A Review of ZeroAccess peer-to-peer Botnet

Ms. Cheenu

M.TECH & Graphic Era Hill University
Dehradun India

***Abstract*— Today ZeroAccess is one of the widespread threats over the internet. The total number of infected systems is in the tens of millions with the number of lively infection. ZeroAccess is a Peer-to-peer botnet that affects Microsoft windows operating systems. It is used to download other malware on an infected machine from a Botnet and works as a platform. ZeroAccess is mostly implicated in bitcoin mining and click fraud, while outstanding hidden on a system using rootkit techniques. In this survey, we will explain the Evolution of ZeroAccess Botnet, the life cycle of ZeroAccess Botnet and concludes what are the challenges in ZeroAccess botnet.**

***Keywords*— Botnet, ZeroAccess botnet, Command and Control (C&C).**

I. INTRODUCTION

A bot is a malicious software instance that runs automatically on a compromised computer system without the user's permission. Some group of criminals professionally writes the bot program. A group of bots is known as Botnet that are under the control of attacker. A Botnet is collection of compromised computer systems (zombies) receiving and responding to commands from a server that serves as a meeting mechanism for commands from a botmaster.

To evade detection, the botmaster can optionally employ a number of proxy machines, called stepping-stone between command and control and itself [1].

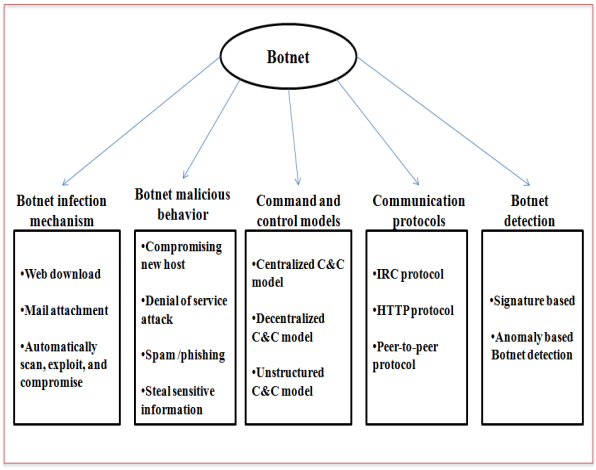

Figure 1: Botnet Taxonomy [1]

The key feature of botnet is its C&C communication, which is categorized in to three categories:

In a centralised architecture of C&C, bots contact the C&C server in order to receive information from the botmaster. Generally, little time is spent in the transmission of a message from the botmaster to all the bots, and this represents one of the major advantages of this architecture. Its disadvantage is the fact that the C&C server constitutes a single point of failure. Thus, if the server shuts down, the complete network is shutdown. Examples of centralised botnets; Eggdrop [2], Gt-Bot and Agobot [3] and Bobax [4].

In a distributed architecture, all the bots in the botnet act simultaneously as servers and clients. This philosophy avoids the existence of a single point of failure, and so this kind of botnet is more resistant than a centralised one. However, the time required for a message to reach all the nodes is much greater than in the centralised case. Example of distributed botnets; Spybot [5], Storm[6], Nugache [7] and Phatbot [8].

Finally, hybrid botnets combine the advantages of the two previous architectures. In this case, there exist one or more distributed networks, each with one or more centralised servers. The disconnection of one of these servers implies, in the worst case, the fall of one of the distributed networks, allowing the rest of the botnet to continue its normal operation. Some examples of hybrid botnets are Torpig [9], Waledac [10] and a new design of botnet proposed by Wang et al. In [11]. More recent and sophisticated hybrid botnets include Alureon/TDL4 [12] and Zeus-P2P.

