Microsoft

A PERSPECTIVE OF THE MIDDLE EASTERN MALWARE LANDSCAPE

Tareq Saade
Microsoft Security Research & Response

Hack In The Box '07

Intro

- Tareq Saade
  - Program Manager
    Microsoft Security Research & Response
    - Design tools & technologies for malware analysis & response
    - Member of the Windows Defender product group
  - Recreational Malware Reverse Engineer
    - Particularly IRC-related threats
    - Involved with various informal groups & task forces

- tareq.saade@microsoft.com

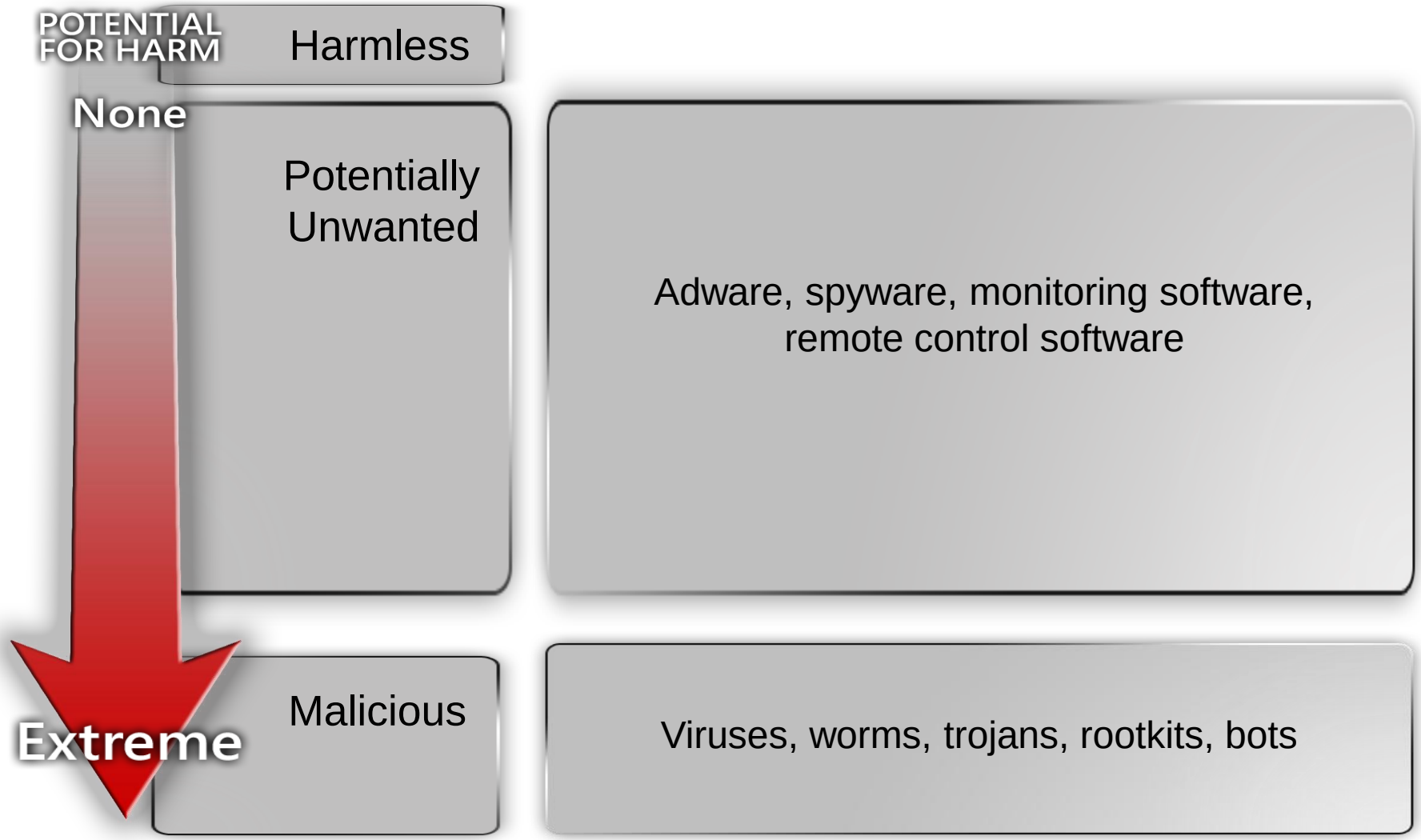
Agenda

- The scene
  - Agenda, terminology, background
- The cast
  - Technologies
- The back story
  - How data is collected
- The data
  - Telemetry & analysis
- The Finale
  - Conclusion + Q&A

