APT在互联网犯罪中的历史形态及其应对建议

宣讲人：E.S.T | 冰血封情

关于APT攻击

关于APT攻击

IDCC

- 高级持续性威胁（Advanced Persistent Threat，APT）

- 隐蔽性：持续深入对目标进行深层的监控及信息数据窃取
  受害目标可能是一切存在数据的存储设备
- 针对性：针对目标量身定制病毒、木马、挖掘漏洞和寻找缺陷
  基于此需求所以经常量身定制兵器
- 综合性：对海量信息的利用以及各种攻击手法的综合整合
  广泛搜集价值信息用于猜解和伪造欺骗

关于APT攻击

IDCC

- 应用于重要性显著的复杂目标 早期主要体现在内网渗透
- 传统四段手法：分析、打点、渗透和控守

- 量身打造：
  针对性免杀突破防御，定制开发，白盒测试，社会工程学欺骗，
  物理侵入等。

- 主要工具：
  加密跳板，堡垒机，下载，前锋，控守，硬件植入，隔离摆渡等。

- 核心原则：
  减小体积，提高效率，长期控制，
  对目标网络日常通信影响最小化。

中国网络安全初时代

中国网络安全初代

IDCC

- 时期：改革开放初期到千禧年之前
- 技术单轨：互联网在中国开始蓬勃发展
  黑客技术掌握在极少数人手中
  缺乏网络安全概念普及
  缺乏技术多极化并行制约
- 运维单纯：网站管理人员缺乏网络安全意识
  显著目标也很少遭到残酷打击
  中国互联网处于淳朴的和谐共享开放状态
- 手段单一：单漏洞横行吃遍天下
  都是简单粗暴低级的漏洞
- 支持单薄：国内专业安全公司极少
  行业难以提供整合式的安全服务
  需教育客户认知安全拓展业务困难

中国网络安全初代

IDCC

- 国内互联网犯罪处于学习阶段
  境外国家和地区的互联网犯罪已经逐步影响境内
  到千禧年前国内已经开始出现有组织的互联网黑产和灰产

- APT在这个时期的形态
  已经长期存在掌握在少数黑客泰斗手中
  互联网淳朴状态致使互联网犯罪成本低
  APT极少应用于这个时期的互联网犯罪

- 在高级黑客常规活动中，他们入侵安全性较高的网络，一直用此手法。
  就像暗网一直存在，APT不是新话题，只是今天赋其名字，给他光环。

互联网犯罪萌生和发展期

互联网犯罪萌生和发展期

IDCC

- 时期：千禧年后的8到10年间

- 技术普及：
  国内互联网上各种网络安全技术交流和安全社区蓬勃发展人才池形成

- 深入浅出：
  大量优秀的信息安全研究团队产生并相辅相成促进安全商业化发展

- 资本侵入：
  商业化感染黑客给APT技术在互联网犯罪中运用以谋取暴利机会

- 沟通密切：
  国际技术交流频繁互联网犯罪团体和国内的不法商人勾结日益密切

互联网犯罪萌生和发展期

IDCC

- 资本侵入双刃的利与弊：
  安全领域催生大量襁褓中优秀的新生代企业
  开放公益的互联网生态遭到赏金和资本的破坏
  当技术共享触犯灰色产业的利益时即遭到恶毒攻击反扑（尘封的秘密）
  2005年末开始2010年中达到顶峰

- 互联网犯罪形势：
  APT技术手法逐渐公开趋向完善
  APT开始广泛应用到互联网犯罪领域
  与灰色产业成鱼水之势

- 灰色产业蔓延的后果：
  使得大量不法商人开始在互联网寻求黑客合作
  导致部分优秀的技术苗子受到暴利诱惑而弃明投暗
  灰色产业的存在已经严重影响到安全人才的转化输出

