ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Study and Investigation of the propagation of Malware in Networks from an International Perspective

Ali Nadhum Abd Ulmajeed Al Rifaie
Msc(IS),
Department Computer Science,
Nizam College-Osmania Universtiy.

T.Ramdas Naik
Assistant Professor,
Department Computer Science (PG),
Nizam College-Osmania Universtiy.

Abstract:

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The solution to this problem is desperately desired by cyber defenders as the network security community does not yet have solid answers. The main scope of our project to investigate how malware propagate in networks from a global perspective. We propose a two layer malware propagation model to describe the development of a given malware at the Internet level.

Compared with the existing single layer epidemic models, the proposed model represents malware propagation better in large-scale networks. We propose a two layer malware propagation model to describe the development of a given malware at the Internet level. Compared with the existing single layer epidemic models, the proposed model represents malware propagation better in large-scale networks.

Keywords:

Malware, Propagation, Computer networks, MNalicious software.

Introduction:

Malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners.6 Malware can gain remote access to an information system, record and send data from that system to a third party without the user‟s permission or knowledge, conceal that the information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity. The information system as computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specification and procedures for their operation, use and maintenance.

Different types of malware are commonly described as viruses, worms, trojan horses, backdoors, keystroke loggers, rootkits or spyware. These terms correspond to the functionality and behaviour of the malware (*e.g.* a virus is self propagating, a worm is self replicating). Experts usually group malware into two categories: family and variant. “Family” refers to the distinct or original piece of malware; “variant” refers to a different version of the original malicious code, or family, with minor changes. Malware is persistent and efficient: Malware is increasingly difficult to detect and remove and is effective at defeating built-in information security counter-measures. Some forms of malware can defeat strong forms of multi-factor authentication and others have been able to undermine the effectiveness of digital certificates.

How does malware work?

Malware is able to compromise information systems due to a combination of factors that include insecure operating system design and related software vulnerabilities. Malware works by running or installing itself on an information system manually or automatically, vulnerabilities, or "holes" in its fabric caused by faulty coding. Software may also be improperly configured, have functionality turned off, be used in a manner not compatible with suggested uses or improperly configured with other software. All of these are potential vulnerabilities and vectors for attack. Once these vulnerabilities are discovered, malware can be developed to exploit them for malicious purposes before the security community has developed a “fix”, known as a patch. Malware can also compromise information systems due to non-technological factors such as poor user practices and inadequate security policies and procedures. Many types of malware such as viruses or trojans require some level of user interaction to initiate the infection process such as clicking on a web link in an e-mail, opening an executable file attached to an e-mail or visiting a website where malware is hosted. Once security has been breached by the initial infection, some forms of malware automatically install additional functionality such as spyware (*e.g.* keylogger), backdoor, rootkit or any other type of malware, known as the payload.

Relatedwork:

“Modeling botnet propagation using time zones,”- AUTHORS: D. Dagon, C. Zou, andW. Lee

Time zones play an important and unexplored role in malware epidemics. To understand how time and location affect malware spread dynamics, we studied botnets, or large coordinated collections of victim machines (zombies) controlled by attackers. Over a six month period we observed dozens of botnets representing millions of victims. We noted diurnal properties in botnet activity, which we suspect occurs because victims turn their computers off at night. Through binary analysis, we also confirmed that some botnets demonstrated a bias in infecting regional populations. Clearly, computers that are offline are not infectious, and any regional bias in infections will affect the overall growth of the botnet. We therefore created a diurnal propagation model. The model uses diurnal shaping functions to capture regional variations in online vulnerable populations. The diurnal model also lets one compare propagation rates for different botnets, and prioritize response. Because of variations in release times and diurnal shaping functions particular to an infection, botnets released later in time may actually surpass other botnets that have an advanced start. Since response times for malware outbreaks is now measured in hours, being able to predict short-term propagation dynamics lets us allocate resources more intelligently. We used empirical data from botnets to evaluate the analytical model.

