制高点、地雷阵和火力支援

——纵深防御体系中的能力点思考

安天 肖新光

（2015/07/09 ●阿里安全峰会）

智者安天下

引子：从塔防说起

信息安全防御变得越来越困难，感觉不管采用怎么强悍的防御手段，都很快会被一些“精妙”的攻击所击破：

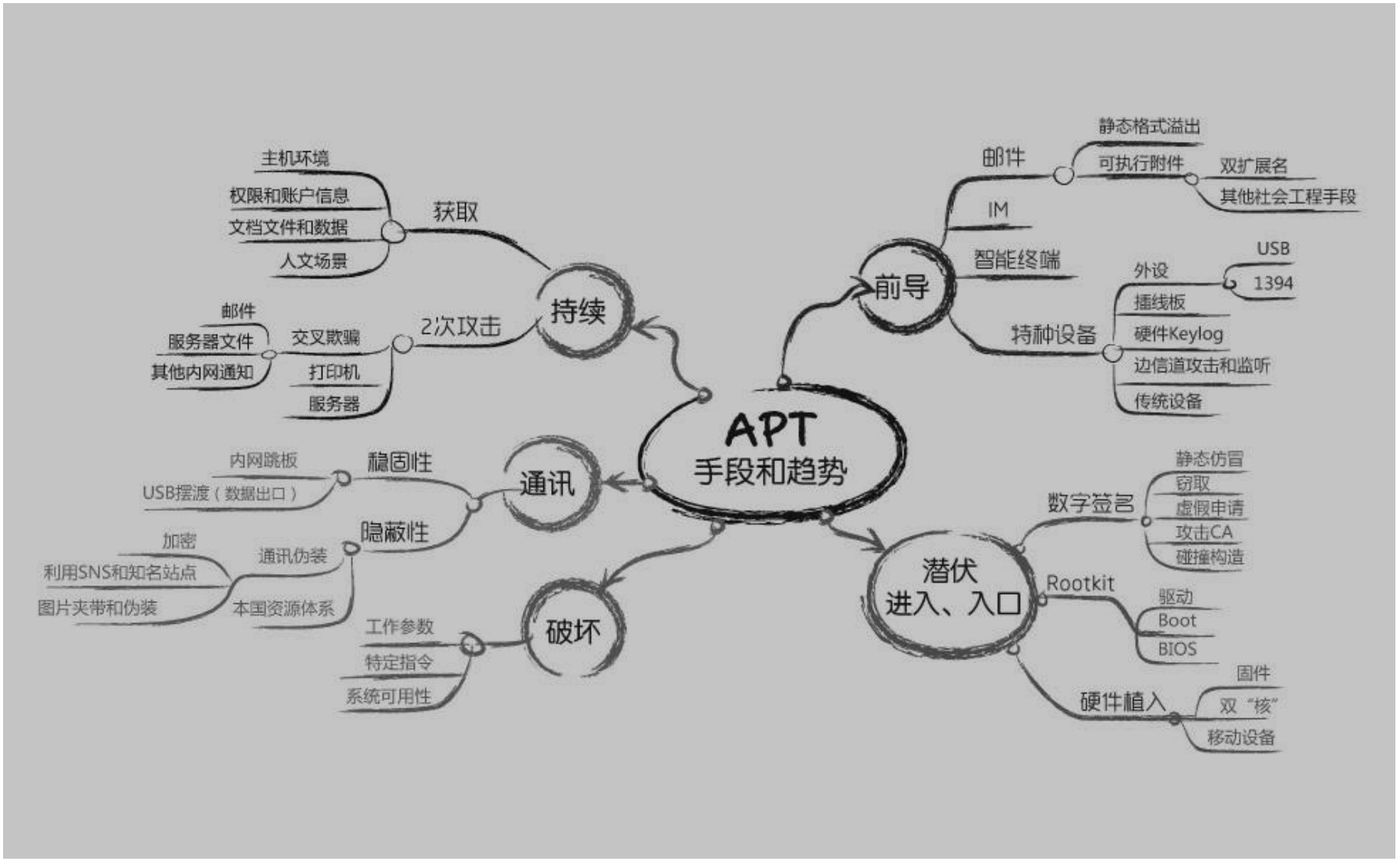
- APT攻击让传统防御手段变得形同虚设；
- 信息交互的刚需使网络隔离难以奏效；
- 各种宣称“解决一起安全问题”的防御技术很快被绕过...

信息安全防守看起来那么让人绝望，重要信息系统就像游戏中的BOSS那样，最终逃不过被打垮的命运...