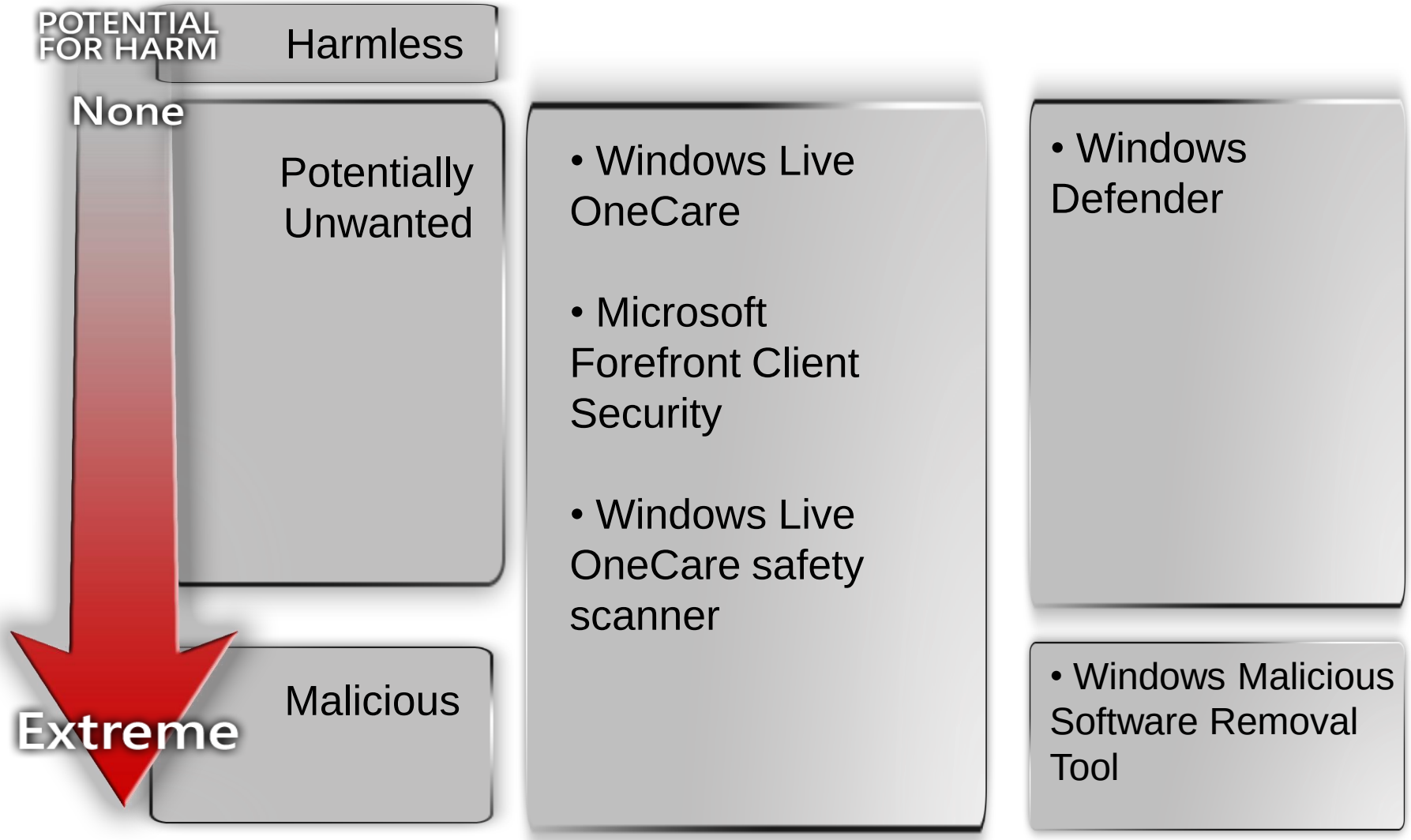
Terms & Technologies

- Gulf Cooperation Community (GCC)
  - Saudi Arabia, UAE, Kuwait, Qatar, Bahrain & Oman
- Geographic ID (GeoID)
  - OS regional identifier defined by customers
- Locale ID (LocID)
  - OS language locale
    - Useful for highly targeted data sets
    - Most people run US-EN
- Microsoft Windows Malicious Software Removal Tool (MSRT/MRT)
- Microsoft SpyNet
  - The Windows Defender component responsible for collecting telemetry
- 'Removals'
  - Removals are reports sent back by clients indicating that a particular threat or piece of unwanted software has been removed from the system
  - This is not the same as a 'detection', which indicates the presence of said software

Malware Spectrum



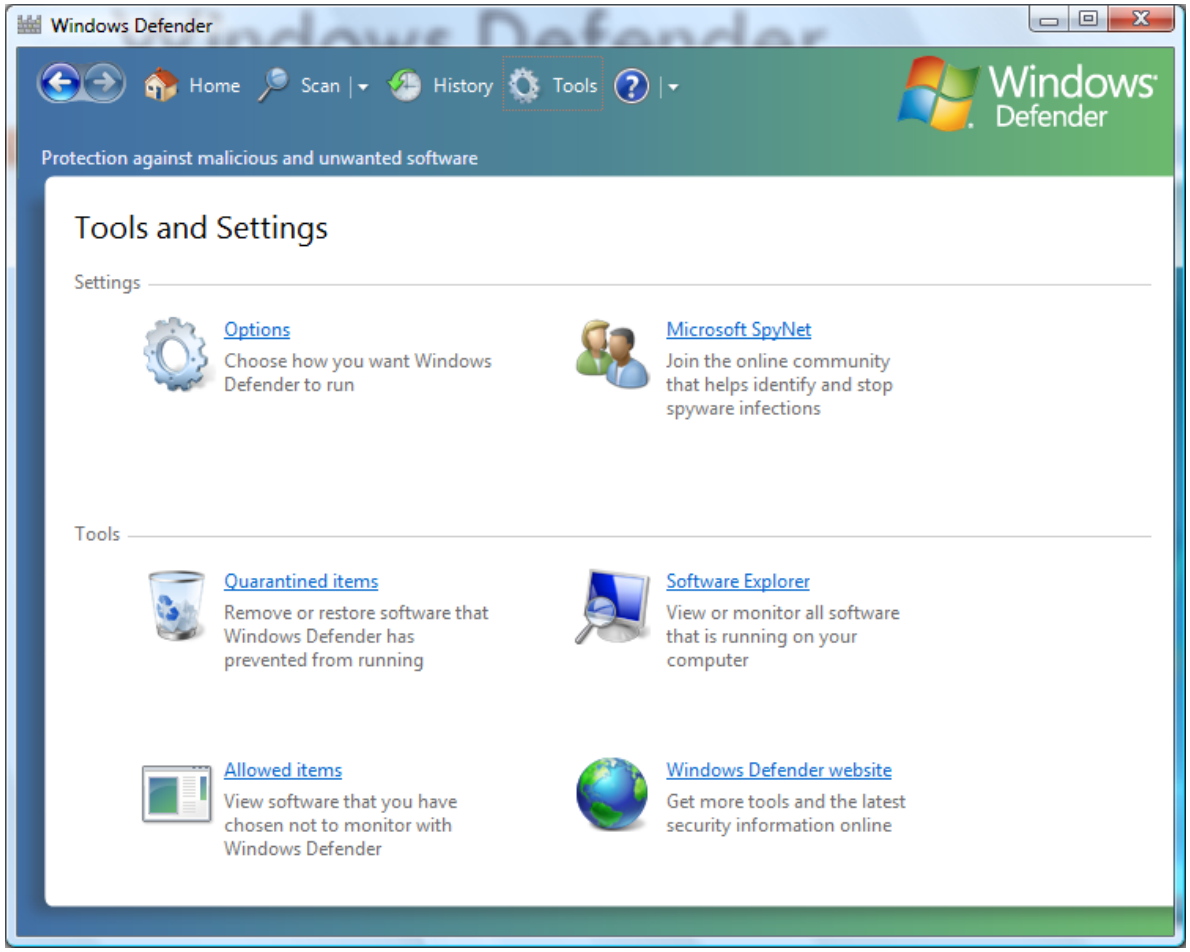
Malware Spectrum (cont.)



