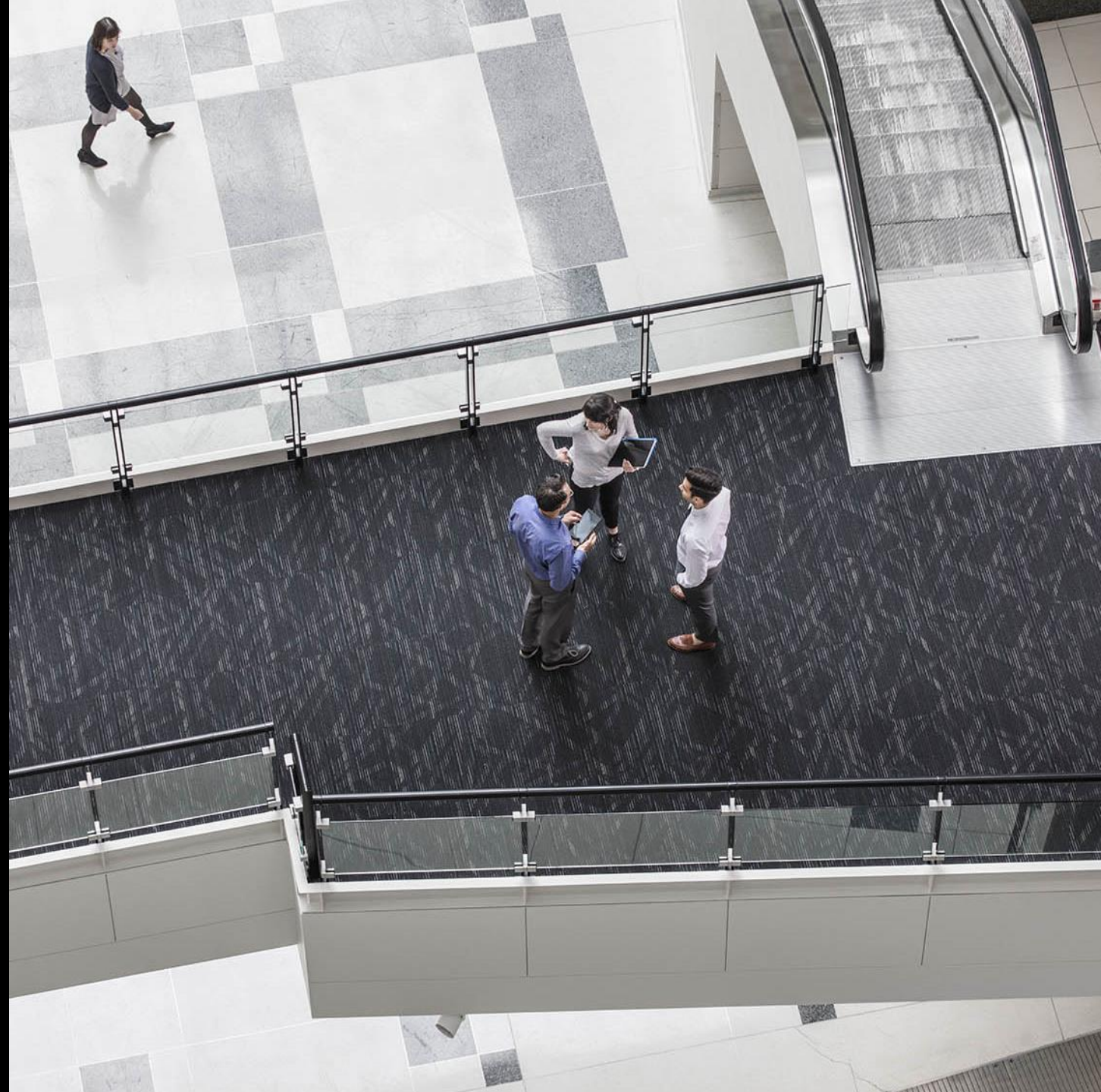
Microsoft

MS08-067 – Incident Retrospect

Ziv Mador, TrustWave
Dustin Childs, Trend Micro
Phillip Misner, Microsoft



MS08-067 (CVE-2008-4250)