页面引自中油瑞飞黄晟《关于网络纵深防御的思考》

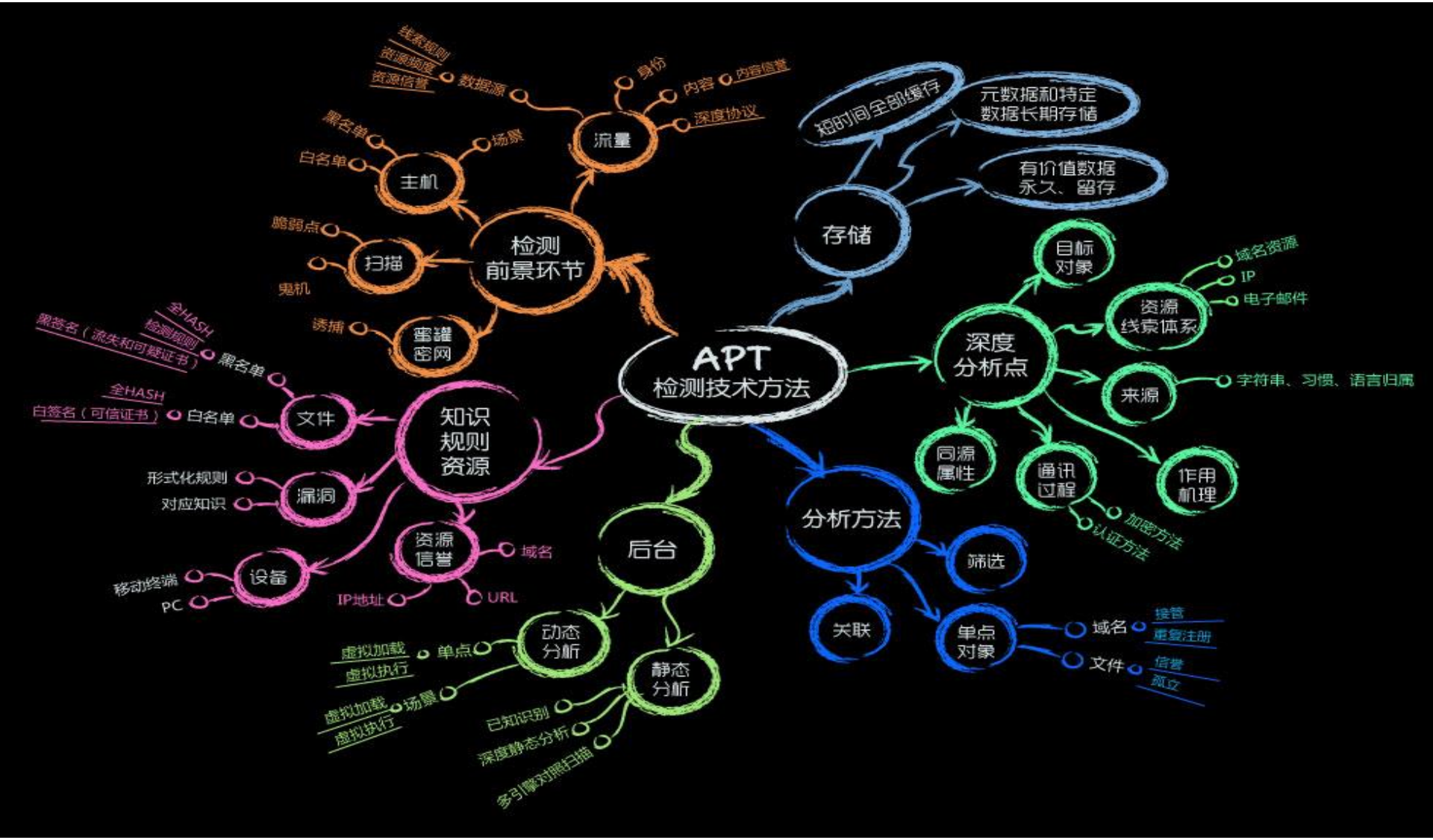
2014年10月的一个雾霾深重的下午，我在某机构小会议室第一次听到黄晟（JOE）讲解“塔防”的思想，并为了听完报告错过了航班。

对手.武器



引自演讲者报告《寻找APT的关键词（2013）》

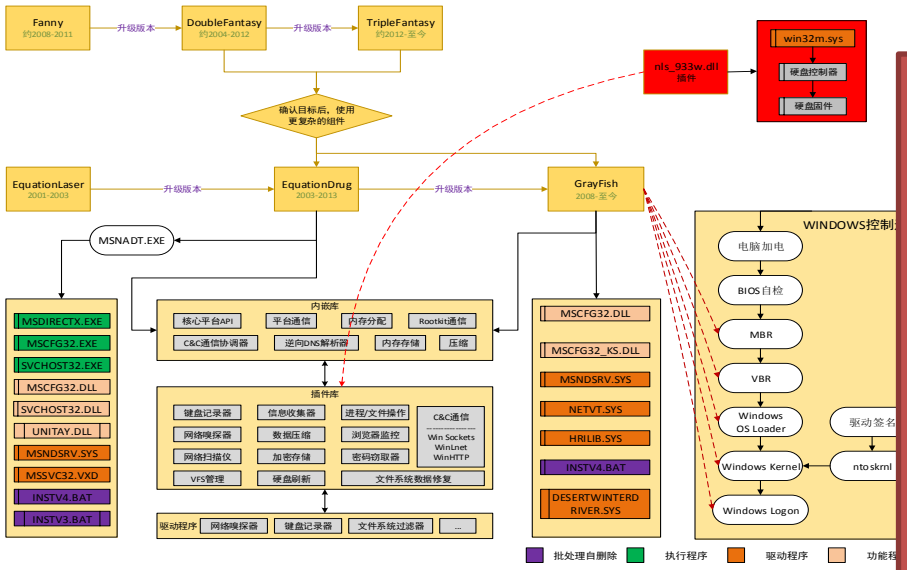
用户.装备



引自演讲者报告《寻找APT的关键词（2013）》

对手.实战

攻击可能是这样的



图引自安天《方程式（EQUATION）组件加密策略分析》

但攻击也可能是这样的

图引自安天《Hangover样本的跟踪挖掘》

但不管是哪样的对手，都把我们『搞定了』☺

神一样的对手：

有充足的0day储备
载荷部分高度复杂，高度模块化
本地加密抗分析，网络严格加密通讯和伪装
不一定通过网络植入，可能为人工植入和物流链劫持。
基本上完整普及了无文件载体技术，内存分段抗分析
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）
完整的覆盖所有操作系统平台（含移动）

猪一样的对手：

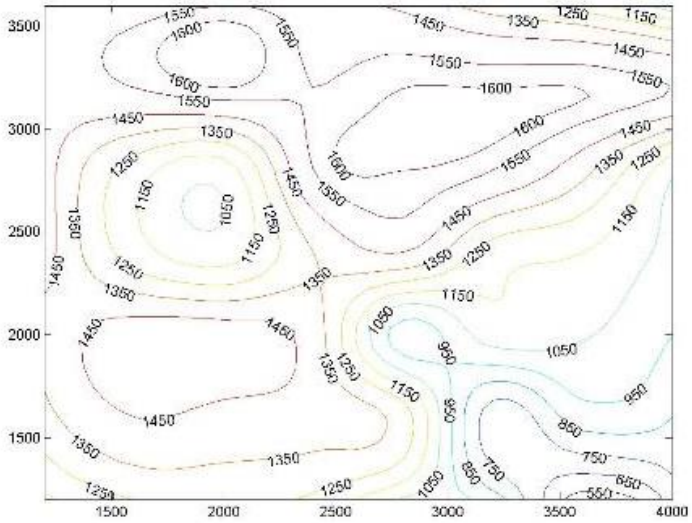
缺乏0day储备，很少使用
载荷编写质量低下
严重依赖网络投放
没有采用必要的Rootkit手段
缺少必要的持久化能力
主要针对Windows系统平台

防御.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

高点.布防

- 一种必须部署的基本能力
- 一种能够杀伤普通对手的能力
- 一种高级攻击者必须绕过的能力
- 传统的AV等基础检测能力才是“制高点”。
- 我们没有神话制高点



