APT

全球高级持续性威胁（APT）2022年中报告

2022年07月

奇安信
威胁情报中心

主要观点

MAIN POINTS

2022 上半年全球范围内，国防军事相关的攻击事件占比达到 21%，成为继政府之后的第二大攻击目标。另外，金融、能源行业相关攻击事件也增长较多，占比分别为 13%、11%。

俄乌冲突使得该地区成为 APT 攻击的重灾区，数据擦除软件攻击不断出现。随着冲突的升级，全球黑客也各自选边站队，卷入乱局。网络信息舆论战也成为网络战中的重要一环。

针对我国国内的攻击主要来自周边地区的 APT 组织，攻击主要集中在 5、6 月份。从受害行业来看，针对金融和互联网科技的攻击较去年有所增长。

2022 上半年以来，0day 漏洞仍是攻击者喜好的一大攻击武器；在经济利益的驱使下，针对金融行业的攻击加剧；受俄乌冲突影响，国防军事目标也成为攻击热点。

2022 年上半年 0day 漏洞的攻击使用整体趋于缓和，比之 2021 年有大幅下降，但同比 2020 年的 0day 在野漏洞攻击依然有所增加。以浏览器为核心的漏洞攻击向量仍然是主流趋势，其中大部分为沙箱逃逸漏洞，主要源自之前漏洞补丁绕过的变种。

摘 要

ABSTRACT

奇安信威胁情报中心使用奇安信威胁雷达对 2022 上半年境内的 APT 攻击活动进行了全方位遥感测绘。数据表明，河南是上半年以来 APT 组织的重点目标地区，经济发达的北京、广东及上海地区依然位为前列，其次是江苏、福建、山东等沿海地区。

针对我国目标进行高频攻击的 APT 组织主要为海莲花、APT-Q-12、金眼狗等。攻击者主要针对我国政府机构、金融、互联网科技等行业进行攻击。

2022 上半年内，奇安信威胁情报中心收录了高级持续性威胁相关公开报告总共 181 篇。其中，提及率最高的 5 个 APT 组织分别是：Gamaredon 6.8%，Lazarus 6.2%，Kimsuky 5.7%，C-Major 4.6%，海莲花 4%。涉及政府的攻击事件占比为 27%，其次国防军事相关事件占比为 21%，金融占比 13%、能源占比 11%。

俄乌冲突中，多方势力在网络空间这个不见硝烟的战场上进行着激烈较量，其中既有国家背景 APT 组织的踪迹，也有普通黑客团体的活跃身影，还有多国在网络信息舆论战上的对抗。

在俄乌冲突背景下的网络战中常出现的攻击手段有：数据擦除攻击、分布式拒绝服务（DDoS）攻击、以信息窃取为目的的 APT 攻击，以及网络信息舆论战。

2022 年上半年 0day 漏洞的攻击使用整体趋于缓和，比之 2021 年有大幅下降，但同比 2020 年却有所上升。奇安信威胁情报中心梳理发现，以浏览器为核心的漏洞攻击向量依然是主流趋势。其中 Chrome，Firefox，Safari 及对应平台下 Windows，MacOS，IOS 的沙箱逃逸漏洞占所有漏洞近 7 成，这里面近 5 成漏洞源自之前漏洞补丁绕过的变种。

关键字：俄乌冲突、高级持续性威胁、APT、0day、军事

目 录

CATALOGUE

第一章 俄乌冲突背景下的网络战

今年上半年 2 月 24 日俄乌战争打响，俄乌冲突与其他战争最显著的不同在于全球众多身处物理战场之外的群体通过网络也参与到对抗之中。战前乌克兰就遭受了一系列针对性的网络攻击，冲突爆发后针对性网络攻击更是常伴随军方的行动发生，网络层面和物理层面的攻击呈现出配合的态势。针对乌克兰的定向网络攻击除了有利用木马后门进行信息窃取与情报收集，还包括借助数据擦除软件瘫痪和破坏特定信息系统。而乌克兰在欧美支持下取得全球范围内网络信息舆论战的优势，吸引了众多黑客团体为其站队。这些黑客团体在开战后频繁向俄罗斯重要组织机构发起攻击，并将攻击得手后获取的内部数据在网上公开。

多方势力在网络空间这个不见硝烟的战场上进行着激烈较量，其中既有国家背景 APT 组织的踪迹，也有普通黑客团体的活跃身影，还有多国在网络信息舆论战上的对抗。本章将对这场网络战演进过程进行简单梳理，并总结此次网络战呈现的一些特点。

一、网络战演进过程

奇安信威胁情报中心根据奇安信内部数据视野及互联网公开渠道收集的网络攻击数据分析，网络空间的交锋早于战争率先开始，在正式进入军事冲突后，双方的网络行动则以破坏性攻击活动为主、网络信息战为辅。随着乌克兰局势的不断升级，多国围绕乌克兰问题的博弈也延伸到网络领域，以美国为首的各国表面上并未参与实际的网络战，却利用自身的互联网优势引导全球黑客选边站队卷入乱局，导致网络战线全面拉开。

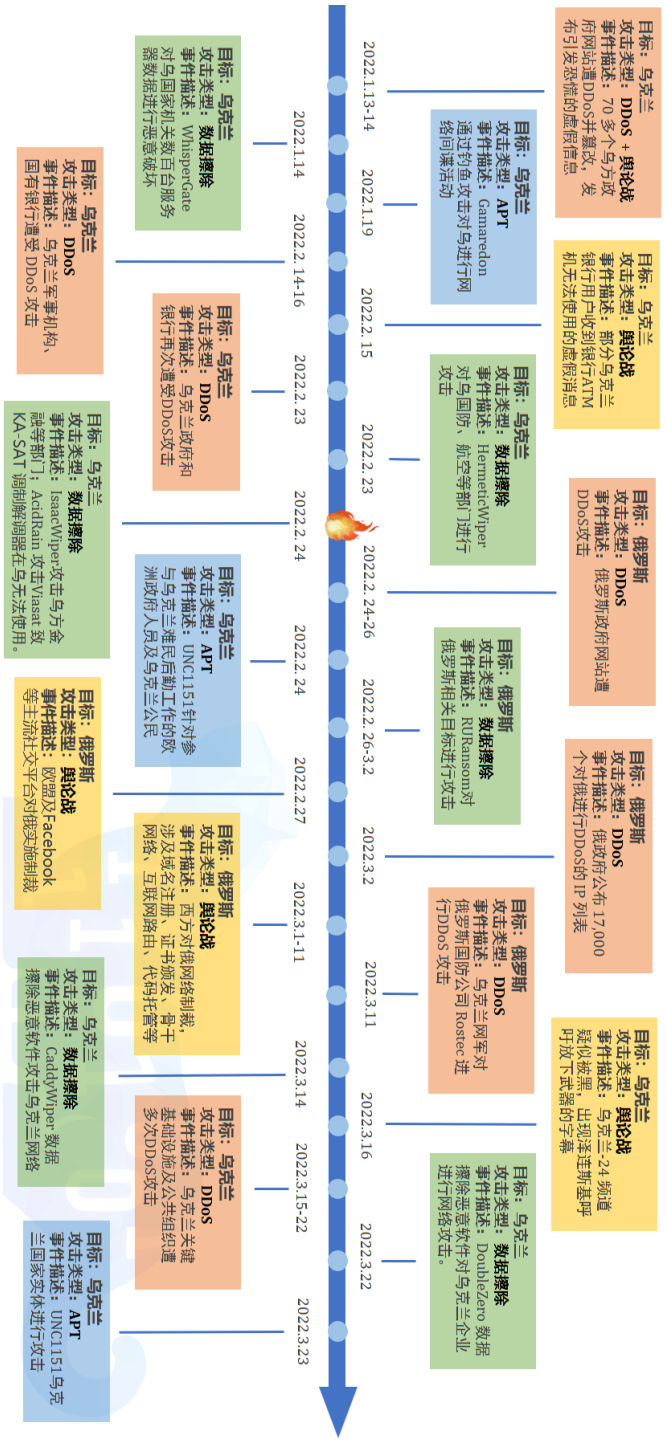
（一）网络战攻击手段与大事件

此次网络战中常出现的攻击手段有：数据擦除攻击、分布式拒绝服务（DDoS）攻击、以信息窃取为目的的 APT 攻击，以及网络信息舆论战。

俄乌冲突期间多款数据擦除型恶意软件被发现，这些恶意软件清除磁盘特定数据，或导致重要文件数据损毁，或直接使系统无法启动，本章后面内容会对这些恶意软件进行具体说明。DDoS 攻击是一种门槛低但效果明显的网络攻击手段，在各方势力参与的网络战中，针对俄乌两国的 DDoS 攻击频繁发生。在国家对抗的背景下，不乏 APT 组织的活动踪迹，APT 攻击以亲俄背景组织为主，这些组织除了被发现与某些数据擦除恶意软件有关，还不断通过定向的网络钓鱼攻击开展情报收集活动，奇安信根据公开报告以及内部数据整理了俄乌冲突背景下的 APT 攻击活动（见附表 1）。网络信息舆论战，有别于直接的网

络攻击，是传统舆论战心理战的升级版，通过网络空间发布有利于己方和不利于对方的虚实信息，混淆视听，或震慑对方心理，或影响判断认知，达到在全球范围内收割同情和支持的目的。

俄乌战争爆发前后涉及两国的网络冲突重大事件如下图所示。



▲ 图 1.1 俄乌冲突背景的网络战大事件

（二）战前网络行动

在俄罗斯特别军事行动之前，乌克兰便爆发了针对其政府机构等关键部门的数据擦除恶意软件攻击和大规模分布式拒绝服务（DDoS）攻击。2022 年 1 月 13 日，数据擦除恶意软件 WhisperGate 出现在乌克兰多个组织的计算机系统中。2022 年 1 月，约 70 个乌克兰政府网站由于遭到 DDoS 攻击而暂时下线。2 月 14 日起，乌克兰的军事、政府、金融等部门的网络系统再次遭到大规模 DDoS 攻击。

```
.3DM .3DS .7z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP .BAK .BAT .BMP .BRD .BZ .BZ2
.CGM .CLASS .CMD .CONFIG .CPP .CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH
.DOC .DOCB .DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM .GIF .GO .GZ .HDD .HTM
.HTML .HWP .IBD .INC .INI .ISO .JAR .JAVA .JPEG .JPG .JS .JSP .KDBX .KEY .LAY .LAY6
.LDF .LOG .MAX .MDB .MDF .MML .MSG .MYD .MYI .NEF .NVRAM .ODB .ODG .ODP .ODS .ODT .OGG
.ONETOC2 .OST .OTG .OTP .OTS .OTT .P12 .PAQ .PAS .PDF .PEM .PFX .PHP .PHP3 .PHP4 .PHP5
.PHP6 .PHP7 .PHPS .PHTML .PL .PNG .POT .POTM .POTX .PPAM .PPK .PPS .PPSM .PPSX .PPT
.PPTM .PPTX .PS1 .PSD .PST .PY .RAR .RAW .RB .RTF .SAV .SCH .SHTML .SLDM .SLDX .SLK
.SLN .SNT .SQ3 .SQL .SQLITE3 .SQLITEDB .STC .STD .STI .STW .SUO .SVG .SXC .SXD .SXI
.SXM .SXW .TAR .TBK .TGZ .TIF .TIFF .TXT .UOP .UOT .VB .VBS .VCD .VDI .VHD .VMDK .VMEM
.VMSD .VMSN .VMSS .VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS .XHTML
.XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .XLW . YML .ZIP
```

▲ 图 1.2 WhisperGate 损毁目标计算机的文件类型列表

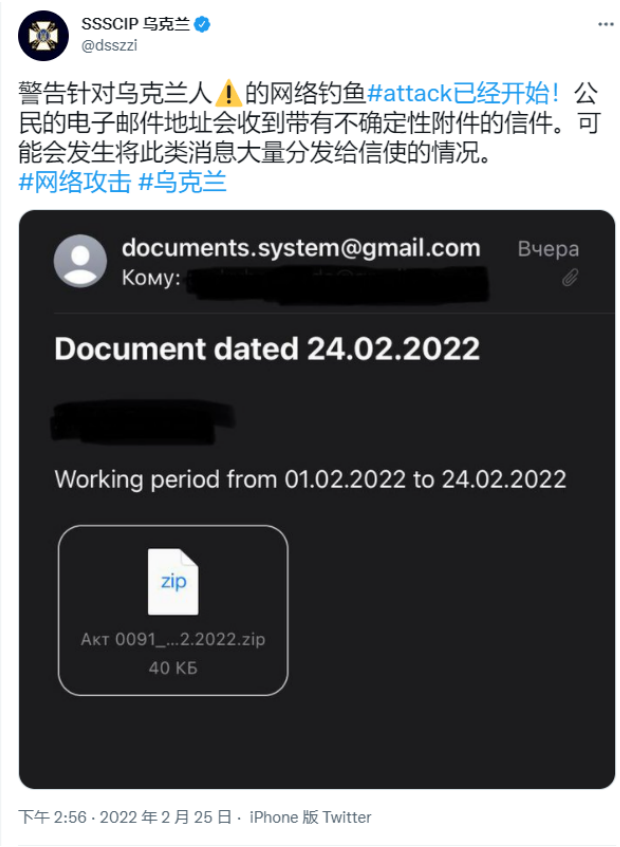
在俄乌两国局势紧张期间，乌克兰除了遭受网络攻击，还受到多起网络信息战行动的影响。2022 年 1 月 13 日，乌克兰政府网站遭到篡改，修改后的网站页面发布了旨在散播恐慌的虚假信息。2 月 15 日，部分乌克兰 Privatbank 银行用户收到银行 ATM 机无法使用的虚假消息。乌克兰有关部门还查封了一个拥有超过 18 万个社交媒体账号、用来散布假新闻的僵尸网络。

（三）战争爆发时的网络攻击

在俄乌战争爆发的时间点附近，又有两种数据擦除恶意软件出现在乌克兰重要组织机构的信息系统中。2022 年 2 月 23 日，俄乌战争爆发前一天，一款被称为 HermeticWiper 的新型数据擦除恶意软件感染了至少五个乌克兰组织的数百台计算机。2 月 24 日，针对乌克兰政府组织的第三种数据擦除恶意软件 IsaacWiper 在新一轮网络攻击中出现，值得注意的是，IsaacWiper 出现在未受 HermeticWiper 影响的乌克兰政府组织中。

与此同时，亲俄背景的 APT 组织也继续利用网络钓鱼攻击进行情报刺探。比如，乌克兰国家特殊通信和信息保护局于 2 月 25 日披露了与 UNC1151 APT 组织相关的网络钓鱼邮件，邮件内容中涉及到 2 月 24

日这个日期。



▲ 图 1.3 乌克兰官方披露的网络钓鱼邮件

（四） 西方国家下场，网络战拉锯相持

以美国为首的西方国家开始下场支持乌克兰，乌克兰方面对俄发动网络攻击，网络战进入拉锯相持阶段。

在网络信息舆论战方面，美国和乌克兰政客鼓动黑客对俄罗斯发起网络攻击，比如乌克兰在战争打响后不久开始筹建 IT 志愿者大军。同时，欧美的主流信息渠道禁言俄罗斯。2 月 27 日，欧盟宣布禁止俄罗斯官方媒体“今日俄罗斯”（RT）和俄罗斯卫星通讯社（Sputnik）在欧盟境内传播信息，随后，主流社交平台和跨国信息科技公司纷纷跟进。西方国家尤其是美国利用自己对全球主流媒体、社交平台的掌控，以及诞生于美国的一批跨国信息科技公司在互联网世界的资源主导权，不断对俄罗斯的舆论发声渠道进行围追堵截。这一系列限制措施导致俄罗斯官方媒体被封而难以发声，对俄罗斯的不利舆论呈一边倒趋势，俄罗斯在全球舆论战场上已落于下风。

在西方国家对国际舆论主导权的加持之下，美乌政客对网络攻击行为的鼓动引起更多黑客组织卷入俄乌纷争，尤其是支持乌克兰一方的组织数量大增。不过根据持续追踪发现，3 月中旬以后各黑客组织公布

的消息逐渐减少。原因是一些黑客为蹭热度而公布的数据“虚有其表”，导致其公信力下降。奇安信总结了自俄乌冲突升级后，各黑客组织参与网络混战的具体情况，详情请参阅附表 2。

开战以后，针对俄乌两国的 DDoS 攻击频发，攻击对象经常是两国的重要网站。在战争爆发后一个多月的时间里，奇安信监测到乌克兰地区被 DDoS 攻击事件 40 余起，俄罗斯地区被 DDoS 攻击事件超 100 起。被 DDoS 攻击的重要网站涉及乌克兰的政府机构、新闻媒体、高等院校，和俄罗斯的政府机构、新闻媒体、金融机构、社交平台。

同时，支持乌克兰的黑客团体选择俄罗斯重要机构发起网络入侵，并导致被攻击机构的数据泄露。攻击团体以 Anonymous（匿名者）、AgainstTheWest (ATW)、乌克兰网络部队为首，目标包括俄罗斯政府机构、国有银行、航天公司、原子能机构、天然气石油公司、国家通讯监管机构、军工企业、国家媒体机构等。

另一方面，乌克兰的关键基础设施也成为网络攻击的重点目标。3 月 28 日，乌克兰互联网服务提供商 Ukrtelecom 遭受网络攻击，导致乌克兰发生俄乌战争以来最严重的流量中断事件。4 月 12 日，乌克兰政府表示针对乌克兰电网的网络攻击已被成功阻止，攻击的破坏行为原计划于 4 月 8 日启动，如果攻击成功实施，将摧毁乌克兰多个变电站和电网，影响范围约为 200 万人，此次攻击行动被认为由 APT 组织 Sandworm 发起。

