The introduction to malicious software computer science

Malware is a collective term for any malicious software which enters system without authorization of user of the system. The term is created from amalgamation the words ‘ malicious’ and ‘ software’. Malware is a very big hazard in today’s computing world. It continues to grow in capacity and advance in complexity. As more and more organization try to address the difficulty, the number of websites distribute the malware is rising at an frightening rate and is getting out of control. Most of the malware enters the system while downloading files over Internet. Once the malicious software finds its way into the system, it scans for vulnerabilities of operating system and perform unintended actions on the system finally slowing down the performance of the system.

Malware has ability to infect other executable code, data/system files, boot partitions of drives, and create excessive traffic on network leading to denial of service. When user executes the infected file; it becomes resident in memory and infect any other file executed afterwards. If operating system has a vulnerability, malware can also take control of system and infect other systems on network. Such malicious programs (virus is more popular term) are also known as parasites and adversely affect the performance of machine generally resulting in slow-down.

Some malware are very easy to detect and remove through antivirus software[1]. These antivirus software maintains a repository of virus signatures i. e., binary pattern characteristic of malicious code. Files suspected to be infected are checked for presence of any virus signatures. This method of detection worked well until the malware writer started writing polymorphic malware [15][16] and metamorphic malware. These variant of

malware avoid detection through use of encryption techniques to thwart signature based detection. Security products such as virus scanners look for

characteristics byte sequence (signature) to identify malicious code. The quality of the detector is determined by the techniques employed for detection. A stealth malware detection[36] technique must be able to identify malicious code that is hidden or embedded in the original program and should have some capability for detection of yet unknown malware. Commercial virus scanners have very low resilience to new attacks because malware writers continuously make use of new obfuscation methods so that the malware could evade detections.

2. 1 Computer Virus

A computer virus[6] is basically a program which is written by the programmers whose behaviour is to replicate itself and spread from one computer to another. The term “ virus” is also normally, but incorrectly, used to refer to other types of malware, including but not limited to adware . and these spyware programs that do not have a reproductive ability.

Malware includes various computer viruses[6], such as computer worms, Trojan horses[17], most of them are rootkits, spyware which are also considered as dishonest adware and other malicious or redundant software, including proper viruses. Viruses are occasionally confused with worms and Trojan horses, which are theoretically different. A worm can exploit security vulnerabilities to spread itself repeatedly to other computers through networks[7], while a Trojan horse is a program that appears nontoxic but hides malicious functions. Worms and Trojan horses[17], like viruses, may

harm a computer system’s data or recital. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious or simply do nothing to call attention to themselves. Some viruses do nothing beyond reproducing themselves.

An example of a virus which is not a malware, but is putatively benevolent, is Fred Cohen’s theoretical compression virus[6]. However, various antivirus professionals[5] don’t admit the concept of kindly viruses, as any beloved function can be implemented without involving a virus automatic compression, for instance, is available under the Windows operating system at the choice of the user. Any virus will by definition make unconstitutional changes to a computer, which is undesirable even if no damage is done or intended. On page one of Dr Solomon’s Virus pdf, the undesirability of viruses, even those that do nothing but reproduce, is thoroughly explained.

2. 1. 1 Academic Work

Veith Risak published[6] the article whose title was as follows “ Selbstreproduzierende Automaten mit minimaler Information subertragung” (Self-reproducing automaton with minimum information switch over). The article described a fully serviceable virus written in assembler language for a particular SIEMENS 4004/35 computer system.

In the year 1980 Jurgen Kraus wrote his thesis on Selbstreproduktion bei Programmen at the University of Dortmund. In his work Kraus guess that computer programs[4] can behave in a way parallel to biological viruses.

In the year of 1984 Fred Cohen at the University of Southern California wrote his paper on the “ Computer Viruses[6] – Theory and Experiments”. It was the first paper of him in which he has explained to clearly call a self-reproducing program a “ virus”, a term introduced by Cohen’s mentor Leonard Adleman. Fred Cohen published a exhibition that there is no algorithm that can perfectly detect all potential viruses.

