安全开发与缓解工具帮助防御网络犯罪

薛锋
资深安全技术经理
微软公司可信赖计算部

Microsoft | 可信赖计算

内容

- 威胁形势
- 微软安全开发生命周期 (SDL)
- 安全缓解工具
- 蓝帽子大奖(BlueHat Prize)
- 行动呼吁
- 资源

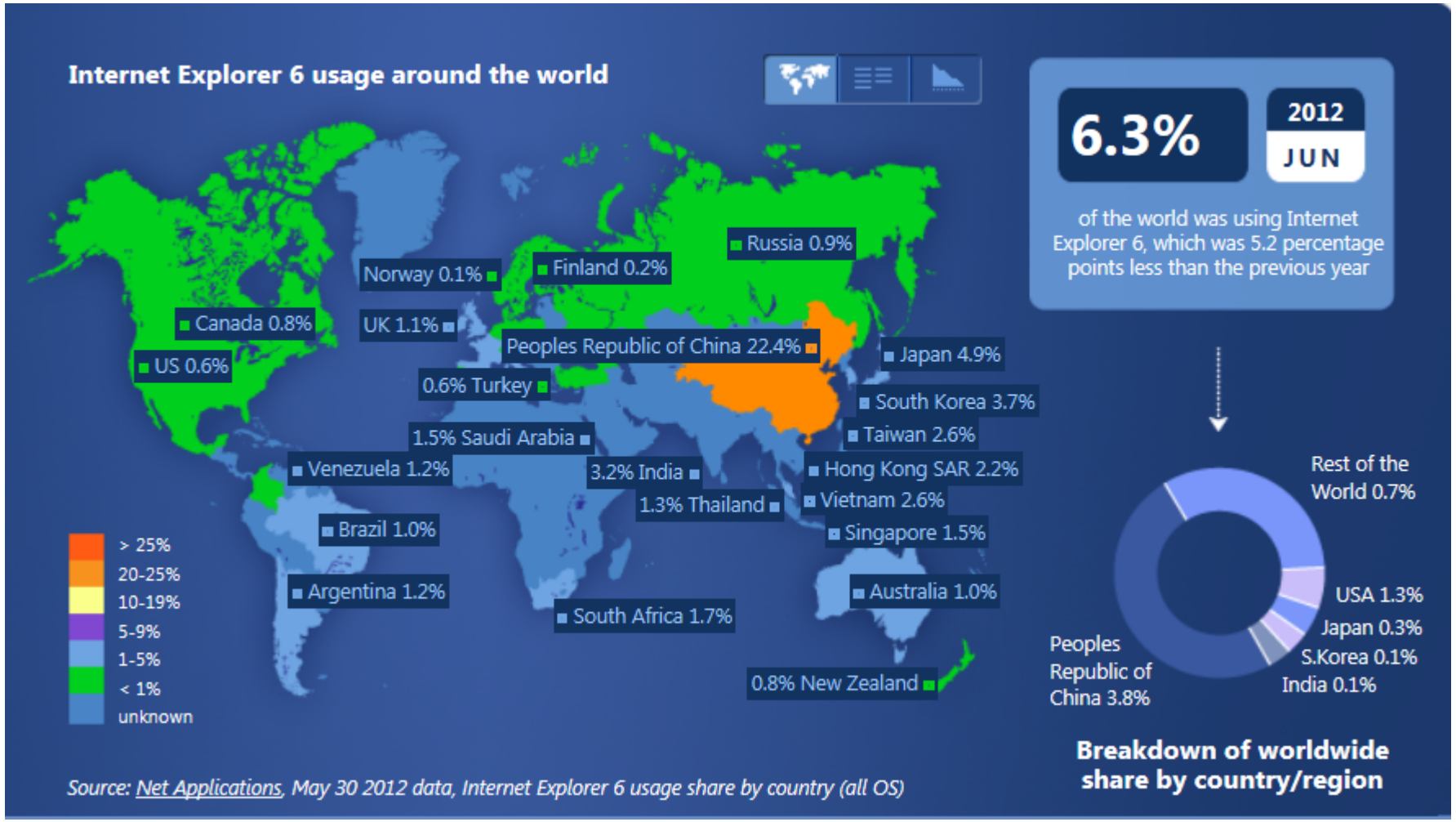
中国互联网统计数据

- 到 2011 年底， 中国有 5.13 亿互联网用户
- 目前中国的互联网普及率为 31.6%
- 中国 41% 的互联网用户年龄在 30 岁以上
- 中国人平均每周的上网时间为 19.8 小时
- 中国有 3.64 亿人使用宽带

CNNIC
中国互联网络信息中心
China Internet Network Information Center

Internet World Stats
Usage and Population Statistics

Internet Explorer 6 在中国的使用情况



安全威胁

微软安全报告

Windows Live Hotmail

bing

Windows Internet Explorer

Microsoft Security Essentials

Windows 恶意软件删除工具

Windows Defender

Microsoft Forefront

Windows安全扫描程序

包括的数据

- 来自 100 多个国家/地区的 6 亿多个系统的威胁信息
- 超过 2.8 亿个活动 Hotmail 帐户带有数十亿封已扫描的邮件
- Microsoft Security Essentials – 有 30 多种语言版本，广泛用于全球
- 恶意软件删除工具在 2011 年上半年内的下载/运行次数超过 47 亿次
- Bing 每天扫描数十亿个页面
- 规范指南帮助针对犯罪活动提供保护