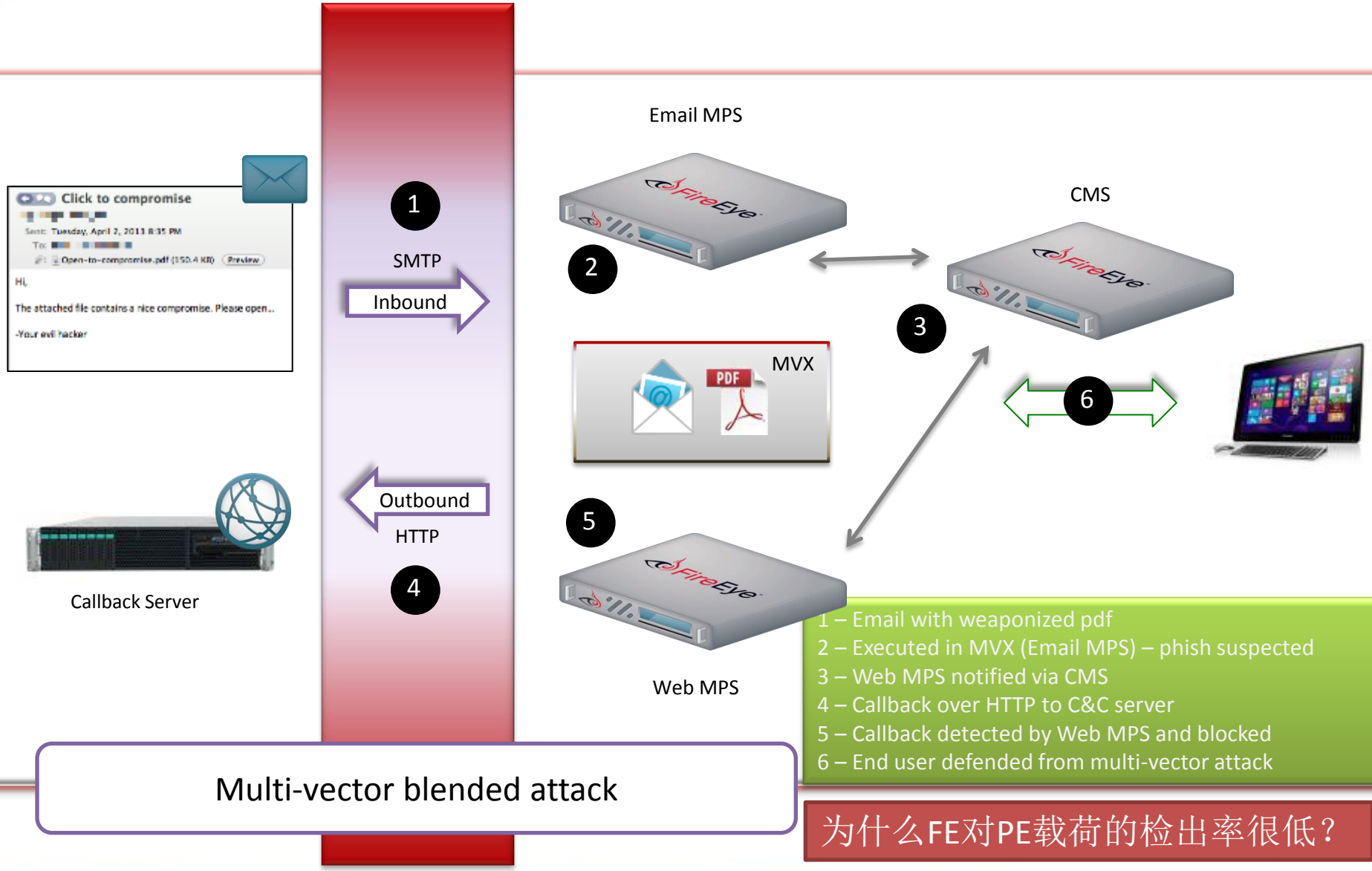
不论在防御和进攻中制高点都能产生一定的有利效果,这种效果是必须考虑的.....就便于运动这一点来说,高处的军队并不是绝对有利的,也不是在任何场合都是有利的。

——克劳塞维茨

导向.重读

- 关于不基于特征的未知威胁检测的导向
  - 恶意代码
  - 0day漏洞利用：shellcode、多种格式文件
- 2013美国国防预算法案932. b
  - 为了克服当前面临的问题和局限性，（下一代网络安全）系统不应依赖于：
  - a. 已知特征机制；
  - b. 需要经常更新的特征机制；
  - c. 需要以数据库形式存储下来的特征机制。
- 932. B真的宣告了传统AV技术的消亡么？

指标.疑惑

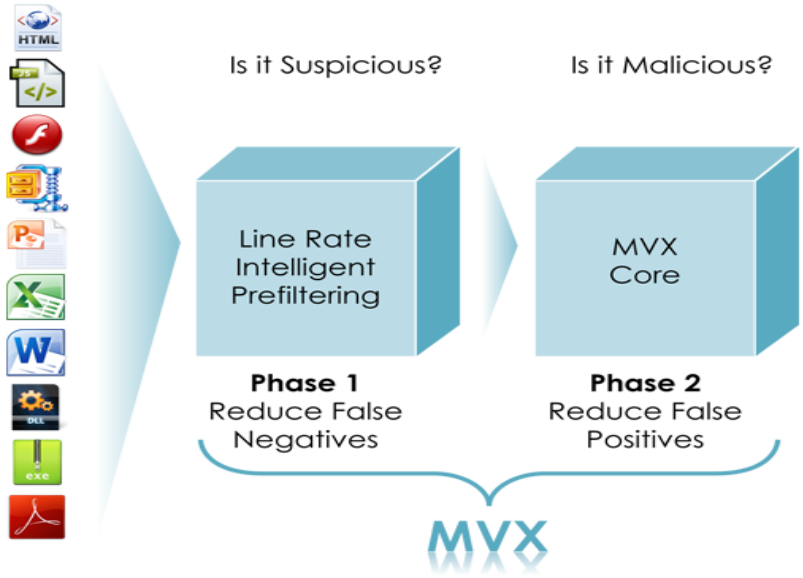


为什么FE对PE载荷的检出率很低？

图片引自Fireeye产品PPT，与本页主题无关

沙箱.反思

- 沙箱的核心优势是针对攻击中数据->指令转换的弱点。
- 在复合鉴定器中，绝大多数检出率是以传统AV为主导的静态机制贡献的。特别是针对PE、脚本等传统载荷。
- 沙箱针对PE对抗没有必然的优势，但其是行为细节（动态向量）的供应器。
- 沙箱本身是传统基础，其本身不是“下一代”技术。对格式攻击等的深度检测能力，以及对载荷行为的有效呈现才是其根本建制。



