
**Laxmi Ahuja**

Amity Institute of Information Technology, Amity University, Uttar Pradesh,Sec 125 Noida (UP)

laxmiahuja@aiit.amity.edu

**Rajbala Simon**

Amity Institute of Information Technology, Amity University, Uttar Pradesh, Sec 125 Noida (UP)

rajbalasingh@aiit.amity.edu

ABSTRACT

• Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming is universally reviled, and has been the subject of legislation in many jurisdictions. Spamming is now considered to be a serious threat to the Internet and is posing a serious threat to both ISP and users' resource. Service providers are under mounting pressure to prevent, monitor and lessen spam attacks directed toward their customers and their infrastructure. The Internet is part of the serious national infrastructure. Attacks that are seen everyday on the Internet include direct attacks, remote reflective attacks, worms, and viruses. Emerging classes of messaging abuse in the mobile environment have led to neologisms like "SMishing," or SMS phishing. A SMiShing attack could introduce viruses or other malware to the network or add massive charges to corporate cell phone bills.

KEYWORDS

•Virus, Spam
• wireline-to-wireless threats
•wireless-specific threats

Attacks of all kinds have become much more complicated and harder to detect. The nature of computer attacks has changed over the past few years. Like early viruses that were often created by hackers whose sole interest was in gaining visibility within the hacker community, the new attacks are much more disturbing and have just the opposite visibility goals; they are usually motivated by the desire for money. The result is often fraud committed on thousands of unsuspecting users, commonly referred to as “crimeware”. For example, capturing personal or company information without the knowledge or consent of the owner of the computer system can lead to catastrophic results for individuals, as well as for businesses, government entities, medical/healthcare organizations and educational institutions. Even the innocent act of playing a music CD on a computer can leave it open to attack. Spyware can accompany the music when it is automatically downloaded onto the hard drive, rendering the computer vulnerable to attack.

## *Types of Attacks*

The most common attacks are no longer simple (or even complex) viruses. Many forms of malware and other unwanted software programs are using complex combinations of attacks to spread — not simply relying on one method alone. The following are some of the major areas of vulnerability that could result in attacks.

- Operating system and software application vulnerabilities.
- Accepting downloads from unknown sources when visiting websites.
- Active-X, Java and scripts can either contain malicious code or download malicious code from various websites.
- Email files attachments.

## *Viruses*

A computer virus is a computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

As stated above, the term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, adware, and spyware programs that do not have the reproductive ability. Malware includes computer viruses, worms, trojans, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software, including true viruses. Viruses are sometimes confused with computer worms and Trojan horses, which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan is a program that appears harmless but hides malicious functions. Worms and Trojans, like viruses, may harm a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious or simply do nothing to call attention to them. Some viruses do nothing beyond reproducing themselves.

There currently are five recognized types of viruses: File Infector Viruses, Boot Sector Viruses, Master Boot Record Viruses, Multi-Partite Viruses and Macro Viruses.

## *Trojan Horses*

Trojan Horses are impostors – files that claim to be something desirable but are, in fact, malicious. A very important distinction between Trojan horse programs and true viruses is that they do not replicate themselves. Trojans contain malicious code that when triggered cause loss, or even theft, of data. For a Trojan horse to spread, you must, “invite” it onto your computers. For example, you could open an email attachment or download and run a file from the Internet.

Trojan horses require interaction with a hacker to fulfill their purpose, though the hacker need not be the individual responsible for distributing the Trojan horse. In fact, it is possible for hackers to scan computers on a network using a port scanner in the hope of finding one with a Trojan horse installed, which the hacker can then use to control the target computer.

A trojan differs from a virus in that only a file specifically designed to carry it can do so.

Due to the growing popularity of botnets among hackers, Trojan horses are becoming more common. According to a survey conducted by BitDefender from January to June 2009, "Trojan-type malware is on the rise, accounting for 83-percent of the global malware detected in the world".

.

### *Worms*

Worms are programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which require the spreading of an infected host file. Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside of it. The entire document will travel from computer to computer. In other words, the entire document could be considered the worm. W32.Mydoom.AX@mm is an example of a worm. Worms spread by exploiting vulnerabilities in operating systems. All vendors supply regular security updates, and if these are installed to a machine then the majority of worms are unable to spread to it. If a vendor acknowledges vulnerability, but has yet to release a security update to patch it, a zero day exploit is possible. However, these are relatively rare. Users need to be wary of opening unexpected email, and should not run attached files or programs, or visit web sites that are linked to such emails. However, as with the ILOVEYOUworm, and with the increased growth and efficiency of phishing attacks, it remains possible to trick the end-user into running a malicious code.