中国的威胁形势

全球一半以上的 Internet Explorer 6 用户分布在中国

中国 有约四分之一的互联网用户使用 Internet Explorer 6

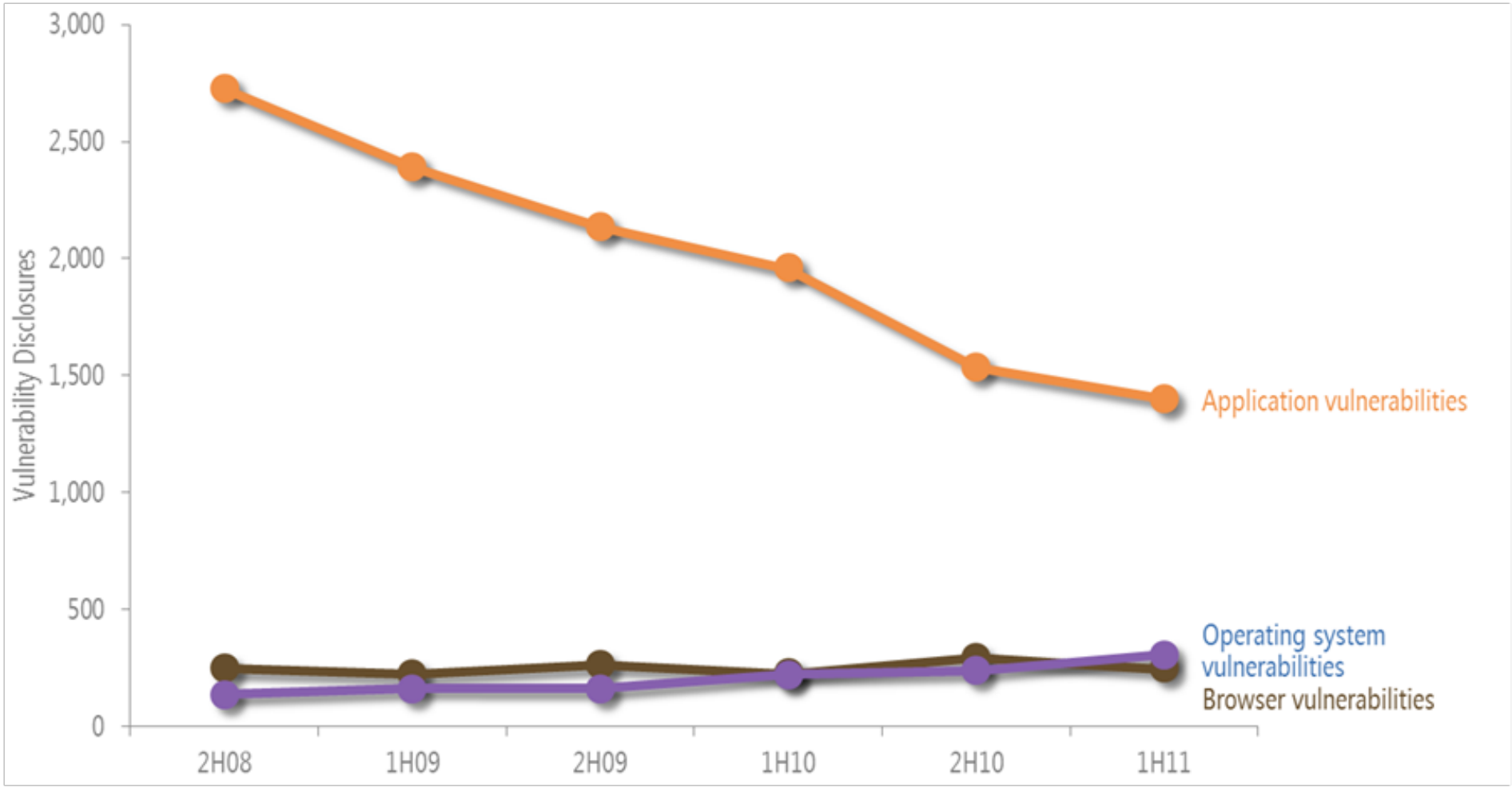
大多数 IE6 用户使用 Windows XP

Windows XP 遭受恶意软件感染的概率是 Windows 7 的 6 倍

2011 年第二季度，我们清理了中国约二百万个系统的恶意软件

国家/地区	2011 年第一季度	2011 年第二季度
美国	10,727,964	10,471,335
巴西	3,463,973	3,724,844
法国	2,351,941	2,674,775
英国	2,175,201	2,089,883
中国	2,017,682	1,883,578
德国	1,622,081	1,530,551
俄罗斯	1,296,208	1,583,857
意大利	1,358,166	1,509,148
加拿大	1,377,173	1,353,164
土耳其	1,248,978	1,359,181

漏洞


3,000
2,500
2,000
1,500
1,000
500
0
Vulnerability Disclosures
2H08
1H09
2H09
1H10
2H10
1H11
Application vulnerabilities
Operating system vulnerabilities
Browser vulnerabilities

微软安全开发生命周期 (SDL)

安全开发生命周期 - SDL

From: Bill Gates

Sent: Tuesday, January 15, 2002 2:22 PM

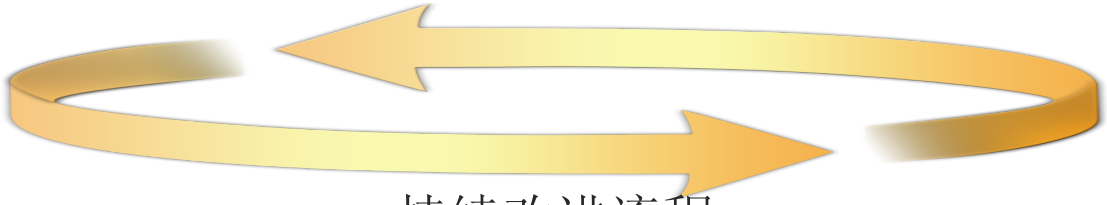
Subject: Trustworthy Computing

...Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing…Every week there are reports of newly discovered security problems in all kinds of software, from individual applications and services to Windows, Linux, Unix and other platforms. We have done a great job of having teams work around the clock to deliver security fixes for any problems that arise. Our responsiveness has been unmatched – but as an industry leader we can and must do better.

