由高级持续性威胁（APT）引发的防御思考

安天 高喜宝

提纲

01 “魔窟”是网络战的预演

02 从战争视角看APT攻击

03 不同水平的APT攻击

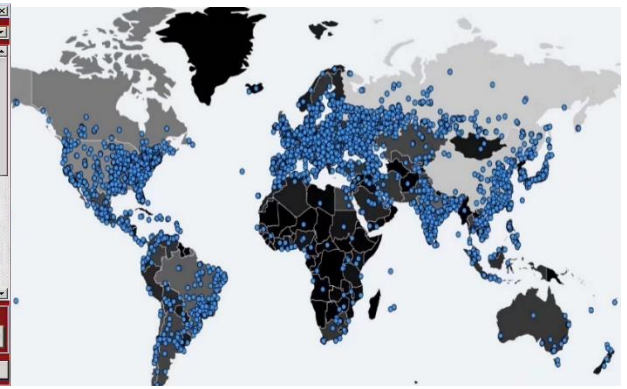
04 布防、支撑与全域融合

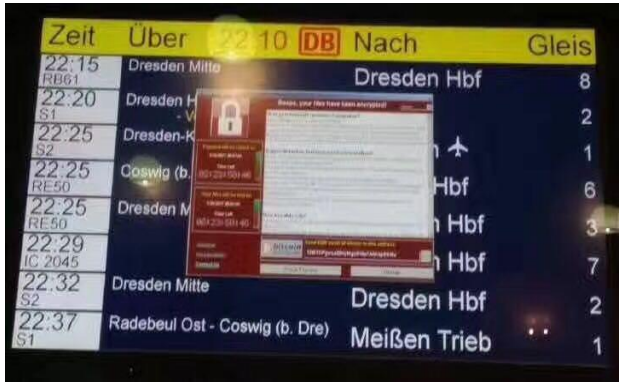
“魔窟”是网络战的预演

- 勒索蠕虫事件背景
- 安全厂商做了什么
- 暴露出来什么问题

“魔窟”（WannaCry）勒索蠕虫横扫全球

- 2017年5月12日20时左右，全球爆发大规模勒索软件感染事件，我国大量用户受到感染，文件被加密
- 蠕虫利用微软SMB漏洞MS17-010，由445端口传播
- 2017年4月14日黑客组织Shadow Brokers（影子经纪人）公开一批NSA使用的网络攻击工具，其中包含了该漏洞的利用程序
- 安天在2015年《一例针对中方机构的准APT攻击样本分析》报告提出：**拥有全球最顶级能力的超级大国，对于有效控制网络攻击武器扩散，应该负起更多的责任**
- 安天CERT在2017年4月14日发布的《2016年网络安全威胁的回顾与展望》预测：**勒索模式带动的蠕虫的回潮不可避免**





安全厂商与时间赛跑

“WannaCry”相关事件时间轴

2017年3月1日

2017年3月14日
微软发布MS17-010 漏洞补丁

2017年3月28日
已发现的WannaCry1.0样本最早的时间戳

2017年4月14日
Shadow Brokers(影子经纪人)
公开黑客组织方程式的多个入侵工具

2017年4月15日
安天对泄露的入侵工具展开分析
形成初版简报

2017年4月17日
安天对泄露的入侵工具
形成完整事件分析简报

2017年5月12日
“蠕虫式”勒索软件WanaCry全面爆发

2017年5月13日
06：00发布《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》
17：25发布《安天应对勒索软件“WannaCry”配置指南》
17：45发布《安天应对勒索者蠕虫病毒WannaCry FAQ》
19：03 安天发布蠕虫病毒WannaCry免疫工具和扫描工具

2017年5月13日
卡巴斯基误判无“域名开关”样本存在

2017年5月14日
卡巴斯基承认误判，说明暂未发现无“域名开关”样本

2017年5月14日
05：00发布《安天应对勒索软件“WannaCry”开机指南》

2017年5月14日 18:42:29
三个新修改样本出现

2017年5月15日 19:00
安天发布变种事件分析

2017年5月18日
发现利用相同漏洞传播的UIWIX勒索样本

2017年5月18日 6:00
安天发布WannaCry支付解密流程分析

2017年5月18日
安天发布UIWIX勒索样本简报

2017年5月19日

安天启动A级（最高级）响应

3月

做出威胁预测

- 安天在基础威胁年报中预测将在一年内爆发大规模勒索软件攻击，随后向CNCERT进行了专报。

5月12日

第一时间通报处置

- 安天第一时间向主管部门通报情况，内部工具开发计划和人员集结工作部署。

09:45
- 第一时间进行用户现场应急处置。

15:00-16:00
- 安天向客户发布预警和防护手册。
- 操作系统应急补丁包推送。

20:20
- 决定启动"A级灾难"响应。

22:45
- 经测试，安天智甲终端防御系统，无需升级即可有效阻断WannaCry的加密行为，安天探海威胁检测系统升级后可以检出WannaCry的扫描包。

启动A级响应

5月13日

06:00
- 发布《安天紧急应对新型"蠕虫"式勒索软件"WannaCry"全球爆发》深度分析报告，微信公众号一天突破31万的阅读量。

17:00-18:00
- 发布《安天应对勒索软件"WannaCry"配置指南》。
- 发布《安天应对勒索者蠕虫病毒WannaCryFAQ-1》针对大量用户的高频问题进行回复。

20:05
- 首批应急响应人员奔向客户现场，进行内网扫描收集用户问题。

19:00-20:00
- 发布WannaCry免疫工具和扫描工具。
- 公安部下属国家计算机病毒应急处理中心，向公众推荐使用安天免疫和专杀工具应对勒索病毒。
- 国家互联网应急中心发布《关于防范Windows操作系统勒索软件Wannacry的情况通报》，向公众推荐使用安天免疫和专杀工具应对勒索病毒。

进驻用户现场

5月14日

发布报告，推出专杀

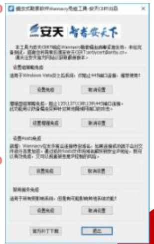
04:30-05:30
- 发布《安天应对勒索者蠕虫病毒WannaCryFAQ-2：传言验证者》。
- 发布《安天应对勒索软件WannaCry开机指南》，应对周一开机安全考验。
- 更新《安天紧急应对新型"蠕虫"式勒索软件"WannaCry"全球爆发》深度分析报告。

15:00
- 现场处置只读U盘（含免疫工具、专杀工具、智甲防勒索版、系统补丁）发布，奔向客户现场。

16:00
- 安天发布加密后的恢复建议，消除用户恐慌。

17:00-18:00
- 国家网信办网络安全检查共享平台，向公众推荐使用安天免疫和专杀工具应对勒索病毒。
- 公安部共享平台向公众推荐使用安天免疫和专杀工具应对勒索病毒。

18:05
- 安天工具持续升级，工具合集已发布至1.4版本。



18:44
- 安天和友商应急团队联合讨论，最终将"WannaCry"中文俗名确定为"魔窟"。

19:00-20:00
- 发布安天智甲防勒索免费版。
- 更新发布免疫工具、专杀工具。

正式命名，更新工具

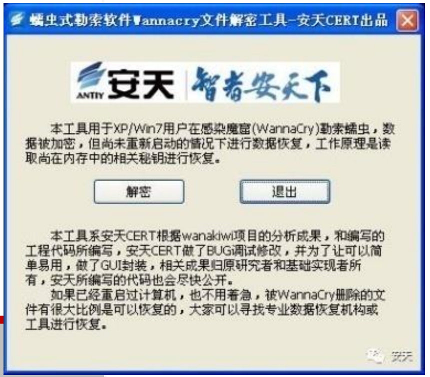
5月15-16日

再次发布报告，提供扩展补丁包

- 15日00:20，安天发布"魔窟"勒索蠕虫内网响应网页工具。
- 15日08:00，针对部分用户提供扩展补丁包。
- 15日凌晨更新《安天应对勒索软件"WannaCry"开机指南》。
- 16日凌晨发布《对"魔窟"（WannaCry）勒索蠕虫变种情况分析》。