“Dissecting android malware: Characterization and evolution,”- AUTHORS: Y. Zhou and X. Jiang

The popularity and adoption of smart phones has greatly stimulated the spread of mobile malware, especially on the popular platforms such as Android. In light of their rapid growth, there is a pressing need to develop effective solutions.However, our defense capability is largely constrained by the limited understanding of these emerging mobile malware and the lack of timely access to related samples. In this paper, we focus on the Android platform and aim to systematize or characterize existing Android malware. Particularly, with more than one year effort, we have managed to collect more than 1,200 malware samples that cover the majority of existing Android malware families, ranging from their debut in August 2010 to recent ones in October 2011. In addition, we systematically characterize them from various aspects, including their installation methods, activation mechanisms as well as the nature of carried malicious payloads.The characterization and a subsequent evolution-based study of representative families reveal that they are evolving rapidly to circumvent the detection from existing mobile anti-virus software. Based on the evaluation with four representative mobile security software, our experiments show that the best case detects 79.6% of them while the worst case detects only 20.2% in our dataset. These results clearly call for the need to better develop next-generation anti mobile- malware solutions.

“Protecting against network infections: A game theoretic perspective,”- AUTHORS: J. Omic, A. Orda, and P. V. Mieghem

Security breaches and attacks are critical problems in today's networking. A key-point is that the security of each host depends not only on the protection strategies it chooses to adopt but also on those chosen by other hosts in the network.The spread of Internet worms and viruses is only one example. This class of problems has two aspects. First, it deals with epidemic processes, and as such calls for the employment of epidemic theory. Second, the distributed and autonomous nature of decision-making in major classes of networks (e.g., P2P, ad- hoc, and most notably the Internet) call for the employment of game theoretical approaches. Accordingly, we propose a unified framework that combines the N-intertwined, SIS epidemic model with a no cooperative game model. We determine the existence of Nash equilibrium of the respective game and characterize its properties. We show that its quality, in terms of overall network security, largely depends on the underlying topology. We then provide a bound on the level of system inefficiency due to the no cooperative behaviour, namely, the "price of anarchy" of the game. We observe that the price of anarchy may be prohibitively high; hence we propose a scheme for steering users towards socially efficient behaviour.

“Power laws, pareto distributions and zipf’s law,”- AUTHORS: M. E. J. Newman,

When the probability of measuring a particular value of some quantity varies inversely as a power of that value, thequantity is said to follow a power law, also known variously as Zipf’s law or the Pareto distribution. Power laws appear widely in physics, biology, earth and planetary sciences, economics and finance, computer science, demography and the social sciences. For instance, the distributions of the sizes of cities, earthquakes, solar flares, moon craters, wars and people’s personal fortunes all appear to follow power laws. The origin of power-law behavior has been a topic of debate in the scientific community for more than a century. Here we review some of the empirical evidence for the existence of power-law forms and the theories proposed to explain them.

“The effect of network topology on the spread of epidemics,”- AUTHORS: A. J. Ganesh, L. Massouli´e, and D. F. Towsley

Many network phenomena are well modeled as spreads of epidemics through a network. Prominent examples include the spread of worms and email viruses, and, more generally, faults. Many types of information dissemination can also be modeled as spreads of epidemics. In this paper we address the question of what makes an epidemic either weak or potent. More precisely, we identify topological properties of the graph that determine the persistence of epidemics. In particular, we show that if the ratio of cure to infection rates is larger than the spectral radius of the graph, then the mean epidemic lifetime is of order log n, where n is the number of nodes. Conversely, if this ratio is smaller than a generalization of the isoperimetric constant of the graph, then the mean epidemic lifetime is of order ena, for a positive constant a. We apply these results to several network topologies including the hypercube, which is a representative connectivity graph for a distributed hash table, the complete graph, which is an important connectivity graph for BGP, and the power law graph, of which the AS-level Internet graph is a prime example. We also study the star topology and the Erdos-Renyi graph as their epidemic spreading behaviors determine the spreading behavior of power law graph.

Existing System:

Malware are malicious software programs deployed by cyber attackers to compromise computer systems by exploiting their security vulnerabilities. Motivated by extraordinary financial or political rewards, malware owners are exhausting their energy to compromise as many networked computersas they can in order to achieve their malicious goals. A compromised computer is called a bot, and all bots compromised by a malware form a botnet. Botnets have become the attack engine of cyber attackers, and they pose critical challenges to cyber defenders. In order to fight against cyber criminals, it is important for defenders to understand malware behavior,such as propagation or membership recruitment patterns, the size of botnets, and distribution of bots.

Disadvantages:

- In existing system only use the access control techniques to block friend in list.
- It is not possible to prevent undesired messages. No matter user who propose them.
- Providing this service is not only a matter of using previously defined web content mining techniques for a different application, rather it requires to design ad-hoc classification strategies.

