FIRST

Improving Security Together

Botnets, Collective Defense, and Project MARS

Jeff Williams

Principal Group Program Manager

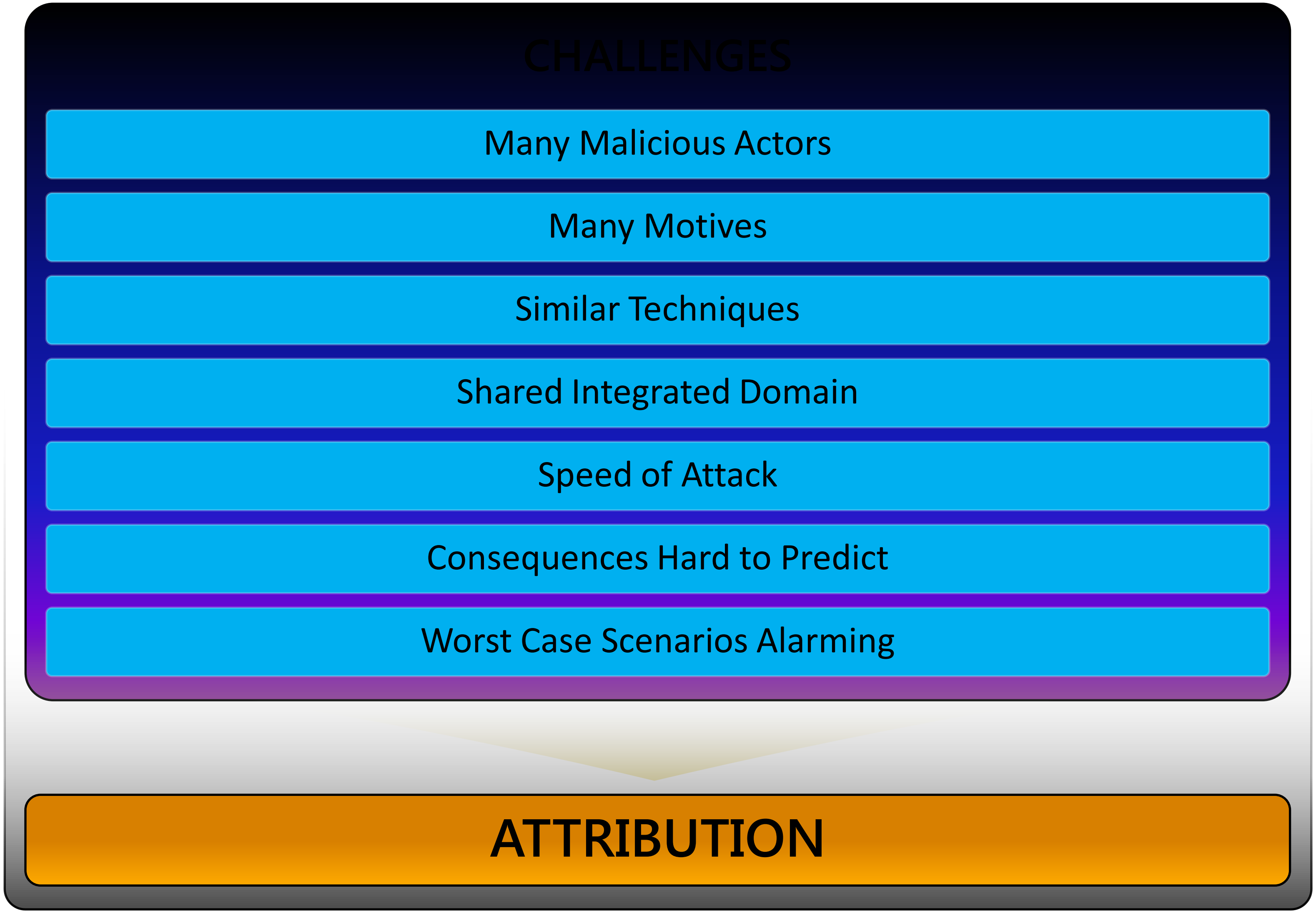
Microsoft Malware Protection Center

12 - 17 June 2011

23rd Vienna

Annual FIRST Conference

The Basics



CHALLENGES

Many Malicious Actors

Many Motives

Similar Techniques

Shared Integrated Domain

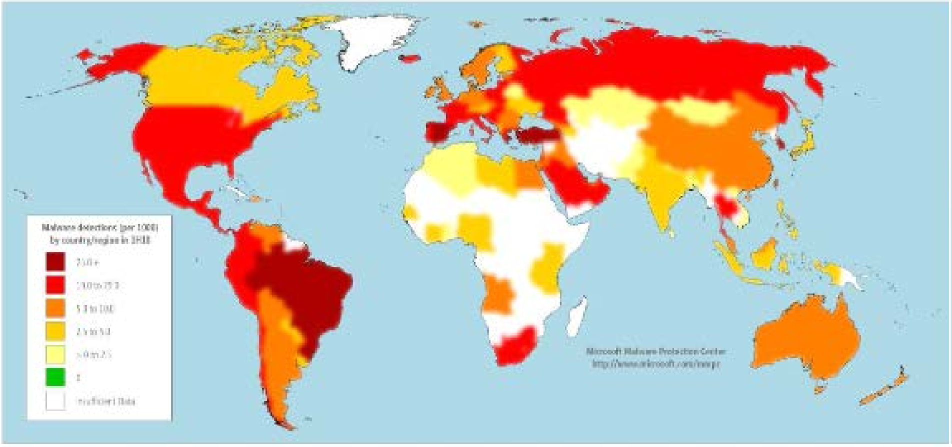
Speed of Attack

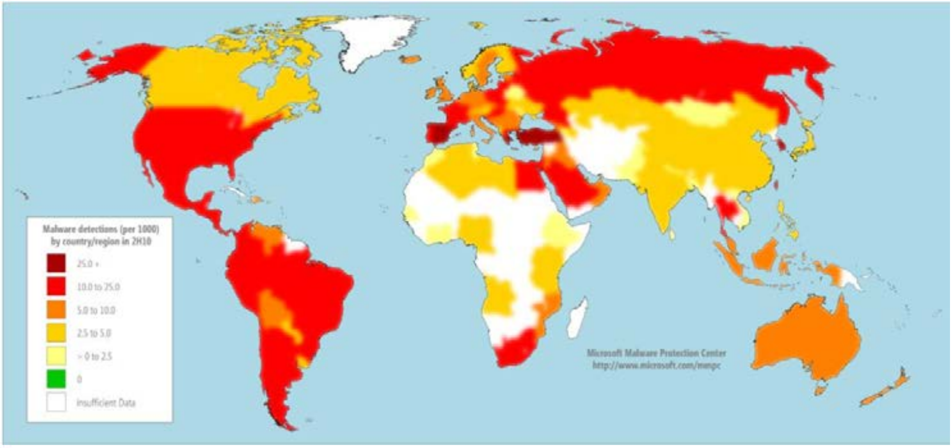
Consequences Hard to Predict

Worst Case Scenarios Alarming

ATTRIBUTION

A Picture of Health?

