ISC 2015 中国互联网安全大会

360互联网安全中心

数据驱动安全

2015 中国互联网安全大会
China Internet Security Conference

歌者之眼：国内APT事例揭秘

奇虎360 胡星儒

报告提纲

- **概述**
- 事例揭秘
- 组织分析
- 经验想法

什么是APT

一些关键词

Spear Phishing
（鱼叉式钓鱼攻击）

Targeted Malicious Email
（针对性恶意邮件）

Advanced Targeted Attacks
（高级针对性攻击）

Threat Intelligence
（威胁情报）

Cybersecurity
（网络空间安全）

Advanced Persistent Threats
（高级持续性威胁）

Watering Hole
（水坑式攻击）

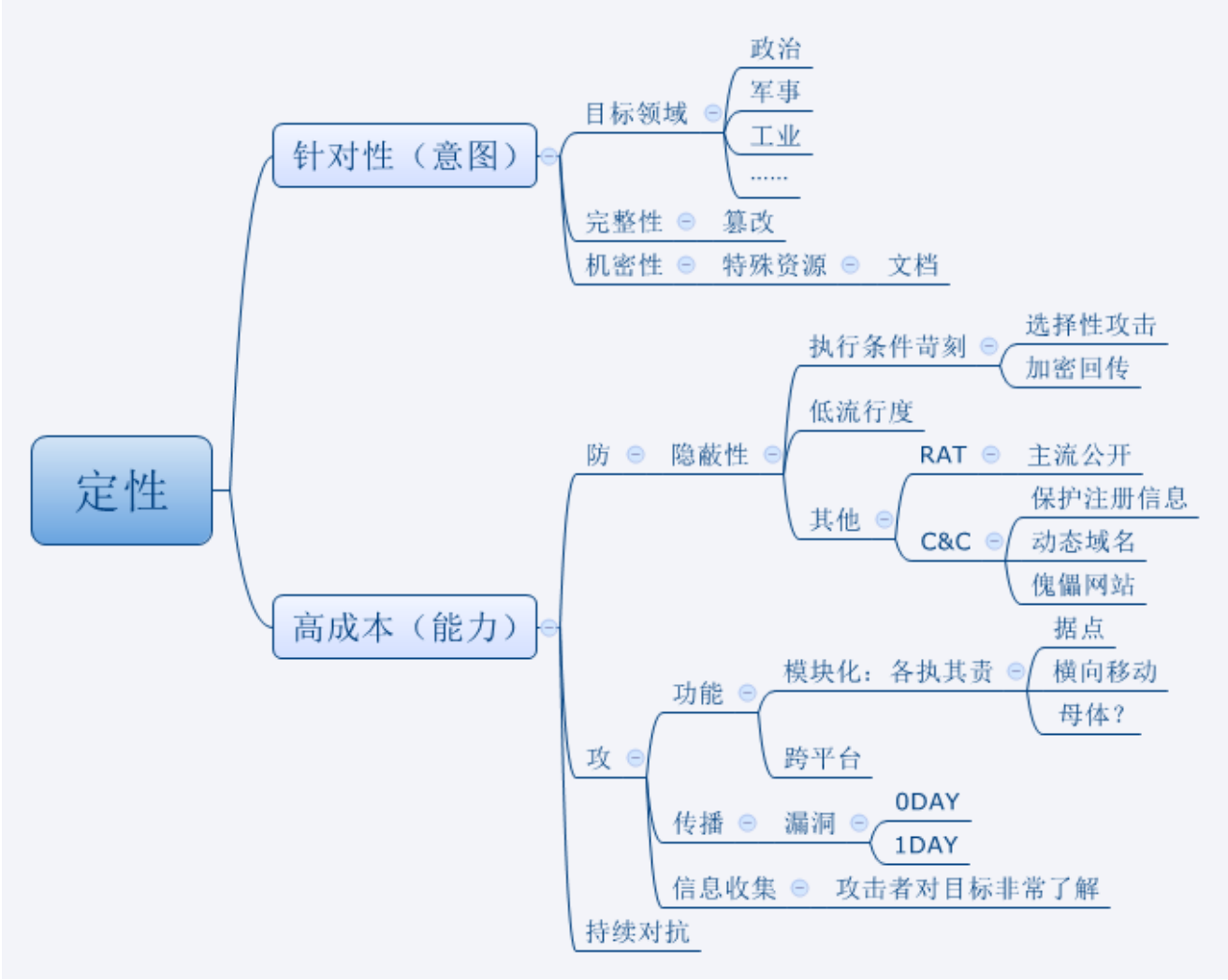
Cyber Espionage
（网络间谍）

Indicators of Compromise
（威胁指标）

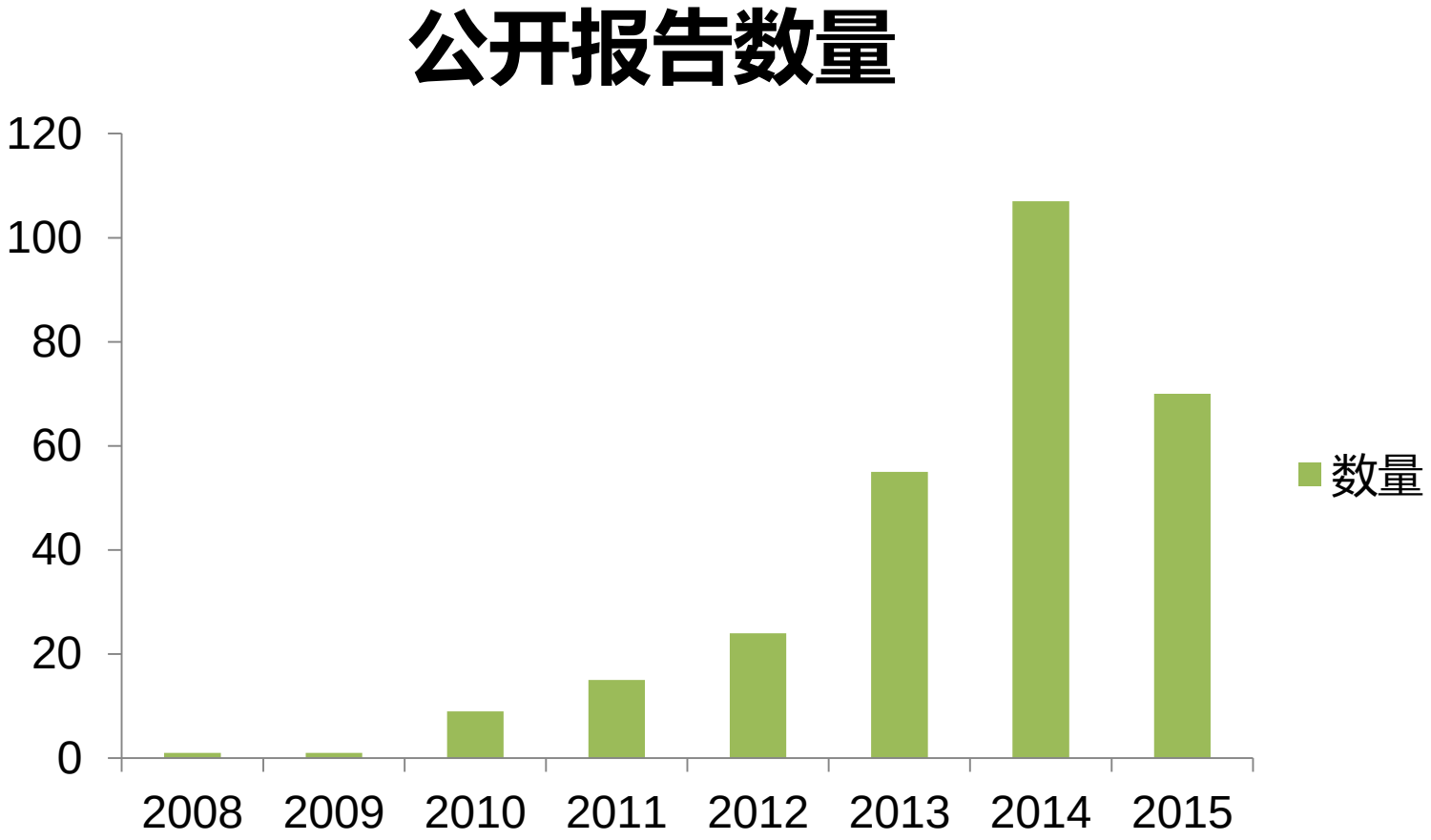
Remote Access Trojan
（远程访问木马）

Targeted Attacks
（针对性攻击、定向攻击）

什么是APT


定性
针对性（意图）
目标领域
政治
军事
工业
……
完整性
篡改
机密性
特殊资源
文档
高成本（能力）
防
隐蔽性
执行条件苛刻
选择性攻击
加密回传
低流行度
其他
RAT
主流公开
C&C
保护注册信息
动态域名
傀儡网站
攻
功能
模块化：各执其责
据点
横向移动
母体？
跨平台
传播
漏洞
0DAY
1DAY
信息收集
攻击者对目标非常了解
持续对抗

