Win32/Msblast: A Case Study from Microsoft's Perspective

Matthew Braverman

Program Manager

Microsoft Corporation

mattbrav@microsoft.com

Win32/Msblast & Win32/Sasser: Overview

	Msblast	Sasser	Advantage
Vulnerability Type	Critical	Critical	Tie
Operating Systems Affected	Windows 2000/XP	Windows 2000/XP	Tie
Time from Vuln to Worm Release	26 days	18 days	Sasser

Microsoft identified over 20 times as many Msblast infections as Sasser infections !

Questions

- Why less Sasser infections ?
- What is the source of the data ?
- How prevalent are Msblast / Sasser today ?

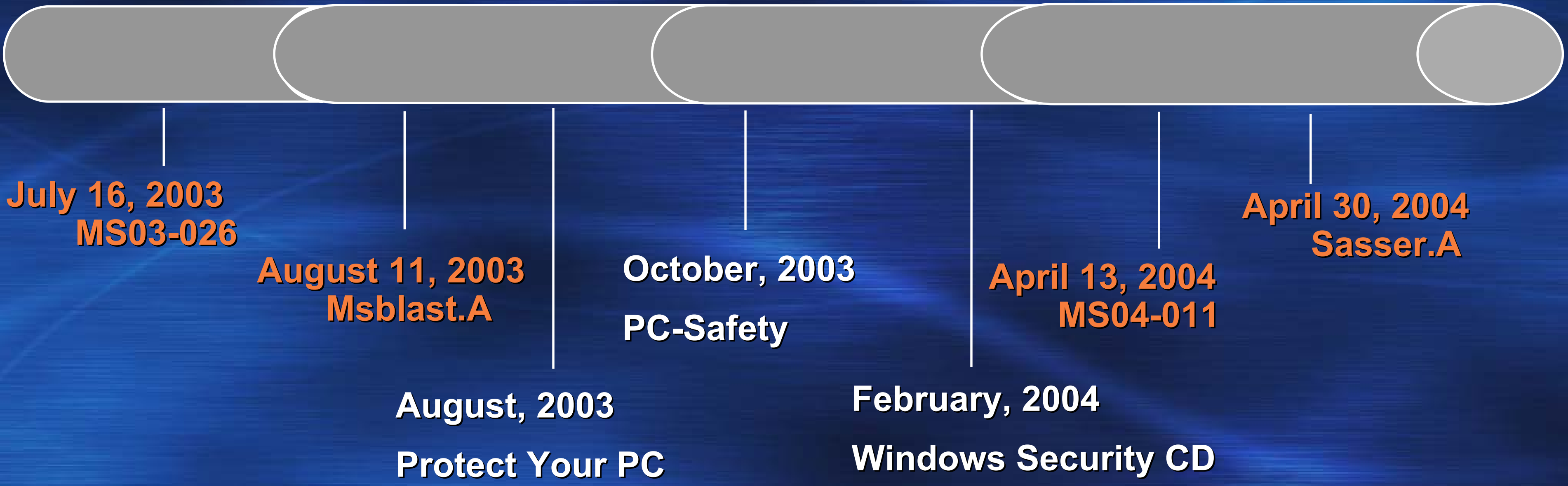
Why Less Sasser Infections ?

Msblast was a wake-up call to the world . . .

- General Security Awareness
- Security Patch Installs
- Wide Cleaner Tool Distribution

Why Less Sasser Infections ?