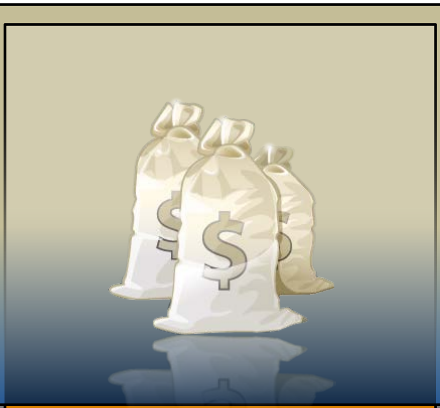

Malware detections (per 1000)
by country/region in 1H10
25.0 +
10.0 to 25.0
5.0 to 10.0
2.5 to 5.0
> 0 to 2.5
0
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc


Malware detections (per 1000)
by country/region in 2H10
25.0 +
10.0 to 25.0
5.0 to 10.0
2.5 to 5.0
> 0 to 2.5
0
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

	Location	1Q2010	2Q10	3Q10	4Q10	Delta
1	United States	11,025,811	9,609,215	11,340,751	11,817,437	4.2% ▲
2	Brazil	2,026,578	2,354,709	2,985,999	2,922,695	-2.1% ▼
3	China	2,168,810	1,943,154	2,059,052	1,882,460	-8.6% ▼
4	France	1,943,841	1,510,857	1,601,786	1,794,953	12.1% ▲
5	United Kingdom	1,490,594	1,285,570	1,563,102	1,857,905	18.9% ▲
6	Spain	1,358,584	1,348,683	1,588,712	1,526,491	-3.9% ▼
7	Korea	962,624	1,015,173	1,070,163	1,678,368	56.8% ▲

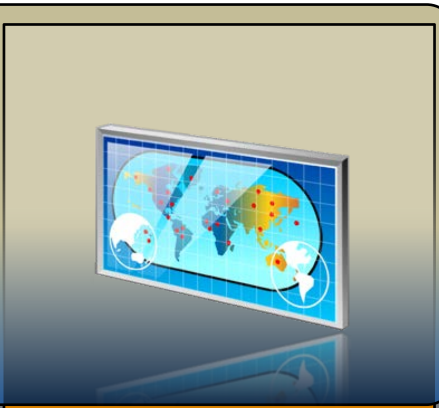
Case Study: Botnets

Cybercrime

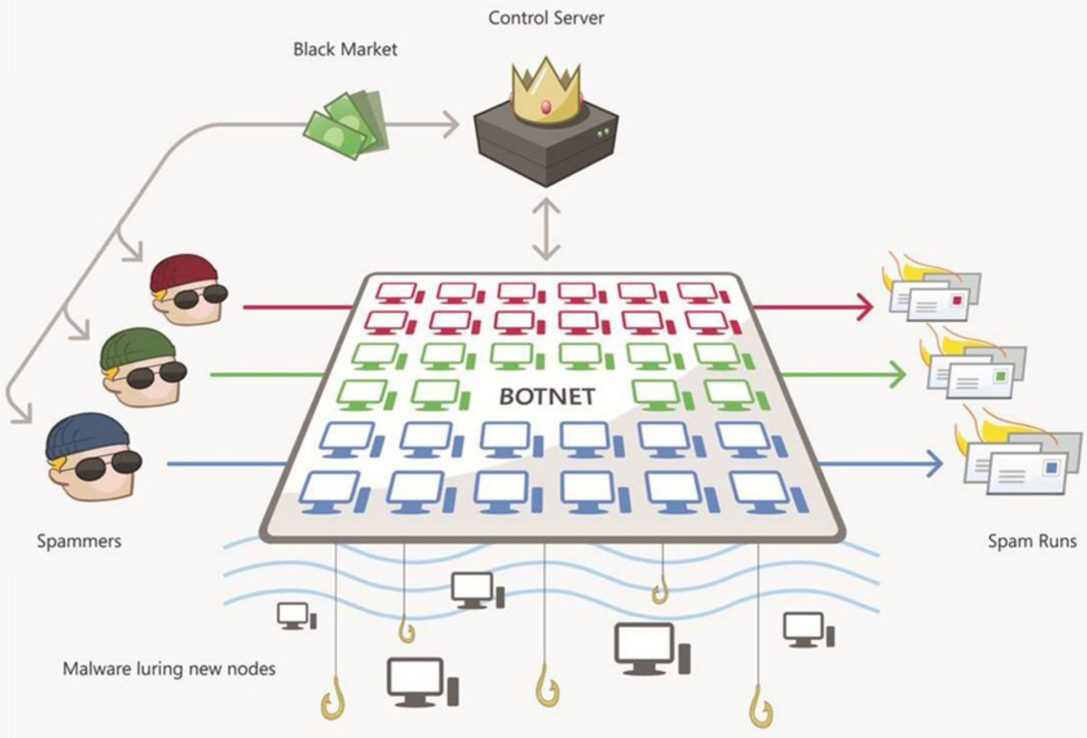


Economic Espionage

Military Espionage



Cyber Warfare

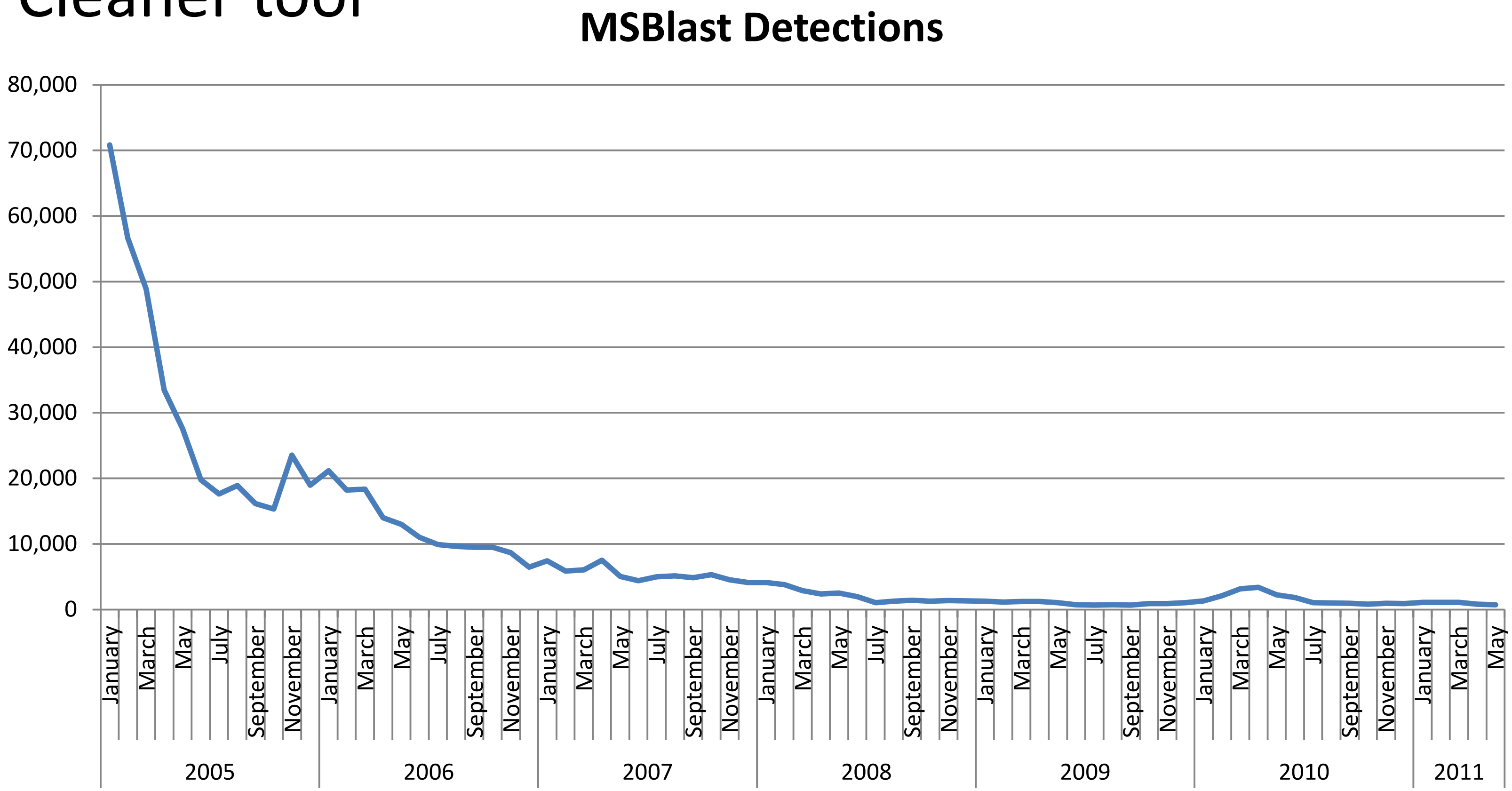


The Maturity of Response Over Time

- Some historic examples
  - Blaster
  - Slammer
  - Zotob
  - WinFixer
  - Cutwail
  - Intercage & McColo de-peerings
  - Mariposa
- More Recent Examples
  - Bredolab
  - Waledac
  - Rustock
  - AFCore

