Botnet Detection on the Analysis of Zeus Panda Financial Botnet

S Sarojini, S Asha

***Abstract:** Banking botnets, those particularly directed at holding away banking extortion, speak to a notable risk for financial institutes all around the world. These malware systems are reliable of immense monetary losses or for leading money laundering activities. As opposed to DDoS and spam malware, the stealthy idea of monetary botnets requires new methods and modern research with a specific end goal to detect,analyze and even to receive them down. This paper exhibits a work-in-advance research went for making a framework ready to moderate the money related botnet issue. The system demonstrated powerful when trialed against various samples of the notable malware Zeus panda and was confirmed further by analysis controlled with the financially.The proposed framework depends on a novel design that has been approved by one of the greatest investment funds banks and functionalities will demonstrate exceptionally helpful to fight banking cybercrime.*

***Index terms:** Botnet, Malware analysis, Banking Trojan,HTTP based.*

I. INTRODUCTION

Most cybercriminals is to theft the cash of unsuspected clients. There are numerous paths for cybercriminals to get to classified money related data, including financial balance accreditations [1].

Banking Trojans remain a best malware risk and have additionally been extending to versatile stages. In modern, directly of the way that help for a considerable lot of the old financial Trojans, for example, Zeus, Citadel or Spyeye has ceased, either intentionally or effect of law requirement activity, new formations of malware like Dyre or Dridex have showed up, the last focusing back-end payment transforming frameworks, Point of Sale (POS) frameworks and banking sector applications [3].Banking Trojans vary from standard Trojans, as they are composed for the express reason to theft private data from victims' financial balances and onlinepayment administrations. They are refined and furnished with Man-in-the-Browser (MiB) methods [5], for example, web injections or redirection systems. Zeus and its initial competition were progressive in the digital cyber-crime scene and were the firsts to utilize Man-in-the-Browser (MiB) systems.Zeus Panda is being solicited by means of Dark Web covered sheets by the designer who set up it together. It is sold in cybercrime-as-a-benefit bundles to other cybercriminals. The variation dubbed Zeus “Panda”/Panda Banker emerged in early 2016. The malware is based on the Zeus VM code base, however, does not contain the virtual machine feature.

The payload is typically ushered in by a malware downloader infection, and email spam campaigns related with Panda show that its operators target company employees rather than send indiscriminate spam to webmail addresses. In latest, Financial Trojans are as yet hitting the worldwide economy, with not a single end to be seen. While real financial Trojans, some of which are as of now dynamic for quite a long time, are propelling new battles, 2017 has seen some concern new families.

A.Zeus

Zeus was first seen in the wild in 2007 and most financial Trojans today are its relatives. Zeus is a general Trojan which targets Windows OS clients, has indirect access abilities, and is equipped for executing controller level capacities on the victim machines. The first Zeus spreading strategies were for the most part through drive-by-downloads and spam attacks utilizing Exploit Kits [19]. Zeus can run configurations and commands sent from its C&C (counting dropping and introducing other malware).

The first Zeus was a cybercrime-as-a-service - a criminal administration which permitshazard players to buy the utilization of a malware. Zeus was the leading in the financial Trojan world until late 2010, when its creator "resigned" and gave the malware's code to the creator of the Spyeye financial Trojan. Zeus' source code was exposure in 2011 [19], and presently numerous new variations and imitators are utilized by various risk performing artists.

According the researchers, the Zeus financial Trojan was progressive in a few regards:

- It was the initial malware to perform web injections.
- It fabricated one of the greatest botnets ever, with a bank ofinfections.
- Its polymorphic plan made it troublesome for security sellers to identify and chunk attacks in light of basic document hashes.
- The first malware and its variations are as yet applicable today.

II. WHAT ISZEUSPANDA

The new Zeus v2 variant known as “Panda” is targeting the URLs of personal online banking services of banks. The malware uses web-injection tactics, which include both technical changes and social engineering, to steal user credentials, take over victim accounts, and initiate fraudulent money transfers. Its target Zeus Panda configurations target bank, payments, card services, airlines, and online betting brands in Europe and North America [6].

