International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 9, August 2016

ISSN: 2394-4404

A Short Review On Models Of Cyber War And Infectious Worms

Akshat

SRM University, Kattankulathur

Abstract: ***"Cyber Terrorism is at the convergence of terrorism and cyberspace ". These are a new and different form of attacks which produces worldwide chaos and violence accomplished through a computer often motivated by the government to confront a particular agenda, ranging from political, to social up to ideological. It may occur as asymmetrical treats with strategic ideas but is actually a large scale cyber warfare.***

Big Power houses of the world in the recent years, are characterizing intense activities towards cyberspace in terms of 'intrusion'. Also coined by the term of 'Improvement of Cyber Capabilities', a real-time cyber-attack consists of is injection of a malicious code or break through the cyber walls and causing harm which concerns large crowds and often the whole of administrable government.

Keywords: Cyber Terrorism, WWIII, Cyber War, Cyber Crime, Internet Security.

I. INTRODUCTION

Oxford dictionary of English defines Cyber War as 'the use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems'. Likewise, Cyber Terrorism is defined as 'the politically motivated use of computers and information technology to cause severe disruption or widespread fear'. Do they look similar? Both of these have a similar background of some agency or strong powerhouse backing up the attackers. Cleverly mixing up their malicious strategies with malicious codes that harm the society and the cyber community as a whole.

The Internet is the primary medium used by attackers to commit computer crimes. Worms' attacks are considered by network experts the highest security risk on computer network. Computers worms are built to propagate without warning or involving any user interaction, which will eventually lead to Cyber-attack. The Attacker uses a malicious worm as a primary tool to target software vulnerabilities. Cyber-attacks occur on a frequent basis and in a near-instantaneous manner. As the world becomes more connected, more machines and more people will be affected by an attack. A successful cyber war could inflict major damage on both a country's information infrastructure and its utility grids.

The Slammer worm, for example, exploited a vulnerability in Microsoft's SQL database software that led to cascading effects in our electronic infrastructure that were certainly not predicted earlier, According to ZDNet, a popular website among the cyber interests, South Korean ISPs and bank Automated Teller Machines (ATMs) were among other systems impacted by Slammer infections. As was also detailed by Yongzhen P et al., (2009) in their work; a delayed SEIQR epidemic model with pulse vaccination and the quarantine measure.

The Slammer worm also significantly degraded computer systems that control monitoring capabilities at the Davis-Besse nuclear power plant in Ohio. The most likely targets of cyber warfare are critical networks. Critical networks are those that if interrupted for significant portions of time (several days or several weeks or indefinitely) or perform erratically or occasionally would disrupt daily life. We can stop these crimes from happening by simply installing the best kind of internet security software available along with regular software updates, hardware permission settings, implementing latest server methods and using access restriction points such as a simple BIOS password to attaching a biometric scanner while logging in to their device. Along with software upgradation, regular and optimal hardware checks are also necessary. From checking on unguarded LAN entry ports to

leaked or unchecked systems and access points in the system such as an open Wi-Fi or unguarded administrator computer.

II. INTRUSION DETECTION SYSTEM

A network intrusion is any unauthorized activity on a computer network. Detecting an intrusion depends on the defenders having a clear understanding of how attacks work. In most cases, such unwanted activity absorbs network resources intended for other uses, and nearly always threatens the security of the network and/or its data. Properly designing and deploying a network intrusion detection system will help block the intruders.

Some Common types of Intrusion Detection include:

✓ NETWORK BASED INTRUSION DETECTION SYSTEM (NETWORK IDS)

Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting.

✓ HOST BASED INTRUSION DETECTION SYSTEM (HIDS)

Often referred to as HIDS, host based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior on a specific device. HIDS generally involves an agent installed on each system, monitoring and alerting on local OS and application activity. The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorized activity. The role of a host IDS is passive, only gathering, identifying, logging, and alerting.

✓ PHYSICAL INTRUSION DETECTION SYSTEM (PHYSICAL IDS)

Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection is most often seen as physical controls put in place to ensure CIA. In many cases physical intrusion detection systems act as prevention systems as well. Examples of Physical intrusion detections include Access Control Systems (Card, Biometric), Firewalls, Man Traps and Motion Sensors

SEIR

An e-epidemic SEIR (susceptible-Exposed-Infectious-Recovered) model, created for the mathematical representation and way of tackling the problem by Pei Yongzhen et al., (2009) in their paper a delayed SEIQR epidemic model with pulse vaccination and the quarantine measure has been explained here.

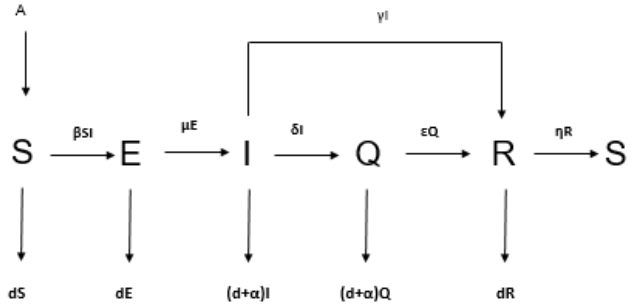

Figure 1

MATHEMATICAL MODEL FORMULATION

A population size $N(t)$ is partitioned into subclasses of nodes which are susceptible, exposed (infected but not yet infectious), infectious, quarantined, and recovered, with sizes denoted by $S(t)$, $E(t)$, $I(t)$, $Q(t)$, $R(t)$ respectively. The assumptions on the dynamical transfer of the population are depicted in the Fig. 1.