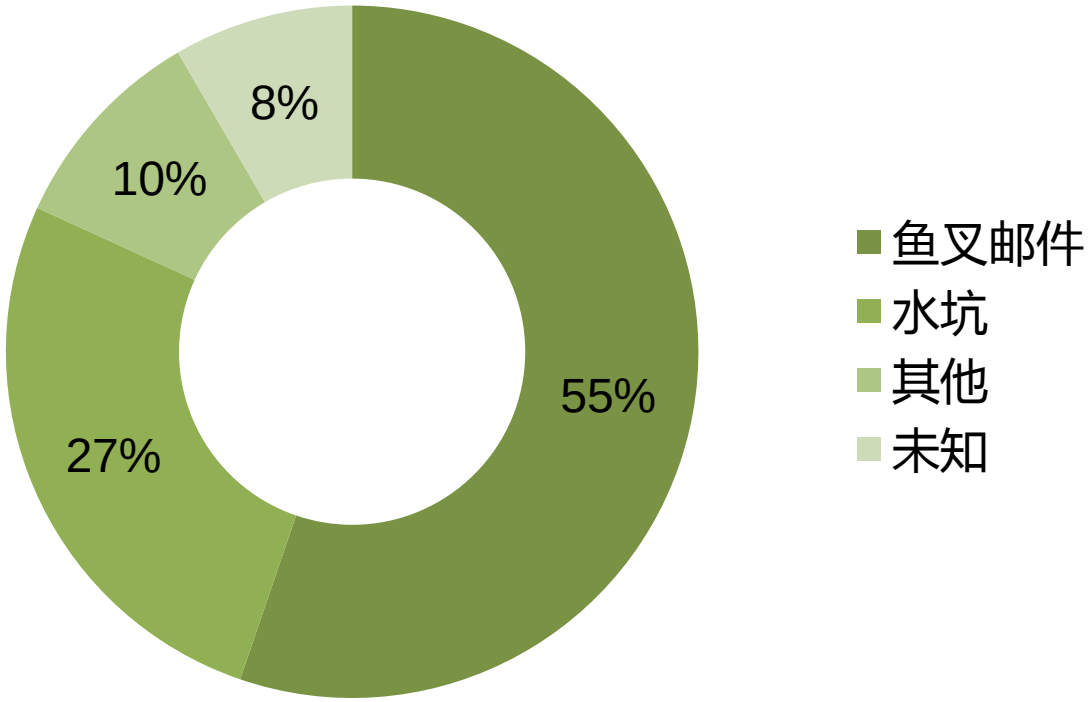
一些数据统计



注：相关数据基于第三方公开资源APTnotes，https://github.com/kbandla/APTnotes

一些数据统计

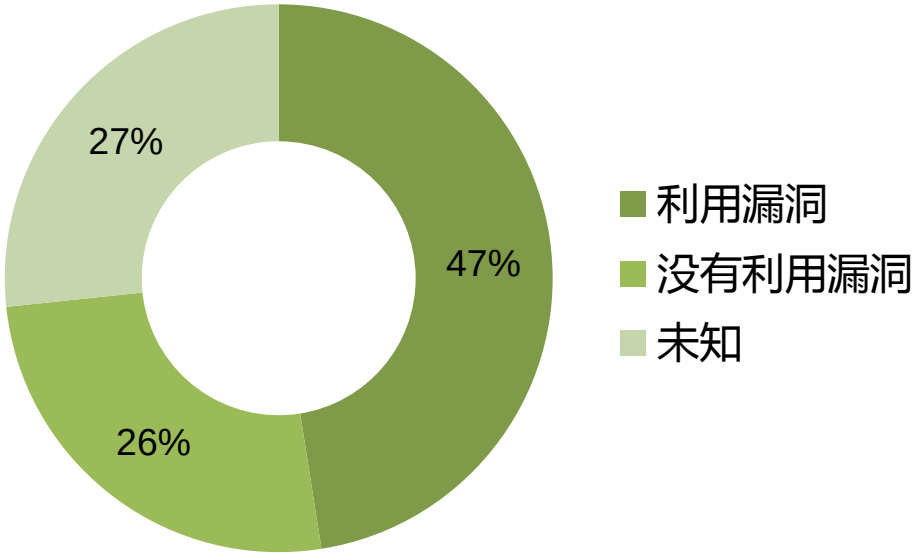
攻击方式

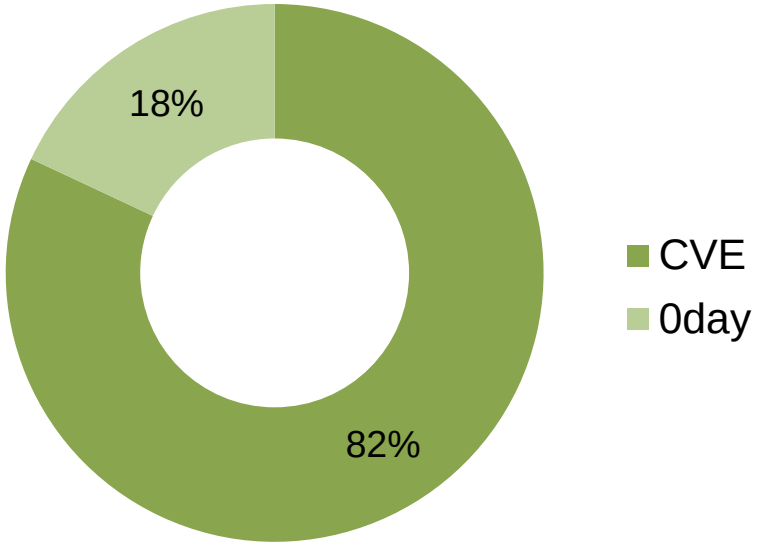


注：相关数据基于第三方公开资源APTnotes，https://github.com/kbandla/APTnotes

一些数据统计

漏洞数量





注：相关数据基于第三方公开资源APTnotes，https://github.com/kbandla/APTnotes

报告提纲

概述

事例揭秘

组织分析

经验想法

监控并发现的APT

APT活动	境内感染量	首次发现时间	最近发现时间	影响省份数	影响行业	感染方式
APT-C-00	1047	2012/4	2015/5/22	30	政府、海洋、海事	鱼叉邮件、水坑
APT-C-01	235	2014/2/15	2015/4/5	28	政府	鱼叉邮件
APT-C-04	17	2014/4/3	2014/6/29	3	科研、教育	鱼叉邮件
APT-C-02	180	2014/8/1	2015/4/14	9	教育	鱼叉邮件
APT-C-03	5	2014/11/3	2014/12/15	2	非政府组织	鱼叉邮件
APT-C-05	12	2015/2/12	2015/3/24	3	政府	鱼叉邮件
APT-C-06	4	2015/2/24	2015/3/7	3	科研	鱼叉邮件