图片引自Fireeye产品文档，与本页主题无关

支点.平衡

FE的六的技术支点

- 场景组合分析
- 复杂流量分析
- 多向量分析
- 信息关联分析
- 云端能力
- 实时防护

图片引自Fireeye产品文档

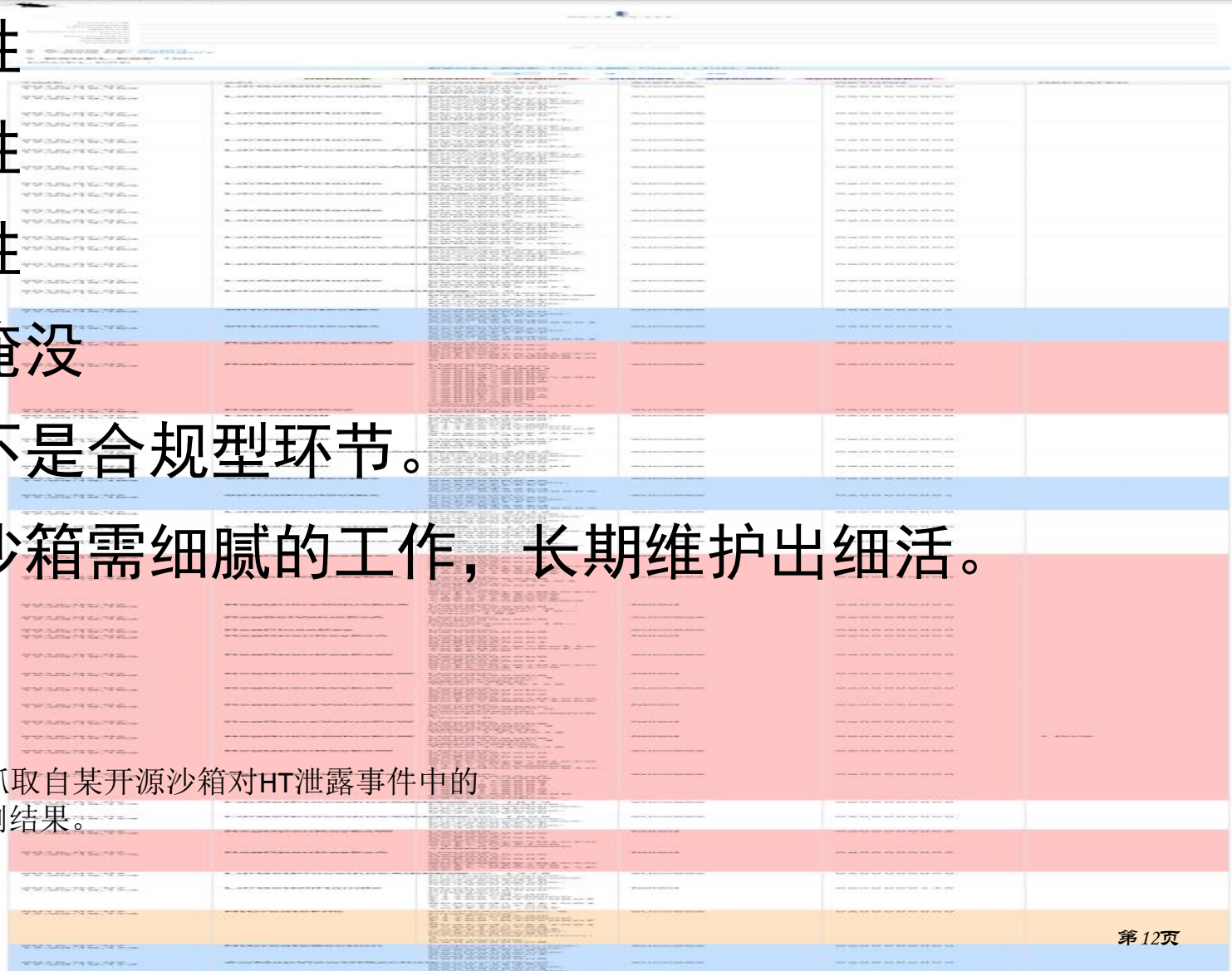
FireEye

相关思路的精华是什么？

- 安全性与保密性的平衡
- 云端能力和本地能力的平衡

沙箱的有无不解决问题

- 完整性
- 有效性
- 准确性
- 信息淹没
- 沙箱不是合规型环节。
- 做好沙箱需细腻的工作，长期维护出细活。



背景图片抓取自某开源沙箱对HT泄露事件中的某0day检测结果。

（AV）软肋.再看

562 software downloads results for "antivirus"

1 2 3 4 ··· 57 Next »

Sponsored match

Vipre Antivirus 2013
Version 6.0 | Added on 09/26/2012
Protect yourself against viruses and malware threats without slowing down your PC.
381,564 total downloads 2,064 last week
User rating out of 189 reviews
Download Now | Buy Now | Save to list

Sponsored match

Trend Micro Titanium Maximum Security 2013
Version 6.0.1215 | Added on 09/10/2012
Stop viruses and spyware automatically before they reach your computer.
Read CNET's review
147,171 total downloads 1,594 last week
Editors' rating
User rating out of 79 reviews
Download Now | Buy Now | Save to list

Sponsored match

acdONE Antivirus + Total Security
Version 15.0.33.1409 | Added on 04/03/2012
Protect your computer from emerging e-threats.
6,325 total downloads 383 last week
Download Now | Save to list

Sponsored match

G Data InternetSecurity 2013
Version 2012 | Added on 07/19/2012
Protect your PC against Trojans, viruses, and all kinds of malware.
1,806 total downloads 600 last week
User rating out of 2 reviews
Download Now | Buy Now | Save to list

