2021
攻击技术发展
趋势报告

北京航空航天大学 华中科技大学 HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY 成都信息工程大学 Chengdu University of Information Technology 浙江警察学院 Zhejiang Police College

NSFOCUS绿盟科技

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

版权声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

NSFOCUS

CONTENTS

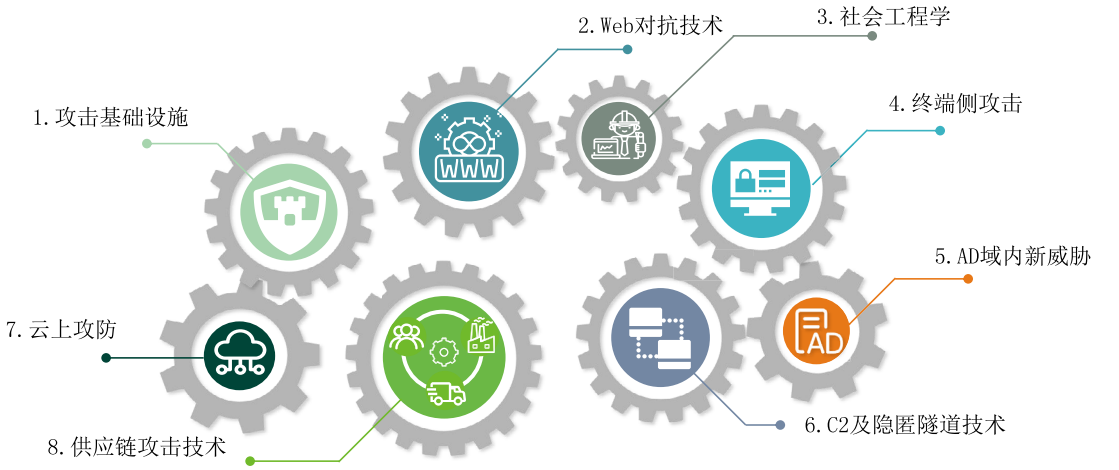
1

年度攻击技术发展趋势

随着网络技术的快速迭代，在日益复杂的国际关系和地缘政治斗争的大背景下，网络空间已然成为大国博弈的激烈对抗领域。以 APT（Advanced Persistent Threat，高级持续威胁）为主的体系化攻击已成为网络空间威胁的常态。在网络空间攻防博弈新变局的复杂形势下，如何正确认知网络空间进攻与防御之间的关系，是认识和理解网络空间威慑问题的关键。

一般而言，网络空间中普遍存在着进攻占据优势（Offence Dominance）的概念，攻击者日益精进的攻击技术和网络武器不断使得网络空间威胁存在多变。为了弥补攻防不对等的状态，作为防守方需要“知己知彼”，提前了解攻击者的能力与手段，才能在行动中占得先机，提前构建有针对性的防护措施，避免发生灾难。作为网络蓝军，更有义务去跟进研究实网威胁，掌握攻击技术发展趋势，从而更好的完成威胁模拟，推动建设网络空间防御体系，达到制衡效果。

绿盟科技联合北京航空航天大学、华中科技大学、成都信息工程大学、浙江警察学院一同发布了行业首个攻击技术发展趋势年度报告，基于对全年网空威胁攻击技术的跟进研究，甄选年度热点攻击技术和在未来可能大规模使用的新型攻击技术，分为八大重点方向进行研究解读并研判攻击技术发展新趋势。



1.1 攻击基础设施云化

攻击组织在实施攻击活动时，必须要应对高强高压的对抗环境。除了大家熟知的自动化利用工具之外，往往需要一系列辅助技术及支撑设施，才能保障在攻击全生命周期中，能够快速、隐蔽、有效地使用攻击武器、实施攻击活动。如攻击者租赁的服务器、域名、第三方网络服务，通过攻击手段或滥用手段恶意利用的服务器、网站及其他服务等，这些辅助技术

及设施都是攻击基础设施。打一个比方，如果将攻防对抗活动看作一次战斗，攻击基础设施则是在战斗前挖掘的阵地战壕。为了更真实地模拟高级攻击活动，验证安全防御体系的防御效果，攻击基础设施已成为蓝军团队必备技术之一。