二、网络战特点

在此次网络战中，以数据擦除攻击为代表的破坏性网络攻击不断出现，双方阵营尽其所能向着对方重要组织机构和关键基础设施发起猛攻，同时双方在网络信息舆论战上也展开了激烈较量。

（一）数据擦除软件不断出现

数据擦除软件通过清除计算机上的重要文件数据或者直接让计算机无法启动，达到破坏或瘫痪相关信息系统的目的。目前已披露的与这场网络战相关的数据擦除型恶意软件有下面几种。

名称	披露时间	特点	相关攻击事件
WhisperGate	2022-01-15	覆盖磁盘的主引导记录，覆盖特定类型文件的数据	2022 年 1 月 13 日针对乌克兰多个组织。
HermeticWiper	2022-02-23	覆盖磁盘主引导记录、主文件表，清除大部分系统文件	2022 年 2 月 23 日在乌克兰多个组织中观察到该数据擦除软件。

名称	披露时间	特点	相关攻击事件
IsaacWiper	2022-03-01	用随机数据覆盖每个磁盘前 0x10000 字节，并擦除磁盘上的文件数据	在 2022 年 2 月 24 日至 26 日针对乌克兰的又一波网络攻击中出现。
RURansom Wiper	2022-03-08	针对俄罗斯，加密磁盘上的文件，每个文件的加密密钥唯一且不会保存，导致加密过程不可逆	在 2022 年 2 月 26 日至 3 月 2 日安全厂商检测到该软件的不同版本。
CaddyWiper	2022-03-15	清除磁盘上的用户数据以及分区信息。借助域策略部署在受害者机器上，恶意软件会避免清除域控主机的数据。	2022 年 3 月 15 日在少数乌克兰组织上发现。2022 年 4 月，Sandworm APT 组织计划针对乌克兰电网的破坏性攻击行动中也使用了 CaddyWiper。
DoubleZero	2022-03-22	使用两种数据清零方法清除文件数据。首先销毁所有磁盘上的一切非系统文件，然后按顺序清除系统文件，最后销毁 Windows 注册表相关数据。	2022 年 3 月 17 日在针对乌克兰企业的攻击中被发现。
AcidRain	2022-03-31	一种基于 MIPS 架构的 ELF 格式恶意软件，被用于擦除调制解调器和路由器上的数据。对 Linux 设备的文件系统和各种已知的存储设备文件执行深度擦除。	2022 年 2 月 24 日，一次网络攻击使 Viasat KA-SAT 调制解调器在乌克兰无法运行，导致 Viasat 在乌克兰的卫星通信服务中断。

▲ 表 1.4 网络战中出现的数据擦除软件

（二）重要组织机构和关键基础设施成为重点攻击目标

参与此次网络战的团体，无论采用何种攻击手段，都更倾向于进攻对方的重要组织机构和关键基础设施：乌克兰遭受的破坏性网络攻击和 APT 攻击直指相关组织机构和重要部门，针对两国的 DDoS 攻击常以重要机构的网站作为目标，普通黑客团体也会拿对方的重要部门开刀发动网络入侵。

重要组织机构和关键基础设施由于关系重大，导致其可用性、完整性、保密性一旦被破坏，将产生深刻的影响，因此在这场国家对抗背景下的网络战中变成了网络攻击者虎视眈眈的目标。这也提醒我们对关键基础设施的保护片刻不能松懈。

（三） 网络信息舆论战的攻心较量

此次网络信息战中网络攻防和涉及信息舆论的认知控制战相互交织，舆论战成为网络战争中的重要一环。在现代网络出现之前，舆论战已经是军事战争中的常规手段，不过如今互联网的触手已经遍及每个人，这使得舆论战的覆盖面和影响度远超从前。无论是冲突前期乌克兰因为传播的虚假信息而引发社会恐慌情绪，还是后面西方国家凭借对主流信息渠道的控制权创造出对俄舆论的压倒性态势，都可以看出在网络攻防之外，左右民众认知的网络舆论战也发挥着不容忽视的作用。

三、由俄乌冲突引发的其他 APT 攻击事件

俄乌冲突背后西方的介入，使得亲俄背景的 APT 组织攻击行动不只针对乌克兰，攻击目标也覆盖到一些西方国家。

自 2022 年 1 月中旬开始，APT29 组织就开展了针对欧洲多国外交机构的网络钓鱼活动。俄乌战争爆发后，UNC1151 APT 组织向欧洲政府发起网络攻击，收集有关乌克兰难民管理的相关情报。2022 年 3 月，乌克兰计算机应急响应小组（CERT-UA）发现了 Gamaredon 组织发送给拉脱维亚政府机构的钓鱼邮件。Turla 组织也被观察到针对波罗的海国防学院等目标的攻击行动。

此外，APT 组织往往会利用时事新闻作为攻击诱饵，而俄乌冲突作为 2022 年的一大热点事件，便成为了攻击者制作诱饵的素材。国外友商在一篇报告中就披露了以俄乌冲突相关事件为诱饵的组织，这些组织分布于拉丁美洲、中东和亚洲，并不局限于特定地区。

组织名称	组织起源	目标部门	目标国家
El Machete	西班牙语国家	金融、政府	尼加拉瓜、委内瑞拉
Lyceum	伊朗	能源	以色列、沙特阿拉伯
SideWinder	疑似印度	未知	巴基斯坦

▲ 表 1.5 以俄乌冲突为诱饵的攻击组织

第二章 中国境内高级持续性威胁综述

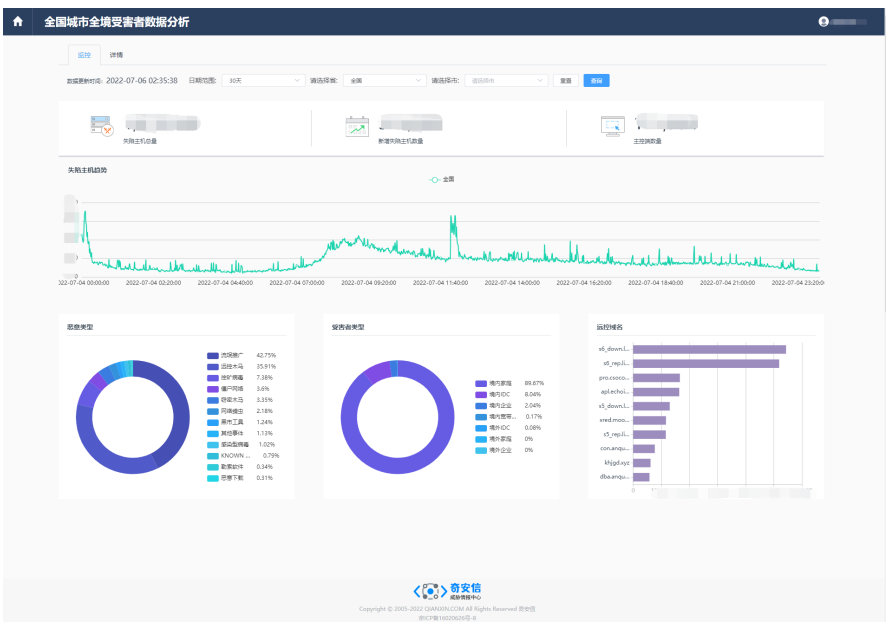
基于中国境内海量 DNS 域名解析和奇安信威胁情报中心失陷检测（IOC）库的碰撞分析（奇安信威胁雷达），是了解我国境内 APT 攻击活动及高级持续性威胁发展趋势的重要手段。

2021 年，奇安信威胁情报中心首次在《全球高级持续性威胁 (APT)2021 年度报告》中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。

本报告继续使用奇安信威胁雷达对 2022 年上半年境内 APT 攻击活动进行遥感测绘，结合奇安信红雨滴团队在客户现场处置排查的真实 APT 攻击事件以及使用奇安信威胁情报的全线产品告警数据，整理与分析后得出本章内容及结论。

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。



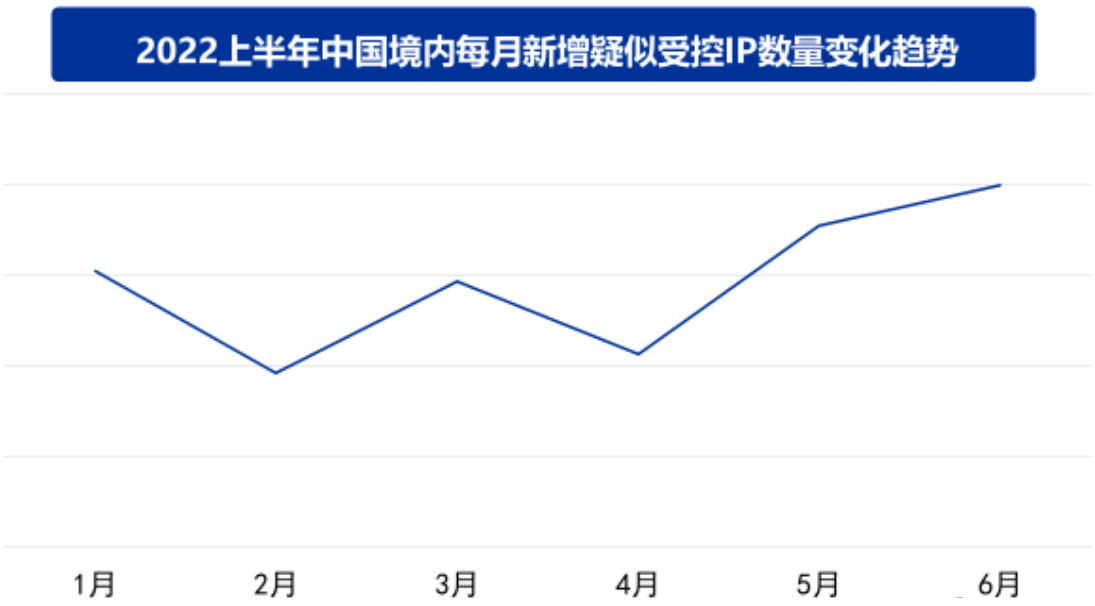
▲ 图 2.1 奇安信威胁雷达境内受害者数据分析

基于奇安信威胁雷达境内的遥测分析，我们从受控 IP 数量和趋势、受害目标区域分布、APT 组织资产分布三方面对我国境内疑似遭受的 APT 攻击进行分析和统计。

（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 2022 上半年监测到我国境内 IP 地址与多个境外 APT 组织 C2 服务器（Command & Control Server，远控服务器）发生通信行为。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。

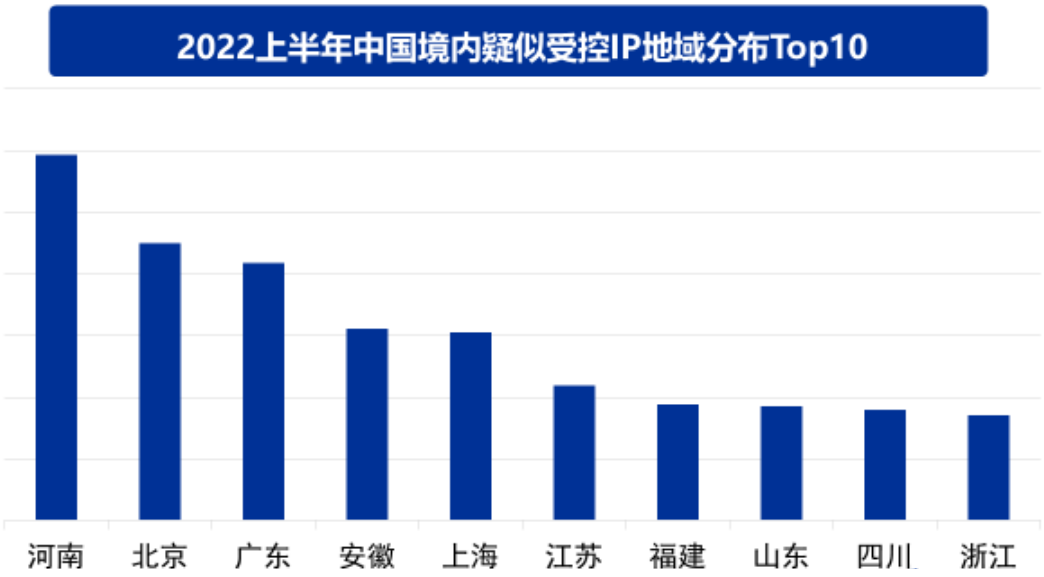
2022 上半年中国境内每月新增疑似被境外 APT 组织控制的 IP 地址数量变化趋势如图 2.2 所示。



▲ 图 2.2 2022 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

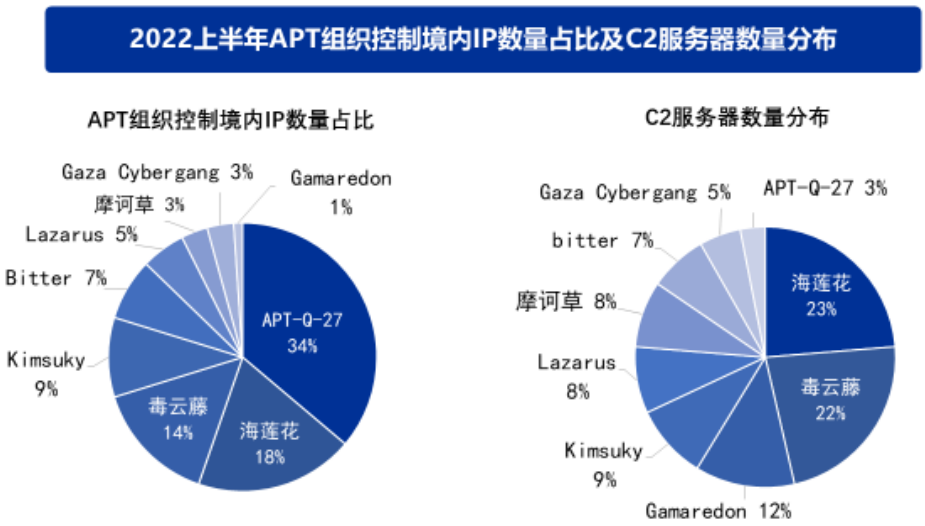
下图为 2022 上半年中国境内疑似连接过境外 APT 组织 C2 服务器的 IP 地址数量较多的前 10 个省份地域。从图中可以看出，河南是上半年以来 APT 组织攻击的重点目标地区，经济发达的北京、广东及上海地区依然位为前列，其次是江苏、福建、山东等沿海地区。



▲ 图 2.3 2022 上半年中国境内疑似受控 IP 地址地域分布

（三）APT 组织资产分布

奇安信威胁雷达检测到 2022 上半年内有数十个境外 APT 组织对我国境内 IP 地址发生过非法连接，下图分别展示了上半年内针对我国境内目标攻击的主要几个境外 APT 组织具体占比情况以及对应组织疑似使用过的 C2 服务器数量分布。



▲ 图 2.4 2022 上半年 APT 组织控制境内 IP 地址数量占比及 C2 服务器所属团伙数量分布

上图数据表明 2022 上半年内我国境内大部分 IP 地址主要被我国周边东亚、东南亚地区的 APT 组织控制，其次是南亚和中东地区。

东亚地区攻击我国境内目标的主要是毒云藤组织，该组织长期针对我国，擅于通过模仿正常域名来实施钓鱼攻击。在近期针对国内多个重点单位的钓鱼活动中，毒云藤组织将目标域名嵌入其钓鱼域名中以达到迷惑作用，目标涵盖了教育、科研、政府、航空等领域。

海莲花是另一个长期以我国为主要攻击对象的 APT 组织，其控制我国境内 IP 地址数量与 C2 服务器数量占比相对一致，说明海莲花组织会在不同攻击活动中使用不同的 C2 服务器。

二、2022 上半年针对我国的活跃组织

基于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，结合使用威胁情报的全线产品产生的告警数据，分析可知针对我国目标进行高频攻击的 APT 组织主要为海莲花、APT-Q-12、金眼狗等。

