

# Locale-specific threats

## Security challenges due to globalization

Anthony Bettini  
McAfee Labs

June 9, 2010



# Agenda



- In the dawn of time
- “Think globally, act locally”
- Audit fatigue
- Local concerns, trends, economics, and even pop culture!
- Vulnerabilities, 0days, and malware
- Leverage what’s already out there
- Partnership
- Wrap up



In the beginning...



© Original Artist  
Reproduction rights obtainable from  
[www.CartoonStock.com](http://www.CartoonStock.com)



Improving Security Together

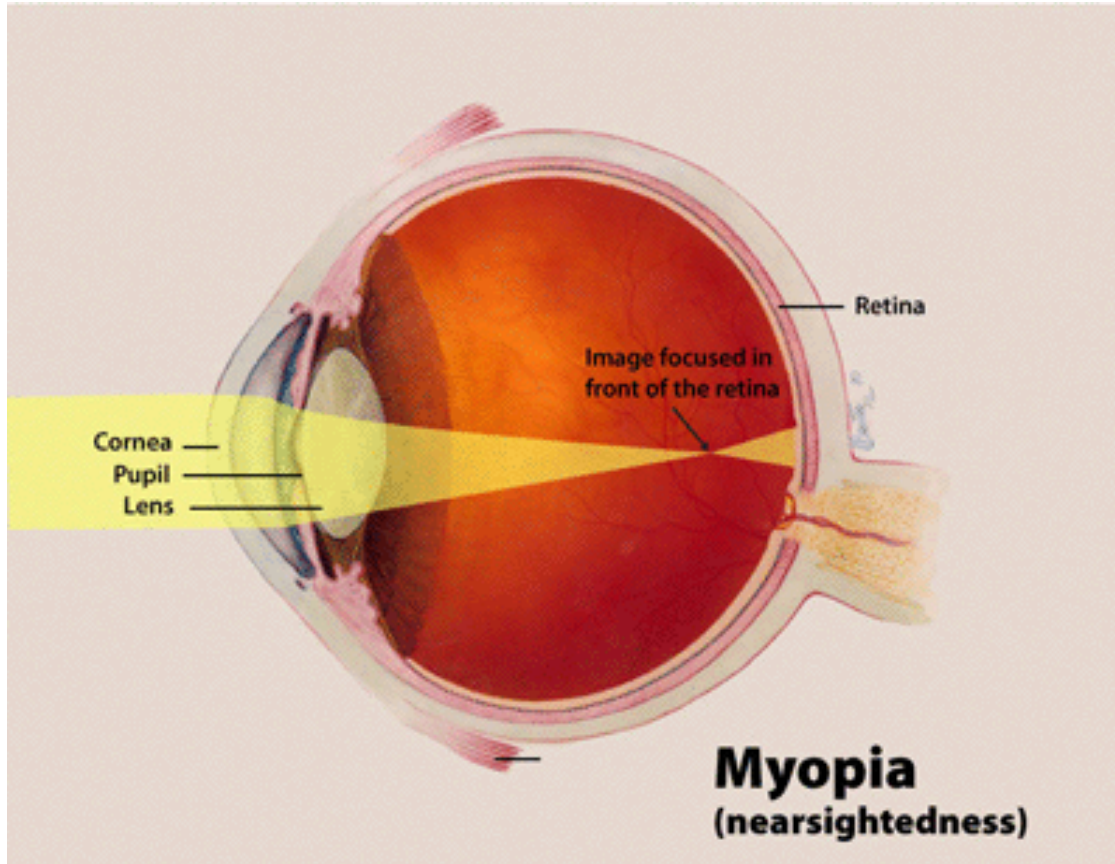
# In the dawn of time



- That's how most business begins, with one headquarters, in one GEO or region
- As the business expands internationally or an IT administrator moves from startups to enterprises, “things change”
- For a long time, both enterprises and even security vendors, were myopic



# (In)security myopia



“Those with myopia see near objects clearly but far away objects appear blurred.”



