A Cloud Forensic Readiness Model Using a Botnet as a Service

Victor R. Kebande¹, Hein. S. Venter²
ICSA Research Group
Department of Computer Science¹, ²
University of Pretoria, Lynwood Road, Private Bag X20, Hatfield 0028,
Pretoria, South Africa.
vickkebande@gmail.com¹, hventer@cs.up.co.za²

ABSTRACT

Cloud forensics has become an inexorable and a transformative discipline in the modern world. The need to share a pool of resources and to extract digital evidence from the same distributed resources to be presented in a court of law, has become a subject of focus. Forensic readiness is a pro-active process that entails digital preparedness that an organisation uses to gather, store and handle incident responsive data with the aim of reducing post-event response by digital forensics investigators. Forensic readiness in the cloud can be achieved by implementing a botnet with non-malicious code as opposed to malicious code. The botnet still infects instances of virtual computers within the cloud, however, with good intentions as opposed to bad intentions. The botnet is, effectively, implemented as a service that harvests digital information that can be preserved as admissible and submissive potential digital evidence. In this paper, the authors’ problem is that there are no techniques that exist for gathering information in the cloud for digital forensic readiness purposes as described in international standard for digital forensic investigations (ISO/IEC 27043). The authors proposed a model that allows digital forensic readiness to be achieved by implementing a Botnet as a service (BaaS) in a cloud environment.

KEYWORDS

Digital, forensics, readiness, evidence, botnet-as a service, cloud, model.

1. INTRODUCTION

Modern computer network infrastructures are being built on cloud infrastructures. Cloud computing enables users to have unprecedented ability in regard to how their data is being handled due to its vast amount of resources. Due to this, the cloud has faced many illegitimate users who have exploited these resources leading to a number of indecipherable issues. Digital investigations in the cloud environment have also faced many forensic challenges due to technological changes, lack of proper policies and procedures on cloud governance and increased crime ware syndicates.

Discounting the above, as computing is going to the cloud and virtualization is becoming the daily norm, there is no flexible forensic readiness model for the cloud that can support future technologies and the escalating types of security incidents. Nevertheless, a majority of consumers in the cloud environment operate on scalable and flexible platforms, and adversaries take this to their advantage to launch attacks.

Owing to this nefarious use of the cloud platform, the authors introduce a mitigation strategy for the above challenge. The authors propose a concept of using a botnet as a service (BaaS). Although originally considered a security threat, the authors are proposing a method through which a botnet can be used at
the application level as a technique for gathering information in the cloud for digital forensic readiness purposes.

The implementation of the authors’ study is motivated by the fact that botnets are widely used for monitoring and capturing users’ information illegally [11]. Equally, the motivation comes from virtual honeypot information systems resources’ ability to manage intrusion detection by trapping, identifying flaws and warnings of the possibility of security intruders by providing security awareness [12].

The rest of this article is structured as follows: Section 2 discusses the background of this study. Thereafter, section 3 discusses the proposed model for achieving cloud forensic readiness. After this, the authors explore section 4 that gives the critical evaluation of the proposed model. Next, section 5 gives the work related to the authors’ study with section 6 closing with conclusion and future work.

The next section discusses the background.

2. BACKGROUND

This section provides an overview of cloud computing, digital forensics, digital forensic readiness, botnets, legal perspective on information privacy and ISO/IEC 27043.

The authors present a brief overview of cloud computing because the entire model as presented in this paper is based on the cloud environment. This model also employs a digital forensic (DF) principle; digital forensic readiness (DFR). Finally, we review the classes of digital forensic investigation processes with DFR as per ISO/IEC 27043 draft international standard to see where DFR fits in the standard. Further, the authors present botnets because they are known to capture information, although not legally.