监控到第三方披露的

APT活动	境内感染量	首次发现时间	最近发现时间	影响省份数	影响行业	感染方式
Desert_Falcon	3	2014/4/30	2015/3/3	3	教育	鱼叉邮件、水坑
GDATA_TooHash	4	2014/6/1	2014/8/31	3	科研	鱼叉邮件
Darkhotel	334	2014/6/1	2015/3/19	29	教育、能源、电信	鱼叉邮件、网络层劫持
DarkSeoul	4	2014/6/5	2015/1/5	3	电信	鱼叉邮件
Epic Turla	14	2014/6/12	2015/3/21	6	科研、教育	鱼叉邮件
NGO_Attack	6	2014/6/18	2015/3/13	6	非政府组织	鱼叉邮件
Dragonfly	2	2014/7/15	2014/8/19	1	能源	鱼叉邮件、水坑
APT28	1	2014/8/7	2014/8/7	1	航空	鱼叉邮件
Anunak	383	2014/9/28	2015/3/26	26	金融、电信、政府科研	鱼叉邮件
CARETO	1	2014/10/28	2014/10/28	1	政府	鱼叉邮件
XSLCmd_OSX	1	2014/10/30	2014/10/30	1	金融	鱼叉邮件
Waterbug	1	2014/12/31	2014/12/31	1	政府	鱼叉邮件、水坑
Snake	1	2015/2/15	2015/2/15	1	金融	U盘
Equation	1	2015/4/16	2015/4/16	1	军工	U盘

回顾5月海莲花

9）2015 年 3 月至今，OceanLotus 针对更多中国政府直属机构发起攻击。

通过对 OceanLotus 组织数年活动情况的跟踪与取证，我们已经确认了大量的受害者。下图为 2014 年 2 月至今，全球每月感染 OceanLotus 特种木马的电脑数量趋势分布。

从地域分布上看，OceanLotus 特种木马的境内感染者占全球感染总量的 92.3%。而在境内感染者中，北京地区最多，占 22.7%，天津次之，为 15.5%。

第二章　OceanLotus 攻击手法

一、　攻击手法概述

OceanLotus 主要使用两类攻击手法，一类是鱼叉攻击，一类是水坑攻击。

鱼叉攻击（Spear Phishing）是针对特定组织的网络欺诈行为，目的是不通过授权访问机密数据，最常见的方法是将木马程序作为电子邮件的附件发送给特定的攻击目标，并诱使目标打开附件。

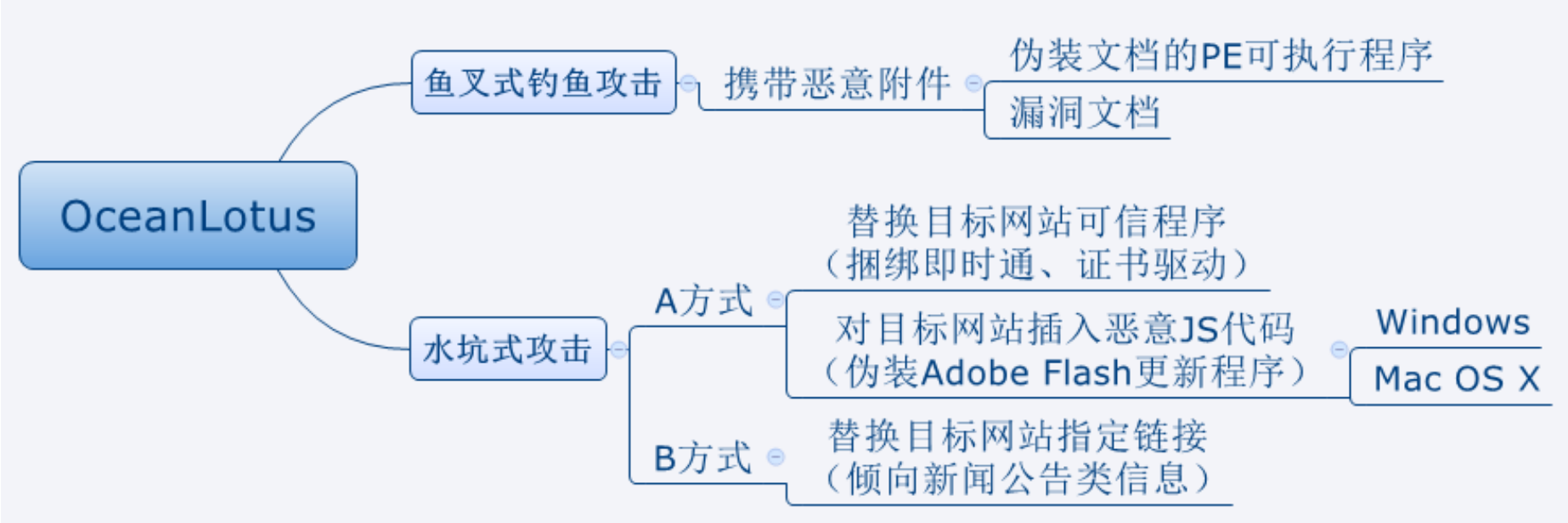
水坑攻击（Water Holing）是指黑客通过分析攻击目标的网络活动规律，寻找攻击目标经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待攻击目标访问该网站时实施攻击。

下图给出了 OceanLotus 使用鱼叉攻击和水坑攻击的基本方法。

从目前受害者遭到攻击的情况看，鱼叉攻击占 58.6%，水坑攻击占 41.4%。

抛砖引玉

由海莲花的攻击方式展开



国内APT事例揭秘

两个典型实例

H组织

- 2011年-2015年，持续4年
- 针对中国等其他国家
- 涉及政府、科研等领域

B组织

- 2007年-2015年，持续8年
- 只针对中国，涉及31个省级行政区
- 涉及政府、国防、科研、教育等领域

H组织概述

5月阶段性分析情况

描述项	具体内容
攻击时间	2014年-2015年5月
漏洞利用情况	无
是否利用0day漏洞	无
针对的国家	中国
关注的行业	政府、科研
RAT种类	4
RAT主流类型的种类	无
C&C是否有动态域名	无

意外之旅

新组织？已知组织？

```
sub_41C0600(v99, (int)&v159);
v100 = v145;
if ( !sub_41B1930(*v145) )
{
  dword_[redacted]
```

```
v80 = 0;
hObject = 0;
ThreadId = 0;
sub_100146E0(&lParam);
v87 = 0;
sub_100146E0(&v82);
```

```
v34 = 0;
v35 = 0;
v36 = 0;
operator delete(v33);
if ( v11 )
  goto LABEL_36;
sub_41C0590(v15, (int)&v29, (int)&NetworkMiner_exe, (int)&unk_41E1E70);
LOBYTE(v44) = 5;
SKIPJACK_Decode((int)&v29);
v27 = v16;
v37 = &v21;
useless3(&v29, (int)&v21);
sub_41BB850((int)&v27, v21, v22, v23, v24, v25, v26);
sub_41BB6F0((int)&v39, v27);
v17 = sub_41BD690(v39);
v18 = (int)(v39 - 8);
if ( _InterlockedDecrement((volatile signed __int32 *)v39 - 1) <= 0 )
{
  v19 = **(_DWORD **)v18;
  v27 = (const CHAR *)v18;
  (*(void (__stdcall **)(int))(v19 + 4))(v18);
}
```

```
DWORD __stdcall sub_10018060(LPVOID lpThreadParameter)
{
  HANDLE hObject; // [sp+10h] [bp-1Ch]@1

  hObject = CreateThread(0, 0, __BuildCatchObjectHelper, 0,
  if ( hObject )
    CloseHandle(hObject);
  while ( g_FindAVTools )
  {
    [redacted]_10001180() || sub_10001240() || sub
  }
  return 0;
}
```

对抗手法（结构不同）

```
v101 = *(_DWORD *)v168;
v102 = DoRemoteCommand(*v100, (int)&v163, &v159, *(int *)v168, (LPARAM)&v163)
v103 = &v134;
v103 = v102;
```

```
v71 = v64;
if ( v64 <= 0 )
  break;
v83 = 0;
```

