

01

2023 年网络安全形势分析	9
----------------	---

02

2023年安全事件数据观察	5
2.1 金融行业与运营商成为重点攻击目标	6
2.2 挖矿事件趋势持续放缓，勒索事件占比最高	7
2.3 社工钓鱼和漏洞攻击为边界突破主要手段	8

03

网络安全趋势与典型事件分析	11
3.1 安全意识成演练对抗永恒主题，权限维持另辟蹊径	12
3.2 Java 应用与 ESXi 成为勒索攻击热点	16
3.3 恶意软件技巧升级，社工钓鱼仍需防范	19
3.4 AI 风潮下的网络安全风险与机遇	27
3.5 汽车电动化、网联化、智能化带来更多网络安全风险	31
3.6 K8S 逐渐成为主流，云安全意识需要提升	38
3.7 地区冲突引发网络战，攻击手段简单粗暴	43

04

安全漏洞变化趋势	45
4.1 安全漏洞趋势分析	46
4.2 重点漏洞盘点	49



05

数据安全风险上升，监管面临新要求	53
5.1 企业和医疗领域成攻击焦点	54
5.2 API 和文件传输应用漏洞成数据泄漏的主要威胁	56
5.3 数据安全法规趋于健全	56

06

典型安全事件汇总	58
6.1 挖矿蠕虫案例	59
6.2 钓鱼邮件案例	63
6.3 勒索攻击案例	67

07

安全建议	74
------	----

08

附录一 . GBT20986-2007 信息安全事件分类分级指南	77
----------------------------------	----

09

附录二 . 绿盟科技事件分类方法	79
------------------	----



2023年度 安全事件观察报告

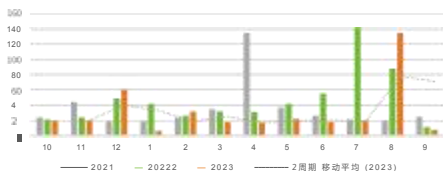


| 巨人背后的专家 |

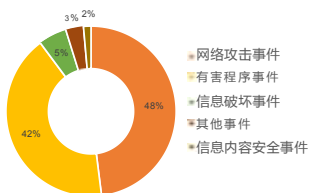
2023年网络安全形势分析

2023年安全事件数据整体呈现出平稳趋势，没有出现明显的波动。绿盟科技2023年接收安全事件376起，比2022年减少33.2%，第一季度事件总量100起，比2022年有所增长；从第二季度起，每季度的事件量均低于2022年同期。在2023年8月事件量达到年度峰值，事件量为135起，较2022年同期增长34.8%，较7月份增加了85.2%。绿盟科技在《GBT20986-2007信息安全事件分类分级指南》指导下，制定了信息安全事件分类方法。对处理的安全事件按照国标和绿盟科技安全事件分类标准分别进行统计。

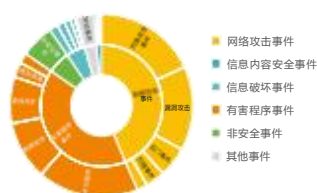
近三年事件发生趋势



国标事件类型分布



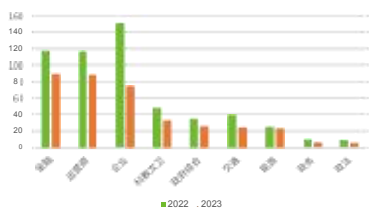
事件类型分布图



2023年安全事件数据观察

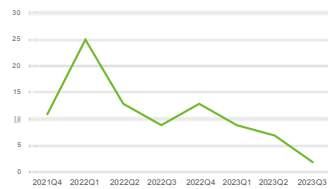
金融行业与运营商成为重点攻击目标。根据最近两年行业事件数据统计分析，可以看到金融、企业、运营商一直都为黑客攻击的重点目标。但与2022年相比，2023年企业应急事件数量降低了近50%，而金融行业与运营商成为了首要攻击目标。这一定程度上反映了目前企业客户防御能力与安全意识的提升，和攻击者目标的转变。

行业事件数统计



挖矿事件趋势持续放缓，勒索事件占比最高。近年来随着终端及流量层安全防护产品能力的提升，挖矿程序越来越难以长期驻留，致使攻击者难以长期的获取有效收益。通过对挖矿事件的统计发现，近两年挖矿事件出现持续减少趋势，从2023年第一季度开始，挖矿事件数量已降至个位数。

