



Jaime Lyndon "Jamz" A. Yaneza,
Senior Threat Analyst

David Sancho
Anti-Malware Specialist



the trend of threats today:
2005 Annual Roundup and 2006 Forecast

2005 annual roundup & 2006 forecast

The antivirus and security industry has witnessed quite a few changes in the past year – and, most notably, over the final few months leading to 2006.

In light of recent developments, trends are changing and new threats have emerged. The Internet has truly come of age as the ultimate tool for marketing, communication and global commerce. Unfortunately, more and more malicious parties also try to abuse the system for their own gains. From ruthless advertisers selling their dubious bodily enhancement pills to crime organisations stealing bank account numbers – life in cyberspace is far from safe. This reality has prompted some to predict that this far-reaching and borderless community would become the “last wild-wild west”.

Blended Threats:

A complex program that targets multiple weaknesses in computer networks and uses multiple distribution methods to spread.

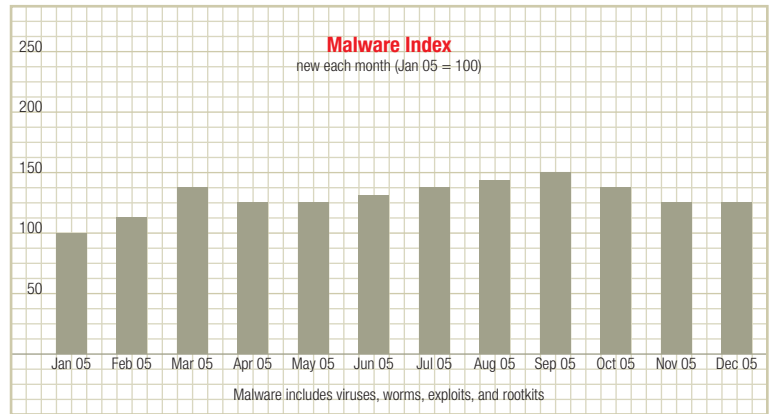


Twelve months ago Trend Micro forecasted that blended threats would continue to hound users. This prediction proved correct with such threats as WORM_BAGLE.BE, a Trojan-spam tandem that caused an outbreak in March 2005; the rise of the AGOBOT family in January; and the MYTOB family, which gained notoriety in 2005 with nearly 300 variants since it was first discovered in February, and still accounted for the largest number of variants among all malware for the month of December. Predictions that writers would employ non-standard file types was also realized by the end of the year, with the appearance of the Windows Meta File (WMF) exploit. While threats related to IRC and P2P communications accounted for 16% of the total threat propagation vectors, spam and phishing continued to be one of the major problems that both consumer and corporate users faced in 2005. Additionally, the dramatic increase of non-English spam in 2005 lent credence to the theory that spammers would continue their attempts to expand their reach to additional markets.

There is an inherent danger that comes with the extraordinary advantages of utilising the Internet today. Password stealers and bot worms have replaced file infectors and script viruses. Spyware and adware programs are hiding behind dubious Web pages. A threat's source, specific targets, and side effects define a new era, that of “multi-purpose threats.”

The report that follows is not only an account and analysis of 2005 threat incidents. It also serves as a forecast of what the future holds in 2006 and onwards. Through Trend Micro's extensive research and analysis of the 2005 incidents, this paper documents how threats evolved into the multi-purpose threat regime – thus providing corporate and home users information on what to do to ensure they remain protected against future threats.

Threat indicator Summary

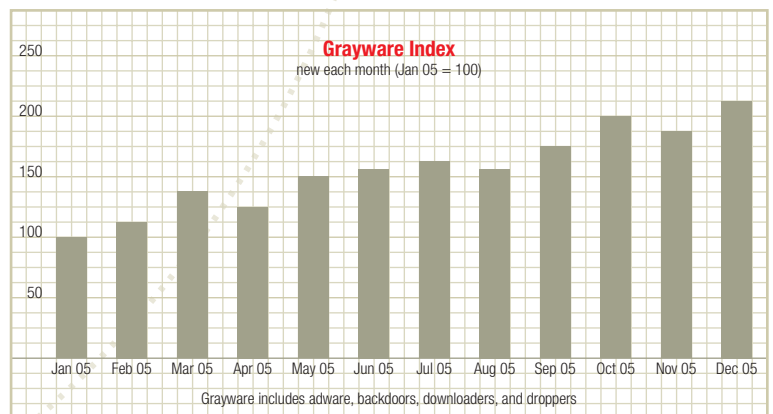


Less new rootkits?

In 2005 the number of new malware variants increased more modestly than recent years. The number of new viruses remained fairly steady throughout the year, while new worms and trojans accounted for most of the modest growth. New rootkits, while small in number showed a dramatic increase in the autumn of 2005. In the last month, however, the introduction of new rootkits appears to have slowed. This may be partly due to reaction to the Sony rootkit furor.



Threat indicator Summary



Same adware but sneakier installs

2005 has witnessed a dramatic shift in the grayware from new variants of adware to sneakier new ways to get grayware installed on victim PCs. Overall, the appearance of new forms of adware has remained steady while the introduction of new backdoors, downloaders, droppers, and other trojan spyware has more than double during 2005.

2005: the grayware year?

2005 could be referred to as the “Year of Grayware”, with 65% of the top 15 threats noted in the chart opposite – responsible for nearly 11 million unique reports – having included some sort of spyware, adware, backdoor, rootkit, or bot functionality.

2005 could be referred to as the “Year of Grayware”, with 65% of the top 15 threats noted in the chart below – responsible for nearly 11 million unique reports – having included some sort of spyware, adware, backdoor, rootkit, or bot functionality.

Some other statistics to note, regarding the total threat landscape of 2005:

- 10% were BOTs
- 11% were Spyware trojans
- 18% were Adware
- 0.60% were Rootkits
- 0.60% were Office macros
- 3% were Scripts
- 25% were viruses or worms
- 27% were Trojan horses (including rootkits)

Shown above are the Top 15 threats of 2005 taken at face value. WORM_NETSKY.P has been on the charts for almost two years since the first variant was discovered in March of 2004 and has remained the top threat affecting computers ever since – with the exception of September 2005, where variants of TROJ_AGENT and TROJ_DLOADER took both of the top spots. The latter two are basic downloader trojans and have been linked to adware and spyware attacks. Their prevalence is noted among the

top grayware threats, with a combined number of installations nearly equal to the number of NETSKY infections.

PE_PARITE.A was first discovered in January 2001 and has proven to be surprisingly tenacious, despite many contemporary antivirus solutions. It injects its code as part of the Windows Explorer.exe file, thereby making itself part of every normal operation. This is a prime example of a pseudo-user-mode rootkit. By affecting how Explorer.exe works PARITE is able to gain pre-control over processes and quickly infect other executables (*.EXE) as well as screen-savers (*.SCR).

First detected in November of 1999, PE_FUNLOVE.4099 is the oldest file-infector to appear in the chart above. This threat also acted as a network worm and thus had the capability to more easily propagate, since network shares have historically proven to be the most effective threat vector. This infector also dropped viral code and patched the files NTLdr and NTOSKrn.exe, thereby enabling it to bypass the file-integrity checking by Windows for the NT Boot Loader Kernel, as well as the integrity checking of infected Windows files. Thus, via a pseudo-kernel-mode rookit function, this malware was able to defeat the security implementation available to protect Windows users from viruses at the time, and continue to be active for more than 5 years. Due to its complex infection routine, FUNLOVE has been



65% of the top 15 thre

used as a payload by both WORM_BRAID and WORM_WINEVAR, and in a recent discovery of double-infections by riding piggy-back on the WORM_BAGLE.H variant which resulted in a new family called WORM_FUNBAG, initially found in March of 2004.