Early Examples: Blaster

- MS03-026
- Customer call downs
- Cleaner tool

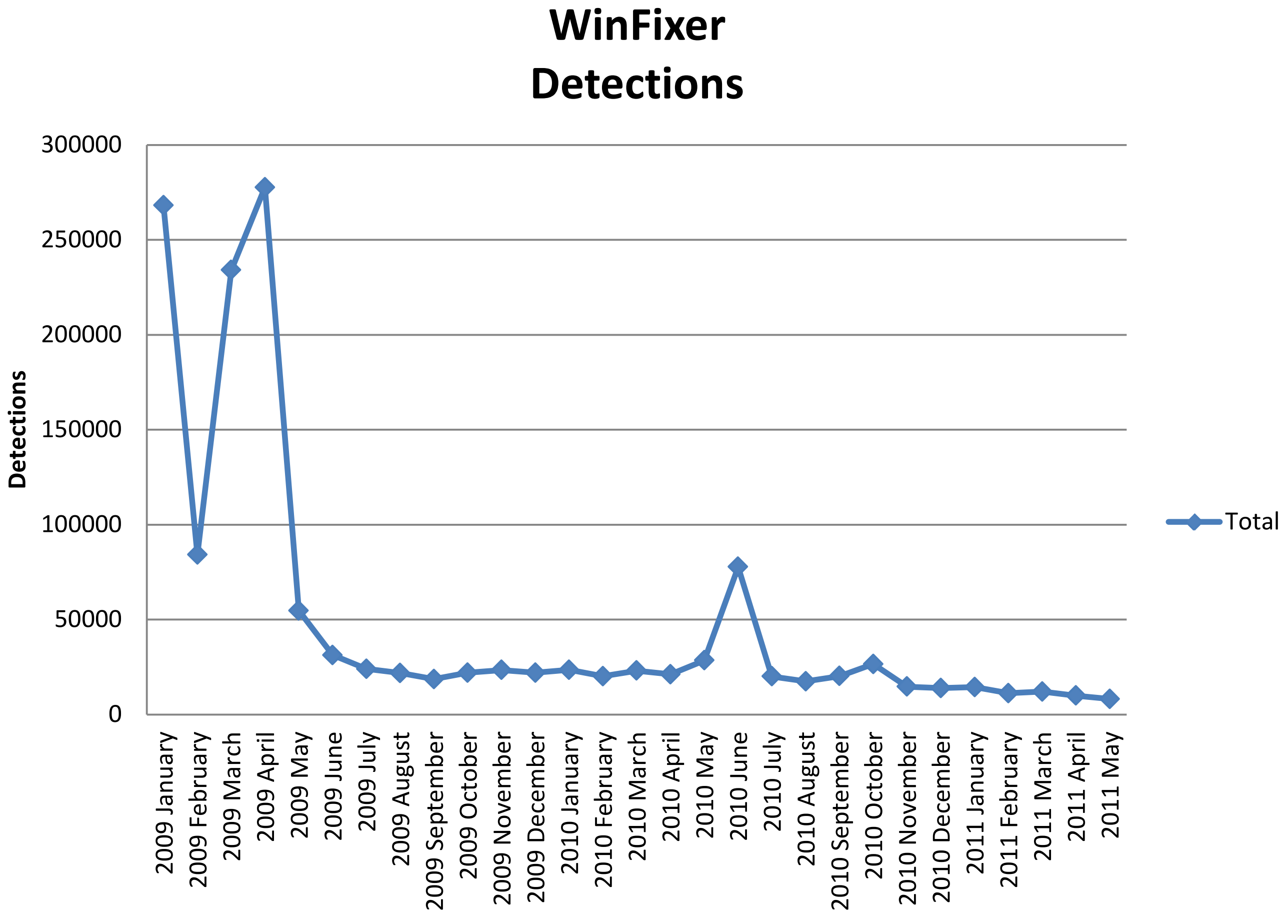


Early Examples (con’t)

- Slammer
  - Vuln patched in July 2002
  - Cross product vulnerability (SQL, MSDE)
  - Unthrottled (impacting response)
  - ISPs
- Zotob
  - actor attribution
  - foreign laws

Early Examples: WinFixer

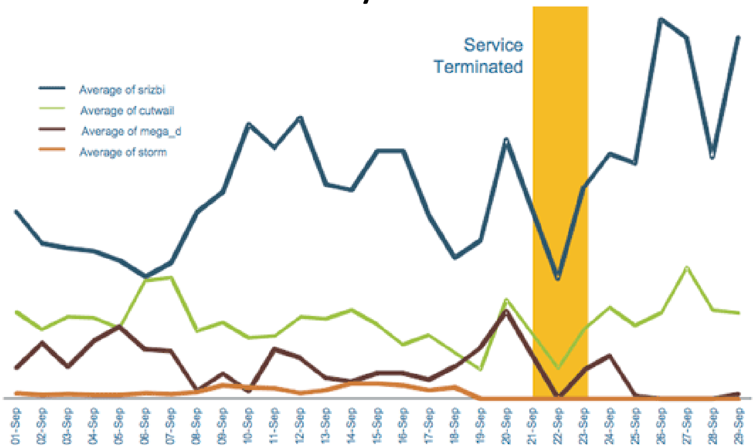
- Initial Microsoft investigation
- Referrals



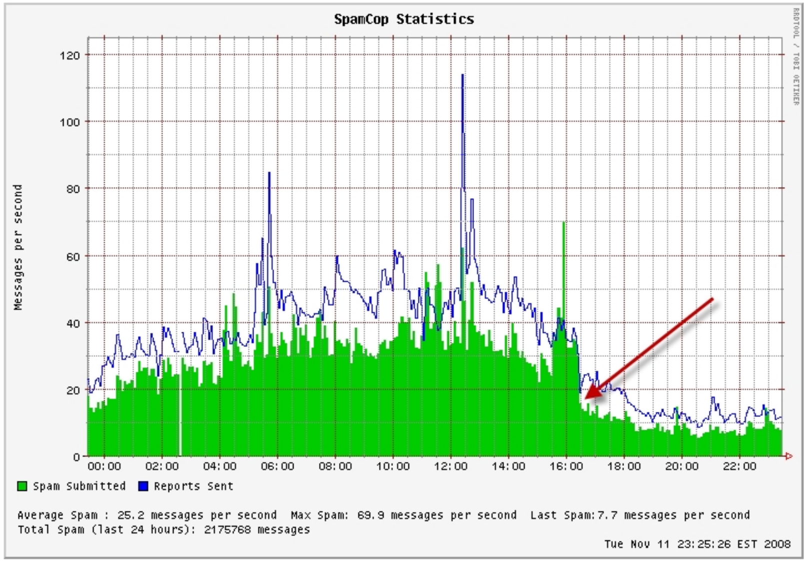
De-Peering

- Atrivo/Intercage
  - Dropped offline
  - Re-peered
  - Dropped again
- McColo de-peering
  - Followed Intercage
  - 75% drop in spam
  - Srizbi connection
  - Rustock connection
  - Re-peered in 4 days

