Sri Lanka Institute of Information Technology

# Computer Worms

**Individual Assignment**

IE2022 - Introduction to Cyber Security

Submitted by:


| Student Registration Number | Student Name |
|---|---|
| IT19952376 | S.A.D.H. Vishwajith |


Date of submission

18-10-2020

# Table of Contents

# 1. Abstract

Computer worms on the Internet have gone from potential premise to a real and very harmful computer network hazard. Computer viruses and worms have evolved from an exception to a daily phenomenon in less than two decades. They are also capable of influencing the Internet, the largest network of our day. Starting from simple and helpful roots, machine worms are now the Internet's scourge and can inflict harm worth billions of dollars in just a few hours, if not minutes. Although virus are initially more prevalent than worms, worm have become the primary threats in past years, coinciding with computer networking growth. Worm outbreaks are also happening amid the widespread use of firewalls and other network security devices and are expected to continue to be a threat in the near future. This means that worm developers employ worms for reasons other than just invasion, such as data stealing and denial of service networks. Recent worms appear as a series of variants that are rapid in succession. While viruses benefit from network services like the Internet for dissemination, currently viruses are much less prevalent than worms, and viruses do not appear to have imitated the magnitude and monetary impact of destructive behaviour. It is necessary to consider the forms of worms, the attackers that might recruit them, and the potential pay to learn the danger posed by machine worms.

## 2. Introduction

The internet has many advantages in our lives. This supports our mission and provides us with so many information that we need right away. It is becoming rapidly unstoppable, together with robust growth of the Internet, to build and spread malicious code that can destroy our machine 's data and computer. There are several forms of malicious malware in the world, such as: viruses, worms, mixed attacks, spyware, trojans, adware and other backdoors [1]. While there are many fascinating topics that can be discussed in depth, this paper would examine one type of malicious code, called a computer worm. Computer worm is a disruptive, self-replicating software virus that by passing over a local area network (LAN) or an Internet connection. inhibits the functionality of software and hardware programs. In many ways, these worms match a computer virus' description. It can also be self-replicated and distributed through networks, for example. That is why worms are referred to as viruses often. Yet, machine worms differ from computer viruses in several respects. Firstly, worms exist as separate entities or stand-alone programs, unlike viruses that need to cling on to files (host files) before they can spread within a device. Host files or programs do not require them. Computer worms do not modify information but reside in active memory and repeat themselves. Program worms use sections of the operating system, which are normally transparent and automated to the user. Many worms are engineered to reproduce only, and do not seek to change the mechanism in which they travel. When machine worms enter a system, they benefit from the file-transport or information-transport features of the system that allow them to migrate without support. For example, as Iran's threatened nuclear reactors, a digital worm dubbed the 'Stuxnet worm' recently turned heads around the world. Reportedly, approximately a fifth of Iran's nuclear centrifuges were killed by this worm, allowing them to spin out of balance by increasing the pressure on the spinning centrifuges, while at the same time demonstrating that it was under control[2]. It regulates this feat by replaying the defense device values of the plant in the control room when the attack was occurring. Based on protection mistakes, program worms also use a computer network to spread themselves onto the target computer. This software worms will use these programming worms as a host to scan for and kill other machines. Using that machines as

hosts, the worm will keep searching and target other machines until these new worm-invaded computers are controlled, and this operation will continue. Worms use recursive methods without a host program to replicate and disperse themselves, depending on the exponential growth law, and then exploit and infect more and more devices in a brief period of time. Worms nearly often do at least some disruption to the network, even if only by bandwidth absorption. In the method, their existence becomes evident only when their unchecked duplication, halting, or blocking other operations in the network absorbs software energy. In order to distribute or use some kind of social engineering tool, machine worms often manipulate the vulnerability of the target device or trick users into executing them.

## Types of Computer Worms

- **E-mail Worms**
  These worms spread through messages through e-mail. The computer worm will usually come in an email, where the worm code is stored in the message body or attachment, but it also connects to code on external site. However from bad architecture, most of e-mail schemes require to the recipient to open an mail attachment specifically to enable the computer worm, but "social engineering" can also be include effectively to promote this, as the writer of the "Anna Kournikova" worm set to illustrate. Computer worm can send itself out if enabled using any local email networks (e.g. MS Office facilities, Functions for Windows MAPI), or explicitly through SMTP. The addresses to which it sends were also extracted from the e-mail system or archives of the infected machines. Since Klez.E in 2002, SMTP worms usually fake the address of the sender, so email worm recipients can presume that they are not sent by the person mentioned in the email message (sender's address) field 'From'.

