网络犯罪心理侧写初探

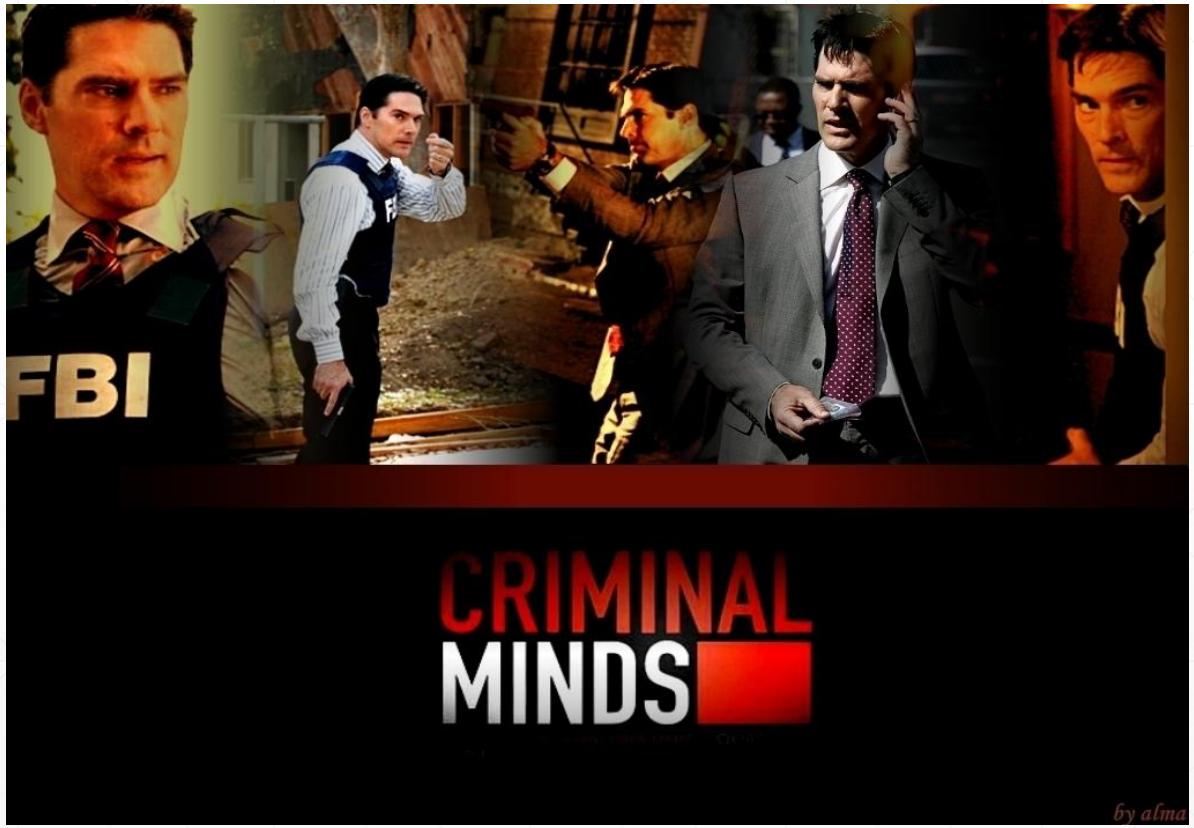
——社会学与心理学·归纳法到演绎法

waterwave@cisrg

目录

网络犯罪心理侧写的起源与研究背景

Criminal Minds



从最近的一篇新闻报道说起

(a) Three samples in criminal ID photo set S_c.

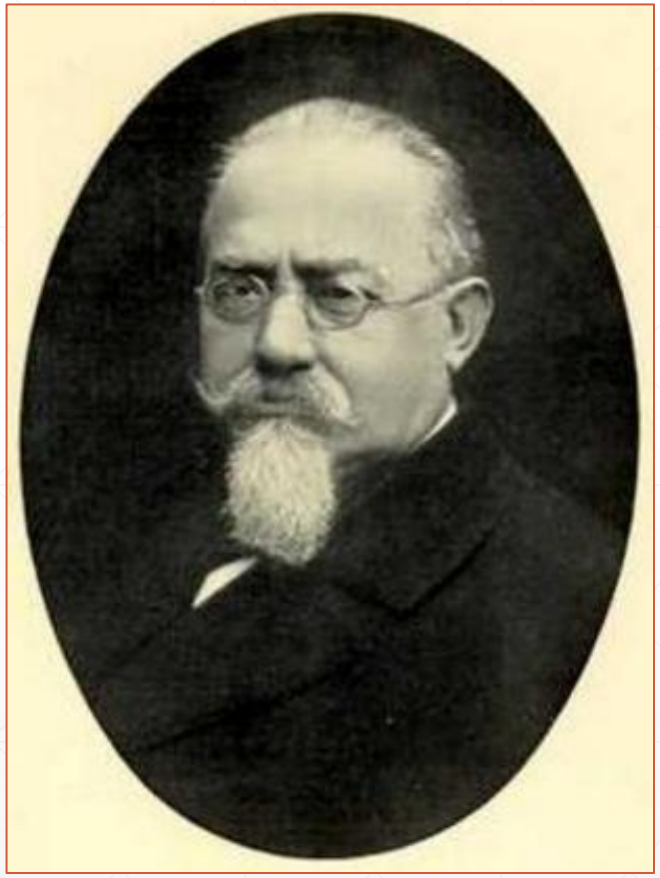
(b) Three samples in non-criminal ID photo set S_n

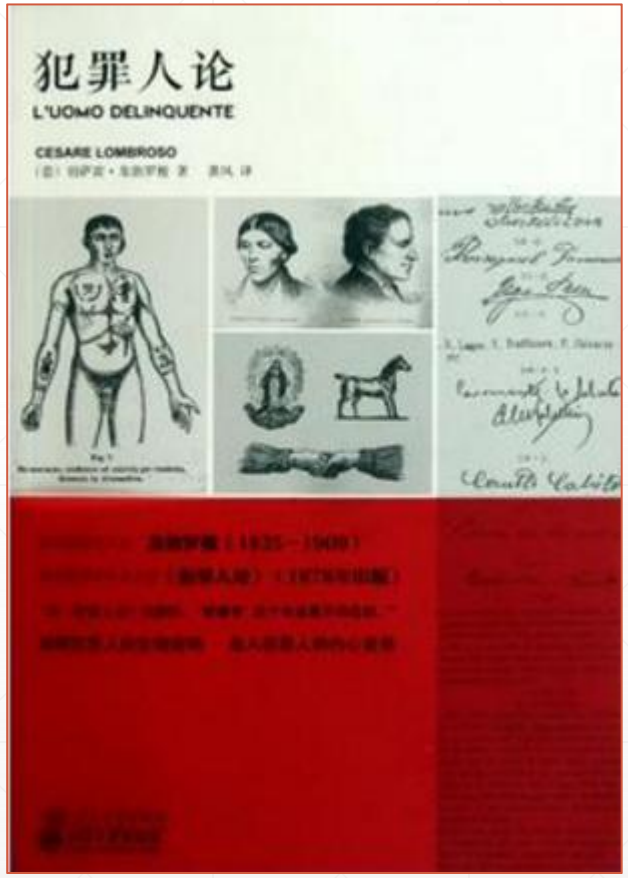
上海交通大学的研究人员吴小林和张希在《arXiv》发表论文称，根据他们前期的研究指出，判断一个人是不是罪犯主要可以根据三个基本的面部特征来进行判断。

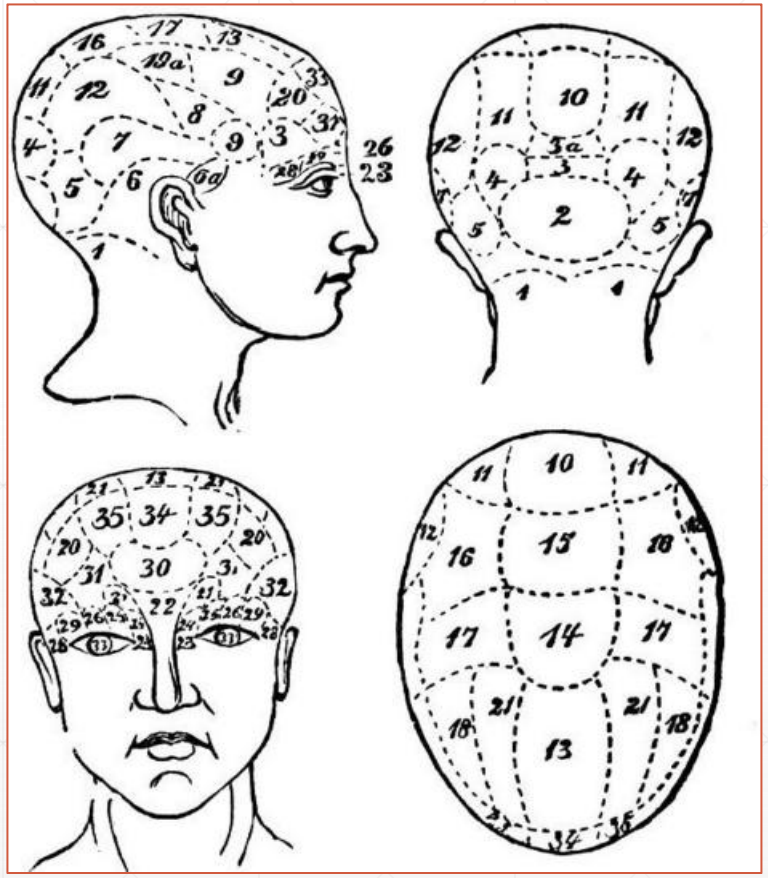
这三个特征包括：嘴唇的弯曲程度；两只眼睛之间距离的大小；鼻尖和嘴角之间角度的大小（可以认为是嘴巴的大小）。