2.1 Cloud Computing

Cloud computing has become one of the fastest emerging fields in the field of distributed computing in the last few years, it is scaled and works in a virtualized environment. The National Institute of Standards Technology (NIST), defines cloud computing as a model for ubiquitous and an on-demand network that is configurable to a shared pool of resources [3]. Cloud forensics as a discipline is basically the application of computer forensic processes in the cloud environment.

Ruan, Kechadi, and Crosbie [6] define cloud forensics as “a cross discipline of cloud computing and digital forensics.” Cloud computing allows resources to be shared at different levels, this can happen through a virtualized environment where control is managed from data centres, this allows many virtual instances to be operated in this environment.

The cloud environment operates on three service models and four deployment models. The service models are Infrastructure as a service (IaaS) that offers storage services, Platform as a service (PaaS) that gives support in building applications and Software as a service (SaaS) that acts as a service provider. IaaS supports data storage services. Cloud computing can be deployed as private cloud, public cloud, community cloud and hybrid cloud [3].

2.2 Digital Forensic Science

Digital forensics is a relatively new area. It is a scientific process of investigation. NIST defines digital forensics as a legal process that involves identifying, collection, examination, extraction, analysing and reporting information as evidence [1]. This legal process takes place while preserving the integrity of the information extracted electronically from a computing device [1].
During the first Digital Forensic Reasearch Workshop (DFRWS) in 2001, Palmer [17] described digital forensic as “the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction events”. Palmer’s view highlighted the scientific digital forensic process of investigation.

2.3 Digital Forensic Readiness

Digital Forensic Readiness (DFR) is a proactive measure that organisations need to enforce, so that when there is a reactive measure or a set-up for forensic investigation, the organisation has the ability to comply to Digital Forensic Investigations (DFI) with sufficient forensic preparedness.

Rowlingson [4] describes forensic readiness as an objective to maximise the environment’s capability of collecting digital forensic information whilst minimising the cost of the forensic investigation during an incident response. Tan [26] identified the following factors that affect digital forensic readiness; evidence handling, forensic acquisition, logging methods and intrusion detection methods.

2.4. Botnets

Bot is a term derived from “ro-bot”. Bot, in this context, is a set of commands or scripts designed to connect to some client and execute a series of commands. The commands are used to create an alliance of so-called ‘zombies’, known as a botnet. They work under the command of a botmaster.

Leder [21], describes a botnet as an alliance of interconnected computers infected with malicious software. When these computers have been infected they become zombies. Generally, they are considered illegal because intentionally they are injected in stealth mode to perform pre-defined functions. These functions range from theft of personal information, spamming to Distributed Denial of service (DDos) [11].

The botmaster operates the bot clients from a remote location where he commands a chain of zombie computers. Botnets have always been attributed to crime ware syndicates and they are considered as the dark side of computing. They perform these actions through searching for a vulnerable computer for initial infection, after this the bot is distributed to clients (target), and then finally they can connect to the botmaster for more instructions as shown in Figure 1.

The genesis of botnets began when Jeff Fisher created the Eggdrop in 1993 which ran from an Internet Relay Chat (IRC) to a variety of distributed computers [13], [14]. Eggdrop was a bot which had interfaces for C modules and TCL scripts that enhanced functionality of the bot [24]. Oikarinen [14] describes that “in a typical IRC set-up an IRC client program (from a botmaster) connects to an IRC server in an IRC network (robot network/botnet) and the default TCP service port for IRC is 6667 ”. The IRC protocol offers the possibility of other channels to communicate faster because malicious codes respond faster.

![Figure 1. A botnet over Networks. Source (New threat landscape White Paper, Cisco)](image-url)
Botnet Operation

The botmaster in Figure 1 infects a bot client in the initial infection phase over the public internet, the bot client communicates back to the master who then uses the Command and Control (C&C) as an update centre to avoid surveillance. Through the public internet another bot client is infected at the consumer Broadband provider that is commanded to infect other clients in the same provider. Then the Enterprise network gets one bot client infected on the LAN segment and Wireless LAN that infects all clients that communicate to the botmaster through the C&C server Data centre server. Through the public internet, consumer Broadband Provider and the Enterprise Network a network of zombie computers is formed that is controlled by the botmaster.

