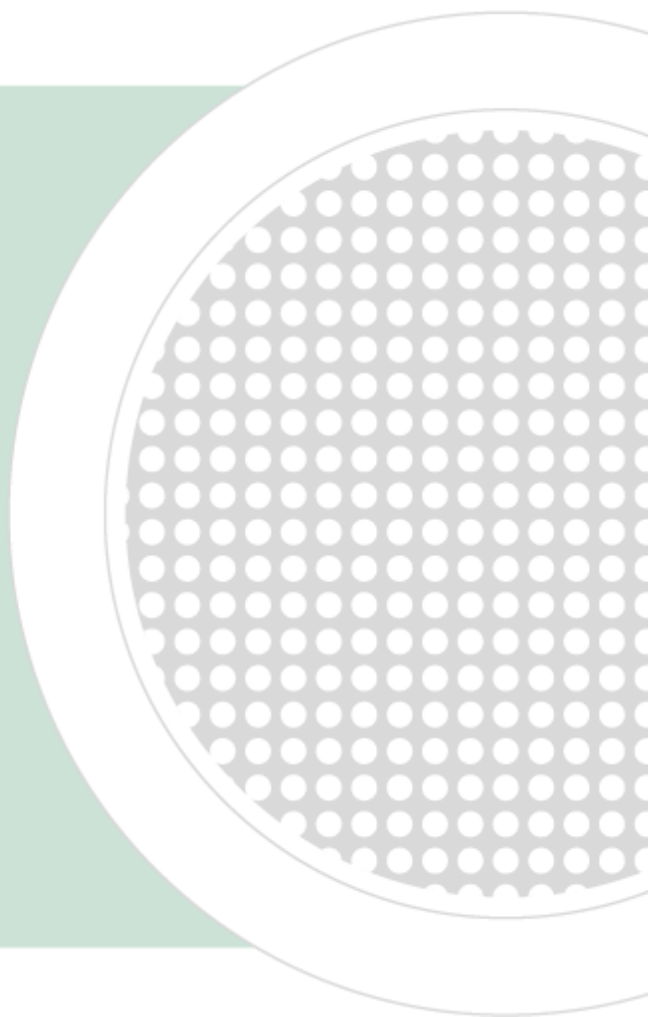


White Paper

Security Trends 2008

By Tom Bowers

Senior Security Evangelist, Kaspersky Lab



Preface

NEWS FLASH!!!

It's all about the content, it's always been about the content, and it will always be about the content. That's why social networking sites such as YouTube and Facebook and corporate technologies such as blogging and podcasting have taken off. We are sharing personal and corporate information at a far greater pace than ever before. Even during the hacking heydays when it was all about reputations, when the reputations depended solely on the prestige of the hacked resource, it was still about content – the sensitive or valuable content that was exposed by the hack.

Unfortunately, 2008 will see cybercriminals with financial motives in mind, and the re-invention of organized crime online. It's time to take a hard look in the mirror, not only at ourselves and our attitudes towards online security, but also at the business motivations and business models of cybercriminals.

This paper attempts to predict what we face in 2008 and how we need to react. We hope that it provides some food for thought and helps you view the world in a more pragmatic fashion...because the landscape is changing.

Table of Contents



Preface	i
Content Is King	1
Malware Ecosystem Development.....	1
Security as a Risk Function	2
Social Networking Sites.....	2
The Disappearing Network Perimeter.....	3
Tighter Integration of Security Solutions.....	4
Conclusions.....	5

Content Is King

Today's CEOs are far more sensitive to the value of information and the accompanying risk unauthorized access to this information represents for corporate operations. Privacy and Breach Notification legislation was the beginning of their sensitivity training. No CEO wants to appear on television or in major business publications offering an apology to loyal customers for an event that has put their data at risk. Unfortunately, it appears that 2008 will become another banner year for corporate data losses.

Many organizations have created Chief Risk Officer (CRO) positions to directly confront this business risk issue. But why is this necessary? Why have criminals become so interested in this corporate data? Why are hackers going after your desktop? The simple answer is this: to make money.

Whether it involves personally identifiable information (PII), bank account or credit card information, or even a company's trade secrets – it's all about converting information into currency. From the Fortune 100 Company to the new start-up, every firm's trade secrets are at risk. Both business and security professionals alike must now temper their decision-making with the question, "How could this action or decision place our information at risk?" Every other trend that will be examined in this paper hinges on the response to that one question.