意外之旅

答案：H组织涉及行动中的历史样本

2014\2015

2011\2012

2013

1、解密算法

```
CoInitialize(0);
ms_exc.registration.TryLevel = 0;
if ( _memicmp(lpCmdLine,
{
  sub_409740(v7);
  Filename = 0;
  memset(&v14, 0, 0x206u);
  if ( GetModuleFileNameW(0, &Filename, 0x104u) )
  {
    Buffer = 0;
    memset(&v16, 0, 0x206u);
    if ( GetTempPathW(0x104u, &Buffer) )
    {
      if ( GetTempFileNameW(&Buffer, 0, 0, &Buffer) )
      {
        if ( sub_4079C0() )
        {
          v17 = 0;
          memset(&v18, 0, 0x80u);
          v10 = 0x81;
          if ( sub_40A300(v5, &v10) )
          {
            if ( sub_40BAD0(&Buffer, &Filename) )
            {
              CommandLine = 0;
              memset(&v12, 0, 0x7FFEu);
              swprintf_s(&CommandLine,
              memset(&StartupInfo.lpReserved, 0, 0x40u);
```

```
CoInitialize(0);
v62 = 1;
v16 = (int)v23;
if ( _memicmp(v23
{
  sub_40A470(v19);
  PathName = 0;
  memset(&v35, 0, 0x206u);
  if ( GetTempPathW(0x104u, &PathName) )
  {
    if ( GetTempFileNameW(&PathName, 0, 0, &PathName) )
    {
      FileName = 0;
      memset(&v33, 0, 0x206u);
      if ( GetModuleFileNameW(0, &FileName, 0x104u) )
      {
        if ( sub_407CD0() )
        {
          v36 = 0;
          memset(&v37, 0, 0x80u);
          v23 = (void *)129;
          if ( sub_40AFF0(v17, &v23) )
          {
            if ( sub_40CEA0((int)&PathName, &FileName) )
            {
              CommandLine = 0;
              memset(&v31, 0, 0x7FFEu);
              swprintf_s(&CommandLine
              memset(&StartupInfo.lpReserved, 0, 0x40u);
```