2.5 Legal Perspective on Admissibility of Digital Evidence

The legal requirements on admissibility of evidence vary across different jurisdictions in the whole world. The following acts describe the rules of admissibility of digital evidence in USA, UK and South Africa at large. The Electronic Communications Privacy Act (ECPA) Act of 1986 of the USA [33], The UK’s Association of Chief Police Officers (ACPO) [34] good practice guide for digital evidence, The Electronic Communication and Transaction (ECT) act [28] of South Africa, Protection of Personal Information (POPI) act of South Africa [29], Regulation of Communications and Provision of Communication Act (RICA) of South Africa [32] and Stored Communications Act (SCA) [35] of USA. The ECPA on digital evidence highlights that intercepted electronic evidence and electronic communication records must be collected to facilitate prosecution in the judicial system. However, the SCA [35], portrays intentionally accessing an electronic facility without authority as unlawful. The ACPO good practice for digital evidence highlights that “digital evidence has to be subjected to the rules and laws that apply to documentary evidence”. The ECT regulates users’ electronic communication and transactions, POPI gives effect to the constitutional right to privacy by safeguarding personal information. RICA regulates the interception, monitoring of communication. However, section 15 of ECT act states that “in legal proceedings, rules of evidence must not be applied to deny admissibility of a data message.” Chapter 4 of POPI act provides an exemption to interfere with privacy of information if the matters are for national security prevention.

However, the acts [28],[29],[32],[33],[34] [35] highlight that the above can only be disregarded if this is for law enforcement purposes and if the parties that are being monitored are aware. The South African Gazette [30] further, describes that exemption is made to interfere with privacy of data subject to interests of national security, prevention, detection and prosecution of offences. Furthermore, Act [32] extends the conditions to historical, statistical or research activity.

2.6 ISO/IEC 27043

In this section, the authors deal with how digital forensic readiness fits in ISO/IEC 27043. However, in this paper forensic readiness is presented as a process from ISO/IEC 27043.

The process that follows analyses how potential digital evidence can be gathered using the readiness process as explained in ISO/IEC 27043 [25] as shown in figure 2. ISO/IEC 27403 [25] is in its final stages of becoming an international standard for digital forensic investigation at the time of writing this paper.
Figure 2 represents the overview of the digital investigation processes as highlighted in ISO/IEC 27043 with the readiness processes that deal with pre-incident investigative processes [25]. The readiness processes as described in ISO/IEC 27043 include: scenario definition, potential evidence identification, planning incident collection, planning incident analysis, detection, storage of potential evidence and implementation of assessment results [25].

The initialisation process deals with the initial commencement of digital investigation. It consists of the following: incident detection, first response, planning and preparation [25]. The acquisitive process involves the physical investigation of a case. At this stage potential digital evidence is identified. It includes:

- potential digital evidence identification, acquisition, storage and transportation.
- The investigative process deals with uncovering of potential digital evidence. It includes the following: potential digital evidence examination, digital evidence interpretation, reporting, presentation and investigative closure.

Finally, the concurrent processes are processes that work along other processes. All sub-processes in the concurrent processes run parallel with other classes. The process includes: Obtaining authorisation, documentation, managing information flow, preserving chain of custody, preserving digital evidence [25].

The next section discusses about the proposed model for botnet as a service.

3. MODEL FOR USING A BOTNET AS A SERVICE

This section proposes a novel model as a contribution to cloud forensic readiness. However, the authors first present an overview of the high level model of the proposed model in figure 3 before a more detailed model is presented in figure 4. Predominantly, the authors’ proposed model is based on actively monitoring and gathering information over the network in a cloud environment.

