寻找APT的关键词

——APT的本质思考

安天实验室 江海客

提纲

查询：APT的图景、起源和已有的定义

回朔：APT的历史与恶意代码历史的比对

总结：重新审视差异化

折射：多余的话

查询：APT的起源和已有的定义

APT的起源

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

UKCERT

定向攻击

2005 2010

参考资料：维基百科 Advanced Persistent Threat
http://en.wikipedia.org/wiki/Advanced_persistent_threat

APT的起源(说法二)

“APT”一词最初起源于2005-2006年间在空军工作的网络安全工程师们对于一些安全事件的描述，他们创造了这个词以使公众不对此类安全事件小题大做……

——Peter Cap在Bruce Blog上的留言


Bruce Schneier

Schneier on Security

A blog covering security and security technology.

« Unlocking any iPad2 using a Smart Cover | Main | Commentary on Strong Passwords »

November 9, 2011

Advanced Persistent Threat (APT)

It's taken me a few years, but I've come around to this buzzword. It highlights an important characteristic of a particular sort of Internet attacker.

A conventional hacker or criminal isn't interested in any particular target. He wants a thousand credit card numbers for fraud, or to break into an account and turn it into a zombie, or whatever. Security against this sort of attacker is relative; as long as you're more secure than almost everyone else, the attackers will go after other people, not you. An APT is different; it's an attacker who -- for whatever reason -- wants to attack you. Against this sort of attacker, the absolute level of your security is what's important. It doesn't matter how secure you are compared to your peers; all that matters is whether you're secure enough to keep him out.

APT attackers are more highly motivated. They're likely to be better skilled, better funded, and more patient. They're likely to try several different avenues of attack. And they're much more likely to succeed.

This is why APT is a ... buzzw...

Subscribe

Subscribe via Kindle



Peter Cap

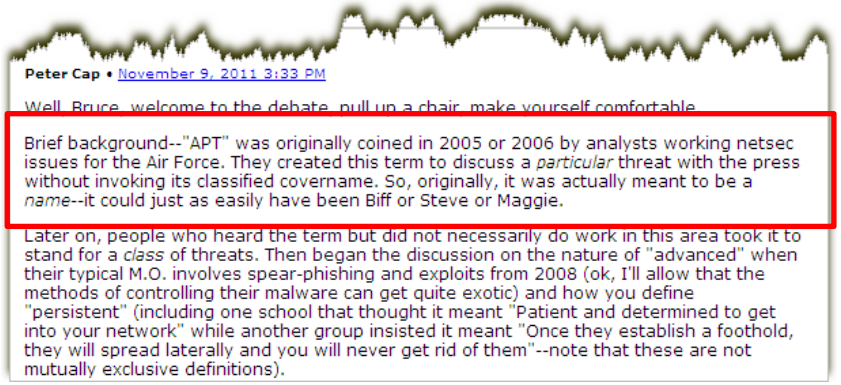
Threat Analyst at Microsoft

Redmond, Washington | Computer & Network Security

Previous Symantec Corporation, US Navy

Education Beloit College

Connect | Send Peter InMail


Peter Cap • November 9, 2011 3:33 PM

Well, Bruce, welcome to the debate, pull up a chair, make yourself comfortable.

Brief background--"APT" was originally coined in 2005 or 2006 by analysts working netsec issues for the Air Force. They created this term to discuss a *particular* threat with the press without invoking its classified covername. So, originally, it was actually meant to be a *name*--it could just as easily have been Biff or Steve or Maggie.

Later on, people who heard the term but did not necessarily do work in this area took it to stand for a *class* of threats. Then began the discussion on the nature of "advanced" when their typical M.O. involves spear-phishing and exploits from 2008 (ok, I'll allow that the methods of controlling their malware can get quite exotic) and how you define "persistent" (including one school that thought it meant "Patient and determined to get into your network" while another group insisted it meant "Once they establish a foothold, they will spread laterally and you will never get rid of them"--note that these are not mutually exclusive definitions).

参考资料：https://www.schneier.com/blog/archives/2011/11/advanced_persis.html

APT的现有定义（一）

通常APT指的是由**特定组织**（政府）针对**某一特定目标**实体具备**持续**且**有效**的攻击**能力**及**动机**的**威胁**。这个词通常也被视为是**网络威胁**，尤其是**采用基于互联网（物联网）方式**的情报收集技术来访问敏感信息的网络威胁。与个体入侵者相比而言，后者缺乏保持**高级**且长期**持续**的足够**资源**。

—— Dell SecureWorks相关文档

The Anatomy of Advanced Persistent Threats

Advanced Persistent Threats (APT) are here, and they represent a threat to an organization's intellectual property, financial assets and even reputation. In many cases, these threats target critical infrastructure and government suppliers – and the defensive tools, procedures and other controls usually put in place are ineffective against targeted APT attacks.

Those behind these new and complex intrusions are dead-focused on a specific target, and are able to customize or adapt their tactics, techniques and penetration procedures to bypass most of your security controls. As in any other case, the first step to managing APT risk is to gain awareness and understanding of these types of threats. In this guide learn about the lifecycle of APT-style attacks, and get tips for protecting against these kinds of intrusions, including:

APT的现有定义（二）

能力优越的攻击团队成功地“扩展”了（攻击）目标，包括政府和国防相关的目标、研究人员、制造商、律师事务所、甚至非盈利组织。

这些攻击看似由受资助的、有组织的群体实施。我们称他们为“高级持续性威胁”

——Mandiant 《M-Trends》

APT的现有标准

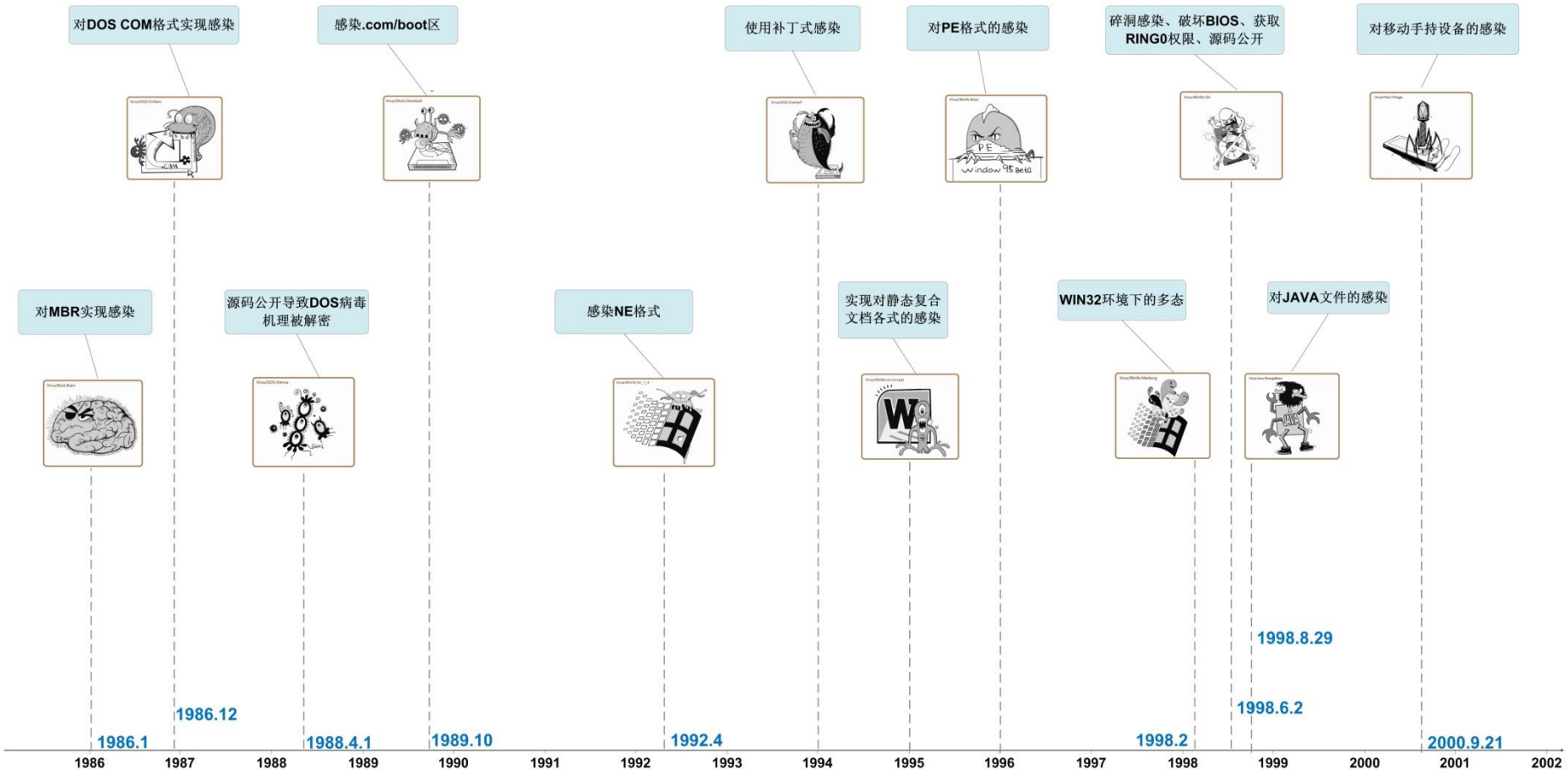
目标	• 威胁终极目标，敌人
时间性	• 投入时间探测并访问你的系统
资源	• 所需知识、工具
风险容忍度	• 保持无法被检测越久
技能与方法	• 所需技能、方法
行动	• 精准行动，精确打击
攻击源点	• 源点数量多寡
攻击相关数字	• 有多少内外部系统牵涉其中，多少内外部人员牵涉其中，影响/重要性大小/高低
知识源	• 在线信息收集，社工方式

