安天 ANTIY

2022 网络安全威胁的回顾与展望

Antiy Annual Security Report

导语

数字经济是未来发展的方向。习近平总书记在党的二十大报告中指出，“加快发展数字经济，促进数字经济和实体经济深度融合”。在百年变局加速演进、世纪疫情持续冲击、国际局势复杂动荡的大背景下，网络安全行业应建立为保障数字经济发展的实战化、体系化、常态化的安全屏障，网络安全企业需要利用自身的安全产品体系来解决数字数据的安全问题。

在每年冬训营上发布年报的预发布版，征求参会专家的意见建议，是安天多年坚持的传统。

在今年的年报中，安天总结了高级持续性威胁（APT）、勒索攻击、挖矿木马、僵尸网络、攻防对抗、数据泄露、工业互联网安全风险、威胁泛化等方向的思考与观点：

关于高级持续性威胁（APT）：安天梳理了 2022 年全球 APT 组织及行动的分布和活跃情况，制作了“全球 APT 攻击行动、组织归属地理位置分布（活跃）图”。

“俄乌冲突”使双方在网络空间中均遭受到了不同程度的损失。网络闪电战成为俄罗斯在“俄乌冲突”过程中的先行军。俄罗斯的作业习惯和技战术是先实施网络攻击，通过网络钓鱼成功针对网络基础设施等目标，最后是在传统动能武器的战场发起协同作战攻击。俄罗斯在网络战中高级攻击技术的应用，已在全球地缘政治活动中产生影响，促使包括俄乌在内的、全球范围内国家地区的地缘政治活动更为剧烈。

数字证据易篡改促使境外 APT 组织利用网络攻击栽赃构陷。2022 年 2 月，安天发布报告揭露了具有印度背景的 APT 组织暗象，发现该组织主要针对印度境内的社会活动人士、社会团体和在野政党等，同时也会窃取印度周边国家如中国和巴基斯坦等国军事政治目标的重要情报。攻击者将此结果密报当地警方前往目标的住宅突袭检查，当场查获这些构陷目的的违法信件作为论罪的数字证据。

利用物联网设备进行战场预置的 APT 攻击活动频繁。2022 年初，安天发现海莲花组织在针对我国的网络攻击活动中，预先通过弱口令爆破、漏洞攻击等手段攻陷遍布我国多处重要省市的公网路由器、摄像头等物联网设备充当跳板，安装流量转发工具，将 Torii 远控木马的窃密和控制流量经一层或多层跳板转发至真实的 Torii 远控服务器。

关于勒索攻击：勒索软件通常作为攻击组织以经济目的为由的犯罪工具，回顾 2022 年发生的勒索攻击事件，发现**部分勒索软件被具有国家背景的攻击组织作为“政治化”犯罪工具，用以实施网络攻击。**在俄乌冲突期间“政治化”勒索攻击案例频频发生并伴随着“破坏式”勒索软件再现，伪装成勒索攻击，但实际目标是破坏系统运行，从而实现网络空间攻击转化为物理空间影响。随着网络安全技术的不断创新和安全设备

筑起坚实的边界防护壁垒，威胁行为者在利用常见执行体传播方式无法实现入侵，雇佣受害目标内部人员实施网络攻击作为新手段。勒索策略也出现了新转变，从传统的勒索软件攻击“窃取+加密”转变为“窃取+删除或破坏”的攻击。跨平台勒索软件执行体帮助威胁行为者渗透到越来越复杂的网络环境中，在执行体分析上也给安全工作者带来了新的挑战。

关于挖矿木马：随着挖矿木马对抗技术的不断完善，越来越多的挖矿木马团伙掌握快速集成漏洞的能力。其连接矿池方式也更加隐蔽，传统情报矿池黑名单检测将逐渐失效。2022 年虚拟货币价格的下跌不仅没有减少恶意挖矿，反而更加活跃。

关于僵尸网络：2022 年全球政治局势不断变幻，利用僵尸网络发起具有政治意味的 DDoS 攻击已然成为大国之间对抗的主要手段；通过对 2022 年披露的漏洞利用情况进行统计后发现，僵尸网络正在积极地利用新出现的漏洞进行传播；采用 P2P 传播方式的僵尸网络在物联网设备间广泛传播。

关于攻防对抗：近年来，攻防对抗成本不对等的情况愈发明显，政企用户往往需要付出大量的网安建设和运营成本才能对抗急速提升复杂性的各类攻击面、难以掌控的供应链产品安全、新基建和信创产品带来的新暴露面和安全风险。但广泛滥用隐藏载荷的制式化网空装备无疑让攻防对抗成本变得更加不对等。与此同时，专业安全从业人员的短缺将持续推动安全运营领域自动化程度的发展，人工智能（AI）将在一系列产品中得到有力的利用，以更快的速度提供增强的安全成果。

关于数据泄露：2022 年，新冠疫情仍然肆虐全球，全球各行各业加快了数字化转型，数据的价值得到进一步凸显的同时，数据泄露也在持续高频发生。数据泄露事件不断地成为新闻热点，涉及的领域包括工业制造、政务、医疗、金融、交通等等，不一而足，面临的形势依然非常严峻。信息化程度越高的行业，数据泄露事件越多，且泄露所造成的危害越大。持续高频发生的数据泄露事件，使得全球数亿人的隐私和安全受到严重威胁。

关于工业互联网安全风险：近年来，我国积极布局工业互联网，在国家政策和市场需求的双重驱动下，我国工业互联网蓬勃兴起，多项应用逐步落地，市场规模不断扩大；在本年度中，工业互联网所面临的网络安全威胁也值得我们给予高度关注，包括但不限于：地缘政治局势紧张加剧，以俄乌冲突为代表的区域性军事冲突、以阿以冲突为代表的领土矛盾流血冲突爆发，其负面影响在一定程度上波及了工业互联网；全球范围内工业互联网基础设施脆弱性风险披露数量超百，且有关脆弱性风险可能导致的严重负面影响不容忽视；面对“Evil PLC Attack”等新型攻击场景风险，工业互联网各相关方应及时变通防御思路，尽快制定行之有效的针对性防御方案；对于“Industrial Spy（工业间谍）”这种与工业互联网安全具有相关性、以被盗数据交易为勾当的暗网市场出现及其发展，工业互联网各相关方也应给予必要的关注和对应防御措施的强化。

关于威胁泛化： 威胁泛化导致用户的资产暴露面增加，攻击者利用增加的攻击面可以产生非授权访问、跳板攻击、入侵“隔离网络”、资产被控、资产破坏、数据泄露等广泛的安全威胁。

1 高级持续性威胁（APT）

2022 年全球高级持续性威胁（APT）活动的整体形势依然非常严峻。基于安天持续监测的内部和外部的情报来源，2022 年全球公开安全研究报告数量 521 篇，其中披露的安全报告涉及 134 个 APT 威胁组织，2022 年新增 57 个 APT 威胁组织，2022 年针对中国的攻击活动不少于 67 次。安天梳理了 2022 年全球 APT 组织及行动的分布和活跃情况，制作了“全球 APT 攻击行动、组织归属地理位置分布（活跃）图”，其中 APT 组织共 490 个（由于图片空间有限仅展示主要攻击组织），根据图示可以发现其主要分布于美国、俄罗斯、印度、伊朗、朝鲜半岛、中东及部分国家和地区，部分组织由于情报较少未能确定归属国家或地区。

图 1-1 2022 年全球 APT 攻击行动、组织归属地理位置分布图

1.1 需要警惕更多的潜藏在网络空间深处的非知名 APT 组织

2022 年，安天跟踪全球 APT 相关报告 500 余篇，涉及 APT 组织 130 余个，其中新增 50 余个 APT 组织。通过研究历史报告发现，全球网络安全机构每年都会曝光披露新的 APT 组织，经过多年的积累后相比于典型的知名 APT 组织，一方面来说这些组织的数量已经非常之多，已经是数倍于典型知名组织；而另一

方面针对这些攻击组织深入研究和归因溯源的报告很少，安全机构和研究者对于他们的技战术、基础设施和幕后背景都缺乏了解；因此这些组织相对于典型知名组织更加复杂、神秘和隐蔽。也正因为如此，这些不知名的组织更需要我们的重视和警惕，他们可能长期潜伏不被发现从而造成相比知名组织更大的危害。

图 1-2 2022 年安天观测到的新增 APT 组织

对这些信息披露极少的非知名 APT 组织，虽然在大多数的情况下安全研究机构可以了解攻击者的一些信息，例如他们的母语或者位置信息，但剩下的缺失的线索信息可能会导致令人尴尬的归因错误或更糟的判断。由于大量的溯源技术报告被公开，身处在暗处的攻击者也在尽一切努力使用各种手段来保证不被发现，即使被捕获也确保不被归因，并尽可能减少留下痕迹。他们实施了多种技术，使分析研究变得更加困难。例如使用商业软件、渗透测试工具和无文件实体技术，通过放置虚假标记来误导安全研究人员，这些反溯源反取证技术会使组织归因成为一种运气。这也是为什么近些年安全研究人员经常能发现新组织的攻击活动，但鲜有挖掘出完整行动和背景归因的原因。未来的 APT 组织追踪与对抗之路，深入跟踪挖掘这些非知名组织也许更为重要。

1.2 网络闪电战成为俄罗斯在“俄乌冲突”过程中的先行军

网络闪电战，旨在探索网络部队与传统作战部队间的协作方式[1]。根据安全厂商 ESET 描述[2]，2022 年 2 月 23 日，针对多个乌克兰组织的使用 HermeticWiper 的破坏性网络攻击活动比其军事行动早了几个小时。根据恶意代码时间线可判断网络攻击已经计划了几个月。攻击者首先通过鱼叉式网络钓鱼等边界突破手段获取了 Active Directory 服务器权限，然后 HermeticWiper 通过默认域策略(GPO)部署。另外在内网里，与之相关的自定义蠕虫 HermeticWizard 通过 SMB 和 WMI 在受感染的网络中传播 HermeticWiper。2022 年 2 月 24 日，俄乌冲突爆发。针对乌克兰政府网络的第二次破坏性攻击开始了，这次投放了新的擦除器 IsaacWiper。目前根据现有威胁情报推断，IsaacWiper 可能是经由前期的入侵成功后横向移动传播的，或者是通过远程访问工具 RemCom 远程投放。

“俄乌冲突”使双方在网络空间中均遭受到了不同程度的损失。支持乌克兰的黑客组织 GhostSec（该组织长期以来一直作为 Anonymous 的一部分运营），此前曾控制过俄罗斯国家和军事组织的打印机。在 2022 年 7 月 20 日，GhostSec 通过编写 KillBus 的工具，用于针对 Modbus 设备的攻击。正如该软件的名称，通过提取信息、覆盖数据，然后将其用作从设备（Modbus 协议中的通信基于在客户端之间传递数据消息的原则），有效地破坏了水力发电厂的工业控制系统服务器，对发电厂系统的干预，随后导致俄罗斯 Gysinoozerskaya 水电站发生爆炸，导致电力计划随后紧急关闭、导致西伯利亚大片地区停电。GhostSec 声称对这次攻击负责。

俄罗斯的作业习惯和技战术是先实施网络攻击，通过网络钓鱼成功针对网络基础设施等目标，最后是在传统动能武器的战场发起协同作战攻击。同时善于利用其他 APT 组织的技战术发起网络攻击。如下图所示，彰显了俄罗斯网络与传统协同作战的特点。以具备俄罗斯国家背景的 STRONTIUMN（APT28）组织攻击活动为例，2022 年 3 月 4 日，STRONTIUMN 在乌克兰城市文尼察的核电公司的计算机网络上横向移动，随后俄罗斯军方袭击并占领了该公司最大的核电站。在同一周，STRONTIUMN 破坏了文尼察政府的计算机网络，两天后在文尼察市的机场发射了八枚巡航导弹[3]。

