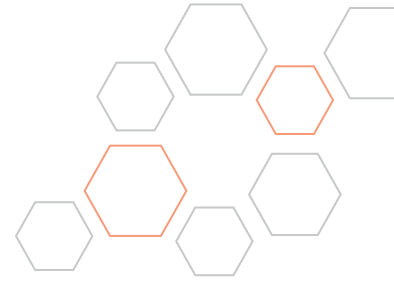






## ➔ Executive Summary



All data provided in this report was gathered from TrendLabs<sup>SM</sup>—Trend Micro's global threat research and support organization that provides customers with 24x7 response to the latest threats—as well as from Trend Micro's Network Security Services.

The era of the global outbreak is over. Today's threats are

- **Stealthy**—they try to remain undetected
- **Regional and targeted**—they go after users in a specific region or country or users of a specific type of Website
- **Blended and sequential**—they use combinations of malware that each play a role in the delivery of the payload
- **Web-based**—they use the Web for delivery, update, and entrenchment and to report back stolen information
- **Profit-driven**—their goal is to make money

There are economies built around the creation, sale and utilization of malware. The first six months of 2007 present several examples of just how the threat landscape has evolved, including "Storm" at the beginning of the year and the "Italian Job" most recently in June.

Trend Micro continues to see explosive growth in Web threats and little abatement in messaging threats. Web threats, threats that use the Internet to perform malicious activities unbeknownst to the PC user, persist in their utilization of automated techniques and exploitation of vulnerabilities to achieve identity and information theft. They target specific groups of users and employ blended techniques to accomplish their goals.

The technologies and techniques used for malicious purposes continue to grow more sophisticated. During the first half of 2007, Trend Micro saw file infectors taking on new roles, social engineering techniques becoming very adept at leveraging current affairs, phishing scams targeting smaller regional establishments, and authentic looking email messages carrying malware. The use of Web 2.0 technologies, such as Javascript, was frequently used for drive-by-downloads, where users need only visit a malicious URL to become infected.

The first half of 2007 also brought with it a renewed vigilante-style interest in undiscovered application and OS vulnerabilities, as various Month of Bugs projects emerged to challenge software developers. As a result, malware exploiting these vulnerabilities was written

and introduced into the wild. Web applications experienced the brunt of the attacks, as latent vulnerabilities were used in XSS and XSRF attacks targeting social networking sites.

Perhaps the most disturbing development is the persistent rise in the use of bots and botnets to distribute spam and malware and perpetrate cyber crimes. Botnets remain the most powerful tool at malware authors' disposal in the bid for computer-automated crime. Several malware activities during this period continue to betray a possible underground economy that harnesses the computing power of compromised computers to perform certain tasks.

In an effort to provide the best analysis, Trend Micro looks for new ways to analyze and understand the threat landscape as it evolves. This report examines threats in the following categories:

1. **Infrastructure vulnerabilities:** Threats that originate from the existence of security weaknesses in applications, network architecture or operating systems.
2. **High-impact threats:** Threats that have the capacity to cause very high localized damage. Examples include global outbreaks and targeted attacks.
3. **Content-based threats:** Threats which are delivered to the target victim as part of content, such as phishing or spam.
4. **Process-based threats:** Threats that are in the form of an executable application resident on the host PC. Examples include malware, spyware and adware.
5. **Distributed threats:** Threats, like bots, where the infection is used to mount an attack on a third-party victim.

## → Infrastructure Vulnerabilities

Malware authors rely on security holes in software applications to be able to introduce malicious code to a user's computer. Some proactively look for vulnerabilities and sell their information in digital black markets. Some wait for public disclosure of the vulnerability, then craft an exploit hoping to reach users before vendor updates are created. Inadvertently helping the cause were initiatives such as the "Month-of" projects—like January's Month of Apple Bugs and March's Month of PHP Bugs—where developers and programmers were encouraged to find and flag software holes.

### XSS: A Bane to the Web 2.0 Boon

Vulnerabilities exist not only in software products but also in Internet applications, such as cross-site scripting. JS\_QSPACE.A, a malicious JavaScript discovered last December, took advantage of a QuickTime HREF Track feature and a MySpace XSS vulnerability. Later in March, a new malicious script exploiting another flaw in QuickTime in conjunction with MySpace was detected as JS\_SPACESTALK.A. It is imperative that developers of Web 2.0 applications balance providing innovative applications and elegant usability with secure applications. Often, security is the second priority.