By Carpenter，参见："An Evolving Crisis"

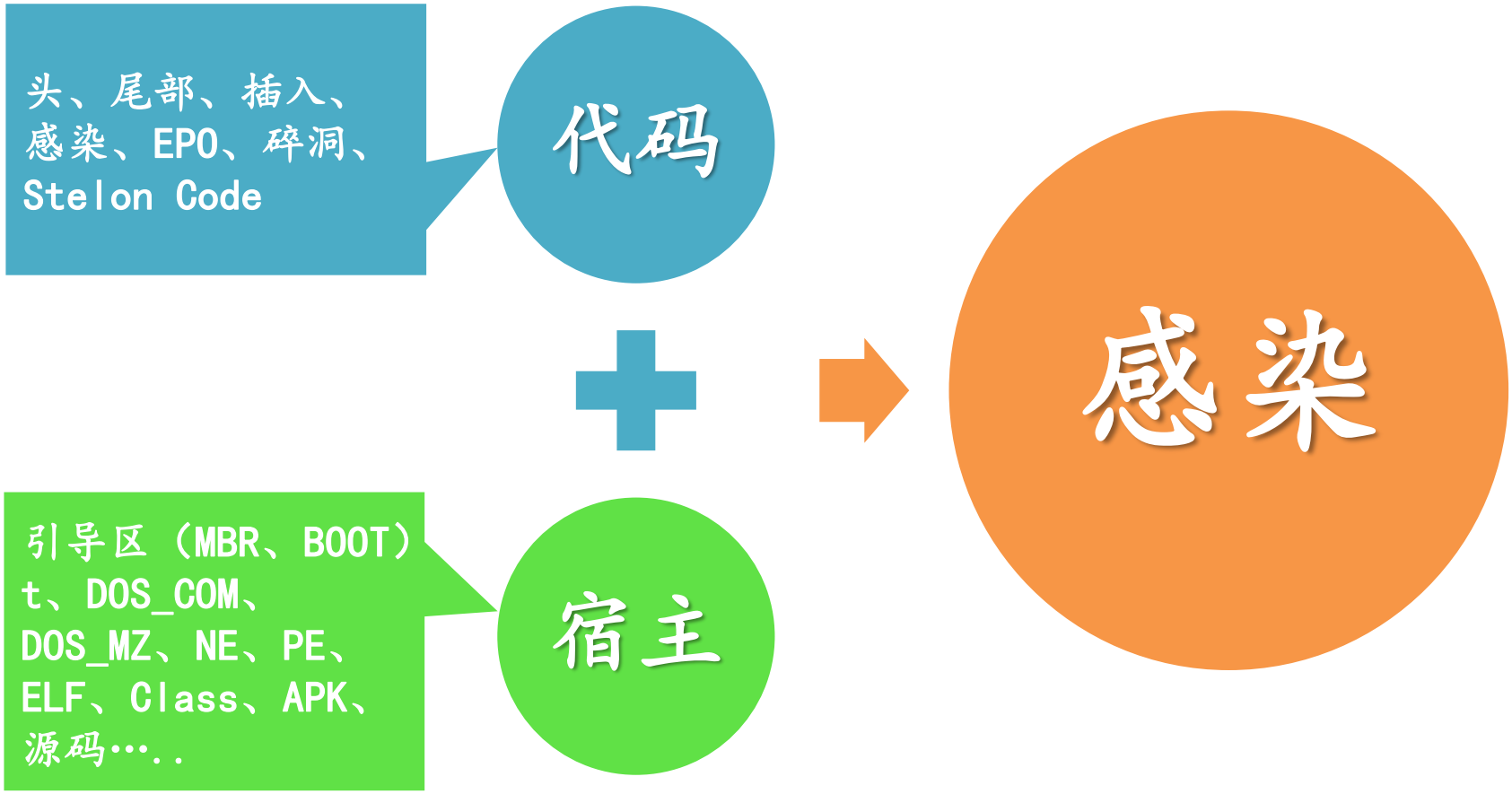
回朔:从恶意代码历史寻找APT的前身

从恶意代码分类说起

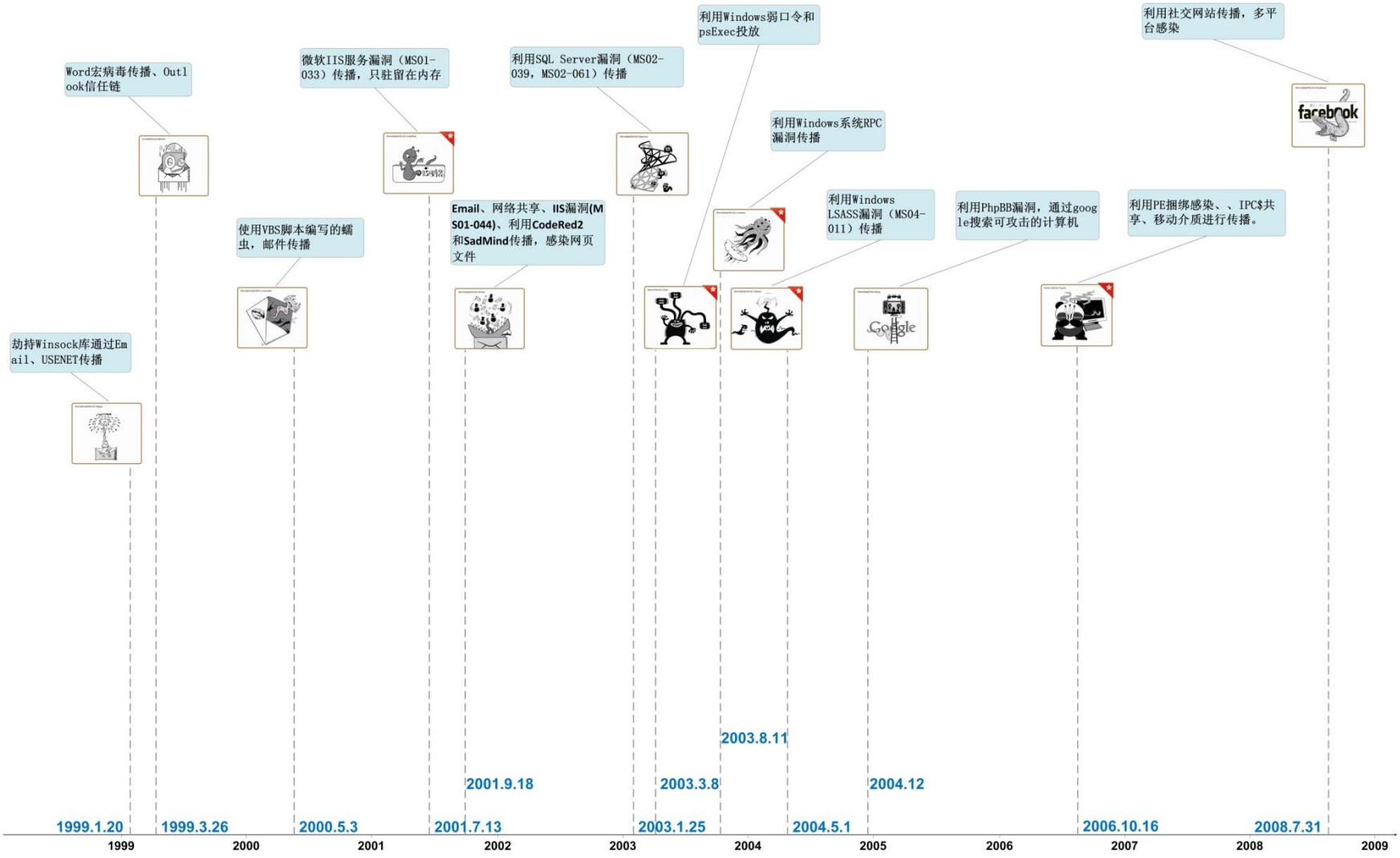
（感染式）病毒的演进


对DOS COM格式实现感染
感染.com/boot区
使用补丁式感染
对PE格式的感染
碎洞感染、破坏BIOS、获取RING0权限、源码公开
对移动手持设备的感染
对MBR实现感染
源码公开导致DOS病毒机理被解密
感染NE格式
实现对静态复合文档各式的感染