Panda banker is a variation of zeus trojan which is famous for stealplenty of cash around world.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

S Sarojini*, PhD, School of Computing Science & Engineering, VIT University, Chennai, Tamil Nadu, India.

S Asha, Associate Professor, School of Computing Science & Engineering, VIT University, Chennai, Tamil Nadu, India.

It records clients' different framework actions without clients assent and authorization. Initially this Trojan was meant to target banks and spread through freeware, web browsing and framework utilities.

Zeus Panda is yet another Zeus v2 Trojan emphasis based upon a similar source code leaked— one that obviously continues empowering the transmission of more monetary financial Trojans into the worldwide.

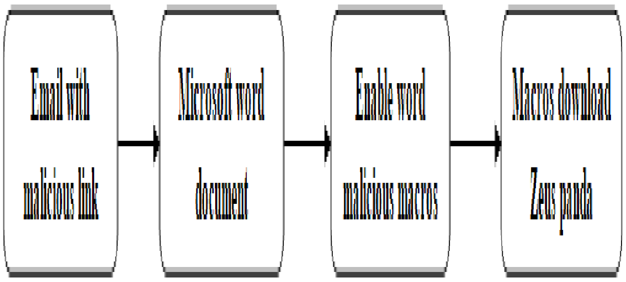

Email with malicious link
Microsoft word document
Enable word malicious macros
Macros download Zeus panda

Fig.1 Flowchart of zeus panda infection

While Panda designs center around focusing on individual internet financial services, they are somewhat various. Different targets incorporate internet payments, prepaid cards and web based infecting accounts.Besides including the URLs of significant banks in the nation, Panda's administrators are additionally inspired by infecting clients who get to transmission services, nearby system security equipment merchants [6]. Different targets incorporate client logins to an organization that offers ATM administration benefits and secure physical access innovation for banks.

In contrast with different Zeus Panda botnets, and most financial Trojan designs as a normal. An insight indicating Panda's administrators' feasible sources is the URL of a web-based internet administration that helps clients with current cash exchanges[17], top-up and profit by means of internet payments stages, payments, repayments through mobile administrators and then some.

III. METHODOLOGY

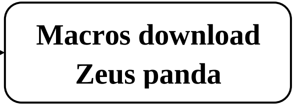
A. Network Traffic Separator

Network Traffic Separator is dependable to isolate HTTP web traffic from whatever is left of activity and posts them to centralized sector. The identical passing of network protocols, HTTP utilizes the HTTP protocoland client-server model: A HTTP customer opens a link and transmit a request message to HTTP server e.g."Get me the document to open url link [7]; the server at that point restores a response message. Laterpassing the response, the server ends the link. In the configuration of HTTP request message, HTTP strategies are to be engaged. Three normal HTTP techniques are "GET", "HEAD" or "POST". HTTP bots associates with their C&C intermittently (e.g. zeus botnet, Black Energy botnet). Subsequently, the traffic is reviewed and if the initial couple of bytes of a HTTP requestinclude"GET", "POST" or "HEAD"; it's the sign of HTTP protocol and isolating those streams and divert them to Centralized sector [8]. Along these lines, the activity set up from exterior host to inward hosts and from interior hosts to outer hosts are kept.

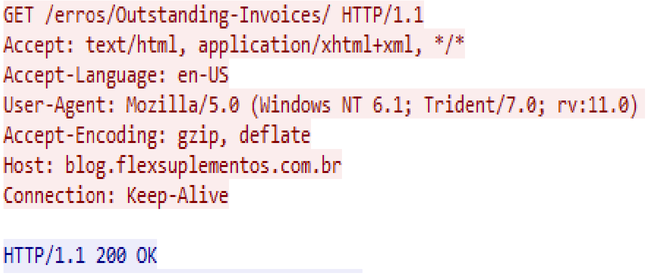
B. Transport Layer Security

Transport Layer Security (TLS) is a cryptographic network protocol that gives protection to applications. TLS is normally actualized over basic protocols, for example, HTTP for Simple Mail Transfer Protocol (SMTP) or web browsing for email. HTTPS is the utilization of TLS over HTTP. This is the most prominent method for securing connection between a web server and customer and is backed by most real web servers.

