BREDOLAB: Shopping in the Cybercrime Underworld

Daan de Graaf[1], Ahmed F. Shosha[2], and Pavel Gladyshev[2]

[1] National High Tech Crime Unit, Netherlands' Police Agency, The Netherlands
Daan.De.Graaf@nhtcu.nl
[2] University College Dublin, Ireland
Ahmed.Shosha@ucdconnect.ie, Pavel.Gladyshev@ucd.ie

Abstract. A recent emerging trend in the underground economy is malware dissemination as a service. Complex botnet infrastructures are developed to spread and install malware for third-party customers. In this research work, a botnet forensic investigation model is proposed to investigate and analyze large-scale botnets. The proposed investigation model is applied to a real-world law-enforcement investigation case that involves investigation of a large-scale malware dissemination botnet called BredoLab. The results of the forensic investigation show the effectiveness of the proposed model in assisting law-enforcement to conduct a successful forensic analysis of BredoLab botnet and its related resources.

Keywords: BredoLab, Botnets, Law-Enforcement Investigations, Malware Forensics, Forensic Investigation Models.

1 Introduction

Over the past few years, cybercrimes on the Internet have gradually transformed to profit-based crimes. A complex underground economy has emerged with complex divisions to manage various cybercriminal activities, e.g. financial crimes on the Internet, identity theft, attacking online services and dissemination of suspicious services, i.e. spam and phishing distribution. These illegal activities are supported with a solid networking infrastructure, such as bulletproof hosting through Virtual Private Network (VPN), to provide the cybercriminals a quality control and management for their malicious activities.

To manage the underground economy, well-defined organizations are established to rule the economic and technical aspects of the malicious service delivery through professional roles, such as, carders, scammers, financial cashiers, malware authors, spammers, spoof-website designers, money launders and botherders [1]. These organizations provide fee-based services on behalf of third-party customers to commit the customers' required criminal activities. In essence, these illegal services are mostly advertised on communication forums that are denoted as "Underground Forums" [2]. Such forums provide a secure communication channel between malicious services' providers and the services' customers through providing an infrastructure, e.g. communication-based dashboard to manage requested services and

M. Rogers and K.C. Seigfried-Spellar (Eds.): ICDF2C 2012, LNICST 114, pp. 302–313, 2013.

to advertise newly developed malicious services. To commit previously aforementioned illegal acts, cybercriminals are usually assisted with botnets. A botnet is a collection of infected computers connected to the Internet and controlled by a botnet commander, usually denoted as bot-herder, and utilized to commit wide variety of cybercrimes, such as denial of Internet-based services [3].

As a bot controller, the bot-herder possesses the ability to download, update and execute malicious binaries on infected systems [3-4]. Fundamentally, he/she utilizes this functionality to update installed bots on the victim's computer with a newly developed malware sample, to allow execution of new binaries determined to commit different malicious activities. This process is denoted as "malware downloader" and describes the ability of a certain botnet to install other malware samples for different purposes. Since malware downloading is an important resource in botnets, bot-herders may offer the resource as a fee-based service to other cybercriminals. As a result, a cybercriminal use such paid service to commit a specific crime, i.e. malware downloader for banking fraud. A complex example of a botnet that was specifically used to offer the bots resources for spam activities and bank fraud is BredoLab.

Researchers and anti-virus companies first saw the BredoLab botnet in 2009. It is a complex downloading platform designed to facilitate malware spread on a massive, large-scale rate and used as fee-based service for installing malware to third-parties customers who could use infected machines (bots) to commit various cybercriminal activities.

From July 2010 till October 2010 the National High Tech Crime Unit of the Netherlands' Police Agency (NHTCU) did an investigation to a specific BredoLab botnet. The investigation has estimated that initial size of the botnet is, at least, three million infected machines. Following the investigation, NHTCU discovered that the networking infrastructure of this BredoLab botnet was running at a large-scale hosting provider in the Netherlands. Thus, on October 25, 2010 the NHTCU successfully took over the control of a BredoLab botnet and got access to servers that were directly connected to the network.

