State Of Security

Andrew Cushman
Sr. Director
Microsoft Security Response & Community
Microsoft Corporation

Microsoft

Before we start…

InfoWorld Log-in | Register

HOME | NEWS | TECHNOLOGIES | BLOGS/COLUMNS | TEST CENTER | AUDIO/VIDEO | CAREERS | IT EXEC-CONNECT

Microsoft security group makes 'worst jobs' list

The Microsoft Security Response Center made Popular Science's list of the worst jobs in science because the daunting work is 'hard and thankless'

By Robert McMillan, IDG News Service
June 26, 2007

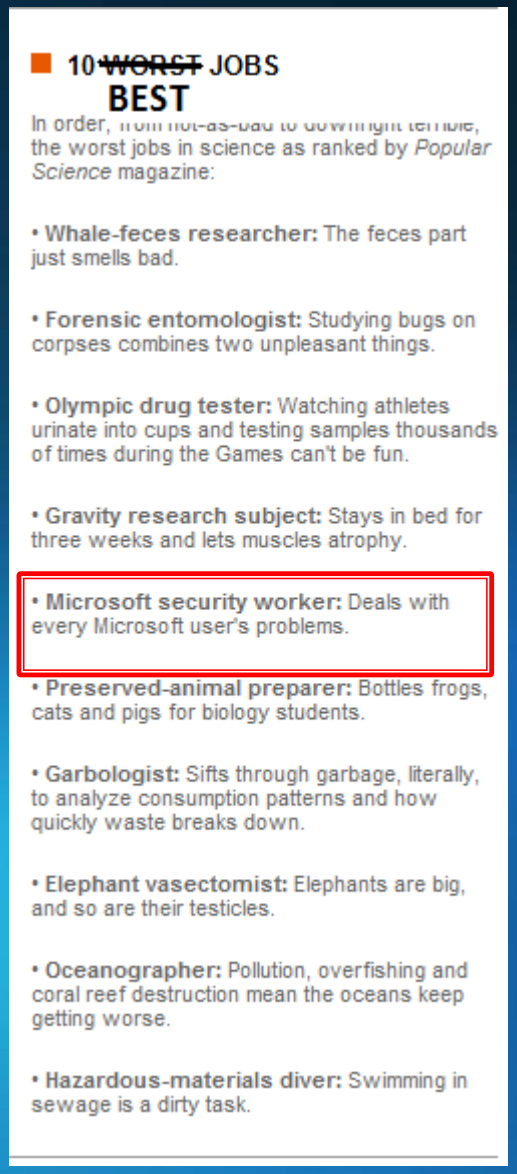
Talkback E-mail Printer Friendly Reprints Text Size A A

What do whale-feces researchers, hazmat divers, and employees of Microsoft's Security Response Center have in common? They all made *Popular Science* magazine's 2007 list of the absolute worst jobs in science.

Related Stories

Judge favors Microsoft search agreement

Popular Science has been compiling the list since 2003, as "a way to celebrate the crazy variety of jobs that there are in science," said Michael Moyer, the magazine's executive editor. Past entrants have included barnyard masturbator, Kansas biology teacher, and U.S. Metric system advocate.



10 ~~WORST~~ JOBS
BEST

In order, from not-as-bad to downright terrible, the worst jobs in science as ranked by *Popular Science* magazine:

- **Whale-feces researcher:** The feces part just smells bad.
- **Forensic entomologist:** Studying bugs on corpses combines two unpleasant things.
- **Olympic drug tester:** Watching athletes urinate into cups and testing samples thousands of times during the Games can't be fun.
- **Gravity research subject:** Stays in bed for three weeks and lets muscles atrophy.
- **Microsoft security worker:** Deals with every Microsoft user's problems.
- **Preserved-animal preparer:** Bottles frogs, cats and pigs for biology students.
- **Garbologist:** Sifts through garbage, literally, to analyze consumption patterns and how quickly waste breaks down.
- **Elephant vasectomist:** Elephants are big, and so are their testicles.
- **Oceanographer:** Pollution, overfishing and coral reef destruction mean the oceans keep getting worse.
- **Hazardous-materials diver:** Swimming in sewage is a dirty task.

Intro

- Joined Microsoft in 1990 – MSMoney, IIS
- Joined Security Team in 2003
- Attended HITB 2005 ☺
- 2007 Director MSRC & Community

Intro

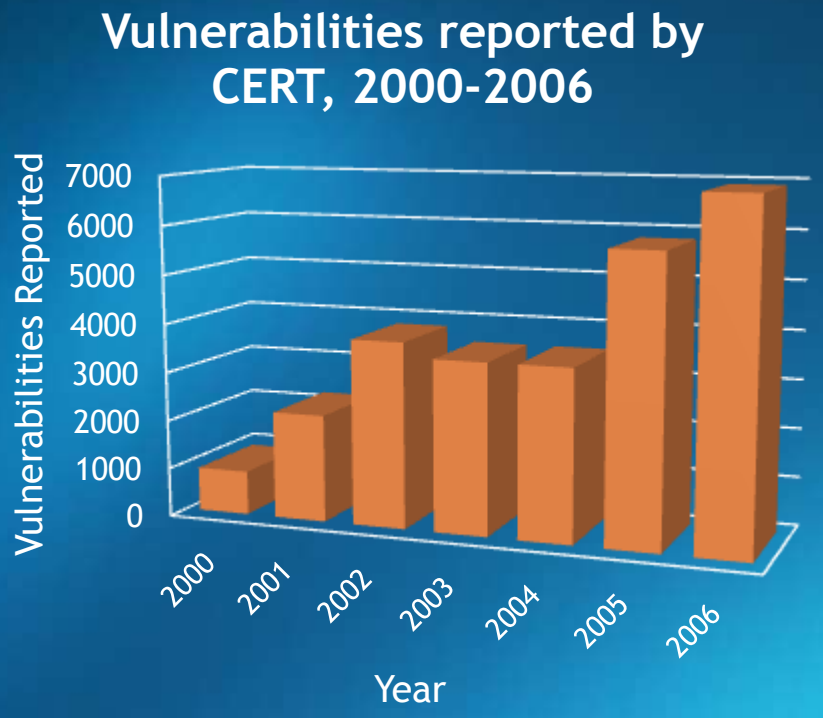
- Security Ecosystem
  - Recent Trends
  - Actors, Economics, Technical
- Evolution of the MSRC
  - MSRC view of the Ecosystem
  - Ecosystem influence on Microsoft & the MSRC
  - Case Studies
- Future Thoughts
  - Continued rapid change
  - New ideas and collaboration needed to help us protect the world

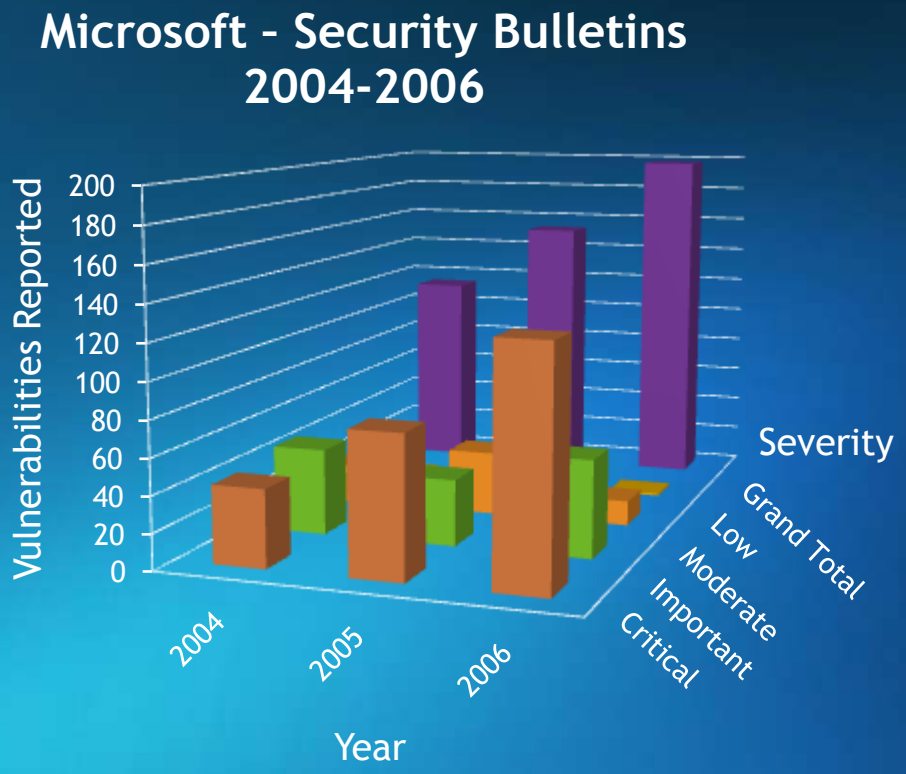
Security Ecosystem Trends

Security Ecosystem Trends

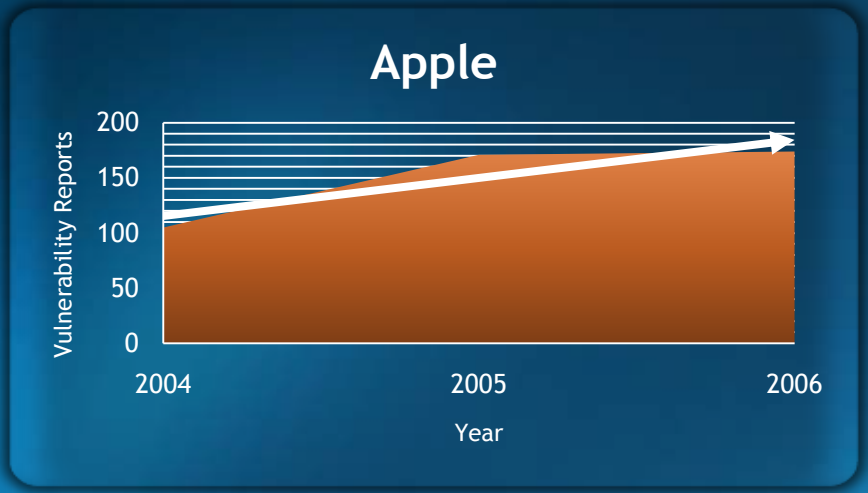
- Increased Volume of Issues
- Increased Scope of Issues
- Increasing Velocity: update to exploit time shrinking
- Each step from update to exploit is being optimized
- Malicious Attacks
- Money Economy
- Weaponization