C. HTTP GET request



HTTP GET request for introduced in Fig. were sent forward through OPTIONS requests and had for the most part a similar source IP addresses. The general measure of GET requests with target port [8].



```
GET /erros/Outstanding-Invoices/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0)
Accept-Encoding: gzip, deflate
Host: blog.flexsuplementos.com.br
Connection: Keep-Alive

HTTP/1.1 200 OK
```

Fig.2 GET requests.

Byte distribution: The byte distribution describes the possibility that particular byte rate shows up in the payload of a packet inside a stream. The byte distribution of a stream can be determined utilizing a variety of counters. The real information standards related with byte distribution are full byte delivery [8], the mean/standard deviation of the bytes and byte entropy. For instance [27], utilizing one counter for each byte rate, a HTTP GET request, "HTTP/1.1.", can be determined by augmenting the comparing counter once for the "H," at that point increasing another counter twice for the two back to back "T" s and so on. In spite of the fact that the byte distribution is kept up as a variety of counters, it can simply be transformed into an appropriate distribution by controlling by the whole number of bytes.

D. Attack Details

The current attacks have been observed to actively deploy against European banking customers. The logical stages of the attack are described in this section, followed by further information about the Zeus “Panda” variation.

1. Zeus Panda’s operators opt to infect users via drive-by downloads and poisoned email attachments using popular crime-as-a-service exploit kits (Angler/Nuclear/Neutrino). Campaign targets are filtered by geography, similar to the way the GozNym Trojan keeps irrelevant endpoints out of country-specific campaigns.

2. The malware attack begins as soon as the infected victim attempts browsing to a targeted web application [17]. The malware hides the bank’s genuine page, and then sends a request to its command and control server requesting an external script.

IV. ANALYSIS

While there are plenty of malware applications out there that attempt to avoid recognition and analysis. Multi-analysis run malware tests in virtual machines, along these lines this approach is a first test at defeating inquiry [9]. What's more, multi tools which are utilized by investigator are likewise checked for: ProcMon, Regshot, Sandboxie, Wireshark, IDA and the SoftICE debugger. Unless the Command and Control (C2) channel is taken out [10], the gathered information heaps up on the framework until the point when it can be offloaded to an alternate C2 server.

Which operate is actuated relies upon the configuration of the malicious, which is downloaded naturally at general interims. So in actuality, ZeuS Panda [16] can transform from being a financial Trojan to being a remote control and spyware for a system throughout a couple of minutes, at the sole attention of the attacker.

A gathering of attackers is utilizing a sequence of man-in-the-browser for financial related keywords, malicious Microsoft Word macros and compromised sites to infected clients with the Zeus Panda bank accreditation stealer.

To define its attack targets and injection choices, Panda's modular structure fetches three separate configuration chunks:

The bot's *initial configuration* arrives with its dropper, but web-injections, malware modules, and advanced configuration options are downloaded from C&C in separate configuration files; the latter can also be removed by the C&C per the botmaster's choice.

Zeus Panda stores its malicious modules in encrypted form inside the Windows Registry. The web-injection configuration file is stored in an encrypted file on disk [16]. Paths specifying the location of all malware files and Registry keys are stored inside the bot's initial configuration chunk. Notably, the botnet communicates over a fast flux network to obfuscate Panda's actual infrastructure's IP address(es). The malware checks for connectivity by browsing to the Russian Yandex.ru search engine, which could be a hint to its operators' origins or whereabouts.

On top of its web-injection schemes, which are based on Zeus v2's code, the Zeus Panda variant at hand further orchestrates fraudulent transactions through a web-injection control panel (ATS) [12]. The web-based panel provides its malicious operators with a Jabber-based instant notification interface to alert the fraudster when new transactions are underway.

