先进持久对抗条件下僵尸网络的数据化生存

潜伏鹰　博士

安全研究员

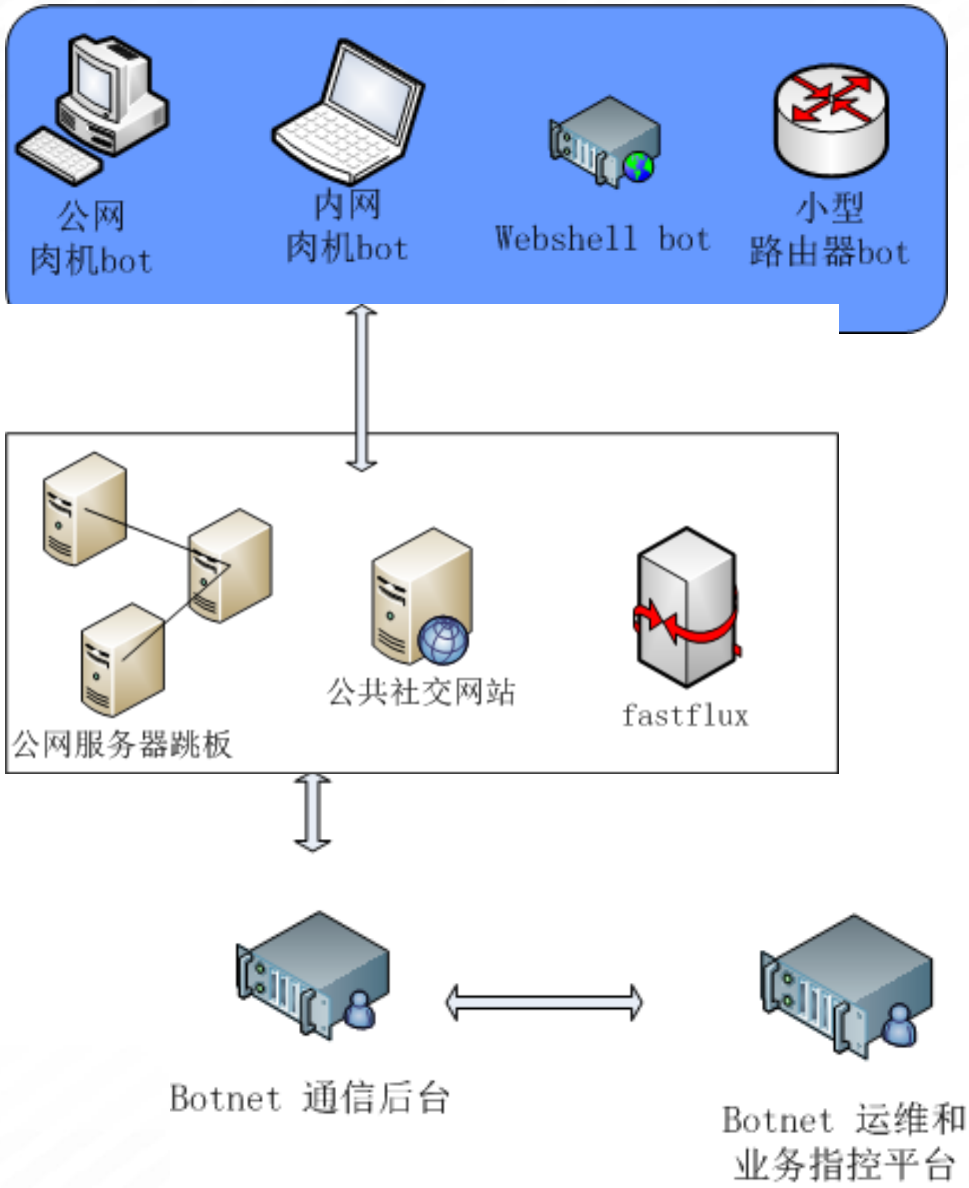
专注于僵尸网络和匿名通信

ISC 2014 中国互联网安全大会

360互联网安全中心

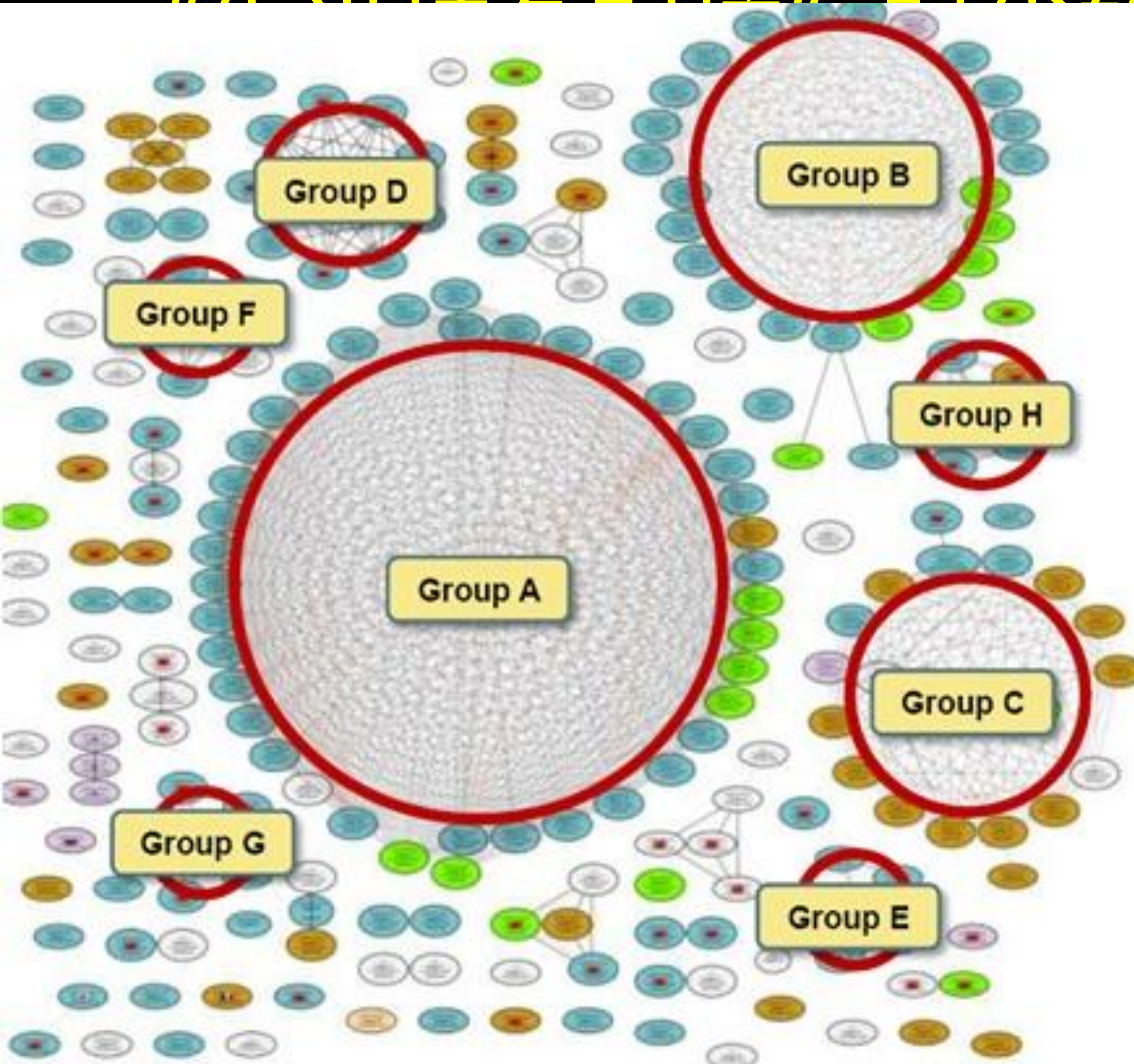
China Internet Security Conference 2014

2014中国互联网安全大会



- 什么是僵尸网络？
  - 前端bot（分布于互联网上的海量肉机）
  - 隐蔽通信跳板
    - 新涌现的社交网路（微博、博客、论坛）
    - VPS/肉机
    - DNS基础设施（DDNS、fastflux、domianflux）
  - Botnet C&C后台（大规模行动指挥平台）

