让每个用户的
数字化更简单、更安全

2023
上半年网络安全观察报告

深信服官方微信　深信服移动官网

深圳市南山区学苑大道1001号南山智园A1栋
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

工业和信息化部电子第五研究所（中国赛宝实验室）　SANGFOR 深信服科技　深信服智安全 SANGFOR SECURITY

摘要 Abstract

▲ 2023 年上半年 0day 漏洞利用数量明显攀升，网络安全形势日益严峻。0day 漏洞利用平均发现天数已经缩短为 2014 年的四分之一，0day 漏洞利用平均发现天数整体呈现下降趋势。

▲ 漏洞危害程度趋向高危化，未修补的漏洞依然是黑客利用的最主要攻击载体。国家级漏洞库披露漏洞中高危和超危漏洞占比超过 50%，根据已知被利用漏洞（KEV）目录收录标准及近 10 年已知被漏洞利用情况分析总结，95% 以上被利用漏洞是 2023 年以前漏洞。

▲ 本地提取漏洞是 2023 上半年实际网络攻击中最常利用的漏洞类型。2023 年上半年 0day 漏洞利用 Top10，微软的 6 个漏洞涉及多个产品，几乎都是本地提权漏洞。从引发威胁的角度看，2023 年上半年由漏洞引发的主要威胁有未授权的信息泄露和管理员访问权限获取。

▲ 2023 年上半年恶意软件攻击次数去年同期相比每月均有小幅度上涨，其类型分布变化不大，其中受影响较大行业为医疗、科研教育和政府等，受影响地区主要是广东省、浙江省和上海市。

▲ 攻击者使用 ChatGPT 生成恶意代码，由于技术门槛降低，使得网络攻击变得更快更容易。地下黑客论坛上已发现了 1500 多条关于如何使用 ChatGPT 进行恶意软件开发的资料，攻击者使用 ChatGPT 等生成式 AI，使网络钓鱼邮件攻击增长 135%。

▲ 我国信创软件安全问题日益凸显，使勒索病毒传播加剧。2023 年 5 月， Tellyouthepass 利用用友 NC 漏洞和亿赛通漏洞进行大规模攻击，信创安全问题日益凸显，加剧勒索病毒传播，严重威胁用户数据安全与财产安全。

▲ 人工智能技术带来的数据安全风险问题成为全球关注新热点。以 ChatGPT 为代表的人工智能技术在 2023 年爆火，人工智能进行交互的过程中敏感数据和隐私内容传输所带来的数据安全风险也成为了新技术场景下需要重点关注和治理的问题。

▲ 数据接口的安全问题是当前导致数据泄露最主要的原因，上半年个人地址信息泄露引发广泛关注。2023 年上半年已经发生多起利用接口导致的泄露事件。政务、医疗、教育行业的数字化数据接口利用是数据泄露的主要原因。

▲ 黑客论坛之间的竞争导致上半年数据泄露事件增加，历史已泄露数据再次遭到泄露。上半年已持续观测到多个新论坛中发布大量历史已泄露数据的合集来吸引黑客，而该行为将持续加大数据泄露的风险。

▲ APT 组织在钓鱼攻击的社工上越发精细，所制作的诱饵越发具有迷惑性。在 2023 年上半年的攻击活动中，APT 组织的钓鱼诱饵制作采取了更加定向的社会工程学分析，并与窃取的真实文件相结合，制作出难以辨别真伪的钓鱼邮件信息。

▲ 供应链攻击将可能成为 APT 组织获取初始权限的流行方式。今年上半年的 3CX 双重供应链攻击事件影响力尤为突出，双重供应链攻击将其传播范围广的特性再次放大，将持续吸引更多组织利用该攻击手法。

▲ BYOVD 技术正广泛应用于各大 APT 攻击活动中。BYOVD 技术从最初被顶尖 APT 组织所使用，发展到如今被越来越广泛的利用在 APT 攻击当中，未来这项技术的使用频率可能会进一步增加，且更加自动化。

▲ 全球 Web3 行业虚拟资产总市值在今年有所下降，但整体资产数量正不断扩大。今年上半年所发生的 Web3 安全事件和去年同期相比数量有所下降。

▲ DeFi（分布式金融）项目依旧是 Web3 领域中被攻击频次最高、损失金额最多的类型。以太坊是所有 Web3 链平台中损失金额最多的，约占 2023 年上半年 75.6% 的损失金额来自，为 3.56 亿美元，

▲ 智能合约漏洞利用是 Web3 攻击中最频发、造成损失最多的攻击手法。在 2023 年上半年，重大智能合约发生安全事件 60 次，造成损失 2.64 亿美元，占所有损失金额的 56%。

CONTENTS 目录

安全漏洞态势

- **安全漏洞治理现状** 02
  - 国外安全漏洞治理现状 02
  - 我国安全漏洞治理现状 02
- **安全漏洞态势** 03
  - 漏洞公开披露情况 03
  - 漏洞利用情况 04
- **关键漏洞分析** 08
  - Windows 08
  - WebLogic 12
  - Chrome 15
  - F5 BIG-IP 17
- **安全漏洞态势小结** 19

恶意软件态势

- **恶意软件态势** 21
  - 恶意软件攻击总体情况 21
  - 恶意软件类型分布 21
  - 恶意软件攻击行业分布 22
  - 恶意软件攻击地区分布 23
  - 活跃恶意软件家族情况 23
- **恶意软件家族分析** 24
  - 挖矿病毒家族 24
  - 勒索病毒家族 26
  - 僵尸网络家族 28
  - 远控木马家族 30
- **恶意软件攻击动态** 32
  - 攻击者利用 ChatGPT 技术进行攻击 32
  - 攻击者利用弱口令爆破和开源工具进行挖矿 32
  - 攻击者利用信创系统漏洞进行勒索攻击 33
- **恶意软件态势小结** 33

数据安全态势

- **数据安全治理情况** 35
  - 国外数据安全治理动向 35
  - 我国数据安全治理动向 35
- **数据交易监控情况** 37
  - 黑灰产交易类型分布 37
  - 重要数据泄露发现渠道分布 37
  - 重要数据泄露影响行业分布 38
- **重点数据泄露事件分析** 39
  - 大量个人地址泄露 39
  - 接口滥用导致敏感数据泄露 39
  - 黑客论坛中的数据泄露 39
- **数据泄露黑客论坛情况** 40
  - 黑客论坛发展态势 40
  - 流行黑客论坛 40
  - 新增黑客论坛 41
- **勒索团伙数据泄露情况** 42
  - 勒索团伙数据泄露数量趋势 42
  - 多重勒索软件团伙活跃排行 43
  - 新活跃多重勒索团伙 43
- **数据安全态势小结** 44

APT 攻击态势

- **APT 攻击活动态势** 46
  - APT 组织攻击总体态势 46
  - 南亚活跃 APT 组织态势 46
  - 东亚活跃 APT 组织态势 48
  - 东欧活跃 APT 组织态势 50

- **APT 攻击流行技术趋势** **51**
  - 软件供应链攻击获取 APT 攻击初始权限 51
  - 开源组件二次开发以降低 APT 攻击成本 53
  - BYOVD 滥用过时驱动以对抗杀软 53
- **典型 APT 攻击事件** **54**
  - 某高校高新行业实验室被高精准社工鱼叉攻击 54
  - 蔓灵花利用开源远控组件攻击某政府机关单位 54
  - UNC4736 组织利用双重供应链攻击 3CX 公司 55
  - 美国情报机构针对 iOS 设备的移动端 APT 活动 55
- **APT 攻击态势小结** **56**

Web3 安全态势

- **Web3 安全态势情况** **58**
  - Web3 安全事件总体态势 58
  - Web3 安全事件损失情况 59
  - Web3 安全事件趋势 62
- **Web3 合约安全情况** **63**
  - Web3 安全攻击手段总览 63
  - Web3 合约安全风险分析 64
  - Web3 合约安全风险的应对策略 67
  - Web3 典型合约安全事件剖析 68
- **Web3 安全产业发展情况** **71**
  - 国家政策对 Web3 安全产业的支持 71
  - 标准组织对 Web3 安全产业的引领 72
  - 资本市场对 Web3 安全产业的推动 73
  - 企业应用在 Web3 安全产业的探索 73
- **Web3 安全态势小结** **75**

参考链接

01 安全漏洞态势

- 安全漏洞治理现状
- 安全漏洞态势
- 关键漏洞分析
- 安全漏洞态势小结

安全漏洞治理现状

国外安全漏洞治理现状

（一）美国相关政策提升漏洞共享能力，强化国家级网络安全漏洞综合治理能力。众观美国网络安全战略，“协调”和“共享”一直是美国网络安全战略的主旋律，2021 年 5 月拜登政府签署《改善国家网络安全的行政命令》，明确提出消除政府和私营部门之间威胁信息共享的障碍。CISA 将统筹漏洞治理作为重要任务，通过协同漏洞披露（CVD）、漏洞披露策略（VDP）、相关约束性操作指令（BOD）等措施加强了联邦政府和私营部门的协调和合作，实现了对关键基础设施漏洞威胁的及时发现和消控，加强漏洞管控统筹协调，提升漏洞资源共享共治水平，强化美国国家级网络安全漏洞综合治理能力。

（二）CISA 新战略计划指出国家努力的重点是确定关键基础设施的脆弱性，旨在降低关键信息基础设施风险并增强防御国家级威胁的能力。2022 年 9 月，CISA 发布“2023-2025 年战略计划”，本计划是 CISA 自 2018 年成立以来第一个全面的战略计划。计划指出国家努力的重点是确定哪些系统和资产对国家真正至关重要，发现关键信息基础设施的脆弱性，并采取行动管理来降低其风险。计划的首要目标就是建立国家级防御网络攻击并从中恢复的能力，CISA 作为美国的网络防御机构，将与全球建立全面战略伙伴关系，共建国家级威胁防御能力。

（三）美国加强已知漏洞的修复，降低已知被利用漏洞的重大风险。2021 年 11 月，CISA 颁布《约束性操作指令 (BOD) 22-01，降低已知利用漏洞的重大风险》，要求所有联邦民事行政部门 (FCEB) 机构都必须在规定的时间内修复已知被利用漏洞（KEV）目录中的漏洞。CISA 强烈建议所有利益相关者将已知被利用漏洞（KEV）目录的漏洞纳入其漏洞管理计划的一部分，通过优先修复目录中列出的漏洞来增强其安全性和恢复能力。

我国安全漏洞治理现状

（一）我国漏洞相关政策的相继出台主要目的是维护国家网络安全，保障网络产品和重要网络系统的安全稳定运行。根据《网络安全法》关于漏洞管理有关要求，工业和信息化部、国家互联网信息办公室、公安部联合制定《网络产品安全漏洞管理规定》，主要目的是维护国家网络安全，保护网络产品和重要网络系统的安全稳定运行，规范漏洞发现、报告、修补和发布等行为，明确网络产品提供者、网络运营者、以及从事漏洞发现、收集、发布等活动的组织或个人等各类主体的责任和义务；鼓励各类主体发挥各自技术和机制优势开展漏洞发现、收集、发布等相关工作。

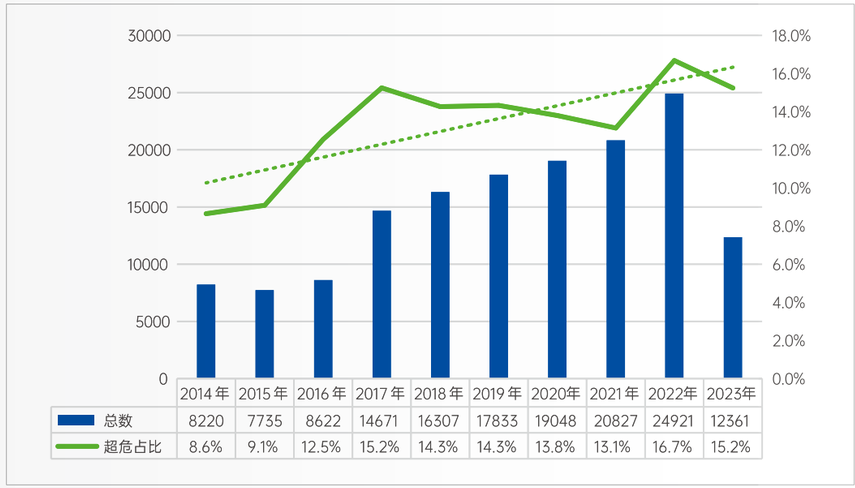
（二）我国持续推进《网络产品安全漏洞管理规定》落实工作，从政策宣贯、机制完善、平台建设多方面抓好落实。一是加强了政策宣贯，做好对相关企业机构的政策咨询和工作指导，引导漏洞收集平台依法依规开展漏洞收集和发布。二是完善了相关工作机制，建立健全漏洞评估、发布、通报等重要环节的工作机制，明确了漏洞收集平台备案方式和报送内容。三是加强了工业和信息化部网络安全威胁和漏洞信息共享平台建设，做好与其他漏洞平台、漏洞库的信息共享，提升平台技术支撑能力。

安全漏洞态势

漏洞公开披露情况

近十年总体情况

截止 2023 年 6 月 10 日，国家信息安全漏洞库（CNNVD）共收录 2023 年漏洞信息 12361 条，近 10 年漏洞收录情况如图 1-1 所示，可以看出，漏洞收录数量逐年增长，超危漏洞占比整体呈上升趋势，超危漏洞占比峰值为 2022 年（占比 16.7%），按照往年超危漏洞占比趋势推测，2023 年下半年超危漏洞占比会进一步增长。



	2014 年	2015 年	2016 年	2017 年	2018 年	2019 年	2020年	2021 年	2022年	2023年
总数	8220	7735	8622	14671	16307	17833	19048	20827	24921	12361
超危占比	8.6%	9.1%	12.5%	15.2%	14.3%	14.3%	13.8%	13.1%	16.7%	15.2%

图 1-1 CNNVD 近十年漏洞收录情况

漏洞危害等级布情况

2023 年 1 月 -6 月，根据国家信息安全漏洞库（CNNVD）收录情况，从漏洞危害程度来看，2023 年上半年，超危漏洞占比 15.2%，高危漏洞占比 35.7%，高危和超危漏洞占比超过 50%，漏洞危害程度趋向高危化，极易被病毒、木马、黑客等利用，导致系统的安全风险加大。

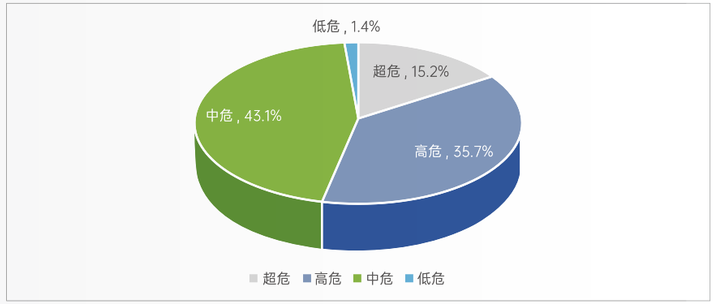


图 1-2 2023 年上半年 CNNVD 收录漏洞危害等级分布

漏洞引发威胁情况

2023 年 1 月 -6 月，根据国家信息安全漏洞共享平台（CNVD）统计数据显示，上半年漏洞引发威胁情况如图 1-3 所示，由漏洞引发的最主要威胁是未授权信息泄露，未授权信息泄露可能会导致个人隐私受到侵犯，造成财务损失，破坏商业信誉，甚至可能导致法律诉讼。未授权信息泄露还有可能是黑客攻击的前置条件，秘钥、token 等敏感信息泄露可以被恶意攻击者进一步利用，访问受保护的资源或执行未经授权的操作。

其次，漏洞引发的威胁是管理员访问权限获取，获取了管理员权限就拥有了完全控制权，攻击者可以访问系统中的敏感数据，更改系统设置，控制整个系统，以及进行其他恶意活动。

黑客攻击手段通常可分为非破坏性攻击和破坏性攻击两类。非破坏性攻击一般是为了扰乱系统的运行，并不盗窃系统资料；破坏性攻击是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的。从漏洞引发威胁的角度来看，我国上半年网络攻击趋向于破坏性攻击，这种攻击可能会导致系统崩溃、数据丢失、服务中断等严重后果，对受害者造成极大的损失。

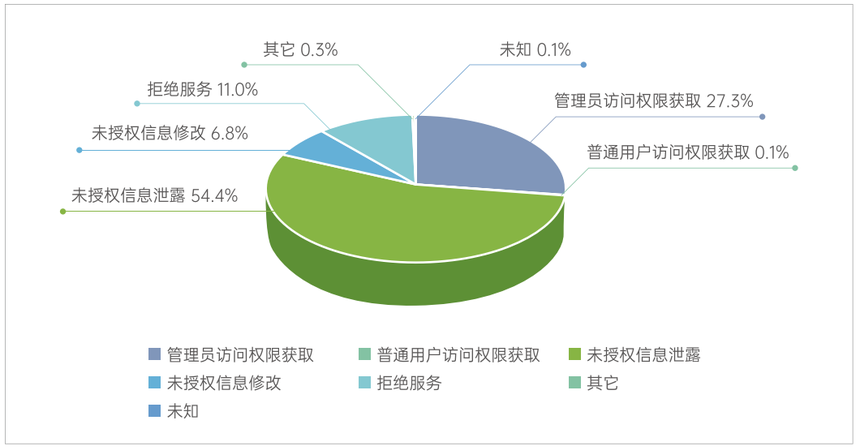


图 1-3 2023 年上半年漏洞引发威胁情况

漏洞利用情况

近十年总体情况

已知被利用漏洞（KEV）目录是为了美国国家安全和网络防御者的利益而创建，自创建以来持续更新，是已知被利用漏洞的权威来源。该目录当前维护了近 1000 个已知被利用漏洞。已知被利用漏洞（KEV）目录收录的三个标准是：漏洞已分配 CVE 编号、有可靠证据表明该漏洞在真实攻击中已被积极利用、漏洞已有明确的补救措施。

未修补的漏洞依然是黑客利用的最主要攻击载体。针对已知被利用漏洞（KEV）进行分析，近 10 年真实漏洞利用数量总体呈现上升趋势，2021 年漏洞利用数量达到峰值 179 个。对比去年数据，2023 上半年新添加漏洞利用情况如图 1-4 黄色图例所示，今年添加各个年份漏洞数量总体来看相差不大，排除 2023 年数据，添加年份为 2022 年的漏洞数量最多。从统计图来看，不仅近两年漏洞被添加到该目录，甚至十年前的漏洞今年仍有被添加，侧面反应出未及时进行补丁安装导致恶意攻击者利用漏洞入侵系统情况广泛存在。

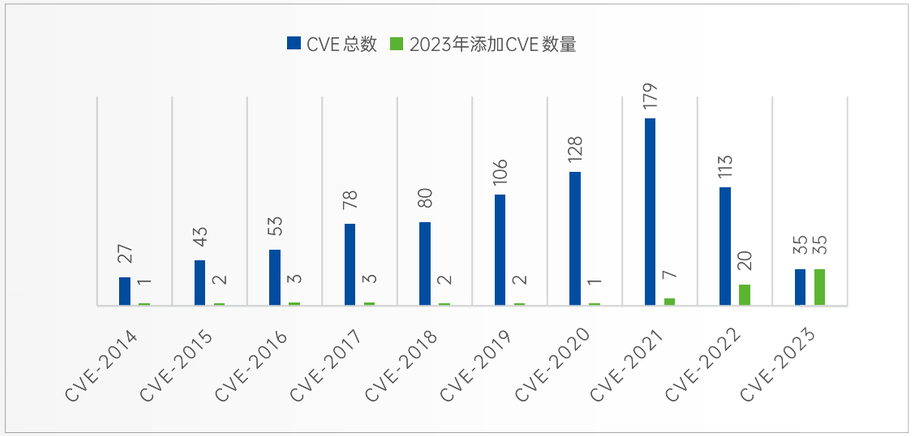


图 1-4 KEV 目录近十年漏洞利用情况

被利用漏洞主要厂商及产品情况

根据已知被利用漏洞（KEV）目录进行统计分析，已知被利用漏洞厂商分布与厂商漏洞增长情况如图 1-5 所示，厂商漏洞排名靠前的有 Microsoft（259 个）、Cisco（64 个）和 Adobe（60 个）。对比去年数据，各厂商已知被利用漏洞增长情况如黄色折线所示，增速较高的是 Apple、Google、Oracle 等厂商，按照增长率推算，预计下半年 Apple、Google、Oracle 等厂商将有较多已知被利用漏洞披露。

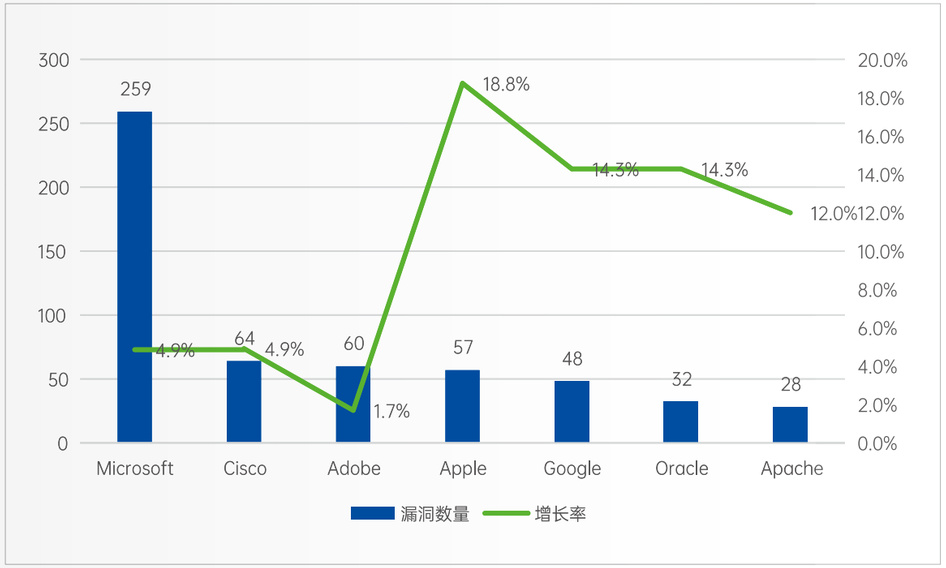


图 1-5 已知被利用漏洞厂商漏洞分布与漏洞增长情况

图 1-6 为已知被利用漏洞产品分布情况，Windows 操作系统是受影响最严重的产品，占比 10.5%。Windows 操作系统是目前应用最广泛的操作系统之一，其用户遍布全球。根据深信服千里目安全技术中心数据显示，Windows 全球公网资产超过 1.2 亿，中国公网资产超过 2200 万，其影响之大可见一斑。建议国内用户重点针对 Windows 操作系统进行漏洞评估，及时修补漏洞，以保障系统的安全性。

排名第二的产品是 InternetExplorer，占比 3.3%，漏洞类型主要以远程代码执行和内存损坏为主。浏览器漏洞的危害性是非常大的，黑客可以利用漏洞来执行恶意代码、窃取用户的敏感信息等。利用钓鱼链接触发浏览器漏洞获取权限是 APT 组织和黑灰产团伙常见攻击手段之一，这种攻击手法隐蔽性更高，用户往往难以察觉攻击的存在，而且攻击者可以通过不断改变攻击方式和手段来规避安全防护措施。

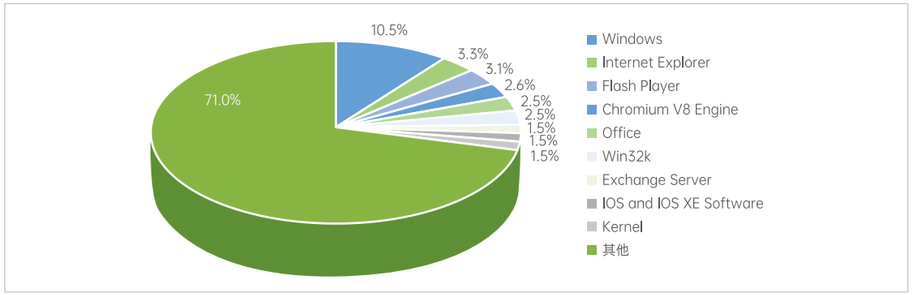


图 1-6 已知被利用漏洞产品分布情况

0day 漏洞利用发现情况

0day 漏洞利用数量明显攀升，网络安全形势日益严峻。根据谷歌团队跟踪的 0day 被利用漏洞情况进行分析，近 10 年 0day 漏洞利用发现情况如下图所示，可以看出，0day 漏洞利用平均发现天数整体呈现下降趋势，2023 年上半年，0day 漏洞利用平均发现天数已经缩短为 2014 年的四分之一，说明被利用 0day 漏洞数量在逐年上升。2021 年 0day 漏洞利用平均发现天数最小，平均而言，每 5.3 天就会发现一个新的被利用 0day 漏洞，但实际上，这些漏洞通常聚集在同一天发现的漏洞链中。

被利用 0day 漏洞数量之所以攀升如此明显，最主要原因是黑客利用 0day 漏洞进行攻击能够更高概率的躲避现有安全体系的防御措施，提高攻击成功率。

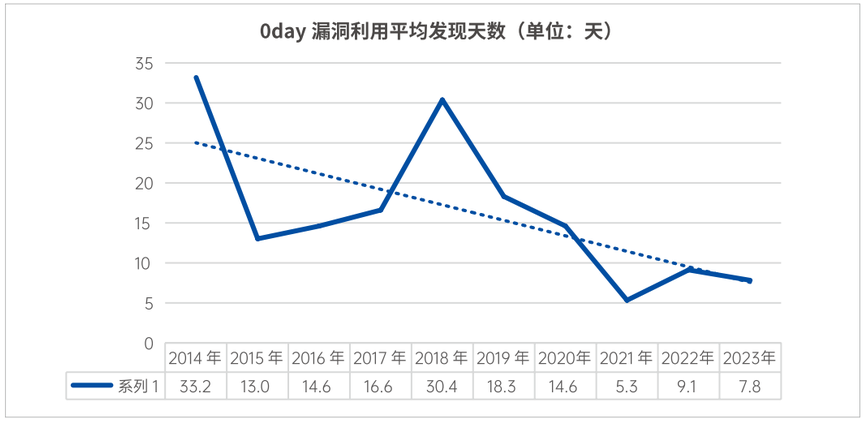


图 1-70day 漏洞利用发现情况

关键被利用 0day 漏洞盘点

本地提权漏洞是上半年实际网络攻击中最主要利用的漏洞类型。根据深信服千里目安全技术中心以及谷歌跟踪 0day 漏洞利用情况综合分析，2023 年上半年被利用 0day 漏洞 Top10 如表 1-1 所示。关键 0day 漏洞的发现时间主要集中在 1 月和 4 月，微软的 6 个漏洞发现时间集中在第一季度，涉及多个产品，几乎都是本地提权漏洞，对权限要求均比较低，无需与用户交互。攻击者利用特权提升漏洞可以执行更多的操作，包括但不限于修改系统配置、读取敏感数据、执行恶意代码等。攻击者还可以利用这些权限来控制整个系统，甚至是整个网络。

浏览器漏洞的危害一直不容小觑，上半年 Chrome 关键被利用 0day 漏洞主要以类型混淆和整数溢出为主。其中，危害等级最为严重的是 Google Chrome Skia 整数溢出漏洞（CVE-2023-2136），由于 Skia 中存在缺陷，当算术运算导致值超过整数类型的最大限制时，会发生整数溢出。攻击者通过诱导用户打开特制的 HTML 页面来触发该漏洞，最终导致在目标系统上任意执行代码。

被利用 0day 漏洞名称	漏洞类型	危害等级	攻击向量			发现时间
			攻击途径	权限要求	用户交互	
Google Chrome Skia 整数溢出漏洞 (CVE-2023-2136)	整数溢出	超危	网络	无	需要	4 月
Google Chrome V8 类型混淆漏洞 (CVE-2023-2033)	类型混淆	高危	网络	无	需要	4 月
Google Chrome 类型混淆漏洞 (CVE-2023-3079)	类型混淆	未知	未知	未知	未知	6 月
Microsoft Outlook 特权提升漏洞（CVE-2023-23397）	权限提升	超危	网络	无	无	3 月
Windows ALPC 特权提升漏洞 (CVE-2023-21674)	权限提升	高危	本地	低	无	1 月
Windows 图形组件权限提升漏洞（CVE-2023-21823）	权限提升	高危	本地	低	无	2 月
Windows CLFS 驱动程序提升权限漏洞（CVE-2023-23376）	权限提升	高危	本地	低	无	2 月
WinSock 特权提升漏洞（CVE-2023-21768）	权限提升	高危	本地	低	无	1 月
Windows CLFS 驱动程序权限提升漏洞（CVE-2023-28252）	权限提升	高危	本地	低	无	4 月
Linux 内核释放后使用漏洞 (CVE-2023-0266)	资源管理错误	高危	本地	低	无	1 月