Unfortunately, it appears that 2008 will become another banner year for corporate data losses.

Malware Ecosystem Development

Our adversaries in the cyberworld are not sitting still; they are getting better organized and establishing loftier business goals. The thrill of hacking into a system or infecting a few thousand desktops for the sake of notoriety was, essentially, child's play. The cybercriminals are organizing, outsourcing, managing risk, and lowering costs – all the things that well-run legitimate businesses do. The groups behind the Storm and Warezov malware threats serve as two current examples. Both are long established, highly-organized, very secretive groups generating millions in cash flow.

It all begins with the Investors. Investors are organized groups who are able to invest large sums of money in the creation and maintenance of a business-grade infrastructure to produce illegal profits. Today's Investors may be organized gangs (Storm and Warezov) or governments. In either case they outsource the project to Consultants. The Consultants include the malware authors, botnet masters, exploit specialists, and spam list holders. The Consultants in turn use a wide variety of methods, such as viruses, worms,

and Trojans, to transmit the malware to users' computers. Once installed, the malware may perform one or more of these functions –

- Serving as a host to infect other computers
- Harvesting email addresses for future spam
- Stealing either personal or corporate information and transmitting it to the Investors

Security as a Risk Function

What happens when the CEO of a large enterprise appears in a public forum to apologize for data theft? Recent experience shows that the firm's share value drops. In business terms, data theft represents a risk to the company's market capitalization. That, in turn, makes it more expensive to obtain funding for growth initiatives. And that means that shareholders will receive lower stock dividends. This is a serious business risk. In a volatile economy, it can even mean the beginning of a negative death spiral for the company.

The fastest growing senior executive position in business today is that of a Chief Risk Officer (CRO). Jackie Bassett of BT Industries explains the CEO's current dilemma by saying, "The CEO of a firm is riding a kayak in Class 5 rapids [most difficult type]. He sees a rock and shifts his kayak to the left. That was not enough and he shifts further to the left. Another boulder and a shift to the right... He knows there is a waterfall somewhere ahead, and he hopes that he has planned effectively for it."

Someone has to plan for the risks the river offers, the twists and turns, the large boulders and of course the waterfall. In large companies this job is falling to the CRO. Sometimes the CRO and Chief Security Officer (CSO) are one and the same; sometimes they're peers reporting to the same executive. Increasingly, security is being seen as a primary business risk function. Therefore, those of us in the security industry have also begun to view ourselves in a new light. That means that we must understand the business implications of what we do, rather than looking exclusively at the IT side of the equation.

Social Networking Sites

Social networking sites, such as MySpace and Facebook, serve a dual purpose in the world of cybercrime – they serve both as an attack vector and as a communication mechanism for security adversaries. These websites have large concentrations of members that, in turn, represent a large amount of processing power and information. This makes them prime targets for attack.

Someone has to plan for the risks the river offers, the twists and turns, the large boulders and of course the waterfall. In large companies this job is falling to the CRO.

The intent may be to plant a Trojan that simply creates a botnet zombie (to secretly spread the malware to others), to plant a keylogger to steal personal information (by recording keystrokes), or to do both.

Social networking attacks represent a relatively new but rapidly growing threat. Organized groups of cybercriminals attempt to get lost in the vast sea of humanity that frequents these social networking spheres. While IRC has long been used as the communication vector of choice, cybercriminals seem to be shifting to these newer social networking venues to keep in contact with one another.

The Disappearing Network Perimeter

Today, information travels faster, farther, and on more diverse devices than ever before. The realm of security is no longer simply a PC sitting behind a firewall. Information is being transmitted via cell phones, PDAs, USB flash drives, cell phone cameras, and even Internet-attached household appliances, such as stoves, furnaces, and refrigerators. As information flows to these devices, the risk to that same information increases dramatically. Do you have firewalls installed on your smart phones or encryption on your USB drives? Probably not. The perimeter of a network, whether at home or in the office, is defined by the outermost points where we either store information or transmit it. The edges of our networks are becoming increasingly fuzzy and elusive.