botnet



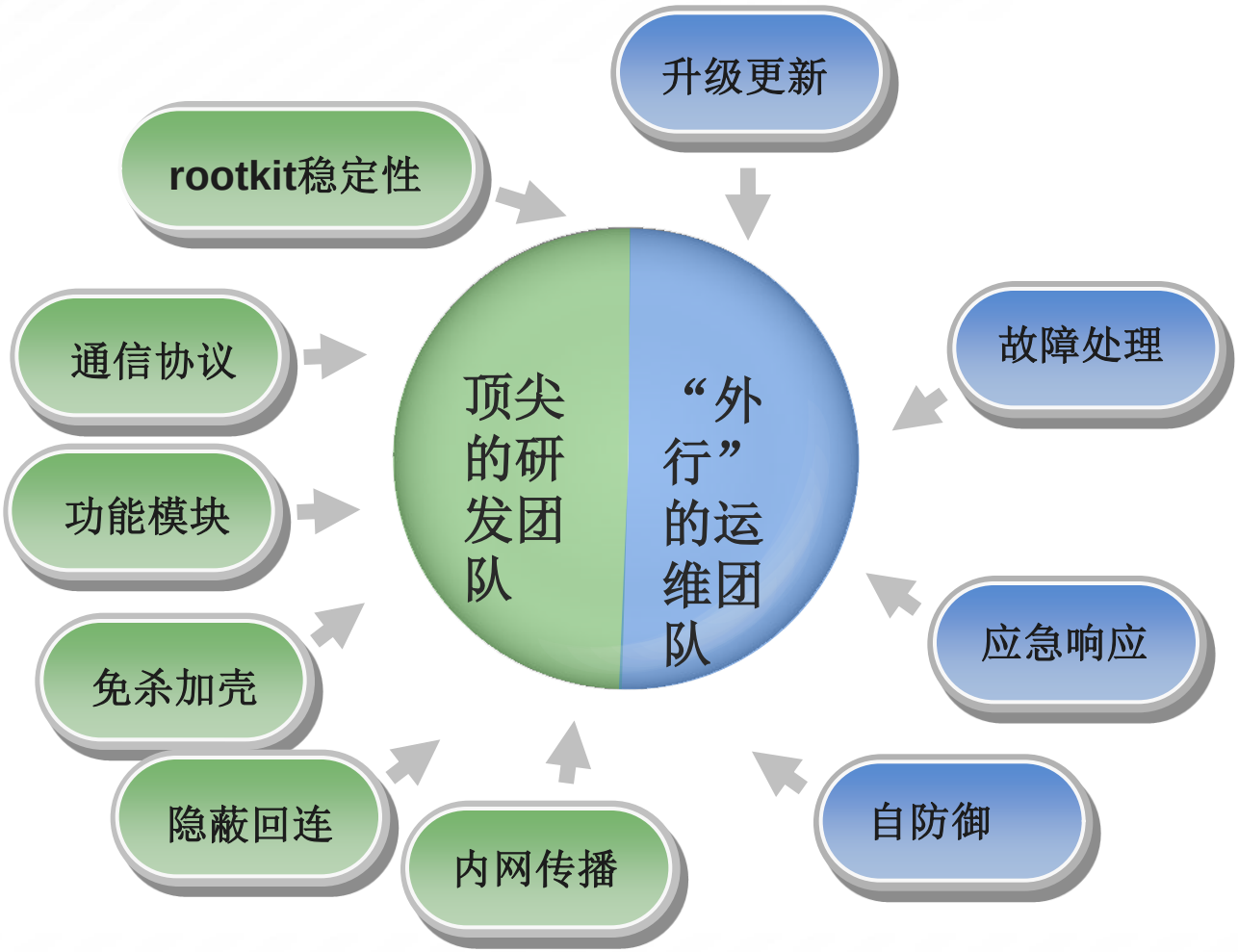
基于大数据的
级纵深主动防
系，小黑们的
击队”战术不
久

- 作为一种可灵
活运用于资源

- 告别“拍脑袋指挥”，让我们迎来“基于对抗态势感知的智能辅助指挥”时代。

一、当前僵尸网络运用中广泛存在的问题

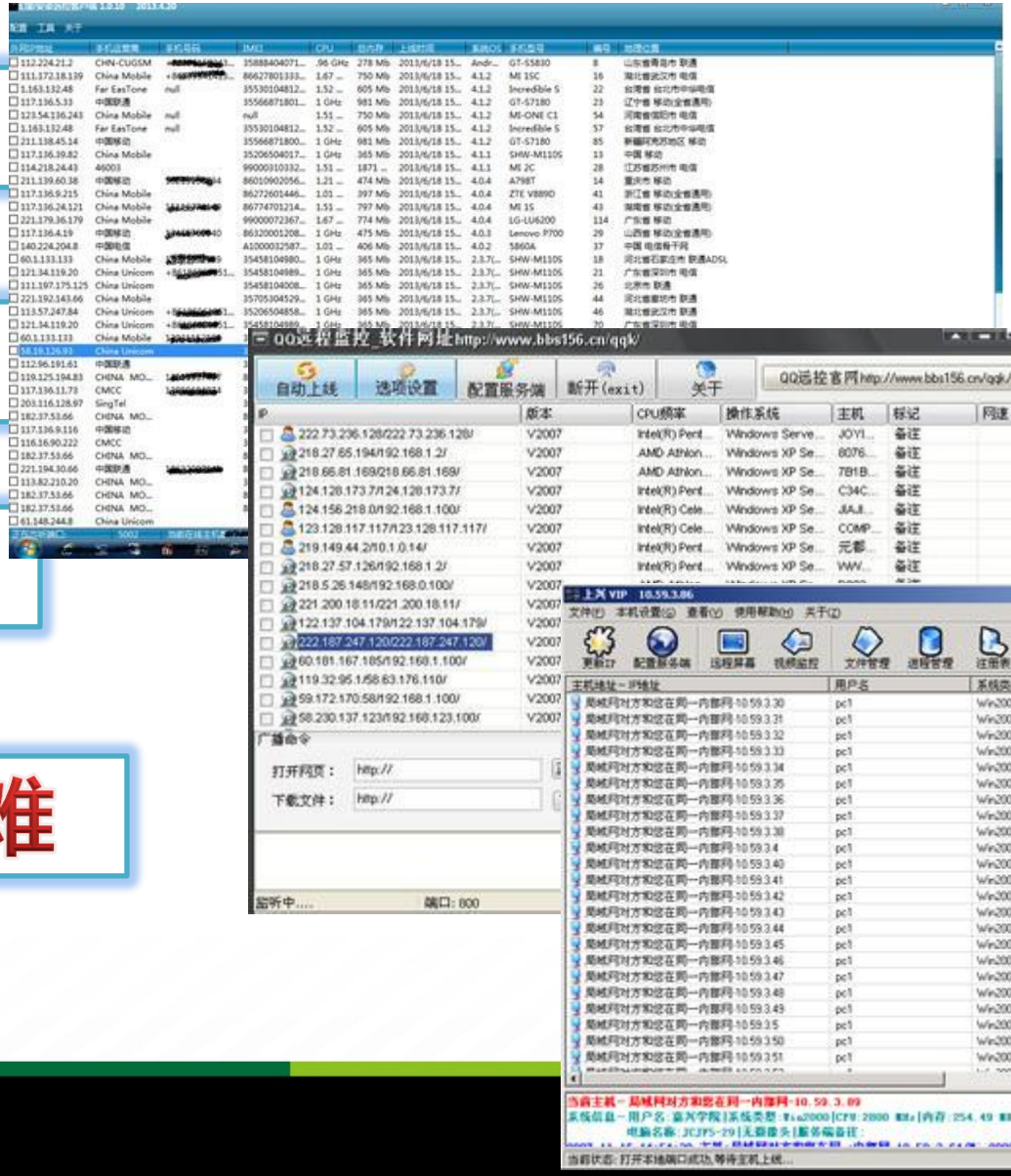
1. 重尖端技术研发、轻运行维护管理



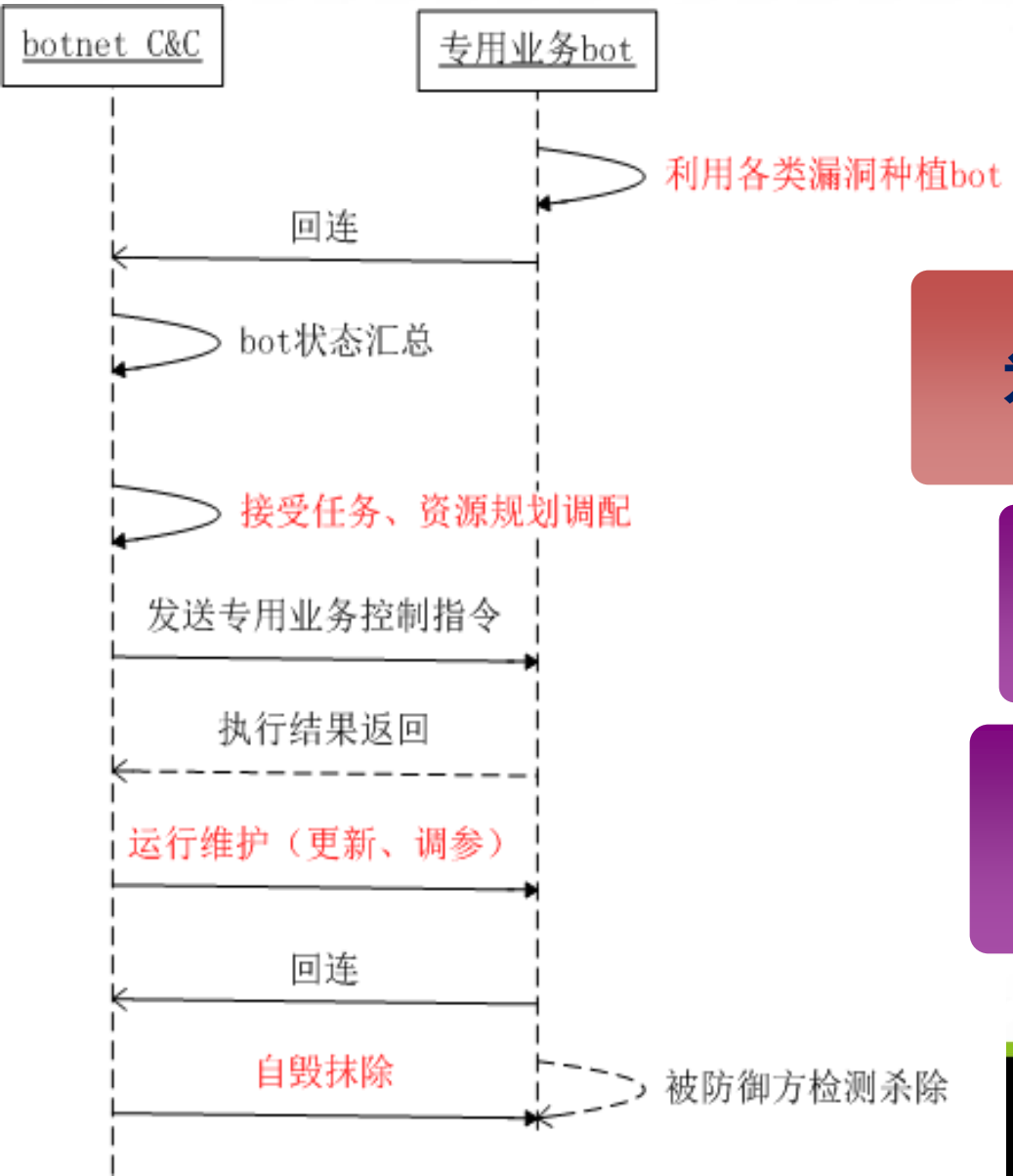
2.复杂的运用环境和薄弱的人才队伍

ISC 2014

- bot型号众多
- 分布环境迥异
- 队伍流动性大
- 运用经验继承难



3.业务指挥呼唤理论化、战术化、科学化



用什么0day、挂马站、工具种bot？
种什么bot?