# What's going on?



- People (and organizations) have a natural tendency to silo or bucketize work, projects, ownership, and responsibilities
- This leads to a virtual myopia, where IT security staff are only responsible for and spending time on the threats most well understood and nearest to them
- Microsoft vulnerabilities seem “more well handled” lately, and Adobe vulnerabilities are “next in line, and being struggled with”
- Flash and Reader aren’t “new risks”, they have been risky for ages



# Are the Adobe threats of late an ocean?



- More likely a wave than an ocean
- If focused on too heavily, certainly a case of myopia could be developing
- What other waves could be causing rising tides in the near future?

“A rising tide lifts all boats.” – President John F. Kennedy



# Threats are more like waves than oceans



- Waves hit land, recede, and repeat
- Some turn into hurricanes or tsunamis
- There's always more coming
- They are all a bit similar and all a bit different
- Some will turn into rising tides, others will fizzle out
- Be ready for surprises!





# “Think globally, act locally”



- May apply well to environmental politics, but this line of thinking only enhances myopia relative to IT security
- Unfortunately for people in IT security (vendors and enterprises) a more apt quote could be “Think globally and locally, act globally and locally”
- What does all this mean?





# Survey says...



- In 2009, McAfee surveyed many of our thousands of risk and compliance as well as IPS (both network and host) customers to gage which international threats were at the tops of our customers minds.
- The question read:
  - “McAfee runs into threats in the field that are specific to a region, geography, country or language. How would you prioritize threat coverage, language support, and regulatory compliance for the following countries?”
- Alphabetically shown here, but randomly sorted to survey participants, the choices were:
  - Brazil, China, France, Germany, Japan, Korea, Mexico, and Russia



# Are the Adobe threats of late an ocean?



- The top choices, consistently were:
  - #1 China (Average of 50% of all surveyed chose China #1)
  - #2 Russia (Average of 25% of all surveyed chose Russia #2)
- All other choices had mixed non-significant rankings
- What does this really mean?



- Proper handling of locale-specific threats are not just about...
  - Translating documentation into Danish
  - Blocking SPAM written in Simplified and Traditional Chinese
  - Repairing malware that is common in Brazil
  - Enabling Host IPS hooks on French versions of Microsoft Windows
- It is about all of these things holistically *and* a whole lot more!



- Network Frontiers (an organization that maps the various standards and regulations to a common framework) estimates that there are more than 400 requirements worldwide that impact IT.
  - “Most large organizations that conduct international business could easily be dealing with upwards of 40 mandates, depending on how diversified their businesses are.” *(De Souza, Evelyn. The Cost of Audits. “McAfee Security Journal”. Summer 2009)*



# Quick questions to ask yourself



- Does your organization operate in more than one country?
- Store health care records?
- Process credit cards transactions?
- Is involved in the storage of health care records?
- Is a publicly traded company?



- The more questions you answered “Yes” to, the more regulations your business is likely to be responsible for compliance to and possibly audited against
- With an average enterprise exposed to over 40 regulations that they must comply with, after talking with many customers, McAfee has termed the resulting feeling “audit fatigue”
- Doing business internationally is one of the main drivers to amplifying regulation count, as regulations like Sarbanes-Oxley often have per-country equivalents that must be adhered to, such as Japan’s Financial Instruments and Exchange Law (often termed “J-SOX” in English)





# Who's on first?



- Once you figure out which regulations and technical controls actually apply to your organization, then you must:
  - Under their impacts
  - Monitor them for changes
  - Enforce them locally and in some cases globally
  - Audit against them
- Often just getting a translation can be a challenge!




- Local *non-security* trends (such as those in pop culture) can ultimately impact threat and response trends globally
- Examples we'll soon cover:
  - Alexa and Chinese BBS'
  - Web search term safety
  - Gold farming
  - Perfect Dark (パーフェクトダーク)



# USA and 中国 – Alexa juxtaposition



## Top Sites in United States

The top 100 sites in United States. 