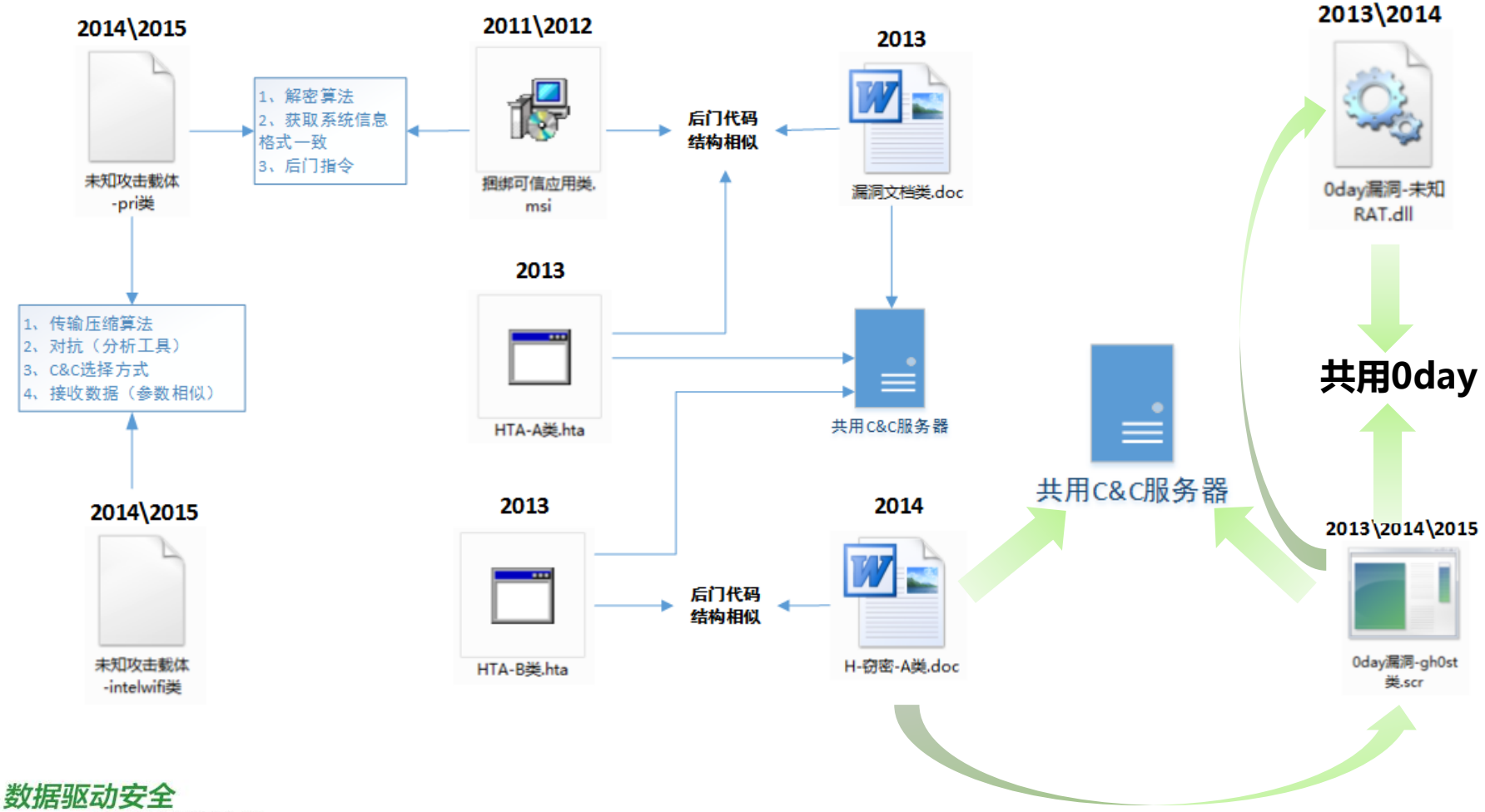
未知攻击载体
-intelwifi类

HTA-B类.hta

H-窃密-A类.doc

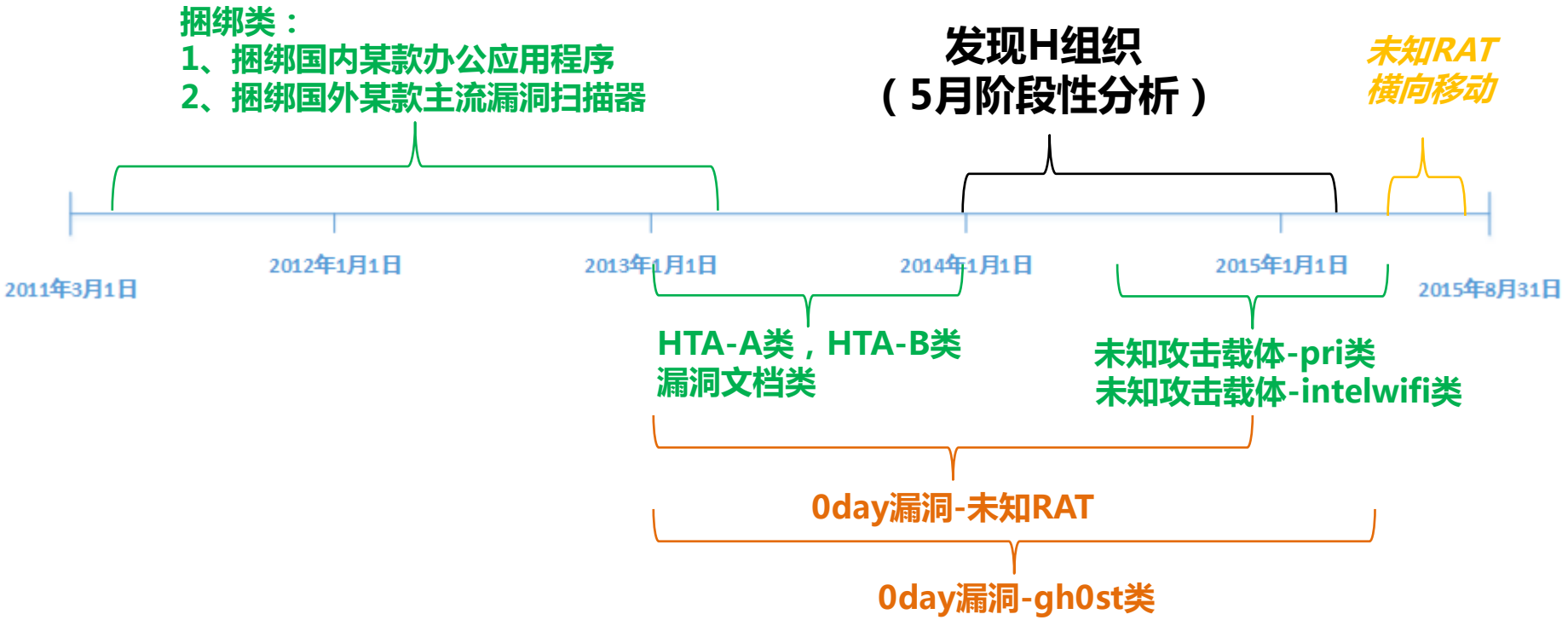
扩大战果

基于H组织样本的主动发掘



追本溯源

H组织同源样本发现过程



能力背后

海量情报数据

全球独有的样本库
- 总样本95亿
- 每天新增900万

全球唯一的主防库
- 覆盖5亿客户端
- 总日志数50000亿条
- 每天新增100亿

最大的中文漏洞库
- 总漏洞数超过40万
- 每天新增达500个

互联网域名信息库
- 50亿递归解析
- 每天新增100万

最大的存活网址库
- 每天查询300亿条
- 每天处理100亿条
- 覆盖国内96%客户端

H组织回顾

样本汇总（5月后补充）

按载体和特性划分	按功能划分（后门类型）
未知攻击载体1（Intel Wifi类）	Fake Tools
0day漏洞-未知RAT	未知RAT
0day漏洞-gh0st类	Gh0st修改版
未知攻击载体2（PRI类）	plutonium
捆绑可信应用类	
文档漏洞类	
HTA类（类型1）	
HTA类（类型2）	H-窃密-A类（5月）
H-窃密-A类	
2015未知RAT类	未知RAT

H组织回顾

相关描述

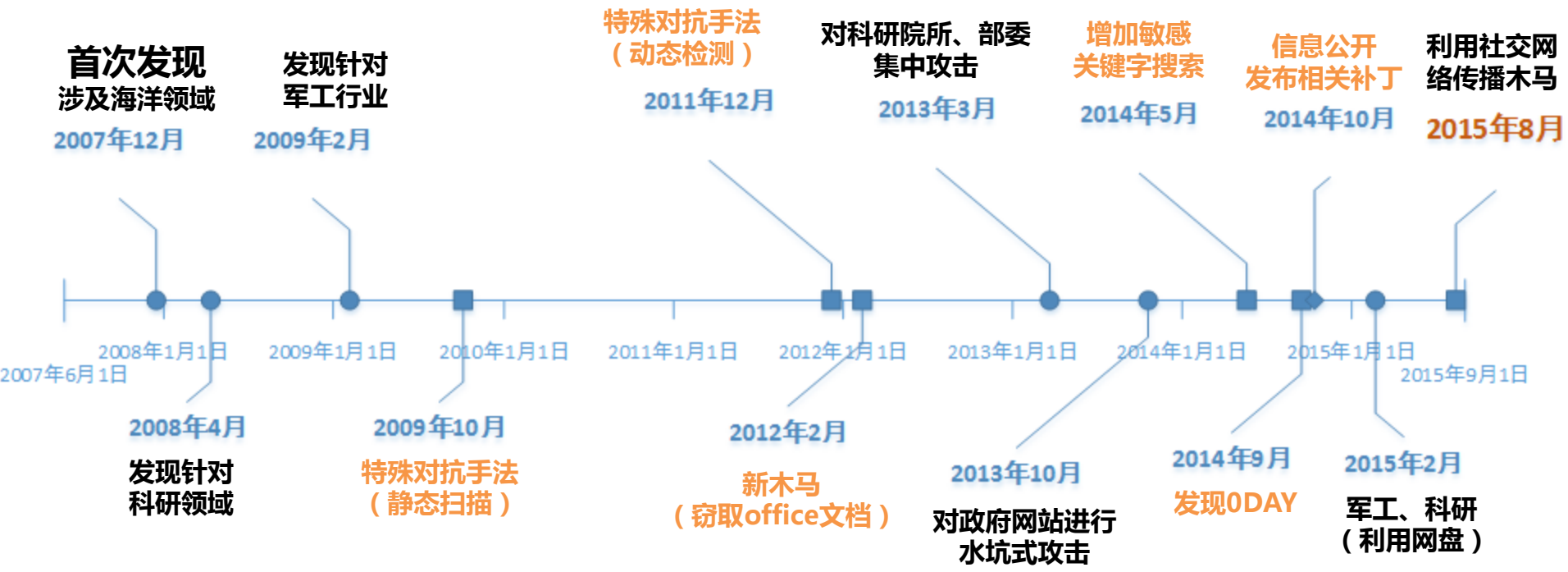
描述项	5月阶段性分析概况	后续汇总补充
攻击时间	2014年-2015年5月	2011年4月-2015年8月
漏洞利用情况	无	有
是否利用0day漏洞	无	有
针对的国家	中国	中国，其他国家
关注的行业	政府、科研	政府、科研、教育、安全等
RAT种类	4	9
RAT主流类型的种类	无	Gh0st
C&C是否有动态域名	无	有

B组织概述

组织描述

描述项	具体内容
攻击时间	2007年-2015年（至今）
漏洞利用情况	有
是否利用0day漏洞	有
针对的国家	中国，涉及31个省级行政区
关注的行业	政府、国防、科研、教育
RAT种类	13
RAT主流类型的种类	7
C&C是否有动态域名	有

持续8年的APT


首次发现
涉及海洋领域
2007年12月
发现针对
军工行业
2009年2月
特殊对抗手法
（动态检测）
2011年12月
对科研院所、部委
集中攻击
2013年3月
增加敏感
关键字搜索
2014年5月
信息公开
发布相关补丁
2014年10月
利用社交网
络传播木马
2015年8月
2007年6月1日
2008年1月1日
2009年1月1日
2010年1月1日
2011年1月1日
2012年1月1日
2013年1月1日
2014年1月1日
2015年1月1日
2015年9月1日
2008年4月
发现针对
科研领域
2009年10月
特殊对抗手法
（静态扫描）
2012年2月
新木马
（窃取office文档）
2013年10月
对政府网站进行
水坑式攻击
2014年9月
发现0DAY
2015年2月
军工、科研
（利用网盘）

13种RAT同源性分析

	开发环境	加密方法	自定义窃密函数	Shellcode	免杀对抗-静	免杀对抗-动	伪装文档等
RAT1	VC++	×	√	×	√	√	√
RAT2	VC++	√	√	√	√	√	√
RAT3	VC++	√	×	√	√	√	×
RAT4	Borland C++	√	×	×	√	×	√
RAT5	Delphi	√	×	√	√	√	×
RAT6	Borland C++	√	×	×	√	×	√
RAT7	Borland C++	×	×	×	×	×	×
RAT8	VC++	√	×	×	√	×	√
RAT9	VC++	√	√	√	√	×	√
RAT10	VC++	√	×	×	√	×	×
RAT11	VC++	√	√	√	√	×	√
RAT12	VC++	√	×	√	√	×	×
RAT13	VC++	√	√	×	√	√	√

