RESEARCH ON CODE RED VIRUS

Vivek kumar[1], Surbhi madan[2]
[1]*CCSIT, TEERTAHANKER MAHAVEER UNIVERSITY , MORADABAD 244001*
[1]vivekkumar0099880@gmail.com
[2]*Surbhi.computers@tmu.ac.in*

Abstract— In this paper we provide a careful analysis of Code Red .The Code Red worm incident of July 2001 has stimulated activities to model and analyse Internet worm propagation. We provide a careful analysis of Code Red propagation by accounting for two factors[1]: one is the dynamic countermeasures taken by ISPs and users; the other is the slowed down worm infection rate because Code Red rampant propagation caused congestion and troubles to some routers[2]. Based on the classical epidemic Kermack- Mckendrick model, we derive a general Internet worm model called the *two-factor worm model*. Simulations and numerical solutions of the two-factor worm model match the observed data of Code Red worm better than previous models do. This model leads to a better understanding and prediction of the scale and speed of Internet worm spreading[3].

Keywords: Internet worm, epidemic model, two-factor worm model, code red, virus, worms, computers.

I. INTRODUCTION

ON JULY 12, 2001, A NEW WORM BEGAN PROPAGATING ACROSS THE INTERNET. ALTHOUGH THE WORM DID NOT YET HAVE A NAME, IT WAS THE FIRST INCARNATION OF WHAT WAS TO BECOME KNOWN AS THE "CODE RED" WORM[4] . THIS INITIAL VERSION OF THE WORM IS COMMONLY REFERRED TO AS CRV1. THE FIRST VERSION OF THE WORM, BEGAN TO SPREAD EVEN MORE RAPIDLY THAN ITS PREDECESSOR A WEEK BEFORE. THE NEW VARIANT OF THE CODE RED WORM WAS REPORTED TO HAVE INFECTED MORE THAN 250,000 SYSTEMS IN JUST NINE HOURS . THIS VARIANT OF THE WORM IS NOW COMMONLY REFERRED TO AS CRV2[5].

The worm scanned the internet, identified weak systems and infected these systems by installing itself. The rate of scanning grew rapidly because each newly installed worm joined others already in existence. not only did the worm result in defaced web pages on the systems it infected, but its uncontrolled growth in scanning resulted in a decrease of speed across the internet—a denial of service attack—and led to extensive outages among all types of systems, not just the Microsoft Internet.[6]

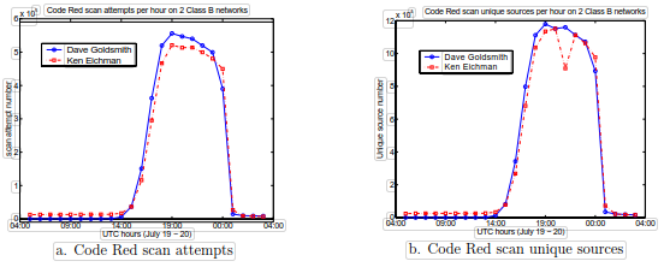
The easy access and wide usage of the Internet makes it a primary target for malicious activities.

The Internet has become a powerful mechanism for propagating malicious software programs. Worms, denied as autonomous programs that spread through computer networks by searching, attacking,[7] and infecting remote computers automatically, have been developed for more than 10 years since the first Morris

worm.

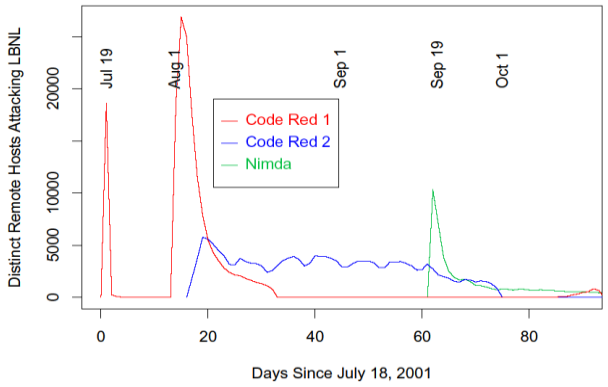
2 LITRATURE REVIEW:

On June 18th 2001 a serious Windows IIS vulnerability was discovered. After almost one month, the first version of Code Red worm that exploited this vulnerability emerged on July 13th, 2001. Due to a code error in its random number generator, it did not propagate well. The truly virulent strain of the worm (Code Red version 2) began to spread around 10:00 UTC of July 19th. This new worm had implemented the correct random number generator. It generated 100 threads. Each of the first 99 threads randomly chose one IP address and tried to set up connection on port 80 with the target machine[9].If the connection was successful, the worm would send a copy of itself to the victim web server to compromise it.



a. Code Red scan attempts b. Code Red scan unique sources

Code Red worm (version 2) was programmed to uniformly scan the IP address space. Netcraft[10] web server survey showed that there were about 6 million Windows IIS web servers at the end of June 2001. If we conservatively assume that there were less than 2 million IIS servers online on July 19th, on average each worm would need to perform more than 2000 IP scans before it could find a Windows IIS server. The worm would need, on average, more than 4000 IP scans to find a target if the number of Windows IIS servers online was less than 1 million. Code Red worm continued to spread on July 19th until 0:00 UTC July 20th, after which the worm stopped propagation by design.

