APT

全球高级持续性威胁（APT）2023年中报告

2023年07月

奇安信
威胁情报中心

主要观点
MAIN POINTS

2023 年上半年全球范围内，政府部门仍是 APT 攻击的首要目标，相关攻击事件占比为 30%，其次是国防军事领域，相关事件占比 16%。与去年同期相比，教育、科研领域相关的攻击事件比例增高，占比分别为 11% 和 9%。

2023 年上半年涉及我国政府、能源、科研教育、金融商贸的高级威胁事件占主要部分，其次为科技、国防、卫生医疗等领域。

2023 年上半年，全球高级威胁活动呈现出以下特点：针对移动平台 iOS/Android 的 0day 攻击逐渐增多，相关攻击团伙的技术实力积累雄厚或者背靠国家机器；路由器、防火墙等网络边界设备成为 APT 组织攻击的主要目标之一，如海莲花、APT28 通常会攻击一些存在漏洞的网络边界设备。被攻陷的网络设备一方面可以作为 C2 的转发器，用于隐藏攻击者的真实 IP，另一方面也可以作为攻击入口进行更深入的横向移动。

上半年内，我们观察到境外黑客组织在针对中国的 APT 攻击活动中大量使用了 0day 以及 Nday 漏洞。6 月初，国外安全厂商卡巴斯基披露了一个针对全球范围内利用 iOS 系统中 iMessage 信息服务的 0-Click 0day 漏洞攻击。我们从该攻击的目标范围、复杂度、攻击技术和跨越时间来看，这是近十年内最顶尖的国家级 APT 攻击活动。通过我们的关联分析和确认，推测该攻击活动至少开始于 2019 年，且涉及国内大量受害者。

2023 年上半年，在野 0day 漏洞的利用情况同比 2022 年有所上升，漏洞数量接近 30 个左右。在漏洞涉及产品的供应厂商中，微软、谷歌、苹果的地位依然稳固，但是相较往年微软、谷歌势强而苹果势微的情况，今年三家厂商在曝出的在野 0day 漏洞数量上呈现出真正意义上的三足鼎立。

摘 要

ABSTRACT

2023 上半年，奇安信威胁情报中心使用奇安信威胁雷达对境内的 APT 攻击活动进行了全方位遥感测绘。监测到国内大量 IP 地址与数十个境外 APT 组织产生过高危通信行为，疑似被攻击。广东省受境外 APT 团伙攻击情况最为突出，其次是北京、上海、浙江等经济发达地区。此外，监测发现中国香港地区也存在一定数量的受害目标。

基于奇安信威胁雷达的测绘分析，海莲花、毒云藤、Winnti、蔓灵花、APT-Q-27、响尾蛇、Lazarus 等组织在 2023 上半年对我国攻击频率最高。我国境内疑似受其控制的 IP 地址比例分别为：毒云藤 27%，海莲花 15%，Winnti 14%，蔓灵花 8%，APT-Q-27 7%，响尾蛇 6%，Lazarus 6%。

本次报告通过综合分析奇安信威胁雷达测绘数据、奇安信红雨滴团队对客户现场的 APT 攻击线索排查情况以及奇安信威胁情报支持的全线产品告警数据，得出以下结论：2023 上半年，我国政府部门、能源、科研教育行业遭受高级威胁攻击情况突出，受影响行业中排名前五的分别是：政府 33%，能源 15%，科研教育 12%，金融商贸 11%，科技 7%。

2023 上半年奇安信威胁情报中心收录了 177 篇高级威胁类公开报告，涉及 64 个已命名的攻击组织或攻击行动。其中，提及率最高的五个 APT 组织分别是：Kimsuky 8.8%，Lazarus 8.0%，Group123 7.4%，SideCopy 5.6%，Gamaredon 4.3%。

2023 上半年全球 APT 活动的首要目标仍是政府部门和国防军事行业，相关攻击事件占比分别为 30% 和 16%，紧随其后的热点攻击行业是教育、科研、金融、医疗、通信等领域。

2023 上半年的在野漏洞利用中，以浏览器为攻击向量依然是主流趋势，Chrome、Safari 浏览器与对应平台 Windows、macOS、iOS 下的提权逃逸漏洞占所有漏洞近 8 成。0day 漏洞利用逐渐成为勒索团伙武器库的备选项。奇安信威胁情报中心在多起利用重要漏洞的攻击行动披露后第一时间跟进调查，发现有些攻击发起时间比预估更早（比如 Outlook 会议预约漏洞），或者影响范围更大（比如 iOS 的 iMessage 漏洞涉及大量国内受害者）。

关键字：全球高级持续性威胁、APT、威胁雷达、0day、iOS、浏览器

目 录

CATALOGUE

第一章 中国境内高级持续性威胁综述

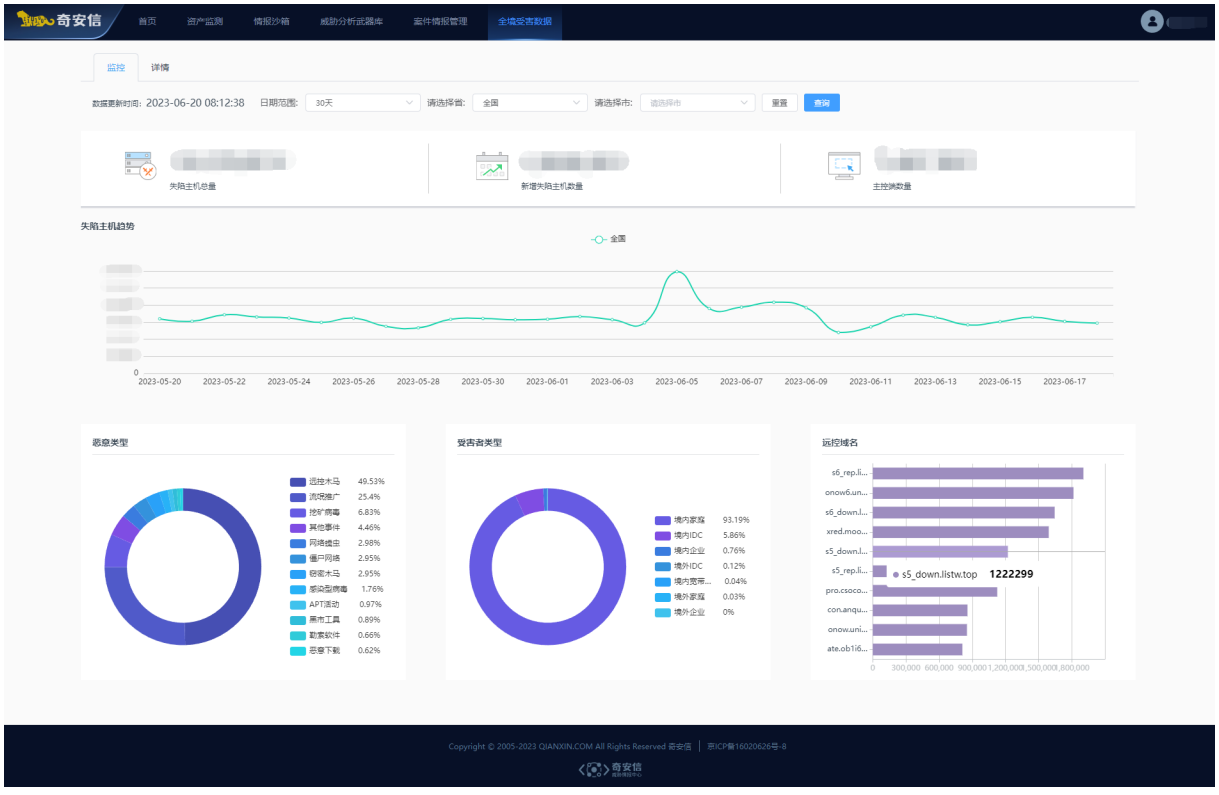
基于中国境内海量 DNS 域名解析和奇安信威胁情报中心失陷检测（IOC）库的碰撞分析（奇安信威胁雷达），是了解我国境内 APT 攻击活动及高级持续性威胁发展趋势的重要手段。

奇安信威胁情报中心通过使用奇安信威胁雷达对境内的 APT 攻击活动进行了全方位遥感测绘，2023 年上半年监测到我国范围内大量 IP 地址疑似和数十个境外 APT 组织产生过高危通信。从地域分布来看，广东省受境外 APT 团伙攻击情况最为突出，其次是北京、上海、浙江等经济发达地区。值得注意的是，中国香港也受到较多攻击。

本章内容及结论主要基于奇安信威胁雷达数据、奇安信红雨滴团队在客户现场处置排查的真实 APT 攻击事件，结合使用了奇安信威胁情报的全线产品告警数据，进行的整理与分析。

一、奇安信威胁雷达境内遥测分析

奇安信威胁雷达是奇安信威胁情报中心基于奇安信大网数据和威胁情报中心失陷检测（IOC）库，用于监控全境范围内疑似被 APT 组织、各类僵木蠕控制的网络资产的一款威胁情报 SaaS 应用。通过整合奇安信的高、中位威胁情报能力，发现指定区域内疑似被不同攻击组织或恶意软件控制的主机 IP，了解不同威胁类型的比例及被控主机数量趋势等。可进一步协助排查重点资产相关的 APT 攻击线索。



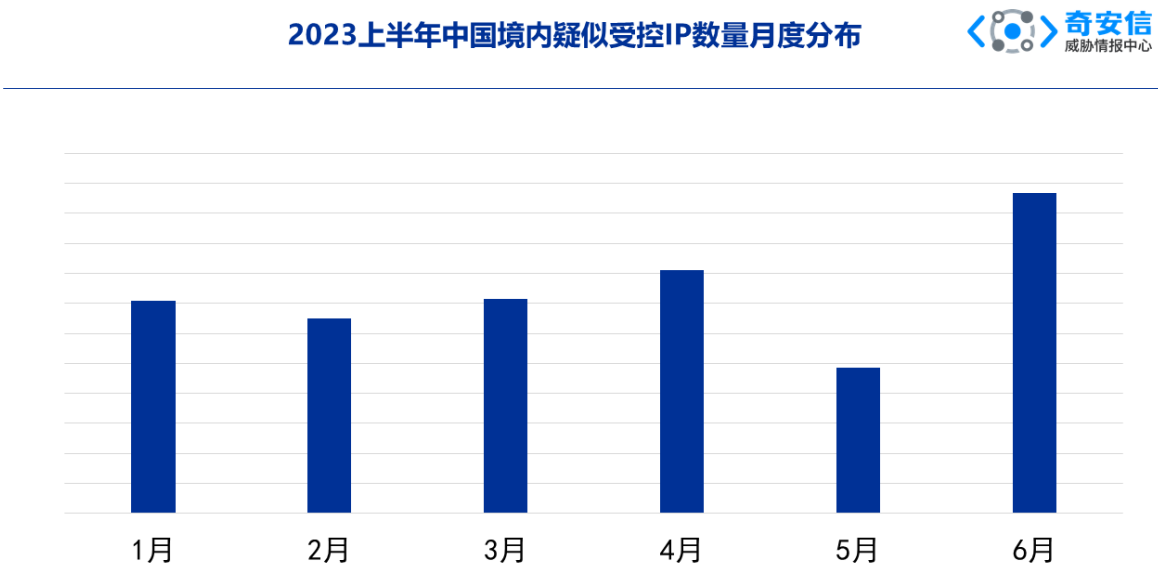
▲ 图 1.1 奇安信威胁雷达境内受害者数据分析

基于奇安信威胁雷达境内的遥测分析，我们从以下方面对我国境内疑似遭受的 APT 攻击进行了分析和统计。

（一） 受控 IP 数量和趋势

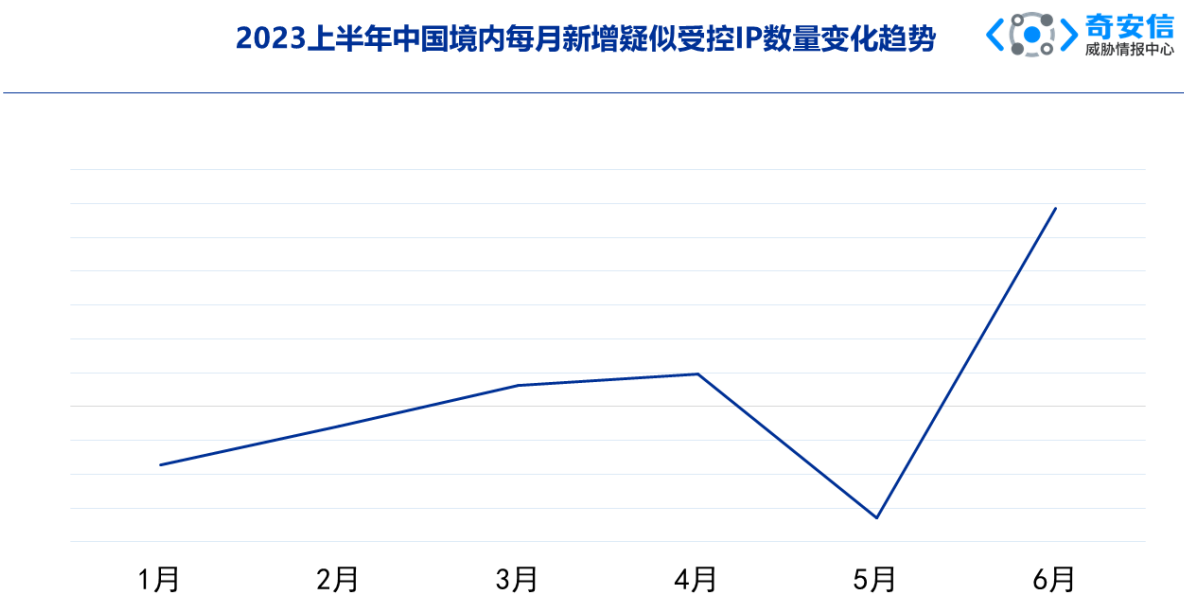
奇安信威胁情报中心基于威胁雷达在 2023 上半年监测到数十个境外 APT 组织针对我国范围内大量目标 IP 进行通信，形成了大量的境内 IP 与特定 APT 组织的网络基础设施的高危通信事件。其中还存在个别 APT 组织通过多个 C2 服务器与同一 IP 通信的情况。

下图为 2023 上半年奇安信威胁雷达遥测感知的我国境内每月连接境外 APT 组织 C2 服务器的疑似受害 IP 地址数量统计。可以看出，1-4 月 APT 团伙攻击频次相对均匀，波动不大，6 月份为上半年境外 APT 攻击高峰。



▲ 图 1.2 2023 上半年中国境内疑似受控 IP 数量月度分布

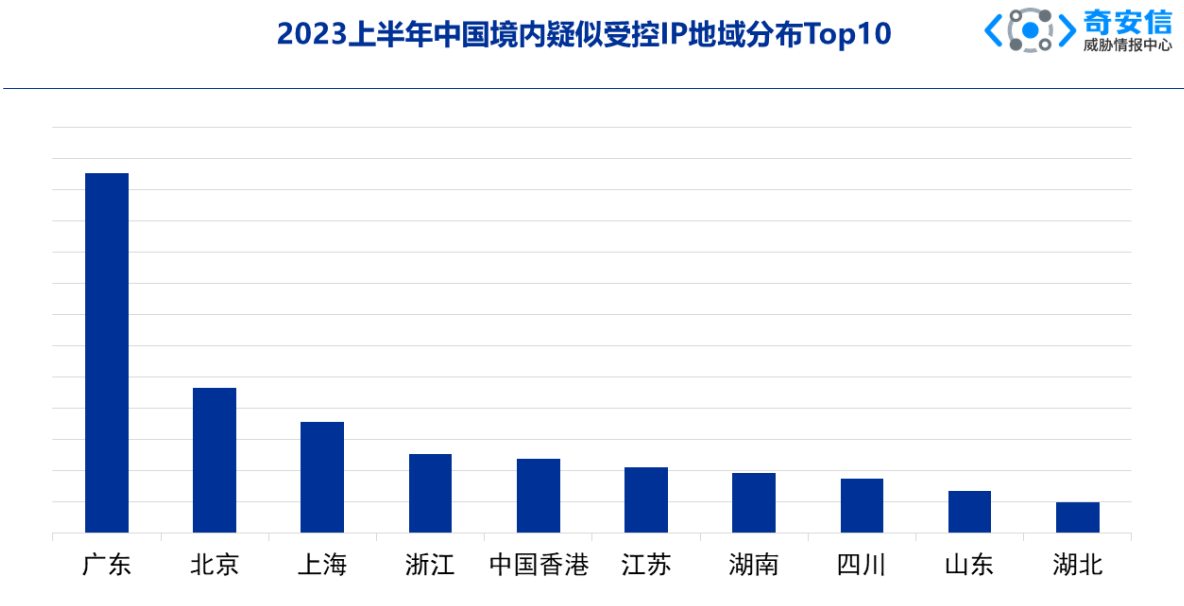
2023 上半年中国境内每月新增疑似被境外 APT 组织控制的 IP 数量变化趋势如图 1.3 所示，反映了 APT 组织攻击活跃度变化走向。新增受控 IP 数量变化趋势也与图 1.2 中每月连接境外 APT 组织 C2 服务器的疑似受害 IP 数量分布相符，前 4 个月疑似受控 IP 数量变化趋势平缓，5 月攻击有所减少，6 月激增。



▲ 图 1.3 2023 上半年中国境内每月新增疑似受控 IP 数量变化趋势

（二） 受害目标区域分布

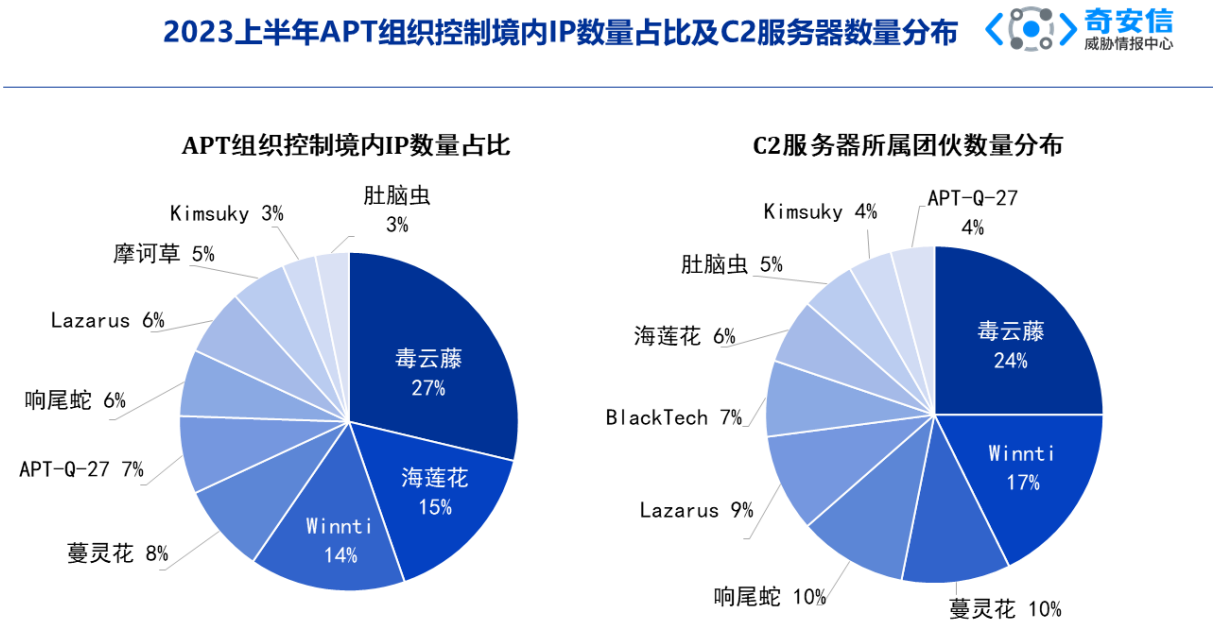
下图为 2023 上半年中国境内疑似连接过境外 APT 组织 C2 服务器的 IP 地址地域分布，分别展示了各省疑似受害 IP 地址的数量：广东省受境外 APT 团伙攻击情况最为突出，其次是北京、上海、浙江等经济发达地区。此外，监测发现中国香港地区也存在一定数量的受害目标。



▲ 图 1.4 2023 上半年中国境内疑似受控 IP 地域分布

（三） APT 组织资产分布

下图分别为 2023 上半年境外 APT 组织疑似控制我国境内目标 IP 数量占比以及境外 APT 组织疑似使用过的 C2 服务器数量分布。



▲ 图 1.5 2023 上半年 APT 组织控制境内 IP 数量占比及 C2 服务器所属团伙数量分布

可以看出，海莲花、毒云藤两个组织依旧是针对国内攻击的主要组织，Winnti、蔓灵花、APT-Q-27、响尾蛇、Lazarus 等 APT 组织也疑似控制了境内大量 IP 地址。这些组织潜伏在我国周边国家和地区伺机发起攻击，其中毒云藤和海莲花长期针对中国。在上半年的攻击中，毒云藤大多以钓鱼为主，目标通常为高校、科研领域，海莲花则主要针对我国关键基础设施。

进一步对这些 APT 组织的 C2 服务器及其控制的境内 IP 地址数据分析后，我们发现：

1. Winnti 组织攻击主要集中在 1-4 月，最高峰为 1 月，该组织使用相对少的 C2 服务器与境内大量 IP 地址进行了非法通信。

2. 毒云藤、蔓灵花、响尾蛇、Lazarus、肚脑虫等组织 C2 服务器比较分散，常在攻击中频繁更换 C2。

3. APT-Q-27、摩诃草、Kimsuky 这几个组织均通过少量的 C2 进行批量攻击。

另外，我们还发现 APT-Q-77 多次针对国内的攻击，目标涵盖政府、科技、媒体、医疗、能源等多个行业。

二、2023 上半年紧盯我国的活跃组织

上半年内，我们观察到针对中国的 APT 攻击仍不乏 0day/Nday 漏洞的使用。6 月初，国外安全厂商卡巴斯基披露了一个针对全球范围内利用 iOS 系统中 iMessage 信息服务的 0-Click 0day 漏洞攻击。我们从该攻击的复杂度、攻击技术和跨越时间来看，这是近十年内最顶尖的国家级 APT 攻击活动。通过我们的关联分析和确认，推测该攻击活动至少开始于 2019 年，且涉及国内大量受害者。部分长期针对我国的 APT 组织具有复杂的攻击技战术，而另一些攻击组织则不断采用新武器或更新攻击手法。

奇安信威胁情报中心通过奇安信红雨滴团队和奇安信安服在客户现场处置排查的真实 APT 攻击事件，结合使用了威胁情报的全线产品告警数据，最终基于被攻击单位、受控设备、APT 组织技战术等多个指标筛选出以下数个对我国攻击频率高或危害大的 APT 组织。

接下来，我们将结合奇安信红雨滴团队的真实 APT 攻击处置案例，逐一盘点 2023 上半年紧盯我国的全球 APT 组织。

（一）APT-Q-31（海莲花）

关键词：供应链、重点单位在境外的资产

海莲花在 2023 上半年没有以往活跃，不过仍然对 IT 和软件公司展开攻击，并成功入侵了某公司的代码服务器，企图发起供应链攻击。此外，海莲花在针对我国重点单位在香港资产的攻击活动中舍弃了以往使用的自签名证书的基础设施，改用 80 端口作为 CobaltStrike 的 C2 服务器端口。在攻击过程中通过入侵域控服务器，开启内网漫游，并在横向移动中使用了新的隧道工具 Ligolo-ng。

README.md

Ligolo-ng : Tunneling like a VPN

An advanced, yet simple, tunneling tool that uses a TUN interface.

