熊猫的伤痕——中国遭遇的APT攻击

安天实验室 首席战略官

方华

安天 智者安天下

提纲

- APT的由来和趋势
- 几例中国遭遇攻击的案例分析
- 技术应对

APT的由来和趋势

关于APT的由来与趋势。

高级持续性威胁开启了新的威胁时代

国家和政治经济集团
为背景发动

横向移动 水坑攻击
SNS夹带 0Day漏洞 数字伪装
格式文档攻击 本地化反弹

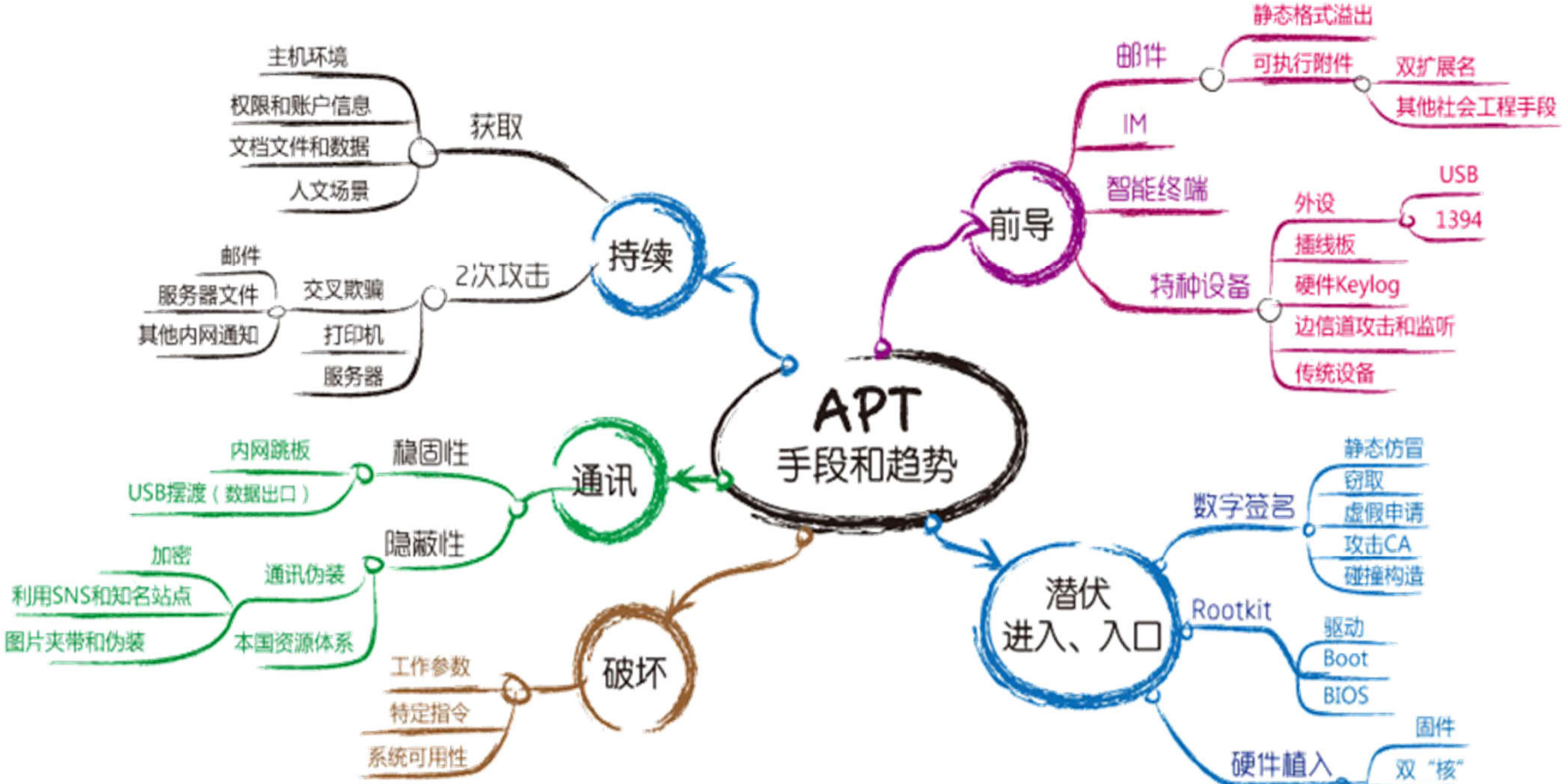
Advanced
高级

Persistent
持续性

Threat
威胁

反复进入
坚定动机 隐蔽通讯 人员带入
作业意志 持久化

高级持续威胁是攻击方法和技巧的集大成者



谁最初创造了“高级持续威胁”一词

Greg Rattray

Managing Director, JP Morgan Chase

New York, New York | 计算机和网络安全

目前就职	JP Morgan Chase
曾经就职	Delta Risk LLC, Finanical Services Roundtable, ICANN
教育背景	Fletcher School of Law and Diplomacy, Tufts University

工作经历：

Managing Director 摩根大通总经理
JP Morgan Chase
2014 年 6 月 – 至今 (1 年 2 个月) | 美国 大纽约地区

Founding Partner Delta Risk创始合伙人
Delta Risk LLC
2007 年 9 月 – 2014 年 6 月 (6 年 10 个月) | Washington DC and San Antonio

Senior Vice President for Security 金融服务圆桌会议安全高级副总裁
Finanical Services Roundtable
2010 年 9 月 – 2011 年 12 月 (1 年 4 个月) | Washington DC

Chief Security Advisor ICANN首席安全顾问
ICANN
2007 – 2010 (3 年)

Commander 美国空军信息战中心业务组指挥官
Operations Group USAF Information Warfare Center
2005 – 2007 (2 年)

Director for Cyber Security 白宫国家安全委员会网络安全主管
National Security Council White House
2002 – 2005 (3 年)

Commander 凯利空军基地23期信息作战中队指挥官
23d Information Operations Squadron, Kelly AFB, TX
2000 – 2003 (3 年)

起源追溯：

APT的第一个标志是来自于专为敏感信息泄露设计的有针对性的、社会工程的电子邮件投放木马，并于2005年被英国和美国组织判定。虽然没有使用 “APT” 这个名字，但是攻击者符合定性其为APT的标准。**2006年，“高级持续性威胁”被美国空军上校Greg Rattray引入。**

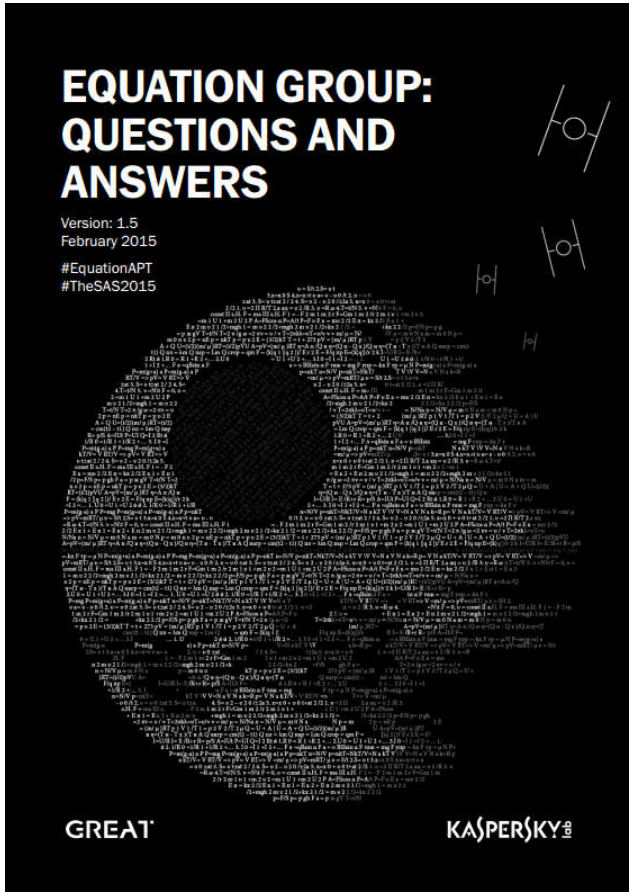
The first signs of APTs came from targeted, socially-engineered emails dropping Trojans designed for exfiltration of sensitive information. They were identified by UK and US CIRT organizations in 2005. Although the name "APT" was not used, the attackers met the criteria that determines an APT. **The term "advanced persistent threat" is cited as originating from the Air Force in 2006 with Colonel Greg Rattray.**

