



# 网络安全行业简史 与网络攻端人才的未来

安络科技谢朝霞

2023年7月20日

# 第一部分

## 网络安全与中国黑客成长简史

# 1995：中国互联网的元年

- 1993年，中科院高能所许榕生通过卫星信道接入美国斯坦福大学SLAC国家实验室。
- 1994年4月20日，第一条64K国际专线接入中国。
- 在1995年，北京和上海的64K的国际专线开通之后，中国全功能接入国际互联网。
- 1995年5月19日，张树新成立中国第一家互联网公司瀛海威。
- 1995年12月14日，田溯宁成立北京亚信网络系统集成公司，承建Chinanet。后丁健任亚信中国董事长。
- 1995年4月，丁磊离开宁波电信局。马化腾架设Ponysoft的CFIDO站台。马云成立杭州海博电脑服务公司。





# 1995:中国的网络安全元年

10:58 企业 动态 企查查

**北京天融信网络安全技术有限公司** 存续

11万+ 91110108101909571P | 发票抬头>

高新技术企业> 隐形冠军企业> 企业技术中心>

简介: 公司愿景: 成为中国第一的世界级网络安全产品... 更多

法定代表人 <b>李雪莹</b>	注册资本 <b>35000万元人民币</b>	成立日期 <b>1995-11-06</b>
企查查行业① 其他IT与互联网服务>	规模① 大型 L	员工① 2875人(2022)

010-82776666 更多1 官网 邮箱

北京市海淀区上地东路1号院3号楼四层

**股东** 1 北京天融信... 大股东 持股比例 100% 投资企业 10 家

**人员** 2 **李雪莹** 执行董事... 关联企业 36 家 **刘蕾杰** 监事 关联企业 10 家

**风险扫描**

自身风险 14 该企业有司法案件 警示信息(1) 其他(13)	关联风险 9 该企业的股东北京 天融信科技有...(1) 其他(8)	历史风险 26 该企业曾因买卖合 同纠纷案由被...(1) 其他(25)
--	---	---

**动态** 2023-07-13  
中标结果: 2022年中国联通资产安全管理平台扩容工程...

**集团** 天融信 成员企业: 35 风险提示: 391

首页 关注 报告 监控 笔记



- 1994年, 贺卫东认识了何德全院士。
- 1995年11月, 天融信成立。
- 1996年, 获得国家统计局600万系统集成标。
- 1997年, 研发天融信防火墙。
- 2011年11月, 贺卫东离开天融信。

# 1998:中国黑客元年

- 1997年龚蔚成立中国第一个民间技术组织：绿色兵团
- 1997年底深圳辰光工作室网站发布
- 1997年底彭泉成立Chinahack
- 1998年绿色兵团成员达到5000人
- 1998年绿色兵团针对印尼排华行动开展网络层面的反击
- 1999年8月，xundi创建安全焦点个人主页

# 1999年：第一代黑客崛起之年

- 99年黄鑫发布冰河木马
- 99年小榕发布流光扫描软件
- 99年5月、8月，绿色兵团、chinahack、辰光工作室等组织对美、台发起网络行动
- 99年底绿色兵团创业团队在北京筹建绿盟公司
- 99年底辰光工作室、chinahack在深圳筹建安络公司
- 袁哥发现第一个windows漏洞
- 99年底以上组织发起对日本政府网络行动
- 99年12月30日，“南海论剑”中国网络安全最高峰会在海口举行，邀请了大部分第一代黑客出席。

# 1996-2000 涌现的网络安全企业

- 1996年6月24日，王佳成立启明星辰。
- 1999年9月，在许榕生的支持下中科网威公司成立。
- 1999年10月，蓝盾公司成立(300027,今年6月30日退市)，曾用名：广东天海威。
- 2000年1月19日，安络科技成立。
- 2000年4月，绿盟成立。

# 1999-2012年: 网络安全公司与黑客技术组织快速发展

- 2001年安全焦点发展为网络安全社区
- 2000年-2002年, 0x557、邪恶八进制、红客联盟等组织成立。
- 2008年左右, T00ls安全社区创建。
- 以上组织和社区为培养各类各层次的网络攻防人才做出了巨大贡献。
- 绿盟、安络等老牌企业也一直重视攻端人才的培养环境, 为行业培养了大量人才。
- 2002年以后, 网络安全企业越来越重视攻防技术, 启明星辰等企业也纷纷建立攻防实验室, 此举既为攻端人才发挥特长提供了机会和舞台, 也是一种保护。
- 绿盟、启明、安络与上述组织和群体联系紧密, 共生共荣。