Security Fix Data



SpamCop Data



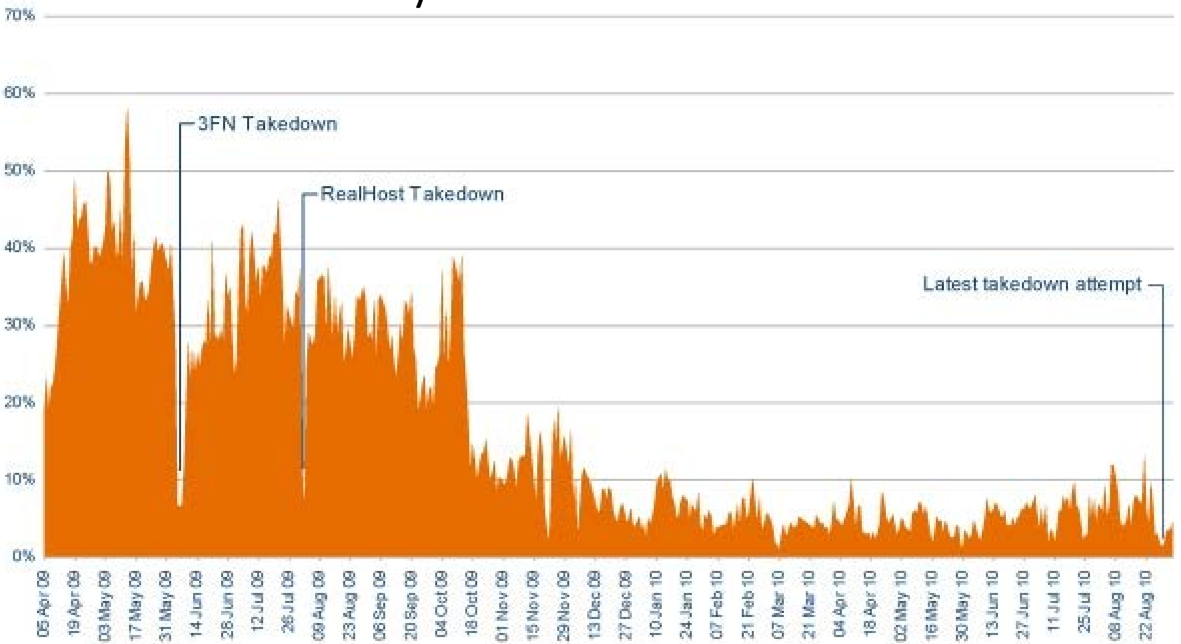
Average Spam : 25.2 messages per second Max Spam: 69.9 messages per second Last Spam:7.7 messages per second
Total Spam (last 24 hours): 2175768 messages

Tue Nov 11 23:25:26 EST 2008

Cutwail

- Prolific spam bot responsible for more than 45% of all spam at its peak (~75 billion msgs/day).
- Disrupted by McColo depeering
- 20 out of 33 C&C Servers disabled by cooperative hosters
- Resurged with 7% of total spam and up to 30x as many infected hosts.

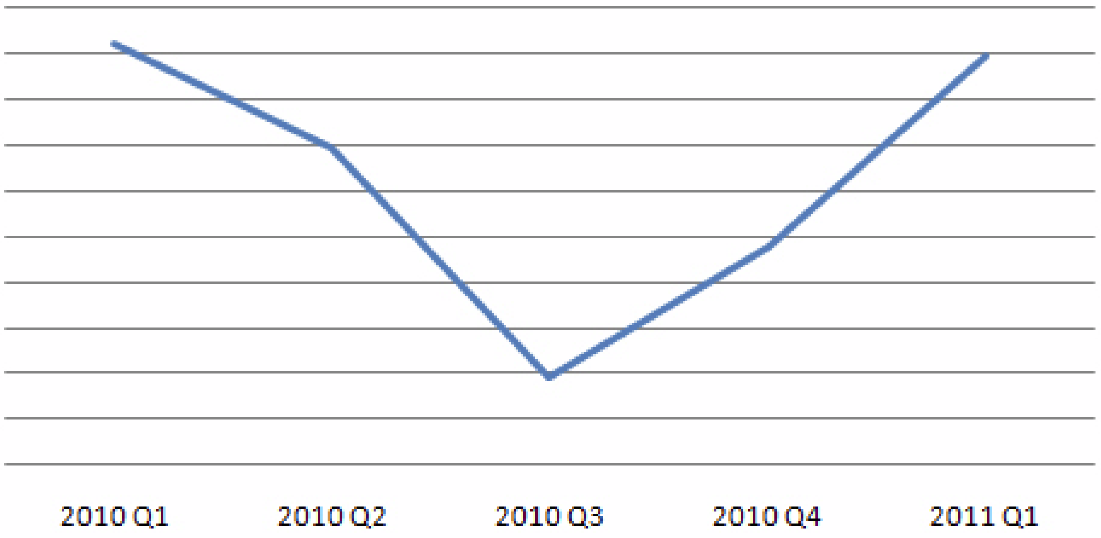
Data from Symantec Hosted Services



Mariposa

- Mariposa
  - Industry partnership with LE and Academia
  - Hoster participation in the investigation
  - Multiple arrests
  - C&C reactivation within 60 days

Data from Trend Micro



Feels quite a lot like this…

Plays Well With Others

- Operation Bot Roast
  - Industry/LE partnerships
  - Broad scale actor attribution
  - Prosecutions of Soloway, Brewer, Ancheta, Downey, Walker and Goldstein
- Operation Bot Roast II
  - Additional indictments on DDoS, Fraud, Wiretap* and other charges
  - Discovery exposes $20+ million in economic losses
- Conficker Working Group
  - Domain control
  - Registrar partnership
  - Intel sharing between industry, academia and law enforcement

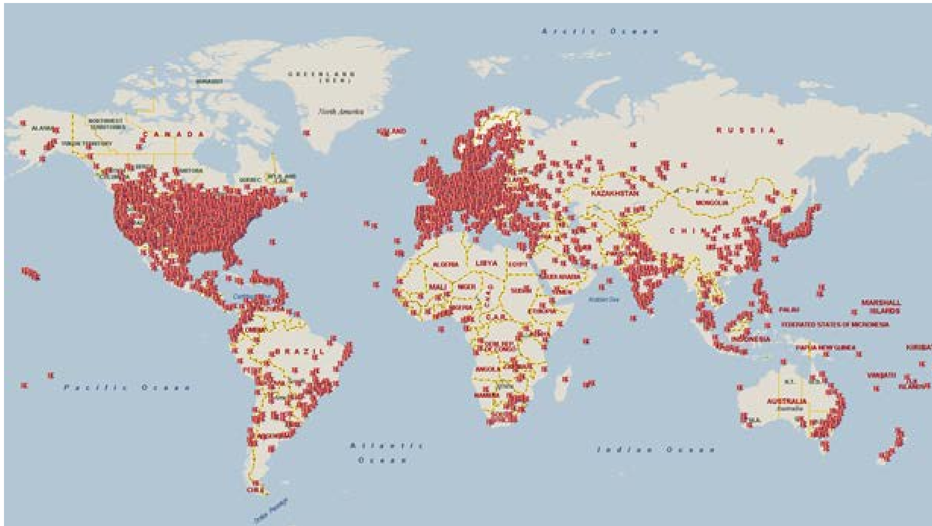
Better Together

- Waledac
  - Takedown of C&C
  - Legal precedent
- Bredolab
  - Command & Control seizure
  - Noftification
  - Arrest
- Rustock
  - Takedown
  - Confiscation of hardware for forensic analysis
  - Cleanup
- Afcore
  - Takedown
  - Shutdown command
  - Coordinated response