General Security Awareness



July 16, 2003
MS03-026

August 11, 2003
Msblast.A

August, 2003

Protect Your PC

October, 2003

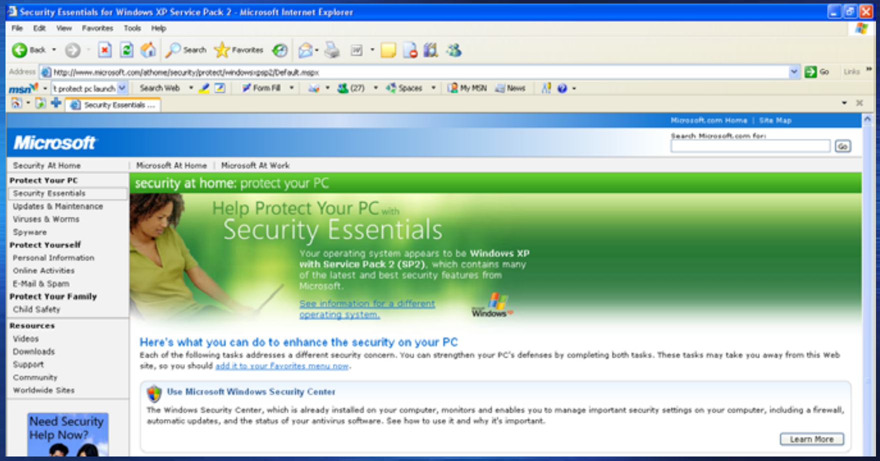
PC-Safety

February, 2004

Windows Security CD

April 13, 2004
MS04-011

April 30, 2004
Sasser.A



Security Essentials for Windows XP Service Pack 2 - Microsoft Internet Explorer

Address http://www.microsoft.com/athome/security/protect/windowsxpsp2/Default.mspx

security at home: protect your PC

Help Protect Your PC with Security Essentials

Your operating system appears to be **Windows XP with Service Pack 2 (SP2)**, which contains many of the latest and best security features from Microsoft.

See information for a different operating system.

Here's what you can do to enhance the security on your PC

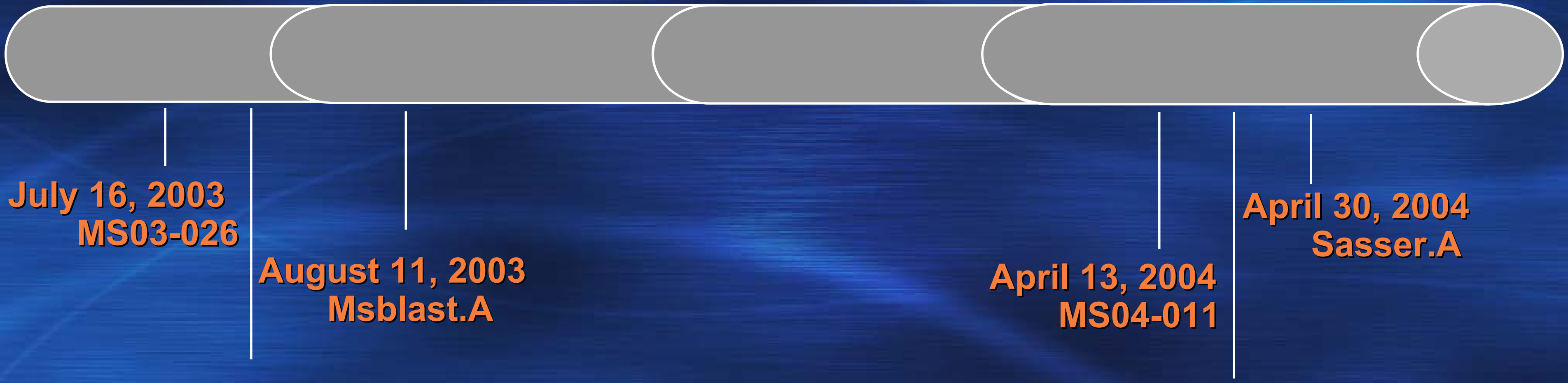
Each of the following tasks addresses a different security concern. You can strengthen your PC's defenses by completing both tasks. These tasks may take you away from this Web site, so you should add it to your Favorites menu now.

Use Microsoft Windows Security Center

The Windows Security Center, which is already installed on your computer, monitors and enables you to manage important security settings on your computer, including a firewall, automatic updates, and the status of your antivirus software. See how to use it and why it's important.

Why Less Sasser Infections ?