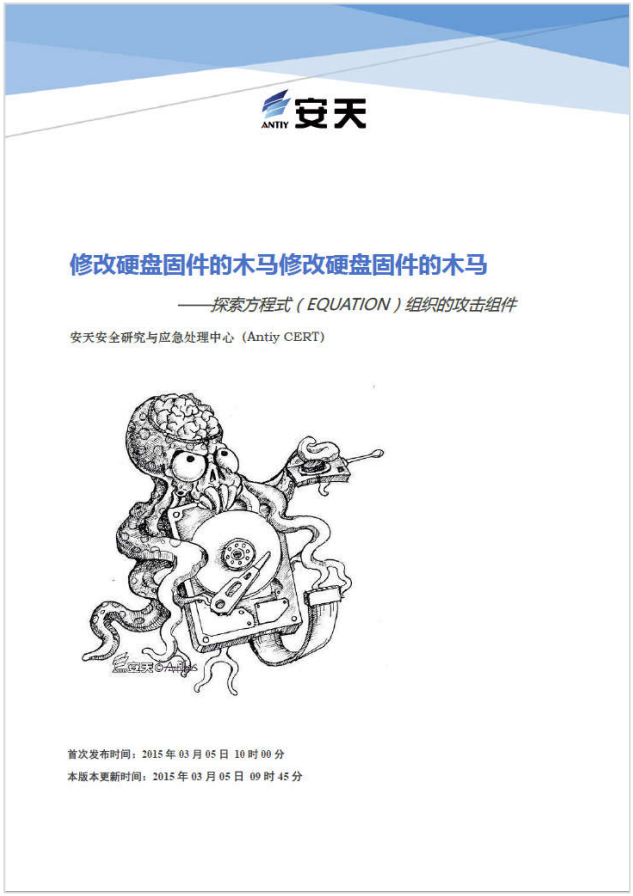
2015年曝光的APT行动情况

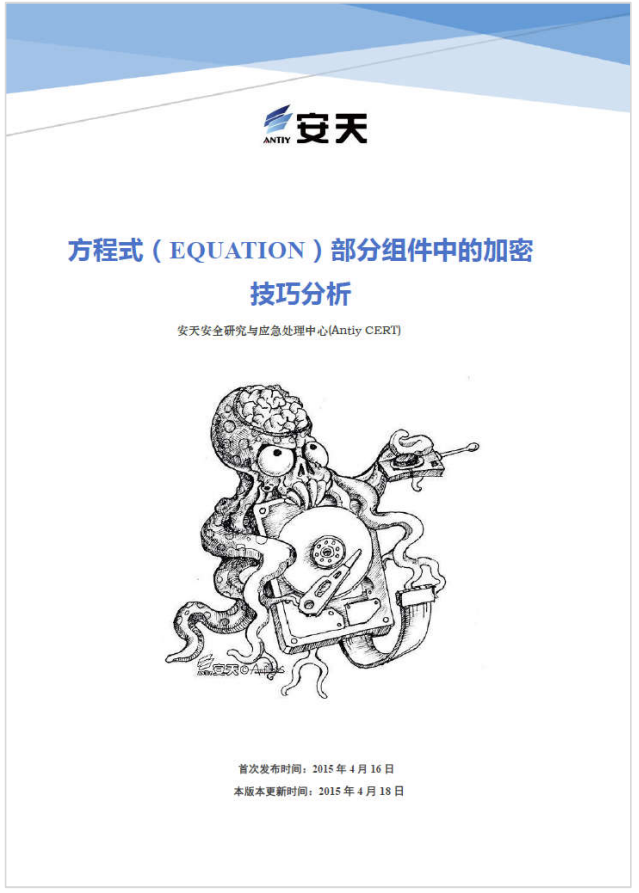
几例中国遭遇攻击的案例分析

这是从我们发现和分析的很多针对中国的攻击事件中，筛选出来的几个案例

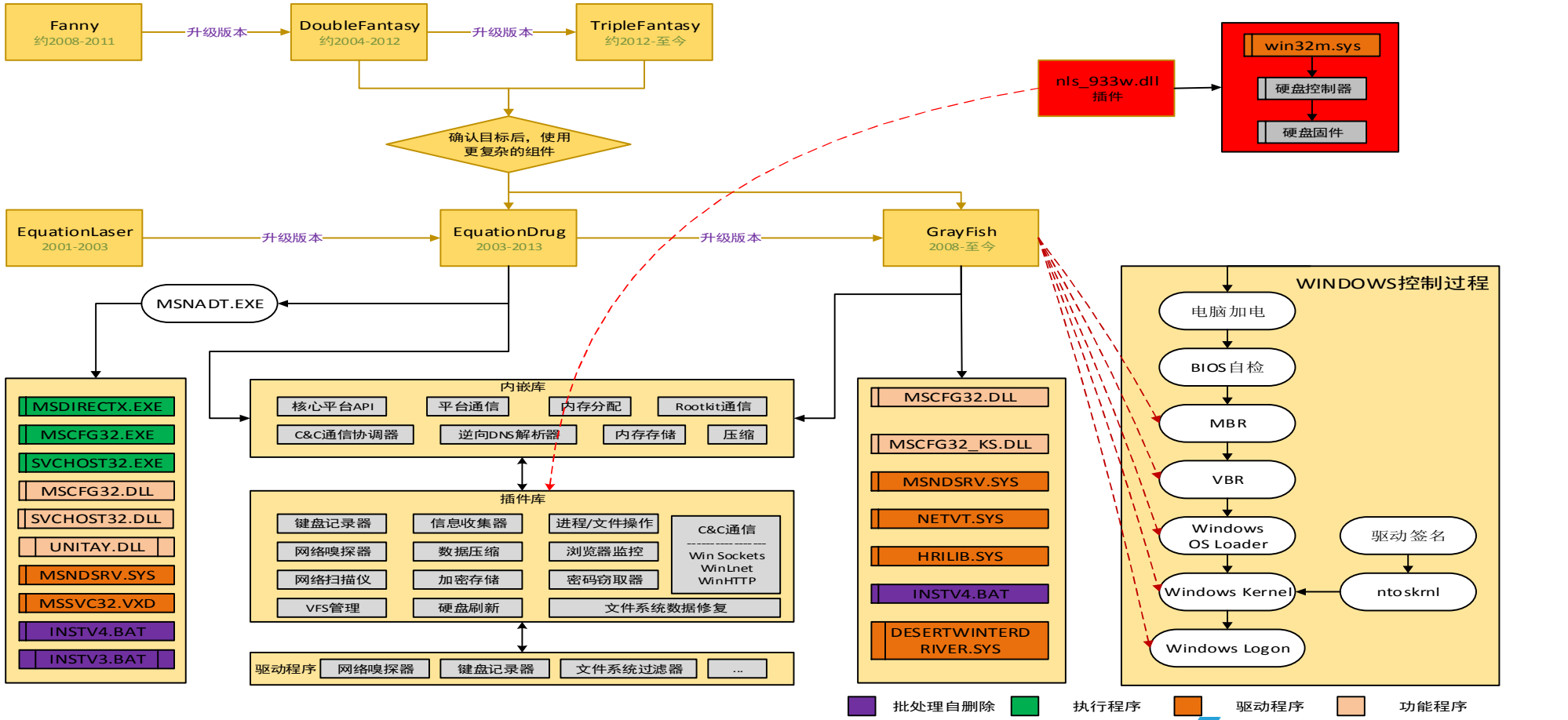
谁在发动针对中国的关键目标和基础设施的行动？



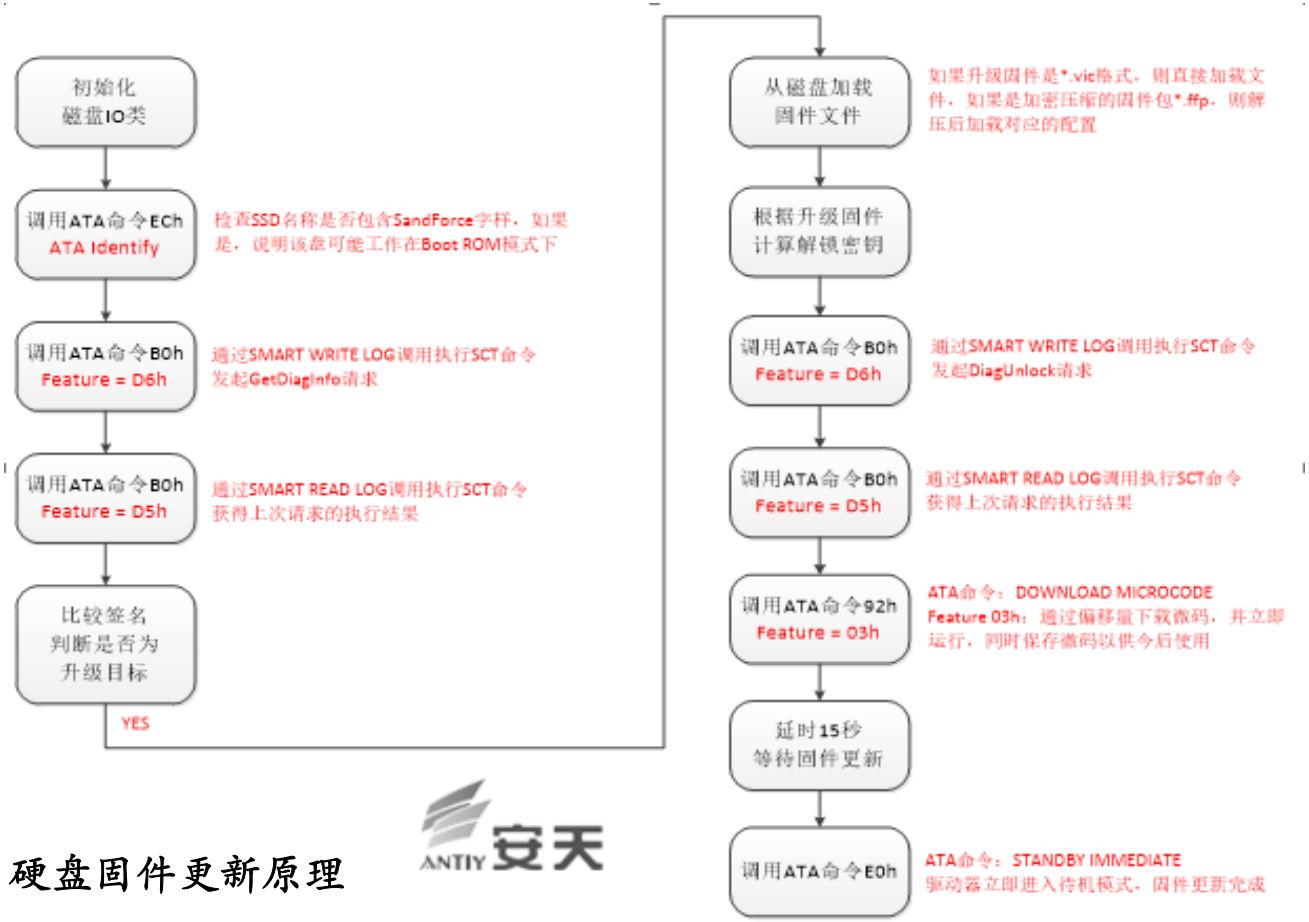




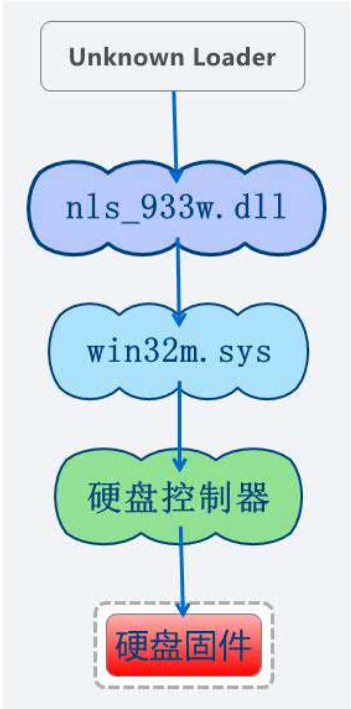
方程式——精密的框架与固件持久化的攻击！



针对硬盘固件的攻击过程

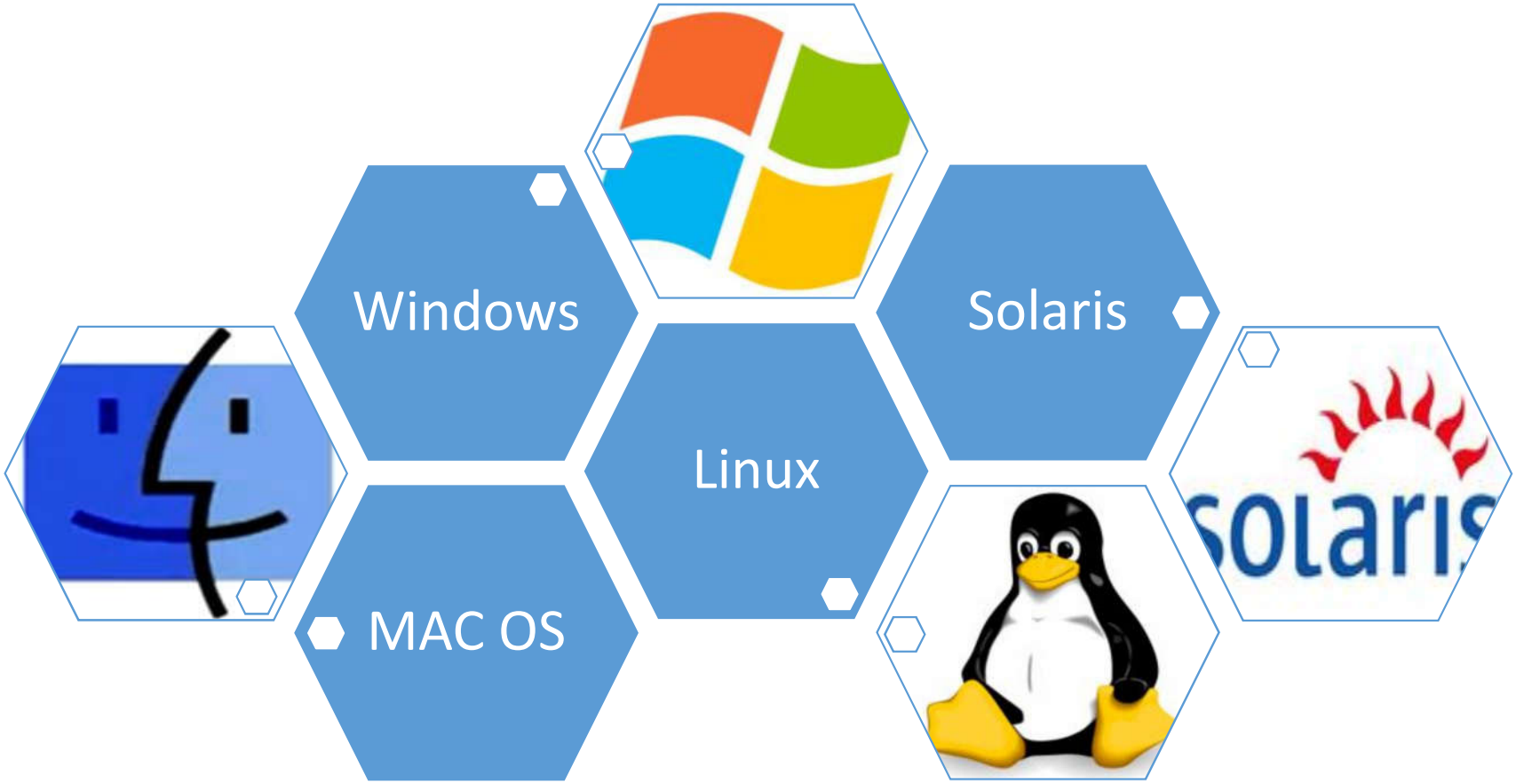


硬盘固件更新原理



方程式针对硬盘固件的攻击

载荷的全平台覆盖能力



精致的指令体系

发包数据第一字节	功能
0x42（B）	清理感染痕迹，删除自身
0x4A（J） 0x92（不可显字符）	创建文件
0x44（D）	写入文件
0x56（V） 0x95（不可显字符）	执行文件
0x53（S）	读取文件回传
0x4B（K）	设置读取文件指针
0x60（‘）	收集大量信息回传（具体格式见下表）
0x70（p）	更新样本配置信息
0x75（u）	更新样本sleep时间，并重新收集信息回传
0x76（v） 0xA2（不可显字符）	更新远程C&C
0x80（不可显字符）	删除指定文件

回包数据第一字节	解释
0x61(a)	收集系统详细信息，大概20类，在上文中对不同系统有过说明
0x42(B)	删除文件成功
0x43(C)	写文件成功
0x44(D)	读取文件
0x47(G)	创建文件成功
0x55(U)	读取完成
0x71(q)	指令执行失败（多个指令失败，都返回此代码）
0x73(s)	设置文件偏移成功
0x74(t)	执行文件失败
0xa1(不可显字符)	更新远程C&C

加密通讯机制

```
.10010119: C745F884000000          mov       d,[ebp][-8],000000084 ;'   ä'
.10010120: C7006351E1B7            mov       d,[eax],0B7E15163 ;'┐ßQc'
.10010126: 41                      inc       ecx
.10010127: 8B5488FC               2mov       edx,[eax][ecx]*4[-4]
.1001012B: 81EA4786C861            sub       edx,061C88647 ;'a╚‡âG'