Products & Technologies

Product Name	Main Customer Segment		Malicious Software		Spyware and Potentially Unwanted Software		Available at No Additional Charge	Main Distribution Methods
	Consumers	Businesses	Scan and Remove	Real-Time Protection	Scan and Remove	Real-Time Protection		
Windows Malicious Software Removal Tool	•		Partial				•	WU / AU, Download Center
Windows Defender	•				•	•	•	Download Center
Windows Live OneCare Safety Scanner	•		•		•		•	Web
Windows Live OneCare	•		•	•	•	•		Web / store purchase
Microsoft ForeFront Client Security		•	•	•	•	•		Web / store purchase

Windows Defender

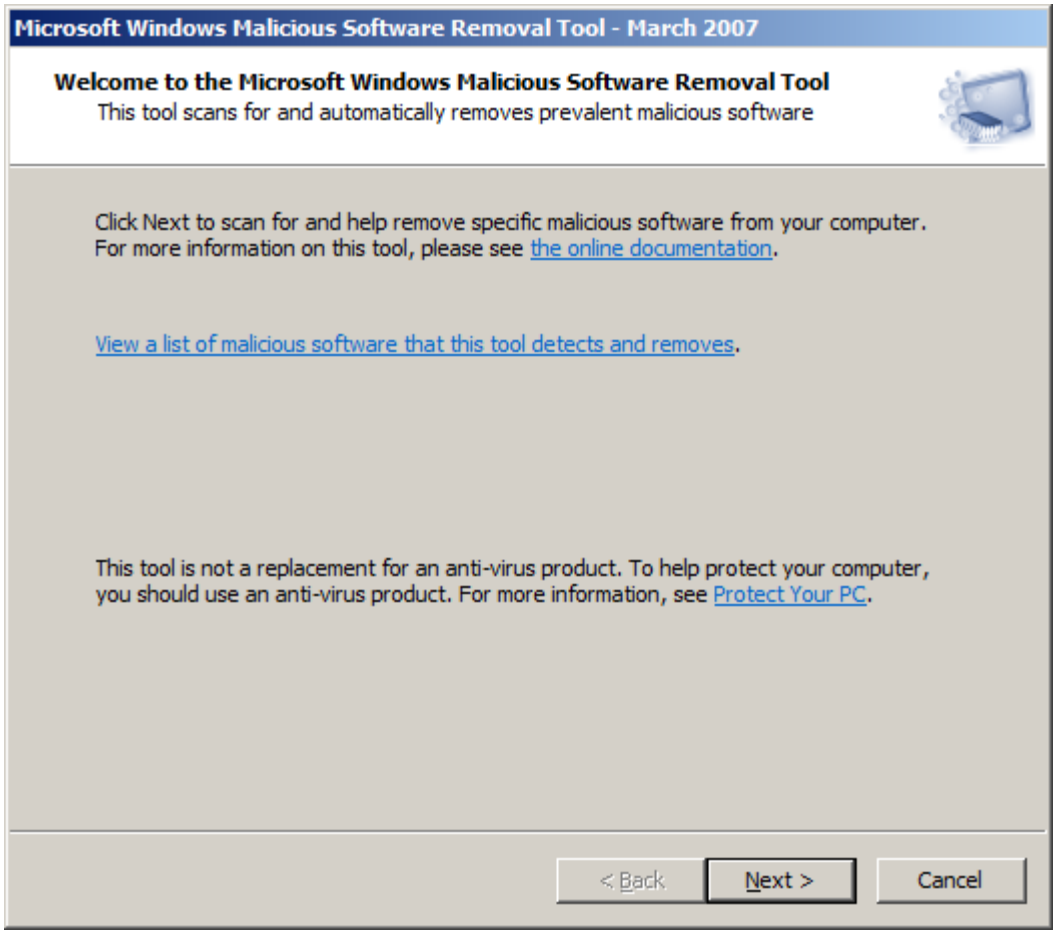


Windows Defender

Reporting

- Reports are sent when:
  - An unknown file triggers some ‘suspicious’ trigger such as writing itself to a system startup location
  - A known bad file is detected on disk
  - A known bad file is detected in memory
- Two member tiers
  - Basic
  - Advanced
  - (and ‘off’)