A. *Initial Attack Vector*

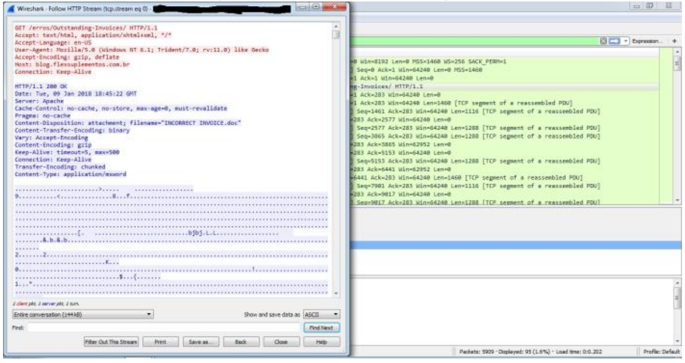
The primary vector used to start this infection method does not seem to be email based. By utilizing composed web servers, the attacker could guarantee that their malicious outcomes would be positioned profoundly inside web crawlers [12], in this way improving the probability that they would be tapped on by hidden victims.

Incidentally we have detected a similar redirection framework and related foundation used to guide victims to technical support and fraudulent AV scams that show pictures advising casualties that their frameworks are affected with Zeus.

B. *Infection Process*

At the point when the malware website pages are collected to by victims, the negotiated websites utilize Javascript to divert customers to Javascript facilitated on an intermediate webpage.

This outcomes in the clients executing and recovering Javascript situated at the address indicated by the document.write() technique. The successive page incorporates comparative services, this time bringing about a HTTP GET inquiry [12] to different page.



Wireshark · Follow HTTP Stream (tcp.stream eq 0) · [redacted]

```
GET /erros/Outstanding-Invoices/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: blog.flexsuplementos.com.br
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 09 Jan 2018 18:45:22 GMT
Server: Apache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="INCORRECT INVOICE.doc"
Content-Transfer-Encoding: binary
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/msword

........................>.....    ................
9..........<..............8...f.........................................
........................................................................
........................................................................
........................................................................
........................................................................
.................[.   .........................bjbj.L.L..................
.......&.b.&.b..........................................................
.......
2.......2...............................................................
..........................K...
0...........................................................!...........
...........................$...{.......
1...*...................................................................
```

```
0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
=1 Ack=1 Win=64240 Len=0
ng-Invoices/ HTTP/1.1
=1 Ack=283 Win=64240 Len=0
=1 Ack=283 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
] Seq=1461 Ack=283 Win=64240 Len=1116 [TCP segment of a reassembled PDU]
=283 Ack=2577 Win=64240 Len=0
] Seq=2577 Ack=283 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
] Seq=3865 Ack=283 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
=283 Ack=3865 Win=62952 Len=0
=283 Ack=5153 Win=64240 Len=0
] Seq=5153 Ack=283 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
=283 Ack=6441 Win=62952 Len=0
=6441 Ack=283 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
] Seq=7901 Ack=283 Win=64240 Len=1116 [TCP segment of a reassembled PDU]
=283 Ack=9017 Win=64240 Len=0
] Seq=9017 Ack=283 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (144 kB)

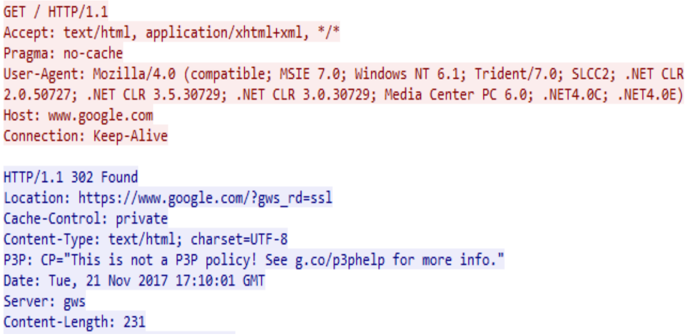
Show and save data as: ASCII

Packets: 5909 · Displayed: 95 (1.6%) · Load time: 0:0.202

Profile: Default

Fig. 3 HTTP 302 server

The intermediate server will then react with a HTTP 302 which diverts clients to different compromised website which is really being utilized to have a malicious Microsoft Word document. Subsequently, the clients will take after this download and redirection the malicious report [13]. This is a strategy ordinarily assigned to as "302 padding" and is usually utilized by exploit kits.

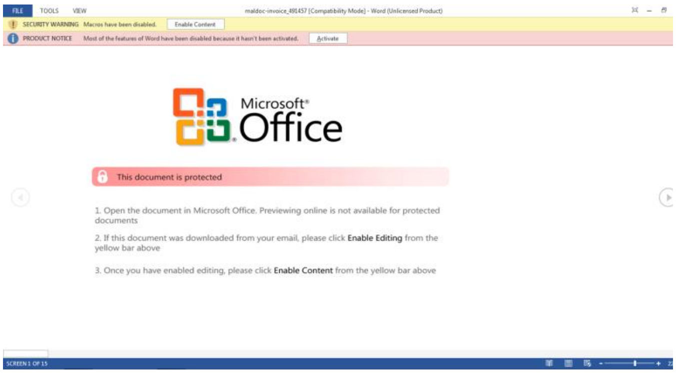