Proposed System:

We propose a two layer malware propagation model to describe the development of a given malware at the Internet level. Compared with he existing single layer epidemic models, the proposed model represents malware propagation better in large scale networks. We find the malware distribution in terms of networks varies from exponential to power law with a short exponential tail, and to power law distribution at its early, late, and final stage, respectively. These findings are firstly theoretically proved based on the proposed model, and then confirmed by the experiments through the two large-scale real-world data sets.

ADVANTAGES OF PROPOSED SYSTEM:

Our rigorous analysis, we find that the distribution of a given malware follows an exponential distribution at its early stage, and obeys a power law distribution with a short exponential tail at its late stage, and finally converges to a power law distribution.

Problem Statement:

Problem of malware distribution at large-scale networks. The solution to this problem is desperately desired by cyber defenders as the network security community does not yet have solid answers. Different from previous modelling methods, we propose a two layer epidemic model: The upper layer focuses on networks of a large scale networks, for example, domains of the Internet; the lower layer focuses on the hosts of a given network. This two layer model improves the accuracy compared with the available single layer epidemic models in malware modelling. Moreover, the proposed two layer model offers us the distribution of malware in terms of the low layer networks.

Module Description:

Store and forward message switching

Hold data until it has a scheduled transfer in network storage. Suppose not view the message means delivery status is not received otherwise receives status.

Propagation Model

1) Early stage. An early stage of the breakout of a malware means only a small percentage of vulnerable hosts have been compromised, and the propagation

Follows exponential distributions.

2) Final stage. The final stage of the propagation of a malware means that all vulnerable hosts of a given network have been compromised.

3) Late stage. A late stage means the time interval between the early stage and the final stage.

Gateway

Gateway is designed to forward bundles between two or more DTN region networks and may optionally act as a host. The bundle overlay of gateways must have persistent storage and allow custody transfers. Gateways link together networks that operate on different lower-layer protocols.

Router

Router works within a single DTN region and is responsible for forwarding bundles. Such user requires persistent storage to queue and keep bundles until outbound.

Implementation of Modules:

In Malware propagation in large scale networks we have the modules such as discussed below.

Malware:

Malware are malicious software programs deployed by cyber attackers to compromise computer systems by exploiting their security vulnerabilities. Motivated by extraordinary financial or political rewards, malware owners are exhausting their energy to compromise as many networked computers as they can in order to achieve their malicious goals. A compromised computer is called a bot, and all bots compromised by a malware form a botnet. Botnets have become the attack engine of cyber attackers, and they pose critical challenges to cyber defenders. In order to fight against cyber criminals, it is important for defenders to understand malware behavior, such as propagation or membership recruitment patterns, the size of botnets, and distribution of bots.

Propagation:

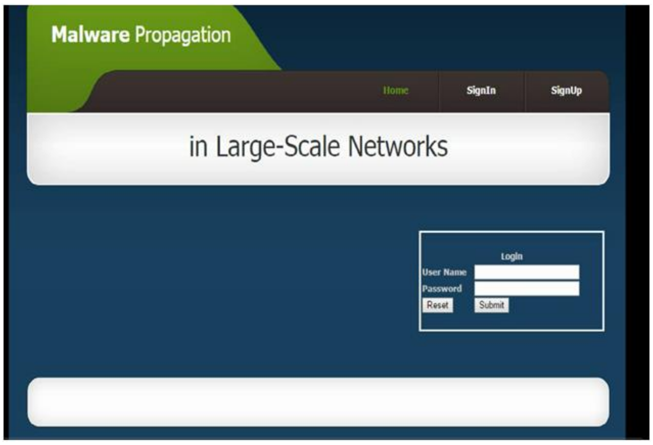
Propagation takes place in three strages such as given below, Early stage: An early stage of the breakout of a malware means only a small percentage of vulnerable hosts have been compromised, and the propagation follows exponential distributions.

Final stage: The final stage of the propagation of a malware means that all vulnerable hosts of a given network have been compromised. Late stage: A late stage means the time interval between the early stage and the final stage.

