我国对外推行政治、经济、科技等领域合作的前站。随着我国国际影响力的不断提升，外事和驻外机构所掌握的政治、经济贸易来往数据，以及我国对外政策方针，直接关系到各国与中国的核心利益。外事和驻外机构势必成为有地缘政治背景支持的APT组织的重点攻击目标。这需要我国外事相关机构引起足够重视，防范来自APT组织的针对性渗透攻击。

3.国防军工

在周边复杂地缘政治环境等多重因素影响下，境外APT组织对我国国防军工领域攻击活动非常活跃。根据360高级威胁研究院监测，2023年针对我国国防军工领域的攻击活动，主要来源于南亚地区的APT组织：APT-C-48（CNC）、APT-C-08（蔓灵花）等，其次为来自东南亚地区的APT-C-00（海莲花）以及东亚地区的APT-C-01（毒云藤）和APT-C-06（DarkHotel）。



▶ 具有国家国防科工背景的教育、科研单位是APT组织重点目标

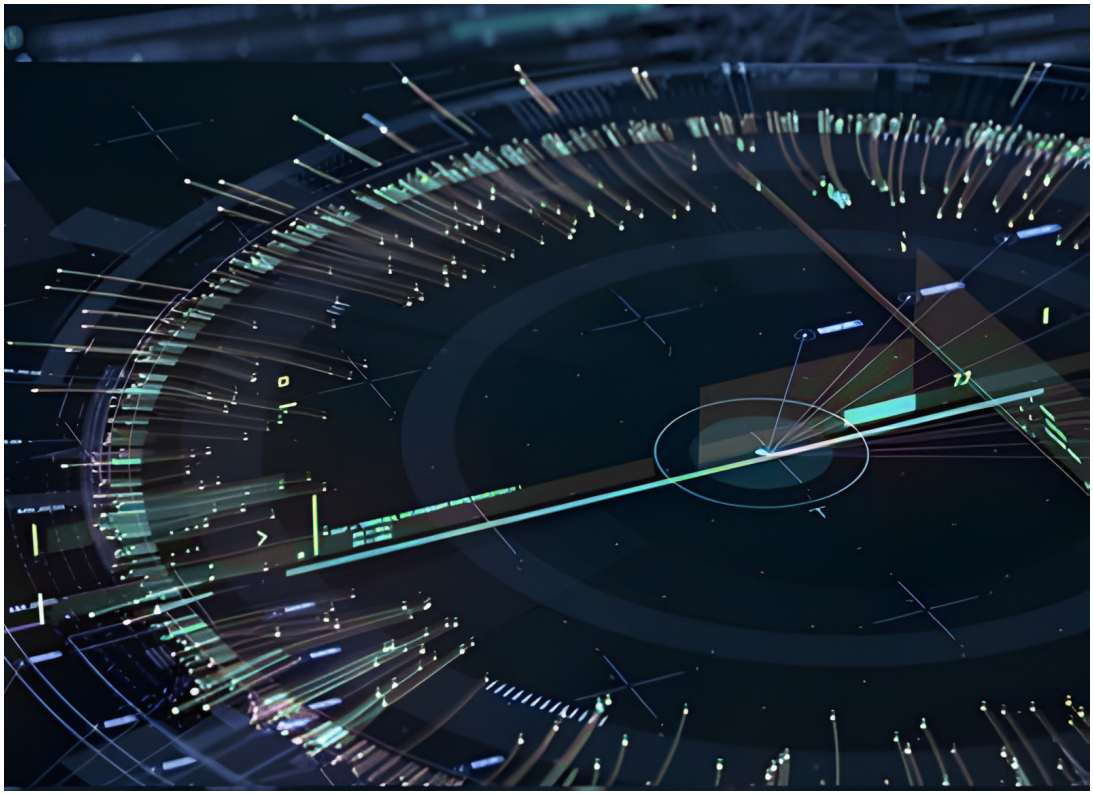
国家国防科工背景的教育、科研单位，在我国基础前沿科技研究和国防科技创新体系中发挥着生力军作用，肩负强军和富国的双重使命。2023年上半年，APT组织针对我国国防军工领域展开的攻击活动中，具有国家国防科工背景教育、科研单位成为APT组织重点攻击目标。

