Design, Deployment and use of HTTP-based Botnet (HBB) Testbed

Esraa Alomari**, Selvakumar Manickam*, B. B. Gupta***, Parminder Singh*, Mohammed Anbar*

**National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Malaysia*

***University of Wasit, Iraq, Wasit*

****National Institute of Technology Kurukshetra, India*

{esraa,selva,parminder,anbar@nav6.org}, gupta@gmail.com

***(Pt9)Abstract*— Botnet is one of the most widespread and serious malware which occur frequently in today's cyber attacks. A botnet is a group of Internet-connected computer programs communicating with other similar programs in order to perform various attacks. HTTP-based botnet is most dangerous botnet among all the different botnets available today. In botnets detection, in particularly, behavioural-based approaches suffer from the unavailability of the benchmark dataset and this lead to lack of precise results evaluation of botnet detection systems, comparison, and deployment which originates from the deficiency of adequate datasets. Most of the datasets in the botnet field are from local environment and cannot be used in the large scale due to privacy problems and do not reflect common trends, and also lack some statistical features.**

To the best of our knowledge, there is not any benchmark data set available which is infected by HTTP-based botnet (HBB) for performing Distributed Denial of Service (DDoS) attacks against Web servers by using HTTP-GET flooding method. In addition, there is no Web access log infected by botnet is available for researchers. Therefore, in this paper, a complete testbed will be illustrated in order to implement a real time HTTP-based botnet for performing DDoS attacks against Web servers by using HTTP-GET flooding method. In addition to this, Web access log with http bot traces are also generated. These real time datasets and Web access logs can be useful to study the behaviour of HTTP-based botnet as well as to proposed different solutions to detect HTTP-based botnet for the researchers who are new to this research domain.

***Keyword*— Cyber attacks, Botnet, DDoS attacks , HTTP-based botnet, HTTP flooding**

Esraa Alomari has done a Bachelor in Computer Science from computer collage- Al-anbar University-IRAQ in 2003 and received her MSc. Degree in Computer Science from University of Technology-IRAQ in 2006. Currently, she is a PhD student in National Advanced Center of Excellence (Nav6) in University Sains Malaysia (USM). Her research interest includes Advances internet security and monitoring, Botnet and Cyber attacks. She is member of the IPv6 Forum Global Education where she plays a role in the validation of IPv6 engineers, trainers and courses worldwide. In addition, she is actively involved in conducting professional courses on IPv6, including Certified IPv6 Network Engineer (CNE6) Level 1&2.

Selvakumar Manickam is Deputy Director at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He received his Bachelor of Computer Science and Master of Computer Science in 1999 and 2002, respectively. He has published more than 80 papers in journals, conference proceedings, book reviews, and technical reports. He has also given several key note speeches as well as dozens of invited lectures and workshops at conferences, international universities and for industry. He has given talks on IPv6, Internet Security, Green ICT and Open Source technologies at various organizations and seminars. Currently, he spearheads a number of key clusters under National Advanced IPv6 Centre, namely Internet Security, Cloud Computing, Android and Open Source Technology, focusing on conducting scientific research in respective areas. He manages two teams, network and system support team and the software and web application team. He holds various research grants in the university at national and international level. Due to his proven expertise in Internet Security, he has also been given the responsibility to lead the Internet Security Working Group of the Malaysian Research and Education Network (MYREN) to facilitate collaboration among researchers and other security enthusiasts nationwide. He is an Executive Council member of Internet Society (ISOC) Malaysian Chapter. He is also an appointed core member of the IPv6 Forum Global Education where he plays a role in the validation of IPv6 engineers, trainers and courses worldwide. He is involved with International Telecommunication Union (ITU) in which he runs online trainings on IPv6 topics. Apart from that, as senior trainer, he is actively involved in conducting professional courses on Android, Web Application Development and IPv6, including Certified IPv6 Network Engineer (CNE6) Level 1&2 and Certified IPv6 Security Engineer (CSE6). He is also involved in the development of next generation network monitoring platform and plays the role of project manager and an avid ANSI C programmer.

B. B. Gupta (gupta.brij@gmail.com) received PhD degree from Indian Institute of Technology Roorkee, India. In 2009, he was selected for Canadian Commonwealth Scholarship and awarded by Government of Canada award. He has published more than 45 research papers in International Journals and Conferences of high repute. Dr Gupta is also holding position of editor of various International Journals and magazines. He also worked as a post doctoral research fellow in UNB, Canada. His research interest includes Information security, Cyber Security, Intrusion detection, Computer networks and Phishing.

Parminder Singh is a visiting researcher at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia and Principle Consultant at DCS1 Enterprise Solutions private Limited. He is a skilled and result oriented professional with 15+ years of experience in the IT industry and working in key managerial and technical positions. He has an edge over technical aspects such as ethical hacking, operating systems, scripting and databases. He is leading the teams of Internet Security, Cloud Computing and Open Source Technology, and focusing on conducting scientific research in respective areas. He is also an active Member of Internet Security Working Group of the Malaysian Research and Education Network (MYREN). He is member of the IPv6 Forum Global Education where he plays a role in the validation of IPv6 engineers, trainers and courses worldwide. In addition, he is actively involved in conducting professional courses on IPv6, including Certified IPv6 Network Engineer (CNE6) Level 1&2 and Certified IPv6 Security Engineer (CSE6).

Mohammed Anbar is a Post Doctoral Fellow in National Advanced IPv6 Centre of Excellence (NAV6) at Universiti Sains Malaysia (USM), Malaysia. He holds a PhD in the area of Advanced Computer Networks, M.Sc. in Information Technology, and B.Sc. in Computer System Engineering. His research interest includes Malware Detection, Web Security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and network monitoring.