ANTIY 安天 | 创造安全每一天

XP停服后对安全威胁版图的影响

安天实验室

提纲

- 威胁动向解析
  - 系统漏洞定位导向
  - 浏览器和OFFICE版本封顶
  - 系统内置安全机制不再更新
- 微软安全演进对我们的启示
- 一点思考

威胁动向解析

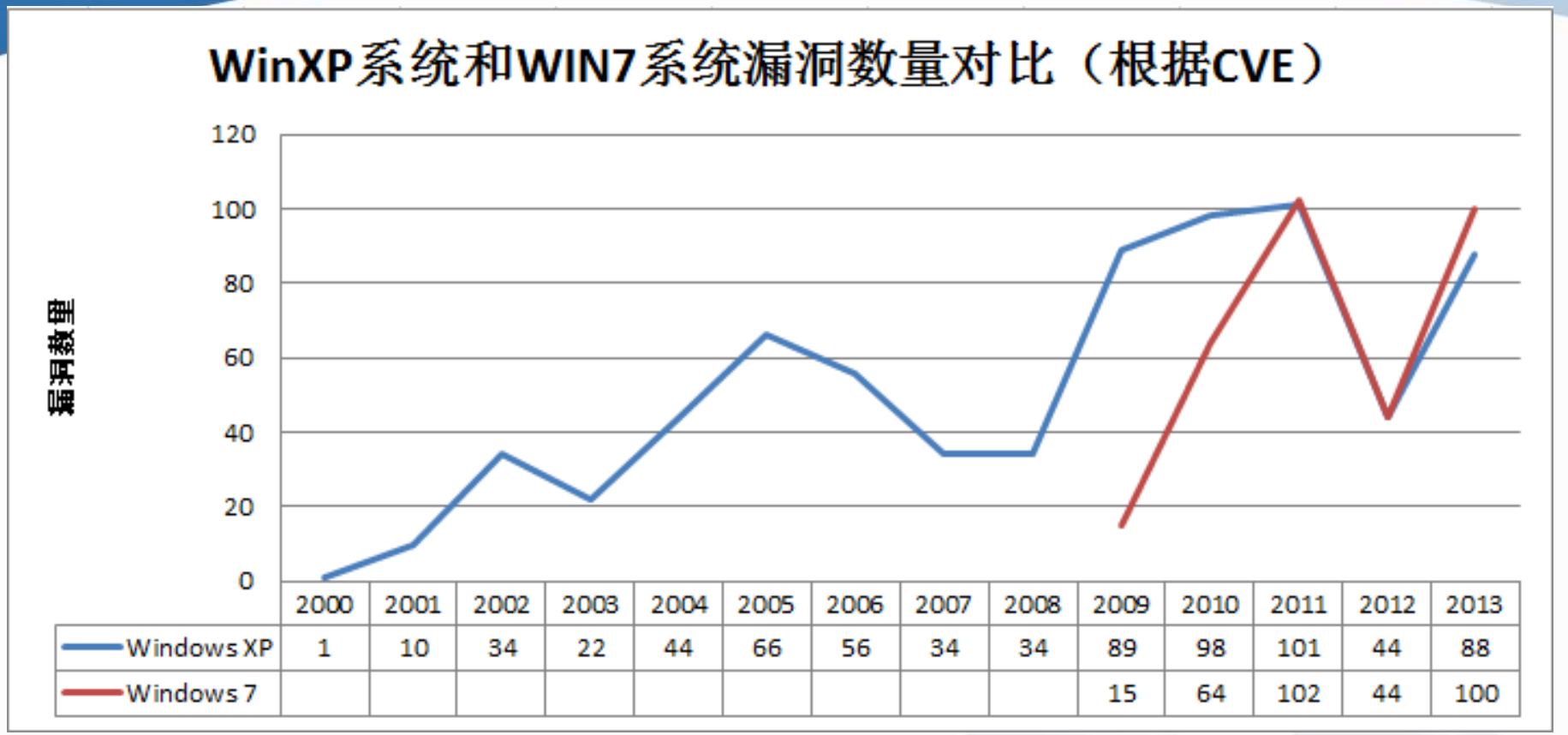
威胁分布

系统漏洞得不到官方修补

浏览器、office版本封顶

系统内置安全机制不再更新

XP与WIN7系统漏洞数量的情况



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Windows XP	1	10	34	22	44	66	56	34	34	89	98	101	44	88
Windows 7										15	64	102	44	100

The increase of vulnerabilities in Windows

Data reveals that the dip in the number of vulnerabilities recorded in Windows 7 and Windows XP in 2012 (50 and 49) has been reversed, with the number rising back up to 102 and 99 vulnerabilities respectively in 2013, almost on par with 2011 figures.

同一个漏洞可能影响多个操作系统

Vendor	Product
Microsoft	Windows Server 2003
Microsoft	Windows Server 2008
Microsoft	Windows Server 2012
Microsoft	Windows Vista
Microsoft	Windows Xp

– References For CVE-2014-0317

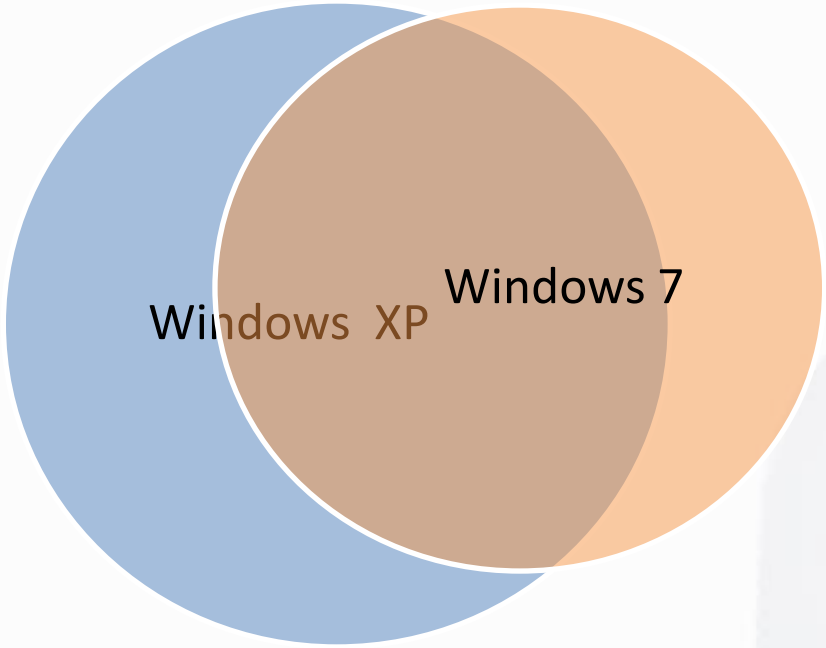
Vendor	Product
Microsoft	Windows 7
Microsoft	Windows 8
Microsoft	Windows 8.1
Microsoft	Windows Server 2003
Microsoft	Windows Server 2008
Microsoft	Windows Server 2012
Microsoft	Windows Vista
Microsoft	Windows Xp

– References For CVE-2014-0301

Vendor	Product
Microsoft	Windows 7
Microsoft	Windows 8
Microsoft	Windows 8.1
Microsoft	Windows Rt
Microsoft	Windows Rt 8.1
Microsoft	Windows Server 2003
Microsoft	Windows Server 2008
Microsoft	Windows Server 2012
Microsoft	Windows Vista
Microsoft	Windows Xp

