弹道有痕

——中国面临的APT攻击的风险与案例分析

安天实验室

提纲

1 引子：中国的网络安全的地缘形势与对手

2 威胁演进与一切都不再可靠的时代

3 不同能力层次攻击对手的作业特点

4 防御体系与新的布防点

01

PART ONE

引子：中国的网络安全的地缘形势与对手

引子：中国的网络安全地缘

中国的网络空间安全地缘特点总结

1

投射

网络空间的安全威胁与态势不是凭空产生的，其是传统的大国博弈与地缘安全态势的投射。

2

风险

与中国的地理地缘一样，中国是网络地缘风险最高的大国。

3

压力

超级大国是中国面临的主要压力方，但不是唯一的压力方。

4

动作

中国面对来自多个对手的网络空间各种动作，既有传统情报作业的延展，也有信息战的前奏准备，这些动作一些已经与传统的博弈策略和手段融为一体。

02

PART TWO

威胁演进与一切都不再可靠的时代

安全威胁的两大走向

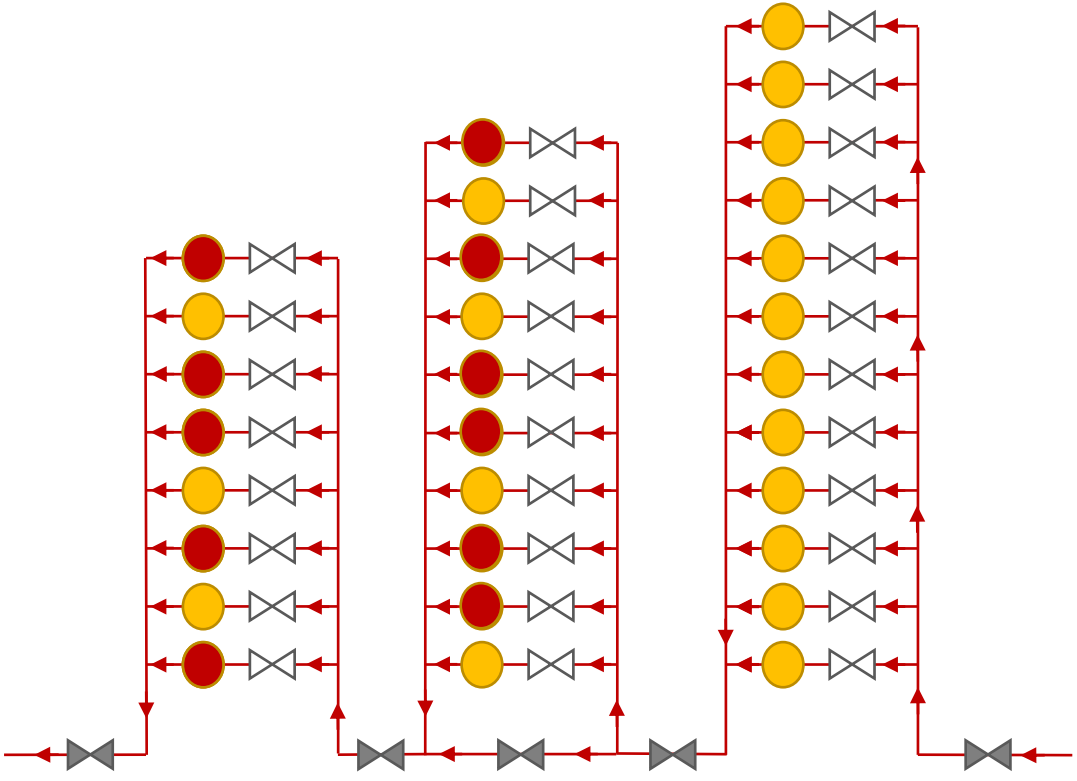
攻击从网络空间到实体空间

故障离心机

正常离心机

离心机阀门

辅助阀门

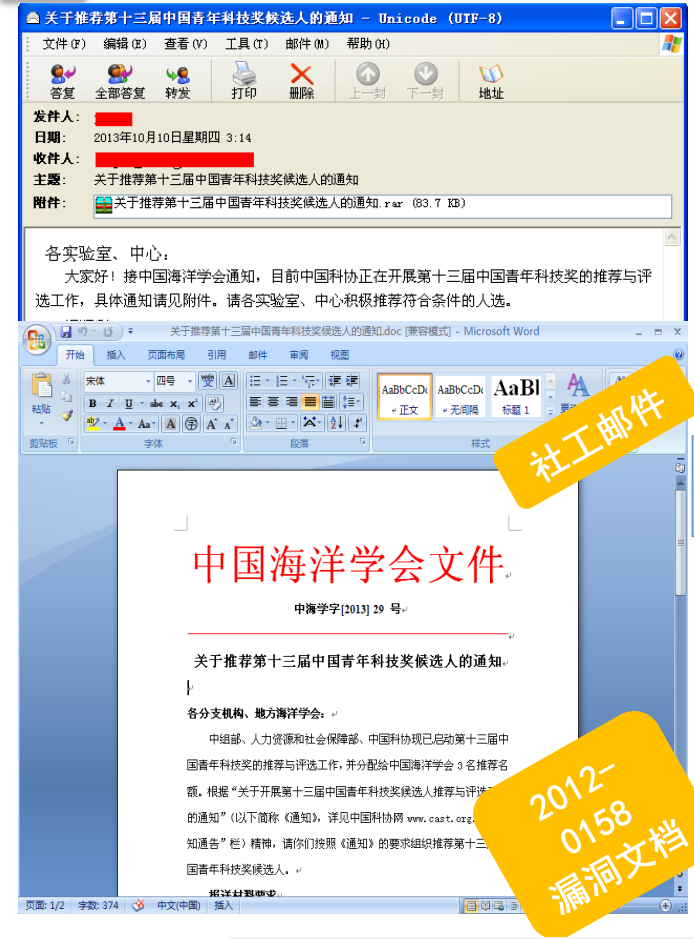


State7	State6	State5	State4	State3	State2	State1	State0
完成	等待攻击	攻击辅助阀门	等待二级压力	读取二级压力	攻击离心机阀门	记录	等待

2014网络安全威胁泛化与分布

攻击延伸到所有领域

各种文档文件都可以用于攻击



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

1. 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。
2. 收集网络信息，主机信息，进程信息，记录在%Application Data%\Microsoft\Windows\Profiles.log
3. 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。

[redacted]

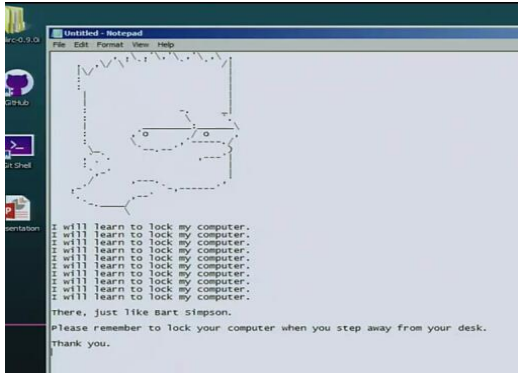
图 27 收集指定关键文件列表

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列关键字中的三个，根据关键字对攻击目标进行收集操[redacted]

二进制样本特点

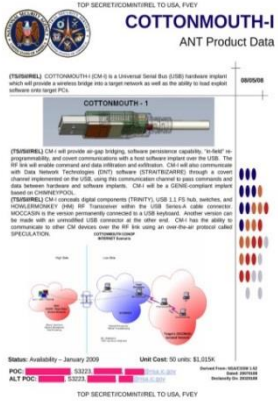
引自安天内部报告《针对中国政府机构的一系列针对性攻击事件的阶段性分析报告》

各种外设都可以被用于攻击（现场演示）



Jakob Lell和Karsten Nohl在2014Blackhat上的展示

安天在2008年 XCON上的展示

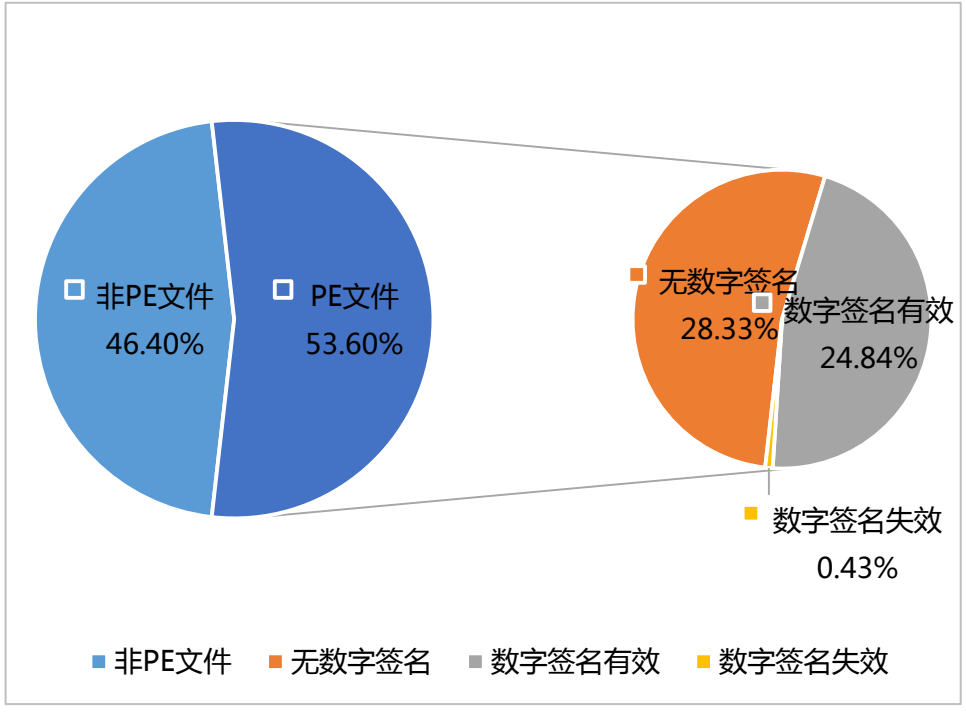


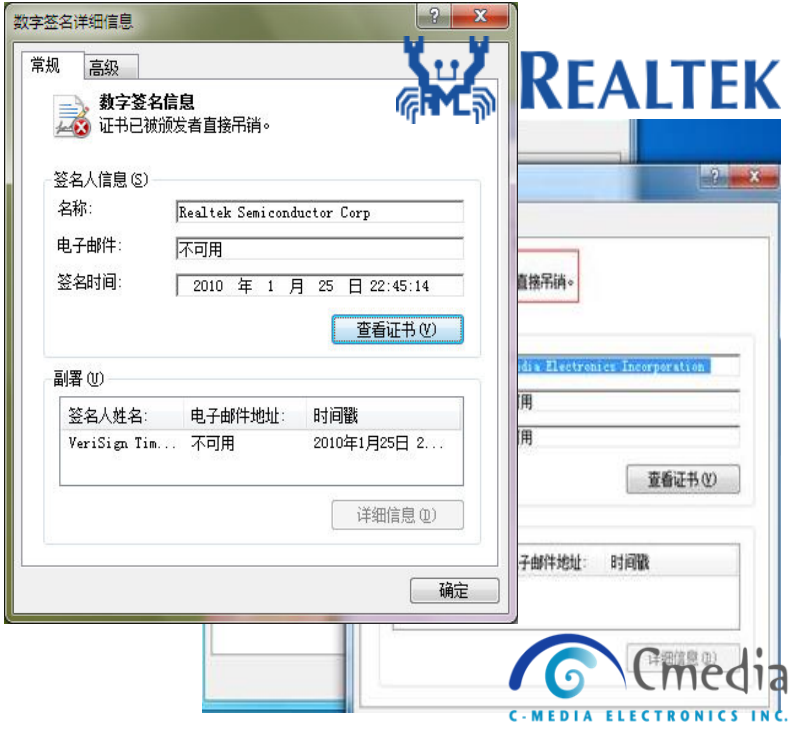
NSA 2008年成型的装备

BadUSB的另一个时间轴

智者安天下

可信计算同样会遭到攻击





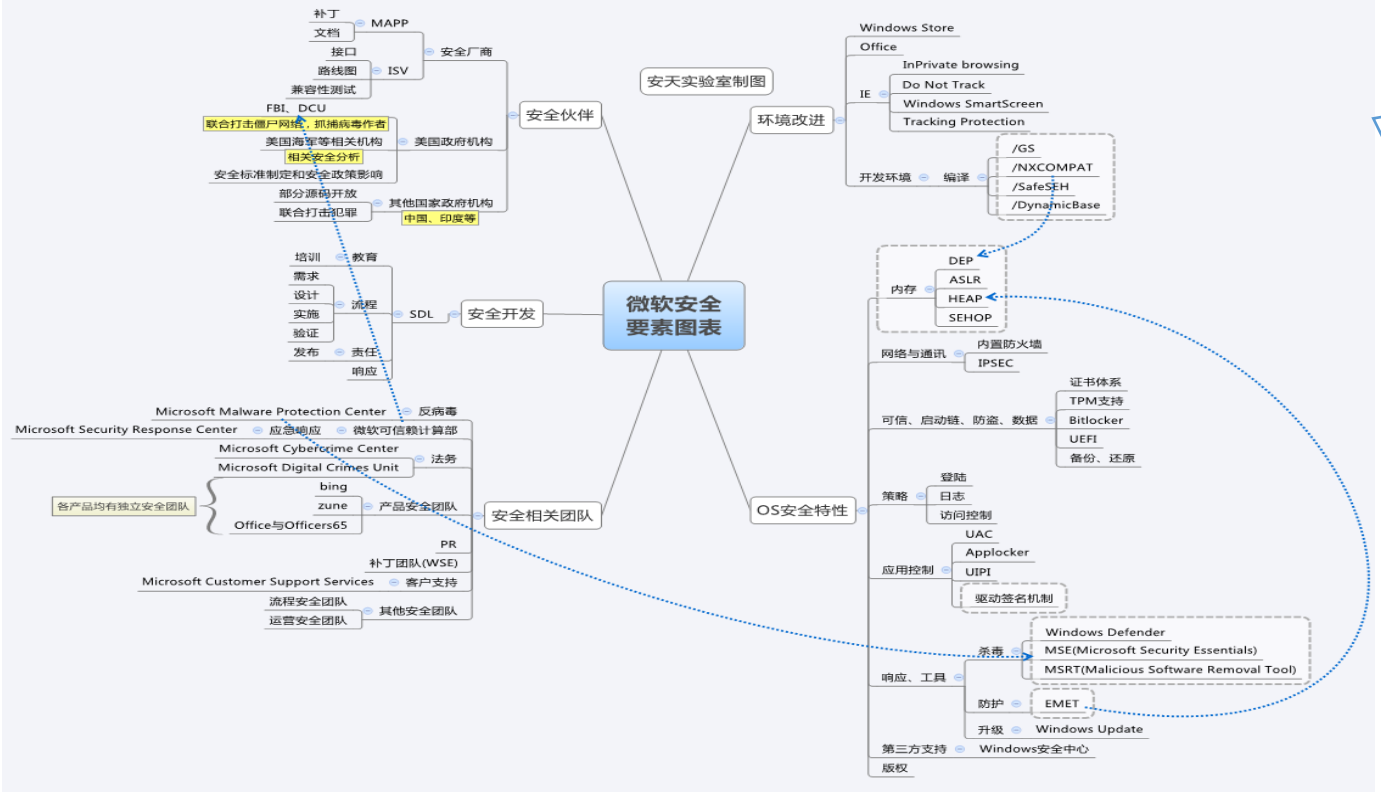
带有数字签名样本已经接近PE样本的一半

震网攻击中盗用的知名厂商证书

TPM和TZ同样被发现漏洞和遭遇攻击

仅仅“自主”不能保证可控

- 美国是全球信息技术最“自主”的国家，但依然面临大量安全威胁与攻击。



左图反应了微软操作系统在安全上做的大量工作，并促进Windows安全状况的改善，如果国产信息化产品不能尊重其中的规律性因素，则同样不能改进安全。

高级持续性威胁开启了新的威胁时代

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

Persisten 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

智者安天下

谁最初创造了“高级持续威胁”一词

旋转门

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)