In the SEIQRS model, the flow is from the *S* class to the *E* class, *E* class to the *I* class, and then directly to the *R* class or to the *Q* class and then to the *R* class and as the recovery is not permanent in the cyber world, it again returns back to the *S* class.

EQUATIONS:

$S'(t) = A - \beta SI - dS + \eta R$
$E'(t) = \beta SI - (d + \mu)E$
$I'(t) = \mu E - (d+\alpha+\gamma+\delta) I$
$Q'(t) = \delta I - (d+\alpha+\varepsilon)Q$
$R'(t) = \varepsilon Q + \gamma I - (d+ \eta)R$

Parameters A, d, β represent the positive constants, and μ, γ, δ, ϵ, η, and α are nonnegative constants. The constant A is the recruitment rate of susceptible nodes to the computer network, d is the per capita natural mortality rate (that is the crashing of nodes due to the reason other than the attack of malicious objects), μ is the rate constant for nodes leaving the exposed class E for infective compartment, δ is the rate constant for nodes leaving the infective compartment I for quarantine compartment, $\alpha$is the disease related death rate (crashing of nodes due to the attack of malicious objects) constant in the compartments I and Q; γ, ϵ are the rates at which nodes recover temporarily after the run of anti-malicious software and return to recovered class R from compartments I and Q respectively; η is the loss of immunity rate constant.

Hence , in the above piece of information , we may see that though having all the theoretical aspects of a mass attack on a cyber-network in a secure space the implementation of which will not only help save us not only form the levels of worms but also planned and signaled single node attacks.

III. TEENAGE INTO CYBER CRIMES

With over thirteen million search results and more than one cybercrime being performed by a teen every hour, it is one of the most important and concerning issues of the new online

era. Often tempted by the excitement of the unknown or the image in the peer group. From changing the wallpapers of the school's systems to leaking confidential data, these teens might be a seed for a series of dark crimes which the future beholds.

With the increasing reach of computers every day , a new group of teens who spend most of their hours in front of codes , also known as 'script kiddies' , often take a path which not only harms the high school servers but also attacks the Fortune 500 companies. They do not restrict themselves to a certain field of data, and attack government agencies, social networking websites and large public databases.

Recent events show how young minds are becoming more active each day in the field of cyber-crime. As goes a recent newspaper report" Florida: Teenager charged with hacking into a school district's computer system and sending a threatening message to students and parents."

Also, the vulnerability of wireless networks to tech savvy teens was in the spotlight again. A handful of teen hackers brought down the mighty Twitter, just to prove it could be done.

Talking about the national statistics, In India, a final year engineering student was expelled from the college when he had logged in to the main servers and changed all the official data relating to the faculty.

But, here arises a very important question. Why are more and more teenagers attracted towards this sort of habit?

According to analysts and Cyber Experts, a few are listed below.

✓ CYBERCRIMINALS ARE THE NEW ROCK STARS

In a 2008 interview with the BBC, Mark Bevan ('a reformed hacker') gave an explanation as to why more teenagers are becoming hackers: "The aim of what they are doing is to get the fame within their peer group". This not only shows the growing trend but also shows the importance of fame and name along with peer pressure in schools today. [8]

✓ EASY CRIME, BIG REWARD

Other explanations also exist to account for the distinct increase in youth cybercrime. Many suggest that youths are committing cybercrimes simply to reap the large illicit rewards that it can provide. Unfortunately, the advent of new internet technologies has given rise to a situation in which opportunistic youths have now been given a means to commit crimes that were commonly perceived to be massively disproportionate to their age. Before the internet era, youth crime was more or less limited to minor offences such as shoplifting and other simple thefts. However, cybercrimes committed by youths can include anything from large-scale software piracy to multi-million dollar credit card fraud.

✓ MALICIOUS CURIOSITY

There are also many youths that actually possess highly technical skills, and are using these skills to increasingly commit serious cybercrimes that reap little to no personal gain. For example, a Canadian newspaper stated how a student was charged with hacking into a school board website and exposing the passwords of 27,000 fellow students. Furthermore in September of 2015 according to a newspaper report, a 17 year old Australian was found to be the creator of a computer worm that crippled Twitter for several hours. The worm exposed a flaw in the microblogging site which allowed other hackers to send unsuspecting users to Japanese pornography sites. When asked to explain why he hacked Twitter, the student's response was 'To see if it could be done.'[4]This answer sums up the major motivation behind many of the more highly skilled young cybercriminals, in particular the young 'black hat' hackers – they simply do it to see if they can, without any thought to the real-world consequences. If they break through a system and cause large amounts of financial damage in the process, it is the system's fault for being 'weak'.