- Vulnerability found in Windows Server Service (netapi32.dll)
- Server service did not handle specially crafted RPC requests
- Triaged as remote unauthenticated code execution at system privileges on XP/Sever 2003
  - Wormable (no user interaction required, self-replicating)
  - Large install base
  - Exploit known; widespread malware probable
  - Bulletin Severity: Critical
  - Security Impact: Remote Code Execution
  - Exploitability Index Rating: 1 – Consistent Exploit Code Likely

Comparing Incidents

	Blaster (August 2003)	Sasser (April 2004)	Zotob (August 2005)	Conficker.B (December 2008)
Alert & Prescriptive Guidance	Within 1 day	Within 2 hours	2 days prior	Before publicly known (MAPP)
Online Guidance/ Webcast	Within 10 days	Within 2 days	Same day	69 days prior (3 offered)
Free Worm Removal Tool	Within 38 days	Within 3 days	Within 3 days	Within 16 days*
# of systems updated in the 1st week	36 million	95 million	127 million	409 million
Days after the patch we knew of 1st exploit	+11 days	+4 days	+2 days	-11 days
Products not affected by exploits	None	None	XPSP2	Vista, Svr 2008

* initial outbreak did not require an out-of-band release of Malicious Software Removal Tool

MS08-067 Response Timeline

Watch
Mon, Oct 6th

- Watch triggers indicate a previously unknown vulnerability is being exploited in the wild
- Immediate escalation to SSIRP team

Alert & Mobilize
Mon, Oct 6th

- MSRC declares new SSIRP in response to customer reports
- Immediate mobilization of our SSIRP Team and First Responders

Assess
Oct 6th – 10th

- Immediately began monitoring for customer impact
- Product team begins investigation
- Variant testing begins
- Work around and mitigation planning occurs
- Plan of Record established (10/10) and attached to November release cycle

Stabilize
Oct 10th –Oct 22nd

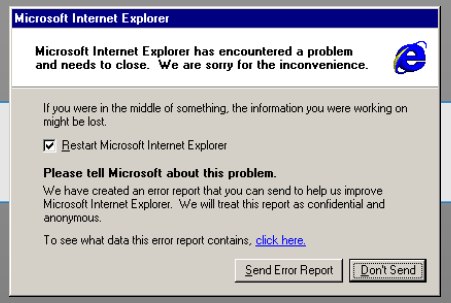
- Product team creates fix packages and testing begins
- Fri, 10/17 – Reports indicate growing threat; Threat level raised to Red
- All teams raise to high alert and engineering plan is accelerated
- Tues, 10/21 – Quality bars met giving the ability to release early
- Wed, 10/22 – Began field & partner outreach
- Wed, 10/22 – Advanced Notification for out-of-band release on 10/23

Resolve
Oct 23rd -Cont…

- Thurs– 10AM –all materials release publicly
  - Security Bulletin, MBSA, SMS, WSUS, Windows Update, Automatic Update, Microsoft Update, MAPP
- Thurs – PR engagement begins aggressive messaging to customers
- Continued monitoring of the threat landscape