Because of the large-scale nature of BredoLab, traditional forensics investigation models were not sufficient to investigate and analyze the bot's resources. A forensics investigation model to investigate large-scale botnets was required.

In this research paper, a large-scale botnet's forensic investigation approach is proposed to analyze the botnet infrastructure. The proposed approach is applied in a real-world law-enforcement investigation of a BredoLab botnet. Finally, an analysis on BredoLab's resources is conducted to provide practical insights on the investigation of the malware selling botnets.

Paper Organization. Section two presents the proposed approach to forensically investigate large-scale botnets. Section three presents a case study of a law-enforcement investigation on the BredoLab botnet. Section four presents a research on the botnet data. Finally, section five concludes the paper.

2 An Approach to Analyze Large-Scale Centralized Botnets

Various forensic analysis and investigation approaches are proposed to analyze botnets, and investigate the underground economies. Most of currently proposed approaches, however, are limited to the analysis of malware samples found in acquired botnets, or focus on analysis of the communication channels to/from the cybercriminals. A comprehensive forensic investigation model to investigate large-scale infrastructure of botnets, however, is still missing.

In this section, we describe the infrastructure model commonly employed in centralized large-scale botnets, and propose a forensic investigation model to analyze the infrastructure. Note that, illustrated infrastructure is based on a real-world investigation case of a BredoLab botnet.

Generally, larges-scale botnets are comprised of several working components, each of which is designated to one or more predefined functionalities. For example, main modules in a large-scale botnet such as BredoLab encompass C&C (Command and Control) servers, databases servers, bot-herder administration panels and customer control panels. The understanding of each module and the interrelationship between instances of each module is crucial for forensic investigation of the botnet's activities and is required for the proper disassembly of the botnet threats.

From a forensic investigation point of view, successful investigative model has to consider the modular nature of a botnet under investigation. Otherwise, investigation of interactions between the botnet's modules may conclude to insufficient results. As a result, the proposed botnet investigation model is decomposed into a set of subcomponents; each component is designated to investigate one or more specific module in the botnet's infrastructure. Note that, proposed model can be used when the botnet is identified and its servers are located.

In the proposed approach, three main investigation stages are defined to analyze the botnet's resources. The first stage includes forensic acquisition of the botnet's resources, i.e. forensic imaging of botnet hosting servers, etc. The second stage includes forensic evidence and data extraction of acquired forensic images and communication networks. Finally, the third stage includes analysis of malware samples found in botnet resources. A detailed analysis of the botnet backend and the re-building of the botnet infrastructure in a controlled environment to reconstruct a full view of the botnet resources is, also, proposed. This allows precise understating of the botnet threats.

As shown in figure 1, wiretap and net-flow components are designed to allow the acquisition of sampled network data from the botnet's communication. The analysis of botnet network data is essential to identify how the botnet modules are interacting and communicating with each other, which facilitates forensic investigation of interrelated modules. Forensic acquisition of the botnet's infrastructure, when the botnet is taken down, is accomplished using the forensic images component. This process includes forensic analysis of the images to extract forensic evidences and information to continue investigation, such as, botnet administrations and customers panels' related information, information about C&C servers, bots' database and downloader malware module.