APT组织针对我国国防科工背景高等教育和科研单位展开的攻击活动，是以此作为突破口，真正目的是我国国防军工的科技创新体系。此种攻击策略代表组织为来自南亚地区的APT-C-48（CNC）、APT-C-09（摩诃草）等。而南亚的APT-C-00（海莲花）和APT-C-08（蔓灵花）组织，则主要针对我国航空航天和驻外涉及军工相关目标展开攻击。

▶ APT组织以窃取军事情报等方式介入地区军事冲突

2023年随着俄乌地区冲突的持续发展，催生了不同势力通过提供后勤、情报等方式介入地区军事冲突的方式，而APT组织在网络空间的情报窃取方面的能力优势有了用武之地。

国外安全机构披露，东欧地区APT组织APT-C-53 (Gamaredon) 在上半年针对而俄乌冲突中的安全部门、军队和政府组织发起多次网络攻击，试图访问和窃取敏感信息，例如军队伤亡人数、敌方作战和空袭计划、军火库库存、军事训练等情报信息，以定向窃取军事情报的方式介入地区军事冲突。



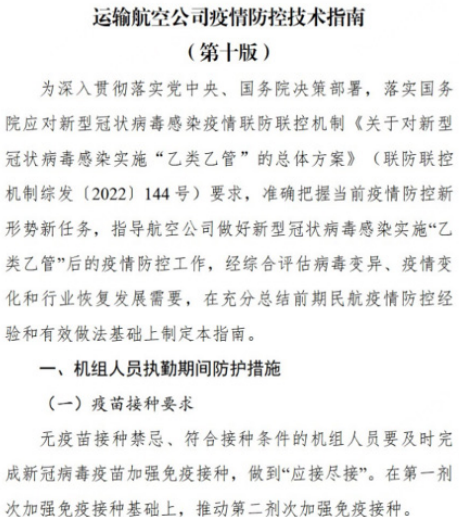
4.交通运输

2023年，APT组织针对交通运输领域的攻击活动明显增多，全球安全厂商披露的涉及交通运输行业的攻击事件，涉及航运、航空运输、铁路运输等多个领域。

报告时间	披露内容	具体领域
2023-02	乌克兰和北约盟国安全局遭受三起网络攻击，可能是APT组织Gamaredon[16]	航空运输
2023-02	针对亚洲医疗和航运组织的新威胁组织Hydrochasma[17]	航运
2023-03	Bad magic：在俄乌冲突地区发现新的APT[18]	运输系统
2023-04	CharmingKitten改进间谍情报技术以攻击高价值目标[19]	运输系统
2023-04	APT-C-01（毒云藤）组织对民航机场等目标展开集中攻击[20]	航空运输
2023-05	RedStinger：自2020年起针对东欧的APT攻击行动[21]	铁路运输
2023-05	APT-C-00（海莲花）持续攻击多个航运相关单位[22]	航运
2023-05	疑似Tortoiseshell组织针对以色列航运和物流公司的水坑攻击行动[23]	航运、物流
2023-08	响尾蛇组织疑似针对巴基斯坦航空公司钓鱼活动样本分析[24]	航空运输
2023-09	多个APT组织利用CVE-2022-47966和CVE-2022-42475攻击航空组织[25]	航空运输
2023-10	Tortoiseshell通过水坑攻击部署IMAPLoader[26]	航运、物流
2023-11	IMPERIAL KITTEN攻击以色列物流和IT公司[27]	物流

我国交通运输行业遭受的攻击活动主要来自于APT-C-00（海莲花）、APT-C-01（毒云藤）和APT-C-08（蔓灵花）。从受攻击影响交通运输领域单位类型看，航空运输、航运、道路运输以及与交通运输相关的高等院校为APT组织关注的重点。

360高级威胁研究院监测到：针对航空运输类单位的攻击活动，主要分布于民航机场类目标，主要由APT-C-01（毒云藤）组织针对民航机场类目标的集中钓鱼攻击所致。毒云藤组织针对机场类目标单位，投递“民航”相关主题的通知类诱饵文档，对目标单位极具迷惑性，提高了其攻击成功率。



