

State Of Security

George Stathakopoulos
General Manager
Security Engineering and Communications
Microsoft Corporation

Intro

- Joined Microsoft in 1991
- Assigned to Security in 1997



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

Focusing minds of the Execs

- “3vil day”
- “g00d day”

Understanding The Security Ecosystem

- Actors
- Technology impact
- Business model

Security Ecosystem

Vulnerability



Finders

Proof of Concept



Exploiters

Payload



Malware houses

Botnet



Attacker

???



Organized

Security Ecosystem

Vulnerability



Finders

Finders (Security Researchers)

- Diverse community
- Working across
 - Technologies
 - Geographies
 - Time zones
- Big headache and best friend
- Blackhat -> Bluehat

Security Ecosystem

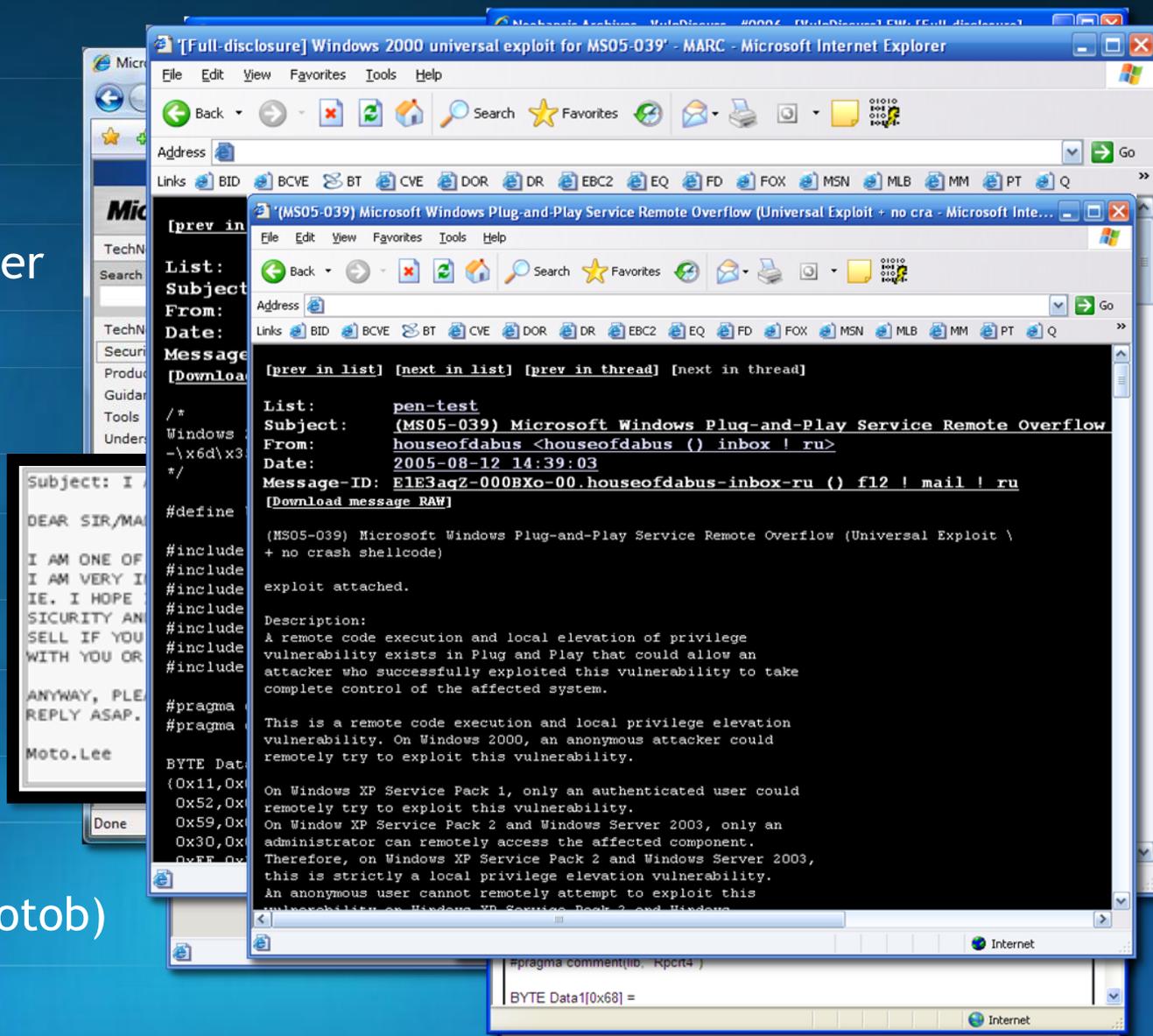
Proof of
Concept



Exploiters

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)

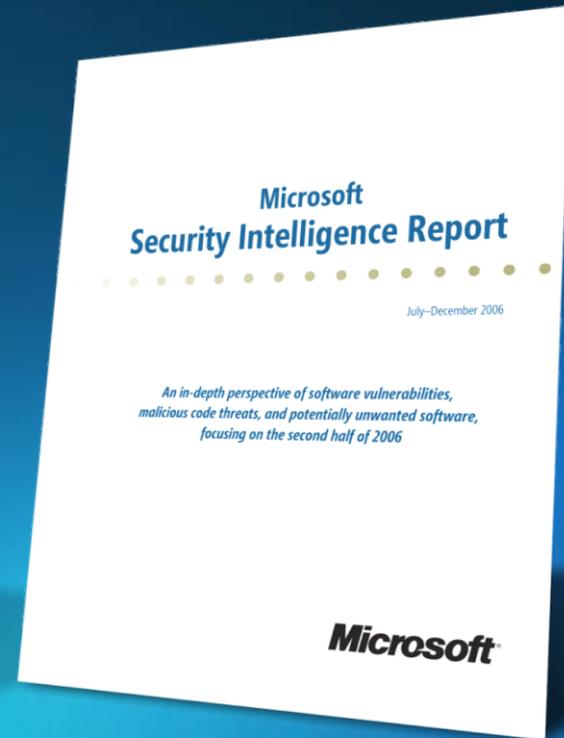
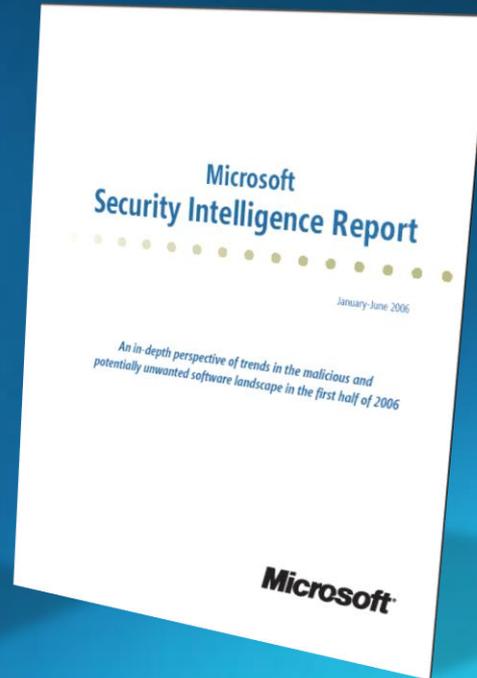


Security Ecosystem

Payload



Security Intelligence Reports



Security Ecosystem

Botnet



Malicious Attacks!