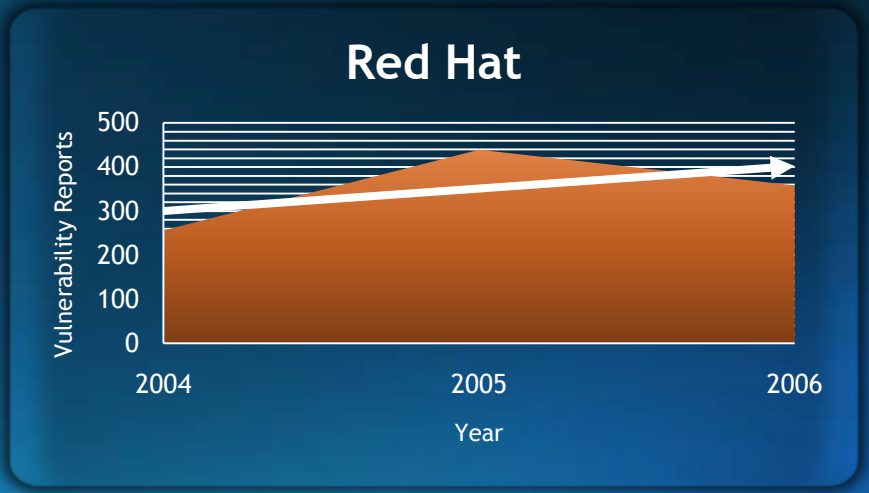
Vulnerability Reports
Year-over-year increase

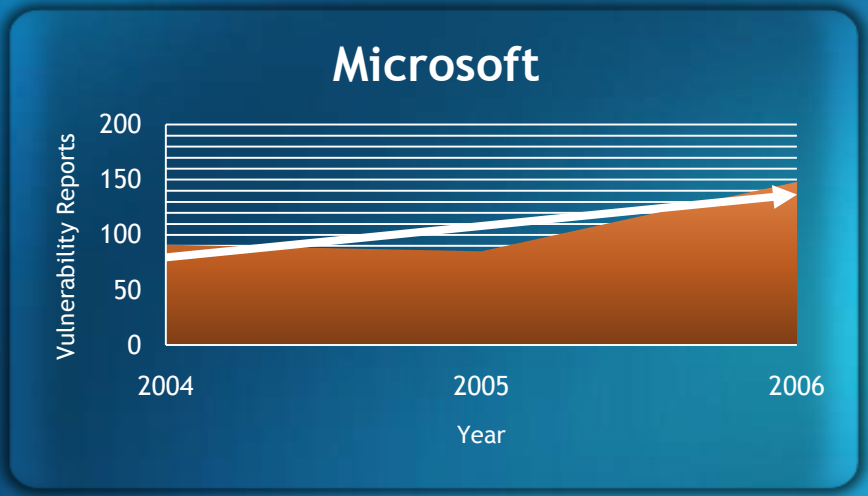


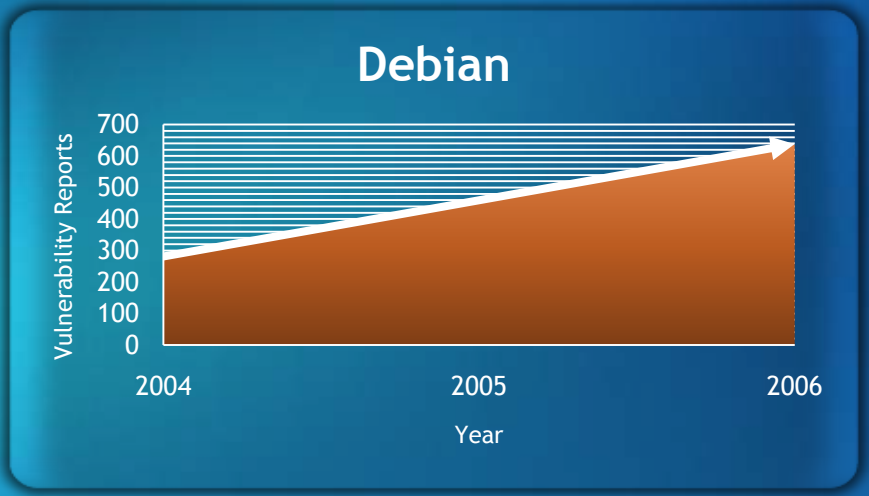


Vulnerability Reports
Comparative trends









Security Ecosystem Trends

- Increased Velocity: update to exploit time shrinking
  - Slammer (year)
  - Blaster (month)
  - Zotob (days)
    - August 9th – update released
    - August 13th – new worm
- Each step from update to exploit is being optimized
  - Update release – people waiting
  - Reverse engineering – tools, sharing
  - Proof of Concept (PoC) – collaboration, toolkits
  - Exploit use (weaponization) – open source

Reduced Barrier to Entry

Easy	• Disassemble the update
Easier	• Wait for PoC on newsgroups
Easiest	• Use a free tool or buy one
Trivial	• Buy a fully supported device

Threat landscape evolution

- From Defacements to Malicious Attacks

Characteristic	Example
Website defacements	2001 Hacking War
Era of the big worms	Blaster, Slammer
Rise of the BotNets	Zotob
Targeted Attacks	Application-level vulnerabilities