PE_ZAFI.B, first seen in June of 2004, may not have been the first file-infector and worm, nor was it the first bi-lingual virus delivering both English and German mass-mailed messages. However, its combination of dropping infected copies in P2P shares and preventing users from checking their tasklist or Windows registry has enabled it to propagate enough to become one of 2005's most widespread infections.

VBS_REDLOF.A is a special case that underlines the danger of using HTML-formatted email or browsing non-work related websites. It exploits an old MS Virtual Machine ActiveX vulnerability and has a patch dating back to October 2000, so it seems surprising that this threat (released in August of 2004) still manages to show up on our radar. Its most dangerous payload is that it infects all web extensions (*.html, *.htm, *.asp, *.php, *.jsp, and *.vbs), as well as the default Outlook Stationary, thereby causing all outgoing messages to be infected – and spreading virally to recipients.

Top 15 Infections for 2005*

Name	Count	Type
WORM_NETSKY.P	1,602,069	Worm
JAVA_BYTEEVER.A	667,448	Java applet
PE_PARITE.A	320,924	File infector
TSPY_SMALL.SN	268,171	Grayware
WORM_NETSKY.D	242,243	Worm
SPYW_GATOR.B	163,495	Grayware
PE_FUNLOVE.4099	147,416	File infector
VBS_REDLOF.A	145,701	VBScript
HKTL_RADMIN.A	63,557	Grayware
PE_ZAFI.B	62,708	File infector
ADW_SOLU180.A	61,929	Grayware
PE_TENGA.A	44,036	File infector
PE_JEEFO.A	27,831	File infector
PE_LOVGATE.AC	25,598	File infector
PE_NIMDA.A	16,824	Worm

ats responsible for nearly 11 million unique reports

2005 global alerts

Outbreaks of 2005*

Name	Date declared	Quarterly	Count
WORM_BEAGLE.AZ	Wednesday, January 26, 2005	Q1 (6)	1
WORM_BROPIA.F	Wednesday, February 2, 2005	Q1 (6)	2
WORM_MYDOOM.BB	Wednesday, February 16 2005	Q1 (6)	3
WORM.BEAGLE.BE	Tuesday, March 01, 2005	Q1 (6)	4
WORM.FATSO.A	Monday, March 07, 2005	Q1 (6)	5
WORM.KELVIR.B	Monday, March 07, 2005	Q1 (6)	6
WORM_SOBER.S	Monday, May 02, 2005	Q2 (7)	7
WORM_MYTOB.ED	Sunday, May 08, 2005	Q2 (7)	8
WORM.MYTOB.EG	Monday, May 09, 2005	Q2 (7)	9
WORM.WURMARK.J	Wednesday, May 11, 2005	Q2 (7)	10
WORM.MYTOB.AR	Sunday, May 29, 2005	Q2 (7)	11
WORM.MYTOB.BI	Tuesday, May 31, 2005	Q2 (7)	12
WORM_BOBAX.P	Friday, June 03, 2005	Q2 (7)	13
WORM_ZOTOB.D	Tuesday, August 16, 2005	Q3 (2)	14
WORM_RBOT.CBQ	Tuesday, August 16, 2005	Q3 (2)	15
WORM_SOBER.AC	Wednesday, October 05, 2005	Q4 (3)	16
WORM_SOBER.AG	Monday, November 21, 2005	Q4 (3)	17
WORM_MYTOB.MX	Thursday, November 24, 2005	Q4 (3)	18

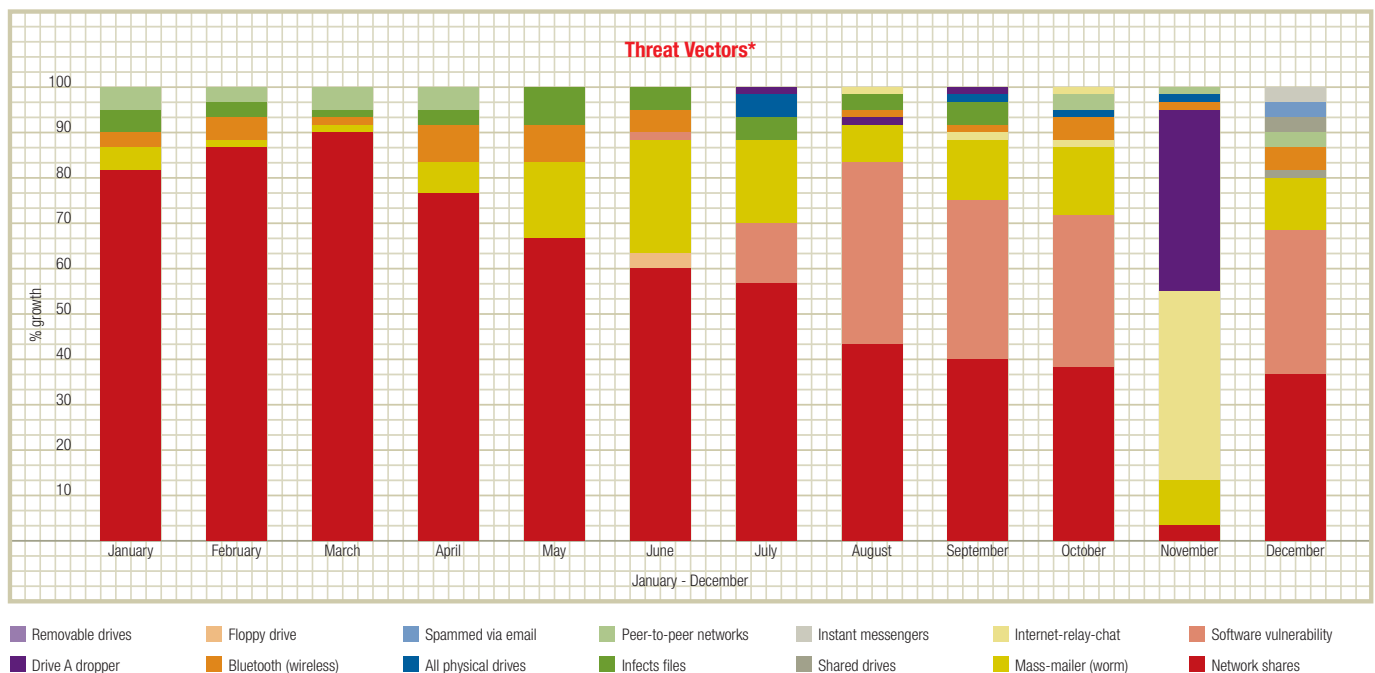


For all the alerts declared during 2005, 26% were due to variants of WORM_MYTOB, a combined threat resulting from grafting parts of WORM_MYDOOM, which caused widespread infections in 2004, with BOT components. Its success stems from a host of previously known effective infiltration techniques such as trumping users seeking help by modifying the HOSTS file, as well as fake mail delivery failure messages leading on users to closely examine errors in transmission.

WORM_SOBER variants comprised 16% of outbreaks in 2005, due to its bi-lingual approach in its spammed messages. Similar to WORM_MYTOB, this threat included retaliation techniques against major antivirus products by attempting to disable them from memory and thus safely drop its malicious components undetected. The use of major world events like the "FIFA World Cup" match in Germany, a technique borrowed from spammers, also lent to this threat's successful propagation.

Through the use of unsecured network shared folders and the wide use of P2P applications, WORM_BAGLE variants accounted for 11% of world wide threats to enterprises. Similar to the top outbreak families of 2005, WORM_BAGLE also used retaliation techniques as well as faked mail delivery errors to bait users.