Malicious Software Removal Tool



Malicious Software Removal Tool

Reporting

- Reports are sent when:
  - A threat is detected
  - A threat is removed

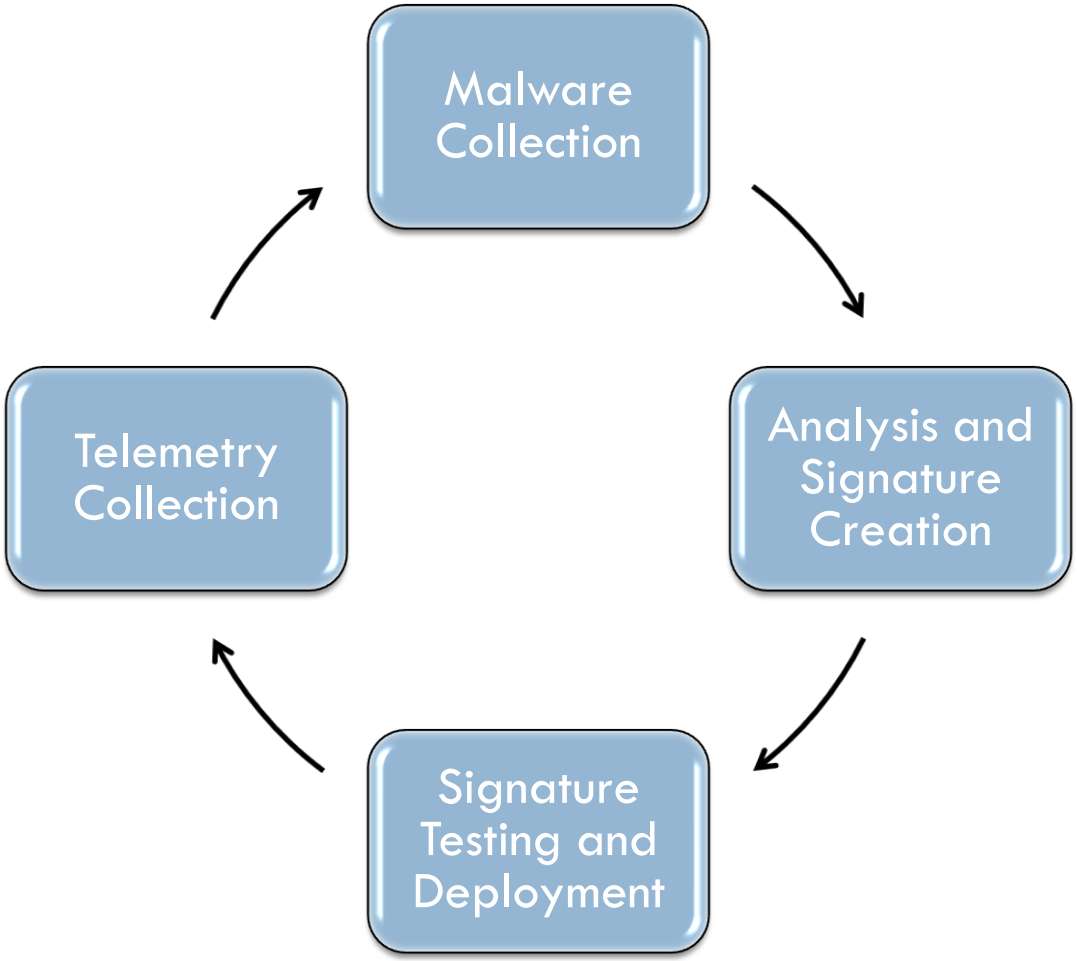
MRT Usage

- Deployed monthly via Windows Update / Automatic Updates since January 2005
- Available in 24 languages
- 5+ billion executions, 300 million unique computers
- Detection for 80+ malware families, 135k+ different variants
- Mostly targets client / consumer threats
- 300+ million downloads per month

Telemetry Collection Summary

- All telemetry reporting requires some for of user opt-in
- Read the EULA/Privacy Policy
- Data used strictly by analysts to help make determinations about software
  - Global outbreak? Localized outbreak?
- 'Controlling Communication with the Internet' for Vista & XP SP2

Anti-Malware Lifecycle



SpyNet Spyware Telemetry

Windows Defender

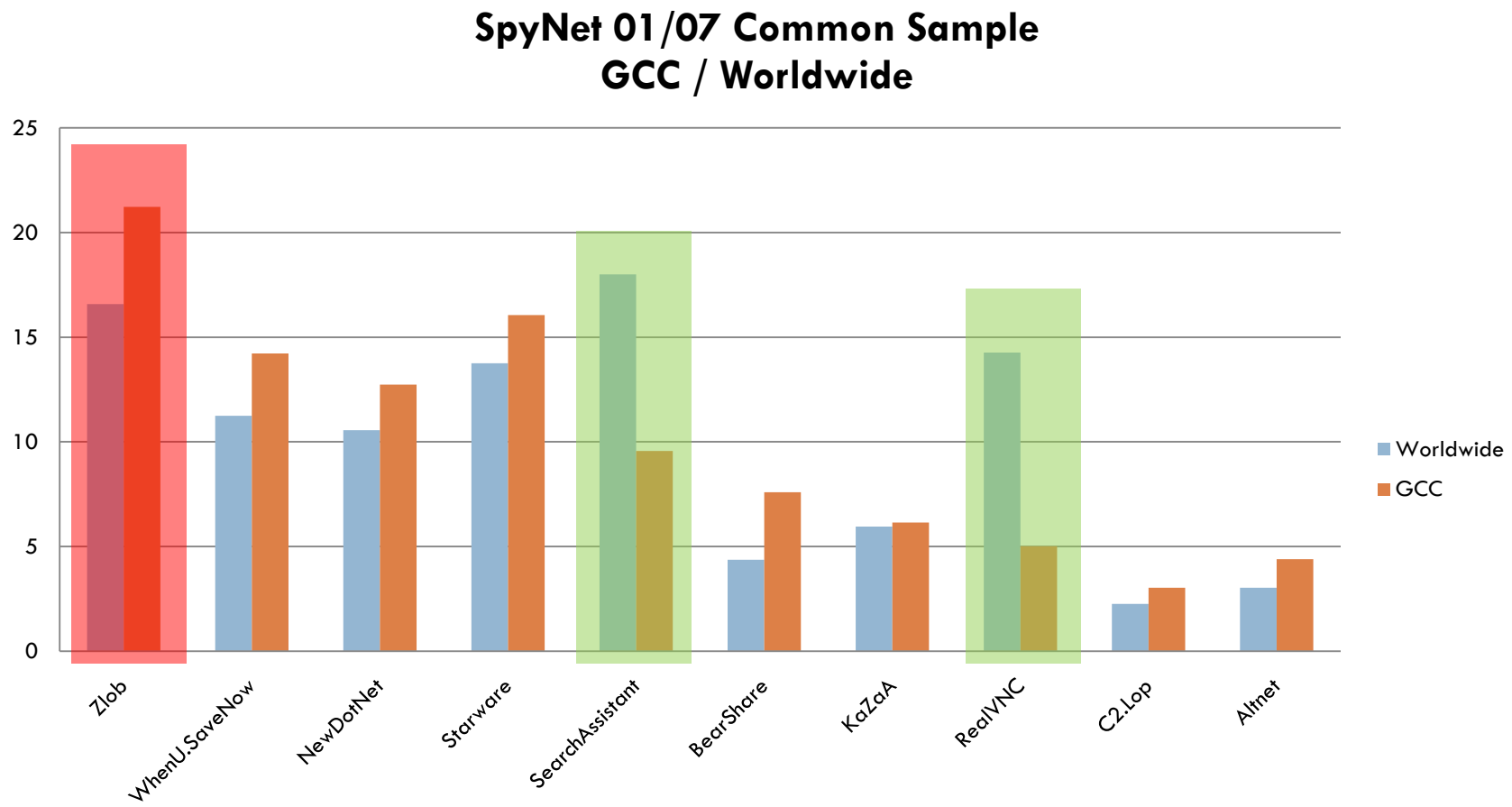
Top Removals – January 2007

Worldwide
Zlob
NewDotNet
Renos
ZangoSearchAssistant
ClickSpring.PuritySCAN
CometSystems
WhenU.SaveNow
Starware
Hotbar
TVMediaDisplay

GCC
Zlob
Starware
WhenU.SaveNow
NewDotNet
ZangoSearchAssistant
BearShare
KaZaA
Hotbar
C2.Lop
CometSystems

