

2023年中国蜜罐行业词条报告

作者 唐文卿

摘要 蜜罐是一种主动式网络防御技术，允许管理员通过工具欺骗攻击者来观察攻击者的行为。它不响应攻击或漏洞，而是通过将注意力转向攻击者本身。该技术通过欺骗乱打攻击节奏，增加攻击复杂性，增加企业响应时间，可对攻击者行为进行分析并预防攻击。

行业 [头豹分类|信息传输、软件和信息技术服务业/软件和信息技术服务业/运行维护服务/运维安全](#) [港股分类法|信息科技/软件服务](#)

关键词 [蜜罐](#) [网络信息安全](#)

1. 蜜罐行业定义

蜜罐是一种**主动式网络防御技术**，允许管理员通过工具欺骗攻击者来观察攻击者的行为。它不响应攻击或漏洞，而是通过将注意力转向攻击者本身。该技术针对攻击的回应方式可以分为回应式和黑洞式，前者可满足攻击者的所有检测和攻击动作，后者则完全不响应，所有攻击都被黑洞吞噬。同时也被黑客利用，攻击者利用蜜罐作为攻击跳板，对攻击者行为进行分析并预防攻击。成熟的蜜罐系统包含三个核心技术：网络欺骗（诱捕环境构建）、监控记录（监控入侵行为）和处置措施（对监控中捕获的数据进行分析从而实现溯源）。网络欺骗是蜜罐系统中的核心组成部分，负责通过技术手段模拟虚拟信息并将其伪装成有价值的信息，从而达到欺骗攻击者的目的。

2. 蜜罐行业分类

蜜罐可按照部署方式和设计标准进行分类，按部署方式可分为产品型蜜罐和研究型蜜罐，按设计标准可分为低交互、中交互和高交互蜜罐。

类型名称	类型说明
产品型蜜罐	由网络安全公司开发的商业蜜罐通常被用作诱饵，尽可能长时间地将黑客攻击捆绑在蜜罐上，为保护真实的网络环境赢得时间。同时也用来收集证据作为起诉黑客的依据。 产品型蜜罐容易部署，不需要管理员投入大量的工作，但收集信息能力有限。
研究型蜜罐	用于研究、攻击诱导、信息收集、新攻击和新黑客工具的检测，以及黑客和黑客群体的背景、目的、活动规律等。 研究型蜜罐能收集更多有价值信息，但维护及使用程序复杂，投入时间成本高。
低交互蜜罐	作为现有系统中运行的仿真服务，低交互蜜罐监听并记录来自指定端口的所有数据包，并提供少量交互功能。 黑客只能在模拟服务预先设定的范围内进行操作
中交互蜜罐	不提供实际的操作系统，而是使用脚本或小程序来模拟服务行为，可以窃听不同的端口，并且通过更复杂的交互， 攻击者可以收集到更多数据错误
高交互蜜罐	由真正的操作系统构建， 为黑客提供真正的系统和服务，可以了解黑客执行的所有操作并获取大量有用的信息 ，包括新型网络攻击方法

3. 蜜罐行业特征

蜜罐主要运用于金融和政府行业，已经成为保障国家重大活动网络安全、促进和推动国家关键信息基础设施安全防护工作的重要利器之一。经过调研有53%的企业已经部署，还有36%的企业计划部署，企业对蜜罐的需求不断提升，但蜜罐的溯源及反制能力仍需增强。

需求量大	过半数企业已经部署蜜罐，还有36%的企业计划部署 从FreeBuf咨询调研结果来看，针对威胁诱捕（蜜罐）产品的选择，有53%的企业已经部署，还有36%的企业计划部署。
大量运用在重点行业	蜜罐产品的企业中，74%为金融和政府行业 已部署威胁诱捕（蜜罐）产品的企业中，74%为金融和政府行业。近年来为保障国家重大活动网络安全、促进和推动国家关键信息基础设施安全防护工作，欺骗防御技术已成为蓝军对抗的利器之一，企业对威胁诱捕（蜜罐）产品的应用需求也在不断提升。
溯源反制能力	溯源和反制能力将成为行业提升的重要领域 随着网络安全日常防护意识的增强和网络攻防演练的常态化展开，知己知彼成为了网络安全攻防的最大核心需求。企业越发注重主动防御。调研结果显示，72%的企业认为蜜罐产品可增强“溯源和反制能力”、“入侵行为分析能力”及“恶样本捕获能力”。