MSRC 1997 – 2007

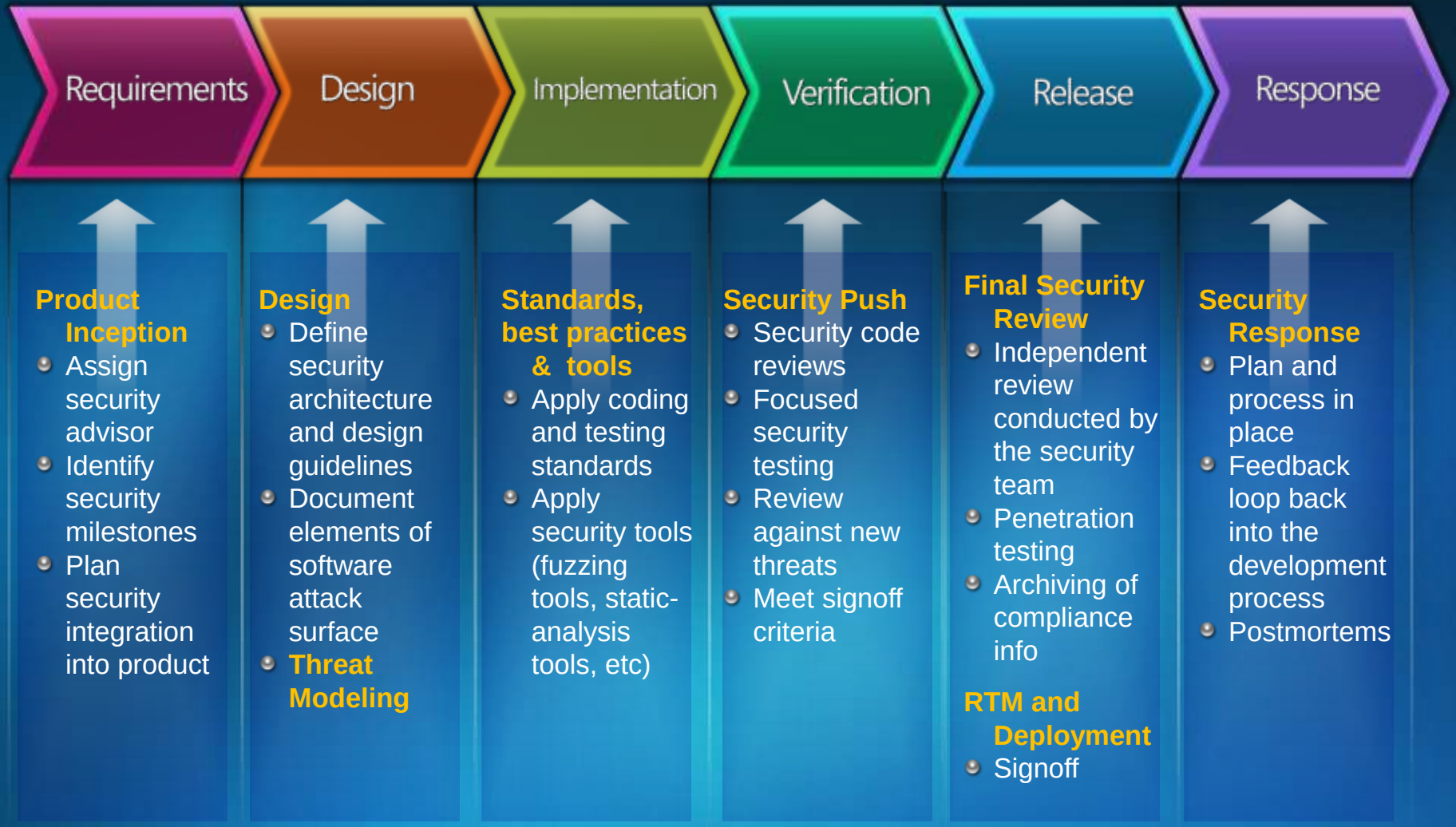
MSRC Today

Industry Leading Vulnerability Response Team

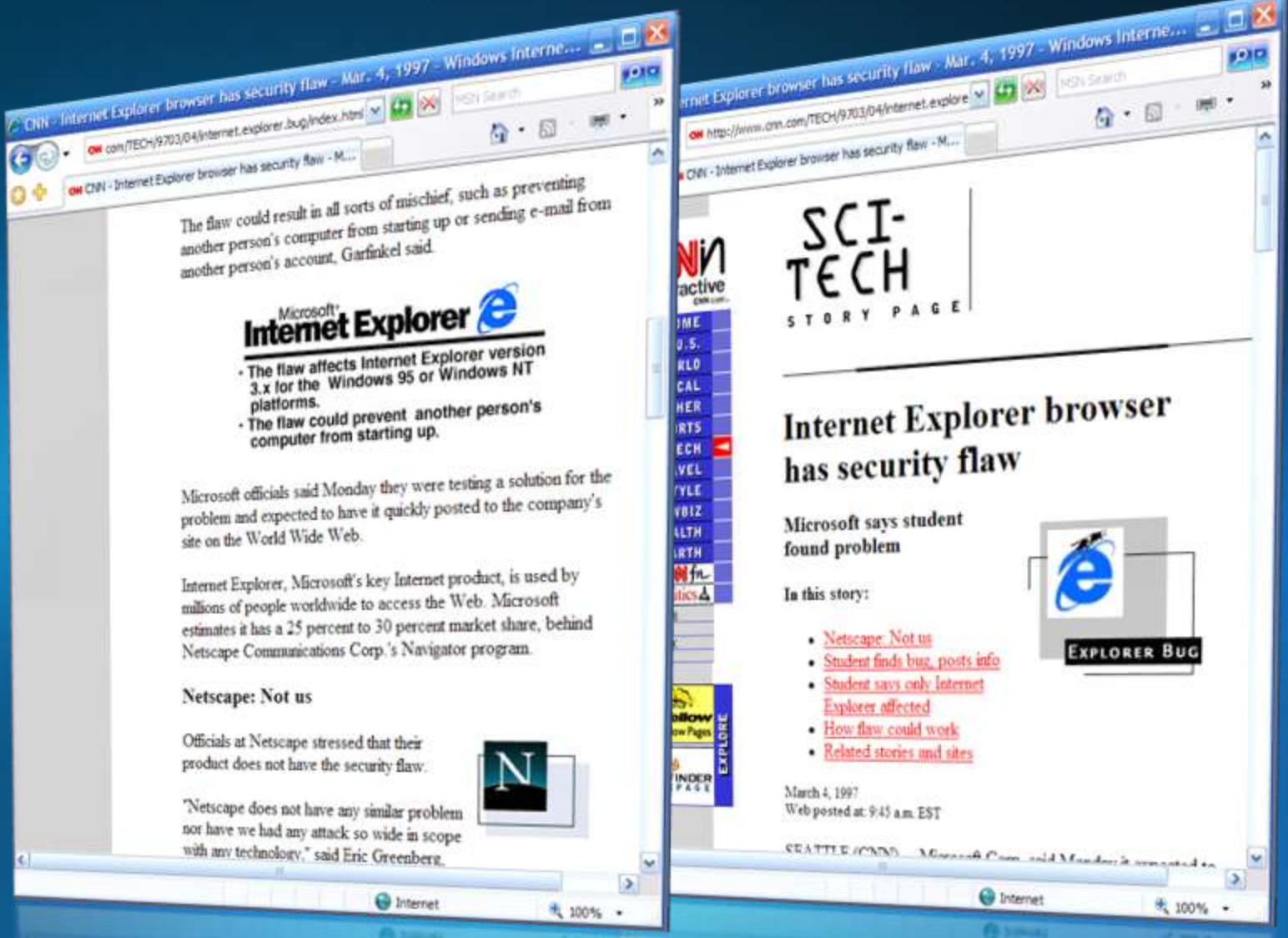
- MSRC Case Managers
- Release Management Team
- Security Engineers (SWIReact & SWIDefence)
- Communications Team
- MSRC Security Community Outreach
- MSRC Partner Outreach (CERTs, ISVs)
- Root Cause Analysis

Security Development Lifecycle

Industry Leading Security Engineering



March ’97

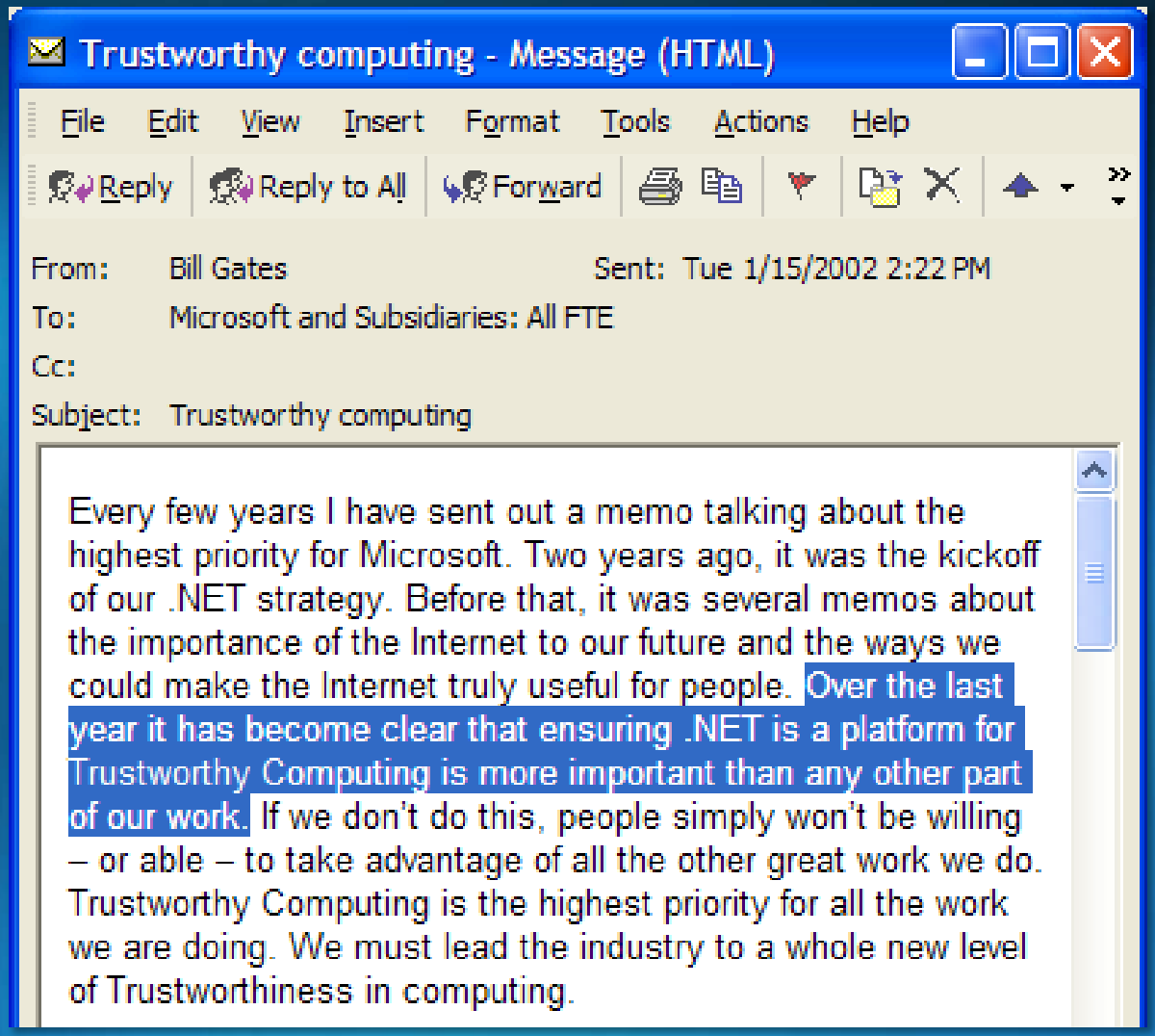

The flaw could result in all sorts of mischief, such as preventing another person's computer from starting up or sending e-mail from another person's account, Garfinkel said.
Microsoft Internet Explorer
• The flaw affects Internet Explorer version 3.x for the Windows 95 or Windows NT platforms.
• The flaw could prevent another person's computer from starting up.
Microsoft officials said Monday they were testing a solution for the problem and expected to have it quickly posted to the company's site on the World Wide Web.
Internet Explorer, Microsoft's key Internet product, is used by millions of people worldwide to access the Web. Microsoft estimates it has a 25 percent to 30 percent market share, behind Netscape Communications Corp.'s Navigator program.
Netscape: Not us
Officials at Netscape stressed that their product does not have the security flaw.
"Netscape does not have any similar problem nor have we had any attack so wide in scope with any technology," said Eric Greenberg,
SCI-TECH
STORY PAGE
Internet Explorer browser has security flaw
Microsoft says student found problem
In this story:
Netscape: Not us
Student finds bug, posts info
Student says only Internet Explorer affected
How flaw could work
Related stories and sites
EXPLORER BUG
March 4, 1997
Web posted at: 9:45 a.m. EST