An article that published on malware that describes “ useful virus functionalities” was available by J. B. Gunn in the title “ Use of virus functions to provide a virtual APL predictor under user control” in 1984.

2. 1. 2 Science Fiction

There are several myths associated with the science. The actual term “ virus” was first used to symbolize a self-reproducing program in a small story by David Gerrold in Galaxy magazine in 1969-and later in his 1972 novel, When HARLIE Was One. In that novel, a attentive computer named HARLIE writes viral software to recover damaging personal information from other computers to blackmail the man who wants to turn him off.

Michael Crichton[7] told as a sideline story of a computer with telephone modem dialing potential, which had been automatic to randomly dial phone numbers until it hit a modem that is answered by another computer. It was an attempt to program the answer computer with its own program, so that the second computer would also begin dialing unsystematic numbers, in search of yet a different computer to program. The program is assumed to spread exponentially through susceptible computers.

2. 1. 3 Virus Programs

The Creeper virus[6] was first detected on ARPANET, the prototype of the Internet, in the early 1970s. Creeper was an new self-replicating program developed by Bob Thomas at BBN Technologies in 1971. Creeper has used the ARPANET to infect DEC PDP-10 computers which are running on the TENEX operating system. Creeper gain admission via the ARPANET and banal itself to the isolated system where there was a message, “ I’m the creeper, catch me if you can!” was displayed. The Reaper program was created to delete Creeper.

A program called which is known as “ Elk Cloner” was the first PC virus to appear in the uncultivated that is, outside the single computer or lab where it was created by Richard Skrenta, it attached itself to the Apple DOS 3. 3 operating system and spread via floppy disk. This virus, created as a practical joke when Skrenta was studying in the high school and was injected in a game on a floppy disk. On his 50th iterative use the Elk Cloner virus would be activate, which prone to infecting the PCs and displaying a short poem beginning “ Elk Cloner: The program with a personality.”

The first IBM PC virus in the natural was a boot sector virus dubbed and created by the Farooq Alvi Brothers in Lahore, Pakistan, seemingly to deter piracy of the software they had written.

Before computer networks[7] became widespread, most viruses spread on removable media, particularly floppy disks. In the early days of the PCs, many users frequently exchanged their information and programs on floppies. Some of the viruses are spread by infecting programs which are

stored on these disks, while others programs installed themselves into the disk boot sector, which ensure that they would be run when the user booted the computer from the disk, usually inadvertently. Personal computers of the period would try to boot from the floppy at first if one had been left in the drive. Until floppy disks rejects, this was the most unbeaten infection strategy and that is why boot sector viruses were the most common in the wild for many years.

Conventional computer viruses[6] emerge in the 1980s, that are driven by the spread of PCs and the consequential increase in BBS, modem use, and software sharing. Bulletin board-driven software giving out contributed directly to the swell of Trojan horse programs, and computer viruses which were written to infect readily traded software. Shareware and bootleg software were equally common vectors for viruses on BB Systems Viruses can increase their chances of spreading over the several other computers which in networks[7] by infecting the files on the particular network file system or a file system which can be access by other computers

Macro viruses have become common since the mid-1990s. Most of these viruses are written in the scripting languages for Microsoft programs such as MS-Word and MS-Excel and spread throughout Microsoft Office by infecting documents and spreadsheets. Since Word processor and Excel spread sheets were also available for Mac OS, most could also spread to Macintosh computers. Although most of these computer viruses[6] may not have the capability to send contaminated email messages to those viruses which did take advantage of the Microsoft Outlook COM interface.

Some old versions of Microsoft Word allow macros to repeat themselves with added blank lines. If two macro viruses concurrently infect a document, the combination of the two, if also self-replicating, can appear as a “ mating” of the two and would likely be detected as a virus unique from the “ parents”.

A virus may also send a web address link as an instant message to all the contacts on an infected machine. If the recipient, thinking the link is from a friend which isa trusted source follows the link to the website, the virus hosted at the site may be able to infect this new computer and continue propagating.