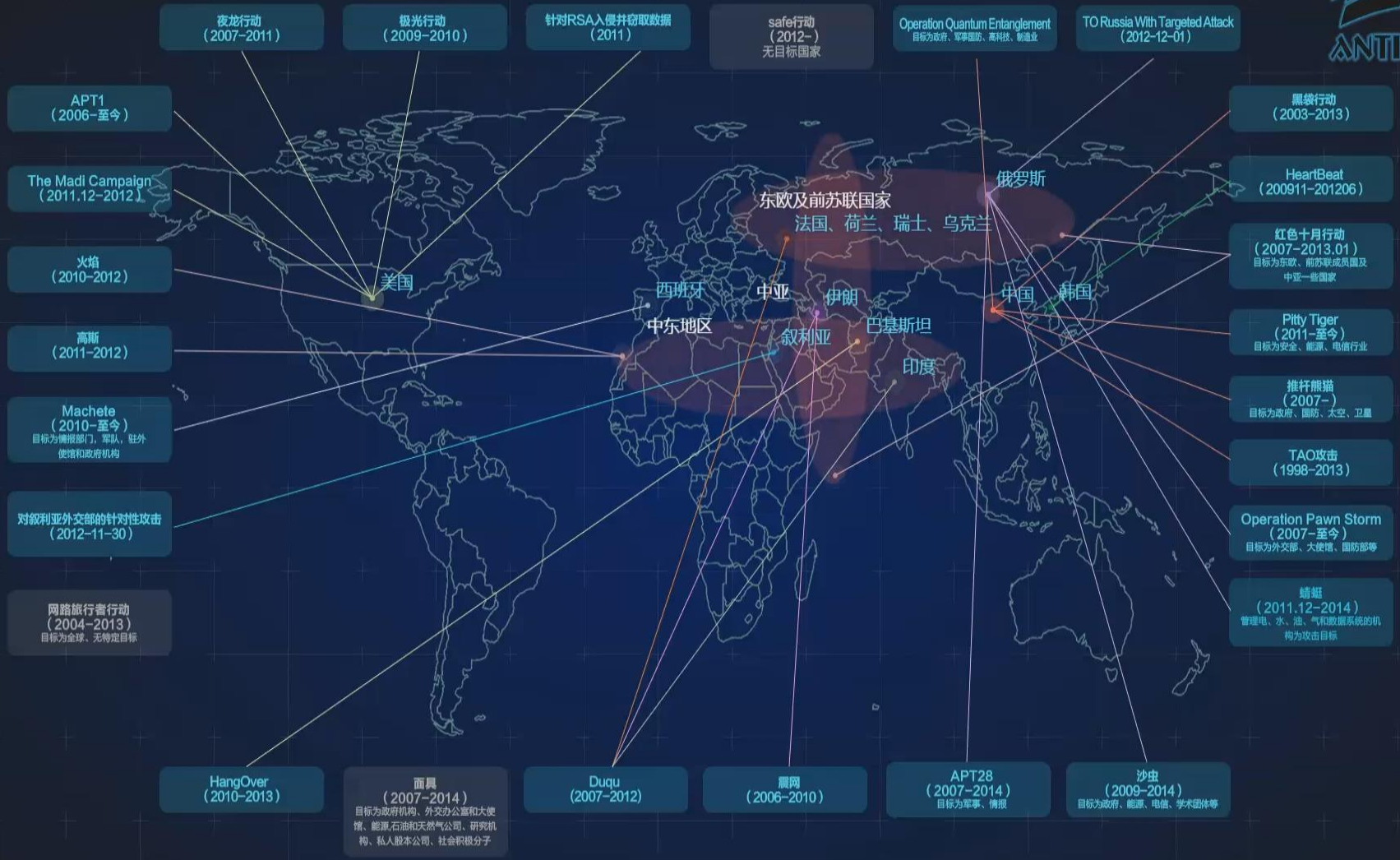
Commander 凯利空军基地23期信息作战中队指挥官
23d Information Operations Squadron, Kelly AFB, TX
2000 – 2003 (3 年)

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.**

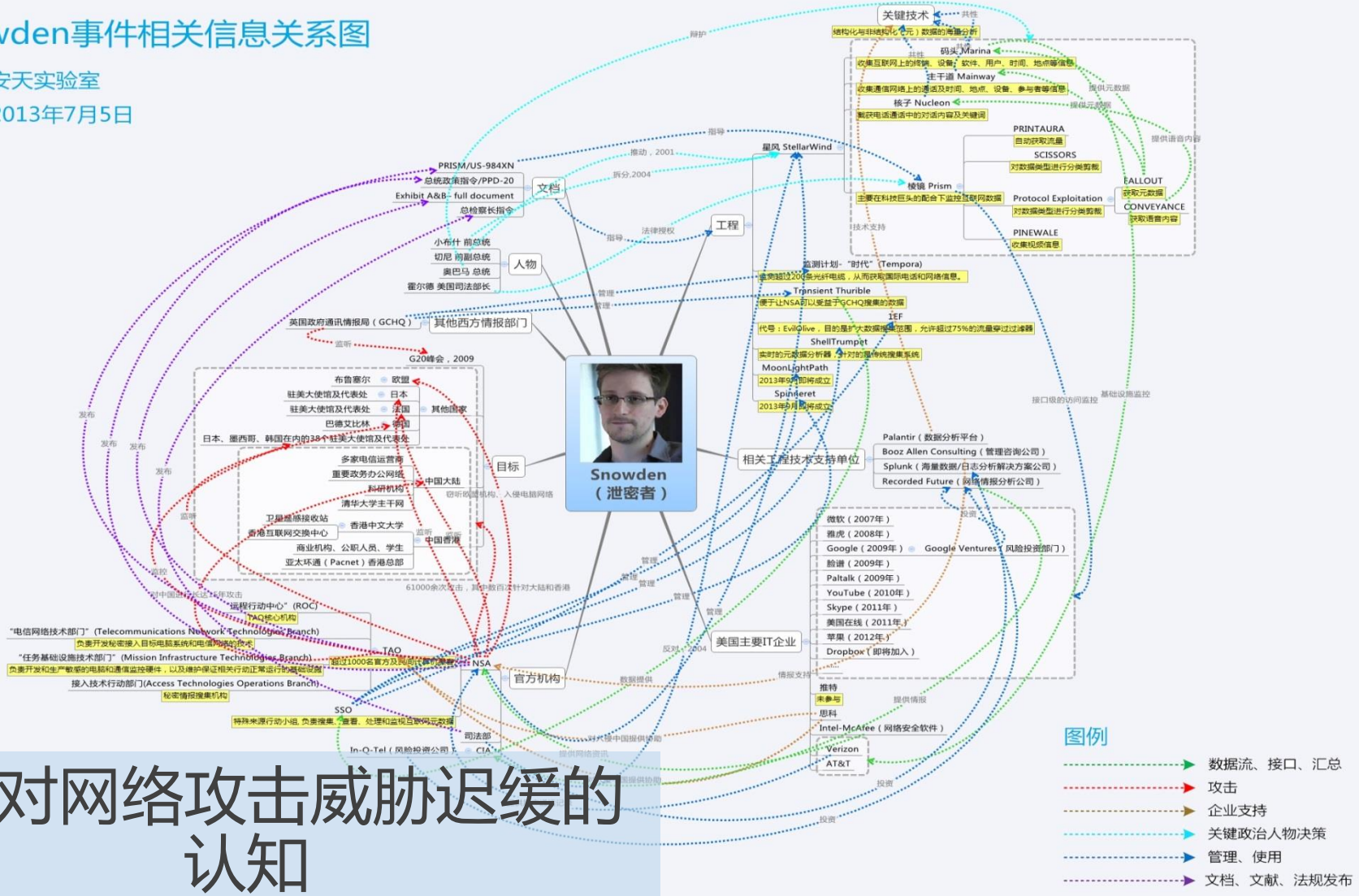
安天安全事件地理场景复现模块：全球近三年APT事件的目标和波及范围



Snowden事件相关信息关系图

绘制：安天实验室

更新：2013年7月5日



中国对网络攻击威胁迟缓的认知

首先必须说清一个问题

美方依靠情报作业能力进行信息获取与美方本身拥有八大金刚等供应链、信息链的优势有一定关系，但两者并不是一回事。

美方在网络空间安全领域的情报作业依靠成建制的网络攻击团队、庞大的支撑工程体系与制式化的攻击装备库、强大的漏洞采集和分析挖掘能力和关联资源储备、以及系统化的作业规程和手册，具有装备体系覆盖全场景、漏洞利用工具和恶意代码载荷覆盖全平台、持久化能力覆盖全环节的特点。

中国网络安全的认知盲点

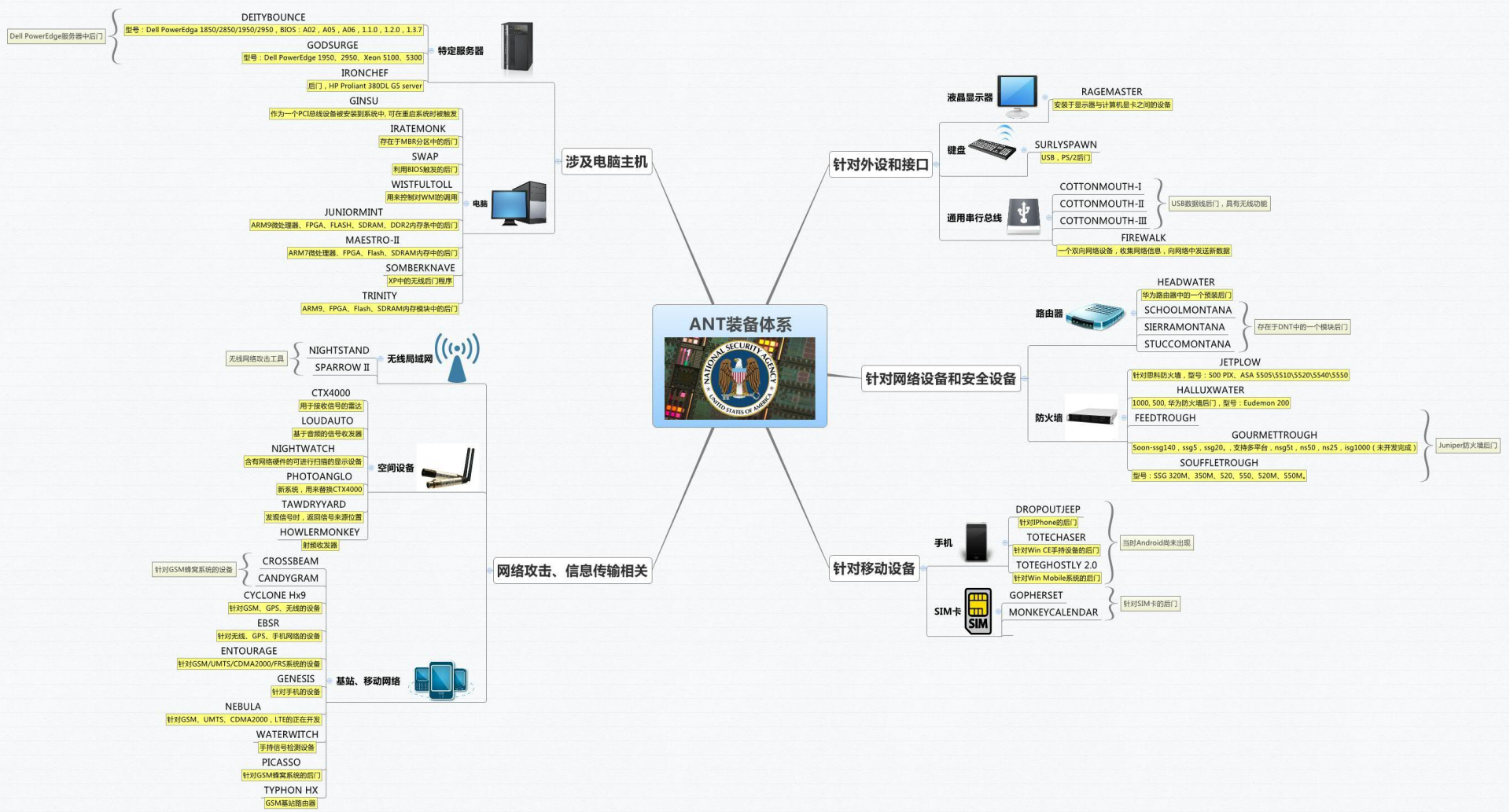
现状	盲点
过多强调以隔离换取安全	忽略信息有效链接和整合是重要的安全手段
过多强调信息技术的自我短板	不积极在安全环节上有效布防
过度强调主要对手的基础优势	缺乏对对手攻击作业方式和作业路径的系统研判
过度看重网站安全	针对重要基础设施网络被入侵，信息被窃取问题，投入甚少

总之，对于互联网+，我们需要关注网络攻击带来的纵深挑战，需要关注对手的实际能力。

PART THREE

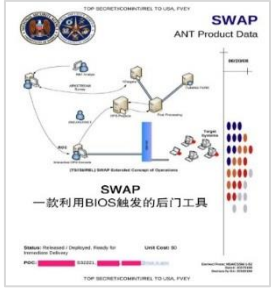
不同能力层次攻击对手的作业特点

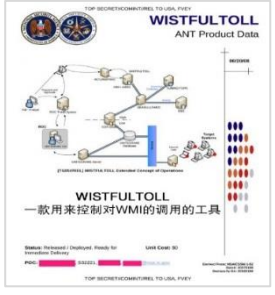
从ANT装备体系说起

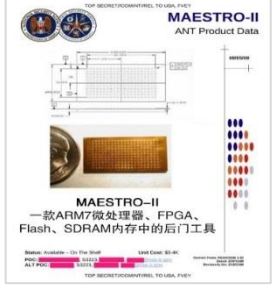

ANT装备体系
涉及电脑主机
特定服务器
Dell PowerEdge服务器中后门
DEITYBOUNCE
型号：Dell PowerEdga 1850/2850/1950/2950，BIOS：A02，A05，A06，1.1.0，1.2.0，1.3.7
GODSURGE
型号：Dell PowerEdge 1950、2950、Xeon 5100、5300
IRONCHEF
后门，HP Proliant 380DL G5 server
电脑
GINSU
作为一个PCI总线设备被安装到系统中，可在重启系统时被触发
IRATEMONK
存在于MBR分区中的后门
SWAP
利用BIOS触发的后门
WISTFULTOLL
用来控制对WMI的调用
JUNIORMINT
ARM9微处理器、FPGA、FLASH、SDRAM、DDR2内存条中的后门
MAESTRO-II
ARM7微处理器、FPGA、Flash、SDRAM内存中的后门
SOMBERKNAVE
XP中的无线后门程序
TRINITY
ARM9、FPGA、Flash、SDRAM内存模块中的后门
网络攻击、信息传输相关
无线局域网
无线网络攻击工具
NIGHTSTAND
SPARROW II
空间设备
CTX4000
用于接收信号的雷达
LOUDAUTO
基于音频的信号收发器
NIGHTWATCH
含有网络硬件的可进行扫描的显示设备
PHOTOANGLO
新系统，用来替换CTX4000
TAWDRYYARD
发现信号时，返回信号来源位置
HOWLERMONKEY
射频收发器
基站、移动网络
针对GSM蜂窝系统的设备
CROSSBEAM
CANDYGRAM
CYCLONE Hx9
针对GSM、GPS、无线的设备
EBSR
针对无线、GPS、手机网络的设备
ENTOURAGE
针对GSM/UMTS/CDMA2000/FRS系统的设备
GENESIS
针对手机的设备
NEBULA
针对GSM、UMTS、CDMA2000，LTE的正在开发
WATERWITCH
手持信号检测设备
PICASSO
针对GSM蜂窝系统的后门
TYPHON HX
GSM基站路由器
针对外设和接口
液晶显示器
RAGEMASTER
安装于显示器与计算机显卡之间的设备
键盘
SURLYSPAWN
USB，PS/2后门
通用串行总线
COTTONMOUTH-I
COTTONMOUTH-II
COTTONMOUTH-III
USB数据线后门，具有无线功能
FIREWALK
一个双向网络设备，收集网络信息，向网络中发送新数据
针对网络设备和安全设备
路由器
HEADWATER
华为路由器中的一个预装后门
SCHOOLMONTANA
SIERRAMONTANA
STUCCOMONTANA
存在于DNT中的一个模块后门
防火墙
JETPLOW
针对思科防火墙，型号：500 PIX、ASA 5505\5510\5520\5540\5550
HALLUXWATER
1000, 500, 华为防火墙后门，型号：Eudemon 200
FEEDTROUGH
GOURMETTROUGH
Soon-ssg140，ssg5，ssg20，，支持多平台，nsg5t，ns50，ns25，isg1000（未开发完成）
SOUFFLETROUGH
型号：SSG 320M、350M、520、550、520M、550M。
Juniper防火墙后门
针对移动设备
手机
DROPOUTJEEP
针对IPhone的后门
TOTECHASER
针对Win CE手持设备的后门
TOTEGHOSTLY 2.0
针对Win Mobile系统的后门
当时Android尚未出现
SIM卡
GOPHERSET
MONKEYCALENDAR
针对SIM卡的后门

