International Journal of Advanced Engineering and Recent Technology
ISSN (Online) : 2455 3522 ;
www.ijaeart.com Volume 6 Issue 1 | April 2016 | PP : 67 - 73

Prediction of Advanced Persistent Threat Malware on Network Traffic

Saranya.N
Department of CSE
Sri Eshwar College of Engineering
Coimbatore, India
saranya.n@sece.in

Monica.G
Department of CSE
Sri Eshwar College of Engineering
Coimbatore, India
monica.g@sece.ac.in

Gayathri Sundara
Design Associate Software Engineer
Tech Mahindra
Bangalore, India
nsgayu@cognizant.com

ABSTRACT Advanced persistent threat (APT) is a important threat to the network. Hackers can get the control of affected systems and hack the sensitive information through APT. To locate the command and control servers DNS is used. In this paper, we propose a novel system placed at the network to predict the malware APT on network to safeguard the sensitive information in the system. To detect the malware we use the DNS analysis to predict the APT malware on network and analyze the traffic in the network. We use signature based technology to detect the malware on network. We used 17 features based on big data to characterize properties of DNS and the features of network traffic. Our research was performed at a large local institute network and all the features were undertaken with big data.

INDEX TERMS APT, malware infections, DNS, intrusion detection.

I. INTRODUCTION

Advanced Persistent Threat (APT) attacks are increasing on the internet nowadays; unfortunately, they are hard to detect. It is a set of stealthy and continuous hacking processes targeting with huge-value information, such as government, military. The intention of an APT attack is to hack data rather than to cause damage to the network or organization. Once hacking into the network has been achieved, the attacker would install APT malware on the infected machine. APT malware, for instance, Trojan horse or backdoor, is tailored for anti-virus software and re walls of the target network. It is not only used for remotely controlling the compromised machines in the APT attack, but also for stealing sensitive information from affected host over an extended period of time. APT malware can evade anti-virus software using polymorphic code, and bypass re wall using protocol on allowed ports.

In an APT attack, the malware needs to maintain a persistent connection to a C&C server. DNS is widely used by the attacker to locate command and control server of the malware. Because if the attacker hardcode the IP of the C&C server into the malware binary, it would cause some kind of failure that cannot be recovered. Once the C&C server goes down or the IP address is detected, the compromised machine would be out of attacker's control. Another reason is that, to hide the real attack source, attackers often use the servers they have controlled or managed in different countries and regions as proxies. Since using domain names is exile to change the IP addresses of the malware C&C servers and migrate the C&C servers, it helps the attacker to hide the true attack source behind proxy server more easily. By analyzing lots of malware samples in virtual machines, we found that malware such as Trojan and other Remote Access Tool (RAT) often uses DNS especially Dynamic DNS to locate command and control server. Dynamic DNS is a method that can update a name server in real time. For the malware such as Trojan, DDNS is a natural. The primary convenience of dynamic DNS is that, the user can change the domain to point to a new IP address at any time.

In this paper, we aim to detect APT malware which relies on DNS to locate command and control servers. These researches focused on detecting malicious services or bots that make use of domain generation algorithm (DGA). Malicious service works similarly with content-delivery networks (CDN) service. It makes use of the same theory as CDN. CDN now is a common method to accelerate delivery of content of websites and reduce web server lag. It is a network that consists of large numbers of machines resided in different countries and regions. Whenever a user sending a request to the web server that is part of CDN network, the nearest server is going to respond the website visitor. CDN is an effective method to accelerate content

delivery of web servers. Malicious service is a DNS technique used by botnet. The difference between content-delivery networks and malicious network is that, the CDN consists of large numbers of legitimate servers, and the malicious network consists of large numbers of infected machines.

Domain Generation Algorithm (DGA) can be used to generate a large number of domain names. APT malware is very different from the bots and worms mentioned above. The primary purpose of APT malware is to remotely control the machines and to steal con denial data, rather than to launch denial-of-service attacks, send spam emails or cause damage. It requires a high degree of stealth over a prolonged duration of operation. For example, in the case of those bots and worms, the attackers need to use the command and control servers to remotely control thousands of infected hosts.