Viruses that spread using cross-site scripting were first reported in 2002, and were academically demonstrated in 2005. There have been multiple instances of the cross-site scripting viruses in the wild, exploiting websites such as MySpace and Yahoo!.

2. 2 Classification

In order to replicate itself, a virus must be permitted to execute code and write to memory. For this reason, many viruses attach themselves to executable files that may be part of legitimate programs (see code injection). If a user attempts to begin an infected program, the virus’ code may be executed concurrently. Viruses can be separated into two types based on their performance when they are executed. Nonresident viruses straight away search for other hosts system or OS which can be infected, or infect those targets, and finally transfer organize to the application program they infected. Tenant viruses do not search for hosts when they are happening. Instead, a resident virus masses itself into memory on execution and

transfers control to the host program. The virus stays active in the background and infects new hosts when those files are accessed by other programs or the operating system itself.

2. 2. 1 Nonresident Viruses

Nonresident viruses can be notion of as consisting of a finder module and a replication module. The finder module is responsible for finding new files to infect. For each new executable file the finder module encounters, it calls the replication module to infect that file.

2. 2. 2 Resident Viruses

Resident viruses contain a replication module which is parallel to the one that is engaged by nonresident viruses. This section, however, is not called by a finder module. The virus[27] masses the duplication module into memory when it is executed instead and ensures that this module is executed each time the operating system is called to carry out a certain operation. The replication module can be called, for example, each time the operating system executes a file. In this case the virus infects every suitable program that is executed on the computer.

Resident viruses are sometimes can be divided into a class of fast infectors and a class of slow infectors. Fast infectors are those which are designed to infect as many files as soon as possible. A fast infector, for instance, can infect every potential host file that is accessed. This pose a special difficulty when using anti-virus software[1], since a virus scanner will access every prospective host file on a computer when it performs a system-wide scan. If

the virus scanner fails to notice that such a virus is present in memory the virus can “ piggy-back” on the virus scanner and in this way infect all files that are scanned. Fast infectors rely on their fast infection rate to spread. The disadvantage of this method is that infecting many files may make detection more likely, because the virus may slow down a computer or perform many suspicious actions that can be noticed by anti-virus software. Slow infectors, on the other hand, are designed to infect hosts infrequently. Some slow infectors, for instance, only infect files when they are copied. Slow infectors are designed to avoid detection by limiting their actions: they are less likely to slow down a computer noticeably and will, at most, infrequently trigger anti-virus software[5] that detects suspicious behavior by programs. The slow infector approach, however, does not seem very successful.

In most of the operating systems which use file extensions to determine program relations such as Microsoft Windows. The extensions may be normally hidden from the user by default. This makes it probable to create a file that is of a different type than it appears to the users or programmers. For example, an executable file may be created named “ picture. png. exe”, in which the user sees only “ picture. png” and therefore assumes that this file is an image and most likely is safe, yet when opened runs the executable on the client machine.

An additional scheme is to generate the virus system from parts of existing operating system files by using the CRC16/CRC32 data. The initial code can be quite small (tens of bytes) and unpack a fairly large virus. This is

analogous to a biological prion in the way it works but is vulnerable to signature based detection. This attack has not yet been seen “ in the wild”.

2. 3 Infection Strategies

Virus avoids detection[31] by users, some viruses employ different kinds of deception. Some of the old viruses, especially on the MS-DOS operating system, make sure that the “ last modified” date of a host file stays the same when the file is infected by the virus. This approach does not fool antivirus software, however, especially those which maintain and date cyclic redundancy checks on file changes.

Some viruses can infect files without increasing their sizes or damaging the files. They accomplish this by overwriting unused areas of executable files. These are called cavity viruses. For example, the CIH virus, or Chernobyl Virus, infects Portable Executable files. Because those files have many empty gaps, the virus, which was 1 KB in length, did not add to the size of the file.

Some viruses try to avoid detection by killing the tasks associated with antivirus software[1] before it can detect them.

As computers and operating systems grow larger and more complex, old hiding techniques need to be updated or replaced. Defending a computer against viruses may demand that a file system migrate towards detailed and explicit permission for every kind of file access.