针对电脑主机的攻击模块

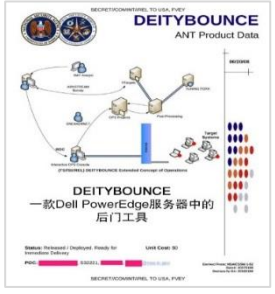
电脑

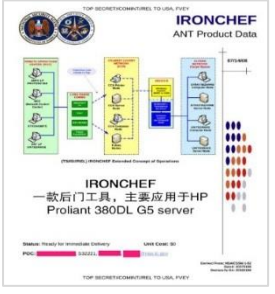






服务器



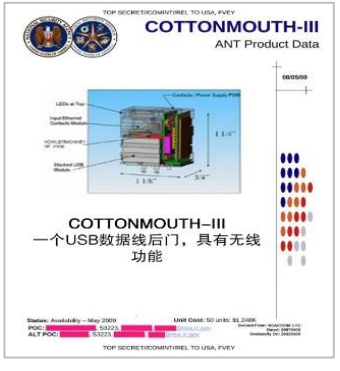


针对外设和接口的攻击模块

显示器

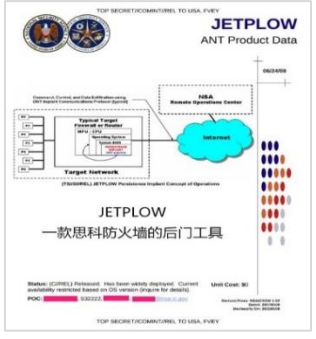
键盘

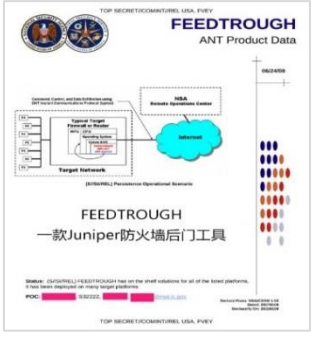
通用串行总线

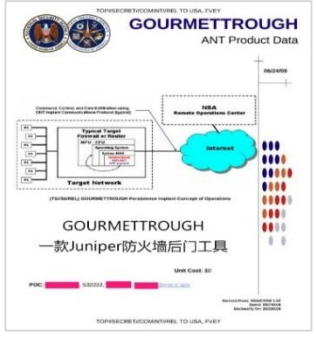


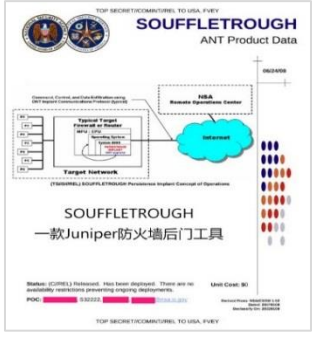
针对网络设备和安全设备

防火墙

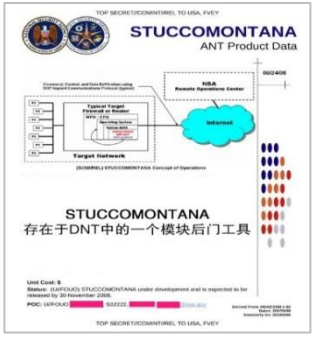


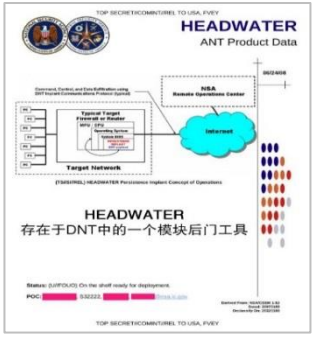


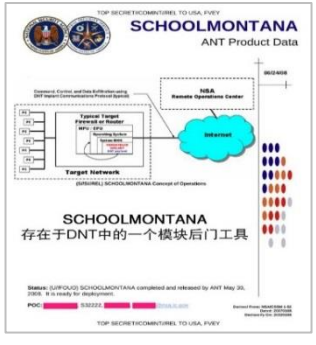




路由器

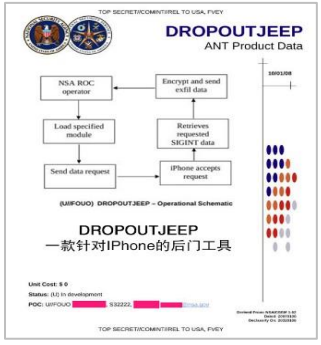


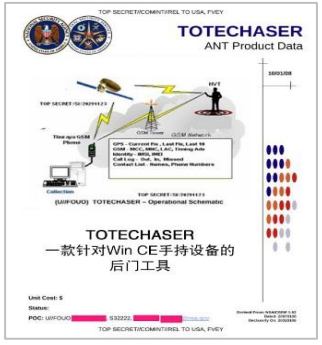


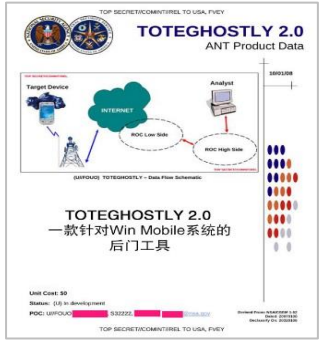


针对移动设备的攻击模块

手机



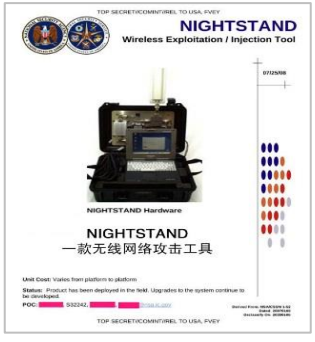


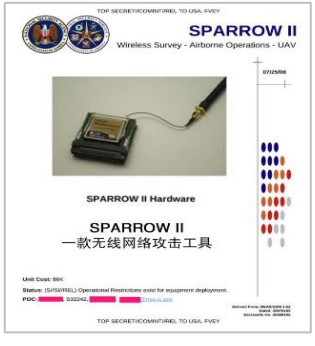


SIM卡

网络攻击、信息传输相关的攻击模块-I

无线局域网

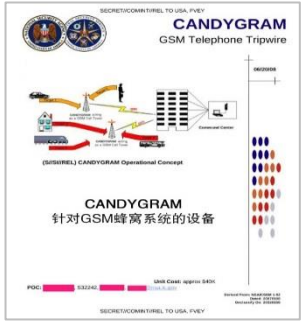




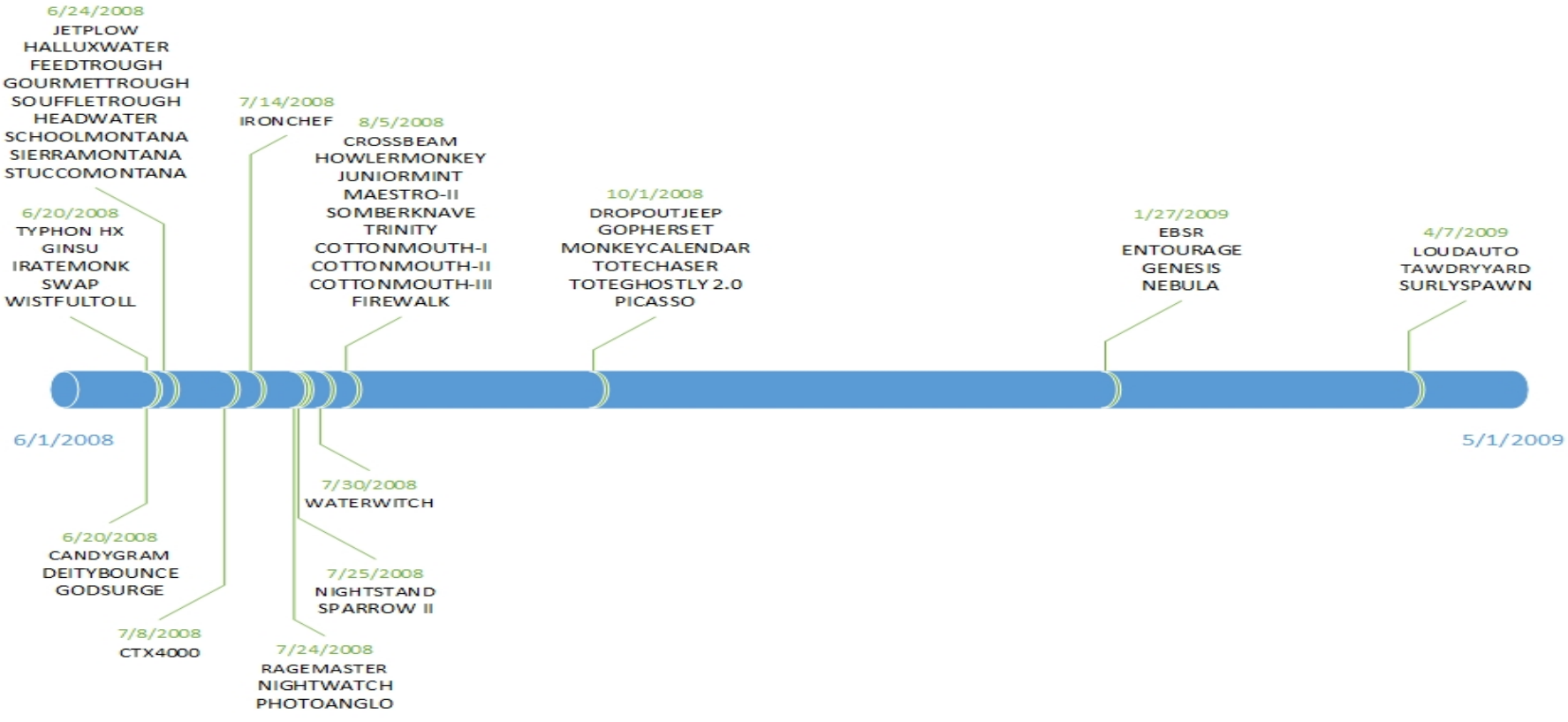
空间设备

网络攻击、信息传输相关的攻击模块-II

基站、移动网络



装备体系的渐进成形


6/24/2008
JETPLOW
HALLUXWATER
FEEDTROUGH
GOURMETTROUGH
SOUFFLETROUGH
HEADWATER
SCHOOLMONTANA
SIERRAMONTANA
STUCCOMONTANA
6/20/2008
TYPHON HX
GINSU
IRATEMONK
SWAP
WISTFULTOLL
7/14/2008
IRONCHEF
8/5/2008
CROSSBEAM
HOWLERMONKEY
JUNIORMINT
MAESTRO-II
SOMBERKNAVE
TRINITY
COTTONMOUTH-I
COTTONMOUTH-II
COTTONMOUTH-III
FIREWALK
10/1/2008
DROPOUTJEEP
GOPHERSET
MONKEYCALENDAR
TOTECHASER
TOTEGHOSTLY 2.0
PICASSO
1/27/2009
EBSR
ENTOURAGE
GENESIS
NEBULA
4/7/2009
LOUDAUTO
TAWDRYYARD
SURLYSPAWN
6/1/2008
5/1/2009
6/20/2008
CANDYGRAM
DEITYBOUNCE
GODSURGE
7/8/2008
CTX4000
7/24/2008
RAGEMASTER
NIGHTWATCH
PHOTOANGLO
7/25/2008
NIGHTSTAND
SPARROW II
7/30/2008
WATERWITCH

攻击者如何“进入” 物理隔离网络

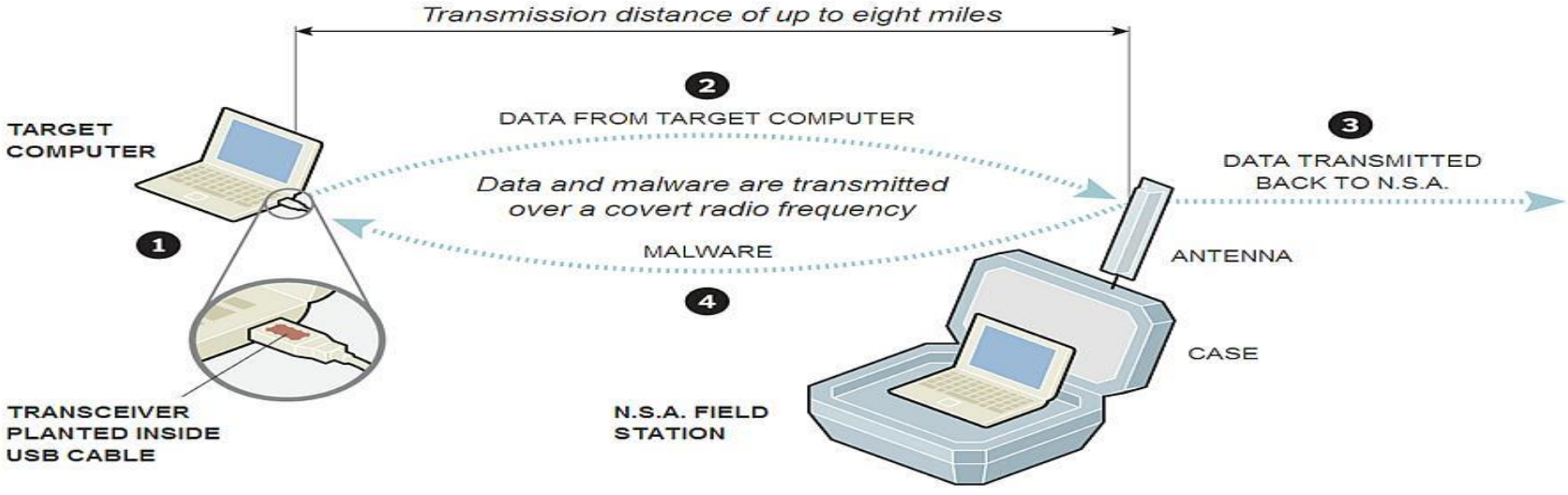
(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

如何从“物理隔离”网络传出信息

How the N.S.A. Uses Radio Frequencies to Penetrate Computers

The N.S.A. and the Pentagon's Cyber Command have implanted nearly 100,000 "computer network exploits" around the world, but the hardest problem is getting inside machines isolated from outside communications.



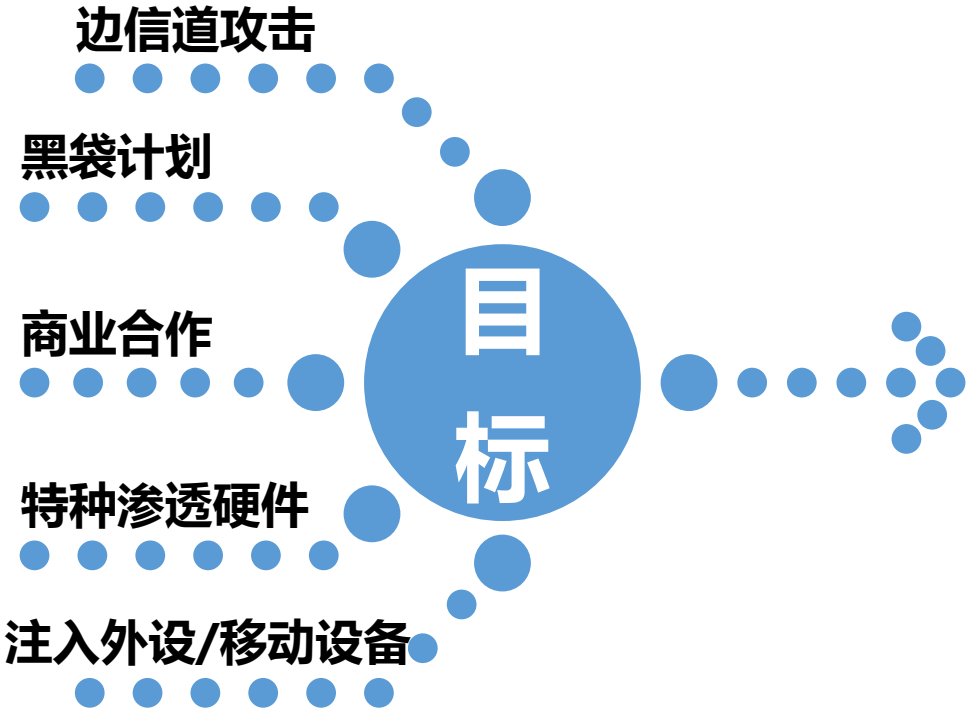
1. Tiny transceivers are built into USB plugs and inserted into target computers. Small circuit boards may be placed in the computers themselves.

2. The transceivers communicate with a briefcase- size N.S.A. field station, or hidden relay station, up to eight miles away.

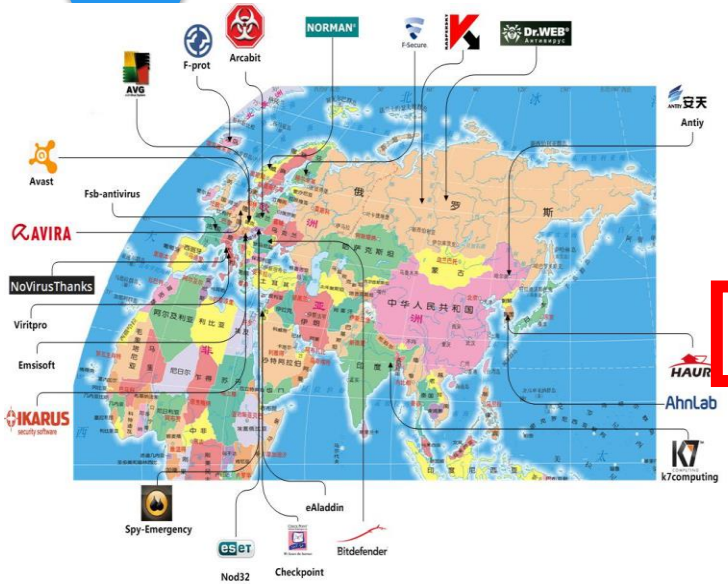
3. The field station communicates back to the N.S.A.'s Remote Operations Center.