But APT attackers do not use the same C&C server to remotely control so many affected end-user machines, because it would increase the risk of exposure. The crafted malware is only used for the end-user machines which are valuable to them. The DNS behavioral features of APT malware are very different from malicious service and DGA. Flux service and DGA domains have some obvious features. For example, ``short life" feature is extracted from domains that are generated by a domain generation algorithm.

To identify malicious domains that are involved in APT malware activity is a challenge. The crafted malware in APT attack do not use malicious service or DGA domains. The domains for APT malware were registered by the attackers. Compared with these bots and worms, crafted malware requires high degree of stealth. To detect APT malware infections in a large network is another challenging problem. In this paper, we propose a novel system ``DnS" placed at the network egress points to detect APT malware infection which relies on DNS to locate command and control servers. The main contributions of this paper are as follows:

We present a novel system placed at the network edge using a combination of malicious DNS detection technology and intrusion detection technology to detect malware infections inside the network. This approach can not only largely reduce the volume of network traffic which needs to be recorded and analyzed, but also improve the sustainability of the system. We need 17 APT malware C&C server domain features including dynamic DNS features by studying large volumes of DNS traffic which can be called big data. 7 Of them have not been proposed before in previous works. And abnormal network traffic features are also de need to help identify the traffic of compromised clients that have been remotely controlled. We build a reputation engine to decide whether an IP address is infected or not by using these feature vectors together.

II. RELATED WORK

A. DNS MALWARE STUDIES

Researchers have recently proposed the method of identifying malicious domains through DNS traffic analysis. Notos [9] build a reputation engine for dynamically assigning a reputation score for a new unknown domain to judge whether it is malicious or not. EXPOSURE [7] studied DNS lookup behavior within a local domain below the DNS resolvers to detect domains for malicious use, such as domains used for malicious, adult website, spam mails, phishing and malware. In paper [10], it gives a summary of the system EXPOSURE [7] which is using passive DNS analysis to automatically detect malicious domains.

Approaches for detecting malware activity by monitoring and analyzing DNS traffic were also studied too. The mechanism relies on detecting group activities in DNS queries simultaneously sent by distributed bots. The authors proposed features to distinguish DNS traffic generated by botnets and benign clients. But they only focus on the group activity property of botnet, and the features they identified are not t to detect APT malware.

No previous work has tried to identify malicious domain names involved in APT malware activity. In this paper, we focus on detecting C&C server domain names for crafted malware in APT activity. We extracted 14 APT malware C&C domain features including features of malicious DDNS, and 7 of them have not been proposed before. We place the system which is called ``IDns" on the edge of the network and also do the network traffic analysis to detect infected machines inside the network.

B. INTRUSION DETECTION STUDIES

In general, the main studies of network intrusion detection include signature-based detection and anomaly-based detection. Signature-based detection is a technology that relies on a existing signature database to detect known malware infections. By using signature-based detection technology, it can identify malware C&C communication traffic through signature-based pattern matching. So for malware infection detection, it is a typical approach. But signature-based detection technology has a fatal drawback; it cannot detect new malware infections if the signature of the new malware is not in the existing signature database.

Anomaly-based intrusion detection is a technology that detect abnormal behaviors that deviates from ``normal" behaviors. The ``normal" behaviors of the network need to be studied and identified at rest. The primary advantage of anomaly-based intrusion detection is the capability to detect new or unknown attacks. Because the new or unknown malware whose signature is not available would also generate abnormal behaviors. The

primary drawback of anomaly-based intrusion detection is that, it is more prone to generating false positives. Because the behaviors of different networks and applications are so complicated, the ``normal" behaviors is very hard to accurately identify. Different from signature-based detection, anomaly-based intrusion detection is a broader match which is based on detect abnormal behaviors. Many legitimate applications perform the same abnormal behaviors as malicious ones.