4. 蜜罐发展历程

蜜罐从概念阶段到初期阶段是从1996年开始。该技术由Cohen在发展初期提出，主要是通过虚拟的操作系统和工具包来欺骗网络入侵者。初期蜜罐技术根据针对攻击的回应方式可以分为回应式和黑洞式，前者可满足攻击者的所有检测和攻击动作，后者则完全不响应，所有攻击都被黑洞吞噬。目前，由于企业网络逐渐呈现架构复杂化、安全报警信息海量化的特点，对蜜罐技术在仿真对象类型、仿真精度、自动化程度等方面提出了更高的要求，厂商和安全研究人员都在不断优化蜜罐技术，逐步增加新型蜜罐、蜜网、分布式蜜罐、分布式蜂网甚至蜜场等多种部署形态

开始时间：1989 结束时间：1998 阶段：概念期 行业动态：作为欺骗攻击者与其进行交互的工具在网络安全领域兴起

开始时间：1998 结束时间：1999 阶段：发展初期 行业动态：Cohen提出欺骗理论框架和模型，并开发欺骗工具包（DTK）

开始时间：1999 结束时间：2003 阶段：完善期 行业动态：Spitzner提出蜜网技术
蜜罐概念被提出，分布式概念引入蜜罐技术的发展

开始时间：2004 结束时间：2020 阶段：应用期 行业动态：起初应用于辅助入侵检测技术来监测网络攻击
扩展并应用至工业控制系统等多个领域

开始时间：2020 结束时间：2022 阶段：创新发展期 行业动态：基于新型攻击方式和威胁形势，结合新一代技术创新蜜罐技术

5. 蜜罐政策梳理

政策名称：《银行业金融机构数据治理指引》 颁布主体：中国银保监会 生效日期：2018-05 影响：0 政策性质：指导性政策
政策内容：银行业金融机构应当建立数据安全策略与标准，依法保护客户隐私，完善数据安全技术，定期审计数据安全
政策解读：大数据及人工智能在银行业领域的监管将得以加强，银行业智能化的发展更趋规范，人工智能在银行业的发展方向变得明确

政策名称：《“十四五”数字经济发展规划》 颁布主体：国务院 生效日期：2021-12 影响：8 政策性质：鼓励性政策
政策内容：强化落实网络安全技术措施同步规划、同步建设、同步使用的要求，确保重要系统和设施安全有序运行。加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，健全完善网络安全应急事件预警通报机制，提升网络安全态势感知、威胁发现、应急指挥、协同处置和攻击溯源能力。
政策解读：2021年12月12日，国务院印发《“十四五”数字经济发展规划》，明确“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务 and 保障措施。《规划》部署了八项重点任务，包括优化升级数字基础设施、充分发挥数据要素作用、大力推进产业数字化转型、健全完善数字经济治理体系、着力强化数字经济安全体系等。

政策名称：《要素市场化配置综合改革试点总体方案》 颁布主体：国务院 生效日期：2021-12 影响：8 政策性质：鼓励性政策
政策内容：加强数据安全保护。强化网络安全等级保护要求，推动完善数据分级分类安全保护制度，运用技术手段构建数据安全风险防控体系。
政策解读：《方案》要求完善公共数据开放共享机制、建立健全数据流通交易规则、拓展规范化数据开发利用场景、加强数据安全保护。聚焦数据采集、开放、流通、使用、开发、保护等全生命周期的制度建设，推动部分领域数据采集标准化，分级分类、分步有序推动部分领域数据流通应用，探索“原始数据不出域、数据可用不可见”的交易范式，实现数据使用“可控可计量”，推动完善数据分级分类安全保护制度，探索制定大数据分析和交易禁止清单。

