

Table of Contents

[Executive Summary](#)

[Software and Infrastructure Vulnerabilities](#)

- Easy Does It: .ANI Exploit Tops Exploit Chart
- The Other Side of Web 2.0
 - Cross-Site Scripting
 - Vector Markup Language Vulnerabilities
 - Web Browsers & Third-Party Plug-ins
- Desktop Applications: The Search for Bugs Continues
- Widgets: The Next Big Little Thing
- Mobile Threat Landscape: Ripe for Mischief

[High-Impact Threats](#)

- Regional Attacks
- Social Engineering Techniques
- Compromised Pages: Abusing Trust in Legitimate Web Sites
- Attacks against Online Entities
- Data Leakage: Human Beings are still the Weakest Link

[Process-Based Threats](#)

- Malware Type Statistics
- Web Threats
- Rogue Antispyware

[Content-Based Threats](#)

- Spam
- Phishing

[Distributed Threats](#)

- Botnets
- Nuwar – The Storm continues

[The Digital Underground Economy](#)

[Summary & Forecast](#)

- Threat Forecast
- Technology Forecast

[Best Practices](#)

- Vulnerability and Patch Management
- Software Resource Management
- End User Education and Policies



Executive Summary

Last year, Trend Micro's *2006 Annual Roundup and 2007 Forecast (The Trend of Threats Today)* predicted the full emergence of Web threats as the prevailing security threat in 2007. Web threats include a broad array of threats that operate through the Internet, are typically comprise more than one file component, spawn a large number of variants, and target a relatively smaller audience. This was predicted to continue the "high focus/low spread" themes seen by some attacks in 2006.

Trend Micro also predicted that the growth and expansion of botnets during 2007 year would be mostly based on new methods, ingenious social engineering, and the exploitation of software vulnerabilities. The roundup also indicated that crimeware would continue to increase and become the prevailing threat motivation in 2007 and onwards.

As we highlight the threats that made rounds in 2007, it will become clear that all of these predictions have indeed materialized, and some in an interesting fashion.

The shifting threat landscape demands a move away from the traditional concept of malicious code. Digital threats today cover more ground than ever. They may come to a user through simply having a vulnerable PC, visiting trusted Web sites that are silently compromised, clicking an innocent-looking link, or by belonging to a network that is under attack by a Distributed Denial of Service attacker.

In the following roundup, Trend Micro summarizes the threats, malware trends, and security highlights seen during 2007. Real-life victims of these security threats include interest groups, individuals, organizations, and on some occasions even countries. Together these examples clearly illustrate the need for improved methods to combat Web threats. All data provided in this report was gathered from TrendLabs – Trend Micro's global threat investigation, research, analytics and support organization.

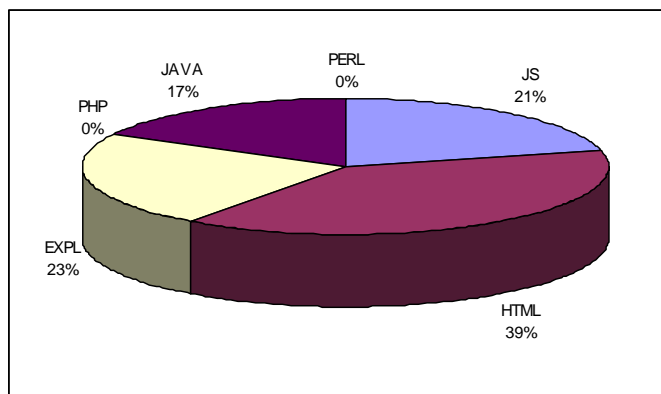
Software and Infrastructure Vulnerabilities

Software and infrastructure vulnerabilities exist in the way programs (whether operating systems or software applications) or infrastructures (like network architecture, mobile communication enablers, etc.) are designed or configured to treat certain data. Often there are holes in the program brought about by programming oversight, misconfiguration, or other factors that could open aspects of the program or system to misuse. Typically, these vulnerabilities are those which allow remote attackers to create exploits that perform malicious commands on the affected system. Threats to the underlying basic technologies of existing applications are of major concern due to the fact that new implementations are built on top of an environment that may already be proven to be exploitable.

Broadly speaking, those programs for which exploits often appear are popular, widely used applications including multi-media players, office applications and even security programs.

Web Technologies

HouseCall scans for Web 2.0 threats in 2007 show that the Windows Animated Cursor exploit (EXPL_ANICMOO) was the most prevalent on a worldwide scale. However, if the analysis is based on components, HTML codes overtake EXPL codes in terms of prominence. This could be attributed to the number of malicious IFRAME detections in 2007. JavaScript detections follow at 21%.



Web Threat Distribution by Component Type

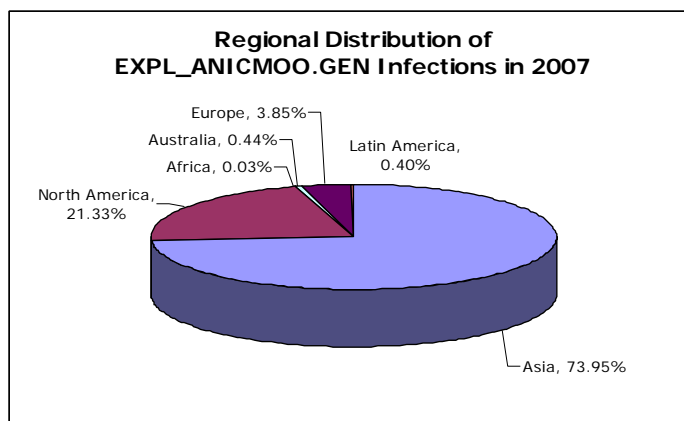
Easy Does It: .ANI Exploit Tops Exploit Chart

The prevalence of the animated cursor exploit and related infection reports prompted Microsoft to release an out-of-cycle patch last April 3 after it had been in the wild for a couple of weeks.

The vulnerability it seeks to exploit is in the way Windows handles animated cursors. .ANI is a file format used for reading and storing animated mouse pointers. It works like a movie film or a cartoon strip in that it is actually made up of several icon frames still-shots programmed into a sequence so that the mouse pointer graphic appears to move. It has a simple file structure, with only the second or latter part of the block of a malicious .ANI file responsible for bringing about exploit activities.

Top Ten Exploit Codes for 2007	% to total exploit codes	CVE
EXPL_ANICMOO.GEN	54%	CVE-2007-0038
EXPL_WMF.GEN	18%	CVE 2005-4560
EXPL_EXECOD.A	9%	CVE-2006-4868
EXPL_DHTML.C	5%	CAN-2004-1319
EXPL_SSLICE.GEN	4%	CVE-2006-3730
EXPL_IFRAMEBO.A	2%	CVE-2006-4777, CAN-2004-1050
EXPL_MHT.AF	2%	CAN-2004-0380
EXPL_MS04-028.A	2%	CAN-2004-0200
EXPL_DHTML.G	1%	CAN-2004-1319
EXPL_TXTRANGE.A	1%	CVE-2006-1359

HouseCall is the free online scanning utility offered by Trend Micro Web site. Data in this report came from its 2007 scan results.

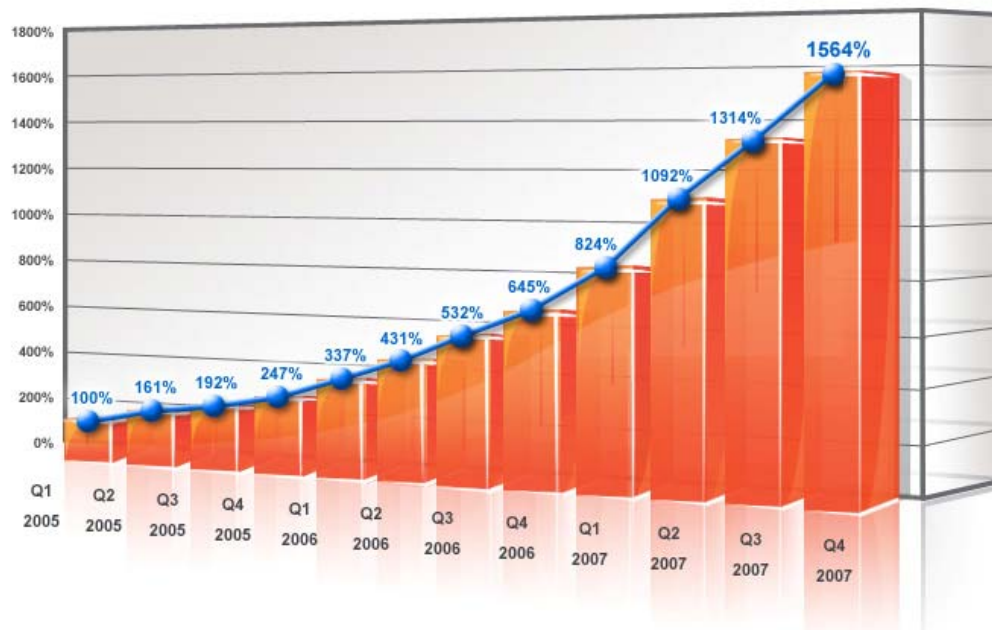


A majority of its infections (74%) in 2007, came from Asia. The same holds true for a related threat detected as TROJ_ANICMOO.AX which embedded the exploit, as 64 percent of computers infected with this threat are actually from China. Its relative success in infecting Asian users, considering its lack of complexity, reflects the appeal of animated cursors to the region and some misconception about the safety of their installation and use. Infection counts for EXPL_ANICMOO.GEN fell only in the month of October 2007.

The Darker Side of the Web

During the past few years, social networking and other tools have expanded the ability for users to participate more actively in the Internet. Over time, as this evolution has happened, companies have also become more comfortable with the idea of embedding remote functions, applications, or objects within corporate Web pages. Also, more often, organizations are looking to harness these new tools by creating user communities or opening their sites to various levels of user input. While this makes the Web more exciting, it involves new and changing risks. This year has seen enormous growth in Web-based attacks that prove this point.

The following table displays the growth of Web threats as tracked by Trend Micro in between 2005 and end 2007. A Web threat is any threat that uses the Web to facilitate cybercrime. Simply explained, the majority of attackers now look to harness the capabilities offered by the Web in order to gain profits. Through different attack mechanisms Trend Micro has tracked how different methods and technologies have been used to effectively attack computer users.



Cross-Site Scripting and Exploitable Interactions

Cross-site scripting vulnerabilities, for example, are the susceptibility of applications to execute arbitrary code when presented with unexpected data. Two cross-site scripting exploits that made it to security news this year are EXPL_YAHOXSS.A, which exploits a cross-scripting vulnerability in *Yahoo! Mail*, and JS_QSPACE.A, which also uses cross-site scripting to hack *MySpace* accounts.

Vulnerability	Detection	Date of Advisory	Description
Cross-site scripting vulnerability in MySpace	JS_QSPACE.A	December 2, 2006	Redirects user to a phishing URL
Cross-site scripting vulnerability in Yahoo! Mail	EXPL_YAHOXSS.A	June 19, 2007	Proof-of-concept (POC) exploit code



EXPL_YAHOXSS.A, which is the detection for a pair of codes that work together to take control of an active Yahoo! Mail session of an infected user, is triggered by a single click on a link that appears very much like the link to legitimate Yahoo! search results lists. JS_OSPACE.A, on the other hand, targets users of *MySpace*. Upon execution, it exploits a cross-site scripting vulnerability in *MySpace* to redirect a user to a phishing URL. It also contains codes to edit the profile of stolen accounts, adding a movie file to it that also contains the phishing URL. When other users visit the hacked *MySpace* account, the JavaScript is downloaded and executed on the user's own profile. It appears that the popularity of social networking sites makes them viable infection vectors for malware authors.

In July, there were reports of a cross-browser scripting vulnerability between *Firefox* and *Internet Explorer*. First seen a month prior, in June 2007, the vulnerability exists in the way IE passes information to Firefox, causing Firefox to execute JavaScript code when a link is clicked. This is due to the registration of a certain Uniform Resource Identifier (URI) called "firefoxurl" in the Windows Registry when Firefox is installed. When certain parameters are part of the "firefoxurl" URI, they are interpreted by Firefox as options, without need for validation. Microsoft issued a security alert on this (*URL Handling Vulnerability in Windows XP and Windows Server 2003 with Windows Internet Explorer 7 Could Allow Remote Code Execution*), and a patch by November. This example represents that malware authors really are determined to discover new vulnerabilities for their misuse.

Vector Markup Language Vulnerability Exploits

Vulnerabilities in several other Web-based elements emphasized the need for caution when browsing and clicking on links. Vector markup vulnerabilities in Internet Explorer (CVE-2007-0024) were exploited even after patches were released by Microsoft to address them. Several variants of these VML exploits followed well into April 2007.

Detection	Date of Advisory	Description
EXPL_EXECOD.C	January 16, 2007	Allows remote users to issue commands on the affected system
HTML_VMLFILL.I	January 24, 2007	Download and executes files
JS_DLOADER.KQZ	February 2, 2007	Download and executes files
HTML_IFRAMEBO.AE	February 12, 2007	Download and executes files
HTML_IFRAMEBO.AC	March 16, 2007	Download and executes files
JS_IFRAMEBO.BG	April 29, 2007	Download and executes files

Vulnerabilities in Browsers and Third-Party Plug-ins

In June, *Safari 3 Beta for Windows* was discovered to have a URL protocol handling problem. In July, soon after the launch of the *iPhone*, it was found that a certain vulnerability in *Safari 3* was also present. This shows that the homogenous use of base components from a vulnerable operating platform logically results in an exploit even when the system moves to new form factors such as gadgets.



Safari 3.0.03 for Windows also contained a vulnerability which allows local zones to access external domains. This provides proof of a previous forecast that cross-platform applications would also pave the way for cross-platform vulnerability and exploitation. Without need for much re-engineering it had been quite easy to break Safari's port in less than three (3) days.

Most multimedia players such as Windows Media Player, Apple QuickTime, VLC and many others support a wide variety of media formats, including audio and video file types. Some file formats are intrinsically unsecure especially if they are .ASX or .ASF files which are just encapsulations of video with a URL redirector. Players may also have extra functions to negotiate network connections and these can also be abused when misconfigured.