WIN32环境下的多态
对JAVA文件的感染
1986.1
1986.12
1988.4.1
1989.10
1992.4
1998.2
1998.6.2
1998.8.29
2000.9.21
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002

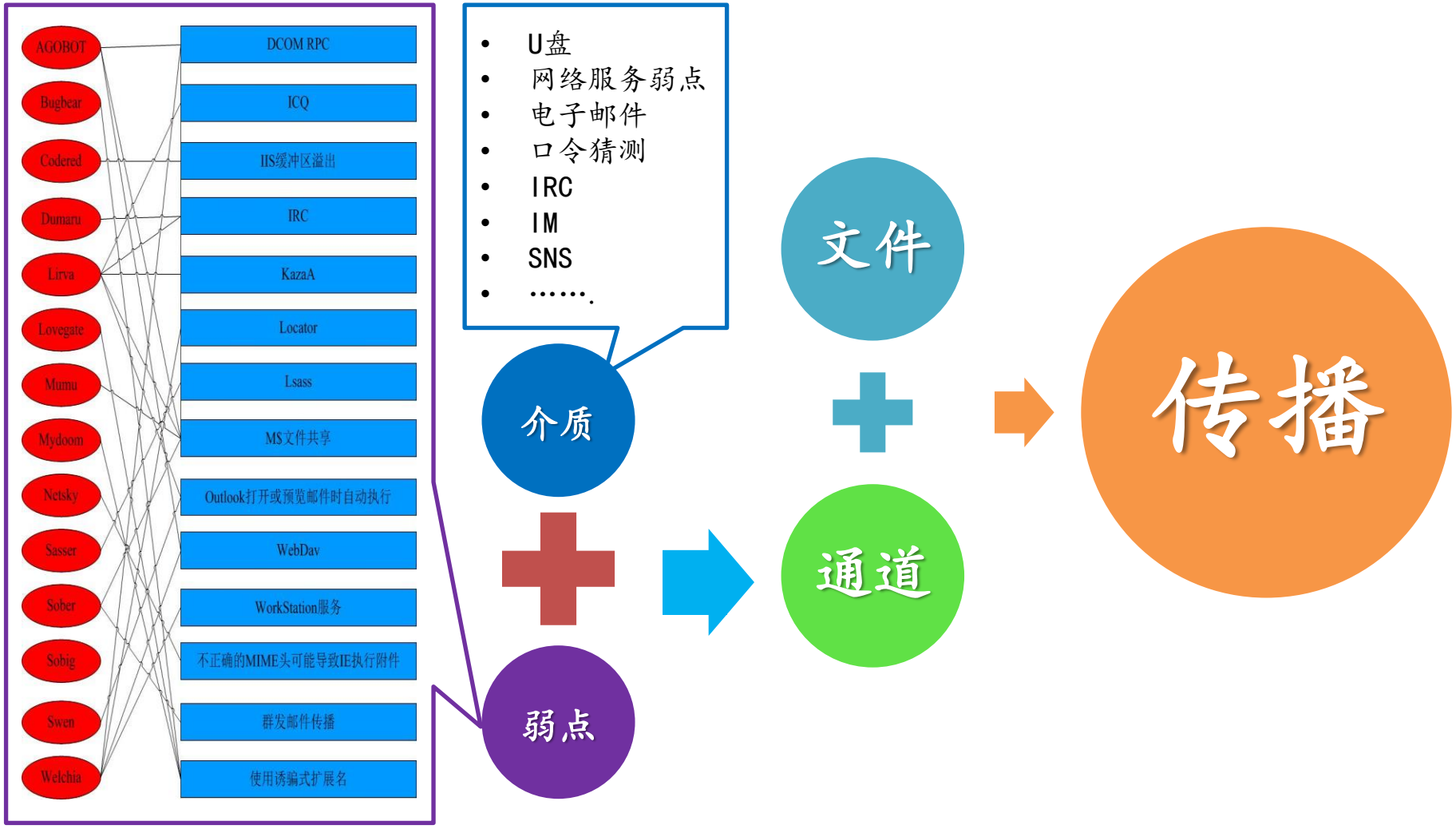
（感染式）病毒的关键词


头、尾部、插入、感染、EPO、碎洞、Stelon Code
代码
引导区（MBR、BOOT）t、DOS_COM、DOS_MZ、NE、PE、ELF、Class、APK、源码…..
宿主
感染