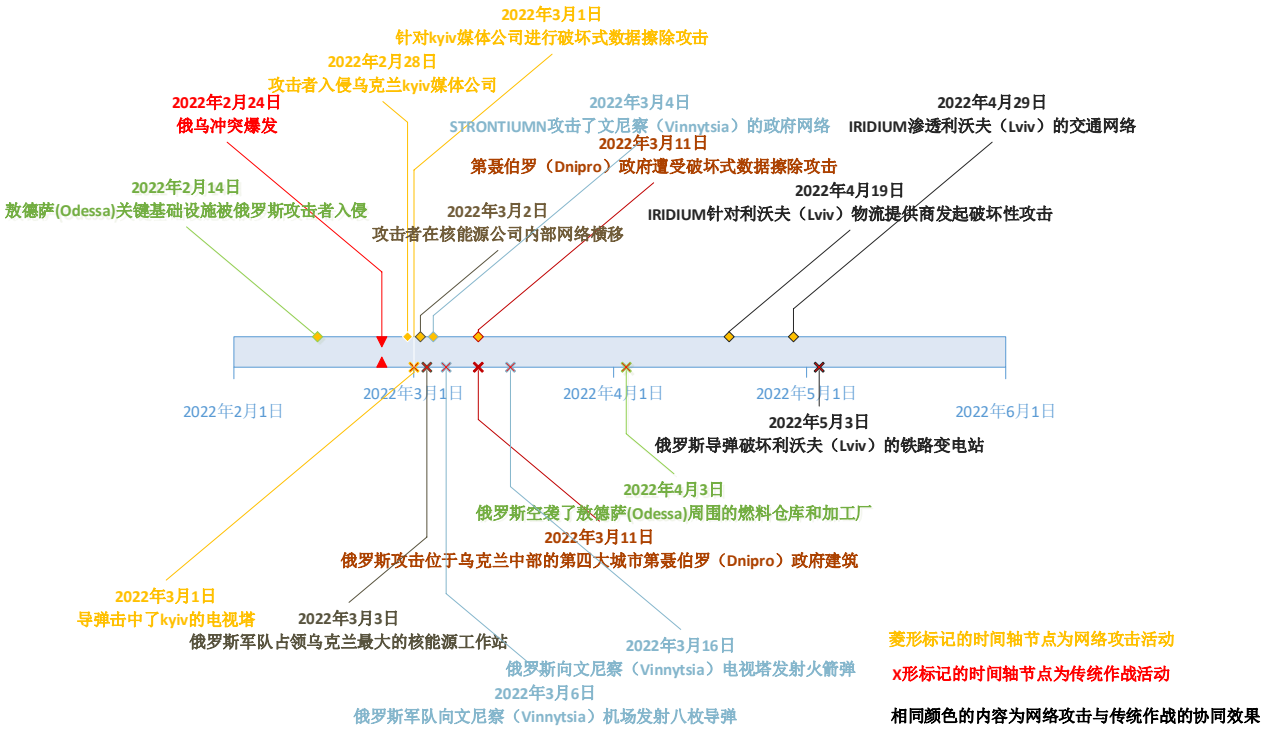


图 1-3 俄罗斯网络与传统协同作战[3]

1.3 俄罗斯在网络战中高级攻击技术的应用，已在全球地缘政治活动中产生影响

美国和欧盟声称，2022 年 2 月 24 日，俄罗斯对属于 Viasat 的名为 KA-SAT 的商业卫星通信网络发起了网络攻击[4]。Viasat 透露，网络攻击袭击了其 KA-SAT 网络，导致欧洲数以千计的调制解调器无法访问。网络攻击旨在破坏乌克兰的指挥和控制行动，并对包括德国、希腊、波兰、意大利和匈牙利在内的其他欧洲国家造成重大溢出影响。直到一个月后，欧洲卫星宽带服务才从事件中恢复。公司专家注意到，恶意代码发出破坏性命令覆盖调制解调器闪存中的关键数据，导致调制解调器无法访问网络，但并非永久无法使用。安全厂商 SentinelLabs 研究人员归因于名为“酸雨”(AcidRain)的新型擦除(wiper)恶意软件，为针对 KA-SAT 的商业卫星通信网络发起网络攻击的恶意代码。AcidRain 旨在远程清除易受攻击的调制解调器和路由器，SentinelLabs 观察到了 AcidRain 和 VPNFilter（VPNFilter 操作归咎于有俄罗斯背景的“FancyBear”又名 APT28 组织恶意软件之间的相似之处。随着欧美各国联盟声张保卫乌克兰的联合，俄罗斯情报机构加强了针对乌克兰境外盟国政府的网络渗透和间谍活动。

另一方面，俄罗斯利用 Konni 基础设施针对欧洲国家波兰、捷克共和国和其他国家的高价值目标的发起攻击。Securonix 威胁研究(STR)团队一直在调查使用一种新的基于 Konni 的恶意软件的攻击活动 STIFF#BIZON[5]。Konni 此前被归因于其他国家背景的 APT 组织远控木马。然而，STR 团队指出，此次攻击和历史数据的 IP 地址、托管服务提供商和主机名与 APT28 之间存在直接的关联。根据相关的威胁情报推

断，STIFF#BIZON 行动可能是 APT28 模仿 APT37 组织的技战术针对欧洲国家发起攻击。具体的技战术包括鱼叉式网络钓鱼成功之后，通过 PowerShell 执行第二阶段的恶意代码，相似的 UAC 技巧绕过，凭证访问窃取 Cookie，相似的 install.bat 安装方式等。但是在 STIFF#BIZON 行动中采用了更多高级的技战术，例如可离线破解 cookie 绕过 MFA、利用维基解密 Vault 7 中泄露的反调试技术通过系统文件 wusa.exe 提权执行恶意代码。

俄罗斯无论在自研的高级攻击技术亦或是学习、利用其他国家背景组织的技战术的实战应用，针对包括以乌克兰为圆心，波罗的海地区、欧美为半径目标区域的网络攻击活动，使得全球范围内以俄乌冲突为主题的钓鱼活动愈发敏感，例如中东地区的伊朗 APT 组织 Lyceum、亚洲地区的印度响尾蛇组织使用有关俄罗斯在乌克兰的攻击活动图片通过电子邮件发起了网络钓鱼攻击。在针对以色列的供应链攻击活动中出现了新的擦除(wiper)恶意软件 Agrius，意味着“擦除性恶意代码”、“供应链”等高级技战术不再是俄罗斯国家背景的 APT 组织独有。这说明**俄罗斯在网络战中高级攻击技术的应用，已在全球地缘政治活动中产生影响，促使包括俄乌在内的、全球范围内国家地区的地缘政治活动更为剧烈。结果是“俄乌冲突”使双方在网络空间中均遭受到了不同程度的损失。**

1.4 数字证据易篡改促使境外 APT 组织利用网络攻击栽赃构陷

数字证据广泛存在于计算机系统软硬件和外围设备及相关网络之中，区别于传统的物证证据，数字证据具有易篡改的特性，传统的书面材料等实物证据被破坏篡改都会留下痕迹，通过笔迹特点、油墨类型、印刷版式等方面进行文件检验学的司法鉴定通常可以发现，而数字证据包括电子文档、音视频等在文件内容和元数据上都可以任意读写改动，除非有第三方加密、加印等存储手段加以监视性保护，不然要从已经被篡改、删除和破坏的电子存储媒介中重新查清痕迹往往十分困难。

2022 年 2 月，安天发布报告揭露了具有印度背景的 APT 组织暗象[6]，发现该组织主要针对印度境内的社会活动人士、社会团体和在野政党等，同时也会窃取印度周边国家如中国和巴基斯坦等国军事政治目标的重要情报。在对其所涉及的 Bhima Koregaon 构陷案件进行复盘时，安天发现暗象组织对印度境内处境窘迫、缺乏网络安全防范意识和手段的社会运动个人长期反复发动鱼叉邮件式攻击，在成功向对方系统植入 NetWire 远控木马后，攻击者将精心制作的包括“购买军火”、“密谋暗杀总理”等内容严重违反印度法律的文档信件，多次借助远控木马传送到目标的笔记本和外接移动存储设备的隐蔽文件目录中，此后**攻击者将此结果密报当地警方前往目标的住宅突袭检查，当场查获这些构陷目的的违法信件作为论罪的数字证据。**

在数字取证的过程中，为了能够向司法机关提供足够可靠的证据，对于犯罪相关的计算机、手机、平板和其他存储介质设备的现场查获、后期的封存移交，以及设备中数字证据的固定、分析、认证都需要严谨的流

程手段和监督。在暗象涉及的案件中，在实现网络层面的操作后，犯罪者的构陷行为从现场查获的阶段便开始了。从后续为翻案提供证据的二次取证的过程来看，杀毒软件记录的计算机系统中进程、文件和网络的详实信息和三者间相互关系的留存发挥了关键的作用，特别是文件系统的 UsnJrnl 记录与历史进程信息的结合证明了违法信件在受害人电脑中的出现是来源于远程控制木马的网络传送。

1.5 利用物联网设备进行战场预置的 APT 攻击活动频繁

物联网是由不需要人工干预的具有传感系统的智能设备组成的网络，在现今的人类社会中，IoT 存在于社会应用的各个角落，如可穿戴设备、车联网、智能家庭、智慧城市、工业 4.0 等。物联网 IoT 设备利用种类繁多的网络协议技术使得网络空间与来自物理世界的信息交互成为可能。但是 IoT 自身具备以下不安全因素：其一，IoT 设备自身多数未嵌入安全机制，同时其又多半不在传统的 IT 网络之内，等于游离于安全感知能力之外，一旦遇到问题也不能有效响应；其二，大部分的 IoT 设备 24 小时在线，其是比桌面操作系统主机更“稳定”的攻击源；其三，路由器、摄像头等 IoT 设备用作代理，能稳定传输攻击、下发、窃密和控制等阶段的流量，由于本身网络流量较大，还可以将攻击流量混入其中达到隐藏隐蔽的作用；其四，在特定场景下，内网设备大多能访问路由器，可作为面向内网的跳板，同时存在于网络边界的路由器、摄像头等有时又暴露于互联网上，攻击者也能直接从互联网访问。以上特点，使得 APT 组织利用物联网 IoT 设备搭建 C2 基础设施获取相对攻击优势成为常见手段。

2022 年初，安天发现海莲花组织在针对我国的网络攻击活动中[7]，预先通过弱口令爆破、漏洞攻击等手段攻陷遍布我国多处重要省市的公网路由器、摄像头等物联网设备充当跳板，安装流量转发工具，将 Torii 远控木马的窃密和控制流量经一层或多层跳板转发至真实的 Torii 远控服务器。通过复盘追溯，安天发现 Torii 远控家族的最早活跃时间可追溯至 2017 年，其功能丰富、适配广泛，本身设计上就是面向各类型物联网系统设备的远控武器，支持生成众多类型如 ARM、x86、x64、MIPS、SPARC、PowerPC、SuperH、Motorola 68000 等 CPU 架构的木马载荷，能对运行于以上架构的服务器、物联网设备、办公主机等进行深度信息窃取和控制，具备 10 组以上的命令控制能力。

2022 年 5 月，Mandiant 公司在调查 APT29 组织从受害者内部网络中收集电子邮件的窃密活动时[8]，发现攻击者使用了一种基于开源 Dropbear SSH 软件魔改而成的新型后门，该后门支持在不受集中式安全管理且无端点侧检测防御手段的物联网设备中运行，基于 Dropbear SSH 功能开启 SOCKS 代理转发流量建立跳板。攻击者将此手段应用于目标网络中版本老旧的会议室 IP 摄像头，由于这些设备直接被暴露在互联网上且位于检测盲点，攻击者将恶意行为混入正常流量中在受害者网络保持潜伏了相当长时间未被发现。

2 勒索攻击

回顾 2022 年发生的勒索攻击事件，部分勒索软件被具有国家背景的攻击组织作为“政治化”犯罪工具，用以实施网络攻击。在俄乌冲突期间“政治化”勒索攻击案例频频发生并伴随着“破坏式”勒索软件再现，伪装成勒索攻击，但实际目标是破坏系统运行，从而实现网络空间攻击转化为物理空间影响。随着网络安全技术的不断创新和安全设备筑起坚实的边界防护壁垒，威胁行为者在利用常见执行体传播方式无法实现入侵，雇佣受害目标内部人员实施网络攻击作为新手段。勒索策略也出现了新转变，从传统的勒索软件攻击“窃取+加密”转变为“窃取+删除或破坏”的攻击。跨平台勒索软件执行体帮助威胁行为者渗透到越来越复杂的网络环境中，在执行体分析上也给安全工作者带来了新的挑战。

2.1 “政治化”勒索攻击

勒索软件通常作为攻击组织以经济目的为由的犯罪工具，回顾 2022 年发生的勒索攻击事件，发现**部分勒索软件被具有国家背景的攻击组织作为“政治化”犯罪工具，用以实施网络攻击。**