为什么今天要调配那批代理跳板？
为什么这次要使用那个botnet?

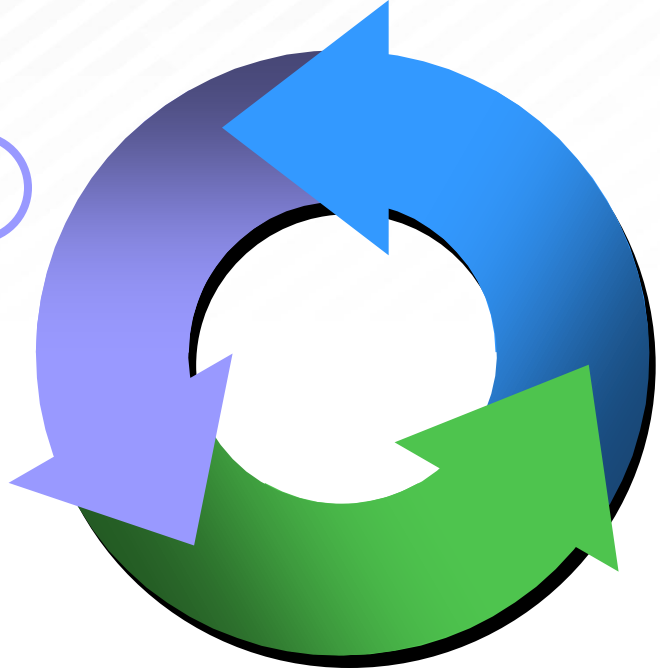
不管各目标区域当前情况如何
“所有木马集群统一行动”？！

新版本/模块频繁升级，
不管是否出现异常情况，
“删除老木马，统一升级新木马”