Waledac- Operation b49

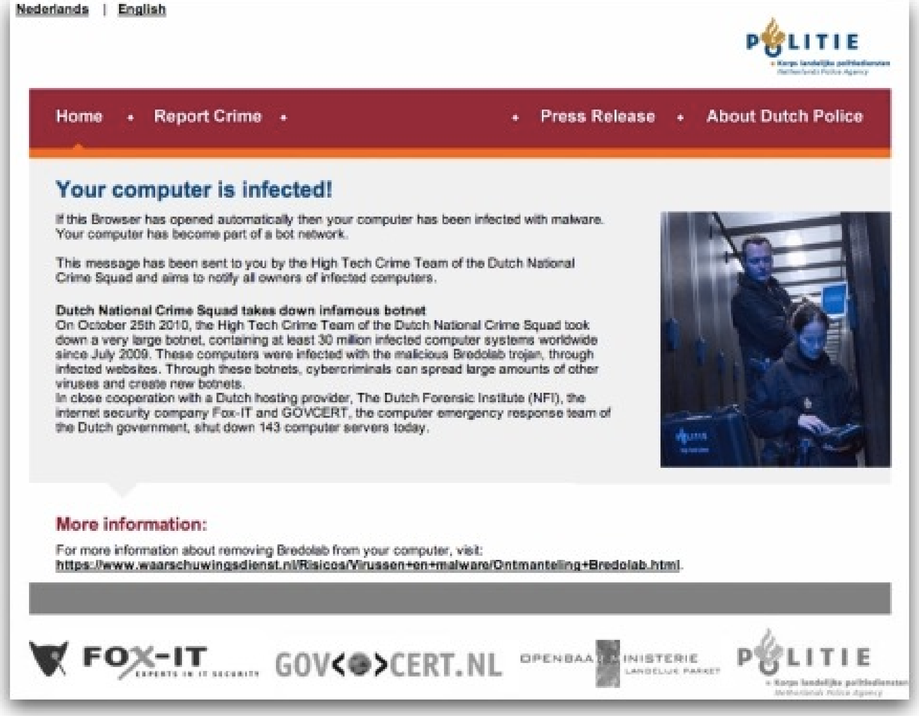
- Novel combination of technical and legal measures.
  - Ex parte TRO after demonstrating damages
  - Partnership with Verisign for domain control of C&C
  - Notification phase
  - Permanent ownership of domains granted after 90 days following outreach to domain owners

- Takedown of C&C
- Legal precedent
- ISP Partnerships



Bredolab

- Coordinated effort involving
  - – Dutch High Tech Crime Unit (THTC)
  - – Dutch hosting provider LeaseWeb
  - – Internet security consultancy FoxIT
  - – GOVCERT.NL
  - – International law enforcement
- Arrest of suspect in Armenia
- Notification



Your computer is infected!

If this Browser has opened automatically then your computer has been infected with malware. Your computer has become part of a bot network.

This message has been sent to you by the High Tech Crime Team of the Dutch National Crime Squad and aims to notify all owners of infected computers.

Dutch National Crime Squad takes down infamous botnet

On October 25th 2010, the High Tech Crime Team of the Dutch National Crime Squad took down a very large botnet, containing at least 30 million infected computer systems worldwide since July 2009. These computers were infected with the malicious Bredolab trojan, through infected websites. Through these botnets, cybercriminals can spread large amounts of other viruses and create new botnets.

In close cooperation with a Dutch hosting provider, The Dutch Forensic Institute (NFI), the internet security company Fox-IT and GOVCERT, the computer emergency response team of the Dutch government, shut down 143 computer servers today.

More information:

For more information about removing Bredolab from your computer, visit: https://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/Ontmanteling+Bredolab.html.

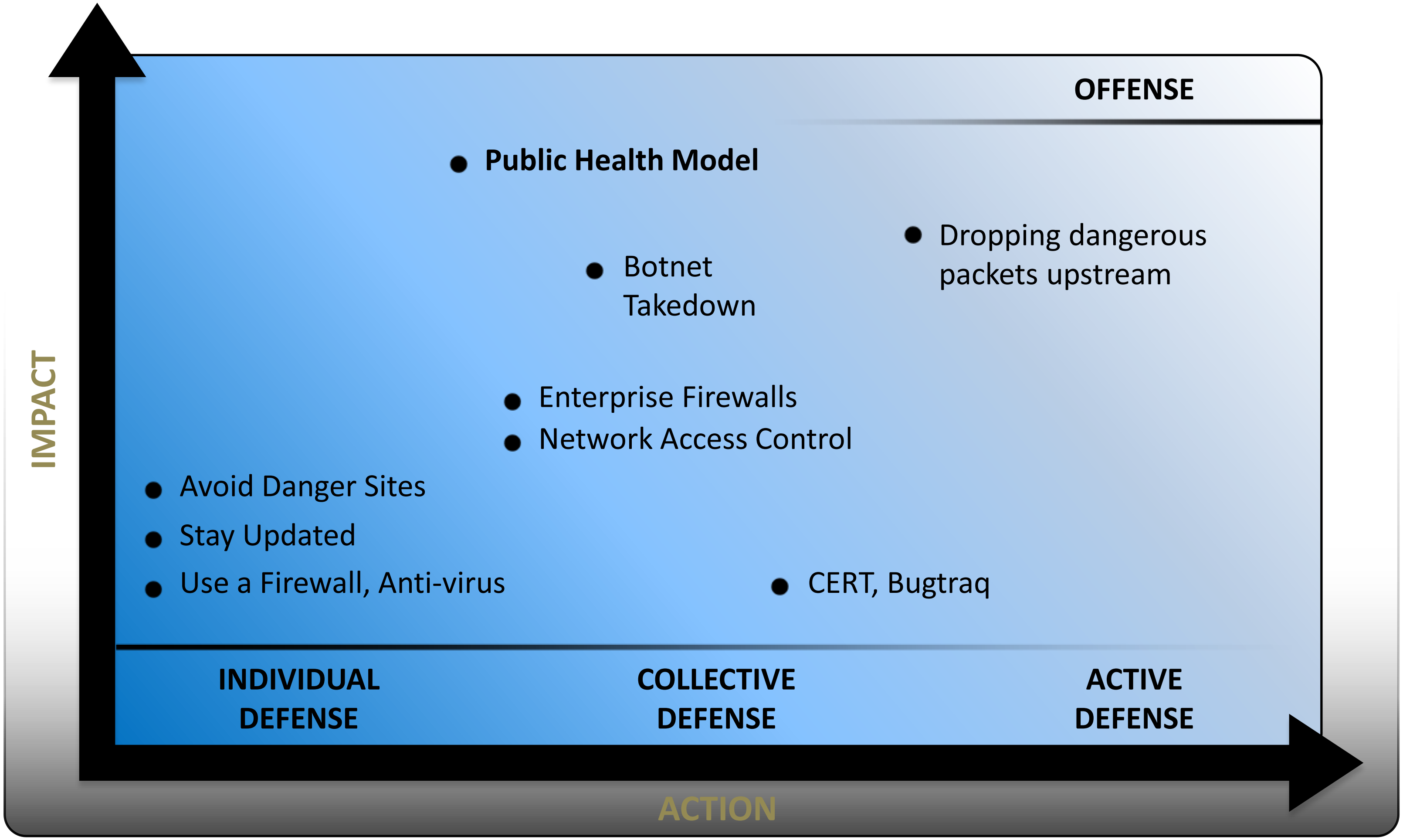
Rustock- Operation b107

- Waledac was a proving ground for us
  - Our success in Operation b49 showed us we could take on larger, more complex threats.
  - We also knew what we could do better in terms of remediation and partnership.
- New legal approach
  - Trademark infringement
    - Microsoft
    - Pfizer’s declaration for the court
    - Lanham Act
- Takedown
  - Ex parte TRO,
  - Coordination with US Marshal Service to seize physical evidence from five hosting providers in seven cities.
  - Confiscation of hardware for forensic analysis
- Cleanup
  - 1.2 Million unique IP addresses
  - Safety Scanner
  - SNDS
  - ISPs and CERTs worldwide