In the enterprise this problem is magnified a thousand fold, particularly by the global trends of workforce mobility and decentralization of staff. While both trends are rooted in practical business efficiencies, they also place greater strain on the security infrastructure. When employers hire remote or virtual employees, how many of them secure the employee's home network? Very few, if any, security plans examine this issue simply because the business cost and risk is simply too great to even consider. A business has no way of determining employees' network configurations, which web sites their children visit, or how often employees apply security patches to their applications. Nevertheless, corporate information resides in these home networks and must be considered by security staff. This problem intensifies when smartphones are added to the mix, simply because there are very few options available for securing these devices.

The more mobile the workforce becomes, the thinner the protection becomes for corporate trade secrets. Don't believe for a minute that cybercriminals haven't noticed the lax security at these fuzzy fringes of the corporate network. Competitive intelligence is one of the fastest growing market segments in business today. It is quite easy to "borrow" a laptop, flash drive, or smartphone, which might contain the marketing plans for the next fiscal year. This trend is accelerating with frightening speed. Thinner protection at

The perimeter of a network, whether at home or in the office, is defined by the outermost points where we either store information or transmit it. The edges of our networks are becoming increasingly fuzzy and elusive.

network edges naturally puts more business information at risk than ever before. As cybercriminals pay more attention to this opportunity, CSOs will be forced to face this blind spot in network security. They, along with their CFOs, may spend more sleepless nights as they attempt to secure the fuzzy and largely unmanaged network perimeter.

Tighter Integration of Security Solutions

How many businesses rely exclusively on Microsoft products for word processing, anti-virus, firewalls, backup solutions, image modifications, web sites, email, spyware protection, and file transfer? It's a safe bet to assume that most businesses do not. Rather, they choose solutions more specialized to each specific task. To varying degrees, most businesses take a "best-of-breed" approach in selecting software, even though there may be some limitations in selection based purely on price points.

In taking a best-of breed approach to security, most enterprises define and periodically review their risk profiles. They look for the best solutions to mitigate threats to the business environment in a reasonable fashion over a reasonable timeframe. Relying on one large security vendor with multiple solutions would make most large enterprises uncomfortable. The "one size fits all" approach probably has more merit in the small-to-medium business (SMB) environment because of cost considerations, even though it is not the most effective security practice. Large enterprises prefer to select best-of-breed components that meet their specific needs, and then try to make those components work with one another in a seamless fashion.

This multi-vendor world does make for some challenges, however. Not all vendor solutions communicate with other vendor solutions, although most do provide simple XML support. Fortunately, more vendors are beginning to realize that they need to make their solutions talk dynamically to one another. With this type of cooperation beginning to emerge between vendors, it's not unfathomable to believe that tomorrow's antivirus solution could detect a zero-day exploit and update the network IDS and firewall rule sets to counteract the threat. The emerging blended NMS/SEIM (Network Monitoring System/Security Event and Incident Management) space is a testament to this type of integration and cooperation. One can only hope that 2008 will see a vast increase in the number of security vendors who begin to forge strategic alliances that will enable them to provide greater future benefit to the customers they serve. This kind of cooperation should prove to be an effective weapon in a multi-faceted arsenal/defense against today's organized cybercriminals.

In taking a best-of breed approach to security, most enterprises define and periodically review their risk profiles. They look for the best solutions to mitigate threats to the business environment in a reasonable fashion over a reasonable timeframe.

Conclusions

To briefly recap our observation of trends to expect in security in 2008 –

- Content will continue to grow and will remain the centerpiece of security concerns.
- Because our adversaries are in it for the money, they will continue to become more organized and resilient. This will push businesses towards a more risk-based approach to managing their security needs.
- Our information is traveling faster and further on mobile devices, making it harder to protect, and the tools and techniques are lacking to secure mobile perimeter devices.
- The integration of best of breed security solutions across multiple platforms and vendors will continue to be the nirvana that every business hopes to experience. 2008 will provide some progress in this direction.

Above all else, content remains front and center as the major influence on what will happen in 2008. With increasingly sophisticated cybercrime networks and complex corporate information systems, collisions and intersections between them are a key factor in risk management for businesses in 2008.



Kaspersky Lab, Inc. • 500 Unicorn Park • Woburn, MA 01801
phone: (781) 503-1800 • fax: (781) 503-1818
www.kaspersky.com

About Us

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for large enterprises, SMBs, home users and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of more than 100 of the industry's leading IT security solution providers.

For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit www.viruslist.com.

Learn more at www.kaspersky.com