- Changes theory to reality
- Were the hard lessons are learned
- Attack meets the defence
- A journey that is constantly evolving

The Vandals

1998-2001

Defacements

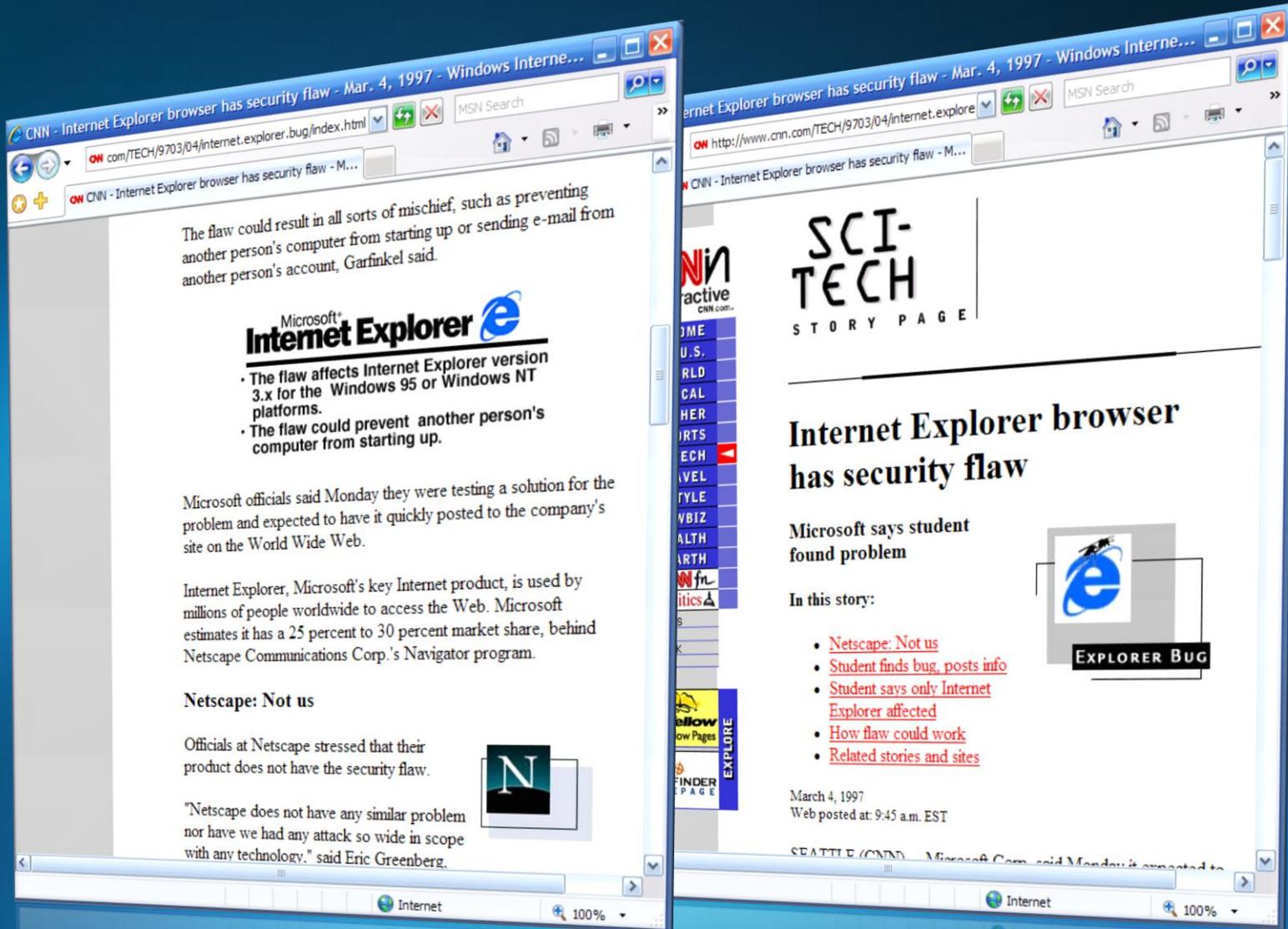


Web Site Defacements

- **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.



March '97



CNN - Internet Explorer browser has security flaw - Mar. 4, 1997 - Windows Interne...

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.

Internet Explorer browser has security flaw - Mar. 4, 1997 - Windows Interne...

