Nonlinear Phenomena in Complex Systems, vol. **17**, no. 3 (2014), pp. 290 - 295

Efficiency Estimation of the Protection Software for Neutralization and Elimination of Botnets

D. P. Zegzhda and T. V. Stepanova
Saint-Petersburg State Polytechnic University,
29 Politechnicheskaya Str, 195251 Saint-Petersburg, RUSSIA
(Received 21 March, 2014)

Today there are no methods to evaluate protection effectiveness that would allow comparing defense and botnet attacks in particular. A set of metrics for efficiency evaluation has been proposed. The proposed efficiency evaluation metrics account for the network nature of modern defense and attack. They will provide quantitative assessment of factors affecting defense or attack efficiency. Therefore, these metrics will allow making a conclusion about results of the network contradiction between benign and malignant agents, and about LAN and WAN protection nodes.

AMS Subject Classification: 05C80, 05C90
Keywords: botnet, efficiency, neutralization, metric

1. Introduction

Botnets are by far one of the most significant threats to the Internet. It has been estimated that approximately one quarter of all computers providing the Internet access are various botnet nodes, and its number is still growing [1]. According to statistics [2] the total number of computers belonging to at least one botnet increased up to 6 times in 2011 (figure 1), new unique botnets showed an increase of 8 per cent every week.

Unlike central attack, botnets organization of distributed attack offers a number of advantages for an attacker. First of all, intrusion detection system impedes attack detection, as there is no conventional attack pattern: every single action is not necessarily an attack. Secondly, with the growing number of exposure sources the attack efficiency is increasing and the localization of all the sources is being hampered.

Botnets agents are different from all other types of malicious software, they work as one coordinated group of attack elements. Those computers that belong to a botnet are infected with various types of malware: viruses, Trojan horse, and worms. Attack agent networks are made to:

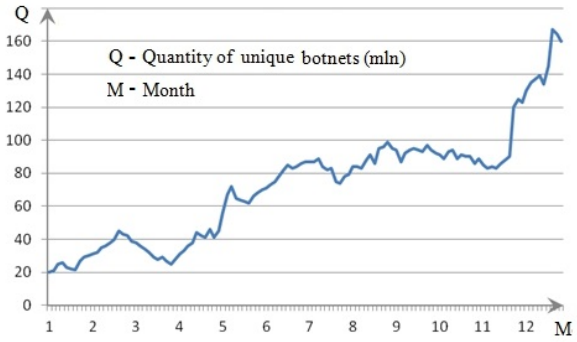

FIG. 1. The growth in the total number of unique botnets in 2011.

1. collect data (authentication, personal, confidential);
2. organize attacks against other host systems aimed at denial of service;
3. send junk e-mails.

Their target objects are:

1. home/corporate computers;
2. servers;
3. network hardware (commutators, routers, modems) [3].

It was necessary to change architecture into a distributed one in order to resist distributed attacks. Distributed protection consists of interrelated defense agents installed on different hosts; these agents allow to gain "promising" overview of the system being defended. Distributed architecture also enhances protection stability against distributed attacks.

Methods of botnets resistance are divided into two groups [4, 5]:

1. Proactive methods. They are aimed at botnet elimination until it is used for attack organization. Proactive methods are applied to complete the following tasks:

– botnet nodes neutralization, that is, elimination of botnet operating load;

– resistance to botnet distribution, which will not allow to cut the likelihood of attack but to reduce its effectiveness;

– detection and neutralization of botnet owner or operator;

– disablement of system control areas;

– avoiding any advantages for a botnet manager (for example, blocking out unauthorized advertising of the programmes that are installed together with a botnet).

2. Reactive methods. They are aimed at "operating load" resistance that is implemented by botnet nodes. Reactive methods are applied to complete the following tasks:

– protection against distributed attacks of service denial;

– protection against junk e-mails;

– protection against "click fraud" and other attacks of that kind;

– protection against espionage, spreading of scumware, personal/confidential data leakage.

The optimal level of protection is likely to increase by the combination of different methods mentioned above. One of the most obvious examples illustrating proactive methods application is antivirus software. It allows detecting and neutralizing botnet nodes. Reactive methods are used in intrusion detection system.

Both botnets and distributed protection represent dynamically developing agent networks installed on different computers and interacting with each other. Attack and defense agent networks are represented in the following way. Network evolution dynamics involves network connection of new agents (host infection, new botnets installation, protection agents installation on new hosts) and elimination of the present agents (protection agent may be disconnected by a botnet or quite the opposite a botnet may be eliminated by protection agent). Exposure vectors of these two confronting network types are directed to each other, that is, there is a contradiction of control over computers between two network types. Both of them are aimed at completing two main tasks: to maintain its own interconnectivity in order to implement the operating load and to eliminate its attacker network interconnectivity and neutralize agents of that network. So, operating benefits are determined by completing these two tasks. It is necessary to study different characteristic features of these networks in order to analyze operating benefits efficiency of network agents.