Security Patch Installs



July 16, 2003
MS03-026

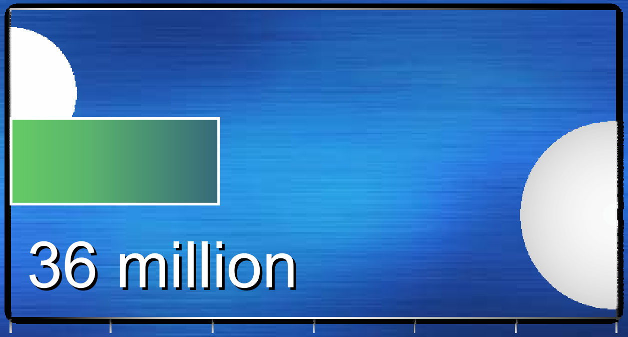
August 11, 2003
Msblast.A

April 13, 2004
MS04-011

April 30, 2004
Sasser.A

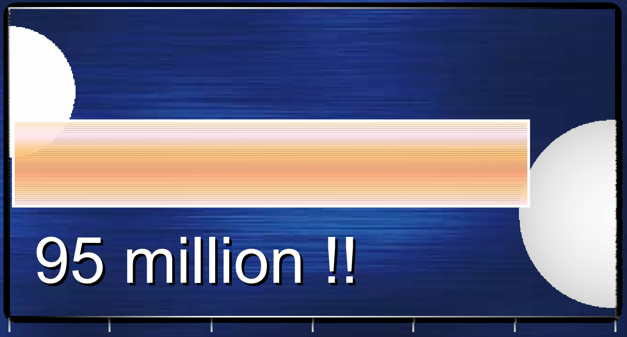
July 23, 2003

MS 03-026 Downloads



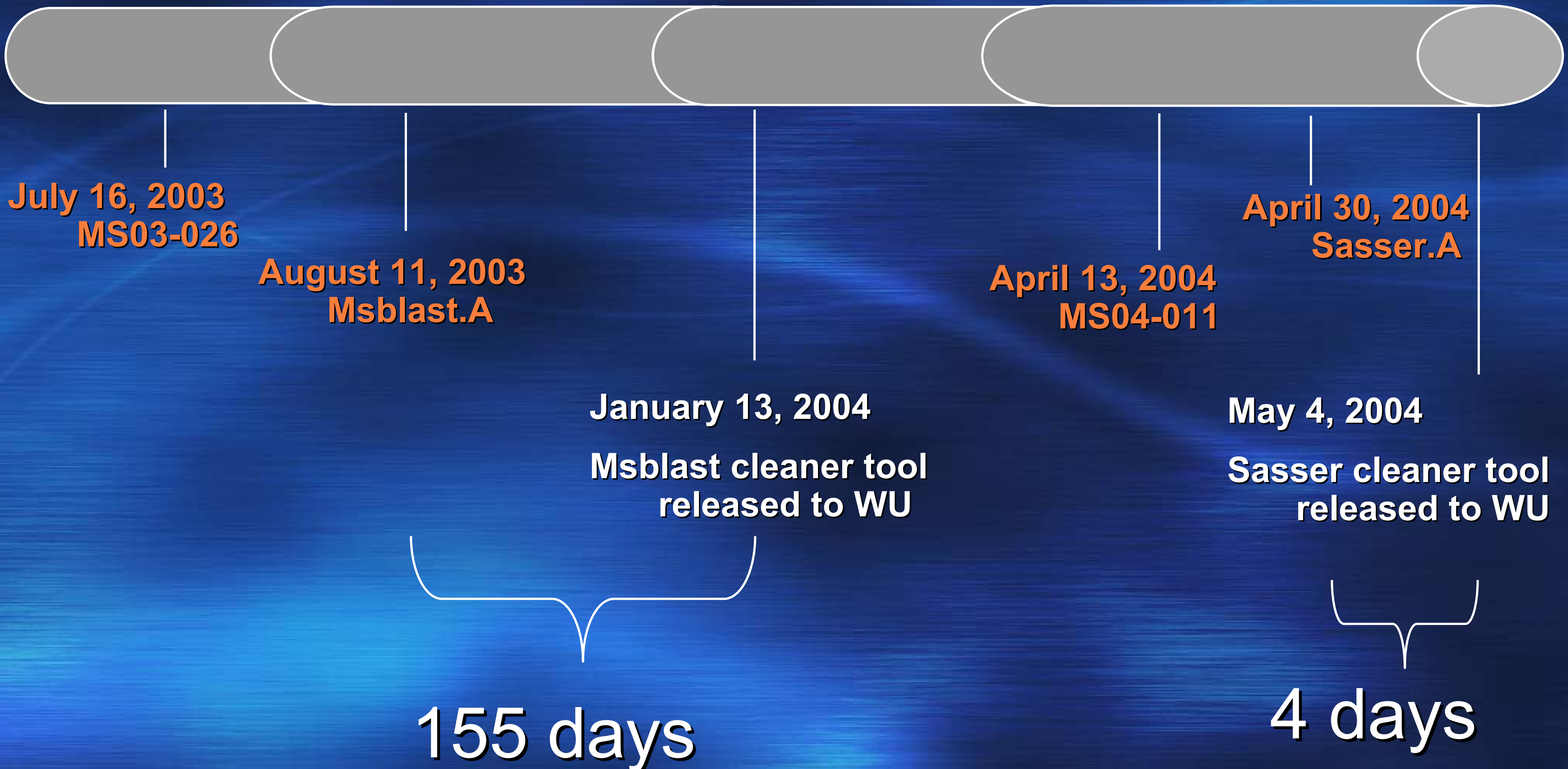
April 20, 2004

MS04-011 Downloads



Why Less Sasser Infections ?

Wide Cleaner Tool Distribution