As an example, in September, *Firefox* had to include a patch to its 2.0.0.7 version to address a cross-application vulnerability, in particular, how the browser can be forced to execute code when a specially-crafted *Apple QuickTime* file is played using the *Apple QuickTime* plug-in. Content-streaming is a good feature but this usually requires a media proxy server which most companies rarely implement. The next recourse is to leave firewall ports open. For many users, this represents an intrusion waiting to happen - and it quite often does.

Browser Helper Objects

Browser Helper Objects are 3rd-party add-ons that extend the capabilities of the browser and usually feature shortcuts to popular services. Due to this feature's popularity however (particularly in Internet Explorer via ActiveX) it eventually turned into one of the most common infection vectors for malicious activity.

A lot of adware and spyware, even malware in general started to masquerade as BHO's by 2006. In 2007 BHO activity peaked in April and dropped to a plateau by August. This comes as no surprise given the popular migration to alternative browsers such as Firefox, Opera, and even Safari.

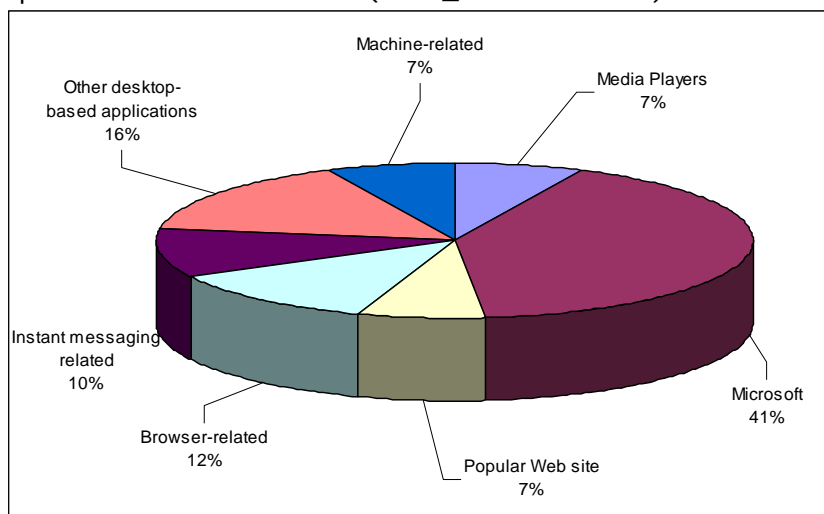
The public release of Windows Vista and its improved IE 7 browser which puts more hoops to malicious BHO installation is also another reason. However, together with alternative browser migration particularly to Firefox has likewise ushered in new attacks in the form of malicious plug-ins which are yet again 3rd-party created. Users need to be a little more careful in this respect as BHO's, plug-ins and other add-ons are no different than other pieces of code that can be used for different intentions.

In Summary:

1. Vulnerabilities in the underlying technologies used as foundation for the digital infrastructures of today are of primary focus due to how each can potentially contribute to the overall threat landscape.
2. Legacy code has been the bane of many new products in the market due in fact to the changing software lifecycle as well as previous views on security versus functionality.
3. Tools that have traditionally been in common use to improve online user experience are now being re-tasked by malicious entities and are therefore some of the leading vectors of compromise.
4. The traditional malware threats of viruses and trojan horses, often attributed to raging hormones of a wannabe hacker, have now been pointedly replaced in the past 3-years by professionally written and socially engineered threats as cybercriminals discover the availability of low hanging fruit even as online usage and acceptance grows worldwide.
5. As user generated code that forego the traditional production life cycles in favor of public feedback and other Self-publishing avenues reach commonplace wide acceptance, such practices have eventually left the door open for opportunistic malice and easy widespread introduction of blended threats into the enterprise and home.

Desktop Applications: The Search for Bugs Continues

2007 saw its share of bugs in several desktop-based applications. Windows vulnerabilities continued to number in the thousands. As seen in an earlier section, malware exploiting the animated cursor vulnerability (CVE-2007-0038) claimed the greatest number of infections each month since the discovery of the exposure from April until well into October (EXPL_ANICMOO.GEN).





Trend Micro researchers observed during 2007 that malware authors seemed to be analyzing information in recently-released Security Bulletins, and subsequently creating codes to exploit them. For instance, in early February 2007, Microsoft released its Security Bulletin. TROJ_DROPPER.FC was found just a week later, exploiting an *MS Excel* vulnerability communicated in the said bulletin. Another example was TROJ_DROPPER.WN exploited a vulnerability in *MS Word* a few days after Microsoft released the security advisory disclosing it. However during the year, vulnerabilities were also discovered at times when no patches were available. For example *Microsoft PowerPoint* (February), Windows help files and the Domain Name System (DNS) Server Service (April), and *Microsoft Access* (September). Malware authors are, in these cases, counting on the "window of vulnerability," the time between a vulnerability makes its way to the public and the time a patch is released.

Other desktop-based applications were hit by proof-of-concept malware, notably:

Vulnerability	Detection	Date of Advisory	Description
Sun Solaris TelNet Remote Authentication Bypass, a known vulnerability found in the Sun Solaris 10/11 TelNet daemon, in.telnetd	ELF_WANUK.A	February 28, 2007	Propagates across networks
iPodLinux platform with Podzilla and Podzilla2 Graphical User Interface (GUI) installed	ELF_PODLOSO.A	April 6, 2007	Proof-of concept (POC) ELF virus
Vulnerability in a ThunderServer ActiveX component in the Web Thunderbolt code ThunderServer.webThunder.1	JS_AGENT.KGN	June 14, 2007	Download a file
Adobe Reader 8.1 and earlier versions, Adobe Acrobat Standard, Professional, and Elements 8.1 and earlier versions, Adobe Acrobat 3D	EXPL_PIDIEF.A	October 16, 2007	Proof-of-concept (POC) exploit code

Further reflecting the growth of localized Web threats, vulnerabilities were exploited in Japanese applications *Ichitaro* (word-processing) and *Lhaz* (archiving), and other applications that are not typical or expected targets. For example:

Vulnerability	Detection	Date of Advisory	Description
<i>XMPlay</i> version 3.3.0.4 media player, wherein specially-crafted .ASX file can cause a buffer overflow	TROJ_MPEXPL.A	December 8, 2006	Drops and executes a file
<i>Lhaca</i> version 1.20, a Japanese archiving application	TROJ_LHDROPPER.A	June 26, 2007	Checks if the affected machine is running a Japanese OS then drops files
Vulnerability in <i>Ichitaro</i> , a popular word processing application in Japan produced by <i>JustSystem</i>	TROJ_TARODROP.Q	August 3, 2007	Drops and executes a file
<i>LHAZ</i> version 1.33, a Japanese archiving application	TROJ_LZDROPPER.A	August 20, 2007	Checks if the affected machine is running a Japanese OS then drops files

Upon execution, the payloads of these malware include the download of other files and the installation of a backdoor. Vulnerabilities in different applications run in the thousands, and further complicating this is a software testing technique known as



"fuzzing", which subjects applications to a barrage of random input meant to determine at what point the program will crash or fail. While this exercise is not malicious by itself, it does serve malware authors wishing to develop exploits on a large scale.

While the search for vulnerabilities is becoming more and more automated, malware authors are indeed moving onto more ambitious goals. In their wake is a large collection of exploits packaged into toolkits, which together with basic tools to create customized malware, give malicious users all they need to fashion an attack. The most popular of these kits, MPack and IcePack, are discussed in the section named "*The Digital Underground Economy*", later in this report.

Widgets: The Next Big Little Thing

The concept of widgets, mini-applications that provide users information at a glance and access to frequently-used tools, introduce another highly vulnerable aspect to the Web. Regardless of the operating platform used, widgets are susceptible to malicious attacks because of the developers' use of asynchronous JavaScript and XML (AJAX) with little or no concern for security, rendering them prone to cross-site scripting attacks.

A flaw in the ActiveX control which could cause a stack-based buffer overflow is the culprit in the possible execution of random code in *Yahoo! Widgets version 4.0.3* (also known as Konfabulator), the engine handling interactive virtual tools or programs such as stock tickers, calendars, alarm clocks, calculators, etc. Version 4.0.5 solves this particular vulnerability.

Microsoft Vista Gadgets is Microsoft's own version of widgets. In early August a vulnerability was identified that enabled a remote attacker to run code on a user's computer with the privileges of the logged-on user. If a user subscribed to a malicious RSS feed in the Feed Headlines Gadget or added a malicious contacts file in the Contacts Gadget, or if a user clicked on a malicious link in the Weather Gadget, an attacker could potentially have run malicious code on the system. Microsoft released a security update on August 14 to address this.

Mobile Threat Landscape: Ripe for Mischief

The number of smartphone operating system-based phones expected to grow at a 30 percent compound annual growth rate for the next five years and the unit volume of smartphones globally already outstrips laptops according to In-Stat, a respected industry analyst firm (<http://www.instat.com/press.asp?Sku=IN0703823WH&ID=2148>). This population of mobile devices represents an increasingly attractive target for any hacker hoping to make an illicit profit.

In-Stat also estimated that 8 million mobile phones were lost in 2007, and of those devices, 700,000 were smartphones (<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026944>). The major risk for such devices is the potential for lost or



compromised information. While news headlines are frequently published regarding lost laptops containing sensitive enterprise data, we will probably also see headlines in the near future regarding smartphones containing sensitive data being lost. Since the current generation of mobiles can accommodate storage cards up to 8 GB, this is a very real possibility. Outside of compromised data, the major risks for mobiles lie in financial loss through fraud along with lost productivity due to malware.

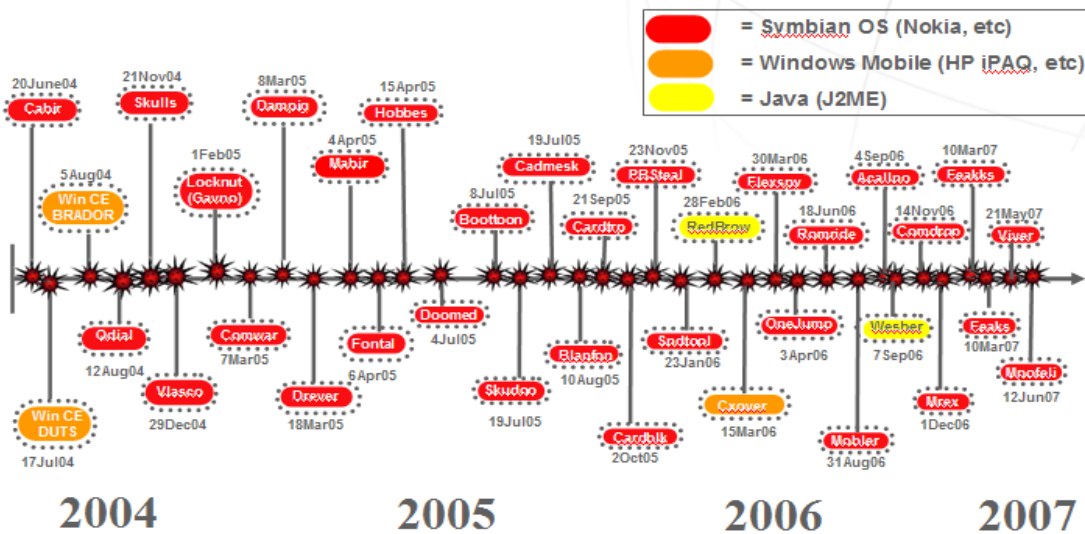
Threats to mobile devices are expected to evolve in a way very similar to the PC. Microsoft operating systems are attractive to malware authors for a number of reasons, the major reason is that the Windows operating system provided a large target population. While operating systems such as IBM OS/2, Mac OS, and Linux were available, Microsoft Windows had the dubious honor of being a primary target for malware. Why focus on niche platforms when you can write code that can infect millions of Windows PCs?

In a similar way, mobile operating systems are becoming attractive to malware authors. Major mobile platforms have become large enough to attract the interest of malware authors. The platforms have sufficient network bandwidth in the form of HSDPA, EV-DO and WiFi networks to download applications with reasonable speed. Technical familiarity with mobile operating systems is sufficiently widespread to enable malware authors to manipulate mobile devices.

The mobile device security landscape highlights the trade-off between security and ease-of-use. Creating an exceptionally secure device typically results in limitations on ease-of-use or places restrictions on software development. An easy-to-use mobile device typically suffers from less-than-robust security. For example, optimal ease of use would dictate that no PIN (Personal Identification Number) be required to access a device, but the inconvenience of entering a PIN results in a more secure device.

New devices typically hit the market focused on ease-of-use since that sells devices. People seldom buy a new device because it is more secure; they typically buy devices because it will improve productivity or look stylish. It typically takes a security breach to raise concerns about security that might impinge on ease-of-use.

The below chart shows how mobile threats have grown between 2004 and 2007. Mobile threats to-date have focused on the dominant mobile operating systems – Symbian OS (used by Nokia, Sony Ericsson, and other handset manufacturers) and Microsoft Windows Mobile.



Note: Chart includes new malware strains, does not include variants

Mobile Vulnerabilities & Malware Impact

All operating systems have vulnerabilities, but it is typically the most popular operating systems that have these vulnerabilities exploited. Trend Micro has identified a number of vulnerabilities in operating system applications that can be used in Denial of Service (DoS) attacks. Such vulnerabilities are typically patched by vendors in subsequent releases, but the thousands of devices in circulation are typically not patched by the device user.

Mobile malware exists, but to date has been more proof of concept than something that has caused widespread damage. Mobile malware that results in fraudulent profits has affected mobile devices using Java was seen in 2006 in the form of RedBrow.

Malware that can be used for data theft cropped up in 2005 with PBSteal which stole phone book information from Nokia devices and in 2006 with Flexspy which can forward phone call and SMS text message information.

Malware that causes inconvenience or incapacitates devices have been seen in modern mobile operating systems since 2004. While data on memory cards and main storage can be destroyed by such malware, service on the infected device can be restored by doing a "hard reset" to a device's "factory" settings. Instructions on how to reset a device are typically included in the device manual or on the manufacturer's website.