### Vector Markup Language Exploits

A week after the January 9th release of Microsoft patches, which addressed the way Windows handles Vector Markup Language, an exploit for the patch appeared in the wild. It was soon followed by several other variants at a rate of almost two a month (Table 1). This illustrates the importance of keeping a computer updated with the latest patches, considering the speed with which exploits are created soon after vulnerabilities are discovered.

Detection Name	Date of Detection
EXPL_EXECOD.C	Jan. 16, 2007
HTML_VMLFILL.I	Jan. 24, 2007
JS_DLOADER.KQZ	Feb. 2, 2007
HTML_IFRAMEBO.AE	Feb. 12, 2007
HTML_IFRAMEBO.AC	Mar. 16, 2007
JS_IFRAMEBO.BG	Apr. 29, 2007

Table 1: Vector Markup Language exploits and dates of detection

### Exploit Toolkits

Another trend is the proliferation of exploit toolkits. These toolkits automate the generation of code that is used to exploit known vulnerabilities. For the MS07-004 release, referenced above, the following exploit kits were identified:

Detection Name	Date of Detection
HKTL_EXPLOITER.J	Mar 28, 2007
HKTL_EXPLOITER.K	Apr 6, 2007
HKTL_EXPLOITER.L	Apr 6, 2007

Table 2: MS07-004 exploit toolkits and dates of detection

Exploit kits for MS07-017 were also discovered. In the same vein, other commercial-grade software, such as MPack which was used in the Italian Job IFrame attack, are being sold and distributed in underground channels. These exploit kits are continuously updated as new vulnerabilities are discovered and purchasers are able to pay to upgrade. This further makes the creation of code targeting unpatched systems easier for script kiddies.

### Other Notable Exploits

Several Trojans were discovered to exploit Windows applications, specifically Microsoft® Office Word. These proof-of-concept Trojans remained in the wild as December's Patch Tuesday (Microsoft's regular release of security bulletins addressing identified software vulnerabilities) came and went. The popularity of this exploit is attributable to the universality of Word. Other variants exploiting Microsoft Office Excel and PowerPoint soon followed.

In December, Microsoft confirmed the existence of the first Windows® Vista flaw, a Proof-of-Concept code that targeted the Client Server Run-Time Subsystem. Other operating platforms were not immune, including the Sun Solaris 10 Telnet service which became exposed in February (ELF\_WANUK.A).

Over past several months there has been an active bounty hunt for software vulnerabilities, translating into an increase in malware exploits. The most notable, the Windows ANI vulnerability relating to the way Windows handles animated cursors, caused Microsoft to release an out-of-cycle patch as reports of infections quickly rose.



## → High-impact Threats

The high-impact threats from the first half of this year illustrate how malware authors can deploy codes that specifically target victims with the help social engineering.



Figure 1: High-Impact Threats Detected from December 2006 to May 2007

### The Stormy Saga of TROJ\_SMALL.EDW Mutations

TROJ_SMALL.EDW Infections Per Region (Dec 06 to May 07)	
North America	57%
Asia	19%
Europe	19%
Australia	5%

Table 3: TROJ\_SMALL.EDW infections by region

The NUWAR family emerged in 2006, but it made headlines in January, when specific Trojan variants arrived via spammed email messages. Leveraging a 200-kph storm ravaging Eastern Europe, a slew of email messages containing the subject “230 dead as storm batters Europe” were spammed to unsuspecting recipients. Concerned and curious, recipients who were lured into opening the attachments named full Clip.exe, full Story.exe, full Video.exe, and read More.exe, inadvertently introduced a Trojan downloader onto their computers.

In April, a WORM\_NUWAR variant was detected to be carrying TROJ\_SMALL.EDW, the same Trojan that made its rounds in Europe earlier in the year, only this time the subject headers were the following ominous but unreal pronouncements:

- Iran Just Have Started World War III (sic)
- Israel Just Have Started World War III (sic)
- Missile Strike: The USA kills more then 1000 Iranian citizens
- Missile Strike: The USA kills more then 10000 Iranian citizens
- Missile Strike: The USA kills more then 20000 Iranian citizens
- USA Declares War on Iran
- USA Just Have Started World War III (sic)
- USA Missle Strike: Iran War just have started (sic)

Email worms from the same family sent other messages with catchy headlines such as: ‘Spyware Activity Detected!’ ‘Virus Alert!’ ‘Worm Detected!’, ‘A Token of My Love,’ ‘Come Dance with Me,’ and ‘Our Love Will Last’. The persistence of these infections relies on the authors’ ability to craft engaging and timely subject headers in order to hook more victims in a short amount of time. As the infection counts show, although more than half of the infections remain in North America, numbers from Asia and Europe are still increasing.