.10010131: 891488                  mov       [eax][ecx]*4,edx
.10010134: 41                      inc       ecx
.10010135: 83F92C                  cmp       ecx,02C ;','
.10010138: 7CED                    jl       .010010127 --↑2
.1001013A: 33D2                    xor       edx,edx
.1001013C: 33DB                    xor       ebx,ebx
.1001013E: 8955FC                  mov       [ebp][-4],edx
.10010141: 33FF                    xor       edi,edi
.10010143: EB03                    jmps     .010010148 --↓3
.10010145: 8B4508                  mov       eax,[ebp][8]
.10010148: 8B75FC                 3mov       esi,[ebp][-4]
```

```
*(_DWORD *)buf = 0xB7E15163;
i = 1;
do
{
*(_DWORD *)(buf + 4 * i) = *(_DWORD *)(buf + 4 * i - 4) - 0x61C88647;
++i;
}
while ( i < 44 );
```

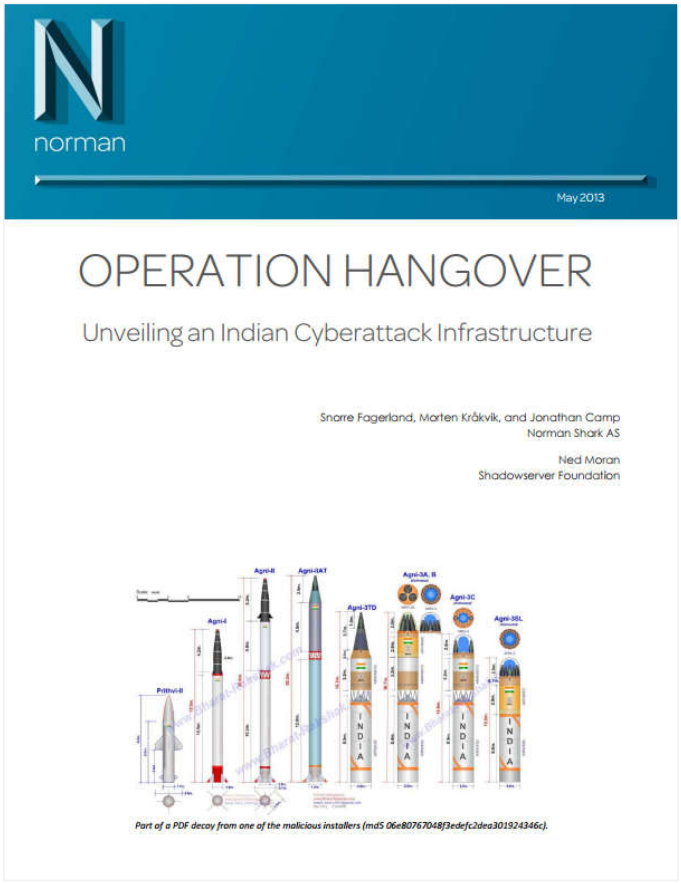
```
do
{
  sub_1000DD99((int)v10, key + 0xB0, key);
  result = 0;
  do
    *(_BYTE *)v4++ = *(_BYTE *)a2++ ^ v10[result++];
  while ( (signed int)result < 16 );
  a3 -= 16;
  v7 = v9-- == 1;
  *(_DWORD *)(key + 0xB0) = *(_DWORD *)v10;
  *(_DWORD *)(key + 0xB4) = *(_DWORD *)&v10[4];
  *(_DWORD *)(key + 0xB8) = *(_DWORD *)&v10[8];
  *(_DWORD *)(key + 0xBC) = *(_DWORD *)&v10[12];
}
while ( !v7 );
```