Table 1: Comparison of P2P botnets

Botnet	Year	C&C Architecture
Slapper [13]	Sep 2002	P2P protocol
Spybot [5]	Apr 2003	Decentralized
Sinit [14]	Sep 2003	Decentralized ,P2P protocol
Nugache [7]	Apr 2006	Decentralized ,Custom protocol
Phatbot [8]	Sep 2004	WASTE- P2P
Minor botnet [15]	Dec 2010	Centralized and distributed, P2P protocol
Kelihos [16]	Dec 2010	Decentralized ,P2P protocol
ZeroAccess [17]	Sep 2011	Decentralized, P2P protocol
TDL-4 [12]	2011	Kad network
THOR	Mar 2012	Decentralized

ZeroAccess (ZA) is one of the peer-to-peer protocols. It is also known as max++, Sirefef [17] and a Trojan malware that

affects windows operating systems. ZeroAccess infected machine will be connected to the P2P network and download plugins and other malwares from a Botmaster. It is mostly implicated in Bitcoin mining and click-fraud, while outstanding unseen on a system using rootkit techniques. The size of zeroaccess botnet is approximately 10's of million infected computers with the number of active infection [18]. It utilizes a peer-to-peer (P2P) mechanism for communication [19]. It is used to make money for the botmaster through click fraud (pay-per-click (PPC) advertising) and bitcoin mining.

II. EVOLUTION OF ZEROACCESS BOTNET

There are two different versions of ZeroAccess: Old version (V1) and new version (V2). Each version of botnet has 32-bit and 64-bit version. It means there are four total number of botnet. The old version (V1) of ZA discovered in May 2011[17]. The new version (V2) of ZA with various modification saw a major redesign of the Trojan's internals, emerged in the summer of 2012. In September, 2013, Zeroaccess V2 is the last modified and most widespread version of the Trojan [20].

Both versions of ZeroAccess communicate with a P2P network on a set of designated ports used to distinguish 32-bit and 64-bit infections. The designated ports for V1 that are used by 32-bit are 21810, 22292, 34354, 34355 and used by 64-bit are 21810, 25700. The designated port for V2 that are used by 32-bit are 16464, 16464 and used by 64-bit are 16470, 16465. All communicating with their infected partners, independently of each other.

There are following four ZeroAccess variants that have been observed:

- ZeroAccess V1- Variant I, II, and III
- ZeroAccess V2- Variant IV

These variant have various different characteristics that are described in detail in the following sections:

In May 2011, the first variant of ZeroAccess was released. It included a rootkit component that was installed as a kernel driver. Hidden files used by the kernel driver and formatted as an NTFS file system and contains core component of zeroaccess. Variant I also included a tripwire driver, which was used to detect important behavioral features of antivirus scanners. In particular, it would check processes for strangely high access counts to the registry. If a process looked at more than fifty service registry key entries in a short period, the process was suspended [21].

The second variant of ZeroAccess was released in July 2012. It also used the rootkit component but modified the way where it covers the core components. It also included tripwire driver. The kernel driver was used the hidden files to allow access. Now these hidden files stored in %Windir%\$KBUnstall [FIVE DIGIT RANDOM NUMBER] $\.

After that in 2012, another variant of zeroaccess (Variant III) was released. It also used the rootkit component but modified the way where it covers the core components same as Variant II. It removed tripwire driver. The kernel driver was used the hidden files to allow access. Now these hidden files stored in %Windir%\$KBUnstall [FIVE DIGIT RANDOM NUMBER] $\ same as Variant II.

The fourth variant of ZeroAccess was released in July 2012 and underwent overhaul. Attacker was shifted code from the kernel mode to user mode [22]. ZeroAccess had developed and with this evolution came a new communication protocol. In this variant of ZeroAccess, C&C protocol also moved away from TCP and instead favoured UDP – a more efficient alternative to TCP for communication. Due to the major change in the design of ZeroAccess became known in the security community as version two (V2) and is referred to as Variant IV in this paper. This is still the most widespread version of ZeroAccess.

In V1, P2P communication was through TCP [23]. Since the release of V2, communication has moved to UDP [19]. In V2's release, the command set was also reduced. Coupled with UDP, this further enhanced the efficiency and resiliency of the communication protocol [24].