– References For CVE-2014-0323

重叠漏洞分布情况



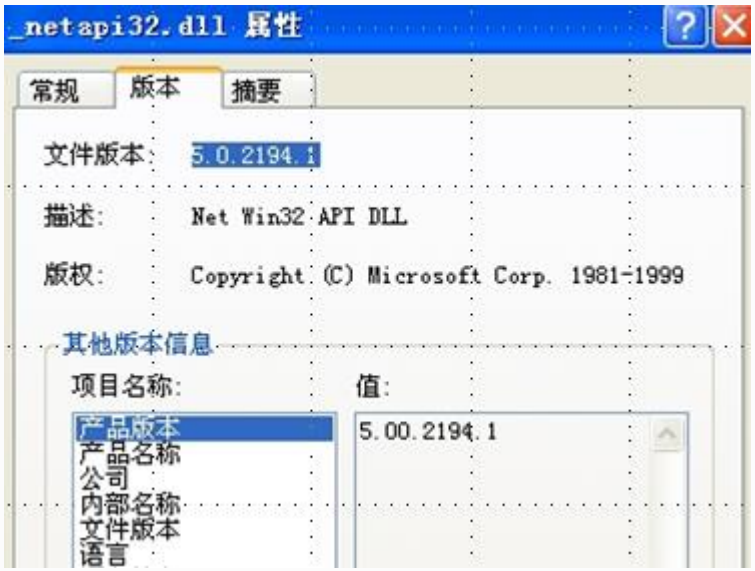
2009-2013
Windows XP 系统漏洞 422
Windows 7系统漏洞 331
其中重叠漏洞 257

漏洞重叠影响的原因-MS OS的演进

自WinXP开始的Windows桌面操作系统基本都是NT架构系统。

补丁比对是最常见漏洞定位的方法

- 以在XP系统根据补丁寻找MS08-067的溢出点为例
- Microsoft 安全公告 MS08-067 ((CVE-2008-4250)

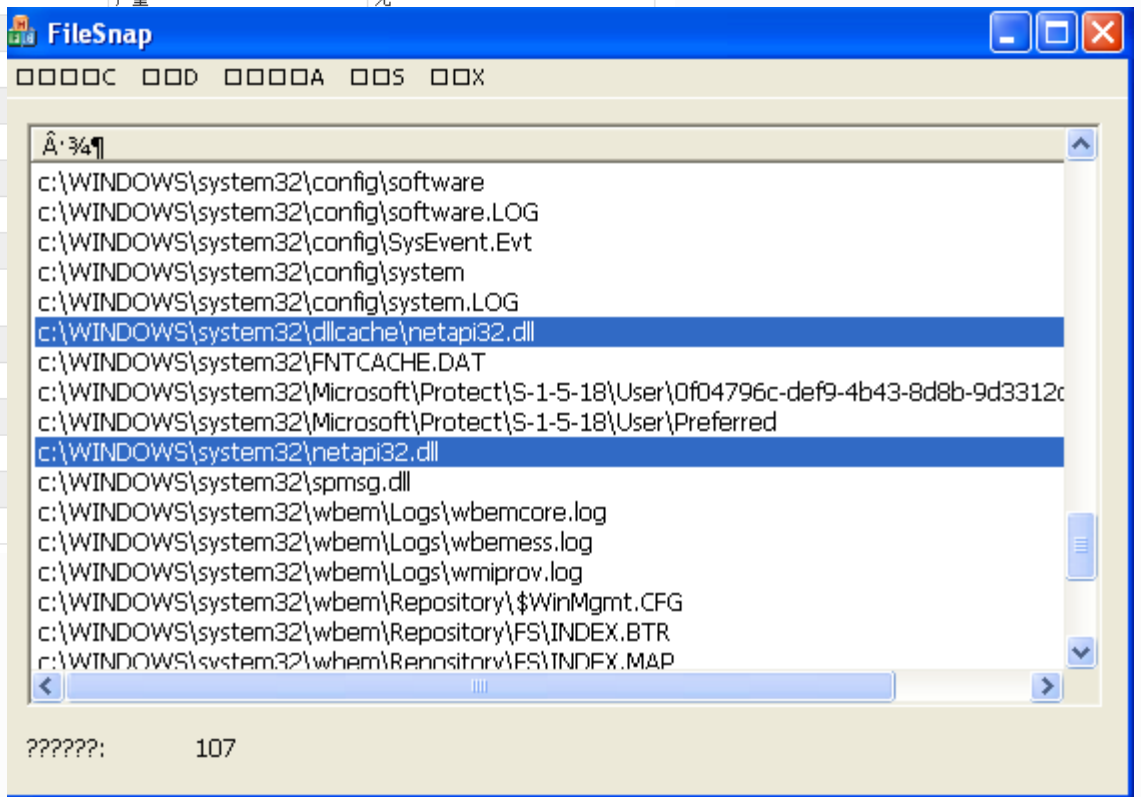


假定漏洞公告不再有XP

- Windows版本各DLL的延续继承关系是一种“已知”知识
- 只需要比对WIN7对应的文件，就可能发现相关问题。

受影响的软件

操作系统	最大安全影响	综合严重等级	此更新替代的公告
Microsoft Windows 2000 Service Pack 4	远程执行代码	严重	MS06-040
Windows XP Service Pack 2	程执行代码	严重	MS06-040
Windows XP Service Pack 3	远程执行代码	严重	无
Windows XP Professional x64 Edition	远程执行代码	严重	MS06-040
Windows XP Professional x64 Edition Service Pack 2	远程执行代码	严重	无
Windows Server 2003 Service Pack 1	远程执行代码		
Windows Server 2003 Service Pack 2	远程执行代码		
Windows Server 2003 x64 Edition	远程执行代码		
Windows Server 2003 x64 Edition Service Pack 2	远程执行代码		
Windows Server 2003 SP1（用于基于 Itanium 的系统）	远程执行代码		
Windows Server 2003 SP2（用于基于 Itanium 的系统）	远程执行代码		
Windows Vista 和 Windows Vista Service Pack 1	远程执行代码		
Windows Vista x64 Edition 和 Windows Vista x64 Edition Service Pack 1	远程执行代码		
Windows Server 2008（用于 32 位系统）*	远程执行代码		
Windows Server 2008（用于基于 x64 的系统）*	远程执行代码		
Windows Server 2008（用于基于 Itanium 的系统）	远程执行代码		
Windows 7 Beta（用于 32 位系统）	远程执行代码		
Windows 7 Beta x64 Edition	远程执行代码		
Windows 7 Beta（用于基于 Itanium 的系统）	远程执行代码		



定位Win7系统修改点

- 根据Wine对应的函数对比和逆向分析找到修改的函数

IDA View-A | Matched Functions | Unmatched Functions | Identical Functions

Engine	Function 1	Function 2
4	sub_5B86A3CE	sub_5B86A272
0	NetpManageIPCConnect(x,x,x,x)	NetpManageIPCConnect(x,x,x,x)
0	CanonicalizePathName(x,x,x,x,x)	CanonicalizePathName(x,x,x,x,x)
4	NetpIsRemote(x,x,x,x)	NetpIsRemote(x,x,x,x,x)
0	I_NetServerSetServiceBits(x,x,x,x)	I_NetServerSetServiceBits(x,x,x,x)

```
      return 0;
    _wcscpy(v4, v5 + 2);
    if ( !v8 )
      return 1;
    v15 = v4;
    v5 = v4;
    for ( j = (int)(v4 - 1); *(_WORD *)j != 92 && j != a1; j -= 2 )
      ;
    v2 = a1;
    v4 = (wchar_t *)(*(_WORD *)j == 92 ? j : 0);
  }
  goto LABEL_6;
}
if ( v7 != 92 )
  break;
if ( v3 )
{
  v14 = v3;
}
else
{
  v6 = (int)(v5 + 2);
  v14 = v5;
}
_wcscpy(v14, (const wchar_t *)v6);
v2 = a1;
LABEL_7:
v1 = *v5;
if ( !*v5 )
  return 1;
```