…After The Dust Settled

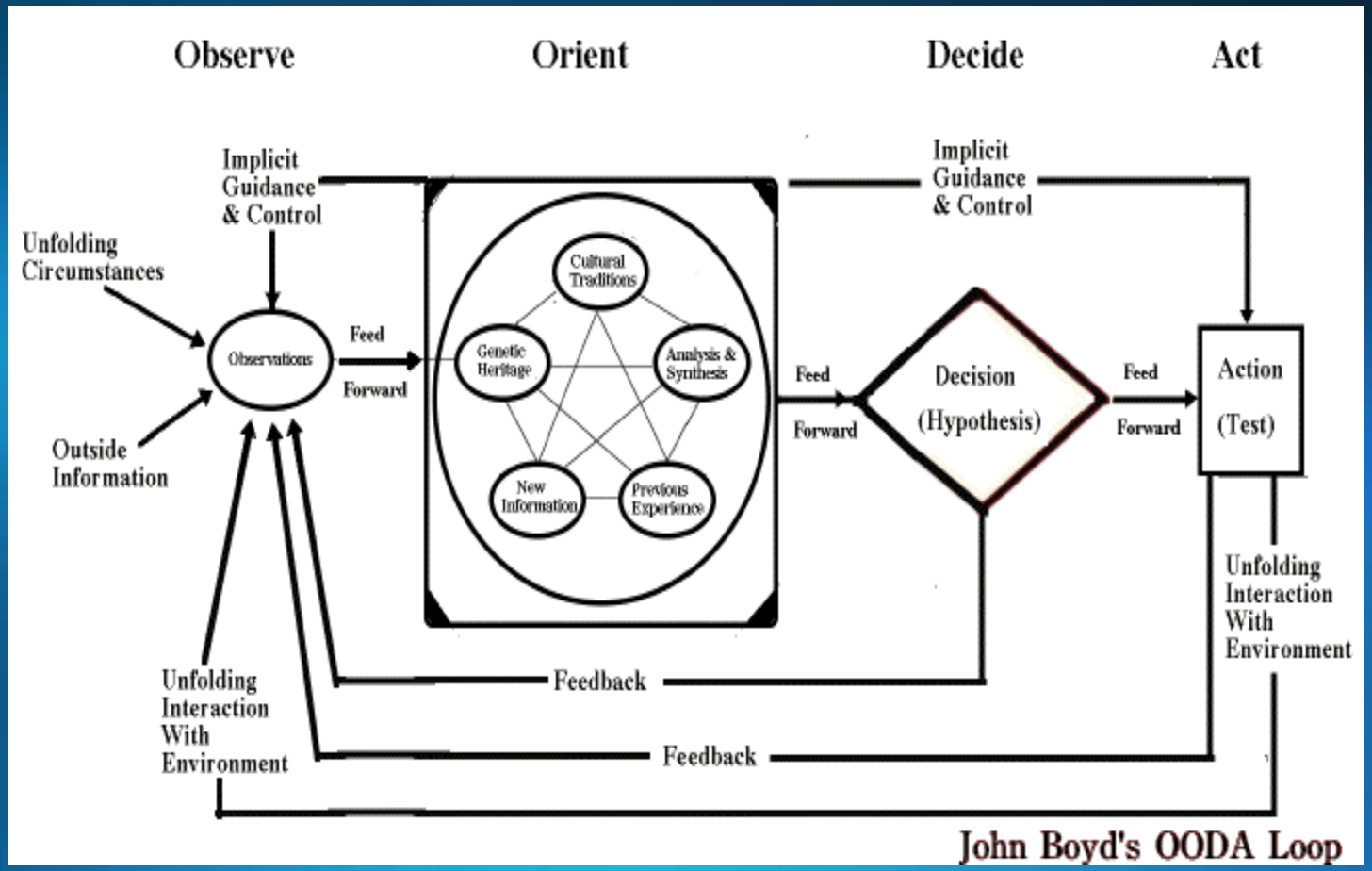
- Created secure@microsoft.com
- Internet Explorer Security Team
- Security Windows Initiative
- Microsoft Security Response Center
- Understood the influence of Security Research Community

Security Development Lifecycle -1997

The TWC Memo


Trustworthy computing - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: Bill Gates Sent: Tue 1/15/2002 2:22 PM
To: Microsoft and Subsidiaries: All FTE
Cc:
Subject: Trustworthy computing
Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing – or able – to take advantage of all the other great work we do. 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.

OODA Loop


Observe
Orient
Decide
Act
Implicit Guidance & Control
Unfolding Circumstances
Observations
Feed Forward
Outside Information
Cultural Traditions
Genetic Heritage
Analysis & Synthesis
New Information
Previous Experience
Implicit Guidance & Control
Feed Forward
Decision (Hypothesis)
Feed Forward
Action (Test)
Unfolding Interaction With Environment
Feedback
Unfolding Interaction With Environment
Feedback
John Boyd's OODA Loop

Security Response Process

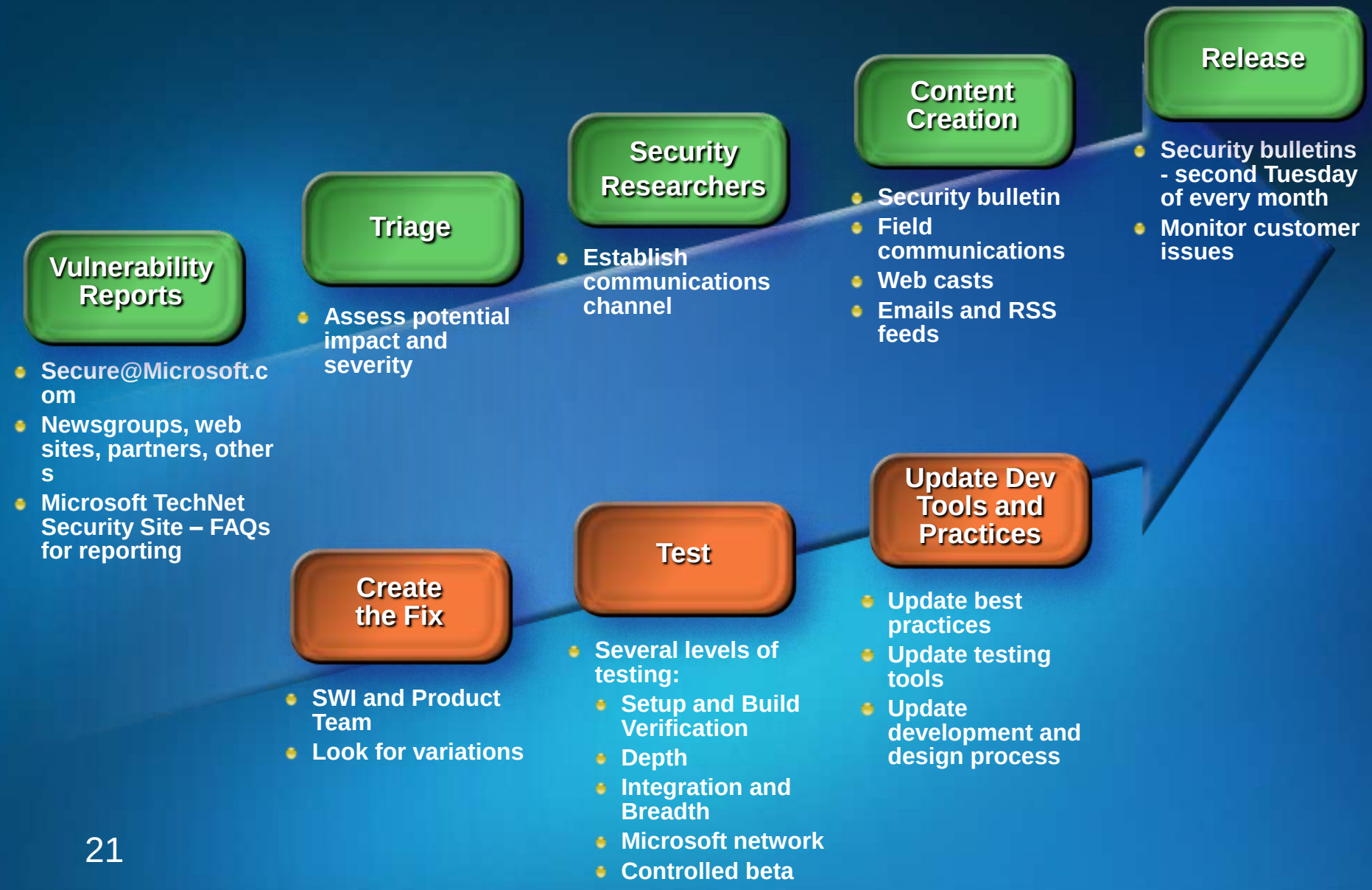
Security Bulletin Release Process

- Repeatable, Consistent, Process
- High Quality Product Updates
- Authoritative Accurate Guidance

Security Incident Response Process

- Timely and Relevant Information
- Mitigations and Protection
- Solution and Guidance

The Response Lifecycle



The SSIRP Lifecycle

Responding to a security incident

- Observe environment to detect any potential issues
- Leverage existing relationships with
  - Partners
  - Security researchers and finders
- Monitor customer requests and press inquiries
- Notify partners: GIAIS and VIA

- Convene and evaluate severity
- Mobilize security response teams and support groups into two main groups
  - Emergency Engineering Team
  - Emergency Communications Team
- Start monitoring worldwide press interest and customer support lines for this issue