奇安信威胁情报中心整理了以上三个组织的真实 APT 攻击处置案例，由此来分析 2022 上半年内针对我国的全球 APT 组织。

（一）APT-Q-31（海莲花）

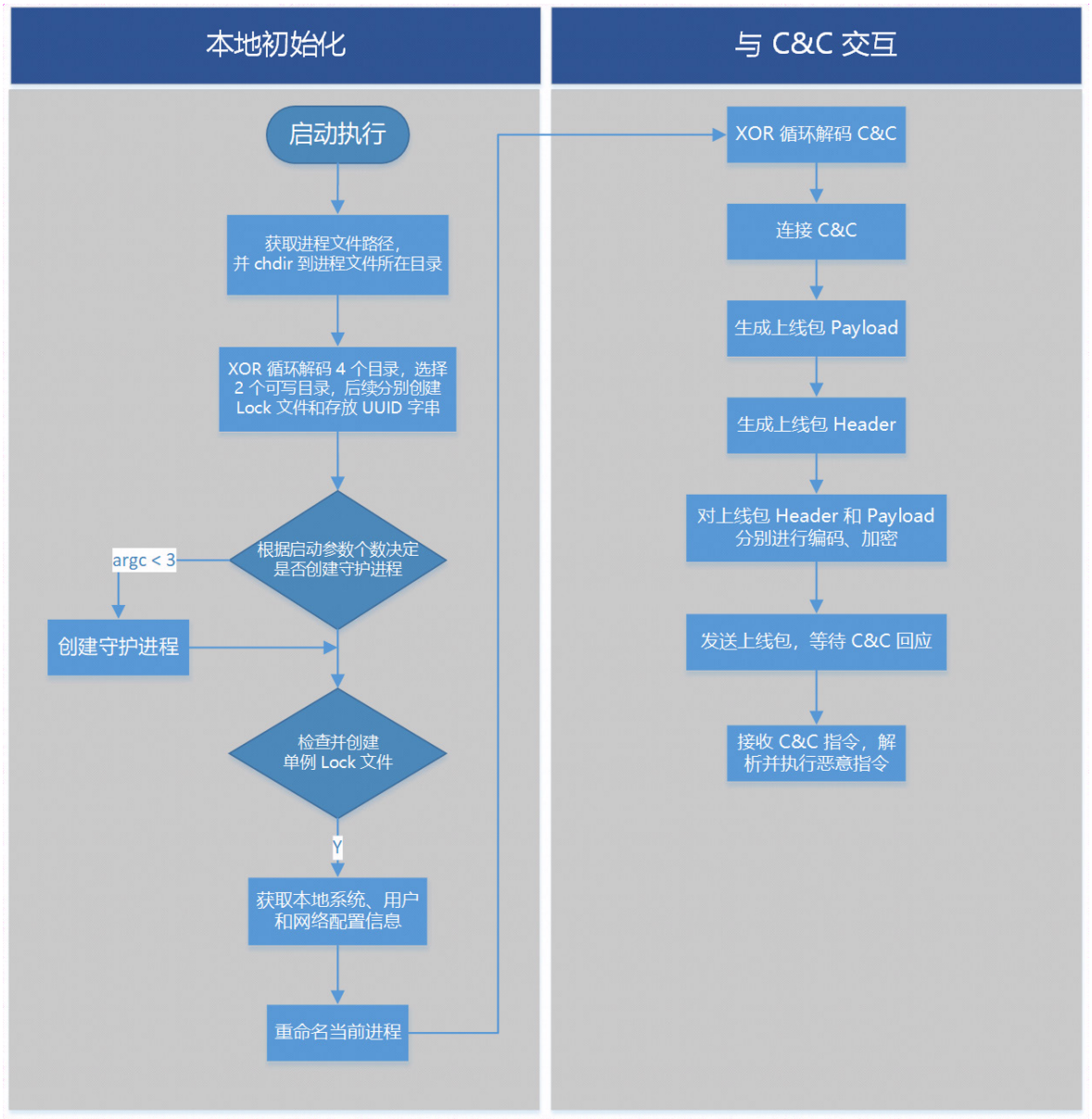
关键词：跳板、国产化系统、Nday 漏洞

海莲花在 2022 年利用测绘平台使用 Nday 漏洞对我国境内资产进行撒网式攻击，受害者中竟存在色情网站，海莲花拿到权限后从中挑出高价值的目标进行内网渗透，剩下的则作为跳板或者代理用来扫描和攻击。

最近我们观察到海莲花开始针对中国台湾、中国香港等地区的 IoT 设备进行批量入侵并将其当作跳板攻击中国大陆重要基础设施。攻击者在攻击过程中尝试上传 busybox 和 Dropbear 等软件包，最终在 IoT 设备上运行端口转发工具 tinyPortMapper，将特定端口的流量转发到自己的 Cobalt Strike 服务器，同时我们在这些受控的 IoT 设备上发现了海莲花最新的 Arm 架构的木马。

在代码层面，海莲花使用 msbuild.exe 编译源码的方式规避杀软查杀，执行 Loader 程序最终内存加载 Cobalt Strike，除此之外还会使用 github 上最新出现的免杀 loader 来加载后续木马，例如 shhhloader 和 Mortar Loader。在有些攻击事件中海莲花仅使用由 Golang 编写的隧道木马来实现远程控制。

经过研判，海莲花在 2022 年 5 月份针对国产化系统进行了定向攻击，我们拿到了海莲花首个针对 mips 架构的木马程序，其代码逻辑和通信协议与 Arm 架构的木马相同，我们将其命名为“Caja”。



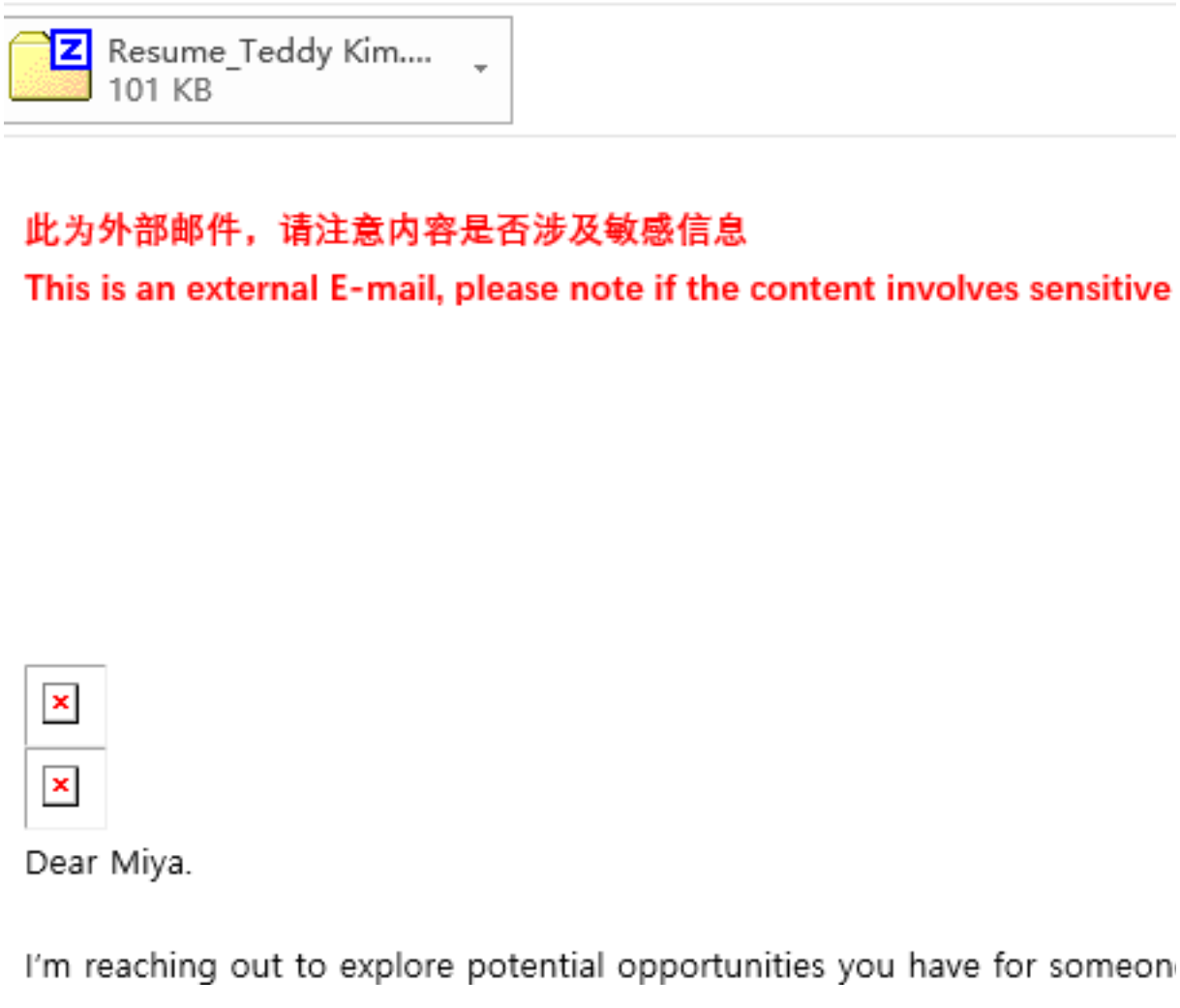
▲ 图 2.5 Caja 木马执行流程

奇安信威胁情报中心会在 2022 年下半年择机披露该组织最新的攻击活动。

（二）APT-Q-12（伪猎者）

关键词：鱼叉、驻韩使馆、芯片制造业、风投公司

由于朝韩地区的 APT 组织通常会给攻击目标的个人邮箱账号投递鱼叉邮件，受害 IP 多为家庭宽带，这加大了我们对该方向的监控难度。APT-Q-12 团伙在今年上半年活动非常猖獗，该团伙将目标瞄准为芯片制造业和风投公司，向上述行业的 HR 投递钓鱼邮件，邮件内容如下：



▲ 图 2.6 APT-Q-12 投递的邮件内容

邮件附件包含一个 LNK 木马，执行流程与我们去年披露的报告一致，不同的是我们获取到了最终的远控木马和下发的键盘记录插件。

```
13  v2 = a2;
14  strncpy_s(Destination, 0x100ui64, Source, a2);
15  v3 = 0i64;
16  v4 = 0;
17  if ( (int)v2 > 0 && (unsigned int)v2 >= 0x40 )
18  {
19    si128 = _mm_load_si128((const __m128i *)&xmmword_7FFB90A1C1C0);
20    v6 = _mm_load_si128((const __m128i *)&xmmword_7FFB90A1C1D0);
21    do
22    {
23      v4 += 64;
24      *(__m128i *)&Destination[v3] = _mm_add_epi8(
25                                       _mm_xor_si128(si128, _mm_loadu_si128((const __m128i *)&Destination[v3])),
26                                       v6);
27      v11[v3 / 0x10] = (__int128)_mm_add_epi8(
28                                   _mm_xor_si128(si128, _mm_loadu_si128((const __m128i *)&v11[v3 / 0x10])),
29                                   v6);
30      v11[v3 / 0x10 + 1] = (__int128)_mm_add_epi8(
31                                       _mm_xor_si128(_mm_loadu_si128((const __m128i *)&v11[v3 / 0x10 + 1]), si128),
32                                       v6);
33      v11[v3 / 0x10 + 2] = (__int128)_mm_add_epi8(
34                                       _mm_xor_si128(si128, _mm_loadu_si128((const __m128i *)&v11[v3 / 0x10 + 2])),
35                                       v6);
36      v3 += 64i64;
37    }
38    while ( (__int64)v3 < (__int64)(v2 & 0xFFFFFFFFFFFFFFC0ui64) );
39  }
40  for ( i = v4; i < v2; ++i )
41    Destination[i] = (Destination[i] ^ 0x53) + 0x80;
42  if ( !(unsigned int)sub_7FFB90A06278((unsigned int)&v9, (unsigned int)aVpfqsqlejofBss_0, 33033, 64, 128) )
43  {
44    sub_7FFB90A070CC(v9, Destination, (unsigned int)v2);
45    sub_7FFB90A06708(v9);
46  }
47  return 0i64;
48 }
```

▲ 图 2.7 键盘记录模块加密逻辑

在年中时我们发现 APT-Q-12 开始投递 hlp 类型的样本，双击运行后会执行恶意 js 代码向远程服务器下载 bmp 图片并解密出第一阶段的木马，将本机信息和文件目录加密打包发送到远程服务器，并等待后续阶段木马的下发。

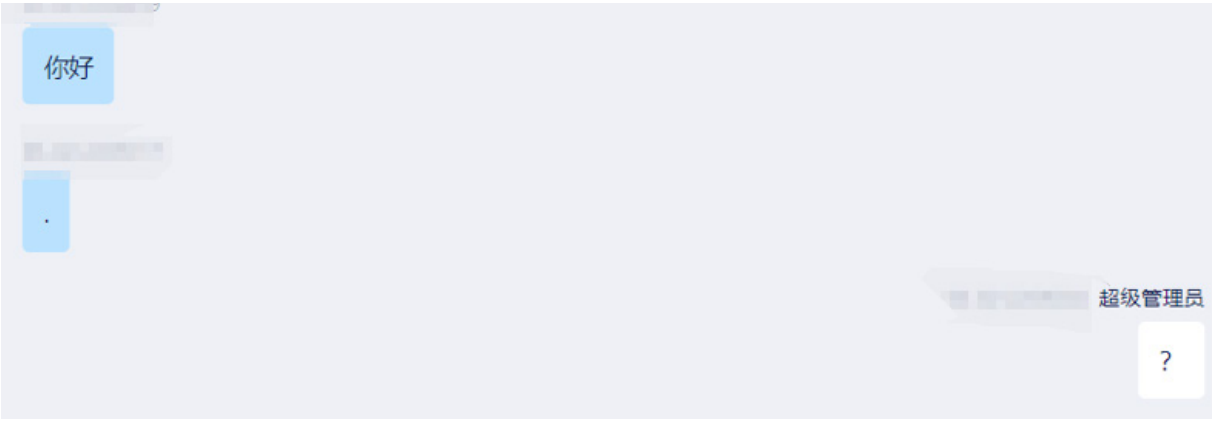
奇安信威胁情报中心会在 2022 年下半年择机披露该组织最新的攻击活动。

（三） APT-Q-27（金眼狗）

关键词：通讯软件 0day、博彩、金融

金眼狗早披露于 2019 年，起初我们认为该团伙投递模式较为单一，但随着数据的积累我们发现该团伙整体水平非常高，其设计的攻击链刻意对 EDR 监控流程进行了规避，这是目前主流 APT 团伙都不曾达到的技术水平。

在 2022 年我们捕获到的 APT-Q-27 最新 0day 攻击活动中，EXP 利用链设计得非常简练，且全过程没有恶意代码落地。金眼狗在窃取文件时设计了两种执行流程：第一种使用 EXP 执行命令将桌面和相关目录的文档上传到云盘；第二种则是借助 Chrome Nday 漏洞实现“白加黑”，在 Chrome 进程中加载 Cobalt Strike 远控木马来窃取文件。我们在其中一个云盘上发现了高达 300G 的博彩从业人员数据，并且推测攻击者用于接收文件数据的云盘和服务器共有 5-10 个，受害面之广超乎想象。0day 漏洞利用截图如下：



▲ 图 2.8 通讯软件 0day 漏洞利用截图

根据奇安信大数据遥测，APT-Q-27 在 2015 年 -2022 年使用了多个通讯软件 0day 漏洞进行攻击，我们捕获到的时间线如下：

1、2015 年使用知名聊天软件的 XX 秀漏洞对博彩行业进行攻击
2、2017 年使用某通讯软件对博彩行业进行攻击
3、2021-2022 年使用某通讯软件对博彩行业进行攻击

这些年来，我们仅捕获到该团伙的三个 0day 漏洞利用，可能只是其攻击活动的冰山一角。奇安信威胁情报中心会在未来择机披露该组织过去的攻击活动。

三、2022 上半年境内受害行业分析

从整体上对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 攻击事件及威胁情报的全线产品告警数据进行分析，得到 2022 上半年境内受害行业分布情况：攻击者主要针对我国政府机构、金融、互联网科技等行业进行攻击。详情如下图所示。

▲ 图 2.9 2022 上半年高级威胁事件涉及境内行业分布情况

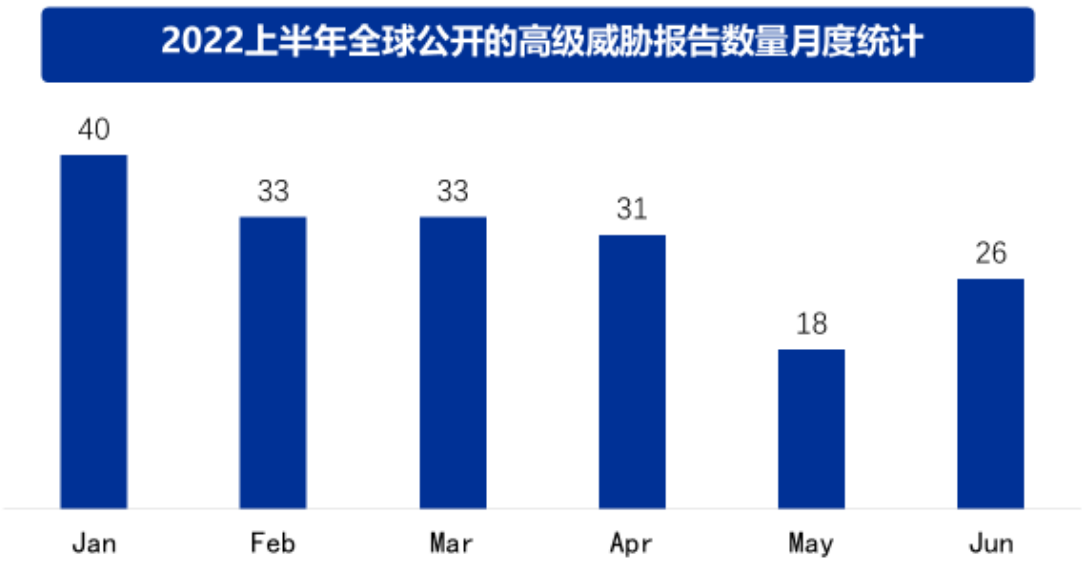
第三章 全球高级持续性威胁综述

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。2022 上半年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行了持续监测，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 2022 上半年监测到的高级持续性威胁相关公开报告总共 181 篇。各月监测数据如图 3.1 所示