Avast Free Antivirus
Version 7.0.1466 | Added on 08/21/2012
Protect your PC against the latest viruses and spyware.
Read CNET's review
216,605,103 total downloads 1,290,195 last week
Editors' rating
User rating out of 23648 reviews
Download Now | Save to list

virustotal

SHA256: 70d030e233bf740f22fc0f934b9eb1bf360bcef47a21b0b6f00a3d3a37690d4a
File name: 1F61D280067E2564999CAC20E386041C
Detection ratio: 37 / 44
Analysis date: 2012-10-20 01:57:09 UTC (0 分钟 ago)

More details

Analysis | Comments | Votes | Additional information

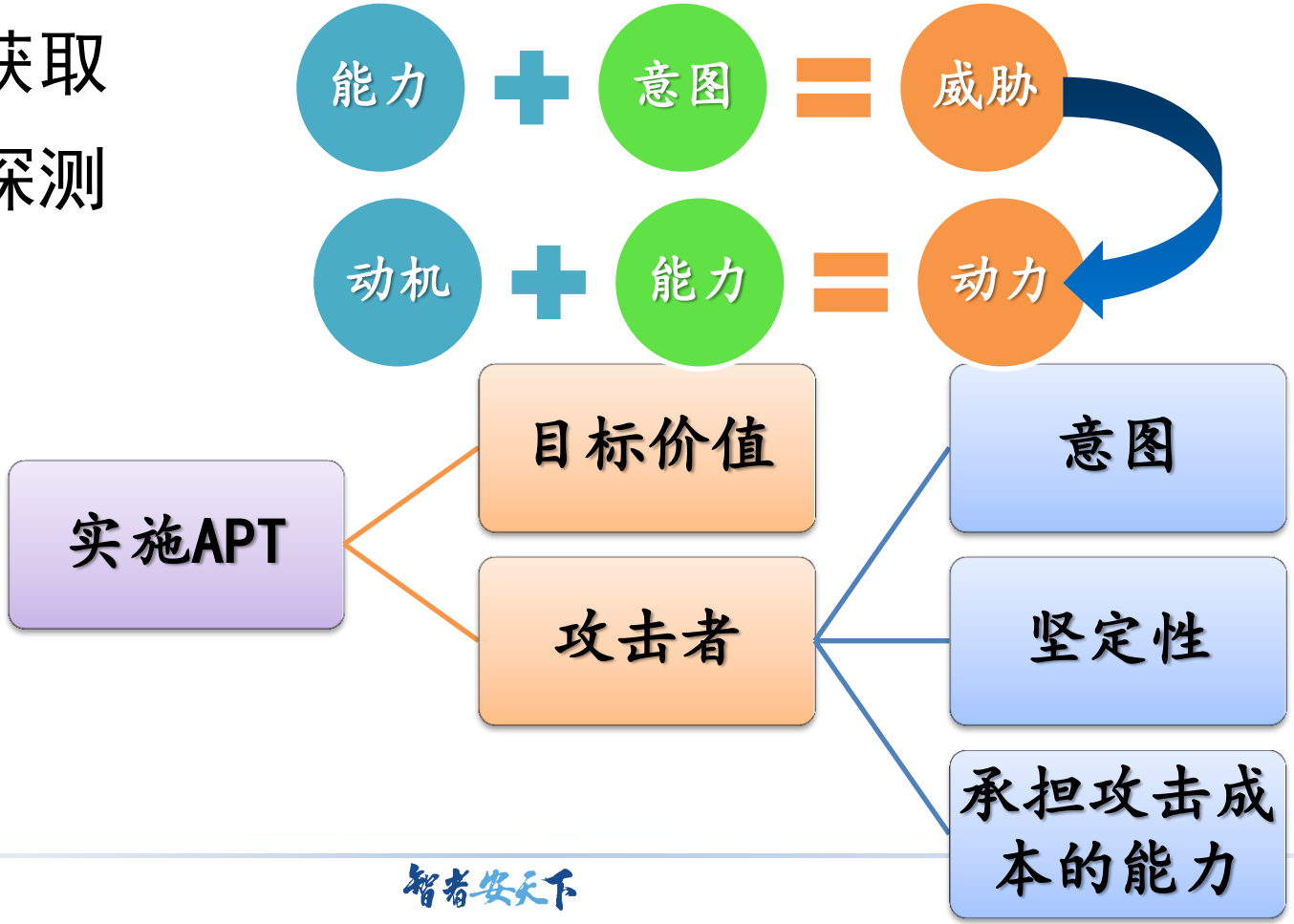
Antivirus	Result	Update
Agnitum	Worm.Flamer!7+VSA4dkgdk	20121019
AhnLab-V3	Win32/Flame.worm.29928	20121019
AntiVir	TR/ATRAPS.Gen	20121020
Antiy-AVL	Worm/Win32.Flame.gen	20121020
Avast	Win32:Skywiper-N [Trj]	20121019
AVG	Worm/Flame.A	20121020
BitDefender	Trojan.Flame.A	20121019
ByteHero	-	20121019
CAT-QuickHeal	-	20121019
ClamAV	-	20121019
Commtouch	-	20121020