License GPLv3 go report A+

Table of Contents

▲ 图 1.6 Ligolo-ng 隧道工具截图

奇安信威胁情报中心将持续对海莲花的活动进行监控。

（二） APT-Q-12

关键词：0day 漏洞、邮件

在 2023 年初，APT-Q-12 针对国内某邮箱 PC 端用户投递带有 0day 漏洞的鱼叉邮件，当受害者使用 PC 客户端邮箱打开邮件后会触发相关漏洞的 Exploit 代码用于执行位于标题中的 JavaScript 代码，JavaScript 代码寻找邮件中指定的 Html 资源，最终通过内部接口的方式执行解密后的 LNK 文件，LNK 后续的攻击链与我们之前披露过的 APT-Q-12 攻击链一致。

▲ 图 1.7 带有 0day 漏洞利用代码的邮件

在我们后续溯源的过程中发现 APT-Q-12 与虎木槿组织存在基础设施上的重叠。

（三）APT-Q-77

关键词：鱼叉邮件、天然气、军工

APT-Q-77 在 2023 年初的攻击活动达到顶峰，国内大部分受害者仍然是攻击者利用边界设备 Nday 漏洞批量入侵所致。相关定向攻击仍然集中在天然气和军工领域。在特定的时间点后，APT-Q-77 只剩下投递鱼叉邮件这一种攻击方式。经过我们的溯源发现该团伙最早活跃时间在 2022 年 7 月份，分别投递过以 CHM、ISO（IMG）、LNK 等载荷的附件，在其针对军工领域的活动中使用了 3proxy 代理工具。

APT-Q-77 的鱼叉攻击活动拥有非常复杂的技战术流程：在第一阶段会使用一个简单的加载器去执行 CobaltStrike 木马，当受害者与 CobaltStrike 建立稳定的连接后释放第二阶段的 Loader 并将 Payload 加密存放在注册表中，第三阶段攻击者将 CobaltStrike 当作加载器内存加载 Rust 语言编写的特马来进行保活。当攻击者控制了几天后觉得还有控制的价值，会使用 Rust 特马的功能将 Linux 和 Windows 双平台特马注入到系统进程中并运行，在后续的横向移动过程中还会内存加载管道特马控制内网其他机器。

在 2022 年末 APT-Q-77 的攻击活动被我们成功阻击后，该团伙成员甚至在 2023 年 1 月份通过相关 VPN 访问奇安信威胁情报中心官网（ti.qianxin.com）并阅读我们公开发表的报告。通过 accesslog 我们发现该团伙针对中国的攻击组成员人数大概有 8-9 人，这在一定程度上可能也解释了为何该团伙能够在相同的攻击时间段内针对不同目标使用了多套完全不相同的加载器，并且渗透手法也不相同。

基于闭源威胁情报，APT-Q-77 还使用 Rust 特马入侵了西方国家的医疗化学领域。

（四）APT-Q-78

关键词：地质、科研

APT-Q-78 是一个具有全球视野的 APT 组织，其主要针对我国的地质领域进行攻击。通过 WEB 层面的 0day/Nday 漏洞作为攻击入口，拥有自己独特的 Webshell，在横向移动过程中擅于使用 Powershell 作为下载者等待下发 Payload。后续攻击中释放了 AnyDesk 和一个基于 BAT 的 API 木马。AnyDesk 的使用与 Karakurt Group 有些相像，攻击者主要通过 API 木马上传数据和执行命令，喜欢使用 Putty 将受害机器的端口转发到攻击者控制的跳板服务器上。

该团伙在针对境外的活动中会捆绑一些常用软件的安装包，诱导受害者下载，释放的木马非常简单，并调用 CMD 执行远程服务器下发的命令并创建计划任务进行持久化操作。

（五）Patchwork

关键词：鱼叉邮件、可信签名

摩诃草 APT 组织（Patchwork）在 2023 上半年针对高校、气象、科研、政府等领域投递鱼叉邮件，整体水平相较于以往有较大的提升，起码在木马方面开始着重于免杀 Loader 的编写和可信签名的使用，同时在尝试使用开源的渗透工具 Havoc，但是在绕过 EDR 检测方面并没有那么的理想。其投递的 LNK 诱饵会被奇安信天擎终端安全软件直接拦截，导致我们看不到后续的 Payload，需要手动下载样本进行分析。

在钓鱼方面，摩诃草组织会伪造高校、政府、部委的邮箱登录页面，意图钓取相关人员的邮箱账号密码。

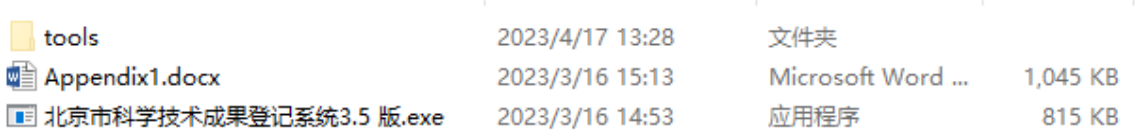
▲ 图 1.8 摩诃草使用的网络钓鱼页面

我们发现摩诃草在 2023 年 1 月份使用 WEB 相关的 Nday 漏洞投递 Havoc 木马入侵国内的一些小企业，我们认为这是一次练手行为，没有造成太大的损失，但这对于南亚方向的 APT 组织来说是一次质的飞跃。

（六）CNC

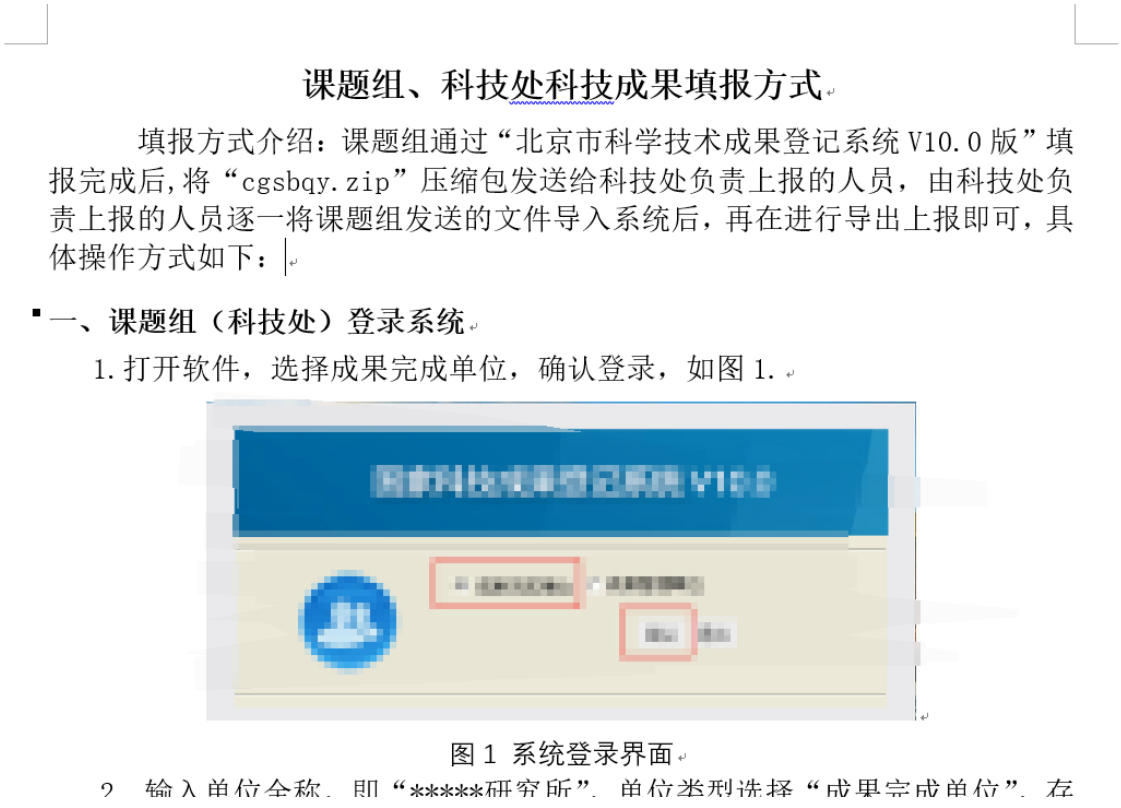
关键词：鱼叉邮件

CNC 作为南亚方向另一个 APT 组织，其水平较弱，攻击方式也比较单一，通常是当受害者在钓鱼页面中输入账号密码后会自动下载一个压缩包，诱导受害者打开压缩包中后缀为“.exe”的文件，其中 tools 为隐藏目录，里面存放着正常功能的软件。



▲ 图 1.9 压缩包截图

Doc 文档是正常软件的使用说明，用于迷惑受害者。



课题组、科技处科技成果填报方式

填报方式介绍：课题组通过“北京市科学技术成果登记系统 V10.0 版”填报完成后，将“cgsbqy.zip”压缩包发送给科技处负责上报的人员，由科技处负责上报的人员逐一将课题组发送的文件导入系统后，再在进行导出上报即可，具体操作方式如下：

一、课题组（科技处）登录系统

1. 打开软件，选择成果完成单位，确认登录，如图 1.

图 1 系统登录界面

2. 输入单位全称，即“*****研究所”，单位类型选择“成果完成单位”，存

▲ 图 1.10 CNC 组织使用的诱饵 Doc 文档截图

（七） APT-Q-94

关键词 :iOS、iMessage、0day

卡巴斯基在 6 月初发表的 Operation Triangulation[119] 一文中提到有黑客组织使用 iOS 系统中 iMessage 信息服务的 0-Click 0day 漏洞针对全球范围进行大规模的攻击。卡巴斯基声称发现公司内部多名员工，包括中高层管理人员为此次攻击的受害者，并认为此次攻击的主要目标不是卡巴斯基。研究人员追溯到最早的感染出现在 2019 年，截至 2023 年 6 月报告发布时，攻击仍在进行。

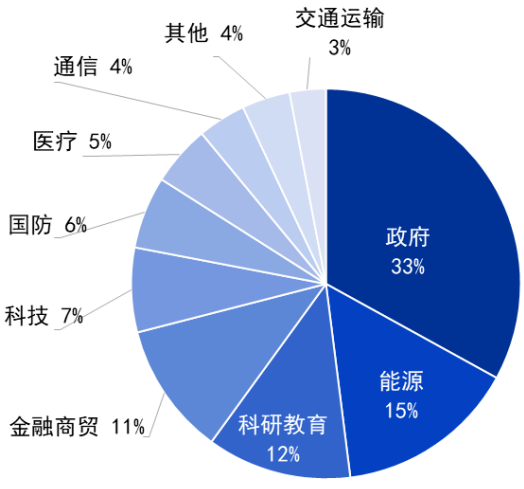
我们结合卡巴斯基的报告在国内范围确认了部分受害者，同时观察到有一部分受害者在没有开启 iMessage 的情况下仍然回连恶意域名，我们推测攻击者在 2019 年至今的活动中应该使用了多个 iOS 的 0day 漏洞进行间谍活动。

结合卡巴斯基的报告和奇安信威胁情报中心的研判调查结果，可以看出攻击者具备超强的攻击能力和资源。从该攻击活动的目标范围、复杂度、攻击技术和跨越时间来看，这是近十年内最顶尖的国家级 APT 攻击活动。且该攻击活动背后的攻击团伙与以往披露的北美地区国家背景的黑客组织十分相似，奇安信以内部编号 APT-Q-94 持续进行跟踪。

三、2023 上半年境内受害行业分析

进一步通过奇安信威胁雷达的遥测感知和奇安信红雨滴团队基于客户现场的 APT 攻击线索，并结合使用了奇安信威胁情报的全线产品告警数据进行分析：2023 上半年涉及我国政府、能源、科研教育、金融商贸的高级威胁事件占主要部分，其次为科技、国防、卫生医疗等领域。相关受影响的境内行业分布如下。

2023上半年高级威胁事件涉及境内行业分布



▲ 图 1.11 2023 上半年高级威胁事件涉及境内行业分布情况

基于上述数据分析，针对我国境内攻击的 APT 组织活跃度排名及其关注的行业领域如下表。

排名	组织名称	涉及行业
TOP1	APT-Q-20 (毒云藤)	国防、政府、科技、教育
TOP2	APT-Q-31 (海莲花)	政府、能源、科研
TOP3	APT-Q-29 (Winnti)	互联网产业、金融、科技
TOP4	APT-Q-37 (蔓灵花)	政府、科研、国防、能源
TOP5	APT-Q-27	博彩、诈骗
TOP6	APT-Q-39 (响尾蛇)	政府、国防、教育
TOP7	APT-Q-1 (Lazarus)	政府、金融
TOP8	APT-Q-36 (摩诃草)	政府、科研、教育、军工
TOP9	APT-Q-2 (Kimsuky)	政府、媒体、教育、金融
TOP10	APT-Q-38 (肚脑虫)	政府、国防

▲ 表 1.12 活跃组织排名及针对的目标行业

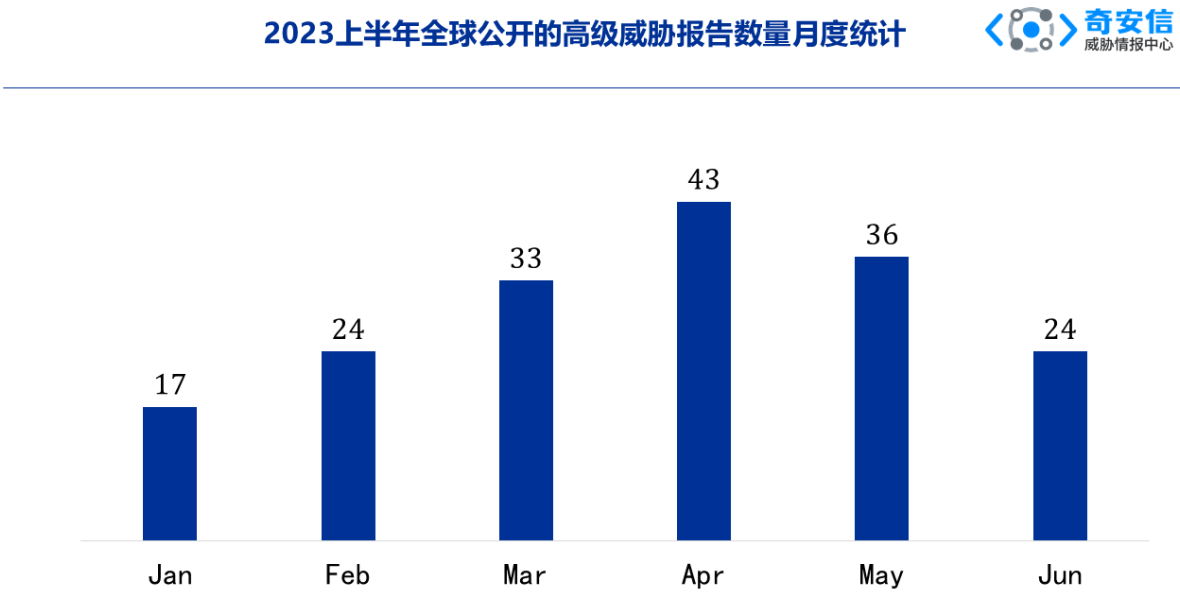
第二章 全球高级持续性威胁综述

公开来源的 APT 情报（以下简称“开源情报”）分析是了解全球网络安全研究机构安全关注，认知全球高级持续性威胁发展趋势的重要手段之一。奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行持续监测，监测内容包括但不限于 APT 攻击组织报告、APT 攻击行动报告、疑似 APT 的定向攻击事件、APT 攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪组织及其相关活动。

本章内容及结论主要基于对上述开源情报以及内部威胁雷达数据的整理与分析。

一、全球高级威胁研究情况

奇安信威胁情报中心在 2023 上半年监测到的高级持续性威胁相关公开报告总共 177 篇。各月监测数据如下图所示。



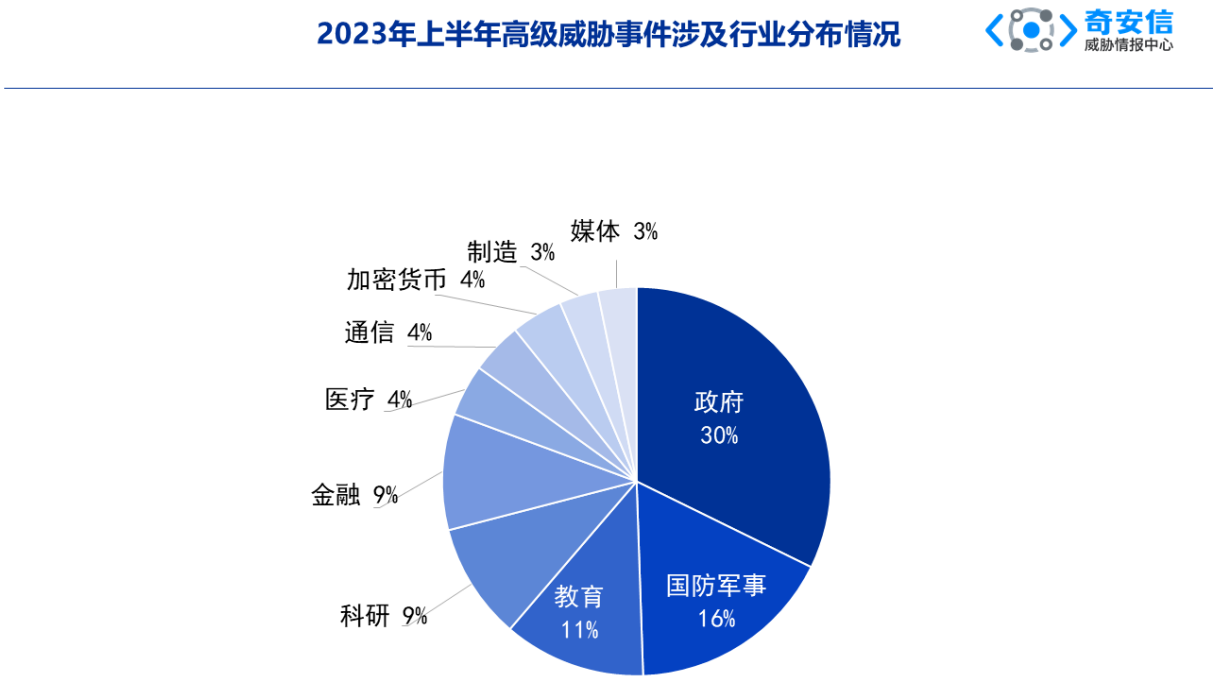
▲ 图 2.1 2023 上半年全球公开的高级威胁报告数量月度统计

二、受害目标的行业与地域

通过对开源情报数据整理分析，在全球 2023 上半年披露的 APT 相关活动报告中，涉及政府（包括外交、政党、选举相关）的攻击事件占比为 30%，其次国防军事相关事件占比为 16%，教育行业占比 11%，