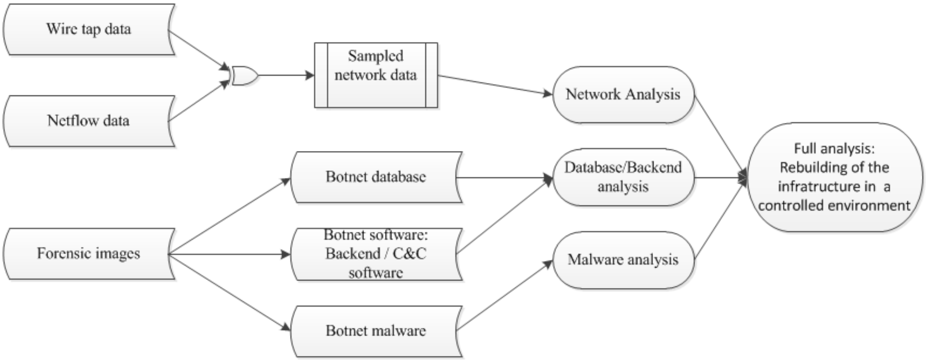

Wire tap data
Netflow data
Sampled network data
Network Analysis
Botnet database
Database/Backend analysis
Full analysis: Rebuilding of the infratructure in a controlled environment
Forensic images
Botnet software: Backend / C&C software
Malware analysis
Botnet malware

Fig. 1. Large-Scale Botnet Forensic Investigation Model

Based on extracted evidence from acquired forensic images a detailed behavior analysis of botnets resources, such as, malware samples behavior is required.

Determining the behavior of malware samples extracted from the botnet downloader database is accomplished through a dynamic malware analysis component. Practically, malware analysis component is a preconfigured controlled dynamic malware analysis environment [5-6] that is used to determine the behavior of malware samples used in botnets. The behavior analysis of malware samples includes identification of actions and activities invoked by the sample in infected bots, security assessment of used exploitation payload and spreading mechanism used by malware sample, and method used to hide their presence in infected bots, and techniques used to ensure persistence. Finally, to ensure that valid forensic investigation conclusions are resulted, a full forensic analysis based on re-building the botnet's resources in a controlled environment is developed. The workflow of service provided by the botnet is traced in the managed environment and are matched to conclusions resulting from the investigation to ensure validity and integrity of the conclusions.

3 Case Study: BredoLab Botnet Investigation

The first BredoLab exploits where seen in May 2009 by anti-virus companies [7-8]. The initial analysis of BredoLab reveals a complex threat posed by the botnet as results of employing different sophisticated attack vectors implemented in various malware samples. Particularly, BredoLab can install a wide range of malware families, e.g. password stealers, rootkits, backdoors, banking trojans, fake anti-virus software and spam malware [8].

In this section, a case study is provided about law-enforcement investigation of a BredoLab botnet. The case study includes procedures used to disassemble the botnet's threat and detailed forensic analysis on data extracted from the botnet for forensic investigation purposes based on the previously presented forensic investigation model.

3.1 NHTCU Investigation

Leaseweb, a large hosting provider located in the Netherlands, started in 2010 with the Community Outreach Project [9]. This project offers free servers and bandwidth in support to the organizations that monitor, identify and combat the sources of spam and crime on the Internet. One of the participants in the project is Abuse.ch, a non-profit organization that analyses different threats on the Internet, such as, Zeus and SpyEye [10]. Through Abuse.ch, Leaseweb was informed about a possible large-scale botnet infrastructure that intersects with their network, since Zeus malware was one of the malware samples spread by BredoLab. Normally, the regular security process of Leaseweb encompasses the immediate interaction with the servers' disseminating malware and blocking all communication channels. Instead, due to the large-scale nature of discovered botnet, Leaseweb decided to involve the National High Tech Crime Unit of the Netherlands' Police Agency (NHTCU) for further tracking of the botnet's resources. Initially, NHTCU acquired the net-flow data from the servers at Leaseweb for further network forensic analysis and investigation. Furthermore, the NHTCU placed additional wiretaps on eleven servers at Leaseweb to control the network communication involving BredoLab bots with a total amount of acquired wiretap data equals to four terabyte.

During the investigation, different malicious servers were fully identified as followed:

- A malware management server that used to hack and distribute newly developed malware samples.
- FTP grabber server used to authenticate credentials used by malware and distributed by the BredoLab botnet.
- A VPN server used for different purposes, such as, management of other servers, hacks to new proxy servers, Denial of Services (DDoS) attacks and communication with partners and personal customers.
- A database server used to store information about infected bots and malware samples distributed by the BredoLab botnet.
- A Jabber server to communicate with various malware samples i.e. commands to Zeus malware.
- Various C&C servers to control the bots.

