



McAfee®

Web 2.0 and Data Protection

Paul Tsang

Security Consultant

McAfee

Criminal Motivators



For Profit



(Credit Cards, PII,
Criminal Infrastructure)

Cyber Warfare



(National Infrastructure,
Defense)

Targeted Attacks

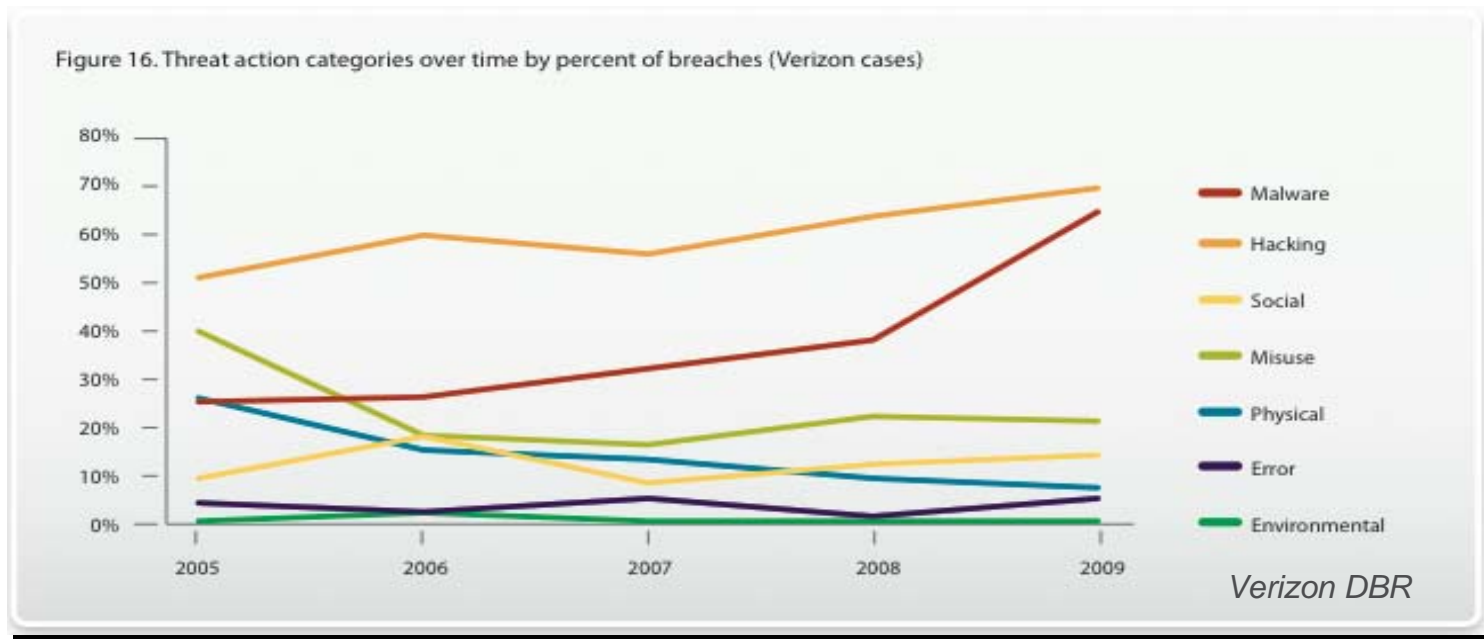


(Nation-State Secrets,
Trade Secrets)

Why Change Tactics?



- Current Malware at an All Time High
- Network Intrusion & Data Exfiltration
- Why Should Attackers Change Tactics?



#1 Because Technology is Changing



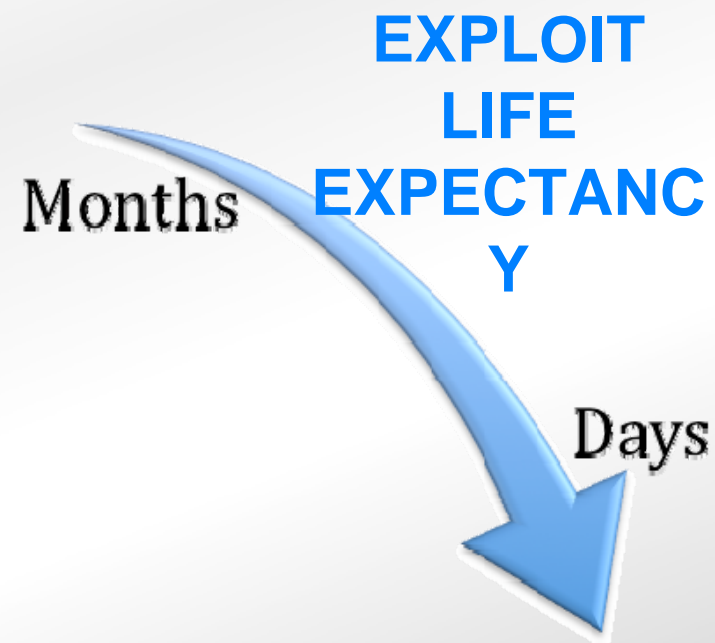
Exploit Mitigation

- Protected Heap
- Stack Cookies
- DEP & ASLR
- SafeSEH

Mature Management

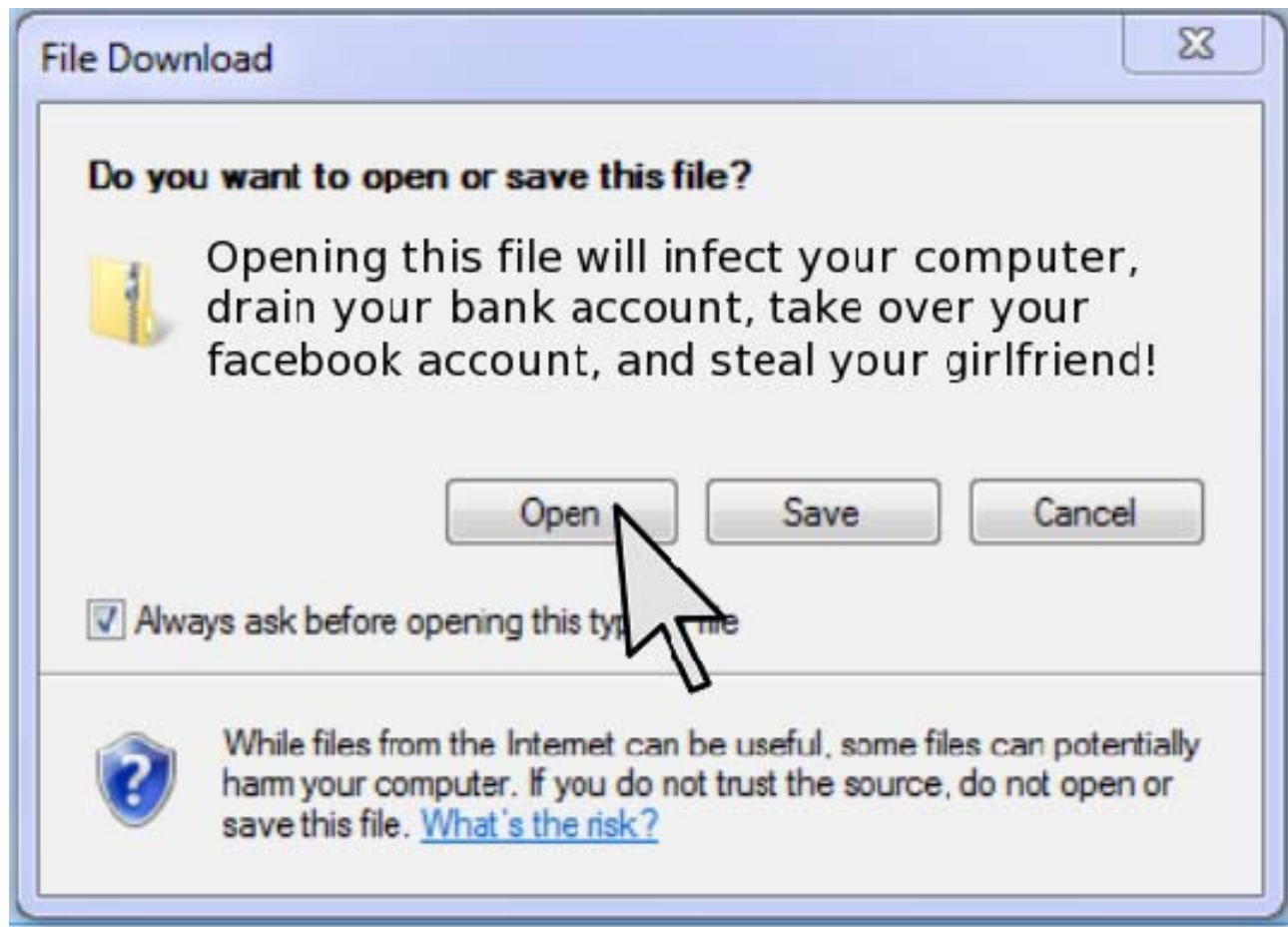
- Patch Mgmt
- Vulnerability Mgmt
- Group Policy
- IR & Forensics

- Growing Complexity
- Longer Time to Develop
- Shorter Lifespan
- Criminal ROI is Shifting
- Shift to Targeted vs. \$\$\$\$



Mass Malware Continues to Exploit the Weak Link ...

... the End User



#2 Because We Are Changing



Mac OS X Potential?