近两年，蓝军研究团队已经开展了体系化的攻击基础设施设计，持续融入前沿技术，维护基础设施，提供辅助能力。在对抗升级的高压下，为了支撑蓝军行动 OPSEC（Operations Security，即行动安全）的要求，攻击基础设施从最初支撑发起攻击活动，发展为作战掩体，同时要具备自动化、弹性、可编排部署等特性。

- 今年 C2 保护技术已经从我们熟知的 CDN 前置、Nginx 等 Web 服务器反向代理前置、端口转发前置及 Tor 前置等技术，转向依托**云原生能力**，如今年在攻防演练中大量出现的 **FaaS 滥用技术，以及我们发现的 CDN 前置结合 FaaS 云原生能力多重隐蔽技术**等；
- 为了满足 OPSEC，支撑高强度对抗和复杂攻击战术的实施，攻击基础设施面临**配置复杂、重复性工作量大、弹性需求急迫的挑战，容器化、编排**和其他现代化技术为其注入了新的活力，促进**攻击云基础设施 DevOps** 发展。
- 云原生服务应用开发和部署的便捷性会为攻击者搭建攻击基础设施提供更灵活的方案，增加其战术技术多样性。据此，**我们提出了可扩展云原生攻击基础设施架构**，将更多的攻击基础设施与云原生能力相结合，进一步为蓝军行动提供高隐蔽性和持续性的辅助能力。

随着云计算、云原生、5G 通信等技术的发展，寻找其可能存在的滥用使用方法，并与之结合在攻击基础设施内，已成为必然趋势。

1.2 Web 对抗高隐匿性及组合利用链

Web 应用作为企业主要的开放入口，仍然是攻击者重点关注的对象。SQL 注入、XSS、反序列化等经典漏洞，由于其利用成本低、攻击效果显著，时至今日仍然被广泛利用。Web 应用从单机架构演变到如今分布式下的云原生架构，DevOps 的各个阶段都离不开 API 的交互调用，Web API 数量正以爆发式的速度增长，传统的 Web 漏洞仍然是其主要的威胁。攻击者常利用 Web 应用来突破目标网络，将 Web 服务器当作跳板转发流量并进入到内网，继而开展后渗透攻击流程。如何在高压对抗环境下支持蓝军 OPSEC 的行动，Web 权限获取以及维持成为了 Web 对抗技术的研究重点。

- 随着攻防对抗的强度越来越高，各大厂商的流量分析、EDR 等专业安全设备已被广泛使用，对于 Webshell 的检测能力也愈发成熟，传统的落地文件型 Webshell 生存空间越来越小。内存型 Webshell（MemWebshell）应运而生，**其具备无文件落地、高隐匿等 OPSEC 的特点**，深受攻击者的青睐。

- OWASP Top 10 Web 应用安全风险在 2021 年进行了更新，相比于 2017 年发布的版本已经发生了巨大的变化。随着防御方的安全建设越来越规范，注入类漏洞的利用难度增加，**称霸榜首多年的注入类风险也被权限控制类风险所替代**。今年已出现的多个漏洞就是**将权限类风险与传统漏洞相结合**，从而打造出更具杀伤力的漏洞利用链。

Web 架构日益复杂，其中涉及的框架、组件、技术越来越多，从底层的云主机的创建和管理，到 CI/CD 持续集成与交付部署的流程，再到上层的 Web 应用服务程序，最后到服务的下线与资源的回收，API 的使用伴随着 DevOps 的生命周期，稍有编码或配置上的不当，就会成为蓝军可以利用的攻击面，突破目标网络最终获取服务器的权限，Web 应用上的攻防对抗仍然是未来的主要战场。

1.3 社工工程学强伪装性和自动化

自《欺骗的艺术》一书问世以来，人们才认识到人为因素才是安全的软肋，利用人心理上的弱点和习惯上的漏洞，一样可以达到攻击效果。利用社会工程学，攻击者可以欺骗用户绕过安全防御措施，甚至使用户主动提供登录凭据等敏感信息。社会工程学已经成为攻击组织、黑灰产组织最常使用的技术手段之一。尽管安全人员已经对社会工程学足够重视，且对其设计了多种防护软件和安全措施，定期组织了人员安全意识培训，但从曝光的多起攻击事件和 APT 组织攻击活动来看，社会工程学结合当前的主流技术进行伪装，依然能让受害者轻易的上钩。