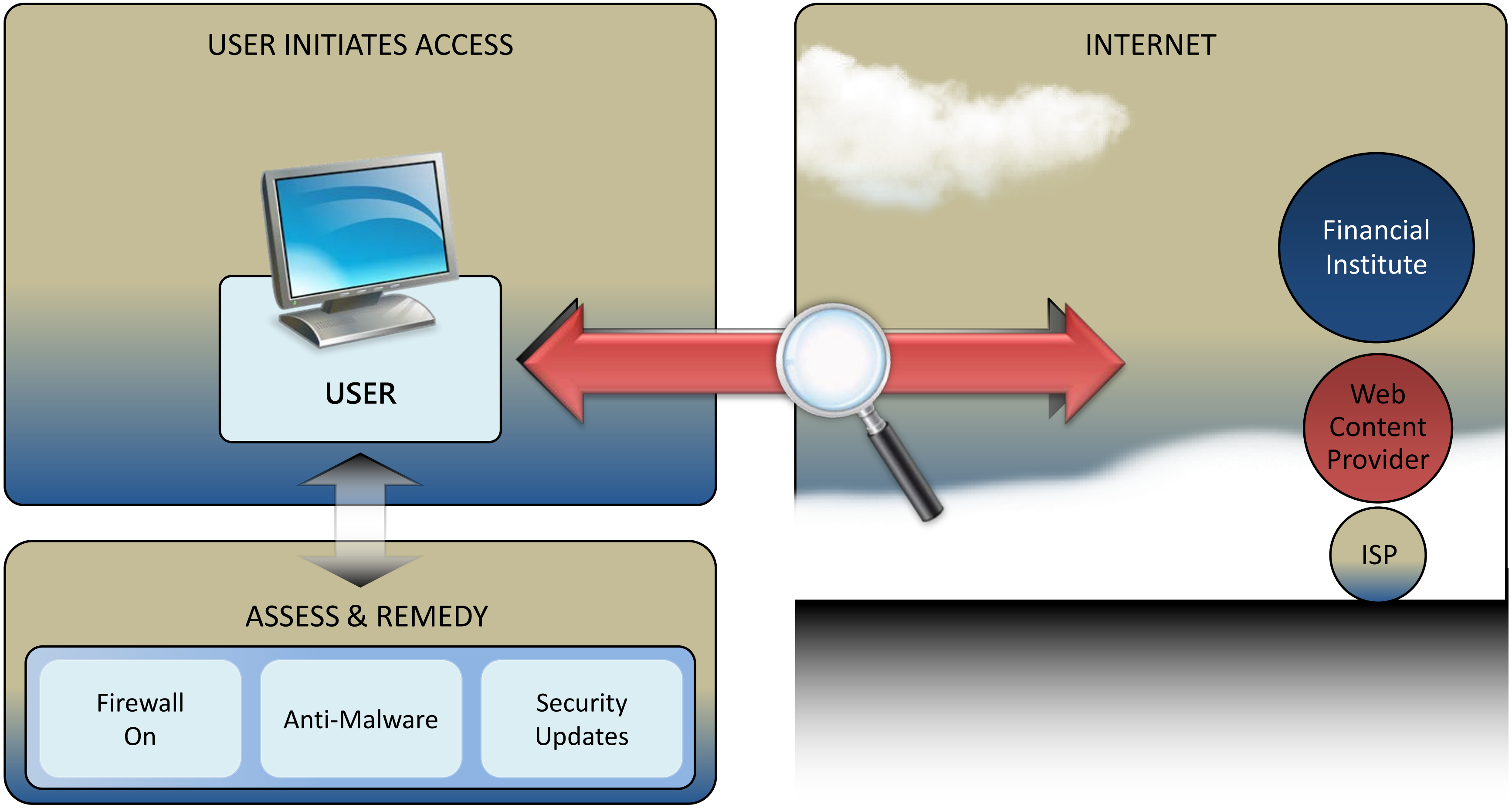
Afcore

- Another example of the combination legal/technical approach
  - Temporary restraining order
  - Seize control of C&C servers
  - Coordinate the release of MSRT with the takedown
  - *Issue a command to unload the bot from memory*
  - Gather consent from victims
  - Remediate
- Partnership with law enforcement
  - Additional variants released just before MSRT release and more updates as the takedown was happening
  - Additional release of MSRT for a broad cleaning of the ecosystem.