安全开发生命周期(SDL)

执行承诺→自 2004 年起，SDL在微软是必须执行的策略

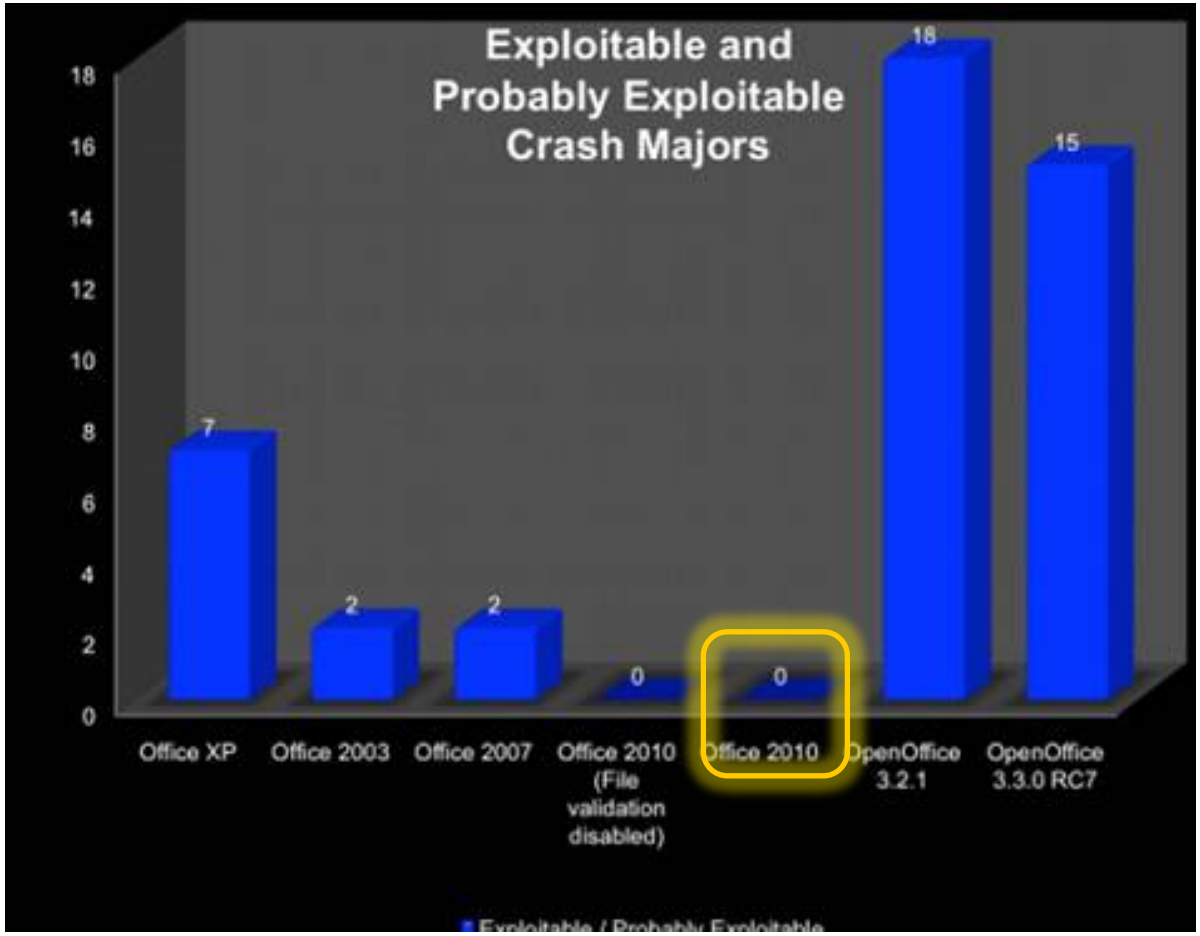
教育　　流程　　责任要求



持续改进流程

微软SDL可减少漏洞利用bug

Office 文件格式漏洞



微软SDL简化实施指南

从利用经济学的视点看问题

攻击者回报 = (每次使用所得利益 X 使用机会) - (获取漏洞的成本 + 实施攻击成本)

可靠的缓解技术

	XP RTM SP1	XP SP2	XP SP3	Vista RTM	Vista SP1	Vista SP2	Win7 RTM
SEH							
SafeSEH	N	Y	Y	Y	Y	Y	Y
SEHOP	N	N	N	N	OptIn	OptIn	OptIn
SEHOP per-process OptIn support	N	N	N	N	N	N	Y
Heap							
Safe unlinking	N	Y	Y	Y	Y	Y	Y
Block header cookies	N	Y	Y	Y	Y	Y	Y
Lookaside/freelist removal	N	N	N	Y	Y	Y	Y
Metadata encryption	N	N	N	Y	Y	Y	Y
Terminate on corruption (32-bit app)	N	N	N	Opt In	Opt In	Opt In	Opt In
Terminate on corruption (64-bit app)	N	N	N	Opt Out	Opt Out	Opt Out	Opt Out
DEP							
NX support (i386)	N	OptIn	OptIn	OptIn	OptIn	OptIn	OptIn
NX support (amd64, 32-bit app)	N	OptIn	OptIn	OptIn	OptIn	OptIn	OptIn
NX support (amd64, 64-bit app)	N	AlwaysOn	AlwaysOn	AlwaysOn	AlwaysOn	AlwaysOn	AlwaysOn
ASLR							
Randomization support							
Images	N	N	N	OptIn	OptIn	OptIn	OptIn
Stacks	N	N	N	OptIn	OptIn	OptIn	OptIn
Heaps	N	N	N	Y	Y	Y	Y
PEBs/TEBs	N	Y	Y	Y	Y	Y	Y
Entropy (bits)							
Images	0	0	0	8	8	8	8
Stacks	0	0	0	14	14	14	14
Heaps	0	0	0	5	5	5	5
PEBs/TEBs	0	4	4	4	4	4	4
APIs							
SetProcessDEPPolicy support	N	N	Y	N	Y	Y	Y

缓解措施

信息的不对称性

加入秘密信息阻止可靠的漏洞利用
/GS: 通过检查Stack cookies
函数指针编码

差异化

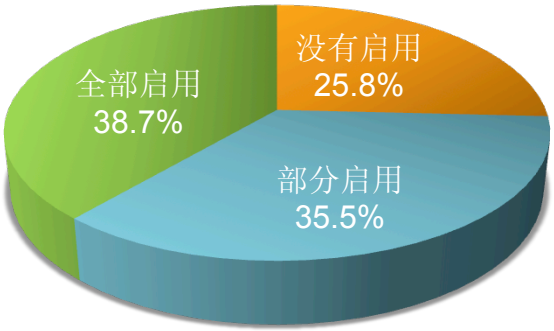
ASLR: 地址空间布局随机化
/DYNAMICBASE

规则

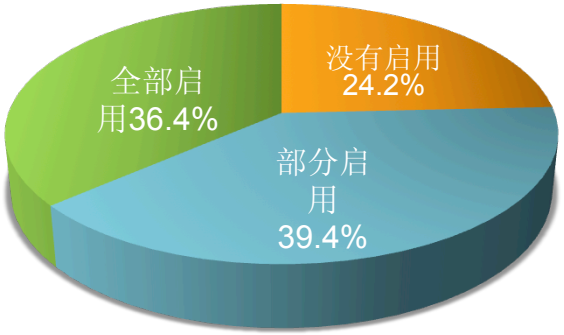
数据执行保护 (DEP)
/NXCOMPAT
SetProcessDEPPolicy()

