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

- **Harmless**
- **Potentially Unwanted**
- **Malicious**

**Extreme**

- Adware, spyware, monitoring software, remote control software
- Viruses, worms, trojans, rootkits, bots
Malware Spectrum (cont.)

- Windows Live OneCare
- Microsoft Forefront Client Security
- Windows Live OneCare safety scanner

- Windows Defender
- Windows Malicious Software Removal Tool
# Products & Technologies

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Main Customer Segment</th>
<th>Malicious Software</th>
<th>Spyware and Potentially Unwanted Software</th>
<th>Available at No Additional Charge</th>
<th>Main Distribution Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Malicious Software Removal Tool</td>
<td>Consumers ●</td>
<td>Partial</td>
<td></td>
<td>●</td>
<td>WU / AU, Download Center</td>
</tr>
<tr>
<td>Windows Defender</td>
<td>Businesses ●</td>
<td></td>
<td></td>
<td>●</td>
<td>Download Center</td>
</tr>
<tr>
<td>Windows Live OneCare Safety Scanner</td>
<td>Consumers ●</td>
<td>●</td>
<td></td>
<td>●</td>
<td>Web</td>
</tr>
<tr>
<td>Windows Live OneCare</td>
<td>Consumers ●</td>
<td>●</td>
<td></td>
<td>●</td>
<td>Web / store purchase</td>
</tr>
<tr>
<td>Microsoft ForeFront Client Security</td>
<td>Consumers ●</td>
<td>●</td>
<td></td>
<td>●</td>
<td>Web / store purchase</td>
</tr>
</tbody>
</table>
Windows Defender

Tools and Settings

- **Options**: Choose how you want Windows Defender to run
- **Microsoft SpyNet**: Join the online community that helps identify and stop spyware infections
- **Quarantined items**: Remove or restore software that Windows Defender has prevented from running
- **Software Explorer**: View or monitor all software that is running on your computer
- **Allowed items**: View software that you have chosen not to monitor with Windows Defender
- **Windows Defender website**: Get more tools and the latest security information online
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

Welcome to the Microsoft Windows Malicious Software Removal Tool

This tool scans for and automatically removes prevalent malicious software.

Click Next to scan for and help remove specific malicious software from your computer.
For more information on this tool, please see the online documentation.

View a list of malicious software that this tool detects and removes.

This tool is not a replacement for an anti-virus product. To help protect your computer,
you should use an anti-virus product. For more information, see Protect Your PC.
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 form 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

- Malware Collection
- Analysis and Signature Creation
- Signature Testing and Deployment
- Telemetry Collection
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

SpyNet 01/07 Common Sample
GCC / Worldwide

*Based on reports
## Windows Defender

### GCC Top 11 (Reports) – Nov’06-Feb’07

<table>
<thead>
<tr>
<th></th>
<th>GCC</th>
<th>Worldwide</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ignore</td>
<td>Quarantine</td>
</tr>
<tr>
<td>Zlob</td>
<td>25.55%</td>
<td>1.03%</td>
</tr>
<tr>
<td>NewDotNet</td>
<td>33.38%</td>
<td>1.54%</td>
</tr>
<tr>
<td>WhenU.SaveNow</td>
<td>44.90%</td>
<td>10.80%</td>
</tr>
<tr>
<td>Starware</td>
<td>61.25%</td>
<td>12.40%</td>
</tr>
<tr>
<td>180Solutions.Zango.SearchAssistant</td>
<td>56.79%</td>
<td>6.41%</td>
</tr>
<tr>
<td>BearShare</td>
<td>83.72%</td>
<td>5.77%</td>
</tr>
<tr>
<td>KaZaA</td>
<td>47.25%</td>
<td>6.91%</td>
</tr>
<tr>
<td>RealVNC</td>
<td>81.70%</td>
<td>3.72%</td>
</tr>
<tr>
<td>C2.Lop</td>
<td>22.98%</td>
<td>0.84%</td>
</tr>
<tr>
<td>Altnet</td>
<td>58.02%</td>
<td>8.45%</td>
</tr>
<tr>
<td>CnsMin</td>
<td><strong>94.10%</strong></td>
<td><strong>0.17%</strong></td>
</tr>
</tbody>
</table>