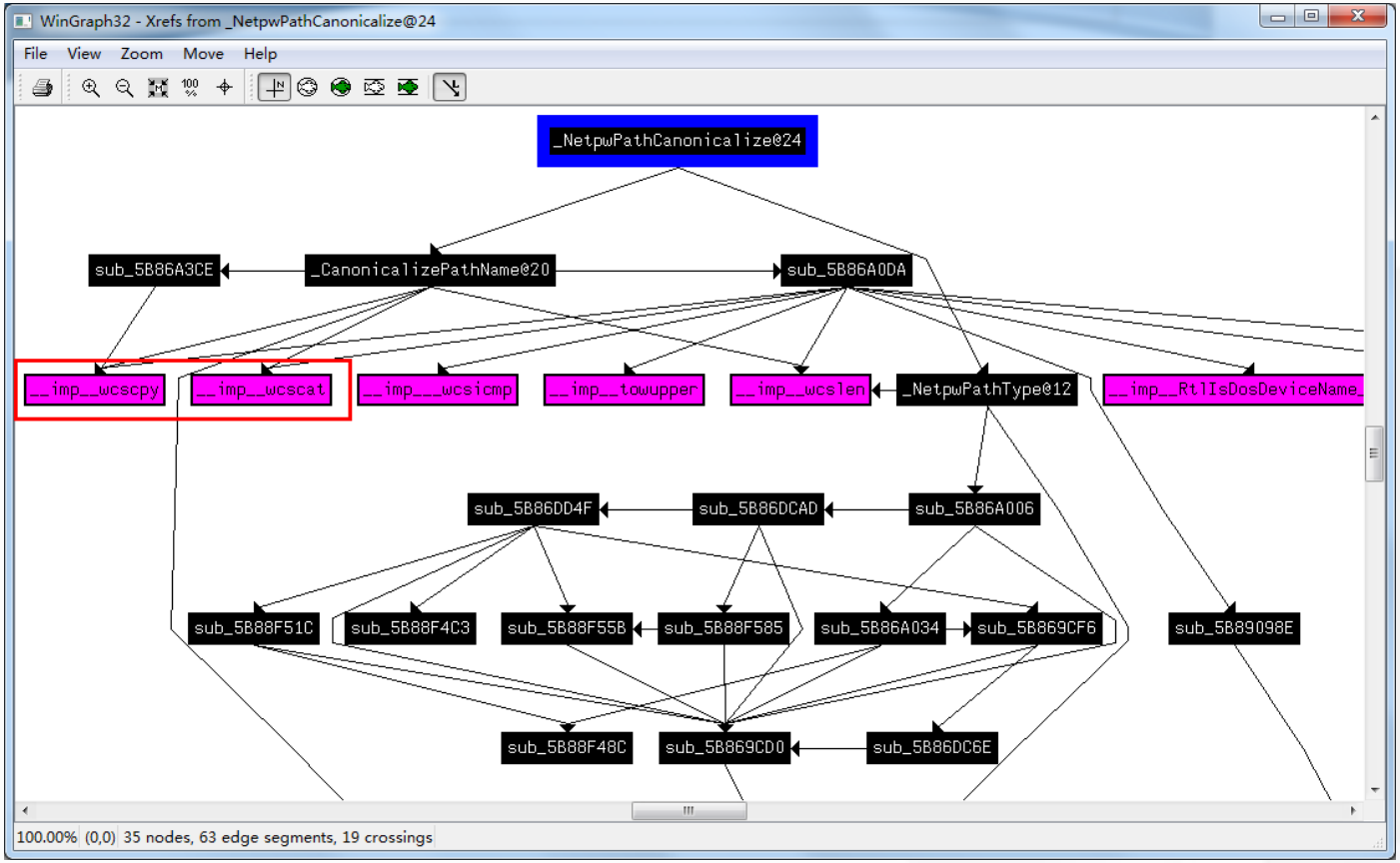
sub_5B86A3CE:65

```
    StringCchCopyW(v6, (signed int)((char *)v15 - (char *)v6) >> 1, (STRSAFE_LPCWSTR)j + 2);
    if ( !v14 )
      return 1;
    v16 = v6;
    j = v6;
    if ( v2 == v6 )
      return 0;
    for ( k = (int)(v6 - 1); *(_WORD *)k != 92 && (const wchar_t *)k != v2; k -= 2 )
      ;
    v6 = (wchar_t *)(*(_WORD *)k == 92 ? k : 0);
  }
  goto LABEL_12;
}
if ( v4 != 92 )
{
  if ( !v4 )
  {
    if ( v16 )
      j = v16;
    *(_WORD *)j = 0;
    return 1;
  }
  goto LABEL_12;
}
v13 = v16;
if ( !v16 )
{
  v3 = (int)((char *)j + 4);
  v13 = (wchar_t *)j;
}
if ( v13 >= v15 )
  return 0;
StringCchCopyW(v13, (signed int)((char *)v15 - (char *)v13) >> 1, (STRSAFE_LPCWSTR)v3);
LABEL_49:
```

sub_5B86A272:74

定位漏洞产生的具体位置

- 通过IDA交叉索引可以定位调用关系，经过一些分析后可以找到漏洞产生位置——wcscpy()函数。



验证XP系统是否存在同样漏洞

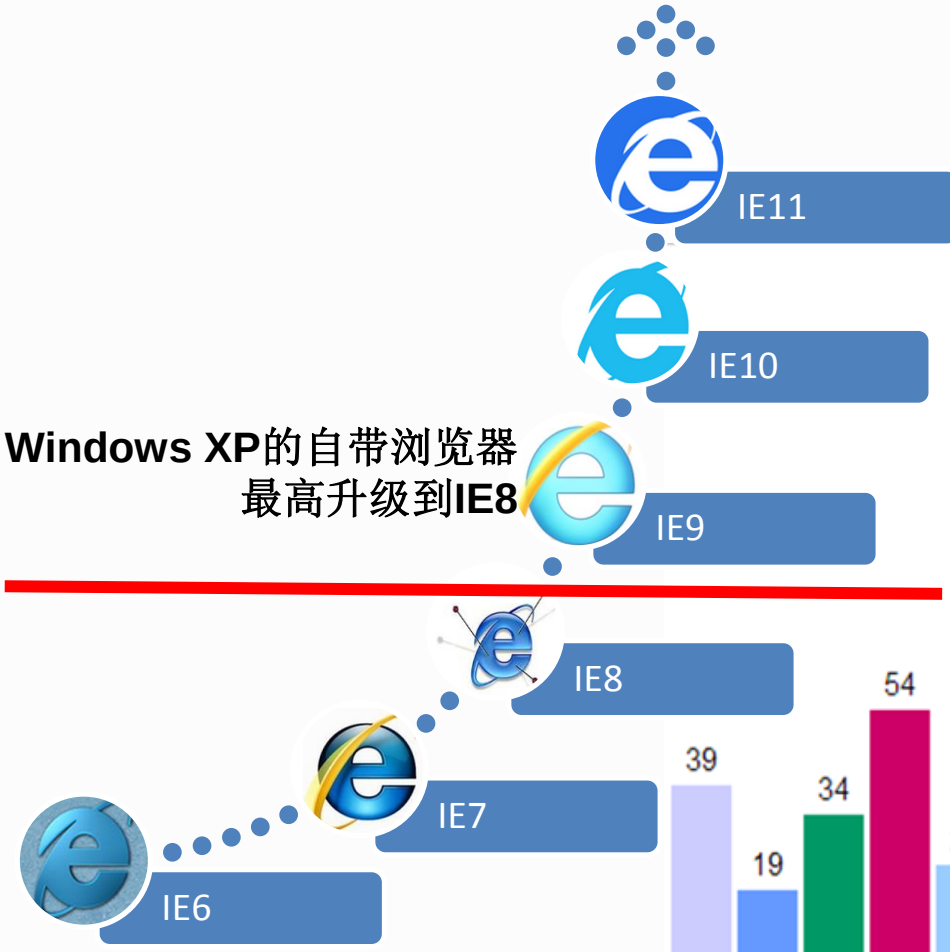
- 找到了关键文件、并定位了溢出函数，就可以重复以上过程去验证目标系统是否存在相同漏洞。

IDA View-A | Pseudocode-A | Matched Functions | Unmatched Functions | Identical Func

