Modeling And Defense Of Camouflaging Worm

[1]Prof. Sumeet S. Pate, [2]Kalpesh S. Ratnaparkhe, [3]Sameer C. Nalawade, [4]Harshal Vishe
[1]Assist. Professor, [2,3,4]BE Student Comp. Engg Dept,
[1,2,3,4]SSJCET, Asangaon, Maharshatra, India.
[1]sumeetpate09@gmail.com, [2]kalpeshratnaparkhe17p@gmail.com, [3]sameernalawade71995@gmail.com,
[4]harshalvishe22@gmail.com

Abstract: - Now day's internet is most widely used and hence security must be needed to maintain to prevent unauthorized access and damage. There are various internet threats includes virus, worm, malware. Worm is self-replicating software program that propagate itself through the network like email. In our case new class of worm is C-worm (Camouflaging Worm). It has ability to successfully camouflage its propagation from existing detection system which tries to capture C-worm traffic according to characteristics of c-worm. This traffic is very less distinguishable in time domain. Hence, Motivated by Inventors, we are using Spectral based approach in which for distribution of scan traffic we uses Power Spectral Density (PSD) and to differentiate the C-Worm traffic from background traffic we are using Spectral Flatness Measure (SFM).Using good matrices we successfully detect the c-worm traffic using Spectral based detection scheme. Also detection scheme effectively detecting not only the C-Worm, but also normal worms as well.

***Keywords*: worm, camouflage, anomaly detection, psd, sfm, cwd.**

I. INTRODUCTION

There are many security threats such as worm, virus, Trojan horse. Worm is a self-replicating program that propagates itself through network. It uses various networks such as email to send copies itself to another network. Worms are harmful to the network by consuming network traffic & also consume the memory by replicating copies, so the computer not responding.

A.TYPES OF WORMS:

Morris worm-: In 1988, Morris worm was one of the first computer worm distributed via Internet. Morris worm affected more than 6,000 university, military and research organization computer.

Melissa worm-: In 1999, Melissa worm is developed by New Jersey Hacker. Melissa worm was programmed to spread via word document of Microsoft. Melissa spread as an email attachment. The body of message is like: Here is the important document for you…don't show anyone & after double clicking the attached document (named LIST.DOC) will affect the computer.

Code Red worm -: In 2001, The code red worm targeted Web server, infecting over 350,000 hosts. It jammed internet traffic when it starts to replicates itself. Each time it found an server is unsecured, the worm copied itself to that server.

Slammer worm -: In 2003, Slammer worm was Fastest spreading worm. It spread rapidly, infecting most of its 75,000 computers within 10 minutes. It affected on Internet performance. It slow down our internet connection & block a few sites.

Email worms-: It is spread using email by attachment message. Worm will arrives as email, where the message body or attachment contain the worm code, & after double click on attachment worm will spread on your computer.

Instant Messaging worm-: Worm is spread via Internet Messaging application that sends a link of infected website to everyone on local contact list.

Internet worms-: Internet worm is spread from one network to another, it arrives with email attachment or downloaded file etc. [13].

Due to damage caused by worms in the past years, there need to be some efforts on developing defense and detecting mechanisms against worms. A network based worm detection system are poses very important role by monitoring, collecting, and analyzing the scan traffic that generated during worm attacks. In this detection system, the detection is based on the self-propagating characteristics of worms such as: later identified a worm-infected computer and infect a vulnerable computer on the Internet, this new affected computer will automatically scan several IP addresses and affect other vulnerable computers. Various existing detection system are based on conducting that each infected computer continue scan the network and propagates itself at the high speed. But, actually there is situation that the worm scans traffic volume and the number of infected computers exhibit increasing patterns.

The C-Worm has a self-propagating behavior same as traditional worms, i.e., it tried to infect many vulnerable computer as possible. But, the C-Worm is quite different from normal worms in which it camouflages any noticeable object in the number of infected computers over time. It successfully achieved its camouflage by manipulating the scan traffic volume of worm-infected computers. Due to its changing nature it cannot be detect by existing detection system, that system tried to detect c-worm in time domain.

