

A background image showing a laptop on a desk with a circular gauge overlay. The gauge has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office or laboratory setting.

# The Future of Threats and Threat Technologies How the Landscape Is Changing

Trend Micro, Incorporated 

 Trend Micro

A Trend Micro Report | December 2009

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing



### CONTENTS

|  |    |
|--|----|
| TOUGH CHALLENGES IN 2009.....  | 4  |
| KEY PREDICTIONS FOR 2010 AND BEYOND .....  | 5  |
| TECHNOLOGICAL AND SOCIAL LANDSCAPE: WHERE WE ARE NOW AND WHERE WE ARE GOING.....                                     | 6  |
| <i>More Choices for Connectivity.....</i>  | 6  |
| <i>Social Networking Sites.....</i>  | 6  |
| <i>Increasing Internet Penetration Worldwide.....</i>  | 7  |
| <i>Google Chrome Operating System.....</i>   | 7  |
| <i>Cloud Computing and Virtualization.....</i>   | 7  |
| NEW AND TOUGHER SECURITY CHALLENGES IN 2010 .....  | 8  |
| <b>Cybercriminals will formulate more direct and brazen extortion tactics to obtain quicker access to cash. ....</b> | 8  |
| <b>Business as usual for botnets, but heavier monetization by botnet herders. ....</b>                               | 9  |
| <b>Mobile threats will have more impact. ....</b>  | 11 |
| <b>Compromised products come straight from the factory. ....</b>   | 12 |
| <b>Web threats will continue to plague Internet users.....</b>   | 13 |
| <i>Poisoned Searches .....</i>   | 13 |
| <i>More Malicious Scripts, Fewer Binaries.....</i>   | 14 |
| <i>Malvertisements .....</i>   | 14 |
| <i>Application Vulnerabilities .....</i>   | 14 |
| Microsoft Windows.....   | 14 |
| Mac Threats .....  | 14 |
| <i>New Technologies Offer Greater Security.....</i>  | 15 |
| <b>Changes to the Internet infrastructure will widen the playing field for cybercriminals.....</b>                   | 16 |
| <i>IPv6 Experimentation Stages.....</i>  | 16 |
| <i>Internationalized Domain Names .....</i>  | 16 |
| <b>Cloud computing will present new security challenges.....</b>   | 16 |
| <i>New Threats to the Data Center and Cloud Computing.....</i>   | 17 |
| <i>Multi-Tenancy in the Cloud May Create New Threats.....</i>  | 18 |
| <i>Data Center Attacks.....</i>  | 18 |
| <i>Unsecure Management Systems .....</i>   | 19 |
| <i>Economic Denial of Service.....</i>   | 19 |
| <i>Higher Levels of Abstraction on Fragile Technologies.....</i>   | 19 |
| <i>New Border Gateway Protocol Tricks .....</i>  | 20 |

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing



- WHAT THIS MEANS FOR USERS: KNOW YOUR THREATS, COME PREPARED ..... 21**
  - Advice for End Users ..... 21**
    - Keep your personal computer current with the latest software updates and patches... 21*
    - Protect yourself and your personal computer..... 21*
    - Choose secure passwords..... 22*
  - Advice for Businesses ..... 22**
    - Use effective solutions to protect your business. .... 22*
    - Safeguard your customers' interests..... 23*
    - Establish and implement effective IT usage guidelines..... 23*
- RESOURCES AND USEFUL LINKS..... 24**



# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

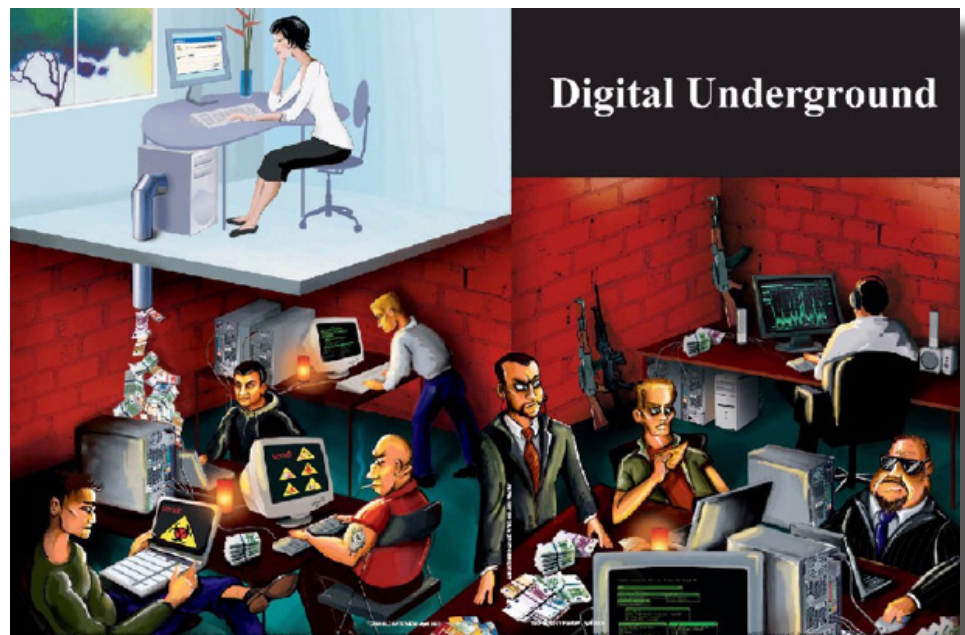
### TOUGH CHALLENGES IN 2009

Trend Micro experts correctly predicted several threat areas that the industry subsequently experienced throughout 2009, including:

- Social networking sites will grow as targets.
- Social engineering will become increasingly prevalent and clever.
- Unlike the global economy, the underground economy will continue to flourish.

In the *Trend Micro 2009 Annual Threat Roundup*<sup>1</sup> released early in 2009, Trend Micro experts correctly predicted several threat areas that the industry subsequently experienced throughout 2009. Among them, that:

- (1) Social networking sites will grow as targets;
- (2) Social engineering will become increasingly prevalent and clever, and;
- (3) Unlike the global economy, the underground economy will continue to flourish.



The Internet today offers wider and deeper online social networks, new and possibly landscape-changing technologies from application to infrastructure level—like cloud computing, IPv6, and virtualization, along with more insidious challenges to security. These challenges are propelled to a certain extent by cybercriminal efforts to obtain profit.