2. 3. 1 Read Request Intercepts

While some antivirus software employ various techniques to counter stealth mechanisms, once the infection occurs any recourse to clean the system is unreliable. In Microsoft Windows operating systems, the NTFS file system is proprietary. Direct access to files without using the Windows OS is undocumented. This leaves antivirus software little alternative but to send a read request to Windows OS files that handle such requests. Some viruses trick antivirus[5] software by intercepting its requests to the OS. A virus can hide itself by intercepting the request to read the infected file, handling the request itself, and return an uninfected version of the file to the antivirus software. The interception can occur by code injection of the actual operating system files that would handle the read request. Thus, an antivirus software[1] attempting to detect the virus will either not be given permission to read the infected file, or, the read request will be served with the uninfected version of the same file.

File hashes stored in Windows, to identify altered Windows files, can be overwritten so that the System File Checker will report that system files are originals.

The only reliable method to avoid stealth is to boot from a medium that is known to be clean. Security software can then be used to check the dormant operating system files. Most security software relies on virus signatures or they employ heuristics, instead of also using a database of file hashes for Windows OS files. Using file hashes to scan for altered files would guarantee removing an infection. The security software can identify the altered files, and request Windows installation media to replace them with authentic versions.

2. 3. 2 Self-Modification

Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for so-called virus signatures. Unfortunately, the term is misleading, in that viruses do not possess unique signatures in the way that human beings do. Such a virus signature is merely a sequence of bytes that an antivirus program looks for because it is known to be part of the virus. A better term would be “ search strings”. Different antivirus programs[1] will employ different search strings, and indeed different search methods, when identifying viruses[6]. If a virus scanner finds such a pattern in a file, it will perform other checks to make sure that it has found the virus, and not merely a coincidental sequence in an innocent file, before it notifies the user that the file is infected. The user can then delete, or in some cases clean or heal the infected file. Some viruses employ techniques that make detection by means of signatures difficult but probably not impossible. These viruses modify their code on each infection. That is, each infected file contains a different variant of the virus.

2. 3. 3 Encryption With A Variable Key

A more advanced method is the use of simple encryption to encipher the virus. In this case, the virus consists of a small decrypting dependent methods and an encrypted copy of the virus code. If the virus is encrypted with the help of different key for each infected file, the only part of the virus that leftovers stable is the decrypting unit, which would (for example) be appended to the end. In this case, a virus scanner will not able to detect directly the virus using signatures, but it can still detect the decrypting unit,

which still makes indirect revealing of the virus possible. Since these would be symmetric keys, stored on the infected host. In fact completely possible to decrypt the final virus, but this is almost certainly not required, since self-modifying code is such a scarcity that it may be basis for virus scanners to at least flag the file as suspicious.

This may be old , but solid, encryption involves XORing each byte in a virus with a even, so that the exclusive-or operation has only to be frequent for decryption. It is doubtful for a code to adjust itself, so the code to do the encryption as wll as decryption may be part of the signature in many virus definition.

2. 3. 4 Polymorphic Code

Polymorphic code was the first technique that posed a serious threat[27] to virus scanners. Likewise various normal encrypted viruses such as a polymorphic virus[15][16] infects files with an encrypted copy of itself, which may be decoded by a decryption method. In the case of polymorphic viruses or polymorphic worms[10], however, this decryption module is also modified on each infection. A well-written polymorphic virus thus has no parts which wait identical between infection, making it very difficult to detect directly using signatures. Antivirus software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body. To enable polymorphic code, the virus has must have a polymorphic engine which is also called mutating engine or mutation engine anywhere in its encrypted body. Some viruses employ polymorphic code in a system that constrain the change rate of the virus appreciably. For example, a virus can

be planned to alter only slightly over time, or it can be programmed to refrain from mutating when it infects a file on a computer that previously contains copies of the virus. The benefit of using such sluggish polymorphic[15][16] code is that it makes it more difficult for antivirus professionals to get representative sample of the virus, because tempt files that are infected in one run will naturally have identical or parallel sample of the virus. This will make it more liable that the detection by the virus scanner will be variable, and that some instances of the virus may be able to avoid detection.