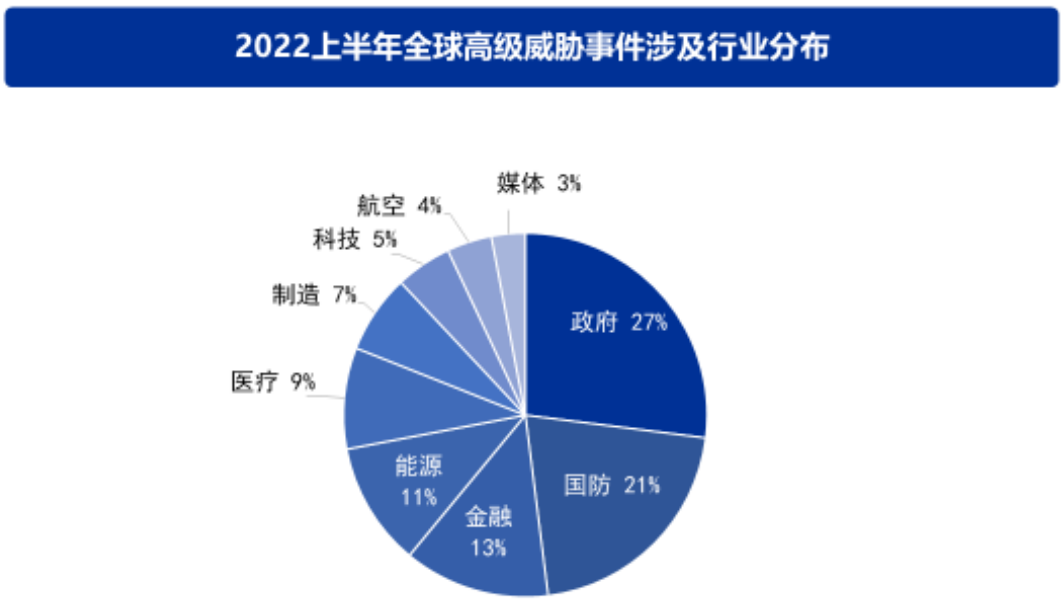


▲ 图 3.1 2022 上半年全球公开的高级威胁报告数量月度统计

二、受害目标的行业与地域

2022 年，在俄乌冲突的影响下，网络攻击发生巨大变化。通过开源情报数据显示：在全球 2022 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 27%，其次国防等军事相关事件占比为 21%、金融占比 13%、能源占比 11%。其中，政府机构仍是主要攻击目标，涉及国防、金融、能源相关的事件增长较多。

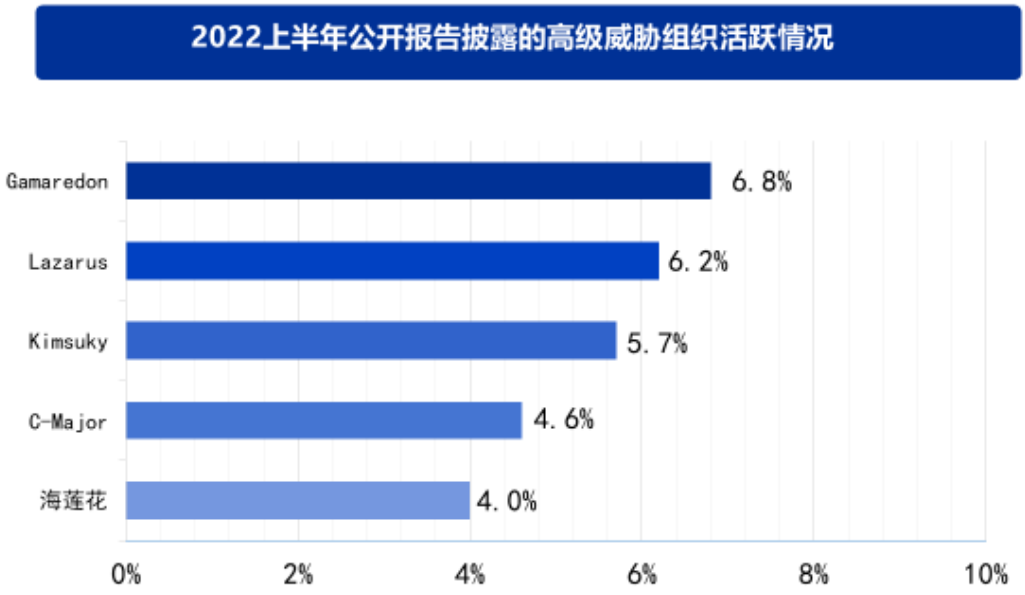
2022 上半年高级威胁事件涉及行业分布情况如下图所示。



▲ 图 3.2 2022 上半年全球高级威胁事件涉及行业分布

三、活跃高级威胁组织情况

本次报告对开源情报中所提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率最高的 5 个 APT 组织分别是：Gamaredon 6.8%，Lazarus 6.2%，Kimsuky 5.7%，C-Major 4.6%，海莲花 4%。



▲ 图 3.3 2022 上半年全球活跃高级威胁组织

四、2022 上半年高级威胁活动特点

（一）受经济利益驱使，金融行业的攻击加剧

在新冠疫情和俄乌冲突的双重冲击之下，经济形势受影响，2022 上半年以来发生了多起针对金融行业的攻击活动，主要通过窃取加密货币获取经济利益。

据公开报告披露，Lazarus 组织多次盯上加密货币公司，同时其目标也包括区块链、投资公司等金融机构。3 月，google 研究人员发现 Lazarus 组织利用 CVE-2022-0609 远程代码执行漏洞开展 Operation Dream Job 和 Operation AppleJeus 活动，其中 Operation AppleJeus 活动针对加密货币和金融科技行业的目标用户，受害者数量超过 85 名。

Bluenoroff group 被认为是 Lazarus 组织的分支。2022 年 1 月，卡巴斯基披露该组织针对与加密货币及智能合约、DeFi、区块链和金融科技行业有关的各种公司，受害者来自俄罗斯、波兰、斯洛文尼亚、乌克兰、捷克共和国、中国、印度、美国、香港、新加坡、阿联酋和越南。

与 Lazarus 一样，具有朝鲜背景的 Kimsuky，在 2022 年上半年也被披露使用包含加密货币信息的 Word 文档作为诱饵，针对加密货币公司发起攻击。

除了加密货币，国外安全厂商还披露了一个从拉丁美洲地区的金融企业中窃取资金的组织，并将其称为“Elephant Beetle”或 TG2003。该团伙通过在常规活动中进行隐藏的欺诈交易，最终窃取了数百万美元。

此外，我们在《Operation Dragon Breath（APT-Q-27）：针对博彩行业的降维打击》一文中披露了金眼狗团伙所在的 Miuuti Group 组织针对博彩、金融行业的定向攻击活动，其通过“黑吃黑”的方式将赌资转移到自己的钱包中，实现财富自由。

（二）国防军事目标成为众矢之的

在俄乌冲突的大背景下，不仅东欧地区针对国防军事目标的攻击活动激增，南亚、中东等地区以国防军事部门为目标的攻击活动也频频发生，国防军事相关目标成为热点攻击对象。

东欧方向的相关攻击组织包括 Turla、Gamaredon、APT28、LOREC53 等，攻击者除了瞄准乌克兰的军事目标，同时也针对其他西方国家目标，比如美国国防承包商、波罗的海国防学院等。

南亚地区老牌 APT 组织摩诃草、肚脑虫、Sidewinder、C-Major、蔓灵花均被多次披露向国防军事目标发起攻击。我们新发现一个疑似具有南亚背景的组织——金刚象（VajraEleph），专注于对军方目标展开间谍情报活动，已经观察到的受害人员主要为巴基斯坦国家的边防军（FC）和特种部队（SSG），尤其是俾路支省边防军（FC BLN），此外还包含少量的联邦调查局（FIA）和警察（Police）。

公开情报披露的攻击国防军事目标的组织还包括 MuddyWater、TunnelVision、双尾蝎以及 Lazarus 组织，相关攻击事件详见下表。

事件名称	披露时间	披露厂商
蔓灵花以“Datails of bill”为诱饵攻击军工企业	2022.1.10	360
Patchwork 借“住房登记”为由针对巴基斯坦国防官员	2022.1.10	安恒
Donot 组织持续攻击南亚政府和军事组织	2022.1.18	ESET
APT28 利用 CVE-2021-40444 针对高级官员及国防工业的间谍活动	2022.1.25	trelix
Gamaredon 针对乌克兰政府和军队在内的多个目标	2022.2.4	Microsoft
LOREC53 针对乌克兰国防、医疗等多个关键机构的大规模网络攻击	2022.2.17	绿盟
APT28 瞄准美国国防承包商发起攻击	2022.2.17	CISA
C-Major 和 SideCopy 模仿军事国防组织的域名进行钓鱼	2022.2.18	奇安信

事件名称	披露时间	披露厂商
伊朗 MuddyWater 组织针对全球政府和商业实体开展间谍活动	2022.2.26	CISA
C-Major 利用手机间谍软件 CapraRat 针对印度军方和政府人员	2022.3.7	恒安嘉新
金刚象组织 VajraEleph 针对巴基斯坦军方人员的网络间谍活动披露	2022.3.31	奇安信
APT-C-23 组织针对以色列官员的攻击活动披露	2022.4.6	Cybereason
Lazarus 利用 Log4j 漏洞针对能源和军事公司	2022.4.27	symantec
Turla 组织新的间谍活动瞄准奥地利经济商会、波罗的海国防学院	2022.5.23	sekoia
TunnelVision 组织网络钓鱼行动针对以色列和美国高级官员	2022.6.15	checkpoint

▲ 表 3.4 2022 上半年国防军事相关攻击活动

（三） 0day 漏洞仍受攻击者欢迎

从去年开始 0day 及 Nday 漏洞就已成为 APT 组织青睐的攻击武器。2022 年上半年，APT 组织使用最多的新漏洞是 Log4j 漏洞 (CVE-2021-44228) 及 Follina 漏洞 (CVE-2022-30190)。

Google 安全团队发现 APT28 组织在针对乌克兰的攻击活动中使用了 Follina 漏洞，该组织通过漏洞利用代码下载并执行一款新型的由 .Net 开发的信息窃取程序。同样，APT28 也利用 Log4j 漏洞针对负责国家安全政策的他国高级政府官员和西亚国防工业的重要人士实施网络间谍活动。

另外，Log4j 漏洞还被 APT35、海莲花、Lazarus、TunnelVision 等组织利用。

第四章 APT攻击中的漏洞利用

相较于 2021 年 0day 漏洞井喷似的爆发，2022 年上半年 0day 漏洞的攻击使用整体趋于缓和，比之 2021 年有大幅下降，但同比 2020 年却有所上升。当将 2021 年这个特殊年份去掉，可以发现 0day 在野漏洞的攻击依然维持一个逐年递增的趋势。以浏览器为核心的漏洞攻击向量依然是主流趋势，Chrome，Firefox，Safari 及对应平台下 Windows，MacOS，IOS 的沙箱逃逸漏洞占所有漏洞近 7 成，其中近 5 成漏洞源自之前漏洞补丁绕过的变种。

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-2022-21882	Microsoft	是	未知	未知
CVE-2022-22587	Apple	否	未知	未知
CVE-2022-22620	Apple	是	未知	未知
CVE-2022-0609	Google	否	Lazarus	Google's Threat Analysis Group
CVE-2022-26485	Mozilla	否	未知	360
CVE-2022-26486	Mozilla	否	未知	360
NA	向日葵	是	海莲花	未知
CVE-2021-22600	Google	否	未知	未知
CVE-2021-39793	Google	否	未知	未知
CVE-2022-1040	Sophos	是	Driftingcloud	未知
CVE-2022-1096	Google	否	未知	未知
CVE-2022-22674	Apple	否	未知	未知
CVE-2022-22675	Apple	否	未知	未知
CVE-2022-26871	Trend Micro	否	未知	Trend Micro Research

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-2022-24521	Microsoft	否	未知	National Security Agency and Crowdstrike
CVE-2022-1364	Google	否	未知	Google's Threat Analysis Group
CVE-2022-26925	Microsoft	否	未知	Bertelsmann Printing Group
CVE-2022-30190	Microsoft	是	未知	Shadow Chaser Group
CVE-2022-26134	Atlassian	是	Driftingcloud	Volexity

▲ 表 4.1 2022 上半年披露的高危漏洞

一、新兴的浏览器巨头：Lazarus

2021 年初，朝鲜 APT 团伙 Lazarus 发起了针对安全人员的攻击事件，攻击中使用了多个浏览器及本地提权漏洞，2022 年初该团伙又针对美国的新闻、IT、加密币及金融行业发起了多起攻击。攻击中使用了 Chrome 浏览器的 0day 漏洞 CVE-2022-0609，结合 Chrome 浏览器的利用特性，这一波攻击中至少还有一个用于提权的未知 0day 漏洞。据 Google 研究人员的分析，Exp 落地前还进行了 Macos/Firefox 相关的环境检测，有理由相信，该组织手中应该还有针对 Safari/Firefox 的 0day 漏洞。同时，该团伙似乎吸取了 2021 攻击时的经验教训，对投递的 0day 利用进行多重保护，包括但不限于：

1. 漏洞跳转的 iframe 只在特定的时间提供
2. 鱼叉邮件中的链接包含唯一 ID，以确保一个漏洞利用的链接只有一次触发机会
3. 漏洞利用的每一个阶段都通过 AES 加密
4. 一个阶段失败，直接放弃攻击

可以看到整个攻击中攻防双方的对抗升级，浏览器尤其是 Chrome 的 0day 检测已经成为除 Google 以外其他安全厂商很难介入的领域。

二、进击的向日葵

向日葵是一款国内流行的远程控制管理工具，其支持远程控制电脑手机，远程管理，内网穿透等功能。

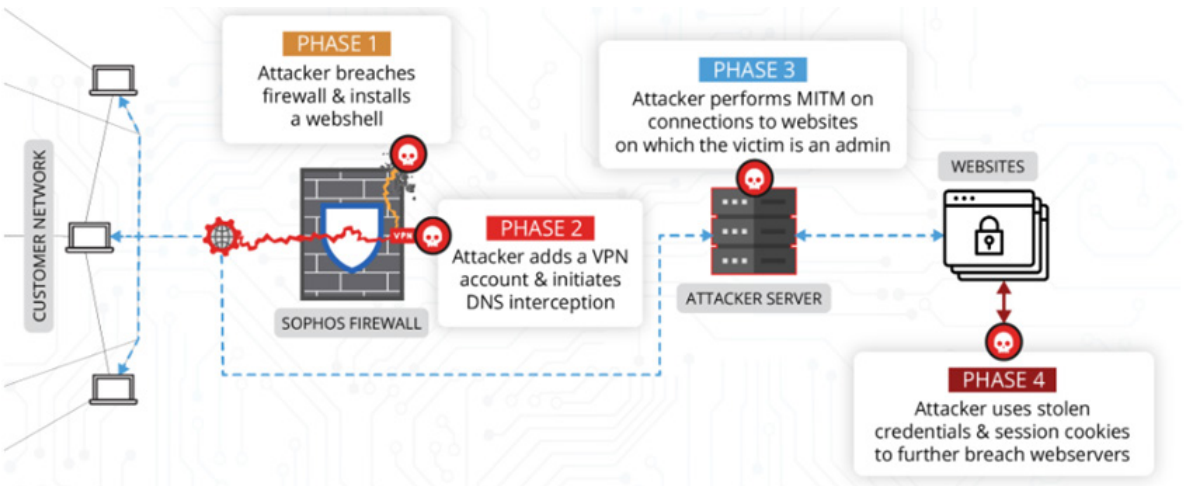
2022 年 2 月，该软件 Windows 版本被曝光存在远程命令执行漏洞，并出现在野利用。其本质上利用了向日葵对外开启的一个危险接口，获取到默认的 CID，从而配合后续的一处命令注入触发代码执行。由于很多企业的安全意识不足，将向日葵的接口主动曝露在公网，在漏洞公开后，大量企业受到了攻击，包括挖矿、勒索、僵尸网络等，其中海莲花曾多次利用该漏洞进行攻击。

三、IoT 路由沦为 APT 团伙攻击的前哨站

APT 团伙攻击时往往需要隐藏自身回连 C2 服务器，以防止后续安全人员的溯源，2022 年上半年，奇安信红雨滴团队捕获到多起海莲花攻击 IoT 路由设备的事件，该团伙通过近两年披露的一些路由器 nday 漏洞，对外网上没有修复的路由设备进行攻击，将这些路由设备作为攻击木马回连 C2 服务器的中转跳板，从而隐藏自己真实的 C2 服务器地址，此类手法已经成为当下海莲花团伙的标配攻击手段。

四、Driftingcloud：新兴的 0day 团伙

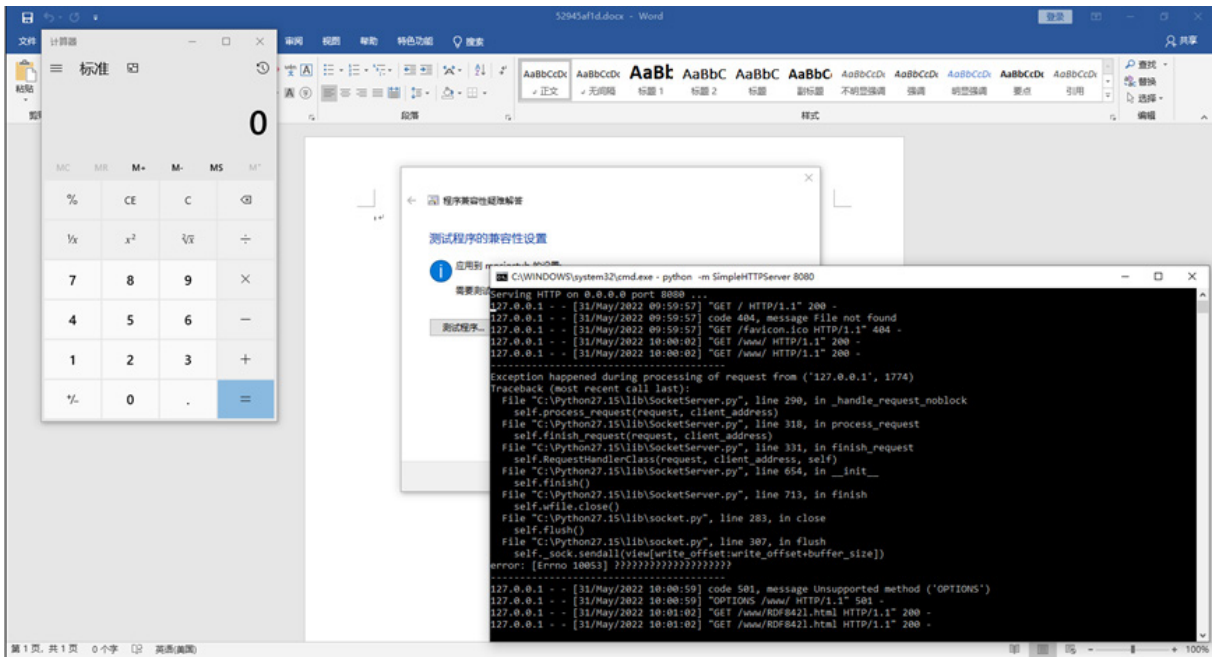
Volexity 于 2022 年 6 月分别披露了两起定向攻击事件，这两起攻击中都使用了 0day 漏洞，其中一个漏洞 CVE-2022-26134 为 Atlassian Confluence Sever 中未经身份验证的远程代码执行漏洞，另一个则是针对 Sophos 防火墙的远程代码执行漏洞 CVE-2022-1040，当通过漏洞攻陷 Sophos 防火墙后，攻击者利用对防火墙的访问权限修改了针对特定目标网站的 DNS 响应，以实现 MITM 攻击，这使攻击者能从对网站内容管理系统 (CMS) 的管理访问中拦截用户凭据和会话 cookie，并以此进行后续的攻击。