- **Instant Messaging Worms**
  Spreading is used by sending links to compromised websites via instant message apps to everyone on the local contact list. The main contrast between those computer worms and e-mail worms is way the connections are delivered.

- **IRC worms**
  The key target is chatting networks and the same form of infection / spreading as above is used, spreading infected files or connections to infect websites. Sending the spread file is less reliable since the user has to validate the acknowledgement, save file, and open it before the infection happens.

- **File-sharing networks worms**
  File-sharing worms can copy itself to a common location, likely stored on the local computer. Under a harmless tag, the computer worm will put a copy of themselves in a shared archive. Computer worm is now standing for downloading from the P2P network and the infected file will begin to spread.

- **Internet worms**
  These worms are these that, instead of going through higher-level protocols like IRC or email, attack low-level TCP / IP ports directly. Blower, which abused a Microsoft RPC vulnerability, is a textbook example. An infected machine searches random machines actively attempting an exploit With port 135 on the local network and the public Internet, the worm travels to the computer if it succeeds.

- **Rabbits & Bacteria**
  A bacterium or a rabbit is a software which absorbs all of a resource class. Some manipulative logic multiplies so exponentially that it becomes overwhelmed by energy. This generates an assault on denial of service.

- **Logic Bombs**
  These worms any deceptive logic allows an actual event to be triggered, such as a user login or midnight arrival. For instance, if she ever leaves the business, A programmer may hide a bit of code, such as the payroll database, that begins to delete files.

  E.g. E.g. A software posted on the USENET news network at the beginning of 1980 agreed to make it easy to handle programs. The following section was buried in the code:

  cd / rm-rf *

# 3. Evolution of the Computer Worms

## The beginning of computer worms

On November 2, 1988, About 8:30 p.m. the Massachusetts Institute of Technology (MIT) launched A malicious software from a computer on the Internet. The computer worm propagated so exponentially that it stopped grinding the machines at an unprecedented speed. In an email later that night, a worried student at the University of California, Berkeley said, "We are definitely under attack." An estimated 6,000 of the nearly 60,000 machines were than linked to the web were influenced within 24 hours. Computer worms don't want a software host, unlike viruses, but could survive and spread on their own. Berkeley had been very far from the perpetrator.

Pseudo-program has corrupted networks in several of elite public, colleges, and private research core that created the initial national electronic network. That came a year prior to the WWW's (World Wide Web) invention. Harvard, Stanford, , Princeton, Johns NASA, Hopkins, and National Laboratory of Lawrence Livermore were among many victims. The computer worm attacked only machines working a single version of Unix os, but it dissemination quickly because it had many attack vectors. For an example, a loophole in the email system on the Internet and a flaw in the "finger" software that detected network users were exploited. And also built to remain hidden. No files were damaged or lost by the worm, but a punch already packed. Military and university critical functions reduced to a crawl. For days, e-mails were has been postponed. The group of the network was trying to find out how the worm worked and how to eliminate it. Some institutions wiped their systems. some, for as much as a week, isolated their machines from the network. It was difficult to calculate the exact impact, but projections began at $100,000 and soared into the millions [3].

The issue of who was accountable became more pressing as computer scientists worked feverishly on a fix. A dismayed programmer contacted two friends shortly after the attack, acknowledging that he had unleashed the worm was spiraling and desperate that it had increasingly out of control. With a brief apology and instructions to uninstall the software, He asked a friend to give him an online anonymous post. Ironically, the worms destroyed the network such that it received the message on time. Some other friend made an individual, anonymous appeal to the New York Times, which might quickly publish on its front pages the news of the attack. A reporter was told by the person that he understood who had designed the software and meant it to be a sinister experiment and that due to a technical mistake it had spread. The friend referred to the maker of the worm unintentionally by his initials, RTM, in follow-up conversations with the reporter. Using that information, The Times soon confirmed and publicly reported that a 23-year-old graduate student from Cornell University named Robert Tappan Morris was the culprit [3].