AV-一种可以低成本获得的安全资源

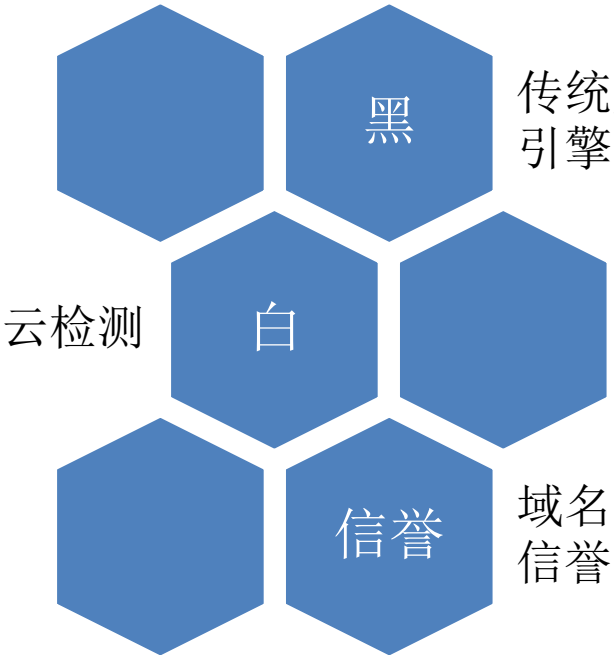
多引擎扫描工程已经非常成熟

（安全产品）软肋.泛化

- APT时代的为达成目标可以获取感知一切周边环节和阻碍的要素。
- 能力的获取
- 能力的探测



知识支撑与双向筛选



传统反病毒引擎

云检测

域名与网址信誉

可信

白名单

可信厂商的签名体系

用户端信誉

判定的高风险对象
已知的高风险对象
未判定对象

不可信的

已知黑名单对象

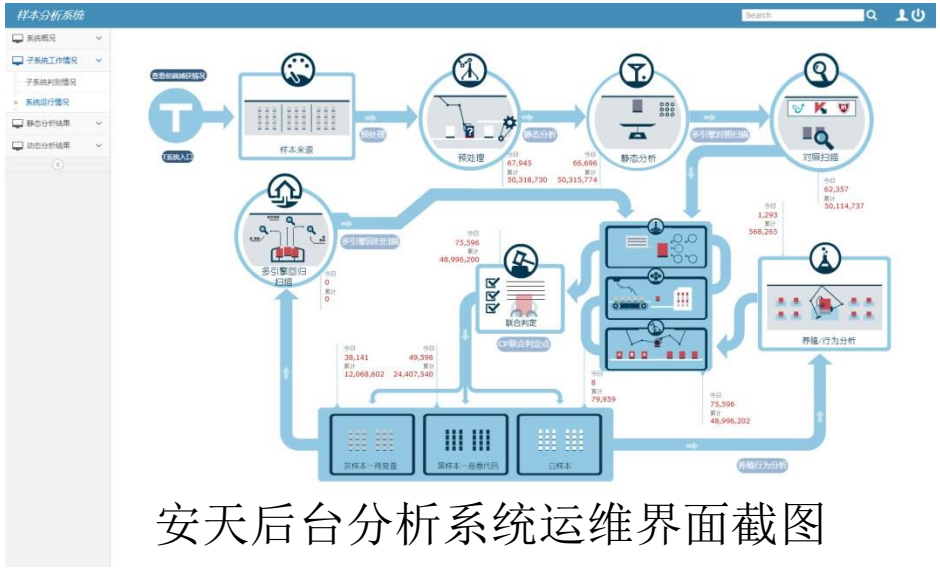
可疑的对象

生僻的对象

地雷阵.不确定性

- 通过制造不确定性来应对攻击，以及一个有趣的例子。
- 但攻击方同样可以通过承担成本的方式来判定不确定性对攻击方的影响。
- 只可言传，不可打字，因此省略若干字。