Apple iPhone & iPod touch

The mobile landscape is exceptionally dynamic. Apple is opening the operating system used by the iPhone and iPod touch to third party developers in February 2008. Given Apple's high profile and device cache, the opening of the operating system will be an opportunity for digital mischief by those who want to tarnish Apple's iconic mobile device.



Google Android

Google has announced the Open Handset Alliance and is working through the alliance to deliver Android, an open and free mobile platform. According to Google (<http://code.google.com/android/what-is-android.html>), Android is a software stack for mobile devices that includes an operating system, middleware and key applications. If Android achieves market acceptance and garners a significant portion of the smartphone market, it would become an attractive target for malware authors.

Widgets

As discussed in an earlier in the report, Widgets are mini-applications that enable users to pull information from their favorite websites, typically using RSS feeds. Such small applications offer the ability to make sense of the flood of information. Widgets provide an attractive attack vector, as demonstrated by the "Secret Crush" malware that posed as a Facebook widget to install itself on about one million PCs in late 2007 and early 2008. If widgets start proliferating on mobiles in a way similar to PCs, this could prove to be an attractive attack vector against mobile devices.

Java and AJAX

Javascript programming language along with Asynchronous JavaScript and XML (AJAX) provide a potential gateway to manipulate mobile devices. Mobile devices typically ship with Java 2 Mobile Edition (J2ME). AJAX is an extension to the JavaScript programming language that can be used to improve the responsiveness of Web sites by automating the exchange of information between browsing software and back-end Web servers. AJAX tools are widely used in a number of ways by sites including Google Maps, Yahoo and MySpace.

While mobile devices have previously functioned in their own web world of sites specifically architected for mobile device, the mobile and PC web worlds are merging. Scripting attacks targeting PCs may also prey on mobile devices.

Blackberry

Blackberry pioneered the enterprise handheld market for push email with its iconic devices and the Blackberry Enterprise Server (BES) backend management. BES has the ability to lock down devices and encrypt user data, mitigating potential threats since users can be blocked from installing applications and data can be secured through encryption.

Vulnerabilities in the Blackberry solution arise when administrators do not lock down devices or encrypt data. While BES provides this ability, many administrators choose not to use this functionality in an effort to avoid user complains about performance degradation. Devices that are not locked down through BES are devices vulnerable to in the event that users install dubious third party software or Trojans.

For users of Blackberry devices that do not connect to enterprises using BES, the risks are very similar to those found in other mobile device operating systems. For example, one software vendor sells software that runs on Windows Mobile, Symbian and Blackberry that can send out inbound and outbound call and SMS traffic information unbeknownst to the user.



In Summary

1. The past decade has been riddled with operating system exploits due likewise to trade-offs of security vs functionality. In the past 3-years TM has seen these attacks take a back seat as companies scramble to include software security review. Today's attacks are now decentralized in the sense that instead of the underlying OS it is now the multitude of desktop and server applications. The new mantra is yet "patch, patch, patch" but this now includes all existing applications aside from the operating system/platform.

2. Each new technology introduced over the years and immediately introduced into public/mass use has had its own growing pains. This fact has resultantly introduced front-end opportunities to do things right the first time, and if not then to fine tune the optimal balance between functionality and security to address the technology or device's current place in the market.

3. Hand-held, mobile, and aesthetic gadgetry that allow cross-platform/form-factor shared use are now a well-known threat vector due to the race of making them available en-masse to the market and yet cheaper to manufacture. Apparently current policies in place in many organizations still have not adapted to the fact that employees who bring unmanaged devices to the office are virtual trojan horses that can leave enterprises open to compromise.

High-Impact Threats

High-impact threats are threats that have the capacity to cause very high localized damage, in a specific region, community, business, or group. They cover both regional and targeted attacks.

Regional Attacks

High-impact threats can be localized and regional or aimed at specific groups of individuals. Instead of viewing malware infections on a global scale, there is more value in diving into regional numbers to see the attacks sustained. This closely follows the nature of Web threats. A summary of the most prevalent malware per region for the year 2007 are found below:

Region	Prevalent Malware based on Submissions
Asia Pacific and Australia (except China and Japan)	TROJ_ZLOB.CHK, HTML_WUKE.AF, WORM_SILLYFDC variants
China	PE_VIRUT.A, TSPY_FRETHOG, TSPY_ONLINEG, TSPY_QQPASS variants
Japan	Several WORM_NUWAR.CQ variants, PE_VIRUT.K, TSPY_LINEAGE
European, Middle East and Africa	Several WORM_NUWAR and TROJ_SMALL variants
Latin America	WORM_RONTKBR.GEN, several TSPY_BANCOS, TSPY_BANPAES, TSPY_BANKER variants
North America	WORM_BRONTOK.HS, EXPL_ANICMOO.GEN, WORM_NUWAR variants

Data collected through Trend Micro customer submission portals

Generic, low-threat Trojans may plague worldwide computers, and the presence of WORM_NUWAR variants in almost all regions signify a broader attack (see section



entitled *Distributed Threats*), but looking closely at malware submissions reveals the prevalence of certain threats in target regions.

In the above chart, Latin America is a favorite target for the spyware families TSPY_BANCOS and TSPY_BANKER. Variants from these families are notorious for displaying Web pages purporting to be legitimate login consoles of Brazilian and other Latin American banks. Users who fall for the ruse inadvertently give away their account information and ultimately their financial assets to the makers of these codes.

By contrast, Chinese users have several spyware variants targeting the active Massive Multiplayer Online Role-Playing (MMORPG) community and the wide user base of *QQ Messenger*, a popular instant messaging application in China.

Social Engineering Techniques

High-impact threats also include those that target a pre-defined set of victims, such as interest groups, local or regional audience, or certain segments of society. Malware authors are becoming extremely adept at crafting strategies in a manner timely enough to convince users of the authenticity of whatever is being offered. The following is a sample of some real-world events that were used in a variety of attacks during 2007:

Real-life Event	Malware Detection Name	Date of Detection
Saddam Execution	TROJ_BANLOAD.BLK	January 7, 2007
Kyrrill Storm	TROJ_SMALL.EDW	January 17, 2007
Vista Release	WORM_SOHANAD.U	February 1, 2007
Superbowl	JS_DLOADER.KQZ	February 3, 2007
Valentine's Day	WORM_NUWAR.AAI	February 14, 2007
Release of IE7	PE_GRUM.B-O	March 31, 2007
Virginia Tech Massacre	TROJ_BANLOAD.CFU	April 19, 2007
Harry Potter Movie	TROJ_DLOADER.NKY	June 22, 2007
iPhone Release	TROJ_AYFONE.A	July 2, 2007
Harry Potter Book Launch	WORM_HAIRY.A	July 4, 2007
US July 4th	WORM_NUWAR.FU	July 5, 2007
Brazilian Plane Crash	TROJ_BANLOAD.CGL	July 18, 2007
Monster.com Compromise	HTML_IFRAME.GN	August 22, 2007
US Labor Day	WORM_NUWAR.AQK	September 4, 2007
NFL Football Season	WORM_NUWAR.AQN	September 11, 2007
New Japan Prime Minister Appointed	BKDR_DARKMOON.BG	September 28, 2007
Burmese Demonstrations	TROJ_MDROPPER.WI	September 28, 2007
Halloween	WORM_NUWAR.ARI	October 31, 2007

Compromised Pages: Abusing Trust in Legitimate Web Sites

Legitimate Web site hacking increased exponentially during 2007, posing one of the most serious threats since it debunks the age-old safe browsing dictum to "not visit untrusted sites". One of the more notable attacks this year was the "Italian Job", a comprising a huge number of legitimate Italian Web pages found to be laced with hidden IFRAMEs detected as HTML_IFRAME.CU. The final number of affected Web sites was in the thousands. Combined, the number of affected sites plus the



individual number of Web pages in each site that were affected are enormous in number.

The attack was carried out at the beginning of the Italian holidays, when users are expected to pursue more socially-inclined interests beyond work or school. This attack is believed to have been conducted using the MPack toolkit, setting a precedent regarding the effectiveness of such techniques. MPack and one of its contemporaries, IcePack, are discussed in a succeeding section of this report, *The Digital Underground Economy*.

Specific Interest Sites

During the first week of February, the official site of the Miami Dolphins Stadium was found to be compromised and silently hosting a Trojan. Super Bowl season in the United States ensured a spike in the Web site's traffic which the hackers were banking on for the success of this drive-by download.

Compromised Web pages are starting points in infection chains that redirect users to other URLs which subsequently introduce spyware, keyloggers and other malware onto affected systems. This infection chain forms a strategy that affords malware authors flexibility in terms of payload: one day the malicious URL may simply display an advert or an inert image, and the next day the same URL may be hosting a backdoor, or may contain a script to install malware.

Given that many of these compromised Web pages are known, trusted sites or were clean prior to an unknown hacking incident, even wary users are bound to get infected without their knowledge.

Abused High-Level Domains

Another trend that was particularly evident this year are the abuse of sites under .GOV domains. The Nigerian Economic and Financial Crime Commission Web site was found to be hacked in June. At around the same time, pages on .GOV domains like the Tulare superior court Web site and Madera.courts.ca.gov sites were found to be abused by search engine optimization (SEO) spammers. SEO spammers rig search engine results by seeding search terms into Web sites so they outrank the legitimate ones whenever a user keys in predictable search terms.

The Arizona Government University site and a California county Web site were also injected with codes that either led to pornographic Web sites or to download other malware. The same thing was seen happening on certain Asian government sites and to a Chinese security site in the same month. Well into November, a Ukrainian government site was hacked to display advertisements for weight loss products.



The increase in number of hacked sites on .GOV domains this year points to an abuse of the perceived trust in pages under .GOV and the persisting indifference by site owners to protect their sites from possible infiltration.

Another way to abuse the trustworthiness of .GOV or .EDU domains is through the use of hacked name server settings. By adding malicious subdomains to the legitimate name server of a .GOV or .EDU domain, malware authors have effectively tricked users into believing that the URL is legitimate. In 2007, there was an increase in instances of compromised DNS settings of several .EDU and .GOV sites. Threat researchers were even able to identify SEO spammers making the switch from free domain names to hacked .EDU and .GOV domains exclusively.

Attacks against Online Entities

As more and more businesses conduct their core activities online, the challenge and opportunity for malware authors have become very tempting. *Monster.com*, *eBay*, and *America Online* all suffered data compromise one way or another. A spyware detected as TSPY_MAMAW.A connects to Web pages related to *Monster.com* in order to steal information like email addresses. This was not the first time *Monster.com* was attacked: in October a phishing page mimicking its legitimate login console was discovered, and in November the site was hacked to host *Neosploit*, an exploit kit. TSPY_EBBOT.A, on the other hand, works as a distributed brute force attack on *eBay*. It accesses certain URLs to retrieve combinations of user names and passwords that could have been gathered from phishing Web sites.

Data Leakage: Human Beings are Still the Weakest Link

According to the Ponemon Institute, 78 percent of data breaches come from authorized insiders of an organization. Loss of proprietary information and intellectual property can trigger fines, litigation, brand damage, and bad press.

Conventional security solutions don't adequately address the rising threat from internal users. Because they have access to data assets, insiders are a major channel for information leaks, whether through deliberate policy breaches or accidental data loss (such as losing a mobile device containing personal records). To protect sensitive data, enterprises need an effective data leak prevention (DLP) solution that monitors potential information leaks at the point of use.

Other Targeted Attacks

- The TROJ_YABE family targeted Germany and other German-speaking regions and other Nordic countries in Europe.
- The TSPY_LDPINCH family initially garnered infections in Russia.
- TROJ_BANLOAD.BLK spammed email in Portuguese.
- TROJ_VB.BLV retrieved a target system's time zone and keyboard layout settings to determine if the system is located in Estonia, Lithuania, or Latvia.
- WORM_SILLY.CQ downloaded several malicious files and installed *Chinese Navigation 2.6.0.0*, a popular search toolbar in China.
- WORM_WALLA.B first determined if the language used by the system is Arabic or Persian before continuing its routines.
- TSPY_ONLINEG appeared to bank on the healthy online gaming community in Asia, particularly in China.



However, the explosion of messaging systems, wireless networking, and USB storage devices has made the protection of critical enterprise data difficult. As a result, enterprises are experiencing an increase in the loss or theft of data assets by employees or contractors who accidentally or maliciously leak data.

The major threat sources facing companies today include:

<u>Insiders</u>	Employees, contractors often with legitimate access to sensitive data, who intentionally or accidentally leak data
<u>External hackers</u>	People who break into corporate network or systems, or physically enter premises to steal data
<u>Outsiders: thieves</u>	People stealing laptops, USB drives or purchasing stolen property containing sensitive data for exploitation or financial gain
<u>Malware</u>	Malicious software that, after infecting a system, will send sensitive data outside the security boundaries of the company

Never before has the threat to corporate data assets been so great—and so costly. According to Attrition.org, an industry monitoring organization, in calendar year 2007, more than 162 million records such as credit cards and Social Security numbers were compromised through December 21. By contrast, Attrition.org reported that 49 million records had been compromised in the previous year. Additionally, the Identity Theft Resource Center lists more than 79 million records compromised in the U.S. through December 18, 2007. That’s nearly a fourfold increase from the 20 million records reported as compromised in 2006.

Prominent Data Leaks in 2007

Below are a few examples of the types of breaches that are occurring and were reported during 2007.

Boeing Breach

“Police reported [of a Boeing employee stealing data] finding a thumb drive that was connected to his computer terminal via a USB cord that ran along the back of the terminal to the storage device that was ‘hidden in a drawer’ in his desk.” Information Week, 7/11/07. Clearly, with the proliferation of removable storage devices and mobile systems, it is becoming more difficult to prevent the leak of sensitive data.

Fidelity NIS Theft

“To avoid detection, [an administrator committing data theft] appears to have downloaded the data to a storage device rather than transmit it electronically.” CSO Magazine, 7/03/07. This theft, at Certegy Check Services, a subsidiary of Fidelity National Information Services, illustrates how employees are becoming increasingly sophisticated in their attempts to steal data. In this case, the administrator assumed that the company had email and network filtering solutions in place, and sought other means to get data out.