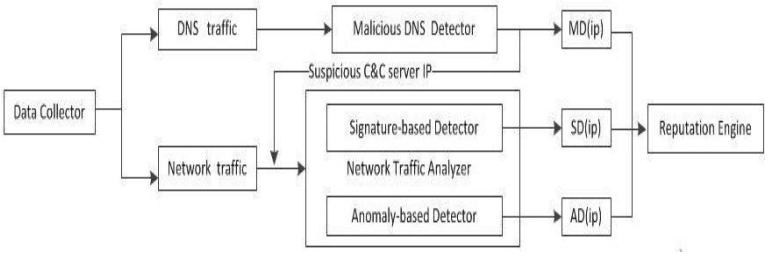

FIGURE 1. Architecture of the System.

III. OVERVIEW OF THE APPROACH

A. EXTRACTING FEATURES FOR DETECTION

IDns is designed to detect malicious domains used for crafted malware in APT attacks and to detect infected machines. For this purpose, we did analysis of large volumes of DNS traffic which can be called big data. And we also analyzed the network traffic of large numbers of suspicious malware C&C servers.

The features we extracted from big data for detection consist of malicious DNS features and network traffic features. By studying the DNS traffic, we achieved to extract distinguishable DNS features that are able to de ne the APT malware C&C domains. By studying the behaviors of the crafted malware and benign applications, we achieved to extract distinguishable network traffic features that are able to de ne the APT malware C&C traffic. Network traffic features, including signature-based detection features and anomaly-based detection features, can help to identify the traffic of compromised clients that have been remotely con-trolled by crafted malware.

B. ARCHITECTURE OF THE SYSTEM

Figure 1 shows us the architecture of system ``IDnS". It consists of four main units:

Data Collector: It is placed at the network edge to record the inbound and outbound traffic produced by the network.

Malicious DNS Detector: It is responsible for analyzing the inbound and outbound DNS traffic produced by the network, and detecting suspicious APT malware C&C domains. It would detect the suspicious APT malware-related domains and provide corresponding suspicious C&C server IP addresses for the ``network traffic analyzer" of the system.

Network Traffic Analyzer: It consists of signature-based detector and anomaly-based detector, for analyzing the network traf c of suspicious C&C server IP addresses. The signature-based detector has defined C&C communication traffic signatures for detecting malware known to the system. The anomaly-based detector detect anomalous behaviors including protocol anomaly, statistical anomaly, application anomaly etc. When the unknown or new malware was identified by anomaly-based detector, new signatures will be de done. All the C&C communication traffic signatures which have been identified will be collected to our TM (Targeted Malware) family.

Reputation Engine: It aims to compute a reputation score for an IP address to judge whether the host or server owning the IP address is infected or not, by using malicious DNS and network traffic feature vectors together.

IV. MALICIOUS DNS FEATURES

In this paper, we identified 17 features to detect APT malware command and control domains (see Table 1) based on big data. 7 Of the features have not been proposed before. And we also give new explanations of some old features that have been proposed before. In this section, we will elaborate on the 17 features that are proposed in this paper and explain the reasons that they can be used for detecting APT malware command and control domains.

A. DOMAIN NAME-BASED FEATURES

Every single domain name is separated to several parts by period. The last part is called the top-level domain (TLD). The second-level domain (2LD) is the last two parts. The third-level domain (3LD) is the last three parts, and so on. For example, given the domain name ``a.b.c.com", TLD of the domain name is ``com", 2LD of the domain is ``c.com", and 3LD of the domain is ``b.c.com". For a dynamic DNS, 2LD ``c.com" is existing part owned by the DDNS provider. The third level sub-domain ``b" in ``b.c.com" is created by the users. We extracted three domain name-based features, the third level sub-domain name of DDNS (dynamic domain name) contains famous name, particular name or phishing name. In previous researches, these 3 features for malware C&C dynamic domain names were not been proposed ever.