While it is difficult to cover every possible threat eventuality that may take place in 2010 and beyond, this report is the collective insight of Trend Micro threat experts, researchers, and engineers. Their combined knowledge of the existing computing landscape plus their years of experience in the field of security enable them to identify real-world technological trends and threats for home users and businesses in 2010 and beyond.

<sup>1</sup> *Trend Micro 2009 Annual Threat Roundup* ([http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend\\_micro\\_2009\\_annual\\_threat\\_roundup.pdf](http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf))

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### KEY PREDICTIONS FOR 2010 AND BEYOND

- No global outbreaks, but localized and targeted attacks.
- It's all about money, so cybercrime will not go away.
- Windows 7 will have an impact since it is less secure than Vista in the default configuration.
- Risk mitigation is not as viable an option anymore—even with alternative browsers/alternative operating systems (OSs).
- Malware is changing its shape—every few hours.
- Drive-by infections are the norm—one Web visit is enough to get infected.
- New attack vectors will arise for virtualized/cloud environments.
- Bots cannot be stopped anymore, and will be around forever.
- Company/Social networks will continue to be shaken by data breaches.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### TECHNOLOGICAL AND SOCIAL LANDSCAPE: WHERE WE ARE NOW AND WHERE WE ARE GOING

#### More Choices for Connectivity

Cybercriminals are driven by money. The money is primarily found where there is a large monoculture or where applications containing lots of valuable data are found. Today this means PCs and Macs are mainly targeted, but shifts in the technology industry coupled with business and consumer adoption mean that these targets are changing. In the future, mobile devices like smartphones and the public/private cloud will become greater targets for cybercrime.

Over the past few years, the threat landscape has shifted, there are no longer any global outbreaks, as were previously experienced with Slammer or CodeRed.

Over the past few years, the threat landscape has shifted, there are no longer any global outbreaks, as were previously experienced with Slammer or CodeRed. Even the much-covered Conficker incident of 2008 and early 2009 was not truly a global outbreak—rather it was a carefully orchestrated and architected attack. Going forward, localized and targeted attacks are expected to grow in number and sophistication.

In a 2009 Trend Micro smartphone survey, over 50% of smartphone users already surf the Web from their device for over 30 minutes per week. Of these, more than 12% are spending more than 120 minutes per week surfing the Web, and the numbers are growing.<sup>2</sup>

In 2010 we expect to see this behavior continue to grow, along with, and for the first time, an increasing handset monoculture. In this report we consider the implication of this development as it relates to the mobile threat.

#### Social Networking Sites

The increasing use of social networking sites will likely give cause to new tacks on old threat methods. Already social networks are heavily targeted by cybercriminals, for example, *Facebook*, which has over 300 million users,<sup>3</sup> was the original target of the KOOBFACE botnet.<sup>4</sup> Going into 2010, it is likely that social networks will continue to be the target of cybercriminals. However, it is also likely that social networks will be further used by legitimate businesses seeking new ways in which to communicate and engage with customers. For the business the challenge is how to harness the benefits of social networks while ensuring their own business networks remain secure. We outline the risks of social media in general later below.

<sup>2</sup> 2009 Smartphone Consumer Market Research Report (<http://trendmicro.mediaroom.com/index.php?s=23&item=503>)

<sup>3</sup> Facebook Press Room (<http://www.facebook.com/press/info.php?statistics>)

<sup>4</sup> The Real Face of KOOBFACE ([http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the\\_real\\_face\\_of\\_koobface\\_jul2009.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf))

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### Increasing Internet Penetration Worldwide

As the number of people from different countries gaining access to the Internet continues to grow, we see more and more non-English content being pushed online. This use of multiple languages increases the potential “market” for malware. Attacks in other languages such as Hindi, Chinese, Russian, and Portuguese are likely to increase in number.

### Google Chrome Operating System

New technologies such as the Google Chrome OS will also alter the cyber playing field. Many IT administrators are tired of the constant patching required with the use of the Microsoft OS, and so are evaluating whether it would prove safer and less time-consuming to switch to a new OS. On page 12 we examine the pros and cons of this opportunity and discuss why changing OSs will not completely remove the cyber threat—though there may be some initial benefits.

### Cloud Computing and Virtualization

Owing to the benefits cloud computing and virtualization offer consumers and businesses, it is likely that adoption rates will rise. A tough economy is also driving companies globally to adopt more cost-effective measures and pursue efficiency. This is one of the main reasons why analysts expect the virtualization industry to hit over US\$7 billion over the next four years.<sup>5</sup>

Cloud computing brings many benefits, of this there is no doubt, but education and awareness of associated risks is also necessary. With cloud computing, servers, like laptops before them, are moving outside the security perimeter and can be co-located in a remote facility among unknown and potentially malicious servers. Independent research and industry analyst reports indicate that 95% of data centers in 2009 are employing virtualization technology and 60% of production virtual machines (VMs) are less secure than their physical counterparts.<sup>6</sup>

Recent cloud-level disasters (like the Microsoft/Danger/Sidekick incident<sup>7</sup>) highlight certain risks associated with cloud computing. Data in the cloud is—broadly speaking—unprotected, unsecure, and often unrecoverable. Backup systems that work at cloud level are vital. Often, cloud providers depend on redundant array of independent/inexpensive disks (RAID) technology to protect data and enable service continuity. Later in this report, we examine some of the most notable threats to cloud computing and data centers.