July 16, 2003
MS03-026

August 11, 2003
Msblast.A

January 13, 2004

Msblast cleaner tool
released to WU

155 days

April 13, 2004
MS04-011

April 30, 2004
Sasser.A

May 4, 2004

Sasser cleaner tool
released to WU

4 days

Questions

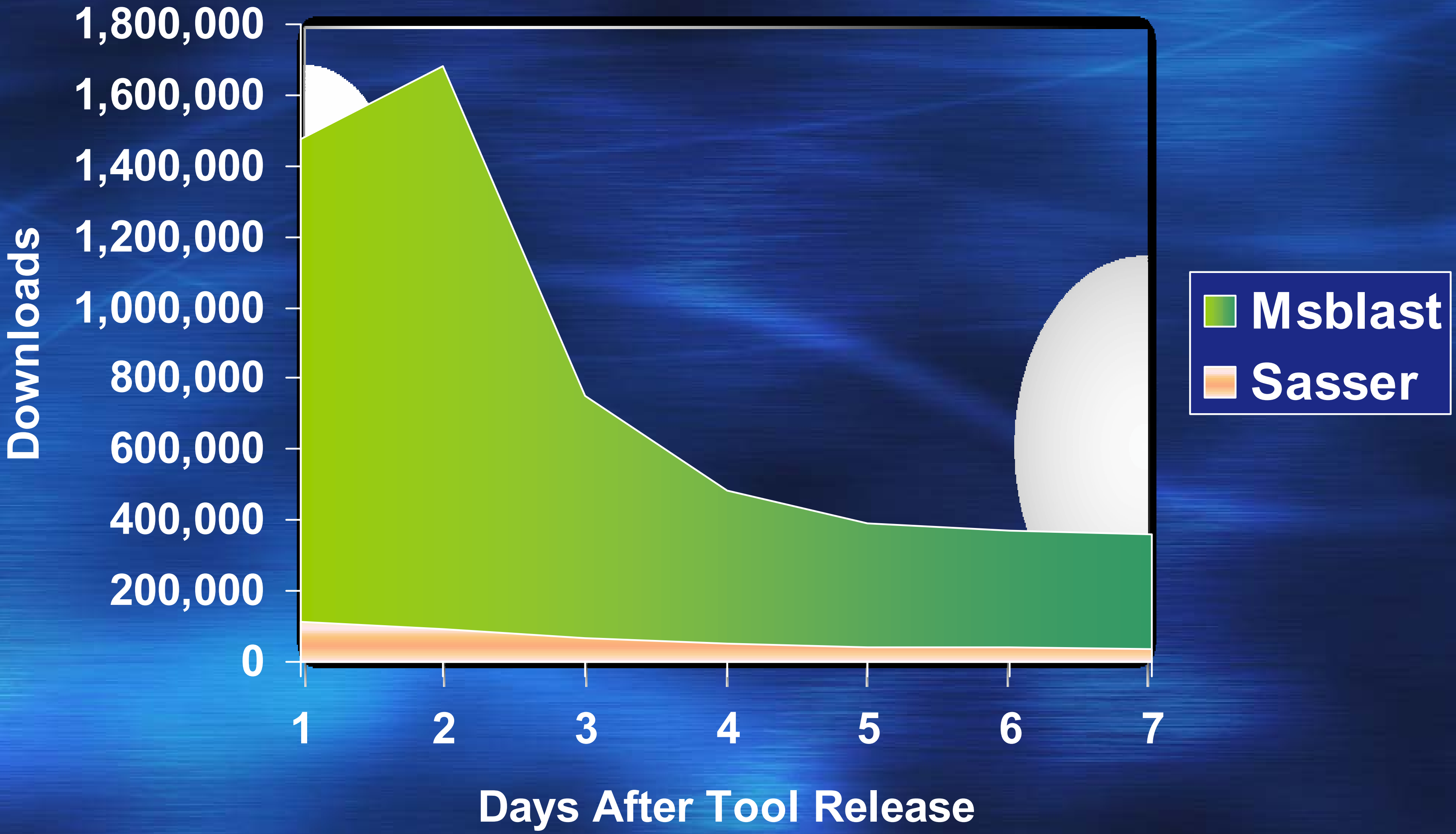
- Why less Sasser infections ?
- What is the source of the data ?
- How prevalent are Msblast / Sasser today ?