表 1-1 2023 年上半年关键 0day 漏洞利用盘点

关键漏洞分析

Windows

产品介绍

Microsoft Windows，是微软以图形用户界面为主推出的一系列专有商业软件操作系统。它于 1985 年问世，起初为运行于 MS-DOS 之下的桌面环境，其后续版本逐渐发展成为主要为个人电脑和服务器用户设计的操作系统，Windows 以超过 90% 的市场份额占领了全球个人计算机市场，并最终获得了世界个人电脑操作系统的垄断地位。

影响分布

根据深信服千里目安全技术中心数据显示，Windows 操作系统流行版本全网使用量分布情况如图 1-8 所示，从服务器操作系统在中国大陆使用量来看，Windows Server 各个版本使用量主要分布在北京、广东省和浙江省，其次使用量较高的是上海和山东。Windows 服务器操作系统在中国大陆公网的资产超过 820 万，其中资产数量最多的版本是 Windows Server 2012，超过 490 万。

桌面操作系统 Windows 中国大陆使用量主要分布在浙江省、北京市和广东省，其次是上海市和江苏省。Windows 7 中国公网资产超过 270 万，占全球比例高达 40.1%。虽然 Windows 7 和 Windows 10 已经发布了很长时间，但它们仍然是当前最流行的桌面操作系统。

根据表 1-2，对 2023 年上半年 Windows 关键漏洞进行盘点，几乎每个关键漏洞都影响了 Windows 操作系统各个流行版本，并且多个漏洞已被发现真实利用情况。Windows 操作系统漏洞对我国的潜在安全影响可能是非常严重的，由于 Windows 操作系统在我国的计算机市场占有率较高，其漏洞可能会影响大量的计算机和用户。这些漏洞可能会导致计算机系统被黑客攻击，造成数据泄露、系统瘫痪、网络瘫痪等问题，给我国的经济和社会带来严重的损失。

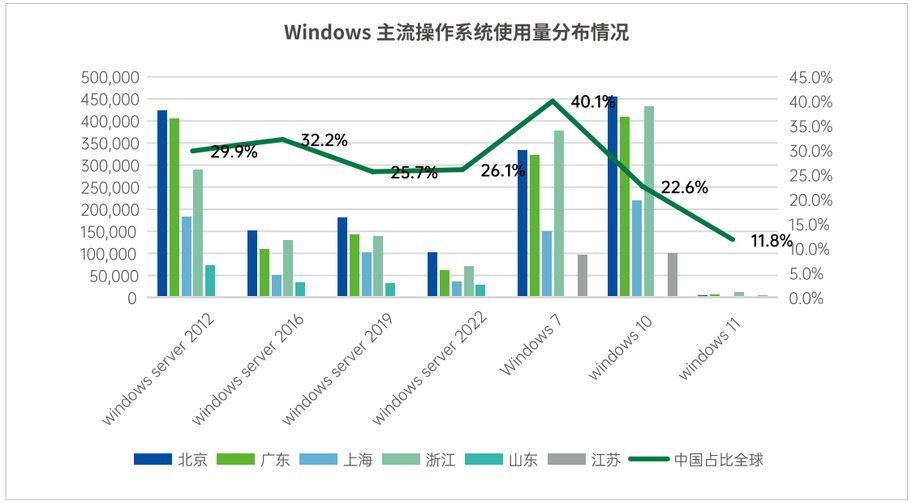


图 1-8 Windows 主流操作系统分布情况

涉及漏洞

根据深信服千里目安全技术中心数据显示，Windows 操作系统流行版本全网使用量分布情况如图 1-8 所示，从服务器操作系统在中国大陆使用量来看，Windows Server 各个版本使用量主要分布在北京、广东省和浙江省，其次使用量较高的是上海和山东。Windows 服务器操作系统在中国大陆公网的资产超过 820 万，其中资产数量最多的版本是 Windows Server 2012，超过 490 万。

桌面操作系统 Windows 中国大陆使用量主要分布在浙江省、北京市和广东省，其次是上海市和江苏省。Windows 7 中国公网资产超过 270 万，占全球比例高达 40.1%。虽然 Windows 7 和 Windows 10 已经发布了很长时间，但它们仍然是当前最流行的桌面操作系统。

根据表 1-2，对 2023 年上半年 Windows 关键漏洞进行盘点，几乎每个关键漏洞都影响了 Windows 操作系统各个流行版本，并且多个漏洞已被发现真实利用情况。Windows 操作系统漏洞对我国的潜在安全影响可能是非常严重的，由于 Windows 操作系统在我国的计算机市场占有率较高，其漏洞可能会影响大量的计算机和用户。这些漏洞可能会导致计算机系统被黑客攻击，造成数据泄露、系统瘫痪、网络瘫痪等问题，给我国的经济和社会带来严重的损失。

产品	CVE 编号	严重等级 / 漏洞影响	受影响的系统	利用情况
Windows ALPC	CVE-2023-21674	重要 特权提升	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Windows 8.1	真实利用
Windows Win32K	CVE-2023-29336	重要 特权提升	Windows 10 Server 2016 Server 2012 R2 Server 2012	真实利用
	CVE-2023-29359	重要 特权提升	Windows Server 2012 Windows Server 2012 R2 Windows Server 2008 Windows Server 2008 R2 Windows Server 2016 Windows Server 2019 Windows 10 Windows 11	易被利用

产品	CVE 编号	严重等级 / 漏洞影响	受影响的系统	利用情况
Windows CLFS	CVE-2023-23376	重要 特权提升	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012	真实利用
	CVE-2023-28252	重要 特权提升	Windows 11 Windows 10 Windows Server 2008 Windows Server 2012 R2 Windows Server 2012 Windows Server 2016 Windows Server 2022	真实利用
Windows DHCP	CVE-2023-28231	重要 远程代码执行	Server 2022 Server 2019 Server 2016 Server 2012 R2 Server 2012	易被利用
Windows NFS	CVE-2023-24941	严重 远程代码执行	Server 2022 Server 2019 Server 2016 Server 2012 R2 Server 2012	易被利用
Windows OLE	CVE-2023-29325	严重 远程代码执行	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012	易被利用
Windows MSHTML 平台	CVE-2023-29324	重要 安全功能绕过	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012	易被利用
Windows Kernel	CVE-2023-24949	重要 特权提升	Windows 10 Windows 11 Windows Server 2019 Windows Server 2022	易被利用
Microsoft PEAP	CVE-2023-21689	严重 远程代码执行	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012	易被利用
Windows Kerberos	CVE-2023-21817	重要 特权提升	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012	不太可能利用
Windows ODBC 驱动程序	CVE-2023-21732	重要 远程代码执行	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1	不太可能利用
	CVE-2023-21797	重要 远程代码执行	Windows 11 22H2 Windows 11 version 21H2 Server 2022 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012	不太可能利用

表 1-2 2023 年上半年 Windows 操作系统关键漏洞盘点

Windows 小结

Windows 操作系统今年上半年漏洞类型主要以特权提升和代码执行为主，且多个重要漏洞几乎影响全版本。今年上半年已发现的被利用漏洞多以特权提升为主，说明在真实攻击中，恶意攻击者利用漏洞进行权限提升是非常普遍的，往往需要通过漏洞去执行恶意代码或者访问受限资源，从而控制系统或者获取更多的敏感信息。预计下半年，Windows 操作系统漏洞将以特权提升类型为主。

在列出的关键漏洞中已被利用的漏洞并非是等级为“严重”的，说明实际漏洞利用情况与 CVSS 评估情况存在一定差异性。在评估漏洞时，需要考虑到实际环境中的因素，以确定漏洞的真实威胁程度。

Windows 11 和 Windows Server 2022 是近一两年发布的，目前相较 Windows 其他版本市场占有率偏低，并且新系统在发布之初相对来说还不够成熟，出现安全问题几率相对较大，预计未来两年影响新发布操作系统漏洞数量居多。

WebLogic

产品介绍

WebLogic 是美国 Oracle 公司出品的一个 application server，WebLogic 是一种 Java EE 应用服务器，确切的说是一个基于 JAVAEE 架构的中间件。它提供了一个环境来开发、部署和管理 Java 应用程序，支持 Java EE 规范，如 Servlet、JSP、EJB、JMS、JDBC 等。WebLogic 还提供了高可用性、可伸缩性和安全性等特性，使其成为企业级应用程序的首选平台之一。WebLogic 还提供了一些管理工具，如 WebLogic Server 控制台和 WebLogic Scripting Tool，以便管理员可以轻松地管理和监控 WebLogic 服务器。

影响分布

根据深信服千里目安全技术中心数据显示，WebLogic 中国大陆公网使用量分布情况如图 1-9 所示，排名靠前的区域有北京市（9673）和浙江省（8692），其次是广东省（5304）和上海市（4993）。中国大陆公网资产近 5 万，WebLogic 部署在内网居多，实际使用量远超公网测绘资产量。

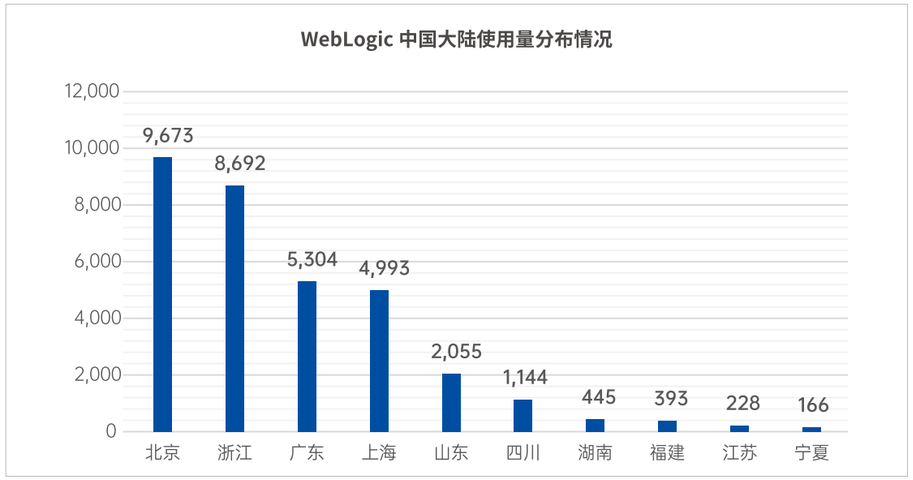


图 1-9 WebLogic 中国大陆使用量分布情况

涉及漏洞

根据深信服千里目安全技术中心数据显示，WebLogic 中国大陆公网使用量分布情况如图 1-9 所示，排名靠前的区域有北京市（9673）和浙江省（8692），其次是广东省（5304）和上海市（4993）。中国大陆公网资产近 5 万，WebLogic 部署在内网居多，实际使用量远超公网测绘资产量。

CVE 编号	漏洞介绍	严重等级 / 利用情况	受影响的软件
CVE-2023-21839	WebLogic Server 远程代码执行漏洞 未经身份验证的远程攻击者通过 T3/IIOP 协议网络访问并破坏易受攻击的 WebLogic 服务器，成功利用此漏洞可能导致 Oracle WebLogic 服务器被接管或敏感信息泄露。	重要 真实利用	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0
CVE-2023-21996	WebLogic Server 拒绝服务漏洞 未经身份验证的远程攻击者通过 HTTP 进行网络访问，从而危害 Oracle WebLogic Server。成功利用此漏洞会导致 Oracle WebLogic Server 挂起或频繁重复崩溃，造成拒绝服务攻击。	重要 未知	WebLogic Server 12.2.1.3.0 Oracle WebLogic Server 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0
CVE-2023-21838	WebLogic Server 拒绝服务漏洞 未经身份验证的攻击者通过 T3、IIOP 进行网络访问，从而危及 Oracle WebLogic Server。成功攻击此漏洞可能导致未经授权的 Oracle WebLogic Server 挂起或频繁重复崩溃（完全 DOS）。	重要 未知	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0
CVE-2023-21964	WebLogic Server 拒绝服务漏洞 未经身份验证的远程攻击者通过 T3 进行网络访问，从而危害 Oracle WebLogic Server。成功利用此漏洞会导致 Oracle WebLogic Server 挂起或频繁重复崩溃，造成拒绝服务攻击。	重要 未知	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0
CVE-2023-21931	WebLogic Server 信息泄露漏洞 未经身份验证的远程攻击者通过 T3 进行网络访问，从而危害 Oracle WebLogic Server。此漏洞的成功攻击可能导致对关键数据的未经授权的访问或对所有 Oracle WebLogic Server 可访问数据的完全访问。	重要 未知	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0

CVE 编号	漏洞介绍	严重等级 / 利用情况	受影响的软件
CVE-2023-21979	WebLogic Server 信息泄露漏洞 未经身份验证的远程攻击者通过 T3 进行网络访问，从而危害 Oracle WebLogic Server。此漏洞的成功攻击可能导致对关键数据的未经授权的访问或对所有 Oracle WebLogic Server 可访问数据的完全访问。	重要 未知	WebLogic Server 12.2.1.3.0 Oracle WebLogic Server 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0
CVE-2023-21842	WebLogic Server 信息泄露漏洞 未经身份验证的攻击者通过 HTTP 进行网络访问，从而危及 Oracle WebLogic Server。成功攻击此漏洞可能导致对关键数据的未授权访问或对所有 Oracle WebLogic Server 可访问数据的完全访问	重要 未知	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0
CVE-2023-21837	WebLogic Server 信息泄露漏洞 未经身份验证的攻击者通过 IIOP 进行网络访问，从而危及 Oracle WebLogic Server。成功攻击此漏洞可能导致对关键数据的未授权访问或对所有 Oracle WebLogic Server 可访问数据的完全访问	重要 未知	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0
CVE-2023-21841	WebLogic Server 信息泄露漏洞 未经身份验证的攻击者通过 T3、IIOP 进行网络访问，从而危及 Oracle WebLogic Server。成功攻击此漏洞可能导致对关键数据的未授权访问或对所有 Oracle WebLogic Server 可访问数据的完全访问	重要 未知	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server 14.1.1.0.0

表 1-3 2023 年上半年 WebLogic 关键漏洞盘点

WebLogic 小结

从今年 Oracle 官网 1 月和 4 月发布补丁情况来看，今年上半年 WebLogic 漏洞类型多以拒绝服务、信息泄露和远程代码执行为主。从漏洞数量方面来看，今年上半年 WebLogic 漏洞数量与去年下半年持平，无明显变化。2022 年下半年 WebLogic 漏洞多为第三方组件引入问题，今年上半年漏洞多为 WebLogic Server 内核问题。

WebLogic Server 内核漏洞可能会导致攻击者远程执行任意代码、绕过安全限制、泄露敏感信息等安全问题。CVE-2023-21839 是今年上半年的一个典型 WebLogic Server 内核漏洞，未经身份验证的远程攻击者通过 T3/IIOP 协议网络访问并破坏易受攻击的 WebLogic 服务器，成功利用此漏洞可能导致 Oracle WebLogic 服务器被接管或敏感信息泄露。

WebLogic 已经稳定运行了多年，是较为成熟的产品，根据近两年 Oracle 发布漏洞数据来看，预计下半年漏洞类型不会有明显变化，或将在内核方面出现更多漏洞。

Chrome

产品介绍

Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具，特点是简洁、快速。它支持多种操作系统，包括 Windows、MacOS、Linux 和 Android 等。Chrome 的特点包括快速的页面加载速度、简洁的用户界面、强大的扩展功能和安全性能。Chrome 还支持多个标签页，可以同时浏览多个网页，并且可以通过 Google 账户同步书签、历史记录和其他设置。Chrome 也支持多种语言，包括中文。此外，Chrome 基于更强大的 JavaScriptV8 引擎，提升浏览器的处理速度。

影响分布

根据深信服千里目安全技术中心数据显示，Chrome 浏览器中国大陆公网使用量分布情况如图 1-10 所示，公网资产超过 100 万的区域有浙江省、北京市、广东省、上海市和山东省，多为互联网发达地区。中国大陆公网资产超过 5000 万，占全球比例 8.5%。StatCounter 的 5 月研究报告显示，Chrome 浏览器凭借 62.85% 的全球份额稳居第一，由于 Chrome 使用范围广泛，因此其漏洞利用会影响大量用户。

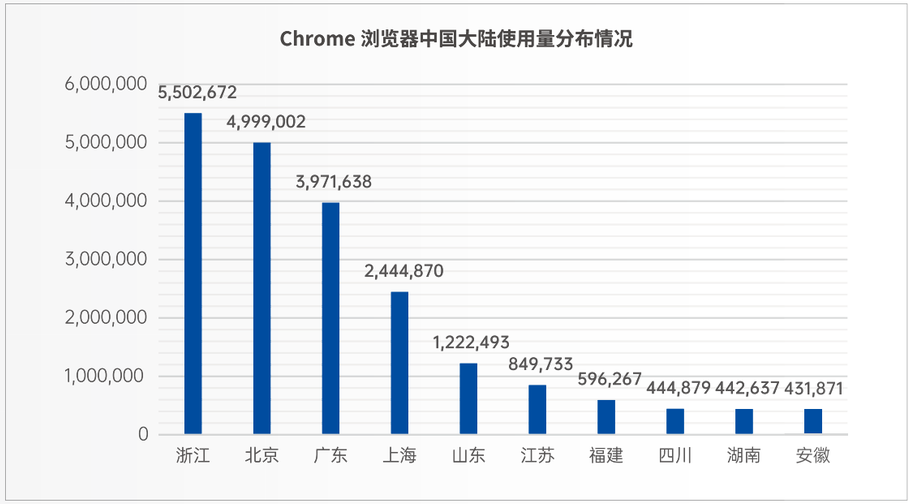


图 1-10 Google Chrome 浏览器中国大陆使用量分布情况

漏洞名称	漏洞类型	漏洞价格	严重等级 / 利用情况	受影响软件
CVE-2023-2136	整数溢出	N/A	重要 真实利用	Google Chrome<112.0.5615.137
CVE-2023-2033	类型混淆	N/A	重要 真实利用	Google Chrome<112.0.5615.121
CVE-2023-3079	类型混淆	N/A	重要 真实利用	Google Chrome<114.0.5735.110

漏洞名称	漏洞类型	漏洞价格	严重等级 / 利用情况	受影响软件
CVE-2023-2724	类型混淆	N/A	重要 未知	Google Chrome<113.0.5672.126
CVE-2023-1214	类型混淆	10000 美元	重要 未知	Google Chrome<111.0.5563.64
CVE-2023-2721	释放后重用	待决定	严重 未知	Google Chrome<113.0.5672.126
CVE-2023-0941	释放后重用	待决定	严重 未知	Google Chrome<110.0.5481.177
CVE-2023-0927	释放后重用	31000 美元	重要 未知	Google Chrome<110.0.5481.177
CVE-2023-0928	释放后重用	13000 美元	重要 未知	Google Chrome<110.0.5481.177
CVE-2023-0471	释放后重用	16000 美元	重要 未知	Google Chrome<109.0.5414.119
CVE-2023-3214	释放后重用	待决定	严重 未知	Google Chrome<114.0.5735.133
CVE-2023-2929	越界写入	15000 美元	重要 未知	Google Chrome<114.0.5735.90
CVE-2023-2457	越界写入	17500 美元	重要 未知	Google Chrome<113.0.5672.114
CVE-2023-1528	资源管理错误	10000 美元	重要 未知	Google Chrome<111.0.5563.110
CVE-2023-1213	资源管理错误	15000 美元	重要 未知	Google Chrome<111.0.5563.64

表 1-4 2023 年上半年 Google Chrome 关键漏洞盘点

Chrome 小结

从 Google Chrome 官网发布补丁情况来看，今年上半年 Chrome 漏洞类型主要以类型混淆、释放后重用、越界写入和资源管理错误为主。今年上半年，已知被利用漏洞（KEV）目录检测到 Chrome 的 3 个被利用漏洞有 2 个为类型混淆漏洞。

根据 Google Chrome 官网披露数据。今年上半年 Chrome 漏洞危害等级为严重的漏洞有 3 个，漏洞类型均为释放后重用，目前尚未给出 3 个漏洞奖金金额。

Google Chrome 漏洞奖励的金额一般从 500 美元到数万美元不等，据不完全统计，今年上半年 Chrome 单个漏洞金额超过 10000 美元的 Chrome 漏洞有 12 个，最高金额为 31000 美元，2023 上半年谷歌公司为 Chrome 中的 69 个漏洞支付赏金总计近 40 万美元，2022 年谷歌公司为 Chrome 中 473 个漏洞支付赏金总计 400 万美元。对比 2022 年赏金数据，今年上半年漏洞数量和奖金总额偏低，有可能 Google 官网未给出上半年全量数据，但就目前披露情况来看，总体低于去年。

根据往年数据推测，预计 2023 年下半年 Chrome 漏洞数量将会进一步增长，根据往年漏洞平均赏金推算，预计下半年平均漏洞赏金将会进一步提高。

F5 BIG-IP

产品介绍

F5 BIG-IP 是一种应用交付控制器（ADC），它是一种网络设备，它可以帮助组织管理和优化其应用程序交付。它提供了负载均衡、应用程序安全、应用程序加速、应用程序性能监控和管理等功能。F5 BIG-IP 可以在物理、虚拟和云环境中部署，支持多种应用程序协议和技术，如 HTTP、HTTPS、TCP、UDP、SSL、TLS、IPSec 等。它还提供了丰富的 API 和集成选项，以便与其他系统和工具集成。F5 BIG-IP 是一种成熟的、可靠的且使用广泛的 ADC 解决方案，被许多企业和服务提供商用于管理其应用程序交付。

影响分布

F5 BIG-IP 既可以用于内网也可以用于外网，具体使用情况取决于组织的需求和网络架构。在内网中，F5 BIG-IP 可以用于负载均衡、应用程序交付、安全等方面，以提高内部应用程序的可用性和性能。在外网中，F5 BIG-IP 可以用于应用程序交付、安全、DDoS 防护等方面，以保护面向互联网的应用程序免受攻击和滥用。

根据深信服千里目安全技术中心数据显示，F5 BIG-IP 中国大陆公网使用量分布情况如图 1-11 所示，使用量较多的省份有天津市（30131）和上海市（25851）。其次是河北省、广东省和四川省。F5 BIG-IP 还多用于内网，实际使用量远超公网资产数量。F5 BIG-IP 美国使用量居多，中国大陆公网资产超过 38 万，仅占全球 8.8%，但其影响依然较大。

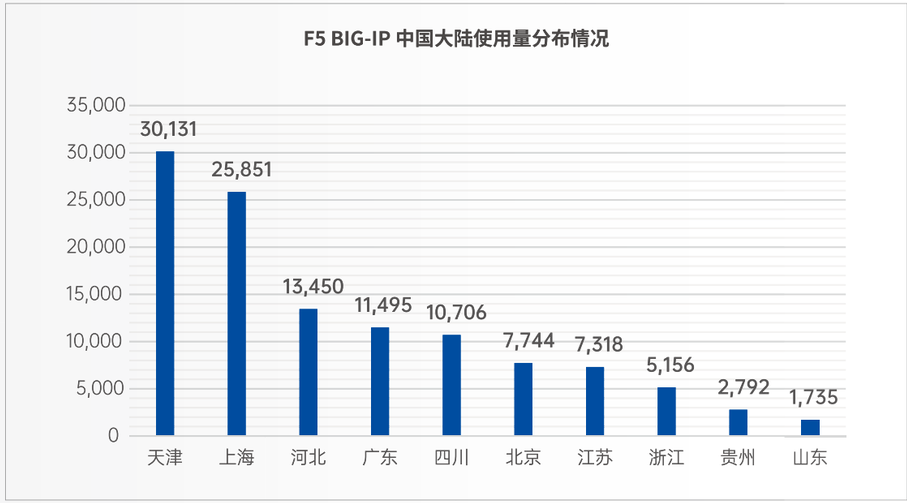


图 1-11 F5 BIG-IP 中国大陆使用量分布情况

CVE 编号	漏洞名称	严重等级 / 漏洞影响	受影响软件
CVE-2023-22326	F5 iControl REST and TMSH 权限管理不当漏洞	重要 权限管理不当	BIG-IP (all modules)
CVE-2023-22302	F5 BIG-IP 拒绝服务漏洞	重要 拒绝服务	BIG-IP (all modules)

CVE 编号	漏洞名称	严重等级 / 漏洞影响	受影响软件
CVE-2023-22418	F5 BIG-IP APM 虚拟服务器开放重定向漏洞	重要 开放重定向	BIG-IP (APM)
CVE-2023-22283	F5 BIG-IP Edge Client for Windows 命令执行漏洞	重要 命令执行	BIG-IP (APM) BIG-IP APM Clients
CVE-2023-23555	F5 BIG-IP Virtual Edition 拒绝服务漏洞	重要 拒绝服务	BIG-IP (all modules) BIG-IP SPK
CVE-2023-22839	F5 BIG-IP DNS 配置文件拒绝服务漏洞	重要 拒绝服务	BIG-IP (DNS, LTM enabled with DNS Services License)
CVE-2023-22422	F5 HTTP 配置文件拒绝服务漏洞	重要 拒绝服务	BIG-IP (all modules)
CVE-2023-22842	F5 BIG-IP SIP 配置文件拒绝服务漏洞	重要 拒绝服务	BIG-IP (all modules)
CVE-2023-22340	F5 BIG-IP SIP 配置文件拒绝服务漏洞	重要 拒绝服务	BIG-IP (all modules)
CVE-2023-23552	F5 BIG-IP AWAF 和 ASM 拒绝服务漏洞	重要 拒绝服务	BIG-IP (ASM)
CVE-2023-22664	F5 BIG-IP HTTP/2 配置文件拒绝服务漏洞	重要 拒绝服务	BIG-IP (all modules) BIG-IP SPK
CVE-2023-22341	F5 BIG-IP APM Oauth 拒绝服务漏洞	重要 拒绝服务	BIG-IP (APM)
CVE-2023-22281	F5 BIG-IP AFM 拒绝服务漏洞	重要 拒绝服务	BIG-IP (APM)
CVE-2023-22323	F5 BIG-IP SSL OCSP 认证配置文件拒绝服务漏洞	重要 拒绝服务	BIG-IP (all modules)
CVE-2023-22358	F5 BIG-IP Windows Edge Client 客户端 DLL 劫持漏洞	重要 DLL 劫持	BIG-IP (APM) BIG-IP APM Clients
CVE-2023-22374	F5 iControl SOAP 权限提升漏洞	重要 权限提升	BIG-IP (all modules)

表 1-5 2023 年上半年 F5 BIG-IP 关键漏洞盘点

影响分布

从 F5 官网发布补丁信息可知，今年上半年 F5 BIG-IP 漏洞类型主要为拒绝服务漏洞，多个漏洞影响 F5 BIG-IP 所有模块。

F5 BIG-IP 拒绝服务类型漏洞：攻击者通过发送恶意请求或数据包，导致设备崩溃或无法正常工作，从而拒绝服务。这种漏洞可能会导致网络中的所有服务不可用，从而影响企业的正常运营。该类型的漏洞危害较为严重。

根据深信服千里目安全技术中心公网资产测绘数据情况来看，天津、上海、河北、广东和四川等区域使用量较大，上半年披露 F5 BIG-IP 漏洞多为高危漏洞，一旦漏洞被成功利用，将造成严重后果，建议上述区域企业用户加强漏洞扫描和安全评估，及时发现和修复漏洞。

安全漏洞态势小结

01 **漏洞危害程度趋向高危化，系统的安全风险加大。**根据 2023 年上半年 CNNVD 漏洞数据分析总结，从国家级漏洞库披露漏洞情况可以观察得出，高危和超危漏洞占比超过 50%，漏洞危害程度趋向高危化，极易被病毒、木马、黑客等利用。

02 **0day 漏洞利用数量明显攀升，网络安全形势日益严峻。**根据谷歌团队近 10 年跟踪的 0day 漏洞利用情况进行分析，2023 年上半年，0day 漏洞利用平均发现天数已经缩短为 2014 年的四分之一，0day 漏洞利用平均发现天数整体呈现下降趋势，说明 0day 漏洞利用数量在逐年上升。

03 **未修补的漏洞依然是黑客利用的最主要攻击载体。**根据已知被利用漏洞（KEV）目录收录标准及近 10 年已知被漏洞利用情况分析总结，95% 以上被利用漏洞是 2023 年以前漏洞，并且均已发布补丁。

04 **本地提取漏洞是 2023 上半年实际网络攻击中最常利用的漏洞类型。**根据深信服千里目安全技术中心以及谷歌跟踪 0day 漏洞利用情况综合分析，2023 年上半年 0day 漏洞利用 Top10，微软的 6 个漏洞涉及多个产品，几乎都是本地提权漏洞，且多个重要漏洞几乎影响全版本。