二、设计构建僵尸网络全局对抗态势感知&辅助指挥平台

“态势感知”远不仅仅是“把存活的bot标在漂亮地图上给领导看”、更不仅是“统计top10”！

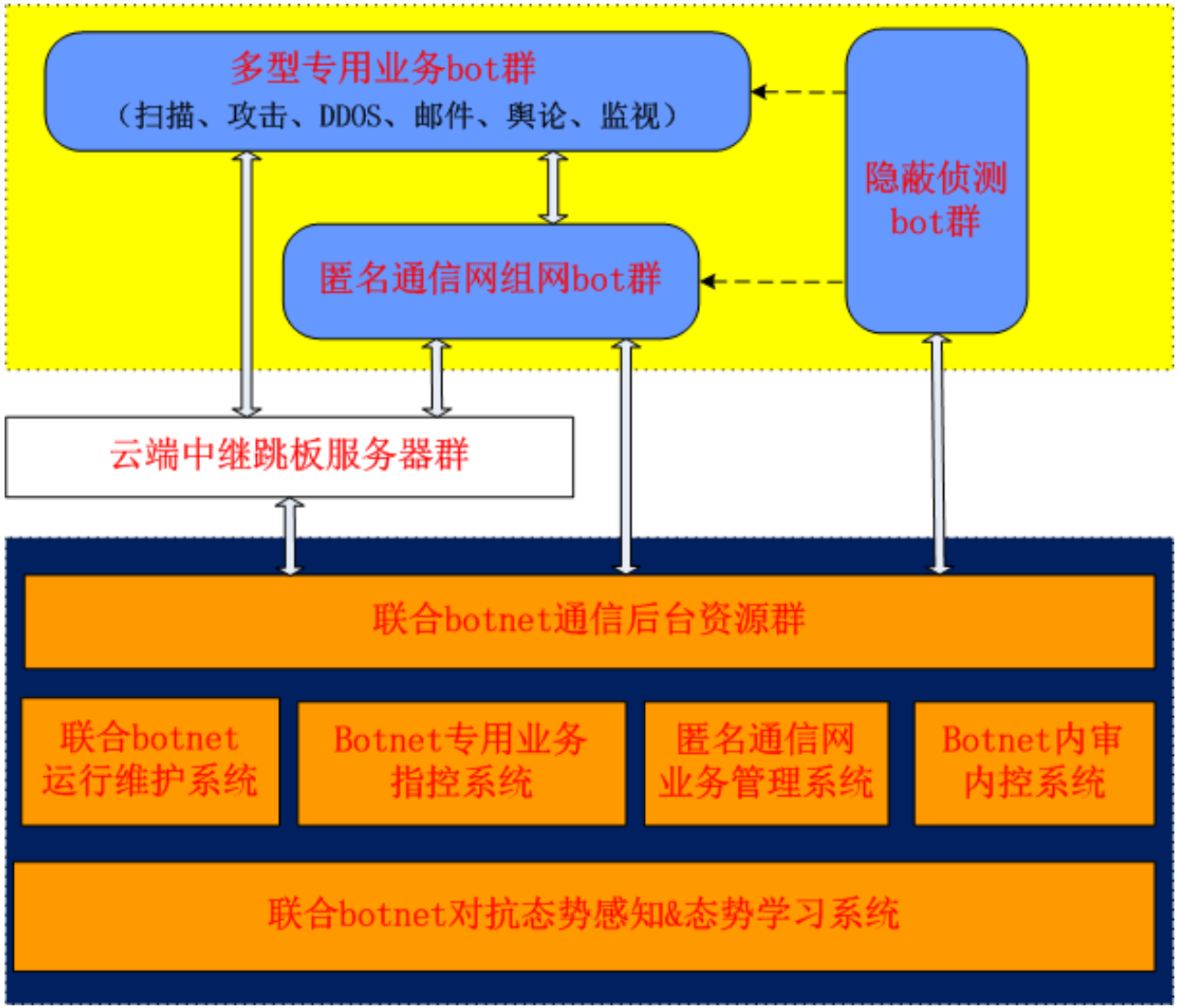
数据挖掘分析



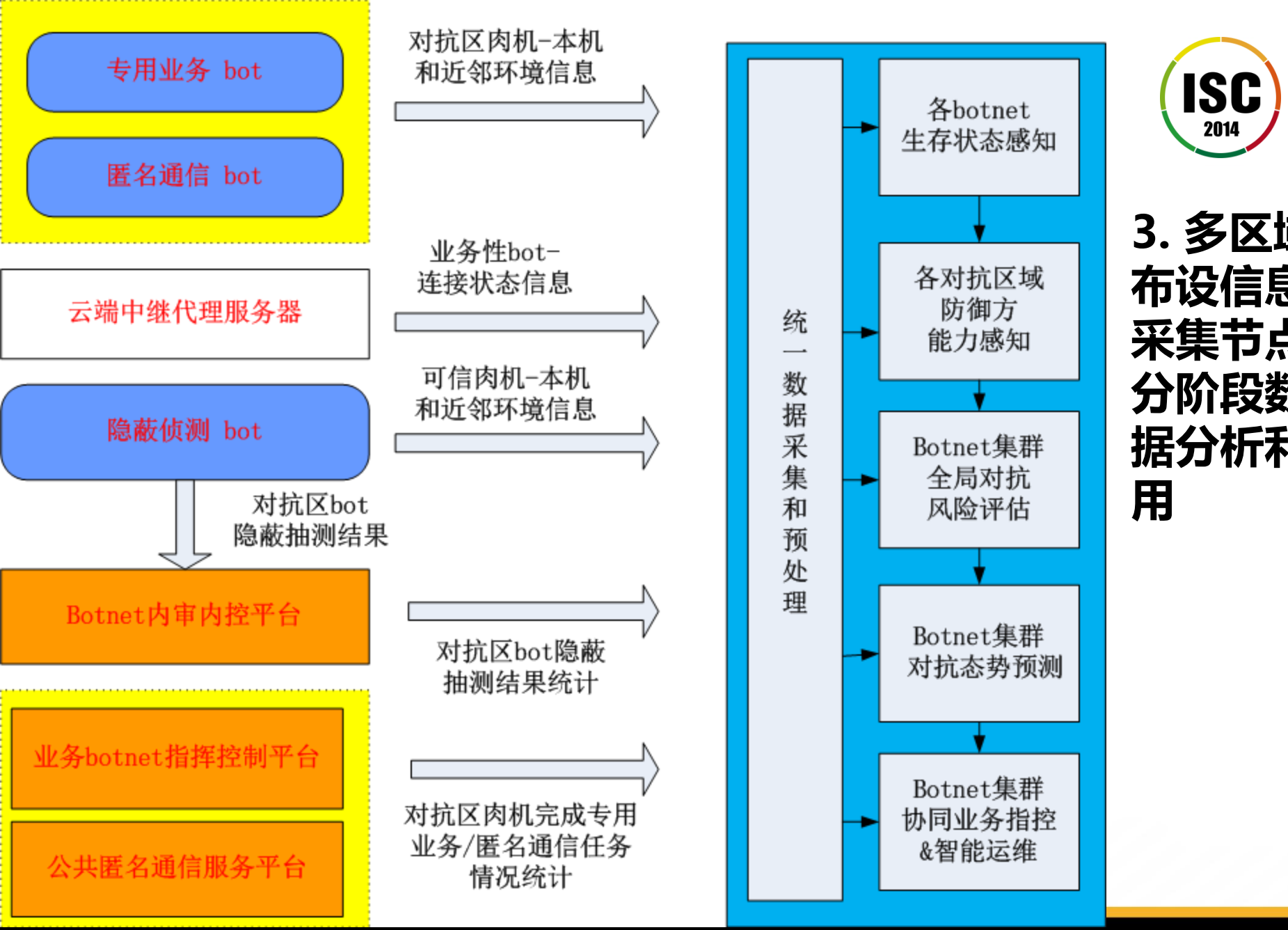
近实时botnet
全维数据采集

数据化管控和指挥

1. 利用四维度数据情报采集和分析增强botnet感知



2. 建设“业务、运维、内审内控、数据分析”四系统分离的botnet一体化指挥平台



ISC 2014

3. 多区域布设信息采集节点，分阶段数据分析利用

获取并统计哪些数据？（1）

信息网络基本情况：
- OS、App、IP、带宽、

用户使用规律：
- 活跃上线时间、
- App使用频率、
- 常用App版本

目标区域情况普查

安全防护水平：
- 漏洞分布、
- 补丁分发频率、
- 应急响应时间、
- 深度防御强度

用户安全素质：
- 打补丁频率、
- 黑客技术普及率、
- 色情资料点击率、
- 电子商务广告点击率

获取并统计哪些数据？（2）

种植方式有效性评估：

- 0day波及范围、
- 区域有效性、
- 区域时效性、
- 方式有效性、

木马生存性评估：

- 不同类型生存率
- 不同区域生存性、
- 不同版本生存率、
- 不同通用功能模块生存率

木马对抗态势评估

获取并统计哪些数据？（3）

按区域运用资源：
- 0day、站点、域名、
- 木马类型、版本、
- 功能模块

按环境管理升级：
- 管控时段、升级包大小
- 升级区域、升级批次
- 流量特征抑制

集群木马
敏捷指挥

按目标投放木马：
- 区分特定和常规目标、
- 不同目标木马失效率、
- 目标防御强弱点、
- 预测/估计恰当升级方式

按态势推进业务：
- 投入更多模块区域、
- 可疑待人工判断区域、
- 非可靠区域不投入
- 新0day、新版本、新模块

从统计数据中提取哪些木马态势特征？

目标特征

OS；
CPU\GPU\RAM;
带宽；
漏洞存在；
内网/外网 ip；
地域/时区；
活跃时间；
钓鱼成功率；
业务价值；
主机安全软件；

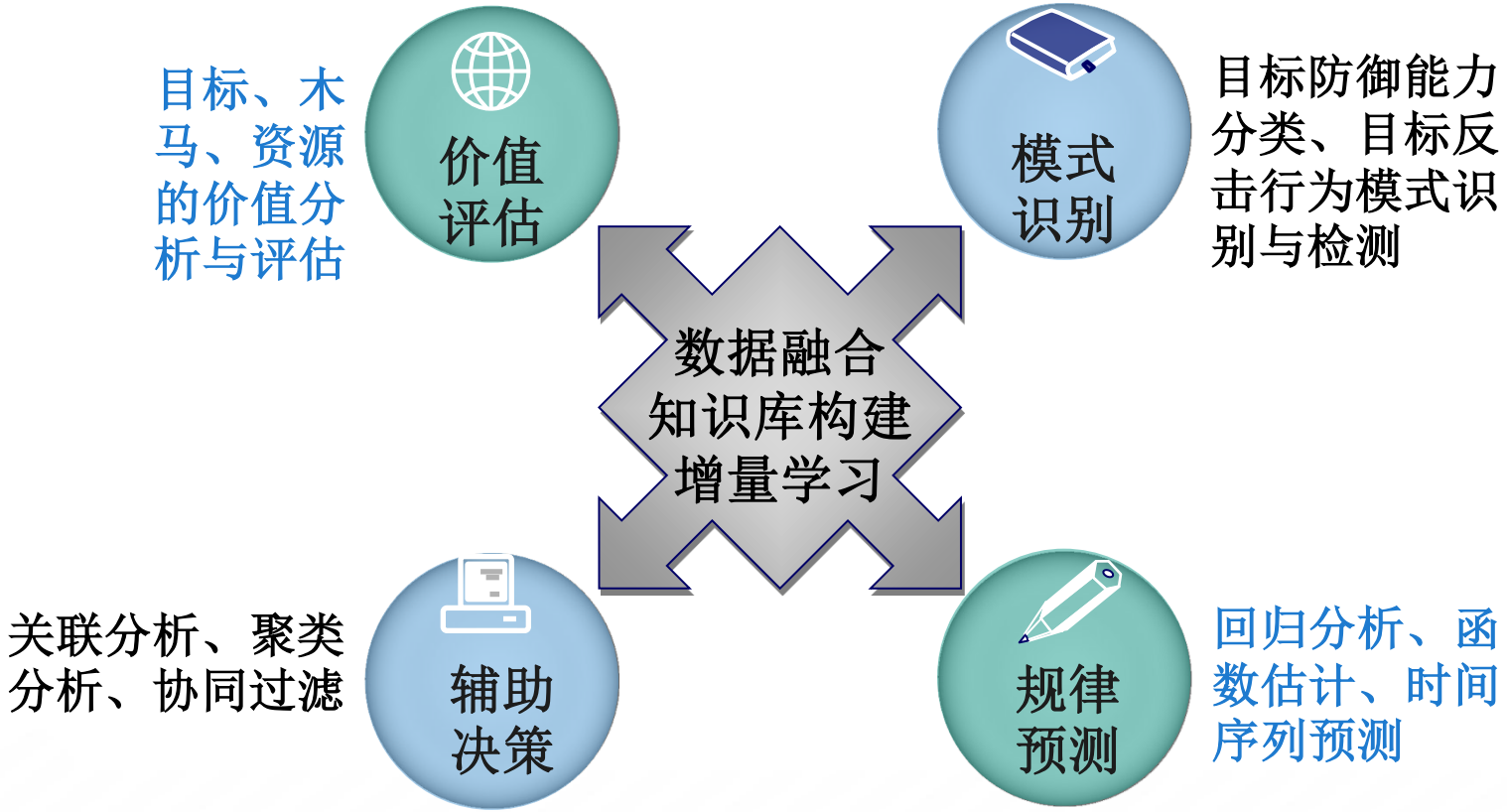
木马特征

种植渠道（email、url）；
名称/版本/语言编码；
C2类型/通信协议；
所携0day/开发库；
文件名/隐藏位置；
验证方式/密钥批次；
功能模块版本；
免杀技术/加密壳；
自启动方式；
代理跳板/（动态）域名/博客（空间）url；

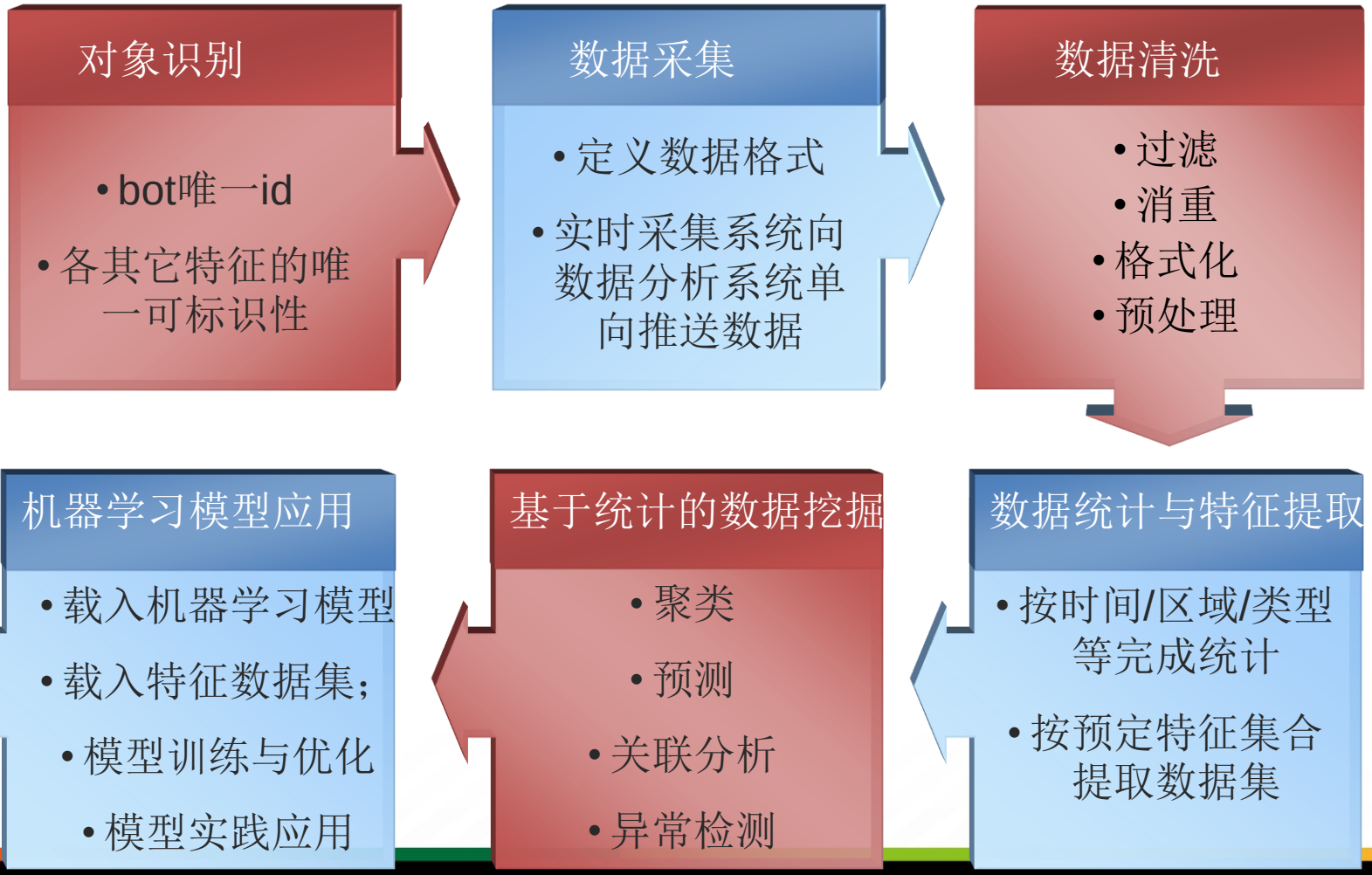
生存态势特征

木马有效模块；
木马最新在线时间；
木马总生存时间；
木马业务完成评价；
种植用email、url生存时间；
C2用代理跳板/（动态）域名/博客（空间）url生存时间；
可信/可疑目标集合；