What is the source of the data ?
Overview

- Msblast / Sasser cleaner tools delivered through several mechanisms
  - Windows Update (WU) / Automatic Updates (AU)
  - Microsoft Download Center
  - ActiveX (Sasser cleaner only)
- Through WU / AU, only likely-infected users were offered the tools
- Download figures closely translate into infections

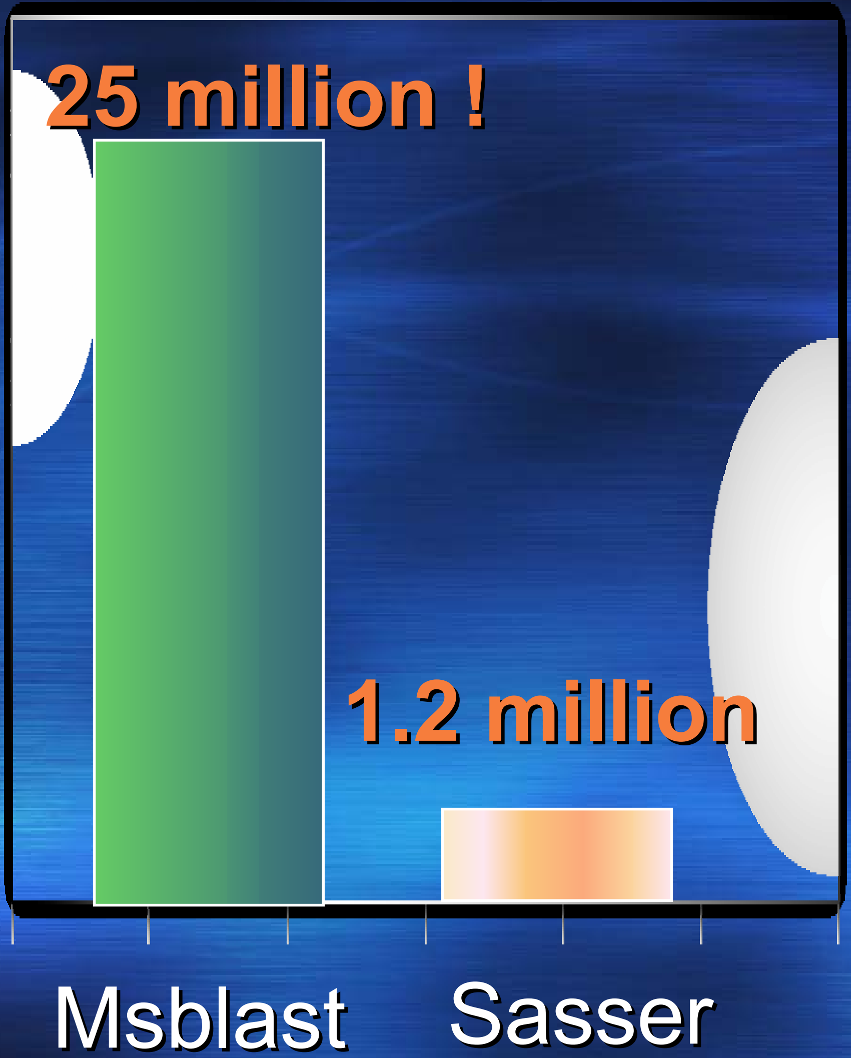
What is the source of the data ?