In most adversarial legal systems, to establish a valid accusation, forensic analysts are required to prove that accused person has a knowledge and control - or what so-called "*mens rea*"[1]- based on evidence and artifacts extracted from case under investigation. In the BredoLab investigation, forensic evidence that establish the knowledge and control of the criminal activity using BredoLab is obtained from the wiretaps of the database server and the VPN server. Various forensic evidence and supporting artifacts, such as, evidence to identify the botnet owners and customers, traces of

[1] *Mens rea* is Latin for "guilty mind". In criminal law, it is viewed as one of the necessary elements of a crime.

malware distribution for different purposes, evidence about launching DDoS attacks and hacking into various websites, are successfully collected during investigation based on wiretapping investigated servers and the analyses of the network traffic to/from identified servers.

3.2 BredoLab Botnet Termination Procedures

On October 25, 2010, BredoLab infrastructure was terminated and taken offline. The NHTCU successfully connected to the backend panel located on one of the C&C servers through exploiting a cookie extracted from wiretap artifacts of the VPN server. After controlling the backend panel, the NHTCU terminated all malicious activity, i.e. active malware distributions tasks. Intuitively, this action will only contribute to limit infecting new computers; however, to disrupt the ability of BredoLab, further actions are required to disinfect previously infected bots. Thus, NHTCU developed a program that is uploaded to all bots in the network and launched a standard browser on the victims' computers to allow infected users to read a press-warning message. This warning message has been viewed over 300,000 times.

BredoLab botnet was let active for a few days in order to reach as much victims as possible. After that, the network connections to all servers were terminated. Suspect servers where confiscated for further forensic investigation by the NHTCU. Additionally, suspect IP's, domain names and malware found during the investigation were distributed to the professional security communities.

During the investigation, the bot-herder was identified as results of wiretap data analysis of the VPN server, since the suspect bot-herder used to use the VPN server for other non-criminal activities, such as: accessing his personal Facebook account, e-mail accounts, and his WebMoney accounts. The NHTCU made an international arrest warrant, through which the suspect got arrested a few days later at the airport of Yerevan, Armenia. The suspect got convicted in Armenia for four years, based on the information provided by the NHTCU.

4 Analysis of BredoLab's Resources and Infrastructure

BredoLab resources' analysis and forensic investigation is accomplished using the forensic investigation model described earlier. Thus, in this section, the analysis's results of the different BredoLab resources, such as, the network data acquired from the communication infrastructure and the layout of the network used in a BredoLab botnet is presented. To reconstruct the network layout, a sampling of the wiretap data was captured and interrelation between captured network packets was reconstructed using a custom-built wiretap analysis tools developed by the NHTCU [11]. Each sampled data packet consists of: source and destination IP addresses, used networking protocol, source and destination port numbers. The sampled packets are correlated together to determine the communication network layout used to maintain BredoLab services. As shown in figure 2, when sampled network data are correlated together, the BredoLab network infrastructure layout can be identified.