Contain Famous Name: We make it interesting that many dynamic domain names registered for C&C servers can tell us they are highly suspicious themselves. We can tell them from the legitimate ones just by the name. Just like we can tell that a long haired man wearing a police uniform is a fake police. Many registered suspicious dynamic domain names contain famous domain names such as windows, yahoo and taobao. And we know that there is little chance that these dynamic domains are

used for Microsoft, Yahoo or Alibaba.

Contain Particular Name: We also nd that many dynamic domain names registered for C&C servers contain some particular name, such as ``web", ``mail", ``news" and ``update". These particular names not only make these domain names easy to remember, but also make these domains more like normal ones. And as observed, the particular name and the famous domain name are usually used together, such as ``yahoomail.xxx.com", ``yahoonews.xxx.com" and ``windowsupdate.xxx.com".

Contain Phishing Name: Phishing is a technology that is usually used in social engineering attacks. The attacker tricks the victim to access a crafted fake website which is malicious. When the victim accesses the phishing website, which will try to install malware on the victim. For tricking the users, we all know the phishing domain has a similar name to a legitimate one. Such as ``youtuhe.com" compared to ``youtube.com", ``yah00.com" compared to ``yahoo.com", etc. we observed that many malicious dynamic domain names used for command and control server of RAT tool not scam server also have a phishing similar name to a legitimate domain one.

B. DNS ANSWER-BASED FEATURES

Silent IP: To hide the C&C server and C&C network traffic, when attackers do not need to send commands to a victim machine, they do not want the domain names to point to the C&C server. For that moment, attackers usually change the domains to point to some specific IPs. Specific IP addresses are usually as follows: 127.0.0.1 (loop back address); 192.168.x.x, 172.16.x.x, 10.x.x.x (private address); x.x.x.255 (broadcast address).

Predefined IP: Some advanced malware in APT attack improved this method. When the attackers were developing and coding the advanced malware, a predefined IP was hard-coded into the malware binary. The silent mechanism works like this, when the domain is resolved to the predefined IP, the malware would turn to silent-mode and would not initiate a connection until the domain is resolved to another IP address. Predefined IP addresses are usually some invalid IP addresses that have obvious features, such as 5.5.5.5, 2.3.3.2.

Number of Distinct IP Addresses & *Number of Distinct Countries*: To hide the true attack source, attackers usually use servers reside in different countries or regions they control or manage as C&C servers. To the attacker, C&C servers better not reside in the same country of the attacker or the victim. Because if C&C servers reside in the same country of the victim, it is easier for the victim country to analyze this attack. If C&C servers reside in the same country of the attacker, it is easier to trace the real source. These 2 features have been used in previous work to detect botnets domains (see [12], [16]).

Number of Domains Share the Same IP With: This is also a feature that EXPOSURE [7] proposed before. And we study and train this same feature to detect malicious dynamic DNS, it works as well. In the APT attack scenario, a single attacker seldom own more than 30 dynamic names to locate command and control server in the same time, because it is not necessary and it is hard to maintain them. So the number of malicious dynamic domains share the same IP with is defined less than 30.

IP in the Same Class B Range of Known C&C Servers: We have performed statistical analysis of numbers of C&C servers that have been detected. The result shows that, there are many C&C servers in the same Class B IP addresses range and even in the same Class A range. There may be two reasons for this. The rest is more and more APT attackers rent VPS servers as C&C servers. Because VPS server is stable, hard to trace back and easy to manage. VPS servers rented from the same service provider are mostly in the same Class B IP addresses range and even in the same Class A range. The second reason is, some advanced attackers constructed special network for C&C servers.

C. TIME VALUE-BASED FEATURES

Daily Similarity: This feature is proposed before in EXPOSURE [7]. They check if there are domains that show daily similarities in their request count change over time, an increase or decrease of the request count at the same intervals everyday. In our detection, we check if the domains have daily similarities in changing IP address at the same intervals everyday. For example, organized APT attackers usually change the domains to point to C&C servers at the start time of one-day work hours, and change the domains to point to silent IP at the end time of one-day work hours. Some malware typically connect to C&C servers at same intervals of everyday, monitoring consistent intervals for DNS requests will help.