与此同时，根据计算机复杂的计算可以得出结论：那些具有嘴巴比较小，眼间距比较小，嘴唇微微向上弯曲的面部特征的人，更有可能是一个罪犯或者骗子。

寻找模式：犯罪研究的必经之路——生理模式







寻找模式：犯罪研究的必经之路——心理模式

变态的（有组织力的）特征	病态的（无组织的）特征
智商在平均值以上	智商的平均值以下
有足够的社交能力	社交能力很差
胜任技能性工作	一般从事非技能性工作
性行为能力正常	正常性行为无能
多为家中长子	多为家中幼子
父亲有稳定工作	父亲工作不稳定
童年时父母管教矛盾或冲突	童年时管教专制且严厉
犯罪时能控制情绪	犯罪中表示出焦虑的情绪
有时犯罪与酗酒有关	较少使用酒精饮料
有突如其来的情境变化和压力	很少有情境压力
与其他人生活在一起	往往独居
开着一辆车况良好的车	居住或生活在犯罪现场附近
犯罪后关注新闻媒体对案件报道	对新闻媒体几乎不感兴趣
可能会变换工作或离开这个城市	作案后有显著行为变化

1. 从来只有中间值，而没有极端，若有则必然是刻意伪装的结果。
2. 任何表象都是一系列因素共同作用的结果。
3. 通过有组织力日常习得的技能在无组织情境下实施犯罪的结果。
4. 这种简单粗暴的二分法对非暴力与高智商犯罪的作用近乎为零。

自称发现绝对真理的人，恰好是个绝对的傻瓜。
——William Blake，《论敌友》

归纳性与演绎性的犯罪心理侧写

统计学与社会学

归纳性犯罪心理侧写

- 由特殊到一般性结论（前提）
- 对小数量事件得出特征结论
- 通过统计数据得出结论

演绎性犯罪心理侧写

- 由一般到特殊，结论直接来自前提
- 由一般行为特征综合得出特殊结论
- 强调个人行为动机

鉴证科学与心理学

犯罪行为-动机类型

- 证明能力型：通过较为柔和犯罪恢复自信或实现自我价值，企图为犯罪行为寻找合理性
- 权力自信型：使用暴力恢复自信或实现自我价值，通过对被害人的掌握、控制和侮辱体现权威
- 愤怒报复型：犯罪指向特定对象，并有指责与侮辱言语表现
- 激怒兴奋型：通过被害人的痛苦与损失获得喜悦与满足
- 利益型：为获取利益而犯罪，目标明确，手段简单，不具备个人感情色彩

网络犯罪心理侧写与犯罪心理侧写的关系

- “网络犯罪（Cyber Crime）”的定义：

➢ 利用计算机与网络为新型工具所实施的常规犯罪

➢ 以计算机网络与数据为作案对象的新型犯罪

1. 远程入侵教育招生考试系统数据库盗取考生信息进行电话诈骗
2. 撬开机房门锁使用移动硬盘拷贝机密数据

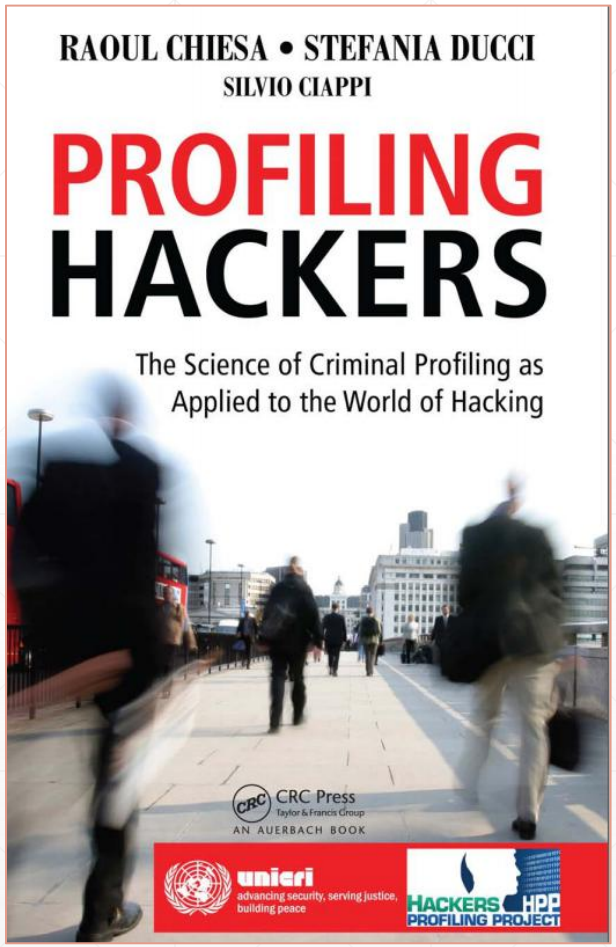
哪种属于我们认知的“网络犯罪”？

“网络犯罪”在本质上仍是发生在特定场合（物理或网络环境），涉及特定要素（计算机网络系统与数据），由特定人群（具备计算机网络技术）所发起的传统犯罪行为，网络犯罪心理侧写方法论自然也可沿用犯罪心理侧写理论。

网络犯罪心理侧写理论与技术框架

基于归纳法

网络犯罪心理侧写的研究与发展



用户行为画像与网络犯罪心理侧写的交叉

ISF 2011关于互联网用户行为画像理论的探索

表名	变量	含义	业务使用场景	TGI	描述性	表总人数	与dm_us	变量枚举值
	pin	用户ID						
search_	cid3	用户图书下感兴趣的	构成情况、TGI、关联品类		1			三级分类码
	weight	权重						连续型数值
	pin	用户ID						
	haschild	是否有孩	构成情况、TGI、模型	1	1			TRUE
								FALSE
	childgender	孩子性别	构成情况、TGI、模型	1	1			only_boy
								only_girl
								boy_girl
								unknown
	gender	顾客性别	构成情况、TGI、模型	1	1			male
								female
	genderconfidenc	顾客性别可信程度	构成情况					high
								medium
								low
								null
	lifecycle	用户生命周期	构成情况、TGI		1			DECLINE
								GROWTH
								LOSS
								SLEEP
								MATURE
								INSPECT
								YOUNG
	valgroup	用户价值分组	构成情况					VG_LOW
	stdscore	标准化价值得分						0
	provincename	省份	构成情况、TGI		1			NULL
	customerconsume	用户购物类型	构成情况、TGI、模型		1			HESITATIVE
								OBJECT_ORIENTED
								RATIONAL
								INPULSIVE
	promotionssensi	用户促销敏感度	构成情况、TGI、模型		1			HIGH
								MIDDLE
								LOW
	skupromotiontyp	单品促销敏感度	构成情况、TGI		1			HIGH
								MIDDLE
								LOW
	suitpromotionty	套装促销敏感度	构成情况、TGI		1			HIGH
								MIDDLE
								LOW
	gppromotiontype	团购优惠促销敏感度	构成情况、TGI		1			HIGH
								MIDDLE
								LOW

某国内领先电商的用户行为画像指标模型

网络犯罪动机角度的作案人类型研究

动机种类	动机说明
探索者	动机由好奇心驱使，很少造成损失（Old School）
责任心过强者	“帮助别人”或炫耀技术动机（白帽子）
挑战者	挑战规定与技术限制，以满足自尊心需要（灰帽或部分黑帽）
不择手段者	为满足个人利益而无节制地使用网络技术
自我认同者	认为自己技高一筹，应该获得更多利益
复仇者	由获得不公正待遇的复仇心驱使
职业罪犯	为获取巨额利益不择手段
间谍	为获取情报采取隐秘手段