运输航空公司疫情防控技术指南

（第十版）

为深入贯彻落实党中央、国务院决策部署，落实国务院应对新型冠状病毒感染疫情联防联控机制《关于对新型冠状病毒感染实施“乙类乙管”的总体方案》（联防联控机制综发〔2022〕144号）要求，准确把握当前疫情防控新形势新任务，指导航空公司做好新型冠状病毒感染实施“乙类乙管”后的疫情防控工作，经综合评估病毒变异、疫情变化和行业恢复发展需要，在充分总结前期民航疫情防控经验和有效做法基础上制定本指南。

一、机组人员执勤期间防护措施

（一）疫苗接种要求

无疫苗接种禁忌、符合接种条件的机组人员要及时完成新冠病毒疫苗加强免疫接种，做到“应接尽接”。在第一剂次加强免疫接种基础上，推动第二剂次加强免疫接种。

2023毒云藤组织针对航空运输目标投放的部分诱饵文档名称
关于印发《中国民用航空安全奖励办法（试行）》的通知民航发〔2023〕9号.pdf
民用航空网络安全保障方案.rar
基于平疫结合的航站楼适应性规划设计.pdf
关于恢复国际客运航班的若干措施.pdf
第四届雁栖航天论坛优秀论文集（以此版为准）.docx
关于加强民航专业工程建设质量管理工作的二十条措施.pdf
运输航空公司疫情防控技术指南-第十版.pdf
国内客运航班运行财政补贴资金申报表.xls

▶ 毒云藤组织针对航空运输目标投放的诱饵文档

5.能源

能源行业作为经济社会发展的重要支撑和战略性基础，是社会和经济运行的重要支撑。近几年全球范围内，由于能源行业遭受网络攻击导致数据泄露，甚至对国家经济和社会生活造成严重影响的事件屡见不鲜。能源领域相关重点单位，一直是APT组织长期重点关注目标。在俄乌冲突中，出现了以能源设施为攻击目标的复杂网络攻击，导致大面积的电力中断，是自俄乌冲突以来第一起因网络攻击导致断电的公开报道。

2023年针对我国能源行业攻击活跃的组织，主要为来自南亚地区的APT-C-00（海莲花）和APT-C-08（蔓灵花）。其中海莲花组织对多个能源相关以及与能源相关的政府管理机构展开攻击。蔓灵花组织则对某电力单位展开持续渗透攻击。另外来自东亚地区的APT-C-06（DarkHotel）和APT-C-01（毒云藤）组织也针对能源行业所属的电力、石油和核工业背景的相关单位展开阶段性攻击。

发布时间	披露内容	涉及具体领域
2023-02	Lazarus组织瞄准医疗研究和技术产业[28]	能源
2023-03	针对独联体国家的政府或能源组织的新APT组织YoroTrooper[29]	能源
2023-03	Kimsuky可能针对能源领域[30]	能源
2023-03	APT-C-01 (毒云藤) 组织针对电力行业展开攻击	电力
2023-04	CharmingKitten改进间谍情报技术以攻击高价值目标[31]	能源、天然气
2023-04	Sandworm针对能源行业的攻击行动[32]	能源
2023-04	X_Trader供应链攻击影响美国和欧洲的关键基础设施组织[33]	能源
2023-05	MuddyWater针对MSP的攻击[34]	石油、天然气
2023-06	APT-C-00 (海莲花) 组织攻击活动持续针对能源相关单位	石油石化、电力
2023-07	APT-C-28 (ScarCruft) 组织针对能源方向投放Rokrat后门活动分析[35]	石油石化
2023-07	Space Pirates针对俄罗斯和塞尔维亚的新攻击行动[36]	能源
2023-11	Sandworm组织去年破坏了乌克兰电网[37]	电力
2023-11	丹麦能源组织遭受大规模网络攻击[38]	能源、电力
2023-11	分析Hellhounds组织的Lahat攻击行动[39]	电力
2023-12	APT-C-00 (海莲花) 针对中国能源行业的攻击	石油