► **Data in the cloud is—broadly speaking—unprotected, unsecure, and often unrecoverable. Backup systems that work at cloud level are vital. Often, cloud providers depend on RAID technology to protect data and enable service continuity.**

<sup>5</sup> *Core Protection for Virtual Machines* (<http://trendmicro.mediaroom.com/index.php?s=43&item=733>)

<sup>6</sup> *Trend Micro Server Security Strategy* (<http://trendmicro.mediaroom.com/index.php?s=43&item=758>)

<sup>7</sup> *Cloud Security Blog* (<http://cloudsecurity.trendmicro.com/danger-and-the-cloud/>)

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### NEW AND TOUGHER SECURITY CHALLENGES IN 2010

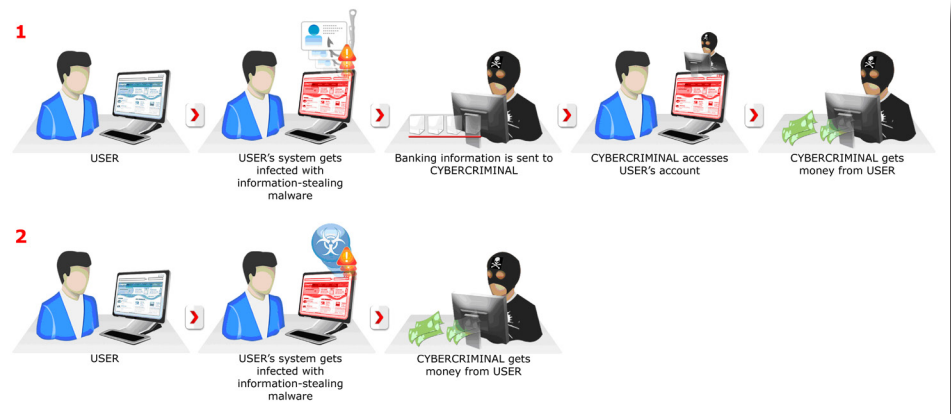
If the DOWNAD/Conficker infestation, Zeus botnet spam attacks, and KOOBFACE's remarkable use of social networking sites seen in 2009 are any indication, the oncoming threats in the following months will only grow in sophistication. Our researchers have identified major themes that have important security implications based on the directions that Internet technologies, user behavior, and cybercriminal activity are likely to take. The following sections discuss these factors in detail.

#### Cybercriminals will formulate more direct and brazen extortion tactics to obtain quicker access to cash.

The underground economy—of which the computing public is largely unaware—continues to attract more criminals partly because of the relatively small investment required to reap huge profits in various sectors of criminal operations. Each sector, from malware developers to anti-detection vendors, to botnet herders, is getting better at its own competency. For instance, in 2009, we have seen more sophisticated schemes to recruit money mules into “work-from-home” scams. These scams are really fronts for laundering cash or monetizing stolen information—the final step in most financially driven info theft.

However, much like legitimate businesses, as more players come into the game, profit margins will inevitably shrink. Additionally, financial companies are coming up with more stringent security measures (multi-factor authentication), making it just a bit harder for cybercriminals to conduct fraud. These will inspire mergers and takeovers among different cybercriminal players. Likewise, this will force some pioneering cybercriminals to formulate better and faster ways to turn stolen information into cash or to go directly after cash. This latter type of theft—called “cyber pickpocketing”—has already been seen in attacks such as BEBLOH, where the malware went beyond “traditional” keylogging by not only stealing credit card information but also accessing the account and transferring funds to another account. Expect there to be more attacks directly targeting victims' bank accounts in the coming year.

... Cyber pickpocketing means going directly after cash as seen in attacks such as BEBLOH, where the malware went beyond “traditional” keylogging by not only stealing credit card information but also accessing the account and transferring funds to another account.



*In 2010, attempts will be made by cybercriminals to go directly after cash.*

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

Moreover, cybercriminals will invent more brazen and uncompromising schemes to extort money from users and organizations. We have, for instance, seen this year new rogue antivirus ploys that no longer just display misleading signs of malware infection, but also employ ransomware components, holding important items such as the users' files or even their Internet connections hostage in exchange for payment. The next few months will likely see a continuation of this type of attack.

### Business as usual for botnets, but heavier monetization by botnet herders.



Botnets are networks of infected computers that communicate with each other without their users' knowledge. One of the first botnets to make it to the headlines is the Storm/NUWAR botnet in 2007, but this is hardly the first botnet ever tracked. Botnets have only become more varied throughout the years.

However, botnet masters do tend to emulate the most successful botnets in terms of evading detection over time. Based on this observation, there will be a preference for a peer-to-peer (P2P)-type botnet architecture as these are more difficult to take down. HTTP-based traffic will also be a communication of choice as it can get past most firewalls. Botnet masters will also look to host their operations on fast-fluxing networks<sup>8</sup> and avail of bulletproof hosting<sup>9</sup> for a certain number of nodes or controllers.

A sure trend is that more and faster monetization will become a priority for bot masters. Botnets will no longer be limited to being rented out for distributed denial of service (DDoS) attacks or spam runs. Bot masters will employ what is called the "pay-per-install" business model, wherein they get paid for every unique instance that the malware they were hired to distribute is installed on a system. We are already seeing this as a rising trend in 2009 when our researchers analyzed the behavior of BREDOLAB malware. BREDOLAB was found to be an enabler in the cybercriminal ecosystem by furthering the businesses (i.e., distributing the malware) of other cybercriminal groups.<sup>10</sup>

<sup>8</sup> Fast-flux networks are ever-changing networks of compromised computers that act as proxies.

<sup>9</sup> Bulletproof hosting is a service that shady Internet service providers (ISPs) sell that allows clients considerable leniency in the use of domains and are thus often favored for housing dubious or malicious operations.

<sup>10</sup> *You Scratch My Back: BREDOLAB's Sudden Rise in Prominence* by David Sancho ([http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/bredolab\\_final.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/bredolab_final.pdf))

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing



*Several players are involved in conducting the different stages and facets of cybercrime.*

### **Social networks and social media will be used more and more by cybercriminals to enter users' "circle of trust."**

► **Social engineering means manipulating people into performing certain acts or divulging information.**

Social engineering (manipulating people into performing certain acts or divulging information) will continue to play a big role on the Web in the propagation of threats. However, a wider demographic is spending more time on social networking sites, and creating and sharing social media. The social communities formed here can only attract cybercriminals into thriving here as well: as predators.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing



*The KOOFACE gang used one social media site after another to get more victims.*

► The features that are made to give the users the ability to build their own “circle of trust” usually cause them to end up mindlessly clicking buttons just to keep pop-ups and notifications from getting in the way of their browsing, making them easy bait for malicious ploys.

Users routinely share videos, pictures, stories and concepts with people they may or may not know in the real world. Through various privacy settings, access permissions, and numerous activity notifications, users are given a sense of control over what happens within their network. However, these features that are made to give the users the ability to build their own “circle of trust” usually end up bombarding the user with information that the users become passive. Users end up mindlessly clicking buttons just to keep pop-ups and notifications from getting in the way of their browsing, making them easy bait for malicious ploys.