The authors propose the novel concept that a botnet can be used as a service in the cloud environment by harvesting digital information in a non-malicious way and preserving it digitally in preparation for digital forensic readiness purposes. This can only be achieved by deploying the botnet to “infect” the instances of virtual computers in any cloud environment in a non-malicious way in order to harvest digital information.

The next two sub-sections discuss the high-level model and the detailed model respectively.
3.1 High-Level Model

Figure 3 represents the high level view of the proposed model.

![Overview of the model]

The cloud service providers (CSPs) in figure 3 offer cloud clients with virtual services. The non-malicious botnet “infects” the virtual instances of computers being accessed by the cloud clients. Digital information is then collected and preserved forensically so as to be ready for a digital forensic investigation (DFI). A more detailed discussion of the model follows in the next section.

3.2 The Detailed Model

Logically, the detailed cloud forensic readiness model shown in figure 4 is organised in the following structure. It is divided into two distinct layers i.e. the back-end layer and the front-end layer as discussed in the next subsections. The back-end layer consists of infrastructure as a service (IaaS) and Platform as a service (PaaS). The front-end layer consists of the application environment where the botnet as a service (BaaS) is implemented inside SaaS.

![Cloud forensic readiness model with BaaS]
3.2 How the Model Works

The cloud service providers (CSPs) in figure 4 at the front-end layer offer the cloud clients virtual services. These services enable the cloud clients to get access to virtual instances in the cloud environment. Within the front-end layer, the BaaS consists of non-malicious botnet infection, digital information harvesting, digital preservation, forensic planning and forensic preparation.

The non-malicious botnet “infects” the virtual instances of computers being accessed by cloud clients in the pro-active DFR process where a botnet is used as a service. This is shown by the down-arrow in the top right of figure 4. Note that “infection” normally has a negative connotation in the field of botnets. In the context of this paper, however, the concept of “infection” is positive, simply meaning that the botnet is installed transparently on a virtual instance within the cloud, rendering the need to modify the cloud architecture for digital forensic readiness purposes, unnecessary. This is advantageous since there is no need for a costly redevelopment of new cloud architecture in order to incorporate digital forensic readiness within any cloud.

After infection, the botnet collects digital information that can be used as potential digital evidence in a digital forensic investigation. The harvested information is digitally preserved in the databases at the back-end layer offered by IaaS. The digitally preserved information is used for digital forensic readiness purposes. The PaaS service model in the back-end layer provides a podium through which the application BaaS and SaaS are deployed. Infrastructure as a service (IaaS) at the back-end layer consists of storage, network and servers.

The reactive process in figure 4 represents the process undertaken during Digital Forensic Investigation (DFI) if an incident is detected. The process illustrates that on incident detection, forensic readiness can be achieved from digitally preserved information through forensic planning and forensic preparation.

The next section presents the critical evaluation of the model.

4. CRITICAL EVALUATION OF THE MODEL

In this section, the authors discuss the possible applicability of the cloud forensic readiness model using a BaaS and how it will be compliant in the cloud environment towards attaining forensic readiness.

The cloud forensic readiness model using a BaaS concept is a new contribution that significantly focuses on forensic planning and preparation for a DFI process.

According to the authors’ view, computer forensic processes in the cloud environment are increasing exponentially as a discipline due to increased usage of computing devices in resolving electronic crime-related issues. As suggested by the problem, hostile botnets, as shown in figure 1, as opposed to the BaaS as implemented in this paper, can capture information illegally when the code involved is malicious and when it is not used for forensic purposes.

Capturing information for forensic readiness purposes without consent using a malicious code (bots) deployed in stealth mode might be offensive and might have legal implications when the logs captured are not for law enforcement purposes. Whilst there exists implications, different jurisdictions laws [28], [29], [32], [33],[34] [35] have a provision if the information is for law enforcement purposes or if it is to be used to facilitate prosecution in a judicial system.