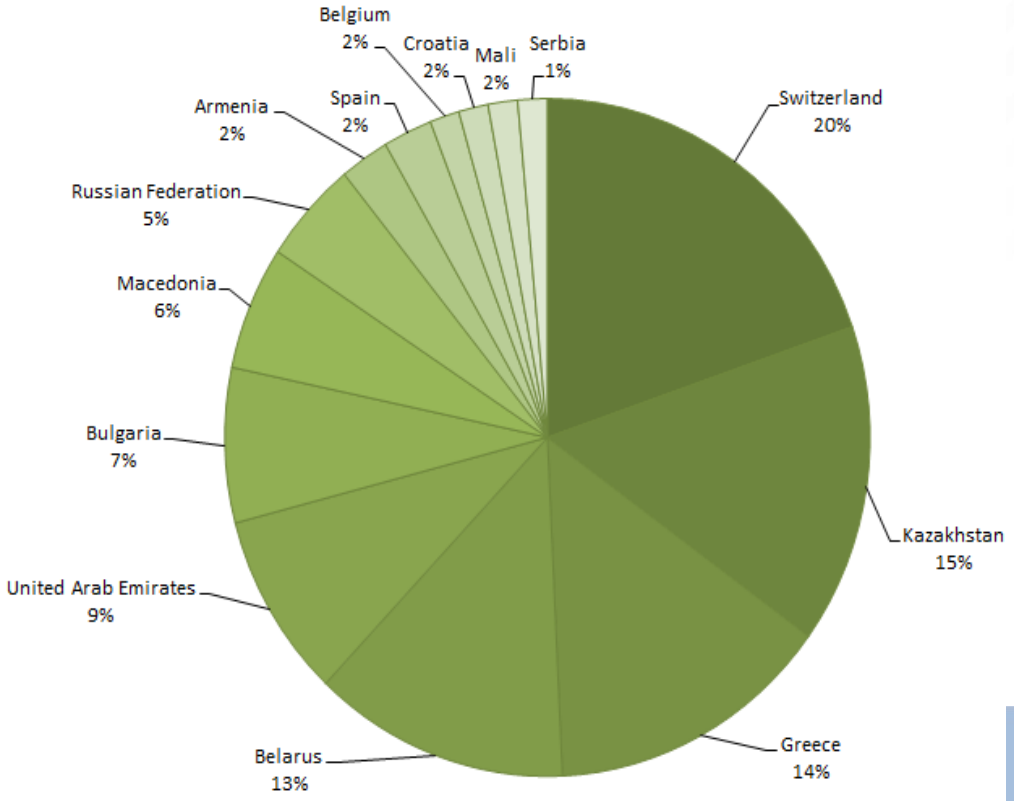
4.深度应用机器学习系统和方法（1）
----领域知识建模



4.深度应用机器学习系统和方法（2）
--从领域模型到样本学习

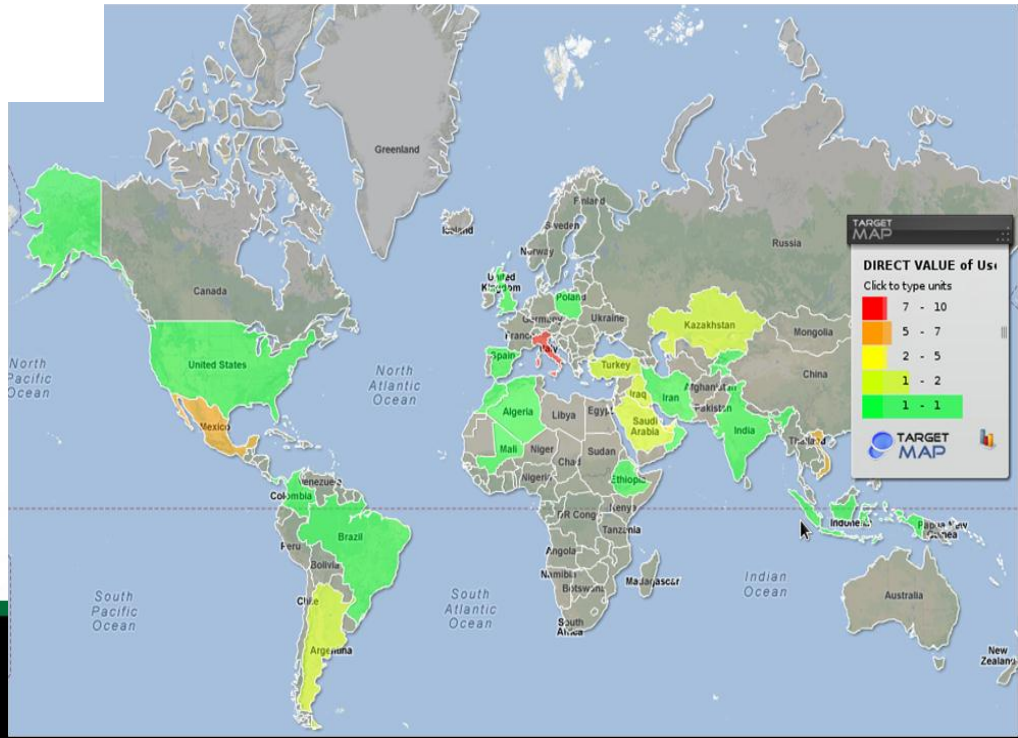


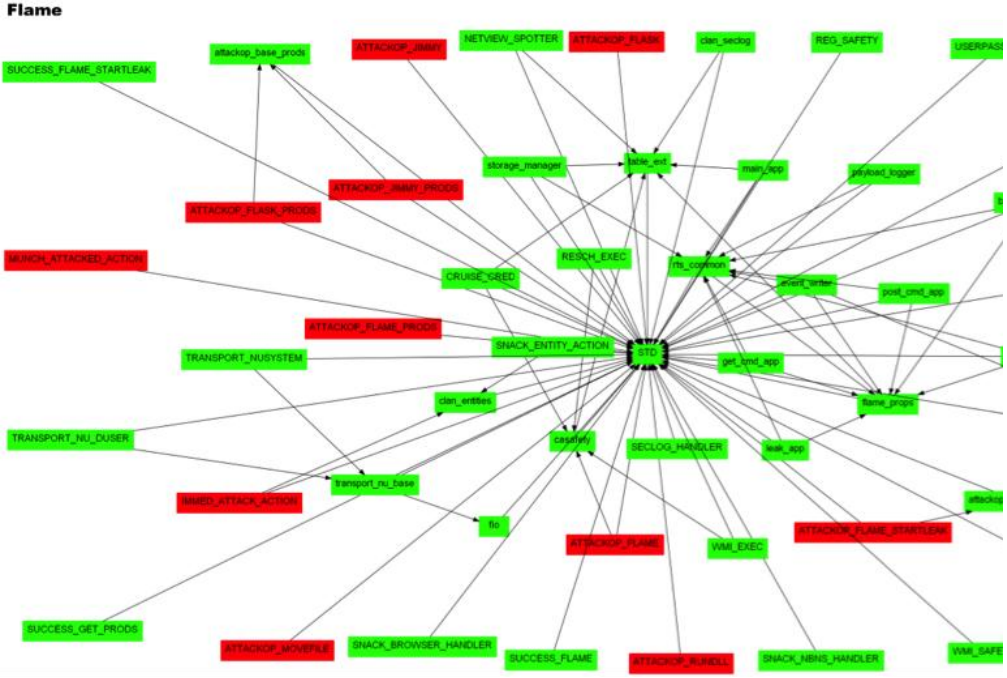
三、僵尸网络的“数据化管控”和“数据化业务指挥”