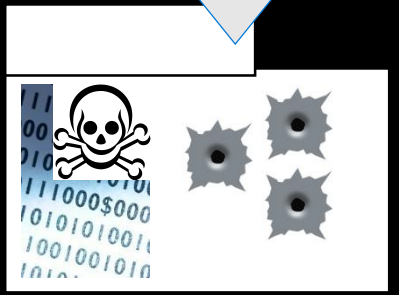
Crashes Feed Telemetry

Victim PC
- Agent built into Windows
- Victim sends crash report



Company.com
Corporate Error
Reporting

Watson Servers

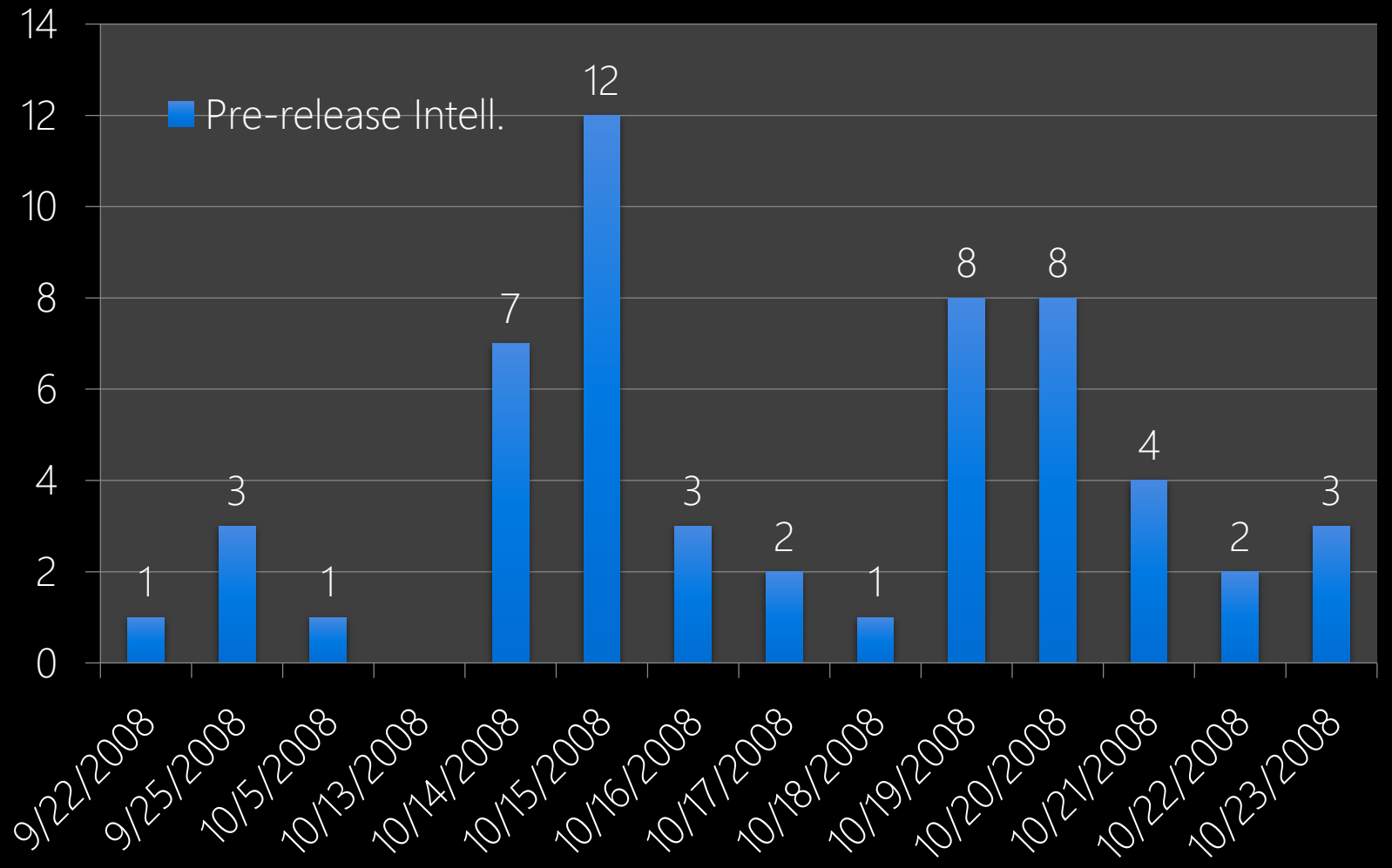


- exploit code
- hijacks

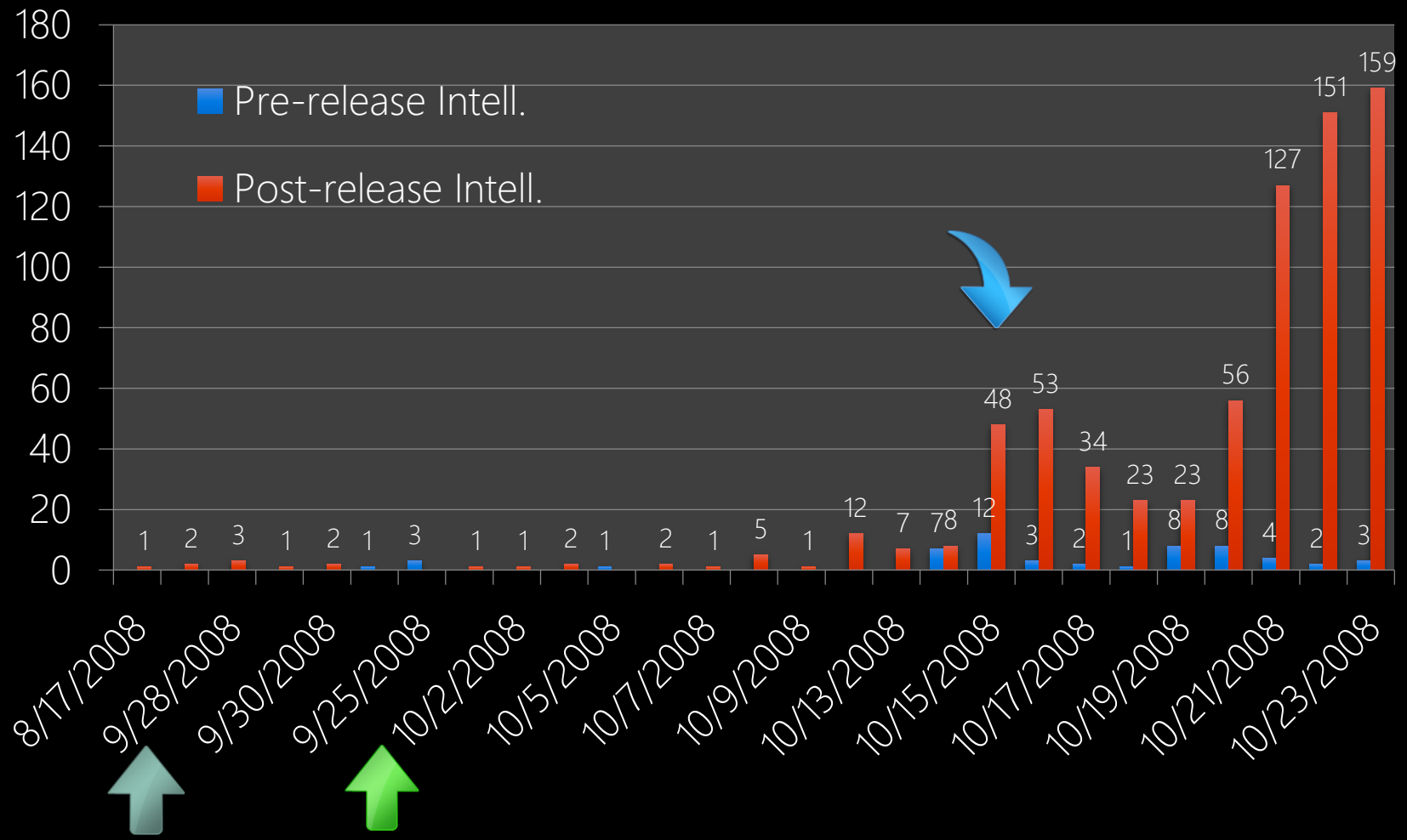
Resolving the Vulnerability

- Resolved by Out-of-Band release as MS08-067 (Critical)
- Security update resolves a privately reported vulnerability in the Server service
- Vulnerability could allow remote code execution if an affected system received a specially crafted RPC request
- On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code.
- It is possible that this vulnerability could be used in the crafting of a wormable exploit

Pre-Release Intelligence



Combining Intelligence



Notification of Imminent Resolution & Threat

Advance Notification for Out-of-Band Release

Posted Wednesday, October 22, 2008 8:38 PM by MSRCTEAM

Hello this is Christopher Budd,

I wanted to let you know that we've just posted an Advance Notification for an out-of-band bulletin release. We plan to release one Windows security bulletin with a maximum severity of Critical; scheduled for a target time of 10:00 a.m. PT on Thursday Oct. 23, 2008. A restart will be required.

We have scheduled a special webcast to cover this release. This will also be on Thursday at 1 p.m. PT. You can register for it here.