5月20日

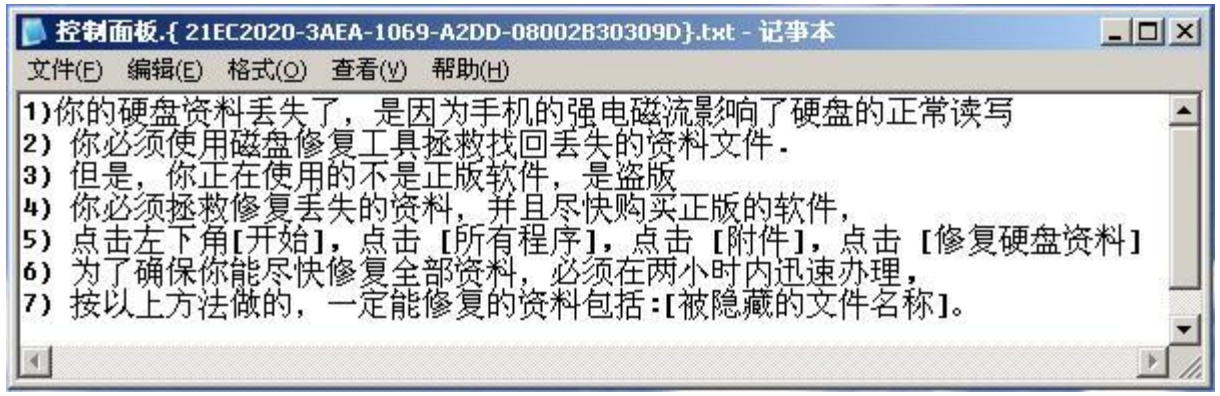
5:02 发布解密工具



安天关于"勒索者蠕虫病毒WannaCry"跟进时间表

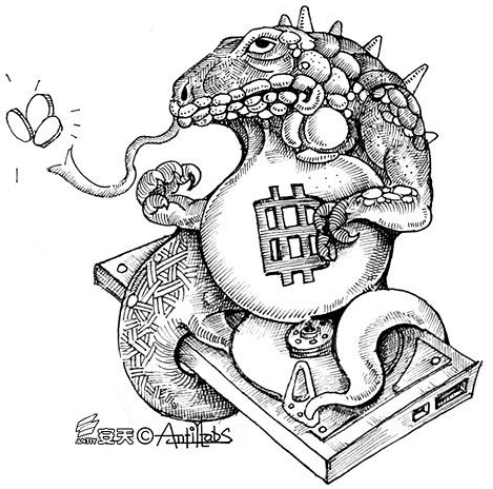
智者安天下

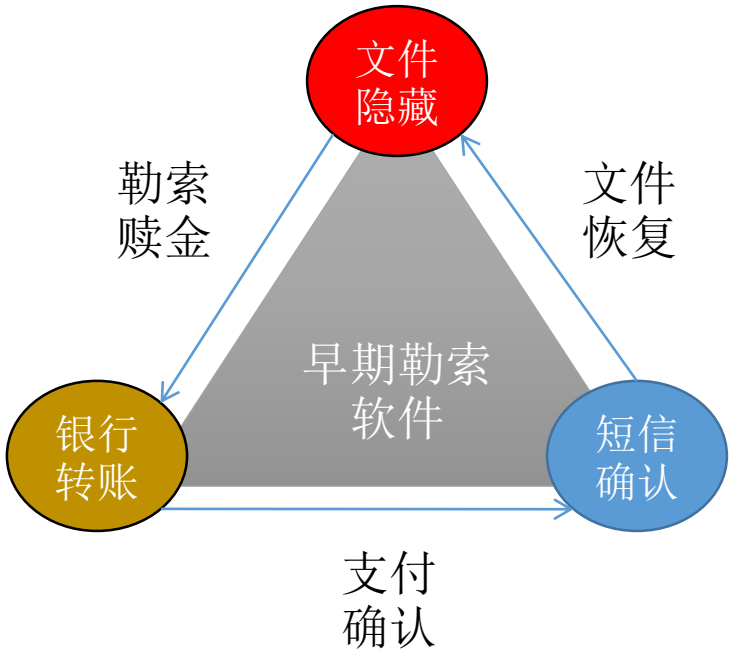
勒索软件

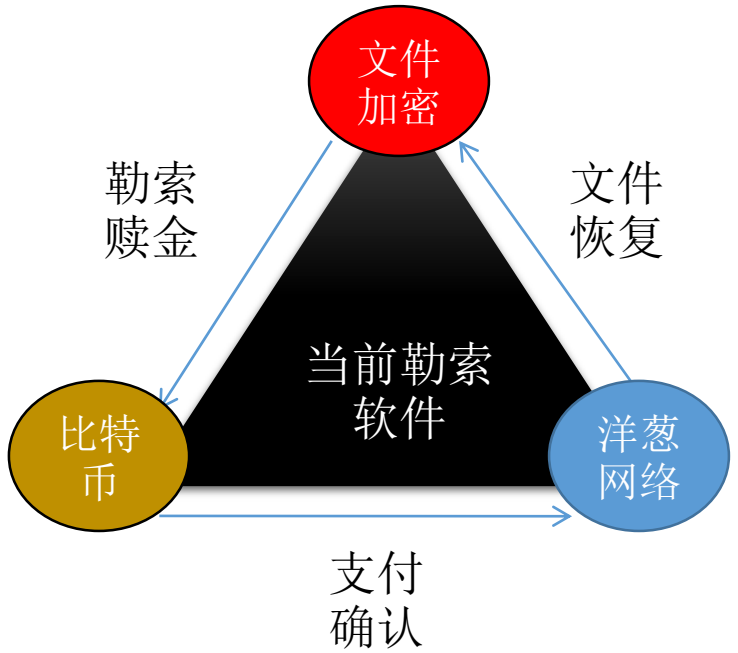


2006年Redplus

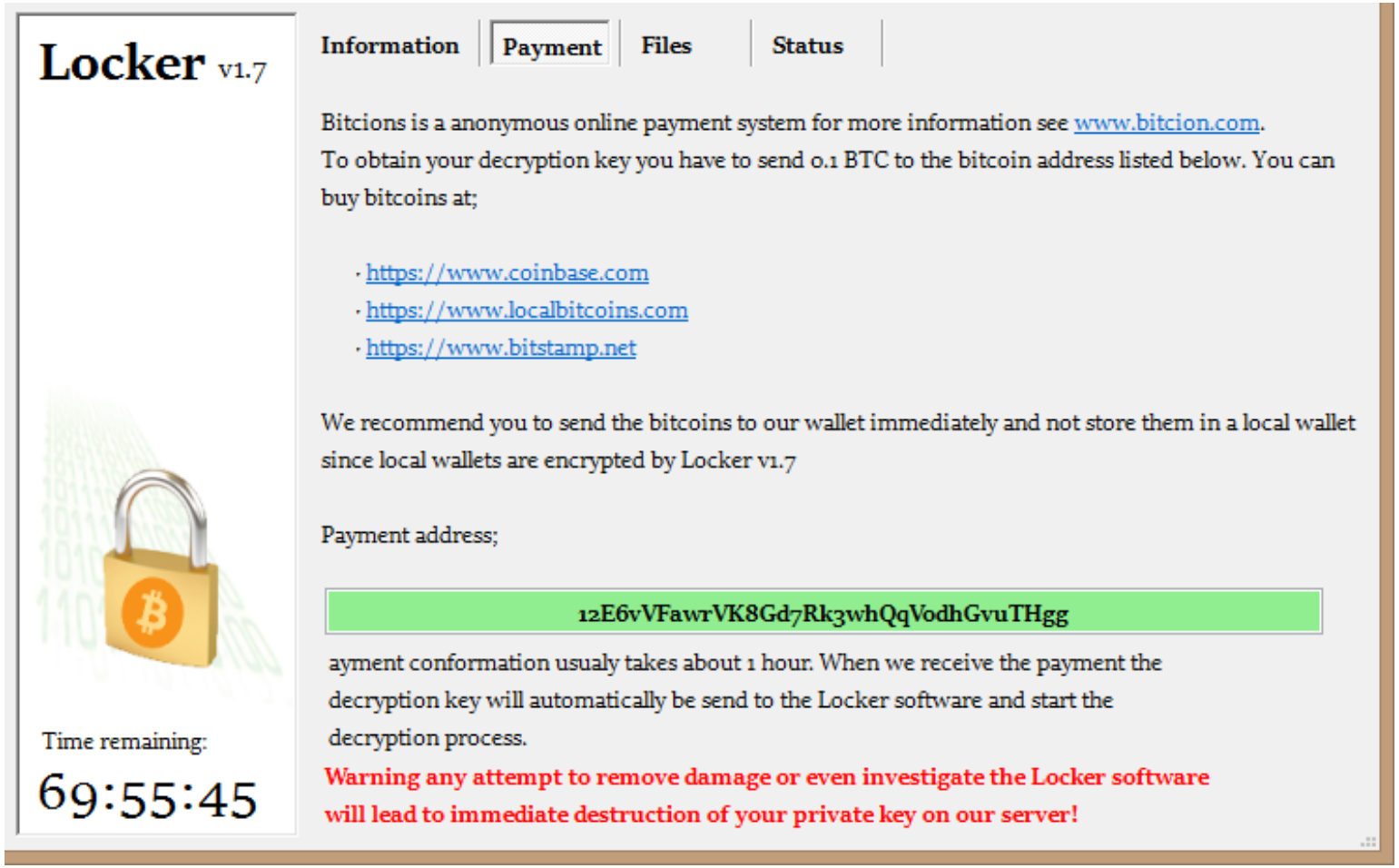
作者欧阳某某于2007年在广州落网，共借助Redplus木马勒索款项95笔，合计人民币7061.05元。法院考虑到其自首情节，最终判其有期徒刑4年。

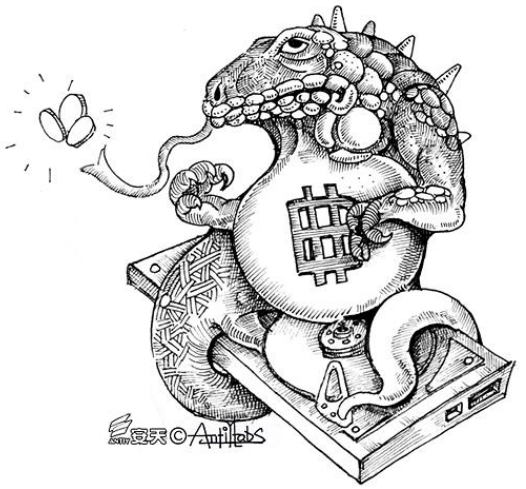






勒索软件





2015年5月底，勒索软件Locker作者公布密钥库，共包含62,703条记录，勒索金额按0.1比特币（当时约175元人民币）计算，收入高达1097万元人民币。

上周 勒索软件“必加”Petya新变种爆发

- 导致乌克兰基辅鲍里斯皮尔机场部分航班延误

CYBER RISK | Tue Jun 27, 2017 | 10:48am EDT

Kiev airport hit by cyber attack, delays possible

Kiev's main airport has been hit by a "spam attack" that could cause some flights to be delayed, the operator, Boryspil, said.

"In connection with the irregular situation, some flight delays are possible," Director Yevhen Dykhne said in a post on Facebook.

(Reporting by Pavel Polityuk; Writing by Alessandra Prentice; Editing by Robin Pomeroy)

乌克兰机场航班延误公告

Lidia Wolanskyj
6月28日 15:28 · Tilda ·

Kyiv's Boryspil Airport's main server is still not working because of yesterday's cyberattack, according to Deputy Director Yevhen Dykhne. Flights are all going out as scheduled and information is being posted to monitors that are manually updated every 15 minutes. Other airport services are all working as usual and no flights have been delayed.

查看翻译

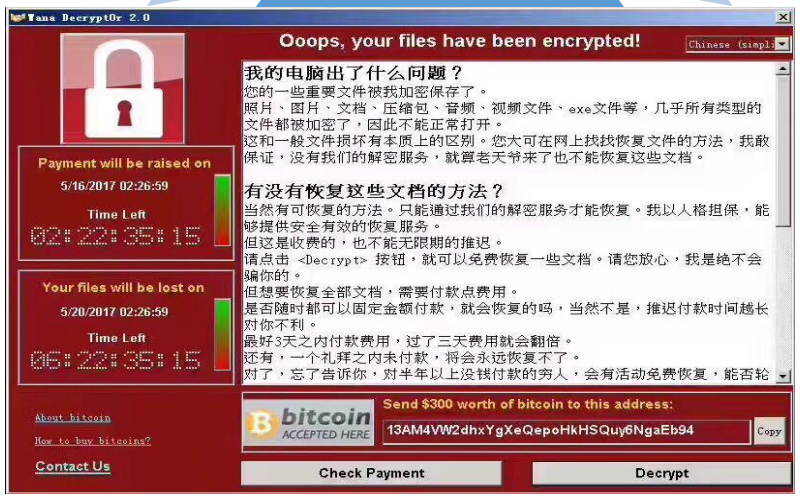
Кібератака на аеропорт Бориспіль: Пасажирів інформують в ручному режимі