“政治化”的勒索攻击大致可以分为两类，一种实质上是伪装为勒索攻击的破坏活动，安天曾于 2017 年关注到针对乌克兰的伪必加“NotPetya”破坏活动[9]；伊朗情报和安全部（MOIS）在伊朗情报部长的领导下，从 2022 年 7 月开始对阿尔巴尼亚政府系统进行了一系列破坏性攻击，包含多次勒索软件攻击，其中隶属伊朗的 APT 组织 MuddyWater 利用公开漏洞入侵受害者系统，从而部署勒索软件[10]；2022 年 10 月，乌克兰计算机应急响应小组（CERT-UA）发布了 Cuba 勒索软件针对该国家发起攻击活动的警告。攻击者投放伪装成来自乌克兰武装部队相关内容的钓鱼邮件，从而诱使受害者查看并下载勒索攻击载荷[11]。另一种是具有“政治化”背景的攻击组织帮助国家谋取利益的勒索攻击活动，例如微软威胁情报中心（MSTIC）发现朝鲜的攻击者开发出的 H0lyGh0st 勒索软件，并且该勒索软件和隶属朝鲜的 APT 组织 Lazarus 存在一定关系，微软分析师猜测其动机可能为帮助朝鲜政府缓解经济压力[12]；隶属朝鲜的 APT38 组织使用 Beaf、PXJ、ZZZZ 和 ChiChi 等勒索软件实施攻击活动[13]。

俄乌冲突时期，多个勒索软件组织宣明各自政治立场。2 月 25 日，Conti 在其暗网的数据泄露平台发布声明，称“如果任何组织决定对俄罗斯发动网络攻击或任何战争活动，我们将动用一切可能的资源，对敌人的关键基础设施进行反击”。Conti 是在俄乌冲突时期第一个表明政治立场的勒索软件组织，但此举遭到了内部工作人员不满，一名据称是乌克兰籍的成员在网上公开了该组织内部聊天记录和勒索软件构建器等资料。Stormous 勒索软件组织表明支持俄罗斯，并于 3 月 1 日发布声明称其攻击了乌克兰外交部[14]。还有部

分勒索软件组织未公开表明政治立场，但实际发动了针对性勒索攻击活动，包括 Freeud、Prestige、NB65 和 HermeticRansom（GoRansom）等勒索软件。

虽然威胁行为者通常会直言不讳地表达自己的意图并声称对攻击负责，但映射现实世界的身份较为困难，并且区分威胁行为者出于政治或经济的犯罪动机越来越具有挑战性。

2.2 “破坏式”勒索软件执行体

“破坏式”勒索软件与常见的勒索软件不同，未采用加密算法对文件进行加密，而是采用数据覆盖或数据擦除的方式，对受害者系统中的文件进行破坏。

俄乌冲突期间曾出现多个“破坏式”勒索软件，1 月 13 日微软曾发现一个名为 MBR Locker，针对乌克兰地区的勒索攻击活动，该活动分为勒索和数据擦除两个阶段，勒索阶段投放的执行体实为佯攻，藏在勒索背后的是 WhisperGate 数据擦除器执行体，在勒索阶段释放的勒索信用以迷惑受害者，其真实目的是为了掩盖 WhisperGate 数据擦除器入侵受害者系统后的恶意行为[15]。HermeticRansom（GoRansom）的勒索软件执行体于 2 月 23 日在乌克兰某网络设施中被发现，其功能与 MBR Locker 攻击活动较为相似，也是在投放勒索软件执行体后，执行 HermeticWiper 数据擦除器执行体[16]。4 月出现在公众视野的 Onyx 勒索软件不同于以往，其采用的加密策略为判断加密文件大小，对小于 2M 的文件正常采用加密算法进行加密，对大于 2M 的文件采用垃圾数据进行覆盖，即使受害者支付赎金也无法恢复大于 2M 的所有文件[17]。

我们曾在 2021 年预测“破坏式”勒索软件再现，以破坏为目的的攻击行动，同样可以伪装为定向勒索攻击行动。由于勒索软件对数据和文件加密会导致系统或业务失能的后果，此前也曾出现过伪装成勒索攻击，但实际目标是破坏系统运行，从而实现网络空间攻击转化为物理空间影响的事件。

2.3 勒索策略转变

常见勒索软件执行体传播包括网络钓鱼、RDP 暴力破解和漏洞利用等方式，随着网络安全技术的不断创新和安全设备筑起坚实的边界防护壁垒，威胁行为者在利用常见执行体传播方式无法实现入侵，但发现当前各企业在执行网络安全建设规划时，内部安全通常被忽视，结合疫情导致的经济因素伴随着缩减支出、裁员等情况，则衍生出**雇佣受害目标内部人员实施网络攻击作为新手段**。Lapsus$勒索软件组织并不依赖于执行体常见传播方式，而是寻找愿意出售其组织内访问权的内部人员，这也可能是导致在 2022 年内，多个大型企业遭受 Lapsus$组织攻击的原因，包括英伟达、三星、育碧、微软和优步等[18]。

采用“双重勒索”方式在勒索软件运营中已经成为主流趋势，即“窃取数据+加密文件”的方式，多个勒索软件利用 Exmatter（又名 Fendr）数据渗透工具作为窃取受害者系统文件的利器，其中知名的包括

BlackMatter 和 BlackCat 等勒索软件。由于勒索软件在开发环节中可能存在漏洞，研究人员可以开发出对应解密工具用以帮助受害单位，从而导致勒索软件开发人员及附属成员无法获取勒索赎金，Exmatter 数据渗透工具开发人员为了解决这一问题，在得到有价值的文件并成功从受害者系统中导出后，对系统内的原文件进行数据覆盖，即不再采用加密算法加密文件，而是窃取成功后对系统内原文件进行损坏，意味着受害者只能通过联系攻击者支付赎金后获取自己的文件。

这种新的数据损坏功能可能是一种新的转变，**从传统的勒索软件攻击“窃取+加密”转变为“窃取+删除或破坏”的攻击**。在这种方法下，附属成员可以保留攻击产生的所有收入，因为他们不需要与加密器开发人员分享一定比例的收入[19]。随着国际上对勒索软件赎金支付的制裁和执法单位对追踪比特币流向技术的提升，勒索软件组织逐渐摒弃使用比特币作为赎金支付的选项并转向其他形式。

2.4 日益增多的跨平台勒索软件执行体

Big Game Hunting（BGH）[20]网络大型游戏狩猎是一种网络攻击计划，通常指勒索软件针对大型、高价值和知名企业单位进行勒索攻击，该计划使得勒索软件威胁行为者已经渗透到越来越复杂的网络环境中。为了造成尽可能多的损害，威胁行为者尝试加密尽可能多的系统，这意味着他们的勒索软件执行体能够在不同的架构和操作系统上运行。实现这个计划的一种方法是用 Rust 或 Golang 等“跨平台编程语言”编写勒索软件，使用跨平台语言还有其他一些原因，部分勒索软件目前可能只针对一个平台，但在跨平台中编写它可以更容易地将执行体移植到其他平台，另一个原因是跨平台执行体在分析上较难一些。在 2022 年已经发现了多个知名的跨平台勒索软件执行体，例如 Linux 版 AvosLocker 和 LockBit 勒索软件执行体针对 VMware ESXi 服务器，TellYouThePass 勒索软件使用 Golang 语言开发新版执行体卷土重来，Hive 勒索软件使用 Rust 语言开发针对 Linux 系统 VMware ESXi 服务器的执行体等。

3 挖矿木马

3.1 越来越多的挖矿木马团伙掌握快速集成漏洞的能力

随着挖矿木马对抗技术的不断完善，越来越多的挖矿木马团伙掌握快速集成漏洞的能力。挖矿木马不仅对抗安全产品，还要阻断同行的竞争，谁能率先快速集成漏洞，谁就能优先获得存在漏洞的公网算力，也就获取到了相应的利润。每当出现影响广泛的漏洞时，全网受影响的设备很难在短时间内修复漏洞，这就给了挖矿木马可乘之机。如 Log4j2 漏洞爆发后，H2Miner[21]等挖矿团伙迅速集成该漏洞并发起攻击。自 Confluence OGNL（CVE-2022-26134）漏洞利用的详细信息公布后，“8220”[22]挖矿组织和 Hezb[23]挖矿木马开始利用

该漏洞进行广泛传播。对企业来说，需要提高快速修复漏洞的能力，避免挖矿木马利用漏洞控制主机权限，制定解决方案，防止在漏洞曝光后，给企业带来挖矿木马传播的风险。

3.2 挖矿木马矿池逐渐隐蔽，传统情报检测将逐渐失效

挖矿木马通常采用两种方式进行挖矿，一种是直连矿池的方式进行挖矿，另一种是矿池代理的方式进行挖矿。挖矿木马直连矿池挖矿通常会让受害者主机直接连接矿池地址上传算力结果，矿池平台根据贡献的算力情况将报酬下发到挖矿木马团伙的钱包中，这种方式的弊端是安全分析人员通过分析攻击脚本等能够获取到挖矿木马团伙的钱包地址，并且还能发现直连的公共矿池地址，这样通过公共矿池网站输入对应的挖矿木马团伙的钱包地址，即可发现有多少受害者在被动挖矿、当前贡献算力总哈希和产出多少门罗币等等。而矿池代理可以轻松解决上述弊端，即矿工和矿池之间添加一个中转环节，矿池代理从公共矿池获取任务转交给矿工进行运算，矿工将运算结果转交给矿池代理进而在转发到公共矿池。近些年来，越来越多的挖矿木马团伙开始使用矿池代理的方式进行挖矿，如 Kthmimu[24]、“8220”[22]、Sysrv-hello、Outlaw[25]等都逐渐开始使用这种方式进行挖矿。矿池代理的普及将真正使用的公共矿池隐蔽起来进行挖矿，可绕过传统情报矿池黑名单检测，使传统黑名单检测失效。

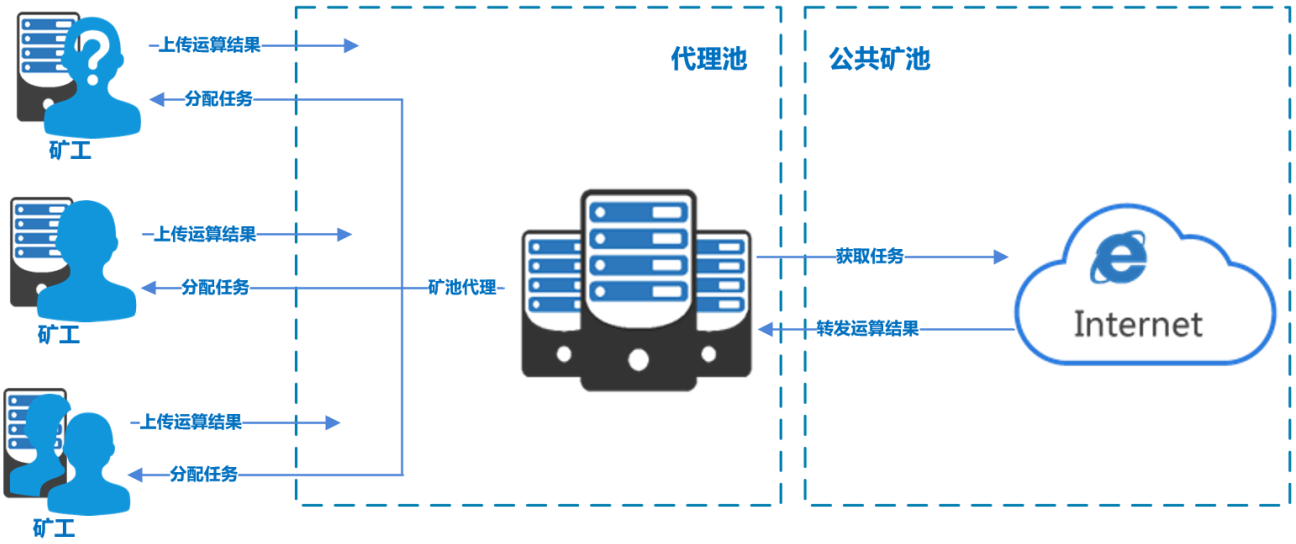


图 3-1 矿池代理示意图

3.3 由于稳定的利润，更多的威胁组织开始从事恶意挖矿

2022 年整个虚拟货币市场遭受巨大冲击，几乎所有币种价格都在下跌。以比特币为例，1 月份每个比特币价格接近 48000 美元，而到了 11 月份，每个比特币的价格仅为 17000 美元，跌幅超过 3 万美元。尽管如此，恶意挖矿并没有减少，反而更加活跃。恶意挖矿最常使用的币种是门罗币，相较于其他币种，门罗币更