2. 3. 5 Metamorphic Code

To avoid being detected by emulation, some viruses revise themselves completely each time they are to infect new executables. Viruses that make use of this technique are said to be metamorphic. To enable metamorphism, a metamorphic engine must be needed. A metamorphic virus is usually very large and complex. For example, W32/Simile consists of over 15, 000 lines of assembly language code, 90% of which is part of the metamorphic engine.

2. 3. 6 Avoiding Bait Files and other Undesirable Hosts

A virus wants to infect hosts in order to multiply further. In some cases, it might be a bad idea to infect a mass program. For example, many antivirus softwares perform an integrity check of their own code. Infecting such programs will therefore increase the likelihood that the virus is detected. For this reason, some viruses are programmed not to infect programs that are known to be part of antivirus software. Another type of host that viruses[27] sometimes avoid are bait files. Bait files (or goat files) are files that are

specially created by antivirus software, or by antivirus professionals themselves, to be infected by a virus. These files can be created for various reasons, all of which are related to the detection of the virus:

Antivirus professionals can use tempt files to take a test of a virus. It is more realistic to store and exchange a small, infected lure file, than to swap a large application program that has been infected by the virus.

Antivirus professionals can use bait files to study the actions of a virus and assess detection methods. This is particularly useful when the virus is polymorphic[15][16]. In this case, the virus can be made to infect a large number of entice files. The grimy files can be used to test whether a virus scanner detects all versions of the virus.

Some antivirus software employ bait files that are accessed regularly. When these files are modified, the antivirus software warns the user that a virus is probably active on the system.

Since bait files are used to detect the virus, or to make detection possible, a virus can benefit from not infecting them. Viruses typically do this by avoiding suspicious programs, such as small program files or programs that contain certain patterns of “ garbage instructions”.

A related strategy to make baiting difficult is sparse infection. Sometimes, sparse infectors do not infect a host file that would be a suitable candidate for infection in other circumstances. For example, a virus can decide on a random basis whether to infect a file or not, or a virus can only infect host files on particular days of the week.

2. 4 Vulnerability and Countermeasures2. 4. 1 The Vulnerability of Operating Systems to Viruses

Just as genetic diversity in a population decreases the chance of a single disease wiping out a population, the diversity of software systems on a network similarly limits the destructive potential of viruses. This became a particular concern in the 1990s, when Microsoft gained market dominance in desktop operating systems and office suites. Microsoft software is targeted by virus writers due to their desktop dominance.

Although Windows is by far the most popular target operating system for virus writers, viruses also exist on other platforms. Any operating system that allows third-party programs to run can theoretically run viruses.

As of 2006, there were at least 60 known security exploits targeting the base installation of Mac OS X (with a Unix-based file system and kernel). The number of viruses[6] for the older Apple operating systems, known as Mac OS Classic, varies greatly from source to source, with Apple stating that there are only four known viruses, and independent sources stating there are as many as 63 viruses. Many Mac OS Classic viruses targeted the HyperCard authoring environment. The difference in virus vulnerability between Macs and Windows is a chief selling point, one that Apple uses in their Get a Mac advertising. In January 2009, Symantec announced the discovery of a Trojan that targets Macs. This discovery did not gain much coverage until April 2009.

While Linux, and Unix in general, has always natively blocked normal users from having access to make changes to the operating system environment,

Windows users are generally not. This difference has continued partly due to the widespread use of administrator accounts in contemporary versions like XP. In 1997, when a virus for Linux was released-known as “ Bliss”-leading antivirus[5] vendors issued warnings that Unix-like systems could fall prey to viruses just like Windows. The Bliss virus may be considered characteristic of viruses-as opposed to worms-on Unix systems. Bliss requires that the user run it explicitly, and it can only infect programs that the user has the access to modify. Unlike Windows users, most Unix users do not log in as an administrator user except to install or configure software; as a result, even if a user ran the virus, it could not harm their operating system. The Bliss virus never became widespread, and remains chiefly a research curiosity. Its creator later posted the source code to Usenet, allowing researchers to see how it worked.