2005 network intrusion techniques



The chart above provides an overview of the most prevalent propagation techniques employed by malware in 2005, based on more than nine-thousand (9,000) new pieces of noteworthy malware collected by Trend Micro throughout the year. According to our analysis, recursively searching and dropping malware onto network shared drives remained the most successful method, accounting for approximately 37% of all cases. It is quite alarming, though not unexpected, that vulnerability exploits were the second most successful method, employed in 19% of instances. Use of mass-mailing code, Internet relay chat (IRC), and default shares each comprised approximately 10% of the remaining vectors abused. Instant messenger (IM) used as a propagation vector was only utilized 4% of the time, and all other methods such as typical file infection and peer-to-peer network shares each only comprised approximately 2% of the attack vectors.

IM Utilized For Worm Attacks

For the past three years, Trend Micro researchers have been warning users about the sporadic yet increasing use of alternative infection vectors. During the first quarter of 2005, we witnessed another wave of attacks from worms KELVIR, FATSO and BROPIA, each which effectively spread to all MSN Messenger contacts of infected computers. Through the use of sender spoofing techniques and the yet immature age of IM-usage, unsuspecting IM users were surprised to learn that their trusted contacts were sending viruses. This turn of events forced Microsoft to release updated versions of the program with enhanced file-transfer filters to prevent further outbreaks on client machines.

Trend Micro tracked 56 unique malware variants that utilise [URL links or downloaders] in 2005, and we expect this technique to gain in popularity.

Shown below is the growth in instant messaging as an infection vector based on the number of new malware using this technique*. There was more than a hundred-fold increase by December, with only four variants seen in January.

*Where index is based on 100% in December denoting the highest value.

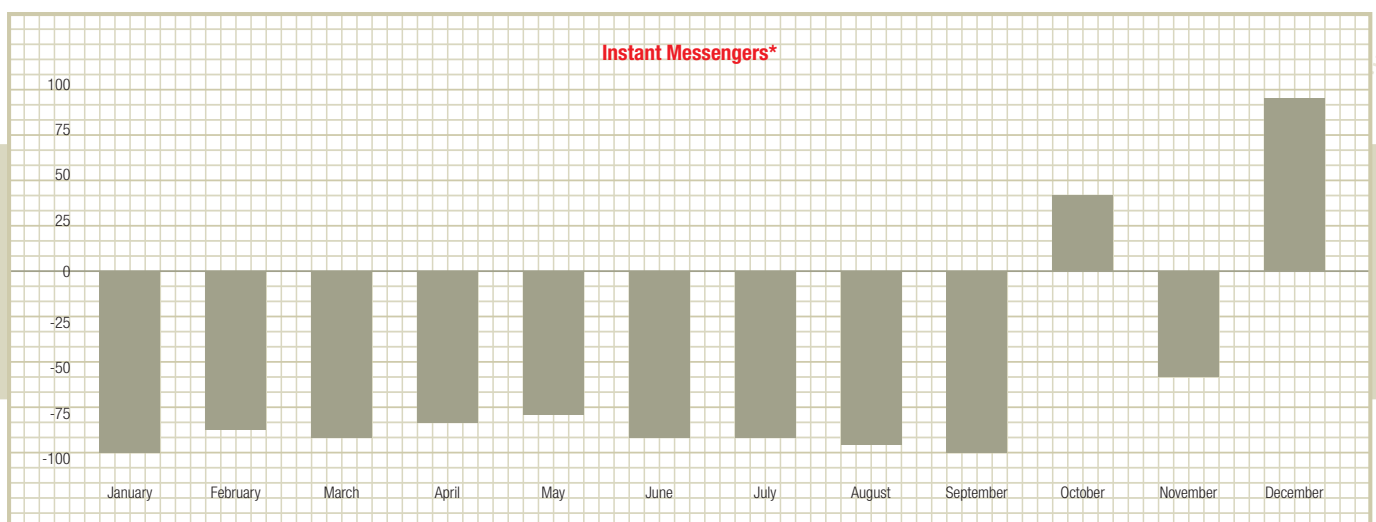
Trojan Tandems

For the past few years, security vendors have recommended blocking and filtering specific extensions – coupled with validating attachments to avoid false positives – as the most effective means of preventing mass-mailed threats. Malware authors responded to this by employing a complex technique of including URL links or simple downloaders in an attempt to foil such a security function. The technique hinges on not having to rely on email as the direct propagator of the threat, but instead using a downloader to drop malicious files onto desktops directly, via the web. This technique also carries the added benefit of enabling the malicious writer to continuously update the malware, without the burden of re-seeding the attack. Trend

Micro tracked 56 unique malware variants that utilised this technique in 2005, and we expect this technique to gain in popularity in 2006 – and the foreseeable future.

Though WORM_BAGLE.AC was the first one to use this technique, BAGLE.BE was the first of its type to provoke a Yellow Alert. These variants used a worm to spam a Trojan whose only function was to download and execute the worm component from a list of predetermined Web sites. Once the worm was run it collected target addresses from the Windows Address Book (*.WAB) and began spamming the Trojan, thus repeating the cycle. This two-component strategy enabled this variant to elude detection long enough to become more widespread and to cause a subsequent outbreak. This worm-trojan tandem technique proved effective again in May with WORM_WURMARK.J and again in June with WORM_BOBAX.P. Since then it has been used by most BAGLE variants.

By September, WORM_BAGLE.DA attempted another complexity by using two downloaders instead of one. This malware spammed a Trojan, which



further downloaded another Trojan from certain sites. The secondary Trojan then finally downloaded the actual worm binary, to start the cycle over again. Such a daisy-chain technique attempted to lengthen the detection process, thereby increasing the lifetime of the attack. Regardless, researchers weren't fooled and already had various solutions in place, including heuristic detection for the spammed downloader Trojans.

To mitigate any future attacks of this type, users should ensure that their security solution integrates solid anti-spam and anti-phishing capabilities with their traditional antivirus defenses. The combination of these three functionalities provides for the qualification of all downloaded files, thus neutralising this technique.

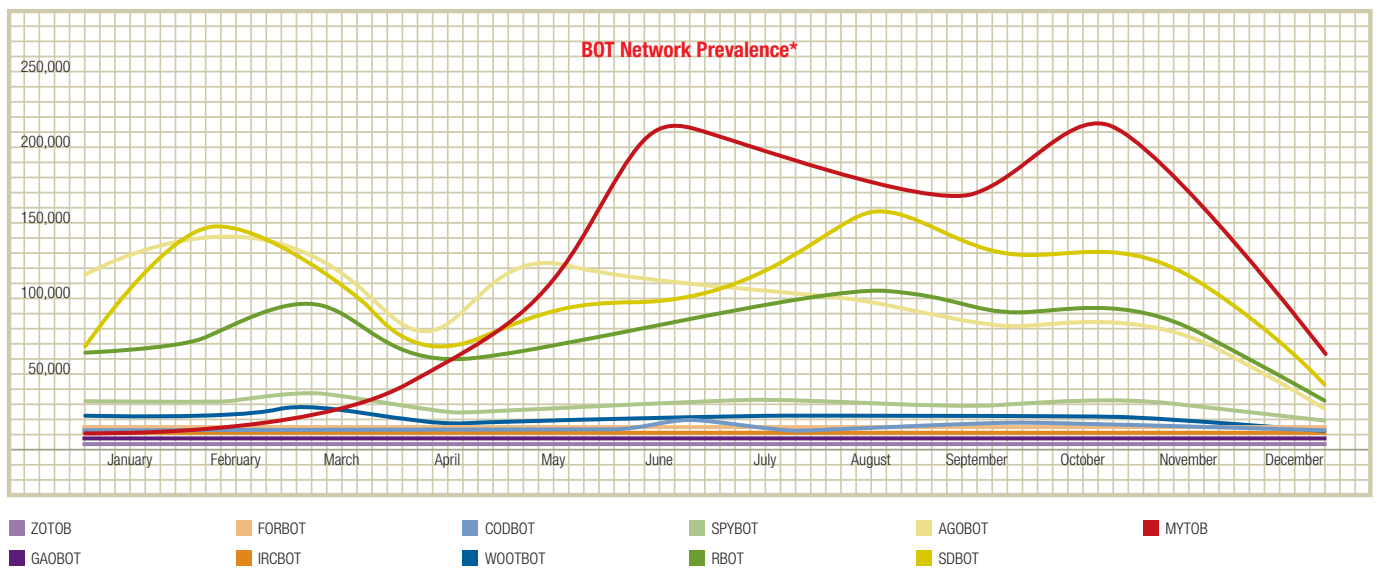
Small is the New Big

Binary packers have been developed to compress executable files, thus making them easier to distribute. Though this process was originally intended for legitimate installation files, the packing process modifies the internal structure of a file, which malware authors can use to their benefit.