### TROJ\_SMALL.GHI Spreads False News of Australian PM’s Death

SMALL continued to find victims. February found unsuspecting Australians clicking on mass-mailed email messages purporting to contain details about the supposed heart attack of Australian PM John Howard.

Among the subject lines the email messages used are the following:

- Current Australia’s Prime Minister survived a hear (sic) attack
- The life of the Prime Minister is in grave danger
- Prime Minister survived a heard (sic) attack

The email message even contained a link to a bogus news site specially crafted to mirror the popular legitimate Web site The Australian. The fake site had a second invisible IFrame that covertly accessed a second URL with obfuscated scripts which, in turn, took advantage of old Internet Explorer vulnerabilities. This set in motion a download routine that was as complex as it was coordinated.

First, a Trojan downloader checked to eliminate systems located in Estonia, Latvia, and Lithuania—possibly because the malware creators were from these countries and wanted to avoid rousing the suspicion of local authorities.

Second, a backdoor component dropped another component that served as its watchdog as it sent and received messages to specific servers via random ports. The servers behaved like botmasters, raising the suspicion that the backdoor could have been a creator of an impromptu zombie network.

### TROJ\_ANICMOO.AX Tricks Asian Animated Cursor Fans



## → Content-based threats

**TROJ\_ANICMOO.AX Infections Per Region  
(Dec 06 to May 07)**

Asia	83%
North America	13%
Europe	4%

Table 4: TROJ\_ANICMOO.AX infections by region

In March, a Trojan exploiting an unknown vulnerability in the way Windows handles animated cursors prompted Microsoft to release an out-of-cycle patch. This .ANI file downloaded other malware from malicious URLs. 83% of the infections occurred in Asian countries. While the motive remains unknown, the attack may provide insight as to where the malware author resides or who his intended victims were.

### JS\_DLOADER.KQZ Spoils Super Bowl Weekend for Football Junkies

**JS\_DLOADER.KQZ Infections Per Region  
(Dec 06 to May 07)**

North America	96%
Asia	2%
Europe	2%

Table 5: JS\_DLOADER.KQZ infections by region

During the first week of February, malware authors attempted to capitalize on Super Bowl XLI in the United States. They created a malicious script, hacked into the official site of the Miami Dolphins Stadium, and delivered a keylogger to anyone who happened to visit the site as part of a "drive-by-download."

The malware associated with this attack included TROJ\_ZLOB.BZE, which downloaded a spyware once the user visited the hacked site, and TSPY\_WOWCRAFT.BL, which gathered sensitive account information from the affected systems. TSPY\_WOWCRAFT.BL is from a family of spyware that specifically stole information related to the popular online game World of Warcraft. Although the attack against the Dolphin Stadium Web site received the most attention, it was the several other Web pages, mostly from gaming sites, which reflect the real intention of the author(s) that planted the codes.

Fortunately, damage to victims of JS\_DLOADER.KQZ from the Dolphin Stadium Web site was limited as security companies working in tandem with law enforcement alerted the site administrators, who were able to remove the malware after a couple of hours.

### SPAM

Unsolicited email messages that contain links which download malware continued to rise during the first months of 2007. Botnets have been implicated for a significant volume of spammed email messages sent out during the previous months. The payloads of worm families NUWAR and STRATION provide evidence of an orchestrated effort to pool computing power for a very specific end: which is to send out unsolicited mail to the most number of users.

Data from TrendLabs shows that spammed email messages are still largely written in English. However, Asian languages such as Japanese and Chinese now claim the top spot in terms of the most popular non-English spam languages and Korean has emerged in the top 10. Spanish and Russian language spam have fallen on the list and now follow Asian language spam. Commercial subject matter remains the popular spam content.