2. 4. 2 The Role of Software Development

Because software is often designed with security features to prevent unauthorized use of system resources, many viruses must exploit software bugs in a system or application to spread. Software development strategies that produce large numbers of bugs will generally also produce potential exploits.

2. 4. 3 Anti-Virus Software and other Preventive Measures

Many users install anti-virus software that can detect and eliminate known viruses after the computer downloads or runs the executable. There are two common methods that an anti-virus software application uses to detect viruses. The first, and by far the most common method of virus detection is

using a list of virus signature definitions. This works by examining the content of the computer’s memory (its RAM, and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives), and comparing those files against a database of known virus “ signatures”. The disadvantage of this detection[32] method is that users are only protected from viruses that pre-date their last virus definition update. The second method is to use a heuristic algorithm to find viruses based on common behaviors. This method has the ability to detect novel viruses that anti-virus security[7] firms have yet to create a signature for.

Some anti-virus programs are able to scan opened files in addition to sent and received email messages “ on the fly” in a similar manner. This practice is known as “ on-access scanning”. Anti-virus software does not change the underlying capability of host software to transmit viruses. Users must update their software regularly to patch security holes. Anti-virus software also needs to be regularly updated in order to recognize the latest threats[27].

One may also minimize the damage done by viruses by making regular backups of data (and the operating systems) on different media, that are either kept unconnected to the system (most of the time), read-only or not accessible for other reasons, such as using different file systems. This way, if data is lost through a virus, one can start again using the backup (which should preferably be recent).

If a backup session on optical media like CD and DVD is closed, it becomes read-only and can no longer be affected by a virus (so long as a virus or infected file was not copied onto the CD/DVD). Likewise, an operating system

on a bootable CD can be used to start the computer if the installed operating systems become unusable. Backups on removable media must be carefully inspected before restoration. The Gammima virus, for example, propagates via removable flash drives.

2. 4. 4 Recovery Methods

A number of recovery options exist after a computer has a virus. These actions depend on the virus. Some may be safely removed by functions available in most anti-virus software products. Others may require re-installation of damaged programs. It is necessary to know the characteristics of the virus involved to take the correct action, and anti-virus products will identify known viruses precisely before trying to “ dis-infect” a computer; otherwise such action could itself cause a lot of damage. New viruses that anti-virus researchers have not yet studied therefore present an ongoing problem, which requires anti-virus packages[1] to be updated frequently.

2. 4. 5 Virus Removal

One possibility on Windows Me, Windows XP, Windows Vista and Windows 7 is a tool known as System Restore, which restores the registry and critical system files to a previous checkpoint. Often a virus will cause a system to hang, and a subsequent hard reboot will render a system restore point from the same day corrupt. Restore points from previous days should work provided the virus is not designed to corrupt the restore files and does not exist in previous restore points. Some viruses disable System Restore and other important tools such as Task Manager and Command Prompt. An example of a virus that does this is Cia Door. Many such viruses can be

removed by rebooting the computer, entering Windows safe mode , and then using system tools.

Many websites run by anti-virus software companies provide free online virus scanning, with limited cleaning facilities (the purpose of the sites is to sell anti-virus products). Some websites allow a single suspicious file to be checked by many antivirus programs in one operation. Additionally, several capable antivirus software programs are available for free download from the internet (usually restricted to non-commercial use), and Microsoft provide a free anti-malware utility that runs as part of their regular Windows update regime.

2. 4. 6 Operating System Reinstallation

Reinstalling any OS is another loom to virus removal. It involves either reformatting the computer’s hard disk drive and installing the operating system and all programs from original media, or may be restoring the entire partition with a clean backup image. User data can be restored by booting from a live Compact Disk, or putting the hard drive into another computer and booting from its operating system, using great care not to infect the second computer by executing any infected programs on the original drive; and once the system has been restored precautions must be taken to avoid re infection from a restored executable file.