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](#)

March 4, 1997
Web posted at: 9:45 a.m. EST

SEATTLE (CNN) - Microsoft Corp. said Monday it expected to

 **EXPLORER BUG**

...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

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

2001-2004

Worms



Slammer

(SQL resolution service issue)

Fixed	July 24, 2002	MS02-39
Exploited	January 2003	

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

Microsoft Security Response Center

Managing and resolving security vulnerabilities and security incidents

Security Bulletins



- Published for each Microsoft security update
- Mitigations and workarounds for fixed vulnerabilities
- Distribution and deployment guidance
- Bulletin ratings
 - Critical
 - Important
 - Moderate
 - Low

Security Advisories



- Supplement Microsoft Security Bulletins
- Provide early information about vulnerabilities, mitigations and workarounds
- Updated throughout incident with new information

MSRC Blog



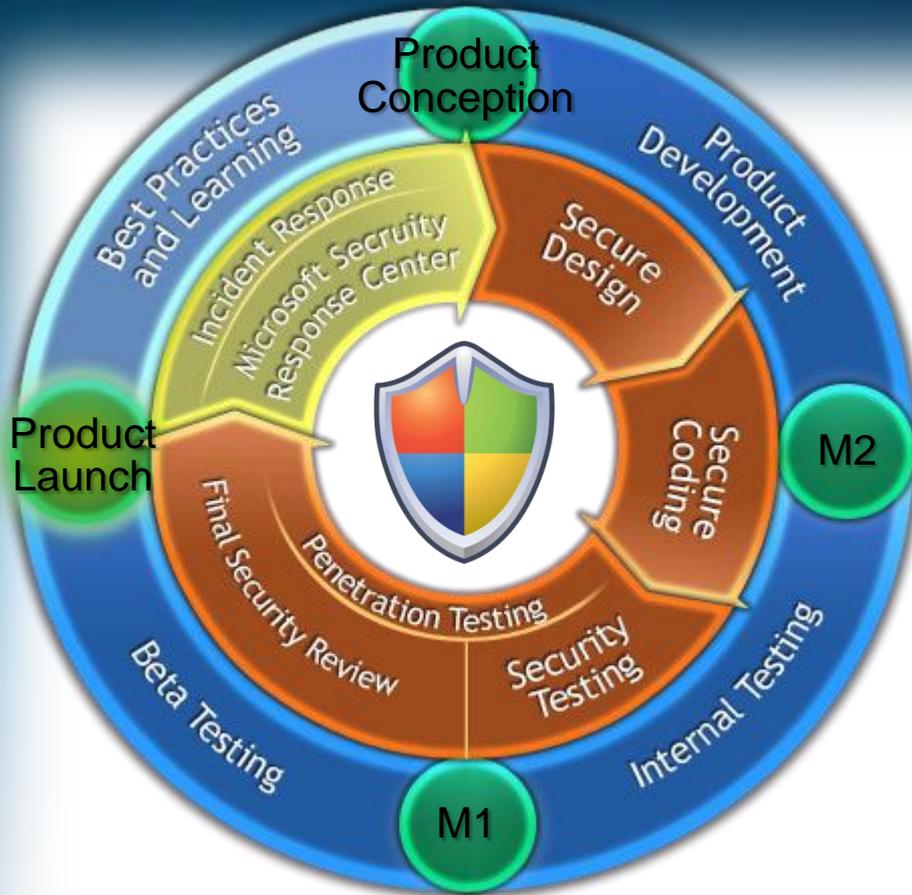
- Insights directly from the MSRC team
- Updates on recent security related news, activities, announcements, and threat issues
- <http://blogs.technet.com/msrc/>

Blaster

(RPC/DCOM Buffer overrun)