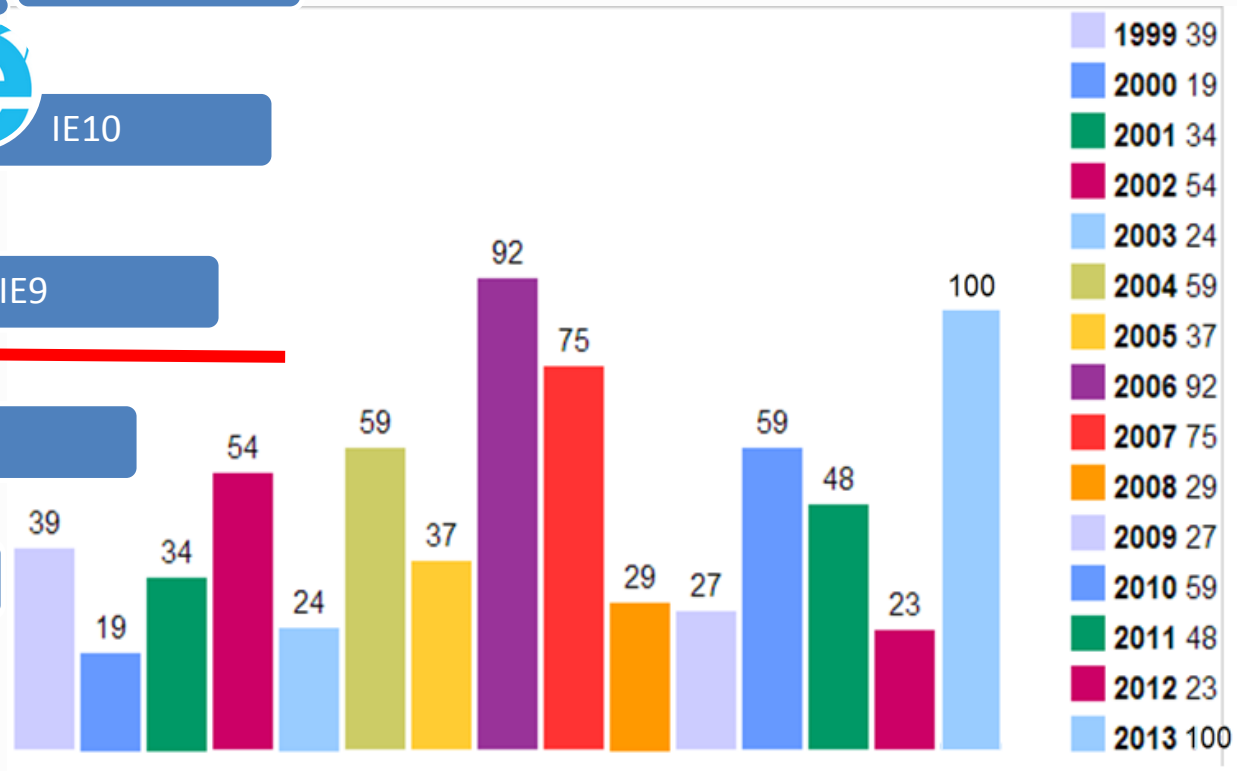
Engine	Function 1	Function 2
0	NetpDcGetName(x,x,x,x,x,x,x,x,x,x,x,x,x,x,x)	NetpDcGetName(x,x,x,x,x,x,x,x,x,x,x,x,x,x,x)
0	NetDfsAddFtRoot(x,x,x,x,x)	NetDfsAddFtRoot(x,x,x,x,x)
4	sub_5B86A51B	sub_5B86A272
0	NetDfsRemoveFtRoot(x,x,x,x)	NetDfsRemoveFtRoot(x,x,x,x)
0	NetDfsRemoveFtRootForced(x,x,x,x,x)	NetDfsRemoveFtRootForced(x,x,x,x,x)
0	CredpValidateUserName(x,x,x)	CredpValidateUserName(x,x,x)
0	ReadDSObjSecDesc(x,x,x,x,x)	ReadDSObjSecDesc(x,x,x,x,x)
0	DfsGetObjSecurity(x,x,x)	DfsGetObjSecurity(x,x,x)

```
      return 0;
    _wcscpy(v4, v5 + 2);
    if ( !v8 )
      return 1;
    v15 = v4;
    v5 = v4;
    for ( j = (int)(v4 - 1); *(_WORD *)j != 92 && j != a1; j -= 2 )
      ;
    v2 = a1;
    v4 = (wchar_t *)(*(_WORD *)j == 92 ? j : 0);
  }
  goto LABEL_6;
}
if ( v7 != 92 )
  break;
if ( v3 )
{
  v14 = v3;
}
else
{
  v6 = (int)(v5 + 2);
  v14 = v5;
}
_wcscpy(v14, (const wchar_t *)v6);
v2 = a1;
sub_5B86A51B:71
```

IE8和更低版本浏览器将吸引更多火力



Windows XP的自带浏览器
最高升级到IE8



cvedetails网站提供的IE漏洞数量统计

IE8 0day漏洞(举例)

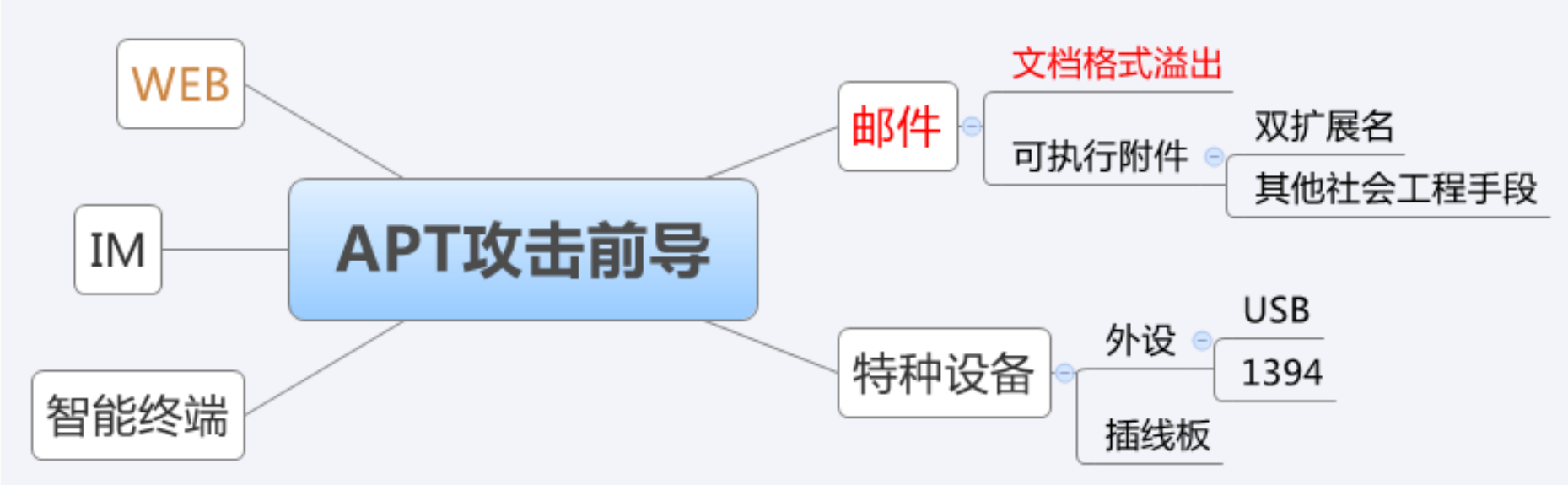
- 2013年5月微软IE8零day漏洞（CVE-2013-1347）
  - 去年该漏洞影响IE8浏览器，无论是个人电脑还是企业网络用户，均有可能因此遭到黑客攻击。据最新的报告显示，IE8在国内的浏览器市场上占有13.93%的份额，按照这个比例测算，约有7000余万用户将受其影响。另近一年来越来越多的APT攻击使用“**水坑式攻击**”，5月初，美国劳工部官方网站和美国能源局SEM (Site Exposure Matrices)相继遭黑客攻击，且均是利用此IE8漏洞