- 2010Q1 - 2.94M Macs Sold
- 33% Increase Over 2009Q1
- User Base Includes Big Targets
 - Corporate Executives
 - Technology Companies
- Immature Management
 - “Anti-Virus is Not Needed”
 - Lack of Central Management
 - Corporate IR Teams Less Prepared



OSX/Puper.A

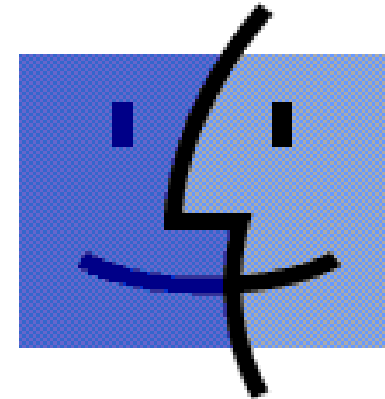
- Discovered Early 2007
- Requires User Installation
- Active for >2yrs
- Prolific on Download sites
- Heart of the Trojan:
 - Malicious Script called “AdobeFlash”
 - Dropped in
/Library/Internet Plug-Ins/



OS X : Predictions

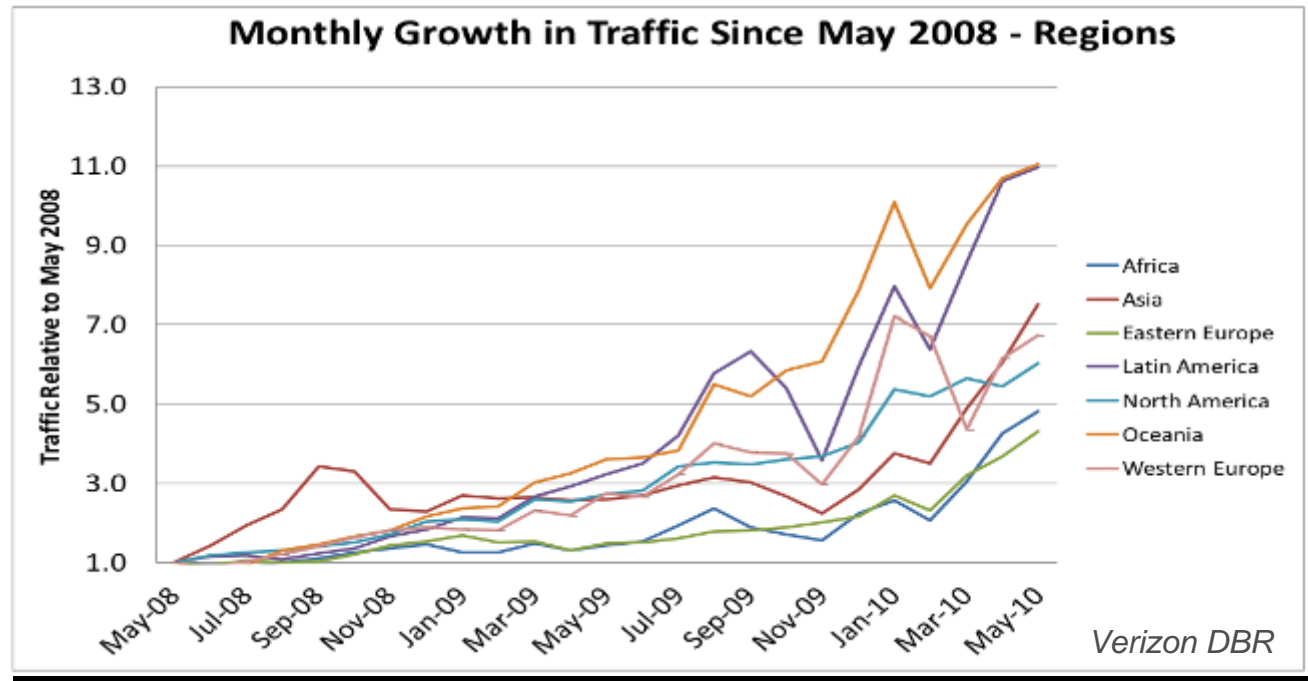


- Misconception of Invulnerability
- Unprepared for Sophisticated Attacks
- Extended Exploitation Before Discovery
- Market Share May Draw “For Profit”
- Greater Potential for “Targeted Attacks”



Mac OS

Mobile Potential?



“Number of smartphones in use will reach 1.32 billion units in 2013”

Gartner, 12/09

“.. in the next 3 years mobile will surpass the PC as the most common web access device worldwide” **Gartner, 12/09**

“30% of mobile users currently use banking services” **Sybase, 8/10**

My Introduction to Mobile Computing



Circa 1990

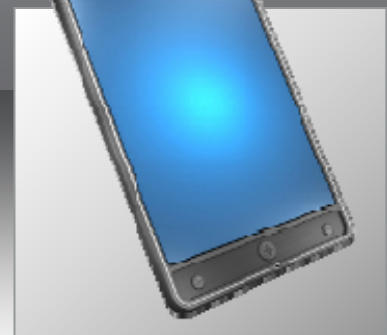
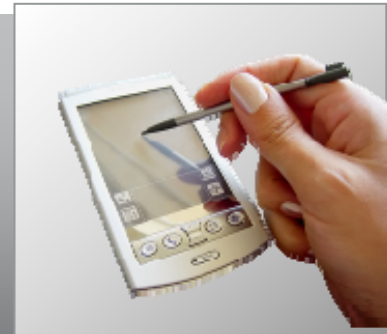
14 lbs

1.44 Floppy Drive

10MB Hard Drive

Retail Price: \$5399 USD

My Mobile Devices Through the Years



Usage Patterns Changing



- Web Sites Formatting For Mobile Devices
- Users Increasing Use Of Smarter Devices To Bank/Control Infrastructure/Access Corporate Apps
- Social Networking Sites
- Email Moving To All Devices
- Teaching Tool
- Access To Corporate Data From Everywhere On/Off-Site



Data Protection requirements



Protect the Device



Protect the User of the Device



Protect the Data on the Device



Don't Let Data Leave the Device



“Windows Mobile game ... dials expensive international phone calls in the background”

iPhone SSH Worms

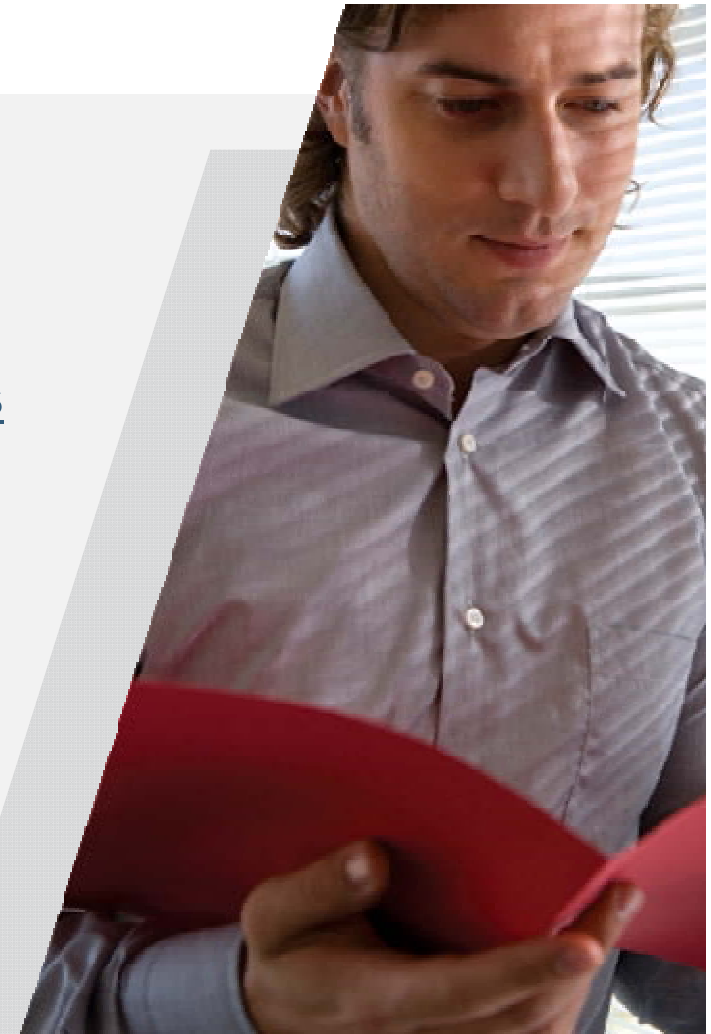
OSX/iPhDownloader.A

OSX/RRoll.C

iPhone/Privacy.A

“Android malware steals info from one million phone owners”

“Banking Trojan hits Android”



Mobile Malware: Predictions



- Initially More Attractive for “Targeted” Attacks
- Shift to \$\$\$ Motive Following Mobile Banking Adoption
- Controlled App Source May Drive Worm Propagation
- IR Capabilities Will Lag Heavily
- Cross Over Malware?
Mobile <-> Desktop



Data Protection for Web 2.0 environment



	Need to Have	Nice to Have
Laptops	Full Disk Encryption Data Loss Prevention Removable Media Control	Pre-Boot Authentication 'LoJack' Solution
USB Media	Encrypted USB Drives	Central Management Password Recovery
Smart Phones	PIN to Unlock Remote Wipe Device Encryption Wipe after X Retries Disallow Jailbreaking	Application Control Over-The-Air Management



McAfee®

Cloud Computing - Global Threat Intelligence
for Individual and Enterprise

Threat Sophistication

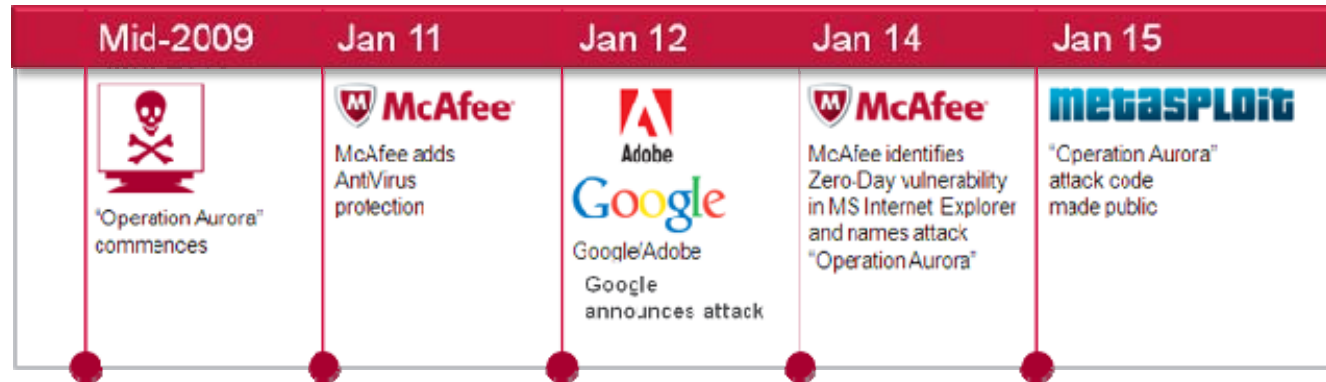


Operation Aurora



- Named By McAfee In Early January
- Long-Term Targeted Attack Against ~20 Major High-tech IT/Security Firms And Defense Contractors
- Exploits A Zero-day Vulnerability In Microsoft IE (CVE 2010-0249)
“Microsoft Internet Explorer DOM Operation Memory Corruption Vulnerability”
- Lures Users To Malicious Websites Via Social Engineering, Installs Trojan Malware On Systems, Uses The Trojan To Gain Remote Access