This is an old trick that became commonplace last year during the worm-wars, although a total of seven alerts since 2002 also employed the technique.

Worm authors used this tactic to distribute an ever-changing worm file masked by dozens of different packers. In the cat-and-mouse game between malicious authors and security vendors, such complexity delayed detection long enough to enable four WORM_MYTOB variants to reach Yellow Alert status in May. Another notable example includes SOBER variants discovered in the last quarter of the year. Trend Micro detected as many as 64 differently packed samples of a single variant, SOBER.AC, which led to an outbreak in October. In November, SOBER.AG utilised the technique with a similar level of success.

In addition to making the attack larger and more intense, such a technique further expands the author's BOT-network, thus enabling future attacks to be more widespread.



Tangled in BOT-nets

The charts above detail some of the major BOT families in 2005. BOTs are a special type of hybrid threat that incorporates many of the techniques used by contemporary malware, with the intent of parasitic and long-term retention in victimized user systems. BOTs attempt to enter the system through such methods as exploited vulnerabilities, spammed email, or network shares. Most of them are functionally geared toward information theft and extend to remote administrative control – typically accomplished through an internet-relay-chat (IRC) session. The main concern of having a single BOT or several different ones in a user's system is that with administrative control, often called "root" control, a malicious entity can bundle affected systems together to affect and compromise other systems via a denial-of-service attack. In addition to making the attack larger and more intense, such a technique further expands the author's BOT-network, thus enabling future attacks to be more widespread.

There were over a thousand AGOBOT variants in the beginning of 2005, accounting for 43% of all BOT infections. But with the explosive growth of BOTs throughout the year, this family's share was diminished to just 11% by December. Aside from its regular antics, AGOBOT also attempted to remove variants of WORM_NETSKY and WORM_BAGLE to avoid conflicting control over affected systems. Its list of security applications to terminate and avoid detection covered almost 600 different programs. Its authors competed with other BOT-clones by improving on its parasitic capability.

Similarly, RBOT accounted for 21% of infections in January and likewise dropped to a mere 11% by the end of the year – though it had grown to 1,500 variants. The aim of RBOT was to steal registration keys for many of the top PC games of 2002 ~ 2004. It borrowed extensively from the AGOBOT framework but was geared more towards theft and had very basic modifications from the original source.

Another competing BOT-clone is SDBOT with a constant 25% prevalence throughout the year, with over 2,000 variants. Its authors appeared to have more understanding of the Windows internal registry and modified it in such a way as to allow faster propagation of the BOT across networks.

Surprisingly, the most prevalent BOTS of 2005 are from the MYTOB family, though there are only 300 variants of this family. The first variant of MYTOB was discovered in February, combining WORM_MYDOOM's functionality with a full-fledged BOT application. MYTOB's effective growth from a mere 2% in March to a disturbing 50% in December needs examining. The continuous modifications to its code – including the use of encryption, numerous file-compression algorithms, and introducing URL links in carefully crafted spammed email to download its executable – enabled newer variants to avoid being filtered at the gateway. A comparable technique was used by variants of BAGLE and SOBER in the latter part of the year. Such a download technique was useful in quickly dropping various other malicious programs onto a victim's system as well as pushing updated versions. It also utilized a lengthy list of email addresses to prevent being detected by honeypots.

With the discovery of ZOTOB in the wild in August, it became clear that bot worm authors possessed both the technology and the intention to add vulnerability exploits in their creations as soon as those vulnerabilities are published. This bot exploited the operating system vulnerability only five days after the Microsoft security advisory was issued, breaking the previous record of two weeks. Two different variants of ZOTOB infected computers in August which caused Trend Micro to declare a Yellow Alert to contain the outbreak. It exploited the MS05-39 Plug-and-Play vulnerability inherent in most current Windows-based installations – including the latest Windows 2003 installation with SP-1.

With the discovery of ZOTOB in the wild in August, it became clear that bot worm authors have both the technology and the intention to add vulnerability exploits in their creations as soon as those vulnerabilities are published.

Lost in Translation

As new users join the Internet, malware authors develop new strategies to gain their trust, in an attempt to deceive them into executing email-attached malware. SOBER variants were especially successful this past year by using different languages (much as ZAFI did in December 2004). SOBER sent German text emails to recipients with German email address, and English to all others. Moreover, the worm itself had the ability to check the infected user's system for the version of the Microsoft OS that was running. If it detected GMX as the domain, it installed one of the German versions; otherwise, it installed one of the English versions. Both the AC and AG variants became widespread in Germany during the last quarter of the year, triggering Yellow Alerts in both cases.

New Social Engineering Techniques

In May SOBER.S utilised a particularly successful social engineering technique, promising free tickets for the upcoming Football World Cup in Germany. The ploy prompted thousands to run the attached worm file, triggering a Yellow Alert.

Trend Micro also detected attempts to use worldwide news and political figures as social engineering elements of malicious emails. Though the technique only had a minimum impact in most cases, it led to a Yellow Alert with WORM_BOBAX.P in June. This worm portrayed news of both Saddam Hussein and Osama Bin Laden having been captured.

From the South Asia tsunami in December 2004 to Osama Bin Laden's apparent discovery, the use of popular interest news is reminiscent of spamming techniques and is becoming a relatively common trend for the propagation of numerous security threats.

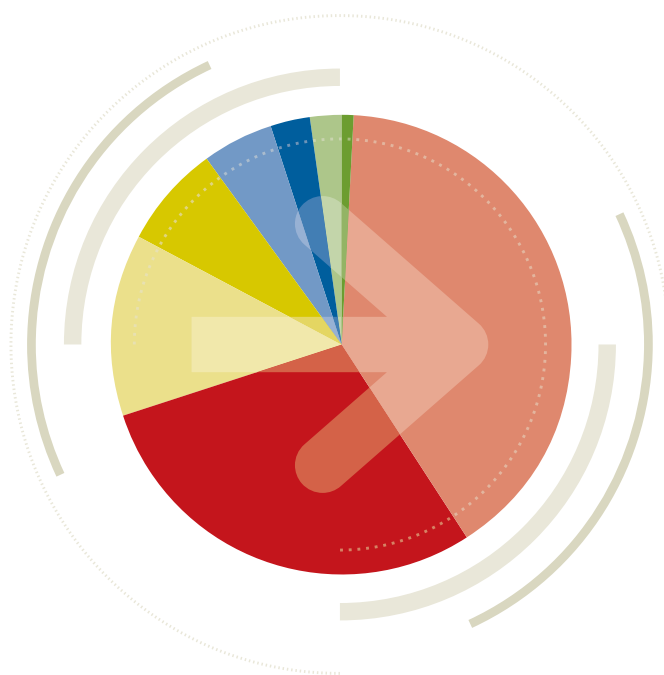
The language of spam

A rise in spam usually follows a growth in ICT and will hopefully be resolved once proper facilities have been put in place in private, public, and government sectors.