PART 04

2023年APT攻击态势总结

PART.04

2023年APT攻击态势总结

Advanced Persistent Threat

1.TOP20 ATT&CK技战术

360高级威胁研究院综合分析2023年全球安全机构和厂商公开披露的APT报告，对披露的APT组织符合ATT&CK知识标准的攻击技术进行了分析统计，给出了APT组织在2023年攻击活动过程中使用最为集中的TOP20 ATT&CK技战术。

技战术编号	技战术名称（英文）	技战术名称（中文）
T1059	Command and Scripting Interpreter	滥用命令和脚本解释器
T1071	Application Layer Protocol	应用层协议
T1566	Phishing	网络钓鱼
T1204	User Execution	依靠用户自行执行
T1027	Obfuscated Files or Information	混淆文件或信息
T1140	Deobfuscate/Decode Files or Information	解码加密/混淆的文件信息

技战术编号	技战术名称（英文）	技战术名称（中文）
T1082	System Information Discovery	检测操作系统和硬件的信息
T1036	Masquerading	伪装
T1547	Boot or Logon Autostart Execution	启动或登录时自动执行
T1083	File and Directory Discovery	收集文件和目录信息
T1041	Exfiltration Over C2 Channel	通过C2通道渗透
T1053	Scheduled Task/Job	计划任务/工作
T1070	Indicator Removal	删除主机上的痕迹
T1057	Process Discovery	收集正在运行的进程的信息
T1105	Ingress Tool Transfer	从外部系统转移文件
T1573	Encrypted Channel	使用已知加密算法
T1574	Hijack Execution Flow	劫持执行流程
T1016	System Network Configuration Discovery	收集系统网络配置信息
T1033	System Owner/User Discovery	获取系统/用户名称
T1583	Acquire Infrastructure	购买基础设施

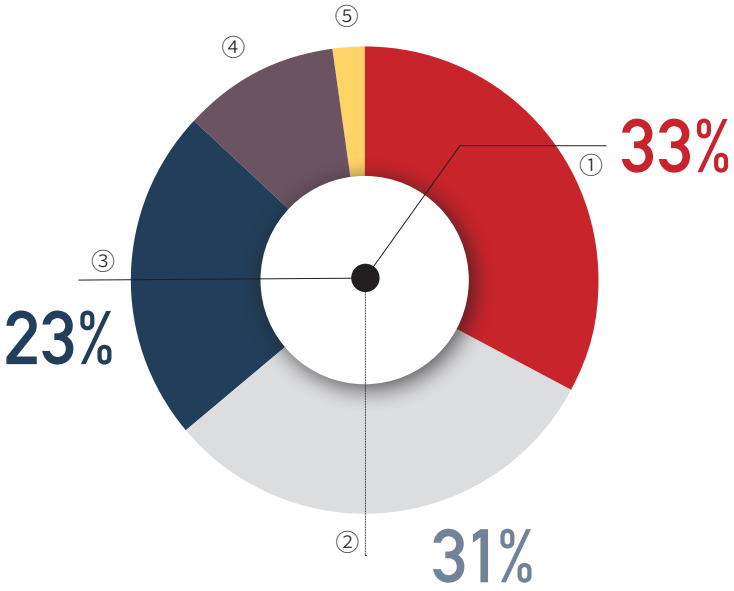
2.APT攻击使用的0Day漏洞集中在操作系统和浏览器

根据统计2023年，APT组织在网络攻击活动中使用的在野0day漏洞共计56个[40]，涉及11个厂商的16个产品，总体数量超过2022年，处于近几年0day漏洞利用数量的高位。我们对全网披露的高级威胁研究报告涉及的0day和Nday漏洞利用情况进行统计：截止2023年12月，全球范围内APT组织在攻击活动中利用的0day和Nday漏洞76个，涉及APT组织27个。

在2023年披露的APT攻击利用的0day漏洞分布看，漏洞集中分布在影响面广的浏览器软件和操作系统，其中针对移动端系统0day漏洞利用数量增长明显，占比达23%。