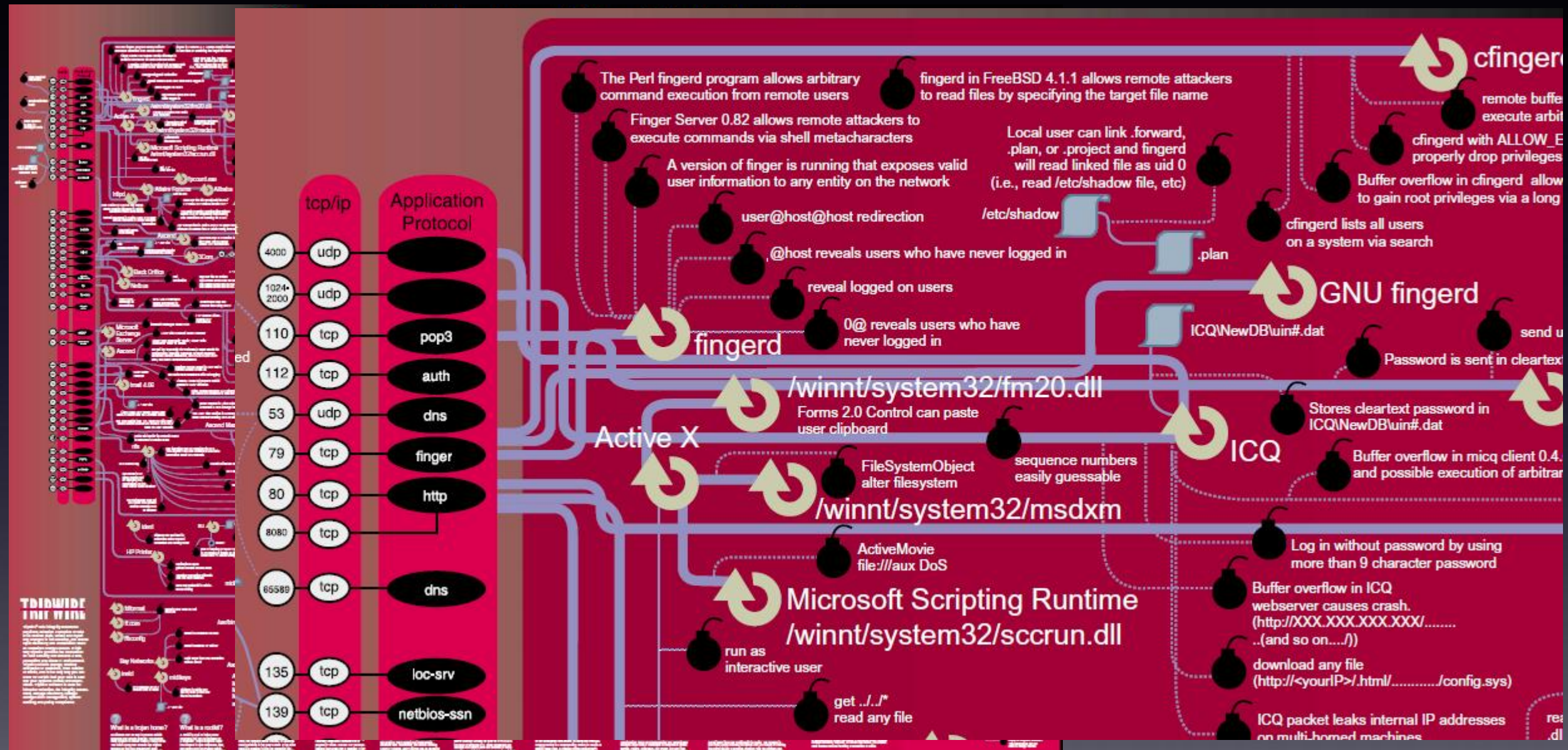
# 2012年-至今

- 2014年2月，第一次全国网络安全和信息化工作会议召开，习总书记首次发表网络安全重要讲话。
- 随着第一批网络安全公司上市，网络安全企业虽然利润率不高，市值却越来越高，超过了软件企业，甚至超过了芯片企业、新材料企业、生物医药和其他科技行业，受到资本市场热捧。
- 国内涌现了上万家网络安全初创企业。
- 网络安全与黑客群体呈现了百花齐放、千家争鸣的局面。