OFFICE版本封顶

Windows XP的最高支持到 Office 2010

虽然微软还会继续支持之前的Office补丁版本更新，但Office2013未来内建的安全能力不会同步给更早的版本

office 格式溢出在APT攻击中占据重要位置



APT 攻击前导大部分为WEB和邮件。

利用office漏洞进行攻击的APT

无法获得新的安全机制的更新

- DEP(数据执行保护,Data Execution Prevention）技术MicrosoftWindowsXPServicePack2(SP2)开始引进
- ASLR(地址空间布局随机化)则是在三年前Vista发布时首次与大家见面是一种针对缓冲区溢出的安全保护技术，通过对栈、共享库映射等线性区布局的随机化防止攻击者定位攻击代码位置
- UAC(User Account Control，用户帐户控制)是微软为提高系统安全而在Windows Vista中引入的新技术
- Win7系统承接以上三种安全保护机制，并根据安全机制对用户的诟病进行修改，例如win7可以对 UAC进行级别设置。
- **而XP系统仅仅包含DEP机制，且不共享新技术保护机制，在包括XP系统停止官方补丁的供应，版本的浏览器的支持，安全机制的匮乏让们对整个XP系统防线的脆弱性感到担忧**

各个版本的主要安全机制更改

	XP	XP SP2	Vista	Win7	win8
ASLR		支持	增强	增强	重大提升
DEP		支持	增强	增强	重大提升
SDL		支持	完整	完整版	完整版
Firewall		支持	升级	升级	升级
Bitlocker			支持全部磁盘加密	支持全部磁盘加密	支持可选磁盘空间加密
UAC			只有开/关	4个档位可调节	4个档位可调节
AppLocker				支持	支持
UEFI (Secure Boot)					支持

带来的后果

定向攻击的成功率增加

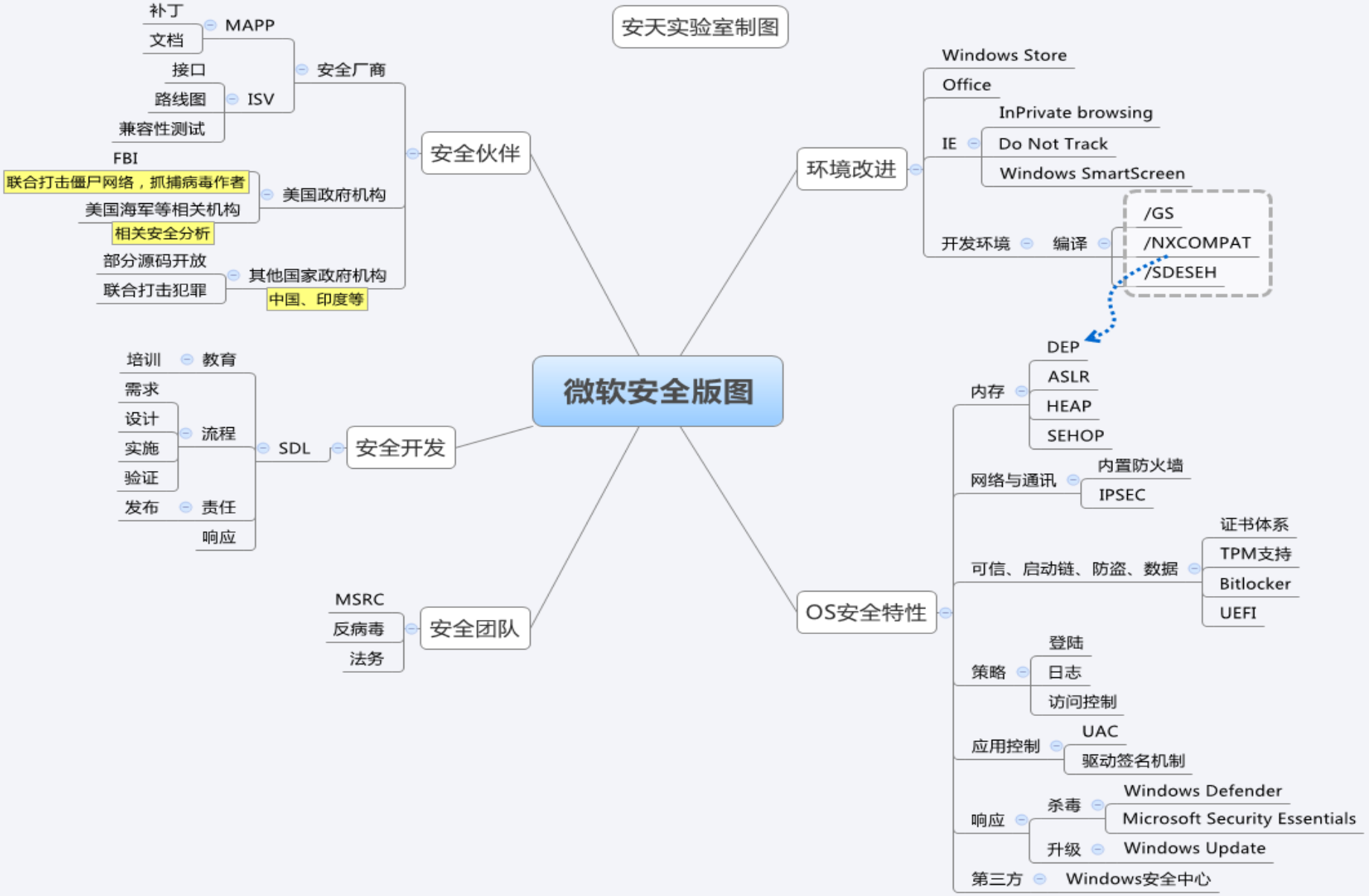
- 利用更多的得不到官方修正的现有漏洞进行攻击，毕竟利用现有漏洞比0day漏洞更加容易
- 攻击者可以利用office漏洞进行伪装释放恶意文件
- XP系统的UAC机制能力能力不强可以导致APT容易提权获取系统资料和横向移动

僵尸网络、挂马可能增加

- 僵尸网络利用漏洞进行肆虐传播
- 针对主机的脆弱性进行组建僵尸网络，利用肉鸡进行下载恶意文件、窃取信息等操作
- 利用的浏览器漏洞使跨站脚本(XSS)等常见漏洞都进行挂马