可探测性

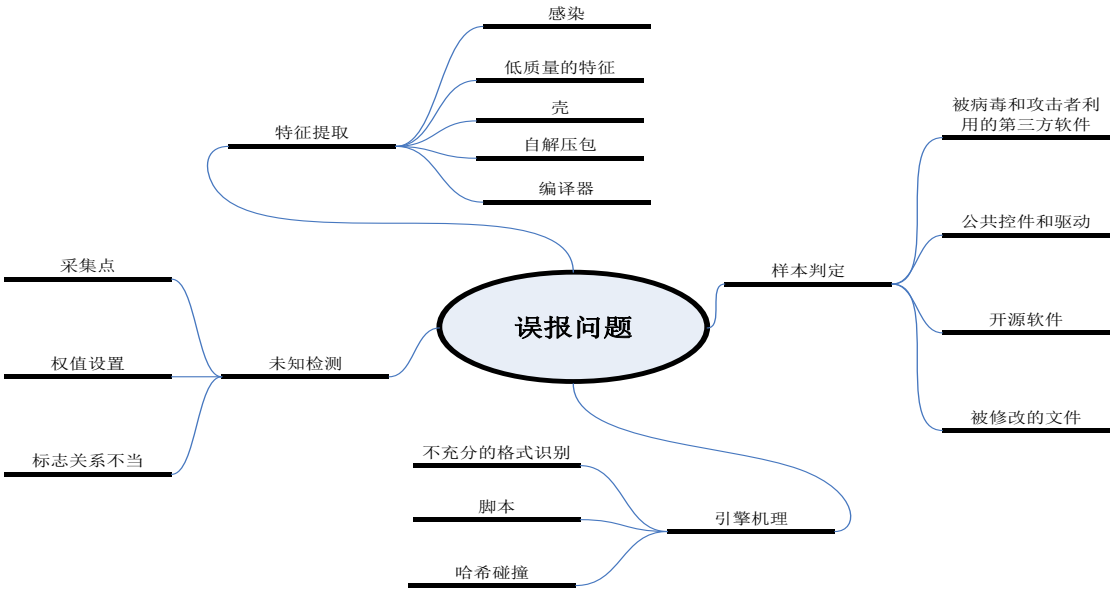


安天后台分析系统运维界面截图

- 产品能力是提供给用户的，但也是暴露在攻击者面前的。

- 产品能力来自其更大的支撑纵深。
- 但其同样是可探测的。

从误报构造攻击说起

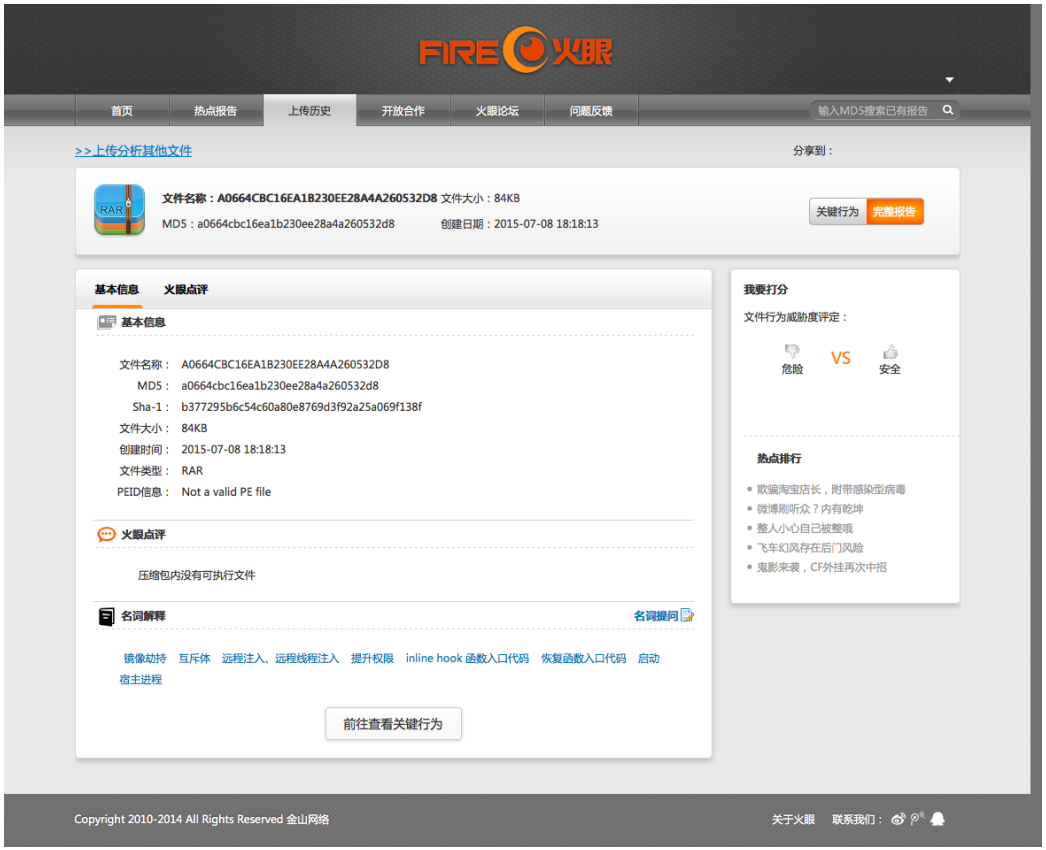


图引自安天《反病毒产品误报问题白皮书》

以我们目前经验判断，Symantec对微软系统文件的误杀，可能是外部发起的一系列误报构造攻击碰撞到了Symantec后台分析系统的一个错误的对比定义翻转。

——《关于赛门铁克查杀中文XP系统文件问题的事件分析（内部版）》

反馈是一种微妙东西



反馈本身是信息采集的动力
但反馈也增加攻击者探测分析的成功率

注：友商图片仅供装饰使用

“Camberdada”计划的警示

BRICKTOP (2009)

Tascom

RusComNet

Kaspersky

Rosoboron export

nstitute of Information & Analytical Technology (IIAT)

Moscow Telecommunication Corporation (ComCor)

Famatech

Comstar

Komet

Sample Email Received by an AV Vendor

PWZA20120510218350000197506

Good day,

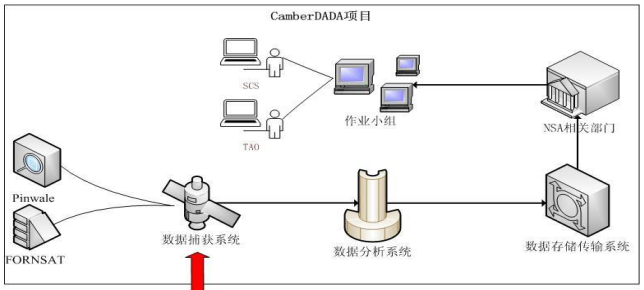
A phishing scam file is attached for your analysis.
Zip file password = **virus**

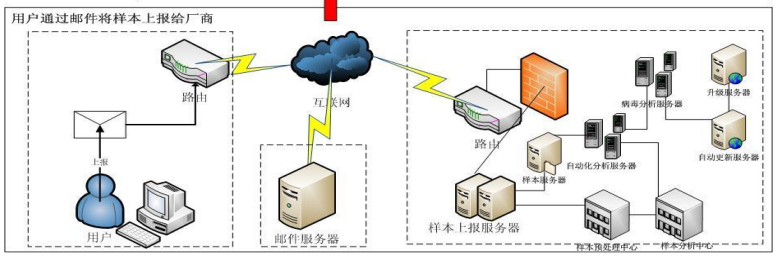
The file tricks the user into giving her/his bank account credentials. This can be verified by clicking on the *Sign In* button.

FYI: https://www.virustotal.com/file/8fb6447fdc9cfe204cde...

Regards,
Francois Picard
www.NewRoma.net

Attachment: BMOFinancialGroup.zip





英文名称	说明
Rosoboron export	俄罗斯国防产品出口公司
Institute of Information & Analytical Technology	信息与分析技术研究所
Tascom	莫斯科城市电话公司
MOSCOW Telecommunication Corporation	莫斯科电信公司
Komet	俄罗斯电信公司
Comstar	俄罗斯电信运营商
RusComNet	俄罗斯电信运营商
Famatech	软件公司，其软件产品 Radmin 为远程控制软件

左上、右上两图引自斯诺登泄露文档《An Easy Win：Using SIGINT to Learn about New Virues|Project Camberdada》