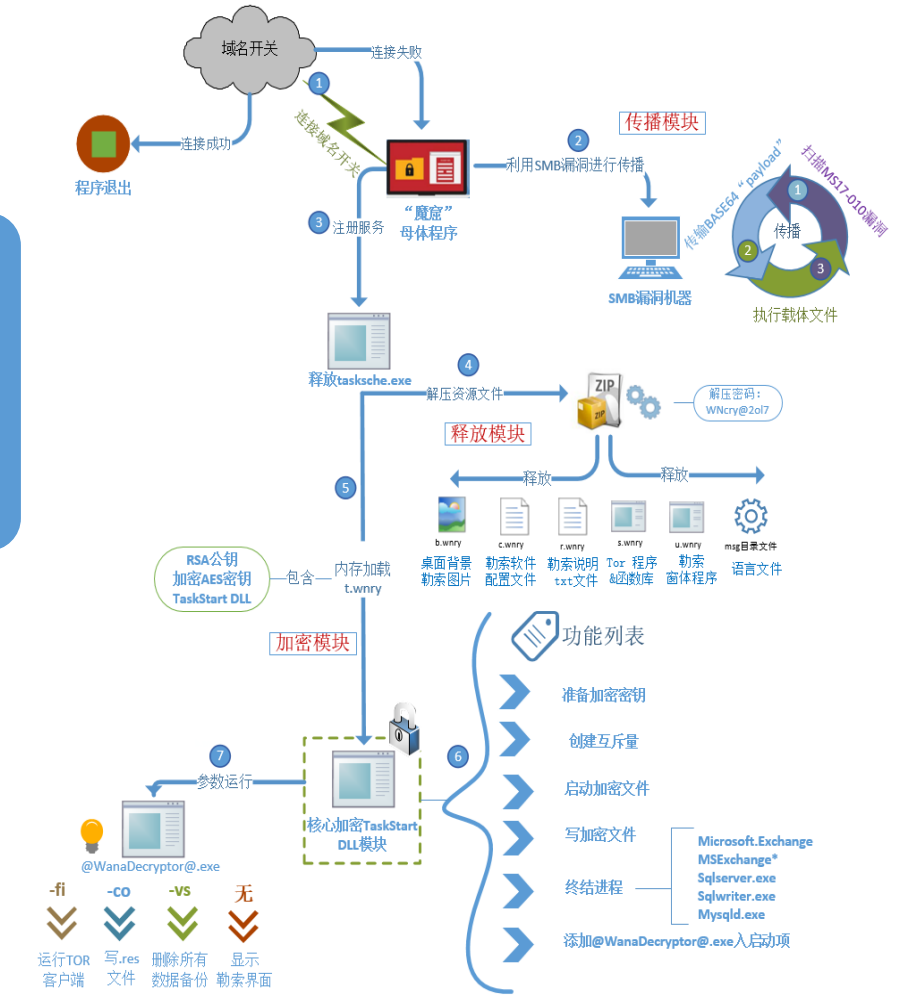
魔窟蠕虫的本质

蠕虫式传播

加密勒索

漏洞利用（MS17-010）

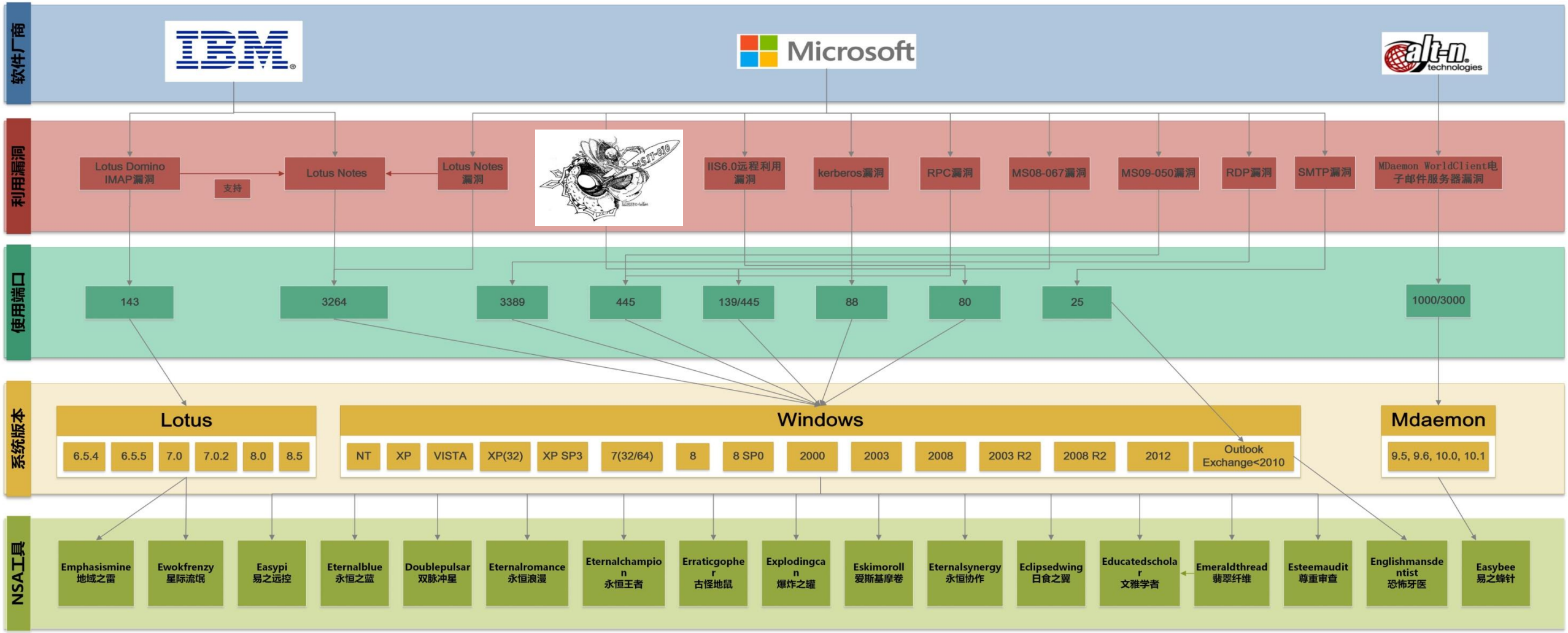




“魔窟”只是冰山一角

2017年4月14日泄露的NSA网络军火装备的漏洞利用关系图

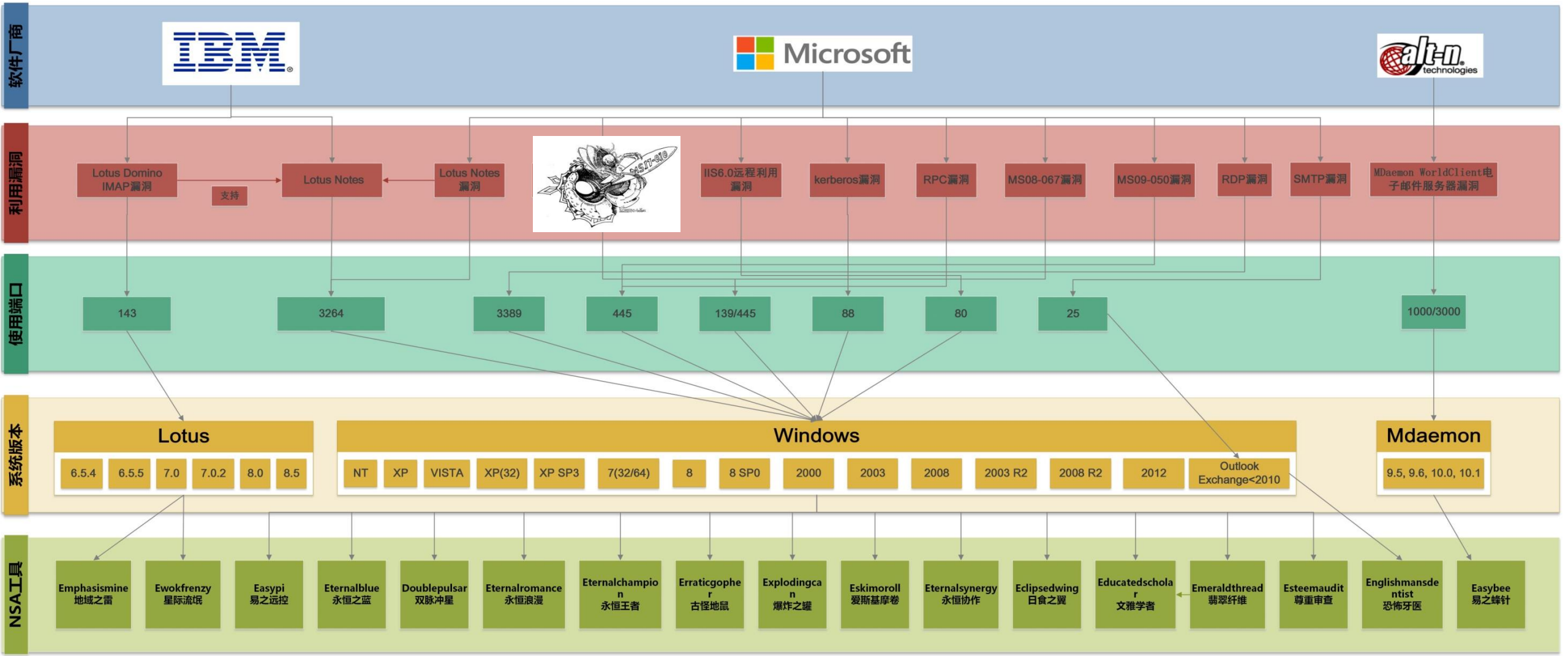
2017年5月21日 安天实验室绘制



NSA组织结构

2017年4月14日泄露的NSA网络军火装备的漏洞利用关系图

2017年5月21日 安天实验室绘制



美国网络空间安全机构

- 美国总统
  - 总统办事机构
    - NSC(国安委)
    - OSTP(白宫科技政策办)
    - ……
  - 内阁
    - DoD(国防部)
      - NSA(国家安全局)
      - DC3(网络空间犯罪中心)
      - JFT-JNO(全球网络行动联合小组)
      - DARPA(国防高级研究计划局)
    - DHS(国土安全部)
      - NPPD(国家保护和方案局)
      - USSS(特勤局)
    - DoS(国务院)
      - INR(情报研究局)
    - DoJ(司法部)
      - FBI(联邦调查局)
    - DoT(财政部)
      - TFI(恐怖主义及金融情报办公室)
    - DoE(能源部)
      - OICI(情报和反情报办公室)
  - 独立机构
    - CIA(中央情报局)
      - DI(情报处)
      - DO(行动处)
      - DS(支援处)
      - ……
    - ……

物理隔离
刀枪不入

一次网络战的预演

- **军用级别网络攻击武器扩散**：NSA军用网络攻击武器的泄露，为黑客提供了国家战略级网络武器，大大加强了恶意黑客组织的攻击能力，使黑客组织的攻击水平从组织级提升到了国家级。
- **暴露出来我国网络安全现状**：对物理隔离网络的盲目自信；恰恰是重要网络缺乏安全监测；终端防护成“重中之重”；常规防护措施无法应对“核弹”级武器；缺少专业团队的应急响应支撑