微软安全演进对我们的启示

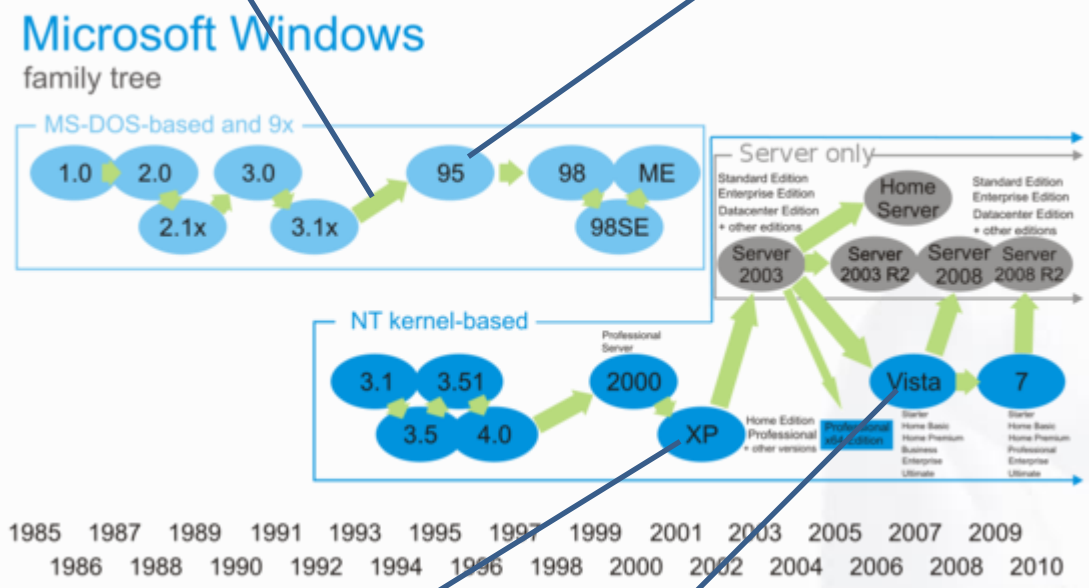
微软安全版图


安天实验室制图
微软安全版图
安全伙伴
补丁
MAPP
文档
安全厂商
接口
路线图
ISV
兼容性测试
FBI
联合打击僵尸网络，抓捕病毒作者
美国政府机构
美国海军等相关机构
相关安全分析
部分源码开放
联合打击犯罪
其他国家政府机构
中国、印度等
安全开发
培训
教育
需求
设计
实施
验证
流程
SDL
发布
责任
响应
安全团队
MSRC
反病毒
法务
环境改进
Windows Store
Office
InPrivate browsing
IE
Do Not Track
Windows SmartScreen
开发环境
编译
/GS
/NXCOMPAT
/SDESEH
DEP
ASLR
HEAP
SEHOP
内存
网络与通讯
内置防火墙
IPSEC
证书体系
TPM支持
Bitlocker
UEFI
可信、启动链、防盗、数据
登陆
日志
访问控制
策略
UAC
驱动签名机制
应用控制
Windows Defender
杀毒
Microsoft Security Essentials
响应
升级
Windows Update
第三方
Windows安全中心
OS安全特性

一些历史尝试

Vsafe
MSAV

OOB等攻击
驱动补丁机制



XP SP2
安全的新探索

Vista
安全应用平衡
尝试

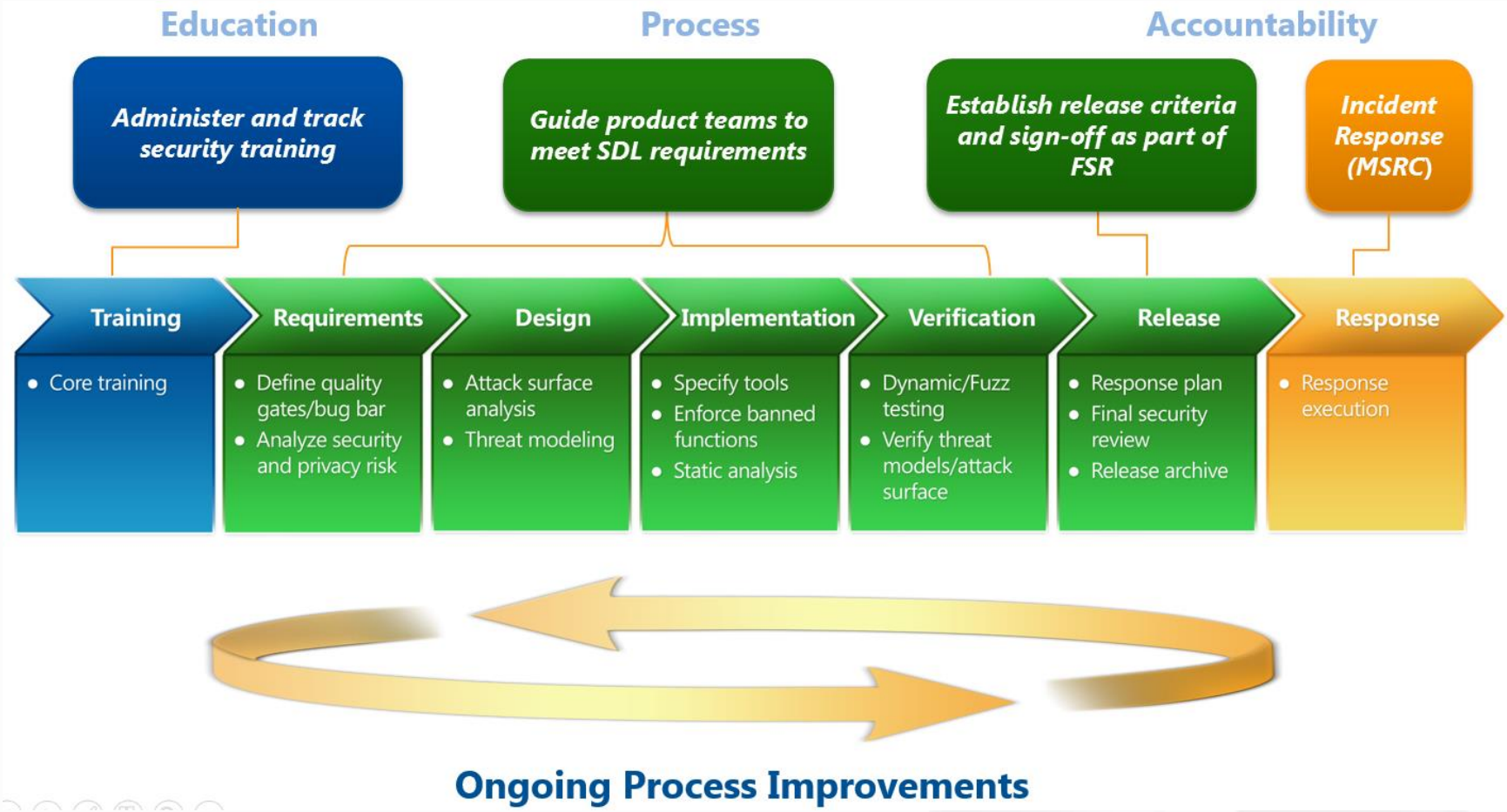
操作系统安全特性的演进

1995	2001	2004	2007	2009	2012
Windows 95 • -	**Windows XP** • Logon (Ctrl+Alt+Del) • Access Control • User Profiles • Security Policy • Encrypting File System (File Based) • Smartcard and PKI Support • Windows Update	**Windows XP SP2** • Address Space Layout Randomization (ASLR) • Data Execution Prevention (DEP) • Security Development Lifecycle (SDL) • Auto Update on by Default • Firewall on by Default • Windows Security Center • WPA Support	**Windows Vista** • Bitlocker • Patchguard • Improved ASLR and DEP • Full SDL • User Account Control • Internet Explorer Smart Screen Filter • Digital Right Management • Firewall improvements • Signed Device Driver Requirements • TPM Support • Windows Integrity Levels • Secure "by default" configuration (Windows features and IE)	**Windows 7** • Improved ASLR and DEP • Full SDL • Improved IPSec stack • Managed Service Accounts • Improved User Account Control • Enhanced Auditing • Internet Explorer Smart Screen Filter • AppLocker • BitLocker to Go • Windows Biometric Service • Windows Action Center • Windows Defender	**Windows 8** • UEFI (Secure Boot) • Firmware Based TPM • Trusted Boot (w/ELAM) • Measured Boot and Remote Attestation Support • Significant Improvements to ASLR and DEP • AppContainer • Windows Store • Internet Explorer 10 (Plugin-less and Enhanced Protected Modes) • Application Reputation moved into Core OS • BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support • Virtual Smartcard • Picture Password, PIN • Dynamic Access Control • Built-in Anti-Virus

安全开发过程的引入

- 微软SDL(Security Development Lifecycle)流程，是一种专注于软件开发安全保障的流程，为了实现保证最终的用户安全，在软件开发各阶段中引入安全和隐私保护。

SDL生命周期


Education
Process
Accountability
Administer and track security training
Guide product teams to meet SDL requirements
Establish release criteria and sign-off as part of FSR
Incident Response (MSRC)
Training
Core training
Requirements
Define quality gates/bug bar
Analyze security and privacy risk
Design
Attack surface analysis
Threat modeling
Implementation
Specify tools
Enforce banned functions
Static analysis
Verification
Dynamic/Fuzz testing
Verify threat models/attack surface
Release
Response plan
Final security review
Release archive
Response
Response execution
Ongoing Process Improvements

