A Brief Survey Of Crypto Virology And Worms

[1]Dr. Varun Tiwari, [2]Dr. Tanvir A. Abbasi, [3]Dr. Kusum Lata Bharti
[1]Associate Professor, [2]Professor, [3]Associate Professor
Comm-IT Career Academy, (Affiliated GGSIP University),

Abstract - Today there are vast quantities of issues because of infection assaults with the goal that counteract key to effectively securing against them. There are a few clients use to assurance systems need to remember the potential force and many-sided quality of infections that are simply around the spot. Numerous quick spreading worms, for example, Skype worm, Flame worm and My fate worm is accustomed to contaminating PC document and access remotely arrange effectively and harm email and so forth same as like a brilliant grub like a mealworm. Hardly any systems and cryptographic apparatuses are utilized to discover the infections and worm in the previous years, we can go over some that use cryptographic instruments in their malignant action. Yet, couple of years' prior that disturbing property, joined with the speed of the purported "super worms", is investigated in the present work. Recommendations for countermeasures and future work are given.

Keywords - Bug, Grubs, cryptography, crypto virology, encryption, worms.

---

1. Introduction

Today Computer assailant is utilized high component and quick assault instruments, for harming firewalls and Storage documents and organizer in the PC. Numerous high security PC patterns or system are accustomed to keeping this sort of assaults utilizing worms. Worms is one of the four most disturbing kinds of the present assaults. The most striking occurrences that caused such concern incorporate the flare-ups of Code Red, Code Red II, Nimda, and, all the more as of late, Linux slapper worms. Each of the four worms were noted for their exceptional proliferations speeds; be that as it may, harm astute, they were evaluated as a low danger. Such an error between the levels of spread strategies and dangerous capacities as instantly spotted, and a few intriguing works were created that (occasionally as well

inwardly) put the circumstance in context and investigated the points of confinement of damaging capability of quick spreading, coordinating malignant substances. Be that as it may, this potential turns out to be considerably all the more overpowering when one endeavors to join the quickness of the worms with the savagery of some infections from the past. Cryptography, as some call attention to, is here and there thought of as a science that provisions us with devices to implement respectability and secrecy; nonetheless, its undoubted qualities is utilized to assault these same properties. Information erased by few of the infections or worms is to recoup once more. This paper investigates the mix of quick worms and cryptovirologic infection procedures. Initially, in Section 2, we give a study of works portraying the Skype worm, Flame or Sky
wiper worm and My fate worm. At that point, in Section 3 we clarify Crypto virology and potential harm that should be possible by infections with cryptographic capacities. In Section 4 is devoted to additionally harm appraisal also, the counter measures to the issue that we propose. At last, Section 5 is finish of the thoughts illustrated in this paper.

2. Overview

2.1 Skype worm

This worms belongs to Dorkbot family of malware and that comes using the internet communication channel in October 2012 and sends a message like "is that your new profile picture?". This type of worms is infected user's contact list and attempting to entice fellow this worm user into click on the particular link, download and install this worm on user computer immediately. Another forms of Dorkbot family, this worm opens an entrance on infected computers, allowing access data for remotely access area. This worm also installing a ransom ware, where the malware creep up to lock a user out of being able to use their computer and demands to pay several lacs of Rupees within a limited time frame otherwise deleted their files immediately.

Computers infected with this worms may also receive a malware message for claimed that computer has been rummage-sale for prohibited activity and user will be reported to centralized establishments unless a payment is finished within a limited of time. This worm is used internet communications platform, for hackers to distribute a "worm" that infects Computer and Laptop. When the users click on an instant message oral communication "is that new profile pic?" they unintentionally download a file containing a Trojan horse malware file. When you click that malware infected files then this worms or Trojan horse enter the computer and allowing hackers to hijack infected PCs and recruit them into a "botnet army". Users can be locked out of their machines and held to ransom. Sophos, is an IT Company says that the modern worm outbreak this network highlights the rank of proactive virus protection. This virus or worms cannot infect Sophos users who were proactively protected against the threat without requiring an update. W32/Pykse-C worm is directly involve to Skype's chat system using a different languages such as English, Russian and Italian. Recipients of the chat messages are invited to click on a link to what they believe will be a .JPG picture, but is in fact a downloadable executable.