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

Security Development Lifecycle



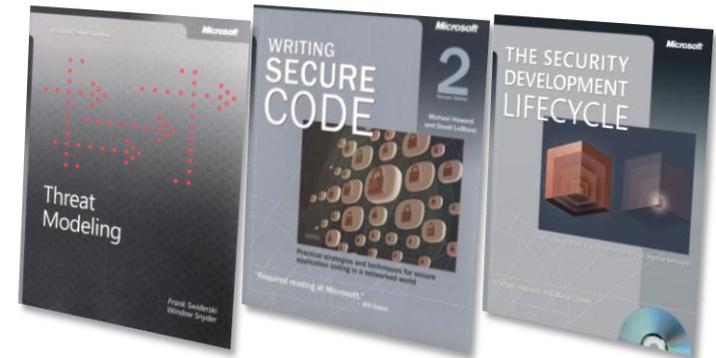
Process

Education

Accountability

 Microsoft Product Development Lifecycle

 Microsoft Security Development Lifecycle



SDL Blog

The screenshot shows a Windows Internet Explorer browser window. The title bar reads "The Security Development Lifecycle : Lessons learned from the Animated Cursor Security Bug - Windows Internet Explorer". The address bar shows the URL "http://blogs.msdn.com/sdl/archive/2007/04/26/lessons-learned-from-the-animate" and the search term "sdl blog". The browser interface includes a menu bar (File, Edit, View, Favorites, Tools, Help) and a toolbar with various icons. The main content area features a header image of a cactus with a paperclip holding a note that says "The Security Development Lifecycle". Below the header is a navigation bar with links for HOME, EMAIL, RSS 2.0, and ATOM 1.0. The article title is "Lessons learned from the Animated Cursor Security Bug" with a five-star rating. The author is Michael Howard. The article text begins with "A core tenet of the SDL is to take and incorporate lessons learned when we issue a security update, and there is a great deal to learn from the recent animated cursor bug, [MS07-017](#), so I want to spend a few minutes to go over some of the things we have learned from this bug." The browser status bar at the bottom shows "Done", "Internet | Protected Mode: On", and "100%".

The Security Development Lifecycle

Welcome to MSDN Blogs [Sign in](#) | [Join](#) | [Help](#)

HOME EMAIL RSS 2.0 ATOM 1.0

Recent Posts

- [SDL Training at the Microsoft Security Response and Safety Summit](#)
- [The Making of a Privacy Savvy Test Team](#)
- [Oil Change or Culture Change?](#)
- [Testing in the SDL](#)
- [Blue Hat 5.0](#)

Tags

Lessons learned from the Animated Cursor Security Bug ★★★★★

Michael Howard here.

A core tenet of the SDL is to take and incorporate lessons learned when we issue a security update, and there is a great deal to learn from the recent animated cursor bug, [MS07-017](#), so I want to spend a few minutes to go over some of the things we have learned from this bug.

Done Internet | Protected Mode: On 100%

Sasser

(LSASS logging issue)