- 1 Google**  
google.com  
Enables users to search the Web, Usenet, and images. Features include PageRank, caching and tra...  
**More**  
★★★★★ Search Analytics ▶ Audience ▶
- 2 Facebook**  
facebook.com  
A social utility that connects people, to keep up with friends, upload photos, share links and ... More  
★★★★★ Search Analytics ▶ Audience ▶
- 3 Yahoo!**  
yahoo.com  
Personalized content and search options. Chatrooms, free e-mail, clubs, and pager.  
★★★★★ Search Analytics ▶ Audience ▶
- 4 YouTube – Broadcast yourself**  
youtube.com  
YouTube is a way to get your videos to the people who matter to you. Upload, tag and share your... More  
★★★★★ Search Analytics ▶ Audience ▶
- 5 Wikipedia**  
wikipedia.org  
An online collaborative encyclopedia.  
★★★★★ Search Analytics ▶ Audience ▶
- 6 Amazon.com**  
amazon.com  
Amazon.com seeks to be Earth's most customer-centric company, where customers can find and disc...  
**More**  
★★★★★ Search Analytics ▶ Audience ▶
- 7 Craigslist.org**  
craigslist.org  
★★★★★ Search Analytics ▶ Audience ▶
- 8 eBay**  
ebay.com  
International person to person auction site, with products sorted into categories.  
★★★★★ Search Analytics ▶ Audience ▶
- 9 Windows Live**  
live.com  
Search engine from Microsoft.  
★★★★★ Search Analytics ▶ Audience ▶
- 10 Twitter**  
twitter.com  
Social networking and microblogging service utilising instant messaging, SMS or a web interface.  
★★★★★ Search Analytics ▶ Audience ▶



## Top Sites in China

The top 100 sites in China. 

- 1 Baidu & MainMusik.com**  
baidu.com  
Music search engine and free MP3 & video streaming for all kind of topic.  
★★★★★ Search Analytics ▶ Audience ▶
- 2 QQ.COM**  
qq.com  
中国最大的门户网站, 提供即时通讯、新闻资讯、网络游戏以及在线拍卖业务, ... More  
★★★★★ Search Analytics ▶ Audience ▶
- 3 淘宝网**  
taobao.com  
包括电脑通讯、数码、男装、女装、童装、化妆品、书籍音像、运动用品、游戏装备等各种商品的买卖, 还有相关的社区交流, 同时提供支付宝网上交易安全保证系统. ... More  
★★★★★ Search Analytics ▶ Audience ▶
- 4 Google**  
google.com.hk  
★★★★★ Search Analytics ▶ Audience ▶
- 5 新浪新闻中心**  
sina.com.cn  
包括即日的国内外不同类型的新闻与评论, 人物专题, 图库。  
★★★★★ Search Analytics ▶ Audience ▶
- 6 网易**  
163.com  
中国最大的网络社区和门户网站  
★★★★★ Search Analytics ▶ Audience ▶
- 7 soso搜搜**  
soso.com  
提供论坛、网页、图片、音乐等类型搜索服务。  
★★★★★ Search Analytics ▶ Audience ▶
- 8 优酷**  
youku.com  
优酷网 (www.youku.com) 是中国第一视频网站。优酷网立足为全球华人提供最快速的视频播放、最快速的视频发布、最快速的视频搜索服务。... More  
★★★★★ Search Analytics ▶ Audience ▶
- 9 Google**  
google.com  
Enables users to search the Web, Usenet, and images. Features include PageRank, caching and tra...  
**More**  
★★★★★ Search Analytics ▶ Audience ▶
- 10 搜狐**  
sohu.com  
资源导航为主要业务的门户网站, 经营综合性业务, 社区, 无线等增值服务。... More  
★★★★★ Search Analytics ▶ Audience ▶

- One of the top groupings of web sites that are popular in China, both in # of hits and time spent, are web portals that maintain forums (often referred to as a bulletin board system (BBS) in China)
- As China is both a large source of new malware and the forums allow user-contributed content, there has been many problems with malicious users linking to malware
- Likely to increase with the usage of URL shorteners like bit.ly and TinyURL
- NOT just a local problem in China though, similar forum sites are popular with Chinese emigrants overseas (such as MITBBS in the USA) and suffer from the same security challenges (drive by downloads, phishing, 0 sized IFRAMEs, etc)