利用网络技术进行的传统犯罪行为如色情、诈骗、诽谤等不在讨论范围

网络犯罪技术水平角度的作案人类型研究

Wannabe Lamer 无水准

Script Kiddie 低水准

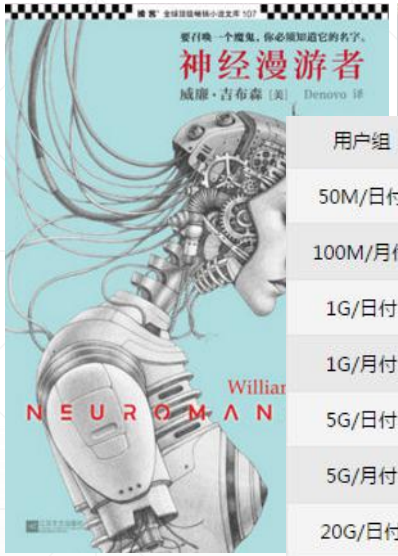
Cracker 中高水准

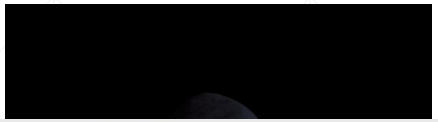
Elite Hacker 高水准

- ✓ 伦理黑客
- ✓ Q.P.S（Quiet，Paranoid，Skilled）黑客
- ✓ 网络军队
- ✓ 工业间谍
- ✓ 政府特工
- ✓ 军事间谍

网络犯罪心理的“黑客亚文化”因素

- 欧美黑客亚文化
  - 赛博朋克（Cyber Punk）
  - Old School Hacker
  - 欧美现代文化因素
- 中国**没有**黑客亚文化
  - “江湖”文化
  - 民族（民粹）主义
  - 拜金与享乐主义





用户组	价　格	有效期	赠送积分	操　作
50M/日付	30元	1天	免费20分钟已升级日付:防止他人恶意浪费	立即开通
100M/月付	500元	30天	（100M/每秒）全自动开通 无限流量 目标地址:IP	立即开通
1G/日付	100元	1天	（1G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
1G/月付	900元	30天	（1G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
5G/日付	300元	1天	（5G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
5G/月付	2800元	30天	（5G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
20G/日付	1150元	1天	（20G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
20G/月付	9800元	30天	（20G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
40G/日付	2000元	1天	（40G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
40G/月付	16800元	30天	（40G/每秒）全自动开通 无限流量 目标地址:IP	立即开通
CC日付	300元	1天	（无视高防 无视CDN加速） 网站地址:http开头必填	立即开通
CC月付	2600元	30天	（无视高防 无视CDN加速） 网站地址:http开头必填	立即开通
高级版CC日付	600元	1天	（无视高防 无视CDN加速 增加五倍威力） 网站地址:http开头必填	立即开通
高级版CC月付	5500元	30天	（无视高防 无视CDN加速 增加五倍威力） 网站地址:http开头必填	立即开通

网络犯罪心理的社会因素

政治经济因素

- 社会形势与思潮变化导致网络群体心理失衡
- 贫富差距与高失业率导致心理失衡与无业人员流失网吧等场所
- 对网络犯罪分子的错误过高评价
- 个人本位、拜金主义、享乐主义的个人价值观
- 网络道德的缺失
- 网络犯罪的低成本、低风险、高收益特性

家庭因素

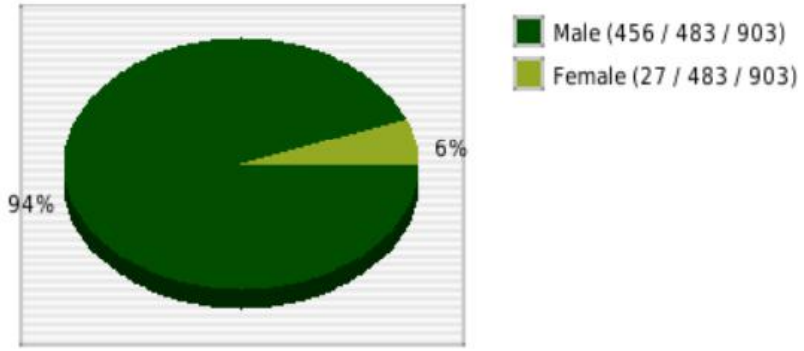
- 溺爱型家庭教育导致个人本位、控制型犯罪心理形成
- 漠视或简单粗暴家庭教育导致自我认同缺失或愤怒型犯罪心理形成
- 家庭不幸导致性格孤僻、冷漠，产生仇视对抗心理

教育与人际因素

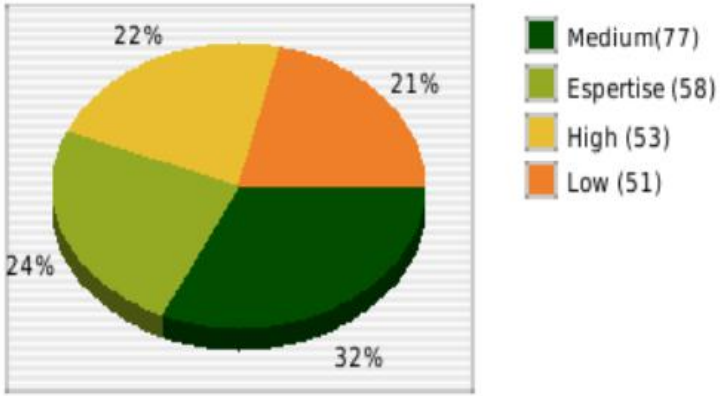
- 学校教育内容失衡
- 网络人际交往难以控制
- 异性交往能力不足
- 现实社交面狭窄

Hackers Profiling Project（HPP）的数据统计

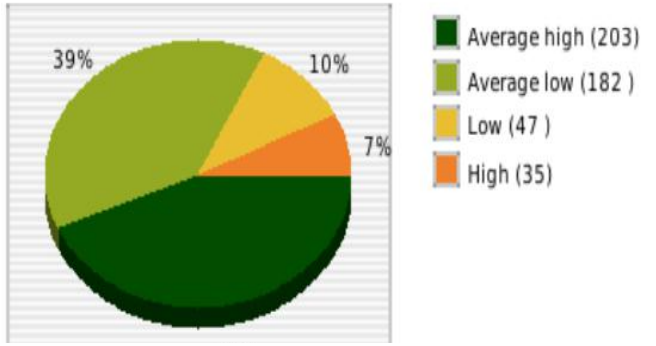
Sex



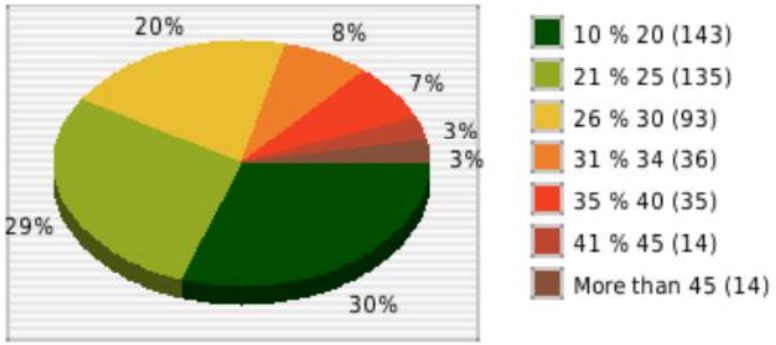
Technical skills [Total: 239, Null: 1180]

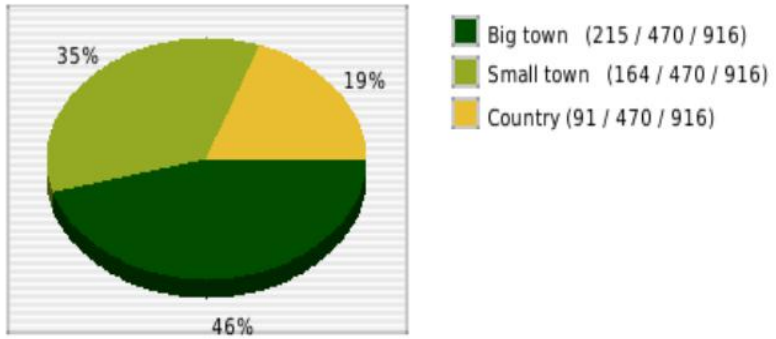


socio-economic status [Totals: 467, Null: 919]

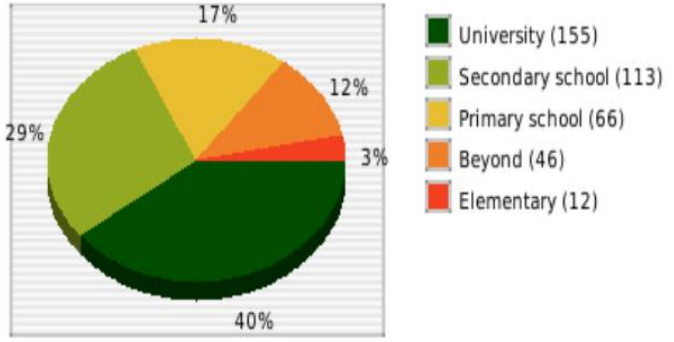


Age [Total: 471, Null: 915]