```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: www.google.com
Connection: Keep-Alive

HTTP/1.1 302 Found
Location: https://www.google.com/?gws_rd=ssl
Cache-Control: private
Content-Type: text/html; charset=UTF-8
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Tue, 21 Nov 2017 17:10:01 GMT
Server: gws
Content-Length: 231
```

Fig. 4 HTTP 1.1 request

Following the download of the malicious Microsoft Word document, the casualty is incited by their web program to Open or Save the document. Whenever opened [27], the record shows the successive message, provoking the infected to "Enable Editing" and snap "Enable Content".



maldoc-invoice_491457 [Compatibility Mode] - Word (Unlicensed Product)

SECURITY WARNING Macros have been disabled.

PRODUCT NOTICE Most of the features of Word have been disabled because it hasn't been activated.

This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents

2. If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

3. Once you have enabled editing, please click **Enable Content** from the yellow bar above

Fig. 5 Execution of malware macro word report

Following these guidelines will bring about the execution of malware macros that have been inserted in the Microsoft Word report. It is these macros that are in charge of downloading and executing a malware executable, subsequently infecting the framework. The macro cipher itself is complicated, and perfectly key. It just downloads the malware executable [21], recovers it into the %TEMP% registry on the framework utilizing the filename, for example, "obodok.exe".

To check what number of various packets captures connections with our virtual environment every day. The outcome is appeared in Fig.In Fig. 6, an extraordinary difference of packets captures every day can be seen, going from malware traffic analysis.

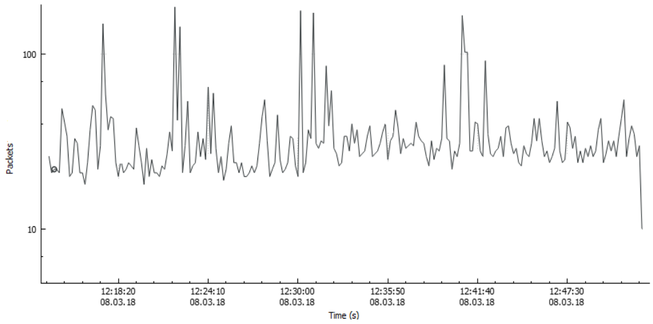


Fig.6 packets captured through traffic analysis

To additionally check the detected domains, we utilize VirusTotal to analysis these domains. As appeared in Table I, domain names are recognized as malicious spaces while others are identified. Note that VirusTotal essentially totals the yield of variousURL scanners and SHA. SHA analyses the hostname generation, bot id, object name generation and data sent by command and control server. It doesn't give a standard answer of malicious control-domain space [26].We gather the outer threat knowledge of this detection rate of domains, for example, DNS records and document communication records, and utilize these data to develop a connection chart of domain.

Domain	SHA-256	Detection rate
blog.flexsuplementos.com	b50abf33fc40a78e2dd5901e4142f0b419f6653ee346002d74238f4f83e2e83f	9/68
evisu.co	d446d7e2cadfe653fd4fe72a1c6e46d1e09aa31245d013d81bb5a9b9a2d5c4ec	7/68
katinka.org	d6023499346836cae4f434e916e962cd8d8f1b4e9326ac6f9e7c06664dde36b6	3/68
rendomunza.gdn	538f31569367cebb992643e46213f223fc20113e63a2e814a1dcb64a858ffb2e	5/68
namingotslon.gdn	538f31569367cebb992643e46213f223fc20113e63a2e814a1dcb64a858ffb2e	7/68
camorata.com	8e44badbfd604ea66e65d086dad66f0498083d2db8a5ca1b1d9f980e10212f6c	5/67
dorothyle.net	8e44badbfd604ea66e65d086dad66f0498083d2db8a5ca1b1d9f980e10212f6c	5/67

V. CONCLUSION