05 **预计 2023 年下半年，Chrome 漏洞数量和漏洞平均赏金将会进一步增长。**2023 上半年谷歌公司为 Chrome 中的 69 个漏洞支付赏金总计近 40 万美元，2022 年谷歌公司为 Chrome 中 473 个漏洞支付赏金总计 400 万美元。就目前披露情况来看，漏洞数量和漏洞平均赏金总体低于去年和前年。

06 **从漏洞引发威胁的角度来看，网络攻击趋向于破坏性攻击。**根据 2023 年上半年 CNVD 收录漏洞进行分析，由漏洞引发的主要威胁有未授权的信息泄露和管理员访问权限获取。网络攻击趋向于破坏性攻击，这种攻击可能会导致系统崩溃、数据丢失、服务中断等严重后果，对受害者造成极大的损失。

02

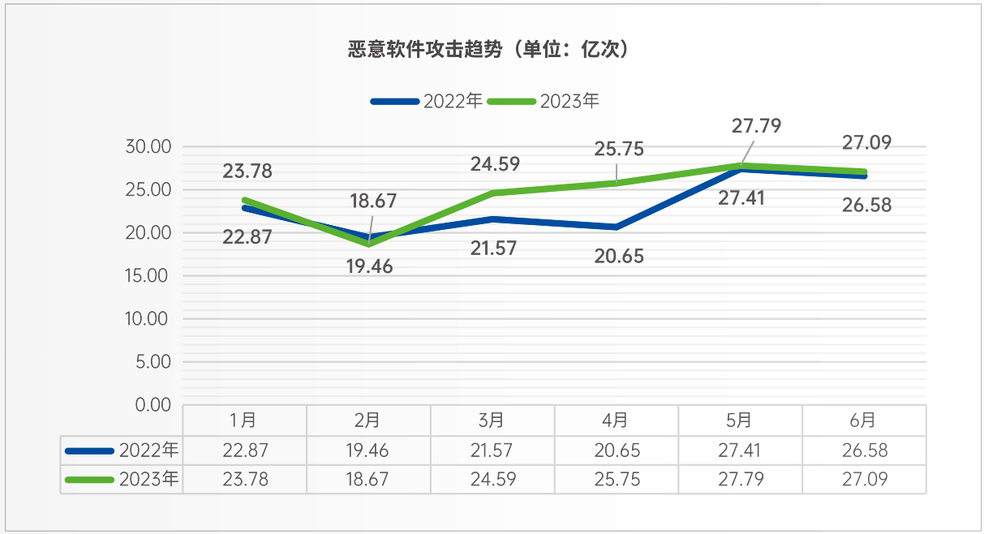
恶意软件态势

- 恶意软件态势
- 恶意软件家族分析
- 恶意软件攻击动态
- 恶意软件态势小结

恶意软件态势

恶意软件攻击总体情况

根据深信服千里目安全技术中心统计数据，2023 年 1 月至 6 月的恶意软件攻击趋势如图 2-1 所示，2023 上半年我国遭受恶意软件攻击总次数达 147.67 亿次，比去年同时段的 138.54 亿次有小幅度上升，同比增长 6.6%。整体来看，2023 年上半年恶意软件各月攻击次数较 2022 年上半年各月攻击次数均有小幅度增长，3 月和 4 月增速较大，去年和今年的攻击高峰期均在 5 月，攻击低峰期均为 2 月。



	1月	2月	3月	4月	5月	6月
2022年	22.87	19.46	21.57	20.65	27.41	26.58
2023年	23.78	18.67	24.59	25.75	27.79	27.09

图 2-1 恶意软件攻击趋势

恶意软件类型分布

根据深信服千里目安全技术中心统计数据，2023 年 1 月 -6 月恶意软件攻击类型分布如图 2-2 所示。2023 年上半年对比 2022 年上半年，恶意软件攻击总次数有小幅度上升，恶意软件类型分布没有太大变化，挖矿病毒和远控木马攻击占比有小幅度上升，挖矿占比由 40.5% 上升到 42.9%，远控木马占比由 23.4% 上升到 26.2%。僵尸网络占比较去年上半年有大幅度下降，占比由去年的 17.4% 下降到 8.3%。蠕虫、后门软件、感染型病毒较去年没有太大变化。为降低挖矿和远控木马感染风险，建议用户及时更新计算机系统，不随意下载和安装未知来源的软件，使用杀毒软件和防火墙等安全工具，以及定期备份重要数据，保障系统安全。

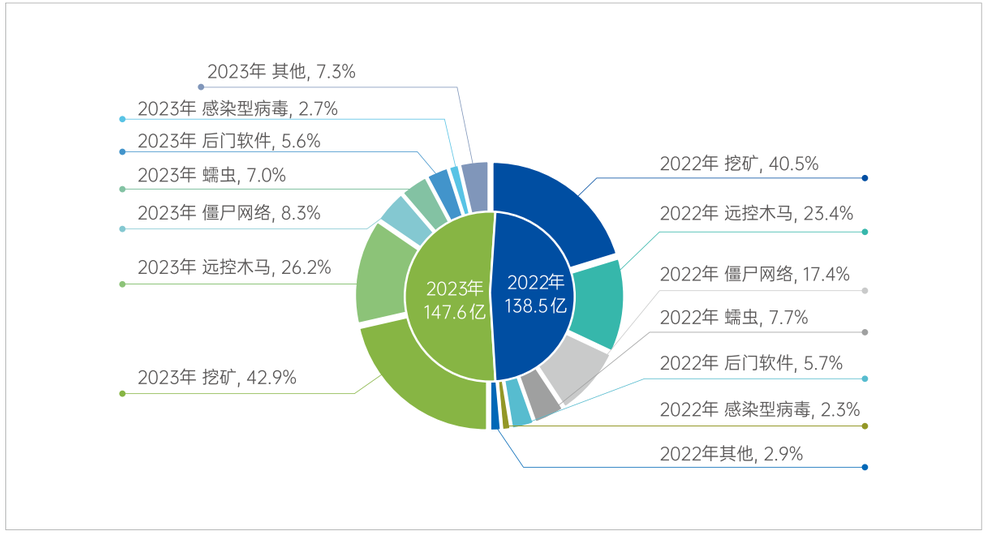


图 2-2 2023 年和 2022 年 1 月 -6 月恶意软件攻击类型分布

恶意软件攻击行业分布

根据深信服千里目安全技术中心统计数据，2023 年 1 月 -6 月恶意软件攻击行业分布如图 2-3 所示。2023 年上半年受恶意软件影响较为严重的行业主要是企业、医疗、科研教育和政府等行业，攻击占比超过 80%。其次，能源、电信和媒体等行业也受到一定影响。针对受恶意软件影响较严重行业，建议采取适当的安全措施来保护其计算机系统和数据，做好安全合规，以免有被监管通报风险，以安全合规为根本 , 建设安全合规管理体系 , 才能不断提高企业安全水平。

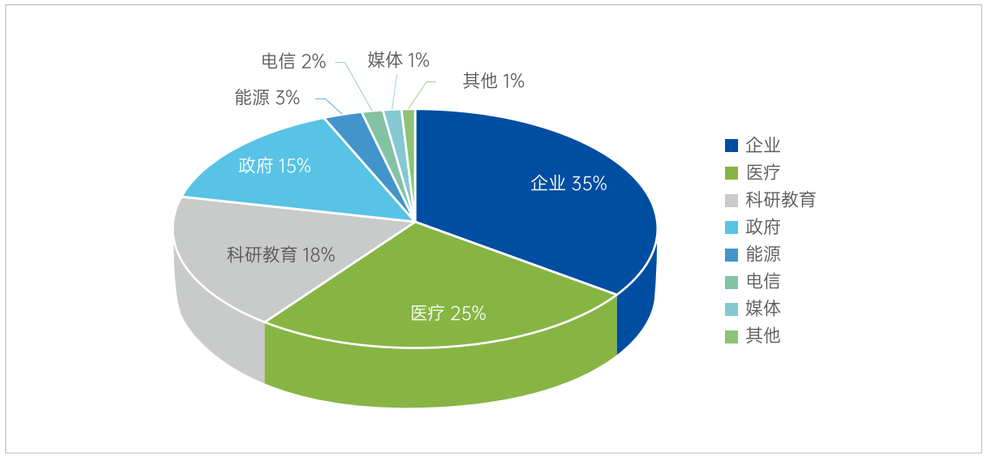


图 2-3 2023 年 1 月 -6 月恶意软件攻击行业分布

恶意软件攻击地区分布

根据深信服千里目安全技术中心统计数据，2023 年 1 月 -6 月恶意软件攻击省份 TOP10 情况如图 2-4 所示。受恶意软件攻击最为严重的区域有广东省、浙江省和上海市，攻击次数均超过 10 亿，分别为 22.2 亿次，13.2 亿次和 11.3 亿次。江苏省、山东省、北京市和河北省也是受影响较为严重地区，攻击次数均在 6 亿次以上，均为互联网较为发达地区。广东省、浙江省和上海市，攻击次数均超过 10 亿，分别为 22.2 亿次，13.2 亿次和 11.3 亿次。

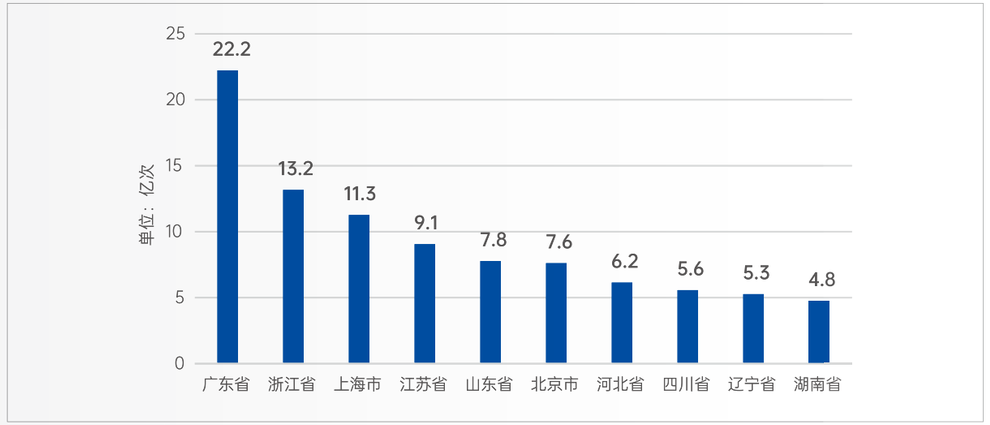


图 2-4 2023 年 1 月 -6 月恶意软件攻击区域分布

活跃恶意软件家族情况

根据深信服千里目安全技术中心统计数据，2022 年和 2023 年 1 月至 6 月活跃恶意软件家族情况如图 2-5 所示。远控木马 Gamarue 家族连续两年蝉联第一，攻击次数较去年有小幅度上升。和去年一样，排在第二名的是挖矿病毒 WannaMine 家族，今年上半年攻击次数有移动成度下降。挖矿病毒 TeamTNT 和蠕虫病毒 Xred 代替蠕虫病毒 Conficker 和挖矿病毒 StartMiner 成为 2023 年上半年活跃恶意软件 TOP5 家族。

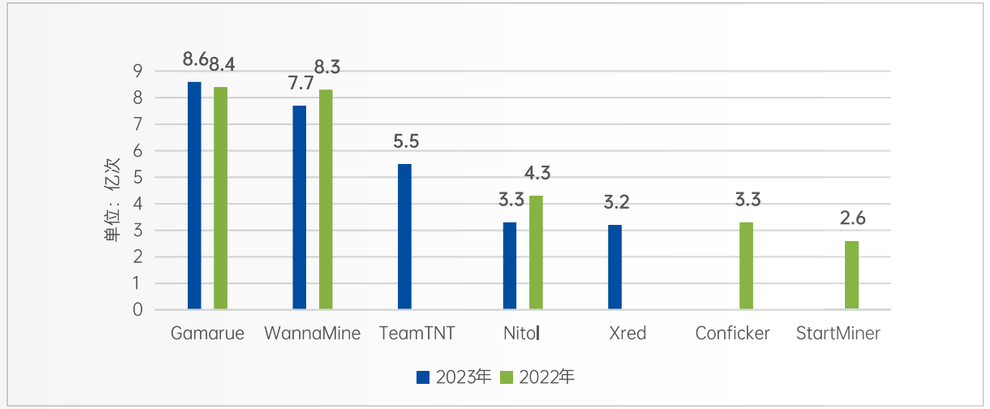


图 2-5 2022 年和 2023 年 1 月 -6 月活跃恶意软件家族

恶意软件家族分析

挖矿病毒家族

挖矿病毒态势

根据深信服千里目安全技术中心统计数据来看，如图 2-6 所示，2023 年上半年我国挖矿病毒活跃家族 TOP5 分别是 WannaMine、TeamTNT、StartMiner、DriveLife 和 LemonDuck。对比去年上半年，活跃家族整体情况无太大变化，TeamTNT 挖矿家族代替 PowerGhost 挖矿家族跃升为今年上半年挖掘活跃家族 TOP5。

PwerGhost 是从 2018 年被发现使用 powershell 无文件方式进行攻击感染的挖矿病毒，其感染方式利用了永恒之蓝，MSSQL 爆破，SSH 爆破，wmi 以及 smb 爆破远程命令执行等，同时对 windows 和 linux 进行攻击，一旦该病毒进入内网，会在内网迅速传播。

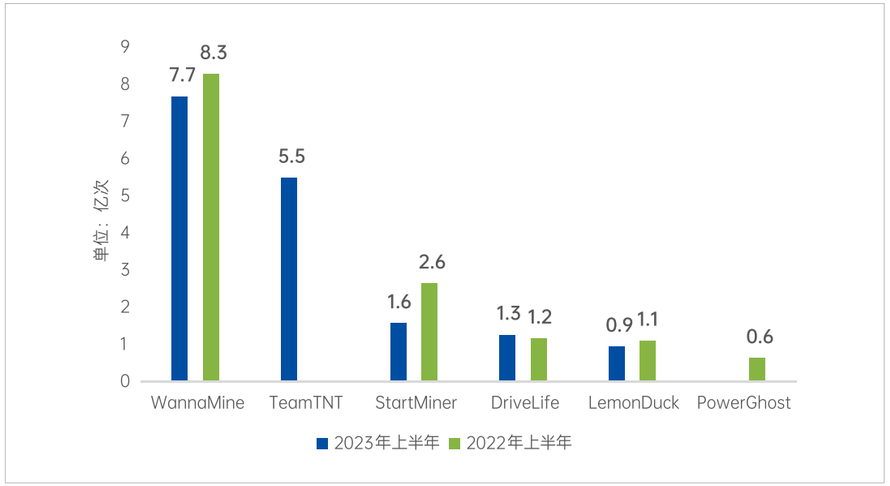


图 2-6 2022 年和 2022 年 1 月 -6 月挖矿病毒活跃家族 TOP5

2023 年 1 月至 6 月挖矿病毒攻击省份 TOP10 情况如图 2-7 所示。攻击量排名第一的是广东省，攻击次数为 5.7 亿次，其次是浙江省、江苏省、北京市和山东省。今年上半年挖矿病毒供给量排名前十的省份攻击次数均超过了 1 亿次，挖矿攻击形势不容乐观。

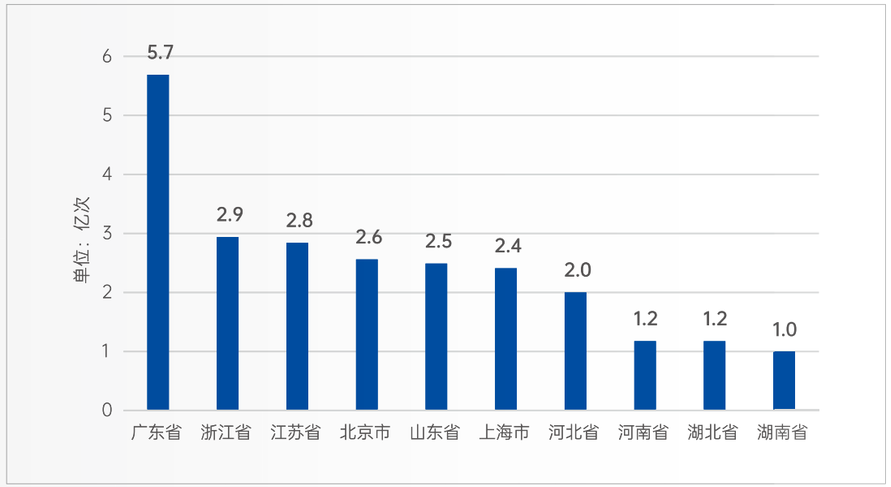


图 2-7 挖矿病毒活跃地区 TOP10

2023 年 1 月 -6 月挖矿病毒主要攻击的行业有企业、教育、医疗、政府和能源等行业，占比分别为 40.5%、19.6%、17.5%、15.7% 和 4.4%。这些行业拥有大量的计算资源，而挖矿病毒在挖矿过程中需要消耗大量计算资源，因此这些行业成为了首选攻击目标。

挖矿病毒新增家族

受利益驱使，以“挖矿”产生的虚拟货币促使了网络黑产快速升级，变相滋生了各种网络犯罪。挖矿病毒不断推陈出新，Hoze 和 ProxyShellMiner 是今年新增挖矿木马家族，这些挖矿家族不仅给受害者带来了经济损失，还会占用计算机资源，导致计算机运行缓慢，甚至崩溃。

（1）Hoze 挖矿木马

Hoze 挖矿木马于 2023 年被国内安全厂商发现用于挖取门罗币，主要是利用 SSH 弱口令暴力破解对 Linux 平台进行攻击。

Hoze 挖矿木马主动扫描 22 端口，利用 SSH 远程访问进行初始访问，并执行 shell 脚本。它通过创建账户、添加 SSH 密钥、计划任务等方式在内部实现持久化。为了规避防御，利用 shc 工具混淆文件、修改文件和目录权限、删除攻击脚本。通过修改系统用户口令以获取凭据访问，并收集系统信息。最终占用 CPU 资源进行资源劫持。

（2）ProxyShellMiner 挖矿团伙

2023 年安全厂商 Morphisec 研究人员发现新恶意程序 ProxyShellMiner 企图滥用 Exchange Server 的 ProxyShell 漏洞 CVE-2021-34473 与 CVE-2021-34523，在受害者系统上植入挖矿软件。

攻击者先通过漏洞获得对组织网络的初始访问权限，再将 .NET 恶意软件负载放入域控制器的 NETLOGON 文件夹中，以确保网络上的所有设备都运行该恶意软件。再下载名为“DC_DLL”的文件并执行 .NET 反射以提取任务调度器、XML 和 XMRig 密钥的参数。矿工创建一个计划任务，配置为在任何用户登录时运行，在受感染机器上获得持久性。最后，创建一个适用于所有 Windows 防火墙配置文件的规则来阻止所有传出流量。

挖矿病毒小结

2023 年上半年对比去年上半年，挖矿病毒活跃家族整体无太大变化。2023 年上半年我国挖矿病毒活跃家族 TOP5 分别是 WannaMine、TeamTNT、StartMiner、DriveLife 和 LemonDuck。TeamTNT 挖矿家族代替 PowerGhost 挖矿家族跃升为今年上半年挖矿活跃家族 TOP5。

受挖矿病毒影响较大的区域有广东省、浙江省、江苏省、北京市和山东省。上半年以上几个区域遭受挖矿攻击的次数均超过了 2.5 亿次，广东省受挖矿攻击最为严重，攻击次数高达 5.7 亿次。今年上半年挖矿病毒供给量排名前十的省份攻击次数均超过了 1 亿次，挖矿攻击形势不容乐观。

2023 年 1 月至 6 月挖矿病毒主要攻击的行业有企业、教育、医疗、政府和能源等行业，占比分别为 40.5%、19.6%、17.5%、15.7% 和 4.4%。这些行业拥有大量的计算资源，而挖矿病毒在挖矿过程中需要消耗大量计算资源，因此这些行业成为了首选攻击目标。

勒索病毒家族

勒索病毒态势

根据深信服千里目安全技术中心统计数据，2023 年 1 月 -6 月我国勒索软件应急响应事件 TOP10 家族如图 2-8 所示，Mallox 和 Tellyouthepass 勒索家族并列第一，应急响应事件 11 起。Phobos、BeijingCrypt、Lockbit3.0 和 Trigona 等勒索家族也较为活跃，上半年应急响应事件均为 3 起以上。对比去年上半年我国勒索软件应急响应事件 TOP10 家族情况，Trigona 和 Crysis 勒索家族代替 Hive 和 Magniber 成为上半年 TOP10 家族。

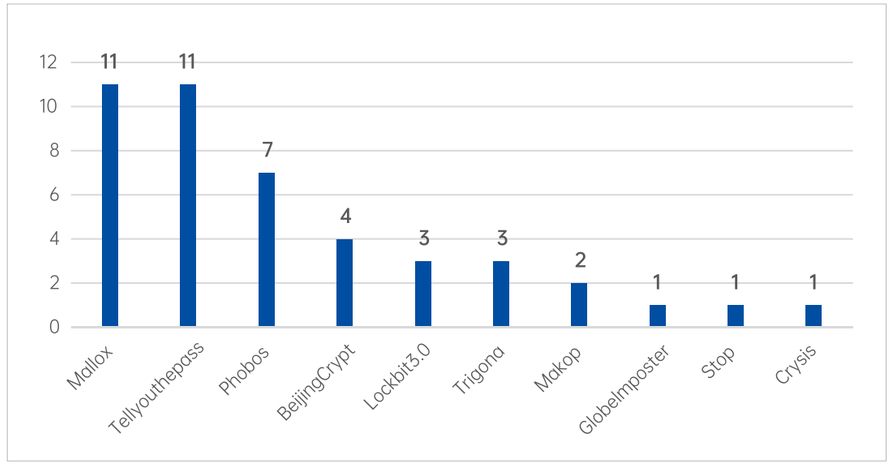


图 2-8 勒索软件病毒活跃家族 TOP10

2023 年 1 月 -6 月勒索软件病毒攻击省份 TOP10 情况如图 2-9 所示。攻击量排名第一的省份是广东省，其次是浙江省，攻击次数分别为 5200 万次、860 万次。其余省市攻击量相差不大，上半年受勒索软件攻击次数均超过 100 万次。

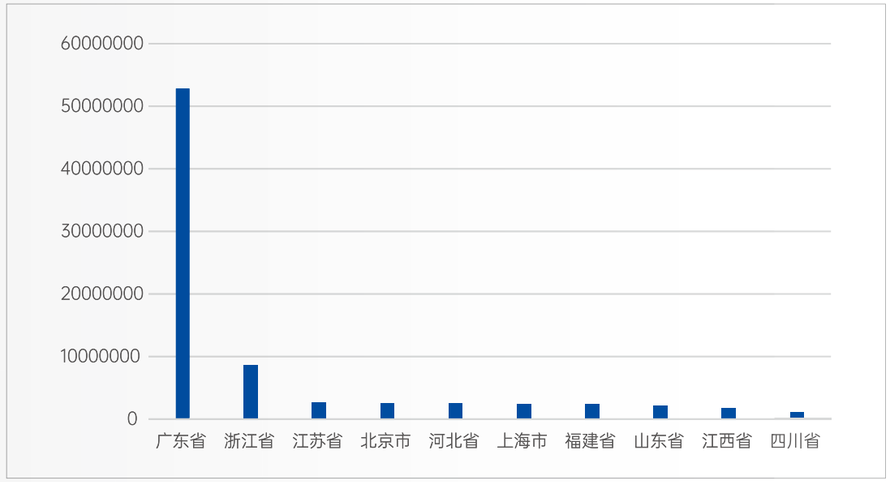


图 2-9 勒索软件病毒攻击地区 TOP10

2023 年 1 月 -6 月共计响应勒索攻击事件 46 起，针对响应勒索攻击事件进行分析，制造业、科技和医疗等行业受勒索软件影响最为严重，分别占比 35%、24% 和 13%。教育和政府也较为频繁的受勒索软件攻击。

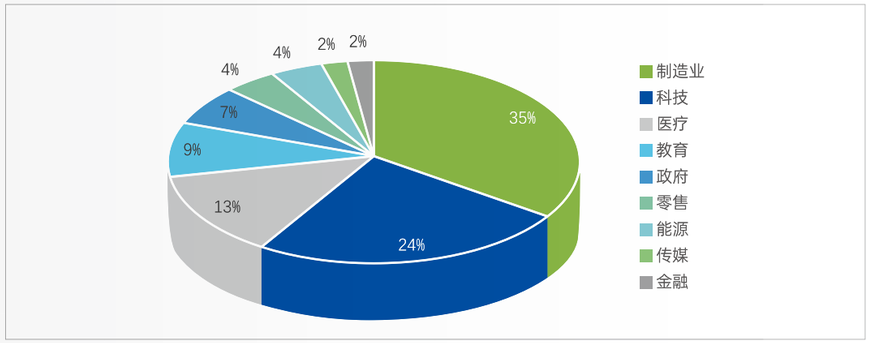


图 2-10 2023 年 1 月 -6 月勒索软件病毒攻击行业分布

勒索病毒新增家族

据不完全统计，2023 年 1 月 -6 月新增了 32 个家族，如 Money Message、RA Group。Money Message 主要攻击大型企业，RA Group 要求受害者通过 qTox 聊天应用程序与该组织取得联系。

（1）Money Message 勒索软件

Money Message 勒索软件于 2023 年 3 月首次被 Cyble 研究人员发现，受害者来自不同行业。因其对知名计算机硬件供应商 MSI（微星国际）的攻击而受到媒体关注，在此次事件中该勒索软件组织窃取了大约 1.5TB 数据，并要求支付 400 万美元的赎金。

Money Message 能够加密网络共享，主要针对 Windows 和 Linux 操作系统。Money Message 勒索采用 ECDH 和 ChaCha20 组合的方式加密目标系统上的文件，并嵌入 json 格式的配置文件以便于设置加密策略。此外，Money Message 还会尝试使用内置的账户密码登录远程主机，并通过横向感染扩大勒索危害。

（2）RA Group 勒索软件

RA Group 勒索软件于 2023 年 4 月被 Cisco Talos 研究人员发现，该组织已侵入 3 个美国组织和 1 个韩国组织，涉及多个垂直行业，包括制造业、金融和医疗等行业。

RA Group 勒索软件是从 Babuk 勒索软件泄露的源代码中衍生出来的，采用双重勒索策略来进行攻击。RA Group 的加密器采用间歇加密，即在加密和不加密文件之间交替，以加快文件的加密速度。此外，RA Group 勒索团伙要求受害者通过 qTox ID 聊天软件与该组织进行联系。

勒索病毒小结

2023 年上半年活跃勒索家族主要有 Mallox、Tellyouthepass、Phobos 和 BeijingCrypt。

Mallox 和 Tellyouthepass 勒索家族并列第一，应急响应事件 11 起。对比去年上半年我国勒索软件应急响应事件 TOP10 家族情况，Trigona 和 Crysis 勒索家族代替 Hive 和 Magniber 成为上半年 TOP10 家族。

上半年勒索病毒攻击量排名第一的省份是广东省，其次是浙江省，攻击次数分别为 5200 万次、860 万次。其余省市攻击量相差不大，上半年受勒索软件攻击次数均超过 100 万次。

2023 年上半年我国制造业、科技和医疗等行业受勒索软件影响最为严重，勒索软件攻击占比别为 35%、24% 和 13%。教育和政府等行业也较为频繁的受到勒索软件攻击。

僵尸网络家族

僵尸网络态势

根据深信服千里目安全技术中心统计数据来看，2022 年和 2023 年 1 月 -6 月活跃僵尸网络家族如图 2-11 所示，2022 年上半年我国受到僵尸网络攻击总次数超过 22 亿次，2023 年上半年我国受到僵尸网络攻击总次数超过 10 亿次，攻击规模大幅度下降。整体来看，2023 年上半年和 2022 年上半年我国僵尸网络攻击仍以老牌僵尸网络 DorkBot 为主，2022 年上半年 DorkBot 僵尸网络占所有僵尸网络攻击的 9.1%，2023 年上半年占比 20.0%。

对比 2022 年上半年，今年上半年僵尸网络 ShellBot 攻击上升较为明显，攻击次数超过 9 千万次，ShellBot 僵尸网络于 2018 年被趋势科技安全研究人员首次披露，ShellBot 僵尸网络由 Ooulaw 组织发布，用 Perl 语言编写，可以攻击 Linux 和 Android 设备以及 Windows 系统。