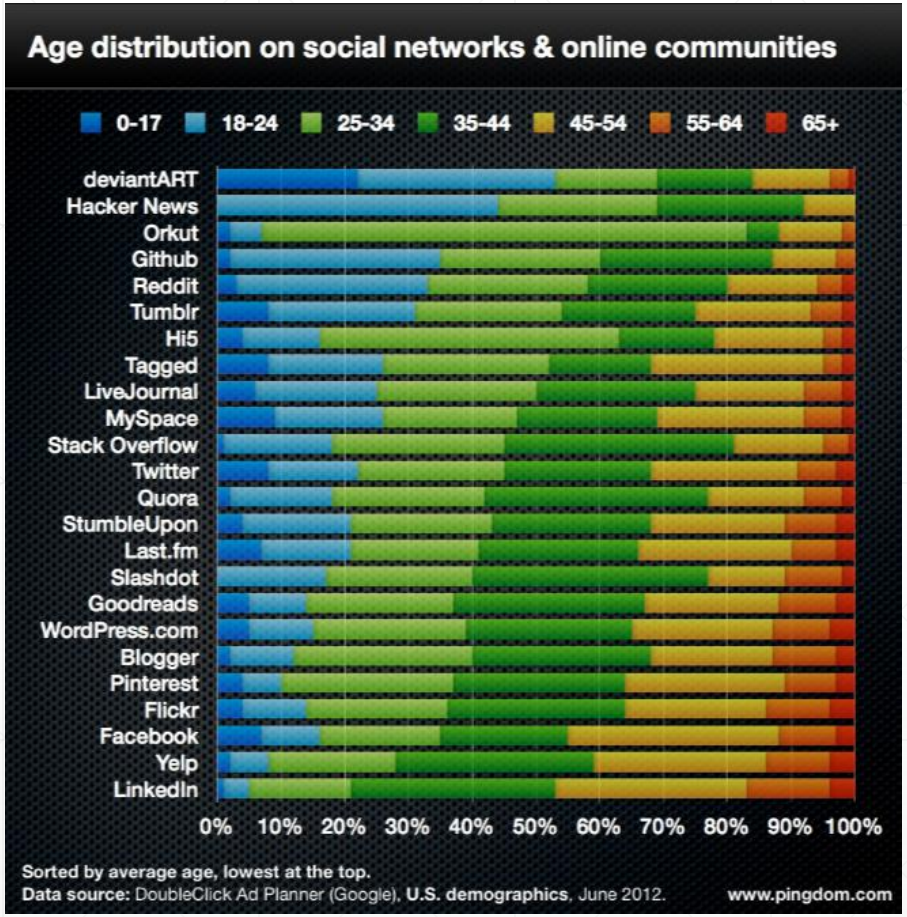


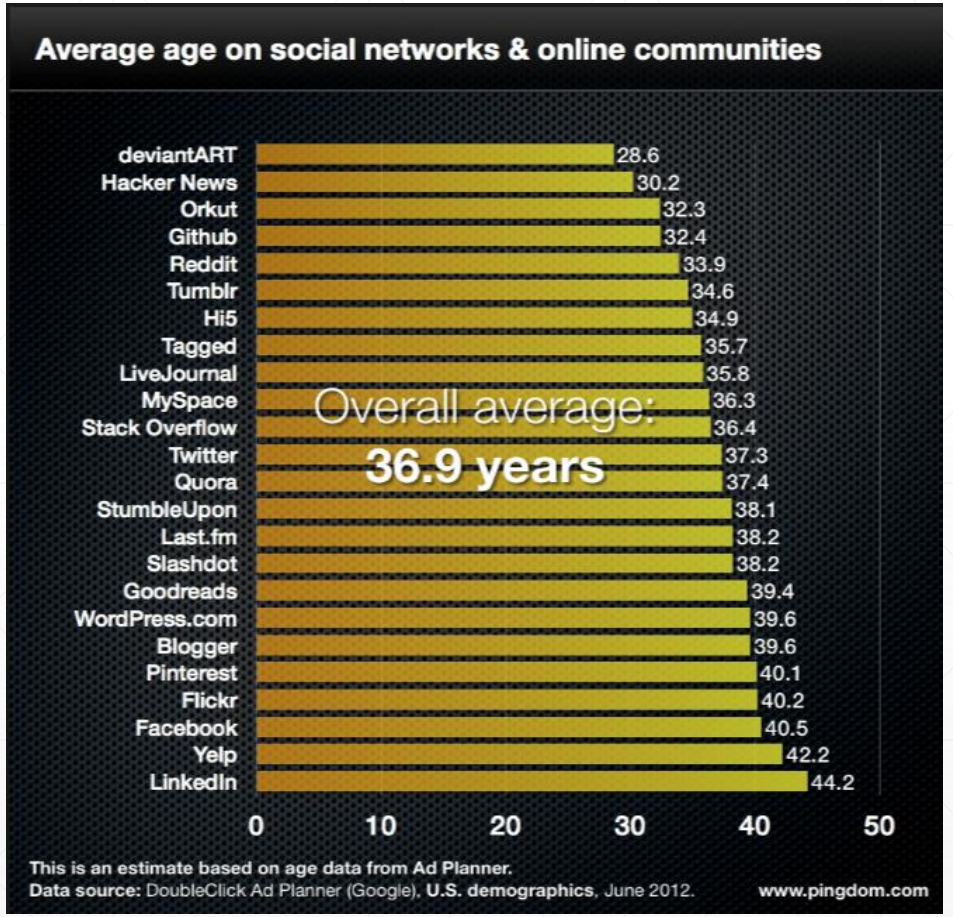


Studies [Total: 426, Null: 954]



网络犯罪的年龄与教育因素





- 年龄分布：14-35岁
- 教育程度：初中-硕士学历不等，受教育程度与其网络犯罪技术水平呈正相关

网络犯罪心理的演进

犯罪自觉性与主动性增强	• 道德观念与避险心理消失 • 作案信心与作案趋利性增强
个人欲望急剧膨胀	• 作案成功体验刺激新欲望产生 • 新欲望产生制造新的作案动机
作案经验丰富	•网络犯罪技能水准提升 •网络犯罪心态更平静与稳定 •伪装、自我保护等反侦察能力提高
犯罪活动向组织化发展	• 建立网络犯罪组织 • 建立组织内部精细化分工体系
犯罪意识弥散性	• 在人际圈内散布网络犯罪合理化言论
犯罪职业化加强	• 与社会疏远与对立，成为职业网络犯罪分子，将网络犯罪所得作为生活来源与满足精神需要的经济来源

网络犯罪者性格分析

- 具备极端性：
  - ✓ 一般情况下较为理智与冷静
  - ✓ 年龄较低的犯罪者具备很强好斗性，看重排名与胜负、虚荣
- 喜好刺激：
  - ✓ 通过挑战高难度犯罪目标寻求刺激
  - ✓ 偏好具有刺激性的消遣娱乐方式如吸烟、酒精、毒品、色情、高速驾驶等
- 自我意识：
  - ✓ 缺乏社会责任感与义务感，缺少自省意识
  - ✓ 具备计划性，具有耐心、毅力，善于应变
  - ✓ 反侦察能力和意识与年龄、性格、技术手段正相关

网络犯罪行为矩阵的组织特征与操作特征

	组织性	组成动机	交流方式
团队	反主流文化倾向，无组织结构，管理松散	被团体归属感或成员个人魅力吸引	以团队形式与其他团体进行整体对话与联系
个人	无组织	挑战自我能力、虚荣心或个人利益	使用邮件、邮件组或BBS相互联系
间谍	雇佣机构组织	经济利益，意识形态，自我宣示	入侵目标主机窃取资料，但极少或不与人交流
网络欺诈者	组织犯罪与个人犯罪皆有可能	经济利益	通过网络欺诈获取经济利益
外来恶意入侵者	独自一人或小团体	抱持恶意进行入侵破坏，原因为恶意、经济利益、虚荣心	入侵目标主机窃取资料并造成破坏，常有故意侮辱行为
内部恶意入侵者	内部员工或前员工	报复或心存不满	低调入侵并破坏

	策划	专业技术水准	入侵方式
团队	有详细、严密的行动计划	技术水平较高，且个人能力可进行团队组合	入侵目标主机与管理员或其它黑客交流
个人	攻击前经过网段扫描选择有漏洞目标	中高水平，通过学习摸索增长经验	较多使用漏洞扫描选择目标
间谍	有详细、周密、严谨的行动计划	职业犯罪者，高水平	任何可能的入侵方式，包括雇佣精英黑客
网络欺诈者	犯罪之前有详细计划	中低水平，欺诈能力比技术能力高	更多选择非技术层面的漏洞与盲点
外来恶意入侵者	没有策划，多为临时起意或冲动性犯罪	恶意破坏者，技术水平参差不齐	选择目标具有随机性且盲目性
内部恶意入侵者	蓄谋已久且做过一次以上试验	水平参差不齐，但熟悉内部情况	使用木马程序进入内部系统

网络犯罪矩阵的行为特征与资源特征

	参与动机	人格特征	潜在弱点
团队	挑战自我能力，共同爱好者交流，共同理想及目标	高智商，具有反主流文化倾向，自信心强	不认为攻击是犯罪行为，乐于公开讨论与炫耀
个人	挑战自我，提高能力，个人利益，个人理想	中高智商，一般水平线以上，自信心强，个人主义	常保留扫描入侵记录、截图及窃取的数据等
间谍	个人及国家利益	高智商，入侵能力强，思维缜密，	对取得数据过于执着而可能忽略自我隐藏
网络欺诈者	个人经济利益	职业诈骗犯人格特征，贪婪狡猾且胆小	过于贪婪，容易被利益诱惑而犯错
外来恶意入侵者	挑战自我智力，个人利益	恶意破坏者，缺乏责任感，易烦躁	攻击行为可能明目张胆，容易犯错
内部恶意入侵者	为报复或经济利益	具有一定技术基础，具有偏执倾向	可能会在内部安全审计体系中留下日志