These methods are obvious straightforward to do, may be faster than not infecting a computer, and are made certain to remove any malicious software. If any OS and programs must be reinstalled from scratch, the time

and try to reinstall, reconfigure again, and restore user preferences must be taken into account.

2. 5 Computer Worm

A computer worm[1] is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself. This is due to security shortcomings on the target computer. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Many worms that have been created are designed only to spread, and don’t attempt to change the systems they pass through. However, as the Morris worm and Mydoom showed, even these “ payload free” worms can cause major disruption by increasing network traffic and other unintended effects. A “ payload” is code in the worm designed to do more than spread the worm-it might delete files on a host system e. g., the Explore Zip worm, encrypt files in a cryptoviral extortion attack, or send documents via e-mail. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a “ zombie” computer under control of the worm author. Networks of such machines are often referred to as botnets and are very commonly used by spam senders for sending junk email or to cloak their website’s address. Spammers are therefore thought to be a source of funding for the creation of such worms and the worm writers have

been caught selling lists of IP addresses of infected machines. Others try to blackmail companies with threat[27]ened DoS attacks.

Backdoors can be exploited by other malware, including worms. Examples include Doomjuice which can spread using the backdoor opened by Mydoom, and at least one instance of malware taking advantage of the rootkit and backdoor installed by the Sony/BMG DRM software utilized by millions of music CDs prior to late 2005.

2. 5. 1 Worms with Good Intent

Beginning with the very first research into worms at Xerox PARC, there have been attempts to create useful worms. The Nachi family of worms, for example, tried to download and install patches from Microsoft’s website to fix vulnerabilities in the host system-by exploiting those same vulnerabilities. In practice, although this may have made these systems more secure, it generated considerable network traffic, rebooted the machine in the course of patching it, and did its work without the consent of the computer’s owner or user. Regardless of their payload or their writers’ intentions, most security experts regard all worms as malware.

Some worms, such as XSS worms, have been written to research how worms[5] spread. For example, the effects of changes in social activity or user behavior. One study proposed what seems to be the first computer worm that operates on the second layer of the OSI model (Data link Layer), it utilizes topology information such as Content-addressable memory (CAM) tables and Spanning Tree information stored in switches to propagate and probe for vulnerable nodes until the enterprise network is covered.

2. 5. 2 Protecting Against Dangerous Computer Worms

Worms spread by exploiting vulnerabilities in operating systems. Vendors with security problems 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 vulnerability is disclosed before the security patch released by the vendor, a zero-day attack is possible.

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 ILOVEYOU worm, and with the increased growth and efficiency of phishing attacks, it remains possible to trick the end-user into running malicious code.

Anti-virus and anti-spyware software are helpful, but must be kept up-to-date with new pattern files at least every few days. The use of a firewall is also recommended.

In the April-June, 2008, issue of IEEE Transactions on Dependable and Secure Computing, computer scientists describe a potential new way to combat internet worms. The researchers discovered how to contain the kind of worm that scans the Internet randomly, looking for vulnerable hosts to infect. They found that the key is for software to monitor the number of scans that machines on a network sends out. When a machine starts sending out too many scans, it is a sign that it has been infected, allowing administrators to take it off line and check it for malware. In addition, machine learning techniques can be used to detect new worms, by analyzing the behavior of the suspected computer.

2. 5. 3 Historical background of worms

The actual term worm’ was first used in John Brunner’s, The Shockwave Rider. In that novel, Nichlas Haflinger designs and sets off a data-gathering worm in an act of revenge against the powerful men who run a national electronic information web that induces mass conformity. “ You have the biggest-ever worm loose in the net, and it automatically sabotages any attempt to monitor it… There’s never been a worm with that tough a head or that long a tail.

On November 2, 1988, Robert Tappan Morris[14], a Cornell University computer science graduate student, unleashed what became known as the Morris worm, disrupting an estimated 10% of the computers then on the Internet and prompting the formation of the CERT Coordination Center and Phage mailing list. Morris himself became the first person tried and convicted under the 1986 Computer Fraud and Abuse Act.