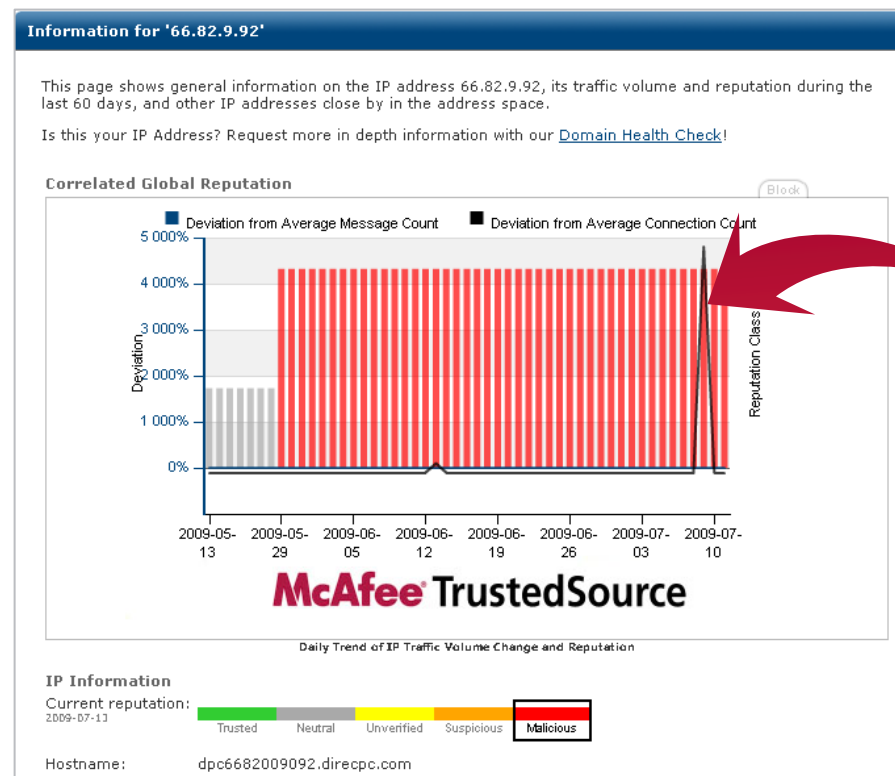
- Uses Remote Access To Gain Entry To Corporate Systems, Access Intellectual Property And Penetrate User Accounts



July 4-10, 2009 Independence Day Attacks

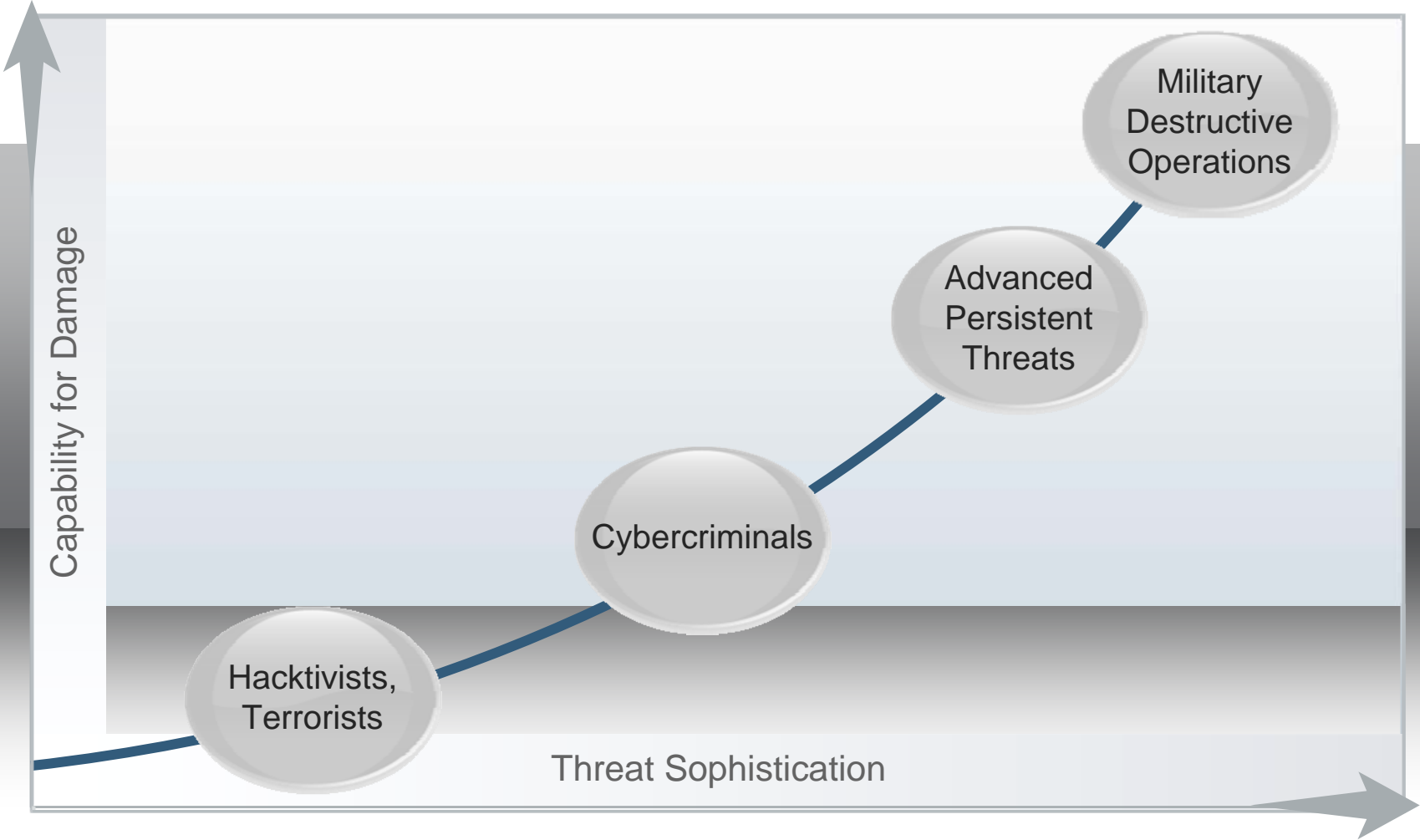


- DDoS on South Korean And US Government Sites
- Botnet Largely In South Korea
- Impact?