	技能资源	装备资源	人力资源
团队	进行过正式或非正式的高水平教育训练	根据具体需求由同伴间共享交流各类装备	由团队同伴支援
个人	通过自学摸索和积累经验	计算机，网络连接	网络社区及各类通讯工具进行信息交换
间谍	各种技能资源皆有可能	根据任务需求配备性能最好的装备	暗中由雇主或组织支持
网络欺诈者	未受过或很少训练	计算机，网络，电话及骗术所需设备	有犯罪团伙支持
外来恶意入侵者	受训练及教育程度参差不齐	计算机，网络连接	网络信息共享，团队支持
内部恶意入侵者	有一定计算机技能，具有自学能力	有进入到目标主机的机会	无

网络犯罪心理侧写的调查实践

基于演绎法

网络犯罪心理侧写步骤与主要指标

侧写步骤

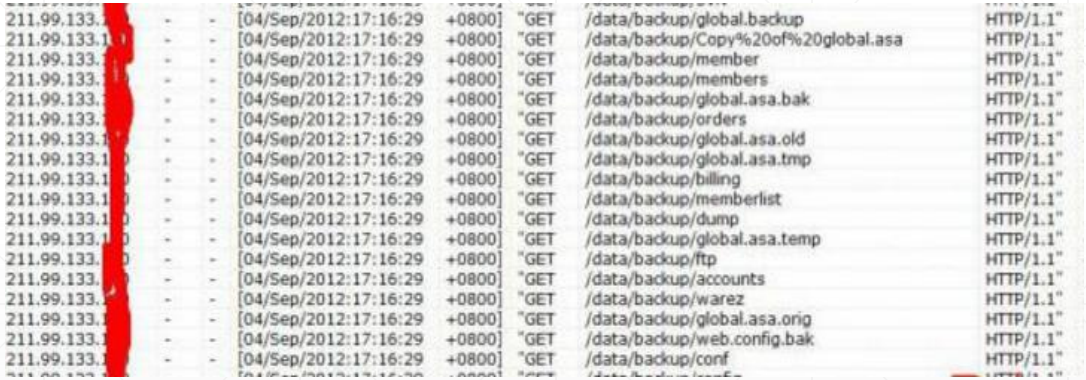
1. 从一般到特殊，重点挖掘个体特征
2. 使用演绎法进行分析
3. 进行情报分析排除侧写对象外在行为不确定性
4. 克服认知偏好，排除内在动机不确定性。

分析指标

- 谨慎的组织力分析
- 个人标记
- 个人特征
  - ✓ 在线时间
  - ✓ 在线频率
  - ✓ 技术水平
  - ✓ 语言风格
  - ✓ 审美取向
- 行为特征

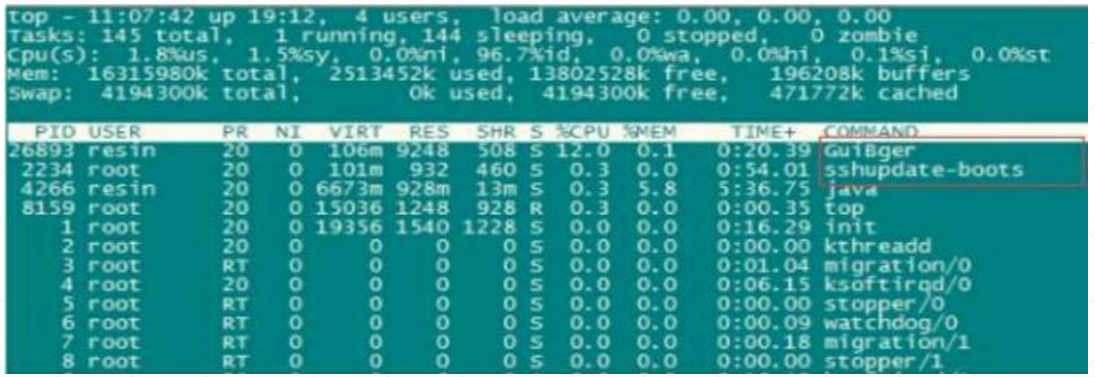
组织力指标分析

无组织力迹象



- 行动具备目的性与步骤性，但对行为风险缺乏评估意识与能力
- 未知防，焉知攻？

有组织力迹象



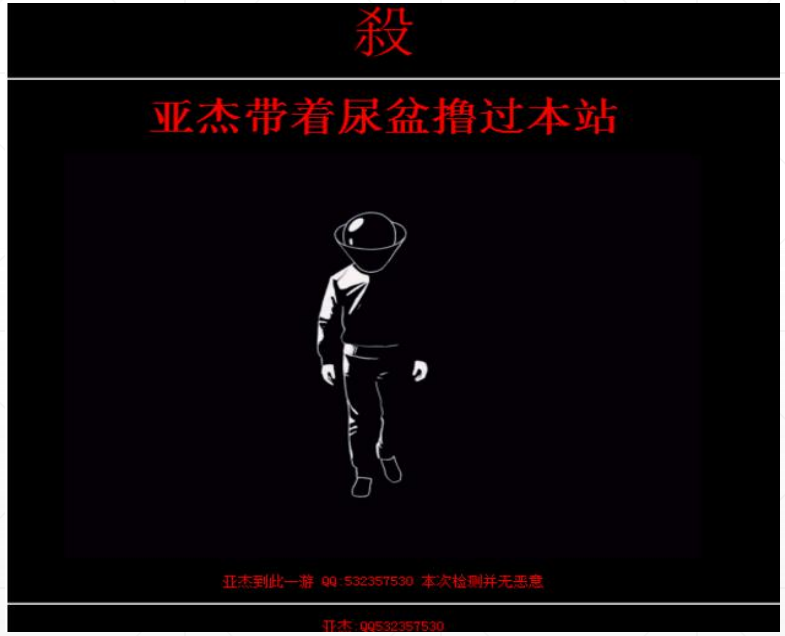
- 行动的每个步骤都缜密计划，最大限度隐藏与伪装自己
- 了解监测与防御体系（经过细致踩点或内部人员作案）

个人标记指标分析

ID类型分析

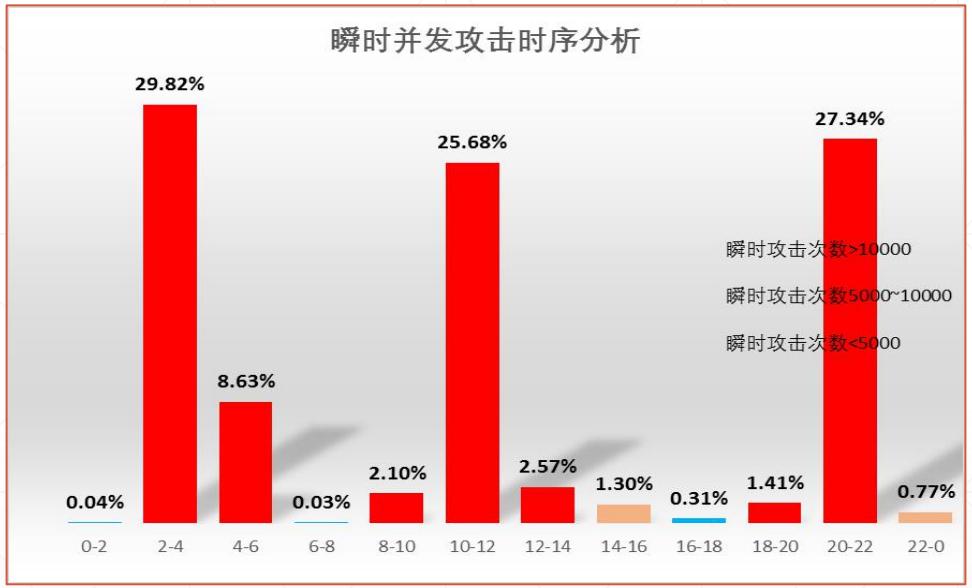
- 媞誰惹ㄋ噯
- Swagrrrrrrr
- 9reaker#470x12
- Chinafans/0x_fans
- Billy
- 莫大先生