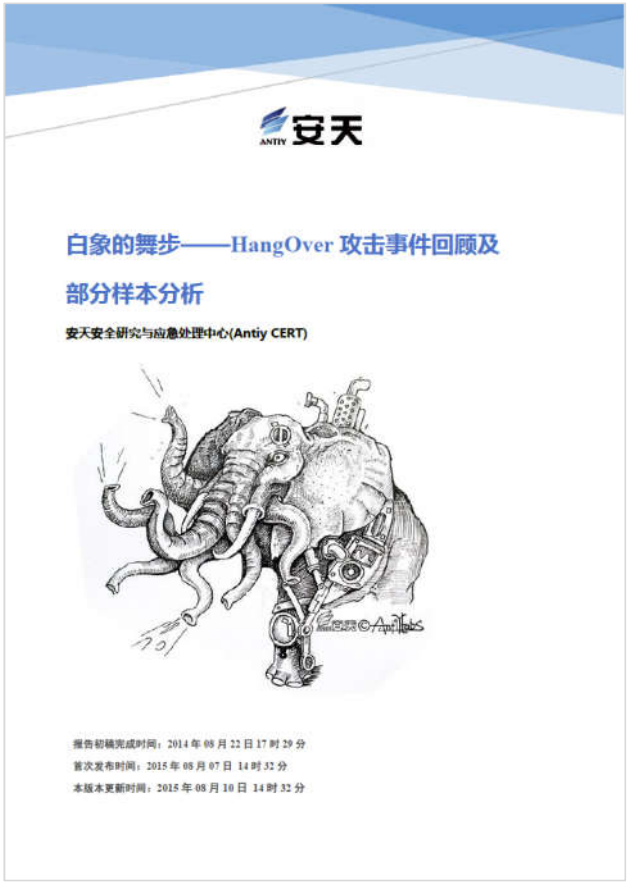
A^2PT——“高级的”APT

神一样的对手

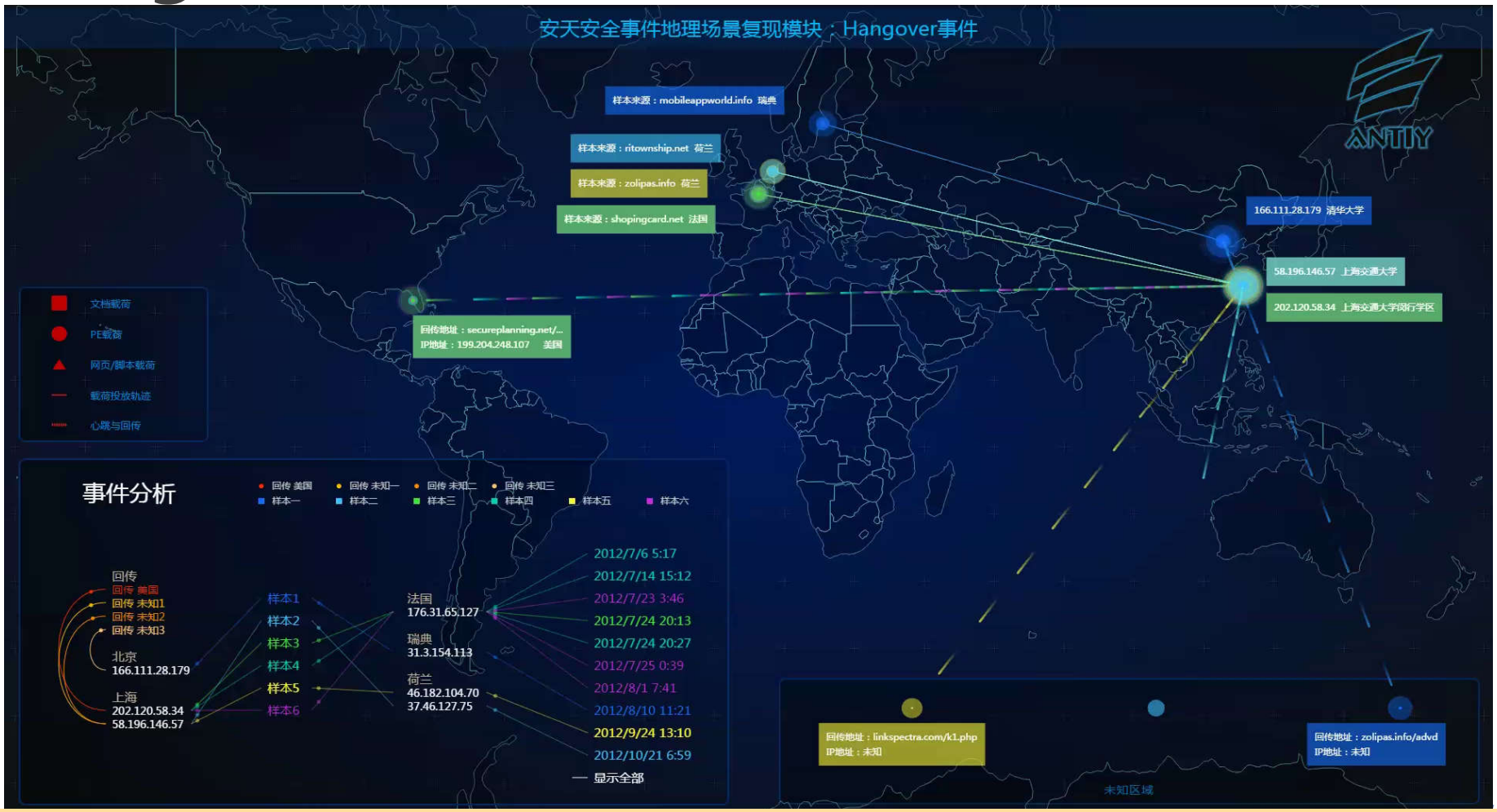
1. 有充足的0day储备
2. 载荷部分高度复杂，高度模块化
3. 本地加密抗分析，网络严格加密通讯和伪装
4. 不一定通过网络植入，可能为人工植入和物流链劫持
5. 基本上完整普及了无文件载体技术，内存分段抗分析
6. 持久化向深度扩展（固件），向广度扩展（防火墙、邮件网关、局网内横向移动）
7. 完整的覆盖所有操作系统平台（含移动）