经济利益驱动

门槛日益降低

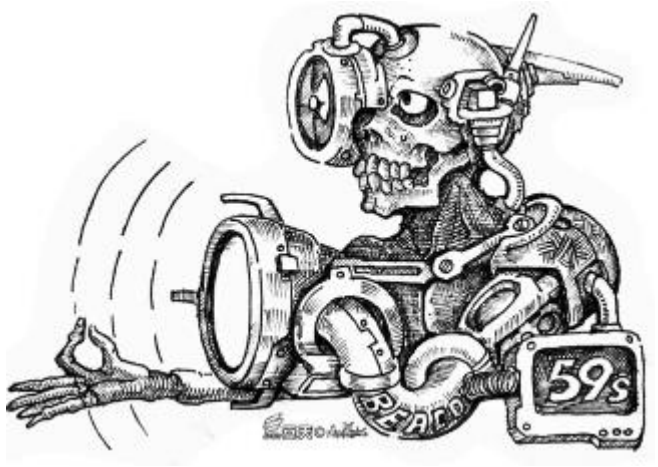
军用工具泄露

安全意识淡薄

防护措施不足

从战争视角看APT攻击

- 什么是APT
- 典型案例
- 为何网络攻击成为本质威胁



高级持续性威胁开启了新的威胁时代

攻击水平

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

国家和政治经济集团
为背景发动

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

作业意志

大国的网络安全能力要由攻击者和窥视者检验

	白象一代	白象二代
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标（如高等院校）	巴基斯坦和中国的大面积目标，包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE 双扩展名、打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114 CVE-2012-0158 CVE-2015-1761
二进制攻击载荷开发编译环境	VC、VB、DEV C++、AutoIT	Visual C#、AutoIT
二进制攻击载荷加壳情况	少数使用 UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10~16 人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

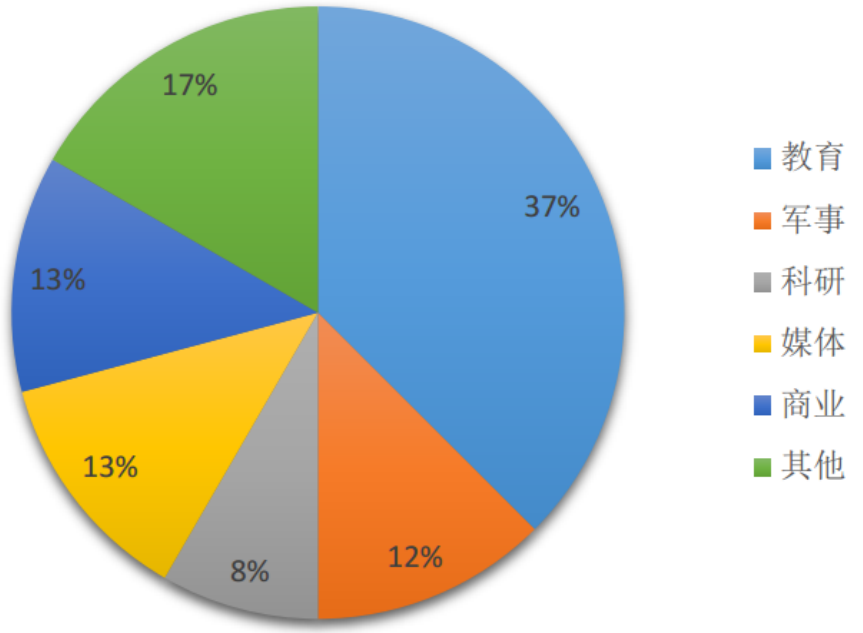
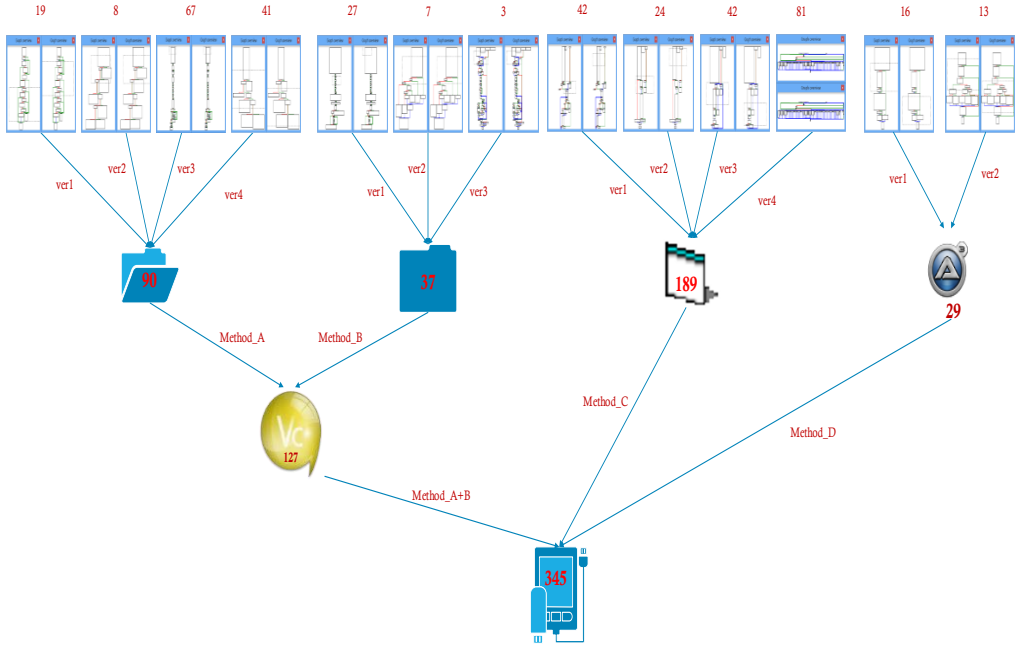
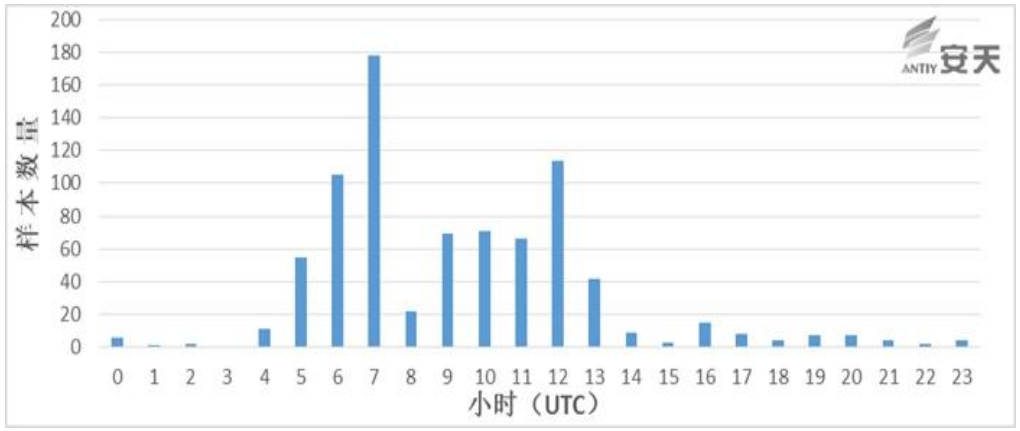


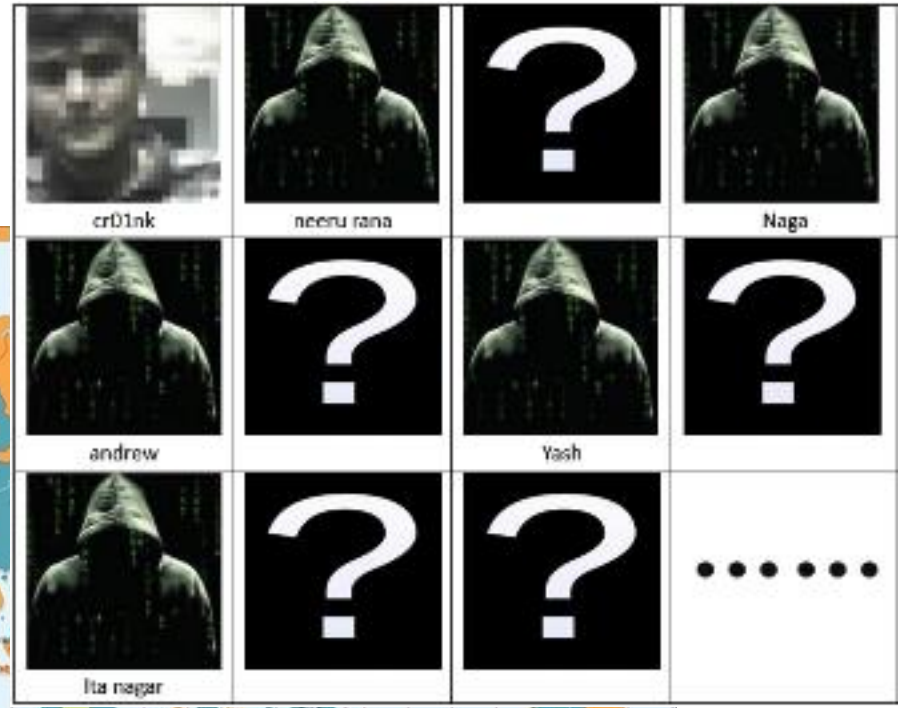
图 3-3 受害领域分布

引自安天技术报告《白象的舞步——来自南亚次大陆的网络攻击》，2016年7月10日首发

来自南亚次大陆某国的APT攻击组织 - 白象组织







安天“赛博超脑”所模拟的乌克兰停电事件

安天安全事件地理场景复现模块：全球近三年APT事件的目标和波及范围

信息安全威胁成为本质性威胁（1977~2006）

	调谢利刃与巴比伦行动（传统物理攻击伊拉克核反应堆）	奥林匹斯行动（网络空间攻击伊朗）
合作攻击方	以色列、美国、伊朗（两伊战争）	美国、以色列
被攻击方	伊拉克（没有成熟的自主国防体系，视图从法国“买来”核能力）	伊朗（有相对成熟的工业体系）
时间周期	1977-1981年	2006-2010年
人员投入	以色列空军、特工人员、伊朗空军、美国空军和情报机构	美、以情报和军情领域的软件和网络专家，还有工业控制和核武器的专家
作业准备	多轮前期侦察和空袭，核反应堆情报	战场预制、病毒的传播和、伊朗核设施情报
各方装备投入	伊朗：2架F-4鬼怪式以12枚MK82减速炸弹-轰炸核反应堆假设工地 10架F-4-袭击伊拉克H-3空军基地。 以色列：2架F-4E（S）-侦察任务；8架F-16A（美方提供）、4架F-15A、2架F-15B、16枚MK84炸弹-空袭反应堆 模拟搭建反应堆 特工人员暗杀伊拉克关键人员 美方：战略卫星和情报、空中加油机	美国： “震网”恶意代码 运维和控制体系 模拟搭建离心机和控制体系 以色列: “毒曲”恶意代码（环境采集准备）
效费比	打击快速，准备期长，耗资巨大、消耗大，行动复杂、风险高	周期长，耗资相对军事打击较低，但更加精准、隐蔽、不确定性后果更低
训练成本	18个月模拟空袭训练，2架F-4鬼怪攻击坠毁，3名飞行员阵亡。	跨越两位总统任期，经过了5年的持续开发和改进
消耗	人力、军力、财力、装备力、情报	人力、财力、情报
毁伤效果	反应堆被炸毁，吓阻了法国供应商，伊拉克核武器计划永久迟滞	导致1000台至2000台离心机瘫痪，铀无法满足武器要求，几乎永久性迟滞了伊朗核武器计划