2. Agent networks classification

Agent network identifies three types of nodes:

1. Operations centre – that is a node responsible for distributing operations in network.

2. Ordinary node – the one that implements operations from operations centre.

3. Operator computer – that is a node responsible for operator commands, for diagnostics and configuration.

In general, one node may have a compound type – for example, both distributing and implementing commands. Connection patterns of nodes are divided into three groups:

1. Centralized network (figure 2a). In networks with this architecture all the agents connect with only one operation centre. The centre waits for new agents connection, register them in its database, monitor them and send its commands that can be generated by both operator and automatically.

2. Hybrid network (figure 2b). This one is an improved type of network with one centre.
In this case, network is divided into subnetworks in which each subnetwork is a network with one single centre. Subnetwork centres are given commands from the centre and distribute these commands to the agents of its subnetwork.
3. Decentralized network (figure 2c). In this network agents connect with several
computers – neighbors. Any node that is connected to an operator's computer can be used as an operation centre. Commands are transmitted from one agent to another: every agent has its neighbors addresses and when it is given a command from one of them, it sends the command to others, providing the command distribution.

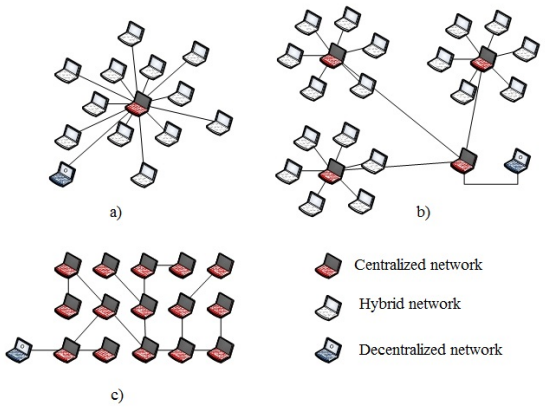

FIG. 2: Agent networks architecture (in color).

Agent networks may also be classified according to two characteristics:

1. Information volume regarding agents in network.

-Every host has information about all the network agents. Every node is aware of any other agent in the network; when making new nodes of information the information is spread to the present nodes, the same procedure is typical of nodes while its eliminating. Examples of nodes of that type are given in [6, 7]. This approach is applied to networks with a small number of agents.

-Every node has information about all the operations centres.

-Every node has information about some subset of numerous network agents.
The size of this subset can be both fixed and unfixed. In effect, these networks are more resistant to attacks.

2. Algorithm for network construction between nodes. The simplest options: random sampling, lists of addresses attached to the node code. These methods do not account for coupling parameters – network capacity, safety, but in effect, they are put in practice [8–10].

Most part of modern botnets have hybrid or decentralized architecture and are characterized by partial information awareness of network agents (botnets Nugache, Zindos, Zeus, TDL-4). Typical organization architectures of modern botnets:

– small world graph where most botnets are linked only to the nearest neighbors;

– random graph where couplings are formed randomly;

– scale-free graph being a graph in which vertex degrees are formed according to power function, that is, distribution function for k vertices is asymptotically proportional to $k^{-\gamma}$ (with some parameter γ); therefore, graph contains a small number of nodes and a large number of couplings.

Most part of agent protection networks have centralized architecture with one master node and many subordinate nodes (computer security packets: F-Secure Antivirus, ESET Nod32 Antivirus) or hybrid architecture with a small number of master nodes and a large one of subordinate nodes (corporate network security packets: Dr.Web Enterprise Suite, ESET NOD32 Antivirus 3.0, ESET Smart Security, Kaspersky Anti-Spam). It is necessary to have a set of characteristics that will allow estimating efficiency of methods and algorithms for both protection and attack in order to compare operating benefits of attack and protection agent

networks, which is aimed at security evaluation of Usenet. Nowadays many different metrics are used for botnets and protection evaluation.

3. Methods of efficiency evaluation of operating agent network

Existing approaches to efficiency evaluation of botnets offer various metrics for networks of different application (see table 1) [11]. Firstly, according to this fact, it is impossible to compare operating benefits of various botnets. Secondly, unified metrics that are used do not allow comparing operating benefits of attack and protection agent networks.

Many different metrics are used for efficiency evaluation of protection, but they do not allow for the network nature of protection organization and therefore do not enable comparing efficiency evaluation of both protection and attack. The most commonly used metrics are shown in table 2.

4. Approach offered to evaluate operating benefits of agent networks

It is necessary to take into account the following factors in order to compare operating benefits of attack and protection agent networks, which is aimed at security evaluation of Usenet:

1. Network ability to exist in harmful environment created by attacker network. In this case, network nodes must respond to control instructions.

2. Network ability to maintain its connectivity even if a number of network nodes become faulty (for example, in the case of other network attack), and when a large number of new nodes connect to the network (in the case of nodes restoring to working condition after attack).

3. Network ability to perform its functions regardless of the number of managed nodes. The network must remain unchanged after the attack even if most part of its nodes become faulty, and when management of a large number of agents is needed – for example, while the network resisting, especially the one that has many agents.