Thanks

Christopher

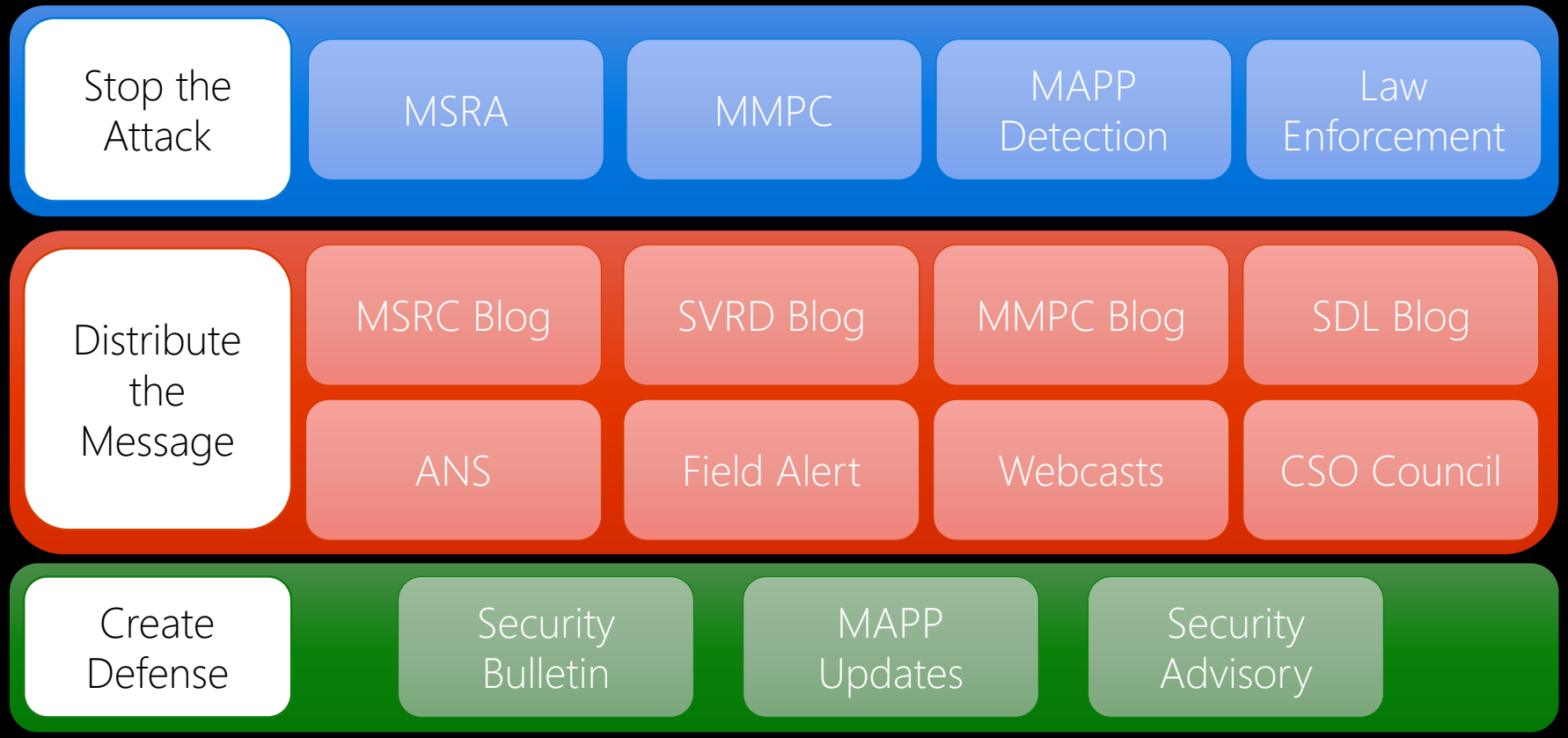
Out of Band Releases

- Out-of-Band releases reserved for the most serious vulnerabilities
  - Active or eminent exploit on a large scale
  - Active or eminent exploit on critical infrastructure