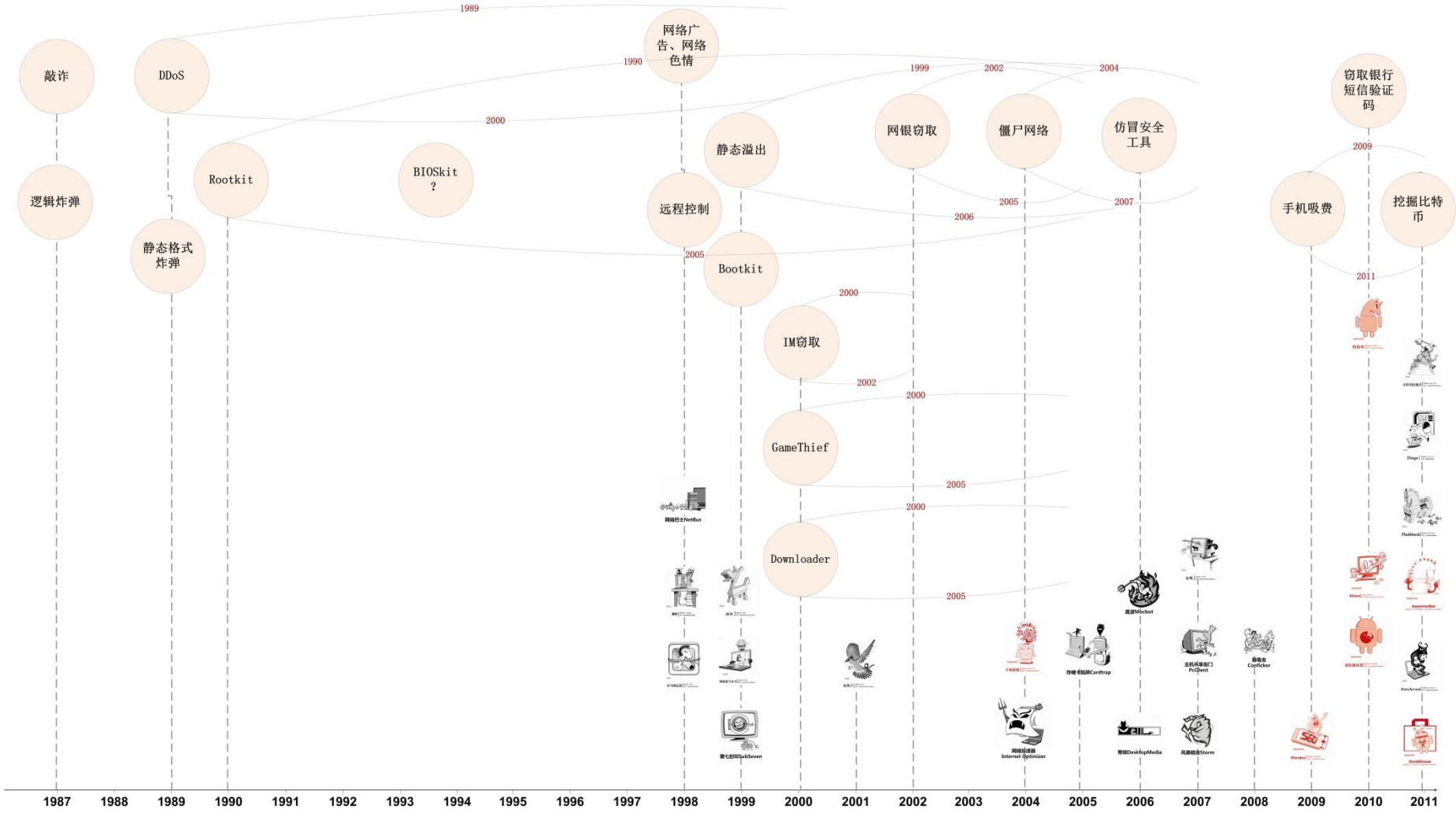
蠕虫的演进


劫持Winsock库通过Email、USENET传播
Word宏病毒传播、Outlook信任链
使用VBS脚本编写的蠕虫，邮件传播
微软IIS服务漏洞（MS01-033）传播，只驻留在内存
Email、网络共享、IIS漏洞(MS01-044)、利用CodeRed2和SadMind传播，感染网页文件
利用SQL Server漏洞（MS02-039，MS02-061）传播
利用Windows弱口令和psExec投放
利用Windows系统RPC漏洞传播
利用Windows LSASS漏洞（MS04-011）传播
利用PhpBB漏洞，通过google搜索可攻击的计算机
利用PE捆绑感染、、IPC$共享、移动介质进行传播。
利用社交网站传播，多平台感染
1999.1.20
1999.3.26
2000.5.3
2001.7.13
2001.9.18
2003.1.25
2003.3.8
2003.8.11
2004.5.1
2004.12
2006.10.16
2008.7.31
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009

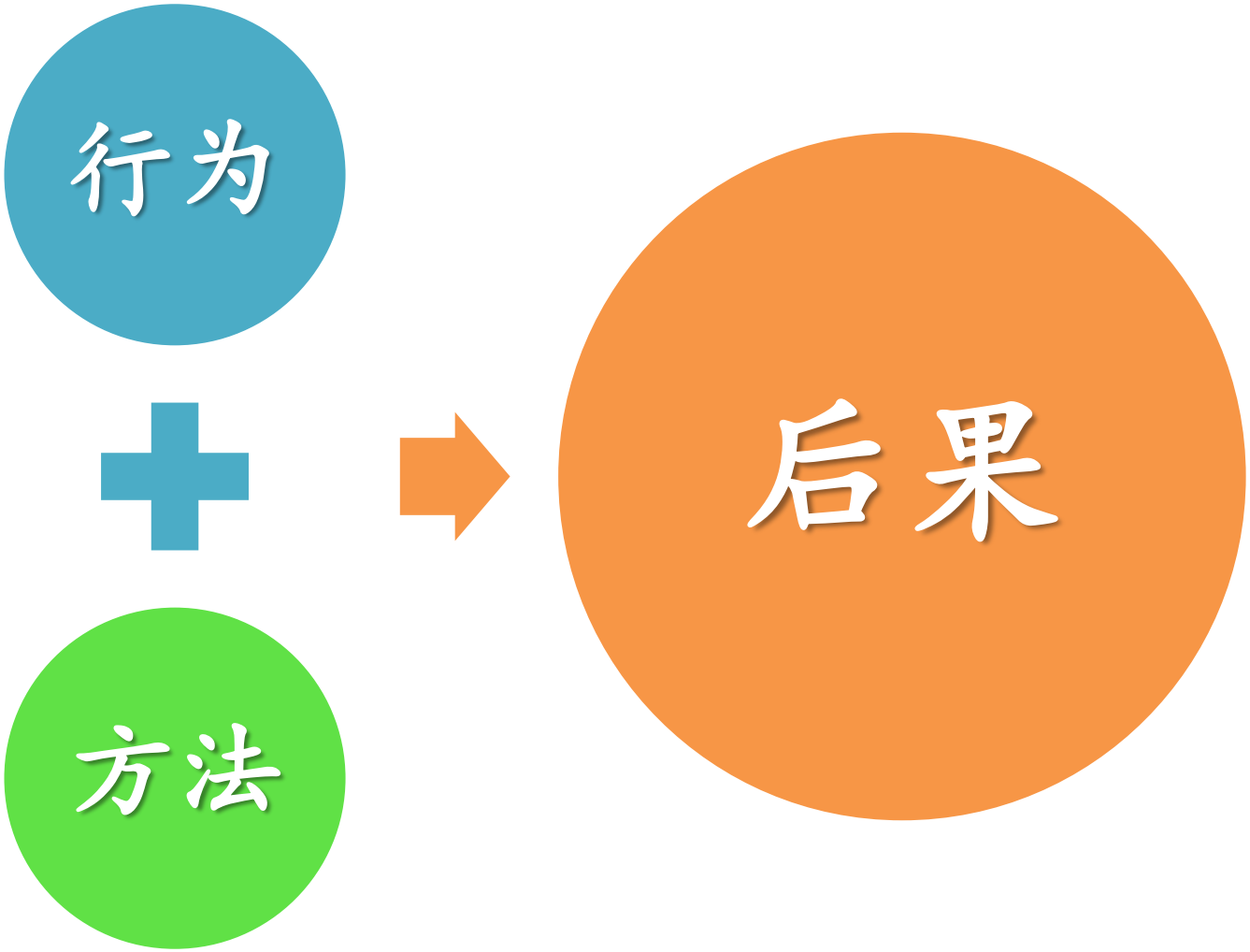
蠕虫的关键词


AGOBOT
Bugbear
Codered
Dumaru
Lirva
Lovegate
Mumu
Mydoom
Netsky
Sasser
Sober
Sobig
Swen
Welchia
DCOM RPC
ICQ
IIS缓冲区溢出
IRC
KazaA
Locator
Lsass
MS文件共享
Outlook打开或预览邮件时自动执行
WebDav
WorkStation服务
不正确的MIME头可能导致IE执行附件
群发邮件传播
使用诱骗式扩展名
U盘
网络服务弱点
电子邮件
口令猜测
IRC
IM
SNS
……
介质
弱点
文件
通道
传播