This cyber worm is steadily expanding at a phenomenal pace and preventing computers from grinding. The August, he started to create a software that could spread over the Internet slowly and secretly. He unjustifiably published it to an MIT computer at Cornell

Terminal in Ithaca, New York, to cover his trip. The FBI initiated an investigation after the incident became public. Agents soon confirmed that Morris was behind the attack and started questioning and decoding his electronic files with him and his friends, resulting in a flood of false evidence. In 1986, the Congress passed the Computer Fraud and Abuse was banning unauthorized access to protected computers. A case against Morris was filed in 1989. He was sentenced by a jury the next year and became the first citizen under the 1986 legislation to be sentenced [4].

## The Computer worms' evolution

Despite widespread deployment of anti-virus tools, firewalls, intrusion detection programs, and other network protection measures, recent worms such as the August 2003 blaster worm and the January 2003 SQL sapphire worm have shown that networking machines continue to operate. They could be prone to new threats. To explain how they have grown in variety over the years, we study the historical evolution of viruses and worms. "Four" rings "from Scotch and Tapeworms in 1979 to the present are mentioned in the history of the evolution of viruses and worms (the term" generation "is less pronounced since worms in one wave are not descended from previous generations). This historical history leads to numerous research on present vulnerability and prediction of potential attacks by worms. It detects the evolution of worms into the preceding waves:

- 1979 to early 1990s
- Early 1990s to 1998
- 1999 to 2001
- 2001 to today.

These waves reflect the cycles in which, on a variety of important occasions, new technical developments started and emerged. Below we will talk about some of the types of computer worms that have spread from the past to the present.

- **Melissa (1999)**
  **Estimated damage: $1.1 billion.**
  First discovered by using holes in Microsoft Outlook on March 26, 1999. Melissa worm shut down Internet mail networks that were blocked by the worm propagating corrupted e-mails. When the original Melissa version was executed, a macro virus was used to spread to the first 50 addresses in the Outlook address book of the user. If Internet connection or Outlook were not available, however, it might copy itself to other Word documents and try to transfer those documents via e-mail, exposing potentially sensitive material [5].

- **I LOVE YOU (2000)**
  **Estimated damage: $8.75 billion**
  On May 4, 2000, the ILOVEYOU worm struck. It came as an email attachment. In order to read a love, note the note requested readers to press on an attachment. The attachment included a Visual Basic program that was interpreted as a

command by Microsoft Outlook and executed. Quite soon, the worm travelled around the globe, impacting the British Parliament, the U. The Congress of S., the U. Air Power of S., and numerous corporations and associations. Filters to block the mail were rapidly created and installed, but the filters were evaded by a spate of copycat worms in the next few days. (for instance, one named "JOKE" and another with an invoice that would be paid to the credit card of the recipient) [6].

- **Code Red (2001)**
  **Estimated damage: $2.6 billion**
  On July 13, 2001, Code Red was a digital worm which was observed on the Internet. Computers running Microsoft's web server IIS have been targeted. It was the first large-scale, mixed threat attack to strike enterprise networks successfully. When it targeted a weakness found by Riley Hassell, Eye Computer Security workers Marc Maiffret and Ryan Permeh first found and studied the Code Red worm. While the worm was launched on July 13th, on July 19th, 2001, the largest swarm of infected computers emerged. The number of infected hosts reached 359,000 that day, [7].

- **Sircam (2001)**
  **Estimated damage: $1.03 billion**
  The first programming worm to be sent to Microsoft Windows systems via email in 2001 was Sarkam. It begins with a text and has an attachment that with certain files from the infected device, will trigger the computer worm. The letter was bug transmitted in any way other than "I give you this file to get your opinion" due to a flaw in the wormTo all who later used the internet at the time and sent unsolicited emails to the worm containing this thread, this was a prank. They are influenced by machines running Windows 95, Windows 98, and Windows ME (Millennium). During its outbreak, Sircam was remarkable for the way it spread itself. Text files (usually .doc or .xls) on the infected device were randomly picked, virus-infected and emailed to the host's address book email addresses. The infected file is opened, and the target computer is infected with the default target [5].

