VRIJE
UNIVERSITEIT
AMSTERDAM

VU Research Portal

Using Malware Analysis to Evaluate Botnet Resilience

Rossow, C.

2013

document version
Publisher's PDF, also known as Version of record

Link to publication in VU Research Portal

citation for published version (APA)
Rossow, C. (2013). *Using Malware Analysis to Evaluate Botnet Resilience*.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:
vuresearchportal.ub@vu.nl

Download date: 26. Sep. 2021

Summary

Botnets, networks of remotely controllable malware-infected PC systems, impose a threat to millions of users by attacks such as spam, identity theft, or denial of service. While we aware of botnets in general, there is no solid understanding of the resilience of these malicious networks. For example, it is unclear how botmasters ensure that botnets remain operational for many years. Similarly, our community does not know which botnets operate for how long and how many infected PCs are part of these botnets.

In this thesis, we aim to improve the current state of botnet resilience research. To bootstrap our botnet resilience analysis, Chapter 3 discusses how to perform malware analysis for sound scientific experimentation. We propose guidelines that enable us to analyze botnet resilience in a safe, transparent, realistic and scientifically correct manner. By surveying 36 academic publications that perform malware experimentation, we highlighted the importance of such guidelines. Most of the surveyed papers would also have benefited from similar best practices. We then used these best practices to propose a dynamic malware analysis system called Sandnet in Chapter 4. We launched Sandnet in February 2010 as a supportive tool to analyze botnet resilience in this thesis.

A complete botnet resilience analysis has to cover two sides of the botnet problem. In particular, botnet resilience is also determined by the infrastructures attackers use to create or enlarge such networks. This thesis has shown that botnets rarely spread themselves anymore, but use malware installation infrastructures to obtain new infected PCs. Thus, next to botnet resilience itself, we also have to analyze the resilience of malware installation networks. This thesis separates the botnet resilience analysis into two parts.

First, in Chapter 5, we outline the workings of 23 malware downloader families. These malware downloaders, as we have shown, persistently drop thousands of malware samples. Attackers use technical and organizational means to improve the resilience of these networks. Technically, attackers encrypt and try to hide C&C channels, often separating C&C infrastructures from malware hosting infrastructures. Next to technical measures, malware downloaders also systematically fluctuate their C&C hosting providers and C&C domain registrars. With these techniques, malware downloaders remain a persistent root cause for suc-

cessful botnet operations. Levering the necessity of malware downloaders to host their infrastructures publicly, we propose two new techniques to automatically acquire malware samples from these infrastructures.

In Chapter 6, we show that botnet architectures themselves can be highly resilient. In particular, we highlight recent trends in the development of peer-to-peer (P2P) botnets, which are explicitly designed to be highly resilient. We compare the resilience of six existing P2P botnets with historic P2P botnets. To test the botnet resilience, we prototype mitigation techniques for each of the botnets. These prototypes have helped to prepare sinkholing operations against P2P botnets such as Zeus and ZeroAccess. Overall, though, we observed trends towards highly resilient P2P botnets that cannot easily be attacked anymore. For example, botmasters use reputation schemes or deploy P2P protocols with self-healing peerlists that mitigate sinkholing attempts. In addition, P2P botnets back off to using secondary C&C backup channels if their P2P C&C component fails. We find that only minor changes in P2P protocols would render such networks highly resilient. As a consequence, we expect further P2P botnets in the near future.

Overall, we analyzed techniques that botmasters use to successfully operate their botnets for many years. Our observations imply that botnet mitigations strategies have to go far beyond disruptions of single C&C servers or C&C domains. Such one-off initiatives would only cause temporary botnet disruptions, and botmasters will use their remaining infrastructures to reactivate the botnets. However, botnet resilience is also determined by relatively easy organizational decisions by the botmasters. For example, if C&C end points are hosted at multiple sites, mitigation efforts have to involve institutions in varying time zones and legislations. Our resilience analyses assists in the complex problem of understanding the overall botnet resilience. Such resilience analyses are, for example, helpful for future botnet mitigation operations. Our discussion raises awareness of these resilient botnets, fostering research to explore alternative counter-measures against these networks.