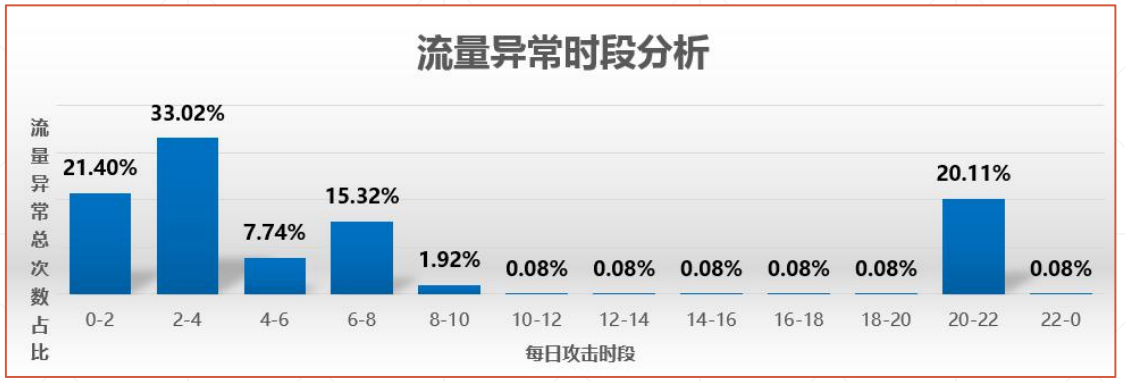
黑页类型分析



挂黑页行为本身即是一种个人标记的表现

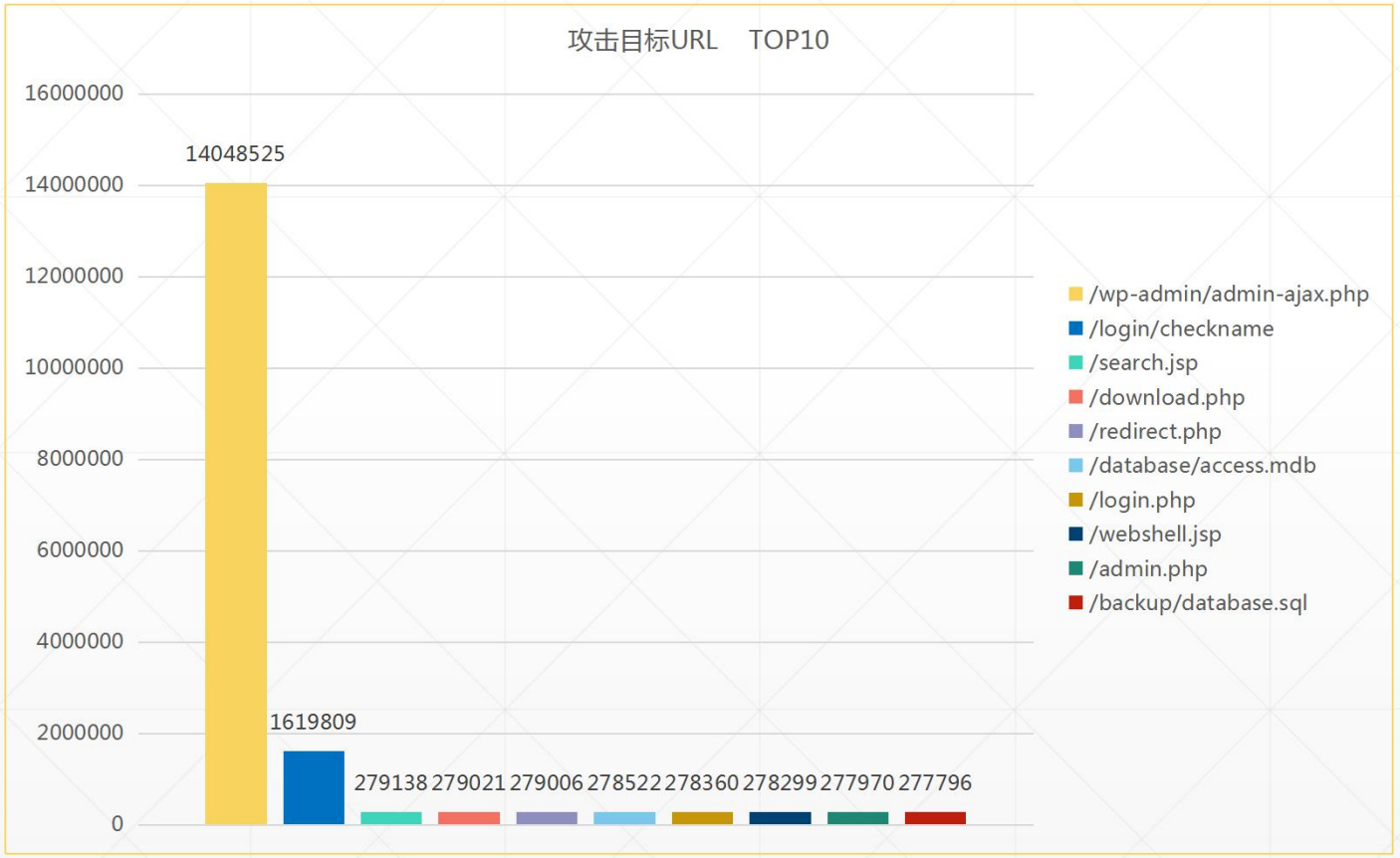
攻击时序与频率指标分析





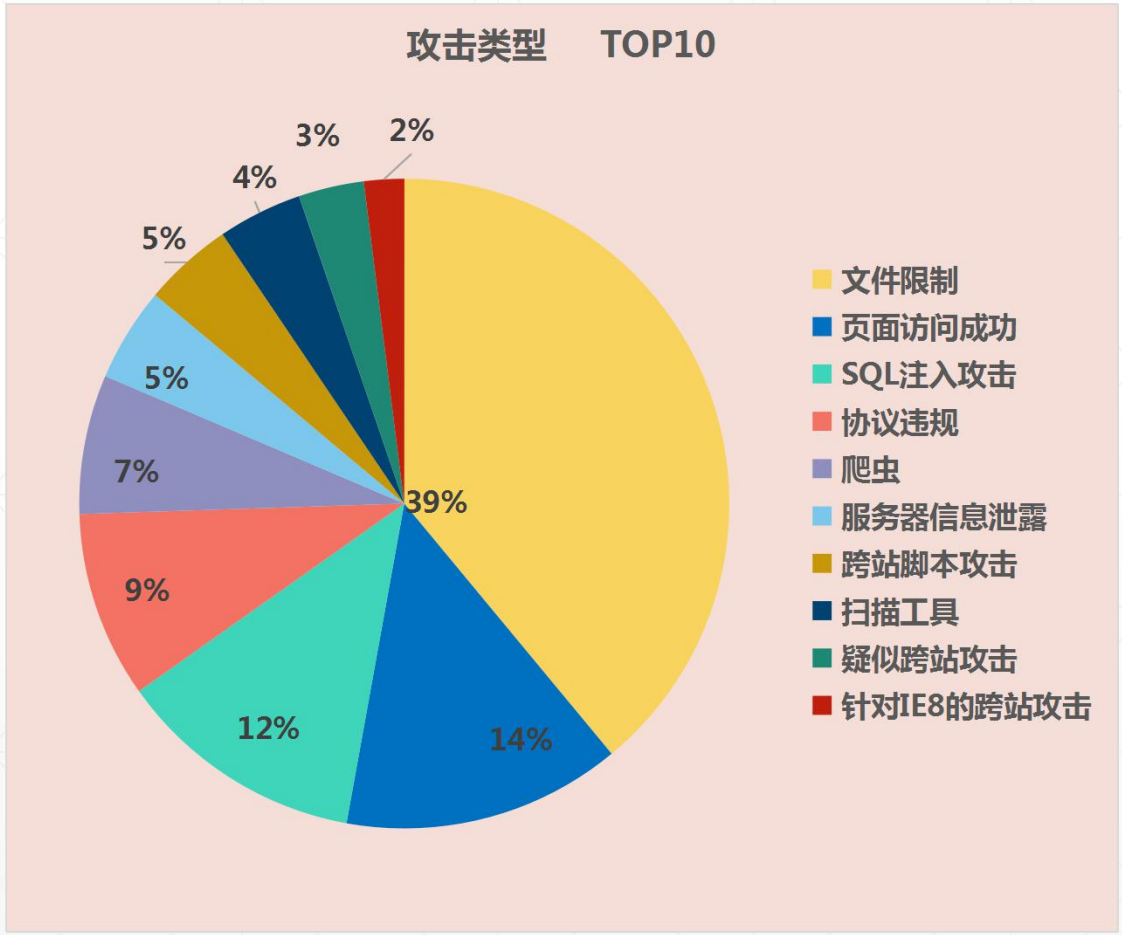
- 业务高峰时段发起C-C攻击的目的性明显
- 凌晨发动流量攻击强度达到顶峰的意图又是什么？