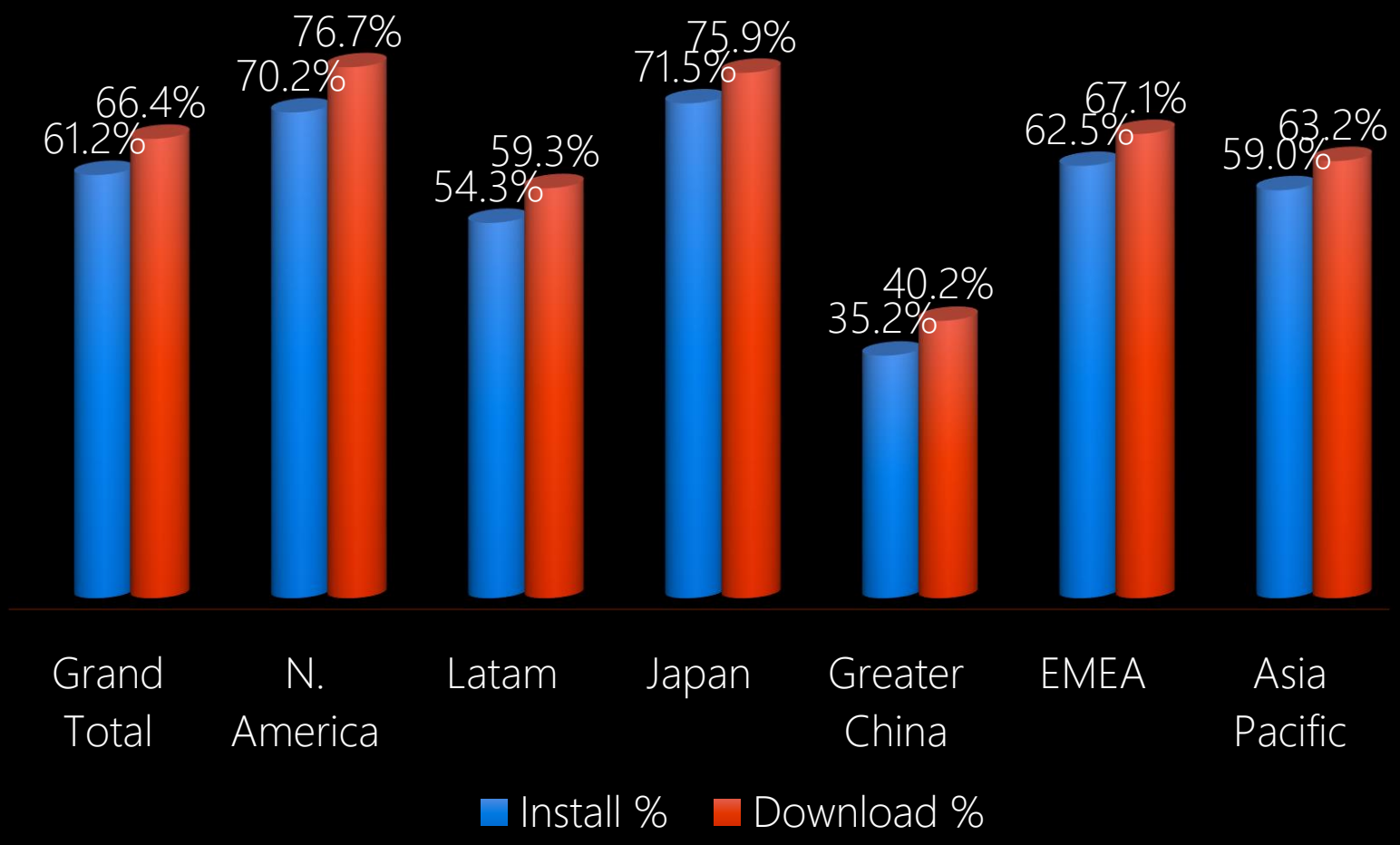
- Out-of-Band releases are costly – both to Microsoft and our customers