Defenses Against Cyber Threat



Internet Health Model: Observing Symptoms



USER INITIATES ACCESS

USER

ASSESS & REMEDY

Firewall On

Anti-Malware

Security Updates

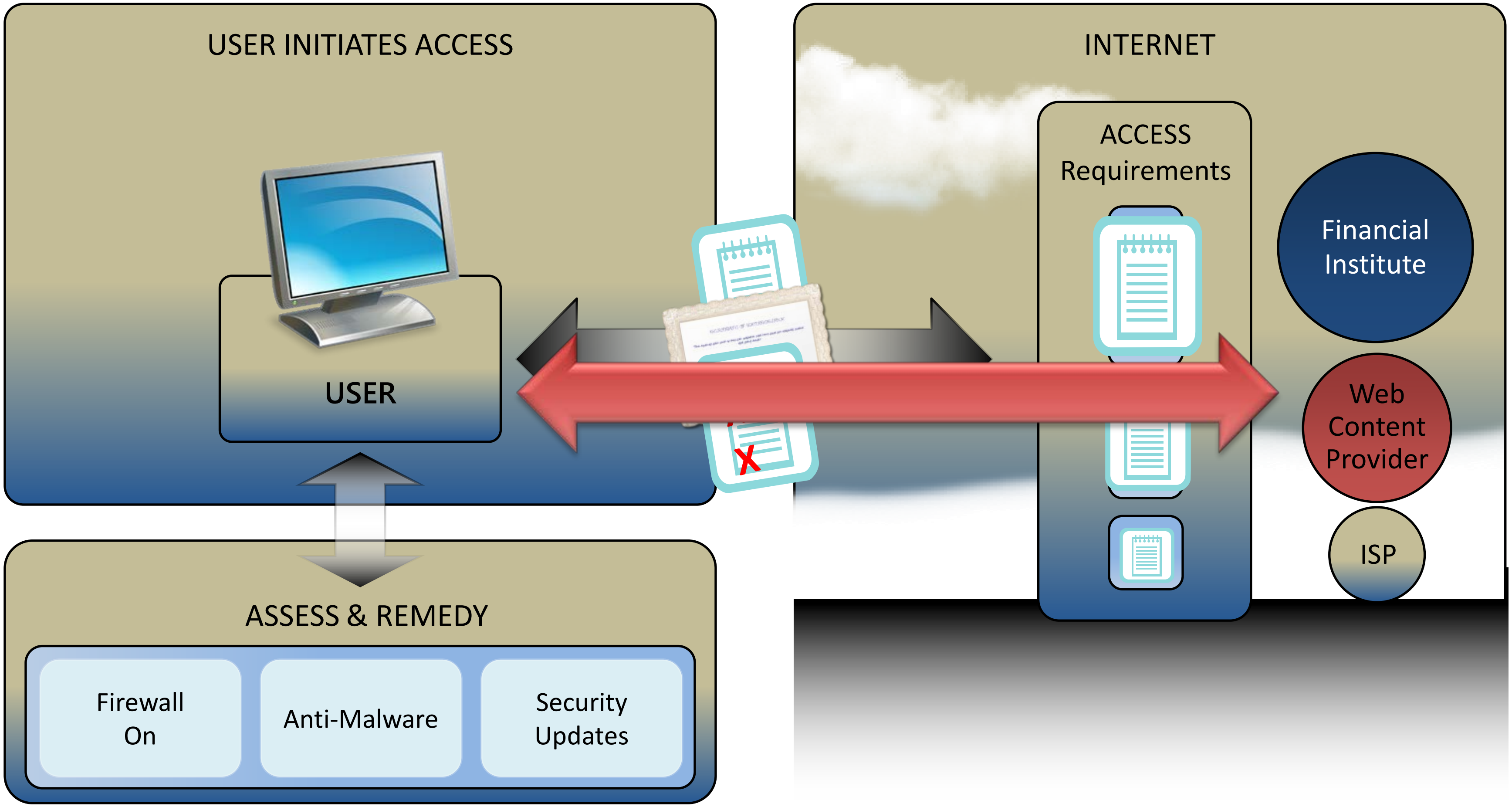
INTERNET

Financial Institute

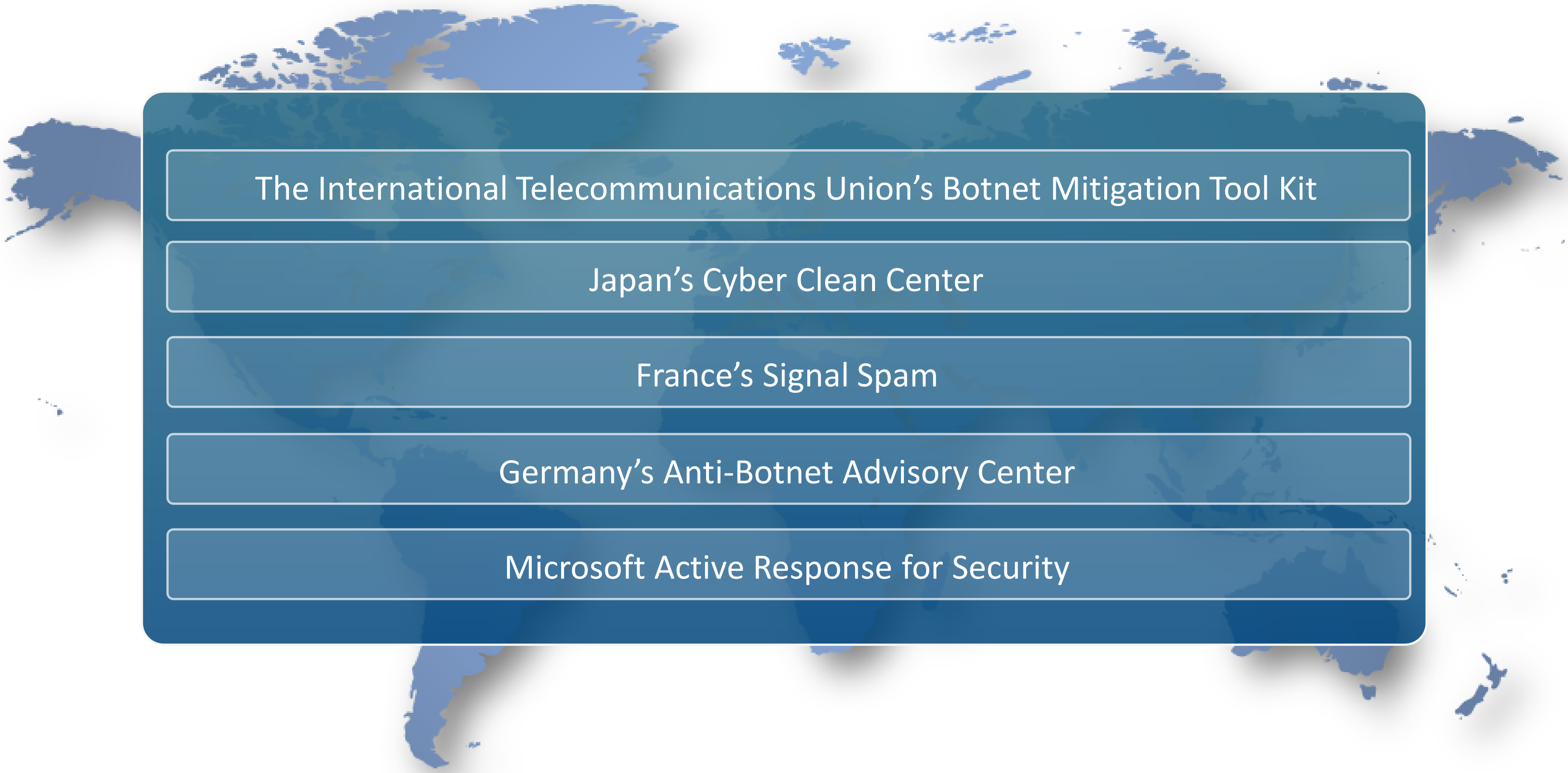
Web Content Provider

ISP

Internet Health Model: Promoting Wellness



Building a Collective Defense



- The International Telecommunications Union’s Botnet Mitigation Tool Kit
- Japan’s Cyber Clean Center
- France’s Signal Spam
- Germany’s Anti-Botnet Advisory Center
- Microsoft Active Response for Security

Helping our Common Customers

Operation b49 Feb 2010

Target: *Waledac*

Cleanup Goal: Build relationships and processes to reach customers

ISP Results

ISP	Reduction
1	97%
2	96%
3	93%
4	78%
5	82%
6	66%

Status

~22,000 infected IPs remaining

~70% reduction world wide

Operation b107 March 2011

Target: *Rustock*

Cleanup Goal: Disinfect systems before attackers regain control

Enhancements:

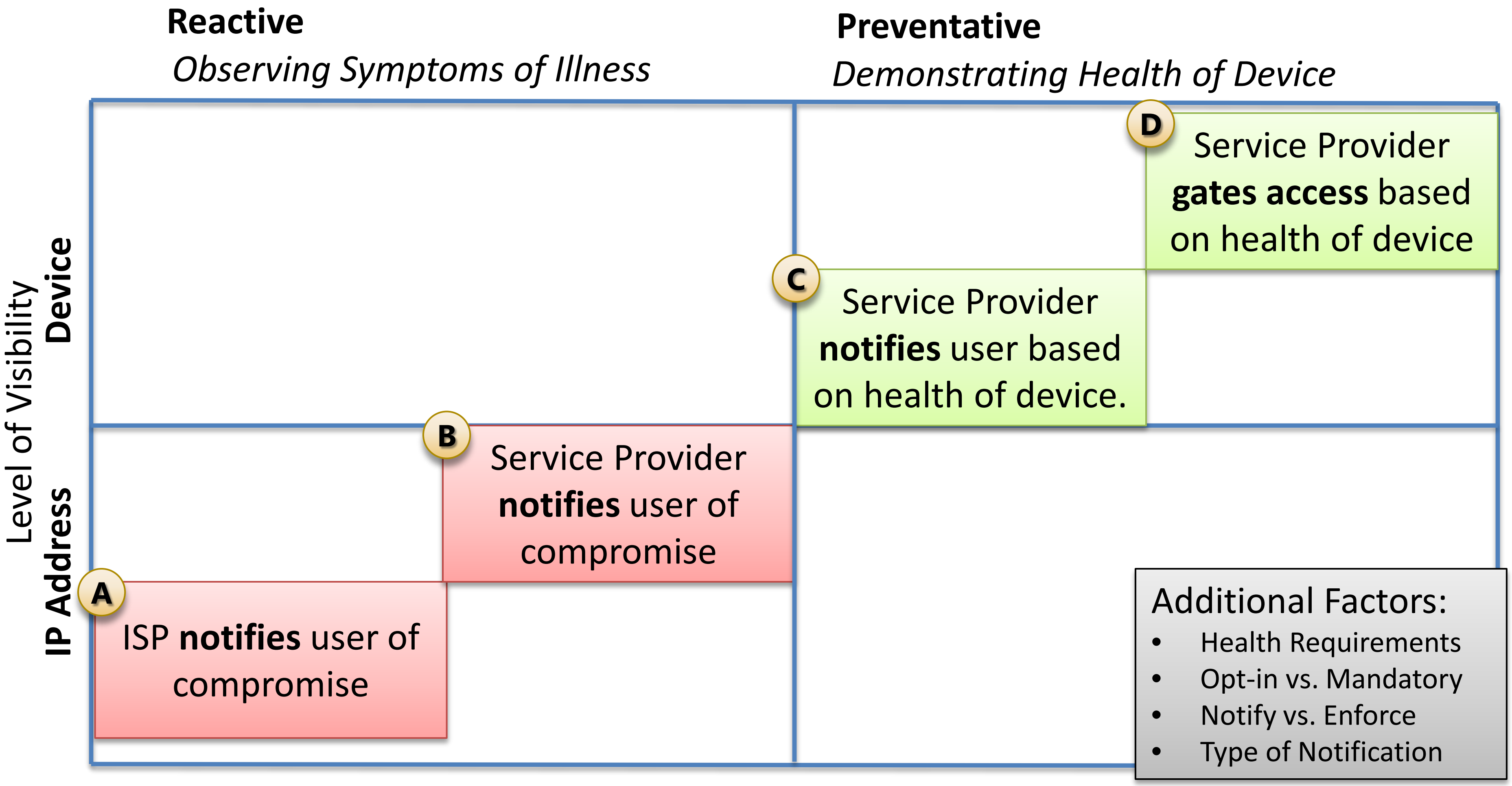
- Expanded Partners
- Removal Tools
- Updated support site