4. Agent network influence coefficient on LAN, on which it is based: the rate to which processing speed of LAN nodes is lowered, and data transmission between its nodes is slowed down. This coefficient also defines probability of agent network detection.

5. Network ability to resist data capture and modification by the attacker network.

Usually, crypto-algorithms for crypto-operation and traffic digital signature, validation of received data are used for this purpose.

Agent network properties can be represented using the following formal characteristics:

– controllability;
– fall-over protection;
– operation constancy;
– scalability;
-imitation resistance.

To estimate each of these properties the following metrics can be used:

1. controllability $C(t)$ is a percentage of currently managing nodes (that respond to operator actions). This metric shows network viability.

2. Fall-over protection R_{max} is a part of network nodes after elimination of which controllability drops up to 0. This metric shows a network ability to operate properly under conditions of mass registration or deactivating of nodes in general and master ones in particular.

3. Operation constancy $\frac{\partial^2 V}{\partial n_{del}^2}$ is the acceleration of traffic volume change that is processed by a network node per unit time depending on network instability level where $V(n_{del})$ is traffic volume. This metric shows agent network operation influence on ordinary operation of LAN, where n_{del} is the number of deleted nodes.

4. Scalability M defined as three component vector $\left(\sigma C_{(k,n)}(t), \sigma R_{(k,n)}, \sigma V_{(k,n)} n_{del}\right)$

Table 1: Existing metrics for efficiency evaluation of operating botnets.

Purpose of botnet	**Metrics being applied**	**Comments**
Attack organization of service denial	Large graph component scale of botnet couplings	If there are more reachable nodes in graph, the more nodes will then be involved in attack organization
Precipitous attack organization (spam, clickfraud, auction fraud)	Graph diameter of botnet couplings	Nodes must provide with an opportunity for cheating a large number of routes
Local resources consumption (storage of illegitimate date, software cracking of lock words	Local botnet node transitivity	If nodes are used for data storage, fallover protection is then needed
Henetal botnets	Level of botnet connectivity $C(p)$ defined as a ratio of a number of nodes in connected subgraph to a number of other nodes	Metric shows network ability to resist nodes alimination

Table 2: Existing metrics for efficiency evaluation of protection.

Metric being applied	**Comments**
Numbers of type I errors	Numbers of false activations
Numbers of type II errors	Numbers of missing events (attacks, etc.)
System coverage ration according to corporate and international standards	Level of system compliance (incompliance) with corporate and international standards
Number of vulnerabilities during a certain period of time (month, quarter, year)	
Number of vulnerabilities that are eliminated during a certain period of time (month, quarter, year)	

of dispersions of controllability, fall-over protection and operation constancy. Here the subscript $(k,\ n)$ was introduced for these metrics to describe a network with capacity from k up to n nodes. This metric shows a network ability to perform its functions properly with both a small and large number of nodes.

5. Imitation resistance is the resistance of crypto-algorithms being applied. This metric evaluates network resistance to control capturing by outsiders.

5. Conclusion

The proposed method of efficiency evaluation of agent networks uses metrics regardless of the agent networks purpose. The properties mentioned above fully describe agent networks operation and make it possible to compare operating benefits of various botnets, protection, botnets neutralization and elimination, and effectiveness of the botnets resistance to various security tools.

References

[1] D. Harley, A. Lee, C. Borghello. *Net of the Living Dead: Bots, Botnets and Zombies*, http://go.eset.com/us/resources/white-papers/Net_Living_Dead.pdf.

[2] *Damballa – Top 10 Botnet Threat Report.* (Damballa Inc., 2011).

[3] A. Nusca, *'Psyb0t' worm infects Linksys, Netgear home routers, modems.* (2009).

[4] S.M. Kuitert. *War on Botnets. Botnet Defense Research Surveyed.* (2010).

[5] D. Plohmann, E. Gerhards-Padilla, F. Leder. *Botnets: Detection, Measurement, Disinfection & Defence.* (2011).

[6] K. Birman, M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu, and Y. Minsky. *Bimodal multicast.* (ACM TOCS, 1999).

[7] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry. Epidemic algorithms for replicated database maintenance. In: *Proc. of the 6th PODC, 1987.* Pp. 1–12,

[8] A.J. Ganesh, A.-M. Kermarrec, L. Massouli. SCAMP: Peer-to-peer lightweight membership service for large-scale group communication. In: *Networked Group Communication*, 2001. Pp. 44–55.

[9] S. Voulgaris, D. Gavidia, M. Steen. Cyclon: Inexpensive membership management for unstructured P2P overlays. Journal of Network and Systems Management. **13**, 197–217 (2005).

[10] J. Leitao, J. Pereira, L. Rodrigues. HyParView: A membership protocol for reliable gossip-based broadcast. In: *Proc. of the 37th DSN, 2007.* Pp. 419–429.

[11] D. Dagon, G. Gu, C. Zou, J. Grizzard, S. Dwivedi, W. Lee, R. Lipton. *A Taxonomy of Botnets.* (2010).