4. It can also transmit malware, including the kind used in attacks against Iran's nuclear facilities.

把门踹倒->第一攻击波

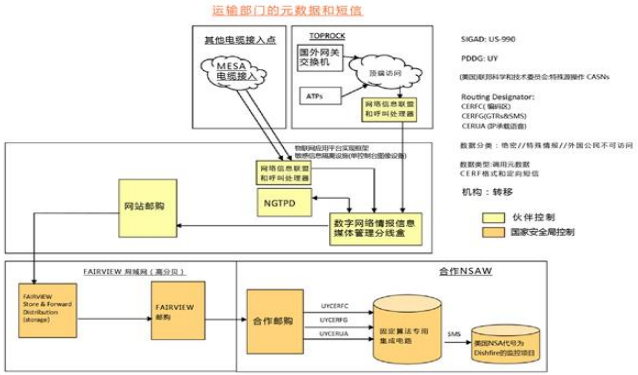


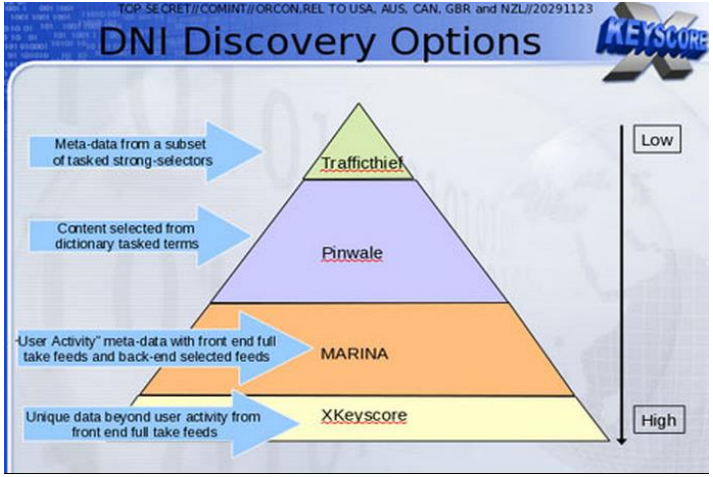
超级大国如何使用基础设施优势



英文名称	说明
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
Institute of Information & Analytical Technology	信息与分析技术研究所
Rosoboron export	俄罗斯国防产品出口公司
Famatech	软件公司，其软件产品 Radmin 为远程控制软件

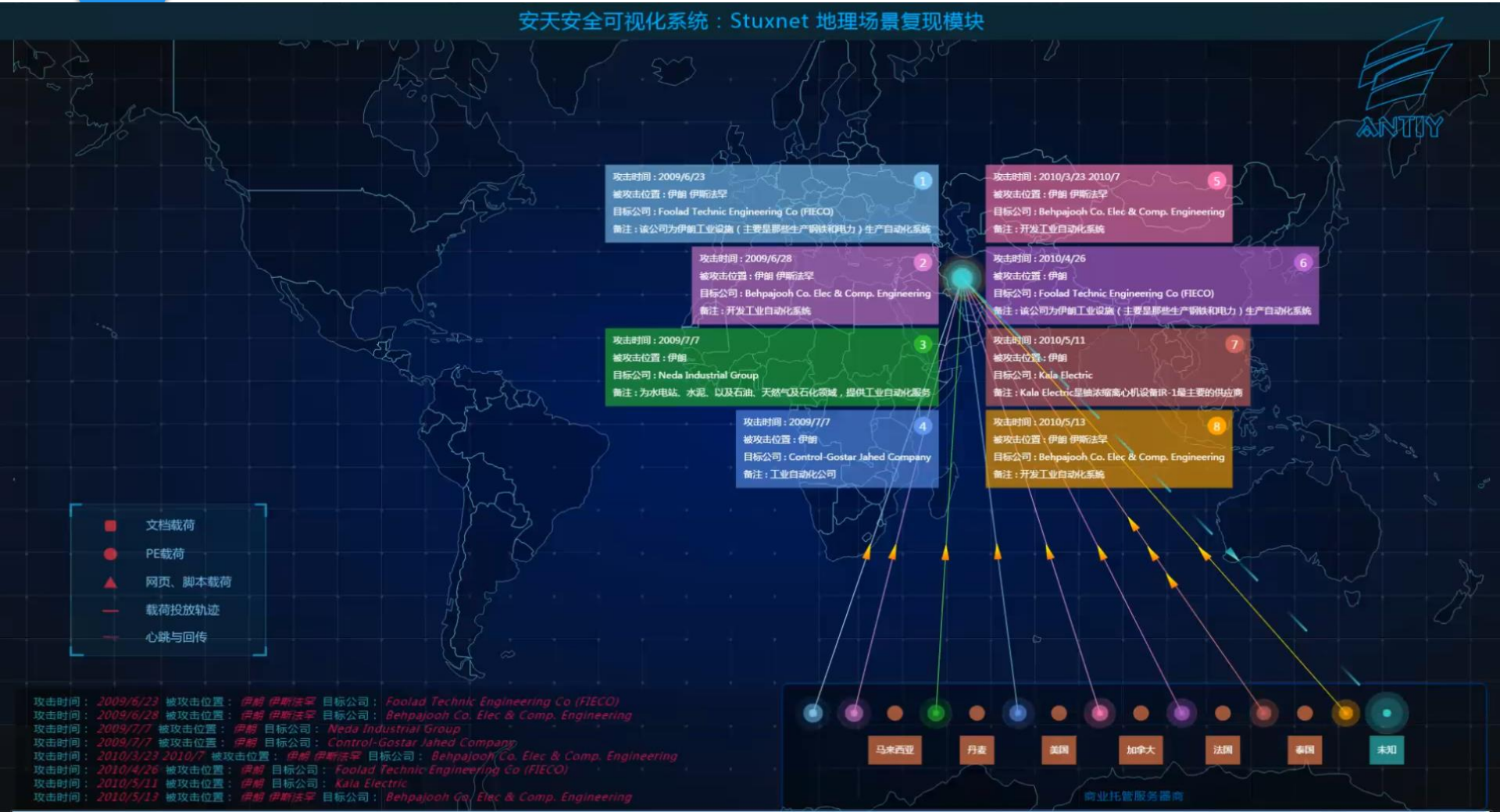
CamberDADA计划展示了战略设施可以获取任何微小的优势



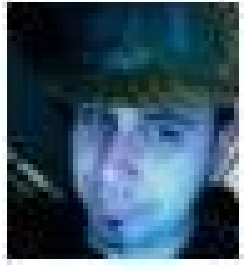


智者安天下

构造战场-震网击穿整个伊朗基础工业体系



Stuxnet是APT？还是A2PT



Michael Cloppert

CIRT Chief Research Analyst at DoD Contractor

美国 华盛顿都会区 | 计算机和网络安全

目前就职 DoD Contractor

曾经就职 US DoD Contractor, USAID, Fifth Third Bank

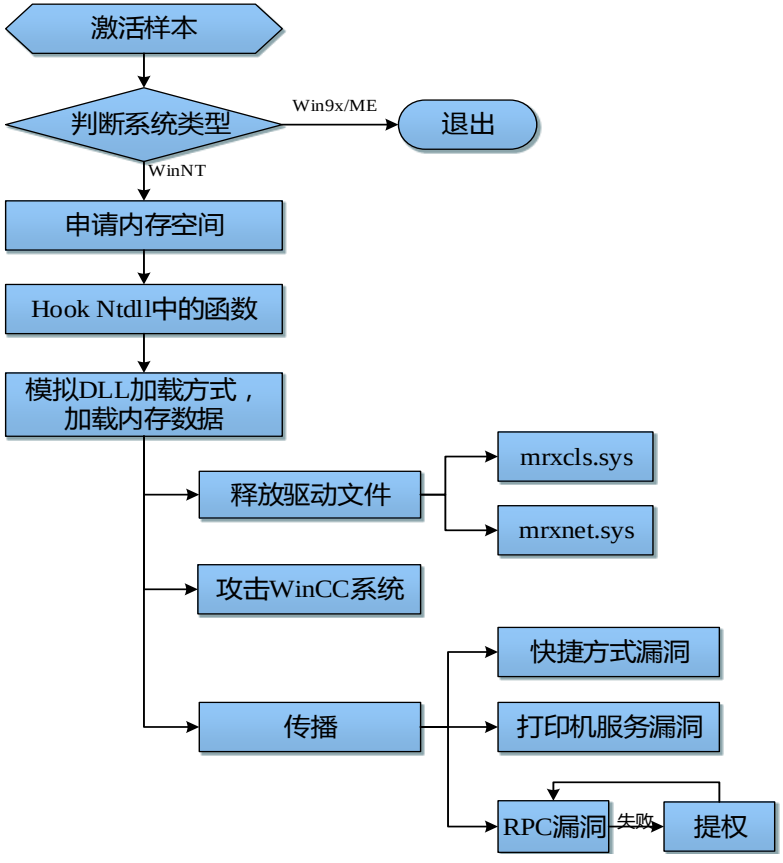
教育背景 The George Washington University

原文: The level of sophistication of Stuxnet is by every account very high. The code is relatively difficult to reverse engineer, contains a PLC rootkit, multiple zero-day exploits, and code that can run on processors with different chipsets. More often than not, the binaries in APT intrusions are relatively straightforward, and exploit a single vulnerability most often in client applications. This enables the adversary to "hide in plain sight" without triggering any heuristic attention through various code obfuscation and file hiding techniques that tend to leave unusual artifacts. After all, with a small target space, the likelihood of discovery is low, and analytical economies of scale will not apply for APT intrusions, meaning survivability against RE efforts is less important to build in.

译文： Stuxnet 蠕虫的复杂程度非常之高。其代码难以进行逆向工程，包含一个 PLC（可编程逻辑控制器）rootkit 和多个零日漏洞，而且代码可以在具备不同芯片组的处理器上运行。很多时候，APT 攻击中的二进制文件相对简单，在客户端应用程序中通常利用单个漏洞。这使得攻击者利用不同的代码混淆和文件隐藏技术，能够“隐藏在众目睽睽下”，而不会触发任何启发式的关注。毕竟，目标空间很小，被发现的可能性也很小，而且规模分析经济体将不适用于 APT 攻击，这意味着针对 RE 响应的生存能力并不那么重要。

来源：摘自<Why Stuxnet Isn‘t APT>，http://digital-forensics.sans.org/blog/2011/03/24/digital-forensics-stuxnet-apt

A²PT：近乎挥霍的0day资源



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

MS10-073

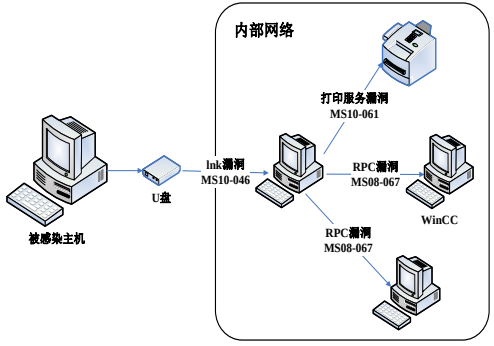
- 内核模式驱动程序漏洞

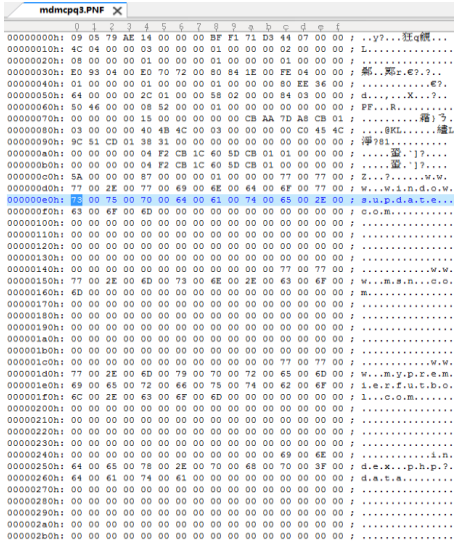
MS10-092

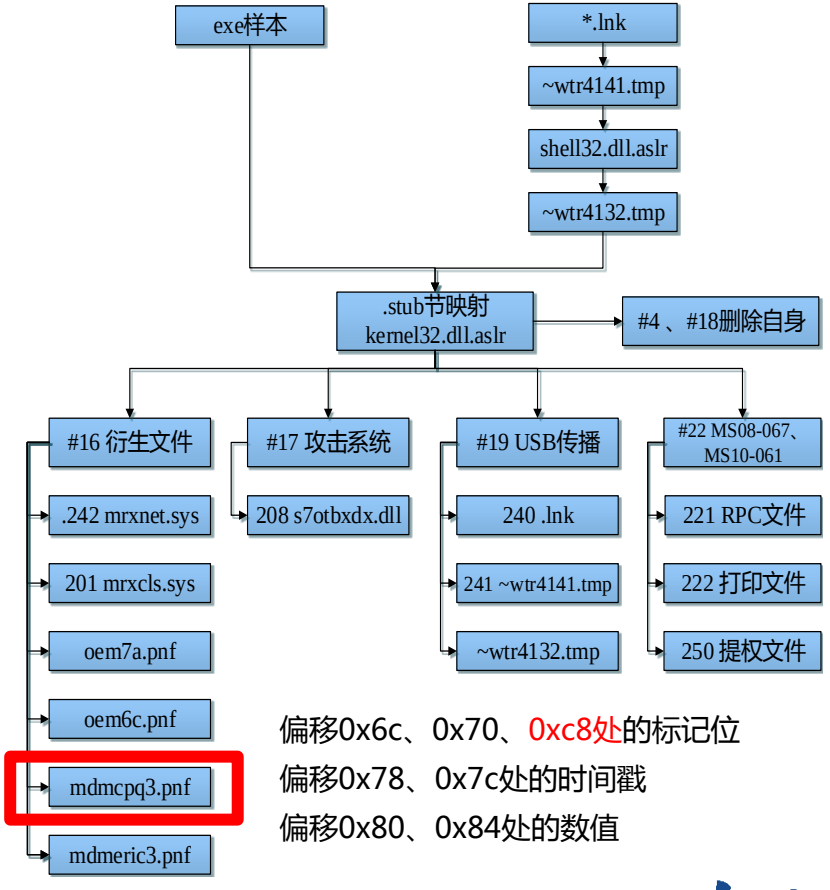
- 任务计划程序程序漏洞

来源：安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》

A²PT：复杂的条件逻辑（震网的U传播）

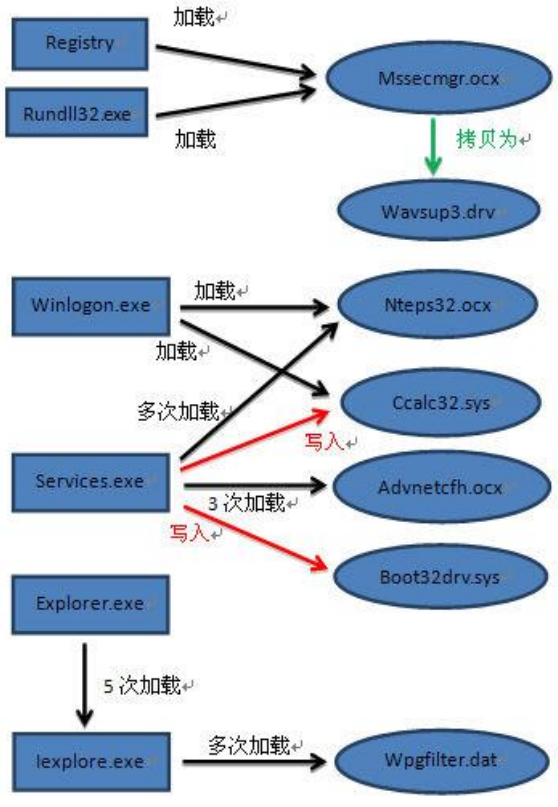




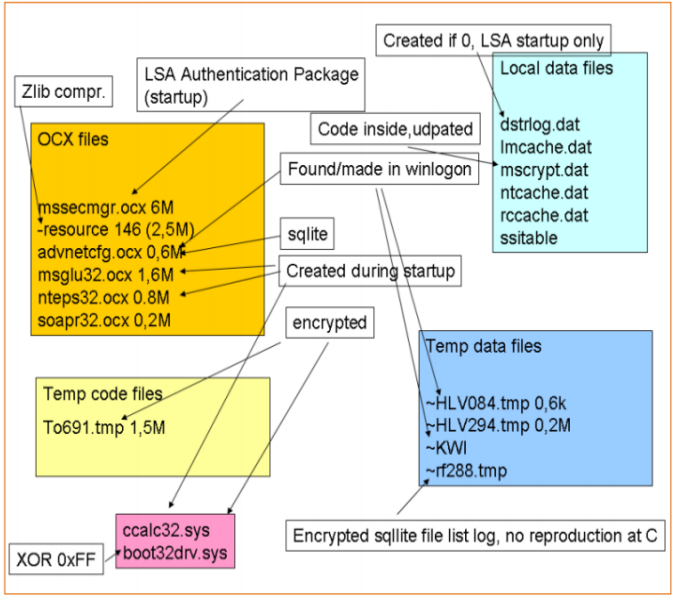


来源：安天《对Stuxnet蠕虫的后续分析报告》，安天技术文章汇编工控卷

A²PT的分析复杂度：火焰（Flame）



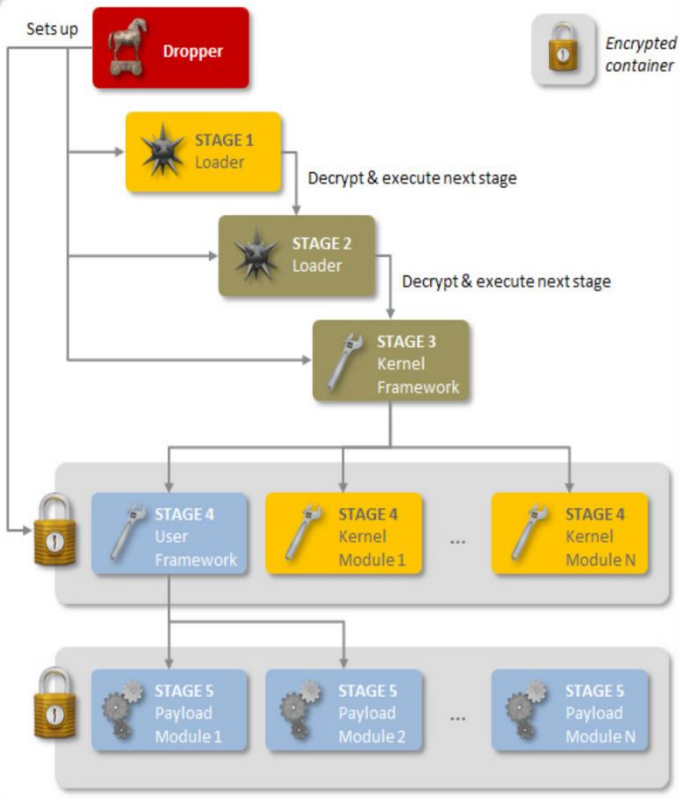
来源：安天《Flame蠕虫样本集分析报告》



mssecmgr.ocx (6 M) 主模块
-- resource 146 (2.5 M) 类似 zlib 的压缩资源文件
advnetcfg.ocx (0.6 M) 感染部分，可能是窃取信息（类似于屏幕截图）
msglu32.ocx (1.6 M) 由主模块创建的文件
nteps32.ocx (0.8 M) 由主模块创建的文件
soapr32.ocx (0.2 M) 基于网络传播的模块
~rf<number>.tmp 包含完整的被感染计算机的文件列表，以 SQLite3 数据库格式

