

# Proactive Botnet Countermeasures – An Offensive Approach

Felix Leder, Tillmann Werner, Peter Martini  
Institute of Computer Science IV, University of Bonn, Germany

March 26<sup>th</sup>, 2009

## 1 Background

A botnet is an alliance of interconnected computers infected with some malicious software (a bot). Bots are commanded by an operator and can typically be advised to send Spam mails, harvest information such as license keys or banking data on compromised machines, or launch distributed denial-of-service (DDoS) attacks against arbitrary targets. New machines are infected in various ways: Some bots have self-spreading behavior and compromise systems via unpatched security holes. Others successfully focus on Spam campaigns with e-mails that trick users into downloading and executing bot clients.

Several thousand distributed DDoS attacks are launched by botnets each month<sup>1</sup>. Recent efforts try to mitigate DDoS by filtering and sinkholing related traffic at border routers. These countermeasures are reactive as they deal with attacks at the time they are occurring. In addition, such mitigation systems require close cooperation of network providers, have limited capacity, and scale only to a certain extent. As a consequence, efforts for null-routing attempts eventually lead to an arms' race. It is thus necessary to evaluate more offensive, proactive strategies for botnet mitigation. In our work, we discuss that today's botnets generally have immanent vulnerabilities which make them attackable by design. Moreover, we argue that even modern botnets based on sophisticated malware can be infiltrated, mitigated and eventually taken down. We will demonstrate our ideas using the examples of *Storm Worm*<sup>2</sup> and *Waledac*, two of the most dangerous malware specimens observed so far. *Kraken* and *Conficker* will also be discussed, botnets with an estimated size of several million infected machines. While it is technically possible to take over most botnets, legal aspects must be taken into consideration.

## 2 Methodology

Bots are constantly spreading. Hence, it is relatively easy to observe and trap samples which can be analyzed afterwards to gain insights into the structural details of the underlying botnet. Further, each infected machine has to communicate with its botnet. With knowledge of the protocol used it is possible to take part in the internal botnet communication. These two facts – the ability to trap bot samples, and the immanent property that everybody is generally allowed to become part of the communication infrastructure – can often be exploited to form actions to defeat the botnet. Once we know how bots are commanded, we could infiltrate the botnet so that we can inject commands ourselves.

*Storm Worm* uses a decentralized P2P network infrastructure lacking a central command-and-control instance, making it much harder to take countermeasures against it. However, peers (infected hosts) query the network for systems which are then asked for commands. We found a way to make sure that these queries are always answered by a machine we control – which basically means that we can instruct other bots to execute our orders (e.g., to remove themselves). We implemented a tool that could be used to cleanse all Storm-infected systems on the Internet<sup>3</sup>. We can even show a similar approach working for the *Waledac* botnet which uses a decentralized HTTP-driven overlay network with strong encryption, i.e. AES and RSA. We will demonstrate how the encryption can be broken using weaknesses of the botnet infrastructure and how bots can again be forced to uninstall themselves. Similar techniques are possible for *Kraken* and *Conficker*, where vulnerabilities in the bot design and rotating C&C components make it even simpler to take the botnet down. These examples show the general weakness in recent botnets' infrastructure and discuss the potentials for proactive countermeasures that are applicable to other botnets, too.

## 3 Legal Aspects

To be effective, a botnet takedown cannot be restricted to affect only systems in a certain region (country or network) but requires a global shutdown to be sustainable. However, this global impact asks urgently for political discussions about authorization and legal feasibility: In most countries it is illegal to execute code on a computer without the owner's permission. On the other hand, botnets pose a major threat to the Internet – which is considered as a critical infrastructure and important to be protected. While technically possible, we argue that proactively fighting botnets requires immediate political and international consensus.

<sup>1</sup><http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.DDoS>

<sup>2</sup>[http://en.wikipedia.org/wiki/Storm\\_botnet](http://en.wikipedia.org/wiki/Storm_botnet)

<sup>3</sup><http://www.heise-online.co.uk/news/112385>