ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Preventing DNS Queries Against DDOS Attack

P.Soniya[1], Mrs.S.Rajeswari[2]

Student/M.E (CSE), Sri Shanmugha College of Engineering & Technology, Tamilnadu, India[1]

AP, Dept. of CSE, Sri Shanmugha College of Engineering & Technology, Tamilnadu, India[2]

ABSTRACT: The botnet controllers prevented to the block malicious from the attacking the network. The stealthy messaging system using botnet controllers protect the privacy which allows multiple entities to pass messages stored secure DNA records. The botmaster to communicate bots of receive new attack commands and updates from the botmaster. The DNS factors of preventing the development of effective large-scale, stealthy botnet command and control, wide-area botnet detection systems are seemingly contradictory. The DNS monitoring the perfect stealth of communication channel, performing comprehensive statistical Analysis, signs that indicate that a certain name is used as part of a malicious operation.IRC bots usually have a way to remotely upgrade victims with new payloads to stay ahead of security efforts. Quantitatively analyze several techniques describe that can be used to hide malicious DNS activities both at the host and network levels. We also present and experimentally evaluate statistical content-analysis Techniques as a countermeasure, which require deep packet inspection. Finally, we provide an extensive evaluation real-world networks, can be secure powerful botnet attacks. Future work defenders of direction complementary to host-based malware detection and prevention solutions, such as the cryptographic provenance verification technique.

I. INTRODUCTION

The botnet is widely used when several IRC bots have been linked and may possibly set channel modes on other bots and users while keeping IRC channels free from unwanted users. This is where the term is originally from, since the first illegal botnets were similar to legal botnets. A common bot used to set up botnets on IRC is egg drop. Botnets sometimes compromise computers whose security defenses have been breached and control conceded to a third party. Each such compromised device, known as a "bot", is created when a computer is penetrated by software from a *malware* (malicious software) distribution. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as IRC and Hypertext Transfer Protocol (HTTP).

The term "botnet" can be used to refer to any group of computers, such as IRC bots, but the term is generally used to refer to a collection of computers (called zombie computers) that have been recruited by running malicious software. A botnet's originator (known as a "bot header" or "bot master") can control the group remotely, usually through an IRC, and often for criminal purposes. This server is known as the command-and-control (C&C) server. Though rare, more experienced botnet operators program command protocols from scratch. These protocols include a server program, a client program for operation, and the program that embeds the client on the victim's machine. These communicate over a network, using a unique encryption scheme for stealth and protection against detection or intrusion into the botnet.

1.1 Introduction about Domain

A bot typically runs hidden and uses a covert channel (e.g. the RFC 1459 (IRC) standard, Twitter, or IM) to communicate with its C&C server. Generally, the perpetrator has compromised multiple systems using various tools (exploits, buffer overflows, as well as others; see also RPC). Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerability a bot can scan and propagate through, the more valuable it becomes to a botnet controller community. The process of stealing computing resources as a result of a system being joined to a "botnet" is sometimes referred to as scrimping.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Botnet servers are typically redundant, linked for greater redundancy so as to reduce the threat of a takedown. Actual botnet communities usually consist of one or several controllers that rarely have highly developed command hierarchies; they rely on individual peer-to-peer relationships. Advanced topology is more resilient to shutdown, enumeration or discovery. However, some topologies limit the marketability of the botnet to third-parties. Many botnet operators used the Internet Relay Chat protocol (IRC) or HTTP servers to pass information. Botnet operators constantly explore new stealthy communication mechanisms to evade detection. HTTP-based command and control is difficult to distinguish from legitimate web traffic. The feasibility of email as a stealthy botnet command and control protocol was studied by researchers and systematically investigates the feasibility of solely using Domain Name System (DNS) queries for botnet command and control. DNS provides a distributed infrastructure for storing, updating, and disseminating data that conveniently fits the need for a large-scale command and control system. The HTTP protocol is for the end-to-end communication between a client and a server. In comparison, DNS provides not only a means of communication between computers, but also systematic mechanisms for naming, locating, distributing, and caching resources with fault tolerance. These features of DNS may be utilized to fulfill a more effective command-and-control system than what HTTP servers may provide.