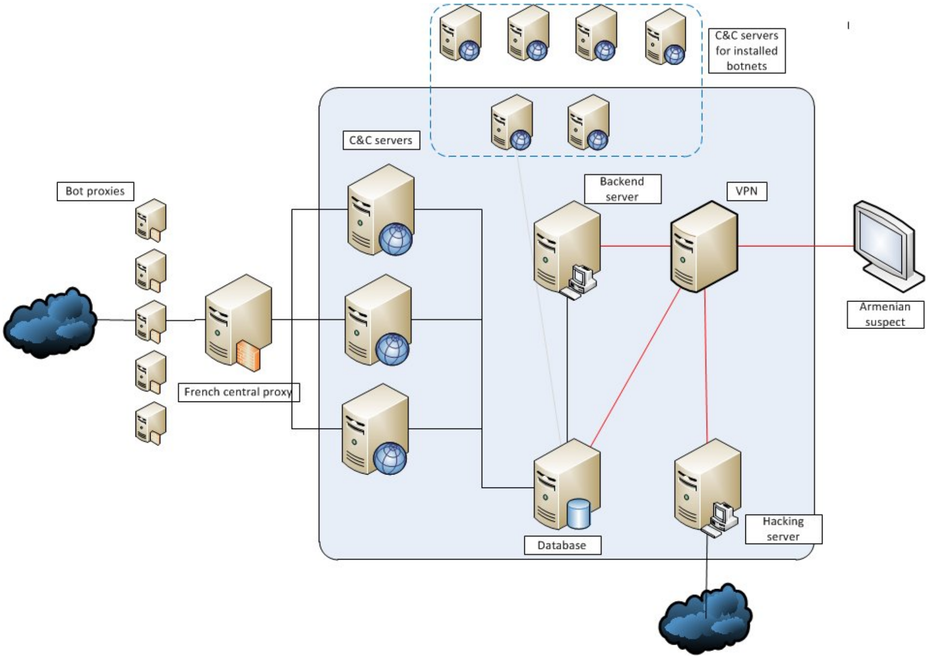


Fig. 2. The BredoLab Infrastructure Layout

The BredoLab infrastructure consisted of: a database server, a central proxy server, several proxies installed on bots, a backend server, a personal hacking server, a VPN server and several C&C servers. The blue square contains the servers that were wiretapped at Leaseweb. The red lines are traffic generated by the administrator from the VPN server. The data created by the previously mentioned wiretap analysis tools showed that all the traffic from the three C&C servers consists of: HTTP traffic going to a main proxy server in France, and plain MySQL code going to one central database server. The database server was used, as well, by one of the installed malware as FTPgrabber malware. Forensic investigation also showed that the VPN server has several encrypted connections to a suspect IP addresses in Armenia and was used to manage other servers.

4.1 Wiretap Data Analysis

Based on determined BredoLab's communication network infrastructure layout, three main C&C servers were identified as active servers. Forensic investigation of these servers' wiretaps revealed communication traffic to a domain called "worldhostdns.com". Further investigations resulted in specified domain is resolve to an IP address of a C&C server through a proxy server that is located in France. Analysis of wiretap data has, additionally, revealed that communication between infected bots and suspect domain is accomplished through various HTTP requests to a web page named "`controller.php`".

```
192.168.1.101 - - [06/Sep/2011:17:17:16 +0200]
"GEThttp://worldhostdns.com/new/controller.php?actio
n=bot&entity_list=1272705710,1272796684,127875990,12
81608998,1283317892&first=0&rnd=981633&uid=1&guid=29
47510467   HTTP/1.0" - - "-" "-"
```

```
192.168.1.101 -- [06/Sep/2011:21:29:32 +0200] " GET
http://worldhostdns.com/new/controller.php?action=re
port&uid=1&guid=3985971469&rnd=123&entity=1259351490
:unique_start;1259970379:unique_start;1271368047:uni
que_start;1278753990:unique_start;1283419228:unique_
start;1283685805:unique_start    HTTP/1.0" - - "-"
"-"
```