- 钓鱼网站攻击作为一种典型的社会工程学技术，已经从注册相似域名、模仿页面样式等伪装技术，转向**依托一些可信的服务、功能来进行伪装**，其中利用可信云服务来托管钓鱼网站的趋势尤为明显；

- 邮件钓鱼作为最常用的社会工程学攻击方式，在邮件安全网关的严防死守下，钓鱼邮件数量不减反增。**利用复杂性技术绕过安全拦截的邮件钓鱼趋势明显**，由于邮件天生的便利性和普及性，在未来邮件钓鱼仍是社会工程学攻击的主要手段；

- **社会工程学攻击趋向自动化**，今年，大量邮件钓鱼活动利用网络钓鱼即服务（PhaaS）进行全过程自动化攻击，而随着自动化技术的进一步发展，水坑攻击、鱼叉钓鱼等其他形式的社会工程学攻击也将出现自动化趋势。

今年，社会工程学已经能借助自动化技术，持续地猎取猎物。蓝军攻击技术研究人员需要掌握社会工程学最新的技术手法，模拟攻击，提前预警，防患于未然。此外，从曝光的多起攻击事件和 APT 组织攻击活动来看，社会工程学因为具备很多特殊的优势而被大量高级攻击组织所使用，通过依托一些可信的服务、功能进行伪装后极具欺骗性。

1.4 终端侧攻击关注合法功能滥用

随着 EDR 等现代化安全防御体系的普及，攻击方已从传统的免杀逐步趋于通过主动对抗、规则绕过、检测规避等隐匿手段来保障完成自己的攻击行为，EDR/EPP 对抗已成为攻击安全社区的热点研究内容。其中针对系统合法功能的滥用技术及 .NET 武器化受到了攻击者的热捧。

- 围绕 EDR 的检测和规避技术已成为终端对抗中的重中之重。**UNHOOK 和 SYSCALL 技术已成为攻击者绕过 EDR 挂钩的共识**，运用这些技术手段可导致 EDR 检测出现缺失，从而使攻击者可以发起更多的攻击而不被 EDR 检测到，降低了暴露风险。此外，针对内核态 EDR 驱动的攻击已出现在今年的安全攻击事件中，**围绕内核和驱动相关的攻防或成为未来 EDR 对抗的新热点**；

- **滥用系统合法功能和 API 的攻击手法明显增多**。CLFS 文件系统、数字签名验证机制等由于其本身的合法性，滥用其隐匿恶意载荷的攻击将难以被发现与拦截，致使绕过安全产品检测，投递至系统平台中并执行变得更加容易，对终端安全造成威胁，这也对现有安全产品的检测能力提出了更高的要求；

- 武器化程度不断提高，在经过 PowerShell 恶意利用的热潮之后，**CSharp 已经接过其热度成为攻击性武器的主力开发语言**。其他新晋语言如 Nim-Lang 的武器化开发项目不断涌现，新的静态特征和行为模式不为现有安全产品所熟悉，对其检测和防御能力相对薄弱。

在持续对抗的过程中，攻防双方不断加码，出现了越来越多的新兴攻击手段，这要求蓝军安全人员需要在真正的攻击发生之前，先敌一步对新型攻击技术进行预判和研究，主动防御攻击、降低威胁，以使终端设备更加安全。

1.5 AD 域攻击面增大

在企业网络的建设当中，经常会使用 AD 域（Active Directory Domain）划分企业组织架构和不同的权限角色，来组织和管理企业内部的人员账号和计算机终端。在 AD 域中，由最高权限的域管理员 DA 来管理域控制器 DC，DC 包含了由该域的账号、密码、计算机、相互之间的权限和信任关系等组成的数据库。因此，AD 域安全在企业内部网络当中显得极其重要，而域控制器 DC 和相关的服务、账号等也成为了攻击者的主要攻击目标，比如域内的打印机服务、CS 证书服务、FS 联合认证服务、Exchange 邮件服务、SQL Server 数据库服务等也均是今年攻击技术社区中的重点研究对象，相关攻击技术不断被曝光。