Table 2: Difference between V1 and V2

Serial number	ZeroAccess Version1 (V1)	ZeroAccess Version2 (V2)
Year	September 2011	April 2012
Command and Control	P2P	P2P
Encryption	RC4	XOR
Career protocol	TCP	UDP
Size	~30,000	~10 millions
Application	Click fraud, spamming	Click fraud, mining bitcoin
Detection	Antivirus, security vendors	Antivirus, security vendors
Memory residence	Rootkit, Payload	Recycle Bin
Port	Hardcoded	Hardcoded
Infection vector	Exploit kit, drive by download, and social engineering techniques	Exploit kit, drive by download, and social engineering techniques

The modified P2P functionality of ZeroAccess V2 makes its P2P network more flexible and robust against outside manipulation. The newL command of ZeroAccess V2 (2012) is used by ZeroAccess to share directly super nodes IP addresses amongst its peers. When a peer receives, a newL command it adds the built-in IP address within the newL command into its internal peer list. The peer also forwards the newL commands to other peers it knows about, magnifying the message's effect. Due to the newL command and sending it to a ZeroAccess peer, it might be possible to introduce a rascal IP address into an infected internal list of ZeroAccess peer and have that rascal newL command distributed to other ZeroAccess peers. Due to the newL command and small fixed length of internal peer list, some of the botnet are sinkhole [25]. However, the modified P2P ZeroAccess V2 (2013) removed the newL command and allows the botnet to filter out rascal IP address [26].

III. LIFE CYCLE OF ZEROACCESS BOTNET

There are following stages of the life cycle of a zeroaccess Botnet indicates how zeroaccess Botnet spreads its infection and propagates:

A. Stage one: Conception

Conception is the first stage of the life cycle of the zeroaccess botnet or any other botnet. It is important to understand the causes underlying botnet creation, and the common architectures and designs employed.

The first stage of the botnet lifecycle can be divided into following three phases:

- Motivation,
- Design, and
- Implementation

1) *Motivation:* Initially attacker needs a good reason to create a botnet. The motivation of zeroaccess botnet is to make money for the attacker through click fraud (pay-per-click) and bitcoin mining. The Symantec Global Internet Security Threat Report [27] shows a detailed catalogue of prices for botnet services. According to Symantec, the ZeroAccess botnet consists of more than 1.9 million infected computers and is used mainly to perform click fraud and Bitcoin mining in order to generate revenues estimated at tens of millions of dollars per year. Machines involved in Bitcoin mining generate Bitcoins for their controller, the estimated worth of which was estimated at 2.7 million US dollars per year in September 2012 [19]. The machines used for click fraud simulate clicks on website advertisements paid for on a pay per click basis. The estimated profit for this activity may be as high as 100,000 US dollars per day [28], costing advertisers a $900,000 a day in fraudulent clicks [29].

2) *Design:* ZeroAccess botnet uses a distributed architecture in which all the bots in the botnet act simultaneously as servers and clients. This philosophy avoids the existence of a single point of failure, and so this kind of botnet is more resistant than a centralised one. However, the time required for a message to reach all the nodes is much greater than in the centralised case. According to Symantec, No C&C server exists for zeroaccess therefore poses a major challenge for anybody to attempting to sinkhole the botnet [20]. Many botnets present a distributed structure, including Spybot, Storm, Nugache, and Phatbot.

3) *Implementation:* Once the botnet has been conceptually conceived and designed, the last process involved in this stage concerns the implementation of the architecture. This task does not present special characteristics, and can be performed following a traditional software development process.

B. Stage two: Recruitment

Recruitment is the second stage of zeroaccess botnet. The implemented botnet software must be deployed for operation in a real environment. For this purpose, bots must be recruited; indeed, the botmaster's aim is to recruit as many as possible. Note that this question is not unique to botnets, but is found in many cyber attack techniques. Recruitment is also known as infection or propagation.