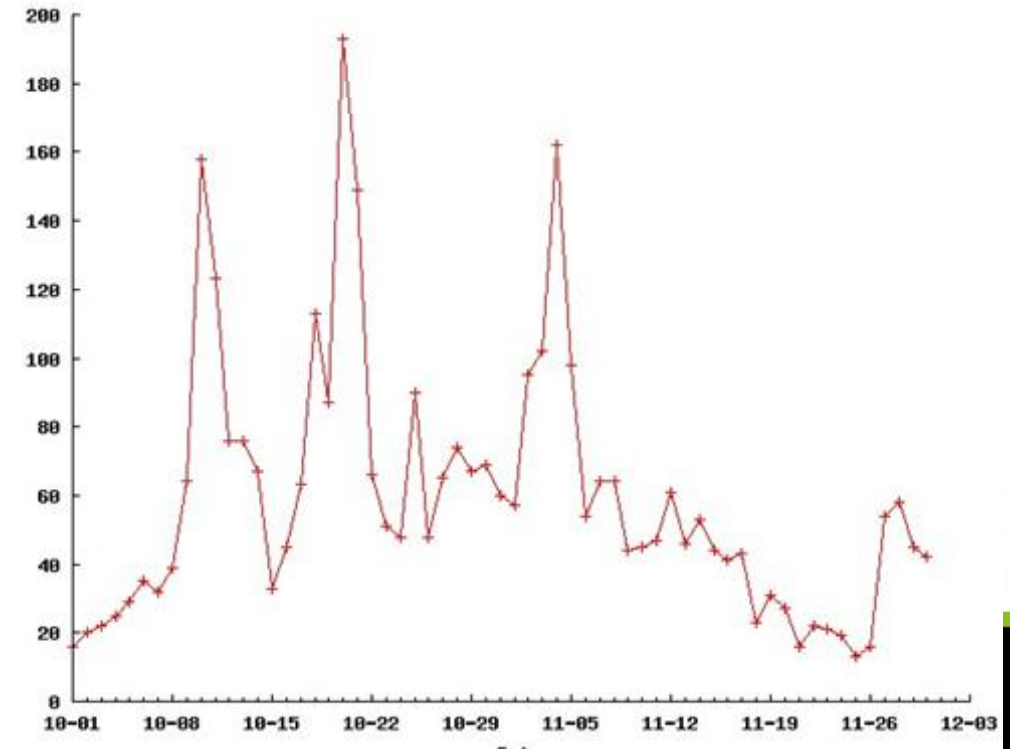


ISC 2014

场景1：基于业务成果统计的目标区域价值评估

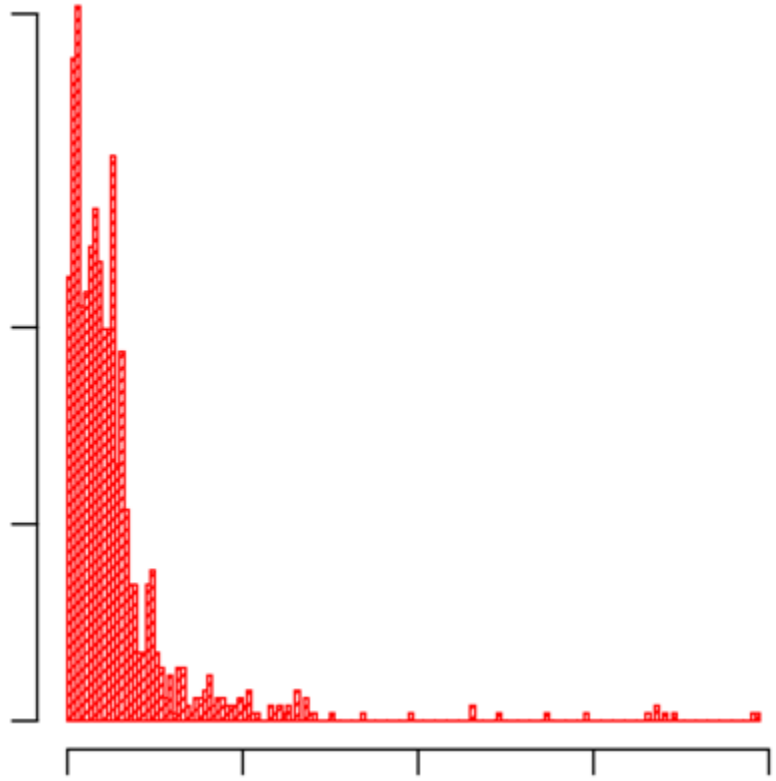






Domain	IP Resolution
bss.publicvm.com	58.64.200.105
central.swordwind.net	58.64.200.105
lwl.publicvm.com	58.64.200.105
mongolia.regionfocus.com	58.64.200.105
mongolia.swordwind.net	58.64.200.105
peaceful.linkpc.net	58.64.200.105
peaceful.publicvm.com	58.64.200.105
peaceful.swordwind.net	58.64.200.105
usa.regionfocus.com	58.64.200.105
blog.cainformations.com	58.64.200.106
bluesnow.alternate009.com	58.64.200.106
loggol.cainformations.com	58.64.200.106
module.cainformations.com	58.64.200.106
mongol1.mine.nu	58.64.200.106
mongolia.regionfocus.com	58.64.200.106
newsgdeep.alternate009.com	58.64.200.106
nuyoahz.alternate009.com	58.64.200.106
oayoahzfks.alternate009.com	58.64.200.106
peaceful.linkpc.net	58.64.200.106
peaceful.publicvm.com	58.64.200.106
transfer.cainformations.com	58.64.200.106
usa.regionfocus.com	58.64.200.106
wing.alternate009.com	58.64.200.106

场景2：基于bot生存率统计的单个资源（域名）可用性评估



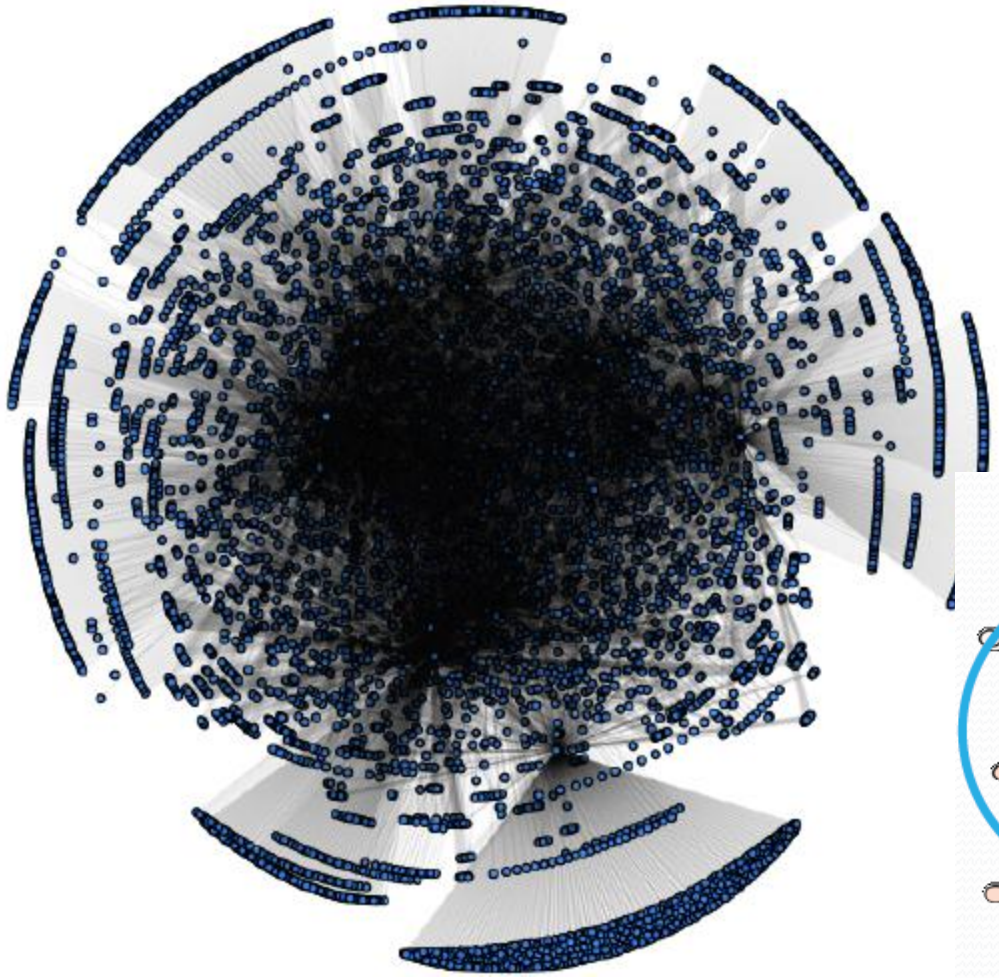
редактирование customconnector.dll.cfg - Far 2.0.1807 x86 Администр

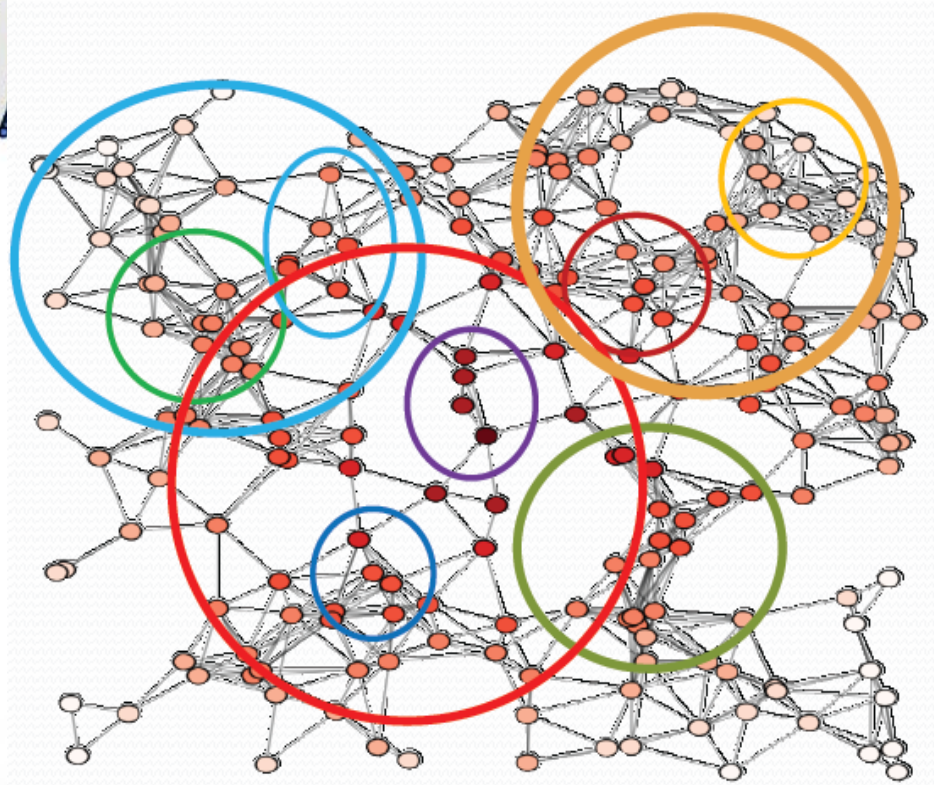
```
:\...tomconnector\customconnector.dll.cfg     1251
ttp://ma        rt.com/~brbrabr00/gate.php;1200
ttp://21        .11/~anter/~brbrabr00/gate.php;1200
ttp://ma        rt.com/~brbrabr00/gate.php;1200
ttp://ma        rt.com/~brbrabr00/gate.php;1200
```