- **PetitPotam 漏洞的出现使得存在了十多年的 NTLM 协议中继攻击实施更加便利，同时也首次证明了针对更安全的 Kerberos 协议的中继攻击可行性。中继攻击能够使得攻击者假冒域内的合法用户，进而访问域内资源或进行权限提升。**
- 随着新特性的增加和功能的扩展，AD 域能更好地满足企业用户兼顾内网与云上服务的使用场景，但同时也引入了新的攻击面。研究发现**针对 AD CS 和 AD FS 两种服务已出现了在野攻击利用**，如在 SolarWinds 供应链攻击事件的后渗透阶段就有所体现。**围绕 AD 服务相关的令牌窃取、横向移动及持久化攻击**技术须持续关注。
- 企业邮件服务器是高级攻防对抗中重要的攻击目标之一，域中的 Exchange 服务又天然具备较高的权限，因此 Exchange 服务是域内的主要攻击目标之一。由 **CAS 支撑的 Exchange Web 服务已成为了主要的攻击面，SSRF、任意文件写入、反序列化远程代码执行等传统 Web 应用漏洞正严重威胁 Exchange 乃至整个 AD 域的安全。**

AD 域攻击技术的发展始终以突破 AD 域的访问边界为目的，通过不断获得更高的权限直至将权限提升为域管理员权限以控制整个域。复杂的业务架构也必将导致更为复杂的攻击链，可预见围绕 AD 域协议认证、AD 服务及应用的漏洞和新型攻击技术所带来的安全风险会持续增多。

1.6 C2 及隐匿隧道技术多样化

C2（Command and Control）技术是攻击者用来与受其控制的系统进行通信的相关技术。攻击者不仅利用其完成命令执行和控制指令的下发，更是用以支撑后渗透阶段的重型作战通道。攻击者通常试图模仿正常的、预期的流量以避免检测。根据受害者的网络结构和防御，攻击者可以通过多种方式建立具有各种隐身级别的 C2。CobaltStrike 作为一款成熟的商业 C2

框架被攻击者广泛使用，基于 CobalStrike 自身脆弱性进行检测捕获的技术也层出不穷，各种对抗技术也应运而生。

另一方面，隐匿隧道技术则帮助攻击者完成命令控制、载荷投递及信息渗出等。包括 DNS 协议在内的替代协议通讯手段一直被攻击方广泛使用，并在攻击实战中涌现出新的利用方式。在云服务蓬勃发展的大环境下，利用公共服务进行的载荷投递与通讯的实战案例日渐增多，手法也呈现多样化。

- BOF（Beacon Object Files）是 Cobalt Strike 为了迎合 OPSEC 需求在 4.1 版本发布时的一项新功能，它将攻击操作局限在了进程内部，规避了进程创建等敏感行为而导致的暴露风险。利用 BOF 技术攻击者可隐匿完成主机信息收集、凭据获取等攻击操作。**BOF 变革性地优化了后渗透阶段的命令执行流程，或成为承载后渗透阶段攻击操作的重要载体**。
- 围绕 Cobalt Strike 攻击载荷的内存对抗已愈发激烈。BeaconEye 是目前检测效果最好的 Beacon 内存检测工具，以堆块中存储的 Beacon 配置信息为扫描对象，可成功应对攻击方大部分的检测规避手段。但攻击方亦未坐以待毙，通过内存特征篡改与利用扫描算法缺陷等手段可巧妙绕过 BeaconEye 的内存检测。内存空间仍是攻防双方进行检测及对抗的必争之地。
- C2 服务器指纹识别定位已成为防守方进行威胁情报关联和溯源的关键手段。利用 Cobalt Strike TeamServer 自身设计缺陷进行的扫描和探测已被大量应用在各类公网资产测绘当中。**规避扫描与隐匿 TeamServer 成为了攻击方必然要解决的 OPSEC 问题**，定制 C2 Profile 与修改 Stage URI 生成算法成为了有效解决手段。
- **DNS 协议被大量应用于载荷投递和命令控制**。利用在合法字段中嵌入额外数据的手法，使攻击流量混入合法流量，具有较强的隐蔽性。在 SolarWinds 等攻击事件中，攻击者借助魔改的 DNS 协议在敲门上报阶段达到隐蔽通信的目的。
- **利用公共服务进行载荷投递与命令控制的手段呈现多样化**，包括公开云存储服务、代码托管、图床等，也出现了利用比特币交易记录这类较为新颖的手法。

攻防领域没有“银弹”，攻防技术在互相博弈中共同发展，并由浅入深地推动对 C2 本质的研究。攻防态势升级带来的军备竞赛为 C2 技术的发展注入了源动力，任何一种具有潜在利用价值的新技术都为新攻击技术诞生创造契机。伴随这种过程，操作安全 OPSEC 的价值