Same Query Numbers in Same Time Window: This feature means in the same time window, the number of domain queries are about the same. When the infected host is online, but there is a connection failure for some reason. The infected host will mistaken DNS errors and send large amounts of repeated DNS queries.

D. TTL VALUE-BASED FEATURES

Time To Live (TTL) is set by an authoritative name server for a DNS record. TTL means how long the a resolver may cache the response result for a domain. If a stub resolver queries the caching name server for the record before the TTL has expired, the caching server will simply reply with the already cached resource record rather than retrieve it from the authoritative

name server again.

Average TTL: Setting TTL values of host names to lower values can help the attacker to change the C&C server rapidly. Moreover, based on our measurements, TTL values of Dynamic Domain Name Service, such as Dyn DNS, NO-IP and Change IP, are usually set to 30, 31, 60, 300 seconds. But not all the malware C&C domains set TTL values to lower values. As we mentioned in ``Very low frequency'', there are advanced malware domains setting higher TTL values, such as 86400 seconds as observed. Because they do not change the resolving IP address for weeks.

V. NETWORK TRAFFIC FEATURE

Our system IDnS uses signature-based detection and anomaly-based detection together to provide the maximum defense for the monitoring network.

A. SIGNATURE-BASED DETECTION FEATURES

Rule set plays a crucial role in signature-based IDS, and the number and accuracy of the rules determine how much infections can be detected. To apply publicly open rule sets of well known signature-based IDS, we use rules from VRT Rule sets [18] of snort. Our system focuses on detecting malware infections, so the rules applied to the system are mainly from malware-backdoor rules, malware- cnc rules, malware-other rules and blacklist rules. After a long detecting period, the system has detected and confirmed a lot of malware infections by malicious DNS detection combined with anomaly-based detection.

Signature-based detection features we mentioned in this paper means the features of C&C network traffic generated when malware communicate with C&C servers. By analyzing the network traffic produced when the malware communicate with command and control servers, we extract network traffic communication features of 21 unknown malware or Trojans. We attribute the unknown malware to our TM (Targeted Malware) family, So all the malware in our TM (Targeted Malware) family can be habitually detected. We will continue to do this work in the future, because it is an efficient way to detect malware infections.

The network traffic generated when malware communicate with a command and control server is more prone to have consistent features. This is because the command and control channel the attacker build between the infected machine and the control server is steady.

B. ANOMALY-BASED DETECTION FEATURES

Anomaly-based intrusion detection is based on detecting anomalous behaviors occurs on the network. The signature-based method needs a database of known signatures. Anomaly-based intrusion detection needs to de ne anomalous or normal behaviors. We defined APT malware behaviors below including protocol anomaly, statistical anomaly, application anomaly:

Encrypted Data Transpire on Uncommonly-Used Port (Protocol Anomaly): Not all the malware communicate with the C&C servers on commonly-used protocol ports. Some malware sometimes communicate with the C&C servers on ports which are seldom used by legitimate applications. And most APT malware C&C traffic data is encrypted to evade detections. So encrypted data transpire on uncommonly-used protocol port is also likely malicious traffic.

Mismatch of Uplink and Downlink Traffic (Statistical Anomaly): Normally, the downlink data traffic low to host is larger than the uplink traffic to server. But the C&C communicating traffic is diametrically opposite. The data traffic that infected host upload to the control server is always larger than the data traffic received from the control server. For example, traffic of HTTP request much more than the HTTP response is very likely malicious traffic.

A number of Small Packets in Long TCP Connection (Statistical Anomaly): When the attacker send sets of command to the infected machine, commands such as le resource search command, le download command would require a lot of waiting time, coupled with the human thinking time, make the connection session a longer duration. And sets of commands are all small packets sent from C&C server to the infected host.