APT-C-06（DarkHotel）和APT-C-68（寄生虫）组织，在2023年的攻击活动中启用了多个0day漏洞。APT-C-06（DarkHotel）组织利用国内某邮件系统0day进行大规模攻击；APT-C-68（寄生虫）组织则在上半年集中利用某行业软件0day漏洞攻击军工、科研等领域。

2023年6月份，国外安全厂商披露了APT-C-40（NSA）组织使用多个iOS平台0day漏洞针对iOS移动设备的攻击活动。攻击者通过iMessage平台使用0-click漏洞进行感染，先后利用多个漏洞获得对设备和用户数据的完全控制。



①浏览器	33%
②桌面操作系统	31%
③移动操作系统	23%
④办公软件	11%
⑤网络硬件	2%

▶ 2023年APT攻击利用0day漏洞分布

3.针对移动平台的APT攻击愈加频繁且复杂

从2023年披露的针对移动平台的APT攻击活动看，越来越多APT组织将攻击活动扩展到移动平台，并且在移动平台的攻击技战术逐渐成熟。这不仅体现在2023年针对移动平台0day漏洞利用数量明显提升，还体现在针对移动平台技战术成熟、影响范围大的APT攻击事件频发。

APT-C-40（NSA）组织在对iOS设备的攻击活动中，巧妙利用了苹果芯片中的硬件机制漏洞。攻击者首先利用CVE-2023-41990漏洞，通过iMessage服务发送恶意pdf文件，之后利用CVE-2023-32434漏洞获取内存读写权限，再使用CVE-2023-38606漏洞绕过内存页面保护，实现对移动设备的完全控制。攻击者还在攻击后利用CVE-2023-32435漏洞清理痕迹。这几乎是迄今为止针对移动平台“最复杂的攻击链”[41]。

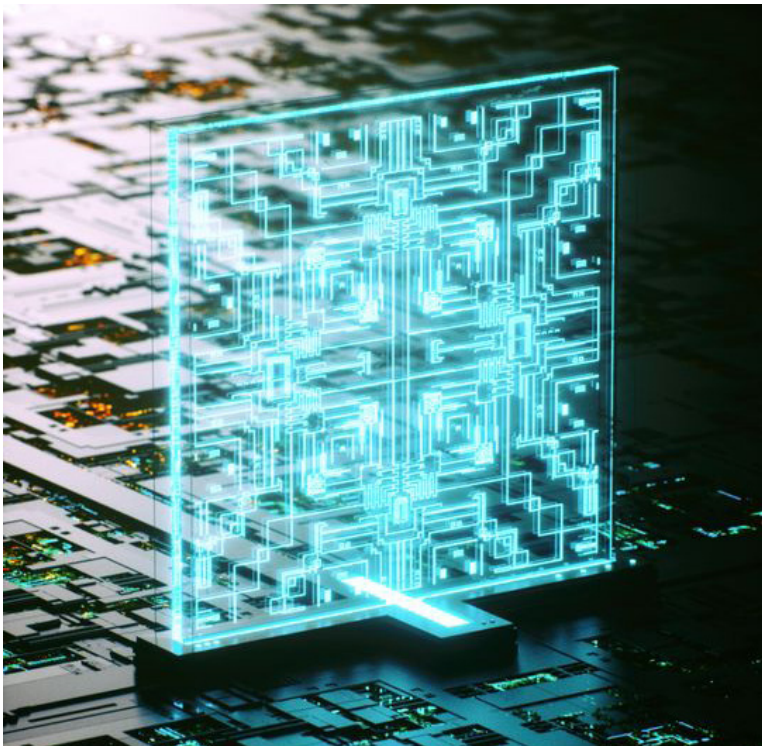
APT-C-56（透明部落）组织2023年针对印度的攻击活动，继续以交友软件为掩护，使用钓鱼网站窃取特定用户信息或者引诱受害者下载安装具备间谍功能的移动端聊天软件[42]。APT-C-23（双尾蝎）组织针近期对移动平台的攻击活动[43]，将恶意应用打包进合法应用，并将恶意行为通过动态加载远程下发的dex实现，通过下载模块化恶意载荷，提升在移动端的反查杀能力。