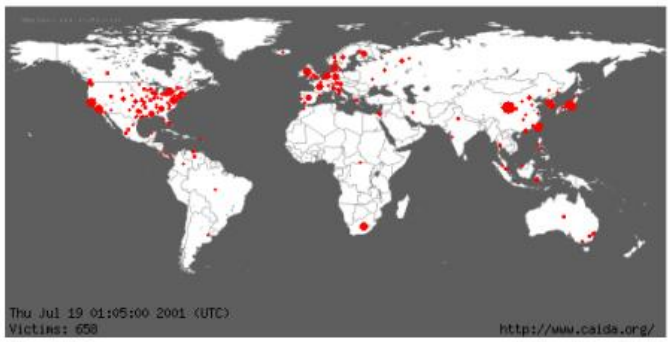


3 COMPARISION:

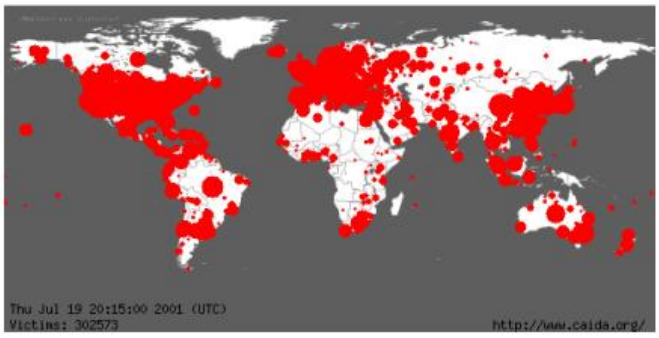
Since Code Red worm was programmed to choose random IP addresses to scan, each IP address is equally likely to be scanned by a Code Red worm. It explains why the Code Red probes on these two Class B networks were so similar to each other as shown in Fig. 1[11].

Each of the two class B networks covers only 1/65536th of the whole IP address space; therefore, the number of unique sources and the number of scans in Fig. 1 are only a portion of active Code Red worms on the whole Internet at that time. However, they correctly exhibit the pattern of Code Red propagation because of the uniform scan of Code Red — this is the reason why we can use the data to study Code Red propagation. Because each infected computer would generate 99 simultaneous scans [12], the number of worm scans was bigger than the number of unique sources. However, Fig. 1 shows that the number of unique sources and the number of scans have the identical evolvement over time — both of them are able to represent Code Red propagation on the Internet. For example, if the number of active Code Red infected computers on the Internet increased[13] 10 times in one hour, both the number of unique

sources and the number of scans observed by Goldsmith and Eichman would increase about 10 times.



July 19 01:05:00 2001



July 19 20:15:00 2001

4 CONCLUSIONS:

In this paper, we present a more accurate Internet worm model and use it to model Code Red worm propagation. Since Internet worms are similar to viruses in epidemic research area, we can use epidemic models to model Internet worms. However, epidemic models are not accurate enough. They can't capture some specific properties of Internet worms. By checking the Code Red worm incident and networks properties, we find that there are two major factors that affect an Internet worm propagation:

One is th effect of human countermeasures against worm spreading, like cleaning, patching, filtering or even disconnecting computers and networks; the other is the slowing down of worm infection rate due to worm's impact on Internet traffic and infrastructure. By considering these two factors, we derive a new general Internet worm model called *two-factor worm* model. The simulations and the numerical solutions of the two-factor worm model show that the model matches well with the observed Code Red worm data of July 19th 200[14].

In our two-factor worm model, the increasing speed of the number of infected hosts will begin to slow down when only about 50% of susceptible hosts have been infected. It explains the earlier slowing down of the Code Red infection in July 19th (Fig. 2). The number of current infected host

Due to the two factors that affect an Internet worm propagation, the exponentially increased propagation speed is only valid for the beginning phase of a worm.[15] If we use the traditional epidemic model to do a worm prediction, we will always overestimate the spreading and damages of the worm.

5 REFERENCES

[1] R. M. Anderson, R.M. May. Infectious diseases of humans: dynamics and control. Oxford University Press, Oxford, 1991.

[2] H. Andersson, T. Britton. Stochastic Epidemic Models and Their Statistical Analysis. Springer-Verlag, New York, 2000.

[3] N. T. Bailey. The Mathematical Theory of Infectious Diseases and its Applications. Hafner Press, New York, 1975.

[4] CERT Advisory CA-2001-23. Continued Threat of the "Code Red" Worm. http://www.cert.org/advisories/CA-2001-23.html

[5] CERT Advisory CA-2000-04. Love Letter Worm. http://www.cert.org/advisories/CA-2000-04.html

[6] CERT Advisory CA-1999-04. Melissa Macro Virus. http://www.cert.org/advisories/CA-1999-04.html

[7] Cisco Security Advisory: "Code Red" Worm - Customer Impact. http://www.cisco.com/warp/public/707/cisco-code-red-

worm-pub.shtml

[8] Cisco Tech. notes: Dealing with mallocfail and High CPU Utilization Resulting From the "Code Red" Worm. http://www.cisco.com/warp/public/63/ ts_codred_worm.shtml

[9] CNN news. "Code Red" worm "minimized" – for now.

[10] J. Cowie, A. Ogielski, B. Premore and Y. Yuan. Global Routing Instabilities during Code Red II and Nimda Worm Propagation. http://www.renesys.com/projects/bgp_instability/

[11] eEye Digital Security. .ida "Code Red" Worm. http://www.eeye.com/html/Research/Advisories/ AL20010717.html

[12] eEye Digital Security. CodeRedII Worm Analysis. http://www.eeye.com/html/Research/Advisories/ AL20010804.html

[13] K. Eichman. Mailist: Re: Possible CodeRed Connection Attempts./http://lists.jammed.com/incidents/20 01/07/0159.html

[14] eWeek news. Code Red Lessons, Big and Small. http://www.eweek.com/article2/0,3959,113815,00.asp

[15] J. C. Frauenthal. Mathematical Modeling in Epidemiology. Springer-Verlag, New York, 1980.