▲ 图 4.2 Driftingcloud 0day 漏洞攻击流程

五、传承：CVE-2022-30190

该漏洞最早由安全人员通过 VT 发现，并命名为 Follina。漏洞利用和去年的 CVE-2021-40444 有很多相似之处，通过 OLE 远程拉取一个恶意 html，该 html 中使用 msdt 协议绕过了 office 自带的保护视图。后续发现微软实际上在攻击不久前就已经尝试修复该问题，但是依旧存在 rtf 文件格式绕过的问题，最后通过 msdt 协议中的一处 powershell 注入导致最终的代码执行。



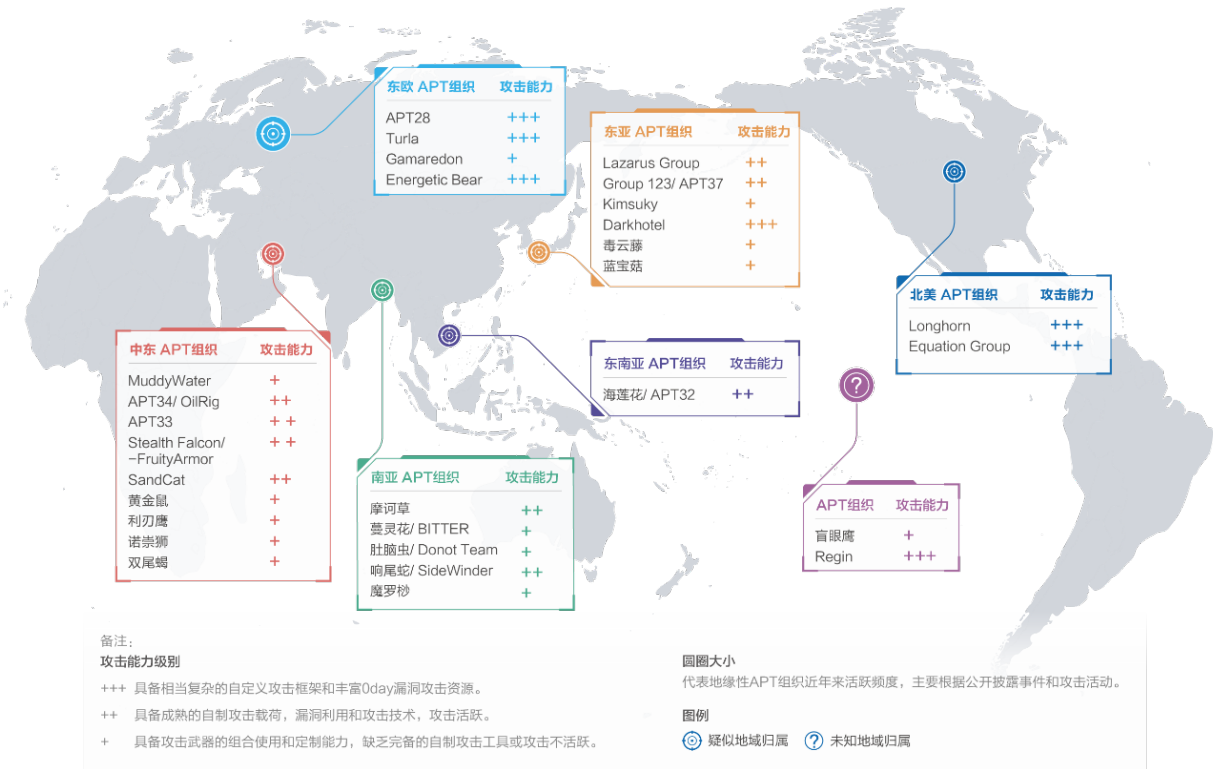
▲ 图 4.3 CVE-2022-30190 漏洞利用

该攻击样本被披露两天之后，便被 TA413 用于实际的鱼叉邮件攻击，之后 APT28 组织也在针对乌克兰的攻击中使用了该漏洞，但是由于该漏洞最终通过 msdt 的方式利用，导致漏洞披露之后，样本非常容易查杀。

第五章 地缘下的APT组织、活动和趋势

地缘政治的格局一定程度上影响着 APT 组织对攻击目标的选择，因而从地域空间的角度来分析 APT 活动有益于了解其攻击意图和趋势。

图 5.1 列举了 2022 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 5.1 2022 上半年全球 APT 组织分布情况

东亚地区的组织与行动
East Asia

2022 上半年以来，东亚地区活跃的 APT 组织主要是 Lazarus 和 Kimsuky。Lazarus 组织依然以经济利益为主要目的，Kimsuky 则主要出于政治动机进行攻击。

▲ 表 5.2 2022 上半年东亚地区活跃 APT 组织

Lazarus 组织在 2022 年上半年针对最多的是韩国，除攻击金融行业外，还使用虚假工作机会作为诱饵针对韩国化工和信息技术相关机构。2022 年 4 月，由于 Covid-19 的肆虐，不少公司使用 VMware 产品进行远程工作，Lazarus 组织趁此机会利用 Log4j 漏洞向未安装安全补丁的 VMware Horizon 产品发起攻击，针对一家在能源和军事领域的公司分发恶意软件。

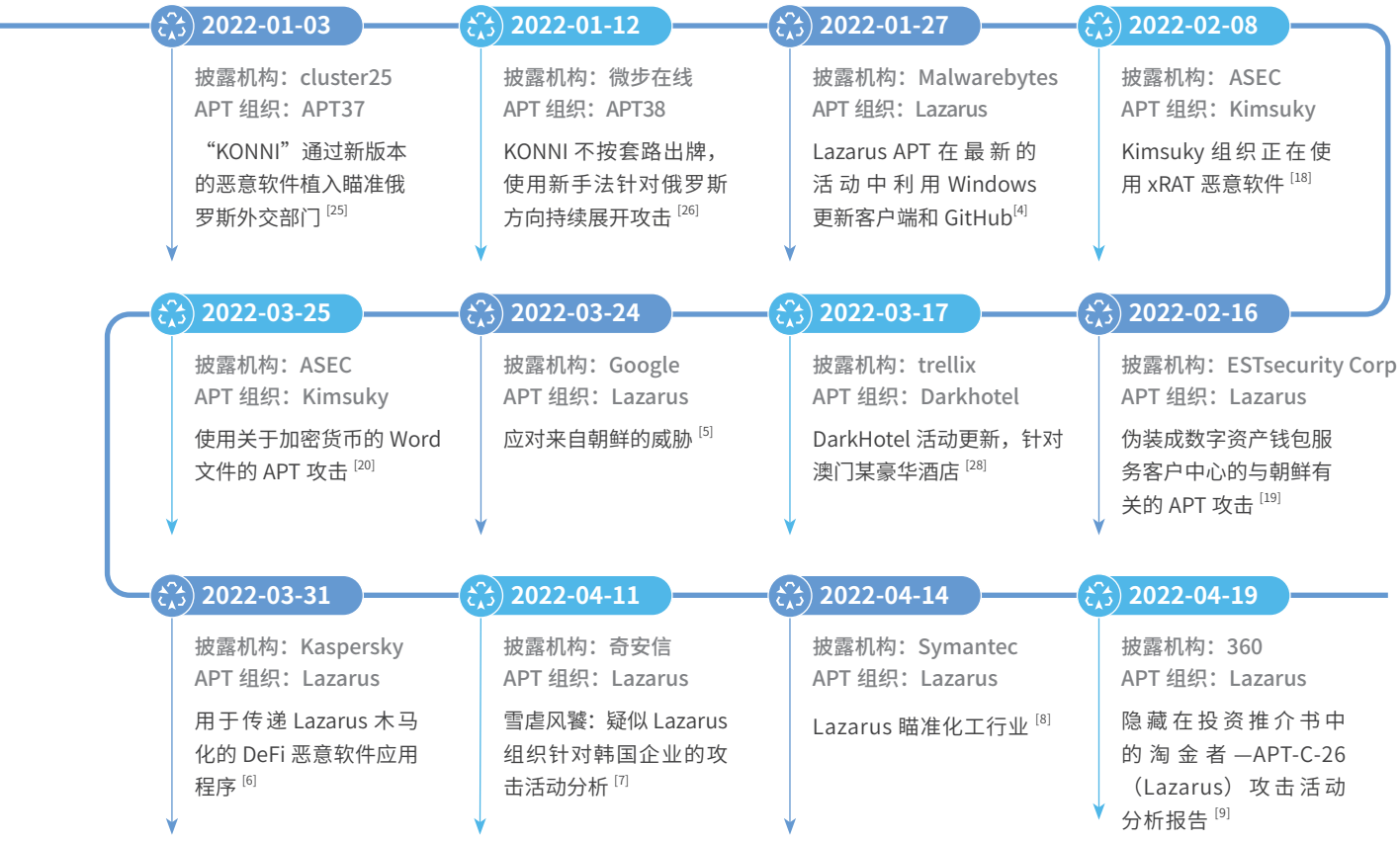
此外，奇安信威胁情报中心还捕获到 Lazarus 组织下属团体 Andariel 利用 Go 语言编写的下载器 [1]，用于向 C2 服务器回传收集到的主机信息然后下载 PE 文件并执行。大部分 Go 下载器被捕获时在 VT 上的检出数量较少，仅为个位数，这可能是攻击者选用 Go 开发恶意软件的一个原因。

Kimsuky 组织作为东亚地区另一活跃的 APT 组织，主要出于政治动机针对韩国和俄罗斯相关目标。但其攻击目标相对较广，会针对新闻、医疗以及与区块链加密货币等相关的金融机构进行钓鱼活动。在《钓

鱼之王——APT-Q-2（Kimsuky）近期以多个话题针对韩国的鱼叉攻击活动分析》[2] 一文中，我们分析了 Kimsuky 组织的鱼叉式钓鱼攻击流程。

DarkHotel 以针对执法、制药和汽车制造商以及其他行业而闻名。其攻击主要针对国防工业基地、军事、能源、政府、非政府组织、电子制造、制药和医疗等部门的公司高管、研究人员和开发人员。多年来，Darkhotel 组织一直保持着使用酒店网络跟踪和打击选定目标的能力，该组织通过使用恶意代码的鱼叉式网络钓鱼活动瞄准酒店和商务酒店访客，从而在入住豪华酒店的首席执行官和销售负责人等企业高管那里窃取敏感数据。今年 3 月，国外友商就曾披露过其利用鱼叉钓鱼攻击对澳门某豪华酒店进行攻击。

除此之外，奇安信威胁情报中心在 2019 年首次披露东亚 APT 团伙“虎木槿”，内部跟踪代号为 APT-Q-11。该团伙在 2019-2021 三年间利用了多个浏览器 0day 漏洞，使用多种攻击手法对目标进行渗透攻击。在《Operation(호랑이머리깃발발)ShadowTiger：盘踞在佛岩山上的过林之虎》[3] 一文中我们详细阐述了其使用的攻击手法，包括普通鱼叉邮件钓鱼、浏览器 0day 和鱼叉邮件攻击、内网水坑攻击、内网 0day 横向移动等攻击方式。



▲ 表 5.3 2022 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

东南亚地区最活跃的 APT 组织依然是海莲花。在 2022 年上半年，我们观察到海莲花组织频繁针对国内多个目标发起攻击，其攻击频率达到平均每月 17 次，目标囊括了政府、科研、能源、医疗、金融等多个领域。

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，自 2012 年 4 月起，该组织针对中国政府、科研院所、海事机构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

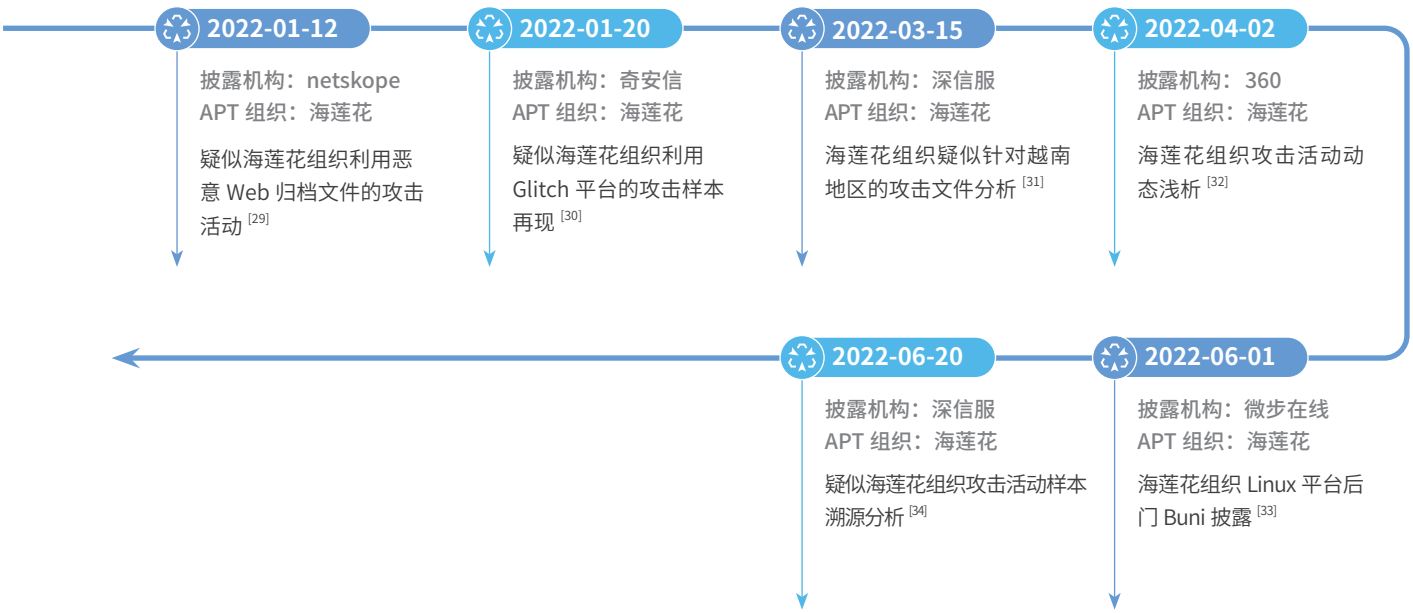
▲ 表 5.4 2022 上半年东南亚地区活跃 APT 组织

海莲花组织近年来入侵目标的方式已经由鱼叉式钓鱼邮件转变为以网络渗透手段为主，在攻击活动中经常使用各种开源的恶意载荷加载器进行免杀，这也使得该组织武器库编程语言除了 C++ 和 C#，还涉及相对小众的 Nim[32]。

2022 年 6 月，该组织 Linux 平台后门 “Buni” 被友商披露 [33]。该后门与去年披露的海莲花 Linux 后门 “双头龙” 以及早期 macOS 后门相似。这一款后门在单一进程实例、信息收集、C2 地址编码等技术特点上和 “双头龙” 几乎一致，但指令类型有所不同，并且流量加密方式较为简单。分析人员在捕获相关样本时发现后门仍处于活跃状态，后门中硬编码的 C2 利用了一些失陷 IoT 设备，并且控制的主机数量较多。

此外，一类使用了与海莲花组织类似手法的攻击样本也出现在我们的视野中 [29,30]。这类样本采用了海莲花组织曾使用过的宏文档类型和代码混淆方法，并且借助 Glitch 平台托管 C2 服务，不过样本也存在一些与海莲花组织历史攻击手法不同的地方。