Windows Defender

Removals – January 2007



*Based on reports

Windows Defender

GCC Top 11 (Reports) – Nov'06-Feb'07

	GCC			Worldwide		
	Ignore	**Quarantine**	**Remove**	**Ignore**	**Quarantine**	**Remove**
Zlob	25.55%	1.03%	73.42%	22.98%	0.73%	76.29%
NewDotNet	33.38%	1.54%	65.08%	22.83%	2.45%	74.70%
WhenU.SaveNow	44.90%	10.80%	44.30%	46.19%	12.33%	41.47%
Starware	61.25%	12.40%	26.36%	64.60%	11.50%	23.88%
180Solutions.Zango.SearchAssistant	56.79%	6.41%	36.80%	57.12%	10.91%	31.95%
BearShare	83.72%	5.77%	10.51%	82.53%	6.87%	10.60%
KaZaA	47.25%	6.91%	45.83%	41.17%	15.90%	42.88%
RealVNC	81.70%	3.72%	14.57%	88.62%	2.55%	8.82%
C2.Lop	22.98%	0.84%	76.17%	15.77%	4.19%	80.01%
Altnet	58.02%	8.45%	33.53%	44.98%	17.24%	37.76%
CnsMin	94.10%	0.17%	5.73%	37.40%	1.64%	60.96%

*Based on reports

MSRT Telemetry

MSRT Top10 Removals

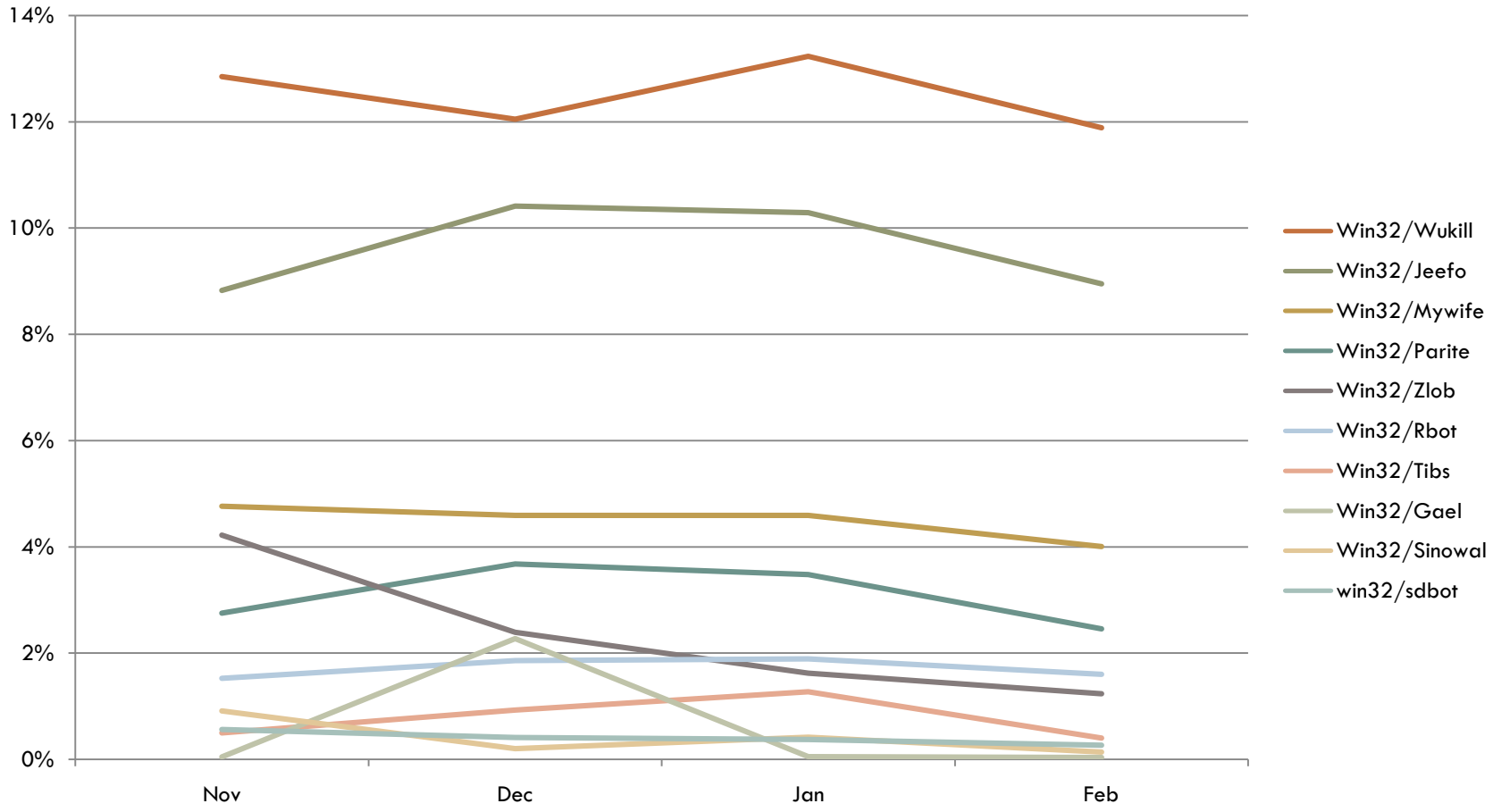
(Nov'06-Feb'07)