4.针对芯片、5G等高科技领域的攻击威胁加剧

2023美国对中国高新科技领域的封锁政策变本加厉，尤其是针对我国芯片发展技术的打压，封锁禁令更是扩展到光刻机技术以及芯片供应链，试图以此来保持其在科技领域的领先地位。

2023年针对我国的芯片、5G等高科技领域的攻击显著增多，涉及多个方向APT组织，其中以美国方向APT-C-39 (CIA) 组织最为典型。该组织自2019年被披露以来，持续针对我国国防军工、通信等领域展开活跃攻击，360在2023年捕获到该组织针对我国芯片、5G通信等领域目标的攻击活动。

APT组织针在现阶段对我国芯片、5G领域的攻击渗透，实际是配合其背后政治势力，在网络空间实施对我国高新科技技术发展的制约和打压。这警醒我在应对APT攻击威胁时，同时关注攻击者背后的政治势力，认清攻击威胁目的和全貌。



5.围绕地理、地质测绘重点目标的攻击频发

通过360监测到的APT攻击活动分析，2023年APT组织对我国地理、地质测绘领域攻击活动明显增加。地理、地质测绘机构掌握的测绘数据属于高价值情报和重要战略性数据资源，成为APT组织重点窃密目标。

2023年7月，我们披露了美国方向黑客组织针对武汉市地震监测中心的网络攻击活动。此次攻击实际是隐藏在窃取高精度地质数据数据之下，对我国战略性数据资源以及军事情报的窃密。通过窃取我国高精度地理、地质测绘数据，可还原出交通、能源、军事等重要领域特定区域的三维地貌图，为侦察监视、军事行动提供关键支持，数据一旦泄露将严重威胁我国的军事安全。

我们通过监测发现，东南亚组织APT-C-00（海莲花）长期针对我国地理信息和环境相关领域展开攻击渗透。2023年该组织攻击目标还包含了我国部分沿海地区的地质科学、地质调查领域的政府和科研机构。南亚组织APT-C-09（摩诃草）和APT-C-48（CNC）也在2023年针对我国地质测绘领域相关科研和教育机构展开攻击活动。

APT组织在网络空间的攻击和窃密，逐渐成为隐藏在其背后政治势力获取竞争优势，刺探各种情报，实现政治乃至战略目的常规手段。

6.以破坏为目的网络攻击在地区冲突对抗中不断出现

2022年俄乌冲突爆发后，越来越多使用擦除器软件的攻击活动被披露。2023年巴以冲突期间，也发现了使用数据擦除器（BiBi-Linux Wiper）软件的攻击活动，恶意软件不仅会破坏文件，甚至还会破坏整个操作系统。

Sandworm组织在2022年对乌克兰能源设施发动的攻击，不仅导致电力中断，乌克兰各地的关键基础设施还紧随其后遭到导弹袭击。此次攻击是罕见的以破坏目标物理设施运行为目的的网络攻击，显示了APT组织在实际冲突对抗中，对关键基础设施的实际破坏能力以及与军事打击之间可以存在的协作能力。

在冲突对抗中，网络攻击不再仅仅是幕后信息窃取情报信息的手段，攻击逐渐转向前台，将对数据、系统、服务以及基础设施的破坏作为直接目的。网络攻击逐渐成为冲突对抗中一种实际而有效的攻击方式，演变成对关键基础设施甚至军事目标的直接威胁。