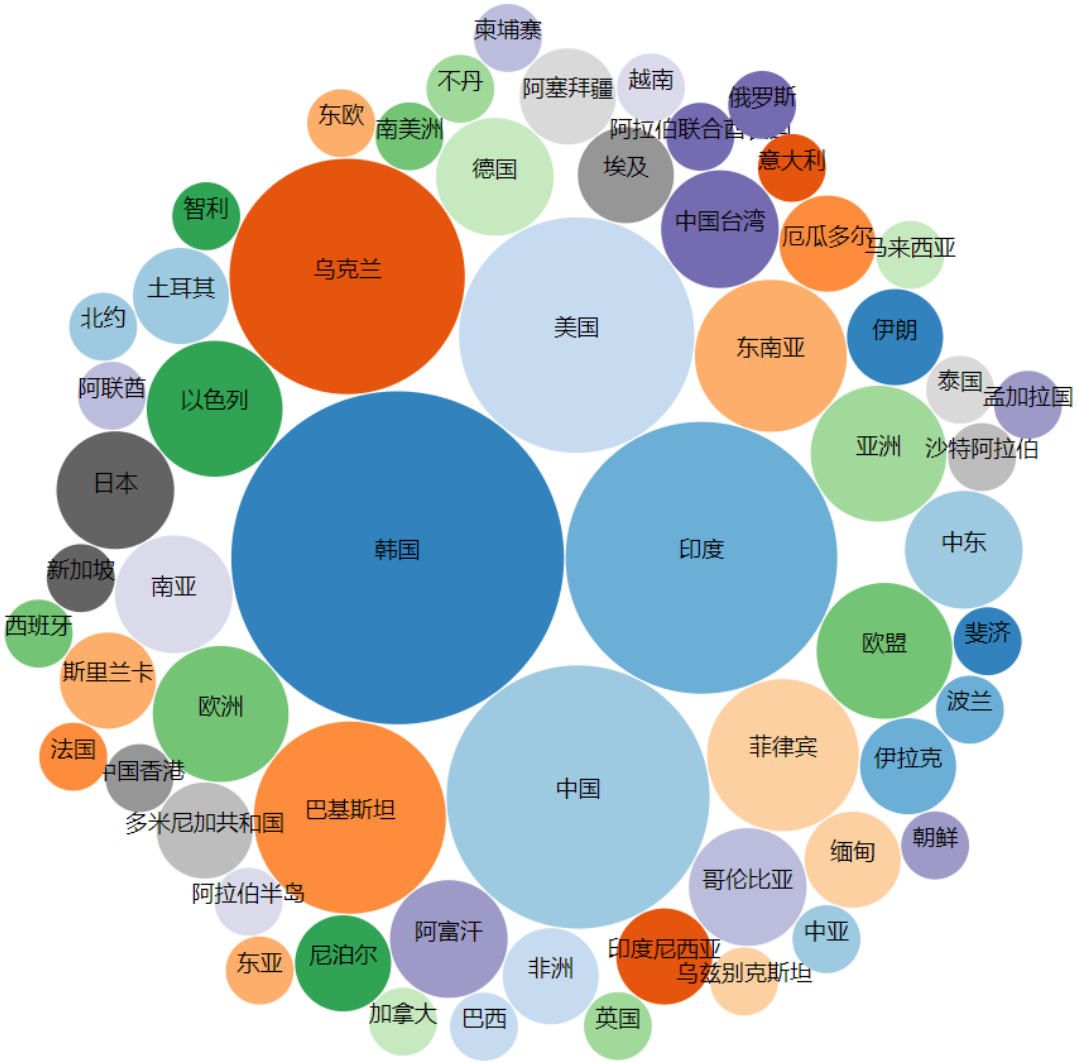
涉及科研、金融行业的占比均为 9%。政府机构、国防军事仍是 APT 攻击的重灾区。与去年相比，教育、科研领域相关的攻击事件所占比例增高。

2023 上半年全球高级威胁事件涉及行业分布情况如下图所示。



▲ 图 2.2 2023 上半年全球高级威胁事件涉及行业分布

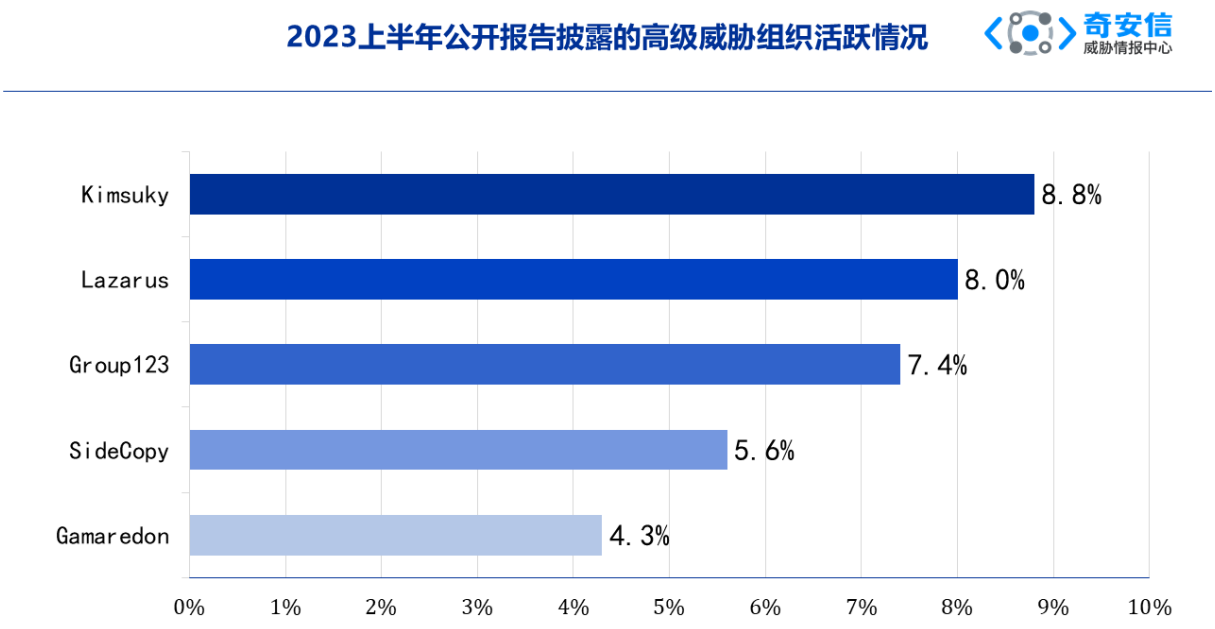
高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到高级威胁攻击活动主要集中在东亚、南亚、东欧的几个国家和地区。



▲ 图 2.3 2023 上半年公开披露的高级威胁活动针对的国家和地区

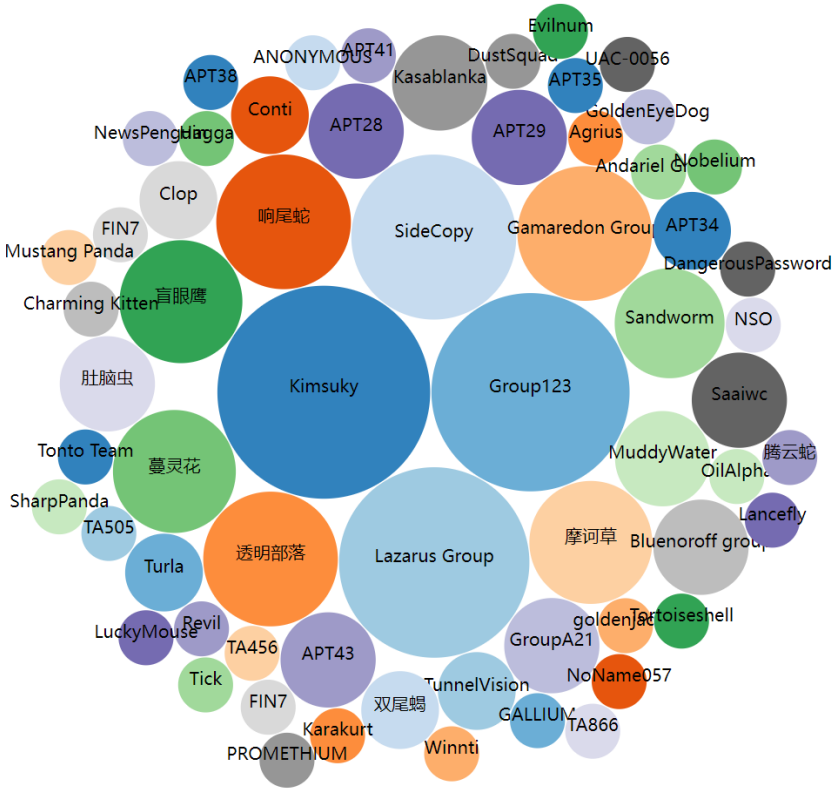
三、活跃高级威胁组织情况

本次报告对开源情报中提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率最高的五个 APT 组织分别是：Kimsuky 8.8%，Lazarus 8.0%，Group123 7.4%，SideCopy 5.6%，Gamaredon 4.3%。



▲ 图 2.4 2023 上半年全球活跃高级威胁组织

进一步对公开报告的高级威胁活动中命名的攻击行动名称、攻击者名称进行统计，并对同一背景来源归类处理后的情况如下，总共涉及 64 个命名的威胁来源。不难看出，这些活跃的 APT 组织所在地域分布相对集中，主要位于东亚、南亚地区。



▲ 图 2.5 2023 上半年公开披露的高级威胁类攻击组织和行动

四、2023 上半年高级威胁活动特点

（一）移动端漏洞攻击风云再起

一直以来，Windows 都是 APT 团伙首要关注的目标平台，而随着近年移动端平台攻击的崛起，针对移动平台 iOS/Android 的 0day 攻击也逐渐增多。相较于 PC 平台，移动端手机在物理上更接近受害者，具备天然的监听优势，同时移动平台中的数据也更加私密且定向。但无论是 iOS 还是 Android 平台，想要实现 0-Click 式的漏洞利用攻击，难度要比传统 PC 平台高上不少，因此能进行相关攻击的团伙通常技术实力积累雄厚或者背靠国家机器。

2023 年 6 月，卡巴斯基披露的 Operation Triangulation[119] 正是这样一起攻击，详细内容可见后文漏洞部分。整个攻击从 2019 年开始，持续了整整四年，其受害者覆盖多个国家的重点企业及重要人物，波及范围之大令人瞠目。

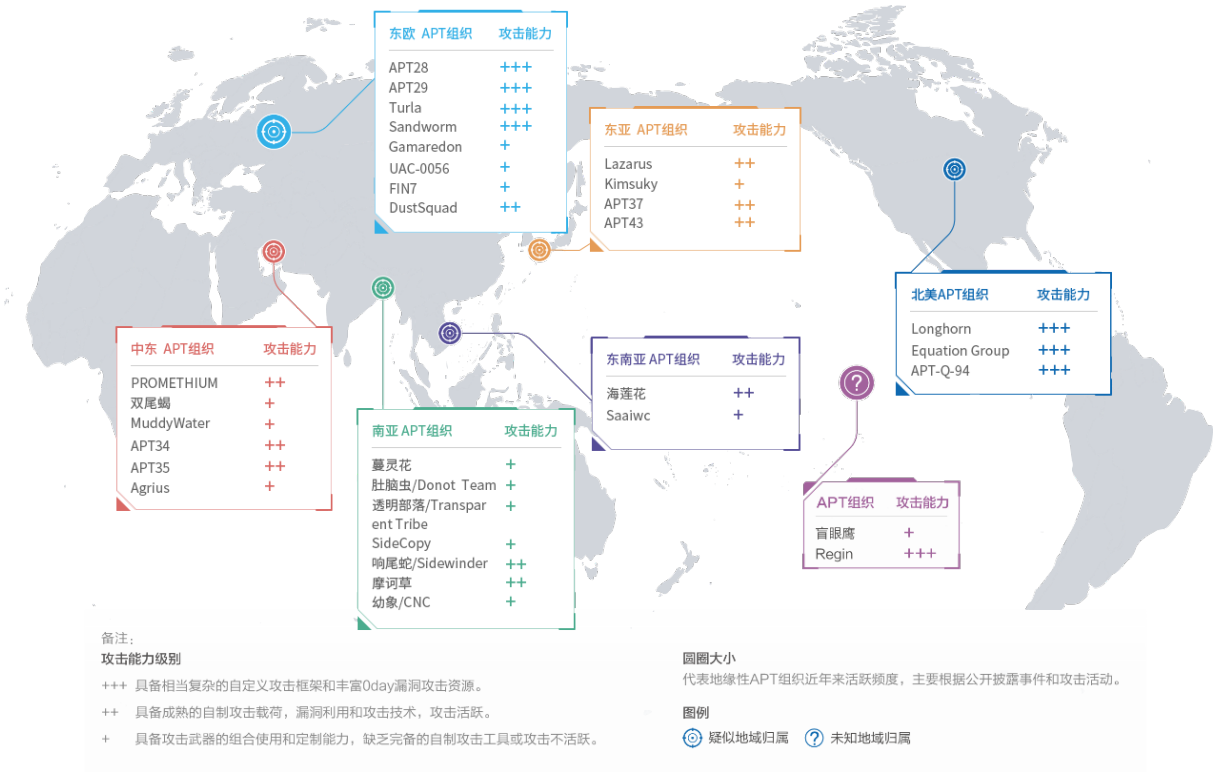
（二）网络设备成为廉价的 C2 屏障及攻击向量

传统的网络设备，如路由器、防火墙等常位于企业网络拓扑的关键位置，但长期以来这些设备的安全性都没得到足够的重视。尽管 NSA 针对防火墙的攻击武器早于 2017 年曝光，实际上关注这些网络设备本身安全性的人员并不多。此外，由于质保过期等各种原因，很多网络设备的安全补丁甚至处于非常滞后的状态，因此近年来网络设备成为了很多 APT 攻击者的目标，如海莲花、APT28，他们都经常攻击一些外网上存在漏洞的网络设备。被攻陷的网络设备一方面可以作为 C2 的转发器，用于隐藏攻击者的真实 IP，另一方面也可以作为攻击入口进行更深入的横向移动。

第三章 地缘下的APT组织、活动和趋势

地域分析是 APT 研究的重要方面。一方面，同一地域范围的 APT 组织和 APT 活动常常出现一些重叠，其可能针对相似的攻击目标或者使用类似的 TTP；另一方面，同一地区发生的很多 APT 活动，都与地缘政治因素密切相关，这对分析 APT 活动的意图和动机很有帮助。

图 3.1 列举了 2023 上半年全球各地区主要活跃的 APT 组织，全球主要 APT 组织列表也可以参见附录 1。

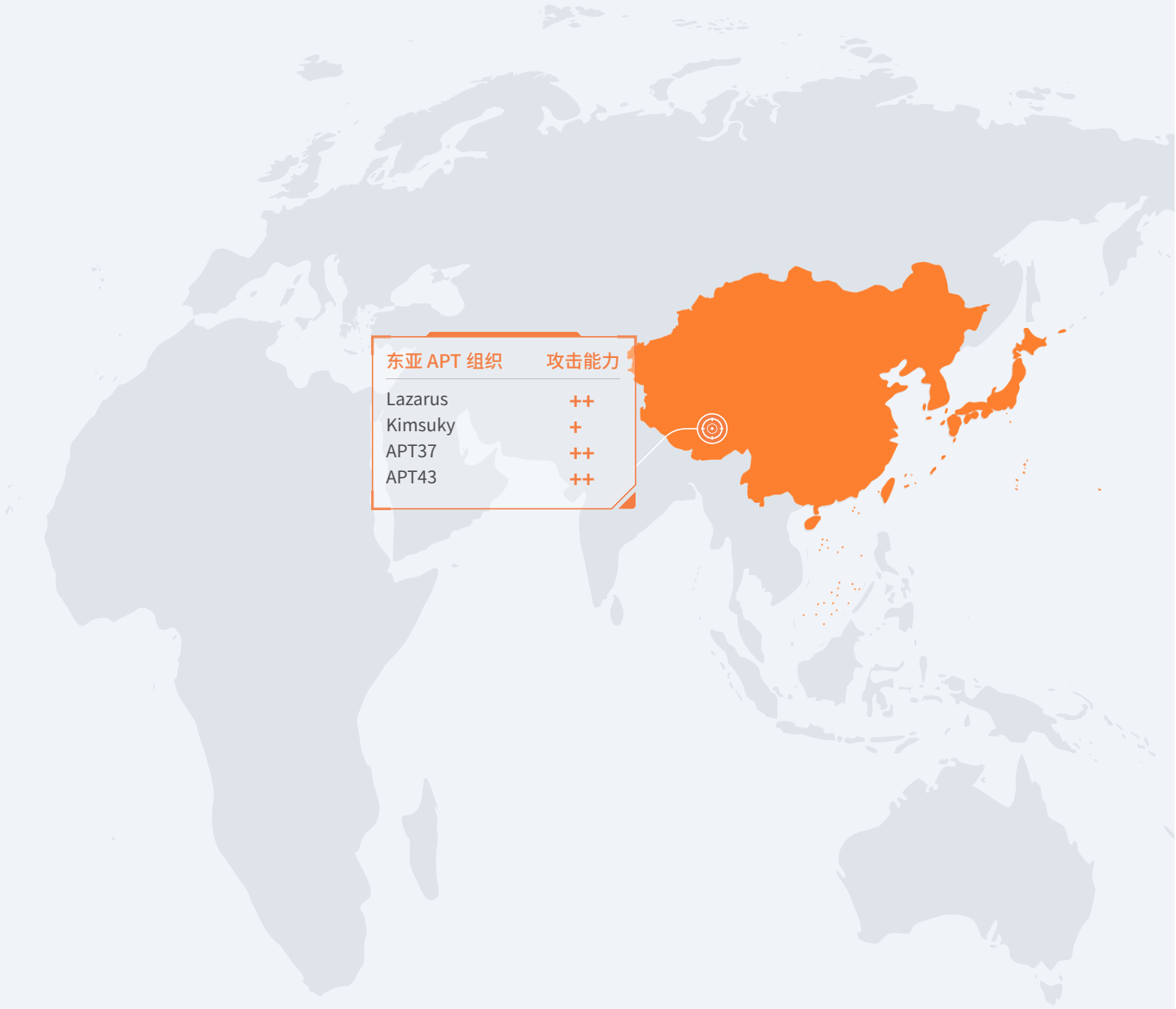


▲ 图 3.1 2023 上半年全球 APT 组织分布情况

东亚地区的组织与行动

East Asia

东亚地区 APT 组织以其攻击活动高度的持续性、攻击方式复杂性和隐蔽性而著称，对政府、军事、金融、能源、教育等多个领域构成了严重的威胁。



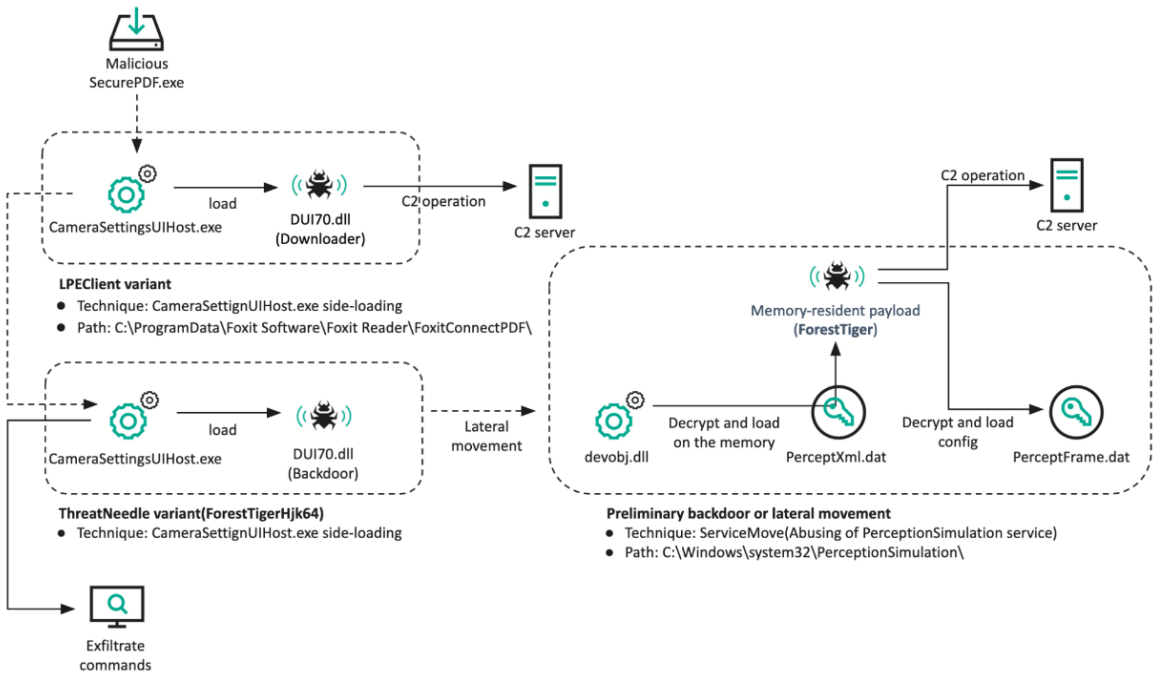
在 2023 年上半年公开披露的东亚地区 APT 组织报告中，我们见证了这些组织所使用的种类繁多的攻击技术，包括复杂的社会工程学手段、供应链攻击、鱼叉式钓鱼攻击和 0day 漏洞攻击等。表 3.2 列出了东亚地区部分 APT 组织的相关信息：

