Technology Solutions to Fight Cybercrime

Kai Koon Ng
Senior Manager, Legal & Public Affairs
Symantec™ Global Intelligence Network

Identifies more threats, takes action faster & prevents impact

**Worldwide Coverage**  
**Global Scope and Scale**  
**24x7 Event Logging**

**Rapid Detection**

**Attack Activity**
- 240,000 sensors
- 200+ countries

**Malware Intelligence**
- 133M client, server, gateways monitored
- Global coverage

**Vulnerabilities**
- 40,000+ vulnerabilities
- 14,000 vendors
- 105,000 technologies

**Spam/Phishing**
- 5M decoy accounts
- 8B+ email messages/day
- 1B+ web requests/day

**Preemptive Security Alerts**

**Information Protection**

**Threat Triggered Actions**

Asia Pacific Regional Workshop on Fighting Cybercrime
So how big is this Social Networking thing?

facebook -> 2 × American flag

twitter -> Brazilian flag
Do you know who you are sharing your information with?

- Hackers have adopted social networking
  - Use profile information to create targeted social engineering
  - Impersonate friends to launch attacks
  - Leverage news feeds to spread SPAM, scams and massive attacks
Social Networks as a Threat

Of course I can trust my friends...

- Shortened URLs hide malicious links, increasing infections
- More shortened URLs leading to malicious websites observed on social networking sites; 73% were clicked 11 times or more
Dark Side of Social Networks

• Criminals using social network sites to perpetrate identity fraud
  – Financial – “Please see me money”
  – Espionage – “Tell me about...”

• Predators target children using social networking sites
  – On average, children have 56 online friends
  – Most (82%) have met in real life, more than half of their online friends
  – 41% has someone they don’t know try to add them as a friend
Koobface Worm

- Infect
- Gather
- Spread
- Botnet

Asia Pacific Regional Workshop on Fighting Cybercrime
Dealing with Threats

Advanced Internet Security Solutions

• Signatures and Heuristics based Anti-virus
• Reputation based

Blacklisting/Whitelisting of Webpages

• Reduce the risk of infection by staying away from ‘bad neighbourhoods’

Common Sense

• The user is usually still the greatest threat...
Mobile: New Frontier, Old Problems

Asia Pacific Regional Workshop on Fighting Cybercrime
The new frontier

• Increasing applications for mobile computing
  – Extension of the desktop & notebooks
  – Worldwide ‘app’ download expected to reach 17.7 billion in 2011

• Increasing capabilities of mobile devices
  – High Definition Camera
  – GPS
  – Massive amounts of storage

• 1.2 billion smartphones users by end 2011
Common Attack Vectors

- Mobile Devices are mini-computers
  - Vulnerabilities that can and will be exploited
- Modification of legitimate apps
  - Trojans inserted
- Target mobile’s inherent billing features
  - Subscribing victim to premium services
- Target sensitive data stored on mobile devices

42% increase

<table>
<thead>
<tr>
<th>Year</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>115</td>
</tr>
<tr>
<td>2010</td>
<td>163</td>
</tr>
</tbody>
</table>

Asia Pacific Regional Workshop on Fighting Cybercrime
Mobile Device Security Models

• Traditional access control:
  - Protects devices by using techniques such as passwords and idle-time screen locking

• Application provenance:
  - Each app is stamped with identity of author and made tamper resistant; enables user to decide whether or not to use app based on identity of author

• Encryption:
  - Conceals data at rest on the device to address device loss or theft
Mobile Device Security Models

• Isolation:
  – Limits app’s ability to access sensitive data or systems on device

• Permissions-based access control:
  – Grants set of permissions to each app and then limits each app to accessing device data/systems within the scope of permissions
# Mobile Platform Security Summary

<table>
<thead>
<tr>
<th>Types of Attack</th>
<th>Apple iOS</th>
<th>Google Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-based attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social engineering attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource abuse/Service attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data loss (malicious and unintentional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data integrity attacks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Little or No Protection
- Moderate Protection
- Full Protection
Increasingly Connected Devices

- iOS and Android devices do not work in a vacuum
  - Connect to one or more cloud-based services (enterprise Exchange server, Gmail, MobileMe, etc.), home or work PC, or all of above

- When properly deployed, both platforms allow users to simultaneously synchronize devices with private and enterprise cloud services without risking data exposure
  - However, there are several scenarios in which services may be abused by employees, resulting in exposure of enterprise data
Mobile Security Solutions

• Mobile antivirus:
  – Scanners for Android, but iOS’s isolation model prevents implementing on iOS devices
  – Effective at detecting known threats, but provide little protection against unknown threats; expect traditional scanners to be replaced by cloud-enabled, reputation-based protection
  – Addresses threats in malware threat category and subset of malware-based attacks in resource abuse, data loss and data integrity categories

• Secure browser:
  – Secure browser apps for iOS and Android checks visited URLs against blacklist or reputation database and blocks malicious pages
  – User must use the third-party secure Web browser to do all surfing
  – Secure browsers address Web-based attacks and social engineering attacks; can also potentially block malware downloaded through browser
Mobile Security Solutions