网络武器可以有许多适应环境的属性。从生命周期成本的角度来看，它们比其他武器系统更优越。*这些系统都具有研究及开发成本，空间计划和传统平台也有很大的生产和部署成本，而网络武器的成本是最低的。网络和太空武器具有非常低的运营和维护成本，而传统武器系统的成本则是非常高的。总之，所有武器的成本曲线最初都是陡峭的，但是网络武器的下降速度最快，其次是空间武器，最后是传统平台。*

——Maren Leed（美国陆军参谋长高级顾问）

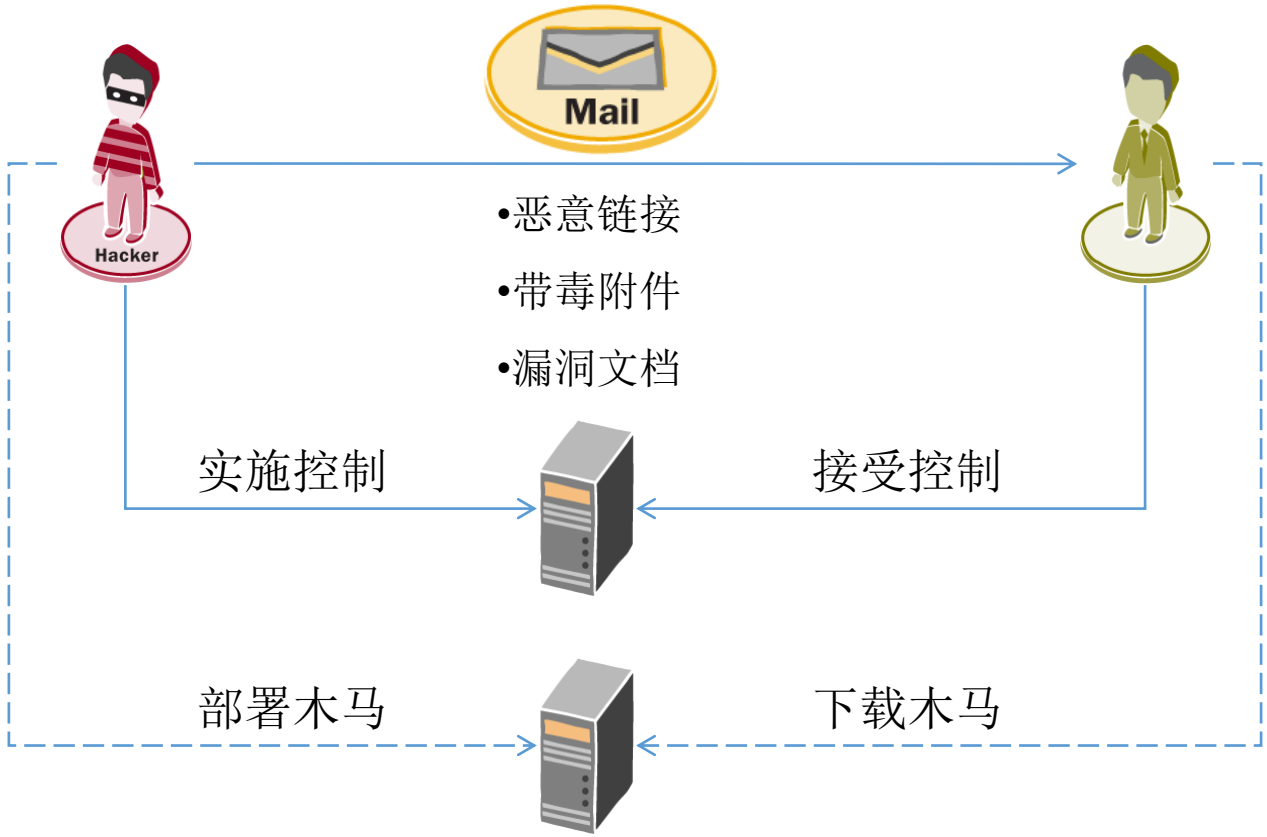
攻击关键基础设施的成本不断下降（2006~2015）

	震网事件	乌克兰变电站遭受攻击事件
主要攻击目标	伊朗核工业设施	乌克兰电力系统
关联被攻击目标	Foolad Technic Engineering Co（该公司为伊朗工业设施生产自动化系统） Behpajooh Co.Elec & Comp.Engineering（开发工业自动化系统） Neda Industrial Group（该公司为工控领域提供自动化服务） Control-Gostar Jahed Company（工业自动化公司） Kala Electric（该公司是铀浓缩离心机设备主要供应商）	乌克兰最大机场基辅鲍里斯波尔机场 乌克兰矿业公司 乌克兰铁路运营商 乌克兰国有电力公司UKrenergo 乌克兰TBS电视台
作用目标	上位机（Windows、WinCC）、PLC控制系统、PLC	办公机（Windows）、上位机（Windows）
造成后果	大大延迟了伊朗的核计划	乌克兰伊万诺-弗兰科夫斯克地区大面积停电
核心攻击原理	修改离心机压力参数、修改离心机转子转速参数	通过控制SCADA系统直接下达断电指令
使用漏洞	MS08-067（RPC远程执行漏洞） MS10-046（快捷方式文件解析漏洞） MS10-061（打印机后台程序服务漏洞） MS10-07（内核模式驱动程序漏洞） MS10-092（任务计划程序漏洞） WINCC口令硬编码	未发现
攻击入口	USB摆渡[24] 人员植入（猜测）	邮件发送带有恶意代码宏的文档
前置信息采集和环境预置	可能与DUQU、FLAME[19][20]相关	BlackEnergy采集打击一体
通讯与控制	高度严密的加密通讯、控制体系	相对比较简单
恶意代码模块情况	庞大严密的模块体系，具有高度的复用性	模块体系，具有复用性
抗分析能力	高强度的本地加密，复杂的调用机制	相对比较简单，易于分析
数字签名	盗用三个主流厂商数字签名	未使用数字签名
攻击成本	超高开发成本 超高维护成本	相对较低

不同水平的APT攻击

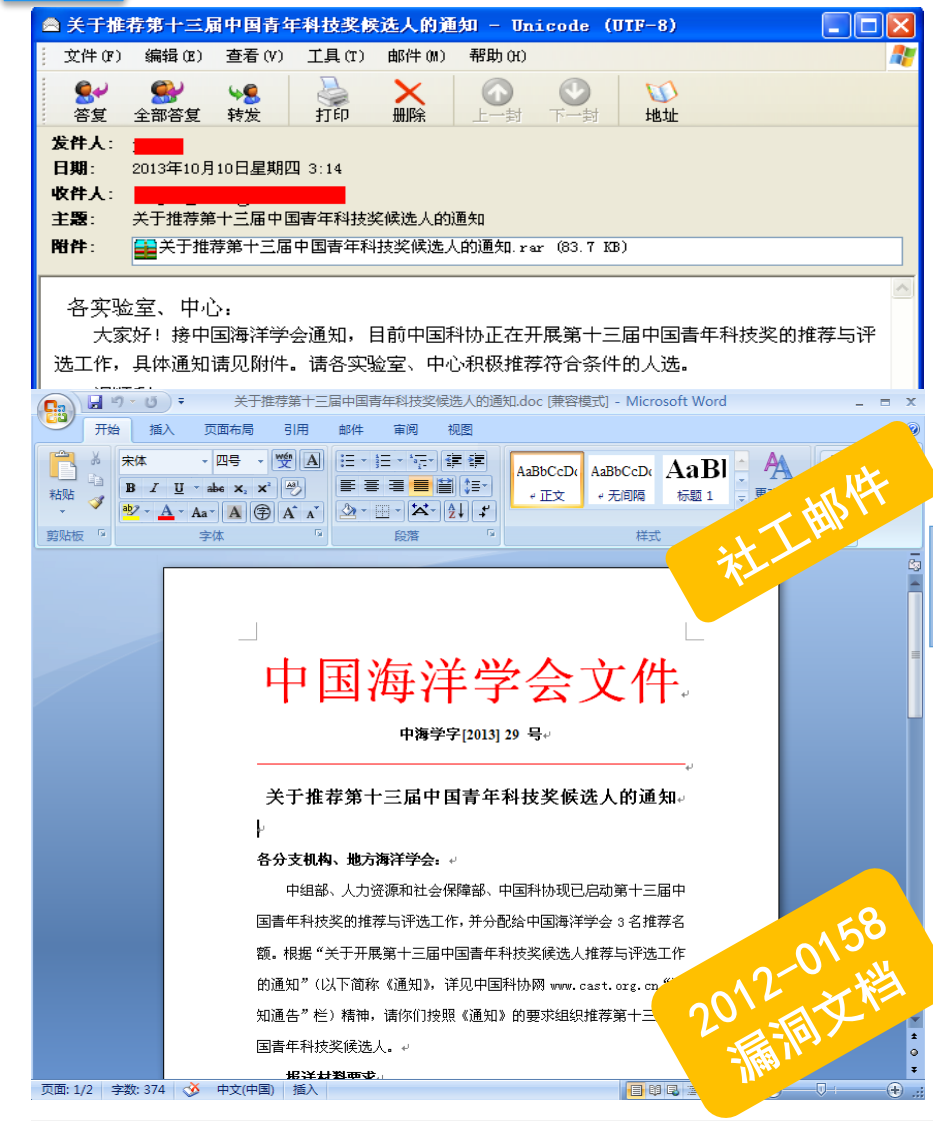
- 典型APT攻击方法
- 不同攻击能力对手

鱼叉式钓鱼 (Spear Phishing)



1. 攻击者部署木马服务器
2. 攻击者构造钓鱼邮件
3. 受害者下载木马并执行
4. 受害者接受控制

基础IT环境的对抗



社工邮件

2012-0158
漏洞文档

下载二进制样本

根据已有样本分析配置后，统计的出样本收集文档的类型：

.doc、*.xls*、*.ppt*、*.wps*、*.pdf

- 获取 IE 自动保存的邮箱账户密码和对应网址，对 IE6 和 IE6 以上的版本采取不同的方法。
- 收集网络信息，主机信息，进程信息，记录在%Application Data%\Microsoft\Windows\Profiles.log
- 样本根据各自的配置，收集全盘包含指定关键字的文件路径、收集 C盘 Program Files 目录下的 EXE 文件，将收集到的文件路径信息同样记录在 Application Data\Microsoft\Windows\Profiles.log。