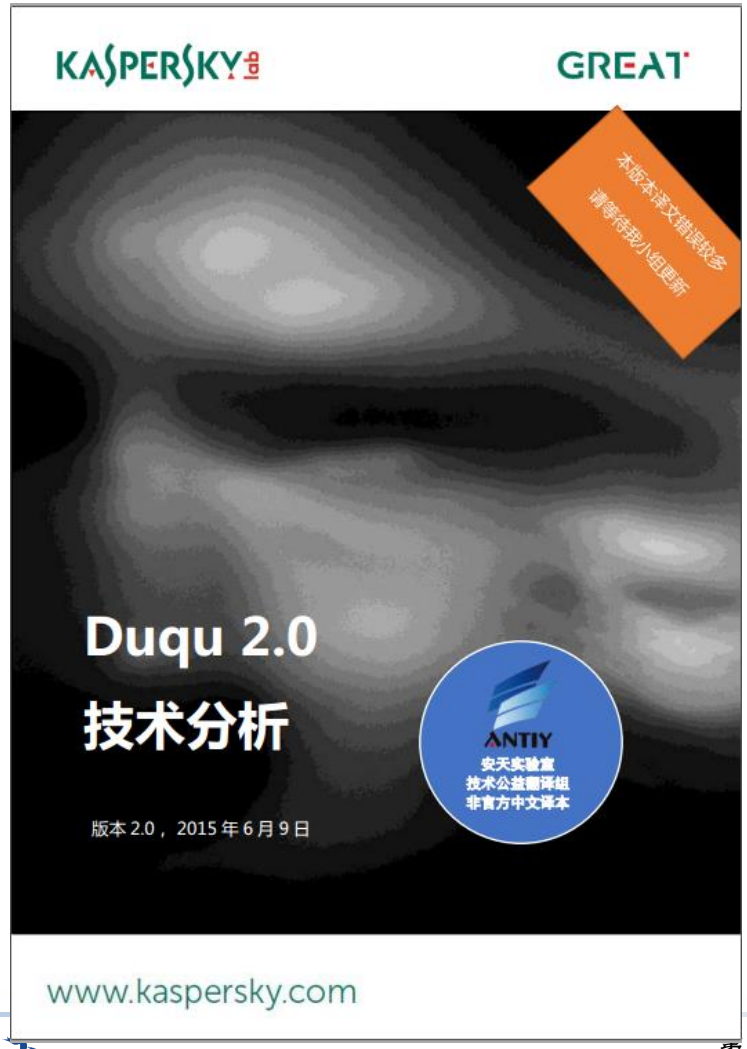
以及

2007

More Targets!

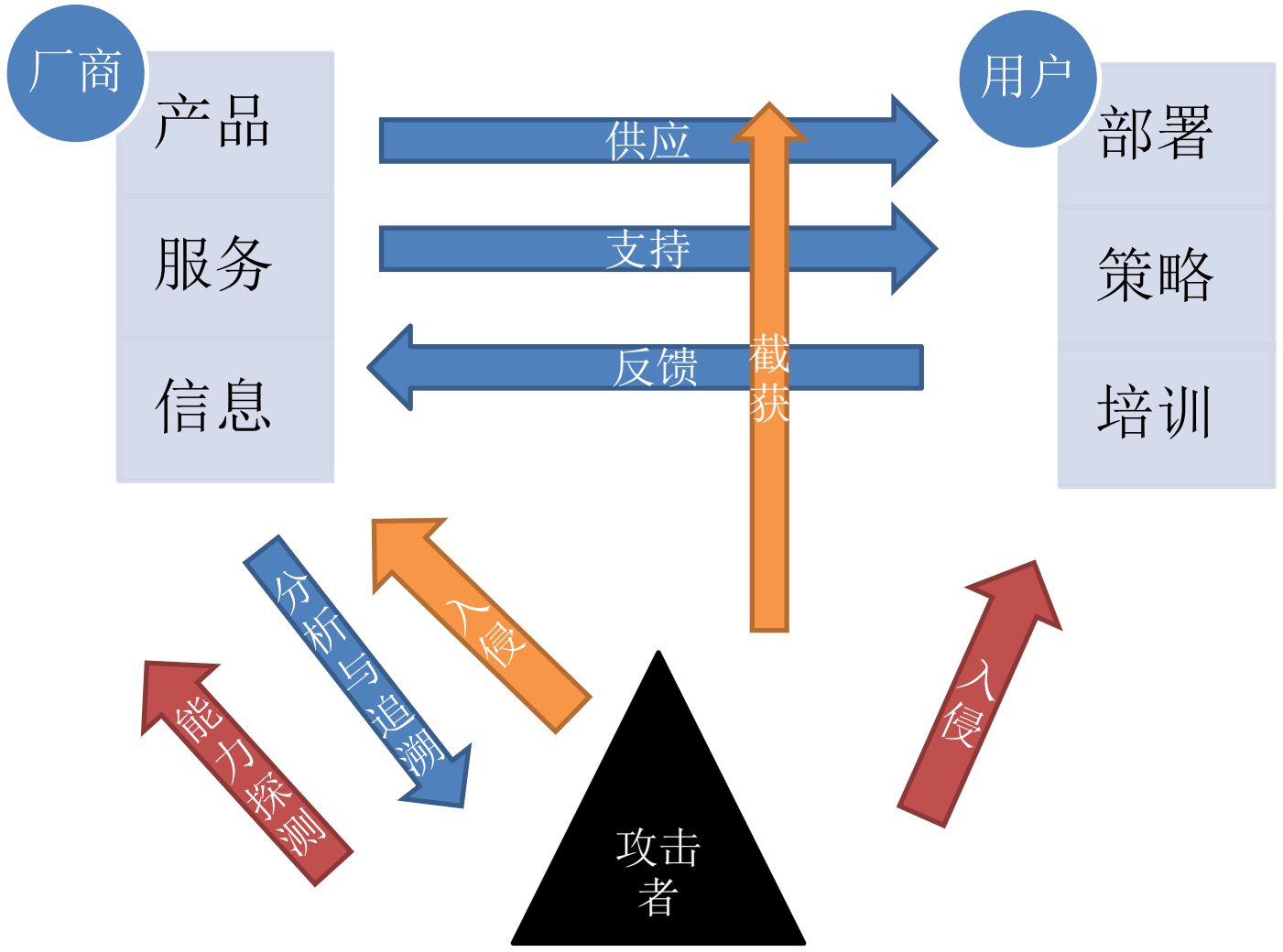
fsb-antivirus (France)
Bit-Defender (Romania)
Viritpro (Italy)
eAladdin (Israel)
Norman (Norway)
AVG (Czech)
F-prot (Iceland)
F-secure (Finland)
DrWeb (Russia)
Hauri (Korea)
k7computing (India)
Ikarus (Austria)
Arcabit (Poland)
Antiy (Chinese)
Avira (Germany)
Spy-Emergency (Slovakia)
Nod32 (Slovakia)
Novirusthanks (Italy)
Ahnlab (S Korea)
Emsisoft (Austria)
Eset (Slovakia)
Avast (Czech)
Checkpoint (Israel)

2014



左图引自斯诺登泄露文档《An Easy Win：Using SIGINT to Learn about New Virues|Project Camberdada》
右图为卡巴斯基报告《The Duqu 2.0 Technical Details》安天公益翻译组提供的非官方翻译版。

传统的战场视野和新视野



结束语

- 在纷纷追求“技术革命”的时候，我们却被看起来幼稚的攻击者用原始的攻击“羞辱”。
- 而更高能的攻击者却早已拉开前所未有的攻击纵深。
- 在更为强大的攻击者面前，安全厂商不再只是用户防御阵地的兵器与支援火力的提供方，其自身也是战场的一部分。
- 防御的复杂性，不止取决于用户、厂商的个体改善，更需要广泛的融合。

感谢大家！

www.antiy.com

Weibo.com/seak