政策名称：《“十四五”市场监管现代化规划》 颁布主体：国务院 生效日期：2021-12 影响：7 政策性质：鼓励性政策
政策内容：推动完善重点产业质量认证制度体系，加大网络安全认证制度推行力度，加快战略性新兴产业领域质量认证制度建设，大力推行高端品质认证和新型服务认证，加快研究和完善国家数据安全标准与认证认可体系。

政策解读：2021年12月14日，国务院印发《“十四五”市场监管现代化规划》，旨在创新和完善市场监管，推进市场监管现代化。规划要求，引导平台经济有序竞争。推动完善平台企业数据收集使用管理、消费者权益保护等方面的法律规范。强化平台内部生态治理，督促平台企业规范规则设立、数据处理、算法制定等行为。健全事前事中事后监管制度，制定大型平台企业主体责任清单，建立合规报告和风险评估制度。

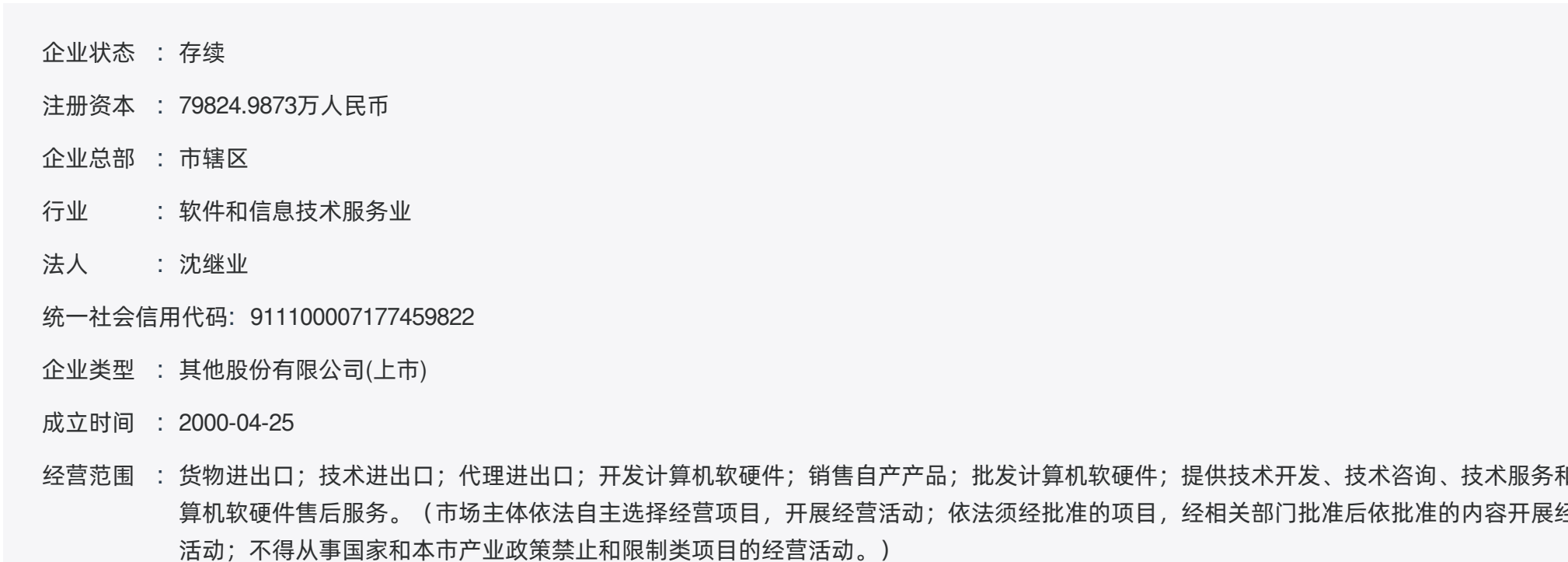
6. 蜜罐竞争格局

蜜罐类产品的主要作用是针对攻击的检测、捕获、分析、取证以及预警等。其中，分析取证在研究攻击的特征和发展趋势上起到关键性作用，只有当被捕获的攻击对象从攻击手段、攻击目的、攻击样本、攻击源等多方面进行风险的关联分析，才能够配合安全部门研究和抵御系统面临的或即将面临的威胁。总来看神州绿盟的产品综合实力较强。
从风险分析功能总体支持情况来看，完全支持的产品虽然只有绿盟科技的一款，广州非凡也达到98%，其他厂商均在90以下，明显拉开差距。
从蜜罐安全管理功能总体支持情况来看，没有完全支持测试要求的受测产品，志航云安全、神州绿盟、安恒信息、广州非凡均在90%以上支持率，其余竞品均在90以下。
从蜜罐安全性相关功能的总体支持情况来看，完全支持的9款产品和支持较好的产品23款，广州非凡稍靠后，但也有95%的支持性。