来源： http://www.crysys.hu/skywiper/skywiper.pdf

A²PT的演进：Rootkit-无文件实体瑞晶(Regin)



Regin的六个阶段

阶段	组件
阶段 0	投放器。安装Regin 至目标计算机
阶段 1	加载驱动程序，初始阶段1驱动程序是计算机上唯一明显可见的代码。所有其他阶段都以加密数据的形式存储……
阶段 2	加载驱动程序
阶段 3	加载压缩、解密、联网及处理加密的EVFS程序。
阶段 4	利用EVFS并加载额外的内核模式驱动程序，包括有效载荷。
阶段 5	主要的有效载荷和数据文件

更强的Rookit特性，无文件实体，难以提取完整载荷

来源： http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

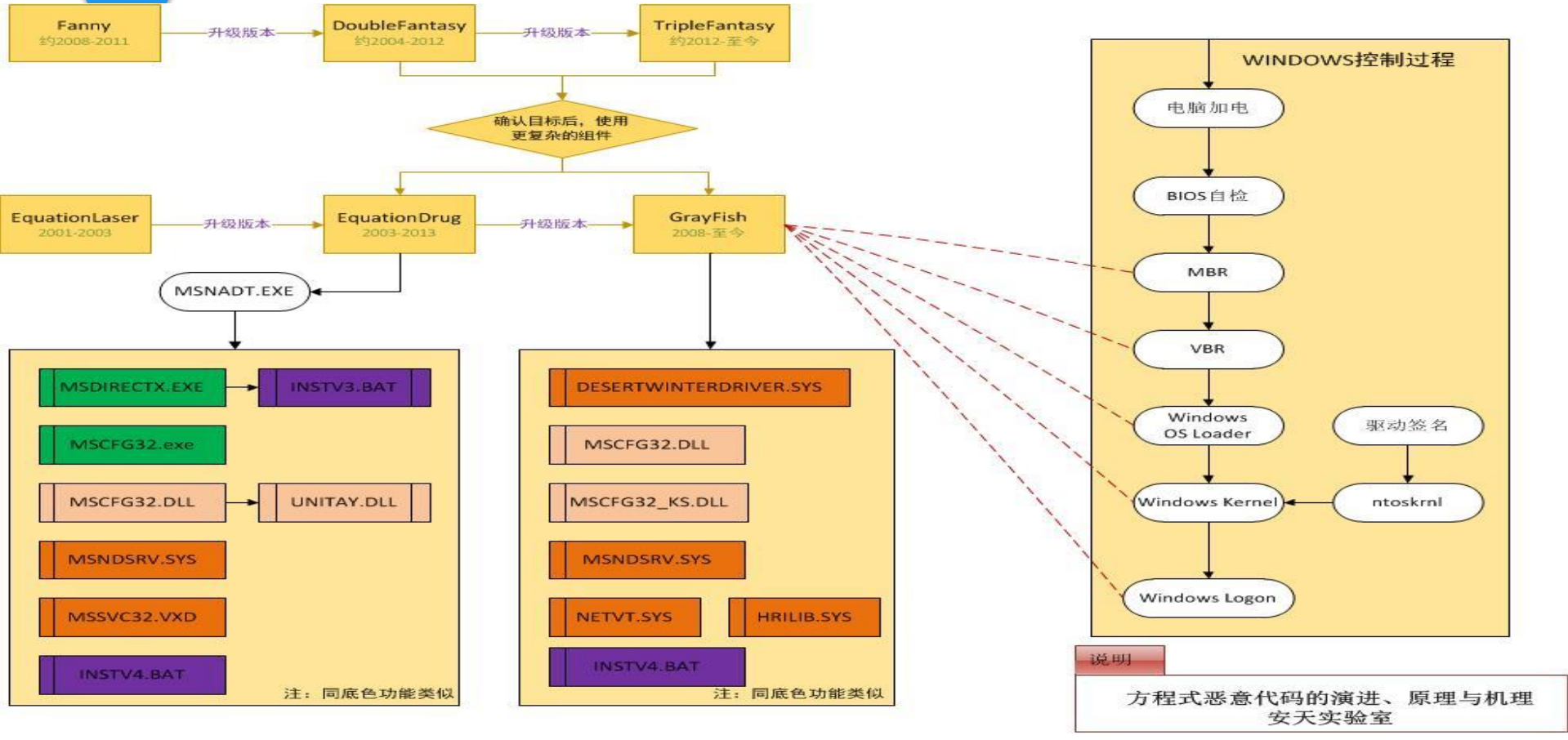
A²PT的演进：模块化 (Regin)

文件类型	编号	描述
SYS	0003	驱动程序
SYS	C433	Rootkit
SYS	C42B	PE加载程序
SYS	C42D	DLL注入
SYS	C3C3	类似WinPcap的网络数据包过滤器驱动程序（协议过滤器版本3.5） 用于设置TCP和UDP穿透过滤器和绕过防火墙。 执行BPF（Berkeley包过滤器）字节码，存储在阶段5的数据文件里。
SYS	CE69	网络端口屏蔽器
DLL	C363	网络数据包捕获
DLL	4E3B	通过注册表或配置文件（如prefs.js, refs.js等）检索网页浏览器（IE浏览器，网景，火狐等）的代理信息。枚举会话和用户账户。
DLL	290B	密码窃取器： • Windows资源管理器凭据 • Windows资源管理器受保护存储记录 • IE合法设置 • 名为 “cryptpp”登陆通知数据包的数据
DLL	C375	C&C HTTP/cookies
DLL	C383	SSL通信
DLL	C361	支持加密功能
DLL	001B	ICMP反向信道
DLL	C399	ApplicationLog.Evt记录创建程序
DLL	C39F	进程文件：%Temp%\~b3y7f.tmp

DLL	C36B	UI manipulation • 截屏 • 记录键盘操作 • 锁定工作站/输入Ctrl-Alt-Del • 点击功能 (通过三条指令：去、点击并释放、返回原始位置) • 结束进程
DLL	C351	文件系统探索元和包括原始NTFS解析器的取证水平探索： • 获取其他文件信息和属性 • 浏览记录 • 读写文件 • 移动和复制文件 • 读取并修复部分或全部被删除的文件 • 计算文件哈希
DLL	2B5D	进程和模块操作： • 读取进程和模块 • 进程运行的时间、限制和权限 • 扫描时，跳过俄语或英语的微软文件 • 检测过去两天里新引进的PE文件
DLL	C3CD	枚举 %System%\CurrentControlSet\Services\Tcpip\Linkage\bind里的TCP/IP接口
DLL	C38F	TCPDump 功能
DLL	C3C5	Libnet 二进制文件
DLL	27E9	IIS 网页浏览器日志窃取 通过COM对象枚举发现IIS日志。检索部分或全部日志信息。 • 部分：日志类型、上一个日志、较早日志的时间戳 • 全部：被发掘的全部日志记录

来源： http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

A²PT的演进：持久化（Equation）-固件

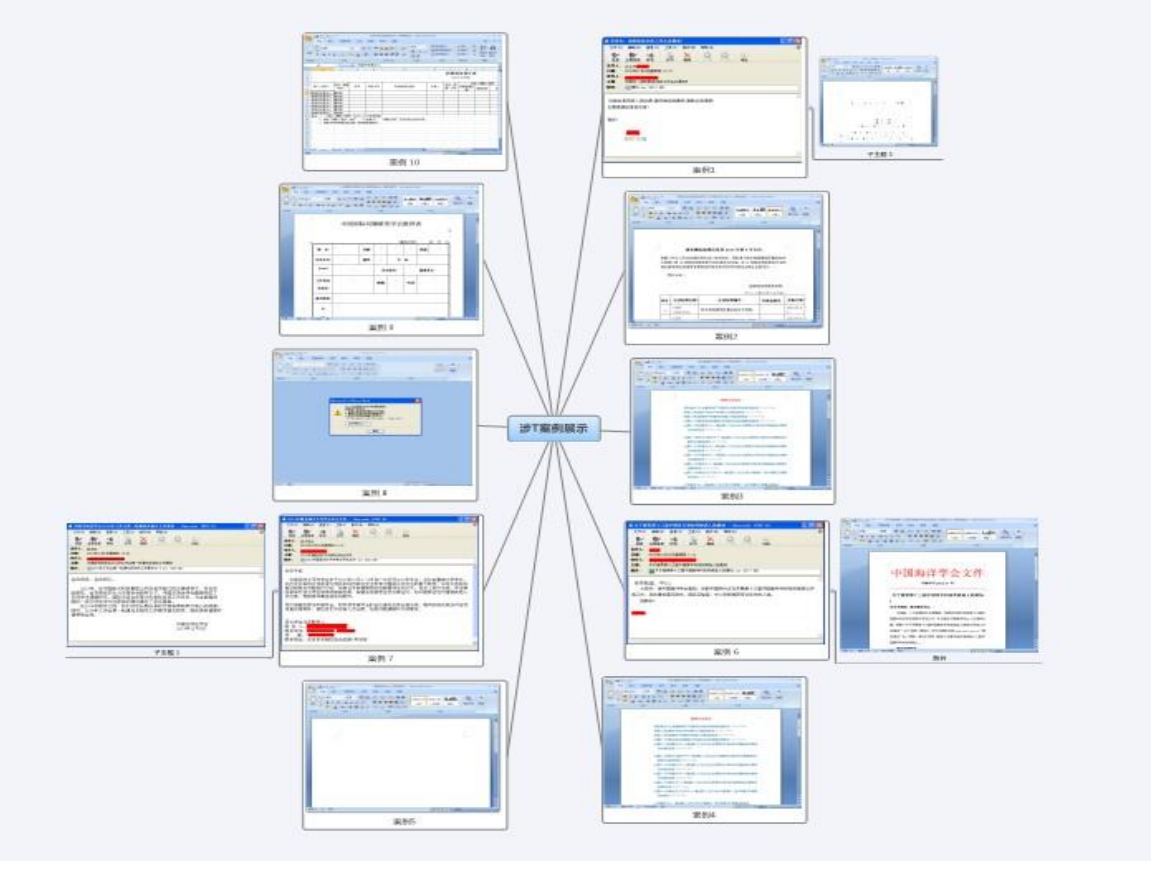


来源：安天《修改硬盘固件的木马（探索方程式（EQUATION）组织的攻击组件）》

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，甚至包括一些小众的商用UNIX

普通的APT-来自某方的攻击



- 原始攻击邮件：4封
- 使用漏洞附件：15个
- 使用漏洞：
  - ✓ CVE-2012-0158
  - ✓ CVE-2014-4114

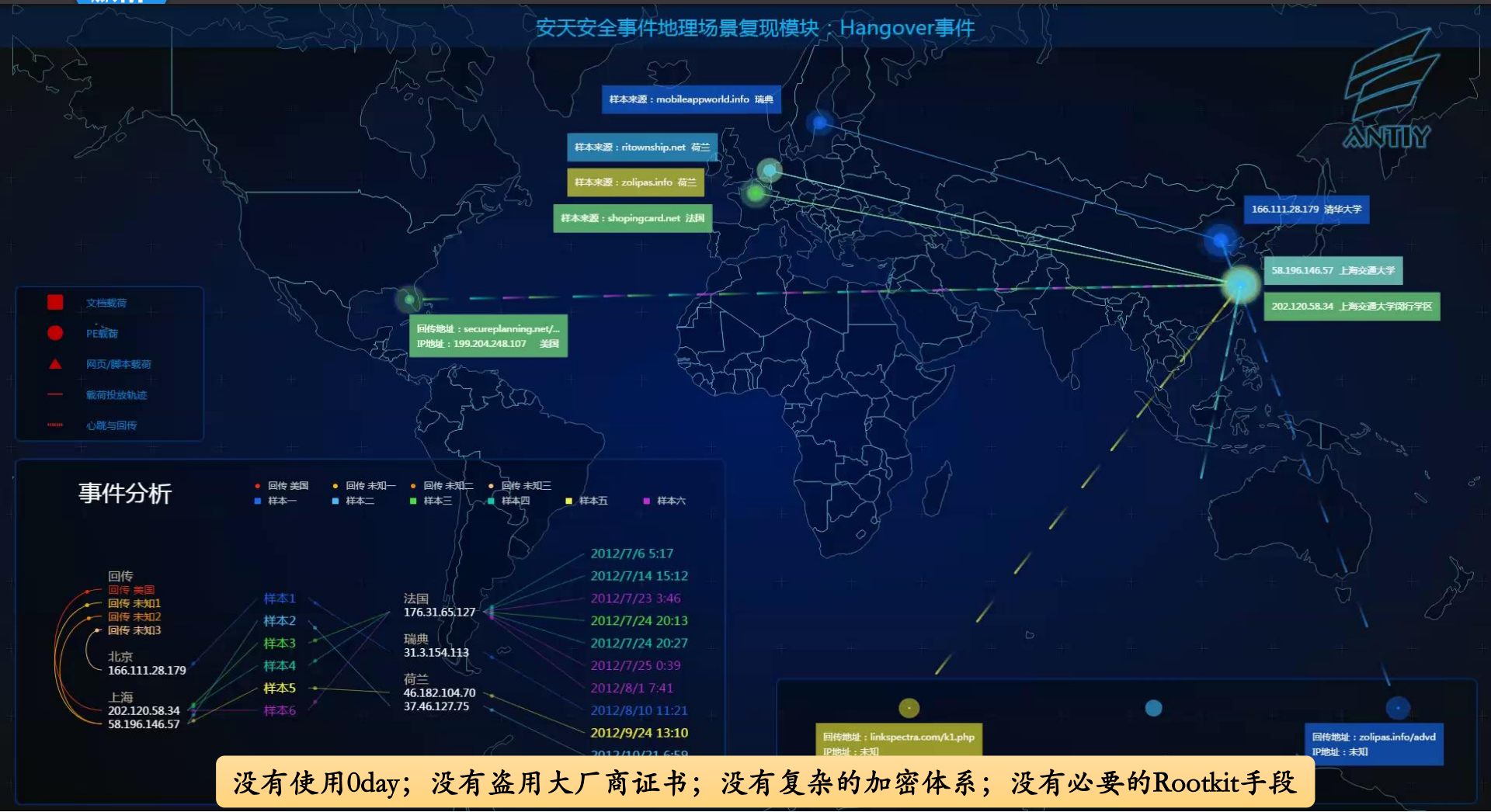
- 部分RAT：
  - ✓ Poison Ivy RAT
  - ✓ Gh0st
  - ✓ HttpBots
  - ✓ ZXSHELL


安天安全可视化系统：持续威胁事件浮现
某攻击事件地理场景复现
EXE
MHT
未知区域
北京
杭州
萌
动态复现模块
基于第三方获取的恶意PE文件统计(近段)
恶意PE文件数量
55
存在C&C域名
50
存在C&C IP
29
存在回传域名
10
存在回传IP
6
2013/12/6
显示全部