2022-2023年度挖矿事件数量统计



数据安全风险上升，企业和医疗领域成攻击焦点

随着互联网的广泛应用和企业数字化的加速推进，数据安全相关事件的数量也日益增多。通过对近年数据安全相关事件统计发现，数据安全事件数量呈现不断增长的趋势。

通过数据安全事件统计发现，黑客的主要目标为企业和医疗卫生行业。这两类行业的数据安全事件数分别占比58%和27%。在企业类数据安全事件中，勒索病毒是主要攻击形式。数据勒索事件的激增进一步增加了企业数据安全事件的占比。另外，医疗卫生行业存在数据量大、用户量多，安全防护能力差的特点，亦使其成为攻击者的重点攻击对象。历年来医院等卫生行业机构的数据泄露事件屡见不鲜。鉴于网络漏洞和口令安全问题导致的数据安全事件频繁发生，相关单位应更加重视漏洞监控和修复，并提升用户和企业的安全意识。

数据安全法规趋于健全

2023年12月8日国家网信办起草发布了《网络安全事件报告管理办法（征求意见稿）》

《网络安全事件分级指南》

小时内向上级管理部门进行报告

《网络安全事

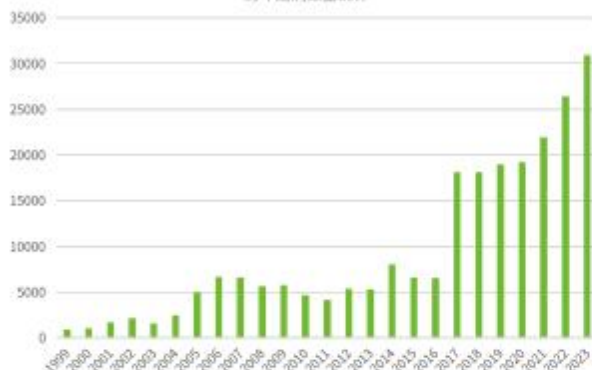
件报告管理办法（征求意见稿）》

安全漏洞变化趋势

系统组成

2023年每月漏洞新增数量在2100-3000之间，安全漏洞形势的严峻性加剧，高危漏洞披露数量持续增长。根据NVD已收录的公开发布漏洞数目观察，2023年新增漏洞数量为30947个，同比去年增加了14.59%。根据NVD数据库提供的CWE条目，可对漏洞成因进行统一分析。2023年收录的漏洞中，共有27856个分配了CWE ID，图4.1.3所示为TOP10 CWE漏洞类型。其中跨站脚本（CWE-79）类型的漏洞数量最多，排名第二的为SQL注入（CWE-89）

历年漏洞数量统计



2023年TOP10漏洞类型



部分高龄漏洞的利用仍旧活跃

根据2023年告警监测数据，盘点了与漏洞利用相关的攻击事件，并筛选出了告警数量最高的10个漏洞（详情见报告）。从表中数据可以发现，具有10年历史的高龄漏洞仍然活跃，告警次数高达三十多万。告警数据TOP3漏洞为：

- CVE-2016-3324：Microsoft Internet Explorer 和 Edge 远程内存破坏漏洞，告警数量 620 万。
- CVE-2017-0146：Windows MS17-010 系列漏洞扫描攻击，告警数量 154 万。
- CVE-2019-6444：NTPsec process_control 越界读取漏洞，告警数量 47 万。

0day漏洞利用呈增长趋势

随着黑客攻击技术的提升和市场化，0day漏洞的数量和利用呈明显增长趋势，大量攻击团伙利用未公开及厂商未及时修复的漏洞对目标系统进行未授权访问、数据窃取或其他恶意活动，这类漏洞的利用往往具有高度隐秘性和攻击性，使得安全防护和应对的难度进一步提高。根据我们监测发现，2023年爆出的被攻击者利用的0day漏洞中，有如下需要重点关注（部分）：

- CVE-2023-20269：Cisco ASA 与 FTD 软件未授权访问漏洞
- CVE-2023-41064：Apple ImageIO 远程代码执行漏洞
- CVE-2023-41061：Apple Wallet frameworks 远程代码执行漏洞