- **SQL Slammer (2003)**
  **Estimated damage: $1.2 billion**
  This worm is a computer virus that, beginning on January 25, 2003 at 05:30 UTC, triggered Dos on some Internet hosts and significantly slowed down general Internet traffic. It spread exponentially, infecting, within 10 minutes, most of its 75,000 victims. The software did not use the SQL language, but it was named 'SQL slammer worm'; in Microsoft's flagship SQL Server database utility, it exploited two buffer overflow bugs [5].

- **My doom (2004)**
  **Estimated damage: $38.5 billion**
  My Doom first appeared in 2004 and is now known to be one of the fastest growing and most disruptive computer viruses of all time. The worm generated up to a quarter of all emails received worldwide at one point. It spreads from compromised Windows machines by scraping email addresses and spreads to victim contacts by submitting a new version of itself as a malicious attachment. The mechanism would repeat if the connection were opened, and My Doom spread to more people, roping them into a botnet that could execute Distributed Denial of Service (DDoS) attacks [5].

- **Sasser (2004)**
  **Estimated damage: $14.8 billion**
  Saucer is a worm that infects Microsoft operating systems on computers running insecure versions of Windows 2000 and Windows XP. By manipulating the device through a compromised port, Saucer spreads. Spreading without user involvement is also extremely viral but can also be effectively prevented by a correctly installed firewall or by installing system updates from Windows Update. Via its MS04-011 bulletin, which released a patch 17 days ago, Microsoft reported the saucer manipulation of a particular void. [5].

- **Zotob (2005)**
  **Estimated damage: $97,000**
- On Sunday, August 14, 2005, a new malware was released to exploit the Risks for plug-and - play (PNP) as illustrated in Microsoft Security Bulletin MS05-039. Quickly after the Microsoft Patch update on Tuesday, August 9th, the Sotob worm emerged. There are actually several worms depending on the same exploit code. Zotob, Esbot, Bobax, WORM RBOT, Spybot, SDbot, IRCbot are known as such. Zotob will affect offline Windows 2000 systems while TCP port 445 is available, while Windows 95 , 98, and ME users will not be affected by the latest versions of Zotob.

- **Stuxnet (2010)**
  Stuxnet is an extremely computer worm that is spreading and infecting computers using many zero-day Windows vulnerabilities. Its purpose was not only to infect provincial councils, but also to extract physical realities from the real world. It specifically opposes the centrifuges used by nuclear bombs and reactors to produce enriched uranium. The Infosec group first defined Stuxnet in 2010, but work on it possibly begun in 2005. Stuxnet does little or no harm to machines not interested in uranium mining, considering its unprecedented potential to propagate and its pervasive infection rate. When a device is compromised, it tests if the computer is connected to particular models of Siemens-manufactured programmable logic controllers (PLCs). PLCs are the way devices, like uranium centrifuges, communicate with and monitor industrial machinery.

- **Welchia worm (2013)**
  Welchia, also known as the Nachi worm, is a computer worm that, similar to the Blaster worm, exploits a flaw in the Microsoft Remote Procedure Call (RPC) application. Unlike Blaster, though, it first scans for and deletes Blaster if it exists, then attempts to download and install Microsoft security patches that will avoid further Blaster contamination, so it is known as a helpful worm. Welchia disabled Blaster successfully, but Microsoft reported that their protection patch was not always effective in implementing it. These worm-infected machines may be exposed by growing security bugs in the Microsoft Windows machine code (ports TFTPD.EXE and TCP on ports 666-765, and the RPC buffer on port 135). Access to infections includes instructing the system to build a remote shell and to delete the worms using TFTP.EXE [8].

- **Win32. IRCBot (2014)**
  Backdoor, backdoor. Win32.IRCBot, W32.Mubla (Symantec), W32 / IRCBot-WB (Sophos), and Backdoor (also known as W32 / Checkout (McAfee). Win32.IRCBot.aaq (Bydoon Centre) is a backdoor computer worm spread by MSN Messenger and Windows Live Messenger. The worm clones itself into a Windows device folder while installed on a PC, generates a new file seen as "Windows Genuine Advantage Validation Update" and becomes part of the automated initialization of the machine. Secondly, it tries to give itself to all MSN contacts by creating an attachment called 'photos.zip.' If this file runs, the worm will be built on the local PC [8]. The Win32.IRCBot worm creates a backdoor server which allows a remote attacker using an Internet Relay Chat channel to gain access which power over the machine. This allows for the delivery to a hacker of classified information.