Researchers have seen the propagation model of the C-Worm and its scan traffic in frequency and time domains. We also that still the C-Worm scan traffic not show noticeable object in the time domain, it differenced a distinct pattern in the frequency domain. Based on this observation, scientist developed frequency domain analysis techniques and develop a detection scheme for defense C-Worm. We develop a spectrum-based detection scheme that Spectral based approach in which for distribution of scan traffic we uses Power Spectral Density (PSD) and to differentiate the C-Worm traffic from background traffic we are using Spectral Flatness Measure (SFM).

Using good matrices we successfully detect the c-worm traffic using Spectral based detection scheme. Also, detection system detecting not only C-worm as well as mostly normal worm.

B. Literature Survey

Centralized Worm Detector (CWD) Algorithm

Signature based detection scheme and Anomaly detection scheme this two are detection schemes. For detecting only known attack signature based detection scheme is used. Signature is the string of characters that comes in or pop-up payload (payload means worms actual code) of worm's packets. Signature database is required to detect the worm. It not interested to know how worm intelligently propagate itself, how search the its target, which technique is used for transmission etc. it really does not care about all these things. It only see at payload and recognize whether it contain or not any harmful worm. But there is a one problem is that every signature must have entry in the database, in database entry is about 200 or 1000 or more contain.

In this each and every packet is match with all entries in the database. For checking each entry it will take more time and sometimes it works very slowly. Most important unknown attacks are not detected by this detection scheme. In contrast, Anomaly can detect the unknown attack; unknown behavior and it generate alarm. It doesn't require any payload format. They just check header of packet to define type of connection to which packet belongs.

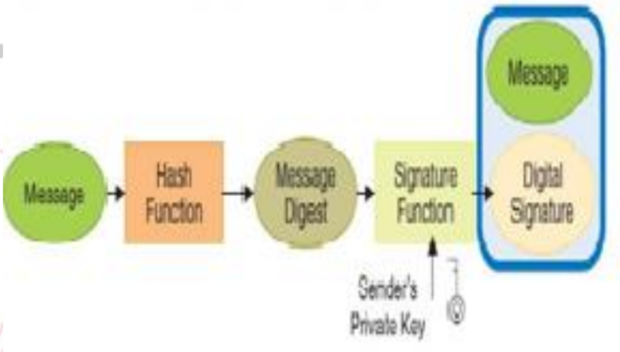


Fig 1: Digital signal creation

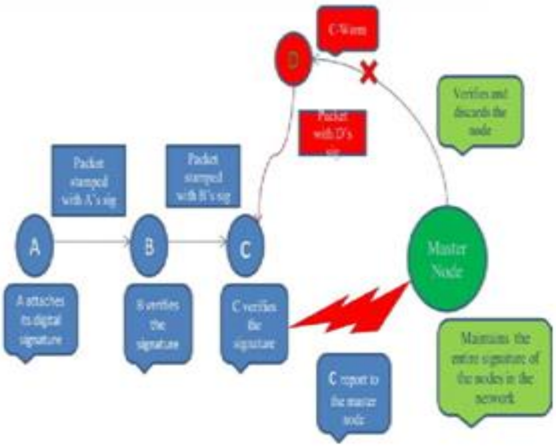

C-Worm
D
Verifies and discards the node
Packet with D's sig
Packet stamped with A's sig
Packet stamped with B's sig
A
B
C
Master Node
A attaches its digital signature
B verifies the signature
C verifies the signature
C report to the master node
Maintains the entire signature of the nodes in the network

Fig 2: Centralized worm detector mechanism

C.Aim and objective

Detecting camouflaging worm using novel spectrum based detection scheme that manipulates its scan traffic volume over period of time during scanning.