越加凸显，攻击者在完成攻击行为的同时越来越注重减少自身暴露风险，推动 C2 保护技术的发展。

1.7 云上攻防聚焦云原生安全

近年来，企业上云不断加速，相关技术落地成熟，公、私、混合云平台及业务得到长足发展。新冠疫情爆发以来，各行各业对远程办公、远程研发的需求大幅增加，进一步促进了云计算技术的发展和落地。进入云计算的下半场，以容器和 Kubernetes 为核心的云原生技术被越来越多的企业采用，大幅提高了生产效率。

与此同时，云计算安全风险和威胁也不断出现。2021 年以来，CVE-2021-30465、CVE-2021-25741 等可能导致容器逃逸的高危漏洞被陆续发现，TeamTNT 团伙利用云原生相关技术发起了多次攻击，这些事件表明，“上云”虽好，“云上”却并不平静。2021 年，以下三种云上攻击技术值得关注：

- **从 CVE-2019-5736 衍生的容器运行时信息收集技术**。利用这种技术，攻击者能够拿到目标容器平台的容器运行时程序文件，从而获得版本及潜在脆弱性信息，指导下一步行动。
- **针对云原生集群网络的中间人攻击技术**。利用这种技术，容器内的攻击者可能对集群网络发起攻击，实现流量劫持的目的。
- **基于 eBPF 机制的容器逃逸技术**。在容器环境的后渗透阶段，攻击者可能利用 eBPF 技术逃逸到宿主机上，进一步实施渗透。

以这三种技术来概括该领域全年的发展势必会挂一漏万。然而，技术是可归纳的，背后的思想和思维方式则是可演绎的；持续的归纳和演绎是攻防发展的驱动力，是价值所在，也是我们列出这三种技术的初衷。

1.8 供应链攻击增多并呈现多样化

供应链是设计、制造和分销产品所需的资源生态系统的组合。在网络安全领域，供应链包括硬件、软件、云或本地存储等各形态产品的分发机制。供应链攻击指的是攻击者通过在上游或中游介入，进行恶意活动并将其产生的后果向下游传播给众多用户。与孤立的安全漏洞相比，成功的供应链攻击往往规模更大，影响更深远。近年来，供应链攻击安全事件激增，供应链攻击已经成为重要的突破手段，值得蓝军团队持续关注。

- 针对开源软件代码的攻击技术方面，今年出现的**伪装补丁隐蔽引入漏洞**攻击模式和 Trojan Source 新型攻击技术都极具潜力，SDL 相关安全技术人员及管理人员需注意防范。
- 今年出现多个利用公共开源存储仓库伪装知名依赖库，通过**依赖混淆、恶意抢注**等攻击手段，传播恶意软件的攻击技术，建议 SDL 技术加入对开源项目来源的管控。
- 通过攻击软件供应商入侵下游企业的事件时有发生，在产品的研发阶段，针对 DevOps 理念在研发环境引入的新特性进行攻击极可能成为未来趋势，如**利用 IDE 社区生态下的第三方插件或扩展程序**组合构成漏洞环境，**利用 DevOps 的“供应链软件”漏洞**获得代码权限，都考验着现有的安全防御机制。随着 IT 云化，供应商的**凭证泄露形式**更加多样，在蓝军拟定攻击计划的范围也应扩大。对于下游企业来说，要严格管控**供应商的信任机制**，减少攻击面。
- 针对固件的攻击仍然是供应链攻击中不可忽视的一环，Intel BSSA DFT 漏洞 CVE-2021-0144（Intel-SA-00525）暴露了**利用 UEFI 生态系统**的复杂性实现大规模供应链攻击的潜在风险。由于**物联网设备厂商安全意识薄弱，设备固件往往缺乏签名等有效的校验机制，设备本身也经常不具备 SecureBoot 等安全机制**，导致物联网设备固件极易受到攻击。**甚至设备在出厂时固件可能就已经存在后门**，在升级 / 流通过程中也易被植入恶意代码。
- 今年欧盟网络安全智能机构欧盟网络与信息安全局（ENSIA）发布了**供应链攻击分类框架**，可以协助安全人员识别供应链攻击类型。