UK Government Breach

CDs containing the confidential personal details of 25 million child benefit HM Revenue & Customs (HMRC). The records contain the names, addresses, Insurance numbers of the entire HMRC child benefit database, which also



details of more than seven million parents, guardians and care givers.
ComputerworldUK, 11/20/07.

A study this year by Cisco and the National Cyber Security Alliance reveals that business users in general still do not consider security issues when using mobile devices. With the focus on getting more work done on the go, organizations or companies such as Marks & Spencer, the NHS, Nationwide Building Society, the Metropolitan Police, and the US Department of Veterans Affairs have become some of the high-profile victims of data theft as a result of stolen or lost laptops.

USBs or thumb drives were also found to either introduce malware to a network or to steal data quickly and efficiently within corporate walls, or to get misplaced so easily, compromising confidential business data that may reside in them. These trends do not mitigate the fact that malicious users are zooming in on corporate data, and increased attacks that target corporation data underscore data encryption as the locked-down safeguard against the possible use of stolen information.

Prognosis for 2008: It's only going to get worse

The inability of security organizations to deal with the insider threat, combined with the lack of education and awareness of employees about company policies for protecting sensitive data, means that this problem is only going to get worse before it gets better.

Overall, high-impact threats this year were characterized by an abuse of trust, and a preference for localized targets.

In Summary

1. As metadata becomes the new boone of the information age, so to is the theft of raw and unfiltered data its bane. Criminals now employ combinations of social engineering, malware, insider information, and the latest technologies by any means to grab a foothold through stolen credentials and exploit initial access to its full potential by staying under the radar until a bigger target has been achieved. Encryption and a means to vet access to data in transit will surely become a focus moving forward.

2. IDG reports mention that in 2007 the top concern of companies was the inadvertent exposure of proprietary or confidential information. Whether intentional or accidental some of the main avenues ranked misuse of corporate email, malware, use of public webmail, media lost in transit, and device theft. This concern is well founded given all the recent news as well as the fact that many data protection policies in place today have not taken into consideration the dropping prices of storage media and that many devices like mp3 players and mobile phones often found in offices are now capable of voluminous data storage.

Process-Based Threats

Process-based threats refer to threats that are in the form of an executable application that is run on affected computers. These individual pieces of code may or



may not be part of a multi-component attack but they, in general, perform harmful activities on computer systems.

Malware Type Statistics

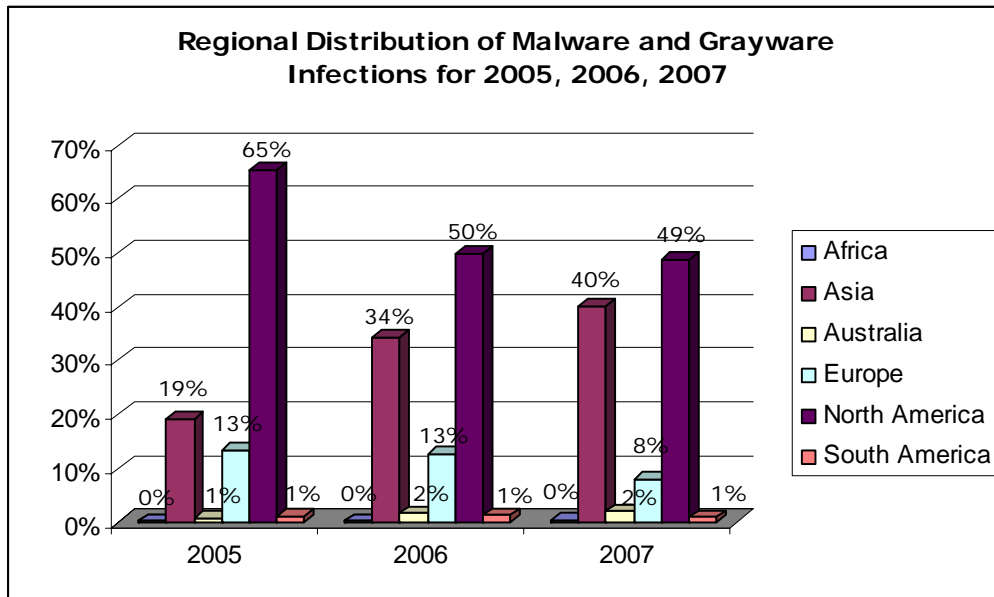
Rank	Top 10 Detections for 2007	
1	WORM_SPYBOT.IS	595,402
2	WORM_GAOBOT.DF	567,895
3	PE_LUDER.CH	539,788
4	TROJ_AGENT.ACSF	414,595
5	PE_PARITE.A	413,880
6	HTML_IFRAME.KQ	287,724
7	WORM_NETSKY.P	283,340
8	EXPL_ANICMOO.GEN	280,532
9	EXPL_WMF.GEN	248,826
10	WORM_NYXEM.E	245,449

The following statistics pertain to 2007 malware trends. As can be seen in the top 10 detections for 2007, two worms make their way to top 2, despite being out of the charts all of the year. Most of these threats have been around for some time, in fact some even as old as from 2004. Since bots are typically used for sending spam, so bot herders could be mobilizing botnets for intensive spamming activities in the coming months. Since these detections are relatively old, they could be taking advantage of newly purchased computer units that join networks without first applying appropriate patches. The

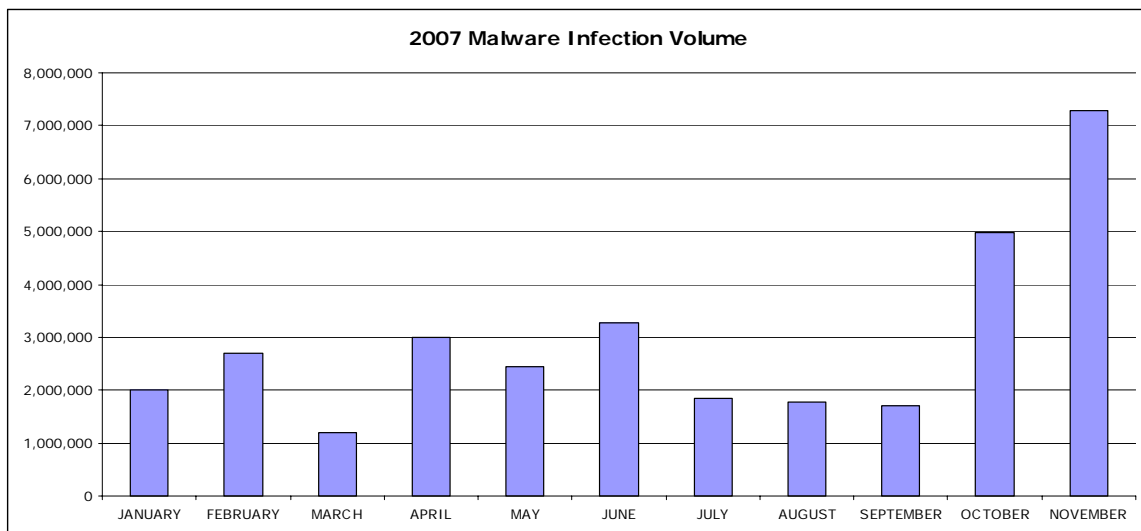
same reason is probably true for the reemergence of EXPL_WMF.GEN, a yearend (2005) exploit. This demonstrates the persistence of vulnerabilities and the importance of regularly checking for software updates.

PE_LUDER.CH spreads via physical and removable drives with infections prominent in the APAC region, as reports point to USB-borne infections in school campuses. The relative ease by which thumb drives are passed onto one person to the next (and one computer to the next) make them ideal infection vectors for malware writers who perhaps intend to ensure the physical proximity of its successful infections.

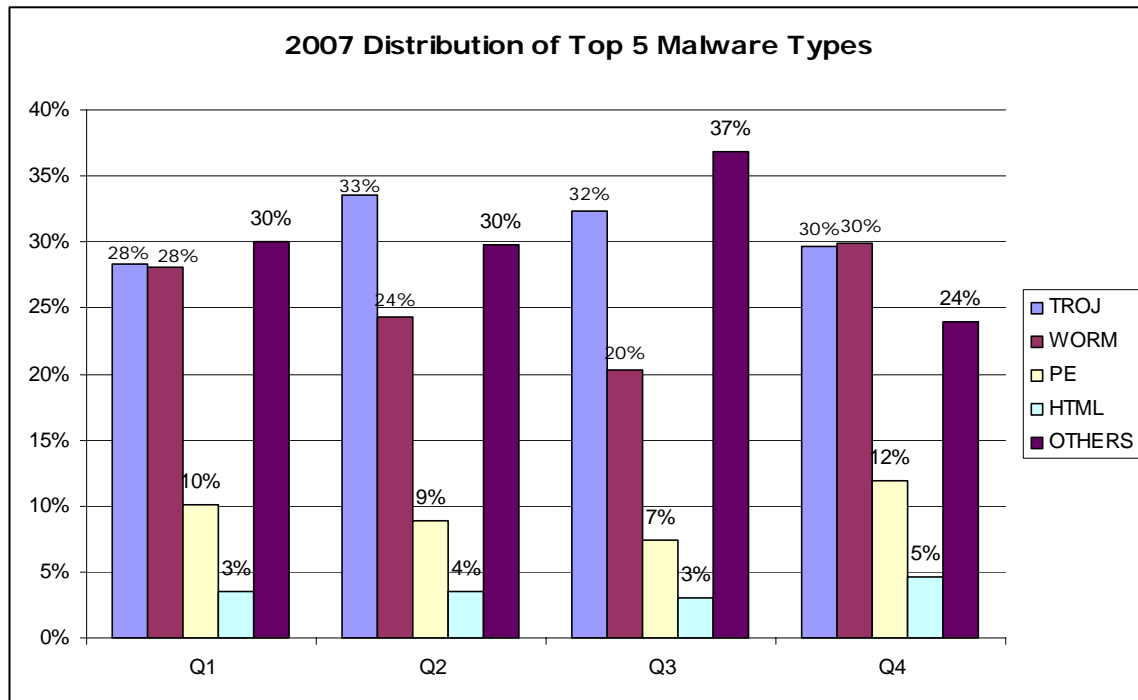
As to regional distribution of malware and grayware infections, the yearly trending shows that Asia is grabbing more and more of the infection pie from North America. Half of the world's infections are still from North America, while Australia and South America remain somewhat consistent in terms of volume, with Europe's number of infections decreasing by 5% relative to other regions this year. This could be due to the prevalence of several Asia-specific malware such as online game info stealers, worms, and the persistence of the .ANI exploit (EXPL_ANICMOO.GEN) for a large part of 2007.



A noticeable trend this year is the sudden spike in infection volumes from September, which more than triples by October and still increases by the first three weeks of November. The worms in the top 20 chart as seen above contribute to this sudden surge and may signify malware authors taking advantage of the holiday seasons as an opportunity to either send spam or deploy spyware as some users may opt to shop online.



As seen below, the most prominent malware types this year are worms and Trojans. More users, however, have had their computers infected by Trojans than any other malware type. The individual malware codes are more often than not part of another malware's routine either as a dropper, a dropped component, a downloader or a downloaded component, a redirector leading users to where other malware are hosted, or hosted on remote sites for access by other malware.



2007 Distribution of malware types with biggest share of infections

Despite the multi-component nature of attacks the past couple of years, there are still identifiable attempts at deploying individual programs that do much damage on their own. Among the most notable is PE_EXPIRO.A which steals credit card information by displaying a fake error message that convinces users to input sensitive account information. TROJ_KILLAV.GG modifies certain functions in Windows which may render affected systems unusable. TSPY_MSTEAL.A displays a fake login screen resembling the login page of *MSN Messenger*, while TSPY_SPEYK.A attempts to do the same for Skype, a popular instant messaging and Voice-over-Internet Protocol application. TROJ_CAPTCHAR.A, on the other hand, poses as a game enticing the user to enter the correct CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) code as displayed by showing a progressively disrobing woman.

The use of fake codecs, as observed last year, continued to plague users this year. TROJ_ZLOB family consistently uses this strategy by preying on users' belief that the installation of a certain codec is required and is to be expected in order to watch online videos. Remarkably, in 2007, ZLOB malware have also begun targeting even Apple users, proving that even alternative operating systems are not safe havens for the online user.

Web Threats

Another way to analyze Web threats is as the software of individual malware and adware enterprises. At one end of a spectrum these enterprises are fully-incorporated, publicly-disclosed corporations. These include enterprises such as



Integrated Search Technologies and Zango. The other end of the spectrum is populated by murkier enterprises loosely confederated under banners such as CoolWebSearch and the Russian Business Network (RBN).

	Web Threat Family	% PCs infected	% all infections	% all detected variants	# variants identified
1	Fun Web Products	33.0%	9.7%	0.2%	35
2	A Better Internet	22.0%	6.5%	0.2%	33
3	Zango	9.2%	2.7%	2.4%	356
4	BYTEVER family of scripts	7.6%	2.2%	0.3%	47
5	Hotbar	6.8%	2.0%	0.6%	92
6	Winfixer	6.1%	1.8%	0.4%	52
7	Drivercleaner	6.0%	1.8%	0.1%	8
8	WhenU	5.4%	1.6%	0.3%	45
9	DLOAD Trojans	5.2%	1.5%	4.8%	726
10	New.net	4.9%	1.4%	0.1%	17
11	Zlob	4.8%	1.4%	0.4%	68
12	IBIS	4.6%	1.3%	0.3%	39
13	Purity Scan	4.1%	1.2%	0.7%	105
14	Softomate	3.8%	1.1%	0.4%	56
15	VIRTUMUNDO	3.5%	1.0%	0.9%	141
16	CDT	3.3%	1.0%	0.4%	65
17	Claria/Gain	2.8%	0.8%	0.4%	61
18	IST	2.7%	0.8%	0.8%	119
19	Comet Systems	2.0%	0.6%	0.3%	41
20	Starware	1.9%	0.6%	0.01%	2

Web threat families are groupings of individual Web threats and variants that serve the same malware enterprises. With multiple pieces of software on individual PCs, the more relevant threat metric is the percent of PCs infected rather than counting up all the software pieces as individual infections or variants.