Social networks, at the same time, are ripe venues for stealing personally identifiable information (PII). On a social engineering standpoint, the quality and quantity of data left lying around by most trusting users on their profile pages and interaction clues are more than enough for cybercriminals to stage identity thefts and targeted social engineering attacks. These can only get worse in 2010, with high-profile personalities suffering from online impersonators or stolen bank accounts. This will not be helped by the fact that meta-search engines will make it easier to get a hold of PII.

### **Mobile threats will have more impact.**

Mobile threats have been around for a while, but historically there has not been any mobile threat that had a high impact. As the mobile OS landscape changes, and with devices comprising a huge amount of memory and storing a host of sensitive data, devices such as the iPhone and Google Android may increase as a popular target for bad guys.

There are some indications that consumer acceptance of mobile phone-based financial activity is increasing, with handset banking applications even being advertised on prime-time television in some countries.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing



At the same time 2009 saw two distinct handset-based rudimentary botnets; one on the Symbian platform<sup>11</sup> which propagated through SMS and aimed to steal International Mobile Equipment Identity (IMEI) details, and one more recently that originated in Australia, and affected only jail-broken iPhones, but was later adapted and aimed at banking customers in the Netherlands, stealing details and passing them to a command and control (C&C) server in Lithuania.

With this change in consumer behavior and also the possibility, for the first time of some sort of handset monoculture being created there is increased potential for more mobile-related malicious activity, the extent of which will be dictated by consumer behavior.

### **Compromised products come straight from the factory.**

Users should be aware of potential threats created by devices that are already compromised or tampered coming off the shelves. Incidents about media players<sup>12</sup> and digital frames shipped with malware have already been reported in previous years. USB devices, while offering the convenience of quick connectivity, are responsible for the spread of autorun malware within networks. Recall that the Conficker/DOWNAD worm creators added a propagation capability that uses removable drives to increase spread. With the added user perception that newly purchased digital devices and accompanying installers and drivers are “clean,” cybercriminals are sure to find ways to step in anywhere between the manufacture of the product to its first use.

A similar risk is application compromise where a “known good” software has an embedded malware component. The user purchases and installs the software, and it does exactly what it is supposed to do, but it has a hidden purpose as well. The malware component is installed by engineers that have been either paid or coerced while in the employ of the company developing the software.

The risk of tainted products extends to hardware. For instance, some credit card dataphone devices used in several retail outlets have been identified as having compromised hardware.<sup>13</sup>

<sup>11</sup> *Signed Malware Coming to a Phone Near You* (<http://blog.trendmicro.com/signed-malware-coming-to-a-phone-near-you/>)

<sup>12</sup> *Get Your iPod Now--And Get a Free Worm!* (<http://blog.trendmicro.com/get-your-ipod-now-and-get-a-free-worm21/>)

<sup>13</sup> *Chip and pin scam 'has netted millions from British shoppers'* (<http://www.telegraph.co.uk/news/newstoppers/politics/lawandorder/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html>)

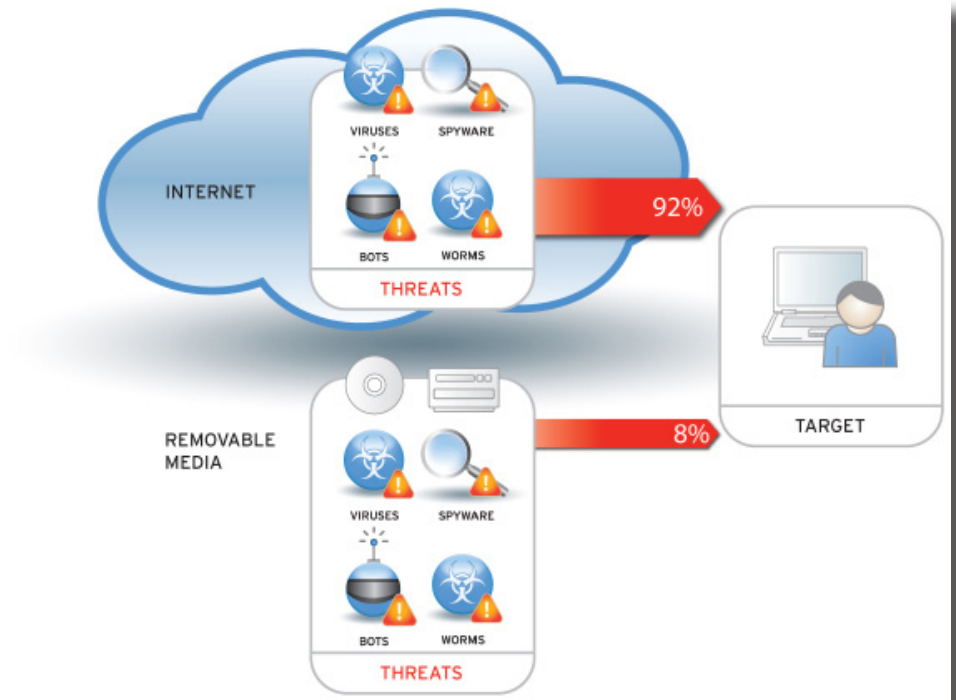
# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

▶ Cybercriminals will continue to abuse Internet-browsing behaviors, platforms, and technologies, finding new and better ways to deliver their different payloads.

### Web threats will continue to plague Internet users.

Trend Micro accurately predicted the rise of Web threats, calling out the shift to financially driven attacks orchestrated over the Web. Unfortunately, Web threats are not going away anytime soon. Cybercriminals will just continue to abuse Internet-browsing behaviors, platforms, and technologies, finding new and better ways to deliver their different payloads.



*The majority of malware threats that affect users today come from the Web.*

### Poisoned Searches

Blackhat search engine optimization (SEO) will become a more frequently used avenue for initiating Web attacks. Cybercriminals will be able to affect a wider range of audiences through data mining and identifying trends on the Web, such as top searches in *Google* and trendy topics in *Twitter*.