*Based on reports*
MSRT Telemetry
## MSRT Top 10 Removals
(Dec’06-Feb’07)

<table>
<thead>
<tr>
<th>Worldwide</th>
<th>Arabic Locale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brontok*</td>
<td>Brontok*</td>
</tr>
<tr>
<td>Zlob</td>
<td>Wukill*</td>
</tr>
<tr>
<td>Jeefo</td>
<td>Jeefo</td>
</tr>
<tr>
<td>Rbot</td>
<td>Mywife*</td>
</tr>
<tr>
<td>Parite</td>
<td>Parite</td>
</tr>
<tr>
<td>Hupigon</td>
<td>Zlob</td>
</tr>
<tr>
<td>Wukill*</td>
<td>Rbot</td>
</tr>
<tr>
<td>Banker</td>
<td>Tibs*</td>
</tr>
<tr>
<td>Alcan</td>
<td>Gael</td>
</tr>
<tr>
<td>Tibs*</td>
<td>Sinowal</td>
</tr>
</tbody>
</table>
MSRT: Top Threats
All Arabic Locales
MSRT: Top Threats
All Arabic Locales

![Graph showing the percentage distribution of various threats over the months of November, December, January, and February. The graph compares different threat types such as Win32/Brontok, Win32/Wukill, etc., and shows their prevalence over time.]
MSRT Top Threats
Arabic/Global Comparison

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

Brontok 61%
Wukill 13%
Jeefo 10%
Mywife 4%
Rbot 2%
Tibs Zlob 1%
Parite 3%
Other 4%

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

Brontok 13%
Zlob 11%
Jeefo 11%
Other 22%
Tibs 3%
Alcan 4%
Banker 4%
Wukill 6%
Hupigon 7%
Parite 9%
Rbot 10%
MSRT: Top Threats (Ar)

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

- Brontok: 61%
- Wukill: 13%
- Jeefo: 10%
- Mywife: 4%
- Parite: 3%
- Zlob: 2%
- Rbot: 2%
- Tibs: 1%
- Gael: 0%
- Other: 4%

11/06:
- Brontok: 61%
- Wukill: 13%
- Jeefo: 10%
- Mywife: 5%
- Parite: 4%
- Zlob: 4%
- Other: 8%

12/06:
- Brontok: 59%
- Wukill: 12%
- Jeefo: 10%
- Mywife: 4%
- Parite: 4%
- Other: 11%

1/07:
- Brontok: 60%
- Wukill: 13%
- Jeefo: 10%
- Other: 9%
- Mywife: 5%
- Parite: 3%

2/07:
- Brontok: 66%
- Wukill: 12%
- Jeefo: 9%
- Other: 7%
- Parite: 2%
- Mywife: 4%
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
Reference
Resources

- Microsoft Malware Removal Tool (MRT)

- Windows Defender

- Windows Live Safety Scanner

- Microsoft Forefront Client Security

- Windows Live OneCare
  [http://onecare.live.com](http://onecare.live.com)

- Anti-Malware Engineering Team Blog
Papers

- Using Windows Vista or Using Windows XP with Service Pack 2: Controlling Communication with the Internet

- Defeating Polymorphism: Beyond Emulation
  [http://go.microsoft.com/fwlink/?LinkId=57019](http://go.microsoft.com/fwlink/?LinkId=57019)

- Win32/Blaster: A Case Study From Microsoft’s Perspective
  [http://go.microsoft.com/fwlink/?LinkId=57018](http://go.microsoft.com/fwlink/?LinkId=57018)

- Behavioral Classification

- Windows Malicious Software Removal Tool: Progress Made, Trends Observed
  [http://go.microsoft.com/fwlink/?LinkId=67998](http://go.microsoft.com/fwlink/?LinkId=67998)

- Microsoft Security Intelligence Report (H106)

- I Know What You Did Last Logon

- Behavioral Modeling of Social Engineering-Based Malicious Software

- An Automated Virus Classification System
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: