WHEN THE HAMMER FALLS -
EFFECTS OF SUCCESSFUL WIDESPREAD DISINFECTION ON MALWARE DEVELOPMENT AND DIRECTION

Matt McCormack
Microsoft Malware Protection Centre, Australia
matt.mccormack@microsoft.com

Agenda

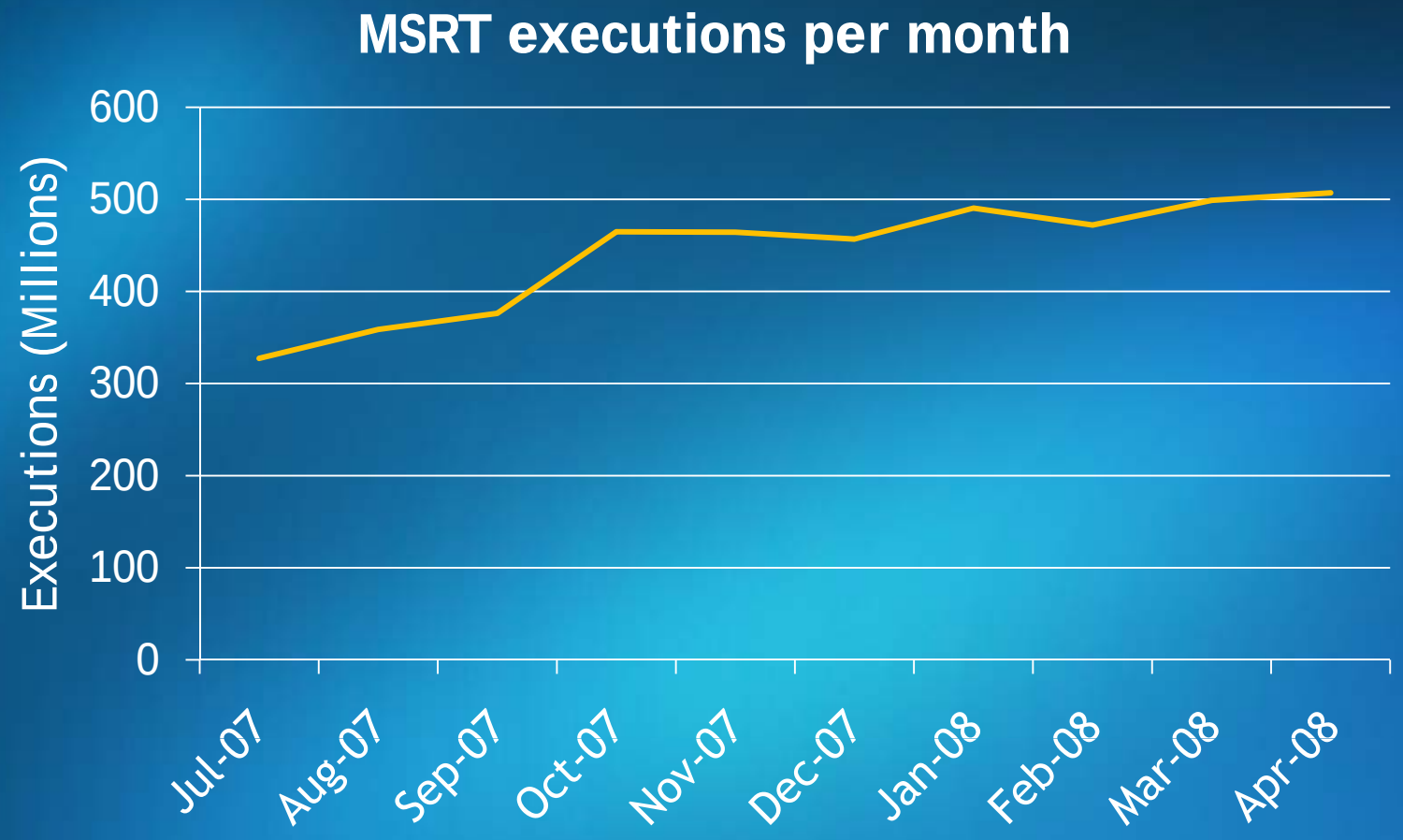
- MSRT – Overview
- MSRT vs Malware
  - Malware before MSRT
  - Impact of MSRT on malware
  - Malware after MSRT
- Correlation
- Conclusions

What is MSRT

- Malicious Software Removal Tool
- Intended to clean the Windows ecosystem
- Optional Windows Update
- Updated with new malware families monthly

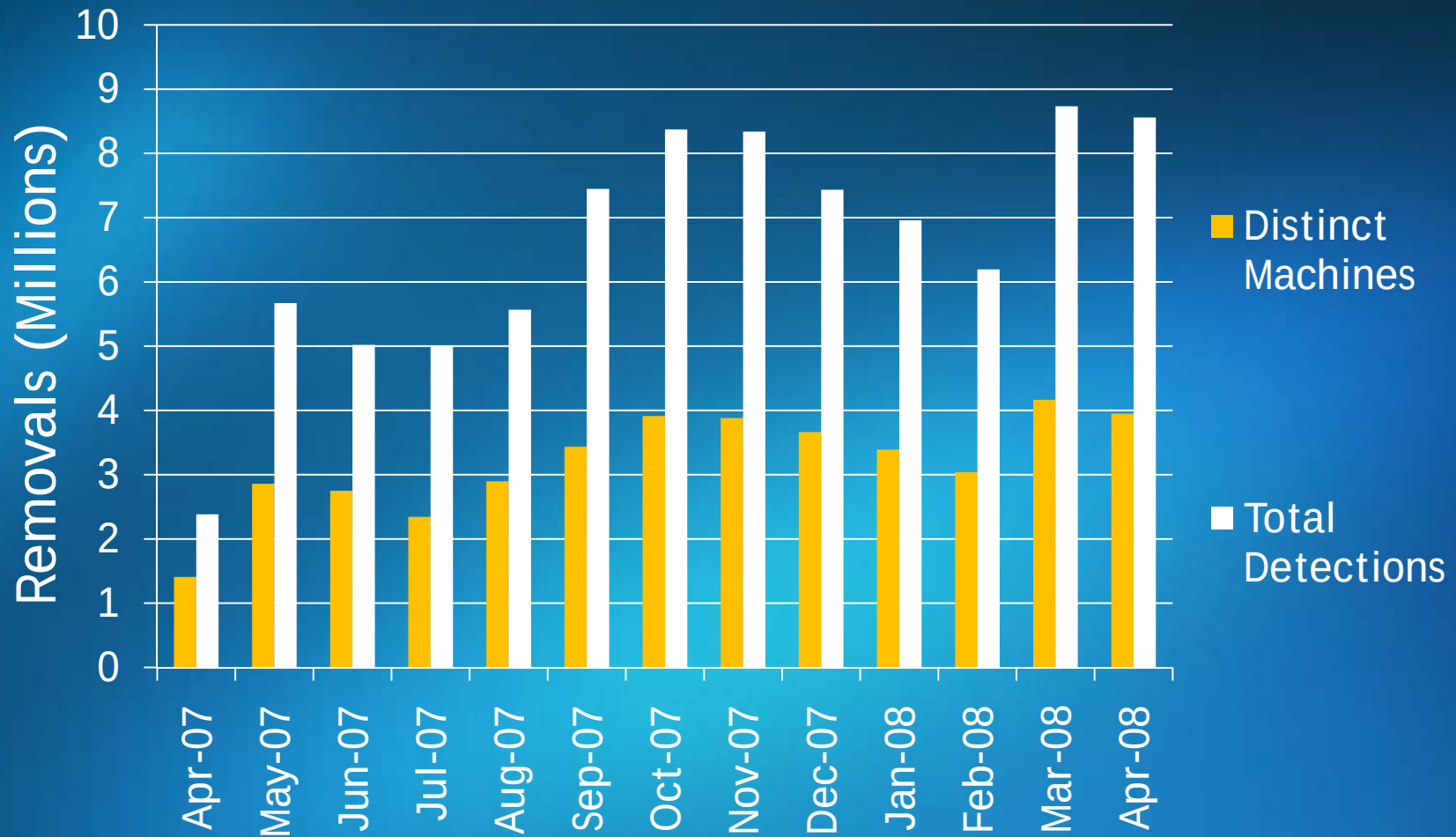
Range of execution

- Execution base ~ 500 million machines



MSRT vs. Malware

- Detections vary according to target family



Notable inclusions

- Win32/Nuwar (alias: ‘Storm worm’) added September 2007
- Win32/Cutwail (alias ‘Pandex’) added January 2008
- Win32/Oderoor (alias ‘Kraken’) added May 2008

In brief: Win32/Nuwar

- Gained notoriety in early 2007
  - ‘Storm worm’
- Distributed P2P spam network
- Large events topic of infection spam
  - European storms January 2007
  - Valentines day ‘e-cards’
- Utilised ‘Tibs’ encryption

In brief: Win32/Cutwail

- Origins as network worm in late 2005
- Template-based spam engine:

```
HELO {MYSERVER}
MAIL FROM:<{MAIL_FROM}>
RCPT TO:<{MAIL_TO}>
```

- Penchant for process injection
- Utilises custom encryption

In brief: Win32/Oderoor

- High volume spam network
  - ‘The Kraken’
- Origins early 2005 (Win32/Bobax)
- Encrypted port 447 communications
- Distributed via instant messenger
  - *img_011.JPEG-<email>@hotmail.com*

Key malware concepts

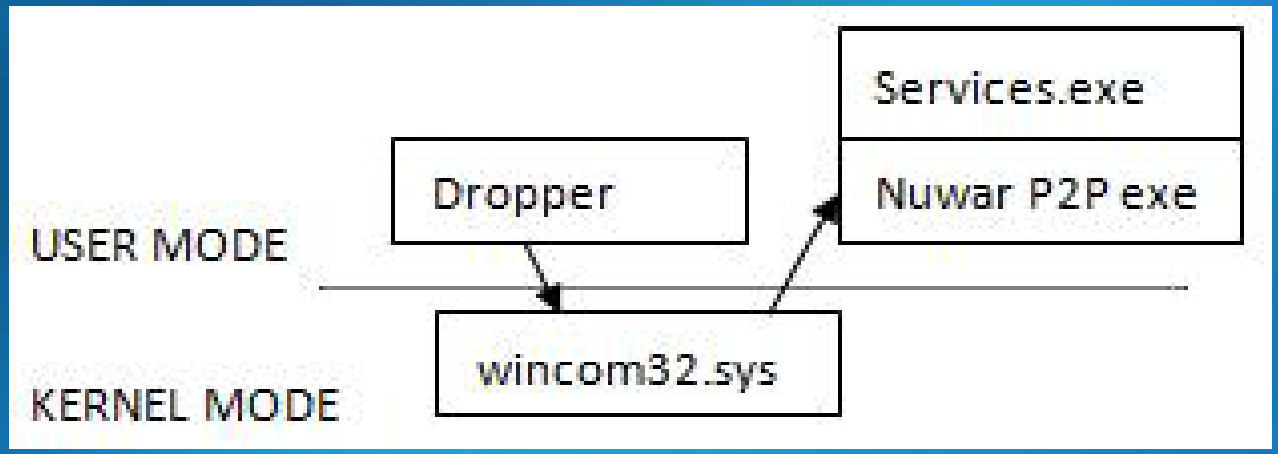
- Evasion
  - Attempt avoiding scanner detections
- Stealth
  - Attempt avoiding being scanned at all
  - Avoid making victim suspicious
- Functionality
  - Extend payloads/functionality over time

Malware direction before MSRT

- Malware authors more concerned with functionality
- Token amounts of protection
- Minimal defensive measures

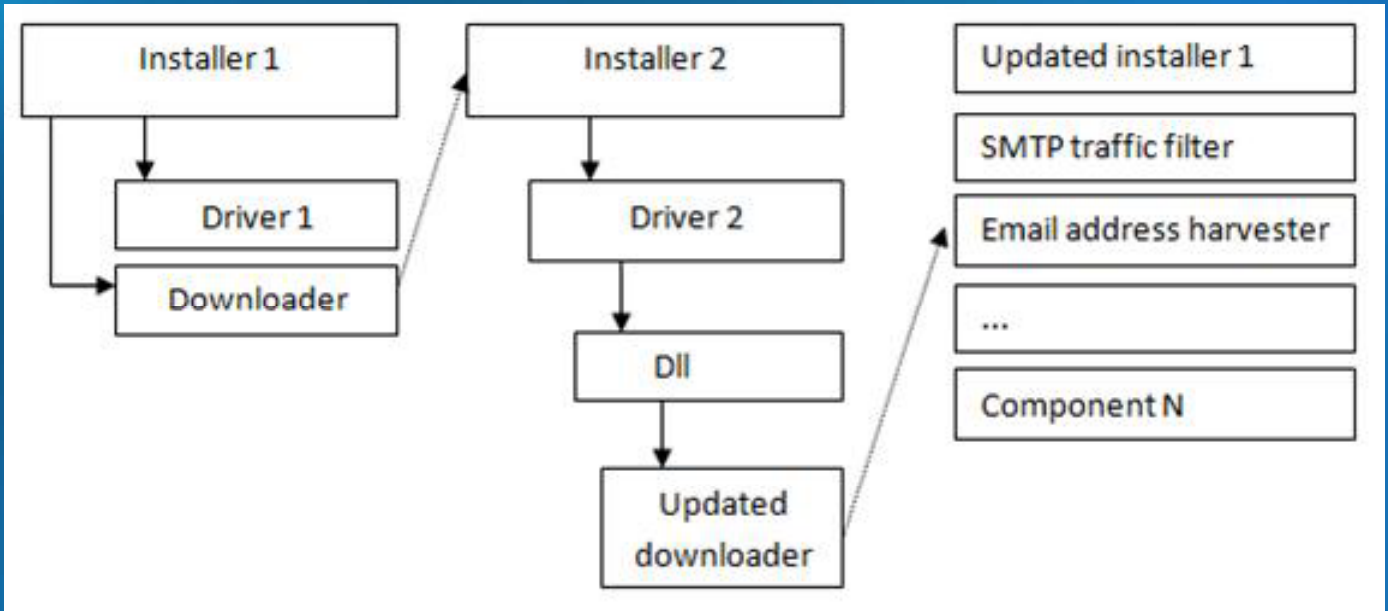
Direction - Win32/Nuwar

- Spam campaigns
- Some evasion and protection
- Slights changes to P2P and architecture



Direction – Win32/Cutwail

- Consistent downloader modular design
- Core downloader modules changed infrequently