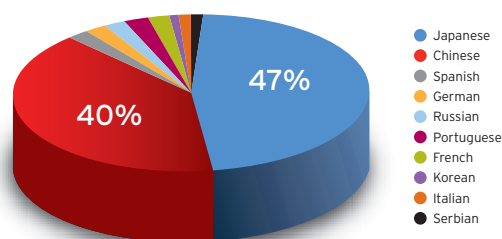


Figure 2: Non-English Spam by language from December 2006 to May 2007

### Trend: A Spike in German Spam

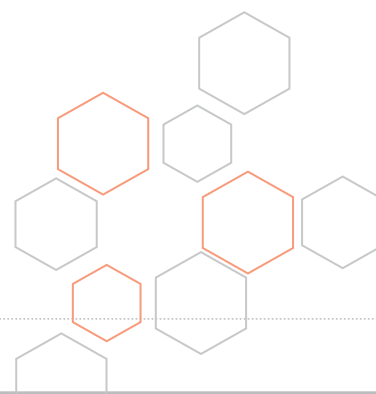
The volume of German spam increased three-fold in the second quarter compared to the first quarter. This surge is due to the thousands of German users who exposed their systems to downloaders (TROJ\_AGENT.IQN) in March by clicking on links or opening .PDF attachments in messages purporting to be invoices or billing statements.

### Trend: Timely Subject Headings Trump Generic Messages

Subject headings of spam this period were extremely timely and relevant (Table 6).



ANTI-SPAM



Real-world Event	Malware Exploiting Event	Date First Seen
Saddam execution	TROJ_BANLOAD.BLK	7-Jan-07
Vista's worldwide release	WORM_SOHANAD.U	1-Feb-07
Release of IE7	PE_GRUM.B-O	31-Mar-07
Virginia Tech Massacre	TROJ_BANLOAD.CFU	19-Apr-07

Table 6: Events and corresponding malware

WORM\_NUWAR variants were quite adept at exploiting real world events, and human interest in doomsday pronouncements of war.

**Trend: Attachment Enhancements**

Malware authors have also been trying to confuse signature-based antivirus engines by using different archiving applications like .RAR and .ZIP (WORM\_NUWAR.RAR and WORM\_NUWAR.ZIP, respectively), which require passwords before they are launched.

**Trend: Decrease in Image Spam Volume Share**

In December 2006, image spam constituted 32% of the total spam volume collected. By the first quarter of 2007, the percentage fell to 12.83% in time with the general decline in holiday zeal. And from the available data for the second quarter, the number had fallen further to 11%. The decline is attributable to the positive effects of the increased awareness and efforts (albeit in reaction to image spam already circulating in the latter part of last year) of security companies in developing smarter OCR technologies.

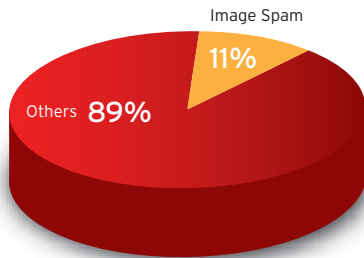


Figure 3. Percentage of Image Spam over Total Spam from April to May 2007

**PHISHING**

Phishing remained prevalent from December to May, with phishers using the same techniques, the most widely-used being the explicit display of the phishing URL, which still manages to lure users into divulging account information. The percentage of reported phishing links which are already found dead at subsequent visits suggest there is a relative ease by which phishers are able to register and evacuate from online domains.

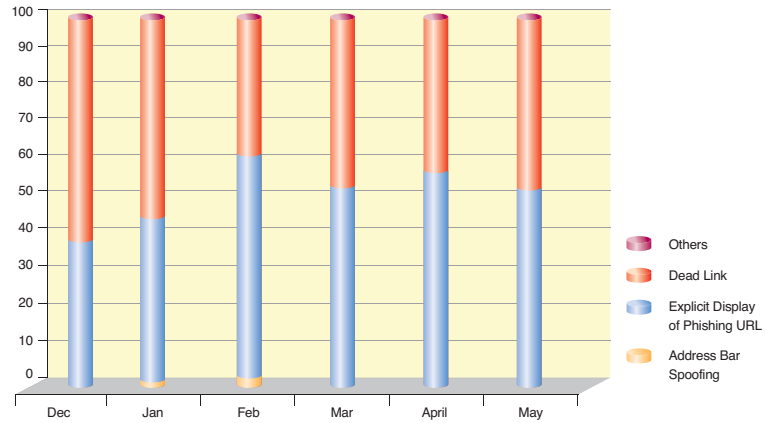


Figure 4: Phishing techniques used by month

The top ten companies whose Web sites were spoofed by phishers during the past six months are:

TOP 10 COMPANIES ATTACKED	
1	eBay
2	Paypal
3	Bank of America
4	Wachovia
5	Fifth Third Bank
6	BB&T
7	Poste Italiane
8	Sparkasse
9	Regions Bank
10	VolksBank

This list sheds light on a new phishing trend: much like malware attacks, phishing attempts are now targeted at smaller, regional banks. Excluding eBay and Paypal, the top half are American banks and the other half are European banks.