• Mobile device management (MDM)
  – Enables admins to remotely manage iOS and Android devices
  – Admins can set security policies such as password strength, VPN settings, screen lock duration; can also disable specific device functions, wipe missing devices and use the device’s GPS to locate missing device
  – Doesn’t specifically protect against any one threat category, but helps reduce risk of attack from many categories

• Enterprise Sandbox
  – Aims to provide secure environment where enterprise resources such as email, calendar, contacts, corporate websites and sensitive documents can be accessed
  – Essentially divides device’s contents into two zones: secure zone for the enterprise data, and insecure zone for the employee’s personal and private data.
  – Focused on preventing malicious and unintentional data loss; though doesn’t block other attack categories explicitly, does limit impact of other attacks
Mobile Security Solutions

- Data loss prevention (DLP)
  - Scan publicly accessible storage areas of device for sensitive materials
  - Due to iOS’s isolation system, iOS-based DLP tools only inspect calendar and contact lists
  - On Android, could scan external flash storage, email and SMS inboxes, as well as calendar and contact lists
  - Due to isolation models, unable to scan data of other apps
Conclusions... and Some Thoughts
Challenges are There...

• The Bad Guys are innovating
  – New vectors of attacks
  – Harness and adopt latest technologies

• Malicious activities are no longer just an annoyance
  – Most usually have a specific goal in mind
  – Financial gain or espionage

• Information is the new Gold
  – System-centric to Information-centric defense
“Predicting rain does not count, Building Arks does.”

Warren Buffett
Building ‘Arks’

Collaborating with Governments around the World

• Jointly funded security research
  – Wombat, Lobster, Antiphish, Vampire
• Jointly funded critical infrastructure protection projects
  – European Programme for Critical Infrastructure Protection (EPCIP)
• Joint deployment of security intelligence technologies
  – Attack Quarantine System (AQS), Deepsight Analyser
• Joint cyber-security exercises
  – Coalition Warrior Interoperability Demonstration (CWID), Cyberstorm, Cybershockwave, Cyber-Endeavour
• Participation in expert groups, committees etc
  – ENISA, ITSCC
• Awareness raising
• Philanthropy/CSR activities
Collaborating with Law Enforcement

**Information Sharing**
- Threat Landscape
  - Internet Security Threat Reports
  - Norton Cybercrime Report
  - MOU with ITU
  - Threat Information

**Norton Cybersecurity Institute**
- Capacity-building Program targeted at law enforcement, and prosecutors

**Public Awareness Programs**
- Cybersecurity Awareness
- Norton Cybercrime Index
Best Practises
Consumer Best Practices

Protect yourself

- Use a modern Internet security solution for maximum protection against online threats that includes:
  - Antivirus protection
  - Intrusion prevention to protect against Web-attack toolkits, unpatched vulnerabilities, and socially engineered attacks
  - Browser protection to protect against Web-based attacks
  - Reputation-based tools that check the reputation and trust of a file before downloading
  - Behavioral prevention that keeps malicious threats from executing even if they get onto your computer
  - URL reputation and safety ratings for websites found through online searches

Keep up-to-date

- Keep virus definitions and security content updated at least daily - if not hourly – to protect your computer against the latest viruses and malicious software (“malware”)

Use an effective password policy

- Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary, since these are easier for cybercriminals to hack
- Do not use the same password for multiple applications or websites
- Use complex passwords (upper/lowercase, punctuation and symbols) or passphrases. (e.g., “I want to go to Paris for my birthday” becomes, “l1t2g2P4mb”)

Asia Pacific Regional Workshop on Fighting Cybercrime
Consumer Best Practices

Know what you are doing

• “Free,” “cracked,” or “pirated” versions of software can contain malware or social engineering attacks
• Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them. Some security risks can be installed because of that acceptance

Guard your personal data

• Limit the amount of personal information you make publicly available on the Internet (including and especially social networks) as it may be harvested by cybercriminals and used in targeted attacks, phishing scams, or other malicious activities
• Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate
• Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections

Think before you click

• Never view, open, or execute any email attachment or click on a URL, unless you expect it and trust the sender.; even if it’s coming from trusted users, be suspicious
• Do not click on shortened URLs without expanding them first using “preview” tools
• Do not click on links in social media applications with catchy titles or phrases; you may end up “liking it” and sending it to all of your friends – just by clicking anywhere on the page
• Be suspicious of warnings that pop-up asking you to install media players, document viewers and security updates; only download software directly from the vendor’s website
Stay Informed: Additional Resources

**Build Your Own ISTR**
[go.symantec.com/istr](go.symantec.com/istr)

**Daily measure of cybercrime risks**
[nortoncybercrimeindex.com](nortoncybercrimeindex.com)

**Follow Us:**
[Twitter.com/threatintel](Twitter.com/threatintel)
[Twitter.com/nortononline](Twitter.com/nortononline)
Thank you!

Kai Koon Ng
kaikoon_ng@symantec.com
+65 9002 0214