Given all the languages in the world, the fact that English alone accounts for 40% of all received spam definitely proves that it is also the most preferred business medium. What is also notable, however, is that Non-English spam grew by 20%. Such an increase supports other observed behavioral patterns, suggesting that spamming runs are becoming more localised for increased effectiveness.

The most recent entry in Trend Micro's language distribution list is Spanish-language formatted spam – at 13% in 2005, compared to just over 2% the previous year. The European Organisation for Economic Co-operation and Development has just presented its recommendations based on Spain's driving factors, which include improved information and communication technology spending, as well as in areas related to high-technology. It has been observed that a rise in spam usually follows a growth in ICT and will hopefully be resolved once proper facilities have been put in place in private, public, and government sectors.

Another surprise is the significant drop in Chinese-language spam, which bodes well for the region given that it is considered an area of rising economic opportunities and hundreds of first-time users online. In September of 2004, China acknowledged their spam problem and began working with the major industry players to mitigate those issues. Conversely, Japanese-language spam continued its steady rise, a few points above its previous mark a year before.

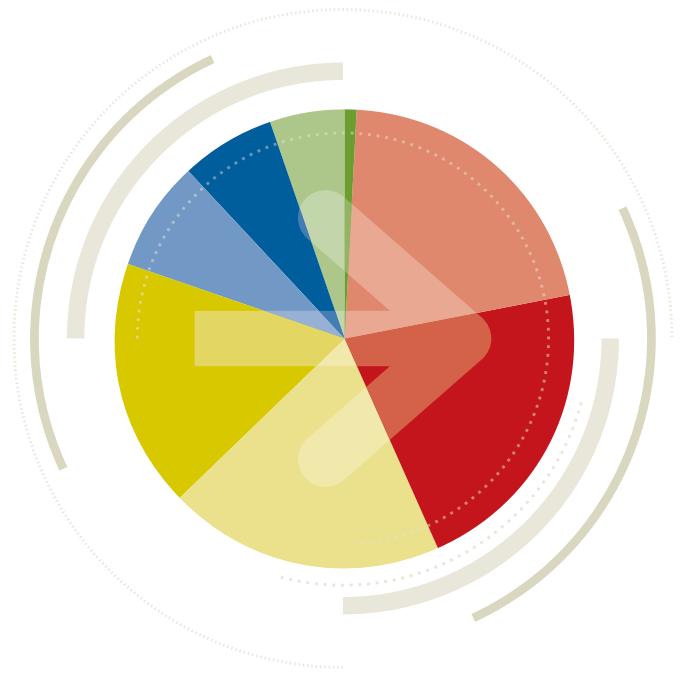


English **40%** Spanish **13%** Italian **5%** Chinese **2%**
Japanese **29%** Korean **7%** Russian **3%** German **1%**

English alone accounts

The subject matter of spam

As with prior years, spam continued to be a significant problem in 2005. However, there were significant changes to its content. In 2005, commercial spam dropped nearly 50% over the prior year, while academic/education related spam increased by 100%. Financial and health related spam dropped a few points from its last index, with health topics dropping as much as 70%. Gambling and games of chance accounted for 22% of spam – a stark contrast to the mere 1% seen in 2004. Similarly, adult related topics increased to 21%, versus 6% in previous years.

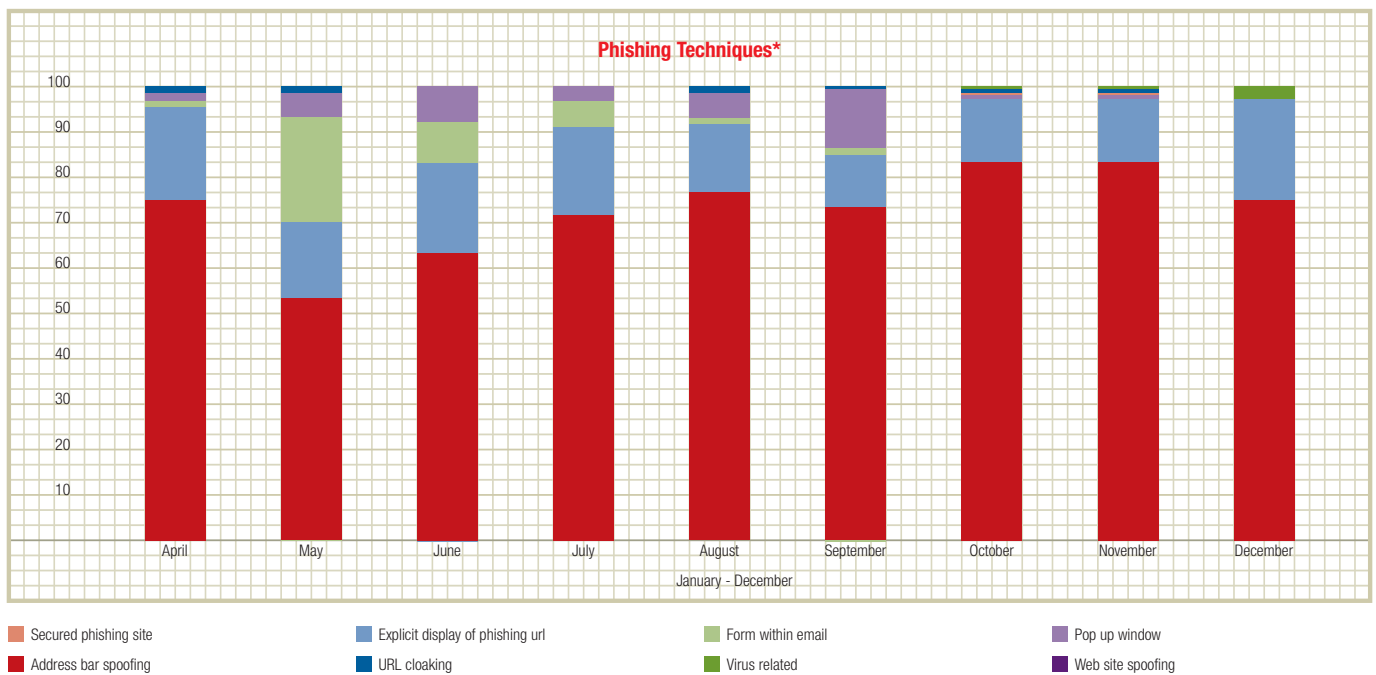


■ Gambling **22.05%**
■ Education **19.35%**
■ Financial **7.83%**
■ Racial **5.19%**

■ Adult **21.47%**
■ Commercial **17.61%**
■ Health **6.48%**
■ Spiritual **.02%**

for 40% of all received spam

phishing: what have we got here?



Phishing attacks are a sub-category under the spam umbrella. Techniques observed here are true for any language across various categories – albeit most are financial or commercial in nature. Address-bar spoofing accounted for 81% of all phishing attacks in 2005, a technique which works mainly on users of Internet Explorer (accounting for close to 90% of users where Microsoft Windows install base accounts for 95% of desktop computers worldwide). The technique abuses Active-X where images cover the actual URL on the browser by displaying a bogus image on top.

By the end of 2005, the explicit display of the phishing URL had diminished to only 13% of attacks, compared to 76% at the beginning of the year.

The use of fill-up forms and scripts embedded in HTML formatted email each accounted for less than 3%, rising 2 points from previous years.