Source Function	Destination Port *	Protocol/ Technology *	Destination Function
Bots	HTTPS (443)	SSH	Bot relay → Bot proxy
Bot proxy	HTTPS (443)	VPN/SSH	C & C
C & C	HTTPS (443)	VPN/SSH	C & C proxy
C & C proxy	HTTPS (443)	SSH	Bot proxy
Bot proxy	HTTPS (443)	SSH	Bot relay → Bots (minions)
Master(s)	HTTPS (443)	VPN/SSH	C & C
Bots	25, 587	SMTP	Email servers (spam)
Bot	[randomize]	DNS	[loopback]
Host	53	DNS	Internal DNS server(s)

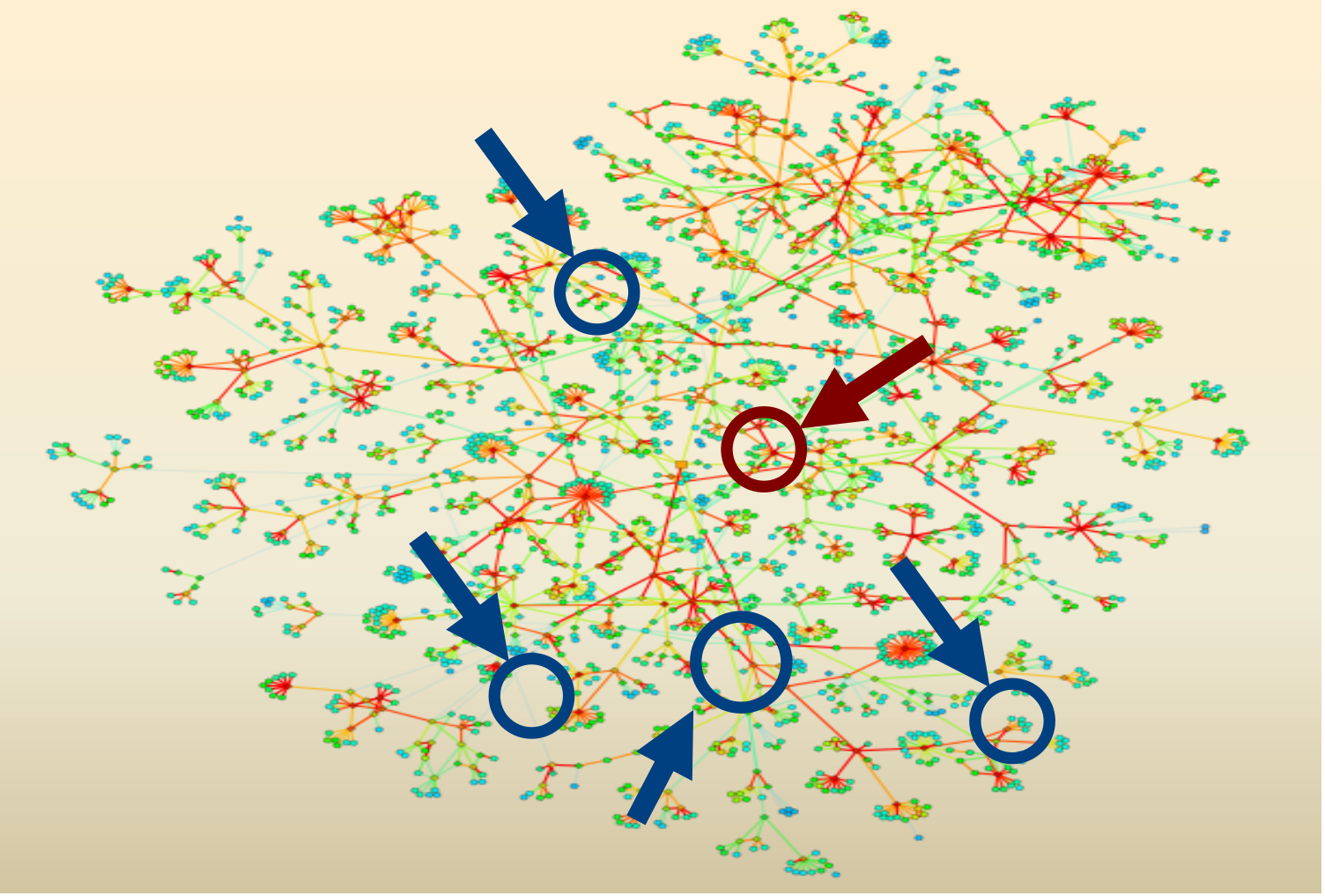
```
0008eb00  32 32 38 00 ff ff ff ff  0e 00 00 00 39 34 2e 31  |228.........94.1|
0008eb10  33 37 2e 31 36 33 2e 32  35 33 00 00 ff ff ff ff  |37.163.253......|
0008eb20  0e 00 00 00 39 35 2e 31  30 34 2e 31 32 32 2e 32  |....95.104.122.2|
0008eb30  30 31 00 00 ff ff ff ff  0d 00 00 00 39 35 2e 34  |01.........95.4|
0008eb40  33 2e 32 32 32 2e 31 39  30 00 00 00 ff ff ff ff  |3.222.190.......|
0008eb50  0d 00 00 00 37 37 2e 32  33 36 2e 31 37 36 2e 37  |....77.236.176.7|
0008eb60  30 00 00 00 ff ff ff ff  0f 00 00 00 31 37 33 2e  |0...........173.|
0008eb70  32 31 37 2e 31 37 35 2e  31 36 35 00 ff ff ff ff  |217.175.165.....|
0008eb80  0d 00 00 00 31 38 38 2e  32 33 30 2e 37 31 2e 32  |....188.230.71.2|
0008eb90  32 00 00 00 ff ff ff ff  0d 00 00 00 39 33 2e 31  |2...........93.1|
0008eba0  32 36 2e 38 37 2e 31 34  38 00 00 00 ff ff ff ff  |26.87.148.......|
0008ebb0  0e 00 00 00 31 37 38 2e  32 30 35 2e 35 30 2e 32  |....178.205.50.2|
0008ebc0  35 35 00 00 ff ff ff ff  0d 00 00 00 37 38 2e 36  |55..........78.6|
0008ebd0  32 2e 31 31 34 2e 32 33  38 00 00 00 ff ff ff ff  |2.114.238.......|
```