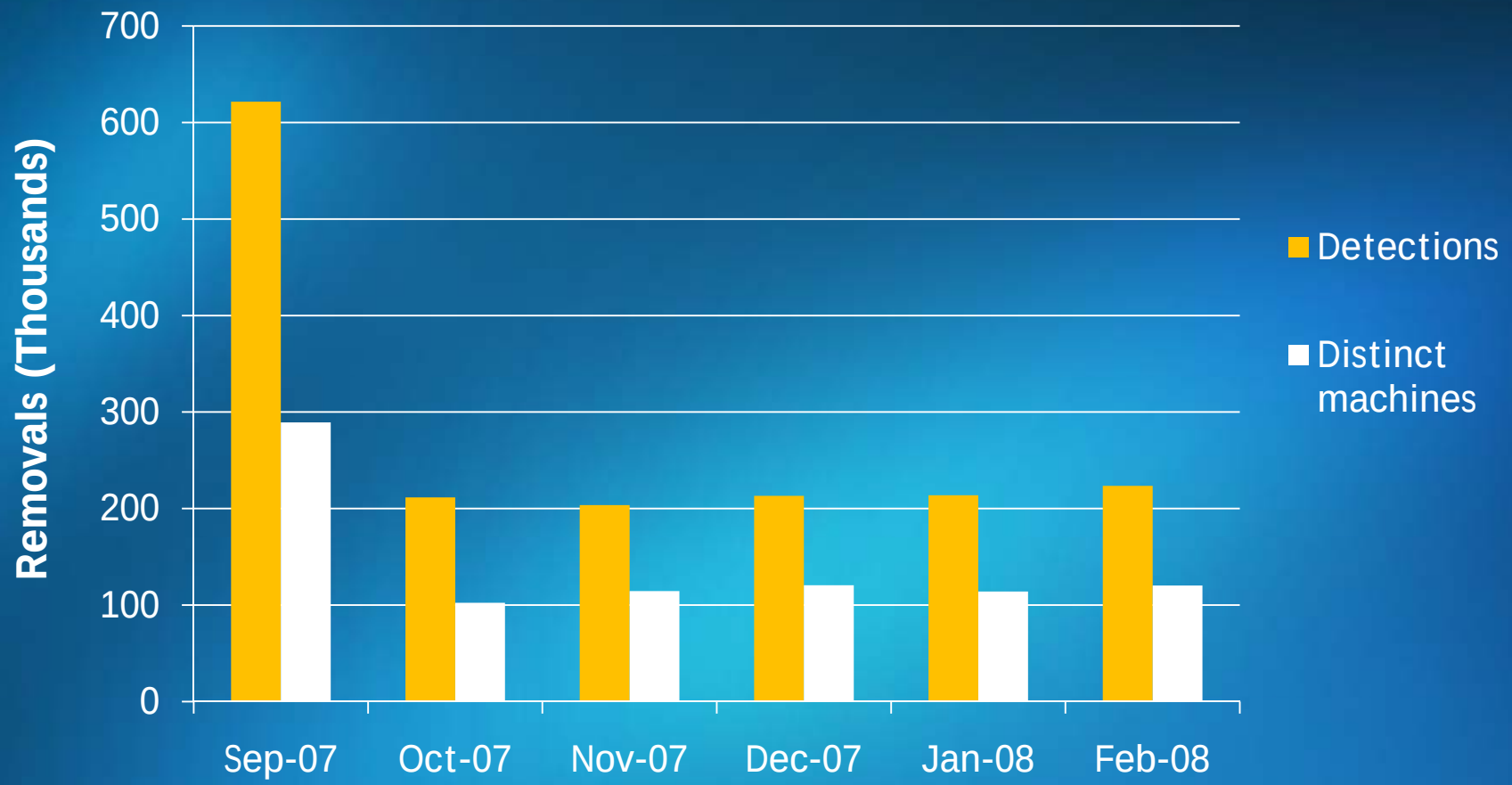


Direction - Win32/Oderoor

- Packers changing over time
- Additional functionality
- Frequent releases

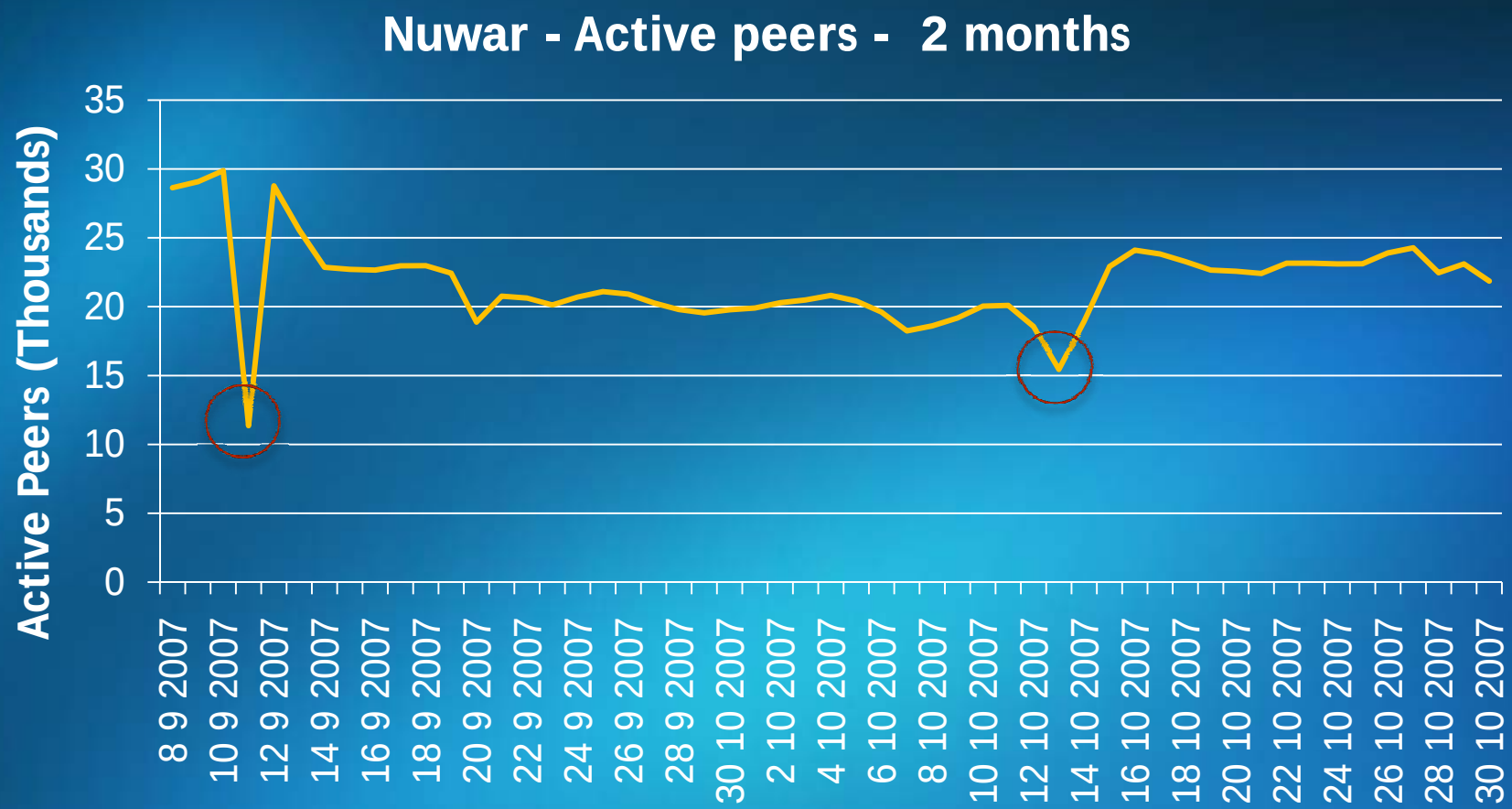