Fixed	April 13, 2004	MS04-011
Exploited	April 30, 2004	

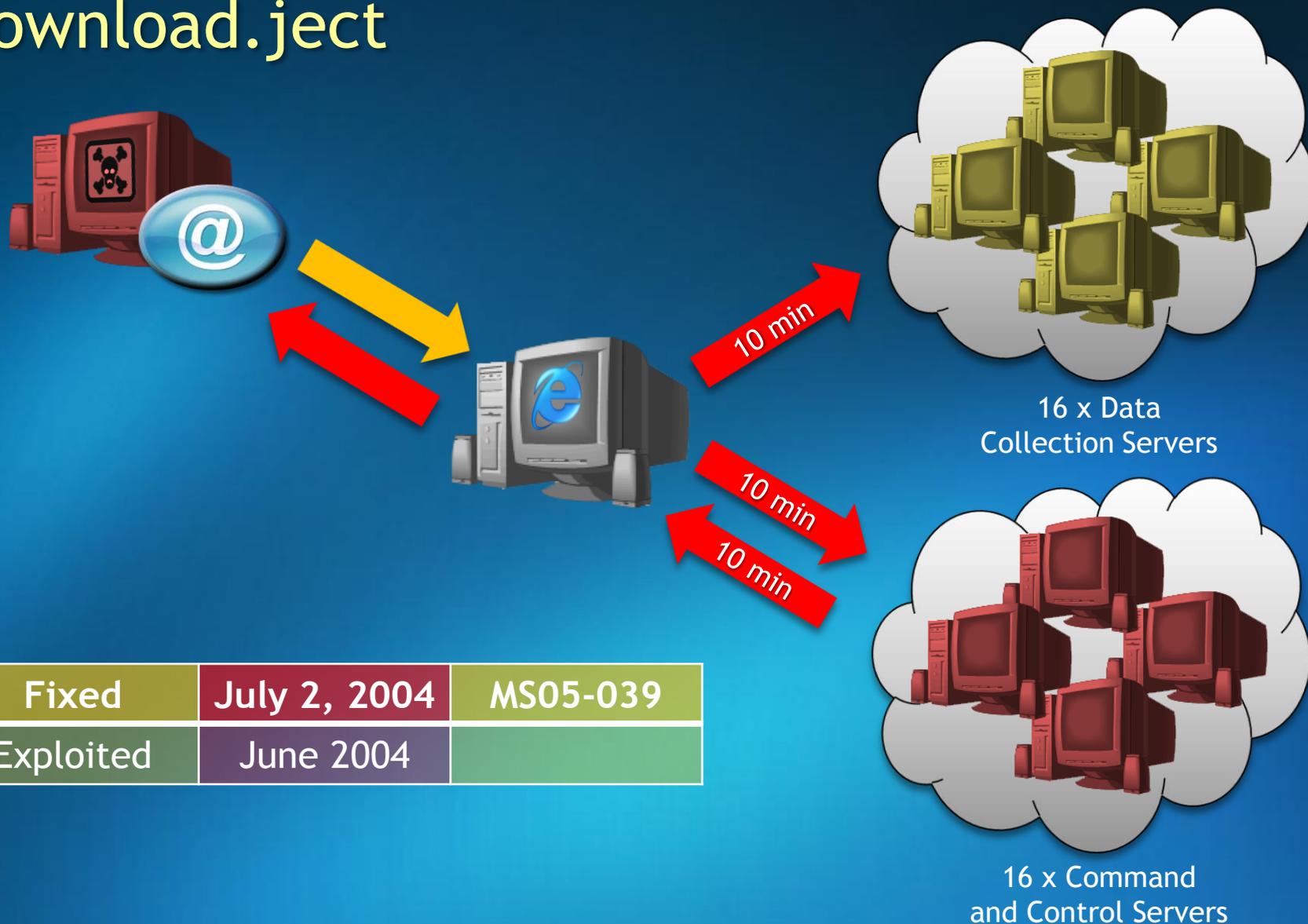
The screenshot shows a Windows Internet Explorer browser window displaying a Microsoft PressPass article. The address bar shows the URL: <https://www.microsoft.com/presspass/press/2004/may04/05-08SasserTelePR.m>. The page title is "Microsoft Reward Program Helps Lead to Information Resulting in Arrest Related to Sasser Intern". The article content includes the following text:

Redmond, Wash., May 8, 2004 — Microsoft Corp. today commended German law enforcement for its prompt arrest relating to the Sasser worm and confirmed that the company's anti-virus reward program investigators had worked with informants on the case during the past week. German authorities

The page also features a "Related Links" section with a link to a transcript by Brad Smith.