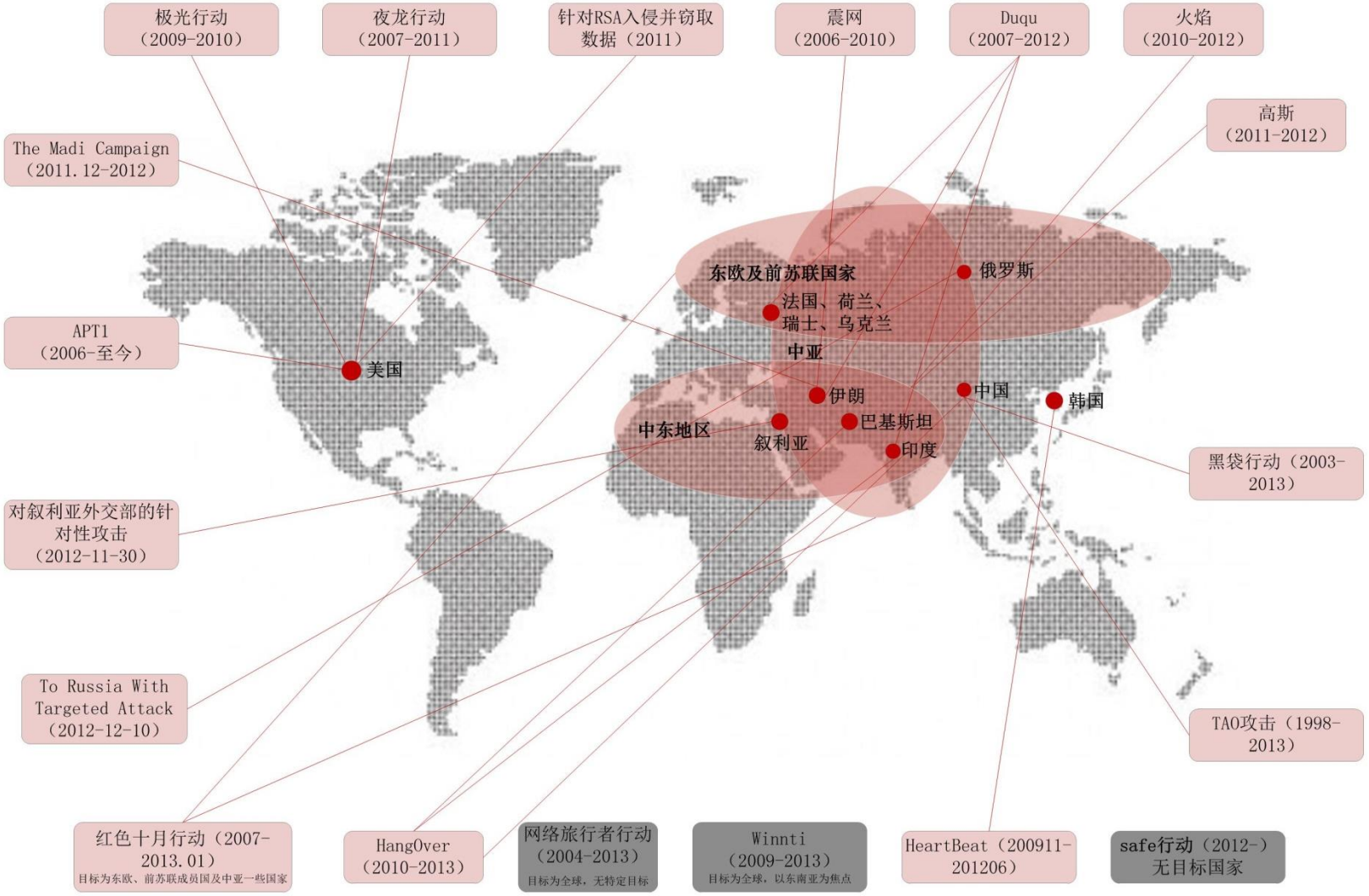
木马的演进


敲诈
DDoS
网络广告、网络色情
窃取银行短信验证码
逻辑炸弹
静态格式炸弹
Rootkit
BIOSkit ?
远程控制
静态溢出
网银窃取
僵尸网络
仿冒安全工具
手机吸费
挖掘比特币
Bootkit
IM窃取
GameThief
Downloader
1989
1990
2000
1999
2002
2004
2009
2005
2006
2007
2011
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011

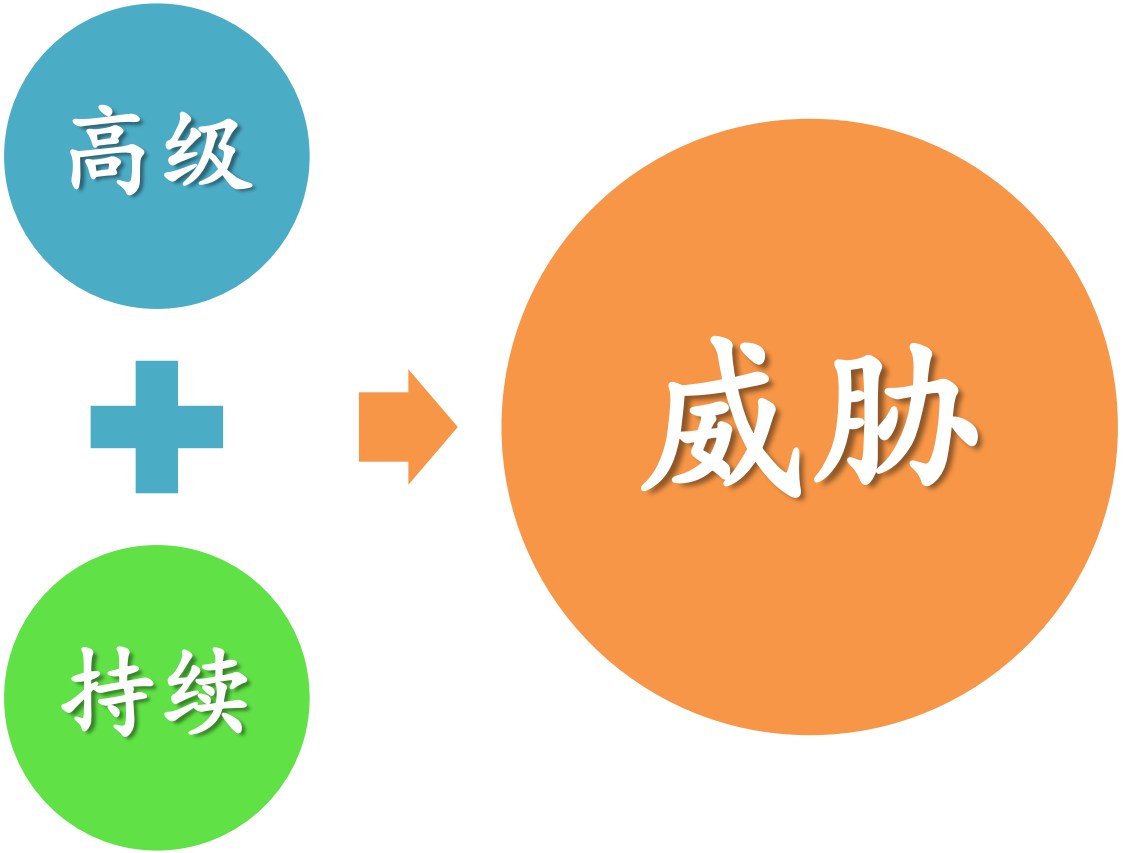
木马的关键词



APT轨迹


极光行动
（2009-2010）
夜龙行动
（2007-2011）
针对RSA入侵并窃取数据（2011）
震网
（2006-2010）
Duqu
（2007-2012）
火焰
（2010-2012）
高斯
（2011-2012）
The Madi Campaign
（2011.12-2012）
APT1
（2006-至今）
美国
东欧及前苏联国家
俄罗斯
法国、荷兰、瑞士、乌克兰
中亚
伊朗
中国
韩国
中东地区
巴基斯坦
叙利亚
印度
黑袋行动（2003-2013）
对叙利亚外交部的针对性攻击
（2012-11-30）
To Russia With Targeted Attack
（2012-12-10）
TAO攻击（1998-2013）
红色十月行动（2007-2013.01）
目标为东欧、前苏联成员国及中亚一些国家
HangOver
（2010-2013）
网络旅行者行动
（2004-2013）
目标为全球，无特定目标
Winnti
（2009-2013）
目标为全球，以东南亚为焦点
HeartBeat（200911-201206）
safe行动（2012-）
无目标国家