组织名	最早活动时间	公开披露时间	组织简介
Lazarus	2009	2009	Lazarus 组织被认为是地属东亚的 APT 组织，其不仅专注于间谍和网络渗透攻击，还以金融机构、虚拟货币交易所等为目标，进行以敛财为目的的攻击活动。
Kimsuky	2013	2013	Kimsuky 最早由卡巴斯基于 2013 年公开披露并命名，攻击活动最早可追溯至 2012 年。其被认为具有东亚地区背景，与 Group123 APT 组织存在基础设施重叠等关联性。
APT37	2012	2016	Group123，也称 ScarCruft，在 2016 年 6 月由卡巴斯基最先进行披露，最早活跃于 2012 年，该组织被认为与 2016 年的 Operation Daybreak 和 Operation Erebus 有关。Group123 和 APT 组织 Kimsuky 存在特征重叠。
APT43	2018	2023	Mandiant 自 2018 年以来一直在跟踪该组织，该组织进行间谍活动的重点区域是韩国、日本、欧洲和美国 , 攻击目标包括政府、商业服务和制造业，以及专注于地缘政治和核政策的教育、研究和智库。

▲ 表 3.2 2023 上半年东亚地区活跃 APT 组织

在 2023 年上半年，Lazarus 组织继续以金钱和情报窃取为驱动力，对加密货币、金融、国防等行业进行了更加激烈的攻击。在公开披露的活动中，Lazarus 组织不仅利用加密货币钱包作为攻击手段，还将目标扩大到卫星通信接收器和调制解调器等领域。特别值得注意的是，2023 年 3 月 29 日，各大安全公司纷纷报道了涉及 3CXDesktopApp 音视频会议软件的供应链攻击事件，后续 CrowdStrike、Kaspersky、Volexity 等安全厂商证实攻击源自 Lazarus 组织。这一事件凸显了该组织在攻击策略和手段方面的持续创新和进步。

另外，Kaspersky 在 2023 年 4 月 12 日发布的博客中指出，他们在追踪由 Lazarus 组织展开的 DeathNote 攻击活动中观察到该组织在攻击目标上的转变以及攻击者在使用工具、技战术流程方面的发展和完善。该活动将攻击重点转移到国防工业领域，并采用了新的感染媒介和策略，以针对国防承包商进行攻击。Lazarus 组织的持续活动显示出其在网络攻击领域的专业能力和资源支持。该组织不断改进攻击技术，使其成为一个对东亚地区甚至全球范围内的经济、金融和国防安全都极具威胁的存在。



▲ 图 3.3 Lazarus 组织针对国防承包商的攻击链 [1]

Kimsuky 组织在 2023 年上半年继续扩大攻击面，尤其该组织在移动端的恶意活动更是频繁。他们擅长利用社会工程学手段进行攻击，并根据时事热点制作诱饵。为增加诱饵的吸引力和成功率，他们通常针对特定的个人、组织或行业对诱饵进行定制化，利用精心设计的诱饵诱使用户点击恶意链接或下载恶意应用以展开定向攻击。Kimsuky 组织采用多种手段来获取特定数据，包括使用钓鱼网站或者植入恶意软件。其钓鱼网站通常伪装成合法的应用或服务，引诱用户提供敏感信息，例如登录凭据、银行账户信息等。此外，他们还会利用植入的恶意代码实现敏感数据窃取或远程监控。

APT37 常采用钓鱼邮件作为初始入侵手段，或者攻陷合法 Web 站点然后展开水坑攻击。该组织擅长利用 0day/Nday 漏洞，并具备漏洞利用开发的技术。APT37 去年曾利用 Internet Explorer 的 JScript 引擎中的 0day 漏洞 CVE-2022-41128 对东亚某国发起攻击。

2023 年上半年，APT37 不断改进其工具和技战术流程，利用多种文件格式执行恶意操作，使用过的文件格式包括 Windows 帮助文件（CHM）、HTA、HWP（Hancom Office）、XLL（MS Excel 插件）和携带宏的 MS Office 文件。APT37 组织还使用 ISO 文件对韩国外交部门进行情报窃取。在此次攻击活动中，投递的 ISO 文件包含两个带有大量无效填充数据的 LNK 文件，运行后释放 HWP 诱饵文档及 BAT 文件，然后执行 Powershell 命令下载后续恶意载荷，最终解密 RokRAT 并与合法的云服务 pCloud 进行通信，获取攻击者下发的恶意指令并执行。

APT43 于今年 3 月份由 Mandiant 披露 [2]。Mandiant 的报告显示 APT43 一直保持着高节奏的活动，在网络钓鱼和凭证收集方面表现出色。它的攻击目标主要集中在韩国、美国、日本和欧洲等区域，并特别关注政府、教育、研究和智库领域，尤其是地缘政治、核政策、商业服务和制造业。除了进行间谍活动外，APT43 还通过网络犯罪活动筹集资金，以支持其情报窃取的主要任务。该组织创造了许多虚假的个人身份信息用于实施社会工程学攻击，或者用于购买操作工具和网络基础设施。

组织名	活动描述	披露时间	披露机构
Kimsuky	Kimsuky 移动端恶意活动瞄向韩国东亚研究所国家安全主任 [3]	2023/1/1	安天
Lazarus	疑似 APT-C-26（Lazarus）组织通过加密货币钱包推广信息进行攻击活动分析 [4]	2023/1/11	360
APT38	TA444：旨在收购（您的资金）的 APT 初创公司 [5]	2023/1/25	Proofpoint
Lazarus	黑客攻击印度医疗机构和能源部门 [6]	2023/2/2	Withsecure
APT37	使用隐写术的韩文 (HWP) 恶意软件：RedEyes[7]	2023/2/14	ASEC
Lazarus	Lazarus 组织使用的反取证技术 [8]	2023/2/15	ASEC
Lazarus	WinorDLL64：来自庞大的 Lazarus 武器库的后门 [9]	2023/2/23	Welivesecurity
Kimsuky	Kimsuky 最新网络钓鱼攻击披露，韩国主流金融 APP 成重灾区 [10]	2023/3/3	安天
Kimsuky	伪装成朝鲜相关问卷的 CHM 恶意软件 [11]	2023/3/13	ASEC
Kimsuky	Kimsuky 试图伪装成“网络安全局”邮件进行黑客攻击 [12]	2023/3/14	ESTsecurity
Kimsuky	Kimsuky 组织伪装成“协议离婚意向确认申请书”分发 QuasarRAT[13]	2023/3/15	ESTsecurity
Kimsuky	Kimsuky 组织似乎正在像网络犯罪团伙一样利用 OneNote[14]	2023/3/17	Medium
APT37	APT37 攻击向量一瞥 [15]	2023/3/21	Zscaler
Lazarus	GhostSec 瞄准卫星接收器 [16]	2023/3/27	Cyble
APT37	APT Reaper 强大武器的 Chinotto 后门技术分析 [17]	2023/3/28	Threatmon
APT43	APT43：利用网络犯罪资助间谍活动 [18]	2023/3/28	Mandiant
Kimsuky	Kimsuky Group 使用 ADS 隐藏恶意软件 [19]	2023/3/29	ASEC
Lazarus	通过 3CX 供应链攻击部署 Gopuram 后门 [20]	2023/4/3	Kaspersky
APT43	保护用户免受来自东亚 APT 组织的攻击 [21]	2023/4/5	Google
Lazarus	跟踪 Lazarus 组织的 DeathNote 活动 [22]	2023/4/12	Kaspersky

组织名	活动描述	披露时间	披露机构
APT43	APT43：对其网络犯罪活动的调查 [23]	2023/4/20	VirusTotal
Lazarus	Linux 恶意软件加强了 Lazarus 与 3CX 供应链攻击之间的联系 [24]	2023/4/20	Welivesecurity
Lazarus	BlueNoroff APT 团伙使用“RustBucket”恶意软件针对 macOS[25]	2023/4/21	Jamf
APT37	APT37 针对韩国外交部下发 RokRAT 的窃密活动分析 [26]	2023/4/28	安恒
APT37	连锁反应：ROKRAT 的缺失环节 [27]	2023/5/1	Checkpoint
Kimsuky	Kimsuky 在新的全球战役中发展侦察能力 [28]	2023/5/4	Sentinelone
Kimsuky	Kimsuky 组织使用 Meterpreter 攻击 Web 服务器 [29]	2023/5/15	ASEC
APT37	ScarCruft 组织利用恶意文档投递 RokRat 攻击活动分析 [30]	2023/5/19	360
APT37	冒充朝鲜人权组织负责人针对朝鲜人权领域代表进行的鱼叉式网络钓鱼攻击 [31]	2023/5/23	Genians
Lazarus	Lazarus 组织以 Windows IIS Web 服务器为目标 [32]	2023/5/23	ASEC
Kimsuky	Kimsuky：使用量身定制的侦察工具包进行持续的活动 [33]	2023/5/23	Sentinelone
APT37	逆向 RokRAT：深入了解 APT37 基于 Onedrive 的攻击向量 [34]	2023/5/31	Threatmon
Kimsuky	网络攻击者冒充目标收集情报 [35]	2023/6/1	NSA
Kimsuky	假借“生日祝福”为诱饵分发 Quasar RAT 的攻击活动分析 [36]	2023/6/5	360

▲ 表 3.4 2023 上半年东亚地区 APT 组织热点攻击活动

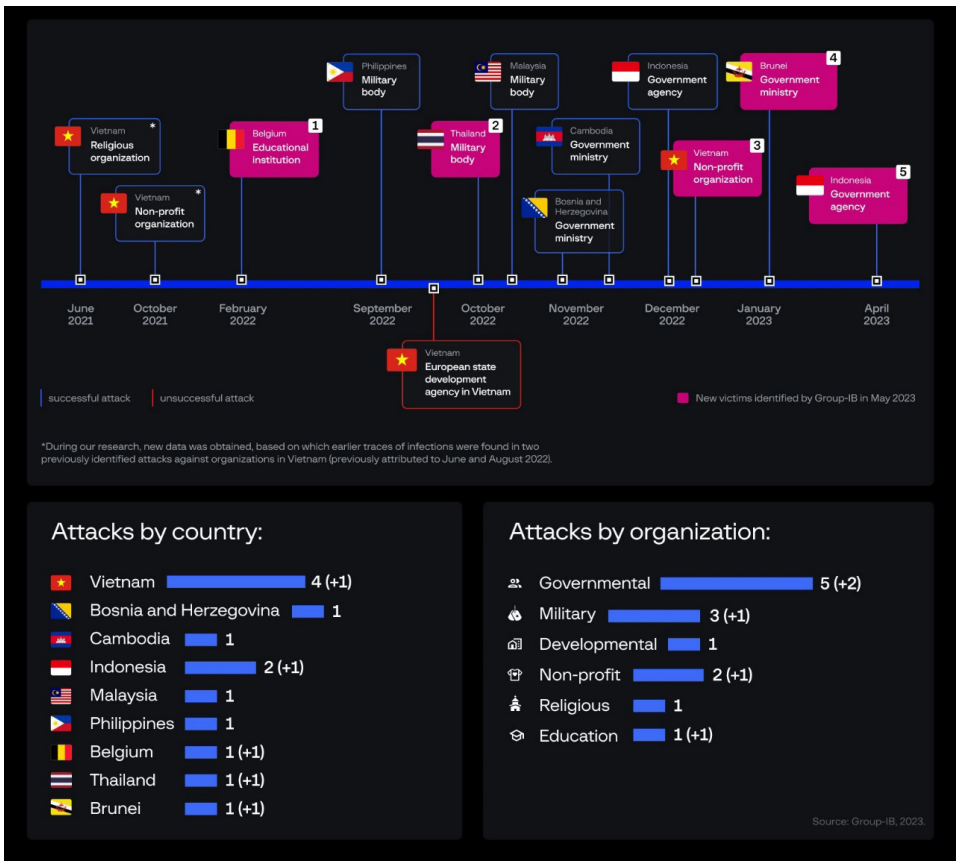
东南亚地区的组织与行动
Southeast Asia

2023 年上半年，一个有着独特 TTP 的攻击团伙 Saaiwc（别名 DarkPink）出现在大众视野中，目标包括东南亚和欧洲多国的政府机构、军事部门。海莲花组织在今年上半年被披露的活动迹象减少，疑似曾针对越南几家大型企业展开情报收集行动。

组织名	最早活动时间	公开披露时间	组织简介
海莲花	2012	2015	海莲花组织是由奇安信威胁情报中心最早披露并命名的一个 APT 组织，其自 2012 年 4 月起，该组织针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。 海莲花组织的攻击目标包括中国和东南亚地区多国，覆盖政府机构、科研院所、媒体、企业等诸多领域。
Saaiwc	2021	2023	Saaiwc 组织又名 DarkPink，于 2023 年 1 月由国内外安全厂商先后披露，活动时间可追溯至 2021 年年中，在 2022 年进入攻击活动高发期。 该组织的攻击目标包括越南境内的宗教、非营利组织，马来西亚、印度尼西亚、柬埔寨、菲律宾、泰国、文莱等东南亚国家的政府和军事机构，以及欧洲国家的政府、教育机构。

▲ 表 3.5 2023 上半年东南亚地区活跃 APT 组织

Saaiwc 组织攻击范围较广，除了东南亚地区多国的政府、军事机构，还涉及欧洲国家波黑的政府机构、比利时的教育机构，以及越南境内的宗教和非营利组织，国外安全厂商还观察到 Saaiwc 曾对欧洲国家发展署位于越南的部门发起攻击，尽管并未成功。



▲ 图 3.6 安全厂商 Group-IB 发现的 Saaiwc 组织攻击目标 [42]

Saaiwc 组织以鱼叉式钓鱼邮件作为初始入侵手段，恶意文件常包含在 ISO 文件中进行投递。其拥有一

套自研的攻击武器，常用 Powershell 脚本，借助 Github 托管后续载荷，后门通过 Telegram API 接收攻击者下发的控制指令。

该组织使用的自研攻击武器如下 [38, 42]：

组织名	最早活动时间
TelePowerBot	Powershell 后门，也被其他安全厂商称为 PowerDism，使用 Telegram API 进行 C2 通信，具有收集信息、执行后续载荷的功能
KamiKakaBot	C# 版本的 TelePowerBot
Cucky	C# 开发的浏览器窃密工具，收集多种浏览器的数据，包括密码、浏览记录、登录信息和 cookie，收集的数据保存在感染设备的指定目录下，由后门完成数据回传
Ctealer	C/C++ 版本的 Cucky
ZMsg	获取感染设备上 Viber、Telegram、Zalo 等通讯软件的数据，收集的数据保存在指定目录下，等待后门完成数据回传
某 Excel 插件	用于检查感染设备上 TelePowerBot 后门是否还存在，当 Excel 启动时执行检查操作。 关键字符串经过 XOR 加密，加密的 key 由进程名和打开文件后缀名两个参数计算得到，只有当进程名为“excel.exe”且文件后缀为“.xlsx”时，才会得到正确的解密 key。

▲ 表 3.7 Saaiwc 组织的自研攻击武器

Saaiwc 组织植入后门的方式有三种。

(1) 方式一

ISO 文件中包含诱饵文档、EXE 文件和恶意 DLL 文件。EXE 文件伪装为文档诱使受害者点击运行，通过 DLL 侧加载执行恶意 DLL 文件。恶意 DLL 文件实现后门 TelePowerBot 的持久化。

采用的持久化方式比较特殊，注册表中设置的自启动项会打开“.abcd”后缀的文件，而在注册表中为“.abcd”后缀文件设置的默认打开方式，则包含了 TelePowerBot 后门代码和启动后门的指令。

(2) 方式二

ISO 文件中包含诱饵文档，诱饵文档通过远程模板注入的方式加载托管在 Github 上带有恶意宏代码的文档，宏代码完成 TelePowerBot 的持久化，与方式一相同。

(3) 方式三

ISO 文件中包含诱饵文档、EXE 文件和恶意 DLL 文件，通过 DLL 侧加载执行恶意 DLL 文件，恶意 DLL 文件实现后门 KamiKakaDropper 的持久化。

恶意 DLL 从诱饵文档中解密出 XML 文件，释放的 XML 文件包含 MSBuild 项目，也包含经过编码的

KamiKakaBot 后门数据。持久化方式为设置注册表，使用户登录系统时调用 msbuild.exe 运行释放的 XML 文件。此外恶意 DLL 还会创建一个周期任务让受害者从系统中登出。

Saaiwc 组织使用的后门检测到感染主机有 U 盘插入或存在网络共享时，会从 Github 下载包含后门程序的压缩包，在 U 盘和网络共享文件夹中创建 LNK 文件伪装为原始文件或文件夹，LNK 文件包含的命令启动后门程序释放器，完成后门在新设备上的持久化。攻击者通过这种方式实现在受害者网络内部的恶意软件传播和横向移动。

攻击者从感染设备上收集的所有数据保存在指定目录中，数据不会立马回传，而是当攻击者下发指令时才将其打包回传。数据回传渠道除了 Telegram，还有 Dropbox，在一些攻击活动中也曾使用过邮件方式回传，攻击者还在近期攻击中借助 Webhook.site 网站服务回传窃取的数据。

Saaiwc 组织常在攻击过程中使用 LOLBin，比如曾用 Windows Defender 的 ConfigSecurityPolicy.exe 组件下载文件。攻击者在渗透过程中会检查感染设备上是否有特定的 LOLBin 文件存在，方便用于之后的恶意代码执行和下载操作。

在 2023 年 1 月公开披露前，Saaiwc 组织攻击链中使用的后续载荷托管在同一个 Github 账户下，曝光后攻击者除了使用新的 Github 账户，也使用 TextBin.net 网站服务分发后续载荷。

2023 年 6 月，Elastic 安全团队披露一起针对越南农业企业的攻击活动 [43]，此次攻击中发现的几款新型恶意软件也出现在 2022 年另一起针对越南金融服务公司的攻击活动中。研究人员认为，两起攻击活动可能与海莲花组织具有一定联系。攻击者使用的几种恶意软件如下：

组织名	最早活动时间
SPECTRALVIPER	经过混淆的 x64 后门，具有的功能包括：PE 加载和注入、文件上传和下载、文件和目录操纵、令牌模拟、命名管道和 HTTP C2 控制
P8LOADER	经过混淆的 Windows PE 文件加载器，并能减少和混淆攻击者在受害者终端上留下的一些日志记录
POWERSEAL	C# 开发的 Powershell 脚本运行器，对 Windows 的日志跟踪和反病毒扫描服务进行内存 patch，以绕过检测

▲ 表 3.8 攻击越南大型企业的恶意软件

奇安信威胁情报中心整理了 2023 上半年公开披露的东南亚地区 APT 组织的主要攻击活动，如下表所示。

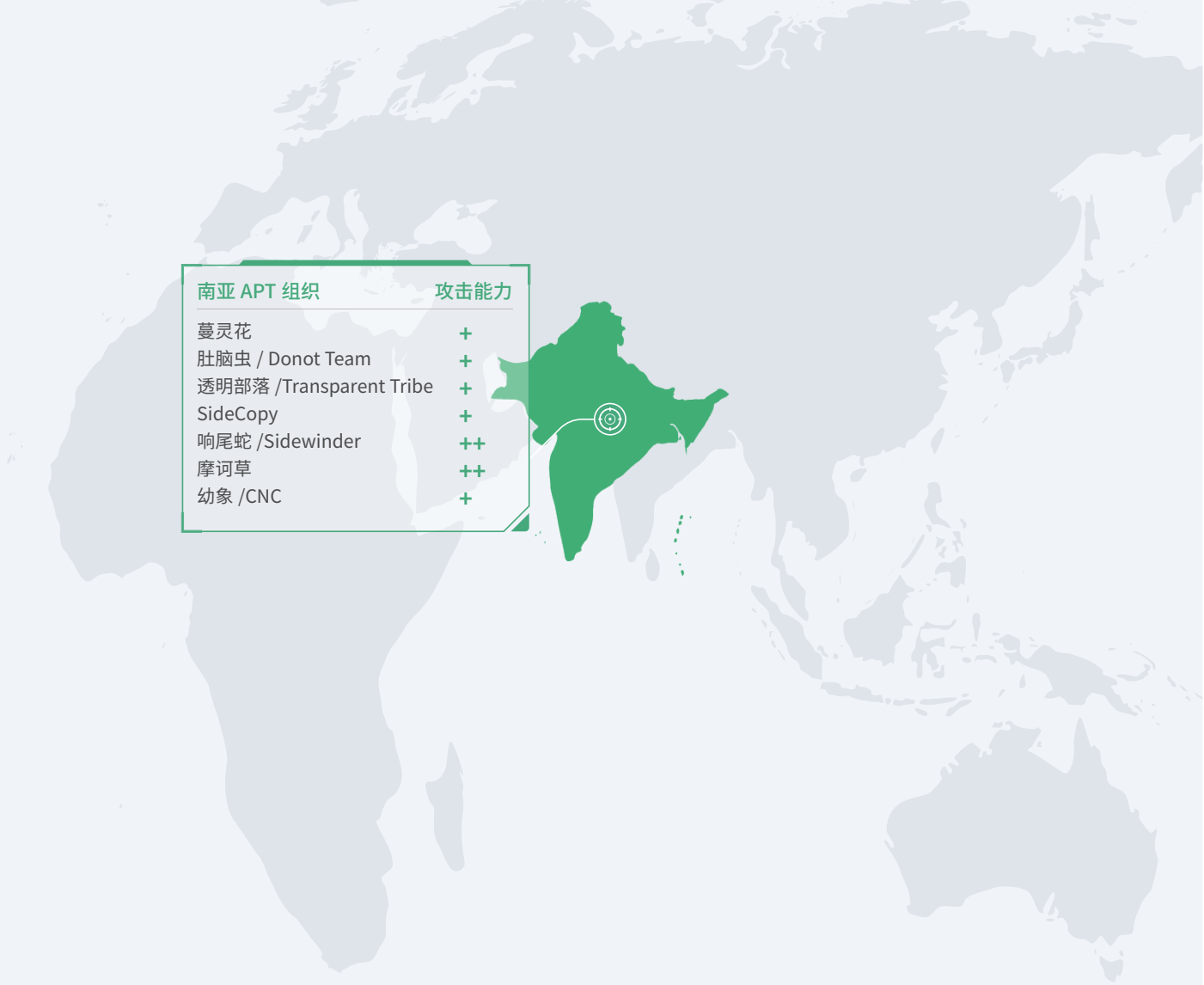
组织名	活动描述	披露时间	披露来源
Saaiwc	Saaiwc 组织针对东南亚军事、财政等多部门的攻击活动分析 [37]	2023-01-06	安恒