In ZeroAccess botnet, the bot itself is increase through the ZeroAccess Rootkit through a variety of attack vectors. First infection vector is a form of social engineering, where a user is in no doubt to execute malicious code either by masking it as a legal file, or including it hidden as an additional payload in an executable which announces itself as, for example, bypassing copyright protection (a keygen). A second infection vector utilizes an advertising network in order to have the user click on an advertisement that redirects them to a site hosting the malicious software itself. A third infection vector used is an affiliate scheme where third party persons are paid for installing the Rootkit on a system [23].

The attacker uses an exploit machine to send fake email notification to the victim machine using email attachment. Victim downloads the attachment and receives fake email notification containing malicious URL on its machine by which it gets compromise. Victim machine transmitted to compromised site and then transmitted to malicious site hosting Blackhole exploit kit [30]. Blackhole exploit determines software vulnerability and drops the malware. The fake email notification has a malicious URL received on the victim's machine opens a back door and connects to a command and control (C&C) server, which allows the remote attacker access to the victim machine.

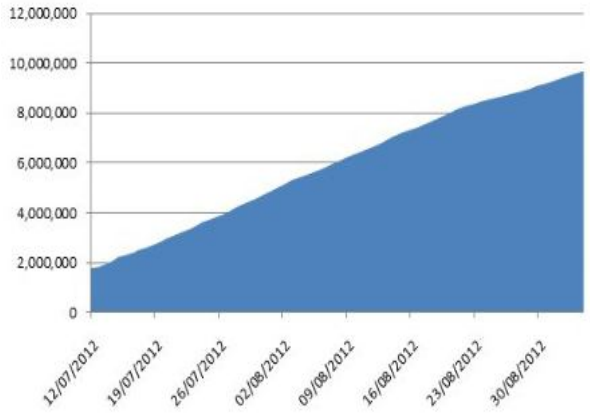

Figure 2: Total number of infected machine [18]

4) *Installation*: ZeroAccess selects randomly one of the computer start drivers and restores it with a completely different malware driver, location its length to that of the original driver. The operating system loads the malware driver instead of the original during system startup. The malware driver loads the original driver from its confidential benefit store. The malware reloads the I/O database to exchange places with the original driver so that the original driver works normally. Once active, the driver prevents disk operations at the lowest layers of the storage stack to present a view of the replaced driver so that it appears normal and cannot be detected by scanning the file. The driver registers a Shutdown

handler, which will repair the malware components on disk. Even if risk images and registry entries are removed, they are restored during shutdown.

Variant III infections are also up to with a malicious shell image [23]. The registry holds an entry similar to;

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\Current Version\Winlogon\ "Shell" = "C:\Documents and Settings\Administrator\Local Settings\Application Data\(any 8-character string)\X"

There is a picture at the path that is called when a user logs in. The picture is capable of re-infecting the system even if the original risk is determined.

Variant IV infections do not contain any kernel components. They are launched from hijacked COM registration entries [19]. For example, HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\ {F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1} changed from C:\WINDOWS\system32\wbem\wbemess.dll to \\.\ globalroot\systemroot\Installer\ {{[RANDOM GUID]}\. HKEY_CURRENT_USER\Software\Classes\clsid\ {42aedc87-2188-41fd-b9a3-0c966feabec1} new key added:

- %User Profile%\Local Settings\Application Data\{[RANDOM GUID]}\

HKEY_CLASSES_ROOT\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1} new key added:

- % User Profile%\Local Settings\Application Data\{[RANDOM GUID]}\n.

Windows 7 and Vista versions also infect the system service image:

- %System%\services.exe

This file is critical to system operation and cannot be removed without rendering the system unbootable.

C. Stage three: Interaction

This stage refers to all the interactions performed during the botnet operation, including the orders sent by the attacker, the messages interchanged between nodes, external communications from the attacker to monitor P2P network information, and the communications of nodes with external servers.

A computer infected with ZeroAccess works as a client and a server in the peer-to-peer network. The infected computer will connect to a peer-to-peer (P2P) network to spread monetization payloads and circulate active peer IP addresses. These monetization payloads carry out the payload functionality and classically perform tasks such as click fraud and Bitcoin mining. The payload of the whole botnet can be altered by seeding new plug-in files into the P2P network.