是谁攻击了中国的高等院校？



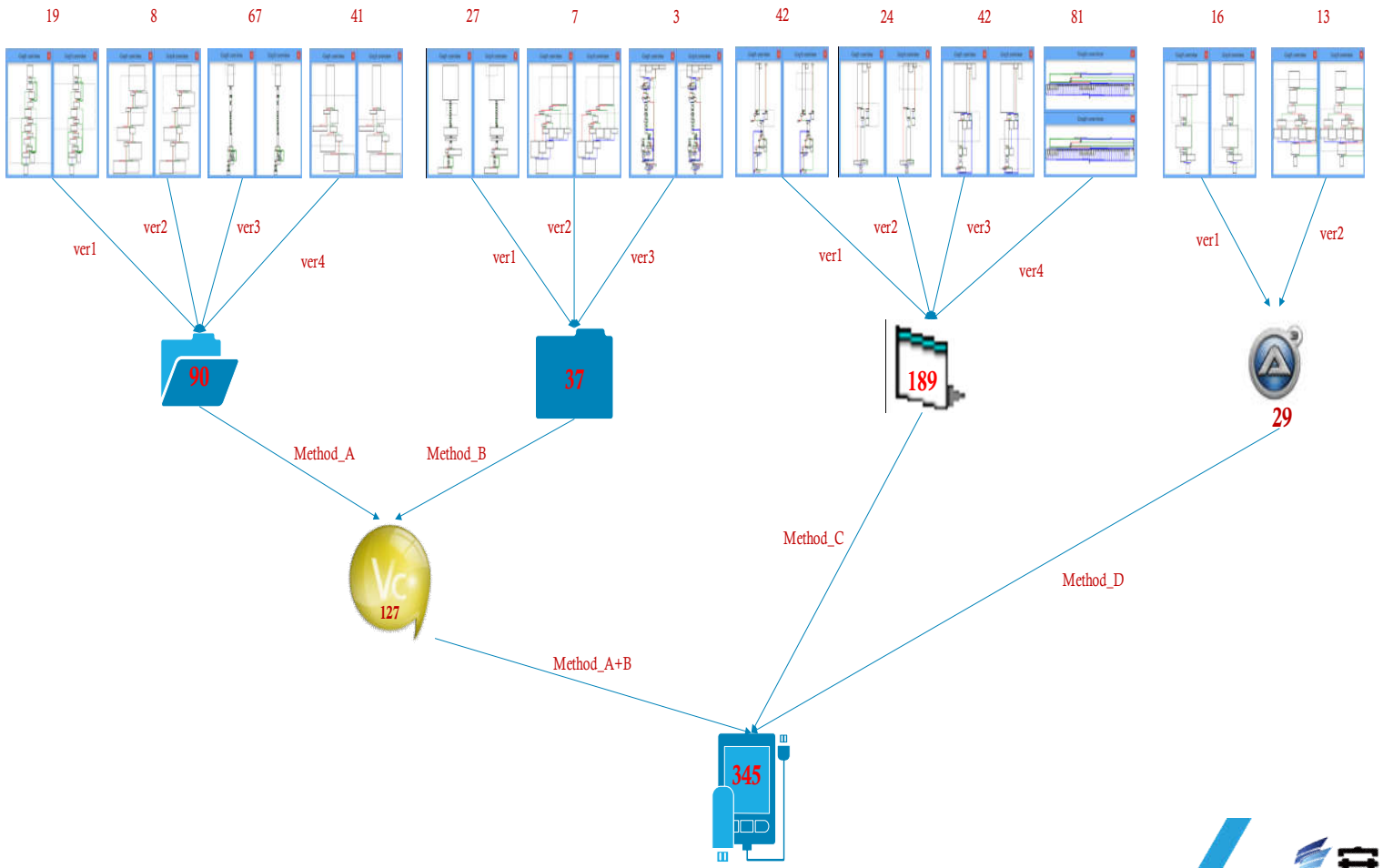


HangOver-攻击过程解析？

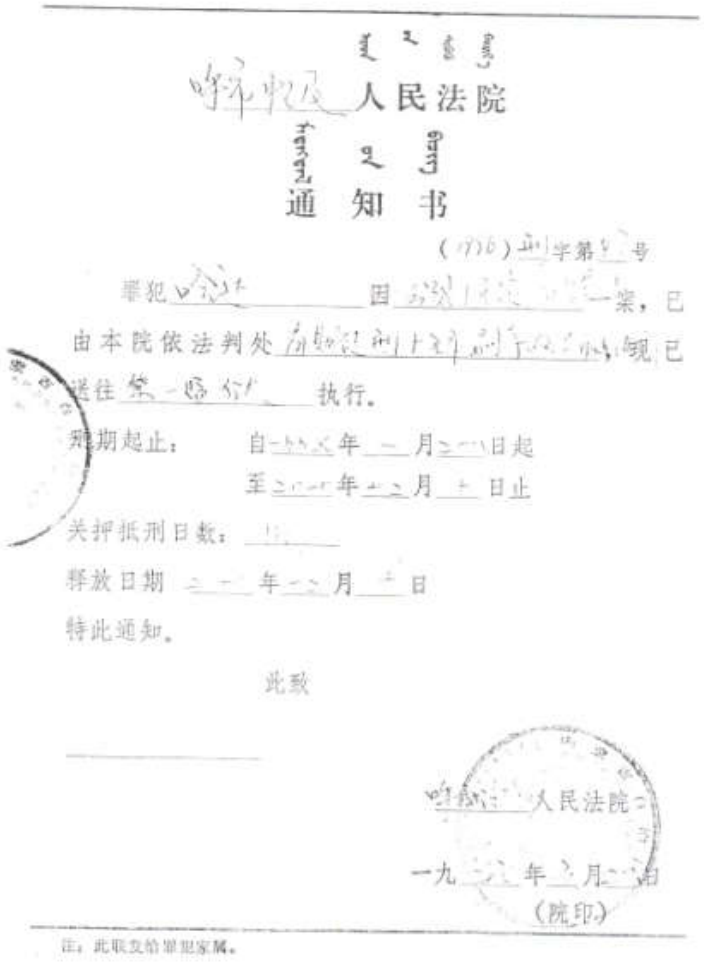


没有使用0day；没有盗用大厂商证书；没有复杂的加密体系；没有必要的Rootkit手段

HangOver——人海战术式的APT！



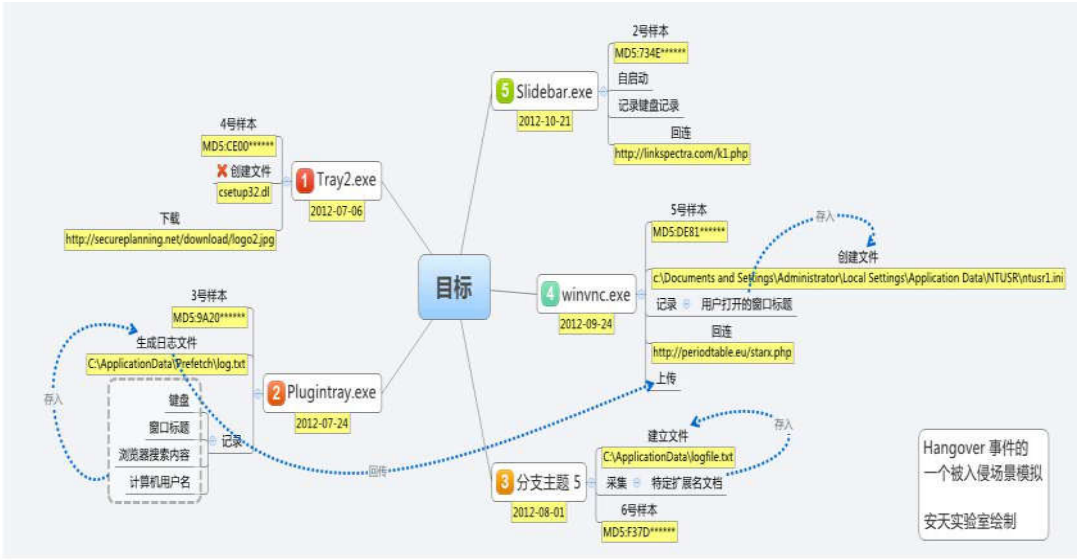
社会工程技巧与模块化投放



通 知 书

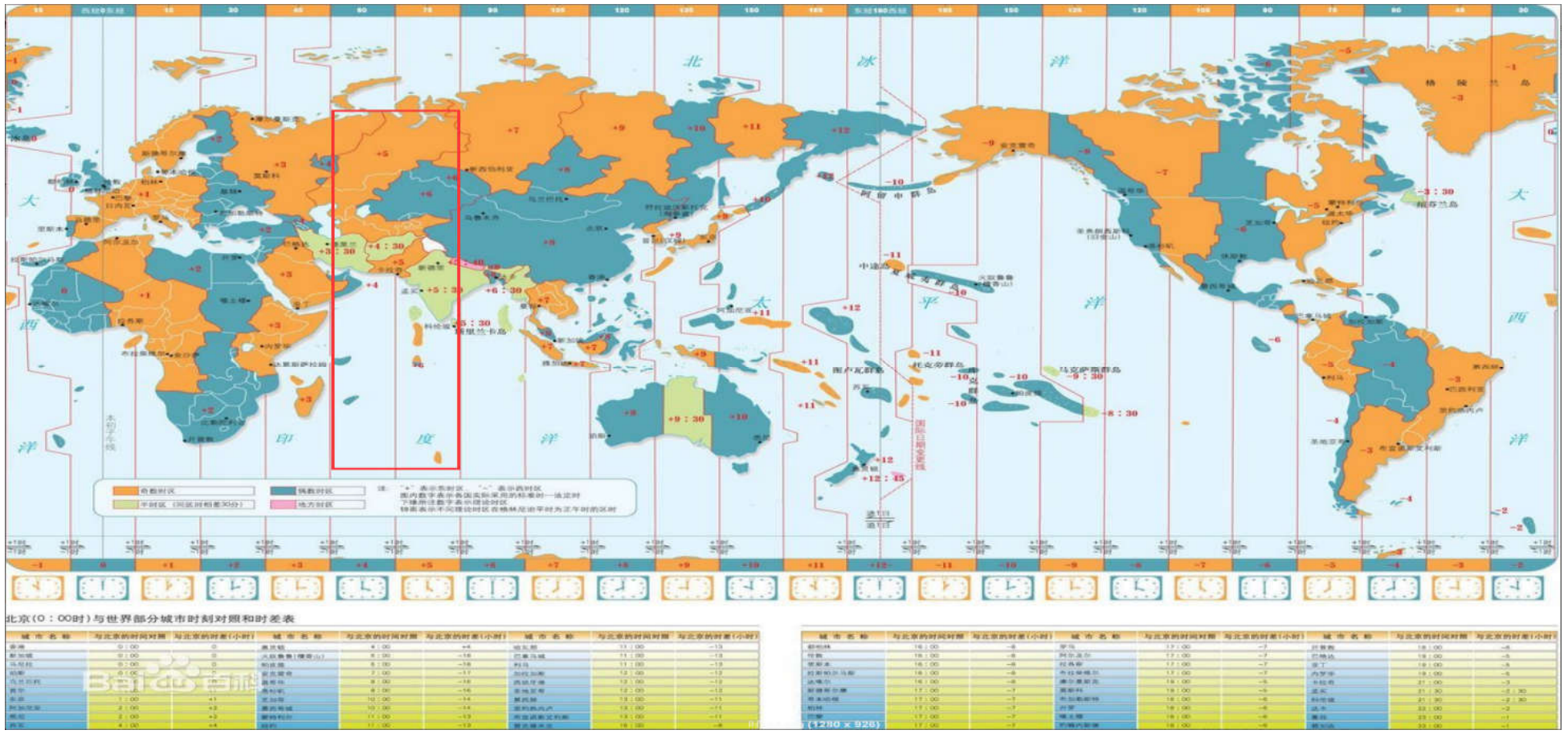
人民法院

（院印）



攻击上海交大的样本组合分析

追踪、再追踪



这些攻击的特点——轻量级APT

01

缺乏0day储备
很少使用0day

02

载荷编写质量
低下

03

严重依赖网络
投放

04

没有采用必要的