What emerges from the above table is another view of the Web threat economy. *Fun Web Products* is a family best known for their “Smiley Central” banner advertisements which actually install toolbars like *MyWay* and *MySearch*. *A Better Internet* (also known as *Direct Revenue*) has a history of illicit installations of their adware by using exploits, worms, and various forms of social engineering.

Rogue Anti-Spyware

With the introduction and popularity of anti-spyware applications over the last five years, a specific threat group has emerged under the label “rogue antispyware”. Its modus operandi begins by serving up advertisements on user browsers informing the user that the system is infected by some malware. The user is then enticed to purchase an application in order to remove the non-existent infection.



Individual rogue anti-spyware applications have proven to be durable digital threats. Comparing the top 10 rogue applications from the beginning and end of a six-month period shows that 8 out of 10 remained in the top 10 throughout the same period (see table below).

Rogue Anti-Spyware			Rogue Anti-Spyware		
2006-Q3			2007-Q1		
Rank	Threat name	%PCs	rank	threat name	%PCs
1	Zlob Trojan	8.2%	1	Zlob Trojan	8.6%
2	Winfixer	3.2%	2	Drivercleaner	5.7%
3	Adclicker	1.8%	3	Winfixer	5.6%
4	Spywarestormer	1.3%	4	Renos Trojan	1.7%
5	SpywareQuake	1.3%	5	Spywarestormer	1.2%
6	Renos Trojan	1.2%	6	Adclicker	0.9%
7	ErrorGuard	1.0%	7	ErrorGuard	0.6%
8	ErrorSafe	0.8%	8	ErrorSafe	0.5%
9	SpySheriff	0.5%	9	SpySheriff	0.5%
10	SpywareNO	0.5%	10	SystemDoctor	0.4%

Top rogue anti-spyware programs measured as portion of computers infected. Eight of ten threats remain in the top 10 for six months.

Just recently, readers of the *Boston Herald* Web site were confronted with a JavaScript alert that was actually a component of a rogue antispyware. There have also been several Shockwave advertisements that pointed to scripts redirecting to rogue antispyware sites.

In Summary

1. In general there are more people online now than ever. In the past 5-years many parts of Asia have started to compete with North America and Europe in terms of online presence. Apparently this high volume also equates to a larger target audience where malware in general can proliferate given the varied degrees of online security education.
2. As already mentioned, the volume of tracked threats in the past 2-years has already surpassed the 1500% mark. Not many of these threats are new but are simple rehashed versions of already pre-existing threats. The main movers are malware threats related to the creation of botnets and the combination of exploits to further this end.
3. A large portion of threats center on tracking user preferences for further aggressive marketing strategies by adware, and the other side of the coin is rogue security products that claim to be solutions but in fact are snake oil tactics to directly steal user information in phishing scams.



Content-based Threats

Content-based threats are delivered to the target victim as part of content, such as phishing or spam.

Motivated by financial gain, spammers are willing to invest considerable resources into optimizing spam. This creates an on-going adversarial relationship between the spammer and anti-spam vendor. As spammers create new spam techniques, anti-spam vendors create technologies to block them—both sides creating more sophisticated responses as the process evolves.

Spam continued to develop throughout 2007, changing in the spam message, its delivery methods, and in the backend systems as well as continued blending with other types of threats and protocols. All of these changes enabled an increase in spam, which now comprises at least 90% of all email. This spam report provides an overview of spam trends in 2007 and predictions for 2008.

1. Spam Messages in 2007

Spammers face the challenge of creating a spam message that is persuasive to the recipient while creating spam content that is able to fool spam filters. And this is a never-ending process—spammers must continue to develop new techniques as spam filters adapt and block current spam attacks. This section highlights how spam outbreaks changed throughout 2007.

1.1 Image Spam

Image spam displays the spam message in an image embedded in the email. This is not a new spam technique. However, in late 2006, spammers started sending more image spam as they realized that this approach made it more difficult for spam filters to identify the spam content. Image spam increased during the first part of 2007, reaching 40 percent of all spam sent. During this time, spam filters adapted and became more effective at blocking image spam. As a result, by mid-2007 image spam declined. In June 2007, image spam represented less than 6 percent of spam and dwindled to less than 2 percent by the end of the year.

1.2 Attachment Spam

As image spam lost its effectiveness, spammers turned to attachment spam in another attempt to conceal the spam message from filters. In June 2007, experimental German PDF spam appeared and by the end of that month, PDF spam had flooded the Internet. PDF spam peaked in mid-August, making up 18 percent of spam. However, it quickly faded as spam filters adapted, decreasing to almost 0 percent by the end of August. Spammers then cycled through numerous attachment types for the remainder of the year, including FDF, ZIP, XLS, RTF, DOC and even MP3 files that played the spam message in an audio file instead of in text or as an image.



Figure 1: PDF Spam for 2nd Half of 2007

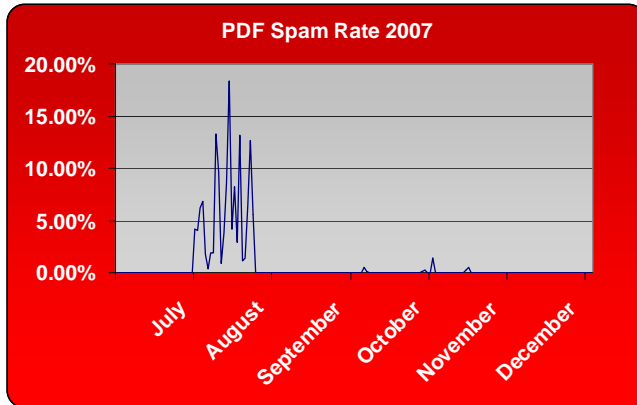
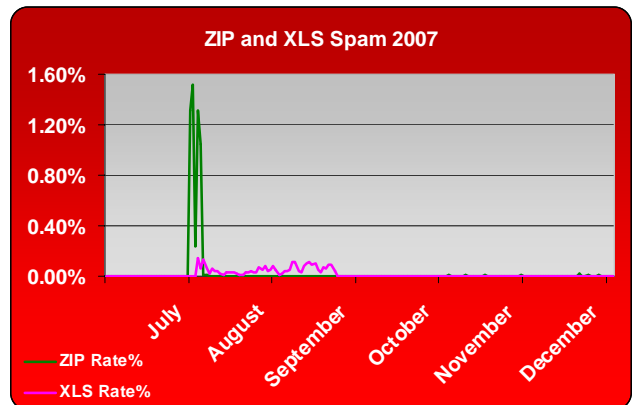


Figure 2: Other Attachment Spam 2nd Half 2007



As seen in Figure 1, attachment spam was a considerable source of spam in July and August but decreased in prevalence for remainder of the year. Although sent out in smaller numbers than PDF spam, ZIP and XLS file spam were sent out in significant amounts. Many attachment spam attacks appear to have been experiments, sending out spam attacks using a specific attachment type, but for very short periods of time. Spammers were most likely attempting to find the most effective spam methods. The ZIP spam shown in Figure 2 may depict this type of attempt.

1.3 Embedded Links in Spam

Spam must contain a call to action. Often this is an embedded link that brings the recipient to a Web site. Spam filters can assign a reputation to URLs in links and can use this reputation to identify and block spam messages. Therefore, spammers have made efforts to conceal or bypass the use of URLs. For example, in January 2007, a spam attack used stars in the URL to avoid detection. The email read, "http://www.printeryml*.com (Important! Remove '*' to make the link working)." This was not a very sophisticated approach but may have had limited success until spam filters adapted to block this technique.

Spammers are also placing URLs in very simple text messages. With limited spam content, it is more difficult to identify the email as spam and assign a reputation to the embedded URL. Spammers do not use the text to communicate their message, but hope the recipients will follow the link to a Web site. Throughout 2007, unsolicited email messages that contain links which download malware continued to rise.

In 2007, spammers relied heavily on "pump and dump" spam. These emails do not contain a URL, but, instead, promote the purchase of a penny stock. The spammer buys cheap stock and then pitches the stock in spam. Many recipients buy the stock and drive up the value, giving the spammer a profit. Pump and dump scams were sent in many types of spam, such as image and attachment spam, including even MP3 files. However, spammers often sent pump and dump spam as just a simple text message, using a variety of punctuation tricks to conceal the stock symbol and other content.



Spammers are continuing to use a range of tricks in attempts to “piggy back” on the good reputation of legitimate domains. An example of this is a URL trick which exploited the “I’m Feeling Lucky” button. Instead of receiving a list of search results, the browser will open the Web page for the most relevant search result. As part of this process, Google creates an “I’m Feeling Lucky” URL that brings users to the Web page. This unique URL occurs behind the scenes and goes unnoticed by the user. However, some spammers discovered how to construct these “I’m Feeling Lucky” URLs and used them to direct users to their spam sites or malicious Web pages. These URLs were embedded in spam emails. Technically the URL took the user through Google to get to the Web page. This trick helped to defeat Web reputation services, because Google is not a spam site.

Spammers are also cycling through domains more quickly, making it more difficult for spam filters to acquire and apply timely URL reputations. In 2003-2004, spammers would maintain spam Web sites for a few days to a week. This time has continued to decrease with some sites now being hosted for less than a day, sometimes for as little as a couple of hours.

1.4 International Spam

As an international company with a global network of research centers, Trend Micro tracked spam in 38 specific languages throughout 2007. The majority of spam was still in English (an average of 73 percent), but non-English spam grew and diversified significantly. After English, the top 2 languages are Japanese and Chinese, both averaging around 10 percent of spam with relatively even spam distribution throughout the year with a small decline at the end. Combined, Japanese and Chinese spam comprise about one fifth of the world’s spam. Organizations, particularly global companies, must have an anti-spam filter that can block spam in double-byte characters and be able to specifically identify Japanese and Chinese spam. See Figure 3 below, which shows the spam rates for the top 3 spam languages in 2007.

All other languages each comprised less than 1 percent of worldwide spam in 2007, collectively making up almost 8 percent of spam. Although seemingly small, the vast amounts of spam make even these low percentages a significant quantity. Figure 4 below shows the percentages for the next top 4 spam languages: Spanish, German, Portuguese, and Russian. Each contributed over 0.35 percent of spam on average. There was a dramatic increase in German email in May and both German and Portuguese rose significantly at the end of the year, while Russian declined steadily throughout 2007.

Figure 3: Top 3 Spam Languages

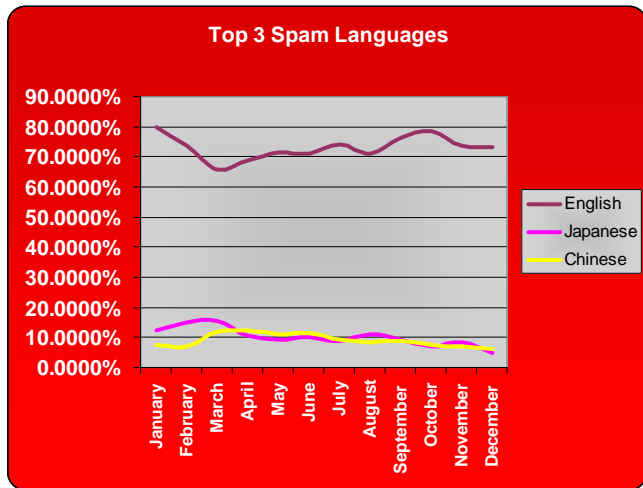
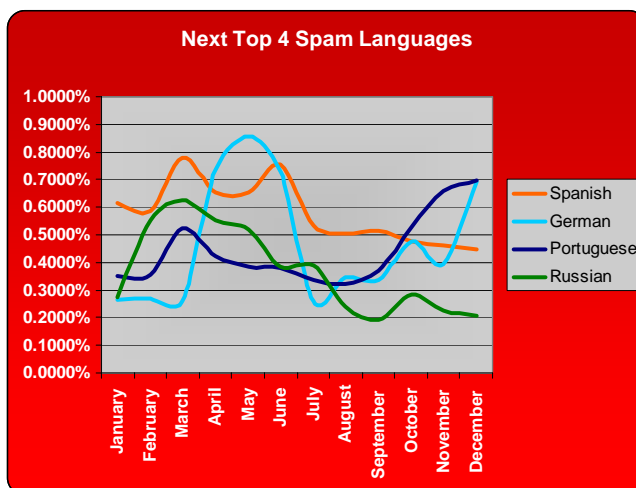


Figure 4: Next Top 4 Spam Languages (Ranked 4-7)



As spam increased during 2007, most spam was in English. However, there was also a steady increase of non-English spam as well (see Figure 5 below). For some languages there was a dramatic spike once or twice in the year (e.g. Catalan, Czech, Indonesian, Latvian, Lithuanian, Norwegian, Slovak, and Slovenian). This may represent an experiment by spammers to determine additional languages in which spam may be effective.