The bad guys regularly check for the most searched for strings, so that they can target those users searching for popular topics such as the death of Michael Jackson with malicious pages promoted through search strings. This poses a huge risk for users as search functionality is probably one of the most used tools on a daily basis.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

▶ Drive-by downloads through the use of malicious scripts will present a grave threat to users since such attacks require minimal interaction—one visit to a tainted website—for the malicious routines to commence.

### More Malicious Scripts, Fewer Binaries

Scripts will in most ways replace binaries in terms of Web attacks. The usage of scripts in the first level of infection as well as in the execution of malicious routines has been observed in recent Web attacks, and is bound to continue, if not prevail, in the future. Scripts serve the same purpose as executable files with the added advantage of being easier to plant in websites and harder for users to detect.

In addition, drive-by downloads are also bound to continue through the use of malicious scripts. This will present a grave threat to users, since such attacks require minimal user interaction—one visit to a tainted website—for the malicious routines to commence.

### Malvertisements

Malvertisements will continue to be a grave threat to both users and legitimate advertisers. Cybercriminals may also change the nature of the tainted advertisements to more mainstream content, making it harder for users to determine which ones are legitimate and which ones are malicious.

### Application Vulnerabilities

#### MICROSOFT WINDOWS

Despite the new channels presented on the Web for malware, cybercriminals will not cease using vulnerabilities to get into systems. Especially with the release of Windows 7 and the rise of the 64-bit platform, cybercriminals will take the challenge presented to them by developers and find vulnerabilities to exploit.

#### MAC THREATS

While cybercriminals are likely to take advantage of any given monoculture (i.e., Windows for desktop computers) in crafting their attacks, they have been found—especially in 2009—to create high-impact malware targeting Mac users. They are unwittingly encouraged by Mac users' preconceived notion that Macs are "safe and virus free." Thus Mac users are more than likely to let their guards down when it comes to security. Threats like OSX\_JAHLAV.I,<sup>14</sup> which pose as legitimate applications and then change the system's Domain Name System (DNS) settings to redirect the victims' browsers to malicious sites without their knowledge, will simply become more sophisticated going into 2010.

<sup>14</sup> *Threat Encyclopedia* entry for OSX\_JAHLAV.I ([http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=OSX\\_JAHLAV.I](http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=OSX_JAHLAV.I))

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### New Technologies Offer Greater Security

The new OS—Google Chrome—offers many IT administrators hope for a safer computing experience. Many of these administrators, IT directors, and chief security officers (CSOs) are tired of the constant system patch battle and constant security software updates. Whether Google Chrome can actually offer this safety is a very difficult question. There is a major cyberwar currently taking place, with the majority of threats created for the primary purpose of theft. Cybercriminals are making a great deal of money from malware, hacking, and other malicious activities.

Cybercriminals currently take advantage of the fact that the desktop market is mostly dominated by Microsoft's OS. For attackers focusing on Microsoft platforms, there are simply enough machines available for them to make sufficient money. This is purely economy of scale. As other OSs (for example, the Mac OS) continue to increase in popularity and gain desktop market share, it is not surprising that, as discussed earlier in this report, we also see an increasing number of attacks aimed at them.

However, with Google Chrome, the OS is very small and open source, and the data and applications are stored in the cloud. This means there should be fewer bugs, as there are fewer lines of code. As it is smaller it is also not so powerful, so locally installed multipurpose malware perhaps could become a thing of the past.

However, this said, we also know that cybercriminals are very adept and agile—their attacks are sophisticated and they regularly alter their focus to misuse the latest technological trends.

Based on this, it is possible that certain attack scenarios could still work such as:

- **It is possible that certain attack scenarios could still work such as:**
- Manipulating the connection to the cloud
- Attacking the cloud itself
- Cloud vendor data breaches

- **Manipulating the connection to the cloud.** If a cybercriminal were to fiddle around with the OS code, just a little bit to change the DNS records. A user might first visit an underground site, which then automatically redirects to his/her Web application page. This might reveal all the user's data, if the communication channel cannot be locked down. It is possible to rely on a combination of IPv6, encryption, and certificates, but this is still a possible attack vector.
- **Attacking the cloud itself.** If cloud-based applications and cloud-driven OSs become mainstream, a 99.99% availability is absolutely critical. A computer is unable to reach the information and application host is useless. Attackers could potentially use standard botnets (as we will certainly see bot-infected computers on standard multipurpose OSs for the next 10 years) to overload the cloud infrastructure of the host. Or an attacker might "ask" for the payment of a small "donation" to ensure that the cloud host, being overwhelmed with requests, could deliver the service again. These would certainly provide a lucrative business for cybercriminals.

In fact, these types of attack are already taking place, albeit on a small scale, but if one business driver (infect desktop computers with malware to misuse them) loses importance or profitability (not enough targets to reach anymore) then another business model will replace it.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

- **Cloud vendor data breaches.** The theft of valuable items (credit card information, social security numbers, login credentials) in the cloud (they can no longer be grabbed from victims' computers) is a major concern and consideration for any business or home user. The question is whether any cloud vendor could reasonably ensure that unauthorized access is not possible—that a hacker will never be able to copy millions of user records, login credentials, online banking information, billing information, transaction records, and the like.

### Changes to the Internet infrastructure will widen the playing field for cybercriminals.

#### IPv6 Experimentation Stages

IPv4 had a major coming of age in the mid- to late-1990s. Many weaknesses were discovered as the Internet came into its own. Much of the same pattern is projected to be seen in IPv6. Protocol and implementation weaknesses will be discovered and the user base expands.

Considering the current low adoption rates and the increase of doom-n-gloom about the exhaustion of IPv4, adoption of IPv6 by malware will not be a major factor in 2010. However, as users start to explore IPv6, so will the cybercriminals. Therefore users can expect to find some proof-of-concept elements in IPv6 to fly in 2010. Possible abuse includes new covert channels or C&C, but not so much on active targeting of the IPv6 address space—at least not in the very immediate future.

#### Internationalized Domain Names

The introduction of regional top-level domains (Russian, Chinese, and Arabic characters) will create new opportunities to age-old attacks through look-alike domains for phishing—using Cyrillic characters in place of similar-looking Latin characters. This will lead to reputation problems and abuse that will be difficult to stop. Considering how difficult it already is to get malicious *.cn* domain names shut down, it is certain that this problem will get worse as new top-level domain names get introduced. Users will need to be ever more vigilant when opening emails and there is no doubt that traditional spam filters will be unable to keep up with this escalating threat.