ASLR(地址空间布局随机化)采用率

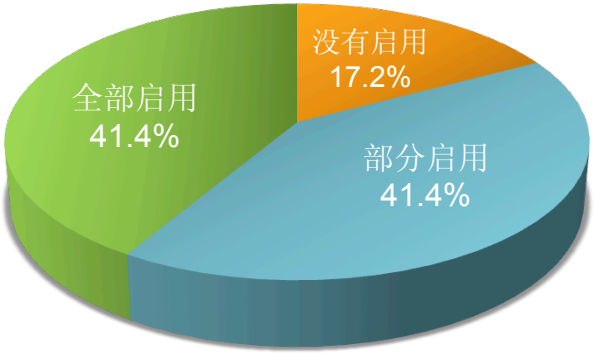
法国



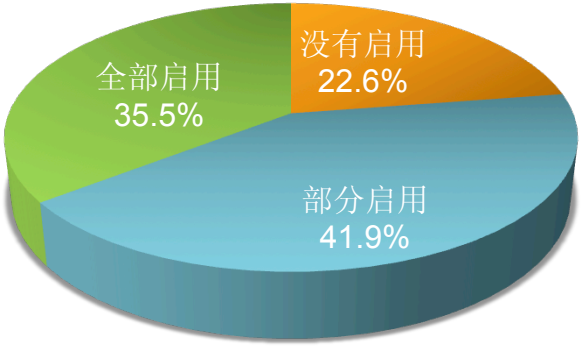
德国



俄罗斯

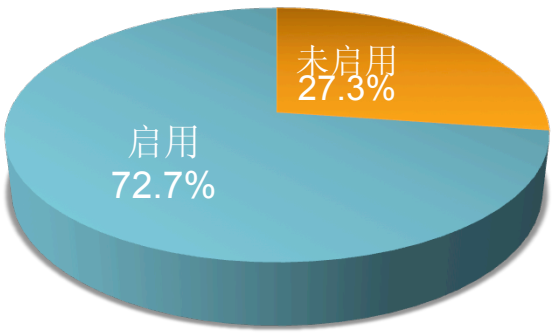


英国

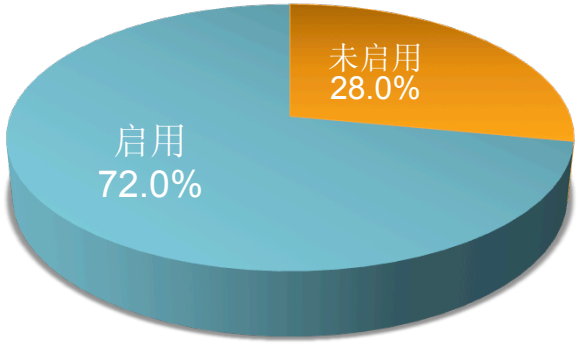


DEP(数据执行保护)采用率

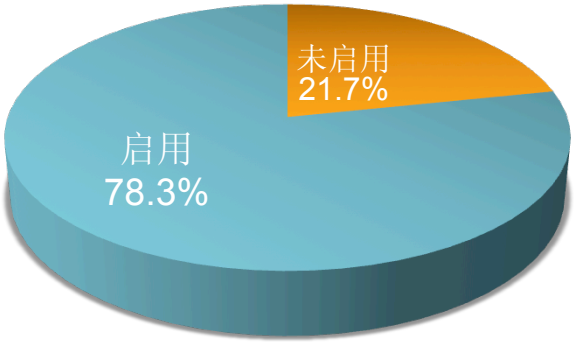
法国



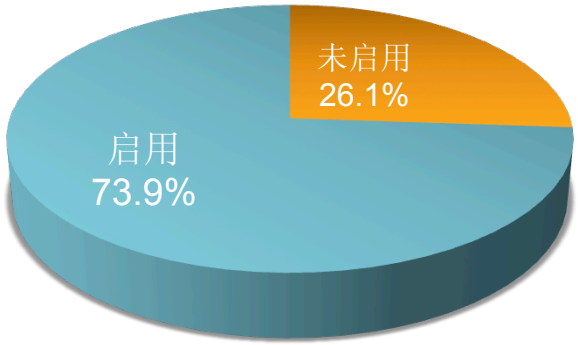
德国



俄罗斯

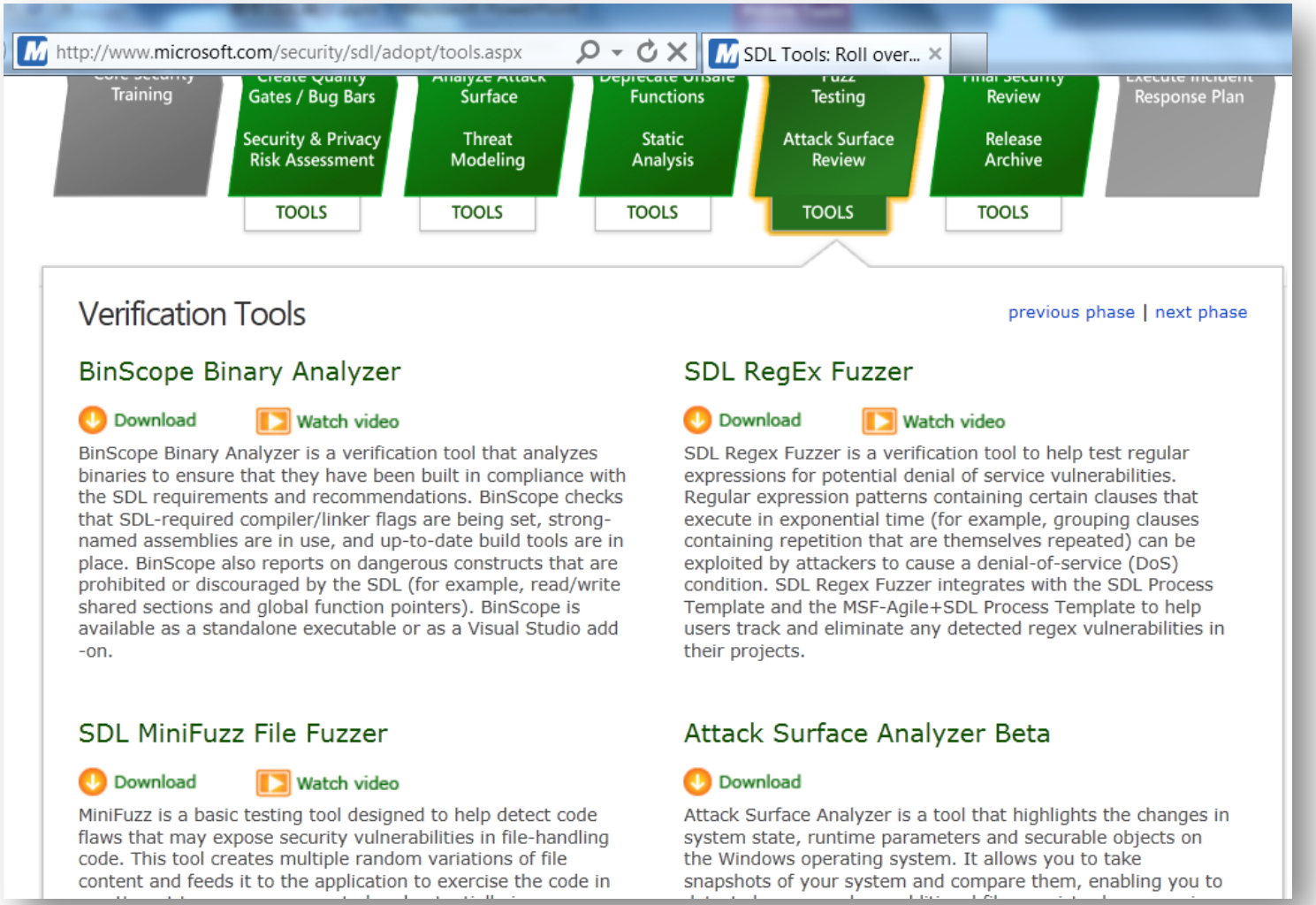


英国

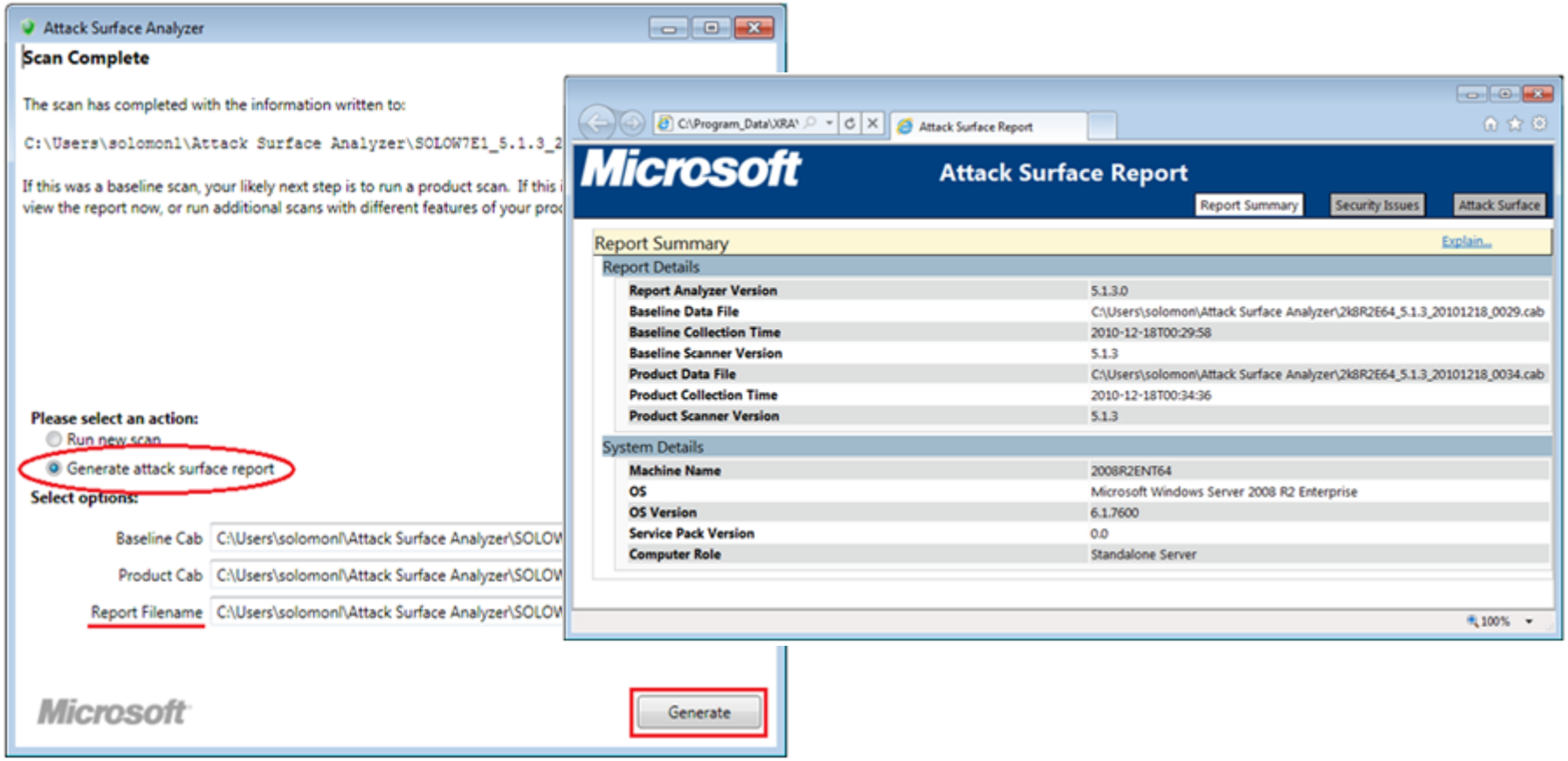


安全缓解工具

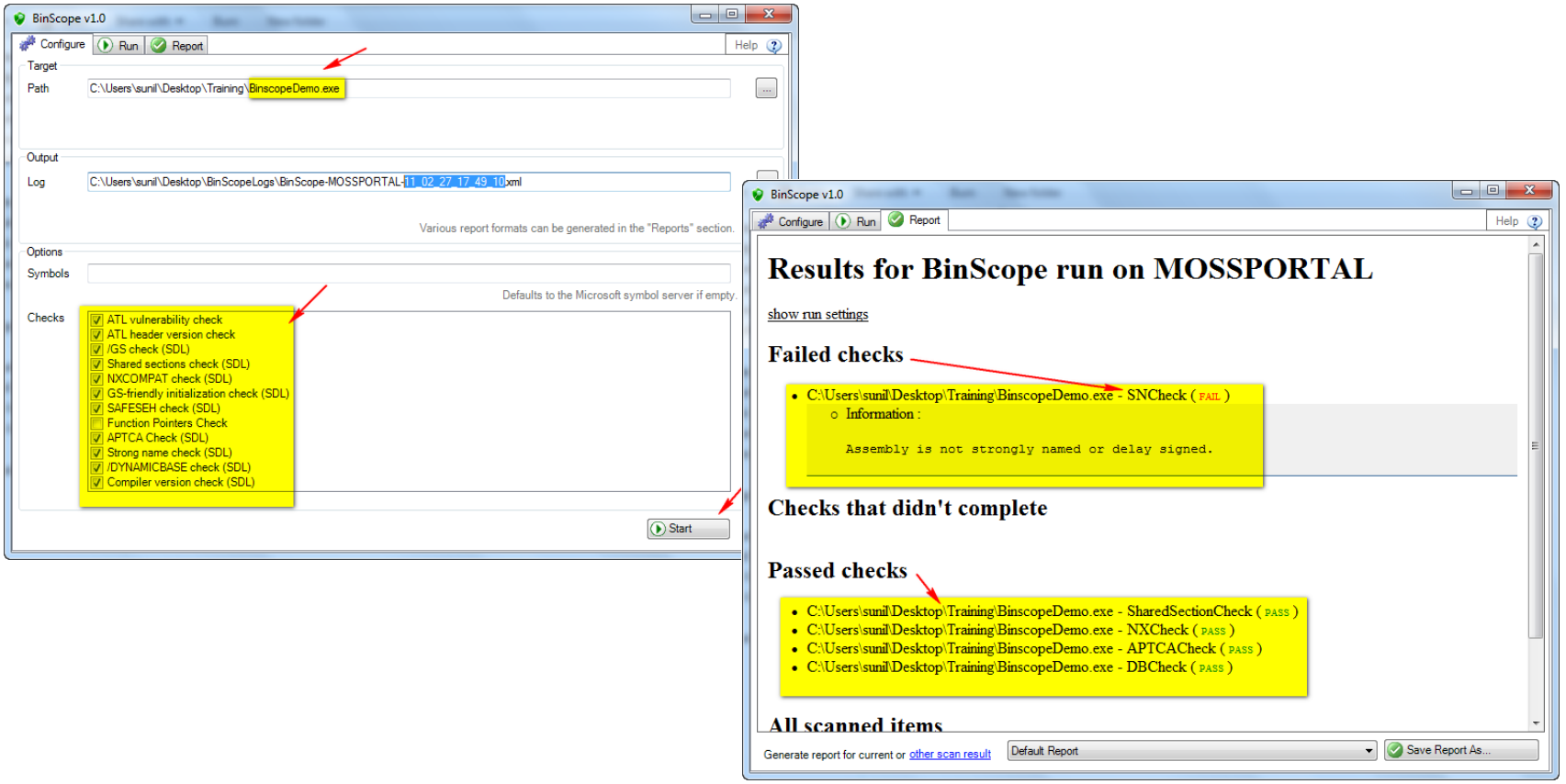
SDL免费工具


http://www.microsoft.com/security/sdl/adopt/tools.aspx
SDL Tools: Roll over...
Training
Gates / Bug Bars
Security & Privacy Risk Assessment
Surface
Threat Modeling
Functions
Static Analysis
Testing
Attack Surface Review
Review
Release Archive
Response Plan
TOOLS
TOOLS
TOOLS
TOOLS
TOOLS
Verification Tools
previous phase | next phase
BinScope Binary Analyzer
Download
Watch video