Figure 5: 2007 English and Non-English Spam Trends

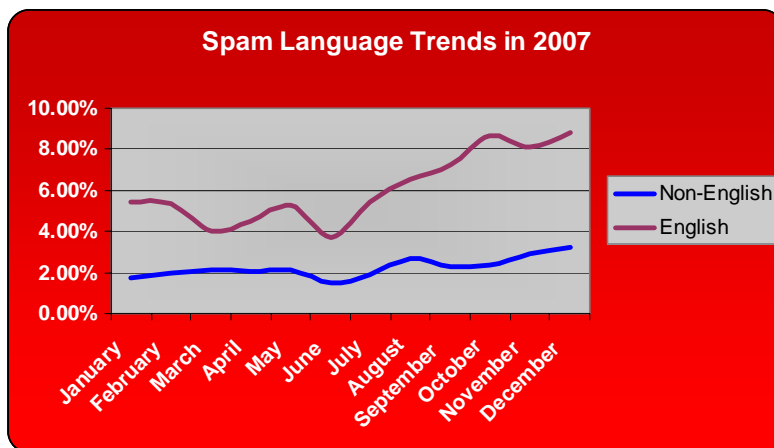




Table 1: Noteworthy 2007 Spam Attacks—Significant in Volume or Approach

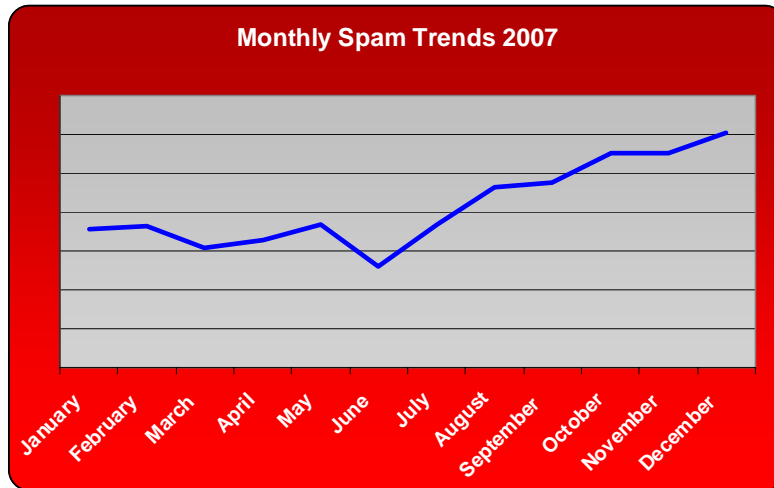
Month	Description of Attack
Jan	Star in URLs to avoid identification
Feb	Pump and Dump Spam - plain text (moving away from image spam)
Mar	Pump and Dump Spam - plain text attacks continuing
Apr	Nuwar Worm - image spam with malware DHA Spam - only small text string in body
Jun	German Pump and Dump German PDF Spam – experiments
Jul	Flood of PDF Spam on Internet Pump and Dump – plain text Excel (XLS) Spam
Aug	Pump and Dump - text crossed out to confound filters FDF Spam - a variant of PDF spam Greeting Card Spam - links to a Web site with malware RTF Spam Invisible Ink Spam Skype Spam
Sep	Word Doc Spam Pump and Dump - punctuation tricks to obscure content You Tube Spam I Feel Lucky Spam - abuses Google “I feel lucky” search
Oct	MP3 Spam PDF Spam with Malware US Election Spam
Nov	Money Mule Spam
Dec	HTML Insert Spam - salad words hidden in style and other tags Chinese Excel Spam DHA Spam - content consists of word salad

1.5 Spam Growth

Not only has spam increased in volume, it has also increased in size. The prevalence of new spam techniques, such as image and attachment spam, has increased the average size of spam email. And with spam comprising over 90 percent of all email, overall email quantities and size are bogging down messaging infrastructures, significantly impacted networks.

The increase in spam size and quantity has added administration, bandwidth, and storage requirements, increasing management and costs. It is no longer sufficient for businesses to block spam from the inbox; they must block the majority of spam before it even enters the network to preserve costly resources. This need makes reputation services a critical component of anti-spam solutions, blocking spam before it even enters the gateway based on the reputation of the sender.

Figure 6: Monthly Spam Trends for 2007



2. Spam Delivery in 2007

Most industry-leading spam filters were able to maintain an effectiveness rate in the high 90s throughout 2007. Spammers had to send considerable volumes of spam to bypass these filters in quantities that achieved a desired profit. Spammers have made considerable investments in creating and maintaining spam delivery mechanisms that maximize the amount of spam sent.

Spammers also want delivery methods that obscure the sender. Although spam is not necessarily an illegal activity, it is often paired with fraud and other malicious activities. Obscuring the sender also helps confound reputation services which block spam based on the reputation of the sender.

In 2007, spammers relied on a delivery approach that increases both spam sending resources and stealth—the botnet. Bot code is malware that, once downloaded, allows hackers to hijack the computers for their own purposes unbeknownst to the owner. These computers are called zombies or bots and when used in conjunction, are called a botnet. Bot code is downloaded using the same methods as other malware, mainly through the Web and email attachments. Many variants of bot code were sent in 2007, including Nuwar (popularly known as Storm) and Stration.

Botnets can be used for numerous purposes, but one of their main uses is sending spam and other email threats. Botnets became more prevalent throughout 2007 and are now responsible for sending over 90 percent of all spam. Botnets are also used to host the malicious Web sites to which spam emails are linked.

The largest botnet in 2007 was the Storm Worm Botnet. It started early in 2007 and continued to grow throughout the year, linking millions of computers. The giant Storm Worm botnet was broken into segments, or smaller networks. Some Storm Worm variants used a 40-byte key to encrypt traffic over the peer-to-peer (P2P) protocol. Using encryption means that communication is only possible between botnet nodes that are using the same key. These separate nodes with different encryption key access enable the Storm worm creators to sell the botnet nodes to



other malicious users (e.g. spammers or DDoS attackers). Further analysis of Storm and other Botnets can be found in a later section of this report, entitled "Botnets"

Spammers use botnets to obscure the spam source. Botnets usually send spam in short bursts, using free dynamic DNS servers to quickly change machines. Spammers have also started "dribbling" spam from individual bots. Unusually high email volumes help to identify spam sources. Quickly changing servers and minimizing the amount of spam sent from individual bots helps to hide the source. These approaches attempt to confound reputation services that block known senders of spam and other email threats.

Botnets provide numerous benefits to spammers. They help to hide the spam source, enable higher spam volumes, and use the resources of the infected machines, minimizing risks and costs while maximizing profits.

3. Backend Changes to Spam Systems in 2007

Originally, spammers would simplify sending efforts, using a single command and control center to send emails out in mass. They were not concerned about delivery failures—the sheer quantity of spam sent ensured a sufficient percentage of successful deliveries. However, these simplified sending methods are used by filters as a spam indicator, forcing spammers to augment their spam systems to avoid detection and increase delivery rates. These backend spam system changes go virtually unnoticed by the average spam recipient, but help spammers to defeat particular filtering technologies.

3.1 Decentralization of Botnets

Originally, botnets used one command and control center, which, if found, could bring down the spam botnet. However, botnets, like the Storm Worm Botnet, evolved to use peer-to-peer protocols, eliminating the central command and control center and making it more difficult to dismantle the botnet.

3.2 Use of MTA Features

Previously, spam systems would not resend messages that received a failure notice. Some anti-spam solutions used this to their advantage by applying graylisting. With this technique, every time an email connection is made to the mail server the system records the IP address, sender's email address, and recipient's email address. The first time the system receives a unique combination of these three identifiers, it issues a temporary error asking the sending server to retry. Email from legitimate mail servers will most likely be resent while spam systems previously did not bother to resend the email. If an email with a combination of the same three identifiers is received a second time, it was processed normally.

To evade graylisting and related techniques, spam systems are starting to behave like legitimate Mail Transfer Agents (MTAs). Some are resending spam emails that are temporarily rejected, making graylisting less effective. Spam filters have to apply other techniques to identify these spam emails.

4. Blended Threats and Protocols

4.1 Blending Threats

Spam originally was used to promote legitimate products and services. However, cyber criminals are now using spam techniques for illegal financial gain. Spam is used to send fraudulent emails including phishing, “pump and dump” spam, and other scams. In addition, spam often contains malware, including bot code, programs that harvest directory information, and other malware that helps to perpetrate the spam cycle.

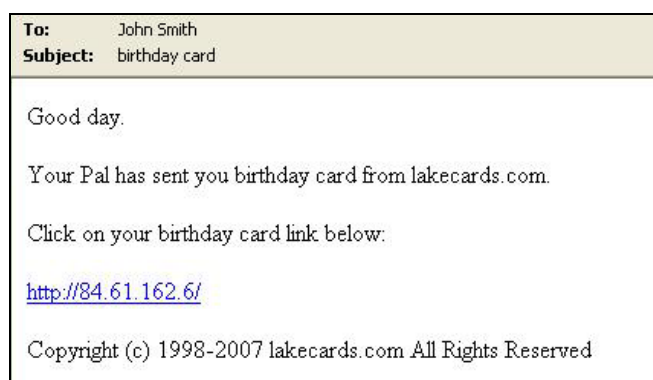
4.2 Crossing Protocols

In addition to blended threats, spam is also crossing protocols. There is an increase in spam on mobile devices as well as on IM. And it is expanding into new forms of communications with spam attacks in 2007 seen on Skype and You Tube. In addition, spam is often the first step in Web threats. Embedded links in spam can take the recipient to dangerous Web sites, such as phishing sites or sites with dangerous downloads.

4.3 Example of Blended Attacks

The e-greeting card spam attacks sent out in 2007 are an excellent example of a blended spam attack that encompasses many of the spam elements discussed in this report. E-greeting card emails were very simple, containing very little text and a URL (using the IP address rather than a domain). The specific spam text varied, but generally these spam told recipients that a friend had sent them an e-greeting card and to follow the link in the email to view the card. Figure 7 below shows an example of one of these emails.

Figure 7: Example of E-greeting Card Spam



The e-greeting card spam used botnets to send the spam and infected recipients' computers with malware if they followed the embedded link, perpetuating the botnet cycle. Not only did the botnets send spam, they were also used to host the malicious Web sites to which the spam emails were linked, using botnets to perpetrate a cross-protocol attack.

Many bot-infected machines were used to host the Web sites, each with its own IP address. A spam template was used to cycle through the available bot IP addresses,



inserting the different links in the spam message as well as varying other text elements. Using the IP address instead of a domain name helped to obscure the link destination, which was a bot-infected server that is otherwise used for legitimate purposes.

The e-greeting card spam blended attacks by using spam techniques for the purpose of downloading malware and crossed protocols by taking the user to a malicious Web site. These attacks also made use of botnets both for sending email and hosting Web sites as well as used URL tricks and spam templates in the backend system to vary the spam message.

Protecting against blended threats and protocols requires a more comprehensive definition of messaging security and an integrated defense.

5. Predictions for 2008

Email will continue to be the primary means of communication in 2008 and it will continue to be abused by spammers and cyber criminals. However, dependence on other types of electronic communications will grow, making these communication vectors more attractive targets for spam and other threats. Spam will increase on mobile phones, IM, Skype, You Tube, and other social networking Web sites.

English will continue to be the primary spam language, but non-English spam will continue to increase and diversify, requiring a global approach to spam filtering.

Spammers will continue to optimize their delivery systems. Botnets will grow in prevalence and the sale of botnet nodes will become more streamlined, possibly becoming a component of automated spam kits. This could lead to rampant botnet infections. And spammers will continue to enhance their backend systems, making spam systems difficult to differentiate from legitimate mail servers.

Web threats will grow and become even more prominent. Web threats are any threat that uses the Web to facilitate cybercrime. Email is often a component of Web threats, delivering emails with links to malicious Web sites or attachments with malware that accesses the Web. In 2008, spam will be used primarily to send users to Web sites, which will deliver the spam message, perpetrate fraud, or conduct dangerous downloads. As a result, spammers will have to create new tricks to conceal URLs. Also, legitimate Web servers will be hijacked and domains cycled through even more quickly to avoid receiving bad Web reputations for embedded links. With the reliance on Web threats, it will become increasingly important to implement security across both email and the Web to achieve comprehensive protection.



Phishers Still after PayPal and eBay

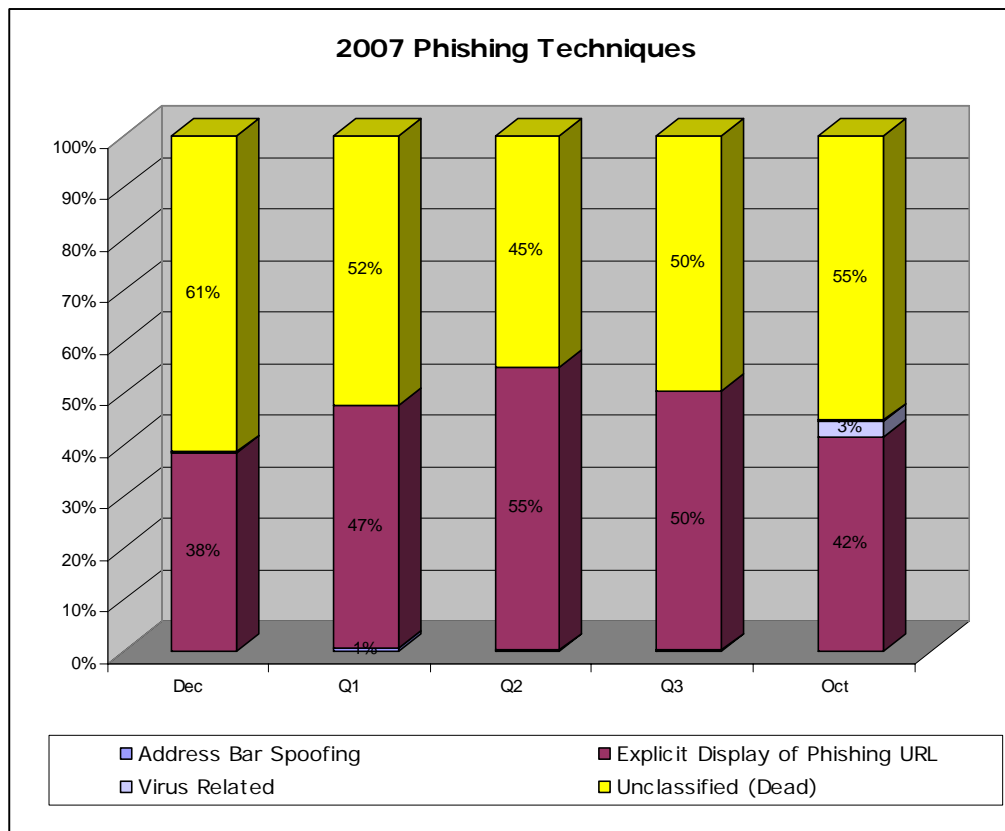
According to Trend Micro's Content Security team, the top 10 companies attacked by phishers are the following:

TOP 10 COMPANIES ATTACKED IN 2007		% of attacks over total	% of attacks over top ten
1	PayPal	7%	24%
2	eBay	6%	23%
3	Bank of America	5%	19%
4	Wachovia	3%	12%
5	BB&T	1%	5%
6	Citizens Bank	1%	4%
7	Fifth Third Bank	1%	4%
8	Poste Italiane	1%	3%
9	Regions Bank	1%	3%
10	Natwest	1%	3%

** Paypal is now part of eBay.*

PayPal and *eBay* are the top online commerce sites attacked by phishers, merely exchanging rankings compared to last year. Phishers also expect to profit from targeting banks, as mostly financial institutions figure next to the top two. Phishing sites for *MySpace* and *Facebook* were not as common but there have indeed been an increase in instances of phishing attacks on social networking sites.