Worldwide
Brontok*
Zlob
Jeefo
Rbot
Parite
Hupigon
Wukill*
Banker
Alcan
Tibs*

Arabic Locale
Brontok*
Wukill*
Jeefo
Mywife*
Parite
Zlob
Rbot
Tibs*
Gael
Sinowal

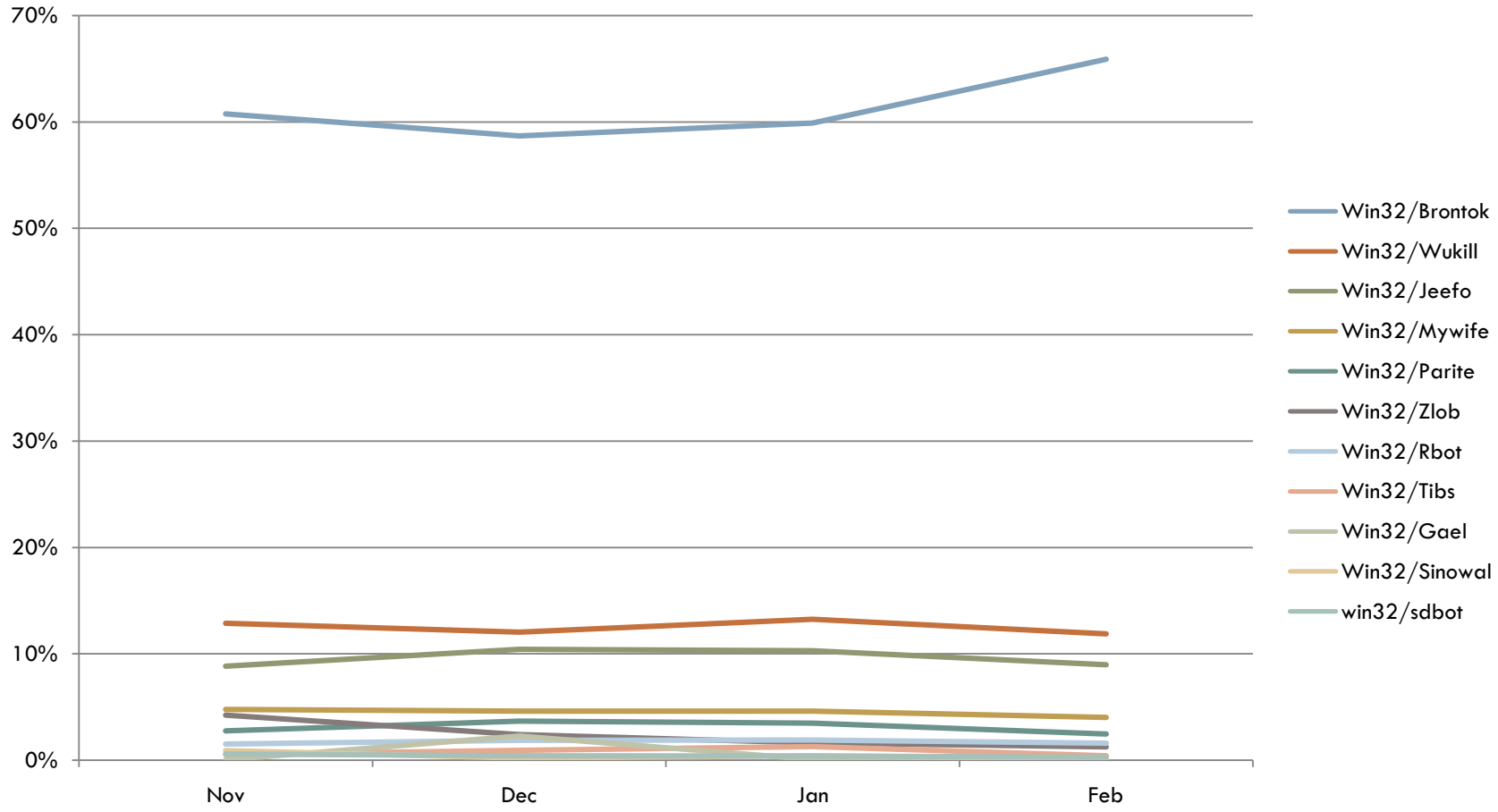
MSRT: Top Threats

All Arabic Locales



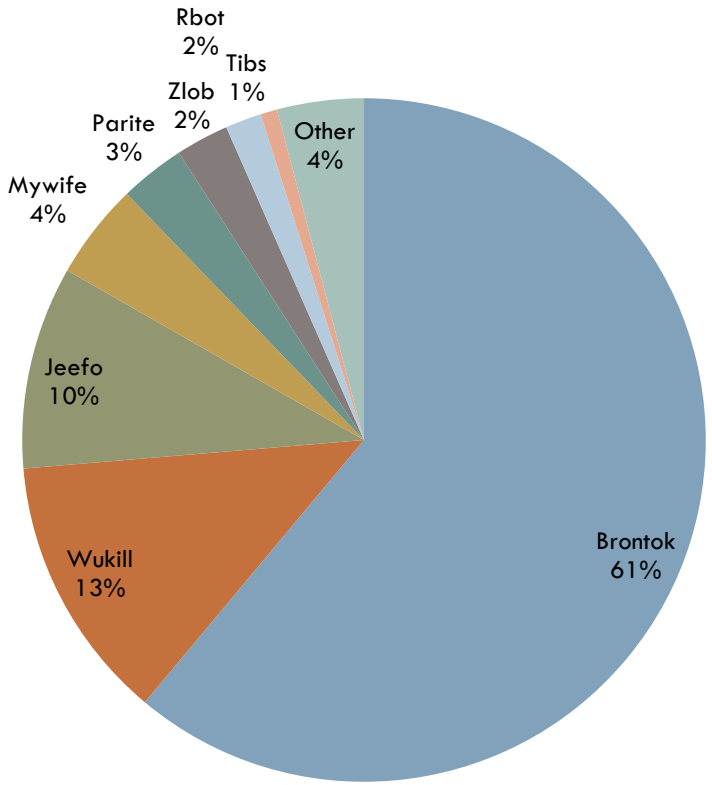
MSRT: Top Threats

All Arabic Locales

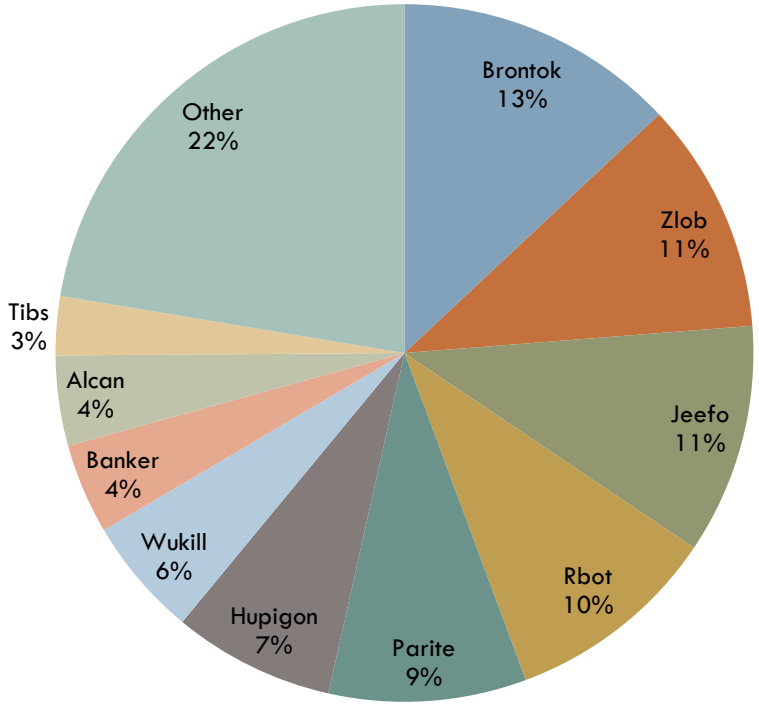


MSRT Top Threats

Arabic/Global Comparison

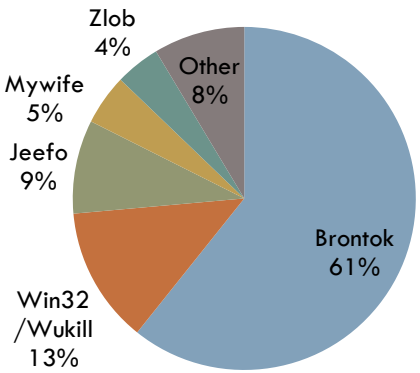


Top Threats (Ar)
11/06-2/07

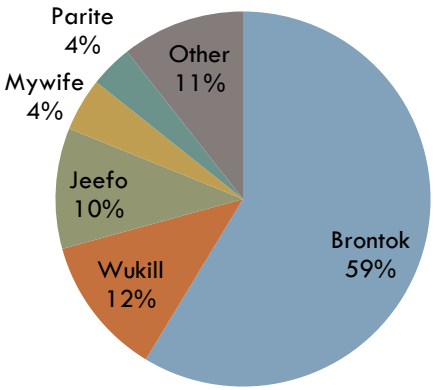


Top Threats (Global)
11/06-2/07

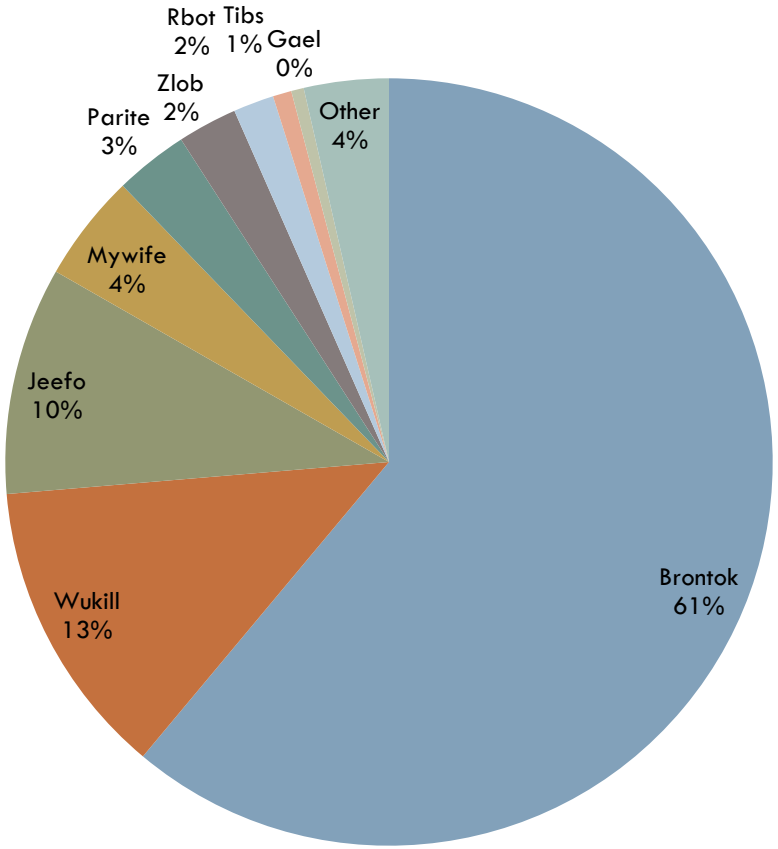