In 2001, the fourth wave of new worms originated and continues today.
Worms such as Code Red and Nimda are depicted, showing faster spread and a new degree of complexity, including

- Blended attacks (combined infection vectors)
- Attempts at new infection vectors (Linux, peer-to-peer networks, instant messaging, etc.)
- Dynamic code updating from the Internet
- Dangerous payloads
- Active attacks against antivirus software.

Although malicious in nature are all the computer worms mentioned above in the time series, not all worms are supposed to be harmful. Such viruses are commonly referred to as "beneficial viruses" or "antivirus" viruses because they target and disinfect other viruses from the networks they have infiltrated. The Den Zuko boot virus37, which was simply a worm that disinfected the Brain virus, is an early example of this. The Brain virus was a malicious code created in Pakistan that corrupted disk boot sectors such that it was not possible to access their content. Brain was the first PC virus that was developed, and MS-DOS was contaminated. The Nachi family of worms, which

terminated and removed the Blaster worm, then attempted to download and install patches to repair the Microsoft DCOM RPC vulnerability in the host system, is another more resentful instance of this action.

## 4. Future development in the area

In the future, we are expected to see increasingly complex worms called "Mega Worms." These worms will implement complex routines with polymorphic and metamorphic behaviour that will allow use of obscuration of the entry point. The latest developments in typical worm production areas do not seem to move us instantly in the direction of the "Mega Worm," but they are steadily obtaining them [9]. The new batch of worms trying to use these behavioural strategies is an example of Spybot. KEG. It is regarded as a dynamic vulnerability detection worm, and it sets high criteria for all programming worms. Spybot. KEG has managed to stay below the radar of most people as it causes no harm, and only reports found vulnerabilities through IRC channels back to the author. Security researchers have already seen the introduction of many versions of another complex worm called Mytob every single day. A phishing trick in the form of a bogus URL referring to a web site that hosts the code of the worm has recently been included in this worm.

Other modern advances in worms include the worm Cabir. The first worm that can invade cell phones is the Cabir Worm. Cabir tends to be a so-called "proof of concept" worm that involves social engineering to accomplish its goal, but once a phone is compromised, it unlocks either time the phone is started, checks Bluetooth-enabled phones nearby, that transmits a copy of itself to every compromised phone it finds. Those designed to spread through instant messaging (IM) are the most popular and instantly dangerous worms that seem to be emerging. Although old but lesser-known worms, such as the Hello worm, have been used to extend Microsoft's Man Messaging, the next big bang with more promise seems to be the new worm community using IM. We can see that there are about 60 identified IM risks if we take a closer look at this threat, and the essence of IM threats involves SPIM (spam mail instead of IM) and phishing attacks. [9].

Yellow Fever is another potential future threat and may evolve into the next "Mega Worm" epidemic. Yellow Fever is an evolved I with some very fascinating traits, showing that the computational sophistication of modern wild I is far from what can be achieved. A Brief virus description: As a device utility, the worm installs itself. It lists all running programs searching for its target (Outlook) at launch. The process for infection is very interesting: the virus has a tiny built-in debugger that is used to bind to the host. Then, it impersonates the host and e-mails itself, using its own "SMTP" engine. "Yellow Fever" is not polymorphic, so a poly-engine might be added to it. The virus will penetrate many of the firewalls at the user level, but it has not been programmed for dissemination. While complex, these worms have not been changed to the point that they can inflict any serious damage, although that could change at any time [10].

As we have noticed, the speed of dissemination for worms is only restricted by their ability to locate new hosts. In the case of Code Red, any IP address in the world searching for compromised networks took about 14 hours to ping, while in the case of Slammer, it only took 20 minutes. According to a Symantec simulation, a similar hazard

targeting IM could lead to the infection of half a million systems in just 30 seconds. This is because the worm will already have a list of compromised computers found on the I d" lists of users. In order to identify compromised devices, any new worm using IM does not have to use time-consuming techniques. An IM worm can do a great deal of harm once within a compromised organization, as it would circumvent all current security protections.

Will the next big epidemic of worms not even include computers? Is the epidemic going to be a recent discovery of conventional methods of dissemination or will it come from emerging places like IM? No matter what form it uses to replicate, history has taught us that it is only a matter of time before we see the next big worm epidemic.