### *Hoax*

Virus hoaxes are messages, almost always sent through e-mail, that amount to little more than chain letters. One of my favorite phrases associated with virus hoaxes is, "Forward this warning to everyone you know!" Most hoaxes are sensational in nature and easily identified by the fact that they indicate that the virus will do nearly impossible things, like blow up the recipient's computer and set it on fire, or less sensationally, delete everything on the user's computer. They often include announcements claimed to be from reputable organizations such as Microsoft, IBM, or news sources such as CNN and include emotive language and encouragement to forward the message. These sources are quoted in order to add credibility to the hoax. Virus hoaxes are usually harmless and accomplish nothing more than annoying people who identify it as a hoax and waste the time of people who forward the message. Nevertheless, a number of hoaxes have warned users that vital system files are viruses and encourage the user to delete the file, possibly damaging the system. Examples of this type include thejdbgmgr.exe virus hoax and the SULFNBK.EXE hoax. Some consider virus hoaxes and other chain e-mails to be a computer worm in and of themselves. They replicate by social engineering—exploiting users' concern, ignorance, and disinclination to investigate before acting. Hoaxes are distinct from computer pranks, which are harmless programs that perform unwanted and annoying

actions on a computer, such as randomly moving the mouse, turning the screen display upside down, etc.

### *Spam*

Spam is not very different from the junk mail you've been getting at home or in the office for decades. Only now, the junk mail is coming through your e-mail accounts to your computers at home and in the office. Nonetheless, spam is by far worse than junk mail. The only real cost of eliminating junk mail is buying a larger recycling bin. Spam and Phishing, which we will discuss later, can actually cost you and your organizations time, money, and worst of all, the loss of data and confidential information. It can also create legal liability issues because of its content. If you talk to some end users they don't see much difference between Spam and the ordinary junk mail that mail carriers have delivered for years. They may say "all you have to do is hit delete". Obviously these people have never had hundreds of Spam messages hit their inbox in a very short period. Additionally they have never run a network or email gateway. The cost to corporations in bandwidth, delayed email, and employee productivity has become a tremendous problem for anyone who provides email services. Many customers think their Internet Service Provider (ISP) should be able to fix the problem. But Spam is a world-wide problem, and email systems around the world are not setup in a consistent manner.

### *Real-time Black-hole Lists (RBLs)*

RBL's are lists on the Internet that track the IP addresses of machines recently known to be Spamming. Subscribers use these lists to check if a sender is a suspected Spammer and reject email from IP addresses on the list. Unfortunately there are several lists, and they don't all work the same. Some actually charge you to get off the list, and then others may block addresses of innocent users that are in the same IP range as a Spammer. Blacklists prevent millions of innocent e-mails from arriving at their destinations. Don't get me wrong. Blacklists mean well, and have been a helpful tool in helping curb Spam, however too many lists run differently sometimes creates a real problem for email administrators, ISP's, and legitimate users of email. But RBL's have also been very helpful in bringing awareness to the Spam problems, and have played an important part in helping curb issues. Hopefully someday the need for RBL's will be obsolete.

Typically the goal of Spam is to sell some product or service. Of course not all of these services are always good and proper, but then again some are. It would be nice if all Spam advertising could be tracked back to a store front like typical advertising, however Spammer's typically do not operate this way. Why, because if it were easily traced it would be easily stopped. Of course there is always the Spam that comes from "off-shore" where laws do not apply. But the majority of todays Spam comes from compromised end user machines. Think about it, if you could use the computer of some unsuspecting person to send out millions of emails to huge lists of people, your now using the resources of someone else's computer, and

some service providers bandwidth to do your "dirty advertising" for free. Then if the recipient of the Spam complains, they are are never really reaching the actual Spam advertiser.

### *Phishing*

Phishing, as the name implies, is when spam is used as a means to "fish" for the credentials necessary to access and manipulate financial accounts. Invariably, the e-mail will ask the recipient for an account number and the related password, explaining that records need updating or a security procedure is being changed that requires confirming an account. Unsuspecting e-mail recipients that supply the information don't know it, but within hours or even minutes, unauthorized transactions will begin to appear their accounts.

By now, most people know that giving this information away on the Internet is a no-no. With Phishing, however, it's almost impossible to tell if the e-mail is a fraud. Like spam, e-mails from Phishers usually contain spoofed FROM or REPLY TO addresses that make the e-mail look as though it came from a legitimate company.

The RapidShare file sharing site has been targeted by phishing to obtain a premium account, which removes speed caps on downloads, auto-removal of uploads, waits on downloads, and cooldown times between downloads.

### *Defenses*

The daily challenge for IT managers and administrators is to continue the freedom of computer users to access to the information they need, but at the same time, protecting all systems from malicious threats. This has been made more difficult by the growing complexity of threats, especially blended threats that combine Viruses and Spam. These new and emerging combined methods of propagation are, in some cases, taking advantage of the vulnerabilities of Operating Systems.