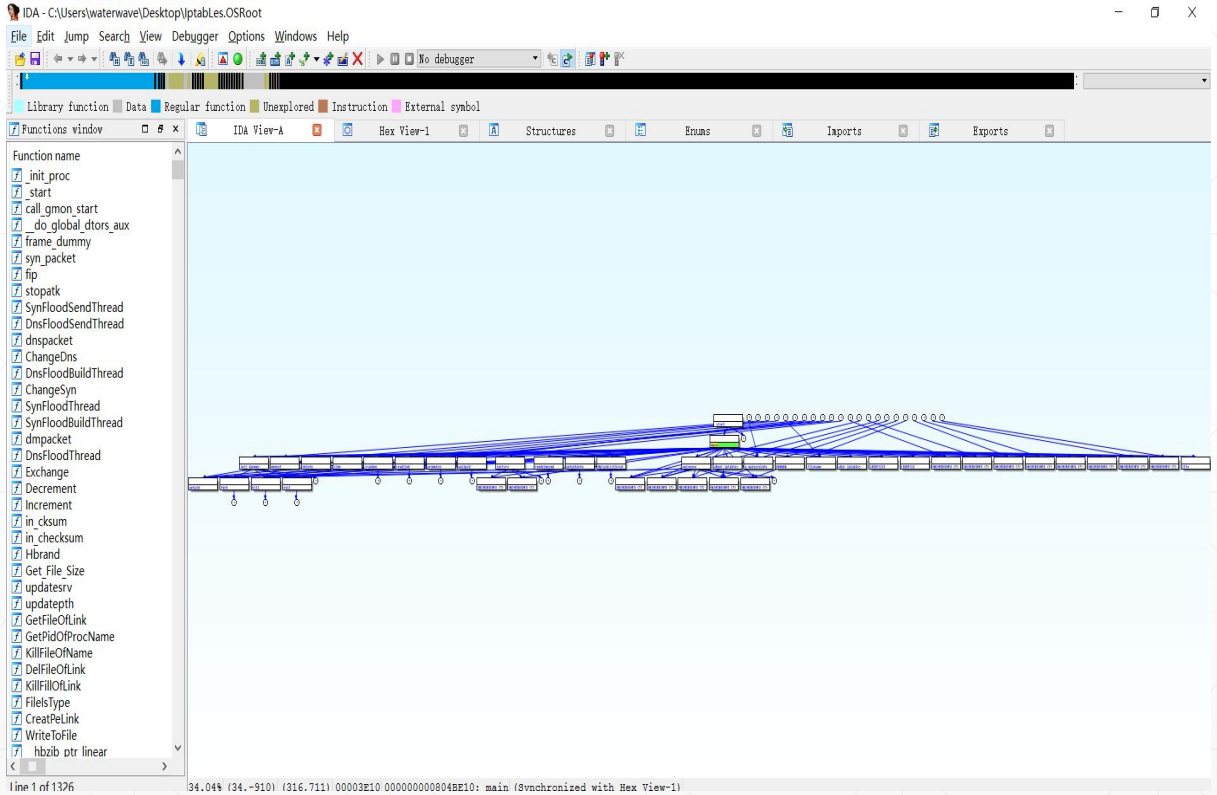
攻击部位指标分析



由左表可以清楚判断出，非法攻击者尝试访问最多的网站目录为网站管理登录页面、搜索页面与数据库文件保存页面、网页后门页面等，所对应攻击手法则为后台管理口令暴力破解、目录越权访问与SQL注入攻击等

攻击水平指标分析

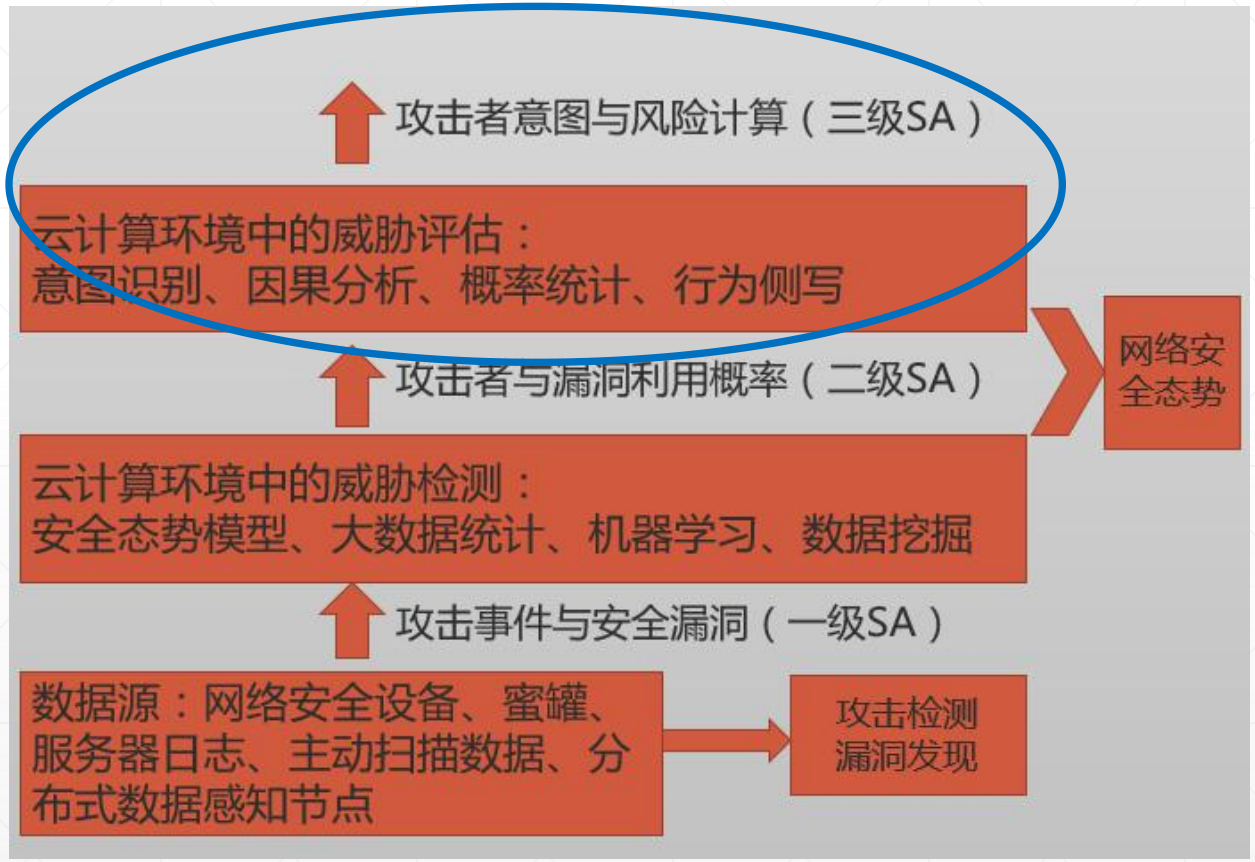

攻击类型 TOP10
39%
14%
12%
9%
7%
5%
5%
4%
3%
2%
文件限制
页面访问成功
SQL注入攻击
协议违规
爬虫
服务器信息泄露
跨站脚本攻击
扫描工具
疑似跨站攻击
针对IE8的跨站攻击


IDA - C:\Users\waterwave\Desktop\IptabLes.OSRoot
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Function name
_init_proc
_start
call_gmon_start
__do_global_dtors_aux
frame_dummy
syn_packet
fip
stopatk
SynFloodSendThread
DnsFloodSendThread
dnspacket
ChangeDns
DnsFloodBuildThread
ChangeSyn
SynFloodThread
SynFloodBuildThread
dmpacket
DnsFloodThread
Exchange
Decrement
Increment
in_cksum
in_checksum
HBrand
Get_File_Size
updatesrv
updatepth
GetFileOfLink
GetPidOfProcName
KillFileOfName
DelFileOfLink
KillFillOfLink
FileIsType
CreatPeLink
WriteToFile
hbzib_ptr_linear
Line 1 of 1326