## 5. How to prevent

There are some protective steps you should take to protect your machine and your network from worms on a daily basis. The fundamental strategies for stopping machine worms and viruses are as follows:

1. **Install good anti-virus software**
   The first security step for the protection of machine worms and viruses is antivirus software. It is a software that defends against viruses, worms, Trojan horses, and malware on your computer. It scans every file on your computer and allows your computer system to avoid harm. Most users use free anti-virus software or the following protection software for Windows, which is not bad but ineffective in safeguarding the device.

2. **Do not download untrusted email attachments**
   When you receive an email from an undisclosed source with an attachment package, it can be a fraudulent email. If you download and open the file, the attachment file will contain a malicious script, and then the malware will run and infect your machine.

3. **Never download software from unreliable sites**
   Viruses are embedded in archives or applications, and if you download software, apps and other content from unknown places, it reaches your computer. Cyber security authorities advised that the apps and services be downloaded only from trustworthy sources, but our typical habit is that the services is downloaded without verifying the web or not.

4. **Keep all software updated**
   You must ensure that all the software you use is upgraded with the new upgrade, from anti-virus software to operating systems, for example. Staying safe from computer viruses and worms is the key justification for downloading and updating the new update of software. Old versions of software can have certain glitches or flaws in the source code, and when the new version of software is released, these types of security flaws are typically patched.

5. **Never open suspicious email attachments**
   Whenever you launch email attachment files with .exe, vbs, shs, pif, cmd, etc. extensions, there is a possibility to infect your computer with a virus. These kinds of extensions are never used in regular file attachments for your kind of material, but they are also used by viruses and worms. Any other attachments can include double-extension executable code, such as hi.doc.exe or name.txt.vbs, and if you open such types of files, the device would be corrupted with viruses.

6. **Regular scan your computer**
   Scanning your computer regularly with antivirus software is one of the fastest and safest ways to avoid machine worms and viruses. You can first search the whole machine after you have installed anti-virus software. If your enabled anti-virus program is capable of automatically scanning files or folders, activate this function at the right time.

7. **Use a firewall**
   A firewall is a security method intended to track incoming and outgoing network traffic and secure the system based on security laws. The key aim is to create a framework for the defines of cyber-attacks across internal and external networks.

## 6. Conclusion

This report discusses how computer worms evolved from the past to the present, and what could happen in the future. It also studies how computer worms came into the world, how much damage they have done to networks, and their lifestyle, classification, and what needs to be done to get rid of these computer worms. This task will make it clear that the computer worm is very dangerous. We can also understand that computer worms have done great harm to the computer world.

# 7. References


[1] Erbschloe, Michael (2005). “Trojan, worms, and spyware: a computer security professional’s guide to malicious code.” Burlington: Elsevier Inc.

[2] Kushner, David. "The Real Story of Stuxnet" ieee.org. IEEE Spectrum. Retrieved 25 March 2014. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/

[3] “The Morris worm,” *Fbi.gov*, 02-Nov-2018. [Online]. Available: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

[4] Morris Worm “history of computer worms [online] Available at http://www.spamlaws.com/history-of-worms.html

[5] B. Hephaestus and H. Books, *Articles on computer worms, including: SQL slammer, code red (computer worm), blaster (computer worm), code red II (computer worm), doomjuice (computer worm), Sasser (computer worm), dabber (computer worm), bolgimo, welchia*. Hephaestus Books, 2011.

[6] “I love you”: How a badly-coded computer virus caused billions in ...”. [Online]. Available: https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html.

[7] “Code Red: *Worm Assault on the Web - Scientific American*”. [Online]. Available: https://www.scientificamerican.com/article/code-red-worm-assault-on/.

[8] Cliff Changchun Zou, Weibo Gong, Don Towsley, “Code red worm propagation modeling and analysis” *Conference on Computer and Communications Security,* Proceedings of the 9th ACM conference on Computer and communications security

[9] “Future-Worm! - Wikipedia”. [Online].
Available: https://en.wikipedia.org/wiki/Future-Worm!

[10] Tang, Y, Luo J, Xiao, B & Wei G (2009). “Concept, characteristic, and defending mechanism of worm.” IEICE TRANS. INF. & SYST.’09, vol. E92-D, No. 5, (pp. 799-809). The Institute of Electronics, Information and Communication Engineers.