On the other hand, numerous company and home networks build use of Network Address Translation (NAT) when connecting to the Internet. This results in the local IP address of the computer being different from the IP address that the computer becomes visible to have on the Internet. Devoid of setting exact port forwarding at the firewall or router, inward connections to a ZeroAccess infected computer that is, using NAT to connect to the Internet will not arrive at it. As shown in figure3.

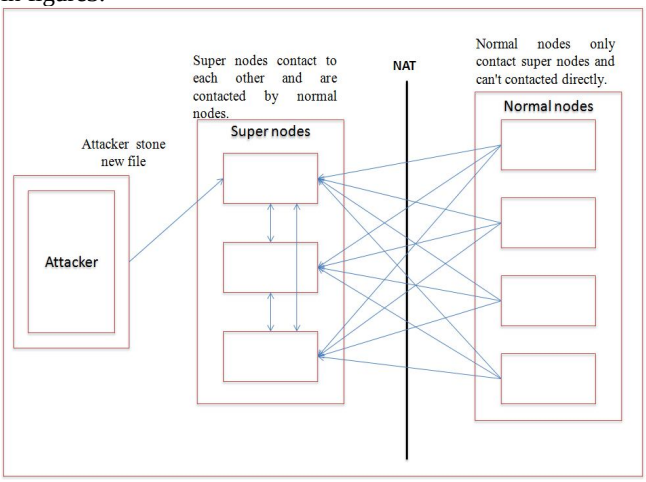

Figure 3: Peer-to-peer protocol overview

Super nodes connects each other and are connected by normal nodes but normal nodes only connect super nodes and cannot be connected directly to the botmaster whose say what the Botnet does by seeding new files onto super nodes that they manage. Super Nodes do the similar action as Normal Nodes in terms of their operation, but they are also answerable for distributing files and IP addresses throughout the botnet. Devoid of Super Node the peer-to-peer, principle would fail [20].

5) C&C communication: When a system infected by ZeroAccess, it has two main objective. The first spread IP addresses and second spread files across the network quickly. Initially each node maintains a list of 256 IP addresses is taken from a dropped file name "@" that is stored in the ZeroAccess folder. ZeroAccess attempts to reach out to each of the IP addresses in succession in order to establish a connection with a peer, retrieve the latest peer list, and join the network. This is done using three commands; getL, retL, and newL.

Table 3: Version 1 and Version 2 supported commands and their description

P2P protocol version V1		P2P protocol version V2	
Commands	**Details**	**Commands**	**Details**
getL	Request for peer list	getL	Request for peer list
retL	Reply to getL command and Includes the list of 256 pairs that initially holds and a list of files and	retL	Reply to getL command. Transmits updated peer list and file metadata information.

	timestamps for each file that it has downloaded.		
getF	Request to file. Download files and store it under hidden folder.	newL	Add new peer list.