The changes and reversals in phishing techniques over the past year appear to be the result of a blatant combination of email vulnerabilities which would allow automatic execution without user intervention on victim computers – all that is needed is for one to open a message in its native HTML format for all kinds of problems down the road. Some of these problems are even attributed to spam and adware when growth of grayware is considered and infection vectors are investigated.

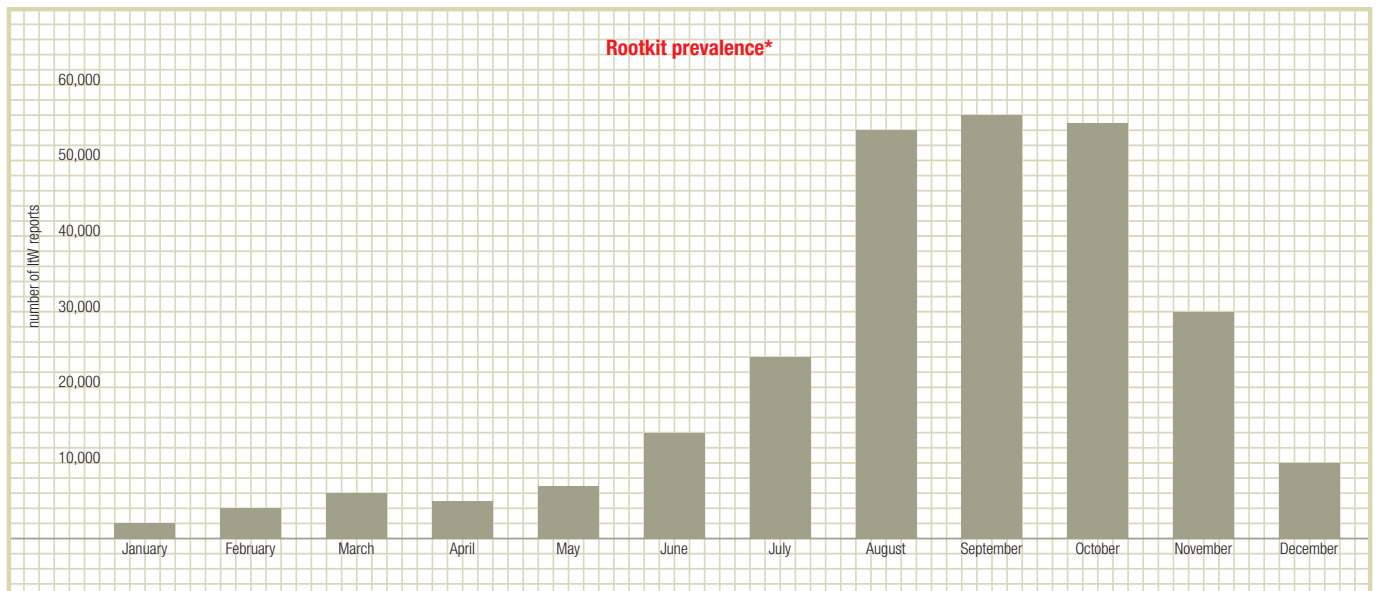
the return of rootkits

...the rootkits we saw at the end of 2005 were coupled with different kinds of threats – all geared toward financial gain as the bottom line

The functionality associated with rootkits to mask the presence of malicious activity is nothing new. To survive, viruses and network worms controlled memory time slices during the old days when computer memory was scarce and file storage was very expensive. In the following years viruses were loaded from boot-sectors, giving them prior access to the operating system – thus enabling the virtual capability to retain a certain block of memory for their use without interfering with normal computing operations.

Though process-hiding malware has been used for some time, their usage has become common once again after several years of dormancy. More importantly, the rootkits we saw at the end of 2005 were coupled with different kinds of threats – all geared toward financial gain as the bottom line. Trend Micro expects this trend to continue in 2006.

Detecting the existence of one or several rootkits in a system is not easy, and analysis of the hidden malware can be difficult. Consequently, parasitic lifetime can be increased exponentially. Add to this the fact that most rootkits are open-source developments and readily available to anybody. Trend Micro continuously discovers more of these threats as usage gathers a following among malware authors. There was an observed rise in the use of rootkits coupled with other threats mid-year 2005 and it is highly probable that this trend will continue through 2006 in attempts to hide spyware and adware.



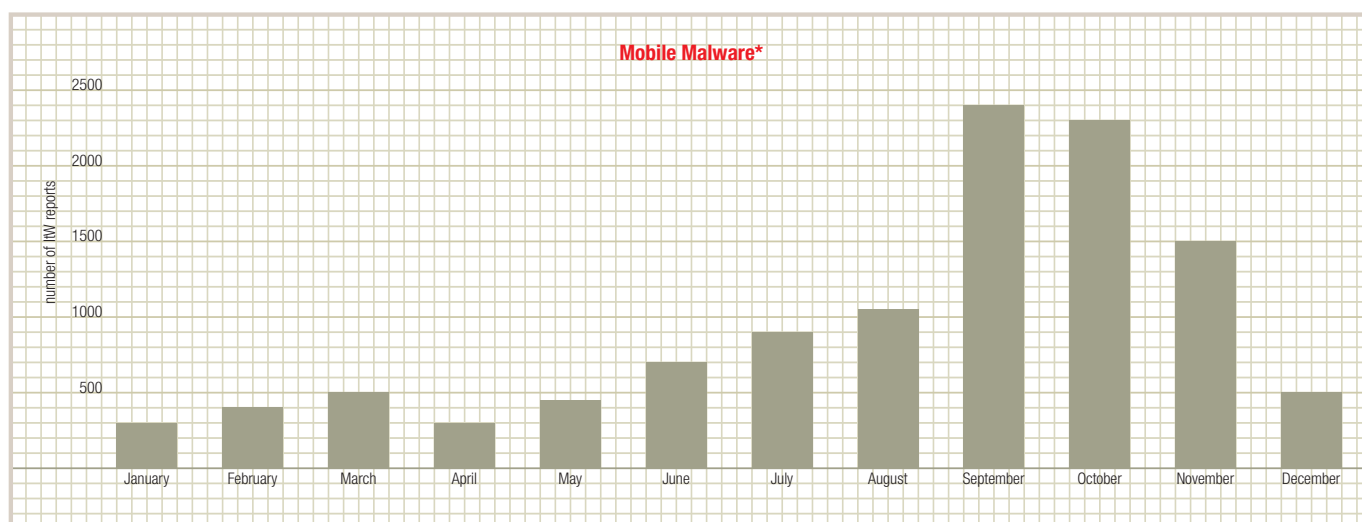
have phone... will travel

The first mobile worm was discovered in August of 2004. Tagged as SYMBOS_CABIR, it used Bluetooth to send itself over the airwaves to unsuspecting victims who thought they had received a security program and proceeded to infect themselves upon installation. CABIR and its variants ran natively on the Symbian 60 operating environment, which accounts for more than 80% of the GSM mobile phone market. Since then, Trend Micro has recorded an increased number of mobile threats abusing other phone technologies such as multi-media messaging (MMS), the ability to surf, as well as to download email attachments.

In September of 2005, SYMBOS_CARDTRP.A attempted to be the first cross-platform mobile worm by dropping worms in the infected memory card including WORM_WUKILL.B. When the card was attached to a Windows computer, it had the ability to open a backdoor to the system and distribute two more worms. Though the attack was not particularly successful, it did demonstrate the ongoing development of mobile malware. If this trend continues, we can expect to see new features being added to the mobile worms, further increasing their potential for a successful attack vector.

In an interesting turn of events, during November of 2005 Trend Micro received samples of a mobile phone malware that attempted to gather all contact details and send them to any other mobile device in range. Trend Micro named this malware SYMBOS_PBSTEAL.A. This malware was, in effect, the first information-stealing threat for mobile phones.