The volume trends of phishing attacks are influenced largely by the available tools for creating phishing sites.



Behind the onslaught of phishing is the increasing popularity of the rock phish technique among fraudsters. Trend Micro Content Security Web Blocking Team estimates rock phish URLs to average anywhere between 20,000 and 60,000 per day. Most of these URLs are hosted on the same IP addresses. The number of rock phish URLs has steadily risen as the year progressed, although overall phishing volume trends followed that of 2006, where September numbers significantly jumped from August.

The group behind rock phish may well be using fast flux to keep phishing sites alive for a longer period. The Anti-Phishing Work Group (APWG) reports in the *eCrime Researchers Summit* that rock phishing contributes to almost half of the attempts recorded. APWG suggests that if this group is really using fast flux, then it is likely that phishing sites will stay up for longer periods to lure more victims.

As if rock phish kits were not enough to help online fraudsters, phishers are now selling a new kit known as *Universal Man-in-the-Middle Phishing Kit*. This new tool helps phishers gather more personal information by allowing potential victims to communicate with a legitimate Web site using a fake URL set up by the phisher. Similar to rock phish kits, universal man-in-the-middle phishing kits provide its users with a Web-based Graphical User Interface (GUI) to create a Web site that resembles the legitimate Web site phishers are targeting. The phisher-created Web site communicates with the legitimate Web site and loads its original Web pages. The potential victim and the legitimate Web site are still communicating, but the phisher conveniently takes all the information provided by the user via the phishing site.



A dangerous strategy that was on the rise in 2007 is the use of DNS-changing techniques. DNS servers are used to reconcile human-readable domain names to IP addresses that connect to other computers servers on the Internet. While most users automatically use the DNS servers of their ISP, DNS-changers modify computers settings to use foreign DNS servers. These servers translate certain domains to other IP addresses that are possibly malicious. For example, users of popular dating sites were found to have the propensity for leaking account information when they are infected with DNS-changing malware. Also, DNS-changers are being used in hard-to-detect click fraud schemes where advertising companies get targeted. In 2007 Trend Micro observed that the DNS Changer botnet has grown substantially.

In Summary:

1. The last 4-years since the CAN-SPAM Act has shown no respite to the existing spam problem. Spammers turned scammers have simply changed the playing field by employing botnets and spam proxy trojans and are using individual user's zombie computers to send these unsolicited emails, an activity that the Act doesn't cover completely.
2. With security vendors recommending for years to vet attachments at the gateway and technologies that attempt to filter spam via keywords, spammers are now using images of the same text and also URLs to trump blockers. Today's current needs therefore require the capability to inspect these links in real-time.
3. There hasn't been any change in the usual targets for phishing and this is just typical of targeting the most successful and largest commercial and banking/finance institutions. The latest twist has been the localization of the language content and the top brands in the area.

Distributed Threats

Botnets

In security industry jargon, bots are malicious programs that report to a central management console and wait to receive commands from it. From the attacker's perspective they are very efficient because as bots spread, the central console gets more populated and is therefore more powerful. Today's botnets can control hundreds of thousands of infected PCs. This puts a lot of computing power and network bandwidth in the hands of criminals. As new computers get infected, the botnet becomes more of a danger.

During 2007, the most popular communication protocol among botnet owners was still IRC -Internet Relay Chat. This is possibly because software to create IRC bots is widely available and easy to implement. However, malicious IRC traffic can be detected relatively easily and that's why attackers have started implementing other internet protocols to control botnets. The focus of botnet owners is to abuse HTTP (the web protocol) and P2P (peer to peer) for these purposes. The reason is that botnet abuse of these protocols is much harder to detect, especially when encryption is used in the data exchange.



P2P protocols can increase the lifespan and redundancy of bots in a botnets significantly. Earlier on, botnets were often controlled by a single central Command and Control (C&C) server. When this C&C server goes down the whole botnet collapses and becomes useless for the bot herder. Introducing P2P communication channels removes this single point of failure. P2P protocols allow the botnet controllers to inject their commands in a number of live nodes of the P2P network. The bots automatically propagate the injected data, while they link up with each other. This adds unprecedented robustness to the whole bot network: These new P2P botnets can work without a central console and to take them down it is necessary to eliminate every single component of the network. This setup is being used in both the Storm and the Spamthru botnets.

The Domain Name System (DNS) is one of the most vulnerable internet protocols, and yet it is essential for the internet to work. During 2007, researchers discovered a proof-of-concept backdoor that uses DNS requests for data communication between botnet controllers and bots. Though this type of data exchange is somewhat obscure and not as efficient as HTTP communication, it does have dangerous applications: it can be used to facilitate information stealing.

In 2008 we expect an increase in the sophistication of botnets. IRCbots will still be used because of their easy access but professional cybercrime gangs with a lot of financial resources will continue to develop the use of other protocols like HTTP and P2P. They will also tend to use strong encryption of malicious data transfer in order to evade detection.

Nuwar: The Storm Continues

The most significant botnet activity this year came from the NUWAR botnet, also known as STORM. Nuwar's nastiest features are its advanced technology, its huge size, aggressive retaliation against anybody who stands in the way and most of all: unprecedented social engineering.

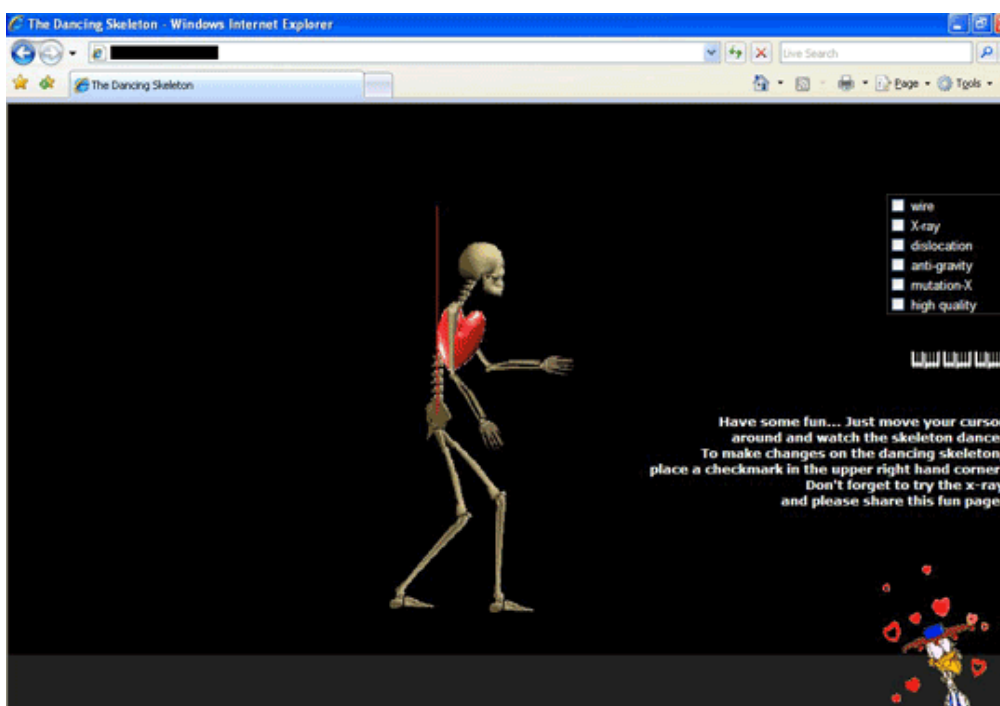
The criminals that created the Nuwar (Storm) botnet have used it to send email spam, to post guestbook spam, to host malicious websites on infected computers and to perform distributed denial of service (DDoS) attacks. Among the DDoS victims were internet security researchers who triggered a possibly automated attack when they started investigating Nuwar. Other victims of these attacks during 2007 included a competing malware gang, often referred to as Stration (Warezov).

The bots in the Nuwar network communicate with each other using a P2P protocol, called Overnet. This means that there is no central Command and Control server that sends instructions to the bots. Instead, instructions propagate through P2P while the bots link up with each other. This technique enhances the redundancy and lifespan of the infected computers.

Nuwar facilitates fast-flux domain hosting and fast-flux DNS. Fast-flux is a Domain Name System technique used by botnets to hide spam, phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as reverse proxies. By using a DNS round-robin technique it is possible to point a domain name to multiple compromised hosts, which can change quickly over time.

Nuwar has enhanced the redundancy and stability of earlier fast-flux botnets. The older types of fast-flux botnets usually fetched web content and DNS data from one central server. Nuwar has already removed this single point of failure: now the bots get the web contents they are supposed to host through P2P traffic.

The Nuwar botnet planted its first seeds late 2006 with doomsday email messages like the death of the United States president. The makers of Nuwar showed their advanced social engineering techniques by consistently taking advantage of recent real-life events, including the Kyrill storm in Central Europe last January, Valentines Day in February, the start of the National Football League season in September, Halloween in October (see below image) and the Christmas season in December.



Other effective lures made use of the interests of young people: a fake, fancy music-sharing program, greeting cards, cute-looking kittens and fear for the RIAA.



KRACKIN V 1.2
The New Global Sharing Network

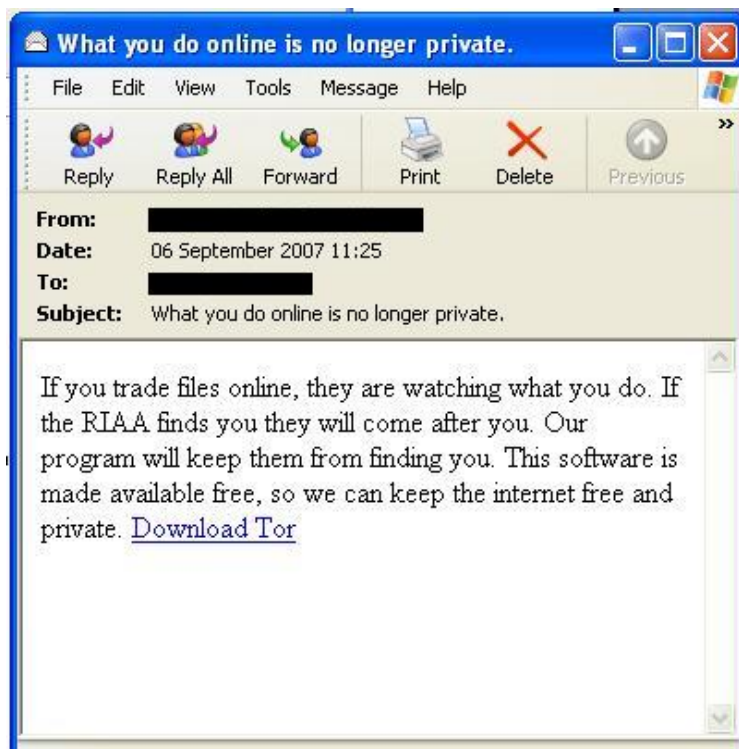
Movies, Music, Blogs, Chatting, Pictures, MP3, Games

1. Search 2. Download 3. Enjoy

- Easy To Install
- Built In Video User Guides
- Automatic Updates
- Auto Search Agent
- 72 Hour Continuous Searching
- IP Blocking To Prevent Tracking
- Favorites Searching
- Auto Virus Scanning
- Adult Content Control
- Multi User Access
- Personalized Interfaces
- Blog and Chat Platforms
- Video Mail
- Away Messaging
- File Conversion
- Multi Source Downloading
- Mobile Access Downloading
- Unwanted User Blocking

➔ **Click Here To Download KRACKIN** ⬅

Nuwar has used various techniques to try to evade detection technologies by arriving as a file contained in a password-protected ZIP or RAR archive, or by using GIF images in the body of the spammed email messages. Since May, Nuwar-infected email messages contained not a copy of the worm but a link to a malicious web page where the malware is hosted.



A study of Nuwar infections shows that 28% of the IP addresses which spammed NUWAR-infected email messages, are from the United States. For a complete geo distribution see figure 1.

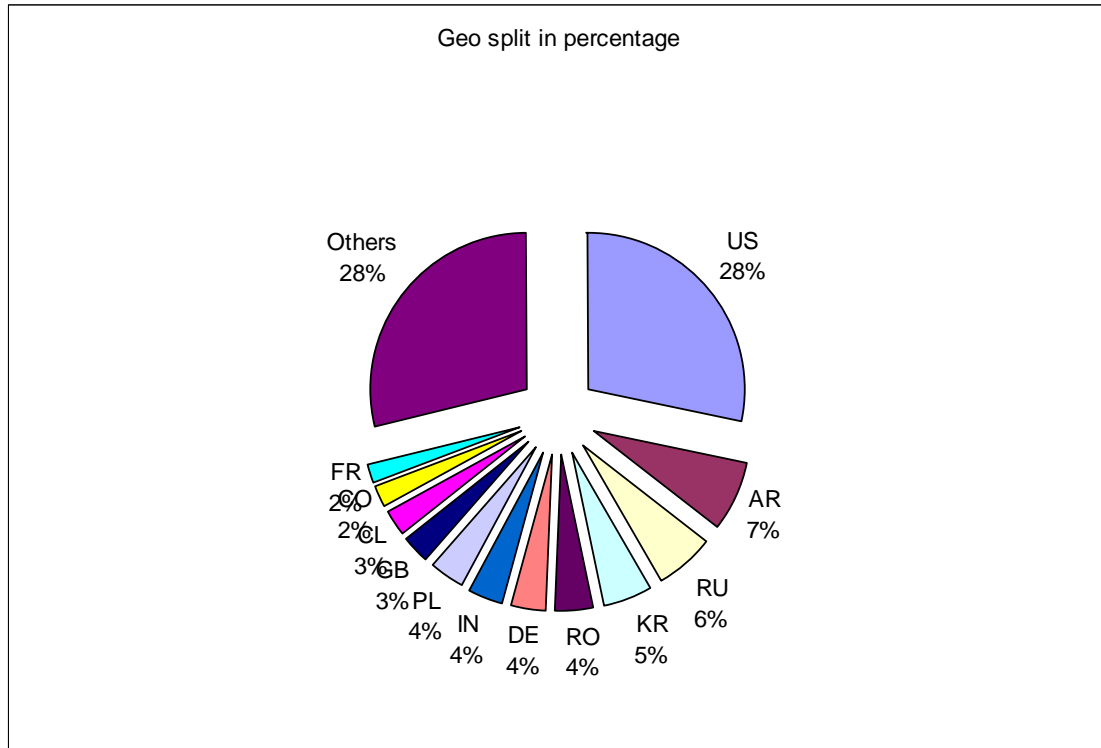


Figure 1: Geo split of Nuwar infected hosts

A significant development in October 2007 was the discovery that the giant botnet split up into segments, each using a different 40-byte key to encrypt traffic over the Overnet peer-to-peer protocol. Encryption means that communication is only possible between botnet nodes that are using the same key. There are several possible reasons for the segmentation. This may be an indication that the Nuwar worm creators are renting the use of the different networks separately. They might even sell them away in malware forums to other malicious parties (spammers or Denial-of-Service attackers).