Fig-1: Image shows infected user Villu Arak by the Skype Worm

This worm contaminated PC and communicates something specific by the client contact list and send clueless message when the snap by the client on the connection and download and introduce the malware payload document. Contaminated or captured PCs (tainted by Skype worms) said in an announcement: "It considers the client encounter important, especially with regards to security.
we know about this malignant action and are working rapidly to ease its effect".

"We intensely say advancement to the most recent Skype form and applying new refreshed security includes on your PC. Botnets are much of the time used to base dispersed dissent of administration (DDoS) assaults - pushing sites disconnected - to run spyware or to send spamming messages. The topic about the risk has made numerous clients careful about tapping on abnormal looking connections posted by means of interpersonal interaction locales, which may have provoked the Computer crooks of this most recent assault to switch methodologies. "The peril is, obviously, that Skype clients might be less in the propensity for being suspicious about connections sent to them than, say, Facebook clients," said Sophos' senior innovation advisor Graham Cluley. A worm that keeps Windows pc clients out of their PCs except if they pay a $200 recover is quickly spreading by means of Skype.

That worm is exploiting the Skype API to garbage out messages like the one beneath: is that your new profile pic? http://goo.gl/[REDACTED]?img=[USERNAME] Clicking on the dubious connections prompts the download of a compress documents (differently called skype_06102012_image.zip or skype _08102012_image.zip) that holds executable records recognized by Sophos hostile to infection items as Troj/Agent-YCW or Troj/Agent-YDC.

The trojan steed entered a Computers and permitting remotely get to and the programmer control the tainted documents and organizer and speaking with a remote server by means of http. Presently execution of malware duplicates itself to %PROFILE%\Application Data\Jqfsfb.exe and sets the auto begin mode empower: Earlier you know it, your passwords could be stolen, your PC could be enlisted into a botnet (the malware is a variation of the Dorkbot worm) and you could have succumbed to a ransomware assault. The risk can likewise might be by means of USB sticks, and different visit informing conventions The peril is, obviously, that Skype clients have been less in the propensity for being suspicious about connections sent to them than, say, Facebook clients. keep in mind forget to be suspicious of spontaneous unusual messages sent to you by your online companions.

Refresh: A Skype delegate individual reached Naked Security to give us the accompanying articulation:

"Skype considers the client encounter important, especially with regards to security. we know about this malignant movement and are working rapidly to alleviate its effect. we firmly prescribe moving up to the most up to date Skype form and applying refreshed security includes on your PC. moreover, following connections – notwithstanding when from your contacts – that look odd or are surprising isn't it was."

2.2 Flame or Sky wiper

Another most intense malware all the more usually alluded to as Flame (or Flamer), in spite of the fact that a couple of security masters group as: Skywiper, or sKyWIper, is a standout amongst the most multifaceted malware stressing to date, the whole size of in excess of 30MB when its at least 20 units and modules have been introduced. it can gather record broad framework data on a tainted machine, and it is observing and parcel sniffing usefulness and also secondary passage capacities that empower