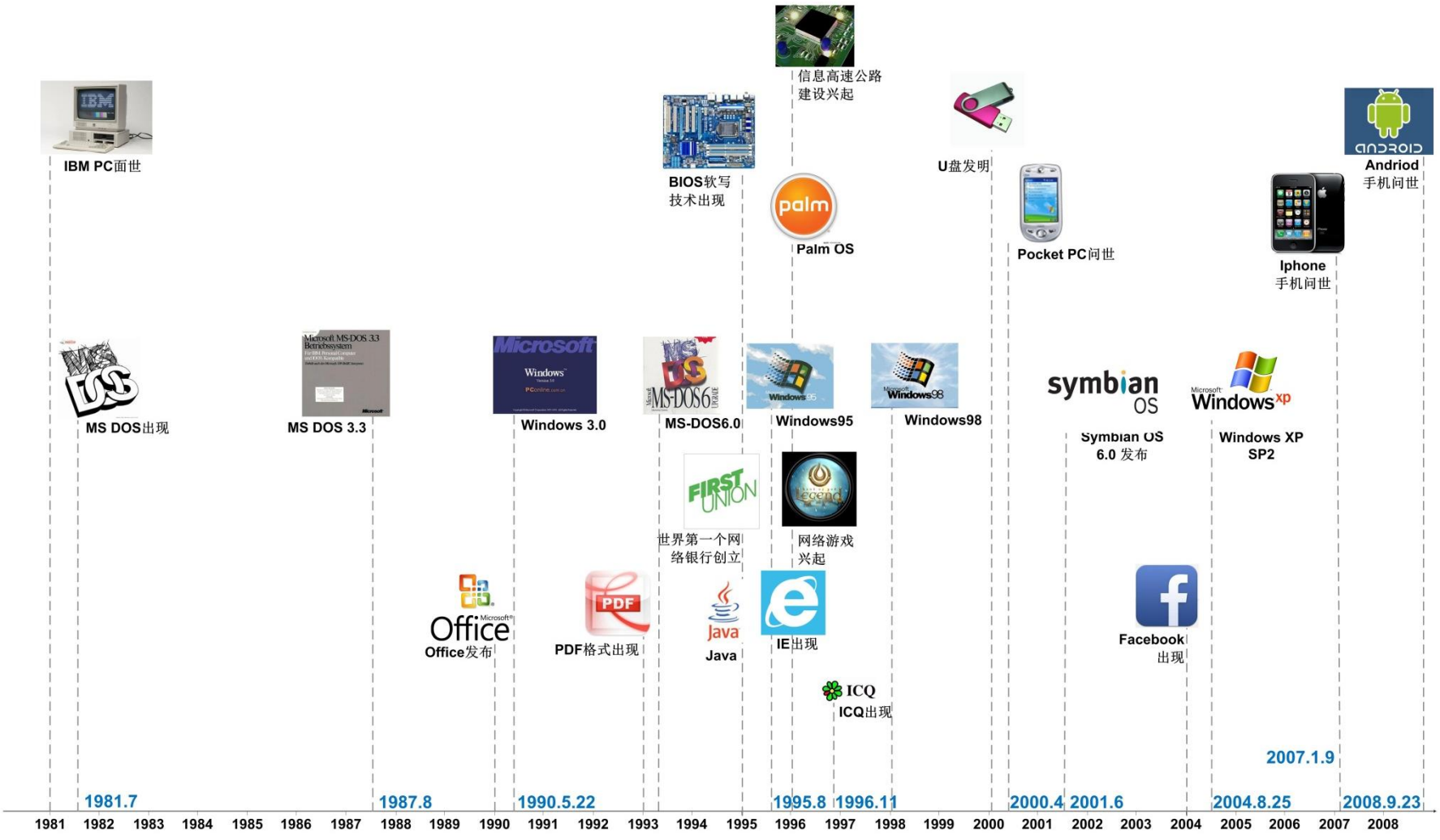
APT的关键词？



真的如此简单？

总结：重新审视差异化

假如我们换一个视图


IBM PC面世
1981.7
MS DOS出现
MS DOS 3.3
1987.8
Office发布
Office
Windows 3.0
1990.5.22
PDF格式出现
PDF
世界第一个网络银行创立
FIRST UNION
Java
IE出现
1995.8
信息高速公路建设兴起
BIOS软写技术出现
Palm OS
ICQ出现
ICQ
1996.11
U盘发明
Windows95
Windows98
Pocket PC问世
2000.4
网络游戏兴起
Symbian OS 6.0 发布
2001.6
Facebook出现
Windows XP SP2
2004.8.25
Iphone手机问世
2007.1.9
Andriod手机问世
2008.9.23
1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008