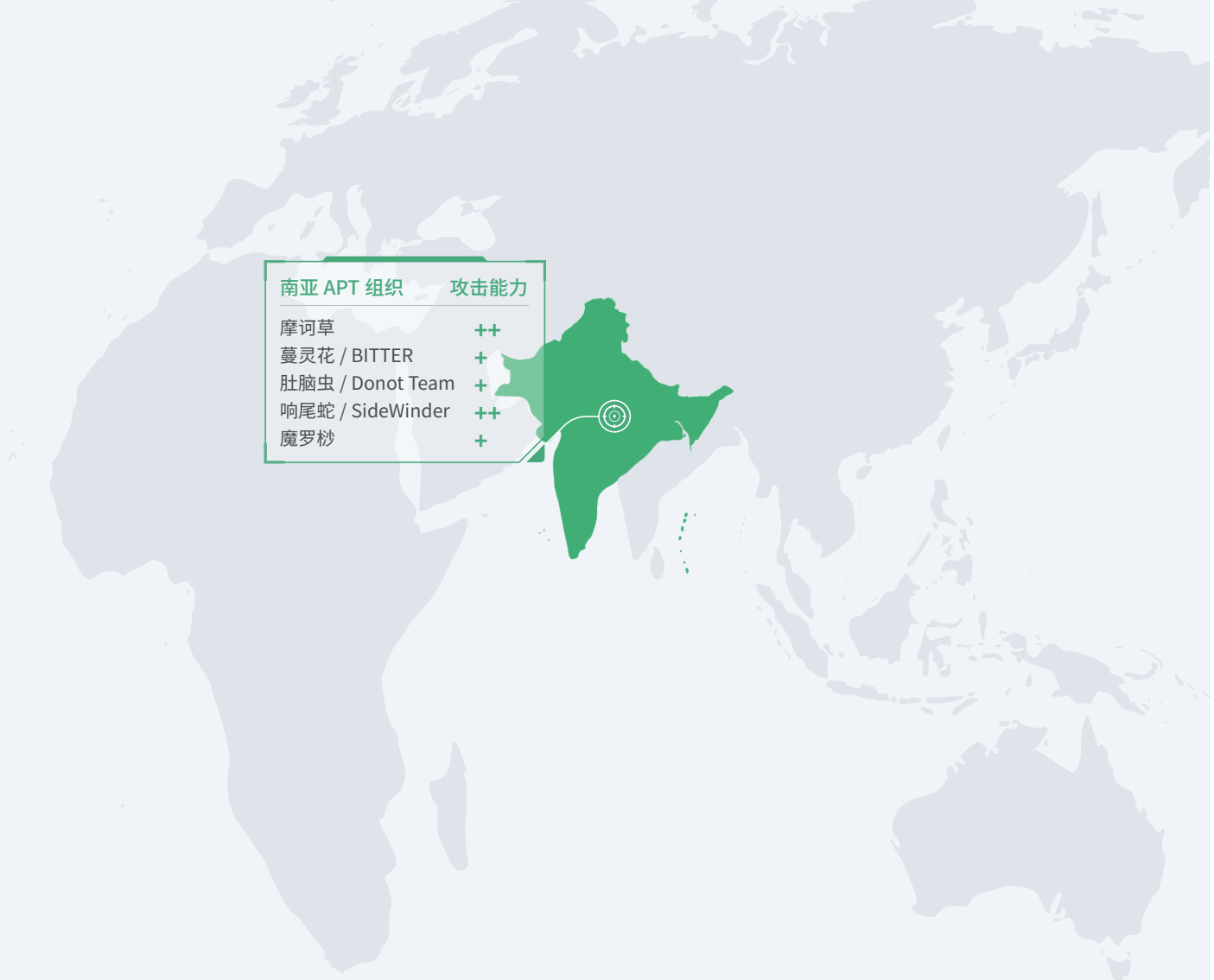
下表总结了 2022 上半年东南亚地区 APT 组织的主要攻击活动。



▲ 表 5.5 2022 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

南亚地区 2022 年上半年活跃的 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、Sidewinder 和摩诃草。此外，我们发现了该地区一个新的 APT 组织——金刚象（VajraEleph）。



2013

摩诃草

最早活动时间：2009
公开披露时间：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

2016

蔓灵花

最早活动时间：2013
公开披露时间：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

2016

Transparent Tribe

最早活动时间：2012
公开披露时间：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

2017

肚脑虫

最早活动时间：2016
公开披露时间：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

2018

Sidewinder

最早活动时间：2012
公开披露时间：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

2020

SideCopy

最早活动时间：2019
公开披露时间：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。因其攻击手法主要以复制 Sidewinder 及其他 APT 组织的 TTP 为主而得名

2022

VajraEleph

最早活动时间：2019
公开披露时间：2020

该 APT 组织最早的攻击活动可以追溯到 2021 年 6 月。疑似来自南亚，主要针对巴基斯坦军方展开了有组织、有计划、针对性的军事间谍情报活动。其攻击目标主要为巴基斯坦国家的边防军（FC）和特种部队（SSG），尤其是俾路支省边防军（FC BLN），此外还包含少量的联邦调查局（FIA）和警察（Police）。奇安信内部跟踪编号为 APT-Q-43

▲ 表 5.6 2022 上半年南亚地区活跃 APT 组织

从 2022 年上半年公开披露的攻击活动来看，南亚地区各 APT 组织活跃度较往年并未出现太大的波动。2022 年在 1 月下旬，奇安信威胁情报中心捕获到来自 SideCopy 组织面向 Linux 64 位系统所使用的窃密样本 [40]，该样本由 Go 语言编写，功能单一，仅实现对受害者主机目录的扫描以及数据窃取的功能。此外，通过关联分析发现回连相同 C2 地址的样本所涉及的目标系统涵盖了 Windows 和 Linux，可以推测此类样本或为该组织某攻击链条中的一个组件，同时表明该组织在策划针对 Windows 和 Linux 多平台的攻击。

根据公开报告显示，2022 上半年南亚地区活跃度最高的是透明部落组织，该组织主要针对印度政府、军队相关目标，上半年仍以其常用的 Crimson RAT 作为载荷。2022 年 2 月，奇安信威胁情报中心发现 Transparent Tribe 组织与 SideCopy 利用相同的基础设施托管恶意软件 [42]，并使用同样伪装为印度政府国家信息中心的 Kavach 身份验证程序进行攻击，这表明两者可能存在较大关联，两个月后我们捕获到了该组织用于针对印度目标的 USBWorm 组件。

蔓灵花组织在 2022 年上半年则积极针对孟加拉国的政府、军事相关目标。我们发现蔓灵花团伙在四月份的攻击活动中投递带有 DDE auto 的文档作为附件 [53]，且观察到蔓灵花正在修改 MSI 木马。

金刚象（VajraEleph）是我们新发现的一个对 Android 平台进行攻击的 APT 组织 [46]，该组织疑似具有南亚背景，主要针对巴基斯坦军方展开有组织、有计划、针对性的军事间谍情报活动。

金刚象组织通常使用公开的社交平台找到关注的目标，然后利用色情话术等方式诱导目标用户安装指定的诱饵聊天攻击应用进行钓鱼攻击。我们将其使用的 Android 平台 RAT 命名为 VajraSpy。通过对该组织的攻击手法进行分析我们发现，该组织带有明显的军事情报窃取意图，擅长使用社交诱导投递和短信投递进行攻击，攻击链中存在与肚脑虫 APT 组织相似的特征。

Sidewinder APT 在 2022 年上半年先后发起了假冒“巴基斯坦政府内阁秘书处，内阁部门国家电信和信息技术安全委员会”对巴基斯坦进行钓鱼攻击 [38]、利用巴基斯坦国庆作为诱饵进行钓鱼活动 [43] 以及模仿巴基斯坦政府合法域 [52] 等攻击活动，并且在此期间，该组织不断对使用的攻击方式进行更新迭代。

下表总结了上述南亚 APT 组织在 2022 年上半年的主要攻击活动。

2022-01-10

披露机构：360
APT 组织：蔓灵花

隐藏在账单下的恶意——APT-C-08（蔓灵花）最新攻击活动简报 [35]

2022-01-10

披露机构：Malwarebytes
APT 组织：摩诃草

Patchwork 利用钓鱼攻击投放 BADNEWS 木马新变种 [36]

2022-01-10

披露机构：安恒
APT 组织：摩诃草

Patchwork APT 组织针对某医疗卫生机构相关人员与巴基斯坦国防官员攻击活动分析 [37]

2022-01-18

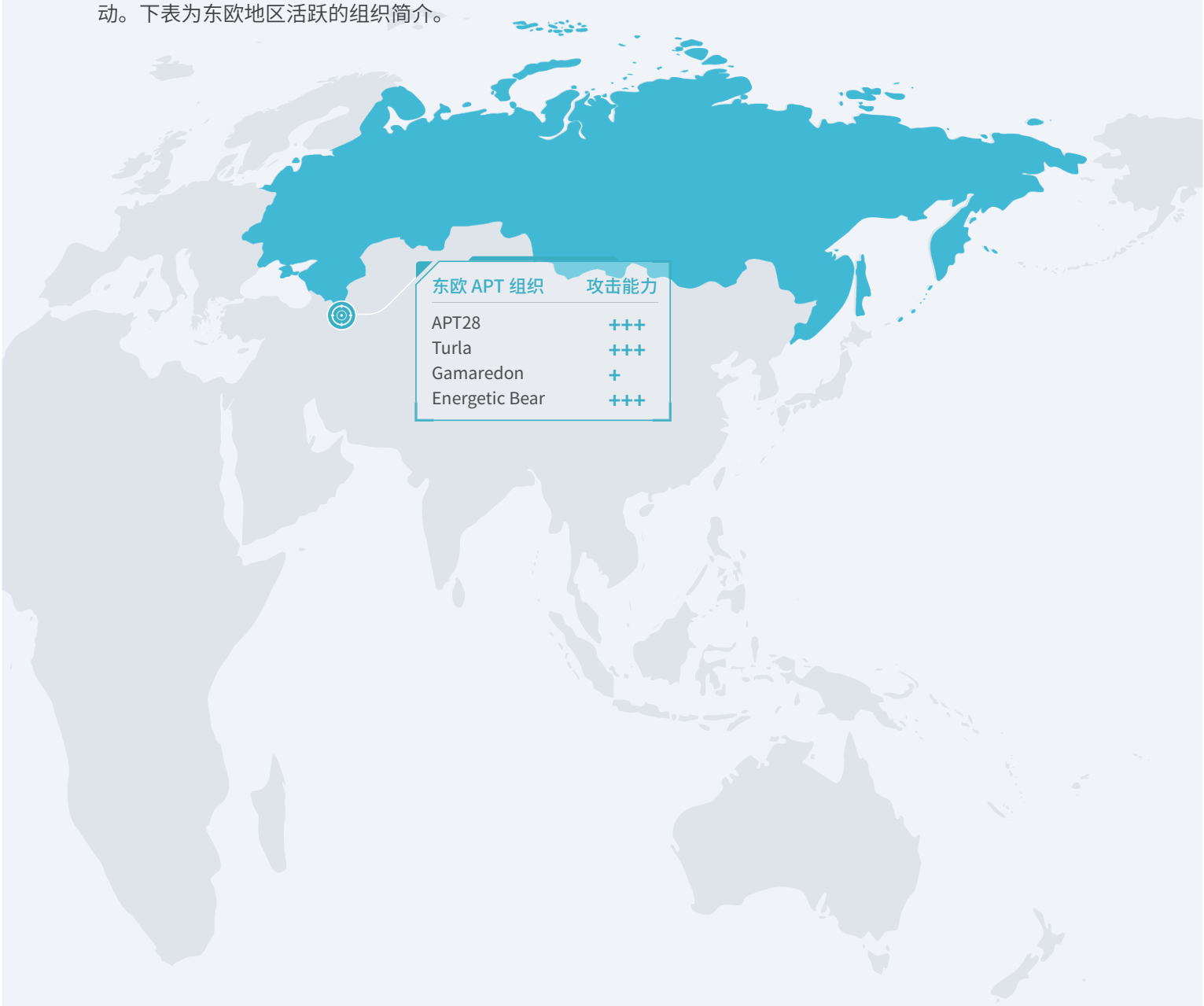
披露机构：深信服
APT 组织：响尾蛇

SideWinder 假冒“巴基斯坦政府内阁“进行钓鱼活动 [38]

▲ 表 5.7 2022 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

由于俄乌冲突，东欧地区 2022 年上半年针对乌克兰的 APT 活动变得十分频繁，其中不乏老牌 APT 组织 APT28、APT29、Gamaredon、Sandworm 的身影。UAC-0056 和 UNC1151 组织也在俄乌冲突中表现得极为活跃。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。下表为东欧地区活跃的组织简介。



东欧 APT 组织	攻击能力
APT28	+++
Turla	+++
Gamaredon	+
Energetic Bear	+++

2013

APT29

最早活动时间：2008
公开披露时间：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

2014

APT28

最早活动时间：2004
公开披露时间：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

2014

Turla

最早活动时间：2007
公开披露时间：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

2015

Gamaredon

最早活动时间：2013
公开披露时间：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

2015

Sandworm

最早活动时间：2009
公开披露时间：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

2020

UNC1151

最早活动时间：2017
公开披露时间：2020

该 APT 组织据称与“Ghostwriter”攻击活动相关，对包括立陶宛、拉脱维亚和波兰等北约相关国家实施网络钓鱼攻击

2022

UAC-0056

最早活动时间：2020
公开披露时间：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

▲ 表 5.8 2022 上半年东欧地区活跃 APT 组织

鱼叉式钓鱼邮件仍是东欧地区 APT 组织常用的一种攻击手段，在俄乌冲突中 Gamaredon、UAC-0056 频繁对乌克兰相关组织机构发起网络钓鱼攻击，APT28、APT29、Turla、UNC1151 的钓鱼攻击目标还涉及到东欧其他国家和欧盟北约的成员国。APT28 会利用刚曝光的漏洞构造恶意文档发起攻击 [54, 84]，APT29 则借助合法的网络服务创建 C&C 信道 [76, 79]，以绕过流量检测并增加攻击活动的隐蔽性。

Sandworm 组织被认为是 Cyclops Blink 恶意软件的幕后黑手 [60]，该恶意软件可以利用 SOHO 网络设备创建僵尸网络。2022 年 4 月，乌克兰计算机应急响应小组 (CERT-UA) 和 ESET 联合披露了该组织计划针对乌克兰电网的攻击 [72]，在此次攻击中出现的针对电力工控系统的恶意软件 Industroyer2 是 Sandworm 组织在 2016 攻击乌克兰电力系统时使用的 Industroyer 的变种，同时该组织还计划使用 CaddyWiper 和 Linux/Solaris 平台的数据擦除软件让受感染的系统难以恢复。

奇安信威胁情报中心整理了 2022 上半年东欧 APT 组织热点攻击活动，如下表所示。

▲ 表 5.9 2022 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

由于动荡不安的政治局势，中东地区的网络攻击活动十分频繁，涉及的 APT 组织众多，攻击目标也极具复杂性，不仅针对特定行业，也会对人权活动家、立法者、官员甚至总统等个人目标进行攻击。

中东 APT 组织	攻击能力
MuddyWater	+
APT34/ OilRig	++
APT33	++
FruityArmor	++
SandCat	++
黄金鼠	+
利刃鹰	+
诺崇狮	+
双尾蝎	+

2013

月光鼠

最早活动时间：2012
公开披露时间：2013

月光鼠组织经常以时事热点制作鱼叉邮件，通过携带的恶意文档传播恶意软件，此外该组织还会将恶意软件包装在安卓应用中进行传播

2015

双尾蝎

最早活动时间：2011
公开披露时间：2015

双尾蝎组织攻击范围主要为中东地区，其针对 Windows 和 Android 双平台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，向政府、金融、媒体、能源、军事等特定目标人群进行攻击

2016

PROMETHIUM

最早活动时间：2012
公开披露时间：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

2016

黄金鼠

最早活动时间：2014
公开披露时间：2016

黄金鼠是一个最早由奇安信披露的 APT 组织。该组织在叙利亚地区活跃，其具备 Windows 和 Android 平台的恶意攻击能力

2016

APT34

最早活动时间：2014
公开披露时间：2016

其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 两个不同的名称分别进行追踪分析

2017

APT33

最早活动时间：2013
公开披露时间：2017

APT33 是 FireEye 披露的 APT 组织，攻击目标包括美国、沙特阿拉伯和韩国，主要针对航空和能源领域实施攻击活动

2017

MuddyWater

最早活动时间：2017
公开披露时间：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

2018

军刀狮

最早活动时间：2015
公开披露时间：2018

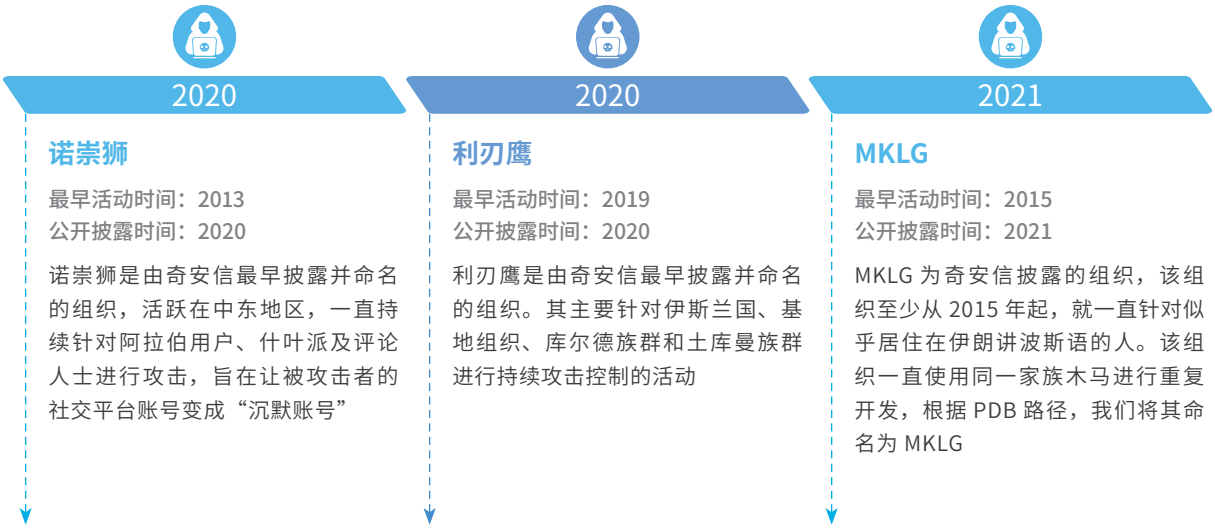
ZooPark（军刀狮）组织最早是由 Kaspersky 于 2018 披露并命名的组织，该组织自 2015 开始活跃，主要攻击目标为伊朗、约旦、埃及、黎巴嫩等中东地区国家，其攻击武器共包含四个迭代版本的 Android 端 RAT，且版本间代码复杂度提升极大