# Internet usage patterns and threats intersect



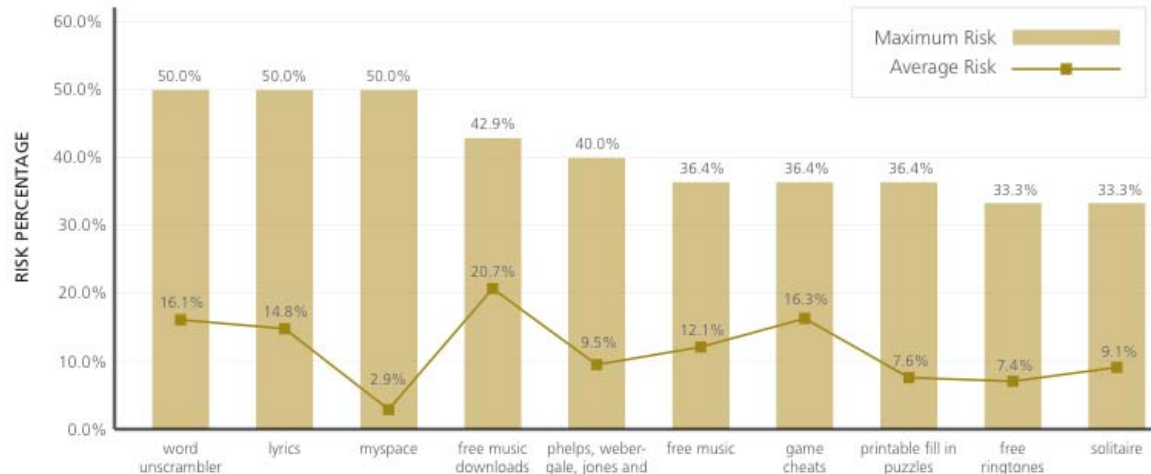
- Next we'll look at the safety of the top 10 search keywords in four countries
  - USA
  - Canada
  - Australia
  - New Zealand
- Poll: How many people expect the keywords to be at least:
  - 75% similar?
  - 50% similar?
  - 25% similar?
  - 10% similar?