高明的对手

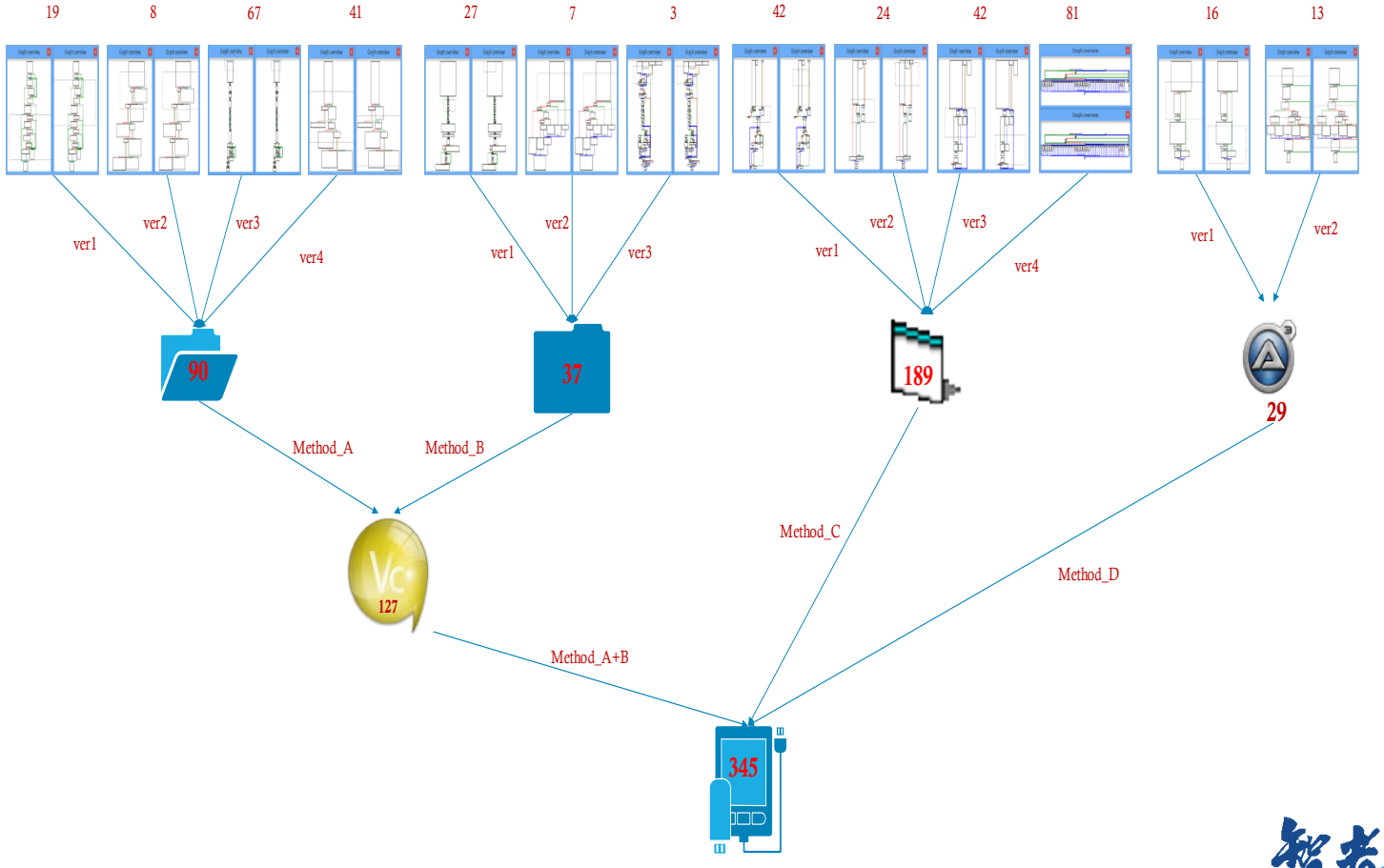
1. 有一定的0day储备，但不够充分
2. 载荷部分高度复杂，高度模块化
3. 部分采用了加密策略，采用SNS等做为逃避检测手段
4. 以网络植入为主
5. 部分采用了无文件载体技术
6. 较好的使用了持久化思路
7. 覆盖主流操作系统平台（含移动）