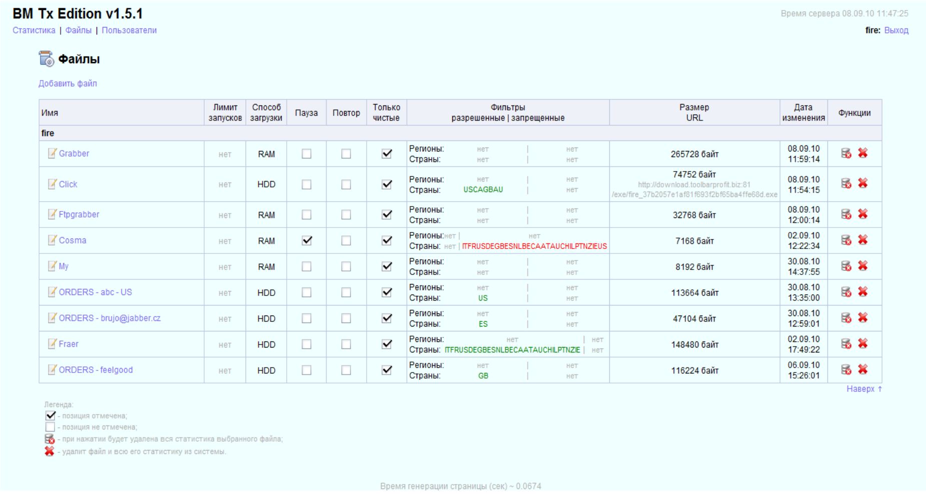
Fig. 3. A sample Communication Packet to a C&C Server

In essence, the communication to the C&C server through "controller.php", as shown in figure 3, is defined in the following steps [8]:

- The infected bots connect to the suspect C&C server to update its infection status and to download newly developed malware through a GET request. Whereas, the C&C server could identify if connected host is an authorized bot, if the "Action" parameter in GET request is set "Bot".
- The C&C server responds to communicate bots with a response message containing malware samples needed to install.
- The bot replies back if a malware installation task was handled successfully or not through specific GET request in which "Action" parameter is set to "Report". Additionally, infected bots alert the server with the task starting timestamp via "Unique_Start" parameter.
- Finally, the C&C server reports back with an acknowledgement message.

4.2 Backend Panels Forensic Analysis

Forensic investigation of BredoLab's network has identified two different backend panels; one is located on a separate backend server, and the other is located on the database server. The backend panel is called "BM Tx Edition v1.5.1." such that, BM is abbreviation for **B**redoLab **M**anager. The Tx and the version numbering is a reference to installed BredoLab's software version. Identified panels are developed in PHP and are used to manage different tasks, like: activate malware orders, start/stop of malware tasks, and manage installing and cleaning of malware. Besides management activities, the backend panels also maintain statistics about installed malware and infected bots. Below is a snapshot sample for information presented in a backend panel.



BM Tx Edition v1.5.1

Статистика | Файлы | Пользователи

Время сервера 08.09.10 11:47:25

fire: Выход

Файлы

Добавить файл

Имя	Лимит запусков	Способ загрузки	Пауза	Повтор	Только чистые	Фильтры разрешенные | запрещенные	Размер URL	Дата изменения	Функции
fire									
Grabber	нет	RAM	□	□	☑	Регионы: нет | нет Страны: нет | нет	265728 байт	08.09.10 11:59:14	⛁ ✖
Click	нет	HDD	□	□	☑	Регионы: нет | нет Страны: USCAGBAU | нет	74752 байт http://download.toolbarprofit.biz:81 /exe/fire_37b2057e1af81f693f2bf65ba4ffe68d.exe	08.09.10 11:54:15	⛁ ✖
Ftpgrabber	нет	RAM	□	□	☑	Регионы: нет | нет Страны: нет | нет	32768 байт	08.09.10 12:00:14	⛁ ✖
Cosma	нет	RAM	☑	□	☑	Регионы:нет | нет Страны: нет | ITFRUSDEGBESNLBECAATAUCHILPTNZIEUS	7168 байт	02.09.10 12:22:34	⛁ ✖
My	нет	RAM	□	□	☑	Регионы: нет | нет Страны: нет | нет	8192 байт	30.08.10 14:37:55	⛁ ✖
ORDERS - abc - US	нет	HDD	□	□	☑	Регионы: нет | нет Страны: US | нет	113664 байт	30.08.10 13:35:00	⛁ ✖
ORDERS - brujo@jabber.cz	нет	HDD	□	□	☑	Регионы: нет | нет Страны: ES | нет	47104 байт	30.08.10 12:59:01	⛁ ✖
Fraer	нет	HDD	□	□	☑	Регионы: нет | нет Страны: ITFRUSDEGBESNLBECAATAUCHILPTNZIE | нет	148480 байт	02.09.10 17:49:22	⛁ ✖
ORDERS - feelgood	нет	HDD	□	□	☑	Регионы: нет | нет Страны: GB | нет	116224 байт	06.09.10 15:26:01	⛁ ✖