## → Process-Based Threats

The latest infection counts show that the growth in the number of infections from heuristically-detected malware have nearly doubled from December 2006 through May 2007. This means that compared to six months ago, users were twice as prone to have been infected with malware.

GENERIC DETECTIONS	2007 Infections	% Growth
TROJ_Generic	940,583	94%
BKDR_Generic	68,001	79%
PE_Generic	50,987	75%
PAK_Generic.001	54,861	86%
WORM_Generic	38,077	79%

Table 7: Infections counts for the first half of 2007 and their growth vs. the latter half of 2006

For specific detections by Trend Micro—malware whose behaviors have been studied and for which a specific antidote has been written—the top twenty threats are as follows:

Top 20 Malware Dec 2006 - May 2007	
1	WORM_NYXEM.E
2	HTML_NETSKY.P
3	WORM_ANIG.A
4	WORM_NETSKY.DAM
5	EXPL_ANICMOO.GEN
6	PE_PARITE.A
7	WORM_RONTKBR.GEN
8	WORM_NETSKY.P
9	ADW_CNSMIN.G
10	WORM_MOFEL.B
11	TROJ_HORST.HF
12	WORM_RONTOKBRO.B
13	ADW_FUNWEB.Q
14	ADW_TCENT.C
15	JAVA_BYTEVER.A
16	WORM_MYDOOM.GEN
17	WORM_NETSKY.D
18	ADW_TCENT.AC
19	PE_SALITY.AS
20	WORM_RJUMP.A

Nine worms made it into the top twenty, reflecting the attractiveness of speedy propagation to malware authors. Worms have been known to be involved with the establishment of botnets.

The proliferation of exploits to subvert the .ANI vulnerability is evident with the entry of EXPL\_ANICMOO.GEN into the top twenty, a mere three months since its discovery. The majority of malware on this list have been around for three to four years before obtaining a similar level of spread.

HTML\_NETSKY.P remains a threat two years after its first discovery, as it is still able to find

unpatched computers with the known vulnerability related to the automatic execution of attachments in email messages. This vulnerability affects Internet Explorer 5.0 and 5.01, suggesting that many users have older PCs or refrain from upgrading to newer versions of the popular browser.

PE\_PARITE.A, the detection for files infected by PE\_PARITE.A-O, was first discovered in 2003, yet it ranks

as the sixth most popular malware. This file infector infects .EXE and .SCR files and spreads via network shares, making computers under corporate LAN set-ups especially prone to infection. Although this file infector does not have a destructive payload, it may cause severe bottlenecks in network and system resources.

### Trend: File Infectors with New Roles

The past few months have seen an increase in file infector families which employ complex infection routines and serve as propagation vectors for other threats. PE\_LOOKED variants downloaded several malware onto the affected system. PE\_FUJACKS is known for its three-pronged propagation routine (including propagation via instant messaging) and involvement in the download of a keylogger. PE\_DARKSNOW possesses an intricate infection scheme as it infects system files and steals system information. Finally, PE\_VIRUT arrived as a spammed email attachment, and had backdoor capabilities.

### Trend: Online Gaming Information Theft

Trojan spyware are still targeting the same type of user information, as illustrated in Fig. 5. Online gaming information accounts for 37%, due mostly to the massive popularity of online gaming in Asia. Spyware stealing bank- or account-related information accounts for 17% while 5% exclusively sought out instant messaging account information, primarily from the Asian IM application QQ Messenger.

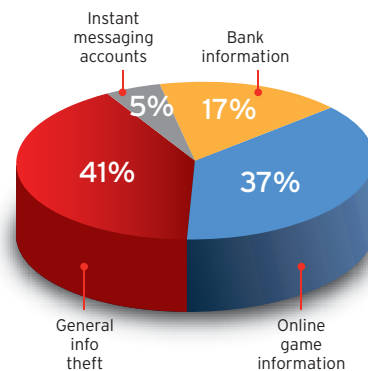


Figure 5: Trojan Spyware Detections for 2007

### Trend: Rise in Rogue Anti-Spyware Infections

Capitalizing on people's inherent paranoia about getting infected are several rogue anti-spyware vendors that first convince users that they have been infected then sell them a product they really do not need. The software purchased online is virtually useless, and the fraudulent company may consequently steal a customer's credit card accounts. Examples of the phony software packages include Winfixer, SpywareQuake, ErrorSafte, ErrorGuard, SpyShield, SpyAxe, SpywareNuker, and most recently, Spyhealer, DriverCleaner, and SystemDoctor.