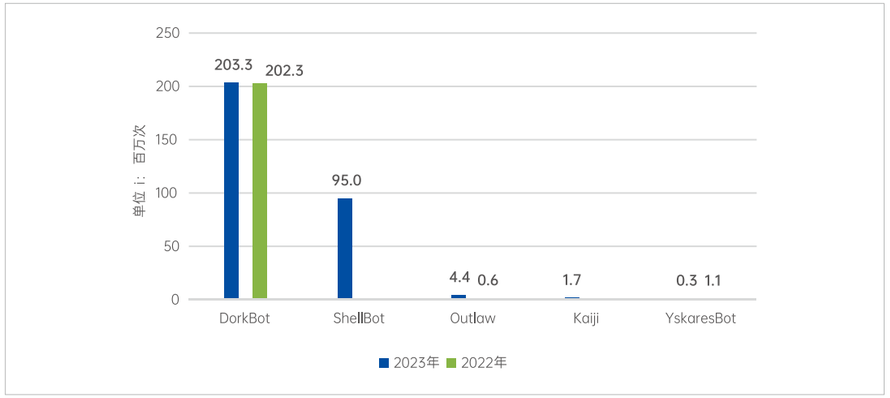


图 2-11 2022 年和 2023 年 1 月 -6 月活跃僵尸网络家族

2023 年 1 月 -6 月僵尸网络病毒攻击省份 TOP10 情况如图 2-12 所示。2023 年上半年有 5 个省市僵尸网络攻击次数超过 1 亿次，攻击量排名第一的是广东省，攻击次数高达 3.64 亿次，其次是四川省、山东省、河北省和北京市。受到僵尸网络攻击的主要行业有教育、企业、政府、医疗、能源等，占比分别为 26.9%、24.7%、23.6%、18.9% 和 3.84%。针对受到僵尸网络攻击较为严重行业和区域，需加强僵尸网络防御工作。

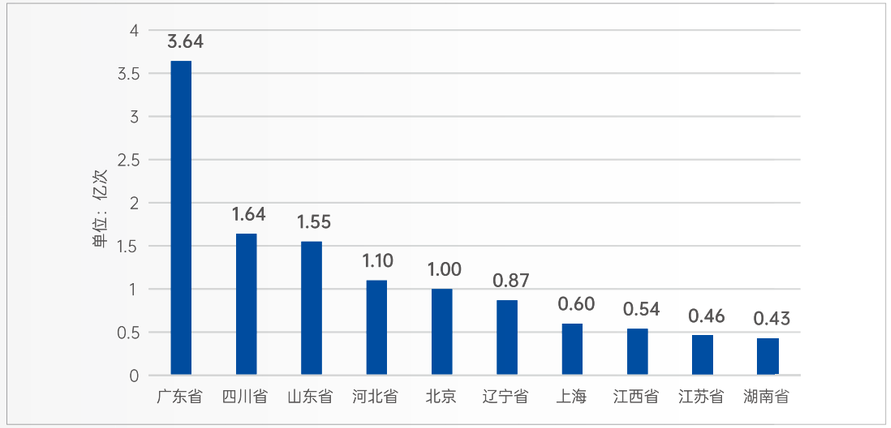


图 2-12 2023 年 1 月 -6 月僵尸网络病毒攻击地区 TOP10

在商业化恶意代码竞争激烈的环境下，网络犯罪分子将建立一个大型僵尸计算机网络，然后将僵尸网络的访问权限以出租或直接出售的形式卖给其他犯罪分子，僵尸网络攻击平均成本和技术门槛持续降低，给网络安全行业带来更严峻的挑战。提升主机安全防护能力、提高网络安全防护意识、加强应急响应处置能力，可以有效防御僵尸网络攻击，提升安全防御水平。

僵尸网络新增家族

据不完全统计，2023 年 1 月至 6 月新增了 8 个家族，如 HinataBot 僵尸网络、AndoryuBot 僵尸网络。新增僵尸网络不再局限于单一 DDoS 攻击模式，DDoS 攻击模式更加多样化。

（1）HinataBot 僵尸网络

HinataBot 是基于 Go 语言编写的 DDOS 僵尸网络，在 2023 年 1 月中旬首次出现，HinataBot 僵尸网络最高可发起 3.3Tbps 大规模 DDoS 攻击。该僵尸网络通过利用已知漏洞来攻击路由器和服务器，支持多种通信方法，包括拨出和侦听传入连接。

HinataBot 旧版本支持 HTTP、UDP、TCP 和 ICMP 等协议泛洪攻击。最新版本中，HinataBot 仅支持 HTTP 和 UDP 两种攻击模式。即使只有两种攻击模式，该僵尸网络依然进行大规模的分布式拒绝服务攻击。HinataBot 运营者正在积极更新，专注于开发逃避检测技术，以规避现有安全体系的防御措施。

（2）AndoryuBot 僵尸网络

AndoryuBot 僵尸网络于 2023 年 2 月被 Fortinet 研究人员发现，它主要是通过 Ruckus 无线管理远程代码执行漏洞 (CVE-2023-25717) 传播僵尸网络。AndoryuBot 僵尸网络主要以 Linux 平台为攻击目标，在 Telegram 上以订阅方式出售。

AndoryuBot 僵尸网络支持 12 种 DDoS 攻击模式，可以进行大规模分布式拒绝服务 (DDoS) 攻击，包含针对不同协议的 DDoS 攻击模式，并使用 SOCKS5 代理协议与命令和控制服务器通信，通过恶意 HTTP 的 GET 请求感染易受攻击的设备。

僵尸网络小结

对比 2022 年上半年，2023 年上半年我国僵尸网络攻击规模大幅度下降。2022 年上半年我国受到僵尸网络攻击总次数超过 22 亿次，2023 年上半年我国受到僵尸网络攻击总次数超过 10 亿次，整体来看，2023 年上半年和 2022 年上半年我国僵尸网络攻击仍以老牌僵尸网络 DorkBot 为主。

2023 年上半年有 5 个省市僵尸网络攻击次数超过 1 亿次，攻击量排名第一的是广东省，攻击次数高达 3.64 亿次，其次是四川省、山东省、河北省和北京市。受到僵尸网络攻击的主要行业有教育、企业、政府、医疗、能源等。

新增僵尸网络 DDoS 攻击模式更加多样化。据不完全统计，2023 年 1 月 -6 月新增了 8 个家族，如 HinataBot 和 AndoryuBot。HinataBot 支持 HTTP、UDP、TCP 和 ICMP 等多种模式 DDoS 攻击，AndoryuBot 僵尸网络支持 12 种 DDoS 攻击模式。

远控木马家族

远控木马态势

随着互联网的不断发展，远控木马的数量和种类也在不断增加和变化。根据深信服千里目安全技术中心统计数据来看，2022 年和 2023 年 1 月至 6 月活跃远控木马情况如图 2-13 所示，连续两年比较活跃的远控木马有 Gamarue、Agent、Nitol 和 Injector。其中，Gamarue、Agent 和 Injector 攻击次数相较去年有所增加，Nitol 攻击次数较去年上半年有大幅度下降。

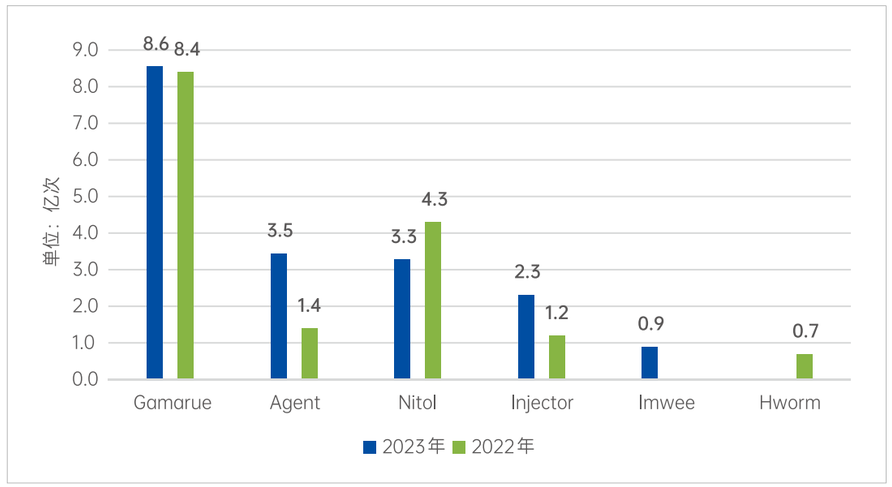


图 2-13 2022 年和 2023 年 1 月 -6 月活跃远控木马

2023 年 1 月至 6 月远控木马攻击省份 TOP10 情况如图 2-14 所示。其中，远控木马攻击量排名第一的是广东省，攻击次数为 8.9 亿次，其次是湖北省和山东省，分别为 3.0 亿次和 2.5 亿次。10 个省份上半年攻击次数均超过 1.0 亿次。

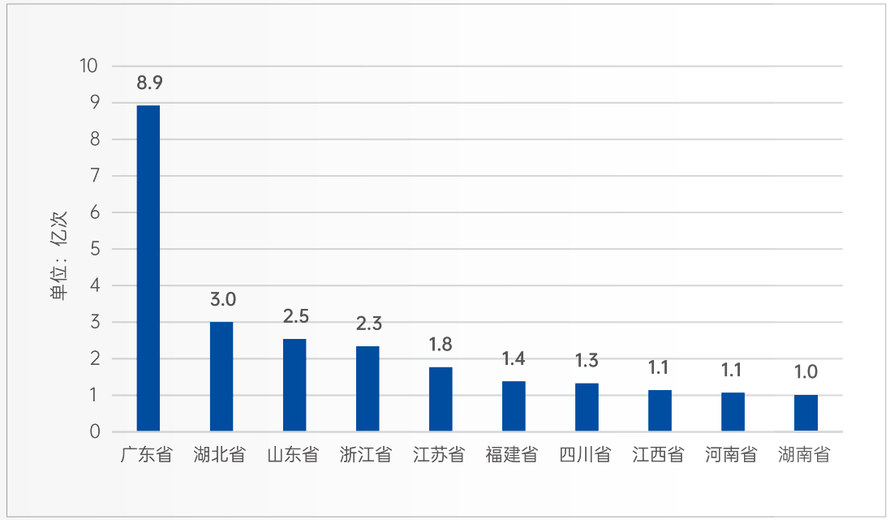


图 2-14 木马远控病毒攻击地区 TOP10

2023 年 1 月至 6 月远控木马攻击主要行业有企业、教育、医疗、政府和能源，占比分别为 49.0%、17.8%、15.3%、12.9% 和 2.9%。针对上述行业建议加强远控木马检测，使用安全软件及时查杀。

远控木马新增家族

据不完全统计，2023 年 1 月至 6 月新增了 12 个家族，如 Pikabot 和 SeroXen。Pikabot 家族利用反分析技术来规避检测，SeroXen 主要通过游戏传播。

（1）Pikabot 远控木马

Pikabot 于 2023 年年初被 Zscaler 研究人员发现，一直处于活跃状态。Pikabot 使用 C/C++ 编写，利用反分析技术来规避检测，研究人员发现当系统语言为格鲁吉亚语、哈萨克语、乌兹别克语或塔吉克语时，Pikabot 程序会自动终止。

一旦 Pikabot 感染受害者主机后，攻击者就可通过 Pikabot 来远程访问受害主机，Pikabot 还可以接收 C2 服务器命令实现进程注入、命令执行、分发其他恶意程序等操作，其主要特征为利用加载程序 / 核心组件拆分，使用 JSON+Base64+crypto 进行流量处理，并广泛使用硬编码字符串。

（2）SeroXen 远控木马

SeroXen 于 2022 年底被 AT&T 发现，并在 2023 年变得越来越流行。SeroXen 主要通过游戏进行传播，目前大多数受害者都是游戏社区的成员。

SeroXen 在逃避静态和动态分析检测方面表现良好，AT&T 在研究报告中指出，SeroXen 开发者利用免费资源开发了一种难以在静态和动态分析中检测到的 RAT，该恶意软件通过无文件攻击驻留内存中，导致一些杀毒软件无法检测到它。根据 AT&T 的分析，黑客通常是通过钓鱼邮件或 Discord 频道推送 SeroXen 进行攻击。

远控木马小结

连续两年比较活跃的远控木马有 Gamarue、Agent、Nitol 和 Injector。其中，Gamarue、Agent 和 Injector 攻击次数相较去年上半年有所增加，Nitol 攻击次数较去年上半年有大幅度下降。

2023 年上半年远控木马攻击量排名第一的是广东省，攻击次数为 8.9 亿次，其次是湖北省和山东省，分别为 3.0 亿次和 2.5 亿次。10 个省份上半年攻击次数均超过 1.0 亿次。

2023 年上半年远控木马攻击主要行业有企业、教育、医疗、政府和能源，占比分别为 49.0%、17.8%、15.3%、12.9% 和 2.9%。针对上述行业建议加强远控木马检测，使用安全软件及时查杀。

新增远控木马规避安全检测技术提升，远控木马变得更难检测。Pikabot 使用 C/C++ 编写，利用反分析技术来规避检测，SeroXen 开发者利用免费资源开发了一种难以在静态和动态分析中检测到的 RAT，该恶意软件通过无文件攻击驻留内存中，导致一些杀毒软件无法检测到它。

恶意软件攻击动态

攻击者利用 ChatGPT 技术进行攻击

攻击者使用 ChatGPT 生成恶意代码，由于技术门槛降低，使得网络攻击变得更快更容易。攻击者使用 ChatGPT 可以准确的编写出用于网络攻击的恶意代码，降低网络攻击技术门槛。Recorded Future 研究人员在地下黑客论坛上已经发现了 1500 多条关于如何使用 ChatGPT 进行恶意软件开发的资料，其中包括如何利用开源库恶意代码对 ChatGPT 进行训练来生成逃避检测的恶意代码。

攻击者使用 ChatGPT 进行网络钓鱼攻击。网络钓鱼是常见网络攻击之一，ChatGPT 的出现加剧了网络钓鱼攻击形势，ChatGPT 可以模仿人类书写方式，可以帮助相关语言写作能力不足的攻击者编写更加符合语言表达的钓鱼邮件内容。根据网络安全公司 Darktrace 公布的最新研究报告，攻击者使用 ChatGPT 等生成式 AI，使网络钓鱼邮件攻击增长 135%。过去 6 个月，诈骗电子邮件和短信的频率增加了 70%，并且 79% 的公司垃圾邮件过滤器错误地阻止了重要的合法电子邮件。

攻击者利用弱口令爆破和开源工具进行挖矿

2023 年 1 月，RapperBot 僵尸网络被发现利用 SSH 弱口令进行门罗币挖矿。其包含自删除、放置设备重启的功能，通过 SSH 弱口令爆破进行传播，RapperBot 的使用的弱口令在样本中以明文的形式出现。

2023 年 3 月，Hoze 挖矿病毒被发现用于门罗币挖矿。Hoze 挖矿病毒主要利用 SSH 弱口令暴力破解来对 Linux 平台进行攻击，并采用 SHC 工具将 shell 脚本转换为二进制可执行文件，以规避防御措施。

2023 年 4 月，韩国网络安全公司 ASEC 研究人员发现，攻击者利用 SHC 编译恶意软件进行挖矿，通过 Linux 弱口令爆破传播。当 SHC 下载器被执行时，将连接 C2 端下载获取多个恶意软件并在设备上执行。

2023 年 4 月，8220 团伙被发现利用开源工具进行门罗币挖矿，其主要采用开源工具 bdvl（Rootkit）进行辅助攻击，目的在于权限提升、抹除痕迹，并对目标进行远程访问。

攻击者利用信创系统漏洞进行勒索攻击

2023 年 5 月，Tellyouthepass 利用信创系统漏洞发起了两次大规模勒索攻击，严重威胁用户数据安全与财产安全。

用友 NC 服务器勒索攻击事件：5 月，深信服千里目安全技术中心发现国内大量主机遭受到了 Tellyouthepass 勒索攻击。攻击者利用用友 NC 文件上传漏洞和用友 NC 任意代码执行漏洞进行勒索攻击。该事件从确定受害主机到执行加密操作的时间间隔较短，且并无明显上传扫描、信息收集等黑客攻击的痕迹，勒索事件并无横向及敏感数据外发的迹象。

亿赛通文档安全管理系统攻击事件：5 月，攻击者利用亿赛通高危漏洞上传 WebShell，通过在受害者机器上部署的 WebShell 直接下发并加载勒索模块，最终，勒索软件宿主进程就是 Web 应用服务的主程序。此类攻击方法的“优点”是能够避开很多传统安全软件的检测，提高其攻击成功率。其通过 RSA+AES 两种算法实现对文件的最终加密。

恶意软件态势小结

01 **2023 年上半年恶意软件各月攻击次数较 2022 年上半年各月攻击次数均有小幅度增长，恶意软件类型分布情况没有太大变化。**2023 上半年我国遭受恶意软件攻击总次数达 147.67 亿次，比去年同时段的 138.54 亿次有小幅度上升，今年和去年的攻击高峰期均在 5 月。挖矿和远控木马攻击占比有小幅度上升，挖矿占比由 40.5% 上升到 42.9%，远控木马占比由 23.4% 上升到 26.2%。

02 **2023 年上半年受恶意软件影响较大行业有医疗、科研教育和政府等行业，影响较大区域有广东省、浙江省和上海市。**企业、医疗、科研教育和政府等行业受恶意软件攻击占比超过 80%。广东省、浙江省和上海市受恶意软件攻击均超过 10 亿次。

03 **攻击者使用 ChatGPT 生成恶意代码，由于技术门槛降低，使网络攻击变得更快更容易。**Recorded Future 研究人员在地下黑客论坛上已经发现了 1500 多条关于如何使用 ChatGPT 进行恶意软件开发的资料。根据网络安全公司 Darktrace 公布的最新研究报告，攻击者使用 ChatGPT 等生成式 AI，使网络钓鱼邮件攻击增长 135%。

04 **我国信创软件安全问题日益凸显，使勒索病毒传播加剧。**2023 年 5 月，深信服千里目安全技术中心监测到两起大规模勒索病毒攻击事件。Tellyouthepass 利用用友 NC 漏洞和亿赛通漏洞进行大规模攻击，信创安全问题日益凸显，使勒索病毒传播加剧，严重威胁用户数据安全与财产安全。

03

数据安全态势

- 数据安全治理情况
- 数据交易监控情况
- 重点数据泄露事件分析
- 数据泄露黑客论坛情况
- 勒索团伙数据泄露情况
- 数据安全态势小结

数据安全治理情况

国外数据安全治理动向

（一）生成式人工智能带来的数据安全风险凸显，多国针对此问题开展治理研究

2023 年上半年 ChatGPT 为代表的人工智能模型爆火，各大行业领域加快对人工智能在工作和生活中的应用。与此同时，人工智能交互过程敏感信息传输带来的数据风险问题受到各国的广泛关注，自 3 月 31 日起，意大利数据保护局以侵犯数据隐私为由，将 ChatGPT 禁用了一个月之久。在意大利带动下，美国、法国、德国、西班牙和欧盟等国家和组织也纷纷开始研究 ChatGPT 带来的数据安全风险问题，并在人工智能服务方面加强数据安全的监管。如，美国有参议员重新引入《人脸识别和生物识别科技暂停法案》，试图停止联邦政府使用面部识别技术，认为其有害隐私和人身自由；欧洲 ENISA 发布了《人工智能网络安全和标准化》报告；英国 ICO 更新《人工智能和数据保护指南》、 加拿大政府更新《人工智能和数据法》配套文件；国际标准组织已发布人工智能风险管理指南。

（二）数据跨境安全治理依旧是各国数据安全治理研究工作的重点

数字时代，数据已然成为国家之间争夺的重要战略资源，数据的流动是数字时代最明显的特征。在此背景下的数据跨境流动安全成为各国首要关注的问题，保护数据跨境流动安全也是保护国家基础性战略资源和国家安全的关键措施。欧美国家此前已形成了较为体系化的数据跨境管理制度，在此基础上了开展定向国家间的数据跨境流动治理研究工作。2023 年 2 月，EDPB 发布《关于欧盟 - 美国数据隐私框架充分性决定草案的意见》，该意见旨在促进跨大西洋数据的安全流动，确保了对从欧盟转移到美国公司的数据的充分保护。此外其余数据跨境制度相对不够完善的国家也在陆续开展数据跨境治理工作，如，韩国将数据跨境传输作为其 2023 年的重点工作领域。

我国数据安全治理动向

（一）我国持续深化数据安全国际合作，呼吁加强人工智能等新兴科技领域安全治理国际合作

2023 年 2 月 21 日，中国正式发布《全球安全倡议概念文件》，文件阐释了全球安全倡议的核心理念与原则，并要求深化信息安全领域国际合作。2023 年 5 月 19 日，中国 - 中亚峰会在西安开展并发布宣告称，中亚五国支撑中方已提出的《全球数据安全倡议》，希望推动达成反映各方意愿、尊重各方利益的全球数字治理规则，共同持续推进落实《中国－阿拉伯联盟数据安全合作倡议》和《“中国 + 中亚五国”数据安全合作倡议》，共同应对各类网络威胁，构建开放包容、公平合理、安全稳定、富有生机活力的全球网络空间治理体系。在人工智能、智慧城市、大数据等新兴科技领域加强国际安全治理合作，共同预防和管控潜在安全风险。

（二）数据安全产业发展规划形成，从七大重点任务着手推动我国数据安全走向繁荣成熟阶段

2023 年 1 月 13 日，工业和信息化等十六部门联合发布《关于促进数据安全产业发展的指导意见》，制定了到 2025 年数据安全实力明显提升和到 2035 年进入繁荣成熟期的发展目标，提出了以实现提高产业创新能力、壮大数据安全服务、推进标准体系建设、推广技术产品应用、构建繁荣产业生态、强化人才供给保障、深化国际合作交流的 7 大重点任务。

（三）行业监管大力推动各地方数据安全管理落地，开展建设典型案例已见成效

2023 年 1 月 1 日，《工业和信息化领域数据安全管理办法》正式实施，重点解决行业内数据安全监管责任和机制，以数据分级分类为原则，要求加强各级别数据的不同稍微安全管理和重点保护。2023 年 2 月 27 日，工业和信息化部办公厅公布工业领域数据安全管理试点典型案例和成效突出地区，确定 29 个工业领域数据安全管理试点典型案例和 5 个试点成效突出地区，以推动全国各地区数据安全管理工作。2023 年 3 月，证监会发布《证券期货业网络和信息安全管理办法》，对网络和信息安全管理提出规范要求，明确提出建立健全投资者个人信息保护体系和管理机制。2023 年 7 月 24 日，为加强中国人民银行业务领域数据安全管理，央行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》（下称《办法》），并向社会公开征求意见。工业和信息化领域和金融领域作为率先推动数据安全管理工作的行业，为其他行业的数据安全管理工作推动起着积极的影响作用。

（四）我国数据跨境安全治理体系持续完善，数据出境安全评估制度已成功落地

2023 年 2 月 24 日，国家互联网信息办公室公布《个人信息出境标准合同办法》，自 2023 年 6 月 1 日起施行。该办法为个人信息处理者向境外提供个人信息的活动提供了规范指引，对《个人信息保护法》中“个人信息跨境提供规则”进行细化落实，成为数据跨境安全治理体系中的重要一环。为为了指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同，国家互联网信息办公室编制了《个人信息出境标准合同备案指南（第一版）》，对个人信息出境标准合同备案方式、备案流程、备案材料等具体要求作出了说明。在数据出境安全评估方面，自《数据出境安全评估办法》施行，各地区快速开展数据出境安全评估工作。2023 年 1 月 18 日，北京市首都医科大学附属北京友谊医院与荷兰阿姆斯特丹大学医学中心合作研究项目取得数据合规出境重要突破，完成全国首个数据合规出境案例，而后多地多个行业的案例陆续落地，为后续的数据出境安全评估工作打下了有力基础。

数据交易监控情况

黑灰产交易类型分布

Tor、Freenet、ZeroNet 等地下网络空间，以及 BTC、XMR 等加密货币的匿名性改变了黑客地下市场生态。这些技术的匿名性为黑客提供了天然的保护伞，让黑客可以在更灵活和安全的平台环境下交流与合作。从监控数据来看，黑客市场非法交易规模逐年增大。随着数字经济推动和加密货币的发展，越来越多的黑客在利益驱动下实施非法交易。在我国的网络监管打击下，网络非法交易场所主要转移到了境外社交平台、境外黑客论坛市场以及暗网交易市场中。

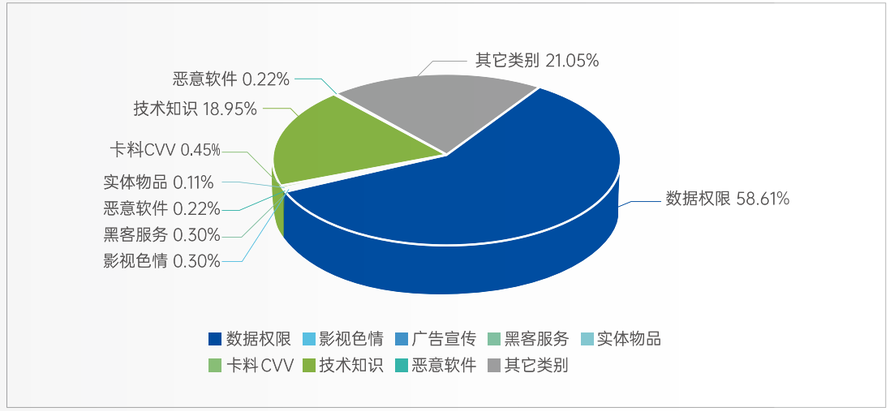


图 3-1 黑灰产交易情报类型分布

深信服千里目安全技术中心对黑灰产交易市场（包括境外社交平台、黑客论坛市场以及暗网市场）进行监控发现，2023 年 1 至 5 月新增约 89753 条涉及我国的交易情报，这些情报的交易类型分布如图 3-1 所示，其中数据权限的交易类型占比高达 58.61%，是黑灰产市场中最主要的交易内容，其中主要包括重要账号凭证、API 接口权限、网络访问权限、个人敏感信息、企业隐私数据等等，该类型情报具有明显的高价值特点，是黑客进行数据窃取的主要原因。

重要数据泄露发现渠道分布

深信服千里目安全技术中心持续监控黑灰产交易市场，对其中高价值情报进行快速发现和分析，2023 年上半年累计发现涉及我国的重要数据泄露事件一百多起，针对其中事件发现渠道进行统计分析，如图 3-2 所示，境外黑客论坛泄露数量占比高达 43%，主要是 BreachedForums 论坛；中文暗网交易市场以售卖我国历史泄露数据为主，上半年在预警事件中的来源占比为 41%；Telegram 频道中主要以传播以上两个渠道已泄露的数据居多，首发来源于 Telegram 的数量偏少，但价值会普遍偏高。从泄露数据影响程度和真实性综合评估来看，三个来源的情报重要性呈现趋势为，黑客论坛 >=Telegram> 中文暗网交易市场。

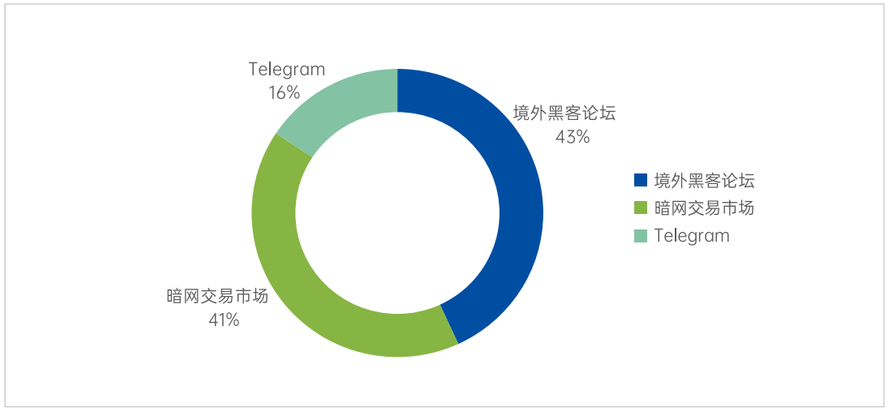


图 3-2 我国重要数据泄露事件发现渠道分布

重要数据泄露影响行业分布

根据深信服千里目安全技术中心 2023 年上半年监测发现，重要数据泄露事件影响行业分布占比由高到低分别为政府、企业、教育、医疗和运营商，如图 3-3 所示，政府和教育行业一直是数据泄露的重灾区，2023 年上半年这两个行业数据泄露占比高达 60%。