At this time it is unclear how popular phone book stealers and malware droppers could become among malware writers in the future. However, it is unlikely that this was the last one we will see. Therefore, it is important to remain vigilant to protect emerging technologies – particularly those geared toward higher mobile bandwidth connectivity such as WiFi, EDGE/GPRS, 3G/UMTS and even up and coming WiMax.



how much is that vulnerability window?

Outbreaks of 2005*				
Name	Vulnerability discovery	Exploit window	Outbreak declaration	Damage cost**
BUGBEAR	Thursday, March 29 2001	550	Monday, September 30, 2002	?
MINDA	Tuesday, October 17, 2000	336	Tuesday, September 18, 2001	\$635,000,000
SQL SLAMMER	Wednesday, July 24, 2002	185	Saturday, January 25, 2003	\$1.3 billion
SLAPPER	Tuesday, July 30, 2002	46	Saturday, September 14, 2002	?
BLASTER	Wednesday, July 16, 2003	26	Monday, August 11, 2003	\$2 billion
SASSER	Tuesday, April 13, 2004	17	Friday, April 30, 2004	\$3.5 billion
ZOTOB	Tuesday, August 09, 2005	5	Saturday, August 13, 2005	\$500,000,000+

Security industry experts estimate that the costs due to damage and recovery for every successful outbreak numbers in the billions of dollars (USD). In fact, the most recent estimate for every year to come will be at least \$11 billion (USD), given the current rate at which new threats are propagated. Rising costs are due to the decreasing window between vulnerability discoveries the time an exploit is actually written and incorporated into a fast spreading worm. This means less time to actually test and quality-assure patches effectively on parallel systems, in the effort to ensure that undesirable side effects do not happen to concurrently-running systems.

2005 and present-day threats: what is

Spy-Phishing: A targeted spyware attack, where a downloaded Trojan is programmed to steal specific information from a specific legitimate URL. The Trojan sits silently on the user's system, until that URL is visited. The Trojan then activates, sending the information to the malicious third party.

In 2005, the vast majority of threats were inspired by financial gain, rather than the apparent desire for notoriety or bragging rights that influenced malicious behavior in prior years. These attackers preyed on users with the intention of information theft. As such, they invented whatever tricks they could, as modern-day con artists with a worldwide field of millions serving as potential victims.

The switch in motivation changed the very fabric of the threat landscape. New malware is mostly inspired by financial gain. We are observing more and more targeted attacks focusing on a certain company and their users, or on a particular group with a common connection. Specially crafted Trojans are spammed to these targets with the hopes that unsuspecting users will fall into the trap. Favoring this kind of slow spreading as opposed to the big worm infection dramatically increases the odds of the malware going undetected for a longer period of time. This strategy allows for gathering more confidential information before the Trojan is detected and removed.

2005 also bore witness to a new kind of attack, which Trend Micro calls "spy-phishing", which borrows techniques from both phishing scams and pharming attacks – along with some new tricks – to target on-line banks, financial institutions, and other password-driven sites. In spy-phishing the author seeds email messages with either a Trojan, or a link to download the Trojan. When downloaded and executed, either manually or via an exploited vulnerability, this malware monitors web traffic until it detects web access to the target page. When this happens, it sends any login or confidential data back to the attacker. There have been different variants targeting specific entities or related web companies, all with the same objective.

The text in the spammed email can be related to the target company, or it can employ other forms of social engineering, similar to those utilised for

traditional viruses. In either case, the effect is more dangerous than traditional Phishing, since it does not have to rely on tricking the user into visiting a spoofed site. And since it is much easier from a technical perspective than launching a Pharming attack, even so-called "script-kiddies" can potentially launch a successful attack. Spy-phishing effectively starts with the authentic bank page when the user willingly logs in. And once the user enters his information, he proceeds to the intended site without interruption, so there is no unusual behavior that may alert him to a potential problem. The only difference is that the user's information has also been diverted to a third party, who is now empowered to use the same to conduct illicit activities.

A prominent trend in 2005 was the de facto usage of blended threats. Motivated by financial gain, attackers did not limit their activities to the theft of bank and e-commerce credentials. Many also infected victims' systems with spyware, adware and other grayware. By including spyware and adware from third parties in their attacks, some malware authors were able to participate in marketing campaigns that offered a commission per unit installed. So the more users the attacker infected, the more money he would make. Multi-trojan attacks started with a downloader/dropper program that only existed to bring more files to the system and install a variety of other trojans, adware, or spyware. This was not rare to see in 2005, and the trend was directly linked to the switch in motivation discussed above.

Each of the aforementioned techniques share one common element – the longer they stay undetected, the higher their prospects for success. Stealing information is an activity that has limited usefulness if its capabilities are active for only one day. The longer they are listening, the higher the probability of obtaining valuable information. This need to avoid detection had two immediate effects in the threatscape of 2005:

different now?

1 Malware authors learned, as far back as 2003, to use different packers in order to mask the internal structure of binary programs. Packer programs compress executable files to make them smaller, but they also make them different from the detection point of view of traditional scanners not using code emulation and behavioral analysis. Using this ability as a stealth factor can potentially prolong the life of the program, as antivirus vendors need to obtain the multiple samples to properly detect the malware variant. In 2005, attackers frequently spammed many different waves of the same malicious Trojan, each compressed with a different packer – and sometimes even using a combination of different packers – in an attempt to elude detection.

2 Attackers have looked for other stealth methods and have found the most effective of them all: rootkits. Towards the end of 2005, rootkits were being used as the ultimate weapon to assist in cloaking malware and grayware activity. Rootkits modify the operating system behavior to hide certain processes, files, folders, and registry entries. This grants unparalleled power to the malicious application while making it vastly more complicated to detect and remove them. Since rootkits are publicly available – many use open source standards – even writers who do not possess the technical skills required to produce a rootkit can potentially utilize them because the work has already been done for them. As rootkits become increasingly popular among the malware writers, content security vendors must hone their tools to detect these devices. Trend Micro has observed rootkits as part of bot and Trojan tandems with increasing regularity, particularly in the third-quarter where more than 150,000 computers were found to have been affected.

Another important trend in malware last year was the increased modularity of malware employed for attacks. Bot worms grew to be the fastest-spreading malware, due primarily to the fact that many of them were readily available from open-source developments, built in a modular fashion. Any miscreant need only download the source code of these bots, select the modules to use and create a new variant.

By adding new modules to bot worms, malicious writers moved bots, a traditionally slow-spreading attack, to a new category: the most flexible malware ever. They can function as email worms, network worms, P2P worms, or all of these things simultaneously. With this increased flexibility, malware writers proved something else last year: they could add any new vulnerability exploit as soon as it was announced. In October of 2000, the NIMDA Worm took nearly a year to exploit the published vulnerability; by 2004, the release of SASSER had cut that number to 17 days; but in 2005, ZOTOB painted an alarming picture where it took only five days from the announcement of the vulnerability to the time when a successful exploit was added to a worm's code.

Now that bot worms have become the Swiss Army Knife of all malware with their email-spreading capabilities, network vulnerability exploitation, companion rootkits, and so on – detection numbers are on the rise. The main bot families have thousands of different variants documented and as such pegged detections are in the millions.

The usage of bot functionality in worms has not changed from the past. Bot-net owners use them to upload spyware/adware, steal information, create spamming platforms, and launch distributed denial-of-service attacks against third parties. All of these offer financial gain to the bot-master in proportion to the number of victims in the bot-net. Once the bot-net has reached a considerable size, it can be sold or portions rented out for other malicious uses: as proxies for sending spammed emails, stealing private data, or uploading spyware or adware to the infected machines.

