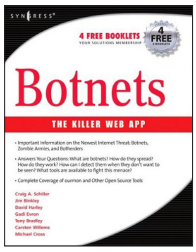
BOOK REVIEW

LET'S KICK SOME BOT!

Martin Overton
Independent researcher, UK



Title: Botnets – The Killer Web App
Author: Craig A. Schiller, Jim Binkley et al.
Publisher: Syngress
ISBN: 1-59749-135-7
Cover Price: $49.95

This book covers what has become a hot topic in the security community since the move by cybercriminals and spam gangs towards business models that involve building and exploiting vast numbers of 'zombie' machines scattered all over the globe. These machines are infected by bots and collected, used, rented and traded by cybercriminals.

So, what does the book cover, and more importantly, does it deliver on the promises it makes?

COVER STORY?

The book's cover claims that it will provide:

- Important information on botnets, zombie armies and bot herders.
- Answers to your questions: What are botnets? How do they spread? How do they work? How can I detect them when they don't want to be seen? What tools are available to fight this menace?
- Complete coverage of *ourmon* and other open source tools.

UNDER THE COVERS

The book contains 12 main chapters and a single appendix. Each chapter starts with what *Syngress* calls 'Solutions in this chapter' (even when the chapter is all about threats, not solutions), and concludes with a summary, FAQ and a 'Solutions fast track' section.

Chapter 1 discusses why the botnet is such a powerful tool (or toolkit). The authors state: 'The software that creates and manages a botnet makes this threat much more than the previous generation of malicious code. It is not a virus; it is a virus of viruses.' I beg to differ: most (if not all) bots are not viruses at all; most are remote access trojans (RATs) or worms.

The next section offers a concise look at 'A conceptual history of botnets', which starts with the birth of IRC itself and GM, the first IRC bot. Next stop is PrettyPark, which the chapter's author claims is the prototype for today's bots.

SubSeven is also mentioned before we move to what I consider to be the real prototypes of modern bots: GTbot and the grand-daddy of most modern bots, SDbot (the first bot to be written in C/C++ and most importantly, its source code was made available). Other bots covered in this section are the usual suspects: Agobot, Spybot, Rbot, Polybot and finally Mytob.

BOTNETS FOR DUMMIES

Moving on, we come to 'Cases in the news', which covers the stories of some of the cybercriminals who have successfully been prosecuted, such as: THr34t-Krew, Axel Gembe and Resili3nt (aka Jeanson James Ancheta) and Farid Essebar (the author of Zotob), amongst others.

Wrapping up Chapter 1 is 'The industry responds', a section covering a brainstorming session in August 2006 – almost a year after the VB2005 conference at which a number of papers on bots and botnets had been presented and a lot of brainstorming and discussion of the problem had taken place.

Chapter 2 continues with the same 'botnets for dummies' approach and covers: 'What is a botnet?', 'The botnet life cycle', 'What does a botnet do?' and 'Botnet economics'. All in all, this is quite a good overview of bots and botnets for those who haven't come across them before and need to know the fundamentals.

Chapter 3 introduces the reader to 'Alternative botnet C&Cs', starting with a look at the 'Historical C&C technology as a road map' and continuing this voyage of discovery with 'DNS and C&C technology' (which is more useful as it covers newer techniques that are increasingly being used in place of traditional IRC command and control infrastructures). These include web-based, command-based, P2P and IM command and control systems or infrastructures. It also includes some of the advanced DNS techniques, such as dynamic and fastflux DNS records which allow botnet C&Cs to be more resilient than previously when they tended to use hard-coded IP addresses in the bots' bodies or configuration files.

Chapter 4 covers common botnets and includes a more in-depth look at Sdbot, Rbot, Agobot, Spybot and Mytob, detailing known aliases, infection, signs of compromise such as common registry keys, filenames, ports and propagation techniques used.

Chapter 5, 'Botnet detection: tools and techniques', opens with 'Abuse', or to put it another way, emails to your 'abuse@company.com' address complaining that your domain is doing something bad, such as spamming, phishing, DDoSing or hosting malware/spyware or other bad stuff. For many, this will be the first clue that part of their network is under someone else's control.

The next section, 'Network infrastructure: tools and techniques', covers the likes of SNMP, netflow, firewalls, switches, hubs, routers and the use of ACLs and logs from these types of devices/services.