APT颠覆了那些普遍性的规律

追随观

恶意代码的进化与变化是围绕者产业和应用发展技术逐步展开的。

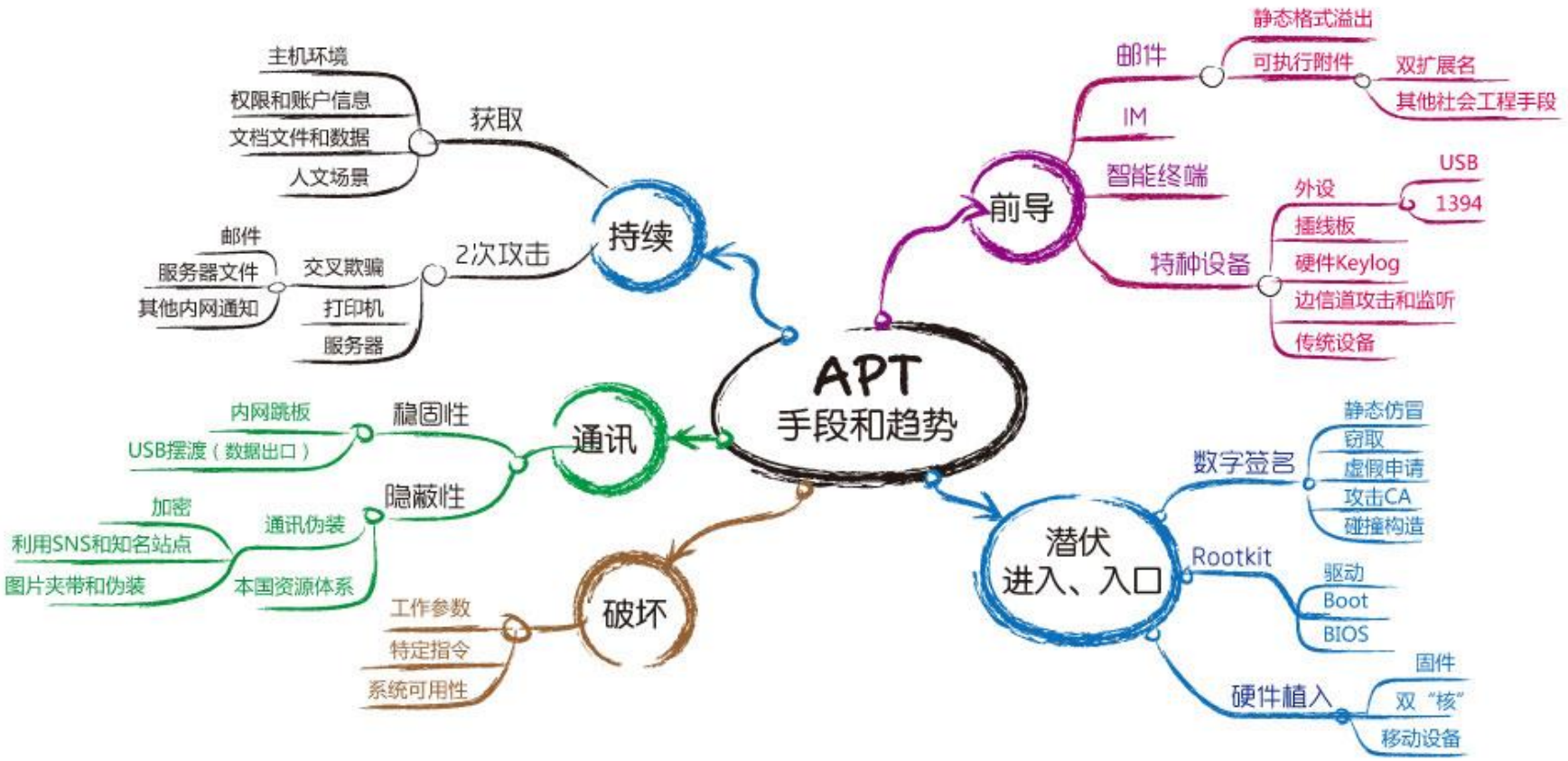
主流观

多数恶意代码围绕主流的操作系统展开，以获得更大的感染量。

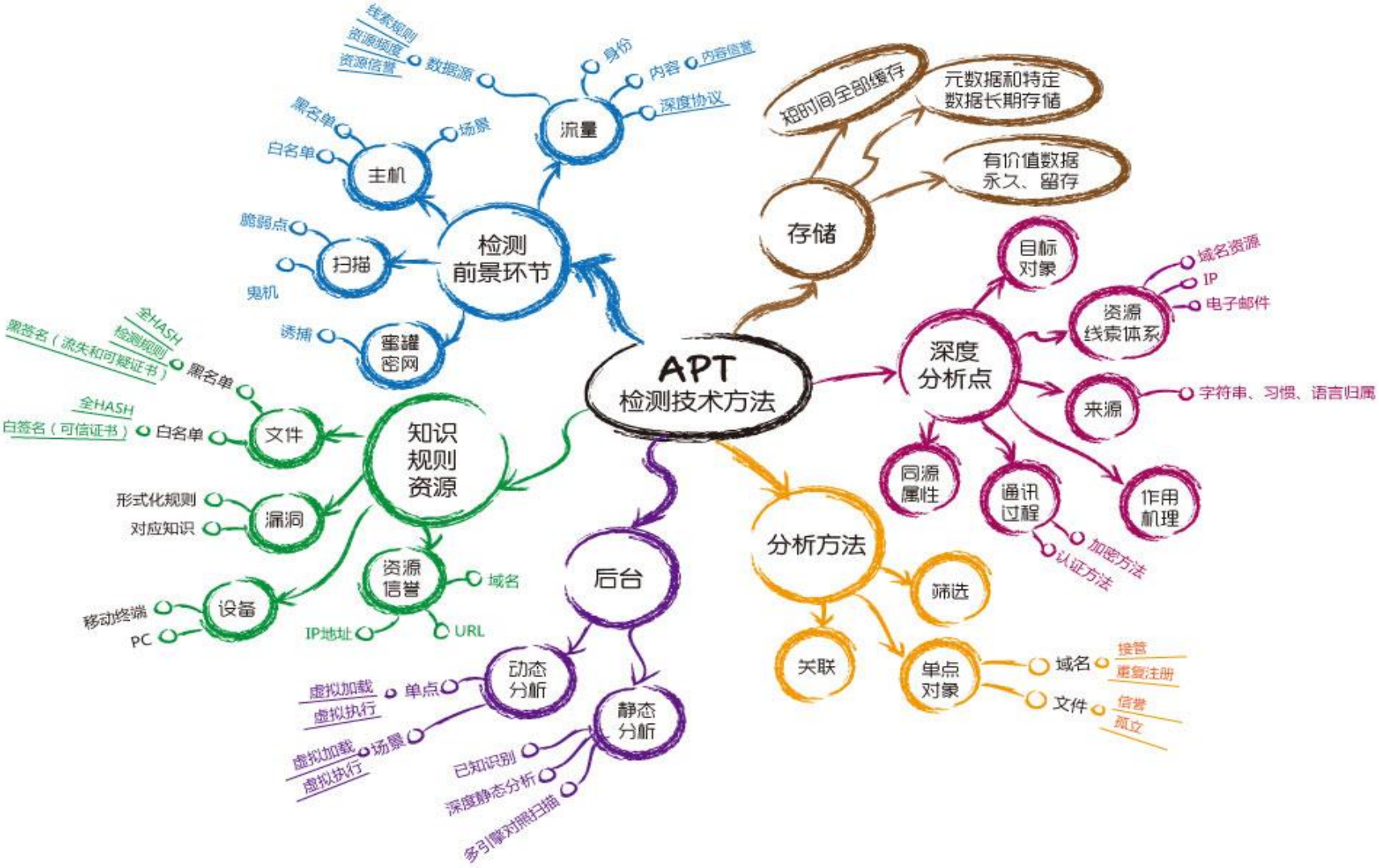
威胁观

通常攻击者者寻找更脆弱、获益更容易的方法实施安全威胁。

重新认识高级（一）


APT
手段和趋势
前导
邮件
静态格式溢出
可执行附件
双扩展名
其他社会工程手段
IM
智能终端
特种设备
外设
USB
1394
插线板
硬件Keylog
边信道攻击和监听
传统设备
持续
获取
主机环境
权限和账户信息
文档文件和数据
人文场景
2次攻击
交叉欺骗
邮件
服务器文件
其他内网通知
打印机
服务器
通讯
稳固性
内网跳板
USB摆渡（数据出口）
隐蔽性
通讯伪装
加密
利用SNS和知名站点
图片夹带和伪装
本国资源体系
破坏
工作参数
特定指令
系统可用性
潜伏
进入、入口
数字签名
静态仿冒
窃取
虚假申请
攻击CA
碰撞构造
Rootkit
驱动
Boot
BIOS
硬件植入
固件
双“核”
移动设备

重新认识高级（二）


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
黑名单
黑签名（流失和可疑证书）
全HASH
检测规则
文件
白名单
白签名（可信证书）
全HASH
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