从供应链攻击发展趋势来看，未来攻击的手段和实施的途径将更加多元化，如何鉴别与防范来自“可信”对象的威胁对安全厂商提出了更高要求。

2

年度高可利用漏洞盘点

攻击者依然将 0day 挖掘和利用作为其占据攻防对抗技术优势的杀手锏。今年以来利用 0day 的攻击仍呈现爆发式增长，0day 攻击仍是攻击者进行网络突破和权限扩大的主要手段之一。另一方面，我们观察到攻击者能迅速利用最近披露的 1day 漏洞来破坏未打补丁的系统，部分原因是 COVID-19 流行期间远程办公使用的业务系统（例如虚拟专用网络 VPN 和基于云的环境），系统的快速扩展和越来越多的使用导致网络防护和运维人员存在维护不及时的情况。绿盟科技天机实验室和天元实验室据此观察统计了本年度被广泛利用的在野高危新增漏洞，建议各组织、单位及时打补丁、升级并可实施集中式补丁管理系统来缓解本报告中列出的漏洞。

漏洞类型	漏洞编号或名称	描述
打印机驱动漏洞	CVE-2021-1675/ CVE-2021-34527	本地权限提升；在域环境中，无需任何用户交互，未经身份验证的远程攻击者可以利用该漏洞以 SYSTEM 权限在域控制器上执行任意代码。
Windows 提权漏洞	CVE-2021-1648	出现在 splwow64.exe 地址空间内的任意指针解引用漏洞，成功利用此漏洞可以将低完整性级别进程提升至中完整性级别，该漏洞可配合 IE 浏览器任意代码执行漏洞实现沙箱逃逸，从而获得中完整性级别权限下的任意代码执行。
	CVE-2021-1732	win32kfull.sys 中的一个越界写漏洞，成功利用该漏洞可实现 Windows 系统下的本地权限提升。
	CVE-2021-31956	ntfs.sys 中的池溢出漏洞，成功利用该漏洞可实现 Windows 系统下的本地权限提升，同时该漏洞可以在浏览器沙箱中进行权限提升，实现沙箱逃逸。
	CVE-2021-36934（HiveNightmare）	权限限制出错，普通用户可以通过访问卷影备份中的 SAM、SECURITY 和 SYSTEM 等文件，并最终导致提权操作。
	CVE-2021-40449	win32k 中的 uaf 漏洞，成功利用该漏洞可实现 Windows 系统下的本地权限提升。
	CVE-2021-36942	LSA 欺骗漏洞，能够强制 Windows 主机向指定地址进行 NTLM 身份认证，与 NTLM 中继攻击可达到凭据窃取和权限提升的效果。
	CVE-2021-42287	该漏洞由于 KDC 对 Kerberos 特权属性证书 (PAC) 判断不严格， 导致攻击者可使用普通机器账户假冒域控制器账户，与 CVE-2021-42278、CVE-2021-42282、CVE-2021-42291 结合利用可达到在 AD 域从普通用户权限提升到域管理员的效果。
Linux 提权漏洞	CVE-2021-3156	sudo 存在基于堆的缓冲区溢出漏洞，普通用户成功利用该漏洞可将权限提升至 root。
	CVE-2021-22555	该漏洞是由于 Linux Netfilter 模块中 memcpy()、memset() 函数在使用过程中存在缺陷，导致攻击者可以利用漏洞实现权限提升，如果在容器场景下，可以从 docker、k8s 容器中实施容器逃逸。
	CVE-2021-31440	Linux 内核 eBPF verifier 存在边界计算错误漏洞，导致检查与运行时不一致，可以造成本地权限提升。
Exchange 漏洞	Proxylogon	SSRF 攻击和任意文件写入漏洞；通过多个漏洞的组合利用，攻击者可写入恶意 WebShell，获取 Exchange 服务器 System 权限，之后攻击者亦可通过 Exchange 管理特权威胁 DC 域控制器。
	Proxyshell	SSRF 攻击获取 PowerShell 执行权限，再恶意利用导出邮件功能可写入 WebShell，Exchange 服务器 System 权限，之后攻击者亦可通过 Exchange 管理特权威胁 DC 域控制器。
	CVE-2021-42321	Exchange 服务的 .Net 反序列化远程命令执行漏洞，攻击者利用此漏洞可成功获取 Exchange 服务器权限，亦可通过 Exchange 管理特权威胁 DC 域控制器。