Power law distribution:

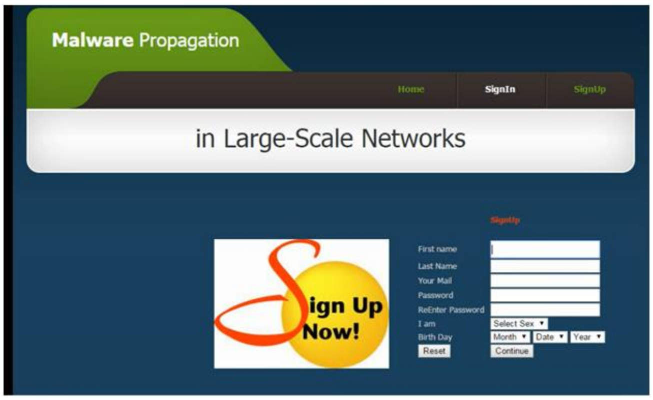
complex networks have demonstrated that the number of hosts of networks follows the power law. People found that the size distribution usually follows the power law, such as population in cities in a country or personal income in a nation. In terms of the Internet, researchers have also discovered many power law phenomenon, such as the size distribution of web files. Recent progresses reported in further demonstrated that the size of networks follows the power law. The power law has two expression forms: the Pareto distribution and the Zip distribution. For the same objects of the power law, we can use any one of them to represent it. However, the Zip distributions are tidier than the expression of the Pareto distributions. In this paper, we will use Zip distributions to represent the power law. The transition from exponential distribution to power law distribution. It is necessary to investigate when and how a malware distribution moves from an exponential distribution to the power law. In other words, how can we clearly define the transition point between the early stage and the late stage.

Screens shots



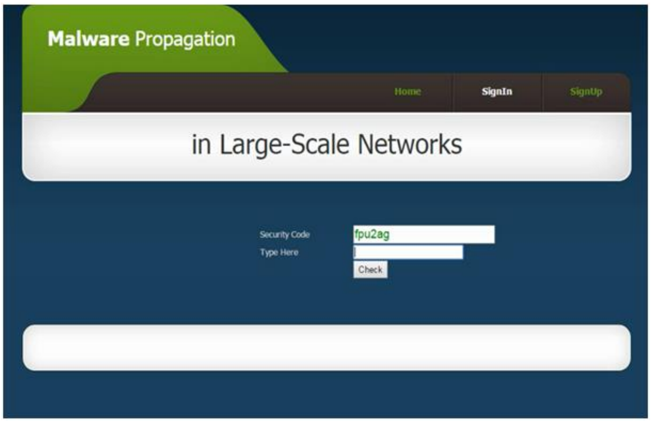
Main screen for login

this screen shot explain main page for log in ,and enter user name and password you create it before and when you finis enter log in press submit to accept log in enter , reset button for empty enter .



screen for sign In

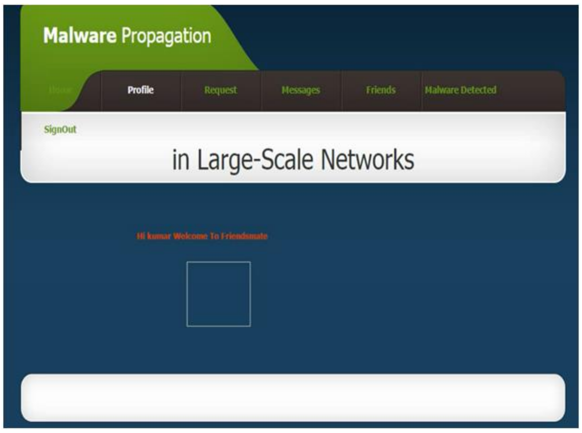
this screen for create new user name and password and enter information first name, last name, your email, re enter password, gender,birthday and after finish input all information press button continue to save all information.



Security Code: fpu2ag

Security code for sign In

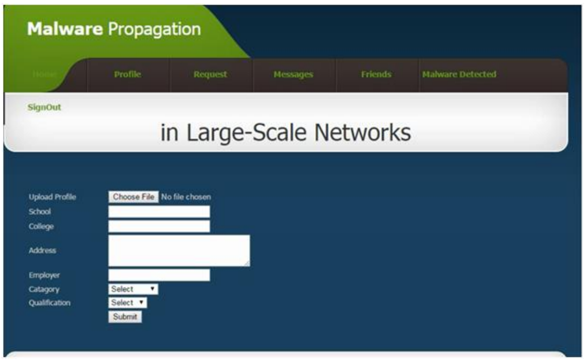
in this figure we check the security code after input the information in [figure 5.2] and input any think for type here like check, update...etc.