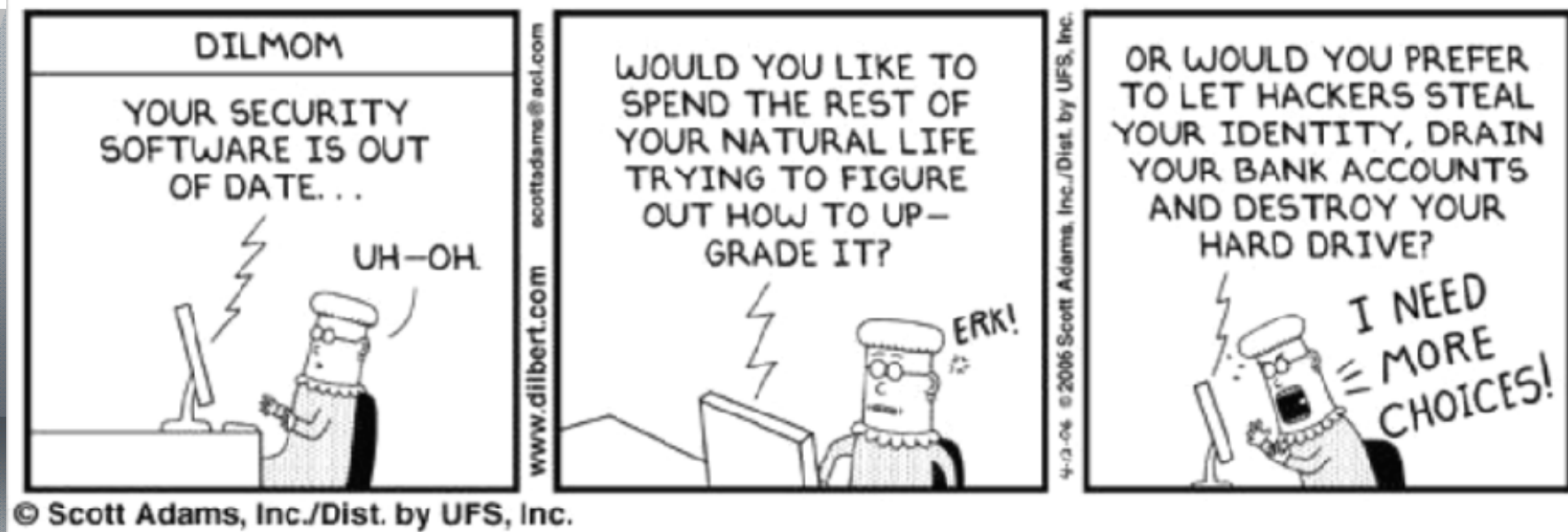


July 4th DDoS

Classification of Attackers



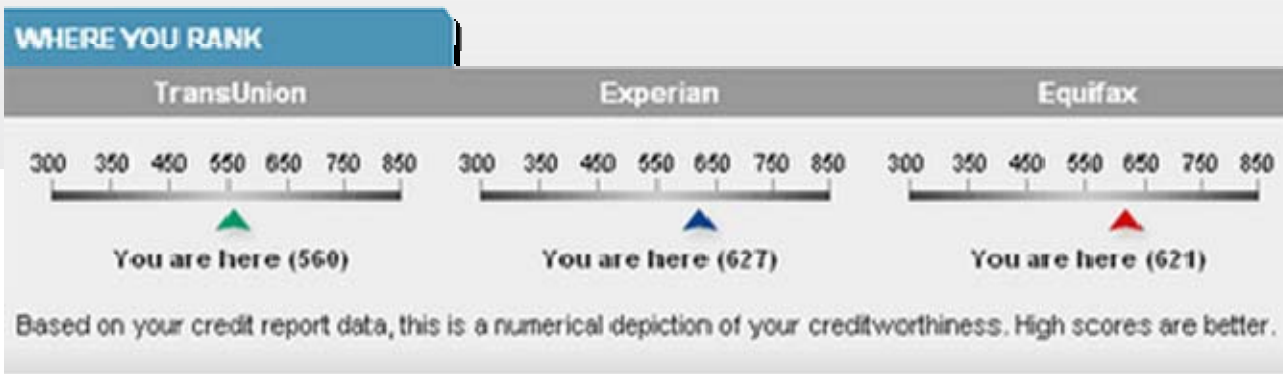
Old Approaches Do Not Work



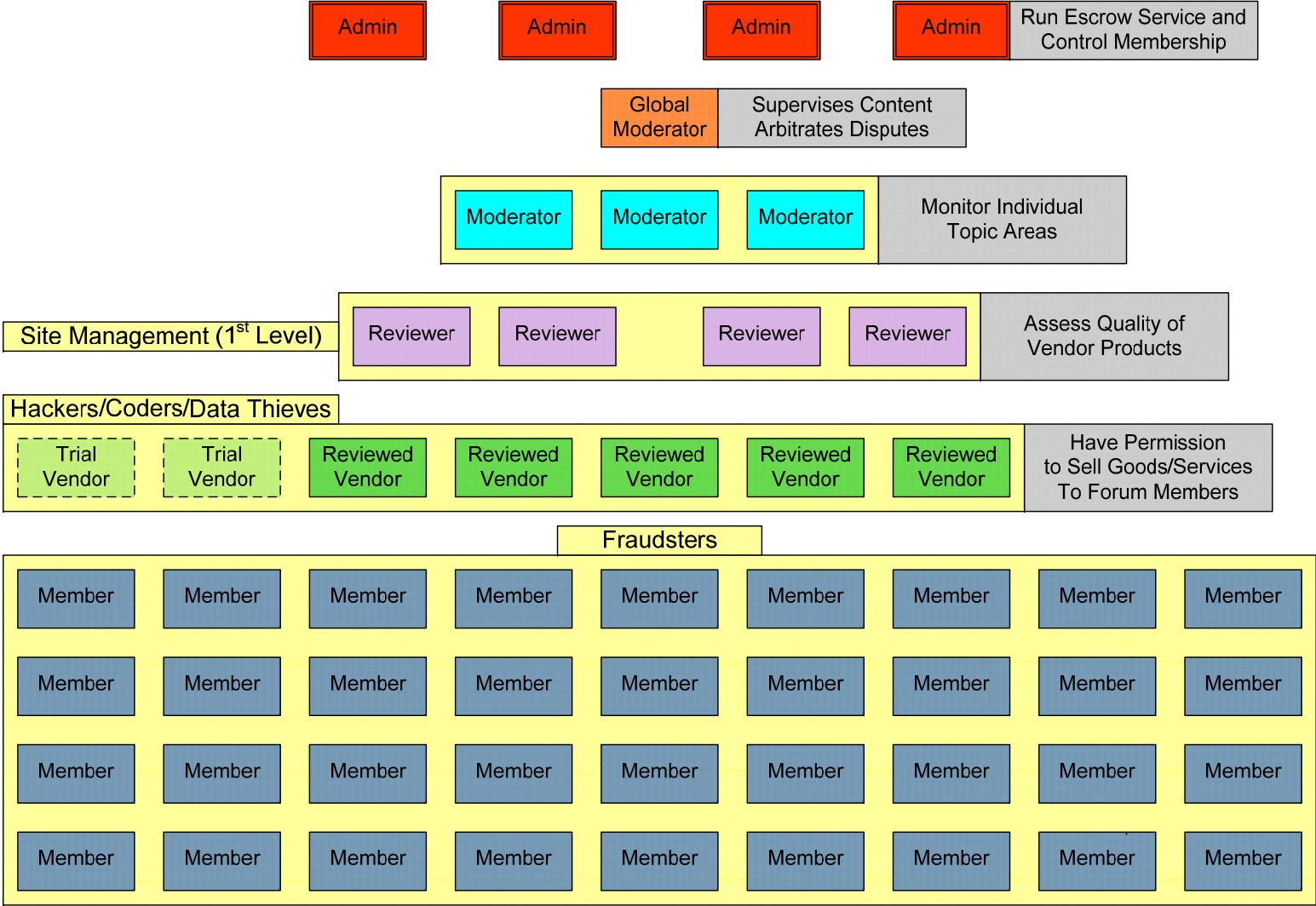
Reputation is Everywhere



Credit Score



Even the Criminals Use Reputations!



McAfee Global Threat Intelligence Reputation System



Threat Intelligence Feeds

Endpoints Appliances Servers Firewalls Other feeds & analysis

McAfee Labs



McAfee ePO

IPS

Firewall

Email

Web

AV

AWL

DLP

Mobile

Collection: Telemetry Scope



Queries

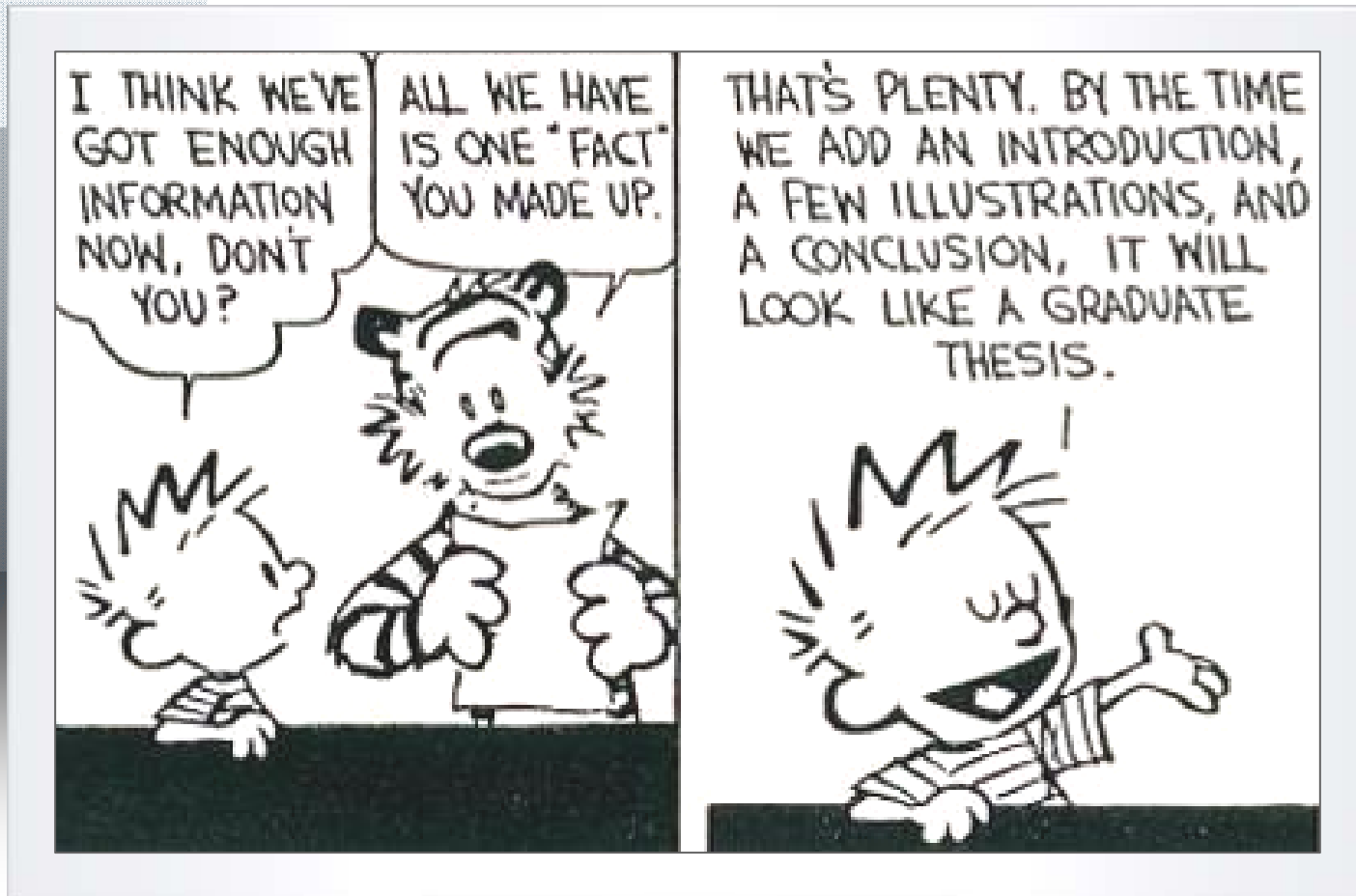
- 2.5B Malware Reputation Queries/Month
- 20B Email Reputation Queries/Month
- 75B Web Reputation Queries/Month
- 2B IP Reputation Queries/Month
- 300M IPS Attacks/Month
- 100M Ntwk Conn Rep Queries/Month
- **100+ BILLION QUERIES**