微软的响应几个时间层次

微软

首先微软获取漏洞

1

美国海军等机构

重要机构接到消息

2

MAPP

合作伙伴升级安全防护系统

3

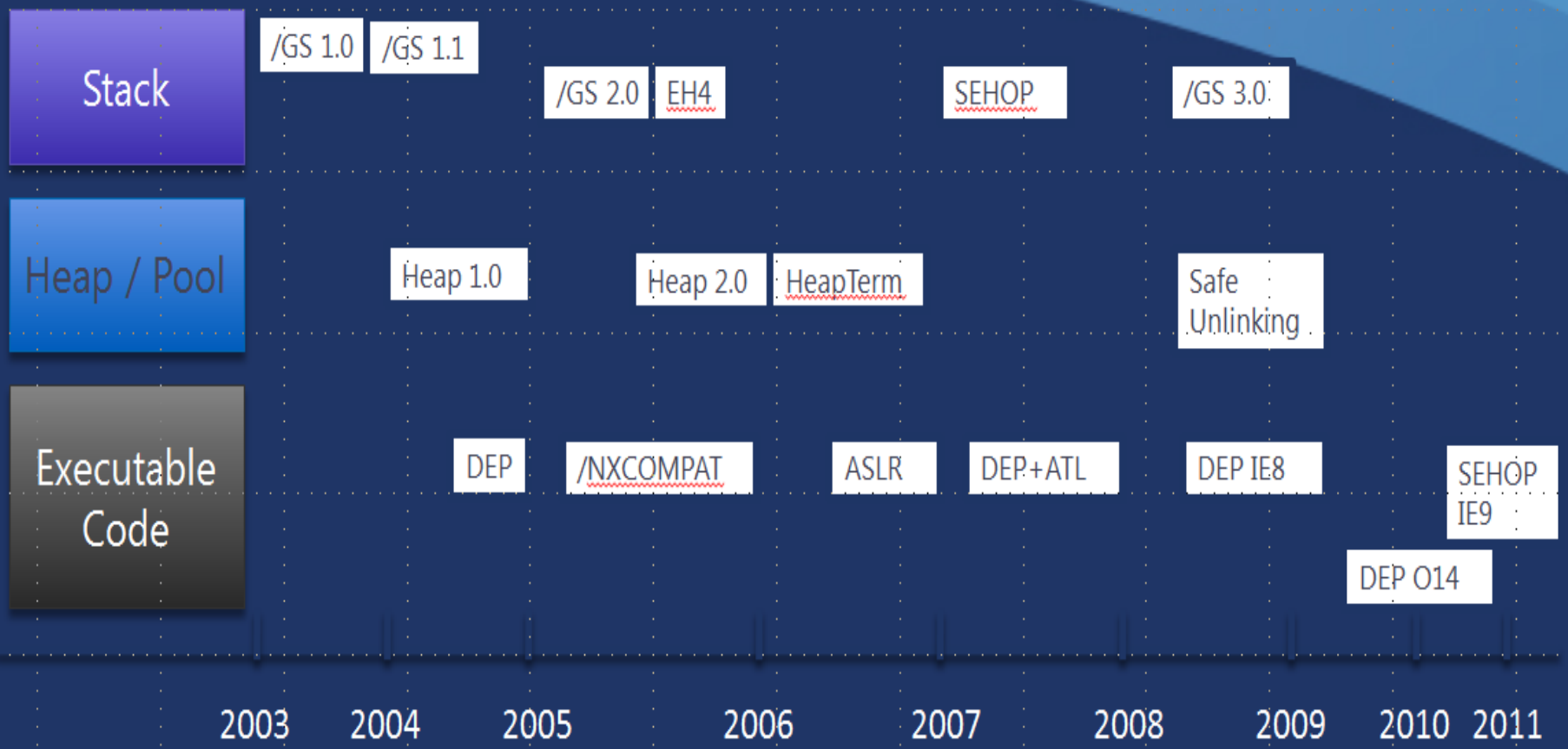
对外发布

公布补丁

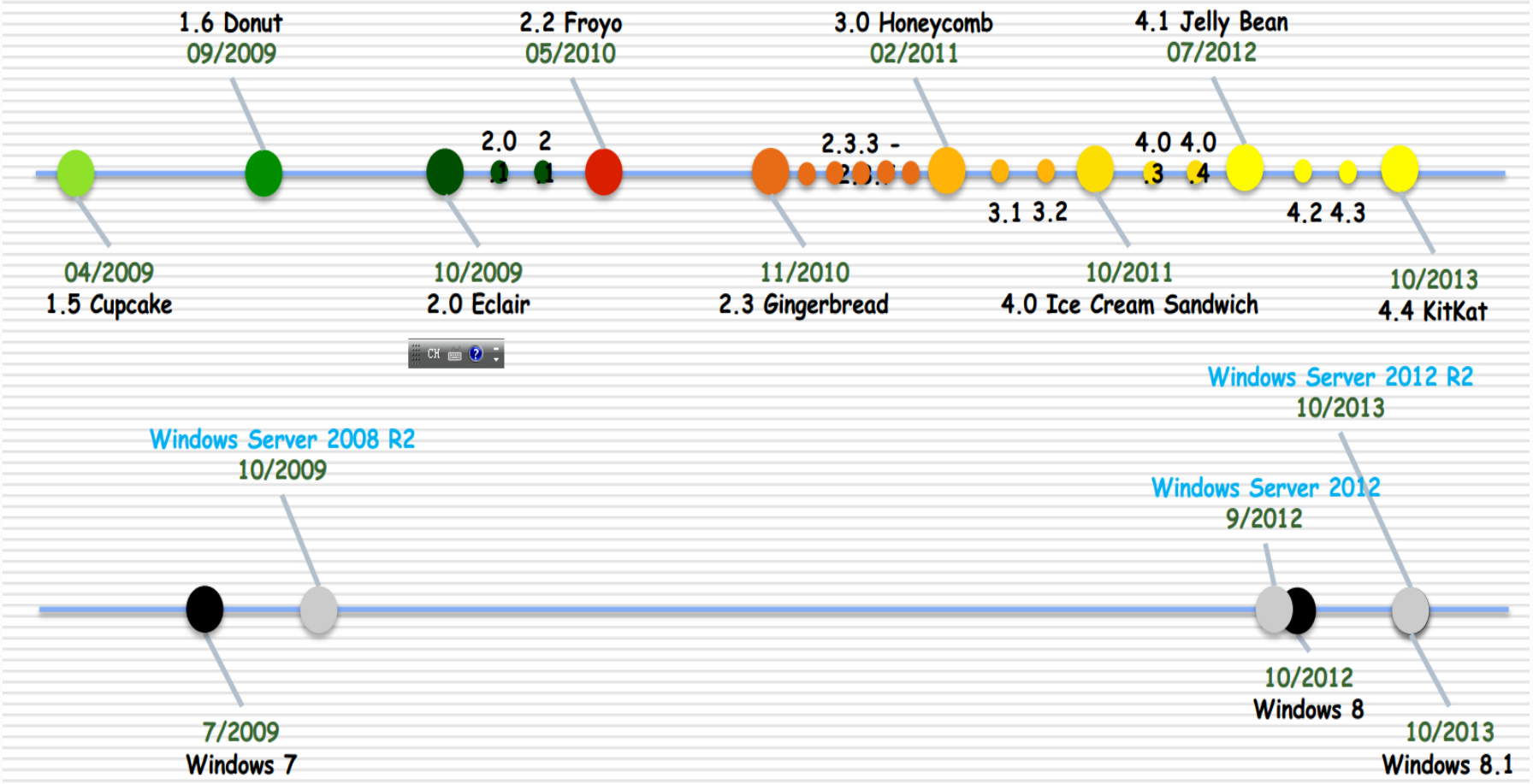
4

微软的应急体制

内存安全的演进之路


Stack
Heap / Pool
Executable Code
/GS 1.0
/GS 1.1
/GS 2.0
EH4
SEHOP
/GS 3.0
Heap 1.0
Heap 2.0
HeapTerm
Safe Unlinking
DEP
/NXCOMPAT
ASLR
DEP+ATL
DEP IE8
SEHOP IE9
DEP O14
2003
2004
2005
2006
2007
2008
2009
2010
2011