### Cloud computing will present new security challenges.

A Trend Micro cloud computing survey<sup>15</sup> conducted in 2009 indicated that businesses considering cloud computing also view security solutions providing protection into the cloud to be important. When asked about potential security threats, 61% of the respondents reported that they are holding off on cloud computing solutions until they are reasonably sure that there are no significant security risks to their network as a result.

• The introduction of regional top-level domains will create new opportunities to age-old attacks through look-alike domains for phishing—using Cyrillic characters in place of similar-looking Latin characters.

<sup>15</sup> *Cloud Computing* (<http://trendmicro.mediaroom.com/index.php?s=23&cat=18>)

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

Trend Micro agrees with industry analysts who have predicted that cloud adoption is about to take off, and grow exponentially. It is likely that the three following reasons will force the hand of businesses:

- **Internet pressures.** Cloud computing is easy and the success of public clouds like *Amazon* means that your internal “clients” have alternatives for computing power readily available to them.
- **Cost savings.** It is cost effective and with the economy still uncertain, cost savings are paramount.
- **Competitive advantages.** It is being adopted by your competition and it will enable competitive advantages.

However, cloud computing will bring some developments to the threat landscape. Below we examine some of the more notable challenges and threats.

### New Threats to the Data Center and Cloud Computing

Often, a challenge for those new to, and beginning to consider cloud computing is differentiating between different cloud threats, depending on the cloud service model. There are currently three primary service models:

- **Software as a service (SaaS).** This refers to Internet-based access to applications (examples: *salesforce.com*, Trend Micro HouseCall).
- **Platform as a service (PaaS).** This refers to services used to deploy customer-created applications to the cloud (examples: *Google AppEngine* and *Microsoft Azure*).
- **Infrastructure as a service (IaaS).** This is sometimes called “utility computing,” which refers to renting processing, storage, network, and other resources (examples: Amazon’s *EC2*, *Rackspace*, and *GoGrid*). The consumer does not manage the underlying cloud infrastructure, but does control the OSs, storage, networking, deployed applications, and select network components (firewall).

So, there are companies dedicated to a particular task and focus on delivering security for that task. On the other hand, having multiple systems secured the same way makes them a more attractive target for cybercriminals. This creates the potential for one customer to get caught up in the bad guy’s attempts to take a fellow customer offline.

One popular discussion point is whether the change to the network perimeter caused by public cloud computing is putting risk upon the applications and OSs deployed using cloud computing. As the cloud computing trend continues and the data entrusted to the cloud becomes more sensitive, the overall risk grows.

Similarly, the increased dependency on service providers is a potential threat in both availability and confidentiality of data. Service providers may go out of business, or may have physical or internal breaches. Giving a high level of trust like this to public providers opens up a number of new threats.

- **Cloud computing currently comes in three primary service models:**
  - SaaS or Internet-based access to applications.
  - PaaS or services used to deploy customer-created applications to the cloud.
  - IaaS, sometimes called “utility computing,” or renting processing, storage, network, and other resources.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

When examining the possible new and emerging threats, there is also a risk of forgetting that all the old problems still apply—it is most likely that cybercriminals will refine their current tactics to take advantage of weaknesses in new technologies.

SaaS/PaaS customers must rely on what the SaaS/PaaS vendor has in place for security. A certain level of trust needs to be placed in the vendor for their security countermeasures. This is certainly an area to consider and track for new and emerging threats.

IaaS is an area owned by enterprise businesses and the IaaS service provider. Threats to this area include those found in OSs and hypervisors (such as Xen, VMware, Hyper-v) along with application vulnerabilities.

A key challenge is that even if an IaaS provider's security is near perfect, the business relying on it, ties itself into one sole provider and loses the benefit of being able to switch between providers at will or in line with business needs.

All of the different OSs, switches, hypervisors, firewalls, and vulnerabilities become the IaaS provider's responsibility to maintain and protect—this offers some benefit for certain organizations but similarly offers an enormous attack surface.

Another risk area is from the inside. In this scenario, rogue internal staff may also have access that enables them to bypass pretty much any or all of the provider's security procedures.

IaaS is appealing to many organizations because they can retain a greater amount of control and because it is probably the easiest of the layers to switch vendors with. The security perimeter is different to what they are used to—instead of being the edge of the data center it becomes the edge of each VM or even the data within that machine. Already several startups in The Valley allow users to seamlessly switch between hardware from leading IaaS players. Many organizations are just waiting for a security model for the cloud which they can own and move with them from vendor to vendor, retaining control and removing the need to alter audited processes and procedures as they migrate their machines.

### Multi-Tenancy in the Cloud May Create New Threats

Threats such as side-channel attacks or information leakage may come about if, for example, a user is issued memory/disk space another user discarded without it being zeroed out.

### Data Center Attacks

Right now, the number of compromised sites is considerable enough to cause worry. These sites are either made to host malware, exploits, or drop points for stolen information. This is not helped by the fact that the associated Web hosting companies lack security. Unfortunately, these infiltrated sites can also be used as stepping stones to attack other servers within the same data center. This might be done by installing rogue DHCP servers, rogue routers, or traffic snoopers. These data center attacks will be the escalated versions of today's mass site compromises.



# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### Unsecure Management Systems

The hypervisor is the software that enables multiple VMs to run within a single computer. Hypervisors bring both new capabilities and new computing risks. As virtualization becomes mainstream, it will become ever more important to find new ways to identify risks and protect these new infrastructures. Hypervisors, while central to all virtualization methods, are a core risk area.



The hypervisor can control all aspects of all VMs running on the hardware, so it is a natural security target. Securing the hypervisor is vital and more complex than it first seems.

VMs make requests to the hypervisor through several different methods, usually involving a specific application programming interface (API) call. An API is the interface created to manage the VMs from the host machine. These APIs are prime targets for malicious code, so substantial effort is made by all virtualization vendors to ensure that the APIs are secure, and that only authentic (authenticated and authorized) requests are made from the VMs. This is a critical path function. It should be noted, however, that speed is a significant requirement in all hypervisors, to ensure that the overall performance is not affected.