- Assess the situation and the technical information available
- Start working on solution
- Communicate initial guidance and workarounds to customers, partners and press
- Notify and inform Microsoft sales and support field
- Deliver appropriate Solution (update, tool, fix, or blog)

- Provide information and tools to restore normal operations
- Conduct internal process reviews and gather lessons learned

MSRC Role & View of the Ecosystem

MSRC Role

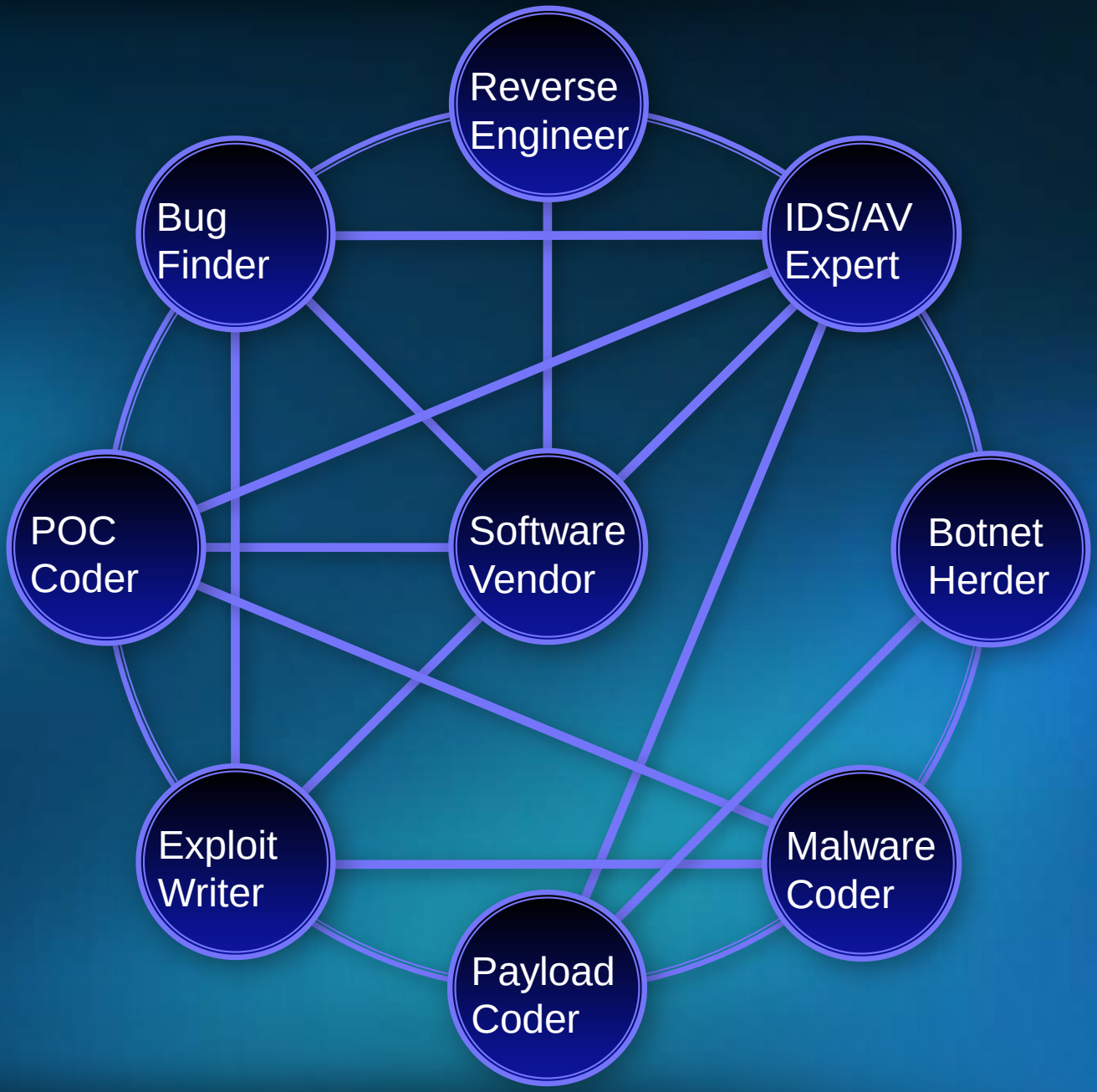
- Microsoft Security Response Center - MSRC
  - Protect our customers
  - Understand the security ecosystem
  - Analyzing threats and respond to them
  - Work with partners as part of distributed defense network
  - Root cause analysis and provide feedback and guidance to product groups
  - When possible attempt to
    - Influence negative trends
    - Balance the asymmetry

Ecosystem Elements

- Actors
  - Understand their decision making process
  - Engage all segments
- Technology
  - Extinguish classes of issues
  - Identify attack and research trends
- Economics
  - Promote legitimate business opportunities
  - Increase the cost of illegal activities

Security Ecosystem: Actors & Technologies

Complexity of Vulnerability Ecosystem



Security Ecosystem

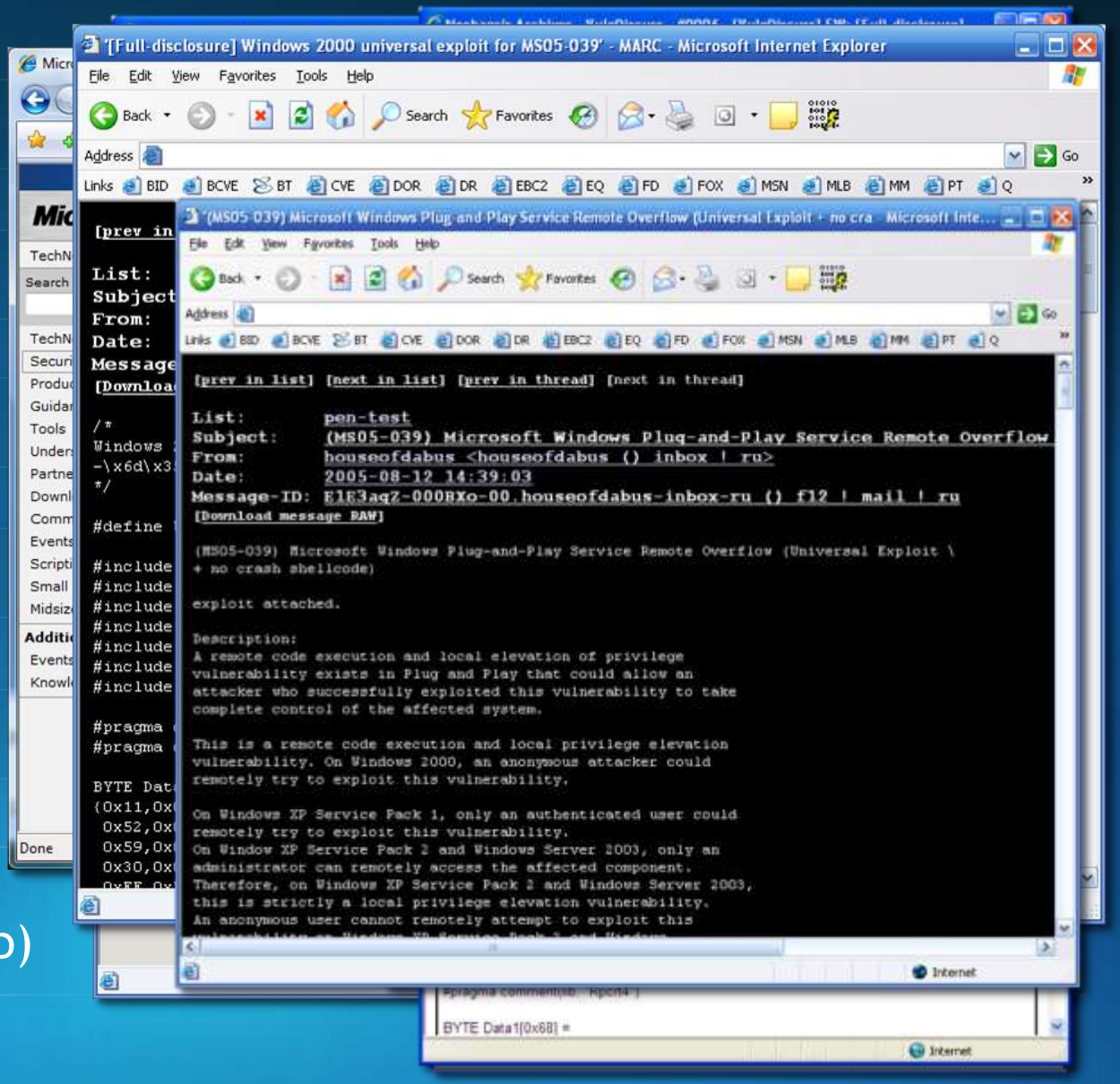
Finders / Security Researchers

- Diverse community
- Working across
  - Technologies
  - Geographies
  - Time zones
- Big headache, good friend & good teacher
- Black Hat -> BlueHat