Rootkit手段

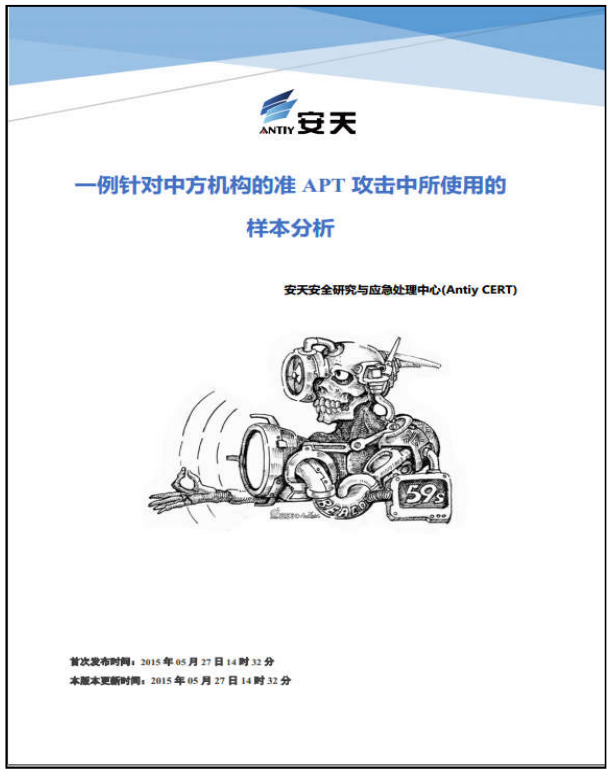
05

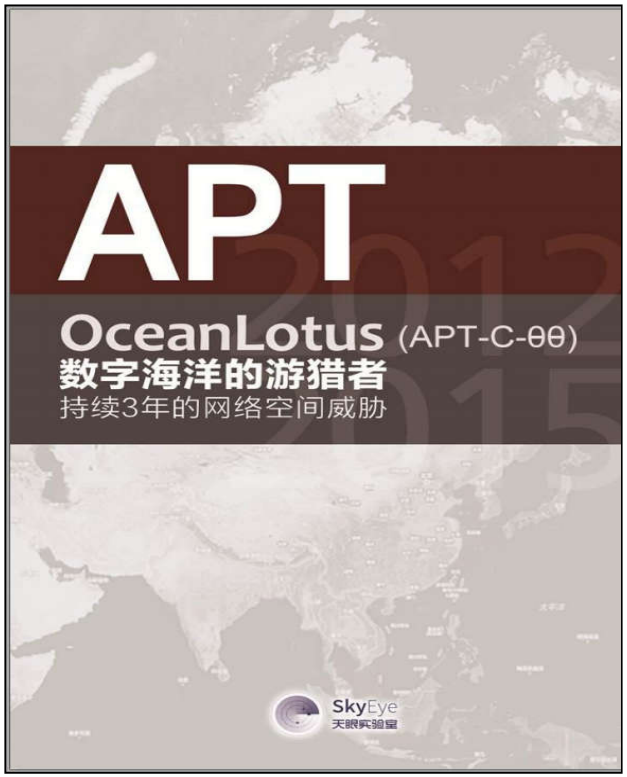
缺少必要的持久
化能力

06

主要针对
Windows系统平
台作业

是谁攻击中国的海事机构？





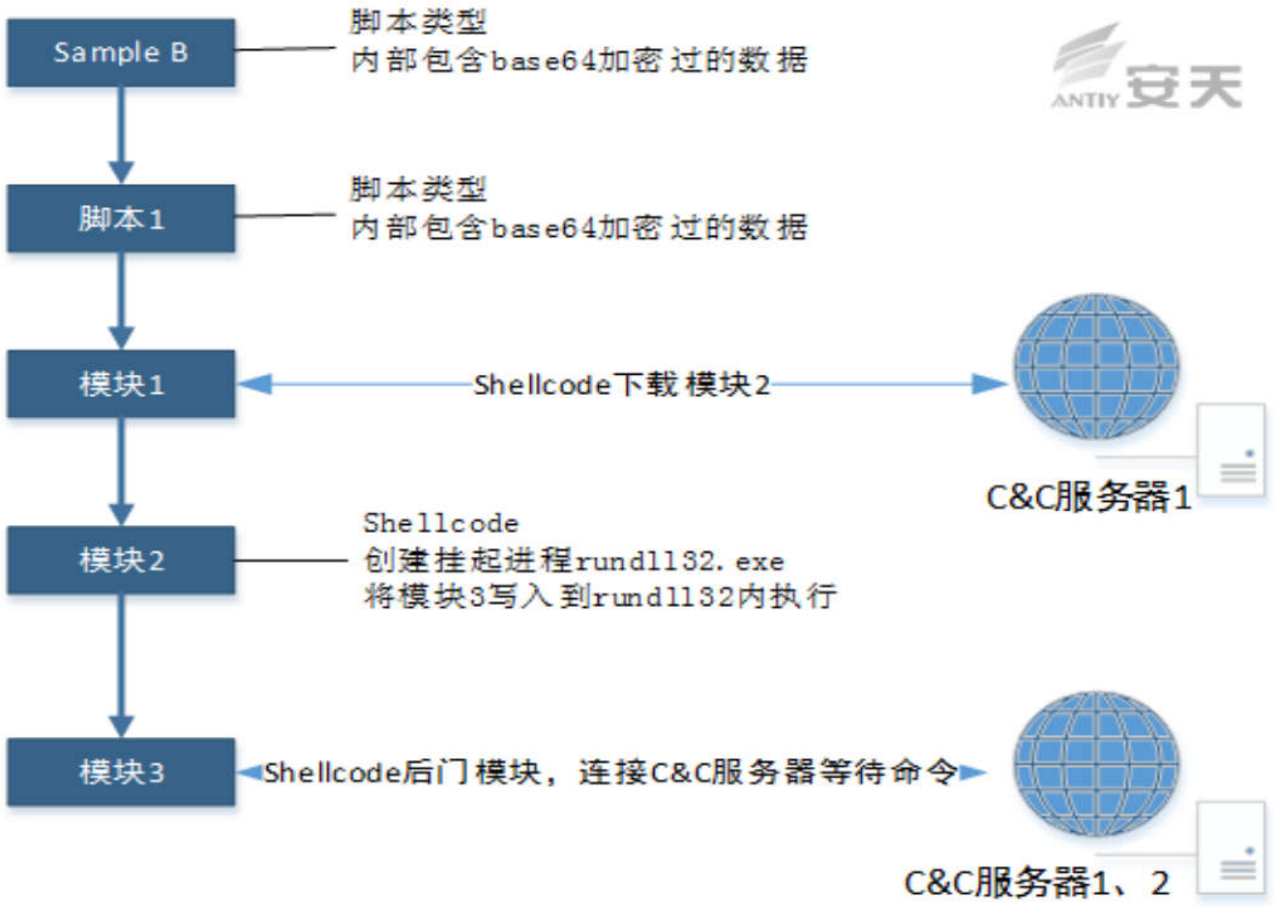
中国厂商自2015年5月27日起连续曝光境外APT，以上三篇文章是针对同一个对手的不同角度解读

解析攻击过程解析


安天安全事件可视化复现系统：APT-TOCS攻击事件
APT攻击流程
APT-TOCS
ANTIY
SECURITY VISUALIZATION TEAM
扫描主机
监听端口
配置武器
攻击成功
发送指令
继续攻击
1、Sample
2、脚本1
3、模块1
4、模块2
5、模块3
攻击者（Cobalt Strike平台）
受害端系统