After 7 days . . .

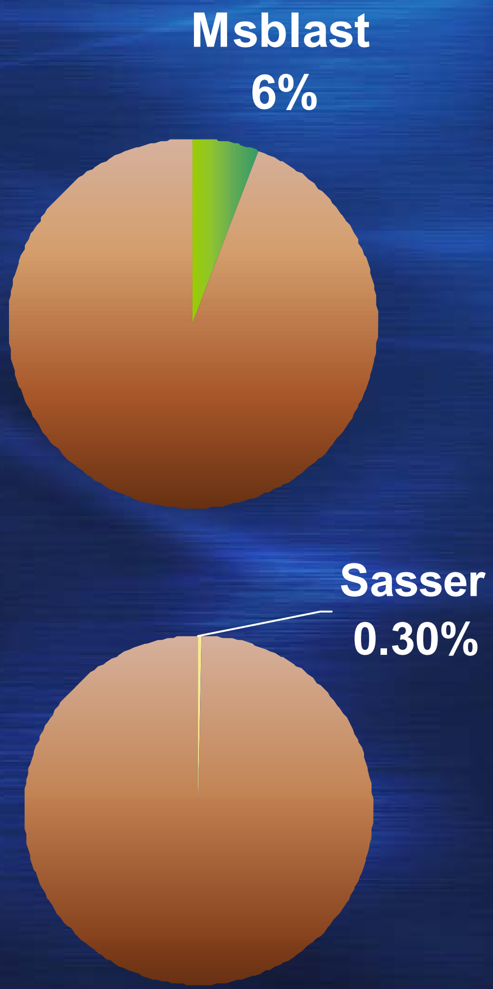


What is the source of the data ?

After 6 months . . .



Infection Percentages



Questions

- Why less Sasser infections ?
- What is the source of the data ?
- How prevalent are Msblast / Sasser today ?

How prevalent are Msblast / Sasser today ?

Background

- First version of Windows Malicious Software Removal Tool released on January 13, 2005
  - Offered to all Windows 2000, XP, and Server 2003 computers via WU / MU / AU
  - Removed Msblast, Sasser, and six other prevalent malware families
- Now released monthly on “Patch Tuesday”
- Current version removes 37 families
  - Over 1 billion total executions since January
  - Covers over 80% of malware on the Wildlist
- Not a replacement for an antivirus product