## 第二部分

# 攻防两端对抗技术 演进简史

# 1997-2007年，网络攻防的思维导图



# 经典攻防元素周期表

## 进攻端元素

## 中性元素

## 防守端元素

<u>Dc</u> 解密									<u>Ec</u> 加密
<u>Ck</u> 密码破解	<u>Oa</u> 溢出攻击						<u>Sk</u> 密钥	<u>Sp</u> SSL协议	<u>Dp</u> 动态密码
<u>Da</u> 反汇编	<u>As</u> ARP欺骗	<u>Sf</u> 嗅探	<u>Fz</u> fuzzing	<u>Rk</u> rootkit	关联分析	<u>Vs</u> Virusscan	<u>Ac</u> 访问控制	<u>Pd</u> 包检测	<u>Pf</u> 包过滤
<u>Sc</u> 扫描	<u>Hj</u> 劫持	<u>Df</u> DNS欺骗	<u>Si</u> Script注入	<u>Ma</u> 中间人	数据碰撞	<u>La</u> 日志审计	<u>Bl</u> 黑名单	<u>Wl</u> 白名单	<u>Vs</u> 漏洞扫描
<u>Ca</u> 跨站	<u>Nf</u> 网络钓鱼	<u>Mb</u> Mailbomb	<u>Hd</u> HashDump	<u>Ra</u> 路由攻击	数据分析	<u>Ta</u> 流量分析	<u>Ds</u> 数字签名	<u>Dr</u> 数据恢复	<u>Db</u> 数据备份
<u>Ba</u> 旁路	<u>Rp</u> 重放	<u>Fa</u> D.o.S	<u>Rb</u> 彩虹表	<u>Hp</u> 鱼叉攻击	信息搜集	<u>Id</u> IDS	<u>Pk</u> PKI	<u>Vp</u> VPN	<u>Vm</u> 虚拟机
<u>Ep</u> 本地提权	<u>Ne</u> 网络提权	<u>Ic</u> Impression clean	<u>Wh</u> 水坑攻击	<u>Wc</u> Wifi破解	社会工程	<u>Ip</u> IPS	<u>Fw</u> 防火墙	<u>Ta</u> 终端管理	<u>Wf</u> WAF



## 2010年-2019年：网络攻端技术成为各国政府关注焦点

- 美国政府、媒体及企业炒作APT
  - 英国跟进...
  - 日本跟进...
  - 欧洲跟进...
- 美国FireEye、Mandiant等针对APT研究的企业浮出水面。
- 俄罗斯黑客崛起，希拉里竞选总统因邮件门事件退出舞台。
- 中国公安部及政数部门于2016年开始，在全国范围内展开护网行动。大批企业攻端人才投入与护网相关的漏洞研究和攻击实战。

# 2010-2019围绕APT对抗研究热点

**APT**，就是高级的、可持续的，长期潜伏于网络深度空间的攻击。

围绕对**APT**研究的深入，厂商逐渐把防范重点向深度空间转移，**APT**的内网横向移动成本提高，潜伏周期缩短

## 一些围绕APT的对抗

安全厂商	获得与部署	攻端研究
微软	国内外通用	提权、数字签名、驱动研究、主动防御、人工智能
FireEye、Mandiant	对中国禁运	过Fire Eye、bluecoat
赛门铁克、趋势、小红伞、卡巴斯基	国内外	过杀软、过主动防御
360及国内安全厂商产品	国内及境外华人机构为主	过杀毒软件、过主动防御

# 2020-至今

EDR、XDR、NDR部署涌现，防守端人机结合增强，攻端生存成本进一步提升

## FireEye XDR 方案愿景 加快安全运营中的人机合作，更快地捕捉更多攻击



©2019 FireEye

# 2016-至今:熟练掌握网络技术的新一代犯罪人口崛起

电信诈骗和新型网络犯罪持续高发、多发，危害十分严重。

仅仅2018年下半年，全国就因电信网络诈骗就造成5名受害人自杀。其中，深圳市发生了震惊中央的“813”网络刷单诈骗致人跳楼自杀的恶性案件！

全国电诈犯罪已经形成了一个庞大、专业的地下配套产业链，涉及面非常广泛，多达40余个，各类黑产技术工具、设备应有尽有，例如：有专门非法获取和买卖公民个人信息的、有专门提供IP语音技术和数据存储服务器的、有专门买卖改号软件和木马病毒的、有专门传播种植木马病毒的、有专门编写诈骗“话术剧本”的、有专门雇佣诈骗“话务员”的、有专门收售他人银行卡和手机卡的、有专门买卖和“圈养”各类网络支付账户的、有专门利用商事改革注册“皮包公司”的、有专门利用网上购买充值“点卡”等易于变现商品进行对倒洗钱的……