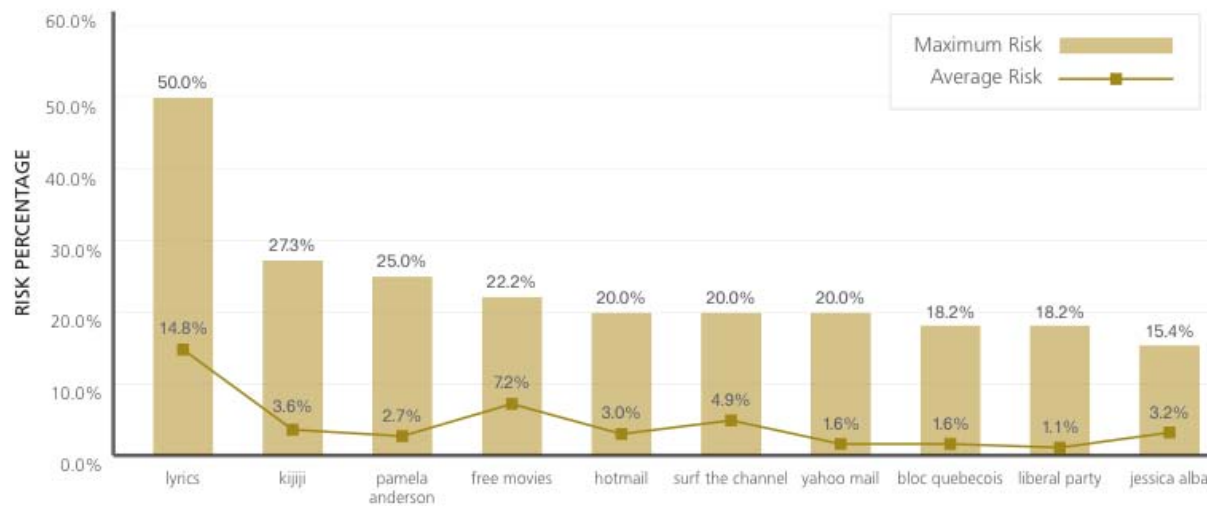
# Dangerous search terms: USA / Canada



### United States' Most Dangerous Search Terms



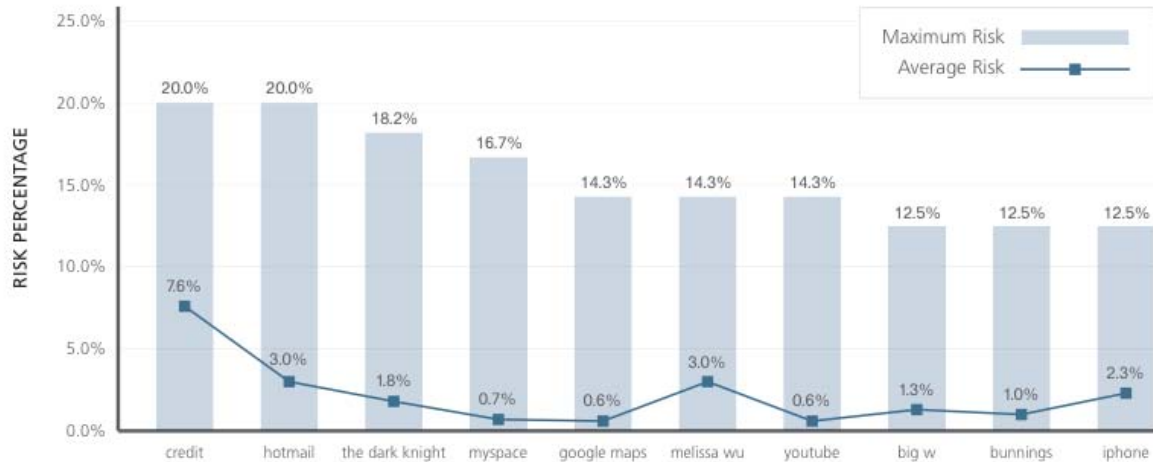
### Canada's Most Dangerous Search Terms



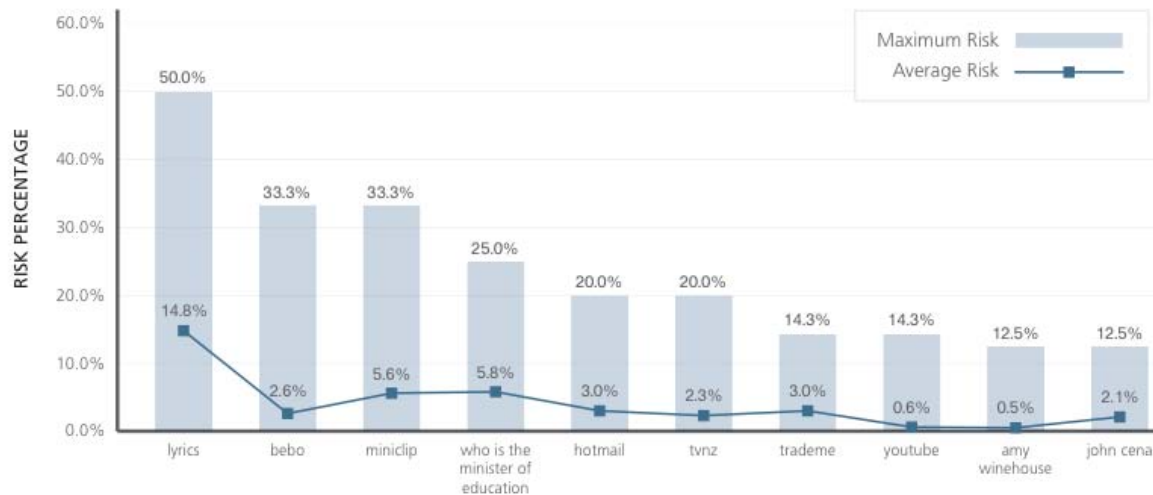
# Dangerous search terms: Australia / New Zealand



Australia's Most Dangerous Search Terms



New Zealand's Most Dangerous Search Terms



# Internet usage patterns and threats intersect



- Answer: 10% in the USA/Canada case, 20% in the Australia/New Zealand case
- In the USA and Canada comparison, only the “lyrics” keyword is shared
- In the Australia and New Zealand comparison, only the “hotmail” and “youtube” keywords are shared
- If these four countries are showing such dissimilar Internet usage/search patterns, how different must the threat landscapes be across countries as dissimilar as Brazil and Singapore? Or Korea and USA?