The botnet discussed in this paper, is non-malicious and it operates in the cloud environment taking the legal acts [28], [29], [32],[33],[34] [35] into account, which shows when to gather and when not to gather digital information for law enforcement purposes.
The model described in figure 4 shows that by using a botnet as a service, sufficient forensic preparedness can be achieved from the digitally preserved information. According to the authors’ opinion, if an incident is detected, the organisation’s hosting services at the cloud, individuals and forensic investigators should refer to organisational policies and procedures on potential digital evidence handling before setting up a DFI process.

From the authors’ interpretation, implementing a botnet as a service at the cloud environment can enable a high level of impact on digital evidence gathering towards forensic readiness within the cloud. From this assertion the digital forensic investigators are able to extract proper digital artifacts that can be used in a legal set up as admissible and submissive evidence. This further simplifies the process of data analysis as it would become easy to pick specific and reliable artifacts from the digital-forensically-ready data collected and preserved by the BaaS.

The next section discusses related work.

5. RELATED WORK

This section presents a discussion on related work on cloud forensic readiness and botnets. From the authors’ study, the botnet has not been used as a service for forensic readiness purposes at the cloud at the time of writing this paper. Besides that, there are still no models that have been proposed for gathering information in the cloud for digital forensic readiness purposes. However a number of digital forensic research papers have culminated in some research focusing on the digital forensic domain.

A research paper by Kent, Chevalier, Grance, and Dang [19] proposed a framework (NIST SP800-86) which highlighted a guide to forensic techniques into organisational incidents. The framework has organisation forensic guidelines and methods for incident investigation and response. The methodologies employed here shows how organisational policies are used in integrating digital forensic processes in incident detection.

A research paper by Van Staden and Venter [8], showed an implementation of digital forensic readiness on the cloud using a learning management system (LMS). LMS was used as a software as a service (SaaS) cloud computing model by hosting it outside the organisation. In this study the cloud allows the collection of live digital forensic data while users access services.

Work by Popovsky and Boucher [7] presents forensic readiness in the cloud (FRC) as “a call on technological and organization strategies to address risks that threaten organizational information”. Further, they described organisation Network Forensic Readiness (NFR) as a method for supporting the collection of digital evidence from networks using checklists, procedures and tools. Their study gives a methodology of operationalising NFR and forensic readiness in the cloud by providing a conceptual approach to proactive evidence collection. Further their study identifies the process and phases effectively employed in the cloud.

A theoretical framework for Organisational NFR by Endicott-Popovsky, Frincke and Taylor [22] shows that the current digital forensics approaches are not scalable enough to handle the growing number of cybercrime cases. However, the framework they presented provided a basis for developing a forensically ready organisational network.

The work by Gummadi, Balakrishnan, Maniatis, and Ratnasamy [23] on improving service availability in the face of botnet attacks presented a Not-A-Bot (NAB) approach by implementing a component called attester that acted as a system for mitigating network attacks by using automatically obtained evidence of human activity.

By acknowledging the previous work which has offered a deep understanding, the authors’ have intuited that this has offered the needed confidence in developing the cloud forensic readiness model using a botnet as a service.
The next section provides a conclusion and future work.

6. CONCLUSION AND FUTURE WORK

This paper described a technique for gathering digital information that may be used for forensic readiness purposes at the cloud environment using a BaaS.

The contributions made by the authors on the cloud forensic readiness model shows that they are able to transcend botnets from illegal information capturing, to legal monitoring and information capturing applications. These applications may be used to gather admissible potential digital evidence that may be used in a court of law during a DFI process.

The cloud forensic readiness model may also be used by organisations to prepare themselves forensically for the process of digital forensic investigations. The authors have also discussed how cloud computing is facing multi-faceted challenges on the part of illegitimate users and the impact of there not being an existing cloud forensic readiness model for gathering information.

The authors plan to expand the model to be standardised and to support future technologies in enabling more proactive processes at the cloud.

7. REFERENCES


Forensics Research Workshop (DFRWS)”. Utica, New York.