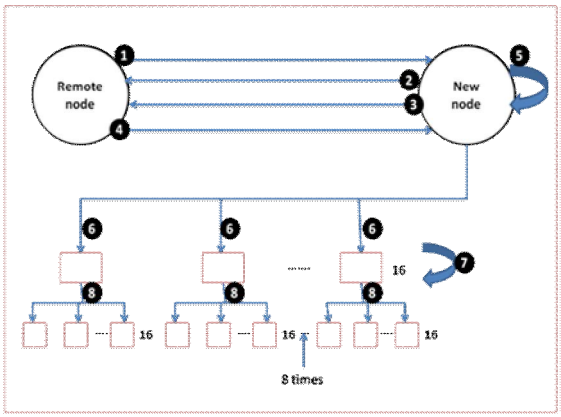

Figure 4: C&C Communication

1. The protocol starts issuing a getL command to the remote peer.
2. The new node then responds with a retL packet, which contains 16 peer IP addresses from new node peers list along with a list of all new node's files that remote node can download. Remote node will add any IP addresses from new node that are newer based on the last contacted timestamp from new node. Remote node may also decide to download files from new node.
3. The New node will transmit a getL+ command to remote (super) node on the normal UDP listening port for the current network (16454, 16455, 16470, or 16471). A getL+ command is the same as a getL command but the difference remote (super) node and new (normal) node.
4. The remote node will respond with a retL+ command to new node. A retL+ command is the same as a retL command but again difference super node and new node. The retL+ command will include 16 peer IP addresses from remote node as well as files that remote node has. New node may replace peers from its list that it received from remote node if they have a lower last contacted timestamp than new node has. New node may also decide to download files from remote node.
5. If new node receives the retL+ response from remote node and since new node originally sent the getL+ command to the normal port for this network, new node knows that remote node is not behind NAT and is likely reachable by other peers. New node checks if remote node's IP address is in its peer list and if not, it is added. In addition, if IP addresses of remote node are not in new node's list, new node will select 16 peers from its list at random.
6. Using the 16 peers selected randomly, new node will send a newL command to those 16 peers with the flag value of the newL command set to eight.
7. Upon receiving the newL command the Random Peer 1 (and any peer that receives the newL commands from new node) will check to see if remote node's IP address is in its list. If remote node's IP address is not in Random Peer1's IP list, it is added. Again, if IP addresses of the remote node are not in Random Peer1's list Random Peer 1 will select 16 peers from its list at random.
8. Using the 16 peers selected randomly, Random Peer 1 will send a newL command to those 16 peers with the flag value of the newL command decremented by one from what it received from new node. This newL propagation will continue until the flag's value reaches zero.

D. Stage four: Attack execution

Once an infected computer has connected to a live peer in the network, it will download monetization or plugin files that carry out the payload functionality of ZeroAccess. These plugin files can be updated at any time and new files can be seeded into the botnet by the attackers. Each files is verified with a 1,024-bit RSA key to prevent a third party seeding the botnet with option files, and each botnet has its own set of plug-ins [19]. There are some monetizations or attacks downloaded by ZeroAccess botnet:

6) Pay per install: Besides the conventional attack vectors, ZeroAccess have also been sold as a service on various underground hacker forums. Originally, ZeroAccess was being sold for US$60,000 for the basic package and up to US$120,000 a year for a more featured version [20]. The customers would be allowed to install their own payload modules on the infected systems.

7) Click fraud: This consists in inducing, by deceit, users to click on online ads or to visit certain websites, and thus either increase third-party website revenues and advertisers budget [31]. The use of botnets makes it possible to simulate the behaviour of millions of legitimate users, and is thus ideal for this kind of attack [32]. Microsoft said that the botnet had been assessment advertisers on Bing, Google Inc and Yahoo Inc an estimated $2.7 million monthly [33].

8) *Bitcoin mining:* Bitcoin mining is stands on performing mathematical operations on computing hardware.

This action has a direct value to the attacker and a cost to innocent victims.

IV. RESEARCH CHALLENGES

E. Detection and mitigation

ZeroAccess selects randomly one of the computer start drivers and restores it with a completely different malware driver, location its length to that of the original driver. The operating system loads the malware driver instead of the original during system startup. The malware driver loads the original driver from its confidential benefit store. The malware reloads the I/O database to exchange places with the original driver so that the original driver works normally. Once active, the driver prevents disk operations at the lowest layers of the storage stack to present a view of the replaced driver so that it appears normal and cannot be detected by scanning the file. The driver registers a Shutdown handler, which will repair the malware components on disk. Even if risk images and registry entries are removed, they are restored again during shutdown.

F. Server takedown

ZeroAccess uses P2P C&C communication architecture that gives the botnet a high degree of availability and redundancy. It does not use any central C&C server that pretences a major challenge for anybody attempting to sinkhole the botnet.