digital aggressors to trigger, refresh or eradicate the malware utilizing by the summon. This malware had been available for use for no less than 2 years before being identified, principally focusing on nations in the center east, and Skywiper is accepted to have been made and led with "country state bolster" because of its abnormal state of many-sided quality and focused on territory of core interest. Fire, otherwise called Flamer, sKyWIper, and Skywiper, is measured pc malware found in 2012 that assaults PCs running the Microsoft Windows working framework. The program is being utilized for focused digital undercover work in center eastern nations. Its disclosure was declared on 28 may 2012 by MAHER Center of Iranian National, Christos Papani kolaou (known as a programmer and pc developer), PC Emergency Response Team (CERT), Kaspersky lab and CrySyS Lab of the Budapest University of Technology and financial matters. The remainder of these expressed in its report that Flame "is positively the most modern malware we experienced amid our training; ostensibly, it's the most complex malware at any point found. "Fire can spread to different frameworks over a nearby system (LAN) or by means of USB stick. It can record sound, screen captures, console movement and system activity. The program additionally records Skype discussions and can transform contaminated PCs into Bluetooth reference points which endeavor to download contact data from adjacent Bluetooth-empowered gadgets. This information, alongside privately put away archives, is sent on to one of a few charge and control servers that are scattered the world over. The program at that point anticipates further directions from these servers. As per gauges by Kaspersky in may 2012, Flame had at first tainted around 1,000 machines, with casualties including legislative associations, instructive foundations and private people. Around then 65th of the contaminations occurred in iran, Israel, Palestine, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt, with a "gigantic lion's share of focuses" inside Iran. Fire has likewise been accounted for in Europe and North America. Fire underpins a "murder" order which wipes all hints of the malware from the PC. The underlying diseases of Flame quit working after its open introduction, and the "murder" order was sent.

Fire was recognized in may 2012 by MAHER Center of Iranian National cert, Kaspersky lab and CrySyS lab (Laboratory of Cryptography and System Security) of the Budapest University of Technology and financial aspects once Kaspersky lab was asked by the assembled countries International Telecommunication Union to examine reports of an infection influencing Iranian Oil Ministry PCs. As Kaspersky lab examined, they found a MD5 hash and filename that seemed just on client machines from center eastern countries . once finding more pieces, specialists named the program "Fire" after one of the principle modules inside the toolbox FROG.DefaultAttacks. An Install Flame]. As indicated by Kaspersky, Flame had been working in the wild since in any event Feb 2010. CrySyS lab revealed that the document name of the fundamental part was seen as ahead of schedule as Dec 2007. be that as it may, its creation date couldn't be resolved straightforwardly, as the creation dates for the malware's modules are dishonestly set to dates as right on time as 1994.

PC experts consider it the purpose behind a strike in Gregorian date-book month 2012 that influenced Iranian specialists to disengage their oil terminals from the web. At the time the Iranian Students news association implied the malware that caused the attack as "Wiper", a name given to it by the malware's creator. Nevertheless, Kaspersky lab assumes that Flame may be "an alternate illness out and out" from the Wiper malware. Due to the size and complexity of the program—depicted as "twenty times" more confounded than Stuxnet—the lab communicated that a full examination could require as long as ten years. We have finished an examination in a joint exertion with a couple of social occasions related with scene response since we were advised of the malware sKyWIper. a bit of these social events included may need to remain obscure; in this way, references in the record are deliberately wrong to keep up a vital separation from recognizing verification of the wellspring of a few information, data, test, code, model, et cetera.

sKyWIper is exorbitantly complicated, making it difficult to be totally inspected with our compelled resources and time. Along these lines, our examinations focused on the "ground breaking strategy", endeavoring to get a first comprehension into the limits, lead, encryption, data storing, spread and exchanges of the malware. essentially more work is required to totally appreciate the inconspicuous components of the action of the malware; in any case, as much research/picture information remains in the code, a distinct examination is from every angle reasonable with additional benefits and time. The filename WAVESUP3.DRV was first seen on Dec 5 2007 in Europe by the Webroot social order. Since, it has been found in the going with geographical districts:

- Europe on Dec 5 2007
- The United Arab Emirates on apr 28 2008
- Islamic Republic of iran on Mar 1 2010

Record sizes

The going with record sizes have been seen:

- 1,153,536 bytes
- 991,232 bytes
- 975,872 bytes

The make date letter header information of the malware uses fake date information for its archives; along these lines we can't totally perceive the goal structure's infection time. regardless, the SQLite related bit of mssecmgr.ocx contains some shape time info(more about the parts later):