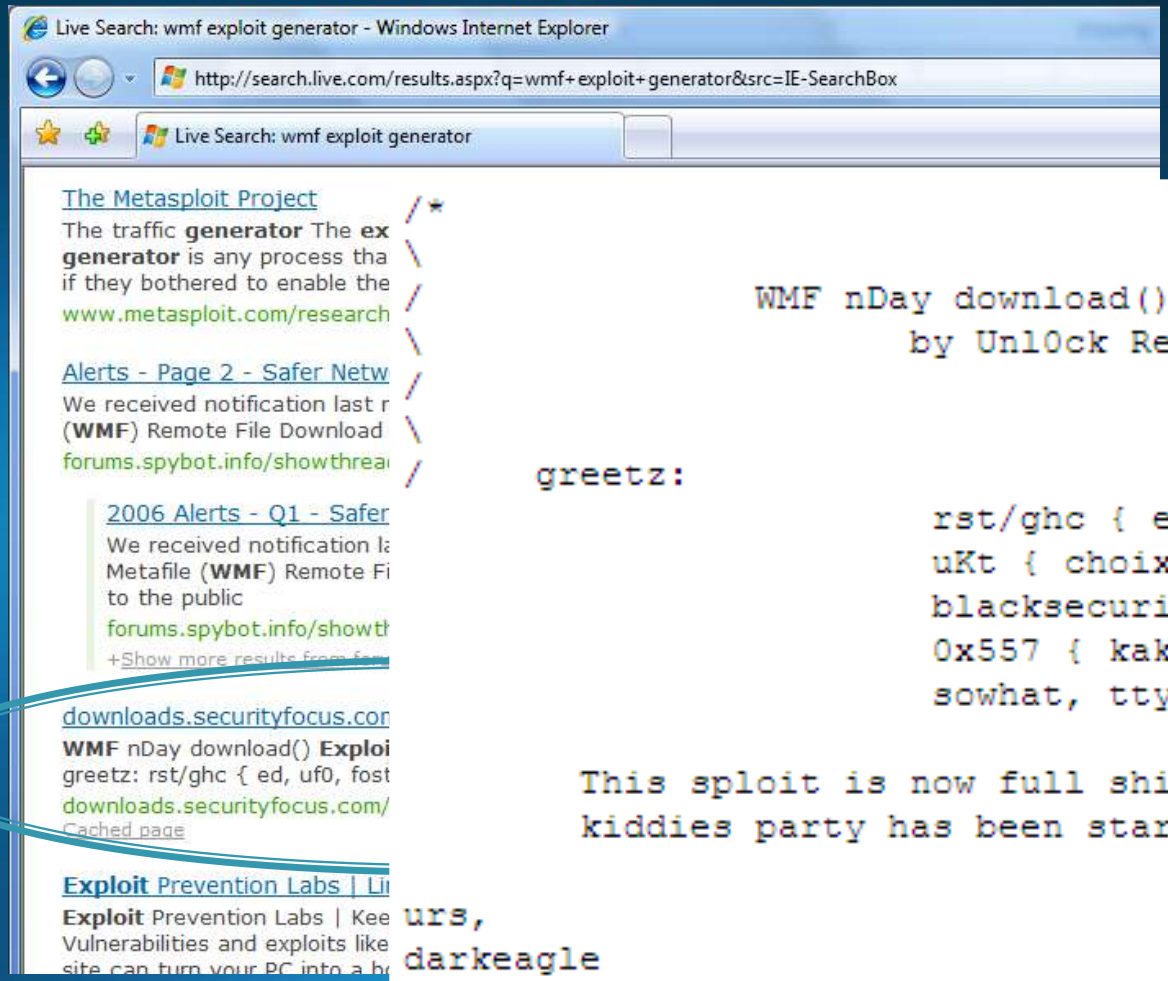
Security Ecosystem

Tracing Our Advisory To An Exploit

1. Original Advisory
2. Newsgroup chatter
3. Private offers
4. 1st Exploit
5. 2nd exploit
6. 3rd exploit
   (which became Zotob)



Weaponization - WMF example




```
/*
\
/                WMF nDay download() Exploit Generator
\                      by Unl0ck Research Team
/
\
/      greetz:
                        rst/ghc { ed, uf0, fost },
                        uKt { choix, nekd0, payhash, antq },
                        blacksecurity { #black } ,
                        0x557 { kaka, swan, sam, nolife },
                        sowhat, tty64 { izik };

          This sploit is now full shit, so...
          kiddies party has been started!!!

urs,
darkeagle
\
/
*/
```

Security Ecosystem

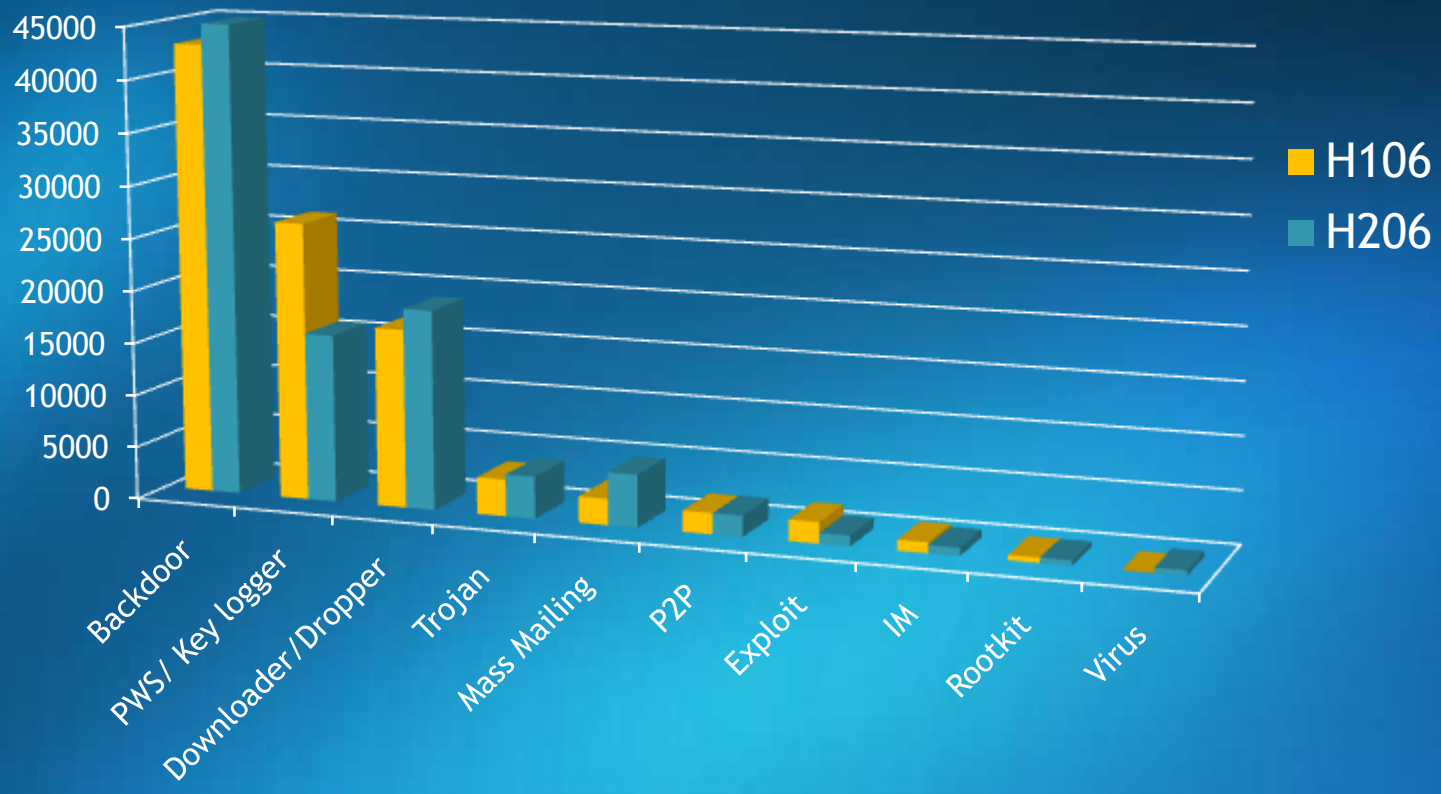
Security Intelligence Reports

Security Ecosystem

“It’s all about making money”

"He says it's all about making money, and that he doesn't care if people remove the worm because it's the spyware stuff that he installs that's making him the money," Taylor said in a conversation with me.

New Malware Variants By Category



Case Studies

The Vandals

1998-2001

Defacements

Web Site Defacements

- 1998 – 1999 Several countries are reported involved in patriotic hacking: United States, Pakistan, China, Brazil
- December 28, 1999 – a hacking group declares cyberwar against Iraq and China
- January 7, 1999 – Several other hacking groups make successful plea for restraint
- March 31, 2001– U.S. and Chinese planes collide
- April / May 2001 – Cyberwar breaks out again.

