Modeling of Computer Viruses

Yuuzou Kobayashi s1070082 Supervised by Hiroshi Toyoizumi

Abstract

We studied that CodeGreen is available for killing CodeRed II or is unavailable in this paper. First, we made CodeGreen infect one of two PC prepared and observed CodeGreen infection. We let the data observed CodeGreen infection make the stochastic model with Birth and Death Process [1]. You can see that CodeGreen is available for killing CodeRed II from the simulation result used Birth and Death Process.

1 Introduction

Today, a lot of people use the Internet as a personal computers (PC) spreads, but all users are not necessarily honest. One of largest PC's problem is the computer virus. A computer virus is not a natural virus that everybody often knows, and computer virus is a malicious program that artificially made. A computer virus is the action that people using PC have trouble. For example, one computer virus destroys the display window in PCs, stops computers and so on. Three types of computer viruses are Virus: a malicious program is to increase itself in single computer, Worm: malicious program spread to other computers through a computer network; and Trojan: a malicious program that deceive users as a good program. PC users do not only come under virus attacks, but they protect their PCs with the firewall and the untie virus software. In recent years, firewall and untie virus soft were not available virus by appearing CodeRed worm and Nimda worm. CodeRed worm and Nimda worm are highly infections and multiply. For instance, the CodeRed worm has the equipment of DOS attack and has no effect against a firewall and can untie virus software which usually prevent viruses. Moreover, CodeRed breeding is more than 359,000 computers in fourteen hours, and CodeRed infection is explosive. The menace still continues.

This purpose is to analyze models of CodeRed II and CodeGreen. CodeRed II is a variety of CodeRed, and has the function of Back Door and DOS Attack with CodeRed. CodeGreen is a variety of Worm, and computer virus specialist calls CodeGreen Good Worm. CodeGreen producer made the virus to kill CodeRed worm series, so CodeGreen doesn't break the infected computer system infecting such as CodeRed worm and Nimda worm. But CodeGreen has a lot of mystery and does not know the well present. We investigate how CodeRed II and CodeGreen act in PC and how many PCs do CodeRed II and CodeGreen infect.

This paper discusses the infectious situation and the model to analyze CodeRed II and CodeGreen. The discussion writes about situations of PC infected in CodeRed II and CodeGreen practically, and draws the graph of probability and exponential function used with Birth and Death Process. You can see that CodeGreen is available for preventing CodeRed II or is unavailable.

2 Computer Virus

2.1 CodeRed II

Official name: CODERED.C
Type: Worm
Language: English
Platform: Windows 2000, Windows NT(Chinese and Japanese)
Encryption: Nothing
Virus size: 3,818 bytes
Performance: the following

First, CodeRed II is to make child thread. The process of CodeRed II is the primary thread which creates 300 or 600 child threads when CodeRed II infects PCs. If a setup language of infected Windows is Chinese, CodeRed II will create 600 children threads. If a setup language of infected Windows isn't Chinese, CodeRed II will create 300 children threads. CodeRed II children thread create random IP(Internet Protocol) addresses and transmit the code of a worm by HTTP(HyperText Transfer Protocol) access which aimed at the security hole. CodeRed II children threads repeating increase and create random IP addresses. If the IP address which the worm accessed is the IIS(Internet Information Server) server which has a security hole, the PC with a security hole will infect CodeRed II [3].

Second, CodeRed II is to install of a hacking tool. The primary thread of CodeRed II makes EXPLORER.EXE the root directory of C:drive and D:drive after starting a child thread. EXPLORER.EXE is a hacking tool. So, everybody can access the local drive of a Web server placed EXPLORER.EXE from the outside. Creation of EX-

PLORER.EXE is a lower preparation for hacking by an external third person. CodeRed II will automatically perform EXPLORER.EXE which is the hacking tool copied by the security hole called Relative Shell Path Vulnerability (brittleness of the relative path of Shell) of Windows NT/2000 next time at the time of Windows starting. A hacker can access a Web server while a hacking tool is working, and so get full control [3].

Third, CodeRed II is to change system. CoddeRed II copies cmd.exe, which is the system file of Windows, to the following paths.

C:\inetpub\scripts\root.exe
D:\inetpub\scripts\root.exe
C:\programfiles\commonfiles\system\MSADC\root.exe
D:\programfiles\commonfiles\system\MSADC\root.exe

CodeRed II changes CodeRed2.exe cmd.exe [4].