X轴名称：安全性功能 **单位：**%

Y轴名称：蜜罐管理功能 **单位：**%

α轴名称：风险分析功能 **单位：**%



X轴为公司蜜罐产品安全性评分，Y轴为蜜罐管理功能评分，气泡大小为风险分析功能评分

股票代码	上市公司	总市值	营收规模	同比增长(%)	毛利率(%)
688244	北京永信至诚科技股份有限公司	2900000000	32,016.59万元	9.78	61.7
300369	绿盟科技集团股份有限公司	8900000000	32,655.36万元	34.64	63.32

7. 蜜罐代表企业分析

绿盟科技集团股份有限公司【300369】											
企业状态	存续										
注册资本	79824.9873万人民币										
企业总部	市辖区										
行业	软件和信息技术服务业										
法人	沈继业										
统一社会信用代码	911100007177459822										
企业类型	其他股份有限公司(上市)										
成立时间	2000-04-25										
经营范围	货物进出口；技术进出口；代理进出口；开发计算机软硬件；销售自产产品；批发计算机软硬件；提供技术开发、技术咨询、技术服务和计算机软硬件售后服务。（市场主体依法自主选择经营项目，开展经营活动；依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动；不得从事国家和本市产业政策禁止和限制类项目的经营活动。）										
股票类型	A股										
品牌名称	绿盟科技集团股份有限公司										
	：										

财务指标	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022(Q1)	2022(Q2)
销售现金流/营业收入	0.85	1.09	0.96	0.94	0.99	1.03	1.09				
扣非净利润同比增长(%)											
资产负债率(%)	36.4038	20.6353	20.7651	29.2201	23.8094	18.8849	17.1466	20.07	23.698	21.519	21.784
毛利润(元)											
营业总收入同比增长(%)	18.1753	12.7795	24.9046	24.2723	15.0745	7.1651	24.2409	20.283	29.798	34.64	8.106
归属净利润同比增长(%)	16.6265	22.3381	34.477	13.2769	-30.781	10.3056	34.7716				
应收账款周转天数(天)	171.0295	193.3197	189.6933	206.1147	209.7047	215.1952	169.022	120	89	190	159
流动比率	2.4989	5.2139	3.5588	2.5379	3.2831	4.0698	4.4892	3.836	3.17	3.462	3.402
每股经营现金流(元)	0.1569	0.7317	0.3758	0.2515	0.0944	0.1069	0.4335	0.559	0.095	0.016	-0.016
毛利率(%)	79.1022	78.0195	78.314	77.811	71.1596	76.9268	71.7094				59.98
流动负债/总负债(%)	100	83.8881	89.2261	93.0223	96.9479	96.9524	94.6379	93.858	88.707	86.174	84.017
速动比率	2.3538	5.0473	3.4897	2.4674	3.2083	3.3747	4.3613	3.758	3.023	3.202	3.183
摊薄净资产收益率(%)											
实际税率(%)											
摊薄总资产收益率(%)	17.4581	14.7554	11.5302	9.082	4.7166	4.411	5.7185	7.122	7.54	-2.476	-4.712
营业总收入滚动环比增长(%)	84.8878	187.7705	251.4563	187.5236	322.712	172.8035	133.8362				
扣非净利润滚动环比增长(%)	1088.9309	155169.0179	10834.3969	1791.7306	627.1917	1872.9315	767.7737				
加权净资产收益率(%)	26.79	16.78	13.44	12.47	6.48	5.61	6.99				
每股净资产(元)											
经营现金流/营业收入	0.1569	0.7317	0.3758	0.2515	0.0944	0.1069	0.4335	0.559	0.095	0.016	-0.016
扣非净利润(元)											
基本每股收益(元)	1.47	1.08	0.55	0.61	0.2	0.21	0.28	0.38	0.44	-0.144	-0.2699
净利率(%)	17.7401	20.5589	22.0447	20.1679	12.162	12.451	13.5414	14.9875	13.2224	-35.0508	-25.7948
总资产周转率(次)	0.9841	0.7177	0.523	0.4503	0.3878	0.3543	0.4223	0.475	0.571	0.07	0.182
归属净利润滚动环比增长(%)	975.2061	1858.6506	24720.4164	1662.8023	1892.4414	1133.719	604.8874				
存货周转天数(天)	43.7631	48.623	35.7427	30.661	34.6744	48.3552	35.1607	36	38	137	87
预收款/营业收入											
营业总收入(元)	6.23亿	7.03亿	8.78亿	10.91亿	12.55亿	13.45亿	16.71亿	20.10亿	26.09亿	3.27亿	8.34亿
每股未分配利润(元)	4.1303	3.0923	1.5811	1.9578	1.0233	1.1531	1.3713	1.615	1.9596	1.8156	1.624
稀释每股收益(元)	1.47	1.08	0.55	0.61	0.2	0.21	0.28	0.38	0.44	-0.1439	-0.2697
归属净利润(元)	1.11亿	1.45亿	1.94亿	2.20亿	1.52亿	1.68亿	2.27亿	3.01亿	3.45亿	-114999926.42	-215557228.62
扣非每股收益(元)	1.35	1.01	0.46	0.54	0.12	0.15	0.23	0.32	0.3	-0.1429	-0.2786
每股公积金(元)	0.5415	2.6657	1.9421	2.5801	1.741	1.7274	1.7301	1.7415	1.6691	1.6994	1.7297