- MS08-067 was the ninth OOB release

Tools that Advanced Response

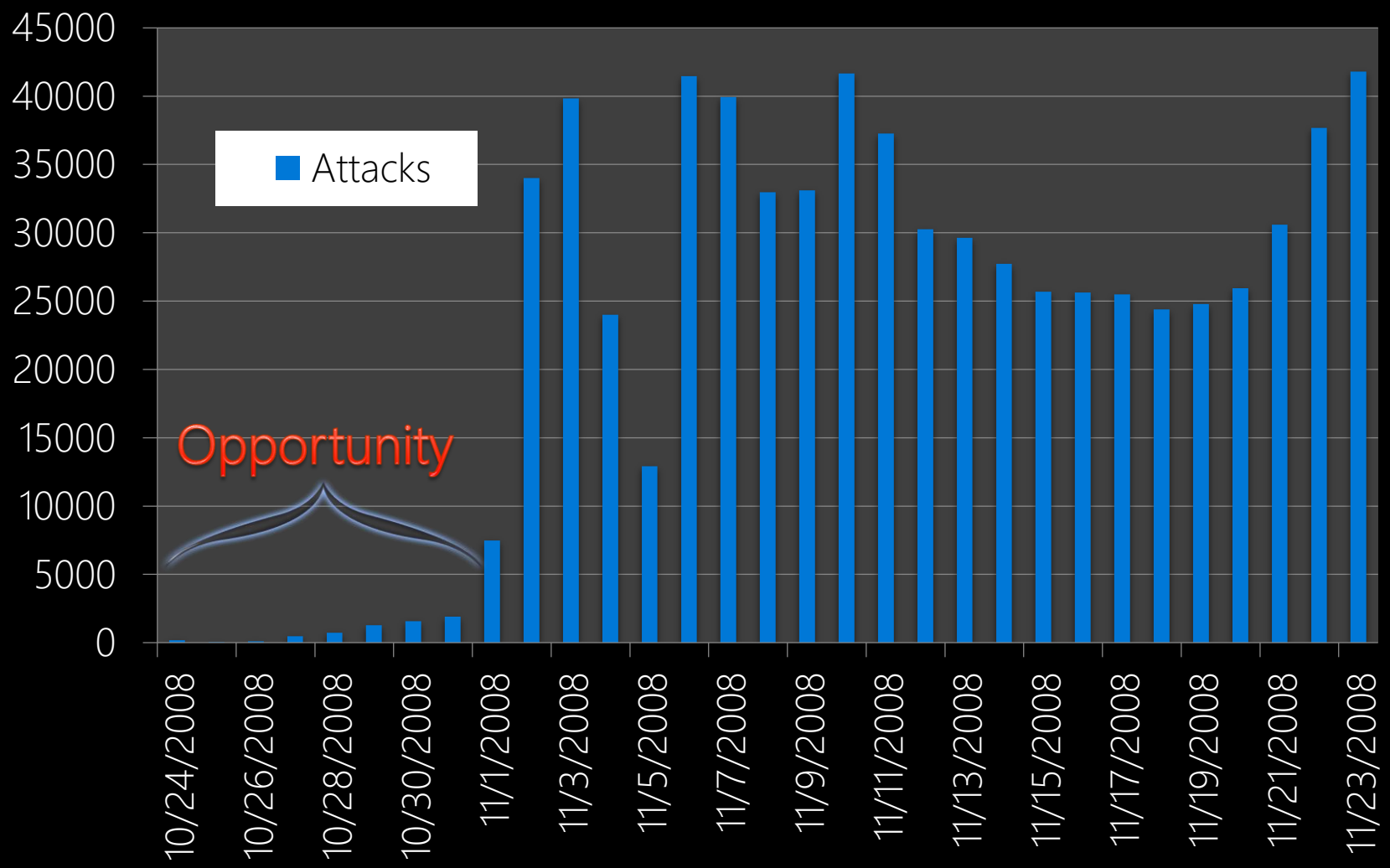


Windows Update Uptake



Regional data shows North America and Japan with the most aggressive up take. It also shows a problem in Greater China which was due to poor reception of the WGA program days earlier.

A Narrow Opportunity



Malware Evolution Timeline

Initial Attack
Aug 17th-Oct 22nd

- Exploits drop TrojanSpy:Win32/Gimmiv
  - Collects information and sends it to a server in Japan
  - A few targeted attacks: Malaysia, Japan, Philippines, Vietnam & Singapore

Bulletin Release
Oct 23rd

- Published a generic signature for the current exploits: Exploit:Win32/MS08067.gen!A
- Added detection to MSRT November and to Windows Defender

Attackers Join In
Oct 24th – Nov 20th

- Shortly after release researchers release new malware – none that self replicate
  - TrojanSpy:Win32/Arpoc
  - Trojan:Win32/Wecorl (The Symantec "worm")
  - Trojan:Win32/Clort

1st Worm
Nov 21st – Dec 28th

- Nearly a month after release, the first worm is detected: Win32.Conficker.A
  - Attacks unpatched systems only
  - Success rates were fairly low

Prevalent Worm
Dec 29th – Cont…

- Over two months after release and one month after the first worm a new resilient variant is found in the wild: Win32.Conficker.B
  - Attacks unpatched systems
  - Replicates to admin$ shares with weak passwords
  - Replicates to all removable media and employs social engineering attack through AutoPlay to further replicate
- Added detection to MSRT January to remove Conficker

© Copyright Microsoft Corporation. All rights reserved.