漏洞类型	漏洞编号或名称	描述
浏览器漏洞	CVE-2021-21220	Chrome 远程代码执行漏洞，攻击者利用该漏洞可以对未开沙箱的 Chrome 浏览器造成远程代码执行；在沙箱环境下，结合沙箱逃逸漏洞可以形成完整攻击链。
	CVE-2021-21224	Chrome V8 类型混淆漏洞，攻击者利用该漏洞可以对未开沙箱的 Chrome 浏览器造成远程代码执行；在沙箱环境下，结合内核提权漏洞 CVE-2021-31956 可以实现沙箱逃逸，形成完整攻击链。
	CVE-2021-30551	Chrome V8 类型混淆漏洞，攻击者利用该漏洞可以对未开沙箱的 Chrome 浏览器造成远程代码执行；在沙箱环境下，结合沙箱逃逸漏洞可以形成完整攻击链。
	CVE-2021-40444	MSHTML 中的远程代码执行漏洞，可通过恶意 Microsoft Office 文档传播，存在该漏洞的计算机下载并点击恶意文档后将会执行远程任意代码。
虚拟化产品漏洞	CVE-2021-21985	未授权远程代码执行漏洞。攻击者不经授权任意调用当前上下文中 Bean 的方法。
	CVE-2021-22005	未授权任意文件写，但文件后缀限制为 JSON。可以通过写入 Crontab 定时任务或覆盖服务配置等方式达到 RCE 的效果。
WEB 应用漏洞	Weblogic 7u21 绕过反序列化漏洞	利用特殊类绕过 Weblogic 黑名单进行二次反序列化，通过 T3 协议发送未授权请求，实现自定义 Java 字节码的执行，完成内存型 Webshell 的注入。
	CVE-2021-44228（Log4Shell）	Log4j2 支持用户通过 JndiLookup 插件远程获取属性信息，由于查询地址未做限制导致的 JNDI 注入漏洞，能够进行代码执行、命令执行等操作。Log4j2 由于使用广泛，主流的组件、框架、应用会用其进行日志记录，导致将漏洞风险二次传播到许多公司业务系统中，产生新的攻击利用链。
安全设备漏洞	集权类和访问控制类安全设备相关漏洞	网络安全设备在企业网络内往往具有较高的管理和控制权限，同时又缺少必要的安全审计，因给了攻击者可乘之机。相关漏洞可能会致使内网大量主机系统权限丢失。

3

参与单位

天元实验室

专注于新型实战化攻防对抗技术研究。

研究目标包括: 漏洞利用技术、防御绕过技术、攻击隐匿技术、攻击持久化技术等蓝军技术，以及攻击技战术、攻击框架的研究。涵盖 Web 安全、终端安全、AD 安全、云安全等多个技术领域的攻击技术研究，以及工业互联网、车联网等业务场景的攻击技术研究。通过研究攻击对抗技术，从攻击视角提供识别风险的方法和手段，为威胁对抗提供决策支撑。

天机实验室

专注于攻防对抗技术。

研究方向主要包括漏洞挖掘技术研究、漏洞分析技术研究、漏洞利用技术研究、安全防御机制及对抗技术研究等。研究目标涵盖主流操作系统、流行的应用系统及软件、重要的基础组件库以及新兴的技术方向。

星云实验室

专注于云计算安全。

基于 IaaS 环境的安全防护，利用 SDN/NFV 等新技术和新理念，提出了软件定义安全的云安全防护体系。承担并完成多个国家、省、市以及行业重点单位创新研究课题，已成功孵化落地绿盟科技云安全解决方案。

天枢实验室
NSFOCUS TIANSHU LAB

天枢实验室

天枢实验室立足数据智能安全前沿研究，一方面运用大数据与人工智能技术提升攻击检测和防护能力，另一方面致力于解决大数据和人工智能发展过程中的安全问题，提升以攻防实战为核心的智能安全能力。

M01N

M01N 战队

绿盟科技 M01N 战队，专注于 Red Team、APT 等高级攻击技术、战术及威胁研究，涉及 WEB 安全、终端安全、AD 安全、云安全等相关领域。通过研判现网攻击技术发展方向，以攻促防，为风险识别及威胁对抗提供决策支撑，全面提升安全防护能力。