Nodes

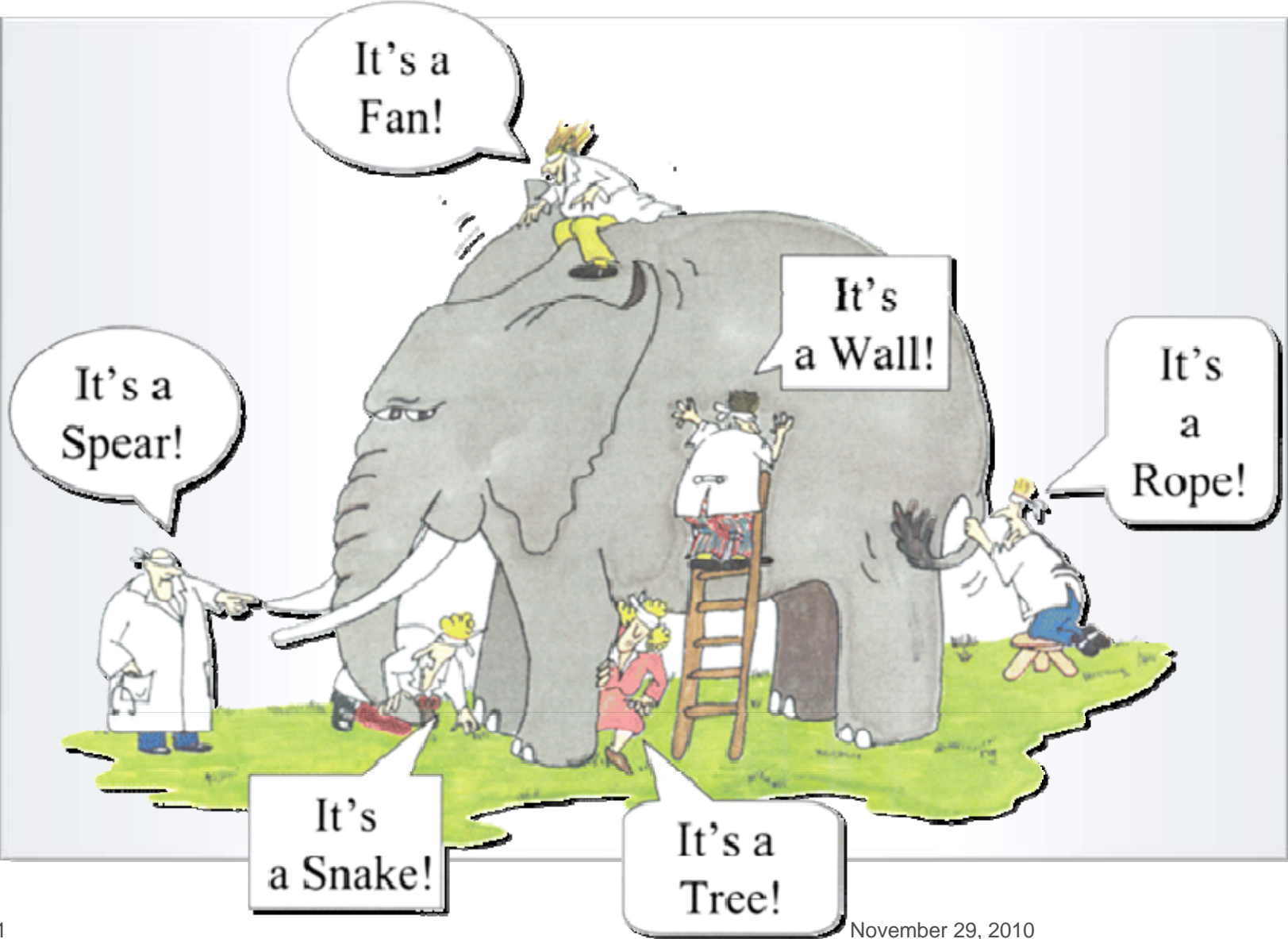
- Malware: 40M Endpoints
- Email: 30M Nodes
- Web: 45M Endpoint and Gateway Users
- Intrusions: 4M Nodes
- **100+ MILLION NODES, 120 COUNTRIES**



Quality of Intelligence



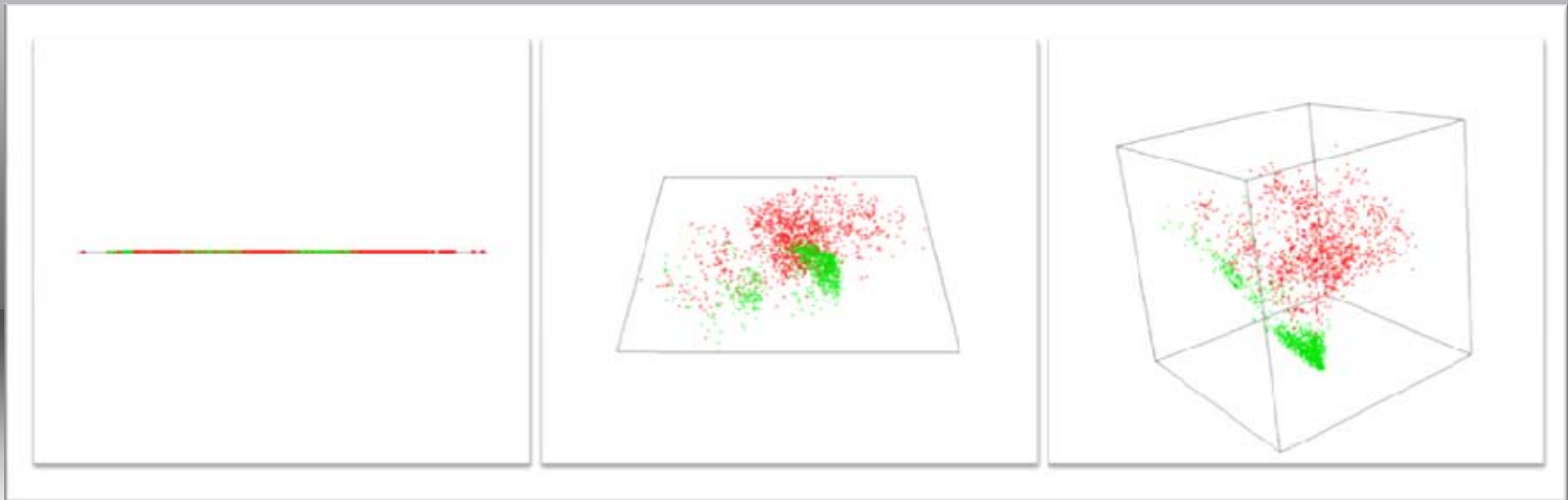
Perspective Matters



More Features → Better Accuracy



Adding Dimensions To Reputation Scores Increases The Confidence Level Of Those Scores



Predictive Mathematical Modeling

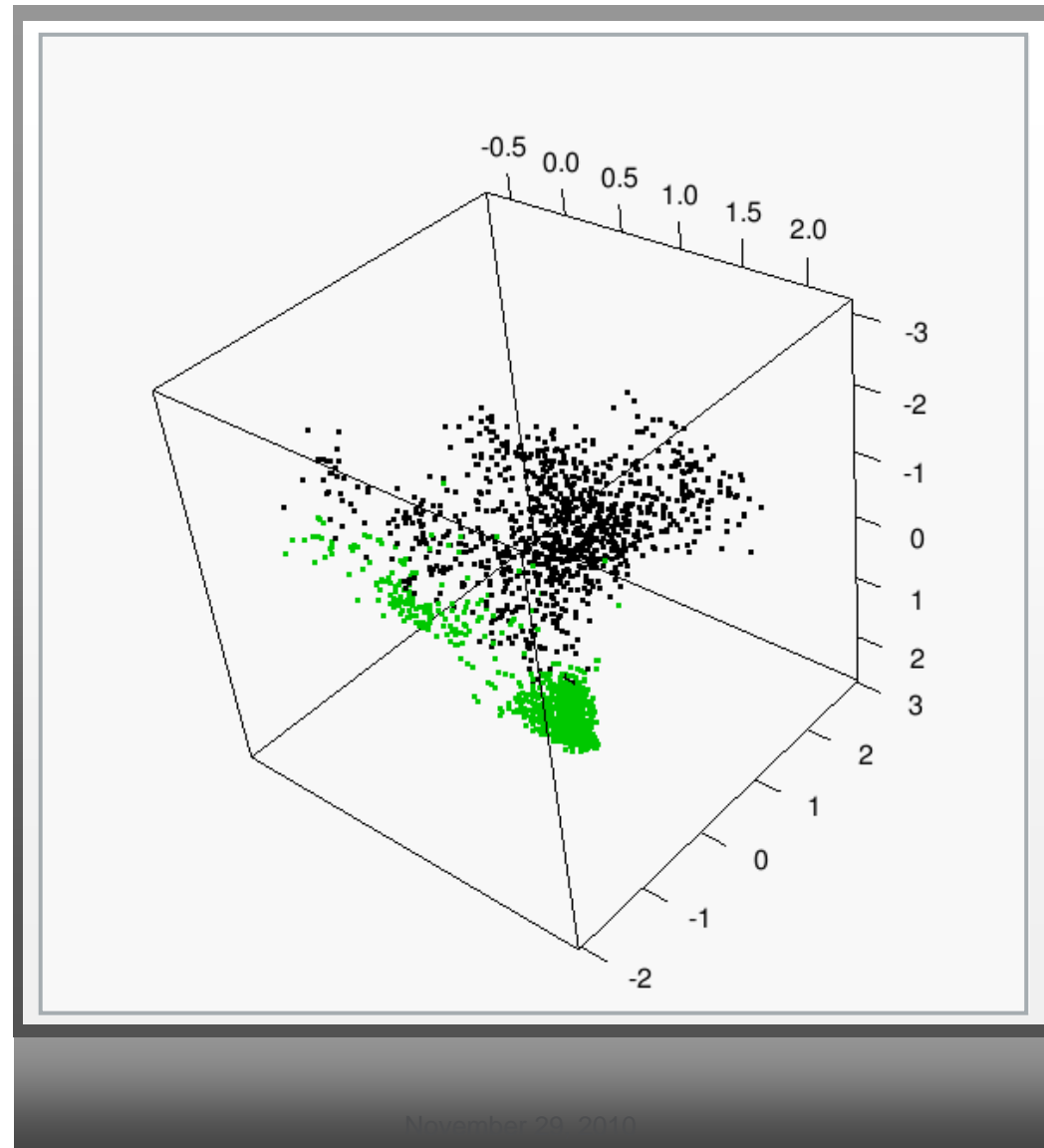
Captures Behavior Not Considered By Heuristic-Based Systems