# Gold farming – Trading higher reward for lower risk



- Trend to target those less likely to result in prosecution
  - Large financial institutions equipped to respond
  - Soft targets more vulnerable and may lead to higher conversion rates
  - Virtual economies booming led to gold farming through labor arbitrage
  - Blocked by eBay (other than Second Life)
  - In June 2009, trade of virtual goods/currency for real-world currency made illegal in China



# パーフェクトダーク



- “Perfect Dark”, or パーフェクトダーク in Japanese, is a popular p2p app in Japan
- Blocking p2p software that is popular in Japan, Korea, and China has been a driver of change for network IPS vendors



Improving Security Together

- Some trends we've seen in vulnerability coverage:
  - Enterprises have built processes around Microsoft (OS and Office) patches
  - Struggling with Adobe
  - FireFox, Java, and to some extent Chrome also “top of mind”
- Poll: How many of you have an office, work in, sell products/services in, or do business in China, Singapore, Hong Kong, Taiwan, or Japan?



- Ichitaro is a Japanese word processing software package, that predates Microsoft Word, and is significantly popular and prevalent on Japanese business systems
- QQ is an instant messaging program that is more popular than Skype, MSN, Yahoo IM, or AIM, and is popular in China, Singapore, Hong Kong, and Taiwan
- Both of these have been targeted by malware exploiting non-public un-patched vulnerabilities
- There's a lot more examples of locale-specific software that is popular in various regions of the world and targeted
- For global businesses, Ichitaro and QQ need monitoring as well and processes need to account for locally prevalent software



# MS06-009 Korean IME



- MS06-009 was a vulnerability in the Korean IME that could allow elevation of privilege
- Not just a problem in Korea!
- Once you install the East Asian language pack/IME for Microsoft Windows, you then have the vulnerable code present on the system
- Users who install it, are likely planning to enable either the Japanese, Korean, or Chinese IME
- Affects systems globally for Korean expats, students, etc
- Vulnerabilities are increasingly both local and global; monitoring processes need to similarly be both local and global



# Leverage what's already out there



- Easiest way to learn more about threats in a given country is to leverage the local Computer Security Incident Response Team Coordination Center (CSIRT/CC)
- JPCERT/CC provides both a English and Japanese language feed of their JVN iPedia JVNDB, which contains information on vulnerabilities in software of Japanese vendors



# The value of JVNDB



- JVNDB contains fully unique threats that are often not found in other sources
- Easy to programmatically poll via the public XML files (i.e. NVD-like)
- Example:
  - JVNDB-2009-00057: ATOK screen lock bypass vulnerability
  - <http://jvndb.jvn.jp/en/contents/2009/JVNDB-2009-000057.html>
  - JVNDB-2009-00018: Ichitaro series buffer overflow vulnerability
  - <http://jvndb.jvn.jp/en/contents/2009/JVNDB-2009-000018.html>



# The value of JVNDB



- Both vulnerabilities were publicized around the same time
- Both are for software made by JustSystems (well known software development company in Japan)
- The Ichitaro vulnerability has many primary source references, like NIST's NVD
- The ATOK vulnerability is almost exclusively found in the JVNDB
- For comprehensive global monitoring, JVNDB is a must!