13种RAT同源性分析

相关关联项

- 加密方式
- 自定义窃密函数
- Shellcode后门
- 子体文件名
- 免杀对抗（静态）
- 免杀对抗（动态）
- ……

能力背后

可视化分析技术

- 基于多维数据的关联，通过多种图形展现方式，构造能够帮助安全专家，对未知威胁进行分析、发现、回溯、跟踪及预警的能力

报告提纲

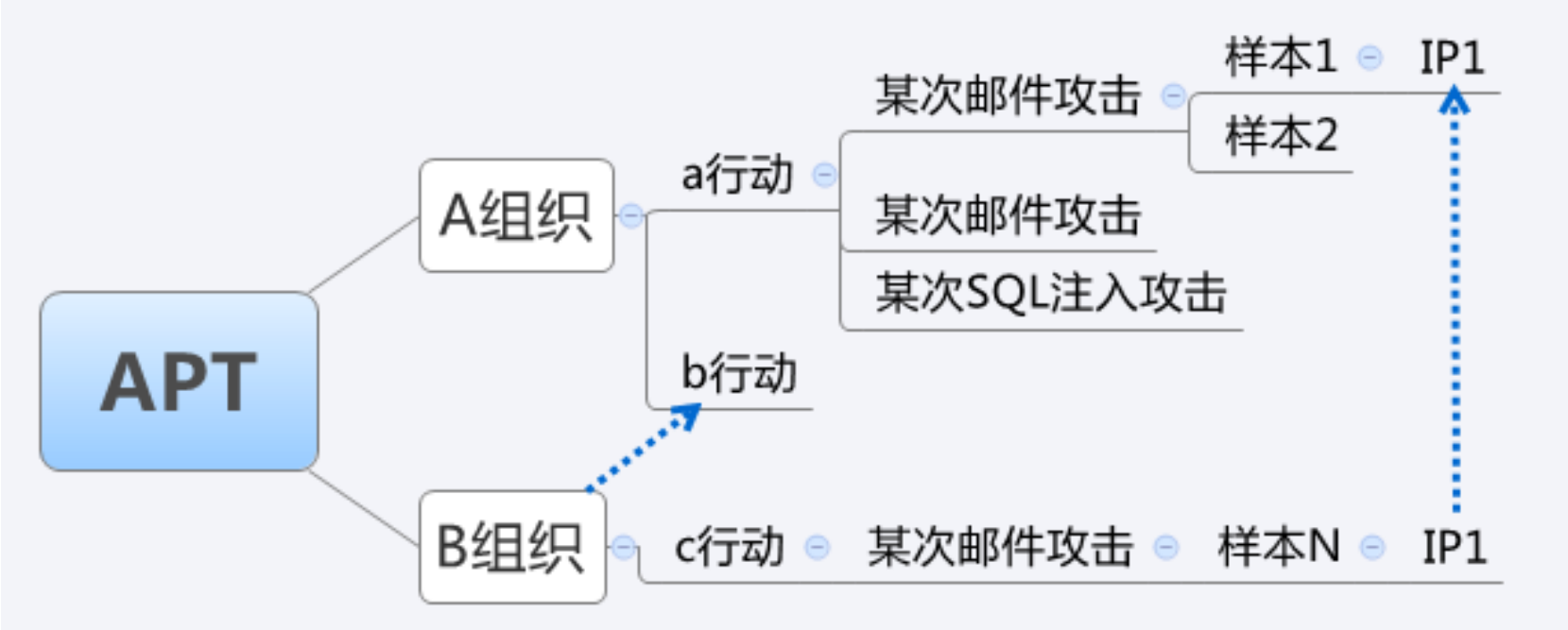
概述

事例揭秘

组织分析

经验想法

组织、行动和事件


APT
A组织
B组织
a行动
b行动
c行动
某次邮件攻击
某次邮件攻击
某次SQL注入攻击
某次邮件攻击
样本1
样本2
样本N
IP1
IP1

组织特性

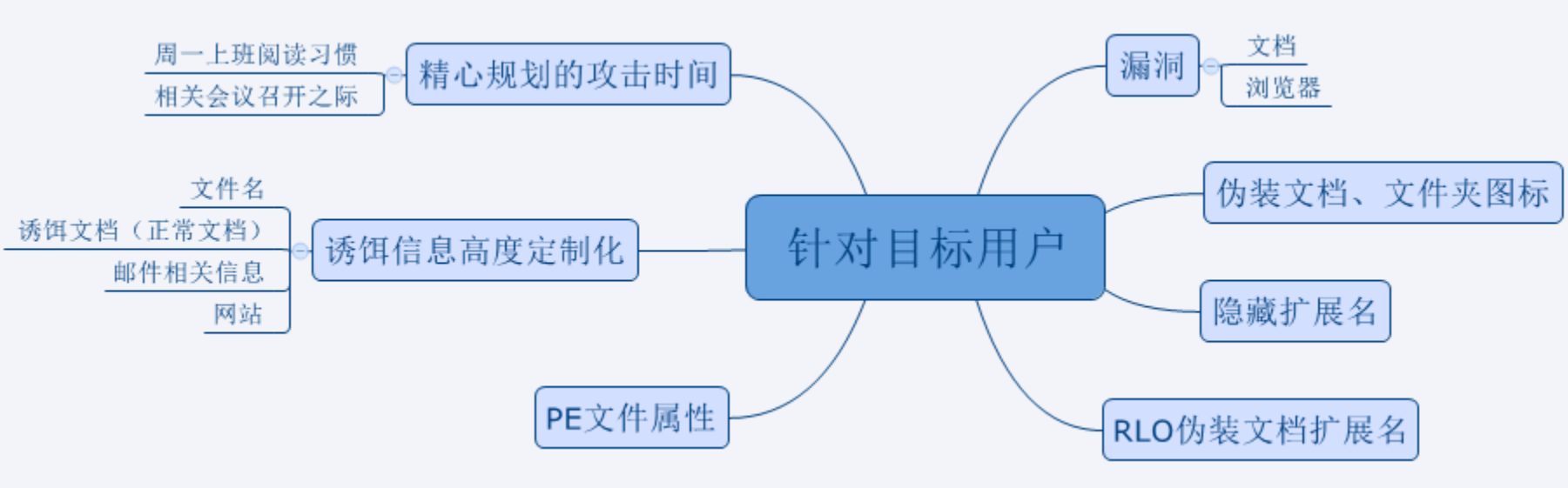
1、对抗手法-如何保证P（持续性）

- 后门选择：公开RAT、商业级别
- 文件形态：文档漏洞、伪装文档
- 攻击方式：高度定制化邮件
- 后门功能：据点、模块化、对抗
- 数据传输：可信网站、SNS、云盘