Multi-Dimensional Correlation

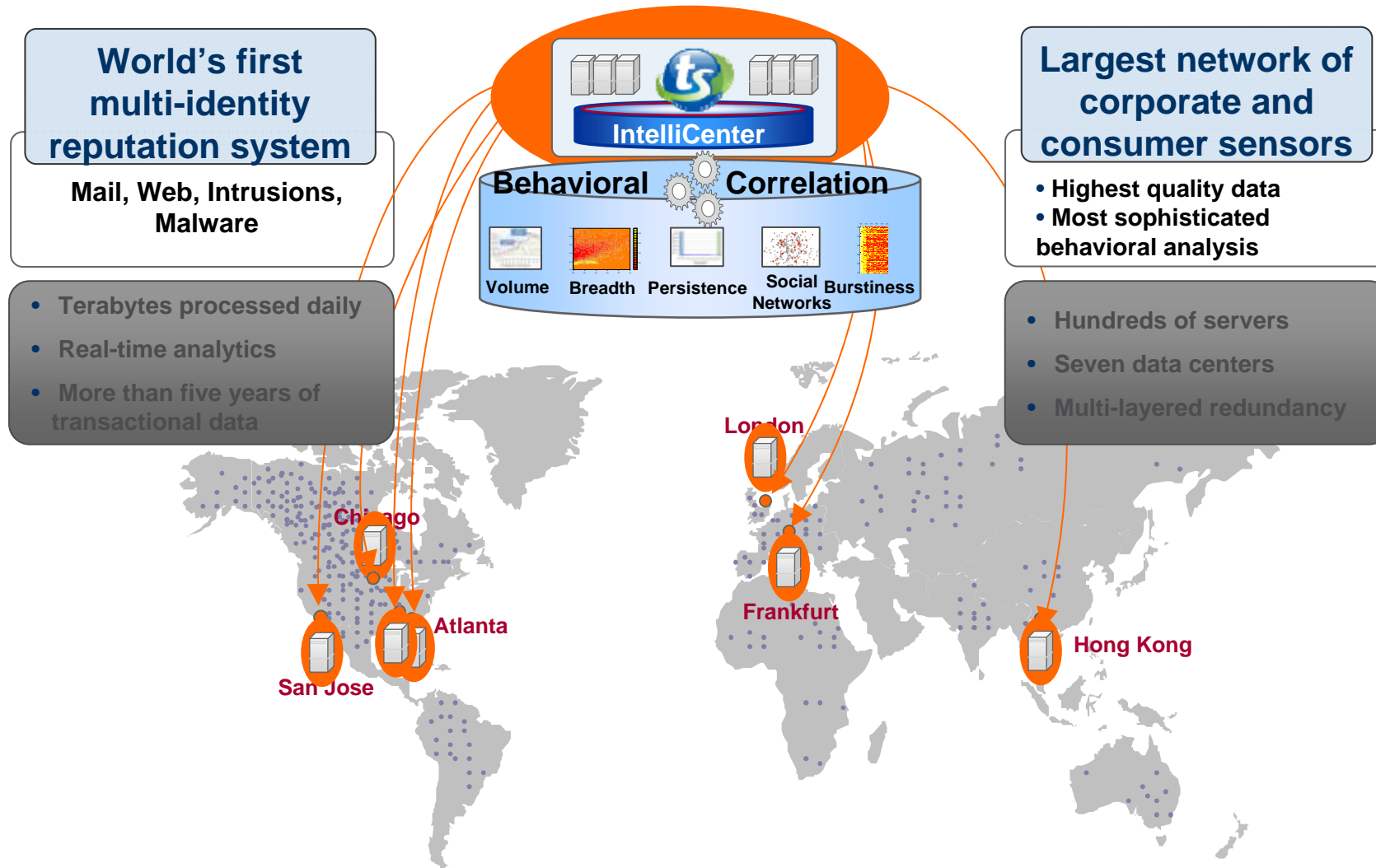
Additional Features Increase Spread For Classification