加稳定，这也受到了其他勒索软件组织的青睐。例如，AstraLocker[26]勒索软件关闭了勒索攻击活动并将自身业务转向到恶意挖矿活动中，这种转变很可能是该勒索软件组织想以更加低调和隐蔽的方式赚取虚拟货币。在各国政府加强了对勒索软件的防御和执法力度之后，勒索软件组织的收益大打折扣，与恶意挖矿不同的是，勒索软件在入侵系统后会影响系统正常运行，赚取赎金的方式主要依靠与受害者沟通，情节严重可能会受到各国政府的打压。而恶意挖矿可以在受害者不知情的情况下赚取虚拟货币，这对勒索软件组织来说风险性相对较低，虽没有勒索受害者支付赎金赚钱，但恶意挖矿近乎零成本赚取虚拟货币，既不用担心电费的价格，也不用担心算力的问题，也可以赚取丰厚的报酬。所以安天 CERT 认为，未来会有更多的威胁组织从事这种低风险、高回报的恶意挖矿活动。

4 僵尸网络

据统计 CNCERT 每月公布的互联网威胁报告发现[27]，2022 年活跃的僵尸网络家族有 Mirai、Mozi、rapperbot、hybridmq、gafgyt 和 moobot 等，这些活跃的僵尸网络家族都具有 DDoS 功能且感染量在国内较大，一旦发起攻击，其破坏和影响巨大。安天发现 **2022 年全球政治局势不断变幻，利用僵尸网络发起具有政治意味的 DDoS 攻击已然成为大国之间对抗的主要手段；通过对 2022 年披露的漏洞利用情况进行统计后发现，僵尸网络正在积极地利用新出现的漏洞进行传播；采用 P2P 传播方式的僵尸网络在物联网设备间广泛传播。**

4.1 由僵尸网络发起的 DDoS 攻击已成为国与国对抗的利器

僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为，如可同时对某目标网站进行 DDoS 攻击，或发送大量的垃圾邮件，或进行“挖矿”等。随着全球政治局势动荡，**越来越多具有国家支持的 APT 攻击组织或个人组织因国际关系，利用僵尸网络发起具有政治意味的网络攻击。**

2022 年初，伴随俄乌冲突，美、欧、俄、乌之间展开了一场没有硝烟的网络战争。据乌克兰媒体报道，（俄乌冲突）正式开战前从 1 月 14 日至 2 月 24 日，先是乌克兰的外交部、教育部、内政部、能源部等 70 多个政府网站遭到来自俄罗斯的 DDoS 网络攻击而关闭，继而国防部、安全局、武装部队、金融机构等多处信息资源（网站和 APP）攻击而瘫痪、服务中断，数百台机器的数据被擦除[28]。据俄罗斯卫星社报道，“匿名者”黑客组织发动大规模 DDoS 攻击，造成克林姆林宫、国防部、外交部等多个俄罗斯政府网站无法完全访问[29]。

国家互联网应急中心（CNCERT）2022 年 3 月 11 日发布监测报告[30]，2 月下旬以来，中国互联网持续遭受境外网络攻击，境外组织通过攻击控制中国境内计算机，进而对俄罗斯、乌克兰、白俄罗斯进行网络攻击。经分析，这些攻击地址主要来自美国，仅来自纽约州的攻击地址就有 10 余个，攻击流量峰值达 36Gbps，87%的攻击目标是俄罗斯，也有少量攻击地址来自德国、荷兰等国家。

2022 年全球政治局势不断变幻，利用僵尸网络发起具有政治意味的 DDoS 攻击已然成为大国之间对抗的主要手段。[31]

4.2 僵尸网络利用新漏洞进行传播

2022 年，安天监测发现僵尸网络运营者通过增加漏洞数量并积极利用 1day 漏洞来扩大僵尸网络规模。以下柱状图中 CNCERT 发布的 2022 年 6 月-11 月 6 个月间捕获的物联网在野传播漏洞种类[27]：

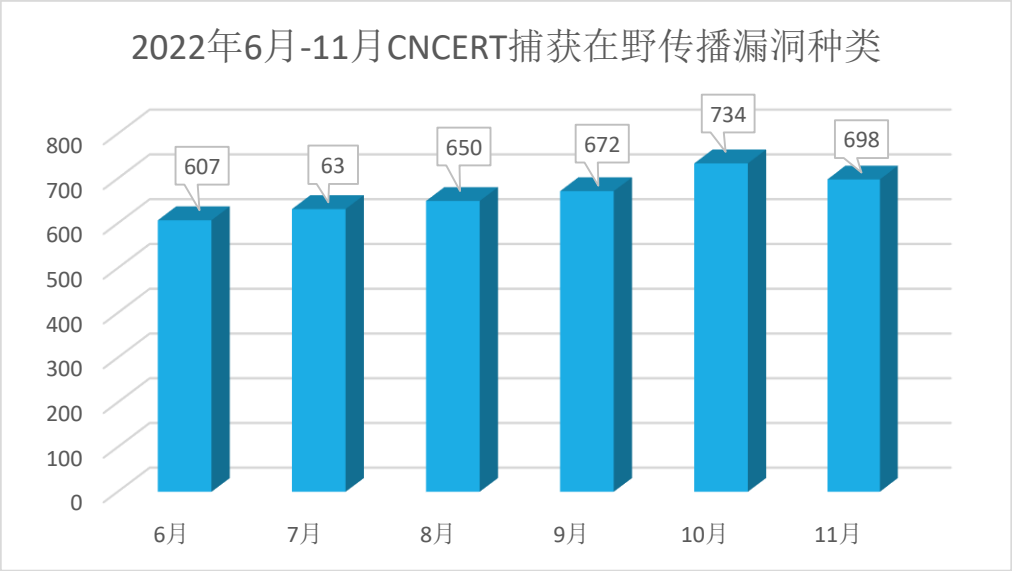


图 4-1 2022 年 6 月至 11 月 CNCERT/CC 捕获在野传播漏洞种类统计图

以 CVE-2022-29591 漏洞为例，该漏洞首次披露于 2022 年 5 月 10 日， 安天在 5 月 17 日即捕获到该漏洞利用的流量，可见 Miori 僵尸网络运营人员对新漏洞具有较高的敏感性并具有一定的漏洞利用能力。

2022 年 11 月，安天蜜罐捕获一个由 Go 编写的 DDoS 类型的僵尸网络家族 zero ，该僵尸网络短时间内出现了 4 个不同的版本，分析人员发现其在版本迭代中持续更新添加漏洞，仅 2022 年各类远程可执行漏洞利用就多达 12 个。

通过对 2022 年披露的漏洞利用情况进行统计后发现，僵尸网络正在积极地利用新出现的漏洞进行传播。

4.3 采用 P2P 传播方式的僵尸网络在物联网设备间广泛传播

随着信息时代高速发展下“万物互联”概念的驱使，物联网设备日益增多，但大多数物联网设备包括严重的安全问题，如弱密码、对管理系统的开放访问、默认管理凭据或弱安全配置等，物联网设备已成为对攻击者有吸引力的目标。攻击者抓住物联网漏洞繁多的特点来控制设备，这使得攻击者可以轻松访问它们，并导致在线服务的中断。且由于物联网设备的感染通常不会被用户注意到，因此攻击者可以轻松地将数十万台此类设备组装成一个强大的僵尸网络，从而能够进行大规模攻击。

P2P 传播方式是部分僵尸网络的传统传播手段之一，具有传播速度快、感染规模大、追溯源头难的特点，例如 Mirai、Mozi 等僵尸网络家族在利用该传播方式后活动异常活跃。2022 年联网智能设备间僵尸网络控制规模持续增大[32]，部分大型僵尸网络通过 P2P 传播与集中控制相结合的方式对受控端进行控制。受感染设备之间仍可继续通过 P2P 通信保持联系，并感染其他设备。随着更多物联网设备不断投入使用，采用 P2P 传播的恶意程序可能对网络空间产生更大威胁。

5 攻防对抗

当前，网络安全对抗模式已演进成为全面体系化的对抗，建制化的攻击组织在大规模工程体系支撑下，依托制式化网空装备完成杀伤链。在持续的新冠疫情下，政企部门加速了云业务、数字化业务，尤其是以新基建、信创为代表的新基础设施引入了更多的攻击面和供应链威胁，攻防对抗长期处于“易攻难守”的不对称局面。

5.1 攻击面管理（ASM）成为攻防对抗的第一扇窗

Gartner 在 2018 年首次提出攻击面管理（Attack surface management，ASM）的概念，随后在 2022 年 2 月将攻击面管理发布在网络安全风险管理趋势中的首位。近年来，因攻击面管理不善导致的安全事件频发（如 Log4j2 远程代码执行漏洞（CVE-2021-44228）在野利用、某市健康码 AccessKey 配置不当导致数据泄露等），近几年攻击面管理的概念开始广泛的在攻防对抗领域反复提及。

受新冠疫情的反复影响，政企部门加速了数字化转型工作、云业务工作，5G 和 IOT 业务的快速落地使原本脆弱的攻击面管理工作变得越发复杂。有关数据表明[33][34][35]，绝大多数企业都认为应该提升攻击面的监控能力，但在漏洞出现时，企业往往需要平均 80 个小时以上来更新自己的攻击面范围，而攻击者仅需 48 小时就可以将漏洞武器化。因此，随着攻防实战演练的活动的深入、大国间网络对抗较量的加剧，攻击面管

理已成为攻防对抗的第一扇窗，攻击者很容易利用脆弱的攻击面将原有的“监测-分析-预警-处置”的安全体系击穿，对企业整体网络安全性造成的影响。

5.2 供应链成为攻防对抗最大的突破口之一

2022 年供应链安全事件频发，NPM 存储库的大规模供应链攻击事件、Spring4Shell 漏洞攻击事件等安全事件证明供应链安全是不容忽视的。据国家信息安全漏洞库（CNNVD）的统计数据，2022 年上半年漏洞总量环比增长达到 12%，超高危漏洞占比超过 50%。随着国际加强了对漏洞发布的管理，在野漏洞利用有进一步加重的趋势。

在我们的观测中，攻防对抗中的流行漏洞关于办公系统、项目管理系统、邮件系统等供应链产品的漏洞占比已超过 50%。在某大型攻防演练活动中，在野利用的办公系统、网络设备、网络安全设备等供应链产品漏洞更高达 20 个，广泛使用攻击链漏洞攻击已是攻防对抗中最常见的手段之一。由于政企用户难以了解供应商的网络安全水准，攻防对抗中往往会使用供应链产品漏洞打造的杀伤链对目标进行精准攻击入侵并控制目标系统设施，实现作战目的。攻击者还可以利用通用的开源组件漏洞对作战目标进行范围打击，再次提高检测和响应的难度，将杀伤链拓展成为杀伤网，以突破更多的作战目标。由此可见，供应链产品漏洞已成为攻防对抗中最大的突破口之一。

5.3 载荷隐藏的滥用是攻防对抗的一大挑战之一

在过去，APT 组织往往使用多种的载荷隐藏技术来规避检测，实现长时间的隐匿。随着实战化攻防演练活动的深入，为了达成演练效果，载荷隐藏技术也被广泛讨论和研究。从最开始的免杀对抗、隧道隐藏到无实体文件落地、签名免杀等更加高级的载荷隐藏方法。仅在某大型攻防演练活动中，我们便观测到 7 种以上的载荷隐藏方法，极大的考验安全团队的响应能力。

- 利用 CDN 域前置和云函数转发攻击样本伪装流量，隐藏 C2 地址，对抗威胁情报；
- 利用代码托管平台托管攻击载荷，干扰沙箱、迷惑受害者和分析人员；
- 利用签名免杀制作样本，对抗多引擎对照结果；
- 利用内存马技术控制，对抗终端反病毒软件；
- 利用分片传输的方式发送数据包，对抗流量检测特征；
- 利用二次开发商业军火工具，对抗流量检测特征；

- 利用 DNS、ICMP 等协议发送载荷，对抗流量协议检测。

这些技术不仅在攻防对抗领域广泛应用，也在社交平台、论坛、博客上广泛讨，极大的降低了原本的使用门槛。我们同时发现，一些攻击者开发的武器化的工具现在也支持多种的载荷隐藏方式并高速迭代，给分析、监测、处置带了极大的挑战，由此可见，载荷隐藏的滥用已然是攻防对抗的一大挑战之一。