重点漏洞盘点

办公类系统仍是核心风险区域。从2023年攻防演练漏洞分布情况来看，在当前日益数字化和网络化的办公环境中，办公软件的复杂性、功能多样性和广泛使用为潜在漏洞提供了更多的攻击面，办公类系统持续被视为攻击者的首要目标。作为企业日常工作的核心系统，其内部存储了大量的敏感资料、业务数据、员工信息等文件，攻击者会利用各种手段对此类系统进行攻击，以获取上述高价值数据。

Windows作为被广泛应用的操作系统，由于其庞大的用户群体和复杂的系统结构，使得安全问题持续存在，且漏洞数量依旧相当大。被公认为是微软旗下安全漏洞最多的产品，几乎每月的安全更新公告中都会涉及Windows各个版本的漏洞修复。这些漏洞中，有些是尚未公开的0day漏洞，有些漏洞甚至已经存在在野利用。

网络安全趋势

01

Java应用与ESXi成为勒索攻击热点

- **Java 应用成为国内勒索主要攻击面**
2023年5月TellYouThePass勒索团伙再次发起大规模勒索攻击，绿盟科技CERT连续收到多个客户遭到加密后缀为.locked1的勒索攻击事件。
- **ESXi 进入更多勒索攻击团伙视线**
随着VMware ESXi成为最流行的虚拟化平台之一，大量勒索团伙都开始发布针对ESXi平台的勒索加密程序，且各个勒索团伙使用的ESXi加密器往往还存在较高相似性。

02

恶意软件技巧升级，社工钓鱼仍需防范

- **云设施服务滥用增多，云助手成远控帮凶**
虽然云服务为我们的工作提供了便利，但也为攻击者提供了机会，他们可以滥用其高可信度，实施高度隐蔽的钓鱼攻击。
- **以社交软件为投递渠道的社工钓鱼攀升**
从2023年的应急事件统计数据中观察到，攻击者通过即时通讯类软件进行社会工程学钓鱼的次数有明显增加的趋势。常见的攻击方式包括但不限于简历投递、远程技术指导以及上级通告文件转发等。

03

AI风潮下的网络安全风险与机遇

- **AI加持下的社工攻击日益猖獗，变声换脸诈骗频发**
随着AI大模型的发展和生成式人工智能的普及和易获取性，近年利用AI变声换脸进行网络诈骗的事件日益增加。
- **数据泄露与滥用等风险涌现，法律监管面临新挑战**
随着AI应用的广度和深度不断拓展，诸如数据滥用、数据泄露、大模型安全等诸多问题也透露出不少风险与隐患。赋能安全产业升级，提升防护能力构建坚实屏障

04

汽车电动化、网联化、智能化带来更多网络安全风险

- **智能化汽车更需要安全化**
主流新能源车企在设计车联网方案时，普遍采用“云-网-端”系统构架，需面对车端和云端的各种风险。
- **智能化汽车亟待加强数据保护**
我国智能网联技术迅速发展，海量的车辆数据和用户个人数据若管理无序，将直接影响百姓生命和财产安全。因此，如何确保汽车安全有序运行以及数据合规使用，已成为社会关注的焦点。

05

K8S逐渐成为主流，云安全意识需要提升

- **K8S集群控制台安全需要重点关注**
由于集群Web控制台可访问和管理整个或者多个集群，其安全性至关重要。若控制台出现口令泄露或者权限失控，可能导致整个集群失控，对攻击者暴露所有信息。
- **容器不安全配置成为云安全短板**
Kubernetes集群的安全风险主要存在于不完善的集群或者容器配置。

06

地区冲突引发网络战，攻击手段简单粗暴

- **DDoS是网络战最主要的攻击方式**
从2022年开始的俄乌冲突到2023年的巴以冲突，都凸显了网络攻击与实体战争的密切关系，而这些网络攻击的主要形式之一是拒绝服务攻击（DDoS攻击）。
- **关键基础设施是网络战的主要目标**
自巴以双方开战以来，黑客组织优先对双方重要的政府、职能机构及关键基础设施发起了大规模的网络攻击。

A decorative graphic on the left side of the page consisting of a grid of small, light gray dots arranged in three columns and twenty rows.

01

2023 年网络安全 形势分析



以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/066042233001010101>