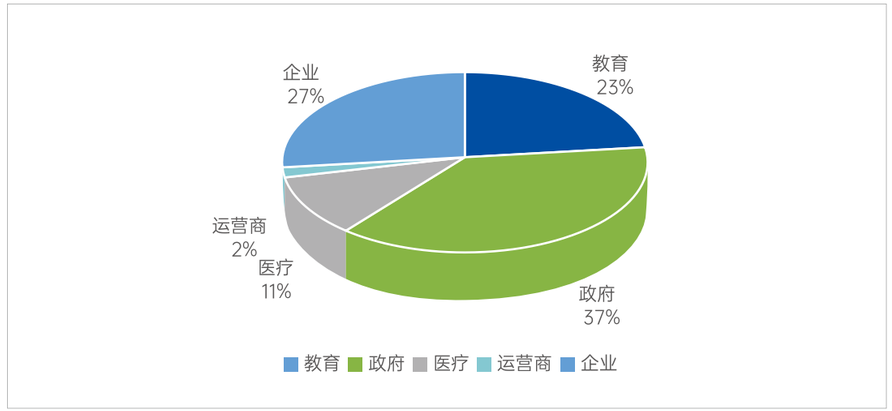


图 3-3 我国重要数据泄露事件影响行业分布

重点数据泄露事件分析

大量个人地址泄露

个人信息是最具价值的数据，也是当前泄漏最严重的数据类型。其中，今年个人地址泄露事件引发广泛关注，涉及大量地址数据的快递物流行业的数据安全问题引起重视，其信息查询的上下游供应链复杂，安全能力参差不齐，使得数据安全的保障难上加难。

接口滥用导致敏感数据泄露

API 接口滥用是当前各行业数据泄露的最主要原因。在上半年观察到多起黑客利用开放接口提供非法数据查询服务或非法爬取数据进行售卖的数据泄露事件。大量黑客紧盯政务、医疗、教育等公共服务行业对外提供的服务接口，通过利用 API 接口的安全漏洞，编写调用程序和爬取程序获取接口返回数据达到获取敏感数据的目的。

黑客论坛中的数据泄露

黑客论坛是黑客活动和交流的主要根据地，黑客在攻击目标单位并窃取数据之后往往会将成果挂在黑客论坛中进行售卖，在获取经济利益的同时还能通过此行为在黑客论坛中打造名气和排名，形成了一个黑客活动社群。今年据观察发现，黑灰产市场的动荡影响着数据泄漏事件的发生，论坛运营者通过公开泄露黑客们关注的数据来进行宣传和竞争，使得泄露数据的事件频繁发生，其中多次泄露数量高达上亿条。

数据泄露黑客论坛情况

从 2021 年起，RaidForums 黑客论坛的崛起，使利用黑客论坛泄露我国数据的情况大幅度增多，尤其是以 AgainstTheWest 为代表的黑客组织在攻击我国大量单位并窃取数据后，使用黑客论坛公布成果并售卖数据以增加影响力。除了针对我国的数据泄露，黑客论坛还涉及全球各国黑灰产交易，各国监管持续打击并逮捕了 RaidForums 黑客论坛运营者，之后出现 BreachedForums 以替代 RaidForums 黑客论坛，成为 2022 至 2023 年的顶级黑客论坛，2023 年 3 月 BreachedForums 也被 FBI 打击并关闭。此后，我们陆续观测到多个黑客论坛的出现和频繁活动，意图顶替 BreachedForums 论坛成为新一代顶级论坛，而这一现象促使 2023 年上半年的数据泄露事件持续增多。对黑客论坛的跟踪和监控是快速掌握我国数据泄露事件发生的有效手段，以下将围绕 2023 年上半年数据泄露相关黑客论坛的发展情况和详细信息盘点。

黑客论坛发展态势

BreachForums 是 2022 至 2023 年期间的顶级黑客论坛。2022 年 3 月，在 RaidForums 下线三周后，在 RaidForums 上非常活跃的黑客 Pompompurin 决定用替代论坛 BreachForums 取代 RaidForums 黑客论坛。在成立的半年内，BreachForums 再次发展成为最受欢迎的黑客讨论平台之一，泄露数据的交易是该论坛的主要内容。2023 年 3 月 20 日，BreachForums 在其管理员 Pompompurin（真名 Conor Brian Fitzpatrick）被捕后关闭，随后另一管理员 Baphomet 声称执法部门已经获得了对论坛服务器的访问权限，并最终决定关闭该论坛。

此后，在 BreachForums 的用户开始向新的论坛转移，一是向本就存在的其他流行黑客论坛转移，例如 XSS、Exploit、Cracked、Nulled 等；二是涌入新出现的意图替代 BreachedForums 的新论坛。而现有论坛大多有较为严格的会员制度，使用门槛和宣传门槛较高，导致黑客们积极寻求新论坛扎根的现象更多。在这一现象的驱动下，不乏有想要成为新一代顶级黑客论坛的运营组织，目前已观测到多个类似于 BreachedForums 的新论坛出现。

流行黑客论坛

XSS 论坛

这个以俄语为基础的黑客论坛由俄罗斯管理员运营，其主要用户群是俄语使用者。该论坛需要注册账号并通过管理员审核才可使用和查看。它包括有关俄罗斯网络犯罪分子、针对俄罗斯的网络攻击或俄罗斯针对俄罗斯威胁行为者和俄罗斯论坛采取的措施的对话。该论坛还主要支持俄罗斯的政治立场，这一点在俄罗斯和乌克兰之间的战斗开始时就变得非常明显。如今，XSS 被认为是俄语社区中最著名、最专业的黑客论坛之一。

XSS 上存在多个 APT 和勒索软件组织活动，包括 Lockbit、REvil、Avoslocker、EternityTeam、Babuk、Darkside 等。XSS 还被用作与黑客和金融欺诈相关的非法数字商品的交易平台，例如泄露的数据库、定制恶意软件、黑客工具、漏洞。在 BreachForums 关闭后不久，有用户将已关闭的 BreachForums 和 RaidForums 论坛中的文件列表在 XSS 论坛中发布。

Exploit 论坛

Exploit 是运行时间最长的地下黑客论坛之一，早在 2005 年就已推出。顾名思义，该网站的最初目的是为恶意行为者提供一个讨论各种漏洞的有效利用的场所。漏洞利用自然演变为涵盖有关其他类型网络犯罪活动的讨论，从社会工程技术到破解密码算法的教程。该论坛主要是俄语论坛，其中有一个市场部分，网络犯罪分子在此交易被盗的信用卡详细信息、恶意软件，甚至零日漏洞。

而该论坛需要付费 100 美元才可以访问，或者通过一系列条件才可免费访问，通过这些条件该论坛成为了一个封闭的优质论坛。

RAMP 论坛

RAMP 2.0（俄罗斯匿名市场）论坛于 2021 年成立，该论坛是在臭名昭著的勒索软件团伙 Babuk 之前使用的域名上搭建的。RAMP 的早期版本于 2012 年至 2018 年搭建在其他域中，它更侧重于买卖非法产品。俄罗斯执法部门关闭了 RAMP 的第一版，但出现了一个专注于网络犯罪的新版本。其中受黑客欢迎的论坛部分包括勒索软件团伙的合作伙伴计划、恶意软件部分以及专门出售系统访问权限。

注册 RAMP 2.0 需要成为 Exploit 和 XSS 的活跃成员至少两个月。在这两个论坛上的良好声誉对于进入 RAMP 也至关重要。该论坛的语言选项已从仅有俄语发展到现在包括普通话和英语。

Nulled 论坛

Nulled 是一个著名的黑客论坛，于 2015 年推出，拥有 450 万用户和超过 3500 万个帖子，涉及破解程序、数据库转储、被盗帐户、黑客工具和漏洞以及黑客教程。该论坛于 2016 年遭到黑客攻击，其数据库（包括 PayPal 电子邮件地址、政府域名电子邮件、密码、购买记录和发票）被泄露后，它成为媒体关注的焦点。执法部门利用这一漏洞追踪在 Nulled 上注册的黑客和网络犯罪分子，但 Nulled 克服了这次攻击，目前 Nulled 是已知最大的各种非法内容论坛之一，内容涵盖泄密、渗透测试和赚钱诈骗等。该论坛不需要注册和登录即可查看其中的内容。

新增黑客论坛

LeakBase 论坛

ARES 威胁组织于 2023 年 4 月 9 日推出了一个名为 LeakBase 的新黑客论坛。该论坛提供免费数据库、交易被盗数据的市场以及用于建立信任的托管支付系统。它还包括黑客相关主题的各种讨论区，例如编程、技巧、教程和绕过安全措施的方法。该论坛的推出正赶上 BreachForums 黑客论坛关停，不少用户进入 LeakBase，其泄露活动明显增加。ARES 被认为正在利用 BreachForums 的关闭来加速其增长并确立其在市场中的地位。

Exposed 论坛

该论坛是在 BreachForums 关闭后第一个声称替代并沿用 BreachForums 论坛结构的新论坛。2023 年 5 月 9 日该论坛运营者之一在 telegram 中进行宣传其论坛，称 Exposed 论坛为 BreachForum 的替换论坛，该论坛本身由一个名为 Impotter 的用户管理。他宣布了该论坛的新功能和政策，该论坛在运营不到两周的时间内就已经拥有约 2000 名用户。另一位运营者 Purism 开始通过公开泄露其他黑客论坛的基础设施和后端服务器信息来扩大自身影响力，目前已泄露多个论坛信息。

截止目前其论坛已停止运营，该论坛运营者称其没有尽力再运营该论坛，并寻求新论坛运营者。

RAID FORUM

该论坛为 2023 年 4 月成立的一个新的黑客论坛，其名称类似于 2022 年 4 月关闭的 RaidForums 论坛，但没有迹象表明新论坛的管理员与前者有任何联系。该论坛包含各种类别，包括有关黑客攻击和泄密的讨论，以及市场和教程部分。自 2023 年 4 月 9 日上线以来，截至目前，论坛已累计会员 1725 人。

BreachForums（新）

该论坛于 2023 年 6 月 12 日出现，其名称类似于 2023 年 3 月关闭的 BreachForums 网站并且其架构也一模一样，该论坛于 exposed 论坛关闭后出现，该论坛运营者 ShinyHunters 发布公告称该论坛运营 团队为曾经关闭的 BreachForums 原始团队，并称可以通过给管理员发消息恢复在此前关闭论坛中的排名。截止 6 月底，该论坛已拥有 6 千多名会员和 2 万多篇帖子。

勒索团伙数据泄露情况

勒索软件已是全球数据泄露的头号威胁，2022 年全球范围内遭到勒索软件团伙公开泄露数据的组织共 2861 家，其中 TOP10 的勒索软件依次为 LockBit、BlackCat(ALPHV)、BlackBasta、Conti、karakurt、Hive、ViceSociety、BianLian、Royal、Quantum。而 2023 年随着国际上监管对勒索软件团伙的打击，勒索软件团伙的活跃度不断变化，曾经活跃团伙销声匿迹，新的勒索团伙持续涌现。

勒索团伙数据泄露数量趋势

2023 年 1 月至 6 月期间，深信服千里目安全技术中心累计发现 2200+ 被公开泄露数据的受害组织，其中涉及中国的共 31 起，2023 年上半年勒索团伙数据泄露数量趋势如图 3-4，其总量与 2022 年同比增长约 62.5%。

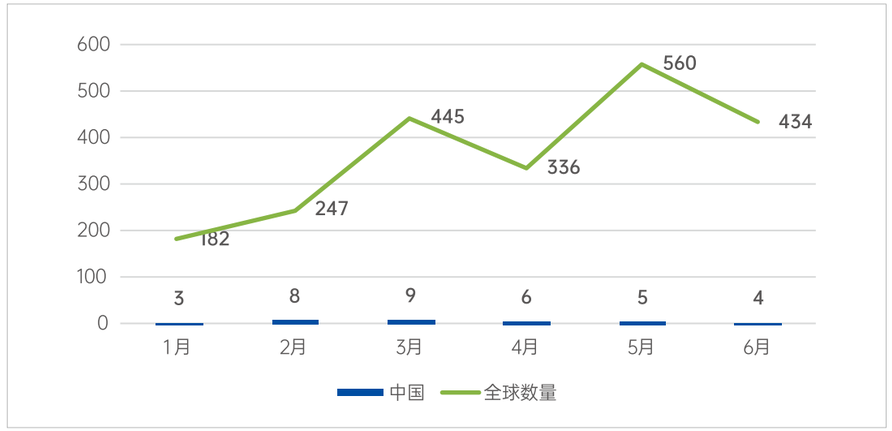


图 3-4 2023 上半年勒索团伙数据泄露数量趋势

多重勒索软件团伙活跃排行

以勒索软件团伙维度统计，如图 3-5 所示，2023 年上半年以数据泄露实行多重勒索的勒索软件团伙 TOP10 依次为 LockBit、BlackCat(ALPHV)、Malaslock、CL0P、Royal、BianLian、PLAY、8BASE、BlackBasta、Medusa。 与 2022 年的活跃排名对比，Malaslock、CL0P、PLAY、8BASE、Medusa 这 5 个团伙是 2023 年新上 TOP10 的活跃团伙，其中 Malaslock、8BASE 是 2023 年首次出现的新勒索软件团伙，首次出现并伴随着密集的攻击活动，跻身于多重勒索软件团伙活跃度 TOP10 之中。

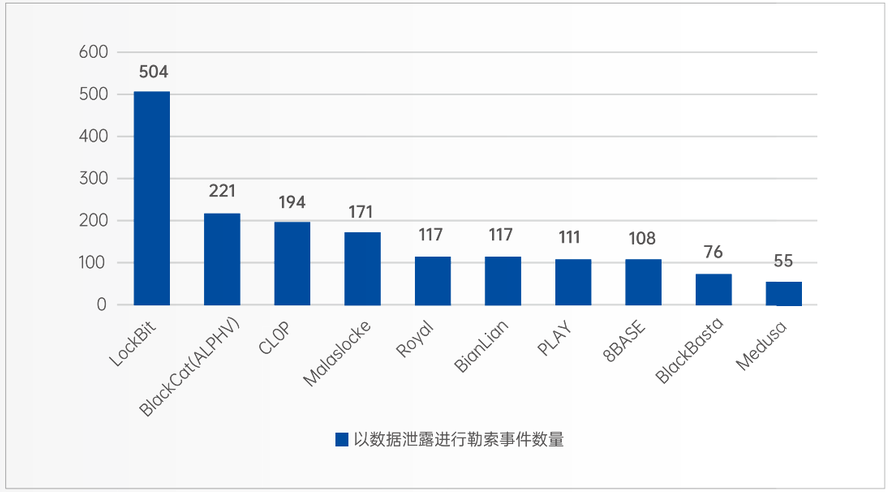


图 3-5 2023 上半年多重勒索软件团伙活跃排行 TOP10

新活跃多重勒索团伙

MalasLocker

MalasLocker 是双重勒索团伙中，他们不要求赎金，而是要求受害者捐款。2023 年 3 月，该勒索团伙出现，开始针对 Zimbra 服务器进行攻击。该勒索软件似乎使用了由著名密码学家 Filippo Valsorda 开发的 Age 加密工具。该工具相当简单，但有效，并且支持各种加密算法，包括 HMAC-SHA256、X25519 和 CharChar20-Poly1305。该组织在勒索信中提到“与传统的勒索软件团体不同，我们不会要求您向我们汇款。我们只是不喜欢公司和经济不平等。我们只是要求您向我们批准的非营利组织捐款。这是双赢的，如果你愿意的话，你可能可以从你的捐赠中获得减税和良好的公关。”

从 2023 年出现以来 MalasLocker 已经攻击 170 多家企业，跻身成为 2023 上半年双重勒索排行第四的团伙。

CL0P

CL0P 勒索软件于 2019 年初出现，与 TA505 威胁组织相关。2021 年 6 月，乌克兰、韩国和美国执法机构联手逮捕了 6 名涉嫌参与 CL0P 勒索软件团伙的人员。自此之后，CL0P 的活跃度大大减少。在沉寂近两年后，CL0P 勒索软件在 2023 年再度活跃，在今年的攻击活动中利用 Fortra GoAnywhere MFT 安全文件共享解决方案中存在的 0day 漏洞，该组织声称他们利用该漏洞在十天内窃取了 130 家公司的数据，其中包括日立能源、西门子能源、加州大学洛杉矶分校。

Cl0p 勒索软件在加密受害者的文件后使用“ .clop ”扩展名。该病毒的一个独特特征是其在勒索字条中留下的字符串“Don’t Worry C|0P”。该勒索软件会尝试禁用 Windows Defender 并删除 Microsoft Security Essentials 以避免检测。

2023 年上半年该组织利用 0day 快速攻击了 190 多家组织，成为上半年活跃度排行第三的双重勒索团伙。

8BASE

2023 年 5 月，8BASE 勒索团伙密集泄露 67 名受害者数据，体现出较为突出的高活跃度，在 2023 上半年总共攻击 108 家组织，成为双重勒索团伙活跃排行第七的勒索团伙。8Base 勒索软件通过多种方式传播，包括网络钓鱼电子邮件、偷渡式下载和漏洞利用工具包。根据 VMware 的威胁分析师的分析来看，该组织在勒索字条、泄露网站的欢迎页面、服务条款页面和常见问题解答页面与 RansomHouse 勒索团伙具有相同的语言和写作风格，而在勒索样本的使用上，8Base 使用了加载 SmokeLoader 的 Phobos 2.9.1 版本，并通过在加密文件中附加‘.8base’来添加自己的品牌定制，但整个附加部分的格式与 Phobos 相同，包括 ID 部分、电子邮件地址和文件扩展名。

数据安全态势小结

01 **人工智能技术带来的数据安全风险问题成为全球关注新热点。**以 ChatGPT 为代表的人工智能技术在2023年爆火，生成式人工智能在数据处理、代码审阅、材料生成上都体现出了让人们惊叹的能力，随即该项技术被快速应用于各企业中。然而在与人工智能进行交互的过程中敏感数据和隐私内容传输所带来的数据安全风险也成为了新技术场景下需要重点关注和治理的问题。目前多个国家已着手针对此问题进行研究并推出了多项政策进行治理。

02 **数据接口的安全问题是当前导致数据泄露最主要的原因，上半年个人地址信息泄露引发广泛关注。**政务、医疗、教育行业的数字化数据接口的利用既不需要获取系统最终权限，也不需要复杂的攻击绕过，只需要通过发现已存在的系统暴露接口，编写可利用程序即可调用该接口获取敏感数据。

03 **黑客论坛之间的竞争导致上半年数据泄露事件增加，历史已泄露数据再次遭到泄露。**尽管各国持续打击这些组织，但泄露的渠道依旧如雨后春笋般涌出，这些论坛都想代替曾经的 breached 成为新一代数据泄露论坛，运营者以泄露高价值数据的方式吸引黑客们关注和驻足来达成目的，而该行为将持续加大数据泄露的风险。

04 APT攻击态势

- APT 攻击活动态势
- APT 攻击流行技术趋势
- 典型 APT 攻击事件
- APT 攻击态势小结

APT 攻击活动态势

APT 组织攻击总体态势

2023 年上半年，根据深信服千里目安全技术中心检测发现南亚、东亚、东欧地区的 APT 组织尤为活跃。

南亚地区 APT 组织以 CNC、BITTER（蔓灵花）、Patchwork（白象）、Conficius（摩罗粆）、SideWinder（响尾蛇）、Donot（肚脑虫）为代表持续对中国、巴基斯坦等南亚周边国家进行长期窃密的攻击活动。其中 CNC、BITTER、Patchwork 组织活动在 2023 年上半年尤为频繁猖獗，这几个 APT 组织很多方面信息存在着交叉，包括但不限于基础设施、攻击手法与战术、相似样本等，不排除这些组织背后存在一定关联性。其目标行业主要集中在教育、航空工业、科研单位、军工、政府等行业。

东亚地区以地缘政治为主要因素的绿斑是活跃 APT 组织代表，其保持长期对我国进行定向钓鱼攻击，持续对我国军工、科研教育、航空航海等技术情报进行窃取。除此之外，Lazarus 和 Kimsuky 对我国的攻击倾向较弱，其重点目标在美国、日本、韩国等地。

东欧地区持续受俄乌战争影响，APT 攻击一直保持高度活跃状态。俄罗斯背景的 APT 组织持续对乌克兰地区的关键信息基础设施进行打击，在情报窃取上，重点倾向在外交情报上。

除以上三个地区外，来自北美的 APT 攻击一直保持对全球范围的攻击，在今年上半年俄罗斯披露美国情报机构利用苹果设备对其俄罗斯境内数千部手机进行情报窃取，其中还包括俄罗斯外交官员，此外包括以色列、叙利亚和中国都在此次监控范围内。

南亚活跃 APT 组织态势

2023 年上半年，深信服千里目安全技术中心监测到了大量疑似南亚地区 APT 组织的相关攻击活动，活跃组织包括 CNC、BITTER（蔓灵花）、Patchwork（白象）、Conficius（摩罗粆）、SideWinder（响尾蛇）、Donot（肚脑虫）等，其中 CNC、BITTER、Patchwork 组织活动尤为频繁猖獗，这几个 APT 组织很多方面信息存在着交叉，包括但不限于基础设施、攻击手法与战术、相似样本等，不排除这些组织背后存在一定关联性。其目标行业主要集中在教育、航空工业、科研单位、军工、政府等行业，各个活跃组织侧重目标稍有不同。值得注意的是近期高度活跃的南亚 APT 组织活动均出于窃密动机，表 4-1 是 2023 上半年南亚高度活跃 APT 的组织基本信息。

组织名称	目标行业	目标国家	攻击动机	目标平台
CNC	航空航天、水利、教育、军工	中国、巴基斯坦、菲律宾、印度尼西亚	间谍行为、数据窃取	Windows
白象	政府、外交、军事、电力	中国、巴基斯坦	间谍行为、数据窃取	Windows、Android
蔓灵花	政府，航空航天，科研机构，军队，国防，核工业，海运，船舶	中国、巴基斯坦、孟加拉国、沙特阿拉伯、新加坡、马来西亚、斯里兰卡、尼泊尔	间谍行为、数据窃取	Windows、Android

■表 4-1 2023 上半年南亚活跃 APT 组织信息

CNC

CNC 组织最早于 2019 年被发现，因其使用的远程控制木马的 PDB 路径信息中包含的 "cnc_client"，该组织被命名为 CNC。该组织主要针对军工、教育、科研机构及航空航天等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等，并且该组织疑似与南亚 APT 组织 Patchwork（摩诃草、白象）存在一定关联。

2023 年上半年，在攻击目标上，CNC 频繁向境内科研院所、航空航天、教育行业发起攻击，其中包括某具有一流科学家和科技队伍的国立科研机构、重点实验室、国家级别工程研究中心，以及某双一流大学的高新科技专业实验室。

攻击载荷上，攻击者至少使用“学术交流”、“科学研究”或“文章出版”等四种伪装程度极高的邮件话术进行鱼叉式钓鱼邮件攻击，受害者运行攻击者提供的程序后，下载后续阶段远控、反弹 shell、浏览器窃密、文件窃密、U 盘摆渡木马等恶意程序，攻击者最终可成功窃取、并持续监控受害者机器上的文档文件。

攻击手法上，CNC 组织在初始打点阶段常使用高度定制的鱼叉式钓鱼攻击，在代码执行和持久化阶段也有诸如反自动化分析、证书伪造等大量防御对抗技巧。

白象

白象最早由国外安全厂商 Norman 披露并命名为 Hangover，在 2015 年的攻击行动被国外安全厂商 Cymmetria 披露为 Patchwork，2016 年其他厂商后续披露了该组织的详细报告，在国内有“白象”称呼。其主要针对 Windows 系统进行攻击，同时也会针对 Android、Mac OS 系统进行攻击。以鱼叉攻击为主，以少量水坑攻击为辅，针对目标国家的政府、军事、电力、工业、外交和经济进行网络间谍活动。

2023 上半年，白象组织活动大多集中在我国境内中部地区，攻击目标上，对多个涉及水利、航空等专业的高等院校发起鱼叉式钓鱼攻击。攻击者疑似先攻击了某大型水利集团，窃取了其内部相关信息和物料，然后再使用包括招聘信息、职场性骚扰事件通报、年度专项项目申报在内的多个主题的钓鱼邮件，向高校内投递了大量钓鱼邮件。除此之外该组织还对某政府气象机关单位发起攻击，窃取了大量相关数据。

攻击手法和工具上，白象常使用鱼叉攻击对目标进行打点攻击，在近期监控到的攻击活动中发现有大量针对中国的定制化攻击工具，同时该组织对以往披露的 BADNEWS 攻击组件也有一定程度的更新，不断加强其窃密、反分析及反取证能力。

蔓灵花

BITTER 组织，又被称“蔓灵花”、“APT-C-08”、“T-APT-17”以及“苦象”，是一个针对中国、巴基斯坦以及孟加拉等国家的 APT 组织。最早由国外安全厂商 Forcepoint 于 2016 年披露其针对巴基斯坦官员进行网络间谍攻击，通过进一步分析，发现该组织于更早的时间 2013 年就开始进行了网络攻击，各个安全公司以及安全团队分析得出其为印度背景的 APT 组织。在此后多年，BITTER 组织常对中国、巴基斯坦等国家发起网络攻击，常针对政府（外交、国防）、核工业、国防、军工、船舶工业、航空工业以及海运等行业进行攻击。该组织的历史活动在 2016 年至 2020 年都十分活跃，

自 2020 年初 COVID-19 病毒流行起来，该组织的活跃程度有所降低，但 2021 年至 2023 年该组织频繁活动又有死灰复燃之势。

攻击手法上，自 2021 年以来，该组织的攻击手法一直都没有发生大的变化，其攻击活动基本依赖于社会工程学，通过鱼叉攻击投递恶意载荷或者进行凭证钓鱼（主要是邮箱），其针对国内的鱼叉攻击使用的邮箱账号多为窃取或购买的 126、163 邮箱，针对国外机构多使用窃取的政府邮箱或 gmail 邮箱，基本上都是通过其投递恶意 chm 文件，诱导目标执行该文件创建恶意计划任务下载第二阶段载荷，命令行使用字符“^”进行混淆，创建计划任务下载执行第二阶段载荷。

攻击载荷上，该组织投递的恶意载荷种类较多，存在使用 chm 文件、远程模板注入文档、lnk 文件以及 winrar 自解压程序等多种方式。恶意载荷通常使用 msi 部署或直接下载该组织特有下载器，再通过下载器下载其他功能组件包括但不限于远控、文件窃密组件以及键盘记录器等黑客工具，虽然其攻击方式依赖社会工程学，但还是发现许多组织或企业被攻击成功。

2023 上半年蔓灵花组织的攻击目标涵盖政府、航天、核工业、军工、船舶、外贸、教育，涉猎十分广泛，国外也有多家厂商对其攻击活动进行了披露。在最新的攻击活动中，监测到其使用新的组件进行攻击，该组织利用 DarkAgent 开源项目对远控组件进行二次修改开发和混淆，还发现该组织将开源项目“Lilith”与以往的下载器结合，以不断增强攻击组件的反分析能力。此外，上半年在蔓灵花对巴基斯坦的攻击中发现，其攻陷的载荷托管点都为 WordPress 站点，由此预测接下来蔓灵花组织将会长期攻陷目标境内 WordPress 站点以部署载荷托管中心。

东亚活跃 APT 组织态势

东亚地区以地缘政治为主要因素以绿斑为活跃代表保持长期对我国的定向钓鱼，持续对我国军工、教育科研、航空航海等技术情报进行窃取，其手法常年保持钓鱼网页和邮件攻击。Lazarus 和 Kimsuky 公认具备东北亚政府背景，其对我国的攻击倾向较弱，其攻击目标重点在于美国、日本、韩国等地。

组织名称	目标行业	目标国家	攻击动机	目标平台
Lazarus	政府，媒体，商贸机构，军队，金融	美国，韩国，墨西哥，巴西，智利，尼日利亚，加蓬，印度，中国台湾，马来西亚	间谍行为，网络经济犯罪	Windows、Android
Kimsuky	政府	韩国，日本，俄罗斯联邦，越南，中国	间谍行为	Windows、Android
绿斑	政府，航空航天，媒体，医疗，科研机构，金融，国防，船舶，能源，外交，军工，智库	中国	间谍行为，数据窃取，系统破坏	Windows、Android

表 4-2 2023 上半年南亚活跃 APT 组织信息

Lazarus

Lazarus 被公开情报普遍认为具有东亚某国政府背景，其作为该地区的一个庞大 APT 组织集团，其下还存在多个子组织，进行分工协作。其攻击目标遍及全球，攻击行业多种多样，包括但不限于数字货币、金融机构、IT 公司、政府机构以及军事机构等，其“初始打点”阶段主要利用社会工程技术，通过邮件、推特、领英、脸书以及 whatsapp 等社交媒体向目标发送恶意文件或链接，诱导目标执行恶意文件或引导目标至漏洞网站、虚假网站触发对应的漏洞利用实现恶意文件植入。