5.4 AI 赋能将为攻防对抗带来更多挑战

ChatGPT[36]是由 OpenAI 开发的一个人工智能聊天机器人程序，于 2022 年 11 月推出，一经推出后，受到全世界广泛关注。很快有安全研究员发现，ChatGPT 可以被训练分析代码缺陷、编写漏洞检测规则，也可以生成恶意代码、生成漏洞 POC、甚至生成钓鱼邮件等。

AI 的加入使攻击者的攻击成本再度降低，一方面，可以将 AI 用于生成黑客军火，对抗安全产品，甚至可以结合舆论战、网络战、信息战实现更大的作战目的，也可以将作战任务自动化、规模化，提升攻防对抗难度；另外一方面，可以利用 AI 驱动网络防御，改进业务代码质量，优化网络安全设备检出能力，自动化阻断网空威胁，大幅缩短威胁发现、响应时间，有效提高防御能力。难以否认的是，随着 AI 算力增强、训练模型日益精准、使用门槛不断降低，AI 的赋能将给攻防对抗带来更多的挑战。

5.5 针对新基建的攻防较量将成为攻防对抗的主阵地

当前国际秩序面临深度调整，全球科技竞争格局正加速重构。新基建作为数字化基建的基础设施，进一步扩大了攻击面，增加了网络安全建设和管理的难度；另外一面，新基建尤其是信创类产品，由于广泛使用开源产品，这必将获得攻击者尤其是超高能力网空威胁行为体的关注，并将其作为重点攻击的目标。因此，随着新基建尤其是信创产品的加速落地，未来针对新基建场景的攻防加量将为成攻防对抗的重要阵地。

5.6 常态化的安全运营，将有效提升政企机构的攻防能力

随着政企机构数字化建设的深化发展，新技术大量应用，线上场景不断丰富，网络安全面临全新风险和挑战。当前一部分政企用户已部署了大量的安全设备，但由此产生的海量告警给日常安全运维带来极大的压力，影响安全运营的效率和效果，难以体现安全建设价值。

通过常态化的安全运营可以持续挖掘和分析网空威胁行为体的关键特征，通过安全产品和安全服务相结合进行威胁发现、防范和处置，协助客户建立有效的安全防护体系。常态化安全运营划分为以下四个层面，可以充分考虑到业务组织和 IT 环境的特征，以及实际安全需求，有效降低安全运维压力，随时掌握安全态势，持续进行威胁对抗，帮助政企机构规避安全风险，有效提高攻防能力。

- 安全运营体系建设：健全安全运营管理制度体系和应急预案体系，强化关键环节的安全运营协同机制，确保政企机构的网络安全工作在安全运营组织机构的带领下能井然有序的开展。
- 前置安全评估：以全生命周期视角看待政企机构的资产安全运营，梳理资产攻击面，发现安全风险。协助客户做好安全运营的起点，把风险管控于系统上线之前
- 事件应急响应：协助客户定位事件源头，及时阻断事件横向蔓延，分析事件发生起因和过程，恢复现场损失，并加固相关脆弱性，防止事件再次发生
- 常态安全运营：基于资产与系统、应用与执行体、网络与拓扑、身份和账户、数据与业务五个层面协助客户构建基础运营的层次，为实现系统、拓扑、业务、数据流向提供建议，协助政企机构实现数据分类分级，持续开展数据安全治理。基于安全产品的运营结果，不断挖掘新的攻击面、脆弱性和威胁事件。联动进行威胁研判是否需要触发重大事件响应处置流程。

6 数据泄露

2022 年，新冠疫情仍然肆虐全球，全球各行各业加快了数字化转型，数据的价值得到进一步凸显的同时，数据泄露也在持续高频发生，数据泄露事件也不断地成为新闻热点，涉及从医疗信息、账户凭证、个人信息、企业电子邮件及企业内部敏感数据等各种信息，涉及的领域包括工业制造、政务、医疗、金融、交通等等，不一而足，面临的形势依然非常严峻。

6.1 2022 年泄露事件持续高频发生

2022 年数据泄露事件持续高频发生，数据泄露事件的数量也有增无减，个人信息泄露量以及文件数据泄露量巨大，对个人以及企业机构造成的影响十分严重。

2022 年影响力较大的数据泄露事件主要发生在互联网及各类型企业，文件数据泄露事件主要涉及能源、医疗、制造业、政府机构等，个人信息数据泄露事件主要涉及互联网、电信运营商、医疗、交通等领域。其中俄罗斯石油公司在德国的分公司 Rosneft Deutschland GmbH 以及 linux 平台的开源软件构建项目 Travis CI 所遭遇的数据泄露最为严重，分别导致了 20TB 文件数据泄露和 7.7 亿条用户日志记录泄露。**信息化程度越高的行业，数据泄露事件越多，且泄露所造成的危害越大。造成 2022 年数据泄露事件的原因主要有黑客窃取、勒索软件攻击以及企业和机构的数据库或者云存储配置不当。持续高频发生的数据泄露事件，使得全球数亿人的隐私和安全受到严重威胁。**

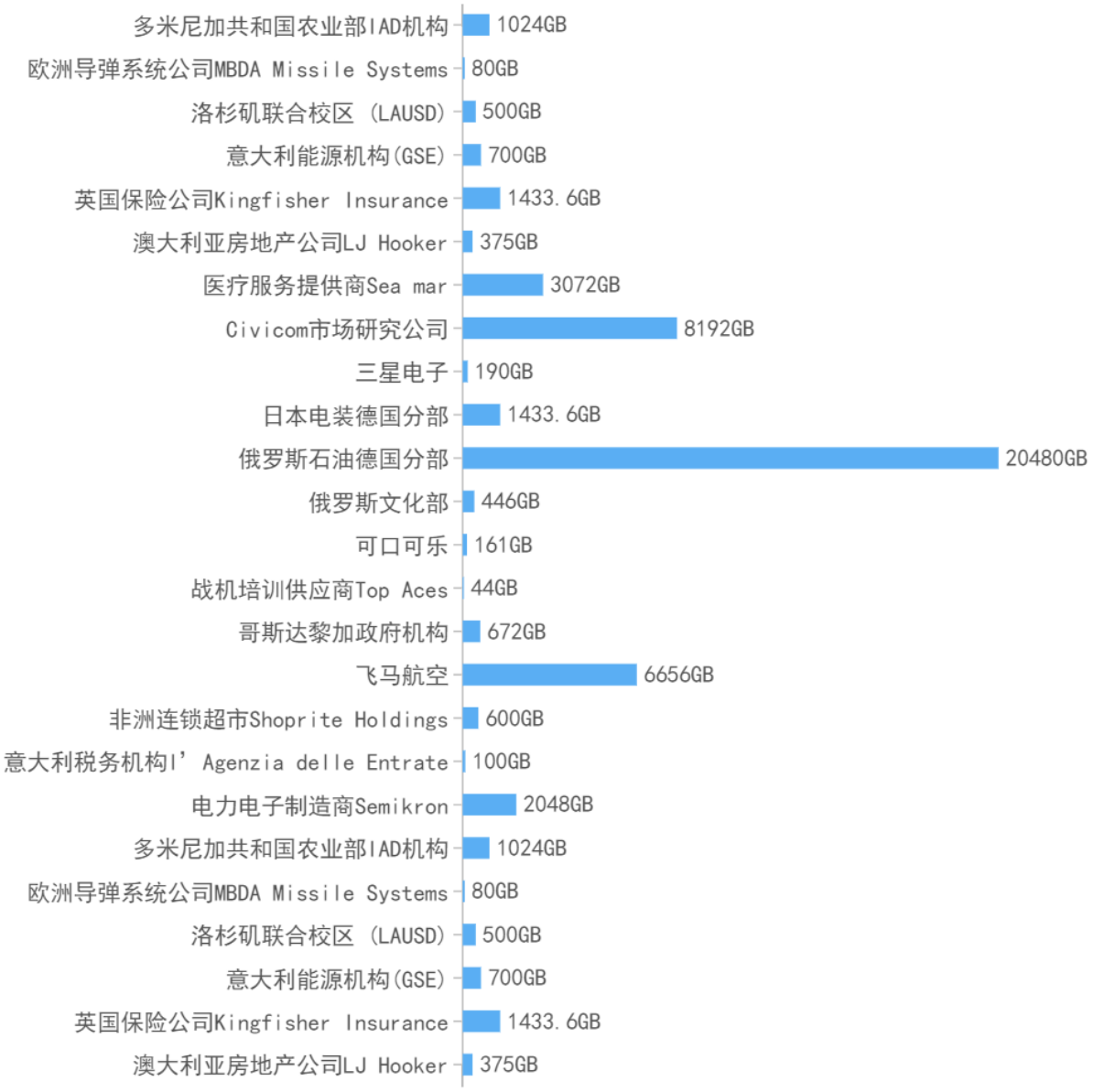


图 6-1 2022 年影响力较大的文件数据泄露事件

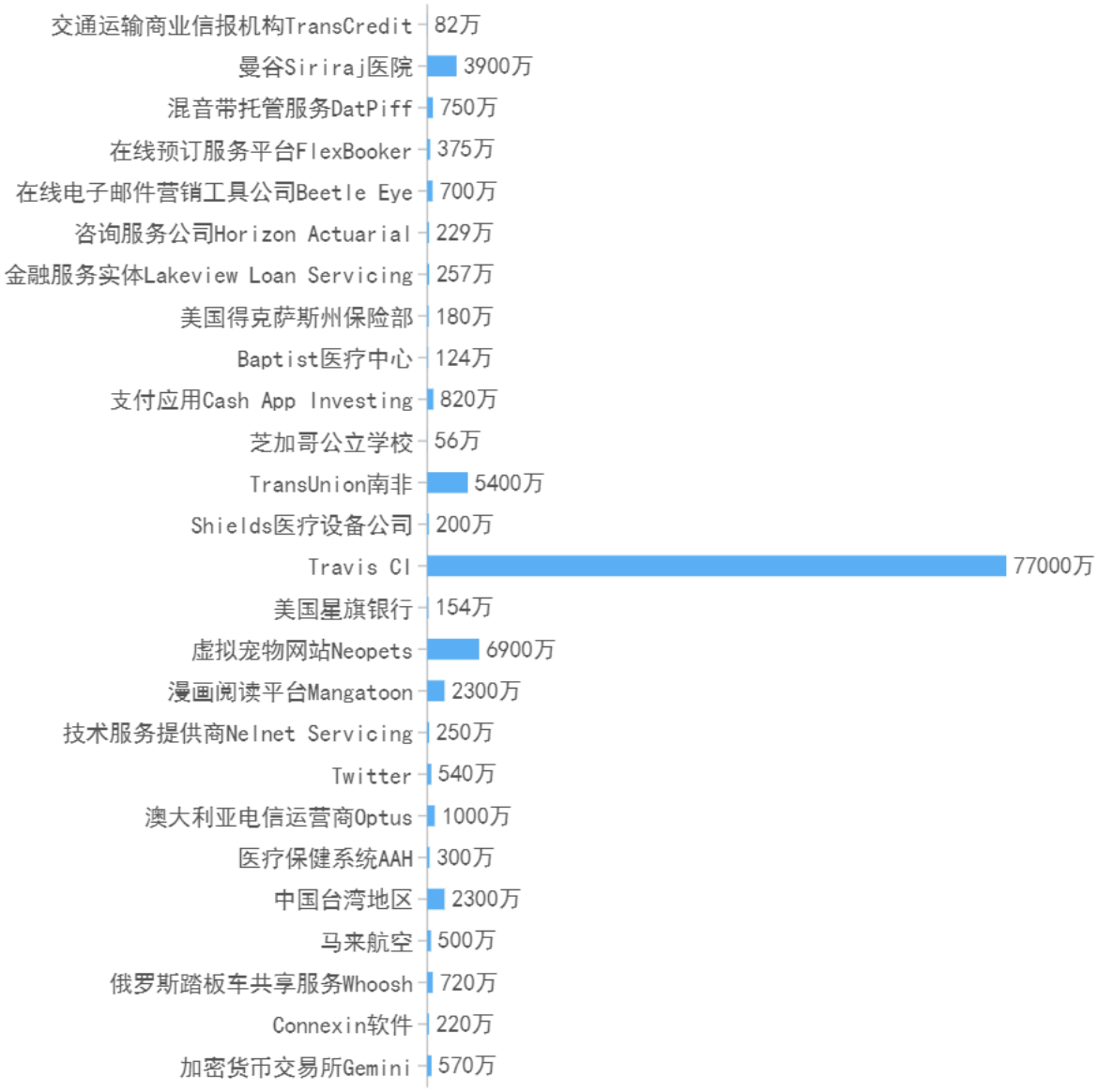


图 6-2 2022 年影响力较大的个人信息数据泄露事件

6.2 黑客论坛被用作网络犯罪活动的平台

数字化时代，数据泄露是推动网络犯罪规模化、产业化的最大动力，黑客论坛成为网络犯罪分子倒卖数据获取利益的平台。7 月 21 日，一名用户在 BreachForums 黑客论坛上发帖出售声称属于 Twitter 的 540 万账户数据，发帖人称其在 2021 年 12 月利用了一个漏洞来收集数据，虽然 Twitter 在 2022 年 1 月修复了这个漏洞，但它仍然暴露了数百万用户的私人电话号码和电子邮件地址；11 月 11 日，BreachForums 黑客论坛的一名用户发布了一个数据库，其中包含大约 720 万俄罗斯踏板车共享服务 Whoosh 的客户的详细信息，卖家还声称，被盗数据包括 300 万个促销代码，人们可以使用这些代码免费租用 Whoosh 滑板车；11 月 16 日，BreachForums 黑客论坛的一名用户发帖出售超 4.87 亿通讯软件 WhatsApp 用户的信息数据，据称数据