G. Disruption

The modified P2P functionality of ZeroAccess V2 makes its P2P network more flexible and robust against outside manipulation. The newL command of ZeroAccess V2 (2012) is used by ZeroAccess to share directly super nodes IP addresses amongst its peers. When a peer receives, a newL command it adds the built-in IP address within the newL command into its internal peer list. The peer also forwards the newL commands to other peers it knows about, magnifying the message's effect. Due to the newL command and sending it to a ZeroAccess peer, it might be possible to introduce a rascal IP address into an infected internal list of ZeroAccess peer and have that rascal newL command distributed to other ZeroAccess peers. However, the modified P2P ZeroAccess V2 (2013) removed the newL command and allows the botnet to filter out rascal IP address. Therefore, it is difficult to disrupt ZeroAccess botnet.

V. CONCLUSIONS

ZeroAccess is one of the widespread threats over the internet. The total number of infected systems is in the tens of millions with the number of lively infection. ZeroAccess is a Peer-to-peer botnet that affects Microsoft windows operating systems. It is used to download other malware on an infected machine from a Botnet and works as a platform. ZeroAccess is mostly involved in bitcoin mining and click fraud, while outstanding hidden on a system using rootkit techniques. It used a UDP carrier protocol and port hardcoded into the bot binaries. Currently its C&C communication channel uses only two commands getL and newL. We have concluded research challenges of ZeroAccess botnet from this survey.

ACKNOWLEDGMENT

I would like to thank my supervisors Mr. Ramesh Singh Rawat, Assistant Professor, Dept. of GEU, Dehradun. I would also like to thanks Mr. Deepak Singh Rana, Assistant Professor, Dept. of GEHU, Dehradun for helpful guidance during the work.

REFERENCES

[1] S. Khattak, N. Ramay, K. Khan, A. Syed, and S. Khayam, "A Taxonomy of Botnet Behaviour, Detection, and Defense," *Communications Surveys & Tutorials, IEEE*, vol. PP, pp. 1-27, 2013.

[2] C. Elliott, "Botnets: To what extent are they a threat to information security?," *Information Security Technical Report*, vol. 15, pp. 79-103, 2010.

[3] L. Jing, X. Yang, G. Kaveh, D. Hongmei, and Z. Jingyuan, "Botnet: classification, attacks, detection, tracing, and preventive measures," *EURASIP journal on wireless communications and networking*, vol. 2009, 2009.

[4] J. Stewart, "Bobax trojan analysis," *SecureWorks, May*, vol. 17, 2004.

[5] C. Li, W. Jiang, and X. Zou, "Botnet: Survey and case study," in *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on*, 2009, pp. 1184-1187.

[6] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study," in *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, 2007, pp. 1-1.

[7] S. Stover, D. Dittrich, J. Hernandez, and S. Dietrich, "Analysis of the Storm and Nugache Trojans: P2P is here," *USENIX; login*, vol. 32, pp. 18-27, 2007.

[8] J. Stewart, "Phatbot trojan analysis," *Retrieved from Secure Works: http://www. secureworks. com/research/threats/phatbot*, 2004.

[9] B. Stone-Gross, M. Cova, B. Gilbert, R. Kemmerer, C. Kruegel, and G. Vigna, "Analysis of a botnet takeover," *Security & Privacy, IEEE*, vol. 9, pp. 64-72, 2011.

[10] G. Sinclair, C. Nunnery, and B.-H. Kang, "The Waledac protocol: The how and why," in *Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on*, 2009, pp. 69-77.

[11] P. Wang, L. Wu, B. Aslam, and C. C. Zou, "A systematic study on peer-to-peer botnets," in *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on*, 2009, pp. 1-8.

[12] E. Rodionov and A. Matrosov, "The evolution of tdl: Conquering x64," *ESET, June*, 2011.

[13] I. n. Arce and E. Levy, "An analysis of the slapper worm," *Security & Privacy, IEEE*, vol. 1, pp. 82-87, 2003.

[14] J. Stewart, "Sinit P2P trojan analysis," *Web publication. Available at URL: http://www. secureworks. com/research/threats/sinit*, 2003.