威胁情报与安全大数据的误区

一级SA觉察 → 二级SA理解 → 三级SA应用

态势感知（SA）过程

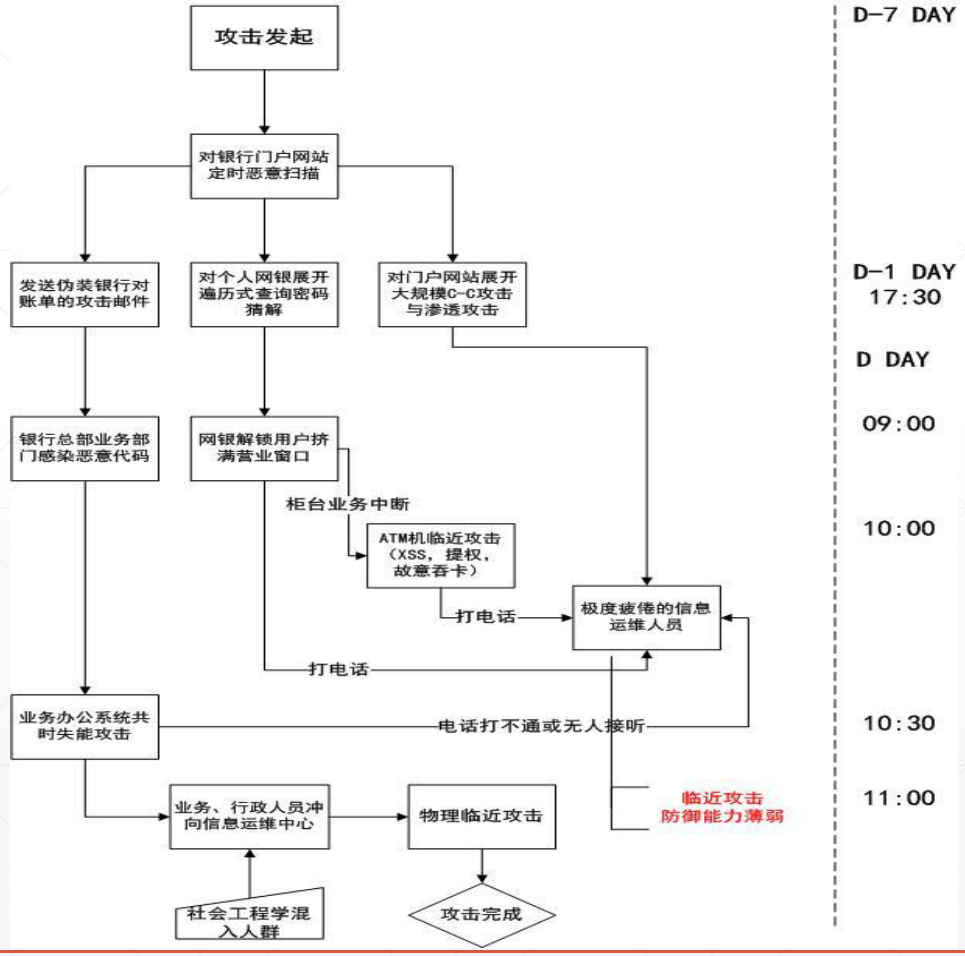


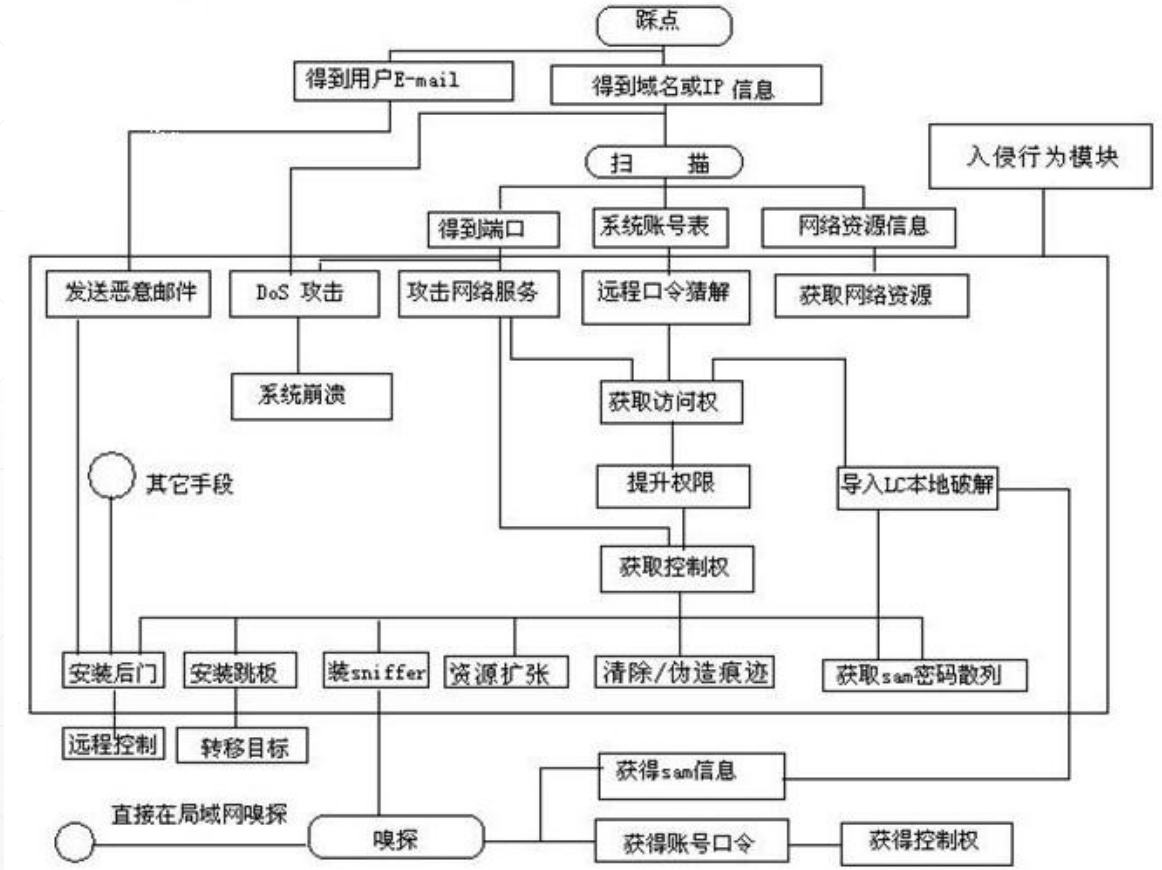
基于安全分析师的网络犯罪心理侧写

网络犯罪心理侧写的目的

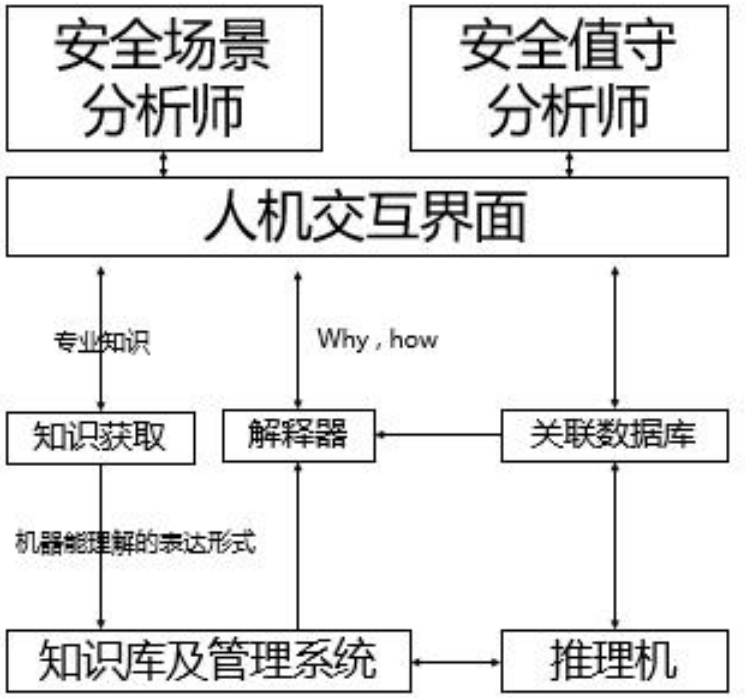
- 在攻防场景下，网络犯罪心理侧写的目的是寻找**攻击行为模式**
- **绝大多数基于“大数据”、“机器学习”等概念声称能做“黑客画像”的，必然会结合威胁情报库、社工库等定位方法，而非“网络犯罪心理侧写”理论所定义的“画像”**
- **Profiling=侧写=侧面画像，直接定位的不叫Profiling**

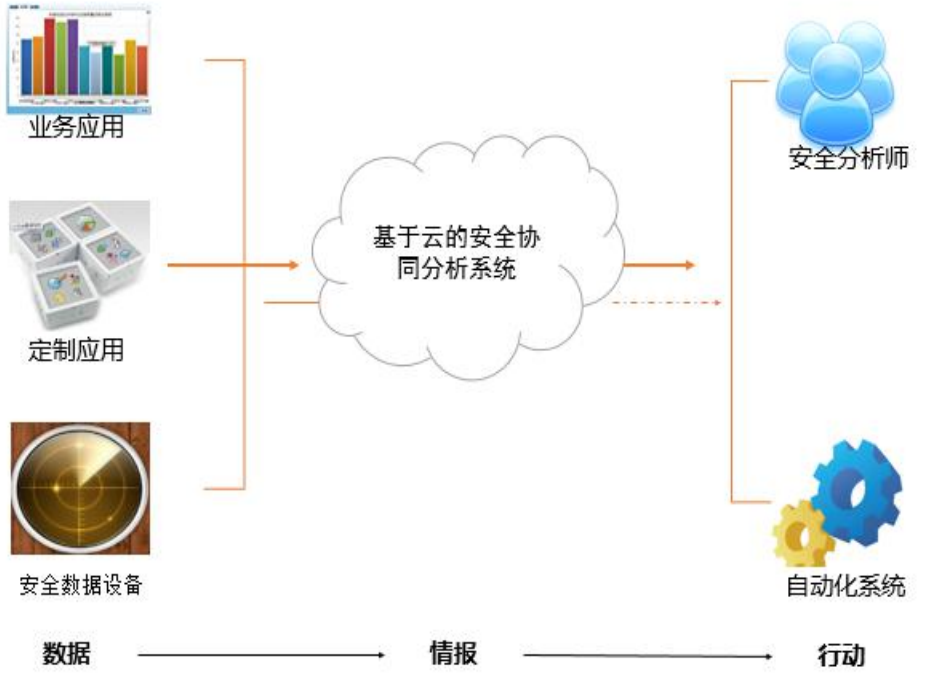
基于安全大数据“中观”层面的攻击场景分析





Analyst on Duty & Analyst in the Situation





- ✓中央安全场景分析师与远程值守分析师协作加强
- ✓基于资源共享的协作：分析资源共享与分析产出共享
- ✓基于内容层面的协作
- ✓基于功能层面的协作：工作流协作

谢谢！