涉及 84 个国家和地区，其中约 3200 万来自美国，4500 万来自埃及、3500 万来自意大利、2000 万来自法国。

6.3 滴滴泄露数据被罚，敲响用户信息数据安全警钟

2021 年 6 月 30 日，滴滴正式在纽交所挂牌上市，在 2022 年 7 月 4 日，国家互联网办公室发布消息称：“根据举报，经检测核实，‘滴滴出行’APP 存在严重给违法违规收集个人信息问题。网信办依据《中华人民共和国网络安全法》相关规定，通知应用商店下架‘滴滴出行’APP。”

2022 年 7 月 21 日，据网信中国发文[37]，“国家互联网信息办公室依法对滴滴全球股份有限公司涉嫌违法行为进行立案调查。”“经查实，滴滴全球股份有限公司违反《网络安全法》《数据安全法》《个人信息保护法》的违法违规行为事实清楚、证据确凿、情节严重、性质恶劣。7 月 21 日，国家互联网信息办公室依据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等法律法规，对滴滴全球股份有限公司处人民币 80.26 亿元罚款，对滴滴全球股份有限公司董事长兼 CEO 程维、总裁柳青各处人民币 100 万元罚款。”在记者会上，网信办表示经查实，滴滴公司共存在 16 项违法事实，归纳起来主要是八个方面。

全球各行业的数字化转型已成主要趋势，但不断累积增长的敏感数据也带来了数据泄露、篡改、滥用等安全问题。随着《网络安全法》、《数据安全法》、《个人信息保护法》、《数据出境安全评估办法》等法律法规相继颁布实施，我国数据监管法律体系日益完善。**此次数据泄露事件也是给国内所有的互联网公司一个警醒，国家信息安全无小事，保护信息安全人人有责。**

6.4 斩断窃密“黑手”，筑牢个人信息保护防火墙

互联网时代，公民个人信息已成为“含金量”极高的商业资源，是窃密者觊觎的重点目标。据安全内参 11 月 21 日报道[38]，哈尔滨市公安局南岗分局网安大队民警在工作中发现，黑客论坛上有一名用户于 2022 年 10 月发帖出售公民个人信息数据，自称持有数据量约 20GB，售价 0.2 比特币，该用户还公布了 29 条数据样本，样本中还包括了公民姓名、联系电话、家庭住址等个人信息。经过专案组民警们 96 小时的艰苦奋战，10 月 22 日，南岗公安分局民警在哈尔滨市平房区将涉嫌非法获取计算机信息系统数据的犯罪嫌疑人麻某抓获，并在其电脑中查获非法获取的公民个人信息 10 万余条。经审讯，犯罪嫌疑人麻某为 IT 行业从业人员，利用某医疗机构微信公众号的系统漏洞，在 2022 年 4 月至 10 月间，通过技术手段非法获取该计算机系统数据 10 万余条，而后在境外某黑客论坛发帖出售，截至落网前，已非法获利 1500 美元。**个人信息的泄露会造成一系列的连锁威胁，敏感信息直接关系公民人身及财产安全，若被非法获取，极易引发关联性犯罪，比如金融诈骗、信用欺诈、勒索等等，泄露的数据还会形成精准的用户画像。**

大数据时代发展至今，个人信息泄露问题已然成为社会发展的隐患，保护个人隐私势在必行，保护公民个人信息不受侵害也成为了网络信息技术飞速发展条件下的必然要求。不但公民自身要提高安全意识，互联网平台也应自觉承担起保护用户敏感信息的责任，关键行业更要尽早做好相应的防范措施，加强技术性管理策略以及防范手段，以最大程度地避免数据泄露带来的风险。

7 工业互联网

依据《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》[39]，工业互联网作为新一代信息技术与制造业深度融合的产物，日益成为新工业革命的关键支撑和深化“互联网+先进制造业”的重要基石，对未来工业发展产生全方位、深层次、革命性影响。工业互联网通过系统构建网络、平台、安全三大功能体系，打造人、机、物全面互联的新型网络基础设施，形成智能化发展的新兴业态和应用模式，是推进制造强国和网络强国建设的重要基础，是全面建成小康社会和建设社会主义现代化强国的有力支撑。

近年来，我国积极布局工业互联网，在《工业互联网发展行动计划（2018-2020 年）》（工信部信管函〔2018〕188 号）[40]、《工业和信息化部办公厅关于推动工业互联网加快发展的通知》（工信厅信管〔2020〕8 号）[41]、《工业互联网创新发展行动计划（2021-2023 年）》（工信部信管〔2020〕197 号）[42]等一系列政策和市场需求的双重驱动下，我国工业互联网蓬勃兴起，多项应用逐步落地，市场规模不断扩大；与此同时，工业互联网所面临的网络安全威胁也值得我们给予高度关注。

7.1 地缘政治军事冲突波及工业互联网

2022 年，地缘政治局势紧张加剧，区域性军事冲突、领土矛盾流血冲突爆发，其负面影响在一定程度上波及了工业互联网。

2022 年 2 月 24 日，俄乌冲突爆发。从冲突正式爆发前夕直至目前，APT28、APT29、Turla、Sandworm（沙虫）、Dragonfly、Gamaredon、UNC1151、乌克兰军事情报局(GURMO)、IT Army of Ukraine 组织、匿名者（Anonymous）组织、GhostSec 组织、AgainstTheWest 等多方网络空间威胁行为体纷纷卷入其中，并将其施加的负面影响从“第五疆域”（网络空间）拓展至现实物理世界，波及有关国家的工业网络安全。

1) 俄乌冲突期间的 4 月 12 日，乌克兰计算机应急响应小组(CERT-UA)和斯洛伐克网络安全公司 ESET 发布公告称：俄罗斯联邦军队总参谋部情报总局（GRU）旗下的 Sandworm 组织针对乌克兰的高压变电站发动了攻击，攻击者使用了一种新的恶意软件变种 Industroyer2；此外，攻击组织还使用了其他几个破坏性的恶意软件，包括 CaddyWiper、ORCSHRED、SOLOSHRED 和 AWFULSHRED。

2) 俄乌冲突期间的 7 月 20 日，俄罗斯 Gysinoozerskaya 水电站发生爆炸，导致电力系统紧急关闭、西伯利亚大片地区停电。GhostSec 组织声称对这次攻击负责，并表示其网络攻击是对俄乌冲突中俄罗斯一方的回应；该组织“领袖”Sebastian Dante Alexander（塞巴斯蒂安·丹特·亚历山大）通过“The Tech Outlook”等公开渠道发声表示：这次袭击经过该组织精心设计，他们编写了名为“KillBus”的工具用于针对 Modbus 设备实施攻击，该工具通过提取信息来重写数据并将其用作从设备，继而破坏了水力发电厂的工业控制系统及其服务器。GhostSec 组织对发电厂系统的恶意干预导致了最终的爆炸。

而 2022 年 3 月下旬以来，阿以冲突(Conflict between Arabian countries and Israel)再次加剧，其负面影响同样波及工业互联网络。

1) 6 月上旬，微软公司表示其阻止了一个名为 Polonium 的黎巴嫩黑客组织使用 OneDrive 云存储平台对以色列组织的攻击。微软还暂停了 Polonium 攻击中使用的 20 多个恶意 OneDrive 应用程序，并通过安全情报更新隔离攻击者的工具。根据分析，在自 2022 年 2 月以来主要针对以色列关键制造业、IT 和国防工业部门的攻击中，Polonium 黑客组织也可能与多个与伊朗有关的攻击者协调他们的攻击行动。

2) 9 月上旬，GhostSec 组织声称，他们已经入侵了以色列组织使用的 55 台 Berghof PLC(可编程逻辑控制器)。GhostSec 在其 Telegram 频道上分享了一段视频，该视频展示了成功登录 PLC 的管理面板，以及显示其当前状态和 PLC 进程控制的 HMI 屏幕图像。与此同时，GhostSec 还发布了更多截图，声称已经获得了另一个控制面板的访问权限，该面板可用于改变水中的氯和 pH 值。研究人员表示，由于 PLC 可以通过互联网访问并存在弱口令，因此可能会被破坏。

7.2 工业互联网基础设施脆弱性风险披露数量超百

2022 年，全球范围内工业互联网基础设施脆弱性风险披露数量超百，且有关脆弱性风险可能导致的严重负面影响不容忽视。

2022 年 11 月，中国工业互联网研究院发布的《全球工业互联网创新发展报告》[43]中观点认为当前全球各国重视并持续升级工业互联网安全防御体系，但针对工业互联网的攻击威胁不断加剧，全球工业互联网安全发展仍面临巨大挑战，其中，包括工控设备网络攻击日益频繁，工控系统普遍缺乏安全设计等；例如，2022 年 3 月，美国罗克韦尔自动化公司的 PLC 和工程工作站软件中曝出 2 个零日漏洞，攻击者可以利用这些漏洞向工控系统注入恶意代码并秘密修改自动化流程。

除此事件之外，2022 年工业互联网基础设施脆弱性风险情况又是如何呢？作为入选国家工业信息安全发展研究中心“2023 年度工业信息安全监测应急支撑单位”[44]的能力型安全企业，安天一直以来都极其关注工业信息安全领域的安全防护和运营，强化能力型安全产品落地，同时加强面向物联网、工业场景的安全价值落地；针对本年度工业互联网基础设施脆弱性风险披露的部分情况[45]，简要汇总如下表所示：

表格 1 2022 年工业互联网基础设施脆弱性风险披露情况（部分）

序号	时间	涉及工业互联网基础设施对象	该对象脆弱性风险相关信息
1	2022 年 3 月	西门子 RUGGEDCOM ROX 和 ROS 设备	西门子发布了 15 个新公告，向客户通报了 100 多个影响其产品的漏洞，其中包括使用第三方组件带来的 90 多个安全漏洞。描述第三方组件漏洞的三个公告与 RUGGEDCOM ROX 和 ROS 设备有关。受影响的组件包括 NSS 和 ISC DHCP。利用该漏洞可导致代码执行、拒绝服务（DoS）或泄露敏感信息。尽管西门子已经针对其中许多漏洞发布了补丁，但对于某些漏洞，这家德国工业巨头仅提供了缓解措施。
2	2022 年 4 月	ABB Symphony Plus SPIET800 和 PNI800 网络接口模块	瑞士工业技术公司 ABB 网络接口模块的漏洞使工业系统面临 DoS 攻击，该企业针对研究人员在该公司产品的一些网络接口模块中发现的三个严重漏洞开发修复补丁。由于这些产品处理某些数据包的方式存在缺陷，对控制网络具有本地访问权限或对系统服务器具有远程访问权限的攻击者可利用这些漏洞进行拒绝服务攻击，用户只能通过手动重启来解决。ABB 表示，利用这些漏洞可能会导致工业环境中断，除了直接影响 SPIET800 和 PNI800 设备外，连接到这些设备的系统也将受到影响。
3	2022 年 4 月	Elcomplus SmartPTT SCADA	自动化公司 Elcomplus 的 SmartPTT SCADA 被披露存在 9 个漏洞。该产品将 SCADA/IIoT 系统的功能与专业无线电系统的调度软件相结合。安全漏洞列表包括路径遍历、跨站脚本(XSS)、任意文件上传、授权绕过、跨站请求伪造(CSRF)和信息泄露漏洞。利用这些漏洞，攻击者可以上传文件、读取或写入系统上的任意文件、获取以明文形式存储的凭证、代表用户执行各种操作、执行任意代码，并提高访问管理功能的权限。
4	2022 年 6 月	Korenix JetPort 工业串行设备服务器	Korenix JetPort 工业串行设备服务器被披露存在后门账户。Korenix JetPort 工业串行设备服务器有一个后门账户，有问题的帐户可以被网络上的攻击者利用来访问设备的操作系统并获得完全控制。攻击者可以重新配置设备，并可能获得连接到服务器的其他系统的访问权。
5	2022 年 6 月	Carrier LenelS2 Mercury 门禁控制面板	Carrier 的 LenelS2 Mercury 门禁控制面板被发现 8 个零日漏洞。这些漏洞影响 LenelS2 Mercury 访问控制面板，该面板用于授予对设施的物理访问权，并与更复杂的楼宇自动化部署集成。其中一些问题需要缓解，而大多数问题可以在固件更新中解决。
6	2022 年 6 月	西门子 SINEMA 远程连接服务器施耐德电气 IGSS SCADA 产品数据服务器模块、C-Bus 家庭自动化产品	西门子和施耐德电气发布了 2022 年 6 月的补丁公告，宣布共修复了 80 多个影响其产品的漏洞。其中 30 个漏洞会影响 SINEMA 远程连接服务器。这些安全漏洞(其中许多会影响第三方组件)可能导致远程代码执行、身份验证绕过、权限提升、命令注入和信息泄露；施耐德电气发布了建议，以解决在 IGSS SCADA 产品的数据服务器模块中发现了七个可用于远程代码执行的严重漏洞，在 C-Bus 家庭自动化产品中发现了两个与身份验证相关的关键漏洞。