重新认识高级（二）

APT的高级不是单点技术的高超、创造性和突破，甚至也未必精彩，其是既往方式的集大成者，其表现出的是组织、体系和支撑。

其高级反应的是积累、组织能力和成本的承担能力。

重新认识持续（一）

感染式病毒

Xorala

Sality

Virut

僵尸网络

Zeus

ZeroAccess

Zitmo

APT

Flame

Duqu

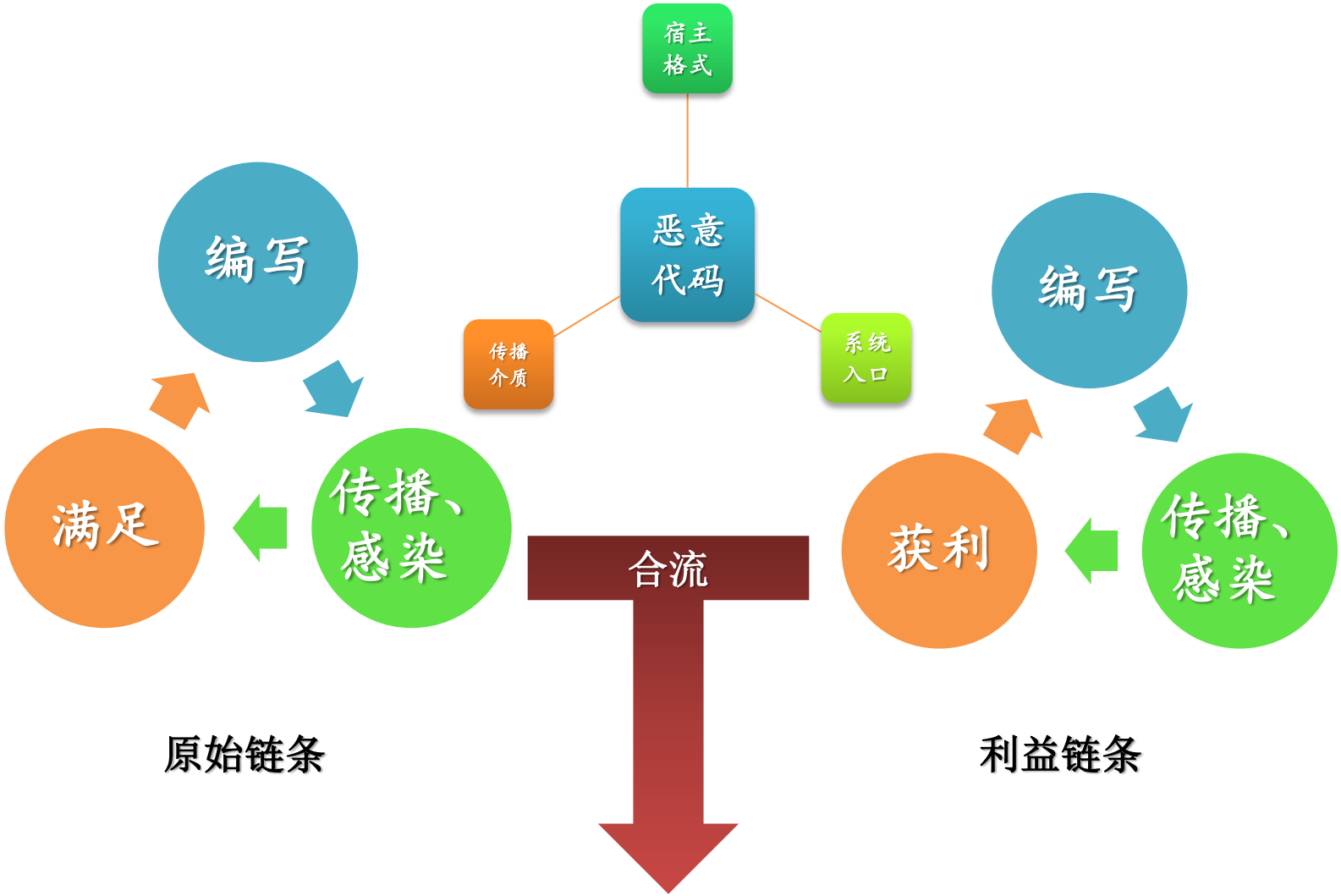
Stuxnet

重新认识持续（二）

APT的持续不是传统的恶意代码的“生命周期”，也不是僵尸网络的“体系规模存续”。

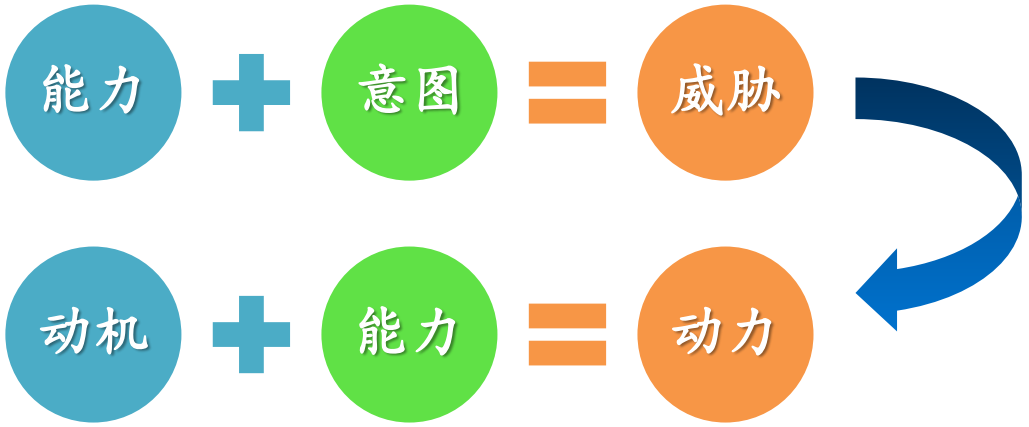
同时也不是简单的数据回送和指令下达的持续，其持续以资源和耐心为支撑，同时反映出攻击方明确的战略导向和意图。

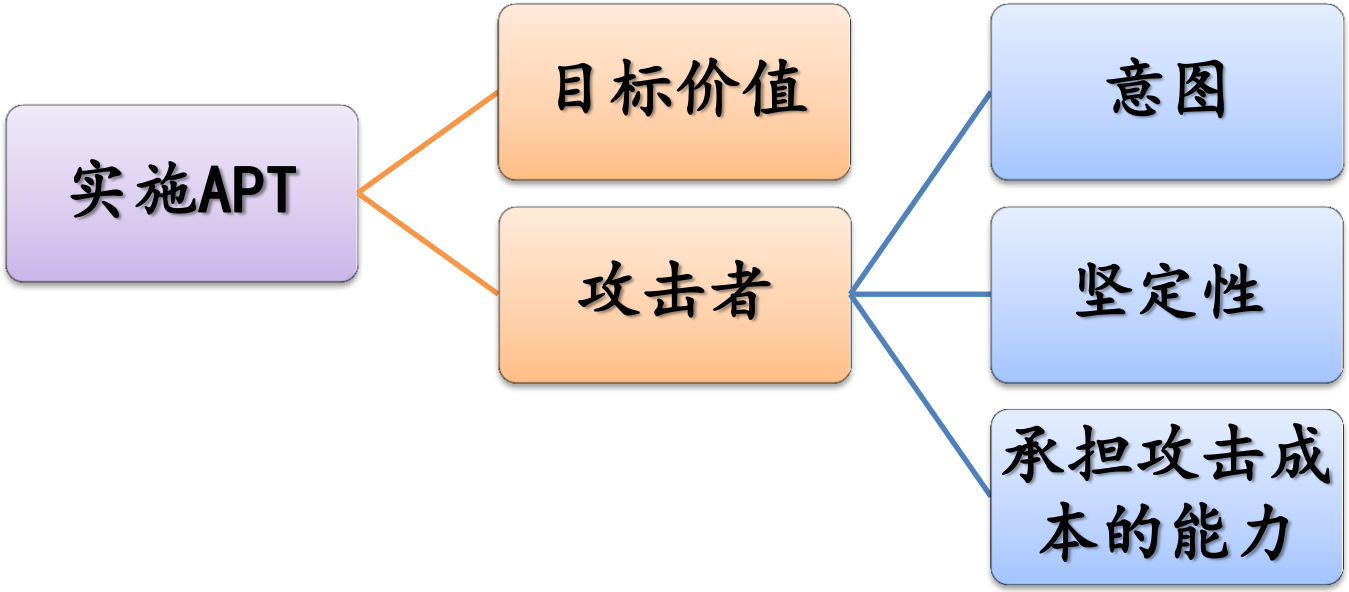
历史循环的动力性因素



APT的动力性因素变化

动力颠覆历史





折射：多余的话

话语权

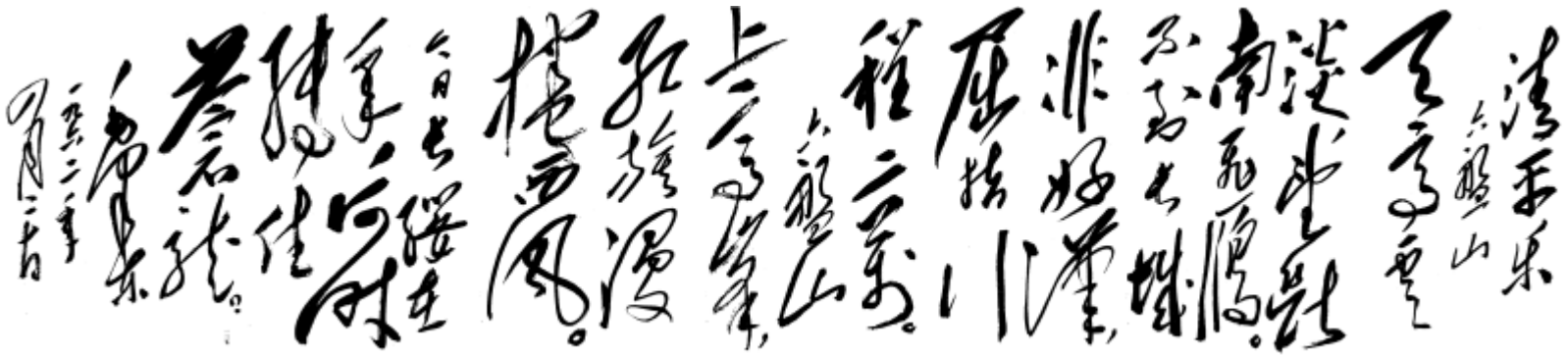
APT在技术上与之前恶意代码和其他攻击技术的发展史一脉相承，并与之前的定向攻击有一定延续性，其只是被单独定义成为新概念而已。

今天全球更多人相信APT的唯一目标是西方政府和机构，却忽略掉了其在Flame->Stuxnet中扮演的角色。

APT所投射出的是一种话语权，它包括：

- 定义
- 转义
- 形式化
- 标准
- 倾向性赋予

谢谢！



- 肖新光
- 安天实验室
- seak@antiy.com
- Weibo.com/seak