图 27 收集指定关键文件列表

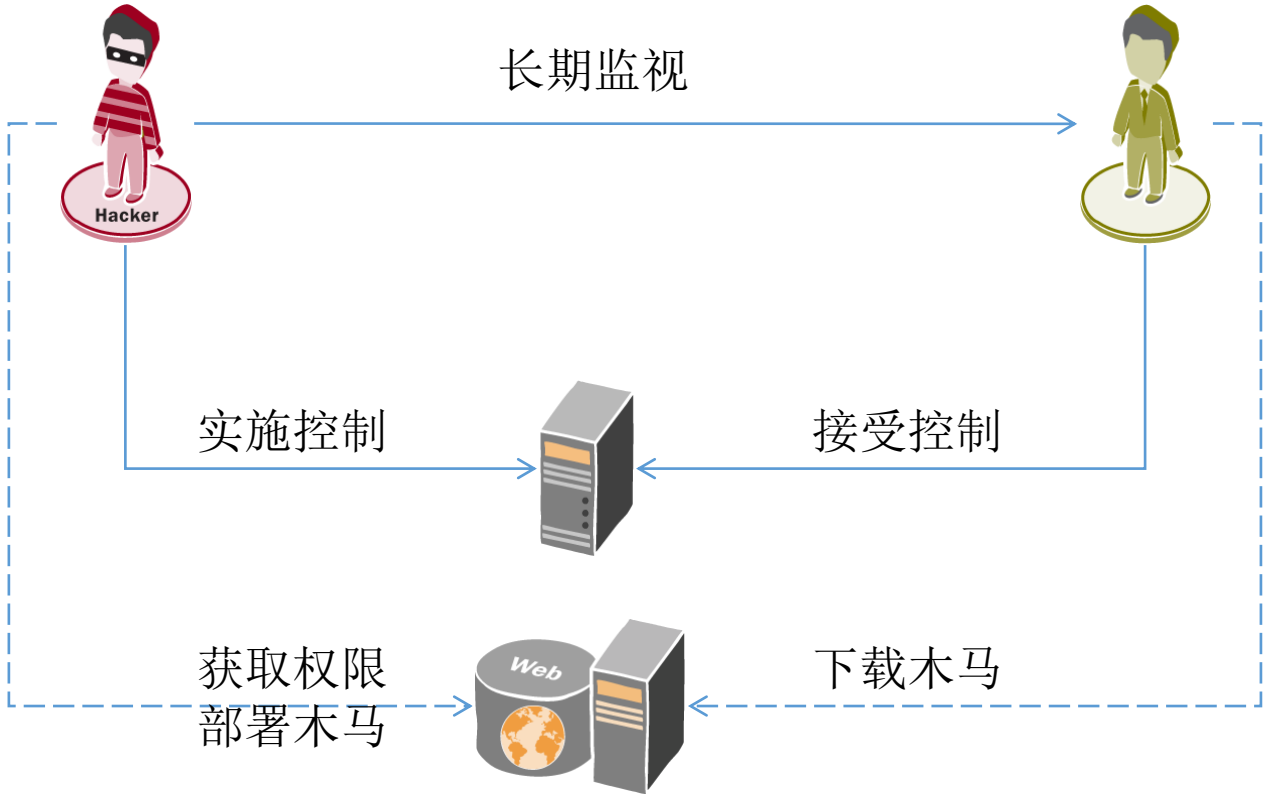
根据目前已捕获样本，我们总结出该系列样本关注的关键字，各个[redacted]列关键字中的三个，根据关键字对攻击目标进行收集操作。

二进制样本特点

在安天监控到的国内机构用户遭遇到APT攻击的案例中有较大比例邮件是发送向关键人员个人邮箱的。而根据安天统计，国内政府机构网站预留信箱中49%使用的是个人免费信箱。这导致威胁的离散，难以有效感知分析。

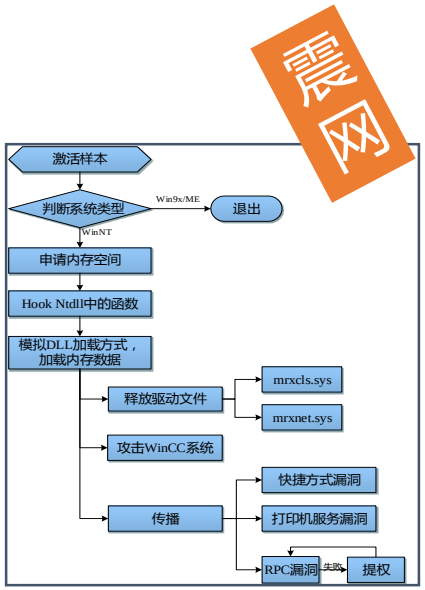
引自安天内部报告《针对中国政府机构的一系列针对性攻击事件的阶段性分析报告》

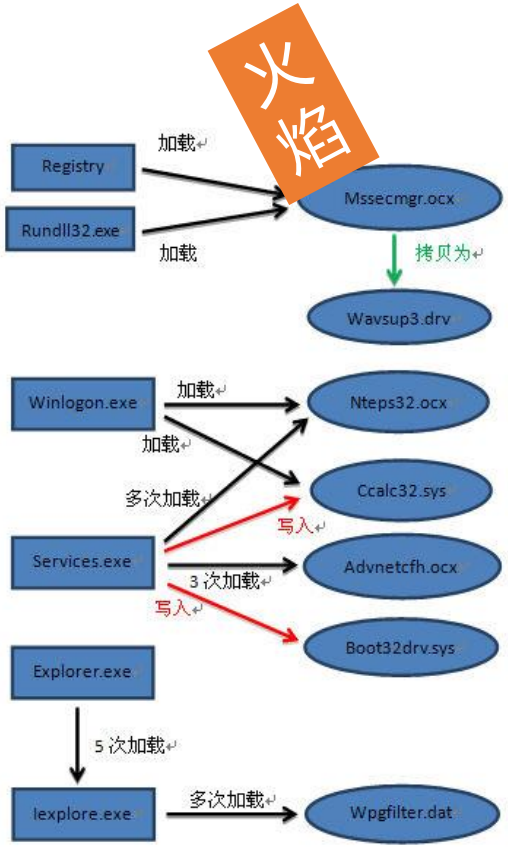
水坑式攻击 (Sinkhole)