组织名	活动描述	披露时间	披露来源
Saaiwc	DarkPink 攻击亚太地区和欧洲 [38]	2023-01-11	Group-IB
Saaiwc	Saaiwc 组织攻击马来西亚、印度尼西亚外交部 [39]	2023-02-13	安恒
Saaiwc	Saaiwc 组织针对印尼政府的攻击活动分析 [40]	2023-03-15	360
Saaiwc	DarkPink 组织针对印度尼西亚外交部门和菲律宾军事部门的攻击活动 [41]	2023-03-20	安天
Saaiwc	DarkPink 组织的多个新受害者 [42]	2023-05-31	Group-IB
未知（疑似海莲花）	SPECTRALVIPER 恶意软件攻击越南大型企业 [43]	2023-06-09	Elastic

▲ 表 3.9 2023 上半年东南亚地区 APT 组织热点攻击活动

南亚地区的组织与行动
South Asia

根据 2023 上半年公开报告整理结果，活跃于南亚地区的 APT 组织依然是该地区的几个老牌 APT 组织，即透明部落、蔓灵花、响尾蛇和摩诃草。表 3.10 为 2023 上半年南亚地区活跃的 APT 组织简介。



南亚 APT 组织	攻击能力
蔓灵花	+
肚脑虫 / Donot Team	+
透明部落 /Transparent Tribe	+
SideCopy	+
响尾蛇 /Sidewinder	++
摩诃草	++
幼象 /CNC	+

组织名称	最早活动时间	公开披露时间	组织简介
蔓灵花	2013	2016	主要针对巴基斯坦、中国两国，其攻击目标为政府部门、电力、军工业相关单位，意图窃取敏感资料，并与摩诃草、魔罗杪存在关联。奇安信内部跟踪编号为 APT-Q-37
肚脑虫	2016	2017	主要针对巴基斯坦、中国、斯里兰卡等南亚地区国家，对政府机构、国防军事部门以及商务领域重要人士实施网络间谍活动。主要使用 yty 和 EHDevel 两套恶意框架。奇安信内部跟踪编号为 APT-Q-38
透明部落 (Transparent Tribe)	2012	2016	主要针对印度政府、军队或相关组织，以及巴基斯坦的激进分子和民间社会，利用社会工程学进行鱼叉攻击，同时也会在移动端发起攻击
SideCopy	2019	2020	主要针对印度、巴基斯坦和阿富汗，以政府、国防、军事等相关组织人员为目标进行网络间谍活动。因其攻击手法主要复制 Sidewinder 及其他 APT 组织的 TTP 而得名
响尾蛇 (Sidewinder)	2012	2018	主要针对巴基斯坦、中国、阿富汗、尼泊尔、孟加拉等国家展开攻击，旨在窃取政府外交机构、国防军事部门、高等教育机构等领域的机密信息。常使用已知漏洞 (CVE-2017-11882) 开展攻击活动。奇安信内部跟踪编号为 APT-Q-39
摩诃草	2009	2013	主要针对中国、巴基斯坦等亚洲地区国家，以政府、军事、电力、工业、外交和经济等领域为主窃取敏感信息。具备 Windows、Android、macOS 三平台攻击能力。奇安信内部跟踪编号为 APT-Q-36
幼象 (CNC, GroupA21)	2017	2019	GroupA21 最早由国内安全公司命名，至少自 2017 年开始活动，主要针对南亚地区各国开展网络间谍活动。该组织的攻击手法与印度背景的 Sidewinder 和 Bitter 组织存在相似之处，但在攻击细节和所用木马方面有着明显的区别

▲ 表 3.10 2023 上半年南亚地区活跃 APT 组织

从 2023 年上半年的公开报告所披露的活动来看，南亚地区各 APT 组织活跃度较往年并未出现太大波动，蔓灵花、响尾蛇、摩诃草以及透明部落一直处于高度活跃的状态。

肚脑虫组织在 2023 年发起多次针对印度克什米尔地区的攻击，攻击中使用的恶意样本涉及 Windows 和 Android 平台。Windows 平台上的样本虽然还是保持着一贯的攻击流程，但是也在尝试不同的恶意代码植入手段，修改了些许攻击组件的代码细节。Android 平台上的样本多数伪装成聊天应用程序，但并不具备正常聊天程序的功能，样本代码经过高度混淆，恶意程序运行后向用户请求访问权限，取得权限后上传联系人信息、通话记录、地理位置等信息到 C2 服务器。

CNC 组织针对国内、巴基斯坦、菲律宾、印度尼西亚等国家的教育科研机构发起攻击。该组织投递的恶意软件检测感染主机是否接入新的驱动器，在接入新驱动器（如 U 盘）后将自身复制过去进行摆渡攻击。在针对国内的攻击中，CNC 组织常伪装为“YoudaoDictDesk.exe”等常用软件，并使用伪造的国内邮箱创建自签名证书。

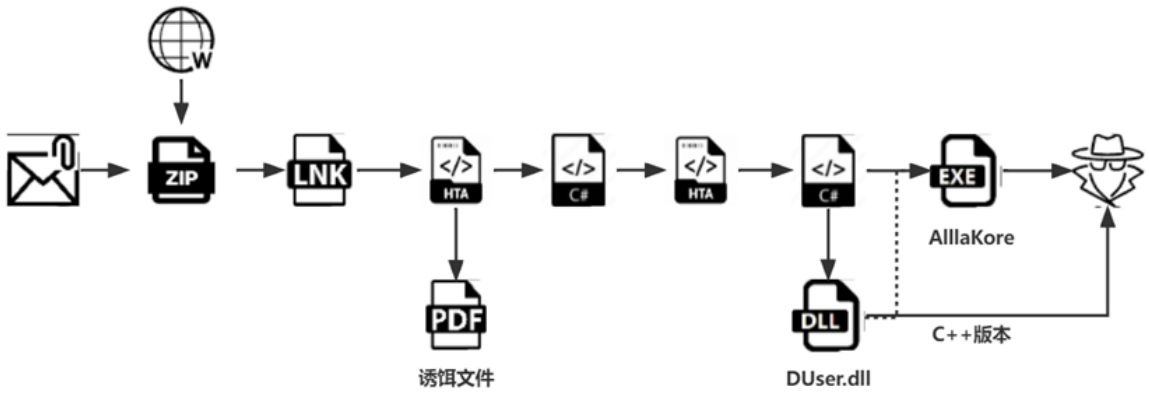
透明部落今年上半年依然活跃，攻击活动多针对印度和巴基斯坦公民，通过简历作为诱饵下发 CrimsonRAT 或者通过钓鱼网站传播恶意 Android 应用。

响尾蛇 APT 组织先后使用“2023 年巴基斯坦海军学院”、“暗网敏感数据泄露”、“公共管理学院工作安排调整通知”等诱饵发起了针对巴基斯坦、中国、尼泊尔、斯里兰卡等国家的攻击，仍通过远程模板注入、CVE-2017-11882 漏洞等方式下载后续载荷。

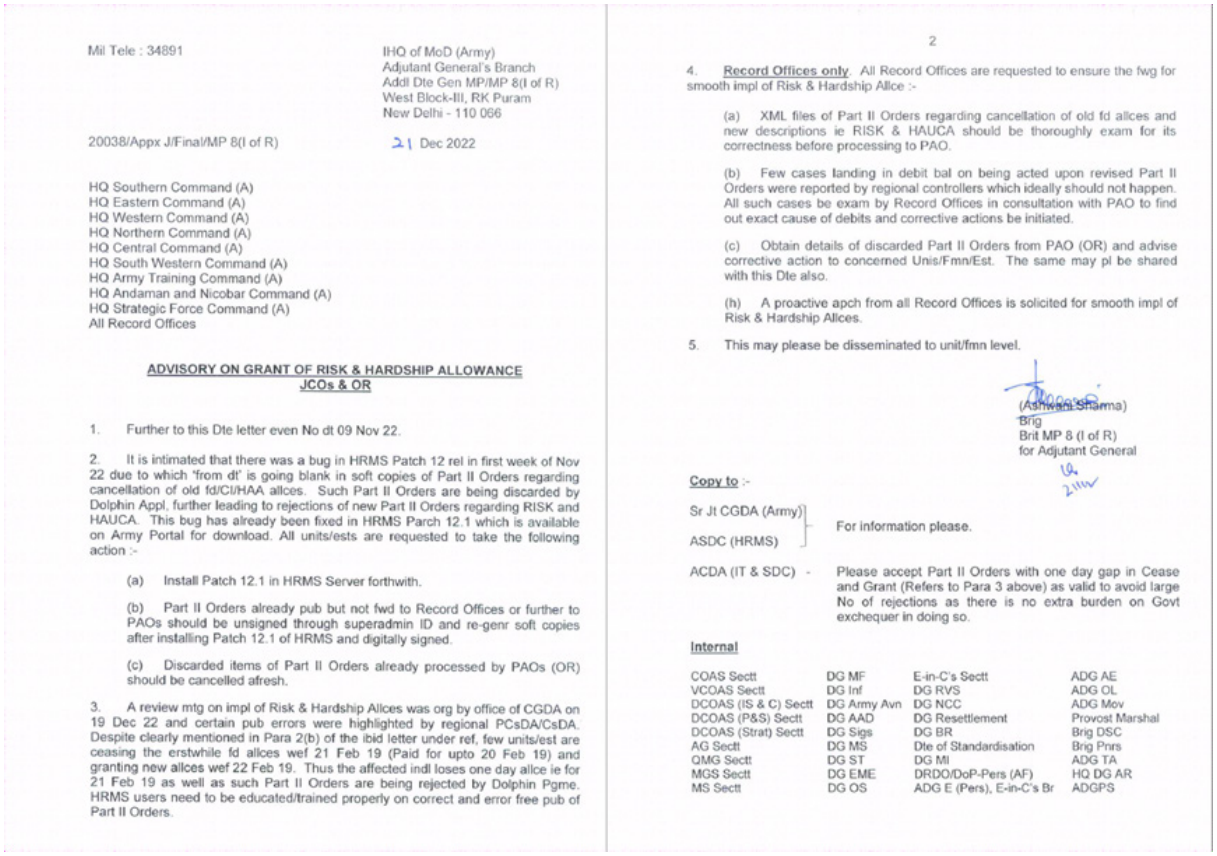
蔓灵花组织伪装为吉尔吉斯大使馆发起了多次针对中国、巴基斯坦等国家的国防、能源部门的攻击，植入恶意软件的手法依然是使用 CHM 文件或 Office 公式编辑器漏洞。

摩诃草组织以“先进结构与复合材料等 4 个重点专项 2023 年度项目申报指南的通知”、“长江设计集团有限公司 2023 年度招聘公告”为诱饵针对我国发起多次攻击，频繁使用开源或商业木马如“NorthStarC2”、“Remcos”等。

自 2023 年 3 月起，奇安信威胁情报中心捕获了一批与 SideCopy 组织有关的攻击样本，SideCopy 的感染链与之前的攻击活动大体一致，以恶意 LNK 文件作为攻击入口，最终载荷使用了新的木马。



▲ 图 3.11 SideCopy 组织攻击活动执行流程 [55]



Mil Tele : 34891

IHQ of MoD (Army)
Adjutant General's Branch
Addl Dte Gen MP/MP 8(I of R)
West Block-III, RK Puram
New Delhi - 110 066

20038/Appx J/Final/MP 8(I of R) 21 Dec 2022

HQ Southern Command (A)
HQ Eastern Command (A)
HQ Western Command (A)
HQ Northern Command (A)
HQ Central Command (A)
HQ South Western Command (A)
HQ Army Training Command (A)
HQ Andaman and Nicobar Command (A)
HQ Strategic Force Command (A)
All Record Offices

ADVISORY ON GRANT OF RISK & HARDSHIP ALLOWANCE JCOs & OR

1. Further to this Dte letter even No dt 09 Nov 22.

2. It is intimated that there was a bug in HRMS Patch 12 rel in first week of Nov 22 due to which 'from dt' is going blank in soft copies of Part II Orders regarding cancellation of old fd/Cl/HAA allces. Such Part II Orders are being discarded by Dolphin Appl, further leading to rejections of new Part II Orders regarding RISK and HAUCA. This bug has already been fixed in HRMS Parch 12.1 which is available on Army Portal for download. All units/ests are requested to take the following action :-

(a) Install Patch 12.1 in HRMS Server forthwith.

(b) Part II Orders already pub but not fwd to Record Offices or further to PAOs should be unsigned through superadmin ID and re-genr soft copies after installing Patch 12.1 of HRMS and digitally signed.

(c) Discarded items of Part II Orders already processed by PAOs (OR) should be cancelled afresh.

3. A review mtg on impl of Risk & Hardship Allces was org by office of CGDA on 19 Dec 22 and certain pub errors were highlighted by regional PCsDA/CsDA. Despite clearly mentioned in Para 2(b) of the ibid letter under ref, few units/est are ceasing the erstwhile fd allces wef 21 Feb 19 (Paid for upto 20 Feb 19) and granting new allces wef 22 Feb 19. Thus the affected indl loses one day allce ie for 21 Feb 19 as well as such Part II Orders are being rejected by Dolphin Pgme. HRMS users need to be educated/trained properly on correct and error free pub of Part II Orders.

2

4. **Record Offices only**. All Record Offices are requested to ensure the fwg for smooth impl of Risk & Hardship Allce :-

(a) XML files of Part II Orders regarding cancellation of old fd allces and new descriptions ie RISK & HAUCA should be thoroughly exam for its correctness before processing to PAO.

(b) Few cases landing in debit bal on being acted upon revised Part II Orders were reported by regional controllers which ideally should not happen. All such cases be exam by Record Offices in consultation with PAO to find out exact cause of debits and corrective actions be initiated.

(c) Obtain details of discarded Part II Orders from PAO (OR) and advise corrective action to concerned Units/Fmn/Est. The same may pl be shared with this Dte also.

(h) A proactive apch from all Record Offices is solicited for smooth impl of Risk & Hardship Allces.

5. This may please be disseminated to unit/fmn level.

(Ashwani Sharma)
Brig
Brit MP 8 (I of R)
for Adjutant General

Copy to :-

Sr Jt CGDA (Army)
ASDC (HRMS) — For information please.

ACDA (IT & SDC) - Please accept Part II Orders with one day gap in Cease and Grant (Refers to Para 3 above) as valid to avoid large No of rejections as there is no extra burden on Govt exchequer in doing so.

Internal

COAS Sectt	DG MF	E-in-C's Sectt	ADG AE
VCOAS Sectt	DG Inf	DG RVS	ADG OL
DCOAS (IS & C) Sectt	DG Army Avn	DG NCC	ADG Mov
DCOAS (P&S) Sectt	DG AAD	DG Resettlement	Provost Marshal
DCOAS (Strat) Sectt	DG Sigs	DG BR	Brig DSC
AG Sectt	DG MS	Dte of Standardisation	Brig Pnrs
QMG Sectt	DG ST	DG MI	ADG TA
MGS Sectt	DG EME	DRDO/DoP-Pers (AF)	HQ DG AR
MS Sectt	DG OS	ADG E (Pers), E-in-C's Br	ADGPS

▲ 图 3.12 SideCopy 组织发送的诱饵示例 [55]

下表总结了上述南亚地区 APT 组织在 2023 上半年的主要攻击活动。

组织名	活动描述	披露时间	披露机构
SideCopy	SideCopy 组织最新攻击武器披露 [44]	2023/1/6	360
CNC	APT 组织“GroupA21”借政府官方文档攻击巴基斯坦 [45]	2023/1/11	微步在线
蔓灵花	APT 组织 Bitter 网络间谍攻击活动实例分析 [46]	2023/1/13	中孚
肚脑虫	APT-C-35（肚脑虫）组织近期攻击活动披露 [47]	2023/2/7	360
蔓灵花	蔓灵花组织 2023 年初攻击行动与新组件揭秘 [48]	2023/2/9	深信服
透明部落	APT-C-56（透明部落）伪装简历攻击活动分析 [49]	2023/2/14	360
SideCopy	SideCopy 针对印度的政府机构分发后门 ReverseRAT[50]	2023/2/21	Dragon Threat Labs
响尾蛇	“响尾蛇”近期攻击活动披露，瞄准国内高校展开钓鱼 [51]	2023/2/22	微步在线
SideCopy	近期 APT 组织 SideCopy 针对印度政府的钓鱼攻击活动分析 [52]	2023/2/25	绿盟

组织名	活动描述	披露时间	披露机构
透明部落	透明部落通过 Android 消息传递应用程序引诱印巴官员 [53]	2023/3/7	Welivesecurity
透明部落	APT-C-56（透明部落）部署 Android 系统 RlmRat、Linux 系统波塞冬新型组件披露 [54]	2023/3/8	360
SideCopy	SideCopy 组织近期以印度国防部相关文档为诱饵的攻击活动分析 [55]	2023/3/21	奇安信
SideCopy	SideCopy APT 组织将目光投向了印度的 DRDO[56]	2023/3/21	Cyble
肚脑虫	暗影重重：肚脑虫（Donot）组织近期攻击手法总结 [57]	2023/3/23	奇安信
蔓灵花	蔓灵花针对中国核能行业的网络钓鱼活动 [58]	2023/3/24	Intezer
蔓灵花	Bitter Group 传播针对中国机构的 CHM 恶意软件 [59]	2023/4/4	AhnLab
透明部落	透明部落攻击印度教育部门 [60]	2023/4/13	SentinelOne
肚脑虫	Donot APT 使用 Android 恶意软件攻击南亚 [61]	2023/4/14	CYFIRMA
CNC	疑似 CNC 组织最新攻击动态分析 [62]	2023/4/14	深信服
透明部落	揭露 APT-36 的新 Linux 恶意软件活动 [63]	2023/4/17	Uptycs
摩诃草	Patchwork 组织更新技术卷土重来，针对境内教育科研单位再次发起攻击行动 [64]	2023/4/20	深信服
SideCopy	SideCopy 组织使用新木马对印度展开攻击 [65]	2023/4/21	奇安信
透明部落	透明部落 APT 在针对教育机构的目标越来越多的情况下积极引诱印度军队 [66]	2023/5/2	Seqrite
SideCopy	SideCopy 疑似分发关于印度国家军事研究机构的钓鱼邮件 [67]	2023/5/4	Fortinet
响尾蛇	Sidewinder 组织针对巴基斯坦政府的最新活动追踪 [68]	2023/5/8	BlackBerry
SideCopy	SideCopy 伪装注册邀请表格进行攻击 [69]	2023/5/11	360
响尾蛇	Sidewinder 组织持续攻击中国和巴基斯坦实体 [70]	2023/5/17	Group-IB
摩诃草	白象组织使用 BADNEWS 和 Remcos 商业木马的最新攻击活动 [71]	2023/5/23	安天
摩诃草	对开源项目情有独钟的 Patchwork 组织 [72]	2023/5/24	深信服
摩诃草	Patchwork 组织新型攻击武器报告 -EyeShell 武器披露 [73]	2023/5/25	知道创宇
蔓灵花	Bitter 组织新攻击武器分析报告 -ORPCBackdoor 武器分析 [74]	2023/5/30	知道创宇

▲ 表 3.13 2023 上半年南亚地区 APT 组织热点攻击活动

东欧地区的组织与行动
Eastern Europe

2023 上半年，东欧地区的各个老牌 APT 组织依旧活跃。除了乌克兰，东欧地区的 APT 组织还把目光放在其他国家上，展开了不间断的网络间谍活动。2023 上半年该地区的 APT 组织发起的攻击多为鱼叉式钓鱼邮件攻击，表 3.14 为 2023 上半年东欧地区活跃的 APT 组织简介。