Objective

- Understanding the self-propagating behavior of the worm.
- Captures the distinct pattern of C-worm in frequency domain.
- Design a novel spectrum based scheme to detect C-worm.
- Scheme uses Power Spectral Density (PSD) for distribution of the scan traffic volume.
- Spectral Flatness Measure (SFM) used to distinguish C-worm traffic from background traffic.
- Scheme detects traditional worms as well.

II. Stages in proposed system

C-worm does not detected by scheme which tries to detect in time domain, because of its intelligently changing nature. Hence encourage by inventers we developed novel spectral based approach that scan traffic in frequency domain.

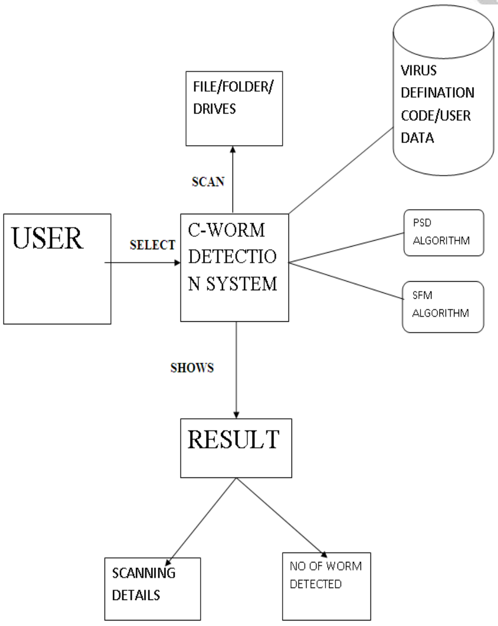


Fig 3: Architecture diagram of C-worm detection system

A. Spreading of the worm (C-Worm)

When a worm is inside your computer, it will spread to another computer via Internet. While transmitting a worm from one computer to another, it scan the numbers of machines to find the weak or vulnerable host to damage. When worm find its victim, it send worm to affect the target. If all these happen successfully, then worm will send thousand or many more copies of itself to this new host. When this new host starts working with worms, worms will tries to affect the other machines. During the process of worm spreading, some computer stop responding or some of working very slowly or forcing the user to restart the computer it all happens because of worms consume the memory space. In this way C-Worm or other worm is spreads.

B. Spectrum-based Detection Scheme

Motivated by researchers we present the details of spectrum-based detection scheme. Similar to other detection scheme we use a “destination count” as the number of the unique destination IP addresses targeted by launched scans during worm propagation.

To know how the destination count information is obtained, recall that an ITM system collects logs from distributed monitors across the Internet. Internet Threat Monitoring (ITM) systems are large deployed facility to detect, analyze, and characterize harmful Internet threats such as worms. An ITM system consists of one centralized data center and a number of monitors distributed across the Internet. Each monitor records traffic that addressed to a range of IP addresses and regularly sends the traffic logs to the data center. The data center analyze traffic LOGS and publishes reports to ITM system users.

To find out *SFM* values of both the C-Worm and normal non-worm scan traffic, we plot the *Probability Density Functions* (PDF) of *SFM* for both C-Worm and normal non-worm scan traffic respectively.

With output in a sampling window w_s, the source count of $S(t)$ is obtained by counting the unique source IP addresses in collected logs. To conduct spectrum analysis, we consider a detection sliding window w_d in the worm detection system. w_d

consist of q(>1) continuous detection sampling windows and each sampling lasts w_s.

The detection sampling window is the unit time interval to sample the detection data. At time i, within sliding window w_d, there are q samples denoted by (S(i-q-1),S(i-q-2),....,S(i)), where S(i-j-1)(j € (1,q)) is the i th destination count from time i-j-1 to i-j.[1].