2.2 CodeGreen

Official name: WORM_CODEGREEN.A
Type: Worm
Language: English
Platform: Windows 2000, Windows NT
Encryption: Nothing
Virus size: 9,216 bytes
Performance: the following passages

First, send packets
CodeGreen creates an IP address at random and transmits an own code at the HTTP request (port number 80) which aimed at the security hole. If an IIS server with the security hole receives this HTTP request (port number 80), overflow of data will take place. Furthermore the program code of the worm directly perform on a memory.

Second, file renaming
If the file named EXPLORER.EXE is in the root directory of C: drive and D: drive, WORM_CODEGREEN.A will rename to the file name AntiCode.Red. File renaming can stop acting of TROJ_CODERED.C which is CODERED.C and CODERED.D.

Third, patch file download
CodeGreen downloads a patch file from Microsoft because of shutting the IIS server which had a security hole. CodeRed series can't infect this machine again.

Forth, change system language
CodeGreen checks the system language in PCs infecting. If the system language is the language except English, CodeGreen will change English. CodeRed II can't act in Windows NT.

We define four performances of CodeGreen as the killing after this.

2.3 Virus Infectious Observation

2.3.1 CodeRed II

CodeRed II infectious pattern differs from IP patterns. You can see the following passage from Network Associates [5].

Nearby network : [50 %]
The same class A network (255.0.0.0) : [37.5 %]
The same class B subnetwork (255.255.0.0) : [12.5 %]
Different network (0.0.0.0) : [0 %]

We can know that CodeRed II infection is 1.8 (PCs/hour) from Predator: Good Will Mobile Codes Combat against Computer Viruses [2]. Windows 2000 shares which protected in no patch file are 510,000 [2]. We would expect numbers of Windows 2000 protected in no patch file infected by CodeRed II if we used Logistics formula [2]. You can see a CodeRed II infectious transition in Figure 1.

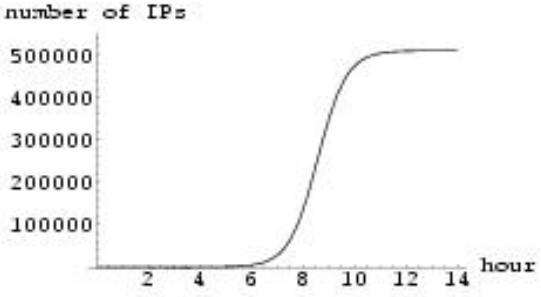

Figure 1: CodeRed II Infectious graph

We found that CoddeRed II is to infect 510, 000 PCs within 14 hours from Figure 1.

2.3.2 CodeGreen

We experimented in making CodeGreen infect PCs in order to investigate CodeGreen's infectious situation and rate. The experimental method is the following procedures.
We prepared two PCs installing Windows 2000 and connected a hub to the two PCs. First, we made CodeGreen infect one of two PCs installing Windows 2000

and recorded CodeGreen infectious cycle and rate with a packet tool : PacMon [6]. Packets sent by CodeGreen were random value one by one, and CodeGreen didn't send packets to LoopBackAdress in this experiment. Packet patterns sent by CodeGreen is Figure 2.

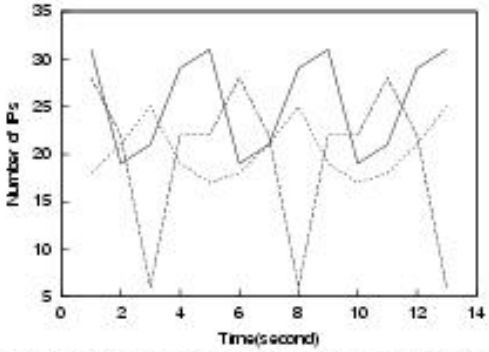

Figure 2: The graph of three packet patterns sent by CodeGreen

We can find that number of packets sent by CaodeGreen are average 108,000 (packets/hour) from Figure 2. Rate of one CodeGreen killing one CodeRed II is about 2.5×10^{-5} (PCs/hour) because the rate 2.5×10^{-5} is to divide 4,261,412,864 (number of IPs excluding LoopBackAdres) into 1 (one of CodeRed II in the network). From the experimental data and Logistics formula [2], you can expect how CodeGreen infects and how CodeGreen kills CodeRed II by changing number of CodeGreen in Figure 3.