在披露的攻击活动中，Lazarus 组织在漏洞积累以及利用方面一直展现出较为先进的研究能力，曾利用 chrome 远程代码执行漏洞子“CVE-2022-0609”对多国的新闻媒体、IT 基础设施服务商进行攻击。在 2023 年的攻击活动中发现除了先前被利用的 INISAFE CrossWeb EX 和 MagicLine4NX 之外，还新确认了 VestCert 和 TCO!Stream 的 0day 漏洞被利用，且利用 BYOVD 技术进行横向移动。

除此之外，该组织近年来紧盯供应商，多次利用供应链攻击进行活动，2021 年 Lazarus APT 组织通过在 VS 项目中设置预构建事件命令，进行基于软件开发工具相关的供应链攻击，目的是为了定向盗取安全研究人员的 0day 漏洞等。2023 年 4 月，Mandiant 将 3CX 双重供应链攻击活动被归因为 UNC4736 组织并认为该组织与北韩有联系，该组织隶属于 Lazarus。2023 年 7 月，GitHub 发现 Lazarus 利用包含恶意 npm 依赖项的软件的 GitHub 存储库以攻击加密货币、在线赌博和网络安全行业的开发人员。Lazarus 可能会越来越多地使用供应链攻击以获得对目标网络的初始访问权限。

Kimsuky

该组织是比较活跃的东亚组织之一，其又名 Mystery Baby、Baby Coin、Smoke Screen、BabySahrk，据分析其可能为从 2012 年开始活动与东亚某国政府有关的 APT 组织，其与 Konni 组织疑似存在联系，该组织的攻击手法并没有太大的变化，主要还是采取发送携带“外交”、“安全”、“国防”、“朝鲜核问题”以及“统一部”等关键字的恶意附件对目标发起鱼叉攻击。自 2022 年 10 月，该组织被发现使用移动恶意软件来攻击 Android 设备并不断对移动设备进行攻击，以窃取目标信息，并尝试通过修改开源 RAT Androspy 来避免检测，与 FastViewer 类似的复杂攻击向量用于攻击指定目标，并利用现有的开源代码来产生高性能变体，Kimsuky 组织的移动端的攻击技巧变得越来越精进，因此对针对 Android 智能手机或设备的复杂攻击保持谨慎非常重要。

在 2023 年 5 月，Kimsuky 组织利用 ReconShark 新恶意软件组件开展全球范围的间谍活动继续围绕各种正在进行的地缘政治主题。例如，最新的重点关注中国和朝鲜之间的核议程。该活动主要利用包含指向托管在 Microsoft OneDrive 上的恶意文档链接的鱼叉式网络钓鱼电子邮件，分发 ReconShark 恶意软件以感染其目标主机。此外，攻击者还使用了两种隐蔽的恶意载荷部署方式，以保持持久性。第一种方法的有效载荷部署涉及编辑与 Chrome、Outlook、Firefox 或 Edge 等流行应用程序关联的 Windows 快捷方式文件 (LNK)。另一种方法则是通过将默认的 Microsoft Office 模板 Normal.dotm 替换为托管在 C2 服务器上的恶意版本，以便在用户启动 Microsoft Word 时加载恶意代码。

绿斑

绿斑，是一个长期针对国内国防、政府、科技和教育领域的重要机构实施网络间谍攻击活动的 APT 团伙，最早可以追溯到 2007 年。该组织惯用鱼叉式钓鱼网络攻击，会选取与攻击目标贴合的诱饵内容进行攻击活动，相关领域包括：海洋（南海、东海、测绘）、军工、涉台问题（两岸关系）、中美关系，惯用的主题包括通知、会议材料、研究报告等或是采用攻击时间段时事主题。除了附件投递木马外，绿斑还惯用钓鱼网站钓鱼，窃取目标的账户密码，进而获得更多重要信息。别名：穷奇、PoisonVine、APT-Q-20、APT-C-01、绿斑、GreenSpot、白海豚、毒云藤。

绿斑在初始攻击环节主要采用鱼叉式钓鱼邮件攻击，在进行攻击之前，其会对目标进行深入调研，开展信息搜集。

通过分析搜集信息，仿冒国内最常使用的社交软件、邮箱系统（126、163 邮箱）、政府机构网站、军工网站、高等院校等网站等进行大规模钓鱼，以此获取定向群体的精确情报。

在 2023 年，该组织活跃度对比 2022 年稍有减弱，但还是持续保持着对我国的攻击，通过持续购买国内邮箱账号，从中筛选出具有一定价值的邮箱账号，进行扩散式钓鱼。对我国航天、海事、军队、教育、政府机构、多行业领域专家持续进行邮件钓鱼活动。

东欧活跃 APT 组织态势

2023 年上半年，东欧地区的 APT 攻击持续受俄乌战争影响，体现出高强度的攻击态势。以 APT29 和 Gamaredon 为代表的老牌俄罗斯背景 APT 组织对乌克兰方以及支持国家表现出持续的攻击活动，表 4-3 中为 2023 年上半年东欧地区攻击活跃 APT 组织基本信息。

组织名称	目标行业	目标国家	攻击动机	目标平台
WarSunflower（战争葵花）	政府	东欧及中亚地区	间谍行为、数据窃取	Windows
Gamaredon	军事、国防、教育	乌克兰、美国、英国、北约	间谍行为，数据窃取	Windows
APT29	政府、教育	美国、东欧、北约	间谍行为，数据窃取	Windows

表 4-3 2023 上半年东欧活跃 APT 组织信息

WarSunflower（战争葵花）

WarSunflower（战争葵花），别名有“APT-LY-1006”、“YoroTrooper”。该组织是在 2022 及 2023 年期间出现的新组织，主要针对东欧及中东、中亚部分国家进行攻击行动，该组织最早攻击行动可追溯到 2022 年 3 月份，该时间接近俄乌战争开始时间（2022 年 2 月），并结合其攻击目标分析，可初步判断该组织是由于俄乌战争而催生出的网络间谍组织。该组织主要活跃于东欧及中亚地区，将其命名为 WarSunflower（战争葵花）以代表其产生来源于俄乌战争。

2023 年上半年该组织主要针对阿富汗、乌兹别克食堂、哈萨克斯坦的政府部门进行钓鱼攻击。在攻击手法上，除了通过钓鱼窃取邮箱凭证外，该组织还投递多种木马对目标进行攻击（主要投递的载荷为 vhdx 文件，并且 vhdx 里包含后门组件或 LNK 文件下载器及诱饵文件等）。攻击目的上，该组织可基本确定诞生于俄乌战争期间，地缘政治以及战争是催生网络间谍组织的最主要力量，该组织目的为收集 CIS 国家的相关政府情报。并且通过分析该组织的各种组件发现，在利用工具上，该组织擅长对开源项目进行改造利用，并未发现技术能力较高的自研组件，且其主要打点方式为鱼叉攻击，暂时未发现较高水平的打点方式，可初步判定该组织的技术水平属于中低水平组织。通过分析其攻击目标地域、行业信息以及活跃时区以及语言习惯等，可初步判定该组织活跃在 UTC+2 至 UTC+4 区域，该地域属于东欧及中亚地区。

Gameradon

也被称为 Primitive Bear 组织，该 APT 组织疑似具有东欧背景，其最早的攻击活动可以追溯到 2013 年，主要针对乌克兰、北约国家 (特别是美国和英国)，长时间以相同组织为目标，其行业目标主要集中在国防和情报咨询公司、非政府组织 (NGO) 和政府间组织 (IGO)、智囊团和高等教育等，以窃取情报为目的。在俄乌战争中，该组织持续对乌克兰的公共机构和关键信息基础设施进行了针对性的网络攻击。其攻击手法主要是通过电子邮件、社交媒体和 LinkedIn 帐户创建伪造身份，并用虚假身份联系感兴趣的人来建立融洽的关系，从而实施钓鱼攻击。Gamaredon 还利用受感染域名，动态 DNS 提供商，俄罗斯和乌克兰国家代码顶级域名（ccTLD）以及俄罗斯托管服务提供商来分发其定制的恶意软件。

在 2023 年上半年，Gamaredon 组织频繁被披露针对乌克兰的间谍活动，在这些活动中观察到以下几方面特点，在攻击目标上，其活动针对于国家安全、军事和政府组织，攻击手法上，被观察到的攻击手段为网络钓鱼邮件和仿冒钓鱼页面来分发恶意软件，并还利用 USB 的摆渡攻击来进一步传播恶意软件。攻击工具上，在今年上半年还多次更新工具包，不断更新基础设施，还利用合法服务作为 C2 服务器，如 telegram 消息服务。

APT29

该组织目前归因于俄罗斯政府情报组织，APT29 至少从 2008 年开始运作，具有 YTTRIUM、The Dukes、Cozy Duke、Cozy Bear、Office Monkeys 等别名，主要针对美国、东欧和北约成员国的政府、研究机构和智库。APT29 一直是东欧地区 APT 组织中能力较为顶尖的，无论从微软报告的 Nobelium 事件或 SolarWinds 事件，该组织一直保持着较高的攻击能力。

2023 年 4 月，APT29 针对北约和欧盟成员国的外交部门开展了间谍活动，活动涉及利用了之前未被发现的恶意软件，APT29 主要通过向外交职位的特定人员发送鱼叉式网络钓鱼电子邮件获取初始访问权限；2023 年 4 月中旬，APT29 拦截了波兰外交部向各个大使馆发出的一份宣传出售位于基辅的二手宝马轿车的合法传单，通过将其嵌入恶意软件，分发给了在基辅工作的数十名外交官。2023 年 6 月，APT29 针对入驻乌克兰大使馆的众多外交官发起了网络间谍攻击，这一活动直接瞄准了乌克兰首都基辅约 80 个外国使团中的至少 22 个外交官。2023 年 7 月，APT29 冒充挪威大使馆，分发了以 " 邀请 - 圣卢西亚庆典 " 为主题的网络钓鱼电子邮件，且该组织使用了更高级的策略，包括使用 SVG Dropper、DLL 实现感染和进行 C2 行为。

APT 攻击流行技术趋势

软件供应链攻击获取 APT 攻击初始权限

供应链攻击技术是 APT 攻击组织常用的攻击技术之一，也是最近一些年 APT 攻击组织使用最多的攻击方式之一，这种攻击方式主要针对特定的企业和用户进行定向攻击活动，并且使用多种多样的攻击方式，其中最主流的是软件供应链攻击。

软件供应链攻击可以分为基于软件源代码、开源软件第三方包和软件开发工具相关的攻击方式。其中，基于软件源代码的攻击方式最为隐蔽、危害最大，也是技术难度最高的一种攻击方式。而基于开源软件第三方包和基于软件开发工具相关的攻击方式相对容易实现。近年来发现，软件供应链攻击在 APT 攻击活动中越发普遍。

基于软件源代码的攻击方式

APT 攻击组织攻陷软件供应商之后，将恶意代码直接嵌入到软件供应商的软件代码当中，通过软件供应商将包含有恶意代码的软件分发给该软件供应商的企业客户，导致所有使用该软件的企业客户感染恶意代码，这种供应链攻击方式非常隐蔽，也是危害最大的一种攻击方式，此前 SolarWinds 供应链攻击事件就是一种基于软件源代码的攻击方式。2023 年 4 月，Lazarus 有关的 UNC4736 组织利用 3CX 桌面应用程序实施了双重供应链攻击，该事件是由于 2022 年该组织针对 X_TRADER 的软件供应链攻击事件导致的，其通过植入恶意代码的 X_TRADER 软件窃取 3CX 公司使用者网络登录凭据，以实施对 3CX 网络的攻击活动，并对 3CX 桌面应用程序使用了同样的恶意注入，持续扩大攻击范围。

基于开源软件第三方包的攻击方式

APT 攻击组织利用 PyPI、NPM 等第三方包进行供应链攻击，这种攻击方式主要目的是定向攻击大型企业的开发人员，通过窃取这些开发人员的登录凭证等信息之后，渗透到企业内网，进行更隐蔽的 APT 攻击活动。2023 年 1 月，某攻击者针对一款流行机器学习框架 PyTorch 进行了供应链攻击活动，攻击者在这些第三方包中插入恶意程序，使开发人员下载软件包并使用后，将在其开发环境主机的 runtime 目录下插入恶意脚本和恶意程序，在通过开发程序的 __init__.py 初始化脚本运行后，将启动 runtime 目录下的 triton 恶意程序。PyTorch 开源软件当前下载量约 1.8 亿次，若被污染的软件包被大量使用在开发程序中，将引发很大安全风险。

基于软件开发工具相关的攻击方式

APT 攻击组织利用伪造的包含恶意软件的软件开发工具或者被感染了恶意代码的软件开发工具的工程项目文件，诱骗企业开发人员安装或使用这些软件开发工具和工程项目文件，安装木马后门进行下一步的攻击活动，Lazarus APT 攻击组织就曾利用这种攻击方式，通过感染了恶意代码的软件开发工具的工程项目文件，定向攻击安全研究人员，此前 XCodeGhost 供应链攻击事件也是这种基于软件开发工具的攻击方式。

未来随着全球云计算虚拟化等平台的高速发展，基于软件供应链攻击的活动越来越多，APT 组织越来越多地瞄准软件供应商来实施定性攻击，这种以更加快速有效的方式获取目标组织的网络访问权限将成为 APT 攻击的一大趋势。

开源组件二次开发以降低 APT 攻击成本

在 2023 上半年检测到的 APT 攻击活动中，越来越多的组织开始利用开源组件二次开发的攻击组件，尤其集中在远控组件上。开源组件的二次开发利用极大的减少了 APT 组织在攻击成本上的消耗，且具备能够快速迭代更新以保持不断变化的攻击能力，主要体现在反调试、反分析，以及目标识别等等。这些快速迭代的对抗技巧也使得 APT 组织和安全企业之间的攻防较量更为复杂和激烈，溯源归因难度也越来越高。在 2023 年上半年发现南亚多个组织利用了多种开源组件开展攻击活动，包括有 Patchwork 和 Bitter 组织。

在最近的一次攻击活动中，Patchwork 组织投递的恶意 lnk 文件用于下载第二阶段 BADNEWS 远控，其使用了 hiiresloader 加载器（该加载器存在特殊字符 hii 并将载荷存储于资源数据进行加载）。通过分析该文件为开源远控（地址：https://github.com/XZB-1248/Spark/tree/master）。

除此之外，我们还捕捉到 Patchwork 组织使用另外一种开源加载器加载开源远控“NorthStarC2”进行攻击。通过分析该加载器为开源加载器（地址：https://github.com/EddieIvan01/gld），该加载器使用 AES-GCM-256 加密载荷并使用 base64 编码存储，而后在解密后内存加载的载荷为开源远控（地址：https://github.com/EnginDemirbilek/NorthStarC2），其连接 C2 为“jillin[.]online”。

BYOVD 滥用过时驱动以对抗杀软

BYOVD，全称为 Bring your own vulnerable driver，即攻击者向目标环境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 / 致盲终端安全软件等，该项技术主要应用于攻击者获得系统权限后的提权操作，利用合法驱动的安全漏洞执行内核级权限操作以关闭杀毒软件，实现长期潜伏并窃取情报的恶意操作。

在 BYOVD 利用工具的选择上，攻击者可能会进行自主开发或利用开源项目，而部分自主开发的工具也是基于开源项目进行改进的，如在 23 年上半年的攻击活动中 APT 组织 UNC2970 和勒索组织 Lockbit 分别使用了自己的 BYOVD 利用工具 LIGHTSHOW 和 AuKill，其中 AuKill 与开源 BYOVD 利用项目 Backstab 存在相似性。另一方面，LockBit 的确在 22 年 11 月的勒索攻击中直接合入了 Backstab 开源工具，同样被勒索组织合入的 BYOVD 利用工具还有 SpyBoy Terminator，该工具于 5 月下旬在网上公开售卖，后被 BlackCat 用于真实的勒索攻击。

在 BYOVD 利用成本上，LOLDrivers 项目记录在案的，可供攻击者滥用的合法驱动程序数量在 700+，除此之外，还存在着一些未被记录的或仅被攻击者所掌握的可用于攻击活动的合法驱动程序，这意味着攻击者拥有一个充足的库来发起 BYOVD 攻击。此外，在 Github 上进行检索可以发现一系列 BYOVD 利用工具，它们分别包括摘除杀软回调、Kill 杀软进程、关闭 / 开启 PPL 保护，和关闭 / 开启强制签名校验等多种高级攻击技巧，这些利用工具涵盖的功能几乎满足了攻击者的所有需求，攻击者也可以基于此系列项目记录的驱动漏洞利用原理，挖掘和开发未知的驱动利用。

这项技术最初主要被如 Turla 和方程式这样的顶级 APT 组织所使用，而随着攻击成本的降低，其它攻击组织也逐渐开始使用这项技术，以 BYOVD 为标签进行检索可以发现在更早些时候就已经有不同的攻击组织在真实攻击活动中使用此项技术。目前，BYOVD 技术从最初被顶尖 APT 组织所使用，发展到如今越来越广泛的利用在 APT 攻击当中。

典型 APT 攻击事件

某高校高新行业实验室被高精准社工鱼叉攻击

2023 年 2 月至 4 月，境内某高校与国内高新产业相关的近百名教职工、学生遭到境外以窃取情报为目的的定向网络攻击，已知至少 3 名教师，2 名学生的个人主机被植入窃密木马，至少 4 台主机被窃取文件。

攻击者至少使用“faculty-confirmation”、“GENO2185234 论文校对”、“APCATS 等会议 Co-chair 邀请”三种伪装程度极高的邮件话术进行钓鱼邮件攻击，受害者运行攻击者提供的程序后，下载后续阶段远控、反弹 shell、浏览器窃密、文件窃密、U 盘摆渡木马等恶意程序，其最终目的是窃取并持续监控受害者机器上的文档文件。

此次攻击中，攻击者疑似首先在暗网获取了大量受害者信息，包括基本信息、邮箱账密等等，对受害者信息了如指掌。在获取到受害者邮箱权限后，攻击者监控到了能够编写定向钓鱼邮件的邮件主题和语料，包含顶会邀请、论文校对等等，使其伪造的钓鱼邮件十分逼真，引发大量受害者点击。攻击者甚至伪装为与教授私交甚好的他国高校教授与受害者进行长达十几封的邮件往来交流也没有被识破身份，极具迷惑性。

在 2023 年上半年实际对我国的 APT 钓鱼攻击事件中发现，APT 组织在对目标组织和目标受害者的社工程度比以往更深，其具备高精准的社工思维和技巧制作大量难辨真伪的诱饵，并通过长期的潜伏伪装让受害者防不胜防。

蔓灵花利用开源远控组件攻击某政府机关单位

2023 年 1 月 11 日，根据深信服千里目安全技术中心监控发现某政府机关单位某终端主机与 APT 组织基础设施存在通信行为。根据进一步排查发现，该终端在 1 月 4 日点击钓鱼邮件中的恶意域名 rusjamstarapp[.]com 并下载了攻击载荷文件。还原攻击过程为攻击者向受害者投递恶意邮件后，受害者点击恶意邮件中的附件，执行 chm 恶意附件导致创建恶意计划任务，从而被 APT 组织控制。

邮件中投递的件 chm 恶意附件在点击后将会创建计划任务“AdobeUpdater”并调用 msiexec 远程下载 cert.msi 文件作为攻击载荷并执行，从而释放了远控组件 scroll_.exe，经过分析，确认该文件为蔓灵花组织一直在使用的 DarkRAT 远控，本次攻击者对该远控进行了混淆，该远控组件由开源远控 DarkAgent 项目修改而成，其参考的开源项目地址为 https://github.com/ilikenwf/DarkAgent。通过进一步分析，确认该下载 cert.msi 文件的远程地址“rusjamystarapp[.]com”为印度 APT 组织蔓灵花的 C2 服务器。

在终端取证中发现该终端还存在异常启动项 ceve.exe，根据启动项定位文件位置，发现该文件创建时间为 1 月 4 日 15:45:40，通过深信服专用 APT 沙箱平台分析发现该程序为远控木马，关联域名 devqrytoprar[.]net，而该域名在开源情报中已经被披露归因为蔓灵花 APT 组织。攻击者还多次尝试使用了远控工具 anydesk，但因为单位策略设置拒绝访问未成功连接。研究员上机取证后，第一时间对失陷终端中的驻留项和恶意文件进行了清除。

开源组件利用在 APT 攻击中越发常见，开源组件二次开发形成恶意组件的方式极大的减少了一些攻击能力较弱的组织的研发成本，并使得攻击溯源更加困难。

UNC4736 组织利用双重供应链攻击 3CX 公司

2022 年 UNC4736 组织对 Trading Technologies 公司开发的 X_TRADER 交易软件进行篡改，在其源代码中插入恶意程序（称为 VEILEDSIGNAL）投放在软件官网上，该恶意程序允许攻击者获得软件使用者的计算机访问权限并窃取网络凭据。2022 年 9 月至 11 月期间，UNC4736 利用木马化的 X_TRADER 应用程序入侵了电力和能源领域的两个关键基础设施组织以及另外两个涉及金融交易的企业。

2023 年 3 月，大型企业级电话管理系统供应商 3CX 遭受严重供应链攻击，该公司 3CX 桌面应用程序软件被 UNC4736 组织注入恶意程序，并投放在广泛下载渠道传播。经过调查发现，此次事件是由 2022 年 X_TRADER 交易软件的供应链攻击事件导致。

根据 Mandiant 对 3CX 公司受攻击情况调查发现，由于 3CX 员工意外下载被污染的 X_TRADER 应用程序，从而被 UNC4736 窃取了 3CX 公司的办公环境的网络登录凭据，UNC4736 使用同样的源代码污染方式在 3CX 桌面应用程序植入恶意代码，并将其投放在官方下载渠道中。此次攻击所涉及该软件的 Windows、Linux 和 MacOS 版本，据 3CX 官网显示，目前，3CX 的产品和服务已经覆盖全球 160 多个国家，并且已经拥有超过 60 万企业用户，日活跃用户超过 1200 万，此事件影响面极大。根据 Mandiant 的调查将此次事件高度归因于 UNC4736 组织，并与东北亚某国家有联系，根据公开情报发现 UNC4736 隶属于 Lazarus 组织。

该事件是首次发现的软件供应链攻击事件导致的软件供应链攻击，被广泛称为 “双重供应链”攻击事件。双重供应链攻击将其传播范围广的特性再次放大，将两条软件供应链上下游给串联起来，实现难以察觉的连环攻击，并保持长期存在的攻击效果。该事件的攻击效果为黑客组织提供了攻击新思路，可能将吸引更多黑客组织转向使用该手段，从攻击目标源头供应商入手，部署更加复杂的软件供应链攻击。

美国情报机构针对 iOS 设备的移动端 APT 活动

俄罗斯联邦安全局（FSB）发现了美国政府新的“监控证据”，俄方确信美国政府正通过入侵数千部 iPhone 手机，来监控俄罗斯本国以及外国公民，受监控的群体还包括一些国家的在俄外交官。总部位于俄罗斯首都莫斯科的著名网络安全公司卡巴斯基实验室也表示，该公司有数十名员工的个人电子设备在美国政府的间谍活动中遭到破坏。

2023 年 6 月 1 日，卡巴斯基发布了一篇报告表示，公司高层和中层管理人员的 iPhone 数据被盗，这是代号为“三角测量行动”的 APT 攻击的一部分。三角测量行动的第一批痕迹可以追溯到 2019 年，此次攻击行动利用的是零点击漏洞，因此不需要用户进行任何交互，通过 iMessage 收到受感染的消息后，设备将被感染，并在受感染的 iPhone 中部署 APT 工具包。

在后续的调查跟进中发现，该植入程序被卡巴斯基命名为 TriangleDB，是在攻击者利用内核漏洞获得目标 iOS 设备的 root 权限后部署的。它部署在内存中，这意味着当设备重新启动时，植入物的所有痕迹都会丢失。因此，如果受害者重新启动设备，攻击者必须通过发送带有恶意附件的 iMessage 来重新感染设备，从而再次启动整个漏洞利用链。如果没有重新启动，植入程序将在 30 天后自行卸载，除非攻击者延长此期限。一旦植入程序启动，它就会开始与 C2 服务器通信，使用 Protobuf 库交换数据。

苹果在 7 月 24 日再次发布了安全更新通告，以解决针对 iPhone、Mac 和 iPad 的攻击中被利用的零日漏洞，该漏洞被追踪为 CVE-2023-38606。据卡巴斯基 GReAT 首席安全研究员 Boris Larin 称，CVE-2023-38606 是用于通过 iMessage 漏洞在 iPhone 上部署三角测量行动间谍软件的零点击漏洞链的一部分。此次修复的漏洞影响的设备列表相当广泛，包括各种 iPhone 和 iPad 机型，以及运行 macOS Big Sur、Monterey 和 Ventura 的 Mac。

美国针对全球无差别的情报监控已陆续被各国发现，俄罗斯和其安全厂商卡巴斯基披露了美国利用 Apple 漏洞一系列的攻击行为，除俄罗斯外，包括以色列、叙利亚和中国都在此次监控范围内。

APT 攻击态势小结

01

APT 组织在钓鱼攻击的社工上越发精细，所制作的诱饵越发具有迷惑性。随着大众对钓鱼攻击和诈骗信息的防范性逐渐提高，APT 组织的钓鱼诱饵制作采取了更加定向性的社会工程学分析并与窃取的真实文件相结合，制作出难以辨别真伪的钓鱼邮件信息，使得受害者防不胜防，在上半年实际捕获的 APT 攻击事件中，APT 组织体现精细的前期打点工作，其通过多种渠道的社工手段将受害者信息和钓鱼背景全面掌握，制造出与受害者日常工作内容几乎一致的钓鱼诱饵，使得其攻击具有极高成功率。

02

供应链攻击将可能成为 APT 组织获取初始权限的流行方式。自影响全球的 SolarWinds 供应链攻击事件爆发以来，越来越多的 APT 组织开始瞄准目标上游供应商，今年上半年的 3CX 双重供应链攻击事件影响力尤为突出，双重供应链攻击将其传播范围广的特性再次放大，将持续吸引更多组织利用该攻击手法。

03

开源组件在 APT 攻击中广泛使用，以降低攻击成本和攻击反溯源效果。在 2023 上半年检测到的APT攻击活动中，越来越多的组织开始利用开源组件二次开发的攻击组件，尤其集中在远控组件上。开源组件的二次开发利用极大的减少了 APT 组织在攻击成本上的消耗，且具备能够快速迭代更新以保持不断变化的攻击能力，主要体现在反调试、反分析，以及目标识别等等。这些快速迭代的对抗技巧也使得 APT 组织和安全企业之间的攻防较量更为复杂和激烈，溯源归因难度也越来越高。

04

BYOVD 技术正广泛应用于各大 APT 攻击活动中。BYOVD 技术从最初被顶尖 APT 组织所使用，发展到如今被越来越广泛的利用在 APT 攻击当中，未来这项技术的使用频率可能会进一步增加，且更加自动化。

05

Web3安全态势

- Web3 安全态势情况
- Web3 合约安全情况
- Web3 安全产业发展情况
- Web3 安全态势小结

Web3 安全态势情况

Web3 是指第三代互联网，旨在重新定义互联网的基本架构和用户体验。它的出现改变了原有的基础架构，将网络的主权转给用户，将分散的数据库和分类账部署在任何人都可以使用的节点上，以此来抵消敏感信息垄断和集中“蜜罐”的风险。Web3 应用场景非常广泛，涵盖了金融、身份认证、市场交易、投票治理等众多领域，已成为近年来行业投资的热点。

Web3 安全事件总体态势

据 FootprintAnalytics 监测分析，2023 年上半年 Web3 领域安全事件频发，依旧呈现高发态势，黑客攻击、钓鱼诈骗和项目方卷款跑路等方面，造成的总损失达到了 6 亿 5561 万美元，如图 5-1 所示。

图 5-1 2023 年上半年 Web3 领域的总损失情况

从类型来看，Hacks（黑客攻击）发生安全事件 108 起，总损失金额约 4 亿 7143 万美元，约为 2022 年上半年的 24.5%， PhishingScams（钓鱼诈骗）发生安全事件 120 起，总损失金额约 1.08 亿美元。RugPull 项目卷款跑路发生安全事件 110 起，总损失约 7587 万美元。

从损失金额来看，如图 5-2 所示，损失金额超过 1 亿美元的安全事件共 1 起，损失在 1000 万美元 ~1 亿美元区间的事件共 7 起。此外，100 万美元 ~1000 万美元区间的事件 23 起。