2019

Lyceum

最早活动时间：2018
公开披露时间：2019

Dragos 披露的一个新的针对 ICS 的攻击团伙，其主要针对关键基础设施，包括石油和天然气以及可能的电信。其最早可能在 2018 年 4 月开始活动

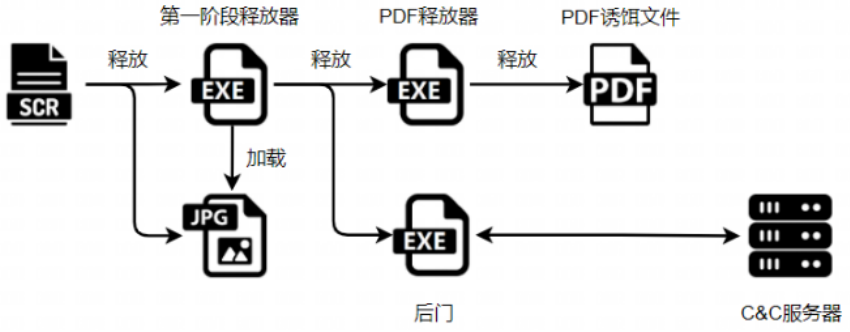


▲ 表 5.10 2022 上半年中东地区活跃 APT 组织

通过跟踪梳理，我们发现中东区域活跃的 APT 组织主要是 MuddyWater、Lyceum 以及 Molerats。Molerats 组织活动主要集中在年初 1、2 月份，针对政府、外交、航空实体 [86] 以及人权活动家 [87] 开展网络间谍活动。

2022 年 1 月 12 日，美国网络司令部将 MuddyWater 组织归属于伊朗情报部 (MOIS)。随后，奇安信威胁情报中心对 MuddyWater 的攻击战术进行分析 [88]，并还原了该组织在全球范围内使用的 PowGoop 变种木马攻击链。MuddyWater 上半年主要针对土耳其相关目标进行攻击，此外还开展了针对全球政府和商业实体的间谍活动。

Lyceum 最早由 Secureworks 于 2019 年公开披露并命名，是一个很少被曝光的威胁组织，其目标是中东地区的石油和天然气公司。上半年，Lyceum 被观察到多次针对能源目标，我们在《瞄准能源企业：Lyceum 组织以军事热点事件为诱饵针对中东地区的定向攻击》[89] 一文中详细分析了该组织相关攻击，通过诱骗受害者点击弹框下载 docm 文件或者伪装的 SCR 屏幕保护程序。



▲ 图 5.11 Lyceum 组织攻击流程

其他 APT 组织如 APT35、双尾蝎等依旧在中东地区比较活跃，其攻击方式和武器库层出不穷，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、水坑攻击、社工等方式建立攻击立足点。结合公开情报，我们整理了中东地区 2022 年上半年主要攻击活动，如下表所示。

2022-01-11
披露机构：checkpoint
APT 组织：APT35
APT35 利用 Log4j 漏洞分发新的模块化 PowerShell 工具包 [95]

2022-01-12
披露机构：SentinelOne
APT 组织：MuddyWater
伊朗国家支持的威胁行为者最近的活动 [90]

2022-01-17
披露机构：奇安信
APT 组织：MuddyWater
继美国网络司令部披露后：MuddyWater 近期攻击活动总结 [88]

2022-01-20
披露机构：zscaler
APT 组织：Molerats
Molerats APT 针对中东用户的新间谍攻击 [99]

2022-01-26
披露机构：cymru
APT 组织：Molerats
与 Molerats APT 有关的管理 IP 地址的分析 [100]

2022-01-31
披露机构：Cisco
APT 组织：MuddyWater
伊朗 APT MuddyWater 通过恶意 PDF、可执行文件针对土耳其用户 [91]

2022-02-01
披露机构：cybereason
APT 组织：APT35
PowerLess 木马伊朗 APT 为间谍活动添加了新的 PowerShell 后门 [96]

2022-02-02
披露机构：Cisco
APT 组织：双尾蝎
AridViper APT 以新一波以政治为主题的网络钓鱼攻击、恶意软件针对巴勒斯坦 [102]

2022-02-08
披露机构：proofpoint
APT 组织：Molerats
与巴勒斯坦结盟的间谍活动的故事 [86]

2022-02-16
披露机构：微步在线
APT 组织：Molerats
中东持续活跃的威胁：月光鼠组织借助云服务展开间谍攻击 [101]

2022-02-24
披露机构：Mandiant
APT 组织：MuddyWater
在最新的伊朗网络间谍活动中发现 Telegram 恶意软件 [92]

2022-02-24
披露机构：CISA
APT 组织：MuddyWater
伊朗政府资助的威胁行为者针对全球政府和商业网络的网络行动 [93]

2022-03-10
披露机构：Cisco
APT 组织：MuddyWater
与 MuddyWater 有关的子组织攻击土耳其和其他亚洲国家 [94]

2022-03-21
披露机构：DFIR report
APT 组织：APT35
APT35 使用 ProxyShell 自动化初始访问 [97]

2022-03-21
披露机构：奇安信
APT 组织：PROMETHIUM
赛博空间的魔眼（续）：PROMETHIUM 伪装为 WinRar.exe 的攻击活动分析 [106]

2022-04-06
披露机构：cybereason
APT 组织：双尾蝎
针对以色列官员的 APT-C-23 活动 [103]

2022-05-10
披露机构：Malwarebytes
APT 组织：APT34
使用新的 Saitama 后门针对约旦政府 [98]

2022-05-10
披露机构：360
APT 组织：Lyceum
Lyceum 组织针对高科技芯片行业攻击活动的简要分析 [107]

2022-06-09
披露机构：zscaler
APT 组织：Lyceum
Lyceum .NET DNS 后门 [108]

2022-06-15
披露机构：安恒
APT 组织：双尾蝎
游走于中东的魅影 -APT 组织 AridViper 近期攻击活动分析 [104]

2022-06-22
披露机构：奇安信
APT 组织：Lyceum
瞄准能源企业：Lyceum 组织以军事热点事件为诱饵针对中东地区的定向攻击 [89]

2022-07-06
披露机构：360
APT 组织：双尾蝎
APT-C-23（双尾蝎）组织伪装 Threema 通讯软件攻击分析 [105]

▲ 表 5.12 2022 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

2022 年全球安全厂商披露出多个具有高级攻击技术，并在本年度持续活跃的 APT 组织、以经济为目的的网络犯罪组织（Hive0117）和网络军火商（KNOTWEED）。

2021

Kasablanka

最早活动时间：2021
公开披露时间：2021

通过 PDF 文诱饵文档和网站对金融、政府组织进行网络钓鱼，主要进行信息收集和间谍活动，其具备 Windows 和 Android 平台的恶意攻击能力 [112]

2022

TA4563

最早活动时间：2021
公开披露时间：2022

该 APT 组织最早的攻击活动可以追溯到 2021 年 12 月。主要针对欧洲金融和投资实体目标等进行攻击活动 [109]

2022

POLONIUM

最早活动时间：2022
公开披露时间：2022

该 APT 组织最早的攻击活动可以追溯到 2022 年。疑似来自黎巴嫩，主要针对以色列的关键制造业、信息技术、交通系统、国防工业基地、政府机构和服务目标等进行攻击活动 [110]

2022

MURENSHARK

最早活动时间：2021
公开披露时间：2022

该 APT 组织最早的攻击活动可以追溯到 2021 年 4 月。来源未知，主要针对土耳其，北塞浦路斯的高校、研究所和军队目标等进行攻击活动。其使用 NiceRender 生成的恶意文档投递 LetMeOut 木马 [111]

2022

Hive0117

最早活动时间：2022
公开披露时间：2022

出于经济动机的网络犯罪组织，主要针对立陶宛、爱沙尼亚和俄罗斯电信、电子和工业部门的用户 [113]

2022

KNOTWEED

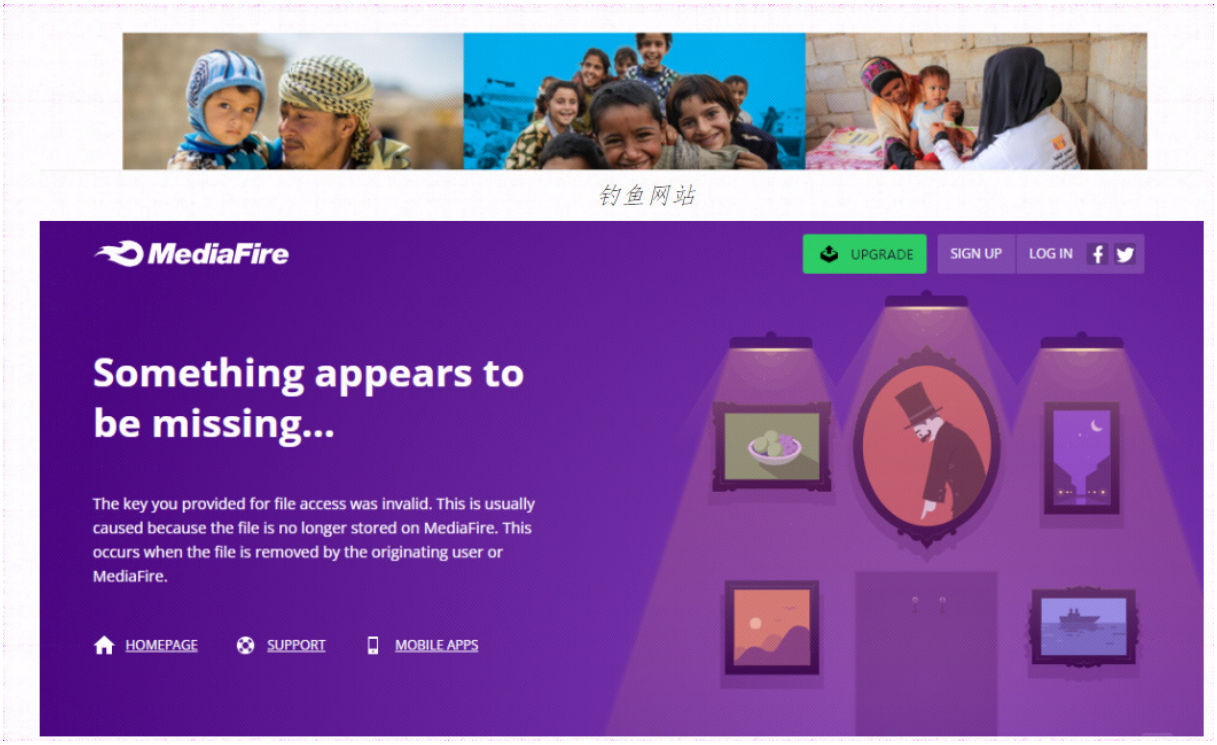
最早活动时间：2021
公开披露时间：2022

来自奥地利的网络军火商，善于利用 0day 进行网络攻击活动 [114]

▲ 表 5.13 2022 上半年其他地区活跃 APT 组织

TA4563 组织主要攻击目标是欧洲金融和投资实体，尤其是那些支持外汇、加密货币和去中心化金融 (DeFi) 的业务的实体，攻击特点是利用 lnk 加载器、javascript 和 powershell 脚本释放 EvilNum 后门组件，用来窃取数据或加载额外的负载 [109]。

Kasablanka 通过网站钓鱼传播 Android 平台间谍软件 SpyNoteRAT，钓鱼网站伪装成也门联合国儿童基金会网站，声称提供移动端应用程序以进行载荷投递，攻击样本存放在钓鱼网站中。该钓鱼网站从 2021 年 7 月开始投入使用，至 2022 年仍然活跃。



▲ 图 5.14 Kasablanka 组织钓鱼页面

该组织恶意 Android 应用图标的伪装对象除了上面提到的也门联合国儿童基金会，还包括联合国、联合国儿童基金会供应司、通话软件等。根据对软件图标伪装对象的分析，受害者应该是也门的政治团体或公益组织。

▲ 图 5.15 Kasablanka 恶意应用的图标

Hive0117 善于利用网络钓鱼邮件下发 DarkWatchman 组件 (一种 JavaScript RAT)，通过 C2 机制实现无文件持久化和其他功能。

KNOTWEED 是来自奥地利的网络军火商，主要针对欧洲、中美洲等地区的目标进行攻击活动。它曾在 2021 年通过 Adobe 0day CVE-2021-28550 及 Windows 提权 0day CVE-2021-31199 和 CVE-2021-31201 进行攻击，在 2022 年利用 CVE-2022-22047 提权 0day 的攻击中投递了恶意软件 Subzero。

▲ 表 5.16 2022 上半年其它地区 APT 组织热点攻击活动

附表1 俄乌冲突下的APT攻击概要

（注：这里只列举东欧地区 APT 攻击活动中与俄乌两国直接相关的部分）

披露时间	组织名	活动描述	披露机构
2022-01-31	Gamaredon	Gamaredon 持续对乌克兰进行网络间谍攻击 [56]	Symantec
2022-02-04	Gamaredon	Gamaredon 针对乌克兰组织的攻击活动 [57]	Microsoft
2022-02-16	UAC-0056	APT 组织 LOREC53（洛瑞熊）近期针对乌克兰的大规模网络攻击活动 [58]	绿盟
2022-02-25	UAC-0056	UAC-0056 针对乌克兰的组织发起鱼叉式网络钓鱼攻击 [61]	PaloAlto Networks
2022-02-26	Gamaredon, UAC-0056	俄乌战争中的网络攻击部队行为分析 [62]	知道创宇
2022-02-28	Gamaredon	APT 组织 Gamaredon 近期在乌克兰卢甘斯克地区的网络钓鱼活动 [63]	绿盟
2022-03-01	UNC1151	Asylum Ambuscade: 针对欧洲官员的网络钓鱼活动 [65]	Proofpoint
2022-03-14	UNC1151	疑似 APT 组织 UNC1151 针对乌克兰等国的攻击活动分析 [66]	奇安信
2022-03-18	Gamaredon	APT-C-53（Gamaredon）在近期攻击中的新变化 [67]	360
2022-03-22	InvisiMole	InvisiMole 组织针对乌克兰国家机构发起鱼叉式钓鱼攻击 [68]	securityaffairs.co
2022-04-01	UAC-0056	UAC-0056 针对乌克兰实体的新活动分析 [69]	Malwarebytes
2022-04-04	Gamaredon	乌克兰发现与 Gamaredon 组织有关的网络钓鱼攻击活动 [71]	CERT-UA
2022-04-12	Sandworm	Sandworm 组织试图攻击乌克兰能源供应商 [72]	ESET
2022-04-20	Gamaredon	Gamaredon 继续针对乌克兰进行网络间谍活动 [74]	Symantec
2022-04-25	UAC-0056	UAC-0056 使用的 Elephant 攻击框架分析 [75]	Bitdefender
2022-05-06	APT28	APT28 使用 CredoMap_v2 恶意软件攻击乌克兰 [77]	CERT-UA
2022-05-10	Gamaredon	Gamaredon 钓鱼样本分析 [78]	安恒

披露时间	组织名	活动描述	披露机构
2022-05-20	Sandworm	Sandworm 使用新版 ArguePatch 攻击乌克兰目标 [80]	ESET
2022-05-26	Gamaredon	Gamaredon APT 近期攻击活动分析 [82]	安恒
2022-05-26	Gamaredon	APT-C-53（Gamaredon）新一轮 DDoS 攻击任务分析 [83]	360
2022-06-13	APT28	APT28 利用对核战争的恐惧在乌克兰传播 Follina 漏洞 (CVE-2022-30190) 利用文档 [84]	Malwarebytes
2022-06-27	Gamaredon	GlowSand: Gamaredon 攻击样本分析 [85]	InQuest