Hi kumar Welcome To Friendsmate

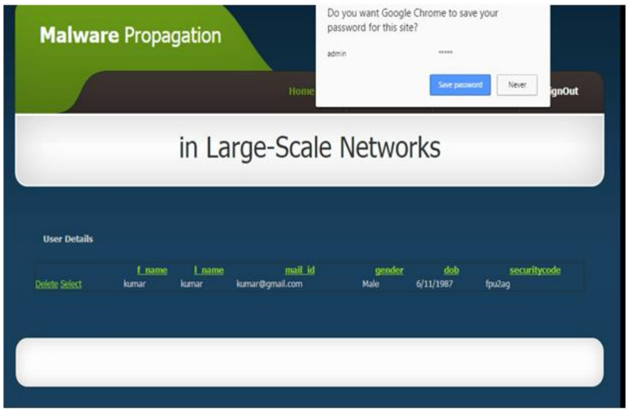
Screen for profile user

in this screen you could see the profile and create it and view profile and check user details in figure [5.5]



Screen for create user profile

in this screen enter the user profile and contain upload file (picture) from any file , input school, college, address, employer if you are employer you write yes if not write no, category, qualification



Do you want Google Chrome to save your password for this site?

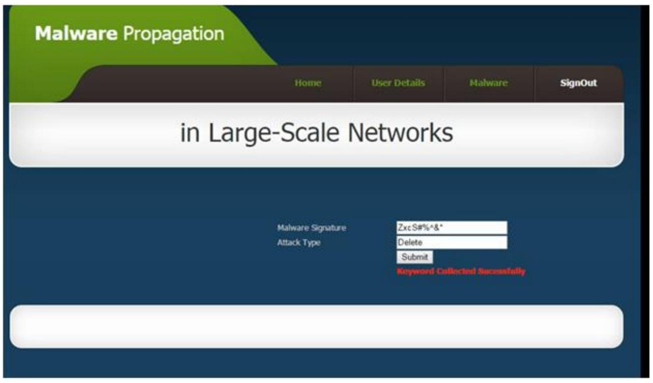
admin *****

User Details

	f_name	l_name	mail_id	gender	dob	securitycode
Delete Select	kumar	kumar	kumar@gmail.com	Male	6/11/1987	fpu2ag

Screen for user details

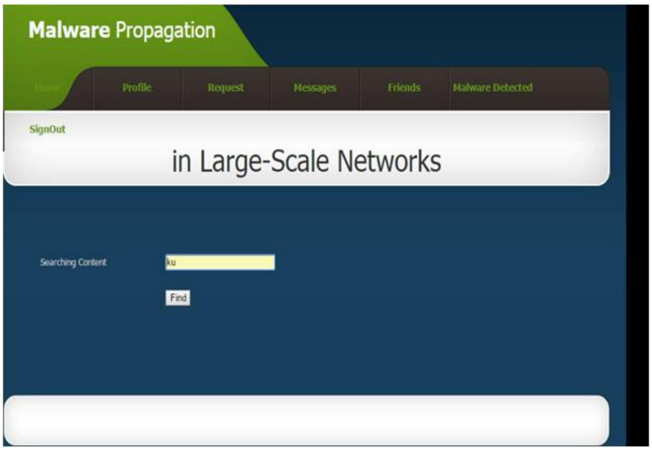
in this screen we see after finish input profile for user ,user details contain name, mail Id ,gender,day of birth(dob), security code



Malware Signature ZxcS#%^&*
Attack Type Delete
Submit
Keyword Collected Successfully

Screen for male ware signature

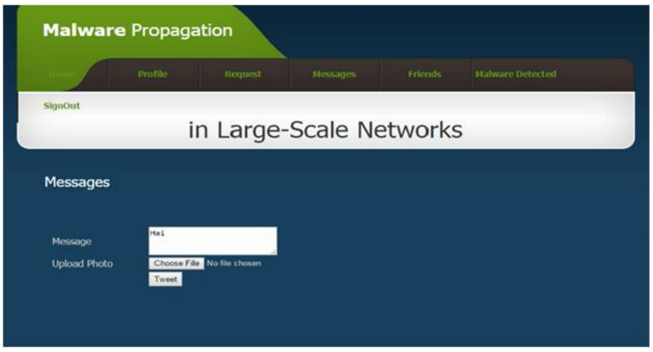
in this screen after we create two user at less and finish creat profile and input all information for user , sign in to admin and go to malware and put in malware signature signiture if ther you find this message to any user sent to another it will be detected and chose attack type like delete or update for this message