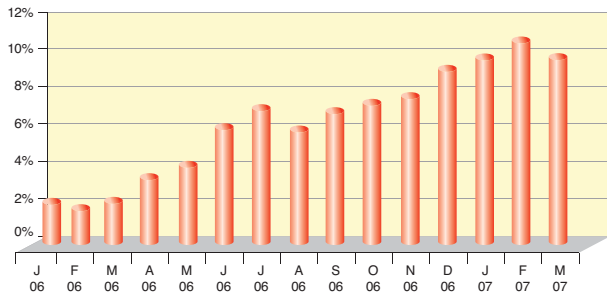


Figure 6: Percent of PCs worldwide infected with rogue anti-spyware

### Further Regional Analysis:

	Africa		Asia		Australia		Europe		North America		South America	
	2006	2007	2006	2007	2006	2007	2006	2007	2006	2007	2006	2007
<b>GRAYWARE</b>												
<b>ADWARE</b>	12%	18%	7%	16%	9%	7%	14%	14%	18%	15%	14%	6%
<b>CRCK</b>	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%
<b>DIAL</b>	0%	2%	0%	0%	0%	0%	4%	2%	2%	0%	2%	1%
<b>EXPL/HKTL</b>	2%	1%	2%	4%	0%	1%	3%	6%	3%	2%	3%	8%
<b>SPYWARE</b>	7%	3%	14%	5%	5%	2%	6%	3%	14%	4%	15%	14%
<b>MALWARE</b>												
<b>BACKDOOR</b>	2%	1%	6%	1%	0%	1%	1%	1%	1%	2%	1%	1%
<b>DOS</b>	0%	0%	0%	0%	0%	0%	2%	0%	0%	0%	0%	0%
<b>HTML</b>	11%	8%	3%	5%	8%	4%	5%	6%	5%	4%	0%	0%
<b>IRC</b>	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
<b>JAVA</b>	2%	0%	2%	0%	8%	3%	8%	7%	7%	5%	6%	2%
<b>JS</b>	0%	1%	0%	0%	1%	1%	3%	1%	0%	1%	0%	0%
<b>PE</b>	7%	7%	10%	11%	1%	51%	3%	0%	6%	6%	18%	7%
<b>TROJ</b>	13%	12%	13%	38%	12%	11%	8%	24%	9%	20%	8%	24%
<b>VBS</b>	0%	0%	1%	0%	0%	0%	0%	0%	0%	1%	0%	0%
<b>WORM</b>	43%	48%	41%	19%	55%	21%	41%	35%	36%	39%	33%	33%
<b>TOTAL</b>	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Table 8: Infection counts by region

Analysis of worldwide infection counts reveals that some security issues are specific to certain regions. By comparing the percentage distribution of infections per malware type from the early part of 2006 to the six months under discussion, trends appear on a localized scope, among them are the following:

- Grayware installations were more pronounced in Asia and Africa in the current period. However, it is in Asia where the increase is nearly 50%, signaling a need for renewed vigilance when it comes to accepting and installing free software offerings from the Internet.
- The 2% spike for EXPL and HKTL threat types in Asia is attributable to the high-impact .ANI vulnerability.
- PE\_PARITE caused a very significant spike in infections in Australia; almost all infections for this period can be traced to either carrying or being infected by PE\_PARITE.A. While this malware is quite old, it is probable that its introduction into a corporate workplace would place all connected computers at risk.
- Users in Europe, North America, and South America experienced an increase in Trojan infections for the current period, with Trojans detected by Trend Micro using heuristic technologies accounting for the largest share. Although typically deemed low threats, the propensity of users to click on suspicious links and attachments despite what prudence dictates is what may lead to increased risk should other destructive Trojans arrive in the same manner.

## ➔ Distributed Threats

Although intelligence gathering processes are underway, the depth and extent of botnet infiltration—how many exist and which computers have been compromised—are still hard to pinpoint. Malware infection may provide clues, inconclusively though, that a said computer may have been involved in a botnet. What is dangerous is that the user is often never made aware that such a compromise exists.