Attackers are always attempting to discover better approaches to decoy clients to run malicious that can be utilized to infect the casualty's PC with different payloads. Malvertising, Spam and watering-hole attacks are generally used to target clients.To prevention of banking Trojan injection incorporates harming advertisements and maintaining a strategic websites commonly used as hub of infected vector, website like adult content, free gaming and torrents to give some examples [25]. Likewise, since Panda Banker and related to financial malware is generally forwarded as email connections, never tap on attachments or links in unwanted email.To help stop risks like Panda Banker, banks and specialist organizations can utilize flexible malware identification configurations and secure client endpoints with malware knowledge that gives legitimate understanding into fraudster methods and abilities.

REFERENCE:

1. S.S.Garasia,D.P.Rana, R.G.Mehta,"Http Botnet Detection Using Frequent Pattern set Mining",International journal of engineering and advanced technology,Volume 2,June 2012.
2. Thomas Vissers , Thamarai Selvi Somasundaramb, Luc Pieters ,Kannan Govindarajan, Peter Hellinckx ,"DDoS defense system for web services in a cloud environment", Sciencedirect, Volume
3. , July 2014, Pages 37-45, Jan 2014.
4. Wang Jin ,Zhang Min, Yang Xiaolong, Long Keping ,XU Jie, "Http-sCAN: Detecting Http-Flooding by Modeling Multi-Features of Web Browsing Behavior From NoisyWeb logs,"IEEE Transaction on network technology and applications,Feb 2015.
5. Kirubavathi Venkatesh, R. Anitha Nadarajan," HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network," Department of Mathematics and Computer Applications PSG College of Technology, Coimbatore.

6. Chris Cain,"Analyzing Man-in-the-Browser (MITB) Attacks," SANS Institute whitepapers, Dec.2014.
7. http://www.securityweek.com/new-panda-banker-trojan-borrows-code-zeus.
8. Kuochen Wanga, Chun-Ying Huan,"A fuzzy pattern-based filtering algorithm for botnet detection" Feb 2015,ScienceDirect transaction on computer networks,Volume 55, Issue 15, 27 October 2011, Pages 3275-3286.
9. Esraa Alomari,Selvakumar Manickam,B. B. Gupta,Parminder Singh,Mohammed Anbar,"Design, Deployment and use of HTTPbased Botnet (HBB) Testbed ",Advanced Communication Technology (ICACT), 2014 16th International Conference on IEEE,16-19 Feb. 2014.
10. Rajab MA, Zarfoss J, Monro se F, Terzis A. "A multifaceted approach to understanding the botnet phenomenon", In: Proceedings of the 6th ACM SIG COMM conference on Internet measurement. New York: ACM; 2006.
11. Basil As Sadhan , Jose M.F. Moura "An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic ",ScirnceDirect Journal of Advanced Research,Volume 5, Issue 4, July 2014, Pages 435-448.
12. S. Garca, M. Grill, J. Stiborek, A. Zunino ,"An empirical comparison of botnet detection methods ",ScienceDirect Computers and Security Volume 45, September 2014, Pages 100-123.
13. Roberto Perdisci , Wenke Lee, and Nick Feamster, "Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces ",ACM Proceeding NSDI'10 Proceedings of the 7th USENIX conference on Networked systems design and implementation, Pages 26-26.
14. David Zhao, Issa Traore , Bassam Sayed, Wei Lu, Sherif Saad , Ali Ghorbani , Dan Garant,"Botnet detection based on traffic behavior analysis and flow intervals ", ScienceDirect Computers and Security,Volume 39, Part A, November 2013, Pages 2-16.