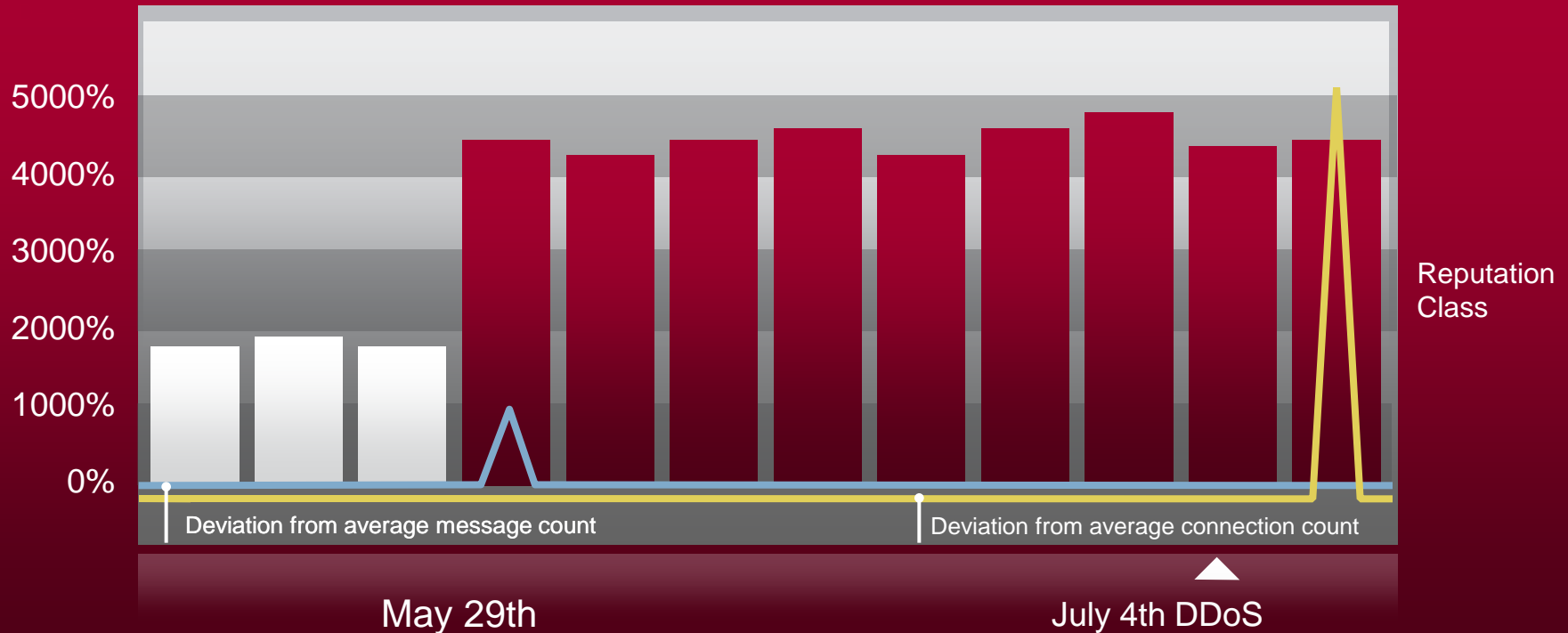


- One of the easiest ways to get a handle on locale-specific threats is to partner with a security vendor who has a global threat intelligence capability
- On the next slide, we'll see how a real world global attack was stopped, just as it started
- Poll: Can anyone guess the attack? It made headlines and is very relevant given recent international political headlines...



# McAfee Global Threat Intelligence in Action

Protecting Against Botnet Attack on U.S. and South Korean Governments



- July 4th 2009: 200,000 zombie Korean botnet launches DDoS against US and South Korean government sites

- McAfee GTI used cross-threat vector correlation to predict the threat and adjusted the reputation of 80% of the IP addresses used to carry out the attack

- Takeaways and call to action:
  - The threat landscape is and has always been dynamic, don't be caught with your head in the sand
  - Be aware of global threats, don't suffer from organizational myopia
  - Prioritize and respond to threats both on a global basis as well as a local basis
  - The point of entry for an attacker is often the weakest link, it's rarely the front door
  - Get help, leverage the various CSIRT/CC and FIRST teams around the world, as well as security vendors who provide global threat intelligence capabilities



# Questions and comments



- Responding to global threats is a challenge, if you need assistance, don't hesitate to ask
- For any additional questions and follow up, I can be reached at:
  - [Anthony\\_Bettini@McAfee.com](mailto:Anthony_Bettini@McAfee.com)