"Unidentified frame, Aug 31 2011 23:15:32 31.....Aug 31 2011 23:15:32"

The going with string shows SQLite frame information, found in the memory dumps:

2010-01-05 15:30:36 28d0d771076111 4a44a1a3a425a6883c661f06e7 NULL

It relates to SQLITE_VERSION "3.6.22" (some bit of the supply code)

Moreover, there is a reference "1.2.3", and we feel this implies zlib interpretation number conceivably used as a piece of SQLite tables.

2.3 Mydoom

Mydoom is accounted for to be the most harming infection or worm ever free, took after nearly by Sobig. It additionally set records for spreading capacity. My fate, otherwise called W32.MyDoom @mm, Novarg, Mimail.R a nd Shimgapi is a PC worm influencing Microsoft Windows. it was first located on January 26, 2004. It turned into the quickest spreading email worm ever (as of Jan 2004), surpassing past records set by the so enormous worm and I LOVEYOU. My fate seems to have been authorized by email spammers in order to send garbage email through tainted PCs. The worm contains the instant message "Andy; I'm simply doing my activity, not all that much, sad," persuading that the worm's maker was paid. At an opportune time, a few security firms communicated here conviction that the worm began from a software engineer in Russia. The genuine creator of the worm is obscure. Theoretical early scope held that the main motivation behind the worm was to execute a conveyed refusal of-benefit assault against SCO gathering. 25 percent of Mydoom.

A-contaminated hosts focused on www.sco.com with a surge of activity. Exchange squeeze guess, impelled alone cases, held this implied the worm was made by a linux or source supporter in countering for SCO Group's disputable lawful activities and open articulations against linux. This hypothesis was dismissed instantly by security specialists. From that point forward, it has been similarly dismissed by law requirement specialists exploring the infection, who credit it to composed online wrongdoing posses.

Introductory examination of Mydoom proposed that it was a variation of the Mimail worm—thus the substitute name Mimail.R—provoking hypothesis that similar people were in charge of the two worms. Later investigations were less indisputable with regards to the connection between the two worms. Mydoom was named by Craig Schmugar, a representative of PC security firm McAfee and one of the most punctual pioneers of the worm. Schmugar picked the name in the wake of seeing the content "mydom" inside a line of the program's code. He noted: "It was clear at an early stage this would be huge. I thought having 'fate' in the name would be fitting.

The MyDoom worm can influence a zombie of your PC To worm makes had zombie armed force to assault SCO site Sophos specialized help has cautioned clients of the W32/MyDoom-A which is spreading generally over the web. The MyDoom worm (otherwise called Novarg or Mimail-R) spreads by means of email, utilizing an assortment of specialized sounding headlines and connection names. On the off chance that the connected record is propelled, and the worm initiated, the tainted PC's hard circle is gathered by the worm for more email delivers to send itself to. The worm opens an indirect access onto tainted PCs that enables programmers to obtain entrance. The worm likewise spreads by means of the KaZaA document sharing system, and dispatches a refusal of administration (DoS) assault from contaminated PCs (known as "zombies") against SCO's site in the vicinity of 1 and 12 february."

MyDoom is not at all like numerous different mass-mailing worms we have found before, in light of the fact that it doesn't attempt to allure clients into opening the connection by offering appealing pictures of VIPs or private messages," said Graham Cluley, senior innovation advisor for Sophos. "

My Doom can act like a specialized sounding message, asserting that the email body has been placed in a connected document. Obviously, on the off chance that you dispatch that document you are conceivably putting your information and would straight be able to under the control of programmers." "When the My Doom worm advances itself through email, it conceivable make its connection in either Windows executable or compress record organize.

it is conceivable the worm's creator did this trying to sidestep organization channels that attempt and square EXE records from achieving their clients from the outside world," proceeded with Cluley. Sophos has distributed sanitization examination and insurance against W32/My Doom-A.