东欧 APT 组织	攻击能力
APT28	+++
APT29	+++
Turla	+++
Sandworm	+++
Gamaredon	+
UAC-0056	+
FIN7	+
DustSquad	++

组织名	最早活动时间	公开披露时间	组织简介
APT28	2004	2014	APT28 组织历史活动非常频繁，主要针对政府、军事和安全组织，相关攻击覆盖 Windows、Linux、Mac、Android 和 iOS，其在 2016 年企图干扰美国大选，在 2022 年上半年被披露发动了针对美国国防承包商的攻击，俄乌冲突中多次向乌克兰投放恶意软件
APT29	2008	2013	APT29 组织的主要目标为西亚、中亚、东非和中东的政府部门和机构。其被认为在 2015 年夏季攻击了美国 DNC，近年来不断针对多国外交机构发起攻击
Turla	2007	2014	该组织拥有非常复杂的 TTP，其受害者覆盖超过 45 个国家，常针对政府、大使馆、军事、教育、研究和制药公司实施鱼叉和水坑攻击
Sandworm	2009	2015	Sandworm 组织大约从 2009 年开始运营，主要针对与能源、工业控制系统、SCADA、政府和媒体相关领域的乌克兰实体，在 2022 年俄乌冲突中策划了针对乌克兰电网的攻击
Gamaredon	2013	2015	主要针对乌克兰执法部门、政府机构和军事力量进行间谍活动和情报收集等攻击。Operation Armageddon 行动与该组织有关，2022 年上半年频繁向乌克兰发起网络钓鱼攻击
UAC-0056	2020	2022	又名 Lorec53（中文名称：洛瑞熊），该组织最早的攻击活动可以追溯到 2020 年 6 月，主要以乌克兰、格鲁吉亚为目标，其攻击活动带有明显的政治意图
FIN7	2013	2017	FIN7 最早由国外安全厂商 FireEye 在 2017 年 3 月份命名，其攻击活动最早从 2015 年开始，针对美国的零售、餐饮、酒店业务，攻击目标还包括金融服务、运输、零售、教育、电子产品等领域。该组织经常使用商业恶意软件。FIN7 有时被称为 CarBanak、Anunak。
DustSquad	2014	2018	DustSquad 组织至少从 2014 年开始活动，主要针对中亚地区，包括地方政府、外交使团和个人。DustSquad 主要使用 delphi 编写恶意软件。

▲ 表 3.14 2023 上半年东欧地区活跃 APT 组织

2023 上半年，东欧地区 APT 组织主要使用的攻击手段仍然是鱼叉式钓鱼邮件，不过这些组织所采取的攻击方式和攻击技术也在不断改进优化。

根据开源情报披露，APT28 组织使用已知漏洞在思科路由器上进行侦察和部署恶意软件，以及伪造 Windows 更新攻击乌克兰政府。乌克兰黑客组织 Cyber Resistance 还曝光了 APT28 组织领导人的个人信息，包括但不限于家庭住址和个人信件。

Sandworm 在 2023 上半年频繁使用文件擦除器攻击乌克兰政府及新闻机构，使用的擦除类恶意软件

包括但不限 CaddyWiper、ZeroWipe、SDelete、AwfulShred、BidSwipe，攻击平台涉及 Windows、Linux 及 FreeBSD 等。

APT29 组织曾利用波兰大使访问美国的机会瞄准援助乌克兰的欧盟政府进行攻击，并且使用 Notion 的 API 作为 C&C 信道来隐藏自身流量及 C2 设施。该组织除了使用“.iso”、“.zip”等格式的文件外还使用“.img”后缀文件投递恶意软件。

去年我们提到 Gamaredon 的武器库一直在更新升级，今年 Gamaredon 暴露的 Web 面板揭示了他们拥有自动化的鱼叉式钓鱼攻击平台，该组织针对乌克兰、拉脱维亚、爱沙尼亚和立陶宛等国家发起了多次攻击。

奇安信威胁情报中心整理了 2023 上半年东欧地区 APT 组织热点攻击活动，如下表所示：

组织名	活动描述	披露时间	披露机构
Turla	Turla 通过 Andromeda 恶意软件攻击乌克兰 [75]	2023/1/5	mandiant
Gamaredon	Gamaredon 使用 Telegram 攻击乌克兰组织 [76]	2023/1/19	BlackBerry
Sandworm	Sandworm 组织借助 5 种擦除器攻击乌克兰新闻机构 [77]	2023/1/27	CERT-UA
Sandworm	Sandworm APT 使用新的 SwiftSlicer 擦除器瞄准乌克兰 [78]	2023/1/28	securityaffairs
Gamaredon	拉脱维亚国防部遭到黑客团伙 Gamaredon 的钓鱼攻击 [79]	2023/1/28	Recorded Future
Gamaredon	Gamaredon 组织针对乌克兰当局开展间谍活动 [80]	2023/2/1	CERT-UA
UAC-0056	Graphiron：针对乌克兰部署的新型信息窃取恶意软件 [81]	2023/2/8	Symantec
Gamaredon	Gamaredon 利用 Hoaxshell 攻击乌克兰组织 [82]	2023/2/15	medium
APT29	APT29 利用 Notion API 瞄准欧盟委员会进行攻击 [83]	2023/3/10	medium
Gamaredon	分析 Gamaredon 针对乌克兰的攻击行动 [84]	2023/3/13	ThreatMon
APT29	NOBELIUM 利用波兰大使访问美国的机会瞄准援助乌克兰的欧盟政府 [85]	2023/3/14	BlackBerry
APT28	黑客组织 APT 28 的领导人被黑 [86]	2023/4/10	Context Information Security
APT29	东欧 APT 组织的间谍活动 [87]	2023/4/13	GovCERT

组织名	活动描述	披露时间	披露机构
FIN7	Ex-Conti 与 FIN7 的新 Domino 后门合作 [88]	2023/4/14	IBM
Gamaredon	Web 面板揭示了 Gamaredon Group 的自动鱼叉式网络钓鱼活动 [89]	2023/4/17	EclecticIQ
APT28	APT28 利用已知漏洞在思科路由器上进行侦察和部署恶意软件 [90]	2023/4/18	CISA
Turla	分析 Tomiris 与 Turla 的联系 [91]	2023/4/24	Kaspersky
APT29	APT29 近期利用 CobaltStrike 开展攻击活动 [92]	2023/4/25	viewintech
FIN7	在针对 Veeam 备份服务器的攻击中发现 FIN7 tradecraft[93]	2023/4/26	withsecure
DustSquad	Nomadic Octopus 在塔吉克斯坦新的监视活动 [94]	2023/4/28	prodaft
APT28	APT28 使用伪造的“Windows 更新”指南来攻击乌克兰政府 [95]	2023/4/28	CERT-UA
Sandworm	疑似 Sandworm 使用 WinRAR 擦除乌克兰国家机构的数据 [96]	2023/4/29	CERT-UA
Sandworm	泄露的 NTC Vulkan 文件中披露的信息可能与 Sandworm 有关 [97]	2023/5/25	trustwave

▲ 表 3.15 2023 上半年东欧地区 APT 组织热点攻击活动

中东地区的组织与行动
Middle East

中东地区复杂的政治外交局势和宗教文化差异使其成为网络攻击和间谍活动的热点区域。地区中主要强国对地缘资本、经济利益和权力地位的争夺导致了情报监控和网络攻击活动的频发，众多 APT 组织牵涉其中。

中东 APT 组织	攻击能力
PROMETHIUM	++
双尾蝎	+
MuddyWater	+
APT34	++
APT35	++
Agrius	+

该地区的 APT 组织常利用网络钓鱼等社会工程学手段和其他攻击技术，针对政府机构、商业企业、学术机构和关键基础设施发起网络攻击，以窃取敏感数据和机密信息。表 3.16 为 2023 上半年度活跃的 APT 组织。

组织名	最早活动时间	公开披露时间	组织简介
PROMETHIUM	2012	2016	PROMETHIUM 组织拥有复杂的模块化攻击武器库与丰富的网络资源，具备 0day 漏洞作战能力，拥有 Windows、Android 双平台攻击武器
双尾蝎	2011	2015	双尾蝎组织攻击范围主要为中东地区，攻击武器针对 Windows 和 Android 双平台，采取鱼叉邮件或水坑网站等攻击方式配合社会工程学手段进行渗透，向政府、金融、媒体、能源、军事等特定目标人群发起攻击
MuddyWater	2017	2017	主要针对中东实施网络间谍活动，也针对欧洲和北美国家。其攻击目标包括电信、政府 (IT 服务) 和石油部门。主要使用基于 Powershell 的初始阶段后门，也被称为 POWERSTATS
APT34	2014	2016	APT34 主要针对中东地区实施攻击，攻击目标包括金融、政府、能源、化工和电信等行业。
APT35	2014	2018	APT35 是 FireEye 于 2018 年披露的 APT 组织，也被称为 Newscaster Team。该组织通常针对美国和中东的军事、外交和政府人员、媒体组织、能源和国防工业基地 (DIB) 以及工程、商业服务和电信部门进行攻击活动。
Agrius	2019	2020	Agrius 组织由国外网络安全公司 SentinelOne 发现并命名的 APT 组织，通过使用恶意软件对受害者系统数据进行恶意抹除进行攻击，并且伪装为勒索攻击掩盖其攻击行为。

▲ 表 3.16 2023 上半年中东地区活跃 APT 组织

APT 组织攻击从未静谧，也从未消失，总是将自己隐藏在隐秘的角落给攻击目标致命一击。在新老技术不断交替的背景下，攻击和对抗呈螺旋上升的趋势。在中东地区的上半年 APT 组织的活动中，可以观察到各大 APT 组织一直在努力更新自己的武器库。

经过对中东地区各 APT 组织的长期追踪，我们发现 MuddyWater 组织依然保持着极高的活跃度。在 2023 年上半年，该组织频繁发动攻击，并对其武器库进行了改进。在针对以色列的活动中，他们传播了带有反以色列内容的虚假信息。此外，他们还利用了 Log4j 漏洞，并部署了包括最近使用的 SyncroRAT 在内的多种 RAT 工具。这表明该组织不断发展其武器库，试图将网络间谍活动的利益最大化。

网络空间中的安全威胁越来越复杂和多样化，而来自 APT 组织的威胁更是手段频出。PROMETHIUM 组织通过模仿 Shagle 服务的仿冒网站分发带有 StrongPity 后门的移动端应用程序。该应用程序是开源

Telegram 应用程序的修改版本，加入 StrongPity 后门代码重新打包，通过 11 个动态触发模块完成短信、通话记录、联系人等敏感信息收集和通话内容记录等监控操作。

此外，像双尾蝎、APT34、APT35 等 APT 组织仍然在中东地区活跃，并不断创新其攻击方式和武器库。它们通常利用地方选举、社会热点等信息制作诱饵，偏好使用鱼叉钓鱼邮件、水坑网站、社会工程学等手段进行攻击。根据公开情报，我们整理了中东地区 2023 年上半年的主要攻击活动，具体内容如下表所示：

组织名	活动描述	披露时间	披露机构
MuddyWater	暗网简介：MuddyWater APT Group[98]	2023/1/2	SOCRadar
PROMETHIUM	针对 Android 用户的 StrongPity 间谍活动 [99]	2023/1/10	Welivesecurity
APT34	新的 APT34 恶意软件瞄准中东 [100]	2023/2/2	Trendmicro
MuddyWater	MuddyWater 对以色列进行网络攻击 [101]	2023/3/9	以色列国家安全局
双尾蝎	APT-C-23（双尾蝎）组织最新攻击活动分析 [102]	2023/3/30	360
双尾蝎	Mantis：用于攻击巴勒斯坦目标的新工具 [103]	2023/4/4	Symantec
MuddyWater	MERCURY 和 DEV-1084：对混合环境的破坏性攻击 [104]	2023/4/7	Microsoft
APT35	Mint Sandstorm 改进贸易技术以攻击高价值目标 [105]	2023/4/18	Microsoft
MuddyWater	跟踪 MuddyWater 的基础设施 [106]	2023/4/18	Group-IB
APT35	APT35 通过改进的工具库瞄准以色列 [107]	2023/4/25	CheckPoint
APT35	深入了解 APT35 的最新恶意软件 [108]	2023/4/26	Bitdefender
MuddyWater	APT 组织 MuddyWater 攻击活动 [109]	2023/5/2	Welivesecurity
Agrius	AGRIUS 在针对以色列组织的攻击中部署 MONEYBIRD[110]	2023/5/24	CheckPoint

▲ 表 3.17 2023 上半年中东地区 APT 组织热点攻击活动

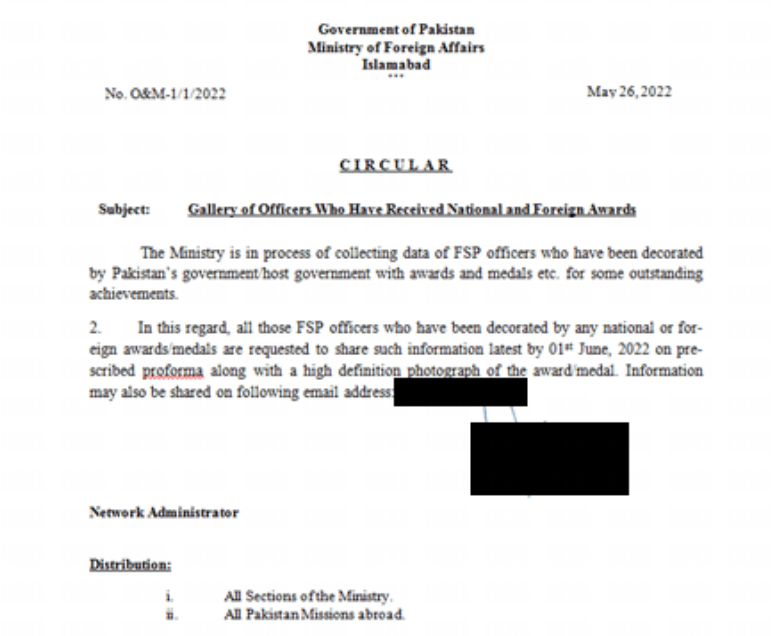
其他地区的组织与行动
Other areas in World

2023 年上半年全球安全厂商披露了多个具有高级攻击技术、并在本年度持续活跃的 APT 组织，其中包括持续活动了四年但直到今年才被披露的 GoldenJackal 间谍活动组织，以及非常活跃且频繁更新组件的老牌 APT 组织 TA505，奇安信威胁情报中心整理上述组织的相关简介，如表 3.18 所示。

组织名	最早活动时间	公开披露时间	组织简介
NewsPenguin	2023	2023	该组织主要针对巴基斯坦，以制造军事技术的公司、民族国家和军队为首要目标 [112]。
OilAlpha	2022	2023	该组织是一个针对政治代表、媒体和记者从事间谍活动的威胁活动组织，主要针对阿拉伯半岛地区的 Android 用户，攻击者几乎完全依赖与也门国有企业公共电信公司 (PTC) 相关的基础设施 [115]。
GoldenJackal	2019	2023	该组织自 2019 年开始活跃，通常针对中东和南亚的政府和外交机构，根据工具集和攻击者的行为，研究人员认为该组织的主要动机是间谍活动 [116]。
UCID902	2021	2023	该组织和威胁组织“Kimsuky”在 TTP、动机和作案手法方面有很多重叠之处 [117]。

▲ 表 3.18 2023 上半年其他地区活跃 APT 组织

GoldenJackal APT 组织主要使用 .NET 开发的恶意软件，包括 JackalControl、JackalWorm、JackalSteal、JackalPerInfo 和 JackalScreenWatcher 等工具，并且具备漏洞利用能力。在 Follina 漏洞公开披露两天后，该组织就投放了一批名为“获得国内外奖项的军官图库 .docx”的 Follina 漏洞诱饵文件，旨在收集有关巴基斯坦政府授勋军官的信息。



Government of Pakistan
Ministry of Foreign Affairs
Islamabad

No. O&M-1/1/2022 May 26, 2022

CIRCULAR

Subject: Gallery of Officers Who Have Received National and Foreign Awards

The Ministry is in process of collecting data of FSP officers who have been decorated by Pakistan's government/host government with awards and medals etc. for some outstanding achievements.

2. In this regard, all those FSP officers who have been decorated by any national or foreign awards/medals are requested to share such information latest by 01st June, 2022 on prescribed proforma along with a high definition photograph of the award/medal. Information may also be shared on following email address: [redacted]

Network Administrator

Distribution:

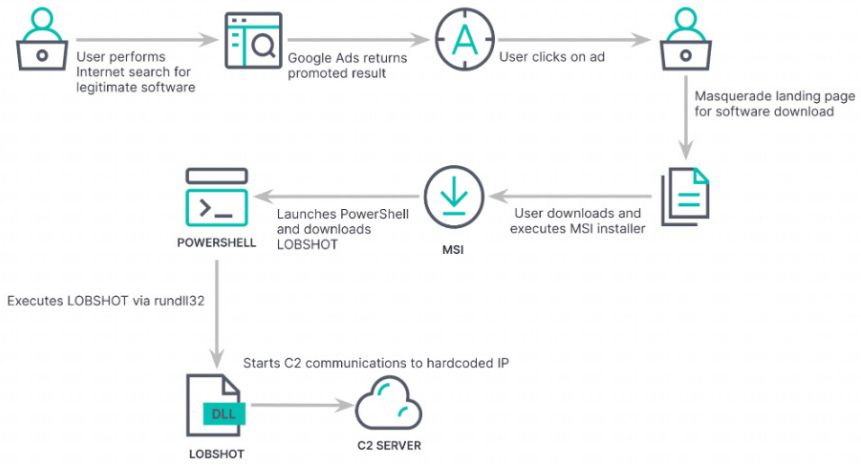
i. All Sections of the Ministry.
ii. All Pakistan Missions abroad.

▲ 图 3.19 Follina 漏洞诱饵文件 [116]

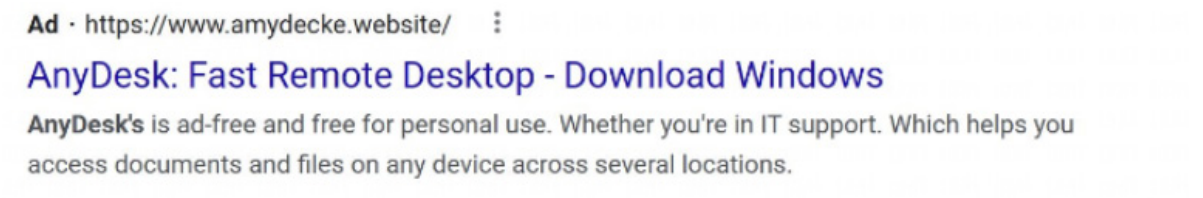
OilAlpha 是一个针对政治代表、媒体和记者从事间谍活动的威胁活动组织，主要目标是使用 Android 设备并讲阿拉伯语的人，其使用了 SpyNote 和 SpyMax 等 Android 平台 RAT。该组织攻击活动最早是在 2022 年 4 月 14 日，其以“安全带部队的公报”主题相关公报为诱饵，使用沙特阿拉伯区域的电话号码通过 WhatsApp 社交软件传播 SpyNote 木马的 APK 文件。

▲ 图 3.20 OilAlpha 利用 WhatsApp 传播 SpyNote 木马的 APK 文件 [115]

TA505 今年利用 Google Ads 推广他们托管恶意软件的虚假网站，并在看似合法的安装程序中嵌入 LOBSHOT 后门，整个感染链如下图所示。在一个案例中，恶意广告是针对合法的远程桌面软件 AnyDesk。