MSRT vs. Nuwar - Detections

- Consistent removals after first month



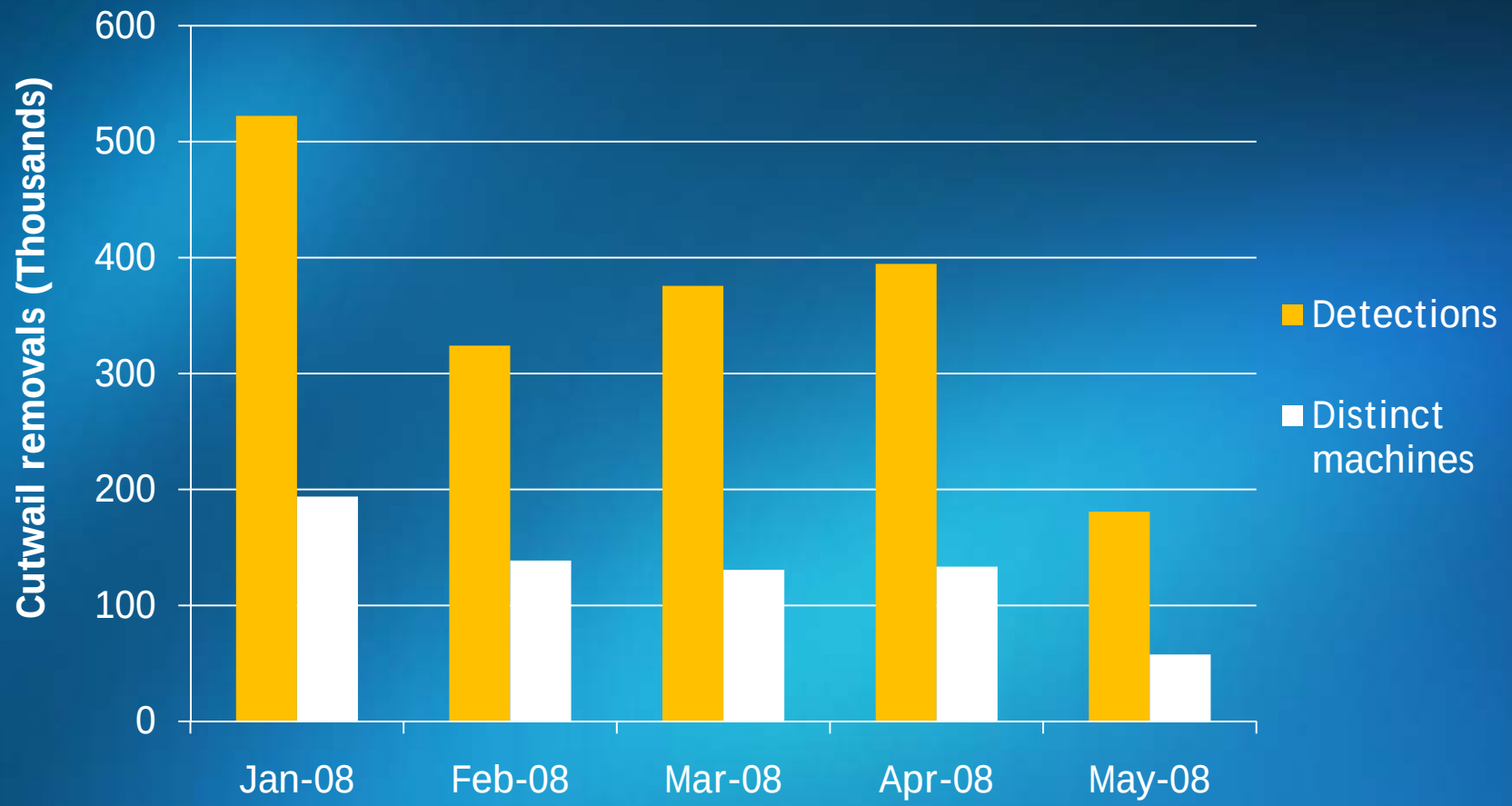
MSRT vs. Nuwar - Disruption

- Dips after MSRT releases