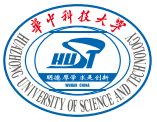
绿盟科技 M01N 团队依靠公司强大的安全研究体系，对焦行业前沿高级威胁及 Red Teaming 技术领域，结合绿盟科技高级威胁研判以情报导向完成对手仿真技术，高度模拟 APT 攻击战术技术，完整覆盖从应用到系统、从边界到内网、从本地到云端的攻击安全研究方向，全方位推动强化防御能力和改进流程。

M01N Team 公众号二维码：

北京航空航天大學

北京航空航天大学

北京航空航天大学（简称北航）成立于 1952 年，由当时的清华大学、北洋大学、厦门大学、四川大学等八所院校的航空系合并组建，是新中国第一所航空航天高等学府，现隶属于工业和信息化部。学校所在地北京，分为学院路校区、沙河校区，占地 3000 多亩，总建筑面积 170 余万平方米。建校以来，北航一直是国家重点建设的高校，是全国第一批 16 所重点高校之一，也是 80 年代恢复学位制度后全国第一批设立研究生院的 22 所高校之一，首批进入“211 工程”，2001 年进入“985 工程”，2013 年入选首批“2011 计划”国家协同创新中心，2017 年入选国家“双一流”建设高校名单。学校第十六次党员代表大会提出以建设扎根中国大地的世界一流大学为发展愿景目标。

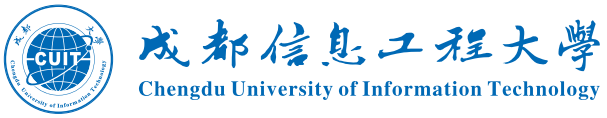


華中科技大學

HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

华中科技大学

华中科技大学是教育部直属的综合性研究型重点大学、国家首批世界一流大学建设高校（A 类），入选 "985 工程 "、"211 工程 "、" 强基计划 " 等。上世纪 80 年代就建立了信息安全实验室，于 2002 年建立了信息安全专业，同年设立硕士、博士学位授予点，是国内较早成立本专业的高校之一。2016 年成立网络空间安全学院，2019 年第一名入选全国一流网安示范学院、并入驻国家网络安全人才与创新基地。在人才培养方面实施“分级通关”综合实践能力培养方案，是目前国内唯一在本科教学中系统性推行综合实践能力培养的学校。承担了包括 973 计划项目“云计算安全基础理论与方法研究”、国家自然科学基金重点项目、科技部网络空间安全重点专项课题等多个国家重要项目，构建了相对领先的黄鹤网络靶场，为实战化人才培养提供平台支持，学院 L3HSec 战队已进入全国攻防第一梯队。



成都信息工程大学

成都信息工程大学是四川省和中国气象局共建、四川省重点发展的省属普通本科院校。学校创建于 1951 年，1956 年改制为中央气象局成都气象学校；1978 年升格为本科院校——成都气象学院；2000 年学校由中国气象局划转四川省，更名为成都信息工程学院；2001 年原隶属国家统计局的四川统计学校整体并入；2015 年更名为成都信息工程大学。学校是国家中西部基础能力建设工程高校、国家首批“卓越工程师教育培养计划”试点院校、四川省首批“一流学科建设”高校、四川省新增博士学位授予单位优先培育高校。

浙江警察学院

学校是浙江省唯一培养公安专门人才的本科高校，承担着本科学历教育、在职民警培训、公安理论研究和重大活动安保等职责，具有鲜明的公安行业特色和普通高校基本属性。学校坚持行业办学、注重内涵建设，现有公安学、公安技术学、网络空间安全 3 个学科，均为省一流建设学科。招生专业 8 个，其中涉外警务、网络安全与执法、治安学、交通管理工程等 4 个专业被认定为国家级一流本科专业建设点，侦查学、刑事科学技术、经济犯罪侦查、警务指挥与战术等 4 个专业被确定为省级一流本科专业建设点。学校是公安部全国县市公安局长培训基地、警务实战训练基地、科技信息化教育训练基地、国际刑警组织中国国家中心局教育训练基地，是公安部、商务部援外（外警）培训点。立足新发展阶段，学校将高举习近平新时代中国特色社会主义思想伟大旗帜，深入贯彻落实习近平法治思想、关于教育的重要论述及重要训词精神，坚持政治建校、从严治校，坚持以学生为中心、以教师为根本，改革创新、实干创业，努力把学校建成高质量内涵式有特色的重点公安院校。

NSFOCUS绿盟科技

扫描绿盟科技官微二维码
可在手机端直接观看报告电子书