Since 2002, bot worms have been growing exponentially, and 2005 was no exception. They are becoming increasingly complex and dangerous and have demonstrated their ability to use network vulnerabilities as soon as they are found. Last year, police and investigation units uncovered bot-nets consisting of more than 200,000 victims worldwide. Bots have easily become one of the most formidable threats to be reckoned with and quite possibly possess the highest potential for damage.

what do we expect in 2006?

Given the current threatscape, Trend Micro expects a continuation of many already established tendencies seen in 2005:

- *Spy-phishing* reports will continue to rise as phishers take advantage of the longevity that parasitic code affords contemporary malware.
- *Bots* will contain increased functionality through the use of rootkits and the closing gap between discovered vulnerabilities to exploits.
- *Spear-phishing* will become the predominant concern for individual companies.
- *Spam* will further permeate other local languages and dialects, but stick to the more profitable culture with the capacity to pay.
- An increased number and variety of *packers* will be used to compress and encrypt malware to avoid scanner detection.
- *Messaging protocols* including IRC, IM, and P2P will continue to tunnel through firewalls and be used as infection vectors.
- *Vulnerability windows* will continue to shorten, thereby warranting more proactive solutions from the security industry.
- The continuously *blurring* line between grayware and malware will prompt security vendors to strengthen their stance on the rights of users to remove these threats.



- **Rise of bots and botnets.** As the use of bots and botnets reward their creators with enormous illegal gains, we expect to see detection numbers increase this year for new variants. Installation bases will slowly consolidate as all the old undetected bots get replaced by improved or competing variants.
- **Increase on stealth methods.** We predict a growth of rootkit and other stealth technologies. The rootkit technique has been increasingly popular and will remain so in the near future. As a mitigating factor, when Microsoft releases its new Windows operating system this year, it might be necessary for rootkit programmers to change their strategies for the new environment. This will not affect current rootkits designed for the most popular Windows versions today.
- **More spy-phishing and targeted attacks** in a fashion similar to phishing techniques. Using phishing-like and other social engineering tricks can increase the impact to the user base. We also expect more targeted attacks on a smaller scale, which can help attackers receive direct information and stay undetected for a longer time. Both kinds are dangerous, because they target confidential information as opposed to the plain destruction that characterized attacks in the past.
- **Prevalence of adware and spyware.** Advertising programs have been very common for a long time. Advertising campaigns generate big amounts of money every year. Many advertising software companies would happily pay to help them install their adware products in as many PCs as possible. Though there have been attempts from governments to regulate and stop this practice, it has been increasing ever since its inception. Now, even malware writers opt to include adware in their creations to further increase their gain. This behavior is likely to maintain its current growing trend.



advice for users to avoid being affected

For companies and corporations:

- Deploy HTTP scanning methods. Many modern threats utilise the Web protocol to spread. It is highly recommended to implement a Web virus scanning system, much in the same way that administrators started deploying email scanning long ago. Detecting and stopping threats before any infected file can reach the end user adds a new layer of protection in the corporate network infrastructure. Spyware protection in the network layer is a bonus because these threats use HTTP exclusively to enter the corporate environment.
- Block unnecessary protocols from entering the corporate network. The most dangerous of them are IM P2P communication protocols and IRC (chat). These two are part of the bot arsenal of weapons to propagate and communicate with their botmaster and should be disallowed in the corporate firewall.
- Deploy vulnerability scanning software in the network. Being constantly up-to-date can minimise the impact of any new network vulnerability and diminish the risk of being infected by this kind of worm.
- Do not give administrator privileges to all users. The most dangerous of all privileges is "load and unload device drivers". This is the most recommended measure to prevent being affected by rootkits. Usually rootkits are implemented as device drivers, in order to have access to all operating systems internals. Redesigning the user policy to limit users in this fashion can be one of the most useful ways to secure a network. If the administrator deprives users of admin rights, there is an added bonus: aggressive malware would not be able to kill antivirus processes in the system.
- Deploy corporate anti-spyware scanning. As they are becoming prevalent threats for corporate businesses, the administrators need to deploy specific software to detect and stop them.
- Educate users; enforce a strict security policy within the network. Not only do software and defense systems help fight against malware. Most of the time, the user needs to take some kind of action to infect the machine. Be it a Web page that installs spyware or an infected email, the user needs to know in advance the ways new malware attack users. User awareness is the key to a clean network, and administrators should conduct ongoing education initiatives to keep users informed and protected with updated malware technology. This is especially important with newer users, as they are the ones malware writers typically target.

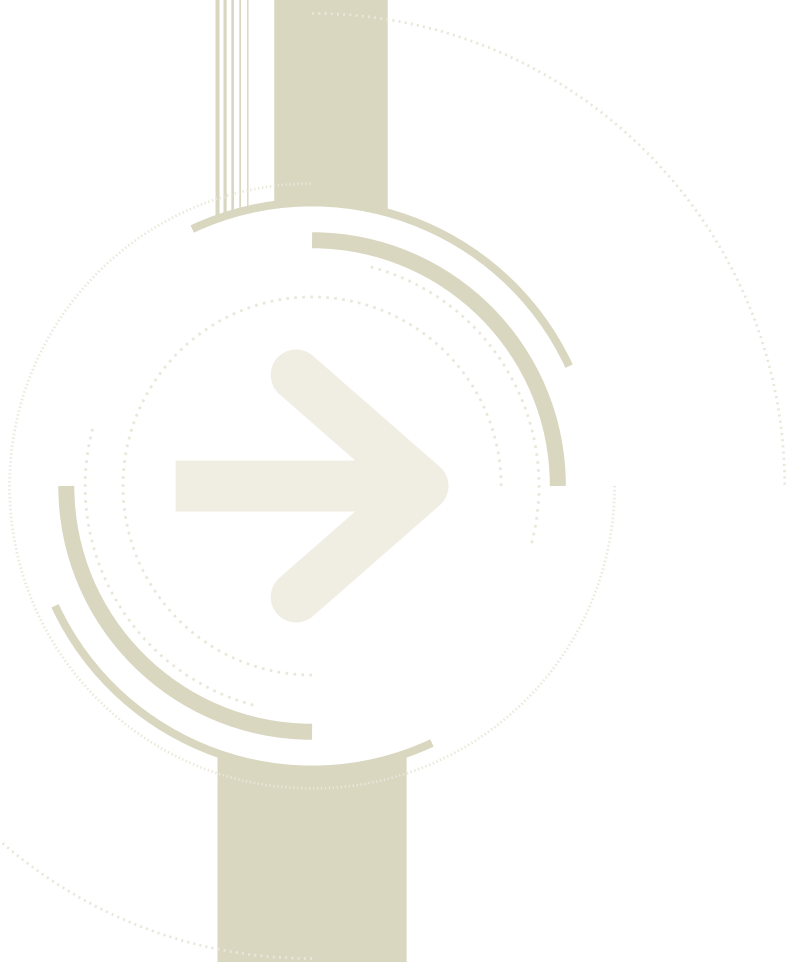
Be constantly up-to-date

by malware trends in 2006

For home users:

- 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 with an updated antivirus and anti-spyware software any program downloaded through the Internet. This includes any downloads from P2P networks, through the Web and any FTP server regardless of the source.
- Beware of unexpected 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 have an antivirus real-time scan service. Monitor regularly that it is being updated and that the service is running.





www.trendmicro.co.uk

Belgium/Luxembourg

+32 2 7092056

Denmark

+ 45 36 94 45 96

Finland

+358 9 4730 8301

Norway

+ 47 22 86 24 40

Iceland

+ 47 22 86 24 40

Netherlands

+31 30 210 6333

Sweden

+46 (0)8 545 298 30

UK/Ireland

+44 1628 400500