绿盟科技集团股份有限公司竞争优势											
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代表处，深入开展全球业务，打造全球网络安全行业的中国品牌。											
绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、无影智能、新型攻防对抗、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、大数据安全、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索，为绿盟科技的核心竞争力的持续提升提供了有力的保障。											
作为巨人背后的专家，绿盟科技将一如既往地以创新精神、精湛技术、优质产品、专业服务，在全球范围内，提供基于自身核心竞争力的企业级网络安全产品、安全解决方案和安全运营服务，成为备受用户信赖的网络安全公司。											

绿盟科技官网

头豹“数字行研”——词条报告

■ 优质企业共建词条报告

——展示企业优势地位

■ 第三方数据机构应用合作招募

——头豹词条数据库流量赋能转化

■ 开通会员账号，查阅数据底稿

——市场规模、竞争格局工作底稿一览无余

详情咨询：400—072—5588

136—1163—4866

■ 体量庞大、创作效率高
➢ 上万词条由概念级、产业级、行业级、产品级分层搭建，为垂直细分研究提供基础

■ 创作全程溯源
➢ 原创内容溯源：创作过程中一手调研资料、访谈纪要、数据底稿（数据来源、预测逻辑、模型公式等）文件均上传头豹脑力擎系统存储，确保每个词条有据可查
➢ 第三方资料溯源：创作过程中的参考文献、权威机构名称及网址等内容精准溯源
➢ AI生成类内容溯源：AI生成的内容进行区分标识

■ 科技赋能
➢ 脑力擎系统，词条数据库、写作指引及视频指南、溯源功能、写作助手、AI生成、专家访谈工具、数字资产确权等功能，实现数字企业
➢ 开源、扩展性：词条内涉及的公司名可与第三方企业库对接获取信息；脑力擎系统接口可与第三方对接，获取实时数据或输出数据

■ 更多免费行业报告 [并购买](#) [www.ipoipo.cn](#)
➢ 词条基于头豹行企研究8-D方法论组成，概述+数据+分析相结合，内容清晰，数据量足，观点结论丰富
➢ 依托多年行研咨询经验，脑力擎Size3.0控件独创市场规模及竞争格局搭建及测算模型

头豹
IPOIPO