### *Wireline-to-wireless threats AND wireless-specific threats*

*These two threat types are considered individually due to technical and economic reasons, which play key roles in how likely they are to proliferate in the wireless environment and what are the appropriate methods to stop them.*

### *Wire line-to-wireless threats*

*Technology convergence has helped decrease the cost of devices and services that bridge traditional wireline services such as email and Web and wireless services such as SMS and WAP. Economic barriers, such as the relatively high cost of sending SMS from a handset, have kept the wireless space almost clear of the volume of messaging abuse seen by wireline networks. This barrier, however, has been lowered by the increasingly seamless interface between the two technologies. Email to SMS gateways enable any email user to send messages free of charge to mobile subscribers around the world. Since spammers are not penalized for sending SMS/text messages, this potentially opens up the possibility of low-profitability spam, like the "Viagra" spam, being an issue for mobile users. Email to SMS is a popular service that subscribers use to reach friends and page groups of users,so discontinuing or severely restricting this service is not a good option. Therefore, mobile operators need to protect their email to SMS gateways with the same type of filters and*

*content analysis systems that large ISPs use to cover their email infrastructure. As mobile customers demand more features currently available only over the Internet, the economic constraints that restrict mobile messaging abuse will disappear, leaving mobile devices vulnerable to the same forms of messaging abuse as those terminating on laptops and computers. To make matters more complicated, email and other forms of communications are extending to new categories of devices beyond just mobile phones and PDAs. Internet connected devices ranging from television set-top boxes to refrigerators are rapidly expanding the footprint of messaging-capable platforms. The latest wave of gaming consoles and portable entertainment devices also have Internet connectivity and messaging capabilities, which raises additional concerns about inappropriate content reaching minors who are the majority of users of these devices. While the incidence of abuse on these platforms is still unknown, the sheer number of these devices together with the affinity of the users makes these platforms compelling targets for spammers*

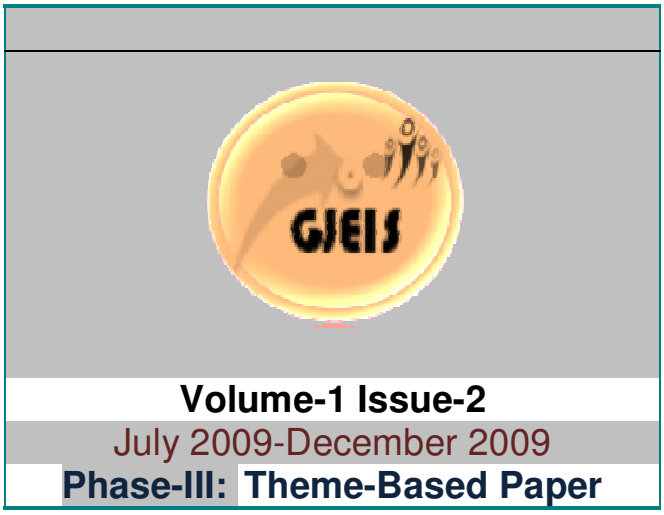
- *Wireless-specific threats*

Wireless-specific messaging threats will be similar to those pioneered in the wireline domain, but will diverge due to specific economic factors. Asia has consistently led the way in mobile content and usage trends, and events there may be indicative of what's to come in other developed mobile markets such as the U.S. and Europe. In Japan and South Korea, where the cost of sending SMS is around a penny, the rate of mobile spam is almost on par with email spam. On 2 Japan's NTT DoCoMo's network, 9 out of 10 messages are spam. In South Korea, subscribers receive on average one spam per day on their mobile phone. Until the per message cost associated with sending SMS drops in the U.S. and Europe, users there will likely see short codes and narrowly-targeted announcements instead of URL s and large broadcast mailings that are prevalent in wireline networks. For example, a user may receive a spam SMS enticing him to sign up for a text service using a short code that is tied in with the mobile operator's billing system or he may be tricked into calling a premium rate number. The ease in setting up premium rate phone numbers makes this type of fraud particularly appealing to scam artists. These "false pretext" messages have a direct and immediate monetary impact on subscribers, leading to high customer dissatisfaction.

## *Conclusion*

To be concluded we can say that In the past, threats have often been managed using separate threat management components, such as anti-virus, anti-spyware, etc. Recent attacks have involved combinations of different kinds of malware, limiting the effectiveness of separate components designed to combat only a single type of attack. A more effective approach is an integrated threat management solution that provides centralized management of all anti-threat capabilities. Cloudmark's flexible; content-agnostic solution is uniquely able to combat mobile spam, phishing and viruses that originate from mobile devices or the Internet. Cloudmark can be implemented to stop

messaging abuse at the network's edge, thus ensuring that spectrum, network resources and service quality are not impacted. For mobile operators, Cloudmark's comprehensive messaging security leadership translates into lower subscriber churn and support, as well as loyal subscribers who can confidently adopt innovative services.




**References:**

1. **http://www.techzoom.net/publications/insecurity-iceberg/**
2. **http://ca.com/Files/WhitePapers/ca_threat_management_wp.pdf**
3. **http://www.purewire.com/purewire_web_security_service.php**
4. **http://www.techzoom.net/publications/insecurity-iceberg/**
5. **http://www.allspammedup.com/anti-spam/knowing-the-threats-of-spam/**
6. **http://www.cloudmark.com/releases/docs/wp_taxonomy_of_mobile_threats_2009-05.pdf**