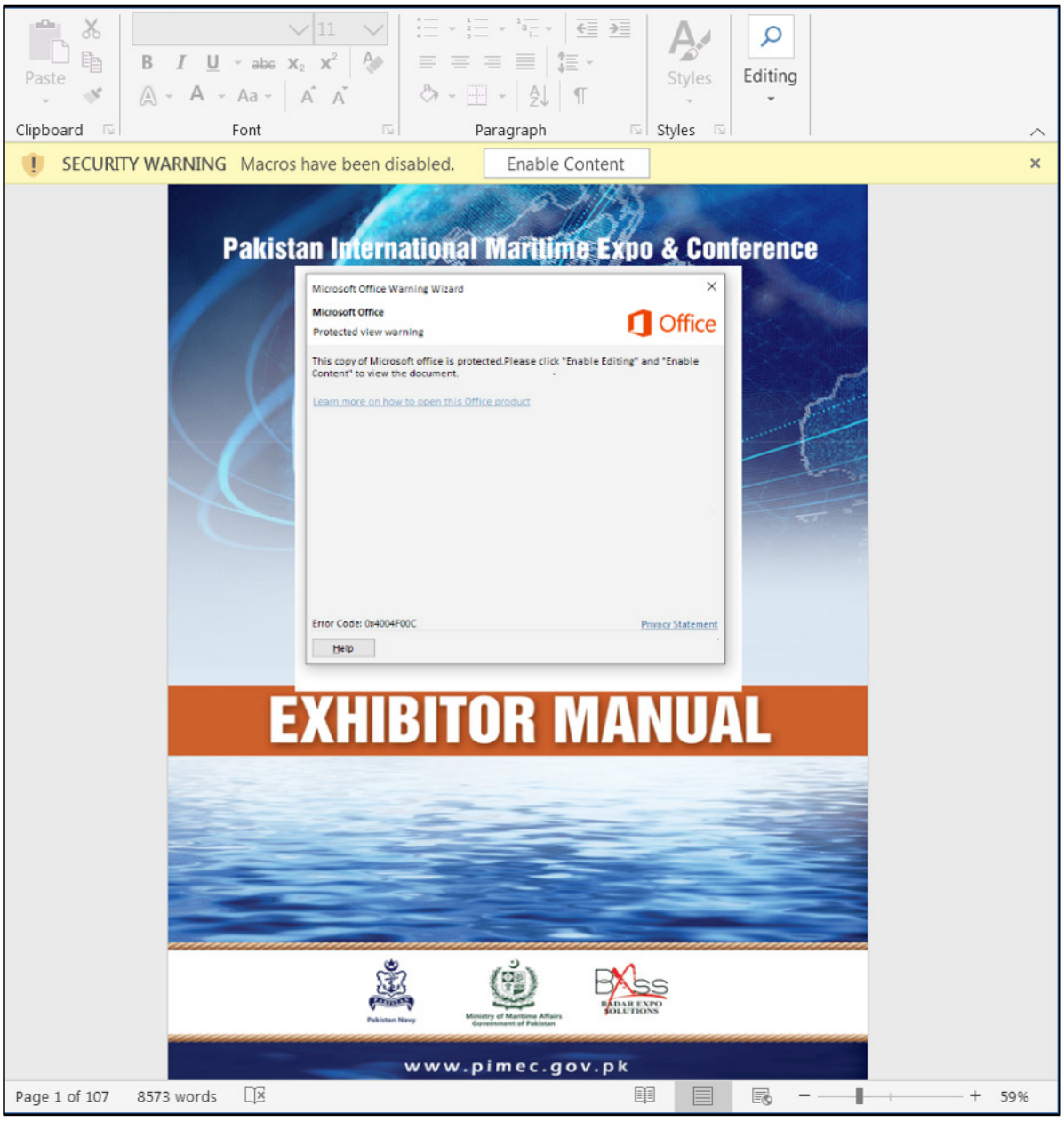


▲ 图 3.21 TA505 加载 LOBSHOT 模块的感染链 [114]



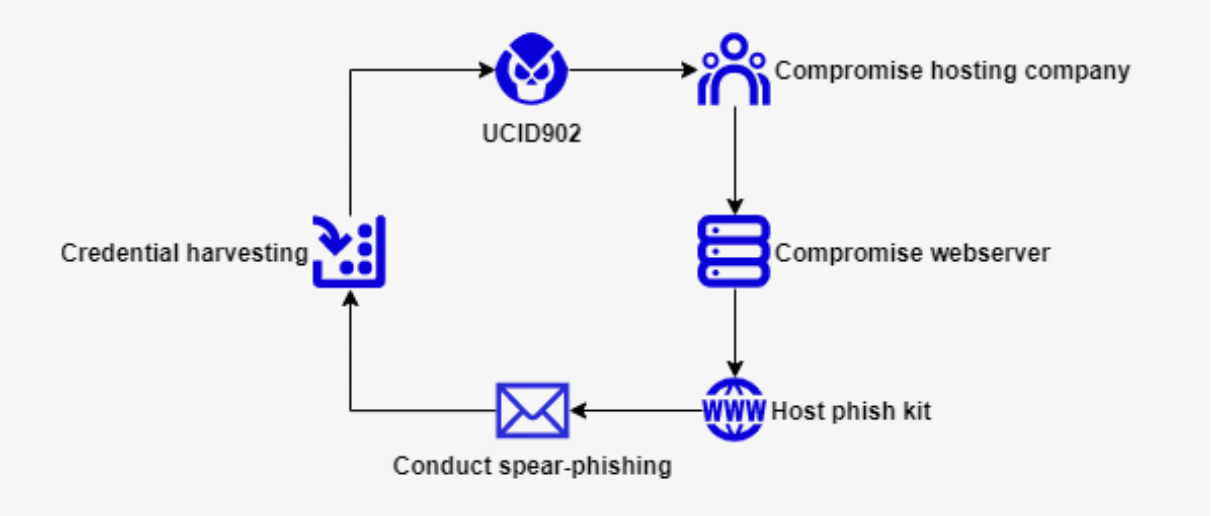
▲ 图 3.22 TA505 投放的恶意谷歌广告 [114]

NewsPenguin 是一个以前不为人知的攻击团伙，使用复杂的有效载荷传递机制瞄准巴基斯坦用户、巴基斯坦国际海事博览会和会议的潜在访客，利用巴基斯坦国际海事博览会和会议 (PIMEC-2023) 作为网络钓鱼电子邮件诱饵进行攻击。



▲ 图 3.23 NewsPenguin 通过鱼叉式网络钓鱼技术传播的恶意诱饵文件 [112]

UCID902 首次被观察到的攻击活动是在 2021 年 7 月 12 日针对韩国激进分子发起的旨在窃取网络登录凭据的钓鱼活动。这些诱饵以 Naver 安全警报的形式出现，提示用户输入凭据。攻击者使用水坑攻击，通过攻陷韩国境内合法组织的网站来托管网络钓鱼页面。



▲ 图 3.24 UCID902 的凭据窃取水坑攻击模式 [117]

组织名	活动描述	披露时间	披露机构
Kasablanka	Kasablanka 组织针对俄罗斯联邦政府合作署、俄罗斯阿斯特拉罕州对外通信部进行活动攻击 [111]。	2023/01/17	奇安信
NewsPenguin	使用复杂的有效载荷传递机制瞄准巴基斯坦的组织，利用巴基斯坦国际海事博览会和会议 (PIMEC-2023) 作为诱饵来欺骗受害者 [112]。	2023/02/09	blackberry
Evilnum	使用英国居民的护照信息作为诱饵文件，内部包含 LNK 伪装的 PNG 图像诱导用户点击执行，实现后续下载 js 插件执行功能 [113]。	2023/03/23	安恒
UCID902	APT 组织 UCID902 针对人权活动家的水坑凭据收集活动披露 [117]	2023/04/20	Interlab
TA505	通过 Google Ads 传播的 hVNC 恶意软件家族 LOBSHOT，用于窃取加密货币钱包 [114]。	2023/04/25	Elastic Security Labs
OilAlpha	使用沙特阿拉伯电话号码通过 WhatsApp 传播 SpyNote 远控 APK[115]。	2023/05/16	CrowdStrike
GoldenJackal	利用 Follina 漏洞攻击巴基斯坦政府，旨在收集有关巴基斯坦政府授勋军官的信息 [116]。	2023/05/23	Kaspersky

▲ 表 3.25 2023 上半年其它地区 APT 组织热点攻击活动

第四章 大量0day漏洞被用于APT攻击

2023 年在野 0day 的利用情况总体比 2022 上半年有所上升，漏洞数量接近 30 个左右。在漏洞涉及产品的供应厂商中，微软、谷歌、苹果御三家的地位依然稳固，但是相较往年微软、谷歌势强，苹果势微的情况，今年三家呈现出真正意义上的三足鼎立。以浏览器为攻击向量依然是主流趋势，Chrome、Safari 浏览器与对应平台 Windows、macOS、iOS 下的提权逃逸漏洞占所有漏洞近 8 成。

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2023-21674	Microsoft	否	未知	Avast
CVE-2023-23529	Apple	否	未知	未知
CVE-2023-21823	Microsoft	否	未知	Mandiant
CVE-2023-21715	Microsoft	是	未知	EXPMON
CVE-2023-23376	Microsoft	否	未知	Microsoft Threat Intelligence Center (MSTIC) & Microsoft Security Response Center (MSRC)
CVE-2023-20963	Google	否	未知	Oversecured Inc
CVE-2023-23397	Microsoft	是	APT28	CERT-UA, Microsoft Incident, Microsoft Threat Intelligence (MSTI)
CVE-2023-24880	Microsoft	是	Magniber 勒索	Google's Threat Analysis Group Microsoft
CVE-2023-21768	Microsoft	是	未知	未知
CVE-2023-0266	Google	否	未知	Google Threat Analysis Group
CVE-2023-26083	ARM	否	未知	Google Threat Analysis Group
CVE-2023-28206	Apple	是	未知	Google Threat Analysis Group
CVE-2023-28205	Apple	否	未知	Google Threat Analysis Group
CVE-2023-28252	Microsoft	是	Nokoyawa 勒索	Kaspersky, Mandiant, 安恒

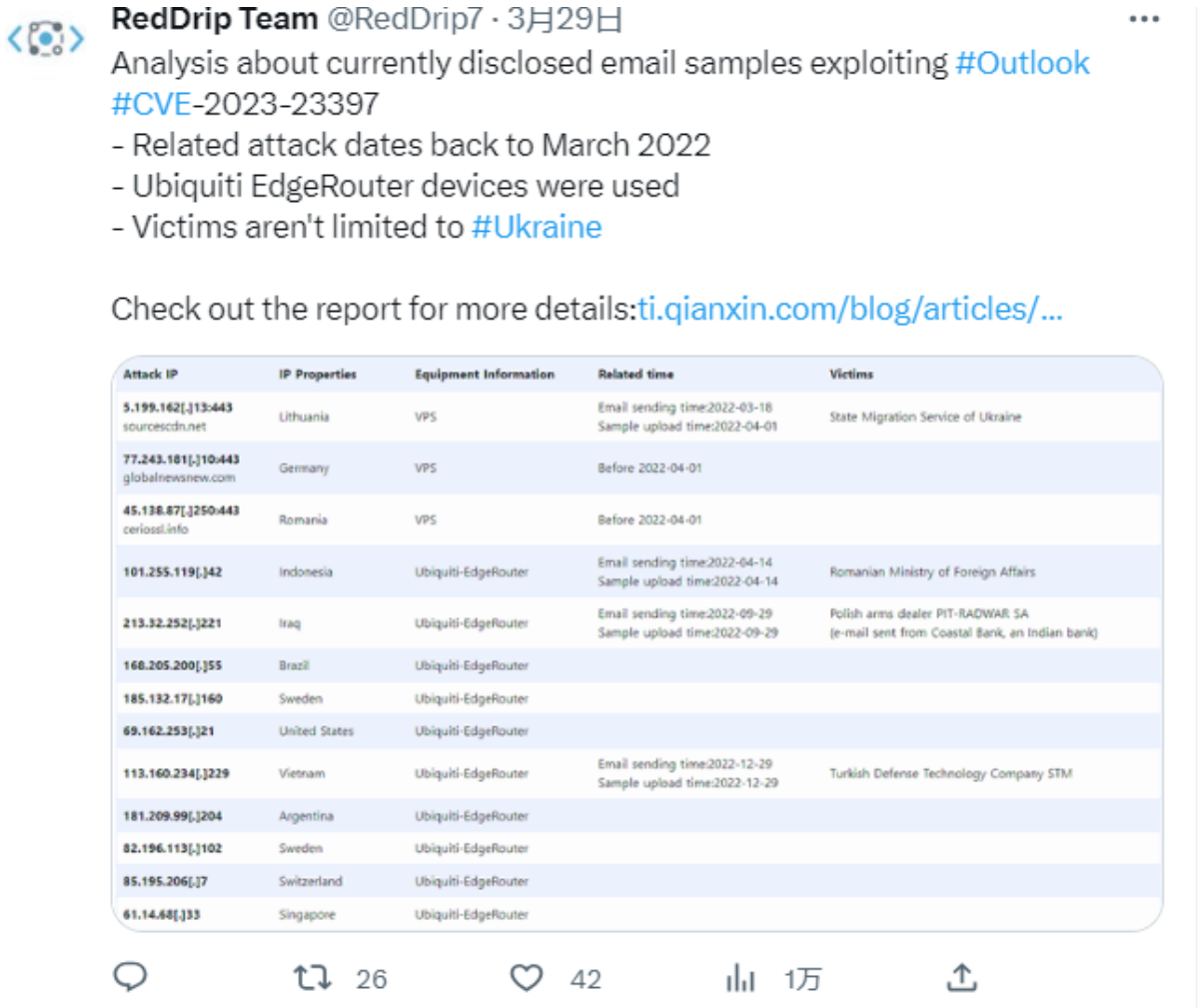
漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2023-2033	Google	否	未知	Google Threat Analysis Group
CVE-2023-2136	Google	否	未知	Google Threat Analysis Group
CVE-2023-21492	Samsung	否	未知	Google Threat Analysis Group
CVE-2023-28204	Apple	否	未知	未知
CVE-2023-32373	Apple	否	未知	未知
CVE-2023-32409	Apple	否	未知	Google Threat Analysis Group
CVE-2023-29336	Microsoft	是	未知	Avast
CVE-2023-2868	Barracuda	是	UNC4841	Barracuda,Mandiant
CVE-2023-3079	Google	否	未知	Google Threat Analysis Group
CVE-2023-32434	Apple	否	Operation Triangulation	Kaspersky
CVE-2023-32435	Apple	否	Operation Triangulation	Kaspersky
CVE-2023-32439	Apple	否	Operation Triangulation	未知

▲ 表 4.1 2023 上半年披露的高危漏洞

一、贪婪的灰熊：Outlook 漏洞 CVE-2023-23397

2023 年 4 月，微软在补丁日修复了存在于 Outlook 中的一个等级为严重的漏洞 CVE-2023-23397，该漏洞被微软确认已存在在野利用。攻击者通过发送带有特定 MAPI 属性的邮件至受害者 Outlook 邮箱，当受害者用 Outlook 打开恶意邮件时，将自动连接该属性指定的由攻击者控制的 SMB 共享服务器 UNC 路径，导致目标受害者的 NTLM Hash 被窃取。

奇安信威胁情报中心第一时间还原了该漏洞，在关联的过程中发现了大量新的可疑受害者，并确认利用该漏洞的攻击可追溯至 2022 年 3 月。我们发现早期用于攻击邮件发送的都是 VPS 服务器，漏洞触发后回连的 UNC 地址也指向同一台 VPS，但在 2022 年 4 月 14 日之后，所有的攻击 C2 都替换成了 Ubiquiti-EdgeRouter 路由器。此次漏洞攻击目标包含乌克兰、土耳其、罗马尼亚等地区的重要组织机构。



Attack IP	IP Properties	Equipment Information	Related time	Victims
5.199.162[.]13:443 sourcescdn.net	Lithuania	VPS	Email sending time:2022-03-18 Sample upload time:2022-04-01	State Migration Service of Ukraine
77.243.181[.]10:443 globalnewsnew.com	Germany	VPS	Before 2022-04-01	
45.138.87[.]250:443 ceriossl.info	Romania	VPS	Before 2022-04-01	
101.255.119[.]42	Indonesia	Ubiquiti-EdgeRouter	Email sending time:2022-04-14 Sample upload time:2022-04-14	Romanian Ministry of Foreign Affairs
213.32.252[.]221	Iraq	Ubiquiti-EdgeRouter	Email sending time:2022-09-29 Sample upload time:2022-09-29	Polish arms dealer PIT-RADWAR SA (e-mail sent from Coastal Bank, an Indian bank)
168.205.200[.]55	Brazil	Ubiquiti-EdgeRouter		
185.132.17[.]160	Sweden	Ubiquiti-EdgeRouter		
69.162.253[.]21	United States	Ubiquiti-EdgeRouter		
113.160.234[.]229	Vietnam	Ubiquiti-EdgeRouter	Email sending time:2022-12-29 Sample upload time:2022-12-29	Turkish Defense Technology Company STM
181.209.99[.]204	Argentina	Ubiquiti-EdgeRouter		
82.196.113[.]102	Sweden	Ubiquiti-EdgeRouter		
85.195.206[.]7	Switzerland	Ubiquiti-EdgeRouter		
61.14.68[.]33	Singapore	Ubiquiti-EdgeRouter		

▲ 图 4.2 CVE-2023-23397 分析报告 [118]

二、三角定位：侵蚀的苹果

2023 年 6 月 1 日，卡巴斯基披露了 Operation Triangulation 攻击活动 [119]，称从 2019 年开始卡巴斯基内部重要员工的 iPhone 手机就遭到 0day 漏洞的攻击，攻击目标不仅限于卡巴斯基，很可能还涉及多个国家的重点公司及政府部门。攻击者通过发送一条带有恶意附件的 iMessage 信息到目标设备上，在无需任何用户交互的情况下，利用该条消息触发代码执行漏洞。漏洞利用所执行的代码会从远程服务器上下载后续阶段的 Payload，其中包含了用于提权的额外利用代码，并最终部署一个功能齐全的木马平台，最后会删除最初触发漏洞利用的漏洞消息。

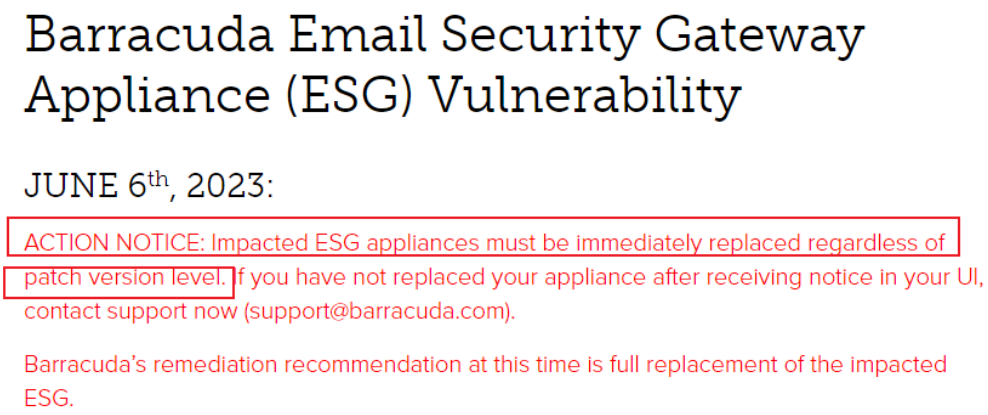
奇安信威胁情报中心第一时间跟进了该事件，并通过奇安信内部数据确认 Operation Triangulation 活动同样波及了国内多个重点单位的相关人员。

▲ 图 4.3 Operation Triangulation[119]

三、潜入深渊的梭子鱼：CVE-2023-2868

Barracuda Networks 于 2023 年 5 月 30 日发布通告，称旗下 ESG(Email Security Gateway) 设备中存在 0day 漏洞 CVE-2023-2868 并已被利用，该漏洞是 ESG 对 tar 文件过滤不严导致的远程命令执行漏洞。利用该漏洞的攻击最早发生于 2022 年 10 月，攻击者通过漏洞获取目标设备的代码执行权限后，下发 SEASPY/SALTWATER 木马。

值得注意的是，Barracuda Networks 在通告发布 7 天后，即 2023 年 6 月 6 日更新了通告内容，指出无论是否安装了漏洞补丁，受影响的 ESG 设备都需要立即更换。背后的原因为攻击者在事件披露后迅速地对常驻木马进行了更新调整，增加了其他持久化机制以试图维持访问。


Barracuda Email Security Gateway Appliance (ESG) Vulnerability

JUNE 6th, 2023:

ACTION NOTICE: Impacted ESG appliances must be immediately replaced regardless of patch version level. If you have not replaced your appliance after receiving notice in your UI, contact support now (support@barracuda.com).

Barracuda's remediation recommendation at this time is full replacement of the impacted ESG.