Heartbeat Packet Traf c (Application Anomaly): After the infected host client connected the command and control server, the server would send packets to the client, making sure the other end is on line. This kind of packet is called heartbeat packet. As heartbeat packets have similar size, we cluster all packets by packet size and check whether packets in the same cluster are sent periodically.

VI. BUILDING DETECTION MODELS

A. CONSTRUCTING THE TRAINING DATA SET

The training data set plays an important role in machine learning algorithm. We aim to train a classifier that can identify domains used for crafted malware C&C servers, and to train a reputation function that can judge whether an IP address is infected or not by crafted malware.

For this purpose, approximate one thousand domains used for crafted malware C&C servers and one thousand benign domains were collected to construct training data set.

we took full advantage of the ``Virus Email Detector System'' which is deployed in this network, and extracted hundreds of malicious domains from hundreds of malware samples in virus email attachments. Sending virus emails to specific targets with attached documents that are packed with exploit code and Trojan horse programmes has become one of the most important attack vectors in APT attack .

The training period of our system was the first four weeks. During this period of four weeks, ``the time-based behavior'' of malware C&C domains can be observed in a better way. During the first four weeks of experimenting at a large local research institute network with different values, we also labeled about 5 hundred malicious domains and more than 2 hundred infected machines inside the network, by manual analysis of the network connections to each suspicious C&C server domains and manual verification of every infected host inside the network. We are conservative when constructing the malicious domain list and infection host list. We apply a preliminary check before labeling a domain as being malicious, an IP address as being infected and using it in our training set. Every infection is confirmed by on-site examination and manual verification with the cooperation of the network administrator of the research institute.

B. CLASSIFIER OF MALICIOUS DNS DETECTOR

The classifier of Malicious DNS Detector is using J48 decision tree algorithm. J48 decision tree is based on C4.5 algorithm and it has been proved to be efficient in classifying benign domains and malicious domains in EXPOSURE [7].

The J48 decision tree clasifier is built in the training period. The condition of some attribute is being examined in every node. Every branch of the tree represents a result of the study.

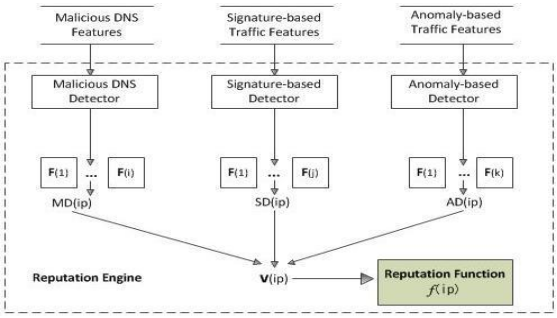

FIGURE 2. Reputation Engine to Assign a Reputation Score.

C. REPUTATION ENGINE

The reputation engine (see Fig. 3) of our system is responsible for detecting whether a host inside the network with
IP address i has behaviors that are similar to a infected host or not. It computes a reputation score for an IP address. The reputation score is assigned between 0 and 1. Score 0 represents low reputation (it means malware infected) and score 1 represents high reputation (it means not infected). We implement this reputation function as a statistical classifier.

We make use of three modules which are malicious DNS detector module, signature-based detector module and anomaly-based detector module to compute three output vectors

VII. EVALUATION

Our experiment was performed at a large local institute network for eight weeks. Note that, during experimental period of 2 months, the rst four weeks of experimenting is training period and the last four weeks is for testing. This large local institute network is a type of network with high value information, it tends to be attacked by advanced persist threat attackers. The network has a professional traf c monitoring equipment at the edge to monitor large volumes of inbound and outbound traf c, including the DNS traf c and C&C server traf c. The large local institute network has more than 30,000 users, during experimental period of two months, and we monitored approximately 400 million DNS queries.

