Botnets: Rise of the Dark Dragon

One of the most significant threats to the internet today is the threat of Botnets “zombie armies”. These are networks of large numbers of “bots” that runs automatically and autonomously. They are remotely controlled by a master host through one or more controller host(s). These “bots” are used for malicious activities: The perpetrators use the master host to relay their commands to the “bots” via the controller hosts. These controllers could be IRC servers that are normally used to relay messages between clients. The “Bots” can be differentiated from other threats by quite a few ways. One of It is that they have communication channels to a controller host. Thus, “Bots” inherits the ability to hide like viruses, propagate like worms, and provide cyber criminals the “perfect” platforms with which to commit their crimes.

This talk describes Bots, Botnets and Bot Controllers. This moves onto a discussion on the areas of Bot involvement on the Internet and then the presentation provides an in-depth and interesting view of some of the most prominent Bot attacks in history

BRIEF BIODATA

Professor Emeritus Sureswaran Ramadass is a Professor at the Malaysian University of Science and Technology (MUST). He is also the Chief Scientist at NLTVC Sdn Bhd, a Next Generation Internet Communications Research and Development company. He heads the Cybersecurity and CyberWarfare Division of the company. He also currently serves as the founding Chairman of the ITU/UN Center for IPv6 and IOT.

He obtained his BsEE/CE (Magna Cum Laude) and Masters in Electrical and Computer Engineering from University of Miami in 1987 and 1990 respectively. He graduated top student from the College of Engineering. He obtained his PhD from Universiti Sains Malaysia in 2000 while serving as a full-time faculty member in the School of Computer Sciences.

Some of his recognitions include being awarded:-

- *Malaysian Innovation Award by the Minister of Science and Technology in 2009. This Award was given in recognition for his contribution to innovative research and development in the area of Advanced Network and IPv6 Security and Monitoring.*

- *The "Anugerah Tokoh Negara" (National Academic Leader) for Innovation and Commercialization in 2008 by the Minister of Higher Education. This award is given to an academic in recognition to his contribution to innovation and commercialization in the area of science and technology.*

- *Malaysian Innovation Award by the Prime Minister in 2007. This Award was given by the Prime Minister in recognition for his contribution to innovative research and development in the area of Advanced and Secure Collaborative Communication Systems.*

- *The Wireless World Research Forum Fellow in April 2010. This fellowship award was presented in recognition to his contribution in the area of Next Generation Networks including security.*

- *Emeritus Chair, APAN Ltd*

- *Emeritus Chair, IPv6 Forum Education Programme.*
- *Professor Emeritus, Malaysia University of Science and Technology*

Prof Sures established the National Advanced IPv6 Centre of Excellence (NAV6) in Universiti Sains Malaysia. As the Founding Director of NAv6, Prof Sureswaran focused on promoting MSc and PhD studies in IPv6, CyberSecurity and Next Generation Internet Communications. He personally supervised over 10 PhD students in Internet Security domain. Under his leadership, NAv6 became self sustaining and the highest consultancy revenue earner for USM. It was ranked the number one department in USM.

Prof Sureswaran is involved in the Global IPv6 Forum and is the Emeritus Chair IPv6 Forum Education Certification Program. He is also the Malaysian IPv6 Forum Chairman. Prof Sureswaran was also one of the founding members of MYREN (Malaysian Research and Education Network) and is currently the IPv6 Domain Head. He was the Chairman of the Asia Pacific IPv6 Task Force (APV6TF) and was involved in promoting IPv6 within the region and globally.

He was Chairman of APAN (Asia Pacific Advanced Networks) from 2014-2015, during which APAN grew stronger and established closer ties with its partnering organisations. He was the Primary Founding Member as well as the Head of APAN Malaysia. He had earlier held positions as WG chair, Area Chair, Director and Treasurer for APAN.

Prof Sureswaran actively participates in the global IPv6 arena. This includes being a consultant to International Telecommunication Union (ITU). His expertise was valuable in formulating a proposal on the expansionary approach to Global IPv6 Address Allocation. He also provided expert feedback on Internet Security issues to ITU.

In 2008, Prof Sures became the Director of Research for IMPACT (International Multilateral Partnership Against Cyber-Terrorism). IMPACT is an Agency to ITU and the United Nations (UN) to focus on Cyber Threats. He and his team focused on Botnets and the effects of Botnets, especially on developing nations. The team also indentified and catalogued signatures of potential treats, including worms which were polymorphic and encrypted. This included time domain based signature analysis for Spam Bots and other areas.

In 2010, Prof Sures established the Cyber Security Research Cluster. As the Chair of this cluster, he established indept research into the field of Botnets. The cluster was supported by over 20 MSc and Phd researchers. The focus was on creating a sustainable echosystem for Botnet Security Research.

In the world of Innovation and Commercialization, Prof Sureswaran founded and headed the team that successfully took Mlabs Systems Berhad, a high technology video conferencing company to a successful listing on the Malaysian Stock Exchange in 2005. Mlabs is the first university based company to be listed in Malaysia. He currently still serves on the Boarf of Mlabs as well as the advisory boards of numerous technology companies.

Prof Sureswaran is the founder of the globally recognized CNE6 (Certified Network Engineering IPv6 Program). He actively assisted numerous training organizations and companies globally to provide and expand their IPv6 Certified Engineering Training Programs. This includes the CSE6 (Certified Security Engineer IPv6) Silver and Gold Courses. He took the lead in the planning and migration of the Pilot IPv6 Migration Projects in Malaysia. He also assists governments and organizations globally to help develop their IPv6 environment, including being a member of the Indian IPv6 Task Force.

Prof Sureswaran's academic contributions are vast and have attracted numerous academic and research ventures to the university and state. He has published research papers in over 200 international and national level journals, research conferences and research presentations. He has filed over 12 patents of which 6 have now been awarded. He has given numerous keynote addresses to global audiences around the world. He has written chapters and provided materials for 9 books. He has chaired numerous international conferences and has reviewed papers for over 30 international and national level publications. He has received over RM20 million in research funding and grants from numerous organizations in the 20 years that he has been with the university. He has also received over 40 International and National level awards for Innovation and Research. He has graduated 20 PhD students till date.

Jan 2017