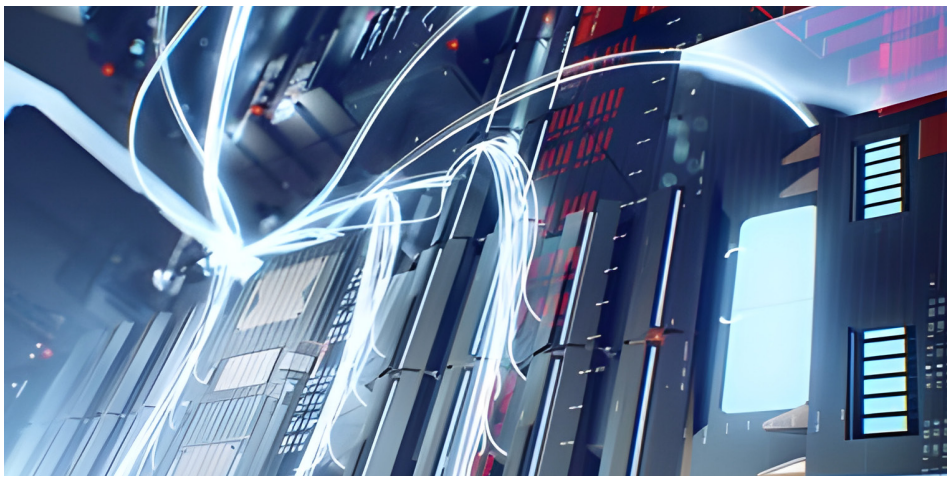
7.“舆论对抗”升温中持续演变

我们曾在在《2022年全球高级持续性威胁（APT）研究报告》中提到：网络犯罪组织逐渐将以往的“技术对抗”不断扩展到“舆论对抗”、“舆论造势”。这一发展趋势在2023年APT攻击发展形势中得到印证。网络空间的“舆论对抗”在持续升温中不断演变。

2023年APT-C-13（Sandworm）组织聚焦于俄乌冲突，利用凭证钓鱼、恶意软件和外部服务等多种手法展开攻击活动[44]。Sandworm组织通过建立虚假在线身份，制造和传播新闻内容，在Telegram上泄露被盗数据，试图影响公众舆论。其背后的动机主要为争夺全球政治和经济力量，另外也尝试通过舆论造势影响社会舆论。2023年10月，网络安全厂商通过分析报告，揭穿了伊朗黑客组织声称攻陷以色列Dorad发电厂的谎言。

360在2023年2月发布的《夯实供应链安全-解密对华黑客组织ATW的供应链攻击伎俩》报告中[45]，分析了ATW组织一系列攻击手法。在ATW持续一整年的攻击活动中，曾在多个平台发布七十多起针对中国企事业单位的网络入侵事件，但并不是所有公开的通过供应链的入侵事件，都是成功的。其目的是通过不断的舆论宣传造势，营造出我国行业的供应链安全有重大隐患的氛围，给相关组织机构的声誉造成了恶劣影响。

另外，在《“黑客帝国”调查报告——美国中央情报局（CIA）（之一）》报告中，我们总结了APT-C-39（CIA）组织在以往多起“颜色革命”事件借助互联网推波助澜，协助发布扩散虚假信息，推动民众抗议活动激化的手段。APT-C-39（CIA）组织形成了一套以提供加密网络通信服务、提供断网通信服务、提供基于互联网和无线通讯的集会游行活动现场指挥工具以及研发“反审查”信息系统等内容的技战术。



8.网络空间对抗成为地缘政治较量的制高点

2023年俄乌冲突持续发展，在军事冲突之外，东欧地区APT组织攻击活动频繁，为地缘政治局势发展推波助澜。由于我国所处的地缘政治环境复杂，周边国家地区背景的APT组织，不断围绕“海洋发展”、“两岸关系”、“和平统一”等地区热点话题，对我国重点目标展开攻击渗透。

我国十八大提出建设海洋强国战略以来，与我国在海洋发展存在利益竞争地缘政治势力，通过网络空间，将我国海洋海事作为重点攻击目标领域，针对我国海洋领域的政府机构、科研、军事等相关单位，展开持续攻击。

根据该领域的特点和热点，制作与海洋发展或我国两岸关系局势等针对性强的诱饵文档。攻击目标涵盖沿海地区或与海洋海事相关的科研、运输、教育等单位。此类网络攻击的实际意图是窃取小到科研成果、海事活动，大到国防军工、国家战略规划等情报。

通过网络空间对抗可以灵活和隐蔽的展开网络攻击渗透，实施网络侦察和情报收集，从而在地缘政治对抗中获得更大的话语权和优势，网络空间对抗逐渐成为地缘政治较量的制高点。地缘政治各方势力为在地缘政治竞争中占据先机，势必会增加投入和精力来争夺网络空间对抗这一制高点。这需要我们不断提升国家网络安全防护和网络空间对抗能力来应对，这也是我国由网络大国迈向网络强国道路上的重要挑战和机遇。