Real-Time Detection

Knowing More At The Time The First Query Is Sent

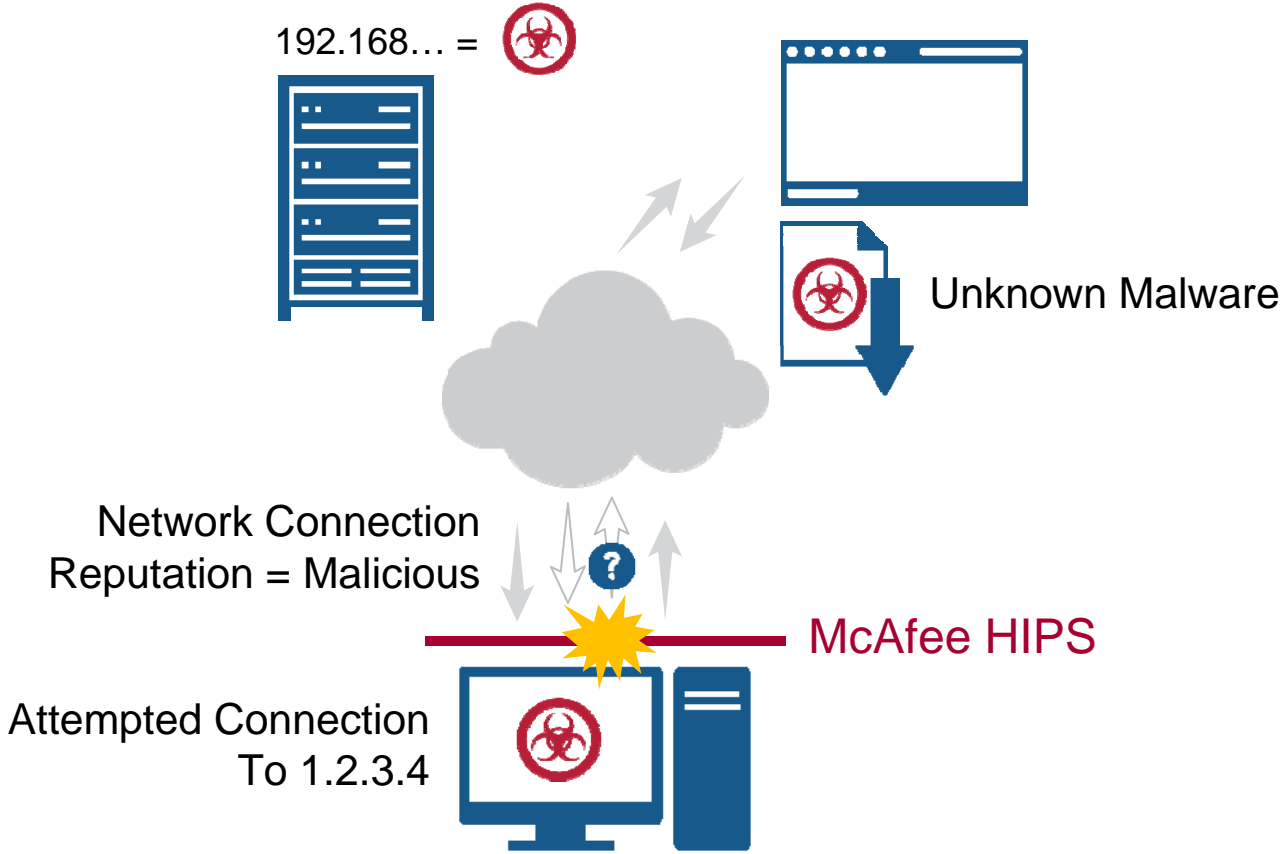


A System That Learns, Reacts, and Shares Knowledge



Reputation in Action

Host Intrusion Prevention vs. Malware



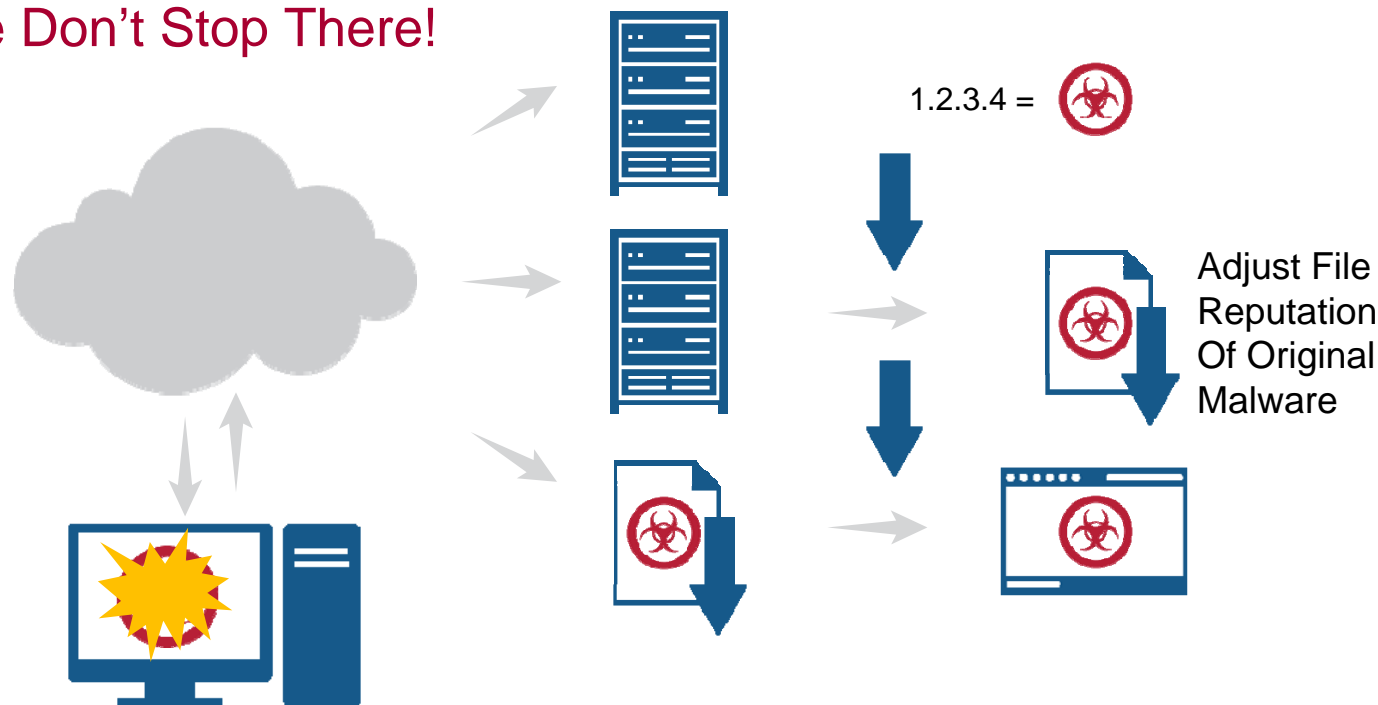
McAfee Host IPS, Using McAfee Global Threat Intelligence Network Connection Reputation, Blocks The Attempted Connection With 1.2.3.4...A Malicious Connection

Reputation in Action

Host Intrusion Prevention vs. Malware, continued



But We Don't Stop There!



Now That We Know The File Is Malware, The Endpoint's Next Cloud Lookup Will Identify It As Such And Our Anti-Malware Will Remove The File

We Also Update Our Systems To Adjust The Reputations Of Other Entities Associated With The Malware Or Malicious Network Connection



McAfee®

Case Study – The many faces of Zeus

What Is Zeus?




- It's a Trojan
 - Credential theft
- It's a bot
 - Can receive commands and updates
 - Can send spam
 - Can be used for denial-of-service (DoS) attacks
- It has a web-based management console
 - Create, manage, and distribute
 - Statistics of infection and success
 - Web forms for operating systems, browsers, and more

Where It Comes From



15-05-2009, 09:20



Special for newbies: Zeus spyware installing!

I do build Zeus 1.2.4.2 + hjects help to set up set help to set up set Special bulk cargo road sesis work for you all offers

The size of the original bildera 71.680bayt New Admin Control Panel

willing to work with the guarantor

Do for \$ 150 build Zeus 1.2.4.2 buider price \$ 250 +Strong Bot Long time life power grabber

I will support your Zeus project any time and consult by any question at and private spoits who interesting pm pe

Sory my bad English i am Rusian but i am understand

ZeusFile Hosting

100% Zeus 1.2.4.2 with back build (back name, build + 5000)

What is ZeusFile Hosting?
ZeusFile is a way of the Zeus Trojan and help support by h3r3n

How does ZeusFile work?
ZeusFile works by actively redirecting traffic from websites to your ZeusFile install page. It will attempt to download and execute the ZeusFile bot on unpatched systems to steal sensitive valuable data. Major file bot is installed on a system it will begin to log all outgoing connections to send malware items.

ZeusFile is capable of the following:

- 1. Log all incoming Internet Explorer (IE) requests
- 2. Log all outgoing HTTP connections
- 3. Log all outgoing POP3 connections
- 4. Log all outgoing SMTP connections
- 5. Log all outgoing IRC connections
- 6. Log all outgoing DNS connections
- 7. Log all outgoing Telnet connections
- 8. Log all outgoing FTP connections
- 9. Log all outgoing HTTP connections
- 10. Log all outgoing HTTPS connections
- 11. Log all outgoing SOCKS connections
- 12. Log all outgoing SSH connections
- 13. Log all outgoing SFTP connections
- 14. Log all outgoing STMP connections
- 15. Log all outgoing Telnet connections
- 16. Log all outgoing TFTP connections
- 17. Log all outgoing VNC connections
- 18. Log all outgoing X11 connections
- 19. Log all outgoing XDMCP connections
- 20. Log all outgoing XMP connections
- 21. Log all outgoing XRPC connections
- 22. Log all outgoing XSPICE connections
- 23. Log all outgoing Xvnc connections
- 24. Log all outgoing Xvncviewer connections
- 25. Log all outgoing Xvncviewer2 connections
- 26. Log all outgoing Xvncviewer3 connections
- 27. Log all outgoing Xvncviewer4 connections
- 28. Log all outgoing Xvncviewer5 connections
- 29. Log all outgoing Xvncviewer6 connections
- 30. Log all outgoing Xvncviewer7 connections
- 31. Log all outgoing Xvncviewer8 connections
- 32. Log all outgoing Xvncviewer9 connections
- 33. Log all outgoing Xvncviewer10 connections
- 34. Log all outgoing Xvncviewer11 connections
- 35. Log all outgoing Xvncviewer12 connections
- 36. Log all outgoing Xvncviewer13 connections
- 37. Log all outgoing Xvncviewer14 connections
- 38. Log all outgoing Xvncviewer15 connections
- 39. Log all outgoing Xvncviewer16 connections
- 40. Log all outgoing Xvncviewer17 connections
- 41. Log all outgoing Xvncviewer18 connections
- 42. Log all outgoing Xvncviewer19 connections
- 43. Log all outgoing Xvncviewer20 connections
- 44. Log all outgoing Xvncviewer21 connections
- 45. Log all outgoing Xvncviewer22 connections
- 46. Log all outgoing Xvncviewer23 connections
- 47. Log all outgoing Xvncviewer24 connections
- 48. Log all outgoing Xvncviewer25 connections
- 49. Log all outgoing Xvncviewer26 connections
- 50. Log all outgoing Xvncviewer27 connections
- 51. Log all outgoing Xvncviewer28 connections
- 52. Log all outgoing Xvncviewer29 connections
- 53. Log all outgoing Xvncviewer30 connections
- 54. Log all outgoing Xvncviewer31 connections
- 55. Log all outgoing Xvncviewer32 connections
- 56. Log all outgoing Xvncviewer33 connections
- 57. Log all outgoing Xvncviewer34 connections
- 58. Log all outgoing Xvncviewer35 connections
- 59. Log all outgoing Xvncviewer36 connections
- 60. Log all outgoing Xvncviewer37 connections
- 61. Log all outgoing Xvncviewer38 connections
- 62. Log all outgoing Xvncviewer39 connections
- 63. Log all outgoing Xvncviewer40 connections
- 64. Log all outgoing Xvncviewer41 connections
- 65. Log all outgoing Xvncviewer42 connections
- 66. Log all outgoing Xvncviewer43 connections
- 67. Log all outgoing Xvncviewer44 connections
- 68. Log all outgoing Xvncviewer45 connections
- 69. Log all outgoing Xvncviewer46 connections
- 70. Log all outgoing Xvncviewer47 connections
- 71. Log all outgoing Xvncviewer48 connections
- 72. Log all outgoing Xvncviewer49 connections
- 73. Log all outgoing Xvncviewer50 connections
- 74. Log all outgoing Xvncviewer51 connections
- 75. Log all outgoing Xvncviewer52 connections
- 76. Log all outgoing Xvncviewer53 connections
- 77. Log all outgoing Xvncviewer54 connections
- 78. Log all outgoing Xvncviewer55 connections
- 79. Log all outgoing Xvncviewer56 connections
- 80. Log all outgoing Xvncviewer57 connections
- 81. Log all outgoing Xvncviewer58 connections
- 82. Log all outgoing Xvncviewer59 connections
- 83. Log all outgoing Xvncviewer60 connections
- 84. Log all outgoing Xvncviewer61 connections
- 85. Log all outgoing Xvncviewer62 connections
- 86. Log all outgoing Xvncviewer63 connections
- 87. Log all outgoing Xvncviewer64 connections
- 88. Log all outgoing Xvncviewer65 connections
- 89. Log all outgoing Xvncviewer66 connections
- 90. Log all outgoing Xvncviewer67 connections
- 91. Log all outgoing Xvncviewer68 connections
- 92. Log all outgoing Xvncviewer69 connections
- 93. Log all outgoing Xvncviewer70 connections
- 94. Log all outgoing Xvncviewer71 connections
- 95. Log all outgoing Xvncviewer72 connections
- 96. Log all outgoing Xvncviewer73 connections
- 97. Log all outgoing Xvncviewer74 connections
- 98. Log all outgoing Xvncviewer75 connections
- 99. Log all outgoing Xvncviewer76 connections
- 100. Log all outgoing Xvncviewer77 connections
- 101. Log all outgoing Xvncviewer78 connections
- 102. Log all outgoing Xvncviewer79 connections
- 103. Log all outgoing Xvncviewer80 connections
- 104. Log all outgoing Xvncviewer81 connections
- 105. Log all outgoing Xvncviewer82 connections
- 106. Log all outgoing Xvncviewer83 connections
- 107. Log all outgoing Xvncviewer84 connections
- 108. Log all outgoing Xvncviewer85 connections
- 109. Log all outgoing Xvncviewer86 connections
- 110. Log all outgoing Xvncviewer87 connections
- 111. Log all outgoing Xvncviewer88 connections
- 112. Log all outgoing Xvncviewer89 connections
- 113. Log all outgoing Xvncviewer90 connections
- 114. Log all outgoing Xvncviewer91 connections
- 115. Log all outgoing Xvncviewer92 connections
- 116. Log all outgoing Xvncviewer93 connections
- 117. Log all outgoing Xvncviewer94 connections
- 118. Log all outgoing Xvncviewer95 connections
- 119. Log all outgoing Xvncviewer96 connections
- 120. Log all outgoing Xvncviewer97 connections
- 121. Log all outgoing Xvncviewer98 connections
- 122. Log all outgoing Xvncviewer99 connections
- 123. Log all outgoing Xvncviewer100 connections

How much is ZeusFile hosting?
ZeusFile hosting is \$100 USD per month via Liberty Reserve.
Selling customers can also pay via Western Union but we do not accept it for that time anymore.