MSRT: Top Threats (Ar)



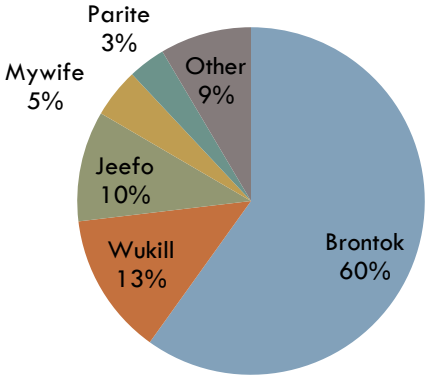
11/06



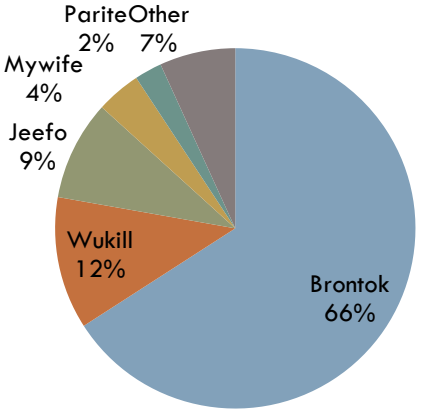
12/06



Top Threats (Ar)
11/06-2/07



1/07



2/07

What is Win32/Brontok?

- Mass mailing worm
- Indonesian e-mail
- Includes an attachment containing malware
  - People still open random attachments?!?!?!?
- Carries out ping flood against several websites

Exploit vs. Social Engineering

Overview

Exploit: Win32/Sasser.B

- Discovered
  - May 1, 2004
- Exploited vulnerability present in Windows 2000, Windows XP
- 450,000 disinfections in first 7 days