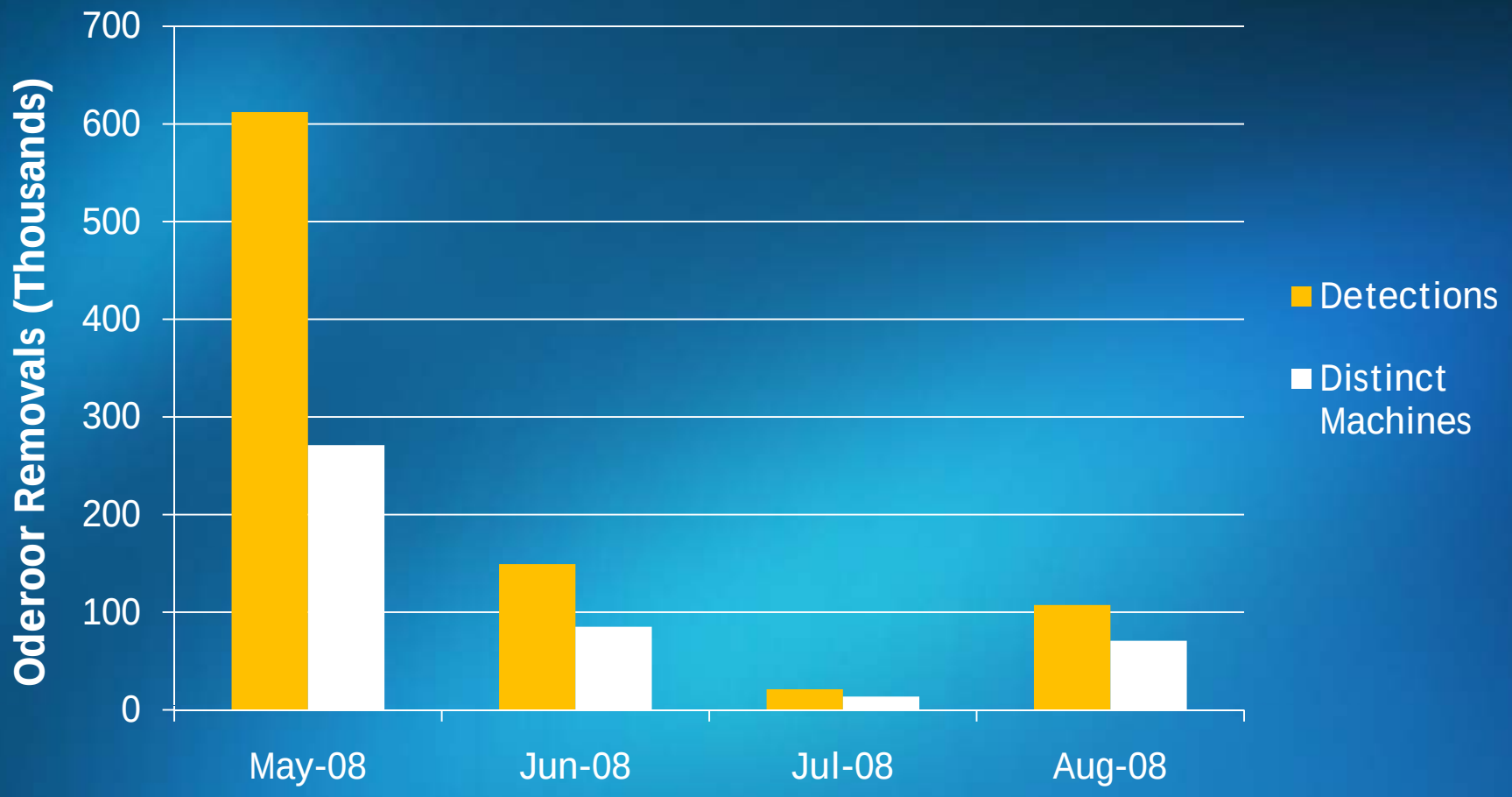
MSRT vs. Cutwail

- More components per machine



MSRT vs. Oderoor

- Similar trend to Nuwar



What do we find?

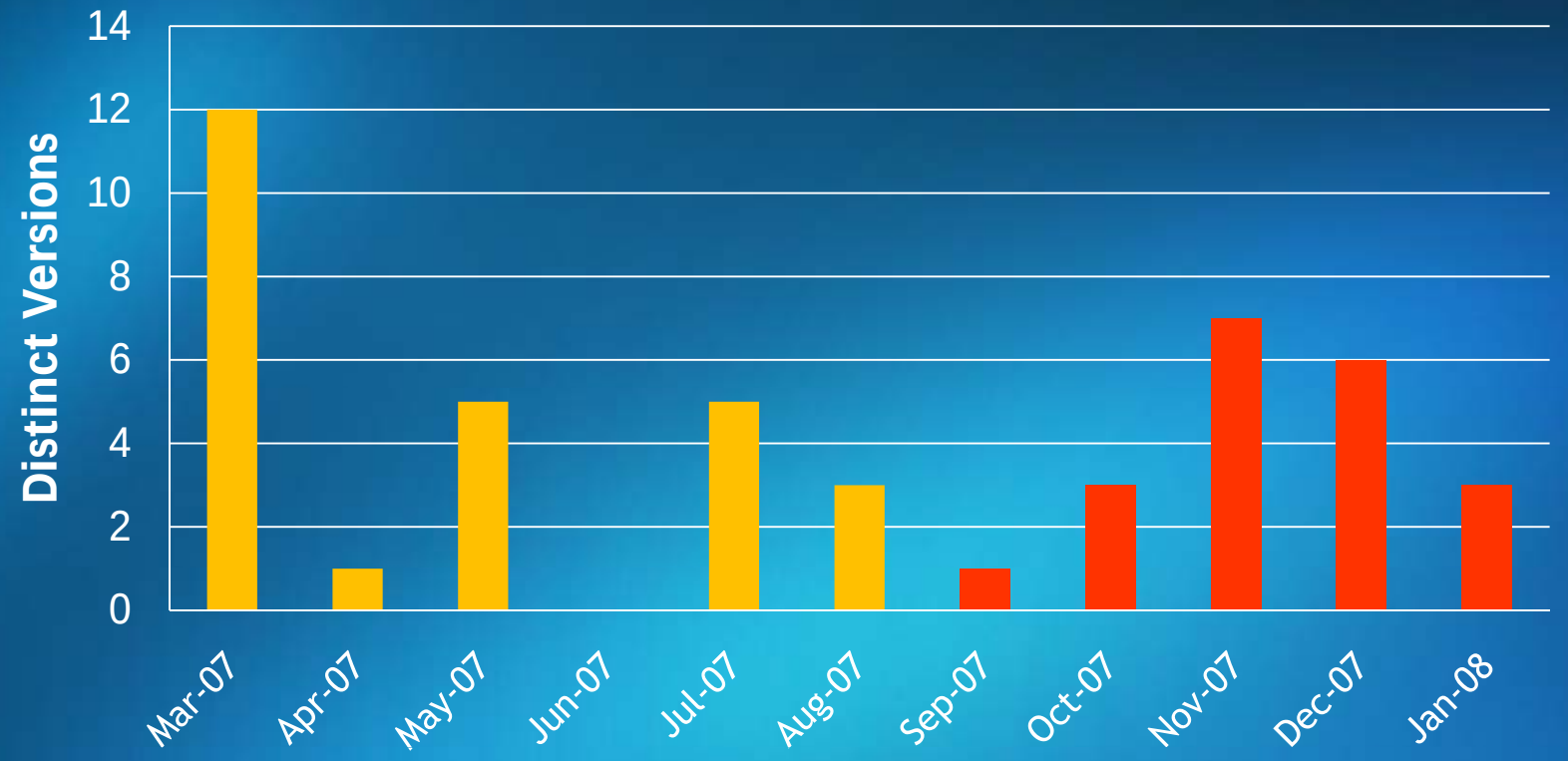
- Major impact on first month
- Detections taper off, but generally maintains consistent impact
- Removals put pressure on malware authors
- … What would we expect to happen?