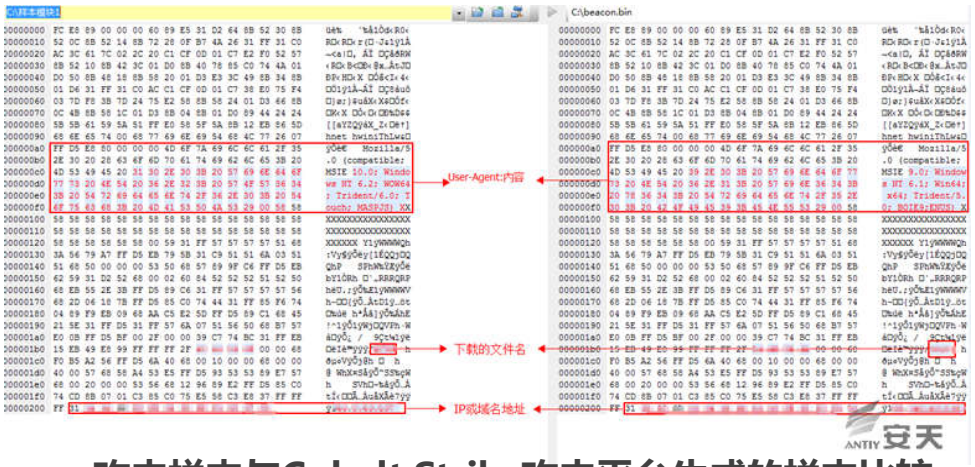
APT-TOCS：使用商业军火的APT攻击

APT-TOCS
模块关系

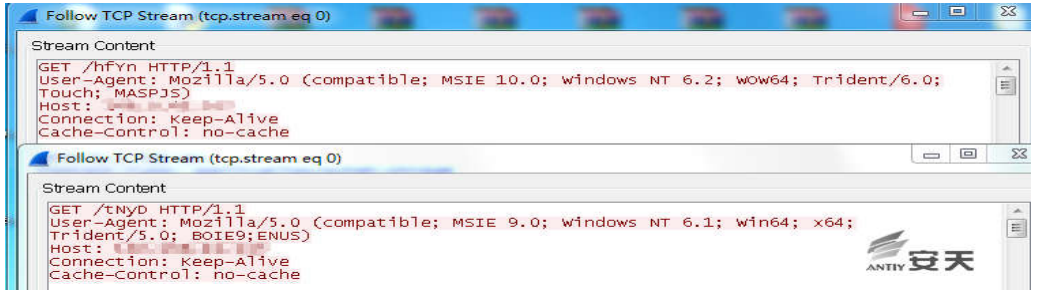


来源：2015.05.28 安天《一例针对中国官方机构的准APT攻击分析》

具有“艺术水准的攻击” 从何而来？



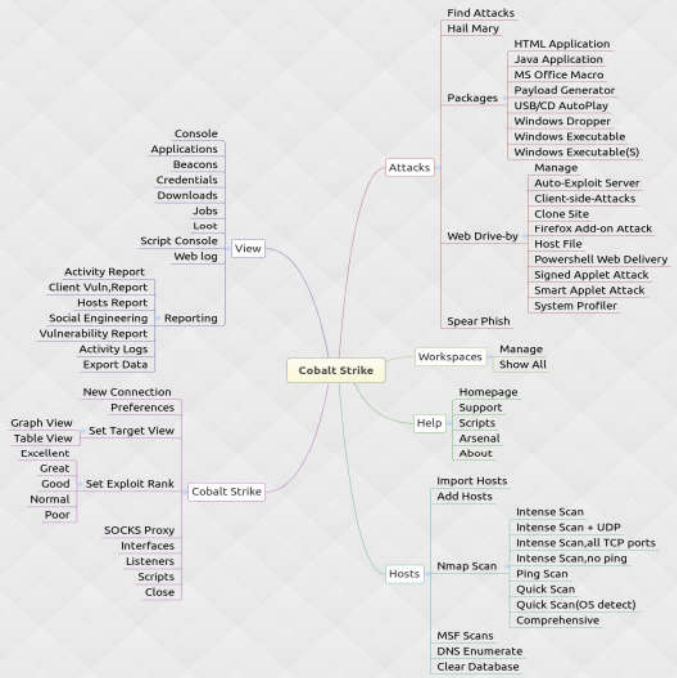
攻击样本与Cobalt Strike攻击平台生成的样本比较



模块1与Cobalt Strike攻击平台生成样本的数据比较

来源：2015.05.28 安天《一例针对中国官方机构的准APT攻击分析》

商业化渗透攻击平台：Cobalt Strike



Packages

- HTML Application
- Java Application
- MS Office Macro
- Payload Generator
- USB/CD AutoPlay
- Windows Dropper
- Windows Executable
- Windows Executable(S)

Web Drive-by

- Manage
- Auto-Exploit Server
- Client-side-Attacks
- Clone Site
- Firefox Add-on Attack
- ……

是谁开发了Cobalt Strike？

- **Cobalt Strike作者**：Raphael Mudge（美国）
  - LLC创始人（the creator of Armitage and founder of Strategic Cyber LLC, develops Cobalt Strike）；
  - 基于华盛顿的公司为RED TEAM开发软件，为Metaslpoit创造了Armitage、sleep程序语言和IRC客户端jIRCii；
  - 曾是美国空军的安全研究员，渗透实验的测试者；
  - 他设置发明了一个语法检测器卖给了Automattic；
  - 发表多篇文章，定期进行安全话题演讲，给许多网络防御竞赛提供RED TEAM，曾参加2012-2014年黑客大会；
- **教育背景**：Syracuse University 美国雪城大学，密歇根科技大学
- **目前就职**：Strategic Cyber LLC（战略网络有限责任公司），特拉华州空军国民警卫队

公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6
Automattic	代码Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息 军官	2004.3-2008-3

商业军火扩散后的攻击特点

01

可能使用商用漏洞

02

使用商业木马

03

采用攻击平台投放

04

依托攻击平台的持久化能力

05

依赖攻击平台设定的联系方式

06

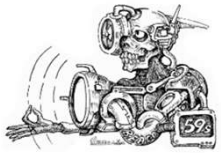
可能覆盖主要操作系统

不同能力的攻击行动

行动能力

成本投入

商业军火支持的APT



2015.5
APT-TOCS

传统的APT

2009.12
Havex

A2PT

2015.2
Equation
方程式

2007或2008
Duqu
毒曲

2010.3
Flame
火焰

2009.6
Stuxnet
震网

初级的APT

2013.5
HangOver

再谈如何定性APT？

APT不是一个严格的技术概念，必须关联其政经背景

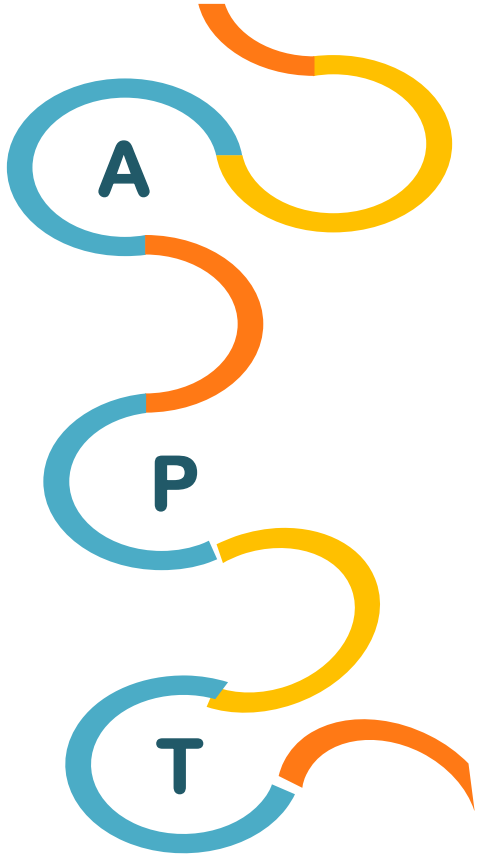
- 发起方与动机
- 受害方与后果
- 作业过程与手段

A的再认识，A具有相对性

- 相对攻击背景体系的能力层次
- 相对被攻击者的势能落差

P是具象的、也是宏观的

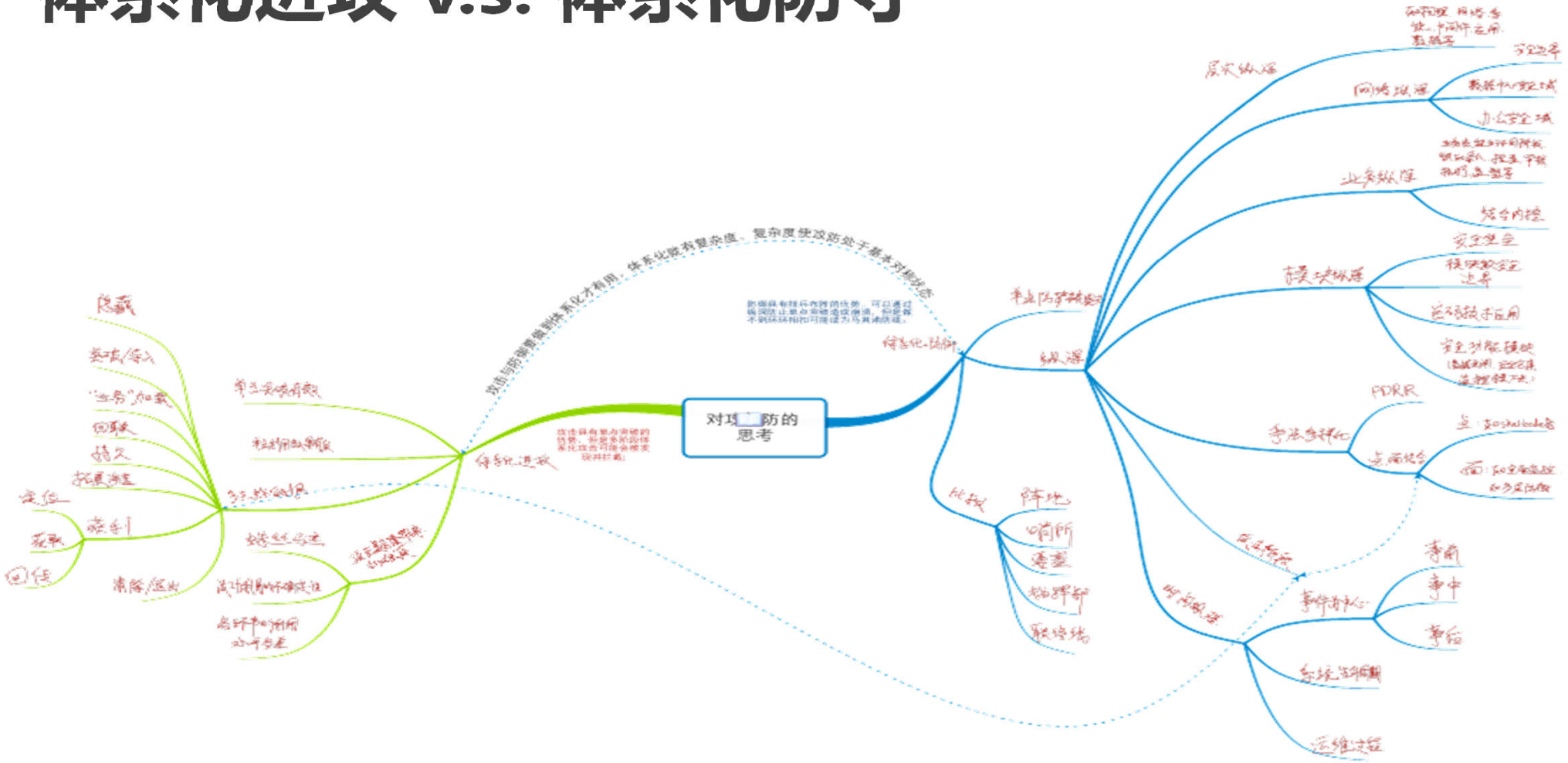
- 具象：其可能是连接能力、也可能是持久化的能力、或者反复进入的能力
- 宏观：取决于攻击方的作业意志的持续和成本支撑能力