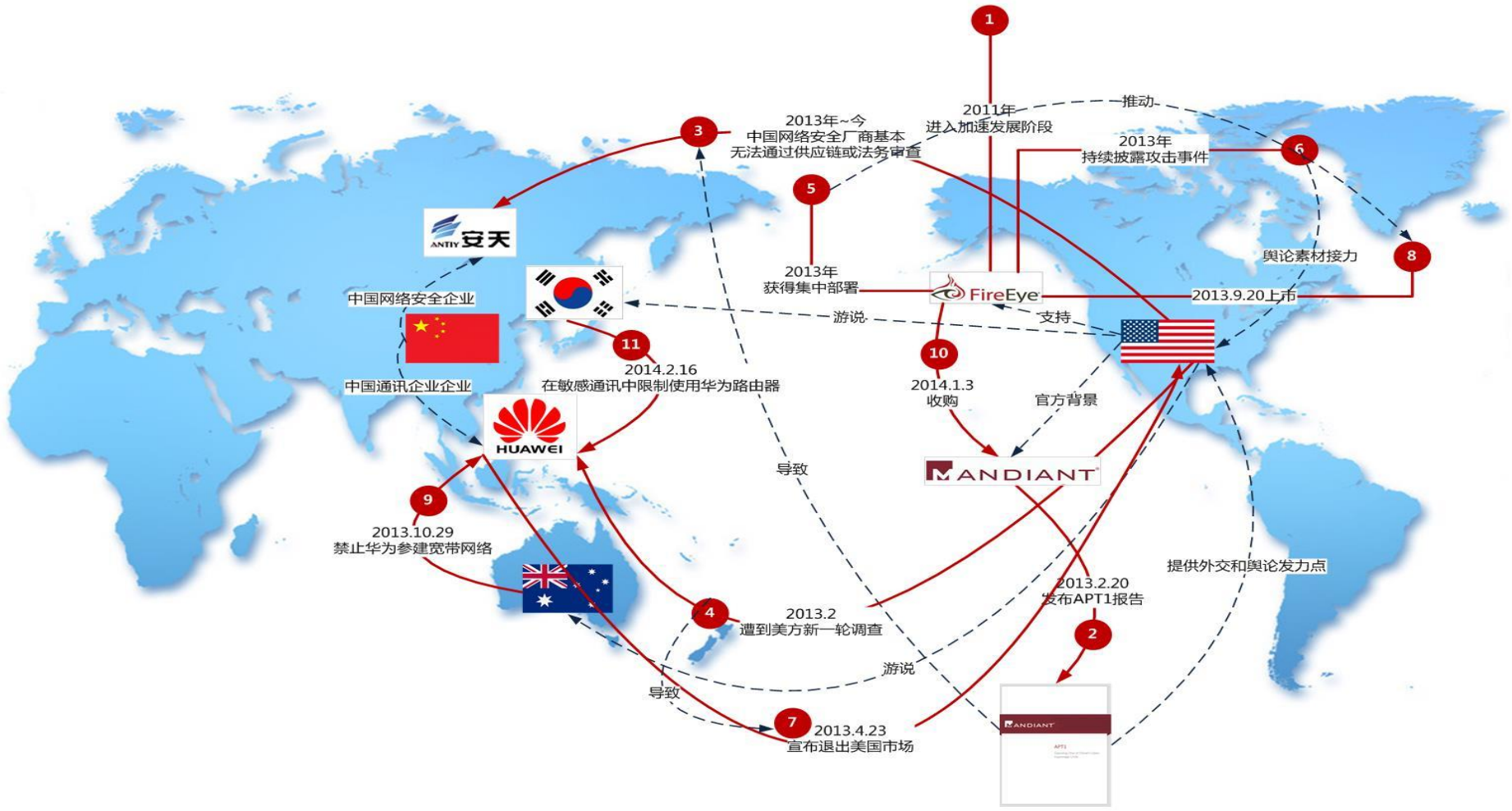
非碎片化优势


1.6 Donut
09/2009
2.2 Froyo
05/2010
3.0 Honeycomb
02/2011
4.1 Jelly Bean
07/2012
2.0 2
2.3.3 -
4.0 4.0
.3 .4
3.1 3.2
4.2 4.3
04/2009
1.5 Cupcake
10/2009
2.0 Eclair
11/2010
2.3 Gingerbread
10/2011
4.0 Ice Cream Sandwich
10/2013
4.4 KitKat
Windows Server 2012 R2
10/2013
Windows Server 2008 R2
10/2009
Windows Server 2012
9/2012
7/2009
Windows 7
10/2012
Windows 8
10/2013
Windows 8.1

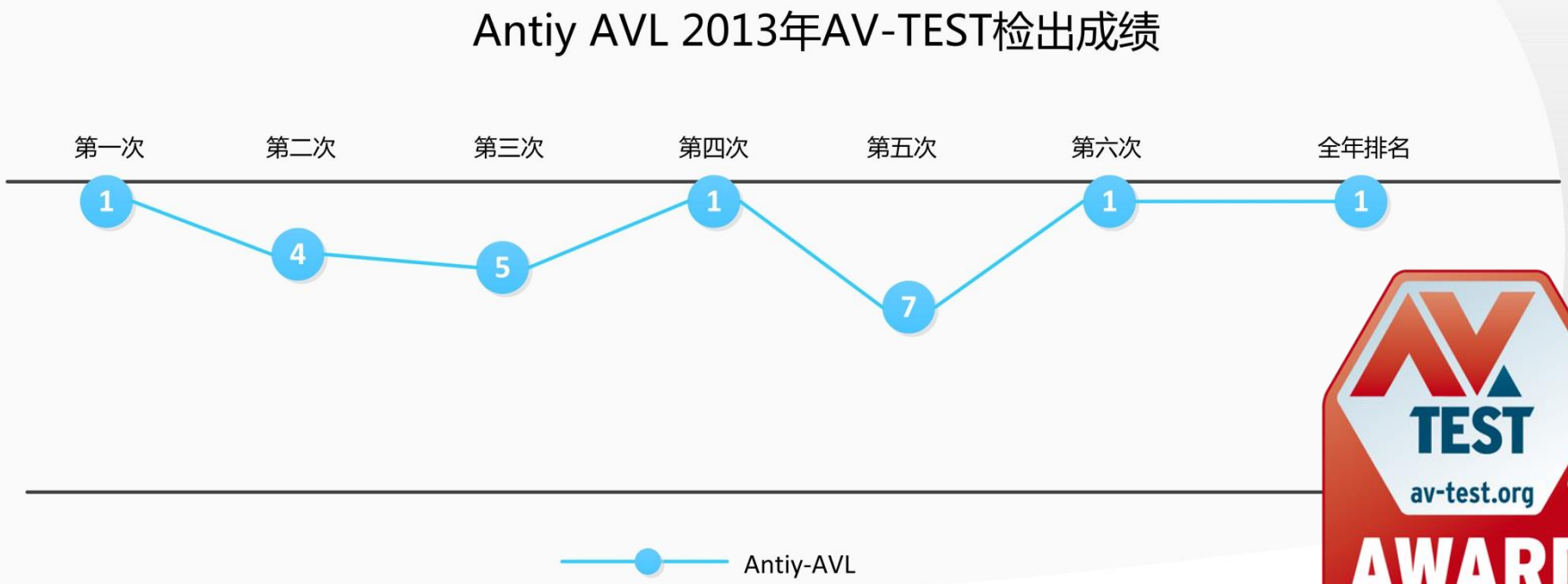
几点思考

- 老话重提-盗版的秘密
- 微软本身进入一个停滞期遭遇国内的自主可控的压力正碰
- 我们信息化是否进入局部停滞期->回顾当年拖住Vista的工作

中国自主安全厂商应该优先卡位



安全发力速度更快，可以为基础信息化争取更长的时间



感谢各位专家和朋友们

- 肖新光
- http://www.antiy.com
- seak@antiy.com
- Weibo.com/seak