Social Engineering: Win32/Netsky.P

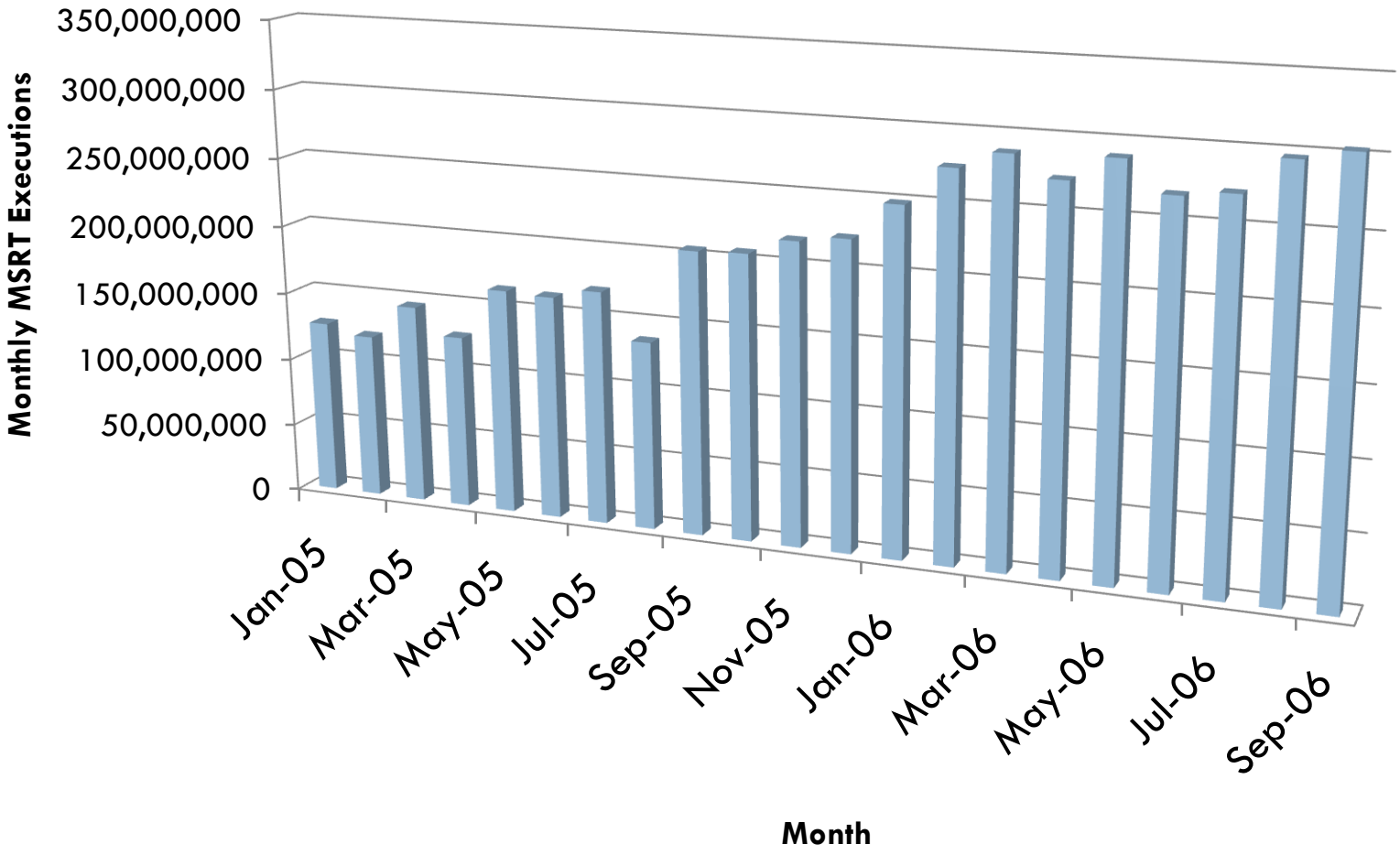
- Discovered
  - March 21, 2004
- Multi-vector social engineering
  - E-mail
  - Peer-to-peer
- <450,000 disinfections in first 7 days

What is Zotob?

- IRC Bot
- Bot herders based in Turkey & Morocco
- Exploits MS05-039 (PnP Vuln)
- Aug 9 - Microsoft Advisory
- Aug 13 – Zotob first detected
- Aug 26 – Moroccan and Turkish police make arrests

Mitigation

It's not all bad news…



Mitigation (cont.)

It's not all bad news…

- Microsoft
  - Security engineering
  - Automatic updates
  - ISA Firewall
  - Data Execute Prevention (DEP)
  - Stack protection
  - System / service hardening
  - Anti-malware tools & technologies
- Security ISVs
  - Intrusion prevention / detection
  - Enhanced antimalware response times
- User education
  - Usage of security products
  - Accelerated patch adoption

Conclusions

- Global aggregates generalize into virtually all locales with sufficient data
- Dynamics of individual threats varies depending on the threat itself
  - Targeted threats exist (ex. Brontok)
  - More granularly targeted threats exist (ex. Antinny)
  - Even more granularly targeted threats are perceivable (ex. 'spear phishing' applied to malware propagation)
- Education & awareness are key components to online safety
  - Particularly in countries with developing internet infrastructure
- Anti-malware scanners are an absolute necessity in today's networked environment

Q&A

Microsoft®

Your potential. Our passion.™

Tareq Saade
Microsoft Security Research & Response

Hack In The Box '07

Reference

Resources

- Microsoft Malware Removal Tool (MRT)
  http://www.microsoft.com/security/malwareremove/default.mspx
- Windows Defender
  http://www.microsoft.com/athome/security/spyware/software/default.mspx
- Windows Live Safety Scanner
  http://onecare.live.com/scan
- Microsoft Forefront Client Security
  http://www.microsoft.com/forefront/clientsecurity/default.mspx
- Windows Live OneCare
  http://onecare.live.com
- Anti-Malware Engineering Team Blog
  http://blogs.technet.com/antimalware/

Papers

- Using Windows Vista or Using Windows XP with Service Pack 2: Controlling Communication with the Internet
  http://www.microsoft.com/downloads/details.aspx?FamilyID=e6a35441-918f-4022-b973-e7fc0d1d2917&DisplayLang=en
- Defeating Polymorphism: Beyond Emulation
  http://go.microsoft.com/fwlink/?LinkId=57019
- Win32/Blaster: A Case Study From Microsoft's Perspective
  http://go.microsoft.com/fwlink/?LinkId=57018
- Behavioral Classification
  http://www.microsoft.com/downloads/details.aspx?FamilyID=7b5d8cc8-b336-4091-abb5-2cc500a6c41a&DisplayLang=en
- Windows Malicious Software Removal Tool: Progress Made, Trends Observed
  http://go.microsoft.com/fwlink/?linkid=67998
- Microsoft Security Intelligence Report (H106)
  http://www.microsoft.com/downloads/details.aspx?FamilyID=1c443104-5b3f-4c3a-868e-36a553fe2a02&DisplayLang=en
- I Know What You Did Last Logon
  http://www.microsoft.com/downloads/details.aspx?FamilyID=0b6321d4-0e65-4133-85e7-44e666cc245a&displaylang=en
- Behavioral Modeling of Social Engineering-Based Malicious Software
  http://www.microsoft.com/downloads/details.aspx?FamilyID=e0f27260-58da-40db-8785-689cf6a05c73&displaylang=en
- An Automated Virus Classification System
  http://www.microsoft.com/downloads/details.aspx?FamilyId=D61708BD-EF96-4A53-A8F8-8A1F00C79747&displaylang=en

What is Win32/Antinny?

- Worm that spreads over the Winny p2p system
- Winny is a Japanese p2p client
  - No localized builds of Winny
- Very localized threat
- Copies random files on an infected host into the Winny shared folder
- Identified as a localized outbreak and integrated into MRT
- Lots of positive press over working with the Japanese community to remove Antinny:
  - http://www.microsoft.com/japan/presspass/detail.aspx?newsid=2434
  - http://www.msnbc.msn.com/id/13283771/