Наверх ↑

Легенда:

☑ - позиция отмечена;

□ - позиция не отмечена;

⛁ - при нажатии будет удалена вся статистика выбранного файла;

✖ - удалит файл и всю его статистику из системы.

Время генерации страницы (сек) ~ 0.0674

Fig. 4. BredoLab Sample Backend Panel

An additional important panel is BredoLab's customers and partners mangement panel. Customers' panel which is resident in the database server was used to upload malware samples and to define prefered number of computers to be infected. Once a malware is uploaded through the panel, malware spread task is activated on the main backend panel and then malware is being dissemenated. Finally, the panel, as well, keeps tracks of open payments and customer related information.

4.3 BredoLab Database Analysis

During post-mortem forensic investigation of the acquired servers' forensic images, a BredoLab malware database was successfully extracted. Database forensic investigation has showed that a database named "BM" is used to store information about infected bots and different malware samples. Fundamentally, a number of essential database tables to assist BredoLab service delivery are identified as follow:

- Malware tasks: A table referencing stored information about infected bots and stored malware to manage outstanding malware infections tasks.
- Bots: A table to store the infected bots information.
- Users: A table that stores information about users and customers who are controlling the botnet.
- An administration table that is used by the backend panel and various C&C servers to assist the BredoLab administrator to control service requests, and payments from customers.

Tasks related to malware activities in the database are divided into two components; a component that is designated to malware management while the other is for statistics operations. The management component assists in 1) Upload new malware and place it directly in the database as BLOB file, 2) Set country and regional variables to the location in which malware should be deployed, 3) Pause, load or reload spreading of a malware. While the statistics component, on the other side, is used to draw malware dissemination graphs, illustrate spread rates and spread dates in the backend panel. Every bot that is infected with a certain malware task gets stored in the statistics table. And for every infection, the backend panel kept track of IP address of the infected machine, date and timestamp of infection, and country and region.

The acquired statistics table contained information about 3,283,644 infected bots with 38 different malware tasks. However, the table counts, only, unique IP addresses. Hence, total infected IP addresses were 477,282 with the 38 different malware tasks. Note that, this number does not define the actual size of the BredoLab botnet, since it is possible that bots do not have active tasks at the database acquisition time.

Additionally, the wiretap from law-enforcement investigation of a C&C server showed that in a month, over one million infected unique IP addresses were identified. Thus, aforementioned statistics present a challenge in determining the actual size of a BredoLab botnet. Two tables in the investigated database are linked directly to the bots and loaders of BredoLab. These tables are used to assist monitoring of active infections of BredoLab via tracking information, such as: timestamps of infection and date of last connection to a C&C server, IP address, country, region and the infected bot GUID. The GUID resembles the serial number of the hard-drive where BredoLab residents. An administration table called "`admtasks`" is, also, identified and is used by the main backend panel and in the administration panel. The "`admtasks`" table is linked to the earlier mentioned malware tasks. "`Admtasks`" is a principal table in administrating active malware tasks and tracking customer information to every task. This includes, customer name, ICQ number of the customer, if found, and all payment details.

A number of 331 malware files dated from July 2009 till October 2010 are extracted from the "`admtasks`" table. Extracted malware files were tested using VTest software in cooperation with Norman IT Security [12]. VTest was recognizing 96% of extracted malware in the database.