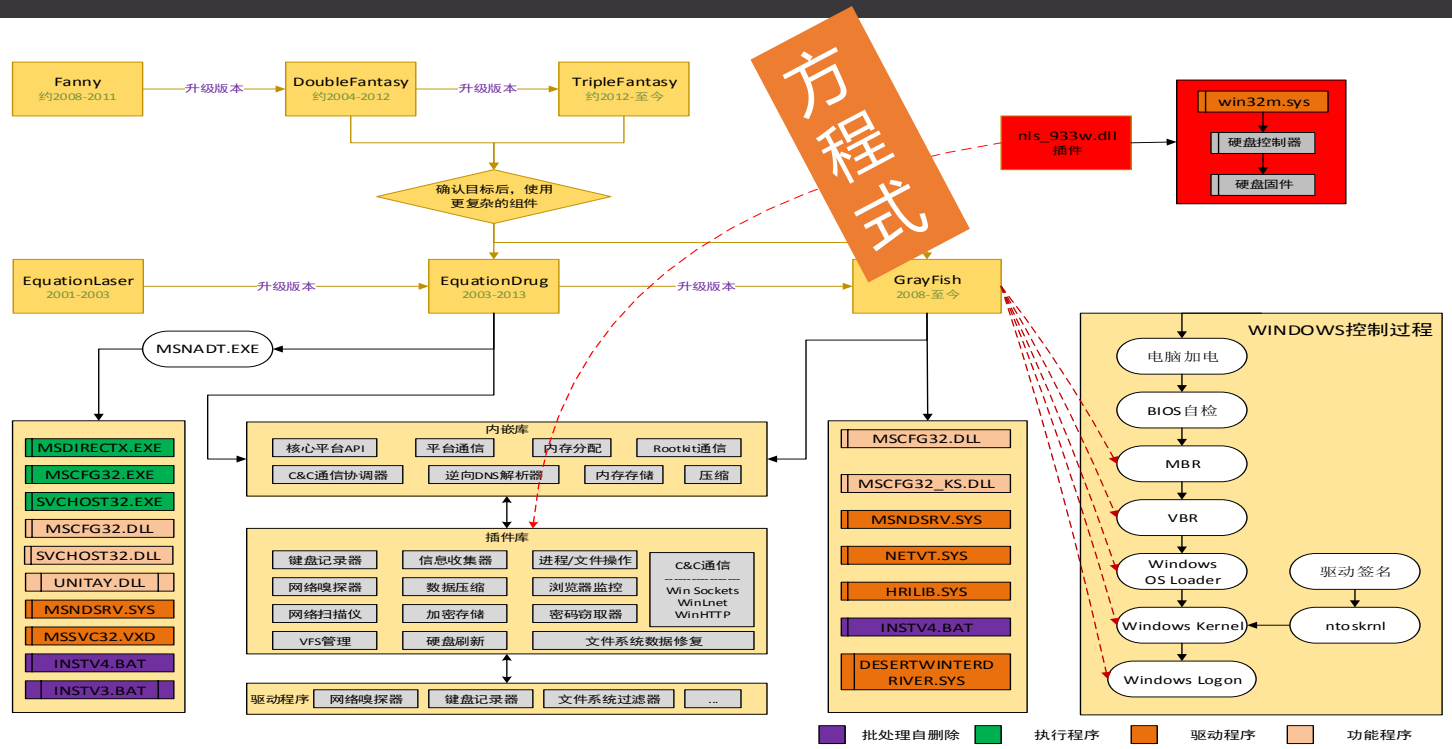


1. 攻击者监测目标网络使用习惯
2. 攻击者获取目标网络权限
3. 受害者访问被
4. 受害者接受控制

规模：恶意代码的复杂度和工程规模持续提升

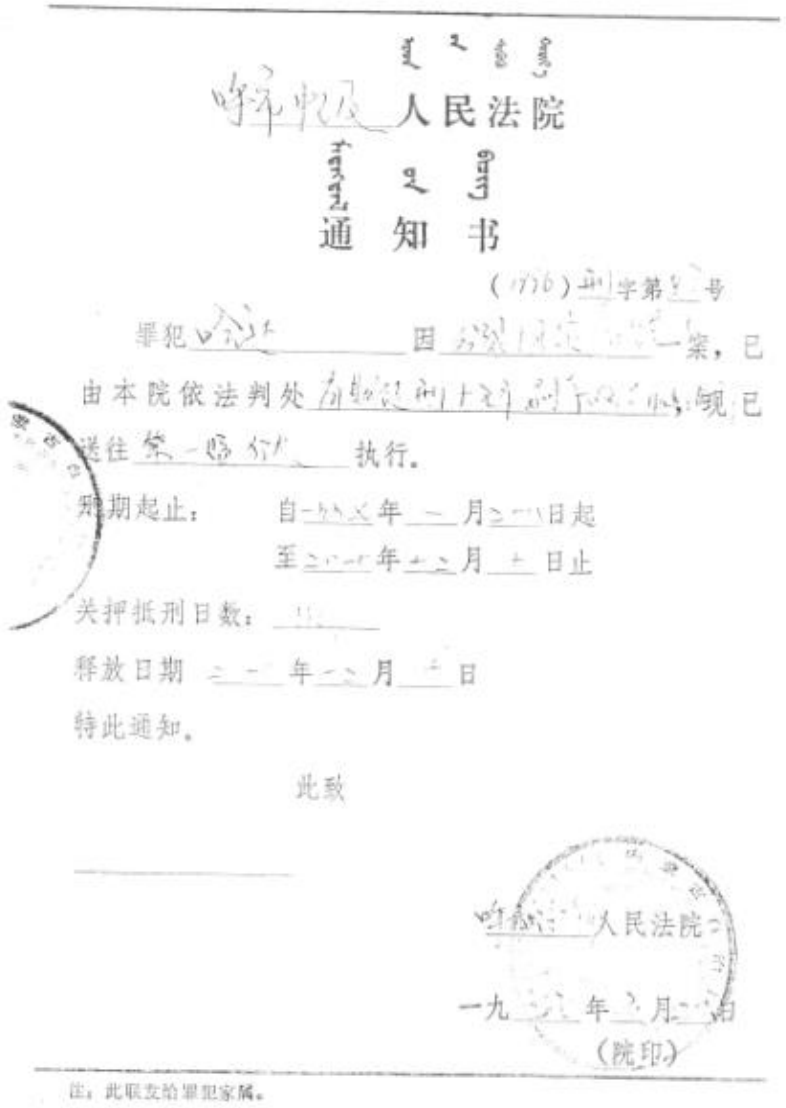






图片分别引自：安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》、**《Flame蠕虫样本集分析报告》和《方程式组件加密策略分析》， A²PT攻击中的恶意代码工程规模已经在几十万行代码到百万行规模。**

当然……也有“鸟枪”



人民法院

通 知 书

（1776）刑字第 号

罪犯 因 一案，已由本院依法判处 ，现已送往 执行。

刑期起止：自 年 月 日起至 年 月 日止

关押抵刑日数：

释放日期 年 月 日

特此通知。

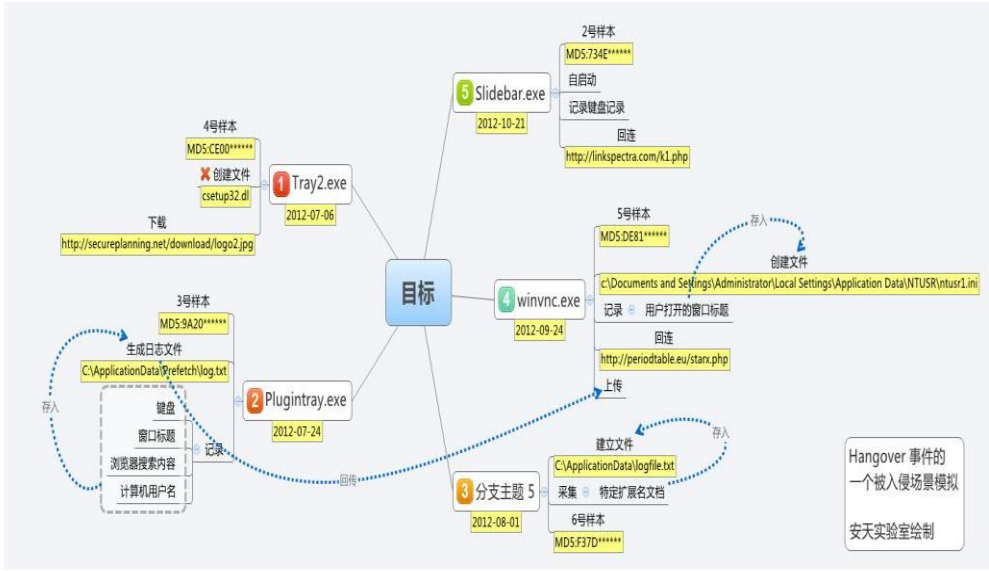
此致

人民法院

一九 年 月 日

（院印）

注：此联发给罪犯家属。



Sample	卡巴	BitDefender	微软	江民	小红伞	McAfee	金山	瑞星	Norton	命中率
Sample 1										0/9
Sample 2	✓	✓		✓	✓					4/9
Sample 3		✓						✓	✓	3/9
Sample 4										0/9
Sample 5	✓									1/9
Sample 6										0/9
以上是样本捕获时入库对照扫描结果										
Sample 1	✓	✓	✓		✓					4/9
Sample 2	✓	✓	✓	✓	✓				✓	6/9
Sample 3	✓	✓	✓	✓	✓				✓	6/9
Sample 4	✓	✓		✓	✓				✓	5/9
Sample 5	✓	✓			✓					3/9
Sample 6	✓	✓	✓	✓	✓			✓	✓	7/9
以上是 2013 年 08 月 20 日对应样本对照扫描结果										

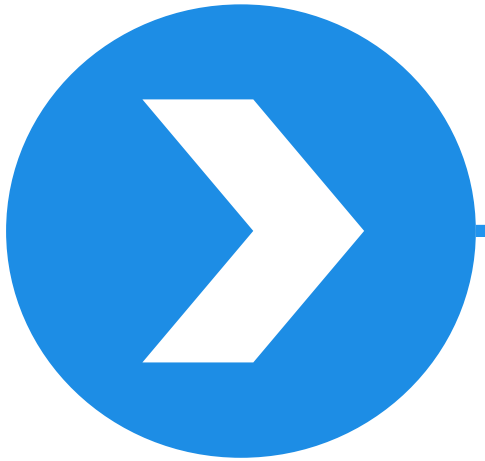
安天对白象I代中攻击的样本组合分析，可见其样本编写比较粗糙，缺少有效的Rootkit手段和加密通讯机制。仅仅在投放前经过了免杀处理。

鸟枪换炮：商业军火引发的军备扩散

网络商业军火的“军火商”

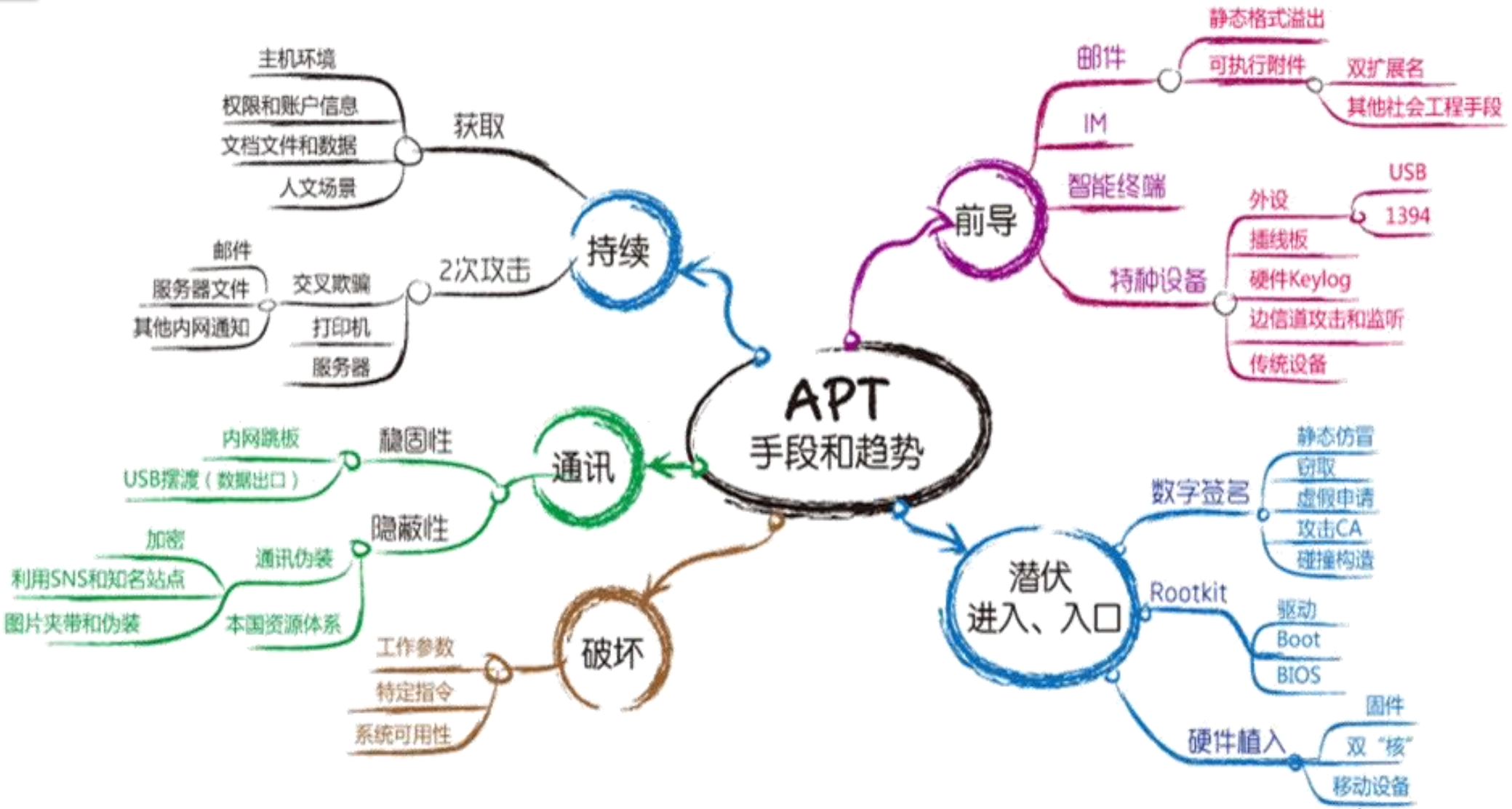
- Cobalt Strike作者：Raphael Mudge（美国）
  - LLC创始人（the creator of Armitage and founder of Strategic Cyber LLC, develops Cobalt Strike）；
  - 基于华盛顿的公司为RED TEAM开发软件，为Metaslpoit创造了Armitage、sleep程序语言和IRC客户端jIRCii；
  - 曾是美国空军的安全研究员，渗透实验的测试者；
  - 他设置发明了一个语法检测器卖给了Automattic；
  - 发表多篇文章，定期进行安全话题演讲，给许多网络防御竞赛提供RED 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