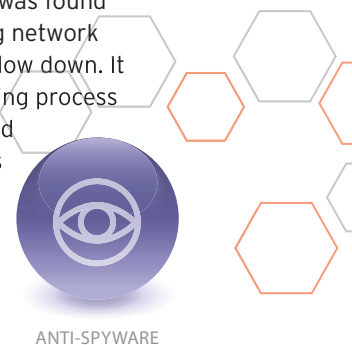
The reason for the proliferation of these attacks is that there are many talented programmers in the world who are faced with slow job markets or are lured by lucrative paychecks. Many of these programmers reside in Latin America, Eastern Europe, and Asia, all of which have a history of organized crime.

Malware activities give clues to the existence and persistence of botnets. Late last year, a malicious Hypertext Preprocessor (PHP) script was detected as being hosted on Web servers, where unsuspecting users may accidentally run it. Upon execution, it opens random ports on the affected system, and may then submit to the commands of a remote user.

In March, Rinbot launched an attack against U.S. media outlets by exploiting newly-published vulnerabilities, causing it to spread across connected systems running on Windows.

Also, as the past few months have demonstrated, there is a distinct effort by botnet masters, particularly those that send out spam (NUWAR and STRAT) to increase their batting average in infection rates by closely monitoring real-world events and crafting timely email messages to increase the likelihood that each spammed message ends up in a hit. As discussed in content-based threats, the changing subject headings are proving to be effective. Unbeknownst to users, launching a worm into the system allows a remote malicious user a foot in the door, as it surreptitiously installs other files, steals information and takes advantage of its computer resources to participate in spamming activities or even Distributed Denial of Service (DDoS) attacks.

And just very recently, WORM\_SOBER.AX was found to corrupt a legitimate system file, causing network connection for the affected computer to slow down. It also performs a variety of routines, including process termination, lowering security settings, and disabling Windows auto-update. What puts suspicion that this is involved in a bigger scheme is its mass-mailing routine and the steps it takes to avoid encountering the authorities by filtering email addresses like .gov and .edu. Its vast capabilities put users in critical danger.

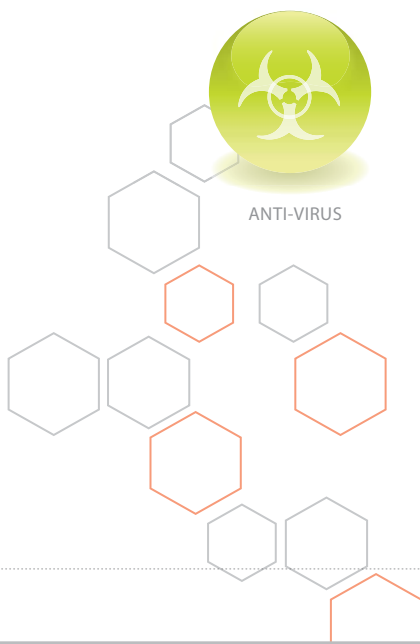


## ➔ 2H 2007 Forecast

Attacks similar to those seen during the past six months are expected to continue in the ensuing months, taking advantage of back-to-school and the holidays as online commerce peaks in December. Malware authors will try to evade signature-based detections, saturating other means apart from compression tools to avoid exposure by security vendors. Trend Micro expects to see the number of Web threats expand due to a variety of reasons. First, the availability of exploit kits and accessibility of bots and botnets makes it extremely easy to implement Web threats. Second, as increasing numbers of Web 2.0 websites emerge, creating interactive Web applications, malware authors will be on the look-out for technical flaws which they may then use to execute their own codes.

Phishing attempts will likely increase as a result of the introduction of phishing kits into the underground markets and the ease of obtaining an online presence (due to cheaper domain registration rates). Attempts need only look more convincing to lure more victims, in the same way image spam may pick up in terms of sophistication, as retaliation against security companies' efforts to weed them out of email traffic.

Botnets remain a threat, and will require a deep, integrated view before authorities begin an attempt at taking them down. Meanwhile, malicious codes will continue to use each and every avenue available to malware authors online, to net the most number of victims. Web threats will continue to permeate the online computing experience for users all over the world, as long as the deployment of malicious code remains a profitable enterprise for malware authors.