是谁攻击了中国的高等院校

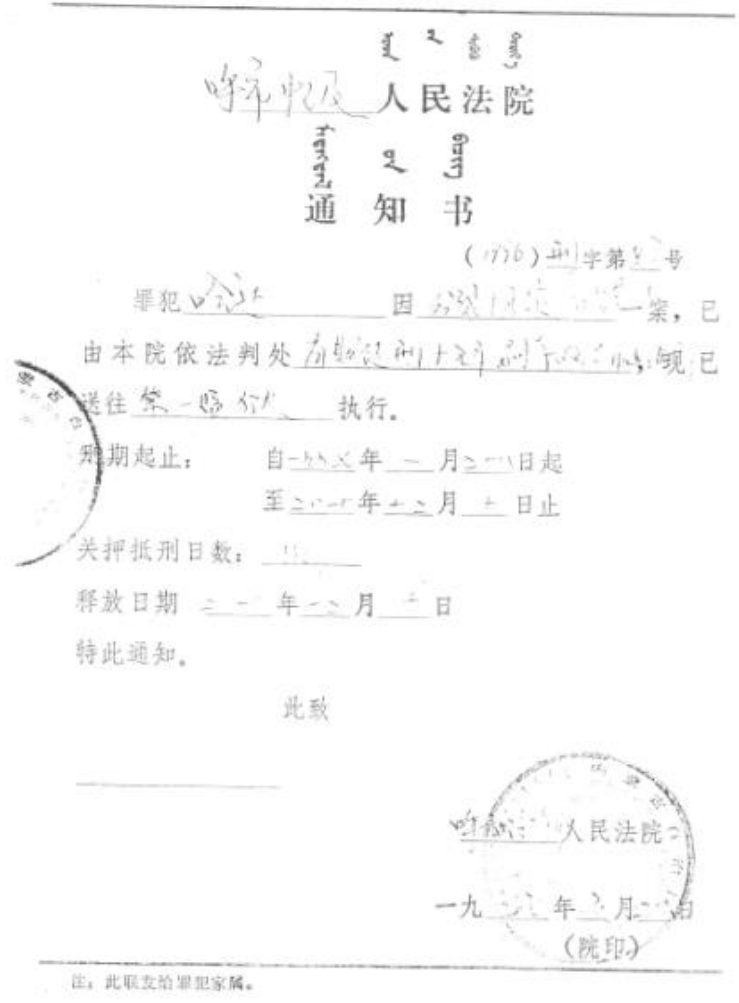


没有使用0day；没有盗用大厂商证书；没有复杂的加密体系；没有必要的Rootkit手段

“不够A”的APT：Hangover中的人海战术



社会工程和样本组合



人民法院

通 知 书

（ ）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。

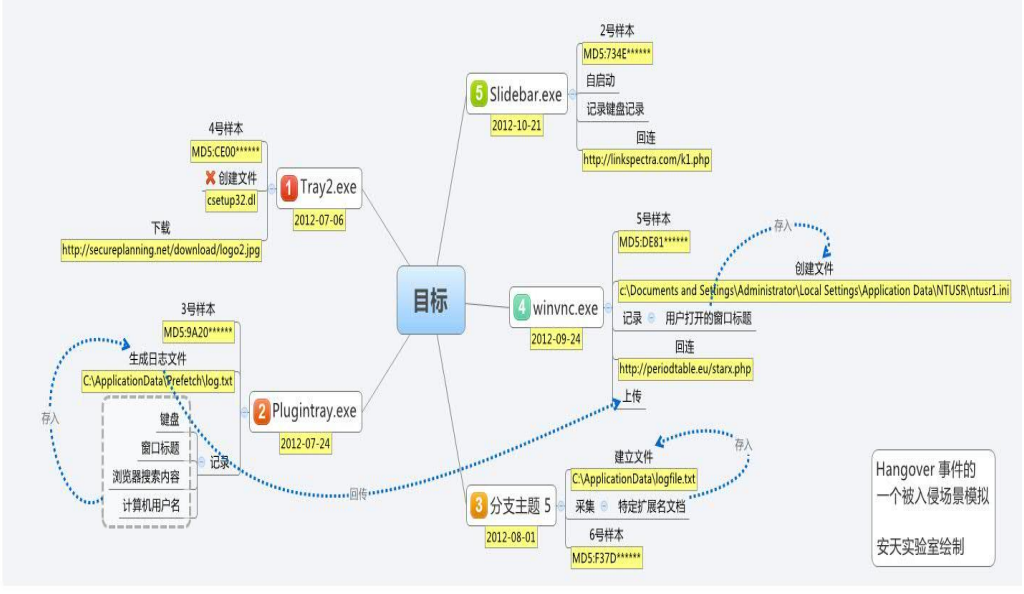
此致

人民法院

一九 年 月 日

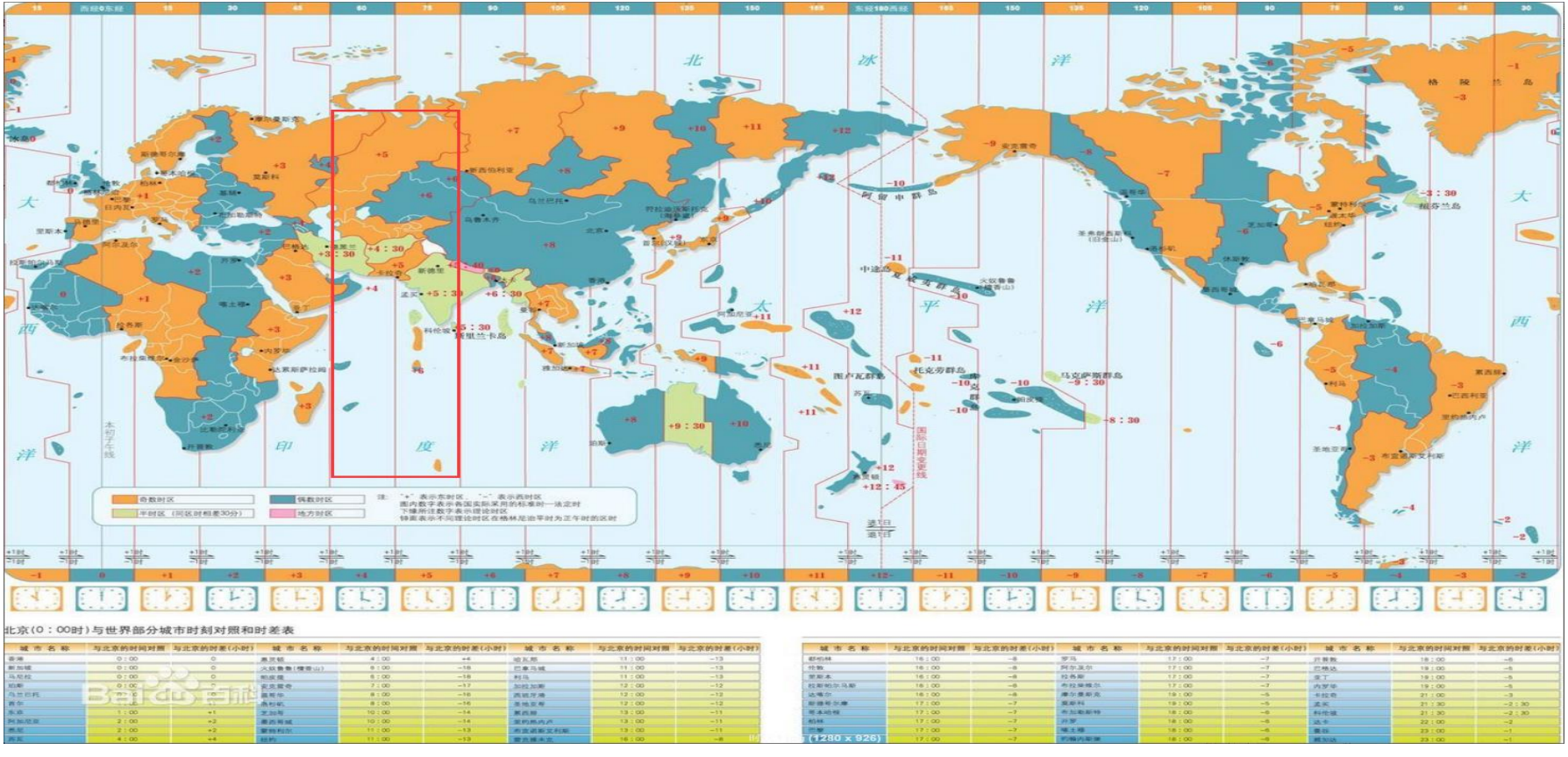
（院印）

注：此联交给罪犯家属。



攻击上海交大的样本组合分析

追踪、再追踪



分析报告请见《安天技术文章汇编.高级持续威胁第二分册》
《HANGOVER攻击事件回顾及部分样本分析》

轻量级APT攻击——火枪弹

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

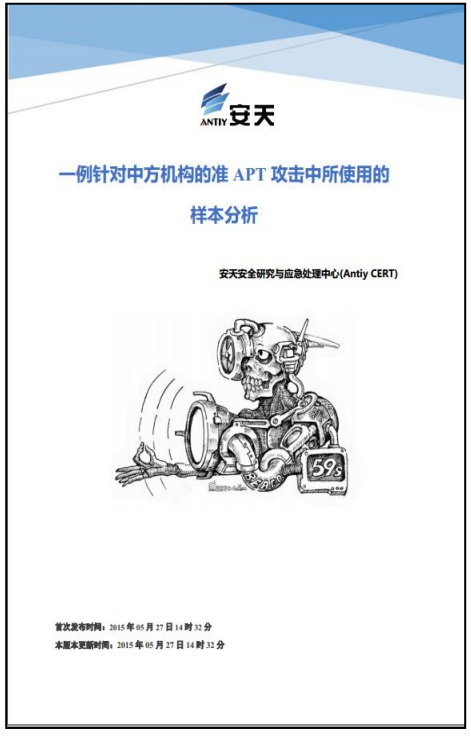
05

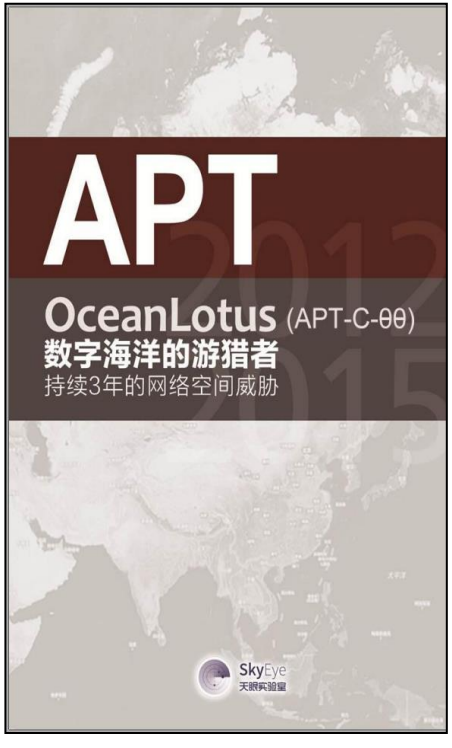
缺少必要的持久
化能力

06

主要针对
Windows系统平
台作业

值得关注的新形势：网络军备扩散（某国相关事件）

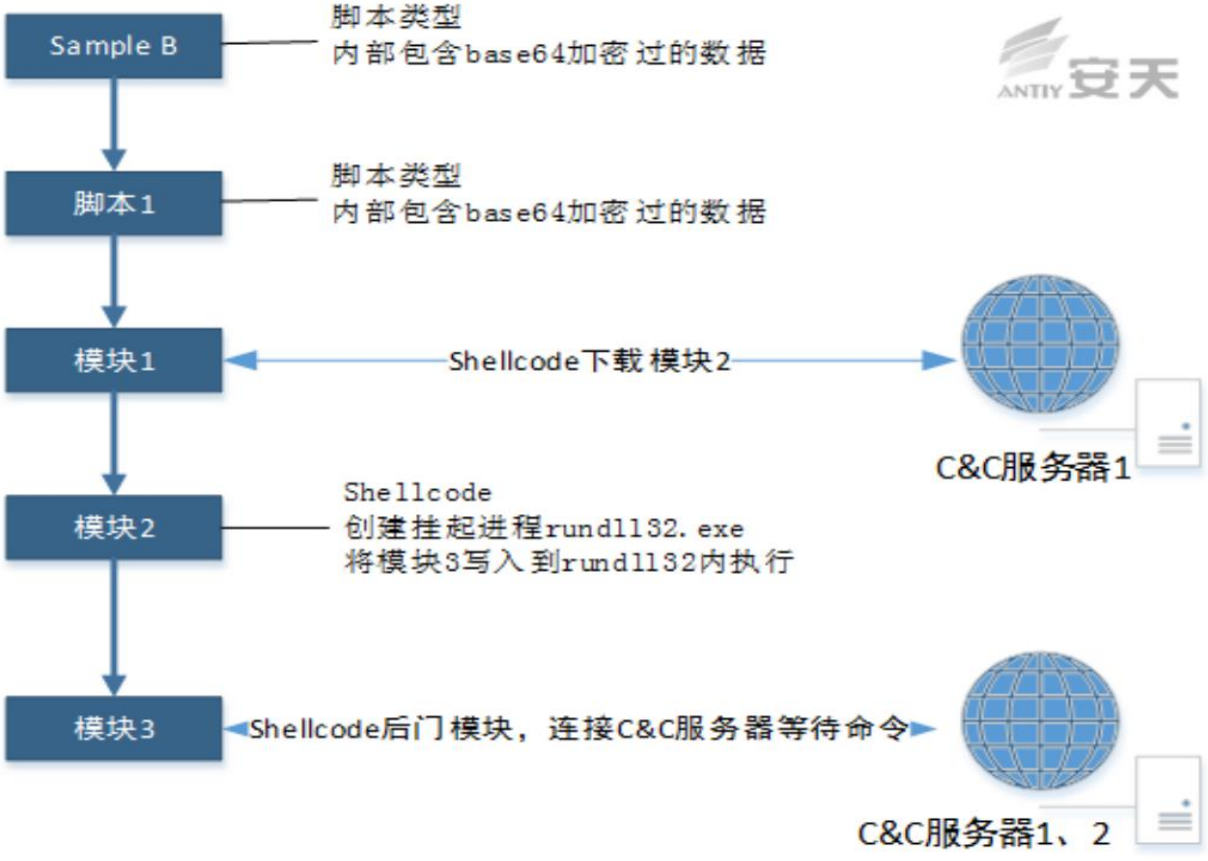




中国厂商自2015年5月27日起连续曝光境外APT，以上三篇文章是针对同一个对手的不同角度解读

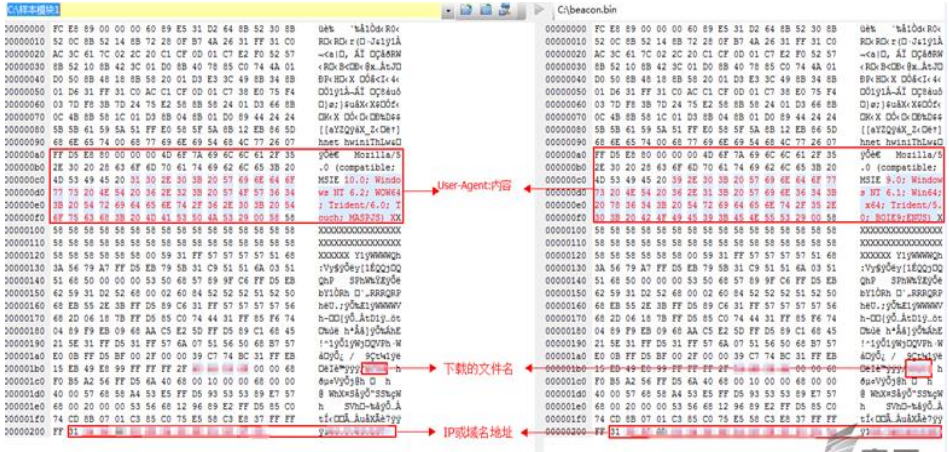
一个场景下的作业手段

APT-TOCS模块关系

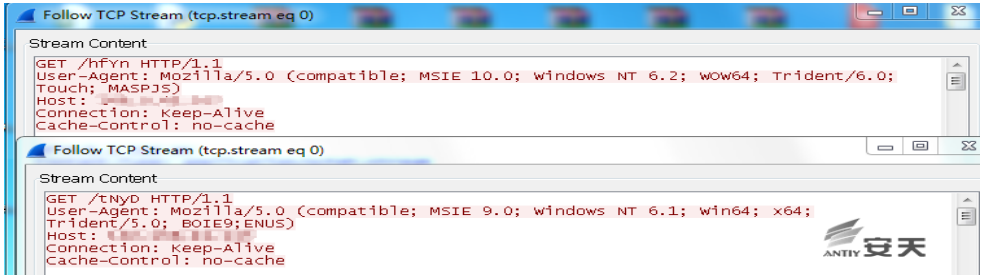


来源：2015.05.28 安天《一例针对中国官方机构的准APT攻击分析》

具有“艺术水准的攻击” 从何而来？



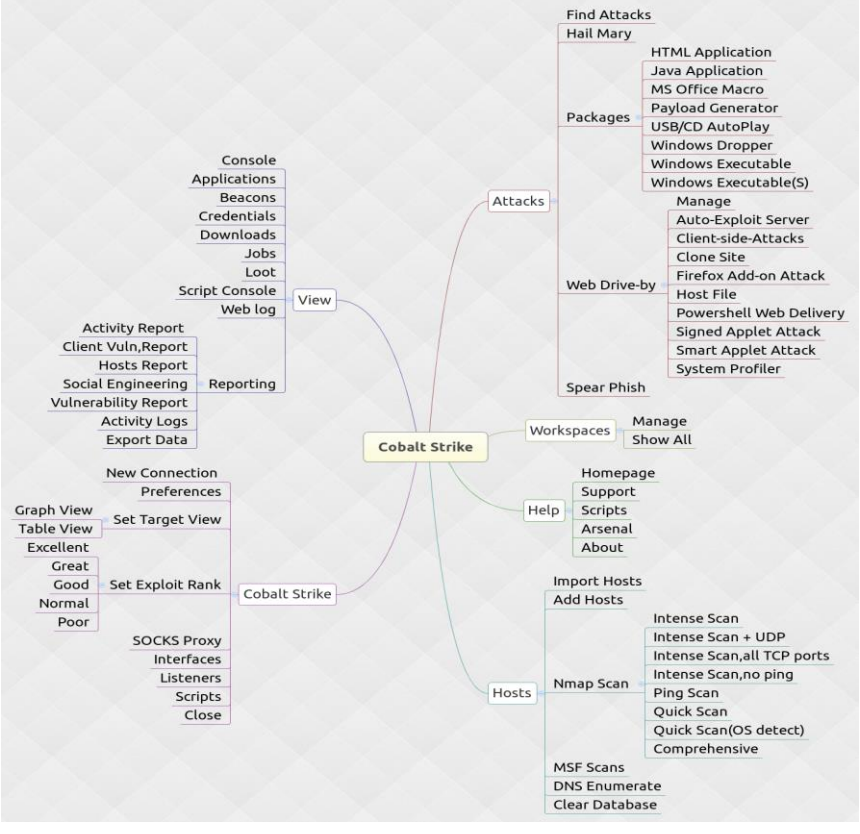
攻击样本与Cobalt Strike攻击平台生成的样本比较



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》

- 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
- ……

CS平台作者信息

- **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

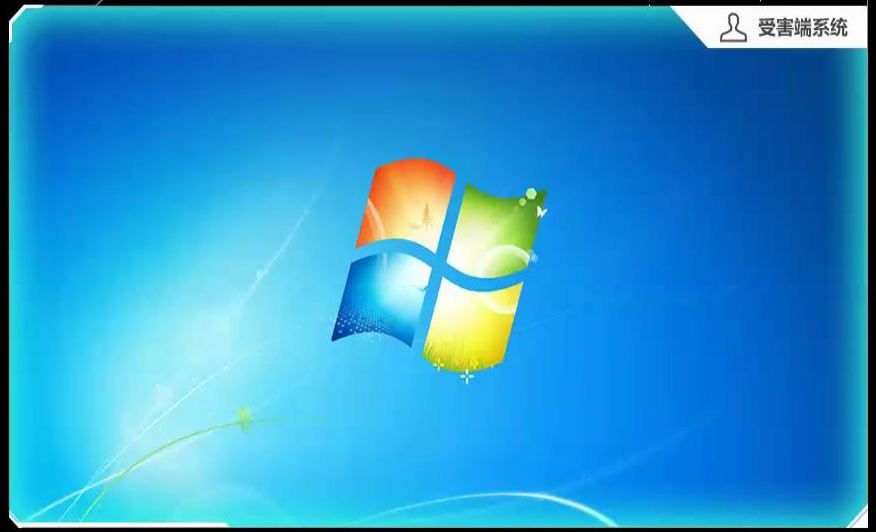
公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6
Automattic	代码Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息 军官	2004.3-2008-3