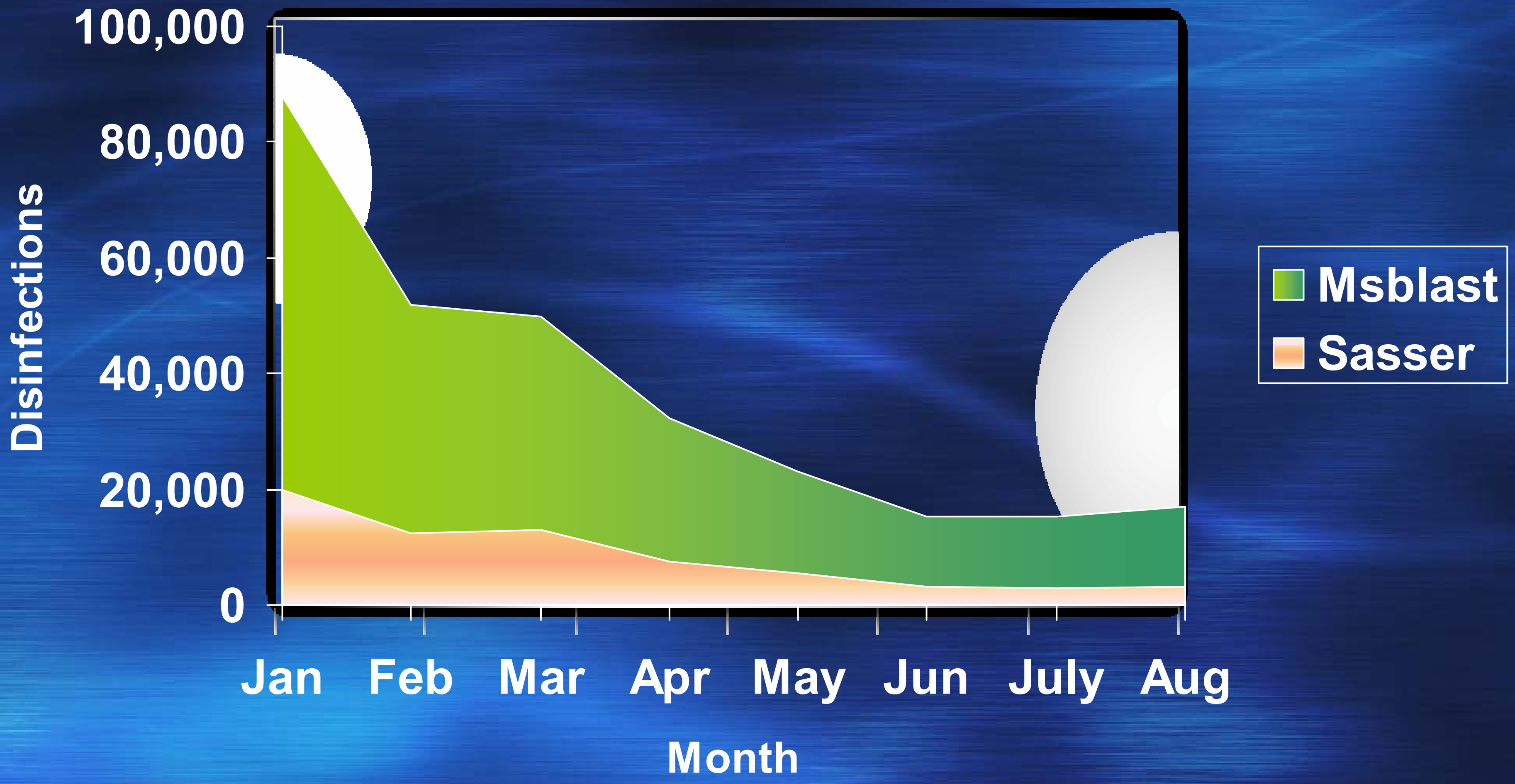
How prevalent are Msblast / Sasser today ?

After 9 months …

Rank	Malware Family
1	Rbot
2	Sdbot
3	Gaobot
4	Netsky
5	Msblast
6	Ispro
7	Korgo
8	FURootkit
9	Berbew
10	Bagle
11	Spybot
12	Mytob
13	Wootbot
14	Sasser
15	Bropia

How prevalent are Msblast / Sasser today ?