[15] T. Werner, "The Miner Botnet: Bitcoin Mining Goes Peer-To-Peer," 2011.

[16] T. Werner, "Botnet Shutdown Success Story: How Kaspersky Lab Disabled the Hlux/Kelihos Botnet," September, 2011.

[17] "Trojan.Zeroaccess | Symantec," *http://www.google.co.in/url?q=http://www.symantec.com/security_response/writeup.jsp%3Fdocid%3D2011-071314-0410-99&sa=U&ei=o19sU4-mOdCWuASZ8YCIDq&ved=0CCgQFjAB&usg=AFQjCNFsvAx3Lrt_OFMJmLSdp8vV2ktpDA*, July 13, 2011.

[18] J. Wyke, "BACK CHANNELS AND BITCOINS: ZeroAccess€™SECRET C&C COMMUNICATIONS," *http://www.sophos.com/es-*

es/medialibrary/PDFs/technical%20papers/Wyke-VB2013.pdf, 2013.

[19] J. Wyke, "The ZeroAccess Botnet: Mining and Fraud for Massive Financial Gain.," *Sophos Technical Paper: ZeroAccess Botnet-Mining and Fraud for Massive Financial Gain*, 2012.

[20] A. Neville and R. Gibb, "ZeroAccess Indepth (Symantec Corporation White Paper)," 2013.

[21] M. Giuliani, "ZeroAccess Rootkit Guards Itself with a Tripwire," http://www.webroot.com/blog/2011/07/08/zeroaccess-rootkit-guards-itself-with-a-tripwire/, July 8th, 2011

[22] J. Wyke, "Major shift in strategy for ZeroAccess rootkit malware, as it shifts to user-mode," http://nakedsecurity.sophos.com/2012/06/06/zeroaccess-rootkit-usermode/, June 6, 2012.

[23] J. Wyke, "The ZeroAccess rootkit | Naked Security," http://www.google.co.in/url?q=http://nakedsecurity.sophos.com/zeroaccess2/&sa=U&ei=o19sU4-mOdCWuASZ8YCIDq&ved=0CC8QFjAC&usg=AFQjCNGqo82wZAWAGFmBz249QvROyjHT7A, 2011.

[24] "ZeroAccess Modifies Peer-to-Peer Protocol for Resiliency," http://www.symantec.com/connect/blogs/zeroaccess-modifies-peer-peer-protocol-resiliency, 20 Aug 2013.

[25] R. Gibb, "Sinkholing the Zeroaccess botnet," http://www.virusbtn.com/pdf/conference_slides/2013/Gibb-VB2013.pdf, 2013.

[26] R. Gibb, "ZeroAccess Modifies Peer-to-Peer Protocol for Resiliency," http://www.symantec.com/connect/blogs/zeroaccess-p2p, 20 Aug 2013.

[27] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf, 2010.

[28] S. Ragan, "Millions of Home Networks Infected by ZeroAccess Botnet," http://www.securityweek.com/millions-home-networks-infected-zeroaccess-botnet, October 31, 2012.

[29] J. E. Dunn, "ZeroAccess bot has infected 2 million consumers, firm calculates. Techworld.," http://www.pcadvisor.co.uk/news/security/3408841/zeroaccess-bot-has-infected-2-million-consumers-firm-calculates/, 2 November 2012.

[30] F. Howard, "Sophos Technical Paper: Exploring the Blackhole Exploit Kit," http://sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf, 2012.

[31] K. C. Wilbur and Y. Zhu, "Click fraud," *Marketing Science*, vol. 28, pp. 293-308, 2009.

[32] N. Daswani and M. Stoppelman, "The anatomy of Clickbot. A," in *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, 2007, pp. 11-11.

[33] T. Reuters, "Huge ZeroAccess botnet disrupted by Microsoft," http://www.cbc.ca/news/technology/huge-zeroaccess-botnet-disrupted-by-microsoft-1.2453707, Dec 06, 2013.