泛滥与急刹

泛滥与急刹

IDCC

- 时期：2010年开始到2013年

- 态势恶化：
  互联网犯罪和灰色产业境内外勾结（黄赌和诈骗类尤其明显）
  各行业网络安全事件频发上升趋势更为明显
  互联网犯罪和灰色产业已经成为安全进步的巨大逆流

- 加强打击：
  对互联网犯罪的打击逐年加大力度
  大量典型案例侦破并公诸天下

泛滥与急刹

IDCC

- 收效显著：
  迫使互联网犯罪得到有效控制
  大量团伙转型侧重境内外勾结的灰色产业

- 灰色产业：
  不合法也不触犯所在国法律的边缘
  触犯法律量刑难或法条不足

- 交易特点：
  暗网（网络黑市）、比特币、地下钱庄、赌场冲抵、第三方支付等。

- 反恐局势：
  APT攻击大量被应用于灰色产业（商业间谍、隐私、外贸、SEO）
  赏金猎手为了巨额诱惑甚至不惜与类似ISIS这样的魔鬼交易
  一定程度上边缘的灰色产业已经开始影响到国家安全（黑帽SEO）
  一种新型的网络恐怖主义（软绑架、交易服务于恐怖）

网络安全中兴盛世新纪元

网络安全中兴盛世新纪元

IDCC

- 时期：2014年至今
- 国家重视与政策扶持：十二五规划中的重点 电子商务电子政务安全问题凸显
- 国际网络安全合作期：针对国际互联网犯罪和网络恐怖主义 国际联手合作打击
- 新生代网络安全企业：新模式和新架构的网络安全企业得到催生和蓬勃发展
- 全民网络安全的培养：安全公司和高校培训机构等的网络安全普及教育媒体宣传
- 整体深化网络安全带：互联网犯罪 商业间谍 隐私管控 反恐 舆情等立体式净网
- 灰色产业转为更为深刻的APT技术运用

APT防范补充建议要点

APT防范补充建议要点

IDCC

- 大量措施资料可查 而此作为APT攻击实施者的建议摒弃理论与抽象直抒补充重点

- 传统安全体系：杀毒软件和软硬墙和密码等的设置和更新（尽管都是马后炮也要做）
- 指令重复确认：非面对面请求均更换通讯重复核实对方身份（有效防止欺骗）
- 数据物理隔离：保密数据非对称加密物理隔离存储尤忌云（隐私、知识产权等）
- 严格交换审计：针对保密数据的交换设备要严格区分定期检查（U盘不混、刻录盘片）
- 移动设备禁入：保密数据的物理隔离内网对一切移动设备禁入（笔记本、手机等）
- 互访加密代理：允许访问公网的机 内对外 内对内都上加密VPN（大部分控守马）
- 定期安全检查：聘请专业的第三方安全公司定期对自身做白盒安全审计

后记

后记

IDCC

- APT技术其实早期主要应用于政治军事对抗，尔后开始进入商业领域，进而接触互联网犯罪，衍生入灰色产业链，通过暗网接轨国际犯罪组织，当前的态势已在互联网黑市形成规模甚至与恐怖组织合作，渐成独特的互联网恐怖主义。
- APT从一种网络安全里的高级技术攻防手段，变成与魔鬼做交易的筹码。
- APT攻击的前世今生，是充满了魔幻色彩的，暗网的曝光也必然逐渐会让APT为众人熟知，攻防技术的公开是为了对一个事物进行了解并更好的驾驭。
- APT在互联网犯罪里的应用精细已可权衡军事政治应用，甚至超越之。其实不奇怪很多商业卫星的性能已超军事卫星。在这个世界，技术是没有领域无可限控的，当资本注入技术，必然会导致市场化，资本和市场的强大甚至会影响政治。除了规范市场使得技术有合适的经济基础土壤之外，就唯有靠文明和道德来引导了，自古如此。于是，在这个信息时代里，落在网络安全企业、培训机构和相关部门身上的责任，是3600年以来的千秋大业。

Thank you!