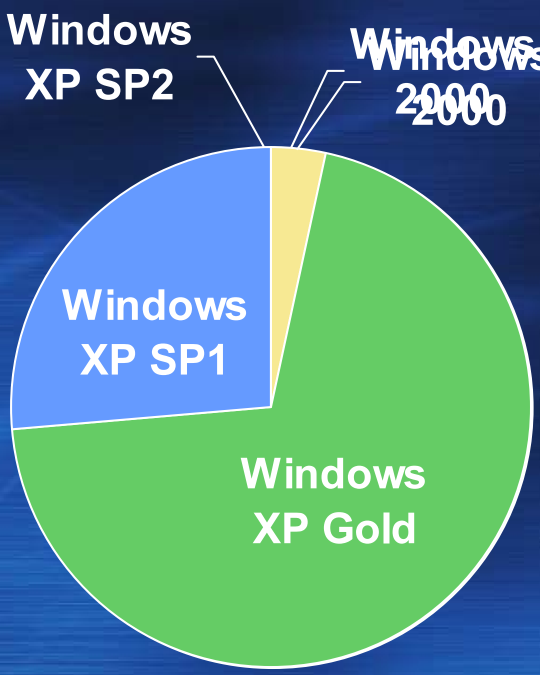
Over 9 months …



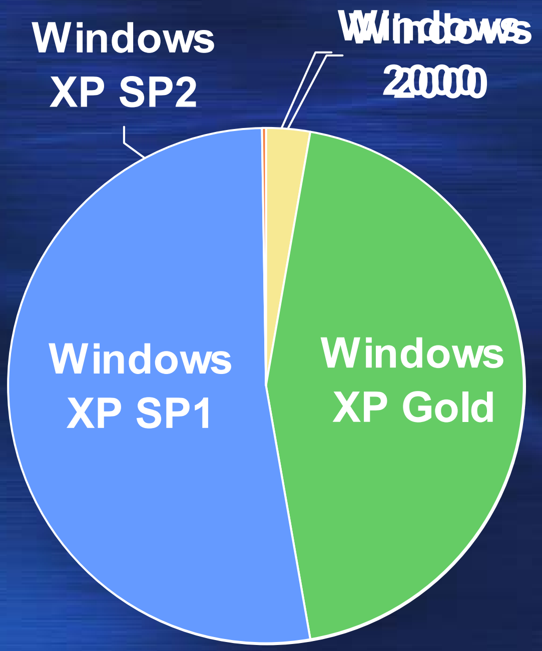
How prevalent are Msblast / Sasser today ?

After 9 months … by operating system

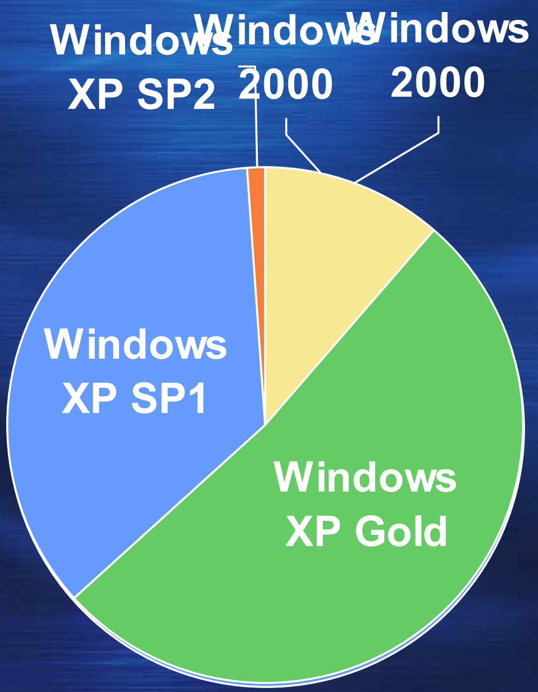
Msblast



Sasser



All Families



The Windows Malicious Software Removal Tool is significantly less likely to remove malware from a Windows XP SP2 system

$$\text{Normalized Infections}_{\text{malware, OS}} = \frac{\text{Distribution}_{\text{malware, OS}}}{\text{Execution Percentage}_{\text{OS}}}$$

Conclusions

- Malware is evolving …
- … but so is the security ecosystem
  - Heightened awareness
  - Faster patch distribution / installation
  - Increased usage of anti-malware products and tools
  - Wide distribution of a cleaner tool for highly prevalent threats
- For more detailed disinfection statistics, be sure to check out Jason Garms' presentation at AVAR 2005 !

Thank you !

- Questions ?

Microsoft®

Your potential. Our passion.™

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.