An independent putting utility cleansing accessible. Venture Manager Customers are naturally ensured at the season of their next planned refresh. Contaminated document through mydoom.

3. Crypto virology

As an endeavor to diagram more solid risk the quickly spreading worms convey, we will quickly depict a recent report on crypto virology. It exhibits a fascinating turn on cryptography, demonstrating its conceivable malevolent applications. The creators begin off by dissecting a few infections with cryptographic abilities that have been seen amid that time. LZR, AIDS Information

Trojan and KOH were infections quickly saw on a few PCs in 1994-1996 that displayed a few qualities that the creators sum up to the principle thought of the paper. The fundamental objective is to influence a casualty to have subordinate upon the infection. They characterize a property of a high survivability of an infection, which can be abridged as "you murder the infection, you lose the information". As a nearby estimate to an exceptionally survivable infection, they propose a situation where an infection influence the casualty to have relied on the originator of the infection. Such infection would scramble some touchy information with some open key, yet it would not contain a private key to unscramble it, hence making any endeavors to recuperate the information by examining its source code futile. The originator of such infection would hold the way to the information, in this manner picking up control over the casualty. Cryptovirologic assaults abuse this reliance to the advantage of the infection originator. The creators consider two cases of such assaults, a reversible dissent of administration assault, and a data coercion assault. In a reversible foreswearing of administration assault, the infection is outfitted with a solid irregular number generator and a solid seeding system, and mounts an assault by producing an arbitrary session key Ks, and an arbitrary instatement vector IV. A basic cryptographic convention shapes the reason for the assault. The message {Ks, IV} is scrambled with the general population key of the infection's originator, bringing about figure content C. Next, the infection scrambles the focused on information on the casualty's framework utilizing Ks,IV, and a symmetric calculation. After fruitful encryption, the infection overwrites the first information. At last, the infection prompts the casualty's administrator to send figure content C to the infection's originator, acquire a decoded form of C, and recover access to their information by unscrambling it with Ks, and IV. We take note of that this assault is more productive with moderately little documents, since encoding an expansive record may uncover the infection and furthermore it entangles the trade procedure. Another fascinating sort of crypto virology assault we will portray here is the data blackmail assault. This sort of assault depends on exchanging access to some objective information in return for other information which is more important to the casualty that the infection figured out how to take a few to get back some composure of. The infection scrambles the touchy information on casualty's host as previously, and after that it ascertains a checksum of a (conceivably extensive) document focused by the assailant. The infection at that point prompts for the trading of figure content C from the past assault that currently likewise contains the checksum, and the focused on information, for the way to the seized casualty's information. Infection proprietor thinks about the checksum to the information got, and if truly is the information wanted, the key is discharged and the casualty securely recoups the information. The rest of the work is devoted to adjusting a crypto infection in such a way so it turns out to be exceedingly survivable. The creators propose disseminating parts of the private key with infection occasions, so entire recuperation is conceivable just if all casualties collaborate, and investigate the different game plans and capacities this approach conveys. We forget the greater part of this dialog, since we feel that the course of action in which the originator of the infection controls the information would be considerably more helpful with regards to quick spreading infections.

The creators depict a simple system of providing programmed input to the creator of tomb infections. So as to take the required information without straightforwardly associating with the casualty, the creator would need to catch one of the casualty's infection's posterity that would contain an encoded duplicate of the information. Be that as it may, they concede that such a situation is very improbable and wasteful, particularly considering the rates at which infections proliferated at the time the paper was composed. A few recommendations for countermeasures are really incorporated into the work. Conventional dynamic infection location and regular reinforcements are proposed. Another recommendation is strict control over cryptographic instruments.

Since incorporating every single vital instrument with the infection would make it extensive, wasteful and simple to identify, the infection really needs to depend on the ones incorporated with the casualty framework, and the creators contend that via precisely controlling such gets to, the infection can be vanquished. Nonetheless, they don't supply any situations of such control; moreover, they concede this would be moderately difficult to uphold.