Status

1.2m Unique IP addresses observed in first 7 days following the takedown

ISP Based Remediation Efforts

Vision: *Improve and maintain the health of endpoints connected to the network to create confident customers and grow the information society.*



Reactive

Observing Symptoms of Illness

Preventative

Demonstrating Health of Device

Level of Visibility

Device

IP Address

A ISP **notifies** user of compromise

B Service Provider **notifies** user of compromise

C Service Provider **notifies** user based on health of device.

D Service Provider **gates access** based on health of device

Additional Factors:

- Health Requirements
- Opt-in vs. Mandatory
- Notify vs. Enforce
- Type of Notification

Rustock Progress

Remediation phase

- Directed engagement with ISPs and CERTs
- Delivery of Tools
- Ongoing delivery of IP Data & Timestamps for infected systems
- Legal agreements allowing for redistribution of the Microsoft Safety Scanner in a walled garden

ISP	Reduction
1	69%
2	56%
3	51%
4	49%
5	49%
6	45%
7	34%
8	32%
9	32%
10	31%

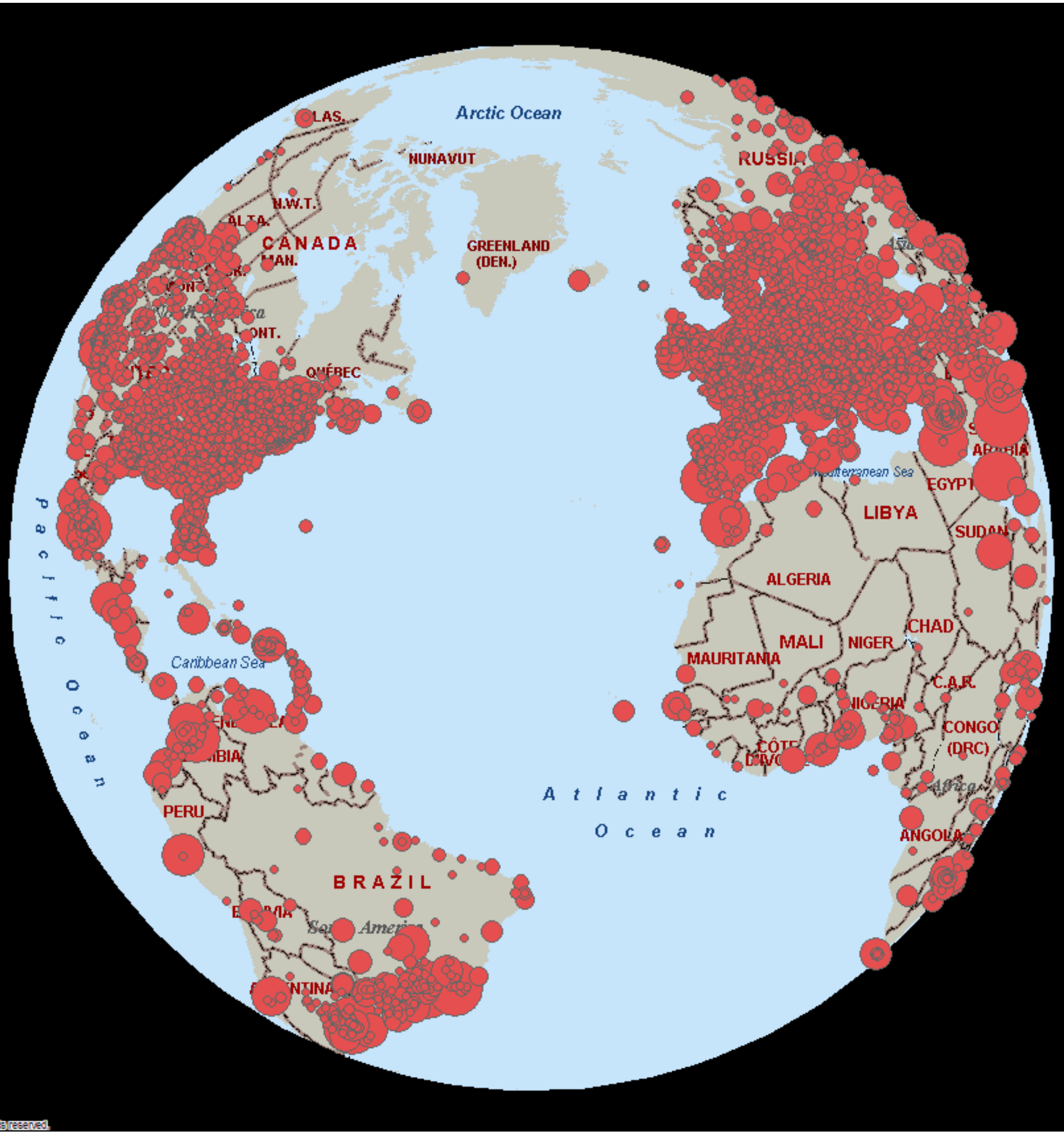
Country	Reduction
1	81%
2	69%
3	68%
4	67%
5	66%
6	64%
7	56%
8	54%
9	54%
10	53%

Additional investigation

- Forensic analysis of C&C hard drives
- Involved parties identified
  - Hoster
- Webmoney
- Notification

Additional collateral

We’re Not Done Yet…



Call to Action

- Solve hard problems in customer notification and remediation
  - Scam proof communications
  - Reliable cleaning tools
- Create next generation collective defenses
  - Device health technologies to prevent infections
  - Definition and measurement of healthy devices
- Share intelligence about infected nodes within an ASN with the ASN owner
  - Provide tools for remediation.
- Leverage SNDS

Whack-a-Mole 2.0

One more thing…

Resources

- http://support.microsoft.com/botnets
- http://www.microsoft.com/security/scanner/en-gb/default.aspx
- http://www.microsoft.com/av
- http://blogs.technet.com/mmpc
- http://www.microsoft.com/sir
- http://blogs.technet.com/ecostrat
- http://postmaster.live.com/snds

- Facebook
  - Microsoft Malware Protection Center
  - Microsoft Digital Crimes Unit
- Twitter
  - @MicrosoftDCU
  - @msftmmpc
  - @jwill_ms

Microsoft®

Be what's next.™

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.