WHEN SIZE DOES MATTER

Escalating Attacks Against Enterprise: the case for for adding more Anti-Malware

According to Deloitte & Touche, ZeuS – a single Trojan engineered to steal on-line banking credentials – was responsible for over $60 million in losses to businesses in North America in 2011 alone. Worldwide losses in cash and time due to cyber-crime are estimated at over $300 billion a year. These funds are able to finance the best and the brightest attackers.

New cybercrime tactics threatening Enterprises in 2012:

- On a daily basis, cybercriminals launch new malware websites on breaking news stories, engineering high rankings by search engines for an extremely effective infector vector.
- Crooks target employees responsible for online banking activities or who have access to sensitive data.
- Criminals will try to take under control the employees’ own devices and then use them to successfully penetrate your corporate network.
- You can’t keep your employees from having Facebook accounts, which create vulnerabilities. Cybercriminals use these to profile employees and engineer targeted attacks.
- Banks cannot be relied upon to alert businesses as to unusual account activity:
  - They are not liable for poor authentication systems
  - Banks have yet to invest in simple protections such as account profiling or “out of band” notification (confirmation via phone or email) of money transfers
- You don’t have to be extra-rich to deserve the attention of a hacker – present-day ‘hacktivists’ can and will target you on general principle.
- A seemingly legitimate “customer request” or “vendor notification” only must win the confidence one employee to infect an entire network.
- One disgruntled former employee is capable of ruining decades of customer trust with a single data breach.
- Today’s cybercriminals are patient. They enter as stealthily as possible and may take years to siphon off stolen data and identities.

Unavoidable cybersecurity threats to Enterprise:

- Internet browsing is required by marketing, research, and lead generation functions
- The importance of staying current on breaking news and trends
- Increasing use of social networking as a marketing tool
- Increasing use of mobile devices and ongoing trend towards the adoption of Bring Your Own Device (BYOD) policy
- Unprecedented rise in hacktivism – idealistic hackers view governments and large corporations as ‘ultimate evil’
- Reliance on professional networks like LinkedIn
- The following popular applications – MS Excel; MS Word; Adobe Flash Player; MS Office; Adobe Reader; Sun Java JDK – possess critical vulnerabilities, allowing malware to bypass security and execute arbitrary code
- Attacks on SQL databases continue to increase

2011’s breakdown of successful attacks by industry sector:

- Finance and Insurance: 29%
- Information: 22%
- Retail Trade: 12%
- Manufacturing: 8%
- Public Administration: 7%
- Transportation and Warehousing: 5%
- Other: 12%

** - According to Verizon 2012 Data Breach Investigations Report
Recent Victims of Cybercriminals

- **Sony** PlayStation Network was hacked repeatedly in 2011, bringing the entire network down for several weeks. Personal data, passwords, and credit card numbers of more than 70 million accounts might have been taken by the perpetrators. The hacking (and the response) cost Sony $24 billion dollars – nearly 10x their revenue for the same period.

- **Citigroup** had its systems breached in May 2011. As a result, approximately 210,000 customers had their private data (including names, account numbers, email addresses, and contact details) stolen.

- **RSA**, best known for its SecurID tokens, was severely jeopardized by a clever cyber attack in spring of 2011. The attackers used social engineering to trick RSA employees into opening a spoofed email and downloading an infected Excel spreadsheet. As a result, the hackers received access to the computer network and then stole SecurID tokens, which were subsequently used to hack military contractors.

- In June 2011, the **International Monetary Fund** (IMF) joined Sony, Citigroup and other high-profile targets, as the victim of a hacker attack. According to reports, hackers reportedly obtained “large quantities” of data, including email addresses and other documents.

- More than seven million consumer records have been exposed in at least 264 data breaches so far this year, according to the latest figures from the Identity Theft Resource Center (www.idtheftcenter.org).

Tips to Increase Enterprise Security

- Ensure that there is C-level security governance – don’t treat security as an IT issue.
- Check workstations to ensure anti-malware updates are current.
- Make sure all systems are updated with the latest application patches.
- Delete all unused software - out-of-date means vulnerable.
- Restrict on-line banking activities to a dedicated computer - not used for any other internet activity.
- Contact your bank to set up alert notification by phone for all money requests or transfers.
- Buy as much security as you can afford. The calculation should be balanced against:
  - the cost of losing valuable company data such as customer lists.
  - compromising customer privacy.
  - losing credibility with customers, vendors and partners.
  - money that could be lost from on-line banking accounts.

What Kaspersky Delivers!

- Fastest response time to provide the smallest possible window of vulnerability.
- Optimum frequency of Updates.
- Best heuristics – ability to identify malware by bad behavior.
- “Cracks” more archives and file types (where most malware is hidden) than other engines.
- Consistently rated the best by independent testing organizations (see table below).

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Kaspersky Lab</th>
<th>Symantec</th>
<th>McAfee</th>
<th>Sophos</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV-Test.org Q1’2012 Protection/Repair/Usability score</td>
<td>6.0 / 5.0 / 5.0</td>
<td>6.0 / 2.5 / 5.0</td>
<td>5.5 / 4.5 / 3.5</td>
<td>4.5 / 3.0 / 5.5</td>
</tr>
<tr>
<td>AV-Comparatives: Mar’ 12 On-Demand Comparative Test</td>
<td>Advanced+ 99.3% Detection</td>
<td>Not included</td>
<td>Advanced 98.6% Detection</td>
<td>Advanced+ 98.5% Detection</td>
</tr>
<tr>
<td>AV-Comparatives: Feb’ 11 Retrospective/Proactive Test</td>
<td>Advanced+</td>
<td>Not included</td>
<td>Not included</td>
<td>Standard</td>
</tr>
<tr>
<td>AV-Comparatives: July’ 11 Whole Product Dynamic Test</td>
<td>Advanced+</td>
<td>Advanced</td>
<td>Failed</td>
<td>Standard</td>
</tr>
<tr>
<td>VB100: Apr’ 11 Reactive/Proactive Protection Score</td>
<td>94.56%</td>
<td>88.58%</td>
<td>84.71%</td>
<td>89.14%</td>
</tr>
<tr>
<td>VB100: Successful Results In Total</td>
<td>64</td>
<td>56</td>
<td>48</td>
<td>61</td>
</tr>
</tbody>
</table>