▲ 图 4.4 Barracuda Networks 漏洞通告 [120]

四、看齐 APT 组织：使用 0day 漏洞的勒索团伙

勒索团伙大多数情况下以经济勒索为目的，本身对 0day 漏洞的需求不大，部分团伙可能会为获取 System 权限内置一些 Nday 提权漏洞，或在传播时使用类似永恒之蓝的 Nday 漏洞。但是从 2022 年底开始，勒索团伙的攻击中不断出现 0day 漏洞。

最早为 2022 年底的 CVE-2022-44698，该漏洞允许攻击者使用一个错误格式的 JS 认证签名绕过 SmartScreen 安全告警，Magniber 勒索团伙通过该漏洞下发后续的勒索软件。

2023 年 3 月，Google TAG 再次捕获到了 Magniber 勒索团伙的 0day 攻击，这次攻击使用了 0day CVE-2023-24880，该漏洞和 CVE-2022-44698 类似，通过一个错误格式的 MSI 认证签名来绕过 SmartScreen 安全告警。

2023 年 4 月，卡巴斯基披露了 Nokoyawa 团伙的 0day 攻击事件，攻击中使用了 0day CVE-2023-28252，该漏洞为 Windows 系统 CLFS 组件中的一处越界写入漏洞，成功利用后将导致权限提升。

随着攻防双方的不断对抗，如今勒索团伙也逐渐加入 0day 的军备竞赛，而作为以经济利益为导向的犯罪团伙，他们可凭借攫取的丰厚不义之财来维系其源源不断的 0day 供应，下半年我们可能会看到更多 0day 利用出现在勒索团伙的攻击中。

附录1 全球主要APT组织列表


莲花
名:OceanLotus、APT32
莲花是奇安信威胁情
中心披露的 APT 组织，
最早活动可追溯至
12 年。该组织主要使
鱼叉攻击和水坑攻击
攻击手法和 Denis 木
Cobalt Strike 等攻击
具，先后针对中国政
海事机构和东南亚国
等开展攻击活动。
金眼
名:GoldenEye、
券幽灵
金眼是奇安信威胁情
中心披露的 APT 组织，
要针对国内证券相关
业实施攻击活动。
蔓灵花
别名:BITTER
蔓灵花针对中国、巴基斯
坦政府等相关目标实施
APT 攻击。奇安信威胁情
报中心后续发现该组织使
用 InPage 漏洞，并与
Confucius 和摩诃草存在
关联。
Group 123
别名:APT37、ScarCruft
Group 123 是网络间谍
组织，至少从 2012 年开
始活跃，该组织早期主要
针对韩国，2017 年后延
伸攻击目标至半岛范围，
包括日本，越南和中东。
索伦之眼
别名:Strider、
ProjectSauron
索伦之眼是一个极为复
杂的网络间谍组织，至少
从 2011 年开始活跃，其
攻击目标包括俄罗斯、中
国、瑞典、比利时、伊朗和
卢旺达等。
APT34
别名:OilRig
APT34 至少从 2014 年
开始针对中东地区实施
攻击，攻击目标包括金
融、政府、能源、化工和电
信等行业。该组织过去以
APT34 和 OilRig 两个不
同的名称被分别进行追
踪分析。
美人鱼
别名:Infy group
美人鱼行动是主要针对
欧盟国家政府机构开展
的持续时间长达 6 年的
网络间谍活动，已经证
实对丹麦外交部实施过
攻击活动，其攻击手法主
要使用水坑攻击。
人面狮
别名:Sphinx
人面狮行动是奇安信威
胁情报中心披露的 APT
攻击活动，它是活跃在中
东地区的网络间谍活动，
主要目标可能涉及到埃
及和以色列等国家的不
同组织，目的是窃取目标
敏感数据信息。活跃时间
主要集中在 2014 年 6 月
到 2015 年 11 月期间，
该组织主要利用社交网
络进行水坑攻击。
MuddyWater
别名:TEMP.Zagros、
Static Kitten
MuddyWater 最早被发
现于 2017 年 2 月至 10
月期间，针对中东国家、
印度和美国实施网络间
谍活动，其主要使用的
PowerShell 后门也被称
为 POWERSTATS。
Longhorn
别名:Lamberts
Longhorn 疑似为国家
情报机构背景的攻击团
伙，至少从 2011 年开始
活动，该团伙使用了多种
后门木马结合 0day 漏
洞进行攻击。，维基解密
于 2017 年 3 月泄露的
Vault 7 项目资料曝光了
其内部的网络武器项目。
BlackTech
别名:Radio Panda
BlackTech 疑似网络间
谍组织，主要针对东亚地
区实施 APT 攻击活动，
攻击目的疑似窃取目标
公司的技术和证书，该组
织常用的恶意工具也被
称为 PLEAD。
双尾蝎
别名:Big Bang
双尾蝎是奇安信威胁情
报中心披露的 APT 组织，
其曾对巴勒斯坦教育机
构、军事机构实施 APT
攻击，攻击范围主要为中
东地区，攻击工具包括
Windows 和 Android 平
台，主要采取鱼叉或水坑
等攻击方式配合社会工
程学手段进行渗透，向特
定目标人群进行攻击。后
续国外安全厂商也将 Big
Bang 攻击行动与双尾蝎
联系到一起。
肚脑虫
别名:Donot
肚脑虫是奇安信威胁情
报中心披露的 APT 组织，
活跃在南亚地区，主要以
巴基斯坦为攻击目标，攻
击工具主要使用 yty 和
EHDevel 两套恶意软件
框架；分析师研究发现
该组织与 Hangover 和
Patchwork 存在联系。
APT33
别名:Elfin
APT33 是 FireEye
的 APT 组织，攻击
包括美国、沙特阿拉
韩国，主要针对航空
源领域实施攻击活动
Charming Kitte
别名:Newscaster、
Parastoo
Charming Kitten 网
间谍组织，从 2014
右开始活跃，主要针
事学术研究、人权和
的个人目标开展攻
动。该组织在 TTP
Magic Hound 组织
大量重叠。
Gamaredon Gr
别名:SectorC08、
Shuckworm
Gamaredon Group
少从 2013 年起活跃
攻击过乌克兰政府
人员。该团伙的攻击
与工具不断演进：
去严重依赖
off-the-shelf 工具
为自定义的恶意软
OPERATIO
ARMA-GEDDON 行
该组织有关。
2016
2017
奇安信披露

奇安信 | 奇安信威胁情报中心

Gorgon

别名：Gorgon Group

Gorgon 的历史攻击活动混合了网络犯罪活动和针对性的网络攻击活动，分析认为其针对性网络攻击活动与 C-Major 行动、ProjectM 存在联系。

黄金鼠

别名：Goldmouse

黄金鼠被安全厂商证实为某电子网军背景的 APT 组织，同时具备 Windows 和 Android 平台的恶意攻击能力。

DarkHydrus

别名：LazyMeerkat

DarkHydrus 主要针对中东的政府机构和教育机构实施攻击，以窃取机密为主，并且大量利用开源工具和自定义有效载荷进行攻击。

Sidewinder

别名：响尾蛇

SideWinder 疑似南亚的 APT 组织，曾针对巴基斯坦进行鱼叉式钓鱼邮件攻击。

黄金雕

别名：APT-Q-90

黄金雕的大部分攻击行动主要是针对哈萨克斯坦国境内的情报收集任务，其中也波及了我国驻哈萨克斯坦境内的机构和人员，除了传统的后门程序，黄金雕组织还采购了 Hacking-Team 和 NSO 的商业间谍软件。

虎木槿

别名：APT-Q-11

虎木槿疑似来自东北亚的 APT 组织，使用的恶意代码有着很强的隐蔽性，且具备 0day 漏洞发掘利用能力，曾通过浏览器漏洞攻击国内重点单位。

诺崇狮

别名：SilencerLion

诺崇狮是奇安信威胁情报中心披露的组织，活跃在中东地区，一直持续针对阿拉伯语用户、什叶派及评论人士展开攻击，旨在让被攻击者的社交平台账号变成“沉默账号”。

MKL

别名：

MKL
报中
针对
织，
追溯
恶意
装成
文件
动。
信的
展分
Feroc

2018 | 2019 | 2020 | 202

蓝宝菇

别名：BlueMushroom

蓝宝菇是奇安信威胁情报中心披露的 APT 组织，主要针对国内政府、军工、科研、金融等机构实施 APT 活动，攻击历史主要关注核工业和科研相关技术。

军刀狮

别名：ZooPark

军刀狮是卡巴披露的一个针对中东目标实施 APT 攻击的组织，其主要通过 Telegram 和水坑攻击分发恶意软件，该组织也重点针对库尔德人目标实施攻击活动。

盲眼鹰

别名：APT-Q-98

盲眼鹰是奇安信威胁情报中心披露的疑似南美洲地区的 APT 组织，从 2018 年 4 月起，针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等实施针对性攻击活动。

拍拍熊

别名：APT-Q-67

拍拍熊是一个针对某武装组织进行持续攻击的 APT 组织，同时拥有针对 Windows 和 Android 的攻击平台。

魔罗纱

别名：Confucius

魔罗纱是奇安信威胁情报中心披露的组织，活跃在南亚地区，一直持续针对中国、巴基斯坦的国防、军工、外交等单位进行攻击，擅长制造钓鱼网站并配合钓鱼邮件进行攻击，散布的恶意软件主要针对 Windows 和 Android 平台。

利刃鹰

别名：BladeHawk

利刃鹰主要针对伊斯兰国、基地组织、库尔德族群和土库曼族群进行持续攻击控制的活动，投递的均为与目标相关性极强的 APK 恶意软件，其中大部分为 Spynote 及其变种。

艾叶

别名：

艾叶
坦用
计划
活动
鱼网
攻击
Andr
锁定
巴基

奇安信威胁情报中心
持续跟踪49个主要APT团伙

奇安信披露

LG

Ferocious Kitten

G 是奇安信威胁情心首个披露的主要中东地区的 APT 组其最早攻击活动可至 2015 年。主要以宏 Word 文档、伪视频文件的可执行为载荷开展攻击活巴斯基根据奇安公开报告进行了拓析并将其命名为cious Kitten。

奇安信披露

摩耶象

别名：APT-Q-41

摩耶象是奇安信威胁情报中心在 2020 年发现的一个位于南亚地区长期针对巴基斯坦、尼泊尔、孟加拉等国进行间谍活动的 APT 组织。其攻击 CC 均为动态域名，木马均基于开源家族修改，主要攻击手段为鱼叉邮件。

奇安信披露

金刚象

别名：VajraEleph

金刚象是奇安信病毒响应中心披露的南亚 APT 组织，其主要针对巴基斯坦军方进行间谍情报活动，同时影响少数尼泊尔人员。该组织通过公开社交平台寻找攻击目标，并结合色情话术等进行钓鱼攻击，主要使用武器 VajraSpy RAT 对 Android 平台攻击。

1

2022

奇安信披露

豹

Snow leopard

豹主要针对巴基斯户展开了有组织、有针对性的长期监控，该组织一般利用钓站进行载荷投递。其击平台主要为oid，攻击目标主要为巴基斯坦用户及斯坦 TLP 政党。

奇安信披露

APT-Q-12

别名：伪猎者

APT-Q-12 是奇安信威胁情报中心内部长期跟踪的东亚 APT 组织，其专门针对贸易行业进行情报窃取活动，主要利用带有恶意 lnk 文件的钓鱼邮件进行攻击。该组织在 2021 年 10 月被国内安全厂商披露并命名为“伪猎者”。

附录2 奇安信威胁情报中心

威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

奇安信 ALPHA 威胁分析平台（https://ti.qianxin.com），是奇安信集团面向安全分析师和应急响应团队提供的一站式云端服务平台，该平台拥有海量互联网基础数据和威胁研判分析结果，为安全分析人员及各类企业用户提供基础数据的查询、攻击线索拓展、事件背景研判、攻击组织解析、研究报告下载等多种维度的威胁情报数据与威胁情报服务，提供全方位的威胁情报能力。

▼ 奇安信威胁情报中心对外服务平台

微信公众号
奇安信威胁情报中心

微信公众号
奇安信病毒响应中心

附录3 红雨滴团队(RedDrip Team)

奇安信旗下的高级威胁研究团队红雨滴（RedDrip Team，@RedDrip7），成立于2015年（前身为天眼实验室），持续运营奇安信威胁情报中心至今，专注于 APT 攻击类高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT 攻击组织的安全研究团队，也是当前奇安信威胁情报中心的主力威胁分析技术支持团队。

目前，红雨滴团队拥有数十人的专业分析师和相应的数据运营和平台开发人员，覆盖威胁情报运营的各个环节：公开情报收集、自有数据处理、恶意代码分析、网络流量解析、线索发现挖掘拓展、追踪溯源，实现安全事件分析的全流程运营。团队对外输出机读威胁情报数据支持奇安信自有和第三方的检测类安全产品，实现高效的威胁发现、损失评估及处置建议提供，同时也为公众和监管方输出事件和组织层面的全面高级威胁分析报告。

依托全球领先的安全大数据能力、多维度多来源的安全数据和专业分析师的丰富经验，红雨滴团队自2015 年持续发现多个包括海莲花在内的 APT 组织在中国境内的长期活动，并发布国内首个组织层面的APT 事件揭露报告，开创了国内 APT 攻击类高级威胁体系化揭露的先河，已经成为国家级网络攻防的焦点。

奇安信红雨滴团队

关注微信公众号

“红雨滴”背后的故事 — “从 100 亿个雨滴中找一个红雨滴”

2006 年 11 月 20 日，因发现 J 粒子而获得诺贝尔奖的著名华裔物理学家丁肇中教授来到中国驻瑞士大使馆，做了一场精彩的讲座。丁肇中教授形容自己发现构成物质的第四种基本粒子——J 粒子的高精度实验时说到：“相当于在北京下雨时，每秒钟有 100 亿个雨滴，如果有一个雨滴是红色的，我们就要从这 100 亿个里找出它来。”

而奇安信威胁情报中心高级威胁分析团队同样需要在海量数据中精准找寻那些红色威胁。最终，我们选择了“红雨滴”作为团队的名称。

附录4 参考链接

1.https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

2.https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

3.https://mp.weixin.qq.com/s/EQ8nrfE3tkfg4nB8F49VLA

4.https://mp.weixin.qq.com/s/W4hkBRJnwN1G32QCpaNNoA

5.https://www.proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds

6.https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf

7.https://asec.ahnlab.com/ko/47622/

8.https://asec.ahnlab.com/ko/47820/

9.https://www.welivesecurity.com/2023/02/23/winordll64-backdoor-vast-lazarus-arsenal/

10.https://mp.weixin.qq.com/s/iAGUMG7UmDFcB96HYhqRDw

11.https://asec.ahnlab.com/en/49295/

12.https://blog.alyac.co.kr/5102

13.https://blog.alyac.co.kr/5103

14.14. https://medium.com/s2wblog/kimsuky-group-appears-to-be-exploiting-onenote-like-the-cybercrime-group-3c96b0b85b9f

15.https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37

16.https://blog.cyble.com/2023/03/27/ghostsec-targeting-satellite-receivers/

17.https://threatmon.io/chinotto-backdoor-technical-analysis-of-the-apt-reapers-powerful/

18.https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage

19.https://asec.ahnlab.com/en/50625/

20.https://securelist.com/gopuram-backdoor-deployed-through-3cx-supply-chain-attack/109344/

21.https://blog.google/threat-analysis-group/how-were-protecting-users-from-government-backed-attacks-from-north-korea/

22.https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

23.https://blog.virustotal.com/2023/04/apt43-investigation-into-north-korean.html

24.https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

25.https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware/#

26.https://mp.weixin.qq.com/s/iCFz9vhYGxz0cd8_0-PhDQ

27.https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/

28.https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/

29.https://asec.ahnlab.com/ko/52662/

30.https://mp.weixin.qq.com/s/RjvwKH6UBETzUVtXje_bIA

31.https://www.genians.co.kr/hubfs/blogfile/threat_intelligence_report_apt37.pdf?hsLang=ko

32.https://asec.ahnlab.com/en/53132/

33.https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/

34.https://threatmon.io/reverse-engineering-rokrat-a-closer-look-at-apt37s-onedrive-based-attack-vector/

35.https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3413621/

us-rok-agencies-alert-dprk-cyber-actors-impersonating-targets-to-collect-intell/

36.https://mp.weixin.qq.com/s/v5JGN15kVr4zGjPkCeuovQ

37.https://mp.weixin.qq.com/s/G3gUjg9WC96NW4cRPww6gw

38.https://www.group-ib.com/blog/dark-pink-apt/

39.https://mp.weixin.qq.com/s/7KOjLgeHsgEI7KuDhFOiKA

40.https://mp.weixin.qq.com/s/_WMljf41eTsBrQDa3BjFTQ

41.https://mp.weixin.qq.com/s/w--fSiFrHQUaIv80AuitZQ

42.https://www.group-ib.com/blog/dark-pink-episode-2/

43.https://www.elastic.co/cn/security-labs/elastic-charms-spectralviper

44.https://mp.weixin.qq.com/s/JbaEpcmvC80EoE8X0DnwKQ

45.https://mp.weixin.qq.com/s/P7VXmHIB5dJl9ZoE1OBDww

46.https://mp.weixin.qq.com/s/7Q2nulqLsofjSftbWQt2kA

47.https://mp.weixin.qq.com/s/rslBGQgTL_jZD73AJqI05Q

48.https://mp.weixin.qq.com/s/SR-m-RrqyT3V2zkOPBm-9g

49.https://mp.weixin.qq.com/s/xU7b3m-L2OlAi2bU7nBj0A

50.https://threatmon.io/apt-sidecopy-targeting-indian-government-entities/

51.https://mp.weixin.qq.com/s/yX8iKaPSr9VS3Z2wsgdisw

52.https://mp.weixin.qq.com/s/RD03YH2ngRUbUmE80d18Uw

53.https://www.welivesecurity.com/2023/03/07/love-scam-espionage-transparent-tribe-lures-indian-pakistani-officials/?web_view=true

54.https://mp.weixin.qq.com/s/lvSraGnMsl3a1jEUubuvyw

55.https://ti.qianxin.com/blog/articles/Analysis-of-SideCopy-Group's-Recent-Attacks-Using-Indian-

Ministry-of-Defense-Documents-as-Lures-CN/

56.https://blog.cyble.com/2023/03/21/notorious-sidecopy-apt-group-sets-sights-on-indias-drdo/

57.https://ti.qianxin.com/blog/articles/Heavy-Shadows:Summary-of-Recent-Attack-Techniques-Used-by-Donot-Group-CN/

58.https://www.intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/

59.https://asec.ahnlab.com/ko/50851/

60.https://www.sentinelone.com/labs/transparent-tribe-apt36-pakistan-aligned-threat-actor-expands-interest-in-indian-education-sector/

61.https://www.cyfirma.com/outofband/donot-apt-targets-individuals-in-south-asia-using-android-malware/

62.https://mp.weixin.qq.com/s/sO2rJbYbqLcYb3AvAUMeGg

63.https://www.uptycs.com/blog/cyber_espionage_in_india_decoding_apt_36_new_linux_malware

64.https://mp.weixin.qq.com/s/Nk2zml2d0HtK0hszyKW2Dw

65.https://ti.qianxin.com/blog/articles/Sidecopy-Group-Launches-Attacks-on-India-Using-a-New-Trojan-CN/

66.https://www.seqrite.com/blog/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions

67.https://mp.weixin.qq.com/s/Lb_NYxhi9iJgmvI2wjY9qg

68.https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan

69.https://mp.weixin.qq.com/s/sYk4pTMJloRuogBMnD3hRg

70.https://www.group-ib.com/blog/hunting-sidewinder/

71.https://mp.weixin.qq.com/s/g8oSytVgRSV2773kwZYUHA

72.https://mp.weixin.qq.com/s/DhQj9-0QLwVSQYH_uGDw2g

73.https://mp.weixin.qq.com/s/WU0VnMCf-FQyXiBkZfZAEw

74.https://mp.weixin.qq.com/s/H-ZRvcofbzwZ8Ikyn5Vu4w

75.https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

76.https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegram-to-target-ukrainian-organizations

77.https://cert.gov.ua/article/3718487

78.https://securityaffairs.com/141473/apt/sandworm-targets-ukraine-swiftslicer.html

79.https://therecord.media/latvia-confirms-phishing-attack-on-ministry-of-defense-linking-it-to-russian-hacking-group/

80.https://cert.gov.ua/article/3761023

81.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer

82.https://mrtiepolo.medium.com/russian-apt-gamaredon-exploits-hoaxshell-to-target-ukrainian-organizations-173427d4339b

83.https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58

84.https://threatmon.io/beyond-bullets-and-bombs-an-examination-of-armageddon-groups-cyber-warfare-against-ukraine/

85.https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine

86.https://informnapalm.org/en/hacked-russian-gru-officer/

87.https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services

88.https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor/

89.https://blog.eclecticiq.com/exposed-web-panel-reveals-gamaredon-groups-automated-spear-phishing-campaigns

90.https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108

91.https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

92.https://www.viewintech.com/html/articledetails.html?newsId=35

93.https://labs.withsecure.com/publications/fin7-target-veeam-servers

94.https://www.prodaft.com/resource/detail/paperbug-nomadic-octopus-paperbug-campaign

95.https://cert.gov.ua/article/4492467

96.https://cert.gov.ua/article/4501891

97.https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/analyzing-the-ntc-vulkan-leak-what-it-says-about-russias-cyber-capabilities/

98.https://socradar.io/dark-web-profile-muddywater-apt-group/

99.https://www.welivesecurity.com/2023/01/10/strongpity-espionage-campaign-targeting-android-users/

100.https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html

101.https://www.gov.il/en/departments/news/_muddywater

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

103.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks

104.https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/

105.https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-

sandstorm-refines-tradecraft-to-attack-high-value-targets/

106.https://www.group-ib.com/blog/muddywater-infrastructure/

107.https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-targeting-israel-via-improved-arsenal-of-tools/

108.https://www.bitdefender.com/blog/businessinsights/unpacking-bellaciao-a-closer-look-at-irans-latest-malware/

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

110.https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/

111.https://ti.qianxin.com/blog/articles/Analysis-of-Recent-Attacks-Against-Russia-by-The-Suspected-Kasablanka-Group/

112.https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool

113.https://mp.weixin.qq.com/s/y8VVzTWeFNG3MMih1KFxFw

114.https://www.elastic.co/cn/security-labs/elastic-security-labs-discovers-lobshot-malware

115.https://www.recordedfuture.com/oilalpha-likely-pro-houthi-group-targeting-arabian-peninsula

116.https://securelist.com/goldenjackal-apt-group/109677/

117.https://interlab.or.kr/archives/18979

118.https://twitter.com/RedDrip7/status/1640966547081662464

119.https://securelist.com/operation-triangulation/109842/

120.https://www.barracuda.com/company/legal/esg-vulnerability

121.https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

奇安信 | 奇安信 威胁情报中心

邮箱：ti_support@qianxin.com
电话：95015
官网：https://ti.qianxin.com
扫描关注我们的微信公众号