15. Joakim Ersson, Esmirald Moradian, "Botnet Detection with Event-Driven Analysis",ScienceDirect Procedia Computer Science,Volume 22, 2013, Pages 662-671.
16. R.Kannan ,A.V.Ramani,"Flow Based Analysis to Identify Botnet Infected Systems ",Journal of Theoretical and Applied Information Technology 20th September 2014. Volume 67.
17. https://www.proofpoint.com/us/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market.
18. https://securityaffairs.co/wordpress/65150/cyber-crime/black-seo-zeus-panda.html.
19. P. Wurzinger, L. Bilge, T. Holz, J. Goebel, C. Kruegel, and E.Kirda,"Automatically generating models for botnet detection," in Computer Security–ESORICS, Springer Berlin Heidelberg, 2009, pp. 232-249, doi:10.1007/978-3-642-04444-1_15.
20. H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M.Debbabi, and L. Wang, "On the analysis of the zeus botnet crimeware toolkit," Eighth Annual International Conference on Privacy Security and Trust (PST 2010), 2010, pp. 31-38, doi:10.1109/PST.2010.5593240.
21. W. Lu, M. Tavallaee, and A.A. Ghorbani, "Automatic discovery of botnet communities on large-scale communication networks," Proc. 4th International Symposium on Information, Computer, and Communications Security, ACM, Mar. 2009, pp. 1-10, doi:10.1145/1533057.1533062.
22. M. Castelluccio, "The most notorious hacks of 2016," Strategic Finance, 98(7), 55, 2017.
23. T.-F. Yen et al., "Beehive: LargeScale Log Analysis for Detecting Suspicious Activity in Enterprise Networks," in Proc. Ann. Computer Security Applications Conference (ACSAC 13), ACM, Dec. 2013.
24. A. K. Seewald and W. N. Gansterer, "On the Detection and Identification of Botnets," Computers & Security, vol. 29, pp. 45-58, 2010.
25. W.T. Strayer, R. Walsh, C. Livadas, and D. Lapsley, "Detecting botnets with tight command and control," Proc. IEEE Conference on Local Computer Networks, IEEE Press, Nov. 2006, pp. 195-202,
26. doi:10.1109/LCN.2006.322100.
27. JS Lee, "The Activity Analysis of Malicious HTTP-based Botnets using Degree of Periodic Repeatability," Security Technology, 2008.
28. Rahbarinia, Babak, Roberto Perdisci, and Manos Antonakakis. "Efficient and Accurate Behavior-Based Tracking of Malware-Control Domains in Large ISP Networks" ACM Transactions on Privacy and Security, Vol. 19, No. 2, Article 4, Publication date: August 2016.
29. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext Transfer Protocol, HTTP/1.1," RFC 2616,1999.

AUTHORS PROFILE

S.Sarojini, is a PhD Candidate at the School of Computing Science and Engineering, VIT University, Chennai. She received her M.S in Software Engineering in 2015 from the VIT University. She enrolled in VIT Chennai to initiate her PhD studies in January 2016 in the field of cyber security, Machine learning, Deep learning and Network Forensics.

Dr. S. Asha, is an Associate Professor from the School of Computing Science and Engineering, VIT University, Chennai. She graduated from Madras University, Chennai and completed her PhD from Anna University Chennai. Her area of interest includes Network security, Biometric security, Computational Intelligence, Cloud security and Cybersecurity.Shehaspublishednearly25papersin international journal and conference. Currently she is working in computational intelligence and Cyber security.