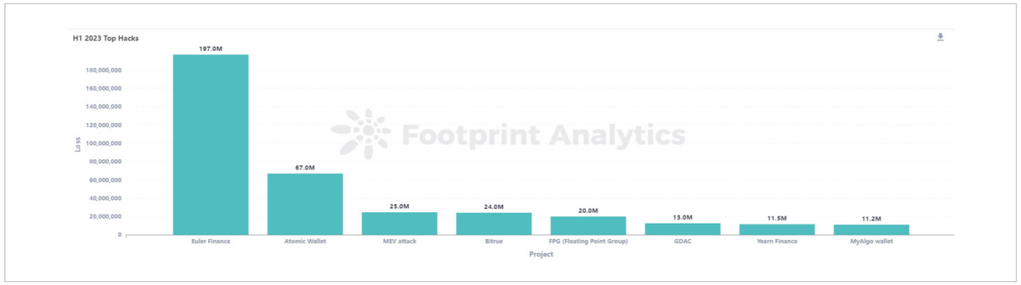


图 5-2 2023 年上半年 Web3 领域重大安全事件损失排行

损失金额超过千万美元的 Web3 领域重大安全事件详情：

■ EulerFinance-1.97 亿美元

3 月 13 日，DeFi 协议 EulerFinance 遭到攻击，损失达到了 1.97 亿美元。4 月 4 日，EulerLabs 在推特上表示，经过成功协商，攻击者已归还了所有盗取资金。

■ AtomicWallet-6700 万美元

6 月 3 日，Atomic 用户在社交媒体发文称自己的 Wallet 资产被盗，统计发现被盗金额至少达到了 6700 万美元。黑客已将被盗资金通过 MixingService 平台 Sinbad 进行了清洗，被攻击原因仍在调查中。

■ MEVattack-2500 万美元

4 月 3 日，MEV 机器人遭受恶意三明治攻击，总共损失约 2500 万美元。

■ Bitrue-2400 万美元

4 月 14 日，BitrueWallet 遭受攻击，损失达 2400 万美元。

■ FPG-2000 万美元

6 月 11 日，FloatingPointGroup(FPG）遭到网络攻击，损失约 2000 万美元的虚拟资产。

■ GDAC-1300 万美元

4 月 9 日，韩国 GDAC 遭到黑客攻击，损失近 1300 万美元。

■ YearnFinance-1150 万美元

4 月 13 日，YearnFinance 的 yusdt 合约遭受黑客攻击，黑客获利超 1000 万美元。

■ MyAlgoWallet-1120 万美元

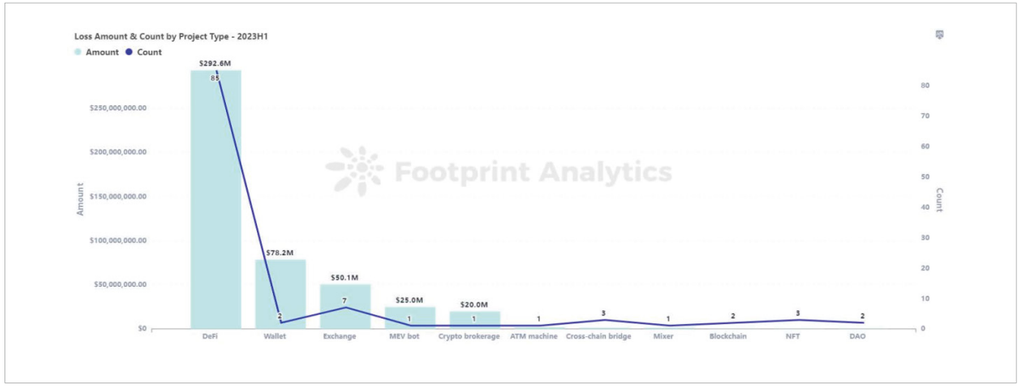
2 月，MyAlgoWallet 遭到中间人攻击，损失达 1120 万美元。

Web3 安全事件损失情况

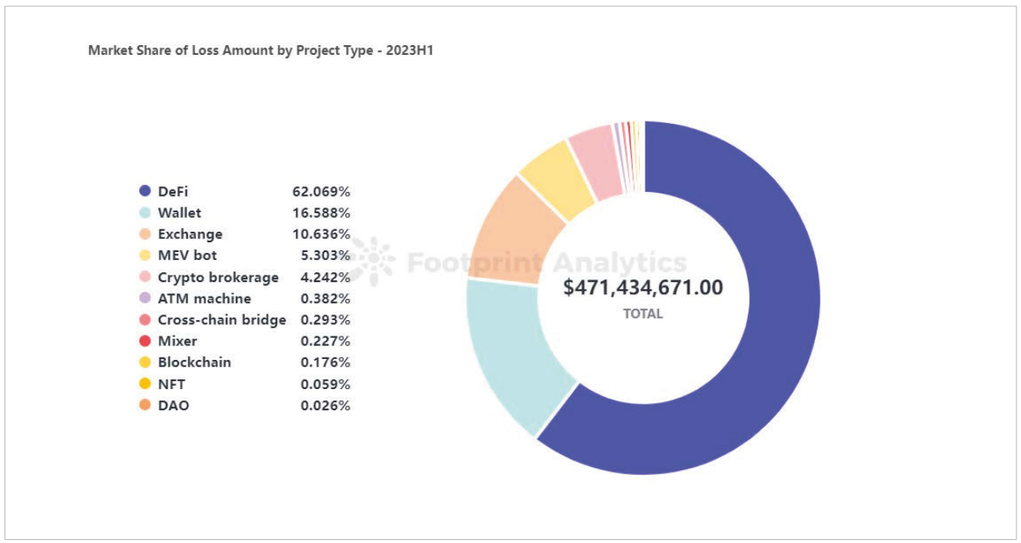
2023 年上半年 Web3 领域发生黑客攻击事件 108 起，总损失金额约 4 亿 7143 万美元，涉及常见 DeFi（分布式金融）、Wallet（钱包）、Exchange 等项目类型，Ethereum（以太坊）、BNBChain（币安智能链）等链平台，安全事件类型呈现出多样性，黑客攻击手段愈发丰富，攻击手法层出不穷等特征。

（一）项目类型分析

从项目类型来看，主要涉及 DeFi（分布式金融）、Wallet（钱包）、Exchange（交易所）、MEVbot（套利机器人）、Cryptobrokerage（经纪商）、ATMmachine（自助提款机）、Cross-chainbridge（链桥）、MixerServices（混币服务）、blockchain（公链）、NFT（数字藏品）、DAO（分布式社区）等，2023 年上半年以上各项目类型发生的安全事件数量分布以及遭受攻击造成的损失占比情况如图 5-3、图 5-4 所示。



■图 5-3 2023 年上半年 Web3 项目类型及安全事件数量分布



■图 5-4 2023 年上半年 Web3 项目安全事件损失占比

其中，DeFi 类型项目共发生 85 次安全事件，占总事件数量的 78.7%。DeFi 总损失金额达到了 2.92 亿美元，占总损失金额的 62%。DeFi 为被攻击频次最高、损失金额最多的项目类型。85 次 DeFi 安全事件里，有 51 起安全事件都源自于合约漏洞利用，损失达 2.49 亿美元，占 DeFi 损失总金额的 85%。

Wallet 类型项目共发生 2 次安全事件，带来了约 7820 万美元的损失，金额占所有项目类型的第二位。其中 AtomicWallet 攻击事件至少损失了 6700 万美元，MyAlgoWallet 攻击事件损失为 1120 万美元。

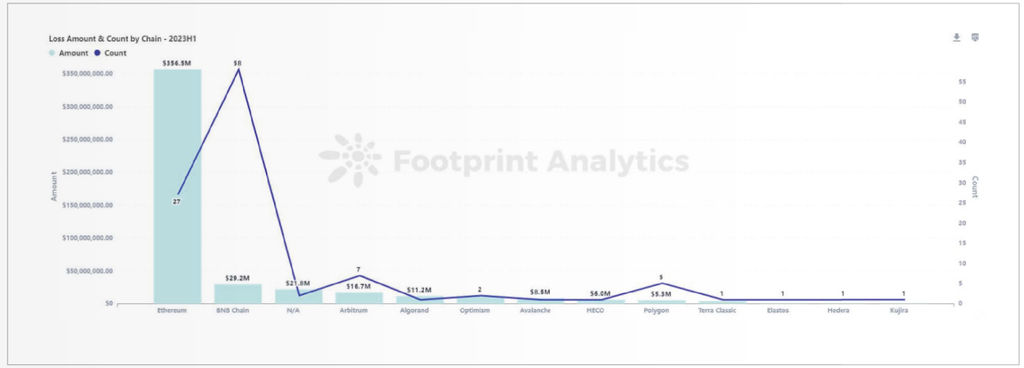
Exchange 类型项目共发生 7 次安全事件，损失约 5014 万美元，金额占所有项目类型的第三位，其在 2022 年全年数据里损失排名也是第三位，今年延续了其攻击频发趋势。

Cross-chainbridge 类型项目的损失情况有所缓和，其在 2022 年损失金额排名第一（18.9 亿美元），而在 2023

年上半年损失大幅下降到了 138 万美元。

（二）链平台类型分析

从链平台类型来看，主要涉及 Ethereum（以太坊）、BNBChain（币安智能链）、Arbitrum、Algorand、Optimism、Avalanche、HECO、Polygon、TerraClassic、Elastos、Hedera、Kujira、N/A（未披露的）等行业主流链平台，2023 年上半年各种链平台发生安全事件的情况如图 5-5 所示。



■图 5-5 2023 年上半年 Web3 链平台及安全事件数量分布

其中，Ethereum 链平台发生主要攻击事件 27 起，损失金额约为 3.56 亿美元。Ethereum 链平台上损失金额居所有链平台的第一位，占比约 75.6%。

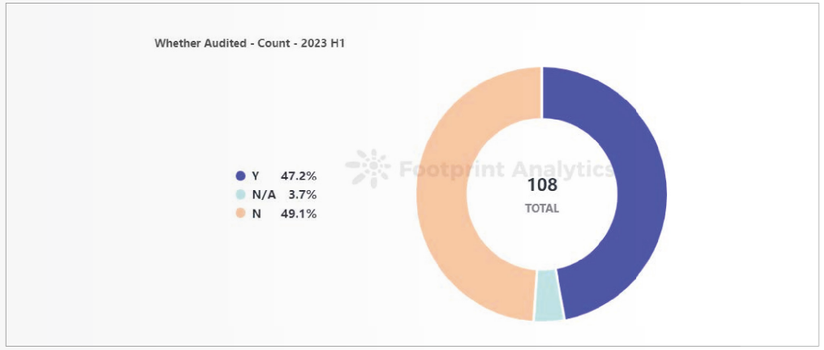
BNBChain 链平台发生主要攻击事件 58 起，损失金额约为 0.292 亿美元，攻击事件总数占所有事件的 53.7%。其中，BNBChain 链平台上发生的 58 次攻击事件里，有 40 个被攻击项目都未经审计。

Arbitrum 链平台发生主要攻击事件 7 起，损失金额约为 0.167 亿美元，安全事件损失金额和数量与 2022 年相比有所增加（Arbitrum 在整个 2022 年只发生过 2 起主要的安全事件）。

2022 年 Solana 链平台上损失金额排所有公链的第三位，而在 2023 年上半年并未监测到主要攻击事件。

（三）审计情况分析

从项目审计情况看，Web3 领域遭受黑客攻击事件中，经过第三方审计服务的项目为 51 个，未经审计的项目为 53 个，未披露的项目为 4 个，项目审计比例与 2022 年情况也大体一致，如图 5-6 所示。



■图 5-6 2023 年上半年 Web3 项目第三方审计情况占比

其中，未接受第三方审计服务的 53 个项目，以及未披露的 4 个项目，因合约逻辑或函数设计不当、合约验证问题、合约重入漏洞等质量缺陷，遭受到了严重的虚拟资产损失，损失金额 3.217 亿美元，占损失金额的 68%。

接受第三方审计服务的 51 个项目，损失金额 1.494 亿美元，占损失金额的 32%。其中，约有 31 个项目因第三方审计服务不充分，导致合约漏洞被黑客利用，审计失效比例约为 60%，远高于 2022 年的 45%。

第三方审计服务能够有效识别出 Web3 项目中存在的质量缺陷和安全漏洞，通过第三方审计服务能够有效，提升项目质量，规避因合约安全问题导致的虚拟资产损失。然而，当前 Web3 第三方审计服务机构良莠不齐，服务技术水平不容乐观，建议项目方积极开展第三方审计服务，寻找更为专业的安全公司提供审计服务。

Web3 安全事件趋势

2023 年上半年，Web3 领域黑客攻击事件的总损失金额较 2022 年有了大幅度下降。2022 年上半年攻击总损失约 19.1 亿美元，2022 年下半年约 16.9 亿美元，而 2023 上半年该数值下降到了 4.7 亿美元，并且其中约有 2.15 亿美元的被盗资产得以追回。

2023 年上半年 Web3 领域的安全趋势，主要呈现状况如下几点所示：

在攻击损失金额方面，从项目类型来看，DeFi（分布式金融）依旧是被攻击频次最高、损失金额最多的类型。85 次 DeFi 安全事件总损失金额达到了 2.92 亿美元，占总损失金额的 62%。从链平台类型来看，75.6% 的损失金额来自 Ethereum（以太坊），约 3.56 亿美元，居所有 Web3 链平台的第一位。

从攻击手法来看，最频发、造成损失最多的攻击手法为 SmartContract（智能合约）漏洞利用。其中，重大智能合约发生安全事件 60 次，造成损失 2.64 亿美元，占所有损失金额的 56%。

从资金流向来看，约有 2.15 亿美元的被盗虚拟资产得以追回，占所有被盗虚拟资产的 45.5%。另外约有 1.13 亿美元的被盗虚拟资产转入了 TornadoCash 协议以及其他 MixingService 混币系统。

从审计情况来看，发生安全事件的 Web3 项目中，约有 49% 的项目没有经过第三方审计，存在业务漏洞。

从攻击数量来看，黑客攻击呈现大幅放缓趋势，促成这一现象的原因包括全球监管体系的逐步完善、执法力度的加大、项目方安全意识的提升、Mixing Service（混币系统）被制裁、AML 反洗钱技术和程序的完善等。另外，也出现了依靠社区力量，通过链下情报对黑客身份进行定位，并迫使黑客返还被窃虚拟资产的案例。

与黑客攻击事件下降的趋势相反的是，针对普通用户的钓鱼诈骗更加频发。上半年出现了以 VenomDrainer 为代表的一系列钱 Drainer 团伙，他们开发恶意工具包后进行售卖，购买者成功钓鱼获利后再与之进行分成。此类钓鱼诈骗波及用户面广，单是 VenomDrainer 这一个团伙就产生了至少 1.5 万个受害者。对于普通用户而言，最好能够经常关注安全公司的提醒，系统性地学习一些防钓鱼防被盗知识，也可以安装一些防钓鱼插件、交易预执行工具等进行提醒。

Web3 合约安全情况

Web3 安全攻击手段总览

2023 年上半年 Web3 领域黑客攻击中，攻击手段愈发丰富，攻击手法层出不穷，主要涉及 Contractvulnerability（智能合约漏洞）、Unclear（攻击手段不确定）、Privatekeycompromise（私钥泄漏）、Arbitrageattack（套利攻击）、Misconfiguration（配置错误）、ManintheMiddle（中间人攻击）、Pricemanipulation（价格操纵）、Socialengineering（社工攻击）、Flashloan（闪电贷攻击）、Governanceattack（治理攻击）、Zero-dayattack（零日攻击）、Front-running（抢先交易攻击）等，如图 5-7、图 5-8 所示。

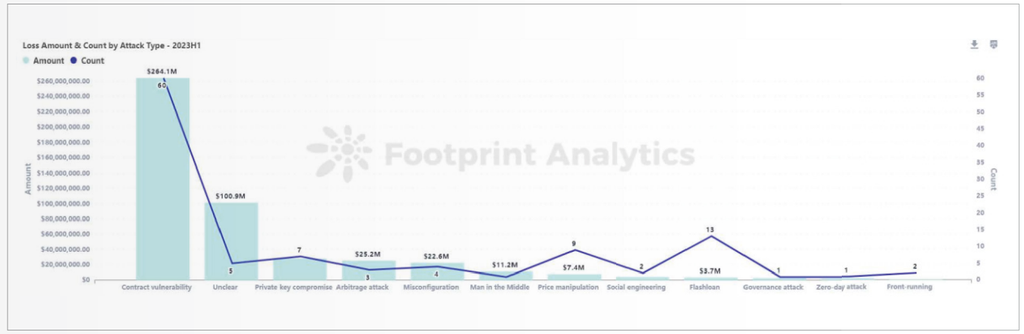


图 5-7 2023 年上半年 Web3 攻击手段及安全事件数量分布

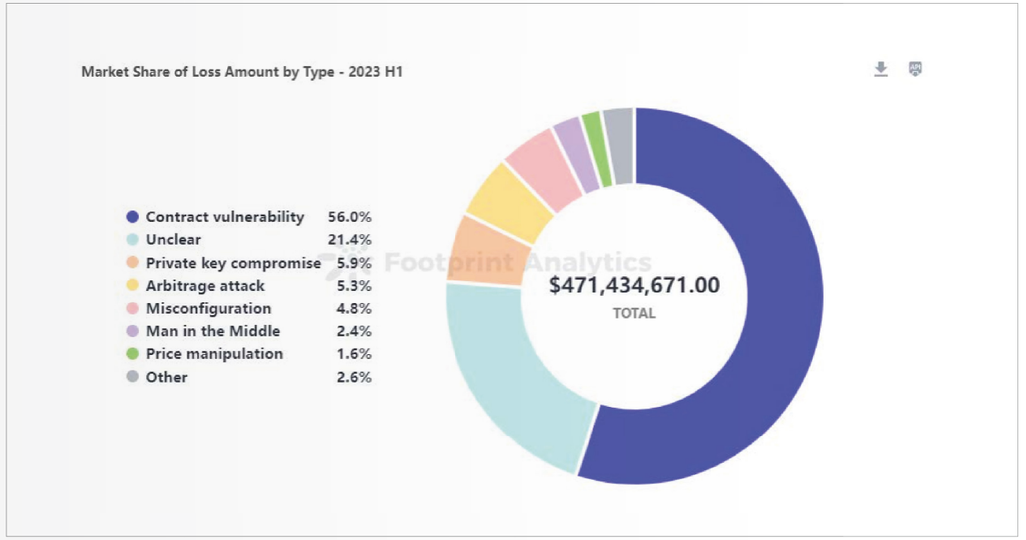


图 5-8 2023 年上半年 Web3 各类攻击手段导致的损失金额占比

其中，2023 年上半年 Web3 领域，共发生 7 次私钥泄露事件，造成了约 2767 万美元的损失，相较 2022 年私钥泄漏事件有所减少。私钥泄露事件一直持续威胁着项目方安全，从一些事件披露来看，加强核心成员的职业道德和安全意识管理尤为重要。

同时，共发生 5 次攻击手法暂不清晰的安全事件，造成了约 1 亿美元的损失，其中包括 AtomicWalletWallet 被 6700 万美元、FPG 被攻击 2000 万美元等事件。此类事件涉及金额大，影响用户众多。建议此类项目在进行事件原因调查的同时，应积极和第三方审计机构合作，及时公布调查结果，采取必要的修复措施，对用户虚拟资产安全肩负起责任。

此外，共发生 60 次合约漏洞事件，造成损失 2.64 亿美元，占所有损失金额的 56%。在合约漏洞中造成损失最多的分别是 Bussinesslogicflaw（业务逻辑缺陷）、Accesscontrol（权限问题）、Reentrancy（重入）、Callinjection（调用注入）、Validationissue（验证）、Overflow（溢出）等手段。尤其是 36 次业务逻辑漏洞共造成了约 2.39 亿美元的损失，占所有因合约漏洞攻击损失的 90%。此类漏洞是开发者最容易遗漏的问题，被攻击后造成的损失往往较大，有 9 起事件的损失金额都超过了 100 万美元，如图 5-10 所示。

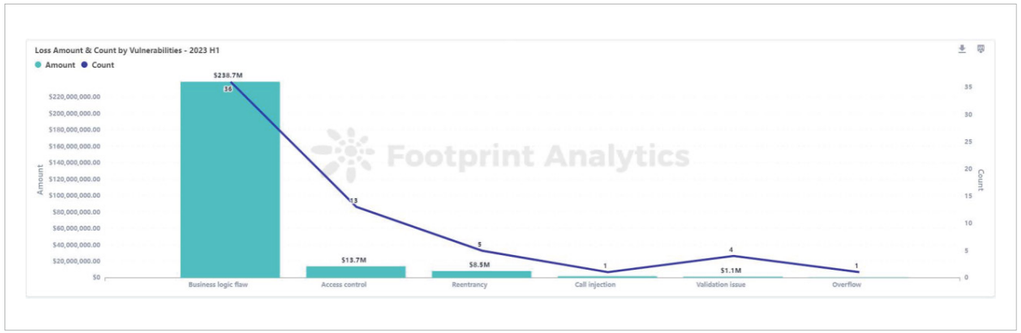


图 5-10 2023 年上半年 Web3 合约漏洞攻击手段及安全事件数量分布

需要重点注意的是，智能合约漏洞利用仍然是 Web3 项目最频发、造成损失最多的攻击手法。因此，有必从第三方审计服务角度，重点针对 Web3 合约进行安全分析，提出应对策略，复盘分析典型安全事件，协助项目方了解 Web3 合约经常存在的安全缺陷，为促进 Web3 项目安全性奠定基础。

Web3 合约安全风险分析

智能合约本质上是部署和运行在区块链上的程序，其负责将 Web3 项目的业务逻辑以代码形式实现、编译并部署，并按照既定的规则或者触发条件从而自动执行，合约的操作对象大多为虚拟资产，也决定了智能合约在具有高价值和高风险。在没有标准的合约模板或编写规范的情况下，很难要求程序员都能够写出最佳实践的代码。当前，Web3 智能合约已知出现的安全风险有 20 多种，如下所示。

01 重入攻击检测

重入漏洞是最著名的以太坊智能合约漏洞，曾导致了以太坊的分叉（TheDAOhack）。Solidity 中的 call.value() 函数在被用来发送 Ether 的时候会消耗它接收到的所有 gas，当调用 call.value() 函数发送 Ether 的操作发生在实际减少发送者账户的余额之前时，就会存在重入攻击的风险。

02 数值溢出检测

智能合约中的算数问题是指整数溢出和整数下溢。Solidity 最多能处理 256 位的数字（2^256-1），最大数字增加 1 会溢出得到 0。同样，当数字为无符号类型时，0 减去 1 会下溢得到最大数字值。

整数溢出和下溢不是一种新类型的漏洞，但它们在智能合约中尤其危险。溢出情况会导致不正确的结果，特别是如果可能性未被预期，可能会影响程序的可靠性和安全性。

03 访问控制检测

访问控制缺陷是所有程序中都可能存在的安全风险，智能合约也同样会存在类似问题，著名的 ParityWallet 智能合约就受到过该问题的影响。

返回值调用验证此问题多出现在和转币相关的智能合约中，故又称作静默失败发送或未经检查发送。在 Solidity 中存在 transfer()、send()、call.value() 等转币方法，都可以用于向某一地址发送 Ether，其区别在于：transfer 发送失败时会 throw，并且进行状态回滚；只会传递 2300gas 供调用，防止重入攻击；send 发送失败时会返回 false；只会传递 2300gas 供调用，防止重入攻击；call.value 发送失败时会返回 false；传递所有可用 gas 进行调用（可通过传入 gas_value 参数进行限制），不能有效防止重入攻击。

如果在代码中没有检查以上 send 和 call.value 转币函数的返回值，合约会继续执行后面的代码，可能由于 Ether 发送失败而导致意外的结果。

04 错误使用随机数

智能合约中可能需要使用随机数，虽然 Solidity 提供的函数和变量可以访问智能合约审计报告明显难以预测的值，如 block.number 和 block.timestamp，但是它们通常或者比看起来更公开，或者受到矿工的影响，即这些随机数在一定程度上是可预测的，所以恶意用户通常可以复制它并依靠其不可预知性来攻击该功能。

05 事务顺序依赖

由于 mint 总是通过代表外部拥有地址（EOA）的代码获取 gas 费用，因此用户可以指定更高的费用以便更快地开展交易。由于以太坊区块链是公开的，每个人都可以看到其他人未决交易的内容。这意味着，如果某个用户提交了一个有价值的解决方案，恶意用户可以窃取该解决方案并以较高的费用复制其交易，以抢占原始解决方案。

06 拒绝服务攻击

在以太坊的世界中，拒绝服务是致命的，遭受该类型攻击的智能合约可能永远无法恢复正常工作状态。导致智能合约拒绝服务的原因可能有很多种，包括在作为交易接收方时的恶意行为，人为增加计算功能所需 gas 导致 gas 耗尽，滥用访问控制访问智能合约的 private 组件，利用混淆和疏忽等等。

07 逻辑设计缺陷

业务逻辑设计缺陷主要指与 Web3 业务设计相关的安全问题，不仅局限于网络层、系统层、代码层等比如登录验证的绕过、交易中的数据篡改、接口的恶意调用（文件上传就是调用后台的 API），都属于业务逻辑漏洞。需要针对业务逻辑进行安全建模，对重要业务场景的各个业务模块逐一进行业务流程梳理，从前台到后台、业务和支撑系统等不同维度进行分析，识别个业务模块的业务逻辑、业务数据流和功能字段等。

08 假充值漏洞

在虚拟资产合约的 transfer 函数对转账发起人 (msg.sender) 的余额检查用的是 if 判断方式，当 balances[msg.sender]<value 时进入 else 逻辑部分并 returnfalse，最终没有抛出异常，我们认为仅 if/else 这种温和的判断方式在 transfer 这类敏感函数场景中是一种不严谨的编码方式。

09 增发虚拟资产漏洞

主要指初始化虚拟资产总量后，虚拟资产合约中是否存在可能使虚拟资产总量增加的函数。

10 冻结账户绕过

主要指虚拟资产合约中在转移代币时，是否存在未校验虚拟资产来源账户、发起账户、目标账户是否被冻结的操作。

在历次的安全事故中，智能合约的漏洞引发在安全问题上占了较多的比重。主要的智能合约的安全漏洞类型，如表 5-1 所示：

类型	数量	占比
权限控制	178925	46.97%
逻辑设计缺陷	61798	16.22%
Call 函数安全	41268	10.83%
错误使用随机数	33809	10.38%
条件竞争	13602	3.57%
事务顺序依赖	9488	2.49%
重入攻击检测	2743	0.72%
冻结账户绕过	1593	0.42%
数值溢出	0	0．00%

表 5-1 智能合约安全漏洞分布图

Web3 合约安全风险的应对策略

01 Web3 智能合约的安全审计

Web3 智能合约往往被用来管理大量的用户虚拟资产和有价凭证，然而大多数 Web3 项目为了增加可信度和透明性，对其项目代码进行开源管理，这样使得项目更容易收到攻击。Web3 智能合约开发者在实现业务功能之外，额外学习大量的安全编码规范，已有漏洞问题、虚拟机安全版本等的成本过高。因此行业中细分出来第三方 Web3 智能合约审计机构，专门对 Web3 智能合约安全进行深度审计。接受专业审计机构的合约代码验证，也可以有效规避合约代码的潜在安全风险。

02 Web3 智能合约的加密

Web3 智能合约不能被第三方明文读取，以此减少 Web3 智能合约因逻辑上的安全漏洞而被攻击。此方法成本较低，但无法用于开源应用。

03 Web3 智能合约的规范设计

根据应用的实际业务逻辑总结 Web3 智能合约优秀模式，开发标准智能合约模板，以一定标准规范智能合约的编写可以提高智能合约质量和安全性。Web3 智能合约往往涉及各种的密码协议和算法实现。在实际应用中需要注意随机数来源是否可靠以及私钥存储安全。

04 Web3 智能合约的升级和恢复

尽量避免在 Web3 智能合约出现漏洞的同时，我们也有必要在 Web3 智能合约中引入发现漏洞时的应急方案。合约暂停恢复和合约升级是两种常见的应急方案。合约的恢复暂停使得合约的管理者可以在发现漏洞的情况下暂停合约的主要功能，并在合适的时间重新恢复合约的功能。合约升级使得合约的管理者可以将当前合约的使用者迁移到已修改漏洞的新合约上。无论采用什么样的应急机制，都需要保证该机制的实现本省没有漏洞，并且只能在受限的情况下被使用。

05 Web3 智能合约的形式化验证

Web3 智能合约形式化验证的含义是根据某个或某些规范或属性，使用数字的方法证明其正确性或非正确性。形式化验证是一个系统性的过程，将使用数学推理来验证设计意图（用户功能需求）在实现（智能合约）中是否得意正确贯彻。