Searching Content ku
Find

Screen for searching content

in this screen we search to user and write just tow word and press find

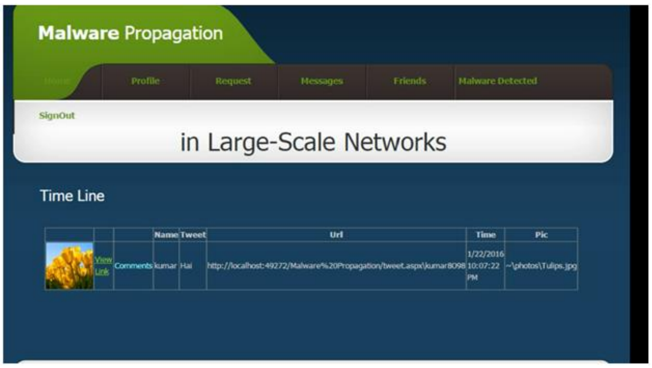


Messages

Message Hai
Upload Photo Choose File No file chosen
Tweet

Screen for messages

in this screen we sent the message to user after writ it and choose file , when you finish press tweat

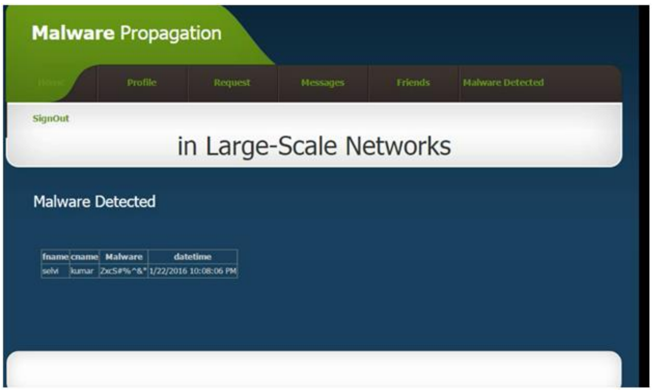


Time Line

			Name	Tweet	Url	Time	Pic
	View Link	Comments	kumar	Hai	http://localhost:49272/Malware%20Propagation/tweet.aspx\kumar8098	1/22/2016 10:07:22 PM	~\photos\Tulips.jpg

Screen for messages

in this screen after search friend we chose time view line and see information about time line



Malware Detected

fname	cname	Malware	datetime
selvi	kumar	ZxcS#%^&*	1/22/2016 10:08:06 PM

Screen for malware detected

in this screen we see malware detected and find details about malware fname, cname, malware, data time

Conclusion:

It describes the problem of malware distribution at large-scale networks. The solution to this problem is desperately desired by cyber defenders as the network security community does not yet have solid answers. Different from previous modelling methods, we propose a two layer epidemic model: the upper layer focuses on networks of a large scale networks, for example,Domains of the Internet; the lower layer focuses on the hosts of a given network. This two layer model improves the accuracy compared with the available single layer epidemic models in malware modelling. Moreover, the proposed two layer model offers us the distribution of malware in terms of the low layer networks.

References:

[1] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, “Your botnet is my botnet: Analysis of a botnet takeover,” in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 635–647.

[2] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging,” in Proc. 1st Conf. 1st Workshop Hot Topics Understanding Botnets, 2007, p. 5.

[3] D. Dagon, C. Zou, and W. Lee, “Modeling botnet propagation using time zones,” in Proc. 13th Netw. Distrib. Syst. Security Symp., 2006.

[4] P. V. Mieghem, J. Omic, and R. Kooij, “Virus spread in networks,”IEEE/ACM Trans. Netw., vol. 17, no. 1, pp. 1–14, Feb. 2009.

[5] Cabir. (2014). [Online]. Available: http://www.f-secure.com/en/ web/labs_global/2004-threat-summary

[6] Ikee. (2014). [Online]. Available: http://www.f-secure.com/vdescs/worm_iphoneos_ikee_b.shtml

[7] Brador. (2014). [Online]. Available: http://www.f-secure.com/vdescs/brador.shtml

[8] S. Peng, S. Yu, and A. Yang, “Smartphone malware and its propagation modeling: A survey,” IEEE Commun. Surveys Tuts., vol. 16, no. 2, pp. 925–941, 2014.

[9] Z. Chen and C. Ji, “An information-theoretic view of networkaware malware attacks,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 530–541, Sep. 2009.

[10] A. M. Jeffrey, X. Xia, and I. K. Craig, “When to initiate HIV therapy: A control theoretic approach,” IEEE Trans. Biomed. Eng., vol. 50, no. 11, pp. 1213–1220, Nov. 2003.