An example of these management systems as a new attack target was seen in the HyperVM/LKLABs issue, where 30,000 websites in the United Kingdom vanished because of a vulnerability in the management system controlling the virtual servers.

Certain virtualization vendors, such as Amazon Web Services have made their APIs public and will undoubtedly become interesting targets for cybercriminals. Those vendors who have not made their APIs public (for example, vSphere), while not usually exposed externally, could potentially become a target for malware within the perimeter.

There is a risk that, owing to the rapid change in the API space and the current race to market, management systems will, in the future, not be secure.<sup>16</sup>

### Economic Denial of Service

When organizations use cloud computing (either public or “cloudburst”—from the private to public, to handle load) there is a danger of economic denial of service (DoS) where malicious DDoS traffic cannot be differentiated from good traffic and the scaling to deal with the load costs the organization money.

### Higher Levels of Abstraction on Fragile Technologies

Border Gateway Protocol (BGP), DNS, and Secure Sockets Layer (SSL) are all technologies that are being built upon more and more. They were developed before security was a consideration and being asked to perform their respective functions under greater loads than ever anticipated during development. There is a risk that at some point they will become vulnerable, if vulnerabilities in such complex applications, running in data centers and public/private clouds cannot be patched.

<sup>16</sup> *Cloud Computing Standards, Dream Vs. Reality* (<http://cloudsecurity.trendmicro.com/cloud-computing-standards-dream-vs-reality/>)

# The Future of Threats and Threat Technologies

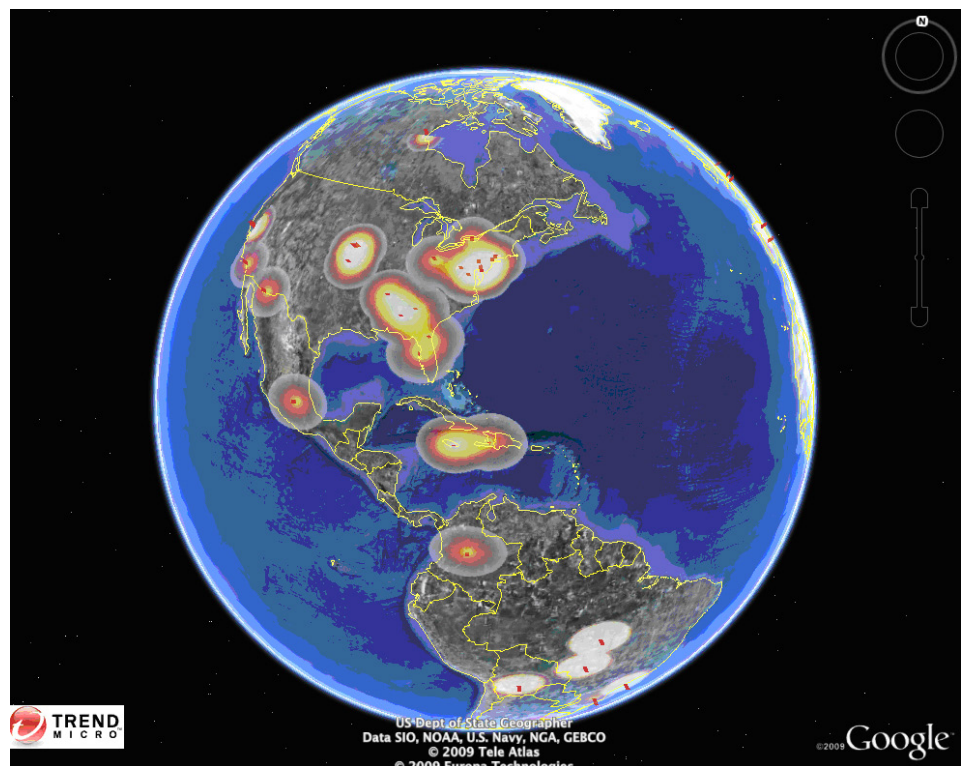
## How the Landscape Is Changing

### New Border Gateway Protocol Tricks

In 2010 and beyond, a continuing concern will be the stability and security of the global routing infrastructure. In February 2008 we saw state-sponsored prefix hijacking.<sup>17</sup> Following this in February 2009 a small Czech Internet provider announced routes with extremely long ASpaths that crashed some neighboring routers, causing widespread outages.<sup>18</sup>

While intentional attacks are currently thought to be few and far between, errors in routing configurations and latent bugs in routing software will present an element of risk in 2010 and beyond.

While intentional attacks are currently thought to be few and far between, errors in routing configurations and latent bugs in routing software will present an element of risk in 2010 and beyond.



A heat map of BGP updates from a 5-minute sample to localize major routing events.

<sup>17</sup> Pakistan blocks YouTube ([http://www.theregister.co.uk/2008/02/25/pakistan\\_blocks\\_youtube/](http://www.theregister.co.uk/2008/02/25/pakistan_blocks_youtube/)) and YouTube (<http://www.ripe.net/info/ncc/presentations/MENOG3-dranse-youtube.pdf>)

<sup>18</sup> Global Internet outage (<http://wiredness.com/2009/02/global-internet-outage/>) and VirtualIt Eliminating Router Bugs (<http://www.cs.princeton.edu/~minlanyu/talk/nanog46.pdf>)

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### WHAT THIS MEANS FOR USERS: KNOW YOUR THREATS, COME PREPARED

TrendLabs analysis indicates that a new piece of malware is now created every 1.5 seconds. Given the speed with which it is being created combined with the malicious intent to defraud innocent computer users and reputable businesses, a new set of technologies and new methods need to be employed. Traditional virus patterns and spam filters alone will not be sufficient.

From this Trend Micro 2009 future threats report, the following points are clear:

- Cybercriminals will formulate more direct and brazen extortion tactics to obtain quicker access to cash.
- Business as usual for botnets, but heavier monetization by botnet herders.
- Social media will be used by malware to enter the users' "circle of trust."
- Web threats will continue to plague Internet users.
- Cloud computing will present new security challenges.
- Changes in the Internet infrastructure will widen the playing field for cybercriminals.