06 防范拒绝服务攻击

由于 Web3 项目的去中心化特性，一个 Web3 智能合约可能需要在多个节点上独立运行，以达成对该 Web3 智能合约运行结果的共识。如果虚拟机中存在可以被 Web3 智能合约触发的拒绝服务漏洞，攻击者就可以通过部署恶意合约瘫痪部分甚至整个 Web3 项目。因此，虚拟机的设计和实现中需要防范此类拒绝服务漏洞。同时，也需要结合区块链技术优势设计防范拒绝服务攻击。

07 防范虚拟机逃逸

虚拟机逃逸是指恶意智能合约可以利用虚拟机逃逸漏洞脱离虚拟机的控制，访问甚至控制虚拟机本身所处的运行环境，进而可以访问和控制其他合约在该虚拟机上的运行。攻击者如果通过虚拟机逃逸漏洞进一步控制 Web3 项目网络中的大多数节点，甚至可以发起 51% 攻击。因此，虚拟机设计和开发中需要尤其关注此类逃逸漏洞。

08 多个 Web3 智能合约运行环境的强隔离

无论采用什么样的虚拟机实现模型，虚拟机，特别是强调隐私保护的 Web3 项目上的虚拟机，需要保证在同时运行多个智能合约时，各个合约的运行环境的相互隔离。例如，不存在测信道使得一个合约可以探测另一个合约的敏感行为，不存在测信道使得一个合约可以影响另一个合约的运行。

Web3 典型合约安全事件剖析

01 EulerFinance 安全事件

事件概要

3 月 13 日，Ethereum 链上的借贷项目 EulerFinance 遭到闪电贷攻击，损失达到了 1.97 亿美元。3 月 16 日，Euler 基金会悬赏 100 万美元以征集对逮捕黑客以及返还盗取资金有帮助的信息。

3 月 17 日，EulerLabs 首席执行官 MichaelBentley 发推文表示，Euler“一直是一个安全意识强的项目”。从 2021 年 5 月至 2022 年 9 月，EulerFinance 接受了 Halborn、Solidified、ZKLabs、Certora、Sherlock 和 Omnisica 等 6 家区块链安全公司的 10 次审计。

3 月 18 日至 4 月 4 日，攻击者开始陆续返还资金。期间攻击者通过链上信息进行道歉，称自己“搅乱了别人的钱，别人的工作，别人的生活”并请求大家的原谅。4 月 4 日，EulerLabs 在推特上表示，经过成功协商，攻击者已归还了所有盗取资金。

漏洞分析

在本次攻击中，Etoken 合约的 donateToReserves 函数没有正确检查用户实际持有的虚拟资产数量和捐赠后用户账本的健康状态。攻击者利用这个漏洞，捐赠了 1 亿个 eDAI，而实际上攻击者只质押了 3000 万个 DAI。

由于捐赠后，用户账本的健康状态符合清算条件，借贷合约被触发清算。清算过程中，eDAI 和 dDAI 会被转移到清算合约。但是，由于坏账额度非常大，清算合约会应用最大折扣进行清算。清算结束后，清算合约拥有 310.93M 个 eDAI 和 259.31M 个 dDAI。

此时，用户账本的健康状态已恢复，用户可以提取资金。可提取的金额是 eDAI 和 dDAI 的差值。但池子中实际上只有 3890 万 DAI，所以用户只能提取这部分金额。

02 BonqDAO 安全事件

事件概要

2 月 1 日，加密协议 BonqDAO 遭到价格操控攻击，攻击者铸造了 1 亿个 BEUR，然后在 Uniswap 上将 BEUR 换成其他虚拟资产，ALBT 价格下降到几乎为零，这进一步引发了 ALBT 的清算。按照黑客攻击时的虚拟资产价格，损失高达 8800 万美元，但是由于流动性耗尽，事件实际损失在 185 万美元左右。

漏洞分析

本次攻击事件攻击者共进行了两种方式的攻击，一种是控制价格大量借出虚拟资产，另一种是控制价格清算他人资产从而获利。

BonqDAO 平台采用的预言机使用函数‘getCurrentValue’，而不是‘getDataBefore’。

黑客通过质押 10 个 TRB（价值约 175 美元）成为了价格报告者，并通过调用 submitValue 函数修改预言机中 WALBT 的价格。价格设置完成后，攻击者调用 Bonq 合约的 createTrove 函数，创建 trove 合约，并向该合约中抵押了 0.1 个 WALBT 进行借款操作。正常来说，借款额度应该是小于 0.1 个 WALBT 的价格，从而保证抵押率维持在一个安全的范围，但是在本合约的借贷过程中，计算抵押物价值的方式是通过 TellorFlex 合约来进行实现的。而在上一步，攻击者已经把 WALBT 价格拉得异常高，导致攻击者在本次借款中，借出了 1 亿枚 BEUR。

攻击者在第二笔交易中将 WALBT 价格设置得异常低，从而使用少量的成本将其他用户所抵押的 WALBT 清算出来。

03 PlatypusFinance 安全事件

事件概要

2 月 17 日，Avalanche 平台的 PlatypusFinance 因函数检查机制问题遭到攻击，损失约 850 万美元。然而攻击者并没有在合约中实现提现功能，导致攻击收益存放在攻击合约内无法提取。2 月 23 日，Platypus 表示，已经联系了 Binance 并确认了黑客身份，并表示将至少向用户偿还 63% 的资金。2 月 26 日，法国国家警察已经逮捕并传唤了两名攻击 Platypus 的嫌疑人。

漏洞分析

攻击原因是 MasterPlatypusV4 合约中的 emergencyWithdraw 函数检查机制存在问题，仅检测了用户的借贷额是否超过该用户的 borrowLimitUSP（借贷上限），而没有检查用户是否归还债务的情况。

攻击者首先通过 AAVE 合约闪电贷借出 4400 万枚的 USDC 存入 Pool 合约中，然后 mint 了 4400 万枚 LP-USDC。接着攻击者调用 borrow 函数借出了 4179 万枚 USP，下一步立马调用了 EmergencyWithdraw 函数。在 EmergencyWithdraw 函数中有一个 isSolvent 函数来验证借贷的余额超过可借贷最大值，返回 true 就可以进入 transfer 操作，而没有考虑验证负债金额是否已经偿还的情况。所以攻击者可以在没有偿还债务的情况下直接调用成功提取出之前质押的 4400 万枚 LP-USDC。攻击者在第二笔交易中将 WALBT 价格设置得异常低，从而使用少量的成本将其他用户所抵押的 WALBT 清算出来。

04 YearnFinance 安全事件

事件概要

2023 年 4 月 13 日，YearnFinance 的 yusdt 合约遭受黑客闪电贷攻击，黑客获利超 1000 万美元。yUSDT 疑似在 1000 多天前部署时便被错误配置，错误地使用了 FulcrumiUSDC 部署，而不是 FulcrumiUSDT。5 月 26 日，Yearn 攻击者已将 4134 枚 ETH 转入 TornadoCash。

漏洞分析

本次攻击主要利用了 yUSDT 虚拟资产合约配置错误，在进行 rebalance 重新选择池子的时候，仅使用了 USDT 作为添加数量，而 USDC 无法添加池子，从而导致了攻击者使用 USDC 将该合约所有 USDT“消耗掉”后，池子余额变为了 0，从而铸了大量的虚拟资产。

05 MEVbot 安全事件

事件概要

2023 年 4 月 3 日，MEV 机器人遭受恶意三明治攻击，损失约 2500 万美元。三明治攻击（sandwichattacks）是 DeFi 里流行的抢先交易技术的一种。为了形成一个“三明治”交易，攻击者会找到一个待处理的受害者交易，然后试图通过前后的交易夹击该受害者。这种策略来源于买卖资产从而操作资产价格的方法。三明治交易的目标是利用意外受害者的滑点，同时也有许多诱饵机器人反过来利用 MEVBot 的策略，例如恶意的诱饵虚拟资产，或者转账函数中特殊的金额指定等，而本次攻击利用了 MEVBot 相关漏洞。

漏洞分析

恶意节点利用 MEV-boost-relay 相关漏洞，然后通过恶意三明治攻击价格操纵并最终获利。正常情况下恶意提议者很难修改 bundles，这是因为双签惩罚，但是攻击 parent_root 和 state_root 被恶意设置为 0x00，会导致 PublishBlock 返回 error，但是由于旧版本没有对返回的 error 进行处理，从而获取已经披露的 Bundles，才导致了事件的发生。

攻击者首先将目标瞄准到流动性很低的池子，并试探 MEV 机器人是否会抢跑交易。攻击者试探成功之后使用预先在 UniswapV3 中兑换出来的大量虚拟资产在低流动性的 V2 池内进行兑换操作，勾引 MEV 使用全部的 WETH 进行抢跑购买不值钱的虚拟资产。然而被抢跑的交易其实才是瞄准了 MEV 的攻击交易，使用了大量的虚拟资产换出 MEV 刚刚进行抢跑的所有 WETH。这时由于 MEV 进行抢跑的 WETH 已经被攻击交易兑换出来，所以 MEV 机器人想要重新换回 WETH 的操作会执行失败。

Web3 安全产业发展情况

全球 Web3 安全产业刚刚兴起，还未形成较大规模和成熟的商业模式，但我们仍看到了各方对 Web3 安全产业的探索和热情。从国家层面的政策支持，到组织机构的标准引领，从资本市场的投资推动，到各家企业的应用探索，都推动了 Web3 安全产业雏形的形成。

国家政策对 Web3 安全产业的支持

01 产业领军国家积极推动 Web3，意图保持国际领先地位

以美国和新加坡为代表的国家利用其在互联网行业和资本市场活跃度上的领先优势，引领全球 Web3 安全产业发展。

在技术产业方面，美国产生了超过一半以上的 Web3 项目，美国开源社区衍生出一批 Web3 安全验证技术。政府对 Web3 安全的研发和政策支持已延伸到数字交易系统、海关贸易、运输管理、边境保护、网络安全保护等多个领域。新加坡被媒体誉为“全球 Web3 创业工厂”，在金融创新和科技创新方面采取了非常开放的态度，尤其是 Web3 安全方向，吸引了大量技术人才和投资者到新加坡发展。

在金融监管方面，美国和新加坡对 Web3 呈现积极态度。美国证券交易委员会（UnitedStatesSecuritiesandExchangeCommission，SEC）承担 Web3 虚拟资产相关监管职责，各州颁布法案加快 Web3 安全应用研究力度，并寻求主导 Web3 安全标准研制，积极抢占 Web3 安全领域制高点。新加坡金融管理局为以 Web3 为核心的金融科技创新创业企业专门发放虚拟资产许可牌照，并提供“监管沙盒、产业沙盒、技术沙盒”政策，允许在新加坡进行金融安全创新试验。

02 产业发达国家紧密跟进 Web3，试图抓住机遇占据优势

以日本和欧盟为代表的国家在产业发展变革中并未占据主导地位，拟依托当前的产业版图，抓住 Web3 新机遇，赢得行业领先地位。

欧洲国家正在积极改变过去安全发展中“小国”众多、难以形成共识的局面，寻求区域联合、协同发展的路径。欧洲自开始建设安全基础服务设施起，已获得 30 个欧洲国家支持，在欧洲范围内开发跨境区块链安全服务。2023 年欧洲数字计划持续推进关于安全基础服务设施的服务创新、安全标准和数字身份等计划，持续推动 Web3 安全技术支撑。

日本政府作为最早颁发虚拟资产交易所牌照的国家，也对 Web3 安全产业展现出浓厚兴趣。日本众议院近期表示 Web3 整合了元宇宙和 NFT 等新的数字服务，有望为日本带来经济增长，尤其是在游戏、动漫、动画等与日本文化密切相关的领域发展全球业务。日本安全技术机构迫切需要研究 Web3 安全保障技术，为实现去中心化的数字社会进行必要安全保障。

03 产业滞后国家积极拥抱 Web3，尝试利用改革扭转格局

对于互联网和经济尚未得到充分发展的国家，转型成本较低，通过制定激进的虚拟资产激励策略，可绕过西方支配的中心化基础设施，重建经济基础设施。

用户价值捕获和金融基础设施成为了产业相对滞后等国家进入 Web3 的最佳切入点。去中心化内容聚合平台 Jambo 通过视频广告、媒体内容、游戏等服务让用户在使用过程中能够“赚钱”，赢得了海量非洲用户。产业相对滞后国家的金融基础设施让 Web3 金融应用在移动支付、资产管理、借贷、抵御通货膨胀等场景中发展迅速。在此过程中，如何有效的保障 Web3 金融应用至关重要，Web3 安全保障需求急聚而生。

04 我国正探索中国特色 Web3，平衡趋势和风险

我国针对 Web3 行业的监管持续发力，但也高度重视 Web3 在产业发展方面的积极作用，逐渐形成一条“技术服务实体、安全标准两翼齐飞”的融合化发展路径。

我国不仅将区块链写入“十四五”规划纲要，统筹布局，加快推动区块链技术和产业创新发展。近期，更是从我国基本国情出发，相关部委组织研讨 Web3 引导政策，强调各领域与 Web3 紧密结合，各部委以及多省市、直辖市、特别行政区持续加大 Web3 政策支持力度，全方位推动 Web3 技术赋能实体经济，形成 Web3 行业平台和创新应用，构建 Web3 安全产业生态体系。

同时，香港特区政府发布《有关香港虚拟资产发展的政策宣言》，政策宣言指出香港特区政府正与金融监管机构合作，创造一个便利的 Web3 创新创业发展环境，以促进香港虚拟资产行业的可持续和负责任的发展。

标准组织对 Web3 安全产业的引领

01 网络领域组织主导数字身份等核心标准，持续保持行业影响力

W3C 仍是 Web3 领域最具权威和影响力的国际标准机构。在 Web3 方面 W3C 主要聚焦数字身份 DID、可验证凭证 VC、安全验证等标准，以持续保持行业影响力。

2021 年 8 月，W3C 发布 DID 技术标准和实施指南，其中 DID 去中心化发行、DID 不依赖底层组织的持久性运营、DID 控制权及其关联信息的加密可验证性、DID 元数据的可解析性构成了 DID 规范的主要支柱。

2022 年 7 月，DID 正式成为官方 Web3 标准，预示着赋予个人和组织对其数据拥有更好的控制权、安全性和隐私保护的时代即将到来。2023 年 3 月，W3C 着力推动 DID 与 VC 相结合，正在多个需要数据真实性和识别的市场中使用，典型应用如美国、加拿大和欧盟正在探索基于用户 DID 的数据共享和访问机制，并引导行业安全机构共同探索 DID 安全集成验证环境。

02 工程领域机构聚焦 Web3 配套实现标准，试图抓住产业新机遇

互联网不仅仅是 TCP/IP 技术，而基于 TCP/IP 协议构建的因特网成为了最主要的互联网实践，Web3 也不仅仅是区块链技术，但基于区块链构建的数字身份和数字资产很可能成为最主要的 Web3 实践。互联网工程任务组（IETF）作为汇聚互联网架构设计、开发、运营者等在内的大型开放社区，专门成立去中心化互联网基础设施工作组研制 Web3 配套实现的相关标准，内容涉及交易协议、网关用例、安全架构等。虽然标准均在草案阶段，但足以看出 IETF 在 Web3 领域探索的决心。

03 开源社区等平台探索 Web3 场景应用，已形成事实性标准

2023 年 Web3 开发人数和活跃度均达到历史高点，月均活跃达到 2.62 万人，对全球 Web3 产业发展贡献巨大。大多数 Web3 项目已逐步形成开源社区治理机制，可通过提案投票等形式推行改进方案，持续提升服务能力。如以太坊开源社区的改进提案（EIP）已评议超过四千多条标准提案，逐步演进形成以太坊应用标准，其中同质化通证标准（ERC20）、非同质化通证标准（ERC721）被很多开源社区广泛使用，Mythril 以太坊智能合约安全分析工具也已成为事实性标准。

资本市场对 Web3 安全产业的推动

01 Web3 投资规模持续扩大，产业投资成果初步显现

纵观全球投资数据，2023 年全球 Web3 投资迎来爆发式增长，尤其是以香港为代表的 Web3 友好市场的加持下，全球 Web3 项目投资火热。在投资数量方面，2023 年上半年 Web3 投资数量相较 2022 年迎来较大增幅，共计发生约 500 起。在投资金额方面，2023 年上半年 Web3 投资金额超过 43 亿美元，受行业周期影响，相比 2022 年获得融资的总额下滑较多。

02 Web3 基础设施持续投入，投资标的追逐行业热点

2020 年起至今，不同领域中的各类 Web3 项目投资持续增长。在基础设施领域，Web3 基础设施和安全服务作为投资的长青领域持续存在，2023 年和 2022 年投资金额增长明显。

在金融科技领域，Web3 去中心化金融投资从 2020 年开始爆发，多为初创型企业围绕数字资产、交易协议、衍生工具和安全服务进行科技金融创新。

在文化创意领域，数字藏品 NFT 项目作为 2022 年最大的行业热点，2023 年呈现国内外两极分化局面，相较海外的风生水起，国内已逐步降温。但不得不说，自 2021 年异军突起以来，Web3 数字文化产业，从无到有发展迅速。

03 传统投资机构布局 Web3，新型投资形式不断涌现

一方面，专门成立针对 Web3 市场的虚拟资产基金，让整个行业的投资规模水涨船高。随着 Web3 的火热和虚拟资产价格在近几年间的不断攀升，早期在投资领域试水的红杉和高盛等传统投资机构开始逐渐全面拥抱 Web3 投资，推出数亿美元投资基金。以 a16z 为代表的部分投资机构率先进入 Web3 投资领域，并获得了大量行业早期发展红利，迅速成为行业投资风向标。

另一方面，去中心化融资为 Web3 投资带来了新模式。为了摆脱项目被中心化资本方的过度控制，尽可能实现分布式的投资过程和治理权利，以 SushiSwapMISO 为代表的首次去中心化交易发行（IDO）和以 Gitcoin 为代表的社区融资模式迅速走红，成为小型 Web3 创业项目的首选。这种新型融资模式让普通投资人和社区支持者能够参与 Web3 投资并以加密货币的形式获得回报，为项目发展构建了更加去中心化的资本格局。

企业应用在 Web3 安全产业的探索

01 互联网龙头企业提前布局 Web3，抢占平台设施先机

以传统互联网技术服务巨头为代表的谷歌和亚马逊，正在积极布局成为 Web3 基础设施和安全技术服务商。2022 年 5 月，谷歌宣布组建 Web3 团队，将目光瞄向了 Web3 世界的基础设施服务提供商，通过为 Web3 开发人员提供全栈服务的方式，以及 Web3 安全仿真验证环境，降低开发人员设计去中心化系统的门槛。

亚马逊的 AWS 服务目前是 Web3 应用最为常见的云计算服务平台，通过全球化的基础设施、强大的网络算力、云中数据湖仓、AI/ML 工具等产品和服务，亚马逊为 Web3 开发者提供可满足业务所需的超低延迟、虚实结合、去中心化、安全可信的 IT 架构等解决方案。

02 中小型初创公司转型进入 Web3，探索安全应用场景

随着 Web3 创业浪潮的到来，在资本市场推动下，Web3 领域涌现出独角兽级应用和安全服务，带动了周边应用场景的快速发展。

一方面，以提高虚拟资产流动性为目的形成多家虚拟资产交易平台，总市值高达数千亿美元。以 UniSwap 为代表的去中心化交易平台，因其创新性的交易协议，迅速成为虚拟资产市场主流的去中心化交易应用，在第三方安全审计机构的加持下，持续构建新型去中心化金融发展格局。

另一方面，得益于数字文化 NFT 市场的快速发展，逐渐形成围绕“DID+NFT+DAO+ 行业”的组合应用模式和服务平台。以 Opensea 为代表的 NFT 交易平台，以及以 YugaLabs 为代表的 NFT 发行平台，迅速成为最热门的 NFT 项目。区块链游戏 AxieInfinity 以其独特的边玩边赚模式和开放经济系统成为范式级 Web3 项目。

03 跨行业组织机构积极参与 Web3，寻找新型产业机会

Web3 不仅为产业带来应用场景革新，还对现有产业带来了全新赋能机会，文化创意和游戏元宇宙成了最佳切入点。

一方面，数字藏品业务在国内持续火热，包括阿里、腾讯等互联网企业纷纷推出自己的区块链和数字藏品平台，并联合文化创意领域发行方，发行多种多样的数字藏品。随着市场泡沫不断被挤出，数字藏品逐渐“脱虚向实”，创作者经济、数字商品凭证均有着广阔前景。

另一方面，消费市场开启元宇宙布局，Meta 正积极研发区块链、NFT、加密货币支付、社交化金融 SocialFi，致力于构建去中心化的社交网络元宇宙；苹果、英伟达等消费电子巨头则在增强现实 AR 领域持续发力，在软硬件生态系统中不断完善 AR 技术和增强现实应用场景，为更多元宇宙概念的游戏、应用打造平台。

Web3 安全态势小结

01 全球 Web3 行业虚拟资产总市值在今年有所下降，但整体资产数量正不断扩大。据 investing 数据统计，2023 年，全球 Web3 行业虚拟资产总市值最高达 1.28 万亿美元，受行业爆雷事件影响，相比去年最高总市值 2.2 万亿美元，今年有所下降，但整体资产数量规模正在不断扩大。

02 Web3 安全事件和去年同期相比数量有所下降。据 FootprintAnalytics 数据统计，2023 年上半年 Web3 安全事件共发生 338 起，总损失达到了 6 亿 5561 万美元。相比 2022 年同期的 431 起安全事件，今年降低了 93 起。

03 DeFi（分布式金融）依旧是被攻击频次最高、损失金额最多的类型。85 次 DeFi 安全事件总损失金额达到了 2.92 亿美元，占总损失金额的 62%。

04 约有 75.6% 的损失金额来自以太坊，为 3.56 亿美元，居所有 Web3 链平台的第一位。

05 最频发、造成损失最多的攻击手法为智能合约漏洞利用。其中，重大智能合约发生安全事件 60 次，造成损失 2.64 亿美元，占所有损失金额的 56%。

参考链接 Reference

▲ CNVD 安全公告，https://www.cnvd.org.cn/webinfo/list?type=14

▲ CNNVD 漏洞通告，https://www.cnnvd.org.cn/home/warn

▲ 已经被利用漏洞（KEV）目录，https://www.cisa.gov/known-exploited-vulnerabilities-catalog

▲ CISA “2023-2025 年战略计划”，https://www.cisa.gov/strategic-plan

▲ 漏洞披露策略（VDP）https://www.cisa.gov/resources-tools/resources/vulnerability-disclosure-policy-vdp-platform-fact-sheet

▲ CISA《约束性操作指令 (BOD) 22-01》，https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

▲谷歌零号计划，https://googleprojectzero.blogspot.com/p/0day.html

▲ MORPHISEC，不要对新的 ProxyShellMiner 活动麻木不仁，https://blog.morphisec.com/proxyshellminer-campaign

▲安天集团，活跃的 hoze 挖矿木马分析 https://mp.weixin.qq.com/s/-mZD0pPbeIgxoTUNNFBnrw

▲ CYBLE，Money Message 勒索软件疑似利用窃取者日志，https://cyble.com/blog/demystifying-money-message-ransomware/

▲ Cisco Talos，新确定的 RA 集团利用泄露的 Babuk 源代码危害美国和韩国的公司，https://blog.talosintelligence.com/ra-group-ransomware/

▲ Akamai 安全情报响应团队，揭秘 HinataBot：深入探讨基于 Go 的威胁，https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet

▲ FortiGuard 实验室，AndoryuBot – 新的僵尸网络活动针对 Ruckus 无线管理远程代码执行漏洞 (CVE-2023-25717)，https://www.fortinet.com/blog/threat-research/andoryubot-new-botnet-campaign-targets-ruckus-wireless-admin-remote-code-execution-vulnerability-cve-2023-25717

▲ Zscaler，Pikabot 技术分析，窥视恶意软件后门，https://www.zscaler.com/blogs/security-research/technical-analysis-pikabot

▲ AT&T，SeroXen RAT for sale，https://cybersecurity.att.com/blogs/labs-research/seroxen-rat-for-sale

▲ FortiGuard 实验室，RapperBot DDoS 僵尸网络扩展到加密货币劫持，https://www.fortinet.com/blog/threat-research/rapperbot-ddos-botnet-expands-into-cryptojacking

▲ 工业和信息化部办公厅关于公布工业领域数据安全管理试点典型案例和成效突出地区名单的通知 https://www.miit.gov.cn/jgsj/waj/wjfb/art/2023/art_b0ac4edb14b64b438d59b530547a7316.html

▲ 个人信息跨境流动法治化取得新成果，http://www.cac.gov.cn/2023-03/07/c_1679832118689585.htm

▲ XSS: The Top Russian Dark Web Forum，https://webz.io/dwp/xss-the-top-russian-dark-web-forum/

▲ 8Base ransomware group leaks data of 67 victim organizations，https://www.helpnetsecurity.com/2023/06/28/8base-ransomware/

▲ Top Cybercrime Forums to Monitor in 2023，https://flare.io/learn/resources/blog/top-cybercrime-forums/

▲ 韩国 PIPC 发布 2023 年工作计划，将跨境数据传输作为重点领域之一，https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=8550

▲ EDPB 发布《关于欧盟 - 美国数据隐私框架充分性决定草案的意见》https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en

▲ UAC-0114 (Winter Vivern) 组织与乌克兰和波兰国家机构相关的活动 (CERT-UA#5909)，https://cert.gov.ua/article/3761023

▲ Shuckworm APT IOC，https://1275.ru/ioc/2192/shuckworm-apt-iocs/

▲ 俄罗斯 APT29 的演变——新的攻击和技术被发现，https://www.avertium.com/resources/threat-reports/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered

▲ 进击的安全巨头：地球龙智携新花样回归，https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html

▲ Stealing the LIGHTSHOW (Part Two) — LIGHTSHIFT and LIGHTSHOW，https://www.mandiant.com/resources/blog/lightshift-and-lightshow

▲ 利用向日葵漏洞传播带有 BYOVD 的 Sliver 恶意软件，https://asec.ahnlab.com/en/47088/

▲ SCATTERED SPIDER 利用 Windows 安全缺陷，通过自带易受攻击的驱动程序策略来尝试绕过端点安全，https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/

▲ 恶意广告用作 BlackCat 的入口媒介，演员还利用 SpyBoy Terminator，https://www.trendmicro.com/en_fi/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-lever.html

▲ “AuKill”EDR 杀手恶意软件滥用 Process Explorer 驱动程序，https://news.sophos.com/en-us/2023/04/19/aukill-edr-killer-malware-abuses-process-explorer-driver/

▲ 马尔维特 | .NET 虚拟化在恶意广告攻击中蓬勃发展，https://www.sentinelone.com/labs/malvirt-net-virtualization-thrives-in-malvertising-attacks/

▲ Spyboy 防御规避工具在线广告 https://www.reddit.com/r/crowdstrike/comments/13wjrgn/20230531_situational_awareness_spyboy_defense/

团队介绍 Team

工业和信息化部电子第五研究所（中国赛宝实验室）

工业和信息化部电子第五研究所

工业和信息化部电子第五研究所（中国赛宝实验室）（以下简称“电子五所”），始建于 1955 年，是工业和信息化部的直属事业单位，中国最早从事可靠性与环境适应性研究的权威机构。围绕“支撑政府的智库、服务行业的平台、质量可靠性技术的引领者”的发展定位，致力于面向政府、社会和企业，提供行业研究、政策咨询、认证计量、试验检测、分析评价、数据服务、软件评测、信息安全、标准信息、工程监理、节能环保、可靠性工程、专用设备、软件研发和技术培训等专业服务，是国家工业和信息化领域制造强国、质量强国、网络强国和数字中国的支撑单位。在网络安全方面，电子五所是国家网络安全智库单位，全国首批网络安全等级保护测评机构和商用密码应用安全性评估机构，长期开展网络和信息安全技术研究，可提供电子政务网络和信息安全服务、工业控制系统网络和信息安全服务、网络安全等级保护测评服务、商用密码应用安全性评估服务、数据安全与个人信息安全评估服务、网络安全攻防综合服务、装备网络安全试验、漏洞挖掘、数据治理与数据入表等网络与信息安全相关业务。

SANGFOR 深信服科技

深信服千里目安全技术中心

深信服千里目安全技术中心专注网络安全各技术领域研究及应用，囊括六大技术实验室和一个创新研究院，聚焦国内外漏洞、攻防对抗技术、终端安全、高级威胁、威胁情报等安全技术领域专业研究，最终赋能于产品。

目极千里 洞见安全

识别左侧二维码

关注深信服千里目公众号

参编人员 Editorial staff

工业和信息化部电子第五研究所：

卢列文 李 帅 云 雷 相里朋 魏光辉 穆帅先 莫泳聪 王 帆 杨学武 刘茂珍

深信服科技股份有限公司：

周 欣 王振兴 叶润国 安东冉 禹廷婷 侯庆茹