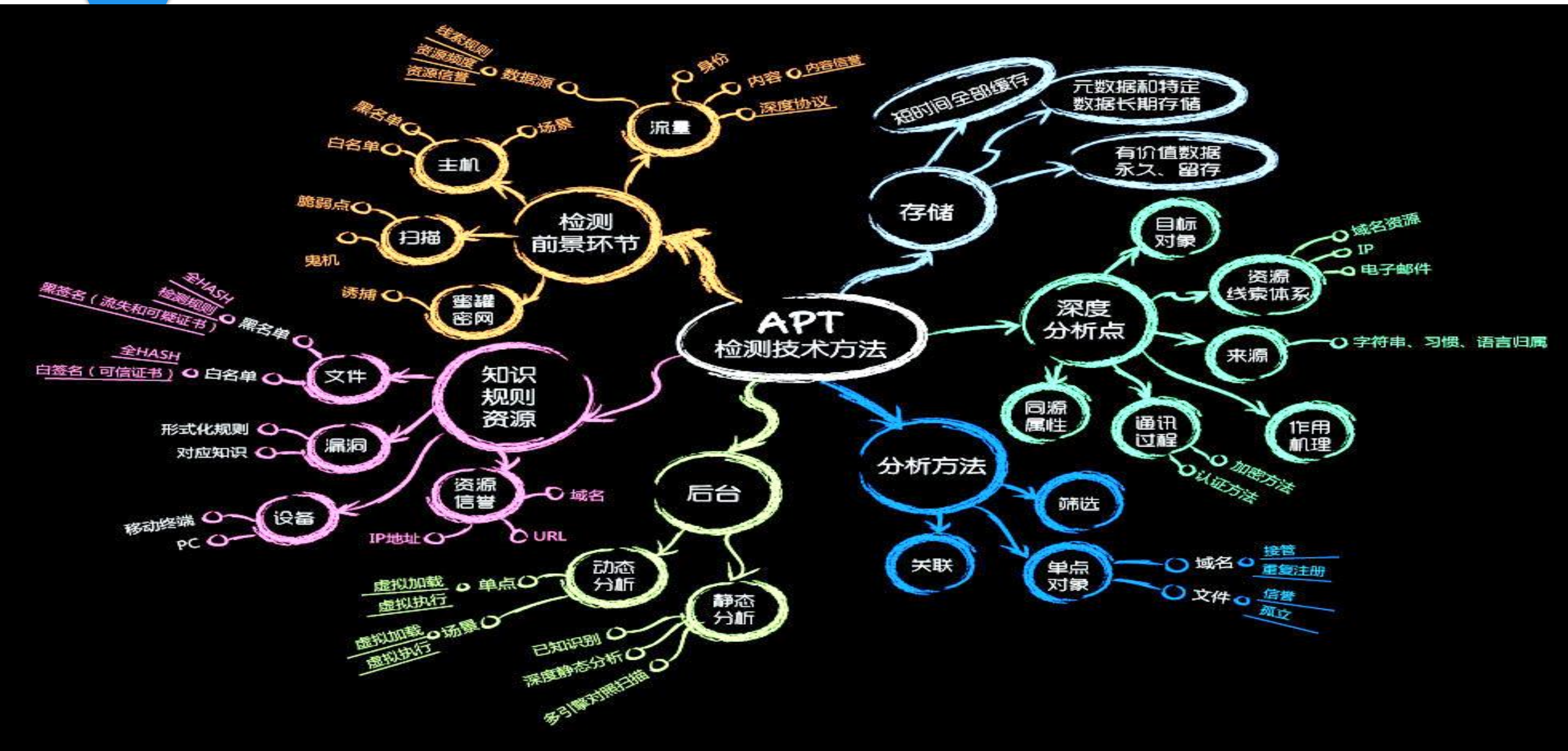


防御——布防、支撑与全域融合

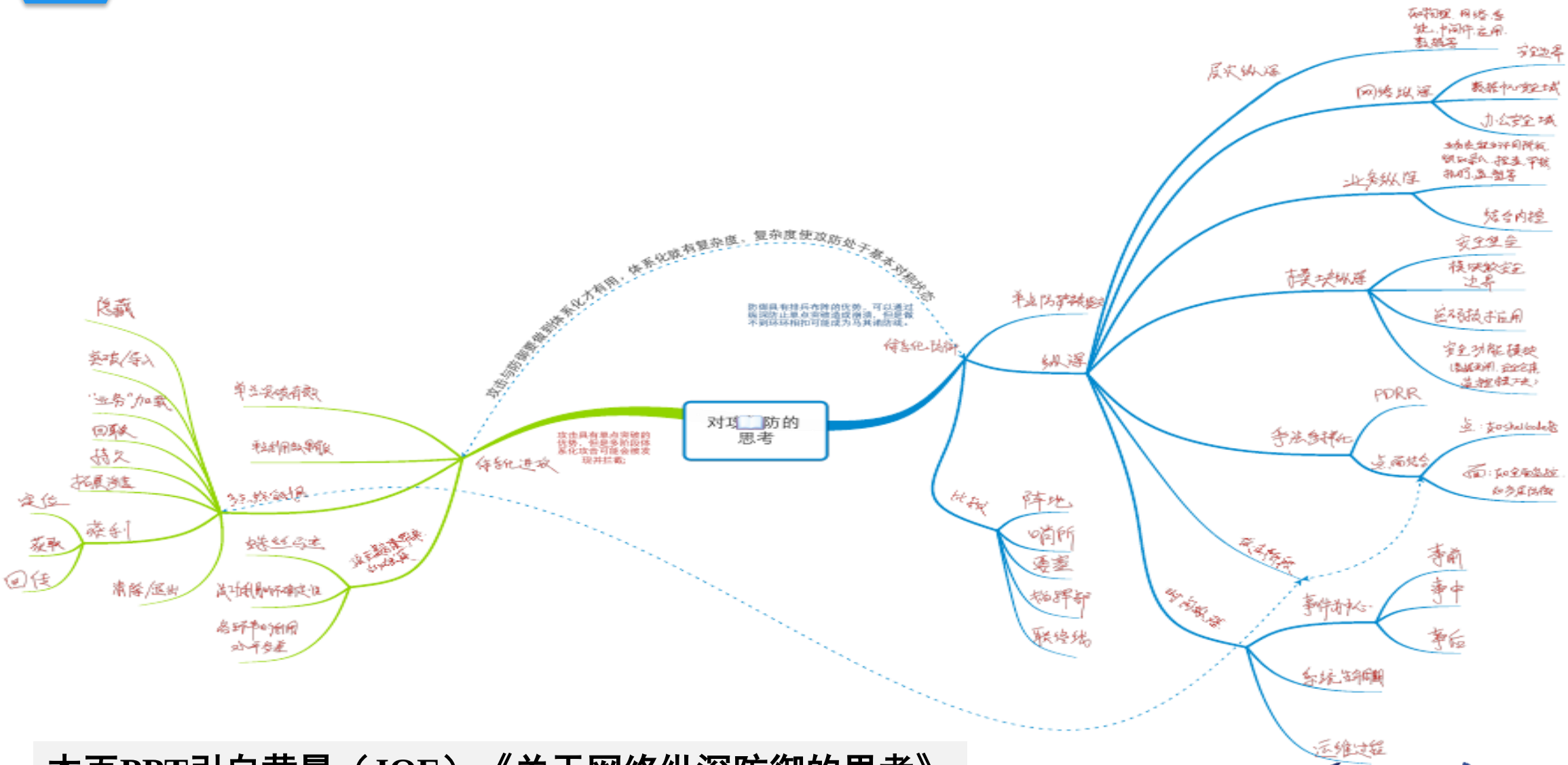
高级持续威胁是攻击方法和技巧的集大成者



从方法对抗到体系对抗


APT
检测技术方法
检测
前景环节
流量
数据源
线索规则
资源频度
资源信誉
身份
内容
内容信誉
深度协议
主机
黑名单
白名单
场景
扫描
脆弱点
鬼机
蜜罐
密网
诱捕
知识
规则
资源
文件
全HASH
检测规则
黑签名（流失和可疑证书）
黑名单
全HASH
白签名（可信证书）
白名单
漏洞
形式化规则
对应知识
设备
移动终端
PC
资源
信誉
域名
IP地址
URL
后台
动态
分析
虚拟加载
虚拟执行
单点
虚拟加载
虚拟执行
场景
静态
分析
已知识别
深度静态分析
多引擎对照扫描
存储
短时间全部缓存
元数据和特定
数据长期存储
有价值数据
永久、留存
深度
分析点
目标
对象
资源
线索体系
域名资源
IP
电子邮件
来源
字符串、习惯、语言归属
同源
属性
通讯
过程
加密方法
认证方法
作用
机理
分析方法
筛选
关联
单点
对象
域名
接管
重复注册
文件
信誉
孤立

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》

安天网络安全态势感知平台

系统运维支撑

权限管理
- 身份认证
- 权限管理
- 访问日志
- 安全审计

运维管理
- 设备配置
- 策略配置
- 运行监控
- 数据备份
- 系统日志
- 错误告警

时钟管理
- 时钟同步

升级管理维护
- 升级管理
- 版本记录

态势感知

- 数据综合分析挖掘
- 掌握网络攻击情况
- 掌握自身网络安全隐患

安全监测

- 监测网络受到的攻击威胁
- 监测系统的安全状况

追踪溯源

- 可视化关联搜索
- 线索挖掘与分析

通报预警

- 汇总、分析、研判威胁情报
- 威胁情况的上报、通报、下达

深度分析、关联挖掘与业务逻辑处理

- 样本深度分析
- 可视化关联引擎
- 数据包深度分析与回溯
- 时间扩展字段索引服务

数据中心

- 样本文件库
- 安全威胁与事件库
- IP/域名资源库
- 漏洞库
- 威胁情报库
- 资产库
- 其他库

事件与数据处理转化

主动获取数据下载与资源
- URL库
- 下载URL管理

数据处理转化
- 事件、数据消重与合并
- 事件初始关联
- 预设条件比对标签化
- 日志泛化处理

事件日志资源标准化
- 木马病毒传播
- 系统攻击
- APT攻击

事件临时存储
- 事件与系统资源接收处理
- 事件与系统资源接收

非标准日志
- 日志汇编
- 日志标准化
- 脚本模块管理器
- 非标准事件日志资源处理

二进制数据
- 二进制数据资源汇率
- 二进制数据资源处理

威胁信息采集

- 主机防御环节（智甲）
- 流量监测设备
- 扫描探测环节
- 蜜罐捕获设备

将我们的心力铸就新的长城！

THANK YOU FOR YOUR ATTENTION