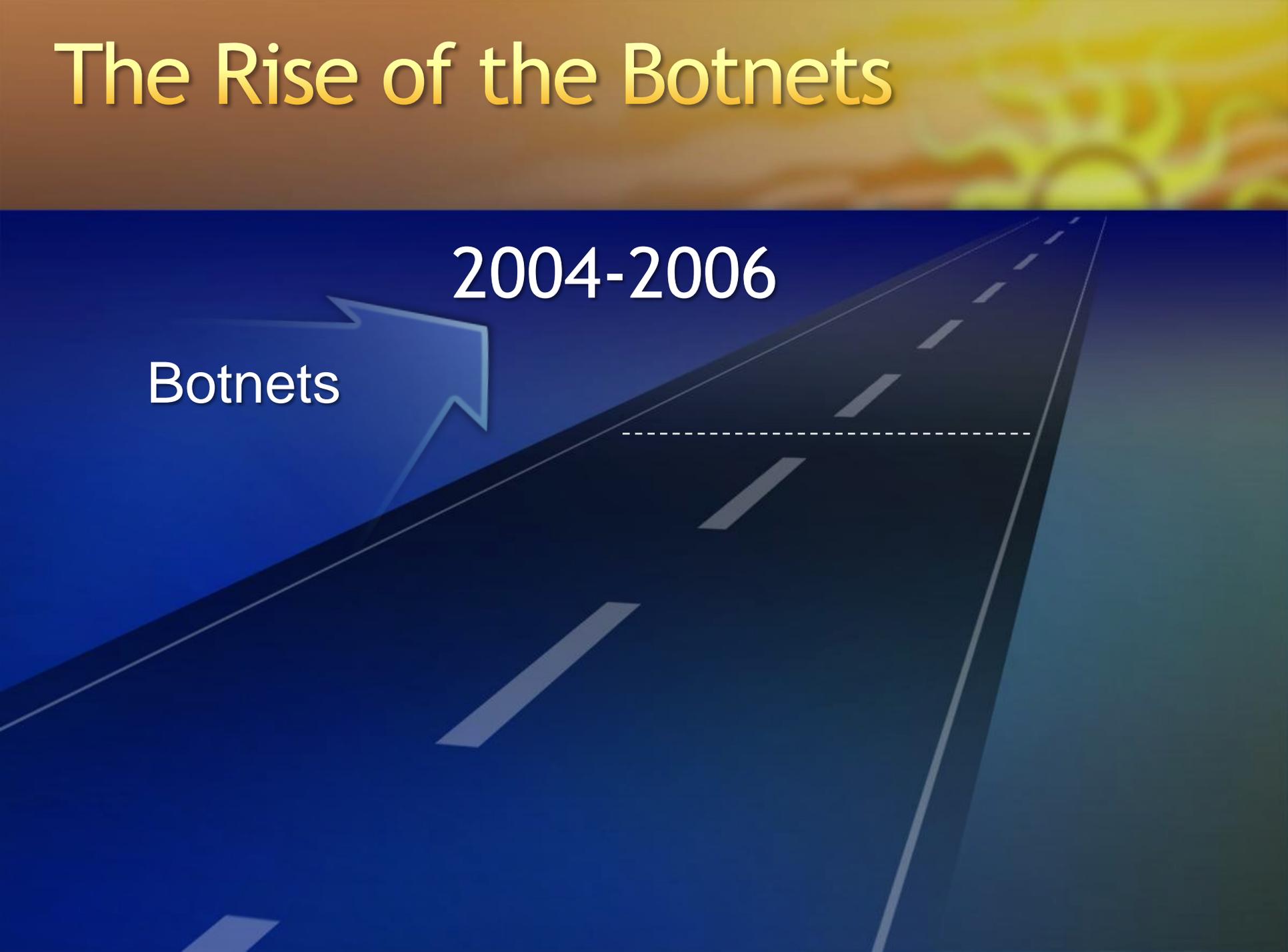
Transitional Event: C&C

Download.ject



Fixed	July 2, 2004	MS05-039
Exploited	June 2004	

The Rise of the Botnets

The image features a perspective view of a dark blue road with white dashed lines, receding towards a bright yellow and orange sunset in the upper right corner. A large blue arrow points from the left towards the center of the road. The text 'Botnets' is written in white on the left side of the arrow. Above the arrow, the years '2004-2006' are written in white. A horizontal dashed white line is drawn across the road, positioned below the years.