3.1 Open Questions

As a generally ongoing improvement, a Linux. slapper worm seemed, by all accounts, to be the primary endeavor to execute an organized malevolent system. The Linux-based worm made a distributed system of contaminated hubs. Correspondence was fundamental, enabling the system to take in its own particular topology, and dispatch DDOS assaults as a solitary unit when instructed from a solitary remote area. Slapper missed the capacity to verify correspondence, and it was immediately contained, mostly because of the provoke reaction by influenced Red Hat Apache server directors. We take note of that in the Curious Yellow plan, facilitated contamination won't not be extremely helpful - divided stage appears an adequate technique to evade covered filtering. Notwithstanding, planned control and refresh components, as we expressed previously, open a large number of chances for vindictive movement.

4. Damage

Give us a chance to envision a cryptovirologic super worm. It would consolidate the proliferation speed of the Skype worm, or a Flame or Sky wiper worm, contingent upon the capacities of the maker; correspondence abilities of My fate, and cryptography-based malevolent payload. Customary dynamic infection identification, proposed as one countermeasure, would be defenseless against such worm, since the updates could be disseminated substantially quicker that the framework directors can clean their framework. The infection remains above water by continually re-tainting the entire Internet utilizing new zero-day vulnerabilities found by the worm proprietor. Notwithstanding the perception that as the worms gets more mind boggling, they turn out to be more powerless and simpler to subvert themselves, a group of exceptionally energetic specialists with a strong damaging arrangement can without much of a stretch deliver a blame free outline and execution of such a worm. Customary updates guarantee imperceptibility even from the Curious Blue worm, which endeavors to purify the casualties. Worm examples watch

plans of access control to cryptographic instruments on the casualties' frameworks and deceive them into enabling access to those devices. All endeavors to dissect the movement and find the worm proprietor fall flat, since all activity is limited - a large portion of the circumstances, it isn't even clear that a casualty is tainted; lastly, we can propose intermittent activity trades to counteract movement investigation. Regardless of whether a portion of these occasional trade messages are watched, it would not be clear if the message, which is, obviously, encoded, really contains some important date (like a refresh), or just is a placeholder message.

We take note of that the full plan, in which all cases of the worm and its maker remain totally mysterious, but then Communication happens on the general premise without uncovering the gatherings included, is yet to be created. In any case, it is shrewd to accept that such a plan can be actualized in the closest future and get ready for the most exceedingly bad. Visit reinforcements would be a to some degree powerful measure against the cryptovirologic assaults of the worm; in any case, remaining undetected for a significant lot of time and deliberately breaking down the data stream on the casualty framework enables the worm to seize the delicate information between the reinforcements. Along these lines, we can infer that none of the countermeasures introduced in the secured works would be a satisfactory reaction to the worm. Moreover, we watch that this worm would undermine the presence of the vast majority of the advanced installment plans too some declaration frameworks. E-money and endorsements can be in a split second subverted, and either exchanged for genuine cash, or same ecash, or for some delicate data.

4.1 Countermeasures

Aside from unclear counsel to play out the reinforcements and fix the frameworks on the consistent premise, there are a couple of things that we can recommend. In particular, for authentications and e-money plans, we can recommend putting away them in encoded frame, so that even if there should arise an occurrence of a disease, the worm would not have the capacity to tell that scrambled information from general documents which introduce no enthusiasm to it. Notwithstanding, that has all the earmarks of being a non-insignificant usage issue, since the casualty needs to some way or another get these, and the specific demand for them may lead the worm to the encoded renditions of authentications and e-cash. Despite the fact that they can't be stolen in encoded frame, regardless they can be subverted once the worm gets some answers concerning the idea of that information. One viable device to battle the crypto virology super worm that we imagine are mechanized reaction empowered Intrusion Detection Systems (IDS). In spite of the fact that cutting edge isn't by then yet, a productive course for research would attempt to create facilitated reaction empowered IDS's that rapidly create marks of obscure assaults and convey them to their associates previously the worm. Particular based IDS's that permit identification of obscure assault and robotized reaction systems are currently being produced at a few research destinations, including the University of California, Davis Computer Security Lab.