思考APT的防御能力

这是从我们发现和分析的很多针对中国的攻击事件中，筛选出来的几个案例

体系化进攻 v.s. 体系化防守



本页PPT引自黄晟（JOE）《关于网络纵深防御的思考》

传统安全环节依然有其的价值

现状

防火墙、IDS

- 未加电或配置为直通状态
- 未得到有效的关注

反病毒

- 由于物理隔离导致一个月到半年升级一次
- 因担心带来不稳定和其他问题不升级

主机环境

- 多半为默认配置，未经过有效的配置强化
- 缺少统一的补丁机制，导致不能打补丁
- 因担心对业务的影响不敢打补丁

应发挥的价值

防火墙、IDS

- 是最基本的边界安全设备
- 是防护基础作业供应方

反病毒

- 对已知恶意代码进行有效检测
- 提供已知恶意代码相关信息
- 应得到及时升级

主机环境

- 需要进行配置强化
- 需要及时打补丁

静态检测引擎已经成为基础能力

从检测器到提供决策支持

全格式解析能力

全格式解析和向量抽取

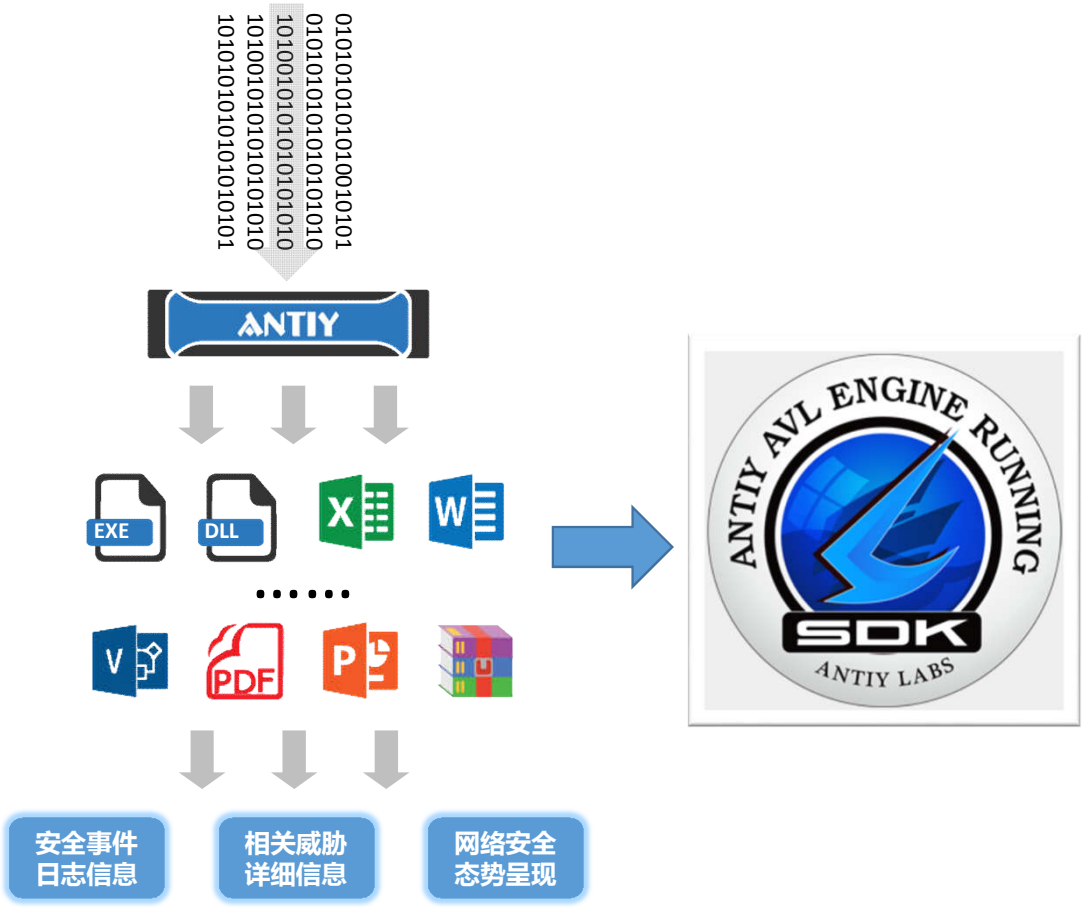
高速、深度、多场景

可以在X86、ARM、MIPS架构上全速工作，支持Windows、Linux、Android等各种操作系统。

综合信誉化判定

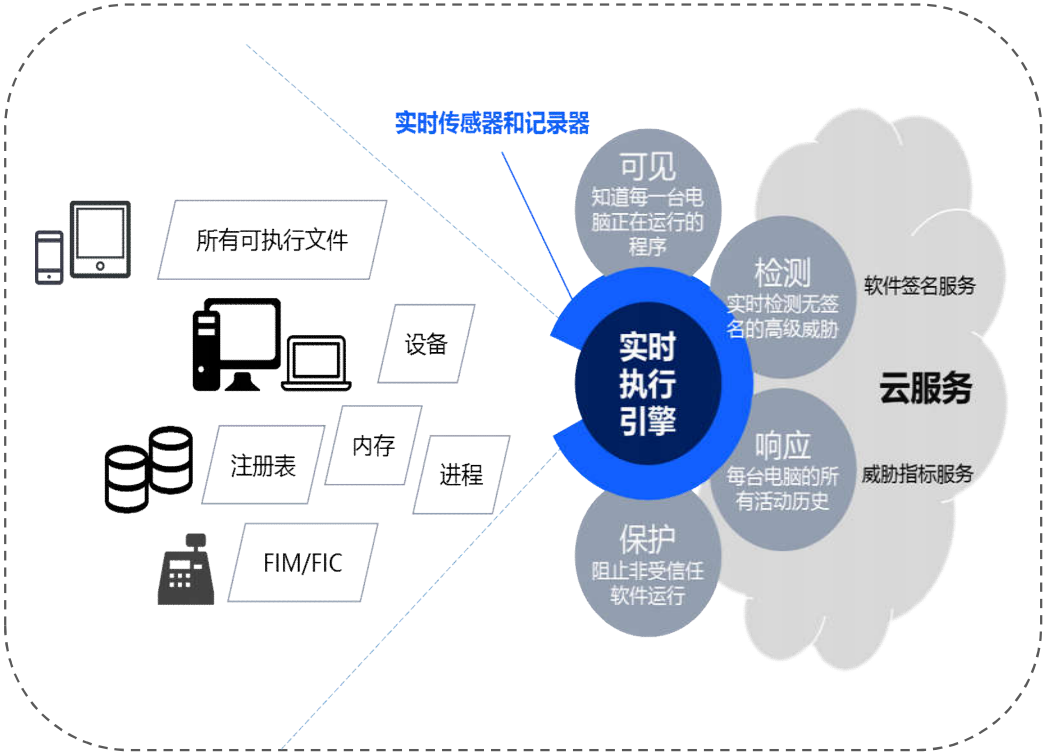
内置多种信誉化支持

流量侧：基础检测与回溯



1. 旁路流量缓存与还原
2. 确认鉴定可疑文件的属性
3. 追溯载荷投放
4. 联动沙箱分析

终端侧：白名单+安全基线的终端防护



1. 阻止恶意代码的入侵和启动
2. 确认鉴定可疑文件的属性
3. 追溯处置恶意文件
4. 建立私有的安全基线和经验

本地化纵深：不依赖与云的本地化沙箱

深度分析

线速智能预处理

阶段1
信誉分析
减少误报

动态引擎

阶段2
环境记录
动态向量提取

1. 可疑文件异步分析
2. 发现未知恶意文件
3. 发现0day/1day漏洞
4. 将发现同步给系统内其他安全设备处置

新布防点总结

01

传统环节

提供一般性威胁的前置过滤能力。

02

静态检测

过滤已知恶意代码过滤，定性已知的高价值威胁。

03

前置沙箱分析

增加文档格式攻击等0day漏洞的发现能力，建立私有化的分析能力。

04

白名单加安全基线

减少攻击者对终端攻击的成功率。

05

网络监控

控制对手的网络横向移动

06

数据集中分析

建立动态信誉能力，建立情报整合能力。

感谢各位专家领导

www.antiy.com

安天 | 智者安天下