C. Power Spectral Density (PSD)

To obtain the *PSD* distribution for worm detection , we need to transform data from the time domain into the frequency domain. For this we use a random process $S(t)$, $t \in [0, n]$ to model the worm detection data. Assuming $S(t)$ is the source count in time period $[t-1, t]$ ($t \in [1, n]$), define the auto-correlation of $S(t)$ by

$$RS(L) = E[S(t)S(t+L)] \cdots\cdots\cdots (a)$$

In Formula (a), $RS(L)$ is the correlation of worm detection data in an interval L. If a recurring behavior exists, a *Fourier* transform of the auto-correlation function of $RS(L)$ can reveal such behavior. Also, the *PSD* function of the scan traffic data is determined using the *Discrete Fourier Transform* (*DFT*) of its auto-correlation function as follows,

$$\psi(RS[L], K) = \sum_{N-1}^{n=0} (RS[L]).e^{-j2\pi kn/N} \cdots\cdots (1)$$

Where K = 0, 1, . . ., N− 1.

As the *PSD* captures any recurring pattern in the frequency domain, the *PSD* function shows a comparatively even distribution across a wide spectrum range for the normal non-worm scan traffic. The *PSD* of C-Worm scan traffic shows spikes or noticeably higher concentrations at a certain range of the spectrum.[1]

D. Spectral Flatness Measure (SFM)

Researchers measure the flatness of PSD to distinguish the scan traffic of the C-Worm from the normal non-worm scan traffic. For this, researchers introduce the *Spectral Flatness Measure (SFM)*, which can capture anomaly behavior in certain range of frequencies. The *SFM is* defined as the ratio of the geometric mean to the arithmetic mean of the *PSD* coefficients.

It can be expressed as,

$$SFM = \frac{[\pi_{k=1}^{n} H(f_k)]^{1/n}}{1/n \sum_{k=1}^{n} H(fk)} \cdots\cdots\cdots\cdots (2)$$

Where H (fk) is a *PSD* coefficient for the *PSD* obtained from the results in equitation (2).*SFM* is a widely existing measure for determine frequencies in various applications such as voiced frame detection in speech recognition. Generally, small values of *SFM* imply the concentration of data at narrow frequency spectrum ranges. C-Worm has unpreventable repeating again behavior in its scan traffic; obviously its *SFM* values are comparatively smaller than the *SFM* values of normal non-worm scan traffic. To be useful in detecting C-Worms, introduce a sliding window to capture noticeably higher concentrations at a small range of spectrum. When such noticeably concentration is recognized, derive the SFM within a wider frequency range. We observe that the *SFM* value for the C-Worm is very small. [1]

III. ALGORITHMS IMPLEMENTATION

A. Algorithms for PSD

1. START
2. a random process $S(t)$, $t \in [0, n]$ to model the worm detection data.
3. Assuming $S(t)$ is the source count in time period $[t-1, t]$ ($t \in [1, n]$).
4. the auto-correlation of $S(t)$ by

$$RS(L) = E[S(t)S(t+L)]$$

Where, $RS(L)$ =correlation of worm detection data in an interval.

5. If a recurring behavior exists, a *Fourier* transform of the auto-correlation function of RX (L) can reveal such behavior

$$\psi(RS[L],K)=\sum_{N-1}^{n=0}(RS[L]).e^{-j2\pi kn/N}$$

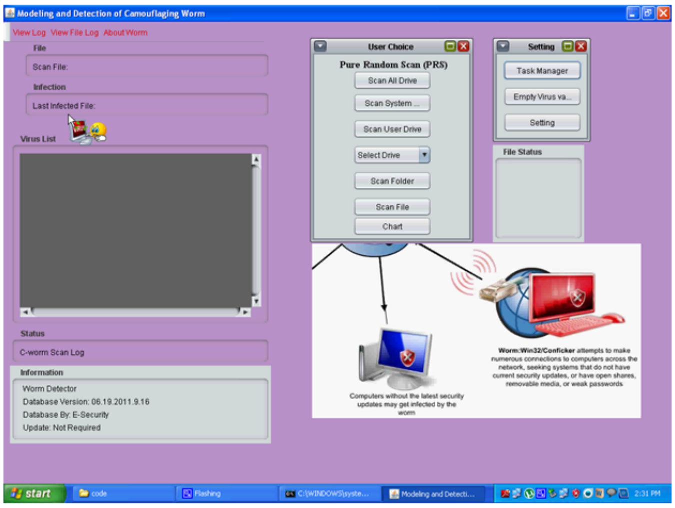
6. *PSD* inherently captures any recurring pattern in the frequency domain.
7. END.