5. Conclusion

By dissecting the effective worm executions, we can infer that exclusive the absence of the reasonable harm procedure spared the Internet this time. The proliferation methodologies utilized as a part of genuine assaults were not the most well-thoroughly considered, either. Obviously, an organized and all around arranged assault can be significantly more crushing except if a few countermeasures are taken. In this work, we attempted to join the most eminent ongoing takes a shot at the quick engendering noxious infections with an intriguing work on infections with cryptographic abilities to investigate the degree of the conceivable harm that should be possible by such a mix. We investigated the inquiries that we felt these works left open. We additionally broke down recommended countermeasures to such a worm, and proposed a couple of countermeasures of our own.

6. References

[1] CERT Coordination Center, 2002 Overview of Attack Trends, http://www.cert.org /archive /pdf/attack_ trends. pdf, last accessed on December 4, 2002.

[2] Staniford S., Paxson V., Weaver N., How to 0wn the Internet in Your Spare Time, Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, 2002.

[3] Weaver, N., Potential Strategies for High Speed Active Worms: A Worst Case Analysis, **Error! Hyperlink reference not valid.**. pdf, last accessed on December 4, 2002.

[4] Young A., Yung M., Cryptovirology: Extortion-Based Security Threats and Countermeasures, IEEE Symposium on Security and Privacy, Oakland, CA, 1996.

[5] Chaum D., Security without Identification: Card Computers to make Big Brother Obsolete, Communications of the ACM, vol. 28 no. 10, October 1985 pp. 1030-1044.

[6] Rivest R., Shamir A., PayWord and MicroMint -- Two Simple Micropayment Schemes, 4th Security Protocols International Workshop, Cambridge, UK, 1996.

[7] International Telecommunications Union, Recommendation X.509 – the Directory Authentication Framework, 1993 [9] http://www.cert.org/advisories/CA-2001- 26.html, last accessed on December 4, 2002.

[8] CERT Coordination Center, CERT® Incident Note IN-2001-09, http://www.cert.org/ incident_notes/IN-2001- 09.html, last accessed on December 4, 2002

[9] CERT Coordination Center, CERT® Advisory CA-2002-27 Apache/mod_ssl Worm, http://www.cert.org/advisories/CA-2002- 27.html, last accessed on December 4, 2002

[10] Slashdot.org, Malicious Distributed Computing, http://slashdot.org/article.pl?sid=02/10/25/141 3220 &mode= thread &tid=172, last accessed on December 4, 2002

[11] BBC news for Skype Worm for Skype Targeted by 'worm' malware infecting Windows PCs by Microsoft. http://www.bbc.com/news/technology-19886241 , Microsoft acquired the Skype video chat service in 2011.
[12] Introduction about Skype worm. http://www.webopedia.com/TERM/S/skype_worm.html &safe=active
[13] Introduction about Mydoom worm. Attack this virus Mydoom to www. Sco.com Microsoft Site **Error! Hyperlink reference not valid.**
[14] Mark Sunner, chief technology officer at Message Labs told BBC News Online for Mydoom Worm Attacks. http://news.bbc.co.uk/2/hi/technology/3432639.stm
[15] Introduction about Flame or Skywiper worm. http://en.wikipedia.org/wiki/Flame (malware)
[16] Article for "Fanning the 'Flames' of Cyberwarfare" http://blogs.mcafee.com/business/security-connected/skywiper-fanning-the-flames-of-cyber-warfare
[17] sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks v1.05 (May 31, 2012) Cryptography and System Security (CrySyS).