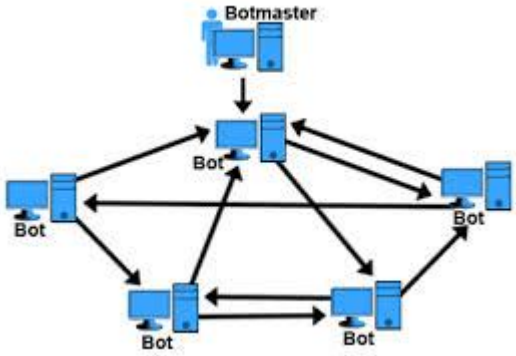

Fig 1.1 Botmaster

The decentralized nature of DNSs with a series of redundant servers potentially provides an effective channel for covert communication of a large distributed system, including botnets. Some botnets implement custom versions of well-known protocols. The implementation differences can be used for detection of botnets. A botnet server structure that lacks redundancy is vulnerable to at least the temporary disconnection of that server. Some newer botnets are almost entirely P2P, with command-and-control embedded into the botnet rather than relying on C&C servers, thus avoiding any single point of failure and evading many countermeasures. Commanders can be identified just through secure keys and all data except the binary itself can be encrypted. A large botnet that learns it is being studied can even attack those studying it. Researchers at Sandia National Laboratories are analyzing botnets behavior by simultaneously running one million Linux kernels as virtual machines on a 4,480-node high-performance cluster. The internet by its inherent characteristic, comprise of finite resources and attackers have traditionally exploited this by exhausting computer & network services with illegitimate requests, thereby denying the legitimate access to these services. The model for denial of service attack has evolved from single attacker machine against single target machine to multiple attacker machines flooding requests to single target. The later DDoS model was refined by attackers by using multiple handlers for directing & managing large number of hosts against a single target. The tools & technology for denial of service attack has evolved over a period of time, they are readily available & easy to use. Controlled Trojans & direct them against DDoS targets via handlers, as the most common attack technique. Interestingly, the use of handler to manage & direct large number of zombie hosts (infected systems under attacker control) has in recent years, largely been replaced by Internet Relay Chat (IRC) networks, acting as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

attacker's virtual command & control centers. Activities & evade detection in disguise of legitimate IRC traffic. The infected hosts connect to attacker hosted IRC channels called "bots "& network of these Bots connect to an IRC channel forms a "botnet".

1.2 Drawbacks

- DNS sensitive data access is not controlled
- Data leaks are not accurately detected
- User intention is required for anomaly detection
- Detection latency is high

II. SCOPES

The DNS query based attack detection scheme is enhanced to provide to the system. Navy Bayesian classification technique is integrated to the system. Small query analysis mechanism is integrated with the system. The DNS query based attack detection scheme is enhanced to provide privacy preserved data traffic analysis. Automated anomaly detection is adapted to the system.

2.1Modules

- Communication channel
- stealthy messaging systems
- botnet attacks
- monitoring the attacks
- controlling and detection of attacks

2.1 Advantages

- DNS sensitive data access is controlled
- Data leaks are accurately detected
- Automated anomaly detection
- Detection latency is minimized

III. CONCLUSIONS

The botnet attacks inspired by anomalous DNS behavior, we stepped into a whole new kind of botnet C&C. This shows that even though many bot families use IRC or HTTP C&C, malware authors still find new ways of instructing their bots. It is obvious that DNS C&C moves botnet C&C one step further into the direction of covert communication. The detection of such botnet C&C even when covert, remains possible.

REFERENCES

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[1] L. Bilge, E. Kirda, C. Krueger, and M. Balduzzi, "Exposure: Finding Malicious Domains Using Passive DNS Analysis," Proc. 18th Ann. Network and Distributed System Security Symp. (NDSS), Feb. 2011.

[2] P. Butler, K. Xu, and D. Yao, "Quantitatively Analyzing Stealthy Communication Channels," Proc. Ninth Int'l Conf. Applied Cryptography And Network Security (ACNS '11), pp. 238-254, 2011.

[3] D. Dagon, "Botnet Detection and Response, the Network Is the Infection," Proc. Domain Name System Operations Analysis and Research Center Workshop, 2005.

[4] DeNiSe, http://c0re.23.nu/c0de/snap/DeNiSe-snap-20021026. tar.gz, 2013.

[5] C.J. Dietrich, C. Rossow, F.C. Freiling, H. Bos, M. van Steen, and N. Pohlmann, "On Botnets that Use DNS for Command and Control," Proc. European Conf. Computer Network Defense, Sept. 2011.

[6] Anti-Spam Resource Center—DomainKeys, http://antispam.yahoo.com/domain keys, 2008

[7] M.T. Goodrich, R. Tamassia, and D. Yao, "Accredited Domain- Keys: Service Architecture for Improved Email Validation," Proc. Conf. Email and Anti-Spam (CEAS '05), July 2005.

[8]M.V.Horenbeeck,"DNS Tunneling," http://www.daemon.be/ Maarten/dnstunnel.html, 2013.

[9] X. Hu, M. Knysz, and K.G. Shin, "Measurement and Analysis of Global IP-Usage Patterns of Fast-Flux Botnets," Proc. 30th Ann. Int'l Conf. Computer Comm. (INFOCOM), 2011.