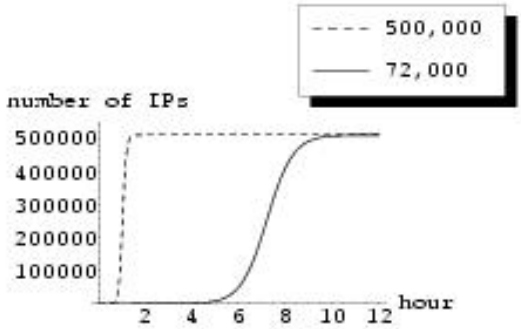

Figure 3: The infectious graph of CodeGreen killing CodeRed II

The dotted line is the infectious graph when number of CodeGreen are 500,000 from Figure 3. We would find that CodeGreen gets rid of CodeRed II in brief time if CodeGreen exists 500,000. The solid line is the infectious graph when number of CodeGreen are 72,000 from Figure 3. We would find that CodeGreen spends 12 hours in order to get rid of CodeRed II if CodeGreen exists 72,000.

3 CodeRed II and CodeGreen

First, one PC which infected CodeRed II exists. Infected PC sends packets because of other PCs infecting. After a while, one of packets hits no infected PC with a security hole, and no infected PC with a security hole infects. Figure 4 is to express CodeRed II infecting.

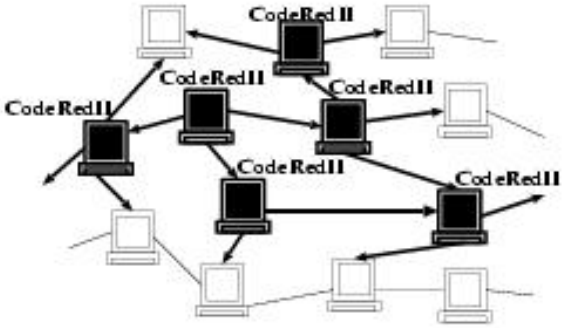

Figure 4: CodeRed II Model

CodeRed II continuous spreads from Figure 4, and CodeRed II becomes a status of Figure 1.

In this experiment, we establish the experiment definition is to release CodeGreen when CodeRed II is infecting to some extent [3]. Figure 5 is to express the experiment definition with a graph.

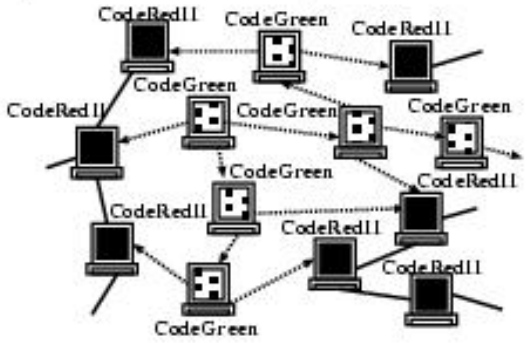

Figure 5: CodeGreen Model

CodeRed II is decreasing by CodeGreen. CodeGreen is furiously increasing on the contrary and becomes a status of Figure 3.

4 Birth and Death Process

An stochastic model expressed with Figure 4 and Figure 5 is Figure 6.

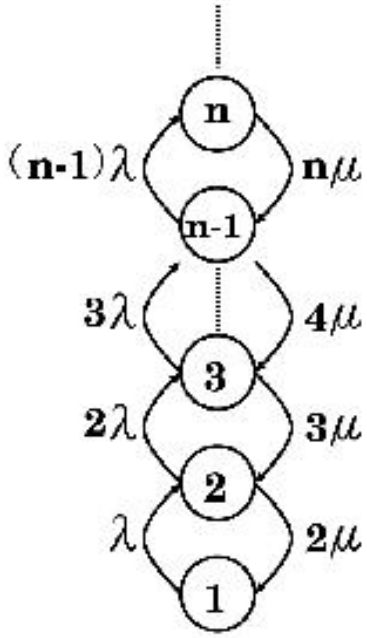

Figure 6: Virus Model

n : A number of PC infected CodeRed II
P_n : Probability of CodeRed II infecting n sets of PC
λ : Birth (CodeRed II infection rate)
μ : Death (Rate of CodeGreen killing CodeRed II)

$$n\mu P_n = (n-1)\lambda P_{n-1}. \tag{1}$$

The point addressed the formula (1) doesn't have a negative value and the probability exceeding 1 in P_n because of probability which is P_n. The following formula (2) is to change the formula (1) about P_n.

$$P_n = -\frac{(\lambda/\mu)^n}{n\log(1-\lambda/\mu)}. \tag{2}$$

This formula (2) is Birth and Death Process [1]. When $0 \leq \lambda/\mu < 1$, Rate of CodeGreen killing CodeRed II exceeds CodeRed II infection rate and is effective in killing CodeRed II. When $\lambda/\mu \geq 1$, Rate of CodeGreen killing CodeRed II is below CodeRed II infection rate and is ineffective in killing CodeRed II.