BinScope Binary Analyzer is a verification tool that analyzes binaries to ensure that they have been built in compliance with the SDL requirements and recommendations. BinScope checks that SDL-required compiler/linker flags are being set, strong-named assemblies are in use, and up-to-date build tools are in place. BinScope also reports on dangerous constructs that are prohibited or discouraged by the SDL (for example, read/write shared sections and global function pointers). BinScope is available as a standalone executable or as a Visual Studio add-on.
SDL RegEx Fuzzer
Download
Watch video
SDL Regex Fuzzer is a verification tool to help test regular expressions for potential denial of service vulnerabilities. Regular expression patterns containing certain clauses that execute in exponential time (for example, grouping clauses containing repetition that are themselves repeated) can be exploited by attackers to cause a denial-of-service (DoS) condition. SDL Regex Fuzzer integrates with the SDL Process Template and the MSF-Agile+SDL Process Template to help users track and eliminate any detected regex vulnerabilities in their projects.
SDL MiniFuzz File Fuzzer
Download
Watch video
MiniFuzz is a basic testing tool designed to help detect code flaws that may expose security vulnerabilities in file-handling code. This tool creates multiple random variations of file content and feeds it to the application to exercise the code in
Attack Surface Analyzer Beta
Download
Attack Surface Analyzer is a tool that highlights the changes in system state, runtime parameters and securable objects on the Windows operating system. It allows you to take snapshots of your system and compare them, enabling you to