7	2022 年 6 月	多个 OT 设备制造商（西门子、摩托罗拉、霍尼韦尔、横河、ProConOS、爱默生、宾利内华达州、欧姆龙和 JTEKT）	多个 OT 设备制造商被披露受到 56 个“ICEFALL”漏洞的影响。安全研究人员发现了 56 个新的漏洞，统称为“ICEFALL”，这些漏洞影响到为关键基础设施组织提供服务的几家最大的 OT 设备制造商。这些漏洞被分为四大类:不安全的工程协议、弱加密或损坏的认证方案、不安全的固件更新和通过本地功能远程执行代码。
8	2022 年 6 月	AutomationDirect PLC 和 HMI 产品	AutomationDirect 宣布已修复其 PLC 和 HMI 产品中的几个漏洞。AutomationDirect 已经修补了其部分可编程逻辑控制器(PLC)和人机界面(HMI)产品中的几个严重漏洞。攻击者可以通过这些漏洞造成破坏，并对目标设备进行未经授权的更改。这些安全漏洞已在固件版本 6.73 中修复。CISA 的另外两项公告描述了 DirectLOGIC PLC 中的漏洞，一项针对串行通信，一项针对以太网通信。
9	2022 年 8 月	NetModule 路由器软件(NRSW)	NetModule 路由器软件中的两个关键漏洞，远程攻击者可以利用这些漏洞绕过身份验证和访问管理功能。
10	2022 年 8 月	OPC UA 协议	研究人员披露 OPC UA 协议漏洞详细信息。软件开发和安全解决方案提供商 JFrog 披露了影响 OPC UA 协议的几个漏洞的详细信息，包括其员工在早些时候的黑客竞赛中利用的漏洞。OPC UA（开放平台通信联合架构）是一种机器对机器通信协议，许多工业解决方案提供商使用它来确保各种类型的工业控制系统（ICS）之间的互操作性。
11	2022 年 9 月	Dataprobe iBoot-PDU 配电单元	美国网络安全和基础设施安全局(CISA)发布了工业控制系统(ICS)警告，指出 Dataprobe 的 iBoot-PDU 配电单元产品存在七个安全漏洞，该产品主要用于工业环境和数据中心，成功利用这些漏洞可能会导致在 Dataprobe iBoot-PDU 设备上执行未经身份验证的远程代码。iBoot-PDU 是一种配电单元(PDU)，它通过 Web 界面为用户提供实时监控功能和复杂的警报机制，从而控制 OT 环境中设备和其他设备的电源。
12	2022 年 11 月	ABB 石油和天然气流量计算机	瑞士工业技术公司 ABB 制造的石油和天然气流量计算机中存在安全漏洞，该漏洞可能允许攻击者造成中断并阻止公用事业公司向其客户收费。整个漏洞攻击链允许未经验证的攻击者以 root 权限执行任意代码，攻击者可以完全控制设备并破坏其测量石油和天然气流量的能力，以此阻止受害公司向其客户收费。

由上表可知，本年度工业互联网基础设施脆弱性问题中，协议、软件、硬件等方面有关风险均有涉及，虽然其中部分脆弱性问题已经得到有关企业修复，但仍存在为数不少且可能不断新增的脆弱性风险处于可被攻击者利用的危险境地，亟待各相关方给予足够重视并采取行之有效的风险降低措施。**同时，国外有关涉事组织所暴露出的脆弱性风险，也为我国同类制造企业和工业互联网安全相关企业提供了重要的警示和参考作用。**

7.3 工业互联网基础设施面临新型攻击场景风险

2022 年 8 月，工业网络安全公司 Claroty 的研究团队 Team 82 通过概念验证（POC）利用及其研究白皮书和 DefCon 演示，揭示了一种新型攻击场景“Evil PLC Attack”[46][47]：攻击者入侵可编程逻辑控制器（PLC）后，并非将其作为攻击终点或最终目标，而是将其用作攻击跳板，使被入侵的 PLC 武器化，感染任何与该 PLC 通信的工程工作站（Engineering Workstation）及其它 PLC。

该团队研究人员为 Evil PLC 攻击设计了三种攻击场景：将 PLC 武器化以实现初始访问（Weaponizing PLCs to Achieve Initial Access）、攻击移动集成商（Attacking Traveling Integrators）、将 PLC 武器化为蜜罐（Weaponizing PLCs as a Honeypot）。其中，在第一种攻击场景中，PLC 是进入安全设施的唯一载体，攻击者入侵并武器化 PLC 后，可以等待工程师连接到该 PLC 并感染工程师工作站/作业终端，或者，故意导致 PLC 出现故障，负责 PLC 运维排障的工程师会被引诱至该 PLC 并使用其工程工作站连接该 PLC 检修故障，进而工程师工作站/作业终端被感染。

在第二种攻击场景中，攻击者可以基于当前工业互联网管理通常涉及与许多不同组织网络和 PLC 交互的第三方系统集成商或承包商工程师的现状，利用他们作为不断入侵全球各地不同组织和站点的摆渡载体，一个被已入侵 PLC 感染的工程师工作站/作业终端可能会将恶意代码传播到其他多个企业，攻击者可以进一步入侵更多其他组织内部新的 PLC 以及工程工作站，从而持续扩大 Evil PLC 的影响范围。

面对上述工业互联网基础设施所面临的新型攻击场景风险，各相关方应及时变通防御思路，尽快制定行之有效的针对性防御方案。

7.4 工业互联网被盗数据交易新市场出现

2022 年 4 月，一个名为“Industrial Spy（工业间谍）”的暗网市场出现，其背后的网空威胁行为体在表层网络设置了用于宣传和引导访问其暗网地址的网站，并在该网站上宣称“在那里，您可以免费购买或下载竞争对手的隐私和不宜泄露的数据。我们公开计划方案、图纸、技术、政治和军事机密、会计报告和客户数据库。所有这些都是从全球最大的公司、企业集团和每一项活动中收集来的。我们利用他们 IT 基础架构中的漏洞收集数据。”；且从此后陆续被网络安全防御方捕获到的 Industrial Spy 恶意代码样本来看，其背后的网空威胁行为体从 2022 年 5 月开始推出了其自己的勒索软件[48]，试图打造从加密到售卖的罪恶“一条龙服务”。

对于此种与工业互联网安全具有相关性、以被盗数据交易为勾当的暗网市场出现及其发展，工业互联网各相关方也应给予必要的关注和对应防御措施的强化。

8 威胁泛化

在 2013 年，安天用恶意代码泛化（Malware/Other）一词表示安全威胁向智能设备、物联网等新领域的演进，此后“泛化”一直是安天所研究的重要威胁趋势。威胁泛化导致用户的资产暴露面增加，攻击者利用增加的攻击面可以产生非授权访问、跳板攻击、入侵“隔离网络”、资产被控、资产破坏、数据泄露等广泛的安全威胁。

党的二十大报告指出，“加快发展物联网，建设高效顺畅的流通体系，降低物流成本。加快发展数字经济，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。”物联网等科学技术的发展对于建设网络强国、实现社会主义现代化强国具有重要意义。2022 年，全球物联网设备数量预计达到 350 亿台，物联网技术将被广泛应用于制造、农业、交通、能源、物流、基建、医疗等多个领域。

然而，物联网的开放性、多源异构性、终端设备和应用的多样性、复杂性，使得物联网安全问题日益凸显。物联网在交互过程中，整个生命周期均有可能被攻击，包括物理攻击、认证攻击、协议攻击、通信攻击等。智能汽车的智能化功能提供了许多便利，但是车载系统及无线钥匙中的安全问题能够让攻击者获取控制权，例如，2022 年 10 月欧洲刑警组织捣毁了一个专门入侵汽车无钥匙解锁系统的黑客团伙，逮捕 31 名嫌疑人并没收超过 100 万美元（约人民币 775 万元）的犯罪资产。又譬如智能家居领域，智能摄像头是智能家居中的重灾区，智能门铃、智能摄像头成为攻击者窃听和偷窥的渠道，人们的居家隐私面临威胁。AI 技术正在被积极应用到各行各业中，然而有研究报告警告，这种新兴技术很容易被网络犯罪分子、不法黑客所利用，例如，攻击者会以领袖人物为目标，使用 AI 进行语音合成模拟，通过人脸识别漏洞绕过身份认证等，期骗 GPS 误导船只、误导自动驾驶车辆、修改 AI 驱动的导弹目标等。复杂多样的物联网设备的脆弱性也使网络攻击者有了更多的选择。2022 年 12 月，安天在《海莲花组织 Torii 远控的网络攻击活动分析》[7]一文中，揭示了海莲花组织针对我国重要政企单位的物联网设备发起的攻击活动。

云计算技术与物联网的深入融合，使得安全场景变得更加复杂和分散，企业内部和云端都会不可避免的管理更宽的攻击面。安全入侵的风险不断增加。云主机和物联网设备成为僵尸网络和挖矿木马的首选目标。大多数物联网设备包括严重的安全问题，如弱密码、对管理系统的开放访问、默认管理凭据或弱安全配置。僵尸网络攻击抓住物联网漏洞的机会来控制设备，并导致在线服务的中断，实现大量的 DDoS 攻击流量，其中 Mirai 是僵尸网络的头号杀手。近两年挖矿木马猖獗，而云端服务的兴起成为挖矿团伙的新战场。目前活跃的挖矿的黑客组织包括 Outlaw、TeamTNT 等都是活跃的针对云主机进行挖矿的组织。对于企业而言，有