We draw a graph of P_n changed a value of λ/μ because of investigating CodeRed II probability in the network which CodeGreen is presenting.

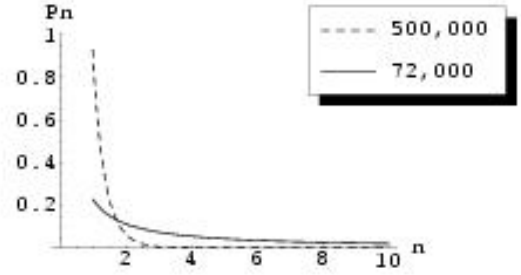

Figure 7: This graph is P_n graph of the formula (2) when number of CodeGreen are 500,000 and when number of CodeGreen are 72,000

P_n is the dotted line when number of CodeGreen are 500,000, the rate of 500,000 CodeGreens killing one CodeRed II is about 20.00 because 20.00 is to multiply 2.5×10^{-5} by 500,000. CodeRed II can infect a few PCs in Figure 3. P_n is the solid line when number of CodeGreen are 72,000, and the rate of 72,000 CodeGreen killing one CodeRed II is about 1.85 because 1.85 is to multiply 2.5×10^{-5} by 72,000. CodeGreen can control the probability under 0.4 when CodeRed II infects more than 10 PCs in Figure 3.

Next, we take an expectation of P_n because of investigating how many sets CodeRed II can infect in the network which CodeGreen is presenting. The following formula is to express the expectation of P_n [1].

$$E[N] = \sum_{n=1}^{\infty} nP_n = -\frac{\lambda/\mu}{(1-\lambda/\mu)\log(1-\lambda/\mu)}. \tag{3}$$

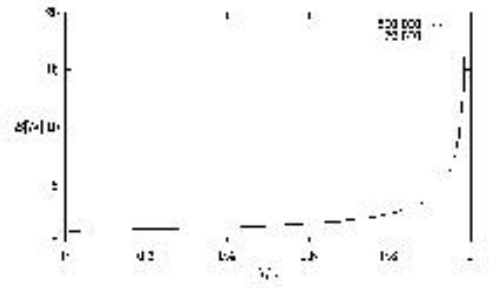

Figure 8: This graph is $E[N]$ graph of the formula (3) when λ/μ is increasing by every one tenth from 0 to 1

You can see that the graph of Figure 8 also becomes larger when the value of λ/μ increases. You can see that CodeRed II infect about 17.5 PCs in the network where CodeGreen exists 72, 000 from the graph of Figure 8 because λ/μ is 1.8/1.85

5 Conclusion and Future Work

We made a model and evaluated the performance confirming CodeGreen effectiveness to prevent CodeRed II. We found that number of PCs infected by CodeRed II are less than 17.5 when CodeGreen exists more than 72, 000 according to working out P_n and $E[P_n]$ with Birth and Death Process. CodeGreen is an effective method for killing CodeRed II.

We propose that CodeGreen is equipped with the multiplication and the existence adequately in future work. CodeGreen inflicts loads on PCs even though CodeGreen is effective in killing CodeRed II. Moreover, CodeGreen changes the system function. A PC can't often act normality by changing the system function. CodeGreen must have the multiplication and the existence adequately in order to be more effective method for killing CodeRed II.

Acknowledgment

Many people helped me. I would like to thank to Prof. H Toyoizumi for helpful comments in this paper and all the Perl-Lab members. I would also like to thank to Prof. Jerold DeHart for my English comment.

References

[1] *Sheldon M.Ross*, Applied Probability Models With Optimization Application, Dover PUBLICATIONS, INC,1992.

[2] *H Toyoizumi and A Kara*, Predator: Good Will Mobile Codes Combat against Computer Viruses, ASM Sigsac New Security Paradigms Workshop, pp.2-3, 2002.

[3] *Trend Micro*, http://www.trendmicro.com/jp/home/enterprise.htm (August, 2002).

[4] *Symantec*, http://www.symantec.co.jp/region/jp/securitycheck/ (August, 2002).

[5] *Network Associates*, http://www.nai.com/japan/ (August, 2002).

[6] *Layer*, http://www.layer.co.jp/