附录

01

360安全大脑

360基于安全大数据、知识库和专家，建设了360网络安全大脑和网络安全基础设施（情报、漏洞、专家、实战、培训、测绘、开发），以云服务方式为政府、企业、个人用户提供安全公共服务，形成了新的安全理念和方法论。

360网络安全大脑强化了“精准防控为要、实战有效为王”的价值取向，着眼安全事件的“高效发现和及时处置”，理顺识别、防御、监测、预警、响应流程，推动一般常见风险及时处置、高级重大威胁有效解决、预防关口主动前移。着眼防范化解重大风险，聚焦最难啃的骨头、最突出的隐患、最明显的短板，及时总结网络安全风险防控经验，研究开发务实有效的安全原生服务。强化互联网体系与政企体系的协同联动，让网络安全体系回归保障业务的本质。

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。

1.http://www.whwx.gov.cn/wlaq/wadt/202307/t20230728_2238379.shtml

2.https://mp.weixin.qq.com/s/ZhbGa7xzgZUxkTYuRtAjDg

3.https://world.huanqiu.com/article/4EX89Zq6zNg

4.https://mp.weixin.qq.com/s/xU7b3m-L2OIAi2bU7nBj0A

5.https://mp.weixin.qq.com/s/IvSraGnMsl3a1jEUubuvyw

6.https://asec.ahnlab.com/ko/52829/

7.https://community.riskiq.com/article/541a465f

8.https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

9.https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

10.https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

11.https://blog.google/threat-analysis-group/ukraine-remains-russiasbiggest-cyber-focus-in-2023/

12.https://go.recordedfuture.com/hubfs/reports/cta-2023-0620.pdf

13.https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-torussian-intelligence-services

14.https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegramto-target-ukrainian-organizations

15.https://mp.weixin.qq.com/s/NomfjAjGYdsOpLBtiOSZpA

16.https://blog.eclecticiq.com/three-cases-of-cyber-attacks-on-the-security-service-of-ukraine-and-nato-allies-likely-by-russian-state-sponsored-gamaredon

17.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering

18.https://securelist.com/bad-magic-apt/109087/

19.https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/

20.https://mp.weixin.qq.com/s/bOJ88Zzk27ZaHShlYUCYgA

21.https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

22.https://www.secrss.com/articles/54898

23.https://www.clearskysec.com/wp-content/uploads/2023/05/Fata-Morgana-Israeli-Websites-Infected-by-Iranian-Group-1.8.pdf

24.https://mp.weixin.qq.com/s/jUuKwhzzqbOwqXacM8cvZA

25.https://www.cisa.gov/news-events/analysis-reports/ar23-250a

26.https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

27.https://www.crowdstrike.com/blog/imperial-kitten-deploys-novel-malware-families/

28.https://www.withsecure.com/content/dam/with-secure/ja/resources/202302_WithSecure_Lazarus_Group_Report_ENG.pdf

29.https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/

30.https://www.bridewell.com/insights/news/detail/bridewell-intelligence-report-kimsuky-apt-group---key-insights-for-uk-energy-cisos

31.https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/

32.https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

33.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

34.https://www.welivesecurity.com/2023/05/02/apt-groups-muddying-waters-msps/

35.https://mp.weixin.qq.com/s/13bQDJCfnTBFVMUbhKgIlw

36.https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/

37.https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

38.https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

39.https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/hellhounds-operation-lahat/

40.https://docs.google.com/spreadsheets/d/1IkNJ0uQwbeC1ZTRrxdtuPLCII7mlUreoKfSIgajnSyY/view#gid=1746868651

41.https://therecord.media/operation-triangulation-iphone-spyware-unknown-hardware-feature%EF%BB%BF

42.https://securelist.com/trng-2023/

43.https://mp.weixin.qq.com/s/NomfjAjGYdsOpLBtiOSZpA

44.https://blog.google/threat-analysis-group/ukraine-remains-russiasbiggest-cyber-focus-in-2023/

45.https://mp.weixin.qq.com/s/_pZuKpgSYhZy07gQQinI8w