Direction after MSRT

- Distinct differences in behaviour post MSRT inclusion
- Changes in Evasion, Stealth and Functionality
- Observations suggest:
  - Focus of authors noticeably shift
  - Avoiding MSRT more of a priority

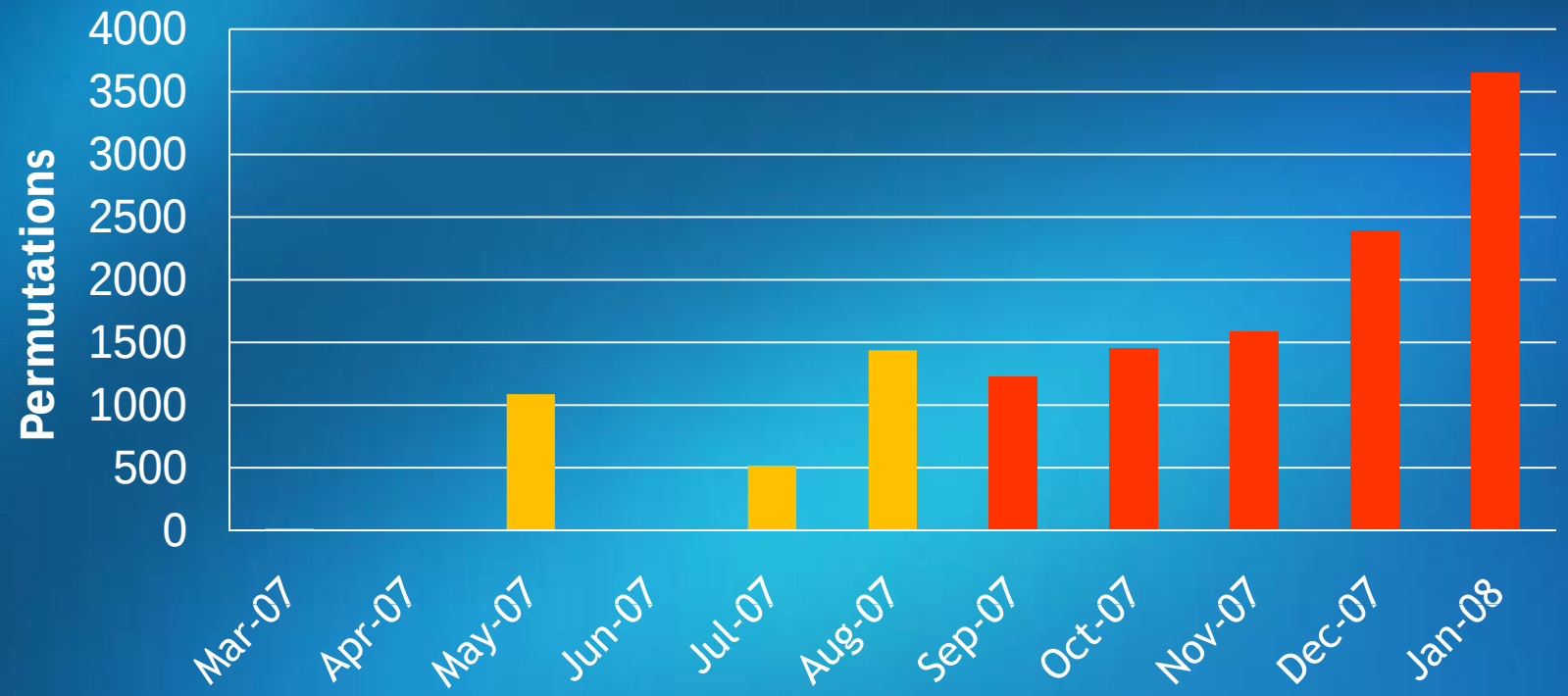
Nuwar post MSRT

- Architectural & Functional changes



Nuwar post MSRT

- Evasion
  - Massive increase in server-side polymorphism
  - Increase in anti-Emulation techniques



Nuwar post MSRT

- Increased spam infection runs
  - December/January
- Additional infection vectors
- MSRT targeted … but missed
  - Windows-KB890830-V1.32.exe
  - V1.33 - September 2007

Cutwail post MSRT

- Evasion
  - Increase in encryption usage
  - Random filenames
- Stealth
  - Change from SDT hooks to callbacks
- Functionality
  - Additional components

Oderoor post MSRT

- Fixed protection ‘weak points’
- Additional memory obfuscation techniques
- Targets MSRT explicitly
- Utilises Random names

Correlations between families

- Focus on evasion
- Intent on keeping infected nodes
- MSRT becomes a target
- … are we surprised?

Conclusions – MSRT

- Sledgehammer effect
- Consistent monthly removals
- Appears we're having an impact

Conclusions – Malware

- Behaviour observed is different post MSRT
  - Consider the scale of change to be extraordinary
- Consider MSRT to be worth avoiding
  - Evasive techniques don't have much effect
- MSRT is but one of many security vectors required to keep malware at bay

Microsoft® Malware Protection Center

Threat Research and Response

http://www.microsoft.com/security/portal

http://blogs.technet.com/mmpc/

Microsoft®

Your potential. Our passion.™