攻击面分析器

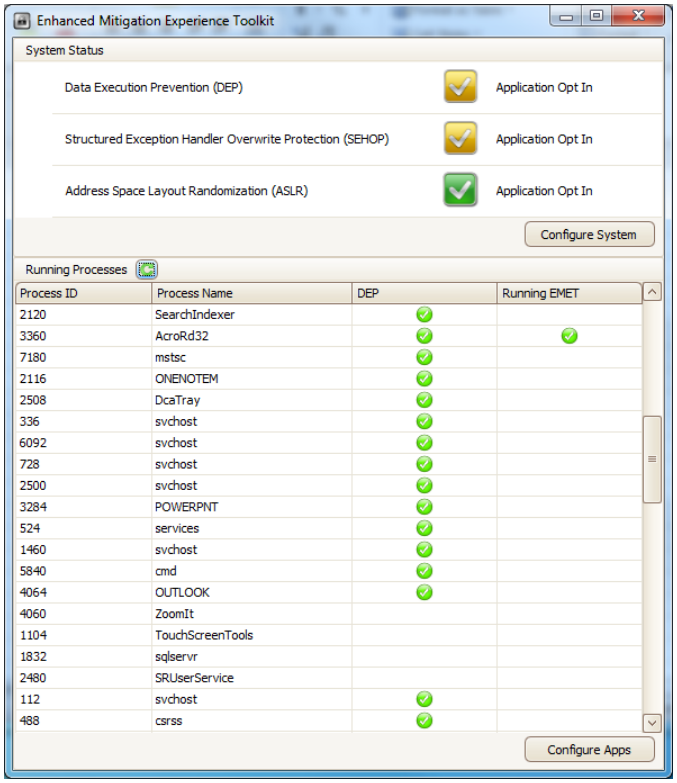

Attack Surface Analyzer
Scan Complete
The scan has completed with the information written to:
C:\Users\solomonl\Attack Surface Analyzer\SOLOW7E1_5.1.3_2
If this was a baseline scan, your likely next step is to run a product scan. If this
view the report now, or run additional scans with different features of your proc
Please select an action:
Run new scan
Generate attack surface report
Select options:
Baseline Cab
Product Cab
Report Filename
Microsoft
Generate
Attack Surface Report
Microsoft
Attack Surface Report
Report Summary
Security Issues
Attack Surface
Report Summary
Explain...
Report Details
Report Analyzer Version 5.1.3.0
Baseline Data File C:\Users\solomon\Attack Surface Analyzer\2k8R2E64_5.1.3_20101218_0029.cab
Baseline Collection Time 2010-12-18T00:29:58
Baseline Scanner Version 5.1.3
Product Data File C:\Users\solomon\Attack Surface Analyzer\2k8R2E64_5.1.3_20101218_0034.cab
Product Collection Time 2010-12-18T00:34:36
Product Scanner Version 5.1.3
System Details
Machine Name 2008R2ENT64
OS Microsoft Windows Server 2008 R2 Enterprise
OS Version 6.1.7600
Service Pack Version 0.0
Computer Role Standalone Server
100%

BinScope


BinScope v1.0
Configure
Run
Report
Help
Target
Path
C:\Users\sunil\Desktop\Training\BinscopeDemo.exe
Output
Log
C:\Users\sunil\Desktop\BinScopeLogs\BinScope-MOSSPORTAL-11_02_27_17_49_10.xml
Various report formats can be generated in the "Reports" section.
Options
Symbols
Defaults to the Microsoft symbol server if empty.
Checks
ATL vulnerability check
ATL header version check
/GS check (SDL)
Shared sections check (SDL)
NXCOMPAT check (SDL)
GS-friendly initialization check (SDL)
SAFESEH check (SDL)
Function Pointers Check
APTCA Check (SDL)
Strong name check (SDL)
/DYNAMICBASE check (SDL)
Compiler version check (SDL)
Start
BinScope v1.0
Configure
Run
Report
Help
Results for BinScope run on MOSSPORTAL
show run settings
Failed checks
C:\Users\sunil\Desktop\Training\BinscopeDemo.exe - SNCheck (FAIL)
Information :
Assembly is not strongly named or delay signed.
Checks that didn't complete
Passed checks
C:\Users\sunil\Desktop\Training\BinscopeDemo.exe - SharedSectionCheck (PASS)
C:\Users\sunil\Desktop\Training\BinscopeDemo.exe - NXCheck (PASS)
C:\Users\sunil\Desktop\Training\BinscopeDemo.exe - APTCACheck (PASS)
C:\Users\sunil\Desktop\Training\BinscopeDemo.exe - DBCheck (PASS)
All scanned items
Generate report for current or other scan result
Default Report
Save Report As...