组织特性

1、对抗手法-针对目标用户

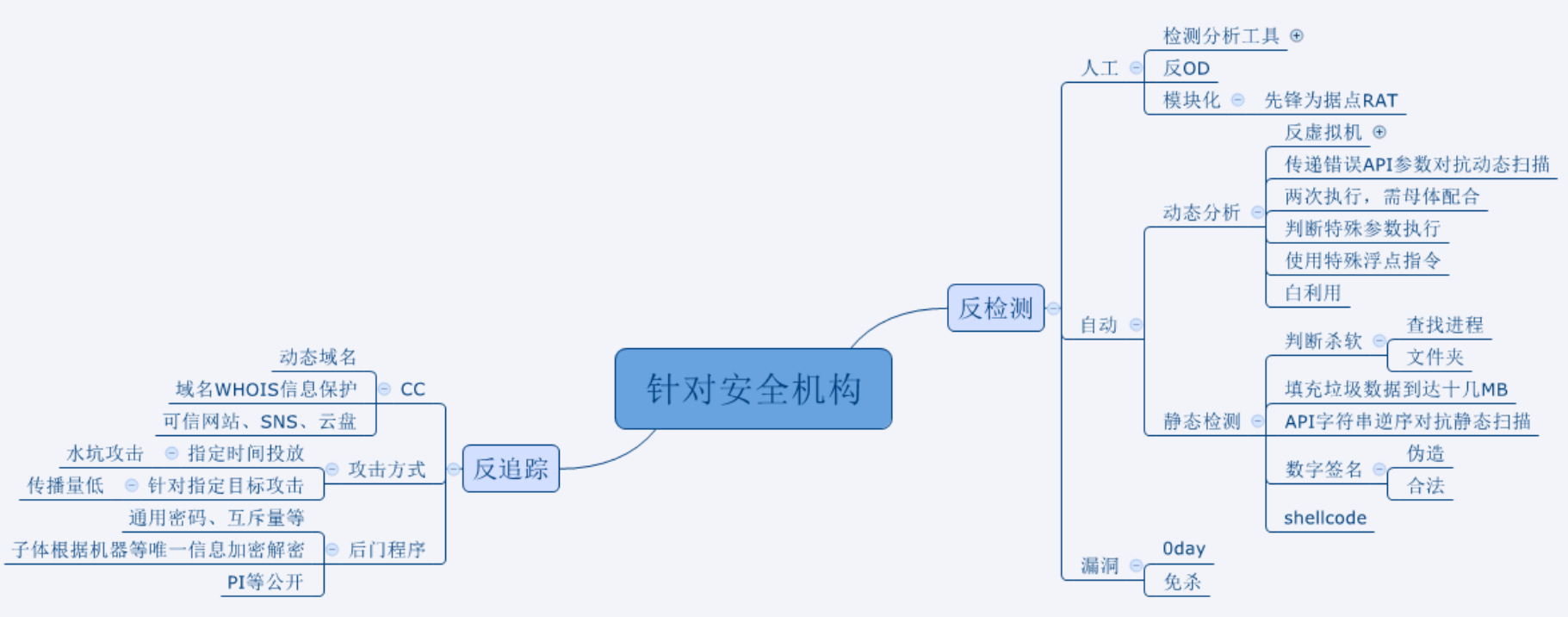
H组织和B组织相关特性



组织特性

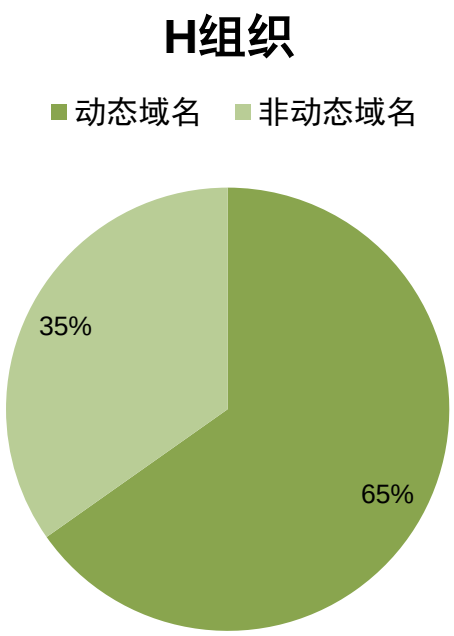
1、对抗手法-针对安全机构

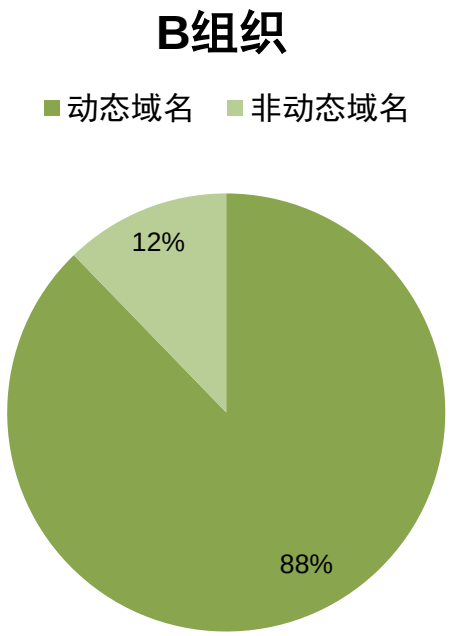
H组织和B组织相关特性

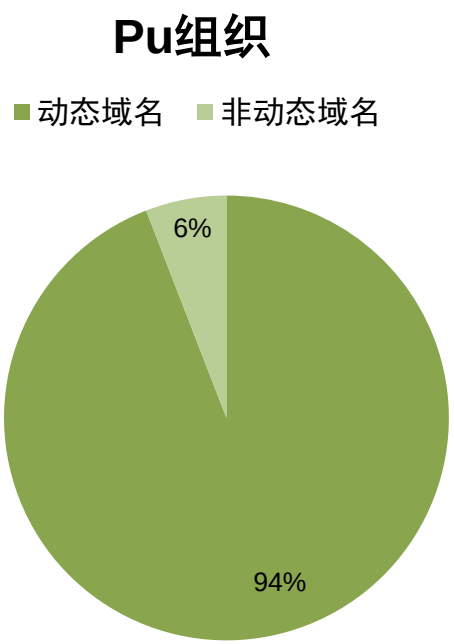


组织特性

2、C&C的使用偏好

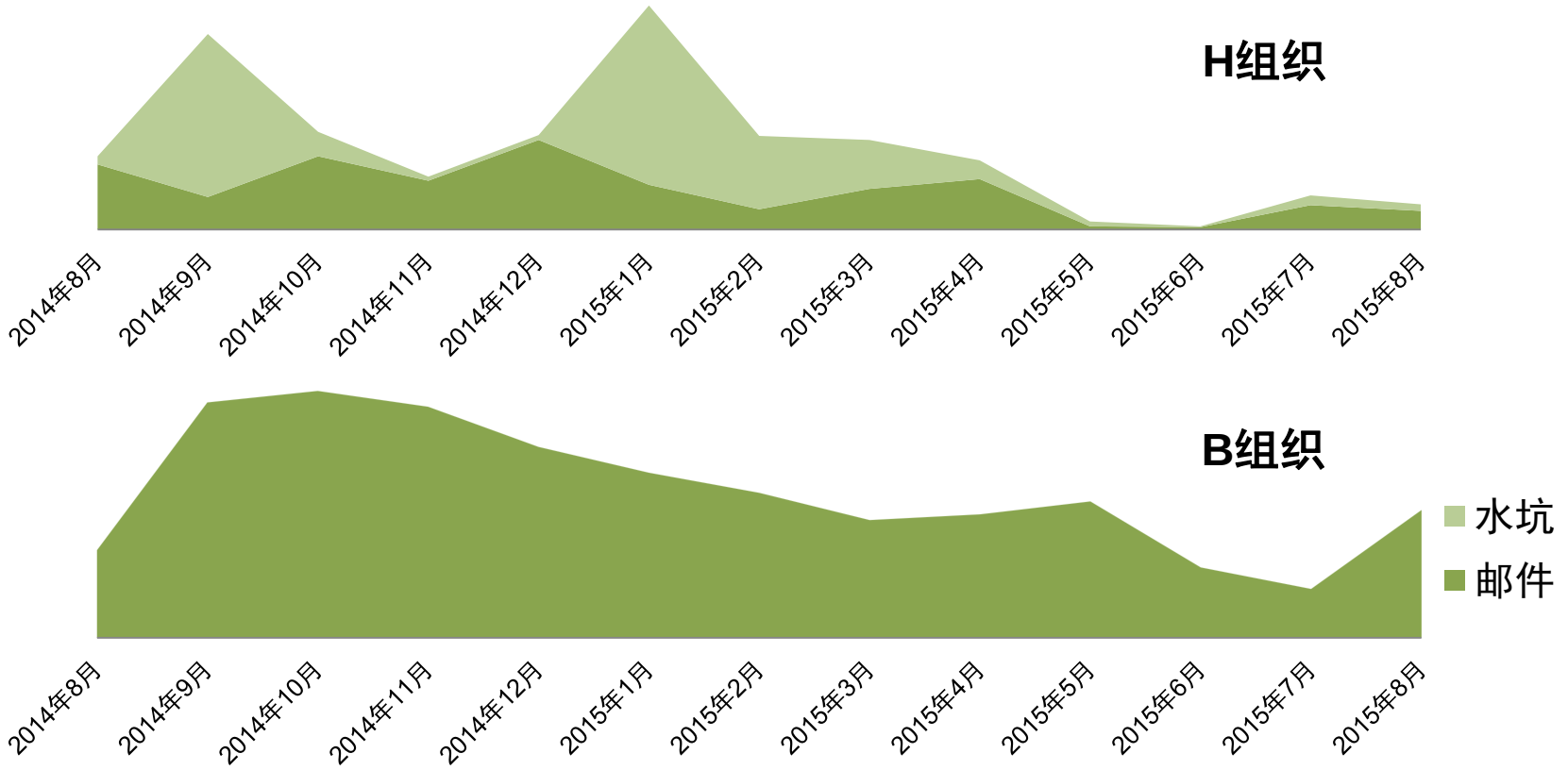






组织特性

3、攻击方式的选择



报告提纲

概述

事例揭秘

组织分析

经验想法

他山之石

基于已知事件的分析

- 发现未知新的行动、组织
- 基于已知行动、组织扩展发现未知新的行动、组织
- 基于已知行动、组织，发现其中的关联关系

国内厂商的优势是具备其他境外厂商不具备的国内资源

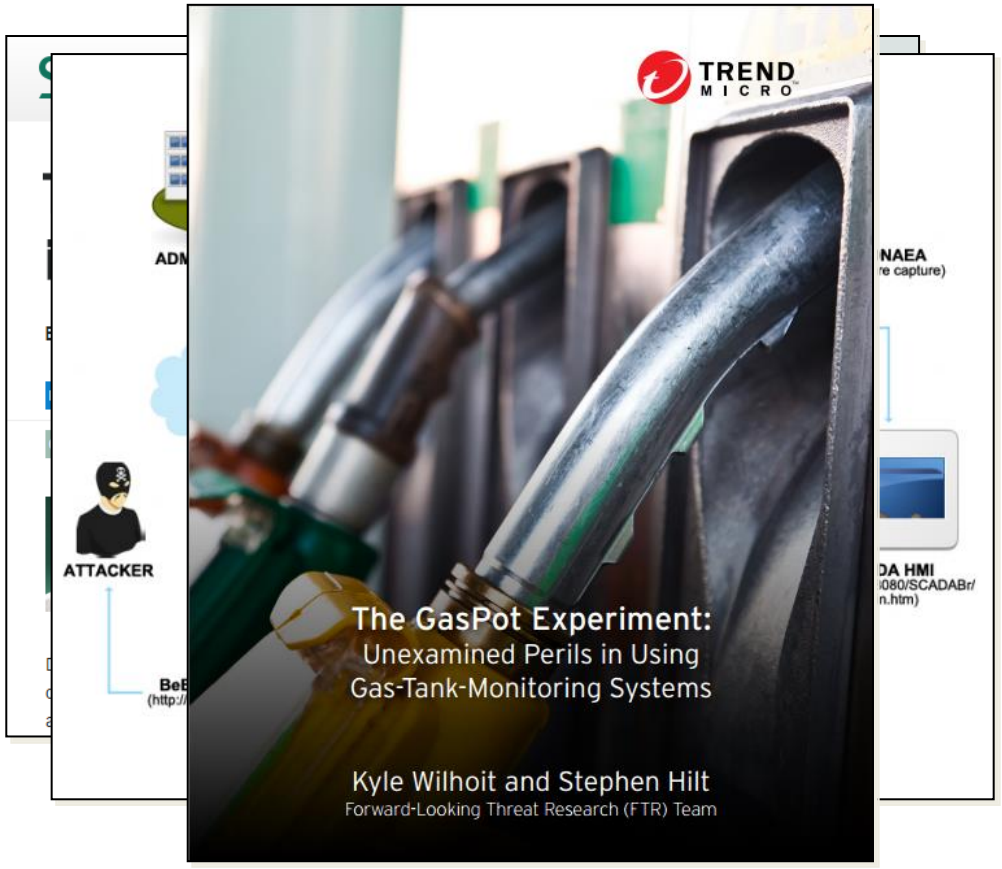