网上诈骗、黄赌毒、贩枪、盗窃、敲诈勒索、销赃等电信网络新型违法犯罪快速出现和疯狂蔓延，电诈犯罪领域严峻形势概括起来就是“五句话”：发案高、损失大，群体增、对手强，黑产厚、涉及广，年轻化、接班快，危害深、破坏大。



# 第三部分

## 网络攻端人才的未来

# 漏洞发现行为的法律风险等级

漏洞discovering发布风险		
	行为类别	风险描述
	• 未经授权发布业主资产漏洞	高民事诉讼风险、中低刑事风险
	• 向CVE等组织提交漏洞	低风险，大规模严重漏洞为行政处罚中风险（案例：Apache server）
	• 业主SRC漏洞响应	低风险
	• 向国家漏洞库提交漏洞	零风险

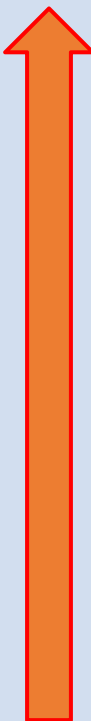
# 渗透测试行为的法律风险等级

## 渗透测试行为法律风险

	行为类别	风险描述
	• 针对境内国家事务、关基、科技的渗透	极高风险、行为犯、入侵即犯罪
	• 针对境内合法商业、民用目标的渗透	高风险、非法破坏、非法控制
	• 针对境外商业目标的渗透获利	高风险，黑产！明确构成犯罪，国内打击
	• 针对境外违法目标的黑吃黑	高风险，黑产！明确构成犯罪，国内打击
	• 针对境外合法资产的有目的渗透	国际刑事指控风险，可能触发国内协查
	• 针对境外合法资产的渗透尝试，无获利、无破坏	低风险-中风险
	• 针对境外违法目标的有关授权	低风险-中风险，考虑管辖权、违法判定
	• 网警针对国内目标授权	低风险
	• HW行动	低风险
	• 业主授权专项渗透测试	接近零风险

# 中风险以上渗透测试行为面临的实际后果

## 渗透测试行为实际后果

	行为类别	后果描述
	• 针对境内国家事务、关基、科技的渗透	网警重点打击对象，较为严重刑事处罚
	• 针对境内合法商业、民用目标的渗透	网警重点打击对象，可能面临较为严重刑事处罚
	• 针对境外商业目标的渗透获利	打击对象，较为严重刑事处罚
	• 针对境外违法目标的黑吃黑	打击对象，刑事处罚
	• 针对境外合法资产的有目的渗透	触发国内协查将可能受到刑事处罚。
	• 针对境外合法资产的渗透尝试，无获利、无破坏	网警批评教育，有其它情形会引发网警采取行动
	• 针对境外违法目标的有关授权	在管辖权有争议的情况下，如果授权方退缩，异地网警约谈甚至采取行动。建议：本地网警授权可以较大降低风险。



# 与网络攻端人才前景命运相关的几个重要形势

- 网络犯罪
- 中美关系

# 攻端人才如何构建安全生存背景？

- 加入名门正派的网络安全公司
  - 加入协助警方打击网络犯罪的知名网络安全公司
  - 参与当地警方特别是网警的工作，建立起实质合作。
- 
- 挖掘境内外网络犯罪线索（境外为主），为警方提供犯罪线索，是最好的合作点，也是提升业务水平的网络空间实战靶场。

# 网络攻端人才安全发展原则

- 确保我们的事业是正义的
- 哪些事业是正义的？
  - 为祖国服务的事业是正义的
  - 为人民服务的事业是正义的
- 为正义的事业奋斗！

**珍贵原声！ 振奋人心！**

**我们的事业是正义的**

毛泽东在第一届全国人大一次会议上致开幕词



**我们的事业是正义的**

## 2016年、2017年、2018年

深圳市委、市政府组织隆重召开了打击治理电信网络新型违法犯罪工作总结表彰会议中，深圳市安络科技有限公司在会议中荣获 **“特别贡献奖”**。