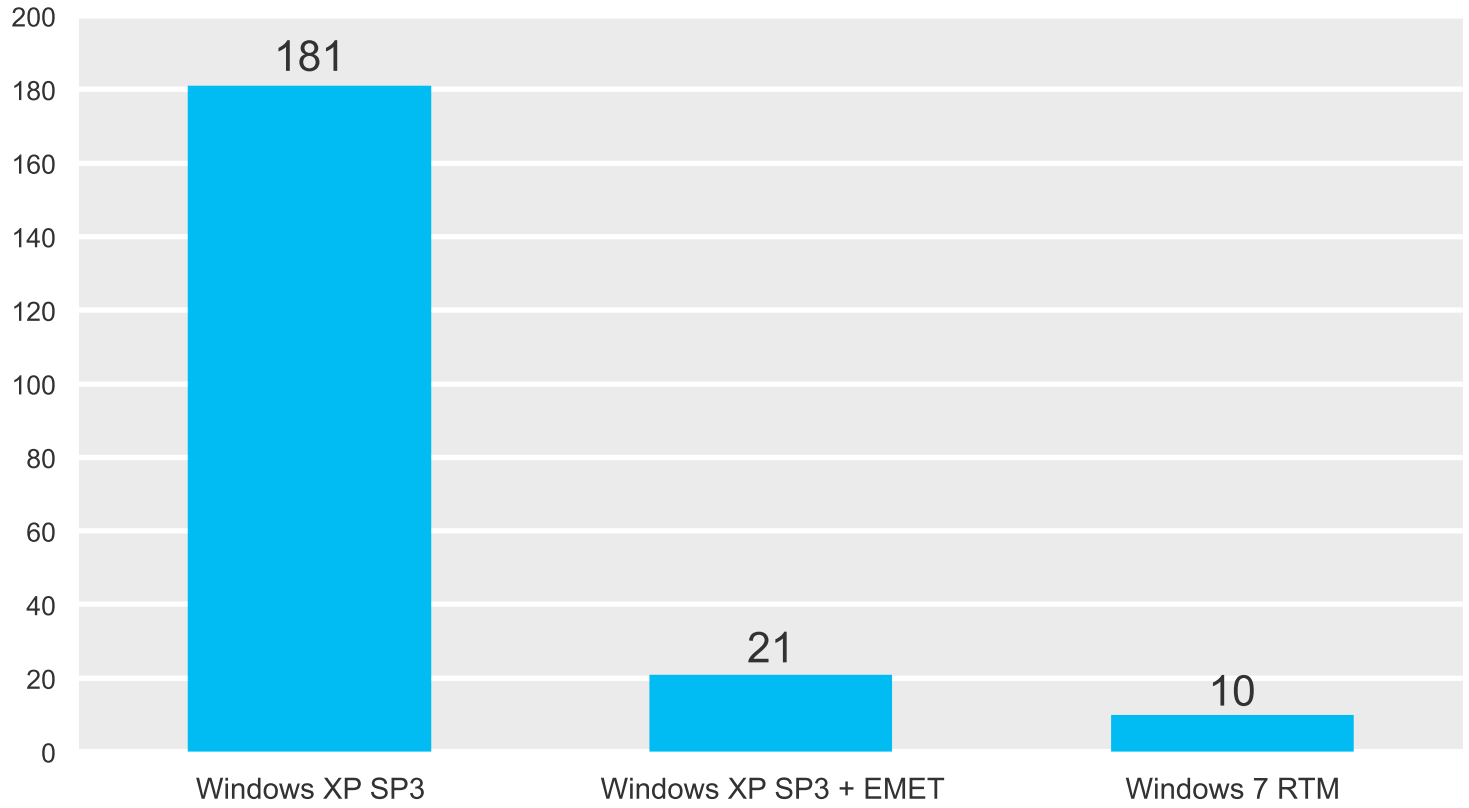
EMET(增强的缓解体验工具包)

- 用于配置和部署安全缓解技术的工具包
- 可用的缓解技术
  - 动态 DEP
  - SEHOP
  - 空页保护
  - 堆喷射分配
  - …



- 支持企业部署
- DEMO

EMET的有效性

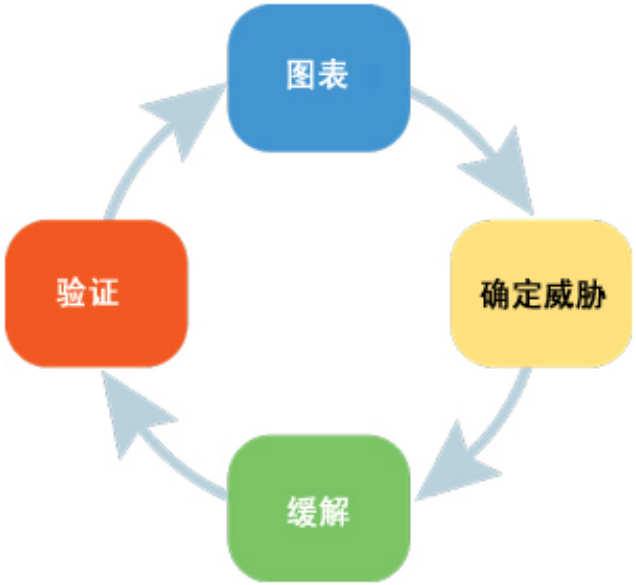


- 为了评估 EMET 应对多个常受到攻击的漏洞的有效性，微软研究人员收集了 184 个应用程序攻击的示例
- 所有攻击均是以开箱即用的方式，围绕运行于一个或多个版本的 Windows 中的常见应用程序展开

威胁建模工具

SDL 威胁建模工具使任何开发人员或软件构架师都能够：

- 就其系统的安全设计进行沟通
- 使用经过证明的方法分析其设计的潜在安全问题
- 针对安全问题建议和管理缓解技术



蓝帽奖(Bluehat Prize)

- 首届蓝帽奖比赛内容:
  - 设计一种新颖的运行时(Runtime)缓解技术, 用于防止对内存安全漏洞的利用
- 参赛时间:2011 年 8 月 3 日 – 2012 年 4 月 1 日
- 已在 2012 年 7 月美国黑帽大会上公布优胜者名单
- 知识产权归参赛者所有, 但应许可微软使用此技术
- 已经EMET3.5技术预览版中采用一项技术

一等奖:	• 200,000 美元(约合 1,300,000 人民币)
二等奖:	• 50,000 美元(约合 325,000人民币)

行动呼吁

- IT 人员
  - 软件是否实施SDL类似的安全流程以减少漏洞数量和使用缓解措施
  - 越新的软件越安全
  - 软件及时安装更新补丁
- 开发人员
  - 使用工具和SDL类似的流程以减少漏洞
  - 采用最新的漏洞对抗措施(compiler flags, DEP, ASLR)
- 用户
  - 打开Windows Update，及时安装最新补丁
  - 告别IE6，升级到IE8, IE9

资源

SDL其它相关资源

SDL 门户
http://www.microsoft.com/sdl

SDL 博客
http://blogs.msdn.com/sdl

MSDN 上的 SDL 进程
http://msdn.microsoft.com/en-us/library/cc307748.aspx

简化的 Microsoft SDL 实施
http://go.microsoft.com/?linkid=9708425

本地资源

微软安全中文博客:

- http://blogs.technet.com/b/twcchina/

官方微博:

- t.qq.com/MicrosoftTwC
- weibo.com/MicrosoftTwC

Microsoft®