Below, are a few examples of the malware samples being used in BredoLab:

- Eighteen malware files were recognized by as Tedroo. Tedroo is known as a malware that is being used to spread spam.
- Nine malware files were being recognized as Zeus or ZBot malware. Zeus is a well-known malware family that is being used for banking cybercrimes.
- More than twenty malware files were recognized as being a fake Anti-Virus program. Fake A/V are used to mislead users into paying money for fake Anti-Virus products.
- Eight files were recognized as BredoLab malware or BredoLab variants.

5 Conclusion and Discussion

Downloader botnets pose a significant challenge to the user and computer security on Internet. A prevalent example of downloader botnet is BredoLab. Although, a significant effort to contain BredoLab's threats by security community and law-enforcement is spent, recent researches showed that BredoLab and its variants are still widely spread. Moreover, complex infection and spreading techniques that are found only in BredoLab malware samples are, unfortunately, now employed in other major malware families [13-14].

To this end, this practical research paper presented a large-scale forensic investigation model that is applied to BredoLab botnet investigation. The proposed model suggested different forensic investigation components to analyze the botnets resources and to extract necessary evidence to assist law enforcement. Furthermore, the paper illustrated the law enforcement procedures to forensically acquire and investigate BredoLab, and to develop required knowledge and control to support prosecution using proposed model. Most take-downs take months or even years of research to attempt a take-down [14,15]. In the case of the Bredolab investigation a wiretap on the VPN server from the main suspect proved to be enough to get the data needed to take-down the botnet and start prosecution. A combination of research in the security community together with law-enforcement might prove the best way to attack these kinds of botnets in the future.

Our future work includes, enhancement to the presented model and integration of security-related research with law-enforcement procedures to provide better countermeasures to cybercrime threats.

Acknowledgement. This work is a result of support provided by the National High Tech Crime Unit from the National Crime Squad part of the Netherlands' Police Agency.

References

1. Schiller, C., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C.: Botnets, the killer web app., pp. 77–85. Syngress Publishing, Canada (2007)
2. Yip, M.: The Underground Economy Ecosystem (2011), `http://www.michaelyip.me.uk/blog/2011/08/the-underground-economy-ecosystem/`
3. Ianelli, N., Hackworth, A.: Botnets as a Vehicle for Online Crime. In: First International Conference on Forensic Computer Science. Carnegie Mellon University, Pittsburgh (2005)
4. Stone-Gross, B., Holtz, T., Stringhini, G., Vigna, G.: The Underground Economy of Spam: A botmaster's perspective of coordinating large-scale spam campaigns. In: 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats. University of California, Santa Barbara (2011)
5. Ligh, M.H., Adair, S., Hartstein, B., Richard, M.: Malware Analyst's Cookbook and DVD, pp. 283–330. Wiley Publishing Inc., Canada (2011)
6. Ligh, M.H., Adair, S., Hartstein, B., Richard, M.: Malware Analyst's Cookbook and DVD, pp. 211–224. Wiley Publishing Inc., Canada (2011)
7. Sancho, S.: You Scratch My Back... Bredolab's Sudden Rise in Prominence. Trend Mirco Inc. (2009)
8. Tenebro, G.: The Bredolab Files. Symantec Corporation (2009)

9. Leaseweb, http://blog.leaseweb.com/2010/08/31/leaseweb-offers-free-web-hosting-to-fight-cybercrime/
10. Abuse.ch The Swiss Security Blog, http://www.abuse.ch
11. National High Tech Crime Unit.: Replay Analyst Toolkit. KLPD, Driebergen (2011)
12. Norman ASA Norway, http://www.norman.com
13. February 2011 Intelligence Report, Bredolab, Zeus and SpyEye stage synchronized, integrated attacks. Symantec Corporation (2011)
14. Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., Vigna, G.: Your Botnet is My Botnet: Analysis of a Botnet Takeover. In: 16th ACM conference on Computer and communications security, pp. 635–647. University of California, Santa Barbara (2009)
15. Dittrich, D.: So You Want to Take Over a Botnet... In: 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats. University of Washington, Seattle (2011)