✓ AN ETHICAL DEFICIT [4]

Teenagers often challenge a particular section of the law and exploit it taking the full advantages of the norms and freedom present in it. For example, a few years back, a teen could only be sent to jail for a cybercrime if he was above eighteen.

As The government's cyber cell states,

Motive behind the Crime could vary from greed to power. These attackers have shown traits of power, revenge and curiosity. These people when questioned, often refer to various forbidden contents they had heard/ read of and try to explore the validity of the piece of information they have just gathered. Though maximum cases involving teens and young minds do not portray any negative mindset, but yes, destructive mindset like theft and revenge are not a rare phenomenon to be exhibited.

IV. CASE STUDY

CYBER CRIME IN INDIA

If crime figures released by NCRB are any indication, more and more teenagers and youths are taking to cybercrimes in the state. Of those arrested for violation of Information Technology Act, majority are teenagers or people under 30 years of age. According to the NCRB's national report, a total of 147 cases were registered under various sections of IT Act in Rajasthan in 2012 compared to 122 in 2011. Of these, Jaipur alone reported 69 cases of IT Act violations.

India stands 5th among cybercrime affected countries of world after US, China, Japan and UAE. This is an alarming call for all the cyber experts as India has most of its population under the age of 25 (National Census 2015) and if even a small fraction of this set of budding future get into the wrong set if codes, they would create a havoc.

With regards to cybercrimes, the State of Andhra Pradesh tops in India. 349 of the total 1,791 cybercrime cases registered last year 2011 were reported from this state. Maharashtra followed closely with 306 cases. When we

examine the stats on a more minute level, Pune is third in instances of cybercrime. These when reflected by the National Crime Records Bureau's reports show how major and important issues they are and they need to be suppressed. Ninety persons were arrested for violation of IT Act last year. Of them, 13 were minors, 55 were in the age group of 18 and 30 years. Youngsters indulged in cybercrimes to get a kick, a police officer said. "Most of them were not even aware that hacking into someone else's account on a social networking site is a crime. They did it either for fun or to take revenge after their relationships went sour," the officer added. [10]

MODERN DAY EXAMPLE (GLOBAL)

A new Cyber warfare tactic was came into use shortly after Julian Assange of WikiLeaks was arrested. Allies of WikiLeaks started attacking different entities perceived to be threatening to WikiLeaks. [6] This was one of a kind of an attack. Several large financial companies saw their servers fail. These attacks were called Distributed Denial of Service (DDoS) attacks. The idea is to overwhelm Internet servers with so much traffic that they cannot respond to it all. Often DDoS attacks are launched using botnets – collections of thousands or ordinary computers that have been compromised by computer viruses so that other people can control their actions. It is also possible to imagine thousands of people doing the same thing by acting together in a coordinated way.

Speaking of viruses, these computer invaders represent another way to break into an Internet server. If a machine is compromised by a virus or a worm, it would allow someone to copy out data on the machine, or log all the keystrokes typed into the machine (which would include account names and passwords).

One of the most amazing worms seen to date is called Stuxnet. Apparently it is a cyber warfare tool designed to damage certain types of industrial machinery, and is specifically thought to be directed at Iran's ability to enrich uranium. The virus attacks computers that control machines found in factory settings.

V. CONCLUSION

What happens in the next decade is going to be a pretty interesting story. With many of these teens becoming Security experts battling their own peers who chose to have the same malicious thoughts would heap the age of internet become a lot more secure and reliable. It would trigger a new revolution into the mindset of the people who look at the internet as a vital aspect of their life. But will the new age of teens be able to start a cyber-war? They can. And if not stopped they will. Will this affect the common man? It will, and it will bad. It can vary from leaking of sensitive information stored by organization to complete blocking of web services in a region. These in worse cases can also leads to the activation of unwanted arms or chemicals leading to catastrophic results. If a cyber-war triggers, it will not be only limited to computers but also to the world outside computers from transport to production industries.

REFERENCES

[1] Pei Yongzhen, Liu Shaoying , Gao Shujing , Li Shuping , Li Changguo. (2009) A delayed SEIQR epidemic model with pulse vaccination and the Quarantine measure.
[2] Jacqueline B. Helfgott. Criminal Behavior: Theories, Typologies and Criminal Justice.
[3] Samuel P. Liles. Cyber warfare as a form of conflict: Evaluation of models of cyber conflict as a prototype to conceptual analysis, *Purdue University*
[4] Pierluigi Paganini (2013). Cyber warfare – Why we need to define a model of conflict?
[5] Bimal Kumar Mishra, Samir Kumar Pandey, (2014). Fuzzy epidemic model for the transmission of worms in computer network.
[6] Mohammad Iqbal, (2004). Defining Cyberterrorism.
[7] Ruwantissa Abeyratne, (2011). Cyberterrorism: The Next Great Threat to Aviation.
[8] Mudawi M. Elmusharaf, (2004). Cyber Terrorism: The New Kind of Terror.
[9] Cyber Crime Blog. Criminal law in the virtual context.
[10] Bimal Kumar Mishra and Apeksha Prajapati (2014). Cyber Warfare: Worms' Transmission Model.