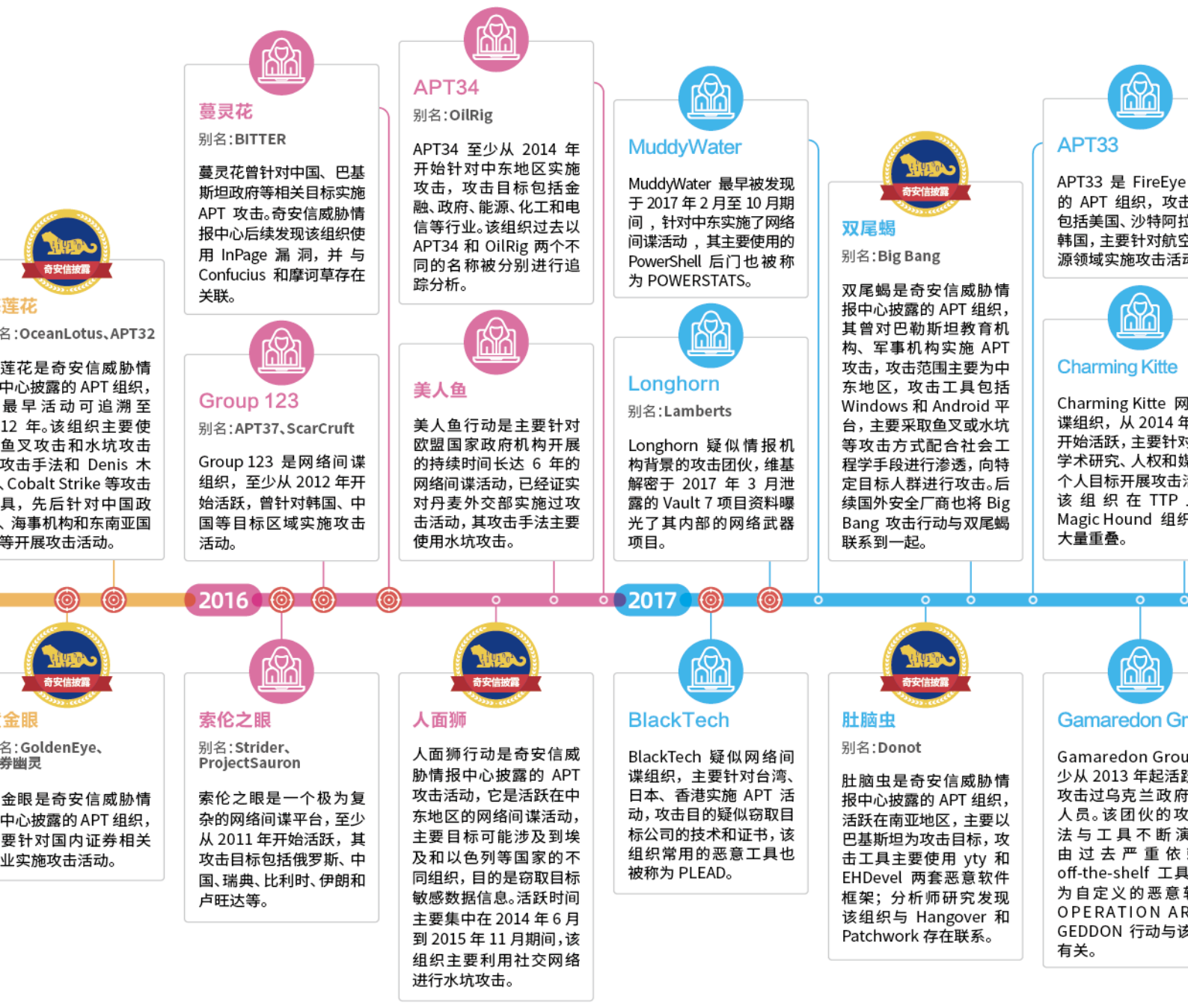
附表2 俄乌冲突下的黑客组织概要

（注：这里只列举东欧地区 APT 攻击活动中与俄乌两国直接相关的部分）

黑客组织	支持阵营	攻击方式	社交媒体	位置	起始日期
AgainstTheWest (ATW)	乌克兰	Data Breach/ 恶意软件	推特、电报	法国	2021 年
Belarusian Cyber Partisans	乌克兰 / 自由白俄罗斯	恶意软件	推特、电报	白俄罗斯	2020 年
Anonymous	乌克兰	DDoS	推特	全球	2022 年 2 月
GhostSec	乌克兰	Hack	推特、电报	不详	2022 年 2 月
乌克兰人自发的数字军团	乌克兰	DDoS	电报	乌克兰	2022 年 2 月
KelvinSecurity Hacking Team	乌克兰	Hack	推特	不详	2022 年 2 月
BlackHawk	乌克兰	DDoS	推特	格鲁吉亚	2022 年 2 月
Anonymous Liberland 和 PWN-BAR hack team	乌克兰	DDoS	推特	全球	2022 年 2 月
NB65	乌克兰	Hack	推特	不详	2022 年 2 月 28
GNG	乌克兰	DDoS	推特	格鲁吉亚	2022 年 2 月 28
Raidforums2	乌克兰	DDoS	推特	不详	2022 年 2 月 28
ContiLeaks	乌克兰	Data Breach	推特	不详	2022 年 2 月 28
SHDWSec	乌克兰	Hack/Activism	推特	全球	2022 年 2 月 28
GhostClan	乌克兰	DDoS/Hack	电报	全球	2022 年 2 月 28
Free Civicilian	俄罗斯	Data Breach	洋葱	不详	2022 年 1 月
Cooming Project	俄罗斯	Data Breach	洋葱	不详	2021 年
Conti Ransomware	俄罗斯	恶意软件	洋葱	俄罗斯	2019 年

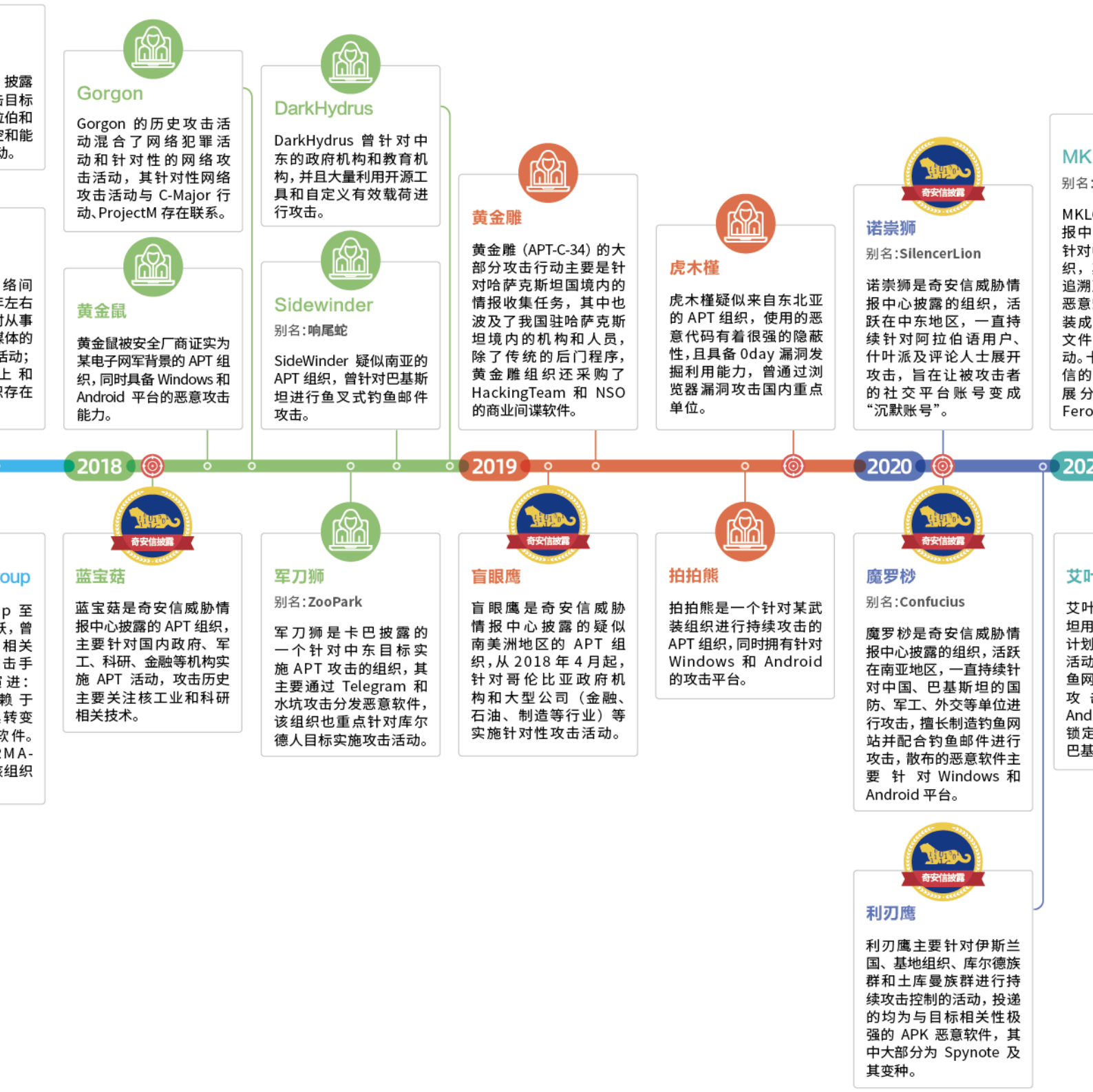
黑客组织	支持阵营	攻击方式	社交媒体	位置	起始日期
The Red Bandits	俄罗斯	Data Breach	推特	俄罗斯	2021 年

附录1 全球主要APT组织列表


奇安信披露
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。
2016
蔓灵花
别名:BITTER
蔓灵花曾针对中国、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，曾针对韩国、中
国等目标区域实施攻击
活动。
索伦之眼
别名:Strider、
ProjectSauron
索伦之眼是一个极为复
杂的网络间谍平台，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
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
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。
2017
MuddyWater
MuddyWater 最早被发现
于 2017 年 2 月至 10 月期
间，针对中东实施了网络
间谍活动，其主要使用的
PowerShell 后门也被称
为 POWERSTATS。
Longhorn
别名:Lamberts
Longhorn 疑似情报机
构背景的攻击团伙，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
BlackTech 疑似网络间
谍组织，主要针对台湾、
日本、香港实施 APT 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
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
Charming Kitte 网
谍组织，从 2014 年
开始活跃，主要针对
学术研究、人权和媒
个人目标开展攻击活
该组织在 TTP
Magic Hound 组织
大量重叠。
Gamaredon Gr
Gamaredon Grou
少从 2013 年起活跃
攻击过乌克兰政府
人员。该团伙的攻
法与工具不断演
由过去严重依
off-the-shelf 工具
为自定义的恶意
OPERATION AR
GEDDON 行动与该
有关。

奇安信 | 奇安信 威胁情报中心

奇安信威胁
49 个主要



情报中心持续跟踪
要 APT 组织

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卡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

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。

21

奇安信披露

针豹

针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roid，攻击目标主要为巴基斯坦用户及斯坦 TLP 政党。

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(Red Drip 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://ti.qianxin.com/blog/articles/lazarus-armory-update-analysis-of-recent-andariel-attacks/

2.https://ti.qianxin.com/blog/articles/king-of-phishing-analysis-of-kimsuky's-recent-spear-phishing-attacks-targeting-south-korea-with-multiple-topics

3.https://mp.weixin.qq.com/s/jX8D8d-4q46pKHS0AIVgjw

4.https://www.malwarebytes.com/blog/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign

5.https://blog.google/threat-analysis-group/countering-threats-north-korea/

6.https://securelist.com/lazarus-trojanized-defi-app/106195/

7.https://ti.qianxin.com/blog/articles/analysis-of-the-lazarus-group-attacks-on-korean-companies/

8.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical

9.https://mp.weixin.qq.com/s/Xs54_RDKU5MvkvsPPCGKEw

10.https://www.cisa.gov/uscert/ncas/alerts/aa22-108a

11.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage

12.https://research.nccgroup.com/2022/05/05/north-koreas-lazarus-and-their-initial-access-trade-craft-using-social-media-and-social-engineering/

13.https://asec.ahnlab.com/en/34461/

14.https://blogs.jpcert.or.jp/en/2022/07/yamabot.html

15.https://mp.weixin.qq.com/s/USitU4jAg9y2XkQxbwcAPQ

16.https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/

17.https://mp.weixin.qq.com/s/R8fvBQDHrTA5-VnKINO5Wg

18.https://asec.ahnlab.com/en/31089/

19.https://blog.alyac.co.kr/4501

20.https://asec.ahnlab.com/en/32958/

21.https://asec.ahnlab.com/en/34694/

22.https://asec.ahnlab.com/ko/34883/

23.https://mp.weixin.qq.com/s/ZV8AOTd7YGUgCTTTZtTktQ

24.https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/

25.https://cluster25.io/2022/01/03/konni-targets-the-russian-diplomatic-sector/

26.https://mp.weixin.qq.com/s/GPpOF-SSJbVR3ZHsx8eXgA

27.https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/

28.https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/suspected-darkhotel-apt-activity-update.html

29.https://www.netskope.com/blog/abusing-microsoft-office-using-malicious-web-archive-files

30.https://ti.qianxin.com/blog/articles/Samples-of-the-OceanLotus-attack-using-the-Glitch-platform/

31.https://mp.weixin.qq.com/s/5gXllrE1srnHtaFCc-86GA

32.https://mp.weixin.qq.com/s/tBQSbv55lJUipaPWFr1fKw

33.https://mp.weixin.qq.com/s/1WtaS7htgiUGhtY_ovERxA

34.https://mp.weixin.qq.com/s/Ah3pFjYk5AOvKvZPwXod6g

35.https://mp.weixin.qq.com/s/NLe4JqmjiB58IQ5Kn6DSLQ

36.https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/

37.https://mp.weixin.qq.com/s/ZNhdLN_AgGfjdk8nG8kLmw

38.https://mp.weixin.qq.com/s/T1-JbC9FsVV2UNnusYPJbw

39.https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/

40.https://ti.qianxin.com/blog/articles/SideCopy's-Golang-based-Linux-tool/

41.https://ti.qianxin.com/blog/articles/Confuser-packed-weapon-of-TransparentTribe/

42.https://ti.qianxin.com/blog/articles/transparent-tribe-and-sidecopy-share-infrastructure/

43.http://blog.nsfocus.net/apt-sidewinder-20220218/

44.https://ti.dbappsecurity.com.cn/blog/articles/2022/03/11/bitter-nepal-army-day/

45.https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html

46.https://mp.weixin.qq.com/s/xKKr5UV26npohwvyv79U0w

47.https://ti.dbappsecurity.com.cn/blog/articles/2022/04/24/bitter-attack-bd/

48.https://mp.weixin.qq.com/s/xRumzCNzQ857I7VDg57mBg

49.https://mp.weixin.qq.com/s/GaYOCLKD77aHcr3fdtZH1w

50.https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html

51.https://mp.weixin.qq.com/s/qsGxZIiTsuI7o-_XmiHLHg

52.https://blog.group-ib.com/sidewinder-antibot

53.https://mp.weixin.qq.com/s/8j_rHA7gdMxY1_X8alj8Zg

54.https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/prime-ministers-office-compromised.html

55.https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

56.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-

espionage-ukraine

57.https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

58.http://blog.nsfocus.net/apt-lorec53-20220216/

59.https://www.cisa.gov/uscert/ncas/alerts/aa22-047a

60.https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

61.https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

62.https://mp.weixin.qq.com/s/j2w_cZgprGsM0zTQ5ngEWA

63.https://mp.weixin.qq.com/s/_3DPj9N3nLhDqlWrqsUcfw

64.https://lab52.io/blog/looking-for-penquins-in-the-wild/

65.https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

66.https://ti.qianxin.com/blog/articles/Analysis-of-attack-activities-of-suspected-aptorganization-unc1151-against-ukraine-and-other-countries/

67.https://mp.weixin.qq.com/s/YsyeLQDR_LQLfKhigSm2_Q

68.https://securityaffairs.co/wordpress/129337/apt/invisimole-targets-ukraine-government.html

69.https://www.malwarebytes.com/blog/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room

70.https://lab52.io/blog/complete-dissection-of-an-apk-with-a-suspicious-c2-server/

71.https://cert.gov.ua/article/39138

72.https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

73.https://inquest.net/blog/2022/04/18/nobelium-israeli-embassy-maldoc

74.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine

75.https://businessinsights.bitdefender.com/deep-dive-into-the-elephant-framework-a-new-cyber-threat-in-ukraine

76.https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns

77.https://cert.gov.ua/article/40102

78.https://mp.weixin.qq.com/s/bIXX0hUITaPkeJ6yf0yWPw

79.https://cluster25.io/2022/05/13/cozy-smuggled-into-the-box/

80.https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/

81.https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/

82.https://mp.weixin.qq.com/s/a94G-QVTGbIc8vu9yL_nww

83.https://mp.weixin.qq.com/s/gJFSlpIlbaI11lcClNN_Xw

84.https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine

85.https://inquest.net/blog/2022/06/27/glowsand

86.https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage

87.https://ti.dbappsecurity.com.cn/info/3065

88.https://ti.qianxin.com/blog/articles/Summary-of-MuddyWater's-recent-attack-activity/

89.https://mp.weixin.qq.com/s/lROsp60YGcOJFbe2vWEmVw

90.https://www.sentinelone.com/labs/wading-through-muddy-waters-recent-activity-of-an-iranian-state-sponsored-threat-actor/

91.https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html

92.https://www.mandiant.com/resources/blog/telegram-malware-iranian-espionage

93.https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf

94.https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html

95.https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

96.https://www.cybereason.com/blog/research/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage

97.https://thedfirreport.com/2022/03/21/apt35-automates-initial-access-using-proxyshell/

98.https://www.malwarebytes.com/blog/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor

99.https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle-east

100.https://team-cymru.com/blog/2022/01/26/analysis-of-a-management-ip-address-linked-to-molerats-apt/

101.https://mp.weixin.qq.com/s/_BQzqAjroi7TBxmT191Vjg

102.https://blog.talosintelligence.com/2022/02/arid-viper-targets-palestine.html

103.https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials

104.https://mp.weixin.qq.com/s/WBCGGLog3IwJhXZmbjxoTQ

105.https://mp.weixin.qq.com/s/1uJaPS-nuGNI8lQ1-ZekIA

106.https://ti.qianxin.com/blog/articles/promethium-attack-activity-analysis-disguised-as-Winrar.exe

107.https://mp.weixin.qq.com/s/yjcCYJNUQq6smc3YsBmYhA

108.https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor

109.https://www.proofpoint.com/us/blog/threat-insight/buy-sell-steal-evilnum-targets-cryptocurrency-forex-commodities

110.https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

111.http://blog.nsfocus.net/murenshark/

112.https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA

113.https://securityintelligence.com/posts/hive00117-fileless-malware-delivery-eastern-europe/

114.https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

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