What if my hosting time out, will I start lose my money?
If you do not pay this, money before your account expires your logs will be disabled, they will wait until your bank, they will still be running files and logging anything some you will not see but we will be there.

How I can to view a back build?
You can view it on our website: www.zeusfile.com

I am official partner of ZeusFile. You can contact me to get more and purchase the package.

Terms of Service

1. I accept copyright, trademark, and other legal notices.
2. I don't need permission, headers, and other metadata, but you can't see. We don't reply questions here.
3. We accept payment by Liberty Reserve only.
4. We install Zeus on our server and install all the traffic available for free, and we also can install Zeus on your server.
5. We are not responsible if we fail to do anything mentioned on this thread, or else we don't get paid.
6. We don't accept any form of payment, but we accept Liberty Reserve.
7. Our hosting is based on Windows XP/Vista/7.

To buy your package please contact with log email addresses, Only 2 slots available now.

Contact log: log@zeusfile.com

29/04

***** Sell fresh ZEUS logs *****

Selling fresh logs ZEUS 1.2.4.2
With critical resources, a record decline in the price!

Available

11.05.2009-23.05.2009
MIX USA + EUROPE

1200mb = 430 wmsz

Custom

Price from 0.75wmsz/mb.
Any country, from 250wmsz.

Terms of Service

1. Logs I have not touched.
2. Logs are sold in one hand.
3. At the last does not sell, there is a price.
4. After the sale of logs removed.
5. I work on an advance or through the guarantor.

JCQ: [redacted]

zeus is bank-trojan formgrabber.

A Global Zeus



	dateadded (UTC)	Level	status	files online	A record	SDL	country	AS number
narts.cn	2009-08-16 08:38:41	4	online	2	222.73.219.87	Not listed		4812
echarts.cn	2009-08-16 08:34:24	2	online	1	222.73.219.87	Not listed		4812
avanqadershem.com								49093
foxsrl.net								8527
venetassicura.com								31034
66.96.219.165								21788
miodickdvd.us								21844
2k90.cn								32613
2w90.co.cc								32613
unistasta.cn								41947
842812.cn								9929
newadmins.ws								24940
securebizcenter.cn								4847
socks5service.cn								3462
mooshoooh.info								32181
wellingboroughportal.com								27431
electronicsense-search.com								21844
afgolion.net								3462
777-zlo.cn								17816
clicksurfcash.net								49365
tertechet-vings.net								9800
basketballsport.cn								49365
advancement-marketing.cn								4812
cutalot.cn	2009-08-09 09:50:35	4	online	3	219.152.120.118	Not listed		4134
ihateyoujess.com	2009-08-08 09:11:42	4	online	1	212.117.177.233	Not listed		44042
nisdjl4bdjsa7:78dsf.com	2009-08-07 18:36:46	1	online	3	212.174.200.125	SDL75306		9121

Top ten Zeus hosting locations (countries)

# of Zeus hosts	country
109	Russian Federation (RU)
82	China (CN)
77	United States (US)
38	Ukraine (UA)
32	Netherlands (NL)
17	Germany (DE)
14	Latvia (LV)
12	Turkey (TR)
11	Taiwan, Province of China (TW)
6	Italy (IT)

Web-Based Botnet Distribution and Control



...come, admin

:: Browsers :: Systems :: Country :: Referers :: Exploits

...come, admin

:: Browsers :: Systems :: Country :: Referers :: Exploits

Exploits	Loads	Efficiency
MDAC	761	54.59 %
PDF Collab	329	23.6 %
PDF Util	175	12.55 %
Microsoft DirectShow	72	5.16 %
Flash 9	56	4.02 %
PDF GetIcon	1	0.07 %

Admin tools: Upload Clean Clear

Many Ways to Deliver the Malware



- Website redirects
 - Legitimate websites
 - Malicious websites
- Spam
 - Attachments
 - Link spam
- Many forms
 - PDFs
 - ActiveX controls
 - Fake video codecs
 - Zero-day exploits

Combating Zeus



McAfee TrustedSource™

Information for IP Address 83.233.30.101

Hostname: Unknown
 Domain: Unknown
 Current reputation: Suspicious
 Detailed score: 31
 First seen: [redacted]
 Last seen: [redacted]
 Country: Unknown

When information
 Registry: R.I.P.E.
 CIDR range: 83.233.30.0/23
 Description: Broadband2 - VE
 Country: Sweden

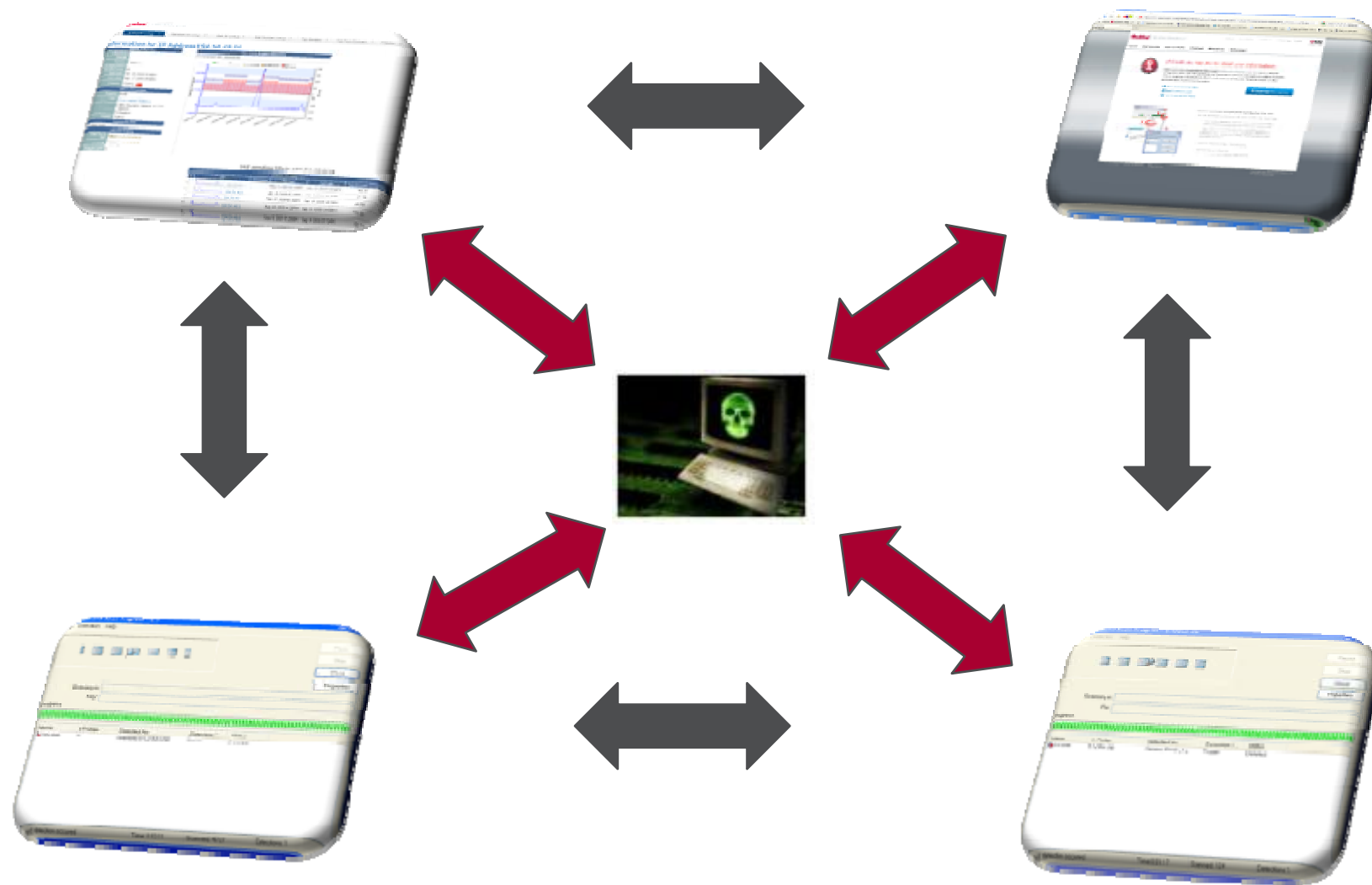
Message volume
 Daily avg 36 days
 Yesterday (+0%)
 Security rules: 0

Daily Trend Volume/Reputation

47 sending IPs in 83.233.30.0/24

#	IP	Hostname	First seen	Last seen	Avg IP score	Country
1	83.233.30.4		Nov 14 2008 07:54AM	Nov 14 2008 08:02AM	0.00	SE
2	83.233.30.10		Aug 25 2009 05:44AM	Sep 15 2009 07:56AM	70.09	SE
3	83.233.30.25		Aug 26 2009 11:42AM	Aug 26 2009 11:42AM	16.07	SE
4	83.233.30.25	8323330025-host.servanet.com	Dec 21 2008 08:04AM	Dec 25 2008 06:39AM	0.02	SE
5	83.233.30.26		Apr 6 2009 11:03AM	Mar 11 2009 07:30PM	0.49	SE
6	83.233.30.36		Mar 19 2009 03:24PM	Sep 14 2009 09:19PM	28.93	SE

Threat Intelligence Yields Predictive Protection



- Intelligence Is Key To An Evolution Of Cybersecurity That Focuses On Situational Awareness
- All Network, Hardware, And Software Assets Must Be Used As Sensors For Intelligence Collection And Analysis
- Global And Local Perspectives Of Threats Are Necessary For Strategic Warning