IV. RESULTS AND DISCUSSION

Table 1: Comparison between Existing (CWD detection scheme) and Proposed (Spectral based detection scheme)

Parameters	**Existing system (CWD detection system)**	**Proposed system (Spectral based detection scheme)**
Traffic Scan	Time domain	Frequency domain
Detection ratio	Less	High
Maximum infection Ratio	More	Less
Detection time	Required more time	Detect in very less period of time

V. EXPECTED OUTPUT

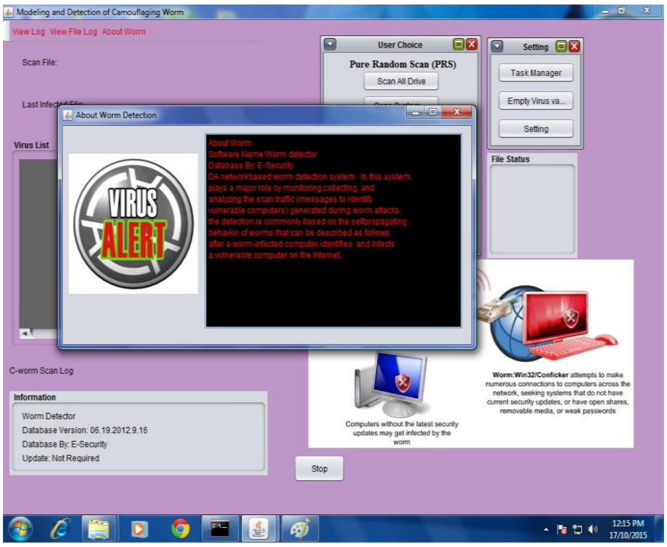


Worm Detector
Database Version: 06.19.2011.9.16
Database By: E-Security
Update: Not Required

Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords

Computers without the latest security updates may get infected by the worm

Fig 4:Home page



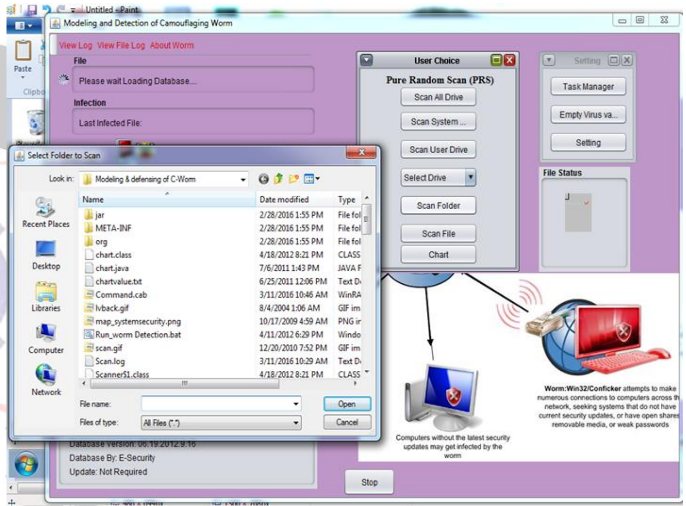
About Worm
Software Name Worm detector
Database By: E-Security
DA networkbased worm detection system In this system, plays a major role by monitoring,collecting, and analyzing the scan traffic (messages to identify vulnerable computers) generated during worm attacks. the detection is commonly based on the selfpropagating behavior of worms that can be described as follows: after a worm-infected computer identifies and infects a vulnerable computer on the Internet.

Worm Detector
Database Version: 06.19.2012.9.16
Database By: E-Security
Update: Not Required

Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords

Computers without the latest security updates may get infected by the worm

Fig 5:Virus alert



Please wait Loading Database....