Key technologies to combat

The impact of the Nuwar botnet in 2007 emphasizes the need to combat abuse of internet protocols that are being used for communication between bots and bot herders. Malicious IRC traffic can be easily detected today but P2P and HTTP traffic is a bigger challenge. In a corporate environment peer to peer traffic should be blocked completely, because it increases the risk of data leakage in any case. For residential internet users malicious P2P traffic can be detected by correlating it with other traffic, like outgoing spam emails. In combination with an up-to-date virus scanner internet users can be protected against these threats. HTTP bot communication can be stopped by blocking traffic to known C & C websites.



The Digital Underground Economy

The security industry is now well-aware of the underground economy that sustains what computer users experience as infections or other forms of online attacks. The profile of malware authors have indeed morphed from the bored teenage hacker to the entrepreneurial cybercriminal.

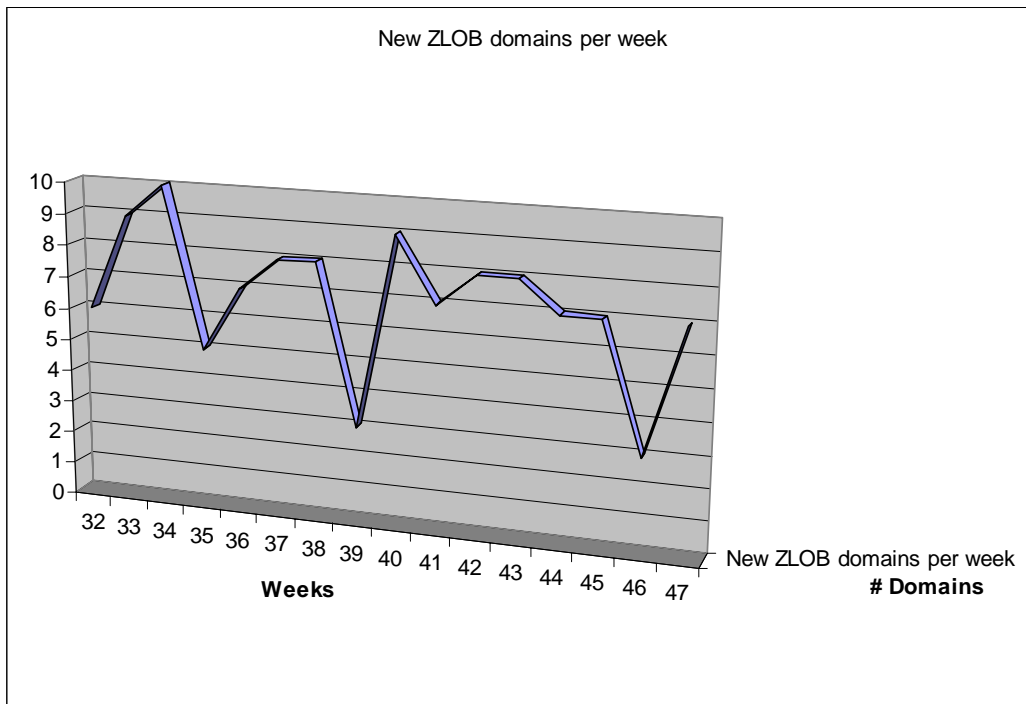
During 2007, new versions of the *MPack* and *IcePack* malware toolkits were released in underground digital forums. These toolkits are commercial-grade software that makes it easier for non-technical people to conduct attacks, allowing them to focus only on the payload or on what exactly the malware is intended to deliver or accomplish. Along with the reported sale of vulnerabilities in underground forums and the incorporation of vulnerabilities in kits as upgrades to bots, evidence of the thriving malware industry is indeed growing into an enterprise that can match the vigor and economic viability of open markets today.

The table below is a sample of the thriving business dynamics of cybercriminals. On one end we can find the sale of exploit kits used in tandem with specific payloads, and at the other end are the 'fruits' of these attacks: batches of stolen account information or unspammed email addresses.

Asset	Going-rate
Pay-out for each unique adware installation	30 cents in the United States, 20 cents in Canada, 10 cents in the UK, 2 cents elsewhere
Malware package, basic version	\$1,000 - \$2,000
Malware package with add-on services	Varying prices starting at \$20
Exploit kit rental – 1 hour	\$0.99 to \$1
Exploit kit rental – 2.5 hours	\$1.60 to \$2
Exploit kit rental – 5 hours	\$4, may vary
Undetected copy of a information-stealing certain Trojan	\$80, may vary
Distributed Denial of Service attack	\$100 per day
10,000 compromised PCs	\$1,000
Stolen bank account credentials	Varying prices starting at \$50
1 million freshly-harvested emails (unverified)	\$8 up, depending on quality

Sample data from research on the underground digital economy in 2007

The following graph shows the number of domains that host malicious code (meaning not the ones that have fake Windows Media player come-ons) for the last weeks of this year. Here it can be seen that malicious authors are creating an average of seven domains per week with an average lifetime of six days per domain. This means that it has become substantially easier for malware authors to find hosting services for their nefarious activities.



In 2006 and 2007, we have seen examples of malware spread by malicious Web sites where each victim gets his own unique version of a Trojan. Some Web sites hosting ZLOB fake codecs, for instance, install a Trojan with a different identifier (also known as the MD5 hash) for each victim. The interesting thing is that cybercriminals can keep the mutation algorithm of the Trojans wholly on the server hosting the malicious files. In contrast to the case of polymorphic viruses, the mutation algorithms do not need to get distributed along with the malware. Thus, the mutation algorithm can remain confidential and it is potentially hard or impossible to write pattern files that cover all malware that are being spread by the malicious Web site. Trend Micro threat researchers expect that polymorphism of malware on the server side will be developed further in 2008.

In Summary:

Distributed Threats and The Digital Underground Economy

1. The overall impact of the Nuwar (Storm) threat in a year of its life-cycle has been the realization of certain facts:
 - Decentralized technologies (P2P and IM) extend the attackers anonymity
 - Law enforcement and legislation across continents are in dire need of standardization in terms of threats in cyberspace/online
 - Economies and employment security are factors in the overall scheme of crime not just in the real world but online
 - Basic user education is still lacking and leaving a gaping hole in whatever current technology available to consumers; yet enterprises with stricter usage policies are more able to appreciate the benefits of content filtering



Summary & Forecast

The trends identified in 2007 closely parallel the predictions made in last year's roundup. 2007 has indeed been about Web threats. Several attacks on online organizations via hacked Web sites, abuse of high-level domains and phishing activities show that attacks are becoming more limited in scope. The expansion and recent activities of the NUWAR botnet has shown us that botnet threats have grown in scope, increasing the risks for potential targets.

In recent years we have seen that prolific malware gangs succeed in getting consistent high-quality Internet connectivity in the US, Asia and Europe for extended periods of time. A clear example is the Russian Business Network (RBN), a hosting company that became infamous in 2007 for hosting the activities of cybercriminals, using fake registrant names to create an infrastructure meant for underground activities. Other examples are the ZLOB gang and the Gromozon gang. In 2008, we expect to see a shift from well-defined no-go areas on the Internet to more distributed locations on the Internet.

Threat Forecast

1. Legacy code used in operating systems and vulnerabilities in popular applications will continue to be attacked in the effort to inject in-process malicious code that criminals can exploit to run malware in efforts to breach computer and network security in the efforts to steal confidential and proprietary information.
2. High profile web sites that run the gamut of social networking, banking/financial, online gaming, search engine, travel, commercial ticketing, local government sectors, news, job, blogging, and e-commerce sites for auction and shopping; will continue to be the most sought after attack vectors by criminals to host links to phishing and identity theft code.
3. Unmanaged devices such as smart phones, mp3 players, digital frames, thumb drives, and gaming stations; will continue to provide opportunities for criminals and malware to infiltrate enterprise's security borders due to their capabilities for storage, computing, and wi-fi functionality. Public access points such as those in coffee shops, bookstores, hotel lobbies, and airports will continue to be distribution points for malware or attack vectors used by malicious entities.
4. Communication services such as email, instant messaging, as well as file sharing will continue to be abused by content threats such as image spam, malicious URLs, and attachments via targeted and localized socially engineered themes due to their effectiveness in luring potential victims as criminals attempt to increase the size of botnets and steal confidential information.
5. Data protection and software security strategies will become standard in the commercial software lifecycle due to the increasing high profile incidents. This will also put a focus on data encryption technologies during storage and transit particularly in the vetting of data access in the information and distribution chain.



Technology Forecast:

The dramatic change in the threat landscape will continue to drive an evolution in the technology needed to effectively protect customers. The days when signature-based antivirus protection was sufficient are long gone. Today, malware writers collaborate to evade detection by generating an excess of constantly morphing unique threats that work to evade signature-based detection methodologies. Their criminal efforts are global, collaborative and malicious—intended to tax and overload the legacy signature-based malware processing systems that have been established and relied upon by antivirus vendors for the past 20 years. The explosive growth of pattern files means it's hard to keep protection up-to-date, and traditional catch rate benchmarking is no longer a valid indicator of a solution's ability to effectively protect customers.

Today, traditional antivirus/anti-spam pattern updates for detecting and eradicating malware using signatures must be used in combination with other techniques and technologies to provide a multi-layered, multiple threat defense against Web threats that take advantage of the interactive nature of the Internet. Baseline deployment of security solutions at the gateway, in the network and on the endpoint is no longer enough. A revolution is needed to ensure that cyber-criminals do not succeed. Beyond baseline protection, "in-the-cloud" security will be the best way to proactively respond to new and emerging Web threats.

"In-the-cloud" security technologies deal with a threat at the source, before the traffic reaches the Internet gateway. Cloud-based databases are updated dynamically, in real time, and reduce reliance on local databases or frequent updates by decreasing the need for pattern matching and other desktop memory- and management-intensive approaches.

Critical in-the-cloud security technologies will include the following:

- Web Reputation Technology:
 - Monitoring of Web sites using URL filtering technology, IP location checks in which IP locations are correlated with URLs, as well as checking against Web site reputation ratings logged in a Web reputation database
 - Database updates occur dynamically/continuously, allowing security vendors to quickly respond to and remediate new email and Web threats
 - Access to malicious Web sites is blocked based on domain reputation ratings

- Email Reputation Technology:
 - Validates IP addresses against both a reputation database and a dynamic service that monitors Internet traffic patterns and IP email sending behavior in real time, stopping Web threats from zombies, botnets, and other new spam sources



- Botnet Identification / Bot Behavior Monitoring Technology:
 - Analyzes network traffic and bot behavior to identify botnet command-and-control servers
 - Continually monitors the servers to verify and block only those that are currently active
 - Delivers a live feed of IP addresses with details on the confidence factor and type of threat
 - Blocks communication to and from command-and-control servers based on IP address

Best Practices

Vulnerability and Patch Management

- Deploy vulnerability scanning software in the network and schedule them to run at least weekly.
- Make sure all operating systems and installed software applications are up-to-date and patched with the vendor's most recent security patches.
- When applicable, enable the automatic Update and installation features.
- Apply new updates as soon as they are announced. Use groupware management software to deploy updates across the enterprise.

- Consumers should use the latest internet security package that includes integrated vulnerability and exploit prevention, firewalls, and content filtering.

Software Resource Management

- Formulate a strict software and internet usage policy and standardize software across network segments.
- Run a security audit and remove all non-business related software in the enterprise.
- Restrict unnecessary ports and protocols to and from the corporate network and evaluate options if P2P, IM, or IRC protocols are business needs.
- Limit all user privileges in the network and avoid unauthorized modification of key operating system components to limit trojan and rootkit activities.
- Deploy groupware managed network-wide scanning of all traffic such as web, file transfer, and email and make sure users cannot bypass them.

- Consumers should use parental controls. It is recommended to use access control features and limit the default user privileges. Most gaming systems are now capable of online access so be aware of this functionality as well in relation to children.

End User Education and Policies

- Use both online and physical security defense strategies. Restrict introduction of personal computing devices via use policies in the enterprise.
- Ensure that content filtering solutions use informative language that explains why a site has been blocked rather than just an error message.
- Use defense in depth strategies with layered defenses that allow for integrated threat reporting and management



- Generate daily reports that prioritize all threats, and review for action. Share results with users together with cause and effect threat analysis.
- Support user awareness campaigns relative to varied computing environments. Formulate basic user guidelines for typical attack scenarios.
- Consumers should pay attention to the technology segment of daily news media as anti-malware companies usually share information to alert the general public on topics such as phishing, online banking, social networks, and so on.

Credits

Contributors:

Jaime Lyndon Yaneza

Todd Thiemann

Christine Drake

Jon Oliver

David Sancho

Feike Hacquebord

Anthony Arrott

George Moore

Joey Costoya

Macky Cruz

Wiebke Lips

Elizabeth Bookman