Intrusion detection is the next area to be discussed, including some coverage of anti-virus, with information on signatures and heuristics. *Snort* is covered in some detail as an example IDS, along with a number of example signatures which are dissected and explained well. Integrity management systems are also covered.

Some material on darknets, honeypots and 'other snares' is then given, before the rest of the chapter covers in more detail how you can use the tools/techniques mentioned in the first half of the chapter to fight back.

BOTNETS FOR TECHIES

Chapter 6 offers an overview of *ourmon*, starting with some case studies and then explaining how it works and how it is installed. In a nutshell, *ourmon* is a network-monitoring tool that the author claims can be used for 'low-level anomaly detection and higher-level detection of botnets'.

Chapter 7 covers *ourmon*'s web interface as well as using it to detect TCP, UDP and email anomalies. In my opinion, chapters 6 and 7 are not suitable for those with little or no computer security/network experience.

Chapter 8 discusses the IRC protocol, then moves swiftly on to 'Ourmon's RRDTOOL statistics and IRC reports'. The chapter is wrapped up with 'Detecting an IRC botnet' and 'Detecting an IRC botnet server'. Chapter 9 is also dedicated to what seems to be the authors' favourite tool. This time it covers advanced *ourmon* techniques. As with the previous *ourmon* chapters, this would not be suitable for non-techies.

Chapter 10 covers the use of sandbox tools. It starts by explaining what a sandbox is and mentions not only a number of well-known sandboxes, but also 'real' systems and virtual machines used for the same purpose, rather than the emulated ones that sandboxes usually use. The rest of the chapter focuses on one of the better-known sandboxes, *CWSandbox*, which is described as 'an application for the automatic behaviour analysis of malware' – a good description of what it does. Yet again, though, this is not suitable for non-techies.

Chapter 11 is entitled 'Intelligence resources', and identifies the information that an organisation should try to gather. It also covers disassemblers (although why this is included here rather than in chapter 5 or 10 is beyond me). Next, a list of places/organizations that provide information about botnets is provided. The short list includes anti-virus and

anti-spyware sites as well as *Microsoft*'s security site. A list of 'Professional and volunteer organizations' includes a number of mailing lists as well as groups such as NANOG, APWG and UNISOG. Interestingly, there is no mention of AVIEN or AVIEWS.

Finally, chapter 12 is entitled 'Responding to botnets'. Here, the authors state that 'giving up is not an option', which seems to be at odds with the data on the front and back covers and in the book's own introduction. Another section asks 'Why do we have this problem?', which may have been more useful at the start of chapter 1. The usual suspects are named: phishing, spam and money, as well as touching on policies and processes (or lack thereof) within organisations.

The final section asks 'What is to be done?', which is a good question, but it's a shame they left it to the last chapter to try and answer it. The answers offered include effective practices for individual and enterprise computer users as well as reporting botnets to some or all of the groups mentioned in the previous chapter. The section is completed with 'Fighting back', which covers the saga of *Blue Security*, and 'Law enforcement', which details how to report a botnet (although no suggestions are given for those of us outside the US). It swiftly covers darknets, honeynets and botnet subversion in very little detail and finishes with 'A call to arms'.

CONCLUSIONS

This book is very good in parts; chapters 5 and 10 are excellent. Chapters 1 to 4 are a good introduction to the subject and could easily have been extended into a 'botnets for dummies' type of book. However, chapters 6 to 9 are far too technical for a non-techie or a techie that doesn't have lots of security and network knowledge/experience.

I'm left with a strong impression that this book was rushed to market, as it seems to be two books in one. The really technical stuff and the *ourmon* chapters belong in an advanced book, while the rest of the material could easily have been expanded and sold as an introductory or intermediate-level guide (in my opinion this would have been a significantly better move by the publishers).

As it stands, the book will be of no real use to those not already in IT or security with at least a year of real hands-on experience, and I suspect that the 'propeller-heads' won't get much out of it either, apart from the material on *ourmon*. However, as a single reference tome, it will end up on many bookshelves in organisations worldwide.

Things may improve if and when the book is revised, or another publisher comes up with another book on botnets. Until then it will be a one-horse race, so for now this book is the de facto winner.