APT攻击流程

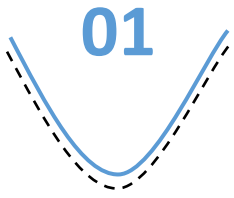
APT-TOCS

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

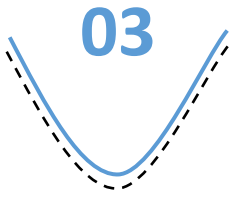


商业军火扩散后的攻击特点——被贩卖的高精度弹

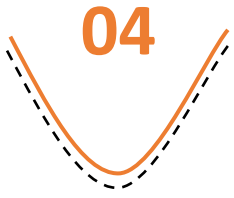


可能使用商用漏洞

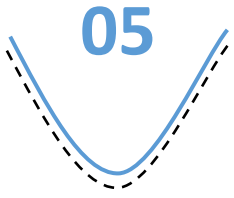
使用商业木马



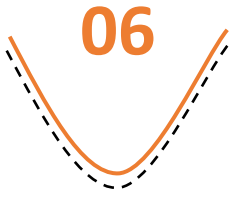
采用攻击平台投放



依托攻击平台的持久化能力

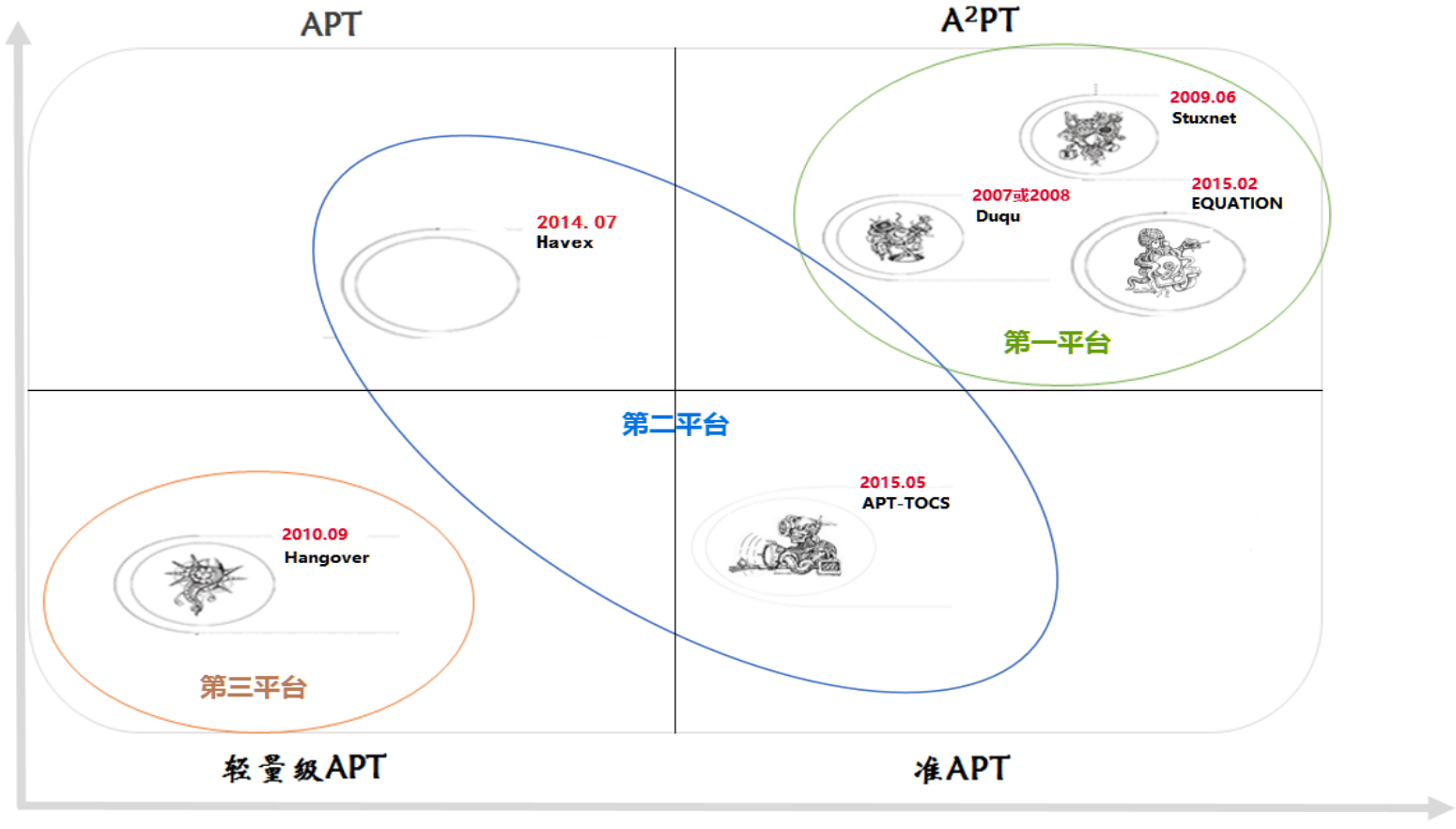


依赖攻击平台设定的联系方式



可能覆盖主要操作系统

总结：不同对手的高级持续攻击的能力层次

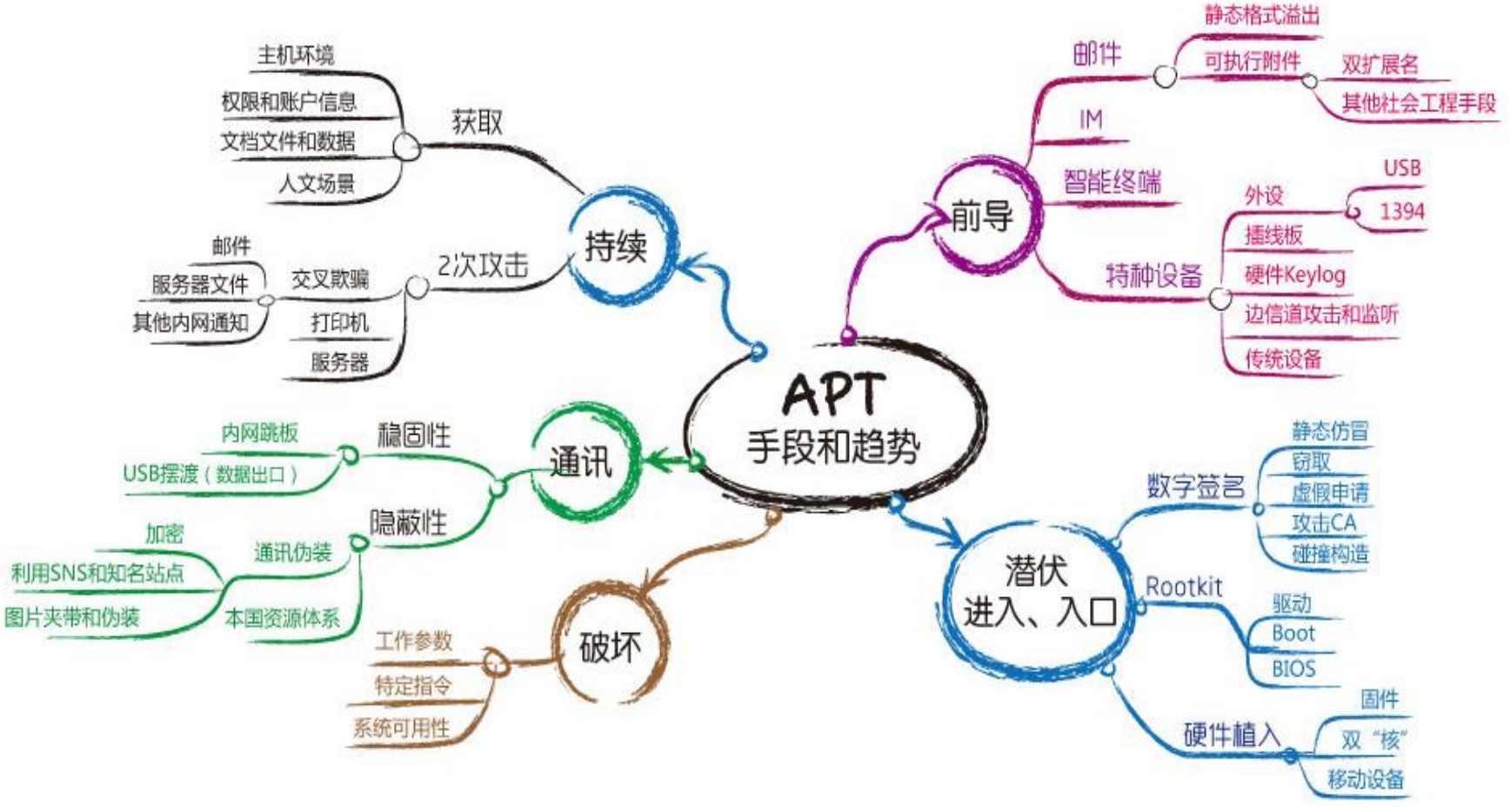


04

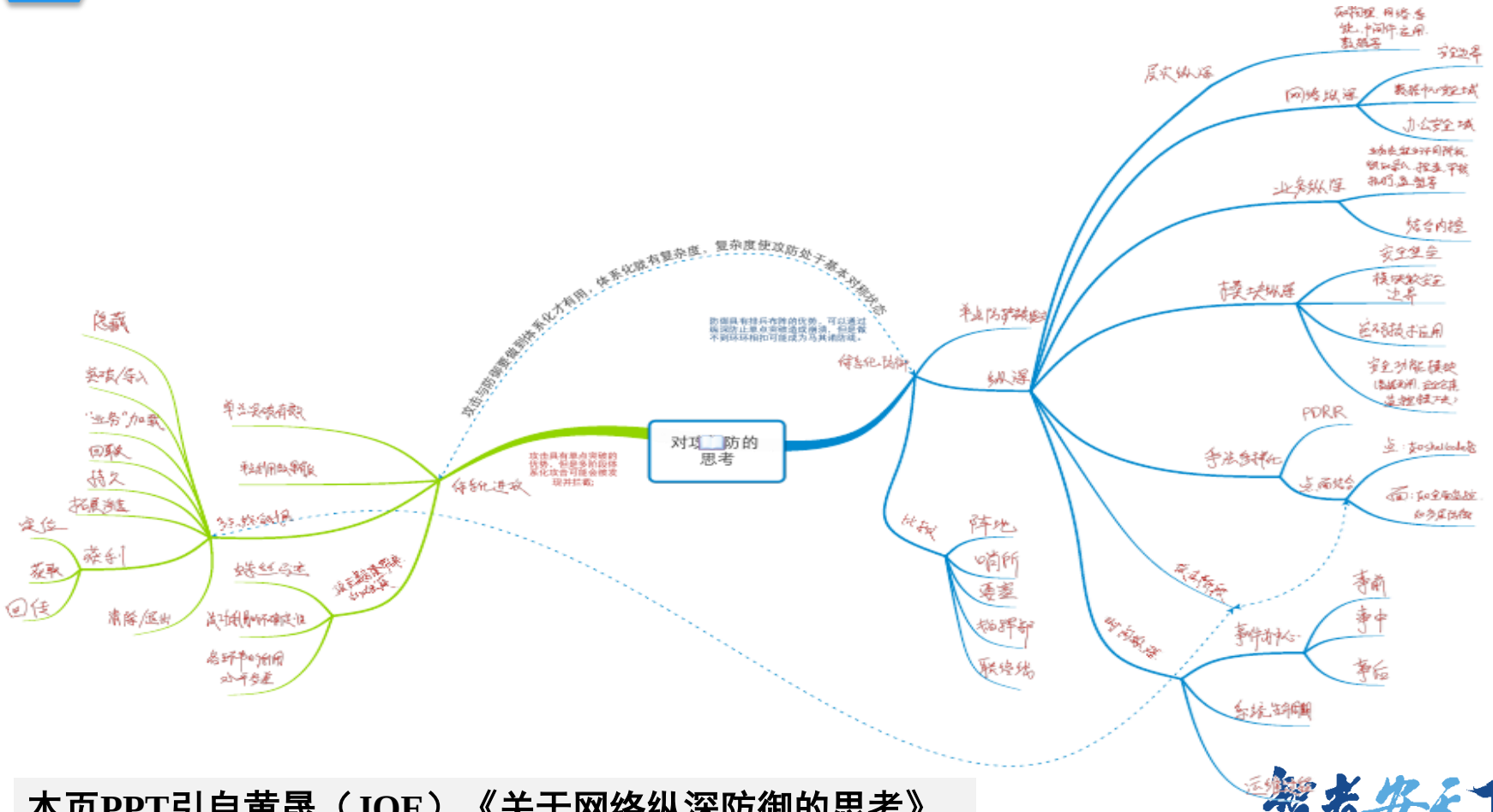
PART Four

防御体系与新的布防点

高级持续威胁是攻击方法和技巧的集大成者



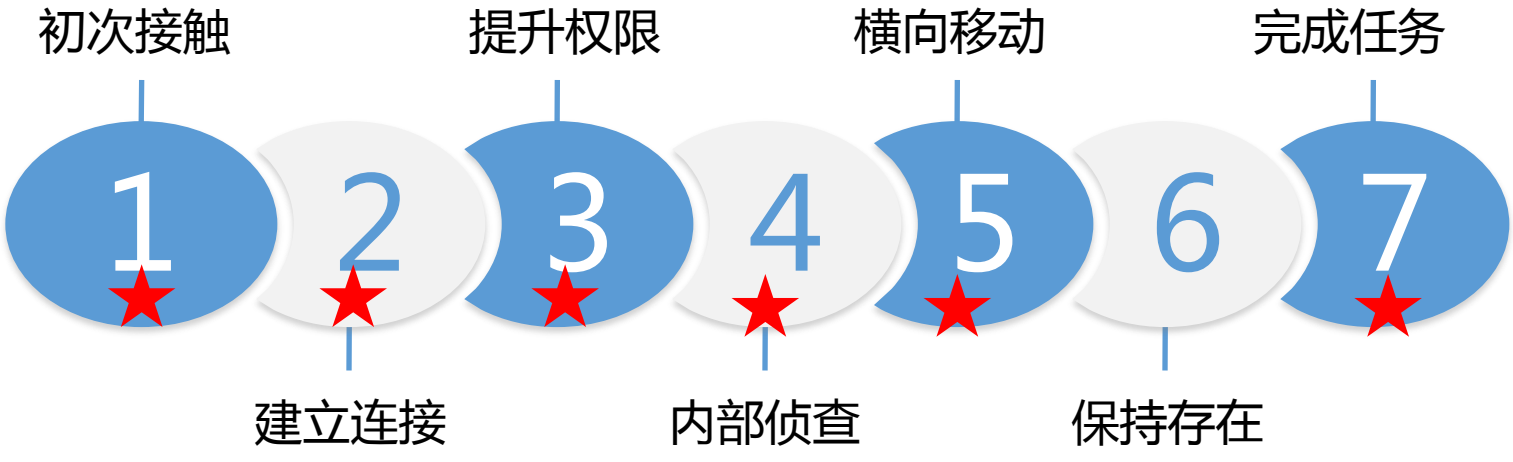
对体系化进攻，需要应对以纵深防御



本页PPT引自黄晟（JOE）《关于网络纵深防御的思考》

核心思路：切断作业链（杀伤链？）

APT一般的攻击步骤：



标星的是恶意代码传输和活跃的步骤

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

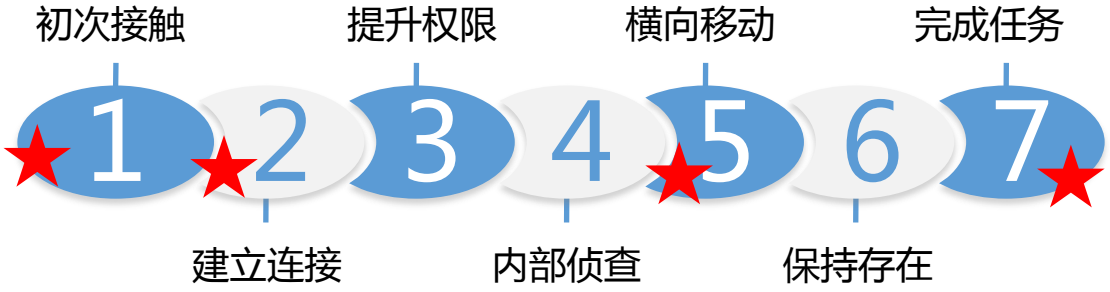
反病毒

- 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

新布防点——入口与关键内网深度检测与缓存



价值—发现威胁

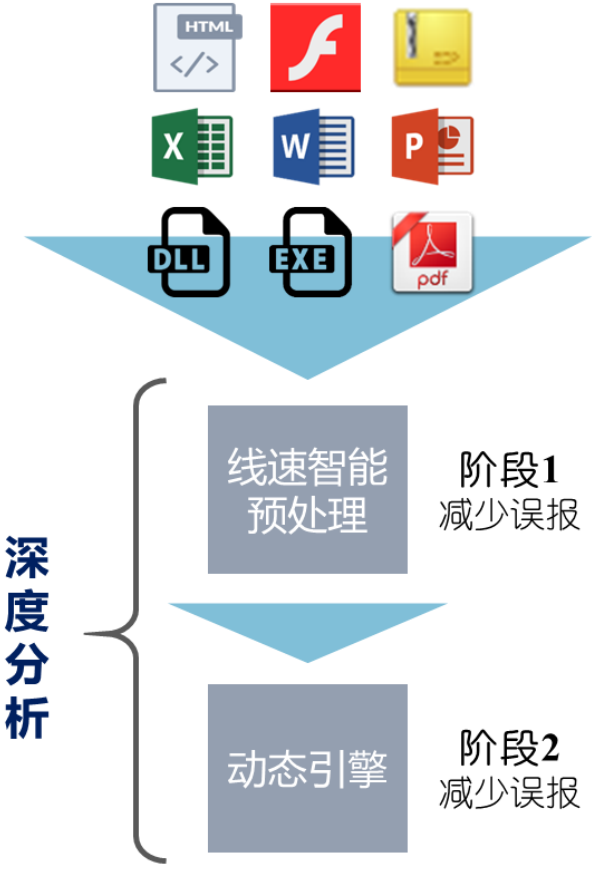
- 恶意代码（木马等）进入网络
- 恶意代码在网内横向移动
- 未知威胁捕获，向分析设备提交
- 威胁追溯（IP、URL、域名）

功能

- 协议解析、文件还原留存
- 威胁元数据记录
- 已知恶意代码检测
- 未知分析能力联动
- 向前回溯
- 横向移动检测

新布防点——本地化沙箱动态分析

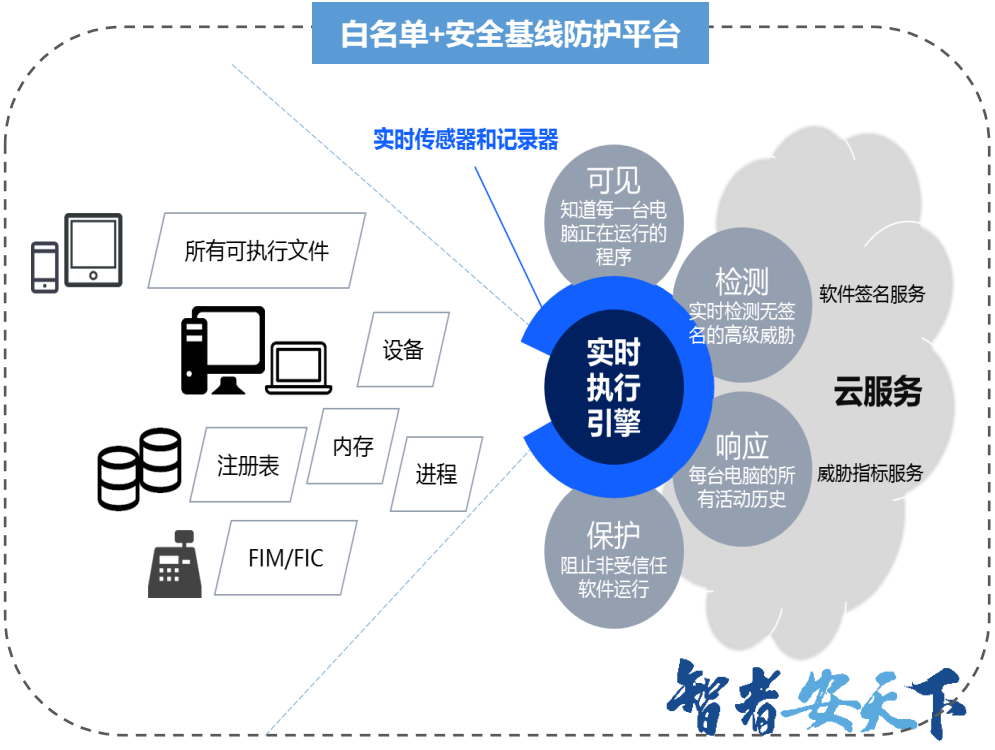
1. 可疑文件异步分析，丰富线索关联
2. 发现未知恶意文件
3. 发现0day/1day漏洞
4. 将发现同步给系统内其他安全设备处置



新布防点：白名单+安全基线

初次接触 → 建立连接 → 提升权限 → 内部侦查 → 横向移动 → 保持存在 → 完成任务

1. 阻止非授权文件的入侵和启动
2. 鉴定可疑文件的属性
3. 追溯处置恶意文件



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。向量提取。

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

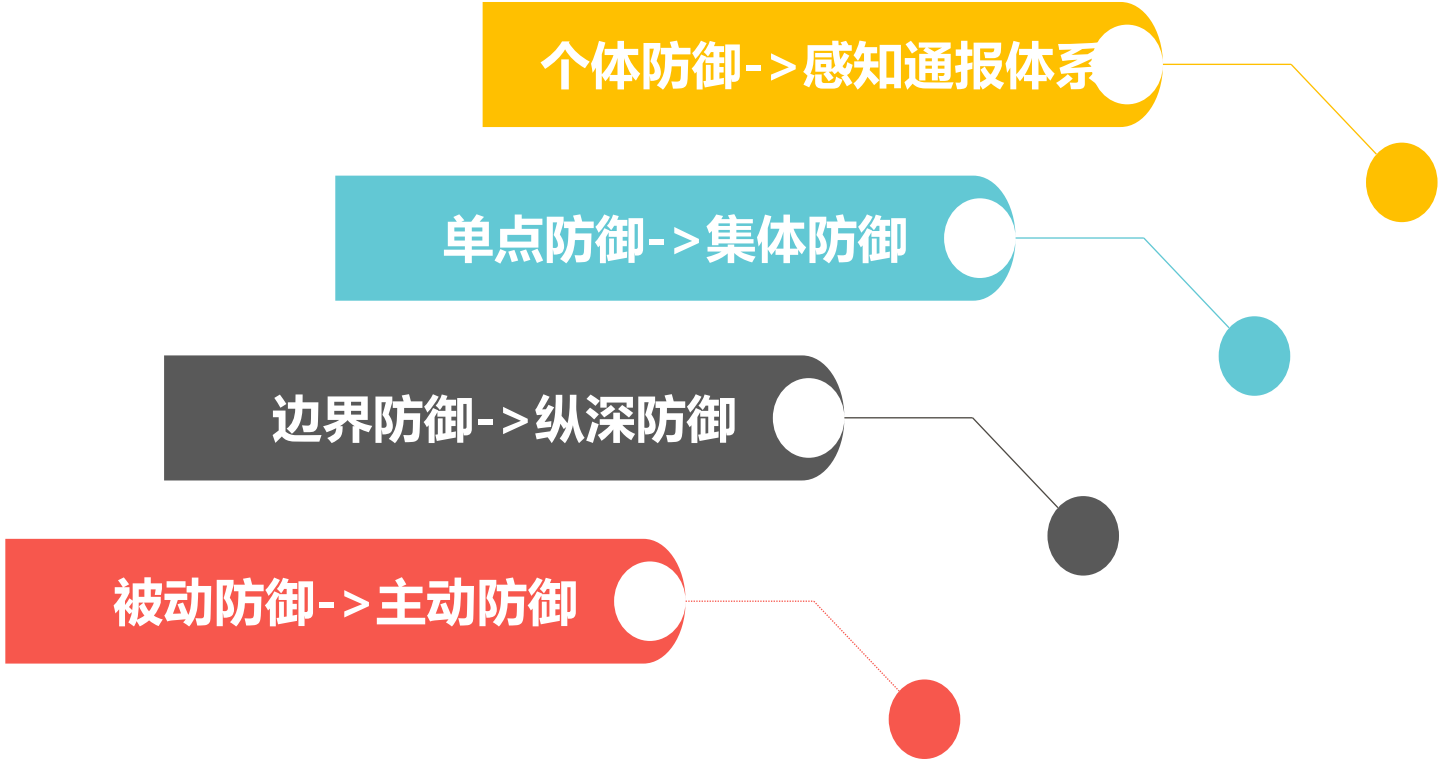
控制对手的网络横向移动

06

数据集中分析

建立动态信誉能力，建立情报整合能力。

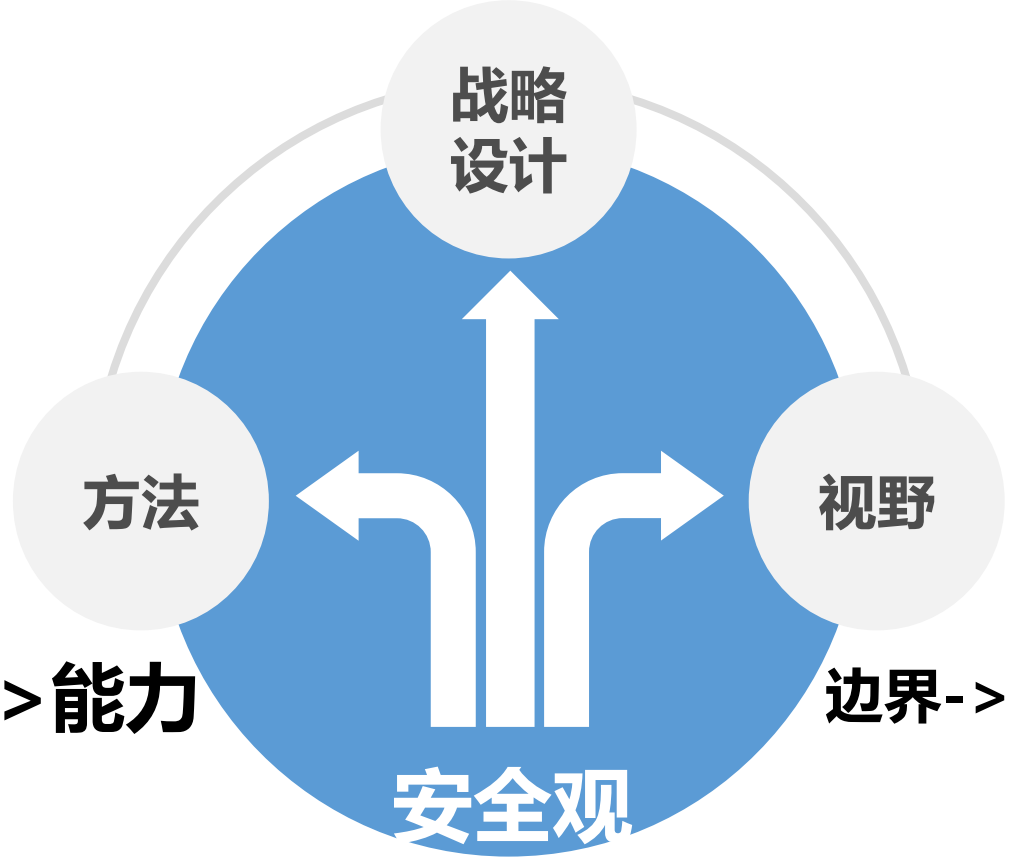
防御能力来自安全思路转换



内部防御能力来自于产品、策略、管理与支撑能力组成的综合工程体系。
外部能力支撑来自于感知、预警、通报、朔源体系。

结尾：安全观的变革

治理->博弈



合规->能力

边界->国土

THANKS

即使面对最高明的狙击手，我们也相信弹道有痕！

智者安天下