## ➔ Best Practices

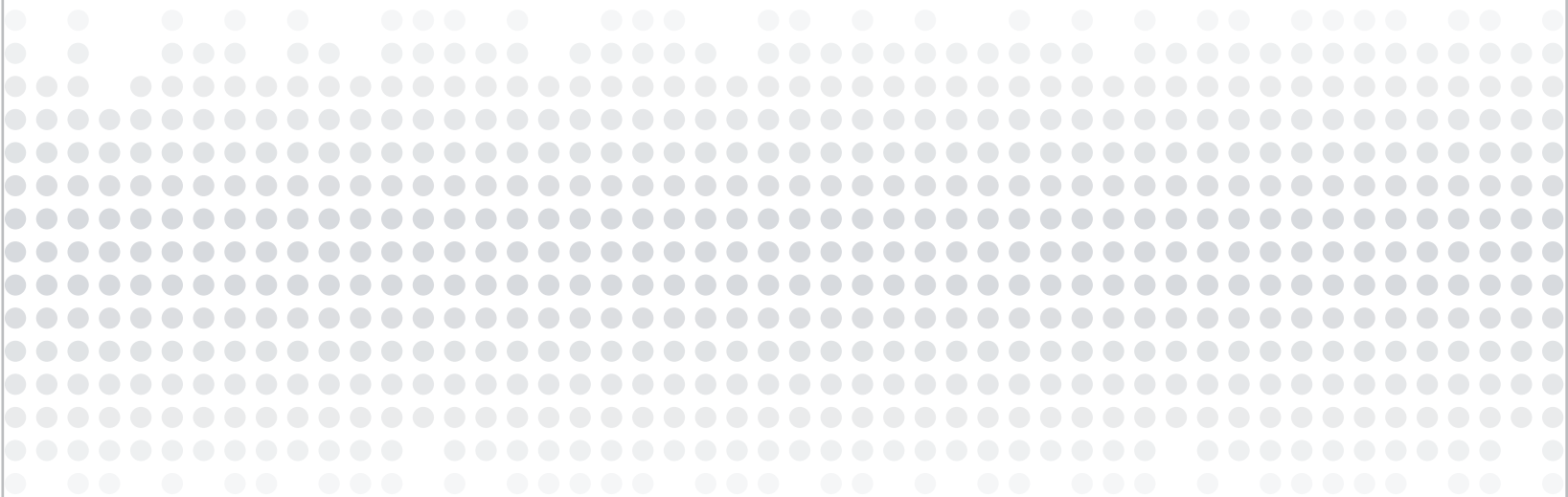
**For enterprises, mid-size corporations and small businesses, Trend Micro recommends a multi-layered approach to protection, including the following:**

- ➔ **Deploy HTTP-scanning methods.** Implement Web-scanning systems in mid- to large-size networks, and make sure users cannot bypass them.
- ➔ **Do not allow unnecessary protocols to enter the corporate network.** The most dangerous of these are P2P communication protocols and IRC (chat), often used by bots to communicate with the botnet.
- ➔ **Deploy vulnerability scanning software in the network.** Make sure all operating systems and other software applications are up-to-date and patched with the most recent security patches.
- ➔ **Restrict user privileges for all network users.** Kernel-level rootkits are implemented as device drivers; therefore, denying users the right to "load and unload device drivers" will largely block them.
- ➔ **Deploy corporate anti-spyware scanning.**
- ➔ **Support user awareness campaigns.** Teach users basic security measures and how to react to typical attack scenarios. Educate them about the types of threats they may encounter and best practices for laptop computing.

**For home users, Trend Micro recommends the following:**

- ➔ **Beware of pages that require software installation.** Do not allow new software installation from your browser unless you absolutely trust both the Web page and the provider of the software.
- ➔ **Scan all programs and files downloaded from email or via the Internet.** Keep all antivirus and anti-spyware software applications up-to-date.
- ➔ **Beware of unexpected or strange-looking emails, regardless of their sender.** Never open attachments or click on links contained in these email messages. Enable the "Automatic Update" feature in your Windows operating system and apply new updates as soon as they are available.
- ➔ **Always run a real-time antivirus scan service.**





**Trend Micro Inc.**  
10101 N. De Anza Blvd.  
Cupertino, CA, 95014, USA

- Toll free: 1+800-228-5651
- Phone: 1+408-257-1500
- Fax: 1+408-257-2003

©2007 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, InterScan, NeatSuite, OfficeScan, Trend Micro Internet Security, VirusWall, WebProtect, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.