Series of unfortunate events

Name	First date seen in wild
Melissa	Friday July 23, 1999
Bubbleboy	Wednesday November 10, 1999
Loveletter	Thursday May 4, 2000
Transition to weaponized vulnerabilities	
Code Red I	Thursday July 12, 2001
Code Red II	Saturday August 4, 2001
Nimda	Tuesday September 18, 2001

The Era of the Big Worms

Code Red

Fixed	June 18, 2001	MS01-33
Exploited	July 13, 2001	

Design Issues :

- Kitchen sink approach – Everything on by default

Code Issues :

- Vuln was in a loop and a MB to Wchar conversion
- Code Red vuln was not discovered by Prefix

```
WCHAR wcsAttribute[200];
            if ( cchAttribute >= sizeof wcsAttribute )
            if ( cchAttribute >= ( sizeof wcsAttribute / sizeof WCHAR ) )
                THROW( CException( DB_E_ERRORSINCOMMAND ) );
             DecodeURLEscapes( (BYTE *)
pszAttribute, cchAttribute, wcsAttribute,
                                webServer.CodePage() );
             if ( 0 == cchAttribute )
                THROW( CException( DB_E_ERRORSINCOMMAND ) );

            DecodeHtmlNumeric( wcsAttribute );
```

Code Red

Engineering / Response Actions :

- Updated Prefix Tool and Usage
  - New plug in development & more frequent runs
- SD3 – Features “Off by Default”
  - Secure by Design, Default and Deployment
- URLScan & Security Roll-up Package
- STPP – Strategic Technology Protection Program

Slammer

Fixed	July 24, 2002	MS02-39
Exploited	January 2003	

Design Issues :

- Features still on by default
- Giblet

Code Issues :

- Anonymous access to RPC endpoints

```
#define INSTREGKEY "SOFTWARE\\Microsoft\\Microsoft SQL Server\\"
#define MAX_RECV_MSG 256

SSRPMSGTYPE SsrpRecvMsg(BYTE *rgbRecvBuf) {
  ...
  bytesRecd = recvfrom( gSvrSock, (char*)rgbRecvBuf, MAX_RECV_MSG, 0,
                        (SOCKADDR *)&gclientAddr, &cClientAddr );

  return((SSRPMSGTYPE)rgbRecvBuf[0]);
}

BOOL SsrpEnum(LPSTR szInstName, ...) {
  ...
  char szregVersion[128];
  ...
  sprintf(szregVersion,"%s%s\\MSSQLServer\\CurrentVersion",INSTREGKEY,szInstName);
```

Slammer
(SQL Resolution Service issue)

Engineering / Response Actions:

- “Giblet” tracking system
- SSIRP Process
- SQL Server 2000 sp3

Blaster

Fixed	July 16, 2003	MS03-26, MS03-03
Exploited	August 11, 2003	

Design Issues :

- Features still on by default
- COM model made for extensibility, not security

Code Issues :

- Anonymous access to RPC endpoints

```
error_status_t _RemoteActivation(WCHAR *pwszObjectName,     ... )  {
    *phr = GetServerPath( pwszObjectName, &pwszObjectName);
```

Port 135 (i.e. The Internet)

```
}

// GetServerPath calls GetMachineName directly w/ pwszOjectName...
HRESULT GetMachineName(
    WCHAR * pwszPath,
    WCHAR   wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN + 1]) {
    pwszServerName = wszMachineName;
    LPWSTR pwszTemp = pswzPath + 2;
    while ( *pwszTemp != L'\\' )
        *pwszServerName++ = *pwszTemp++;
    ...
```

Blaster

(RPC/DCOM Buffer overrun)

Engineering / Response Actions:

- XPSP2
- Authenticated RPC in XPsp2
- AutoUpdate WU and monthly updates
- Firewall turned on and rules

Image Parsers – WMF, ANI…

Design Issues :

- Lots of formats
- Lots of complexity

Code Issues :

- Legacy support and App Compat
- Cut ‘n Paste reuse

Bulletin Number	File Type
00-090	ASX
01-042	NSC
02-072	MP3
03-030	MIDI
04-007	ASN.1

Bulletin Number	File Type
04-022	JOB
04-023	CHM
04-025	GIF
04-028	JPG
04-034	ZIP

Bulletin Number	File Type
05-002	ANI
05-002	BMP
05-002	CUR
05-002	IOC
05-009	PNG

Bulletin Number	File Type
05-035	DOC
05-036	ICC
05-052	GIF
05-053	EMF
05-053	WMF

Bulletin Number	File Type
06-001	WMF
06-002	EOT
06-003	TNEF
06-005	BMP
06-012	XLS

Case Study – Parser Bugs… WMF, ANI

Engineering / Response Actions:

- Creation of a Tools team in SEC
- Fuzzing now a requirement for MSRC and SDL
- Partner w/ product teams
  - SEC provides an extensible Fuzzing framework
  - Teams provide protocol / file format expertise

Case Study: /gs, NX & ASLR

Design Issues :

- Asymmetry btw Attacker and Defender
- Ability to Execute Data as Code
- Homogeneous Windows Environment

Code Issues :

- Impossible to find and fix all BO's

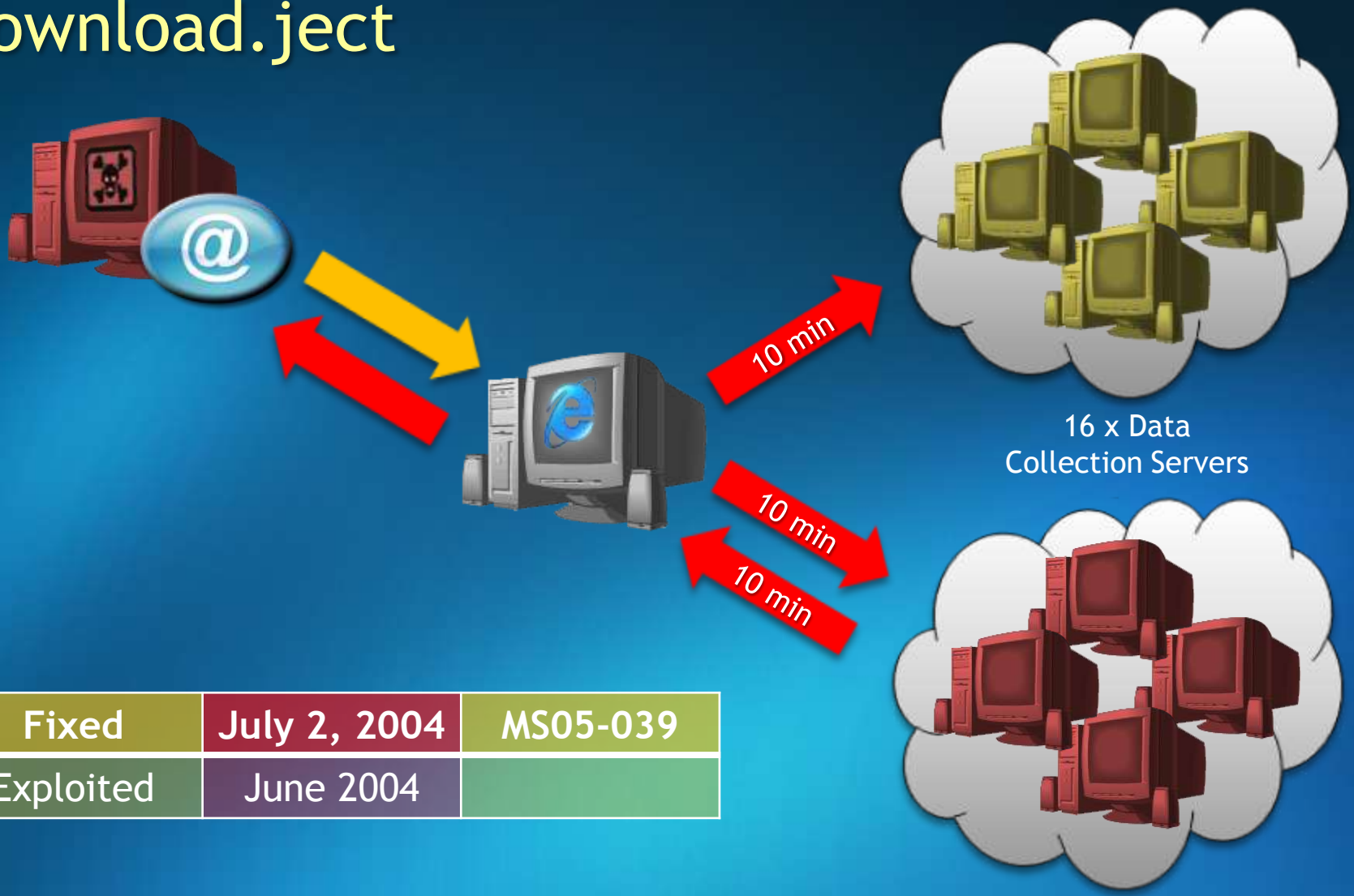
Engineering / Response Actions:

- Rev'ed / gs multiple times
- Addition of ASLR in Windows Vista
- Windows Vista heap corruption mitigations