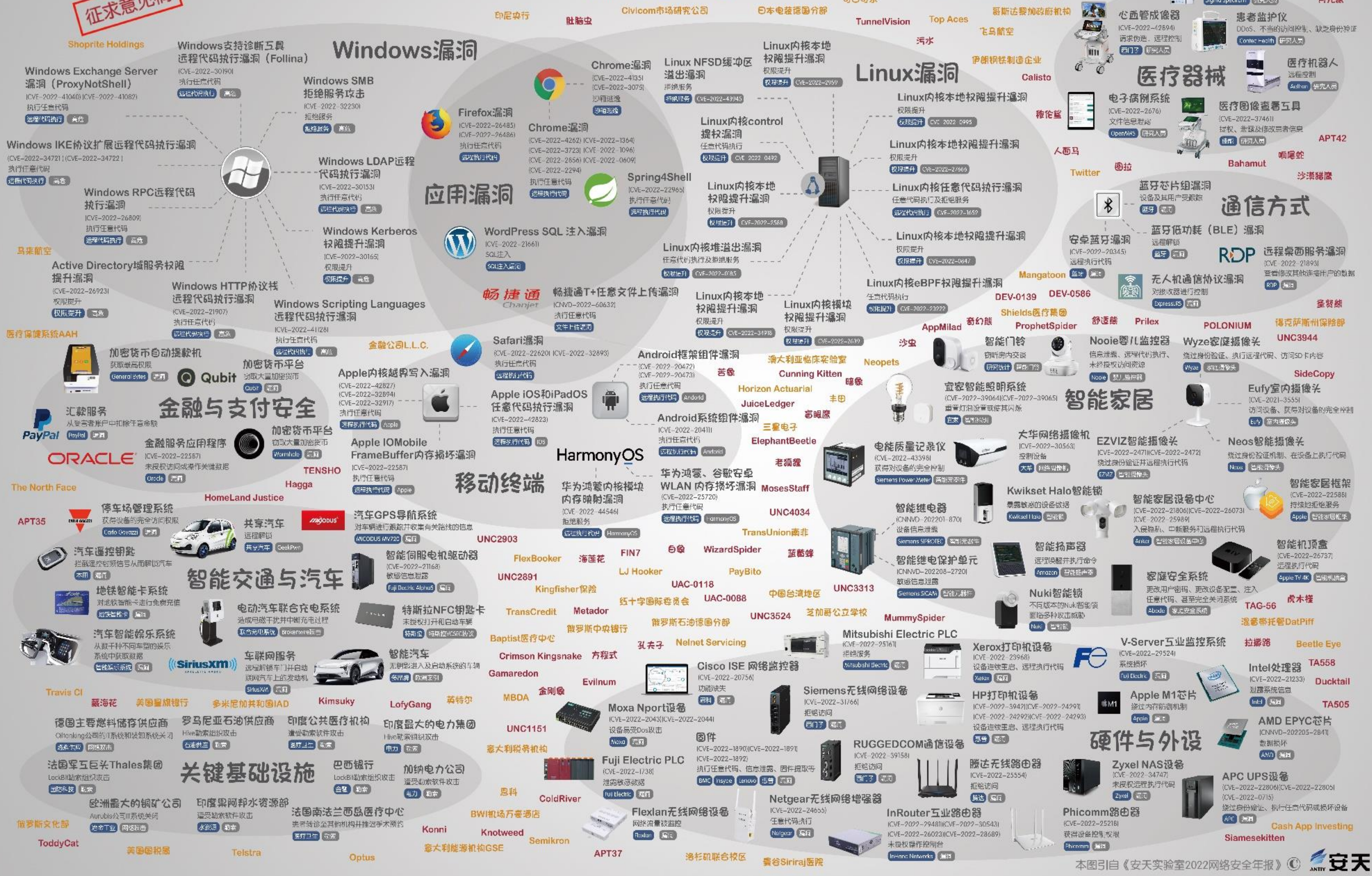
效的安全策略就是尽可能地提前做好预判和准备：掌握有价值的云资产在哪里？哪些云应用缺陷有可能影响业务运转，在此基础上，安全人员需要尽快解决必要的云安全问题。

此外，针对关键基础设施的攻击日益严重。一方面，网络战已经成为现代战争中的重要部分，“俄乌冲突”中双方针对关键基础设施的攻防成为网络战的关键，大规模的攻击直接导致交通、医疗、通信、电力及基础设施瘫痪。另一方面，网络犯罪组织也对关键基础设施发起一系列复杂的网络攻击，其中针对医疗机构的攻击尤为突出。许多机构组织忽视设备的安全性，加上关键基础设施设备常常会涉及硬件、固件方面的安全问题，导致物联网设备无法得到及时的更新，许多设备中仍然存在已知漏洞，留下了安全隐患。金融、电力、医疗等设施面临诸多挑战。一个个技术漏洞、产品后门，都是深埋着的“定时炸弹”，随时可能被主动或被动地引爆，给上到国家下到百姓的利益带来灾难性的打击。

当前，安全威胁泛化已经成为常态。安天依然采用与前几年年报中发布“网络安全威胁泛化与分布”一样的方式，以一张新的图表来说明 2022 年威胁泛化的形势。

2022网络安全威胁泛化与分布

征求意见稿



本图引自《安天实验室2022网络安全年报》 © 安天

附录一：参考资料

[1] 清华大学人工智能国际治理研究院.【AIIG 观察第 107 期】美国国家情报委员会前主席：亟需重新定义互联网治理，保护互联网的非政治地位和开放性
https://www.d-arts.cn/article/article_info/key/MTIwMzU3OTAwNDOD33mrsIa0cw.html

[2] ESET.HermeticWiper: New data-wiping malware hits Ukraine
https://www.eset.com/sg/about/newsroom/press-releases1/products/hermeticwiper-new-data-wiping-malware-hits-ukraine/

[3] Microsoft.Defending Ukraine: Early Lessons from the Cyber War
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[4] Juan Andres Guerrero-Saade and Max van Amerongen.AcidRain | A Modem Wiper Rains Down on Europe
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/#:~:text=AcidRain%20is%20the%207th%20wiper%20malware%20associated%20with,in%20the%20February%2024th%20attack%20against%20their%20modems.

[5] Securonix Threat Labs, Threat Research: D. Iuzvyk, T. Peck, O. Kolesnikov.Securonix Threat Labs Initial Coverage Advisory: STIFF#BIZON Detection Using Securonix – New Attack Campaign Observed Possibly Linked to Konni/APT37 (North Korea)
https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/

[6] 安天.“暗象”组织：潜藏十年的网络攻击
https://www.antiy.com/response/20220617.html

[7] 安天.海莲花组织 Torii 远控的网络攻击活动分析
https://www.antiy.cn/research/notice&report/research_report/20221202.html

[8] Mandiant.UNC3524: Eye Spy on Your Email
https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

[9] 安天针对攻击乌克兰等国的“必加”(PETYA)病毒分析与应对
https://www.antiy.com/response/petya/petya.pdf

[10] U.S. DEPARTMENT OF THE TREASURY.Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities
https://home.treasury.gov/news/press-releases/jy0941

[11] CERT-UA.Кібератака на державні організації України з використанням шкідливої програми RomCom. Можлива причетність Cuba Ransomware aka Tropical Scorpius aka UNC2596 (CERT-UA#5509)
https://cert.gov.ua/article/2394117

[12] Microsoft Threat Intelligence Center (MSTIC),Microsoft Digital Security Unit (DSU). North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware
https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

[13] Sergiu Gatlan.New ransomware strains linked to North Korean govt hackers
https://www.bleepingcomputer.com/news/security/new-ransomware-strains-linked-to-north-korean-govt-hackers/

[14] Trend Micro Research.Cyberattacks are Prominent in the Russia-Ukraine Conflict
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

[15] Microsoft Threat Intelligence Center (MSTIC),Microsoft Digital Security Unit (DSU),Microsoft Defender Threat Intelligence,Microsoft Detection and Response Team (DART).Destructive malware targeting Ukrainian organizations
https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[16] kaspersky daily.Ransomware as a distraction
https://www.kaspersky.com/blog/hermeticransom-hermeticwiper-attacks-2022/43825/

[17] Lawrence Abrams.Beware: Onyx ransomware destroys files instead of encrypting them
https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

[18] Lawrence Abrams.Microsoft confirms they were hacked by Lapsus$ extortion group
https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/

[19] Sergiu Gatlan.Ransomware data theft tool may show a shift in extortion tactics
https://www.bleepingcomputer.com/news/security/ransomware-data-theft-tool-may-show-a-shift-in-extortion-tactics/

[20] CrowdStrike.CYBER BIG GAME HUNTING
https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/#:~:text=Cyber%20big%20game%20hunting%20is,organizations%20or%20high%2Dprofile%20entities.

[21] 安天.双平台传播——活跃的 H2Miner 组织挖矿分析

https://www.antiy.cn/research/notice&report/research_report/20211117.html

[22] 安天.“8220”挖矿组织活动分析

https://www.antiy.cn/research/notice&report/research_report/20220428.html

[23] 安天.活跃的 Hezb 挖矿木马分析

https://www.antiy.cn/research/notice&report/research_report/20220705.html

[24] 安天.活跃的 Kthmimu 挖矿木马分析

https://www.antiy.cn/research/notice&report/research_report/20220527.html

[25] 安天.典型挖矿家族系列分析一 丨 Outlaw（亡命徒）挖矿僵尸网络

https://www.antiy.cn/research/notice&report/research_report/20221103.html

[26] Sergiu Gatlan.AstraLocker ransomware shuts down and releases decryptors

https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/

[27] 国家互联网应急响应中心.CNCERT/CC 互联网安全威胁报告

https://www.cert.org.cn/publish/main/45/index.html

[28] BBC.Ukraine cyber-attack: Russia to blame for hack, says Kyiv

https://www.bbc.com/news/world-europe-59992531

[29] 中国新闻网.俄媒：“匿名者”黑客组织宣布发起对俄“网络战争”

https://www.chinanews.com.cn/gj/2022/02-25/9685853.shtml

[30] 国家互联网应急响应中心.我国互联网遭受境外网络攻击

https://www.cert.org.cn/publish/main/8/2022/20220311172614196863695/20220311172614196863695_.html

[31] 河北网络安全（河北省委网信办信息安全测评中心官方号）.物联网僵尸网络已成为助长 DDoS 攻击的土壤

https://baijiahao.baidu.com/s?id=1741489828389779000&wfr=spider&for=pc

[32] CNCERT 国家工程研究中心.物联网安全威胁情报

https://mp.weixin.qq.com/s/t7gMWthB6W3vF_SA7gk_QA

[33] Randori. The State of Attack Surface Management 2022

https://www.randori.com/reports/the-state-of-attack-surface-management-2022/

[34] ISC 2022，零零信安 CEO 王宇.外部攻击面管理（EASM）技术发展与实践

http://vd3.bdstatic.com/mda-nerbmg8n8fsead78/360p/h264/1653553480461981126/mda-nerbmg8n8fsead78.mp4

[35] 中国信息安全测评中心.《2022 上半年网络安全漏洞态势观察》

http://www.itsec.gov.cn/zxxw/202209/t20220902_112723.html

[36] 安全内参.ChatGPT 在信息安全领域的应用前景
https://www.secrss.com/articles/49912
[37] 网信中国.国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定
https://mp.weixin.qq.com/s/JvME41TaNixTLQXC2mYMqg
[38] 安全内参.某医疗机构公众号系统漏洞遭利用，攻击者窃取 10 余万条公民数据境外售卖被抓
https://www.secrss.com/articles/49228
[39] 国务院.国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见
http://www.gov.cn/zhengce/content/2017-11/27/content_5242582.htm
[40] 工业和信息化部.关于印发《工业互联网发展行动计划（2018-2020 年）》和《工业互联网专项工作组 2018 年工作计划》的通知
https://www.miit.gov.cn/zwgk/zcwj/wjfb/zh/art/2020/art_3feeff24ae854421b06134a9efd73753.html
[41] 工业和信息化部办公厅.工业和信息化部办公厅关于推动工业互联网加快发展的通知
https://www.miit.gov.cn/jgsj/xgj/wjfb/art/2020/art_56f2702b081743bfa6be118b6d2e336e.html
[42] 工业和信息化部.关于印发《工业互联网创新发展行动计划（2021-2023 年）》的通知
https://www.miit.gov.cn/jgsj/xgj/gzdt/art/2021/art_ecb6ec1ddbf748eebe05ac69c086339d.html
[43] 中国工业互联网研究院.全球工业互联网创新发展报告
https://www.china-aii.com/achievements?id=754ae9ca-9f42-46f4-9f1d-2a7bc7b28936&ty=2
[44] 安天.安天入选 2023 年度工业信息安全监测应急支撑单位
https://mp.weixin.qq.com/s/exhZeF8oNsyDkcKyGvYqaQ
[45] 安天.威胁分析与研究-威胁资讯-每日安全资讯
https://www.antiy.cn/research/respond/safe_info/index.html#
[46] Team82, Claroty Research Team.EVIL PLC ATTACK : WEAPONIZING PLCS
https://claroty-statamic-assets.nyc3.digitaloceanspaces.com/resource-downloads/team82-evil-plc-attack-research-paper.pdf
[47] CNCERT 国家工程研究中心.PLC 成攻击跳板--邪恶的 PLC 攻击：将 PLC 武器化
https://mp.weixin.qq.com/s?__biz=MzUzNDYxOTA1NA==&mid=2247530557&idx=2&sn=1b7fead602769b072c6318fb7e0e600b&scene=21#wechat_redirect
[48] Atinderpal Singh.Technical Analysis of Industrial Spy Ransomware
https://www.zscaler.com/blogs/security-research/technical-analysis-industrial-spy-ransomware