Look in: Modeling & defensing of C-Worm

Name	Date modified	Type
jar	2/28/2016 1:55 PM	File fol
META-INF	2/28/2016 1:55 PM	File fol
org	2/28/2016 1:55 PM	File fol
chart.class	4/18/2012 8:21 PM	CLASS
chart.java	7/6/2011 1:43 PM	JAVA F
chartvalue.txt	6/25/2011 12:06 PM	Text D
Command.cab	3/11/2016 10:46 AM	WinRA
lvback.gif	8/4/2004 1:06 AM	GIF im
map_systemsecurity.png	10/17/2009 4:59 AM	PNG ir
Run_worm Detection.bat	4/11/2012 6:29 PM	Windo
scan.gif	12/20/2010 7:52 PM	GIF im
Scan.log	3/11/2016 10:29 AM	Text D
Scanner$1.class	4/18/2012 8:21 PM	CLASS

Database Version: 06.19.2012.9.16
Database By: E-Security
Update: Not Required

Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords

Computers without the latest security updates may get infected by the worm

Fig 6: Selecting folder

VI. CONCLUSIONS

C-Worm successfully and intelligently hides its propagation in the time domain, its camouflaging nature differentiate as a distinct pattern in the frequency domain. Based on observation, researchers developed a spectrum-based detection scheme to detect the C-Worm. Evaluation data showed that this scheme achieved best detection performance against c-worm as well as normal worm.

REFERENCES

[1] Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao ‘*Modeling and Detection of Camouflaging Worm’* IEEE transactions on dependable and secure computing, vol. 8, no. 3, may-june 2011.

[2] D. Moore, C. Shannon, and J. Brown, “*Code-red: a case study on the spread and victims of an internet worm*,” in Proceedings of the 2-thInternet Measurement Workshop (IMW), Marseille, France, November2002.

[3] D. Moore, V. Paxson, and S. Savage, “*Inside the slammer worm*,” in IEEE Magazine of Security and Privacy, July 2003.CERT, CERT/CC advisories, http://www.cert.org/advisories/.

[4] P.R.Roberts, Zotob Arrest Breaks Credit Card Fraud Ring,http://www.eweek.com/article2/0,1895,1854162,00.asp. .

[5] R. Vogt, J. Aycock, and M. Jacobson, *“Quorum sensing and self-stopping worms,*” in Proceedings of 5th ACM Workshop on Recurring Malcode (WORM), Alexandria VA, October 2007.

[6] S. Staniford, V. Paxson, and N. Weaver, “*How to own the internet in your spare time*,” in Proceedings of the 11-th USENIX Security Symposium(SECURITY), San Francisco, CA, August 2002.

[7] J. Ma, G. M. Voelker, and S. Savage, “*Self-stopping worms*,” in Proceedings of the ACM Workshop on Rapid Malcode (WORM), Washington D.C, November 2005.

[8] Min Gyyng Kang, Juan Caballero, and Dawn Song, *“Distributed evasive scan techniques and countermeasures*,” in Proceedings of International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA), Lucerne, Switzerland, July 2007.

[9] Charles Wright, Scott Coull, and Fabian Monrose, *“Traffic morphing: An efficient defense against statistical traffic analysis*,” in Proceedings of the 15th IEEE Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2008.

[10] S. Venkataraman, D. Song, P. Gibbons, and A. Blum, *“New streaming algorithms for super spreader detection,*” in Proceedings of the 12-thIEEE Network and Distributed Systems Security Symposium (NDSS),San Diego, CA, February 2005.

[11] J. Wu, S. Vangala, and L. X. Gao, “*An effective architecture and algorithm for detecting worms with various scan techniques*,” in Proceedings of the 11-th IEEE Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2004.

[12] Prof. Chavan M.K1, Madane P.V2 1Assistant Professor, Information Technology Department, Vidya Pratishthan’s College of Engineering, Baramati. ‘Modeling and Detection of Camouflaging Worms-A Survey. (ISSN 2250-24