The Rise of the Botnets

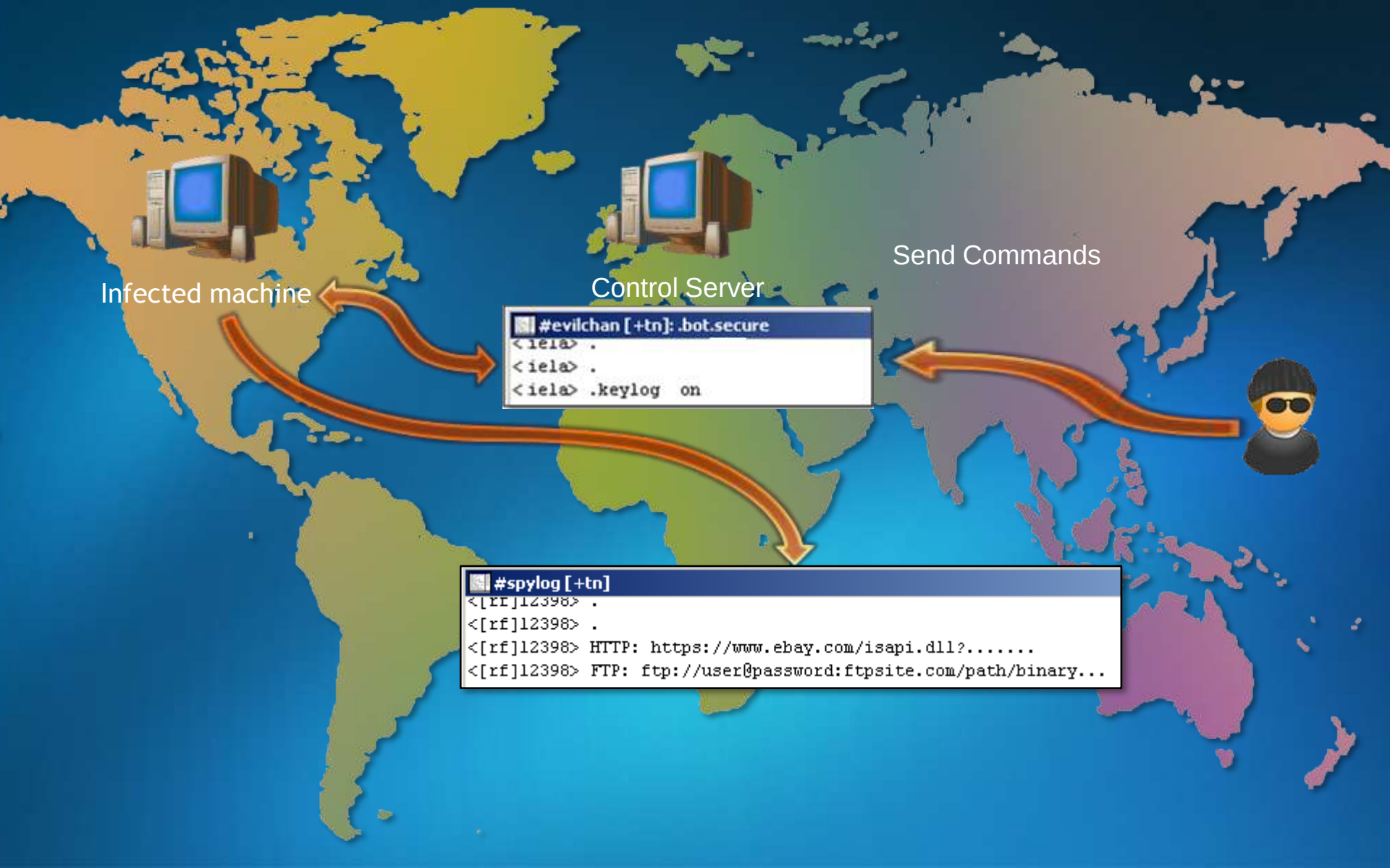
Transitional Event: C&C

Download.ject



Fixed	July 2, 2004	MS05-039
Exploited	June 2004	

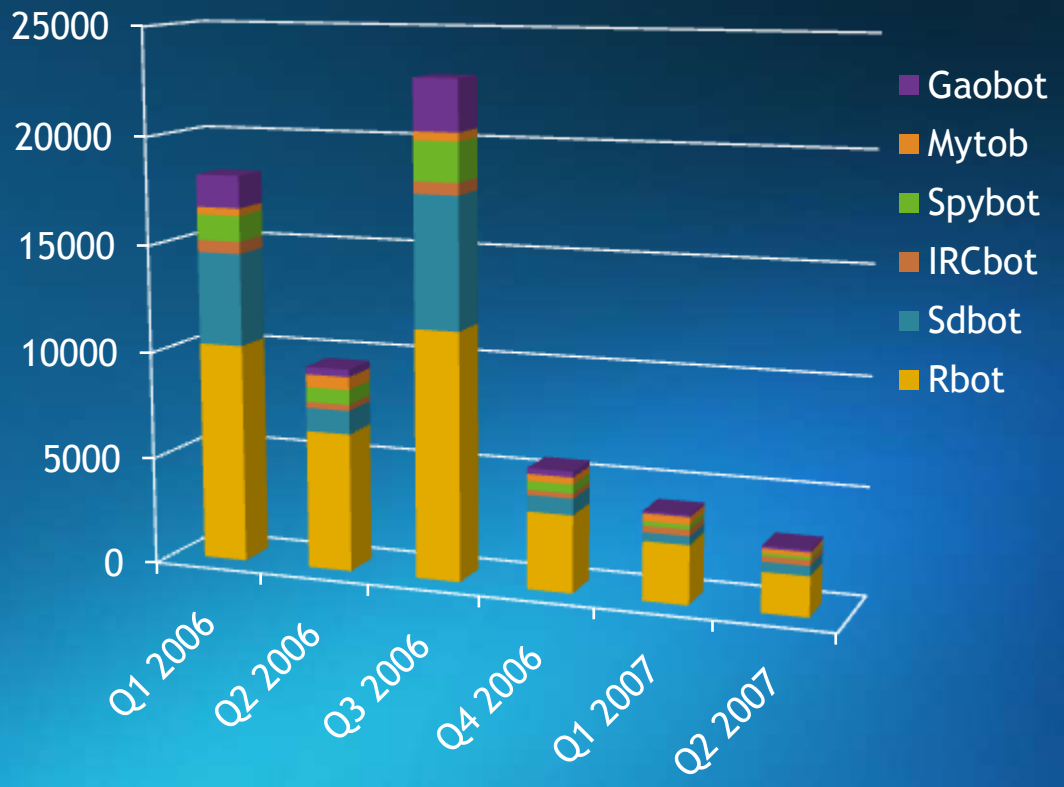
Anatomy Of A Botnet



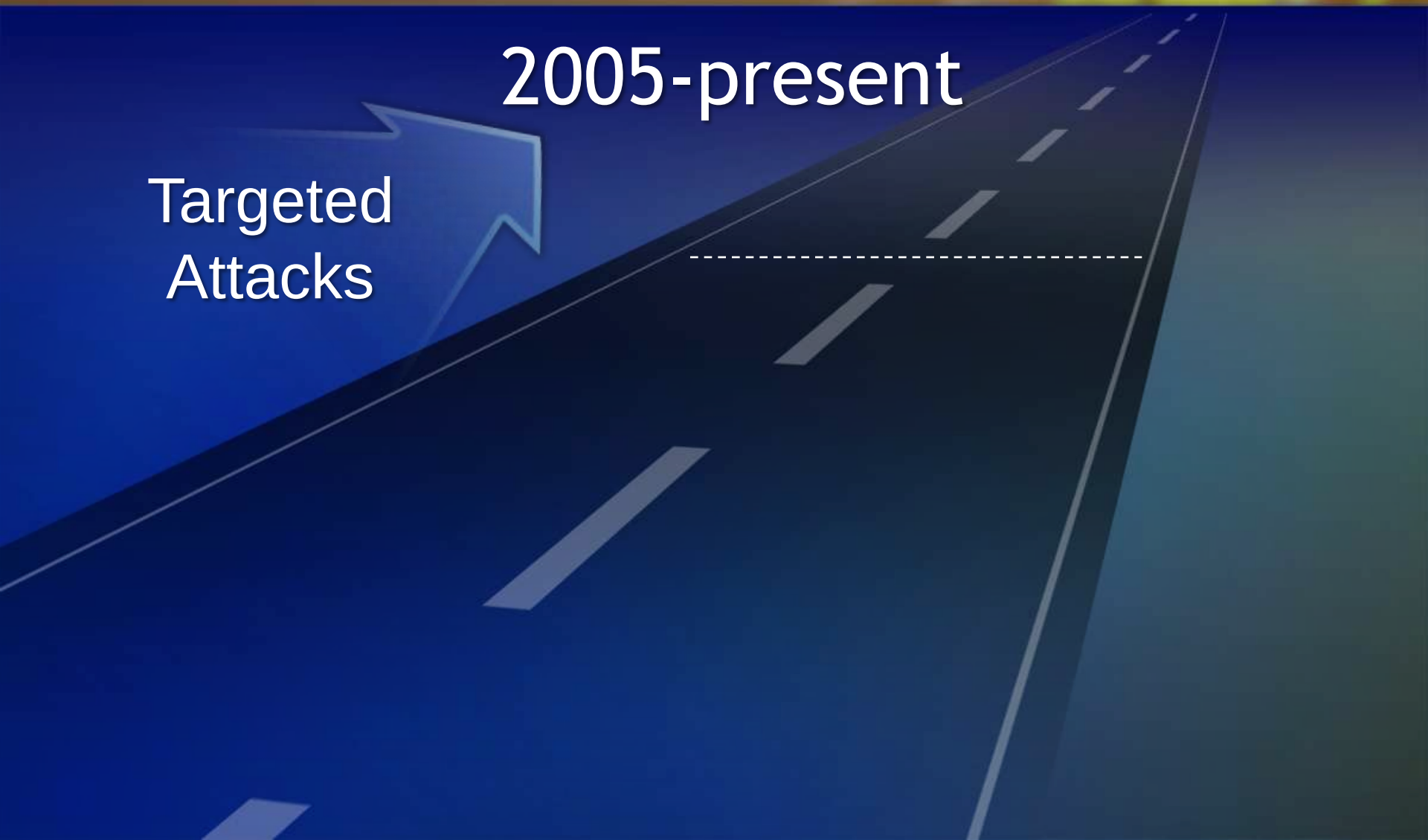
New Bot Variants

- Variants since Jan 2006

Family	Variants
Rbot	36,518
Sdbot	13,164
IRCbot	2,214
Spybot	4,470
Mytob	2,241
Gaobot	4,711



The Era of Purpose



Security Market Forces

- New cases w/ Organized elements
  - Command and Control
  - Distraction tactics
  - Hiding in plain sight
  - Careful target selection

Escalation and Focus

- What if the organization had
  - Significant resources
  - Institutional Support
  - Time horizon
  - Focus on specifics…right down to the individual
- The intensity of the threat increases
- Our products will face increased scrutiny
- Securing our customers becomes more complex

Call To Action

Community-based defense

Rapid response communications

Investment in defensive security knowledge

Denying opportunities to malicious software

Support of worldwide law enforcement and legislatures

Microsoft®

Your potential. Our passion.™