首发	后续新发现
icefog	Javafog
Hangover	Hangover2
Anunak	Carbanak
The Epic Turla Operation	Satellite Turla

如何进一步发现

我们难以掌握和确定的

更多的资源：

- 攻击者的相关资源：
  Hacking Back
- 被攻击目标的相关资源：
  取证分析
- 被攻击目标的相关资源：
  蜜罐诱饵

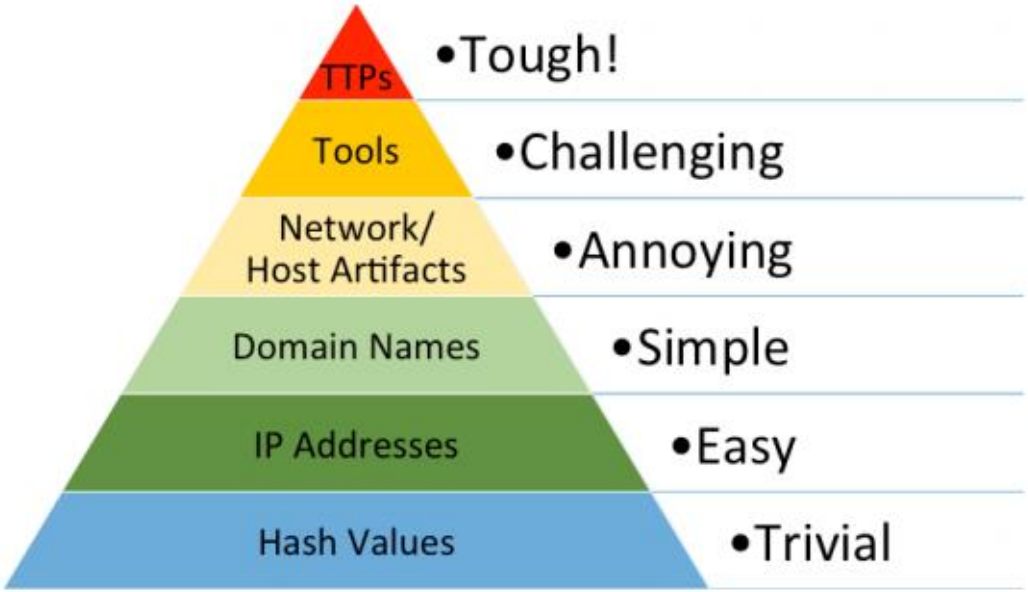


如何进一步发现

我们难以掌握和确定的

幕后组织：

- 难以定性，另外存在嫁祸、假情报等情况：
  客观陈述，避免主观臆断



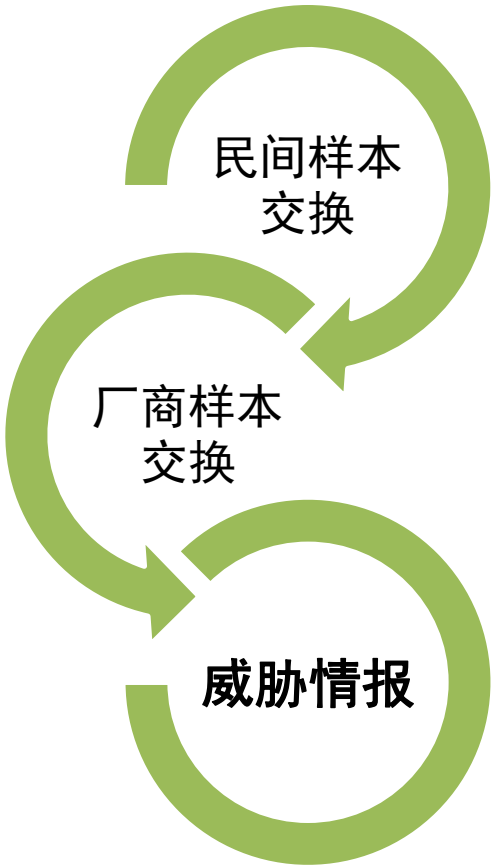
众人拾柴火焰高

从样本交换说起

民间样本交换：主要以个人

厂商样本交换：国内外厂商之间的样本交换。从样本到URL，从PC到移动，已形成交换平台（NSS\MUTE）

威胁情报交换：IOC，STIX等标准



最后

面对新的安全威胁，我们应该怎么做？

开放、合作

谢谢！