Central to protection from Trend Micro is the Trend Micro Smart Protection Network. This next-generation cloud-client content security infrastructure is designed to block threats before they reach your network. It combines Internet-based—or "in-the-cloud"—technologies with smaller, lighter-weight clients that provide you with immediate access to the latest protection wherever and however you connect—from home, within your company's network, or on the go. More information on this and other Trend Micro technologies is available at [TrendWatch](#).

**To stay safe amid the current threat landscape, end users should:**

- Keep their PCs current with the latest software updates and patches.
- Protect themselves and their PCs.
- Choose secure passwords.

### Advice for End Users

#### Keep your personal computer current with the latest software updates and patches.

- Apply the latest security updates and patches to your software programs and OSs and enable automatic updates where possible. Since cybercriminals typically take advantage of flaws in the software to plant malware on your PC, keeping your software current will minimize your exposure to vulnerabilities.

#### Protect yourself and your personal computer.

- If you receive an email requesting personal or confidential information, do not respond or provide this information via links or phone numbers in the email. Legitimate organizations such as credit card companies and banks will never request this information via email.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

- Beware of unexpected or strange-looking emails and instant messages (IMs) regardless of sender. Never open attachments or click links in these emails and IMs. If you trust the sender, scan the attachments before opening. Never provide personal information in your email or IM responses.
- Regularly check your bank, credit, and debit card statements to ensure that all transactions are legitimate.
- Beware of Web pages requiring software installation. Scan programs before executing them. Always read the end-user license agreement (EULA) and cancel if you notice other programs being downloaded in conjunction with the desired program.
- Do not provide personal information to unsolicited requests for information.
- If it sounds too good to be true, it probably is. If you suspect an email is spam, delete it immediately. Reject all IMs from people whom you do not know.
- When shopping, banking, or making other transactions online, make sure the website address contains an *s* as in *https://www.bank.com*. You should also see a lock icon in the lower right area of your Web browser.

### Choose secure passwords.

- Use a combination of letters, numbers, and symbols and avoid using your first and last names as your login name.
- Avoid using the same password for all your login needs. Do not use the same password for your banking site that you use for your social networking sites.
- Change your password every few months.

### Advice for Businesses

#### Use effective solutions to protect your business.

- To protect your company network, deploy solutions that use cloud-based protection. Technology such as the Trend Micro Smart Protection Network combines Internet-based (“in-the-cloud”) technologies with lighter-weight, clients to help businesses close the infection window and respond in real time before threats can even reach a user’s PC or compromise an entire network. By checking URLs, emails, and files against continuously updated and correlated threat databases in the cloud, customers always have immediate access to the latest protection wherever they connect.
- Phishing poses a significant threat for organizations. Phishing sites can compromise your brand and/or your company’s image as well as your ability to keep your customers’ confidence while conducting business over the Internet. Protect your employees and customers by procuring all brand-related and look-alike domain names.

• To stay safe amid the current threat landscape, organizations should:

- Use effective solutions to protect their business.
- Safeguard their customers’ interests.
- Establish and implement effective IT usage guidelines.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

- Stay ahead of the threats by reading security-related blogs and related information pages (i.e., Threat Encyclopedia and TrendLabs Malware Blog) which can help warn and educate users who might otherwise be drawn to web sites under false pretenses.
- Educate your employees about how cybercriminals lure victims to their schemes, make use of threat information provided on security vendor sites like [TrendWatch](#).
- Try downloading tools such as the Trend Micro [Threat Widget](#) to help raise awareness

### Safeguard your customers' interests.

- Standardize company communications and let your customers know about your email and website policies. This way, you can help your customers better identify legitimate messages.
- Avoid sending “phishy”-looking email messages by following these guidelines:
  - Do not request personal information through email.
  - Personalize email when possible.
  - Do not redirect to another domain from the URL provided to customers.
  - Do not rely on pop-up windows for data collection, especially those with no address bars or navigational elements.
  - Do not use instant messaging or chat with customers unless they initiate the communication.
  - Be explicit in the detail of communications that require the immediate action or attention of recipients.

Protecting a business requires education about safe cybersecurity practices.

### Establish and implement effective IT usage guidelines.

- Just as you would never leave your front door unlocked when you are not home, you must take the same precautions with your computer system to make sure your business is protected. Protecting your business requires you to educate yourself and your employees about safe cybersecurity practices. A comprehensive set of IT usage guidelines should focus on the following:
  - **Prevention.** Identify solutions, policies, and procedures to reduce the risk of attacks.
  - **Resolution.** In the event of a computer security breach, you should have plans and procedures in place to determine what resources you will use to remedy a threat.
  - **Restitution.** Be prepared to address the repercussions of a security threat with your employees and customers to ensure that any loss of trust or business is minimal and short-lived.

# The Future of Threats and Threat Technologies

## How the Landscape Is Changing

### RESOURCES AND USEFUL LINKS

- *A Security Guide to Social Networks* by threat researcher David Sancho is available for download at <http://us.trendmicro.com/us/trendwatch/research-and-analysis/white-papers-and-articles/index.html>.
- Trend Micro Free Prevention and Remediation Tools are available at <http://free.antivirus.com/>.
- Further information for the awareness and prevention of threats for large enterprises through to home users is available at <http://us.trendmicro.com/us/trendwatch/awareness-and-prevention/index.html>.
- Current events in threat and vulnerability information can be found at <http://us.trendmicro.com/us/trendwatch/current-threat-activity/index.html>.
- Informative articles outlining the latest Web threats are available at <http://us.trendmicro.com/us/trendwatch/research-and-analysis/web-threat-spotlight/index.html>.
- *TrendLabs Malware Blog*: <http://blog.trendmicro.com/>
- *Trend Micro Cloud Security Blog*: <http://cloudsecurity.trendmicro.com/>
- *Trend Micro CounterMeasures Blog*: <http://countermeasures.trendmicro.eu/>
- For the latest information about Trend Micro's revolutionary cloud security technology visit <http://us.trendmicro.com/us/trendwatch/core-technologies/index.html>.

#### TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).

#### TREND MICRO INC.

10101 N. De Anza Blvd.  
Cupertino, CA 95014

**US toll free:** 1 +800.228.5651

**Phone:** 1 +408.257.1500

**Fax:** 1 +408.257.2003

[www.trendmicro.com](http://www.trendmicro.com)