2004-2006

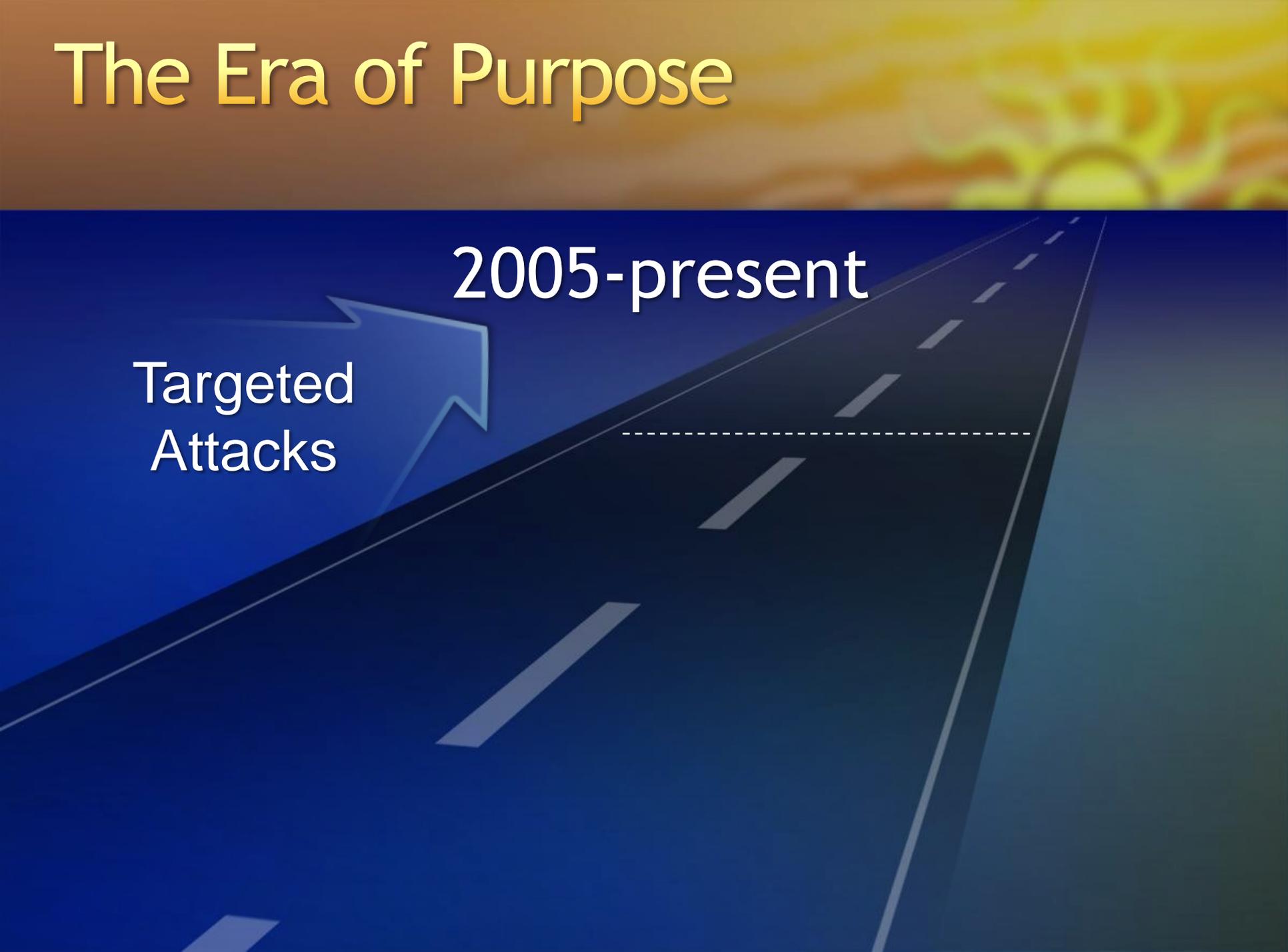
Botnets

Zotob

(Plug and play issue in Win2000)

Fixed	August 9, 2005	MS05-039
Exploited	August 15,2005	

The Era of Purpose



2005-present

Targeted
Attacks

Security Market Forces

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



Escalation and Focus

- What if the organization had
 - Significant resources
 - Intuitional 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.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.