The professional traf c monitoring equipment can provide us the monitoring traf c by rules of ``Source IP address'', ``Destination IP address'', ``Source Port'' or ``Destination Port''. During experimental period, we can submit the suspicious C&C server IP as the rule of ``Source IP address'' and ``Destination IP address;'' to the monitoring equipment at any time. Therefore, the C&C server traf c our system should record and analyze is small.
a group of bots, referred to as a botnet, which are remotely controlled by a C&C server and can be used for sending spam mails, launching DDoS attacks etc. The authors de ned feature ``group activity'' to detect botnet. The feature is iden-ti ed based on the judgement that the number of bots which queried botnet domain is xed in general. The group activity is formed by simultaneous DNS queries sent by a number of distributed bots. Most legitimate domain names are queried continuously but not simultaneously.

This anomaly-based detection mechanism can detect bot-net which is unknown or new to us. But this approach have intrinsic limits, it can only detect botnet consist of large numbers of bots. To reduce the risk of being detected, advanced attackers seldom use the same C&C server and domain to remotely control large numbers of compromised end-user machines.

In this paper, we propose a novel system IDnS placed at the network egress points to detect malware infections inside the network combined with DNS traffic analysis. We extracted new features and built a reputation engine based on big data, which includes approximately 400 million DNS queries. The experimental results show that our security approach is good at detecting APT malware infections and is feasible for improving

the sustainability of the system. The system processes advantages of high ef ciency and accuracy. We believe that IDnS is a useful intrusion system that can help to ght against cyber-crime especially theft of information from infected host.

REFERENCES

[1] F. C. Freiling, T. Holz, and G. Wicherski, ``Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks," *Lect. Notes Comput. Sci.*, vol. 10, no. 2, pp. 319 335, 2005.

[2] A. Karasaridis, B. Rexroad, and D. Hoe in, ``Wide-scale botnet detec-tion and characterization," in *Proc. 1st Conf. 1st Workshop Hot Topics Understand. Botnets*, 2007, p. 7.

[3] J. Jung, M. Konte, and N. Feamster, ``Dynamics of online scam hosting infrastructure," in *Proc. 10th Int. Conf. Passive Active Netw. Meas.*, 2009, pp. 219 228.

[4] H. Porras, H. Saïdi, and V. Yegneswaran, ``A foray into Concker's logic and rendezvous points," in *Proc. USENIX Conf. Large-Scale Exploits Emergent Threats, Botnets, Spyware, Worms, More*, 2009, p. 7.

[5] S. Yadav, A. K. K. Reddy, A. L. N. Reddy, and S. Ranjan, ``Detecting algo-rithmically generated malicious domain names," in *Proc. ACM SIGCOMM Conf. Internet Meas.*, 2010, pp. 48 61.

[6] J. Wolf. (2008). *Technical Details of Srizbi's Domain Generation Algorithm*. [Online]. Available: http://tinyurl.com/6mdasc

[7] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi, ``EXPOSURE: Finding malicious domains using passive DNS analysis," in *Proc. NDSS*, 2011.

[8] E. Stalmans and B. Irwin, ``A framework for DNS based detection and mitigation of malware infections on a network," in *Proc. Inf. Secur. South Africa (ISSA)*, Aug. 2011, pp. 1 8.

[9] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, ``Build-ing a dynamic reputation system for DNS," in *Proc. 19th USENIX Secur. Symp.*, 2010, pp. 273 290.

[10] LASTLINE. (2015). *Using Passive DNS Analysis to Automatically Detect Malicious Domains*. [Online]. Available: https://www.lastline. com/papers/dns.pdf

BIOGRAPHY

Ms.Saranya. N has received her B.E.degree in Computer Science and Engineering from Avinshilingam University, India,in2010,the M.E. degree in Computer Science and Engineering from Sasurie College of Engineering, India in 2012. She is an Assistant professor in Department of Computer Science

Mrs.Monica. G has received her B.E.degree in Information Technology from V.L.B Janakiyammal College of Engineering, India,in2010,the M.E. degree in Software Engineering from Ramakrishna College of Engineering, India in 2012. She is an Assistant professor in Department of Computer Science

S.Gayathri completed his B.E degree in computer Scienceand Engineering in from PACET and joined TechMahindra and plays her role as Design Associative Software Engineer.