场景3：基于bot效能计算的最佳资源组合策略探索

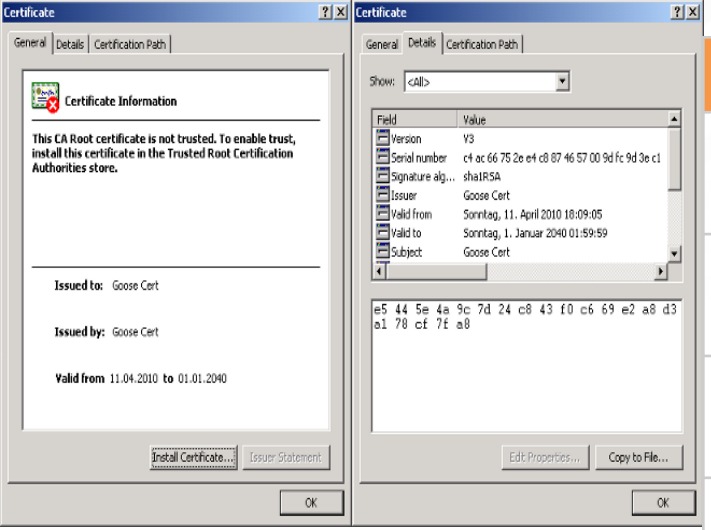




场景4：botnet组网拓扑抗毁性评估

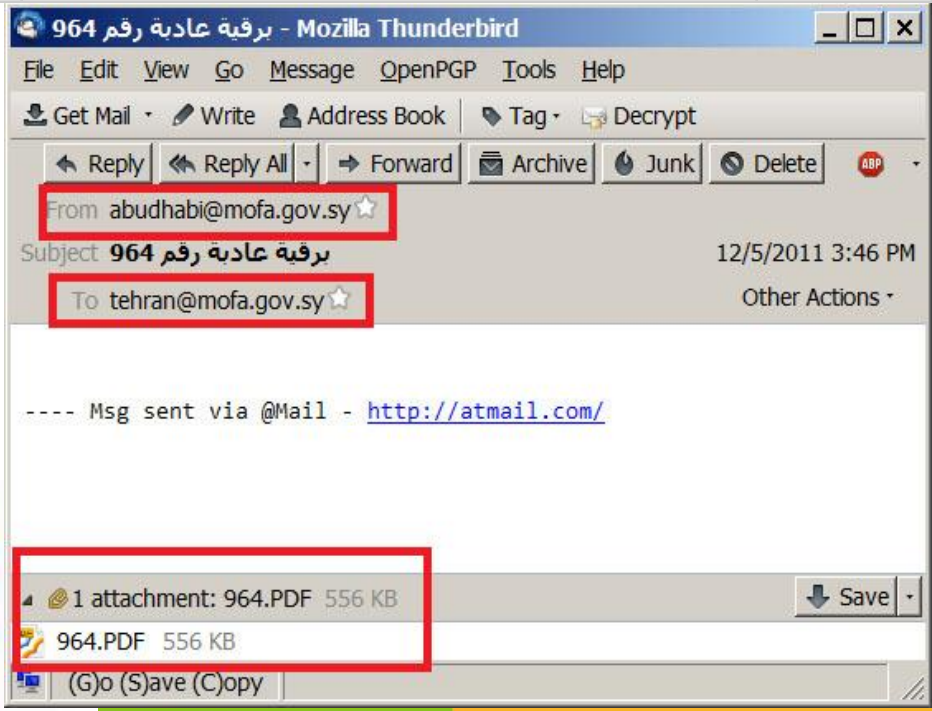


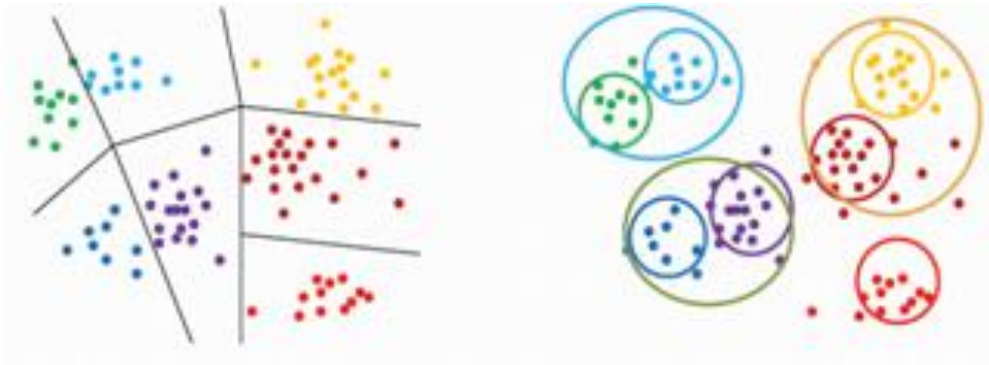
场景5：对方可能实施主动攻击的节点区域预测



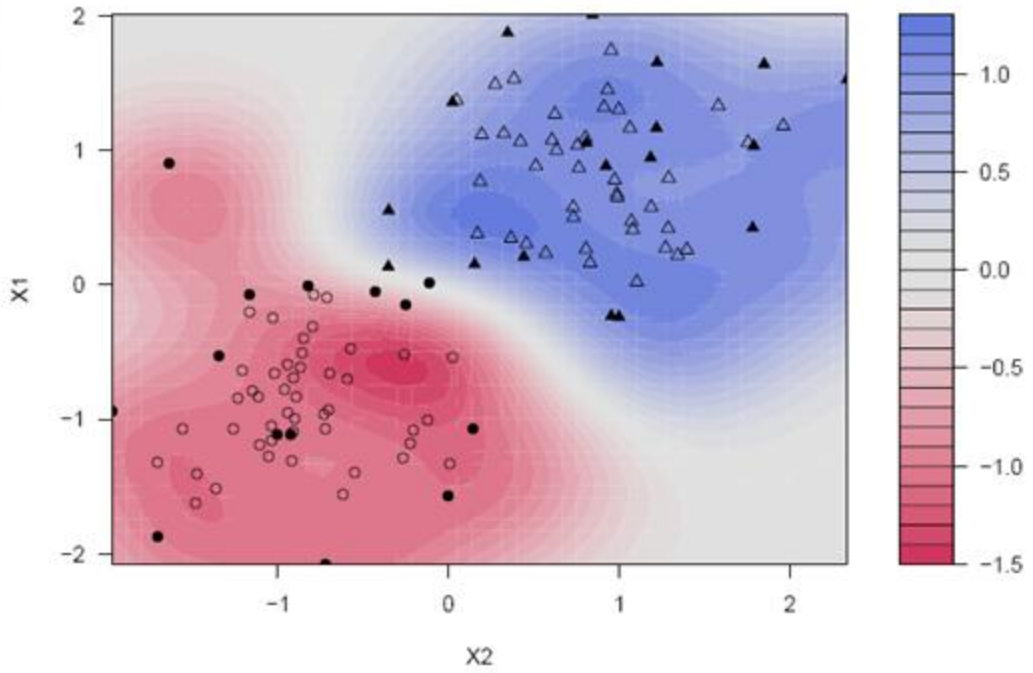
CVE	BID	Description	Discovered
2012-1875	53847	Microsoft Internet Explorer CVE-2012-1875 Same ID Property Remote Code Execution Vulnerability	May 2012
2012-1889	53934	Microsoft XML Core Services CVE-2012-1889 Remote Code Execution Vulnerability	Jun 2012
2012-4969	55562	Microsoft Internet Explorer Image Arrays Use-After-Free Remote Code Execution Vulnerability	Sep 2012
2012-4792	57070	Microsoft Internet Explorer 'CDwnBindInfo' Use-After-Free Remote Code Execution Vulnerability	Dec 2012

场景6：不同地域运用不同“email主题-email地址-文件0day-木马数字签名”组合策略的聚类分析：业务工作模式特征识别与混淆

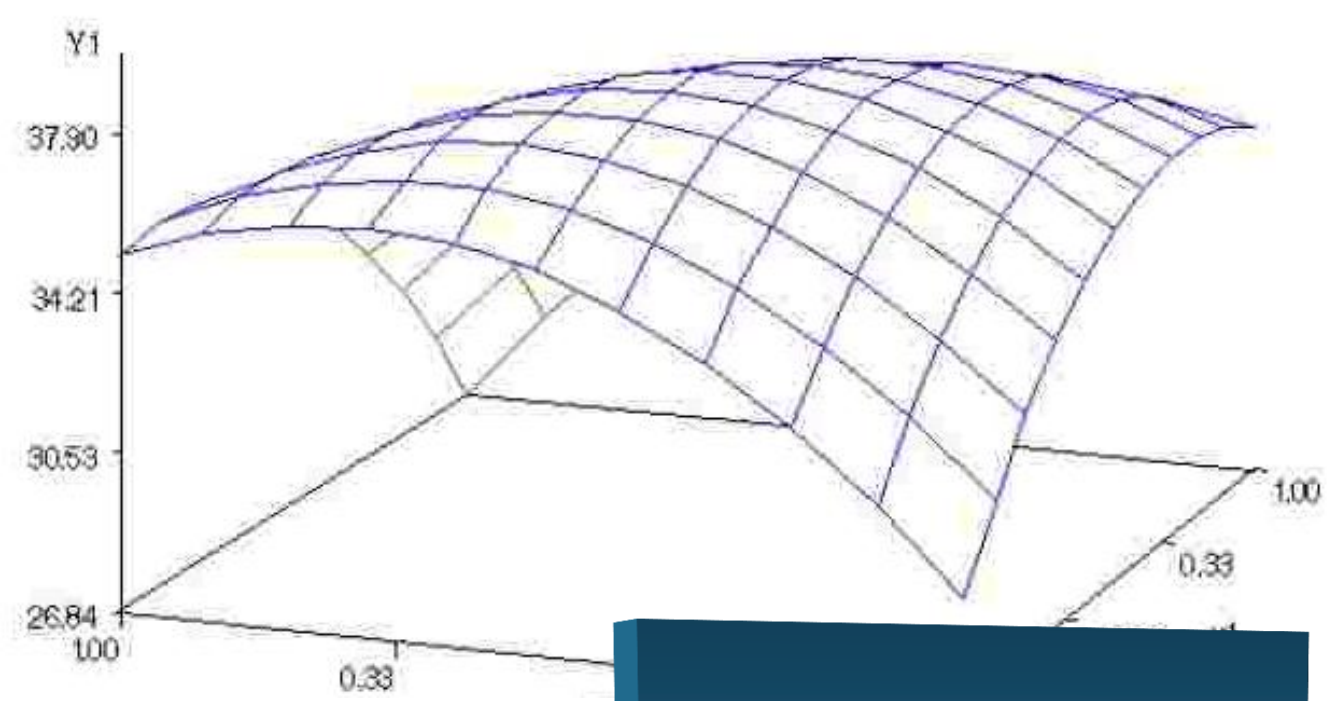




排序	可疑的sink-hole代理节点
1	al.sdflt.com
2	zh.mckueo.com
3	launcher.warcraftchina.com
4	0915.ficy.info
5	t.twilightparadox.com



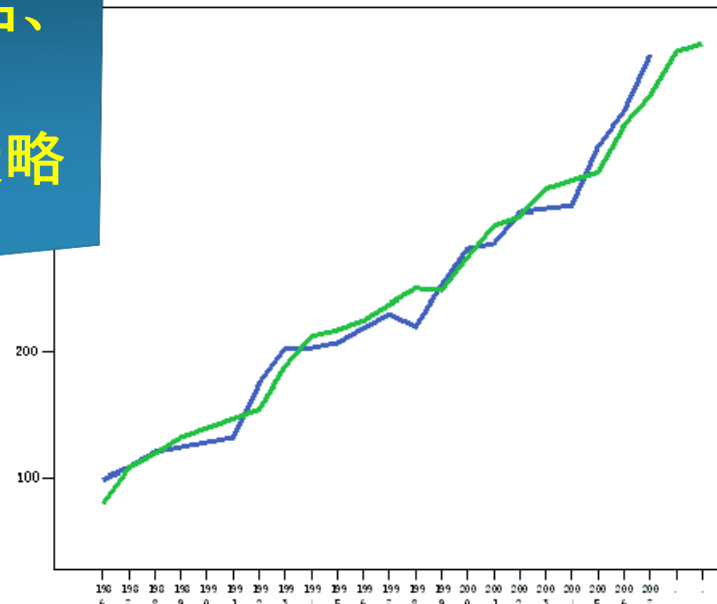
场景7：基于botnet长期监测数据的对方恶意资源识别



对抗措施综合选型：

- 0day、站点、域名、
- 木马类型、版本、
- 功能模块、升级策略

场景8：特定区域当前/未来最佳对抗策略评估选型



行者，踏雪无痕

来而不往，非礼也